

セキュアファイアウォールとMicrosoft Entra IDを使用したSAMLのグループポリシー割り当ての設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[FMC SAMLの設定](#)

[FMC RAVPNトンネルグループの設定](#)

[FMC RAVPNグループポリシーの設定](#)

[FTDメタデータ](#)

[MicrosoftエントリID](#)

[確認](#)

[FTD](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Secure Firewall上のCisco Secure ClientのSAML認証にMicrosoft Entra IDを使用してグループポリシーを割り当てる方法について説明します。

前提条件

要件

次の項目に関する知識があることを推奨しています。

- CiscoセキュアクライアントAnyConnect VPN
- Cisco Firepower Threat Defense(FTD)またはCisco Secure Firewall ASAリモートアクセスVPNおよびシングルサインオン(SSO)サーバオブジェクトの設定
- Microsoft Entra ID Identity Provider (IdP)の構成

使用するコンポーネント

このガイドの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

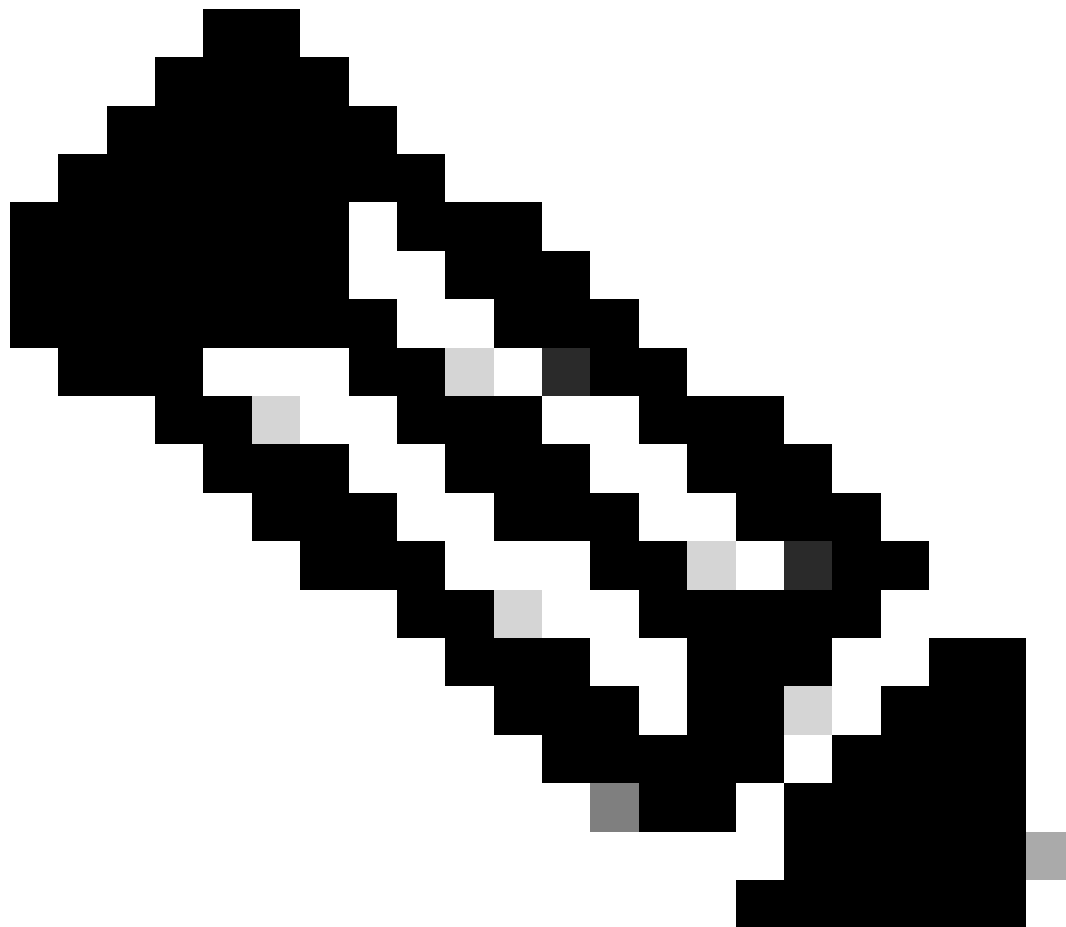
- FTDバージョン7.6
- FMCバージョン7.6
- MS Entra ID SAML IdP

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

SAML(Security Assertion Markup Language)は、セキュリティドメイン間で認証および許可データを交換するためのXMLベースのフレームワークです。ユーザ、サービスプロバイダー(SP)、およびアイデンティティプロバイダー(IdP)の間に信頼の輪を作り、ユーザが複数のサービスに対して一度にサインインできるようにします。SAMLは、ASAおよびFTD VPNヘッドエンドへのCisco Secure Client接続のリモートアクセスVPN認証に使用できます。ASAまたはFTDは、トラストサークルのSP部分です。

このドキュメントでは、IdPとしてMicrosoft Entra ID/Azureを使用します。ただし、グループポリシーはSAMLアサーションで送信可能な標準属性に基づいているため、他のIdPを使用して割り当てすることもできます。



注：各ユーザはMS Entra ID上の1つのユーザグループにのみ属する必要があります。
ASAまたはFTDに送信される複数のSAML属性が原因で、グループポリシーの割り当てに
問題が発生する可能性があります(Cisco Bug ID CSCwm33613を参照)

設定

FMC SAMLの設定

FMCで、Objects > Object Management > AAA Server > Single Sign-on Serverの順に移動します。
エンティティID、SSO URL、ログアウトURL、およびアイデンティティプロバイダー証明書
は、IdPから取得されます。「Microsoft Entra ID」の項の手順6を参照してください。ベース
URLとサービスプロバイダー証明書は、設定が追加されるFTDに固有です。

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オブジェクトの設定

FMC RAVPNトンネルグループの設定

FMCで、Devices > VPN > Remote Access > Connection Profileの順に移動し、設定するFTDのVPNポリシーを選択するか、作成します。選択したら、次のような接続プロファイルを作成します。

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

FMC接続プロファイルのアドレス割り当て

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:

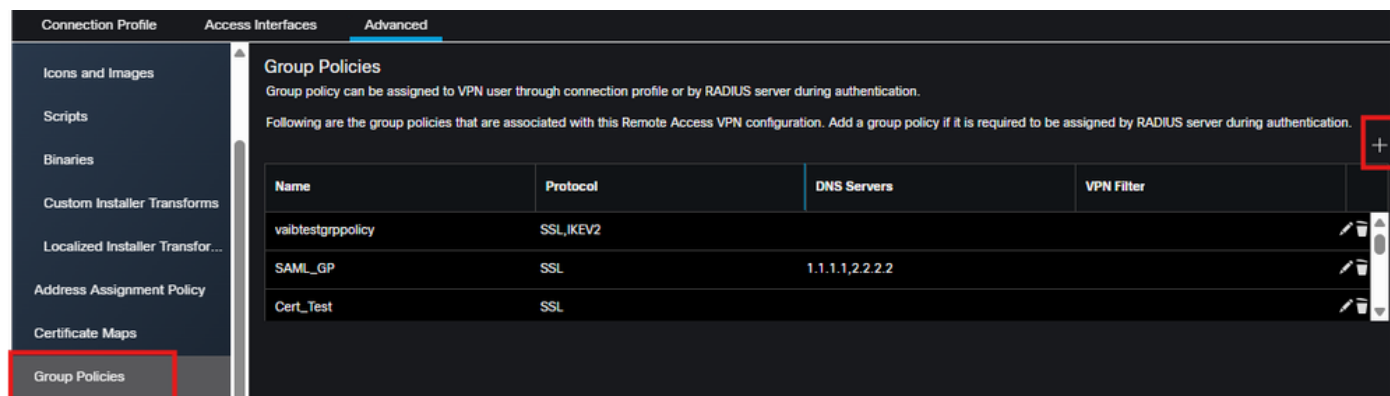
▶ [Advanced Settings](#)

[Cancel](#) [Save](#)

FMC接続プロファイルのAAA設定

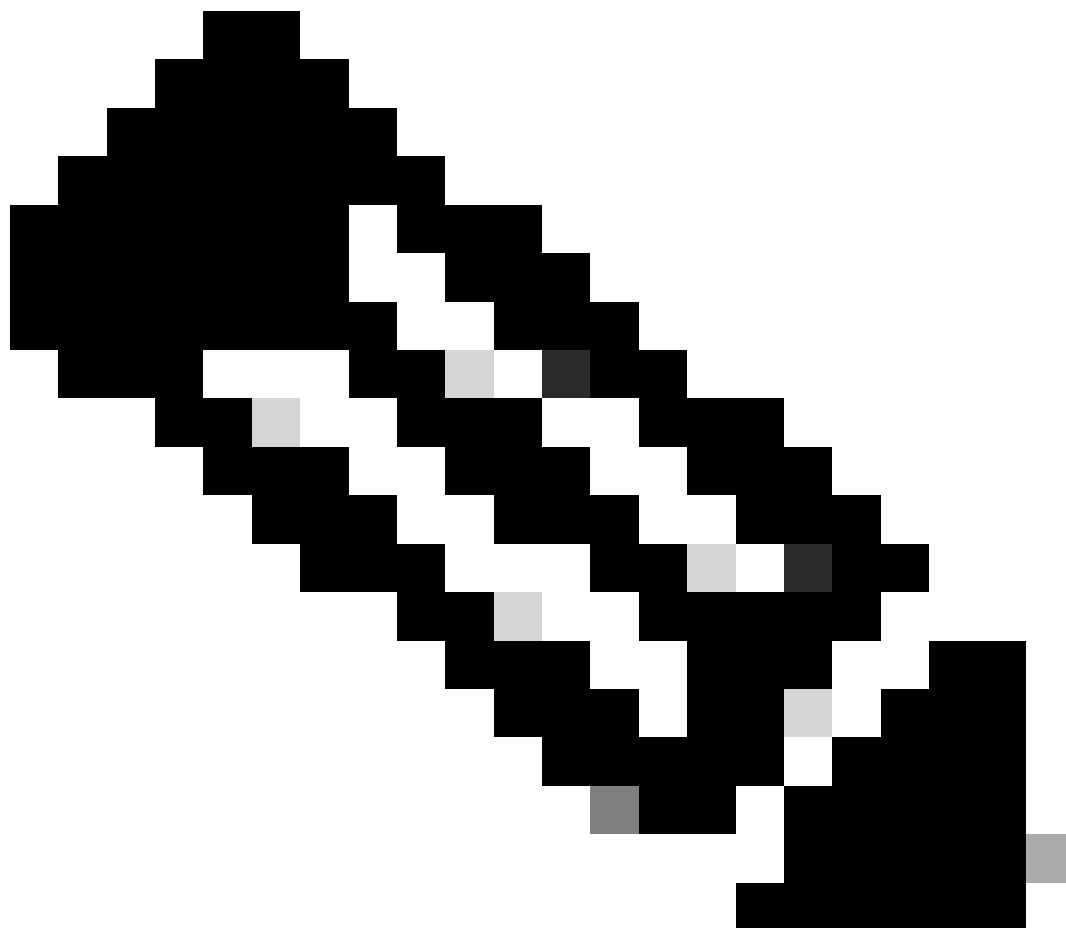
FMC RAVPNグループポリシーの設定

1. エントリIDの各ユーザグループに必要なオプションでグループポリシーを作成し、設定中のFTDのRAVPNポリシーに追加する必要があります。それには、Devices > VPN > Remote Access > Advanced の順に選択し、左側でGroup Policiesを選択してから、右上の+ をクリックしてグループポリシーを追加します。



FMCグループポリシーの追加

2. ポップアップの[+]をクリックすると、新しいグループポリシーを作成するためのダイアログが表示されます。必要なオプションを入力して保存します。



注：必要なグループポリシーがすでに作成されている場合は、このステップを省略してステップ3に進むことができます

Group Policy

Available Group Policy



Search

新しいグループポリシーの作成

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

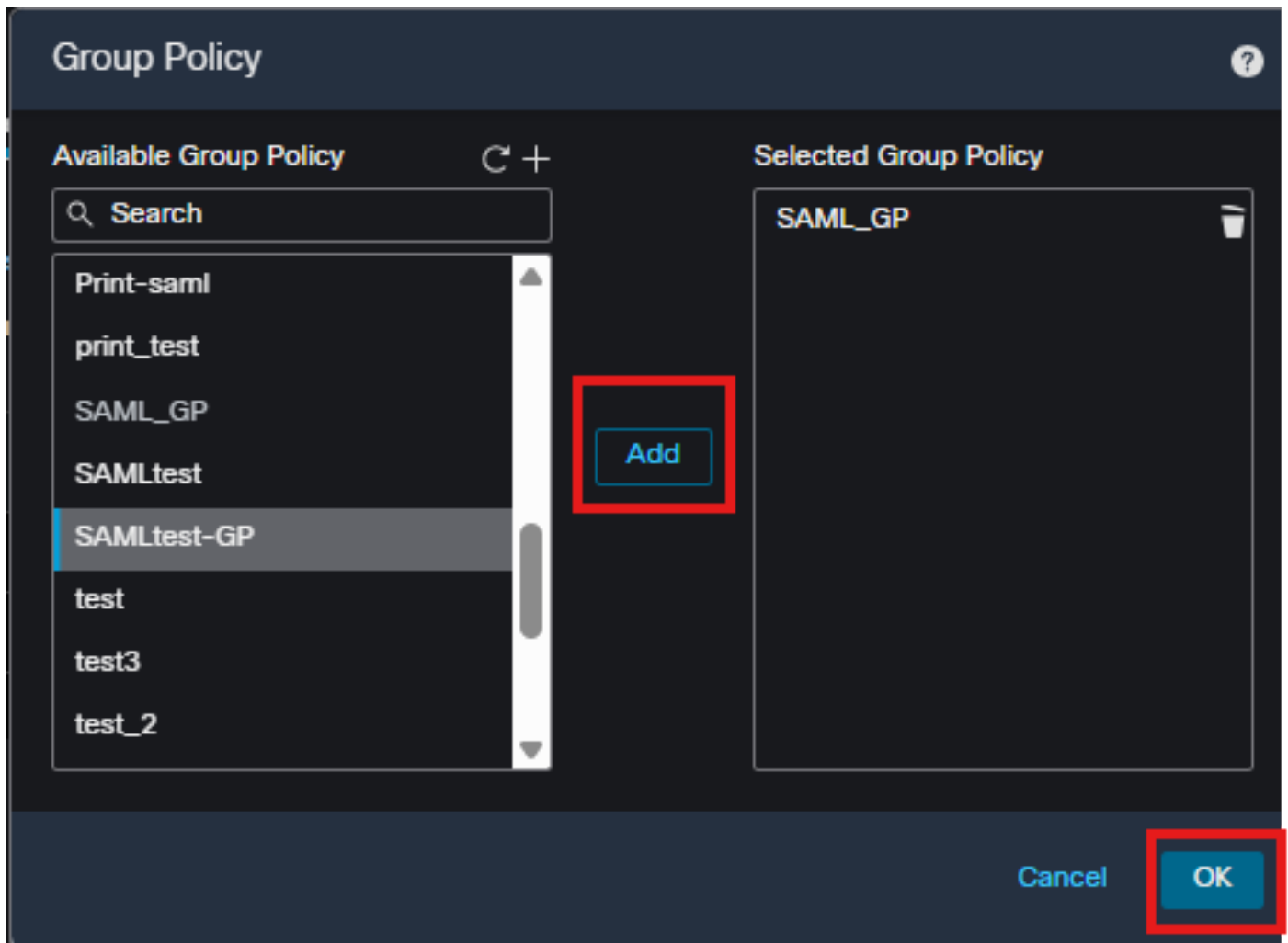
☒ IPsec-IKEv2

Cancel

Save

グループポリシーオプション

3. 左側のリストで新しく作成したグループポリシーを選択し、Addボタンをクリックしてから、Okをクリックしてリストを保存します。



グループポリシーの追加

FTDメタデータ

設定がFTDに展開されたら、FTD CLIに移動してコマンド「show saml metadata <tunnel group name>」を実行し、FTD エンティティIDとACS URLを収集します。



注：メタデータ内の証明書は、簡略化のために省略されています。

<#root>

FTD# show sam1 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>
MIIFWzCCBE0gAwIBAgITRwAAAAGZ9Nmfv5mpJQAAAAACDANBgqhkiG9w0BAQsF
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 エントリ ID

1. Microsoft Azure ポータルで、左側のメニューから Microsoft Entra ID を選択します。



Create a resource



Home



Dashboard



All services



FAVORITES



All resources



Resource groups



App Services



Function App



SQL databases



Azure Cosmos DB



Virtual machines

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

IdPが必要なクレームを送信していることを確認するには、VPNに接続している間に「debug webvpn saml 255」の出力を収集します。デバッグでアサーション出力を分析し、属性セクションをIdPで設定されているものと比較します。

<#root>

<Attribute Name="cisco_group_policy">

<AttributeValue>

SAMLtest-GP

</AttributeValue>

</Attribute>

トラブルシュート

<#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
```

関連情報

[シスコテクニカルサポートおよびダウンロード](#)

[ASA設定ガイド](#)

[FMC/FDM構成ガイド](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。