

Configuración de SAML Auth para Múltiples Perfiles de Conexión RAVPN en FTD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuraciones](#)

[Información general sobre configuración:](#)

[Configurar](#)

[Configuración en Azure IdP](#)

[Configuración en el FTD a través de FMC](#)

[Verificación](#)

[Configuración en la línea de comandos de FTD](#)

[Registros de inicio de sesión desde el identificador de entra de Azure](#)

[Troubleshoot](#)

Introducción

Este documento describe la autenticación SAML con el proveedor de identidad de Azure para múltiples perfiles de conexión en Cisco FTD administrado por FMC.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Configuración de cliente seguro en firewall de última generación (NGFW) gestionado por Firepower Management Center (FMC)
- Valores SAML y metatada.xml

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firepower Threat Defence (FTD) versión 7.4.0
- FMC versión 7.4.0
- Azure Microsoft Entra ID with SAML 2.0

- Cisco Secure Client 5.1.7.80

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Esta configuración permite a FTD autenticar a usuarios de cliente seguro usando dos aplicaciones SAML diferentes en Azure idp con un solo objeto SAML configurado en 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]..

En un entorno de Microsoft Azure, varias aplicaciones pueden compartir el mismo Id. de entidad. Cada aplicación, asignada normalmente a un grupo de túnel diferente, necesita un certificado único, lo que requiere la configuración de varios certificados dentro de la configuración IdP del lado FTD bajo un único objeto IdP SAML. Sin embargo, Cisco FTD no soporta la configuración de múltiples certificados bajo un objeto SAML IdP, como se detalla en Cisco bug ID [CSCvi29084](#).

Para superar esta limitación, Cisco ha introducido la función de anulación del certificado IdP, disponible desde la versión 7.1.0 de FTD y la versión 9.17.1 de ASA. Esta mejora ofrece una solución permanente al problema y complementa las soluciones temporales existentes descritas en el informe de errores.

Configuraciones

Esta sección describe el proceso para configurar la autenticación SAML con Azure como proveedor de identidad (IdP) para varios perfiles de conexión en Cisco Firepower Threat Defense (FTD) administrado por Firepower Management Center (FMC). La función de invalidación del certificado IdP se utiliza para configurar esto de manera efectiva.

Información general sobre configuración:

Se deben configurar dos perfiles de conexión en Cisco FTD:

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

En este ejemplo de configuración, la URL de gateway VPN (FQDN de Cisco Secure Client) se establece en nigarapa2.cisco.com

Configurar

Configuración en Azure IdP

Para configurar sus aplicaciones empresariales SAML para Cisco Secure Client de manera eficaz, asegúrese de que todos los parámetros estén configurados correctamente para cada grupo de túnel siguiendo estos pasos:

Acceso a aplicaciones empresariales de SAML:

Navegue hasta la consola administrativa de su proveedor SAML donde se enumeran sus aplicaciones empresariales.

Seleccione la aplicación SAML adecuada:

Identifique y seleccione las aplicaciones SAML correspondientes a los grupos de túnel de Cisco Secure Client que pretende configurar.

Configure el identificador (Id. de entidad):

Establezca el identificador (Id. de entidad) para cada aplicación. Debe ser la URL base, que es el nombre de dominio completamente calificado (FQDN) de Cisco Secure Client.

Establezca la URL de respuesta (URL de servicio de consumidor de aserción):

Configure la URL de respuesta (URL de servicio de consumidor de aserción) con la URL base correcta. Asegúrese de que esté alineado con el FQDN de Cisco Secure Client.

Agregue el nombre del grupo de túnel o perfil de conexión a la URL base para garantizar la especificidad.

Verifique la configuración:

Verifique que todas las URL y los parámetros se hayan ingresado correctamente y que correspondan a los grupos de túnel respectivos.

Guarde los cambios y, si es posible, realice una autenticación de prueba para asegurarse de que la configuración funciona según lo previsto.

Para obtener una guía más detallada, consulte "Agregar Cisco Secure Client desde la Galería de aplicaciones de Microsoft" en la documentación de Cisco: [Configuración de ASA Secure Client VPN con Microsoft Azure MFA a través de 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]

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

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.

Index

Default

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](#)

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]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

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

5

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

Ahora asegúrese de que tiene la información y los archivos necesarios para configurar la autenticación SAML con Microsoft Entra como su proveedor de identidad:

Busque el identificador de Microsoft Entra:

Acceda a la configuración de ambas aplicaciones empresariales SAML dentro del portal Microsoft Entry.

Tenga en cuenta el Microsoft Entra Identifier, que sigue siendo uniforme en ambas aplicaciones y es crucial para su configuración SAML.

Descargar certificados de IdP Base64:

Desplácese hasta cada aplicación empresarial SAML configurada.

Descargue los respectivos certificados IdP codificados en Base64. Estos certificados son esenciales para establecer la confianza entre su proveedor de identidad y su configuración de Cisco VPN.



Nota: Todas estas configuraciones SAML requeridas para los perfiles de conexión FTD también se pueden obtener de los archivos metadata.xml provistos por su IdP para las respectivas aplicaciones.



Nota: Para utilizar un certificado de IdP personalizado, debe cargar el certificado de IdP generado personalizado tanto en el IdP como en el FMC. Para Azure IdP, asegúrese de que el certificado esté en formato PKCS#12. En el FMC, cargue sólo el certificado de identidad del IdP, no el archivo PKCS#12. Para obtener instrucciones detalladas, consulte la sección "Cargar el archivo PKCS#12 en Azure y FDM" en la documentación de Cisco: [Configuración de varios perfiles RAVPN con autenticación SAML en FDM](#)

Configuración en el FTD a través de FMC

Inscribir certificados IdP:

Navegue hasta la sección de administración de certificados dentro de FMC e inscriba los certificados de IdP con codificación Base64 descargados para ambas aplicaciones SAML. Estos certificados son vitales para establecer la confianza y habilitar la autenticación SAML.

Para obtener información detallada, consulte los dos primeros pasos de "Configuración en el FTD mediante FMC" en la documentación de Cisco disponible en: [Configure el Cliente Seguro con](#)

Autenticación SAML en FTD Administrado a través de 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	
> 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

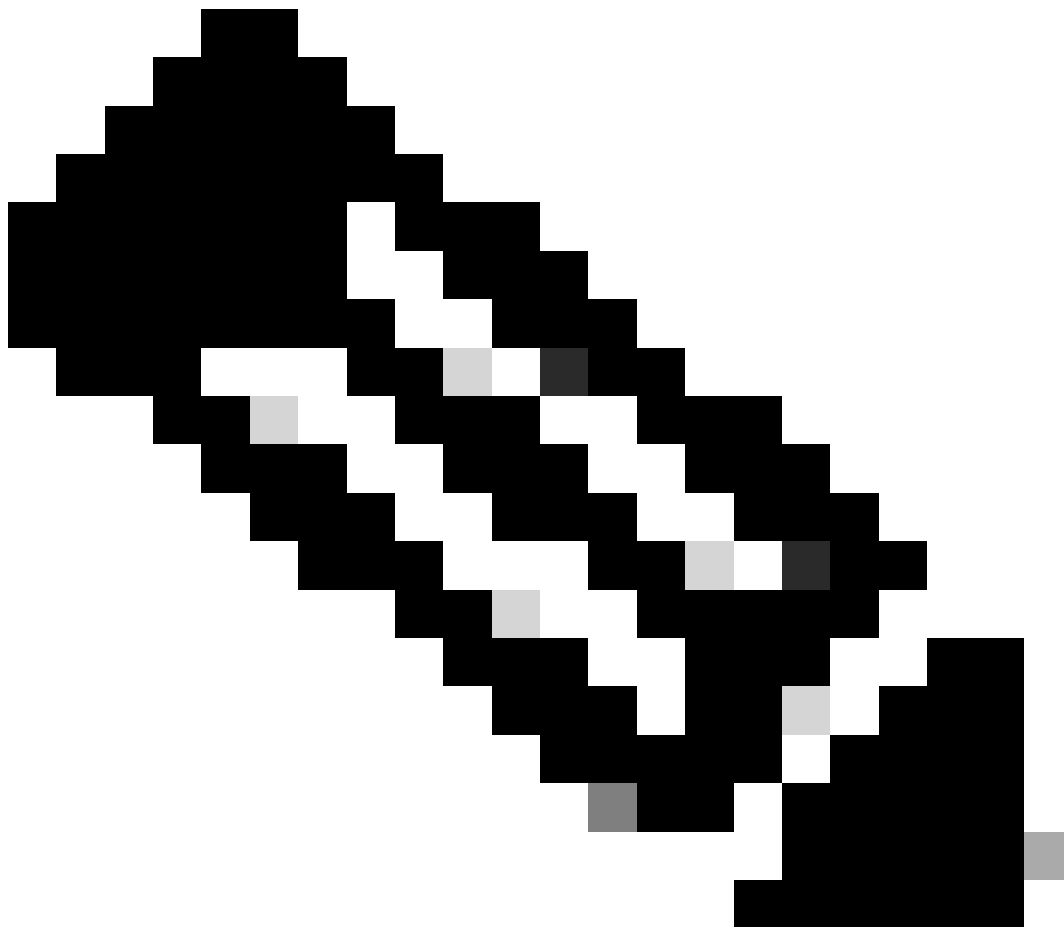
- Status : Available
- Serial Number : 20894f0831ede99490c7c64dda7bee8
- Issued By : CN : Microsoft Azure Federated SSO Certificate
- Issued To : CN : Microsoft Azure Federated SSO Certificate
- Public Key Type : RSA (2048 bits)
- Signature Algorithm : RSA-SHA256
- Associated Trustpoints : FTD-SAML-1-ldp-cert
- 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: La imagen se ha editado para mostrar ambos certificados simultáneamente para una mejor visualización. No es posible abrir ambos certificados al mismo tiempo en FMC.

Configuración de los parámetros del servidor SAML en Cisco FTD mediante FMC

Para configurar los parámetros del servidor SAML en Cisco Firepower Threat Defense (FTD) mediante Firepower Management Center (FMC), implemente estos pasos:

1. Vaya a Configuración del servidor de Single Sign-on:

- Vaya a Objetos > Administración de objetos > Servidores AAA > Servidor de Single Sign-on.
- Haga clic en Add Single Sign-on Server para comenzar a configurar un nuevo servidor.

2. Configuración de los parámetros del servidor SAML:

- Con los parámetros recopilados de sus aplicaciones empresariales SAML o del archivo metadata.xml descargado de su Identity Provider (IdP), rellene los valores SAML necesarios en el formulario New Single Sign-on Server.
- Entre los parámetros clave que se deben configurar se incluyen:

- ID de entidad del proveedor SAML: entityID de metadata.xml
- URL DE SSO: SingleSignOnService de metadata.xml.
- URL de cierre de sesión: SingleLogoutService de metadata.xml.
- URL BASE: FQDN del certificado de ID SSL de FTD.
- Certificado del proveedor de identidad: Certificado de firma IdP.
 - En la sección Certificado del Proveedor de Identidad, adjunte uno de los certificados de IdP inscritos
 - Para este caso de uso, estamos utilizando el certificado IdP de la aplicación FTD-SAML-1.
- Certificado de proveedor de servicios: Certificado de firma de FTD.

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The left sidebar shows the navigation menu with categories like AAA Server, RADIUS Server Group, Single Sign-on Server, Access List, Address Pools, Application Filters, AS Path, BFD Template, Cipher Suite List, Community List, DHCP IPv6 Pool, Distinguished Name, DNS Server Group, External Attributes, File List, FlexConfig, Geolocation, Interface, Key Chain, Network, PKI, Policy List, Port, Prefix List, Route Map, Security Intelligence, and Sinkhole. The main panel shows the 'Single Sign-on' configuration page. A modal dialog titled 'Edit Single Sign-on Server' is open, allowing configuration for a specific server. The dialog includes 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 are 'Cancel' and 'Save' buttons. The background interface shows a table of single sign-on servers with columns for Name, Identity Provider Entity ID, SSO URL, Logout URL, Base URL, Identity Provider Certificate, Service Provider Certificate, Request Signature, and Request Timeout. The table currently displays two rows: 'Azure-SAML-SSO' and 'FTD-SAML-Object'. The 'FTD-SAML-Object' row is selected. The bottom status bar indicates 'Displaying 1 - 2 of 2 rows' and 'Page 1 of 1'.



Nota: En la configuración actual, sólo el certificado del proveedor de identidad se puede reemplazar del objeto SAML dentro de la configuración del perfil de conexión. Desafortunadamente, funciones como "Solicitar reautenticación de IdP al iniciar sesión" y "Habilitar IdP solo accesible en la red interna" no se pueden habilitar o deshabilitar individualmente para cada perfil de conexión.

Configuración de perfiles de conexión en Cisco FTD mediante FMC

Para finalizar la configuración de la autenticación SAML, debe configurar los perfiles de conexión con los parámetros adecuados y establecer la autenticación AAA en SAML mediante el servidor SAML previamente configurado.

Para obtener una guía más detallada, consulte el quinto paso en "Configuración en el FTD a través de FMC" en la documentación de Cisco: [Configure el Cliente Seguro con Autenticación SAML en FTD Administrado a través de FMC](#).

Firewall Management Center
Devices / VPN / Edit Connection Profile

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 11 ⚙️ ? admin | cisco **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	🗑️

Extracto de la Configuración AAA para el Primer Perfil de Conexión

A continuación se muestra una descripción general de las opciones de configuración AAA para el primer perfil de conexión:

Firewall Management Center
Devices / VPN / Edit Connection Profile

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 11 ⚙️ ? admin | cisco **SECURE**

10.106.65.25_VPN Save Cancel

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

Connection Profile Access Interfaces Advanced

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

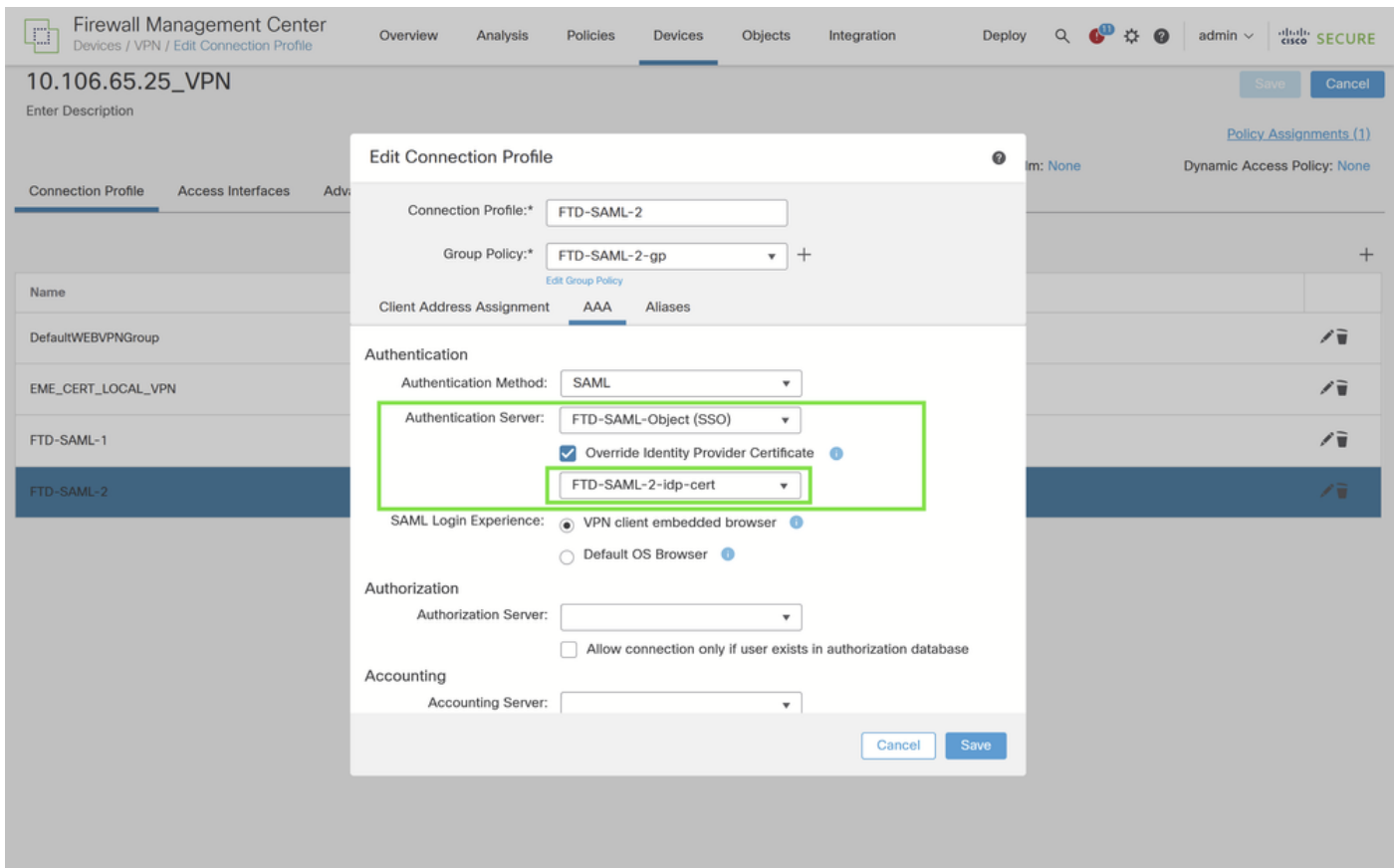
Configuración de la Anulación del Certificado IdP para el Segundo Perfil de Conexión en Cisco FTD

Para asegurarse de que se utiliza el certificado del proveedor de identidad (IdP) correcto para el

segundo perfil de conexión, habilite la anulación del certificado IdP siguiendo estos pasos:

Dentro de la configuración del perfil de conexión, localice y habilite la opción "Override Identity Provider Certificate" (Anular certificado de proveedor de identidad) para permitir el uso de un certificado de IdP diferente al configurado para el servidor SAML.

En la lista de certificados de IdP inscritos, seleccione el certificado inscrito específicamente para la aplicación FTD-SAML-2. Esta selección asegura que cuando se realiza una solicitud de autenticación para este perfil de conexión, se utiliza el certificado IdP correcto.



Implementación de la configuración

Navegue **Deploy > Deployment** hasta el FTD correcto y selecciónelo para aplicar los cambios de VPN de autenticación SAML.

Verificación

Configuración en la línea de comandos de 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 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#

Registros de inicio de sesión desde el identificador de entra de Azure

Acceda a la sección Registros de inicio de sesión en aplicación empresarial. Busque solicitudes de autenticación relacionadas con los perfiles de conexión específicos, como FTD-SAML-1 y FTD-SAML-2. Compruebe que los usuarios se están autenticando correctamente a través de las aplicaciones SAML asociadas a cada perfil de conexión.

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	73291e2-7434-4d7f-92dd-5...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Success	2001:420:5448:1301:c8d1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:58:54	2e065523-1914-4213-b91e-...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Interrupted	2001:420:5448:1301:c8d1ae...	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:c8d1ae...	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:c8d1ae...	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:c8d1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication
01/12/2024, 15:49:17	b242f5fe-8eb7-44a4-af40-c...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Interrupted	2001:420:5448:1301:c8d1ae...	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-4b07-b6bb-3...	NAGA NITHIN CHOWDARY ...	FTD-SAML-2	Success	2001:420:5448:1301:c8d1ae...	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:c8d1ae...	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:c8d1ae...	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:c8d1ae...	Wilmington, Delaware, US	Not Applied	Multifactor authentication

Registros de inicio de sesión en Azure IdP

Troubleshoot

1. Puede resolver problemas utilizando DART desde el PC del usuario de Secure Client.
2. Para resolver un problema de autenticación SAML, utilice este debug:

```
<#root>
```

```
firepower#
```

```
debug webvpn saml 255
```

3. Verifique la configuración de Secure Client como se explicó anteriormente; este comando se puede utilizar para comprobar el certificado.

```
<#root>
```

```
firepower#
```

```
show crypto ca certificate
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).