

Configurazione di Cisco Secure Access per RA VPNaaS con Entra ID

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione di Azure](#)

[Configurazione Cisco Secure Access](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Azzurro](#)

[Cisco Secure Access](#)

Introduzione

In questo documento viene descritto passo a passo come configurare una VPN RSA su Cisco Secure Access per l'autenticazione con Entra ID.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza tramite Azure/Entra ID.
- Conoscenza di Cisco Secure Access.

Requisiti

Prima di procedere, è necessario soddisfare i seguenti requisiti:

- Accedere a Cisco Secure Access Dashboard come amministratore completo.
- Accesso ad Azure come amministratore.
- [Provisioning utente](#) già completato per Cisco Secure Access.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Access Dashboard.

- Portale di Microsoft Azure.
- Cisco Secure Client AnyConnect VPN versione 5.1.8.105

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazione di Azure

1. Accedi al dashboard di Cisco Secure Access e copia il nome di dominio completo (FQDN) globale della VPN. Questo FQDN è in uso nella configurazione dell'applicazione aziendale di Azure.

Connetti > Connettività utente finale > Rete privata virtuale > FQDN > Globale

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 globale VPN

2. Accedere ad Azure e creare un'applicazione enterprise per l'autenticazione VPN per l'Autorità registrazione integrità. È possibile usare l'applicazione predefinita "Cisco Secure Firewall - Autenticazione client sicura (in precedenza AnyConnect)".

Home > Applicazioni enterprise > Nuova applicazione > Cisco Secure Firewall - Autenticazione client sicura (in precedenza AnyConnect) > Crea

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.

Crea app in Azure

3. Rinominare l'applicazione.
Proprietà > Nome

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 

Rinomina l'applicazione

4. Nell'applicazione enterprise, assegnare gli utenti autorizzati all'autenticazione tramite la VPN AnyConnect.

Assegna utenti e gruppi > + Aggiungi utente/gruppo > Assegna

[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

Utenti/gruppi assegnati

5. Fare clic su Single Sign-On e configurare i parametri SAML. In questa sezione viene usato l'FQDN copiato nel passaggio 1 e il nome del profilo VPN che si sta configurando in "Configuration Cisco Secure Access" più avanti nel passaggio 2.

Ad esempio, se il nome di dominio completo (FQDN) globale della VPN è example1.vpn.sse.cisco.com e il nome del profilo VPN ad accesso sicuro di Cisco è VPN_EntraID, i valori per (ID entità) e URL di risposta (URL servizio consumer asserzione) sono:

Identificatore (ID entità): https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID

URL risposta (URL servizio consumer asserzione):

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

[Add reply URL](#)

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

Parametri SAML in Azure

6. Scaricare il file XML dei metadati federativi.

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

Configurazione Cisco Secure Access

1. Accedi al dashboard di Cisco Secure Access e aggiungi un pool IP.

Connetti > Connettività utente finale > Rete privata virtuale > Aggiungi pool IP

Regione: Selezionare l'area in cui verrà distribuita la VPN dell'Autorità registrazione.

Nome visualizzato: Nome del pool IP della VPN.

Server DNS: Creare o assegnare gli utenti del server DNS utilizzati per la risoluzione DNS una volta connessi.

Pool IP di sistema: Utilizzata da Secure Access per funzionalità quali l'autenticazione Radius, la richiesta di autenticazione ha origine da un indirizzo IP compreso in questo intervallo.

Pool IP: Aggiungere un nuovo pool IP e specificare gli IP che gli utenti ottengono una volta connessi alla VPN dell'Autorità registrazione.



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](#)

Aggiungi profilo 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 ⓘ

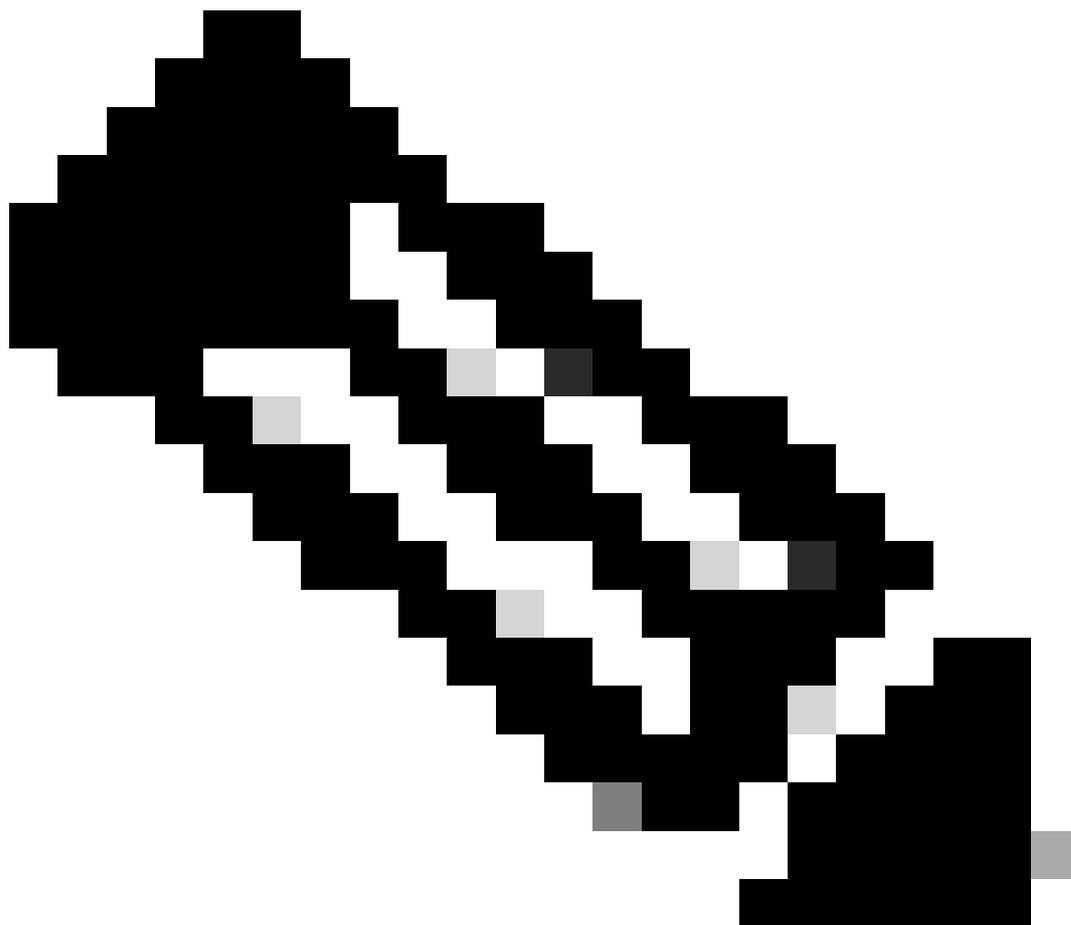
172.16.1.0/24

Configurazione del pool IP - Parte 2

2. Aggiungere un profilo VPN.

Connetti > Connettività utente finale > Rete privata virtuale > + Profilo VPN

Impostazioni generali



Nota: Nota: Il nome del profilo VPN deve corrispondere al nome configurato in "Azure di configurazione" nel passaggio 5. In questa guida alla configurazione è stato utilizzato VPN_EntraID, quindi in Cisco Secure Access viene configurato lo stesso nome del profilo VPN.

Nome profilo VPN: Nome per questo profilo VPN, visibile solo nel dashboard.

Nome visualizzato: Il nome che gli utenti finali visualizzano nel menu a discesa 'Secure Client - Anyconnect' mostra quando si connettono a questo profilo VPN per l'Autorità registrazione.

Dominio predefinito: Una volta connessi alla VPN, gli utenti del dominio.

Server DNS: Server DNS utilizzato dagli utenti VPN una volta connessi alla VPN.

Area specificata: Utilizza il server DNS associato al pool IP della VPN.

Personalizzato specificato: È possibile assegnare manualmente il DNS desiderato.

Pool IP: IP assegnati agli utenti una volta connessi alla VPN.

Impostazioni profilo: Per includere questo profilo VPN per il [tunnel macchina](#) o per includere il nome di dominio completo (FQDN) regionale in modo che l'utente finale selezioni la regione a cui desidera connettersi (soggetta ai pool IP distribuiti).

Protocolli: Selezionare il protocollo che gli utenti VPN devono utilizzare per il tunneling del traffico.
Postura tempo di connessione (facoltativa): Se necessario, eseguire [VPN Posture](#) al momento della connessione. Ulteriori informazioni

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](#)

Configurazione profilo VPN - Parte 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.

Autenticazione, autorizzazione e accounting

Protocolli: Selezionare SAML.

Autenticazione con certificati CA: Se si desidera eseguire l'autenticazione utilizzando un certificato SSL e l'autorizzazione per un provider SAML IdP.

Forza riautenticazione: Forza una riautenticazione ogni volta che viene stabilita una connessione VPN. La riautenticazione forzata è basata sul timeout della sessione. Potrebbe essere soggetto alle impostazioni del provider di identità SAML (Azure in questo caso).

Caricare il file XML metadati federazione file XML scaricato in "Configura Azure" nel passaggio 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](#)

Configurazione SAML

Traffic Steering (split tunnel)

Modalità tunnel:

Connetti ad accesso sicuro: Tutto il traffico viene inviato attraverso il tunnel (Tunnel All).

Ignora accesso sicuro: Solo il traffico specifico definito nella sezione Exceptions è tunneling (Split Tunnel).

Modalità DNS:

DNS predefinito: Tutte le query DNS vengono spostate nei server DNS definiti dal profilo VPN. In caso di risposta negativa, le query DNS possono anche passare ai server DNS configurati sulla scheda fisica.

Tunnel per tutti i DNS: Eseguire il tunnel di tutte le query DNS tramite VPN.

Dividi DNS: Solo le query DNS specifiche vengono spostate nel profilo VPN, a seconda dei domini specificati di seguito.

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

Configurazione Traffic Steering

Cisco Secure Client Configuration

Ai fini di questa guida, non stiamo configurando nessuna di queste impostazioni avanzate. Le funzioni avanzate possono essere configurate qui, ad esempio: TND, Always-On, Corrispondenza certificati, Accesso LAN locale e così via. Salvare le impostazioni qui.

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

Impostazioni avanzate

3. Il tuo profilo VPN deve avere questo aspetto. È possibile scaricare e pre-distribuire il profilo xml agli utenti finali (in "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile") per iniziare a utilizzare la VPN o fornire loro l'URL del profilo da immettere nell'interfaccia utente di Cisco Secure Client - AnyConnect VPN.

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](#)

Q 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	SAM	Bypass Secure Access 1 Exception(s)	13 Settings	<code>sse.cisco.com/VPN_EntraID</code> Copy	Download XML

FQDN globale e URL profilo

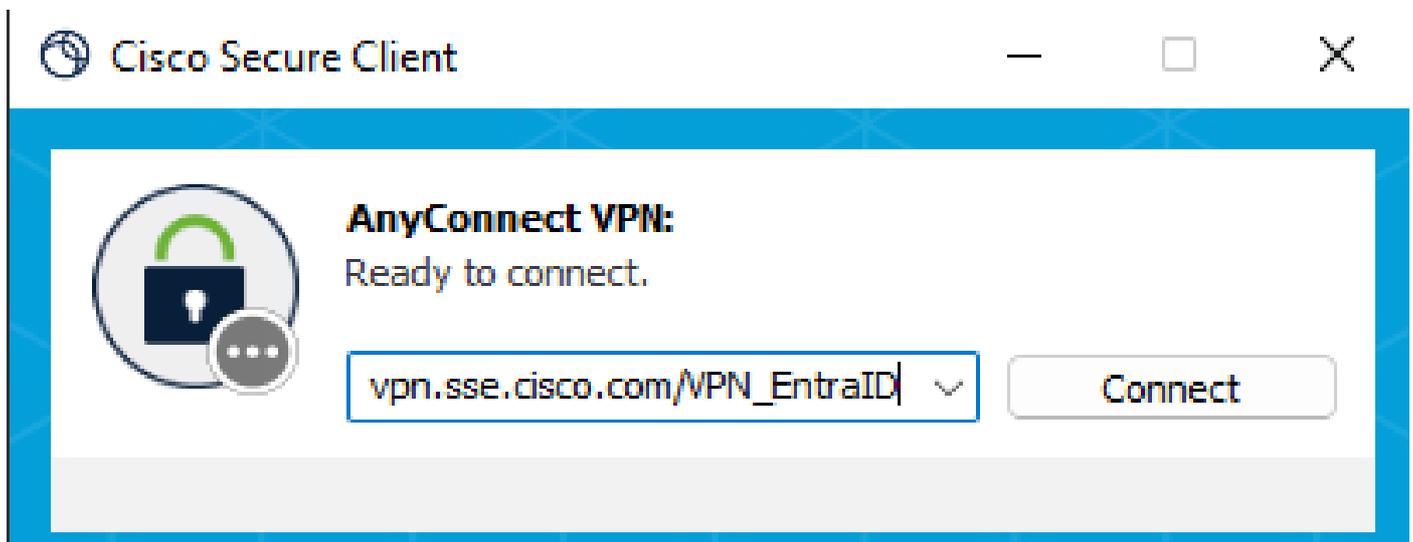
Verifica

A questo punto, la configurazione della VPN dell'Autorità registrazione deve essere pronta per il test.

Notare che la prima volta che gli utenti si connettono, devono ricevere l'indirizzo URL del profilo o pre-distribuire il profilo xml nei loro PC in "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile", riavviare il servizio VPN e devono vedere nel menu a discesa l'opzione per connettersi a questo profilo VPN.

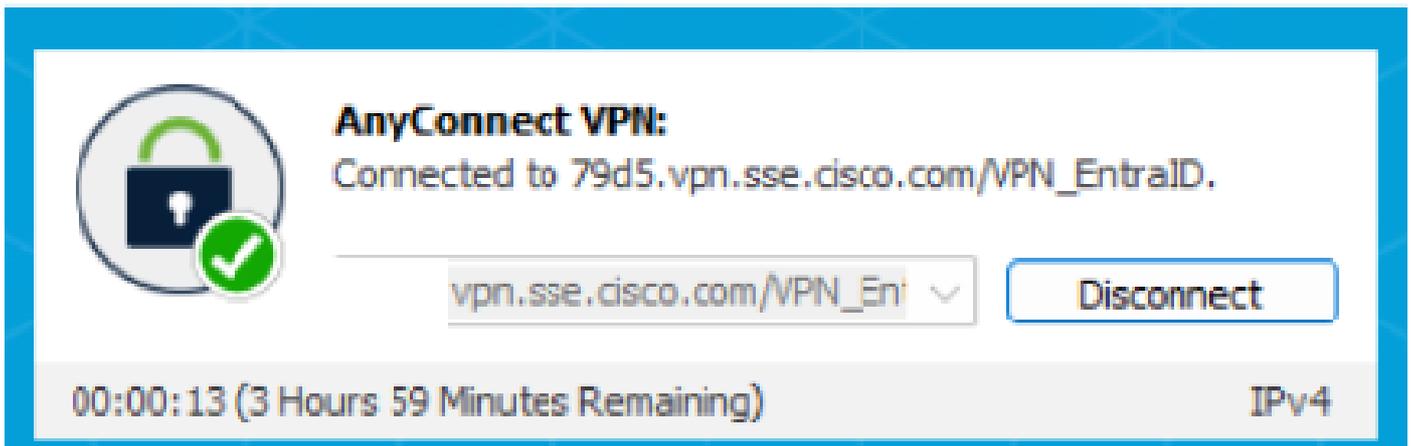
In questo esempio, viene fornito all'utente l'indirizzo URL del profilo per il primo tentativo di connessione.

Prima della prima connessione:



Connessione VPN precedente

Immettere le credenziali e connettersi alla VPN:



AnyConnect VPN:
Connected to 79d5.vpn.sse.cisco.com/VPN_EntraID.

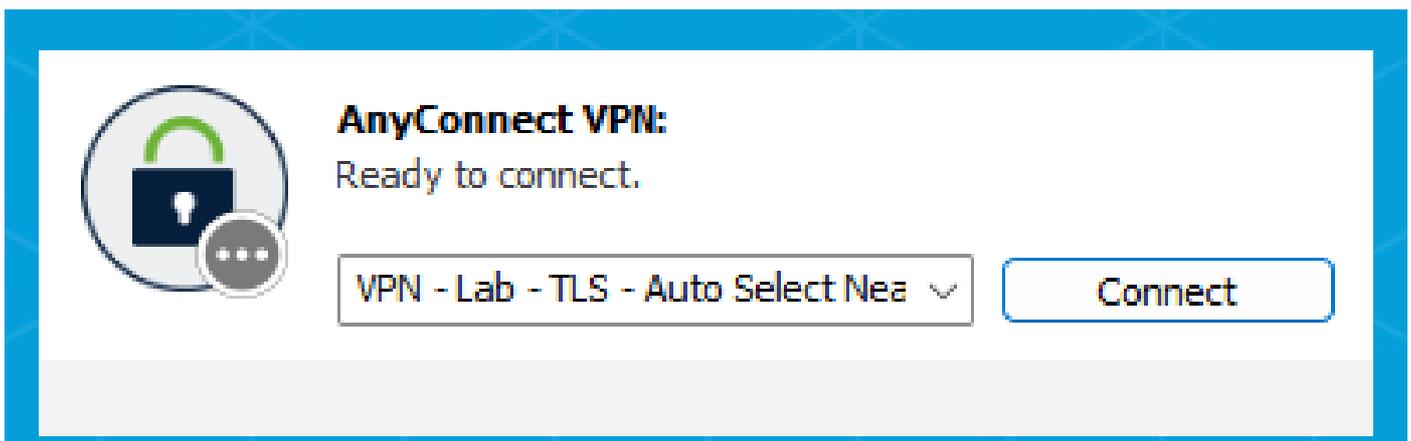
vpn.sse.cisco.com/VPN_En

Disconnect

00:00:13 (3 Hours 59 Minutes Remaining) IPv4

Connesso a VPN

Dopo aver effettuato la connessione per la prima volta, dal menu a discesa, è necessario poter visualizzare ora l'opzione per connettersi al profilo VPN "VPN - Lab":



AnyConnect VPN:
Ready to connect.

VPN - Lab - TLS - Auto Select Nea

Connect

Dopo la prima connessione VPN

Archiviare i registri di Accesso remoto a cui l'utente è riuscito a connettersi:

Monitor > Registro di accesso remoto

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

Log in Cisco Secure Access

Risoluzione dei problemi

Di seguito viene descritta la risoluzione dei problemi di base che è possibile eseguire per alcuni problemi comuni:

Azzurro

In Azure verificare che gli utenti siano stati assegnati all'applicazione enterprise creata per l'autenticazione con Cisco Secure Access:

Home > Applicazioni enterprise > Cisco Secure Access RSA VPN > Gestisci > Utenti e gruppi

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

The screenshot shows the 'Users and groups' management page for the 'Cisco Secure Access RA VPN' application in the Azure portal. The page title is 'Cisco Secure Access RA VPN | Users and groups' with a sub-label 'Enterprise Application'. The left-hand navigation pane includes: Overview, Deployment Plan, Diagnose and solve problems, Manage (expanded), Properties (selected), Owners, Roles and administrators, and Users and groups. The main content area features a top bar with '+ Add user/group', 'Edit assignment', and 'Remove assignment' buttons. A light blue information banner states: 'The application will appear for assigned users within My Apps. Set \'visi...'. Below this is the instruction: 'Assign users and groups to app-roles for your application here. To creat...'. A search box contains the text 'First 200 shown, search all users & groups'. A table with the header 'Display name' shows one user entry: a checkbox, a blue circular profile picture with the letter 'J', and the name 'Josue'.

Verifica assegnazione utenti

Cisco Secure Access

In Cisco Secure Access verificare di aver eseguito il provisioning degli utenti a cui è consentito connettersi tramite la VPN RSA e che anche gli utenti a cui è stato eseguito il provisioning in Cisco Secure Access (in utenti, gruppi e dispositivi endpoint) corrispondano agli utenti in Azure (gli utenti assegnati nell'applicazione enterprise).

Connetti > Utenti, gruppi e dispositivi endpoint

Secure Access

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

Utenti in Cisco Secure Access

Verificare che all'utente sia stato assegnato il file XML corretto sul PC o che all'utente sia stato assegnato l'URL del profilo, come indicato nel passaggio "Verifica".

Connetti > Connettività utente finale > Rete privata virtuale

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.cisco.com/VPN_EntraID	

URL del profilo e profilo XML

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).