SSO configureren voor SD-WAN met behulp van Microsoft Entra ID

Inhoud

Inleiding

In dit document wordt beschreven hoe u Single Sign-On (SSO) configureert voor Cisco Catalyst Software-Defined Wide-Area Networks (SD-WAN) met Microsoft Entra ID.

Voorwaarden

Vereisten

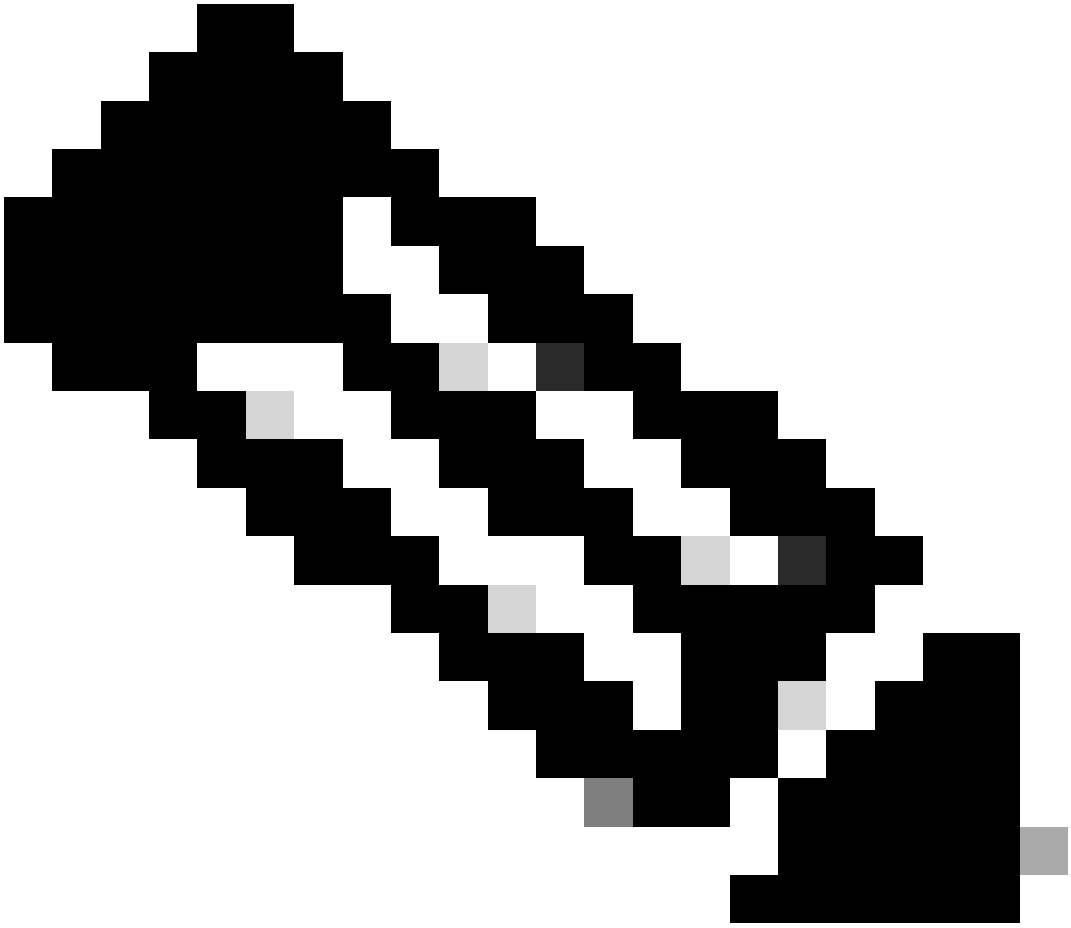
Cisco raadt u aan om algemene kennis te hebben van de volgende onderwerpen:

- eenmalige aanmelding
- Cisco Catalyst SD-WAN-oplossing

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Cisco Catalyst SD-WAN Manager release 20.15.3.1
- Microsoft Entra ID



Opmerking: De oplossing die voorheen bekend stond als Azure Active Directory (Azure AD) wordt nu Microsoft Entra ID genoemd.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Single Sign-On is een verificatiemethode waarmee gebruikers veilig toegang hebben tot meerdere onafhankelijke toepassingen of websites met behulp van één set referenties. Met SSO hoeven gebruikers zich niet langer afzonderlijk aan te melden bij elke toepassing: zodra ze zijn geverifieerd, hebben ze naadloos toegang tot alle toegestane bronnen.

Een veel voorkomende manier om SSO te implementeren is door middel van federatie, die vertrouwen tussen een identiteitsprovider (IdP) en een serviceprovider (SP) vestigt met behulp

van protocollen zoals SAML 2.0, WS-Federation of OpenID Connect. Federation verbetert de veiligheid, betrouwbaarheid en gebruikerservaring door authenticatie te centraliseren.

Microsoft Entra ID is een veelgebruikte cloudgebaseerde identiteitsprovider die deze federatieprotocollen ondersteunt. In een SSO-installatie met Cisco Catalyst SD-WAN fungeert Microsoft Entra ID als de IdP en treedt Cisco SD-WAN Manager op als de serviceprovider.

De integratie werkt als volgt:

1. Een netwerkbeheerder probeert zich aan te melden bij Cisco SD-WAN Manager.
2. Cisco SD-WAN Manager stuurt een verificatieverzoek naar Microsoft Entra ID.
3. Microsoft Entra ID vraagt de beheerder om zich te verifiëren met hun Entra ID (Microsoft)-account.
4. Zodra de referenties zijn gevalideerd, stuurt Microsoft Entra ID een veilig antwoord terug naar de Cisco SD-WAN Manager om de verificatie te bevestigen.
5. Cisco SD-WAN Manager verleent toegang zonder dat hiervoor aparte referenties nodig zijn.

In dit model:

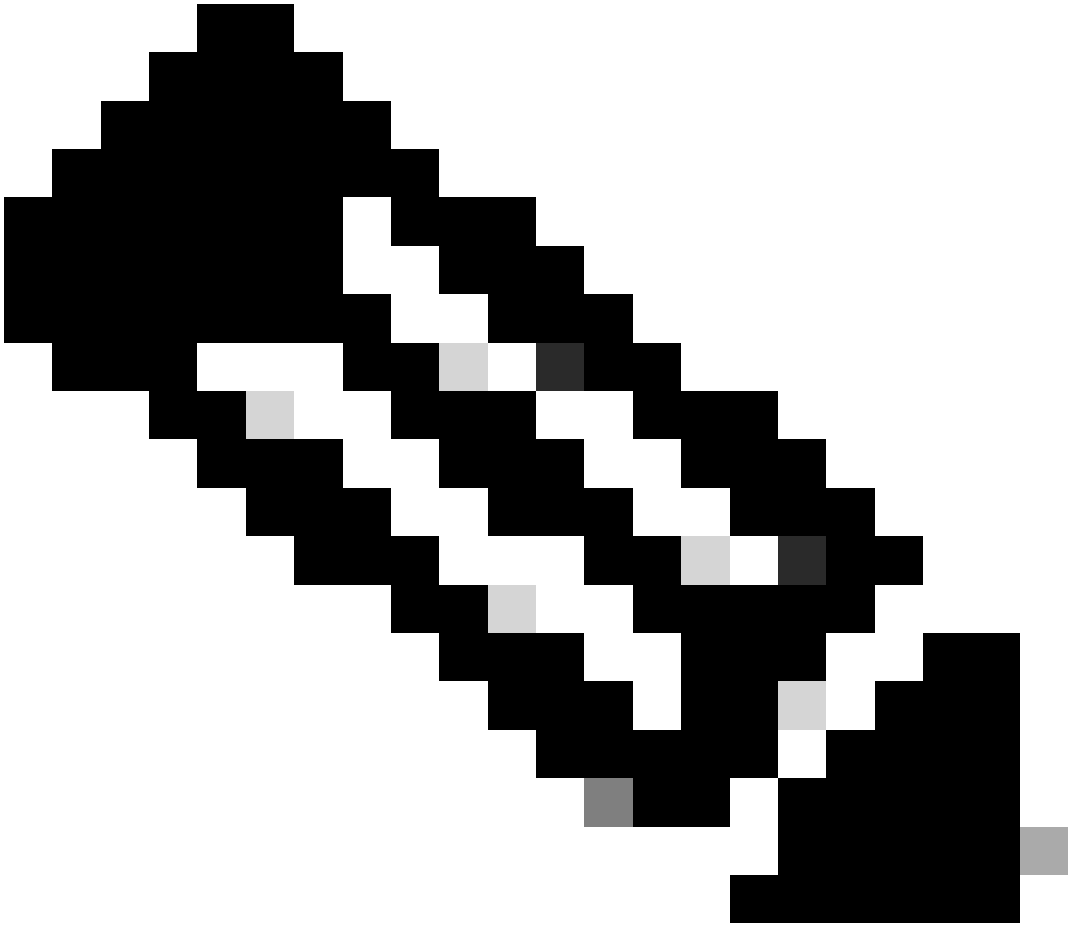
- Identity Provider (IdP) – slaat gebruikersgegevens op, valideert referenties (bijvoorbeeld Microsoft Entra ID, Okta, PingID, ADFS).
- Serviceleverancier – host de toepassing die moet worden geopend (bijvoorbeeld Cisco SD-WAN Manager).
- Gebruikers – hebben een account in de IdP-directory en zijn bevoegd om toegang te krijgen tot de serviceprovider.

Cisco Catalyst SD-WAN is compatibel met elke SAML 2.0-compatibele IdP wanneer deze is geconfigureerd volgens industriestandaarden.

Voordelen van Single Sign-On

- Centraliseert het beheer van referenties via de Identity Provider.
- Versterkt de authenticatiebeveiliging door meerdere zwakke wachtwoorden te elimineren.
- Stroomlijnt veilige toegang voor beheerders.
- Hiermee kunt u met één klik toegang krijgen tot Cisco Catalyst SD-WAN Manager en andere geautoriseerde toepassingen.

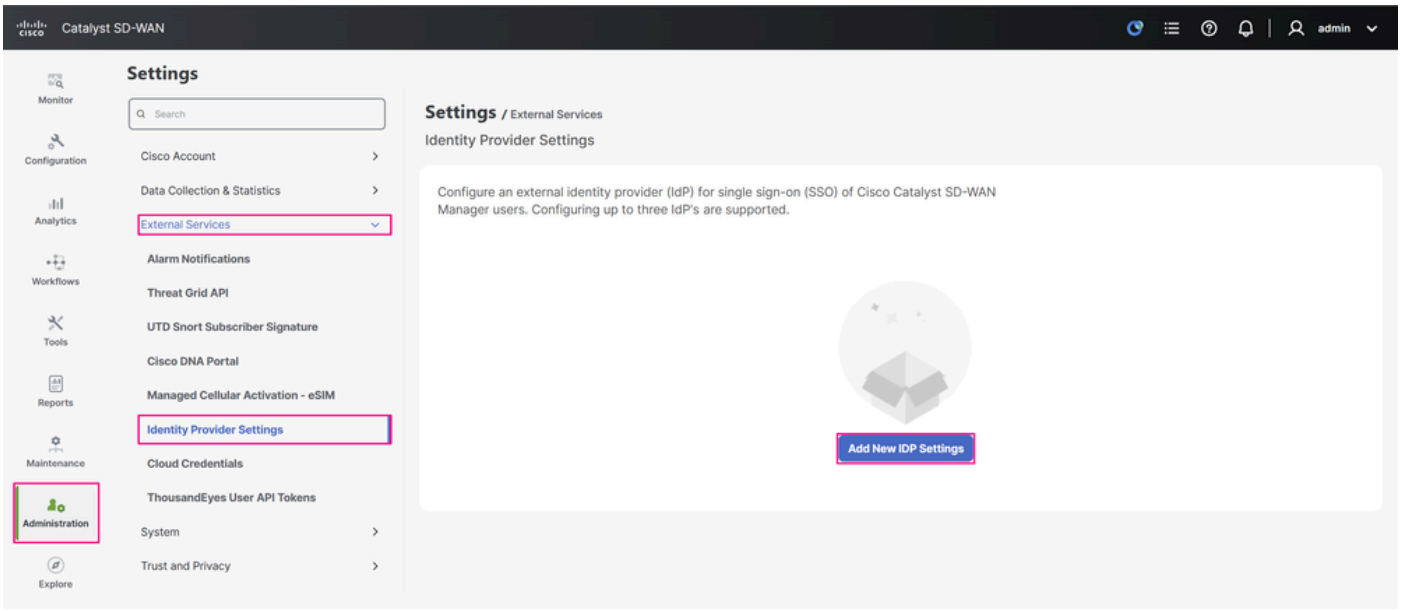
Configureren



Opmerking: Minimale ondersteunde versie: Cisco Catalyst SD-WAN Manager versie 20.8.1.

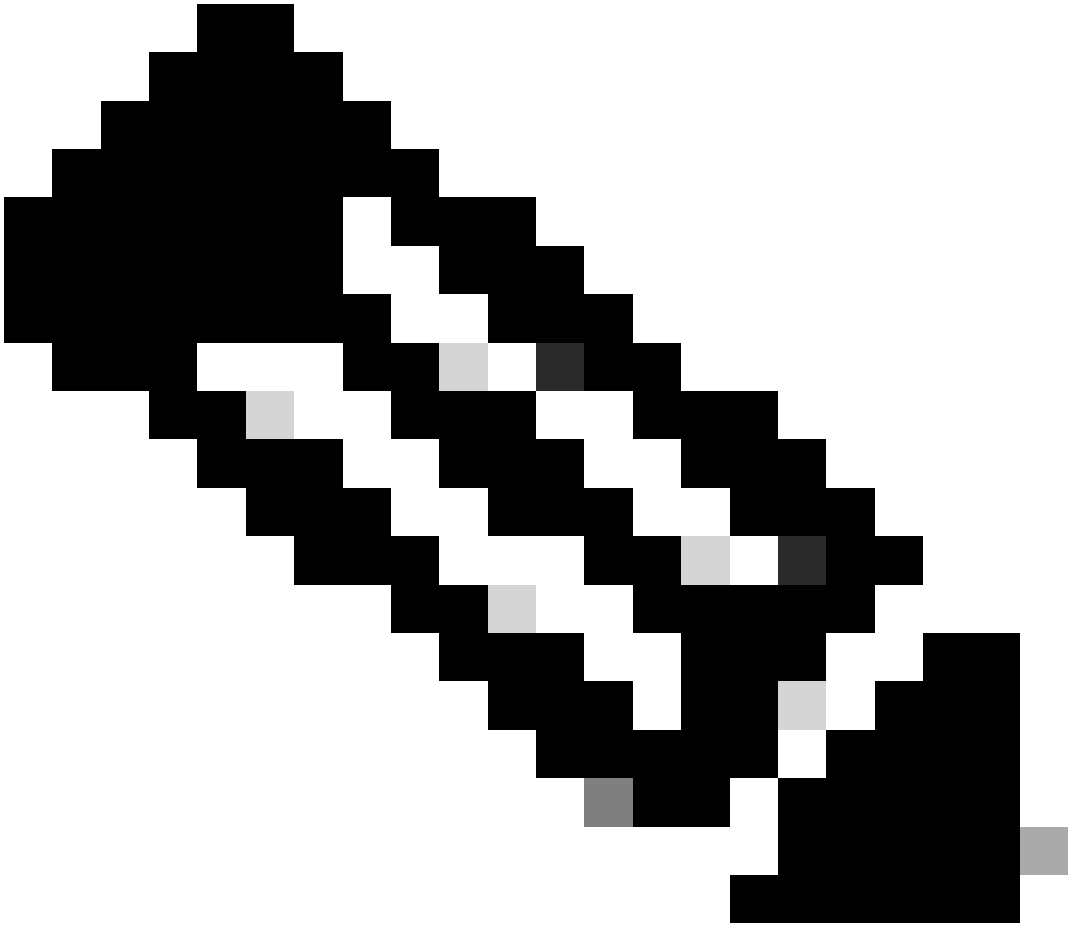
Stap 1. De Cisco SD-WAN Manager SAML-metagegevens verkrijgen

- Navigeer in Cisco SD-WAN Manager naar Beheer > Instellingen > Externe services > Instellingen van identiteitsprovider en klik op Nieuwe IDP-instellingen toevoegen.



Cisco SD-WAN Manager UI

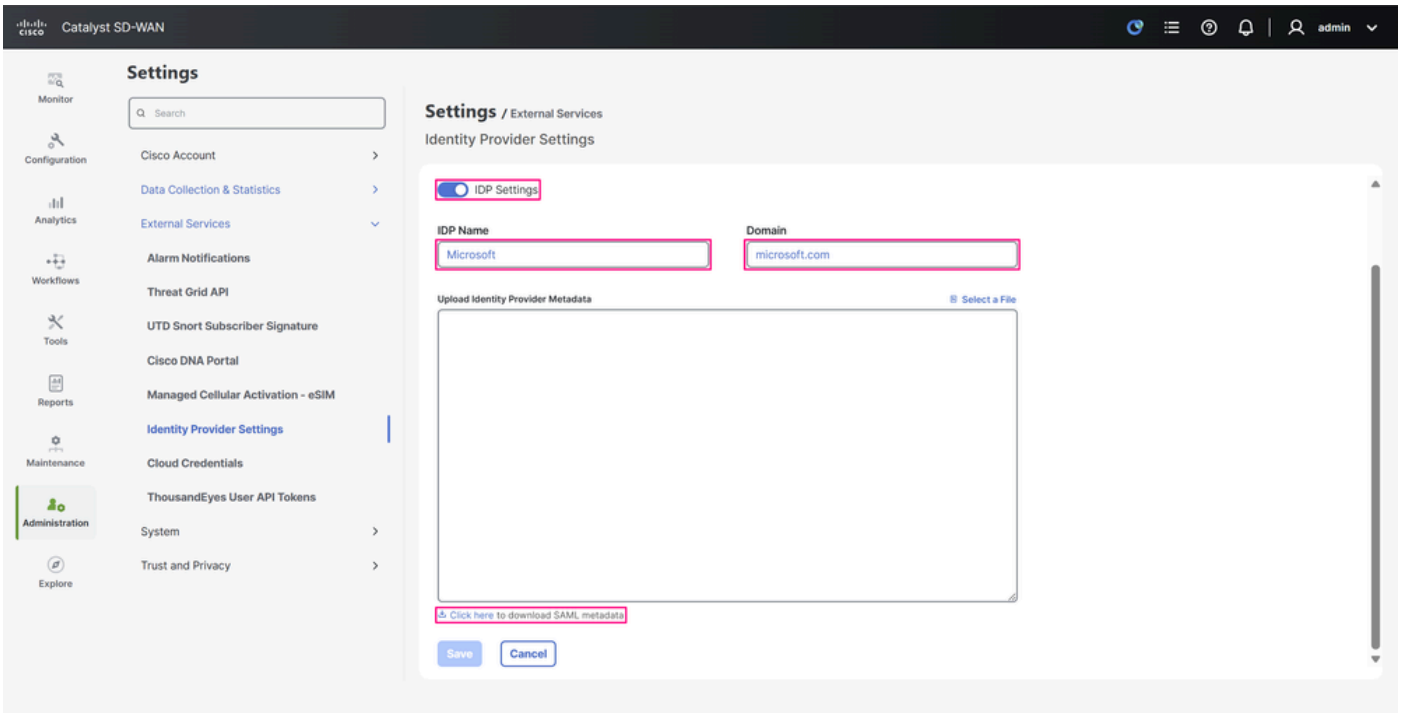
- Schakel IDP-instellingen in om de instellingen van de identiteitsprovider in te schakelen. Voer in het veld IDP-naam een naam in die verwijst naar de IdP die u gebruikt en voer in het veld Domein een domein in dat overeenkomt met de domeinnamen die door de gebruikers in de bedrijfstoepassing van uw organisatie worden gebruikt. Klik hier om de SAML-metagegevens te downloaden en het XML-bestand met metagegevens op uw computer op te slaan. Dit bestand wordt gebruikt om SSO in Microsoft Entra ID in de volgende stap te configureren.



Opmerking: in dit voorbeeld verwijst het XML-bestand met metagegevens rechtstreeks naar het IP-adres van de Cisco SD-WAN-manager, maar in veel productieomgevingen verwijst het naar de volledig gekwalificeerde domeinnaam (FQDN). Voor een standalone Cisco SD-WAN Manager komt de Entity ID in de metagegevens overeen met de URL die u gebruikt om in te loggen bij de Cisco SD-WAN Manager op het moment dat u deze downloadt. Dit betekent dat het werkt met ofwel het IP-adres of de FQDN, omdat het een single-node setup.

Voor een Cisco SD-WAN Manager-cluster geldt hetzelfde principe: de FQDN wijst naar een van de clusternodes en de metagegevens bevatten dit domein als de Entity ID. Het verschil is dat, of u nu metadata gebruikt met de FQDN van het cluster of van een specifieke node met behulp van het IP-adres, zodra de SSO-integratie met Microsoft Entra ID met succes is voltooid, de andere knooppunten ook doorverwijzen naar de IdP-aanmeldingsprompt.

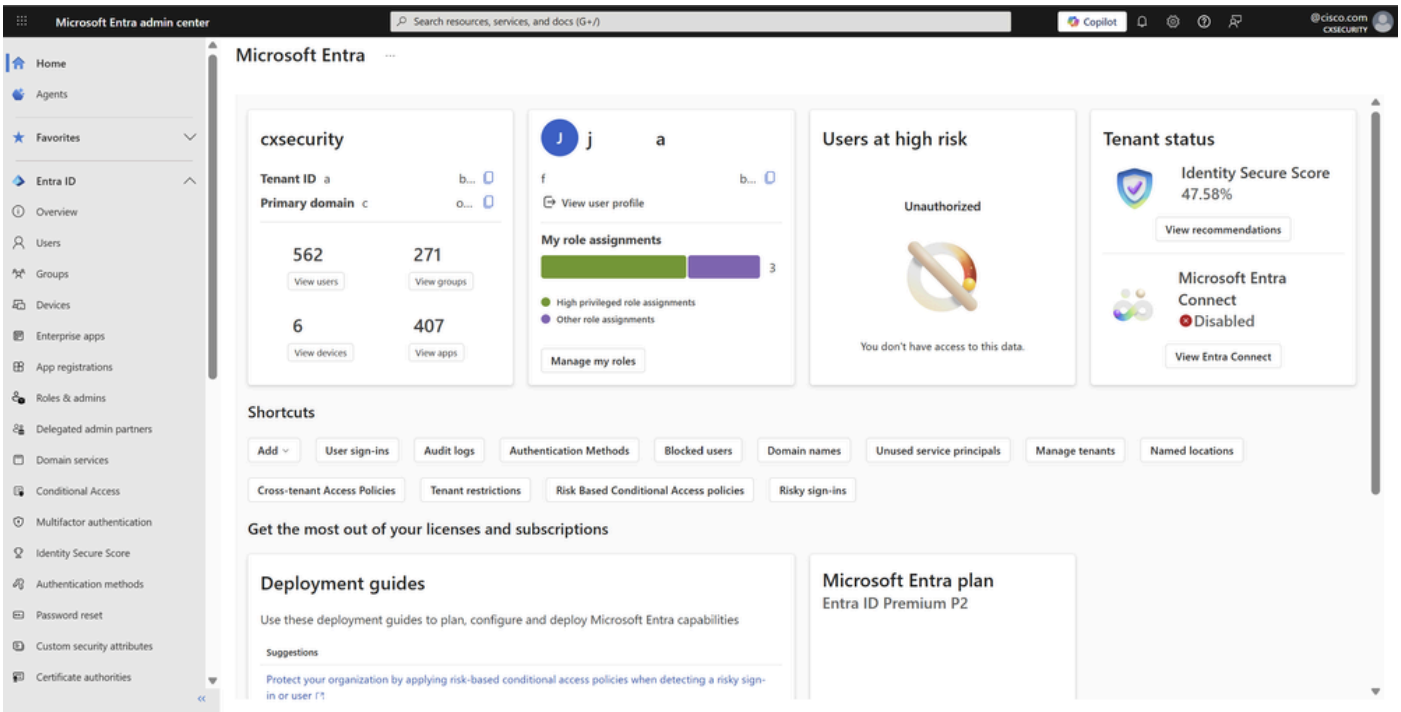
De belangrijkste vereiste in beide scenario's is dat de Entity ID die u gebruikt in Cisco SD-WAN Manager, of het nu gaat om een IP-adres of een FQDN, overeenkomt met de ID die aan de IdP-zijde is geconfigureerd.



Configuratiepagina IDp-instellingen

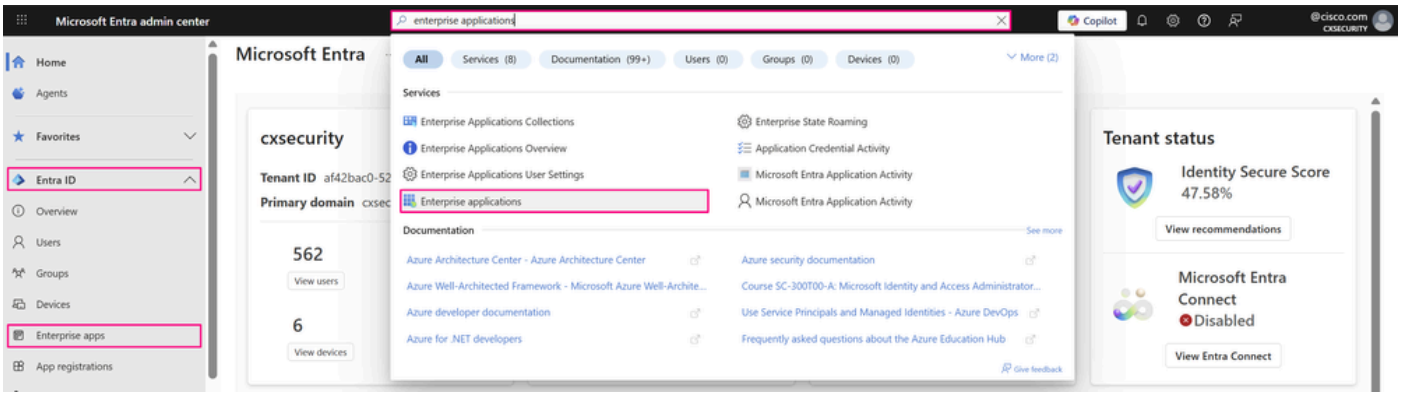
Stap 2. Een bedrijfstoepassing configureren voor SSO in Microsoft Entra ID

- Meld u aan bij het Microsoft Entra-beheerderscentrum met een van deze rollen: cloudtoepassingsbeheerder, toepassingsbeheerder of eigenaar van de hoofdservice.



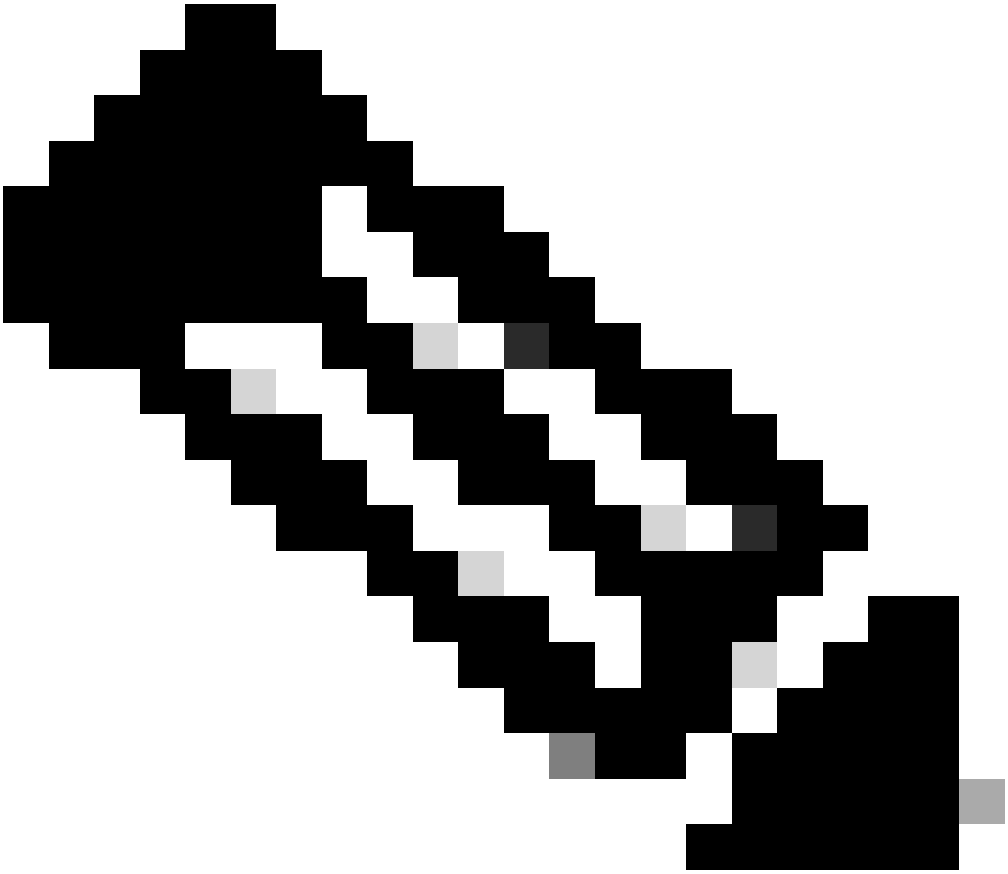
Microsoft Entra Admin Center Portal

- Navigeer naar Entra ID > Enterprise-apps, of u hebt ook toegang tot deze service wanneer u bedrijfstoepassingen invoert in de zoekbalk boven aan het portaal en kiest vervolgens Enterprise-toepassingen.

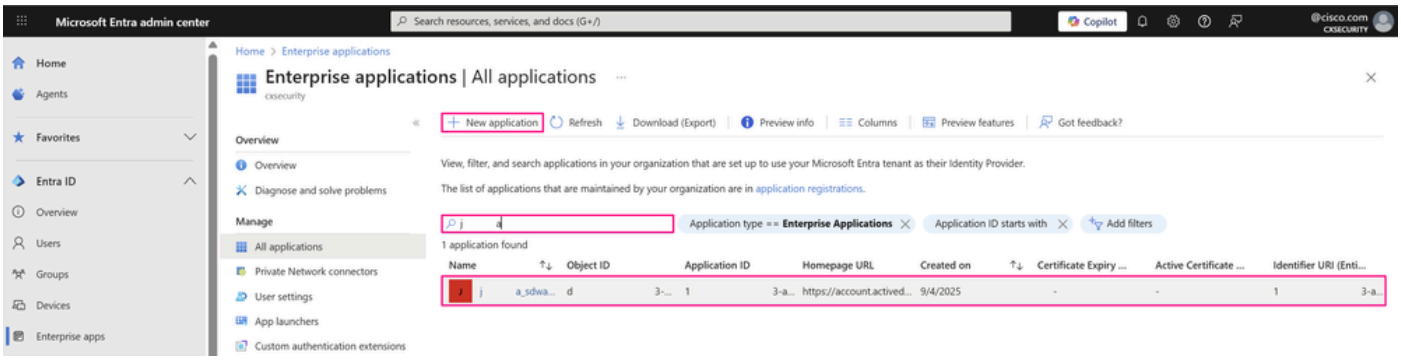


Microsoft Entra Admin Center Portal

- De pagina Alle toepassingen wordt geopend. Voer de naam van uw bestaande toepassing in het zoekvak in en kies vervolgens de toepassing uit de zoekresultaten.

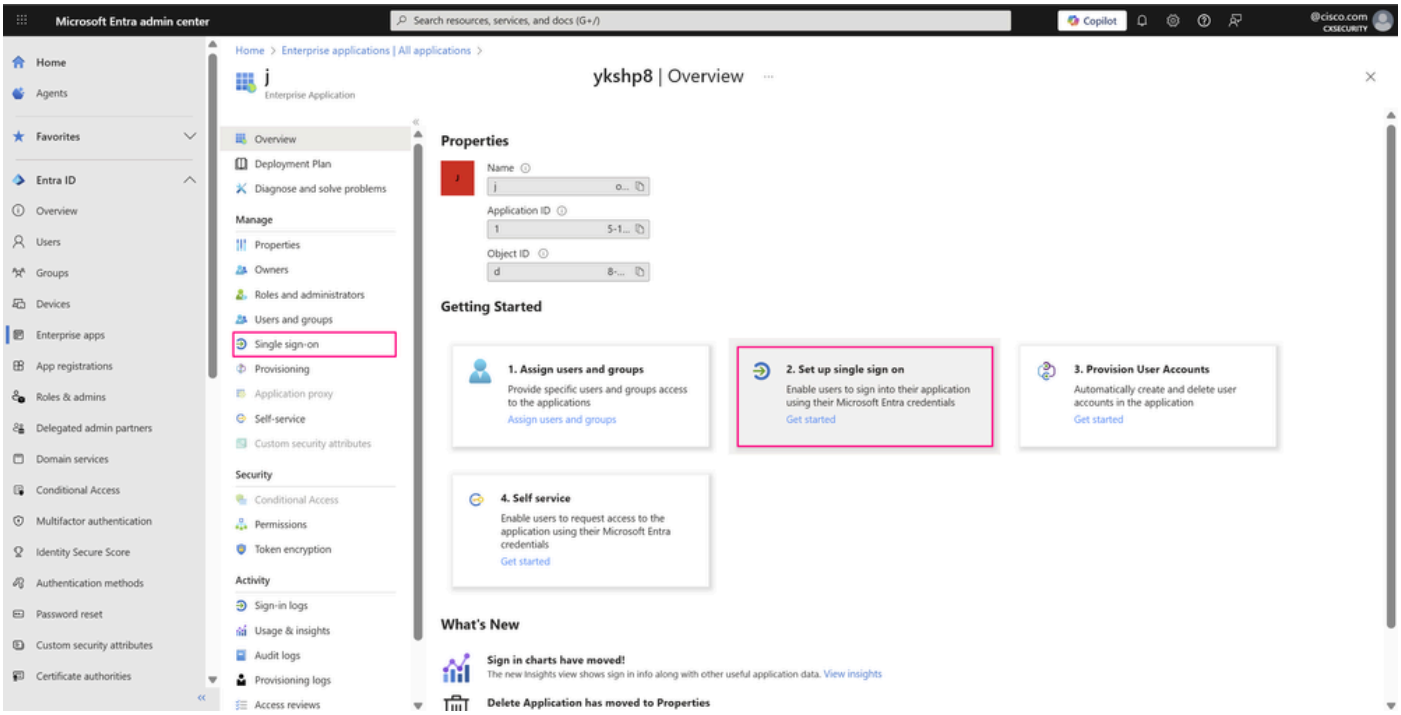


Opmerking: op dezelfde pagina kunt u een aangepaste bedrijfstoepassing maken op basis van de vereisten van uw organisatie en deze configureren met SSO-verificatie als u dat nog niet hebt, wanneer u op Nieuwe toepassing klikt.



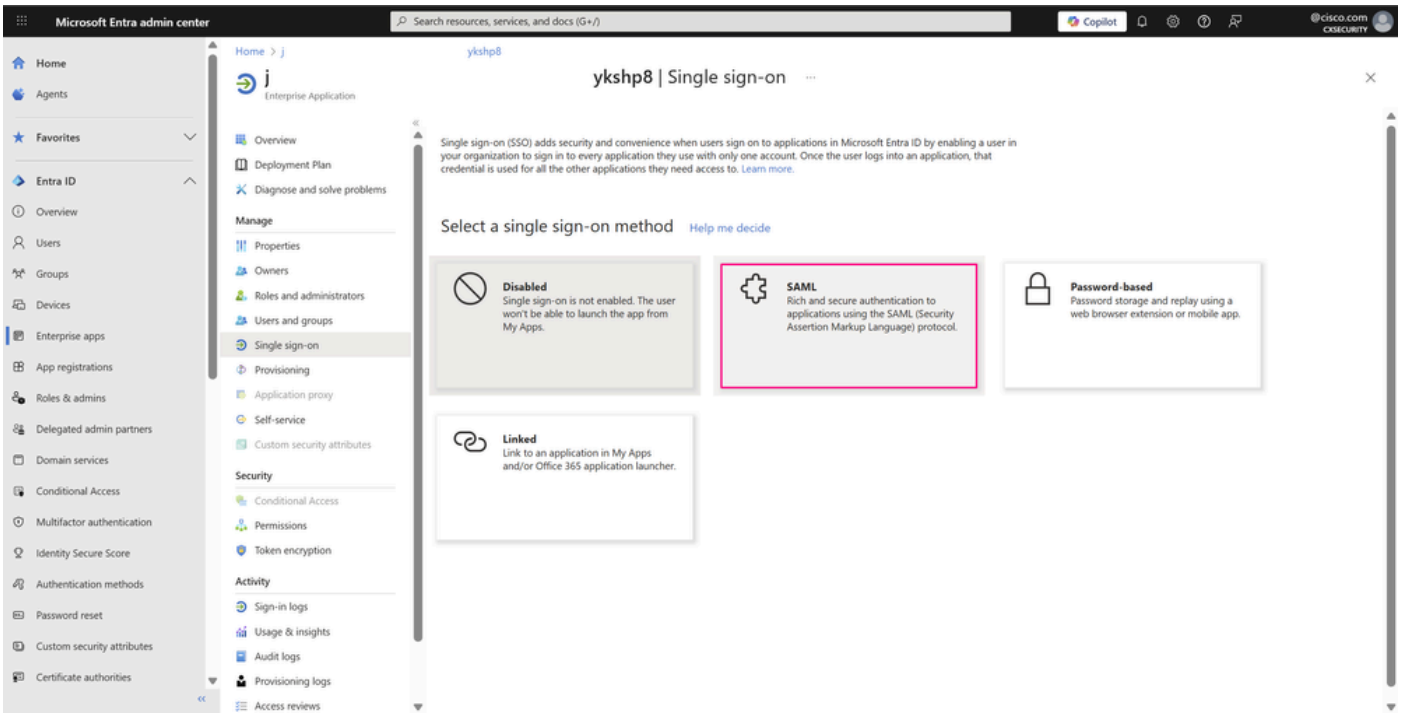
Dashboard voor bedrijfstoepassingen

- Klik in het gedeelte Beheren van het linkermenu op Eenmalige aanmelding, of klik in het deelvenster Aan de slag in het gedeelte Overzicht op 2. Stel een eenmalige aanmelding in om het deelvenster Eenmalige aanmelding te openen voor bewerking.



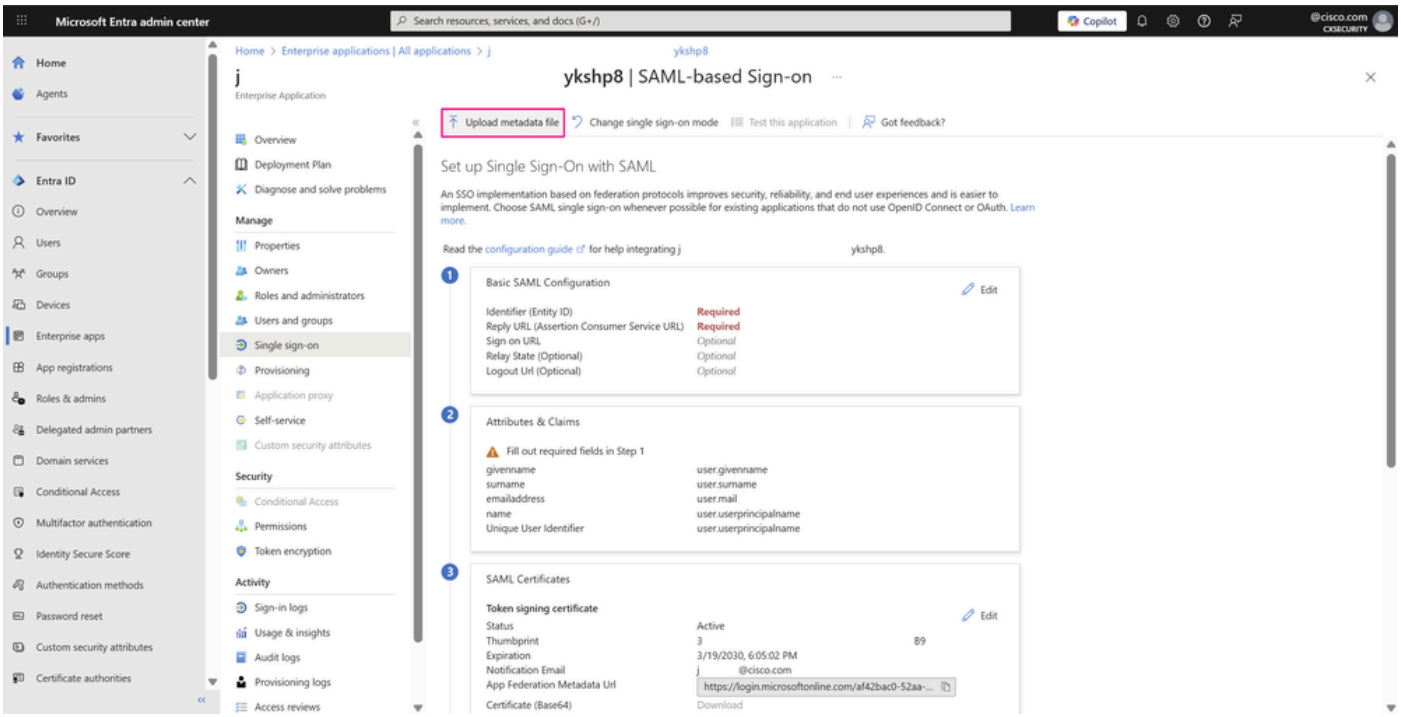
Overzicht van bedrijfstoepassingen

- Selecteer SAML om de configuratiepagina voor eenmalige aanmelding te openen.



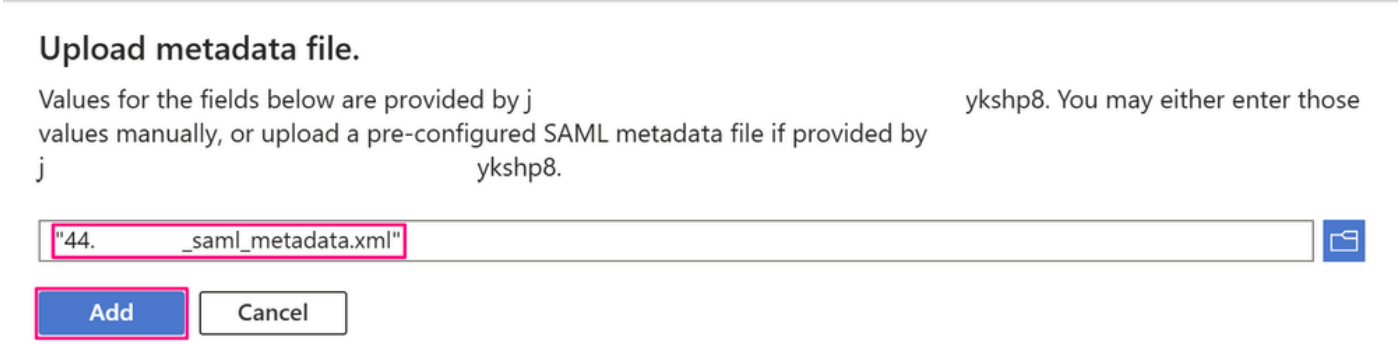
aanmeldingsvenster

- Klik op de pagina Eenmalige aanmelding met SAML instellen op Metagegevensbestand uploaden.



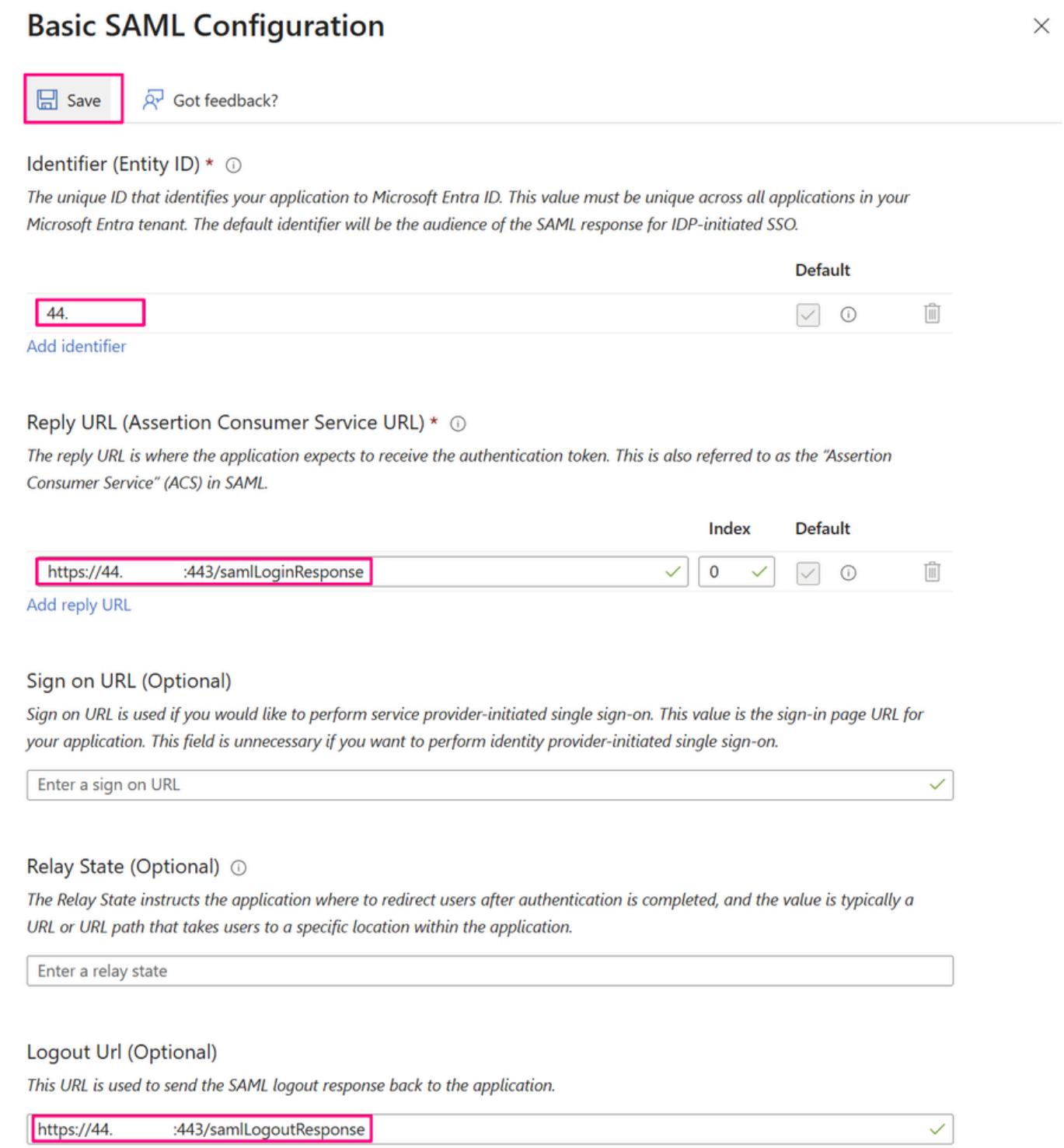
SSO met SAML-configuratiepagina

- Blader in het venster Metagegevensbestand uploaden naar het XML-bestand met metagegevens dat u eerder hebt gedownload en klik op Toevoegen.



Venster Metagegevensbestand uploaden

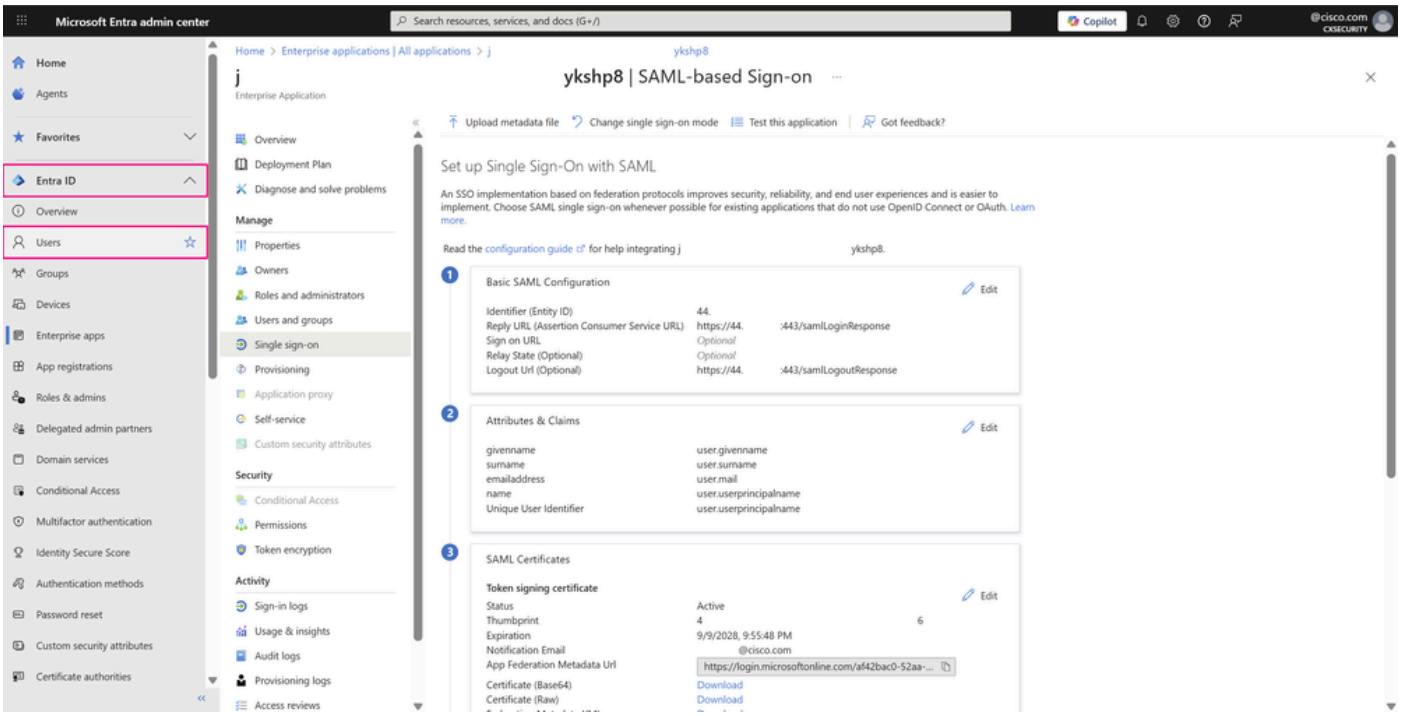
- In het venster Basic SAML Configuration is de ID (Entity ID) meestal de URL die specifiek is voor de toepassing, in dit geval de Cisco SD-WAN Manager, waarmee u integreert (zoals uitgelegd in de vorige stap). De waarden voor de URL voor antwoorden en de URL voor afmelden worden automatisch ingevuld zodra het bestand is geüpload. Klik op Opslaan om door te gaan.



Basisvenster SAML-configuratie

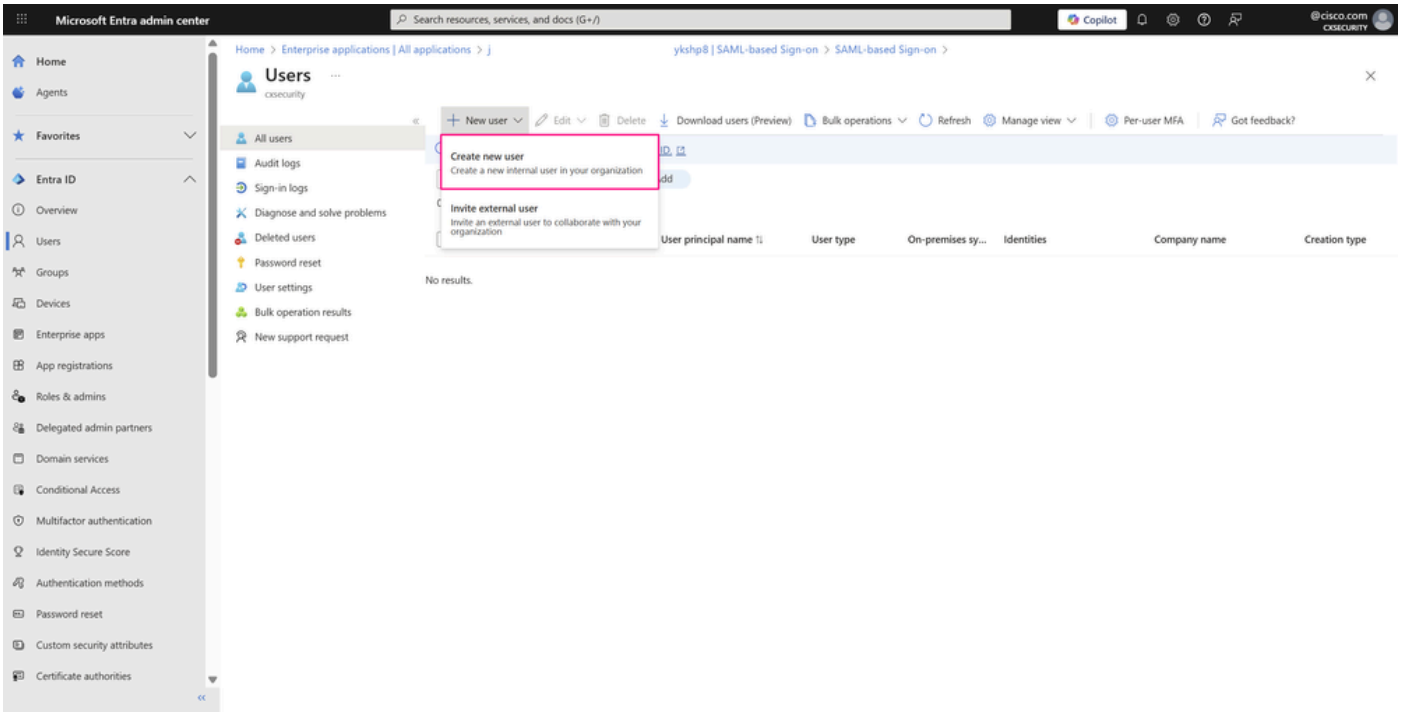
Stap 3. Een gebruikers- of groepsaccount toevoegen aan de Enterprise-toepassing

- Als de SAML-configuratieparameters van de toepassing zijn gedefinieerd, gaat u verder met het toevoegen van de gebruikers of groepen in de bedrijfstoepassing die zich aanmelden bij de toepassing. Navigeer hiervoor eerst naar Entra ID > Gebruikers, of u kunt deze service ook gebruiken wanneer u de servicenaam zoekt in de zoekbalk boven in het portaal, zoals in een vorige stap wordt weergegeven.



SSO met SAML-configuratiepagina

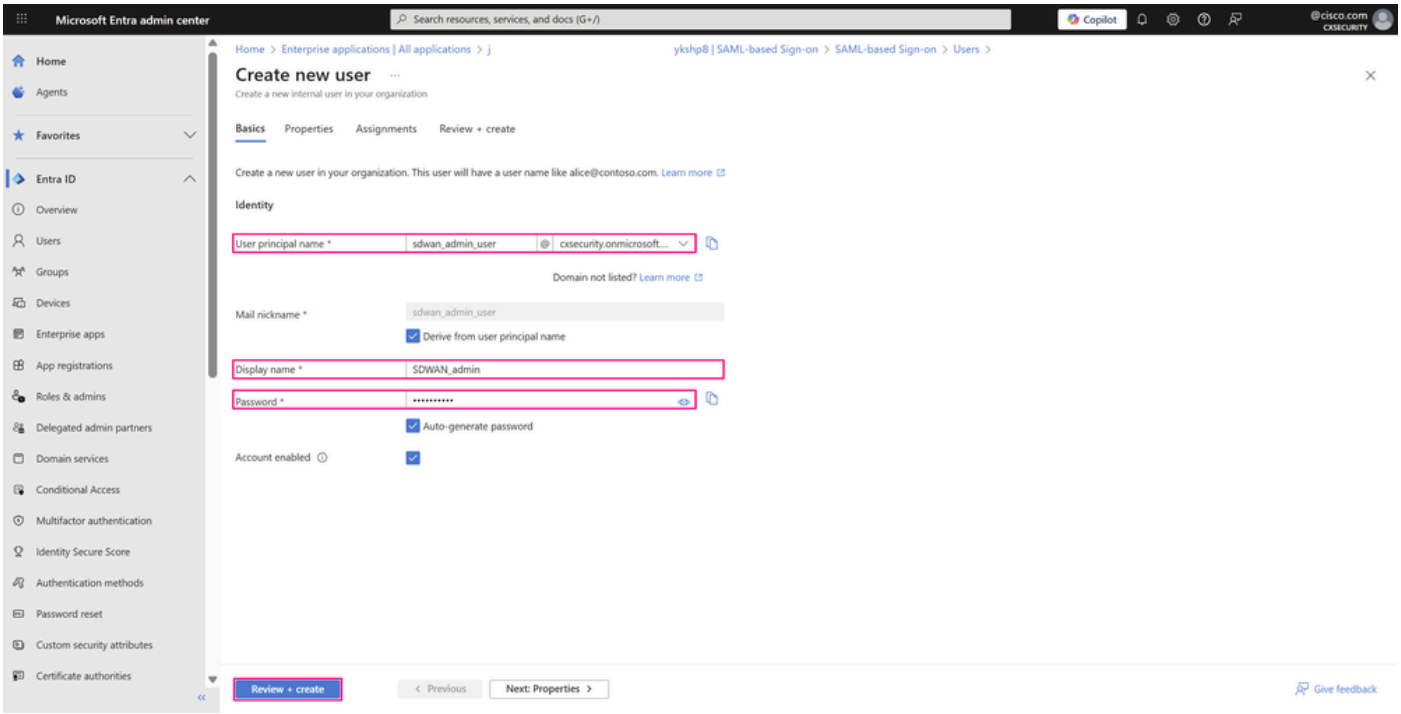
- Maak een gebruiker die u associeert met een groep om SSO-verificatie te illustreren met Cisco SD-WAN Manager en een van de gebruikersgroepen, netadmin, die het meest voorkomt in productieomgevingen. Om dit te doen, navigeert u naar Entra ID > Gebruikers. Klik vervolgens op Nieuwe gebruiker en kies Nieuwe gebruiker maken.



gebruikersdashboard

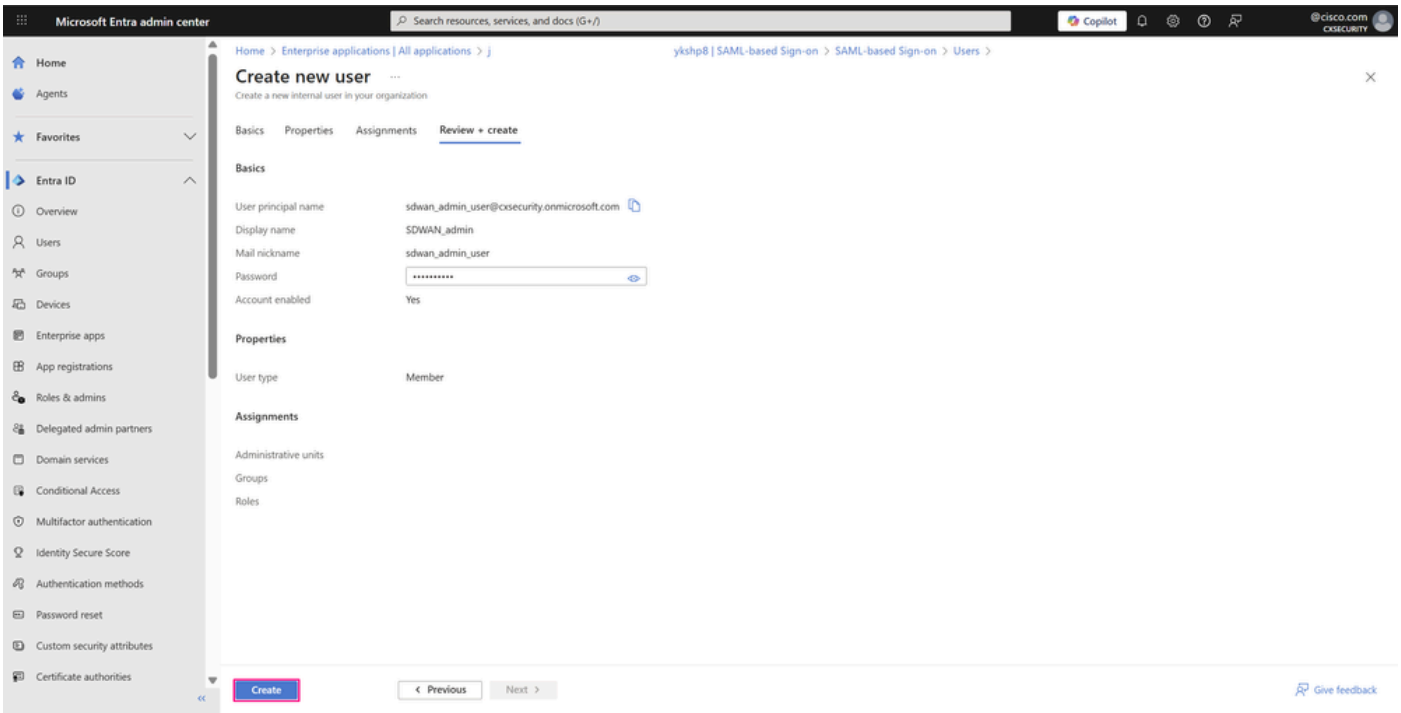
- Het tabblad Basisprincipes bevat de kernvelden die nodig zijn om een nieuwe gebruiker te maken.
  - Voer voor de hoofdnaam van de gebruiker een unieke gebruikersnaam in en kies een domein in de vervolgkeuzelijst met domeinen die beschikbaar zijn in uw organisatie.

- Voer een weergavenaam voor de gebruiker in.
- Schakel het selectievakje Wachtwoord automatisch genereren uit als u een aangepast wachtwoord wilt invoeren of schakel deze optie in zodat het automatisch wordt gegenereerd.
- U kunt de gebruiker toevoegen aan een groep op het tabblad Toewijzingen, maar omdat het groepslidmaatschap nog niet is gemaakt, klikt u op Bekijken + maken.



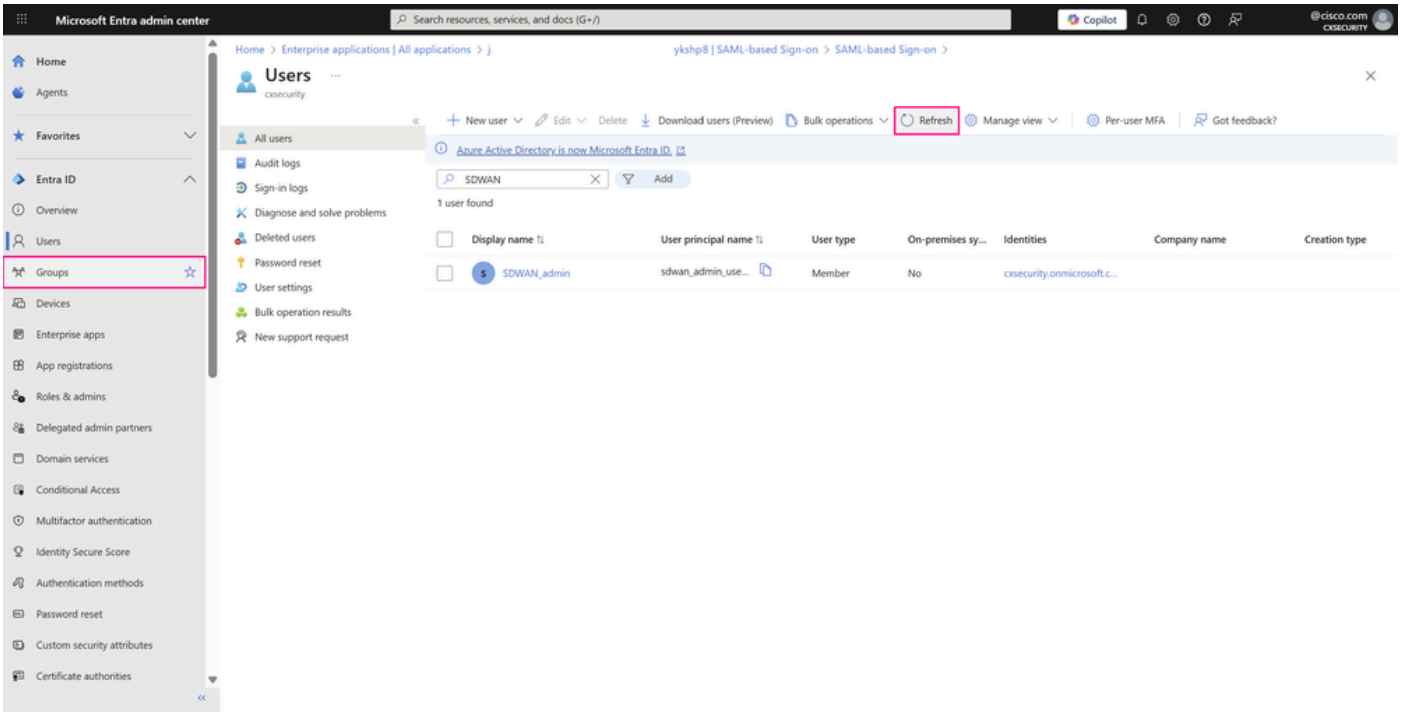
Pagina voor het maken van gebruikers

- Het laatste tabblad toont de belangrijkste details van de werkstroom voor het maken van gebruikers. Bekijk de details en klik op Aanmaken om het proces te voltooien.



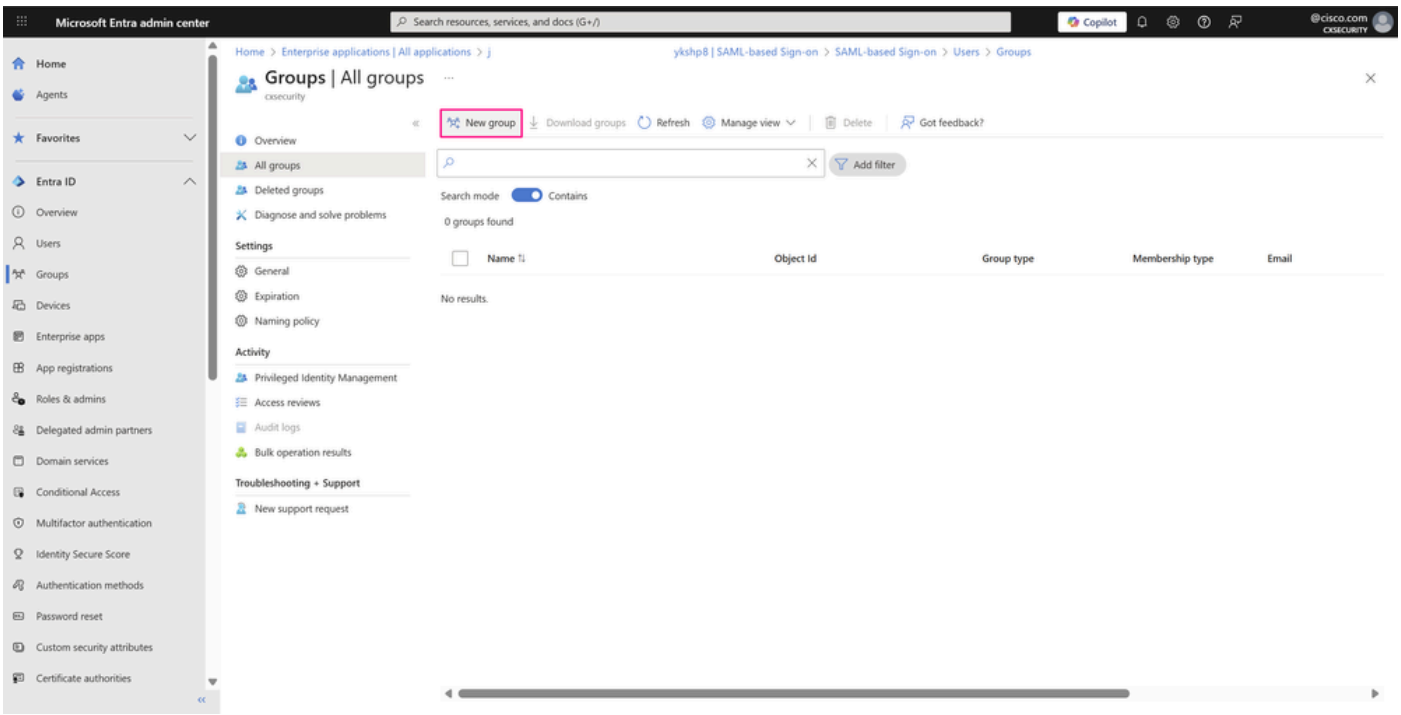
Pagina voor het maken van gebruikers

- De nieuwe gebruiker verschijnt kort daarna. Als dit niet het geval is, klikt u op Vernieuwen en zoekt u de gebruiker met de zoekbalk in de service. Navigeer vervolgens naar Invoeren > Groepen > Alle groepen om de nieuwe groep te maken.



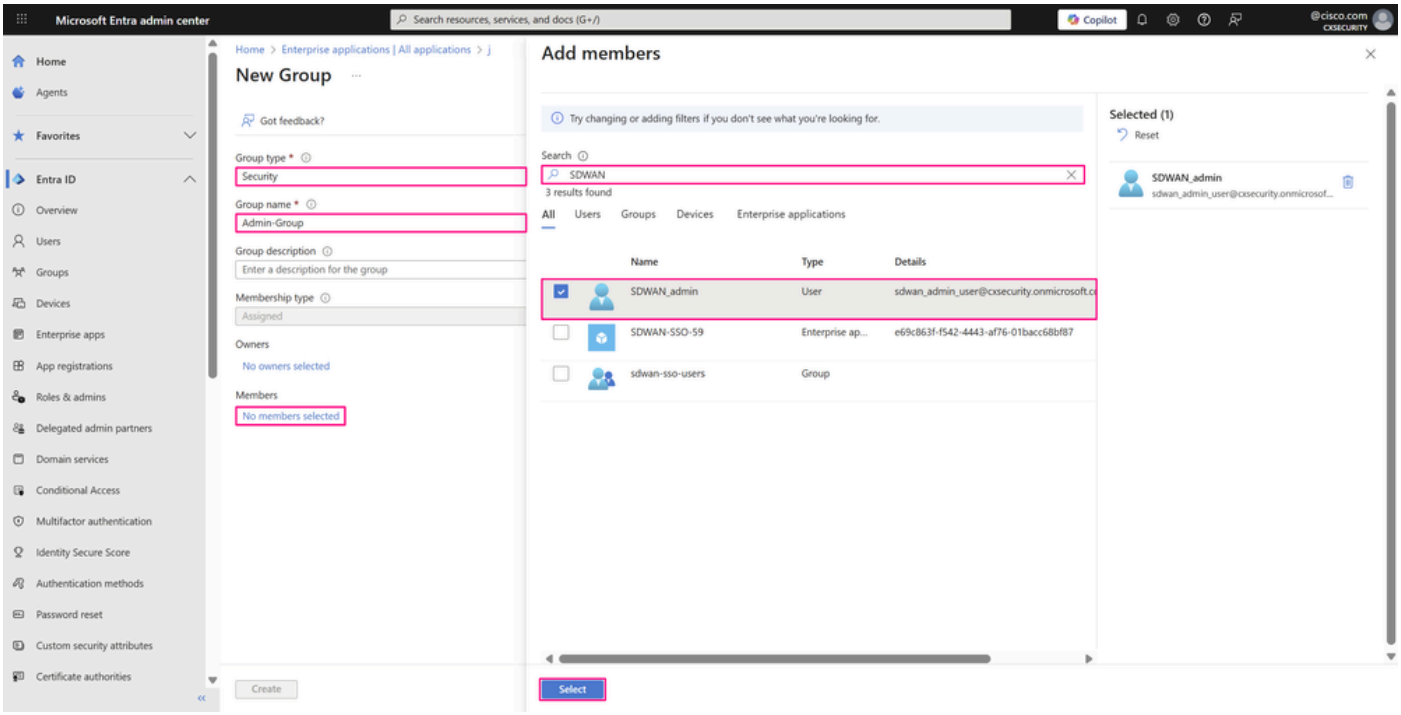
gebruikersdashboard

- Op deze pagina beheert u de verschillende groepen en hun machtigingen binnen uw organisatie. Klik op Nieuwe groep om de groep aan te maken met netwerkbeheerdersbevoegdheden.



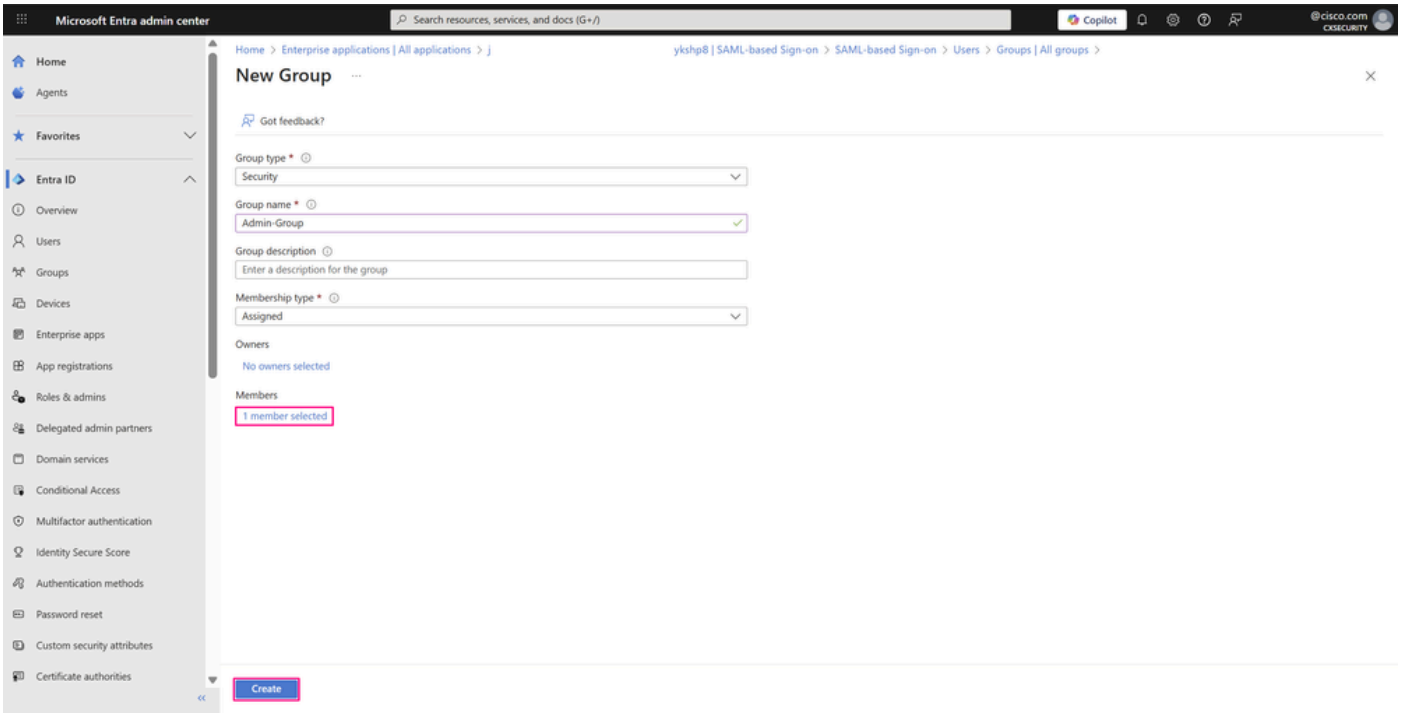
Pagina Alle groepen

- Kies een groepstype in de vervolgkeuzelijst - in dit geval Beveiliging, omdat alleen toegang tot gedeelde bronnen vereist is. Voer een groepsnaam van uw keuze in die verwijst naar de rol of machtigingen van de groep. Koppel gebruikers nu aan de groep wanneer u op de geselecteerde leden klikt in het veld Leden.
    - Blader in het venster Leden toevoegen en kies de gebruikers die u wilt toevoegen - in ons voorbeeld de gebruiker die u zojuist hebt gemaakt - en klik vervolgens op Selecteren.



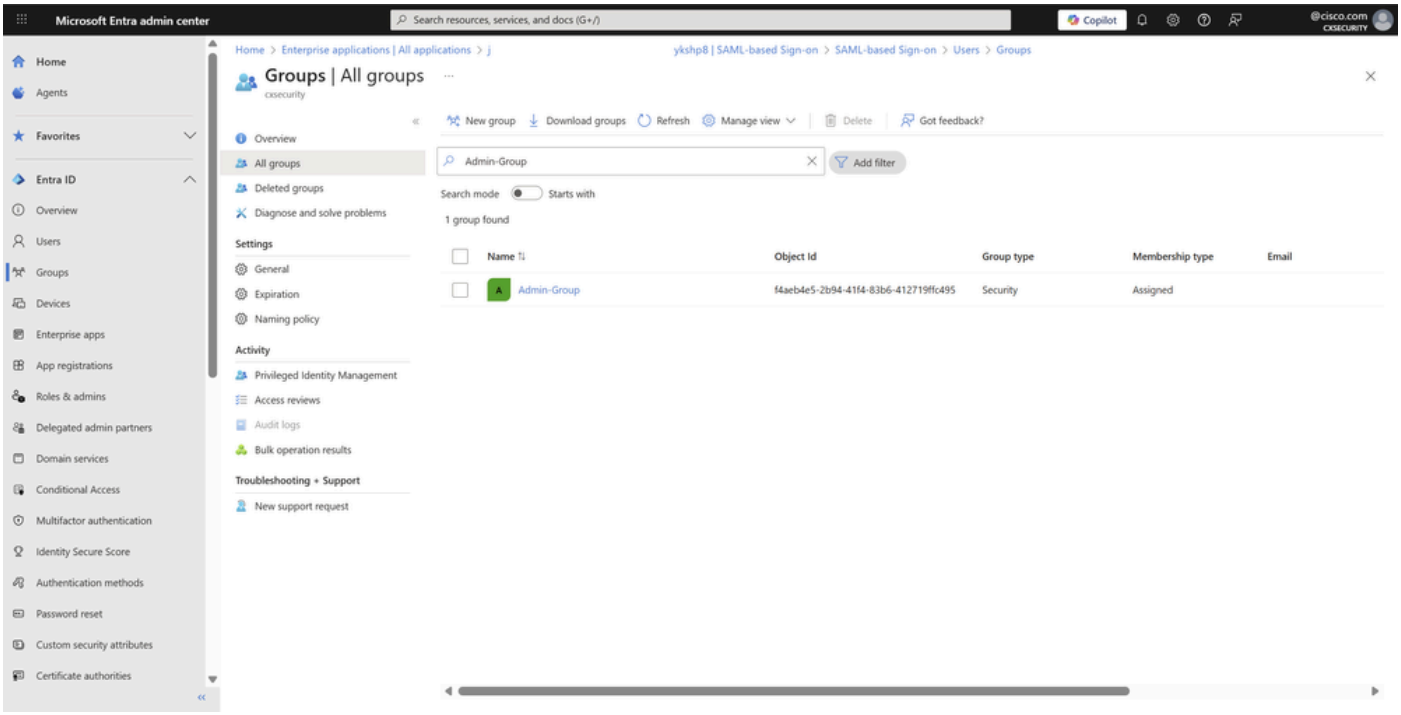
Pagina Groepcreatie

- Klik op Maken om de groep aan te maken.



Pagina Groepcreatie

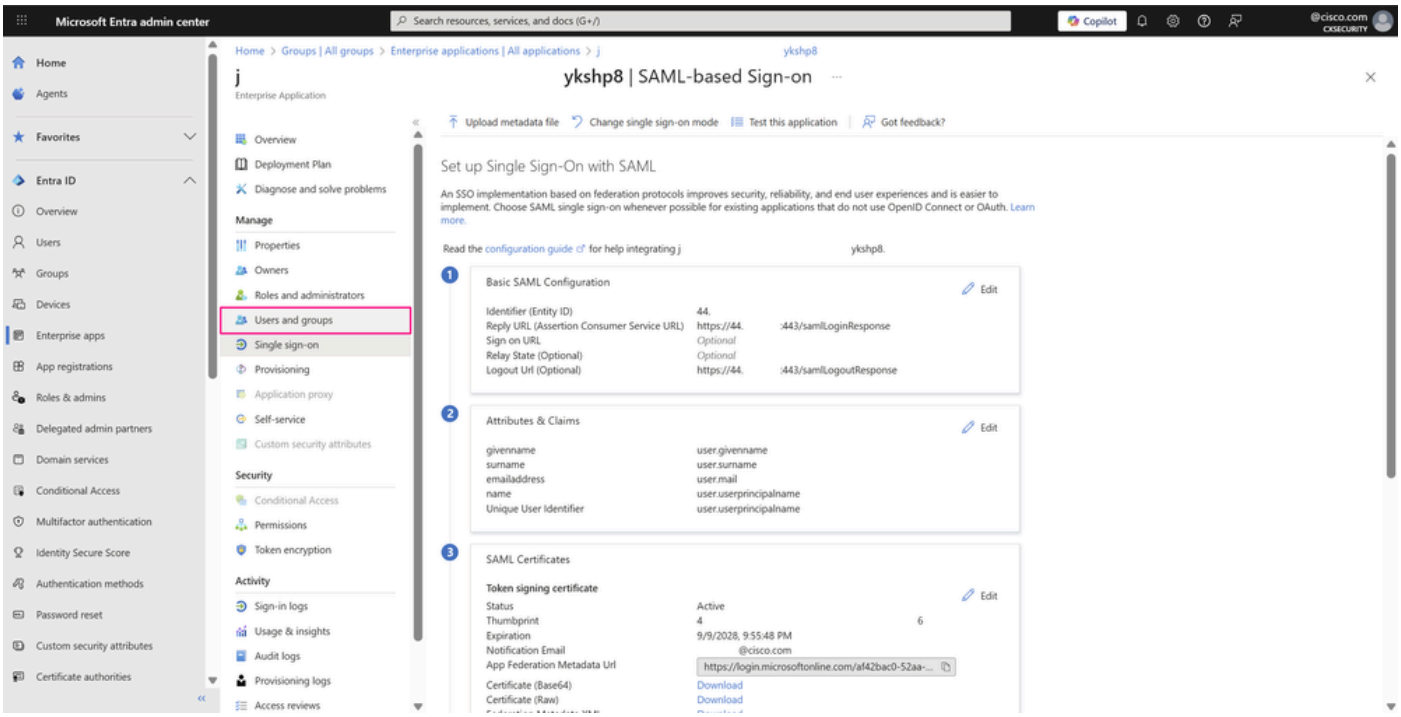
- De nieuwe groep verschijnt kort daarna. Als dit niet het geval is, klikt u op Vernieuwen en zoekt u naar de groepsnaam met de zoekbalk in de service. Herhaal de voorgaande stappen om een andere gebruiker aan te maken en deze toe te voegen aan een ander groepslidmaatschap om de aanmelding voor SSO met de toepassing en een van de andere gebruikersgroepen, zoals operator, te valideren.



Pagina Alle groepen

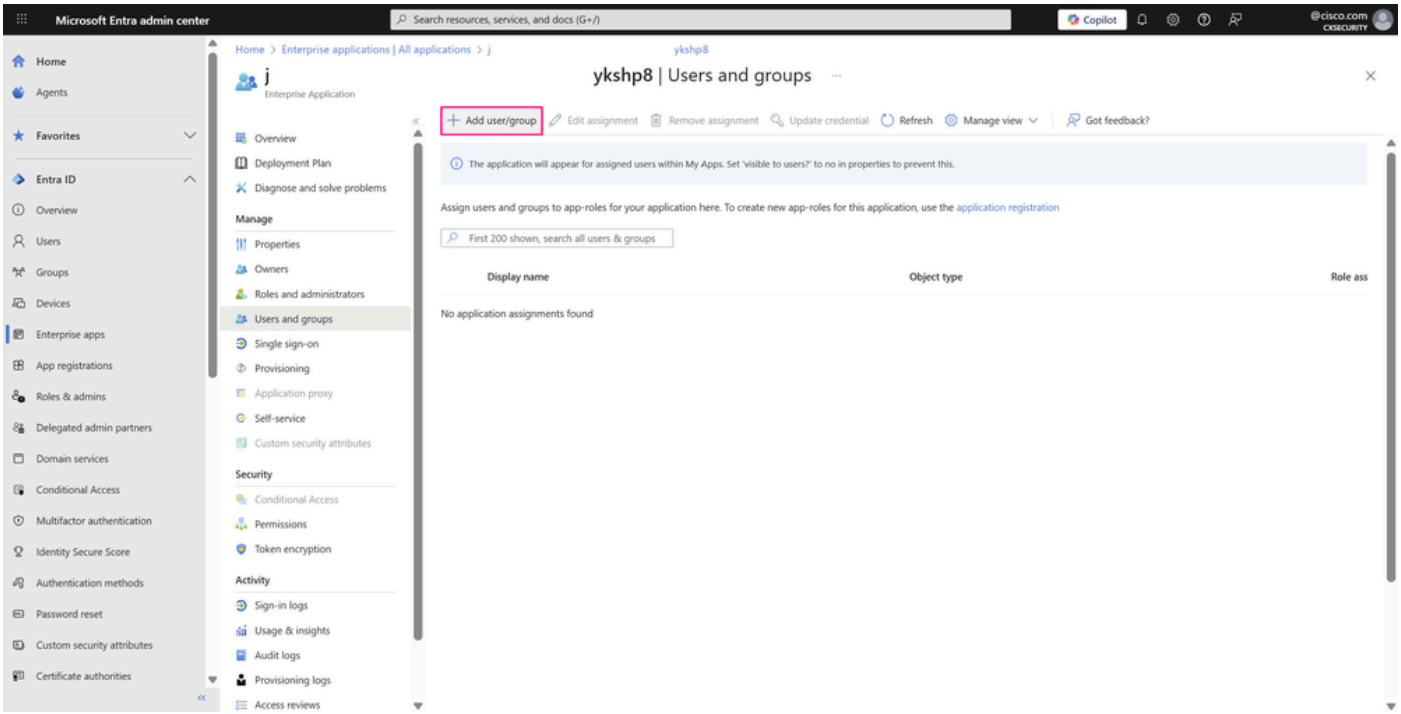
Stap 4. SAML Group Provisioning configureren voor Microsoft Entra ID

- Als u de groepen of de gebruikers die aan deze groepen zijn gekoppeld in de SAML-configuratie wilt aanbieden, moet u deze toewijzen aan uw bedrijfstoepassing, zodat ze inlogrechten hebben voor uw toepassing, bijvoorbeeld de Cisco SD-WAN Manager. Navigeer terug naar Entra ID > Enterprise-apps en open uw bedrijfstoepassing. Klik in het gedeelte Beheren van het linkermenu op Gebruikers en groepen.



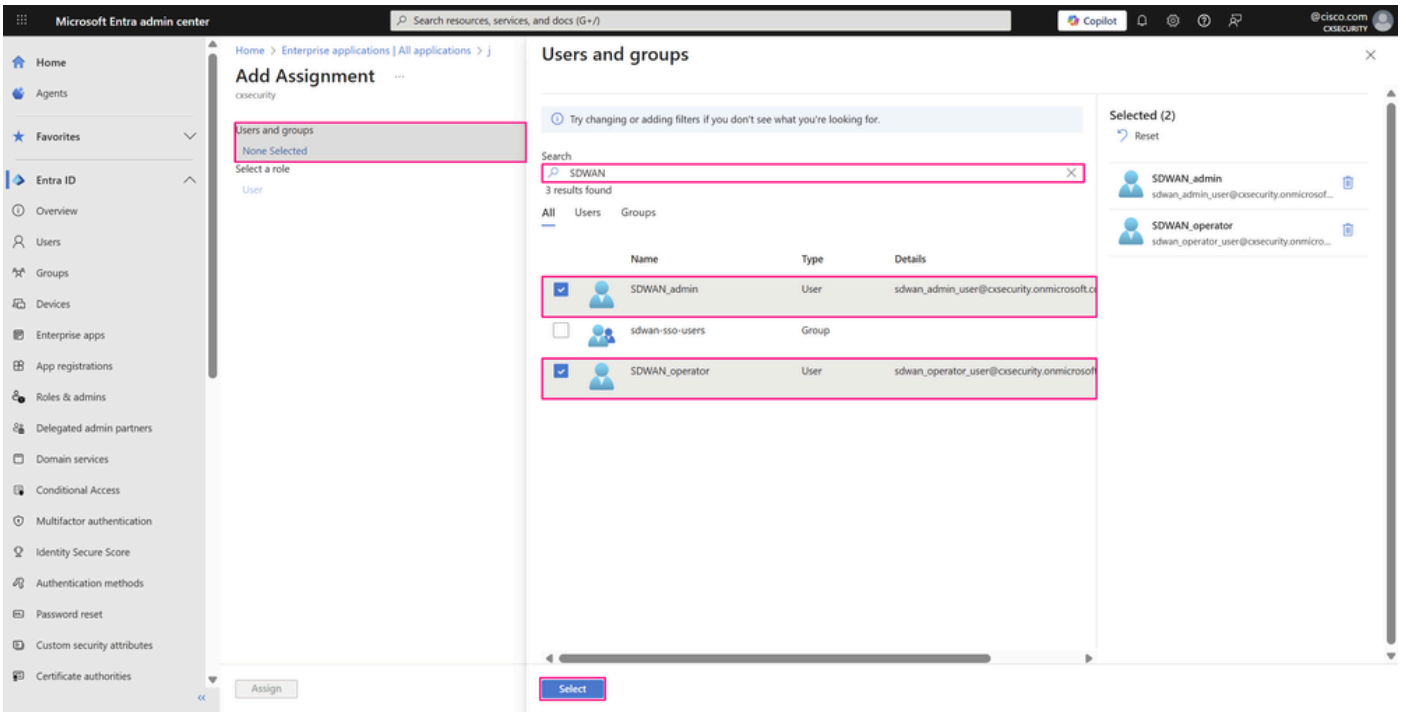
SSO met SAML-configuratiepagina

- Klik vervolgens op Gebruiker/groep toevoegen.



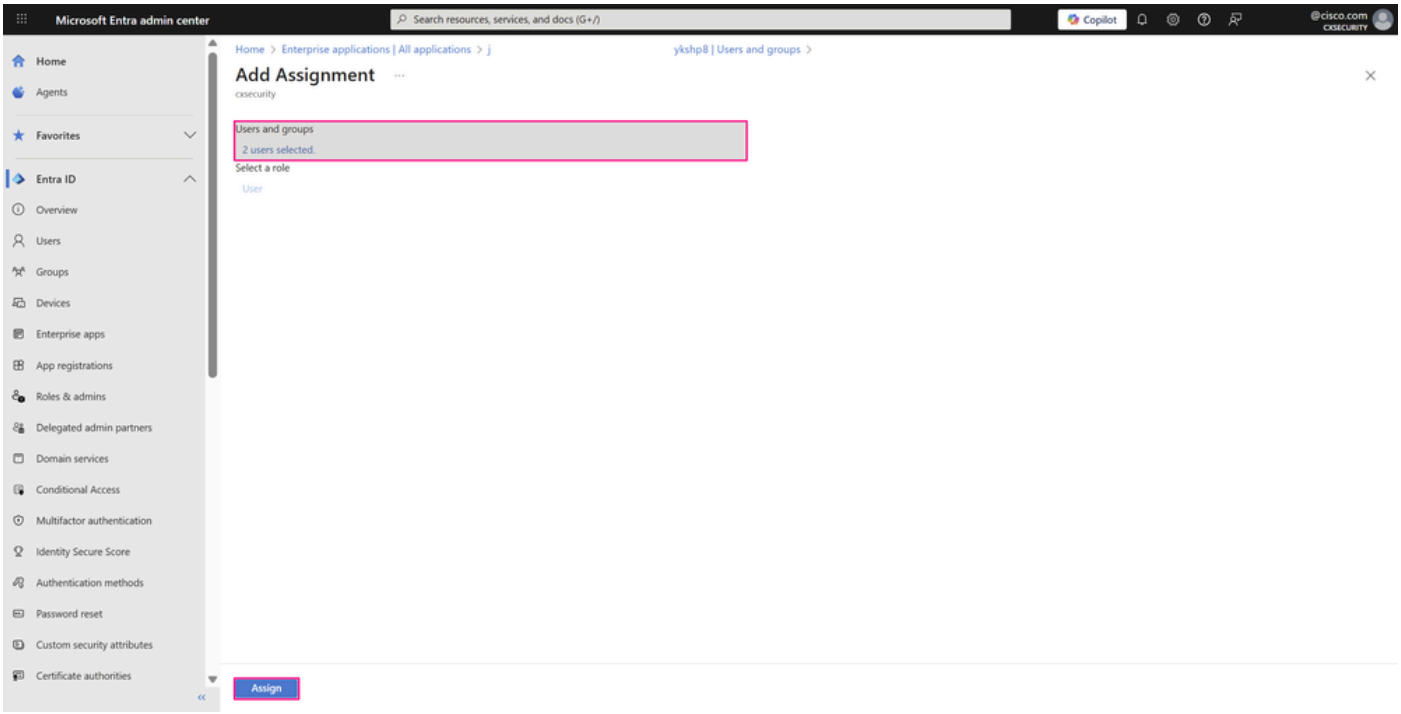
Pagina Gebruikers en groepen

- Klik in het deelvenster Toewijzing toevoegen op Geen geselecteerd onder het veld Gebruikers en groepen. Zoek en kies de gebruiker of groep die u aan uw toepassing wilt toewijzen - in ons voorbeeld de twee gebruikers die in de vorige stappen zijn gemaakt - en klik vervolgens op Selecteren.



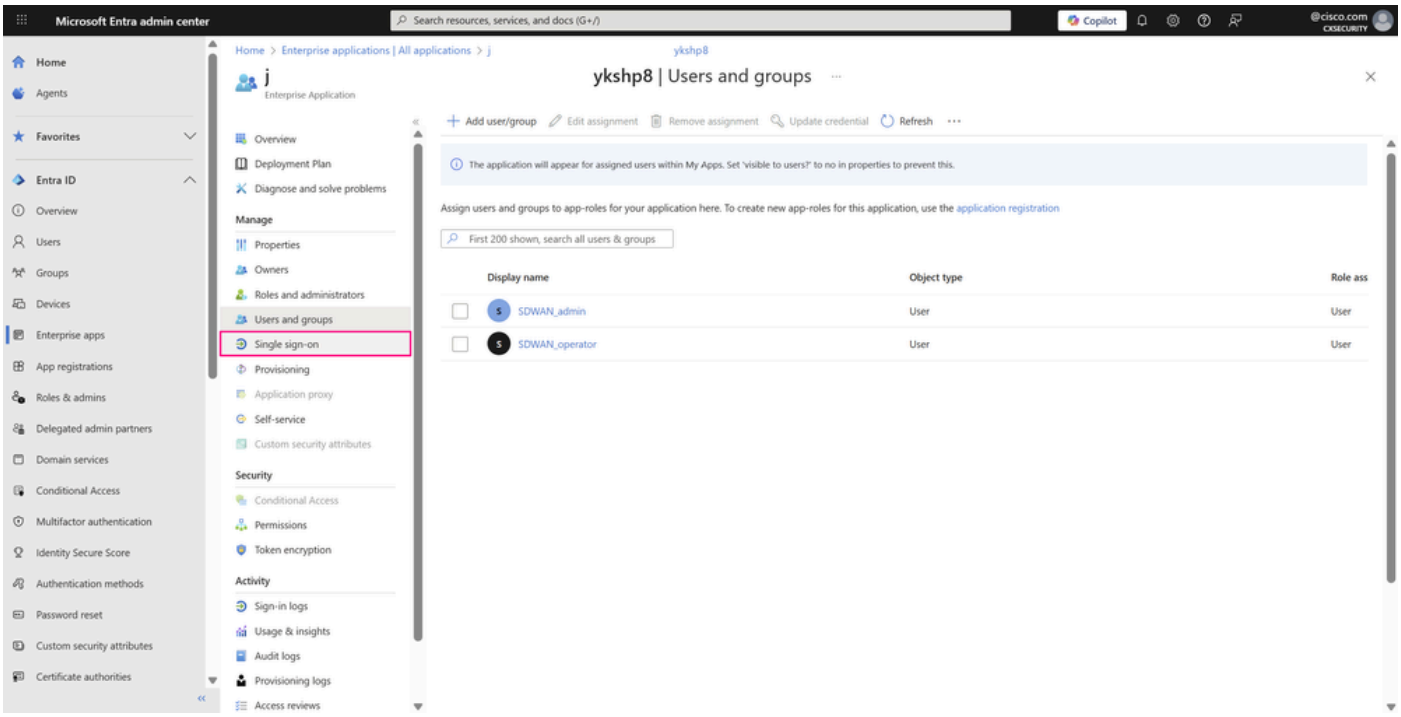
Deelvenster Gebruiker/groepstoewijzing

- Klik op Toewijzen om de gebruiker of groep aan de toepassing toe te wijzen.



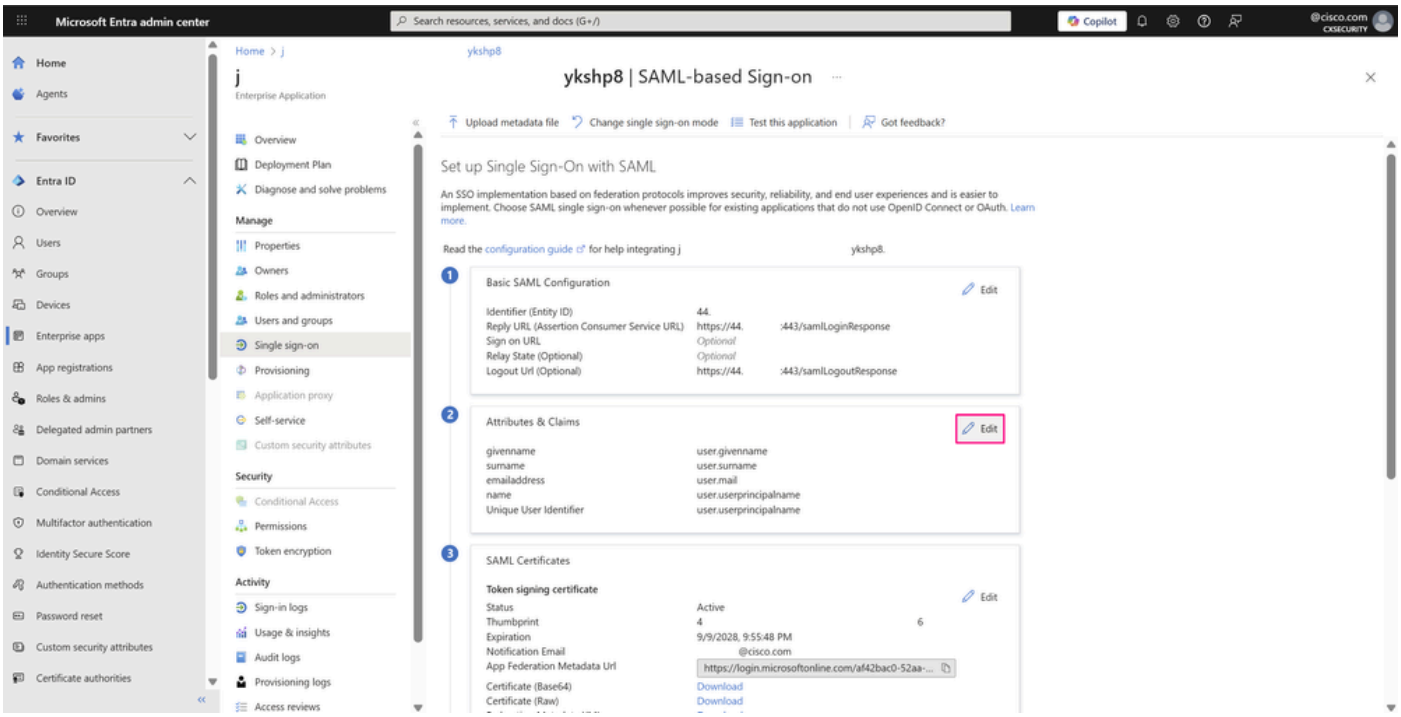
Deelvenster Gebruiker/groepstoewijzing

- De gebruikers die aan uw bedrijfstoepassing zijn toegewezen, worden kort na de toewijzing vermeld. Klik op Eenmalige aanmelding in het gedeelte Beheer van het linkermenu om toegang te krijgen tot de SAML-configuratie van uw toepassing en de resterende vereiste configuratie te voltooien.



Pagina Gebruikers en groepen

- Klik op de pagina Eenmalige aanmelding met SAML instellen onder Eigenschappen en claims op Bewerken.

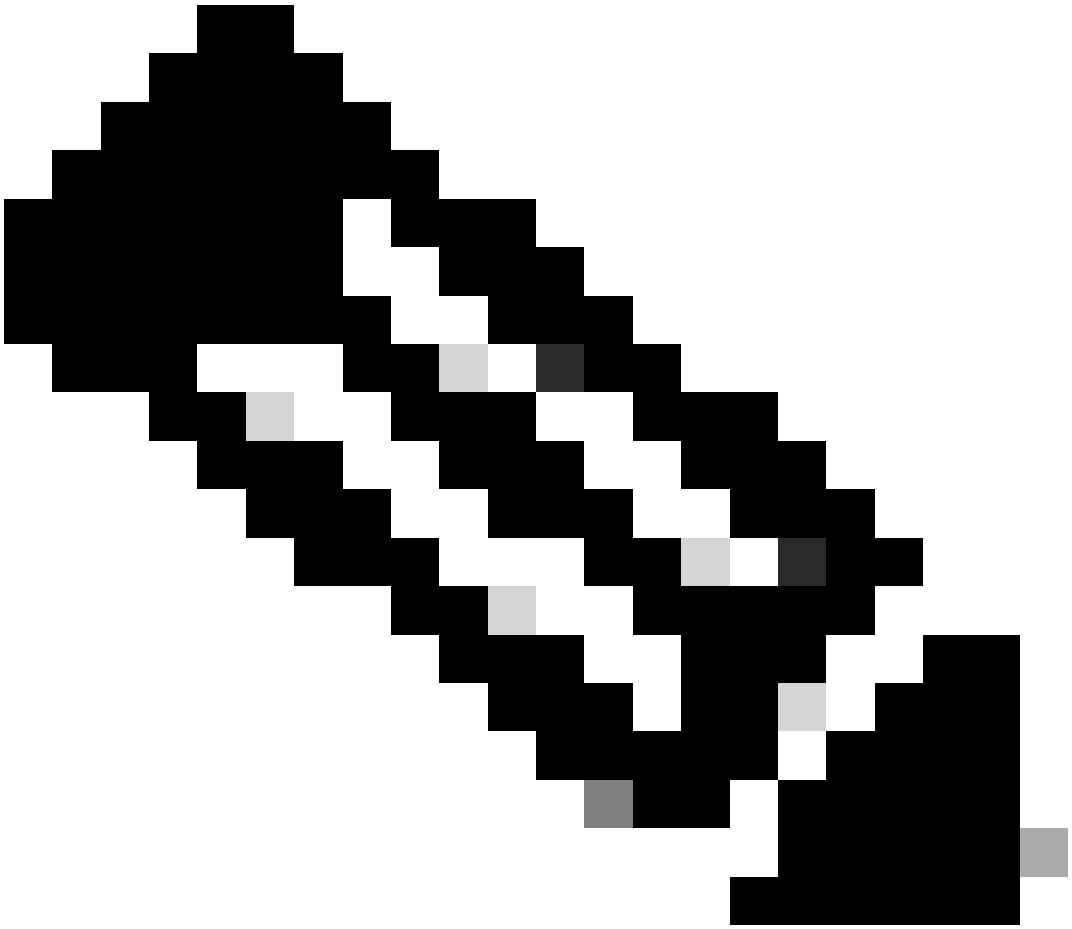


SSO met SAML-configuratiepagina

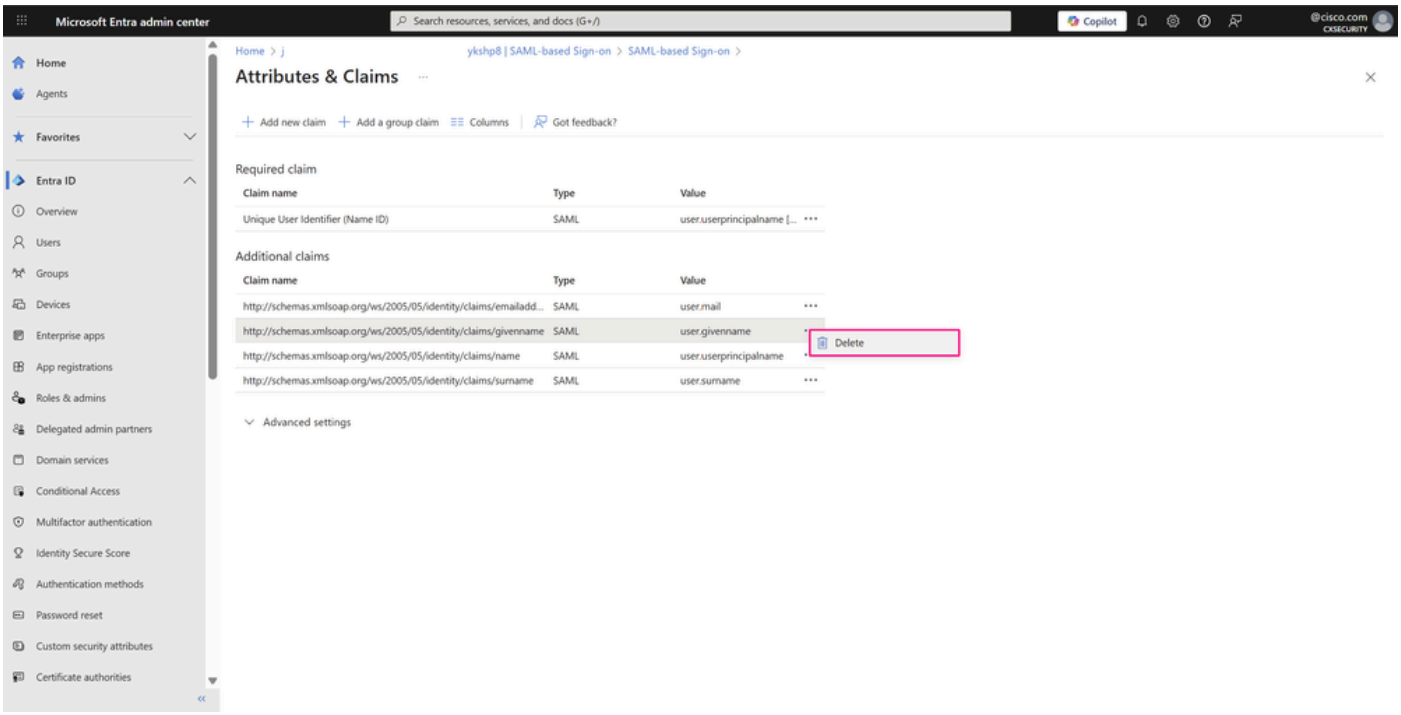
- Op de pagina Attributen en claims klikt u op het pictogram met drie punten en vervolgens Verwijderen om de claim te verwijderen met de waarde user.givenname en de claim met de waarde user.surname, omdat ze niet nodig zijn voor dit voorbeeld.Alleen de volgende claims zijn vereist voor basis-SSO-verificatie met uw toepassing:
    - E-mailadres van de gebruiker –user.mail

- Hoofdgebruikersnaam (UPN) van de gebruiker –user.userprincipalname

---

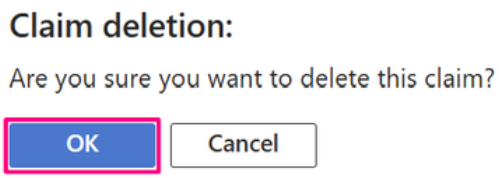


Opmerking: uw organisatie kan aanvullende claims eisen, afhankelijk van de specifieke behoeften.



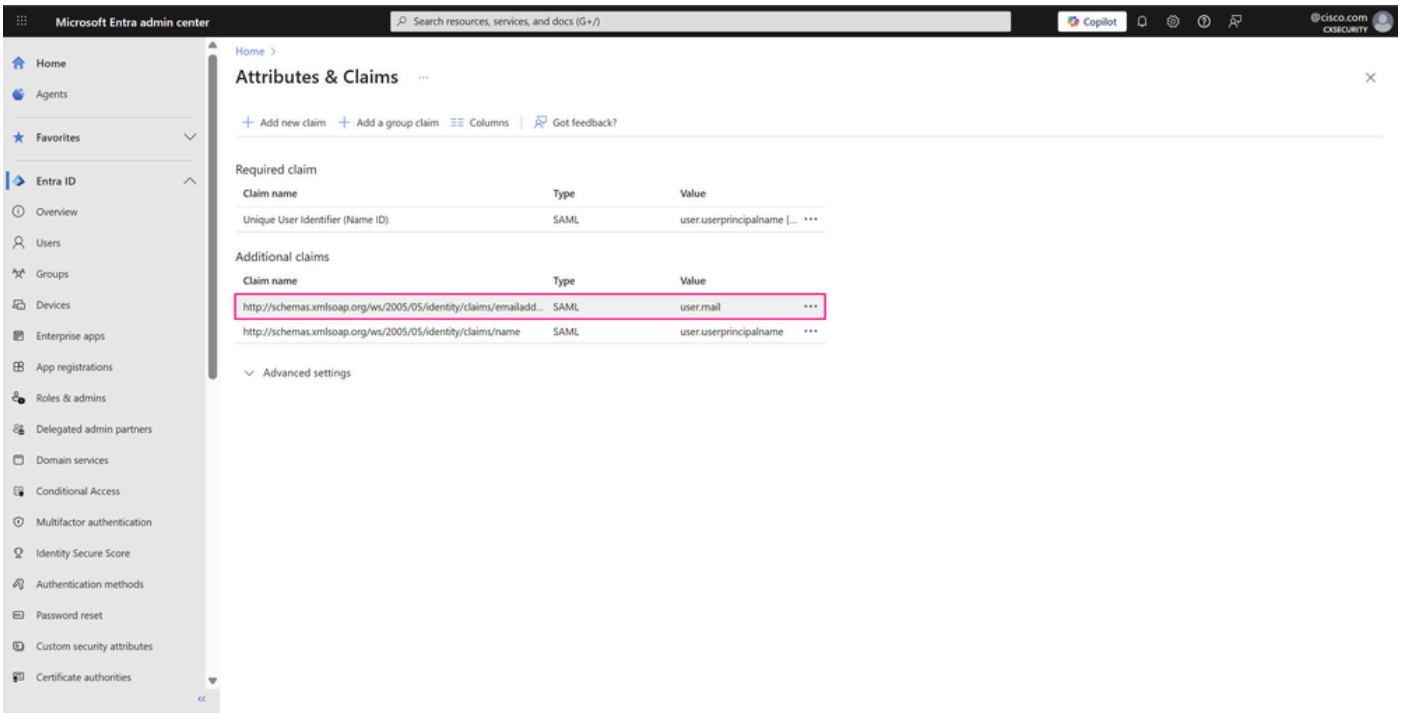
Pagina Attributen en claims

- Klik in het venster Claim verwijderen op OK om de claim te verwijderen.



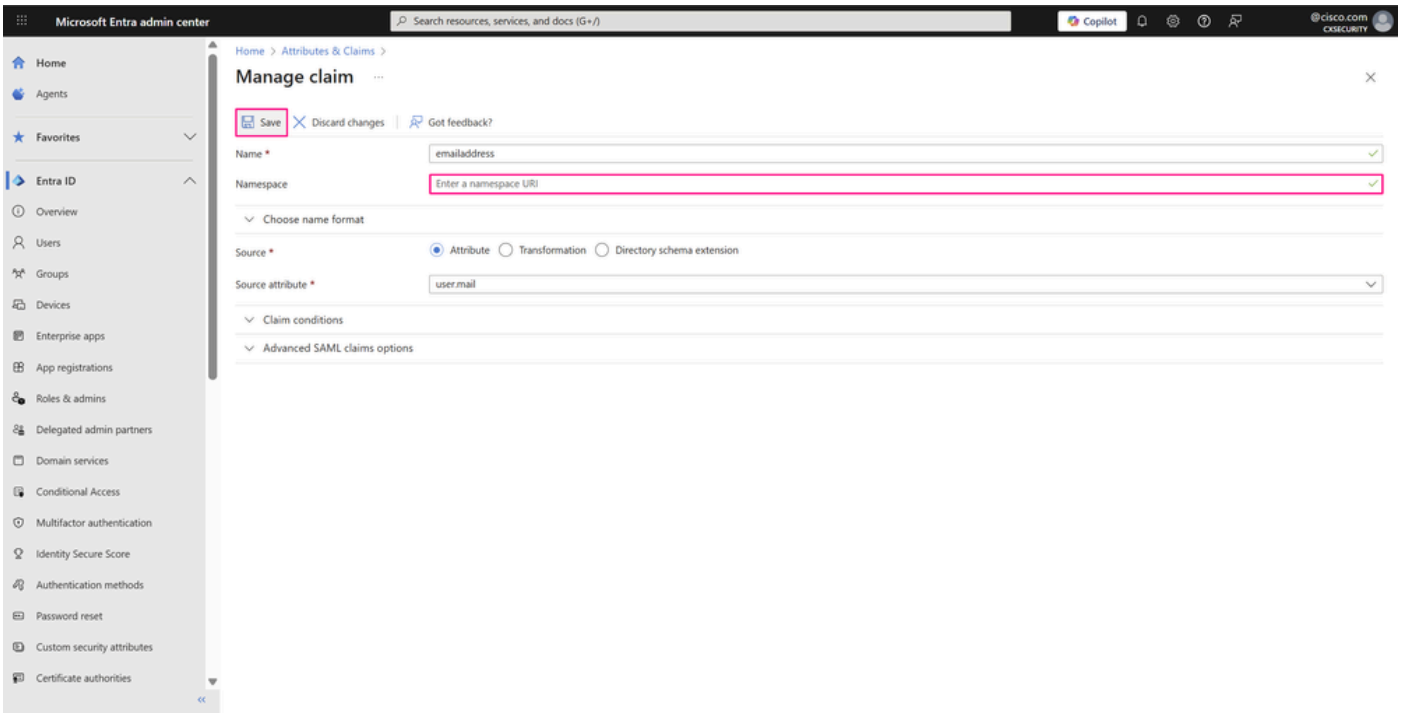
Venster Claim verwijderen

- Verwijder vervolgens de naamruimte uit de claimnaam in de twee resterende claims, aangezien dit veld optioneel is. Deze wijziging maakt het mogelijk de werkelijke naam van elk te worden weergegeven op deze pagina voor eenvoudiger identificatie. Beweeg de muis over elke claim en klik erop om toegang te krijgen tot de instellingen.



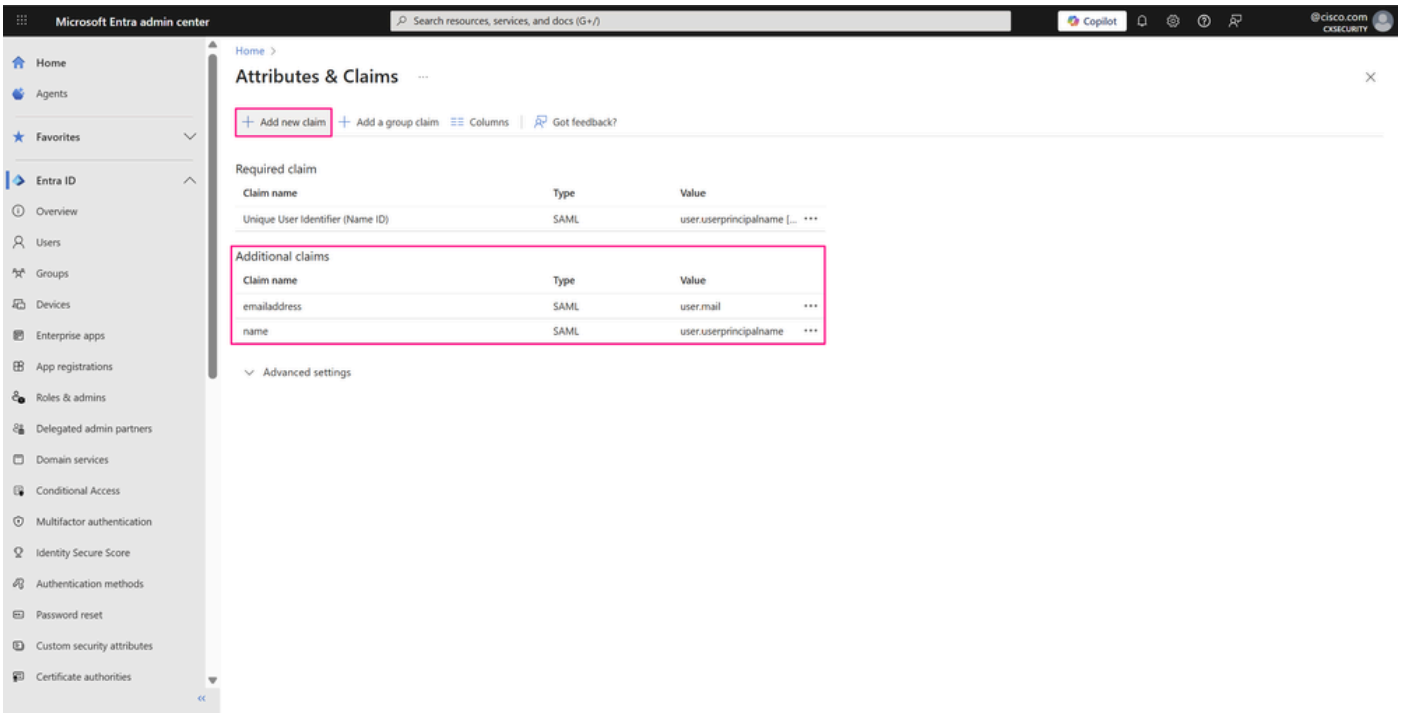
Pagina Attributen en claims

- Verwijder op de pagina Claim beheren het veld Naamruimte en klik op Opslaan om de wijzigingen toe te passen.



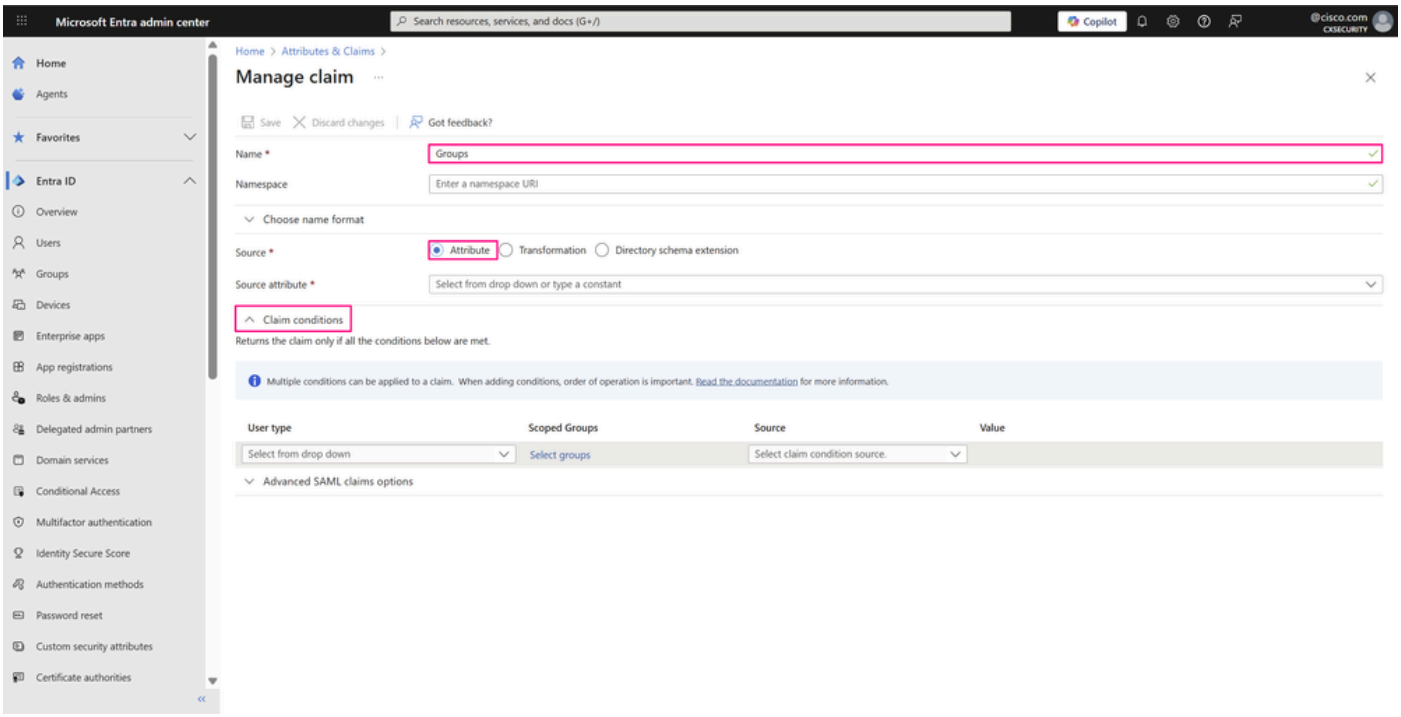
Claimpagina beheren

- De namen van de twee vereiste claims zijn nu te zien. Er is echter nog een extra claim vereist om de groepen te definiëren waartoe de gebruikers behoren en die bevoegd zijn om toegang te krijgen tot toepassingsbronnen. Klik hiervoor op Nieuwe claim toevoegen.



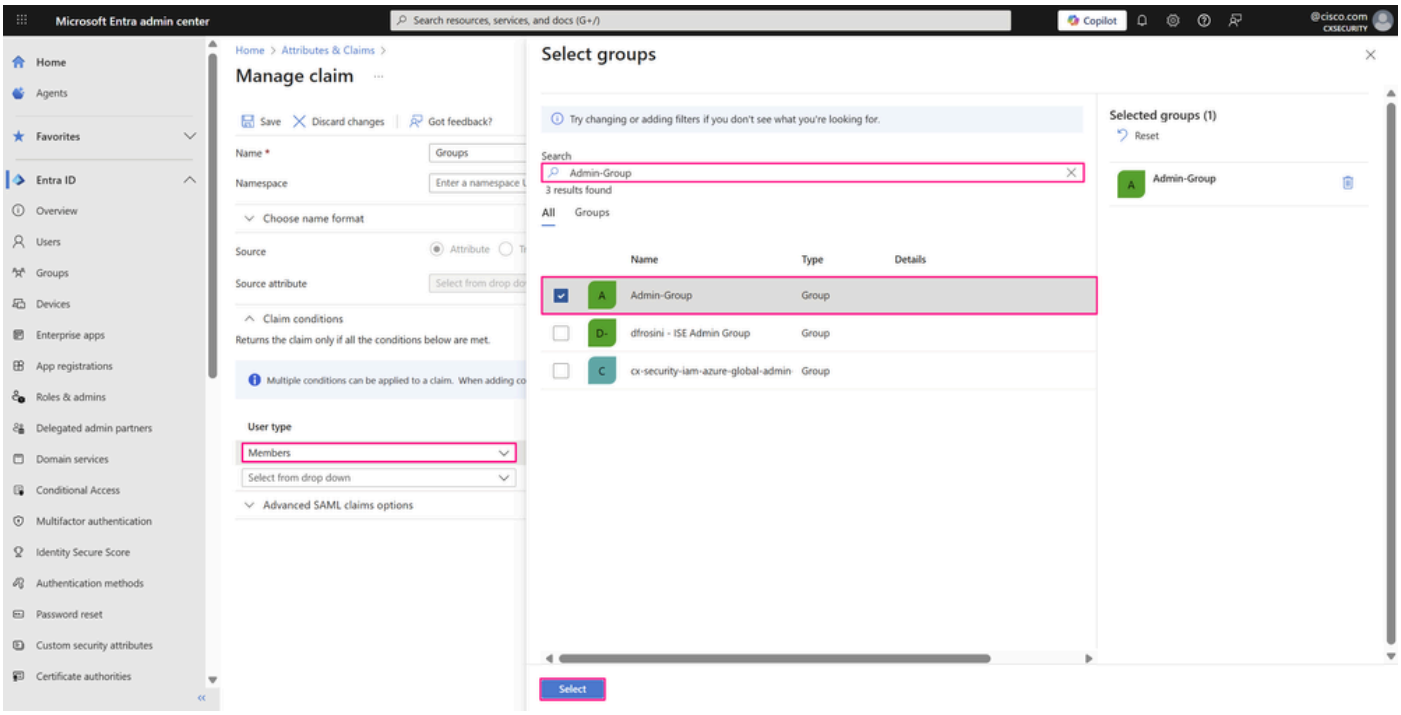
Pagina Attributen en claims

- Voer een naam in om deze claim te identificeren. Selecteer Attribuut naast Bron. Klik vervolgens op Claimvoorwaarden om de opties uit te vouwen en meerdere voorwaarden te configureren.



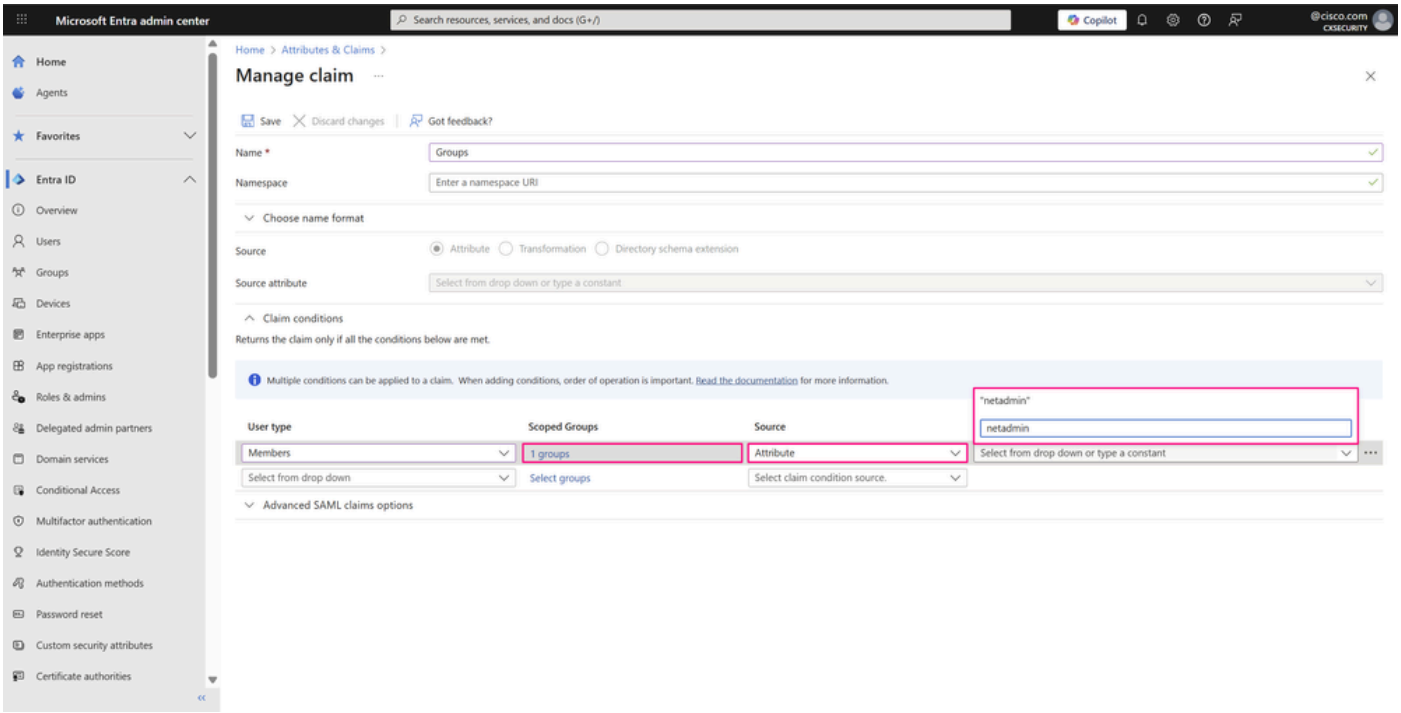
Claimpagina beheren

- Kies in de claimvoorwaarde Leden uit de vervolgkeuzelijst Gebruikerstype en klik op Groepen selecteren om de groep(en) te kiezen waartoe de gebruiker moet behoren en klik vervolgens op Selecteren.



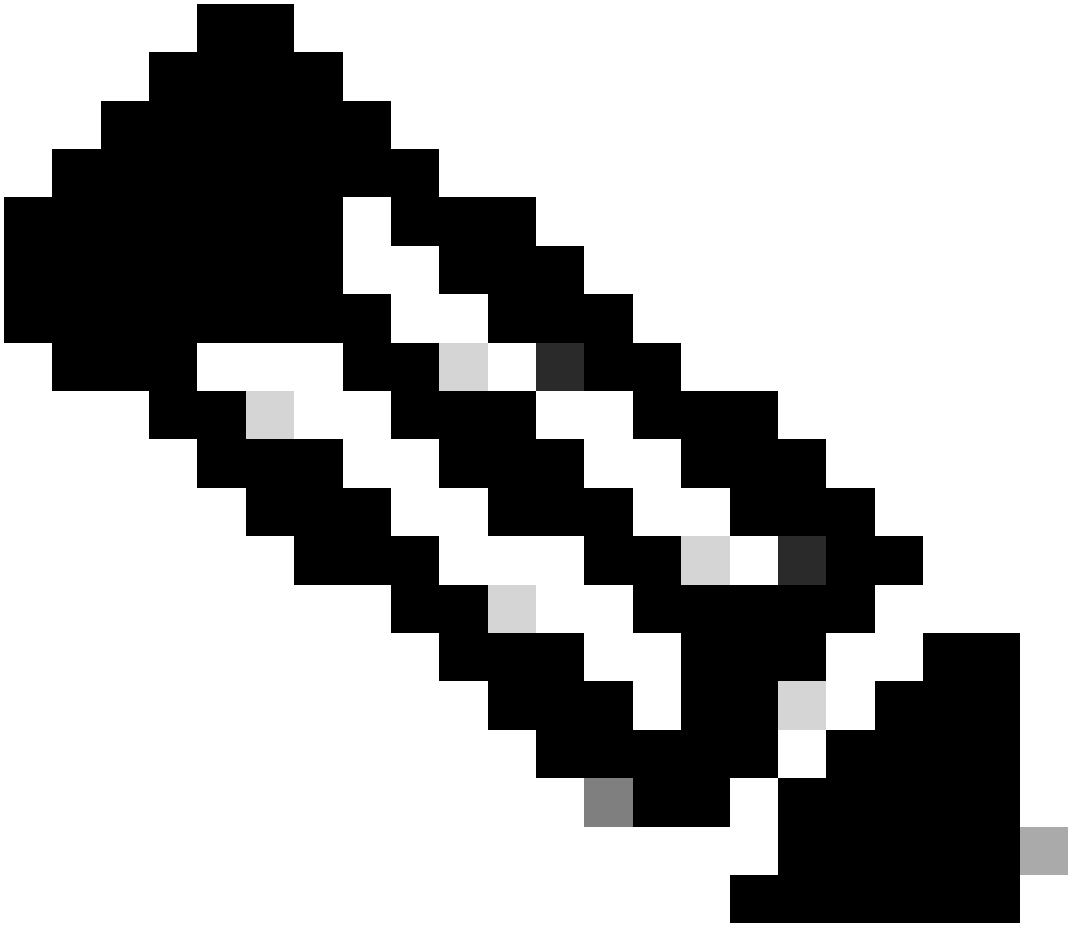
Claimpagina beheren

- Kies Attribuut uit de vervolgkeuzelijst Bron waar de claim de waarde ophaalt. Voer in het veld Waarde het aangepaste kenmerk van de gebruiker in dat verwijst naar de gebruikersgroep die in uw toepassing is gedefinieerd. In dit voorbeeld is netadmin een van de standaard gebruikersgroepen in Cisco SD-WAN Manager. Voer de attribuutwaarde in zonder aanhalingstekens en druk op Enter.

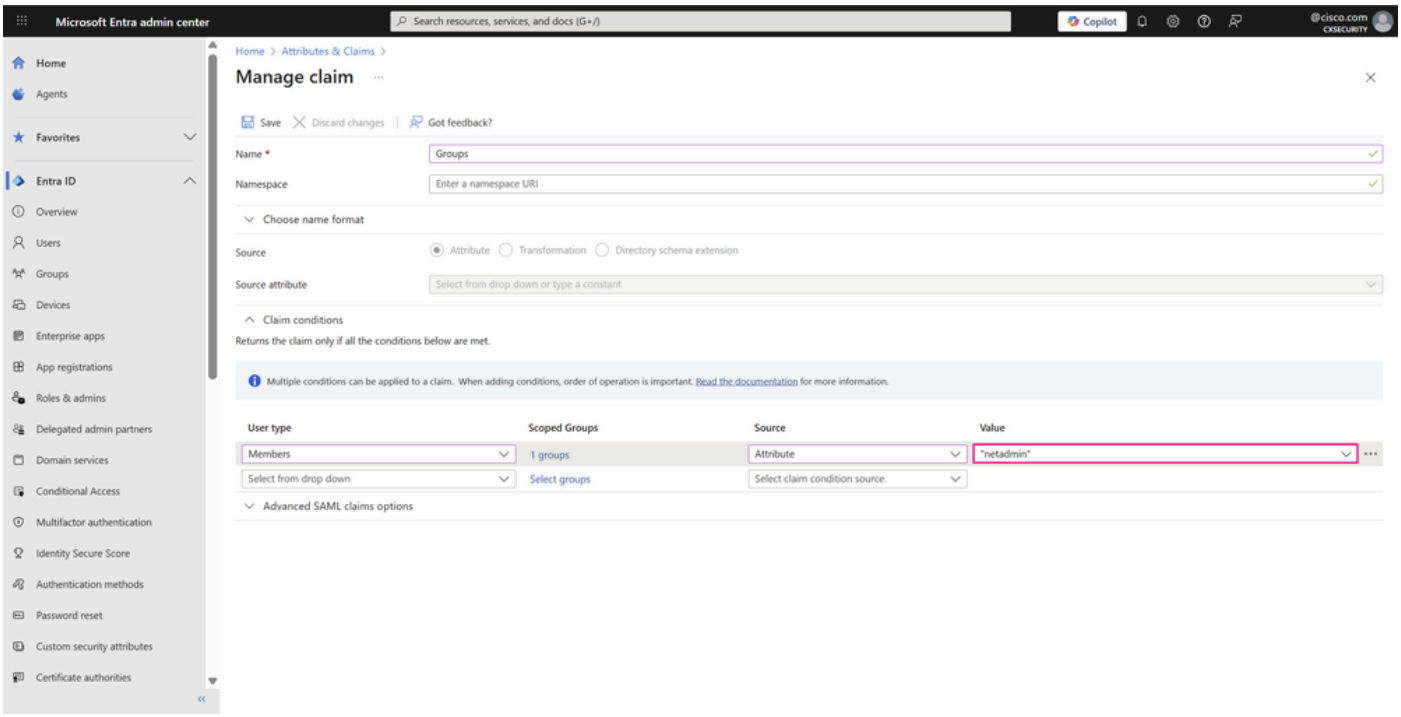


Claimpagina beheren

- Onmiddellijk daarna wordt de attribuutwaarde weergegeven met aanhalingstekens, omdat Microsoft Entra ID deze waarde als een tekenreeks behandelt.

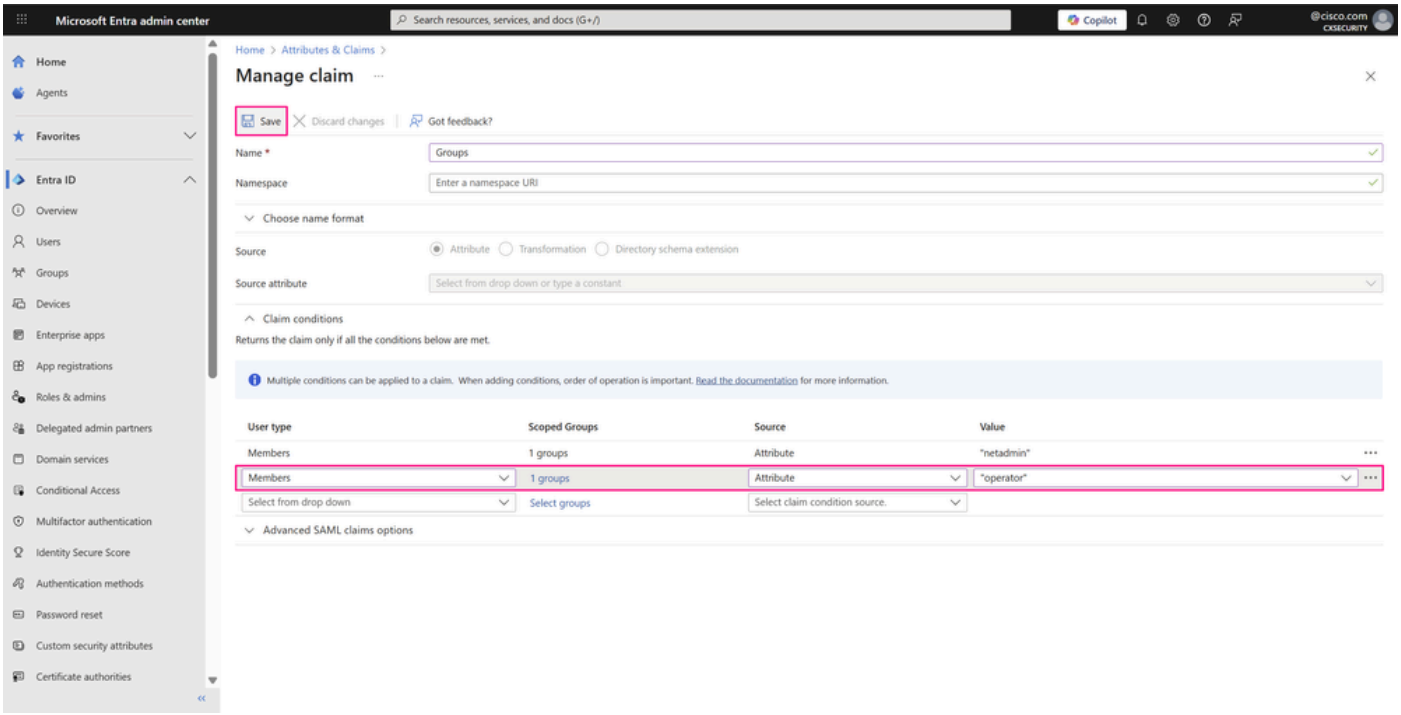


Opmerking: Deze parameters binnen de claimvoorwaarden zijn zeer relevant in de SSO SAML-configuratie van de bedrijfstoepassing, omdat deze aangepaste kenmerken altijd moeten overeenkomen met de gebruikersgroepen die zijn gedefinieerd in Cisco SD-WAN Manager. Deze overeenkomst bepaalt de rechten of machtigingen die aan gebruikers worden verleend op basis van de groep waartoe ze behoren op Microsoft Entra ID.



Claimpagina beheren

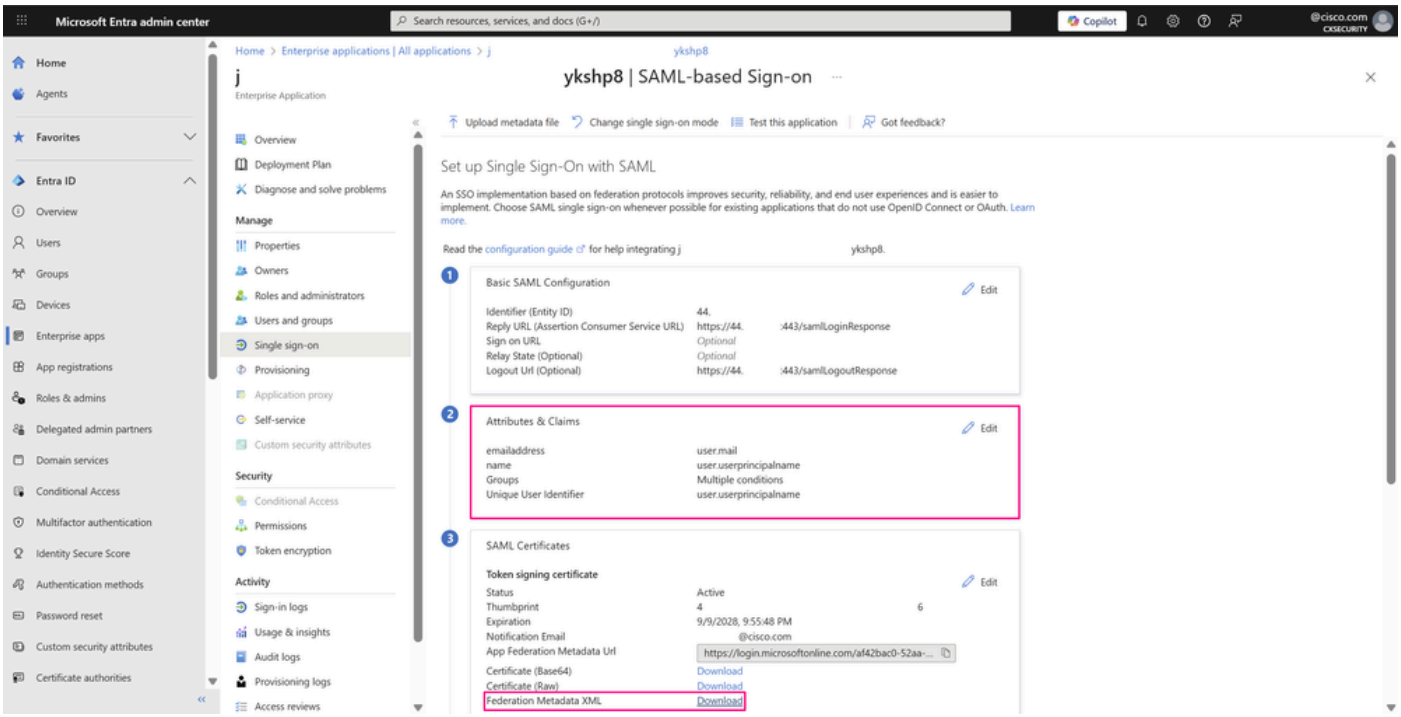
- Herhaal dezelfde stappen voor een tweede claimvoorwaarde voor de tweede groep die is gemaakt en die is toegewezen aan de operator-gebruikersgroep in Cisco SD-WAN Manager. Dit proces is vereist voor elke verschillende groep met specifieke machtigingen die u wilt aanmelden bij de toepassing. U kunt ook meerdere groepen toevoegen binnen één voorwaarde. Klik op Opslaan om de wijzigingen op te slaan.



Claimpagina beheren

- Op de pagina Eenmalige aanmelding met SAML instellen, toont het gedeelte Eigenschappen en claims de nieuwe wijzigingen. Als u de configuratie in de Microsoft Entra ID onder SAML-

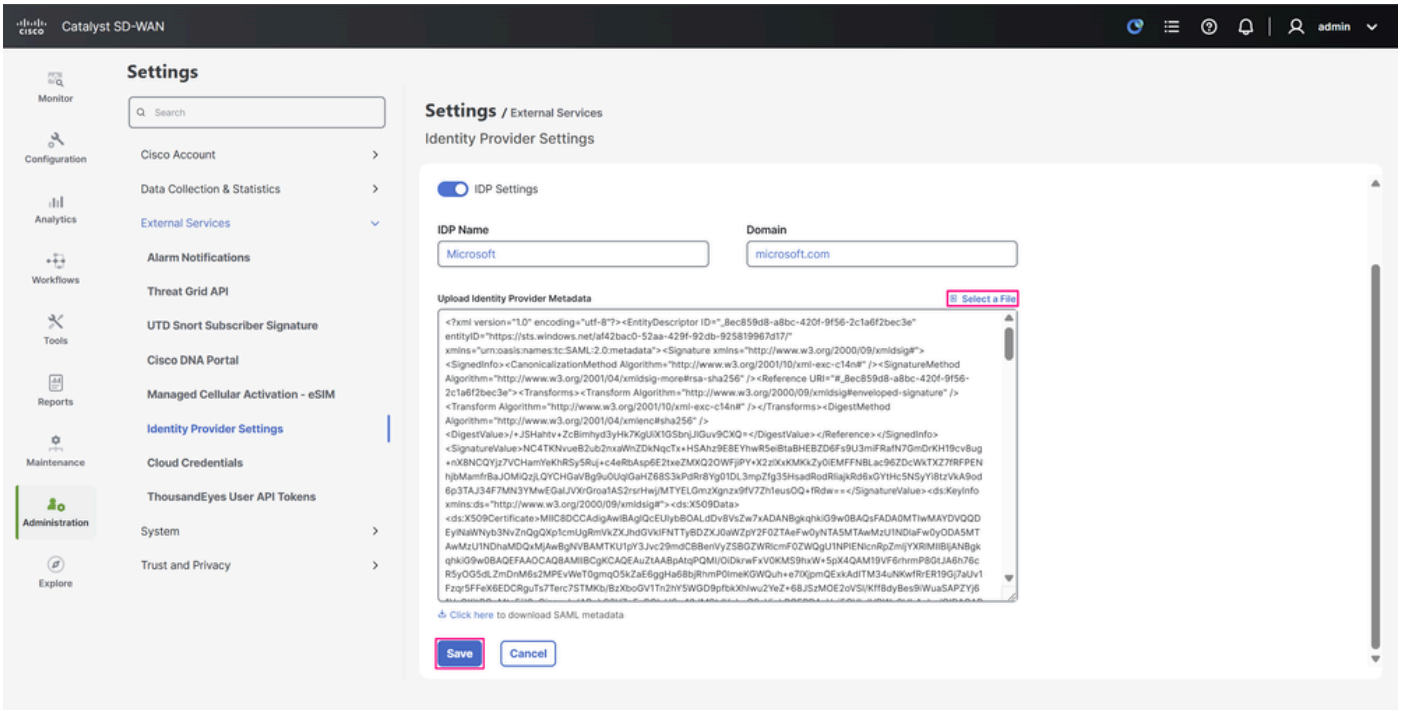
certificaten wilt afsluiten, klikt u op Downloaden naast Metagegevens XML van de Federatie om het XML-bestand te downloaden dat identiteitsservices voor de toepassing biedt.



SSO met SAML-configuratiepagina

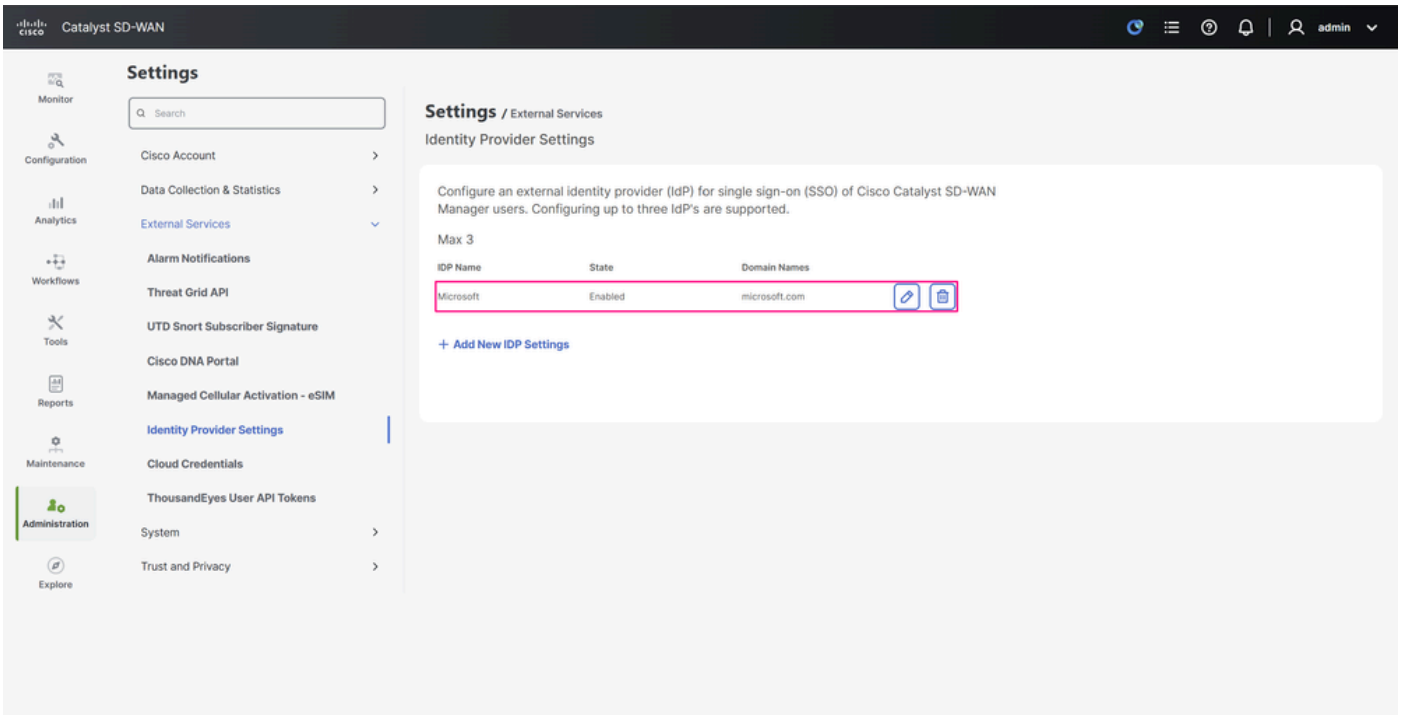
Stap 5. Het Microsoft Entra ID SAML-metagegevensbestand importeren in Cisco SD-WAN Manager

- Als u de metagegevens van de federatie wilt uploaden naar Cisco SD-WAN Manager, gaat u naar Beheer > Instellingen > Externe services > Instellingen van identiteitsprovider en klikt u op Een bestand selecteren. Kies het bestand dat u zojuist hebt gedownload van Microsoft Entra ID en klik vervolgens op Opslaan.



Configuratiepagina IDp-instellingen

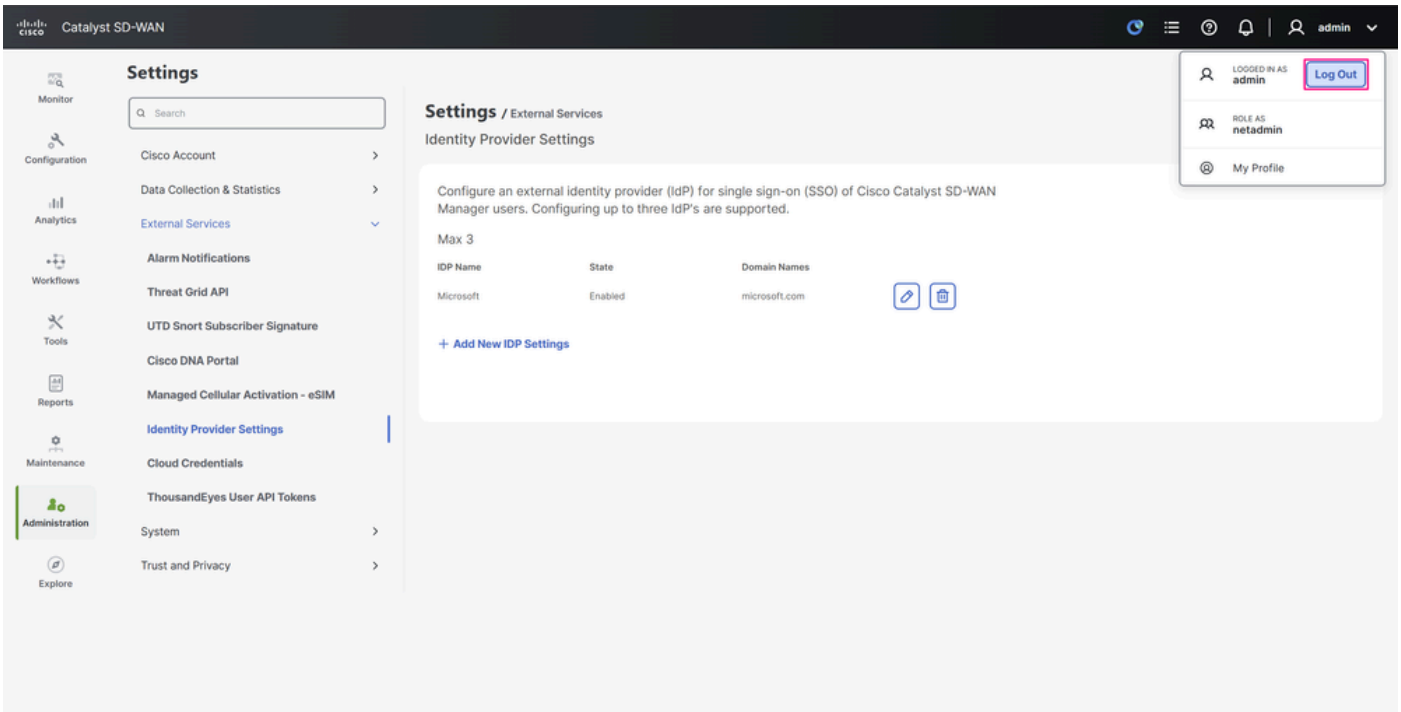
- De IdP-instellingen en metagegevens worden nu opgeslagen.



Configuratiepagina IDp-instellingen

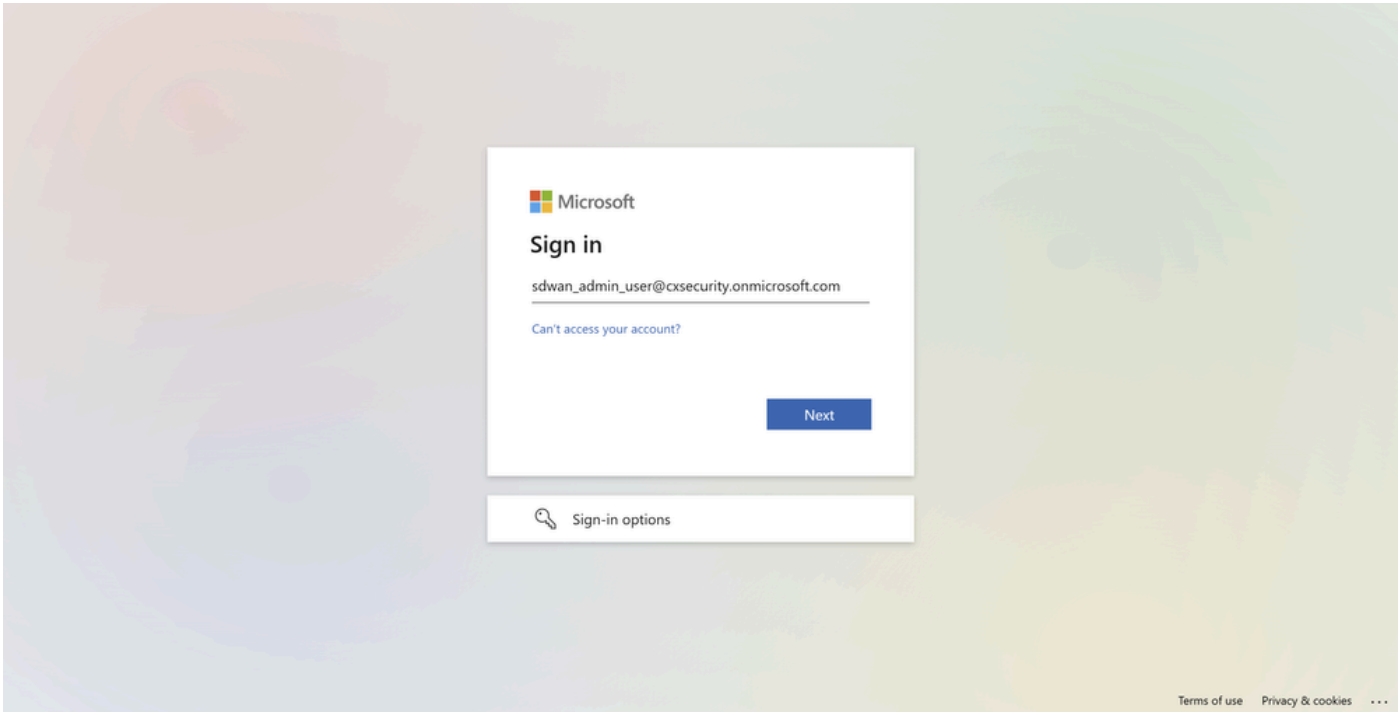
Verifiëren

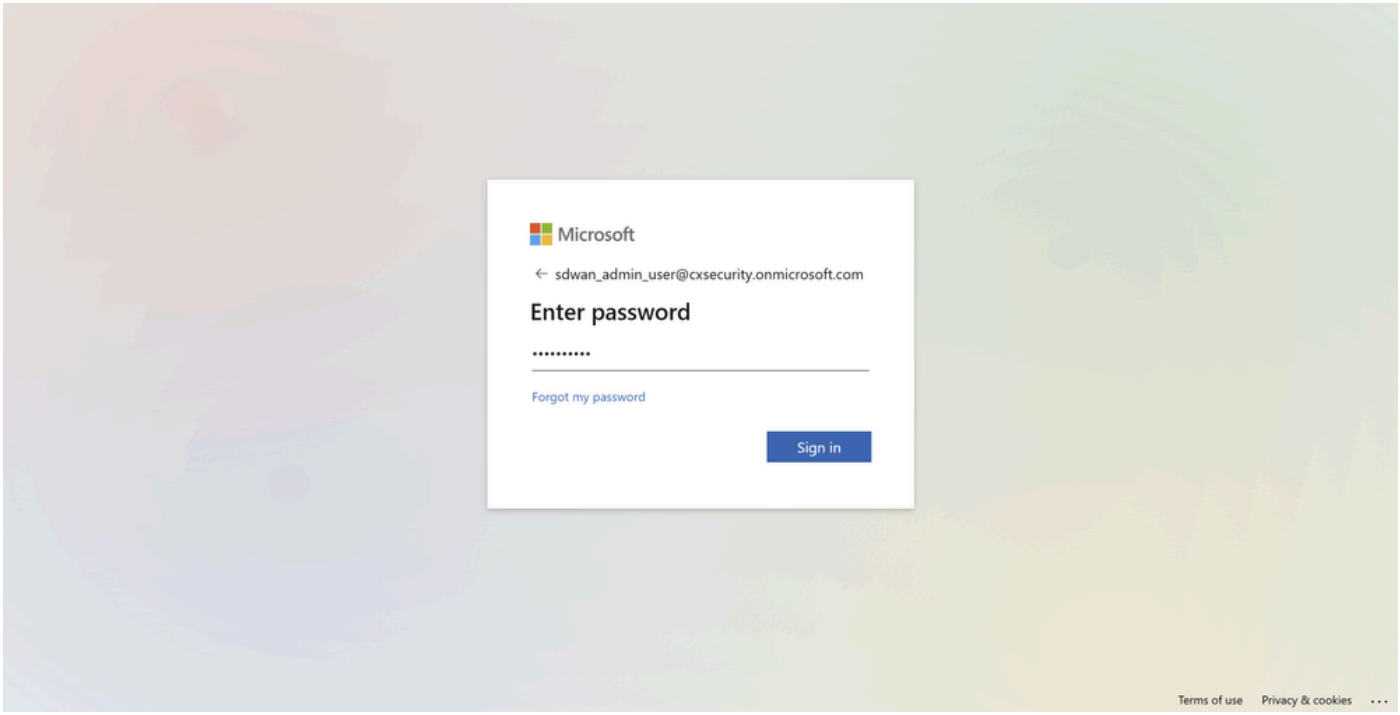
- Klik op uw profielnaam in de rechterbovenhoek van de gebruikersinterface om de opties uit te vouwen en klik vervolgens op Uitloggen om u af te melden bij de portal.



Menu Profiel

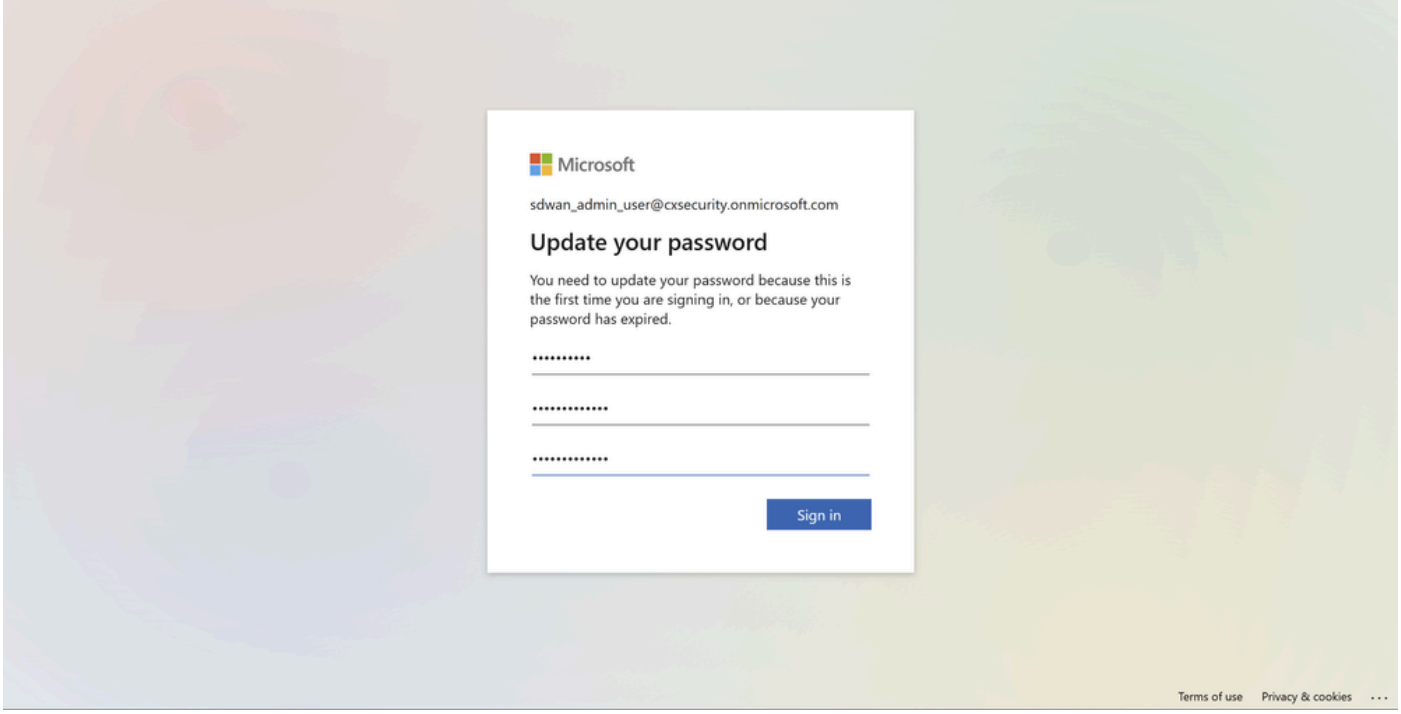
- U wordt onmiddellijk doorgestuurd naar het Microsoft-verificatiescherm, waar u zich aanmeldt met de referenties van de Microsoft Entra ID SSO-gebruikers.





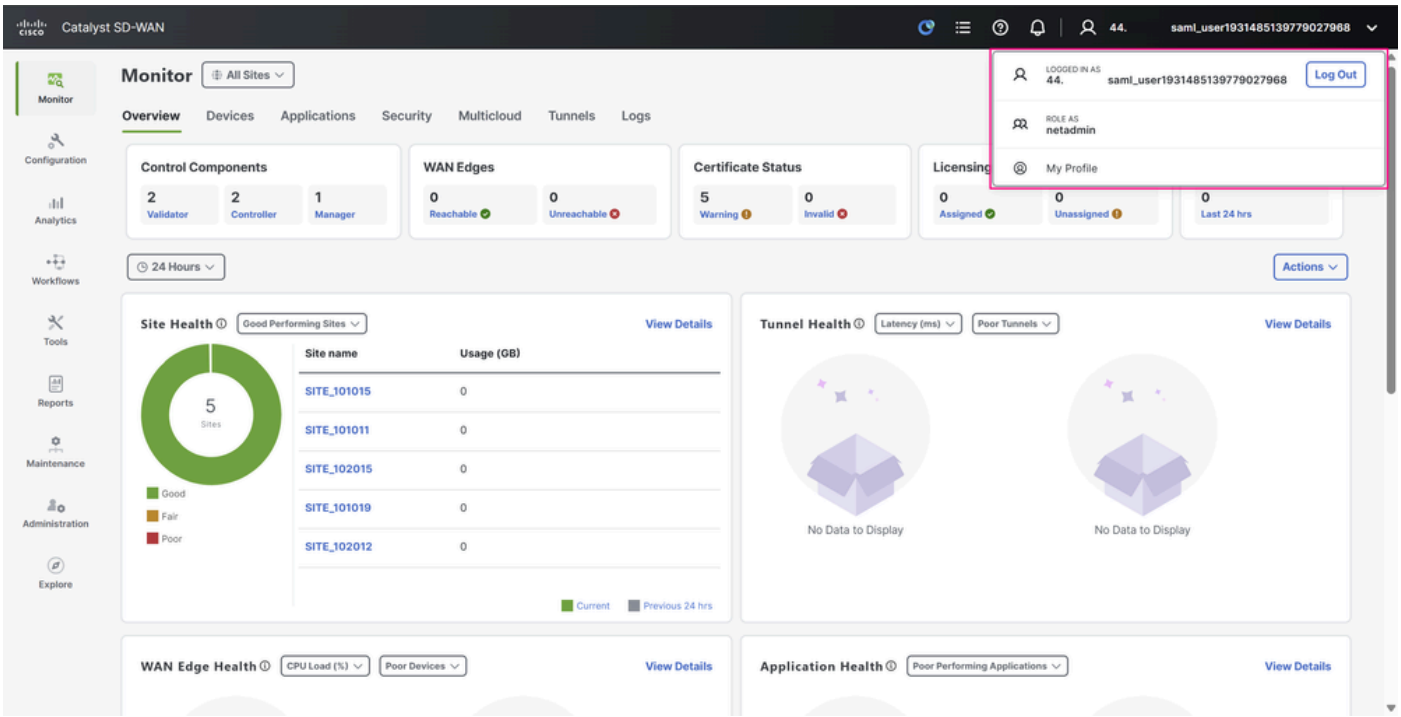
Microsoft-inlogscherm

- Omdat dit de eerste keer is dat de SSO-gebruiker zich aanmeldt, vraagt de prompt om een wachtwoordwijziging.



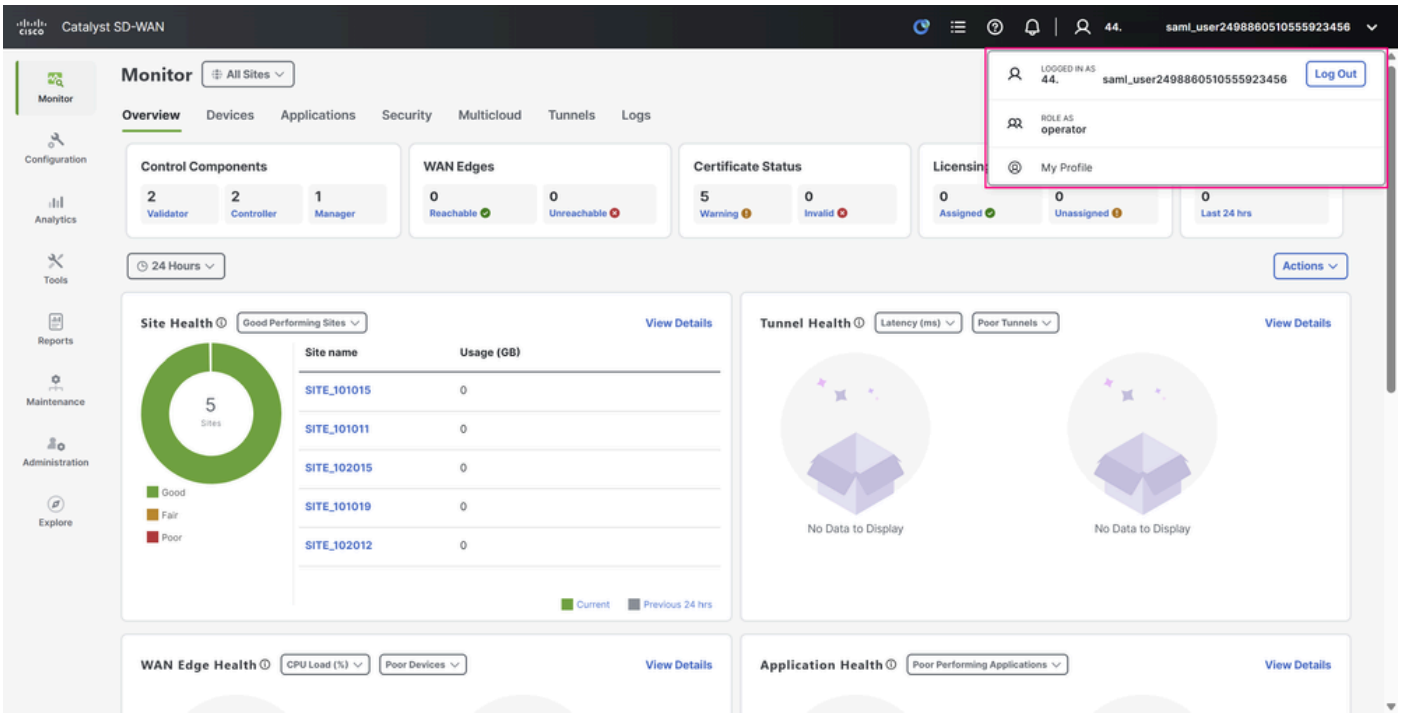
Microsoft-inlogscherm

- Nadat u zich hebt aangemeld, vouwt u de details van uw profiel opnieuw uit in de rechterbovenhoek van het dashboard en kunt u bevestigen dat de gebruiker wordt gedetecteerd met een netadmin-rol, precies zoals geconfigureerd in Microsoft Entra ID.



Cisco SD-WAN Manager UI

- Voer ten slotte dezelfde inlogtest uit met de andere gebruiker. U ziet hetzelfde gedrag - de gebruiker wordt nu geïdentificeerd met de rol van de operator.



Cisco SD-WAN Manager UI

Gerelateerde informatie

- [Single Sign-On configureren voor Cisco IOS XE Catalyst SD-WAN]

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.