

Groepsbeleidstoewijzing configureren voor SAML met behulp van Secure Firewall en Microsoft Entra ID

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuratie FMC SAML](#)

[Configuratie FMC RAVPN Tunnel Group](#)

[Beleidsconfiguratie FMC RAVPN Group](#)

[FTD-metagegevens](#)

[Microsoft Entra ID](#)

[Verifiëren](#)

[FTD](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe groepsbeleid kan worden toegewezen met behulp van Microsoft Entra ID voor SAML-verificatie van Cisco Secure Client op Cisco Secure Firewall.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen:

- Cisco Secure Client AnyConnect VPN
- Cisco Firepower Threat Defense (FTD) of Cisco Secure Firewall ASA-serverobjectconfiguratie voor externe toegang VPN en Single Sign-on (SSO)
- Configuratie Microsoft Entra ID Identity Provider (IdP)

Gebruikte componenten

De informatie in deze handleiding is gebaseerd op de volgende hardware- en softwareversies:

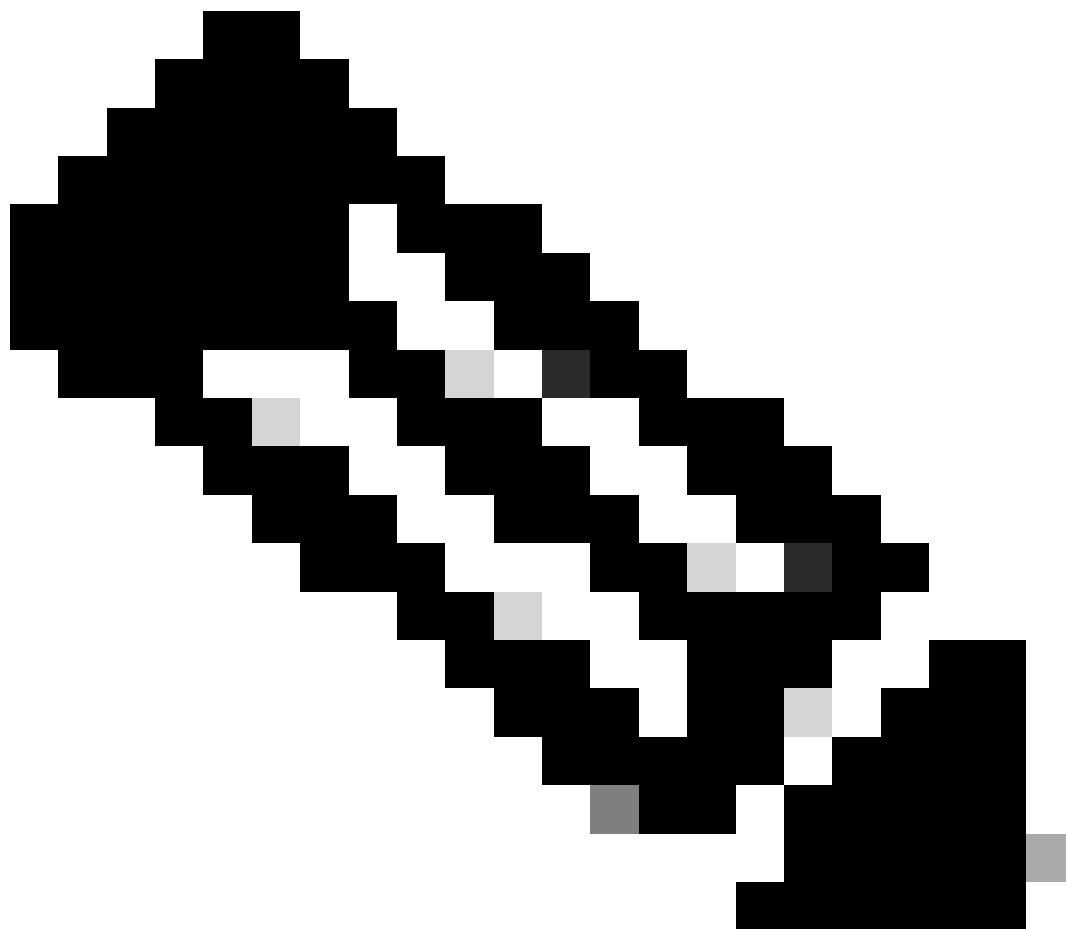
- FTD versie 7.6
- FMC versie 7.6
- MS Entra ID SAML IdP

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

SAML (Security Assertion Markup Language) is een op XML gebaseerd framework voor het uitwisselen van authenticatie- en autorisatiegegevens tussen beveiligingsdomeinen. Het creëert een vertrouwenscirkel tussen de gebruiker, een Service Provider (SP) en een Identity Provider (IdP), waardoor de gebruiker zich in één keer kan aanmelden voor meerdere diensten. SAML kan worden gebruikt voor Remote Access VPN-verificatie voor Cisco Secure Client-verbindingen met ASA- en FTD VPN-headends, waarbij de ASA of FTD het SP-deel van de vertrouwenscirkel is.

In dit document wordt Microsoft Entra ID/Azure gebruikt als de IdP. Het is echter ook mogelijk om groepsbeleid toe te wijzen met behulp van andere IdP's, omdat het is gebaseerd op standaardkenmerken die kunnen worden verzonden in de SAML-bewering.



Opmerking: elke gebruiker mag slechts tot één gebruikersgroep op MS Entra ID behoren, omdat meerdere SAML-attributen die naar de ASA of FTD worden verzonden, problemen kunnen veroorzaken met de toewijzing van het groepsbeleid zoals beschreven in Cisco bug ID [CSCwm33613](#)

Configureren

Configuratie FMC SAML

Navigeer in de FMC naar Objecten > Objectbeheer > AAA-server > Single Sign-on Server. De Entiteit-ID, SSO-URL, Logout-URL en Identity Provider-certificaat worden verkregen van de IdP, zie stap 6 in de Microsoft Entra ID-sectie. De basis-URL en het certificaat van de serviceprovider zijn specifiek voor de FTD waaraan de configuratie wordt toegevoegd.

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

FMC SSO-objectconfiguratie

Configuratie FMC RAVPN Tunnel Group

Navigeer in de FMC naar Apparaten > VPN > Externe toegang > Verbindingsprofiel en selecteer of maak het VPN-beleid voor de FTD die u configureert. Nadat u deze optie hebt geselecteerd, maakt u een verbindingsprofiel dat vergelijkbaar is met het volgende:

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

Adrestoewijzing FMC-verbindingsprofiel

?

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

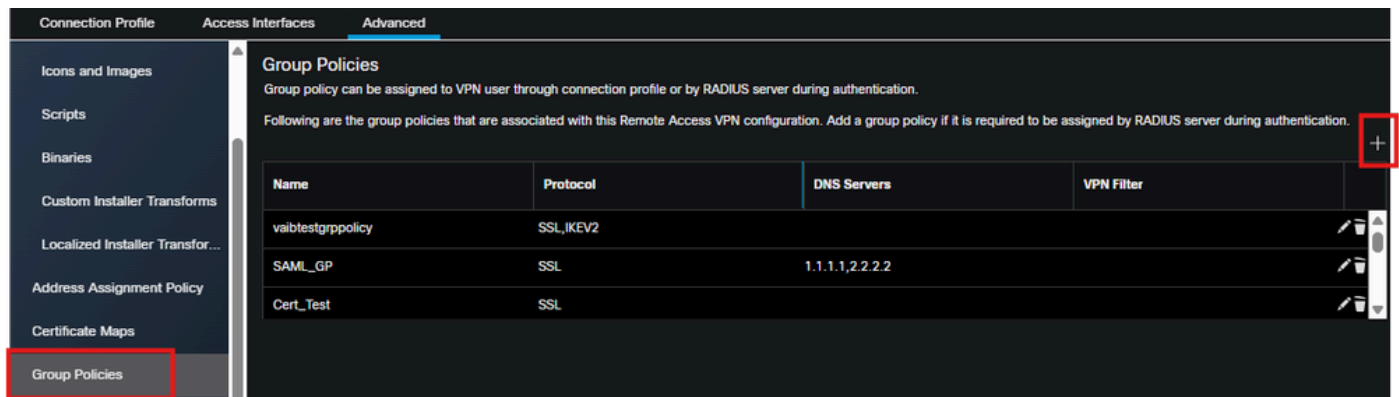
Cancel

Save

AAA-configuratie van het FMC-verbindingsprofiel

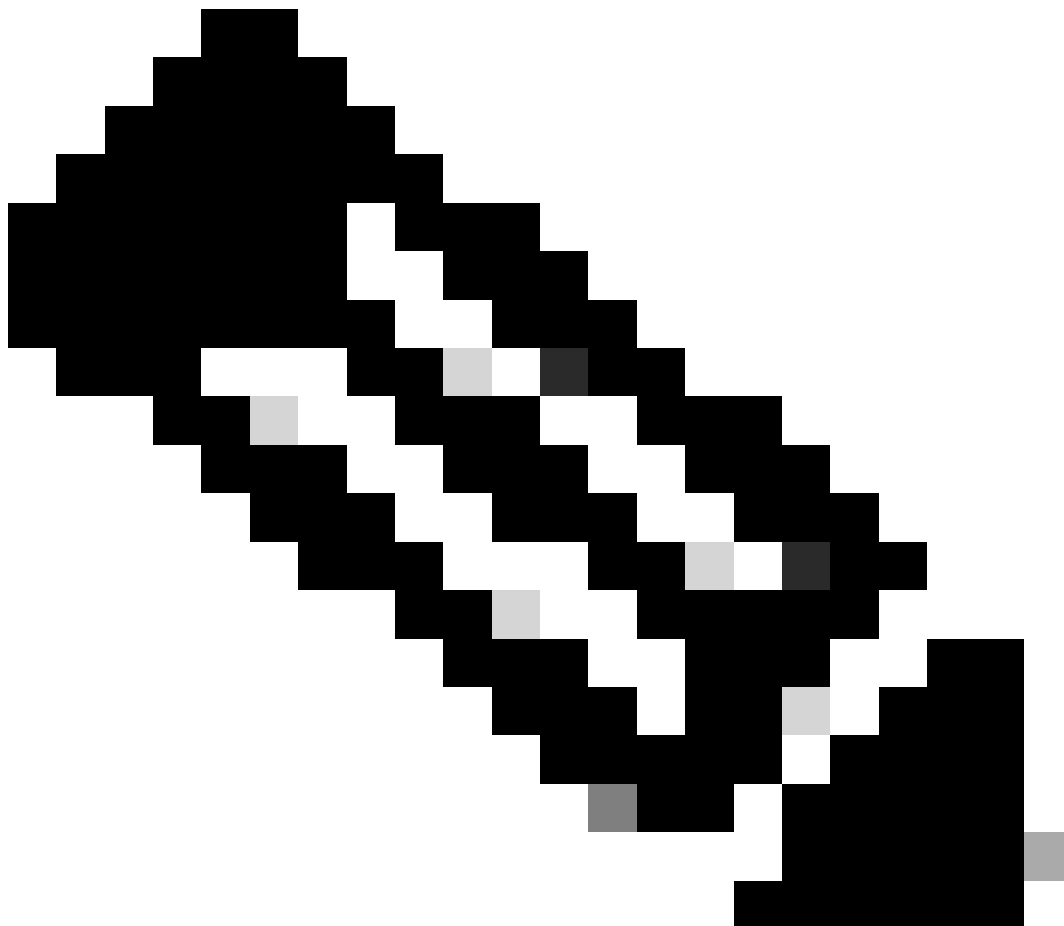
Beleidsconfiguratie FMC RAVPN Group

1. U moet een groepsbeleid maken met de vereiste opties voor elke gebruikersgroep op Entra ID en toevoegen aan het RAVPN-beleid voor de FTD die wordt geconfigureerd. Dit wordt bereikt door naar Apparaten > VPN > Externe toegang > Geavanceerd te navigeren en Groepsbeleid aan de linkerkant te selecteren en vervolgens rechtsboven op + te klikken om een groepsbeleid toe te voegen.



FMC-groepsbeleid toevoegen

2. Klik op + in het pop-upvenster om het dialoogvenster te openen voor het maken van een nieuw groepsbeleid. Vul de gewenste opties in en sla op.



Opmerking: als u het vereiste groepsbeleid al hebt gemaakt, kunt u deze stap overslaan en doorgaan met stap 3

Group Policy

Available Group Policy



Search

Nieuw groepsbeleid maken

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

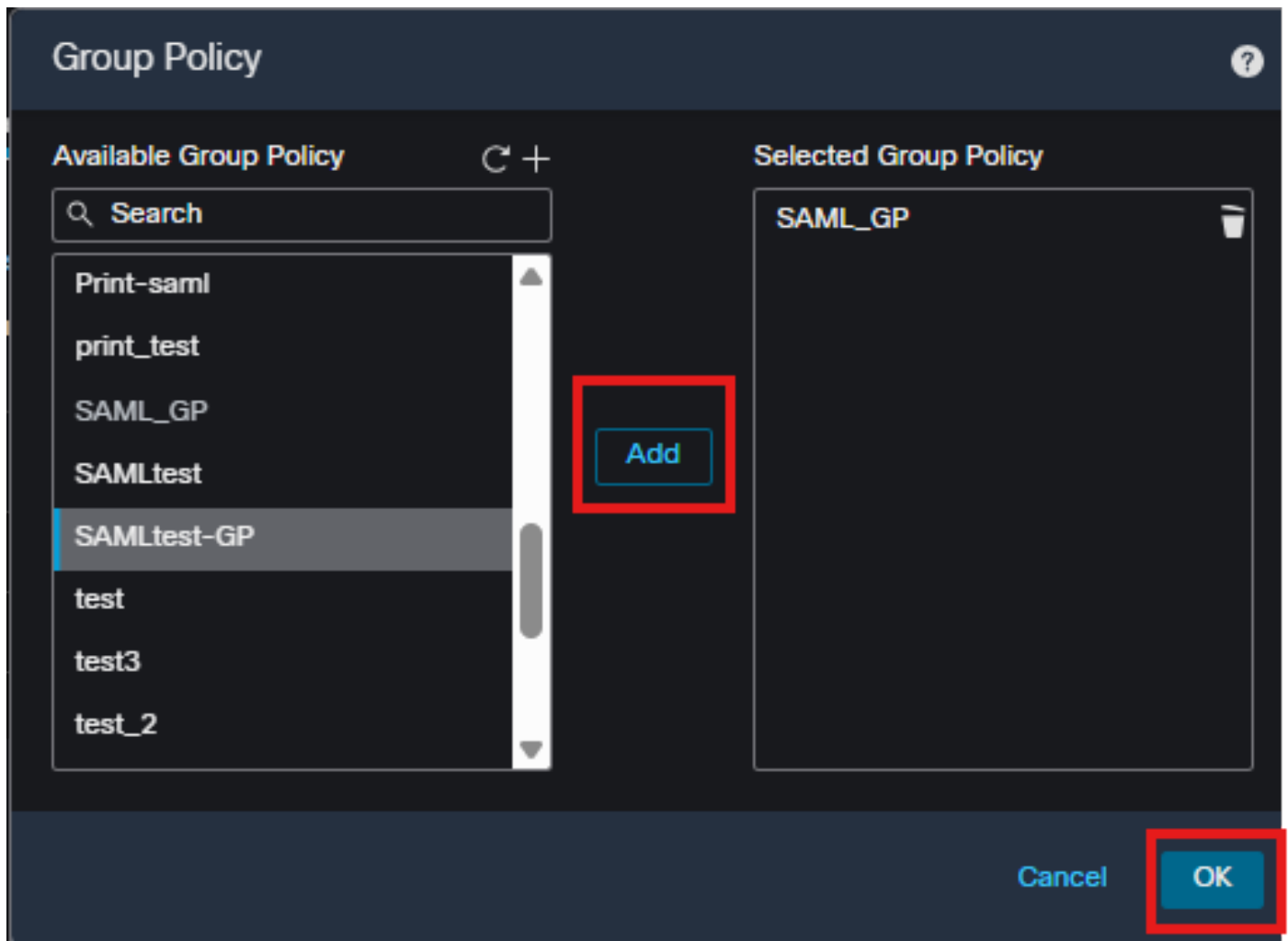
☒ IPsec-IKEv2

Cancel

Save

Groepsbeleidsopties

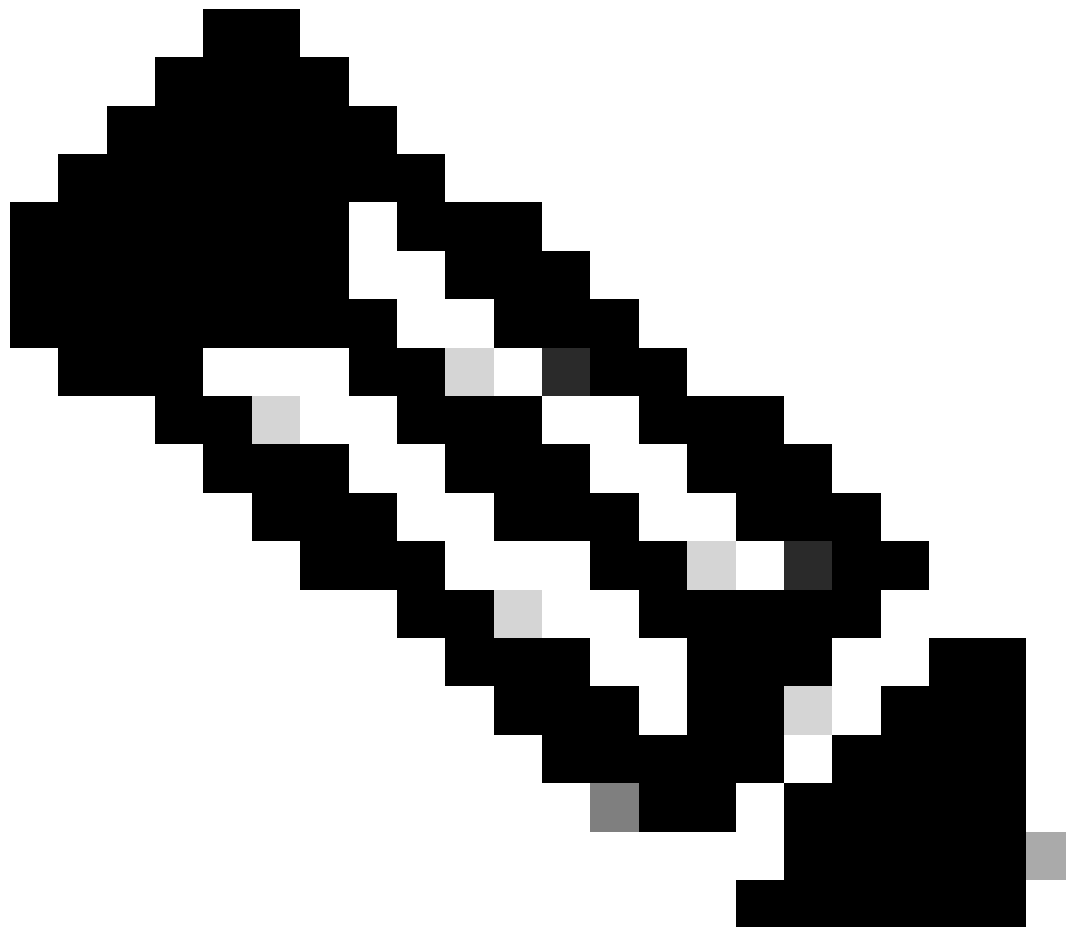
3. Selecteer het nieuw gemaakte groepsbeleid in de lijst aan de linkerkant en klik op de knop Toevoegen en klik vervolgens op OK om de lijst op te slaan.



Groepsbeleid toevoegen

FTD-metagegevens

Zodra de configuratie is geïmplementeerd in de FTD, navigeert u naar de FTD CLI en voert u de opdracht "toon kleine metagegevens <tunnelgroepnaam>" uit en verzamelt u de FTD-entiteit-ID en ACS-URL.



Opmerking: het certificaat in de metagegevens is kort afgekapt.

<#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>
MIIFWzCCBE0gAwIBAgITRwAAAAGZ9Nmfv5mpJQAAAAACDANBgkqhkiG9w0BAQsF
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>

Microsoft Entra ID

1. Selecteer in het Microsoft Azure Portal de optie Microsoft Entra ID in het menu aan de linkerkant.



Create a resource



Home



Dashboard



All services



FAVORITES



All resources



Resource groups



App Services



Function App



SQL databases



Azure Cosmos DB



Virtual machines

: Als er al een Enterprise Application is geconfigureerd voor de FTD RAVPN-configuratie, slaat u de volgende stappen over en gaat u verder met stap 7.



Enterprise applications | All applications



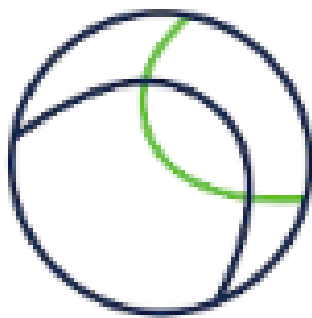
New application



Refresh

MS Entra ID Enterprise Application

4. Selecteer Cisco Secure Firewall - Secure Client (voorheen AnyConnect)-verificatie onder Aanbevolen toepassingen. Geef de toepassing een naam en selecteer Maken.



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

Cisco Systems, Inc.



MS Entra ID Cisco Secure Firewall Secure Client (voorheen AnyConnect)-verificatietoepassing

5. Selecteer Gebruikers en groepen in de toepassing en wijs de benodigde gebruikers- of groepsnamen aan de toepassing toe.



SAMLtest | Overview

Enterprise Application



Overview



Deployment Plan



Diagnose and solve problems



Manage



Properties



Owners



Roles and administrators

met de ID (Entity ID) en de Reply (ACS) URL die zijn opgehaald uit de FTD-metagegevens en sla deze op.

The screenshot shows the 'Basic SAML Configuration' page in the Azure AD portal. The left sidebar contains navigation links: Overview, Deployment Plan, Diagnose and solve problems, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on (selected), Provisioning, Self-service, Custom security attributes, and Security. The main content area is titled 'Set up Single Sign-On with SAML' and includes a 'Basic SAML Configuration' section with fields for Identifier (Entity ID), Reply URL, Sign on URL, Relay State, and Logout URL. The 'Identifier (Entity ID)' field is highlighted with a red box and contains the value 'https://vpn.example.net/saml/sp/metadata/SAMLtest'. The 'Reply URL' field is also highlighted with a red box and contains the value 'https://vpn.example.net/+CSCOE+/saml/sp/acs/?name=SAMLtest'. The 'Edit' button is highlighted with a red box. The right sidebar shows the 'Basic SAML Configuration' section with the same fields and a 'Got feedback?' link.

Basis SAML-configuratie

8. Selecteer Bewerken voor Attribuu en claims en klik op Nieuwe claim toevoegen

The screenshot shows the 'Attributes & Claims' section in the Azure AD portal. The left sidebar contains navigation links: 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, and Security. The main content area is titled 'Attributes & Claims' and includes a table with columns for 'Attribute' and 'Value'. The table contains the following data:

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

The 'Edit' button is highlighted with a red box.

Eigenschappen en claims

9. De nieuwe claim moet de naam cisco_group_policy hebben.

Manage claim ...

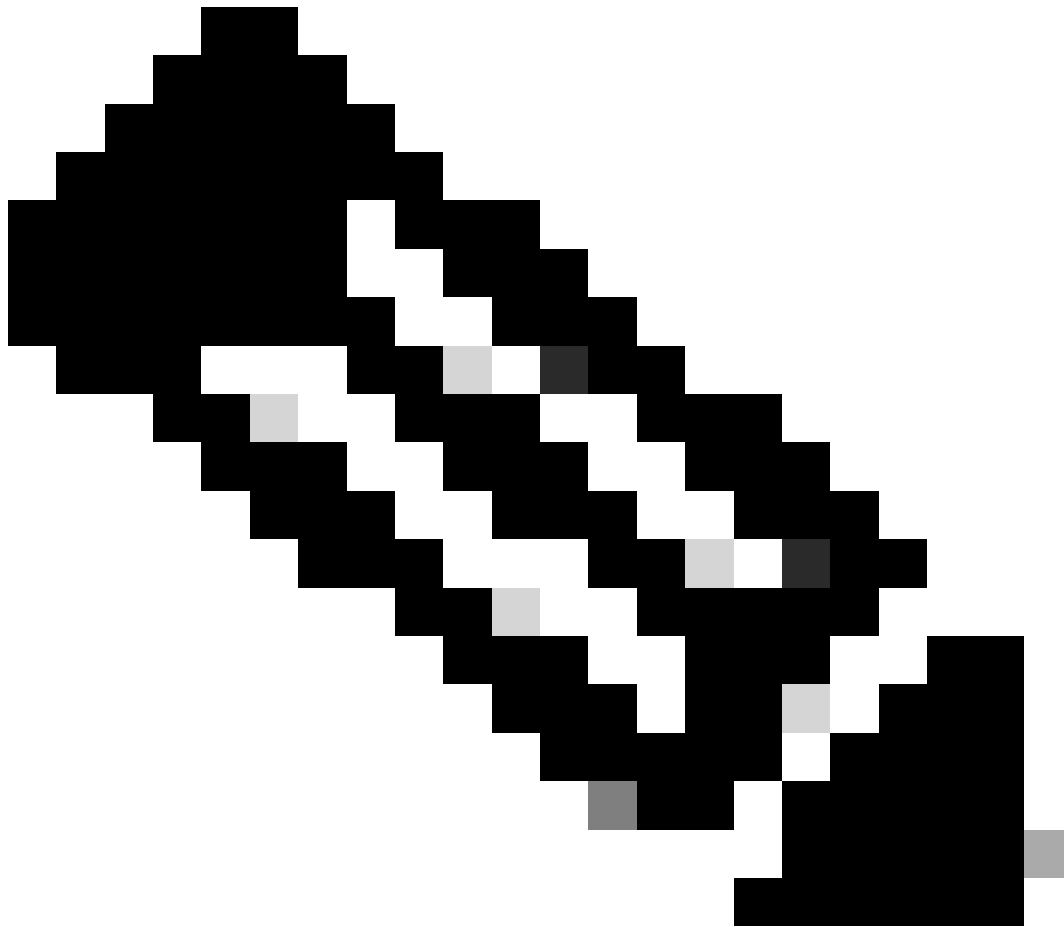
Save Discard changes | Got feedback?

Name *

cisco_group_policy

Claim beheren

10. Vouw het gedeelte voor claimvoorwaarden uit. Selecteer het gebruikerstype en de gescande groepen, kies vervolgens Attribuu voor de bron en voeg de juiste naam voor het groepsbeleid toe uit de FTD-configuratie in het veld Waarde en klik op Opslaan.



Opmerking: De aangepaste naam voor het groepsbeleid van de FTD die in dit voorbeeld wordt gebruikt, is het groepsbeleid met de naam SAMLtest-GP dat is gemaakt in de sectie FMC RAVPN Group Policy Configuration van deze handleiding. Deze waarde moet worden vervangen door de naam van het groepsbeleid uit de FTD die overeenkomt met elke gebruikersgroep op de IdP.

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

MS Entra ID claimvoorwaarde

Verifiëren

FTD

Om het gewenste groepsbeleid te verifiëren, valideert u de uitvoer van "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

Om te controleren of de IdP de gewenste claim verzendt, verzamelt u de uitvoer van "debug webvpn saml 255" terwijl u verbinding maakt met de VPN. Analyseer de assertion output in de debugs en vergelijk het attribuut gedeelte met wat is geconfigureerd op de IdP.

<#root>

<Attribute Name="cisco_group_policy">

<AttributeValue>

SAMLtest-GP

</AttributeValue>

</Attribute>

Problemen oplossen

<#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
```

Gerelateerde informatie

[Technische ondersteuning en downloads van Cisco](#)

[ASA-configuratiehandleidingen](#)

[Configuratiehandleidingen voor FMC/FDM](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.