

SAML을 통해 Microsoft Azure MFA를 사용하여 ASA AnyConnect VPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[SAML 구성 요소](#)

[서명 및 암호화 작업용 인증서](#)

[네트워크 다이어그램](#)

[구성](#)

[Microsoft App Gallery에서 Cisco AnyConnect 추가](#)

[앱에 Azure AD 사용자 할당](#)

[CLI를 통해 SAML에 ASA 구성](#)

[다음을 확인합니다.](#)

[SAML 인증으로 AnyConnect 테스트](#)

[일반적인 문제](#)

[엔터티 ID 불일치](#)

[시간 불일치](#)

[잘못된 IdP 서명 인증서가 사용됨](#)

[잘못된 어설션 대상](#)

[어설션 소비자 서비스에 대한 잘못된 URL](#)

[적용되지 않는 SAML 구성 변경](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Microsoft Azure MFA를 통해 ASA(Adaptive Security Appliance) AnyConnect를 중점적으로 사용하여 SAML(Security Assertion Markup Language)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA의 RA VPN 구성에 대한 기본 지식
- SAML 및 Microsoft Azure에 대한 기본 지식
- AnyConnect 라이선스 활성화(APEX 또는 VPN 전용)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Azure AD 구독입니다.
- Cisco ASA 9.7+ 및 Anyconnect 4.6+
- AnyConnect VPN 프로파일 작업

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SAML은 보안 도메인 간에 인증 및 권한 부여 데이터를 교환하기 위한 XML 기반 프레임워크입니다. 사용자, 서비스 공급자(SP) 및 IdP(ID 공급자) 간에 신뢰 순환이 이루어져 여러 서비스에 대해 한 번에 로그인할 수 있습니다. Microsoft Azure MFA는 Cisco ASA VPN 어플라이언스와 원활하게 통합되어 Cisco AnyConnect VPN 로그인에 대한 추가 보안을 제공합니다.

SAML 구성 요소

메타데이터: IdP와 SP 간의 안전한 트랜잭션을 보장하는 XML 기반 문서입니다. IdP와 SP가 계약을 협상할 수 있습니다.

디바이스(IdP, SP)에서 지원되는 역할

디바이스는 둘 이상의 역할을 지원할 수 있으며 SP와 IdP 모두에 대한 값을 포함할 수 있습니다. 포함된 정보가 Single Sign-On IdP용인 경우 EntityDescriptor 필드 아래에 IDPSSODescriptor가 있고, 포함된 정보가 Single Sign-On SP용인 경우 SPSSODescriptor 아래에 있습니다. SAML을 성공적으로 설정하려면 해당 섹션에서 올바른 값을 가져와야 하므로 이 작업이 중요합니다.

엔티티 ID: 이 필드는 SP 또는 IdP의 고유 식별자입니다. 단일 디바이스에는 여러 서비스가 있을 수 있으며 다른 엔티티 ID를 사용하여 이들을 구분할 수 있습니다. 예를 들어, ASA에는 인증해야 하는 서로 다른 터널 그룹에 대해 서로 다른 엔티티 ID가 있습니다. 각 터널 그룹을 인증하는 IdP에는 각 터널 그룹에 대해 별도의 Entity ID 항목이 있어 해당 서비스를 정확하게 식별할 수 있습니다.

ASA는 여러 IdP를 지원할 수 있으며 각 IdP에 대해 별도의 엔티티 ID를 가지고 차별화합니다. 어느 한쪽이 이전에 구성된 엔티티 ID가 없는 디바이스에서 메시지를 수신하는 경우, 디바이스는 이 메시지를 삭제하며 SAML 인증에 실패할 수 있습니다. 엔티티 ID는 entityID 옆의 EntityDescriptor 필드 내에서 찾을 수 있습니다.

서비스 URL: SP 또는 IdP에서 제공하는 SAML 서비스의 URL을 정의합니다. IdP의 경우 이 서비스는 대개 단일 로그아웃 서비스 및 단일 로그인 서비스입니다. SP의 경우 일반적으로 Assertion Consumer Service 및 Single Logout Service입니다.

IdP 메타데이터에 있는 Single Sign-On 서비스 URL은 SP에서 사용자를 인증을 위해 IdP로 리디렉션하는 데 사용됩니다. 이 값이 잘못 구성되면 IdP가 SP에서 전송한 인증 요청을 수신하지 못하거나 성공적으로 처리할 수 없습니다.

SP 메타데이터에 있는 Assertion Consumer Service URL은 IdP에서 사용자를 다시 SP로 리디렉션하고 사용자 인증 시도에 대한 정보를 제공하는 데 사용됩니다. 이 구성이 잘못 구성되면 SP에서 어설션(응답)을 수신하지 않거나 성공적으로 처리할 수 없습니다.

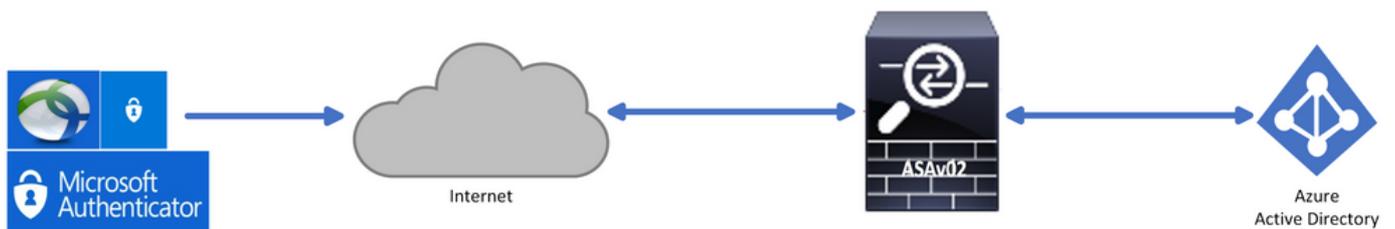
단일 로그아웃 서비스 URL은 SP와 IdP 모두에서 찾을 수 있습니다. SP에서 모든 SSO 서비스를 로그아웃하는 데 사용되며 ASA에서는 선택 사항입니다. IdP 메타데이터의 SLO 서비스 URL이 SP에 구성되어 있는 경우 사용자가 SP의 서비스에서 로그아웃하면 SP는 요청을 IdP로 보냅니다. IdP가 서비스에서 사용자를 성공적으로 로그아웃하면 해당 사용자는 다시 SP로 리디렉션되고 SP 메타데이터에 있는 SLO 서비스 URL을 사용합니다.

서비스 URL에 대한 SAML 바인딩: 바인딩은 SP에서 서비스에 대한 정보를 IdP로 또는 그 반대로 전송하는 데 사용하는 방법입니다. 여기에는 HTTP 리디렉션, HTTP POST 및 아티팩트가 포함됩니다. 각 방법마다 데이터를 전송하는 방법이 다릅니다. 서비스에서 지원하는 바인딩 방법은 해당 서비스의 정의에 포함되어 있습니다. 예: SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location=<https://saml.example.com/simplesaml/saml2/idp/SSOService.php/> >. ASA는 아티팩트 바인딩을 지원하지 않습니다. ASA는 항상 SAML 인증 요청에 HTTP 리디렉션 방법을 사용하므로 IdP에서 이를 예상하도록 HTTP 리디렉션 바인딩을 사용하는 SSO 서비스 URL을 선택해야 합니다.

서명 및 암호화 작업용 인증서

SP와 IdP 간에 전송되는 메시지에 대해 기밀성과 무결성을 제공하기 위해 SAML에는 데이터를 암호화하고 서명하는 기능이 포함되어 있습니다. 데이터를 암호화 및/또는 서명하는 데 사용되는 인증서는 메타데이터 내에 포함될 수 있으므로 수신하는 쪽에서 SAML 메시지를 확인하고 해당 메시지가 예상 소스에서 온 것인지 확인할 수 있습니다. 서명 및 암호화에 사용된 인증서는 메타데이터 내에서 KeyDescriptor use="signing" 및 KeyDescriptor use="encryption", X509Certificate의 순서로 찾을 수 있습니다. ASA는 SAML 메시지 암호화를 지원하지 않습니다.

네트워크 다이어그램



구성

Microsoft App Gallery에서 Cisco AnyConnect 추가

1단계. Azure Portal에 로그인하고 Azure Active Directory를 선택합니다.

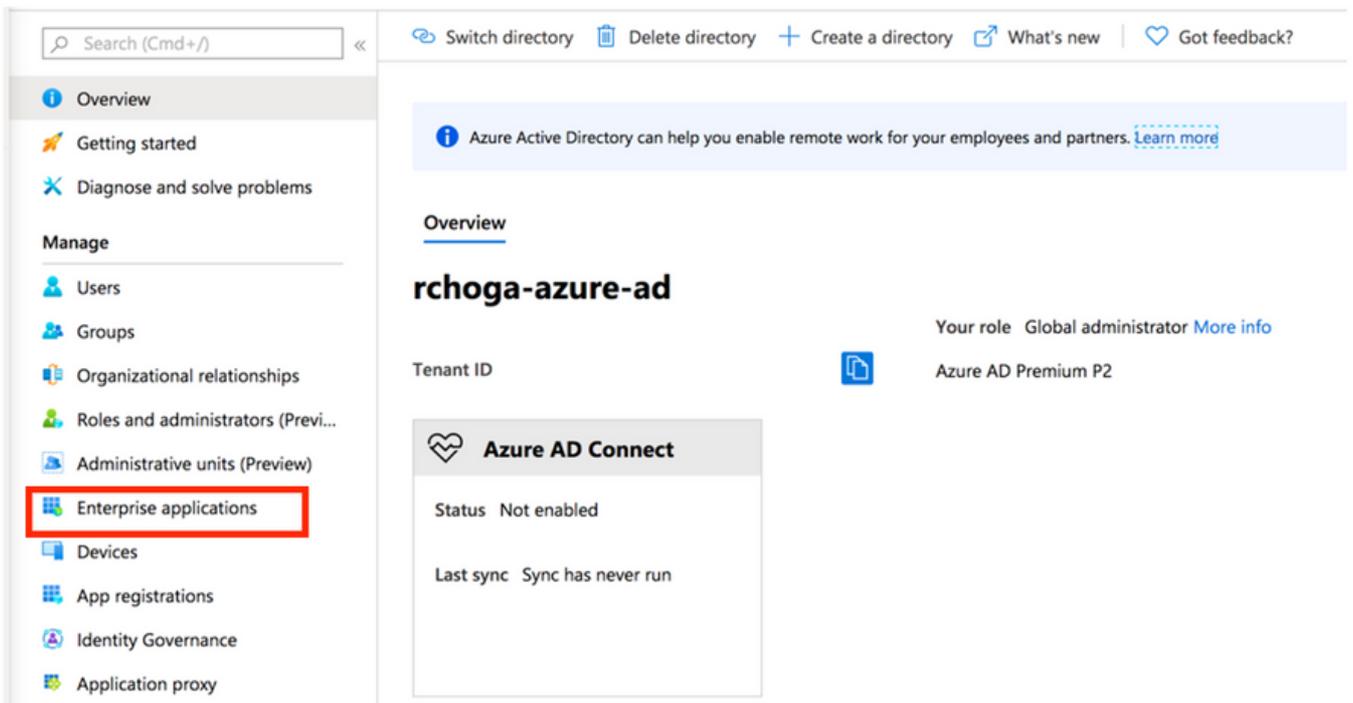
Azure services



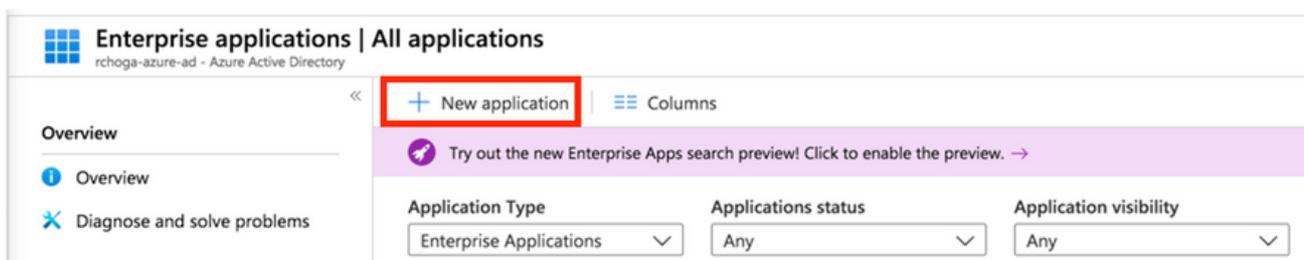
Navigate



2단계. 이 이미지에 표시된 대로 엔터프라이즈 애플리케이션을 선택합니다.



3단계. 이제 이 이미지에 표시된 대로 New Application(새 애플리케이션)을 선택합니다.



4단계. Add from the gallery(갤러리에서 추가) 섹션의 검색 상자에 AnyConnect를 입력하고 결과 패널에서 Cisco AnyConnect를 선택한 다음 앱을 추가합니다.

Add an application

Click here to try out the new and improved app gallery. →

Add your own app

- Application you're developing**
Register an app you're working on to integrate it with Azure AD
- On-premises application**
Configure Azure AD Application Proxy to enable secure remote access.
- Non-gallery application**
Integrate any other application that you don't find in the gallery

Add from the gallery

Category: All (3422) | **AnyConnect**

1 applications matched "AnyConnect".

Name	Category
Cisco AnyConnect	Business management

Add app

Cisco Systems, Inc.

Empower your employees to work from anywhere, on company laptops or personal mobile devices, at any time. AnyConnect simplifies secure endpoint access and provides the security necessary to help keep your organization safe and protected.

Use Microsoft Azure AD to enable user access to Cisco AnyConnect.

Requires an existing Cisco AnyConnect subscription.

Name: Cisco AnyConnect

Publisher: Cisco Systems, Inc.

Single Sign-On Mode: SAML-based Sign-on

URL: https://www.ciscoanyconnect.com/

Logo:

Add

5단계. 이 이미지에 표시된 대로 단일 로그인 메뉴 항목을 선택합니다.

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

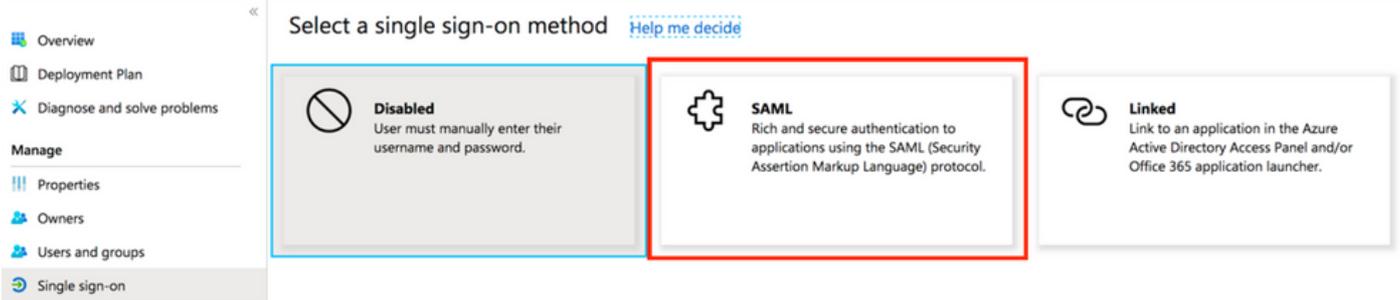
Application ID

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](#)

6단계. 이미지에 표시된 대로 SAML을 선택합니다.



7단계. 이러한 세부 정보로 섹션 1을 편집합니다.

<#root>

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

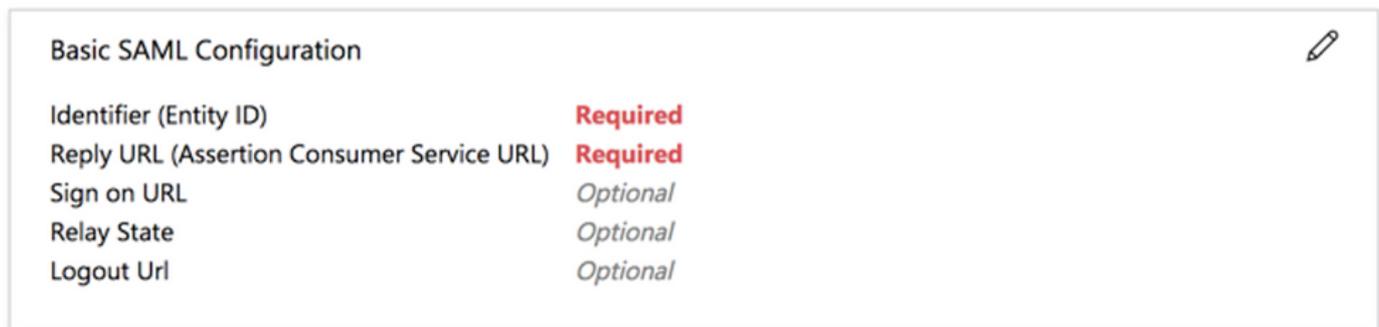
b. Reply URL (Assertion Consumer Service URL) - `https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<TUNNEL-G`

Example: vpn url called

`asa.example.com`

and tunnel-group called

`AnyConnectVPN-1`



8단계. SAML Signing Certificate(SAML 서명 인증서) 섹션에서 Download(다운로드)를 선택하여 인증서 파일을 다운로드한 다음 컴퓨터에 저장합니다.

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](#)

9단계. 이는 ASA 컨피그레이션에 필요합니다.

- Azure AD Identifier - VPN 구성의 동일한 idp입니다.
- Login URL(로그인 URL) - URL 로그인입니다.
- Logout URL(로그아웃 URL) - URL 로그아웃입니다.

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](#)

앱에 Azure AD 사용자 할당

이 섹션에서는 Cisco AnyConnect 앱에 대한 액세스 권한을 부여하므로 Test1이 Azure Single Sign-On을 사용하도록 설정됩니다.

1단계. 앱의 개요 페이지에서 사용자 및 그룹, 사용자 추가를 선택합니다.

Cisco AnyConnect | Users and groups
Enterprise Application

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

Overview

- Deployment Plan
- Diagnose and solve problems

Manage

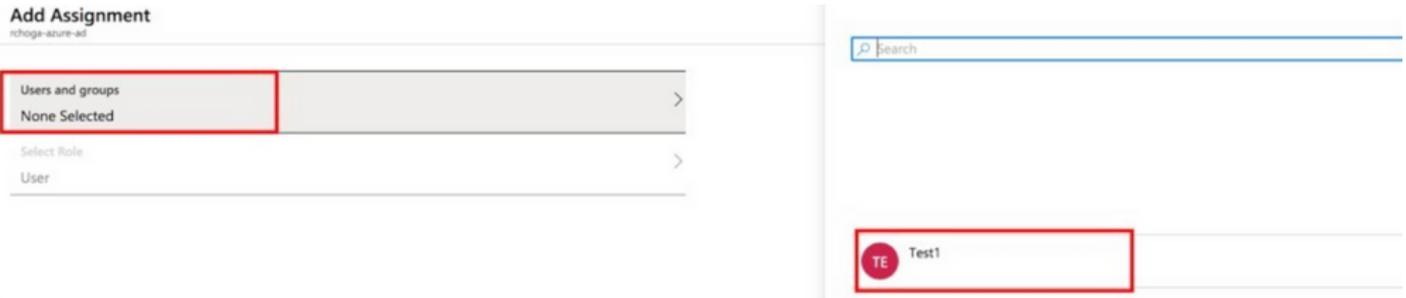
- Properties
- Owners
- Users and groups**
- Single sign-on

Users and groups

Display Name **Object Type** **Role assigned**

No application assignments found

2단계. [할당 추가] 대화 상자에서 [사용자] 및 [그룹]을 선택합니다.



3단계. Add Assignment(할당 추가) 대화 상자에서 Assign(할당) 버튼을 클릭합니다.



CLI를 통해 SAML에 ASA 구성

1단계. 신뢰 지점을 생성하고 SAML 인증서를 가져옵니다.

```
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
```

2단계. 이 명령은 SAML IdP를 프로비저닝합니다.

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
```

3단계. VPN 터널 컨피그레이션에 SAML 인증 적용

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

write memory
```

 참고: IdP 컨피그레이션을 변경하는 경우 터널 그룹에서 saml identity-provider 컨피그레이션을 제거하고 다시 적용해야 변경 사항이 적용됩니다.

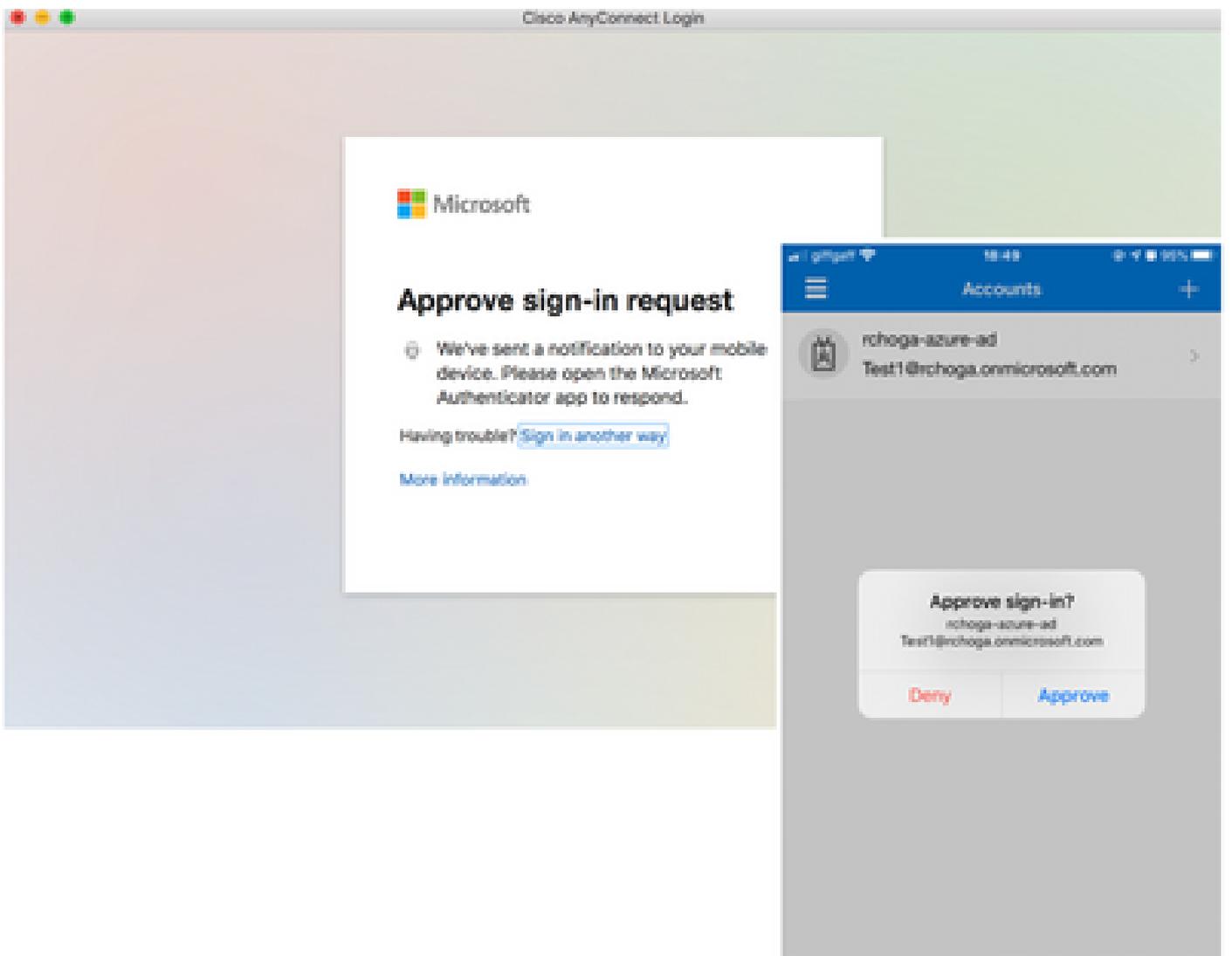
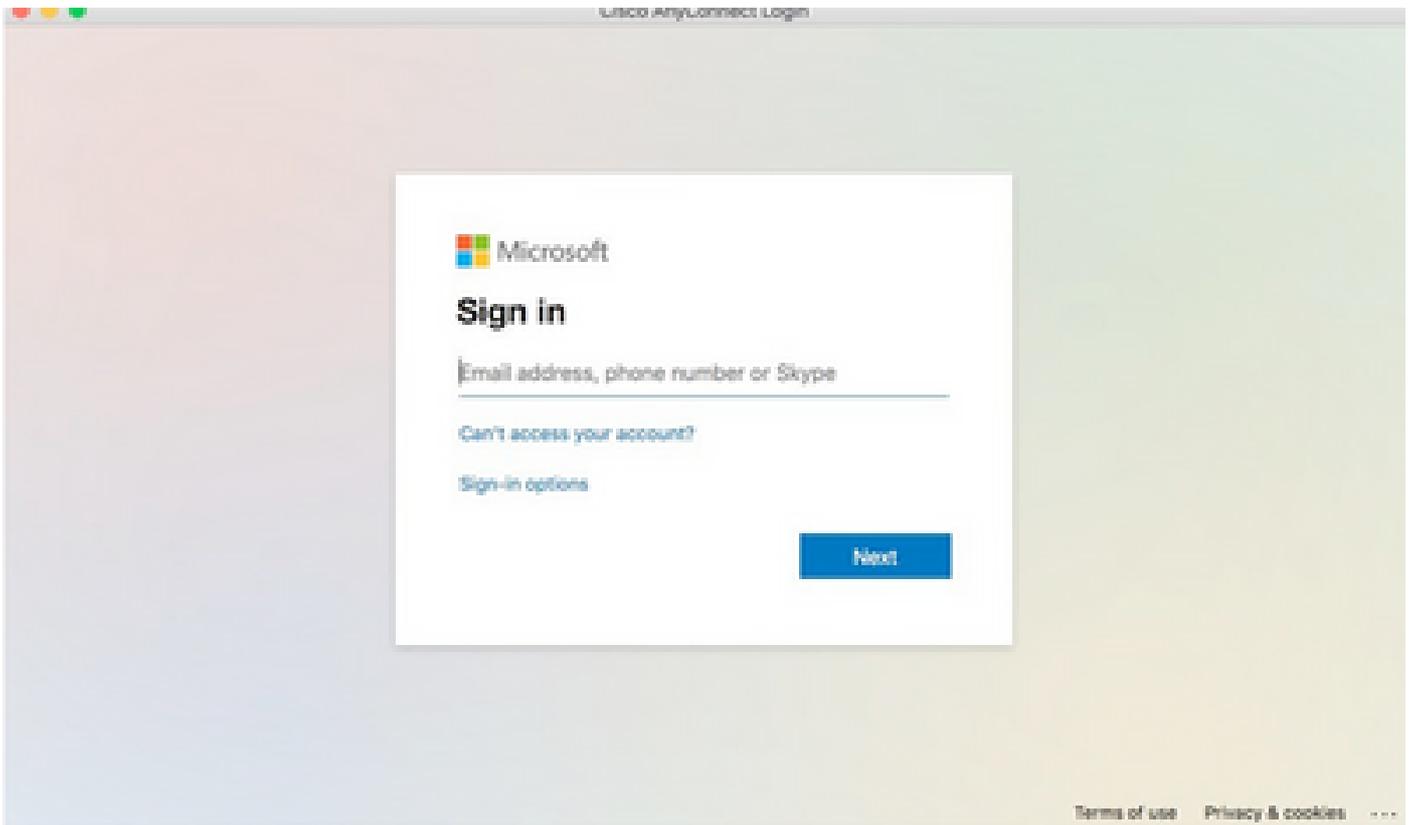
다음을 확인합니다.

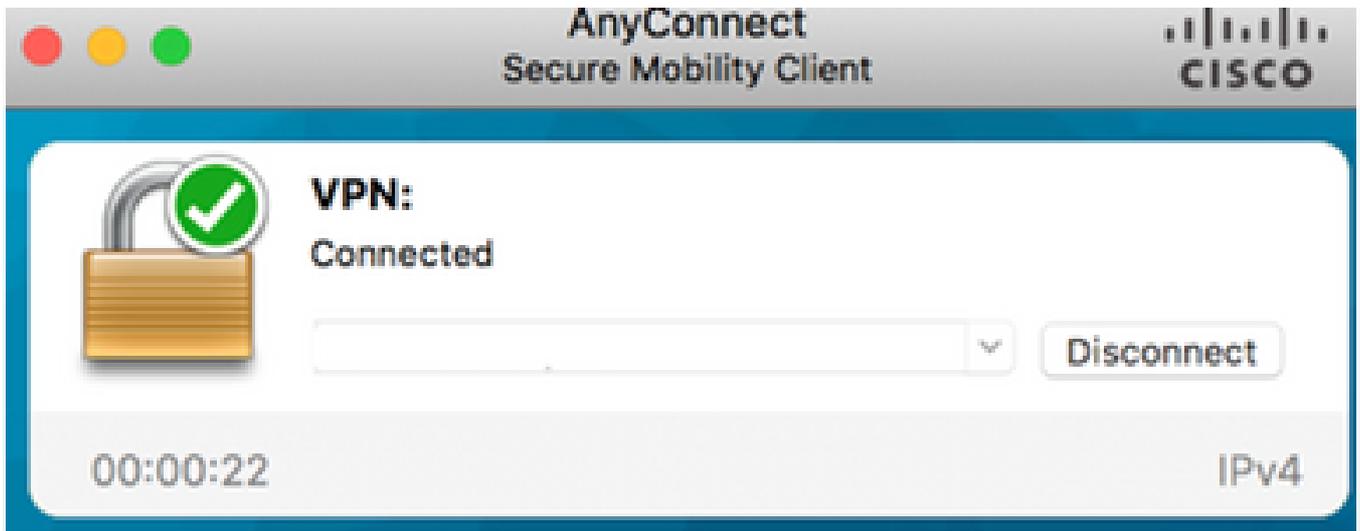
SAML 인증으로 AnyConnect 테스트

1단계. VPN URL에 연결하고 Azure AD 세부 정보에 로그를 입력합니다.

2단계. 로그인 요청을 승인합니다.

3단계. AnyConnect가 연결되었습니다.





일반적인 문제

엔터티 ID 불일치

디버그 예:

[SAML] consumer_assertion: 공급자의 식별자는 #LassoServer 알 수 없습니다. #LassoServer 객체에서 공급자를 등록하려면 lasso_server_add_provider() 또는 lasso_server_add_provider_from_buffer() 메서드를 사용해야 합니다.

문제: 일반적으로 ASA의 webvpn 컨피그레이션에 있는 saml idp [entityID] 명령이 IdP 메타데이터에 있는 IdP 엔티티 ID와 일치하지 않음을 의미합니다.

해결 방법: IdP 메타데이터 파일의 엔티티 ID를 확인하고 이에 맞게 saml idp [entity id] 명령을 변경합니다.

시간 불일치

디버그 예:

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

[SAML] expense_assertion: 어설션이 만료되었거나 유효하지 않습니다.

문제 1. ASA 시간이 IdP 시간과 동기화되지 않았습니다.

해결 방법 1. IdP에서 사용하는 것과 동일한 NTP 서버로 ASA를 구성합니다.

문제 2. 지정된 시간 사이에 어설션이 유효하지 않습니다.

해결 방법 2. ASA에 구성된 시간 초과 값을 수정합니다.

잘못된 IdP 서명 인증서가 사용됨

디버그 예:

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

[SAML] consumer_assertion: 프로필에서 메시지의 서명을 확인할 수 없습니다.

문제: ASA에서 IdP로 서명된 메시지를 확인할 수 없거나 ASA에서 확인할 서명이 없습니다.

해결 방법: ASA에 설치된 IdP 서명 인증서가 IdP에서 전송한 것과 일치하는지 확인하십시오. 이것이 확인되면 서명이 SAML 응답에 포함되어 있는지 확인합니다.

잘못된 어설션 대상

디버그 예:

```
[SAML] consult_assertion: 어설션 대상이 잘못되었습니다.
```

문제: IdP가 잘못된 대상을 정의합니다.

해결 방법: IdP에서 대상 그룹 구성을 수정하십시오. ASA의 엔티티 ID와 일치해야 합니다.

어설션 소비자 서비스에 대한 잘못된 URL

디버그 예: 초기 인증 요청을 전송한 후에는 디버그를 수신할 수 없습니다. 사용자는 IdP에서 자격 증명을 입력할 수 있지만 IdP는 ASA로 리디렉션되지 않습니다.

문제: IdP가 잘못된 Assertion Consumer Service URL에 대해 구성되어 있습니다.

해결 방법: 구성의 기본 URL을 확인하고 올바른지 확인하십시오. ASA 메타데이터를 show로 확인하여 Assertion Consumer Service URL이 올바른지 확인합니다. 테스트하려면 ASA에서 모두 올바르게 IdP를 확인하여 URL이 올바른지 확인합니다.

적용되지 않는 SAML 구성 변경

예: SSO(Single Sign On) URL이 수정되거나 변경된 후에도 SP 인증서인 SAML이 여전히 작동하지 않고 이전 컨피그레이션을 전송합니다.

문제: ASA에 영향을 주는 구성 변경이 있을 경우 메타데이터를 다시 생성해야 합니다. 자동으로 실행되지 않습니다.

해결 방법: 변경 후 영향받는 tunnel-group remove 아래에서 saml idp [entity-id] 명령을 다시 적용합

니다.

문제 해결

대부분의 SAML 문제 해결에는 SAML 구성을 확인하거나 디버그를 실행할 때 찾을 수 있는 잘못된 구성이 포함됩니다. 대부분의 문제를 해결하려면 디버그 webvpn saml 255를 사용할 수 있지만 이 디버그가 유용한 정보를 제공하지 않는 시나리오에서 추가 디버그를 실행할 수 있습니다.

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

관련 정보

- [애플리케이션 프록시를 사용하는 온프레미스 애플리케이션용 SAML SSO\(single sign-on\)](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.