

Configurazione di ASA AnyConnect VPN con Microsoft Azure MFA tramite SAML

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Componenti SAML](#)

[Certificati per le operazioni di firma e crittografia](#)

[Esempio di rete](#)

[Configurazione](#)

[Aggiungi Cisco AnyConnect da Microsoft App Gallery](#)

[Assegna utente di Azure AD all'app](#)

[Configurazione di ASA per SAML tramite CLI](#)

[Verifica](#)

[Test di AnyConnect con autenticazione SAML](#)

[Problemi comuni](#)

[ID entità non corrispondente](#)

[Tempo non corrispondente](#)

[Utilizzato certificato di firma IdP errato](#)

[Gruppo di destinatari asserzione non valido](#)

[URL errato per il servizio consumer di asserzione](#)

[Modifiche alla configurazione SAML che non hanno effetto](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare SAML (Security Assertion Markup Language) con particolare attenzione alle appliance ASA (Adaptive Security Appliance) AnyConnect tramite Microsoft Azure MFA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione della VPN ASA su ASA.
- Conoscenze base di SAML e Microsoft Azure.

- Licenze AnyConnect abilitate (APEX o VPN Only).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Sottoscrizione di Microsoft Azure AD.
- Cisco ASA 9.7+ e Anyconnect 4.6+
- Funzionamento del profilo AnyConnect VPN

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

SAML è un framework basato su XML per lo scambio di dati di autenticazione e autorizzazione tra domini di protezione. Crea un cerchio di fiducia tra l'utente, un provider di servizi (SP) e un provider di identità (IdP) che consente all'utente di accedere una sola volta a più servizi. Microsoft Azure MFA si integra perfettamente con l'appliance VPN Cisco ASA per fornire una maggiore sicurezza per gli accessi VPN di Cisco AnyConnect.

Componenti SAML

Metadati: Si tratta di un documento basato su XML che garantisce una transazione sicura tra un IdP e un SP. Consente a IdP e SP di negoziare accordi.

Ruoli supportati dai dispositivi (IdP, SP)

Un dispositivo può supportare più ruoli e può contenere valori sia per un SP che per un IdP. Sotto il campo EntityDescriptor è presente un IDPSSODescriptor se le informazioni contenute si riferiscono a un IdP Single Sign-On o a un SPSSODescriptor se le informazioni contenute si riferiscono a un SP Single Sign-On. Questa operazione è importante in quanto per impostare correttamente SAML è necessario utilizzare i valori corretti delle sezioni appropriate.

ID entità: Questo campo è un identificatore univoco per un SP o un IdP. Un singolo dispositivo può disporre di più servizi e utilizzare ID entità diversi per differenziarli. Ad esempio, l'appliance ASA ha ID di entità diversi per gruppi di tunnel diversi che devono essere autenticati. Un IdP che autentica ogni gruppo di tunnel dispone di voci di ID entità separate per ogni gruppo di tunnel al fine di identificare con precisione tali servizi.

L'ASA può supportare più IdP e ha un ID entità separato per ciascun IdP per differenziarli. Se uno dei due lati riceve un messaggio da un dispositivo che non contiene un ID entità configurato in precedenza, è probabile che il dispositivo lo rifiuti e l'autenticazione SAML non riesce. L'ID entità è disponibile nel campo EntityDescriptor accanto a entityID.

URL servizio: Definiscono l'URL di un servizio SAML fornito dall'SP o dall'IdP. Per gli IdP, si tratta in genere del servizio Single Logout e del servizio Single Sign-on. Per gli SP, in genere si tratta del servizio consumer di asserzione e del servizio di disconnessione singola.

L'URL del servizio Single Sign-on trovato nei metadati IdP viene utilizzato dall'SP per reindirizzare l'utente all'IdP per l'autenticazione. Se questo valore non è configurato correttamente, l'IdP non riceve o non è in grado di elaborare correttamente la richiesta di autenticazione inviata dall'SP.

L'URL del servizio consumer di asserzione trovato nei metadati SP viene utilizzato dall'IdP per reindirizzare l'utente all'SP e fornire informazioni sul tentativo di autenticazione dell'utente. Se la configurazione non è corretta, l'SP non riceve l'asserzione (la risposta) o non è in grado di elaborarla correttamente.

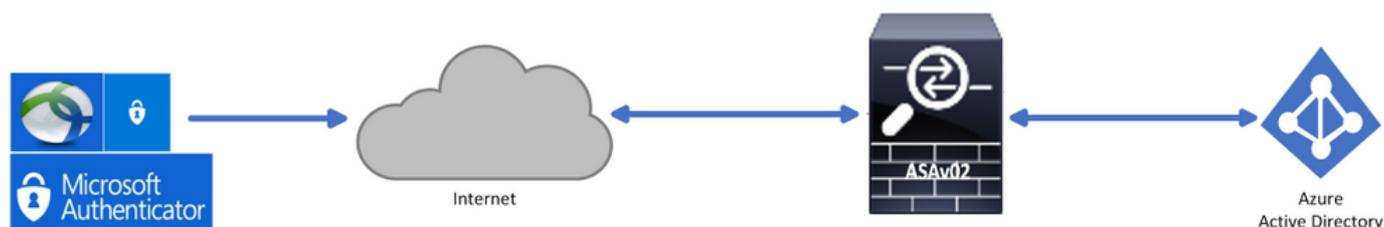
L'URL del servizio di disconnessione singola è disponibile sia nell'SP che nell'IdP. Viene utilizzato per facilitare la disconnessione di tutti i servizi SSO dall'SP ed è facoltativo sull'appliance ASA. Quando l'URL del servizio SLO dai metadati IdP è configurato sull'SP, quando l'utente si disconnette dal servizio sull'SP, l'SP invia la richiesta all'IdP. Una volta che l'IdP ha eseguito correttamente la disconnessione dell'utente dai servizi, reindirizza l'utente all'SP e utilizza l'URL del servizio SLO trovato nei metadati dell'SP.

Associazioni SAML per URL servizio: Le associazioni sono il metodo che lo Storage Processor utilizza per trasferire le informazioni all'IdP e viceversa per i servizi. Sono inclusi Reindirizzamento HTTP, HTTP POST e Artifact. Ogni metodo ha un modo diverso di trasferire i dati. Il metodo di associazione supportato dal servizio è incluso nella definizione di tali servizi. Ad esempio: SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="<https://saml.example.com/simplesaml/saml2/idp/SSOService.php/>". L'appliance ASA non supporta il binding Artifact. ASA utilizza sempre il metodo di reindirizzamento HTTP per le richieste di autenticazione SAML, quindi è importante scegliere l'URL del servizio SSO che utilizza il binding di reindirizzamento HTTP in modo che l'IdP lo preveda.

Certificati per le operazioni di firma e crittografia

Per garantire la riservatezza e l'integrità dei messaggi inviati tra l'SP e l'IdP, SAML offre la possibilità di crittografare e firmare i dati. Il certificato utilizzato per crittografare e/o firmare i dati può essere incluso nei metadati in modo che l'estremità che riceve possa verificare il messaggio SAML e assicurarsi che provenga dall'origine prevista. I certificati utilizzati per la firma e la crittografia sono disponibili nei metadati in KeyDescriptor use="signature" e KeyDescriptor use="encryption", rispettivamente, quindi in X509Certificate. L'ASA non supporta la crittografia dei messaggi SAML.

Esempio di rete

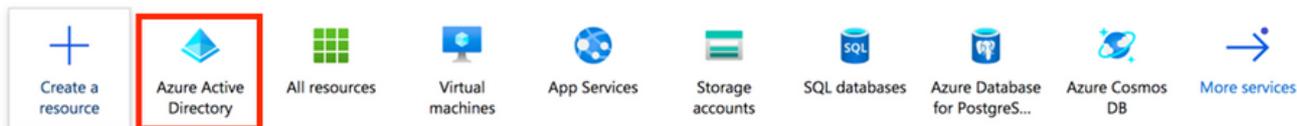


Configurazione

Aggiungi Cisco AnyConnect da Microsoft App Gallery

Passaggio 1. Accedere al portale di Azure e selezionare **Azure Active Directory**.

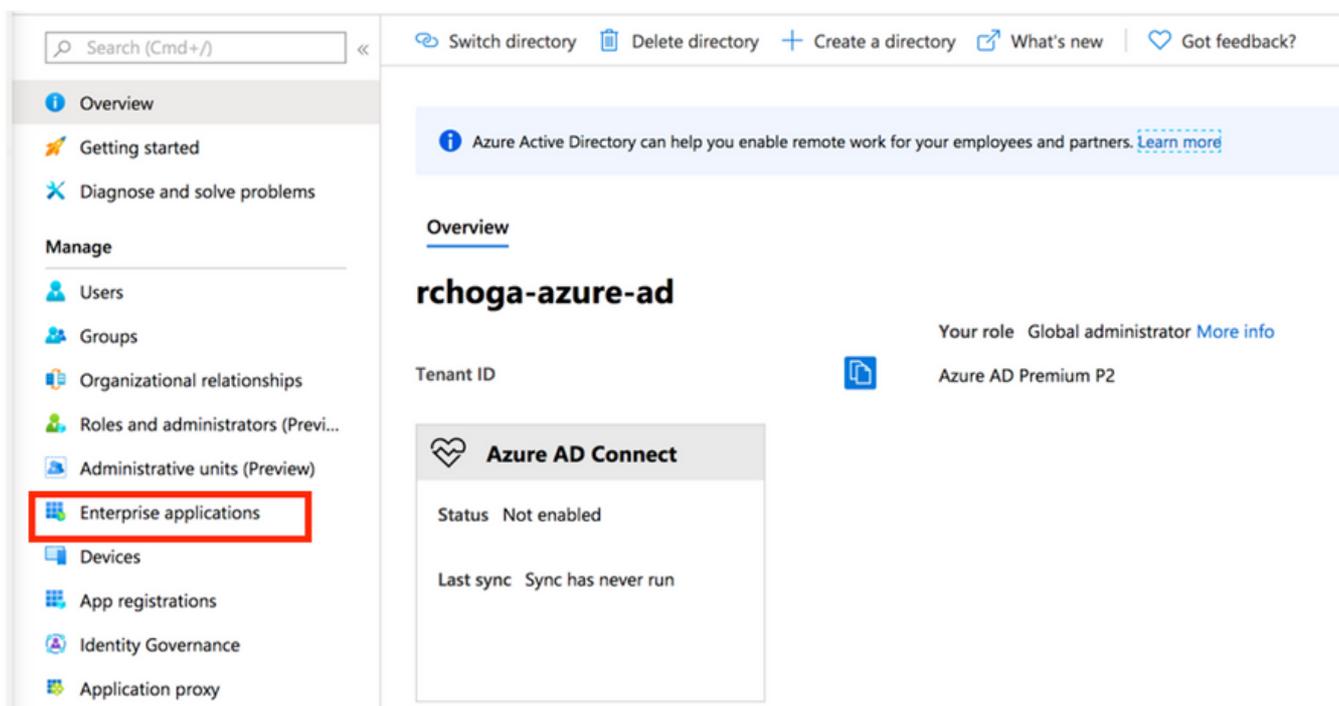
Azure services



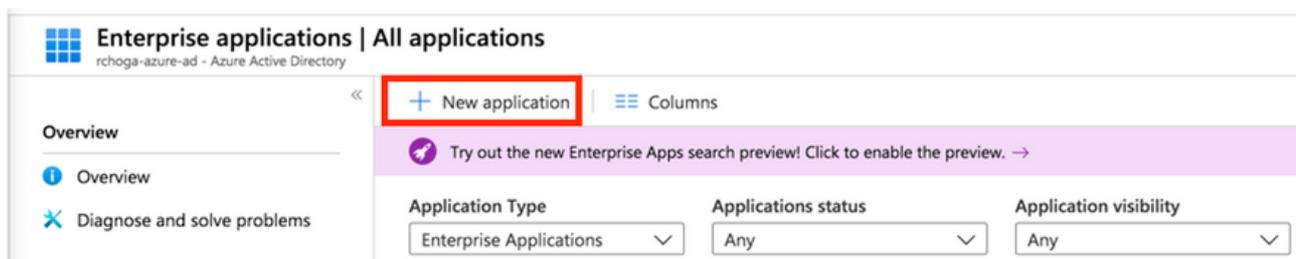
Navigate



Passaggio 2. Come mostrato in questa immagine, selezionare **Applicazioni enterprise**.



Passaggio 3. Selezionare **Nuova applicazione**, come mostrato nell'immagine.



Passaggio 4. Nella sezione **Aggiungi dalla raccolta**, digitare **AnyConnect** nella casella di ricerca, selezionare **Cisco AnyConnect** dal pannello dei risultati, quindi **aggiungere** l'app.

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

Passaggio 5. Selezionare la voce di menu **Single Sign-on**, come illustrato in questa immagine.

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

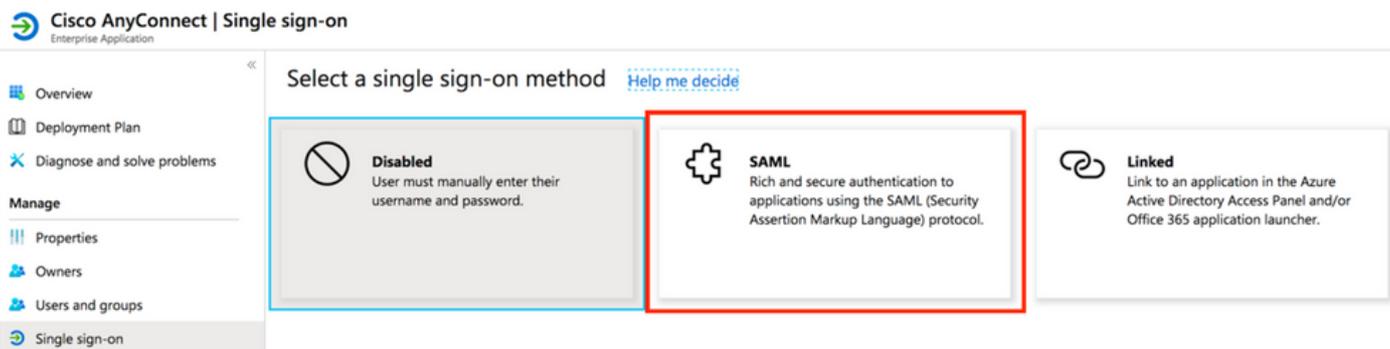
Application ID

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](#)

Passaggio 6. Selezionare **SAML**, come mostrato nell'immagine.

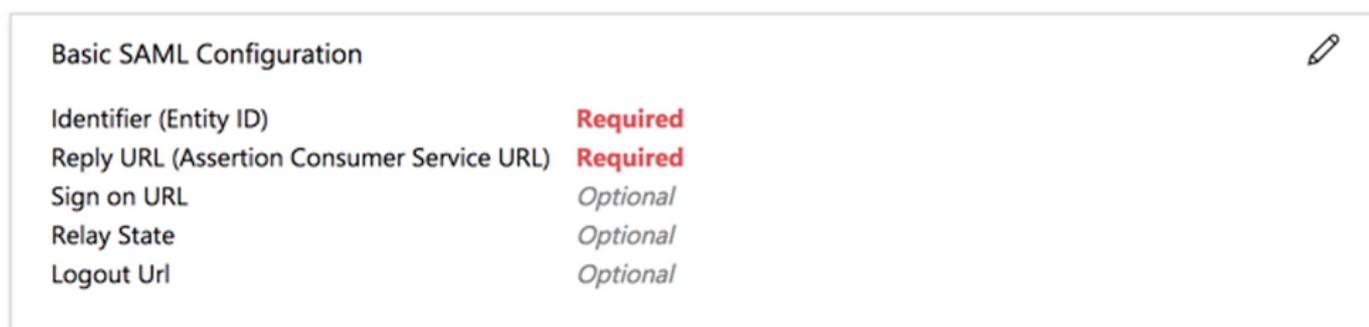


Passaggio 7. Modificare la **sezione 1** con questi dettagli.

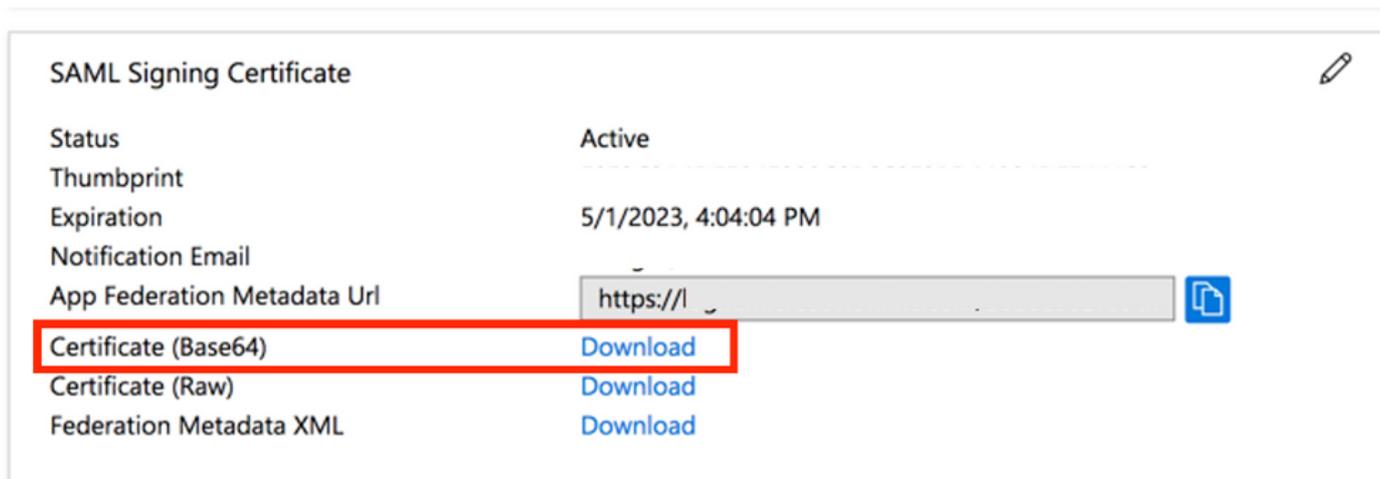
a. Identifier (Entity ID) - `https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME>`

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

Example: vpn url called **asa.example.com** and tunnel-group called **AnyConnectVPN-1**



Passaggio 8. Nella sezione **Certificato di firma SAML**, selezionare **Scarica** per scaricare il file del certificato e salvarlo sul computer.



Passaggio 9. Questa operazione è obbligatoria per la configurazione dell'ASA.

- Azure AD Identifier - Si tratta dell'ID saml nella configurazione VPN.
- URL di accesso: URL di accesso.
- URL di disconnessione - URL di disconnessione.

Set up AnyConnectVPN

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

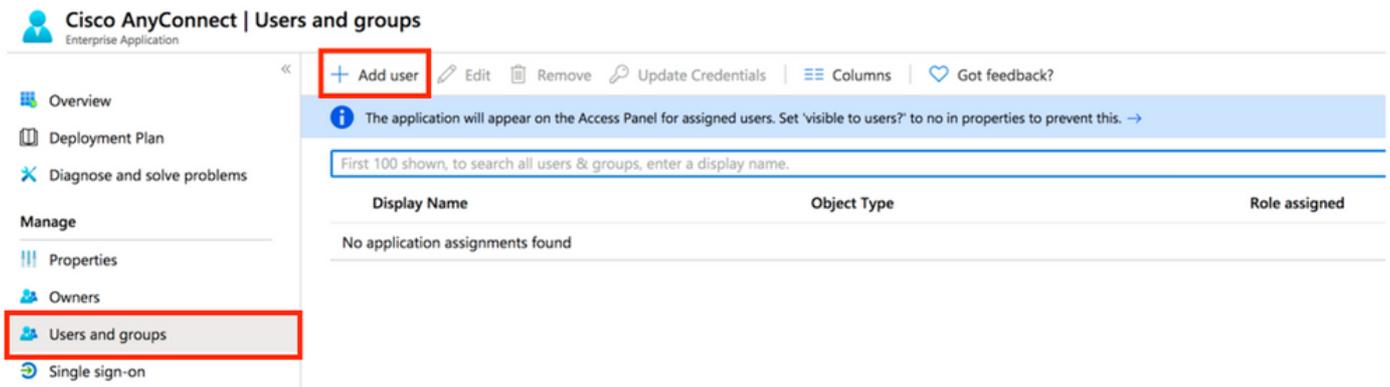
| | | |
|---------------------|---------------------------------------|--|
| Login URL | <input type="text" value="https://"/> | |
| Azure AD Identifier | <input type="text" value="https://"/> | |
| Logout URL | <input type="text" value="https://"/> | |

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

Assegna utente di Azure AD all'app

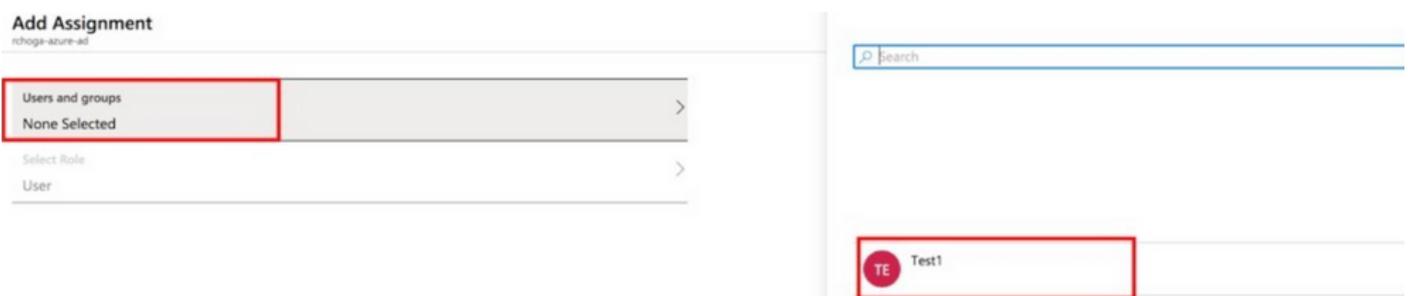
In questa sezione, **Test1** è abilitato per l'uso di Azure Single Sign-On quando si concede l'accesso all'app Cisco AnyConnect.

Passaggio 1. Nella pagina di panoramica dell'app, selezionare **Utenti e gruppi** e quindi **Aggiungi utente**.



The screenshot shows the 'Cisco AnyConnect | Users and groups' page. The left sidebar has 'Users and groups' highlighted. The main area has a '+ Add user' button highlighted. Below it is a table with columns 'Display Name', 'Object Type', and 'Role assigned'. The table is currently empty with the message 'No application assignments found'.

Passaggio 2. Selezionare **Utenti e gruppi** nella finestra di dialogo Aggiungi assegnazione.



The screenshot shows the 'Add Assignment' dialog box. On the left, 'Users and groups' is selected in a dropdown menu. On the right, a search bar is visible, and a user named 'Test1' is highlighted in a list.

Passaggio 3. Nella finestra di dialogo **Aggiungi assegnazione** fare clic sul pulsante **Assegna**.



Configurazione di ASA per SAML tramite CLI

Passaggio 1. Creare un trust point e importare il certificato SAML.

```
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
```

Passaggio 2. Questi comandi eseguono il provisioning del provider di identità SAML.

```
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
```

Passaggio 3. Applica autenticazione SAML a una configurazione tunnel VPN.

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

write memory
```

Nota: Se si apportano modifiche alla configurazione IdP, è necessario rimuovere la configurazione del provider di identità saml dal gruppo di tunnel e riapplicarla per rendere effettive le modifiche.

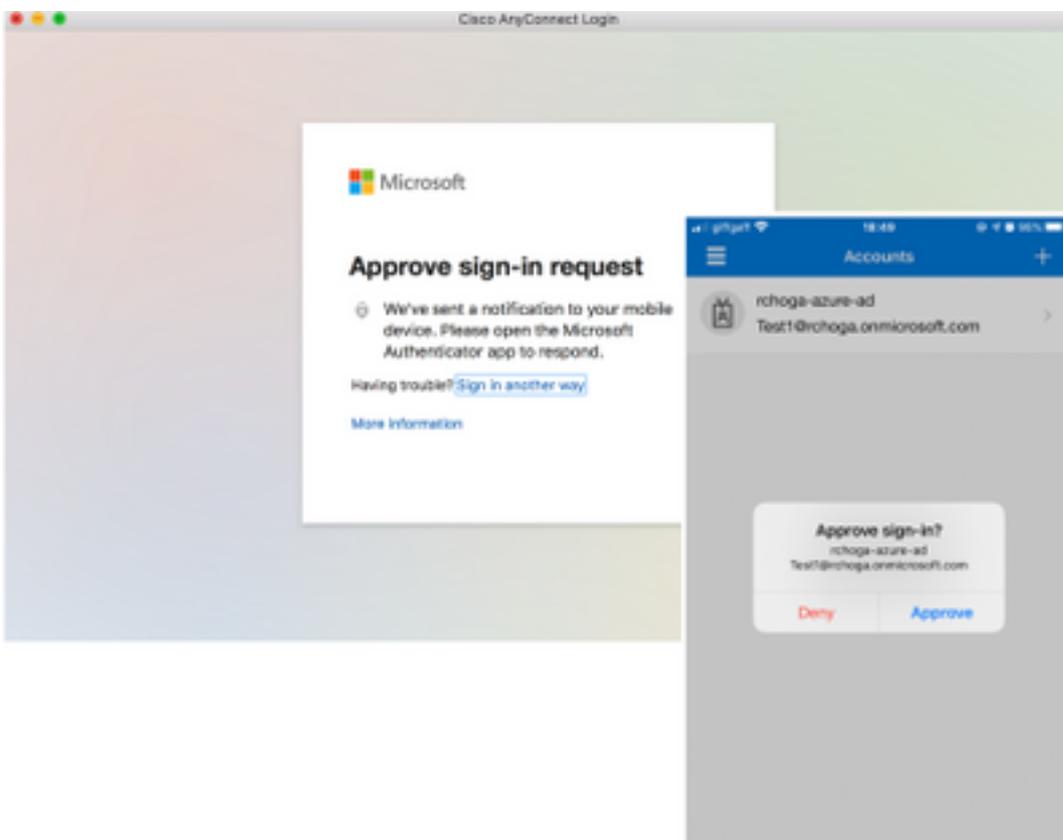
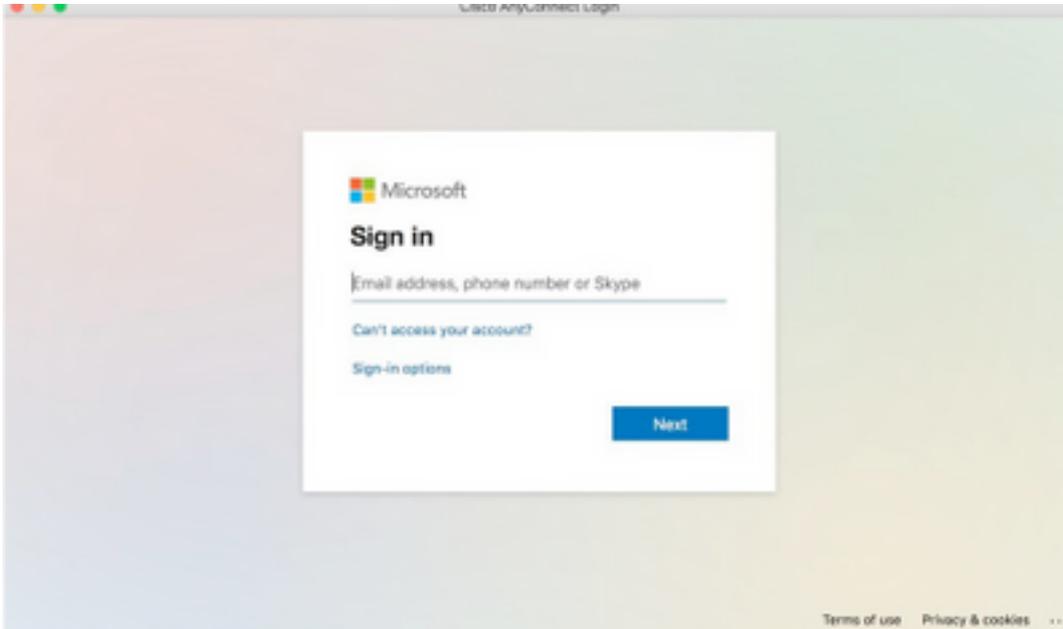
Verifica

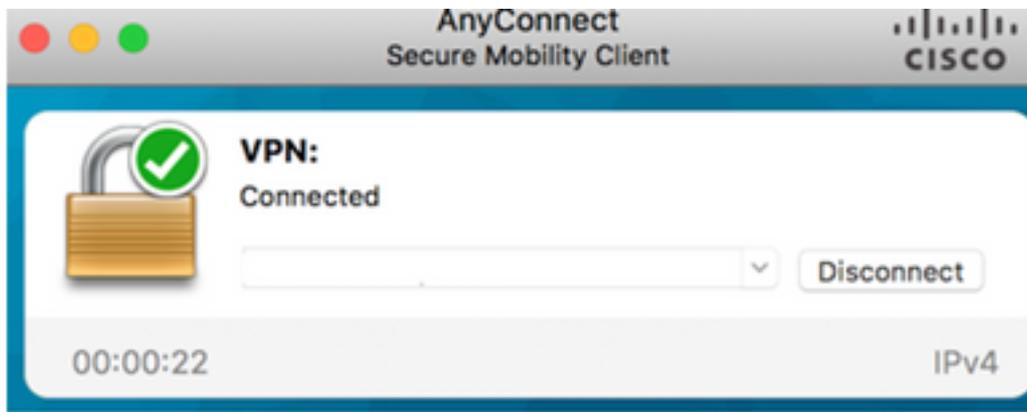
Test di AnyConnect con autenticazione SAML

Passaggio 1. Connettersi all'URL della VPN e immettere i dettagli di accesso ad Azure AD.

Passaggio 2. Approvare la richiesta di accesso.

Passaggio 3. AnyConnect è connesso.





Problemi comuni

ID entità non corrispondente

Esempio di debug:

[SAML] consume_assertion: L'identificatore di un provider è sconosciuto a #LassoServer. Per registrare un provider in un oggetto #LassoServer, è necessario utilizzare i metodi `lasso_server_add_provider()` o `lasso_server_add_provider_from_buffer()`.

Problema: In genere, indica che il comando `saml idp [entityID]` nella configurazione webvpn dell'ASA non corrisponde all'ID entità IdP trovato nei metadati dell'IdP.

Soluzione: Controllare l'ID entità del file di metadati dell'IdP e modificare il comando `saml idp [entity id]` in modo che corrisponda a questo.

Tempo non corrispondente

Esempio di debug:

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

[SAML] consume_assertion: asserzione scaduta o non valida

Problema 1. Ora ASA non sincronizzata con l'ora dell'IdP.

Soluzione 1. Configurare l'ASA con lo stesso server NTP usato da IdP.

Problema 2. Asserzione non valida tra l'ora specificata.

Soluzione 2. Modificare il valore di timeout configurato sull'appliance ASA.

Utilizzato certificato di firma IdP errato

Esempio di debug:

[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=signatures.c:line=493:obj=rsa-sha1:subj=EVP_VerifyFinal:error=18:i dati non corrispondono:la firma non corrisponde

[SAML] consume_assertion: Impossibile verificare una firma sul messaggio

Problema: L'ASA non è in grado di verificare il messaggio firmato dall'IdP o non è presente alcuna firma da verificare per l'ASA.

Soluzione: Controllare il certificato di firma IdP installato sull'appliance ASA per verificare che corrisponda a quanto inviato dall'IdP. Se la risposta è confermata, assicurarsi che la firma sia inclusa nella risposta SAML.

Gruppo di destinatari asserzione non valido

Esempio di debug:

[SAML] consume_assertion: gruppo di destinatari dell'asserzione non valido

Problema: IdP definisce il gruppo di destinatari non corretto.

Soluzione: Correggere la configurazione del gruppo di destinatari nel provider di identità. Deve corrispondere all'ID entità dell'ASA.

URL errato per il servizio consumer di asserzione

Debug di esempio: Impossibile ricevere i debug dopo l'invio della richiesta di autenticazione iniziale. L'utente può immettere le credenziali nell'IdP ma l'IdP non reindirizza all'ASA.

Problema: IdP è configurato per l'URL del servizio consumer di asserzione errato.

Soluzione/i: Verificare l'URL di base nella configurazione e accertarsi che sia corretto. Controllare i metadati ASA con show per verificare che l'URL del servizio consumer di asserzione sia corretto. Per verificarlo, esaminarlo. Se entrambi i metodi sono corretti sull'appliance ASA, controllare l'IdP per verificare che l'URL sia corretto.

Modifiche alla configurazione SAML che non hanno effetto

Esempio: Dopo la modifica o la modifica di un URL Single Sign-On, il certificato SP, SAML non funziona e invia configurazioni precedenti.

Problema: L'appliance ASA deve rigenerare i metadati quando una modifica alla configurazione influisce su di essa. Questa operazione non viene eseguita automaticamente.

Soluzione: Dopo aver apportato le modifiche, nel gruppo di tunnel interessato rimuovere e riapplicare il comando saml idp [entity-id].

Risoluzione dei problemi

La maggior parte delle procedure di risoluzione dei problemi SAML implica una configurazione errata che può essere rilevata quando si controlla la configurazione SAML o si eseguono i debug. debug webvpn saml 255 può essere utilizzato per risolvere la maggior parte dei problemi. tuttavia, in scenari in cui questo debug non fornisce informazioni utili, è possibile eseguire altri debug:

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

Informazioni correlate

- [Single Sign-On SAML per applicazioni locali con proxy di applicazione](#)