

Microsoft Azure MFA で SAML を利用した ASA AnyConnect VPN 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コンポーネント](#)

[署名および暗号化操作の証明書](#)

[ネットワーク図](#)

[設定](#)

[Microsoft App GalleryからのCisco AnyConnectの追加](#)

[Azure ADユーザーのアプリへの割り当て](#)

[CLIによるSAML用のASAの設定](#)

[確認](#)

[SAML認証を使用したAnyConnectのテスト](#)

[一般的な問題](#)

[エンティティIDの不一致](#)

[時間の不一致](#)

[誤ったIdP署名証明書の使用](#)

[無効なアサーションオーディエンス](#)

[アサーションコンシューマサービスのURLが正しくありません](#)

[SAML設定の変更が有効にならない](#)

[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、Adaptive Security Appliance(ASA)AnyConnectからMicrosoft Azure MFAを使用してSecurity Assertion Markup Language(SAML)を設定す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が推奨されます。

- ASAでのRA VPN設定に関する基本的な知識。
- SAMLおよびMicrosoft Azureに関する基本的な知識
- AnyConnectライセンス対応 (APEXまたはVPN-Only)

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。

- Microsoft Azure ADサブスクリプション。
- Cisco ASA 9.7+およびAnyconnect 4.6+
- AnyConnect VPNプロファイルの動作

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。これにより、ユーザ、サービスプロバイダー(SP)、および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アイデンティティプロバイダー(IdP)の間に信頼関係が構築されます。Microsoft Azure MFAはCisco ASA VPNアプライアンスとシームレスに統合され、Cisco AnyConnect VPNロゲインのセキュリティを強化します。

SAMLコンポーネント

メタデータ : IdPとSP間の安全なトランザクションを保証するXMLベースのドキュメントです。IdPとSPが契約を交渉できる

デバイスでサポートされるロール(IdP、SP)

デバイスは複数のロールをサポートでき、SPとIdPの両方の値を含むことができます。EntityDescriptorフィールドの下には、含まれている情報がシングルサインオンIdP用の場合はIDPSSODescriptorが、含まれている情報がシングルサインオンSP用の場合はSPSSODescriptorが表示されます。SAMLを正しく設定するには、適切なセクションから正しい値を取得する必要があるため、これは重要です。

エンティティID : このフィールドは、SPまたはIdPの一意の識別子です。1つのデバイスに複数のサービスを設定し、異なるエンティティIDを使用してそれらを区別することができます。たとえば、認証が必要なトンネルグループごとにASAのエンティティIDが異なる場合などです。各トンネルグループを認証するIdPには、これらのサービスを正確に識別するために、各トンネルグループに対して個別のエンティティIDエントリがあります。

ASAは複数のIdPをサポートでき、IdPごとに個別のエンティティIDを持って区別します。いずれかの側が、以前に設定されたエンティティIDを含まないデバイスからメッセージを受信した場合、デバイスはこのメッセージをドロップする可能性があり、SAML認証は失敗します。エンティ

ティIDは、entityIDの横のEntityDescriptorフィールドに表示されます。

サービスURL:SPまたはIdPによって提供されるSAMLサービスへのURLを定義します。IdPsの場合、これは最も一般的にはシングルログアウトサービスとシングルサインオンサービスです。SPの場合、これは通常、アサーションコンシューマサービスとシングルログアウトサービスです。

IdPメタデータに含まれるSingle Sign-On Service URLは、SPが認証のためにユーザをIdPにリダイレクトするために使用します。この値が正しく設定されていない場合、IdPはSPから送信された認証要求を受信しないか、正常に処理できません。

SPメタデータで見つかったアサーションコンシューマサービスURLは、IdPによってユーザをSPにリダイレクトし、ユーザの認証の試行に関する情報を提供するために使用されます。この設定が正しくない場合、SPはアサーション（応答）を受信しないか、正常に処理できません。

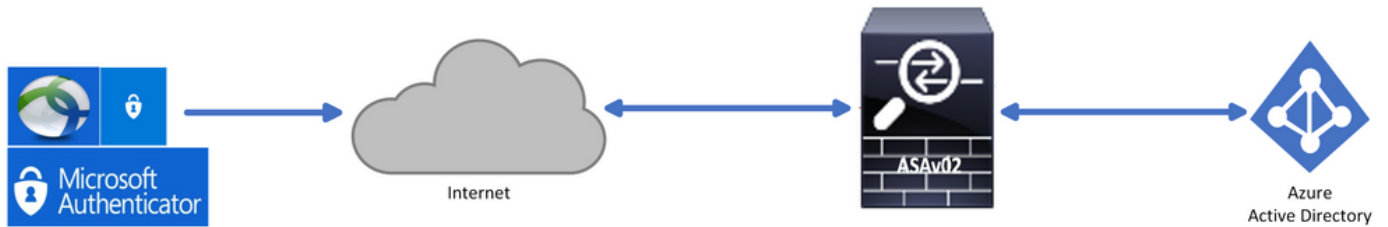
シングルログアウトサービスURLは、SPとIdPの両方にあります。これは、SPからのすべてのSSOサービスのログアウトを容易にするために使用され、ASAではオプションです。IdPメタデータからのSLOサービスURLがSPで設定されている場合、ユーザーがSP上のサービスからログアウトすると、SPはIdPに要求を送信します。IdPは、ユーザをサービスから正常にログアウトすると、ユーザをSPにリダイレクトして戻し、SPのメタデータ内にあるSLOサービスURLを使用します。

サービスURLのSAMLバインディング：バインディングは、SPが情報をIdPに転送したり、サービスをIdPに転送したりするために使用する方法です。これには、HTTPリダイレクト、HTTP POST、アーティファクトが含まれます。データを転送する方法は、それぞれの方法で異なります。サービスによってサポートされるバインド方式は、そのサービスの定義内に含まれます。例：
SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location=<https://saml.example.com/simplesaml/saml2/idp/SSOService.php/> >ASAはアーティファクトのバインドをサポートしていません。ASAはSAML認証要求に対して常にHTTPリダイレクト方式を使用するため、HTTPリダイレクトバインディングを使用するSSOサービスURLを選択して、IdPがこれを想定することが重要です。

署名および暗号化操作の証明書

SPとIdPの間で送信されるメッセージの機密性と整合性を確保するために、SAMLにはデータを暗号化して署名する機能が含まれています。データの暗号化や署名に使用される証明書をメタデータに含めることで、受信側はSAMLメッセージを検証し、そのメッセージが予期されるソースから送信されていることを確認できます。署名と暗号化に使用される証明書は、KeyDescriptor use="signing"、KeyDescriptor use="encryption"の下のメタデータに含まれており、それぞれX509Certificateの下にあります。ASAはSAMLメッセージの暗号化をサポートしていません。

ネットワーク図

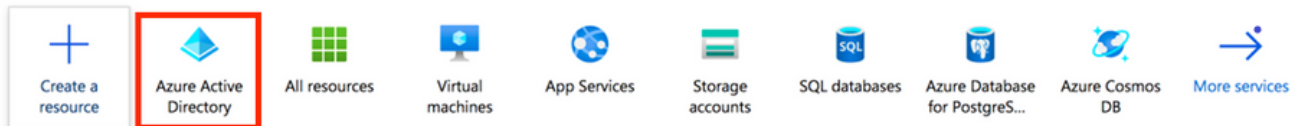


設定

Microsoft App GalleryからのCisco AnyConnectの追加

ステップ1: Azure Portalにログインし、Azure Active Directoryを選択します。

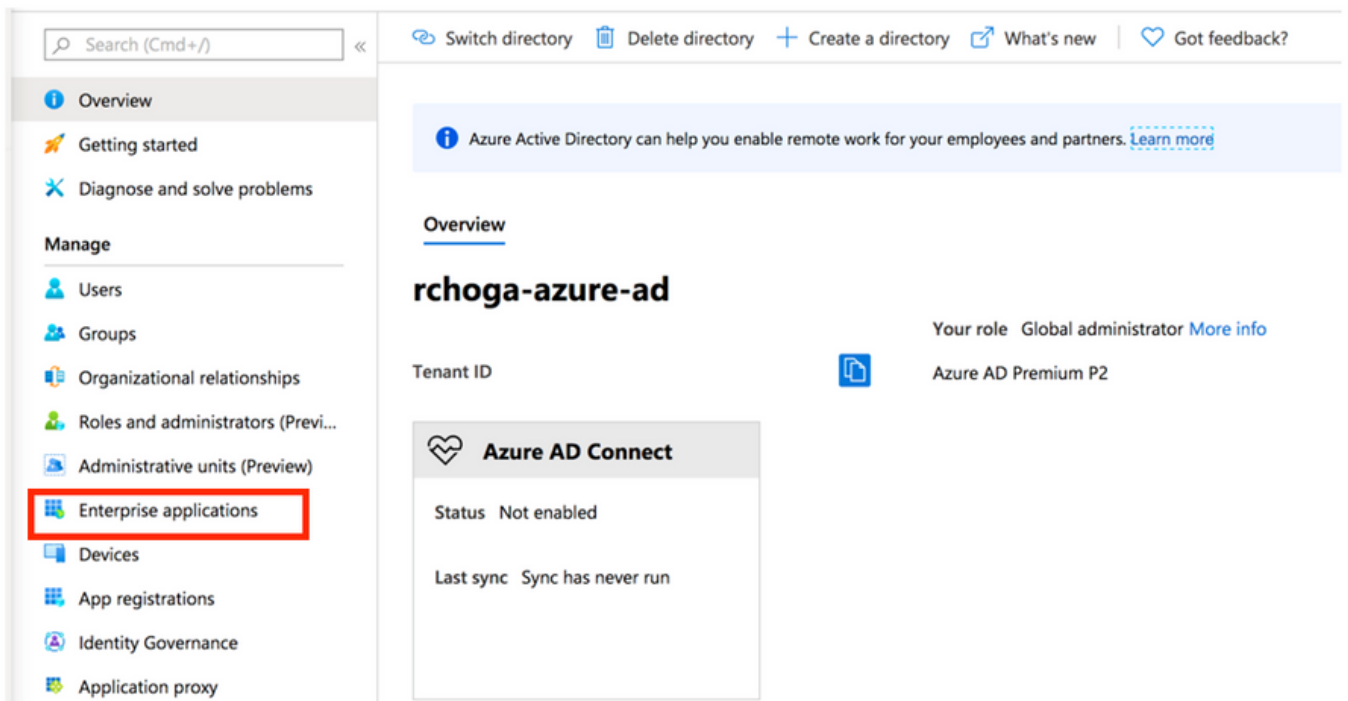
Azure services



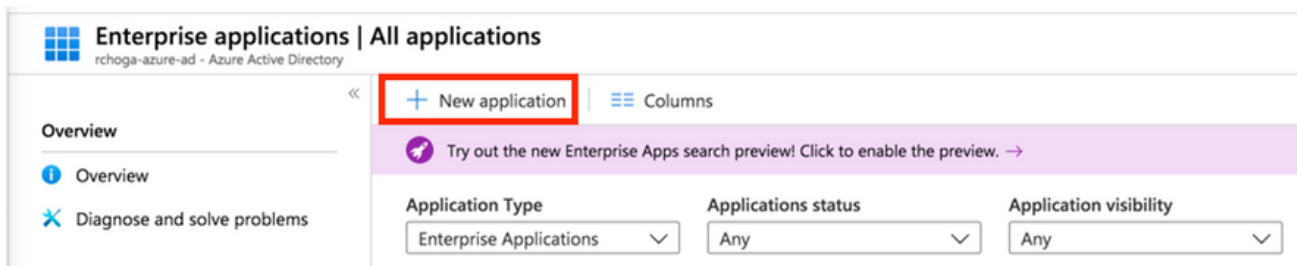
Navigate



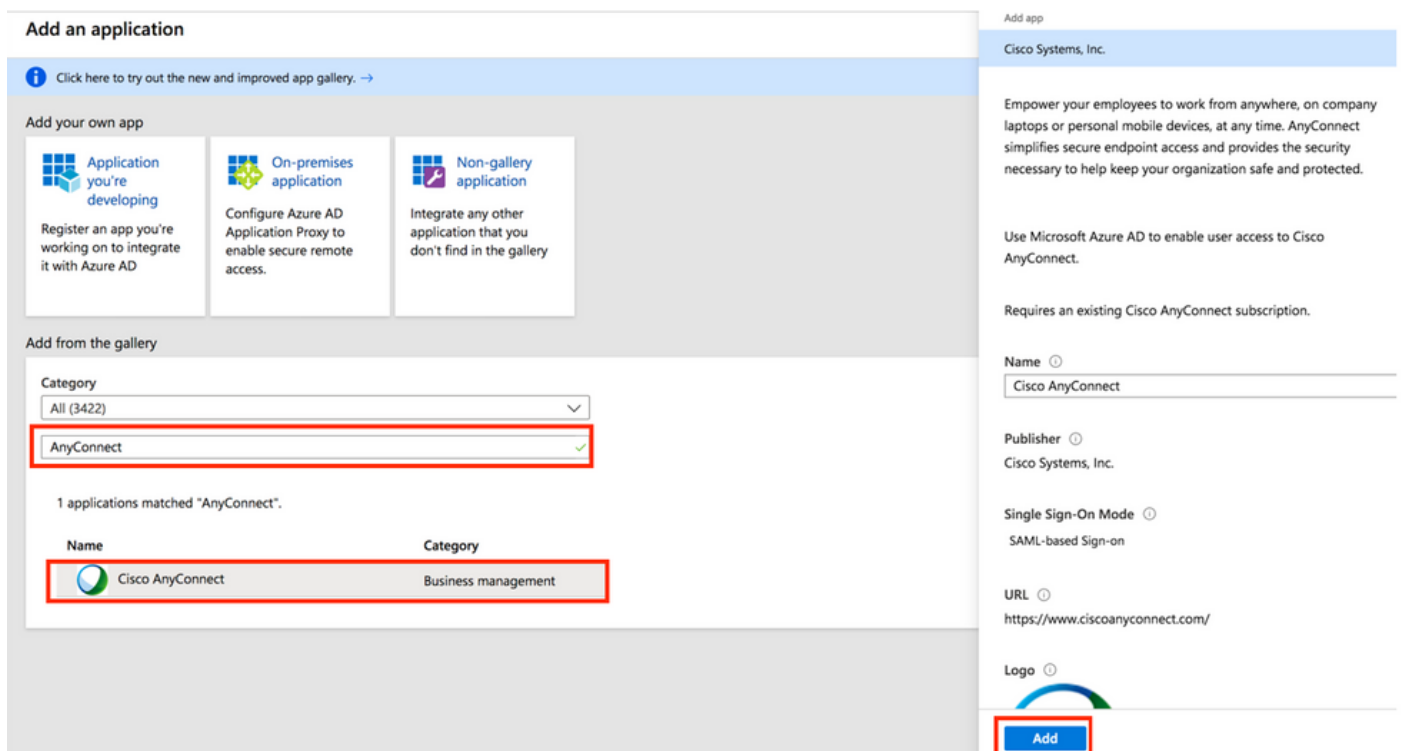
ステップ2: 次の図に示すように、Enterprise Applicationsを選択します。



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。



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



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。

手順 6 : 図に示すように、SAMLを選択します。

手順 7 : これらの詳細を使用してセクション1を編集します。

<#root>

a. Identifier (Entity ID) - `https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME>`


b. Reply URL (Assertion Consumer Service URL) - `https://<VPN URL>/+CSCO+/saml/sp/acs?tgname=<TUNNEL-G`

Example: vpn url called

`asa.example.com`


and tunnel-group called


`AnyConnectVPN-1`

Basic SAML Configuration 

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

ステップ 8 : SAML Signing Certificateセクションで、Downloadを選択して証明書ファイルをダウンロードし、コンピュータに保存します。

SAML Signing Certificate 




Status	Active
Thumbprint	-----
Expiration	5/1/2023, 4:04:04 PM
Notification Email	
App Federation Metadata Url	<input type="text" value="https://"/> 
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

ステップ 9 : これはASA設定に必要です。

- Azure AD Identifier – これはVPN構成のsaml idpです。
- Login URL (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 AnyConnectVPN

You'll need to configure the application to link with Azure AD.

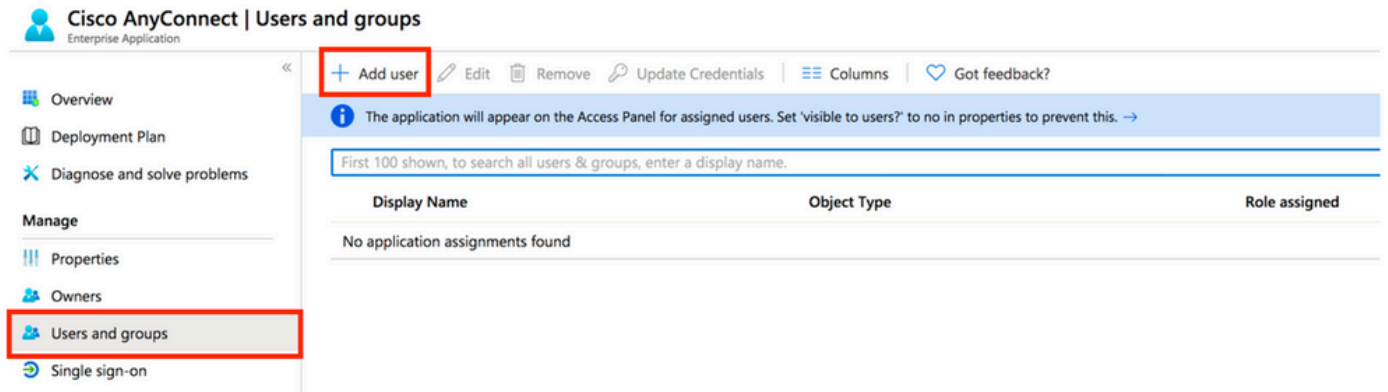
Login URL	<input type="text" value="https://"/> 
Azure AD Identifier	<input type="text" value="https://"/> 
Logout URL	<input type="text" value="https://"/> 

[View step-by-step instructions](#)

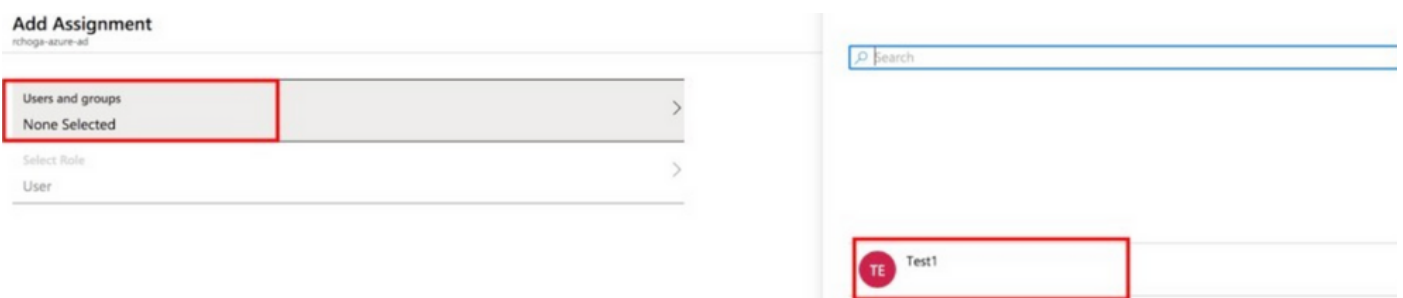
Azure ADユーザーのアプリへの割り当て

このセクションでは、Cisco AnyConnectアプリへのアクセス権を付与する際に、Test1でAzureシングルサインオンの使用が有効になります。

ステップ 1 : アプリの概要ページで、Users and groups、Add userの順に選択します。



ステップ 2 : Add AssignmentダイアログでUsers and groupsを選択します。



ステップ 3 : Add Assignmentダイアログで、Assignボタンをクリックします。



CLIによるSAML用の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。

```
config t
```

```
crypto ca trustpoint AzureAD-AC-SAML
  revocation-check none
  no id-usage
```



```
enrollment terminal
no ca-check
crypto ca authenticate AzureAD-AC-SAML
-----BEGIN CERTIFICATE-----
...
PEM Certificate Text you downloaded goes here
...
-----END CERTIFICATE-----
quit
```

ステップ 2：これらのコマンドは、SAML IdPをプロビジョニングします。


webvpn

```
saml idp https://xxx.windows.net/xxxxxxxxxxxxx/ - [Azure AD Identifier]
url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
url sign-out https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 - Logout URL
trustpoint idp AzureAD-AC-SAML - [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：VPNトンネル設定へのSAML認証の適用

```
tunnel-group AnyConnectVPN-1 webvpn-attributes
  saml identity-provider https://xxx.windows.net/xxxxxxxxxxxxx/
  authentication saml
end

write memory
```

 注:IdP設定を変更した場合、トンネルグループからsaml identity-provider設定を削除し、変更を有効にするために再適用する必要があります。

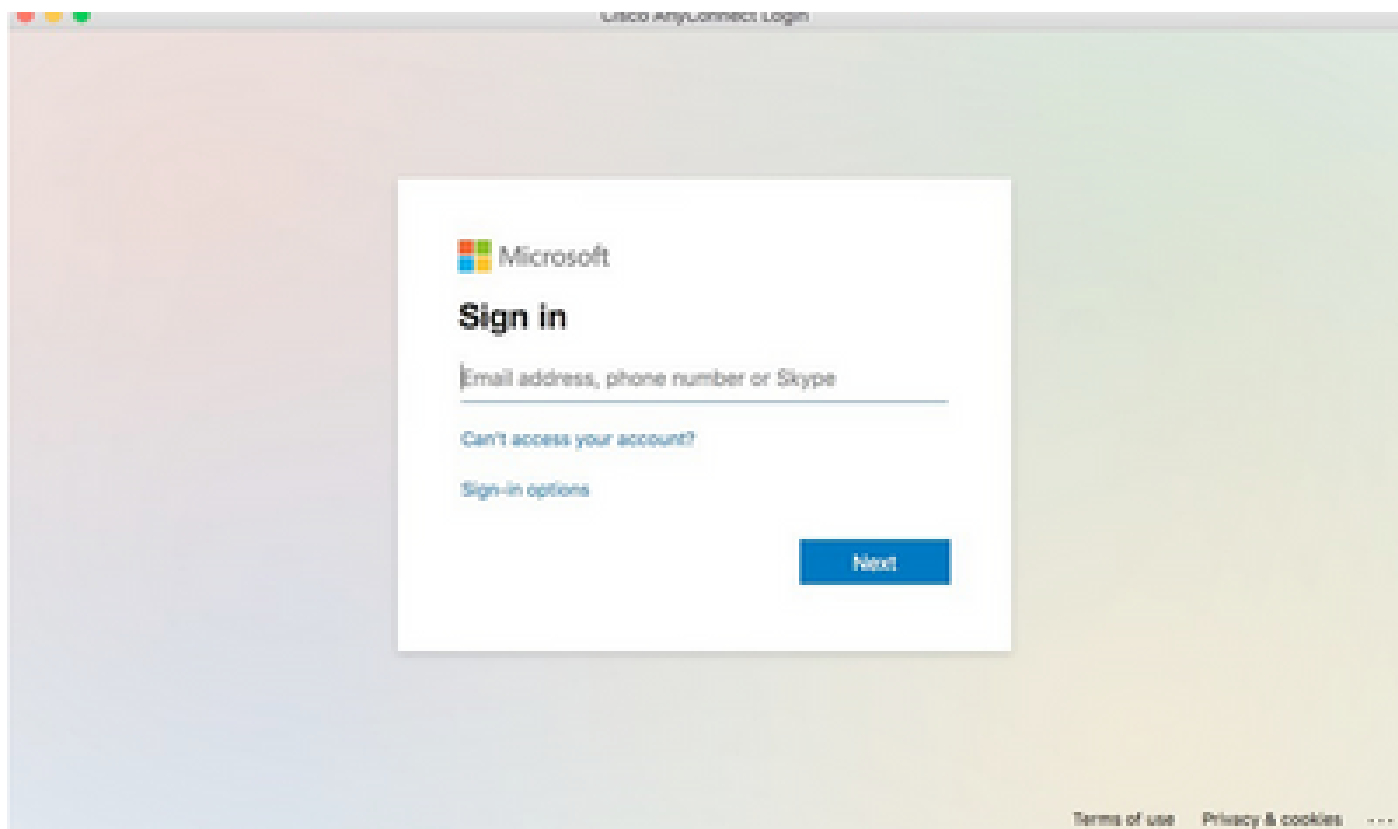
確認

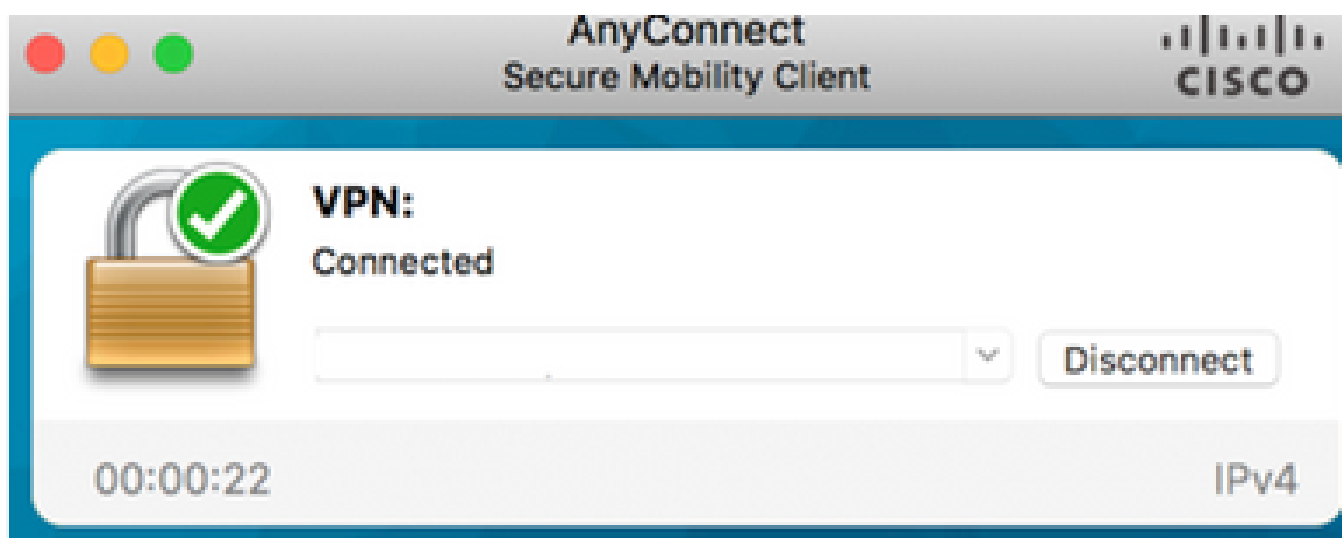
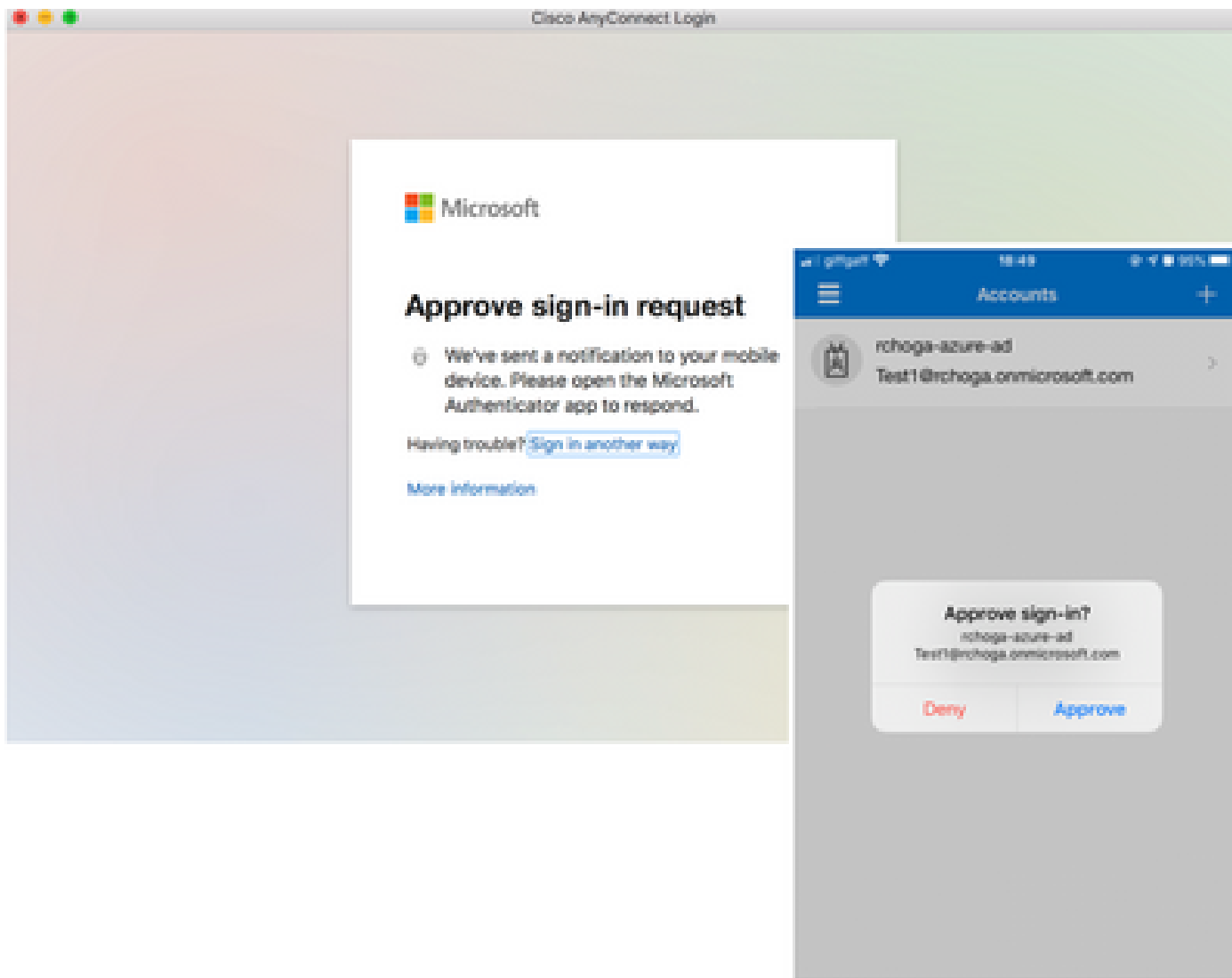
SAML認証を使用したAnyConnectのテスト

ステップ 1：VPN URLに接続し、Azure ADの詳細にログを入力します。

ステップ 2：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。





一般的な問題

エンティティIDの不一致

デバッグ例：

[SAML] consume_assertion : プロバイダーの識別子が不明#LassoServerです。#LassoServerオブジェクトにプロバイダを登録するには、lasso_server_add_provider()またはlasso_server_add_provider_from_buffer()メソッドを使用する必要があります。

問題：通常、ASAのwebvpn設定でのsaml idp [entityID]コマンドが、IdPのメタデータで見つかったIdPエンティティIDと一致しないことを意味しています。

解決策：IdPのメタデータファイルのエンティティIDを確認し、これに一致するようにsaml idp [entity id]コマンドを変更します。

時間の不一致

デバッグ例：

[SAML] NotBefore:2017-09-05T23:59:01.896Z NotOnOrAfter:2017-09-06T00:59:01.896Zタイムアウト：0

[SAML] consume_assertion : アサーションが期限切れか、有効ではありません

問題 1. ASA時間がIdPの時間と同期されていません。

解決策 1.IdPで使用されるのと同じNTPサーバを使用してASAを設定します。

問題 2. 指定された時間の間はアサーションが無効です。

解決策 2. ASAで設定されているタイムアウト値を変更します。

誤ったIdP署名証明書の使用

デバッグ例：

[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=signatures.c:line=493:obj=rsa-sha1:subj=EVP_VerifyFinal:error=18:data do not match:signature do not match (データが一致しない)

[SAML] consume_assertion : プロファイルはメッセージの署名を確認できません

問題：ASAがIdPによって署名されたメッセージを確認できないか、確認するASAの署名がありません。

解決策:ASAにインストールされているIdP署名証明書を調べて、IdPによって送信される証明書と一致することを確認します。これが確認されたら、シグニチャがSAML応答に含まれていることを確認します。

無効なアサーションオーディエンス

デバッグ例：

[SAML] consume_assertion : アサーションオーディエンスが無効です

問題：IdPは正しくない対象ユーザを定義しています。

解決方法：IdPの対象ユーザー構成を修正します。ASAのエンティティIDと一致している必要があります。

アサーションコンシューマサービスのURLが正しくありません

デバッグの例：初期認証要求の送信後にデバッグを受信できない。ユーザはIdPでクレデンシャルを入力できますが、IdPはASAにリダイレクトしません。

問題：IdPが間違ったアサーションコンシューマサービスURLに対して設定されています。

解決方法：構成のベースURLを確認し、正しいことを確認してください。showを使用してASAメタデータをチェックし、Assertion Consumer Service URLが正しいことを確認します。これをテストするには、参照します。ASAで両方とも正しい場合は、IdPをチェックしてURLが正しいことを確認します。

SAML設定の変更が有効にならない

例：シングルサインオンURLが変更または変更された後も、SP証明書、SAMLはまだ機能せず、以前の設定が送信されます。

問題：ASAに影響する設定変更があった場合、ASAはメタデータを再生成する必要があります。これは自動的に実行されません。

解決策：変更が行われた後、影響を受けるtunnel-groupでsaml idp [entity-id]コマンドを削除し、再適用します。

トラブルシューティング

ほとんどのSAMLトラブルシューティングには、SAML構成のチェック時またはデバッグ実行時に見つかる可能性のある構成の誤りが含まれています。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、このデバッグで役に立つ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

- [アプリケーションプロキシを使用したオンプレミスアプリケーション用のSAMLシングルサインオン](#)

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。