

Configuration de Cisco Secure Access pour RA VPNaaS avec Entra ID

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Configuration Azure](#)

[Configuration de Cisco Secure Access](#)

[Vérifier](#)

[Dépannage](#)

[Azure](#)

[Accès sécurisé Cisco](#)

Introduction

Ce document décrit étape par étape comment configurer RA VPN sur Cisco Secure Access pour l'authentification par rapport à l'ID d'entrée.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance à l'aide d'Azure/Entra ID.
- Connaissances avec Cisco Secure Access.

Exigences

Ces exigences doivent être remplies avant de poursuivre :

- Accédez à votre tableau de bord Cisco Secure Access en tant qu'administrateur complet.
- Accès à Azure en tant qu'administrateur.
- [La mise en service utilisateur](#) est déjà terminée pour Cisco Secure Access.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Tableau de bord Cisco Secure Access.

- Portail Microsoft Azure.
- Cisco Secure Client AnyConnect VPN version 5.1.8.105

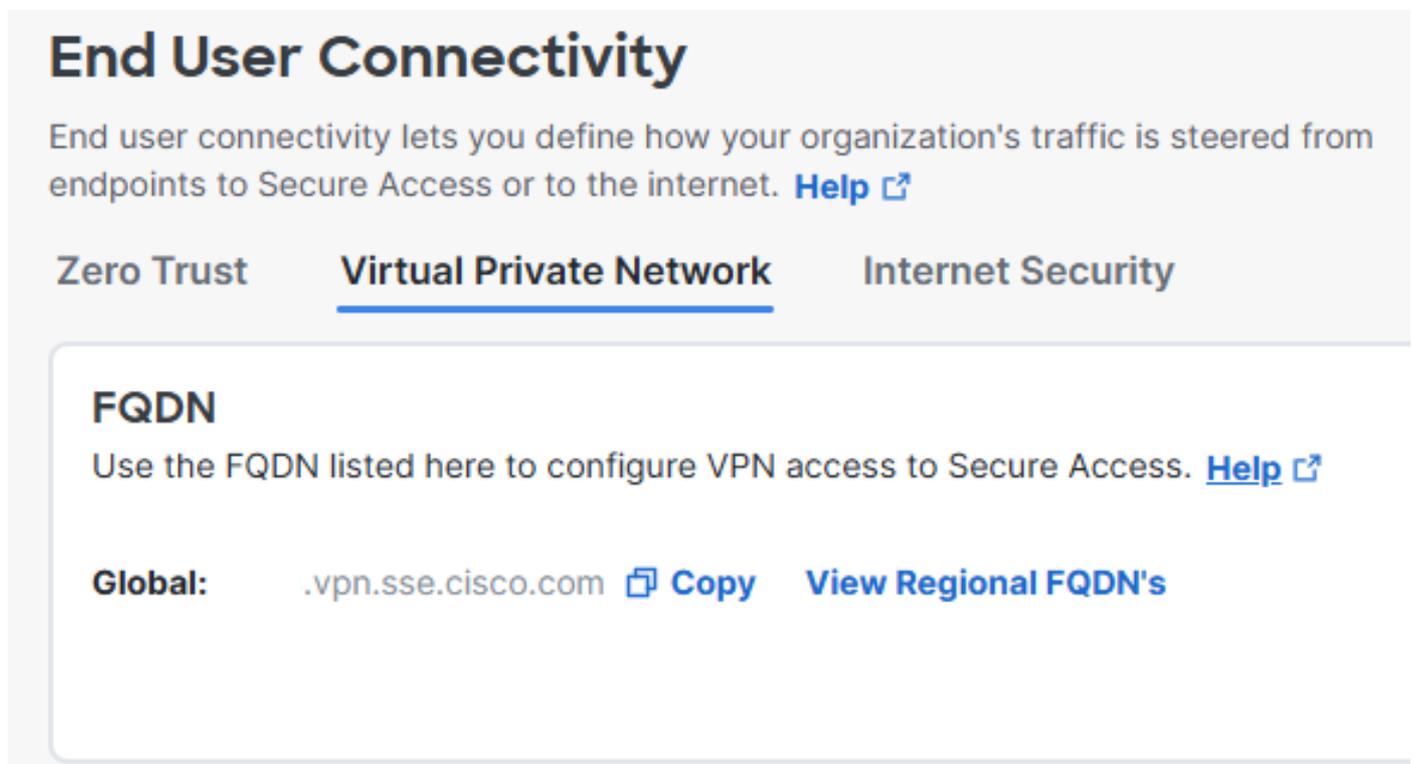
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Configuration Azure

1. Connectez-vous au tableau de bord Cisco Secure Access et copiez le FQDN global VPN. Nous utilisons ce nom de domaine complet dans la configuration de l'application d'entreprise Azure.

Connect > End User Connectivity > Virtual Private Network > 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](#)

FQDN global VPN

2. Connectez-vous à Azure et créez une application d'entreprise pour l'authentification VPN RA. Vous pouvez utiliser l'application prédéfinie nommée « Cisco Secure Firewall - Authentification Secure Client (anciennement AnyConnect) ».

Accueil > Applications d'entreprise > Nouvelle application > Cisco Secure Firewall - Authentification Secure Client (anciennement AnyConnect) > Créer

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.

Créer une application dans Azure

3. Renommez l'application.
Propriétés > Nom

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 

Renommer l'application

4. Dans l'application d'entreprise, attribuez les autorisations d'authentification aux utilisateurs à l'aide du VPN AnyConnect.

Affecter des utilisateurs et des groupes > + Ajouter un utilisateur/groupe > Affecter

[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

Display name

No application assignments found

Utilisateurs/Groupes affectés

5. Cliquez sur Single sign-on et configurez les paramètres SAML. Ici, nous utilisons le nom de domaine complet copié à l'étape 1, ainsi que le nom du profil VPN que vous configurez à la section « Configuration de Cisco Secure Access » plus loin à l'étape 2.

Par exemple, si votre nom de domaine complet global VPN est example1.vpn.sse.cisco.com et que le nom de votre profil VPN d'accès sécurisé Cisco est VPN_EntraID, les valeurs pour (ID d'entité) et l'URL de réponse (URL du service client d'assertion) sont :

Identifiant (ID d'entité) : https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID

URL de réponse (URL du service client d'assertion) :

https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tname=VPN_EntraID

Identifiant (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
<input type="text" value="https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID"/>	<input checked="" type="checkbox"/> ⓘ

[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
<input type="text" value="https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tname=VPN_EntraID"/>	<input type="text"/>	<input checked="" type="checkbox"/> ⓘ

[Add reply URL](#)

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

Paramètres SAML dans Azure

6. Téléchargez le fichier XML des métadonnées de fédération.

SAML Certificates

Token signing certificate  Edit

Status	Active
Thumbprint	B3194903628E192F48BC0CB44E7614867F79F17E
Expiration	3/28/2028, 11:50:10 AM
Notification Email	
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/71414a41-5159..."/> 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)  Edit

Required	No
Active	0
Expired	0

Configuration de Cisco Secure Access

1. Connectez-vous à votre tableau de bord Cisco Secure Access et ajoutez un pool d'adresses IP.

Connect > End User Connectivity > Virtual Private Network > Add IP Pool

Région : Sélectionnez la région où votre VPN RA sera déployé.

Nom complet : Nom du pool d'adresses IP VPN.

Serveur DNS : Créez ou attribuez le serveur DNS que les utilisateurs utilisent pour la résolution DNS une fois connectés.

Pool d'adresses IP système : Utilisée par l'accès sécurisé pour des fonctionnalités telles que l'authentification Radius, la demande d'authentification provient d'une adresse IP comprise dans cette page.

Pool IP : Ajoutez un nouveau pool d'adresses IP et spécifiez les adresses IP que les utilisateurs obtiennent une fois connectés au VPN RA.



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](#)

Ajouter un profil VPN

Parameters

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

Region

 ⊗ ▾

Display name

DNS Server

 ▾ [+ Add](#)

DDNS Servers updates

System IP Pool ⓘ

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 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

Configuration du pool d'adresses IP - Partie 2

2. Ajoutez un profil VPN.

Connect > End User Connectivity > Virtual Private Network > + Profil VPN

Paramètres généraux



Remarque : Remarque : Le nom du profil VPN doit correspondre au nom que vous avez configuré dans « Configuration Azure » à l'étape 5. Dans ce guide de configuration, nous avons utilisé VPN_EntraID afin de configurer le même nom dans Cisco Secure Access que le nom du profil VPN.

Nom du profil VPN : Nom de ce profil VPN, visible uniquement dans le tableau de bord.

Nom complet : Le nom des utilisateurs finaux apparaît dans le menu déroulant « Secure Client - Anyconnect » lors de la connexion à ce profil VPN d'annonce de routeur.

Domaine par défaut : Les utilisateurs du domaine se connectent une fois au VPN.

Serveurs DNS : Serveur DNS : les utilisateurs VPN sont connectés au VPN une fois.

Région spécifiée : Utilise le serveur DNS associé au pool d'adresses IP VPN.

Personnalisé spécifié : Vous pouvez attribuer manuellement le DNS souhaité.

Pools IP : Les adresses IP attribuées aux utilisateurs une fois connectés au VPN.

Paramètres du profil : Pour inclure ce profil VPN pour le [tunnel de machine](#) ou pour inclure le nom de domaine complet régional afin que l'utilisateur final sélectionne la région à laquelle il souhaite se connecter (est sujet aux pools d'adresses IP déployés).

Protocoles : Sélectionnez le protocole que vos utilisateurs VPN doivent utiliser pour la transmission tunnel du trafic.

Position temporelle de connexion (facultatif) : Si nécessaire, faire la [position VPN](#) au moment de la connexion. Plus d'informations ici

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](#)

Configuration du profil VPN - Partie 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.

Authentification, autorisation et administration (AAA)

Protocoles : Sélectionnez SAML.

Authentification avec certificats CA : Si vous souhaitez vous authentifier à l'aide d'un certificat SSL et vous autoriser auprès d'un fournisseur SAML IdP.

Forcer une nouvelle authentification : Force une nouvelle authentification chaque fois qu'une connexion VPN est établie. La réauthentification forcée est basée sur le délai d'expiration de la session. Cela pourrait être soumis aux paramètres du fournisseur d'identité SAML (Azure dans ce cas).

Téléchargez le fichier XML de métadonnées de fédération de fichier XML téléchargé dans « Configurer Azure » à l'étape 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](#)

Configuration SAML

Orientation du trafic (split tunnel)

Mode tunnel :

Connexion à un accès sécurisé : Tout le trafic est envoyé via le tunnel (Tunnel All).

Contourner l'accès sécurisé : Le trafic spécifique défini dans la section Exceptions est uniquement tunnelisé (split tunnel).

Mode DNS :

DNS par défaut : Toutes les requêtes DNS transitent par les serveurs DNS définis par le profil VPN. Dans le cas d'une réponse négative, les requêtes DNS peuvent également aller aux serveurs DNS qui sont configurés sur la carte physique.

Tunnel All DNS : Tunnel toutes les requêtes DNS via le VPN.

DNS fractionné : Des requêtes DNS spécifiques se déplacent dans le profil VPN, en fonction des domaines spécifiés ci-dessous.

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

Configuration du pilotage du trafic

Configuration du client sécurisé Cisco

Dans le cadre de ce guide, nous ne configurons aucun de ces paramètres avancés. Les fonctionnalités avancées peuvent être configurées ici, par exemple : TND, Always-On, Certificate Matching, Local Lan Access, etc. Enregistrez les paramètres ici.

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

Paramètres avancés

3. Votre profil VPN doit ressembler à ceci. Vous pouvez télécharger et pré-déployer le profil xml sur les utilisateurs finaux (sous « C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile ») pour commencer à utiliser le VPN, ou leur fournir l'URL du profil à entrer dans l'interface utilisateur VPN de Cisco Secure Client - AnyConnect.

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](#)

Search

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

FQDN global et URL de profil

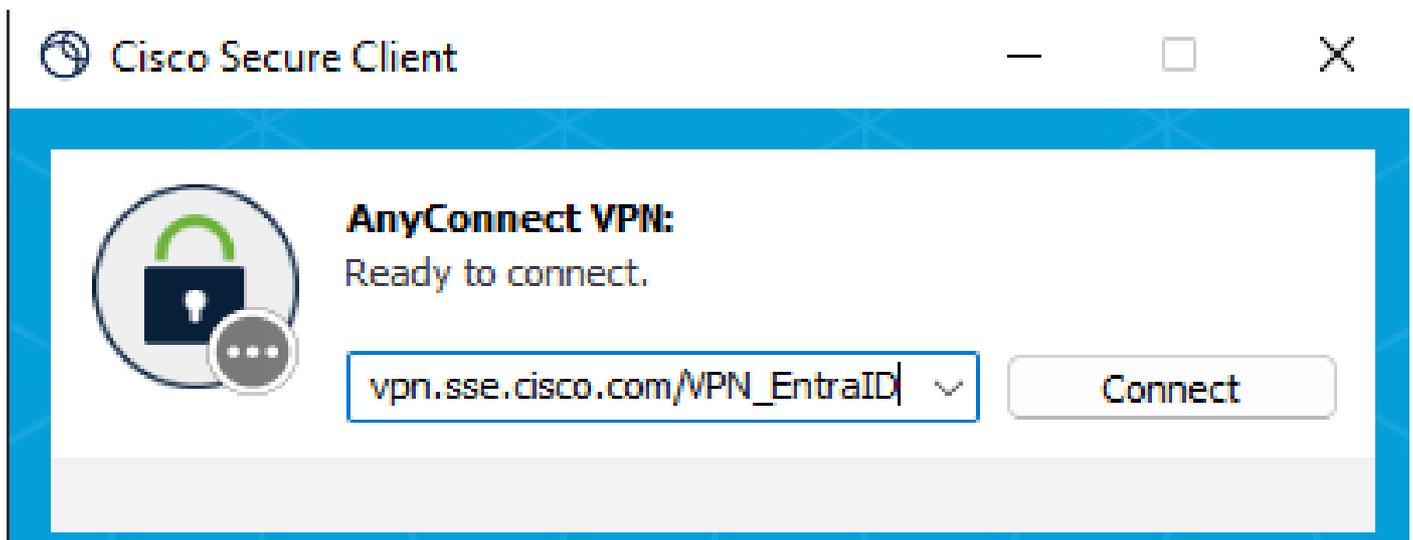
Vérifier

À ce stade, votre configuration VPN RA doit être prête pour le test.

Notez que la première fois que les utilisateurs se connectent, ils doivent recevoir l'adresse URL du profil ou pré-déployer le profil xml sur leurs PC sous « C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile », redémarrer le service VPN et ils doivent voir dans le menu déroulant l'option pour se connecter à ce profil VPN.

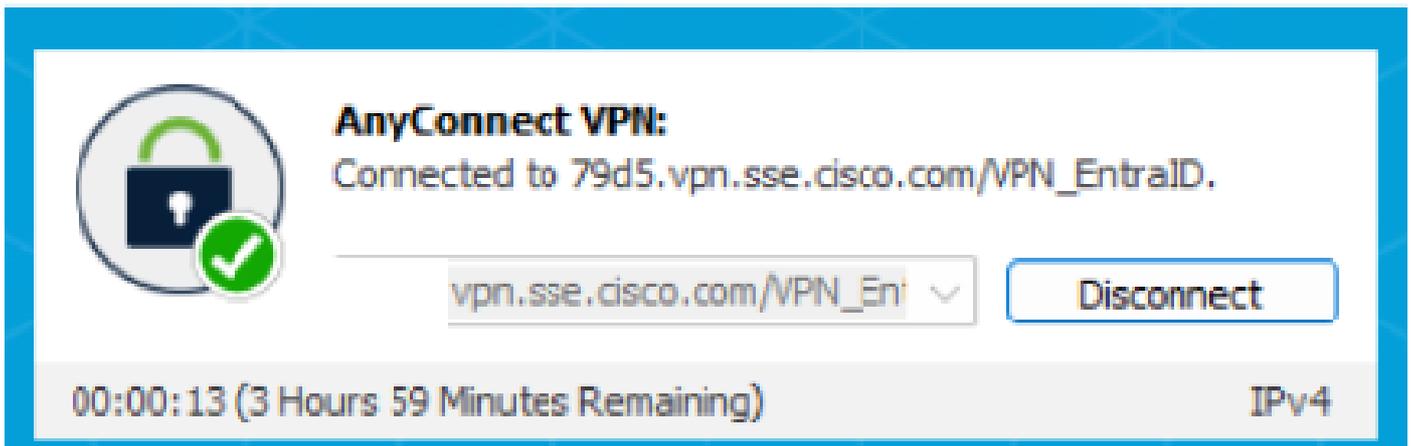
Dans cet exemple, nous donnons l'adresse URL du profil à l'utilisateur pour la première tentative de connexion.

Avant la première connexion :



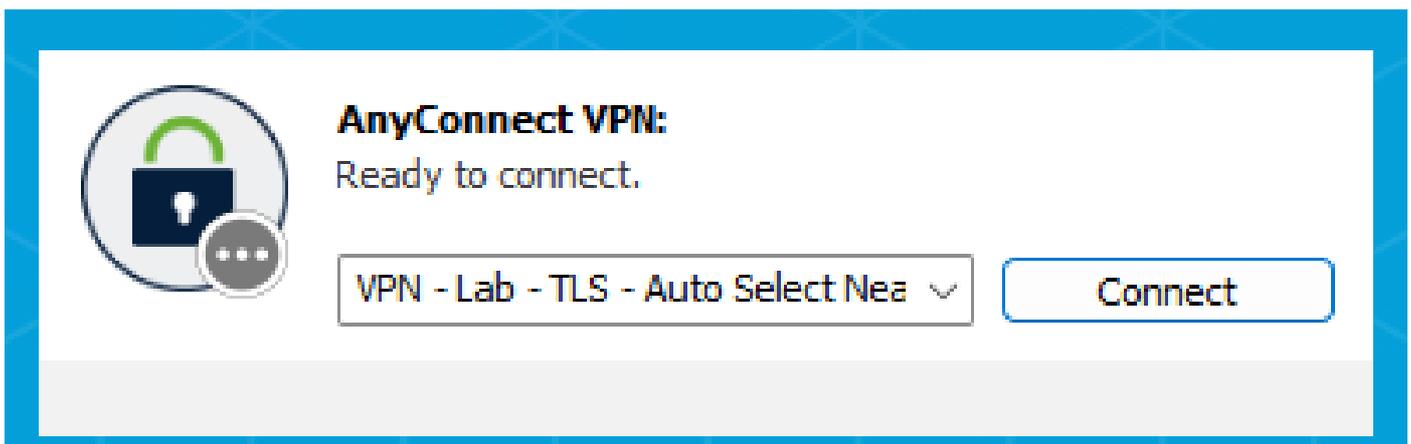
Connexion VPN précédente

Saisissez vos informations d'identification et connectez-vous au VPN :



Connecté au VPN

Après la première connexion, à partir du menu déroulant, vous devez être en mesure de voir maintenant l'option pour se connecter au profil VPN "VPN - Lab" :



Après la première connexion VPN

Vérifiez dans les journaux d'accès à distance que l'utilisateur a pu se connecter :

Contrôle > Journal d'accès distant

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

Connexion à Cisco Secure Access

Dépannage

Voici une description du dépannage de base qui peut être effectué pour certains problèmes courants :

Azure

Dans Azure, assurez-vous que les utilisateurs ont été affectés à l'application d'entreprise créée pour l'authentification avec Cisco Secure Access :

Accueil > Applications d'entreprise > Cisco Secure Access RA VPN > Gérer > Utilisateurs et groupes

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 show this application in My Apps.

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

🔍 First 200 shown, search all users & groups

	Display name
<input type="checkbox"/>	 Josue

Vérifier l'affectation des utilisateurs

Accès sécurisé Cisco

Dans Cisco Secure Access, assurez-vous que vous avez configuré les utilisateurs autorisés à se connecter via RA VPN et que les utilisateurs configurés dans Cisco Secure Access (sous Utilisateurs, groupes et terminaux) correspondent aux utilisateurs dans Azure (les utilisateurs attribués dans l'application d'entreprise).

Connect > Utilisateurs, groupes et terminaux

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](#)

3 results

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

Utilisateurs dans Cisco Secure Access

Vérifiez que l'utilisateur a été approvisionné avec le fichier XML correct sur le PC ou que l'utilisateur a reçu l'URL de profil, comme indiqué à l'étape « Vérifier ».

Connect > End User Connectivity > 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](#)

Q VPN 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.cis.co.com/VPN_EntraID	

URL du profil et profil .xml

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.