

在安全防火牆上配置Azure Entra強制網路門戶

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[圖表](#)

[終端、FTD和Azure Entra之間的強制網路門戶](#)

[設定](#)

[第1階段：初始FMC和DNS配置](#)

[步驟 1:啟用思科動態屬性聯結器\(CSDAC\)](#)

[步驟 2:建立代表FTD輸入介面的完全限定網域名稱網路物件](#)

[步驟 3:配置DNS A記錄](#)

[第2階段：公開金鑰基礎架構組態](#)

[步驟 1:將內部CA證書匯入FMC](#)

[步驟 2:使用CA簽署服務提供商證書](#)

[步驟 3:將SP證書部署到FTD](#)

[第3階段：Azure配置](#)

[步驟 1:為SAML工具包建立Entra Enterprise應用程式](#)

[步驟 2:配置Entra ID應用註冊](#)

[步驟 3:為應用程式註冊配置Microsoft Graph API許可權。](#)

[步驟 4:配置事件中心\(EH\)名稱空間](#)

[步驟 5:在事件中心名稱空間中選擇或建立共用訪問策略](#)

[步驟 6:從EH名稱空間收集並記錄共用訪問簽名\(SAS\)資訊](#)

[步驟 7:在事件中心名稱空間中建立事件中心例項](#)

[步驟 8:在事件中心名稱空間中建立事件中心例項使用者組](#)

[步驟 9:驗證收集的值](#)

[步驟 10:配置Entra ID審計日誌流到事件中心](#)

[第4階段：整合Azure和FMC/FTD主動身份驗證配置](#)

[步驟 1:使用FMC嚮導配置Azure SAML/Entra ID領域](#)

[步驟 2:在Azure企業應用程式中實施FMC配置的SAML SP後設資料](#)

[步驟 3:使用FMC嚮導配置Azure SAML/Entra ID領域 \(續\)](#)

[步驟 4:檢查下載的使用者](#)

[第5階段：在FMC中配置策略](#)

[步驟 1:配置解密策略](#)

[步驟 2:配置解密策略規則](#)

[步驟 3:建立身份策略](#)

[步驟 4:配置身份策略規則](#)

[步驟 5:配置訪問控制策略](#)

[步驟 6:將配置部署到思科安全防火牆裝置](#)

[驗證](#)

[GUI](#)

[CLI](#)

[疑難排解](#)

[強制網路門戶調試](#)

[使用者身份轉儲](#)

[可能的問題](#)

[強制網路門戶未知證書頒發機構](#)

[Captive Portal "找不到伺服器](#)

[相關資訊](#)

簡介

本文檔介紹用於思科安全防火牆上的強制網路門戶（主動身份驗證）的Microsoft Azure Entra ID的配置。

必要條件

需求

思科建議瞭解以下主題：

- 安全斷言標籤語言(SAML)
- Microsoft Azure
- 思科安全防火牆管理中心(FMC)
- 思科安全防火牆威脅防禦(FTD)

在Azure for Event Hub建立中，你必須具有可用的標準定價層。此外，必須在啟用智慧許可和匯出控制功能的情況下啟用裝置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全FTD版本10.0
- Cisco安全FMC版本10.0

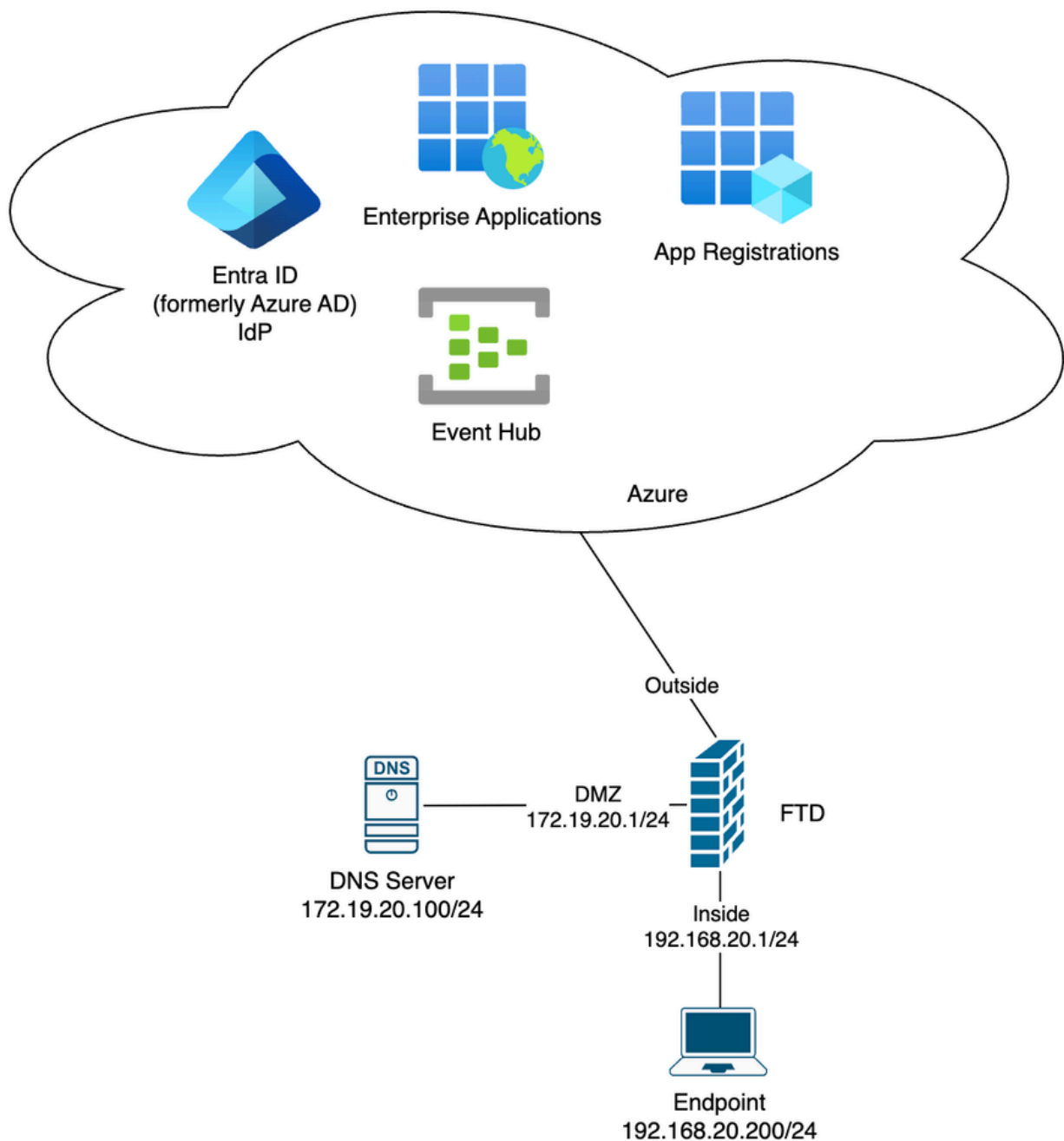
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

由於傳統的基於IP的安全架構難以跟上動態混合工作環境的步伐，與SAML整合的思科安全防火牆主動身份驗證提供了一個以身份為中心的強大解決方案。通過將Microsoft Entra ID(Azure AD)作為集中身份提供程式，此配置使管理員能夠超越靜態網路規則，並根據經過驗證的使用者身份而不是不穩定的網路地址實施粒度訪問控制。此整合通過無縫的單點登入(SSO)和強制的多因素身份驗證(MFA)最佳化了使用者體驗，同時確保統一的安全狀態，從而在無邊界網路中保持嚴格的可視性和策略實施。

圖表

終端、FTD和Azure Entra之間的強制網路門戶



終端和Azure Entra之間的強制網路門戶

設定

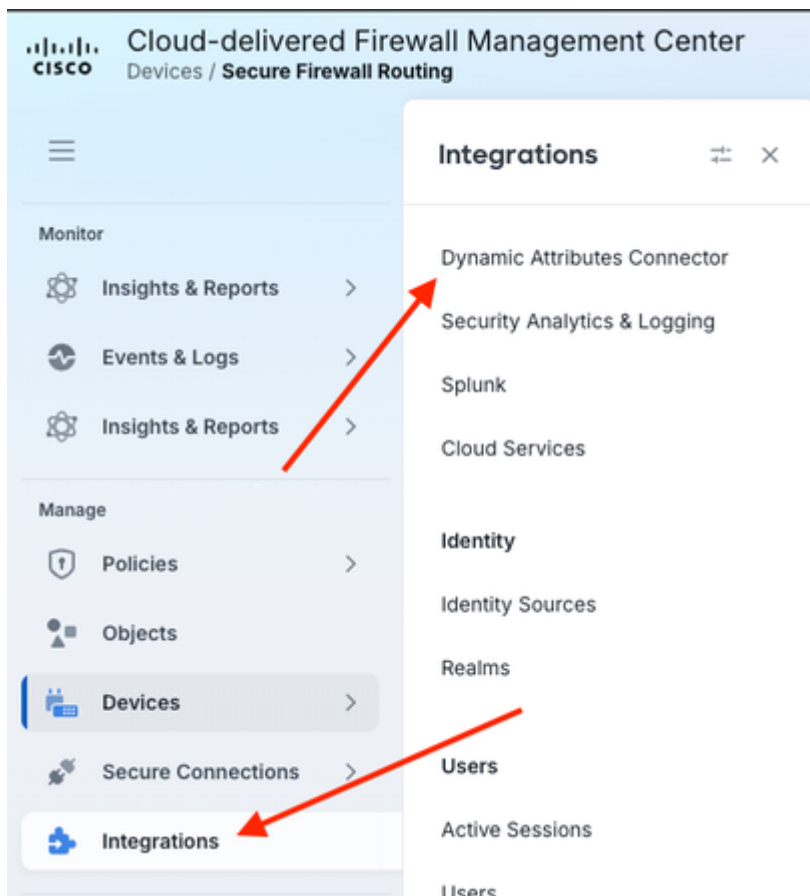
第1階段：初始FMC和DNS配置



附註：本實驗使用雲交付的防火牆管理中心(cdFMC);但是，內部現場故障修復管理模組的步驟保持不變。

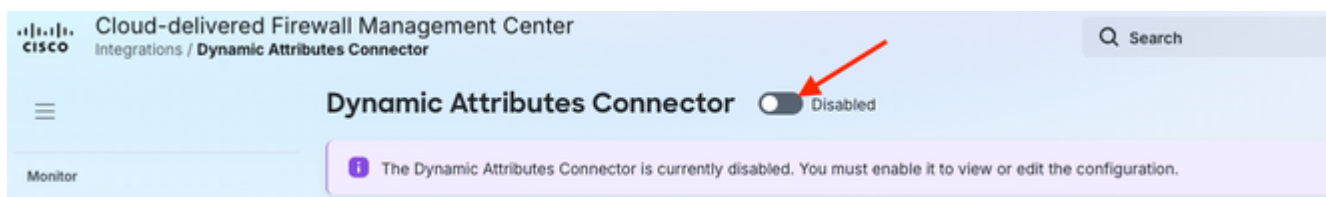
步驟 1: 啟用思科動態屬性連結器(CSDAC)

1) 選擇 Integrations > Dynamic Attributes Connector。



選擇整合動態屬性連結器

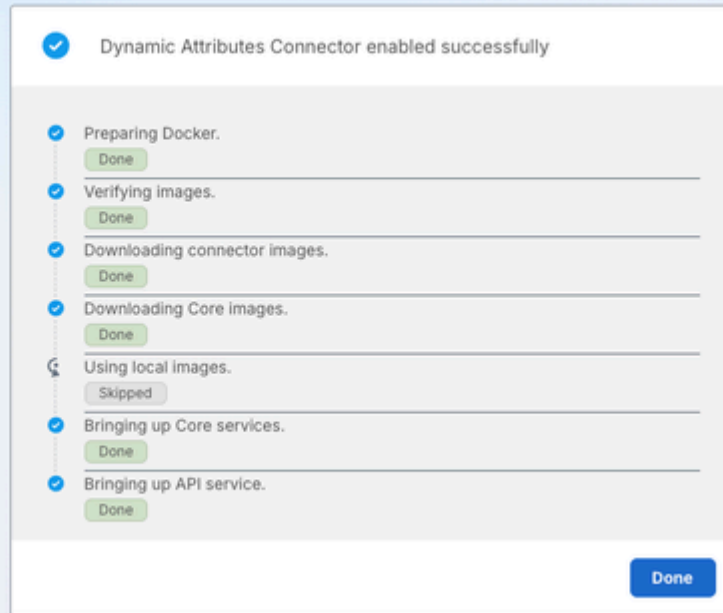
2) 按一下 Disabled 字串旁的控制元件以啟用 CSDAC。



啟用思科動態屬性連結器

c) CSDAC 啟用完成後，按一下 Done。

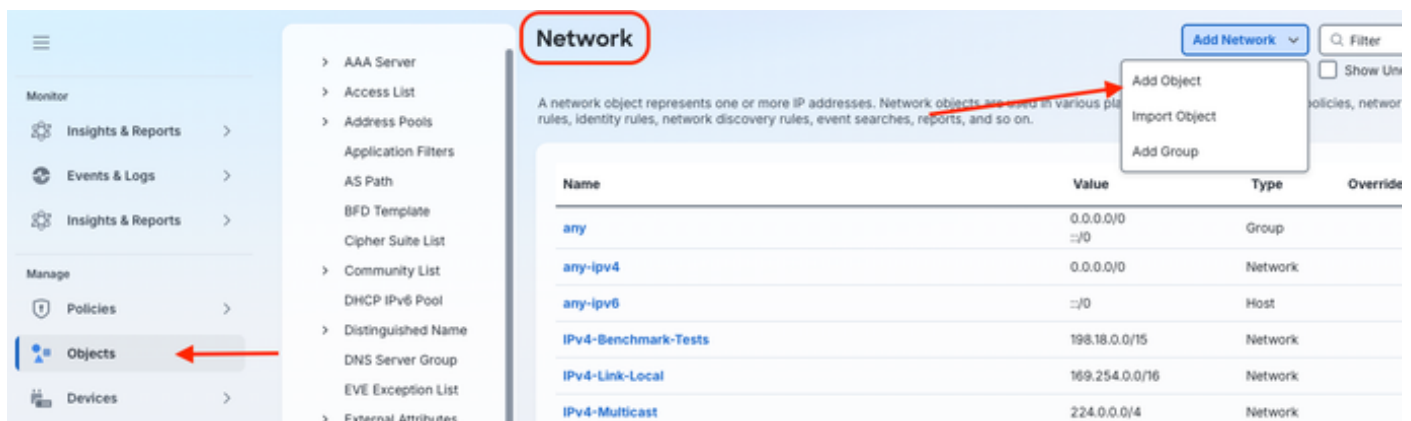
Dynamic Attributes Connector



啟用思科動態屬性連結器狀態

步驟 2: 建立代表FTD輸入介面的完全限定網域名稱網路物件

1) 選擇 Objects > Add Network > Add Object.



建立新的完全限定域名網路對象

2) 使用完全限定域名(FQDN)為網路對象命名。輸入FQDN，並通過按一下相應的單選按鈕將網路對象指定為FQDN型別。按一下「Save」。

Edit Network Object ?

Name

Description

Network
☐ Host ☐ Range ☐ Network ☒ FQDN

Note:
You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

Lookup:

☐ Allow Overrides

Cancel Save

配置FQDN網路對象變數

步驟 3:配置DNS A記錄

1)此處顯示的範例使用Windows Server 2025;如果需要，請參閱特定名稱解析伺服器的文檔。

	Name	Type	Data
DC	(same as parent folder)	Start of Authority (SOA)	[1], dc., hostmaster.
Forward Lookup Zones	(same as parent folder)	Name Server (NS)	dc.
example.com	ftd-inside	Host (A)	192.168.20.1
Reverse Lookup Zones			
Trust Points			

Windows Server DNS A記錄配置



附註：執行主動身份驗證的客戶端必須能夠解析此DNS A記錄。

第2階段：公開金鑰基礎架構組態

內部證書頒發機構(CA)可用作活動身份驗證配置的公鑰基礎架構(PKI)。Cisco FMC和FTD要求將內部CA公鑰和配對的私鑰作為內部CA對象上載，以執行必要的SSL偵聽和Decrypt-Resign操作。此外，內部CA必須在執行活動身份驗證的客戶端瀏覽器中受信任。請參閱使用者端瀏覽器檔案，以檢查如何確認瀏覽器信任憑證。

步驟 1:將內部CA證書匯入FMC

1)選擇Objects > PKI > Internal CAs。按一下「Import CA」。



附註：內部CA也可直接在FMC上建立。

Import Internal Certificate Authority ⓘ

Name:

Certificate Data or, choose a file:

-----BEGIN CERTIFICATE-----
-----END PRIVATE KEY-----

Key or, choose a file:

-----BEGIN CERTIFICATE-----
-----END PRIVATE KEY-----

☒ Encrypted, and the password is:

將內部證書頒發機構匯入防火牆管理中心



附註：在本文檔的內容中，出現空白區域，覆蓋影象中的各個欄位值，這是本文檔發佈時

有意造成的。在您配置時，會反映環境的實際值。

步驟 2: 使用CA簽署服務提供商證書

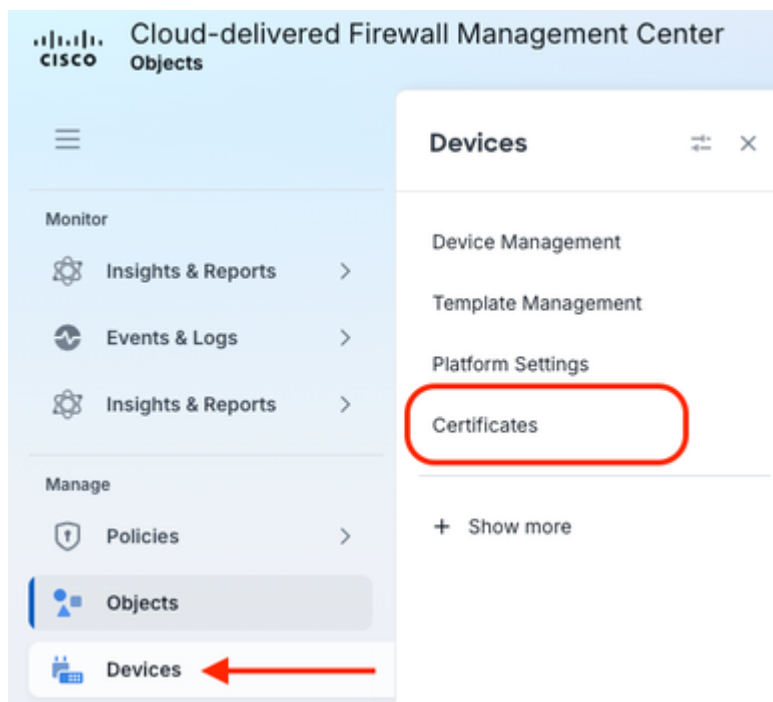
1) 服務提供商(SP)證書必須由受信任的證書頒發機構(CA)簽名並以PKCS#12(.p12)格式返回。



附註：此CA可以內部簽名。唯一的警告是客戶端裝置必須信任內部CA。

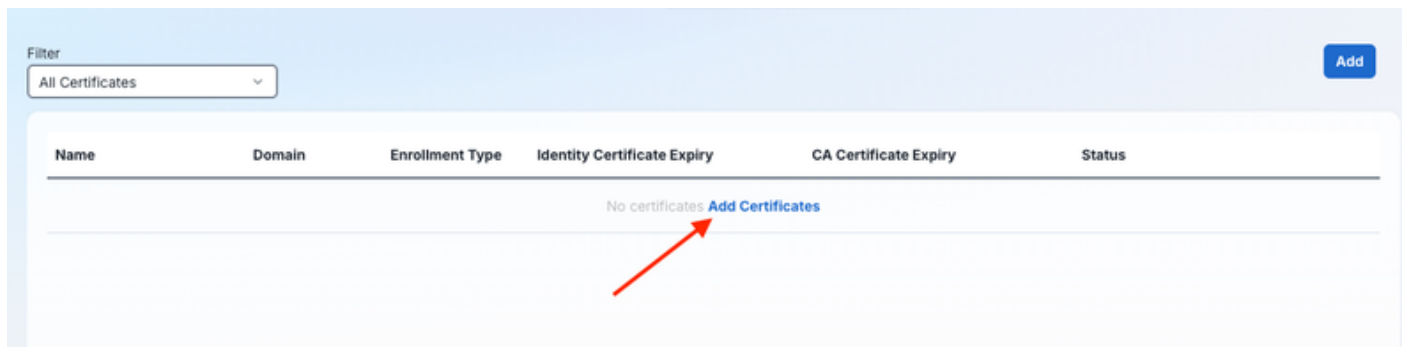
步驟 3: 將SP證書部署到FTD

1) 選擇Devices > Certificates。



導覽至Devices and Certificates

2) 按一下Add Certificates。



新增新裝置證書

3)從執行Active Authentication的下拉選單中按一下裝置，然後按一下+圖示以建立新的Certificate Enrollment。

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:
FTD

Certificate Enrollment*:
+

Cancel Add

選擇FTD並新增憑證註冊

4)為Certificate Enrollment命名，然後在Enrollment Type下拉選單中選擇PKCS12 file。

Add Certificate Enrollment ?

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:*

Challenge Password:

Confirm Password:

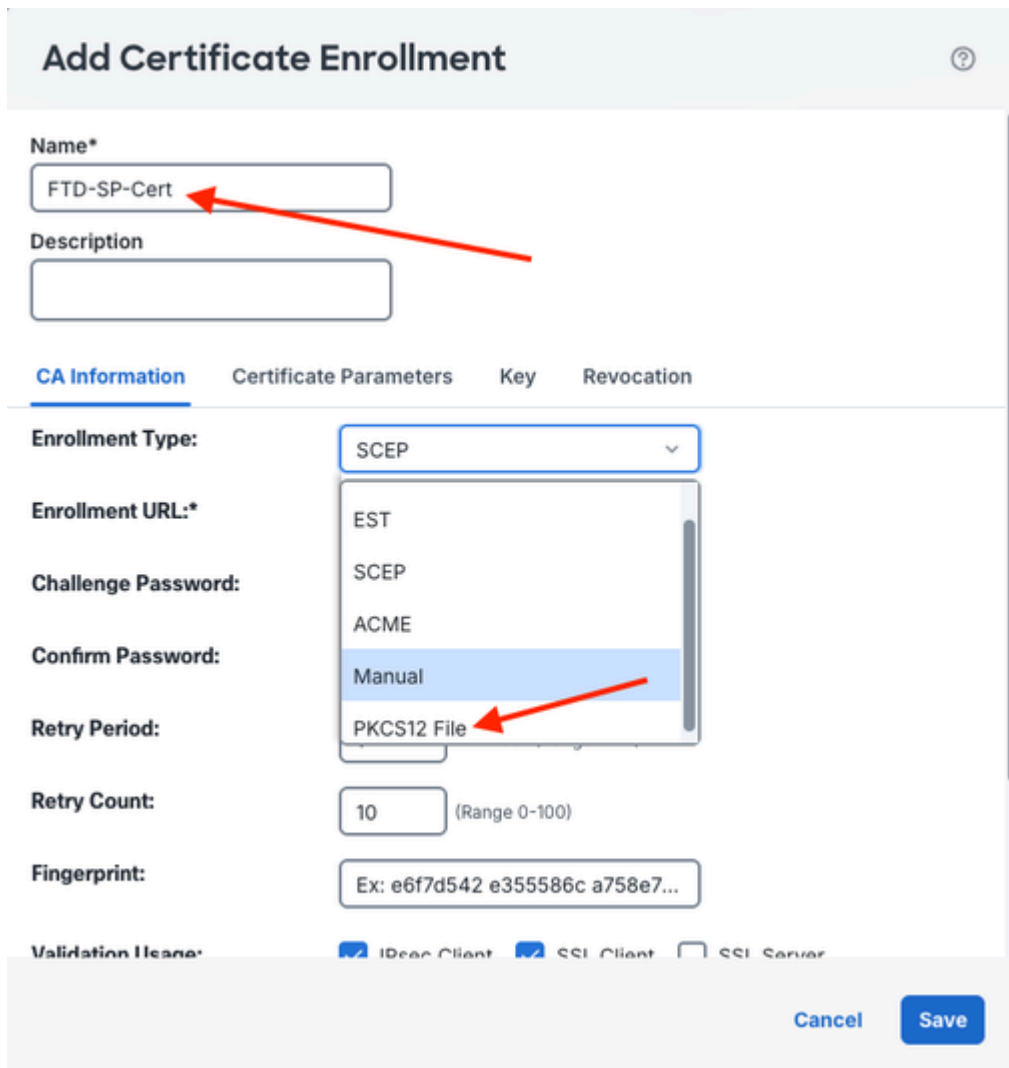
Retry Period:

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7...

Validation Usage: ☒ IPsec Client ☒ SSL Client ☐ SSL Server

Cancel Save



證書註冊設定和型別

5)按一下Browse PKCS12 File匯入PKCS#12檔案，然後輸入所需的密碼短語。按一下「Save」。

Add Certificate Enrollment

Name*
FTD-SP-Cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: SP.p12 [Browse PKCS12 File](#)

Passphrase*:

Validation Usage: ☒ IPsec Client ☒ SSL Client ☐ SSL Server

☐ Skip Check for CA flag in basic constraints of the CA Certificate

☒ Allow Overrides

> Override (0)

Cancel Save

瀏覽和匯入PKCS12檔案

6)確認登記詳細資訊是否正確，然後點選Add。

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD

Certificate Enrollment*: FTD-SP-Cert +

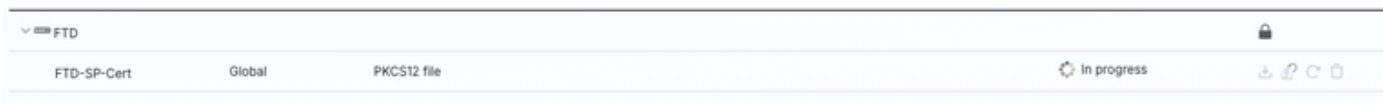
Certificate Enrollment Details:

Name:	FTD-SP-Cert
Enrollment Type:	PKCS12 file
Enrollment URL:	N/A

Cancel Add

確認證書註冊詳細資訊

7)進口反映進行中。



匯入完成後，可以通過按一下已配置證書的ID圖示來驗證SP證書資訊。

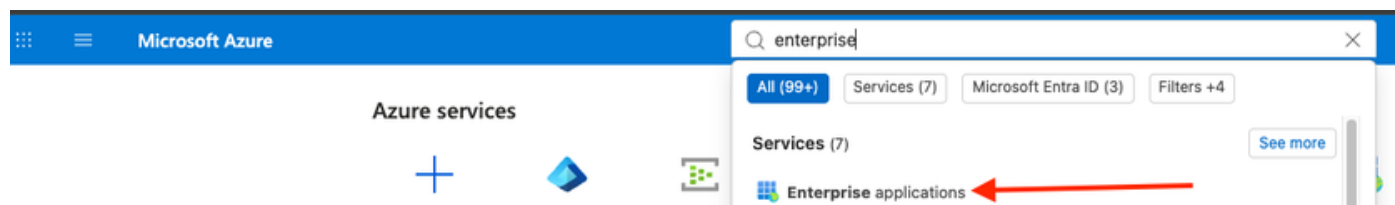
Filter						Add	
All Certificates							
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status		
FTD-SP-Cert	Global	PKCS12 file	Dec 18, 2028	Sep 12, 2036			

證書匯入正在進行狀態

第3階段：Azure配置

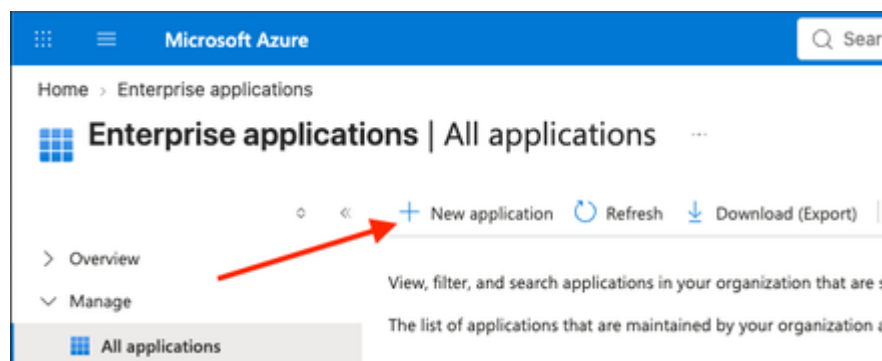
步驟 1:為SAML工具包建立Entra Enterprise應用程式

1)搜尋並按一下Enterprise Applications。



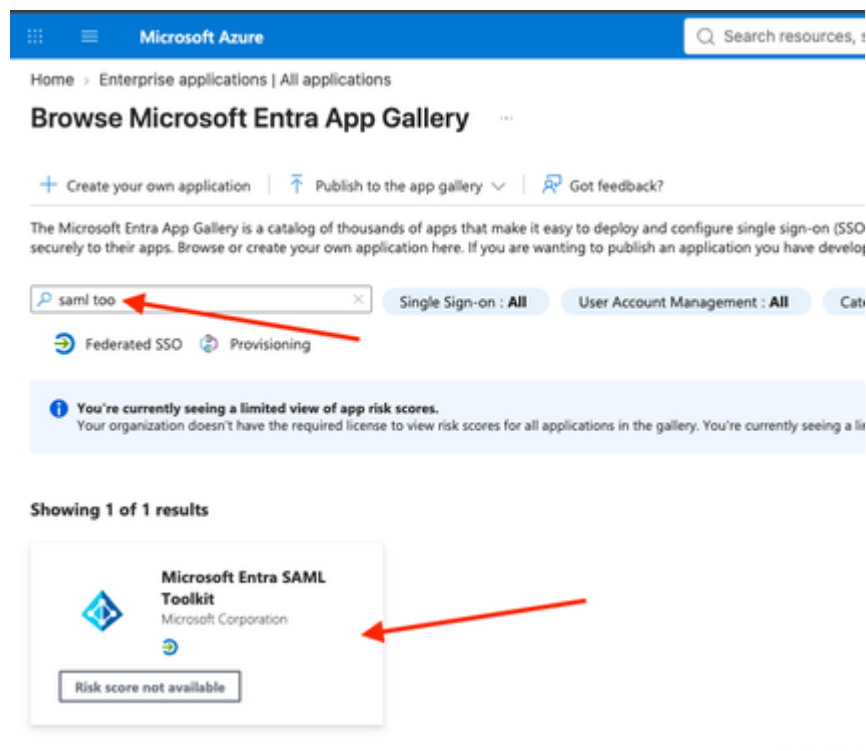
搜尋和訪問企業應用程式

2)按一下+ New Application。



選擇企業應用程式中的新應用程式

3)搜尋Microsoft Entra SAML Toolkit，然後按一下其縮略圖。



搜尋並選擇Microsoft Entra SAML Toolkit

4)為Microsoft Entra SAML Toolkit Enterprise Application分配名稱，然後按一下Create。(來自Microsoft的參考：[請閱讀我們的Microsoft Entra SAML工具包整合教程](#))。

Microsoft Entra SAML Toolkit

Got feedback?

Logo 

Name *

Publisher  Microsoft Corporation

Provisioning  Automatic provisioning is not supported

Single Sign-On Mode  SAML-based Sign-on
Linked Sign-on

URL  <https://www.microsoft.com/>

[Read our step-by-step Microsoft Entra SAML Toolkit integration tutorial](#)

This is the sample SAML app which customers can use to test the SAML single sign-on integration with Microsoft Entra ID.

You're currently seeing a limited view of app risk scores.
Your organization doesn't have the required license to view risk scores for all applications in the gallery. You're currently seeing a limited view. To access full risk scoring upgrade to [Microsoft Entra Suite](#) or [Microsoft Entra Internet Access](#).

Create

為SAML工具包應用程式指定名稱

5)在Overview頁面上，將特定使用者和組分配給SAML Toolkit Enterprise Application。在本示例中，測試帳戶(captive-portal-user)是active-auth-lab組的成員。

 **1. Assign users and groups**

Provide specific users and groups access to the applications

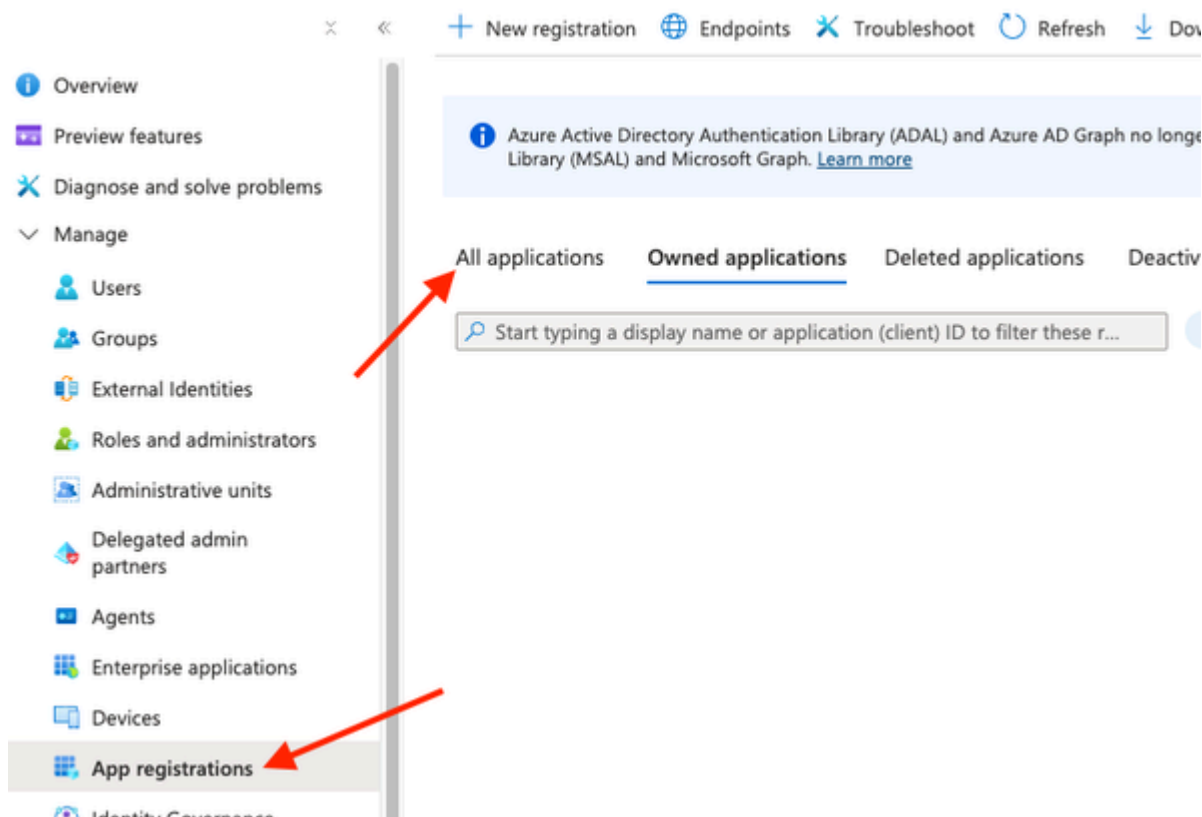
[Assign users and groups](#)

將使用者和組分配給應用程式

6)此企業應用程式的配置將在後續步驟中繼續。

步驟 2:配置Entra ID應用註冊

1)導航回Entra ID，然後從左側導航選單中選擇App registrations。按一下All applications過濾器並搜尋為Enterprise Application指定的名稱。按一下相應的應用程式。



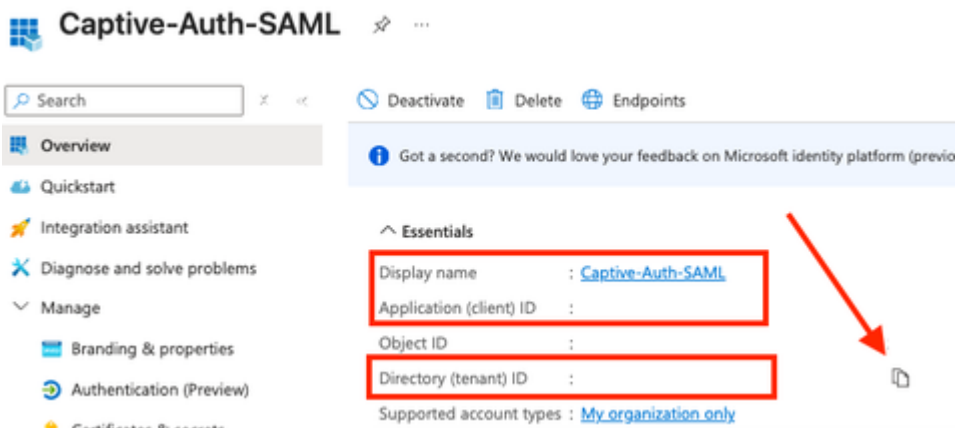
導航到應用程式註冊和所有應用程式

2)收集並記錄Enterprise App Registration下的Essentials值。



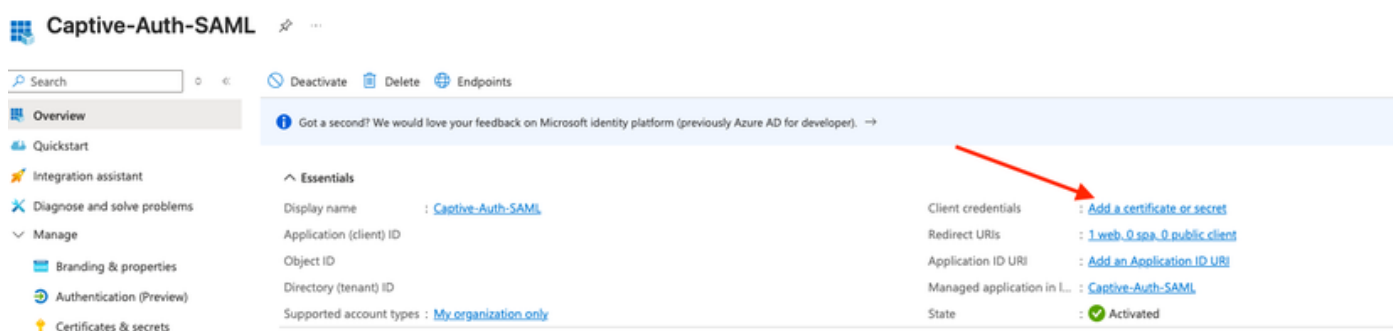
重要：將滑鼠懸停在值上，以顯示複製到剪貼簿，並在Overview頁面上的Essentials下收集值：

- 顯示名稱
- 應用程式（客戶端）ID
- 目錄（租戶）ID



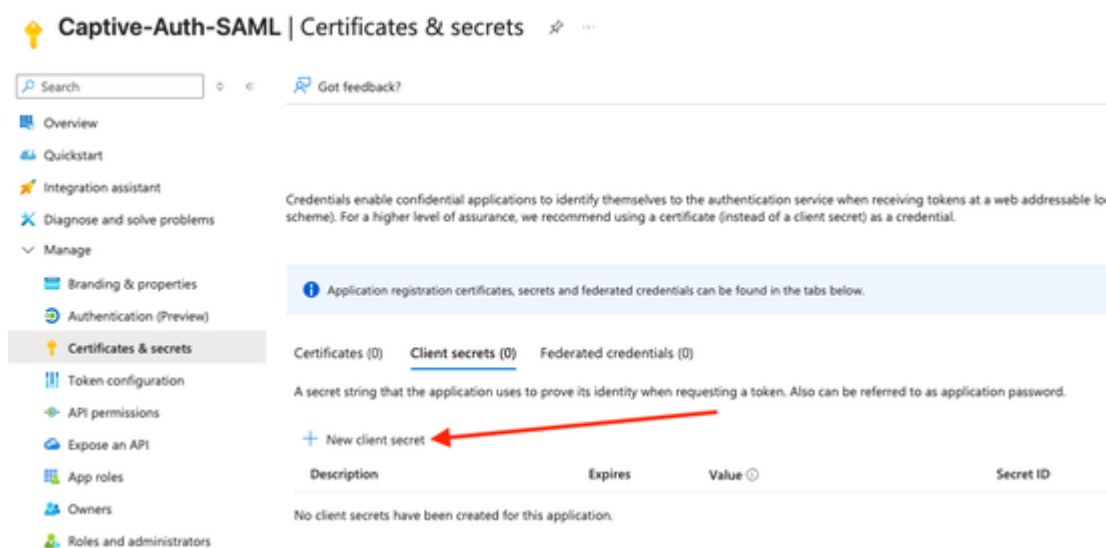
收集顯示以及應用程式和目錄ID值

3)按一下Add a certificate or secret超鏈接。



新增證書或密碼超連結

4)按一下+ New client secret。



新增新的客戶端密碼

5)提供密碼說明，並根據需要調整到期。按一下「新增」。

Add a client secret ✕

Description saml-secret

Expires Recommended: 180 days (6 months) ▼

Add Cancel

提供客戶端金鑰的說明

6)複製Secret。



重要：記下複製到剪貼簿的機密值。

Captive-Auth-SAML | Certificates & secrets ✱ ...

Search Got feedback?

Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication (Preview)
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

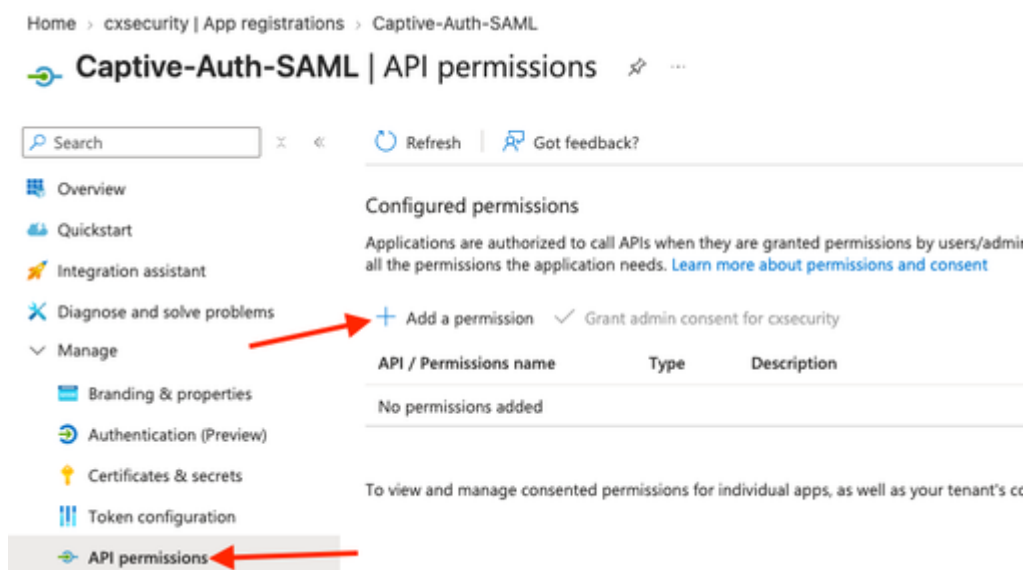
+ New client secret

Description	Expires	Value	Secret ID
saml-secret	3/14/2027		

複製客戶端加密值

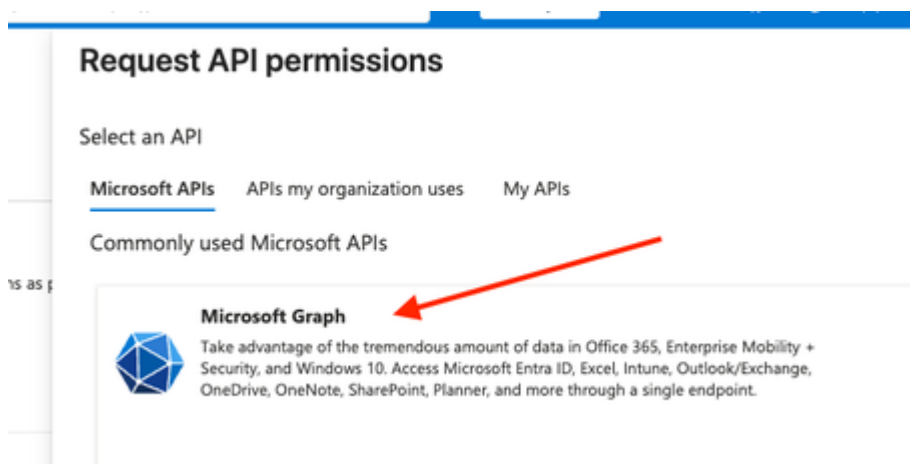
步驟3.為應用程式註冊配置Microsoft Graph API許可權。

1)從左側導航選單中選擇API Permissions，然後按一下+ Add a permissions。



配置API許可權

2)按一下Microsoft Graph API。



選擇Microsoft Graph API

3)授予Delegated User.Read許可權，然後按一下「添加許可權」。

Request API permissions

[← All APIs](#)

 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

 User.Read

Permission	Admin consent required
> AgentIdUser	
> IdentityRiskyUser	
▼ User (1)	
☒ User.Read ⓘ Sign in and read user profile	No
☐ User.Read.All ⓘ Read all users' full profiles	Yes
☐ User.ReadBasic.All ⓘ Read all users' basic profiles	No

[Add permissions](#) [Discard](#)

授予委派使用者讀取許可權

4)授予Application User.Read.All許可權 (選中覈取方塊)。

Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Permission	Admin consent required
> IdentityRiskyUser	
User (1)	
☒ User.Read.All ⓘ Read all users' full profiles	Yes

授予應用程式讀取所有許可權

5) 搜尋並選中 Group.Read.All 覈取方塊以授予 Group Read 許可權。按一下 Add permissions。

Select permissions

[expand all](#)

Permission	Admin consent required
Group (1)	
☒ Group.Read.All ⓘ Read all groups	Yes

[Add permissions](#) [Discard](#)

儲存API許可權

6) 確認配置的許可權是否一致的，並為他們授予管理同意許可權。

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for ...
User.Read	Delegated	Sign in and read user profile	No	...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for ...

授予許可權的管理同意

7)顯示一旦授予管理員同意後的輸出。

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

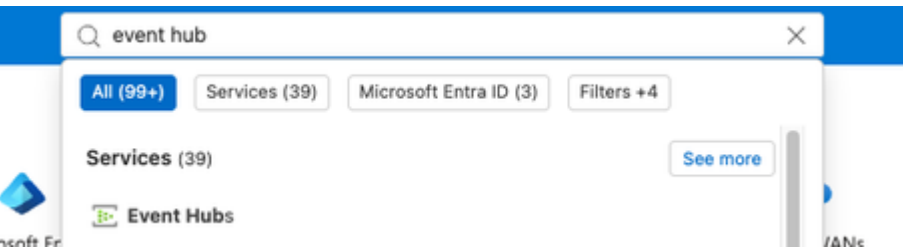
✓ Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	✔ Granted for ...
User.Read	Delegated	Sign in and read user profile	No	✔ Granted for ...
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for ...

授予的管理同意輸出

步驟 4:配置事件中心(EH)名稱空間

1)搜尋並按一下Event Hub(事件集線器)。



搜尋事件中心配置

2)建立新的EH命名空間。



No event hubs namespaces to display

An Event Hubs namespace is a management container for event hubs which provides DNS-integrated network endpoints and a range of access control and network integration management.

[+ Create](#)

[Learn more about Event Hubs](#)

建立事件中心名稱空間

3)配置EH命名空間。



附註：必須選擇Standard定價層或更高版本。基本定價層阻止領域使用。

請參閱[Azure事件中心文檔](#)，以瞭解對事件中心高級設定以及對特定需求的適用性的進一步評估。

按一下「Review + Create」。



Create Namespace

Event Hubs

[Basics](#) [Advanced](#) [Networking](#) [Tags](#) [Review + create](#)

Project Details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *

[Create new](#)

Instance Details

Enter required settings for this namespace, including a price tier and configuring the number of units (capacity).

Namespace name * ☒ .servicebus.windows.net

Region * ☒
i The region selected supports Availability zones. Your namespace will have Availability Zones enabled. [Learn more](#)

Pricing tier * ☒
[Browse the available plans and their features](#)

Throughput Units *

Enable Auto-Inflate ? ☐

[Review + create](#)

< Previous

Next: Advanced >

配置事件中心名稱空間設定

4)驗證成功後，按一下Create。

Home > Event Hubs

Create Namespace

Event Hubs

Validation succeeded.

Basics Advanced Networking Tags Review + create

Event Hubs Namespace
by Microsoft

Basics

Namespace name	captive-auth-ad-eh
Subscription	
Resource group	
Region	East US
Pricing tier	Standard
Throughput Units	1
Availability Zones (Zone Redundancy)	Enabled
Auto-inflate Maximum Throughput Units	Disabled

Networking

Connectivity method	Public access
Network Protocol Preference	IPv4 only

Security

Minimum TLS version	1.2
Local Authentication	Enabled

Create < Previous Next >

建立事件中心名稱空間部署

5)確認部署完成，然後按一下轉至資源。

Home

captive-auth-ad-eh | Overview

Deployment

Search x <<

Delete Cancel Redeploy Download Refresh

Overview

- Inputs
- Outputs
- Template

Your deployment is complete

Deployment name : captive-auth-ad-eh
Subscription :
Resource group :

> Deployment details

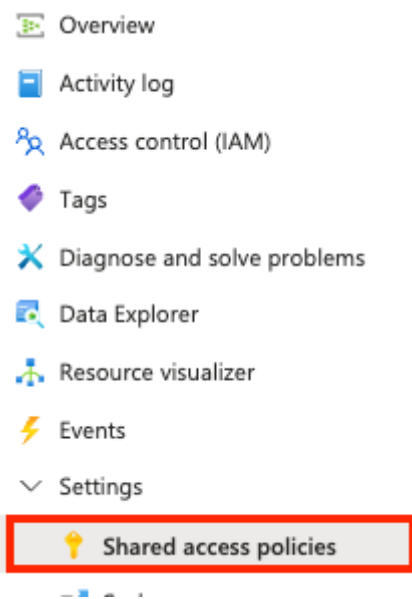
Next steps

Go to resource

轉到事件中心名稱空間資源

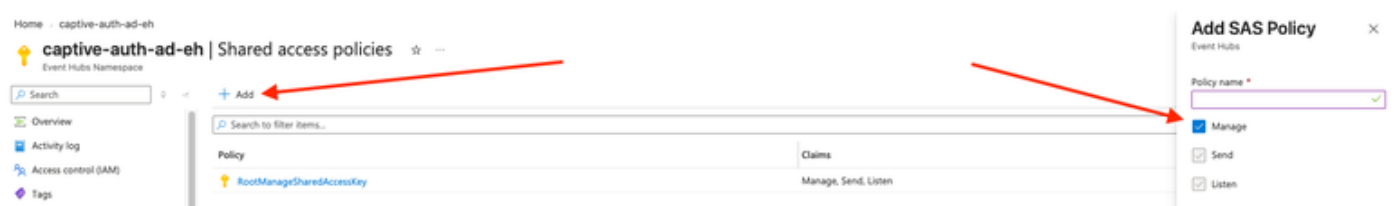
步驟 5:在事件中心名稱空間中選擇或建立共用訪問策略

1)從左側導航選單中選擇「設定」>「共用訪問策略」。



導航到共用訪問策略

2)按一下+ Add並輸入新的Policy name，然後選中Manage覈取方塊。按一下Add SAS Policy選單面板底部的Create。



新增新的共用訪問策略



建立共用訪問策略

步驟 6:從EH名稱空間收集並記錄共用訪問簽名(SAS)資訊

1)按一下新的「共用訪問」策略;「EH SAS Policy (EH SAS策略)」顯示在右側的面板中。

Regenerate primary key Regenerate secondary key Delete

Event Hubs access control with Shared Access Signatures [Learn more](#)

Claims

- ☒ Manage
- ☐ Send
- ☐ Listen

Primary key

Secondary key

Primary connection string

Secondary connection string

© 2019 Microsoft Corporation. All rights reserved. See [Terms of Use](#).

複製主連線字串



重要：複製並記下Primary連線字串。

步驟 7:在事件中心名稱空間中建立事件中心例項

1)從Namespace選單中選擇Entities > Event Hub。按一下+ Event Hub以建立新的EH例項。

Search << + Event Hub Refresh Help

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Data Explorer

Resource visualizer

Events

Settings

Entities

Event Hubs

Schema Registry

Search to filter items by name...

Name

No Event Hubs yet.

建立新的事件中心例項

2)為新的EH例項分配名稱，然後按一下Review + create。

Home > Event Hubs > captive-auth-ad-eh | Event Hubs

Create Event Hub

Event Hubs

Basics Capture Review + create

Event Hub Details

Enter required settings for this event hub, including partition count and message retention.

Name * ⓘ captive-auth-ad-eh-1 ✓

Partition count ⓘ 1

Retention

Configure retention settings for this Event Hub. [Learn more](#)

Cleanup policy ⓘ Delete

Retention time (hrs) * ⓘ 1
min. 1 hour, max. 168 hours (7days)

Review + create < Previous Next: Capture >

為事件中心例項分配名稱

3)驗證成功後，按一下Create以設定Event Hub例項。

Create Event Hub ...

Event Hubs

✓ Validation succeeded.

Basics Capture Review + create

Event Hubs Instance
by Microsoft

Basics

Name captive-auth-ad-eh-1
Partition count 1

Retention

Cleanup policy Delete
Retention time (hrs) 1

Capture

Capture Status Off

Create

< Previous

Next >

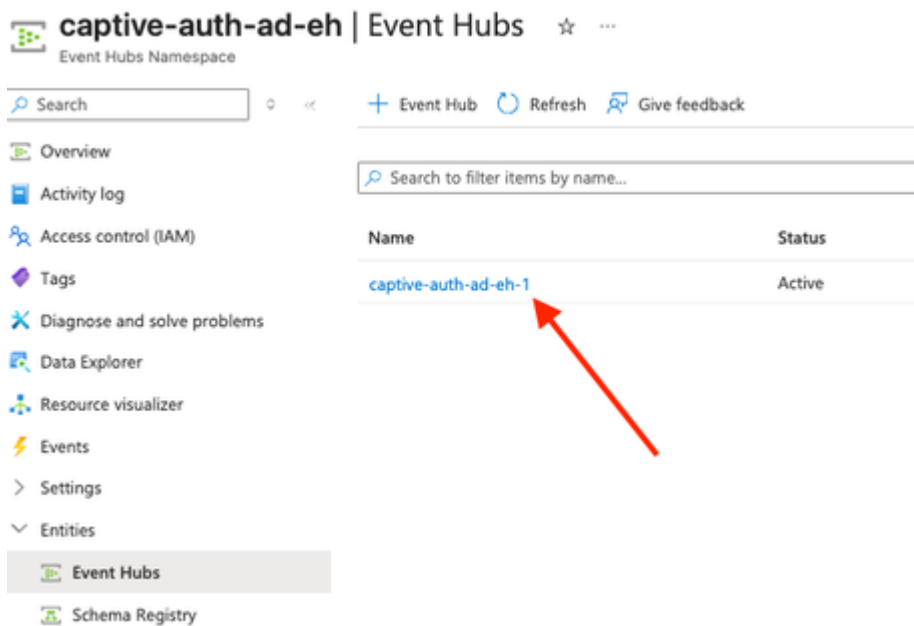
設定事件中心例項



重要：複製並記下Event Hub例項名稱。

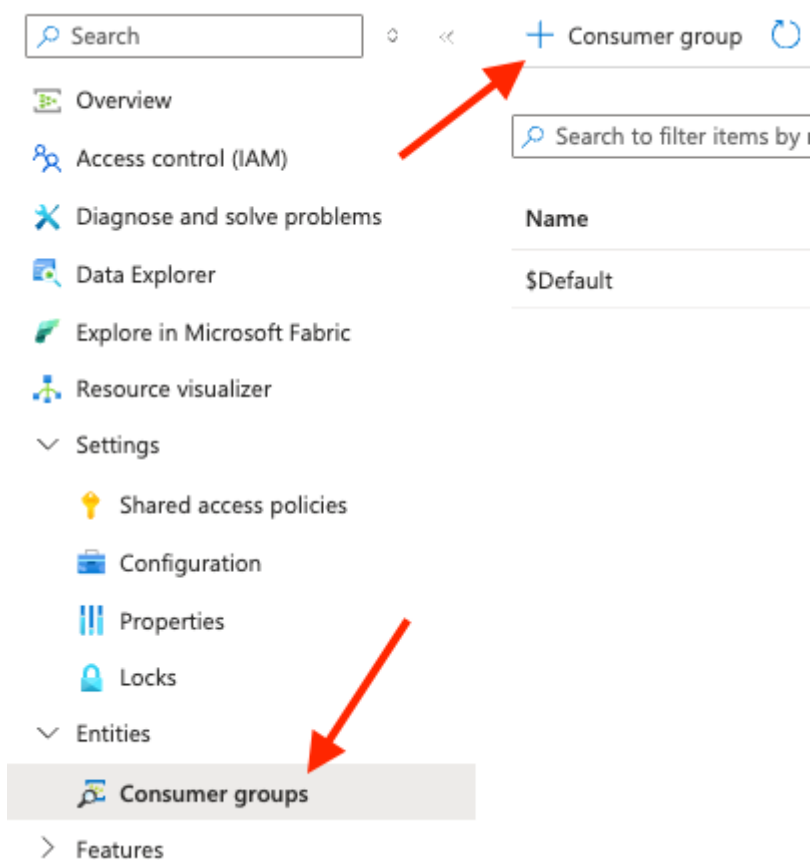
步驟 8: 在事件中心名稱空間中建立事件中心例項使用者組

1) 按一下上一步中配置的新EH例項。



訪問事件中心例項配置

2)在EH例項中，選擇實體>使用者組，然後建立新的使用者組。



建立使用者組

3)為使用者組命名，然後按一下Create。

Create consumer group

Consumer groups

Name *

captive-auth-ad-eh-cg

✓

Create

為使用者組分配名稱



重要：複製並注意Event Hub例項Consumer組名稱。

步驟 9:驗證收集的值

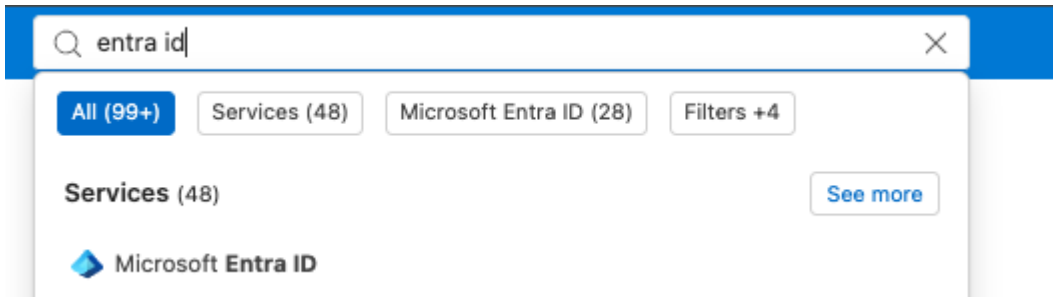
1)此時，請注意前面步驟中的這些值。如果未記錄任何值，請引用收集值的適用步驟：

- 第3階段第2步 — 應用程式註冊(針對此進程建立的企業應用程式，由收集的顯示名稱引用)
 - 步驟2，子步驟2
 - 顯示名稱
 - 應用程式 (客戶端) ID
 - 目錄 (租戶) ID
 - 步驟2，子步驟6
 - 客戶端密碼
- 第3階段第6步 — 事件中心
 - 步驟6，子步驟1
 - EH名稱空間
 - 主連線字串
 - 步驟7，子步驟3
 - EH例項 (事件中心) 名稱

- 步驟8，子步驟3
 - EH使用者組名稱

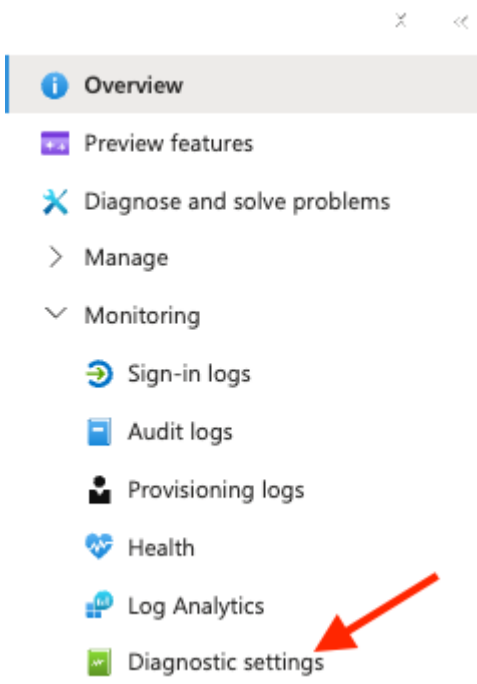
步驟 10:配置Entra ID審計日誌流到事件中心

1)導航回Entra ID租戶配置。



搜尋並導航至Entra ID租戶配置

2)從左側選單中選擇Monitoring > Diagnostic Settings。



診斷設定監視

3)選擇Diagnostic settings > General，然後按一下+ Add diagnostic setting。

Refresh Feedback

Diagnostic settings

General

Custom security attributes

Diagnostic settings are used to configure streaming export of platform logs

Diagnostic settings

Name	Storage account
	-
	-
	-

+ Add diagnostic setting

新增新診斷設定

4)為診斷設定分配所需的名稱，選中AuditLogs覈取方塊以記錄，選中Stream to an event hub覈取方塊。參照之前配置中記錄的值，並在完成後按一下Save。

Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name * captive-portal-auth

Logs

Categories

- ☒ AuditLogs
- ☐ SignInLogs
- ☐ NonInteractiveUserSignInLogs
- ☐ ServicePrincipalSignInLogs
- ☐ ManagedIdentitySignInLogs
- ☐ ProvisioningLogs
- ☐ ADFSSignInLogs
- ☐ RiskyUsers
- ☐ UserRiskEvents
- ☐ NetworkAccessTrafficLogs

Destination details

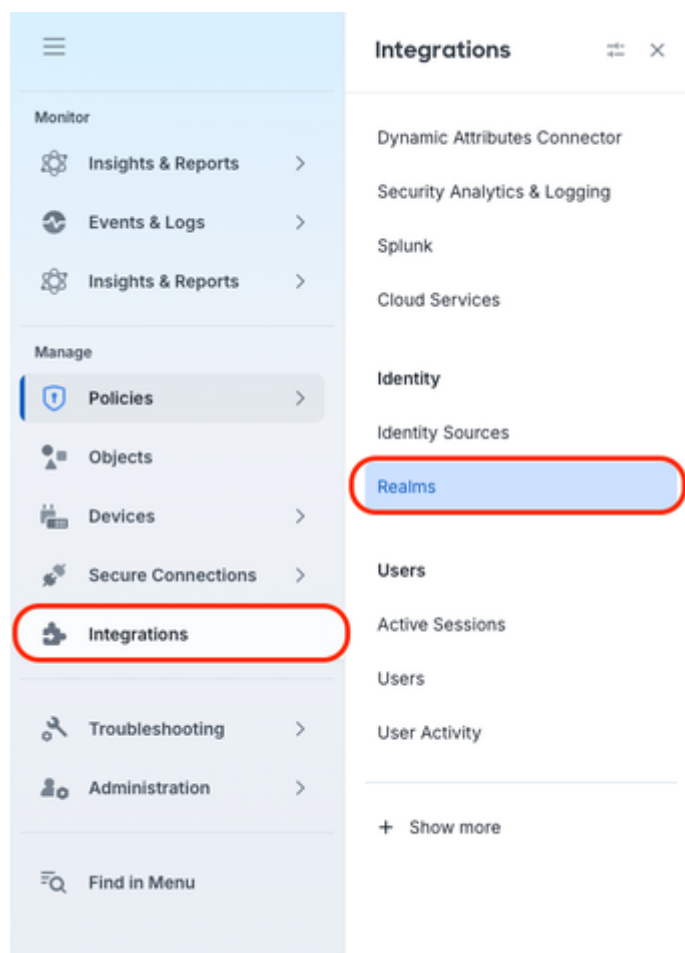
- ☐ Send to Log Analytics workspace
 - ☐ Archive to a storage account
 - ☒ Stream to an event hub
- For potential partner integrations, [click to learn more about event hub integration](#).
- Subscription
- Event hub namespace * captive-auth-ad-eh
- Event hub name (optional) captive-auth-ad-eh-1
- Event hub policy name
- ☐ Send to partner solution

將稽核日誌流式傳輸到事件中心

第4階段：整合Azure和FMC/FTD主動身份驗證配置

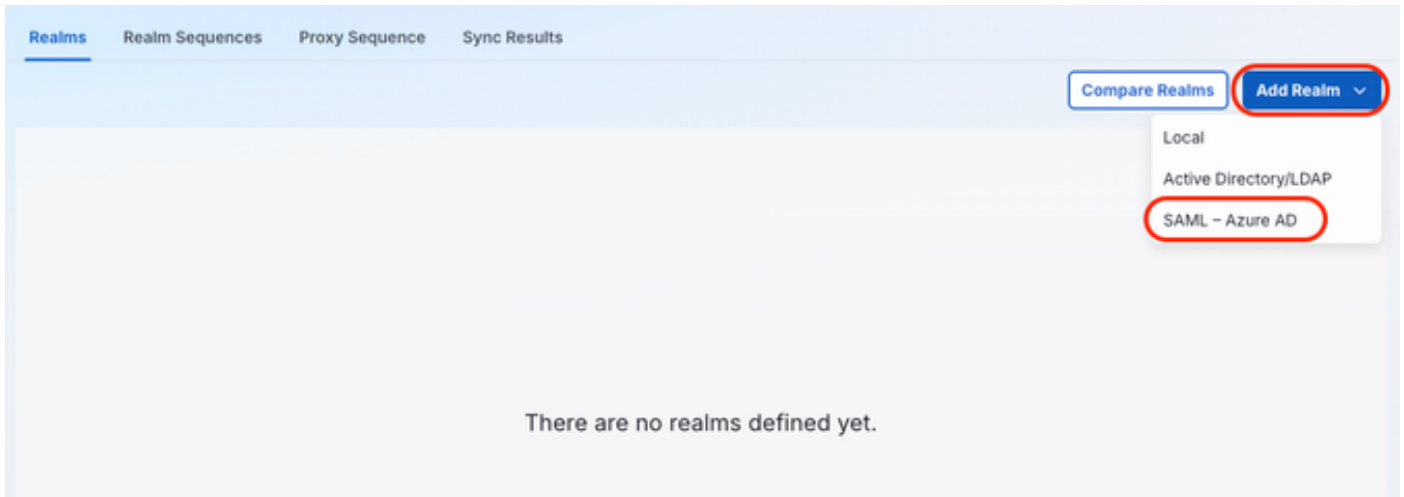
步驟 1:使用FMC嚮導配置Azure SAML/Entra ID領域

1)在FMC中，選擇Integrations > Identity > Realms。



身份領域配置

2)按一下Add Realm下拉選單，然後選擇SAML - Azure AD。



新增SAML Azure AD領域

3)為Azure領域分配名稱和描述以描述其使用，並確保從配置型別下拉選單中選擇使用Azure AD被動身份驗證或使用強制網路門戶和Azure AD。按「Next」（下一步）。

配置Azure AD領域設定

4)選擇以前配置的FQDN對象作為基本URL。輸入帶有以下字串格式的實體ID:

`https://<fqdn-base-url>/<uniqueSuffix>`

- 配置SAML實體ID字尾（在下一個配置示例中帶綠色下劃線）時，請確保該字尾在環境中的其他SSO實現中具有唯一性。此值也必須與Azure SAML配置匹配。基本URL在整個組態中保持不變。
- Assertion Consumer Services(ACS)URL會自動填充且不可變。
- 在Devices > Certificates下，選擇FMC中之前工作流程步驟中註冊的服務供應商(SP)證書。
- 輸入這些值後，按一下Download Service Provider Metadata以簡化配置過程，並確認預期的值已寫入Azure。

Add SAML – Azure AD Realm

1 Realm Details
Edit

Name	azure-entra-saml
Description	Active Authentication IdP
Identity Provider	Azure AD
Configuration Type	Authenticate passively with Azure AD or using captive portal with Azure AD

2 SAML Service Provider (SP) Metadata

Base URL *

active_auth_fqdn

Must resolve to the interface(s) of source security zones used in an identity policy.

Entity ID *

https://ftd-inside.example.com/saml/sp/metadata/activeAuthEntID

Unique, alphanumeric identifier for a SAML entity.

Assertion Consumer Services (ACS) URL *

https://ftd-inside.example.com/+CSCOE+/saml/sp/acs?tname=azure-entra

URL at which the service provider receives SAML assertions from Azure AD.

Service Provider Certificate *

FTD-SP-Cert

Certificate used for SAML authentication and TLS/SSL communication with the secure threat defense device. The certificate must have the value you specify for Base URL that must match the Common Name (CN) or Subject Alternative Name (SAN). The certificate, which must be in PKCS12 format, must be trusted by clients.

Download Service Provider Metadata

Next

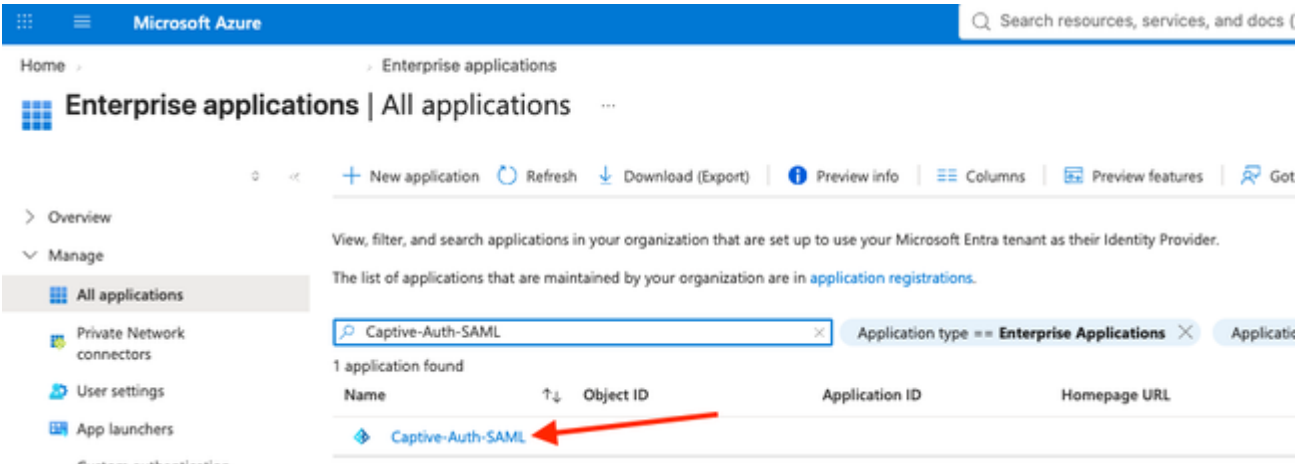
配置基本URL和實體ID並下載SAML後設資料

5)按一下Next轉到「領域」配置的第3序列。

步驟 2:在Azure企業應用程式中實施FMC配置的SAML SP後設資料

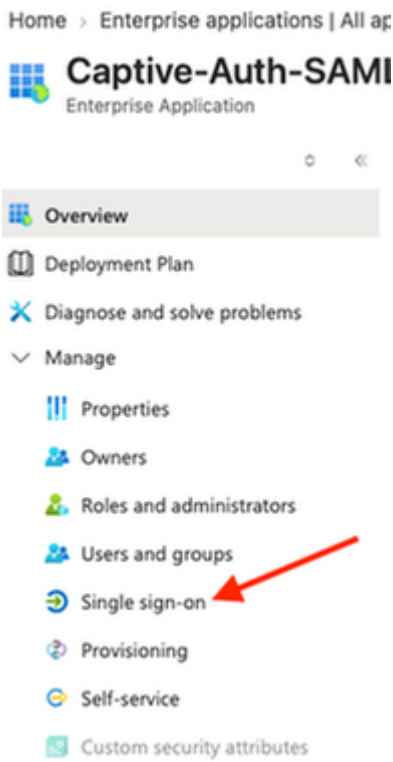
1)導航回Azure，然後選擇Entra ID > Manage > Enterprise Applications。搜尋以前建立的Microsoft

Entra SAML工具包企業應用程式例項。



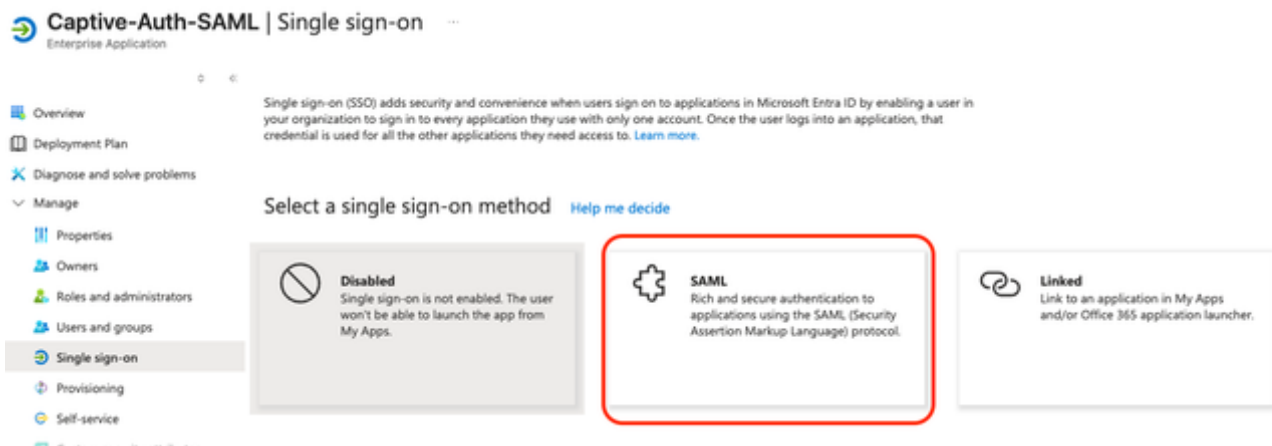
查詢Microsoft Entra SAML工具包應用程式

2)從側面導航選單中選擇「管理」>「單一登入」。



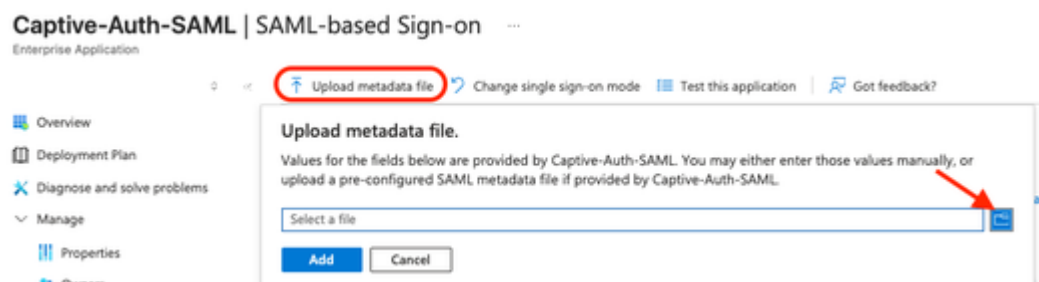
管理單一登入配置

3)按一下SAML Single Sign-On(SSO)模式。



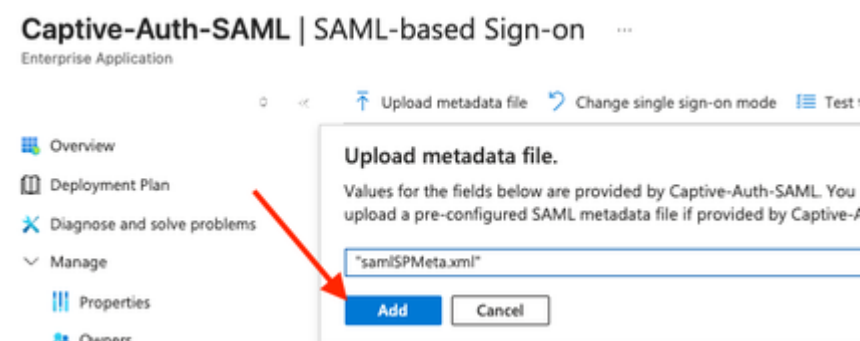
SAML單一登入模式選擇

4)按一下Upload metadata file，然後按一下藍色資料夾圖示瀏覽本地檔案系統，查詢從FMC下載的SAML元資料檔案。



從防火牆管理中心上載後設資料檔案

5)上傳完成後，按一下Add。



新增SAML配置應用程式

6)出現「基本SAML配置」的側面板，並且從FMC發起的SP後設資料XML檔案中提取並自動應用諸如識別符號（實體ID）和ACS URL之類的值。但是，登入URL未填充，儲存之前需要該選項。

Basic SAML Configuration

 Save |  Got feedback?

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





[Add identifier](#)

Patterns: https://samltoolkit.azurewebsites.net

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



0



[Add reply URL](#)

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*

Patterns: https://samltoolkit.azurewebsites.net/

✗ Please enter a valid URL starting with "https://". If your URL has query parameters, ensure that there is a slash preceding the question mark (i.e. /?)

✗ This field is required

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.



基本SAML配置提取

7)使用給定的登入URL模式，複製並貼上值，並在完成時按一下頂部的Save。

Basic SAML Configuration

 Save  Got feedback?

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



[Add identifier](#)

Patterns: https://samltoolkit.azurewebsites.net

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

0

☒

ⓘ



[Add reply URL](#)

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL *

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

*



Patterns: https://samltoolkit.azurewebsites.net/

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.



登入URL配置條目

向下滾動到SAML Certificates，然後匯出Azure生成的聯合元資料XML文件，以便匯入到Cisco Secure FMC。

3 SAML Certificates

Token signing certificate		Edit
Status	Active	
Thumbprint		
Expiration		
Notification Email		
App Federation Metadata Url		Download
Certificate (Base64)		Download
Certificate (Raw)		Download
Federation Metadata XML		Download

Verification certificates (optional) [Edit](#)

Required	No
Active	0
Expired	0

匯出聯合後設資料XML檔案

步驟 3:使用FMC嚮導配置Azure SAML/Entra ID領域 (續)

1)導航回到FMC。在Sequence 3, SAML Identity Provider(IdP)Metadata下，將從Azure下載的匯出聯合後設資料XML檔案上載到FMC以自動填充所需的值。

3 SAML Identity Provider (IdP) Metadata

Entity ID *

Unique, alphanumeric identifier for a SAML entity.

Single Sign-On (SSO) URL *

URL to your identity provider. You must include the scheme (e.g., https://).

IdP Certificate *

[+](#)

Choose a certificate from the list or upload a new certificate in manual format.

Federation XML you downloaded from Azure AD. If you upload this, you don't have to enter the other values in this section.

上載聯盟後設資料XML檔案

2)上載後，值將填充如圖所示。

3 SAML Identity Provider (IdP) Metadata

Entity ID *

Unique, alphanumeric identifier for a SAML entity.

Single Sign-On (SSO) URL *

URL to your identity provider. You must include the scheme (e.g., https://).

IdP Certificate *

+

Choose a certificate from the list or upload a new certificate in manual format.

 Click to upload or drag and drop a file.

Upload XML

Federation XML you downloaded from Azure AD. If you upload this, you don't have to enter the other values in this section.



Next

自動填充的SAML身份提供程式值



附註：部分輸出如下圖所示。

3)輸入截至此點的整個實施過程中收集的值：

- 應用註冊
 - 應用程式 (客戶端) ID
 - 客戶端密碼
 - 目錄 (租戶) ID
- 事件中心
 - EH名稱空間主機名
 - EH名稱空間主連線字串
 - EH例項 (事件中心) 名稱
 - EH使用者組名稱

Add SAML – Azure AD Realm



4 Azure AD Details

Client ID * 851607f9-969f-4fed-90ec-829607c1c Application ID (also referred to as client ID you created in Azure AD).	Client Secret * Secret string that the application uses to prove its identity when requesting a token.
Tenant ID * af42bac0-52aa-429f-92db-9258199f Microsoft Entry ID entity that typically encompasses an organization. Displayed in Azure Entra ID → Properties.	Event Hubs Host Name * captive-auth-ad-eh.servicebus.windows.net Hostname of the Event Hub Namespace. Displayed in Event Hubs → Event Hubs Namespace.
Event Hub Name * captive-auth-ad-eh Name of your event hub. Displayed in Event Hubs Name Space → Overview.	Consumer Group Name * captive-auth-ad-eh-cg A view of an entire event hub. Consumer groups enable consuming applications to each have a separate view of the event stream.
Event Hub Connection String * Endpoint=sb://captive-auth-ad-eh.servicebus.windows.net;SharedAccessKeyName= Event Hub Connection String: Unique identifier for the event hub (also referred to as topic or endpoint). It is displayed on the Azure AD portal in Event Hubs → (name of your event hub) → Shared access policies → (name of policy).	
USER GROUPS ☒ ☐ Excluded User Groups ☒ Included User Groups Enter each group name on a separate line active-auth-lab Enter one or more groups from which to download users for identity control. Users in these groups will be available for use in access control policies.	

Test

Test connection succeeded

Next

輸入應用程式和事件中心資訊

輸入後，按一下測試以檢查連線，並確認可以使用提供的資訊訪問Azure。



附註：如果適用，請確保排除/包含的使用者組與Entra配置保持一致

4)嚮導的最後一步允許您配置SAML強制網絡門戶使用者超時。預設值為1440分鐘。

5 User Session Timeout

SAML Captive Portal Users

1440

Minutes

Range 0–35791394

5)按一下Next繼續。

After the timeout is exceeded, the user's session ends; if the user continues to access the network without logging in again, the user is seen by the management center as Unknown (except for Failed Captive Portal Users).

Next

使用Azure AD領域配置前進

6)嚮導提供已實施的配置的摘要。在驗證和確認輸入的值之後，按一下摘要結尾的儲存。

5 User Session Timeout

Edit

SAML Captive Portal Users
ISE Users

1440 Minutes
1440 Minutes

Cancel

Save

領域配置摘要儲存按鈕

步驟 4:檢查下載的使用者

1)使用Integrations > Identity > Realms 工作流中的Download Now按鈕，確認可以從Azure Entra下載使用者。

Name	Type	Description	Proxy	Status	Value	
azure-entra-saml	SAML - Azure AD (captive portal)	Active Authentication IdP	Not Applicable	Ok	Tenant ID: af42bac0-f	Enabled Download Now

從Azure AD下載使用者

2)響應對話方塊提示，按一下Yes。

Sync Groups and Users for Realm

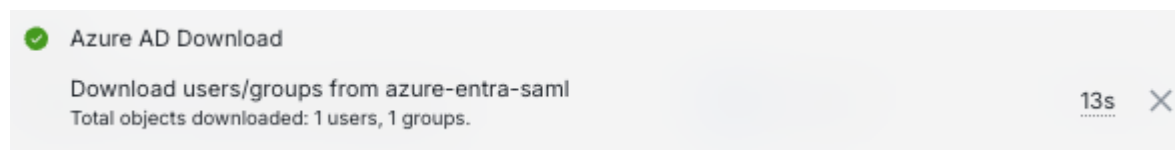
Are you sure you want to download users/groups for realm azure-entra-saml?

No

Yes

確認從Azure AD下載使用者

3)下載任務會產生1個使用者和1個已下載的組，如Notifications > Tasks下所確認。

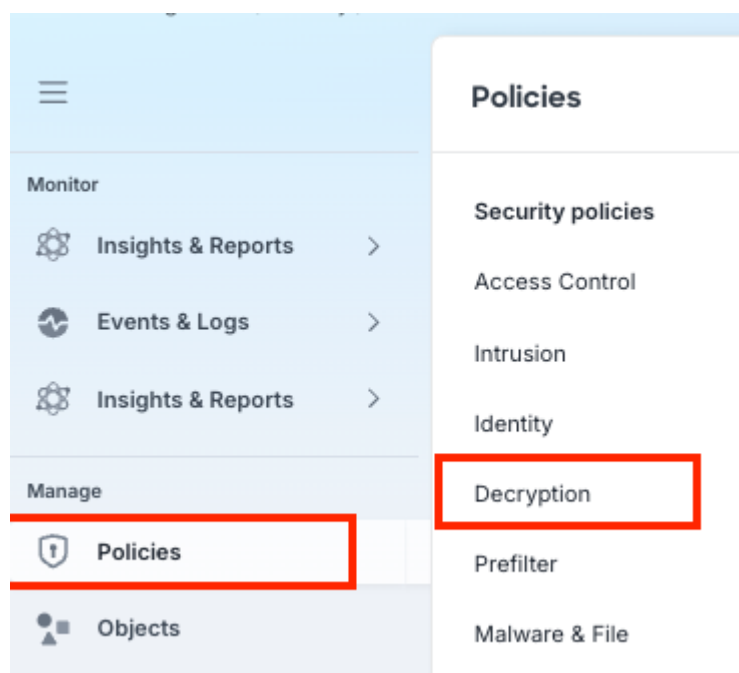


用於從Azure AD下載使用者的通知條目

第5階段：在FMC中配置策略

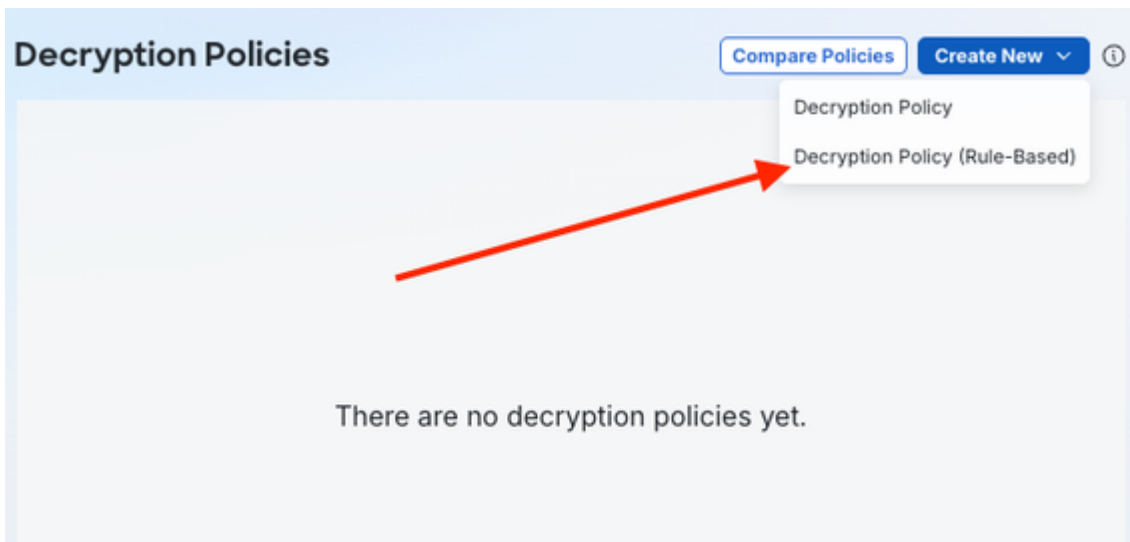
步驟 1:配置解密策略

1)在FMC中，選擇Policies > Security Policies > Decryption。



導航到Decryption Policy

2)按一下Create New下拉選單，然後選擇Decryption Policy(Rule-Based)。



建立新的基於規則的解密策略

3)為基於規則的新解密策略分配名稱和說明（如果需要），然後按一下Outbound Connections(User Protection)頁籤選項，以實施強制網路門戶身份驗證（主動身份驗證）所需的Decrypt-Resign功能。

實施出站連線策略詳細資訊

4)從同一對話框中的適用下拉清單中選擇先前應用的內部CA。按「Next」（下一步）。

5)根據需要自定義選項。

Create Decryption Policy ?

1 **Policy Details**
Enter name, description, choose policy type and certificates.

2 **Blocking**
(Optional) Configure blocking based on TLS version and certificate status

3 **Decryption Exclusions**
(Optional) Configure exclusions for outbound connections.

☐ **Block inbound and outbound connections based on TLS version**
We recommend blocking the following because they are not secure. [Reset to default](#)
SSL v3.0 X TLS v1.0 X TLS v1.1 X

☐ **Block inbound and outbound connections based on server certificate status**
We recommend blocking the following because they are not secure. [Reset to default](#)
Invalid Signature X Expired X Not Yet Valid X

[Cancel](#) [Skip](#) [Back](#) [Next](#)

自定義解密策略選項

6)在本例中，使用預設值，但所需的Policy Details除外。按一下Create Policy完成配置嚮導。

Create Decryption Policy

1 Policy Details
Enter name, description, choose policy type and certificates.

2 Blocking
(Optional) Configure blocking based on TLS version and certificate status

3 Decryption Exclusions
(Optional) Configure exclusions for outbound connections.

Decryption Exclusions

☐ Bypass decryption for sensitive URL categories
In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Customize the list below to bypass inspection for designated categories.
Note: URL License is Required
URL Categories: Finance Online Trading Health and Medicine + Add

☒ Bypass decryption for undecryptable distinguished names
Bypass decryption based on Cisco's list of known undecryptable distinguished names.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported distinguished names.
[56 Distinguished names included](#)

☒ Bypass decryption for undecryptable applications
Certain applications are not supported for decryption due to a variety of reasons (certificate pinning, client certificate authentication, and so on). This option bypasses decryption based on Cisco's list of known undecryptable applications.
Note: This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported applications.
[59 Applications included](#)

Intelligent Decryption Bypass

☐ Bypass decryption for very low-risk connections
Bypass decryption for very low-risk clients connecting to trusted servers.
Note: Do not decrypt traffic for very low-risk clients connecting to trusted servers, based on the threat confidence levels of clients

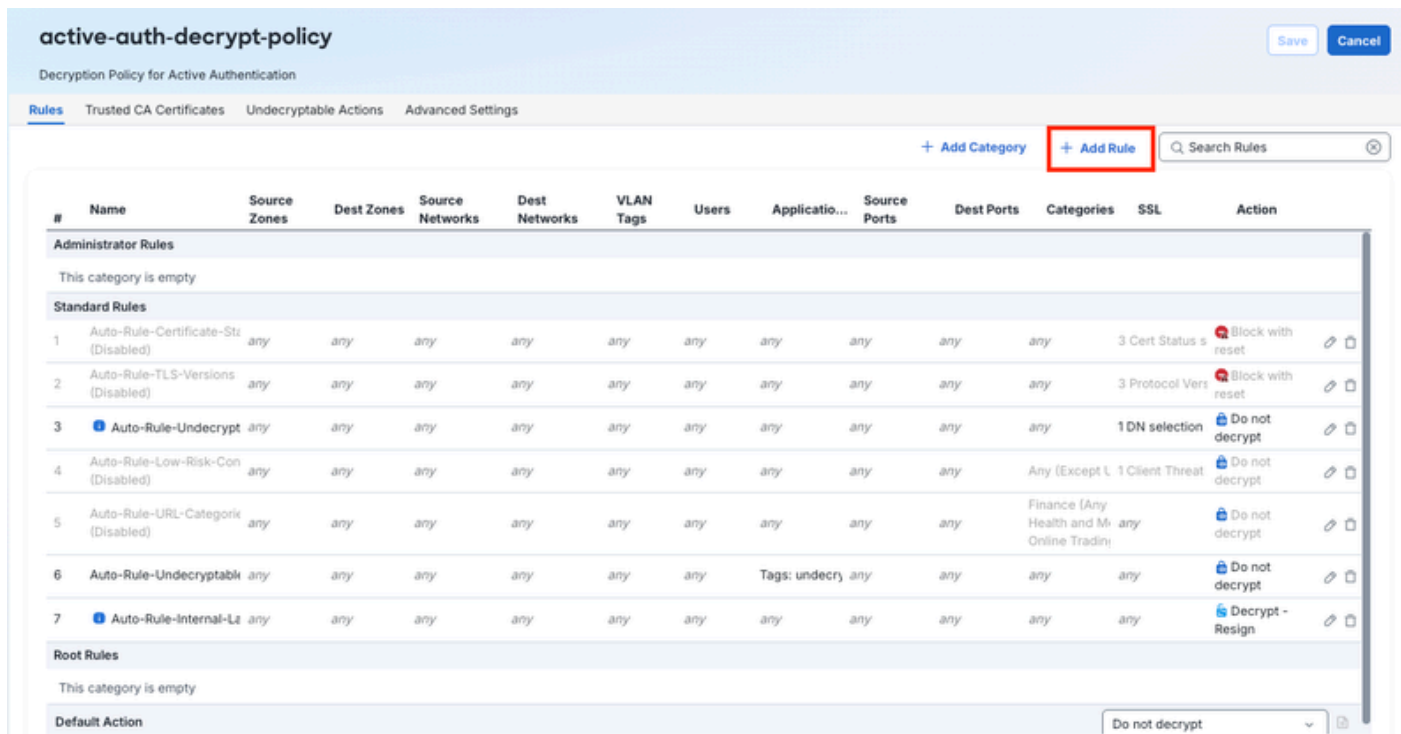
Cancel Skip Back Create Policy

建立最終解密策略

步驟 2:配置解密策略規則

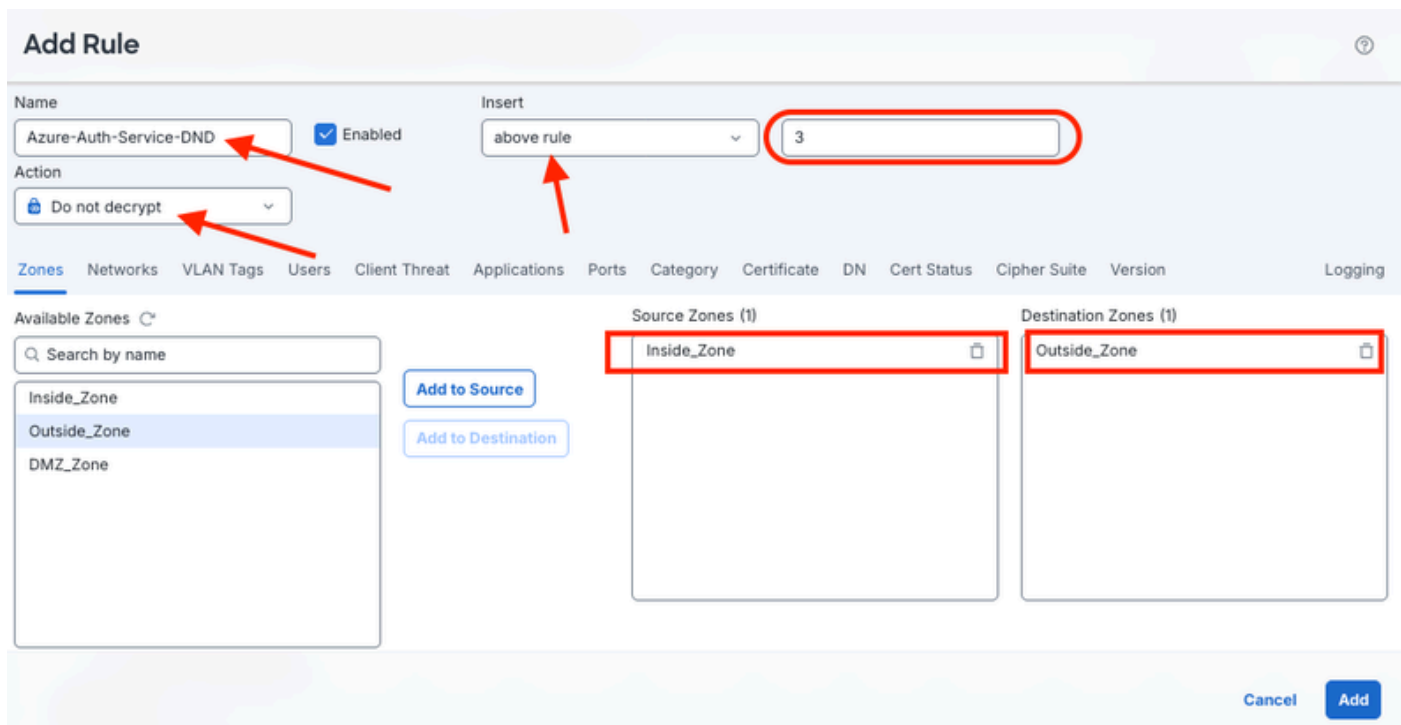
1)此處顯示了基於規則的解密策略的預設佈局。與預設啟用的規則不匹配的流量，例如規則3（引用未解密域名的預分配清單）和規則6（引用標籤為未解密的應用程式），將接受規則7下的「解密 — 重新簽名」操作。這些預設值和預設操作可以根據需要進行修改。預設情況下，不匹配其他規則的流量配置為Do Not Decrypt。

不能將Azure身份驗證服務流量解密以進行檢查，因此會為其建立專用規則。按一下+ Add Rule開始。



新增規則並顯示基於預設規則的解密佈局

2)為新的Decryption Policy rule項分配一個名稱，從Action下拉選單中選擇Do not decrypt，並將規則放在不太具體的頂端規則上。還實施源/目標區域以進一步縮小規則範圍。



配置不解密規則

3)在新增規則之前，按一下Applications頁籤，搜尋並按一下Azure身份驗證服務應用程式。按一下Add to Rule，然後按一下Add。

Add Rule

Name: ☒ Enabled Insert:

Action:

Zones Networks VLAN Tags Users Client Threat **Applications** Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Application Filters Available Applications (2)

Risks (Any Selected)

- ☐ Very Low 809
- ☐ Low 715
- ☐ Medium 2239
- ☐ High 1823
- ☐ Very High 609

Business Relevance (Any Selected)

- ☐ Very Low 809

Available Applications (2)

Search:

All apps matching the filter

- Azure Arc
- Azure Authentication Service**

Selected Applications and Filters (0)

新增Azure身份驗證服務應用程式規則

4)按一下Save。

active-auth-decrypt-policy

Decryption Policy for Active Authentication

You have unsaved changes.

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

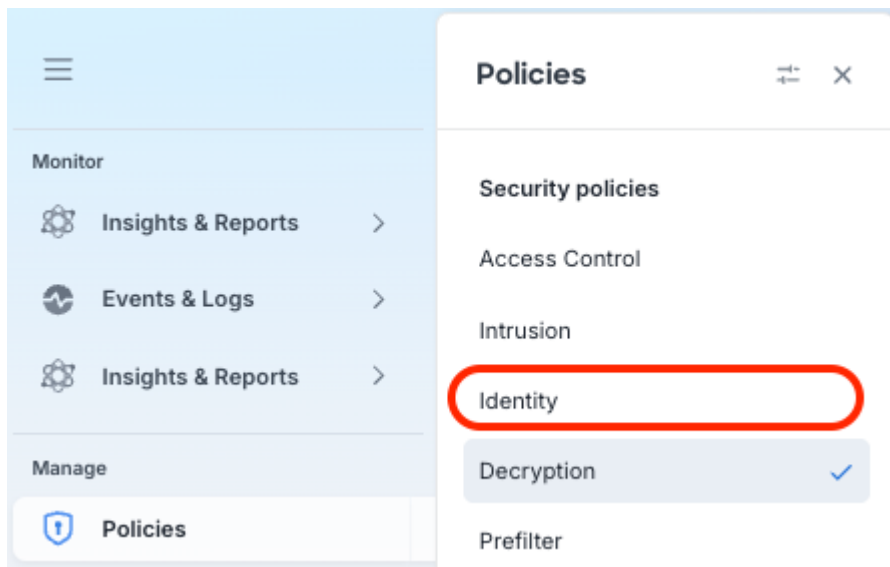
+ Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Application...	Source Ports	Dest Ports	Categories	SSL	Action
Standard Rules													
1	Auto-Rule-Certificate-St (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Cert Status s	Block with reset
2	Auto-Rule-TLS-Versions (Disabled)	any	any	any	any	any	any	any	any	any	any	3 Protocol Ver	Block with reset
3	Azure-Auth-Service-	Inside_Zone	Outside_Zon	any	any	any	any	Azure Authent	any	any	any	any	Do not decrypt

儲存解密策略

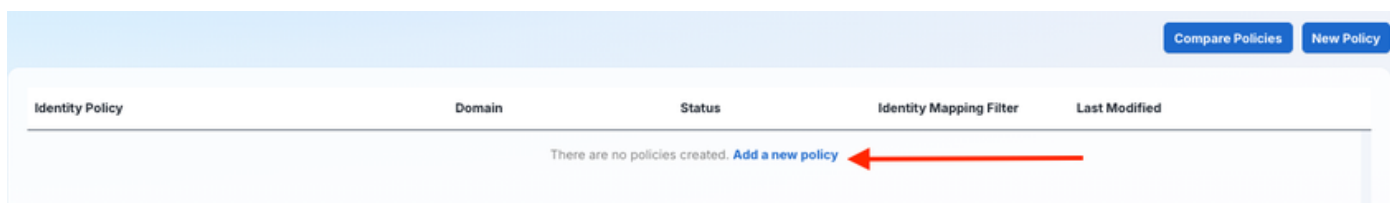
步驟 3:建立身份策略

1)選擇Policies > Security Policies > Identity以建立Identity Policy。



建立身份策略

2)建立新的身份策略，然後按一下新增新策略。



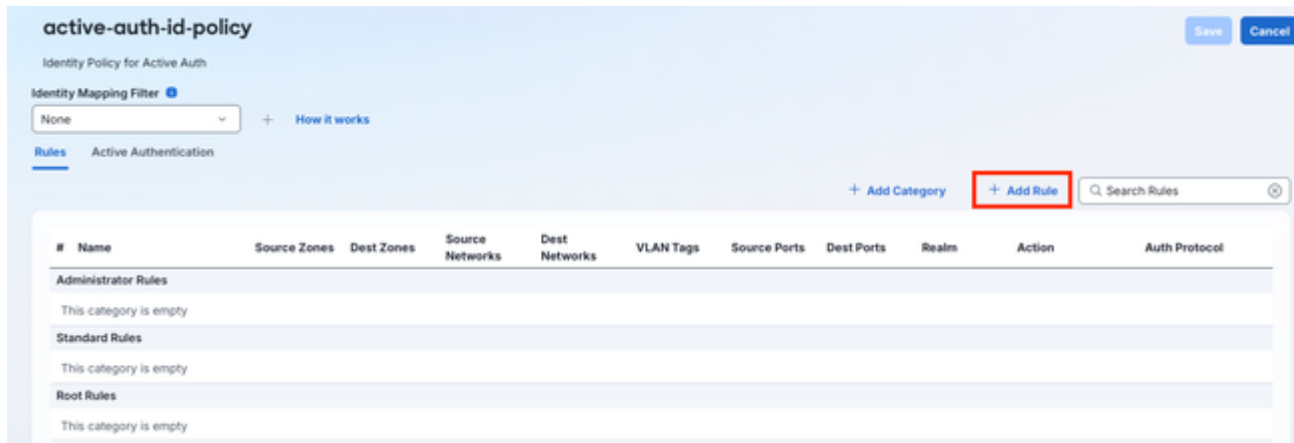
新增新的身份策略配置

3)為新身份策略分配名稱和說明 (如果適用)。按一下「Save」。

命名新身份策略

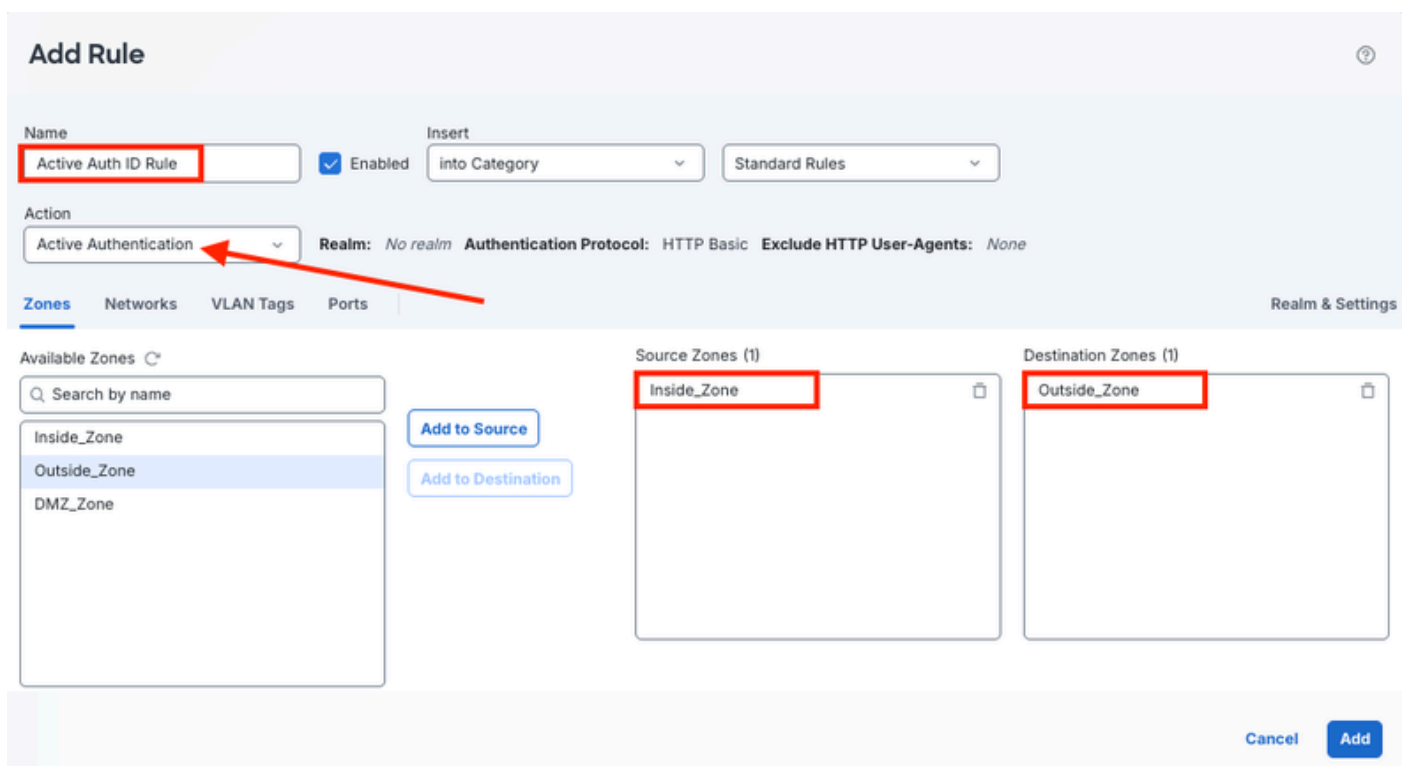
步驟 4:配置身份策略規則

1)按一下+新增規則(Add Rule)新增新規則。



新增新的身份策略規則

2)為新規則命名名稱，從Action下拉選單中選擇Active Authentication，並縮小與規則匹配才能執行Active Authentication的特定區域/網路範圍。



配置活動身份驗證規則設定

3)按一下Add之前，在規則編輯器內按一下Realm and Settings頁籤。確認在上述步驟中配置的領域被選為身份驗證領域，然後按一下Add。

Add Rule

Name: Active Auth ID Rule ☒ Enabled Insert: into Category Standard Rules

Action: Active Authentication **Realm:** azure-entra-saml (S... **Authentication Protocol:** SAML **Exclude HTTP User-Agents:** None

Zones Networks VLAN Tags Ports [Realm & Settings](#)

Authentication Realm *
azure-entra-saml (SAML)

☐ Use passive identity if available.
Active identity realm is going to be used as a passive identity realm.

Authentication Protocol
SAML

▶ HTTP User Agent Exclusions

Cancel Add

配置身份規則的領域和設定

4)新增並配置規則。按一下「Save」。

active-auth-id-policy

Identity Policy for Active Auth

Identity Mapping Filter: None [How it works](#)

[Rules](#) Active Authentication

[+ Add Category](#) [+ Add Rule](#)

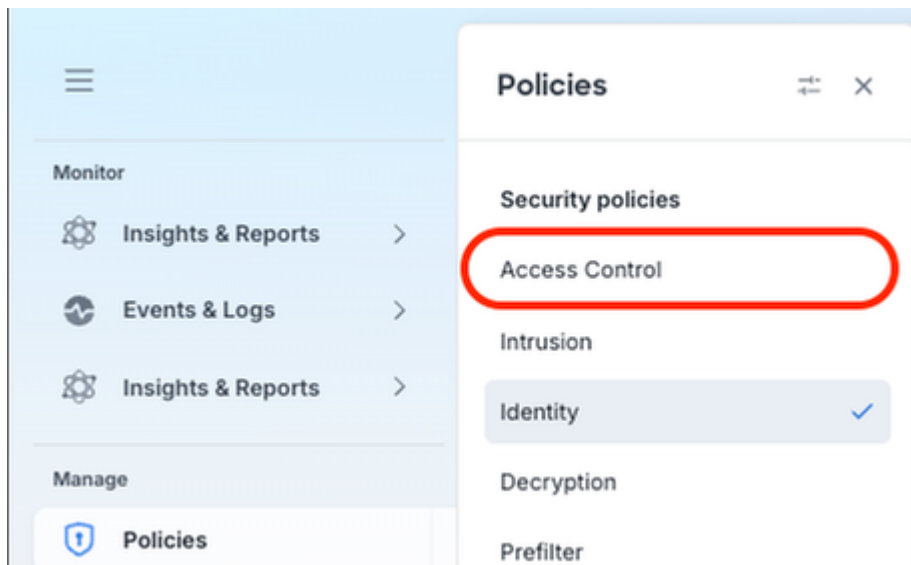
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	Active Auth ID Rule	Inside_Zone (Ro	Outside_Zone (f	any	any	any	any	any	azure-entra-san	Active Authentication	SAML
Root Rules											
This category is empty											

You have unsaved changes [Save](#) [Cancel](#)

儲存身份策略規則配置

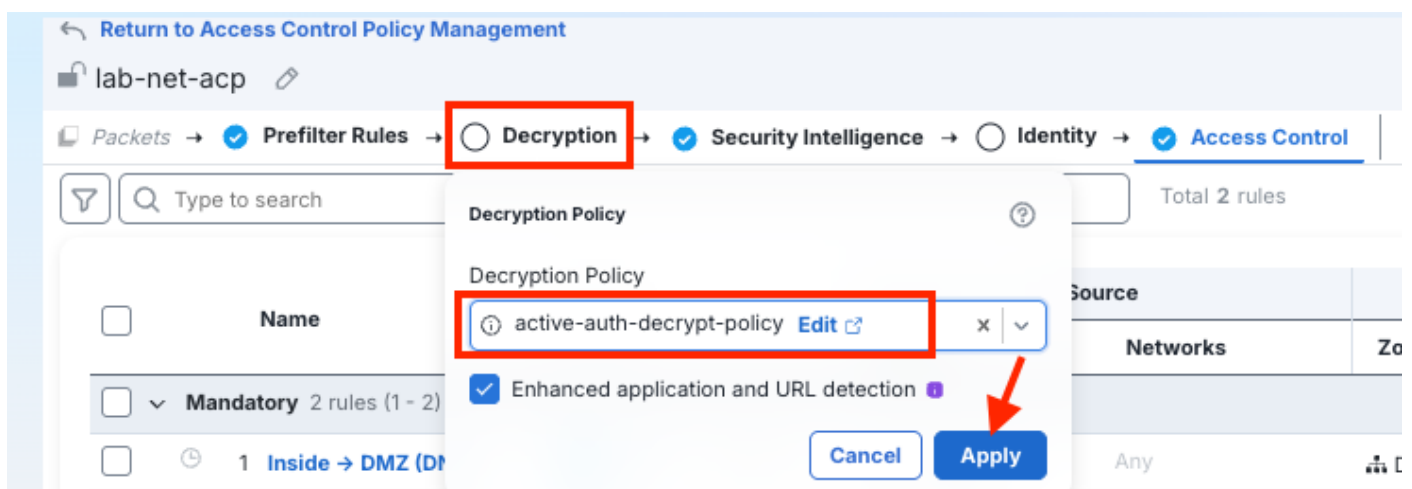
步驟 5:配置訪問控制策略

1)選擇Policies > Security Policies > Access Control，然後點選FTD分配到的Access Control Policy。



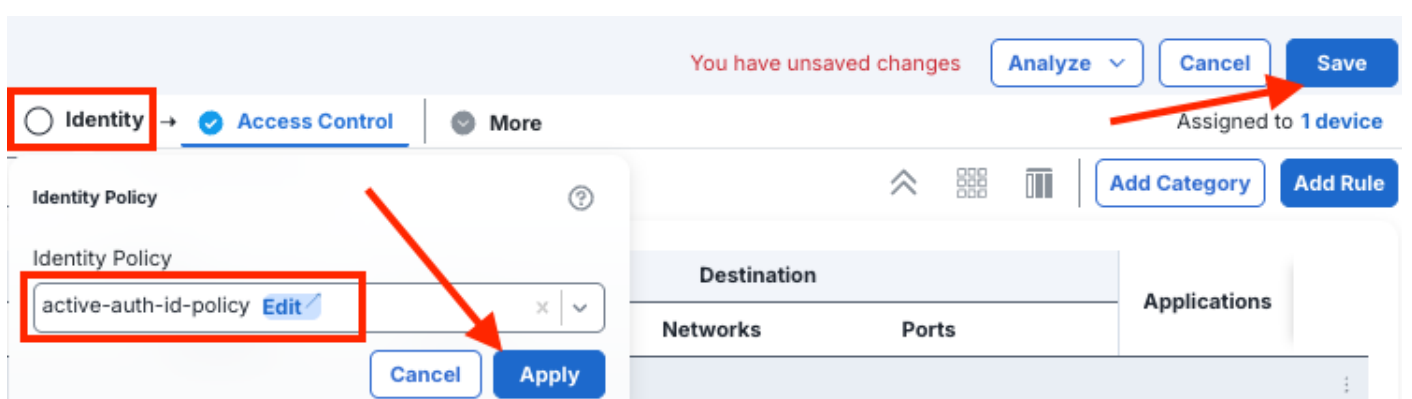
訪問控制策略配置

2)確認在前面步驟中配置的解密策略已應用於訪問控制策略。



將解密策略應用於訪問控制

3)確認前面步驟中配置的身份策略也應用於訪問控制策略。儲存策略更改。



將身份策略應用於訪問控制

4)確認存在允許客戶端資料平面流量在成功進行主動身份驗證後通過安全防火牆的規則。此處顯示的示例使用給定實驗室環境的較寬規則集。

☐	Name	Action	Source		Destination			Applications
			Zones	Networks	Zones	Networks	Ports	
☐ Mandatory 2 rules (1 - 2)								
☐	1 Inside → DMZ (DNS)	Allow	Inside_Zone	Any	DMZ_Zone	Any	Application Default	DNS
☐	2 DMZ-Inside → Outside	Allow	DMZ_Zone Inside_Zone	Any	Outside_Zone	Any	Any	Any
☐ Default (No rules)								

使用者資料平面流量規則集

步驟 6:將配置部署到思科安全防火牆裝置

部署後，傳送流量的客戶端將通過Microsoft登入網頁提示，以便使用Azure Entra執行主動身份驗證。

有關此處記錄的進程的其他上下文，請參閱[為主動身份驗證（強制網路門戶）建立Microsoft Azure AD\(SAML\)領域 — 章節：FMC裝置設定指南10.x中的領域。](#)

驗證

使用本節內容，協助確認組態是否正常運作。

GUI

驗證FMC中的使用者會話和活動：

- 選擇Integrations > Users > Active Sessions。

Cloud-delivered Firewall Management Center

Integrations / Users / Active Sessions

Search

Switch to legacy UI

Select...

Refresh

Delete

Showing the 1 and only session

...

Login Time

Last Seen

Login Time

Realm/Username

Last Seen ↓

Authentication Type

Current IP

Session Duration

Realm

Username

2026-10-07 02:10:02

azure-entra-saml/captive-pc

2026-10-07 02:10:02

Active Authentication

1 min 40 sec

azure-entra-saml

captive-portal-user

Monitor

Insights & Reports

Events & Logs

Manage

FMC活動會話輸出

- 選擇Integrations > Users > User Activity。

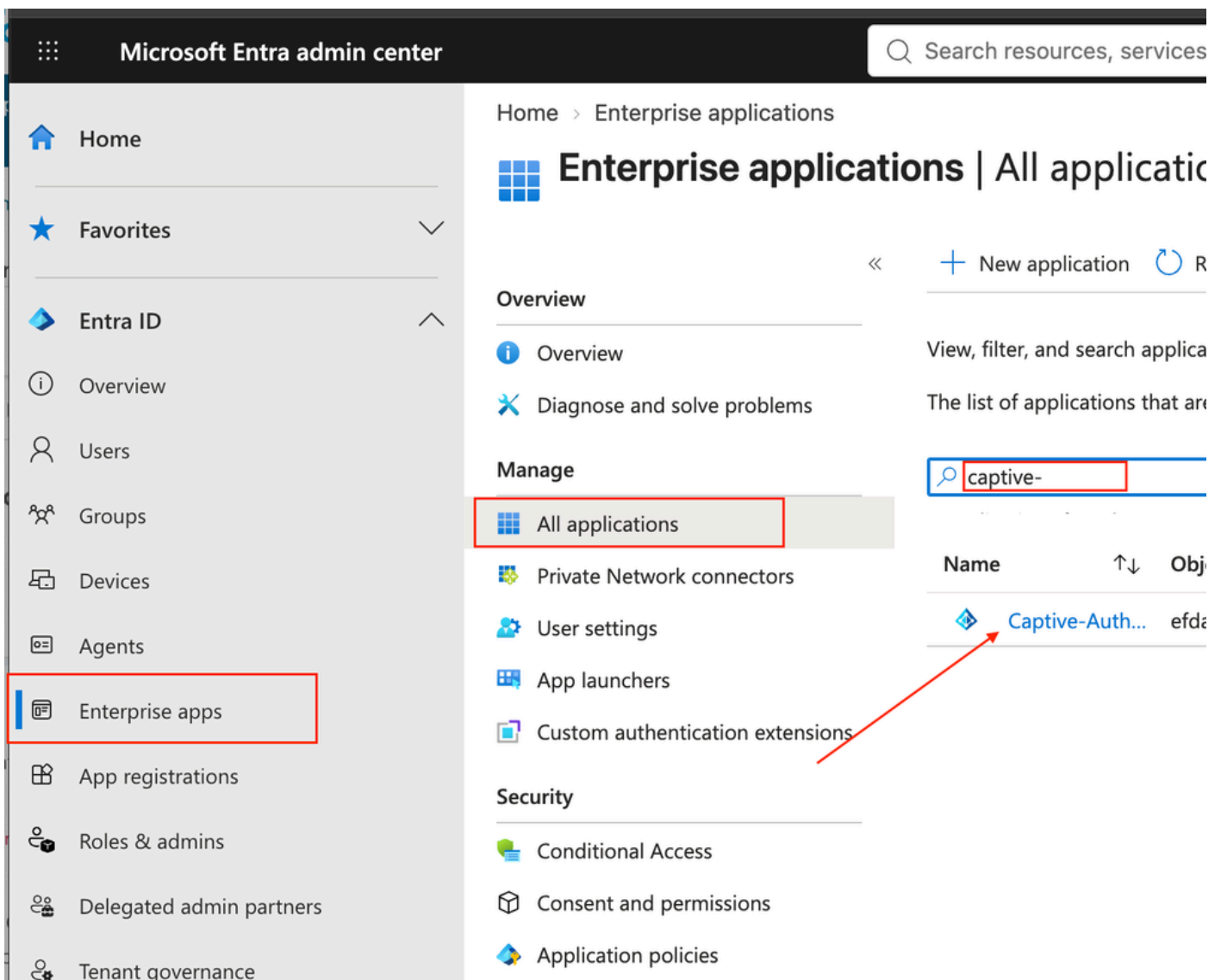


Time	Username	Event	Realm	Discovery Application	Authentication Type	IP Address	Start Port
2026-10-07 02:10:02	captive-portal-user	User Login	azure-entra-saml	Microsoft Azure	Active Authentication		
2026-10-07 02:10:01	captive-portal-user	User Login	azure-entra-saml	Microsoft Azure	Active Authentication		

FMC使用者活動輸出

在Azure上，導航到Microsoft Entra管理中心：

- 篩選Enterprise Apps，搜尋/按一下適用的應用。



Microsoft Entra admin center

Home > Enterprise applications

Enterprise applications | All applications

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Private Network connectors
- User settings
- App launchers
- Custom authentication extensions

Security

- Conditional Access
- Consent and permissions
- Application policies

Search resources, services

Search: captive-

Name	Obj
Captive-Auth...	efda

Azure Entra管理中心企業應用導航

- 選擇Activity > Sign-in logs。

Home > Enterprise applications | All applications > Captive-Auth-SAML



Captive-Auth-SAML | Sign-in logs

Enterprise Application

«

Download

Export data Settings

Troubleshoot

Refresh

Manage view

Got feedback?

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Want to switch back to the legacy signin logs experience? Click here to leave the preview.

Add filter

Show dates as: UTC

Date range: 10/7/2026 - 10/7/2026

Application contains

User sign-ins (interactive)

User sign-ins (non-interactive)

Service principal sign-ins

Managed identity sign-ins

Date ↓	Request ID	User principal name	Application	Status
2026-10-07T06:10:02Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:01Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:10:00Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:59Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:58Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:52Z		captive-portal-user@...	Captive-Auth-SAML	Success
2026-10-07T06:09:51Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted
2026-10-07T06:09:29Z		captive-portal-user@...	Captive-Auth-SAML	Interrupted

Azure企業應用程式登入活動日誌

CLI

- 在FTD CLI中，您可以看到與SAML和強制網路門戶響應相關的統計資訊：

<#root>

>

debug menu captive-portal 6

```
SAML passed requests captive-portal 14
SAML failed requests captive-portal 0
SAML passed responses captive-portal 4
SAML failed responses captive-portal 0
Total captive-portal bee-client messages processed 4
Total captive-portal bee-client messages successful 4
Total captive-portal bee-client messages failed 0
Total bee-client reconnects 0
```

疑難排解

強制網路門戶調試

- `system support captive-portal-debug`命令可用於FTD。輸出顯示如何啟用調試，並記錄輸出的關鍵部分，以幫助瞭解強制網路門戶流量。

```
<#root>
```

```
>
```

```
system support captive-portal-debug
```

```
Enable firewall-debug too? [n]:
```

```
y
```

```
Enable identity-debug too? [n]:
```

```
y
```

```
Please specify an IP protocol:
```

```
tcp
```

```
Please specify a client IP address:
```

```
192.168.20.200
```

```
Please specify a client port:
```

```
Please specify a server IP address:
```

```
Please specify a server port:
```

```
Enable daq-debug too? (WARNING: current packet debug configs and logs will be overwritten) [n]:
```

```
Monitoring captive_portal and firewall and identity debug messages
```

```
!---
```

```
Baseline output pending user Captive Portal authentication
```

```
...
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 match rule order 1, id 1 action Captive por
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 didn't find active binding, initiating capt
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 captive portal authentication started
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 defer trust until captive portal redirect i
```

```
192.168.20.200 53650 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 Current state = S_INIT, Event = EVT_CP_RULE
```

```
...
```

```
!---
```

```
Captive Portal probe intercepted and redirected to SAML IdP (generate_204)
```

```
...
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 AppID session with service_id: 676, url: http
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 Current state = S_PENDING_USER, Event = EVT_
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 app event changes: service, client, host, ur
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 using ipv4 address 192.168.20.1 for redirect
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 encrypted redirect url: https://ftd-inside.e
192.168.20.200 53659 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 Current state = S_REDIRECTING, Event = EVT_F
...
!---
```

SAML authentication completes, identity binding created

```
...
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 looked for user_id with realm_id 2 auth_type
192.168.20.200 54023 -> 198.51.100.280 6 AS=0 ID=2 GR=1-1 found active binding for user_id 0 usernames
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 IdentityFlowSetupEventHandler Retrieved iden
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 New firewall session
192.168.20.200 54023 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 allow action
...
!---
```

Authenticated binding persists across subsequent, unrelated destinations (no further redirects)

```
...
192.168.20.200 54024 -> 198.51.100.2 80 6 AS=0 ID=2 GR=1-1 found active binding for user_id 0 usernames
192.168.20.200 54025 -> 198.51.100.1 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 54026 -> 198.51.100.2 80 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 54027 -> 198.51.100.3 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
192.168.20.200 19935 -> 198.51.100.4 443 6 AS=0 ID=1 GR=1-1 found active binding for user_id 0 usernam
...
```

使用者身份轉儲

- 要獲取FTD上當前使用者身份狀態資料的快照，請在FTD CLI上運行system support firewall-engine-dump-user-identity-data命令：

```
> system support firewall-engine-dump-user-identity-data
```

```
Successfully commanded snort.
```

```
>
```

- 在專家模式CLI中，使用FTD裝置的本機管理員憑證登入時，在
/ngfw/var/sf/user_enforcement/user_identity.dump中檢視轉儲檔案的內容

```
<#root>
```

```
>
```

```
expert
```

```
admin@ftd:~$
```

```
sudo su
```

```
Password:
```

```
root@ftd:/home/admin#
```

```
root@ftd:/home/admin#
```

```
ls -lah /ngfw/var/sf/user_enforcement/user_identity.dump
```

```
-rw----- 1 root root 5.6K Oct  7 07:51 /ngfw/var/sf/user_enforcement/user_identity.dump
```

```
root@ftd:/home/admin#
```

```
root@ftd:/home/admin#
```

```
less /ngfw/var/sf/user_enforcement/user_identity.dump
```

```
...
```

```
-----
```

```
IP:USER
```

```
-----
```

```
!--- Host IP is aligned with the user authenticated via Captive Portal/Active Authentication
```

```
-----
```

```
Host ::ffff:192.168.20.200
```

```
-----
```

```
::ffff:192.168.20.200:0 realm 2 type 8, username azure-entra-saml\captive-portal-user@onmicrosoft.examp
```

```
::ffff:192.168.20.200: SXP initialized 0 sgt 0
```

```
ABP values: None
```

```
-----
```

```
SXP MAPPING:
```

```
-----
```

```
...
```

可能的問題

強制網路門戶未知證書頒發機構

問題：嘗試進行身份驗證時，客戶端瀏覽器返回未知的頒發者錯誤。

可能原因:在客戶端瀏覽器中，內部證書頒發機構不受信任。

解析度：確認瀏覽器中信任該CA。此處顯示的範例確認內部CA憑證是否受信任。

Captive Portal "找不到伺服器

問題：當客戶端瀏覽器嘗試載入強制網路門戶時，在嘗試訪問基本URL或類似內容時，它會針對基本URL返回「找不到伺服器」。

可能原因:DNS可達性或DNS配置錯誤。

解析度：確認客戶端配置了用於解析A記錄的相應DNS伺服器。確認伺服器具有對映到FQDN的A記錄，並且伺服器可訪問且能夠響應。

相關資訊

- [為主動身份驗證（強制網路門戶）建立Microsoft Azure AD\(SAML\)領域 — FMC裝置配置指南 10.x](#)
- [Azure事件中心文檔](#)
- [技術支援與文件 - Cisco Systems](#)

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）。