

為FTD上的多個RAVPN連線設定檔設定SAML驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[組態](#)

[配置概述：](#)

[設定](#)

[Azure IdP上的配置](#)

[透過FMC在FTD上設定](#)

[驗證](#)

[FTD指令行上的組態](#)

[從Azure entra識別符號登入日誌](#)

[疑難排解](#)

簡介

本文檔介紹使用Azure身份提供程式對由FMC管理的思科FTD上的多個連線配置檔案進行SAML身份驗證。

必要條件

需求

思科建議瞭解以下主題：

- 由Firepower管理中心(FMC)管理的下一代防火牆(NGFW)上的安全客戶端配置
- SAML和metatada.xml值

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower威脅防禦(FTD)版本7.4.0
- FMC版本7.4.0
- 使用SAML 2.0的Azure Microsoft Entra ID
- 思科安全使用者端5.1.7.80

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

此配置允許FTD在Azure idp上使用兩個不同的SAML應用程式對安全客戶端使用者進行身份驗證，並在FMC上配置單個SAML對象。

Name	↑↓	Object ID	Application ID	Homepage URL	Created on↑↓	Certificate ...	Active Ce...	Identifier URI (Entity I...
 FTD-SAML-1		44988e73-c06f-4008-be74...	0cff60a9-271f-4976-9848-...	https://*.YourCiscoServer....	25/11/2024	✔ Current	25/11/2027	https://[redacted]...
 FTD-SAML-2		dbe20be6-5440-4951-863...	2400bc8b-21b7-4f29-85c4...	https://*.YourCiscoServer....	25/11/2024	✔ Current	27/11/2027	https://[redacted]..

在Microsoft Azure環境中，多個應用程式可以共用相同的實體ID。每個應用程式（通常對映到不同的隧道組）都需要一個唯一的證書，要求在單個SAML IdP對象下的FTD端的IdP配置中配置多個證書。但是，思科FTD不支援在一個SAML IdP對象下設定多個憑證，如思科錯誤ID [CSCvi29084所述](#)。

為克服此限制，思科引入了IdP憑證覆寫功能，該功能可從FTD 7.1.0版和ASA 9.17.1版獲得。此增強功能提供永久的解決問題解決方案，並補充了錯誤報告中所述的現有解決方法。

組態

本節概述在Firepower管理中心(FMC)管理的Cisco Firepower威脅防禦(FTD)上，將Azure作為身份提供程式(IdP)配置SAML身份驗證的過程。利用IdP證書覆蓋功能可有效地進行設定。

配置概述：

在Cisco FTD上設定兩個連線設定檔：

- FTD-SAML-1
- FTD-SAML-2

在此配置示例中，VPN網關URL（思科安全客戶端FQDN）設定為[nigarapa2.cisco.com](#)

設定

Azure IdP上的配置

要為Cisco Secure Client有效配置SAML企業應用，請完成以下步驟，確保為每個隧道組正確設定所有引數：

訪問SAML企業應用程式：

導航到列出企業應用程式的SAML提供程式的管理控制檯。

選擇適當的SAML應用程式：

識別並選擇與要配置的思科安全客戶端隧道組對應的SAML應用。

配置識別符號 (實體ID) :

設定每個應用程式的識別符號 (實體ID)。這必須是基本URL，它是您的思科安全客戶端完全限定域名(FQDN)。

設定回覆URL (斷言使用者服務URL) :

使用正確的基本URL配置回覆URL (斷言使用者服務URL)。確保它與思科安全客戶端FQDN一致。

將連線配置檔案或隧道組名稱附加到基本URL以確保特異性。

驗證設定 :

仔細檢查是否所有URL和引數都已正確輸入，並且對應於相應的隧道組。

儲存更改，如有可能，執行測試身份驗證以確保配置按預期運行。

有關更詳細的指導，請參閱思科文檔中的「從Microsoft應用庫新增Cisco安全客戶端」：[通過SAML配置Microsoft Azure MFA的ASA安全客戶端VPN](#)

FTD-SAML-1

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1

FTD-SAML-1 | SAML-based Sign-on

Enterprise Application

» [Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#)

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experience. Choose SAML single sign-on whenever possible for existing applications that do not have a native SSO implementation.

Read the [configuration guide](#) for help integrating FTD-SAML-1.

1

Basic SAML Configuration

Identifier (Entity ID)	https://[redacted].cisco.com/saml/sp/metadata/FTD-SAML-1
Reply URL (Assertion Consumer Service URL)	https://[redacted].cisco.com/+CSCOE+/SAML/SP/ACS
Sign on URL	Optional
Relay State (Optional)	Optional
Logout URL (Optional)	Optional

2

Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3

SAML Certificates

Token signing certificate	Active
Status	3125987754C6B7CCBE86DD214BD
Thumbprint	25/11/2027, 18:23:11
Expiration	
Notification Email	

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.

https://[redacted].cisco.com/saml/sp/metadata/FTD-SAML-1

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.

https://[redacted].cisco.com/+CSCOE+/saml/sp/acs?tgname=FTD-SAML-1

Add reply URL

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

Sign on URL (Optional)

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.

Enter a sign on URL

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.

Enter a relay state

FTD-SAML-1 | SAML-based Sign-on

Enterprise Application

» [Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Certificates

Token signing certificate

Status	Active
Thumbprint	3125987754C687CCBE86DD214BD...
Expiration	25/11/2027, 18:23:11
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

Set up FTD-SAML-1

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

Login URL	https://login.microsoftonline.com/...
Microsoft Entra Identifier	https://sts.windows.net/477a586b...
Logout URL	https://login.microsoftonline.com/...

Test single sign-on with FTD-SAML-1

SAML Signing Certificate

Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

[Save](#) [+ New Certificate](#) [Import Certificate](#) [Got feedback?](#)

Status	Expiration Date	Thumbprint	
Active	25/11/2027, 18:23:11	3125987754C687CCBE86DD214BD...	...

Signing Option [Sign SAML assertion](#)

Signing Algorithm [SHA-256](#)

Notification Email Addresses

4

Set up FTD-SAML-1

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

Login URL	https://login.microsoftonline.com/477a586b-61c2...
Microsoft Entra Identifier	https://sts.windows.net/477a586b-61c2-4c8e-9a4...
Logout URL	https://login.microsoftonline.com/477a586b-61c2...

5

FTD-SAML-2

FTD-SAML-2 | SAML-based Sign-on

Enterprise Application

» [Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#)

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experience. Choose SAML single sign-on whenever possible for existing applications that do not support OpenID Connect.

Read the [configuration guide](#) for help integrating FTD-SAML-2.

1

Basic SAML Configuration

Identifier (Entity ID)

https://[redacted].cisco.com/saml/2

Reply URL (Assertion Consumer Service URL)

https://[redacted].cisco.com/+CSCOE+FTD-SAML-2

Sign on URL

Optional

Relay State (Optional)

Optional

Logout URL (Optional)

Optional

2

Attributes & Claims

givenname

user.givenname

surname

user.surname

emailaddress

user.mail

name

user.userprincipalname

Unique User Identifier

user.userprincipalname

3

SAML Certificates

Token signing certificate

Status

Active

Thumbprint

F1CF8A1B07E704EE793A7132AF04...

Expiration

27/11/2027, 02:33:11

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.

https://[redacted].cisco.com/saml/sp/metadata/FTD-SAML-2

[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.

https://[redacted].cisco.com/+CSCOE+/saml/sp/acs?tgname=FTD-SAML-2

[Add reply URL](#)

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

Sign on URL (Optional)

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.

Enter a sign on URL

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.

Enter a relay state

FTD-SAML-2 | SAML-based Sign-on

Enterprise Application

» [Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#)

3

SAML Certificates

Token signing certificate

Status

Active

Thumbprint

F1CF8A1B07E704EE793A7132AF04...

Expiration

27/11/2027, 02:33:11

Notification Email

[redacted]

App Federation Metadata URL

https://login.microsoftonline.com/...

Certificate (Base64)

Download

Certificate (Raw)

Download

Federation Metadata XML

Download

Verification certificates (optional)

Required

No

Active

0

Expired

0

4

Set up FTD-SAML-2

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

Login URL

https://login.microsoftonline.com/...

Microsoft Entra Identifier

https://sts.windows.net/477a586b...

Logout URL

https://login.microsoftonline.com/...

SAML Signing Certificate

Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

[Save](#) [New Certificate](#) [Import Certificate](#) [Got feedback?](#)

Status	Expiration Date	Thumbprint	
Active	27/11/2027, 02:33:11	F1CF8A1B07E704EE793A7132AF044629C31FD9A7	...
Signing Option			
Sign SAML assertion			
Signing Algorithm			
SHA-256			
Notification Email Addresses			
[redacted]			

Set up FTD-SAML-2

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

Login URL	https://login.microsoftonline.com/477a586b-61c2...
Microsoft Entra Identifier	https://sts.windows.net/477a586b-61c2-4c8e-9a4...
Logout URL	https://login.microsoftonline.com/477a586b-61c2...

現在，請確保您擁有使用Microsoft Entra作為身份提供程式配置SAML身份驗證的必要資訊和檔案：

找到Microsoft Entra識別符號：

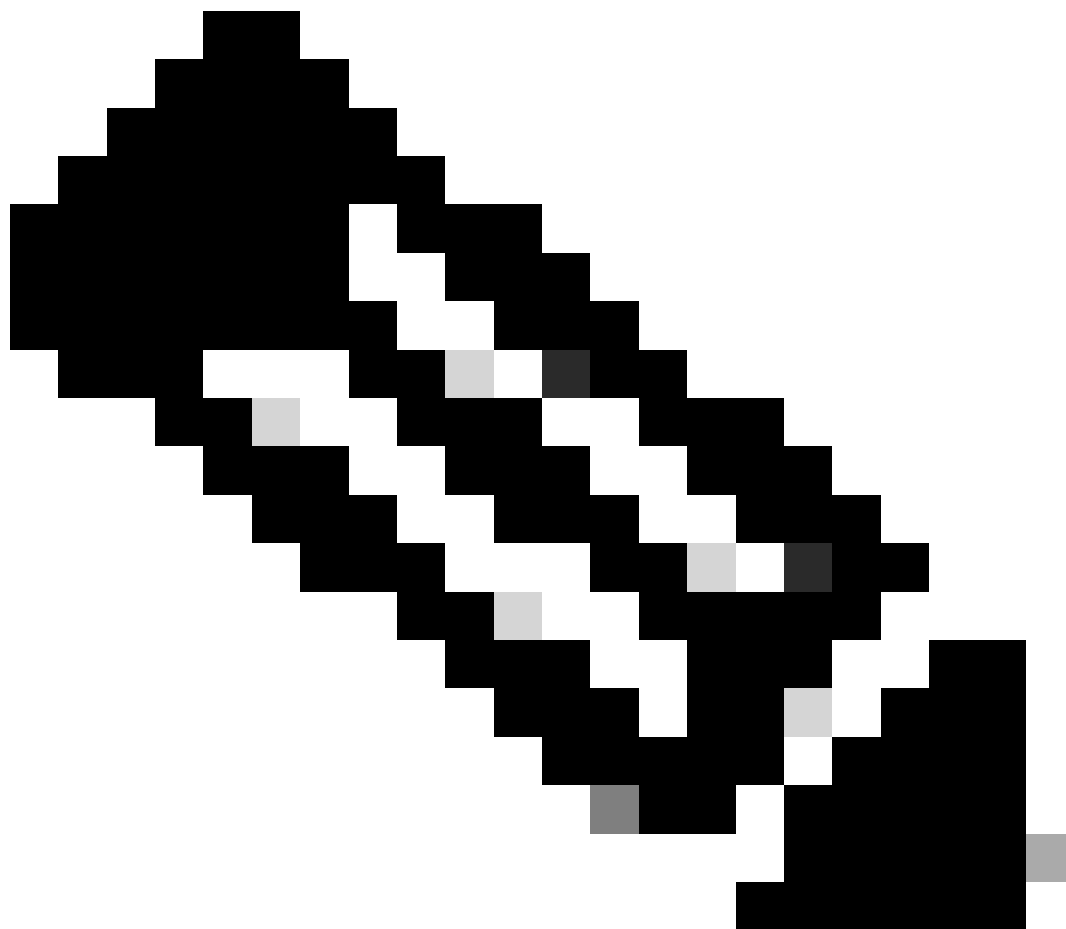
訪問Microsoft Entra門戶中的兩種SAML企業應用程式的設定。

請注意Microsoft Entra識別符號，它在兩個應用程式之間保持一致，並且對於您的SAML配置至關重要。

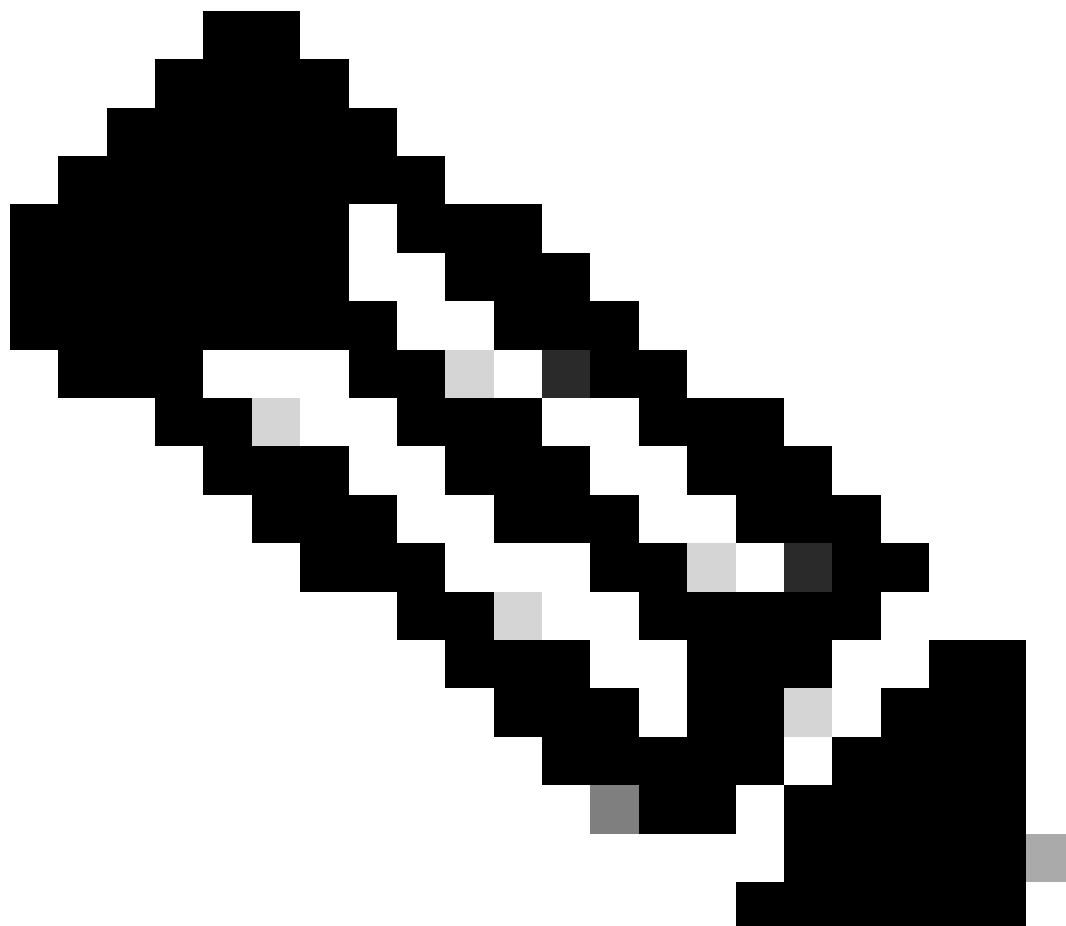
下載Base64 IdP證書：

導航到每個已配置的SAML企業應用程式。

下載各自的Base64編碼IdP證書。這些證書對於在您的身份提供商和Cisco VPN設定之間建立信任至關重要。



附註：FTD連線設定檔所需的所有這些SAML設定，均可從IdP為各自的應用提供的metadata.xml檔案取得。



附註：要使用自定義IdP證書，您需要將自定義生成的IdP證書上傳到IdP和FMC。對於 Azure IdP，請確保證書採用PKCS#12格式。在FMC上，僅從IdP上傳身份證書，不從PKCS#12檔案上傳。有關詳細說明，請參閱思科文檔中的「在Azure和FDM上傳PKCS#12檔案」部分：[在FDM上使用SAML身份驗證配置多個RAVPN配置檔案](#)

透過FMC在FTD上設定

註冊IdP證書：

導航到FMC中的證書管理部分，並為兩個SAML應用程式註冊下載的Base64編碼的IdP證書。這些證書對於建立信任和啟用SAML身份驗證至關重要。

如需詳細指導，請參閱以下網址上提供的思科文檔中「透過FMC在FTD上設定」下的前兩個步驟：[在通過FMC管理的FTD上配置具有SAML身份驗證的安全客戶端](#)。

Filter

All Certificates

Add

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status	
> 1						
>						
10.106.65.25						
2	Global	Manual (CA & ID)		Dec 12, 2029		
FTD-SAML-1-ldp-cert	Global	Manual (CA Only)		Nov 25, 2027		
FTD-SAML-2-ldp-cert	Global	Manual (CA Only)		Nov 27, 2027		

CA Certificate

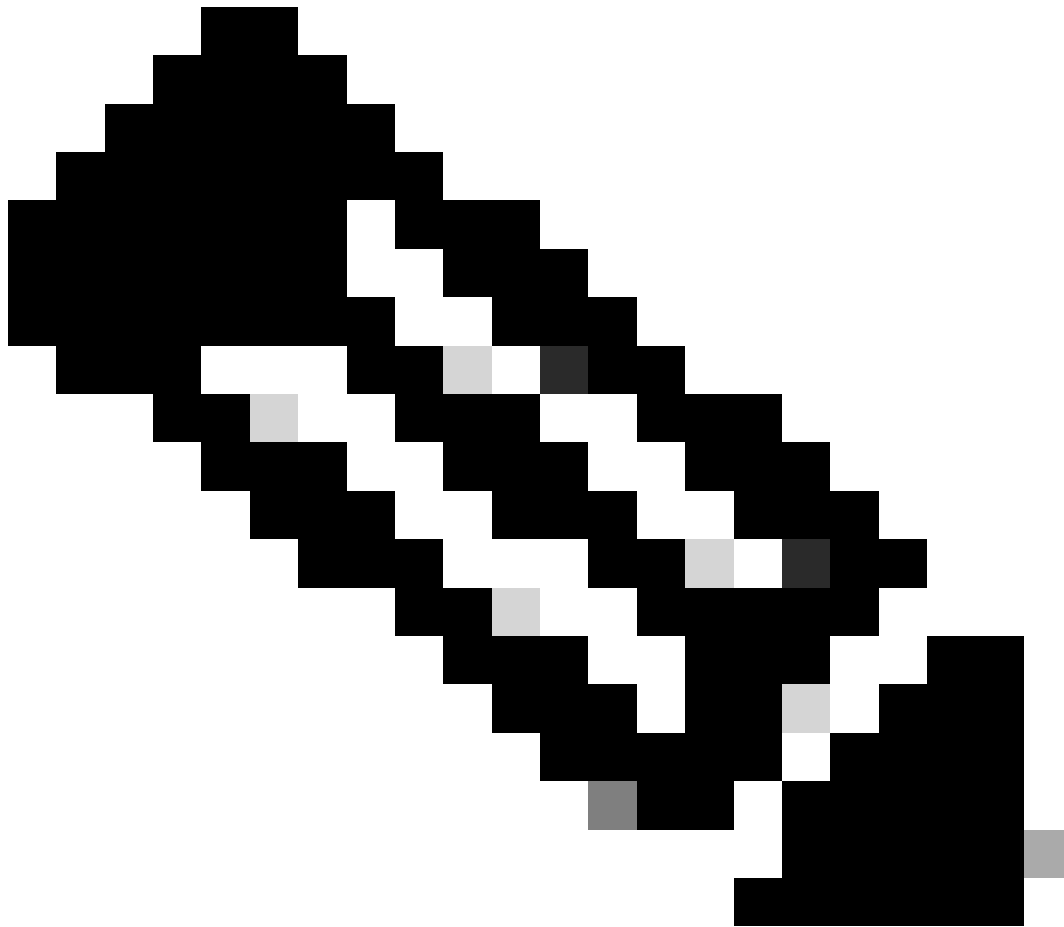
- Status : Available
- Serial Number : 208P94F0831ede99490c7c64dda7bee8
- Issued By :
CN : Microsoft Azure Federated SSO Certificate
- Issued To :
CN : Microsoft Azure Federated SSO Certificate
- Public Key Type : RSA (2048 bits)
- Signature Algorithm : RSA-SHA256
- Associated Trustpoints : FTD-SAML-1-ldp-cert
- Valid From : 12:53:11 UTC November 25 2024
- Valid To : 12:53:11 UTC November 25 2027

Close

CA Certificate

- Status : Available
- Serial Number : 2758279b3b5cc98044c60399906bee61
- Issued By :
CN : Microsoft Azure Federated SSO Certificate
- Issued To :
CN : Microsoft Azure Federated SSO Certificate
- Public Key Type : RSA (2048 bits)
- Signature Algorithm : RSA-SHA256
- Associated Trustpoints : FTD-SAML-2-ldp-cert
- Valid From : 21:03:11 UTC November 26 2024
- Valid To : 21:03:11 UTC November 26 2027

Close



附註：影象已經過編輯，可以同時顯示兩個證書，以便更好地檢視。無法在FMC上同時開啟兩個憑證。

通過FMC在Cisco FTD上配置SAML伺服器設定

要使用Firepower管理中心(FMC)配置Cisco Firepower威脅防禦(FTD)上的SAML伺服器設定，請執行以下步驟：

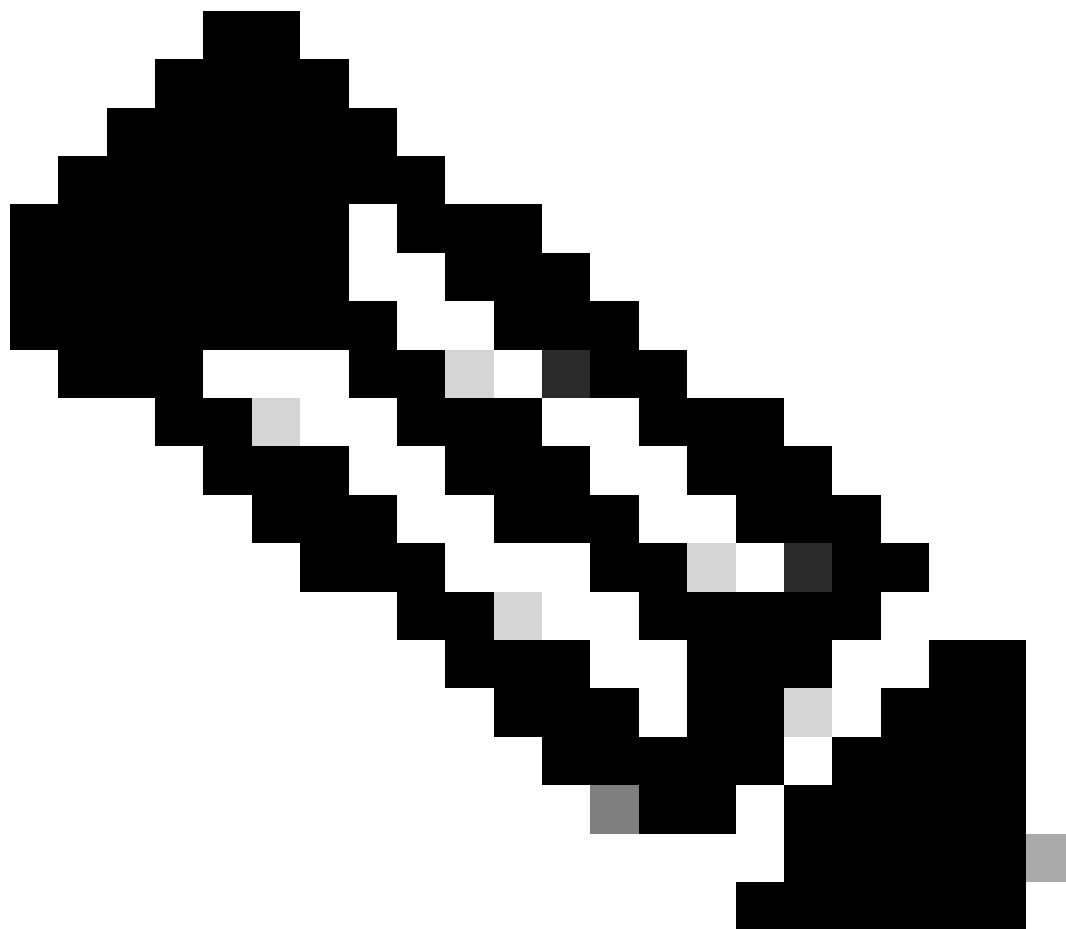
1. 導航至Single Sign-on Server Configuration:
 - 導航到Objects > Object Management > AAA Servers > Single Sign-on Server。
 - 按一下Add Single Sign-on Server開始配置新伺服器。
2. 配置SAML伺服器設定：
 - 使用從SAML企業應用程式或從身份提供程式(IdP)下載的metadata.xml檔案中收集的參數，在「New Single Sign-on Server」表單中填寫必要的SAML值。
 - 要配置的關鍵引數包括：
 - SAML提供程式實體ID:metadata.xml中的entityID
 - SSO URL:來自metadata.xml的SingleSignOnService。

- 註銷URL:來自metadata.xml的SingleLogoutService。
- 基本URL:FTD SSL ID證書的FQDN。
- 身份提供程式證書：IdP簽名證書。
 - 在Identity Provider Certificate部分下，附加其中一個已註冊的IdP證書
 - 在本使用情形中，我們使用來自FTD-SAML-1應用程式的IdP憑證。
- 服務提供商證書：FTD簽署憑證。

The screenshot displays the Cisco Firewall Management Center (FMC) interface. On the left, a navigation pane shows the 'Single Sign-on Server' configuration. The main area shows the 'Edit Single Sign-on Server' dialog box. The dialog box contains the following fields:

- Name***: FTD-SAML-Object
- Identity Provider Entity ID***: https://sts.windows.net/477a586b
- SSO URL***: https://login.microsoftonline.com/
- Logout URL**: https://login.microsoftonline.com/
- Base URL**: https://[redacted].cisco.com (highlighted with a green box)
- Identity Provider Certificate***: FTD-SAML-1-idp-cert (highlighted with a green box)
- Service Provider Certificate**: [redacted]2
- Request Signature**: --No Signature--
- Request Timeout**: Use the timeout set by the provide

At the bottom of the dialog box, there are 'Cancel' and 'Save' buttons. The background shows the FMC interface with a table of Single Sign-on Servers.



附註：在當前配置中，只能從連線配置檔案設定中的SAML對象覆蓋身份提供程式證書。遺憾的是，「登入時請求IDp重新身份驗證」和「僅在內部網路上啟用IDp可訪問」等功能無法針對每個連線配置檔案單獨啟用或禁用。

透過FMC在Cisco FTD上設定連線設定檔

要完成SAML身份驗證設定，您需要使用適當的引數配置連線配置檔案，並使用先前配置的SAML伺服器將AAA身份驗證設定為SAML。

如需更多詳細指導，請參閱思科檔案內「透過FMC在FTD上設定」下的第五步：[在通過FMC管理的FTD上配置具有SAML身份驗證的安全客戶端](#)。

Firewall Management Center
Devices / VPN / Edit Connection Profile

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⓘ ⚙️ ? admin ▾ **SECURE**

10.106.65.25_VPN Save Cancel

Enter Description [Policy Assignments \(1\)](#)

Local Realm: **None** Dynamic Access Policy: **None**

Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: <i>None</i> Authorization: <i>None</i> Accounting: <i>None</i>	DfltGrpPolicy	
EME_CERT_LOCAL_VPN	Authentication: <i>Kavin (RADIUS)</i> Authorization: <i>Kavin (RADIUS)</i> Accounting: <i>Kavin (RADIUS)</i>	LocalLAN	
FTD-SAML-1	Authentication: FTD-SAML-Object (SSO) Authorization: <i>None</i> Accounting: <i>None</i>	FTD-SAML-1-gp	
FTD-SAML-2	Authentication: FTD-SAML-Object (SSO) Authorization: <i>None</i> Accounting: <i>None</i>	FTD-SAML-2-gp	

提取第一個連線配置檔案的AAA配置

以下是第一個連線配置檔案的AAA配置設定的概述：

Firewall Management Center
Devices / VPN / Edit Connection Profile

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⓘ ⚙️ ? admin ▾ **SECURE**

10.106.65.25_VPN Save Cancel

Enter Description [Policy Assignments \(1\)](#)

Connection Profile Access Interfaces

Name

DefaultWEBVPNGroup

EME_CERT_LOCAL_VPN

FTD-SAML-1

FTD-SAML-2

Edit Connection Profile ⓘ

Connection Profile:*

Group Policy:* +

[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method:

Authentication Server: ⓘ

☐ Override Identity Provider Certificate

SAML Login Experience: ☒ VPN client embedded browser ⓘ ☐ Default OS Browser ⓘ

Authorization

Authorization Server:

☐ Allow connection only if user exists in authorization database

Accounting

Accounting Server:

▶ Advanced Settings

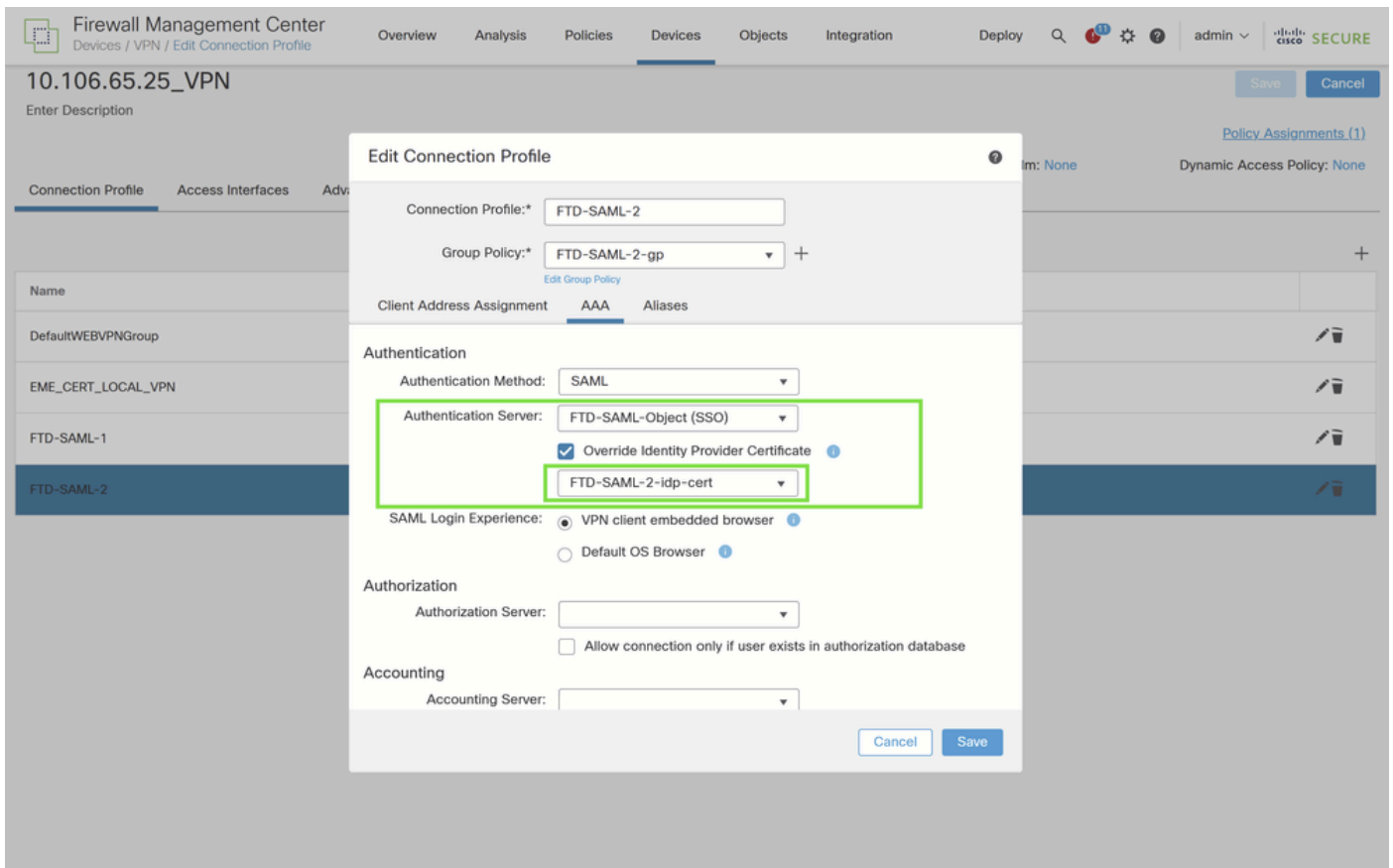
Cancel Save

在Cisco FTD上設定第二個連線設定檔的IdP憑證覆寫

要確保第二個連線配置檔案使用正確的身份提供程式(IdP)證書，請完成以下步驟以啟用IdP證書覆蓋：

在連線配置檔案設定中，找到並啟用選項「覆蓋身份提供程式證書」，以允許使用與SAML伺服器配置的IdP證書不同的證書。

從已註冊IdP證書清單中，選擇專門為FTD-SAML-2應用程式註冊的證書。該選擇可確保當對此連線配置檔案發出身份驗證請求時，使用正確的IdP證書。



配置部署

導覽至Deploy > Deployment並選擇適當的FTD以套用SAML驗證VPN變更。

驗證

FTD指令行上的組態

<#root>

```
firepower# sh run webvpn
webvpn
  enable outside
  http-headers
    hsts-server
      enable
      max-age 31536000
      include-sub-domains
      no preload
    hsts-client
      enable
  x-content-type-options
```

```
x-xss-protection
content-security-policy
Secure Client image disk0:/csm/Secure Client-win-4.10.08025-webdeploy.pkg 1 regex "Windows"
Secure Client enable
```

```
saml idp https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/
```

```
url sign-in https://login.microsoftonline.com/477a586b-61c2-4c8e-9a41-1634016aa513/saml2
```

```
url sign-out https://login.microsoftonline.com/477a586b-61c2-4c8e-9a41-1634016aa513/saml2
```

```
base-url https://nigarapa2.cisco.com
```

```
trustpoint idp FTD-SAML-1-idp-cert
```

```
trustpoint sp nigarapa2
```

```
no signature
```

```
force re-authentication
```

```
tunnel-group-list enable
cache
  disable
error-recovery disable
firepower#
```

```
<#root>
```

```
firepower# sh run tunnel-group FTD-SAML-1
tunnel-group FTD-SAML-1 type remote-access
tunnel-group FTD-SAML-1 general-attributes
  address-pool secure-client-pool
  default-group-policy FTD-SAML-1-gp
tunnel-group FTD-SAML-1 webvpn-attributes
  authentication saml
  group-alias FTD-SAML-1 enable
```

```
saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/
```

```
firepower#
```

```
<#root>
```

```
firepower# sh run tunnel-group FTD-SAML-2
tunnel-group FTD-SAML-2 type remote-access
tunnel-group FTD-SAML-2 general-attributes
    address-pool secure-client-pool
    default-group-policy FTD-SAML-2-gp
tunnel-group FTD-SAML-2 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-2 enable

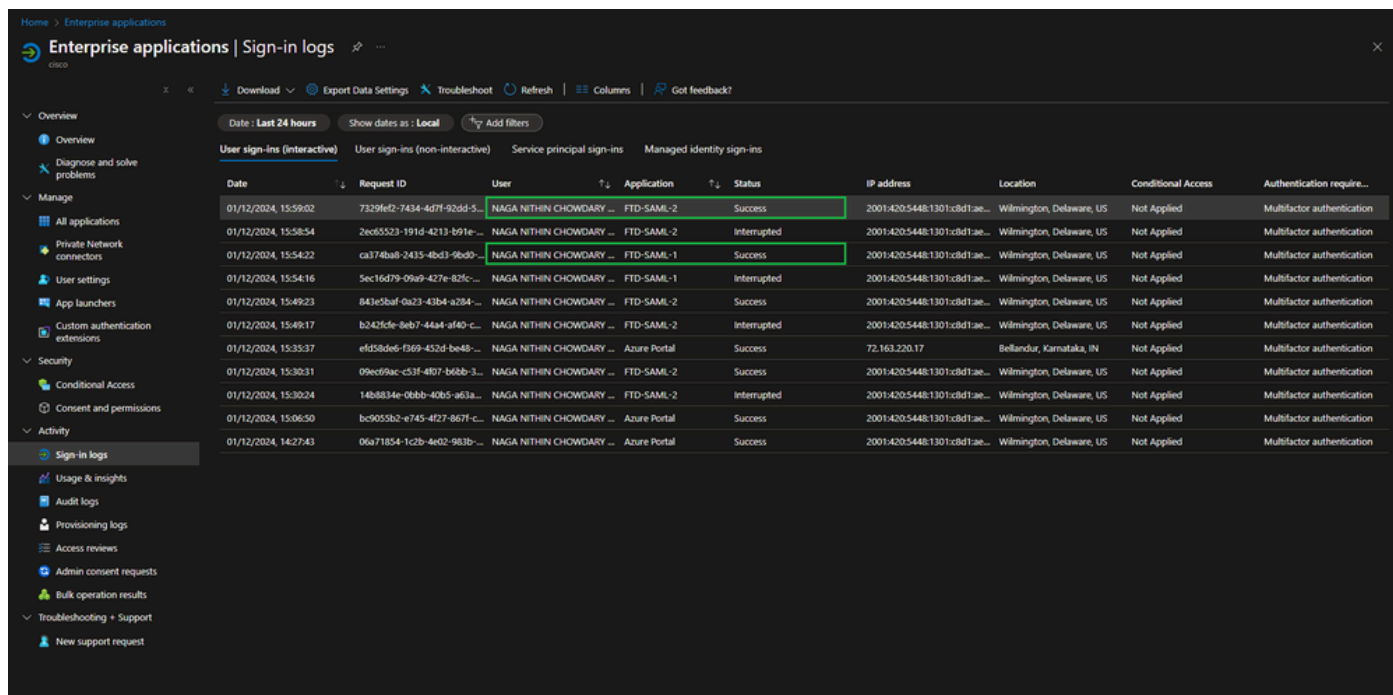
saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/

saml idp-trustpoint FTD-SAML-2-idp-cert
```

firepower#

從Azure entra識別符號登入日誌

訪問企業應用程式下的登入日誌部分。查詢與特定連線配置檔案(如FTD-SAML-1和FTD-SAML-2)相關的身份驗證請求。驗證使用者是否通過與每個連線配置檔案關聯的SAML應用程式成功進行身份驗證。



Enterprise applications Sign-in logs										
Date: Last 24 hours Show dates as: Local Add filters										
User sign-ins (interactive) User sign-ins (non-interactive) Service principal sign-ins Managed identity sign-ins										
	Date	Request ID	User	Application	Status	IP address	Location	Conditional Access	Authentication require...	
	01/12/2024, 15:59:02	7329fe2-7434-4d7f-92dd-5...	NAGANITHIN CHOWDARY ...	FTD-SAML-2	Success	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	
	01/12/2024, 15:58:54	2ec65523-191d-4213-b91e-...	NAGANITHIN CHOWDARY ...	FTD-SAML-2	Interrupted	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	
	01/12/2024, 15:54:22	ca374ba8-2435-4bd3-9bd9-...	NAGANITHIN CHOWDARY ...	FTD-SAML-1	Success	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	
	01/12/2024, 15:54:16	Sec16d79-09a9-427e-82fc-...	NAGANITHIN CHOWDARY ...	FTD-SAML-1	Interrupted	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	
	01/12/2024, 15:49:23	841e5baf-0a23-43b4-a284-...	NAGANITHIN CHOWDARY ...	FTD-SAML-2	Success	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	
	01/12/2024, 15:49:17	b342f5fe-bab7-44a4-af40-c...	NAGANITHIN CHOWDARY ...	FTD-SAML-2	Interrupted	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	
	01/12/2024, 15:35:37	efd58de6-fb69-452d-be48-...	NAGANITHIN CHOWDARY ...	Azure Portal	Success	72.163.220.17	Bellandur, Karnataka, IN	Not Applied	Multifactor authentication	
	01/12/2024, 15:30:31	09ecd9ac-c53f-4807-b6bb-3...	NAGANITHIN CHOWDARY ...	FTD-SAML-2	Success	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	
	01/12/2024, 15:30:24	14b8834e-0bbb-40b5-a61a-...	NAGANITHIN CHOWDARY ...	FTD-SAML-2	Interrupted	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	
	01/12/2024, 15:06:50	bc9055b2-e745-4f27-867f-c...	NAGANITHIN CHOWDARY ...	Azure Portal	Success	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	
	01/12/2024, 14:27:43	06a71854-1c2b-4e02-983b-...	NAGANITHIN CHOWDARY ...	Azure Portal	Success	2001:420:5448:1301:cbd1:ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication	

Azure IdP上的登入日誌

疑難排解

1. 您可以從安全客戶端使用者PC使用DART進行故障排除。
2. 要排除SAML身份驗證問題，請利用以下調試：

<#root>

firepower#


```
debug webvpn saml 255
```

3. 按照上述說明驗證安全客戶端配置；此命令可用於檢查證書。

```
<#root>
```

```
firepower#
```

```
show crypto ca certificate
```

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）。