

在安全防火牆上配置零信任遠端訪問部署

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[先決條件配置](#)

[常規配置](#)

[配置應用程式組](#)

[應用組1：使用Duo作為IdP](#)

[應用程式組2：使用Microsoft Entra ID\(Azure AD\)作為IdP](#)

[配置應用程式](#)

[應用程式1：測試FMC Web UI \(應用程式組1的成員\)](#)

[應用程式2:CTB Web UI \(應用程式組2的成員\)](#)

[驗證](#)

[監視](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文描述在安全防火牆上配置無客戶端零信任訪問遠端訪問部署的過程。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower Management Center (FMC)
- 基本ZTNA知識
- 基本安全斷言標籤語言(SAML)知識

採用元件

本檔案中的資訊是根據以下軟體版本：

- 安全防火牆版本7.4.1
- Firepower管理中心(FMC)版本7.4.1

- Duo作為身份提供者(IdP)
- 作為IdP的Microsoft Entra ID (以前稱為Azure AD)

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。

背景資訊

零信任訪問功能基於零信任網路訪問(ZTNA)原則。ZTNA是一種零信任安全模型，消除了隱性信任。該模型在驗證使用者、請求上下文以及分析訪問被授予的風險後，授予最小許可權訪問許可權。

目前ZTNA的要求和限制如下：

- 受FMC 7.4.0+版 (Firepower 4200系列) 管理的安全防火牆版本7.4.0+支援
- 受FMC版本7.4.1+管理的安全防火牆版本7.4.1+支援 (所有其他平台)
- 僅支援Web應用程式(HTTPS)。不支援要求解密豁免的場景
- 僅支援SAML IdP
- 遠端訪問需要公共DNS更新
- 不支援IPv6。不支援NAT66、NAT64和NAT46方案
- 只有啟用Snort 3後，威脅防禦功能才可用
- 受保護的Web應用程式中的所有超連結都必須具有相對路徑
- 在虛擬主機或內部負載平衡器後面運行的受保護的Web應用程式必須使用相同的外部 and 內部 URL
- 在單獨模式群集上不受支援
- 啟用了嚴格HTTP主機標頭驗證的應用程式不支援
- 如果應用程式伺服器託管多個應用程式並根據TLS客戶端Hello中的伺服器名稱指示(SNI)標頭提供內容，則零信任應用程式配置的外部URL必須與特定應用程式的SNI匹配
- 僅在路由模式下支援
- 需要智慧許可證 (無法在評估模式下工作)

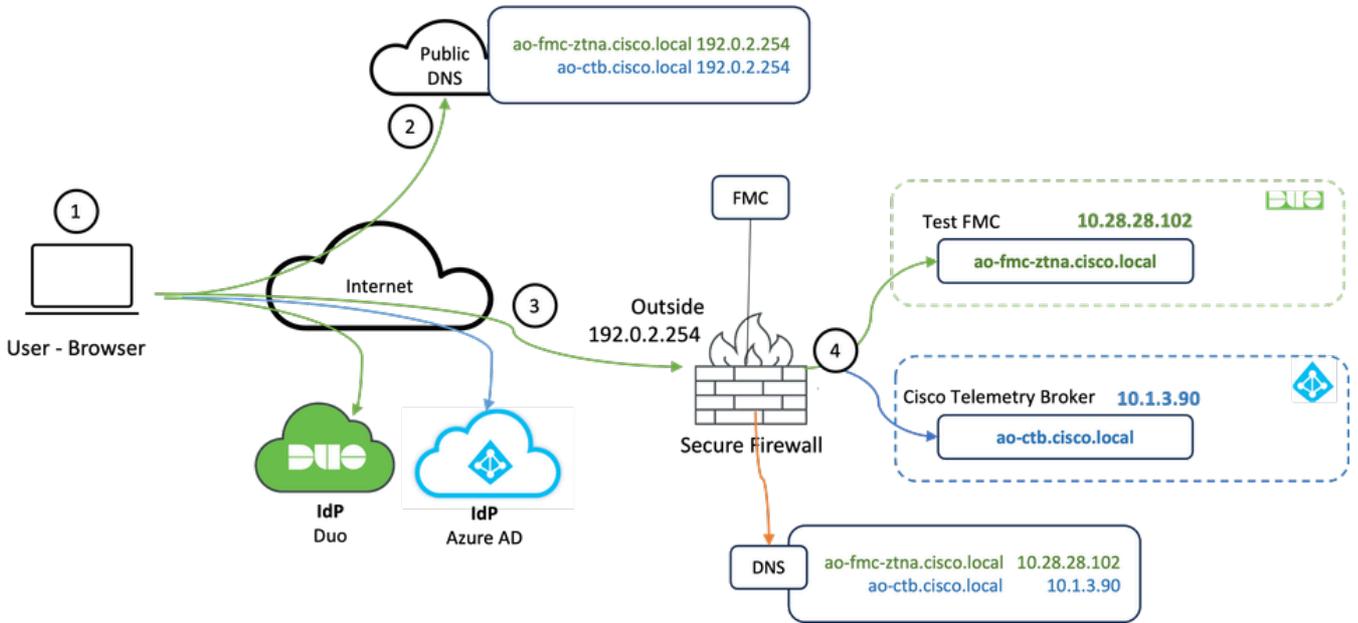
有關安全防火牆中零信任訪問的詳細資訊和詳細資訊，請參閱[思科安全防火牆管理中心裝置配置指南7.4](#)。

設定

本文檔重點介紹ZTNA的遠端訪問部署。

在此示例場景中，遠端使用者需要訪問測試FMC和思科遙測代理(CTB)的Web使用者介面(UI)，它們託管在安全防火牆之後。訪問這些應用程式由兩個不同的IdP分別授予：Duo和Microsoft Entra ID，如下圖所示。

網路圖表



拓撲圖表

1. 遠端使用者需要訪問安全防火牆後託管的應用程式。
2. 每個應用程式在公共DNS伺服器中必須有一個DNS條目。
3. 這些應用程式名稱必須解析為安全防火牆外部介面的IP地址。
4. 安全防火牆解析為應用程式的實際IP地址，並使用SAML身份驗證對每個應用程式驗證每個使用者。

先決條件配置

身分識別提供程式(IdP)和網域名稱伺服器(DNS)

- 必須在SAML身份提供程式(IdP)中配置應用程式或應用程式組，例如Duo、Okta或Azure AD。在此示例中，Duo和Microsoft Entra ID用作IdP。
- 在安全防火牆上配置應用程式時，會使用由IdP生成的證書和後設資料

內部和外部DNS伺服器

- 外部DNS伺服器 (由遠端使用者使用) 必須具有應用程式的FQDN條目，並解析到安全防火牆外部介面IP地址
- 內部DNS伺服器 (由Secure Firewall使用) 必須具有應用程式的FQDN條目，並解析為應用程式的實際IP地址

憑證

ZTNA策略配置需要以下證書：

- 身份/代理證書：由安全防火牆用於偽裝應用程式。此處的安全防火牆充當SAML服務提供商 (SP)。此證書必須是與專用應用程式的FQDN相匹配的萬用字元或使用者替代名稱(SAN)證書 (在預身份驗證階段代表所有專用應用程式的通用證書)
- IdP證書：用於身份驗證的IdP為定義的每個應用程式或應用程式組提供證書。必須配置此證書，以便安全防火牆能夠驗證傳入SAML斷言上的IdP簽名 (如果這是針對應用程式組定義的，則同一證書將用於整個應用程式組)
- 應用證書：從遠端使用者到應用的加密流量需要由安全防火牆解密，因此，必須將每個應用的證書鏈和私鑰新增到安全防火牆。

常規配置

要配置新的零信任應用程式，請執行以下步驟：

1. 導航到Policies > Access Control > Zero Trust Application，然後點選Add Policy。
2. 填寫必填欄位：

a) General：輸入策略的名稱和說明。

b) 域名：這是新增到DNS中的名稱，必須解析到訪問應用程式的威脅防禦網關介面。



注意：域名用於為應用程式組中的所有專用應用程式生成ACS URL。

c) 身份證書：這是代表預身份驗證階段的所有專用應用程式的通用證書。



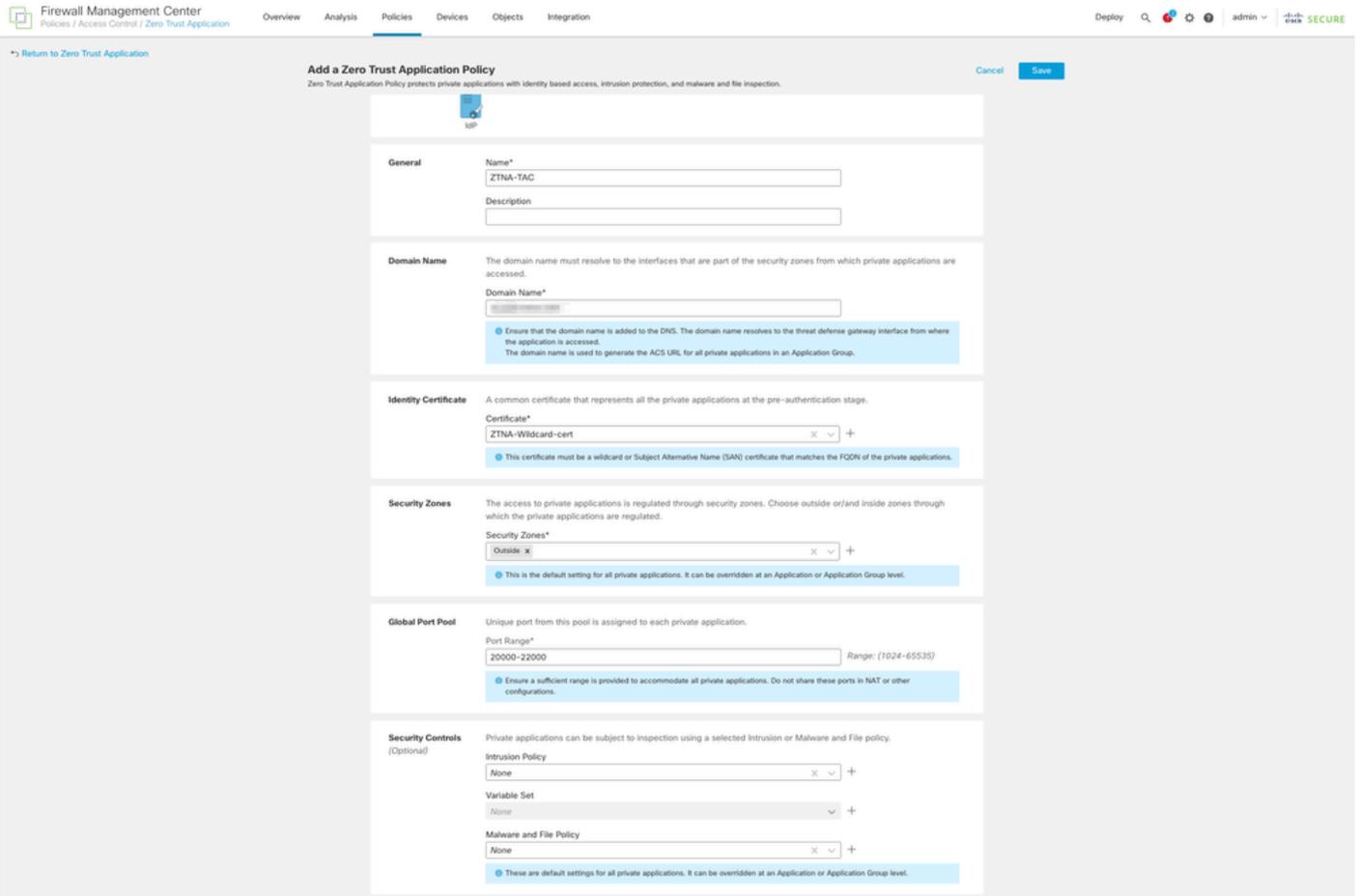
注意：此證書必須是與專用應用程式的FQDN相匹配的萬用字元或使用者替代名稱(SAN)證書。

d) Security Zones：選擇用於管理專用應用程式的outside或/和inside zones。

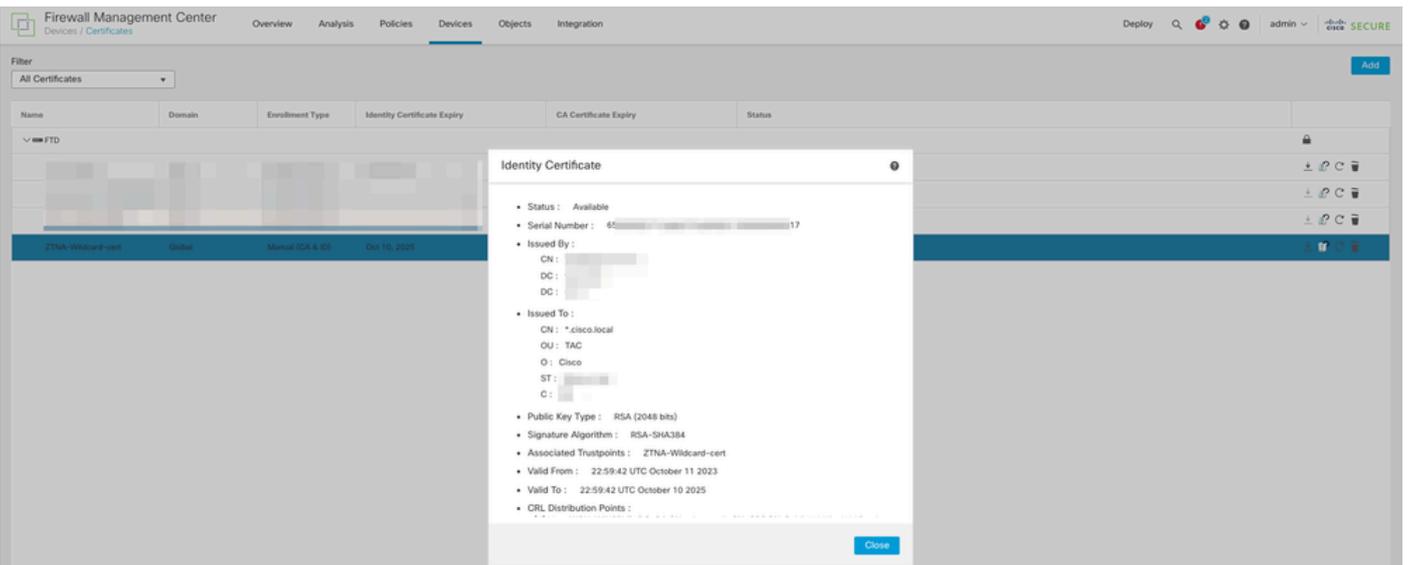
e) 全域性埠池：此池中的唯一埠分配給每個專用應用程式。

f) 安全控制 (可選)：選擇是否對私人申請進行檢查。

在此範例組態中，輸入以下資訊：



在此案例中使用的身份/代理證書是與專用應用程式的FQDN匹配的萬用字元證書：



3.儲存策略。

4. 建立新的應用程式組和/或新的應用程式：

- 應用定義具有SAML身份驗證、介面訪問、入侵和惡意軟體以及檔案策略的專用Web應用。
- Application Group允許您對多個應用程式進行分組，並共用通用設定，例如SAML身份驗證、介面訪問和安全控制設定。

在此範例中，設定兩個不同的應用程式群組和兩個不同的應用程式：一個用於Duo進行驗證的應用程式（測試FMC Web UI），另一個用於Microsoft Entra ID(CTB Web UI)進行驗證的應用程式。

配置應用程式組

應用組1：使用Duo作為IdP

a. 輸入應用程式組名稱，然後按一下下一步以顯示的SAML服務提供程式(SP)後設資料。

Add Application Group ? ×

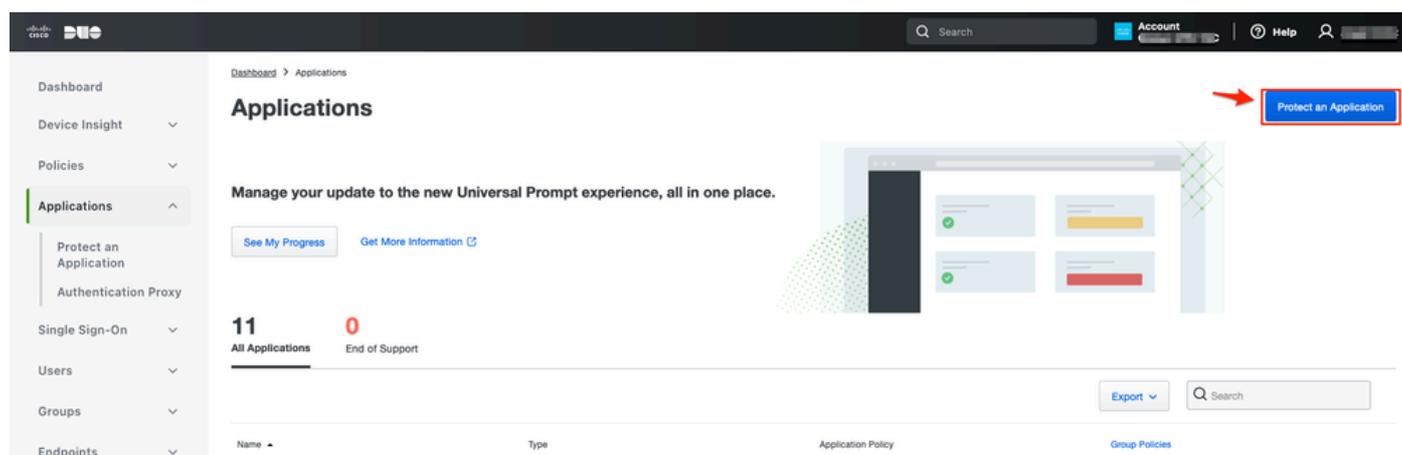
An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- Application Group** Edit
Name: External_Duo
- SAML Service Provider (SP) Metadata**
The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.
Entity ID: Copy
Assertion Consumer Service (ACS) URL: Copy
Download SP Metadata Next
- SAML Identity Provider (IdP) Metadata
- Re-Authentication Interval
- Security Zones and Security Controls

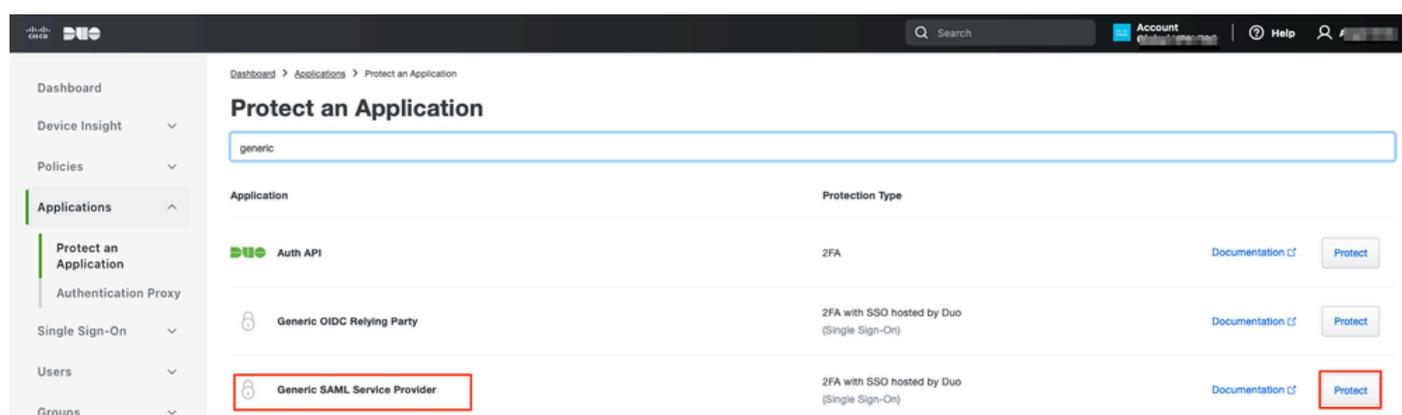
Cancel Finish

b. 顯示SAML SP後設資料後，請轉到IdP並配置新的SAML SSO應用程式。

c. 登入到Duo，然後導航到Applications > Protect an an Application。



d. 查詢通用SAML服務提供程式，然後按一下保護。



e. 從IdP下載證書和SAML後設資料，因為在Secure Firewall上繼續配置需要該後設資料。

f. 輸入ZTNA應用程式組（在步驟a中生成）的實體ID和斷言使用者服務(ACS)URL。

- Dashboard
- Device Insight ▼
- Policies ▼
- Applications ▲**
 - Protect an Application
 - Authentication Proxy
- Single Sign-On ▼
- Users ▼
- Groups ▼
- Endpoints ▼
- 2FA Devices ▼
- Administrators ▼
- Trusted Endpoints
- Trust Monitor ▼
- Reports ▼
- Settings
- Billing ▼

You're using the new Admin Panel menu and left-side navigation.

[Provide feedback](#)

[Temporarily switch to the old experience](#)

Generic SAML Service Provider - Single Sign-On 1

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<code>https://sso-.../metadata</code>	Copy
Single Sign-On URL	<code>https://sso-8.../sso</code>	Copy
Single Log-Out URL	<code>https://sso-i.../slo</code>	Copy
Metadata URL	<code>https://sso-8.../metadata</code>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<code>9E:5...5C</code>	Copy
SHA-256 Fingerprint	<code>?:85:...E9:52</code>	Copy

Downloads

Certificate	Download certificate	Expires: 01-19-2038
SAML Metadata	Download XML	

Service Provider

Metadata Discovery None (manual input) ▼

[Early Access](#)

Entity ID * `https://.../External_Duo/saml/sp/metadata`

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL * `https://.../External_Duo/+CSCOE+/saml/sp/ac`

[+ Add an ACS URL](#)

g. 根據您的特定要求編輯應用程式，僅允許目標使用者訪問應用程式，然後按一下儲存。

Type Generic SAML Service Provider - Single Sign-On

Name
 Duo Push users will see this when approving transactions.

Self-service portal Let users remove devices, add new devices, and reactivate Duo Mobile
 See [Self-Service Portal documentation](#)
 To allow Duo to notify users about self-service portal activity, select [Settings > Notifications](#)

Username normalization Username normalization for Single-Sign On applications is controlled by the enabled authentication source. Please visit your [authentication source](#) to modify this configuration.
 Controls if a username should be altered before trying to match them with a Duo user account.

Voice greeting
 Specify the message read to users who use phone callback, followed by authentication instructions. Maximum 512 characters.

Notes
 For internal use. Maximum 512 characters.

Administrative unit

Permitted groups Only allow authentication from users in certain groups

 When unchecked, all users can authenticate to this application.

Allowed Hostnames Since this application is using Frameless Duo Universal Prompt, configuring allowed hostnames is no longer supported.
 [Get more information](#)

h. 使用從IdP下載的檔案導航回到FMC，並將SAML IdP後設資料新增到應用程式組。

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

- 1 Application Group** Edit
Name External_Duo
- 2 SAML Service Provider (SP) Metadata** Edit
Entity ID https://[redacted]/External_Duo/saml/sp/metadata
Assertion Consumer Service (ACS) URL https://[redacted]/External_Duo/+CSCOE+/saml/sp/acs?tgname=D...

3 SAML Identity Provider (IdP) Metadata

Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.

Import IdP Metadata
 Manual Configuration
 Configure Later

Import IdP Metadata

Drag and drop your file here
[or select file](#)
External Applications ZTNA - IDP Metadata.xml

Entity ID*
https://sso-8[redacted] N

Single Sign-On URL*
https://sso-8[redacted] N

IdP Certificate
MIIDDTC[redacted]yDQYJKoZI
[redacted]

Next

Cancel Finish

i. 按一下Next，然後根據要求設定Re-Authentication Interval和Security Controls。檢視摘要配置，然後按一下Finish。

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group	Name	External_Duo	Edit
2 SAML Service Provider (SP) Metadata	Entity ID	https://[redacted] External_Duo/saml/sp/metadata	Edit
	Assertion Consumer Service (ACS) URL	https://[redacted] External_Duo/+CSCOE+/saml/sp/acs?tname=D...	
3 SAML Identity Provider (IdP) Metadata	Entity ID	https://ssc [redacted]	Edit
	Single Sign-On URL	https://ssc [redacted]	
	IdP Certificate	External_Duo-1697063490514	
4 Re-Authentication Interval	Timeout Interval	1440 minutes	Edit
5 Security Zones and Security Controls	Security Zones	Inherited: (Outside)	Edit
	Intrusion Policy	Inherited: (None)	
	Variable Set	Inherited: (None)	
	Malware and File Policy	Inherited: (None)	

Cancel

Finish

應用程式組2：使用Microsoft Entra ID(Azure AD)作為IdP

a.輸入應用程式組名稱，然後按一下下一步以顯示的SAML服務提供程式(SP)後設資料。

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group

Edit

Name Azure_apps

2 SAML Service Provider (SP) Metadata

The service provider's metadata for the Application Group are dynamically generated and cannot be modified. Copy or download the SP metadata file as required for use in your IdP.

Entity ID

https://[redacted]/Azure_apps/saml/sp/metadata

Copy

Assertion Consumer Service (ACS) URL

https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tgname=[redacted]

Copy

Download SP Metadata

Next

3 SAML Identity Provider (IdP) Metadata

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

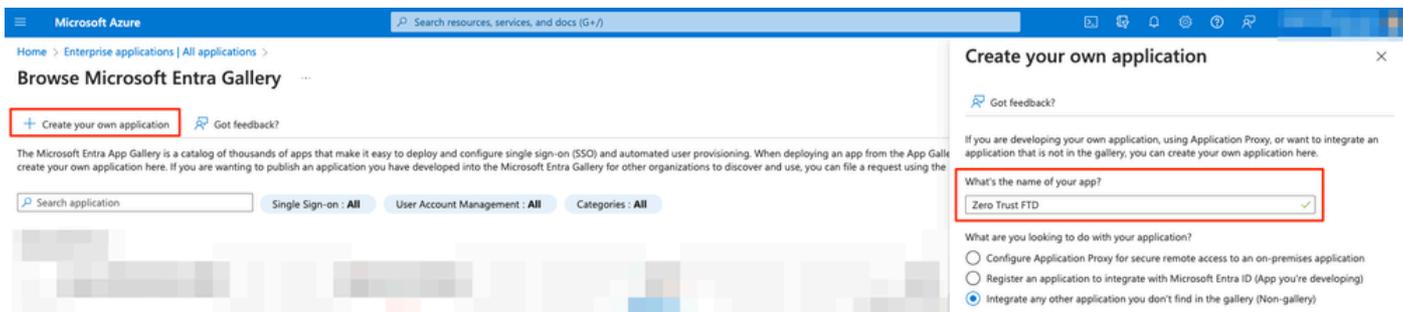
Finish

b.顯示SAML SP後設資料後，請轉到IdP並配置新的SAML SSO應用程式。

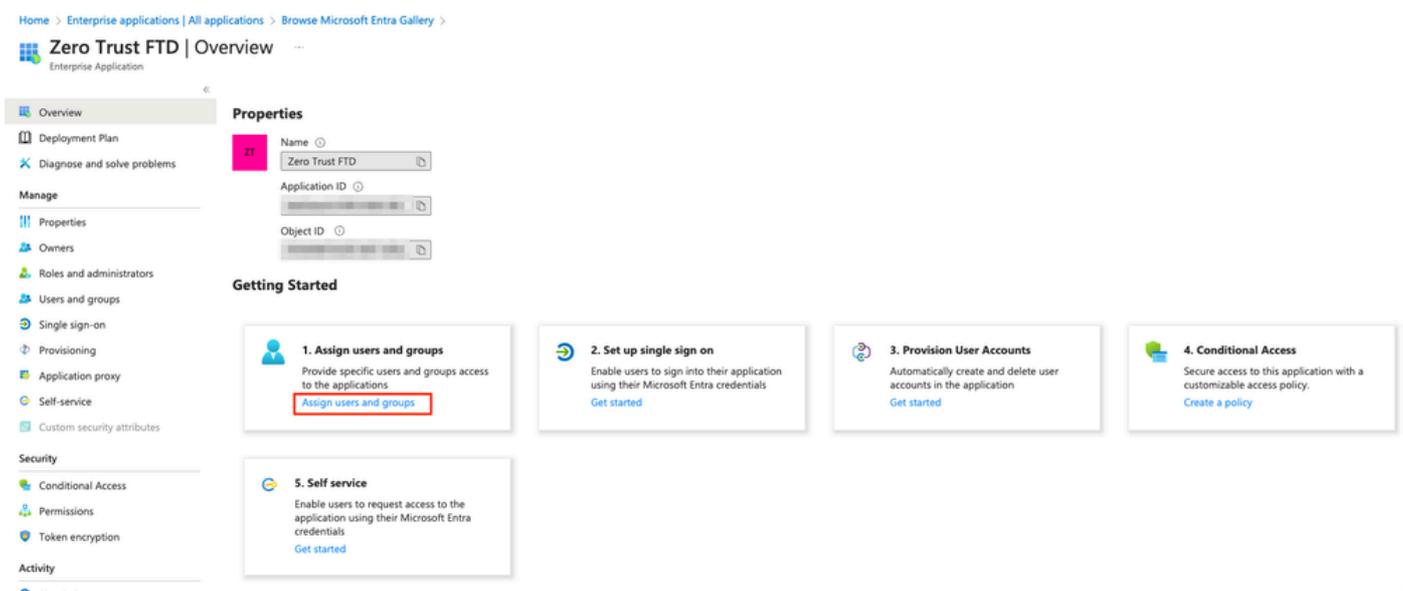
c.登入到Microsoft Azure，然後導航到「企業應用程式」>「新應用程式」。

The screenshot shows the Microsoft Azure portal interface for managing Enterprise applications. The breadcrumb navigation is 'Home > Enterprise applications'. The main heading is 'Enterprise applications | All applications'. Below the heading, there are several action buttons: '+ New application' (highlighted with a red box), 'Refresh', 'Download (Export)', 'Preview info', 'Columns', 'Preview features', and 'Got feedback?'. The main content area displays a table of applications with columns for Name, Object ID, Application ID, Homepage URL, and Created on. The table shows 77 applications found. The left sidebar has a 'Manage' section with 'All applications' highlighted by a red box.

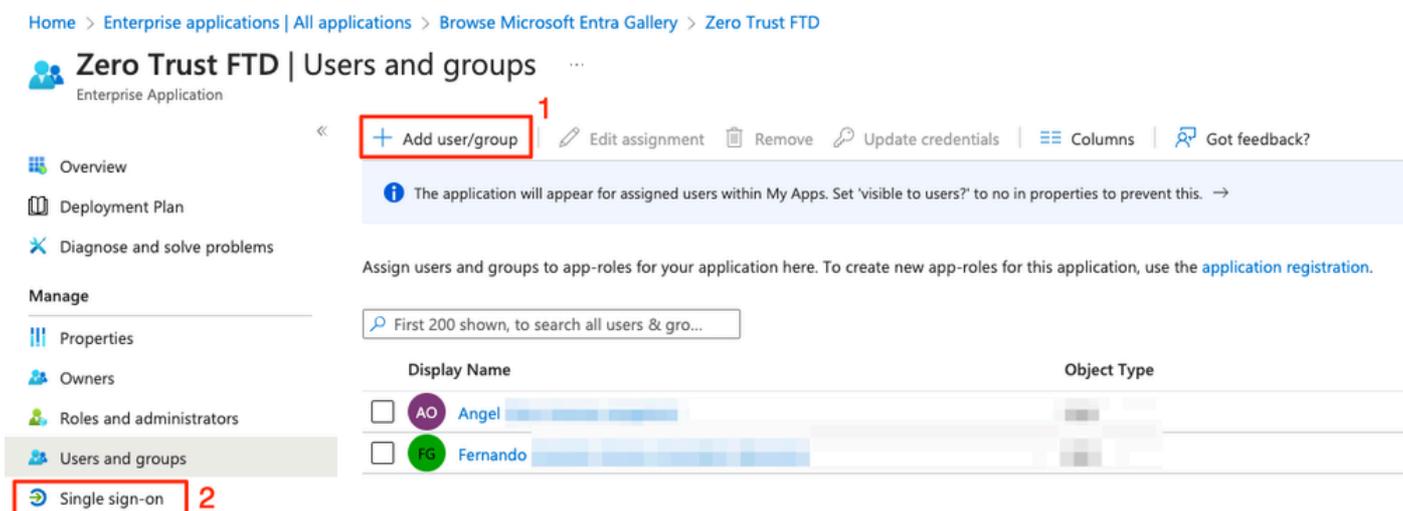
d.按一下建立自己的應用程式>輸入應用程式的名稱>建立



e. 開啟應用程式，然後按一下分配使用者和組，以定義允許訪問應用程式的使用者和/或組。



f. 按一下Add user/group > Select the needed users/groups > Assign。分配正確的使用者/組後，按一下單點登入。



g. 在Single sign-on部分中，按一下SAML。

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Zero Trust FTD

Zero Trust FTD | Single sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy

Select a single sign-on method [Help me decide](#)

 **Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

 **SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

 **Password-based**
Password storage and replay using a web browser extension or mobile app.

h. 按一下Upload metadata file 並選擇從服務提供商(Secure Firewall)下載的XML檔案，或手動從ZTNA應用程式組輸入Entity ID和Assertion Consumer Service(ACS)URL(在步驟a中生成)。

 **注意：**請確保也下載聯合後設資料XML或單獨下載證書（基本64），並從IdP（登入和註銷URL和Microsoft Entra識別符號）複製SAML後設資料，因為這些內容是繼續安全防火牆上的配置所必需的。

Zero Trust FTD | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs
 - Provisioning logs
 - Access reviews
- Troubleshooting + Support
 - New support request

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Zero Trust FTD.

- Basic SAML Configuration** Edit

Identifier (Entity ID)	https://[redacted]/Azure_apps/saml/sp/metadata
Reply URL (Assertion Consumer Service URL)	https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tgname=DefaultZeroTrustGroup
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims** Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates**

Token signing certificate Edit	Active
Status	Active
Thumbprint	[redacted]
Expiration	[redacted]
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download
Verification certificates (optional) Edit	
Required	No
Active	0
Expired	0
- Set up Zero Trust FTD**

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://[redacted]
Microsoft Entra Identifier	https://[redacted]
Logout URL	https://[redacted]

i. 使用從IdP下載的後設資料檔案或手動輸入所需資料，導航回到FMC，然後將SAML IdP後設資料匯入到應用程式組2。

Add Application Group



An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group

Name Azure_apps

Edit

2 SAML Service Provider (SP) Metadata

Entity ID https://[redacted]/Azure_apps/saml/sp/metadata
Assertion Consumer Service (ACS) URL https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=Def...

Edit

3 SAML Identity Provider (IdP) Metadata

Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.

Import IdP Metadata

Manual Configuration

Configure Later

Import IdP Metadata

Drag and drop your file here
or select file
Zero Trust FTD.xml

Entity ID*

https://[redacted]

Single Sign-On URL*

https://[redacted]

IdP Certificate

MIIC8DCCAdigAwIBAgIQdTt7Lwlj7aRGm1m212dU/DANBgkqhkiG9w0B

[redacted]

Next

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel

Finish

j. 按一下下一步，然後根據要求配置重新身份驗證間隔和安全控制。檢視摘要配置，然後按一下 Finish。

Add Application Group ? X

An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1	Application Group		Edit
	Name	Azure_apps	
2	SAML Service Provider (SP) Metadata		Edit
	Entity ID	https://[redacted]/Azure_apps/saml/sp/metadata	
	Assertion Consumer Service (ACS) URL	https://[redacted]/Azure_apps/+CSCOE+/saml/sp/acs?tname=Def...	
3	SAML Identity Provider (IdP) Metadata		Edit
	Entity ID	https://[redacted]	
	Single Sign-On URL	https://[redacted]	
	IdP Certificate	[redacted]	
4	Re-Authentication Interval		Edit
	Timeout Interval	1440 minutes	
5	Security Zones and Security Controls		Edit
	Security Zones	Inherited: (Outside)	
	Intrusion Policy	Inherited: (None)	
	Variable Set	Inherited: (None)	
	Malware and File Policy	Inherited: (None)	

Cancel
Finish

配置應用程式

建立應用程式組後，按一下Add Application以定義要遠端保護和訪問的應用程式。

1. 輸入應用程式設定：

a) 應用程式名稱：已配置應用的識別符號。

b) 外部URL：公用/外部DNS記錄中應用程式的已發佈URL。這是使用者用於遠端訪問應用程式的URL。

c) 應用程式URL：應用程式的實際FQDN或網路IP。這是Secure Firewall用於訪問應用程式的URL。

注意：預設情況下，外部URL用作應用程式URL。取消選中此覈取方塊可指定其他應用程式URL。

d) Application Certificate：要訪問的應用程式的證書鏈和私鑰(從FMC首頁>對象>對象管理> PKI >內部證書新增的)

e)IPv4 NAT源 (可選) : 在將資料包轉發到應用程式之前, 會將遠端使用者的源IP地址轉換為所選地址 (僅支援具有IPv4地址的主機和範圍型別網路對象/對象組)。可以對此進行配置, 以確保應用程式具有通過安全防火牆返回到遠端使用者的路由

f)應用程式組 (可選) : 選擇是否將此應用程式新增到現有應用程式組, 以使用為其配置的設定。

在本示例中, 使用ZTNA訪問的應用程式是測試FMC Web UI和位於安全防火牆後面的CTB的Web UI。

必須在對象>對象管理> PKI >內部證書中新增應用程式的證書 :

Add Known Internal Certificate ?

Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----  
[Redacted Certificate Data]  
T  
G  
1Y
```

Key or, choose a file:

```
-----BEGIN RSA PRIVATE KEY-----  
[Redacted Private Key Data]
```

Encrypted, and the password is:

 注意 : 確保為要使用ZTNA訪問的每個應用程式新增所有證書。

將證書新增為內部證書後，繼續配置其餘設定。

為此示例配置的應用程式設定如下：

應用程式1：測試FMC Web UI (應用程式組1的成員)

Add Application ? ×

Enabled

1 Application Settings

Application Name*
FMC

External URL* ⓘ
https://ao-fmc-ztna.cisco.local

Application URL (FQDN or Network IP)*
https://ao-fmc-ztna.cisco.local

Use External URL as Application URL
By default, External URL is used as Application URL. Uncheck the checkbox to specify a different URL. For e.g., https://10.72.34.57:8443

Application Certificate* ⓘ
ao-fmc-ztna.cisco.local × ▼ +

IPv4 NAT Source ⓘ
Select... ▼ +

Application Group
External_Duo × ▼

Next

2 SAML Service Provider (SP) Metadata

3 SAML Identity Provider (IdP) Metadata

4 Re-Authentication Interval

5 Security Zones and Security Controls

Cancel **Finish**

將應用程式新增到應用程式組1後，將繼承此應用程式的其餘設定。您仍然可以使用不同的設定覆蓋安全區域和安全控制。

檢視已配置的應用程式，然後按一下Finish。

Add Application ? ×

Enabled

1 Application Settings Edit

Application Name	FMC
External URL	https://ao-fmc-ztna.cisco.local
Application URL	https://ao-fmc-ztna.cisco.local
IPv4 NAT Source	-
Application Certificate	ao-fmc-ztna.cisco.local
Application Group	External_Duo

2 SAML Service Provider (SP) Metadata

Configurations are derived from Application Group 'External_Duo'

3 SAML Identity Provider (IdP) Metadata

Configurations are derived from Application Group 'External_Duo'

4 Re-Authentication Interval

Configurations are derived from Application Group 'External_Duo'

5 Security Zones and Security Controls Edit

Security Zones	Inherited: (Outside)
Intrusion Policy	Inherited: (None)
Variable Set	Inherited: (None)
Malware and File Policy	Inherited: (None)

Cancel Finish

應用程式2:CTB Web UI (應用程式組2的成員)

下面是此應用程式的配置摘要：

Enabled

1 Application Settings Edit

Application Name	CTB
External URL	https://ao-ctb.cisco.local
Application URL	https://ao-ctb.cisco.local
IPv4 NAT Source	ZTNA_NAT_CTBT
Application Certificate	ao-ctb.cisco.local
Application Group	Azure_apps

2 SAML Service Provider (SP) Metadata
Configurations are derived from Application Group 'Azure_apps'

3 SAML Identity Provider (IdP) Metadata
Configurations are derived from Application Group 'Azure_apps'

4 Re-Authentication Interval
Configurations are derived from Application Group 'Azure_apps'

5 Security Zones and Security Controls Edit

Security Zones	Inherited: (Outside)
Intrusion Policy	Inherited: (None)
Variable Set	Inherited: (None)
Malware and File Policy	Inherited: (None)

Cancel Finish

 **注意：**請注意，對於此應用程式，網路對象「ZTNA_NAT_CTBT」配置為IPv4 NAT源。通過此配置，遠端使用者的源IP地址將轉換為已配置對象內的IP地址，然後再將資料包轉發到應用程式。

進行此配置是因為應用程式(CTBT)預設路由指向除安全防火牆之外的網關，因此返回流量未傳送到遠端使用者。通過此NAT配置，已在應用上配置靜態路由，使子網ZTNA_NAT_CTBT可以通過安全防火牆訪問。

配置好應用程式後，它們現在顯示在相應的應用程式組下。

ZTNA-TAC / Targeted: 1 device
Groups: 3 Applications:

Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled
Azure_apps (1 Application)			https://sts.v...	Outside (Inherited)	None (Inherited)	None (Inherited)	True
<input type="checkbox"/> CTBT	https://ao-ctb.cisco.local	https://ao-ctb.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True
External_Duo (1 Application)			https://sso-...	Outside (Inherited)	None (Inherited)	None (Inherited)	True
<input type="checkbox"/> FMT	https://ao-fmc-ztna.cisco.local	https://ao-fmc-ztna.cisco.local		Outside (Inherited)	None (Inherited)	None (Inherited)	True

最後，儲存更改並部署配置。

驗證

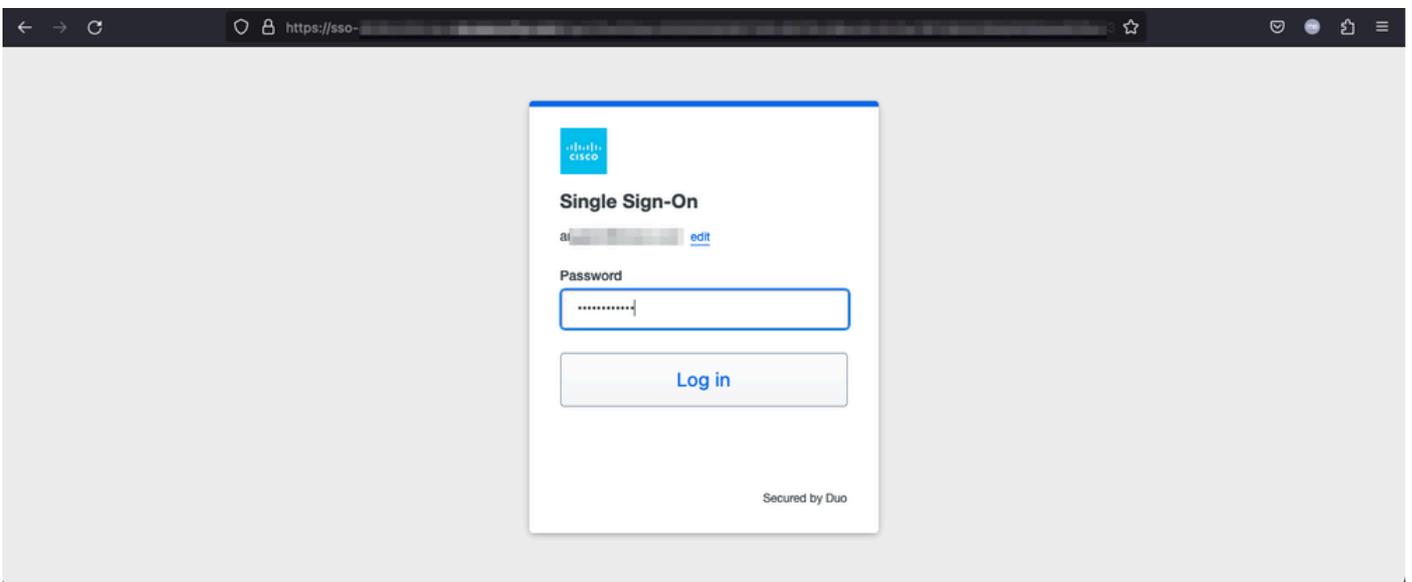
配置到位後，遠端使用者可以通過外部URL訪問應用程式，並且如果相應IdP允許他們訪問。

應用程式1

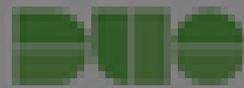
1.使用者開啟Web瀏覽器並導航到應用程式1的外部URL。在這種情況下，外部URL為「https://ao-fmc-ztna.cisco.local/」

 注意：外部URL名稱必須解析為已配置的安全防火牆介面的IP地址。在本例中，它解析為外部介面IP地址(192.0.2.254)

2.由於這是新訪問，因此使用者被重定向到為應用程式配置的IdP登入門戶。



3.向使用者傳送Push for MFA (這取決於IdP上配置的MFA方法)。



Accounts

Add



Are you logging in to **External Applications ZTNA?**

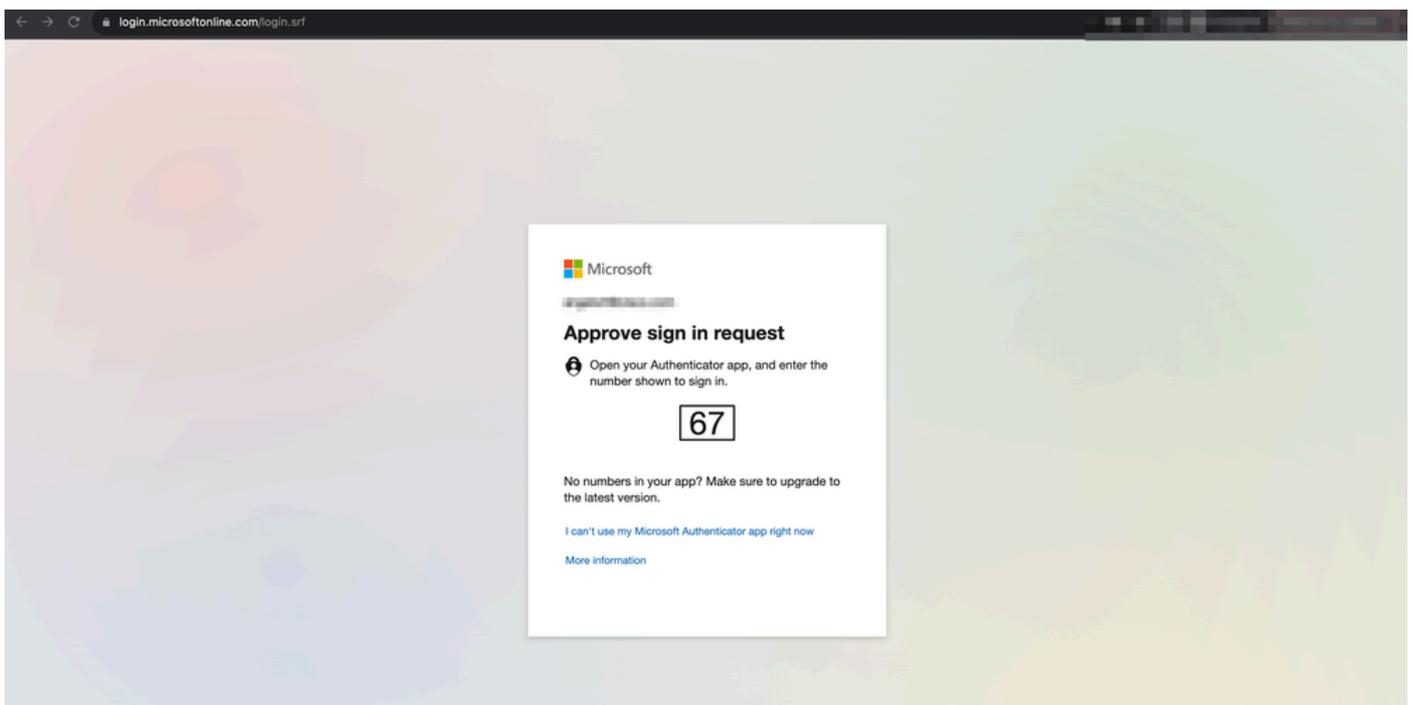
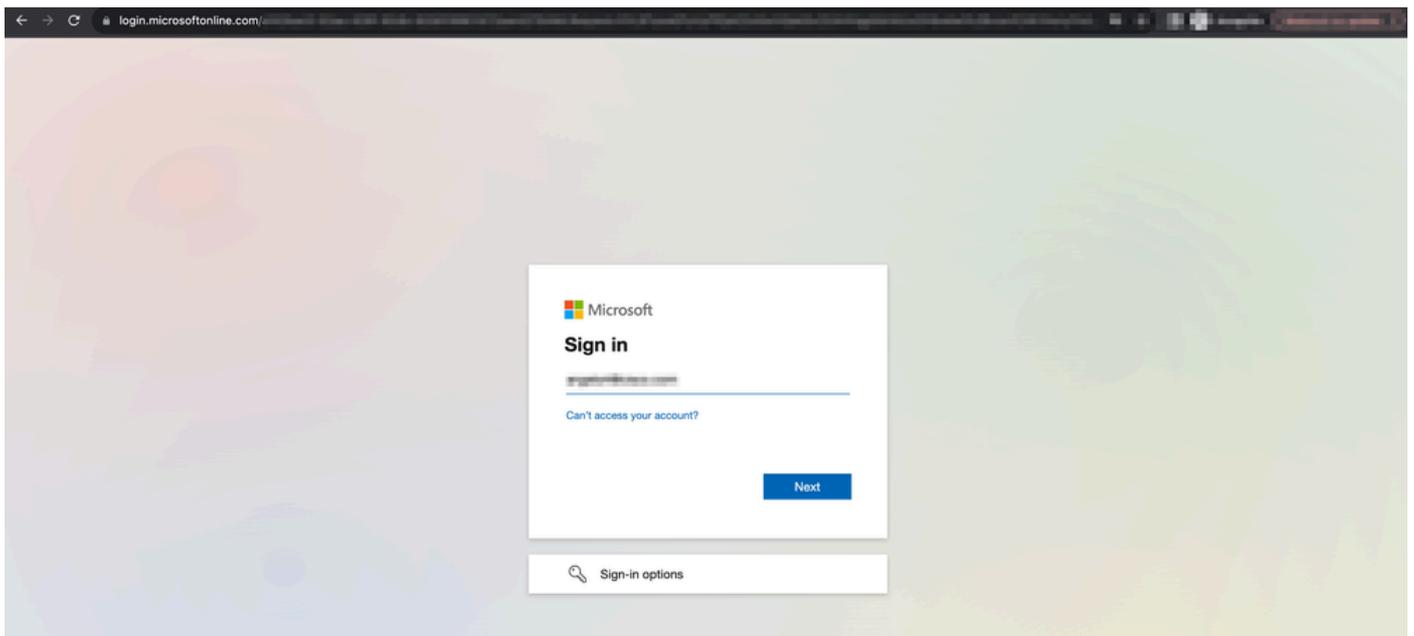
🌐 Global VPN TAC

🌐 [Redacted]

🕒 1:13 p.m.

👤 [Redacted]

2. 由於這是新訪問，因此使用者被重定向到為應用程式配置的IdP登入門戶。



3. 向使用者傳送Push for MFA (這取決於IdP上配置的MFA方法)。

4:24



Are you trying to sign in?



Enter the number shown to sign in.

Enter number

No, it's not me

Yes

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）。