# Configure SAML Auth for Multiple RAVPN Connection Profiles on FTD

## Contents


**Introduction**

**Prerequisites**

- Requirements
- Components Used

**Background Information**

**Configurations**

- Configuration Overview:
- Configure
  - Configuration on Azure IdP
  - Configuration on the FTD via FMC

**Verify**

- Configuration on the FTD command line
- Sign-in logs from Azure entra identifier

**Troubleshoot**


## Introduction

This document describes SAML Authentication with Azure identity provider for multiple connection profiles on Cisco FTD managed by FMC.

## Prerequisites

### Requirements

Cisco recommends knowledge of these topics:

- Secure Client configuration on Next Generation Firewall (NGFW) managed by Firepower Management Center (FMC)
- SAML and metatada.xml values

### Components Used

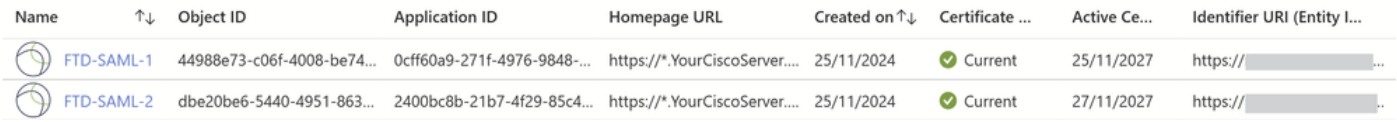
The information in this document is based on these software and hardware versions:

- Firepower Threat Defense (FTD) version 7.4.0
- FMC version 7.4.0
- Azure Microsoft Entra ID with SAML 2.0
- Cisco Secure Client 5.1.7.80

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Background Information

This configuration allows FTD to authenticate secure client users using two different SAML application on Azure idp with a single SAML object configured on 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:// |
| FTD-SAML-2 | dbe20be6-5440-4951-863... | 2400bc8b-21b7-4f29-85c4... | https://*.YourCiscoServer.... | 25/11/2024 | Current | 27/11/2027 | https:// |

In a Microsoft Azure environment, multiple applications can share the same Entity ID. Each application, typically mapped to a different tunnel group, necessitates a unique certificate, requiring the configuration of multiple certificates within the FTD side's IdP configuration under a single SAML IdP object. However, Cisco FTD does not support the configuration of multiple certificates under one SAML IdP object, as detailed in Cisco bug ID CSCvi29084.

To overcome this limitation, Cisco has introduced the IdP certificate override feature, available from FTD version 7.1.0 and ASA version 9.17.1. This enhancement offers a permanent solution to the issue and complements the existing workarounds described in the bug report.

# Configurations

This section outlines the process for configuring SAML authentication with Azure as the identity provider (IdP) for multiple connection profiles on Cisco Firepower Threat Defense (FTD) managed by Firepower Management Center (FMC). The IdP certificate override feature is utilized to set this up effectively.

## Configuration Overview:

Two connection profiles are to be configured on Cisco FTD:

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

In this configuration sample, the VPN gateway URL (Cisco Secure Client FQDN) is set to nigarapa2.cisco.com

## Configure

### Configuration on Azure IdP

To configure your SAML enterprise applications for Cisco Secure Client effectively, ensure all parameters are set correctly for each tunnel group by completing these steps:

**Access SAML Enterprise Applications:**

Navigate to the administrative console of your SAML provider where your enterprise applications are listed.

**Select the Appropriate SAML Application:**

Identify and select the SAML applications corresponding to the Cisco Secure Client tunnel groups you intend to configure.

**Configure the Identifier (Entity ID):**

Set the Identifier (Entity ID) for each application. This must be the Base URL, which is your Cisco Secure Client Fully Qualified Domain Name (FQDN).

**Set the Reply URL (Assertion Consumer Service URL):**

Configure the Reply URL (Assertion Consumer Service URL) using the correct Base URL. Ensure it aligns with the Cisco Secure Client FQDN.

Append the connection profile or tunnel group name to the base URL to ensure specificity.

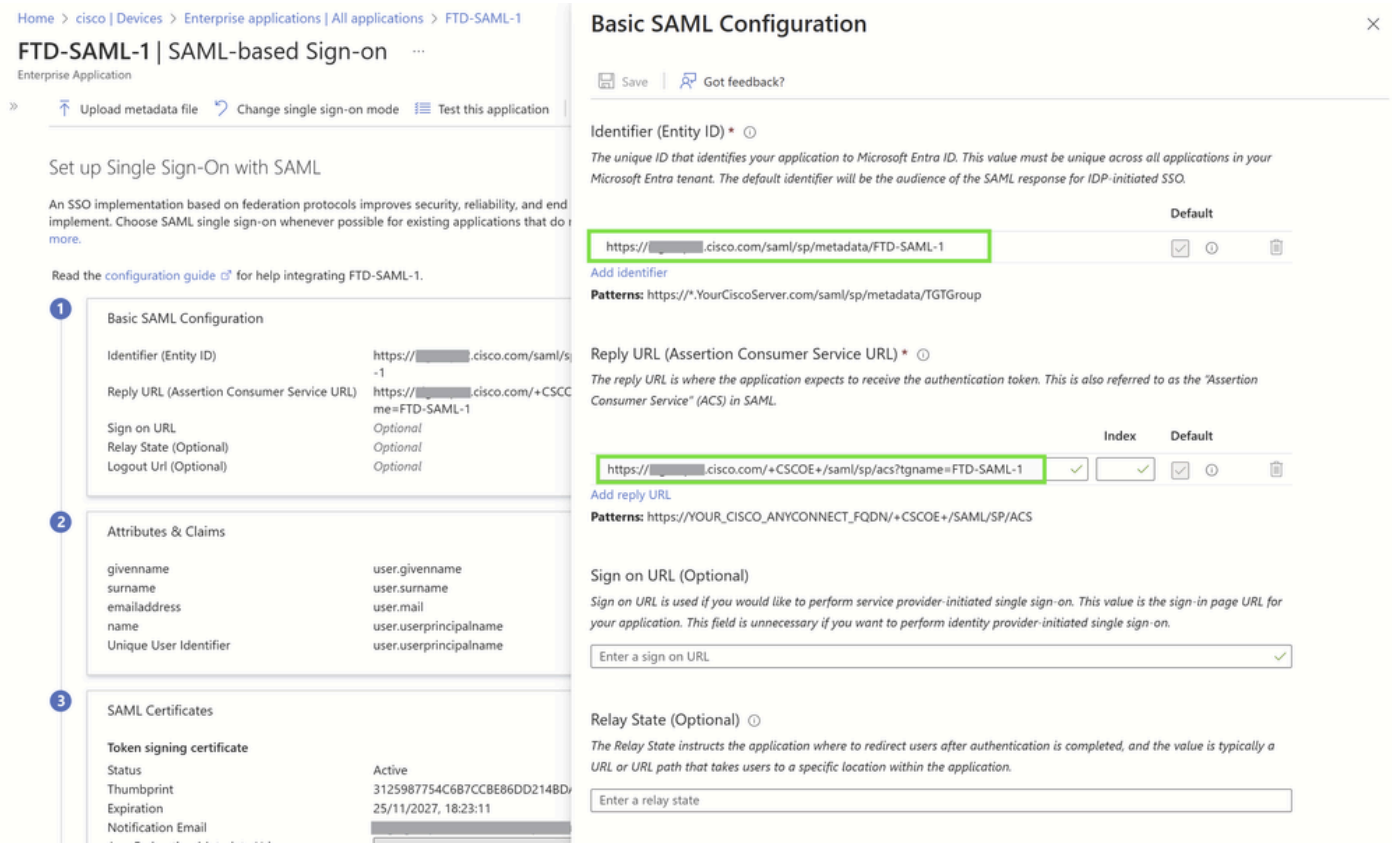
**Verify Configuration:**

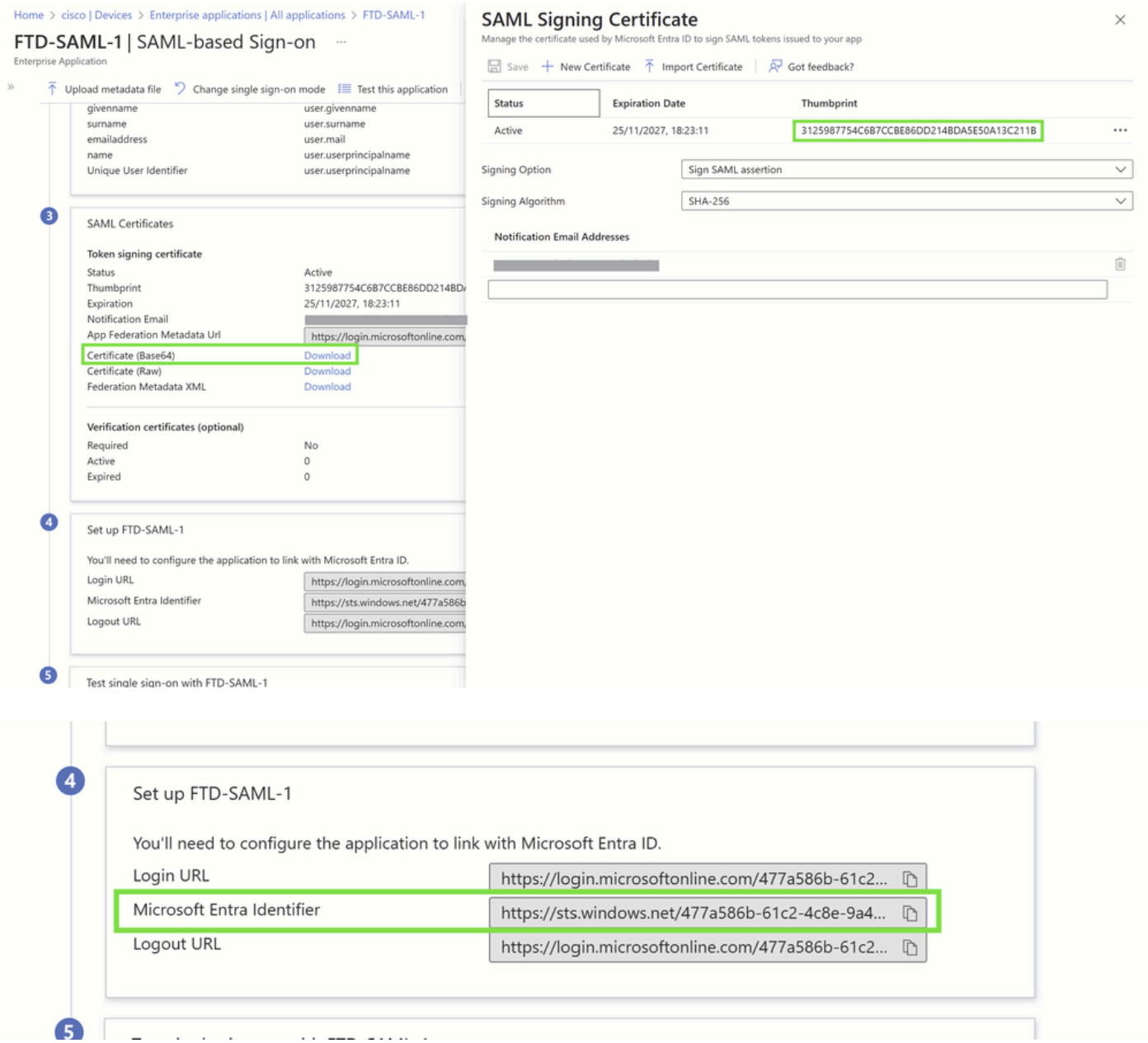
Double-check that all URLs and parameters are correctly entered and correspond to the respective tunnel groups.

Save changes and, if possible, perform a test authentication to ensure the configuration is working as expected.

For more detailed guidance, refer to the "Add Cisco Secure Client from the Microsoft App Gallery" in the Cisco documentation: [Configure ASA Secure Client VPN with Microsoft Azure MFA through SAML]

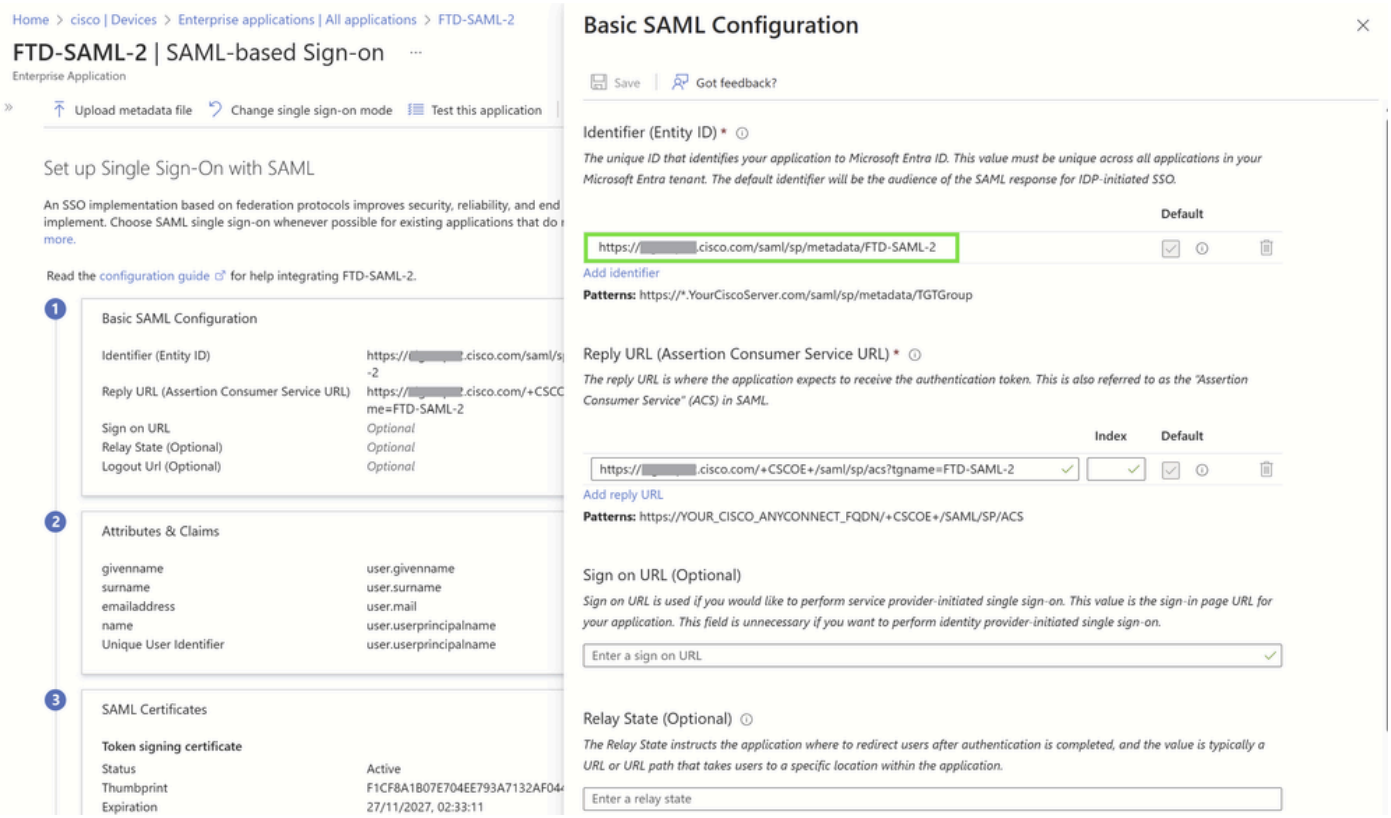
**FTD-SAML-1**

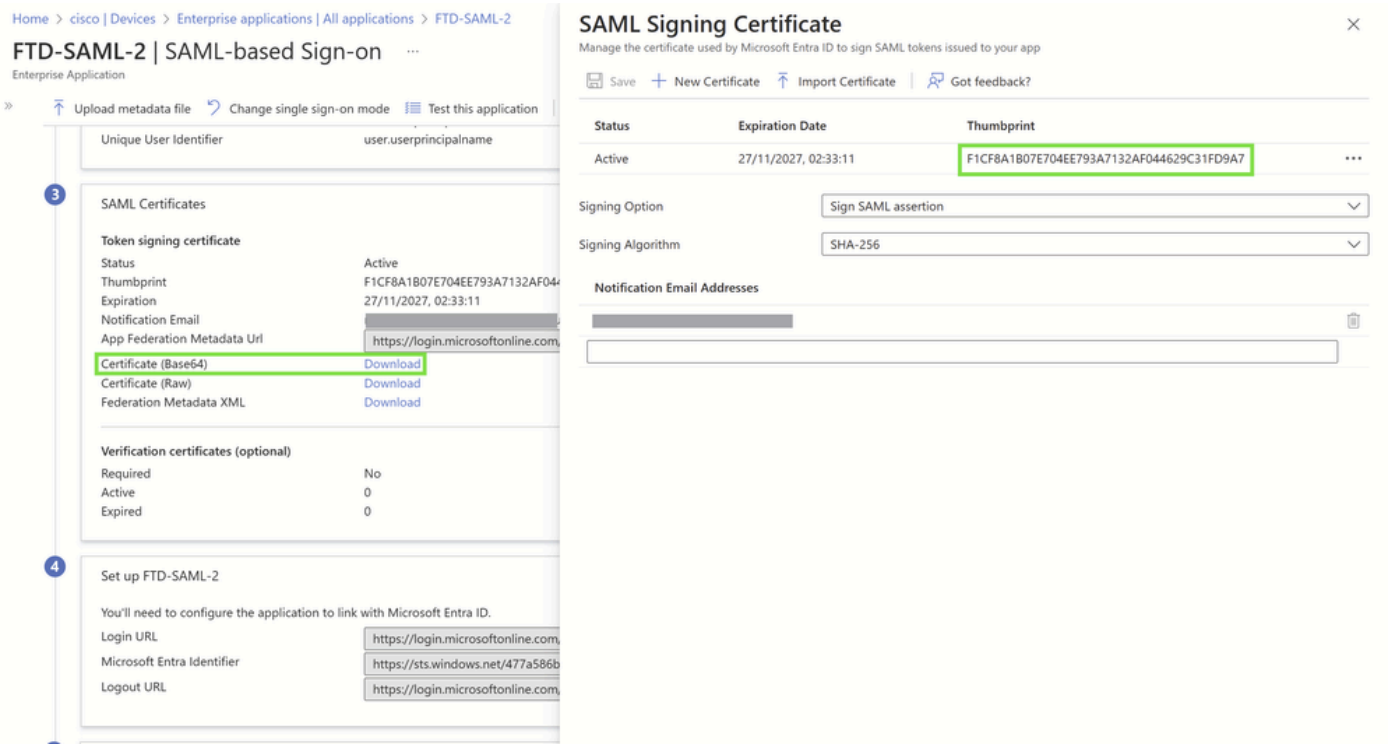


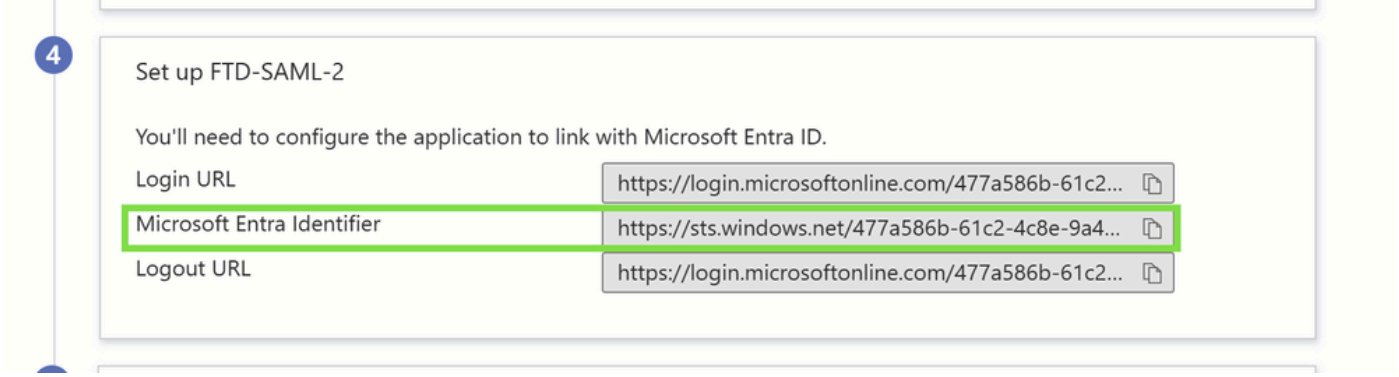

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
givenname
user.givenname
surname
user.surname
emailaddress
user.mail
name
user.userprincipalname
Unique User Identifier
user.userprincipalname
SAML Certificates
Token signing certificate
Status
Active
Thumbprint
Expiration
25/11/2027, 18:23:11
Notification Email
App Federation Metadata Url
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
Microsoft Entra Identifier
Logout URL
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
3125987754C6B7CCBE86DD214BDA5E50A13C211B
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**


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
implement. Choose SAML single sign-on whenever possible for existing applications that do
more.
Read the configuration guide for help integrating FTD-SAML-2.
1
Basic SAML Configuration
Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)
Sign on URL
Relay State (Optional)
Logout Url (Optional)
Optional
Optional
2
Attributes & Claims
givenname
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Thumbprint
Expiration
Active
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.
Default
https://.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.
Index
Default
https://.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


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
3
SAML Certificates
Token signing certificate
Status
Thumbprint
Expiration
Notification Email
App Federation Metadata Url
Certificate (Base64)
Certificate (Raw)
Federation Metadata XML
Active
27/11/2027, 02:33:11
https://login.microsoftonline.com/
Download
Download
Download
Verification certificates (optional)
Required
Active
Expired
No
0
0
4
Set up FTD-SAML-2
You'll need to configure the application to link with Microsoft Entra ID.
Login URL
Microsoft Entra Identifier
Logout URL
https://login.microsoftonline.com/
https://sts.windows.net/477a586b
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




Now please ensure you have the necessary information and files for configuring SAML authentication with Microsoft Entra as your identity provider:

**Locate the Microsoft Entra Identifier:**

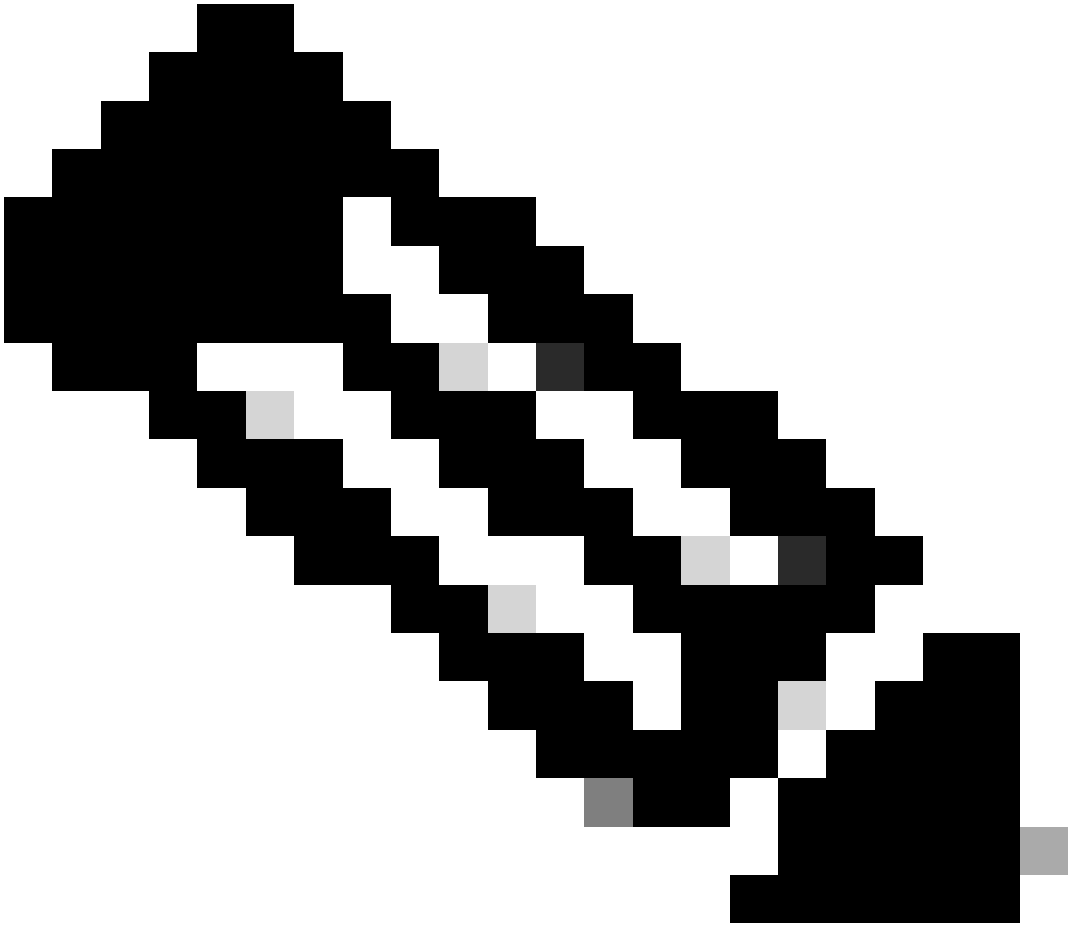
Access the settings for both SAML enterprise applications within your Microsoft Entra portal.

Note the Microsoft Entra Identifier, which remains consistent across both applications and is crucial for your SAML configuration.

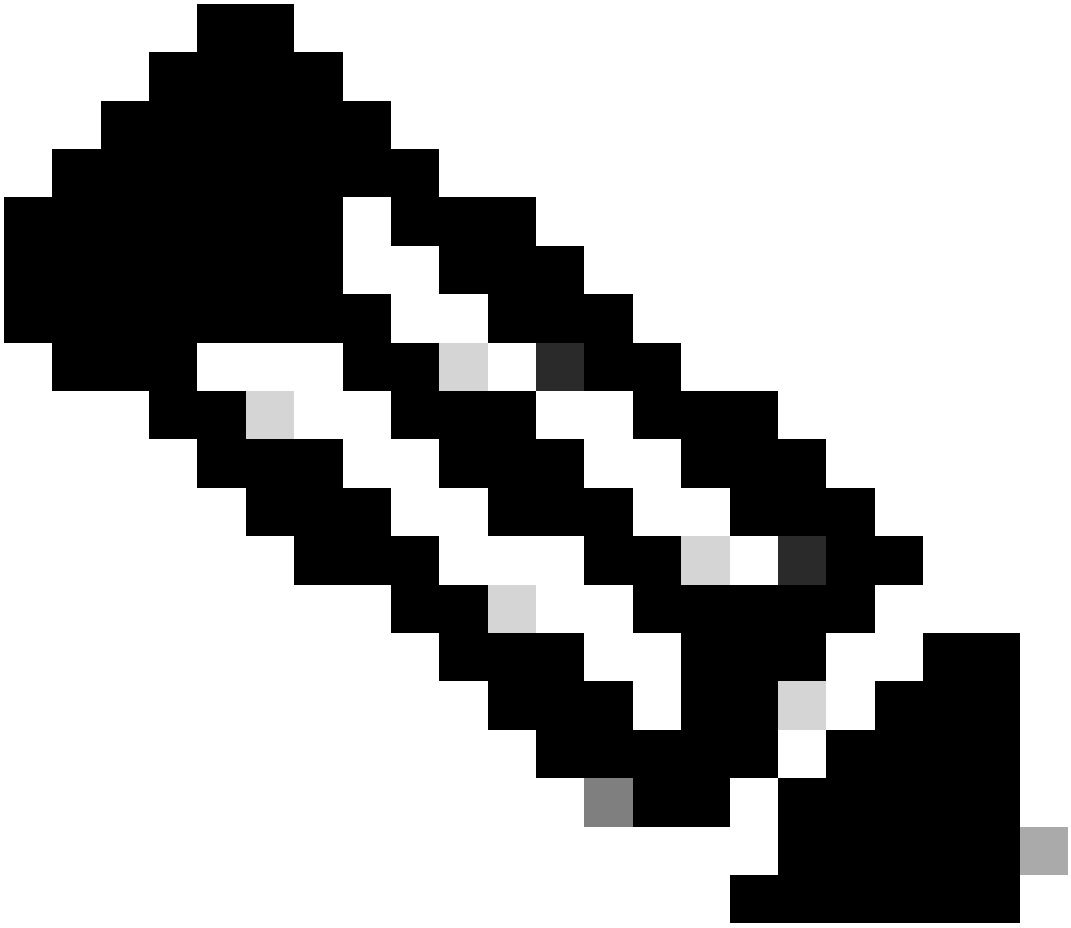
**Download Base64 IdP Certificates:**

Navigate to each configured SAML enterprise application.

Download the respective Base64-encoded IdP certificates. These certificates are essential for establishing trust between your identity provider and your Cisco VPN setup.



**Note**: All these SAML configurations required for the FTD connection profiles can also be sourced from the metadata.xml files provided by your IdP for the respective applications.



**Note**: To use a custom IdP certificate, you need to upload the custom-generated IdP certificate to both the IdP and FMC. For Azure IdP, ensure the certificate is in PKCS#12 format. On the FMC, upload only the Identity certificate from the IdP, not the PKCS#12 file. For detailed instructions, refer to the section "Upload the PKCS#12 File on Azure and FDM" in the Cisco documentation: Configure Multiple RAVPN Profiles with SAML Authentication on FDM

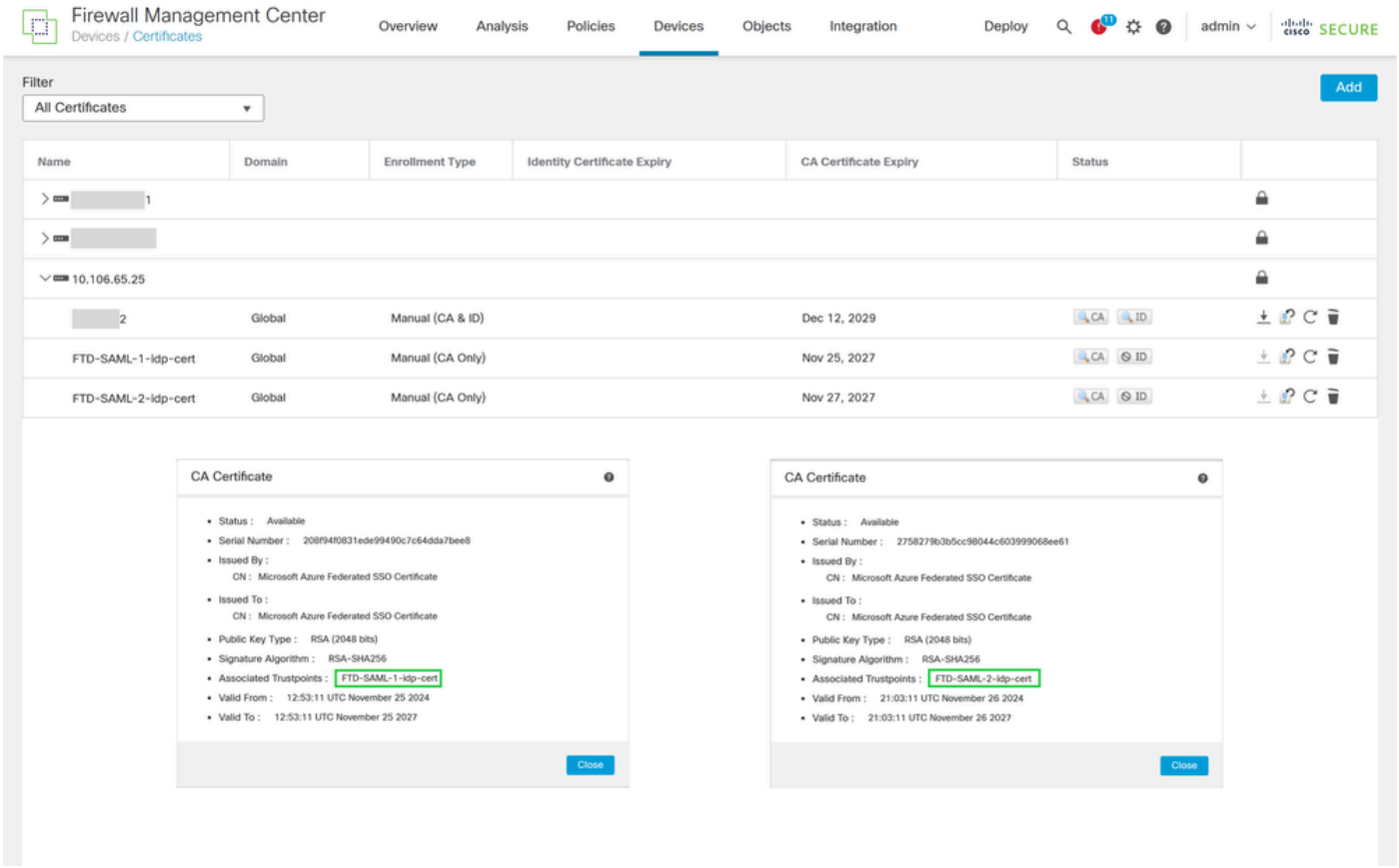
---

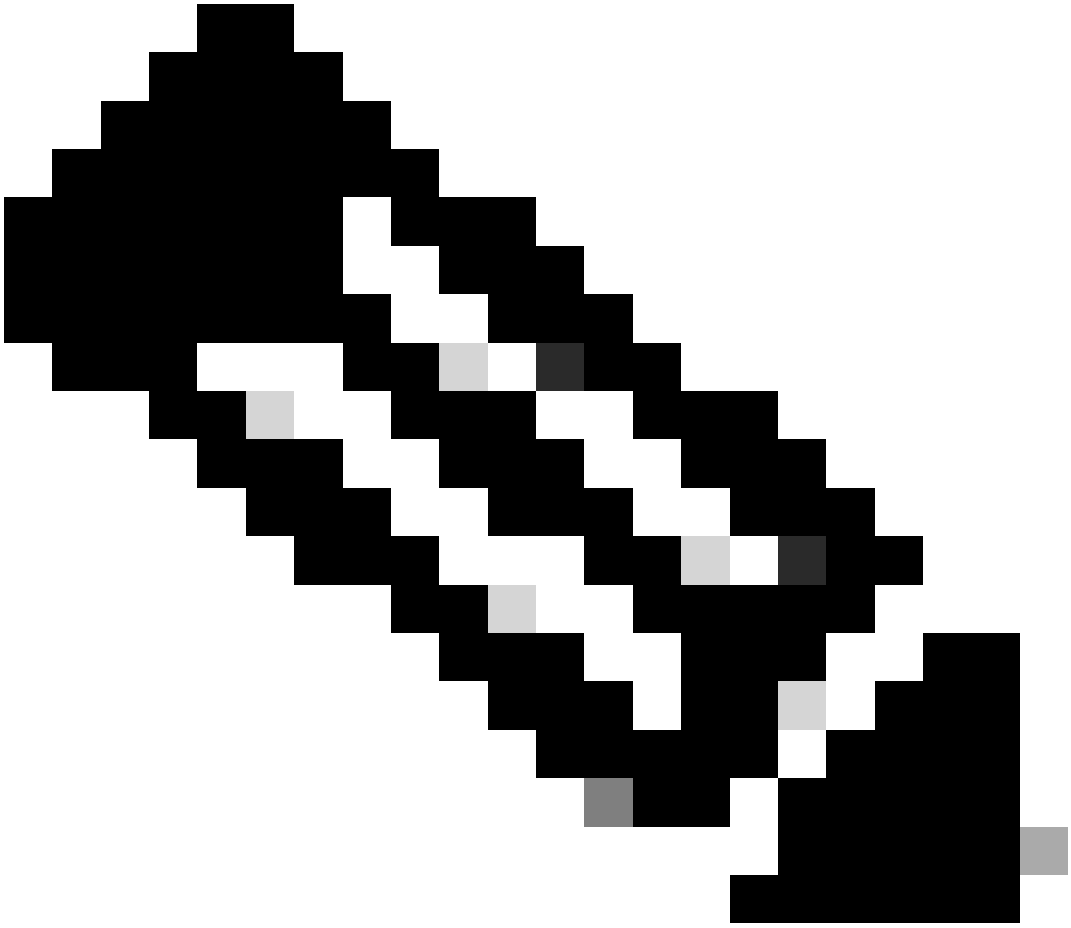
**Configuration on the FTD via FMC**

**Enroll IdP Certificates:**

Navigate to the certificates management section within FMC and enroll the downloaded Base64-encoded IdP certificates for both SAML applications. These certificates are vital for establishing trust and enabling SAML authentication.

For detailed guidance, please refer to the first two steps under "Configuration on the FTD via FMC" in the Cisco documentation available at: Configure Secure Client with SAML Authentication on FTD Managed via 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
10.106.65.25
Global
Manual (CA & ID)
Dec 12, 2029
FTD-SAML-1-idp-cert
Global
Manual (CA Only)
Nov 25, 2027
FTD-SAML-2-idp-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-idp-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-idp-cert
Valid From : 21:03:11 UTC November 26 2024
Valid To : 21:03:11 UTC November 26 2027
Close



**Note**: The image has been edited to display both certificates simultaneously for better viewing. It is not possible to open both certificates at the same time on FMC.

---

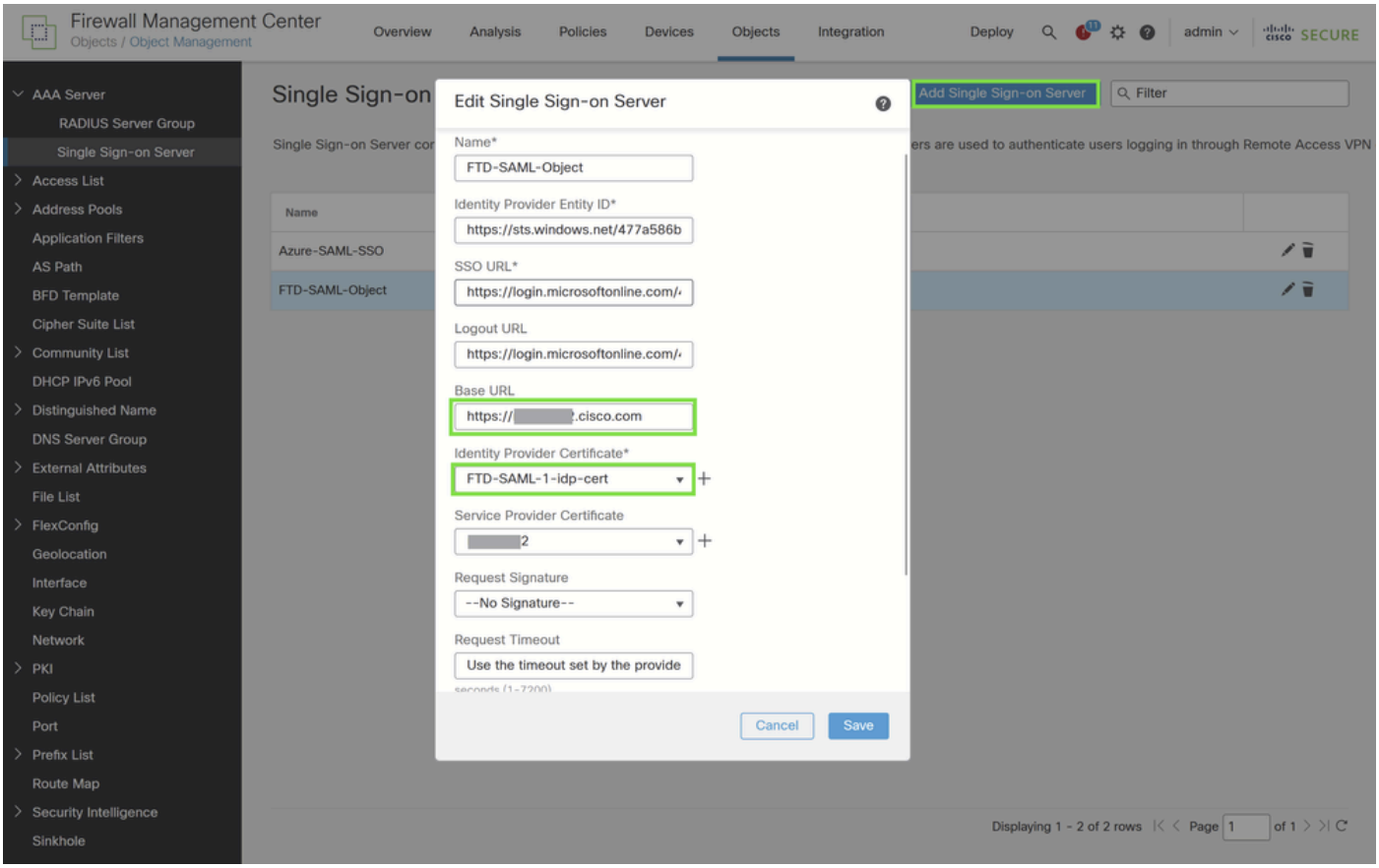
**Configuring SAML Server Settings on Cisco FTD via FMC**

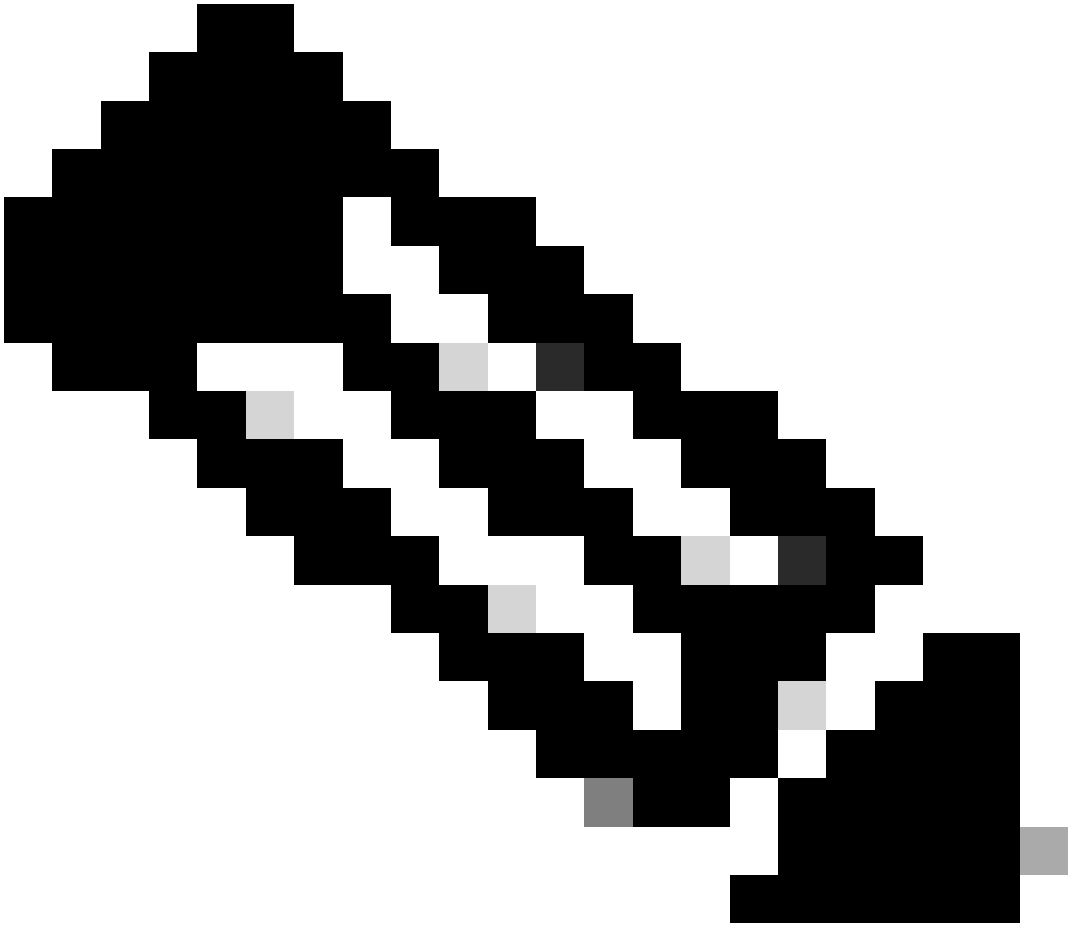
To configure the SAML server settings on your Cisco Firepower Threat Defense (FTD) using the Firepower Management Center (FMC), implement these steps:

1. Navigate to Single Sign-on Server Configuration:
   - Navigate to **Objects > Object Management > AAA Servers > Single Sign-on Server**.
   - Click **Add Single Sign-on Server** to begin configuring a new server.

2. Configure SAML Server Settings:
   - Using the parameters collected from your SAML enterprise applications or from the metadata.xml file downloaded from your Identity Provider (IdP), fill in the necessary SAML values in the New Single Sign-on Server form.
   - Key parameters to configure include:
     - SAML Provider Entity ID: entityID from metadata.xml
     - SSO URL: SingleSignOnService from metadata.xml.
     - Logout URL: SingleLogoutService from metadata.xml.
     - BASE URL: FQDN of your FTD SSL ID Certificate.

- Identity Provider Certificate: IdP Signing Certificate.
  - Under the Identity Provider Certificate section, attach one of the enrolled IdP certificates
  - For this use case, we are using the IdP certificate from the FTD-SAML-1 application.
- Service Provider Certificate: FTD Signing Certificate.

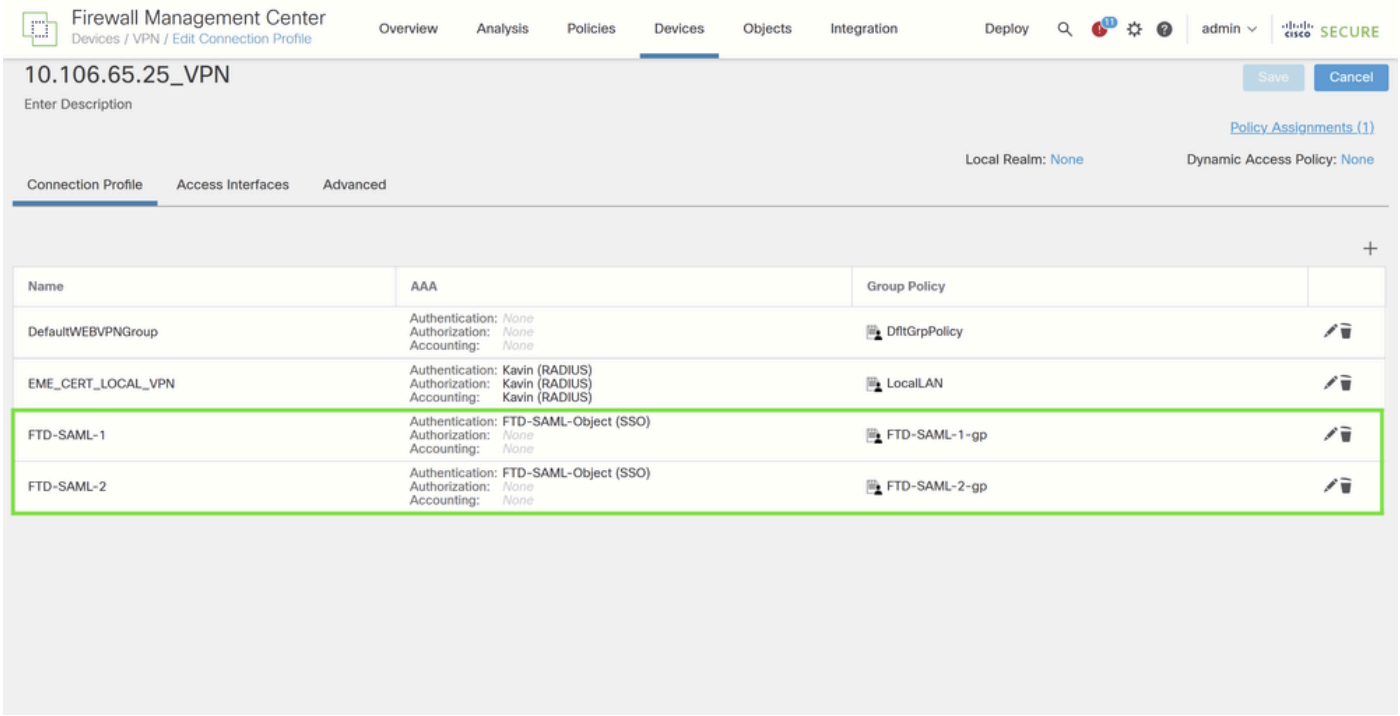




**Note**: In the current configuration, only the Identity Provider certificate can be overridden from the SAML object within the connection profile settings. Unfortunately, features such as "Request IdP re-authentication on login" and "Enable IdP only accessible on internal network" cannot be individually enabled or disabled for each connection profile.

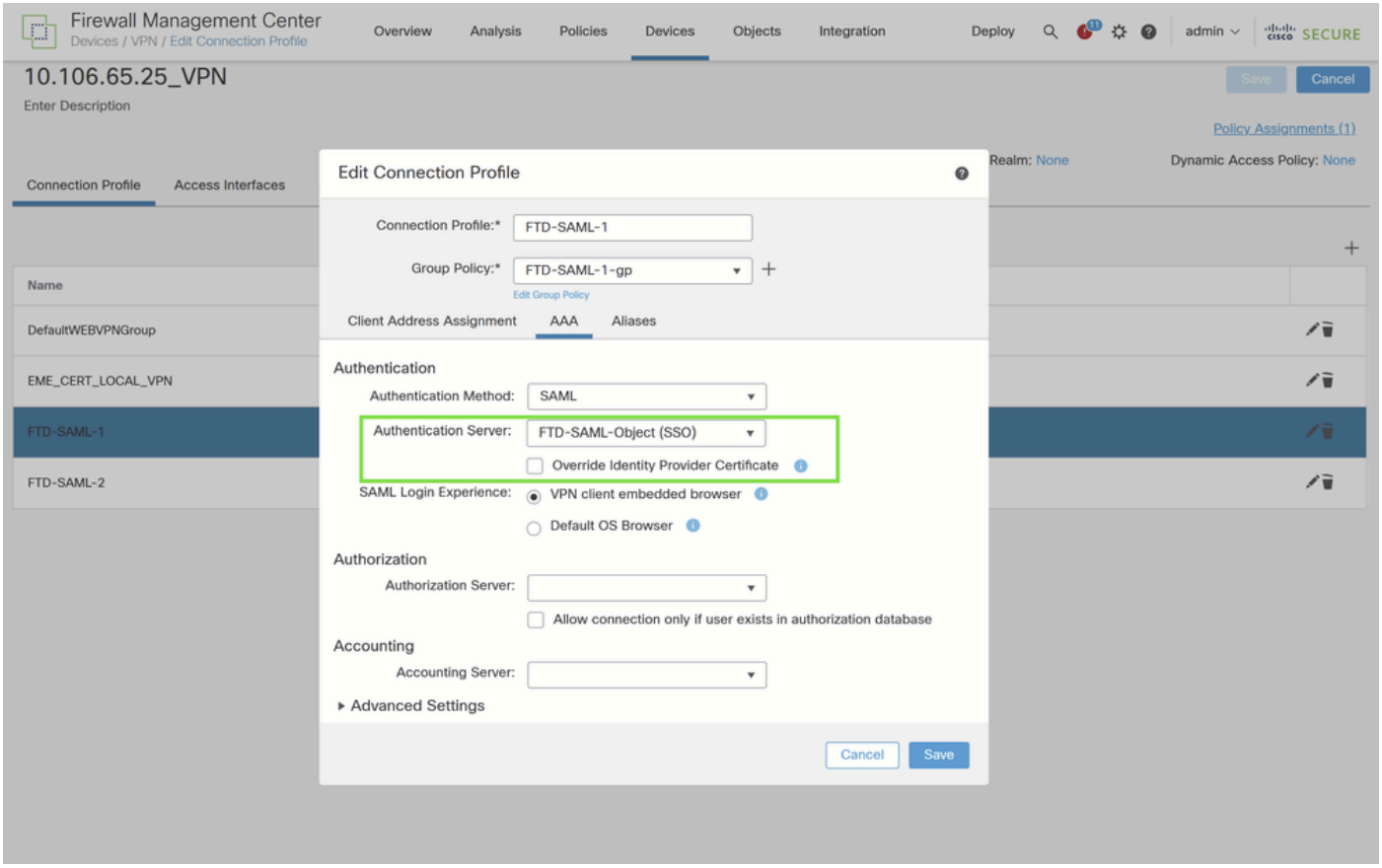
**Configuring Connection Profiles on Cisco FTD via FMC**

To finalize the SAML authentication setup, you need to configure the connection profiles with the appropriate parameters and set AAA authentication to SAML using the previously configured SAML server. For more detailed guidance, refer to the fifth step under "Configuration on the FTD via FMC" in the Cisco documentation: Configure Secure Client with SAML Authentication on FTD Managed via FMC.




**Extract of AAA Configuration for First Connection Profile**

Here is an overview of the AAA configuration settings for the first connection profile:



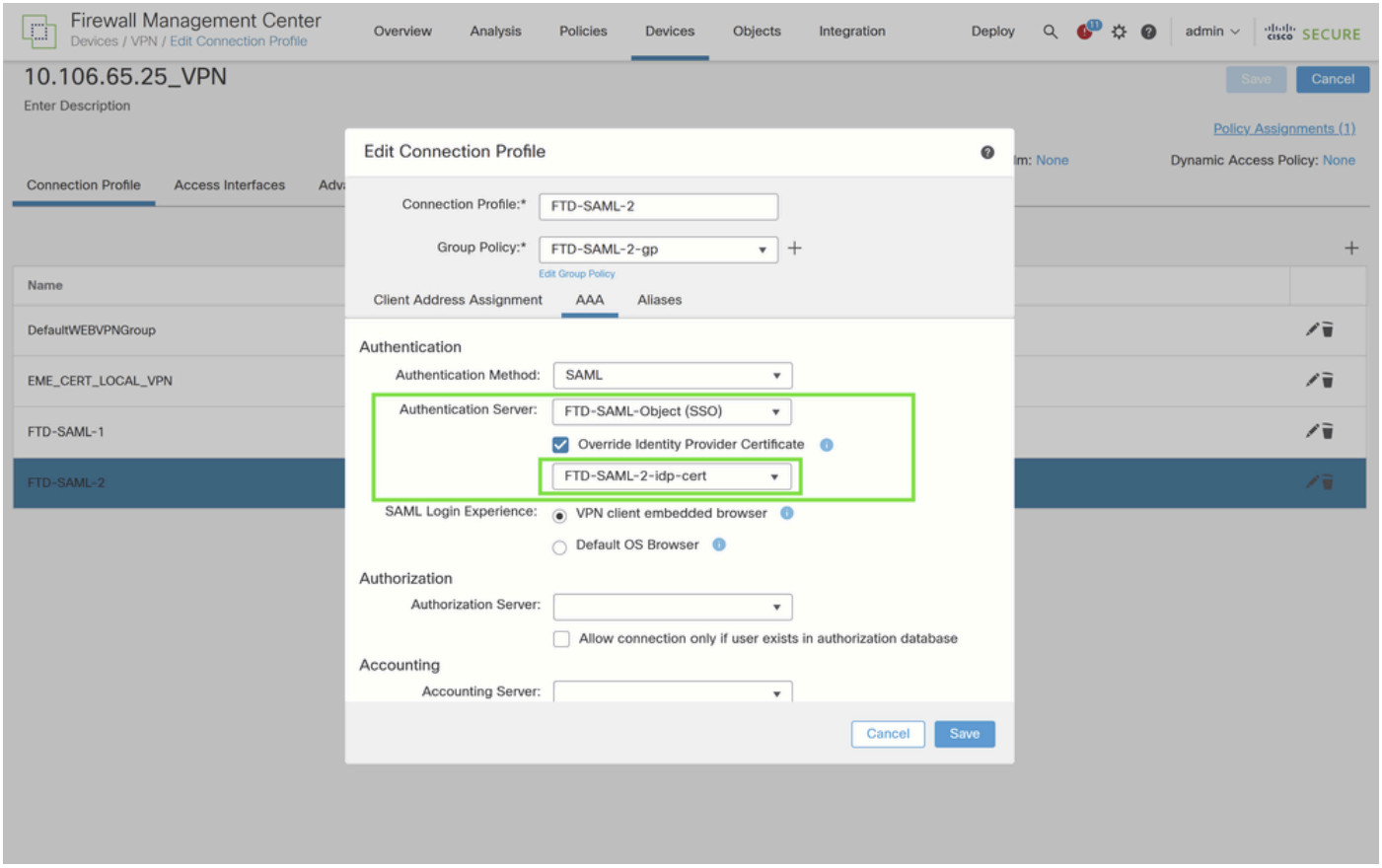

**Configuring the IdP Certificate Override for the Second Connection Profile on Cisco FTD**

To ensure the correct Identity Provider (IdP) certificate is used for the second connection profile, enable the IdP certificate override by completing these steps:

Within the connection profile settings, locate and enable the option "Override Identity Provider

Certificate" to allow the use of a different IdP certificate than the one configured for the SAML server.

From the list of enrolled IdP certificates, select the certificate specifically enrolled for the FTD-SAML-2 application. This selection ensures that when an authentication request is made for this connection profile, the correct IdP certificate is used.




### Deployment of configuration

Navigate to**Deploy** > **Deployment**and select the proper FTD  to apply the SAML Authentication VPN changes.

# Verify

### Configuration on the FTD command line

<#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
```

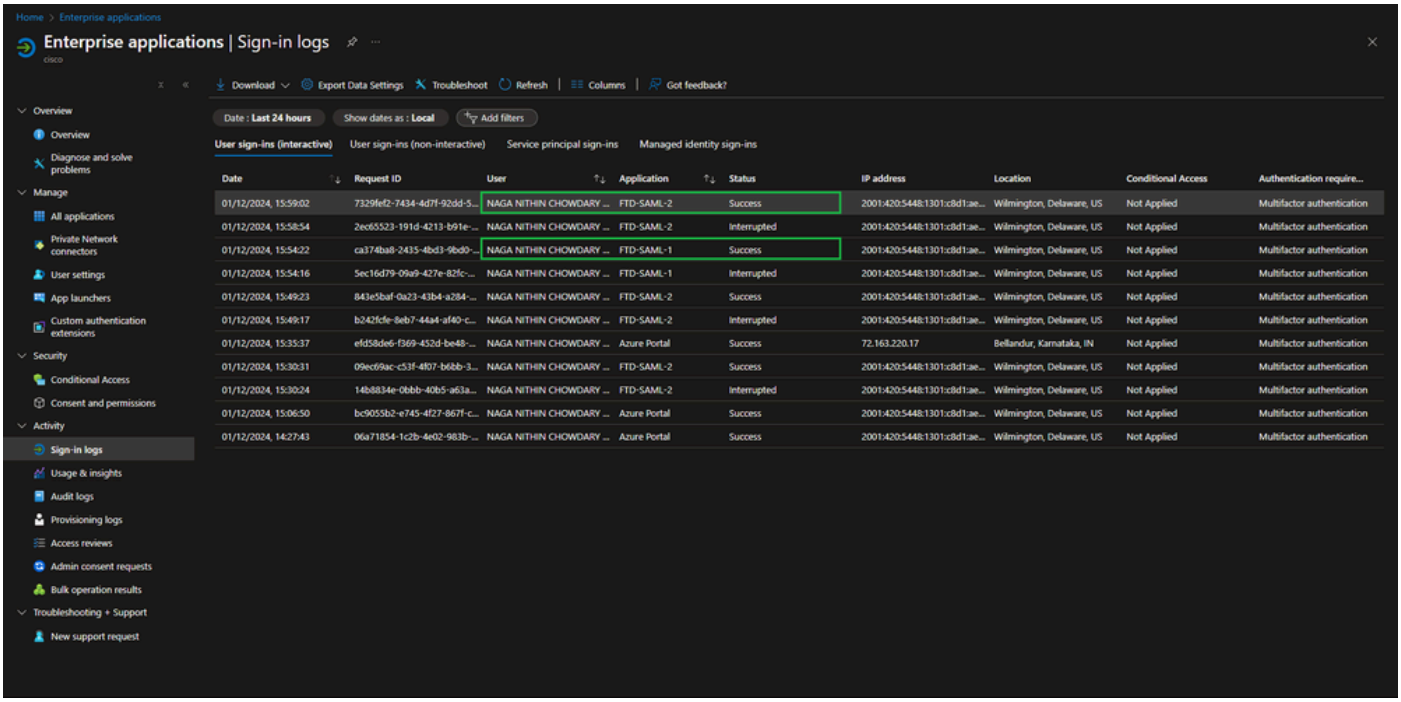
```
    address-pool secure-client-pool
    default-group-policy FTD-SAML-2-gp
tunnel-group FTD-SAML-2 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-2 enable
    saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/


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

firepower#
```

### Sign-in logs from Azure entra identifier

Access the Sign-in Logs section under enterprise application. Look for authentication requests related to the specific connection profiles, such as FTD-SAML-1 and FTD-SAML-2. Verify that users are successfully authenticating through the SAML applications associated with each connection profile.




*Sign-in Logs on Azure IdP*

# Troubleshoot

1. You can troubleshoot using DART from the Secure Client user PC.
2. To troubleshoot a SAML authentication issue, utilize this debug:

   <#root>

   ```
   firepower#
    debug webvpn saml 255
   ```

3. Verify the Secure Client configuration as explained above; this command can be used to check the

certificate.

<#root>

```
firepower#
 show crypto ca certificate
```