为FTD上的多个RAVPN连接配置文件配置SAML身份验证

目录

简介

本文档介绍使用Azure身份提供程序对由FMC管理的思科FTD上的多个连接配置文件进行SAML身份验证。

先决条件

要求

建议掌握下列主题的相关知识：

- 下一代防火墙(NGFW)上由Firepower管理中心(FMC)管理的安全客户端配置
- SAML和metatada.xml值

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower威胁防御(FTD)版本7.4.0
- FMC版本7.4.0
- 带SAML 2.0的Azure Microsoft Entra ID
- 思科安全客户端5.1.7.80

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

此配置允许FTD使用两个不同的SAML应用程序在Azure idp上对安全客户端用户进行身份验证，并在FMC上配置单个SAML对象。

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://
FTD-SAML-2	dbe20be6-5440-4951-863...	2400bc8b-21b7-4f29-85c4...	https://*.YourCiscoServer....	25/11/2024	Current	27/11/2027	https://

在Microsoft Azure环境中，多个应用程序可以共享相同的实体ID。每个应用程序（通常映射到不同的隧道组）都需要一个唯一的证书，要求在单个SAML IdP对象下的FTD端的IdP配置中配置多个证书。但是，思科FTD不支持在一个SAML IdP对象下配置多个证书，如思科Bug ID CSCvi29084中所述。

为了克服此限制，思科引入了IdP证书覆盖功能，该功能可从FTD 7.1.0版和ASA 9.17.1版中获取。此增强功能提供了永久性的问题解决方案，并补充了错误报告中介绍的现有解决方法。

配置

本节概述在Firepower管理中心(FMC)管理的Cisco Firepower威胁防御(FTD)上，将Azure配置为多个连接配置文件的身份提供程序(IdP)的SAML身份验证配置过程。 利用IdP证书覆盖功能有效地进行设置。

配置概述:

在思科FTD上配置两个连接配置文件：

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

在此配置示例中，VPN网关URL（思科安全客户端FQDN）设置为nigarapa2.cisco.com

配置

Azure IdP上的配置

要为Cisco安全客户端有效配置SAML企业应用，请完成以下步骤，确保为每个隧道组正确设置所有参数：

访问SAML企业应用：

导航到SAML提供商的管理控制台，其中列出了您的企业应用。

选择适当的SAML应用：

识别并选择与要配置的思科安全客户端隧道组对应的SAML应用。

配置标识符（实体ID）：

设置每个应用程序的标识符（实体ID）。必须是基本URL，即您的思科安全客户端完全限定域名(FQDN)。

设置回复URL（断言消费者服务URL）：

使用正确的基本URL配置回复URL（断言消费者服务URL）。确保它与思科安全客户端FQDN一致。

将连接配置文件或隧道组名称附加到基本URL以确保特异性。

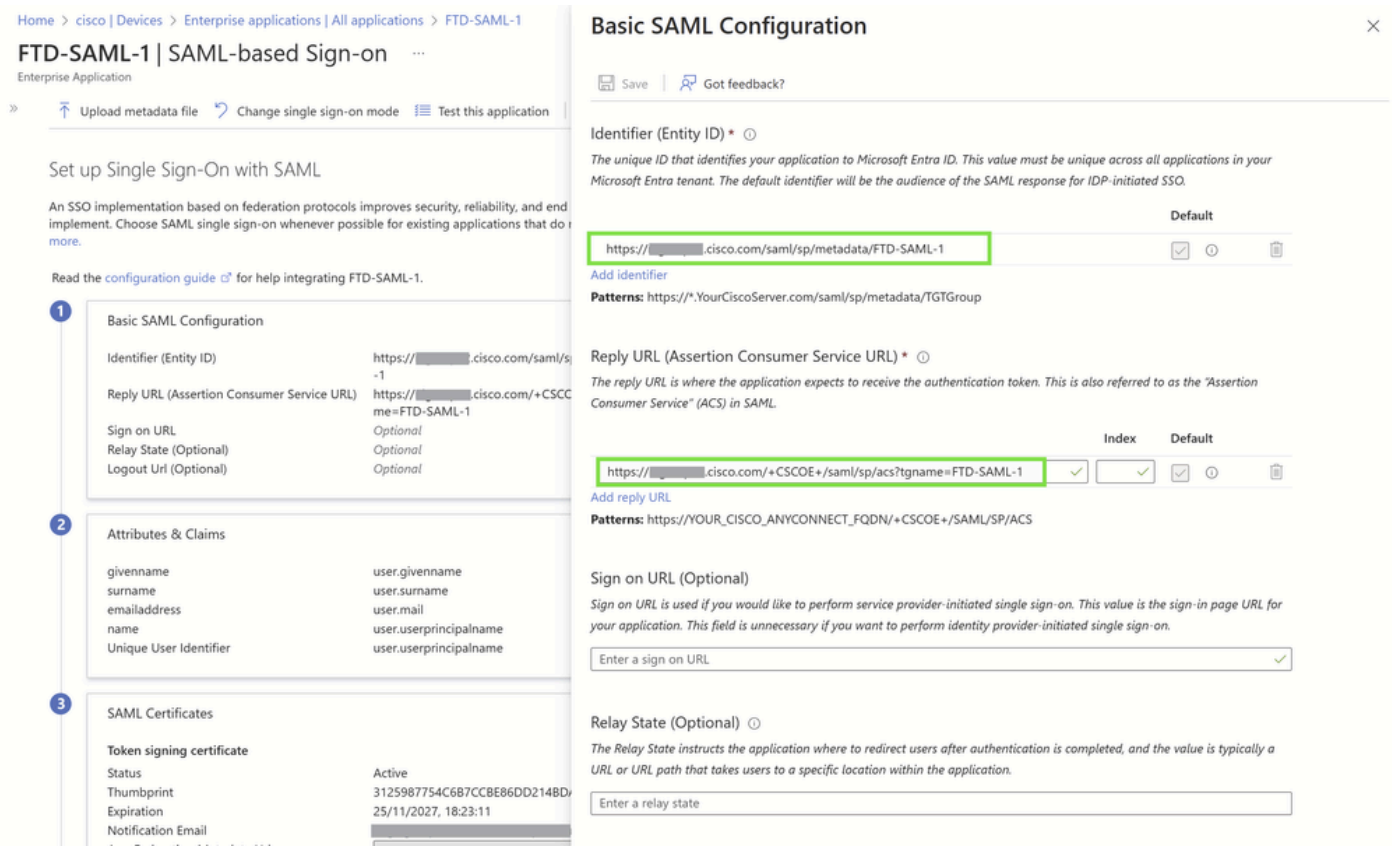
验证配置:

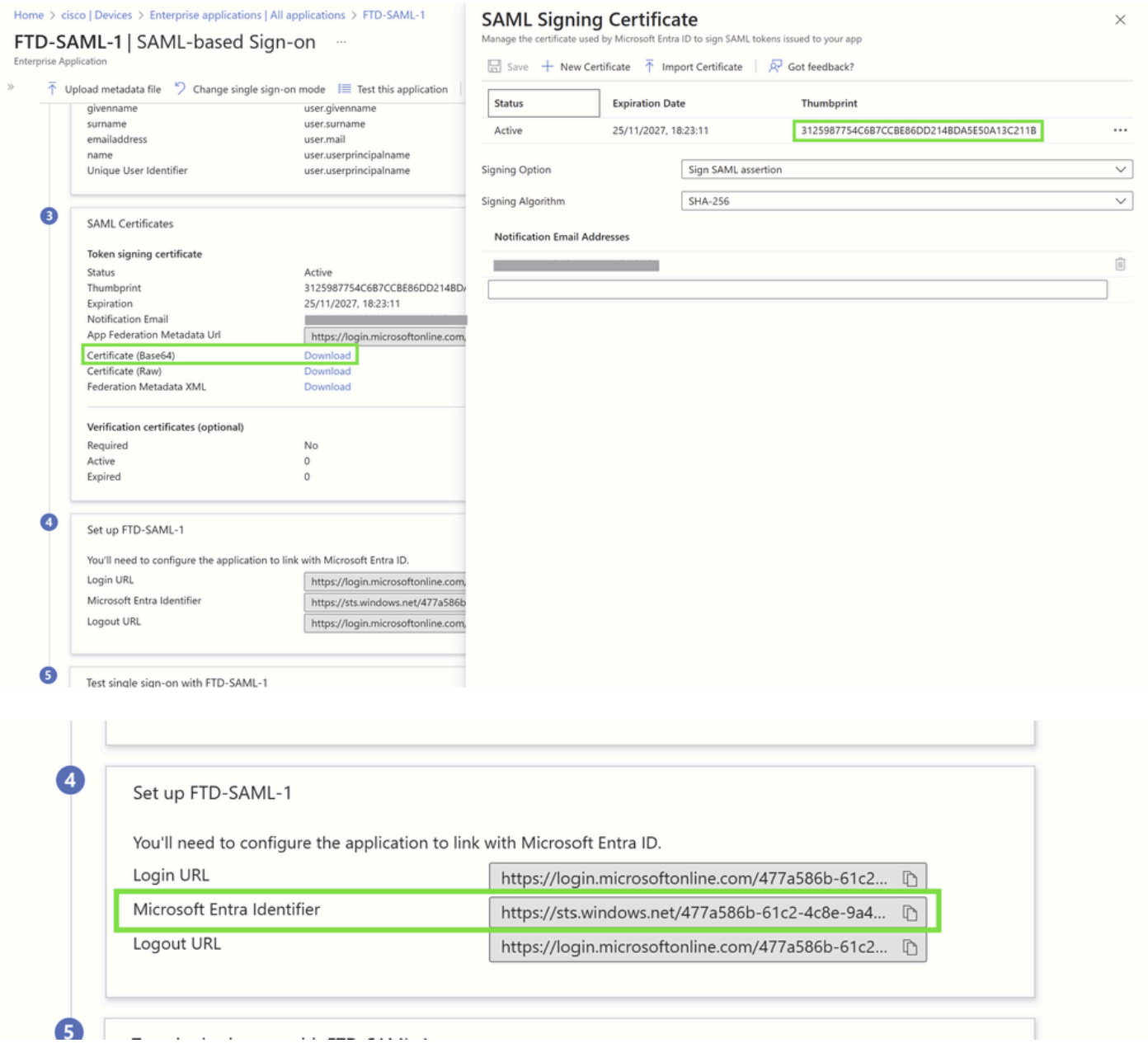
仔细检查是否所有URL和参数都已正确输入且与相应的隧道组相对应。

保存更改，如有可能，执行测试身份验证以确保配置按预期运行。

有关更详细的指导，请参阅思科文档中的“从Microsoft应用库添加Cisco安全客户端”：使用Microsoft Azure MFA通过SAML配置ASA安全客户端VPN

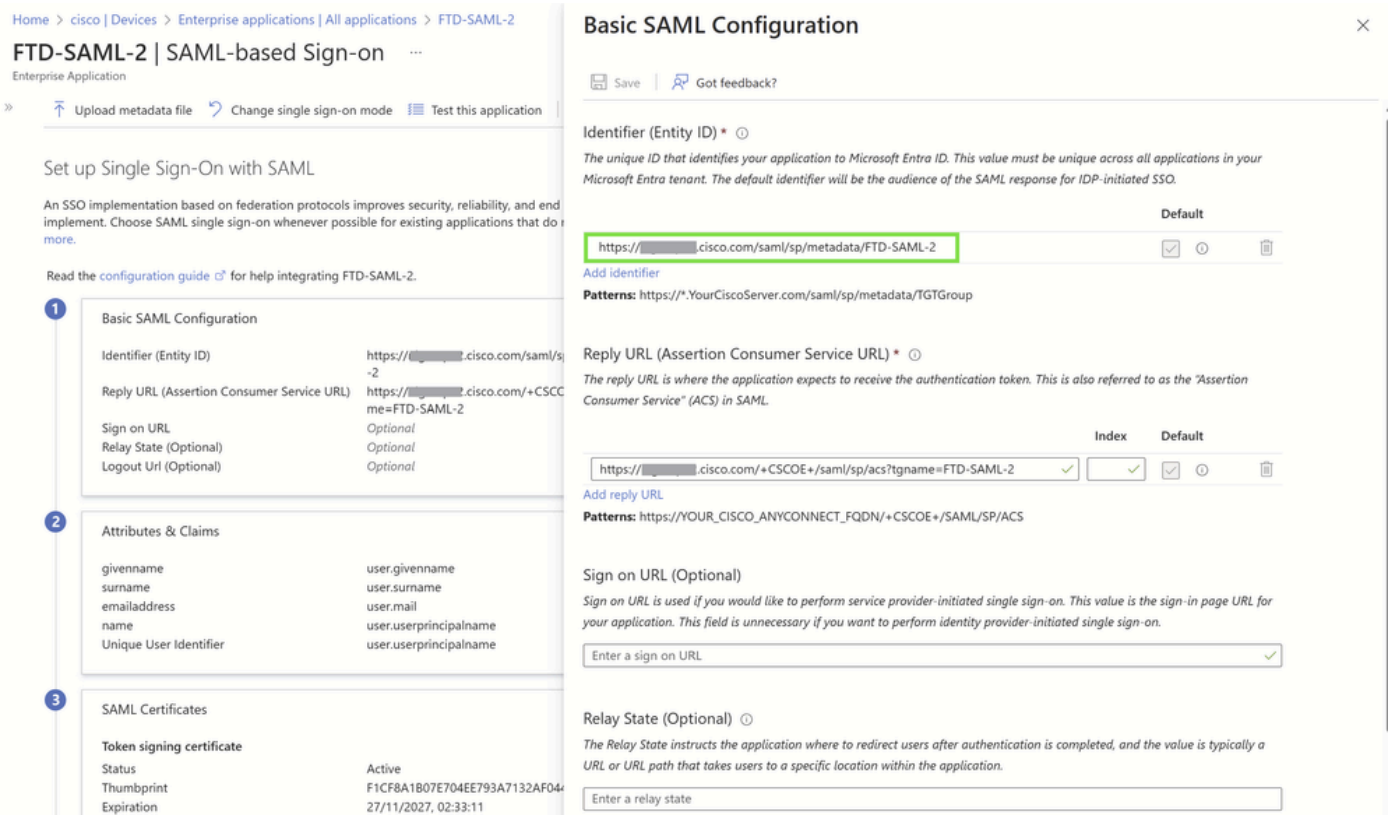
FTD-SAML-1

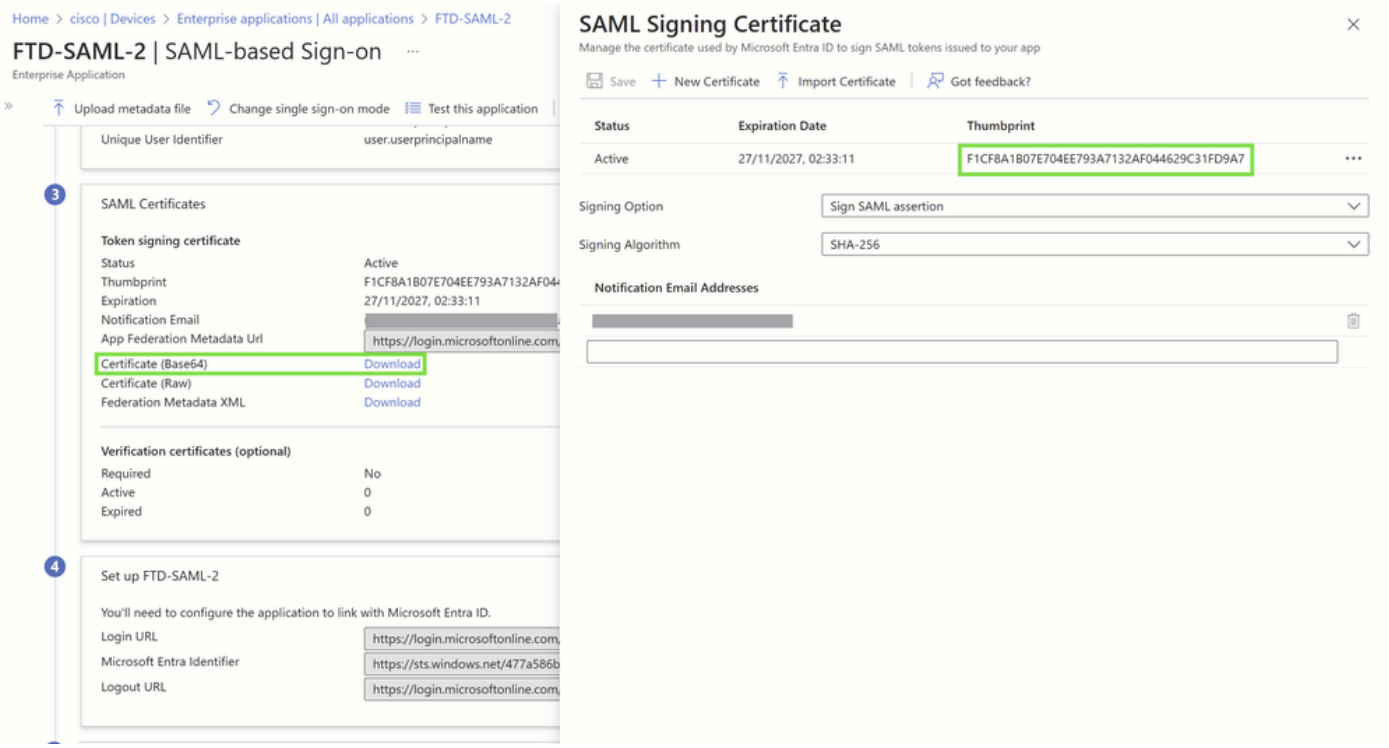


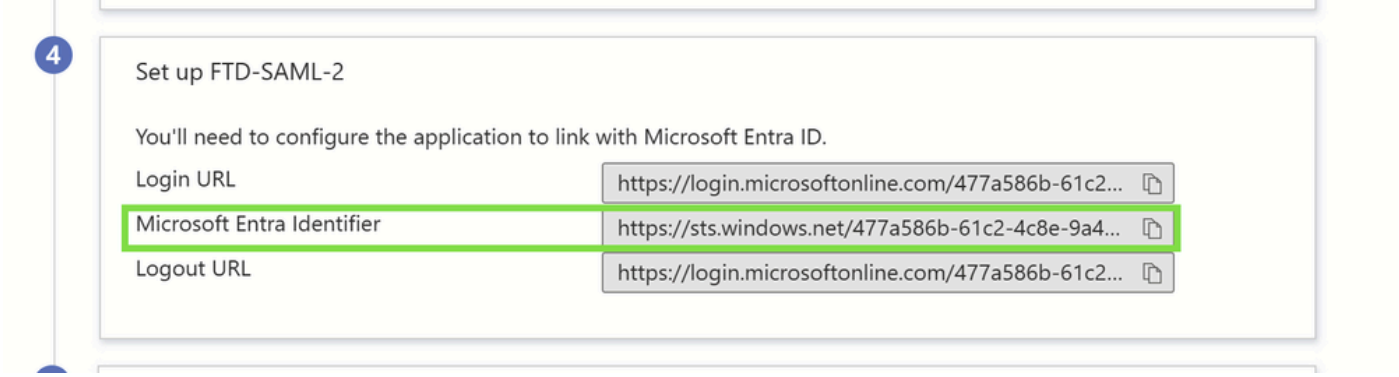

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
givenname
user.givenname
surname
user.surname
emailaddress
user.mail
name
user.userprincipalname
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



现在请确保您具有配置SAML身份验证的必要信息和文件，并将Microsoft Entra用作您的身份提供程序：

找到Microsoft Entra标识符：

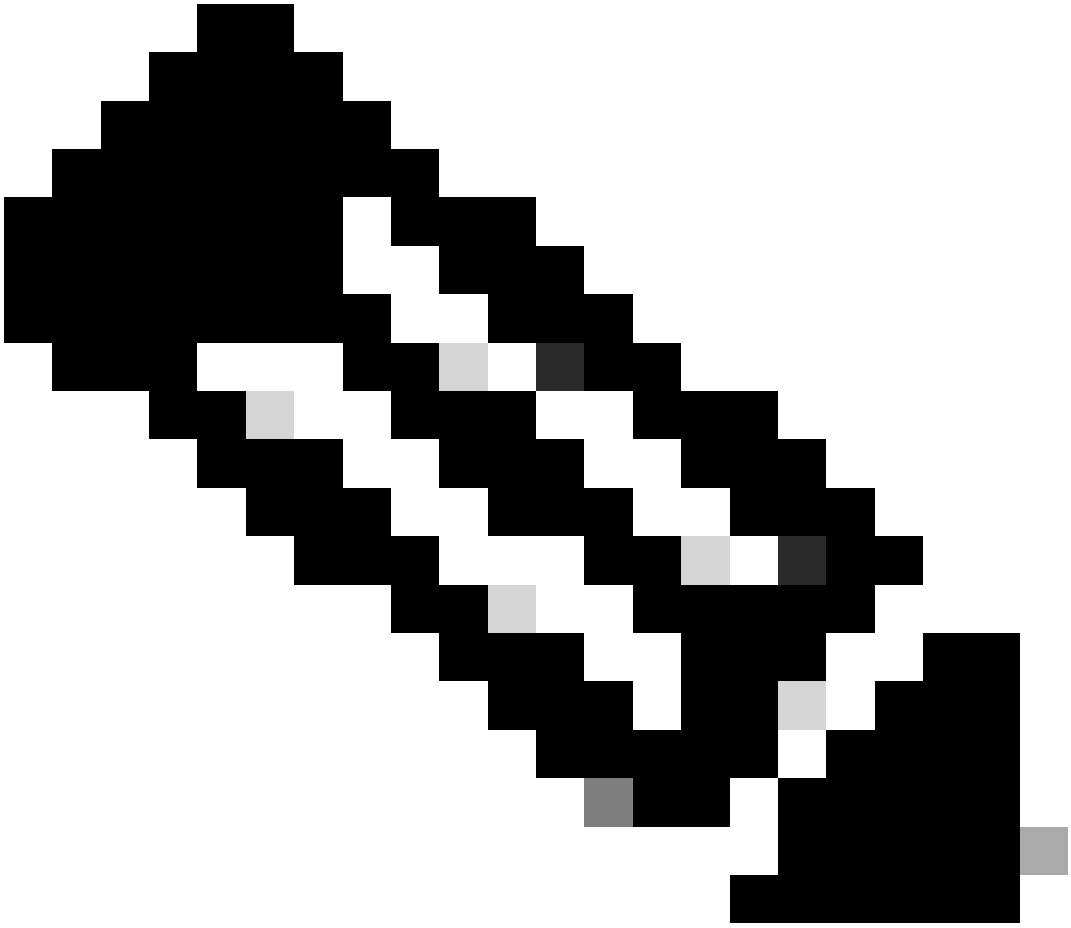
访问Microsoft Entra门户中的两个SAML企业应用的设置。

注意Microsoft Entra标识符，它在两个应用中保持一致，对SAML配置至关重要。

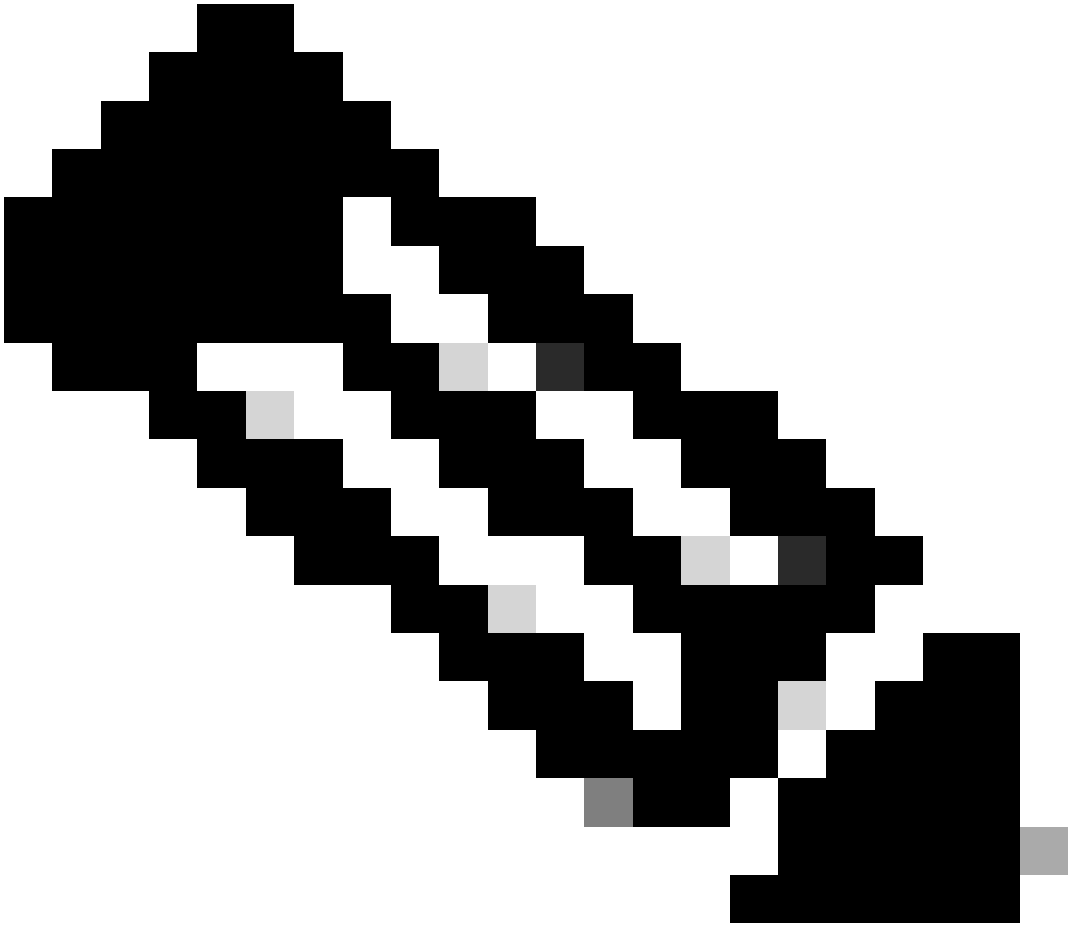
下载Base64 IdP证书：

导航到每个已配置的SAML企业应用。

下载各自的Base64编码IdP证书。这些证书对于在身份提供者和Cisco VPN设置之间建立信任至关重要。



注意：FTD连接配置文件所需的所有这些SAML配置也可从IdP为各个应用提供的metadata.xml文件获得。



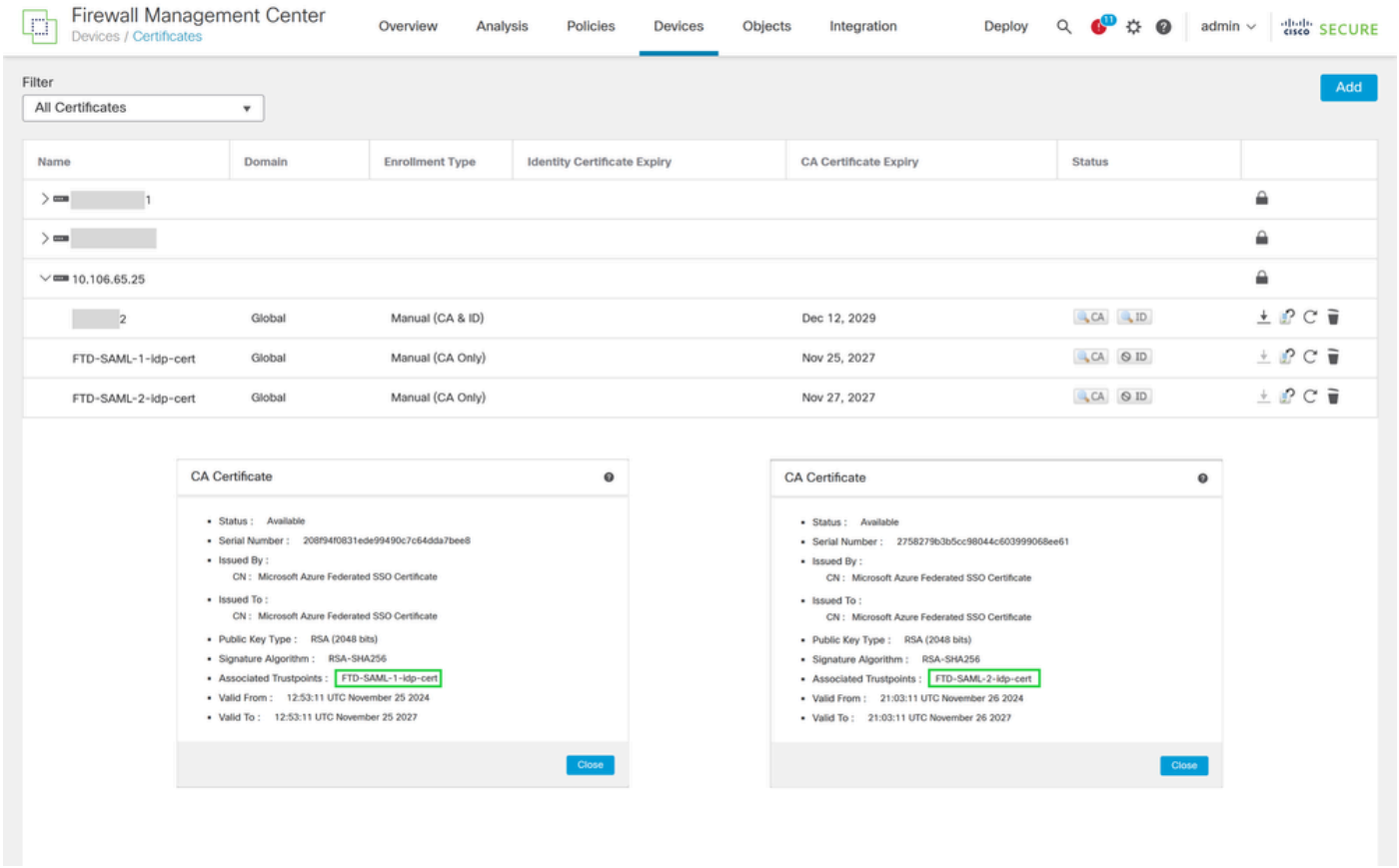
注意：要使用自定义IdP证书，您需要将自定义生成的IdP证书上传到IdP和FMC。对于Azure IdP，请确保证书采用PKCS#12格式。在FMC上，仅从IdP上传身份证书，而不上传PKCS#12文件。有关详细说明，请参阅思科文档中的“在Azure和FDM上上传PKCS#12文件”部分：在FDM上使用SAML身份验证配置多个RAVPN配置文件

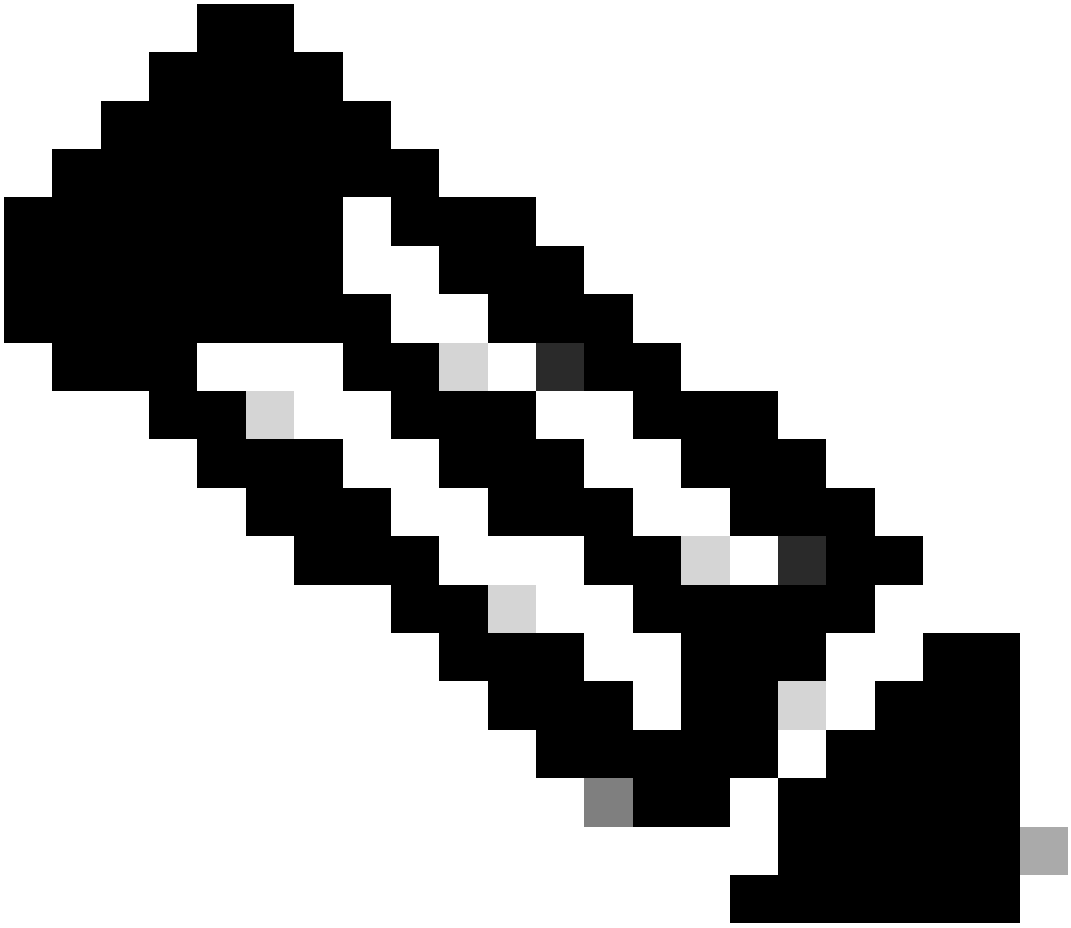
通过FMC在FTD上进行配置

注册IdP证书：

导航到FMC中的证书管理部分，并为两个SAML应用注册下载的Base64编码的IdP证书。这些证书对于建立信任和启用SAML身份验证至关重要。

有关详细指导，请参阅以下网址上提供的思科文档中“通过FMC在FTD上进行配置”下的前两个步骤：在通过FMC管理的FTD上配置具有SAML身份验证的安全客户端。


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



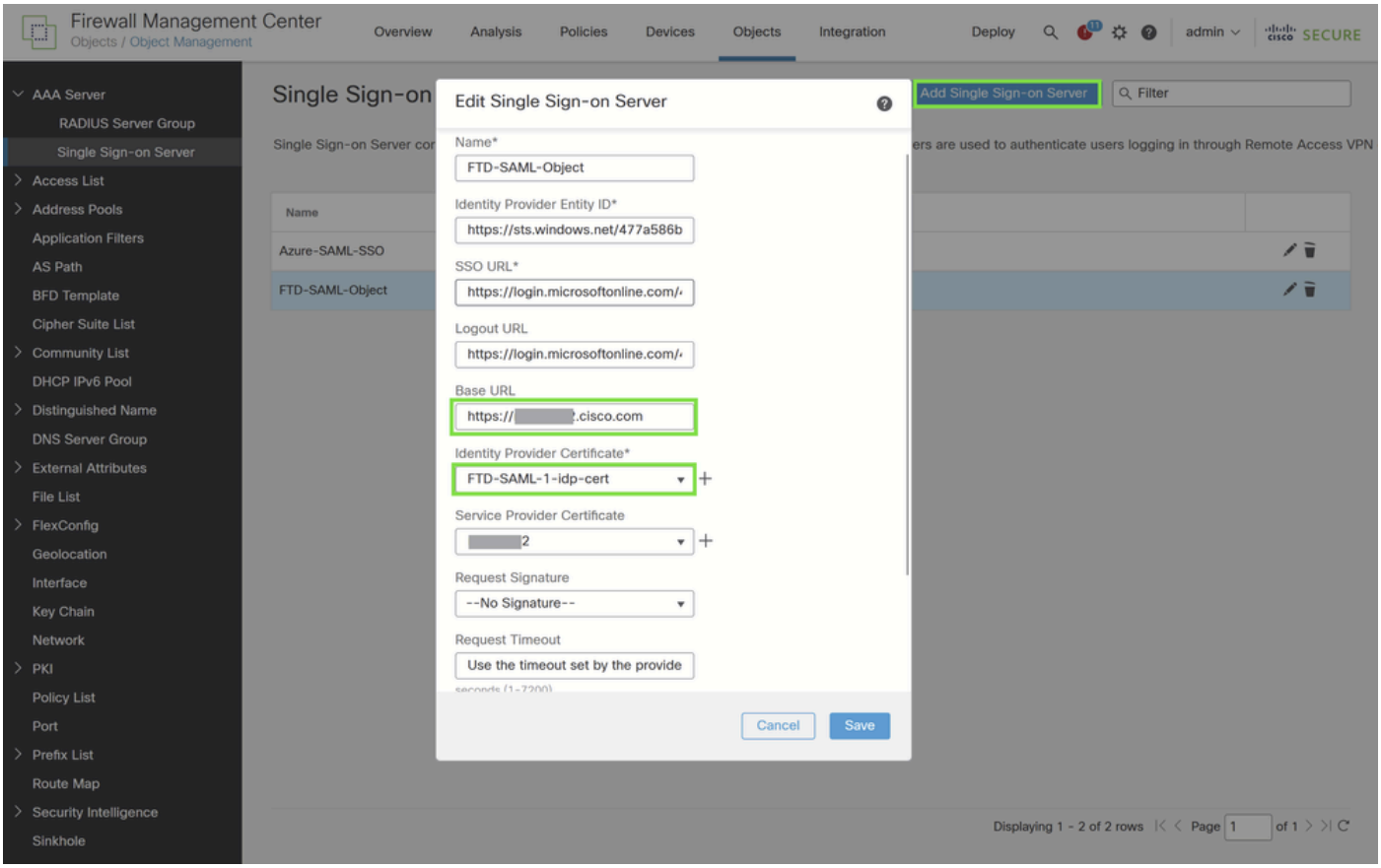
注意：图像已经过编辑，可以同时显示两个证书，以便更好地查看。无法在FMC上同时打开两个证书。

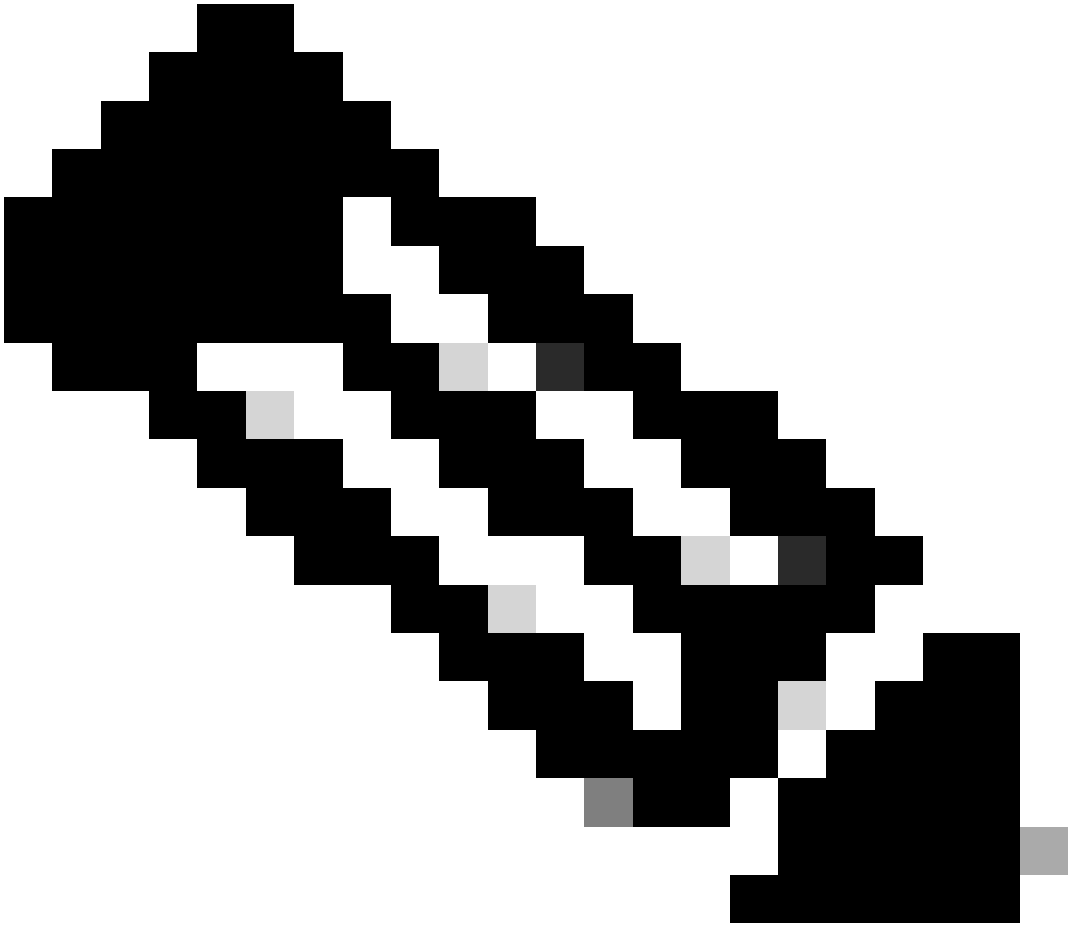
通过FMC在思科FTD上配置SAML服务器设置

要使用Firepower管理中心(FMC)在思科Firepower威胁防御(FTD)上配置SAML服务器设置，请执行以下步骤：

1. 导航至Single Sign-on Server Configuration:
   - 导航到对象>对象管理> AAA服务器>单点登录服务器。
   - 单击Add Single Sign-on Server开始配置新服务器。
2. 配置SAML服务器设置：
   - 使用从SAML企业应用程序或从身份提供程序(IdP)下载的metadata.xml文件中收集的参数，在New Single Sign-on Server表单中填写必要的SAML值。
   - 要配置的关键参数包括：
     - SAML提供程序实体ID:metadata.xml中的entityID
     - SSO URL:来自metadata.xml的SingleSignOnService。

- 注销URL:来自metadata.xml的SingleLogoutService。
- 基本URL:FTD SSL ID证书的FQDN。
- 身份提供程序证书：IdP签名证书。
  - 在Identity Provider Certificate部分下，附加一个已注册的IdP证书
  - 在本使用案例中，我们使用来自FTD-SAML-1应用的IdP证书。
- 服务提供商证书：FTD签名证书。



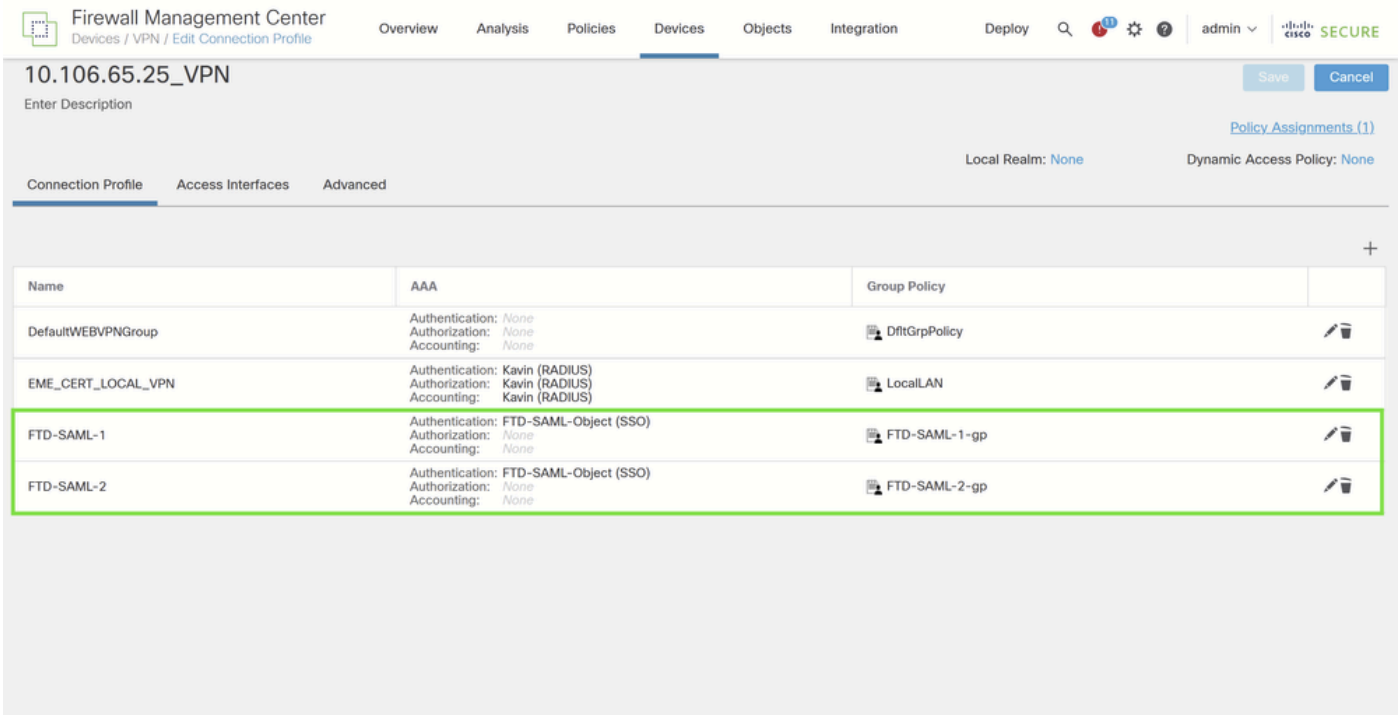


注意：在当前配置中，只能从连接配置文件设置中的SAML对象覆盖身份提供程序证书。遗憾的是，“登录时请求IDp重新身份验证”(Request IdP re-authentication on login)和“仅在内部网络中启用IDp可访问”(Enable IdP only accessible on internal network)等功能无法为每个连接配置文件单独启用或禁用。

通过FMC在思科FTD上配置连接配置文件

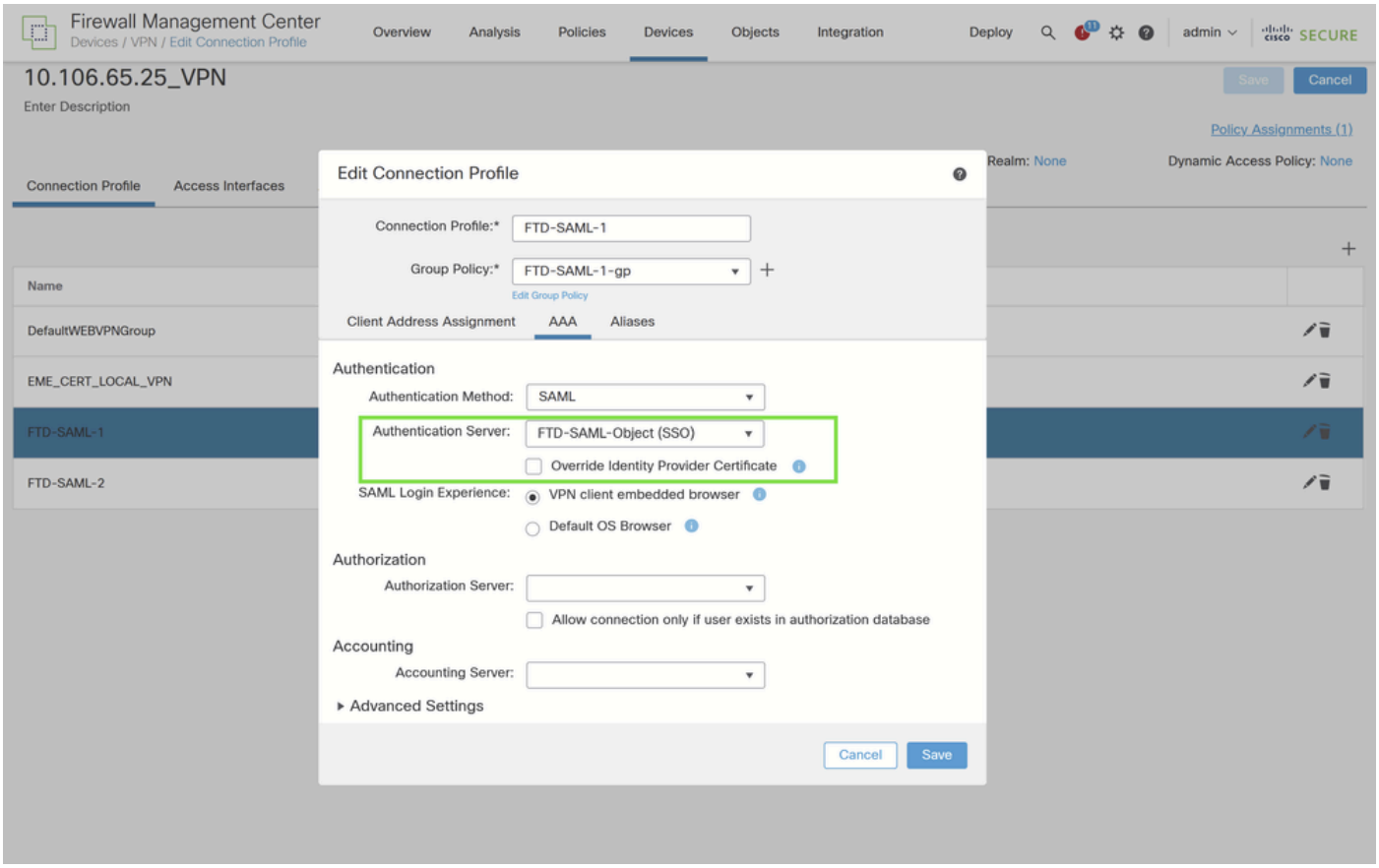
要完成SAML身份验证设置，您需要使用适当的参数配置连接配置文件，并使用先前配置的SAML服务器将AAA身份验证设置为SAML。

有关更详细的指导，请参阅思科文档中“通过FMC配置FTD”下的第五步：在通过FMC管理的FTD上配置具有SAML身份验证的安全客户端。



提取第一个连接配置文件的AAA配置

以下是第一个连接配置文件的AAA配置设置的概述：

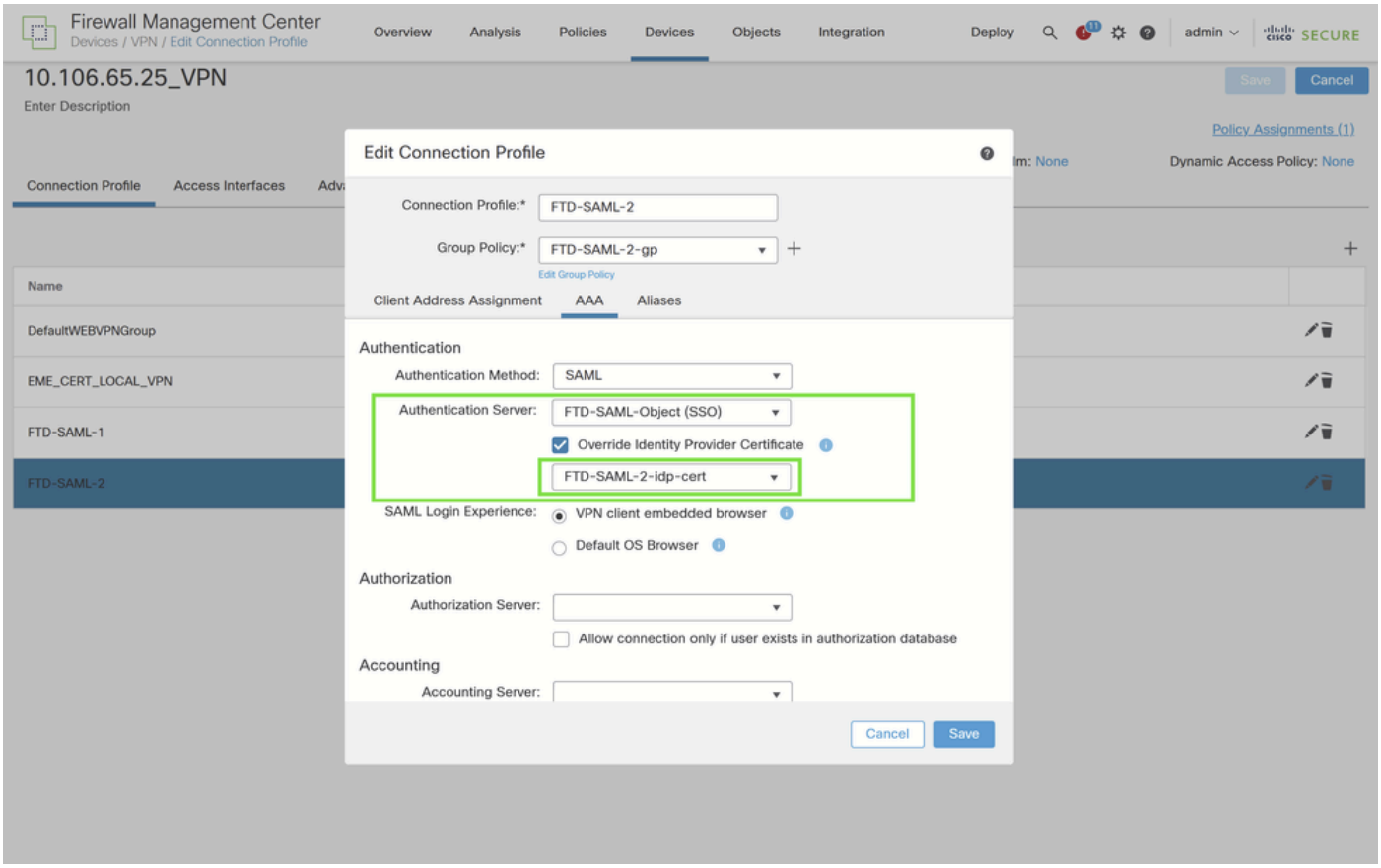


为思科FTD上的第二个连接配置文件配置IdP证书覆盖

要确保将正确的身份提供程序(IdP)证书用于第二个连接配置文件，请完成以下步骤以启用IdP证书覆盖：

在连接配置文件设置中，找到并启用选项“Override Identity Provider Certificate”，以允许使用与SAML服务器配置的IdP证书不同的证书。

从已注册IdP证书列表中，选择专门为FTD-SAML-2应用注册的证书。此选项可确保当为此连接配置文件发出身份验证请求时，使用正确的IdP证书。



配置部署

导航**Deploy** > **Deployment**至并选择适当的FTD以应用SAML身份验证VPN更改。

验证

FTD命令行上的配置

<#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>

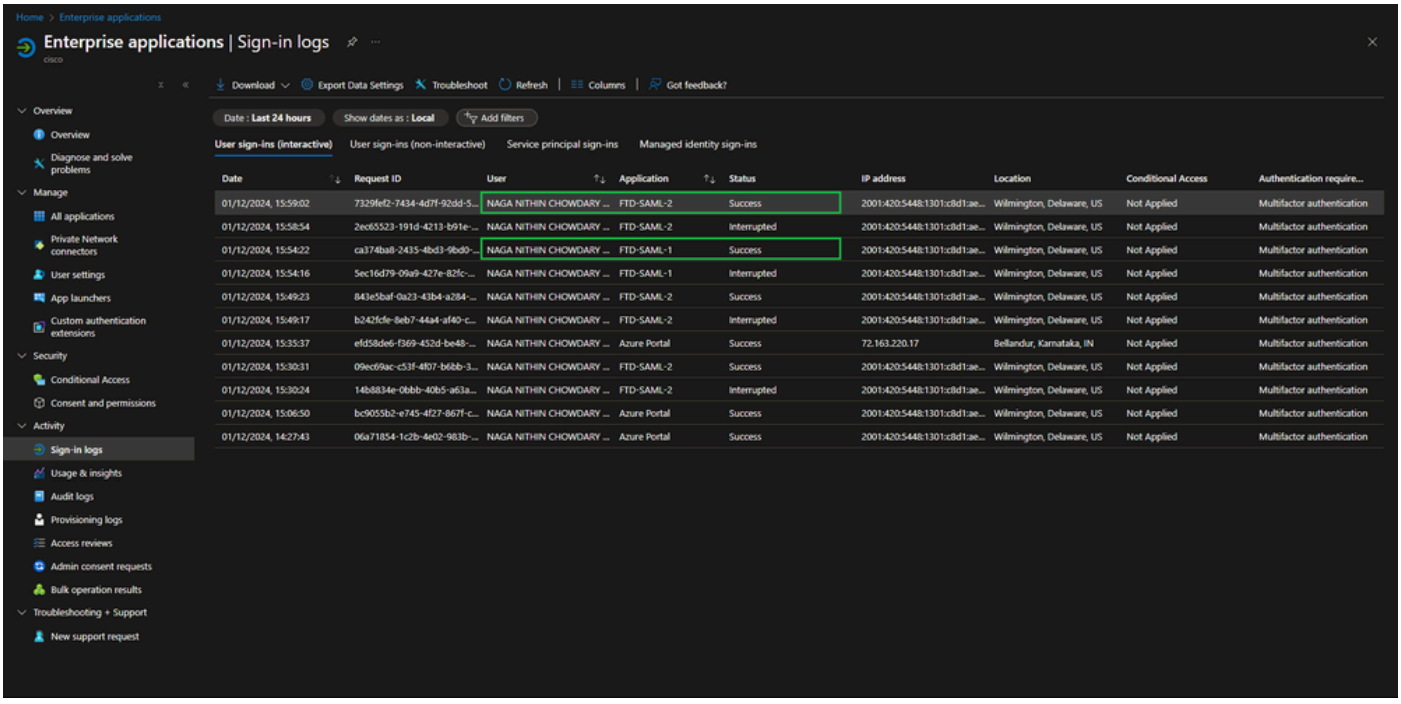
```
firepower# sh run tunnel-group FTD-SAML-1
tunnel-group FTD-SAML-1 type remote-access
tunnel-group FTD-SAML-1 general-attributes
    address-pool secure-client-pool
    default-group-policy FTD-SAML-1-gp
tunnel-group FTD-SAML-1 webvpn-attributes
    authentication saml
    group-alias FTD-SAML-1 enable


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#
```

从Azure entra标识符登录日志

访问enterprise application下的Sign-in Logs部分。查找与特定连接配置文件(例如FTD-SAML-1和FTD-SAML-2)相关的身份验证请求。验证用户是否正在通过与每个连接配置文件关联的SAML应用程序成功进行身份验证。



Azure IdP上的登录日志

故障排除

1. 您可以从安全客户端用户PC使用DART进行故障排除。
2. 要对SAML身份验证问题进行故障排除，请使用以下调试：

```
<#root>
firepower#
```

```
debug webvpn saml 255
```

3. 按照上述说明验证安全客户端配置；此命令可用于检查证书。

```
<#root>
firepower#
show crypto ca certificate
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。