

使用Entra ID為RA VPNaS配置思科安全訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[Azure配置](#)

[思科安全存取組態](#)

[驗證](#)

[疑難排解](#)

[Azure](#)

[Cisco Secure Access](#)

簡介

本文分步介紹如何在Cisco Secure Access上配置RA VPN以根據Entra ID進行身份驗證。

必要條件

思科建議您瞭解以下主題：

- 使用Azure/Entra ID的知識。
- 思科安全訪問知識。

需求

在繼續操作之前，必須滿足以下要求：

- 以完全管理員身份訪問您的思科安全訪問控制面板。
- 以管理員身份訪問Azure。
- [已完成對](#)思科安全訪問的使用者調配。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Secure Access Dashboard。
- Microsoft Azure門戶。
- Cisco安全使用者端AnyConnect VPN版本5.1.8.105

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

Azure配置

1. 登入思科安全訪問控制面板並複製VPN全域性FQDN。我們在Azure企業應用程式配置中使用此FQDN。

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](#)

VPN全域性FQDN

2. 登入Azure並建立用於RA VPN身份驗證的企業應用程式。您可以使用名為「思科安全防火牆 — 安全客戶端 (以前稱為AnyConnect) 身份驗證」的預定義應用程式。

首頁>企業應用程式>新應用程式> Cisco Secure Firewall - Secure Client (以前稱為AnyConnect) 身份驗證>建立

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.

在Azure中建立應用

3.重新命名應用程式。
屬性>名稱

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 

重新命名應用程式

4. 在企業應用程式中，分配使用者允許使用AnyConnect VPN進行身份驗證。
分配使用者和組 > +新增使用者/組 > 分配

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

分配的使用者/組

5. 按一下單點登入並配置SAML引數。此處我們使用步驟1中複製的FQDN，以及步驟2後面的「配置Cisco安全訪問」中配置的VPN配置檔名稱。

例如，如果您的VPN全域性FQDN為example1.vpn.sse.cisco.com，而您的思科安全訪問VPN配置檔名稱為VPN_EntraID，則（實體ID）和回覆URL（斷言使用者服務URL）的值如下：

識別符號 (實體ID) : https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntralD

回覆URL (斷言使用者服務

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

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_EntralD"/>	<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_EntralD"/>	<input type="text"/>	<input checked="" type="checkbox"/> ⓘ

[Add reply URL](#)

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

Azure中的SAML引數

6. 下載聯合後設資料XML。

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	

思科安全存取組態

1. 登入您的Cisco Secure Access控制面板，並新增IP池。

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

地區：選擇要部署RA VPN的區域。

顯示名稱：VPN IP池的名稱。

DNS伺服器：連線後建立或分配使用者用於進行DNS解析的DNS伺服器。

系統IP池：安全存取使用諸如Radius驗證等功能，驗證要求源自此範圍中的IP。

IP池：新增新的IP池，並指定使用者連線到RA VPN之後獲得的IP。



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](#)

新增VPN配置檔案

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 ⓘ

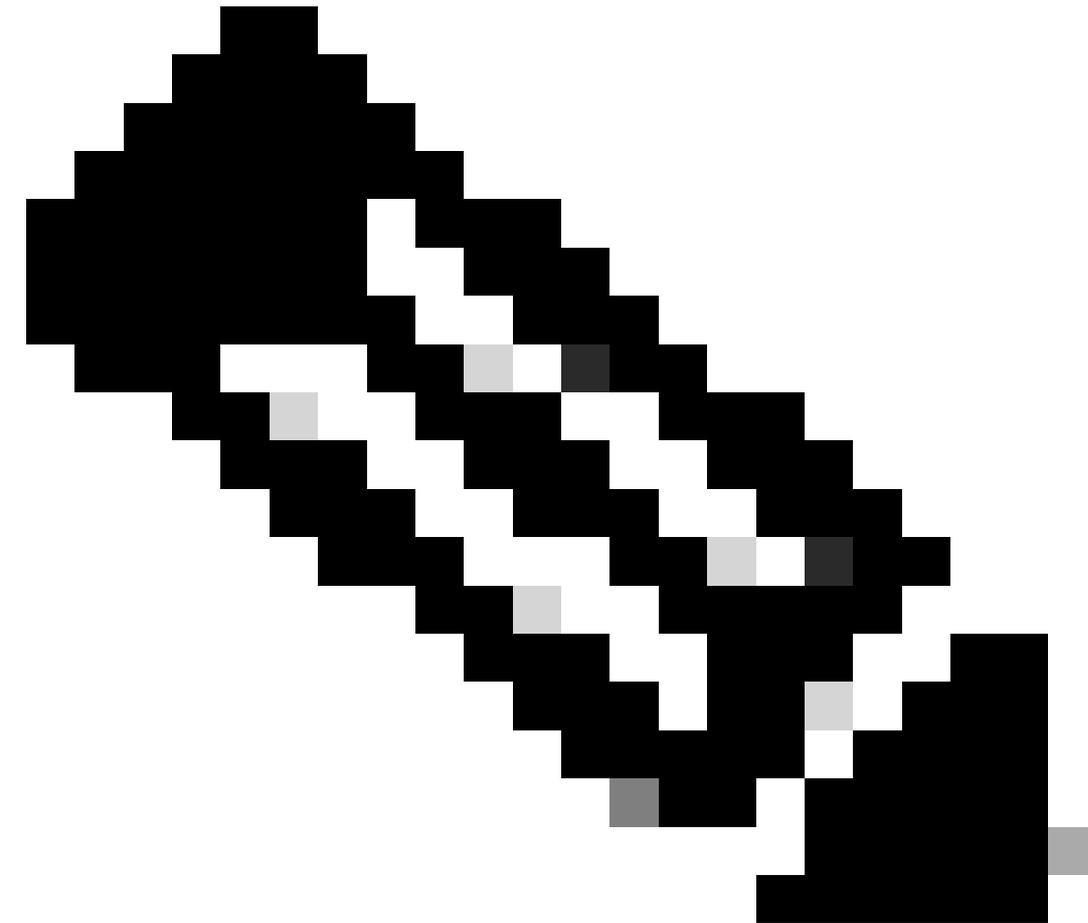
172.16.1.0/24

IP池配置 — 第2部分

2. 新增VPN配置檔案。

連線>終端使用者連線>虛擬專用網路> + VPN配置檔案

常規設定



附註：附註：VPN配置檔案的名稱必須與您在步驟5中的「配置Azure」中配置的名稱相匹配。在此配置指南中我們使用VPN_EntraID，因此我們在思科安全訪問中配置與VPN配置檔名稱相同的名稱。

VPN配置檔名稱：此VPN配置檔案的名稱，僅在儀表板中顯示。

顯示名稱：命名終端使用者在「Secure Client - Anyconnect」下拉選單上看到，當連線到此RA VPN配置檔案時，請參閱。

預設域：域使用者一旦連線到VPN。

DNS伺服器：DNS伺服器VPN使用者一旦連線到VPN。

指定的區域：使用與VPN IP池關聯的DNS伺服器。

自定義指定：您可以手動分配所需的DNS。

IP池：連線到該VPN後分配給使用者的IP。

配置檔案設定：包括此[Machine Tunnel](#)的VPN配置檔案或包括區域FQDN，以便終端使用者選擇要連線到的區域（取決於部署的IP池）。

通訊協定：選擇希望VPN使用者用於流量隧道的協定。

連線時間狀態（可選）：如果需要在連線時執行[VPN狀態](#)。此處顯示更多資訊

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配置檔案配置 — 第1部分

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配置檔案配置 — 第2部分

驗證、授權及記帳

通訊協定：選擇SAML。

使用CA憑證的驗證:如果您希望使用SSL證書進行身份驗證，並根據IdP SAML提供程式進行授權。
強制重新驗證：每次建立VPN連線時都強制重新進行身份驗證。強制重新身份驗證基於會話超時。
這可能會受SAML IdP設定的影響（本例中為Azure）。

上載在步驟6的「配置Azure」中下載的XML檔案聯合後設資料的XML檔案。

The screenshot displays the SAML configuration interface. At the top, under 'Protocols', 'SAML' is selected in a dropdown menu. Below this, there is a checkbox for 'Authenticate with CA certificates' which is currently unchecked. The 'SAML Configuration' section includes two options: 'External browser authentication' (unchecked) and 'Forced re-authentication' (checked). The main area is titled 'SAML Metadata XML Configuration' and contains three numbered steps: 1. 'Download Service Provider XML file' with a 'Download service provider XML file' button; 2. 'Generate IdP Security Metadata XML File' with sub-steps 'a. Upload the Service Provider XML file to your IdP.' and 'b. From your IdP, create and download an IdP Security Metadata XML file.'; 3. 'Upload IdP security metadata XML file' with a status message 'File 'Cisco Secure Access RA VPN.xml' uploaded.' and 'Replace' and 'Delete' buttons.

SAML配置

流量控制（分隔通道）

通道模式：

連線到Secure Access:所有流量都以通道傳送（全部通道）。

繞過安全訪問：只有在Exceptions部分中定義的特定流量通過隧道傳輸（拆分隧道）。

DNS模式：

預設DNS:所有DNS查詢都通過VPN配置檔案定義的DNS伺服器。在出現否定響應的情況下，DNS查詢還可以轉到在物理介面卡上配置的DNS伺服器。

通道所有DNS:通過VPN隧道傳輸所有DNS查詢。

拆分DNS:僅特定的DNS查詢通過VPN配置檔案，具體取決於下面指定的域。

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

流量控制配置

思科安全客戶端配置

就本指南而言，我們不配置任何這些高級設定。可在此處配置高級功能，例如：TND、永遠線上、證書匹配、本地Lan訪問等。請在此處儲存設定。

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

高級設定

3. 您的VPN配置檔案必須如下所示。您可以將xml配置檔案下載並預部署給終端使用者(在「C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile」下)，以開始使用VPN，或向他們提供要在Cisco Secure Client - AnyConnect VPN UI中輸入的配置檔案URL。

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	sse.cisco.com/VPN_EntraID	Download XML

全域性FQDN和配置檔案URL

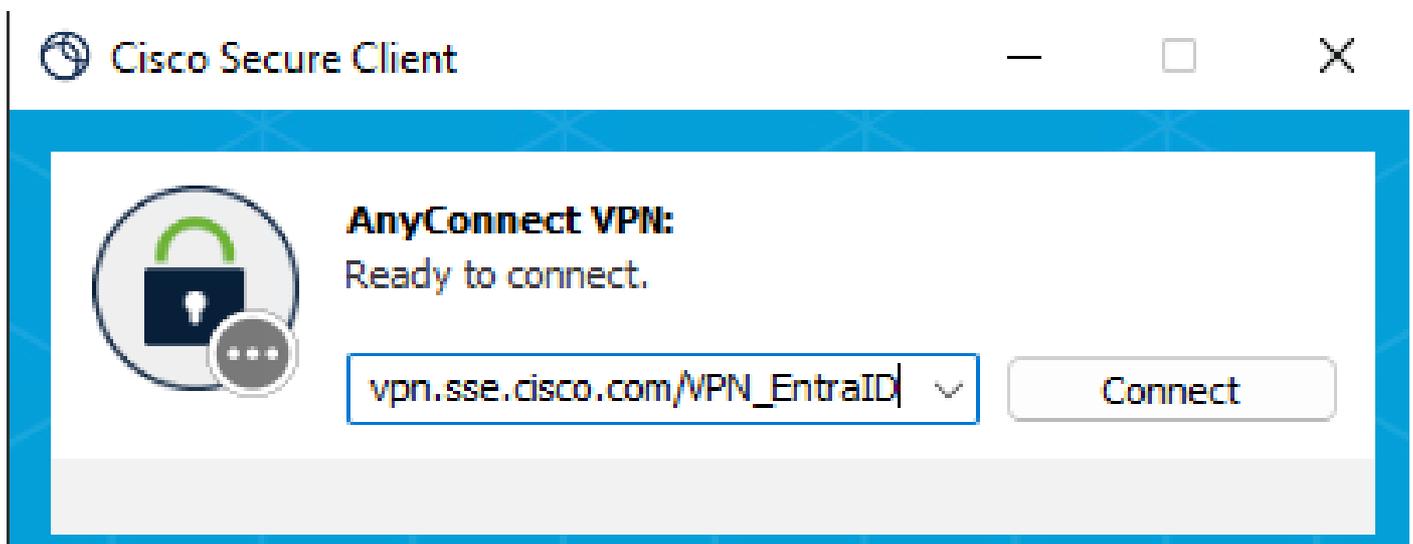
驗證

此時，您的RA VPN配置必須準備好進行測試。

請注意，使用者首次連線時，需要為其提供配置檔案URL地址或預部署PC中「C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile」下的xml配置檔案，重新啟動VPN服務，並且他們必須在下拉選單中看到連線到此VPN配置檔案的選項。

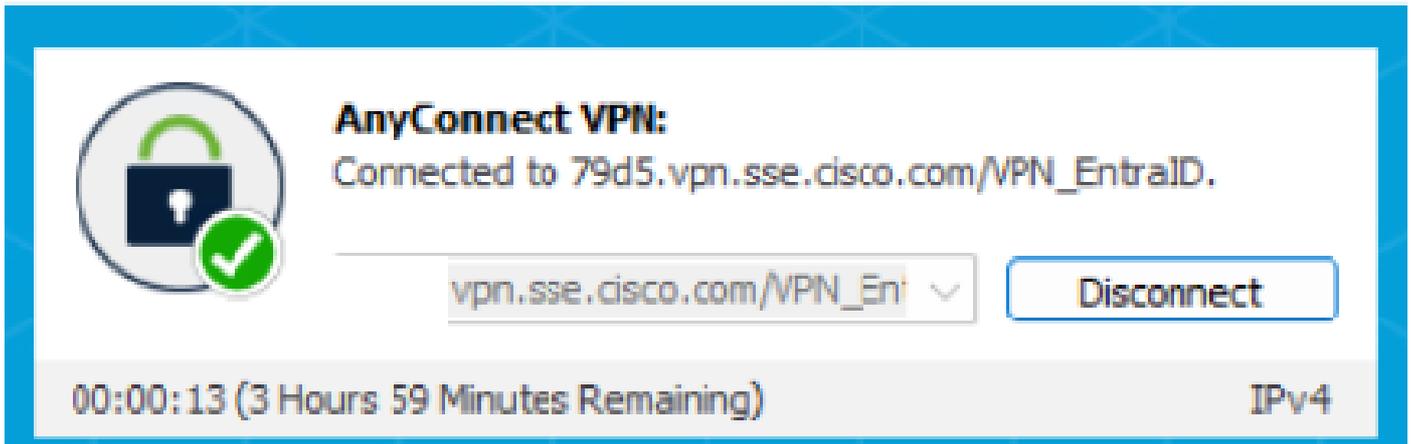
在本例中，我們為首次連線嘗試的使用者提供配置檔案URL地址。

在第一個連線之前：



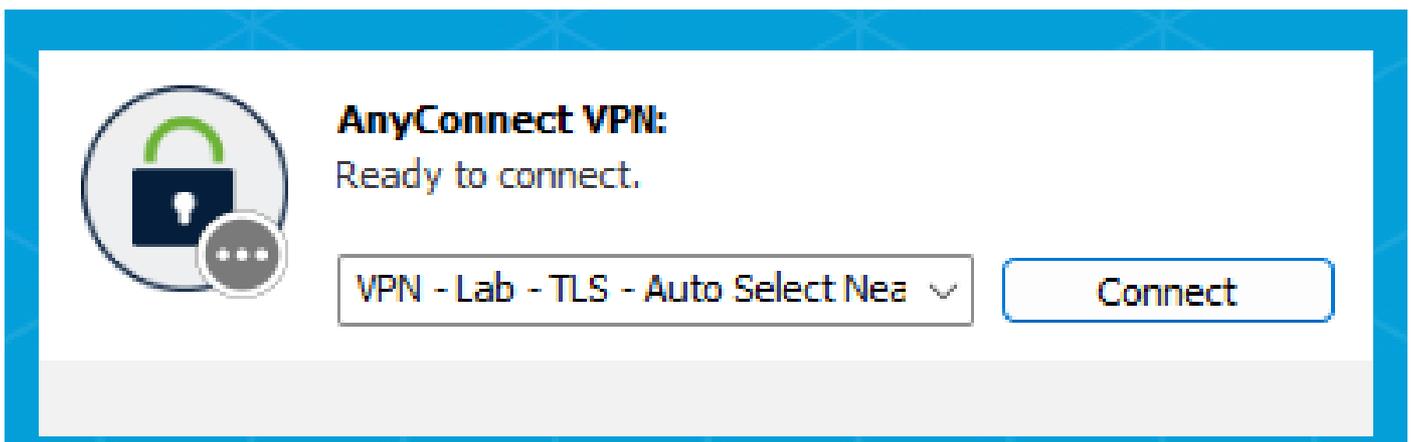
先前的VPN連線

輸入您的憑證並連線到VPN:



已連線到VPN

首次連線後，從下拉選單中，您必須現在能夠看到連線到「VPN - Lab」VPN配置檔案的選項：



第一個VPN連線之後

簽入使用者能夠連線的遠端訪問日誌：

Monitor > Remote Access Log

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

登入Cisco Secure Access

疑難排解

以下是可對某些常見問題執行的基本故障排除：

Azure

在Azure中，確保已將使用者分配到針對思科安全訪問進行身份驗證的企業應用程式：

首頁>企業應用程式> Cisco Secure Access RA VPN >管理>使用者和組

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

驗證使用者分配

Cisco Secure Access

在Cisco Secure Access中，確保您已調配了允許通過RA VPN連線的使用者，並且在Cisco Secure Access中調配的使用者（在使用者、組和終端裝置下）也與Azure中的使用者（在企業應用程式中分配的使用者）匹配。

Connect > Users , Groups , and Endpoint Devices

The screenshot shows the Cisco Secure Access console interface. The main heading is "Users, Groups, and Endpoint Devices" with a subtitle "Provision and manage the authentication of users, groups, and endpoint devices, for access control purposes." Below this, there are three tabs: "Users" (7), "Groups and Organizational Units" (4), and "Endpoint Devices" (2). The "Users" tab is active. The "Users" section contains a search bar with "josue" entered, and filters for "Source" and "Directory". It shows "3 results". Below the search is a table with columns: Name, Email, Username, Source, and Directory. The table contains one entry for "Josue" with email "josue@", username "josue@", source "azure", and directory "Entra ID".

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

思科安全訪問中的使用者

驗證已在PC上為使用者調配了正確的XML檔案，或已為使用者提供了配置檔案URL（如「驗證」步驟中所述）。

連線>終端使用者連線>虛擬專用網路

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](#)

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	

配置檔案URL和.xml配置檔案

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。