

Konfigurieren von Cisco Secure Access für RA VPNaaS mit Entra-ID

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Azure-Konfiguration](#)

[Cisco Secure Access - Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Azure](#)

[Sicherer Zugriff von Cisco](#)

Einleitung

In diesem Dokument wird Schritt für Schritt beschrieben, wie Sie RA VPN auf Cisco Secure Access für die Authentifizierung anhand der Entra-ID konfigurieren.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse mit Azure/Entra-ID.
- Umfassende Expertise mit Cisco Secure Access

Anforderungen

Diese Anforderungen müssen erfüllt sein, bevor weitere Schritte unternommen werden können:

- Zugriff auf Ihr Cisco Secure Access Dashboard als Volladministrator
- Zugriff auf Azure als Administrator
- [Die Benutzerbereitstellung für](#) Cisco Secure Access wurde bereits abgeschlossen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Access-Dashboard

- Microsoft Azure-Portal
- Cisco Secure Client AnyConnect VPN Version 5.1.8.105

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Azure-Konfiguration

1. Melden Sie sich beim Cisco Secure Access Dashboard an, und kopieren Sie den globalen VPN-FQDN. Wir verwenden diesen FQDN in der Azure Enterprise-Anwendungskonfiguration.

Verbinden > Endbenutzerverbindungen > Virtuelles privates Netzwerk > FQDN > Global



End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust **Virtual Private Network** **Internet Security**

FQDN

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

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

Globaler VPN-FQDN

2. Melden Sie sich bei Azure an, und erstellen Sie eine Enterprise-Anwendung für die RA VPN-Authentifizierung. Sie können die vordefinierte Anwendung mit dem Namen "Cisco Secure Firewall - Secure Client (ehemals AnyConnect)-Authentifizierung" verwenden.

Startseite > Unternehmensanwendungen > Neue Anwendung > Cisco Secure Firewall - Secure Client (ehemals AnyConnect)-Authentifizierung > Erstellen

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 in Azure erstellen

3. Umbenennen der Anwendung

Eigenschaften > Name

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? ① Yes No

Name * ① 

Homepage URL ① 

Logo ① 

Umbenennen der Anwendung

4. Weisen Sie in der Enterprise-Anwendung die Benutzer zu, die sich mithilfe des AnyConnect VPN authentifizieren können.

Benutzer und Gruppen zuweisen > + Benutzer/Gruppe hinzufügen > Zuweisen

[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

① 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

Zugewiesene Benutzer/Gruppen

5. Klicken Sie auf Single Sign-on und konfigurieren Sie die SAML-Parameter. Hier verwenden wir den in Schritt 1 kopierten FQDN sowie den VPN-Profilnamen, den Sie in "Cisco Secure Access-Konfiguration" weiter unten in Schritt 2 konfigurieren.

Wenn Sie beispielsweise den globalen VPN-FQDN `example1.vpn.sse.cisco.com` und den Namen Ihres Cisco Secure Access VPN-Profiles `VPN_EntraID` verwenden, lauten die Werte für (Element-ID) und die Antwort-URL (Assertion Consumer Service-URL):

Kennung (Element-ID): https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID

Antwort-URL (Assertion 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-Parameter in Azure

6. Laden Sie die Verbundmetadaten-XML herunter.

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 - Konfiguration

1. Melden Sie sich bei Ihrem Cisco Secure Access-Dashboard an, und fügen Sie einen IP-Pool hinzu.

Verbinden > Endbenutzerverbindungen > Virtuelles privates Netzwerk > IP-Pool hinzufügen

Region: Wählen Sie die Region aus, in der Ihr RA VPN bereitgestellt werden soll.

Anzeigename: Der Name für den VPN-IP-Pool.

DNS-Server: Erstellen oder zuweisen Sie die DNS-Server-Benutzer, die für die DNS-Auflösung verwendet werden, sobald eine Verbindung hergestellt ist.

System-IP-Pool: Die Authentifizierungsanforderung wird von Secure Access für Funktionen wie Radius Authentication verwendet und bezieht sich auf eine IP-Adresse in diesem Bereich.

IP-Pool: Fügen Sie einen neuen IP-Pool hinzu, und geben Sie die IPs an, die Benutzer nach dem Herstellen der Verbindung mit dem RA VPN erhalten.



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-Profil hinzufügen

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 ⓘ

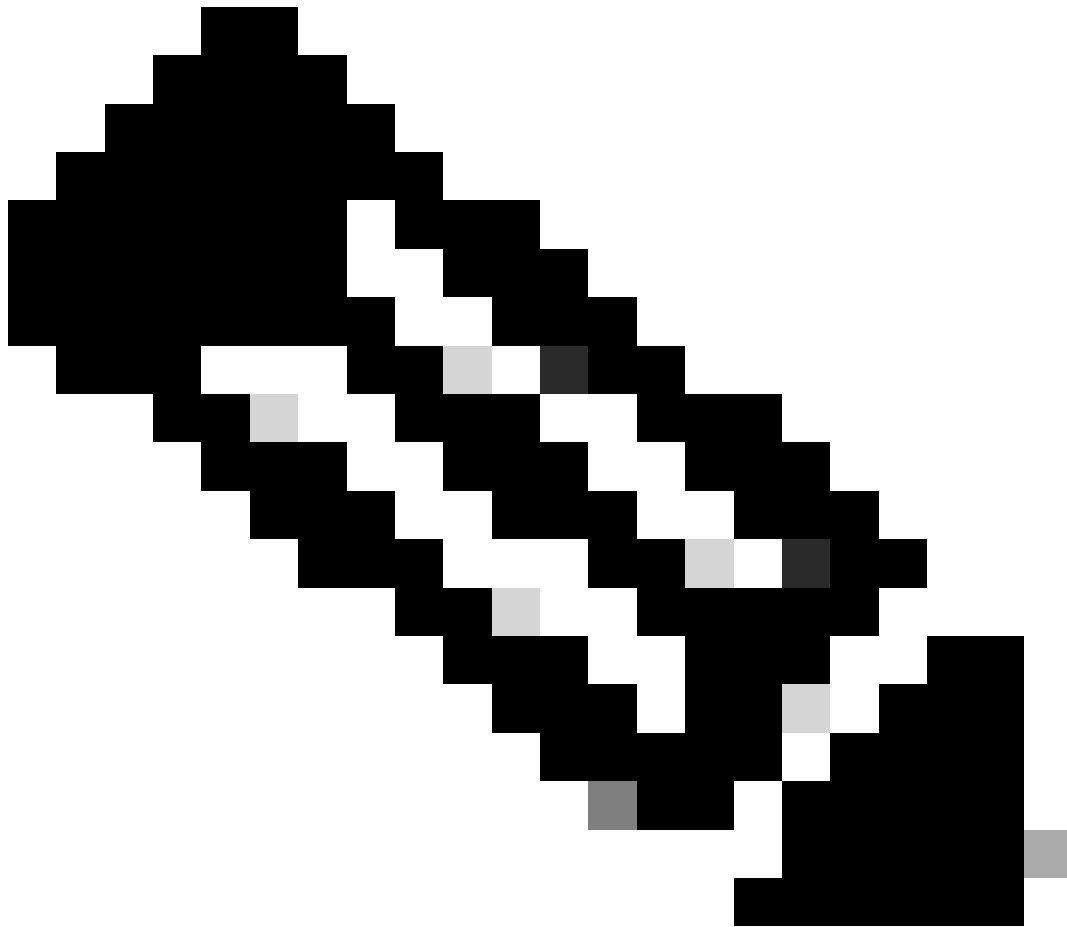
172.16.1.0/24

Konfiguration des IP-Pools - Teil 2

2. VPN-Profil hinzufügen

Verbinden > Endbenutzerverbindungen > Virtuelles privates Netzwerk > + VPN-Profil

Allgemeine Einstellungen



Anmerkung: Anmerkung: Der Name des VPN-Profiles muss mit dem Namen übereinstimmen, den Sie in "Configuration Azure" in Schritt 5 konfiguriert haben. In diesem Konfigurationsleitfaden wurde "VPN_EntraID" verwendet, daher konfigurieren wir in Cisco Secure Access denselben Namen wie "VPN Profile Name".

VPN-Profilname: Name für dieses VPN-Profil, nur im Dashboard sichtbar.

Anzeigename: Name der Endbenutzer siehe Dropdown-Menü "Secure Client - AnyConnect".
Siehe, wenn Sie eine Verbindung mit diesem RA VPN-Profil herstellen.

Standarddomäne: Domänenbenutzer erhalten eine Verbindung mit dem VPN.

DNS-Server: DNS-Server, den die VPN-Benutzer erhalten, sobald sie mit dem VPN verbunden sind.

Angegebene Region: Verwendet den DNS-Server, der dem VPN-IP-Pool zugeordnet ist.

Benutzerdefiniert: Sie können den gewünschten DNS manuell zuweisen.

IP-Pools: IPs, die Benutzern zugewiesen werden, sobald sie mit dem VPN verbunden sind.

Profileinstellungen: Aufnahme dieses VPN-Profiles für [Maschinentunnel](#) oder Einbeziehung des regionalen FQDN, sodass der Endbenutzer die Region auswählt, mit der er sich verbinden möchte

(abhängig von den bereitgestellten IP-Pools).

Protokolle: Wählen Sie das Protokoll aus, das Ihre VPN-Benutzer für das Tunneling des Datenverkehrs verwenden sollen.

Verbindungszeitstatus (optional): Falls erforderlich, [VPN-Status](#) zum Zeitpunkt der Verbindung ausführen. Weitere Informationen finden Sie 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

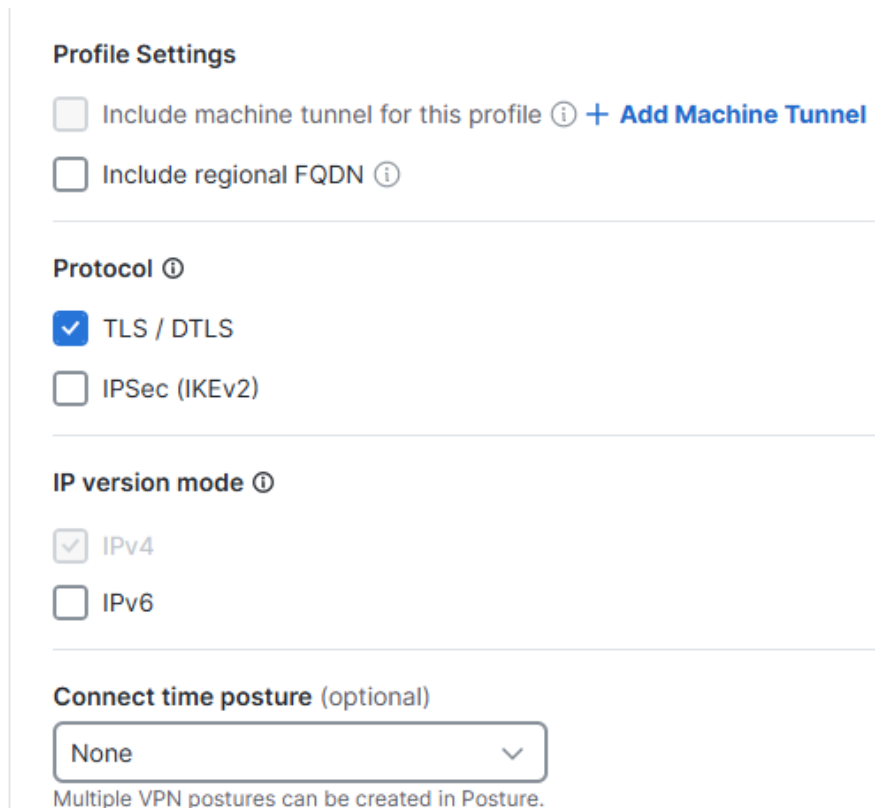
[View DNS servers](#) mapped to regions

☐ Custom Specified

☐ DDNS Servers updates

IP Pools ⓘ

[Edit assigned IP pools](#)



The screenshot shows a 'Profile Settings' configuration page. It includes several sections: 'Include machine tunnel for this profile' with a checkbox and a link to 'Add Machine Tunnel'; 'Include regional FQDN' with a checkbox; 'Protocol' with radio buttons for 'TLS / DTLS' (selected) and 'IPSec (IKEv2)'; 'IP version mode' with radio buttons for 'IPv4' (selected) and 'IPv6'; and 'Connect time posture (optional)' with a dropdown menu set to 'None'. A note at the bottom states 'Multiple VPN postures can be created in Posture.'

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.

VPN-Profilkonfiguration - Teil 2

Authentisierung, Ermächtigung und Buchhaltung

Protokolle: Wählen Sie SAML.

Authentifizierung mit Zertifizierungsstellenzertifikaten: Wenn Sie sich mithilfe eines SSL-Zertifikats authentifizieren und eine Autorisierung für einen IdP-SAML-Provider vornehmen möchten.

Erzwungene erneute Authentifizierung: Erzwingt eine erneute Authentifizierung, wenn eine VPN-Verbindung hergestellt wird. Die erzwungene erneute Authentifizierung basiert auf dem Sitzungstimeout. Dies könnte den SAML-IdP-Einstellungen unterworfen werden (in diesem Fall Azure).

Laden Sie die XML-Datei für die Verbundmetadaten-XML-Datei hoch, die in Schritt 6 unter "Azure konfigurieren" heruntergeladen wurde.

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-Konfiguration

Verkehrssteuerung (Split-Tunnel)

Tunnelmodus:

Verbindung mit sicherem Zugriff herstellen: Der gesamte Datenverkehr wird durch den Tunnel geleitet (Tunnel All).

Sicheren Zugriff umgehen: Nur der im Abschnitt "Ausnahmen" definierte spezifische Datenverkehr wird getunnelt (Split-Tunnel).

DNS-Modus:

Standard-DNS: Alle DNS-Abfragen durchlaufen die DNS-Server, die durch das VPN-Profil definiert sind. Bei einer negativen Antwort können die DNS-Abfragen auch an die DNS-Server geleitet werden, die auf dem physischen Adapter konfiguriert sind.

Gesamten DNS tunneln: Tunneling aller DNS-Abfragen über das VPN.

Split-DNS: Nur bestimmte DNS-Abfragen durchlaufen das VPN-Profil, abhängig von den unten angegebenen Domänen.

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

Konfiguration der Datenverkehrssteuerung

Cisco Secure Client-Konfiguration

Für die Zwecke dieses Leitfadens konfigurieren wir keine dieser erweiterten Einstellungen. Hier können erweiterte Funktionen konfiguriert werden, z. B.: TND, Always-On, Zertifikatzuordnung, lokaler LAN-Zugriff usw. Speichern Sie die Einstellungen hier.

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

Erweiterte Einstellungen

3. Ihr VPN-Profil muss wie folgt aussehen. Sie können das XML-Profil für die Endbenutzer herunterladen und vorab bereitstellen (unter "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile"), um das VPN zu verwenden, oder ihnen die Profil-URL bereitstellen, die in die Cisco Secure Client - AnyConnect VPN-Benutzeroberfläche eingegeben werden muss.

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	sse.cisco.com/VPN_EntraID	Download XML

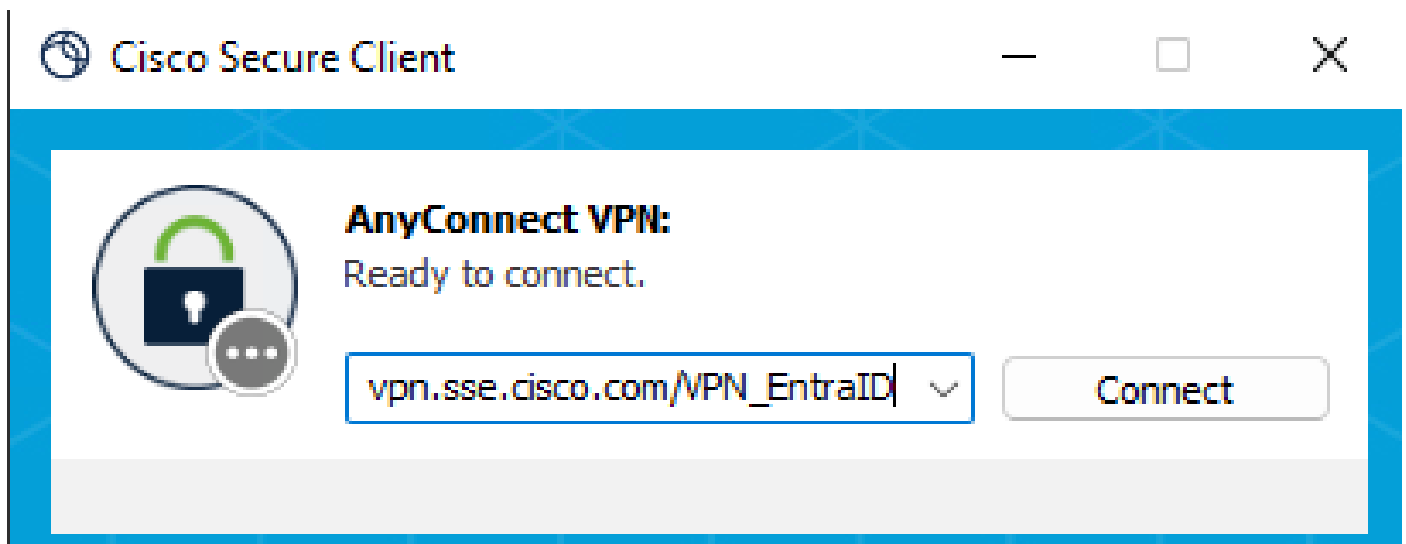
Globaler FQDN und Profil-URL

Überprüfung

Ihre RA VPN-Konfiguration muss zu diesem Zeitpunkt testbereit sein.
Beachten Sie, dass die Benutzer bei der ersten Verbindungsherstellung die Profil-URL-Adresse erhalten oder das XML-Profil auf ihren PCs unter "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile" vorab bereitstellen müssen. Starten Sie den VPN-Dienst neu, und Sie müssen im Dropdown-Menü die Option sehen, eine Verbindung zu diesem VPN-Profil herzustellen.

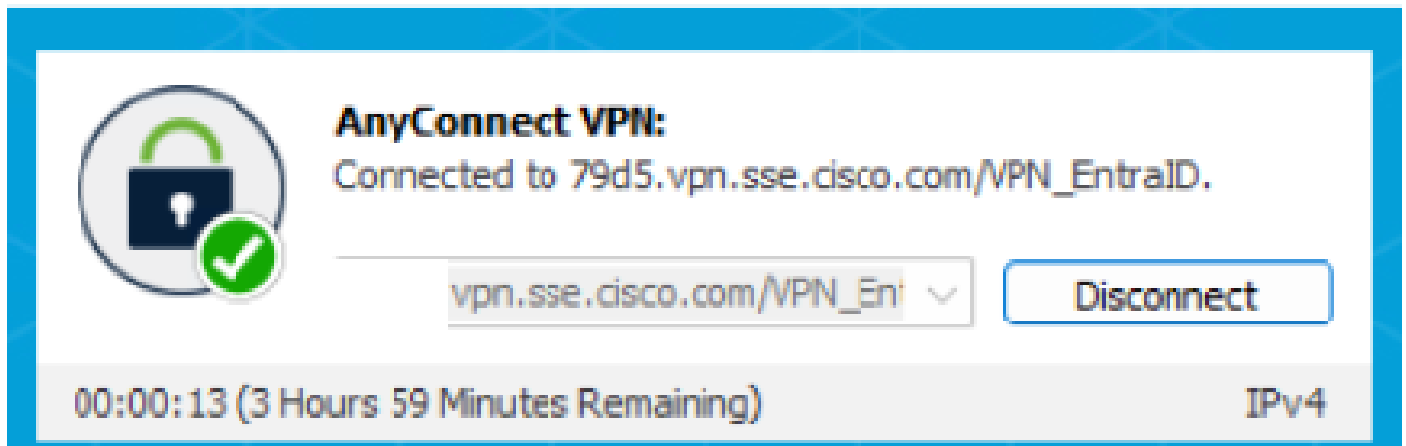
In diesem Beispiel geben wir die Profil-URL-Adresse für den ersten Verbindungsversuch an den Benutzer weiter.

Vor der ersten Verbindung:



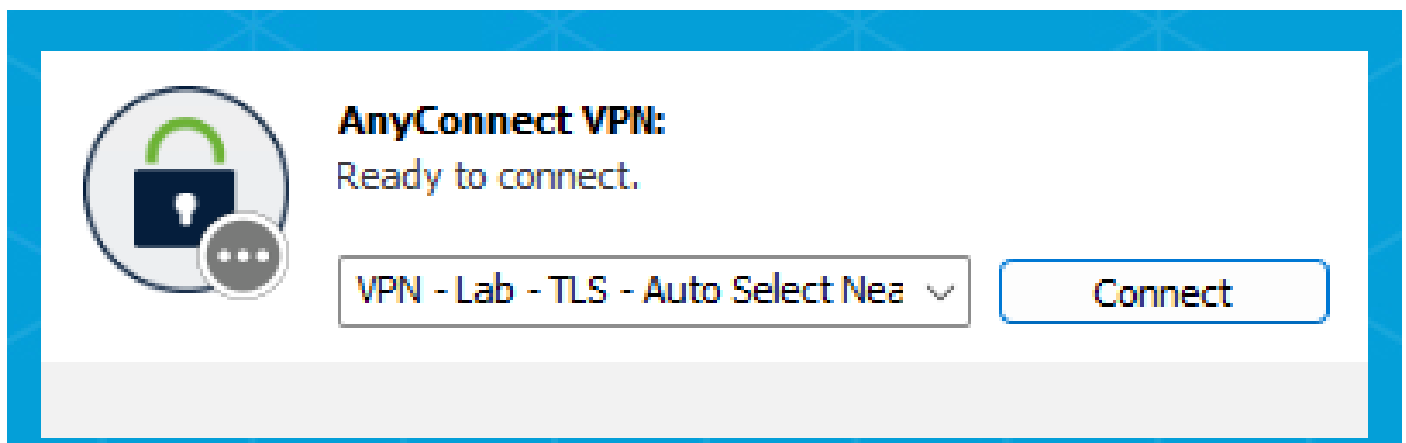
Frühere VPN-Verbindung

Geben Sie Ihre Anmeldeinformationen ein, und stellen Sie eine Verbindung zum VPN her:



Mit VPN verbunden

Nachdem Sie das erste Mal eine Verbindung hergestellt haben, müssen Sie nun im Dropdown-Menü die Option sehen können, sich mit dem VPN-Profil "VPN - Lab" zu verbinden:



Nach der ersten VPN-Verbindung

Einchecken der RAS-Protokolle, mit denen der Benutzer eine Verbindung herstellen konnte:

Überwachung > Remotezugriffsprotokoll

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

Anmelden bei Cisco Secure Access

Fehlerbehebung

Im Folgenden wird die grundlegende Fehlerbehebung beschrieben, die bei einigen gängigen Problemen durchgeführt werden kann:

Azure

Stellen Sie in Azure sicher, dass die Benutzer der Enterprise-Anwendung zugewiesen wurden, die für die Authentifizierung mit Cisco Secure Access erstellt wurde:

Startseite > Unternehmensanwendungen > Cisco Secure Access RA VPN > Verwalten > Benutzer und Gruppen

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 'visible' to 'true' to make it visible.

Assign users and groups to app-roles for your application here. To create a new user or group, click the + icon.

🔍 First 200 shown, search all users & groups

	Display name
☐	 Josue

Zuweisung von Benutzern überprüfen

Sicherer Zugriff von Cisco

Stellen Sie in Cisco Secure Access sicher, dass Sie die Benutzer bereitgestellt haben, die über RA VPN eine Verbindung herstellen dürfen, und dass auch die in Cisco Secure Access bereitgestellten Benutzer (unter Benutzer, Gruppen und Endgeräte) mit den Benutzern in Azure (den in der Unternehmensanwendung zugewiesenen Benutzern) übereinstimmen.

Verbinden > Benutzer, Gruppen und Endgeräte

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

Benutzer in Cisco Secure Access

Vergewissern Sie sich, dass dem Benutzer entweder die richtige XML-Datei auf dem PC bereitgestellt wurde, oder dass ihm die Profil-URL zugewiesen wurde, wie im Schritt "Verifizieren" angegeben.

Verbinden > Endbenutzerverbindungen > Virtuelles privates Netzwerk

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	

Profil-URL und XML-Profil

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.