Configurar SAML Auth para vários perfis de conexão RAVPN no FTD

Contents

Introdução

Este documento descreve a Autenticação SAML com o provedor de identidade do Azure para vários perfis de conexão no Cisco FTD gerenciado pelo FMC.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Configuração segura do cliente no firewall de próxima geração (NGFW) gerenciado pelo Firepower Management Center (FMC)
- Valores SAML e metatada.xml

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Threat Defense (FTD) versão 7.4.0
- FMC versão 7.4.0
- ID do Azure Microsoft Entra com SAML 2.0
- Cisco Secure Client 5.1.7.80

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Esta configuração permite que o FTD autentique usuários de cliente seguro usando dois aplicativos SAML diferentes no idp do Azure com um único objeto SAML configurado no 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://

Em um ambiente do Microsoft Azure, vários aplicativos podem compartilhar a mesma ID de entidade. Cada aplicativo, normalmente mapeado para um grupo de túneis diferente, necessita de um certificado exclusivo, exigindo a configuração de vários certificados dentro da configuração IdP do lado do FTD em um único objeto IdP SAML. No entanto, o Cisco FTD não suporta a configuração de vários certificados em um objeto SAML IdP, conforme detalhado no bug da Cisco ID CSCvi29084.

Para superar essa limitação, a Cisco introduziu o recurso de substituição de certificado IdP, disponível no FTD versão 7.1.0 e no ASA versão 9.17.1. Esse aprimoramento oferece uma solução permanente para o problema e complementa as soluções alternativas existentes descritas no relatório de erros.

Configurações

Esta seção descreve o processo para configurar a autenticação SAML com o Azure como o provedor de identidade (IdP) para vários perfis de conexão no Cisco Firepower Threat Defense (FTD) gerenciado pelo Firepower Management Center (FMC). O recurso de substituição de certificado IdP é utilizado para configurar isso de forma eficaz.

Visão geral sobre a configuração:

Dois perfis de conexão devem ser configurados no Cisco FTD:

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

Neste exemplo de configuração, o URL do gateway de VPN (FQDN do Cisco Secure Client) está definido como nigarapa2.cisco.com

Configurar

Configuração no IdP do Azure

Para configurar seus aplicativos empresariais SAML para o Cisco Secure Client de forma eficaz,

certifique-se de que todos os parâmetros estejam definidos corretamente para cada grupo de túneis, concluindo estas etapas:

- Acessar SAML Enterprise Applications:

  Navegue até o console administrativo do provedor SAML onde os aplicativos empresariais estão listados.

- Selecione o aplicativo SAML apropriado:

  Identifique e selecione as aplicações SAML correspondentes aos grupos de túneis do Cisco Secure Client que você pretende configurar.

- Configure o Identificador (ID da Entidade):

  Defina o Identificador (ID da Entidade) para cada aplicativo. Este deve ser o URL base, que é o seu FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) do Cisco Secure Client.

- Defina a URL de Resposta (URL do Serviço do Consumidor de Asserção):

  Configure a URL de Resposta (URL de Serviço do Consumidor de Asserção) usando a URL Base correta. Certifique-se de que ele esteja alinhado com o FQDN do Cisco Secure Client.

  Anexe o perfil de conexão ou o nome do grupo de túneis à URL base para garantir a especificidade.

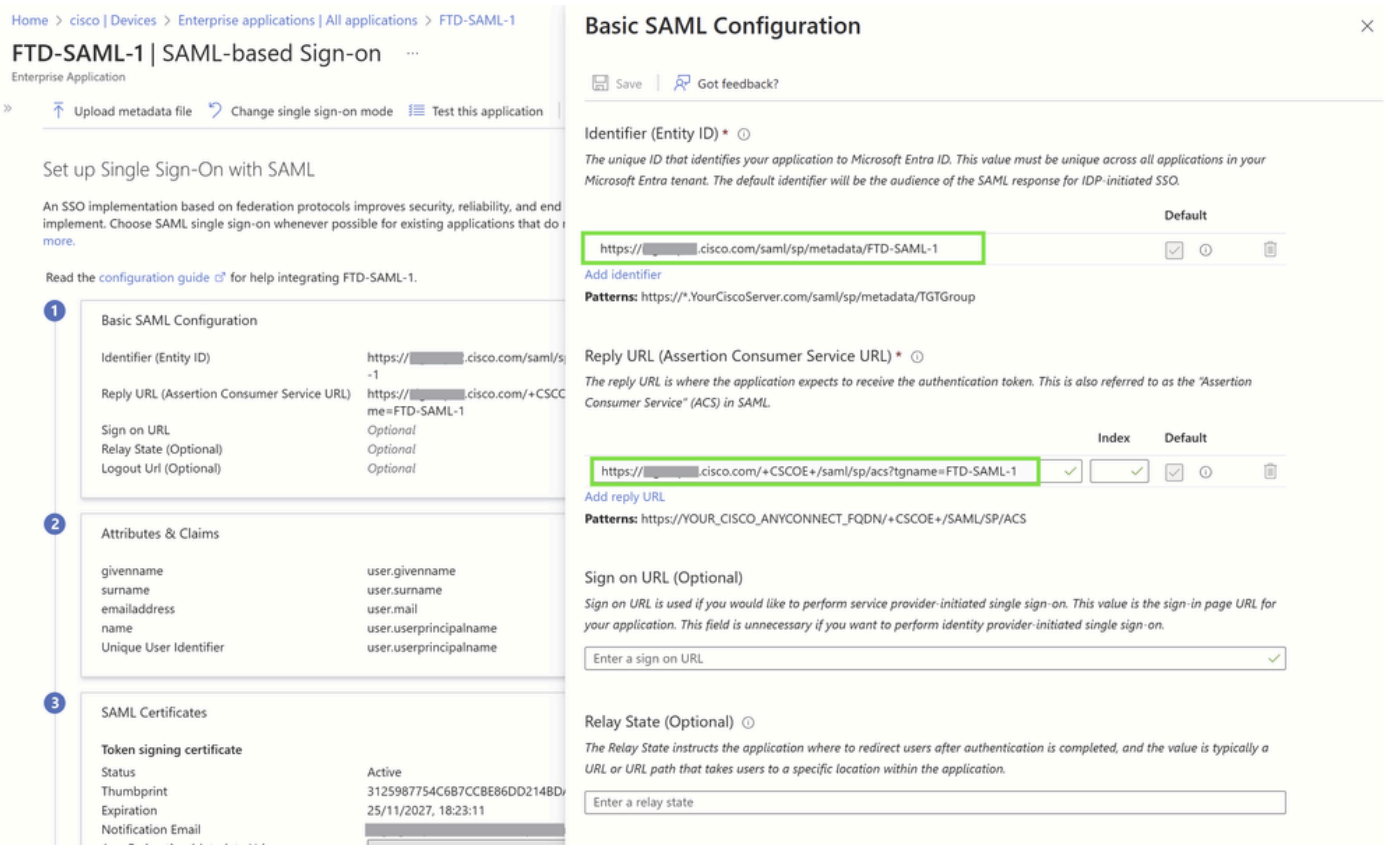
- Verificar configuração:

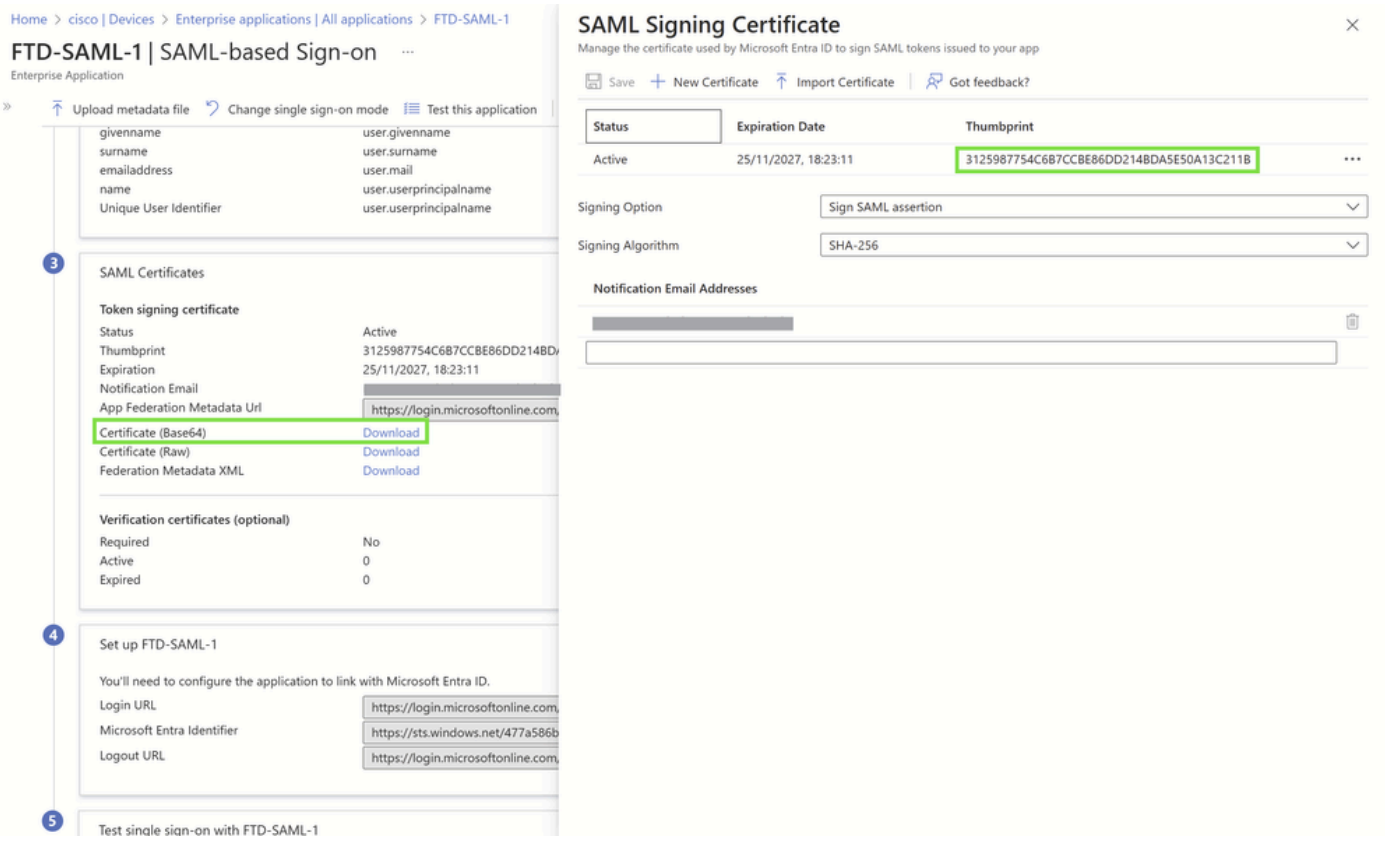
  Verifique se todos os URLs e parâmetros foram inseridos corretamente e correspondem aos respectivos grupos de túneis.

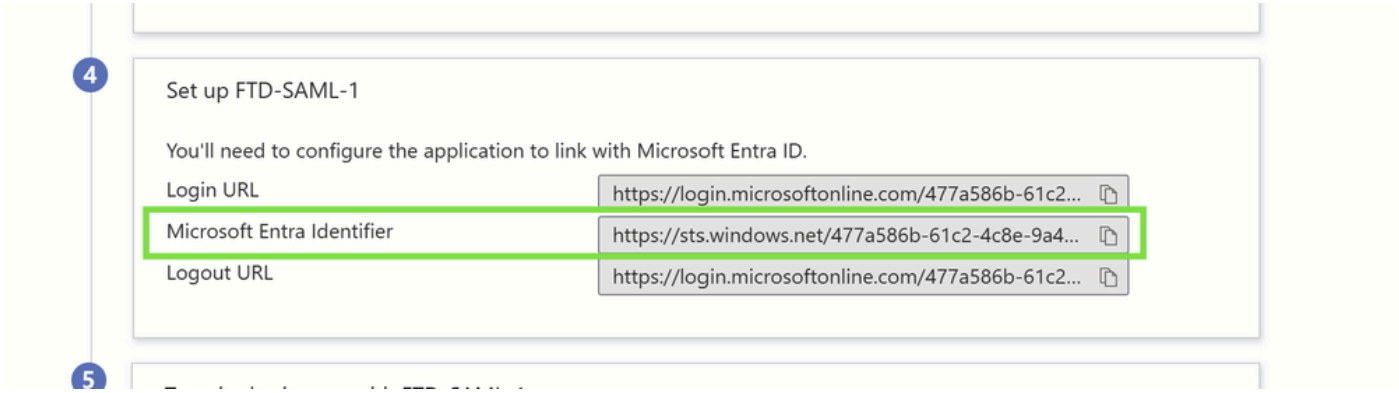
  Salve as alterações e, se possível, execute uma autenticação de teste para garantir que a configuração esteja funcionando conforme esperado.

Para obter orientação mais detalhada, consulte "Add Cisco Secure Client from the Microsoft App Gallery" na documentação da Cisco: Configurar o ASA Secure Client VPN com o Microsoft Azure MFA por meio de SAML

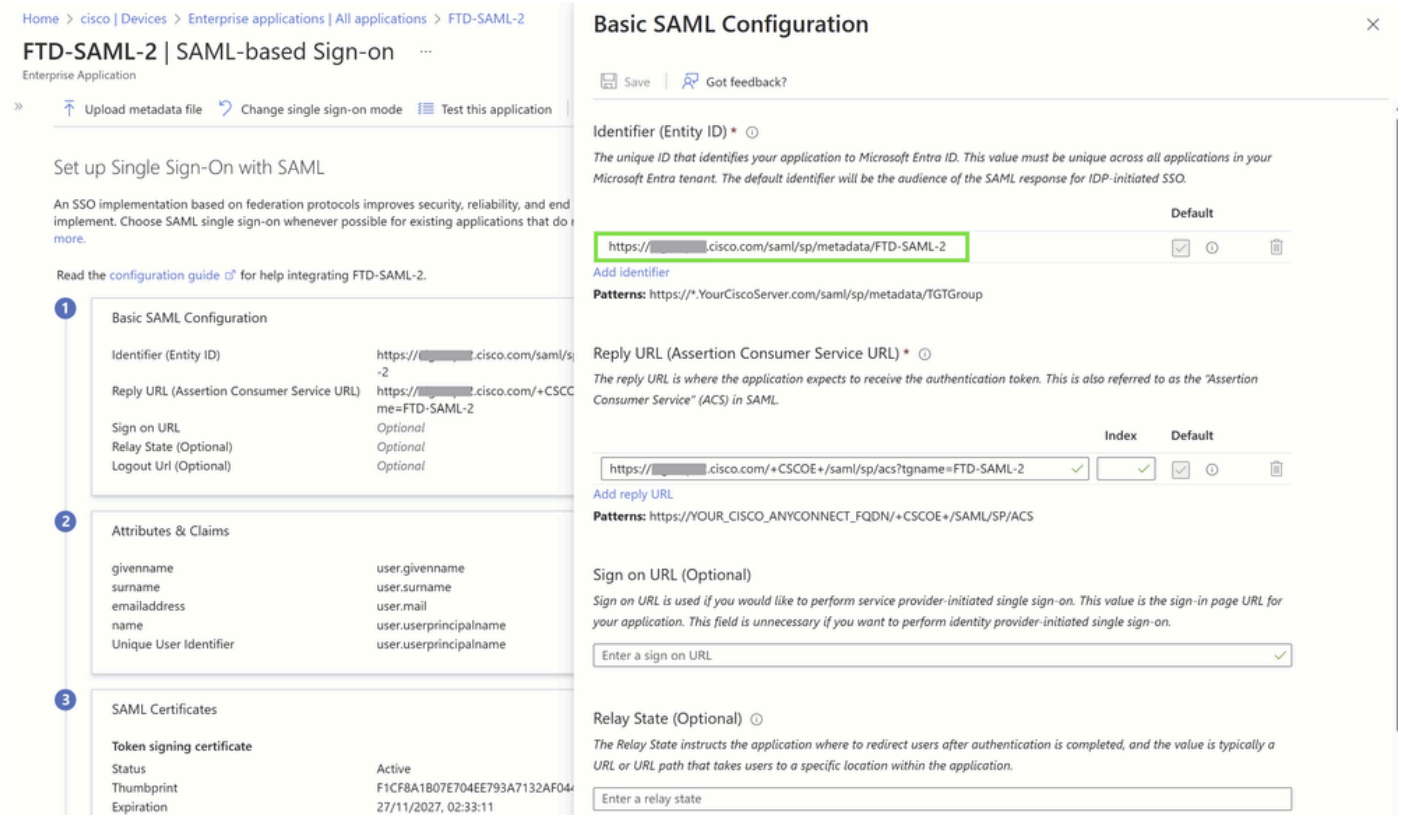
FTD-SAML-1

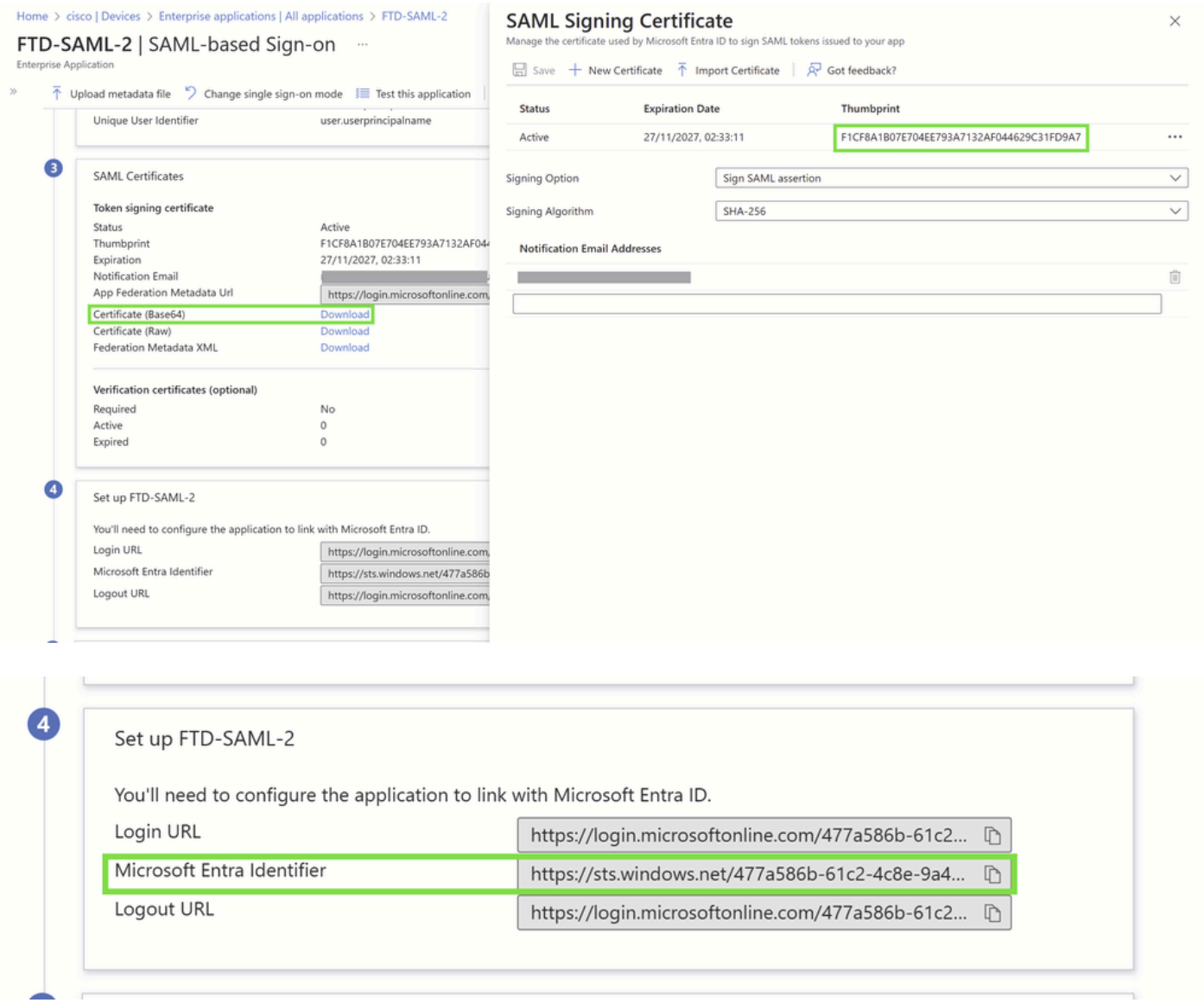

Home > cisco | Devices > Enterprise applications | All applications > FTD-SAML-1
FTD-SAML-1 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, 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-1.
1
Basic SAML Configuration
Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)
Sign on URL
Relay State (Optional)
Logout Url (Optional)
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
Active
Thumbprint
Expiration
25/11/2027, 18:23:11
Notification Email
Basic SAML Configuration
Save
Got feedback?
Identifier (Entity ID) *
The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.
Default
https://.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://.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


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
surname
emailaddress
name
Unique User Identifier
user.givenname
user.surname
user.mail
user.userprincipalname
user.userprincipalname
3
SAML Certificates
Token signing certificate
Status
Active
Thumbprint
Expiration
25/11/2027, 18:23:11
Notification Email
App Federation Metadata Url
https://login.microsoftonline.com/
Certificate (Base64)
Download
Certificate (Raw)
Download
Federation Metadata XML
Download
Verification certificates (optional)
Required
No
Active
0
Expired
0
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/
Microsoft Entra Identifier
https://sts.windows.net/477a586b
Logout URL
https://login.microsoftonline.com/
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
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
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
.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
.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



Agora, certifique-se de que você tenha as informações e os arquivos necessários para configurar a autenticação SAML com o Microsoft Entra como seu provedor de identidade:

Localize o Identificador do Microsoft Entra:

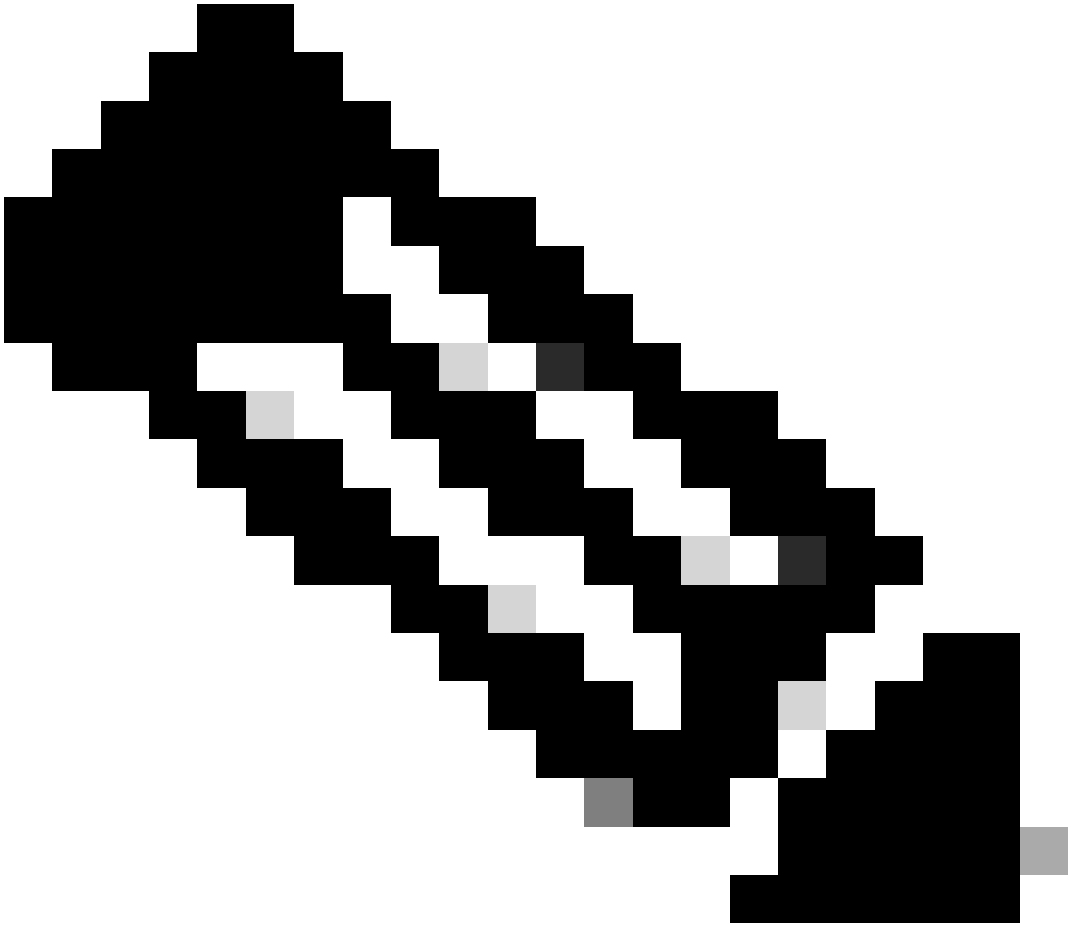
Acesse as configurações para ambos os aplicativos corporativos SAML no portal do Microsoft Entra.

Observe o Microsoft Entra Identifier, que permanece consistente em ambos os aplicativos e é crucial para a sua configuração SAML.

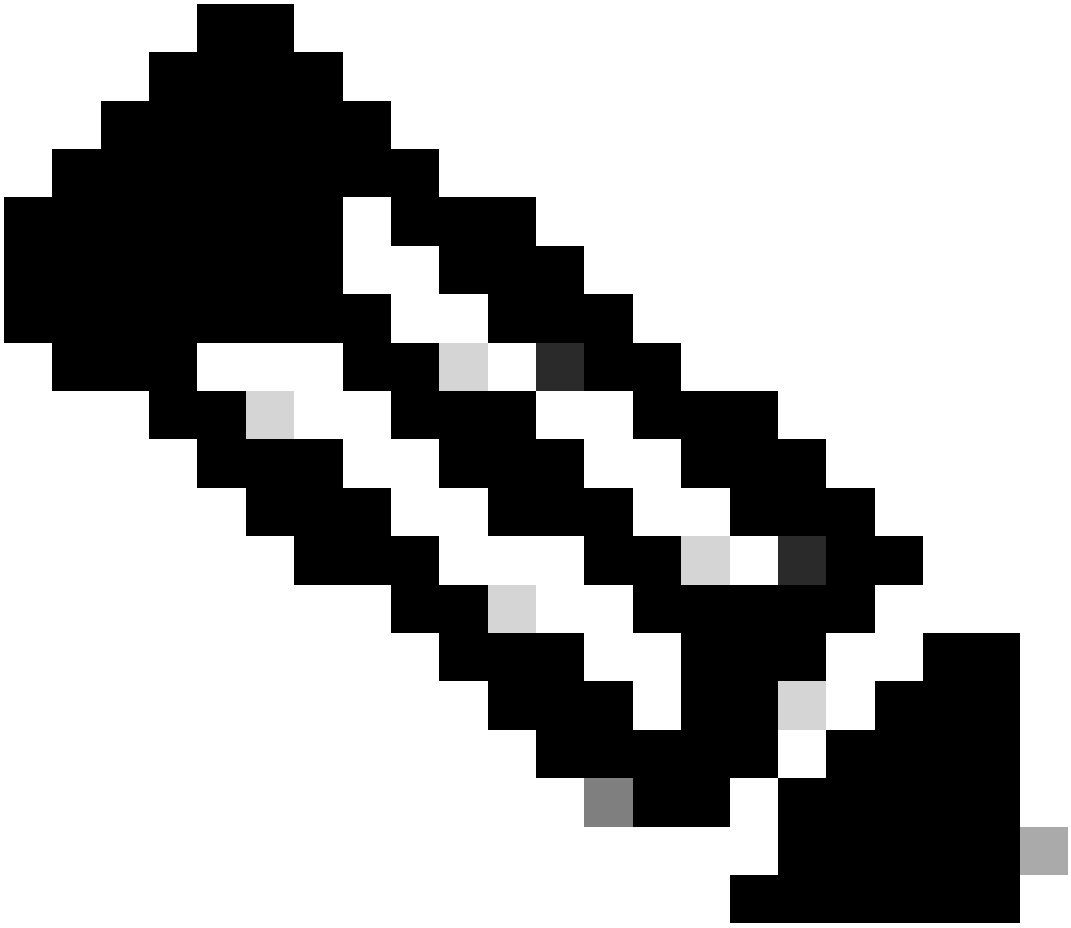
Fazer download de certificados IdP Base64:

Navegue até cada aplicativo corporativo SAML configurado.

Baixe os respectivos certificados IdP codificados na Base64. Esses certificados são essenciais para estabelecer a confiança entre o provedor de identidade e a configuração da VPN Cisco.



Note: Todas essas configurações SAML necessárias para os perfis de conexão FTD também podem ser originadas dos arquivos metadata.xml fornecidos pelo seu IdP para as respectivas aplicações.



Note: Para usar um certificado IdP personalizado, você precisa carregar o certificado IdP gerado de forma personalizada para o IdP e o FMC. Para o Azure IdP, verifique se o certificado está no formato PKCS#12. No FMC, carregue somente o certificado de identidade do IdP, não o arquivo PKCS#12. Para obter instruções detalhadas, consulte a seção "Carregar o arquivo PKCS#12 no Azure e no FDM" na documentação da Cisco: Configurar Vários Perfis RAVPN com Autenticação SAML no FDM

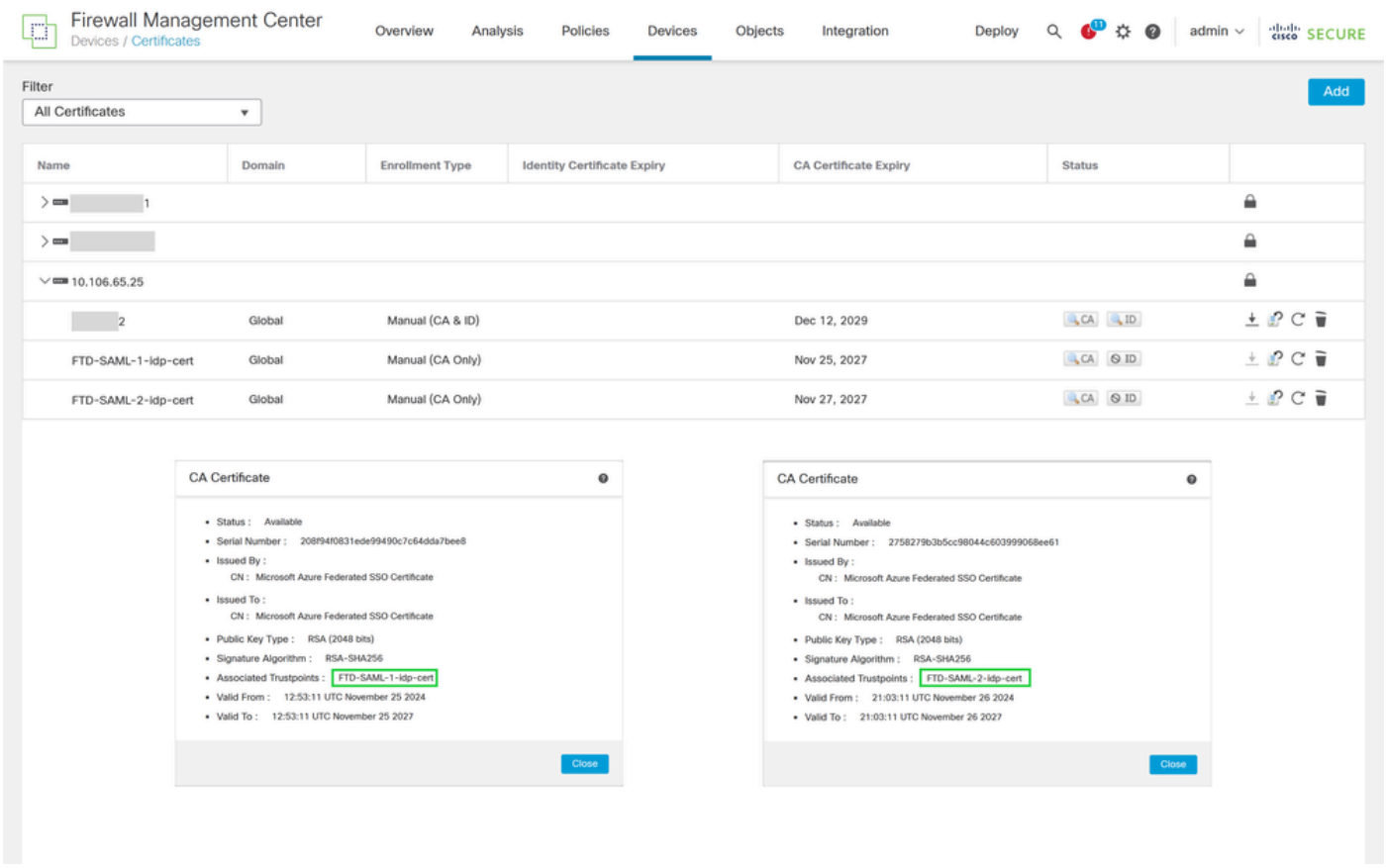
Configuração no FTD via FMC

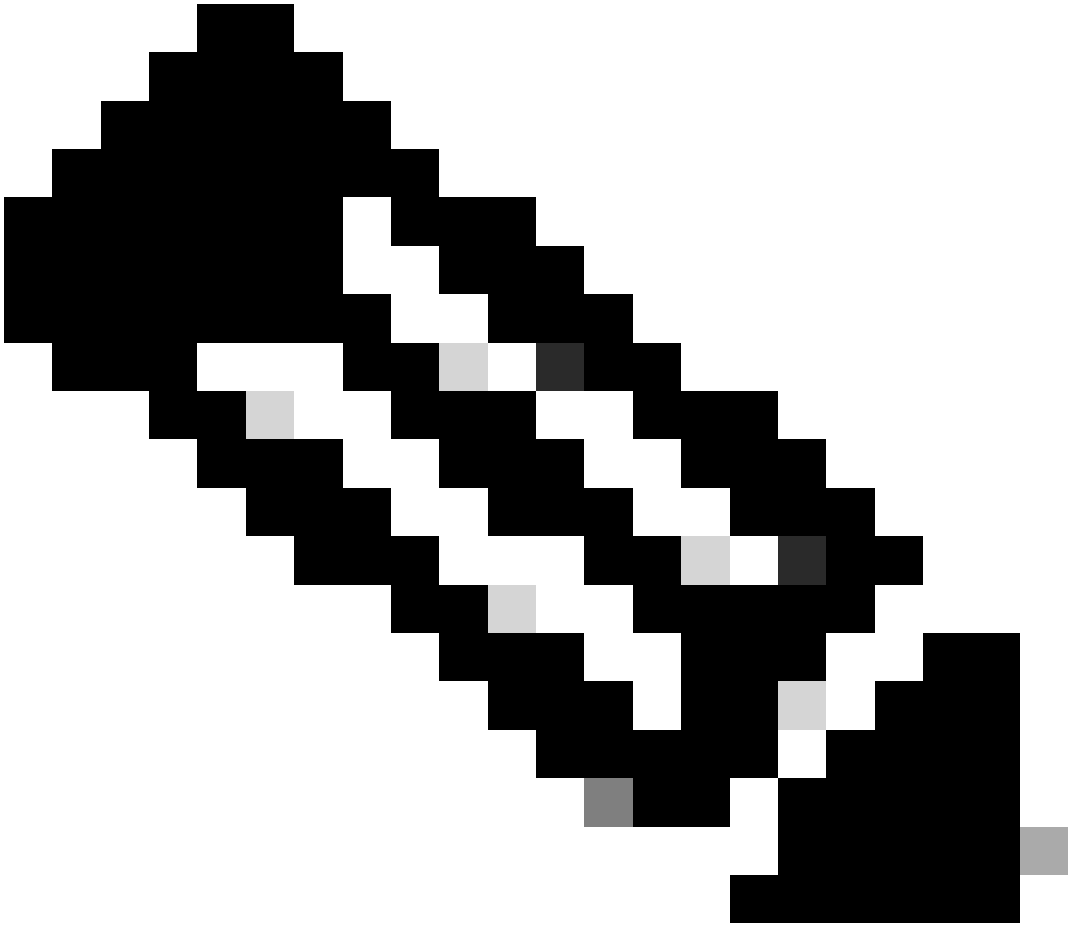
Registrar certificados IdP:

Navegue para a seção de gerenciamento de certificados no FMC e registre os certificados IdP codificados na Base64 baixados para ambos os aplicativos SAML. Esses certificados são vitais para estabelecer confiança e habilitar a autenticação SAML.

Para obter orientação detalhada, consulte as duas primeiras etapas em "Configuração no FTD via FMC" na documentação da Cisco disponível em: Configure o cliente seguro com autenticação

SAML no FTD gerenciado via FMC.





Note: A imagem foi editada para exibir os dois certificados simultaneamente para melhor visualização. Não é possível abrir os dois certificados ao mesmo tempo no CVP.

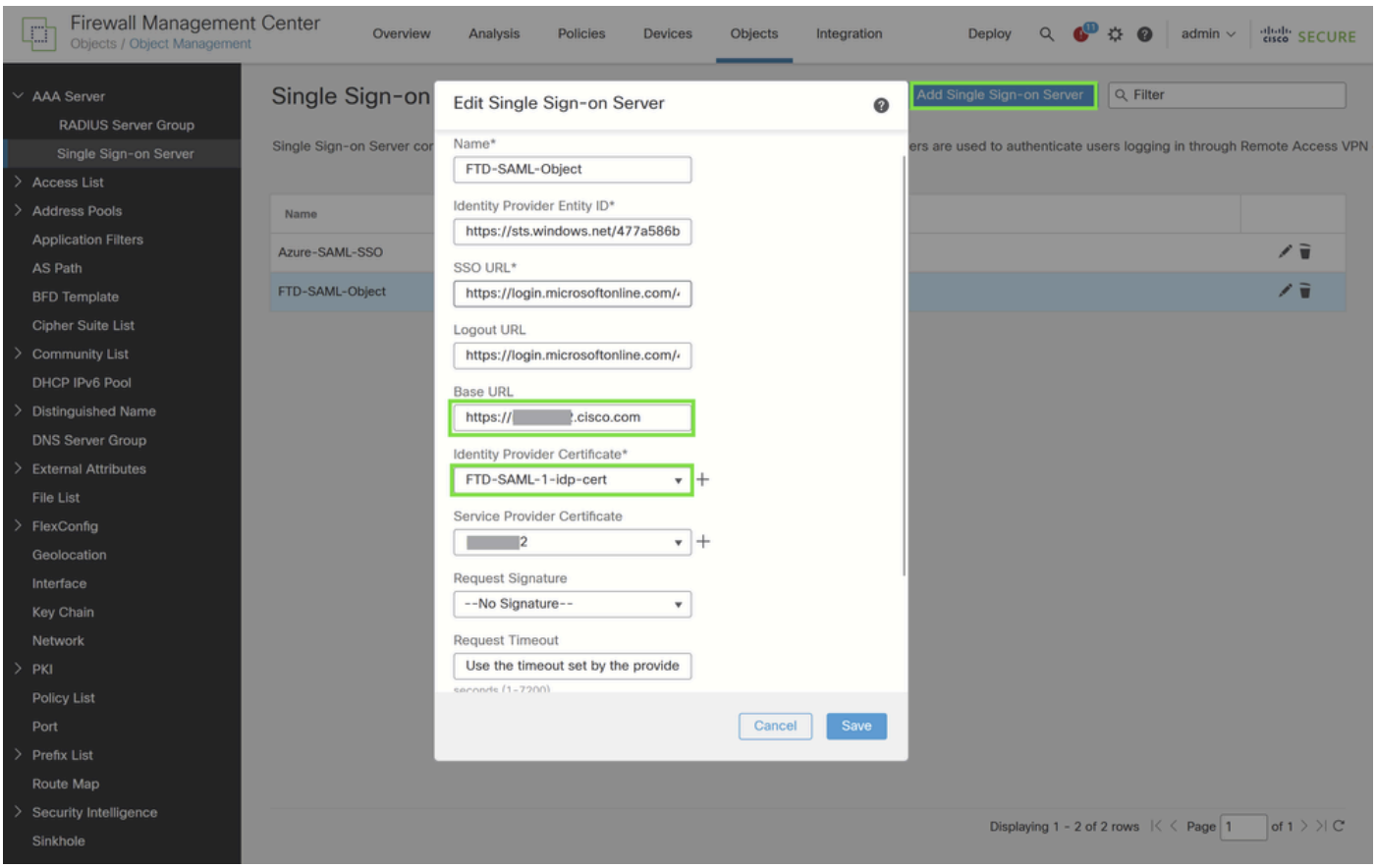
Definindo as configurações do servidor SAML no Cisco FTD via FMC

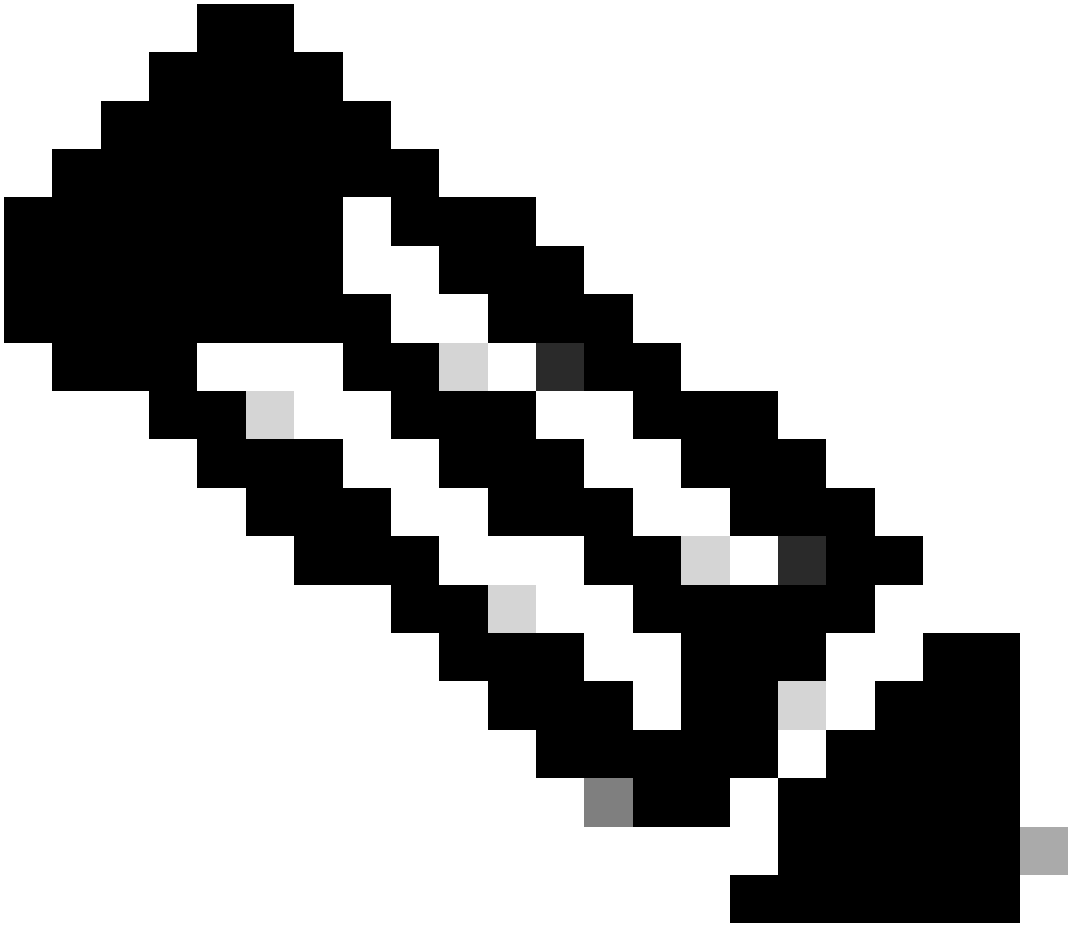
Para definir as configurações do servidor SAML no Cisco Firepower Threat Defense (FTD) usando o Firepower Management Center (FMC), execute estas etapas:

1. Navegue até Configuração do Servidor de Signon Único:
    - Navegue até Objects > Object Management > AAA Servers > Single Sign-on Server.
    - Clique em Adicionar Servidor de Signon Único para começar a configurar um novo servidor.

2. Definir configurações do servidor SAML:
    - Usando os parâmetros coletados dos seus aplicativos empresariais SAML ou do arquivo metadata.xml baixado do seu Provedor de Identidade (IdP), preencha os valores SAML necessários no formulário Novo Servidor de Signon Único.
    - Os principais parâmetros a serem configurados incluem:

- ID da entidade do provedor SAML: entityID de metadata.xml
- URL SSO: SingleSignOnService a partir de metadata.xml.
- URL de logoff: SingleLogoutService de metadata.xml.
- URL BASE: FQDN do seu Certificado de ID SSL do FTD.
- Certificado do provedor de identidade: Certificado de assinatura IdP.
  - Na seção Identity Provider Certificate, anexe um dos certificados IdP registrados
  - Para este caso de uso, estamos usando o certificado IdP do aplicativo FTD-SAML-1.
- Certificado do provedor de serviços: Certificado de Autenticação FTD.



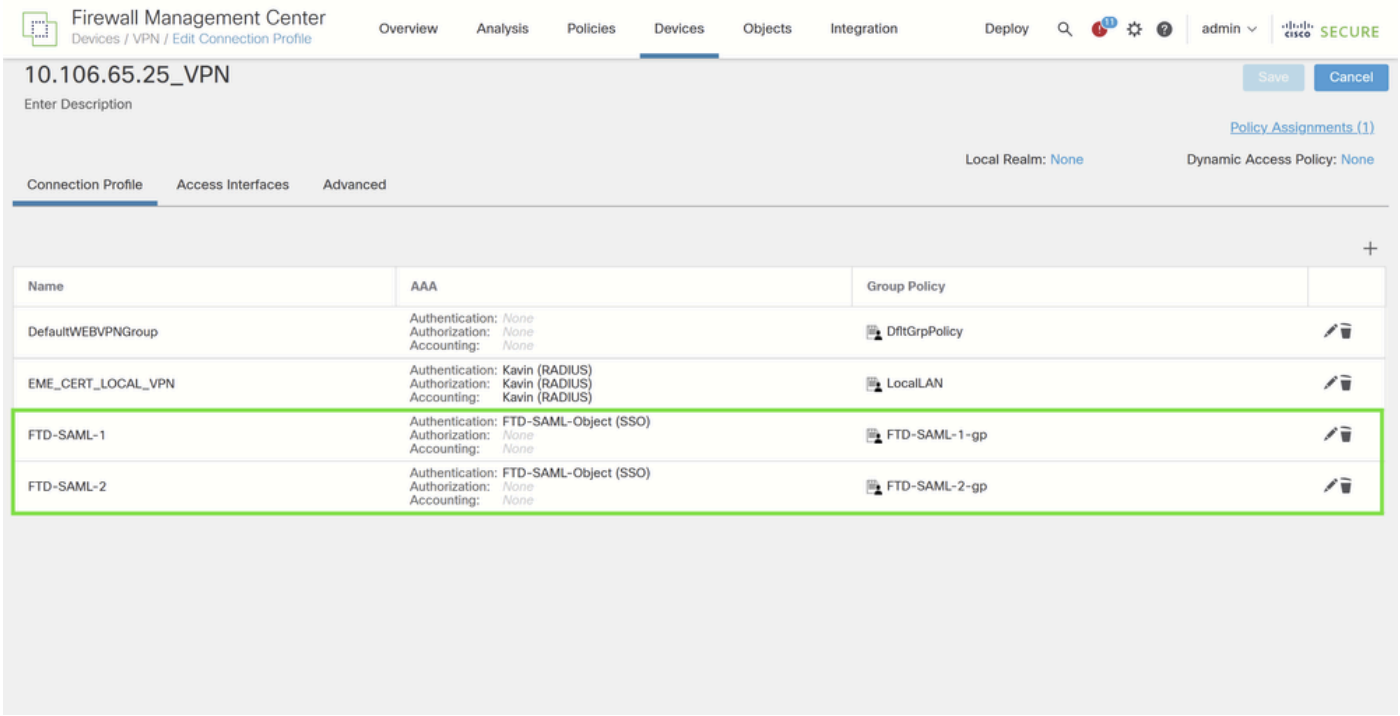


Note: Na configuração atual, somente o certificado do Provedor de Identidade pode ser substituído do objeto SAML nas configurações do perfil de conexão. Infelizmente, recursos como "Solicitar reautenticação do IdP no login" e "Ativar IdP acessível apenas na rede interna" não podem ser individualmente habilitados ou desabilitados para cada perfil de conexão.

Configuração de perfis de conexão no Cisco FTD via FMC

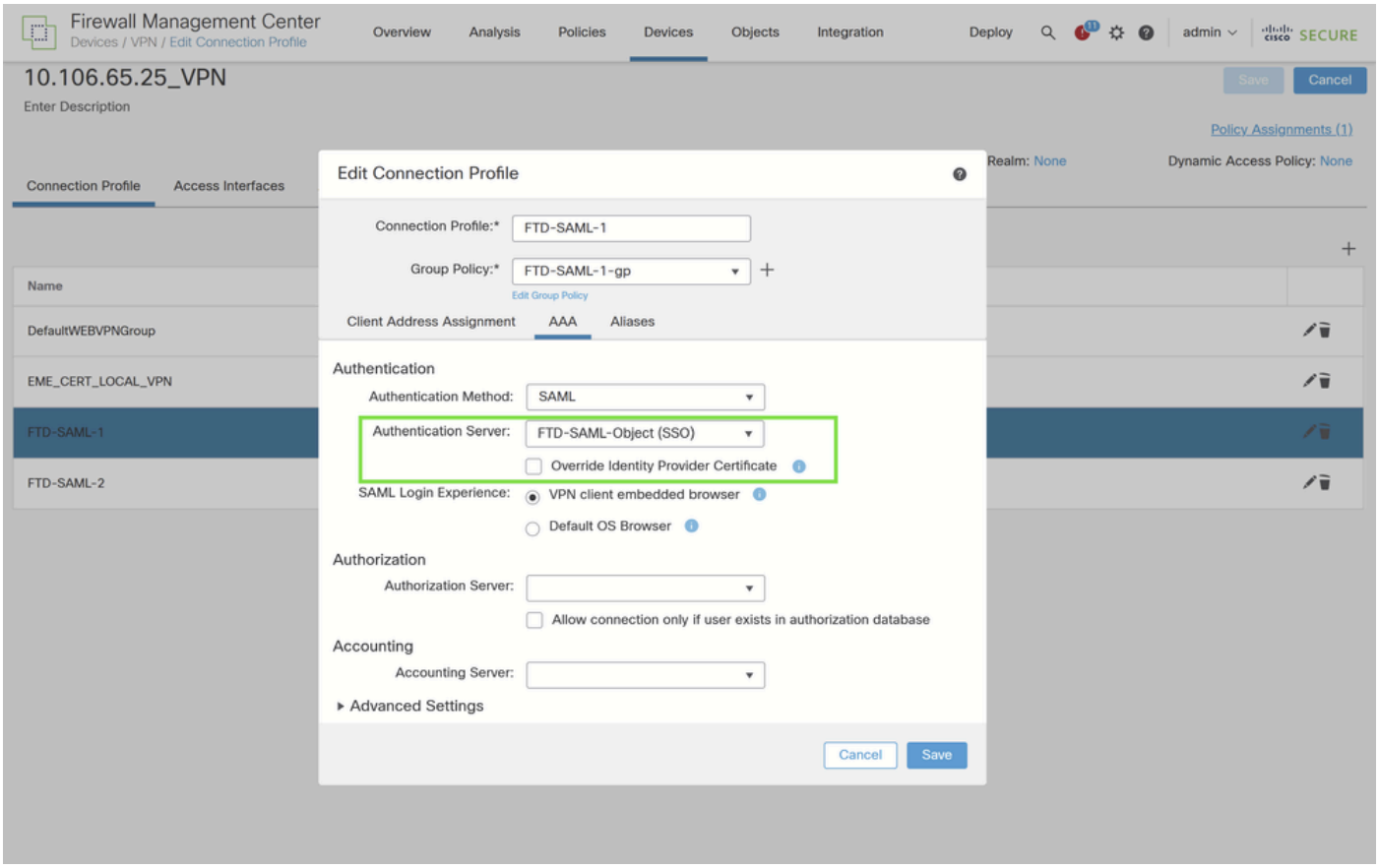
Para finalizar a configuração da autenticação SAML, você precisa configurar os perfis de conexão com os parâmetros apropriados e definir a autenticação AAA como SAML usando o servidor SAML configurado anteriormente.

Para obter orientação mais detalhada, consulte a quinta etapa em "Configuração no FTD via FMC" na documentação da Cisco: Configure o cliente seguro com autenticação SAML no FTD gerenciado via FMC.



Extrato de configuração AAA para o primeiro perfil de conexão

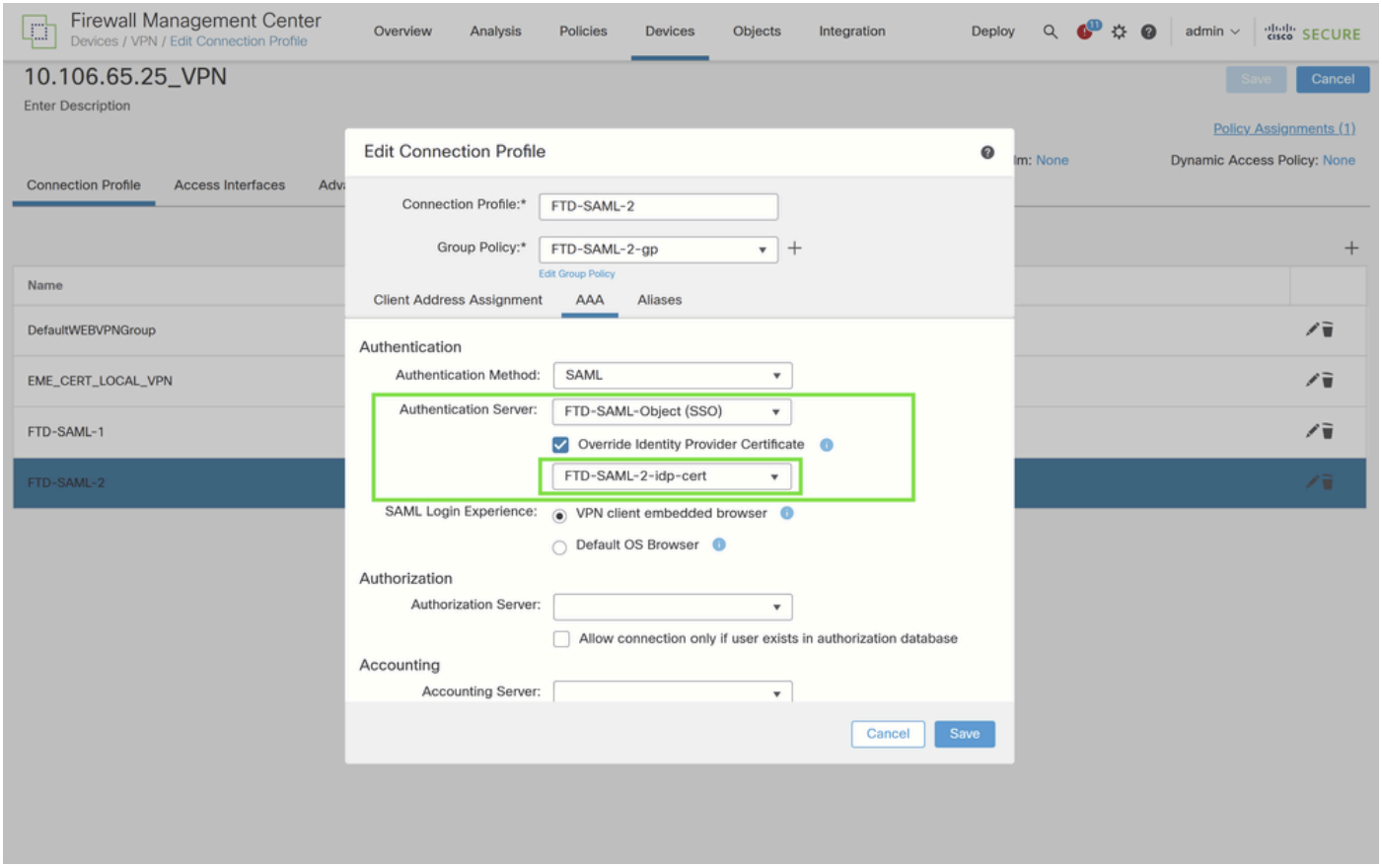
Esta é uma visão geral das definições de configuração de AAA para o primeiro perfil de conexão:



Configurando a substituição de certificado IdP para o segundo perfil de conexão no Cisco FTD
Para garantir que o certificado correto do Provedor de Identidade (IdP) seja usado para o segundo perfil de conexão, habilite a substituição do certificado IdP seguindo estas etapas:

Nas definições do perfil de conexão, localize e ative a opção "Sobrepor Certificado do Provedor de Identidade" para permitir o uso de um certificado IdP diferente daquele configurado para o servidor SAML.

Na lista de certificados IdP registrados, selecione o certificado especificamente registrado para o aplicativo FTD-SAML-2. Essa seleção garante que, quando uma solicitação de autenticação for feita para esse perfil de conexão, o certificado IdP correto seja usado.



Implantação da configuração

Navegue**Deploy** > **Deployment**para e selecione o FTD apropriado para aplicar as alterações de VPN de Autenticação SAML.

Verificar

Configuração na linha de comando do 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
```

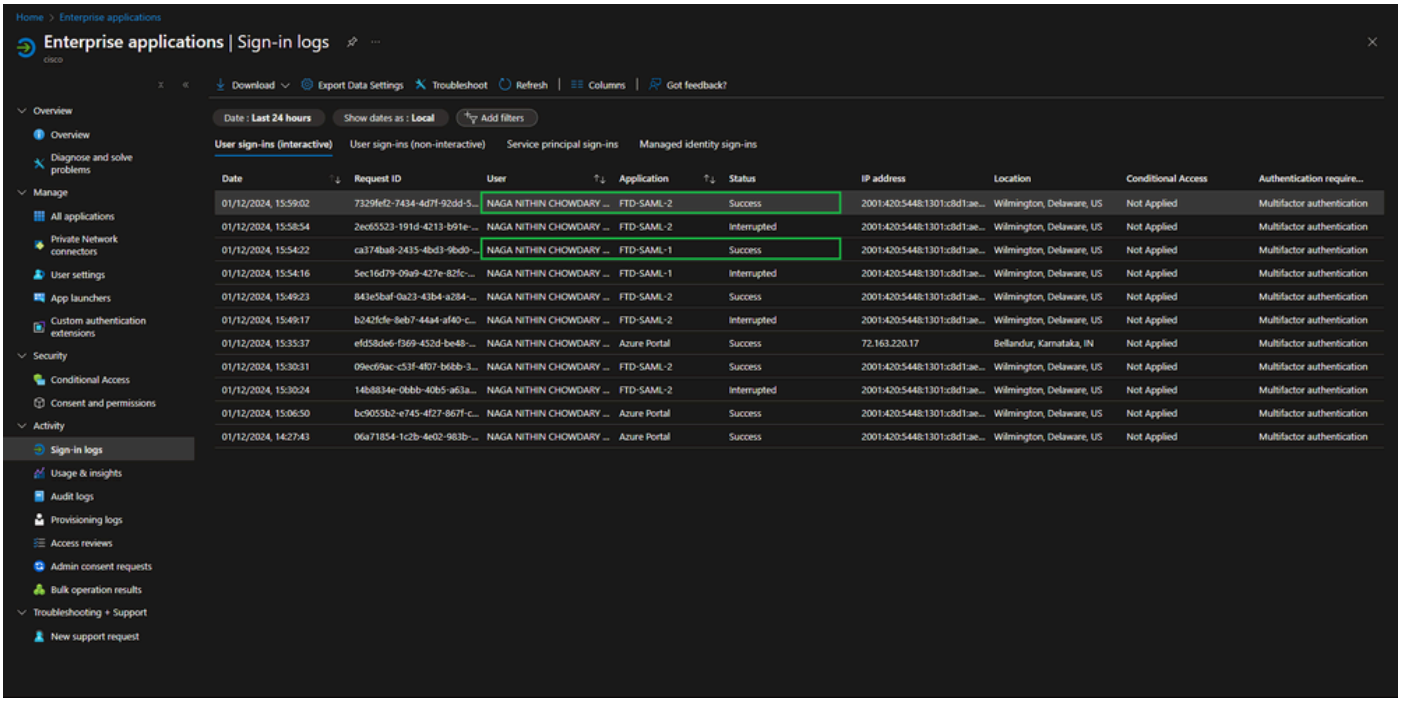
saml identity-provider https://sts.windows.net/477a586b-61c2-4c8e-9a41-1634016aa513/

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

```
firepower#
```

Logs de entrada do identificador de entrada do Azure

Acesse a seção Logs de início de sessão em aplicativo empresarial. Procure solicitações de autenticação relacionadas aos perfis de conexão específicos, como FTD-SAML-1 e FTD-SAML-2. Verifique se os usuários estão se autenticando com êxito por meio das aplicações SAML associadas a cada perfil de conexão.



Logs de Entrada no Azure IdP

Troubleshooting

1. Você pode solucionar problemas usando o DART no PC do usuário do Secure Client.
2. Para solucionar um problema de autenticação SAML, utilize este comando debug:

<#root>

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

3. Verifique a configuração do Secure Client conforme explicado acima; esse comando pode ser usado para verificar o certificado.

<#root>

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.