

ASAでのSAMLによる複数のトンネルグループの設定

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](#)

[SAML SPが開始したSSO](#)

[コンフィギュレーション](#)

[ギャラリーからのCisco Secure Firewall - Secure Clientの追加](#)

[Azure ADユーザーをアプリに割り当てる](#)

[CLIによるASAの設定](#)

[確認](#)

[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 ASA上の複数のトンネルグループに対するAzure Identity Providerを使用したSAML認証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が推奨されます。

- 適応型セキュリティ アプライアンス (ASA)
- Security Assertion Markup Language(SAML)
- Secure Socket Layer(SSL)証明書
- Microsoft Azure

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA 9.22(1)1
- SAML 2.0を使用したMicrosoft Azure Entra ID

- Cisco Secureクライアント5.1.7.80

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

Microsoft Azureでは、同じエンティティIDに対して複数のアプリケーションをサポートできます。（異なるトンネルグループにマッピングされた）各アプリケーションには、一意の証明書が必要です。ASAでは、IdP証明書機能により、異なるOverride Identity Provider(IdP)で保護されたアプリケーションを使用するように複数のトンネルグループを設定できます。この機能を使用すると、管理者は、各トンネルグループの特定のIdP証明書で、シングルサインオン(SSO)サーバオブジェクトのプライマリIdP証明書を上書きできます。この機能は、ASAバージョン9.17.1以降で導入されました。

SAML SPが開始したSSO

エンドユーザがASAにアクセスしてログインを開始すると、サインオン動作は次のように行われます。

1. VPNユーザがSAML対応のトンネルグループにアクセスまたは選択すると、エンドユーザは認証のためにSAML IdPにリダイレクトされます。ユーザがグループURLに直接アクセスしない限り、ユーザにプロンプトが表示されます。この場合、リダイレクトはsilentになります。
2. ASAがSAML認証要求を生成し、ブラウザがその要求をSAML IdPにリダイレクトします。
3. IdPはエンドユーザにクレデンシャルの入力を求め、エンドユーザはログインします。入力したクレデンシャルは、IdP認証の設定を満たしている必要があります。
4. IdP応答がブラウザに返送され、ASAサインインURLに送信されます。ASAが応答を確認してログインを完了します。

コンフィギュレーション

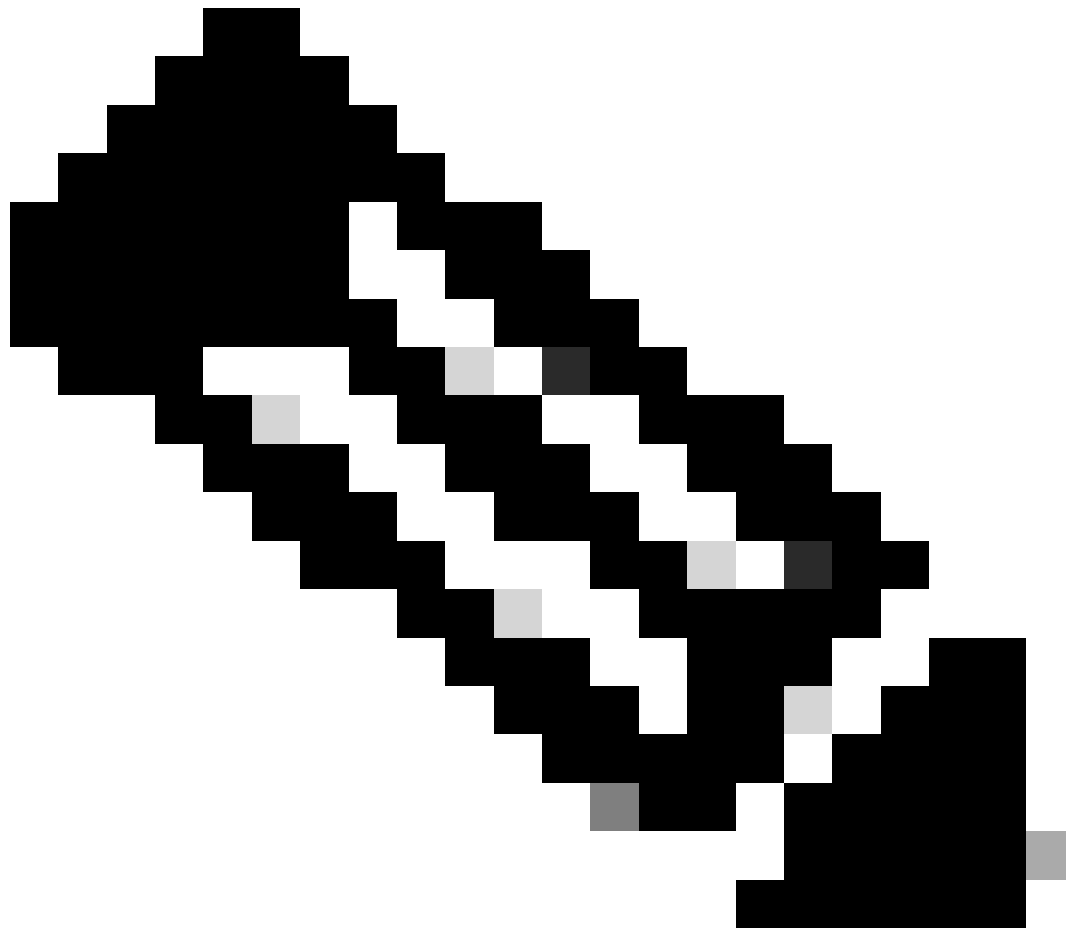
ギャラリーからのCisco Secure Firewall - Secure Clientの追加

この例では、Microsoft Entra SSOとCisco Secure Firewall - Secure Client on Azureの統合が、ASAで設定された2つのトンネルグループに追加されます。

- SAML1
- SAML2

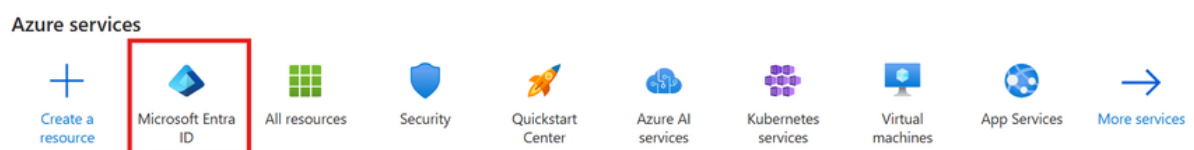
Microsoft Entra IDへのCisco Secure Firewall - Secure Clientの統合を設定するには、ギャラリーから管理対象SaaSアプリケーションのリストにCisco Secure Firewall - Secure Clientを追加する必

必要があります。



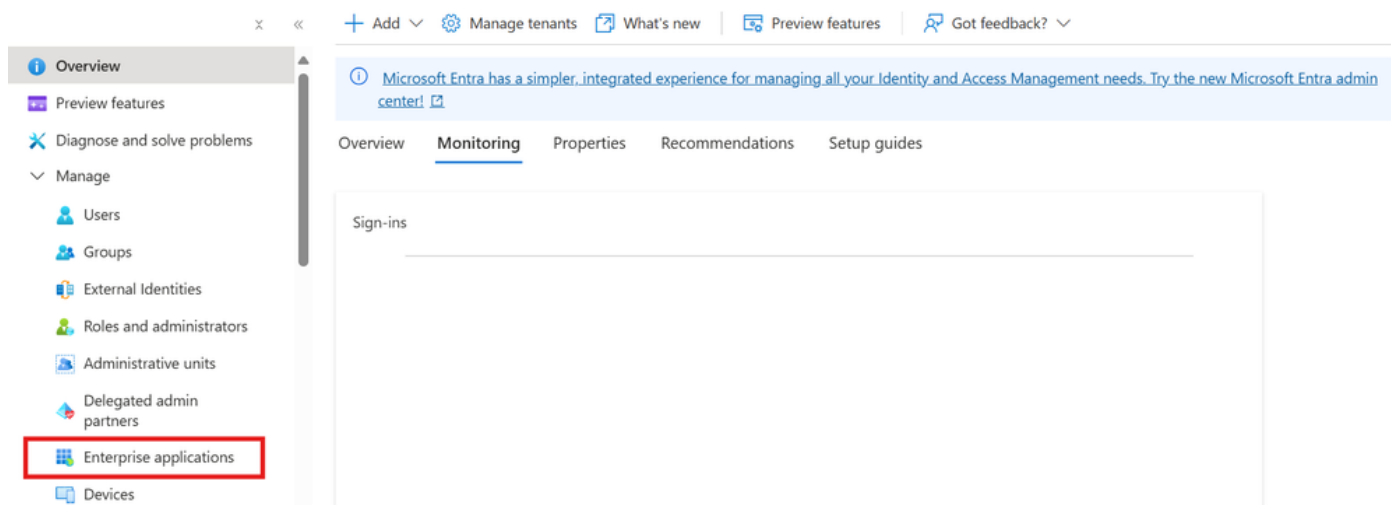
注：これらの手順は、最初のトンネルグループSAML1のギャラリーにCisco Secure Firewall - Secure Clientを追加するためのものです。

ステップ 1：Azure Portalにログインして、Microsoft Entra IDを選択します。



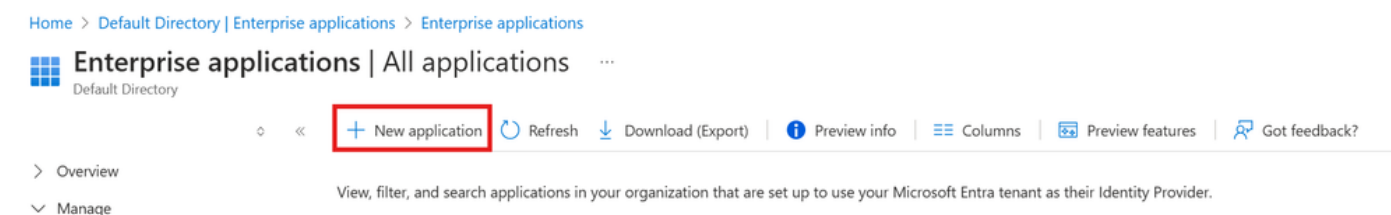
MicrosoftエントリD

ステップ 2 : この図に示すように、Enterprise Applicationsを選択します。



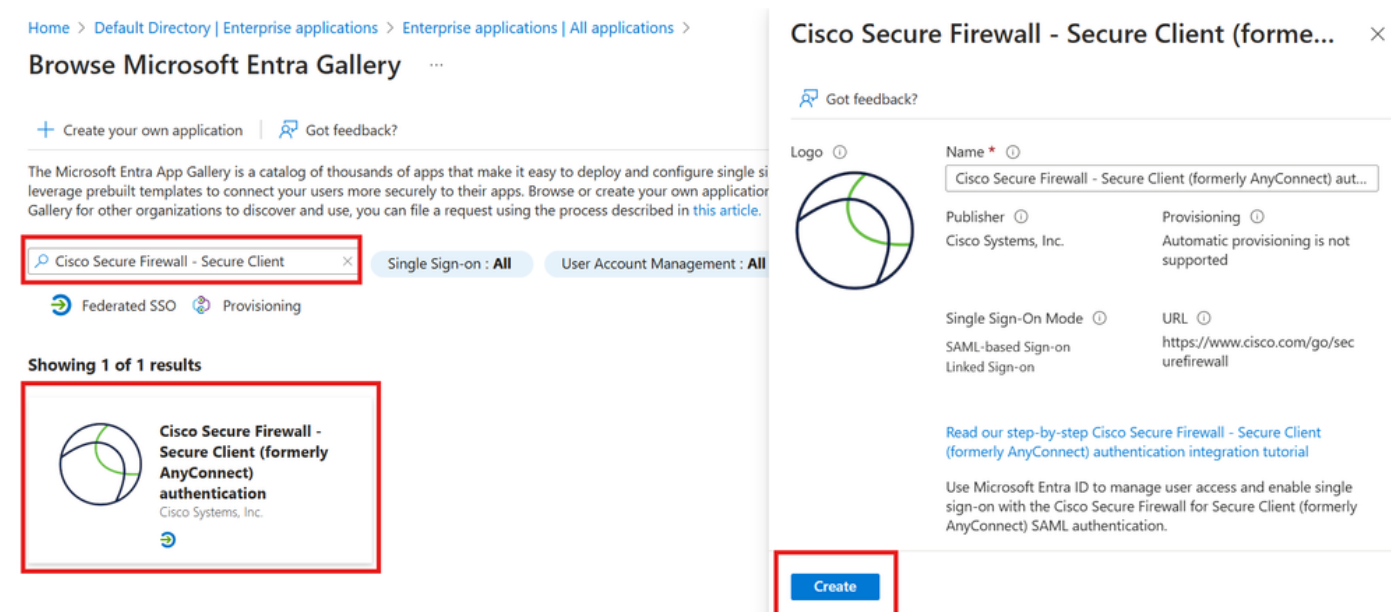
企業アプリケーション

ステップ 3 : ここで、次の図に示すように New Applicationを選択します。

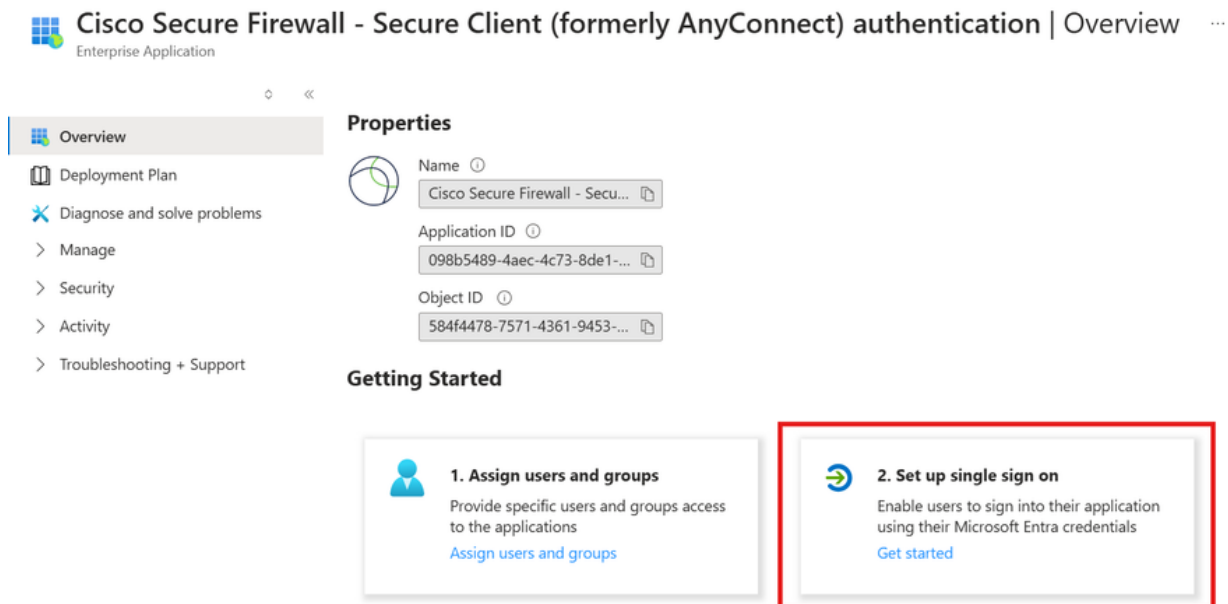


新しいアプリケーション

ステップ 4 : Add from the galleryセクションで、検索ボックスにCisco Secure Firewall - Secure Clientと入力し、結果パネルからCisco Secure Firewall - Secure Clientを選択して、アプリケーションをaddします。

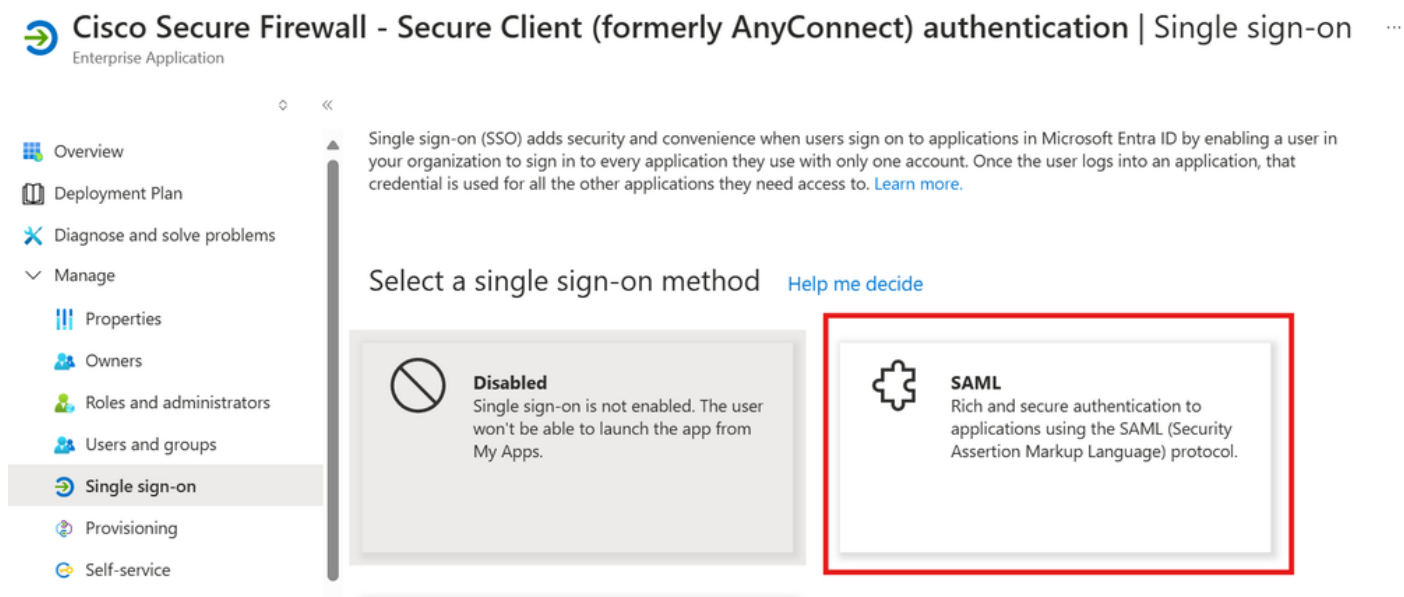


ステップ 5：次の図に示すように、Single Sign-onメニュー項目を選択します。



シングルサインオンのセットアップ

手順 6：Select a single sign-on メソッドページで、SAMLを選択します。



SAML

手順 7：Set up single sign-on with SAMLページで、Basic SAML Configurationの編集/ペンアイコンをクリックし、設定を編集します。

Basic SAML Configuration



Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

基本的なSaml設定

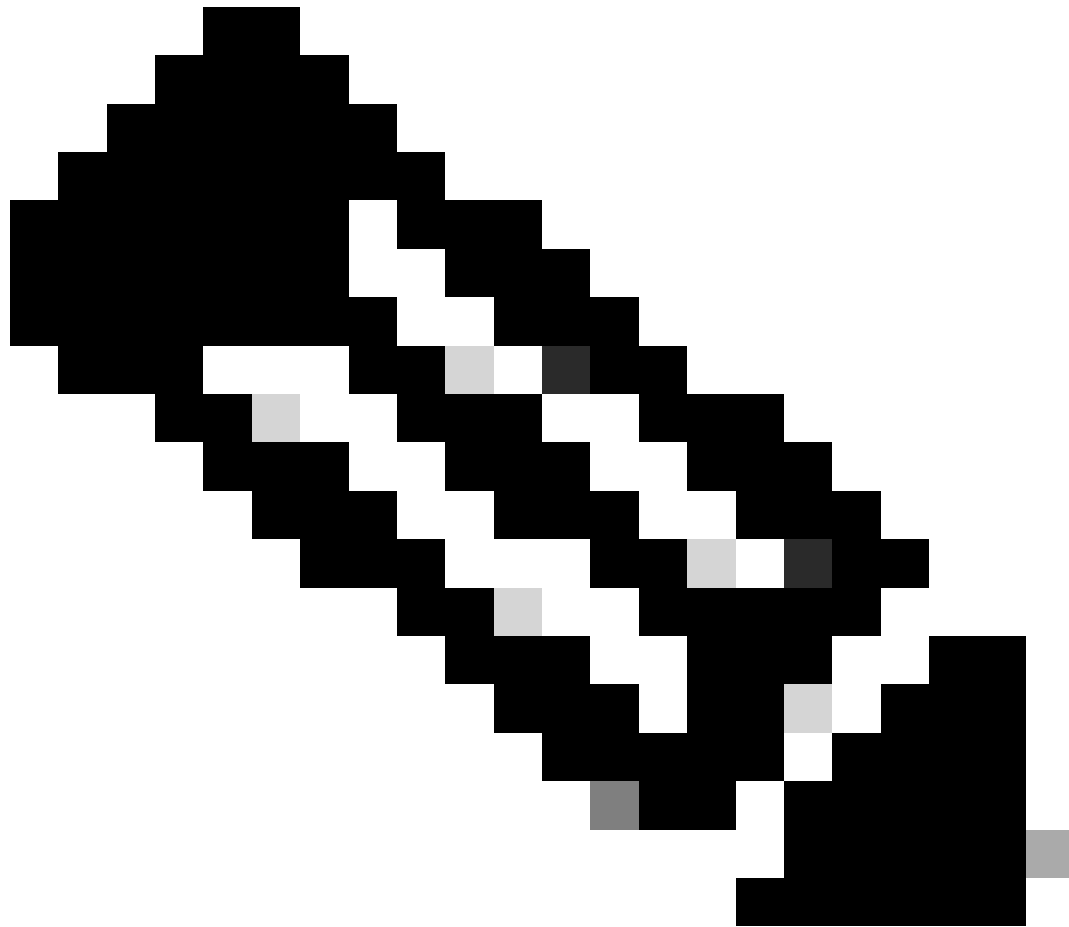
ステップ 8 : Set up single sign-on with SAMLページで、次のフィールドの値を入力します。

a. 「識別子」テキストボックスに、次のパターンを使用してURLを入力します。

`https://<VPN URL>/saml/sp/metadata/<Tunnel_Group_Name>`

b. 「返信URL」テキスト・ボックスに、次のパターンを使用してURLを入力します。

`https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<Tunnel_Group_Name>`
`[Tunnel_Group_Name = SAML1]`



注:Tunnel_Group_Nameでは大文字と小文字が区別されるため、値にドット「。」やスラッシュ「/」を含めることはできません。

ステップ 9 : Set up single sign-on with SAMLページのSAML Signing Certificateセクションで、Certificate (Base64)を見つけ、Downloadを選択し、証明書ファイルをダウンロードしてコンピュータに保存します。

SAML Certificates

Token signing certificate

[Edit](#)

Status

Active

Thumbprint

1040191128945102

Expiration

2/4/2028, 4:33:14 PM

Notification Email

nishi.ashimaru@gmail.com

App Federation Metadata Url

https://

Certificate (Base64)

[Download](#)

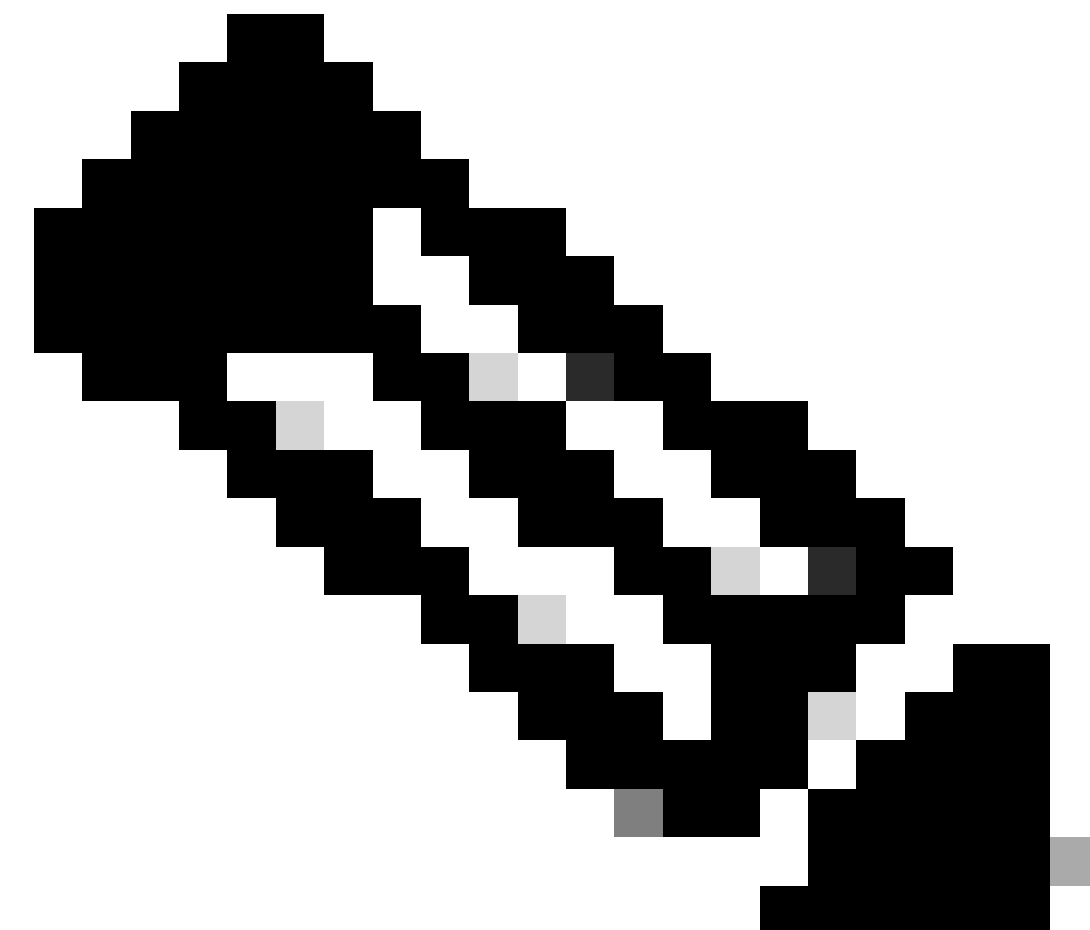
Certificate (Raw)

[Download](#)

Federation Metadata XML

[Download](#)

証明書(Base64)のダウンロード



注：このダウンロードされた証明書は、ASAトラストポイントAzureAD-AC-SAML1にインポートされます。詳細については、「ASAの設定」セクションを参照してください。

ステップ 10 : Cisco Secure Firewall - Secure Clientの設定セクションで、要件に基づいて適切なURLをコピーします。これらのURLは、ASAでSSOサーバオブジェクトを設定するために使用されます。

- Microsoft Entra Identifier : これはVPN設定のSAML IDです。
- ログインURL : これはURLサインインです。
- Logout URL : これはURLのサインアウトです。

Set up Cisco Secure Firewall - Secure Client (formerly AnyConnect) authentication

You'll need to configure the application to link with Microsoft Entra ID.

Login URL

<https://login.microsoftonline.com/65d917a5-74a4...> 

Microsoft Entra Identifier

<https://sts.windows.net/65d917a5-74a4-42aa-8e3...> 

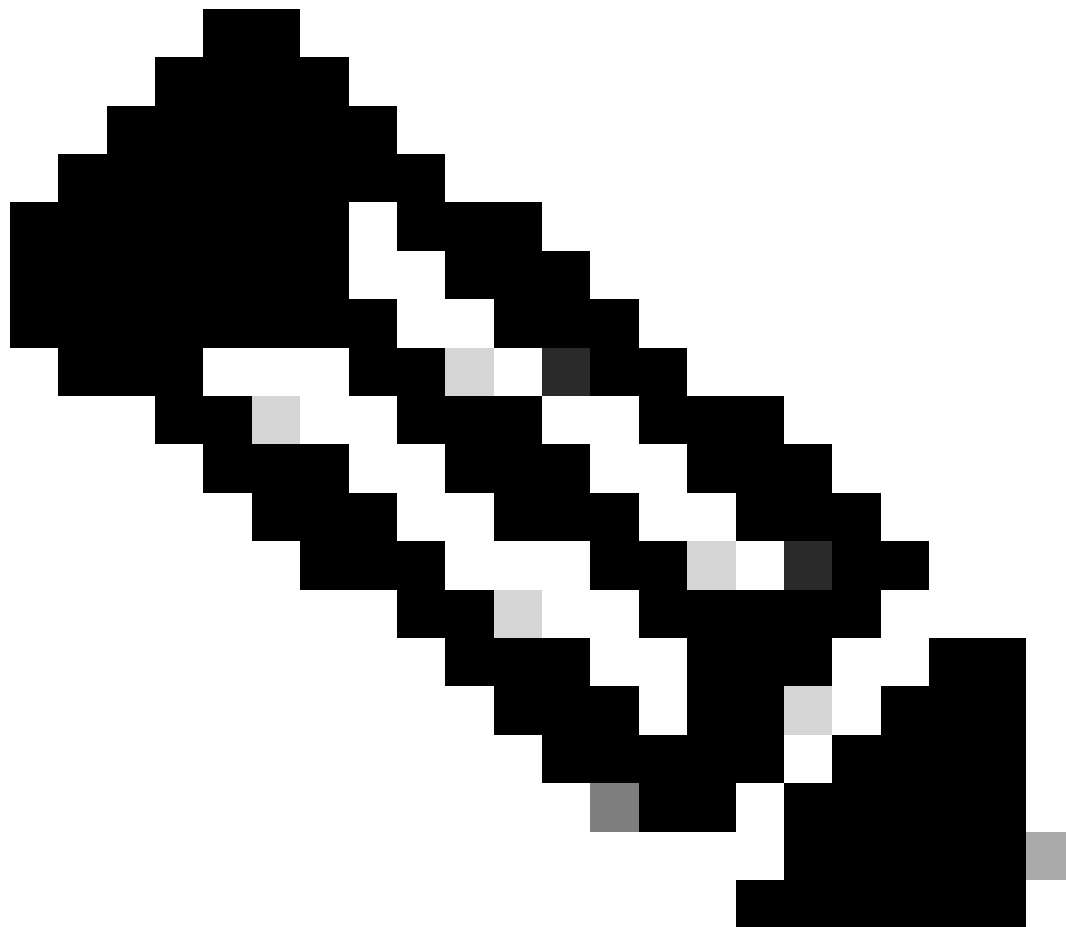
Logout URL

<https://login.microsoftonline.com/65d917a5-74a4...> 

SSOのURL



注：前述の設定手順を繰り返して、2番目のトンネルグループのギャラリーからCisco Secure Firewall - Secure Clientアプリケーションを追加します。この場合の2番目のトンネルグループ名はSAML2です。



注:2番目のトンネルグループ(SAML 2)にCisco Secure Firewall - Secure Clientアプリケーションを追加する際に、手順8.でダウンロードしたAzure証明書がASAトラストポイント AzureAD-AC-SAML2にインポートされます。

Azure ADユーザーをアプリに割り当てる

このセクションでは、Cisco Secure Clientアプリへのアクセスを許可するときに、Test1とTest2でAzure SSOの使用が有効になります。

最初のIdPアプリケーションの場合：

ステップ 1：最初のIdPアプリケーション概要ページで、Users and groups、Add userの順に選択します。

Cisco SAML 1 | Users and groups ...
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups ☆
Single sign-on

+ Add user/group Edit assignment Remove assignment Update credential Refresh Manage view Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#)

First 200 shown, search all users & groups

Display name	Object type
No application assignments found	

ユーザとグループ

ステップ 2：割り当ての追加ダイアログでユーザまたはグループを選択します。

Add Assignments
Default Directory

Try changing or adding filters if you don't see what you're looking for.

Search

4 results found

All Users

Users
None Selected
Select a role
Default Access

 Test1	User
---	------

課題1の追加

ステップ 3：割り当ての追加ダイアログで、割り当てボタンをクリックします。

Add Assignment ...

Default Directory

Users

1 user selected.

Select a role

Default Access

Assign

Test1ユーザ割り当て

2番目のIdPアプリケーションの場合：

上記の図に示すように、2番目のIDPアプリケーションに対して上記の手順を繰り返します。

Add Assignment ...

Default Directory

Users

1 user selected.

Select a role

Default Access

Assign

課題2の追加

Home > Default Dir

Add Assignment

Default Directory

Users

Try changing or adding filters if you don't see what you're looking for.

Search



4 results found

All Users

	Name	Type	Details
☐	 Test2	User	

Selected (0)

Reset

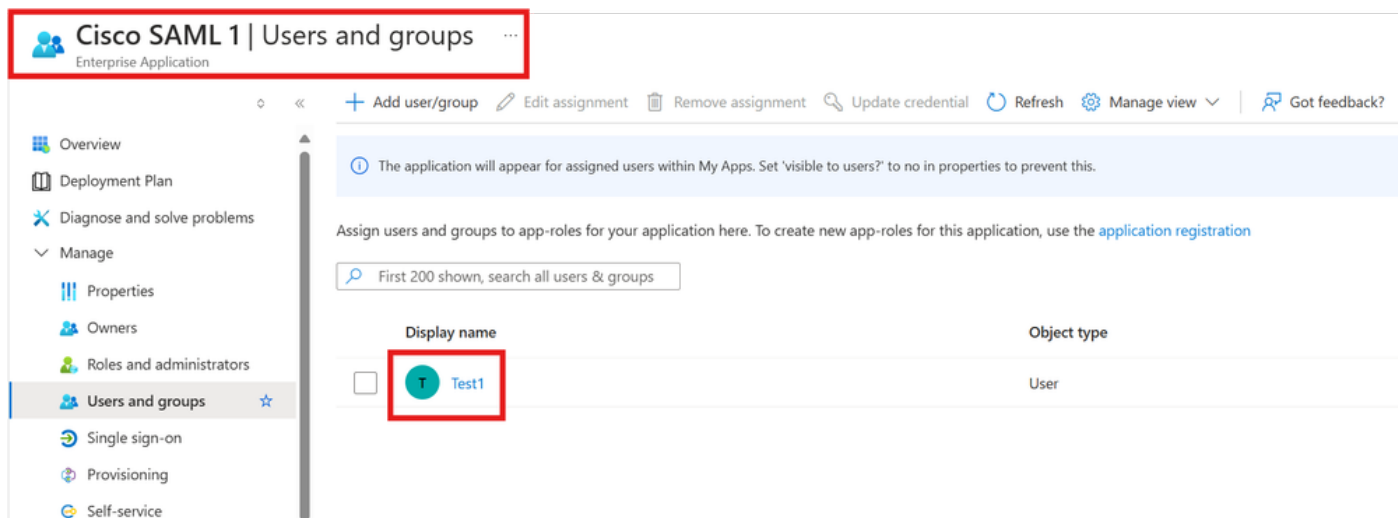
No items selected

Assign

Select

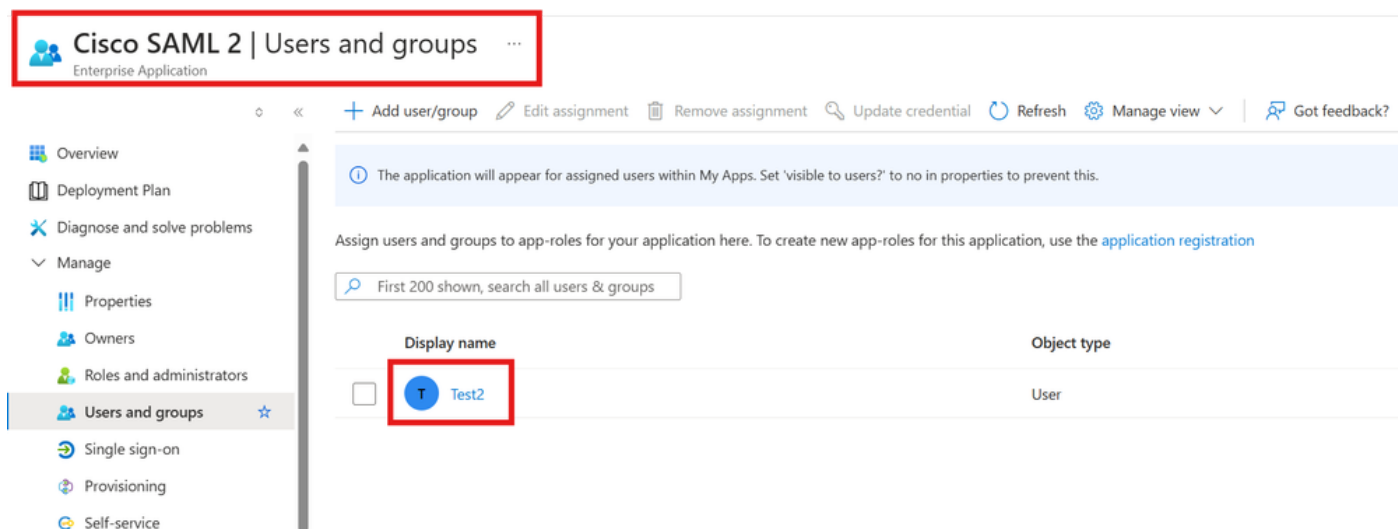
Test2ユーザ割り当て

Test1ユーザ割り当て :



テスト1のユーザ割り当て

Test2ユーザ割り当て：



テスト2のユーザ割り当て

CLIによるASAの設定

ステップ 1：トラストポイントを作成し、SAML証明書をインポートします。

2つのトラストポイントを設定し、各トンネルグループのそれぞれのSAML証明書をインポートします。

```
<#root>
```

```
config t
```

```
crypto ca trustpoint
```

```
AzureAD-AC-SAML1
```

```
revocation-check none
no id-usage
```

```
enrollment terminal
no ca-check
crypto ca authenticate
```

AzureAD-AC-SAML1

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
PEM Certificate Text you downloaded from AzureAD goes here
```

```
...
```

```
-----END CERTIFICATE-----
```

```
quit
```

```
!  
!
```

```
crypto ca trustpoint
```

AzureAD-AC-SAML2

```
revocation-check none
no id-usage
enrollment terminal
no ca-check
crypto ca authenticate
```

AzureAD-AC-SAML2

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
PEM Certificate Text you downloaded from AzureAD goes here
```

```
...
```

```
-----END CERTIFICATE-----
```

```
quit
```

ステップ 2 : SAML IdPを設定します。

SAML IdP設定をプロビジョニングするには、次のコマンドを使用します。

```
webvpn
```

```
saml idp https://xxx.windows.net/xxxxxxxxxxxxx/ - [Azure AD Identifier]
url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
url sign-out https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxx/saml2 - [Logout URL]
trustpoint idp AzureAD-AC-SAML1 - [IdP Trustpoint]
trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
no force re-authentication
no signature
base-url https://asa.example.com
```

ステップ 3最初のVPNトンネルグループにSAML認証を適用します。

AzureAD-AC-SAML1 IdPトラストポイントでSAML1トンネルグループを設定します。

<#root>

```
tunnel-group SAML1 webvpn-attributes
authentication saml
group-alias SAML1 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML1 <---- Overrides the primary IDP certificate in the Single Sign-On (SSO) configuration.

ステップ 4 : 2番目のVPNトンネルグループにSAML認証を適用します。

AzureAD-AC-SAML2 IdPトラストポイントでSAML2トンネルグループを設定します。

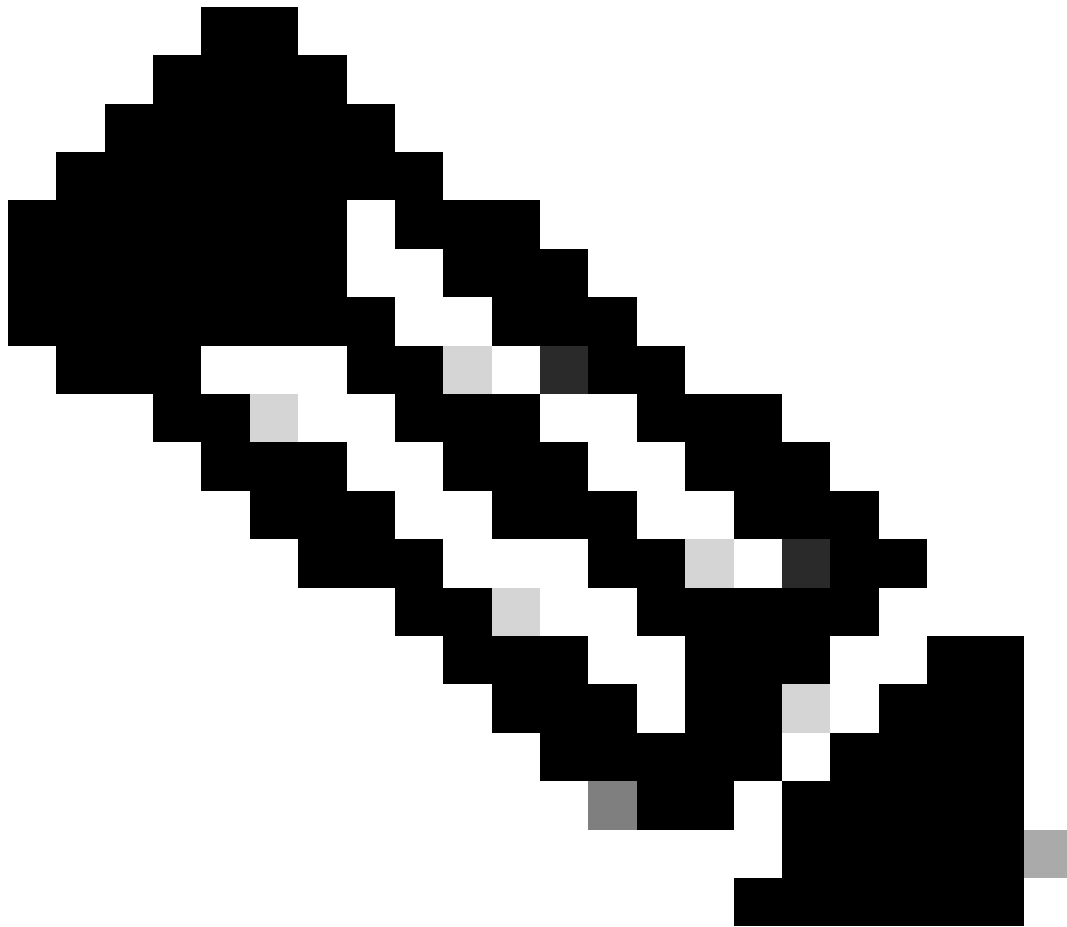
<#root>

```
tunnel-group SAML2 webvpn-attributes
authentication saml
group-alias SAML2 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML2 <---- Overrides the primary IDP certificate in the Single Sign-On (SSO) configuration.

ステップ5 : 設定を保存します。

write memory



注:IdP設定を変更した場合、変更を有効にするには、トンネルグループからSAML IDプロバイダー設定を削除し、再適用する必要があります。

確認

SAML認証を使用したAnyConnectのテスト

ステップ 1 : VPN URLに接続し、Azure ADの詳細にログインします。

ステップ2: (オプション) サインイン要求を承認します。

ステップ3:AnyConnectが接続されます。

トラブルシュート

SAMLのトラブルシューティングのほとんどは、SAMLの設定をチェックするか、デバッグを実行すると判明する誤設定を含んでいます。debug webvpn saml 255は、ほとんどの問題のトラブルシューティングに使用できますが、このデバッグで有用な情報が提供されないシナリオでは、追加のデバッグを実行できます。

```
debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
```

関連情報

- [Microsoft Azure MFA で SAML を利用した ASA AnyConnect VPN の設定](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

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。