Cisco Secure Access configureren voor RA VPNaaS met Entra ID

Inhoud

Inleiding

In dit document wordt stap voor stap beschreven hoe u RA VPN configureert op Cisco Secure Access om te verifiëren met Entra ID.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis met behulp van Azure/Entra ID.
- Kennis van Cisco Secure Access.

Vereisten

Aan deze voorwaarden moet worden voldaan voordat verder kan worden gegaan:

- Toegang tot uw Cisco Secure Access Dashboard als Full Admin.
- Toegang tot Azure als beheerder.
- Gebruikersinrichting al voltooid voor Cisco Secure Access.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Access Dashboard.
- Microsoft Azure Portal.

- Cisco Secure Client AnyConnect VPN versie 5.1.8.105

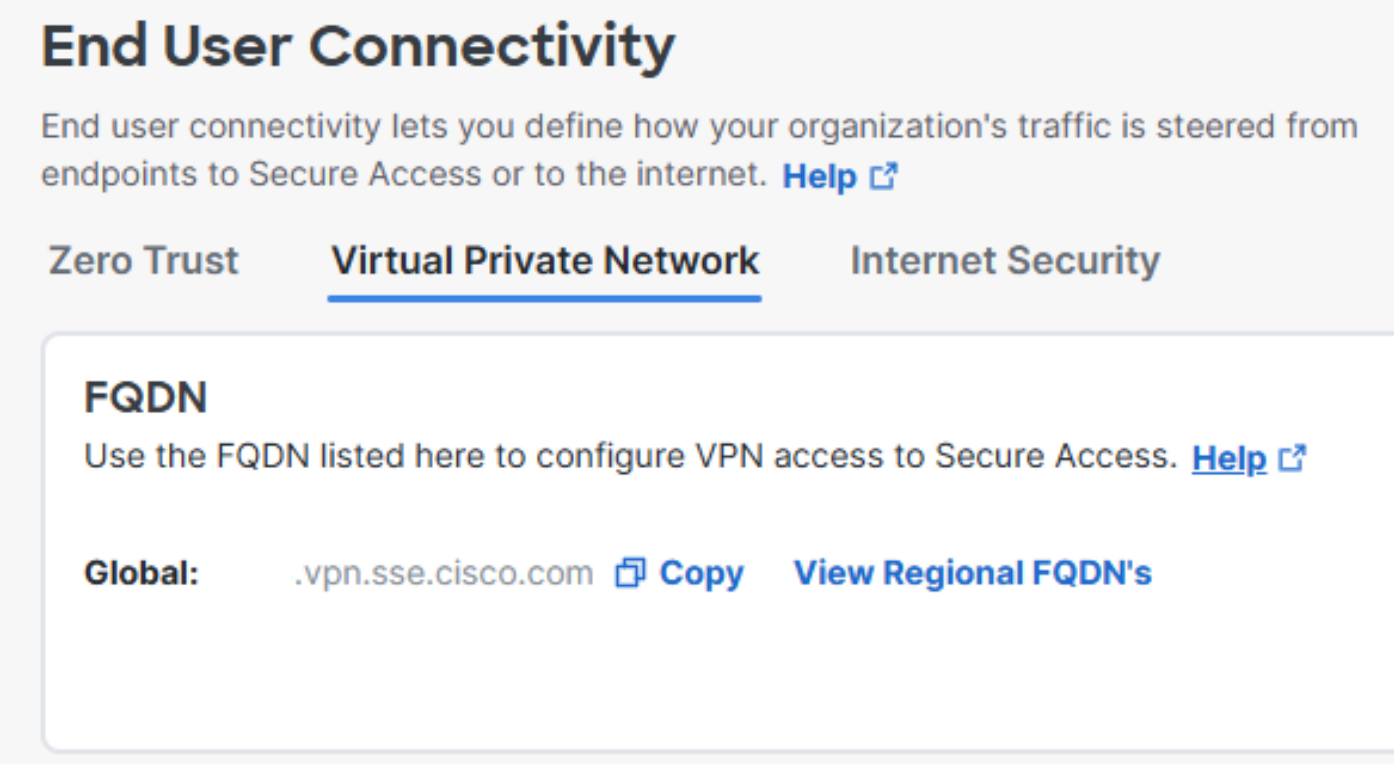
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Azure Configuration

1. Meld u aan bij het Cisco Secure Access-dashboard en kopieer de VPN Global FQDN. We gebruiken deze FQDN in de Azure Enterprise Application-configuratie.

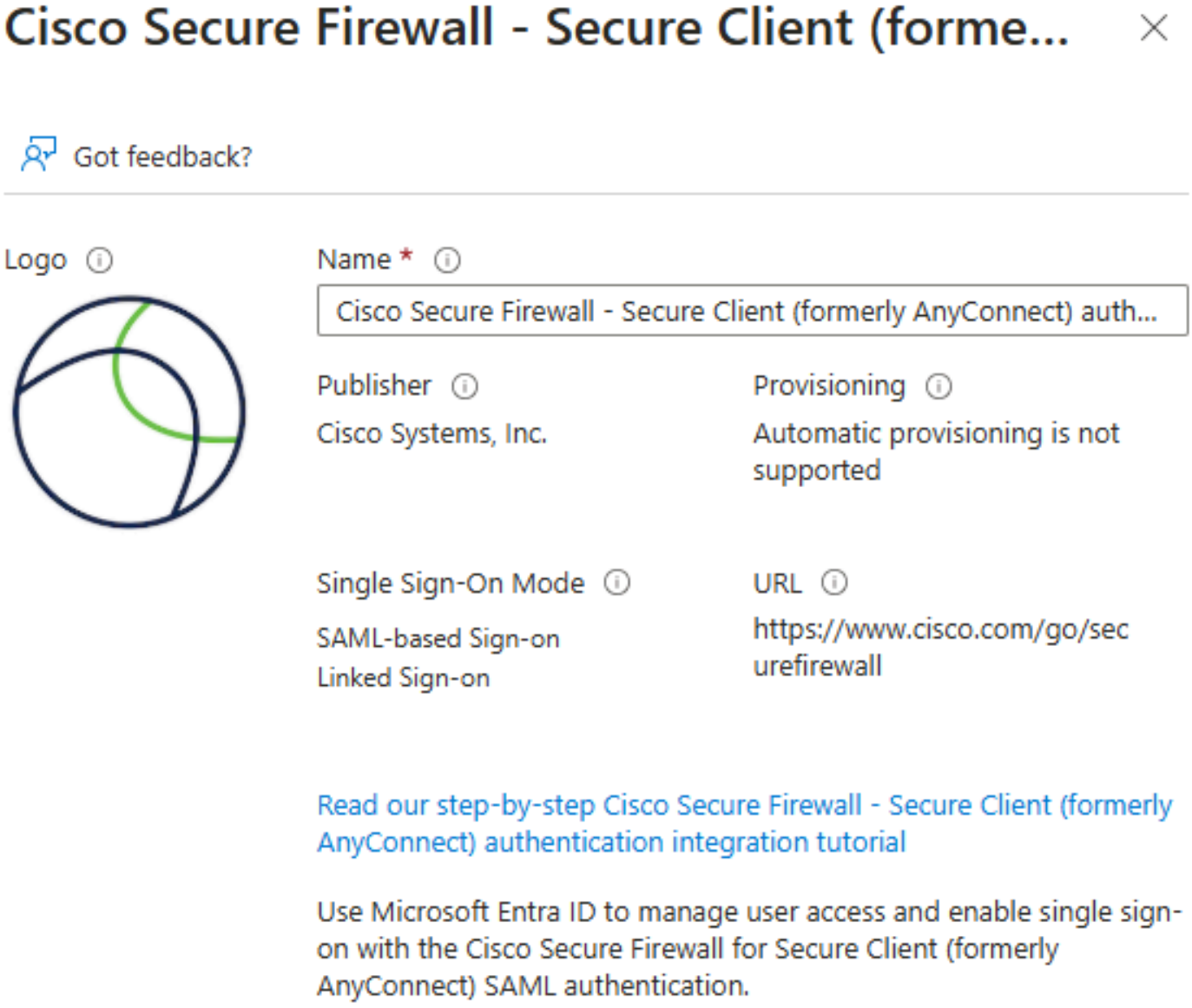
Verbinding maken > Connectiviteit voor eindgebruikers > Virtual Private Network > FQDN > Algemeen



VPN Global FQDN

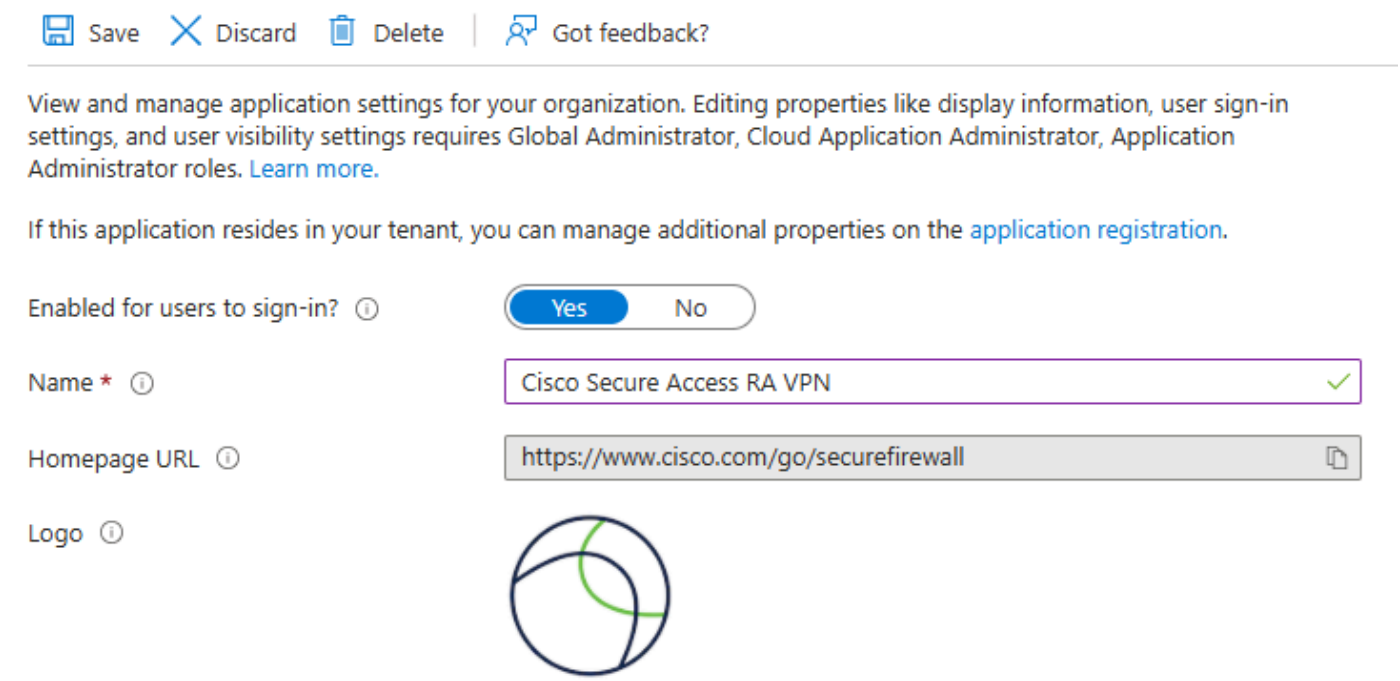
2. Meld u aan bij Azure en maak een bedrijfstoepassing voor de RA VPN-verificatie. U kunt de vooraf gedefinieerde toepassing "Cisco Secure Firewall - Secure Client (voorheen AnyConnect)-verificatie" gebruiken.

Home > Bedrijfstoepassingen > Nieuwe toepassing > Cisco Secure Firewall - Secure Client (voorheen AnyConnect)-verificatie > Maken



App maken in Azure

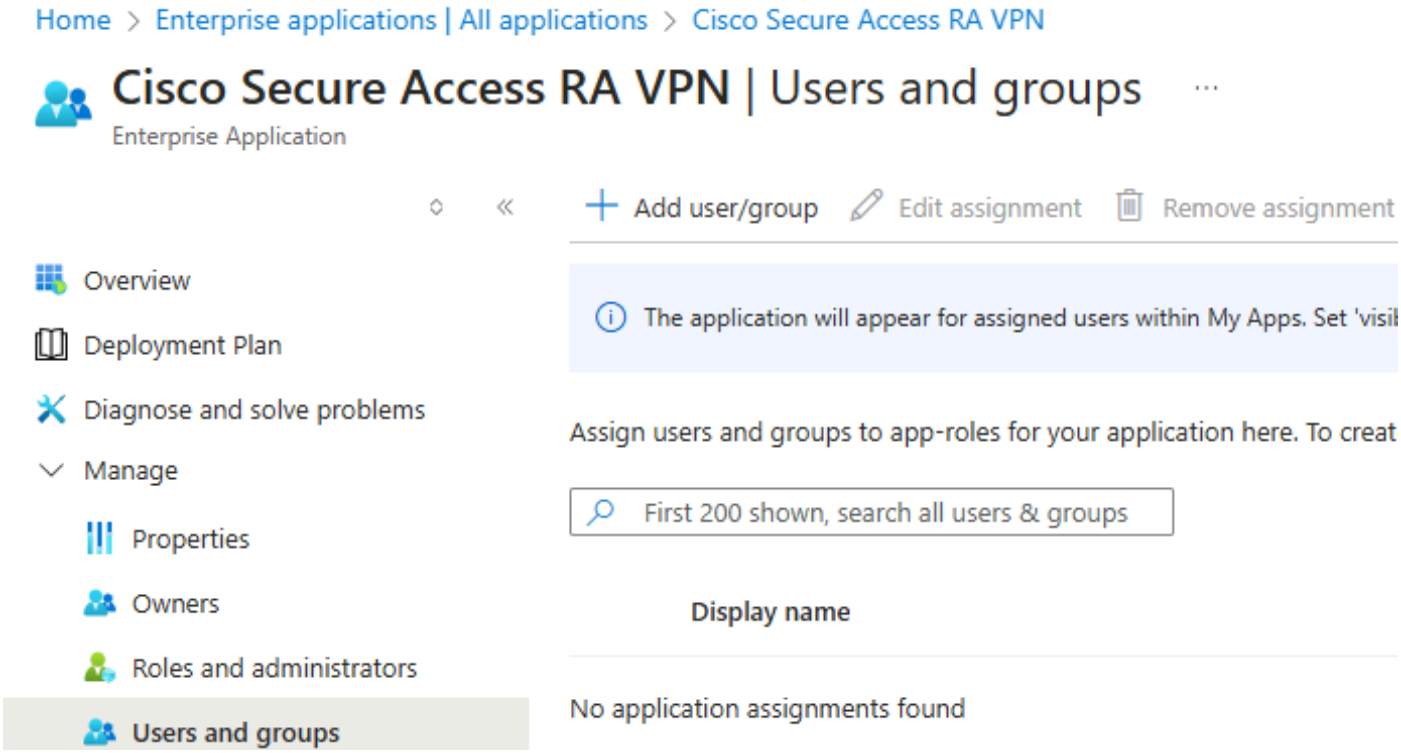
3. Wijzig de naam van de toepassing.
   Eigenschappen > Naam



De naam van de toepassing wijzigen

4. Wijs in de Enterprise-toepassing de gebruikers toe om zich te laten verifiëren met behulp van de AnyConnect VPN.

Gebruikers en groepen toewijzen > + Gebruiker/groep toevoegen > Toewijzen

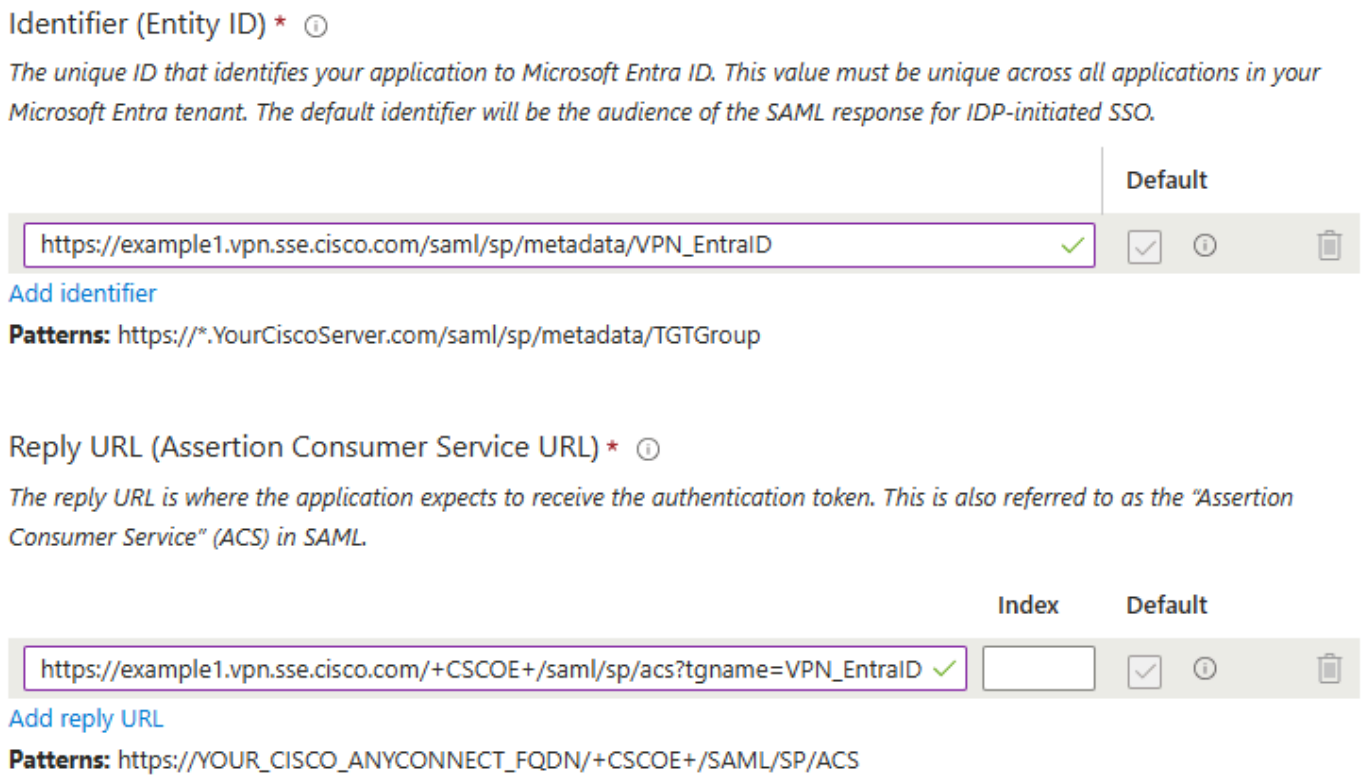


Toegewezen gebruikers/groepen

5. Klik op Eenmalige aanmelding en configureer de SAML-parameters. Hier gebruiken we de FQDN gekopieerd in stap 1, en ook de VPN-profielnaam die u configureert in "Configuratie Cisco Secure Access" later in stap 2.

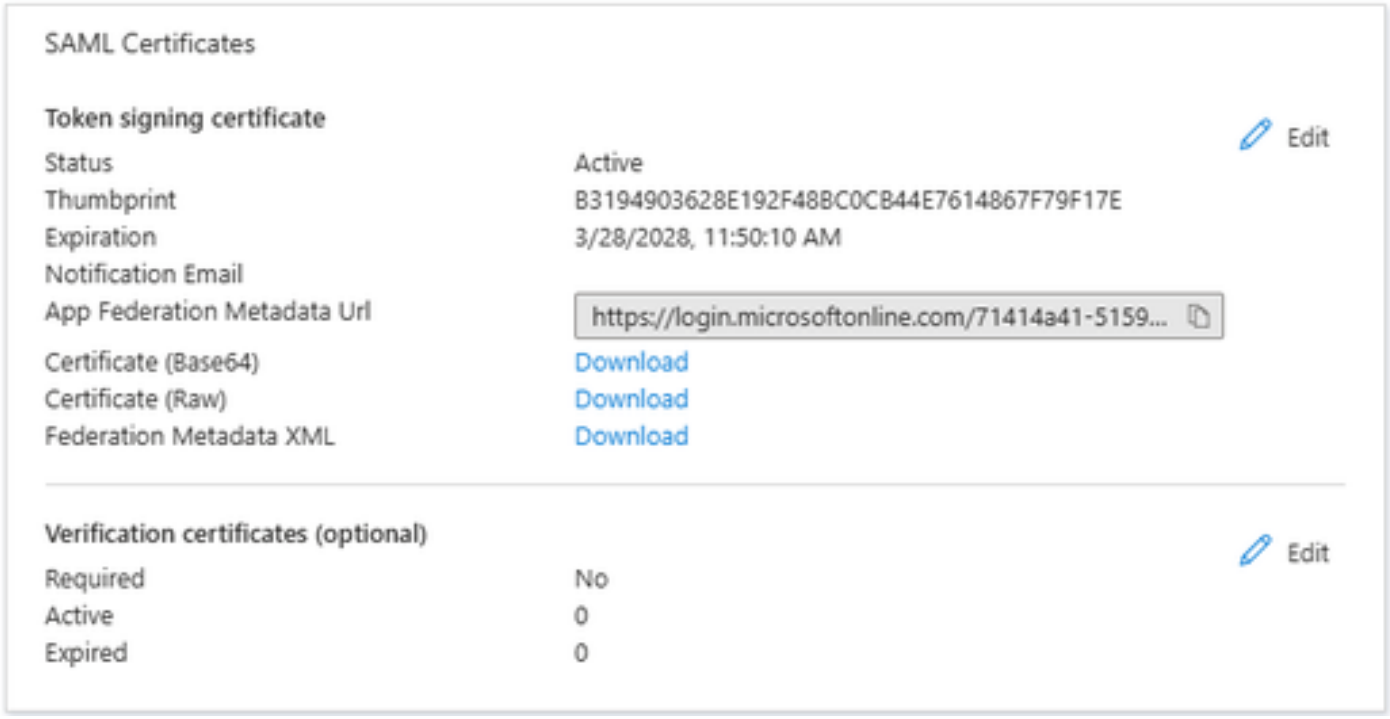
Als u VPN Global FQDN bijvoorbeeld example1.vpn.sse.cisco.com gebruikt en uw Cisco Secure Access VPN-profielnaam VPN_EntraID is, zijn de waarden voor (Entity ID) en de Reply URL (Assertion Consumer Service URL):

Identificatiecode (Entiteit-ID): https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID
Beantwoord-URL (Bewering Consumer Service-URL): https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=VPN_EntraID



SAML-parameters in Azure

6. Download de Federation Metadata XML.



Cisco Secure Access-configuratie

1. Meld u aan bij het Cisco Secure Access-dashboard en voeg een IP-pool toe.

Verbinding maken > Connectiviteit voor eindgebruikers > Virtueel particulier netwerk > IP-pool toevoegen

Regio: Selecteer de regio waar uw RA VPN wordt geïmplementeerd.
Display name: De naam voor de VPN IP-pool.
DNS-server: maken of toewijzen van de DNS-server die gebruikers gebruiken voor DNS-resolutie zodra ze verbinding hebben gemaakt.
Systeem-IP-pool: Gebruikt door Secure Access voor functies zoals Radius-verificatie, is het verificatieverzoek afkomstig van een IP binnen dit bereik.
IP-pool: voeg een nieuwe IP-pool toe en geef aan welke IP-adressen gebruikers krijgen wanneer ze verbinding maken met de RA VPN.

Setup VPN profiles

No VPN profiles added. To configure VPN profiles, you must first setup IP pools and then add profiles that map to users. Help

Add IP Pool

VPN-profiel toevoegen

Parameters

Edit this IP pool's parameters including its mapped region, DNS servers, and IP addresses

Region

Canada (Central)

Display name

RA VPN

DNS Server

DNS (208.67.222.222)

+ Add

DDNS Servers updates

System IP Pool

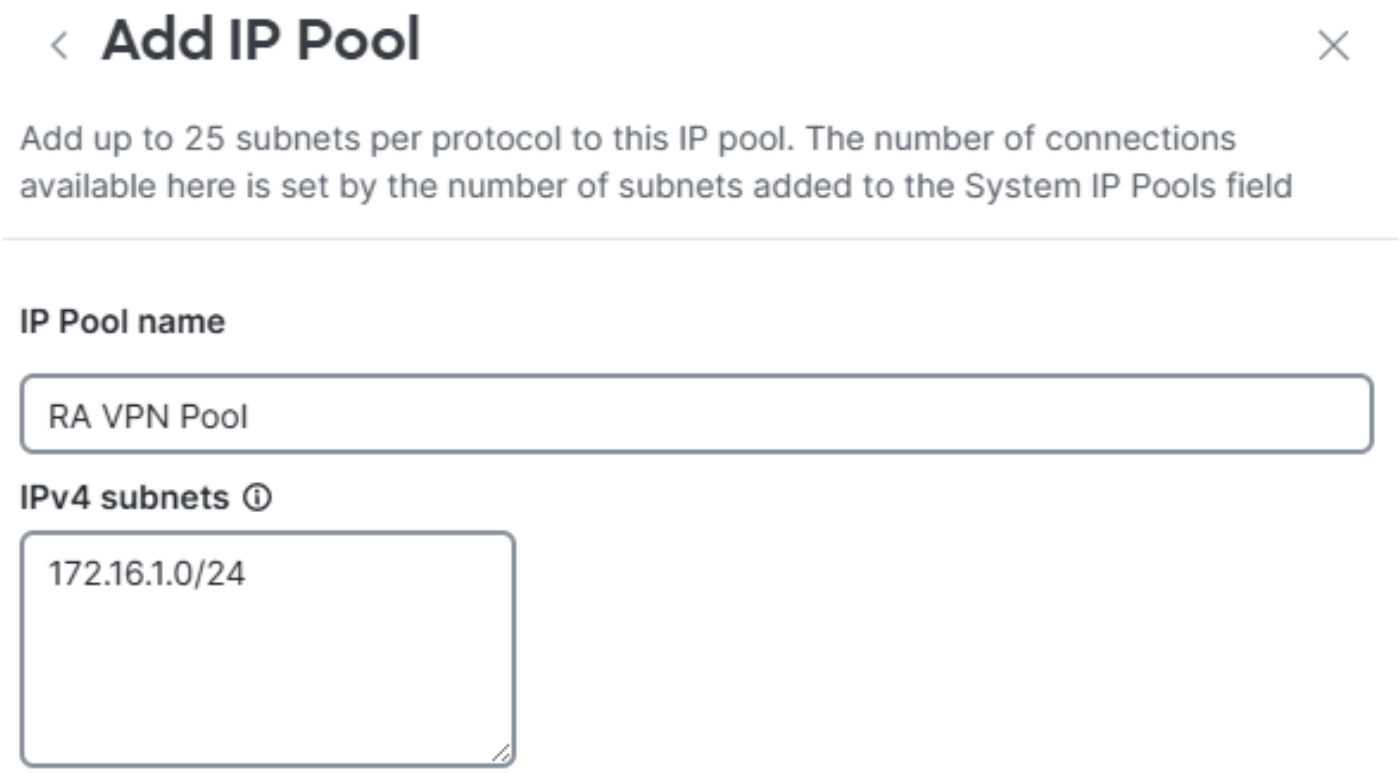
172.16.2.0/24

IP Pools

Add the IP pools this region will use. You can add a maximum of 25 IPV4 and 25 IPV6 subnets per IP pool. Help

+ Add

Configuratie van IP-pool - Deel 1

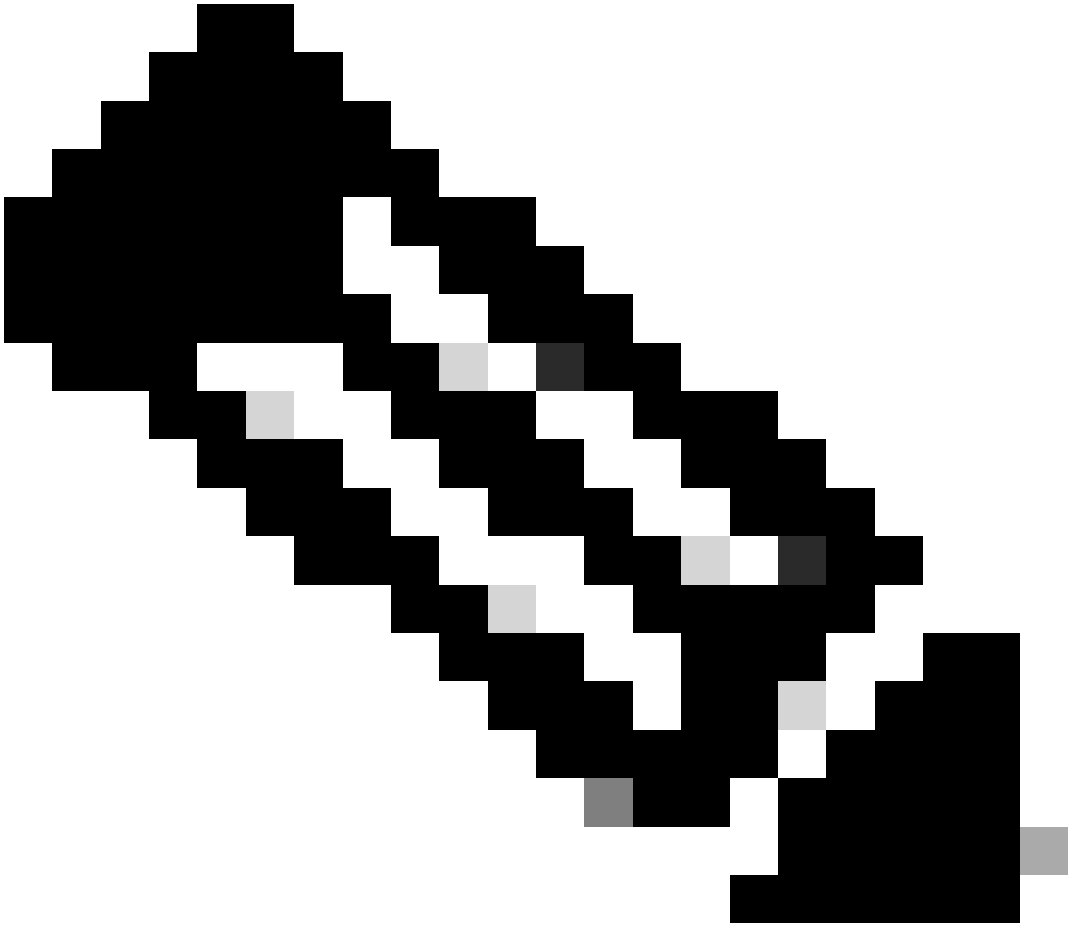


Configuratie van IP-pool - Deel 2

2. Voeg een VPN-profiel toe.

Verbinding maken > Connectiviteit van eindgebruiker > Virtueel privé-netwerk > VPN + profiel

Algemene instellingen

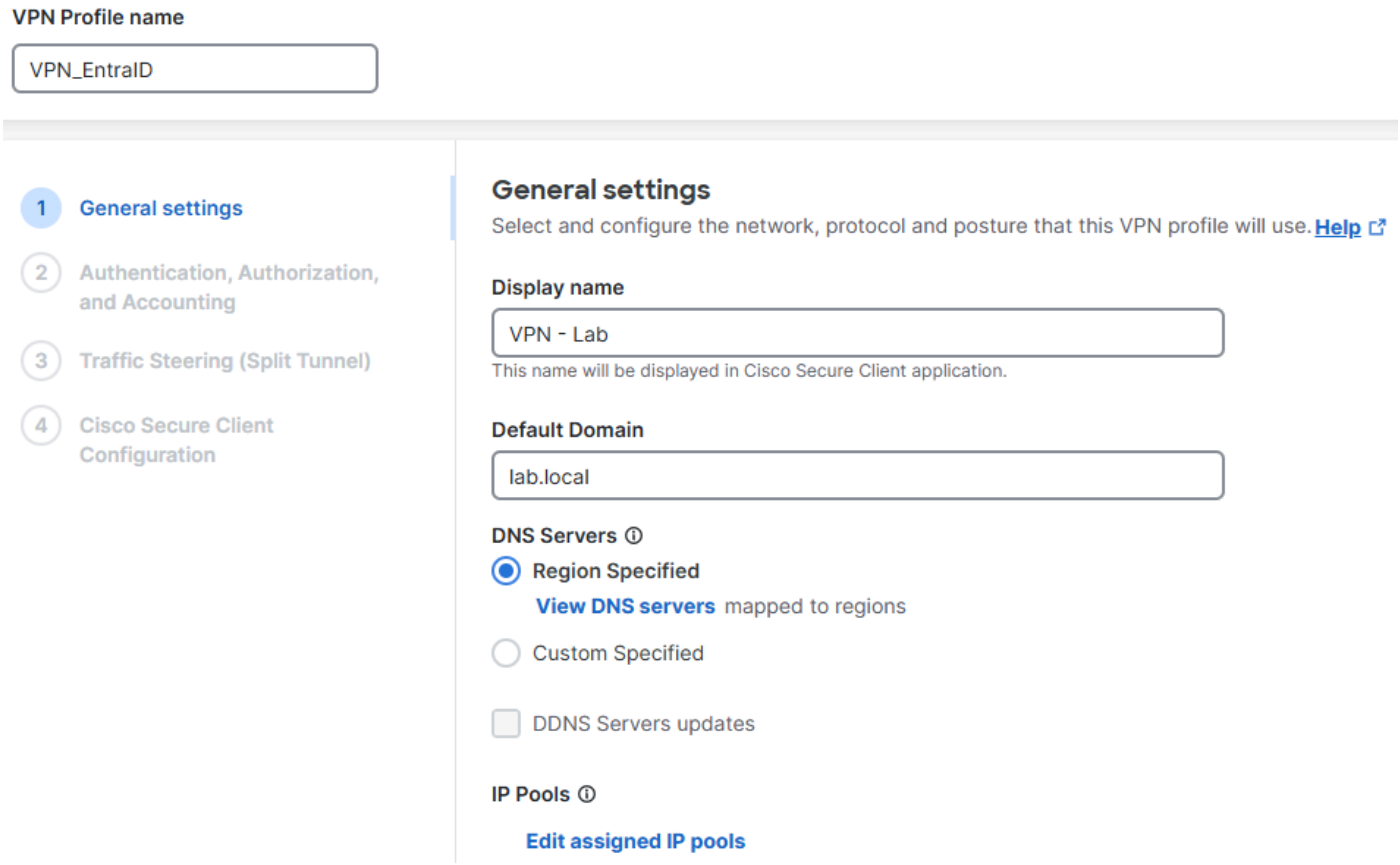


> Opmerking: De naam van het VPN-profiel moet overeenkomen met de naam die u in "Configuration Azure" in stap 5 hebt geconfigureerd. In deze configuratiehandleiding hebben we VPN_EntraID gebruikt, dus we configureren hetzelfde in Cisco Secure Access als de VPN-profielnaam.

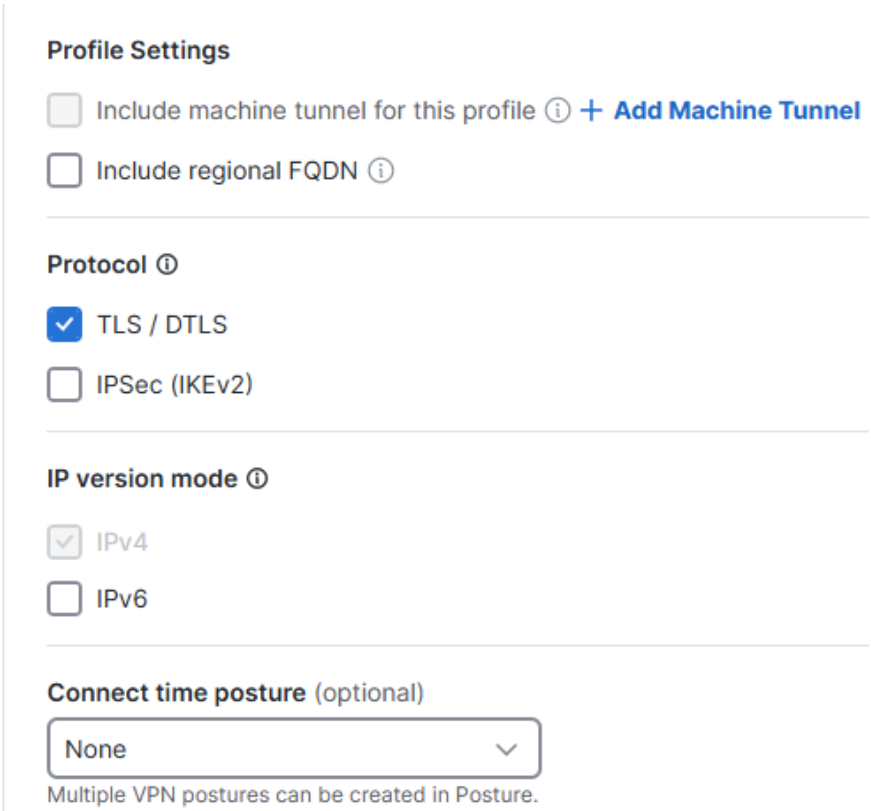
VPN-profielnaam: Naam voor dit VPN-profiel, alleen zichtbaar in het dashboard.

Display name: Naam eindgebruikers zie in het keuzemenu 'Secure Client - Anyconnect' (Beveiligde client - Anyconnect), zie wanneer u verbinding maakt met dit RA VPN-profiel.
Standaarddomein: Domeingebruikers worden eenmaal verbonden met de VPN.
DNS-servers: DNS-server de VPN-gebruikers krijgen eenmaal verbonden met de VPN.
  Regio opgegeven: gebruikt de DNS-server die is gekoppeld aan de VPN IP-pool.
  Aangepast opgegeven: u kunt handmatig de gewenste DNS toewijzen.
IP-pools: IP's die de gebruikers krijgen toegewezen zodra ze met de VPN zijn verbonden.
Profielinstellingen: Dit VPN-profiel voor Machine Tunnel opnemen of regionale FQDN opnemen zodat de eindgebruiker de regio selecteert waarmee hij verbinding wil maken (afhankelijk van de geïmplementeerde IP-pools).

Protocollen: Selecteer het protocol dat u wilt dat uw VPN-gebruikers gebruiken voor het tunnelen van het verkeer.
Verbindingstijdhouding (optioneel): indien nodig om VPN Posture te doen op het moment van verbinding. Meer informatie hier



VPN-profielconfiguratie - Deel 1

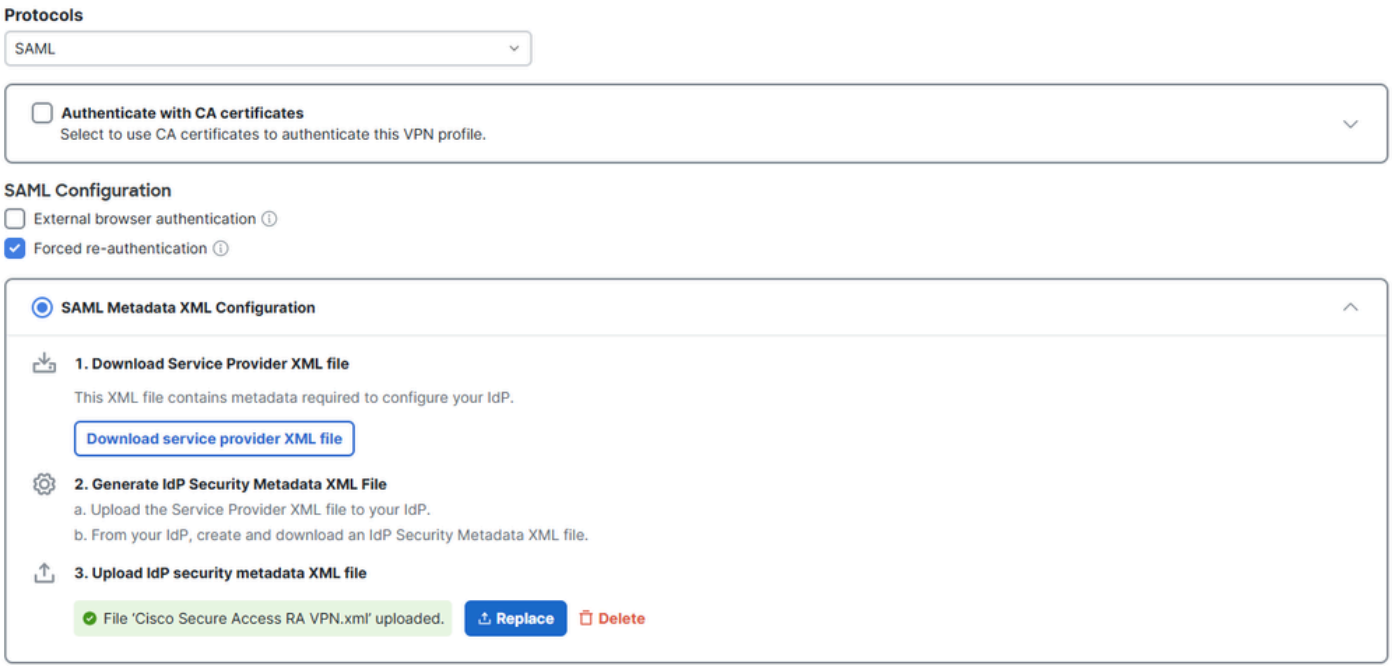


Verificatie, autorisatie en accounting

Protocollen: Selecteer SAML.

Authenticatie met CA-certificaten: Als u wilt authenticeren met behulp van een SSL-certificaat en autoriseren tegen een IdP SAML-provider.
Herverificatie forceren: dwingt een herverificatie af wanneer een VPN-verbinding wordt gemaakt. Gedwongen herauthenticatie is gebaseerd op Session Timeout. Dit kan worden onderworpen aan de SAML IdP-instellingen (Azure in dit geval).

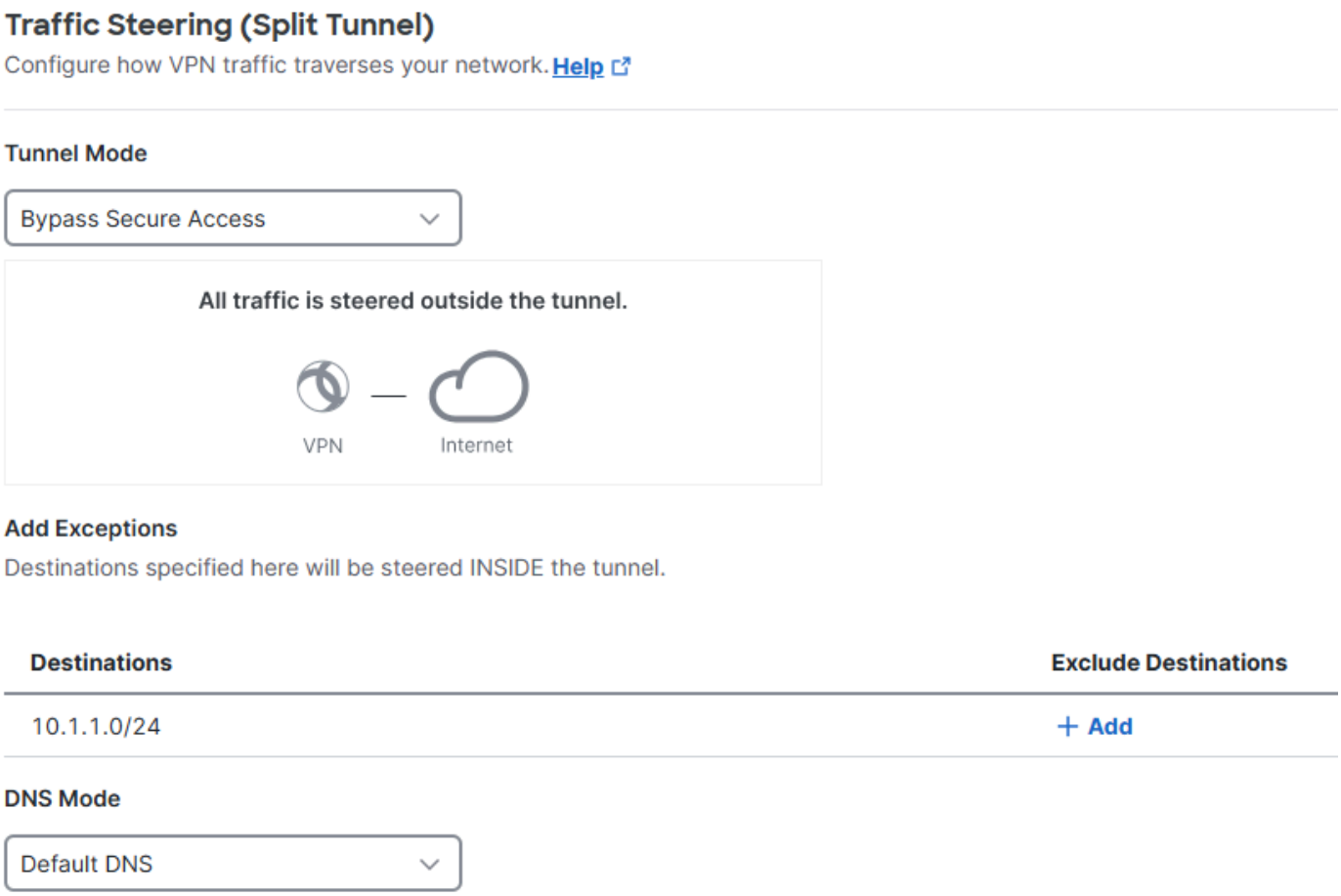
Upload het XML-bestand Federation Metadata XML-bestand gedownload in "Configure Azure" in stap 6.



SAML Config

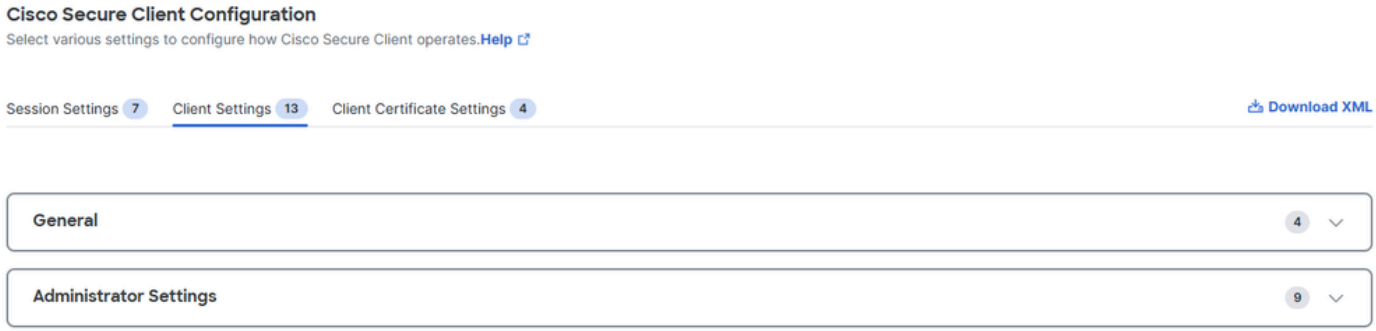
verkeerssturing (split tunnel)

Tunnelmodus:
Verbinding maken met beveiligde toegang: al het verkeer wordt verzonden via de tunnel (alle tunnels).
Veilige toegang omzeilen: Alleen specifiek verkeer dat is gedefinieerd in het gedeelte Uitzonderingen is getunneld (Split Tunnel).
DNS-modus:
Standaard DNS: Alle DNS-query's worden verplaatst via de DNS-servers die zijn gedefinieerd door het VPN-profiel. In het geval van een negatieve respons kunnen de DNS-query's ook naar de DNS-servers gaan die op de fysieke adapter zijn geconfigureerd.
Tunnel All DNS: Tunnels alle DNS-queries via de VPN.
Splitsen van DNS: Alleen specifieke DNS-query's gaan door het VPN-profiel, afhankelijk van de onderstaande domeinen.



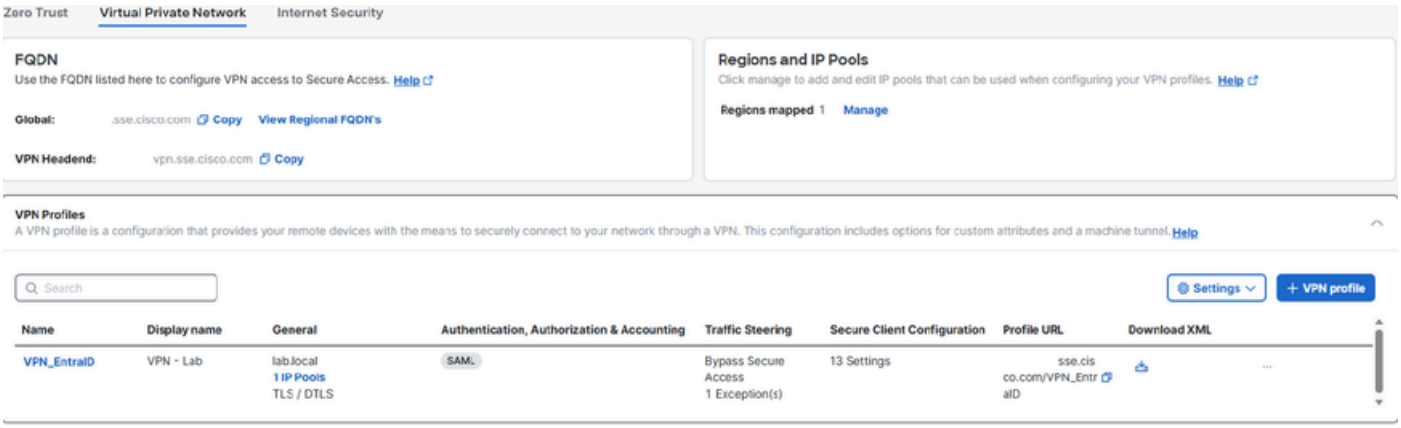
verkeersstuurconfiguratie

Cisco Secure Client Configuration
In het kader van deze handleiding configureren we geen van deze geavanceerde instellingen. Geavanceerde functies kunnen hier worden geconfigureerd, bijvoorbeeld: TND, Always-On, Certificate Matching, Local LAN Access, enzovoort. Sla de instellingen hier op.



Geavanceerde instellingen

3. Uw VPN-profiel moet er zo uitzien. U kunt het xml-profiel downloaden en vooraf implementeren bij de eindgebruikers (onder "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile") om de VPN te gebruiken, of hen de profiel-URL geven die moet worden ingevoerd in de Cisco Secure Client - AnyConnect VPN UI.



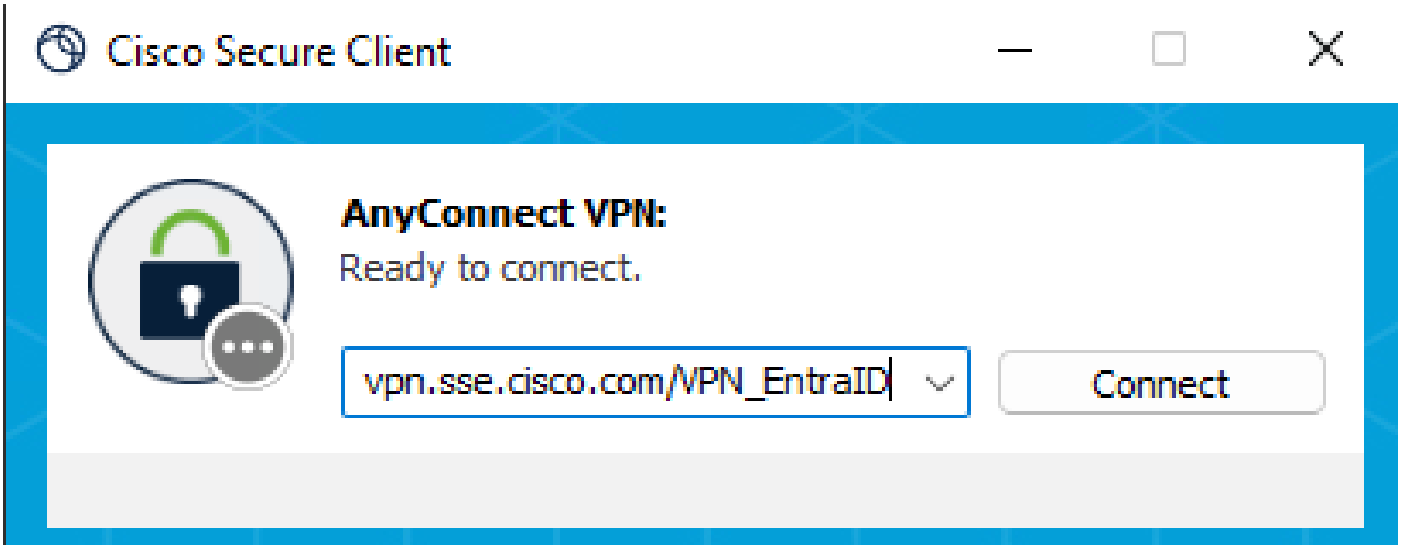
Globale FQDN en profiel-URL

Verifiëren

Op dit punt moet uw RA VPN-configuratie klaar zijn voor testen.
Merk op dat de eerste keer dat de gebruikers verbinding maken, ze het profiel-URL-adres moeten krijgen of het xml-profiel vooraf op hun pc's moeten implementeren onder "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile", de VPN-service opnieuw moeten starten en ze in het vervolgkeuzemenu de optie moeten zien om verbinding te maken met dit VPN-profiel.

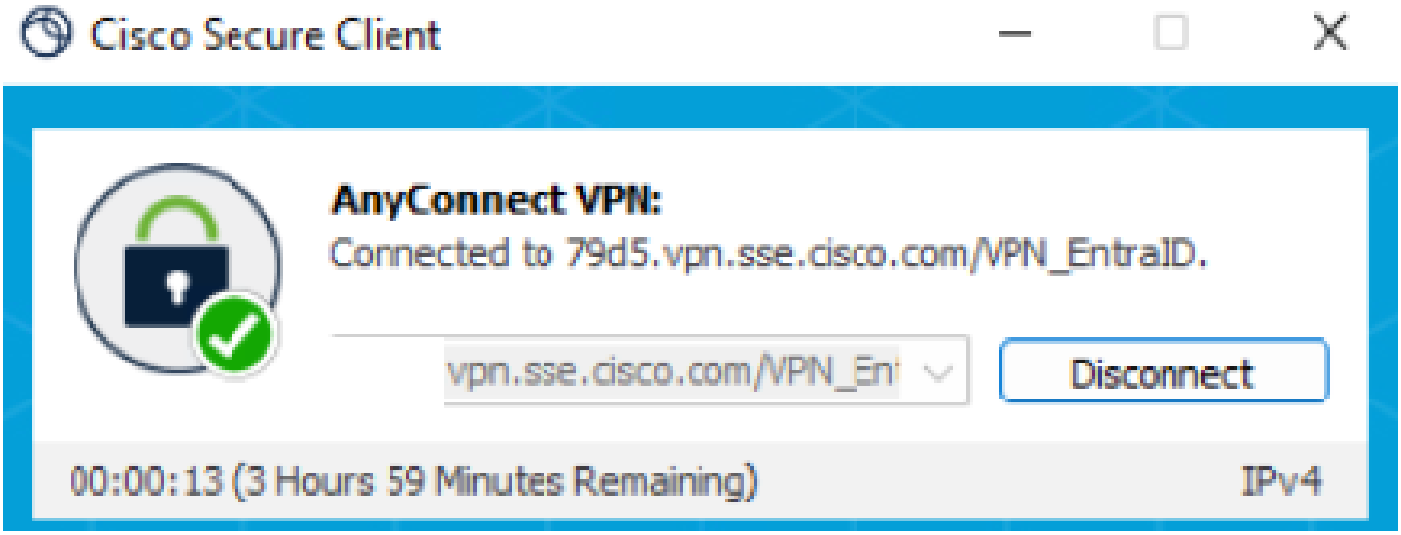
In dit voorbeeld geven we het profiel-URL-adres aan de gebruiker voor de eerste poging tot verbinding.

Voorafgaand aan de eerste verbinding:



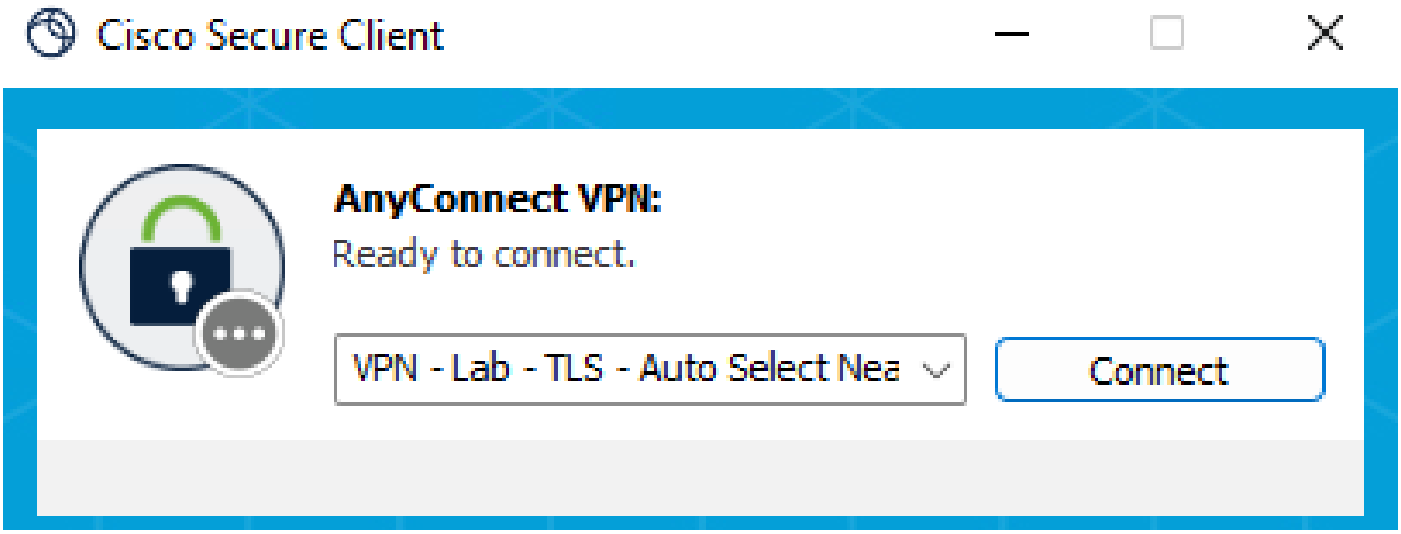
Eerdere VPN-verbinding

Voer uw referenties in en maak verbinding met de VPN:



Verbonden met VPN

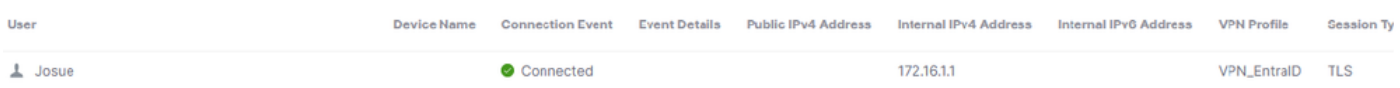
Nadat u de eerste keer verbinding hebt gemaakt, moet u nu in het vervolgkeuzemenu de optie kunnen zien om verbinding te maken met het VPN-Lab-VPN-profiel:



Na de eerste VPN-verbinding

Controleer in de logboeken voor externe toegang dat de gebruiker verbinding kon maken:

Monitor > Logboek externe toegang



Logboeken in Cisco Secure Access

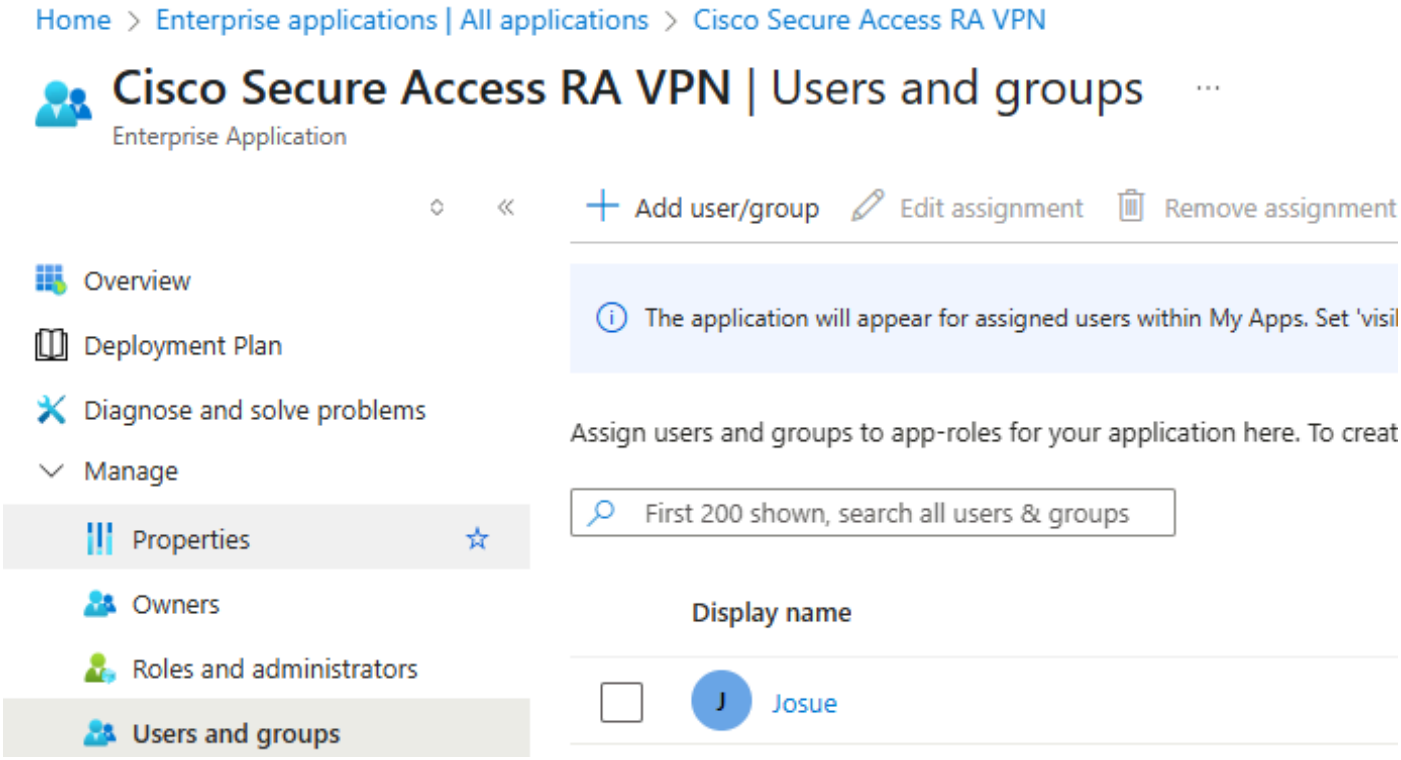
Probleemoplossing

Hier wordt de basis probleemoplossing beschreven die kan worden uitgevoerd voor een aantal veelvoorkomende problemen:

Azure

Zorg er in Azure voor dat de gebruikers zijn toegewezen aan de Enterprise Application die is gemaakt voor de verificatie tegen Cisco Secure Access:

Home > Bedrijfstoepassingen > Cisco Secure Access RA VPN > Beheren > Gebruikers en groepen

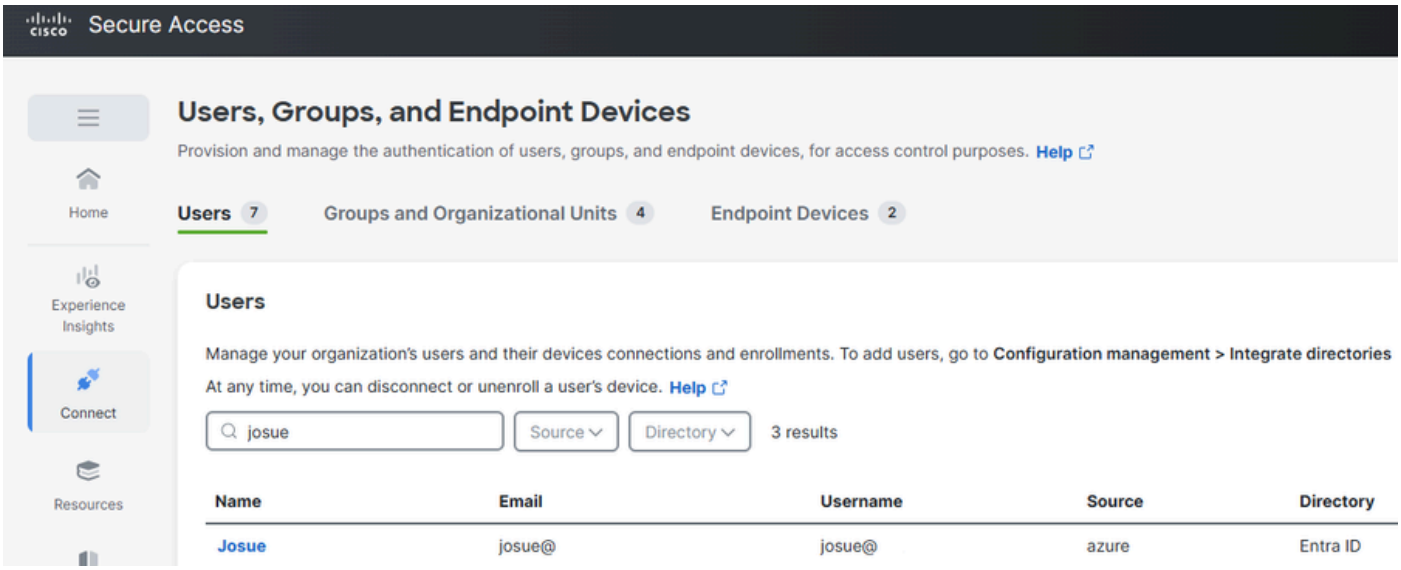


Toewijzing van gebruikers controleren

Cisco Secure Access

Zorg er in Cisco Secure Access voor dat u de gebruikers hebt voorzien die verbinding mogen maken via RA VPN en dat ook de gebruikers die zijn voorzien in Cisco Secure Access (onder gebruikers, groepen en eindpuntapparaten) overeenkomen met de gebruikers in Azure (de gebruikers die zijn toegewezen in de bedrijfstoepassing).

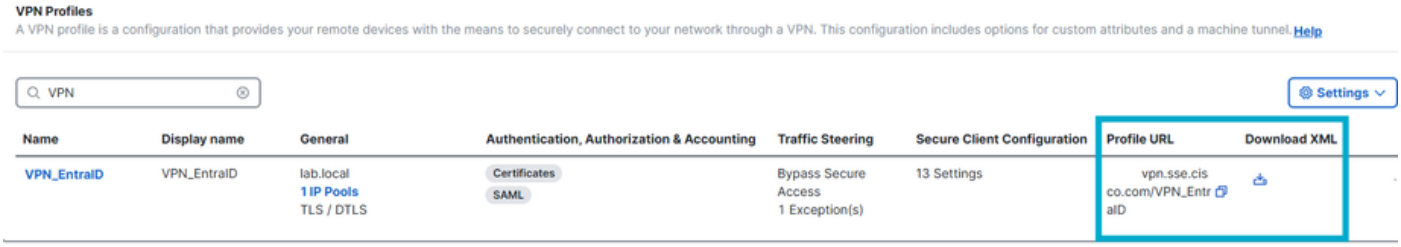
Verbinden > Gebruikers, groepen en eindpuntapparaten



Gebruikers in Cisco Secure Access

Controleer of de gebruiker het juiste XML-bestand op de pc heeft ontvangen of dat de gebruiker de profiel-URL heeft gekregen, zoals vermeld in de stap "Verifiëren".

Verbinding maken > Connectiviteit voor eindgebruikers > Virtual Private Network



Profiel URL en .xml profiel

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.