

Configurar Atribuição de Política de Grupo para SAML Usando Firewall Seguro e ID do Microsoft Entra

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configuração SAML do FMC](#)

[Configuração do grupo de túneis FMC RAVPN](#)

[Configuração da política de grupo FMC RAVPN](#)

[Metadados de FTD](#)

[ID do Microsoft Entra](#)

[Verificar](#)

[FTD](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como atribuir políticas de grupo usando o Microsoft Entra ID para autenticação SAML do Cisco Secure Client no Cisco Secure Firewall.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Cisco Secure Client AnyConnect VPN
- Configuração de objeto de servidor do Cisco Firepower Threat Defense (FTD) ou Cisco Secure Firewall ASA de acesso remoto VPN e Single Sign-on (SSO)
- Configuração do Provedor de Identidade (IdP) do Microsoft Entra ID

Componentes Utilizados

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

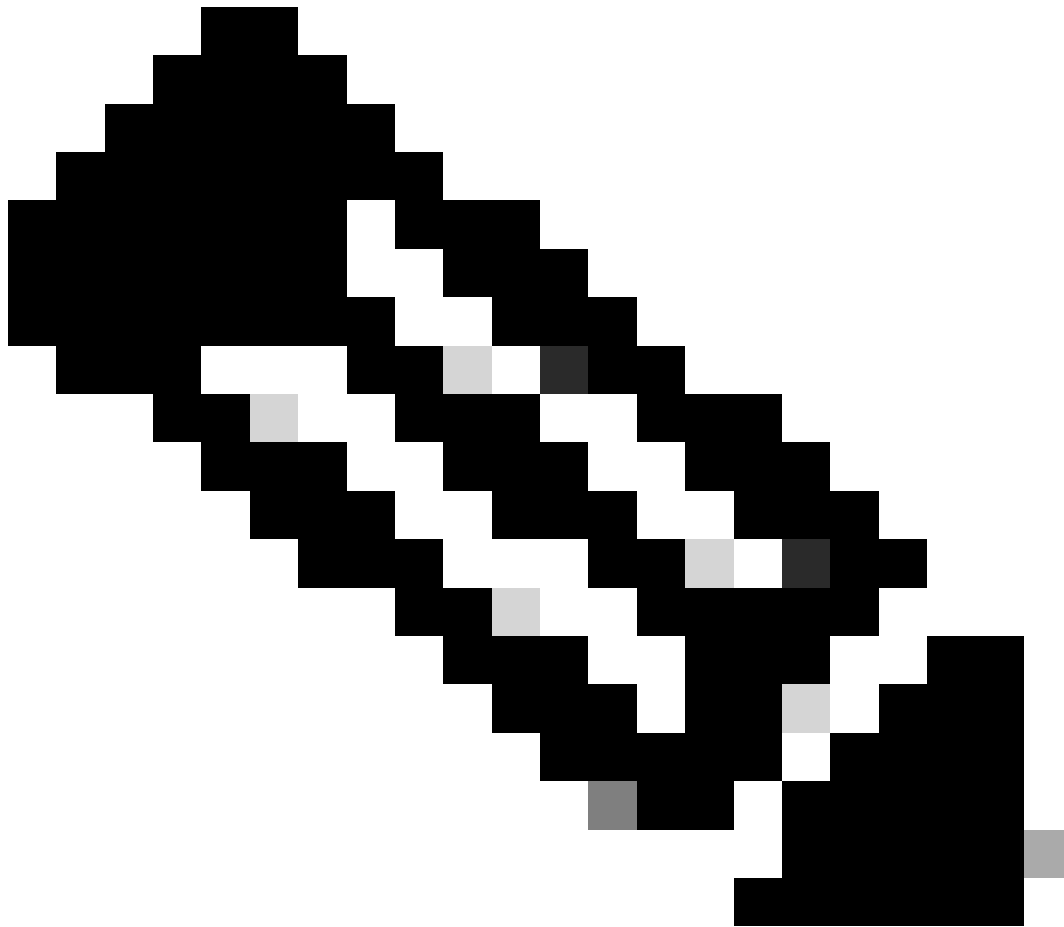
- FTD versão 7.6
- FMC versão 7.6
- IdP SAML do MS Entra ID

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

SAML (Security Assertion Markup Language) é uma estrutura baseada em XML para troca de dados de autenticação e autorização entre domínios de segurança. Ele cria um círculo de confiança entre o usuário, um provedor de serviços (SP) e um provedor de identidade (IdP) que permite que o usuário entre uma única vez para vários serviços. O SAML pode ser usado para autenticação de VPN de acesso remoto para conexões do Cisco Secure Client com headends de VPN do ASA e do FTD, onde o ASA ou o FTD é a parte do SP do círculo de confiança.

Neste documento, o Microsoft Entra ID/Azure é usado como o IdP. No entanto, também é possível atribuir políticas de grupo usando outros IdPs, pois ele se baseia em atributos padrão que podem ser enviados na asserção SAML.



Note: Esteja ciente de que cada usuário deve pertencer somente a um grupo de usuários no MS Entra ID, pois vários atributos SAML sendo enviados ao ASA ou FTD podem causar problemas com a atribuição de política de grupo, conforme detalhado no ID de bug da Cisco CSCwm33613

Configurar

Configuração SAML do FMC

No FMC, navegue até Objects > Object Management > AAA Server > Single Sign-on Server. O certificado Entity ID, SSO URL, Logout URL e Identity Provider são obtidos do IdP, consulte a Etapa 6 na seção Microsoft Entra ID. O URL base e o certificado do provedor de serviços são específicos do FTD ao qual a configuração está sendo adicionada.

Edit Single Sign-on Server

Name*
SAMLtest

Identity Provider Entity ID*
https://sts.windows.net/af42ba...

SSO URL*
https://login.microsoftonline.co...

Logout URL
https://login.microsoftonline.co...

Base URL
https://vpn.example.com

Identity Provider Certificate*
SAMLtest +

Service Provider Certificate
+

Request Signature
--No Signature--

Request Timeout
Use the timeout set by the provi...

Cancel Save

Configuração do objeto SSO do FMC

Configuração do grupo de túneis FMC RAVPN

No FMC, navegue para **Devices > VPN > Remote Access > Connection Profile** e selecione ou crie a política de VPN para o FTD que você está configurando. Depois de selecionado, crie um perfil de conexão semelhante a este:

Edit Connection Profile

?

Connection Profile:*

SAMLtest

Group Policy:*

DfltGrpPolicy

+

Edit Group Policy

Client Address Assignment

AAA

Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools:

+

Name	IP Address Range	
SAML_pool	192.168.55.1-192.168.55.10	 

DHCP Servers:

+

Name	DHCP Server IP Address	

Cancel

Save

Atribuição de endereço de perfil de conexão FMC

Edit Connection Profile ?

Connection Profile:* SAMLtest

Group Policy:* DfltGrpPolicy +
[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: SAML

Authentication Server: SAMLtest (SSO)

☐ 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:

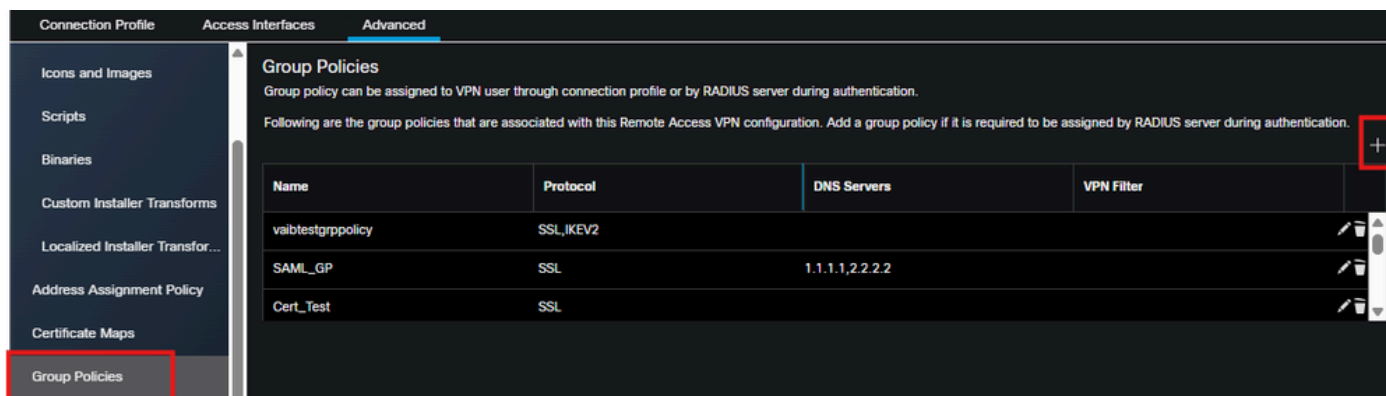
▶ Advanced Settings

Cancel Save

Configuração AAA do perfil de conexão FMC

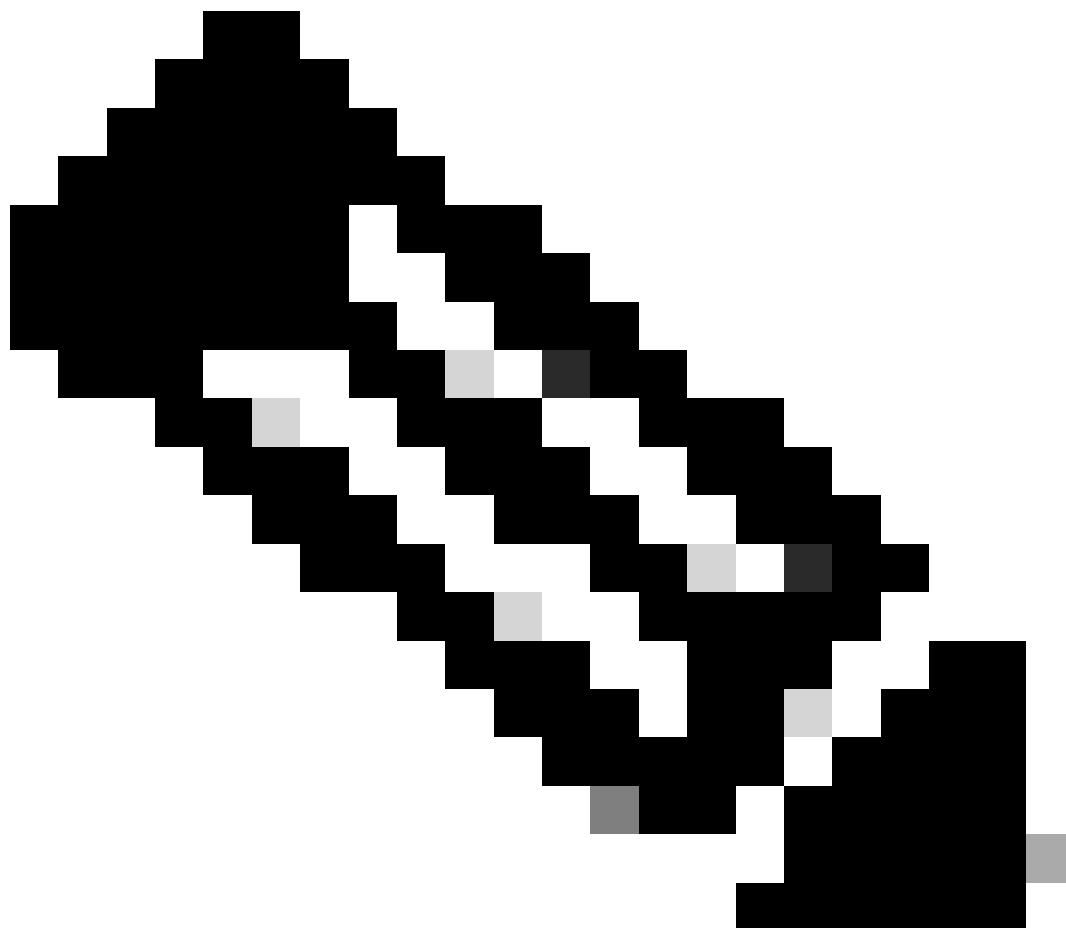
Configuração da política de grupo FMC RAVPN

1. Você deve criar uma política de grupo com as opções necessárias para cada grupo de usuários no Entra ID e adicionar à política RAVPN para o FTD que está sendo configurado. Para isso, navegue até **Devices > VPN > Remote Access > Advanced** e selecione **Group Policies** no lado esquerdo e, em seguida, clique no + no canto superior direito para adicionar uma política de grupo.



FMC adicionar política de grupo

2. Clique no + no pop-up para abrir a caixa de diálogo para criar uma nova Política de grupo. Preencha as opções necessárias e salve.



Note: Se você já criou a diretiva de grupo necessária, ignore esta etapa e continue na etapa 3

Group Policy

Available Group Policy



Search

Criar nova política de grupo

Add Group Policy

Name:*

SAMLtest-GP

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

☒ SSL

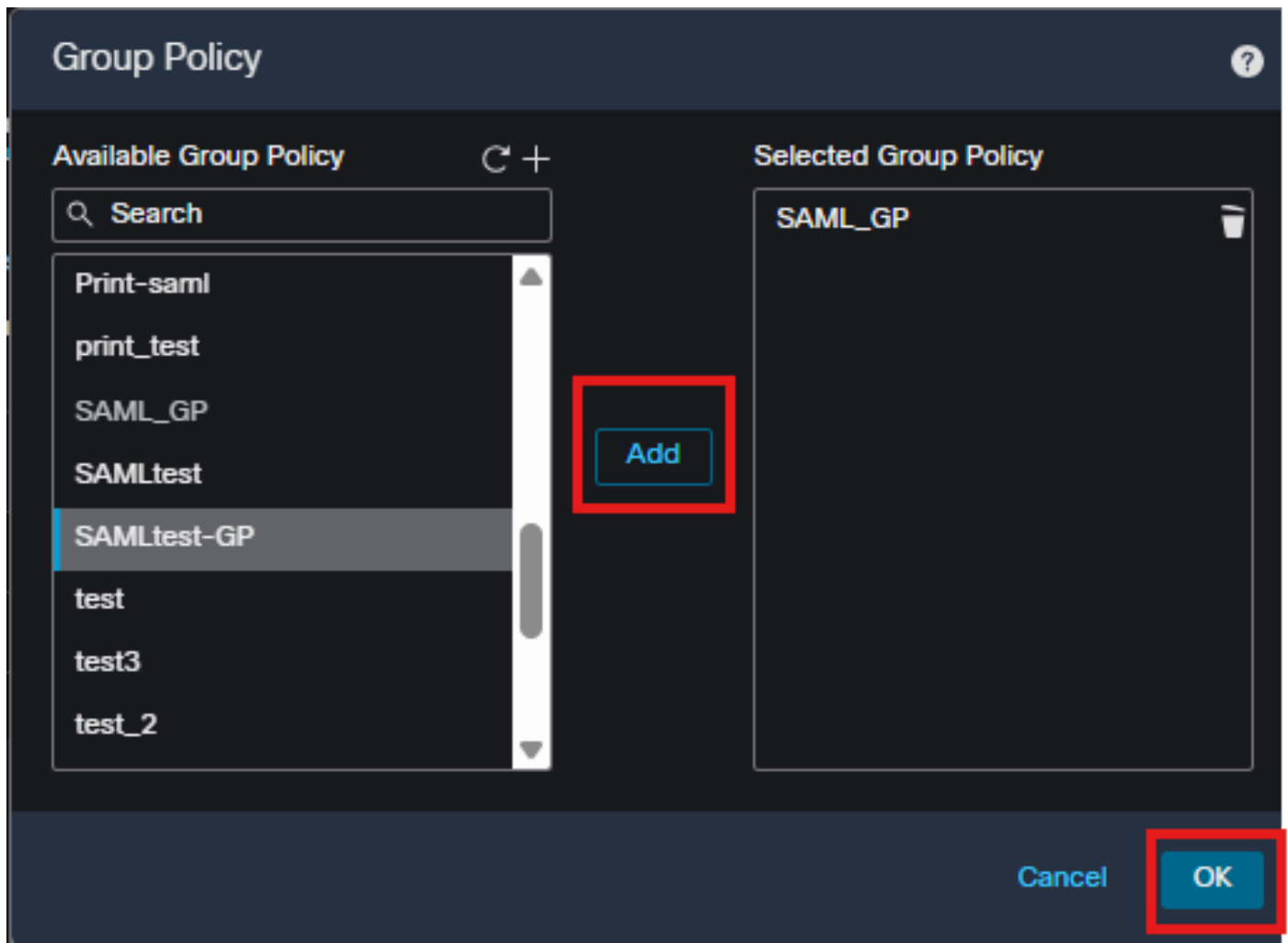
☒ IPsec-IKEv2

Cancel

Save

Opções de Política de Grupo

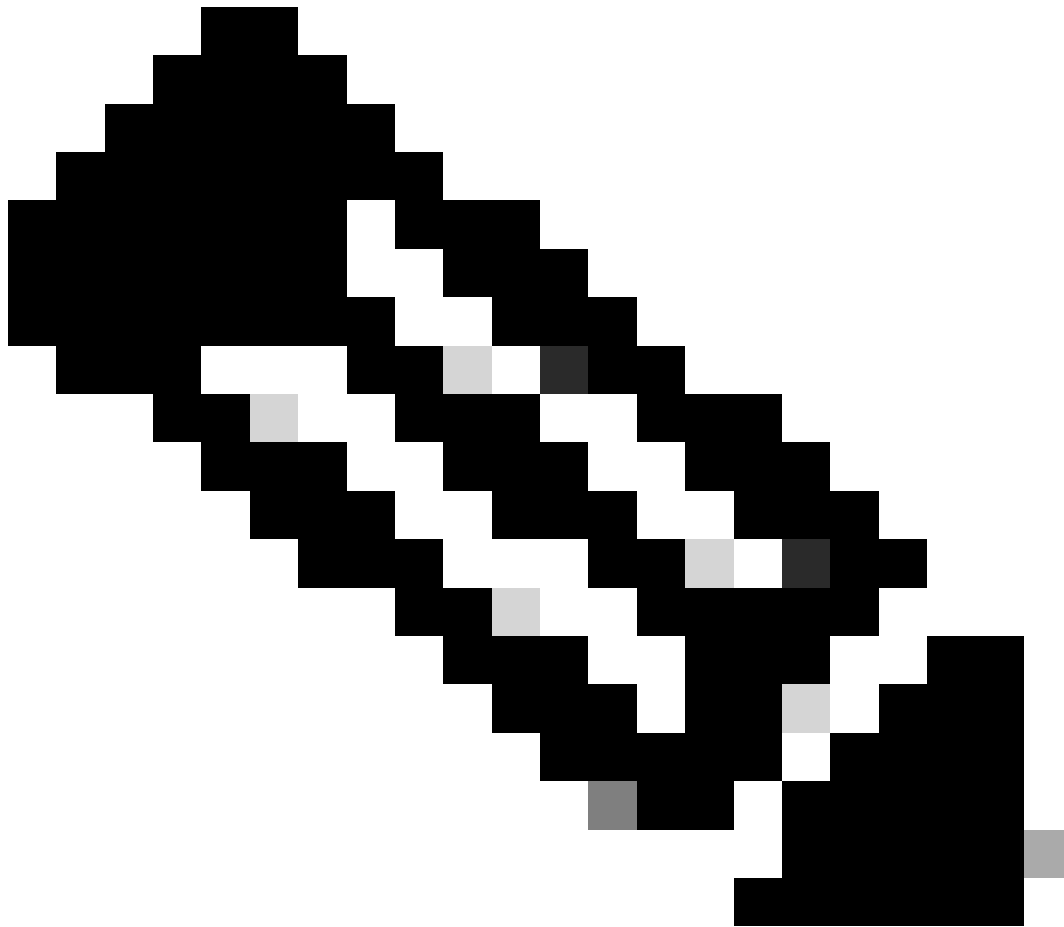
3. Selecione a política de grupo recém-criada na lista à esquerda e clique no botão Adicionar. Em seguida, clique em Ok para salvar a lista.



adicionar política de grupo

Metadados de FTD

Depois que a configuração tiver sido implantada no FTD, navegue até a CLI do FTD e execute o comando "show saml metadata <tunnel group name>" e reúna o ID da Entidade do FTD e o URL do ACS.



Note: O certificado nos metadados foi truncado para abreviar.

<#root>

FTD# show saml metadata SAMLtest
SP Metadata

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="

<https://vpn.example.net/saml/sp/metadata/SAMLtest>

" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIIFWzCCBE0gAwIBAgITRwAAAAGZ9Nmfv5mpJQAAAAACDANBgkqhkiG9w0BAQsF
ADBJMRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGcnRwdnBu
MRowGAYDVQQDExFydHB2cG4tV010QVVUSC1DQTAeFw0yNTAzMjUxNzU5NDZaFw0y
NzAzMjUxNzU5NDZaMDAxDzANBgNVBAoTB1JUUUFZQTJEdMBsGA1UEAxMUcnRwdnBu

LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
5B0tH9RIjvG0MxhpDT3/BpDEffTcVE2w2fxu5m8gZFTeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9F04LE88attuGuVMquV+10DRPA06a6QNwkehB0Un7XzTNepJ02JQtxdNR2t

</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</KeyDescriptor>

<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP

https://vpn.example.net/+CSCOE+/saml/sp/acs?tgname=SAMLtest

" />

<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://vpn

</EntityDescriptor>

ID do Microsoft Entra

1. No Portal do Microsoft Azure, selecione ID do Microsoft Entra no menu à esquerda.



Create a resource



Home



Dashboard



All services



FAVORITES



All resources



Resource groups



App Services



Function App



SQL databases



Azure Cosmos DB



Virtual machines

: Se já houver um aplicativo empresarial configurado para a configuração FTD RAVPN, ignore as próximas etapas e continue na etapa 7.



Enterprise applications | All applications



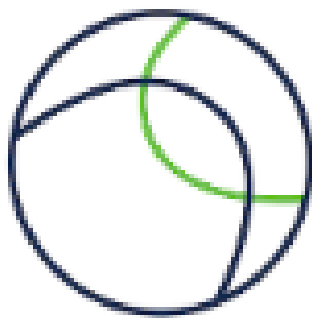
New application



Refresh

Aplicativo Empresarial MS Entra ID

4. Selecione Cisco Secure Firewall - Secure Client (anteriormente AnyConnect) authentication em Aplicativos em destaque. Dê um nome ao aplicativo e selecione Criar.



**Cisco Secure Firewall -
Secure Client (formerly
AnyConnect)
authentication**

Cisco Systems, Inc.



Aplicativo de autenticação MS Entra ID Cisco Secure Firewall Secure Client (antigo AnyConnect)

5. Uma vez no aplicativo, selecione Usuários e grupos e atribua os nomes de usuário ou grupo necessários ao aplicativo.



SAMLtest | Overview

Enterprise Application



Overview



Deployment Plan



Diagnose and solve problems



Manage



Properties



Owners



Roles and administrators

com o URL do Identificador (ID da Entidade) e da Resposta (ACS) recuperado dos metadados do FTD e salve.

Dashboard > csecurity > Enterprise applications > Enterprise applications | All applications > SAMLtest

SAMLtest | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Self-service
 - Custom security attributes
- Security

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating SAMLtest.

1

Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout URL (Optional)	Optional

Edit

2

Attributes & Claims

Fill out required fields in Step 1

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

https://vpn.example.net/saml/sp/metadata/SAMLtest

Add identifier

Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the 'Assertion Consumer Service' (ACS) in SAML.

https://vpn.example.net/+CSCOE+/saml/sp/acs/?name=SAMLtest

Add reply URL

Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS

Configuração SAML básica

8. Selecione Edit para Attribute & Claims e clique em Add new claim

2

Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
cisco_group_policy	Multiple conditions
Unique User Identifier	user.userprincipalname

Atributos e reivindicações

9. A nova reivindicação deve ter o nome cisco_group_policy.

Manage claim ...

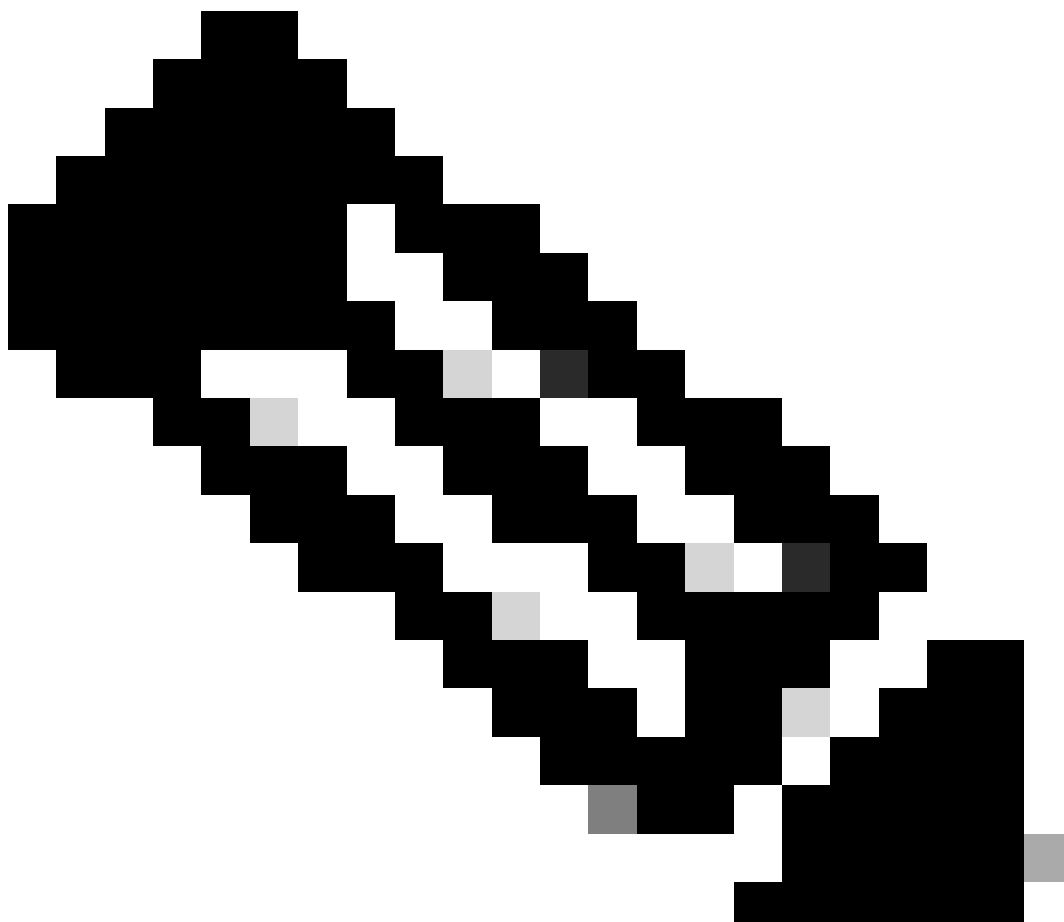
Save | Discard changes | Got feedback?

Name *

cisco_group_policy

Gerenciar reivindicação

10. Expanda a seção para Condições da reivindicação. Selecione o Tipo de usuário e os Grupos com escopo, escolha Atributo para a Origem e adicione o nome de política de grupo correto da configuração de FTD no campo Valor e clique em Salvar.



Note: O nome da política de grupo personalizada do FTD usado neste exemplo é a política de grupo chamada SAMLtest-GP criada na seção Configuração de Política de Grupo FMC RAVPN deste guia. Esse valor deve ser substituído pelo nome da política de grupo do FTD que corresponde a cada grupo de usuários no IdP.

User type	Scoped Groups	Source	Value
Any	1 groups	Attribute	"SAMLtest-GP"

Condição de declaração de ID do MS Entra

Verificar

FTD

Para verificar a política de grupo desejada, valide a saída de "show vpn-sessiondb anyconnect".

<#root>

```
FTD# show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

Username : RTPVPNtest

Index : 7110

Assigned IP : 192.168.55.3 Public IP : 10.26.162.189

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA256

Bytes Tx : 105817 Bytes Rx : 63694

Group Policy :

SAMLtest-GP

Tunnel Group : SAMLtest

Login Time : 16:54:17 UTC Fri May 9 2025

Duration : 0h:11m:19s

Inactivity : 0h:00m:00s

VLAN Mapping : N/A VLAN : none

Audt Sess ID : ac127ca101bc6000681e3339

Security Grp : none Tunnel Zone : 0

Para verificar se o IdP está enviando a declaração desejada, obtenha a saída de "debug webvpn saml 255" ao conectar-se à VPN. Analise a saída de asserção nas depurações e compare a seção do atributo com o que está configurado no IdP.

```
<#root>
```

```
<Attribute Name="cisco_group_policy">
```

```
<AttributeValue>
```

SAMLtest-GP

```
</AttributeValue>
```

```
</Attribute>
```

Troubleshooting

```
<#root>
```

```
firepower#
```

```
show run webvpn
```

```
firepower#
```

```
show run tunnel-group
```

```
firepower#
```

```
show crypto ca certificate
```

```
firepower#
```

```
debug webvpn saml 255
```

```
firepower#
```

```
debug webvpn 255
```

```
firepower#
```

```
debug aaa authorization
```

Informações Relacionadas

[Suporte técnico e downloads da Cisco](#)

[Guias de configuração do ASA](#)

[Guias de configuração do FMC/FDM](#)

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.