

Configurazione dell'autenticazione SAML per più profili di connessione RAVPN su FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazioni](#)

[Panoramica della configurazione:](#)

[Configurazione](#)

[Configurazione in Azure IdP](#)

[Configurazione sul FTD tramite FMC](#)

[Verifica](#)

[Configurazione sulla riga di comando FTD](#)

[Registri di accesso da identificatore entra di Azure](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta l'autenticazione SAML con il provider di identità di Azure per più profili di connessione su FTD Cisco gestito da FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione client sicura su Next-Generation Firewall (NGFW) gestito da Firepower Management Center (FMC)
- Valori SAML e metatada.xml

Componenti usati

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

- Firepower Threat Defense (FTD) versione 7.4.0
- FMC versione 7.4.0
- ID di Azure Microsoft Entra con SAML 2.0

- Cisco Secure Client 5.1.7.80

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

Premesse

Questa configurazione consente a FTD di autenticare gli utenti client sicuri utilizzando due diverse applicazioni SAML nell'idp di Azure con un singolo oggetto SAML configurato in FMC.

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]..

In un ambiente Microsoft Azure, più applicazioni possono condividere lo stesso ID entità. Ogni applicazione, in genere mappata a un gruppo di tunnel diverso, richiede un certificato univoco, che richiede la configurazione di più certificati all'interno della configurazione IdP del lato FTD in un singolo oggetto IdP SAML. Tuttavia, Cisco FTD non supporta la configurazione di più certificati in un oggetto SAML IdP, come descritto nell'ID bug Cisco [CSCvi29084](#).

Per superare questo limite, Cisco ha introdotto la funzione di sostituzione del certificato IdP, disponibile dalla versione 7.1.0 di FTD e dalla versione 9.17.1 di ASA. Questo miglioramento offre una soluzione permanente al problema e integra le soluzioni esistenti descritte nel report del bug.

Configurazioni

In questa sezione viene descritto il processo di configurazione dell'autenticazione SAML con Azure come provider di identità (IdP) per più profili di connessione su Cisco Firepower Threat Defense (FTD) gestiti da Firepower Management Center (FMC). La funzionalità di sostituzione del certificato IdP viene utilizzata per impostare questa opzione in modo efficace.

Panoramica della configurazione:

Sull'FTD Cisco devono essere configurati due profili di connessione:

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

In questo esempio di configurazione, l'URL del gateway VPN (Cisco Secure Client FQDN) è impostato su nigarapa2.cisco.com

Configurazione

Configurazione in Azure IdP

Per configurare in modo efficace le applicazioni SAML enterprise per Cisco Secure Client,

verificare che tutti i parametri siano impostati correttamente per ogni gruppo di tunnel eseguendo i seguenti passaggi:

Accedere alle applicazioni SAML Enterprise:

Passare alla console di amministrazione del provider SAML in cui sono elencate le applicazioni enterprise.

Selezionare l'applicazione SAML appropriata:

Identificare e selezionare le applicazioni SAML corrispondenti ai gruppi di tunnel Cisco Secure Client che si desidera configurare.

Configurare l'identificatore (ID entità):

Impostare l'identificatore (ID entità) per ogni applicazione. Deve essere l'URL di base, ossia il nome di dominio completo (FQDN) di Cisco Secure Client.

Impostare l'URL di risposta (URL servizio consumer asserzione):

Configurare l'URL di risposta (URL del servizio consumer di asserzione) utilizzando l'URL di base corretto. Verificare che sia allineato all'FQDN di Cisco Secure Client.

Aggiungere il profilo di connessione o il nome del gruppo di tunnel all'URL di base per garantire la specificità.

Verifica della configurazione:

Verificare che tutti gli URL e i parametri siano stati immessi correttamente e corrispondano ai rispettivi gruppi di tunnel.

Salvare le modifiche e, se possibile, eseguire un test di autenticazione per verificare che la configurazione funzioni come previsto.

Per ulteriori informazioni, fare riferimento a "Add Cisco Secure Client from the Microsoft App Gallery" (Aggiungi Cisco Secure Client dalla Microsoft App Gallery) nella documentazione di Cisco: [Configurazione della VPN client sicura ASA con Microsoft Azure MFA tramite SAML](#)

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 support OpenID Connect.

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

1

Basic SAML Configuration

Identifier (Entity ID)	https://[redacted].cisco.com/saml/sp
Reply URL (Assertion Consumer Service URL)	https://[redacted].cisco.com/+CSCOE+/me=FTD-SAML-1
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	3125987754C687CCBE86DD214BD
Expiration	25/11/2027, 18:23:11
Notification Email	[redacted]

FTD-SAML-1 | 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	3125987754C687CCBE86DD214BD
Expiration	25/11/2027, 18:23:11
Notification Email	[redacted]

App Federation Metadata URL [https://login.microsoftonline.com/\[redacted\]](https://login.microsoftonline.com/[redacted])[Certificate \(Base64\)](#) [Download](#)[Certificate \(Raw\)](#) [Download](#)[Federation Metadata XML](#) [Download](#)

Verification certificates (optional)

Required	No
Active	0
Expired	0

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/\[redacted\]](https://login.microsoftonline.com/[redacted])Microsoft Entra Identifier [https://sts.windows.net/477a586b-\[redacted\]](https://sts.windows.net/477a586b-[redacted])Logout URL [https://login.microsoftonline.com/\[redacted\]](https://login.microsoftonline.com/[redacted])

5

Test single sign-on with FTD-SAML-1

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

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	3125987754C687CCBE86DD214BDA5E0A13C211B	...

Signing Option

Sign SAML assertion

Signing Algorithm

SHA-256

Notification Email Addresses

[redacted]

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

Home > cisco | Devices > Enterprise applications | All applications > 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://cisco.com/saml/sp/metadata/FTD-SAML-2
Reply URL (Assertion Consumer Service URL)	https://cisco.com/+CSCOE+/saml/sp/metadata/TGTGroup
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	F1CF8A1B07E704EE793A7132AF04...
Thumbprint	27/11/2027, 02:33:11
Expiration	

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.

[Add identifier](#)

Default

<https://cisco.com/saml/sp/metadata/FTD-SAML-2> ☒ ☐ [Delete](#)

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.

[Add reply URL](#)

Index Default

<https://cisco.com/+CSCOE+/saml/sp/acs?tgname=FTD-SAML-2> ☒ ☐ ☒ ☐ [Delete](#)

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.

☒

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.

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-2

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

Enterprise Application

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

Unique User Identifier: user.userprincipalname

SAML Certificates

Token signing certificate

Status	Active
Thumbprint	F1CF8A1B07E704EE793A7132AF04...
Expiration	27/11/2027, 02:33:11
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-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

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

Verificare di disporre delle informazioni e dei file necessari per configurare l'autenticazione SAML con Microsoft Entra come provider di identità:

Individuare il codice identificativo Microsoft Entra:

Accedere alle impostazioni di entrambe le applicazioni SAML enterprise all'interno del portale Microsoft Entra.

Si noti l'identificatore Microsoft Entra, che rimane coerente in entrambe le applicazioni ed è fondamentale per la configurazione SAML.

Scarica certificati IdP Base64:

Passare a ciascuna applicazione SAML enterprise configurata.

Scaricare i rispettivi certificati IdP con codifica Base64. Questi certificati sono essenziali per stabilire la fiducia tra il provider di identità e la configurazione della VPN Cisco.



Nota: Tutte queste configurazioni SAML necessarie per i profili di connessione FTD possono anche essere originate dai file metadata.xml forniti dal provider di identità per le rispettive applicazioni.



Nota: Per utilizzare un certificato IdP personalizzato, è necessario caricare il certificato IdP generato in modo personalizzato sia in IdP che in FMC. Per Azure IdP, verificare che il certificato sia nel formato PKCS#12. Nel CCP, caricare solo il certificato di identità dall'IdP, non il file PKCS#12. Per istruzioni dettagliate, fare riferimento alla sezione "Upload the PKCS#12 File on Azure and FDM" nella documentazione di Cisco:

[Configurazione di più profili RAVPN con autenticazione SAML in FDM](#)

Configurazione sul FTD tramite FMC

Registra certificati IdP:

Passare alla sezione Gestione certificati in FMC e registrare i certificati IdP con codifica Base64 scaricati per entrambe le applicazioni SAML. Questi certificati sono fondamentali per stabilire la fiducia e abilitare l'autenticazione SAML.

Per istruzioni dettagliate, fare riferimento alle prime due fasi in "Configurazione sull'FTD tramite FMC" nella documentazione Cisco disponibile all'indirizzo: [Configurare Secure Client con](#)

[autenticazione SAML su FTD Gestito tramite FMC.](#)

Firewall Management Center

Devices / Certificates

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

Filter

All Certificates

Add

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status	
> [Redacted] 1						
> [Redacted]						
✓ 10.106.65.25						
[Redacted] 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 : 208f94f0831ede99490c7c64dda7bee8
- 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 : 2758279b3b5cc98044c603999068ee61
- 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



Nota: L'immagine è stata modificata in modo da visualizzare entrambi i certificati contemporaneamente per una migliore visualizzazione. Non è possibile aprire entrambi i certificati contemporaneamente nel CCP.

Configurazione delle impostazioni del server SAML su Cisco FTD tramite FMC

Per configurare le impostazioni del server SAML su Cisco Firepower Threat Defense (FTD) tramite Firepower Management Center (FMC), implementare i seguenti passaggi:

1. Passare alla configurazione del server Single Sign-on:
 - Passare a Oggetti > Gestione oggetti > Server AAA > Server Single Sign-On.
 - Fare clic su Aggiungi server Single Sign-on per avviare la configurazione di un nuovo server.
2. Configurare le impostazioni del server SAML:
 - Utilizzando i parametri raccolti dalle applicazioni SAML enterprise o dal file metadata.xml scaricato dal provider di identità (IdP), immettere i valori SAML necessari nel modulo Nuovo server Single Sign-on.

- I parametri chiave da configurare includono:
 - ID entità provider SAML: entityID da metadata.xml
 - URL SSO: SingleSignOnService da metadata.xml.
 - URL di disconnessione: SingleLogoutService da metadata.xml.
 - URL DI BASE: FQDN del certificato ID SSL FTD.
 - Certificato provider di identità: Certificato di firma IdP.
 - Nella sezione Certificato provider di identità allegare uno dei certificati IdP registrati
 - In questo caso, utilizziamo il certificato IdP dell'applicazione FTD-SAML-1.
 - Certificato provider di servizi: Certificato di firma FTD.

The screenshot displays the Cisco Firewall Management Center (FWMC) interface. The left sidebar shows the navigation menu with categories like AAA Server, RADIUS Server Group, and Single Sign-on Server. The main content area is titled 'Single Sign-on' and shows a list of servers. A modal window titled 'Edit Single Sign-on Server' is open, showing the configuration for a server named 'FTD-SAML-Object'. The configuration fields include:

- 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
- Identity Provider Certificate*: FTD-SAML-1-idp-cert
- Service Provider Certificate: [redacted]2
- Request Signature: --No Signature--
- Request Timeout: Use the timeout set by the provide

The 'Add Single Sign-on Server' button is highlighted in green in the top right of the modal. The bottom of the screen shows a pagination bar indicating 'Displaying 1 - 2 of 2 rows' and 'Page 1 of 1'.



Nota: Nella configurazione corrente, solo il certificato del provider di identità può essere sostituito dall'oggetto SAML nelle impostazioni del profilo di connessione. Purtroppo, funzionalità quali "Richiesta di riautenticazione IdP all'accesso" e "Abilita IdP accessibile solo sulla rete interna" non possono essere abilitate o disabilitate singolarmente per ciascun profilo di connessione.

Configurazione dei profili di connessione su Cisco FTD tramite FMC

Per completare la configurazione dell'autenticazione SAML, è necessario configurare i profili di connessione con i parametri appropriati e impostare l'autenticazione AAA su SAML utilizzando il server SAML configurato in precedenza.

Per istruzioni più dettagliate, fare riferimento alla quinta fase in "Configurazione sull'FTD tramite FMC" nella documentazione di Cisco: [Configurare Secure Client con autenticazione SAML su FTD Gestito tramite FMC](#).

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	

Estratto della configurazione AAA per il primo profilo di connessione

Di seguito è riportata una panoramica delle impostazioni di configurazione AAA per il primo profilo di connessione:

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

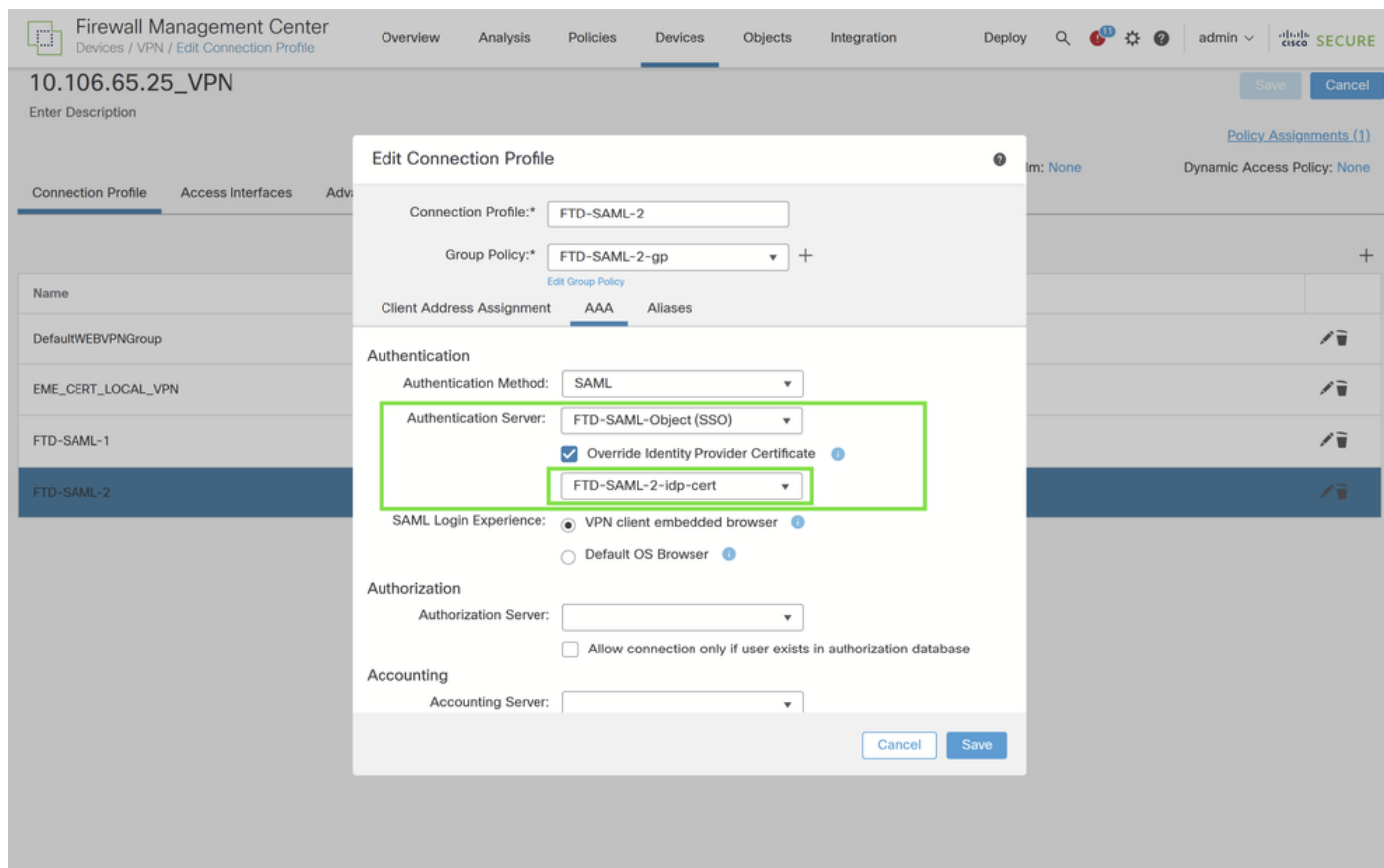
Cancel Save

Configurazione dell'override del certificato IdP per il secondo profilo di connessione su Cisco FTD
Per assicurarsi che venga utilizzato il certificato del provider di identità (IdP) corretto per il secondo profilo di connessione, abilitare la sostituzione del certificato del provider di identità

eseguendo i passaggi seguenti:

Nelle impostazioni del profilo di connessione, individuare e abilitare l'opzione "Ignora certificato provider di identità" per consentire l'utilizzo di un certificato IdP diverso da quello configurato per il server SAML.

Dall'elenco dei certificati IdP registrati, selezionare il certificato specificamente registrato per l'applicazione FTD-SAML-2. Questa opzione garantisce che, quando viene effettuata una richiesta di autenticazione per questo profilo di connessione, venga utilizzato il certificato IdP corretto.



Distribuzione della configurazione

Individuare **Deploy > Deployment** e selezionare l'FTD appropriato per applicare le modifiche alla VPN di autenticazione SAML.

Verifica

Configurazione sulla riga di comando FTD

<#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 sam1
    group-alias FTD-SAML-2 enable

sam1 identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/

sam1 idp-trustpoint FTD-SAML-2-idp-cert
```

firepower#

Registri di accesso da identificatore entra di Azure

Accedere alla sezione Log di accesso in applicazione enterprise. Cercare le richieste di autenticazione relative ai profili di connessione specifici, ad esempio FTD-SAML-1 e FTD-SAML-2. Verificare che l'autenticazione venga eseguita correttamente tramite le applicazioni SAML associate a ogni profilo di connessione.

Home > Enterprise applications

Enterprise applications | Sign-in logs

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

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

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Admin consent requests

Bulk operation results

Troubleshooting + Support

New support request

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...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Success	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:58:54	2e065523-191d-4213-b91e-...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Interrupted	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:54:22	ca374ba8-2435-4bd3-9bd0-...	NAGA NITHIN CHOWDARY ...	FTD-SAML-1	Success	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:54:16	5ec16d79-09a9-427e-82fc-...	NAGA NITHIN CHOWDARY ...	FTD-SAML-1	Interrupted	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:49:23	843e5baf-0a23-43b4-a284-...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Success	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:49:17	b242fde-8eb7-44a4-af40-c...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Interrupted	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:35:37	efd58de6-f369-452d-be48-...	NAGA NITHIN CHOWDARY ...	Azure Portal	Success	72.163.220.17	Bellandur, Karnataka, IN	Not Applied	Multifactor authentication
01/12/2024, 15:30:31	09ec99ac-c53f-4807-b6bb-3...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Success	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:30:24	14b8834e-0bbb-40b5-a61a-...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Interrupted	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:06:50	bc9053b2-e745-4f27-867f-c...	NAGA NITHIN CHOWDARY ...	Azure Portal	Success	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 14:27:43	06a71854-1c2b-4602-983b-...	NAGA NITHIN CHOWDARY ...	Azure Portal	Success	2001:420:5448:1301:cbd1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication

Accedi a Azure IdP

Risoluzione dei problemi

1. È possibile risolvere i problemi relativi all'utilizzo di DART dal PC utente Secure Client.
2. Per risolvere un problema di autenticazione SAML, utilizzare questo comando di debug:

```
<#root>
```

```
firepower#
```

```
debug webvpn saml 255
```

3. Verificare la configurazione di Secure Client come spiegato in precedenza; questo comando può essere utilizzato per controllare il certificato.

```
<#root>
```

```
firepower#
```

```
show crypto ca certificate
```

Informazioni su questa traduzione

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