Configure Group Policy Assignment for SAML Using Secure Firewall and Microsoft Entra ID

Contents

Introduction

This document describes how to assign group policies using Microsoft Entra ID for SAML authentication of Cisco Secure Client on Cisco Secure Firewall.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- Cisco Secure Client AnyConnect VPN
- Cisco Firepower Threat Defense (FTD) or Cisco Secure Firewall ASA remote access VPN and Single Sign-on (SSO) server object configuration
- Microsoft Entra ID Identity Provider (IdP) configuration

Components Used

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

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

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

SAML (Security Assertion Markup Language) is an XML-based framework for exchanging authentication and authorization data between security domains. It creates a circle of trust between the user, a Service Provider (SP) and an Identity Provider (IdP) which allows the user to sign in a single time for multiple services. SAML can be used for Remote Access VPN authentication for Cisco Secure Client connections to ASA and FTD VPN headends, where the ASA or FTD is the SP part of the trust circle.

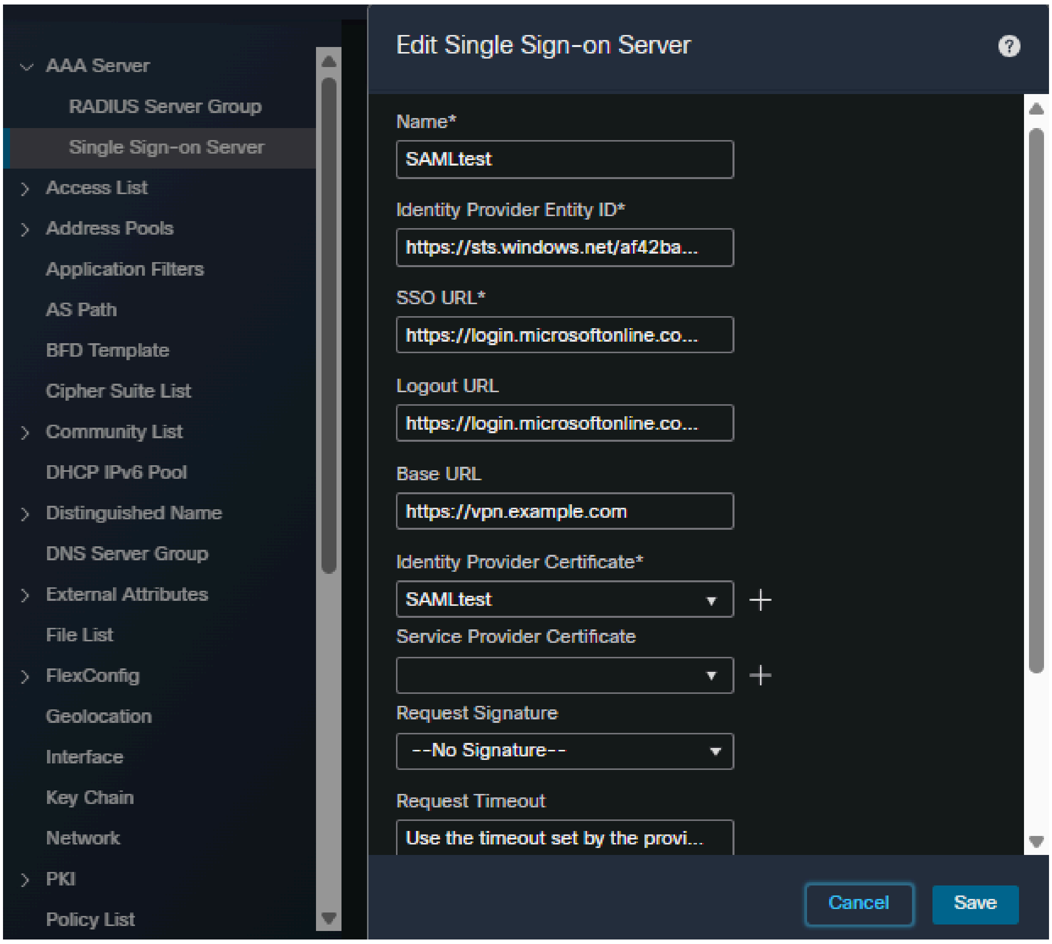
In this document, Microsoft Entra ID/Azure is used as the IdP. However, it is also possible to assign group policies using other IdPs since it is based on standard attributes that can be sent in the SAML assertion.

Note: Be aware that each user must only belong to one User Group on MS Entra ID, as multiple SAML attributes being sent to the ASA or FTD can cause issues with the group policy assignment as detailed in Cisco bug ID CSCwm33613

Configure

FMC SAML Configuration

On the FMC, navigate to **Objects > Object Management > AAA Server > Single Sign-on Server.** The Entity ID, SSO URL, Logout URL, and Identity Provider certificate are obtained from the IdP, see Step 6 in the **Microsoft Entra ID** section. The Base URL and Service Provider certificate are specific to the FTD the configuration is being added to.



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:

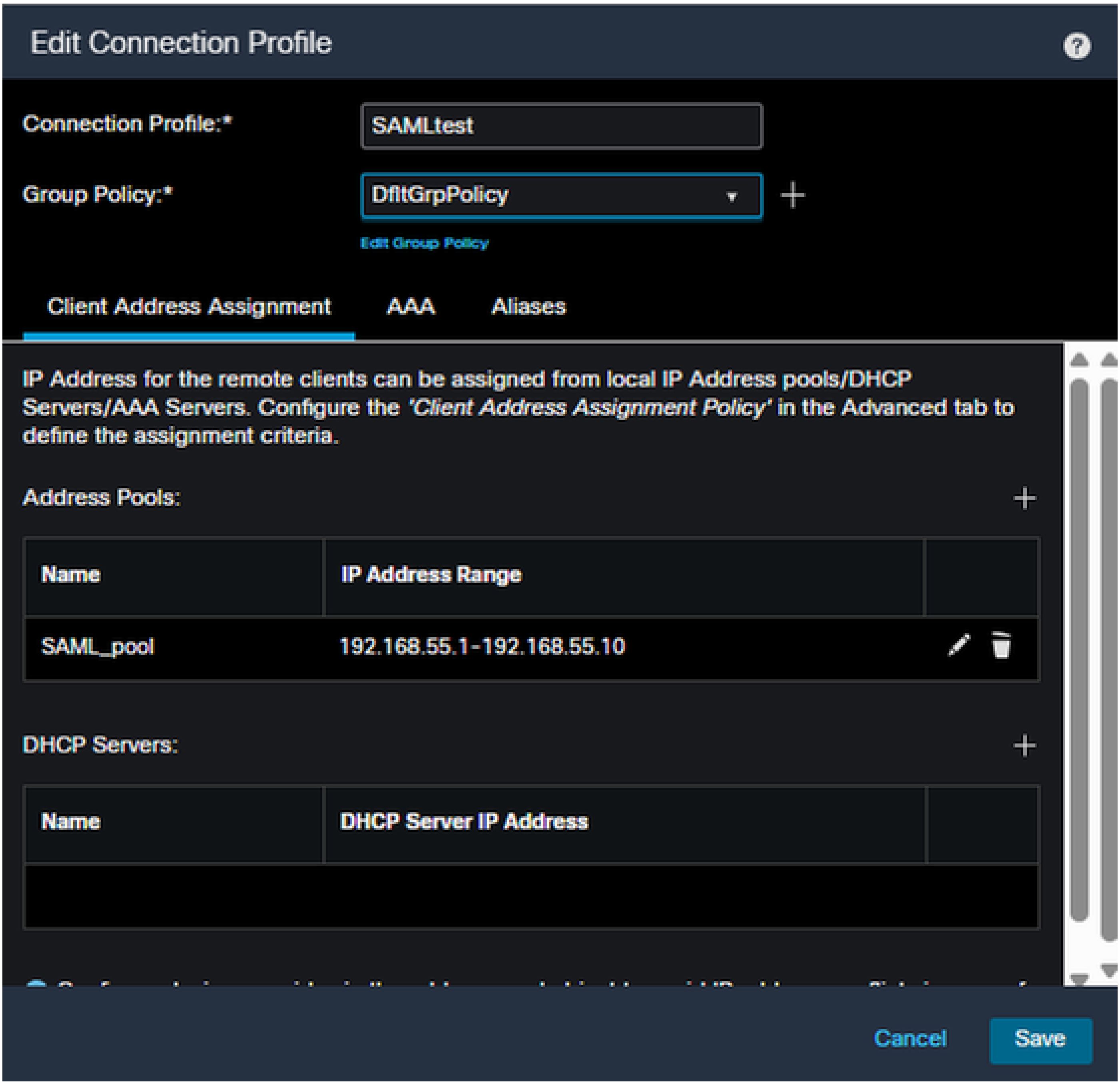
Request Signature: --No Signature--

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

FMC SSO Object Configuration

FMC RAVPN Tunnel Group Configuration

On the FMC navigate to **Devices > VPN > Remote Access > Connection Profile** and select, or create, the VPN policy for the FTD you are configuring. Once selected, create a connection profile similar to this:



Connection Profile:* SAMLtest

Group Policy:* DfltGrpPolicy

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.

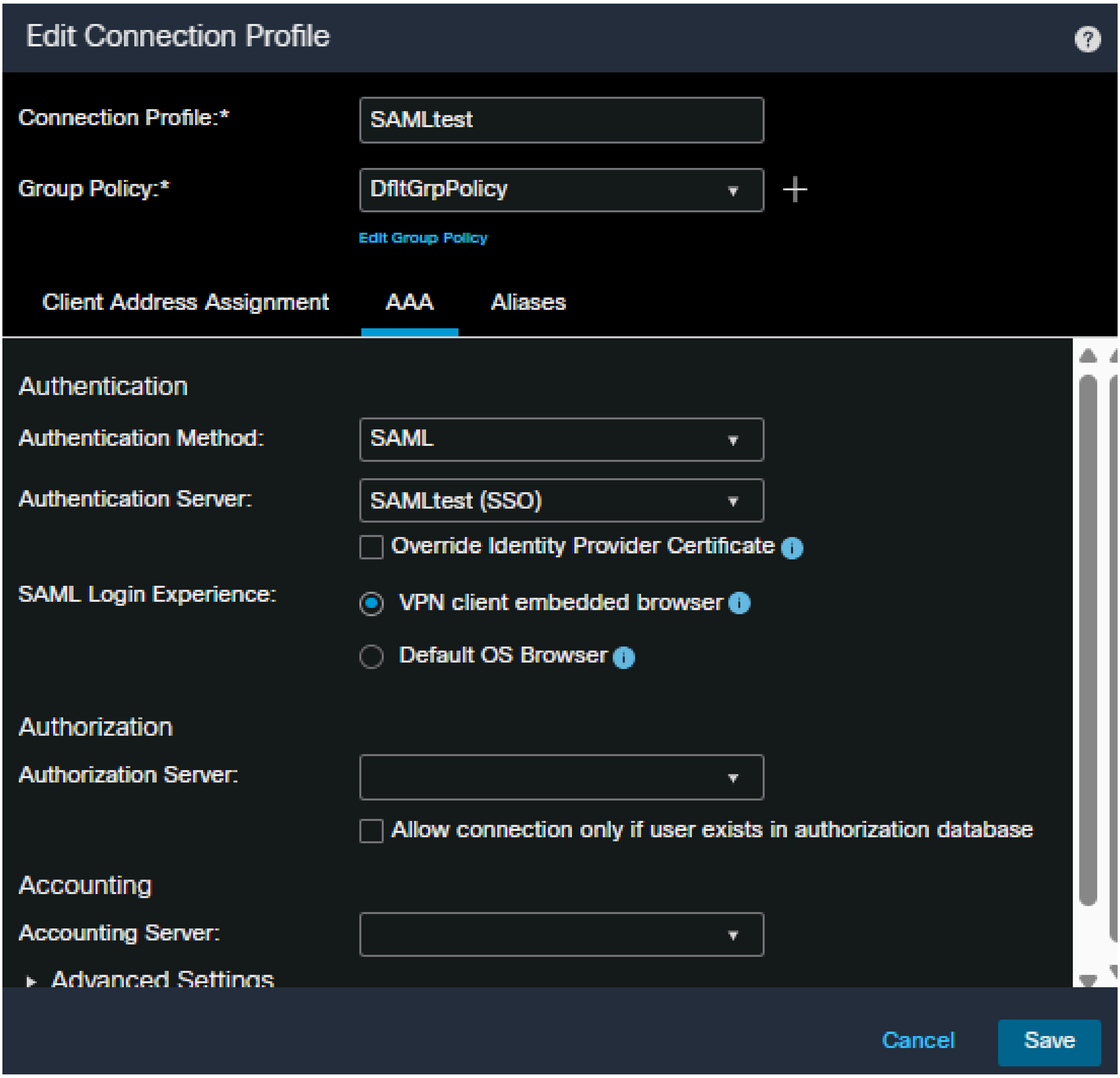
Address Pools:

Name	IP Address Range	
SAML_pool	192.168.55.1-192.168.55.10	

DHCP Servers:

Name	DHCP Server IP Address	

FMC Connection Profile Address Assignment



Edit Connection Profile

Connection Profile:* SAMLtest

Group Policy:* DfltGrpPolicy

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

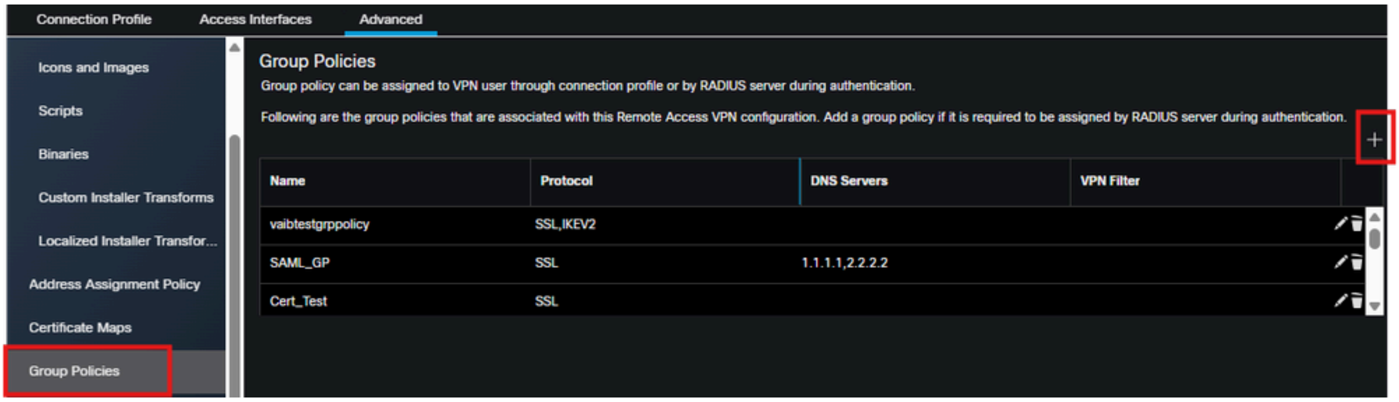
Accounting

Accounting Server:

FMC Connection Profile AAA configuration

FMC RAVPN Group Policy Configuration

1. You must create a group policy with the required options for each user group on Entra ID and add to the RAVPN policy for the FTD being configured. This is accomplished by navigating to **Devices** > **VPN** > **Remote Access** > **Advanced** and selecting **Group Policies** from the left side, then clicking the **+** in the upper right to add a group policy.



Group Policies

Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.

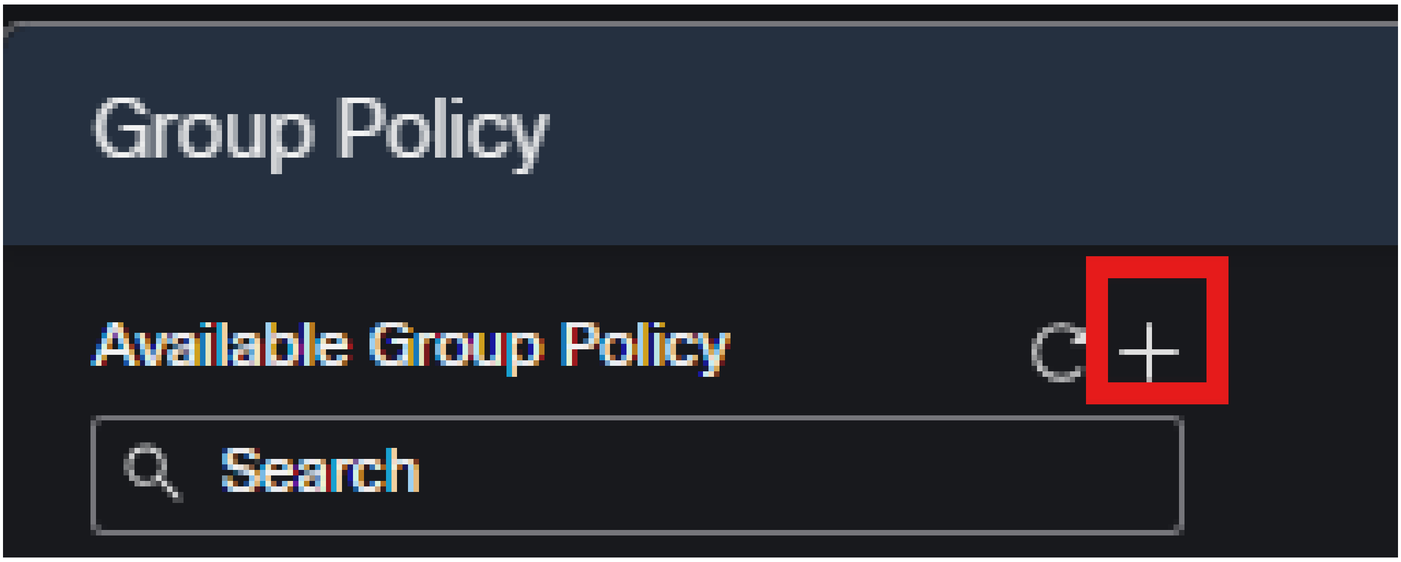
Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.

Name	Protocol	DNS Servers	VPN Filter
vaibtestgrppolicy	SSL,IKEV2		
SAML_GP	SSL	1.1.1.1,2.2.2.2	
Cert_Test	SSL		

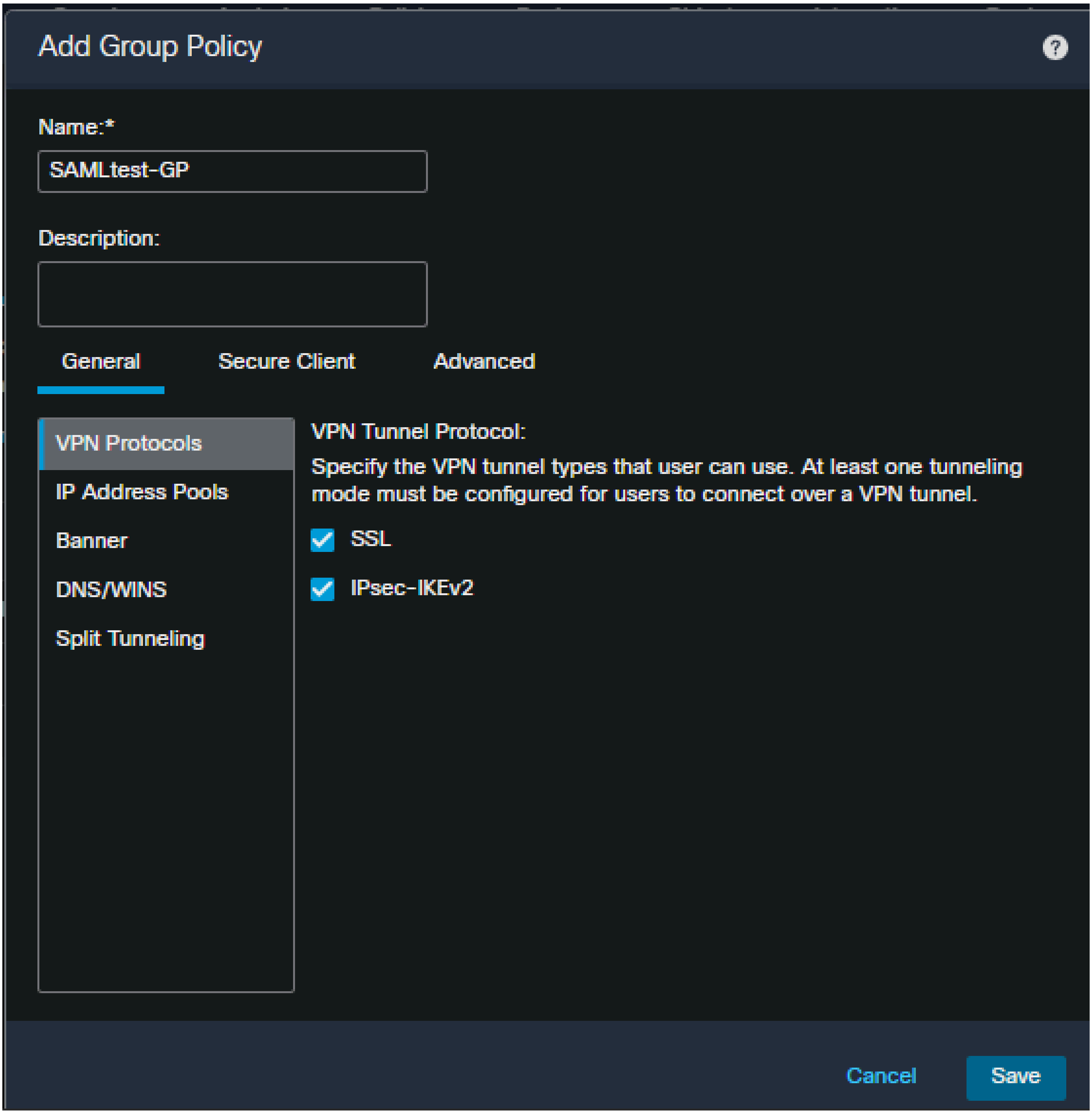
FMC add group policy

2. Click the + in the pop-up to bring up the dialog to create a new Group Policy. Fill in the required options and save.

Note: If you have already created the required group policy, you can skip this step and continue with step 3



Create new group policy



Add Group Policy

Name:*

SAMLtest-GP

Description:

VPN Tunnel Protocol:

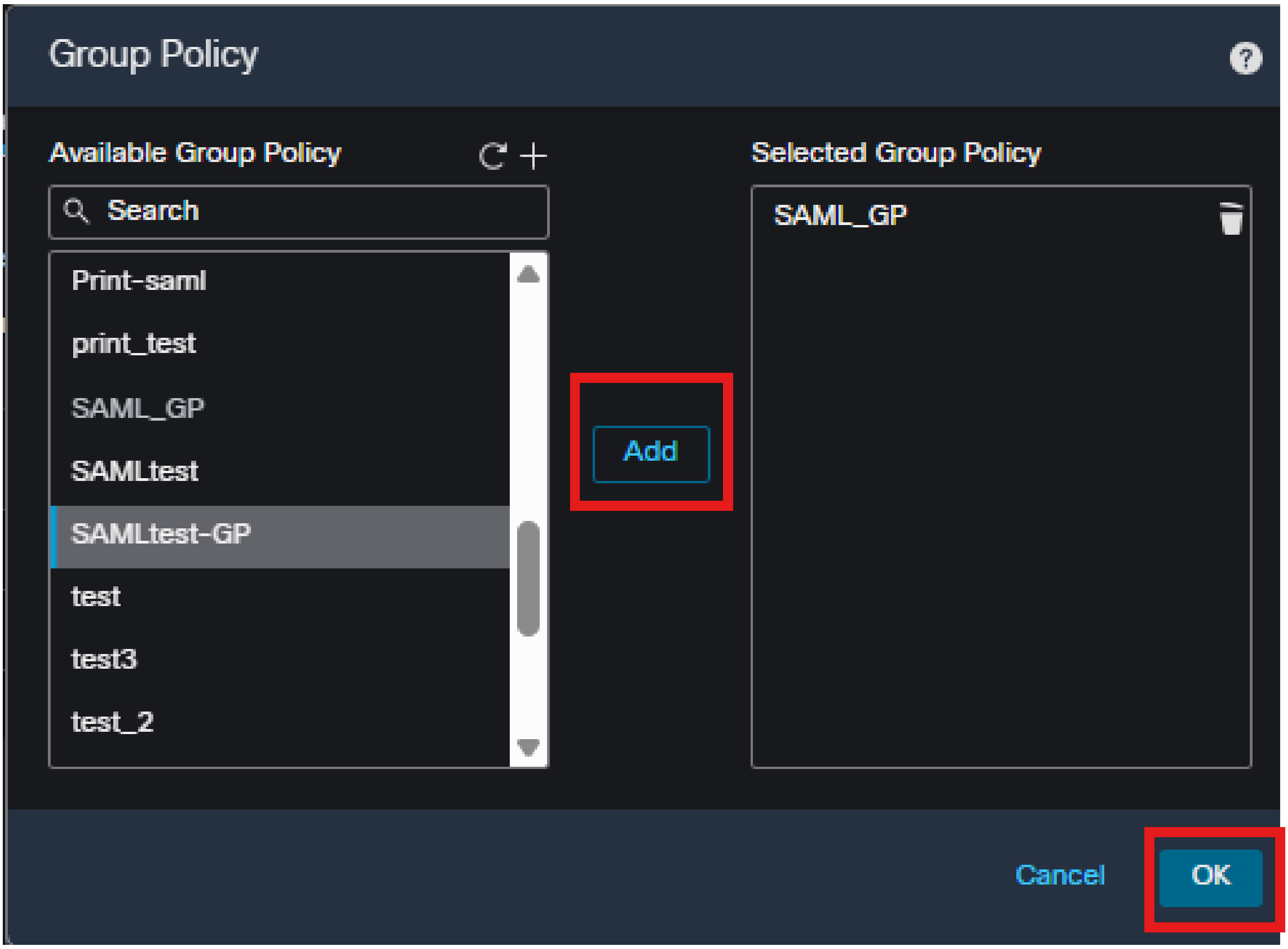
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

☑ SSL

☑ IPsec-IKEv2

Group Policy options

3. Select the newly created group policy in the list on the left and click the **Add** button, then click **Ok** to save the list.



add group policy

FTD Metadata

Once the configuration has been deployed to the FTD, navigate to the FTD CLI and execute the command "**show saml metadata <tunnel group name>**" and gather the FTD **Entity ID** and **ACS URL.**

Note: The certificate in the metadata was truncated for brevity.

<#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="ur
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFWzCCBEOgAwIBAgITRwAAAAgZ9Nmfv5mpJQAAAAAACDANBgkqhkiG9w0BAQsF
ADBJMRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGcnRwdnBu
MRowGAYDVQQDExFydHB2cG4tV0lOQVVUSC1DQTAeFw0yNTAzMjUxNzU5NDZaFw0y
NzAzMjUxNzU5NDZaMDAxDzANBgNVBAoTBlJUUFZQTjEdMBsGA1UEAxMUcnRwdnBu
LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
```

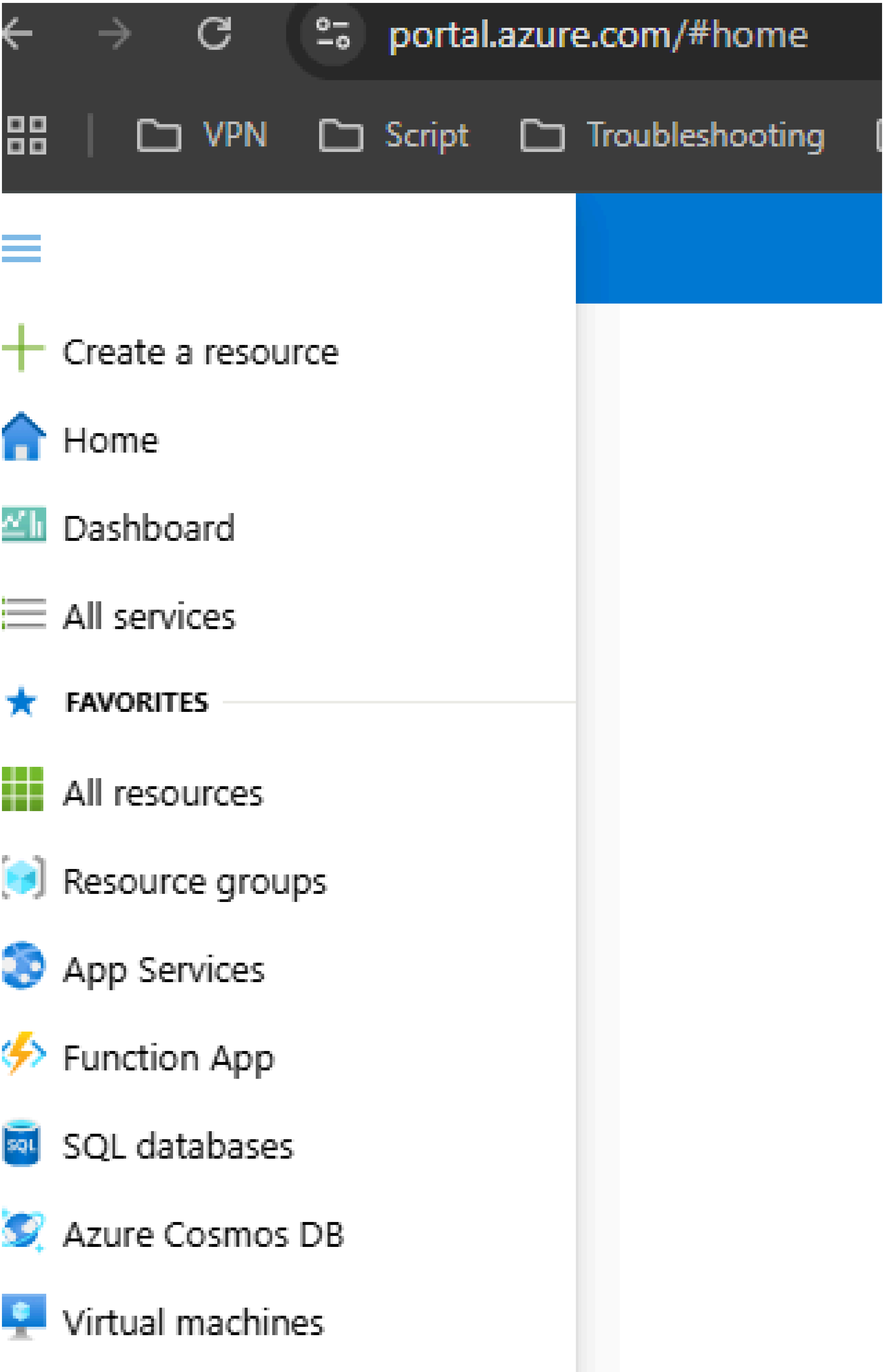
```
5B0tH9RIjvG0MxhpDT3/BpDEFfTcVE2w2fxu5m8gZFTeeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9F04LE88attuGuVMquV+10DRPA06a6QNwkehB0Un7XzTNepJ02JQtxdNR2t

</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`

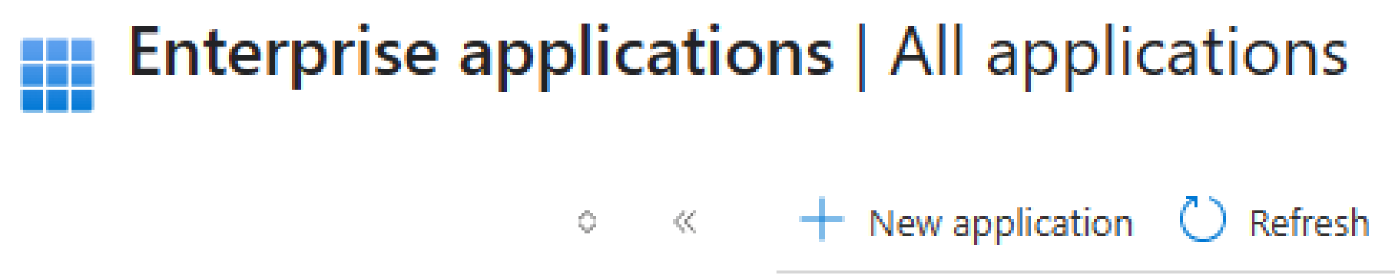
```
" />
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://vpn
</EntityDescriptor>
```

Microsoft Entra ID

1. On the Microsoft Azure Portal, select **Microsoft Entra ID** from the menu on the left.


portal.azure.com/#home
VPN
Script
Troubleshooting
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines

: If there is already an Enterprise Application configured for the FTD RAVPN configuration, skip the next steps and continue on step 7.

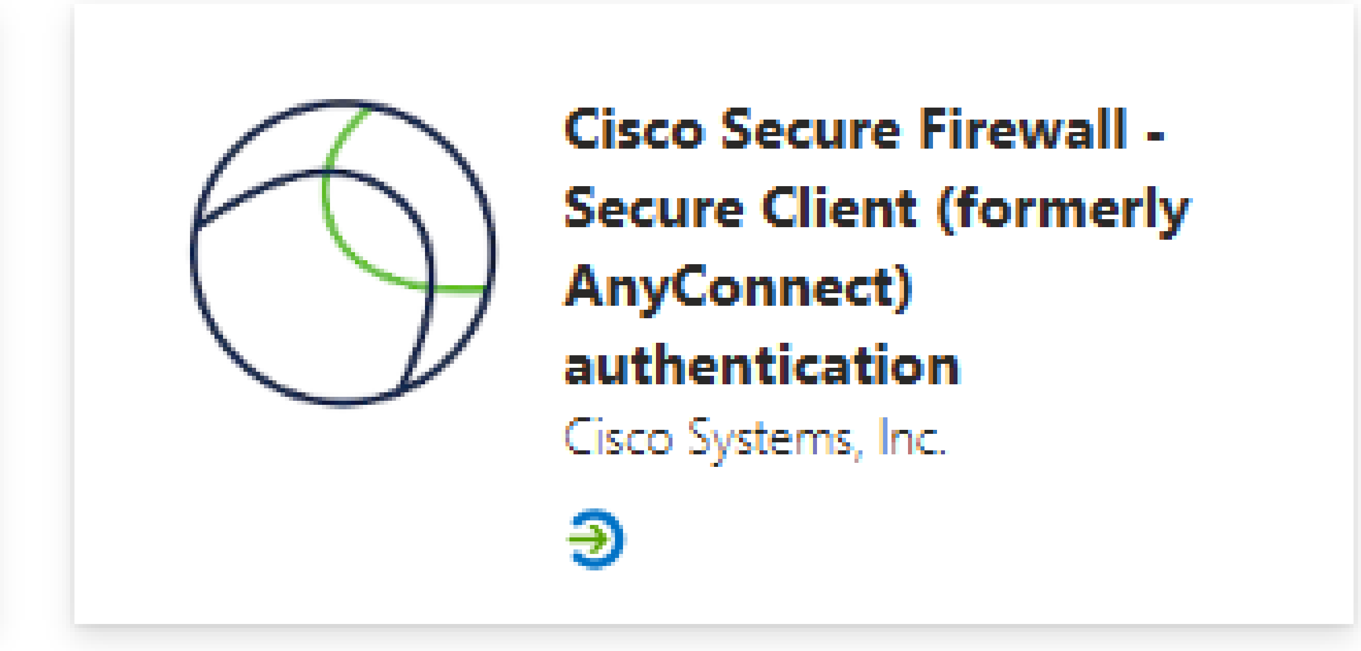


Enterprise applications | All applications

+ New application Refresh

MS Entra ID Enterprise Application

4. Select **Cisco Secure Firewall - Secure Client (formerly AnyConnect) authentication** under **Featured Applications**. Give the application a name and select **Create**.

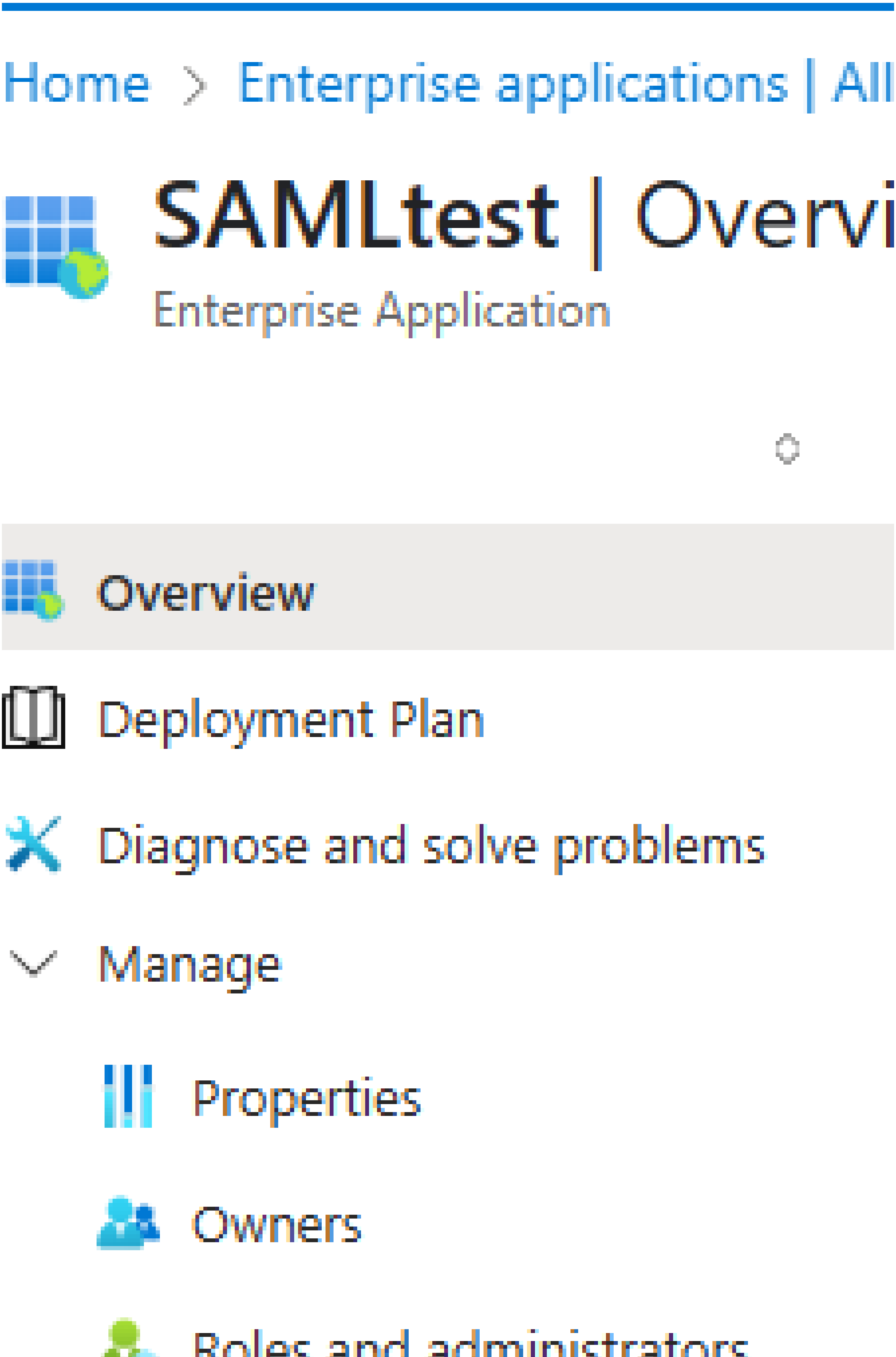


Cisco Secure Firewall - Secure Client (formerly AnyConnect) authentication

Cisco Systems, Inc.

MS Entra ID Cisco Secure Firewall Secure Client (formerly AnyConnect) authentication application

5. Once in the application, select **Users and groups** and assign the needed user or group names to the application.



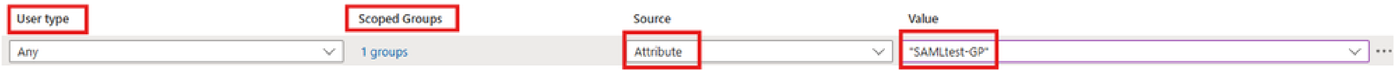
Home > Enterprise applications | All

SAMLtest | Overvi

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators

section of this guide. This value must be replaced with the group policy name from the FTD that corresponds to each user group on the IdP.



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

MS Entra ID claim condition

Verify

FTD

To verify the desired group-policy, validate the output of "**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
```

To verify the IdP is sending the desired claim, gather the output of "**debug webvpn saml 255**" while connecting to the VPN. Analyze the assertion output in the debugs and compare the attribute section to what is configured on the IdP.

<#root>

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

SAMLtest-GP

</AttributeValue>
</Attribute>
```

Troubleshoot

<#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
```

Related Information

Cisco Technical Support and Downloads

ASA Configuration Guides

FMC/FDM Configuration Guides