

ASA AnyConnect VPN met Microsoft Azure MFA configureren via SAML

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[SAML-componenten](#)

[Certificaten voor ondertekenings- en versleutelingsbewerkingen](#)

[Netwerkdigram](#)

[Configureren](#)

[Cisco AnyConnect toevoegen vanuit de galerie met apps van Microsoft](#)

[Azure AD-gebruiker toewijzen aan de app](#)

[ASA voor SAML configureren via CLI](#)

[Verifiëren](#)

[AnyConnect testen met SAML-verificatie](#)

[Veelvoorkomende problemen](#)

[Niet-overeenkomende entiteits-id](#)

[Niet-overeenkomende tijd](#)

[Onjuist handtekeningcertificaat voor IdP gebruikt](#)

[Ongeldige doelgroep voor bewerking](#)

[Onjuiste URL voor Assertion Consumer Service](#)

[Wijzigingen in de SAML-configuratie die niet van kracht worden](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u Security Assertion Markup Language (SAML) configureert op een ASA (adaptieve security applicatie) met AnyConnect via Microsoft Azure MFA.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van RA VPN-configuratie op ASA.
- Basiskennis van SAML en Microsoft Azure.

- AnyConnect-licenties ingeschakeld (APEX of VPN Only).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Een Microsoft Azure AD-abonnement.
- Cisco ASA 9.7+ en AnyConnect 4.6+
- Een werkend AnyConnect VPN-profiel

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 is een op XML gebaseerd framework voor het uitwisselen van verificatie- en autorisatiegegevens tussen security domeinen. Op deze manier wordt een vertrouwenscirkel tussen de gebruiker, een serviceprovider (SP) en een identiteitsprovider (IdP) tot stand gebracht, zodat de gebruiker zich in één keer voor meerdere services kan aanmelden. Microsoft Azure MFA kan naadloos worden geïntegreerd met de Cisco ASA VPN-applicatie om extra security te bieden voor de aanmeldingen bij Cisco AnyConnect VPN.

SAML-componenten

Metagegevens: het is een op XML gebaseerd document dat een veilige transactie tussen een IdP en een SP waarborgt. Hiermee kunnen de IdP en SP over overeenkomsten onderhandelen.

Ondersteunde rollen door de apparaten (IdP, SP)

Een apparaat kan meer dan één rol ondersteunen en kan waarden bevatten voor zowel een SP als een IdP. Onder het veld EntityDescriptor bevindt zich een IDPSSODescriptor als de opgenomen informatie betrekking heeft op een IdP voor eenmalige aanmelding of een SPSSODescriptor als de opgenomen informatie betrekking heeft op een SP voor eenmalige aanmelding. Dit is belangrijk omdat de juiste waarden uit de juiste secties moeten worden gehaald om SAML in te stellen.

Entiteits-ID: Dit veld is een unieke id voor een SP of een IdP. Eén apparaat kan meerdere diensten hebben en verschillende ID's van entiteiten gebruiken om ze te onderscheiden. Een ASA heeft bijvoorbeeld verschillende entiteits-id's voor verschillende tunnelgroepen die moeten worden geverifieerd. Een IdP die elke tunnelgroep authenticert, heeft een aparte entiteit-ID-vermeldingen voor elke tunnelgroep om deze diensten nauwkeurig te identificeren.

Een ASA kan meerdere IdP's ondersteunen en heeft een aparte entiteits-id voor elke IdP om onderscheid te kunnen maken tussen deze IdP's. Als een van beide partijen een bericht ontvangt van een apparaat dat geen entiteits-id bevat die eerder is geconfigureerd, wordt dit bericht waarschijnlijk verwijderd en mislukt de SAML-verificatie. De entiteits-id vindt u in het veld EntityDescriptor naast entityID.

Service-URL's: deze definiëren de URL naar een SAML-service die is geleverd door de SP of IdP.

Voor IdP's zijn dit meestal de SLO-service (eenmalige afmelding) en de SSO-service (eenmalige aanmelding). Voor SP's zijn dit meestal Assertion Consumer Service en de SLO-service.

De URL van de SSO-service in de IdP-metagegevens wordt gebruikt door de SP om de gebruiker om te leiden naar de IdP voor verificatie. Als deze waarde onjuist wordt geconfigureerd, kan de IdP de verificatieaanvraag die is verzonden door de SP niet ontvangen of niet goed verwerken.

De URL van Assertion Consumer Service in de SP-metagegevens wordt gebruikt door de IdP om de gebruiker weer terug te leiden naar de SP en informatie te geven over de verificatiepoging van de gebruiker. Als deze URL onjuist is geconfigureerd, ontvangt de SP de bewering (het antwoord) niet of kan deze bewering niet worden verwerkt.

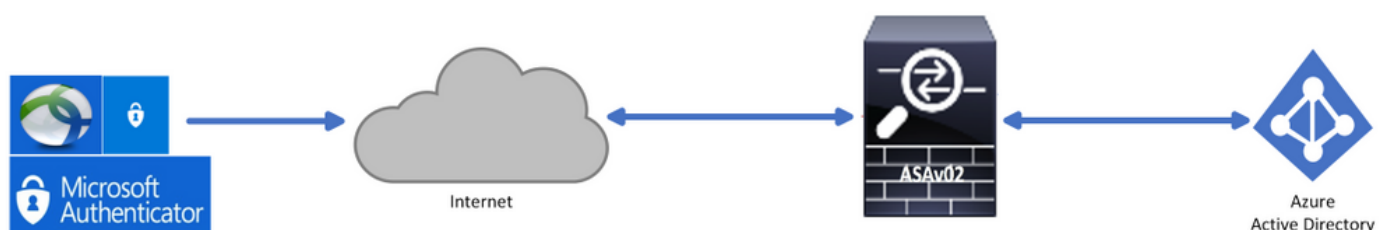
De URL van de SLO-service (eenmalige afmelding) kan zowel op de SP als op de IdP worden gevonden. Deze service wordt gebruikt om het afmelden bij alle SSO-services (eenmalige aanmelding) vanaf de SP te vereenvoudigen en is optioneel op de ASA. Als de URL van de SLO-service uit de IdP-metagegevens is geconfigureerd op de SP, wordt de aanvraag naar de IdP verzonden als de gebruiker zich op de SP afmeldt bij de service. Zodra de IdP met succes de gebruiker uit de diensten heeft gelogd, leidt het de gebruiker terug naar de SP en gebruikt de DSL-dienst die binnen de metagegevens van de SP wordt gevonden.

SAML-bindingen voor service-URL's: bindingen worden door de SP gebruikt om gegevens voor services uit te wisselen met de IdP. Hierbij gaat het onder andere om HTTP Redirect, HTTP POST en Artifact. Elke methode heeft een andere manier om gegevens over te dragen. De ondersteunde bindingmethode door de service is opgenomen in de definitie van die service. Voorbeeld: SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="<https://saml.example.com/simplesaml/saml2/idp/SSOService.php/>" >. De ASA biedt geen ondersteuning voor de binding Artifact. De ASA gebruikt altijd de methode HTTP Redirect voor SAML-verificatieaanvragen, dus het is belangrijk om de URL van de SSO-service te kiezen die de binding HTTP Redirect gebruikt, zodat de IdP dit verwacht.

Certificaten voor ondertekenings- en versleutelingsbewerkingen

Om de vertrouwelijkheid en integriteit van de verzonden berichten tussen de SP en de IdP te waarborgen, omvat SAML de mogelijkheid om de data te versleutelen en te ondertekenen. Het certificaat dat wordt gebruikt om de gegevens te versleutelen en/of te ondertekenen kan worden opgenomen in de metagegevens, zodat het ontvangen einde het SAML-bericht kan verifiëren en ervoor kan zorgen dat het van de verwachte bron komt. De gebruikte certificaten voor ondertekening en versleuteling vindt u in de metagegevens onder respectievelijk KeyDescriptor use="signing" en KeyDescriptor use="encryption". De ASA biedt geen ondersteuning voor de versleuteling van SAML-berichten.

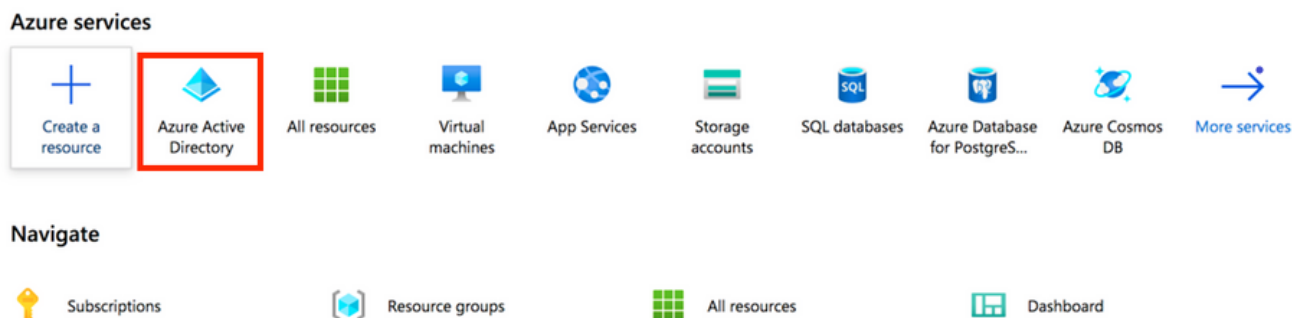
Netwerkdigram



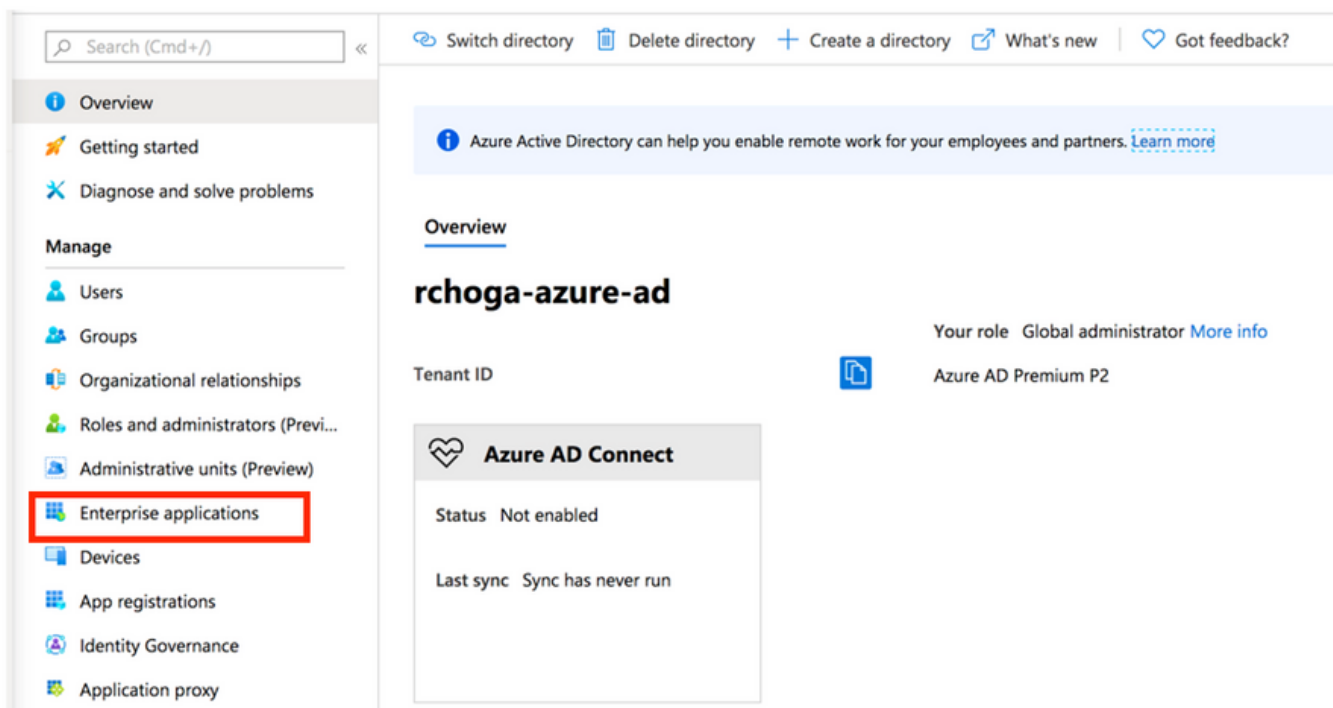
Configureren

Cisco AnyConnect toevoegen vanuit de galerie met apps van Microsoft

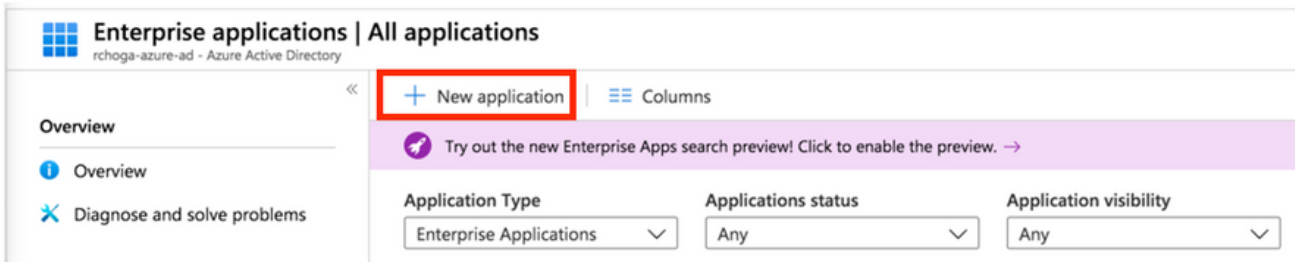
Stap 1. Meld u aan bij Azure Portal en selecteer Azure Active Directory.



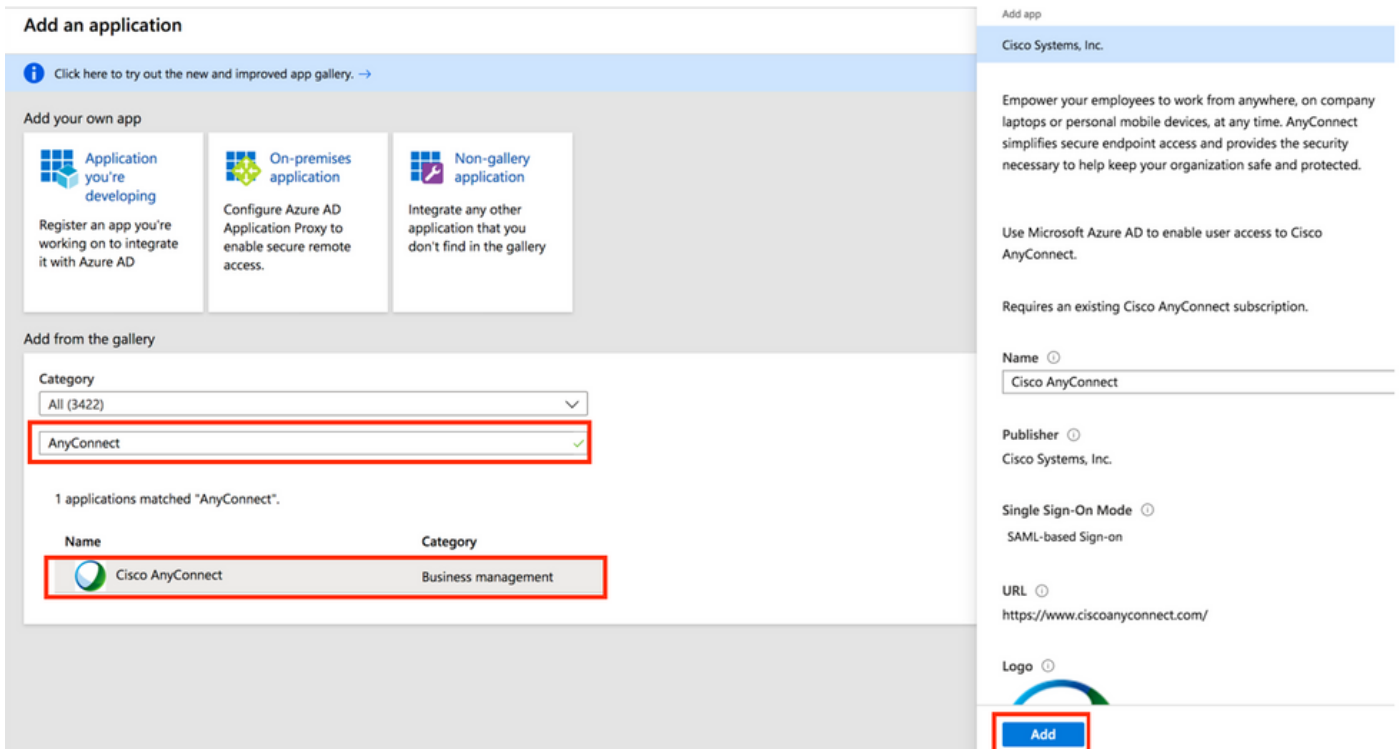
Stap 2. Selecteer **Bedrijfstoeepassingen**, zoals weergegeven in deze afbeelding.



Stap 3. Selecteer nu **Nieuwe toepassing**, zoals weergegeven in deze afbeelding.



Stap 4. In de sectie **Toevoegen uit de galerie** typt u **AnyConnect** in het zoekvak. Selecteer vervolgens **Cisco AnyConnect** in het deelvenster met resultaten en **voeg** de app toe.



Stap 5. Selecteer het menu-item **Single Sign-on** (Eenmalige aanmelding), zoals weergegeven in deze afbeelding.

AnyConnectVPN | Overview
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service

Security

Conditional Access
Permissions
Token encryption

Activity

Sign-ins
Usage & insights (Preview)

Properties

Name: AnyConnectVPN
Application ID
Object ID

Getting Started

- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
[Get started](#)
- 3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)
- 4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)
- 5. Self service**
Enable users to request access to the application using their Azure AD credentials
[Get started](#)

Stap 6. Selecteer **SAML**, zoals weergegeven in de afbeelding.

Cisco AnyConnect | Single sign-on
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Users and groups
Single sign-on

Select a single sign-on method [Help me decide](#)

- Disabled**
User must manually enter their username and password.
- SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
- Linked**
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

Stap 7. Bewerk **Sectie 1** met deze details.

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


b. Reply URL (Assertion Consumer Service URL) - `https://<VPN URL>/+CSCOE+/saml/sp/acs?tname=<TUNNEL-GROUP NAME>`

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>

Stap 8. Selecteer **Downloaden** in de sectie **SAML-handtekeningcertificaat** om het certificaatbestand te downloaden en op te slaan op uw computer.


SAML Signing Certificate 

Status: Active

Thumbprint: -----

Expiration: 5/1/2023, 4:04:04 PM

Notification Email: -----

App Federation Metadata Url: 

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)


Federation Metadata XML [Download](#)


Step 9. U heeft de volgende gegevens nodig voor de ASA-configuratie.


- Azure AD-id: dit is de SAML-id in onze VPN-configuratie.
- Aanmeldings-URL: dit is de URL voor aanmelden.
- Afmeldings-URL: dit is de URL voor afmelden.

Set up AnyConnectVPN

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

Login URL 

Azure AD Identifier 

Logout URL 






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


Azure AD-gebruiker toewijzen aan de app

In deze sectie wordt **Test1** ingeschakeld om eenmalige aanmelding van Azure te gebruiken wanneer u toegang tot de Cisco AnyConnect-app verleent.

Step 1. Op de overzichtspagina van de app selecteert u **Users and groups** (Gebruikers en groepen) en vervolgens **Add user** (Gebruiker toevoegen).

Cisco AnyConnect | Users and groups
Enterprise Application

[+ Add user](#)     

 The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
No application assignments found		

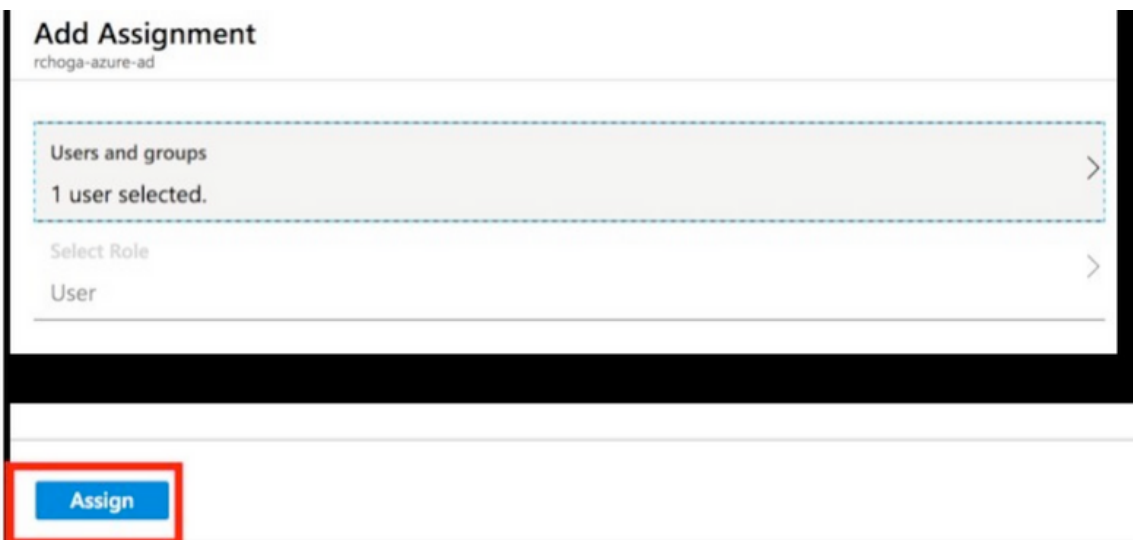
Navigation menu:

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

Step 2. Selecteer **Users and groups** (Gebruikers en groepen) in het dialoogvenster Add Assignment (Toewijzing toevoegen).



Stap 3. Klik in het dialoogvenster **Add Assignment** (Toewijzing toevoegen) op de knop **Assign** (Toewijzen).



ASA voor SAML configureren via CLI

Stap 1. Maak een vertrouwenspunt en importeer ons SAML-certificaat.

```
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
```

Stap 2. Met deze opdrachten richt u uw SAML-IdP in.

```
webvpn

saml idp https://sts.windows.net/xxxxxxxxxxxxx/ - [Azure AD Identifier]
url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxxxx/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
```

Stap 3. SAML-verificatie toepassen op een VPN-tunnelconfiguratie.

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


end

write memory

Opmerking: Als u wijzigingen wilt aanbrengen in de IdP-configuratie, moet u de configuratie van de SAML-identiteitsprovider uit uw tunnelgroep verwijderen en opnieuw toepassen om de wijzigingen van kracht te laten worden.

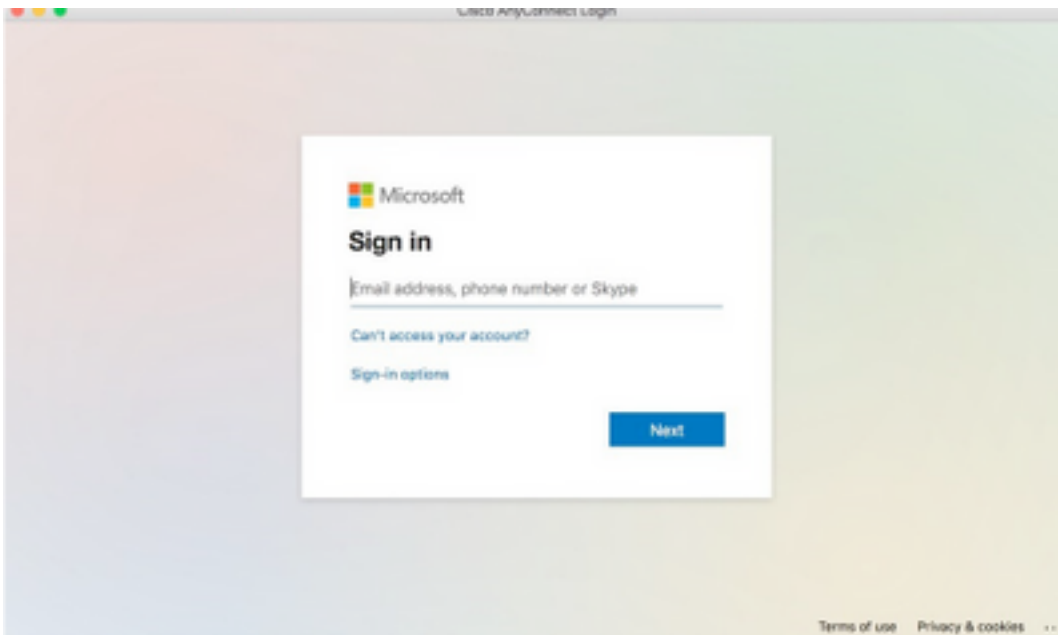
Verifiëren

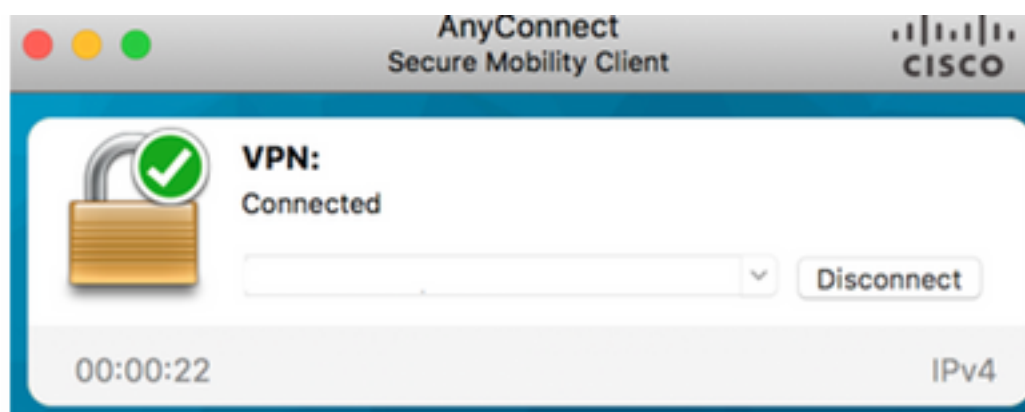
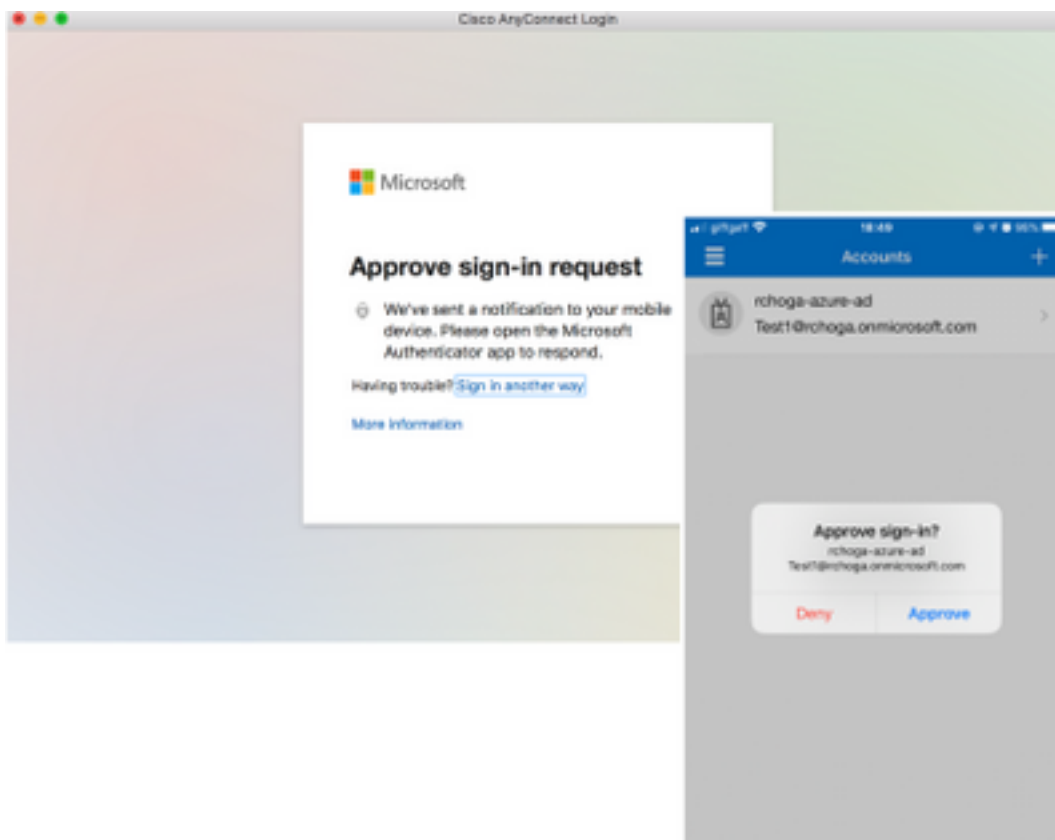
AnyConnect testen met SAML-verificatie

Stap 1. Maak verbinding met uw VPN-URL en voer uw aanmeldingsgegevens voor Azure AD in.

Stap 2. Keur de aanmeldingsaanvraag goed.

Stap 3. AnyConnect is verbonden.





Veelvoorkomende problemen

Niet-overeenkomende entiteits-id

Voorbeeld van debug:

[SAML] consume_assertion: De identificatie van een provider is onbekend voor #LassoServer. Als u een provider in een #LassoServer-object wilt registreren, moet u de methode `lasso_server_add_provider()` of `lasso_server_add_provider_from_buffer()` gebruiken.

Probleem: In het algemeen betekent dit dat de opdracht **idp [entityID]** onder de webvpn-configuratie van de ASA niet overeenkomt met de IDp-entiteit-id in de metadata van IdP.

Oplossing: Controleer de entiteits-id van het metagegevensbestand van de IdP en pas de opdracht **saml idp [entity id]** hieraan aan.

Niet-overeenkomende tijd

Voorbeeld van debug:

```
[SAML] NotBefore:2017-09-05T23:59:01.896Z NotOnOrAfter:2017-09-06T00:59:01.896Z timeout: 0
```

```
[SAML] consume_assertion: bewering is verlopen of ongeldig
```

Probleem 1. ASA-tijd is niet gesynchroniseerd met tijd van IdP.

Oplossing 1. Configureer de ASA met de NTP-server die wordt gebruikt door IdP.

Probleem 2. De bewering is niet geldig in de opgegeven periode.

Oplossing 2. Wijzig de geconfigureerde time-outwaarde op de ASA.

Onjuist handtekeningcertificaat voor IdP gebruikt

Voorbeeld van debug:

```
[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=signatures.c:line=493:obj=rsa-sha1:subj=EVP_VerifyFinal:error=18:data do not match:signature do not match
```

```
[SAML] consume_assertion: het profiel kan een handtekening voor het bericht niet verifiëren
```

Probleem: De ASA kan het bericht ondertekend door de IdP niet verifiëren of er is geen handtekening om te verifiëren voor de ASA.

Oplossing: Controleer het IdP-handtekeningcertificaat dat op de ASA is geïnstalleerd om er zeker van te zijn dat dit overeenkomt met wat door de IdP is verzonden. Na bevestiging controleert u of de handtekening is opgenomen in de SAML-respons.

Ongeldige doelgroep voor bewering

Voorbeeld van debug:

```
[SAML] consume_assertion: doelgroep van bewering is ongeldig
```

Probleem: IdP definieert het onjuiste publiek.

Oplossing: Corrigeer de doelgroepconfiguratie op de IdP. Het moet overeenkomen met de entiteit-ID van de ASA.

Onjuiste URL voor Assertion Consumer Service

Voorbeeld van debug: Kan geen debug-opdrachten ontvangen nadat de initiële verificatieaanvraag is verzonden. De gebruiker kan gebruikersreferenties invoeren op de IdP, maar de IdP leidt niet om naar de ASA.

Probleem: IdP is niet voor de juiste Assertion Consumer Service-URL geconfigureerd.

Oplossing(en): Controleer de basis-URL in de configuratie en zorg dat deze correct is. Controleer de ASA-metagegevens met de opdracht show om er zeker van te zijn dat de URL voor Assertion Consumer Service correct is. Test de URL door deze te bezoeken en uit te proberen. Als beide URL's correct zijn op de ASA, controleert u de IdP om er zeker van te zijn dat de URL klopt.

Wijzigingen in de SAML-configuratie die niet van kracht worden

Voorbeeld: Nadat een URL voor eenmalige aanmelding is gewijzigd, werkt de SAML van het SP-certificaat nog steeds niet en worden eerdere configuraties verzonden.

Probleem: ASA moet zijn metagegevens regenereren wanneer er een configuratieverandering is die het beïnvloedt. Dit gebeurt niet automatisch.

Oplossing: Nadat wijzigingen zijn aangebracht, onder de betreffende tunnelgroep het kleine idp [entity-id]-commando verwijderen en opnieuw toepassen.

Problemen oplossen

De meeste SAML-fouten hebben betrekking op onjuiste configuraties die kunnen worden gevonden als de SAML-configuratie wordt gecontroleerd of als er debug-opdrachten worden uitgevoerd. De opdracht debug webvpn saml 255 biedt in de meeste gevallen uitkomst, maar in scenario's waarin deze debug-opdracht geen nuttige informatie oplevert, kunnen aanvullende debug-opdrachten worden uitgevoerd:

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

Gerelateerde informatie

- [Enmalige aanmelding op basis van SAML voor on-premises toepassingen via toepassingsproxy](#)