

Cisco Secure Access configureren voor RA VPNaaS met Entra ID

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Azure Configuration](#)

[Cisco Secure Access-configuratie](#)

[Verifiëren](#)

[Probleemoplossing](#)

[Azure](#)

[Cisco Secure Access](#)

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



The screenshot shows the 'End User Connectivity' section of the Cisco Secure Access dashboard. It has three tabs: 'Zero Trust', 'Virtual Private Network' (which is selected and underlined), and 'Internet Security'. Under the 'Virtual Private Network' tab, there is a section titled 'FQDN' with the text: 'Use the FQDN listed here to configure VPN access to Secure Access. [Help](#)'. Below this, it shows 'Global: .vpn.sse.cisco.com' with a 'Copy' button and a link to 'View Regional FQDN's'.

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

Cisco Secure Firewall - Secure Client (forme...



Got feedback?

Logo ⓘ



Name ★ ⓘ

Cisco Secure Firewall - Secure Client (formerly AnyConnect) auth...

Publisher ⓘ

Cisco Systems, Inc.

Provisioning ⓘ

Automatic provisioning is not supported

Single Sign-On Mode ⓘ

SAML-based Sign-on
Linked Sign-on

URL ⓘ

<https://www.cisco.com/go/securefirewall>

[Read our step-by-step Cisco Secure Firewall - Secure Client \(formerly AnyConnect\) authentication integration tutorial](#)

Use Microsoft Entra ID to manage user access and enable single sign-on with the Cisco Secure Firewall for Secure Client (formerly AnyConnect) SAML authentication.

App maken in Azure

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

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional properties on the [application registration](#).

Enabled for users to sign-in?  Yes No

Name *  

Homepage URL  

Logo  

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

[Home](#) > [Enterprise applications | All applications](#) > [Cisco Secure Access RA VPN](#)



Cisco Secure Access RA VPN | Users and groups

Enterprise Application

 Add user/group
  Edit assignment
  Remove assignment

 Overview

 Deployment Plan

 Diagnose and solve problems

 Manage

 Properties

 Owners

 Roles and administrators

 **Users and groups**

 The application will appear for assigned users within My Apps. Set 'visi

Assign users and groups to app-roles for your application here. To creat

 First 200 shown, search all users & groups

Display name

No application assignments found

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?tname=VPN_EntraID

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID ✓	☒ ⓘ

[Add identifier](#)

Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tname=VPN_EntraID ✓		☒ ⓘ

[Add reply URL](#)

Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS

SAML-parameters in Azure

6. Download de Federation Metadata XML.

SAML Certificates

Token signing certificate

Status

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

Active

B3194903628E192F48BC0CB44E7614867F79F17E

3/28/2028, 11:50:10 AM

[https://login.microsoftonline.com/71414a41-5159...](#)

[Download](#)

[Download](#)

[Download](#)

Edit

Verification certificates (optional)

Required

Active

Expired

No

0

0

Edit

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](#)

< Add IP Pool



Add up to 25 subnets per protocol to this IP pool. The number of connections available here is set by the number of subnets added to the System IP Pools field

IP Pool name

RA VPN Pool

IPv4 subnets ⓘ

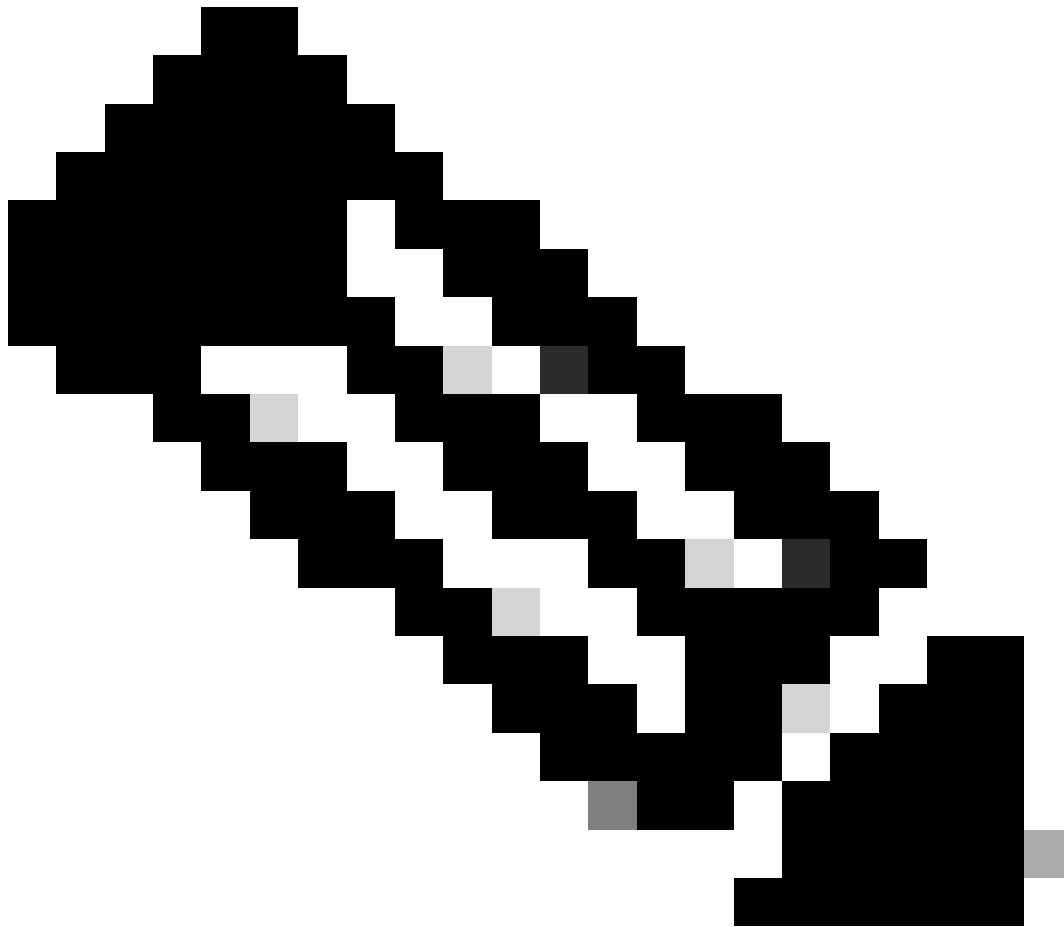
172.16.1.0/24

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 Profile name

VPN_EntraID

1 General settings

2 Authentication, Authorization, and Accounting

3 Traffic Steering (Split Tunnel)

4 Cisco Secure Client Configuration

General settings

Select and configure the network, protocol and posture that this VPN profile will use. [Help](#)

Display name

VPN - Lab

This name will be displayed in Cisco Secure Client application.

Default Domain

lab.local

DNS Servers ⓘ

☒ Region Specified

[View DNS servers](#) mapped to regions

☐ Custom Specified

☐ DDNS Servers updates

IP Pools ⓘ

[Edit assigned IP pools](#)

VPN-profielconfiguratie - Deel 1

Profile Settings

☐ Include machine tunnel for this profile ⓘ [+ Add Machine Tunnel](#)

☐ Include regional FQDN ⓘ

Protocol ⓘ

☒ TLS / DTLS

☐ IPsec (IKEv2)

IP version mode ⓘ

☒ IPv4

☐ IPv6

Connect time posture (optional)

None

Multiple VPN postures can be created in Posture.

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.

Protocols

SAML

☐ **Authenticate with CA certificates**
Select to use CA certificates to authenticate this VPN profile.

SAML Configuration

☐ External browser authentication ⓘ

☒ Forced re-authentication ⓘ

SAML Metadata XML Configuration

1. **Download Service Provider XML file**
This XML file contains metadata required to configure your IdP.
[Download service provider XML file](#)

2. **Generate IdP Security Metadata XML File**
a. Upload the Service Provider XML file to your IdP.
b. From your IdP, create and download an IdP Security Metadata XML file.

3. **Upload IdP security metadata XML file**
File 'Cisco Secure Access RA VPN.xml' uploaded. [Replace](#) [Delete](#)

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.

Traffic Steering (Split Tunnel)

Configure how VPN traffic traverses your network. [Help](#)

Tunnel Mode

Bypass Secure Access

All traffic is steered outside the tunnel.



Add Exceptions

Destinations specified here will be steered INSIDE the tunnel.

Destinations

10.1.1.0/24

Exclude Destinations

[+ Add](#)

DNS Mode

Default DNS

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.

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings 7

Client Settings 13

Client Certificate Settings 4

[Download XML](#)

General

4

Administrator Settings

9

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.

Zero Trust
Virtual Private Network
Internet Security

FQDN

Use the FQDN listed here to configure VPN access to Secure Access. [Help](#)

Global: `sse.cisco.com` [Copy](#) [View Regional FQDN's](#)

VPN Headend: `vpn.sse.cisco.com` [Copy](#)

Regions and IP Pools

Click manage to add and edit IP pools that can be used when configuring your VPN profiles. [Help](#)

Regions mapped 1 [Manage](#)

VPN Profiles

A VPN profile is a configuration that provides your remote devices with the means to securely connect to your network through a VPN. This configuration includes options for custom attributes and a machine tunnel. [Help](#)

[Settings](#)
[+ VPN profile](#)

Name	Display name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
VPN_EntraID	VPN - Lab	lab.local 1 IP Pools TLS / DTLS	SAML	Bypass Secure Access 1 Exception(s)	13 Settings	<code>sse.cisco.com/VPN_EntraID</code> Copy	Download XML

Globale FQDN en profiel-URL

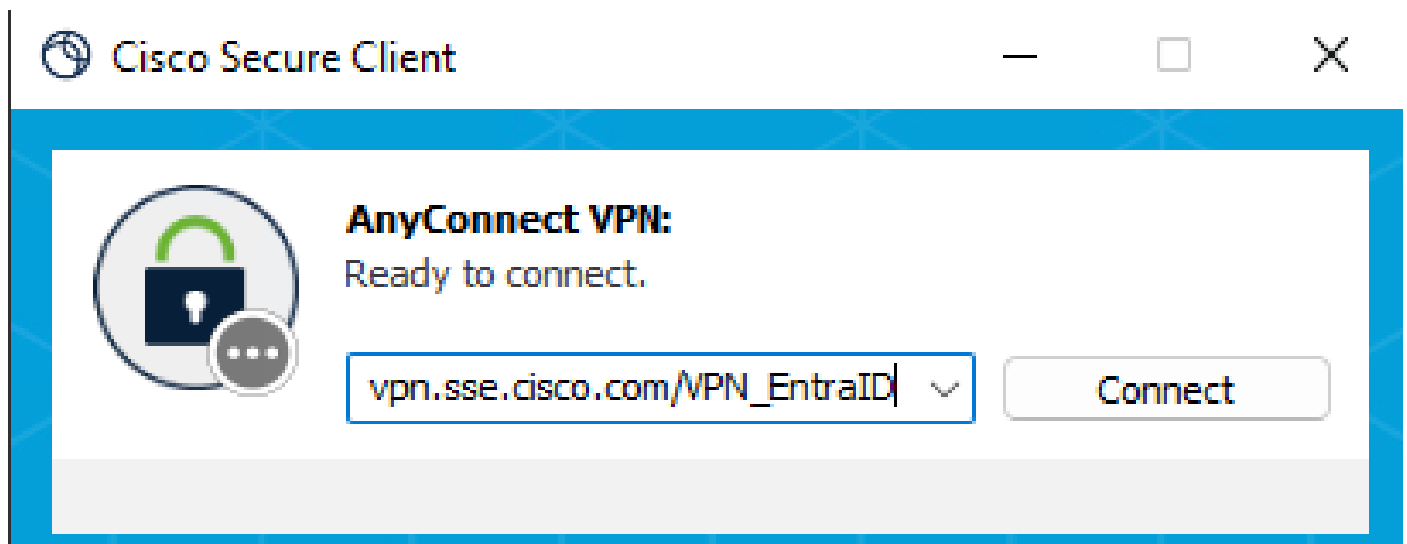
Verifiëren

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.

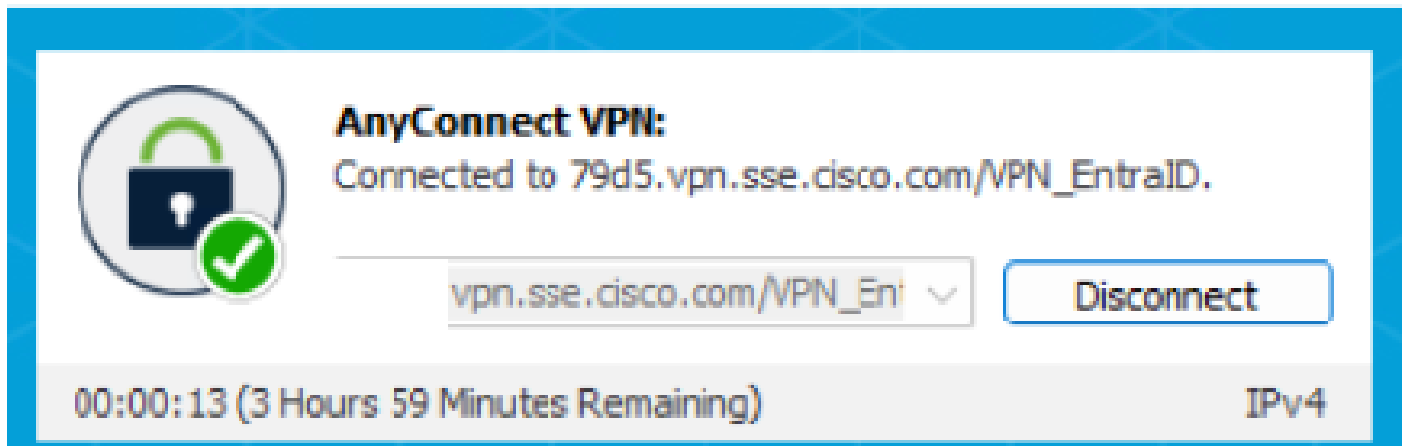
In dit voorbeeld geven we het profiel-URL-adres aan de gebruiker voor de eerste poging tot verbinding.

Voorafgaand aan de eerste verbinding:



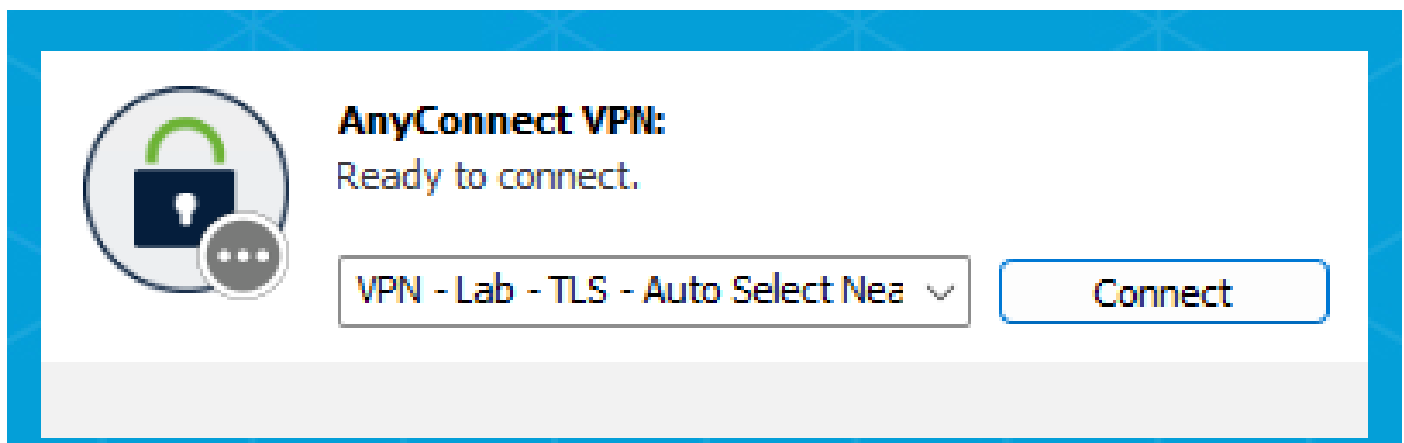
Eerdere VPN-verbinding

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

User	Device Name	Connection Event	Event Details	Public IPv4 Address	Internal IPv4 Address	Internal IPv6 Address	VPN Profile	Session Ty
Josue		Connected			172.16.1.1		VPN_EntraID	TLS

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 > Bedrijfstoeepassingen > Cisco Secure Access RA VPN > Beheren > Gebruikers en groepen

Home > Enterprise applications | All applications > Cisco Secure Access RA VPN

Cisco Secure Access RA VPN | Users and groups ...

Enterprise Application

 Add user/group  Edit assignment  Remove assignment

-  Overview
-  Deployment Plan
-  Diagnose and solve problems
-  Manage
 -  Properties 
 -  Owners
 -  Roles and administrators
 -  Users and groups

 The application will appear for assigned users within My Apps. Set 'visi

Assign users and groups to app-roles for your application here. To creat

 First 200 shown, search all users & groups

	Display name
☐	 Josue

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 bedrijfstoeepassing).

Verbinden > Gebruikers, groepen en eindpuntapparaten

Secure Access

☰

Home

Experience Insights

Connect

Resources

Users, Groups, and Endpoint Devices

Provision and manage the authentication of users, groups, and endpoint devices, for access control purposes. [Help](#)

Users 7

Groups and Organizational Units 4

Endpoint Devices 2

Users

Manage your organization's users and their devices connections and enrollments. To add users, go to **Configuration management > Integrate directories**. At any time, you can disconnect or unenroll a user's device. [Help](#)

Source ▼

Directory ▼

3 results

Name	Email	Username	Source	Directory
Josue	josue@	josue@	azure	Entra ID

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

VPN Profiles

A VPN profile is a configuration that provides your remote devices with the means to securely connect to your network through a VPN. This configuration includes options for custom attributes and a machine tunnel. [Help](#)

Settings ▼

Name	Display name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
VPN_EntraID	VPN_EntraID	lab.local 1 IP Pools TLS / DTLS	Certificates SAML	Bypass Secure Access 1 Exception(s)	13 Settings	vpn.sse.cisco.com/VPN_EntraID	

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.