

Konfigurieren von ASA AnyConnect-VPN mit Microsoft Azure MFA über SAML

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[SAML-Komponenten](#)

[Zertifikate für Signatur- und Verschlüsselungsvorgänge](#)

[Netzwerkdiagramm](#)

[Konfigurieren](#)

[Hinzufügen von Cisco AnyConnect aus der Microsoft App-Galerie](#)

[Zuweisen von Azure AD-Benutzern zur App](#)

[Konfigurieren der ASA für SAML über die CLI](#)

[Überprüfung](#)

[Testen von AnyConnect mit SAML-Authentifizierung](#)

[Häufige Probleme](#)

[Entitäts-ID stimmt nicht überein](#)

[Zeit stimmt nicht überein](#)

[Falsches IdP-Signaturzertifikat verwendet](#)

[Ungültige Assertion-Zielgruppe](#)

[Falsche URL für Assertion Consumer Service](#)

[SAML-Konfigurationsänderungen, die nicht wirksam werden](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration der Security Assertion Markup Language (SAML). Der Schwerpunkt liegt auf Adaptive Security Appliance (ASA) AnyConnect über Microsoft Azure MFA.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegende Kenntnisse der RA-VPN-Konfiguration auf der ASA
- Grundkenntnisse in SAML und Microsoft Azure

- Aktivieren von AnyConnect-Lizenzen (APEX oder VPN-Only)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Ein Microsoft Azure AD-Abonnement
- Cisco ASA 9.7+ und AnyConnect 4.6+
- Funktionierendes AnyConnect-VPN-Profil

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

SAML ist ein XML-basiertes Framework für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen. Es schafft einen Vertrauenskreis zwischen dem Benutzer, einem Service-Provider (SP) und einem Identitätsanbieter (IdP), mit dem sich Benutzer für mehrere Services nur einmal anmelden müssen. Microsoft Azure MFA lässt sich nahtlos in die Cisco ASA VPN-Appliance integrieren, um zusätzliche Sicherheit für die Cisco AnyConnect-VPN-Anmeldungen zu bieten.

SAML-Komponenten

Metadaten: Es handelt sich um ein XML-basiertes Dokument, das eine sichere Transaktion zwischen einem IdP und einem SP gewährleistet und es ihnen ermöglicht, Vereinbarungen auszuhandeln.

Von den Geräten unterstützte Rollen (IdP, SP)

Ein Gerät kann mehrere Rollen unterstützen und Werte für einen SP und einen IdP enthalten. Unter dem Feld „EntityDescriptor“ befindet sich ein IDPSSODescriptor, wenn die enthaltenen Informationen für einen Single Sign-On-IdP sind, oder ein SPSSODescriptor für einen Single Sign-On-SP sind. Dies ist wichtig, da die richtigen Werte aus den entsprechenden Abschnitten entnommen werden müssen, um SAML erfolgreich einzurichten.

Entitäts-ID: Dieses Feld ist eine eindeutige Kennung für einen SP oder einen IdP. Ein einzelnes Gerät kann mehrere Services umfassen und unterschiedliche Objektkennungen verwenden, um diese zu differenzieren. Die ASA hat beispielsweise verschiedene Entitäts-IDs für verschiedene Tunnelgruppen, die authentifiziert werden müssen. Ein IdP, der jede Tunnelgruppe authentifiziert, verfügt für jede Tunnelgruppe über separate Entity-ID-Einträge, um diese Services genau zu identifizieren.

Die ASA kann mehrere IdPs unterstützen und hat eine separate Entitäts-ID für jeden IdP, um sie zu unterscheiden. Wenn eine Seite eine Meldung von einem Gerät empfängt, das keine zuvor konfigurierte Entitäts-ID enthält, verwirft das Gerät diese Meldung wahrscheinlich und die SAML-Authentifizierung schlägt fehl. Die Entitäts-ID befindet sich im Feld „EntityDescriptor“ neben „entityID“.

Service-URLs: Diese definieren die URL eines vom SP oder IdP bereitgestellten SAML-Dienstes. Bei IdPs sind dies meist der Single Logout- und der Single Sign-On-Dienst. Bei SPs sind es normalerweise der Assertion Consumer Service und der Single Logout-Dienst.

Die Single Sign-On Service-URL in den IdP-Metadaten wird vom SP verwendet, um den Benutzer zur Authentifizierung an den IdP weiterzuleiten. Wenn dieser Wert falsch konfiguriert ist, empfängt der IdP die vom SP gesendete Authentifizierungsanfrage nicht oder kann sie nicht erfolgreich verarbeiten.

Die Assertion Consumer Service-URL in den SP-Metadaten wird vom IdP verwendet, um den Benutzer zurück zum SP zu leiten und Informationen über den Authentifizierungsversuch des Benutzers bereitzustellen. Wenn dies falsch konfiguriert ist, erhält der SP die Zusicherung (die Antwort) nicht oder kann sie nicht erfolgreich verarbeiten.

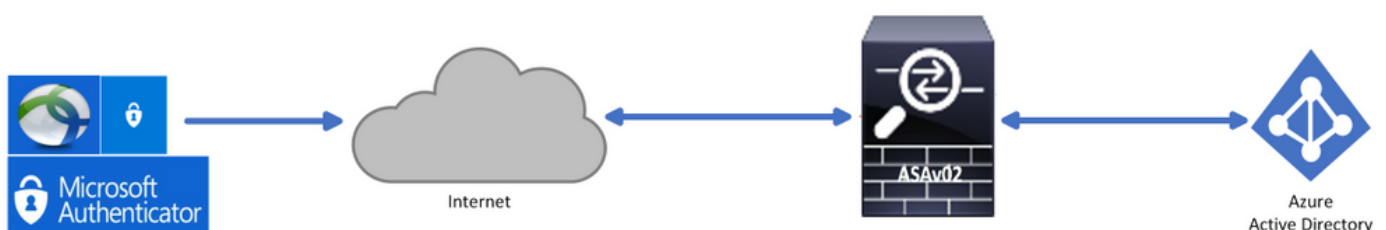
Die Single Logout Service-URL befindet sich sowohl auf dem SP als auch auf dem IdP. Sie wird verwendet, um das Abmelden von allen SSO-Services vom SP zu erleichtern, und ist auf der ASA optional. Wenn die SLO-Service-URL aus den IdP-Metadaten auf dem SP konfiguriert ist und sich der Benutzer beim Service auf dem SP abmeldet, sendet der SP die Anfrage an den IdP. Sobald der Benutzer vom IdP erfolgreich bei den Services abgemeldet wurde, leitet er den Benutzer zurück zum SP und verwendet die SLO-Dienst-URL, die in den Metadaten des SP enthalten ist.

SAML-Bindungen für Service-URLs: Bindungen sind die Methode, mit der der SP Informationen vom und an den IdP für Services überträgt. Dazu gehören HTTP-Umleitung, HTTP-POST und Artefakt. Jede Methode hat eine andere Möglichkeit, Daten zu übertragen. Die vom Dienst unterstützte Bindungsmethode ist in der Definition dieser Dienste enthalten. Beispiele: SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="<https://saml.example.com/simplesaml/saml2/idp/SSOService.php/>" >. Die ASA unterstützt die Artefaktbindung nicht, sondern verwendet immer die HTTP-Umleitungsmethode für SAML-Authentifizierungsanforderungen. Daher ist es wichtig, die SSO-Service-URL auszuwählen, die die HTTP-Umleitungsbindung verwendet, damit der IdP dies erwartet.

Zertifikate für Signatur- und Verschlüsselungsvorgänge

Um die Vertraulichkeit und Integrität der zwischen SP und IdP gesendeten Meldungen zu gewährleisten, beinhaltet SAML die Möglichkeit, die Daten zu verschlüsseln und zu signieren. Das zur Verschlüsselung und/oder Signierung der Daten verwendete Zertifikat kann in die Metadaten aufgenommen werden, sodass das empfangende Ende die SAML-Nachricht überprüfen und sicherstellen kann, dass sie von der erwarteten Quelle stammt. Die für die Signierung und Verschlüsselung verwendeten Zertifikate finden Sie in den Metadaten unter „KeyDescriptor use="signing"“ bzw. „KeyDescriptor use="encryption"“ > „X509Certificate“. Die ASA unterstützt keine Verschlüsselung von SAML-Meldungen.

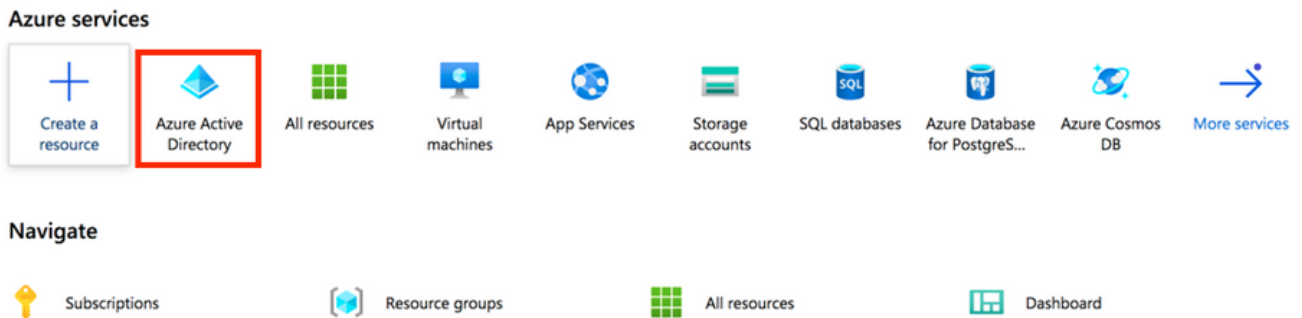
Netzwerkdiagramm



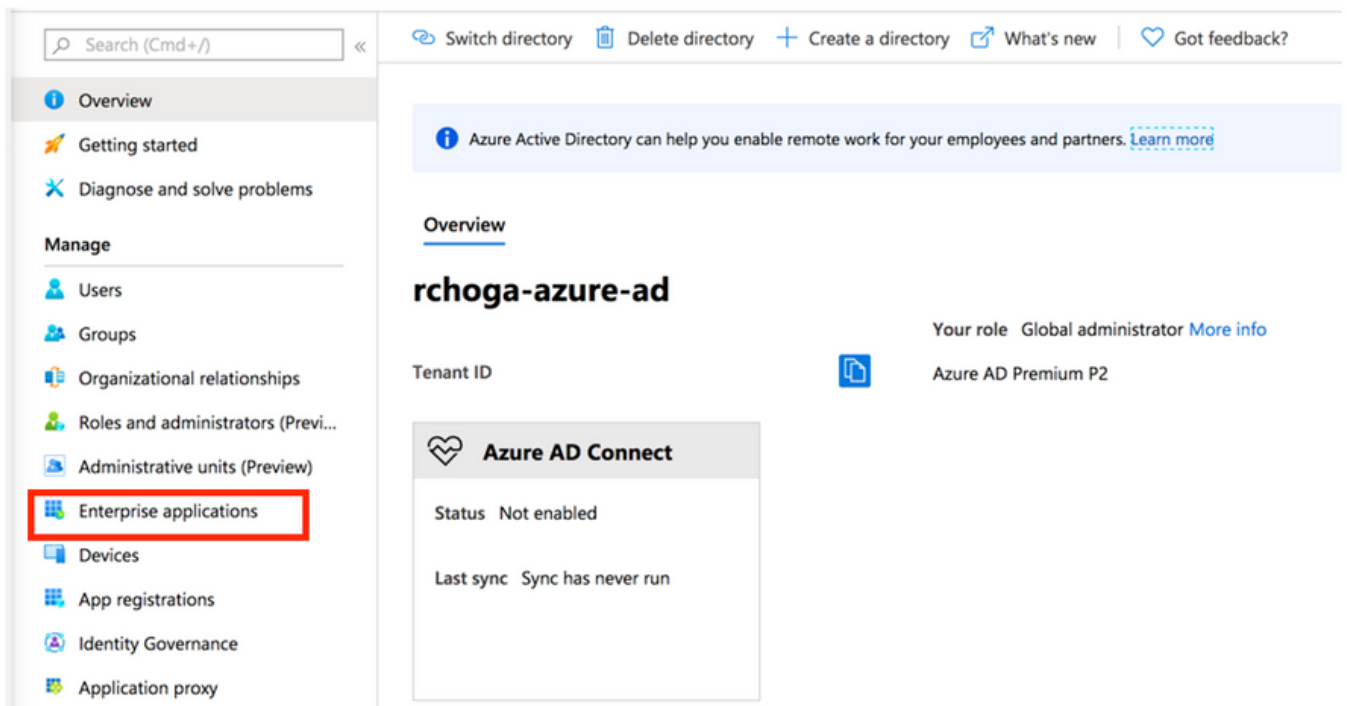
Konfigurieren

Hinzufügen von Cisco AnyConnect aus der Microsoft App-Galerie

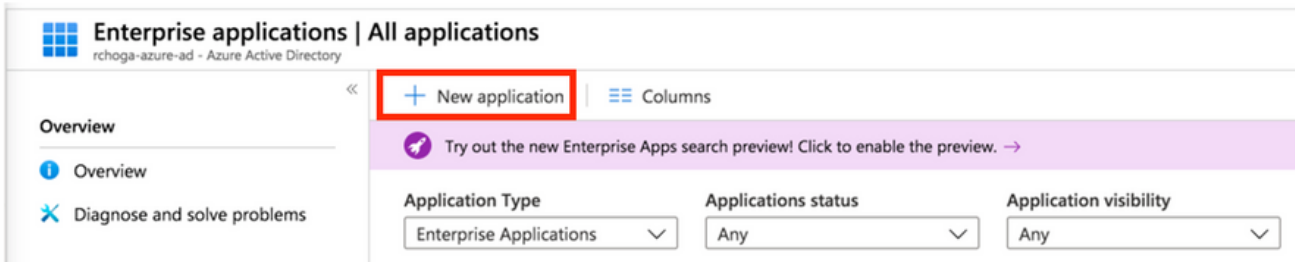
Schritt 1: Melden Sie sich beim Azure Portal an und wählen Sie Azure Active Directory aus.



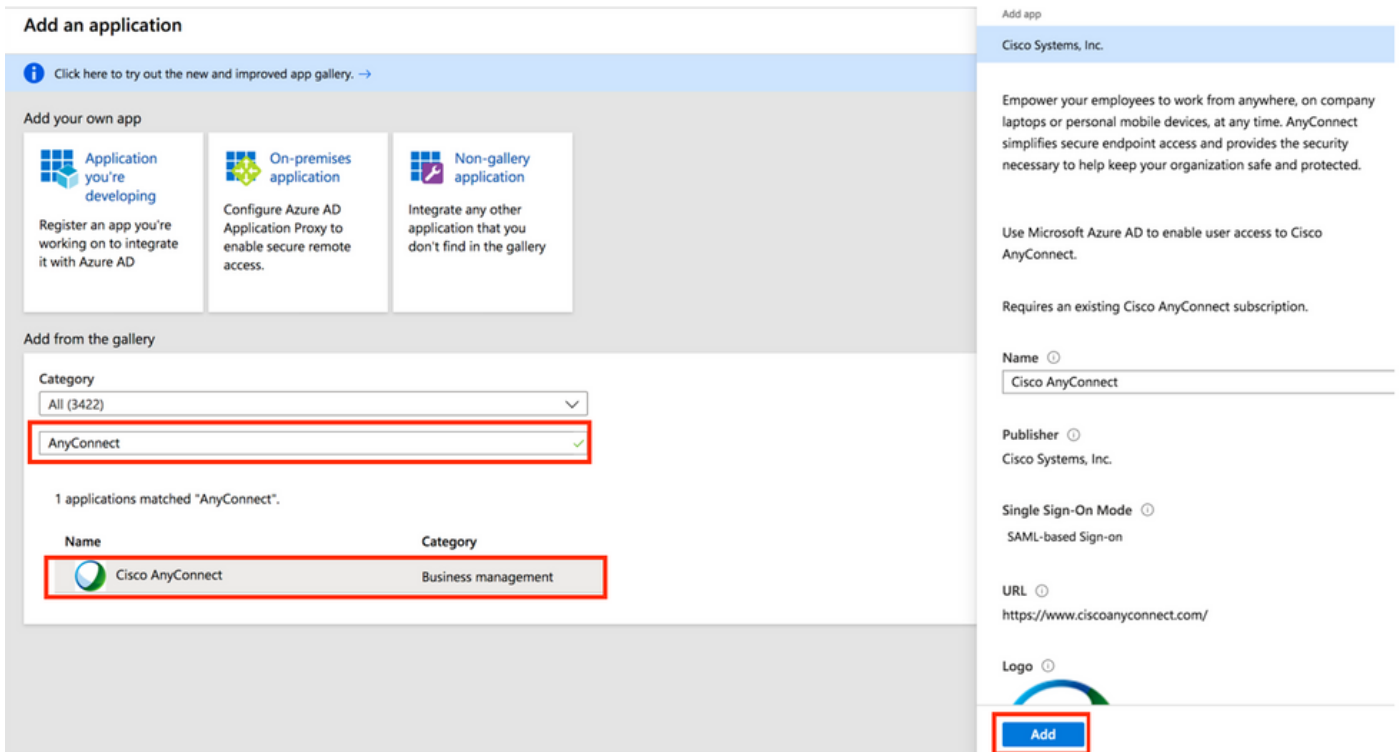
Schritt 2: Wählen Sie, wie in dieser Abbildung dargestellt, die Option **Enterprise Applications** aus.



Schritt 3. Wählen Sie nun **Neue Anwendung**, wie in diesem Bild dargestellt.



Schritt 4. Geben Sie im Abschnitt Aus der Galerie hinzufügen im Suchfeld AnyConnect ein, wählen Sie Cisco AnyConnect aus dem Ergebnissenfenster aus, und fügen Sie dann die App hinzu.



Schritt 5. Wählen Sie den Menüpunkt Single Sign-on (einmalige Anmeldung), wie in diesem Bild dargestellt.

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](#)

Schritt 6. Wählen Sie **SAML**, wie im Bild dargestellt.

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.

Schritt 7: Bearbeiten Sie **Abschnitt 1** mit diesen 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>

Schritt 8. Wählen Sie im Abschnitt **SAML-Signaturzertifikat** die Option **Herunterladen** aus, um die Zertifikatsdatei herunterzuladen und auf Ihrem Computer zu speichern.


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](#)


Schritt 9. Beachten Sie, dass dies für die ASA-Konfiguration erforderlich ist.


- Azure AD Identifier: Dies ist der SAML-IdP in unserer VPN-Konfiguration.
- Login URL: Dies ist die URL-Anmeldung.
- Logout URL: Dies ist die URL-Abmeldung.

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](#)

Zuweisen von Azure AD-Benutzern zur App

In diesem Abschnitt ist **Test1** für die Verwendung des Single Sign-On von Azure aktiviert, wenn Sie Zugriff auf die Cisco AnyConnect-App gewähren.

Schritt 1: Wählen Sie auf der Übersichtsseite der App **Benutzer und Gruppen** und dann **Benutzer hinzufügen aus**.

Cisco AnyConnect | Users and groups
Enterprise Application

[+ Add user](#) [Edit](#) [Remove](#) [Update Credentials](#) [Columns](#) [Got feedback?](#)

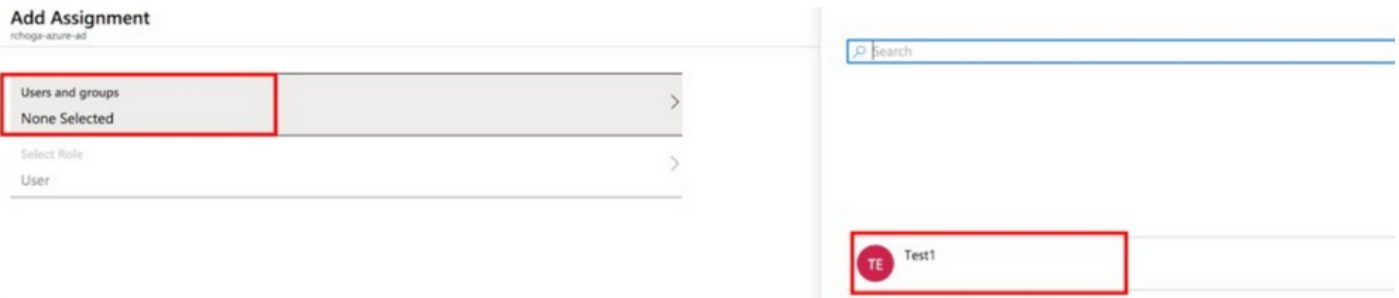
i The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

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

Display Name	Object Type	Role assigned
No application assignments found		

Navigation: Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, **Users and groups**, Single sign-on)

Schritt 2: Wählen Sie im Dialogfeld "Zuweisung hinzufügen" die Option **Benutzer und Gruppen**.



Schritt 3: Klicken Sie im Dialogfeld **Zuweisung hinzufügen** auf die Schaltfläche **Zuweisen**.



Konfigurieren der ASA für SAML über die CLI

Schritt 1: Erstellen Sie einen Vertrauenspunkt, und importieren Sie unser SAML-Zertifikat.

```
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
```

Schritt 2. Diese Befehle stellen Ihre SAML-IDp bereit.

```
webvpn

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

Schritt 3: Anwenden der SAML-Authentifizierung auf eine VPN-Tunnelkonfiguration.

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


Anmerkung: Wenn Sie Änderungen an der IdP-Konfiguration vornehmen, müssen Sie die Konfiguration des SAML Identity-Providers aus Ihrer Tunnelgruppe entfernen und erneut anwenden, damit die Änderungen wirksam werden.

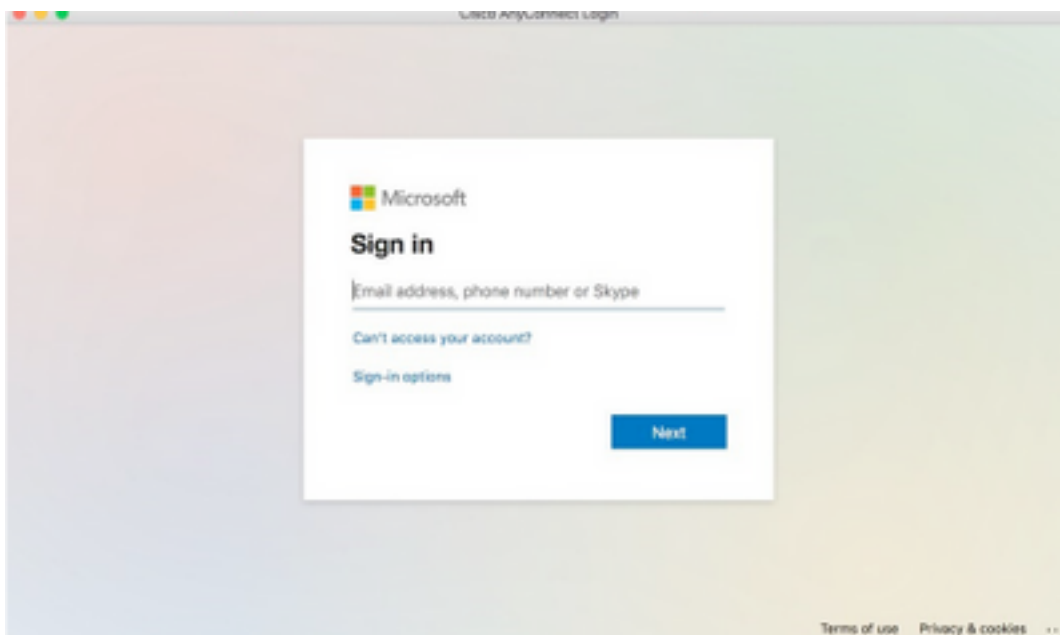
Überprüfung

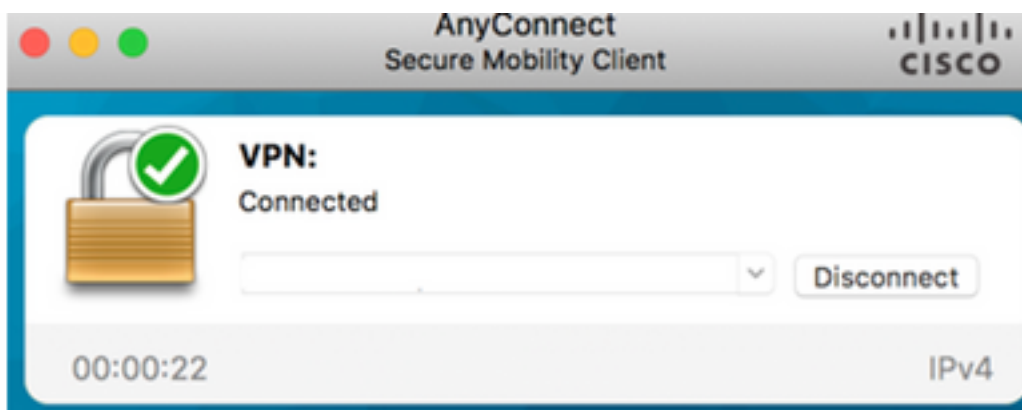
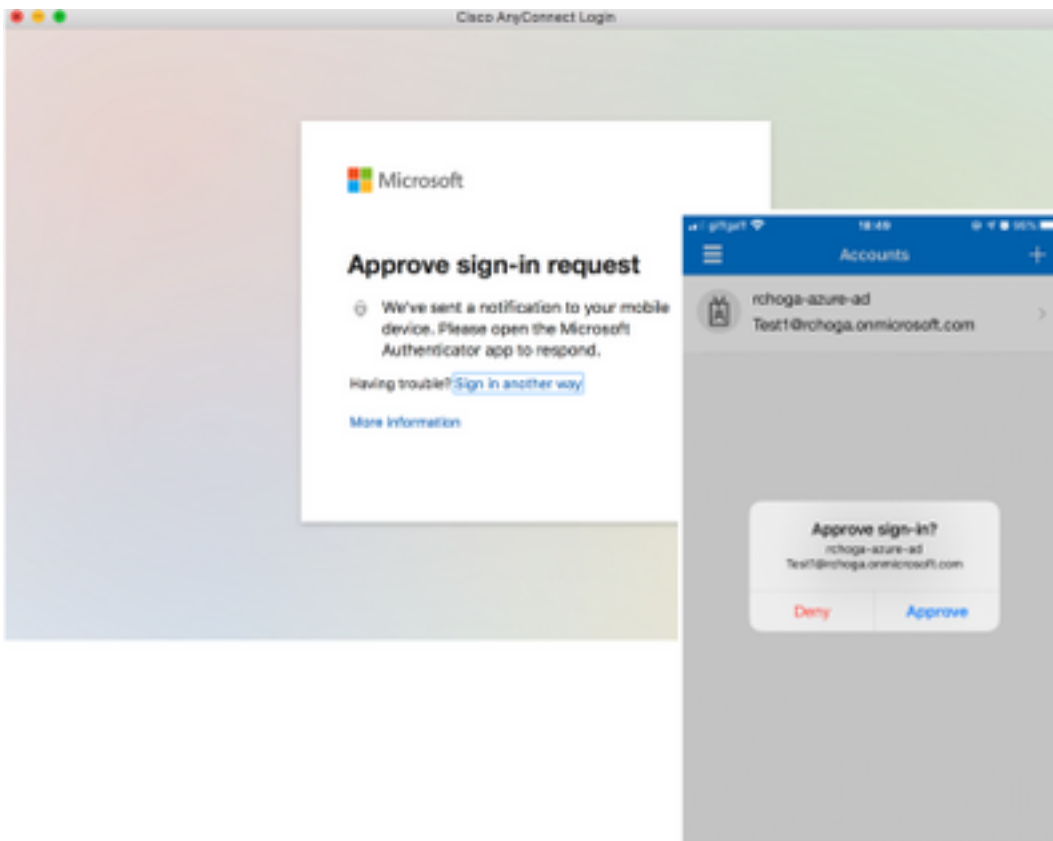
Testen von AnyConnect mit SAML-Authentifizierung

Schritt 1: Stellen Sie eine Verbindung mit Ihrer VPN-URL her, und geben Sie die Azure AD-Details für die Anmeldung ein.

Schritt 2: Anmeldeantrag genehmigen.

Schritt 3: AnyConnect ist verbunden.





Häufige Probleme

Entitäts-ID stimmt nicht überein

Debug-Beispiel:

[SAML] consume_assertion: Die ID eines Provider ist dem #LassoServer unbekannt. Um einen Provider in einem #LassoServer-Objekt zu registrieren, müssen Sie die Methoden `lasso_server_add_provider ()` oder `lasso_server_add_provider_from_buffer ()` verwenden.

Problem: Im Allgemeinen bedeutet dies, dass der Befehl `saml idp [entityID]` in der Web-VPN-Konfiguration der ASA nicht mit der IdP-Objektkennung in den Metadaten der IdP übereinstimmt.

Lösung: Überprüfen Sie die Entitäts-ID der Metadatenfile des IdP und ändern Sie den Befehl `saml idp [entityID]` entsprechend.

Zeit stimmt nicht überein

Debug-Beispiel:

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

[SAML] consume_assertion: assertion is expired or not valid (Assertion ist abgelaufen oder ungültig)

Problem 1. Die ASA-Zeit wurde nicht mit der IDp-Zeit synchronisiert.

Lösung 1. Konfigurieren Sie die ASA mit dem von IdP verwendeten NTP-Server.

Problem 2. Die Assertion ist zwischen dem angegebenen Zeitpunkt nicht gültig.

Lösung 2. Ändern Sie den auf dem ASA konfigurierten Timeout-Wert.

Falsches IdP-Signaturzertifikat verwendet

Debug-Beispiel:

```
[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: The profile cannot verify a signature on the message (Das Profil kann eine Signatur der Meldung nicht überprüfen)

Problem: Die ASA kann die vom IdP signierte Meldung nicht überprüfen, oder es gibt keine Signatur, die von der ASA überprüft werden kann.

Lösung: Überprüfen Sie das auf der ASA installierte IdP-Signaturzertifikat, um sicherzustellen, dass es mit dem vom IdP gesendeten Zertifikat übereinstimmt. Wenn dies bestätigt wird, stellen Sie sicher, dass die Signatur in der SAML-Antwort enthalten ist.

Ungültige Assertion-Zielgruppe

Debug-Beispiel:

```
[SAML] consume_assertion: assertion audience is invalid (Assertion-Zielgruppe ist ungültig)
```

Problem: IdP definiert die falsche Zielgruppe.

Lösung: Korrigieren Sie die Zielgruppenkonfiguration auf dem IdP. Sie muss mit der Objektkennung der ASA übereinstimmen.

Falsche URL für Assertion Consumer Service

Debug-Beispiel: Nach dem Senden der ersten Authentifizierungsanfrage können keine Debugs empfangen werden. Der Benutzer kann Anmeldeinformationen bei IdP eingeben, aber IdP leitet nicht an die ASA weiter.

Problem: IdP ist für die falsche Assertion Consumer Service-URL konfiguriert.

Lösung(en): Überprüfen Sie die Basis-URL in der Konfiguration und stellen Sie sicher, dass sie korrekt ist. Überprüfen Sie die ASA-Metadaten mit „show“, um sicherzustellen, dass die Assertion Consumer Service-URL korrekt ist. Um sie zu testen, durchsuchen Sie sie. Wenn beide auf der ASA korrekt sind, überprüfen Sie den IdP, um sicherzustellen, dass die URL korrekt ist.

SAML-Konfigurationsänderungen, die nicht wirksam werden

Beispiel: Nachdem eine Single Sign-On-URL geändert wurde, funktioniert das SP-Zertifikat, SAML jedoch immer noch nicht und sendet vorherige Konfigurationen.

Problem: ASA muss seine Metadaten neu generieren, wenn sich eine Konfigurationsänderung auf sie auswirkt. Dies geschieht nicht automatisch.

Lösung: Nachdem die Änderungen vorgenommen wurden, entfernen Sie unter der betroffenen Tunnelgruppe den Befehl `saml idp [entity-id]`, und wenden Sie ihn erneut an.

Fehlerbehebung

Die meisten SAML-Fehlerbehebungen beinhalten eine Fehlkonfiguration, die gefunden werden kann, wenn die SAML-Konfiguration überprüft oder Debugging ausgeführt wird. „debug webvpn saml 255“ kann zur Behebung der meisten Probleme verwendet werden. In Szenarien, in denen dieses Debugging keine nützlichen Informationen liefert, können jedoch weitere Debugging-Aktionen ausgeführt werden:

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

Zugehörige Informationen

- [SAML Single Sign-On für lokale Anwendungen mit Anwendungsproxy](#)