

Cisco IQ Virtual Appliance 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 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 u in staat stelt proactieve, geïnformeerde beslissingen te nemen en processen te stroomlijnen voor klantbetrokkenheid en succes.

Cisco IQ On-Prem Air-Gapped is een van de implementatiemodi van Cisco IQ, ontworpen voor klanten in sterk gereguleerde industrieën met strenge compliance, gegevenssoevereiniteit en beveiligingsvereisten. In deze modus wordt Cisco IQ geleverd als een op zichzelf staande virtuele machine (VM), aangeduid als de Cisco IQ Virtual Appliance (VA). De VA draait volledig op het terrein van de klant en opereert volledig geïsoleerd van externe netwerken. Om deze isolatie te behouden, worden software-updates en onderhoudspakketten verkregen van Cisco IQ SaaS en overgedragen aan de VA via een goedgekeurd, handmatig proces.

Cisco IQ On-Prem Air-Gapped breidt de belangrijkste mogelijkheden van Cisco IQ SaaS uit naar air-gapped omgevingen, waardoor bedrijfskritieke teams kunnen werken met snelheid en diagnostische intelligentie die vergelijkbaar is met cloud-verbonden ondernemingen.

Om toegang te krijgen tot de Cisco IQ VA, opent u een ondersteunde browser en navigeert u naar <https://<fqdn-of-the-appliance>>. Meld u aan met de gebruikersnaam en het wachtwoord van de beheerder die tijdens het installatieproces zijn ingesteld.

 **Opmerking:** De Cisco IQ VA is momenteel beperkt tot klanten die zijn ingeschreven voor het Controlled Availability-programma. Downloadtoegang voor de VA-systeemsoftware en aanvullende operationele pakketten (modules, regels en rechten) van het Cisco IQ-portaal is uitsluitend beschikbaar voor geselecteerde klanten. Neem contact op met uw accountvertegenwoordiger voor meer informatie.

Verbindingsbeheer (gegevensverzameling)

Cisco IQ VA is een on-premises oplossing voor het verzamelen van netwerkgegevens om een

diep inzicht 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 bestaat uit:

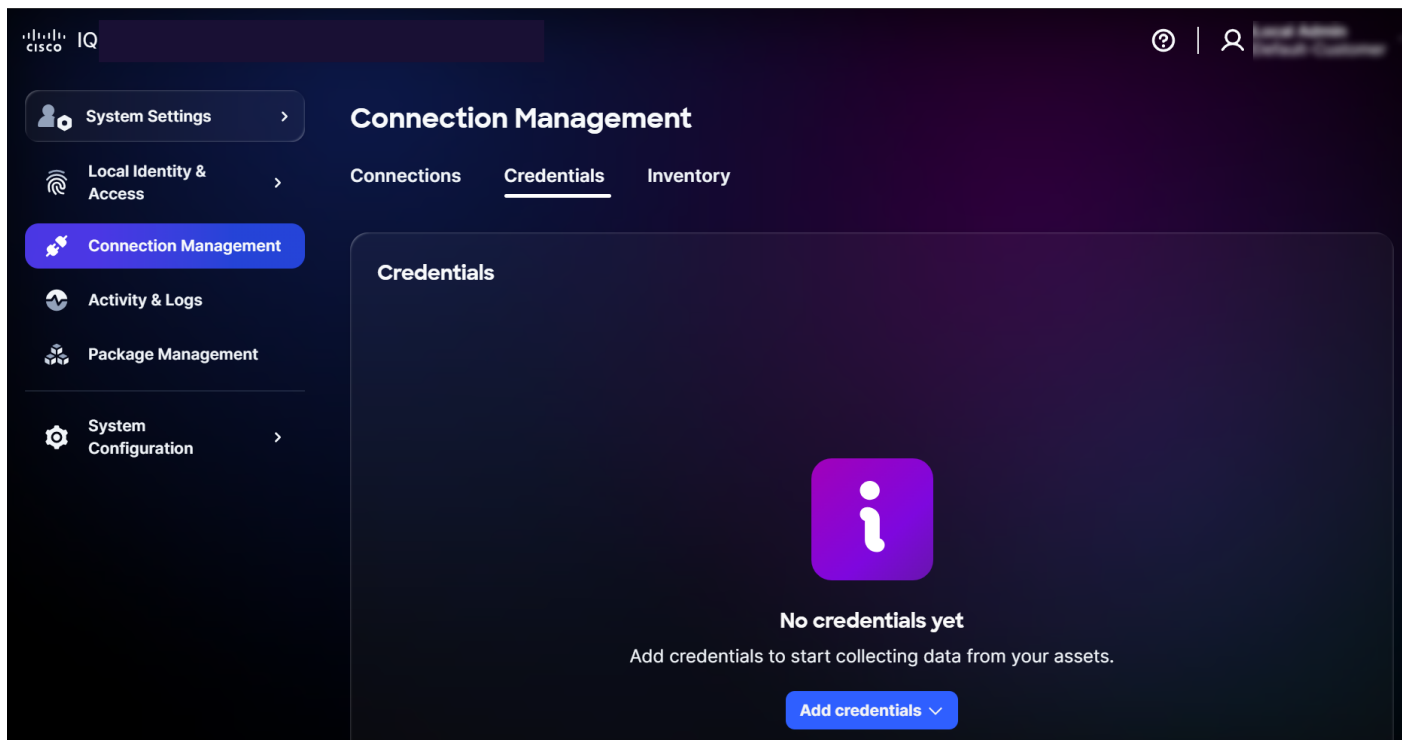
- Credential Sets maken: stel de verificatieprotocollen vast (bijvoorbeeld Simple Network Management Protocol (SNMP) v1/v2c/v3) om te communiceren met uw netwerkapparaten. Door inloggegevens te centraliseren op beveiligingszone of -locatie (bijvoorbeeld "SanJose-SNMPv3") kunt u wachtwoorden op één locatie 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

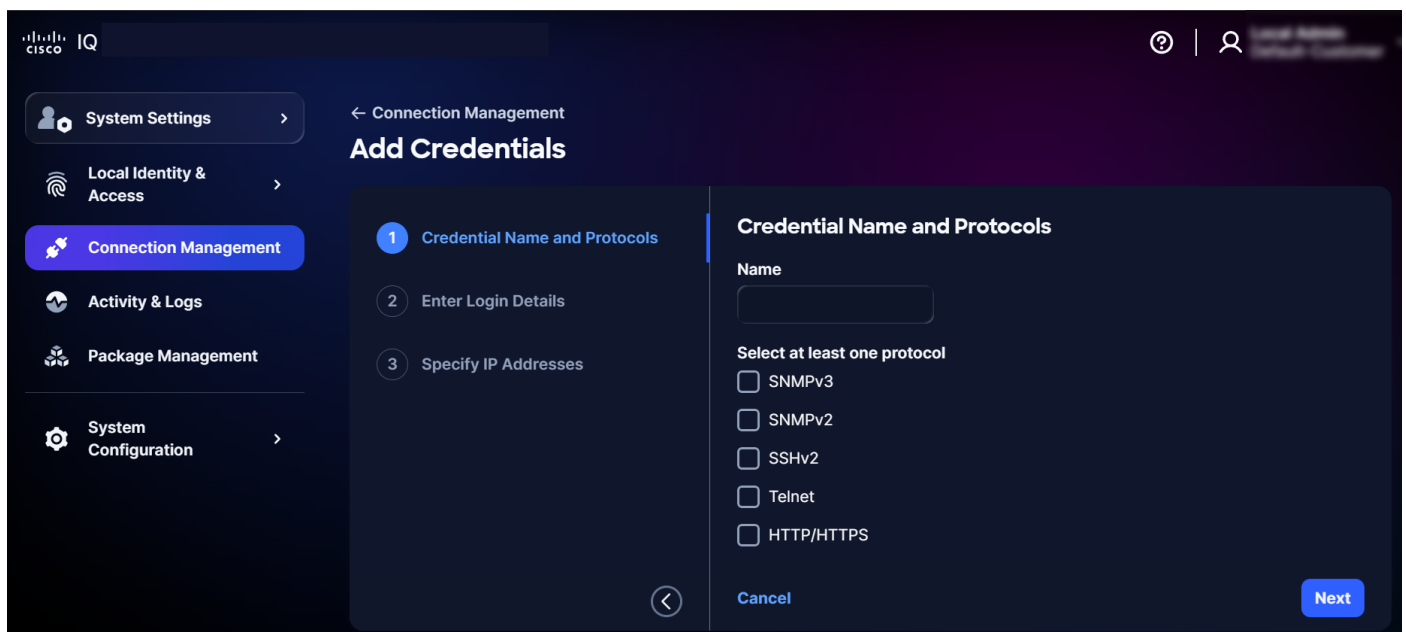
U moet eerst inloggegevens toevoegen om de gegevensverzameling uit te voeren. U voegt als volgt referenties toe:

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 een naam in.

5. Schakel alle toepasselijke protocolselectievakjes in.

6. Klik op Next (Volgende).

The screenshot shows the 'Add Credentials' window in the Cisco IQ Link. The left sidebar contains navigation options: System Settings, Local Identity & Access, Connection Management (highlighted), Activity & Logs, Package Management, and System Configuration. The main area is titled 'Add Credentials' and has three steps: 1. Credential Name and Protocols, 2. Enter Login Details, and 3. Specify IP Addresses. Step 2 is active. The 'Enter Login Details' section includes fields for Username, Engine ID (optional), Authorization algorithm, Authorization password, Privacy algorithm (optional), and Privacy password. There are 'Show' buttons for the passwords. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons.

Credentials toevoegen - Details



Opmerking: in de afbeelding hierboven wordt de weergave weergegeven wanneer alle protocollen in de vorige stap zijn geselecteerd. In de interface worden alleen de gekozen protocollen weergegeven.

7. Voer de aanmeldingsgegevens in voor elk geselecteerd protocol.

8. Klik op Next (Volgende).

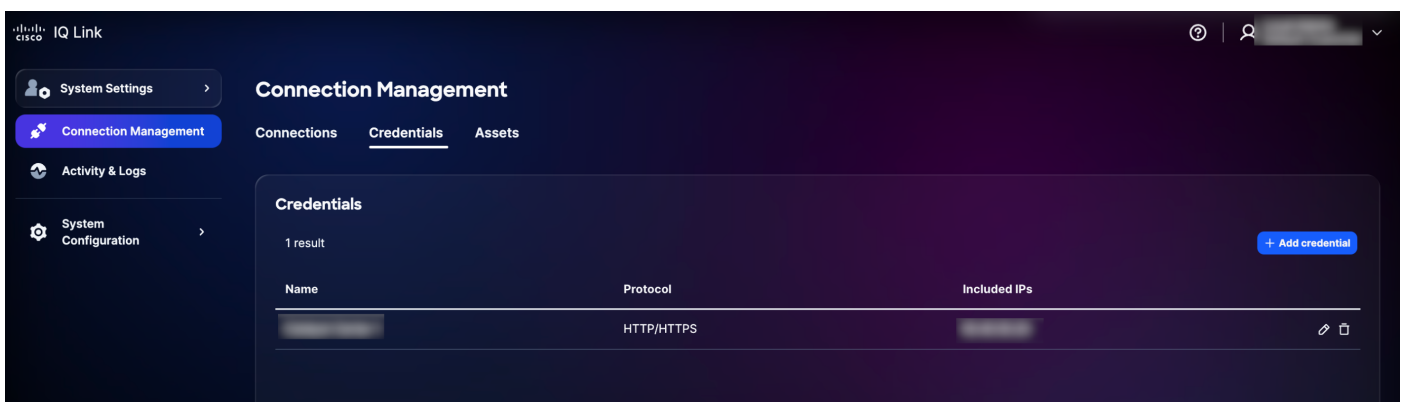
The screenshot shows the 'Add Credentials' window in the Cisco IQ Link, specifically the 'Specify IP Addresses' step. The left sidebar is the same as in the previous screenshot. The main area is titled 'Add Credentials' and has three steps: 1. Credential Name and Protocols, 2. Enter Login Details, and 3. Specify IP Addresses. Step 3 is active. The 'Specify IP Addresses' section includes a text area for 'Included IPs' with a placeholder example: 'e.g. *-*-*, 192.168.1.0/24, 172.16.*.*'. At the bottom, there are 'Cancel', 'Back', 'Save and add another credential', and 'Save' buttons.

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)
 - 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 1: 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)
10.10.2.15	10.10.2, 10.10.*	10.10.2.* (Meer specifiek)
10.10.5.50	10.10. .	10 .10.. (Meer specifiek)

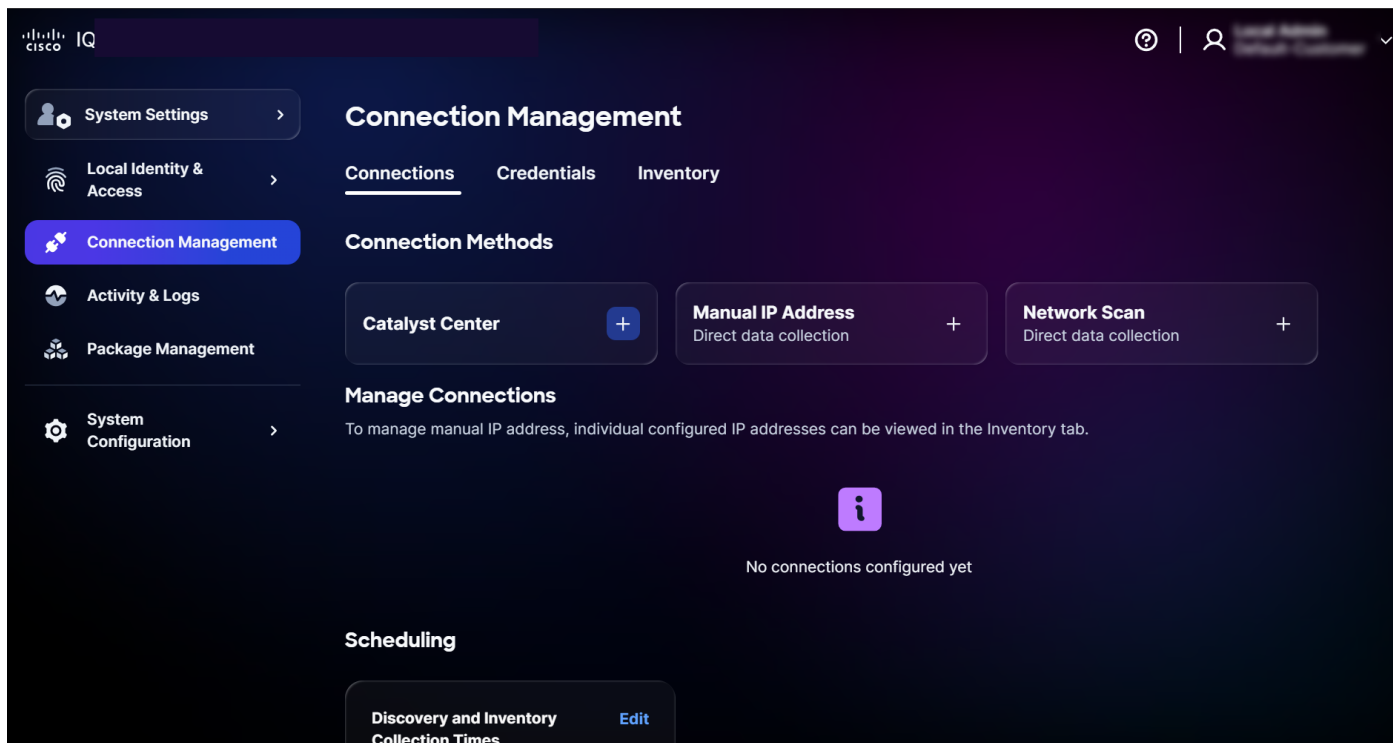
 **Opmerking:** Als een apparaat in meerdere overlappende categorieën valt, selecteert het systeem altijd de set met de hoogste specificiteit (met andere woorden, de minste achterliggende jokertekens).

Gegevensverzameling met Catalyst Center

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

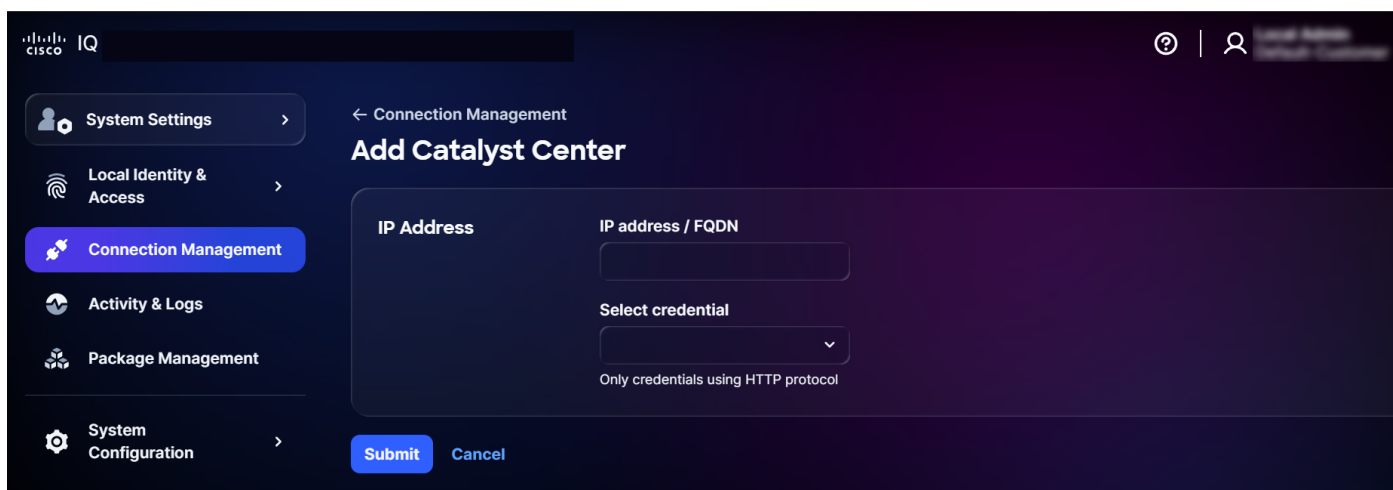
Voor gegevensverzameling met Catalyst Center:

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 Selecteer referenties.
5. Klik op Indienen. Er wordt een bevestiging weergegeven (dit kan maximaal 75 minuten duren). U kunt het nieuw toegevoegde Catalyst Center bekijken onder Configured

Connections.

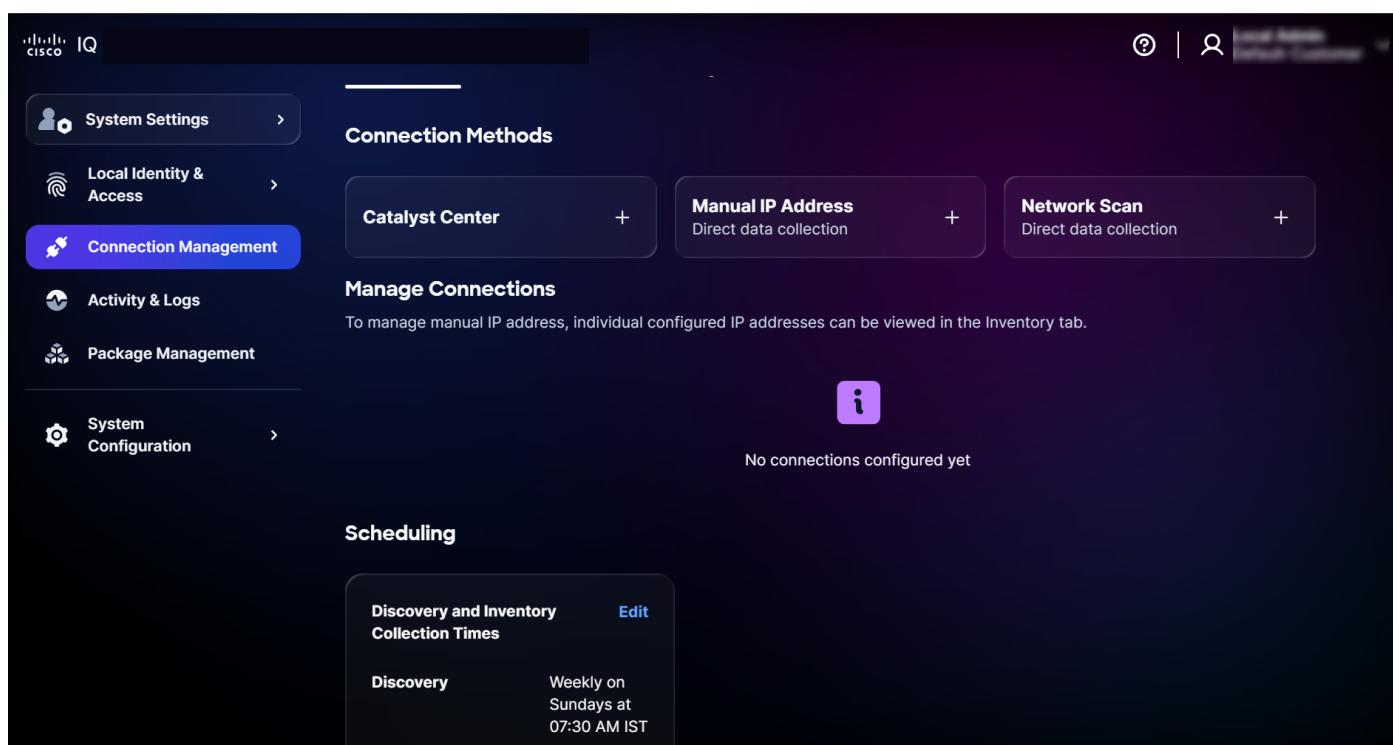
6. Plan een verzameling in. Zie [Planning](#) voor meer informatie.

 **Opmerking:** Cisco IQ VA 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.

handmatige gegevensverzameling

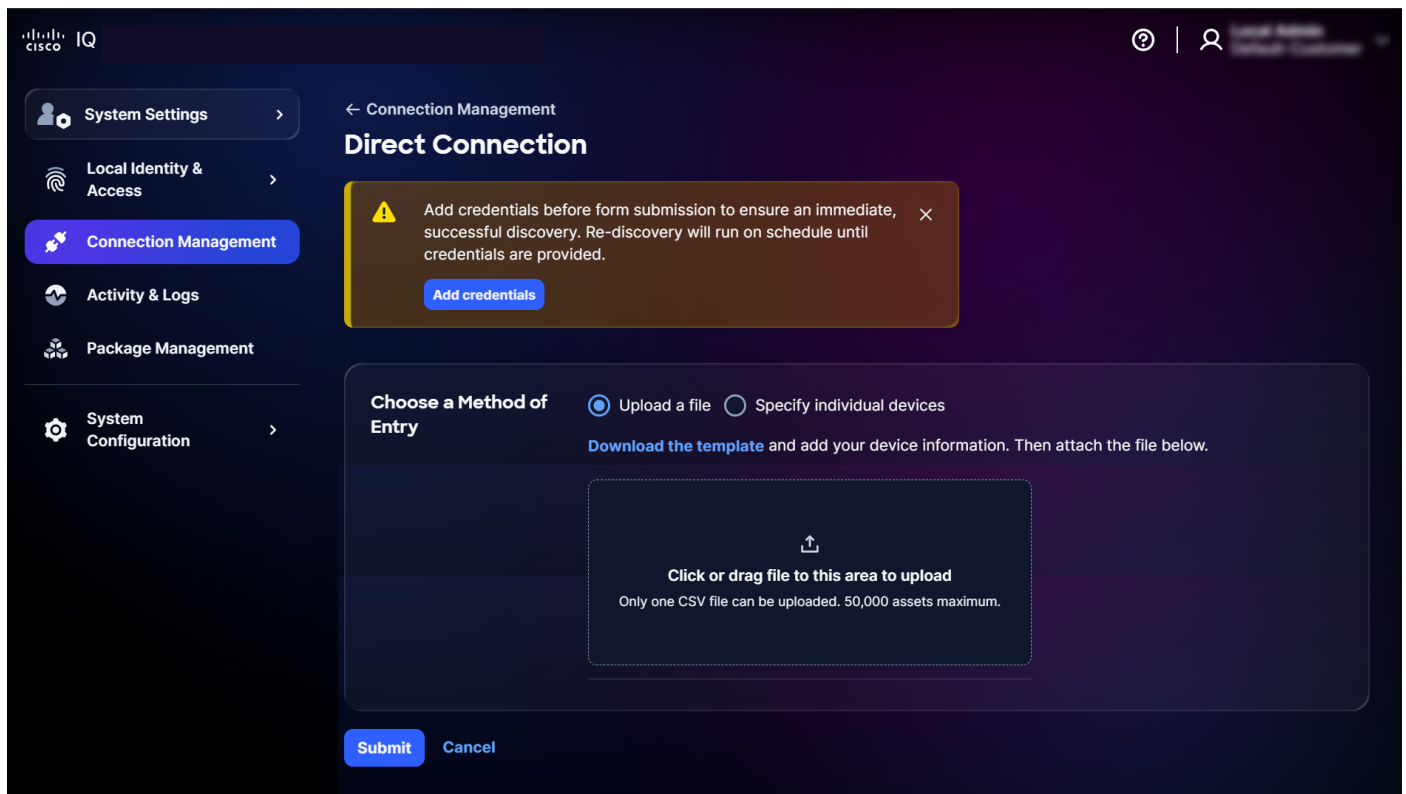
Apparaten voor directe gegevensverbinding toevoegen:

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



Verbindingsbeheer

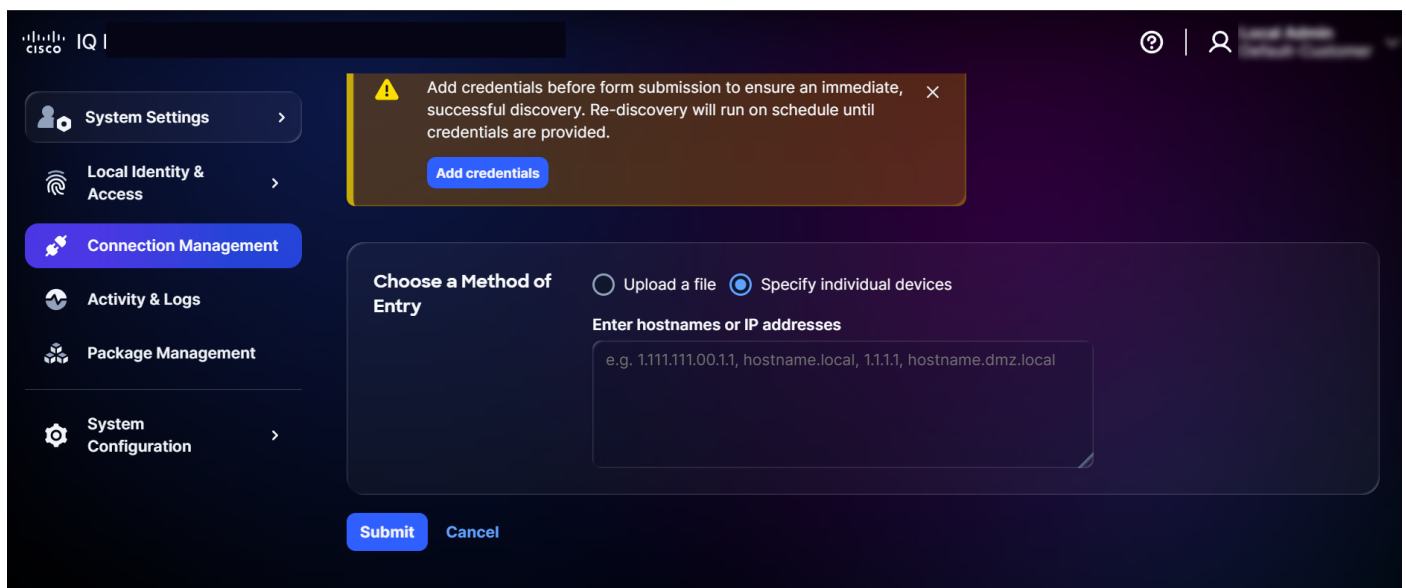
2. Klik op Handmatig IP-adres. De pagina Directe verbinding wordt weergegeven met twee (2) opties om gegevens te verzamelen.



Bestand uploaden

3. Klik op de voorkeursoptie van Kies een invoermethode en geef uw apparaatgegevens op met een van de volgende methoden:

- Een bestand uploaden: klik of sleep het bestand



Afzonderlijke apparaten opgeven

- Afzonderlijke apparaten opgeven: Voer een enkele hostnaam, IP-adressen of een door komma's gescheiden lijst met hostnamen en/of IP-adressen in

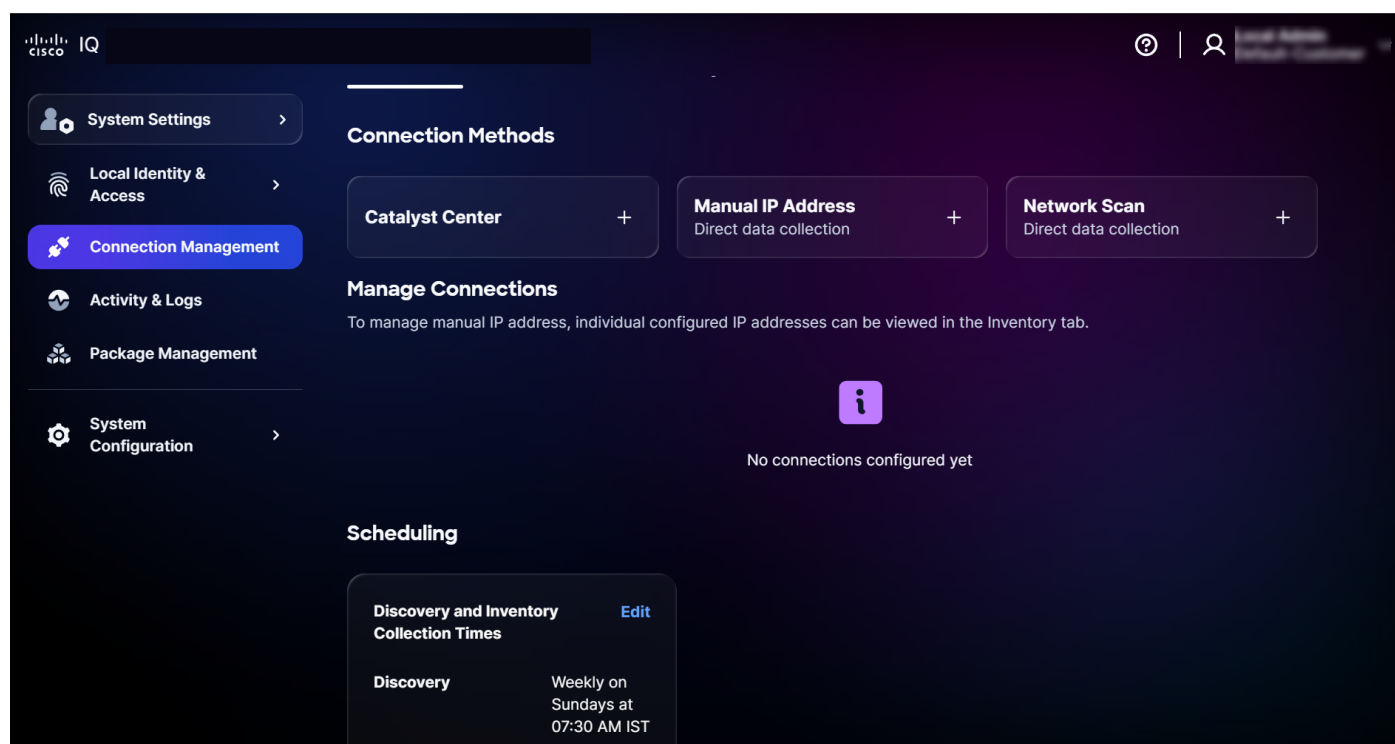
4. Klik op Indienen. U wordt doorgestuurd naar het tabblad Activa na succesvolle indiening.

5. Plan een verzameling in. Zie [Planning](#) voor meer informatie.

 **Opmerking:** Cisco IQ VA 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.

Netwerkscan

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



Netwerkscan

2. Klik op Netwerkscan. Op de pagina Verbinding maken via netwerk scannen worden drie (3) opties weergegeven.

- IP-bereik opgeven: een bereik van IP-adressen definiëren voor doelapparaten binnen dat bereik voor netwerkdetectie- of beheertaken
 - Discovery Protocol (CDP/LLDP) opgeven: Kies het te gebruiken netwerkdetectieprotocol
 - Bestand uploaden: een bestand uploaden, zoals configuratiebestanden of gegevens
3. Voer een naam in.
 4. Voer IP Start en IP End in.
 5. Kies onder Scannen plannen de optie Frequentie en tijd.
 6. Klik op Assets verbinden.

planning

Met Scheduling kunt u bepalen wanneer Cisco IQ VA 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 verzamelingschema's te synchroniseren en nauwkeurig weer te geven binnen Virtual Appliance.

Installeren van pakketten (modules, regels en rechten)

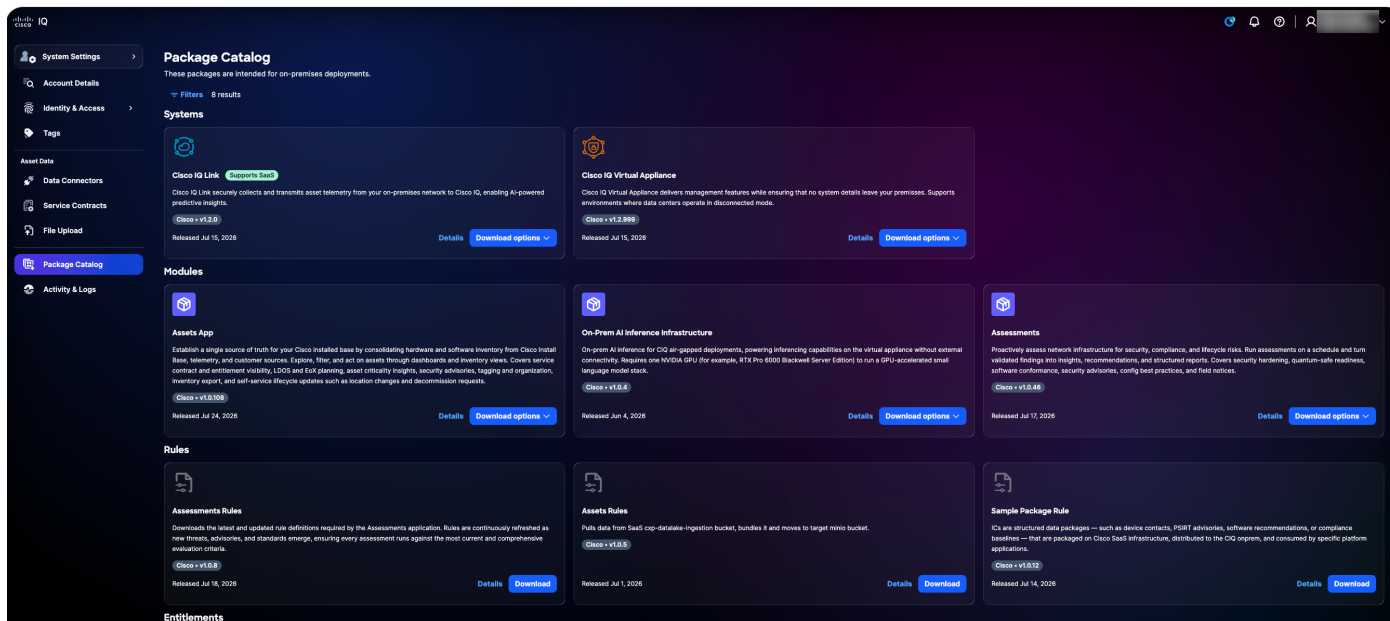
U kunt de levenscyclus van de software (dat wil zeggen installatie en configuratie) van operationele modules, regels, rechten en gespecialiseerde AI-aangedreven functies binnen de VA beheren. U kunt ze installeren door de nieuwste versies van Cisco IQ (SaaS) te downloaden door naar de pakketcatalogus te navigeren. In de Pakketcatalogus worden de software-instanties weergegeven die voor u beschikbaar zijn. Het stelt u in staat om updates naadloos te bewaken en te beheren, waardoor u uw systeeminstanties efficiënt kunt volgen en beheren.

Modules toevoegen

Een module is een op zichzelf staand softwarepakket dat kernfunctionaliteit biedt binnen de VA. Het is een onafhankelijke service met een eigen levenscyclus, die installatie, onderhoud en grootte mogelijk maakt. Het resourceverbruik, inclusief CPU, Graphics Processing Unit (GPU) en RAM, wordt dynamisch toegewezen op basis van de implementatiegrootte (klein, gemiddeld of

groot) die tijdens de eerste installatie is geselecteerd.

1. Meld u aan bij [Cisco IQ](#).
2. Ga naar Systeeminstellingen > Pakketcatalogus.

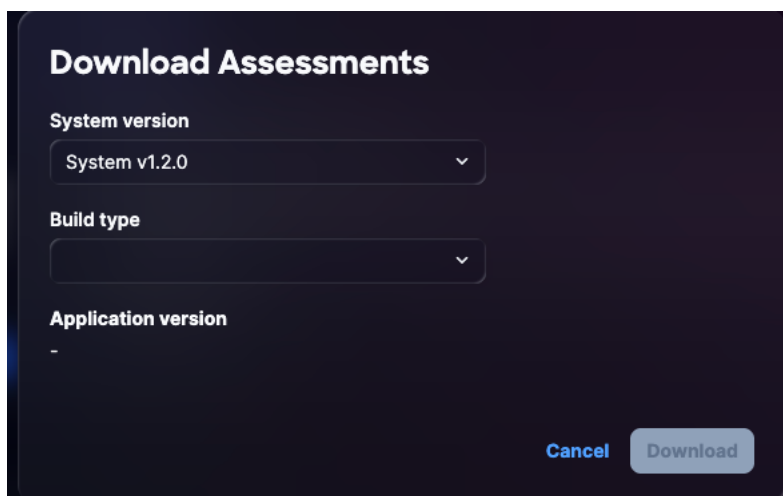


Pakketcatalogus

3. Klik op de gewenste modulekaart op Downloadopties > Installatiepakketten. Het venster Downloaden wordt geopend.



Opmerking: voor de voorbeeldimages wordt de evaluatiemodule gebruikt.



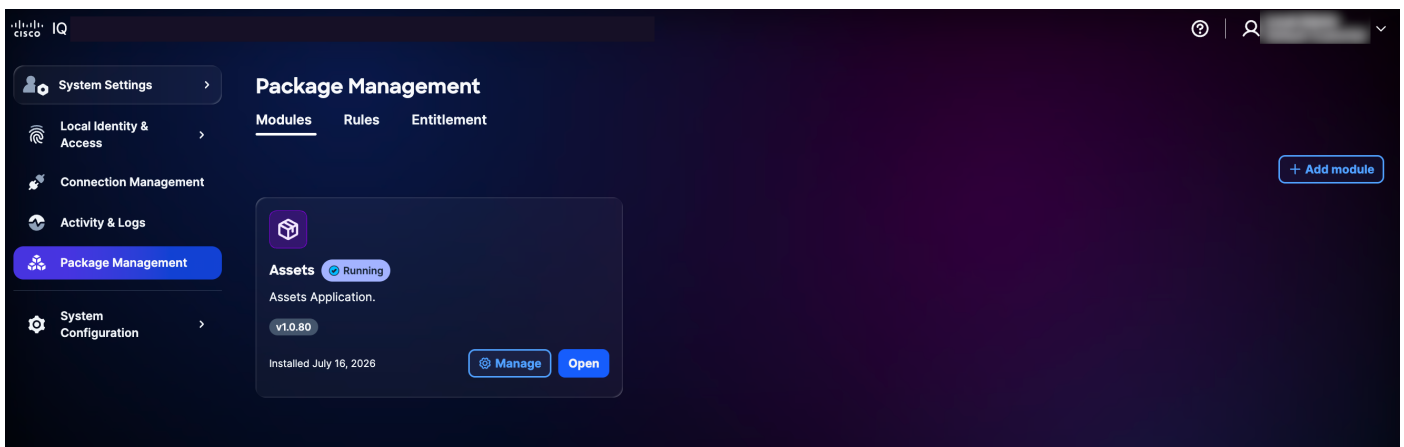
downloaden

4. Kies een systeemversie in de vervolgkeuzelijst.
5. Kies een bouwtype in de vervolgkeuzelijst.
6. Klik op Download om het bestand lokaal op te slaan.



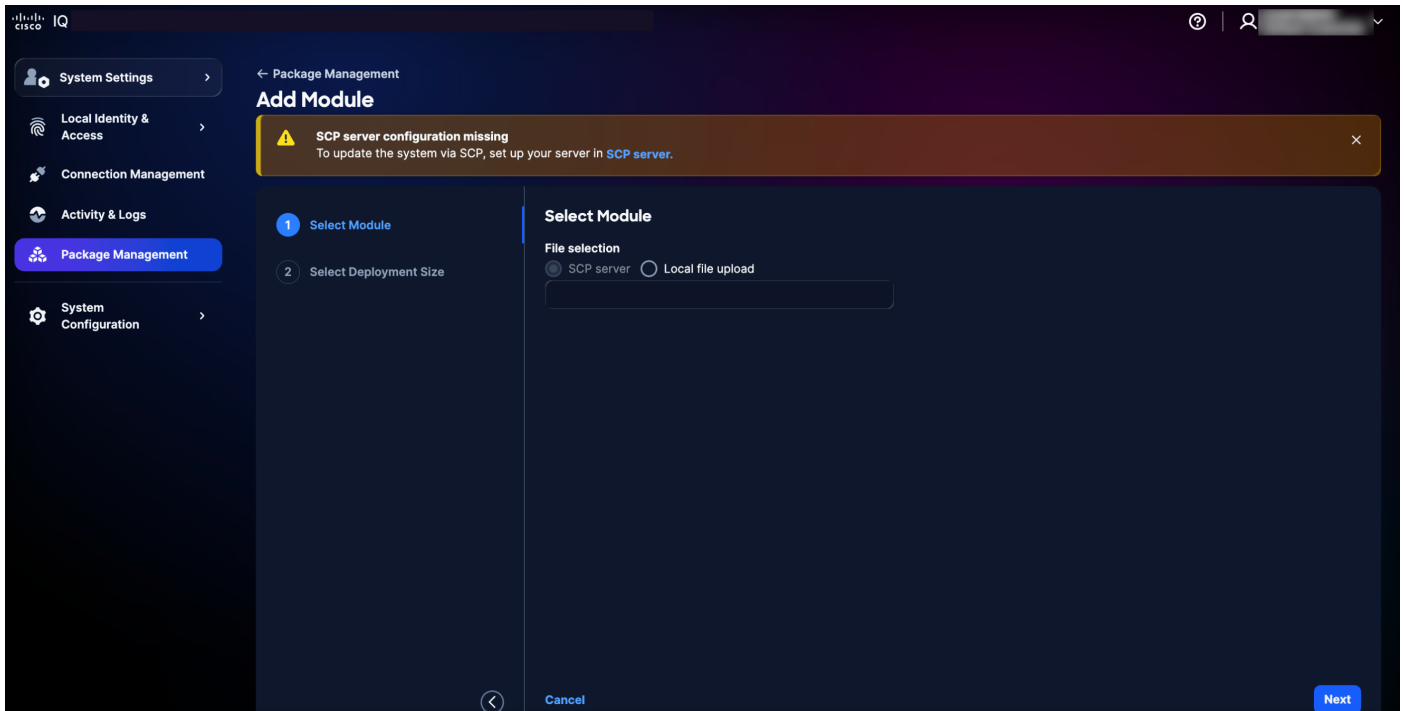
Opmerking: de installatiebestanden zijn groot (10-25 GB); zorg ervoor dat u voldoende schijfruimte hebt voordat u downloadt.

7. Navigeer naar VA.
8. Navigeer naar Home > Systeeminstellingen > Pakketbeheer. De pagina Pakketbeheer wordt weergegeven met de volgende tabbladen:
 - Modules
 - reglement
 - rechten



Modules

9. Klik op Module toevoegen.

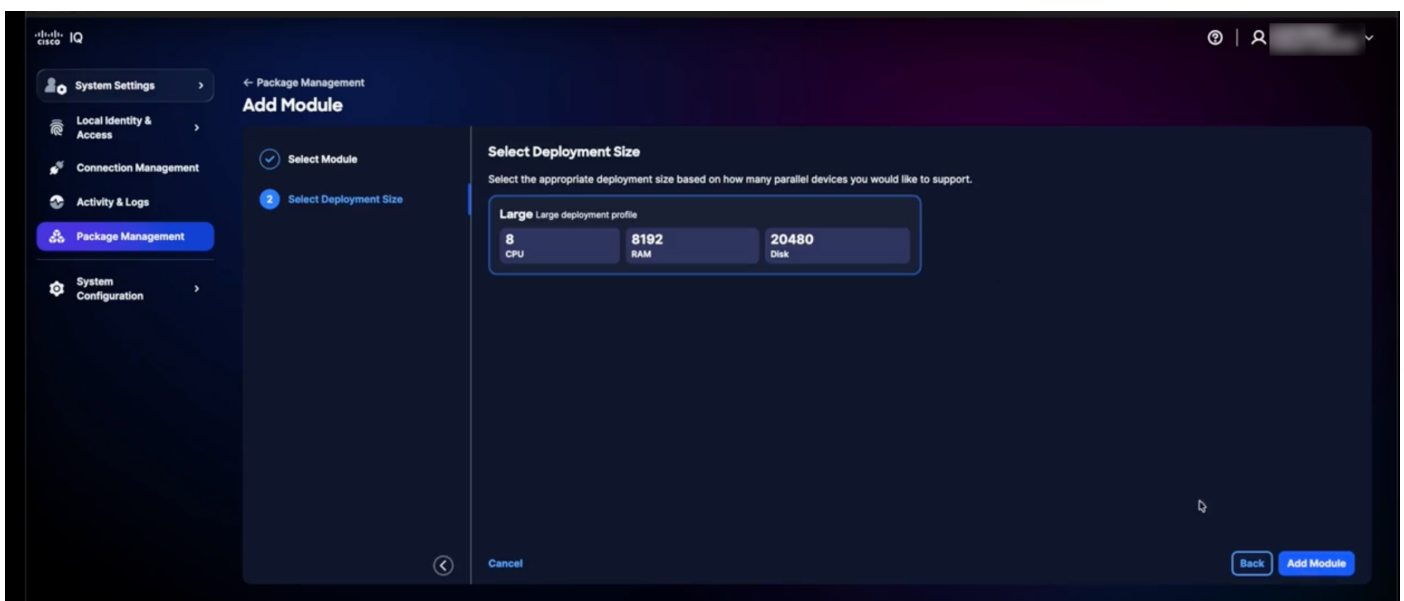


Module toevoegen

10. Kies de gewenste optie voor bestandskeuze:

- SCP-server: Voer de exacte bestandsnaam van het installatiepakket in (aanbevolen voor grote bestanden)
- Lokaal bestand uploaden: Sleep het gedownloade installatiebestand (niet aanbevolen voor bestanden van 30 GB of groter vanwege de uploadtijd)

11. Klik op Next (Volgende).

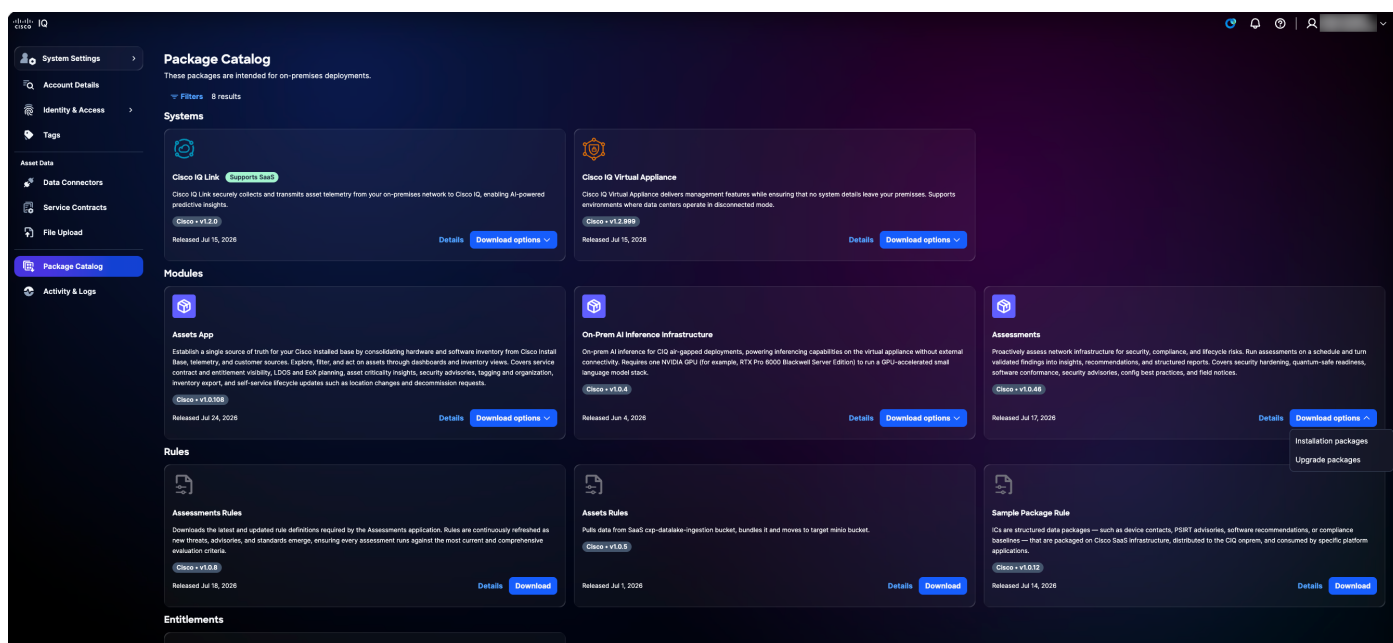


Grootte van implementatie

12. Kies de implementatiegrootte (bijvoorbeeld Klein, Gemiddeld of Groot). Deze formaten zijn vooraf gedefinieerd en bepalen de vereiste middelen.
13. Klik op Module toevoegen. De nieuw geïnstalleerde module wordt weergegeven op het tabblad Modules in Pakketbeheer. Na voltooiing verandert de modulestatus in "Running" en wordt de knop Open beschikbaar.

Een module upgraden

De nieuwste modules worden voortdurend bijgewerkt in Package Catalog (in Cisco IQ). Upgraden naar de nieuwste versie:



Verbind bedrijfsmiddelen met een netwerkscan

1. Klik op de gewenste modulekaart op Downloadopties > Upgradepakketten. Het venster Downloaden wordt geopend.



Opmerking: de evaluatiemodule wordt gebruikt als voorbeeld voor de images.

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

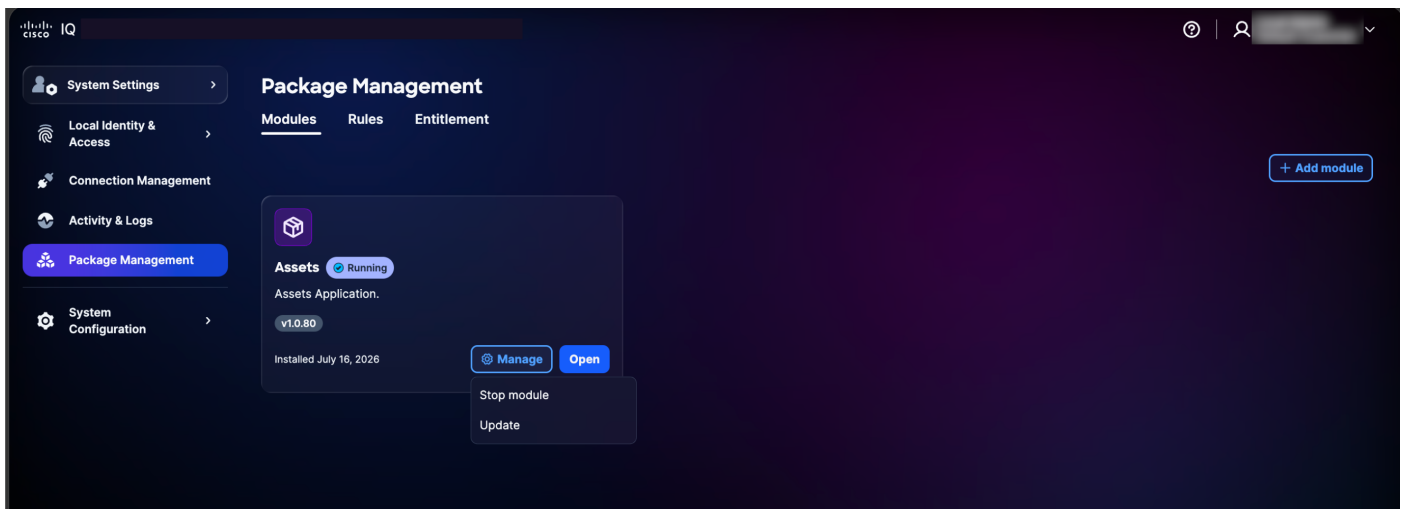
Download

downloaden

2. Kies een systeemversie in de vervolgkeuzelijst.
3. Kies een huidige app uit de vervolgkeuzelijst.
4. Kies een bouwtype in de vervolgkeuzelijst.
5. Klik op Download om het bestand lokaal op te slaan.
6. Ga naar VA en voltooi de installatie van het gedownloade bestand.

Modules beheren

Nadat u een module hebt toegevoegd, kunt u deze wijzigen op de pagina Pakketbeheer door op Beheren te klikken. De beschikbare wijzigingsopties omvatten het wijzigen van de grootte en het upgraden naar een hogere versie. Om een module te beheren:



Type update

1. Klik op de pagina Pakketbeheer op Beheer > Bijwerken voor de gewenste module.
2. Kies het updatetype:
 - Alleen implementatiegrootte wijzigen
 - Versie bijwerken
3. Als Implementatiegrootte wijzigen is geselecteerd, klikt u op Volgende en kiest u de nieuwe implementatiegrootte op de volgende pagina.

OF

Als Versie bijwerken is geselecteerd, wordt de optie Bestandselectie weergegeven. Kies SCP Server en voer de exacte bestandsnaam van het installatiepakket in of kies Lokaal bestand uploaden en het gedownloade installatiebestand slepen en neerzetten.

4. Klik op Next (Volgende). De pagina Updateschema selecteren wordt weergegeven.
5. Kies uit de volgende keuzerondjes om het schema bij te werken:
 - Nu bijwerken
 - Later bijwerken



Opmerking: sommige modules ondersteunen updates zonder downtime. Als downtime vereist is, worden de details weergegeven in een banner.

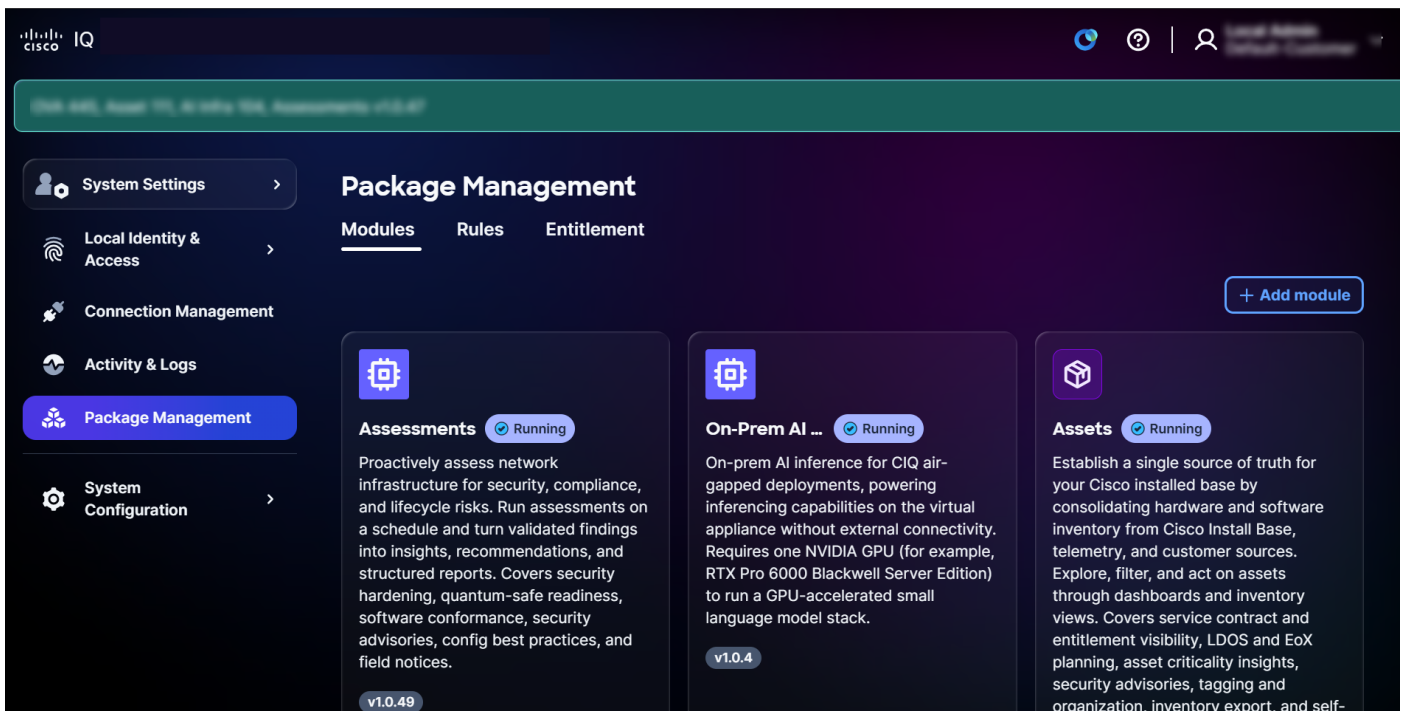
6. Als Later bijwerken is geselecteerd, voert u de datum en tijd in.
7. Klik op Next (Volgende). Het updateoverzicht wordt weergegeven.

 **Opmerking:** U kunt de opmerkingen bekijken in de samenvatting van de update.

8. Klik op Module bijwerken en ga naar het tabblad Module. De module geeft de status "Gepland bijwerken" weer.

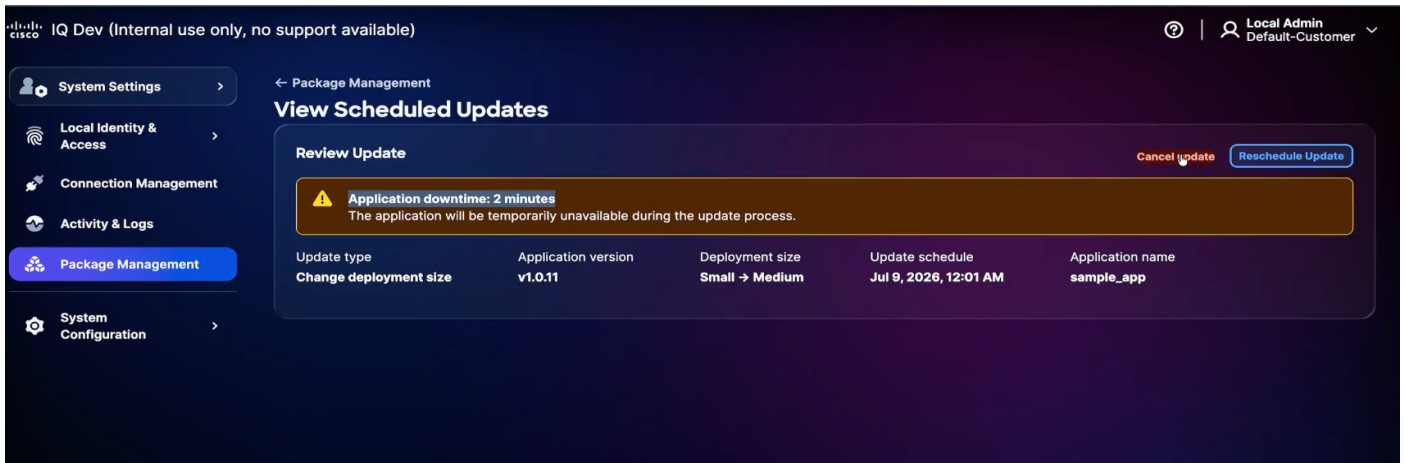
Planningen bewerken

U kunt ook geplande updates bekijken, bewerken of annuleren. Een geplande update bewerken of annuleren:



Bewerkingsschema

1. Klik op de pagina Pakketbeheer op Beheren > Geplande update van de gewenste module bekijken. Het venster Geplande updates bekijken wordt weergegeven.



Updates plannen

2. Klik op Bijwerken annuleren of Bijwerken opnieuw plannen zoals vereist.
3. Volg de instructies op het scherm om de bewerkingen te voltooien.

 **Opmerking:** Als een modulebewerking (bijvoorbeeld installatie, upgrade of formaat wijzigen) mislukt, kiest u een van de volgende opties:

Opnieuw proberen: de gebruikersinterface geeft een knop Opnieuw proberen weer, zodat u de bewerking opnieuw kunt proberen. Logs: als er een fout blijft optreden, klikt u op Logs om gedetailleerde diagnostische informatie weer te geven. Dit is de primaire methode voor het identificeren van de oorzaak van installatie- of runtime-fouten.

Regels installeren

Een regel is een gespecialiseerde component of "add-on" die de functionaliteit van een bestaande module uitbreidt of wijzigt. Regels zijn niet ontworpen om als zelfstandige programma's te worden uitgevoerd; ze zijn "aangesloten" op een module om specifieke regels, logica of functies te bieden. Regels zijn gekoppeld aan specifieke modules. Wanneer een regel is geïnstalleerd, wordt deze gekoppeld aan de module die deze ondersteunt. Regels maken het mogelijk om het systeem te updaten of aan te passen zonder dat een volledige upgrade van de kernmodule nodig is. Als een nieuwe set regels of functies nodig is, kunt u eenvoudig een nieuwe regel toevoegen aan de bestaande module.

Een regel downloaden:

1. Meld u aan bij [Cisco IQ](#).

2. Navigeer naar Systeeminstellingen > Pakketcatalogus.
3. Klik op de gewenste regelkaart op Downloaden.



Opmerking: het volgende voorbeeld is voor een regel voor elementen.

Download Assets Rules

Target app version

assets v1.0.0



Cancel

Download

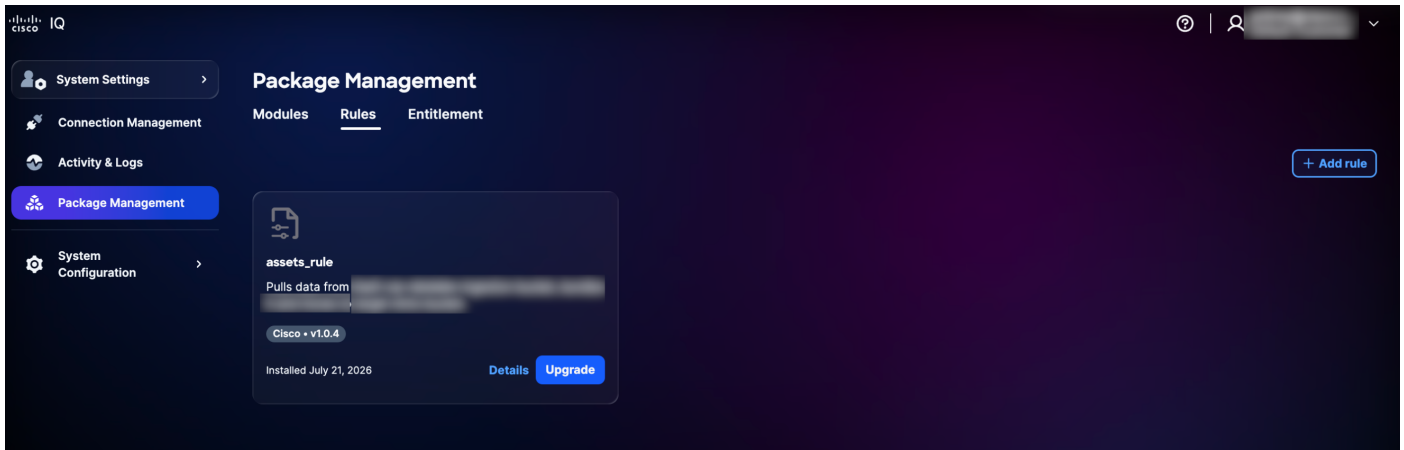
downloaden

4. Kies een versie van de doelapp in de vervolgkeuzelijst.
5. Klik op Download om het bestand lokaal op te slaan.



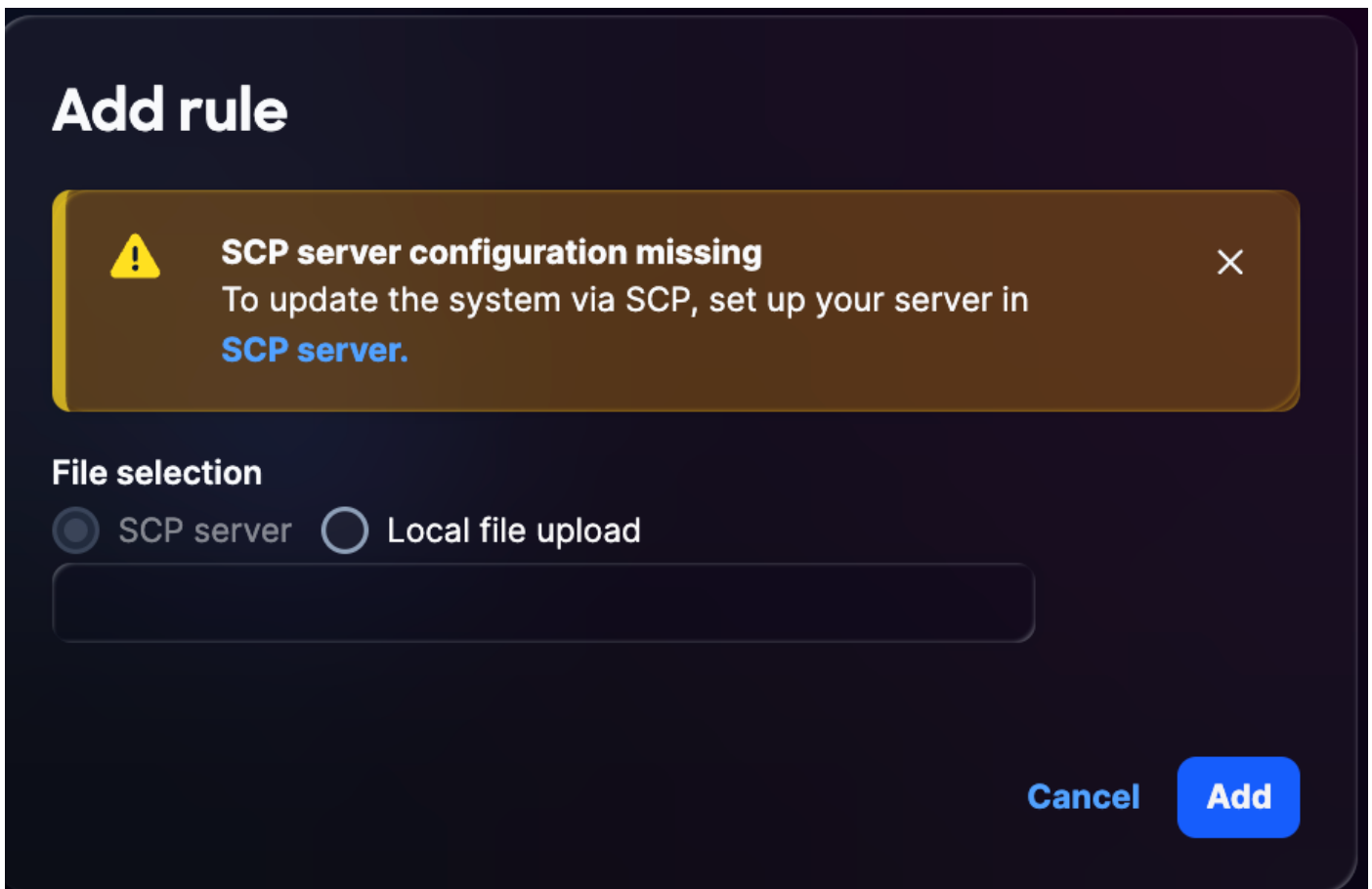
Opmerking: installatiebestanden zijn groot (10-25 GB); zorg ervoor dat u voldoende schijfruimte hebt voordat u downloadt.

6. Navigeer naar VA.
7. Navigeer naar Home > Systeeminstellingen > Pakketbeheer. De pagina Pakketbeheer wordt weergegeven met de volgende tabbladen.
 - Modules
 - reglement
 - rechten
8. Klik op het tabblad Regels.



pakketbeheer

9. Klik op Regel toevoegen.



Regel toevoegen

10. Kies de gewenste optie voor bestandskeuze:

- SCP-server (Secure Copy Protocol): Voer de exacte bestandsnaam van het installatiepakket

in. Deze methode wordt aanbevolen voor grote bestanden.

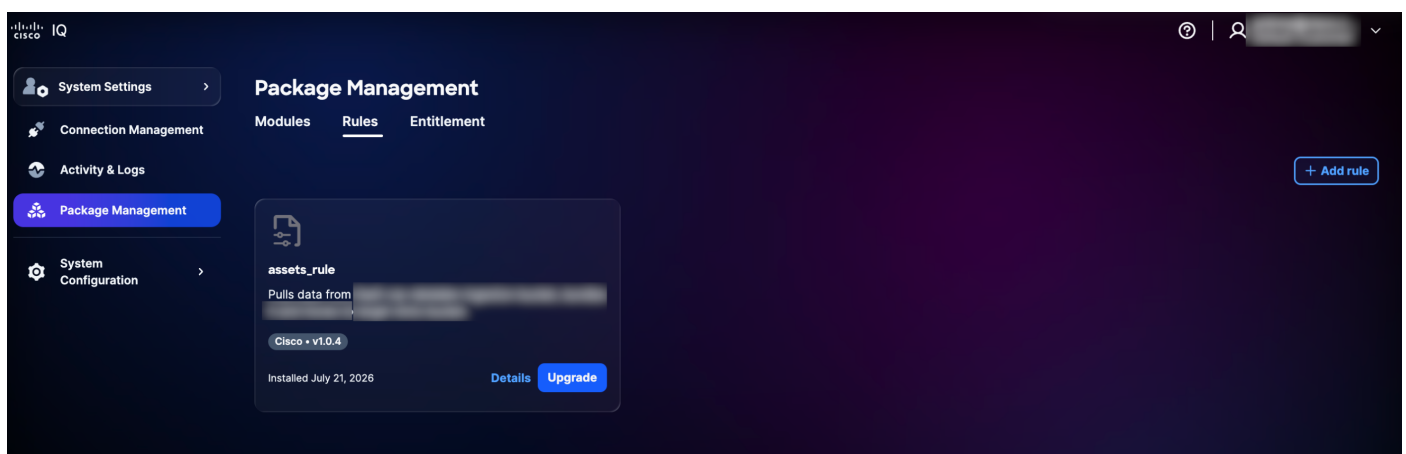
- Lokaal bestand uploaden: Sleep het gedownloade installatiebestand.

11. Klik op Add (Toevoegen). De toegevoegde regel wordt weergegeven in Pakketbeheer.

Regels bijwerken

Regels bijwerken:

1. Navigeer naar Systeeminstellingen > Pakketbeheer in VA.



Upgraden

2. Klik in de gewenste regel op Bijwerken. Het venster Upgraderegel wordt geopend.

Upgrade Rule

File selection

☒ SCP server ☐ Local file upload

Cancel

Add

Upgraderegel

3. Kies de gewenste optie voor bestandskeuze:

- SCP-server (Secure Copy Protocol): Voer de exacte bestandsnaam van het installatiepakket in. Deze methode wordt aanbevolen voor grote bestanden.
- Lokaal bestand uploaden: Sleep het gedownloade installatiebestand.

4. Klik op Add (Toevoegen).

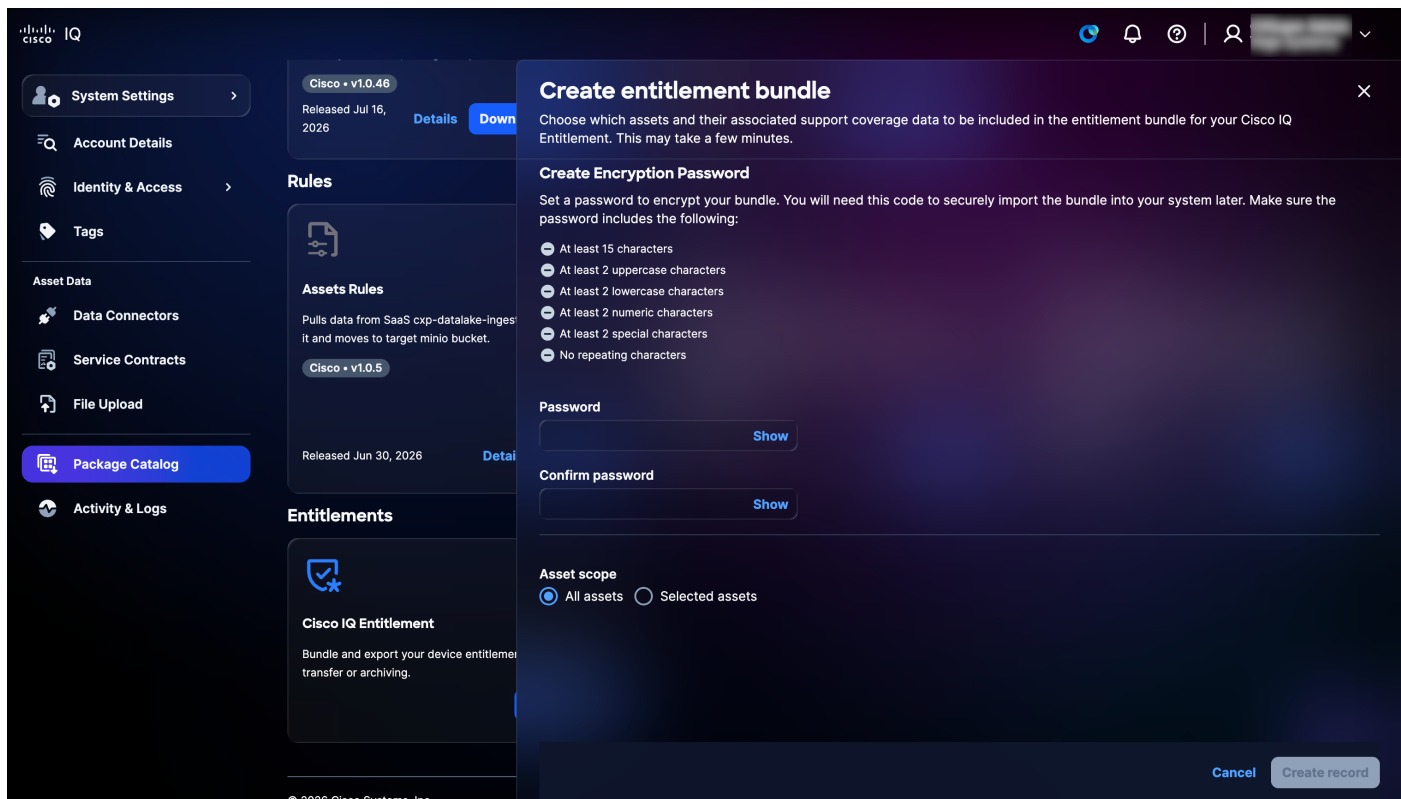


Opmerking: Deze regels worden toegepast bij de periodieke telemetrieverzameling van geplande apparaten. Voor onmiddellijke toepassing kunt u handmatig de telemetrieverzameling van het apparaat starten.

Rechten installeren

Een Recht biedt validatie van het recht van uw organisatie om specifieke softwarefuncties, modules of services te gebruiken. Om een recht te installeren:

1. Meld u aan bij [Cisco IQ](#).
2. Navigeer naar Systeeminstellingen > Pakketcatalogus.
3. Klik op de rechtenkaart op Record maken. Het venster Rechtenbundel maken wordt geopend.



Rechtenbundel maken

4. Voer een wachtwoord in. Raadpleeg de regels voor het maken van wachtwoorden die op het scherm worden weergegeven.
5. Voer hetzelfde wachtwoord opnieuw in Wachtwoord bevestigen.
6. Kies het gewenste keuzerondje Assetbereik.
 - Alle activa: omvat alle activa die aan u zijn gekoppeld
 - Geselecteerde elementen: hiermee kunt u specifieke apparaten kiezen die zijn afgestemd op uw omgeving. Als deze optie is geselecteerd, schakelt u de selectievakjes van alle toepasselijke elementen in
7. Klik op Record maken om het bestand lokaal op te slaan.

 **Opmerking:** Nadat u de rechtenbundel hebt gemaakt, navigeert u niet weg van het huidige scherm. Als u naar een andere pagina navigeert, wordt de bundel ongeldig gemaakt en moet u deze opnieuw genereren om de downloadoptie in te schakelen.

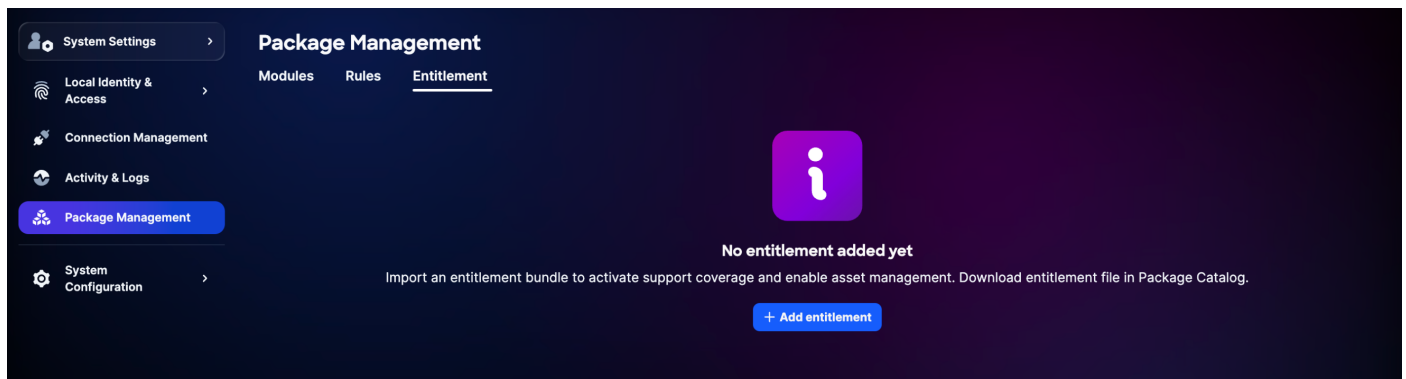
 **Opmerking:** installatiebestanden zijn groot (10-25 GB); zorg ervoor dat u voldoende schijfruimte hebt voordat u downloadt.

8. Log in bij VA.

9. Navigeer naar Home > Systeeminstellingen > Pakketbeheer. De pagina Pakketbeheer bevat de volgende tabbladen:

- Modules
- reglement
- rechten

10. Klik op het tabblad Rechten.



Tabblad Rechten

11. Klik op Rechten toevoegen.

Add Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

[Show](#)[Cancel](#)[Add](#)

Rechten toevoegen

12. Kies de gewenste optie voor bestandskeuze.

- Secure Copy Protocol (SCP)-server: Voer de exacte bestandsnaam van het installatiepakket in; deze methode wordt aanbevolen voor grote bestanden
- Lokaal bestand uploaden: Sleep het gedownloadte installatiebestand

13. Voer een wachtwoord in.

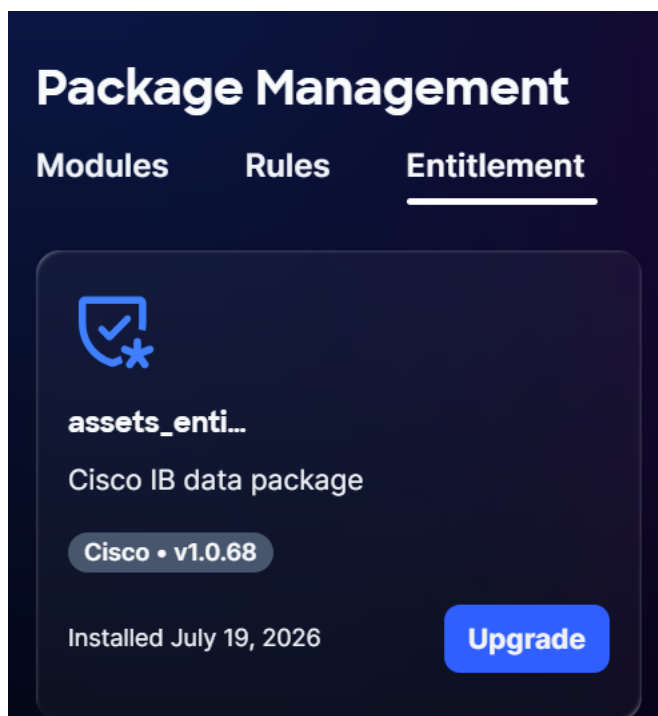
14. Klik op Add (Toevoegen). Het nieuw geïnstalleerde recht wordt weergegeven op het tabblad Rechten in Pakketbeheer.

15. Om rechten in te schakelen, wacht u 5 tot 10 minuten na het toevoegen ervan en start u vervolgens de telemetrieverzameling van het apparaat.

 **Opmerking:** Door een servicecontract toe te voegen aan het rechtenproces worden alle apparaten die aan dat contract zijn gekoppeld, toegevoegd aan de inventaris van de bedrijfsmiddelen op locatie. U kunt apparaten filteren op serienummer, meerdere account-ID's gebruiken of specifieke apparaten selecteren om rechten te beheren.

Verbetering van toeslagrechten

Een recht upgraden:



rechtenupgrade

1. Klik in het gewenste overzicht op Upgrade.

Upgrade Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

[Show](#)[Cancel](#)[Add](#)

upgraderecht

2. Kies de gewenste optie voor bestandskeuze:

- Secure Copy Protocol (SCP)-server: Voer de exacte bestandsnaam van het installatiepakket in; deze methode wordt aanbevolen voor grote bestanden
- Lokaal bestand uploaden: Sleep het gedownloade installatiebestand

3. Voer een wachtwoord in.

4. Klik op Add (Toevoegen).

AI-functies

De On-Prem AI Inference Infrastructure-module maakt on-premises AI-aangedreven mogelijkheden in VA mogelijk. Het draait lokaal een Small Language Model (SLM), waardoor het systeem kan reageren op AI-aangedreven vragen. Eenmaal geïnstalleerd, kunt u er rechtstreeks mee communiceren binnen de VA-interface.

De volgende querytypen worden ondersteund:

- Activa: identificeren van activa die risico lopen als gevolg van de status van het einde van de levenscyclus, de valuta of non-conformiteit van de software, beveiligingslekken en leemten in de dekking van contracten
- Voorraad: vraag een AI-gestuurde analyse aan over de assets in uw voorraad

Het On-Prem AI Inference Infrastructure-installatiepakket is beschikbaar in de Cisco IQ Package Catalog en wordt op dezelfde manier gedistribueerd als andere modules, zoals Assets.

 Opmerking: per GPU kan slechts één (1) On-Prem AI Inference Infrastructure tegelijk worden uitgevoerd. De installatie duurt ongeveer 40-45 minuten om te voltooien. De installatiebestanden zijn groot (ongeveer 30 GB); zorg ervoor dat u voldoende schijfruimte hebt voordat u downloadt.

Vereisten voor On-Prem AI Inference Infrastructure

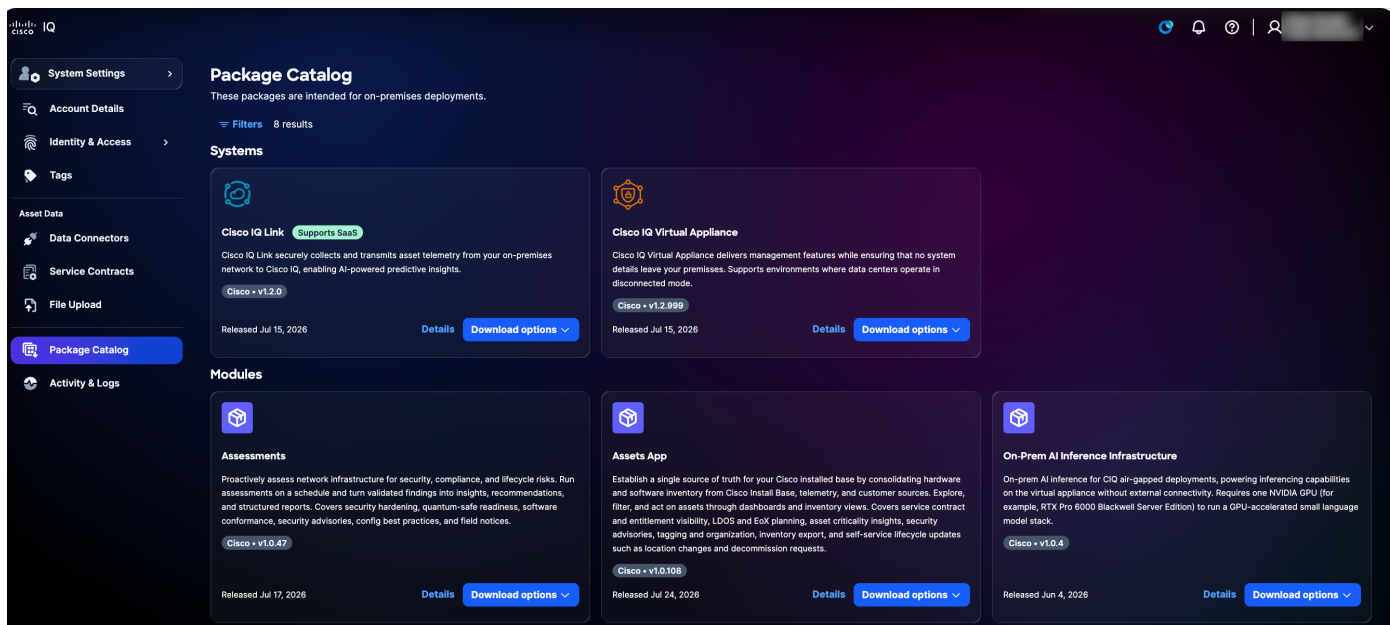
Voordat de On-Prem AI Inference Infrastructure wordt geïnstalleerd, moet aan de volgende voorwaarden worden voldaan:

- De VA moet een VM met GPU-toegang bevatten; de SLM heeft een GPU nodig en kan niet zonder
- De GPU VM moet 80 GB of meer GPU VRAM beschikbaar hebben

On-Prem AI-inferentie-infrastructuur installeren

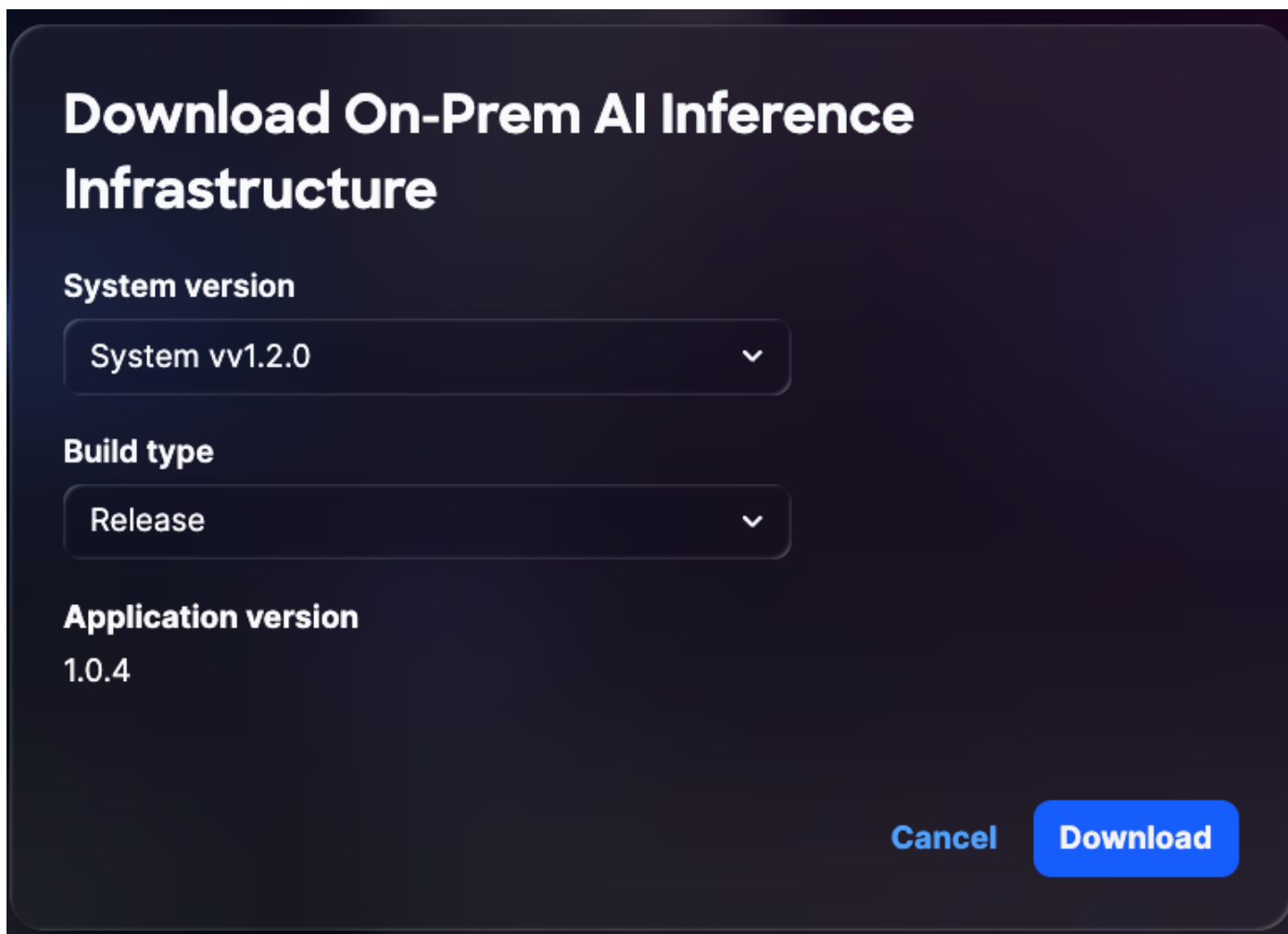
Om de On-Prem AI Inference Infrastructure op de VA te installeren, downloadt u de On-Prem AI Inference Infrastructure-module van Cisco IQ SaaS:

1. Meld u aan bij [Cisco IQ](#).
2. Navigeer naar Systeeminstellingen > Pakketcatalogus.



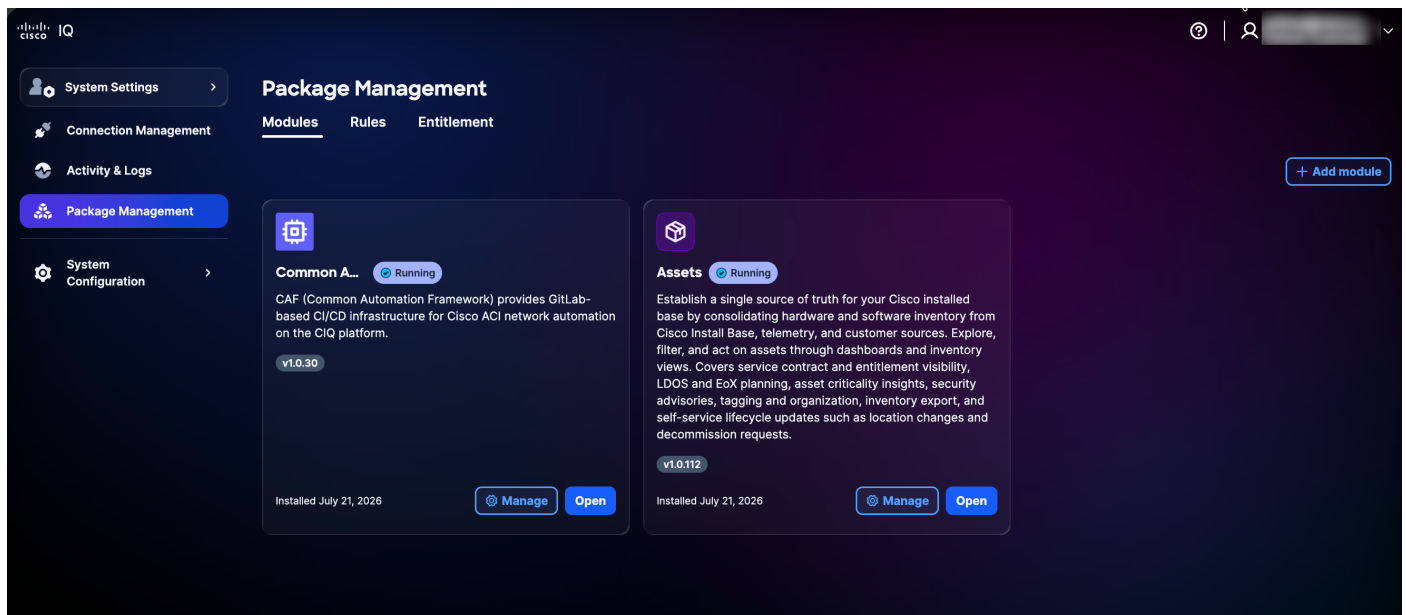
Installatiepakket

-
-
3. Klik op de On-Prem AI Inference Infrastructure-kaart op Downloadopties > Installatiepakketten. Het venster Toepassing downloaden wordt geopend.



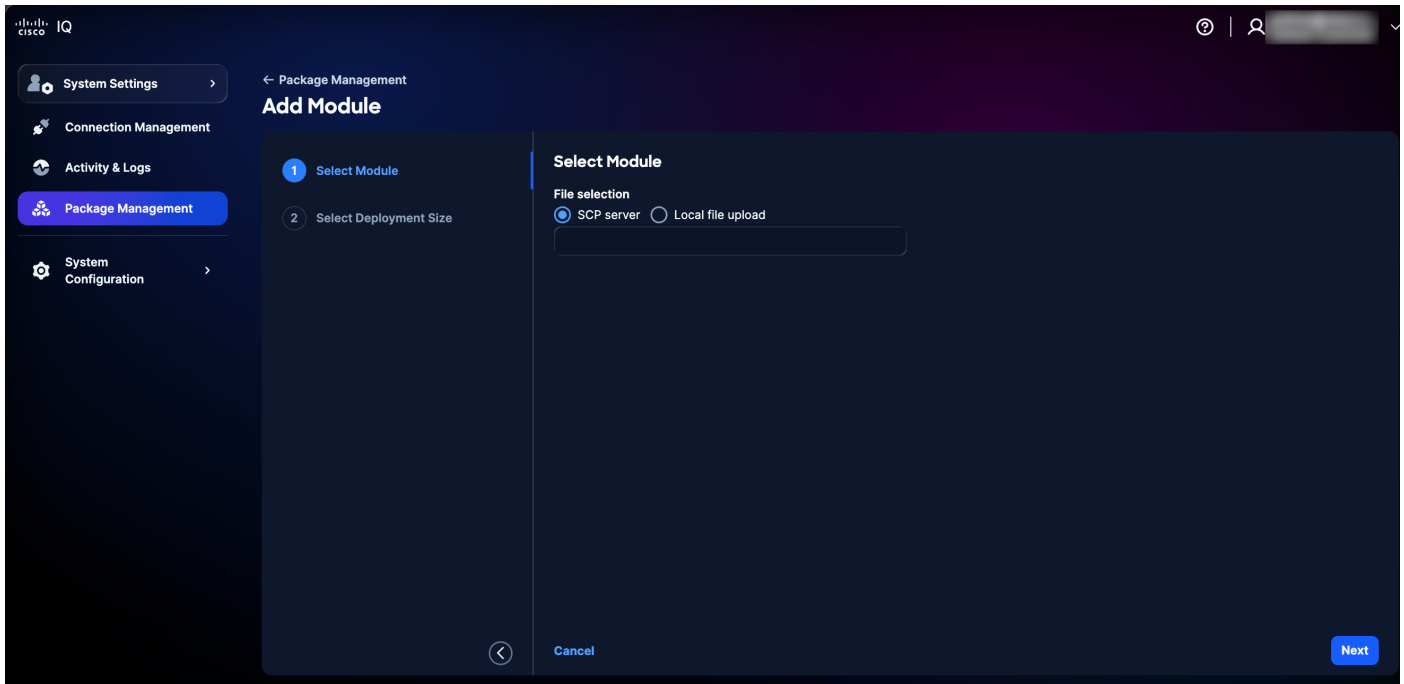
AI-inferentie-infrastructuur downloaden

4. Kies een systeemversie in de vervolgkeuzelijst.
5. Kies een bouwtype in de vervolgkeuzelijst.
6. Klik op Download (Downloaden).
7. Navigeer naar VA.



pakketbeheer

8. Navigeer naar Home > Systeeminstellingen > Pakketbeheer. De pagina Pakketbeheer wordt weergegeven met de volgende tabbladen:
 - Modules
 - reglement
 - rechten
9. Klik op het tabblad Modules op Modules toevoegen.



Selecteer module

10. Kies de gewenste optie voor bestandskeuze:

- SCP-server: Voer de exacte bestandsnaam van het installatiepakket in (aanbevolen voor grote bestanden).
- Lokaal bestand uploaden: Sleep het gedownloade installatiebestand (niet aanbevolen voor bestanden van 30 GB of groter vanwege de uploadtijd). Opmerking: de methode voor het uploaden van lokale bestanden heeft een drempel van 20 minuten. Als het uploadproces langer duurt, mislukt de installatie. Het gebruik van een SCP-server is de voorkeursmethode voor een succesvolle en stabiele installatie.

11. Klik op Next (Volgende). Het systeem begint met het uploaden van het bestand.

12. Kies een implementatiegrootte (bijvoorbeeld Klein, Gemiddeld of Groot).

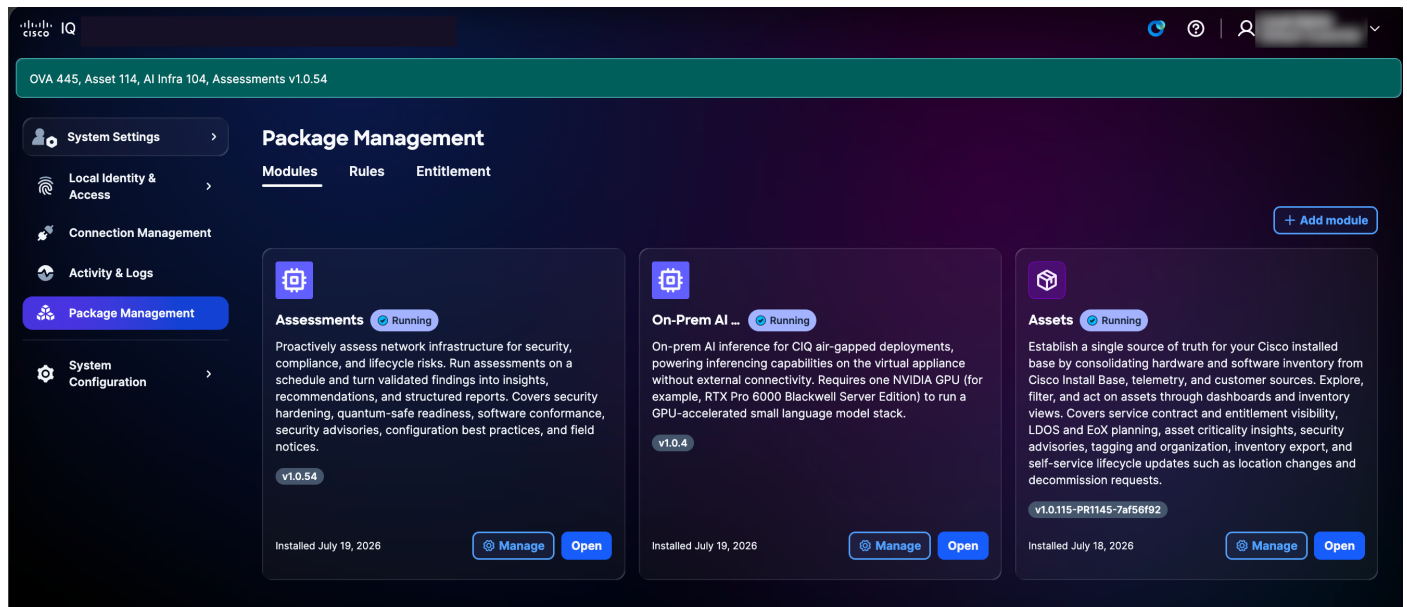
13. Klik op Module toevoegen. De installatie begint en duurt ongeveer 40-45 minuten om te voltooien.

Zodra de installatie is voltooid, wordt On-Prem AI Inference Infrastructure weergegeven op het tabblad Module in Pakketbeheer.

 Opmerking: per GPU kan slechts één On-Prem AI Inference Infrastructure-module worden uitgevoerd. De module gebruikt ongeveer 90% van GPU VRAM. Pogingen om een extra exemplaar op dezelfde GPU te installeren, worden niet ondersteund.

De On-Prem AI Inference Infrastructure-module beheren

Eenmaal geïnstalleerd, kan de On-Prem AI Inference Infrastructure-module worden beheerd via het tabblad Toepassingen in Pakketbeheer.



AI-inferentie-infrastructuur bewerken

Om de module te beheren, klikt u op Beheren naast de module On-Prem AI Inference Infrastructure. Zie [Modules beheren](#) voor meer informatie.

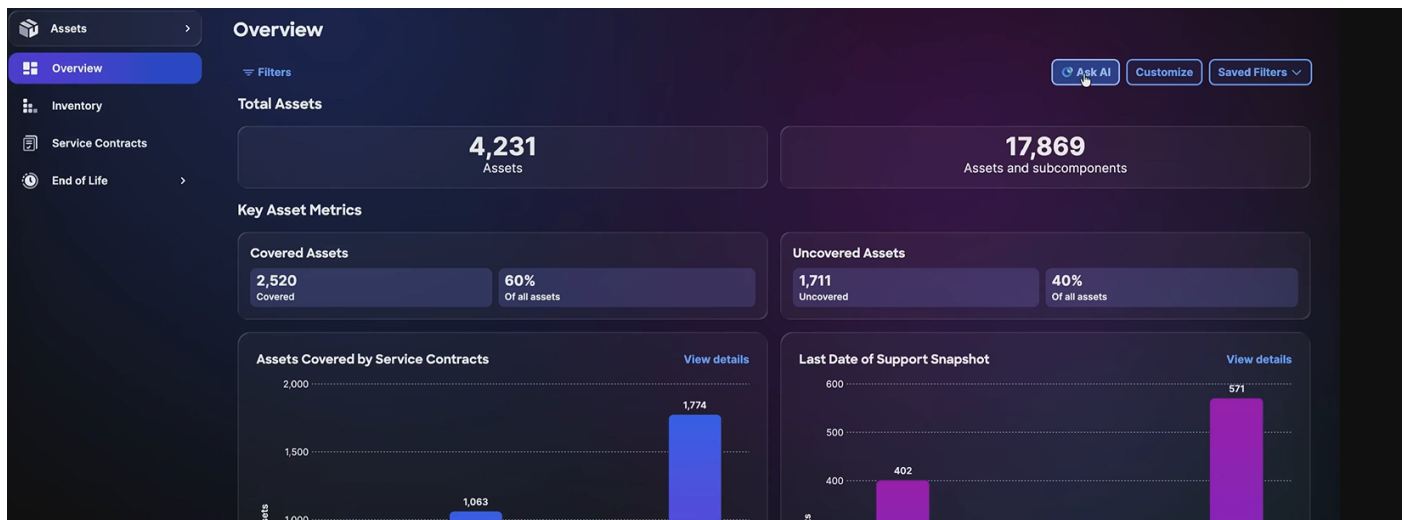
AI-functies gebruiken

Nadat de On-Prem AI Inference Infrastructure-module met succes is geïnstalleerd, wordt de knop Ask AI beschikbaar in de VA-interface.

Vraag AI in assets

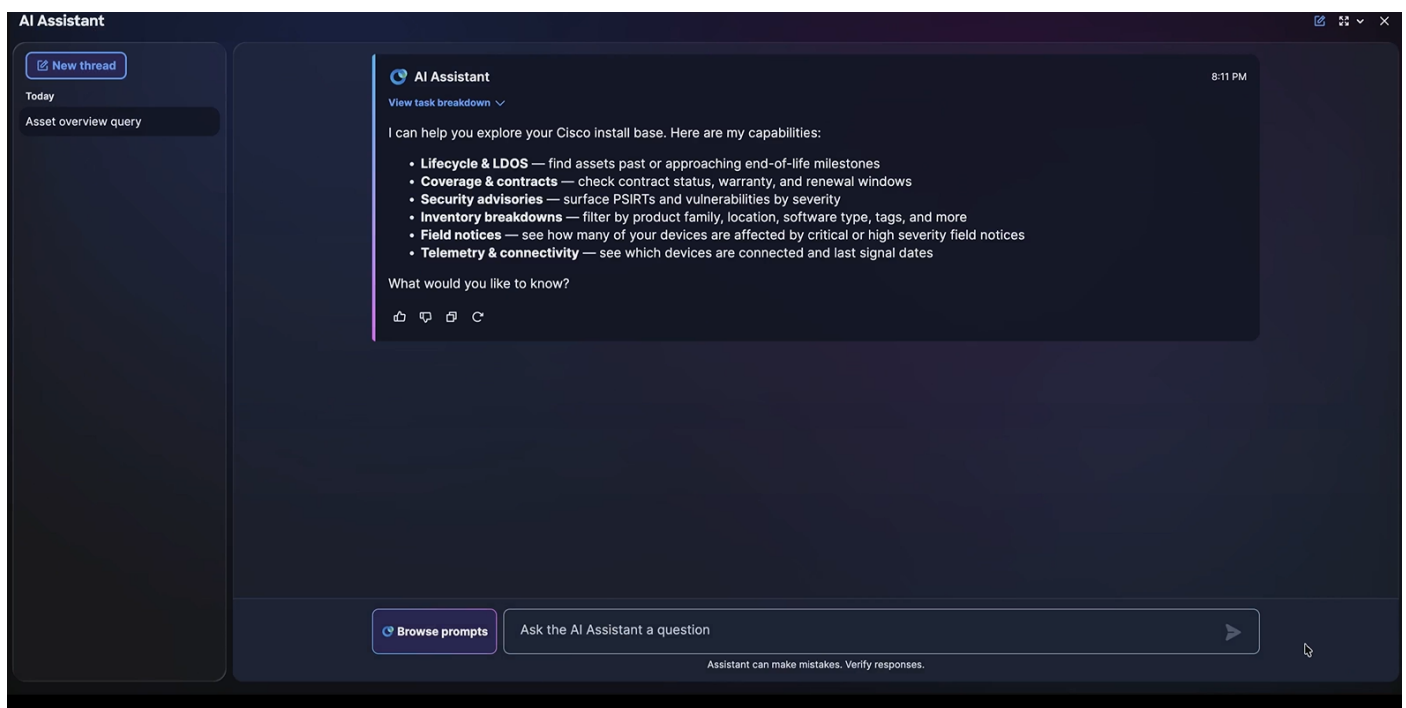
Om Ask AI te gebruiken in assets:

1. Kies het menu Home > Activa. De pagina Activa wordt weergegeven.



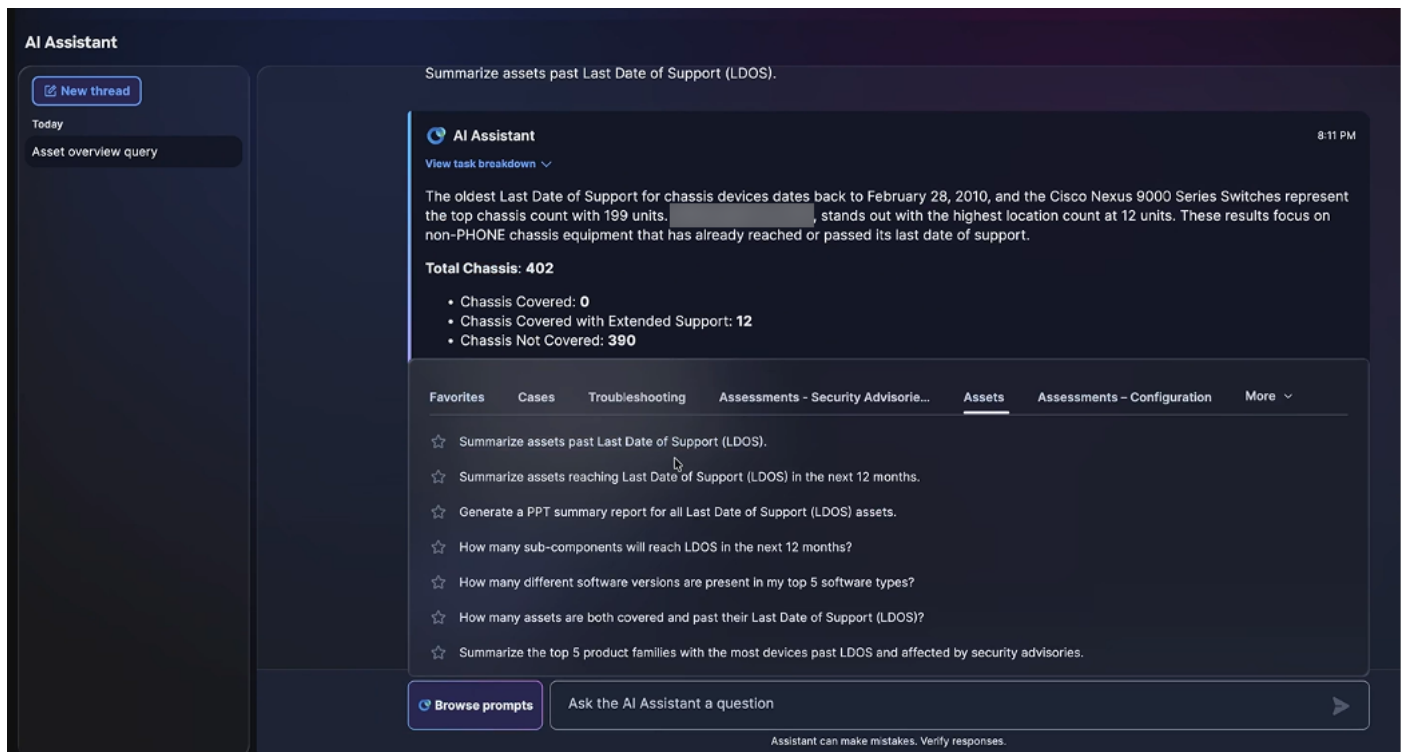
Activa pagina

2. Klik op Ask AI. De On-Prem AI Inference Infrastructure wordt gelanceerd.



Bladeren door prompts

3. Klik op Bladeren om beschikbare vragen te bekijken of voer een aangepaste vraag in het veld Vraag het de AI-assistent.



Set van prompts

4. Klik op de gewenste prompt of druk op Enter. De on-premises SLM genereert een reactie.

AI-analyse in inventaris

De On-Prem AI Inference Infrastructure-module biedt geautomatiseerde AI-gestuurde analyse in de sectie Inventory. De analyseresultaten worden automatisch weergegeven zodra de voorraadgegevens zijn ingevuld.

AI-analyse bekijken in Inventory:

1. Selecteer het menu Home > Voorraad. De pagina Voorraad wordt weergegeven.

Assets

Overview

Inventory

Service Contracts

End of Life

Assets

Q Search

1 Equipment type

Filters (1)

4231 results

Reset filters

Export

Saved Filters

Insights

Asset inventory analysis filtered to chassis equipment, covering lifecycle status, support coverage, telemetry enrollment, and software version diversity.

- Of the **1,711 assets with no active coverage**, 1,028 (60.1%) belong to the Cisco Nexus 9000 Series Switches product family. Within that uncovered population, 390 assets (46.0%) are already at **Last Date of Support**, meaning they no longer receive security patches or bug fixes from Cisco. Prioritize upgrade planning for Nexus 9000 assets that are both uncovered and past LDOS. [View](#)
- 1,711 assets (40.4%)** across the inventory are **not covered** by an active support contract, compared to 2,520 (59.6%) that are covered. Assets without coverage may have limited access to Cisco support resources if a failure occurs. Conduct a coverage review and prioritize renewal for business-critical chassis. [View](#)
- 295 assets (7.0%)** have an End of Service Contract Renewal date within the next 6 months, from Jul 8, 2026 through Jan 8, 2027, with the earliest deadline on Jul 25, 2026. Assets that pass this milestone without renewal may lose the ability to reinstate contracted support. Begin renewal planning now to avoid coverage lapses. [View](#)
- Among 453 assets with no active coverage, 280 (61.8%) have End of Software Maintenance as their next milestone. Once this milestone passes, software defect fixes will no longer be available from Cisco, compounding the risk of operating without a support contract. Prioritize coverage renewal or upgrade planning for these assets before the milestone is reached. [View](#)
- Assets with telemetry enabled average **5.1 affected Security Advisories**, while assets with telemetry not enabled average **0.0 affected Security Advisories**. This gap indicates that unconnected assets are not being evaluated for known vulnerabilities within Cisco IQ, not that they have none. Enroll chassis assets in telemetry to enable accurate advisory tracking. [View](#)

Full Analysis

Name	Product ID	Product Type	Equipment Type	Serial Number	Next Milestone	Next Milestone...	Contract Number	Coverage Status	Telemetry Status	Security Adviso...	
			Chassis			Jun 25, 2028	—	🔒	🟢	0	
			Chassis			—	204599980	🟢	🟢	35	
			Chassis			—	204599980	🟢	🟢	35	
			Chassis			Oct 29, 2026	—	🔒	🟢	3	
			Chassis			Apr 26, 2028	—	🔒	🟢	7	
			Chassis			Jul 31, 2027	—	🔒	🟢	7	
			Chassis			—	—	🔒	🟢	2	

inventaris

2. Bekijk de AI-gegenereerde analyse. De resultaten worden weergegeven in de voorraadweergave zodra de gegevens beschikbaar zijn.

 Opmerking: klik op Volledige analyse voor visualisaties zoals grafieken, dashboards en grafieken die extra inzichten bieden.

Gemeenschappelijke kenmerken voor modules

In dit gedeelte worden de kernfuncties beschreven die voor alle modules worden gedeeld. Deze functies bieden een consistente gebruikerservaring, optimaliseren de systeemprestaties en stroomlijnen administratieve workflows

Gegevens analyseren

Het panel Insights levert een AI-gestuurde analyse van de gegevens op die pagina en biedt bruikbare inzichten om de veiligheid en gezondheid van uw netwerkomgeving te verbeteren.

 Opmerking: de analysefunctie is alleen beschikbaar op geselecteerde pagina's.

Assets

Q Search Product family Product ID Location Tags Filters (1) 1716 results Reset filters Export

Insights

- 69 assets that are **not covered** by any support contract have already reached **Last Date of Support**, leaving them without security patches or bug fixes. Prioritize upgrades or replacements for these assets to mitigate operational risks. [View](#)
- 175 Cisco Catalyst 9300 Series Switches (49.7% of **not covered** assets) lack active support contracts, which may limit access to Cisco support resources. Align renewal planning with the channel partner for these business-critical switches. [View](#)
- 73 assets with **telemetry not enabled** are at **End of Software Maintenance**, reducing visibility within Cisco IQ for proactive alerts and lifecycle planning. Enable telemetry for these assets to restore full monitoring capabilities. [View](#)
- 75 assets (4.4%) have **coverage expiring** between **Apr 24, 2026** and **Oct 24, 2026**, with the earliest deadline on **Apr 30, 2026**. Review these contracts to avoid lapses in vendor support and potential cost increases. [View](#)
- 75 assets (4.4%) have **End of Service Contract Renewal** dates between **May 1, 2026** and **Oct 24, 2026**, starting with a deadline on **May 1, 2026**. Coordinate with the selling partner to renew these contracts before expiry. [View](#)

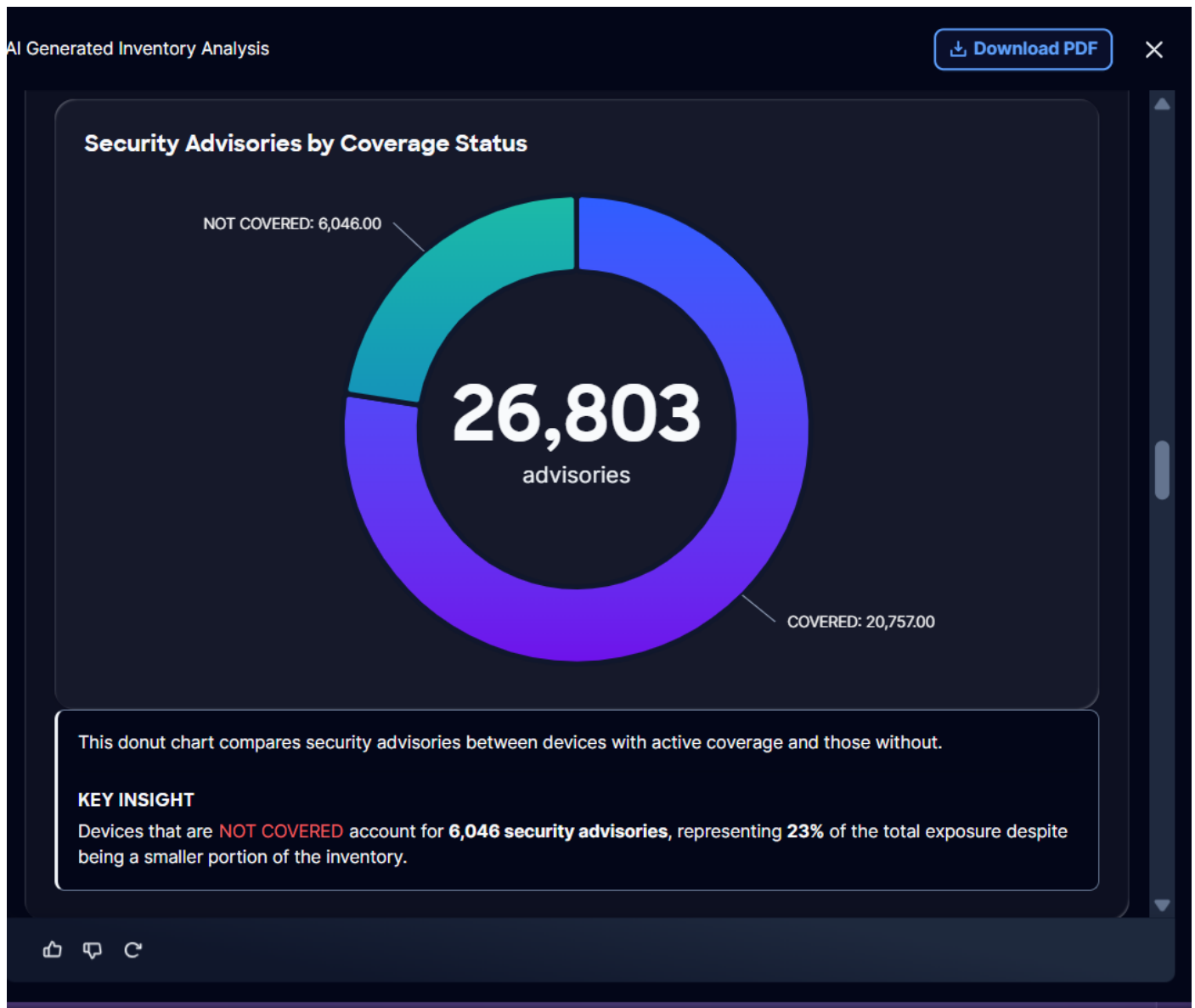
Full Analysis

Name	Product ID	Product Type	Serial Number	Next Milestone	Next Milesto...	Contract Number	Coverage Status	Telemetr y Status	Securit y...
		Cloud and ...		End of Ser...	Jun 25, 2028	—	🔒	🔵	0
		Switches		End of Ser...	Jan 29, 2027	—	🔒	🔵	4
		Switches		—	—		🔒	🔵	23
		Switches		—	—		🔒	🔵	23
		Switches		—	—		🔒	🔵	23

Inzichtenpaneel

De volgende opties zijn beschikbaar in het deelvenster Inzichten:

- Klik op het pictogram Uitvouwen om het deelvenster uit te vouwen en extra inzichten weer te geven
- Klik op het pictogram Thumbs Up of Thumbs Down om feedback te geven over de AI-gegenereerde informatie
- Klik op Volledige analyse om aanvullende informatie, diepere analyse en visualisaties zoals grafieken, dashboards en grafieken weer te geven



volledige analyse

De volgende opties zijn beschikbaar in een volledige analyse:

- Klik op PDF downloaden om een offline kopie van de analyse op te slaan voor uw records of voor samenwerking

Informatie exporteren

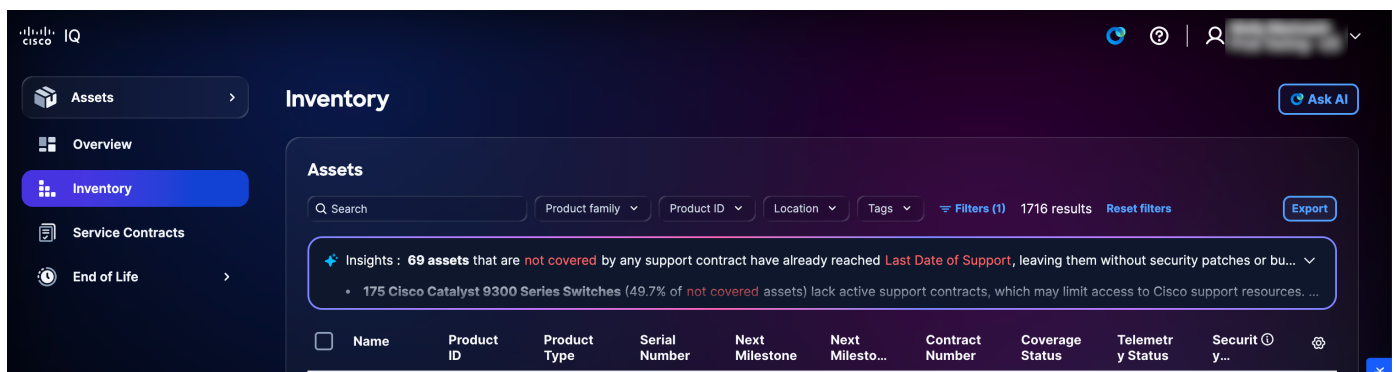
Met de exportfunctie kunt u aangepaste weergaven voor elementen en beveiligingsinformatie exporteren in de indeling .xls of .csv.



Opmerking: de exportfunctie is alleen beschikbaar voor bepaalde pagina's.

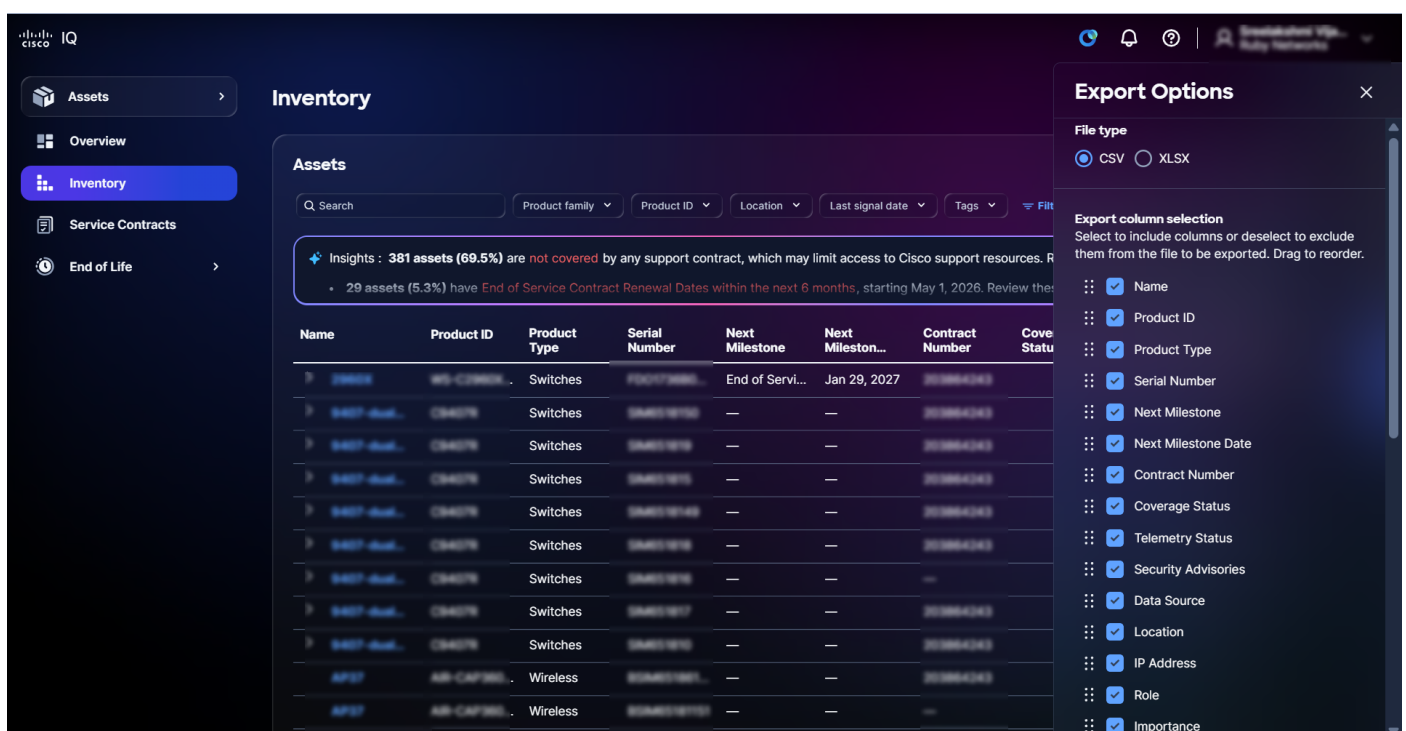
Zo exporteert u informatie van een pagina:

1. Navigeer naar de pagina.



Voorraad exporteren in de module Activa

2. Klik op Exporteren. Het display Exportopties.



Exportopties

3. Selecteer een bestandstype.

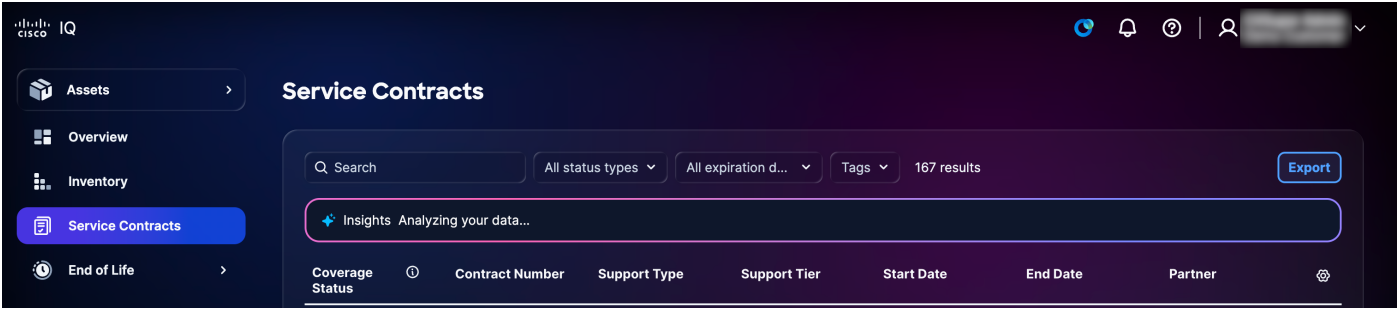
4. Schakel het selectievakje in de gewenste kolom(en) in.

5. Klik op Exporteren. Het bestand wordt gedownload naar de lokale downloadmap van de

browser.

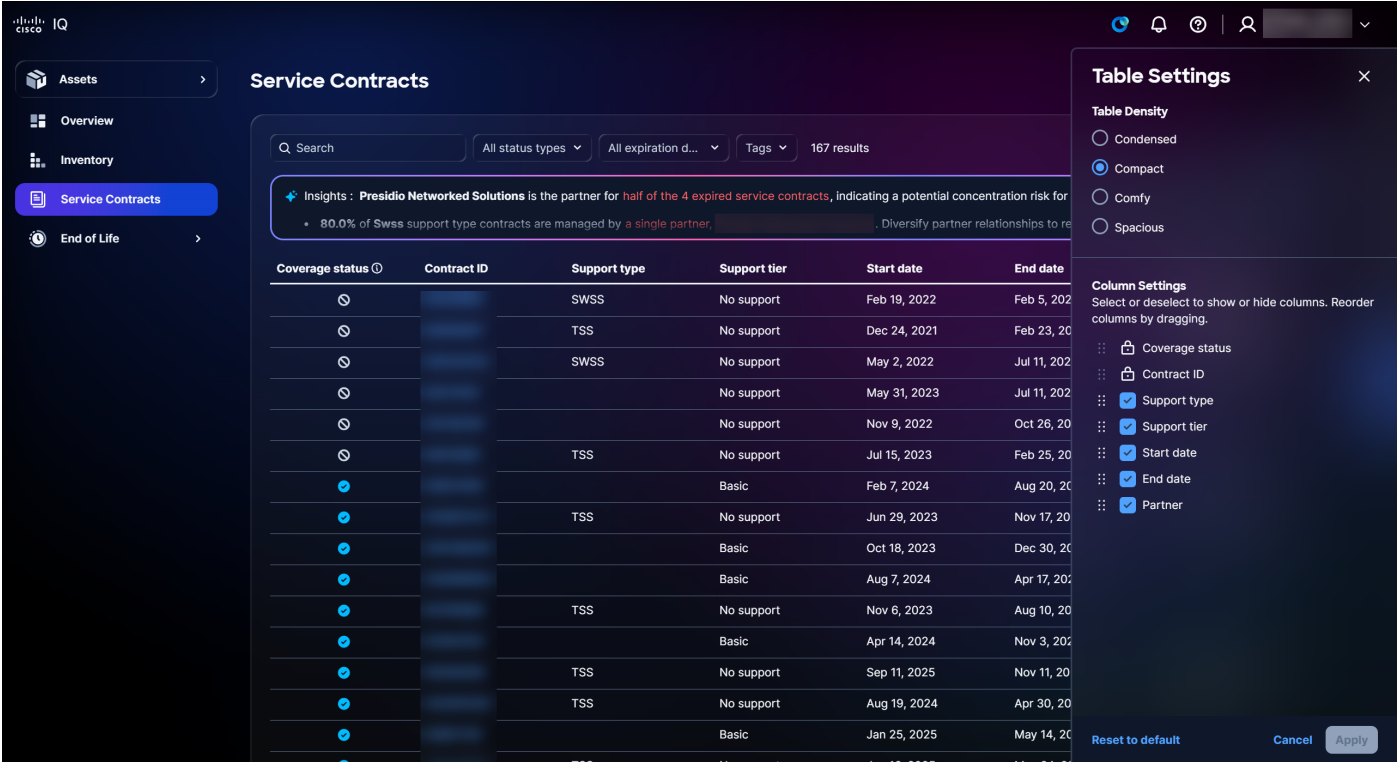
Tabelinstellingen

U kunt tabelinstellingen configureren om aangepaste en verfijnde weergaven voor verschillende modulefuncties te maken.



Tabelinstellingen

Als u de kolommen op geselecteerde pagina's wilt wijzigen, klikt u op het pictogram Tabelinstellingen. De tabelinstellingen worden weergegeven.



Tabelinstellingsopties

Tabelweergave wijzigen

De tabelweergave wijzigen:

1. Selecteer een van de volgende opties voor tabeldichtheid:

- Gecondenseerd: minimaliseert visuele elementen en afstand om meer informatie weer te geven
- Compact: vermindert witruimte en scherpt de afstand tussen UI-elementen aan
- Comfortabel: maakt gebruik van meer witruimte en grotere afstand tussen elementen
- Ruim: benadrukt overvloedige witruimte en grotere UI-elementen

2. Klik op Apply (Toepassen).

Kolommen toevoegen en verwijderen

U kunt als volgt kolommen toevoegen of verwijderen:

1. Schakel de selectievakjes Kolominstellingen in of uit.

2. Klik op Apply (Toepassen).



Opmerking: de kolom Naam kan niet uit de tabelweergave worden verwijderd.

Kolomvolgorde wijzigen

Zo wijzigt u de kolomvolgorde:

1. Sleep de kolomnaam om de items in de gewenste volgorde te rangschikken.

2. Klik op Apply (Toepassen).

Dashboards aanpassen

Met de functie Aangepast dashboard kunt u standaarddashboards personaliseren via een reeks intuïtieve aanpassingsopties:

- Dashboardwidgets of deelvensters opnieuw rangschikken met de functie slepen en neerzetten
- Verwijder alle onderdelen die niet relevant zijn voor uw workflow
- Uw gepersonaliseerde dashboardlay-out wordt veilig opgeslagen in uw gebruikersprofiel en automatisch toegepast op alle sessies en apparaten
- Herstel de oorspronkelijke dashboardlay-out met een eenvoudige resetoctie

Een dashboard aanpassen:

1. Navigeer naar het dashboard.



aanpassen

2. Klik op Aanpassen.



Dashboard bewerken

3. Wijzig het dashboard naar wens:

- Herschikken: Sleep de widgets naar de gewenste lay-out
- Verwijderen: Klik op het Verwijderen pictogram om een widget te verwijderen
- Resetten: Klik op Resetten om de standaardinstelling te wijzigen om het dashboard terug te zetten naar de oorspronkelijke lay-out

4. Klik op Save (Opslaan). Er wordt een bericht Dashboard Saved weergegeven.

De lay-out van het dashboard wordt automatisch toegepast op alle sessies en apparaten.

Filters aanpassen

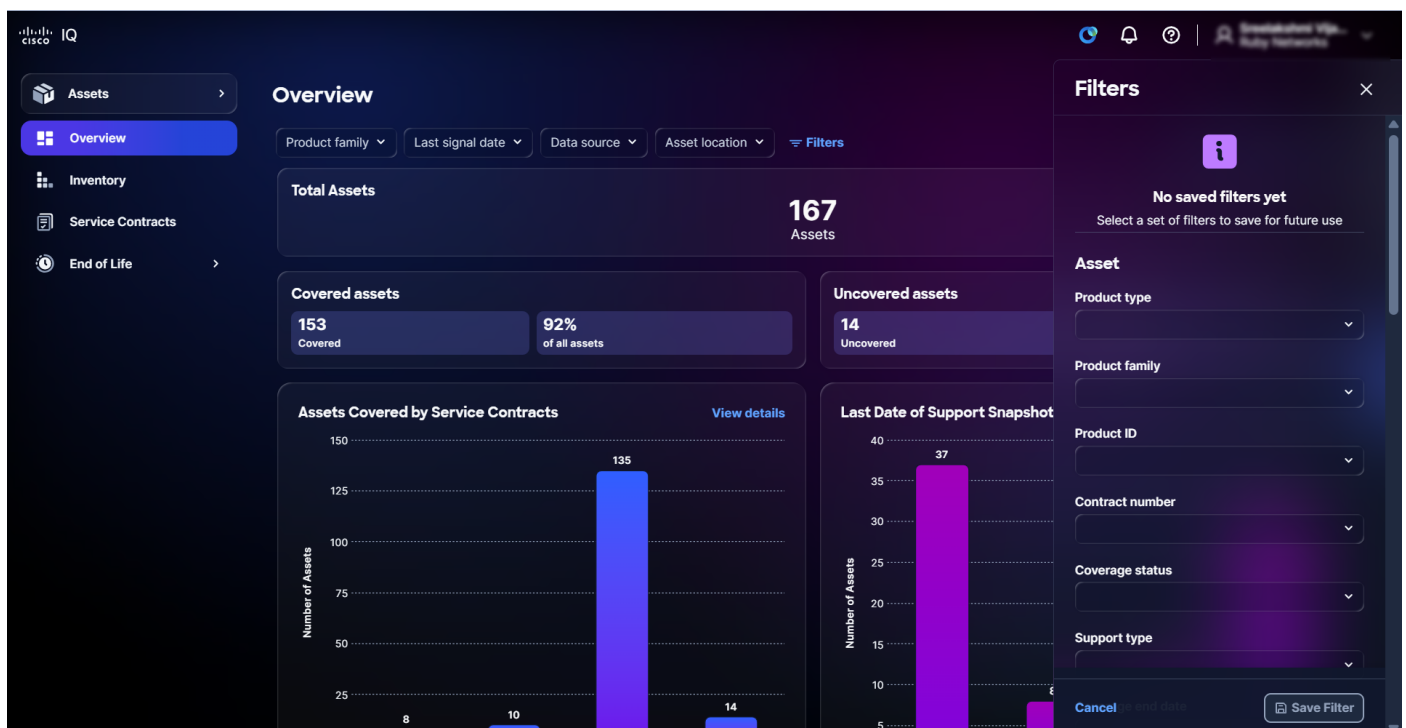
U kunt aangepaste filterconfiguraties opslaan voor elke dashboardweergave, zodat u eenvoudig naar uw voorkeursinstellingen kunt terugkeren als dat nodig is. Alle filtervoorkeuren worden veilig

opgeslagen per gebruiker, per account, waardoor een gepersonaliseerde en consistente ervaring wordt gegarandeerd elke keer dat u Cisco IQ gebruikt.

Een filter maken

U maakt als volgt een aangepast filter:

1. Navigeer naar het dashboard.
2. Klik op Filters.



Filters

3. Kies de gewenste filters uit de vervolgkeuzelijsten.
4. Klik op Filter opslaan. Het venster Naam opgeslagen filter wordt geopend.

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

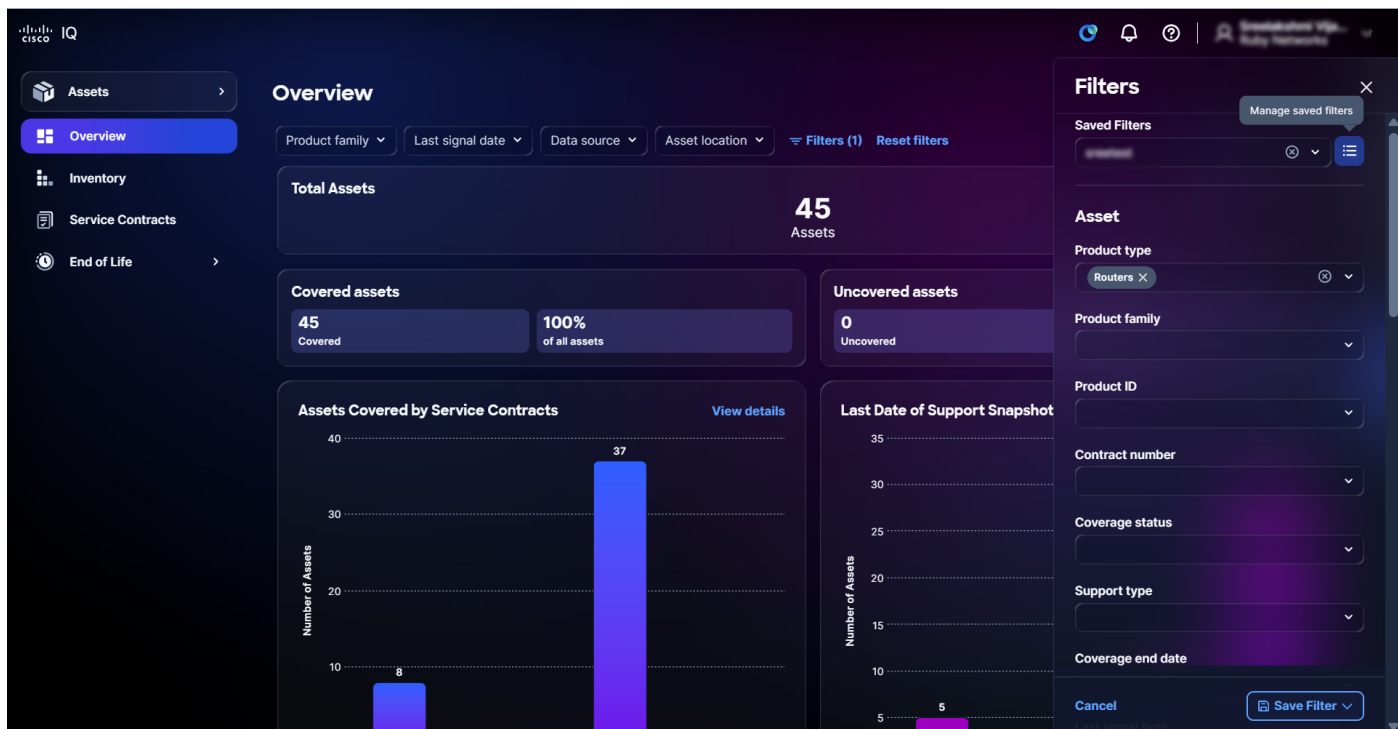
Naam filter

5. Voer een filternaam in.
6. Klik op Filter opslaan om te bevestigen.

Een filternaam bewerken

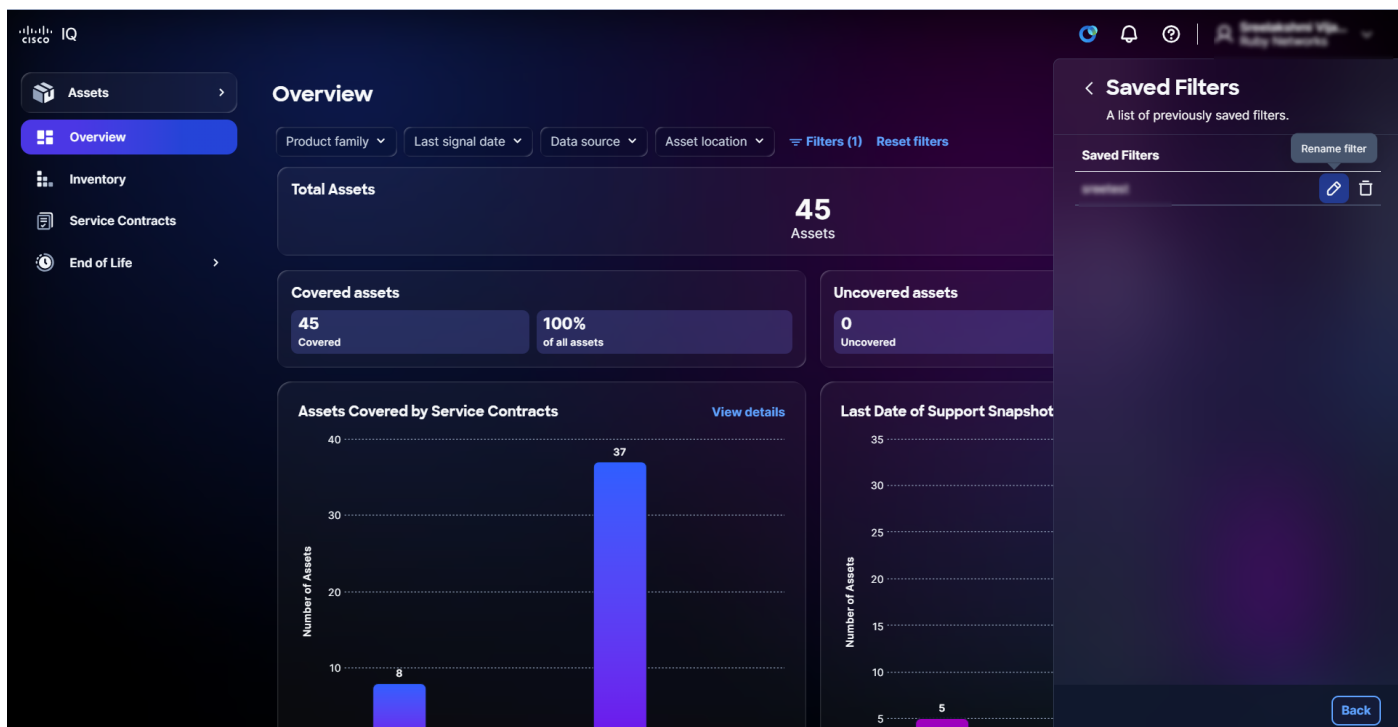
Een aangepast filter bewerken:

1. Klik op Filters.



Opgeslagen filters beheren

2. Klik op het pictogram Opgeslagen filters beheren.
3. Navigeer naar het filter.



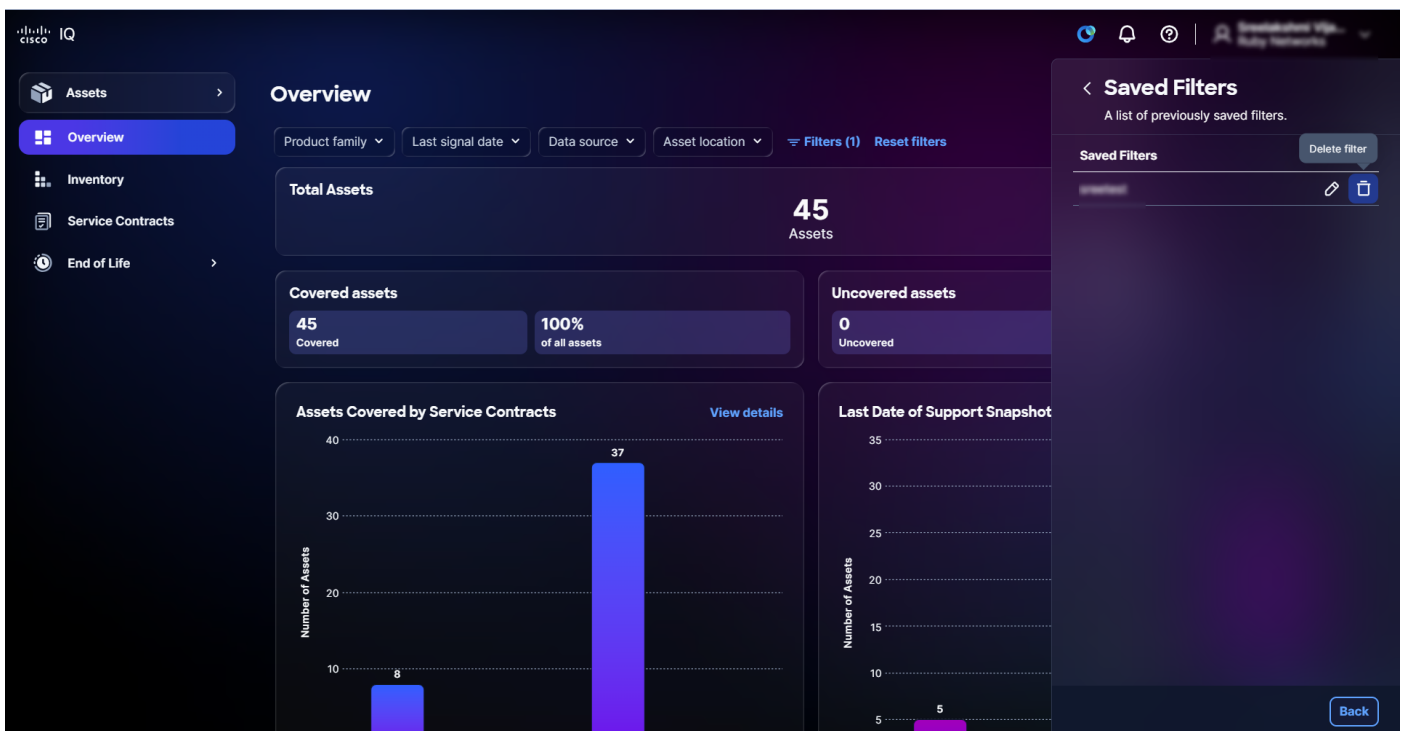
Filter bewerken

4. Klik op het pictogram Bewerken. Het venster Naam opgeslagen filter wordt geopend.
5. Bewerk de filternaam.
6. Klik op Filter opslaan om te bevestigen.

Een filter verwijderen

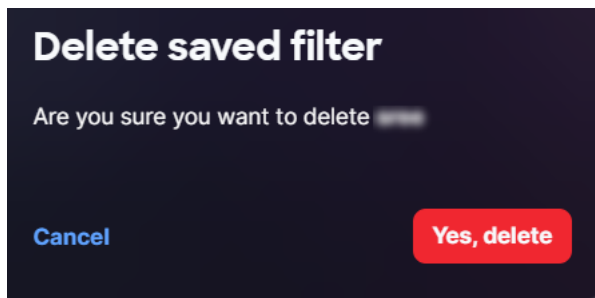
U verwijdert als volgt een aangepast filter:

1. Klik op Filters.
2. Klik op het pictogram Beheerde opgeslagen filters
3. Navigeer naar het filter.



Opgeslagen filter verwijderen

4. Klik op het pictogram Verwijderen. Het venster Opgeslagen filter verwijderen wordt geopend.



Opgeslagen filterbevestiging verwijderen

5. Klik op Ja, verwijderen om te bevestigen.

Activa-module

De Assets-module biedt uitgebreide zichtbaarheid en beheermogelijkheden voor Cisco-bedrijfsmiddelen en vormt de basis van Cisco IQ, met een gecentraliseerde lijst van alle apparaten binnen een organisatie. Door informatie uit meerdere bronnen te verzamelen, fungeert het als een enkele bron van waarheid voor apparaatinventaris. Het bijhouden van een volledige en nauwkeurige lijst met bedrijfsmiddelen is essentieel, omdat andere modules binnen Cisco IQ, zoals de evaluatiemodule, op deze gegevens vertrouwen om de gezondheid en beveiliging van uw apparaten te beoordelen.

Kernbegrippen

De Assets-module is gebaseerd op de volgende kernconcepten:

- **Asset:** elk fysiek apparaat, hardware of software dat wordt geïnventariseerd en beheerd als onderdeel van de dienstverlening van Cisco, met gedetailleerde tracking van de identiteit, functie, servicedekking en levenscyclus
- **Activa uit hoofde van contracten:** activa die rechtstreeks uit gekoppelde gegevens van servicecontracten in de inventaris worden opgenomen, in plaats van via telemetrie. Cisco IQ neemt de volgende apparatuurtypen uit contractgegevens in: chassis, modules, voedingen en ventilatoren. Deze activa zijn zichtbaar in de Inventory, zelfs als er geen telemetrieverbinding aanwezig is
- **Last Date of Support (LDOS):** mijlpaaltracering voor het einde van de levenscyclus en het einde van de support voor Cisco-producten
- **Servicedekking:** actieve supportcontracten, garanties en rechtenniveaus voor een specifiek hardware- of softwarepakket

- Asset Tag: een door de gebruiker gedefinieerd label dat is toegewezen aan een bedrijfsmiddel voor organisatie-, filter- en operationele workflows
- Apparaatsignaal: verwijst naar wanneer Cisco voor het laatst een apparaat heeft waargenomen (op basis van het serienummer) op basis van apparaattelemetrie, ondersteuningscases en contractverlengingen; telemetriegegevens van bedrijfsmiddelen worden ingenomen en verrijkt via een gegevenspijplijn met meerdere lagen

Access Assets Module

Als u toegang wilt krijgen tot functies voor bedrijfsmiddelenbeheer in Cisco IQ, kiest u het menu Home > Bedrijfsmiddelen of klikt u op Bedrijfsmiddelen in het gedeelte Toepassing van de startpagina > Launchpad tabblad. De pagina Overzicht wordt weergegeven.

Overzicht van bedrijfsmiddelen

Op de pagina Overzicht wordt een dashboard weergegeven waarmee u snel de gezondheid en status van apparaten kunt evalueren.

100k Assets, Asset ID: 100k Assets, Asset ID: 100k Assets



Assets



Overview



Inventory



Service Contracts



End of Life



Overview

Filters

Ask AI

Customize

Saved Filters

Total Assets

199

Assets

928

Assets and subcomponents

Key Asset Metrics

Covered Assets

186

Covered

93%

Of all assets

Uncovered Assets

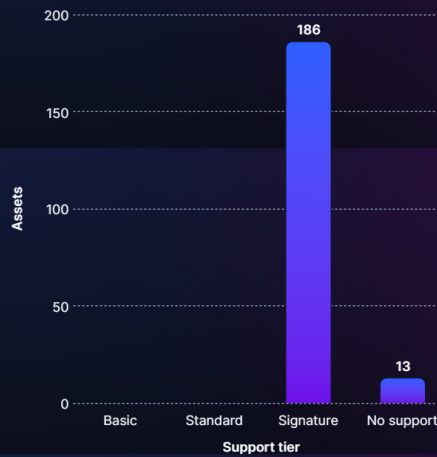
13

Uncovered

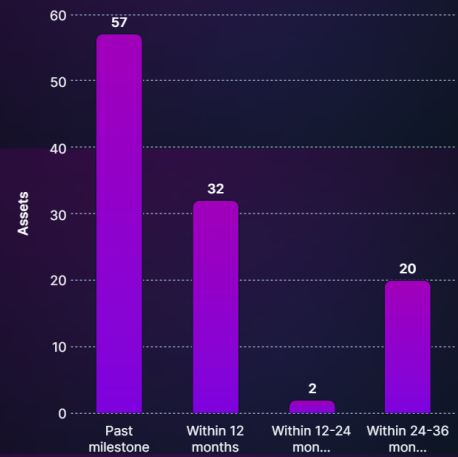
7%

Of all assets

Assets Covered by Service Contracts [View details](#)



Last Date of Support Snapshot [View details](#)



Assets With Telemetry Enabled

186

With telemetry

93%

Of all assets

Assets Without Telemetry Enabled

13

Without telemetry

7%

Of all assets

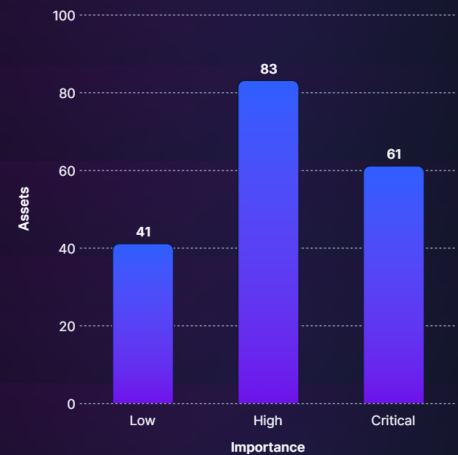
Assets With Critical or High Security Advisories [View details](#)



Of the 186 assets with telemetry enabled, 170 have critical or high Security Advisories

Assets by Importance [View details](#)

Importance can be evaluated for 185 assets.

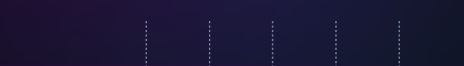


Asset Breakdown

Top 5 Product Families [View details](#)



Top 5 Install-At Locations [View details](#)



Overzicht van bedrijfsmiddelen

Het dashboard geeft de volgende informatie weer:

- Totale activa: het totale aantal activa binnen de Cisco IQ-account
- Belangrijkste bedrijfsmiddelenstatistieken: aanvullende belangrijke statistieken zoals telemetriestatus, kritieke beveiligingsadviezen en LDOS-informatie
- Gedekte activa: het totale aantal en percentage activa die onder dienstencontracten vallen
- Niet-gedekte activa: het totale aantal en percentage activa die niet onder dienstencontracten vallen
- Activa die vallen onder servicecontracten: een uitsplitsing van het aantal activa — hardware of software — dat onder servicecontracten valt, gecategoriseerd op rechtenniveau
- Laatste datum van momentopname van ondersteuning: een uitsplitsing van het aantal activa dat LDOS heeft overschreden of LDOS heeft bereikt
- Activa waarvoor telemetrie is ingeschakeld: Totaal aantal en percentage van activa waarvoor telemetrie is ingeschakeld
- Activa zonder telemetrie ingeschakeld: Totaal aantal en percentage activa zonder telemetrie ingeschakeld
- Activa met kritieke of hoge beveiligingsadviezen: het percentage van de totale activa waarvoor telemetrie is ingeschakeld en die kritieke of hoge beveiligingsadviezen hebben
- Activa op belangrijkheid: een uitsplitsing van de prioriteit die is toegewezen aan een apparaat ten opzichte van andere apparaten in het netwerk.
- Uitsplitsing van bedrijfsmiddelen: een gedetailleerde weergave van bedrijfsmiddeleninformatie, zoals productfamilies, installatielocaties, softwareversies en bedrijfsmiddelenrollen

Weergaven voor elementen filteren

U kunt de dashboardweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op Filters te klikken en een optie te kiezen in de lijst met beschikbare filters.



Opmerking: sommige filters kunnen worden verborgen, afhankelijk van de

 schermzoominstellingen. Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

Details bekijken voor bedrijfsmiddelen

Wanneer u op Details weergeven klikt, wordt de pagina omgeleid naar de pagina Voorraad. Zie [Voorraad](#) voor meer informatie.

Asset Criticality Insights

Cisco IQ bevat Asset Criticality Insights, een nieuwe mogelijkheid in de Assets-module die de functionele rol en het zakelijke belang van netwerkapparaten voorspelt. Door apparaatconfiguraties en ingeschakelde functies te analyseren, helpt Asset Criticality Insights u te bepalen welke middelen de grootste impact op uw netwerk hebben, zodat u ze kunt prioriteren voor beveiligingsherstel, software-upgrades, End-of-Life (EOL) planning en dekkingsbeslissingen.

 **Opmerking:** Asset Criticality Insights zijn uitsluitend beschikbaar voor activa met standaard- of handtekeningniveaus die actieve telemetrieverbindingen hebben. Zorg ervoor dat uw bedrijfsmiddelen voldoen aan de configuratievereisten om deze inzichten in het dashboard in te vullen.

Asset Criticality Insights zijn beschikbaar in de Assets-app op de volgende gebieden:

- Activa-overzicht: uitsplitsingen filteren en weergeven op basis van eigenschappen van Asset Criticality Insights
- Inventarisatie van bedrijfsmiddelen: apparaten weergeven, zoeken, filteren en sorteren op rol en belang
- Asset Details: bekijk de rol en het belang van afzonderlijke apparaten, met informatieve tooltips waarin elke waarde wordt uitgelegd

Overheersende rol en belangrijkheidsclassificaties

Cisco IQ voorspelt automatisch de rol en het belang van elk actief op basis van telemetriegegevens. Accountbeheerders kunnen deze classificaties handmatig corrigeren wanneer de geautomatiseerde voorspelling de functie of kritieke positie van het bedrijfsmiddel in het netwerk niet nauwkeurig weergeeft.



Opmerking: besturingselementen voor overschrijven zijn alleen beschikbaar voor accountbeheerders. De waarden Rol en Belang zijn alleen-lezen voor alle andere gebruikersrollen.

Classificaties overschrijven uit de inventaristabel

De rol of het belang voor een of meer elementen negeren:

1. Navigeer naar Bedrijfsmiddelen > Voorraad.
2. Klik op het selectievakje van de gewenste rij met bedrijfsmiddelen. Als u meerdere elementen tegelijk wilt bijwerken, schakelt u meerdere selectievakjes in.

The screenshot shows the Cisco IQ Inventory page. On the left is a sidebar with navigation options: Assets, Overview, Inventory (selected), Service Contracts, and End of Life. The main area is titled 'Inventory' and contains an 'Assets' section. At the top of the Assets section, there's a search bar, filters (2), 20 results, and buttons for Export and Saved Filters. Below this, an insights box states: 'Of the 1 assets where Coverage Status is not covered, 1 (100.0%) have Product Description NCS 560 Route...'. A bar indicates '4 items selected' with 'Cancel' and 'Manage Tags' buttons. The table below has columns: Name, Product ID, Product Name, Equipment Name, Serial Number, Next Mile, Next Mile, Contract, Coverage, Telemetry, and a final column with values 0, 0, 1, 0. The third row is selected.

	Name	Product ID	Product Name	Equipment Name	Serial Number	Next Mile	Next Mile	Contract	Coverage	Telemetry	
☐			Modules	Module		—	—		✓	✓	0
☐			Modules	Module		—	—		✗	✓	0
☒			Unified ...	Chassis		—	—		✓	✓	1
☐			Storage...	Chassis		—	—		✓	✓	0

Rol en belang

3. Kies in de kolom Rol of Belang de juiste waarde in de vervolgkeuzelijst van de rij met elementen.
4. Klik op Toepassen om de overschrijving te bevestigen.

Middelen met handmatig overschreven waarden geven een visuele indicator weer in de kolom Rol of Belang.



Opmerking: Als u een eerder geconfigureerde overschrijving wilt verwijderen en wilt terugkeren naar de automatische voorspelling, selecteert u de optie streepje (—) in de vervolgkeuzelijst Rol of Belang.

Classificaties overschrijven op basis van gegevens over bedrijfsmiddelen

De rol of het belang overschrijven vanuit de detailweergave van het bedrijfsmiddel:

1. Navigeer naar Assets > Inventory en klik op een asset.
2. Zoek de velden Rol en Belang in het paneel met activumgegevens.
3. Klik op de vervolgkeuzelijst voor het veld dat u wilt bijwerken en selecteer de juiste waarde.
4. Klik op Toepassen om te bevestigen.

De detailweergave van een actief geeft ook een uitleg van de telemetriekenmerken die de oorspronkelijke geautomatiseerde voorspelling hebben geïnformeerd, om te helpen bij het bepalen of een overschrijving geschikt is.

Het controlespoor negeren bekijken

Alle belangrijke en belangrijke overschrijvingen worden geregistreerd in een controletraject op accountniveau. Toegang tot het controlespoor:

1. Kies Home > Systeeminstellingen > Activiteit en logboeken.
2. Kies Filters > Actietype > Overschrijven om alleen override-gebeurtenissen weer te geven.

In het controlespoor worden de naam van het bedrijfsmiddel, de vorige en nieuwe waarden, de gebruiker die de wijziging heeft aangebracht en de datum en tijd van de wijziging weergegeven. Het controlespoor kan worden geëxporteerd met de optie Exporteren.



Opmerking: het controlespoor kan worden gefilterd op datumbereik, gebruiker en activanaam.

inventaris

Op de pagina Voorraad vindt u een lijst met alle Cisco-bedrijfsmiddelen in het Cisco IQ-account.

inventaris

Weergaven voor bedrijfsmiddelen zoeken en filteren

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op Filters te klikken en een optie te kiezen in de lijst met beschikbare filters. U kunt ook naar elementen zoeken door de naam van het element in te voeren in het veld Zoeken.

 **Opmerking:**

- Sommige filters zijn mogelijk verborgen, afhankelijk van de schermzoominstellingen.
- Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

voorraadanalyse

Het Insights panel op de Inventory pagina toont een AI-gestuurde analyse die een samenvatting van assets geeft met een focus op support dekking, connectiviteit en mijlpalen. Klik op Volledige analyse voor visualisaties zoals grafieken, dashboards en grafieken die extra inzichten bieden. Zie [Gegevens analyseren](#) in gemeenschappelijke modulefuncties voor meer informatie.

Voorraad exporteren

Klik op Exporteren om een gefilterde inventarislijst op te slaan in .xls- of .csv-indeling. Zie [Informatie exporteren](#) in Gemeenschappelijke modulefuncties voor meer informatie.

Gegevens over bedrijfsmiddelen bekijken

Klik op een actief om de details van het actief te bekijken. De detailweergave van een element wordt weergegeven met de volgende tabbladen:

- Details: hiermee worden details van bedrijfsmiddelen weergegeven, zoals product-, signaalgegevens, identiteit, locatie, garantie- en dekkingsinformatie

Assets

Overview

Inventory

Service Contracts

End of Life

← Inventory

10.197.236.131

Ask AI

Cisco Catalyst Center Appliance (Gen 2) - 44 Core

Details

Product Alerts

Hardware

Software

Product

Product ID

Product type

Product family

Last Date of Support

Identity

Serial number

IP address

Hostname

Software version

Role

Importance

Tags

Sold by

Location

Install-at

Signals

Last signal

Last signal type

Telemetry

Telemetry status

Last data collection

Data connector

Warranty

Warranty type

Warranty end date

Coverage

Coverage status

Contract number

Support tier

Coverage end date

Gegevens over bedrijfsmiddelen

- Productwaarschuwingen: hiermee worden gerelateerde productwaarschuwingen

weergegeven, zoals veiligheidsadviezen en veldmeldingen

- Hardware: biedt een gedetailleerde tijdlijnweergave voor hardware-EOL (bijvoorbeeld Einde van de verkoop, Laatste verzending en Laatste datum van supportdatums)
- Software: biedt een gedetailleerde tijdlijnweergave voor software-EOL

Asset-tags

Asset-tags zijn aangepaste labels die u toewijst aan inventarismiddelen in Cisco IQ. Een tag is een key: value-paar (bijvoorbeeld Environment: Prod of Label: Campus) dat u definieert. U kunt tags toewijzen aan afzonderlijke bedrijfsmiddelen of meerdere bedrijfsmiddelen tegelijk en u kunt uw voorraad filteren op tag om snel de bedrijfsmiddelen te vinden waar u om geeft.

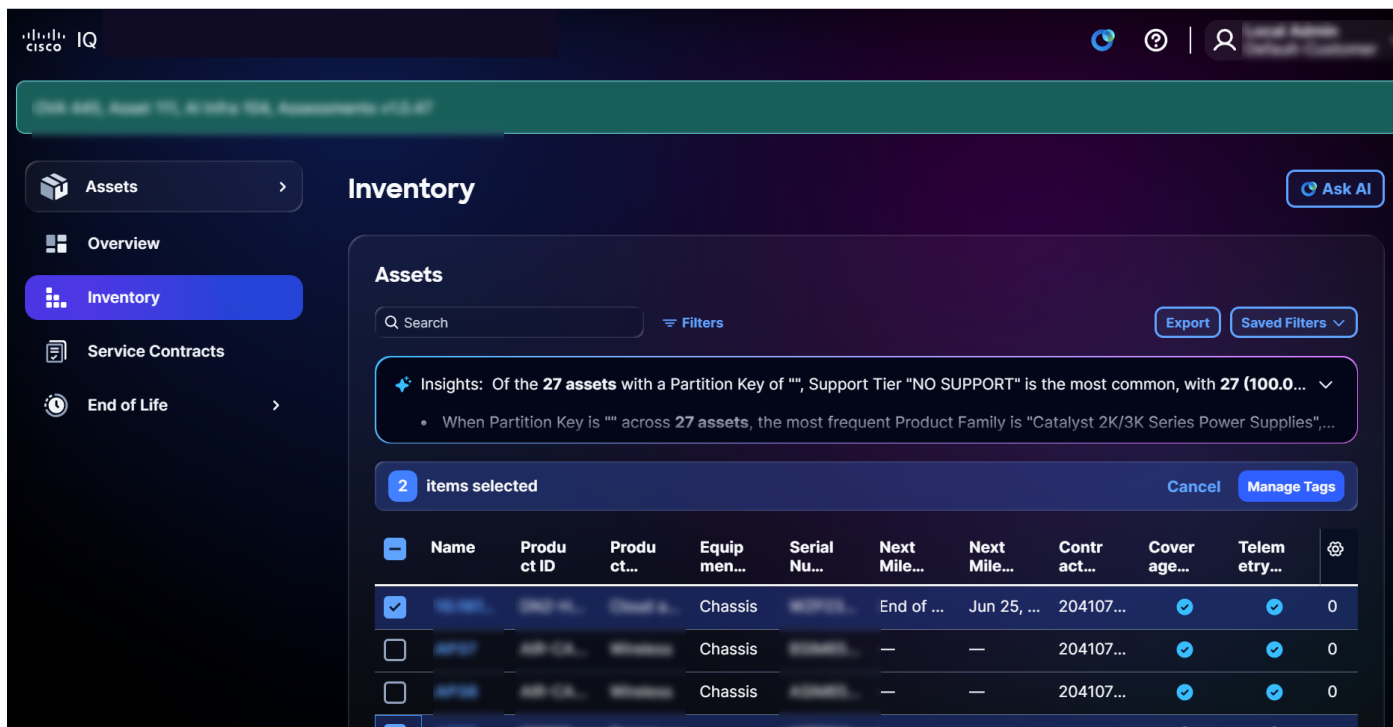
 **Opmerking:** nadat een tag is gemaakt door een accountbeheerder, kunnen gebruikers een tag toewijzen aan een actief.

Tags toewijzen

Door tags toe te wijzen aan geselecteerde elementen in de weergave Voorraad kunnen assets worden geordend en gecategoriseerd voor verbeterde filtering, rapportage en beheer.

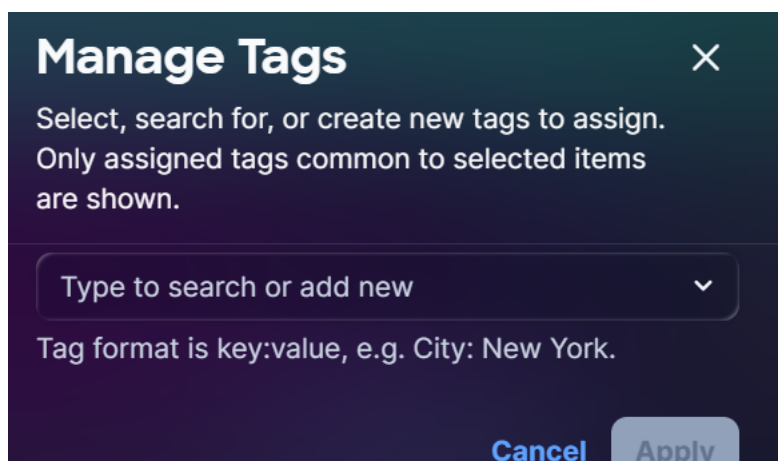
Om een tag aan een asset toe te wijzen:

1. Navigeer naar Bedrijfsmiddelen > Voorraad.



elementen labelen

2. Selecteer de selectievakjes van de gewenste elementen.
3. Klik op Tags beheren. Het venster Tags beheren wordt geopend.



Tags toewijzen

4. Voer in het tekstveld de labelnaam in of selecteer deze uit de bestaande opties en druk op Enter.



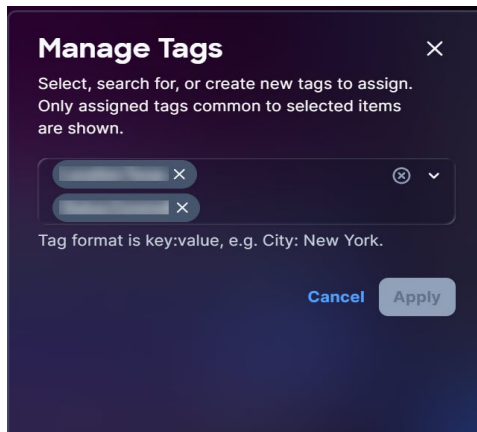
Opmerking: Tags zijn in sleutel: waarde formaat (bijvoorbeeld City: NYC).

5. Klik op Apply (Toepassen).

Asset-tags verwijderen

U verwijdert een tag als volgt uit een of meer elementen:

1. Navigeer naar Bedrijfsmiddelen > Voorraad.
2. Schakel het selectievakje naast een of meer elementen in.
3. Klik op Tags beheren. Het venster Tags beheren wordt geopend.



Tags verwijderen

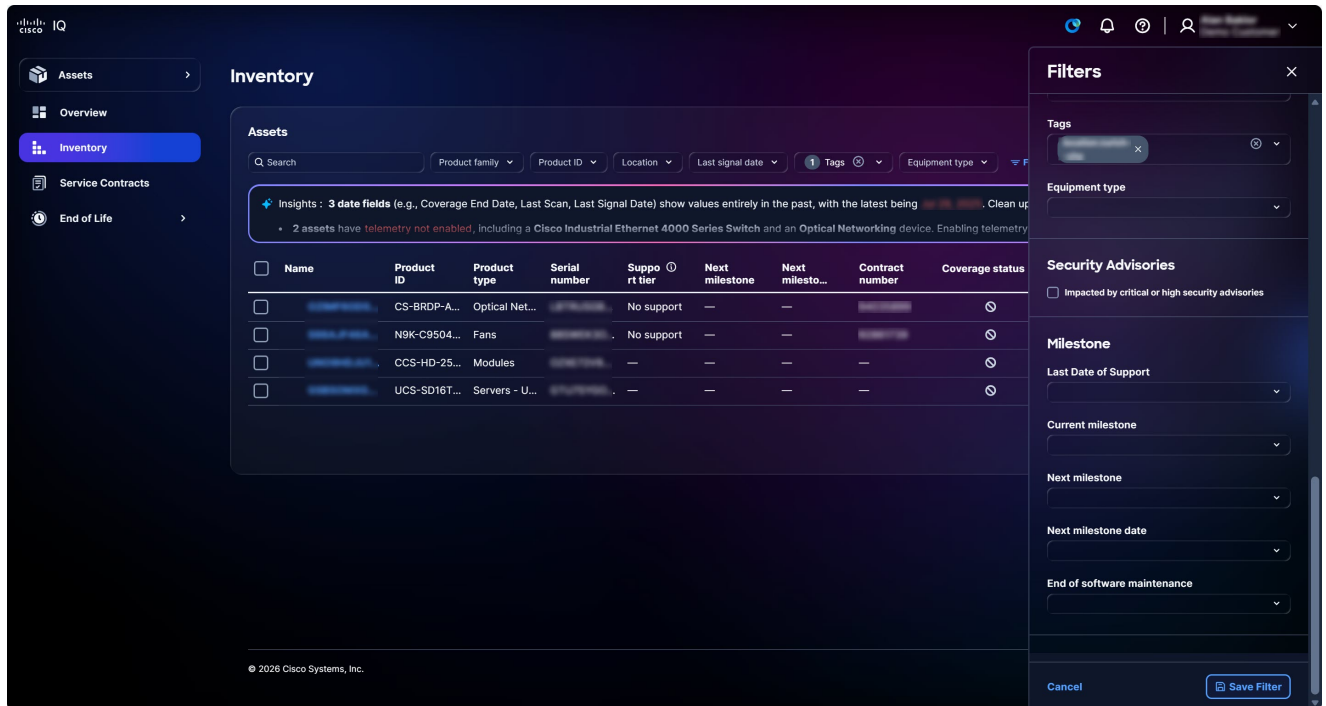
4. Klik op de X op een tag om deze uit de selectie te verwijderen.
5. Klik op Apply (Toepassen).

Asset-tags als filters gebruiken

Nadat u een tag hebt gemaakt, kunt u de tag als filter gebruiken.

Om een tag als filter te gebruiken:

1. Navigeer naar de pagina Inventaris.
2. Klik op Filters. Het venster Filters wordt geopend.

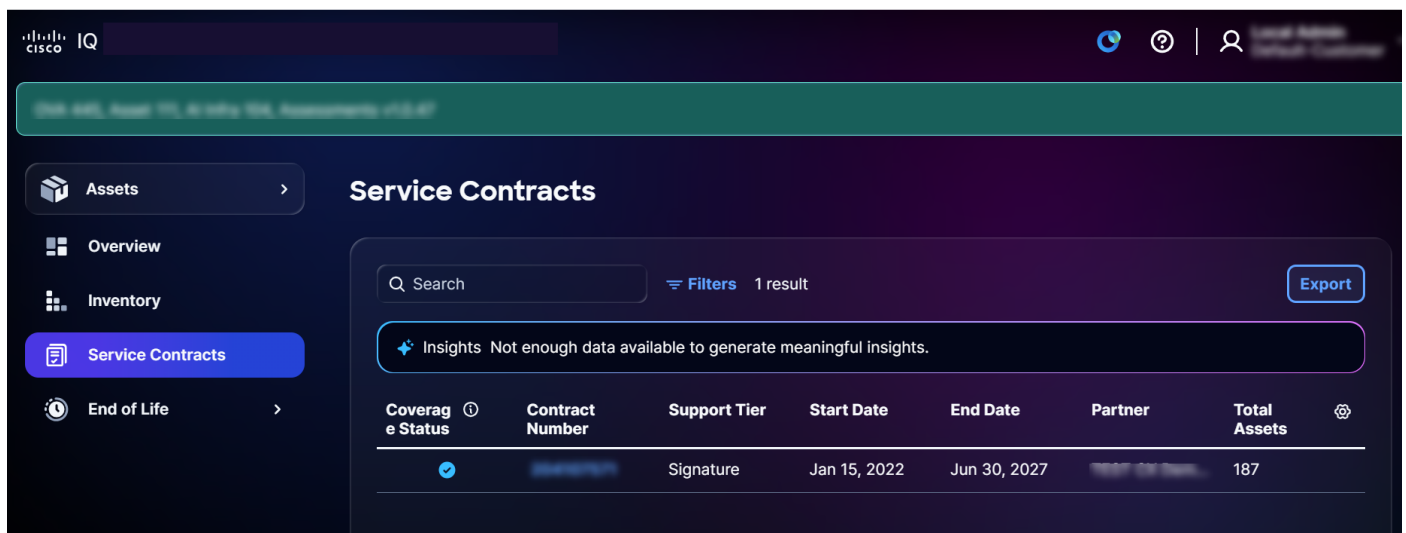


Tag als filter gebruiken

- Schakel in de vervolgkeuzelijst Tags de selectievakjes van de gewenste tags in. Nadat u de tag hebt geselecteerd, wordt de weergave op de voorraadpagina bijgewerkt naar de gefilterde weergave.

Dienstencontracten

De pagina Servicecontracten stroomlijnt het toezicht op het ondersteuningscontract door samenvattingen en gedetailleerde contractinformatie te bieden, ter ondersteuning van effectieve planning en dekkingstrategieën voor verlenging.



Dienstencontracten

Weergaven zoeken en filteren voor servicecontracten

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten. U kunt ook naar servicecontracten zoeken door het contractnummer in het veld Zoeken in te voeren.

Dienstencontracten exporteren

Klik op Exporteren om een gefilterde lijst met contracten op te slaan in .xls- of .csv-indeling. Zie [Informatie exporteren](#) in Gemeenschappelijke modulefuncties voor meer informatie.

Services EA-overzicht

De overzichtspagina van de Enterprise Services Agreement (EA) biedt een geconsolideerd overzicht van de groei van de installatiebasis voor uw gehele activaportefeuille. De gegevens zijn rechtstreeks afkomstig uit Cisco's Install Base-records, waardoor u en accountteams een consistent beeld hebben van wijzigingen in de portefeuille in de loop van de tijd.

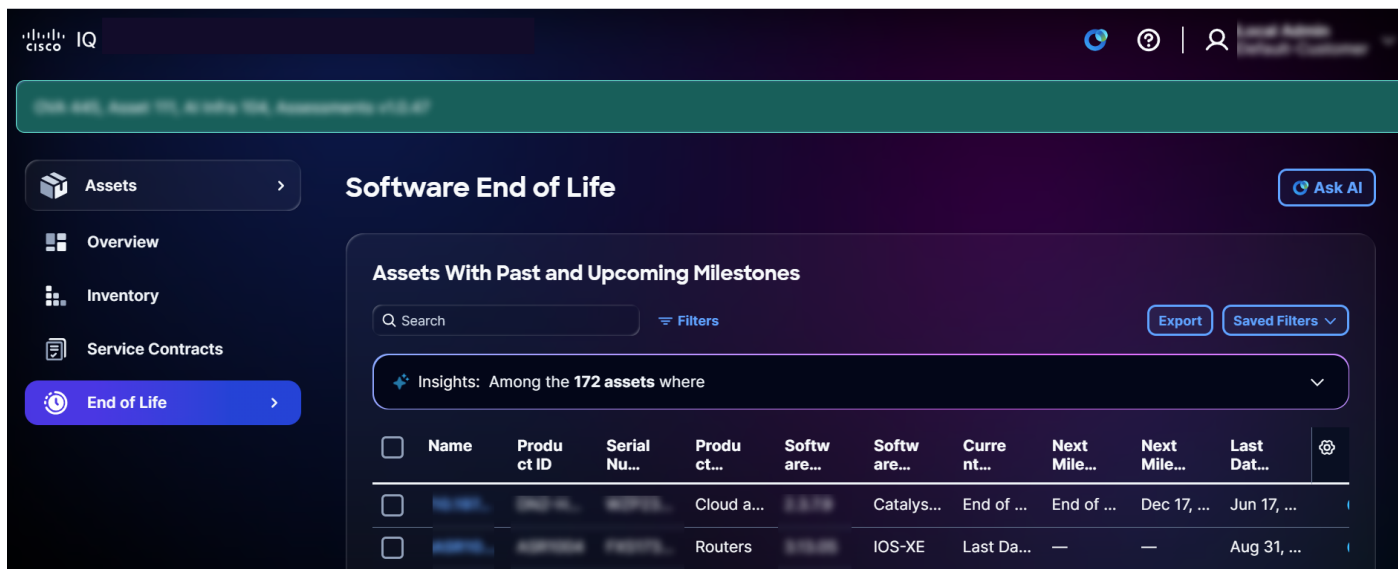
Op de pagina Services EA Summary wordt de volgende informatie weergegeven:

- Toegevoegde activa: nieuwe activa toegevoegd aan de installatiebasis tijdens de verslagperiode
- Nettowijziging: de totale wijziging in de omvang van de installatiebasis voor de verslagperiode

 Opmerking: de toegang tot de overzichtspagina van EA Services kan afhankelijk zijn van de rol- en machtigingsvereisten. Neem contact op met uw accountbeheerder als deze pagina niet zichtbaar is in uw navigatie.

levenseinde

De pagina's Hardware End of Life en Software End of Life bieden gedetailleerde EOL-informatie en bieden gebruikers de ondersteuning die nodig is om productvernieuwingscycli en supportdekking proactief te beheren. Als u op een actief klikt op de pagina's Einde levensduur, wordt u doorverwezen naar het betreffende actief op de pagina Inventaris.



Einde van de levensduur van software

Analyse van het levenseinde

Het paneel Insights op de pagina End of Life toont een AI-gestuurd overzicht van assets met een gedefinieerde Last Day of Support. Klik op Volledige analyse voor visualisaties zoals grafieken, dashboards en grafieken die extra inzichten bieden. Zie [Gegevens analyseren](#) in gemeenschappelijke modulefuncties voor meer informatie.

Exporteren einde levensduur

Klik op Exporteren om een gefilterde lijst met EOL-elementen op te slaan in .xls- of .csv-indeling. Zie [Informatie exporteren](#) in Gemeenschappelijke modulefuncties voor meer informatie.

evaluatiemodule

De evaluatiemodule biedt een beoordelingskader waarmee u proactief risico's met betrekking tot beveiliging, stabiliteit, capaciteit, naleving en veroudering kunt onderzoeken en beperken, waardoor netwerken veilig, stabiel en betrouwbaar blijven.

Kernbegrippen

De evaluatiemodule is gebaseerd op de volgende kernconcepten:

- **Beoordeling:** een systematische evaluatie van infrastructuurentiteiten aan de hand van vooraf gedefinieerde criteria om prestaties, naleving, beveiliging of operationele capaciteit te meten; Beoordelingen worden op verzoek, volgens een schema of door een gebeurtenis uitgevoerd
- **Evaluatie-uitvoering:** een instantie of een enkele uitvoering van een evaluatie; elke uitvoering maakt een nieuwe uitvoeringsrecord die het bereik, het triggermechanisme, de tijdstempel en de resulterende gegevens die door de evaluatie worden geproduceerd, bijhoudt
- **Bevinding:** een gevalideerde, bruikbare observatie die een hiaat, risico, probleem of opmerkelijke toestand identificeert. Bevindingen vertegenwoordigen de gegevens op grondniveau tijdens een evaluatie
- **Inzicht:** Een analytische conclusie op een hoger niveau die is afgeleid van patronen of trends in meerdere bevindingen. Inzichten interpreteren wat bevindingen betekenen in een bredere zakelijke of operationele context
- **Aanbeveling:** een specifiek, uitvoerbaar voorschrift dat is gekoppeld aan bevindingen of inzichten; aanbevelingen bieden duidelijke richtsnoeren voor de noodzakelijke stappen om vastgestelde problemen aan te pakken of kansen te benutten
- **Rapport:** een gestructureerd document waarin bevindingen, inzichten en aanbevelingen voor een doelgroep worden samengevoegd; Rapporten zijn het primaire hulpmiddel voor het communiceren van beoordelingsresultaten aan klanten, leidinggevend en technische teams

Toegang tot evaluatiemodule

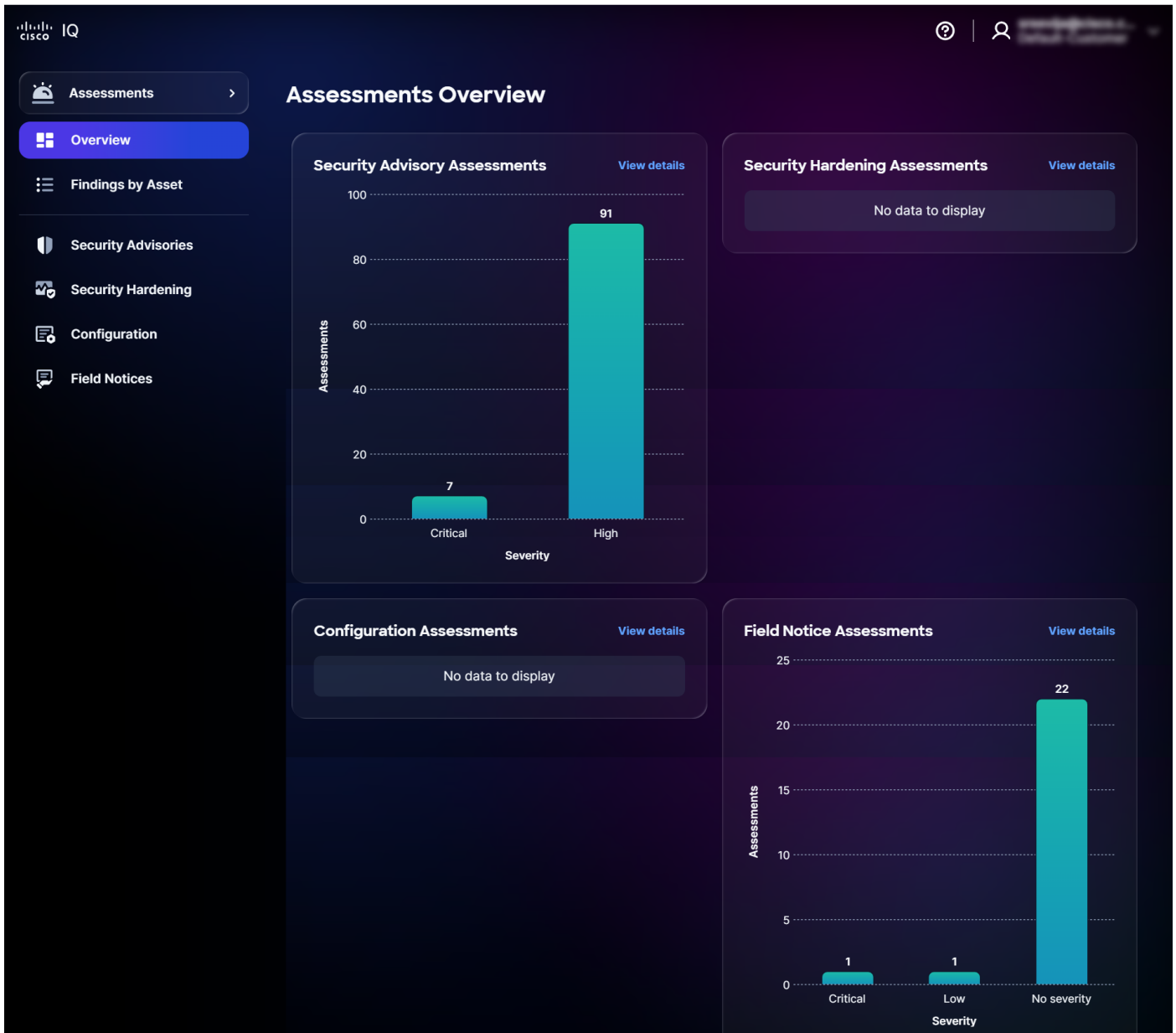
Als u toegang wilt krijgen tot beveiligings- en beoordelingsfuncties in Virtual Appliance, kiest u het menu Home > Assessments of klikt u op Assessments in de sectie Application van de Home-pagina > Launchpad tab. De pagina Overzicht van beoordelingen wordt weergegeven.



Opmerking: de evaluatiemodule kan ook worden gestart vanuit Systeemconfiguratie > Pakketbeheer.

Overzicht van beoordelingen

Op de pagina Overzicht van beoordelingen wordt het volgende dashboard weergegeven:



Overzicht van beoordelingen

Het dashboard geeft de volgende informatie weer:

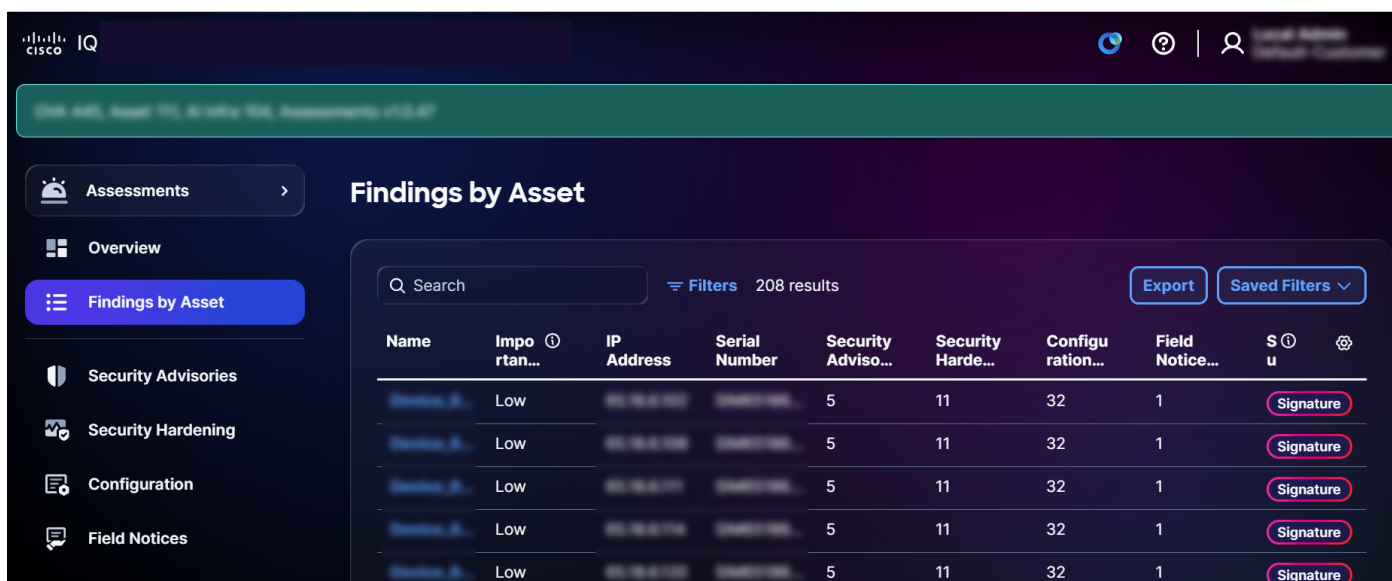
- Beoordelingen van beveiligingsadvies: geeft beoordelingen van beveiligingsadviezen weer, gecategoriseerd op kritieke en hoge ernst
- Beoordelingen van beveiligingsharddering: geeft aan welke bedrijfsmiddelen de regels voor beveiligingshardding niet naleven, gecategoriseerd op Hoog, Gemiddeld, Laag en Informatieve ernst
- Configuratiebeoordelingen: geeft bedrijfsmiddelen weer die niet voldoen aan de regels voor naleving van de configuratie, gecategoriseerd op kritieke, hoge, gemiddelde, lage en informatieve ernst

- Evaluaties van veldmeldingen: geeft beoordelingen van veldmeldingen weer, gecategoriseerd naar kritieke, hoge en niet-toepasselijke ernst

 **Opmerking:** u kunt alleen de middelen bekijken die u kunt gebruiken.

Bevindingen per asset

Op de pagina Bevindingen per bedrijfsmiddel vindt u een lijst met bedrijfsmiddelen die zijn geëvalueerd aan de hand van ten minste een van de volgende beoordelingen: Beveiligingsadviezen, Beveiliging, Configuratie en Veldmeldingen.



Findings by Asset

Q Search Filters 208 results Export Saved Filters

Name	Importance	IP Address	Serial Number	Security Advisories	Security Hardening	Configuration	Field Notices	Signature
Device A	Low	10.10.10.1	1000000001	5	11	32	1	Signature
Device B	Low	10.10.10.2	1000000002	5	11	32	1	Signature
Device C	Low	10.10.10.3	1000000003	5	11	32	1	Signature
Device D	Low	10.10.10.4	1000000004	5	11	32	1	Signature
Device E	Low	10.10.10.5	1000000005	5	11	32	1	Signature

Bevindingen per activa

Weergaven zoeken en filteren voor bevindingen op bedrijfsmiddel

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op **Filters** te klikken en een optie te kiezen in de lijst met beschikbare filters. U kunt ook zoeken naar Bevindingen op basis van activa in het veld Zoeken.

 **Opmerking:**

- Sommige filters zijn mogelijk verborgen, afhankelijk van de schermzoominstellingen.
- Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

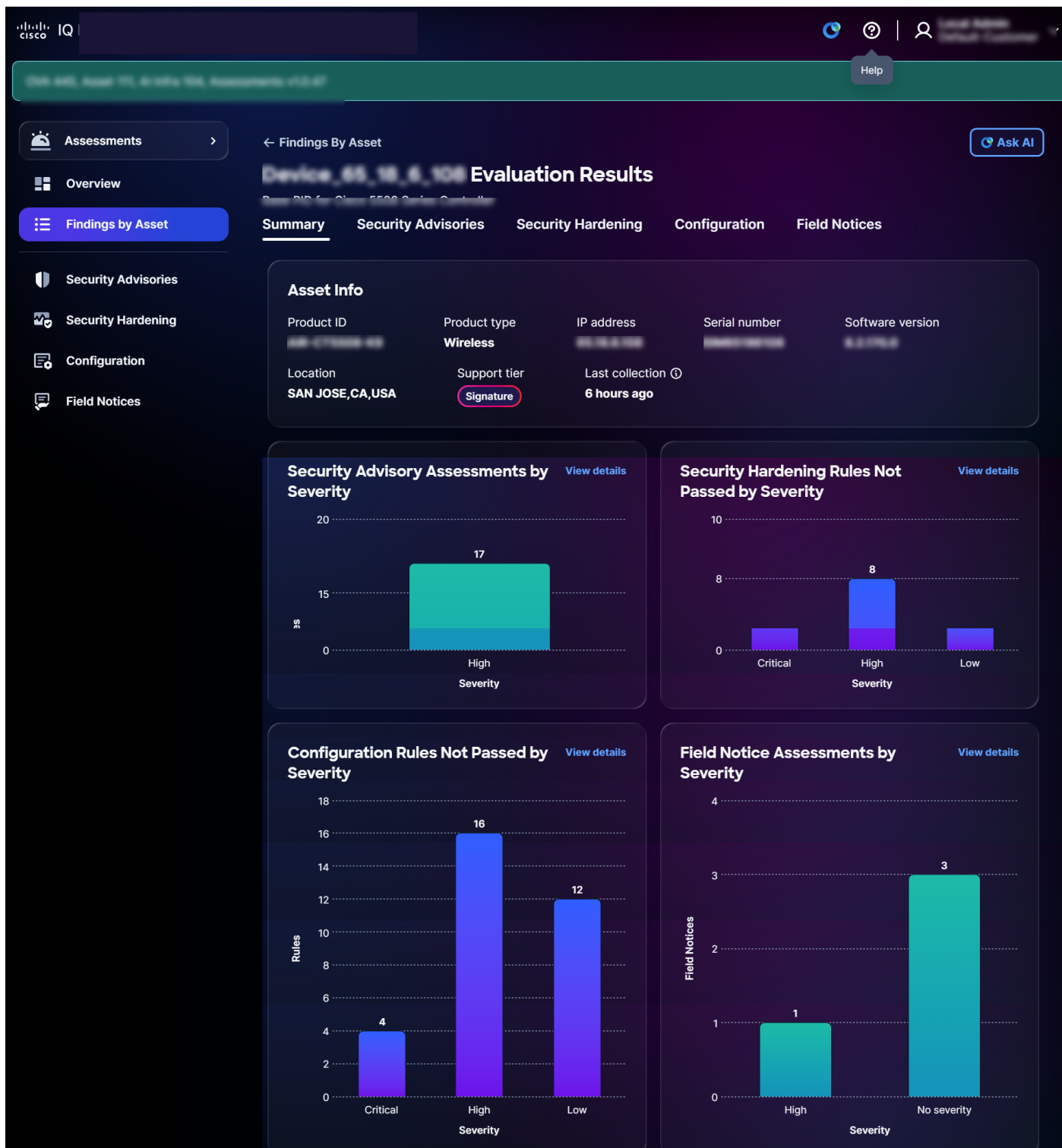
Bevindingen exporteren per activum

Klik op Exporteren om de weergave Bevindingen op basis van activa te exporteren. Zie [Informatie exporteren](#) voor meer informatie.

Bevindingen bekijken op basis van gegevens over bedrijfsmiddelen

Als u Bevindingen op basis van details van bedrijfsmiddelen wilt bekijken, klikt u op een bedrijfsmiddel. De volgende tabbladen geven details weer voor het geselecteerde element:

- Samenvatting: biedt gedetailleerde informatie over bedrijfsmiddelen, waaronder het aantal beveiligingsadviezen, beveiligingshaarden, configuratie en veldmeldingen
- Beveiligingsadviezen: biedt een lijst met gerelateerde beveiligingsadviezen
- Security Hardening: biedt een lijst met activa die niet voldoen aan de regels voor Security Hardening
- Configuratie: biedt een lijst met middelen waarvoor de regels voor best practices voor configuratie niet werken
- Berichten in het veld: biedt een lijst met gerelateerde beoordelingen in het veld Berichten



Bevindingen op basis van Asset Details

Wanneer u op Details weergegeven op een tegel klikt, wordt de pagina omgeleid naar de betreffende pagina in de module.

Wanneer u klikt op Volledige activumgegevens weergegeven, wordt de detailweergavepagina weergegeven.

Beveiligingsadviezen

Beveiligingsadviesbeoordelingen identificeren kwetsbaarheden en prioriteren deze op basis van hun risico, ernst en kritikaliteit, waardoor de risicobeheermogelijkheden van de organisatie worden verbeterd. Beveiligingsadviezen bieden gedetailleerde inzichten in kwetsbaarheden, helpen kritieke bedreigingen sneller te beperken en zorgen voor afstemming op naleving en bedrijfsdoelstellingen. Dit versterkt de beveiligingspositie, optimaliseert de toewijzing van middelen en bevordert de veerkracht tegen evoluerende bedreigingen in de hele onderneming. Beveiligingsadviezen worden automatisch bijgewerkt in Cisco IQ zodra ze worden vrijgegeven.

De pagina Beveiligingsadviezen bevat een lijst met alle beveiligingsadviezen met zwakke punten die binnen de organisatie zijn gedetecteerd. Als u op een advies klikt in de beoordelingslijst van de beveiligingsadviseur, navigeert u naar de bijbehorende detailweergave.

Assessment	Severity	Affected Assets	Potentially Affected...	CVE	Last Updated
Cisco IOS and I...	High	0	12		Oct 4, 2019
Cisco IOS and I...	High	0	1		Sep 25, 2019
Cisco IOS and I...	High	1	0		Mar 23, 2016
Multiple Vulner...	High	0	1		Jan 11, 2016
Cisco IOS and I...	High	0	1		Jul 26, 2017
Cisco IOS and I...	High	1	0		Sep 28, 2016

Beveiligingsadviezen

Zoeken en filteren van weergaven voor beveiligingsadviezen

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijst. U kunt ook zoeken naar beoordelingen van beveiligingsadvies door de naam van de beoordeling in te voeren in het veld Zoeken.



Opmerking: sommige filters kunnen worden verborgen, afhankelijk van de

 schermzoominstellingen. Sommige filters kunnen worden verborgen, afhankelijk van de schermzoominstellingen. Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen. Ontbrekende waarden voor de ernst worden weergegeven als "-" met een beschrijvende knopinfo.

Beveiligingsadviezen exporteren

Klik op Exporteren om beoordelingen van de beveiligingsadviesservice te exporteren. Zie [Informatie exporteren](#) voor meer informatie.

Gegevens van de beoordeling van het beveiligingsadvies bekijken

Klik op een evaluatie om aanvullende details te bekijken. De detailpagina bevat informatie zoals de Common Vulnerability Scoring System (CVSS) Score, Common Vulnerabilities and Exposures (CVE), Severity en een link naar de Cisco Security Advisory waarnaar wordt verwezen.

U kunt de volgende soorten resultaten bekijken in de tabel met beoordelingsresultaten:

- **Getroffen:** Geeft aan dat het actief of onderdeel een bevestigde kwetsbaarheid heeft die door een aanvaller kan worden misbruikt en moet worden verholpen
- **Potentieel getroffen:** geeft aan dat het actief of de component tekenen vertoont die tot kwetsbaarheid kunnen leiden, maar het is niet definitief bevestigd; verder onderzoek kan nodig zijn

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

← Security Advisories

Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability

About the Assessment

A vulnerability in the common Session Initiation Protocol (SIP) library of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on an internal data structure....

Show more

Severity

High

CVE

CVSS score

8.8

Version

1.1

First published

Sep 25, 2019

Last updated

Oct 4, 2019

References

Security Advisory

Asset Results

Q Search

Filters 12 results

Export

Saved Filters

Asset	Result	Product ID	IP Address	Serial Number	Support Tier
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
Isr4431	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature

Details beveiligingsadviezen

Weergaven zoeken en filteren voor evaluatieresultaten van bedrijfsmiddelen

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op Filters te klikken en een optie te kiezen in de lijst met beschikbare filters. U kunt ook naar elementen zoeken door de naam van het element in te voeren in het veld Zoeken.

Opmerking: sommige filters kunnen worden verborgen, afhankelijk van de schermzoominstellingen. Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

Resultaten van de evaluatie van bedrijfsmiddelen bekijken

Als u details van een evaluatieresultaat wilt bekijken, klikt u op een element in de tabel met evaluatieresultaten. De pagina Evaluatieresultaten wordt weergegeven.

Result

Security Advisories > Cisco Secure Boot Hardware Tampering Vulnerability

Device: 65_10_4_108

Assessment: Cisco Secure Boot Hardware Tampering Vulnerability

Result Details Potentially affected

Evidence

- ✓ Matched on software type
- ✓ Matched on chassis product ID
- ✓ Matched on module product ID

Additional Verification Needed

1) Software Releases are not checked for the automation of this Security Advisory. You must manually check your software release against the information in the advisory. 2) Module/Chassis PID level Automation is not done for the following product families. Please refer to the Security Advisory for the impacted PIDs and determine the Vulnerability of the device Cisco 4000 Series Integrated Services Routers Cisco Catalyst 6800 Series Switches Cisco Network Convergence System 5500 Series Routers

About the Assessment

A vulnerability in the logic that handles access control to one of the hardware components in Cisco's proprietary Secure Boot implementation could allow an authenticated, local attacker to write a modified firmware image to the component. This vulnerability affects multiple Cisco products that support hardware...

[Show more](#)

Severity	CVE	CVSS score
High		6.7
First published	Last updated	
May 13, 2019	Nov 20, 2019	
References		
Security Advisory		

About the Asset View evaluated asset

Product ID	Product type	IP Address
	Switches	
Serial Number	Software version	Location
		SAN JOSE, CA, USA
Support tier		
Signature		

Resultaatdetails

Resultaten van bedrijfsmiddelen exporteren voor beveiligingsadviezen

Klik op Exporteren om resultaten van bedrijfsmiddelen te exporteren. Zie [Informatie exporteren](#) voor meer informatie.

veiligheidshardening

Security Hardening biedt automatisch, bijna real-time inzicht in de beveiligingspositie van uw netwerkinfrastructuur door routers, switches en firewalls voortdurend te evalueren aan de hand van industriestandaard benchmarks. Het identificeert configuratiehiaten en biedt bruikbare richtlijnen voor probleemoplossing, waardoor accountbeheerders het aanvalsoppervlak effectief kunnen verminderen en een consistente afstemming kunnen behouden met de rigoureuze best practices voor beveiliging van Cisco. Door de compliance-

monitoring te centraliseren en het hardingsproces te vereenvoudigen, transformeert de module beveiligingsbeheer van een reactieve taak in een proactieve, datagestuurde strategie, waardoor een veerkrachtig en veilig bedrijfsnetwerk wordt gewaarborgd.

 **Opmerking:** Evaluaties van beveiligingsharddering zijn uitsluitend beschikbaar voor middelen met standaard ondersteuningsniveaus.

Beoordelingen van beveiligingsharddering bekijken

Op de pagina Evaluatie van beveiligingshardingsupdates wordt de volgende informatie weergegeven:

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Security Hardening Assessment

This assessment only applies to assets with Standard or Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against Cisco OS Hardening Guides. It detects configuration deviations across your infrastructure that may affect security posture, or risk exposure. Each security hardening rule is evaluated across your covered assets, with findings prioritized by severity to help you...
[Show more](#)

Execution Outcome for Jul 20, 2026, 5:40 AM

Summary

Rule evaluations

179

Assets included

146

Rule evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search

Filters

179 results

Export

Saved Filters

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Appli...	Soft war...
Console M...	Medium	6	0	0	6	0	IOS
IGP MD5 A...	High	6	0	0	6	0	IOS
Minimum P...	High	31	31	0	0	0	AireOS

veiligheidshardening

- Over de evaluatie: geeft aanvullende details door het doel van de evaluatie samen te vatten
- Uitvoeringsuitkomst: biedt een samenvatting van de resultaten van de beoordeling van bedrijfsmiddelen, inclusief het totale aantal evaluaties van regels en opgenomen bedrijfsmiddelen
- Regel-evaluaties: biedt gedetailleerde informatie over de regel, inclusief ernst, beoordeelde activa, niet geslaagd, geslaagd, niet overtuigend, niet van toepassing en

softwaretype

- Ernst: geeft het belang of de impact van de evaluatie van de regel aan
- Geëvalueerde activa: geeft het totale aantal activa aan dat is beoordeeld aan de hand van de criteria van de regel
- Niet geslaagd: biedt de activa die tijdens de beoordeling niet aan de regelcriteria voldeden
- Geslaagd: levert de activa die tijdens de beoordeling aan de regelcriteria voldeden
- Niet overtuigend: levert de activa waarvoor de beoordeling niet kon leiden tot falen
- Niet van toepassing: geeft de activa of scenario's aan waar de regel niet van toepassing is of niet relevant is
- Softwaretype: biedt het softwaretype van middelen

Weergaven zoeken en filteren op regels

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op Filters te klikken en een optie te kiezen in de lijst met beschikbare filters. U kunt ook zoeken naar een regel door de naam van de regel in te voeren in het veld Zoeken.



Opmerking: sommige filters kunnen worden verborgen, afhankelijk van de schermzoominstellingen. Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

Evaluatiedetails van regels bekijken

Klik op een regel als u meer informatie over een regelevaluatie wilt bekijken. De pagina met evaluatiedetails van de regel wordt weergegeven met de volgende informatie:

The screenshot shows the Cisco IQ interface for a Security Hardening Assessment. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (highlighted), Configuration, and Field Notices. The main content area is titled 'Minimum Password Length Policy' and shows it was evaluated on Jul 20, 2026, at 5:39 AM. An 'Ask AI' button is in the top right.

About the Rule

Check 'Min. Password length' in show switch config, and warn if it is lower than 8. Proper security configuration protects the wireless infrastructure from unauthorized access, data interception, and compliance violations.

Severity: **High** (High icon) | Software type: **AireOS** | Assets evaluated: **31**

Results Summary 31 assets

0 Passed ✓	31 Didn't pass ✖	0 Inconclusive ⚠	0 Not applicable ⚙
----------------------	----------------------------	----------------------------	------------------------------

Asset Results

Search: [] Filters: 31 results [Export] [Saved Filters]

Asset	Result	Product ID	Serial Number	IP Address	Support Tier
Device_...	✖ Didn't pass	...	...	...	Signature
Device_...	✖ Didn't pass	...	...	...	Signature
Device_...	✖ Didn't pass	...	...	...	Signature
Device_...	✖ Didn't pass	...	...	...	Signature
Device_...	✖ Didn't pass	...	...	...	Signature

Regelweergave

- Over de regel: geeft details over de regel, zoals ernst, softwaretype, versie en geëvalueerde middelen en bevat beschrijvende gelabelde links naar relevante brondocumentatie
- Samenvatting van resultaten: biedt een samenvatting van de resultaten van bedrijfsmiddelen die verband houden met de regel, zoals geslaagd, niet geslaagd, niet overtuigend en Niet van toepassing
- Resultaten van bedrijfsmiddelen: biedt een lijst met bedrijfsmiddelen met details zoals bedrijfsmiddelen, resultaten, product-ID, serienummer, IP-adres en ondersteuningsniveau

 **Opmerking:** Cisco IQ biedt duidelijke richtlijnen wanneer een beoordelingsbevinding "niet overtuigend" is, waarbij de oorzaak wordt uitgelegd (bijvoorbeeld ontbrekende telemetrie of niet-ondersteund besturingssysteem) en stappen worden aanbevolen zoals het verifiëren van gegevensverzameling, het bijwerken van referenties of het vernieuwen van gegevens. Er worden ook gelabelde links naar relevante documentatie verstrekt om problemen op te lossen.

Weergaven zoeken en filteren voor regels voor bedrijfsmiddelen

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op Filters te klikken en een optie te kiezen in de lijst met beschikbare filters. U kunt ook zoeken naar resultaten van de beoordeling van bedrijfsmiddelen door de naam van het bedrijfsmiddel in te voeren in het veld Zoeken.



Opmerking: sommige filters kunnen worden verborgen, afhankelijk van de schermzoominstellingen. Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

Resultaten van bedrijfsmiddelen exporteren

Klik op Exporteren als u evaluatieresultaten voor regels wilt exporteren. Zie [Informatie exporteren](#) voor meer informatie.

Weergaven voor bedrijfsmiddelen zoeken en filteren

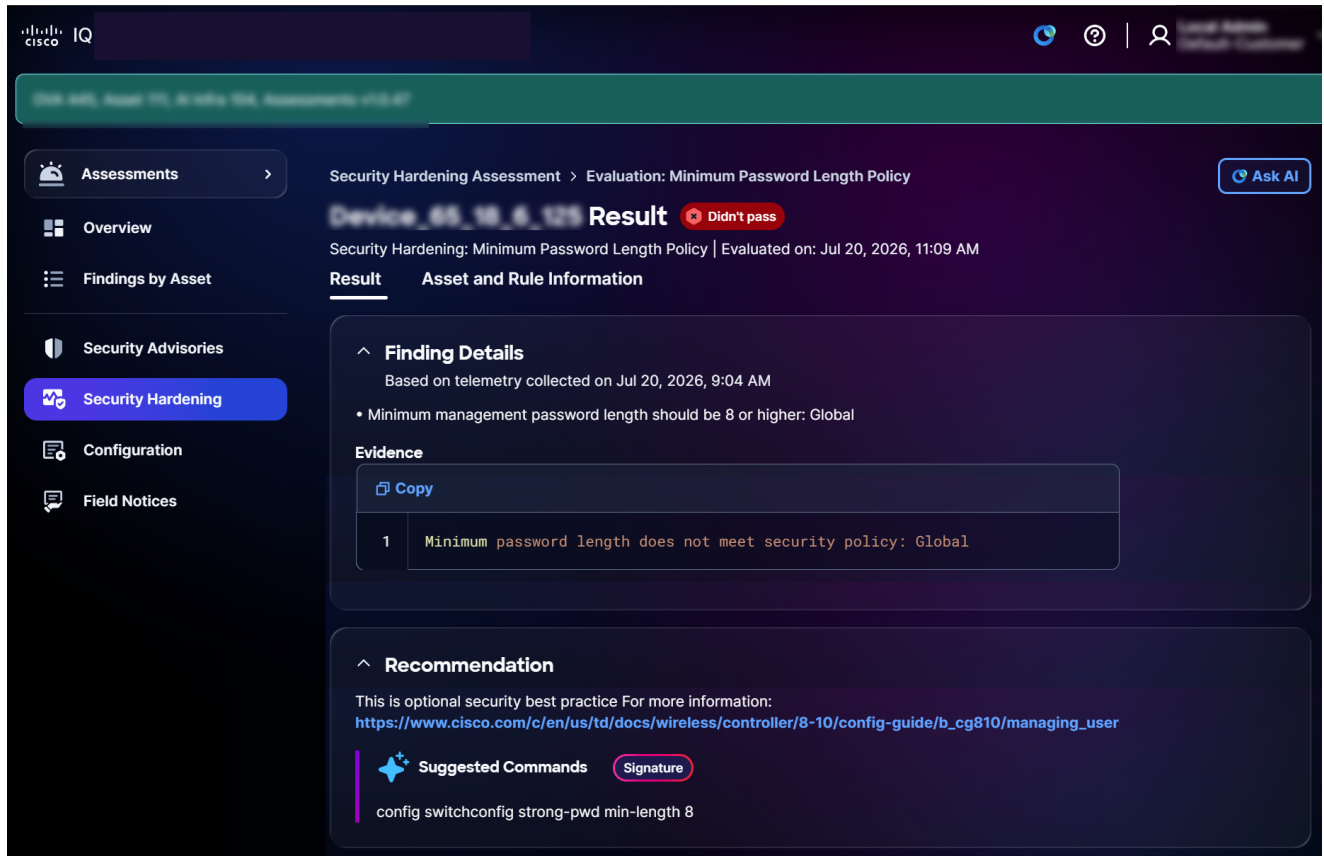
U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op Filters te klikken en een optie te kiezen in de lijst met beschikbare filters. U kunt ook naar bedrijfsmiddelenresultaten zoeken door de naam van het bedrijfsmiddel in te voeren in het veld Zoeken.



Opmerking: sommige filters zijn mogelijk verborgen, afhankelijk van de schermzoominstellingen. Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

Resultaten van bedrijfsmiddelen bekijken voor beveiligingshardening

Klik op een actief uit Asset Results om de details te bekijken. Op de resultaatdetailpagina van het actief wordt informatie weergegeven op basis van uw rechte niveau of -niveau.



standaardniveau voor beveiligingsharding

- standaardniveau
- Details zoeken: biedt informatie over de configuratieafwijkingen die tijdens de beoordeling zijn geïdentificeerd, samen met bewijslogboeken
- Aanbevelingen: biedt richtlijnen om de bevindingen aan te pakken en de consistentie van de configuratie te waarborgen

Informatie over bedrijfsmiddelen en regels bekijken voor beveiligingshardening

Als u de details van een asset en de regels ervan wilt bekijken, klikt u op het tabblad Asset en Rule Info. De pagina Asset and Rule Info wordt weergegeven.

Over het bedrijfsmiddel: geeft de details van het bedrijfsmiddel weer, zoals Product-ID, Producttype, IP-adres, Serienummer, Softwareversie, Locatie en Ondersteuningsniveau

- Over de regel: biedt details over de regel (inclusief ernst en softwaretype) en het belang van die specifieke controle van de harding

Configuratie

Configuratiebeoordelingen evalueren uw bedrijfsmiddelen aan de hand van aanbevolen best practices op basis van de bewezen expertise van Cisco om configuratieafwijkingen te detecteren die van invloed kunnen zijn op de beschikbaarheid, beveiliging of prestaties van

uw infrastructuur. Elke regel voor beste praktijken wordt beoordeeld voor alle gedekte bedrijfsmiddelen en de bevindingen worden geprioriteerd op basis van de ernst om consistentie in de configuratie, verbeterde veerkracht en verminderd operationeel risico te garanderen.

 **Opmerking:** Configuratiebeoordelingen zijn uitsluitend beschikbaar voor middelen met standaard ondersteuningsniveaus.

Configuratiebeoordelingen bekijken

Op de pagina Configuratiebeoordeling wordt de volgende informatie weergegeven:

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Configuration Assessment

This assessment only applies to assets with Standard and Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against recommended best practices based on Cisco's proven expertise. It detects configuration deviations across your infrastructure that may affect availability, security, or performance. Each best practice rule is evaluated across your covered assets, with findings prioritized b...
[Show more](#)

Execution Outcome for Jul 20, 2026, 05:40 AM

Summary

Rule evaluations

729

Assets included

146

Rule Evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search

Filters

729 results

Export

Saved Filters

Rule	Severity	Assets	Did Not...	Passed	Inconclus...	Not...	Category
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging

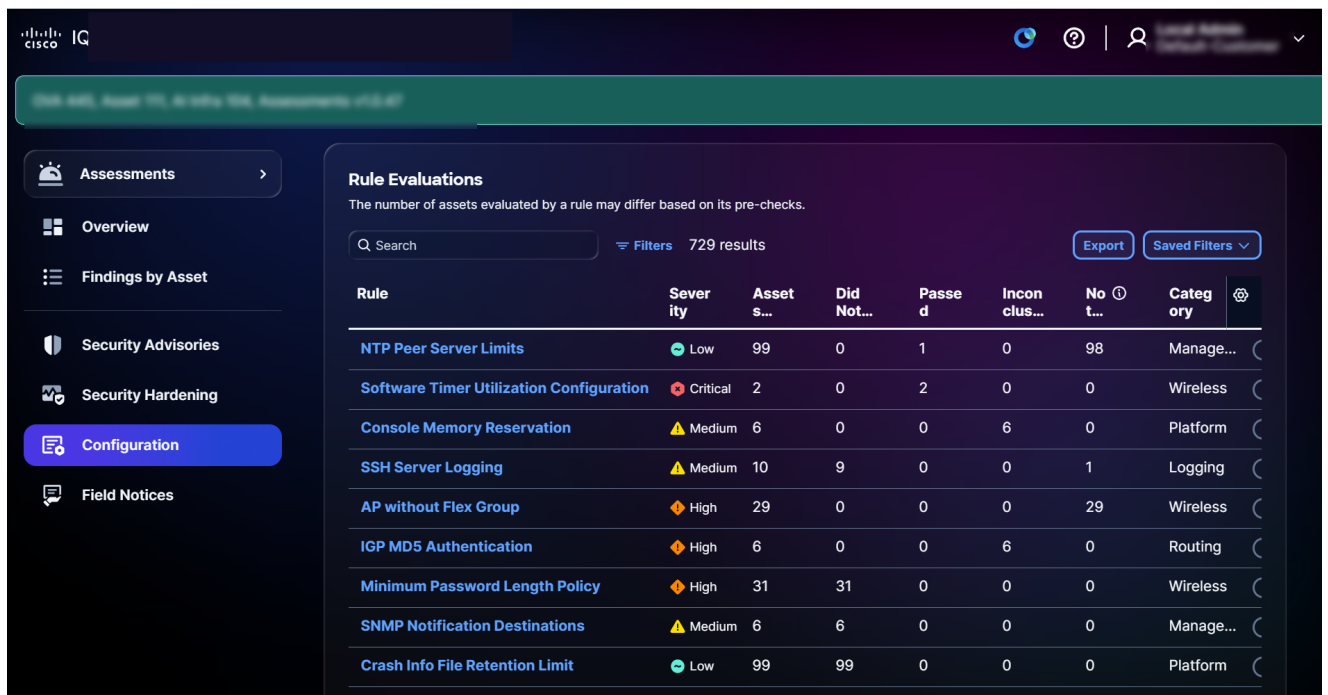
Configuratiebeoordeling

- Over de evaluatie: geeft aanvullende details door het doel van de evaluatie samen te vatten
- Samenvatting: biedt een samenvatting van de uitvoering van de configuratie, zoals beoordeelde regels en beoordeelde bedrijfsmiddelen
- Inzichten: biedt inzicht in geïdentificeerde configuratiehiaten die worden gegenereerd door patroonanalyse en een correlatie van bevindingen; ze worden weergegeven als

intelligent gegroepeerde sleutelkaarten om de meest kritieke gebieden te markeren die aandacht vereisen

- Regel-evaluaties: biedt gedetailleerde informatie over de regel, inclusief ernst, beoordeelde activa, niet geslaagd, geslaagd, niet overtuigend, niet van toepassing, categorie en softwaretype
- Ernst: geeft het belang of de impact van de evaluatie van de regel aan
- Geëvalueerde activa: geeft het totale aantal activa aan dat is beoordeeld aan de hand van de criteria van de regel
- Niet geslaagd: geeft het totale aantal activa aan dat tijdens de beoordeling niet aan de regelcriteria voldeed
- Niet overtuigend: geeft het totale aantal activa aan waarvoor de beoordeling niet kon worden uitgevoerd
- Geslaagd: levert de activa die tijdens de beoordeling aan de regelcriteria voldeden
- Niet van toepassing: geeft de activa of scenario's aan waar de regel niet van toepassing is of niet relevant is
- Categorie: Hiermee geeft u het domeingebied op waartoe de regel behoort
- Softwaretype: geeft het type software aan waarop de regel van toepassing is

Weergaven zoeken en filteren op regels



The screenshot shows the Cisco IQ Rule Evaluations page. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area is titled 'Rule Evaluations' and includes a search bar, a filter icon, and a count of 729 results. Below this is a table with the following columns: Rule, Severity, Asset s..., Did Not..., Passe d, Incon clus..., No t..., and Categ ory. The table lists several rules with their respective severity levels and counts.

Rule	Severity	Asset s...	Did Not...	Passe d	Incon clus...	No t...	Categ ory
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging
AP without Flex Group	High	29	0	0	0	29	Wireless
IGP MD5 Authentication	High	6	0	0	6	0	Routing
Minimum Password Length Policy	High	31	31	0	0	0	Wireless
SNMP Notification Destinations	Medium	6	6	0	0	0	Manage...
Crash Info File Retention Limit	Low	99	99	0	0	0	Platform

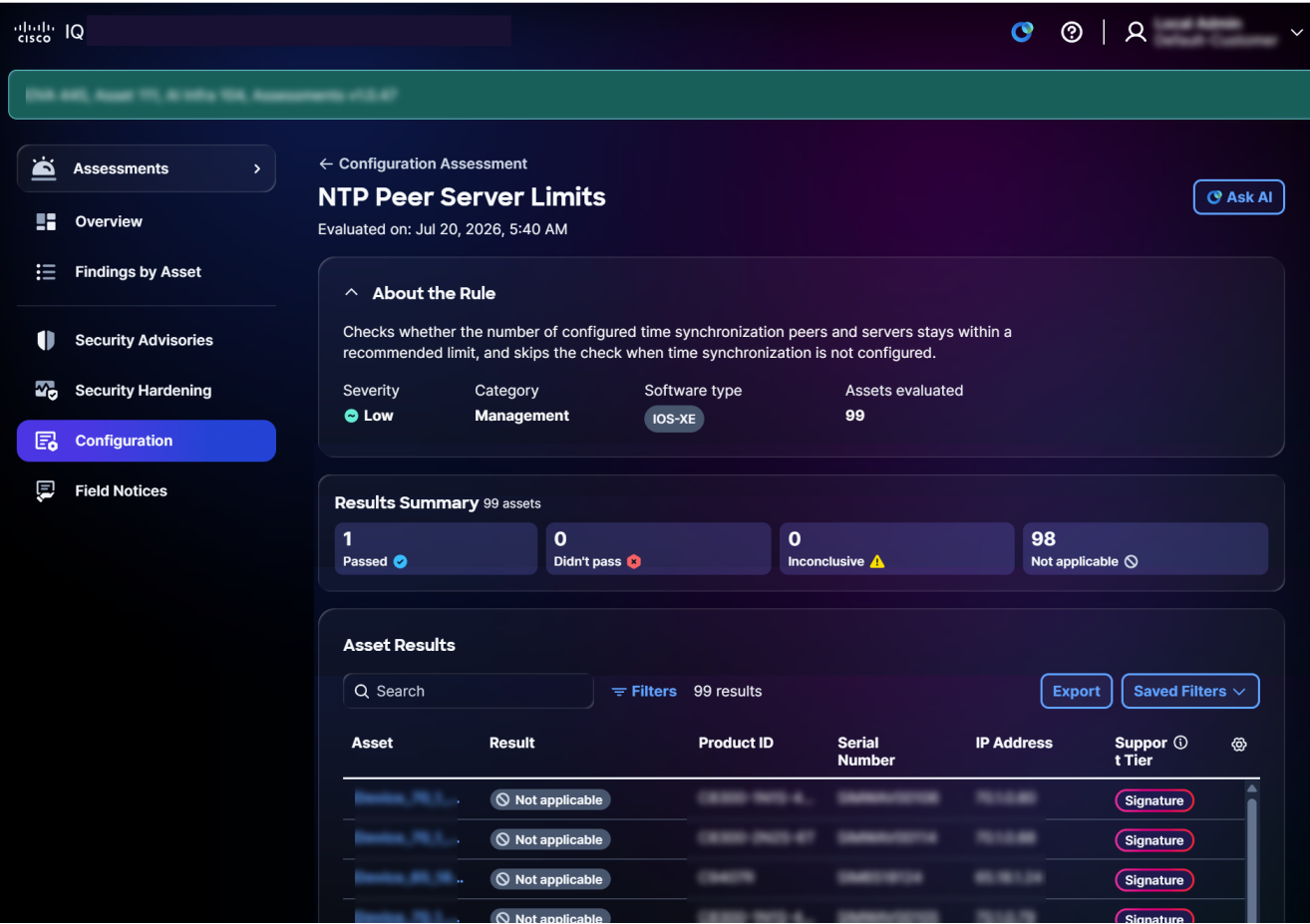
Regelevaluaties

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op Filters te klikken en een optie te kiezen in de lijst met beschikbare filters. U kunt ook zoeken naar een regel door de naam van de regel in te voeren in het veld Zoeken.

 **Opmerking:** sommige filters zijn mogelijk verborgen, afhankelijk van de schermzoominstellingen. Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

Evaluatiedetails van regels bekijken

Klik op een willekeurige regel als u meer informatie over een regevaluatie wilt bekijken. De pagina met evaluatiedetails van de regel wordt weergegeven met de volgende informatie:



The screenshot shows the Cisco IQ interface for a Configuration Assessment titled "NTP Peer Server Limits". The page is evaluated on Jul 20, 2026, at 5:40 AM. It includes a sidebar with navigation options like Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (selected), and Field Notices. The main content area shows details about the rule, including its severity (Low), category (Management), software type (IOS-XE), and the number of assets evaluated (99). A Results Summary section shows 1 Passed, 0 Didn't pass, 0 Inconclusive, and 98 Not applicable. Below this is an Asset Results table with columns for Asset, Result, Product ID, Serial Number, IP Address, and Support Tier. The table shows several rows of assets, all with a "Not applicable" result.

evaluatie

- Over de regel: biedt details over een regel zoals ernst, categorie, softwaretype en geëvalueerde middelen en bevat beschrijvende gelabelde links naar relevante brondocumentatie
- Samenvatting van resultaten: biedt algemene resultaten van bedrijfsmiddelen door het aantal bedrijfsmiddelen weer te geven in Geslaagd, Niet geslaagd, Niet overtuigend en Niet van toepassing statussen
- Resultaten van bedrijfsmiddelen: geeft een lijst van bedrijfsmiddelen met

resultaatstatus die door de geselecteerde regel worden beïnvloed

 Opmerking: Cisco IQ biedt duidelijke richtlijnen wanneer een beoordelingsbevinding "niet overtuigend" is, waarbij de oorzaak wordt uitgelegd (bijvoorbeeld ontbrekende telemetrie of niet-ondersteund besturingssysteem) en stappen worden aanbevolen zoals het verifiëren van gegevensverzameling, het bijwerken van referenties of het vernieuwen van gegevens. Er worden ook gelabelde links naar relevante documentatie verstrekt om problemen op te lossen. De evaluatiemodule ondersteunt selectie van regels voor meerdere categorieën, waardoor simultane verwerking en evaluatie in meerdere regelcategorieën mogelijk is.

Resultaten van bedrijfsmiddelen exporteren

Klik op Exporteren als u resultaten van bedrijfsmiddelen wilt exporteren voor regels. Zie [Informatie exporteren](#) voor meer informatie.

Weergaven voor bedrijfsmiddelen zoeken en filteren

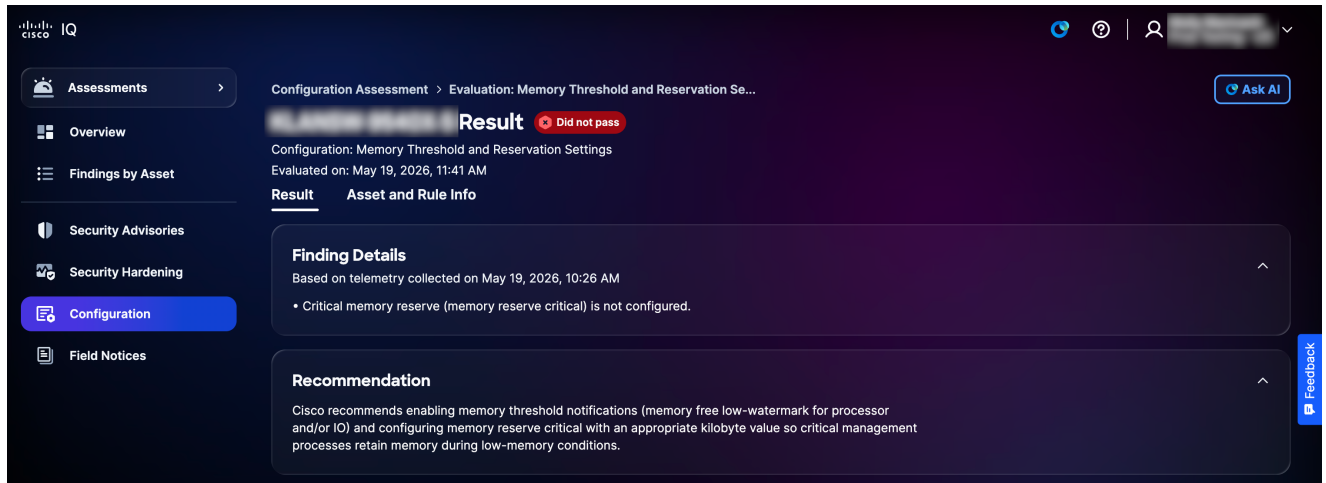
U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op Filters te klikken en een optie te kiezen in de lijst met beschikbare filters. U kunt ook naar bedrijfsmiddelenresultaten zoeken door de naam van het bedrijfsmiddel in te voeren in het veld Zoeken.

 Opmerking: sommige filters zijn mogelijk verborgen, afhankelijk van de schermzoominstellingen. Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

Bedrijfsmiddelenresultaten bekijken voor configuratiebeoordelingen

Klik op een actief uit de resultaten van het actief om details van de resultaten van het actief weer te geven.

Op de resultaatdetailpagina van het actief wordt informatie weergegeven op basis van uw rechte niveau of -niveau.

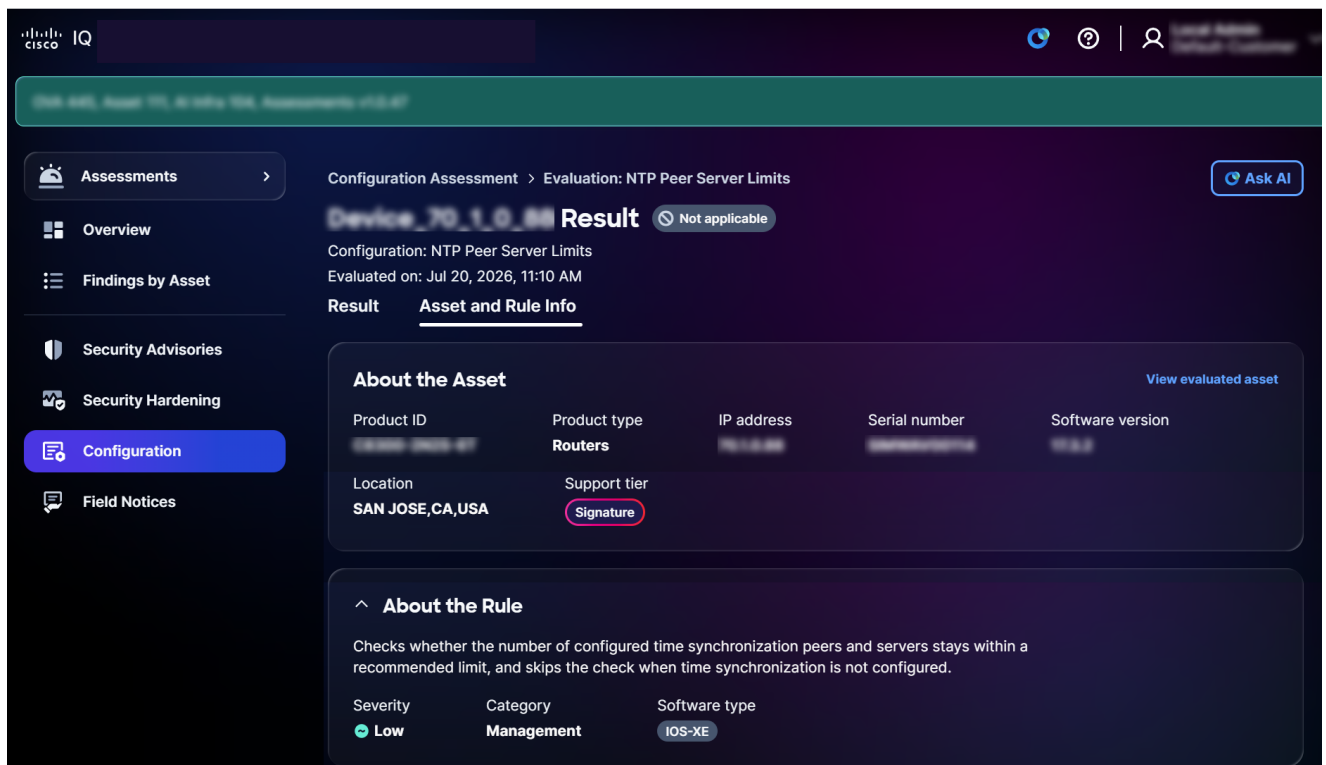


Configuratie standaardniveau

- standaardniveau
- Details zoeken: biedt informatie over de configuratieafwijkingen die tijdens de beoordeling zijn geïdentificeerd, samen met bewijslogboeken
- Aanbevelingen: biedt richtlijnen om de bevindingen aan te pakken en de consistentie van de configuratie te waarborgen

Informatie over bedrijfsmiddelen en regels weergeven voor configuratiebeoordelingen

Als u informatie over elementen en regels wilt bekijken, klikt u op het tabblad Gegevens over elementen en regels.



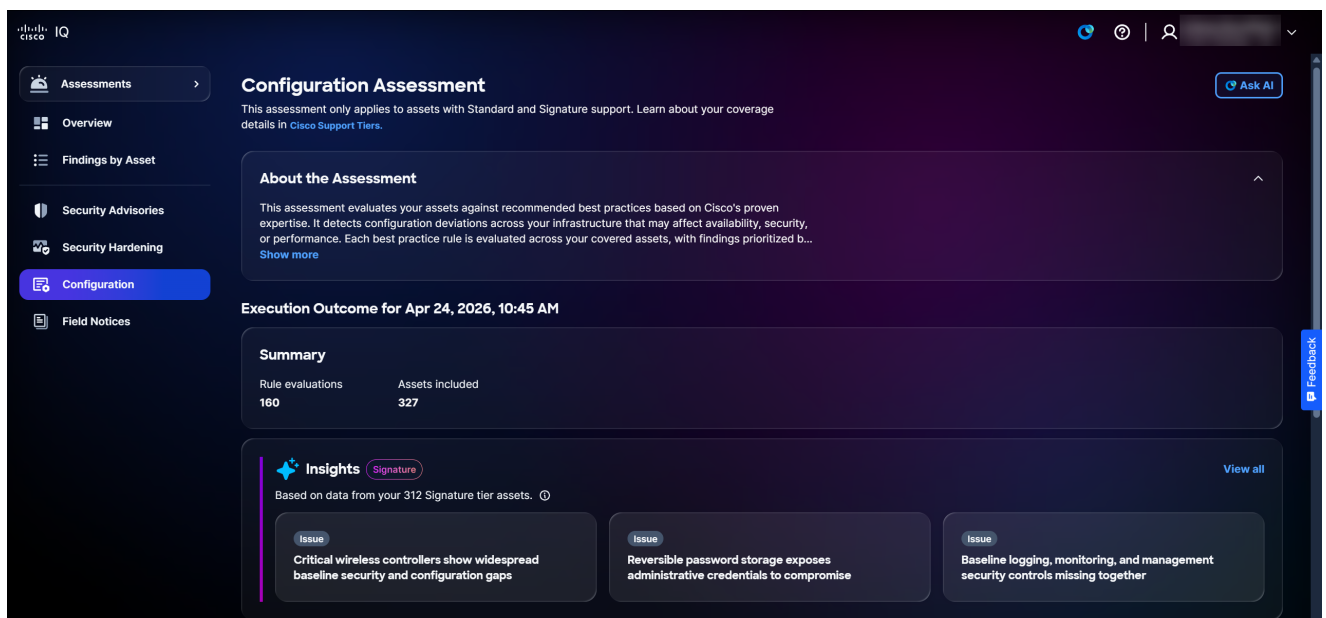
Informatie over bedrijfsmiddelen en regels

De pagina Asset and Rule Info wordt weergegeven met de volgende informatie:

- Over het bedrijfsmiddel: biedt de details van een bedrijfsmiddel, zoals Product-ID, Producttype, IP-adres, Serienummer, Softwareversie, Locatie en Supportniveau
- Over de regel: geeft details over een regel zoals ernst, categorie en softwaretype

Inzichten bekijken

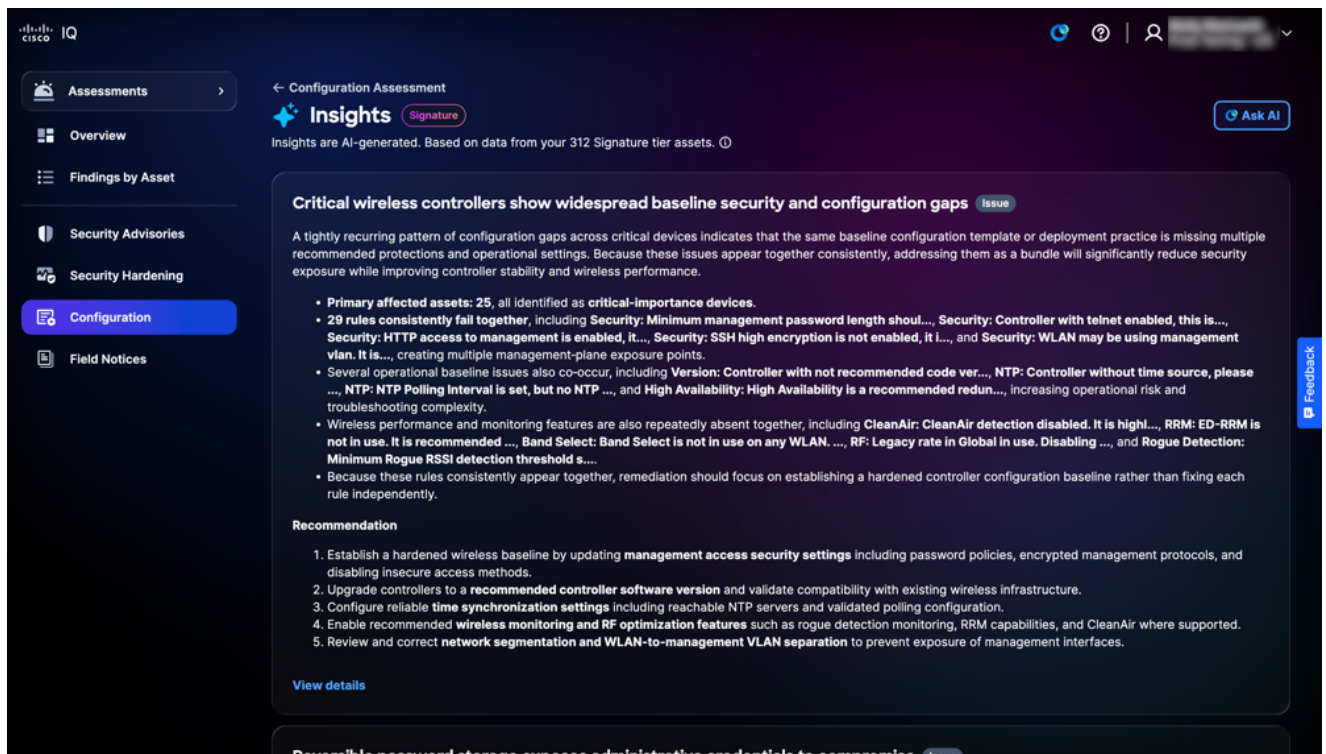
Insights zijn AI-gegenereerd en dienen als een intelligent dashboard dat beoordelingsgegevens synthetiseert in geprioriteerde sleutelkaarten, waarbij kritieke configuratieverschillen over meerdere bevindingen worden benadrukt. Het stelt u in staat om de meest impactvolle infrastructuurrisico's efficiënt aan te pakken door u te richten op deze urgente gebieden. Het benadrukt ook sterke punten door gebieden te identificeren waar uw infrastructuur goed presteert volgens best practices.



inzicht

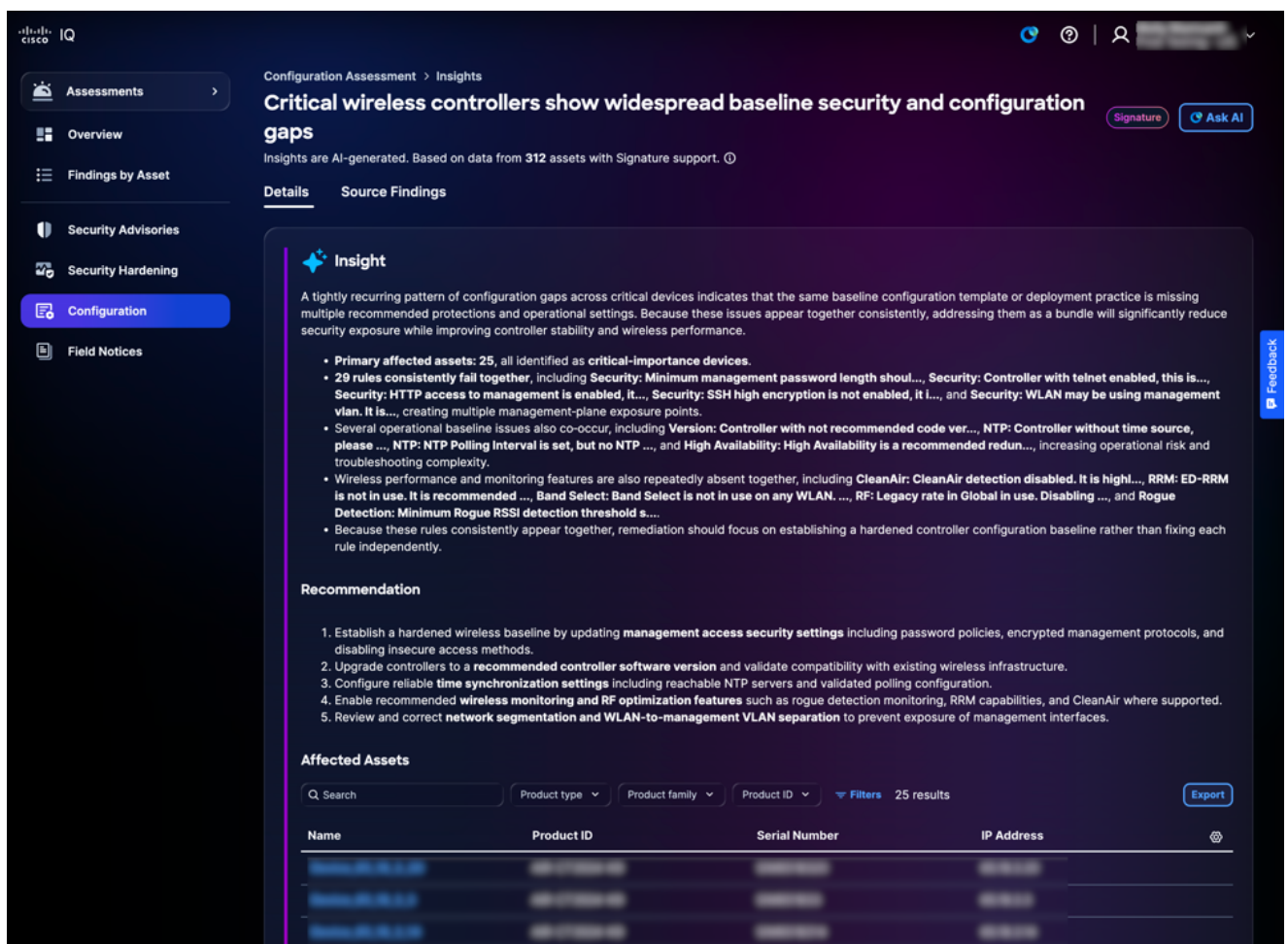
Om Insights details te bekijken:

1. Klik in het deelvenster Inzichten op Alles weergeven. Op de pagina Inzichten worden alle inzichten weergegeven.



Insights-pagina

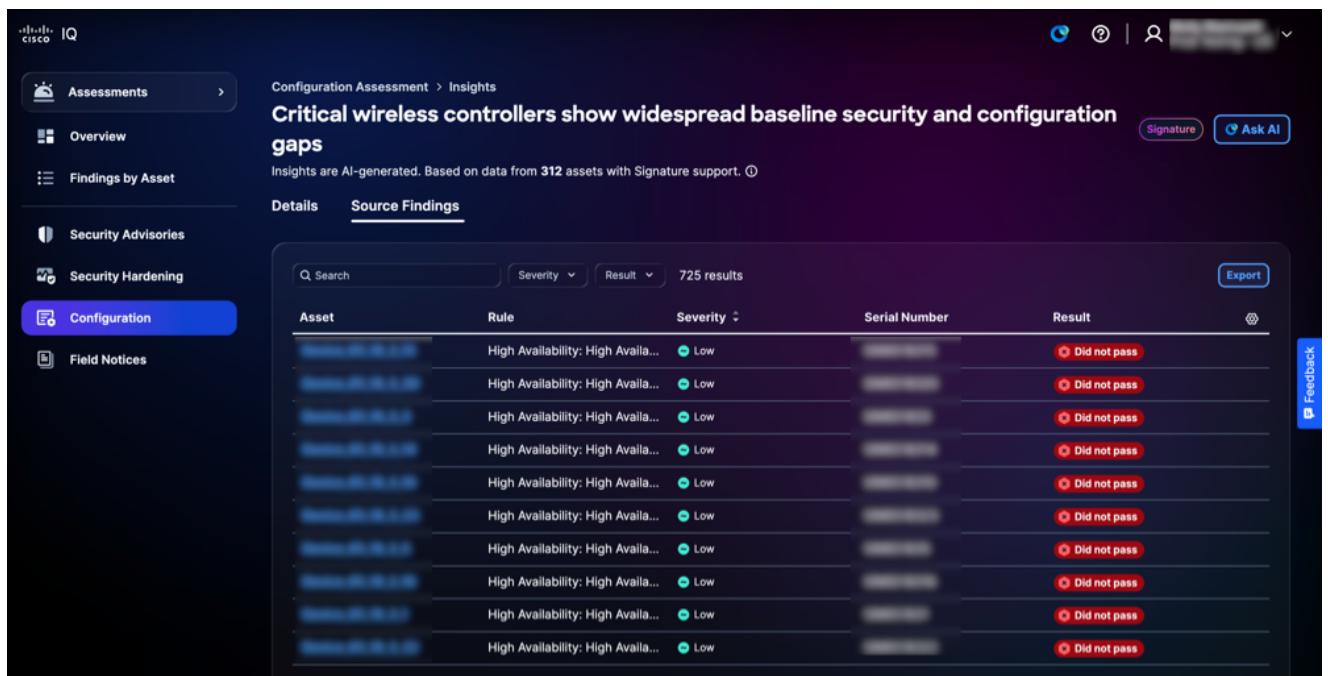
2. Klik op Details bekijken of klik op een kaart. De detailpagina Inzichten wordt weergegeven met de volgende informatie:



Insights Detail

- Inzicht: biedt een samenvatting die terugkerende patronen van configuratieafwijkingen benadrukt die zijn geïdentificeerd door middel van uitgebreide analyse van meerdere bevindingen, evenals gebieden van uitmuntendheid in uw infrastructuur waar configuraties overeenkomen met best practices
- Aanbeveling: biedt uitvoerbare stappen om de geïdentificeerde configuratiehiaten te verhelpen
- Betrokken bedrijfsmiddelen: biedt een lijst met specifieke apparaten waarbij de configuratieafwijking is geïdentificeerd zoals gedefinieerd in de sectie Inzicht

3. Klik op Bronbevindingen. De pagina Bronbevindingen toont de gedetailleerde individuele bevindingen die uw inzichten ondersteunen.



Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

Insights are AI-generated. Based on data from 312 assets with Signature support. ⓘ

Details Source Findings

Search [] Severity [] Result [] 725 results [Export]

Asset	Rule	Severity	Serial Number	Result
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass

Bronbevindingen

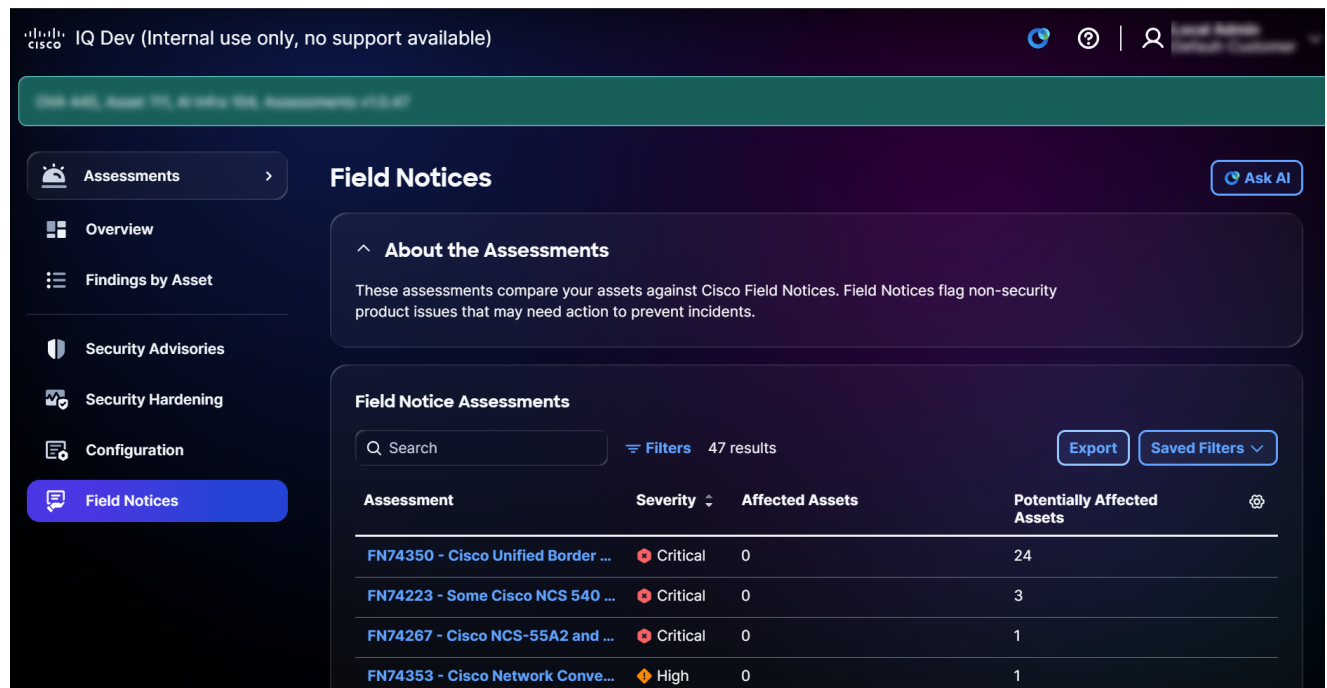
U kunt de tabelweergave filteren door een filter te kiezen in de vervolgkeuzelijsten Prioriteit en Resultaat.

 **Opmerking:** Aanbevelingen en getroffen bedrijfsmiddelen zijn optioneel, afhankelijk van de output van elk inzicht.

Berichten in het veld

Veldmeldingen identificeren belangrijke niet-beveiligingsgerelateerde productproblemen en organiseren deze op basis van de ernst van de impact en de kritikaliteit ervan, waardoor de organisatie beter in staat is om productrisico's te beheren. Field Notices bieden bruikbare inzichten in productdefecten, versnellen de mitigatie door middel van aanbevolen upgrades

of oplossingen en zorgen voor afstemming op operationele en zakelijke doelstellingen. Dit versterkt de betrouwbaarheid van het product, optimaliseert de toewijzing van middelen en bevordert de veerkracht tegen veranderende productuitdagingen in de hele onderneming.



Berichten in het veld

Weergaven zoeken en filteren voor veldmeldingen

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten. U kunt ook zoeken naar beoordelingen in het veld Berichten door de naam van de beoordeling in te voeren in het veld Zoeken.

Beoordelingen bekijken voor mededelingen in het veld

Als u meer informatie over een veldmelding wilt bekijken, klikt u op een beoordeling. De volgende beoordelingsdetails worden weergegeven:

- Over de beoordelingen: geeft aanvullende details door het doel van de beoordeling samen te vatten
- Evaluaties van veldmeldingen: geeft een lijst weer met elementen die zijn beïnvloed door de geselecteerde veldmelding, waaronder elementen met gedetecteerde kwetsbaarheden

Field Notices

FN74223 - Some Cisco NCS 540 Series Medium Density Routers May Become Unresponsive After Upgrade to Cisco IOS XR Software Release 7.11.1 or Later - Workaround Provided

About the assessment

Some medium density Cisco Network Convergence System (NCS) 540 Series Routers may not boot when subjected to a field programmable device (FPD) upgrade during installation of Cisco IOS XR Software Release 7.11.1 or later.

Severity: **Critical** | Last updated: **Dec 11, 2024** | Bugs: [Redacted]

References: [Field Notice](#)

Asset Results

Search: [Input] | Filters: 3 results | Export | Saved Filters

Asset	Result	Product ID	Serial Number	Product Type	Product Family	Sup po...
Device_70_1...	Potentially affected	[Redacted]	[Redacted]	Routers	Cisco Network...	Signature
Device_70_1...	Potentially affected	[Redacted]	[Redacted]	Routers	Cisco Network...	Signature
Device_70_1...	Potentially affected	[Redacted]	[Redacted]	Routers	Cisco Network...	Signature

Beoordelingen bekijken voor mededelingen in het veld

Weergaven voor bedrijfsmiddelen zoeken en filteren voor mededelingen in het veld

U kunt de lijstweergave filteren door een filter te kiezen in de vervolgkeuzelijsten of door op Filters te klikken en een optie te kiezen in de lijst met beschikbare filters. U kunt ook naar bedrijfsmiddelenresultaten zoeken door de naam van het bedrijfsmiddel in te voeren in het veld Zoeken.

Opmerking: sommige filters zijn mogelijk verborgen, afhankelijk van de schermzoominstellingen. Er zijn verschillende filters beschikbaar, afhankelijk van uw rollen en machtigingen.

Resultaten van bedrijfsmiddelen exporteren voor veldmeldingen

Klik op Exporteren om de resultaten van de evaluatie van elementen voor veldmeldingen te exporteren. Zie [Informatie exporteren](#) voor meer informatie.

Resultaten van de evaluatie van bedrijfsmiddelen bekijken voor mededelingen in het veld

Als u de details van het beoordelingsresultaat van een actief wilt bekijken, klikt u op een actief uit de resultaten van de beoordeling van activa. De pagina met de details van het evaluatieresultaat van het bedrijfsmiddel wordt weergegeven.

U kunt de volgende soorten resultaten bekijken:

- Betrokken: Geeft aan dat elementen voldoen aan alle criteria die automatisch zijn gecontroleerd voor een melding in het veld en geen aanvullende handmatige verificatie vereisen om te bevestigen dat ze zijn beïnvloed
- Potentieel getroffen: geeft objecten aan die voldoen aan alle automatisch gecontroleerde criteria voor een melding in het veld, maar waarvoor aanvullende handmatige verificatie is vereist om te bevestigen of ze echt zijn getroffen

De volgende vragen zijn beschikbaar onder het tabblad Beoordelingen – Beveiliging:

- Wat zijn de beste praktijken van Cisco voor het verbeteren van de beveiliging van netwerkkapparaten?
- Hoe verhard ik mijn Cisco IOS XE-apparaten?
- Maak een lijst van de belangrijkste stappen voor het verbeteren van de beveiliging voor routers en switches.
- Wat zijn aanbevolen baseline harding instellingen voor Cisco apparaten?
- Hoeveel bedrijfsmiddelen zijn in strijd met de best practices op het gebied van beveiliging?

lokale verificatie

Accountbeheerders dienen de volgende referenties te gebruiken om zich succesvol aan te melden bij VA:

- Standaardgebruikersnaam: admin
- Standaardwachtwoord: het wachtwoord dat is ingesteld tijdens het VA-installatieproces; raadpleeg de handleiding Aan de slag voor meer informatie
- Standaardaccountcontext: standaardklant

Na 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).



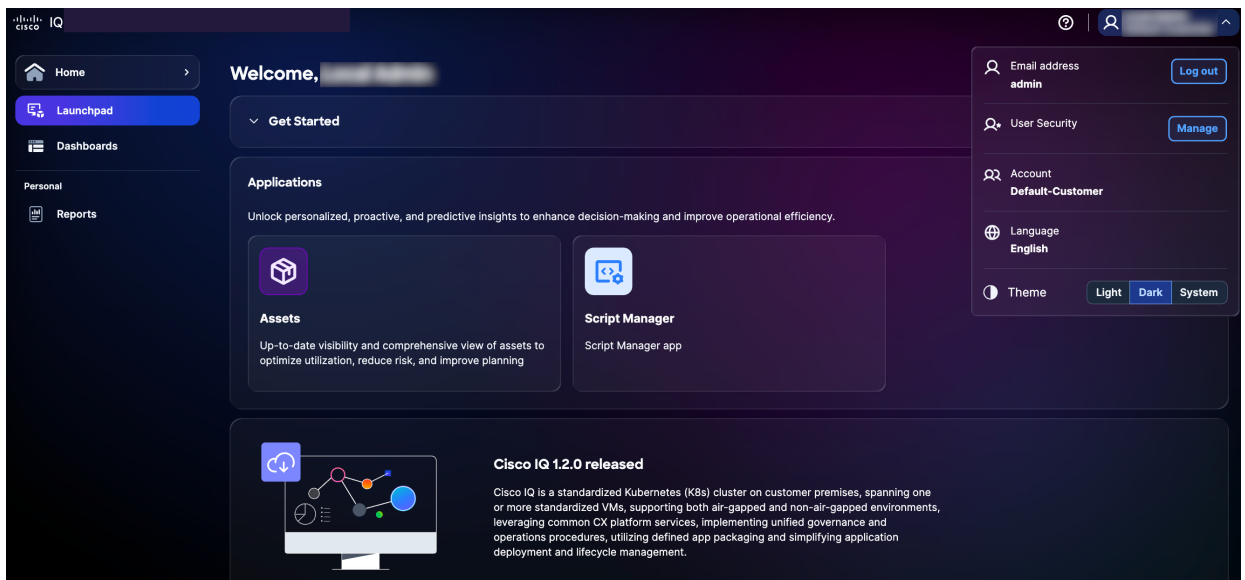
Opmerking: u hebt drie (3) pogingen om het juiste wachtwoord binnen een periode van 15 minuten in te voeren. Als alle drie (3) pogingen niet succesvol zijn, wordt uw account tijdelijk gedurende 30 minuten vergrendeld om uw beveiliging te beschermen. U kunt niet proberen in te loggen tijdens de logout 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.



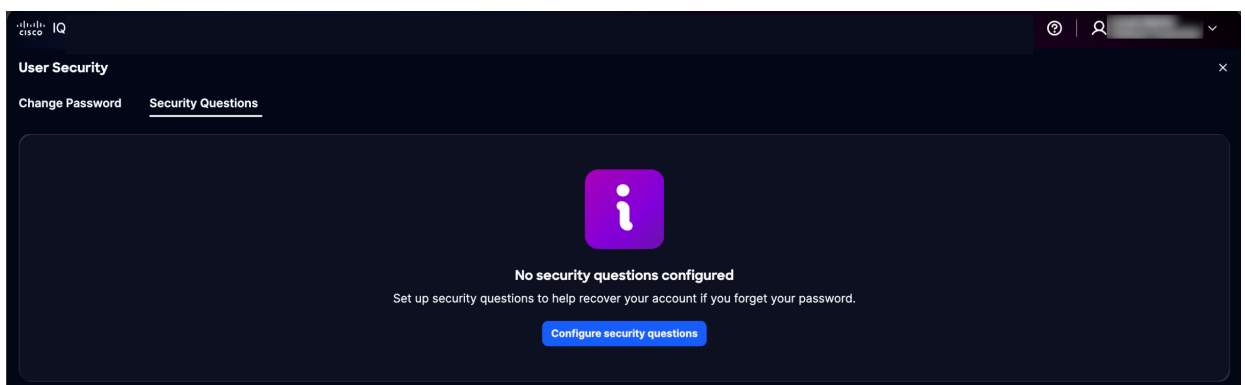
Beveiliging gebruiken

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



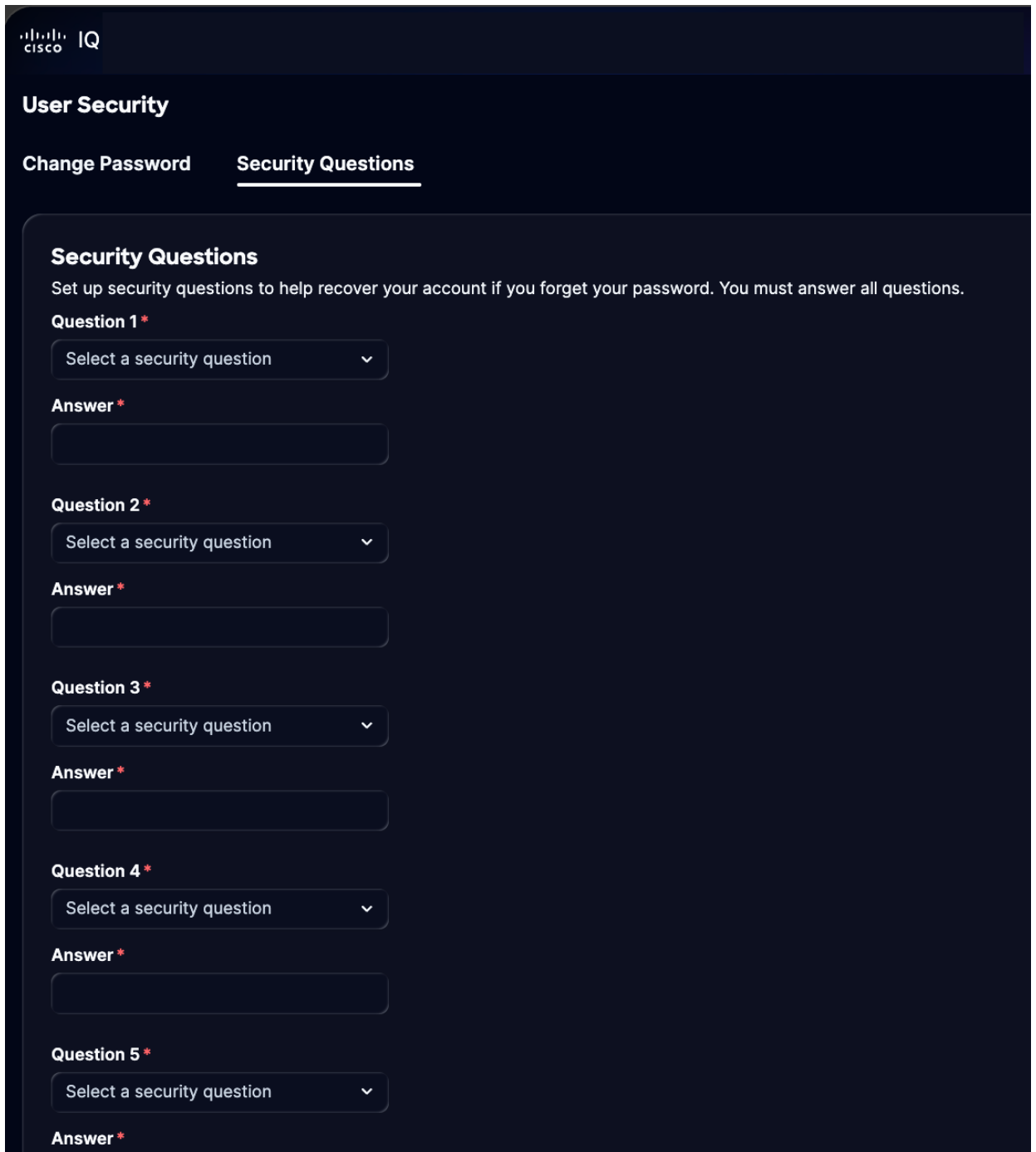
Veiligheidsvragen

3. Klik op Beveiligingsvragen om het tabblad te openen.



Tabblad Beveiligingsvragen

4. Klik op Beveiligingsvragen configureren.



The screenshot shows the Cisco IQ User Security interface. At the top, there's a header with the Cisco logo and 'IQ'. Below it, the 'User Security' section is active, with two tabs: 'Change Password' and 'Security Questions'. The 'Security Questions' tab is selected and underlined. The main content area is titled 'Security Questions' and includes a sub-header 'Set up security questions to help recover your account if you forget your password. You must answer all questions.' Below this, there are five identical question blocks. Each block consists of a 'Question' dropdown menu (labeled 'Question 1 *' through 'Question 5 *') and an 'Answer' text input field (labeled 'Answer *'). The dropdown menus currently show 'Select a security question'.

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, wat betekent dat "Smith" en "Smith" identiek worden behandeld. Onthoud hoe u uw antwoord hebt ingevoerd (bijvoorbeeld volledige namen versus bijnamen). Gebruik eenvoudige antwoorden die je jaren later nog zult herinneren. Kies voor vragen met antwoorden die in de loop van de tijd niet zullen veranderen.

 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 het wachtwoord 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 kunt krijgen tot het systeem (indien geconfigureerd op 0, is de vervaldatum van het wachtwoord uitgeschakeld).

Voorwaarden

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

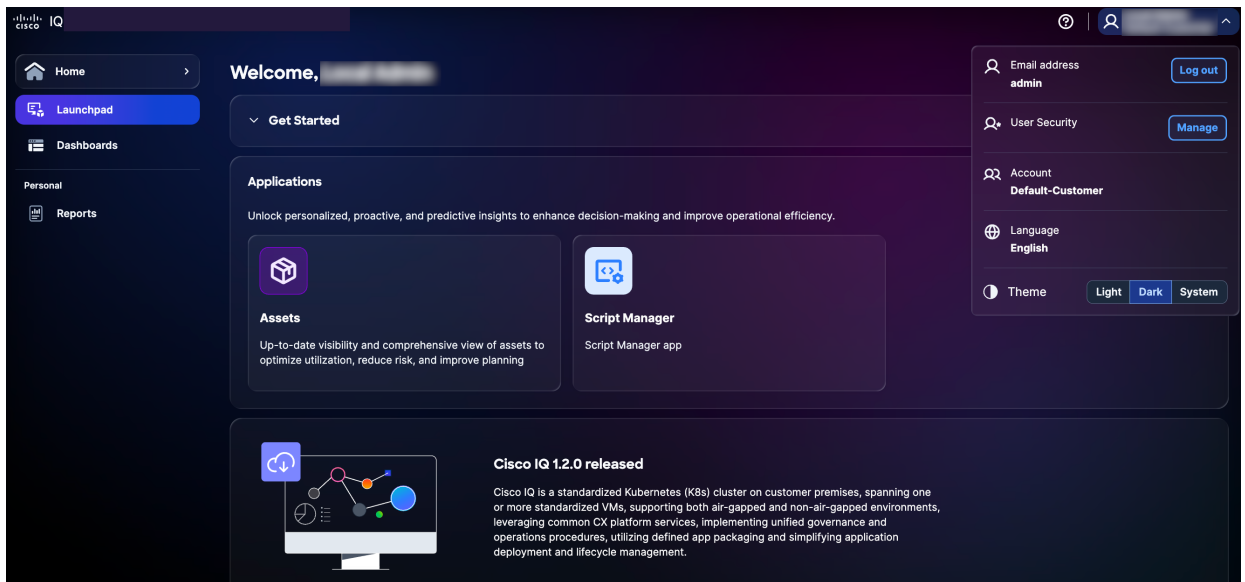
- U bent een lokale accountbeheerder of -gebruiker
- U gebruikt een lokaal account (geen eenmalige aanmelding of externe verificatie)
- Je bent ingelogd bij Cisco IQ

- U kent het huidige wachtwoord

Wachtwoorden wijzigen

Zo wijzigt u het wachtwoord:

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



Gebruikersbeveiliging beheren

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).

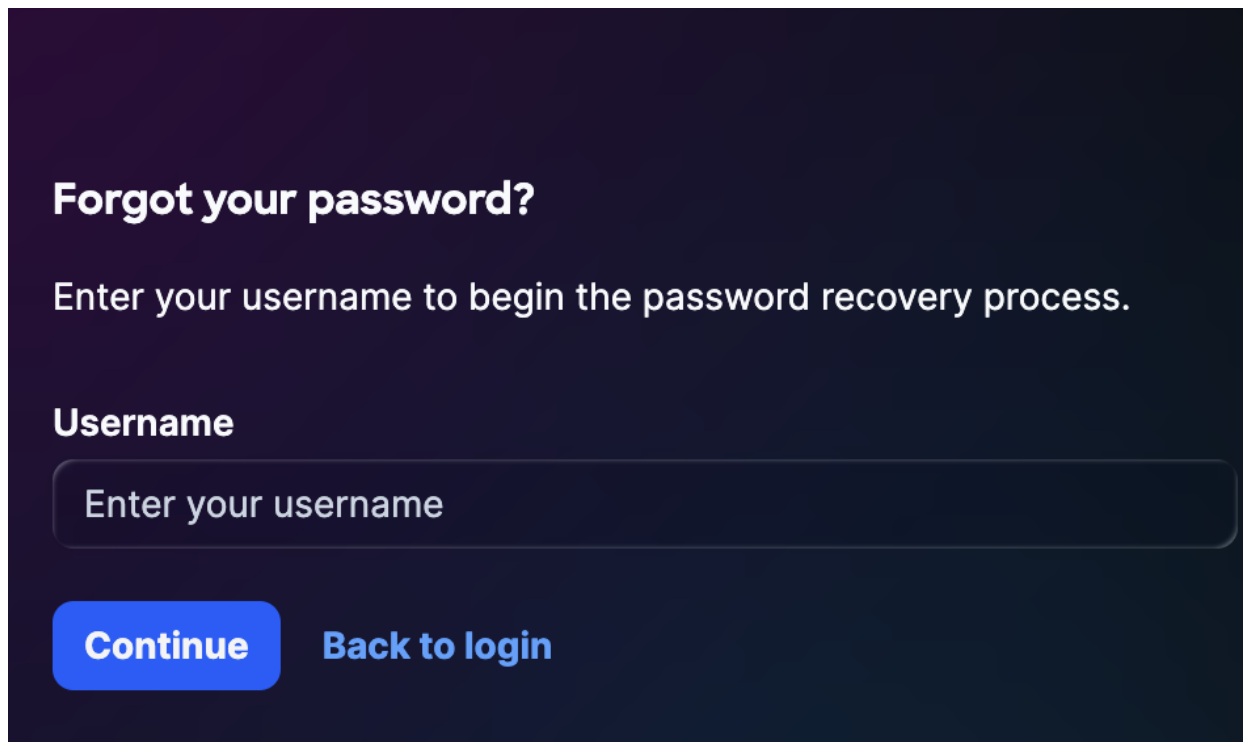
Het wachtwoord wordt bijgewerkt in het Cisco IQ-systeem, inclusief de Cisco IQ VM.

Een vergeten wachtwoord opnieuw instellen

U kunt een wachtwoord opnieuw instellen met behulp van het verificatieproces voor beveiligingsvragen.

Om een vergeten wachtwoord opnieuw in te stellen:

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



Forgot your password?

Enter your username to begin the password recovery process.

Username

Enter your username

Continue **Back to login**

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.

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

Enter your answer

Show

What is your mother's maiden name?

Enter your answer

Show

What was the name of your elementary school?

Enter your answer

Show

Verify and continue

Back to login

Identiteit verifiëren

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.

Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

[Show](#)

Confirm password

[Show](#)[Reset password](#)[Back to login](#)

Wachtwoord herstellen



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 logout 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.

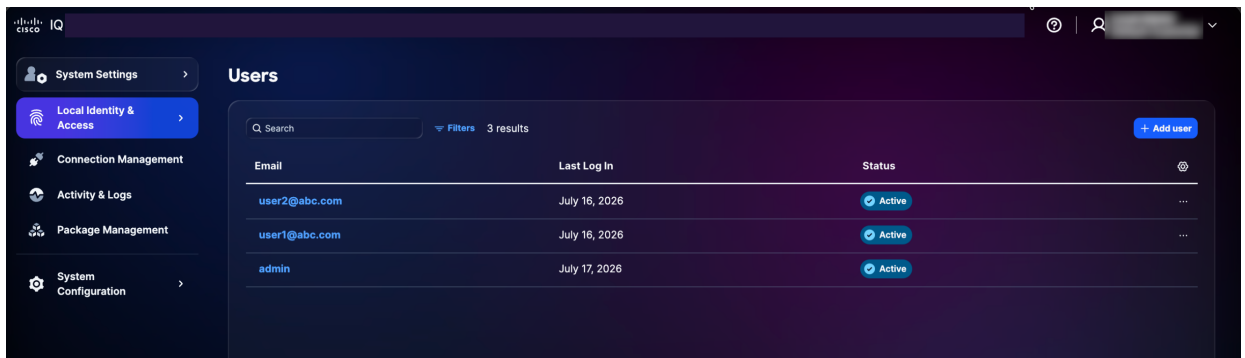
7. Voer het nieuwe wachtwoord in.
8. Voer het wachtwoord opnieuw in om te bevestigen.
9. Klik op Indienen.

Lokale gebruikers toevoegen

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

nieuwe gebruiker toevoegen:

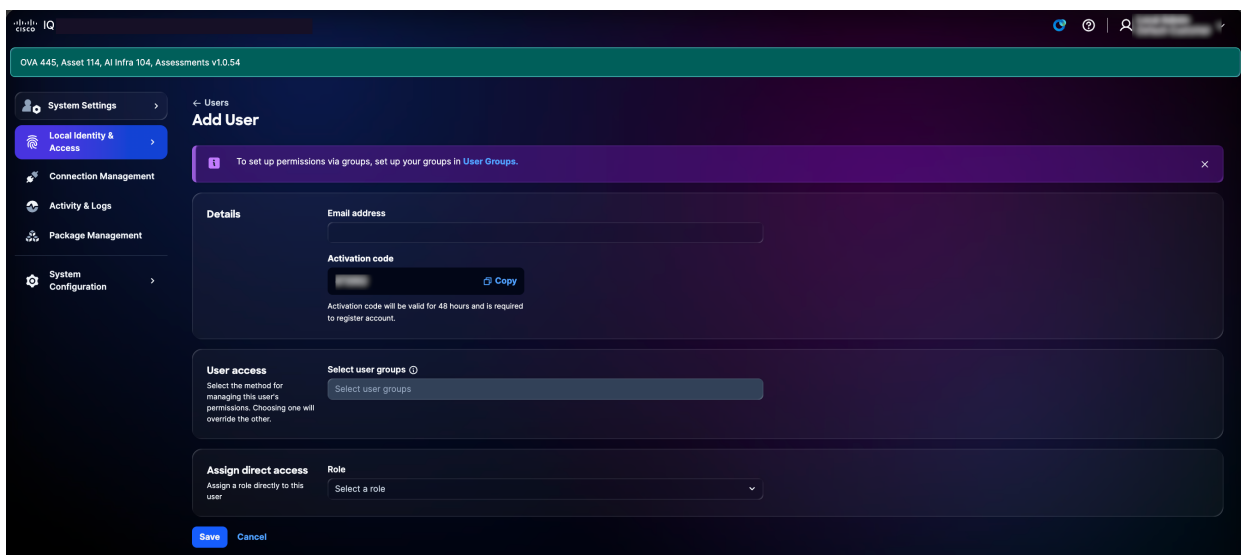
1. Navigeer naar Systeeminstellingen > Lokale identiteit en toegang > Gebruikers. De pagina Gebruikers wordt weergegeven. Het geeft een overzicht van alle bestaande lokale gebruikers, samen met hun status.



Gebruikerspagina

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

- 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 de



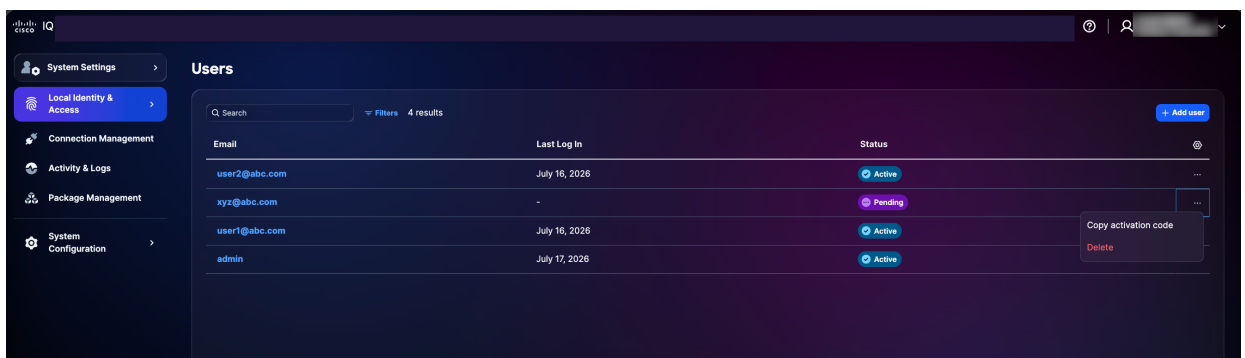
weergegeven activeringscode met de gebruiker, zoals vereist voor registratie.

5. In Gebruikerstoegang kiest u de gebruikersgroep in de vervolgkeuzelijst Gebruikersgroepen selecteren.



Opmerking: gebruikers erven toegang van de geselecteerde groep.

6. In Directe toegang toewijzen, kiest u de rol in de vervolgkeuzelijst Rol. Er zijn twee (2) rollen beschikbaar:
 - Viewer: toepassingen weergeven en openen
 - Accountbeheerder: toegang tot modules en beheer systeeminstellingen, behalve System Management en Identity Provider (IDP)
7. Klik op Save (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.
8. Zoek de nieuwe gebruiker in de lijst en bevestig dat de kolom Status in behandeling wordt weergegeven.
9. Klik op het pictogram Meer opties naast de nieuwe gebruiker.



Activeringscode kopiëren

10. Selecteer de activeringscode voor kopiëren in de vervolgkeuzelijst. De activeringscode wordt naar het klembord gekopieerd.
11. 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.

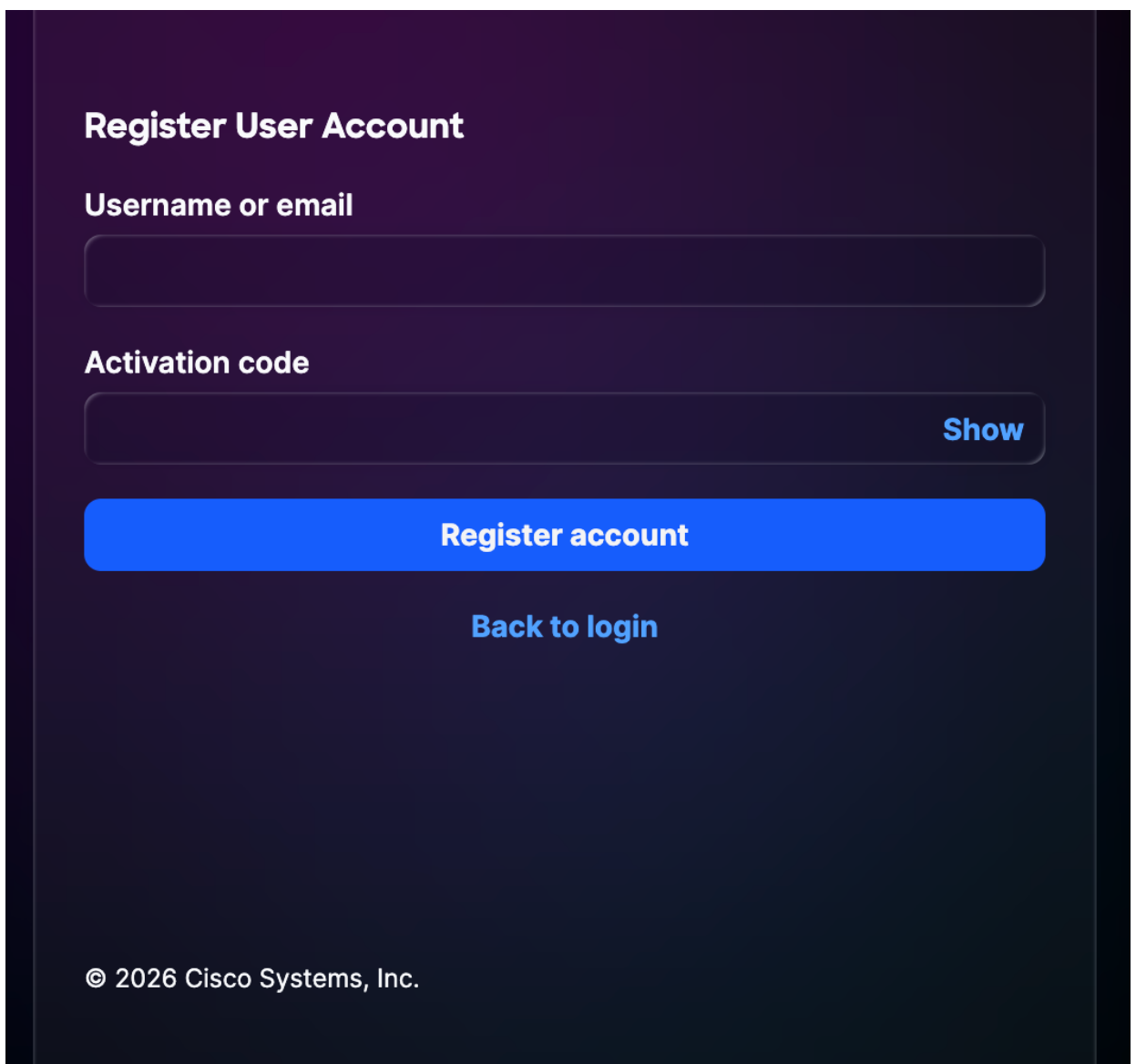
 Activeringscodes zijn 48 uur geldig. Neem contact op met uw accountbeheerder om een nieuwe code aan te vragen als de code verloopt.

12. Als u zich wilt afmelden, klikt u op het pictogram Gebruikersprofiel in de rechterbovenhoek en selecteert u Afmelden. U keert terug naar de aanmeldingspagina van Cisco IQ.

Nieuwe gebruikersaccounts registreren

Om de nieuwe gebruikersaccount te registreren:

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



Register User Account

Username or email

Activation code

 Show

Nieuwe gebruikersaccount

2. Voer de gebruikersnaam of het e-mailadres in dat werd gebruikt toen de gebruiker werd gemaakt (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.

Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Show

Confirm password

Show

Reset password **Back to login**

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 instellen](#)).

Beheren van lokale gebruikersgroepen

Gebruikersgroepen stellen de accountbeheerder in staat om rollen voor meerdere lokale gebruikers tegelijk te beheren. In plaats van een rol aan elke gebruiker

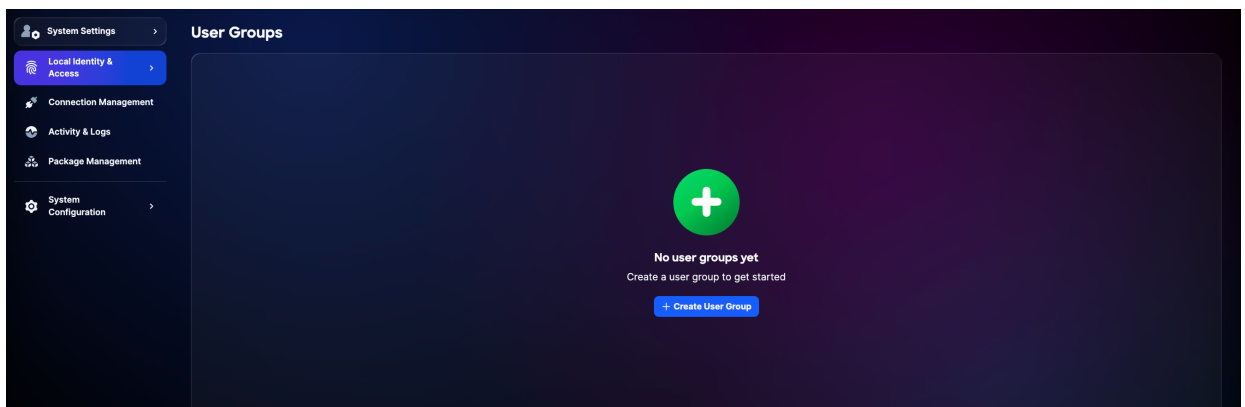
afzonderlijk toe te wijzen, kunt u een groep maken, er een rol en een set gebruikers aan koppelen en de rol of het lidmaatschap op één plaats bijwerken. Alle gebruikersgroepbeheer wordt uitgevoerd vanaf de pagina Lokale identiteit en toegang.

 **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. Zie [Lokale gebruikers toevoegen](#) voor meer informatie.

Een gebruikersgroep maken

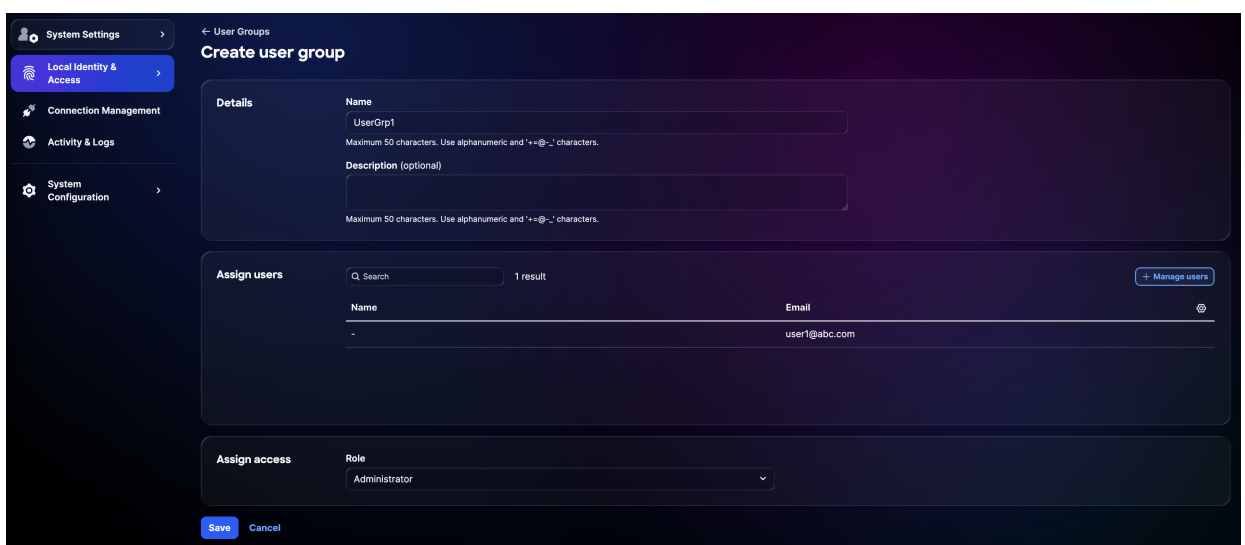
U maakt als volgt een gebruikersgroep:

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: bekijk- en toegangsmodules (alleen-lezen)
- Beheerder: toegang tot modules en beheer systeeminstellingen

4. Klik op Save (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. Kies het pictogram Meer opties > Bewerken van de gewenste groep. De pagina Gebruikersgroep bewerken wordt weergegeven.

The screenshot shows the 'Edit user group' interface. On the left is a sidebar with navigation links: System Settings, Local Identity & Access (highlighted), Connection Management, Activity & Logs, and System Configuration. The main content area is titled 'Edit user group' and contains three sections: 'Details' with input fields for 'Name' (containing 'UserGrp1') and 'Description (optional)'; 'Assign users' with a search bar and a table showing one user with email 'user1@abc.com'; and 'Assign access' with a 'Role' dropdown menu set to 'Administrator'. At the bottom are 'Save' and 'Cancel' buttons.

Gebruikersgroep bewerken

3. Breng de gewenste veranderingen aan.

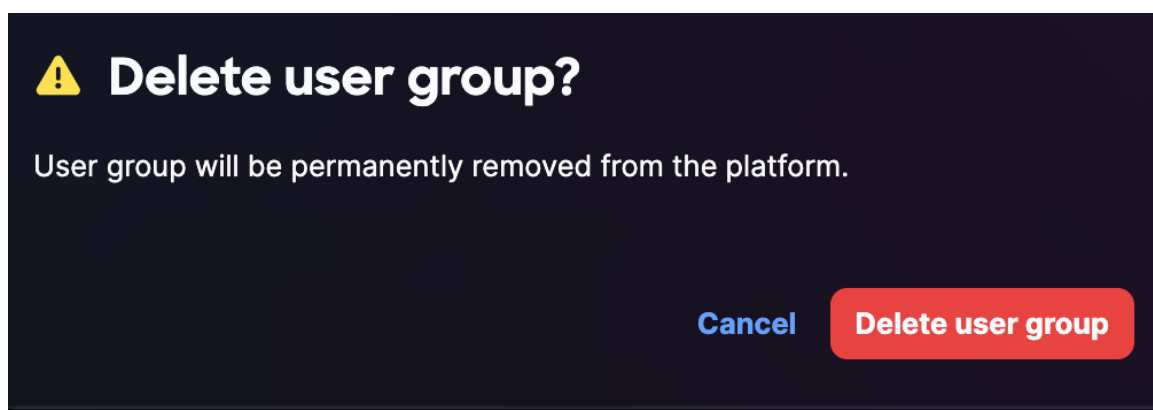
4. Klik op Save (Opslaan).

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

Eenmaal ingelogd bij VA kunnen accountbeheerders verschillende instellingen configureren. Accountbeheerders kunnen inloggen met behulp van lokale administratie of IDP-configuratie.

Okta IDP SAML-configuratie voor SSO

Vereisten voor het configureren van IDP SAML

- Toegang van lokale beheerders tot Cisco IQ

- Toegang tot IDP-portal

IDP SAML-configuratie voor SSO

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

1. Navigeer naar uw IDP-portal.

Tabel 2: Cisco IQ-kenmerken

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

Tabel 3: SAML-configuratieparameters

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

5. Configureer de attribuut statements.



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: .*

6. Configureer de instellingen voor Single Logout (SLO) in de toepassing.

Tabel 4: 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 metagegevens van de Service Provider (SP) 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

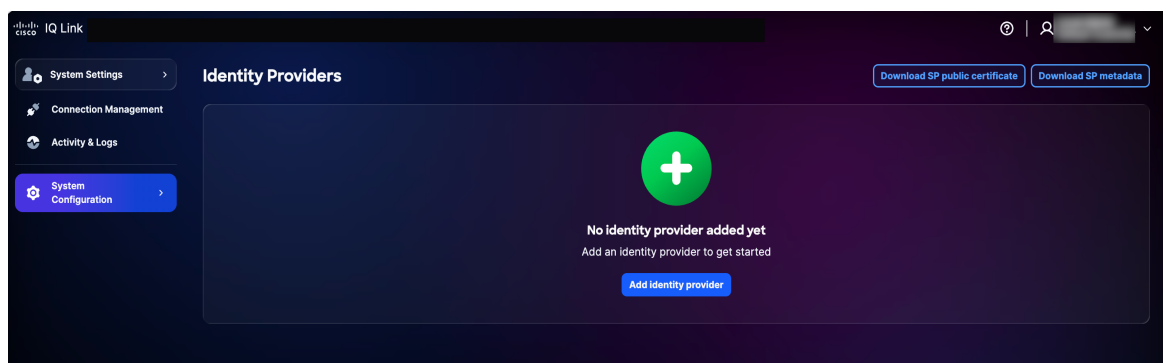
8. Klik op het pictogram Download om het bestand "IDP Metadata XML" te downloaden.

9. De applicatie beschikbaar stellen of maken zoals vereist door de provider.

Okta IDP toevoegen

Een IDP toevoegen aan Cisco IQ:

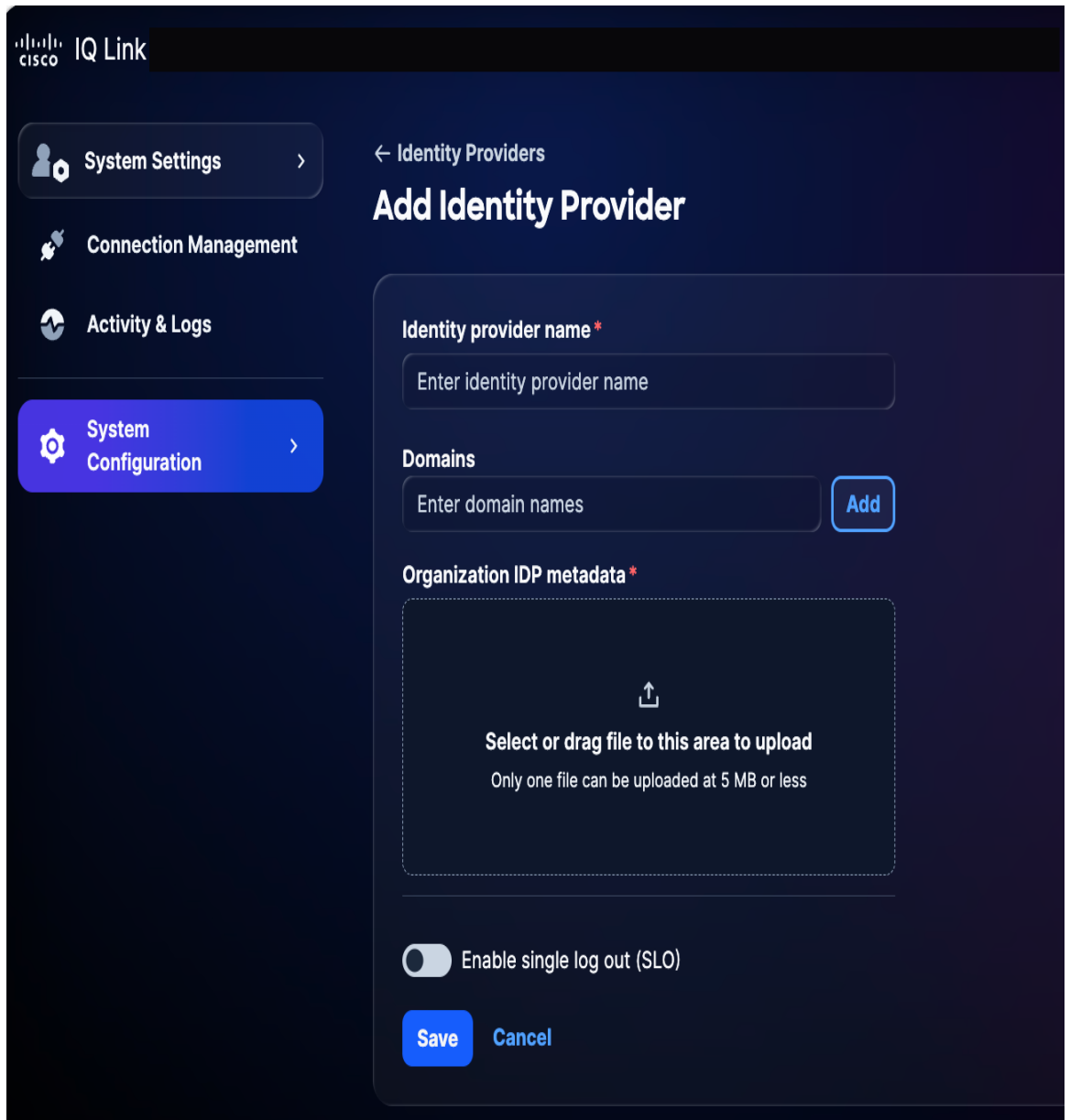
1. Kies in Systeeminstellingen de optie Systeemconfiguratie > Identiteitsproviders. De pagina Identiteitsproviders wordt weergegeven.



IDP-startpagina

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

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



System Settings >

Connection Management

Activity & Logs

System Configuration >

← Identity Providers

Add Identity Provider

Identity provider name *

Enter identity provider name

Domains

Enter domain names **Add**

Organization IDP metadata *

Select or drag file to this area to upload
Only one file can be uploaded at 5 MB or less

☐ Enable single log out (SLO)

Save **Cancel**

Identiteitsprovider toevoegen

3. Voer de naam van de identiteitsprovider in.
4. Klik op Toevoegen om een door Cisco IQ geconfigureerde domeinnaam toe te voegen aan het veld Domein(en).
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 certificaatdetails en SP-entiteitsgegevens.

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

7. Klik op Save (Opslaan).

Configuratie roltoewijzing

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

×

Map identity provider roles to system roles to assign permissions.

Map User Roles

IDP Role	System Role
iq-demo-user ×	General Account... × ▼ 🗑
	▼ 🗑
	▼ 🗑
	▼ 🗑
	▼ 🗑

+ Add identity provider role

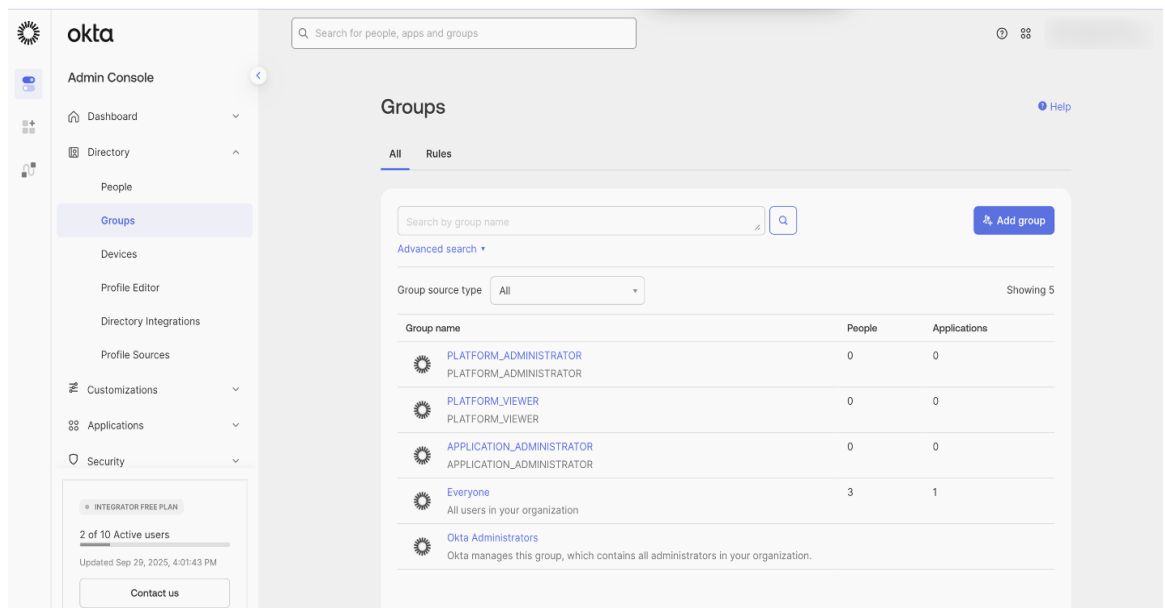
Save

Gebruikersrollen toewijzen

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.



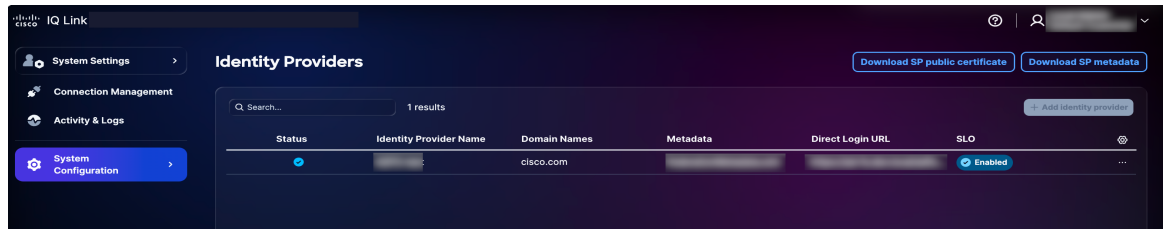
referentie voor roltoewijzing

3. Voeg extra rollen toe zoals vereist door te klikken op Identiteitsproviderrol toevoegen.
4. Klik op Save (Opslaan). Eenmaal geconfigureerd, geeft de aanmeldingspagina een optie weer om in te loggen met SSO (via IDP).

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 startpagina van Identity Providers op Openbaar SP-certificaat downloaden.



SP Public Certificate

2. Sla het gedownloade bestand 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. Voer de SLO-URL in (bijvoorbeeld <https://ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com/saml/logout>).
6. Voer de SP-uitgever in (bijvoorbeeld ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com).
7. Klik op Indienen.
8. Download het IDP-metagegevensbestand opnieuw.
9. Kies op de pagina Identiteitsproviders het pictogram Meer opties van de toegevoegde IDP > Bewerken.
10. Schakel de knop Single Log Out (SLO) inschakelen in.
11. Upload het nieuw gedownloade metagegevensbestand.
12. 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 uitpakket
- Als SLO is ingeschakeld, is de SLO-configuratie compleet met het echte handtekeningcertificaat
- End-to-end SSO- en SLO-flow wordt met succes getest

Problemen met IDP oplossen

In de volgende tabellen worden veelvoorkomende problemen en mogelijke oplossingen weergegeven om problemen met betrekking tot de IDP-status, certificaatfouten, SSO-aanmeldingsfouten en SLO-configuratie snel te identificeren en op te lossen:

Tabel 5: 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 (FS) als de SAML IDP voor Cisco IQ, met ondersteuning voor wachtwoordgebaseerde en Public Key Infrastructure (PKI) of op certificaten gebaseerde verificatie.

Vereisten voor het configureren van ADFS IDP SAML voor SSO

- ADFS 6.0+ wordt aanbevolen
- Windows Server 2016 + (aanbevolen 2019)
- AD-integratie met gebruikersaccounts configureren
- SSL/TLS-certificaten op ADFS-server
- Toegang voor beheerders tot Cisco IQ
- Administratieve toegang tot ADFS-server (Windows Server)
- PowerShell-toegang op ADFS-server
- Netwerkconnectiviteit tussen ADFS en Cisco IQ
- Enterprise Certificate Authority (CA) (geïnstalleerd of bereikbaar)
- Domeinbeheerder of Enterprise Administrator-bevoegdheden (alleen vereist voor PKI)

- Configuratiegegevens ADFS-server (zoals weergegeven in onderstaande tabel)

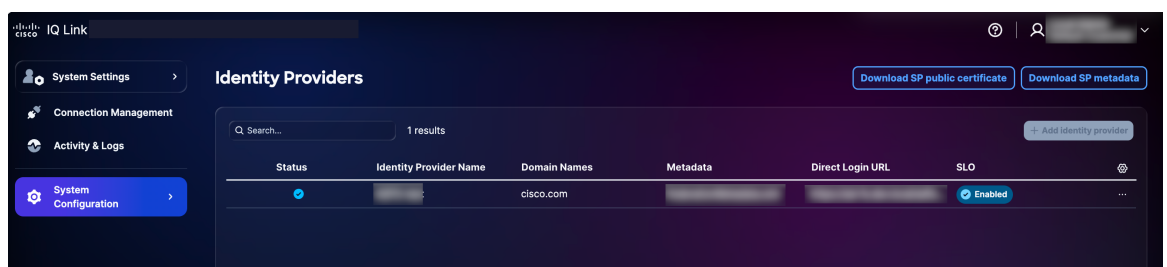
Tabel 6: Overzicht van de verificatiestroom

Item	Beschrijving	Voorbeeld
Cisco IQ FQDN	Hostnaam voor gebruikersimplementatie	<Your-CIQ-FQDN> Bijvoorbeeld dev35-23.cx-xxx-xxx.cisco.com
ADFS Server-URL	Adres ADFS-server gebruiker	https://<Your-ADFS-HOSTNAME> Bijvoorbeeld https://adfs.dev.local
bedrijfsdomein	E-maildomein	<Uw-domein>
AD-groepen	Active Directory-groep Domeinnamen (DN)	CN=RoI - CXIQ-ontwikkelaars OU=groepen, DC=dev, DC=lokaal
Naam CA (PKI)	Enterprise CA-naam	<Uw-CA-naam>
Cert Auth-poort (PKI)	ADFS alternatieve TLS-poort	49443
Thumbprint SSL-certificaat	ADFS server SSL certificaat	<Uw SSL-CERT-THUMBPRINT>

Basis-ADFS SAML 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 de ADFS-server (bijvoorbeeld C:\).

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 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 "Cisco IQ"), 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 niet "Iedereen toestaan met MFA" tenzij uw ADFS-server een geregistreerde Multi-Factor Authentication (MFA)-adapter heeft (bijvoorbeeld Azure MFA, 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
```

To set "Permit everyone" (no MFA requirement), run the following command:

```
Set-AdfsRelyingPartyTrust -TargetName "
```

```
"
```

```
-AccessControlPolicyName "Permit everyone"
```

You can also create the trust through 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/permit", Value =
```

```
"true");
```

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 7: Vereiste vorderingen

aanspraak	Doel	bron
Email	Gebruikersidentificatie	AD Mail
Weergavenaam	Volledige naam van de gebruiker	AD-weergavenaam
UPN	PKI/certificaatverificatie	ADFS koppelt het clientcertificaat aan een AD-gebruiker via 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 - Production").

```
$relyingPartyName = "Your-RP-Name"
```

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"
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
@RuleTemplate = "LdapClaims"
@RuleName = "Send UPN"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"),
query = ";userPrincipalName;{0}", param = c.Value);
@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.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "email");
@RuleName = "Send Group Membership"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/group"),
query = ";memberOf;{0}", param = c.Value);
'@
```

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

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

Write-Host "Claimregels succesvol geconfigureerd!" -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 door de volgende opdracht uit te voeren:

```
$username = "username"
```

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 met de volgende opdracht:

```
$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 het TrustedPeople-archief:

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

2. Kies een van de volgende opties:



Opmerking: het SP-certificaat wordt uitgegeven door een interne 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
```

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

```
Import-Certificate -FilePath "C:-ca.cer" -CertStoreLocation  
"Cert:"
```

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

Restart-Service adressrv

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. Controleer de 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 ECU (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 ECU 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
- Onderwerpsnaam: 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 de hoofdnaam van de gebruiker (User Principal Name, UPN) 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,
```

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 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:

```
EEnable-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
```

Certificaatverificatie inschakelen als primaire

Zo schakelt u de certificaatverificatie in als primaire optie:

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

```
Set-AdfsGlobalAuthenticationPolicy `\  
-PrimaryIntranetAuthenticationProvider @(“CertificateAuthentication”, “WindowsAuthentication”)\  
-PrimaryExtranetAuthenticationProvider @(“CertificateAuthentication”, “FormsAuthentication”)
```


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)

De stappen in de volgende secties verhelpen CERT_E_UNTRUSTEDROOT (0x800B0109)-fouten die voorkomen dat certificaatverificatie 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 onderhandeling over clientcertificaten ingeschakeld met 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 de volgende opdracht:

```
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)" -Fore
```

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

```
$bad | Move-Item -Destination Cert:\IntermediateCA
Write-Host "Moved $($bad.Count) cert(s) from Root to Intermediate CA store" -Foreground
```

3. Controleer of er geen niet-zelf-ondertekende certificaten in het Trusted Root-archief 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 de volgende opdrachten:

```
Set-ItemProperty -Path $regPath -Name "ClientAuthTrustMode" -Value 2 -Type DWord  
Set-ItemProperty -Path $regPath -Name "SendTrustedIssuerList" -Value 0 -Type DWord
```

Tabel 8: Instellingen van het 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 in het SystemCertificates-archief worden opgeslagen 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 behulp van de volgende opdracht:

```
$exists = Test-Path "HKLM:\caThumbprint"
```

Als het certificaat niet wordt gevonden, importeert u het in het LocalMachine-archief:

```
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 Meta  
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> en vervang "<your-adfs-server>" door de hostnaam van uw ADFS-server.
2. 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 de knop Enkelvoudige afmeldoptie inschakelen indien nodig 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"] }
```

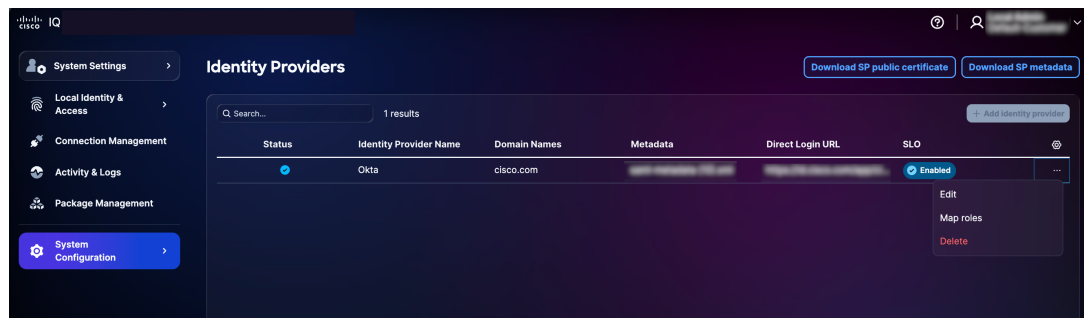
Het systeem zoekt AD rechtstreeks op via het Lightweight Directory Access Protocol (LDAP), waarvoor geen extra modules nodig zijn.

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
```

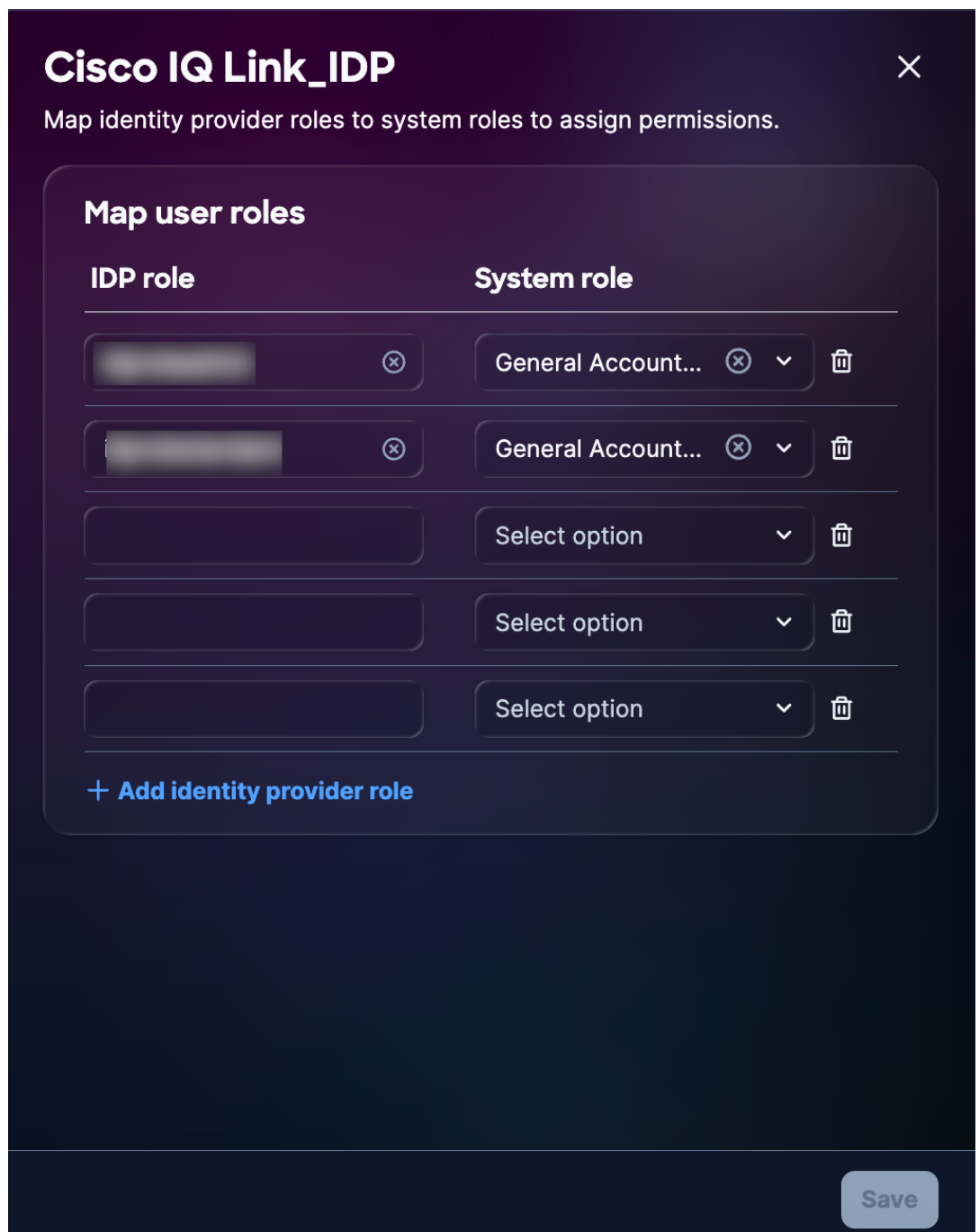
Als de vereiste groepen niet worden vermeld, moeten deze in AD worden gemaakt door een accountbeheerder voordat u de toewijzing van de ADFS-rollen kunt voltooien.

Roltoewijzing configureren:



roltoewijzing

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 DN's.

3. Klik op Save (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 het testen van de browser voor PKI-stroom, moet u ervoor zorgen dat het gebruikerscertificaat is geïnstalleerd in MacOS Keychain (zie [Gebruikerscertificaat importeren op clientsysteem \(MacOS\)](#)). 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 een 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-/formulieverificatie.
3. Voer een gebruikersnaam in.
4. Voer een wachtwoord in.
5. Controleer of de aanmelding geslaagd 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 9: 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
Decodering mislukt	"Mislukt om assertion te decoderen" in logs	Configuratie controleren op ADFS-certificaatconfiguratie
aanmeldingslus	Vastgelopen in verificatie- of	◦ Ongeldige ACS-URL: Verifiëren:

uitgeven	Symptomen / beschrijving aanmeldingslus	Oorzaken / Controles / Workarounds en Fixes
		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 - Production" |  
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 - Production" |  
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 op wachtwoord gebaseerde als PKI of Certificate-Based Authentication (CBA) ondersteunt.

Vereisten voor het configureren van Entra ID SAML voor SSO

- 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 10: 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

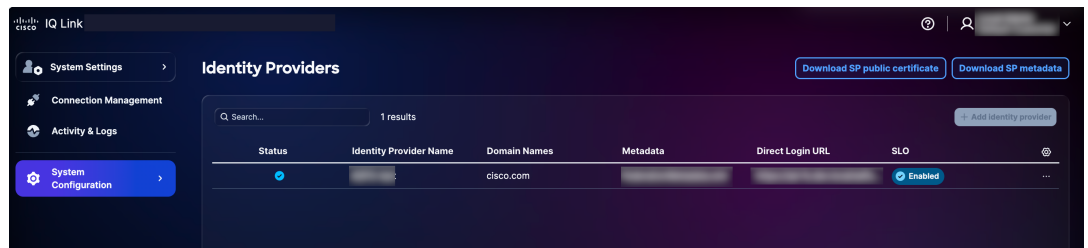
Een bedrijfstoepassing maken

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 het verkrijgen door de volgende stappen uit te voeren van 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 SAML-gebaseerde scherm voor eenmalige aanmelding na het uploaden.

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:

4. Navigeer in de Enterprise-toepassing naar Eenmalige aanmelding en kies SAML.
5. Klik in de sectie Basic SAML Configuration op Edit en voer het volgende in:
 - Identificatiecode (Entiteit-ID): <YOUR-CIQ-FQDN>
 - Reply URL (ACS URL): https://<YOUR-CIQ-FQDN>/saml/acs
 - Aanmelden URL: https://<YOUR-CIQ-FQDN>/saml/login
 - Afmeldings-URL: https://<YOUR-CIQ-FQDN>/saml/logout
6. 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.

7. Als u SAML-kenmerken en -claims wilt configureren, klikt u op Bewerken in de sectie Kenmerken en claims.

8. Configureer de volgende claims:

Tabel 11: 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/emailaddress
voornaam	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
familienaam	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
naam	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
groepen	gebruiker.toewijzende droles	(LEEG — de naamruimte wissen)



Opmerking: Voor de claim groepen:

- Gebruik user.assignedroles als bron - niet user.groups
- 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 Apply (Toepassen).



Opmerking: maak rollen die overeenkomen met uw vereisten voor roltoewijzing van Cisco IQ (bijvoorbeeld CXIQ-beheerders, CXIQ-ontwikkelaars of 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 Identifier (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. Kies in de Enterprise-toepassing voor Single Sign-On > SAML Signing Certificate.

2. Download Federation Metadata XML (opslaan als entra-id-metadata.xml).

OF

Download Certificate (Base64) voor handmatige certificaatinvoer.

3. Let op de volgende waarden in 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 de knop Enkelvoudige afmeldoptie inschakelen indien nodig 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 12: Systeemrollen

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

 Opmerking: Gebruik de tekenreeksen voor de waarde van de app-rol precies zoals geconfigureerd in Entra ID (zie [App-rollen configureren](#) voor meer informatie)

4. Klik op Save (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 success"
```

verwachte productie

SAML 2.0-compatibele verificatie succesvol voor gebruiker:
user@domain.com met volledige naam: N/A en 1 groepen

Geëxtraheerde groep: CXIQ-beheerders (origineel: CXIQ-beheerders)

Totaal aantal gewonnen groepen: 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 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 opdrachten uit om het certificaat te genereren:

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

4. Voer de volgende opdracht uit om de aanvraag bij de CA 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 CA 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

"
```

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. Onder Vertrouwen, ingesteld 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. Schakel CBA in en voeg de doelgebruikers of -groepen toe.
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 (SAN) van het certificaat toegewezen aan de gebruiker van 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 de e-mail 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 ander gebruikerscertificaat of een verlopen certificaat) 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 13: Problemen oplossen

uitgeven	Oorzaak	Oplossen
Ongeldige SAML-reactie - ontbrekende e-mail	SAML-bevestiging heeft geen NameID of e-mailkenmerk	Controleer de claimconfiguratie van Entra ID (zie SAML Single Sign-On configureren voor meer informatie). Controleer of de gebruiker het e-mailkenmerk heeft ingevuld.
Totaal aantal geëxtraheerde groepen: 0	Groepen claimen 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 voor meer informatie).
Claims voor dubbele groepen	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 Rollenbenadering (zie App Rollen configureren voor meer informatie).
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	Download de metagegevens opnieuw van de Entra ID en upload deze opnieuw naar Cisco IQ.
AADSTS500191	CRL niet bereikbaar vanaf internet	Publiceer de CRL naar een openbaar toegankelijke URL of gebruik de zelfondertekende CA-

uitgeven	Oorzaak	Oplossen
Certificaat niet gevraagd	Certificaat niet in sleutelhanger, CA niet vertrouwd op client of CBA niet ingeschakeld	benadering (zie CRL Workaround voor problemen met bereikbaarheid voor meer informatie).
		Controleer of het gebruikerscertificaat is geïmporteerd in MacOS Keychain Access (zie Gebruikerscertificaat importeren op clientsysteem (MacOS) voor meer informatie), of de KBA is ingeschakeld in Entra ID met de vereiste instellingen (zie KBA inschakelen in Verificatiemethoden voor Entra ID voor meer informatie) en of Chrome opnieuw is gestart om wijzigingen toe te passen.
		Verhoog de clock_skew_seconds in de plugin configuratie (de standaard is 300; gebruik 30000 voor het lab).
SAML-bevestiging verlopen	Klok scheef tussen systemen	
Status "Onvolledig" in virtueel toestel	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 Cisco Discovery Protocol (CDP), probeert Entra ID geen CRL-validatie uit te voeren.

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

- Een bedrijfstoepassing (niet-galerij) maken in Entra ID
- Configureren van een Basic SAML-configuratie 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
- Download de Federatie Metadata XML

Cisco IQ-configuratie

- Voeg een IDP toe aan Cisco IQ door Entra ID-metagegevens te uploaden
- De roltoewijzing configureren om app-rolwaarden 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)

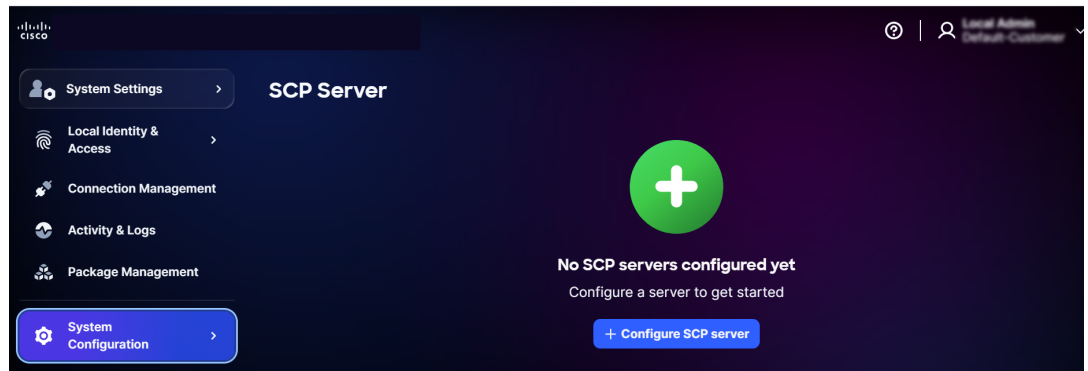
- Certificaatsjabloon maken op AD CS met Client Authentication ECU
- Geef een gebruikerscertificaat af met een UPN die overeenkomt met de gebruikersidentificatie van Entra
- Een gebruikerscertificaat exporteren als een PFX-bestand en installeren op het clientsysteem
- Vertrouw het CA-certificaat op het clientsysteem
- Het CA-basiscertificaat uploaden naar Entra ID onder Bescherming > Certificaatautoriteiten
- De KBA inschakelen in verificatiemethoden
- Gebruikersnaambinding configureren (PrincipalName en userPrincipalName)
- Controleren of CBA-aanmelding end-to-end werkt

SCP-server toevoegen

Een SCP-server 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. De pagina SCP-server configureren wordt weergegeven.

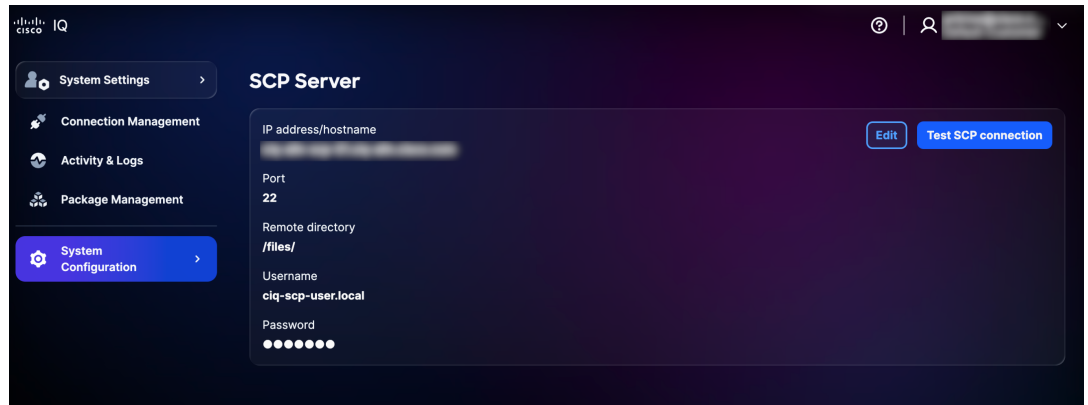
SCP-server configureren

3. Voer een IP-adres/hostnaam in.
4. Voer een poort in.
5. Voer een externe directory in.
6. Voer een gebruikersnaam in.
7. Voer een wachtwoord in.
8. Klik op Save (Opslaan). Er wordt een bevestiging weergegeven.

Een bestaande SCP-server bewerken

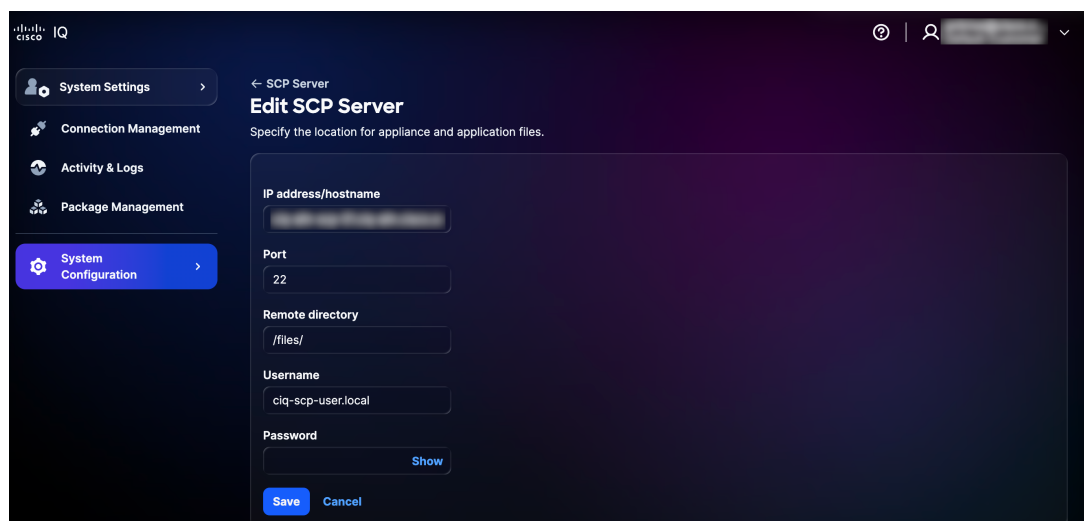
U bewerkt als volgt een bestaande SCP-server:

1. Navigeer naar de pagina SCP Server.



SCP-server toegevoegd

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



SCP-server bewerken

3. Wijzig de gegevens zoals vereist.

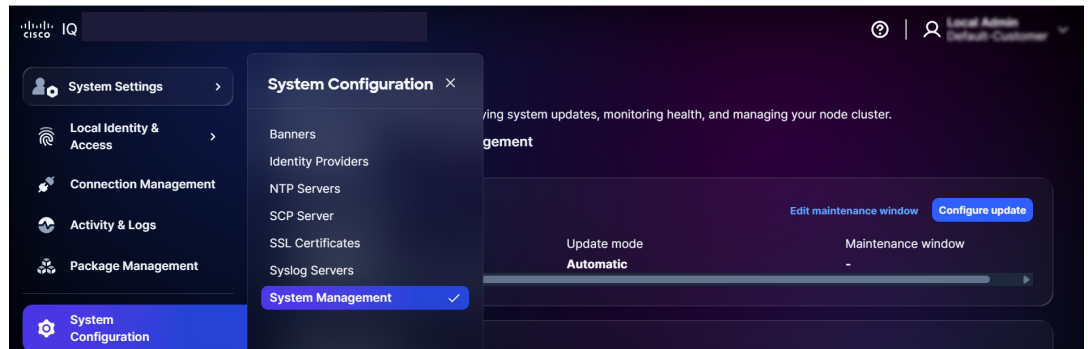
4. Klik op Save (Opslaan).

stysteembeheer

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

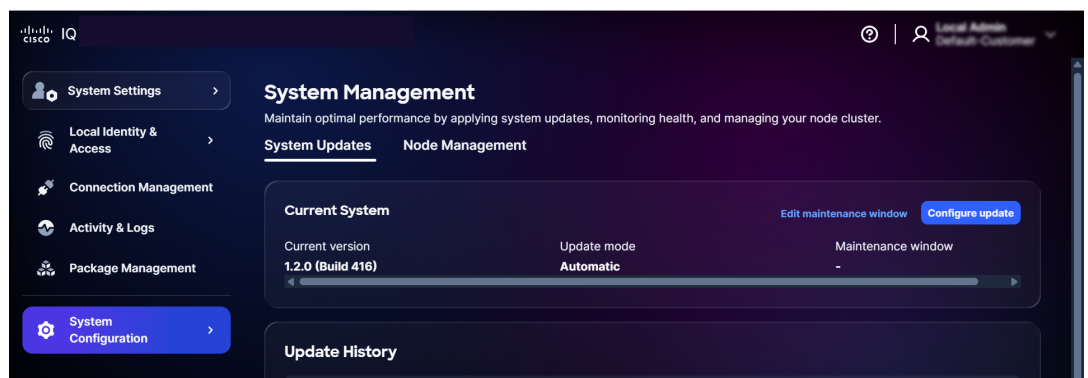
Systeemupdate opnieuw plannen

De systeemupdate opnieuw plannen:



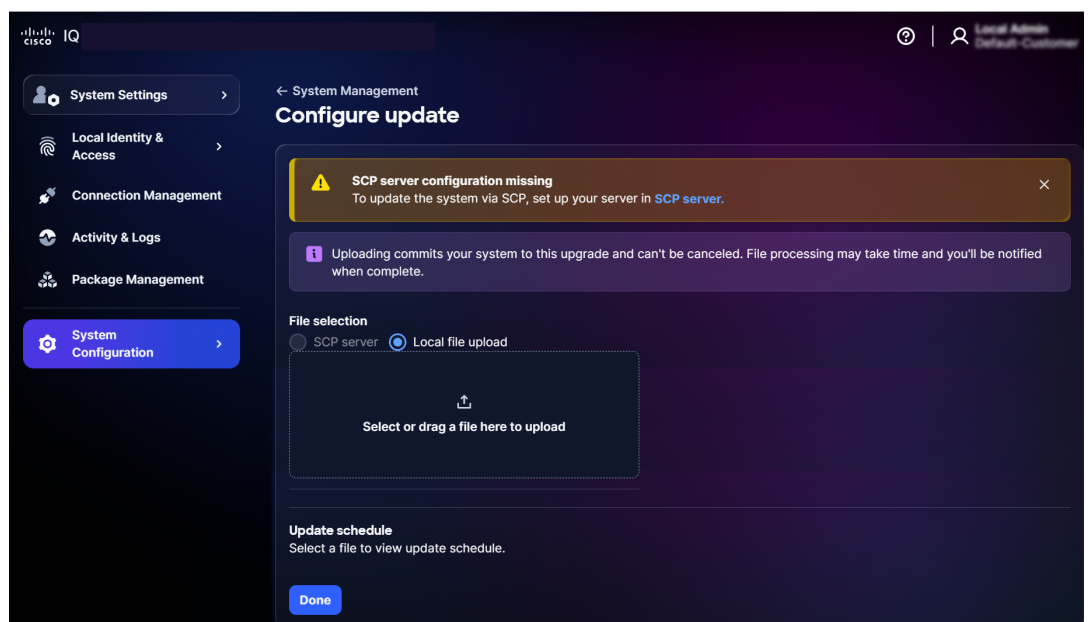
stelsysteembeheer

1. Kies Stelsysteemconfiguratie > Stelsysteembeheer in Stelsysteeminstellingen. De pagina Stelsysteembeheer wordt weergegeven. Op deze pagina wordt de stelsysteemversie weergegeven die momenteel wordt uitgevoerd. Als er geen updates zijn geconfigureerd, is het gedeelte Updategeschiedenis leeg.



Stelsysteemupgrade

2. Klik op Update configureren. De pagina Bijwerken configureren wordt weergegeven.



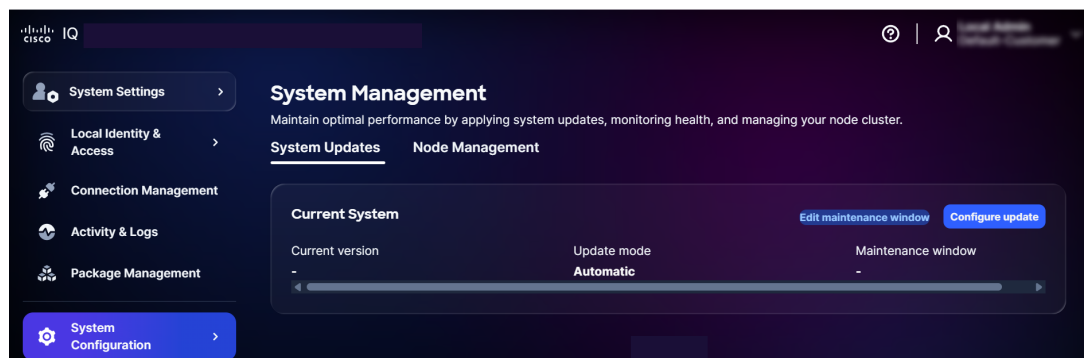
Upgrade configureren

3. Kies het updateschema om een andere tijd in te plannen.
4. Wacht tot het uploaden van het bestand is voltooid; de duur is afhankelijk van de bundelgrootte en de netwerksnelheid.

Bevestig dat de update is voltooid door het vinkje te controleren dat wordt weergegeven onder de kolom Status bijwerken.

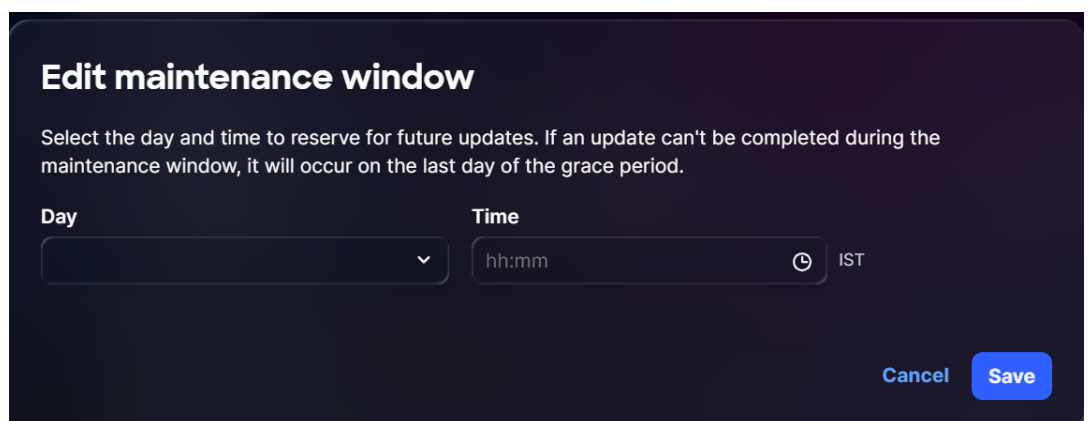
Planningen voor systeemupgrades bewerken

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:



Onderhoud bewerken

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



Onderhoudsvenster bewerken

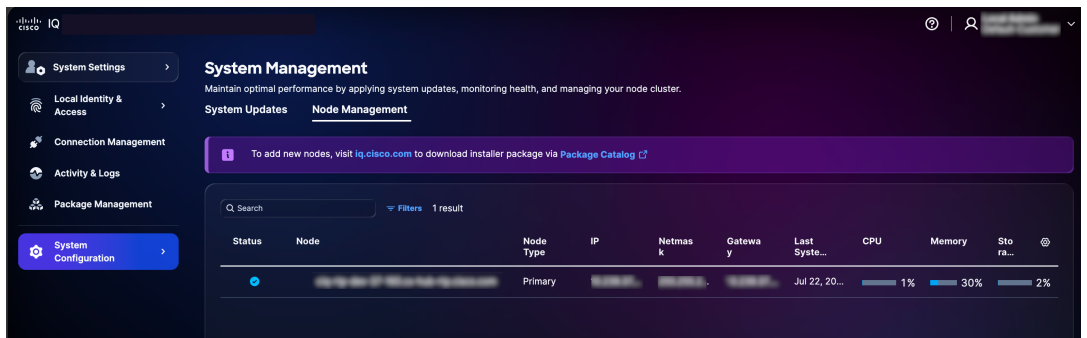
2. Kies een optie uit de vervolgkeuzelijsten Dag en Tijd.
3. Klik op Save (Opslaan). Het onderhoudsvenster is met succes

gepland. De update wordt geactiveerd volgens het weergegeven schema.

 **Opmerking:** als er geen upgradeschema is geconfigureerd, worden er standaard perioden van twee (2) weken afgeschreven voor upgrades die niet opnieuw worden opgestart en vier (4) weken voor upgrades die opnieuw moeten worden opgestart. Na deze respijtp perioden 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.

Nodebeheer

1. Navigeer naar Systeemconfiguratie > Systeembeheer > Nodebeheer om de knooppunten in uw cluster te bekijken en te beheren.



Status	Node	Node Type	IP	Netmask	Gateway	Last System Update	CPU	Memory	Storage
	...	Primary	...	...	...	Jul 22, 20...	1%	30%	2%

Nodebeheer

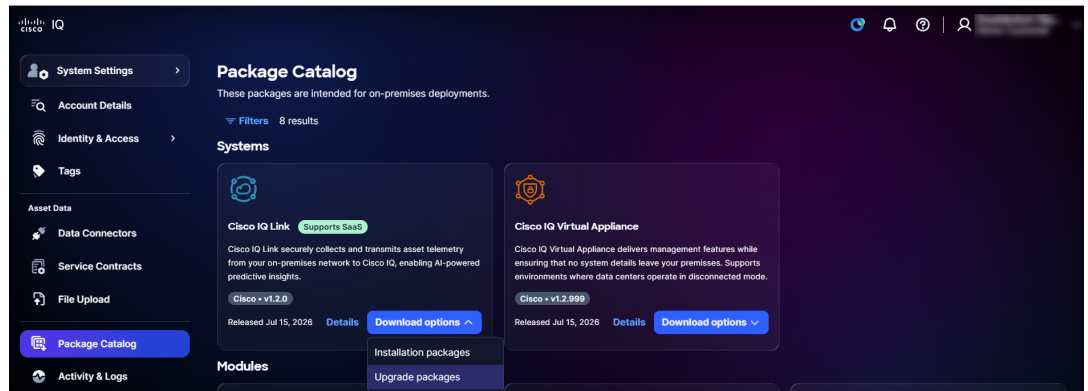
2. In de lijst met knooppunten worden de status, hostnaam, knooppunttype, IP-adres, netmask, gateway en laatste synchronisatietijd van elke node weergegeven.

 **Opmerking:** een blauw vinkje in de kolom Status geeft aan dat de node actief is.

Het systeem handmatig upgraden

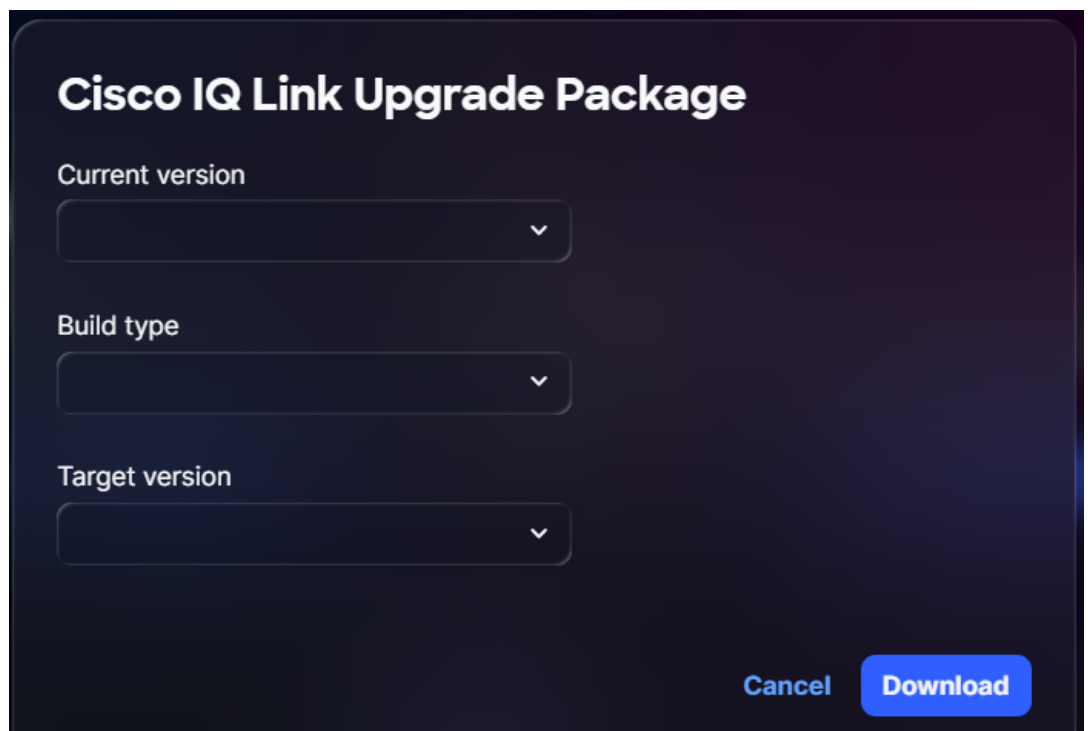
In scenario's waarin automatische distributie van Cisco IQ SaaS niet beschikbaar of vertraagd is, kunt u handmatig een systeemupgrade uitvoeren door de upgradebundel rechtstreeks van Cisco IQ SaaS te downloaden. U kunt het systeem als volgt handmatig bijwerken:

1. Meld u aan bij [Cisco IQ SaaS](#).
2. Navigeer naar Home > Systeeminstellingen > Pakketcatalogus.



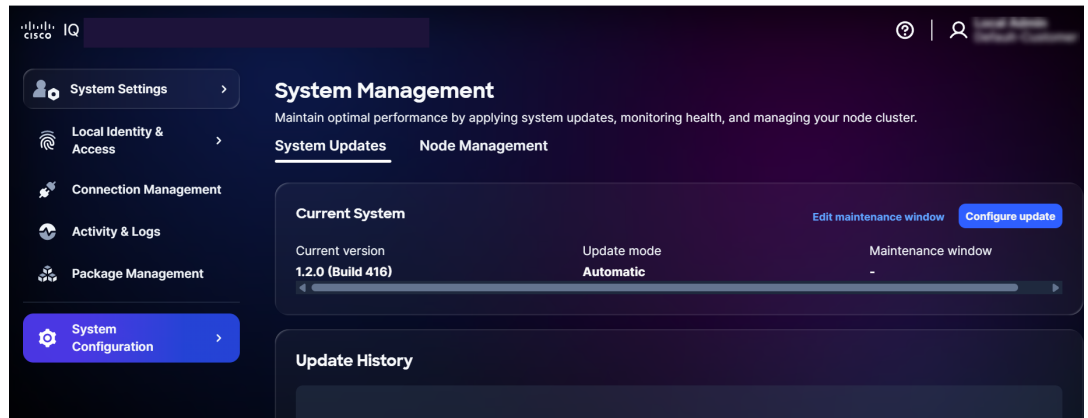
softwarecatalogus

3. Klik op de Cisco IQ Virtual Appliance-kaart op Downloadopties > Upgradepakketten.



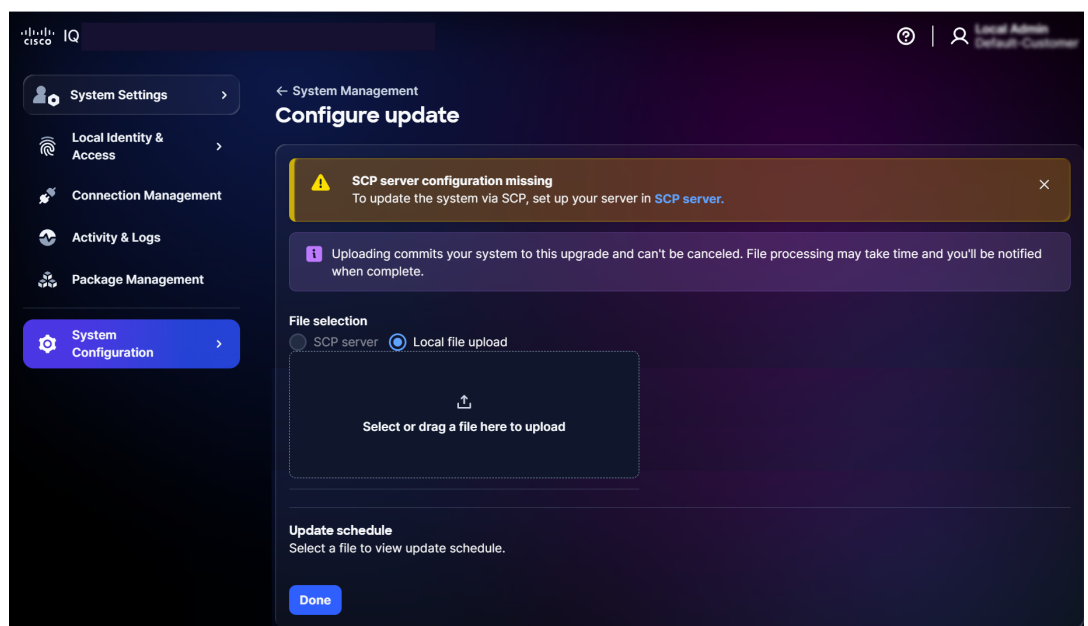
Upgradepakket

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 VA.
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. Wacht tot het uploaden van het bestand is voltooid; de duur is afhankelijk van de bundelgrootte en de netwerksnelheid.

Configuratie SSL-certificaten

Een standaard zelf ondertekend certificaat is vooraf geïnstalleerd en ingeschakeld in Cisco IQ, maar u kunt optioneel 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.

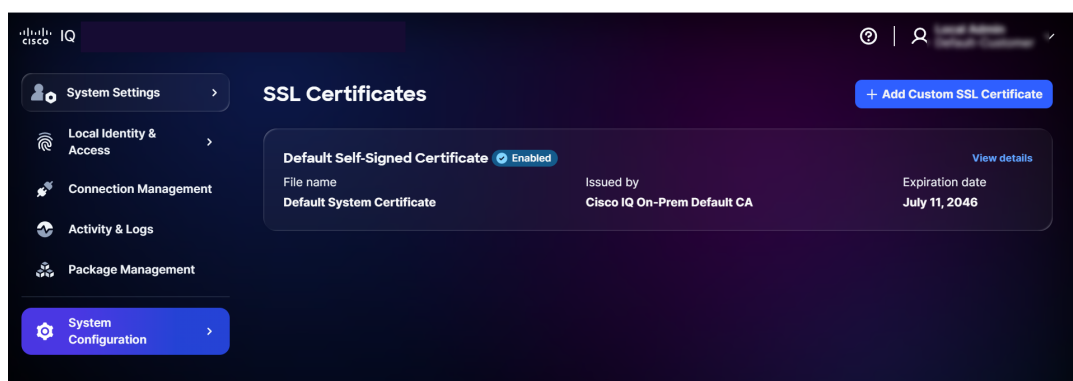


Opmerking: het certificaat moet nog ten minste 90 dagen geldig zijn. Een certificaat wordt beschouwd als "bijna vervallen" wanneer het minder dan 90 dagen heeft tot de vervaldatum. Nadat u een SSL-certificaat hebt toegevoegd, bewerkt of verwijderd, moet u het nieuwe SSL-certificaat uploaden zoals beschreven in [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.

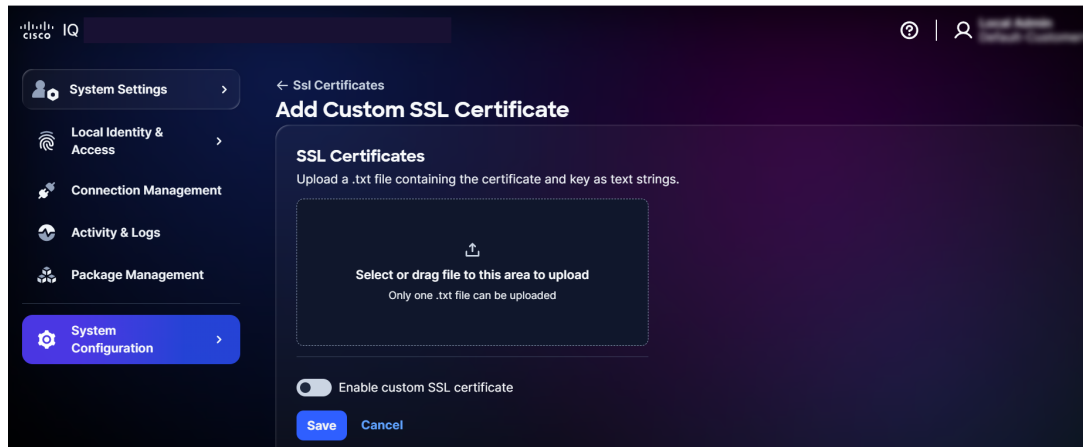


SSL-certificaat toevoegen

2. Klik op Aangepast SSL-certificaat toevoegen.

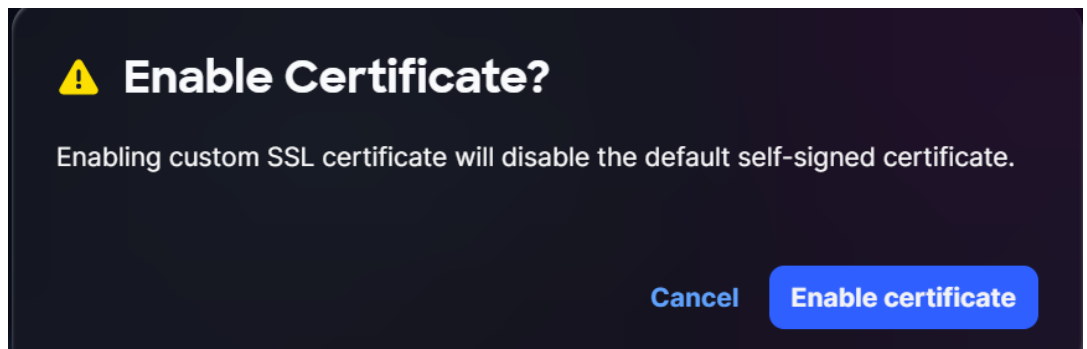


Opmerking: Upload een .txt-bestand dat zowel het Privacy-Enhanced Mail-gecodeerde certificaat als de sleutel bevat als tekstreeksen. Er kan maar één .txt bestand tegelijk worden geüpload. Het bestand moet zowel het certificaat als de privésleutel bevatten.



SSL-certificaat uploaden

3. Sleep of upload het aangepaste SSL-certificaat onder het gedeelte 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.

Aangepast SSL-certificaat 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.

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).

Aangepast SSL-certificaat 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.
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.

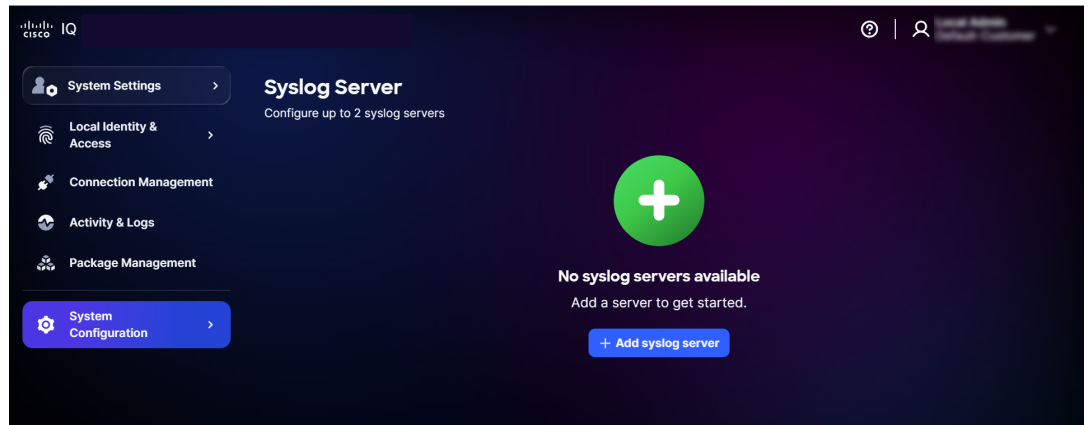


Opmerking: De Syslog-server moet worden opgegeven als een IP-adres en niet als een volledig gekwalificeerde domeinnaam (FQDN).

Syslog-server toevoegen

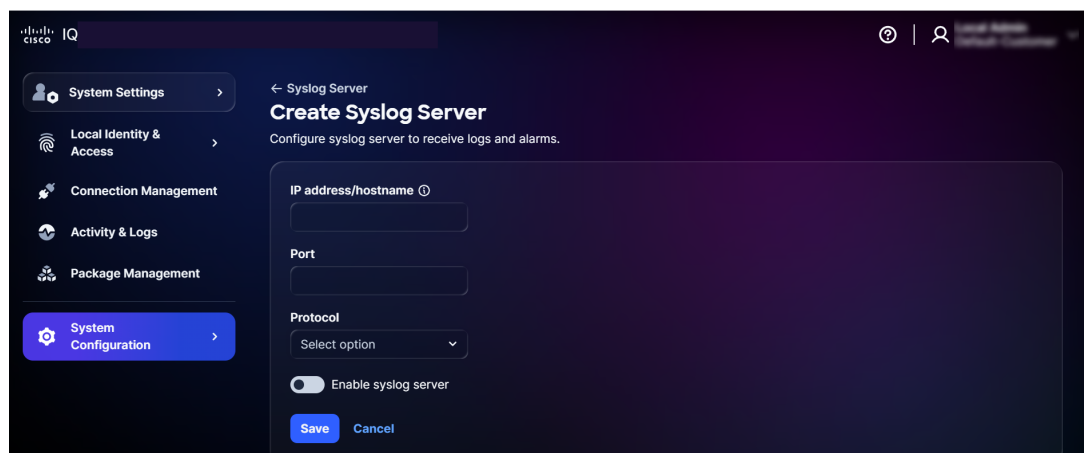
Een syslog-server toevoegen:

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 de poort in.
5. Selecteer het toepasselijke protocol in de vervolgkeuzelijst Protocol (bijvoorbeeld UDP, 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-server 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.
3. Bewerk details of schakel de schakelaar Syslog-server inschakelen uit.
4. Klik op Save (Opslaan).

Geconfigureerde SYSLOG-server 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.
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.

Event	Action	Email	User	Date and time	Activity ID	Report ID	Log level	Affected resource	Error code	Account
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Syslog ...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...
POST ...	Create	admin	Local A...	2026-0...	data_cr...	932dfd...	error	API Res...	403	unknown
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	error	Banner	404	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	API Res...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	Applica...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	User Pr...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...

Activiteit en logboeken

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

Activiteit en logboeken:

- Registreert alle API-bewerkingen op gatewayniveau
- Ondersteunt filters, paginering en zoekfuncties om u te helpen

informatie eenvoudig te vinden en te beheren

De volgende filteropties zijn beschikbaar:

- Laatste geregistreerde datum: Filters logt in een specifiek tijdsbereik
- Logniveau: logbestanden filteren op ernst (bijvoorbeeld fout, waarschuwing en informatie)
- Activiteitstype: Filterlogboeken op type systeemactiviteit
- Foutcode: Filters voor een specifieke foutcode

Banners

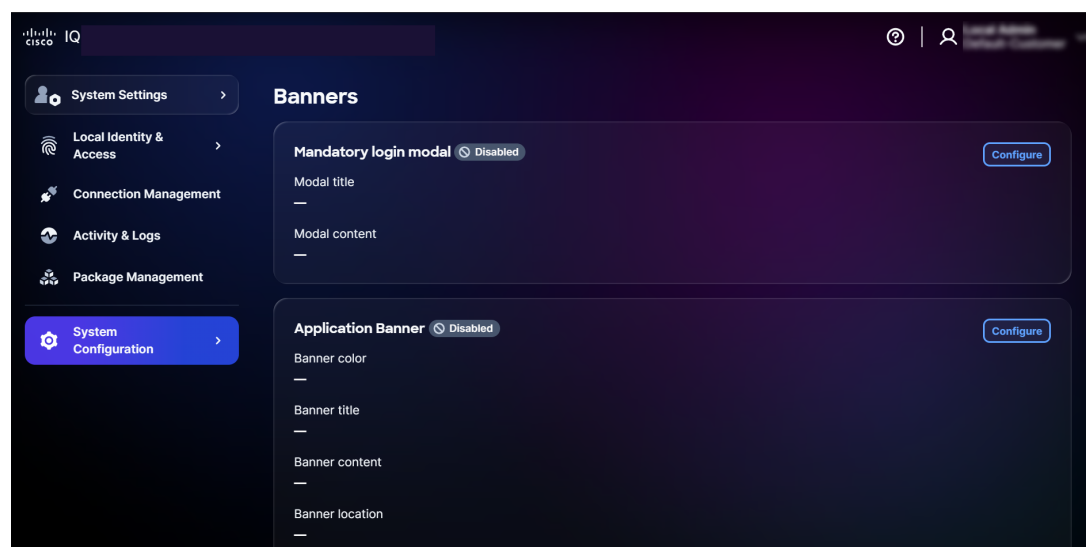
Accountbeheerders kunnen systeembrede banners configureren om te voldoen aan de beveiligings- en nalevingsnormen.

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

Verplichte aanmeldingsmodal banners configureren

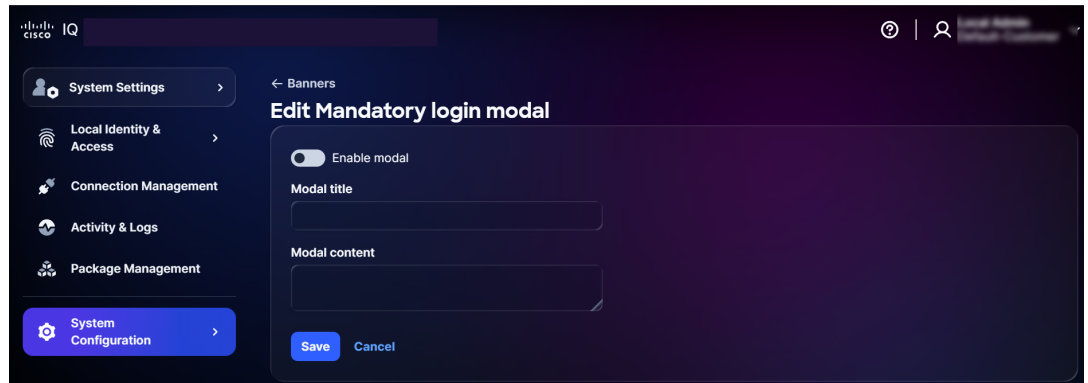
Een verplichte banner configureren:

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.



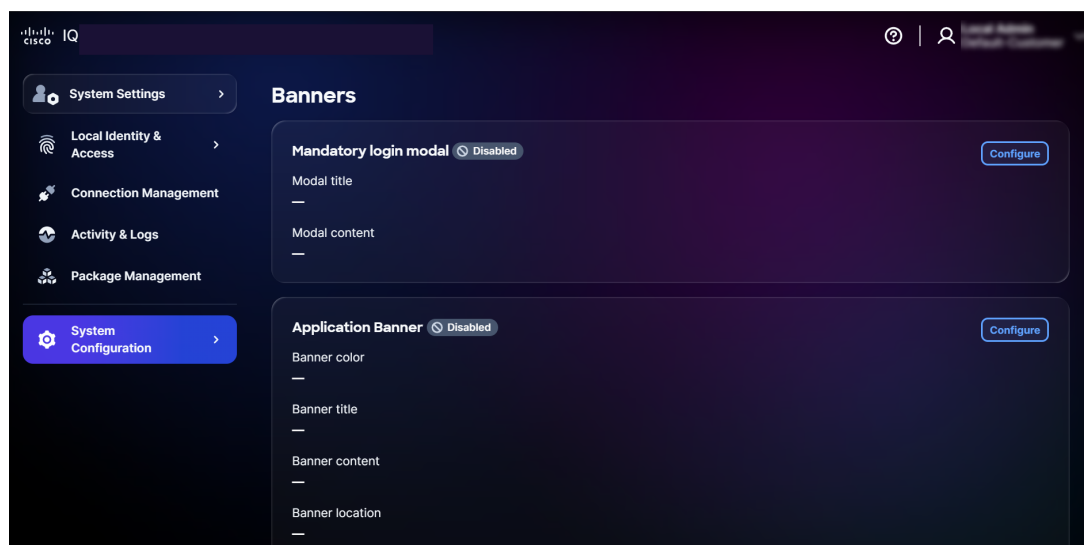
Bewerken Verplichte login modal banner

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

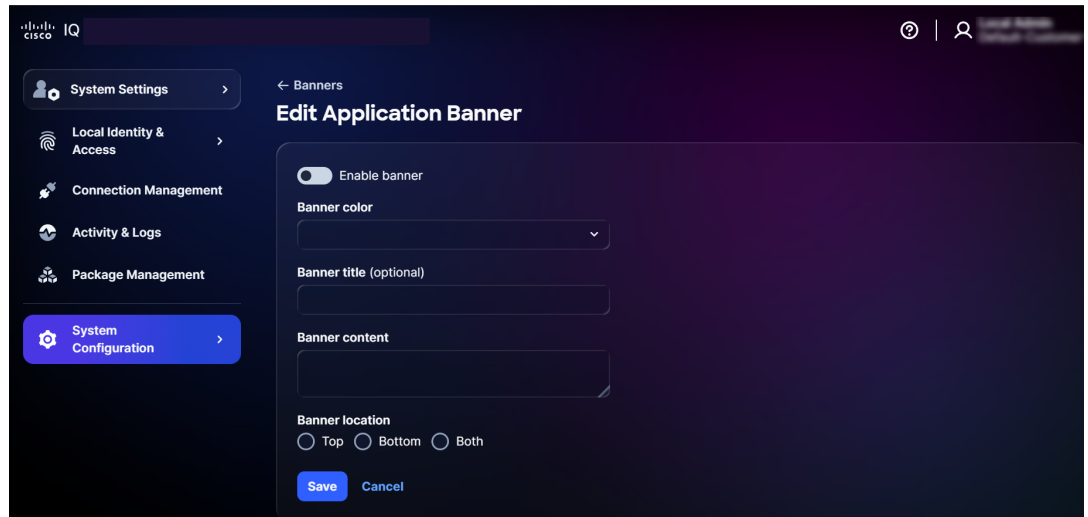
U configureert als volgt een toepassingsbanner:

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.



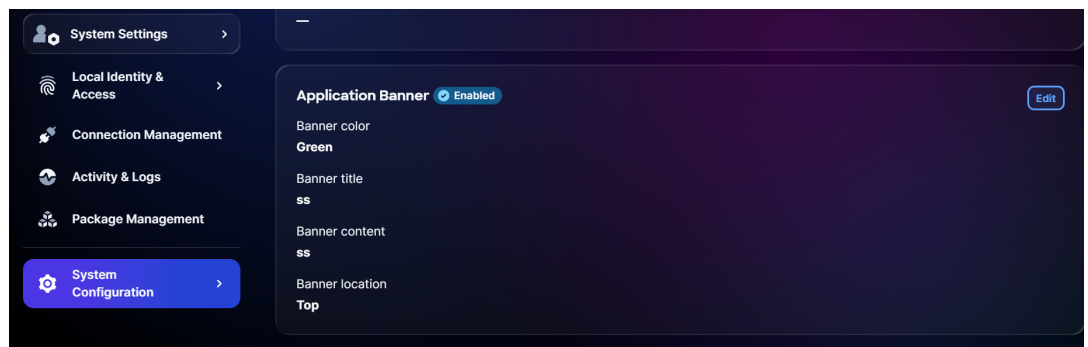
Toepassingsbanner bewerken

3. Klik op de schakelaar om de banner in of uit te schakelen.
4. Kies een bannerkleur.
5. Voer de titel van de banner in.
6. Voer de inhoud van de banner in.
7. Kies een bannerlocatie.
8. Klik op Save (Opslaan). De banner wordt weergegeven in de hele toepassing.

Banners bewerken

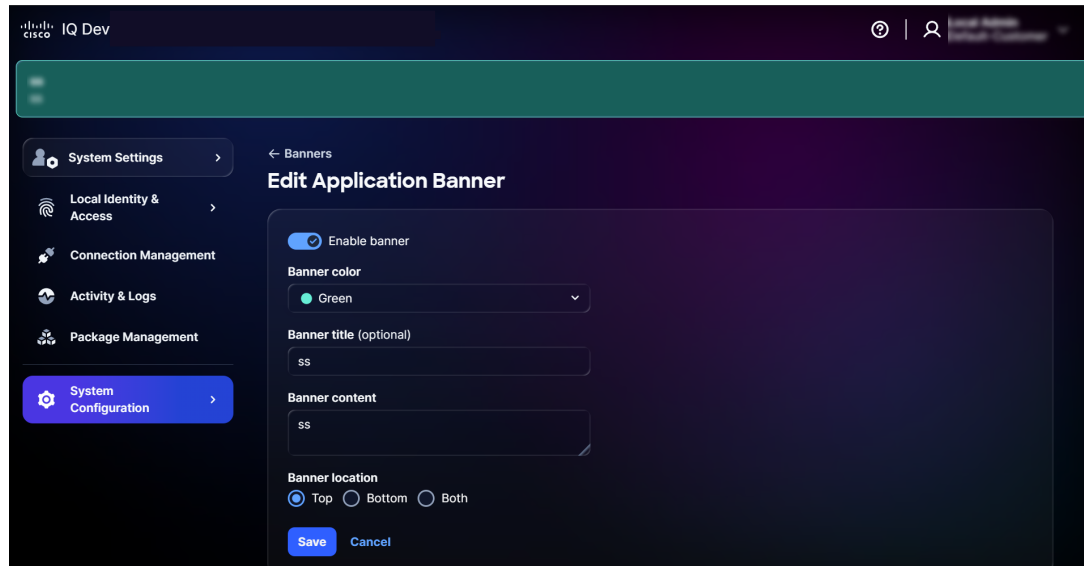
Om een banner te bewerken:

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

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.

```
CISCO IQ

Navigation Main Menu

SYSTEM STATUS
Cisco IQ On-Prem Installed

CONFIGURATION SETTINGS
IP Address/Mask
Gateway IP
DNS List
Search Domain
NTP List
Hostname

MAIN MENU
[1] Configure Network Settings DISABLED because the platform is installed
[2] Configure System Orchestrator DISABLED because the platform is installed
[3] System Diagnostics
[4] Help
[5] About
[q] Quit
```

Hoofdmenu

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

```
CISCO IQ

Navigation Main Menu > System Diagnostics

Please provide the following server connection details:

[Enter SCP/SFTP Server Address: ]
Valid IP address ✓
[Enter SCP/SFTP Server Port (e.g. 22): ]
Valid port ✓
[Enter SCP/SFTP Server Path (e.g. /var/log/support/): ]
Valid server path ✓

PROTOCOL SELECTION
[1] SCP (Secure Copy Protocol) - Default
[2] SFTP (SSH File Transfer Protocol)

[Select protocol [1]/[2] (default: SCP): 1]
scp
✓ Selected protocol: SCP
[Enter Username: ]
Valid username ✓
[Enter Password: ]

Continue with System Diagnostics? ([c]ontinue/[B]ack):
```

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.



```
Navigation Main Menu > System Diagnostics

Checking Reachability ..... ✓
Collecting System Info ..... ✓
Collecting Kubernetes Info ..... ✓
Collecting Logs ..... ✓
Preparing System Diagnostics Bundle ..... ✓
Uploading System Diagnostics Bundle ..... ✓
System Diagnostics Bundle is 'CIQ_Diagnostics_██████████.tar.gz'
System Diagnostics operation completed successfully!

Press Enter to return to main menu...█
```

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.

Ondersteuningsmodule

U kunt VA- en modulespecifieke supportcases maken van Cisco IQ SaaS. De Support-module is beschikbaar in Cisco IQ SaaS en biedt een geconsolideerd overzicht van uw supportcases. Hiermee kunt u de

weergave van de lijst met casestudy's filteren, sorteren en aanpassen, zodat u inzicht krijgt in zowel open als gesloten gevallen waartoe u toegang hebt. Zie de handleiding voor het starten van de [Cisco IQ SaaS voor](#) meer informatie over de ondersteuningsmodule in Cisco IQ SaaS.



Opmerking: klanten van Cisco IQ VA hebben toegang tot de meeste functies van de Cisco IQ SaaS Support-module, waaronder het openen van gevallen van het Technical Assistance Center (TAC) met betrekking tot Cisco IQ VA en de modules ervan, evenals het maken en beheren van productcases.

Een supportcase maken

U kunt VA- en modulespecifieke cases maken in Cisco IQ SaaS. Om een case aan te maken:

1. Meld u aan bij [Cisco IQ \(SaaS\)](#).
2. Klik op het Help-pictogram > Een probleem melden. Het venster Een probleem melden wordt geopend.

Report an Issue

Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.

Issue type

☐ Portal login issues ☐ Error message ☐ Data discrepancy ☐ Other

Issue description

Describe what happened.

The more detail you give, the faster we can help.

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel Submit

Een probleem melden

3. Verstrek de vereiste details.
4. Klik op Indienen.

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.