Configurazione di più gruppi di tunnel con SAML su ASA

Sommario

Introduzione

In questo documento viene descritta l'autenticazione SAML con Azure Identity Provider per più gruppi di tunnel su Cisco ASA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Adaptive Security Appliance (ASA)
- SAML (Security Assertion Markup Language)
- Certificati SSL (Secure Sockets Layer)
- Microsoft Azure

Componenti usati

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

- ASA 9.2(1)1

- ID Entra di Microsoft Azure con SAML 2.0
- Cisco Secure Client 5.1.7.80

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

Microsoft Azure può supportare più applicazioni per lo stesso ID entità. Ogni applicazione (mappata a un gruppo di tunnel diverso) richiede un certificato univoco. Sull'appliance ASA, è possibile configurare più gruppi di tunnel per usare applicazioni protette con Override Identity Provider (IdP) diverse a causa della funzionalità del certificato IdP. Questa funzionalità consente agli amministratori di eseguire l'override del certificato IdP primario nell'oggetto server Single Sign-On (SSO) con un certificato IdP specifico per ogni gruppo di tunnel. Questa funzione è stata introdotta sull'appliance ASA a partire dalla versione 9.17.1.

SSO avviato da SP SAML

Quando l'utente finale avvia l'accesso tramite l'appliance ASA, il comportamento dell'accesso procede come segue:

1. Quando l'utente VPN accede o sceglie un gruppo di tunnel abilitato SAML, viene reindirizzato all'ID SAML per l'autenticazione. Se l'utente non accede direttamente all'URL del gruppo, viene visualizzato un messaggio che indica che il reindirizzamento non è attivo.

2. L'ASA genera una richiesta di autenticazione SAML che il browser reindirizza all'IdP SAML.

3. L'IdP richiede all'utente finale le credenziali e l'utente finale esegue l'accesso. Le credenziali immesse devono soddisfare la configurazione di autenticazione IdP.

4. La risposta dell'IdP viene inviata nuovamente al browser e inviata all'URL di accesso all'ASA. L'ASA verifica la risposta per completare l'accesso.

Configurazioni

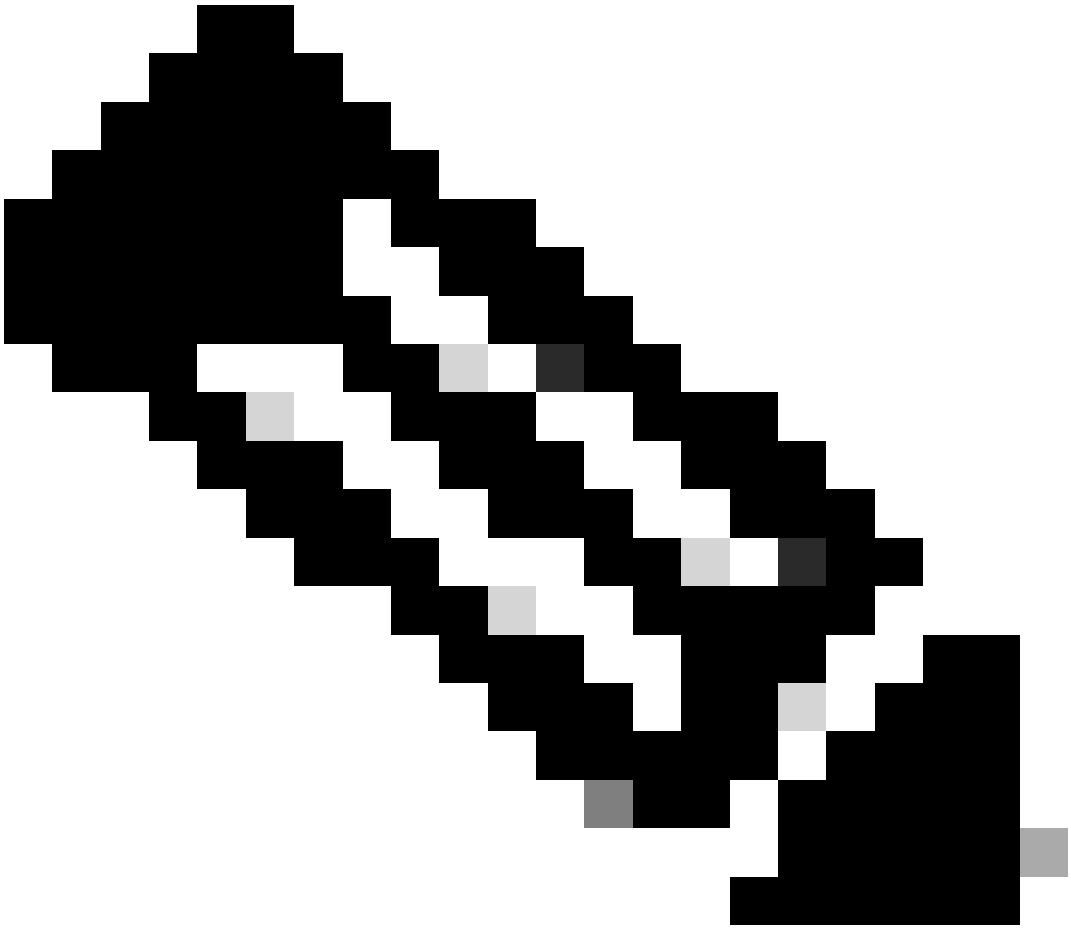
Aggiungi Cisco Secure Firewall - Secure Client dalla raccolta

In questo esempio, viene aggiunta l'integrazione Microsoft Entra SSO con Cisco Secure Firewall - Secure Client in Azure per due gruppi di tunnel configurati su ASA:

- SAML1
- SAML2

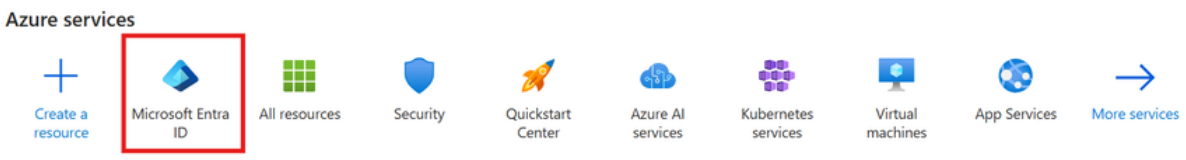
Per configurare l'integrazione di Cisco Secure Firewall - Secure Client in Microsoft Entra ID, è

necessario aggiungere Cisco Secure Firewall - Secure Client dalla raccolta all'elenco di app SaaS gestite.



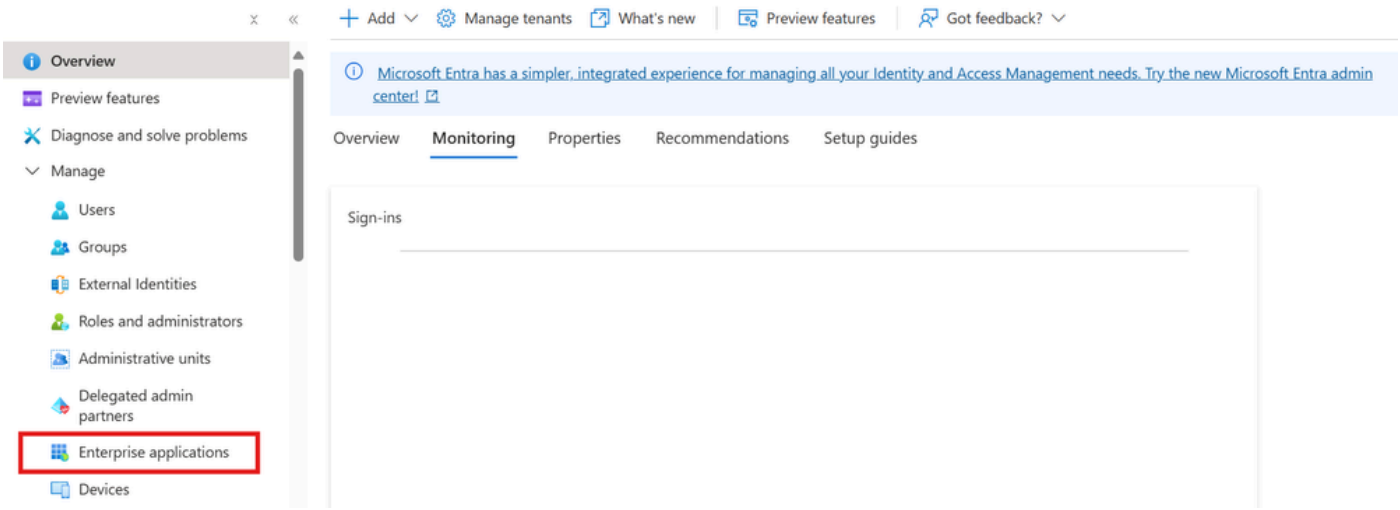
Nota: La procedura descritta di seguito consente di aggiungere Cisco Secure Firewall - Secure Client alla raccolta per il primo gruppo di tunnel, SAML1.

Passaggio 1. Accedere al portale di Azure e scegliere Microsoft Entra ID.



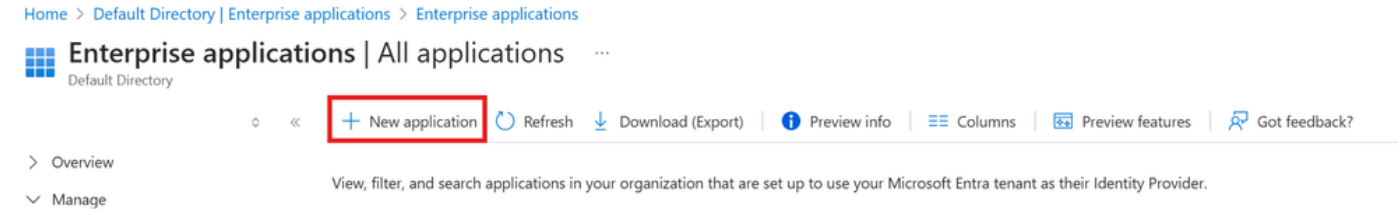
ID Entra Microsoft

Passaggio 2. Come mostrato in questa immagine, scegliere Applicazioni enterprise.



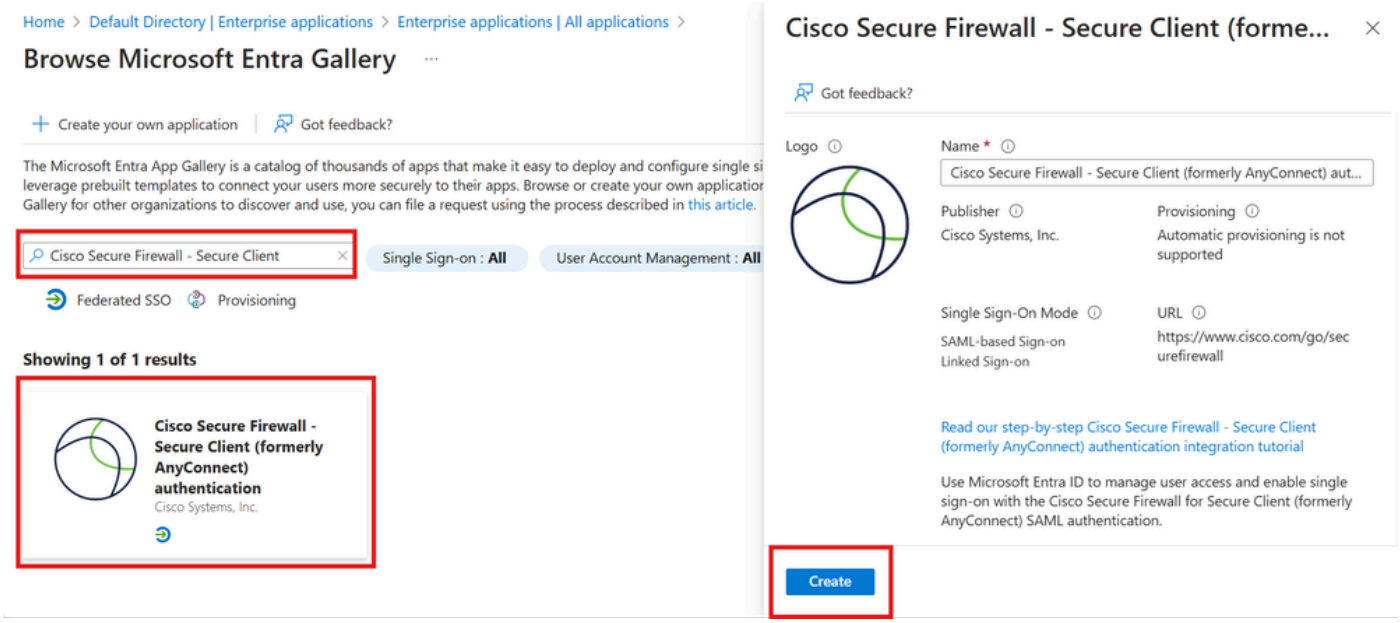
Applicazione aziendale

Passaggio 3. Scegliere Nuova applicazione, come mostrato nell'immagine.

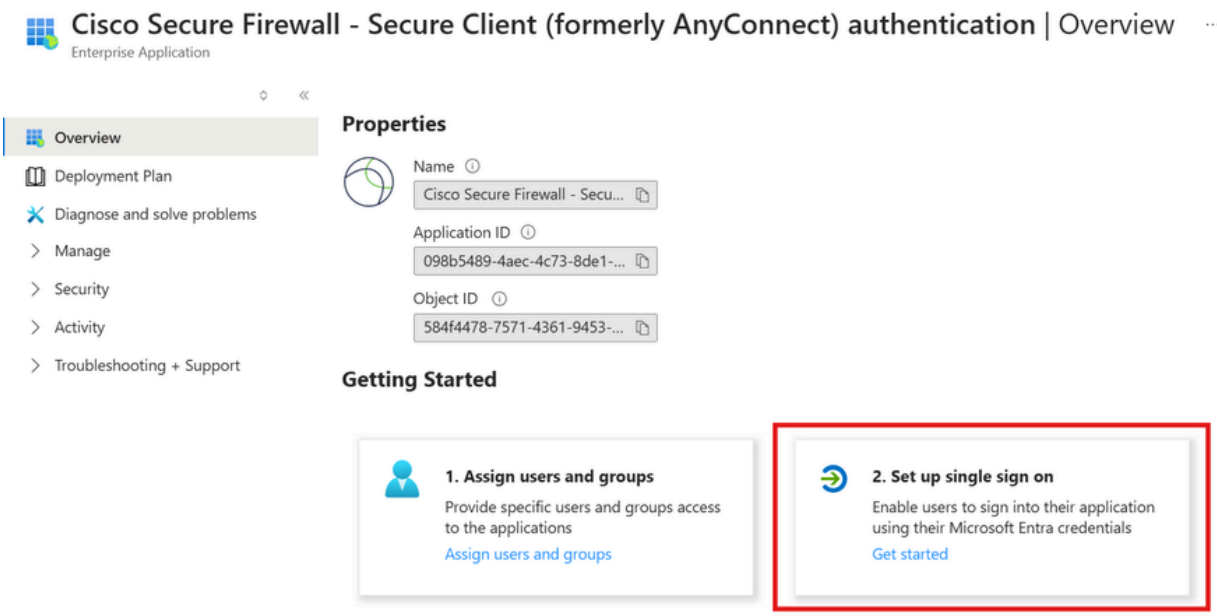


Nuova applicazione

Passaggio 4. Nella sezione Aggiungi dalla raccolta, digitare Cisco Secure Firewall - Secure Client nella casella di ricerca, scegliere Cisco Secure Firewall - Secure Client dal pannello dei risultati, quindi aggiungere l'app.

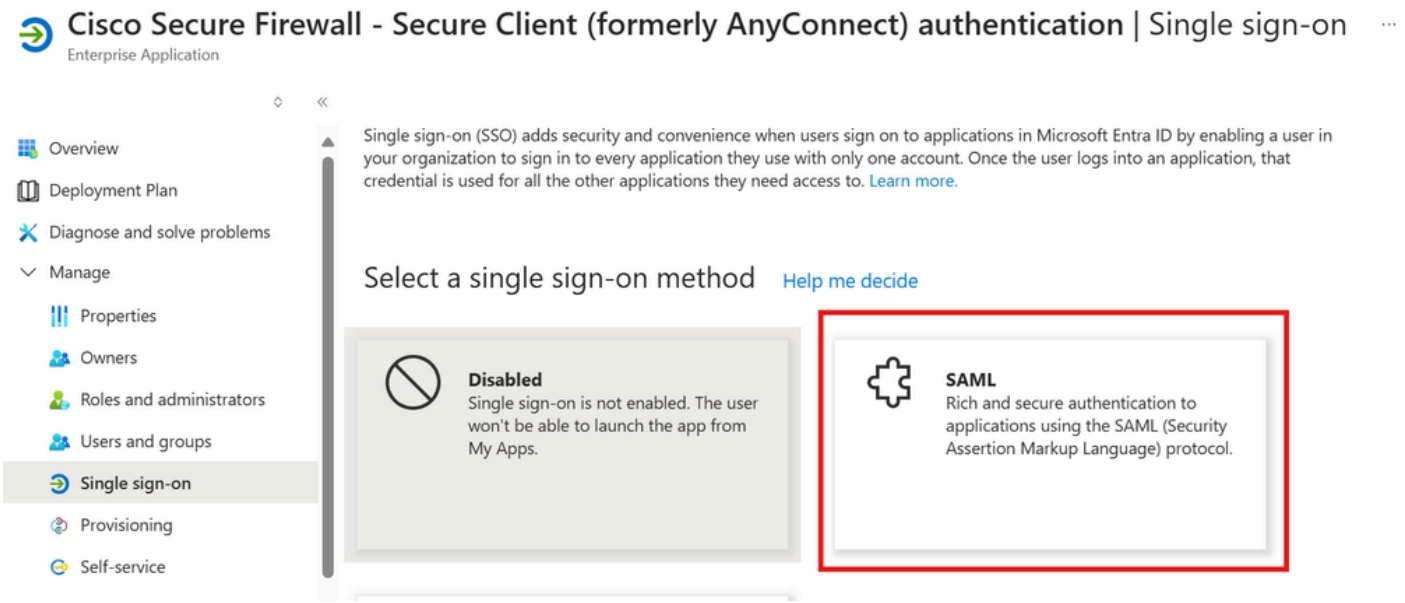


Passaggio 5. Scegliere la voce di menu Single Sign-on, come illustrato in questa immagine.



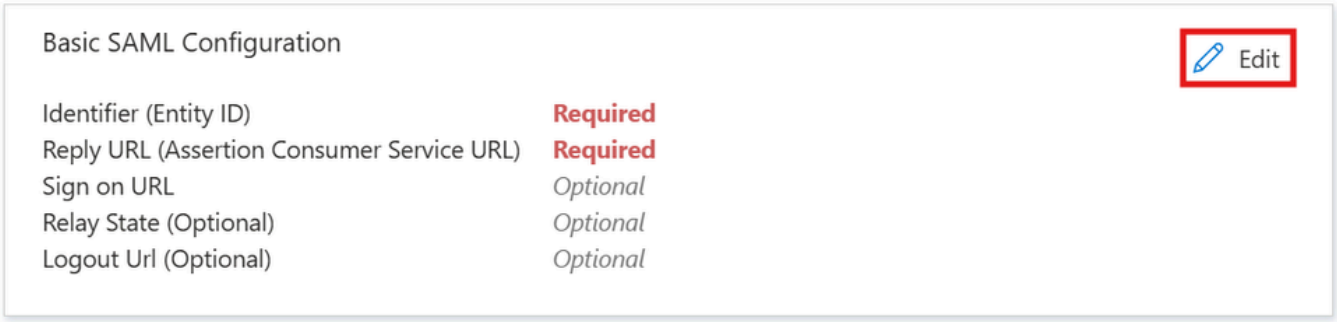
Configura Single Sign-On

Passaggio 6. Nella pagina Selezionare un metodo Single Sign-On, scegliere SAML.



SAML

Passaggio 7. Nella pagina Configurazione del servizio Single Sign-on con SAML, fare clic sull'icona Modifica/Apri per Configurazione SAML di base per modificare le impostazioni.



Configurazione Saml Di Base

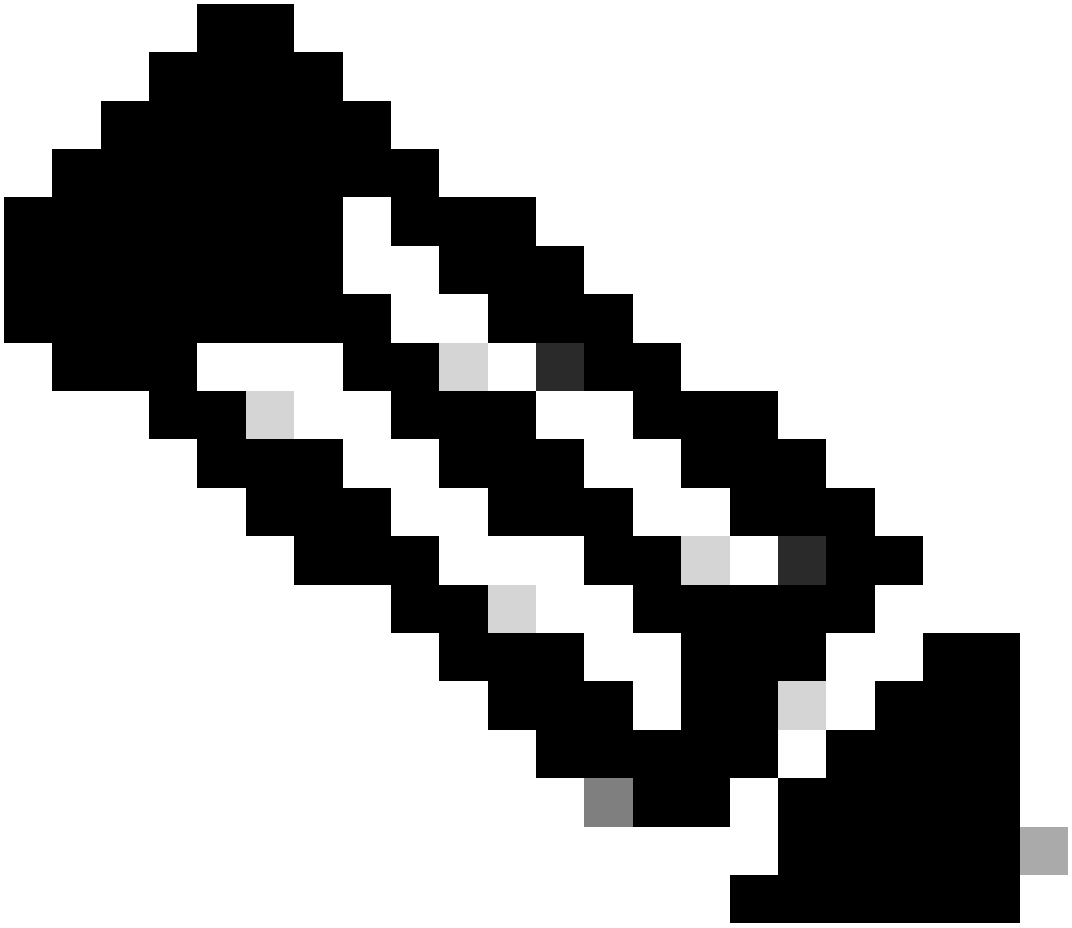
Passaggio 8. Nella pagina Imposta servizio Single Sign-on con SAML immettere i valori nei campi seguenti:

r. Nella casella di testo Identificatore digitare un URL utilizzando il modello seguente:

https://<URL VPN>/saml/sp/metadata/<Nome_Gruppo_Tunnel>

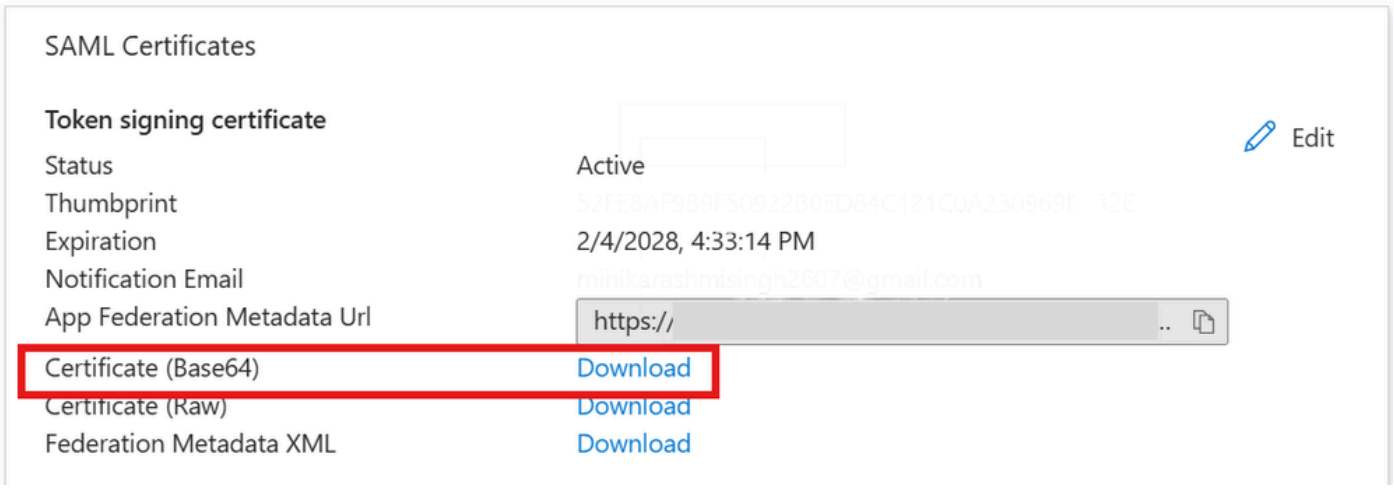
b. Nella casella di testo URL di risposta digitare un URL utilizzando il modello seguente:

https://<URL VPN>/+CSCOE+/saml/sp/acs?tgname=<Nome_Gruppo_Tunnel>
[Nome_Gruppo_Tunnel = SAML1]

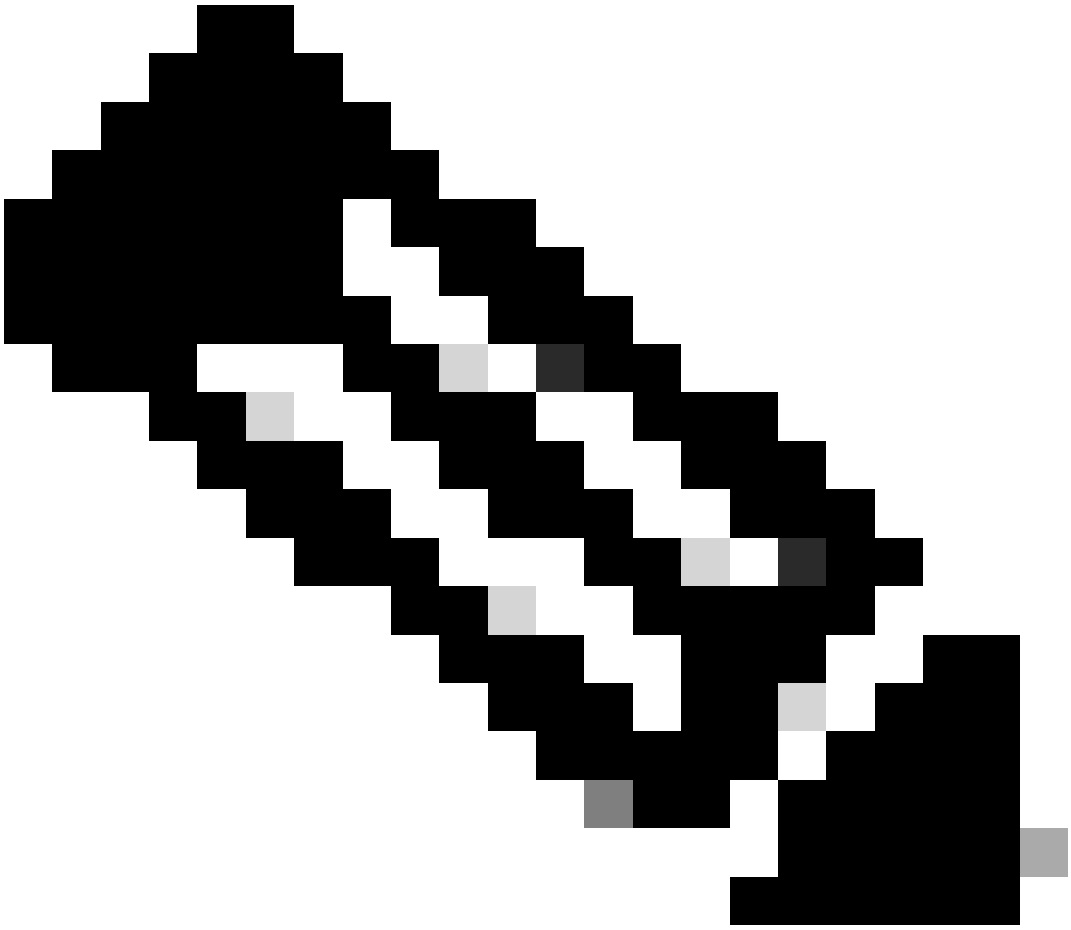


Nota: Tunnel_Group_Name fa distinzione tra maiuscole e minuscole e il valore non deve contenere punti '.' e barra '/'.

Passaggio 9. Nella sezione Certificato di firma SAML della pagina Configurazione del servizio Single Sign-on con SAML individuare Certificate (Base64) e scegliere Download per scaricare il file del certificato e salvarlo nel computer.



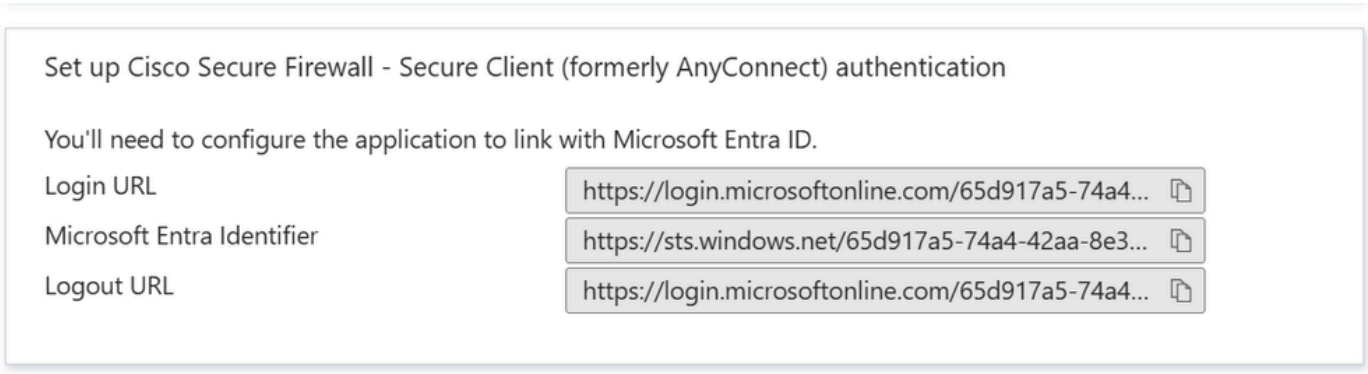
Download certificato (Base64)



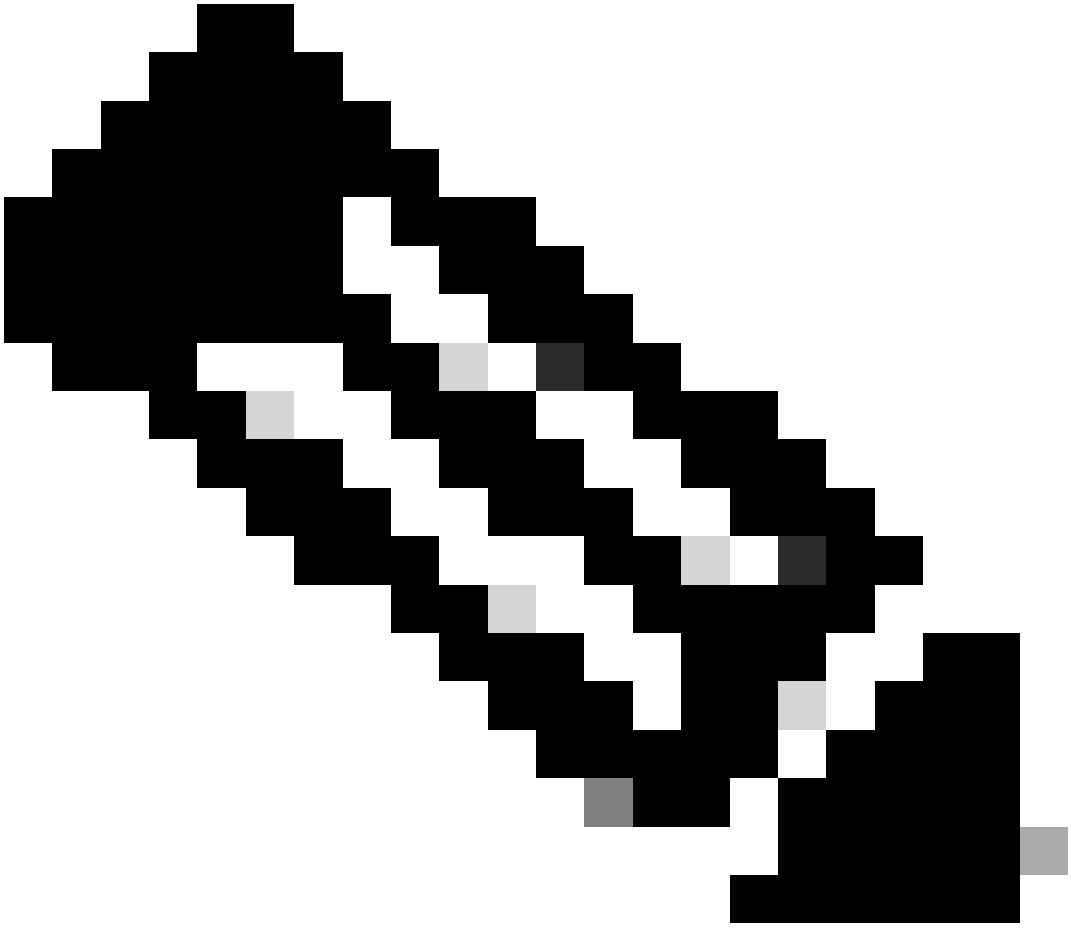
Nota: il certificato scaricato viene importato nel trust ASA AzureAD-AC-SAML1. Per ulteriori informazioni, vedere la sezione Configurazione ASA.

Passaggio 10. Nella sezione Configurazione di Cisco Secure Firewall - Client sicuro, copiare gli URL appropriati in base ai requisiti dell'utente. Questi URL vengono utilizzati per configurare l'oggetto server SSO sull'appliance ASA.

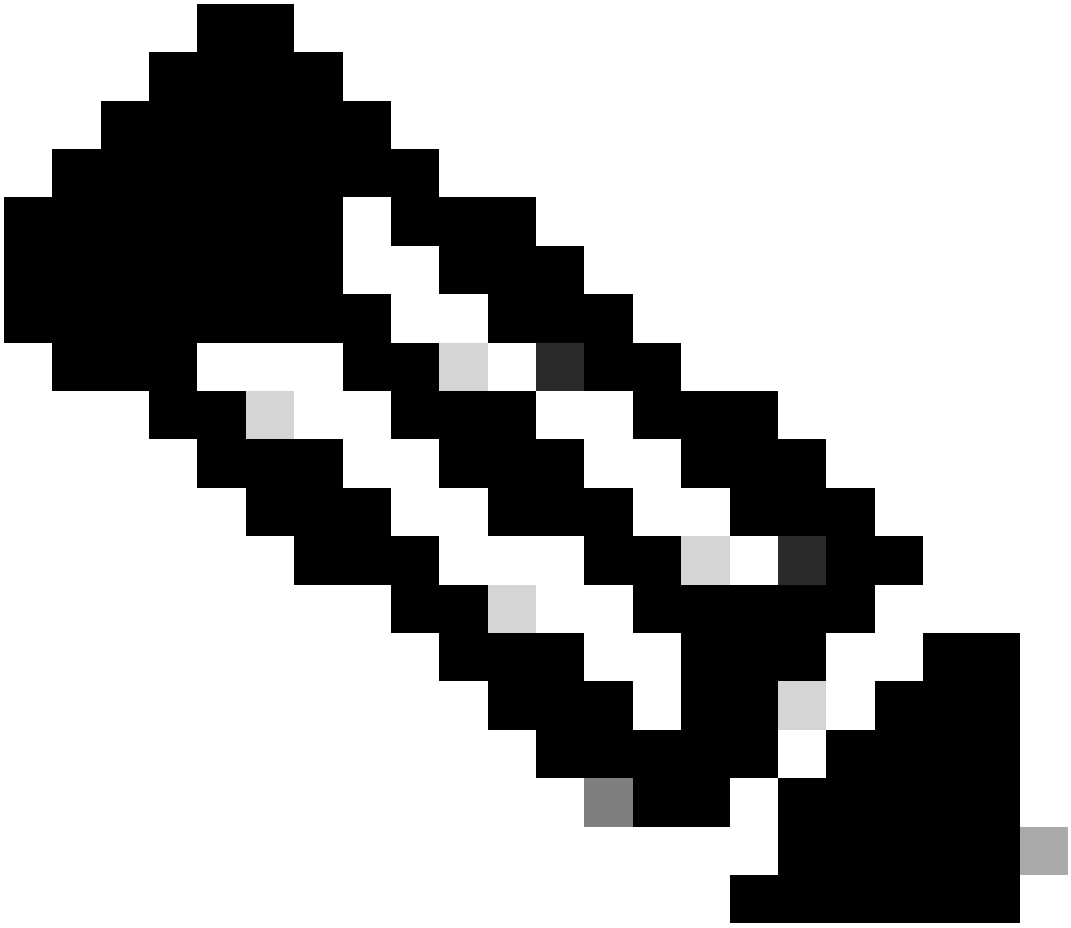
- Microsoft Entra Identifier - Si tratta dell'idp SAML nella configurazione VPN.
- Login URL: l'URL di accesso.
- Logout URL: l'URL di disconnessione.



URL SSO



Nota: Ripetere i passaggi di configurazione precedenti per aggiungere l'app Cisco Secure Firewall - Secure Client dalla raccolta per il secondo gruppo di tunnel. Il secondo nome di gruppo di tunnel in questo caso è SAML2.



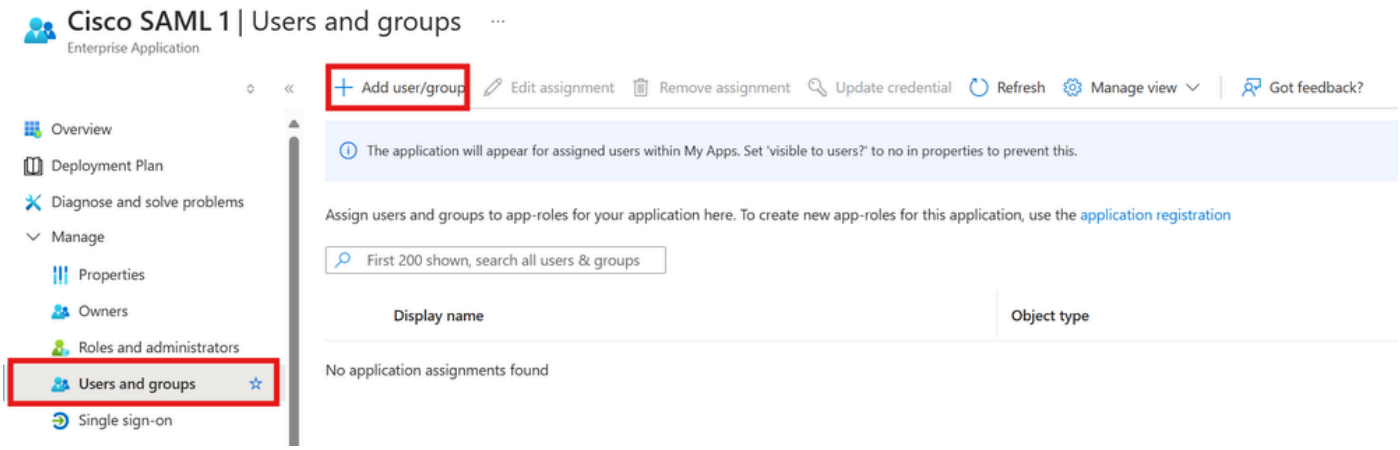
Nota: durante l'aggiunta dell'app Cisco Secure Firewall - Secure Client per il secondo gruppo di tunnel (SAML 2), il certificato di Azure scaricato nel passaggio 8. viene importato nel trust ASA AzureAD-AC-SAML2.

Assegna utenti di Azure AD all'app

In questa sezione, Test1 e Test2 sono abilitati per l'utilizzo di Azure SSO quando si concede l'accesso all'app Cisco Secure Client.

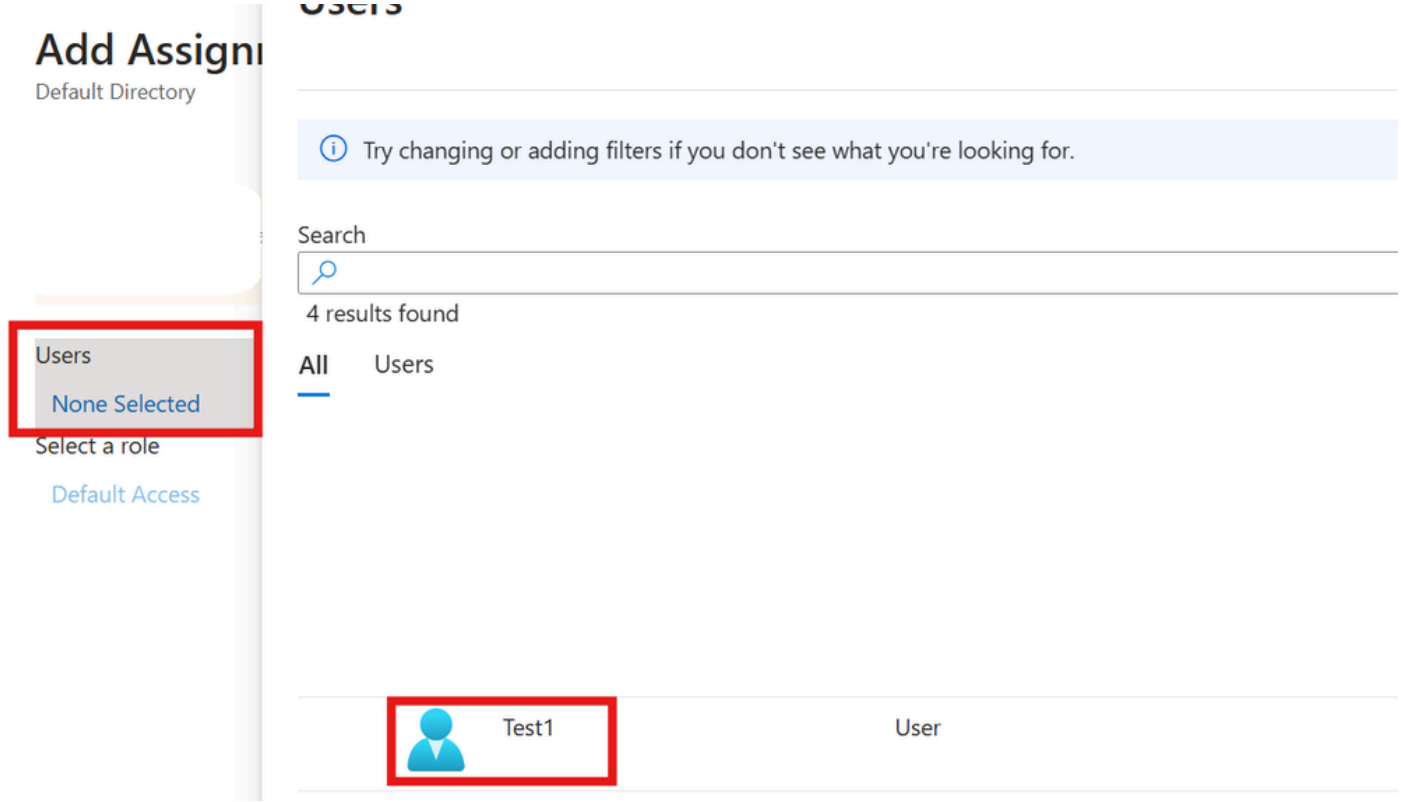
Per la prima applicazione IdP:

Passaggio 1. Nella prima pagina di panoramica dell'applicazione IdP, scegliere Utenti e gruppi, quindi Aggiungi utente.



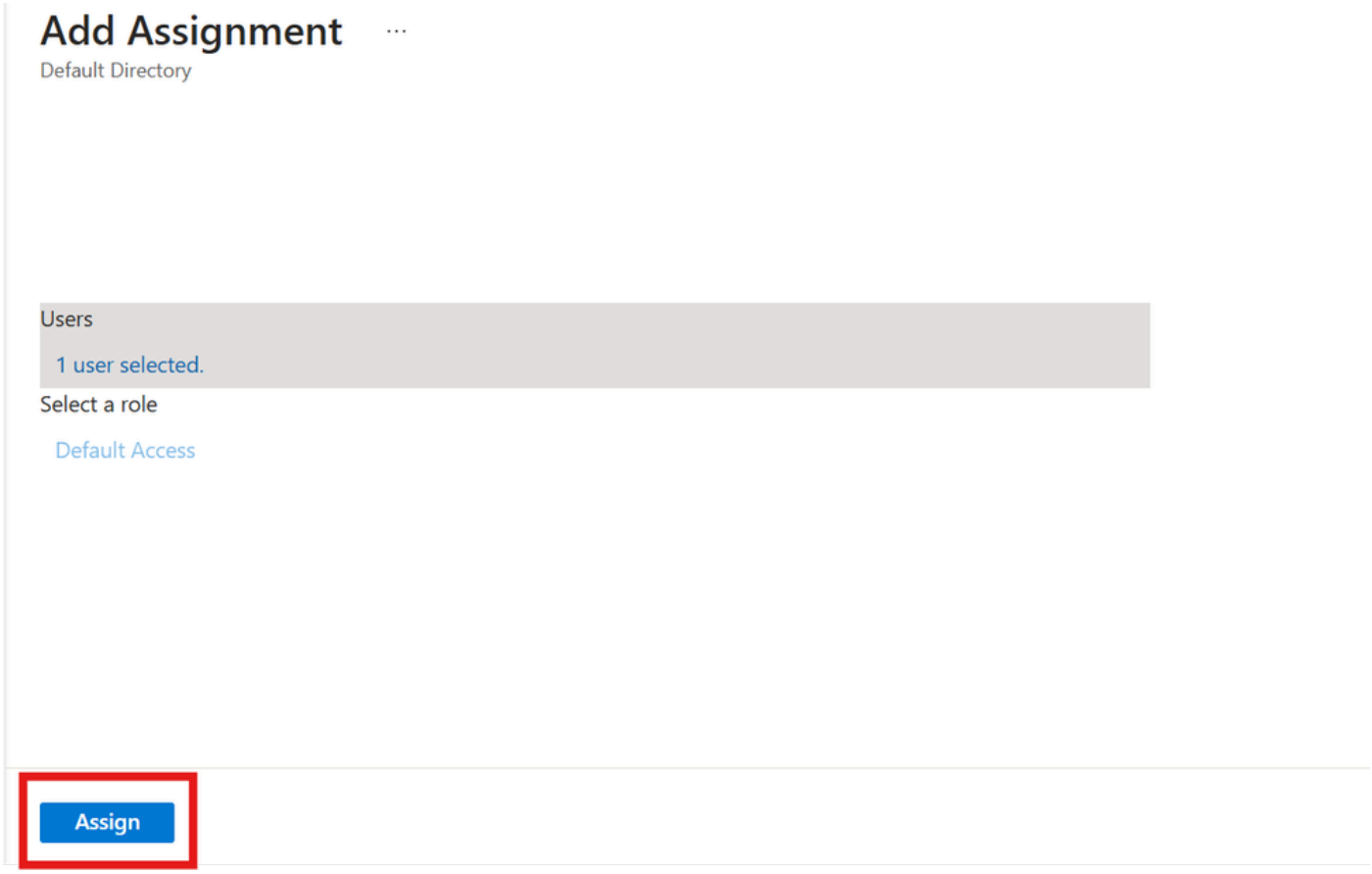
Utenti e gruppi

Passaggio 2. Scegliere Utenti o gruppi nella finestra di dialogo Aggiungi assegnazione.



Aggiungi assegnazione 1

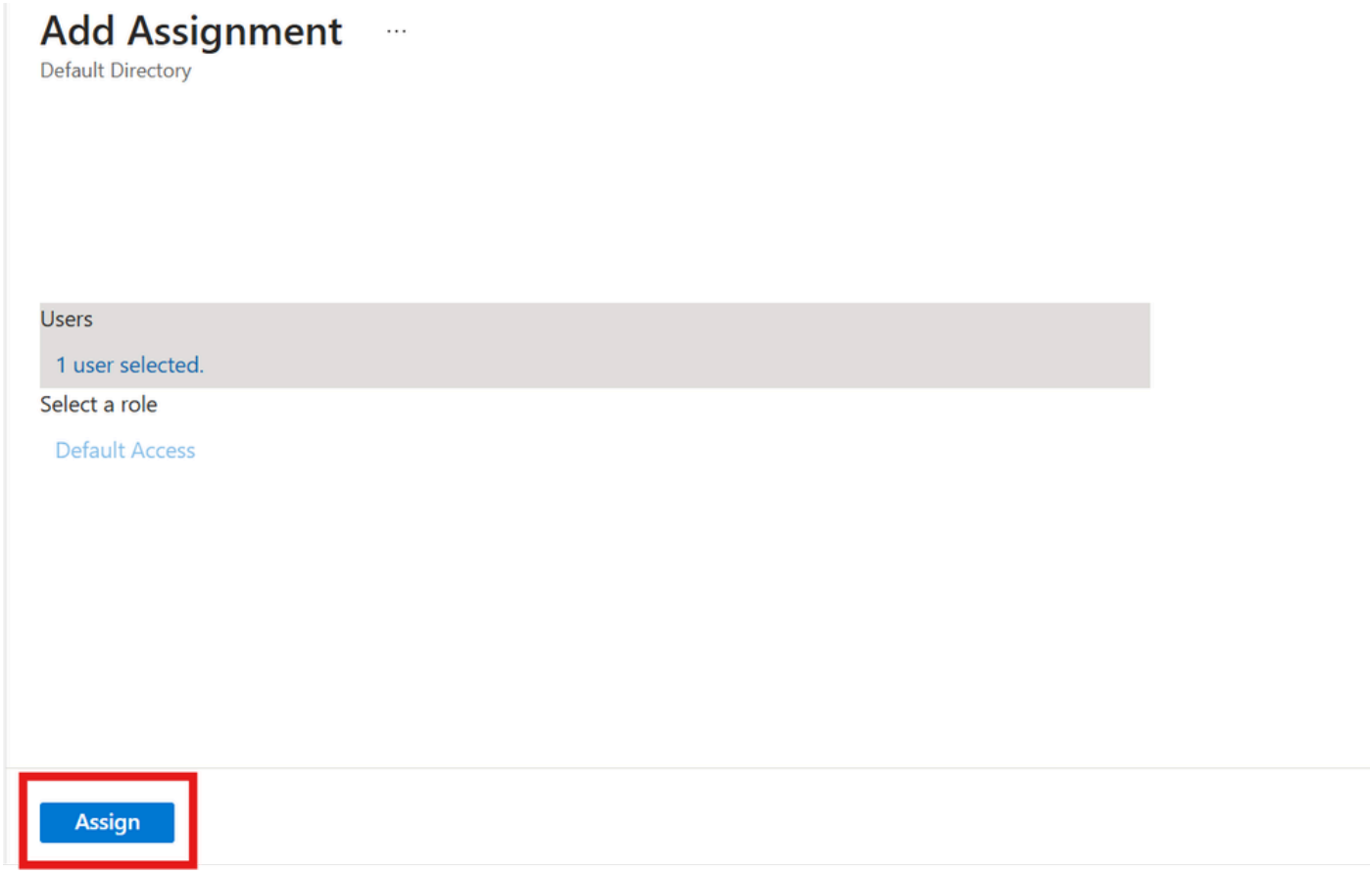
Passaggio 3. Nella finestra di dialogo Add Assignment (Aggiungi assegnazione), fare clic sul pulsante Assign (Assegna).



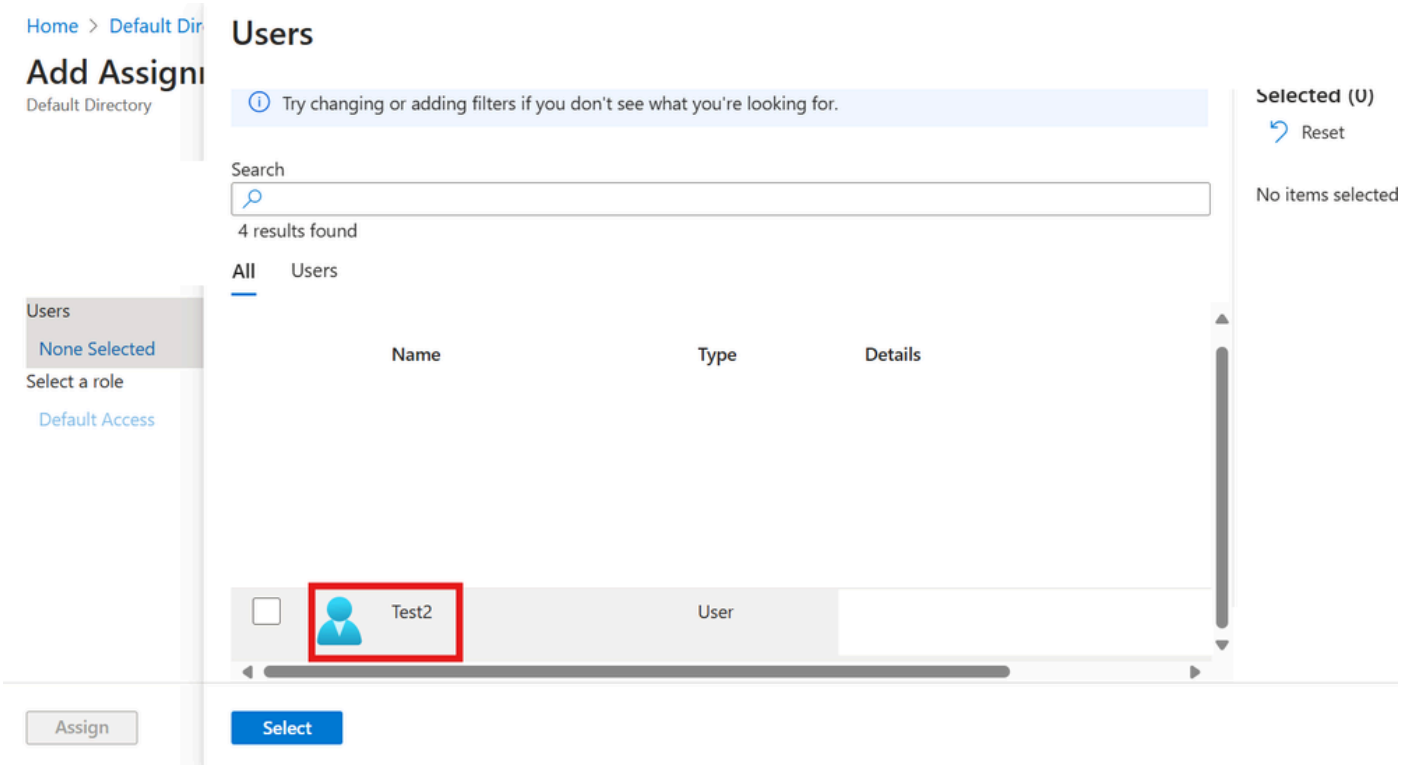
Test1 Assegnazione utente

Per la seconda applicazione IdP:

Ripetere i passaggi precedenti per la seconda applicazione Idp come mostrato in queste immagini.

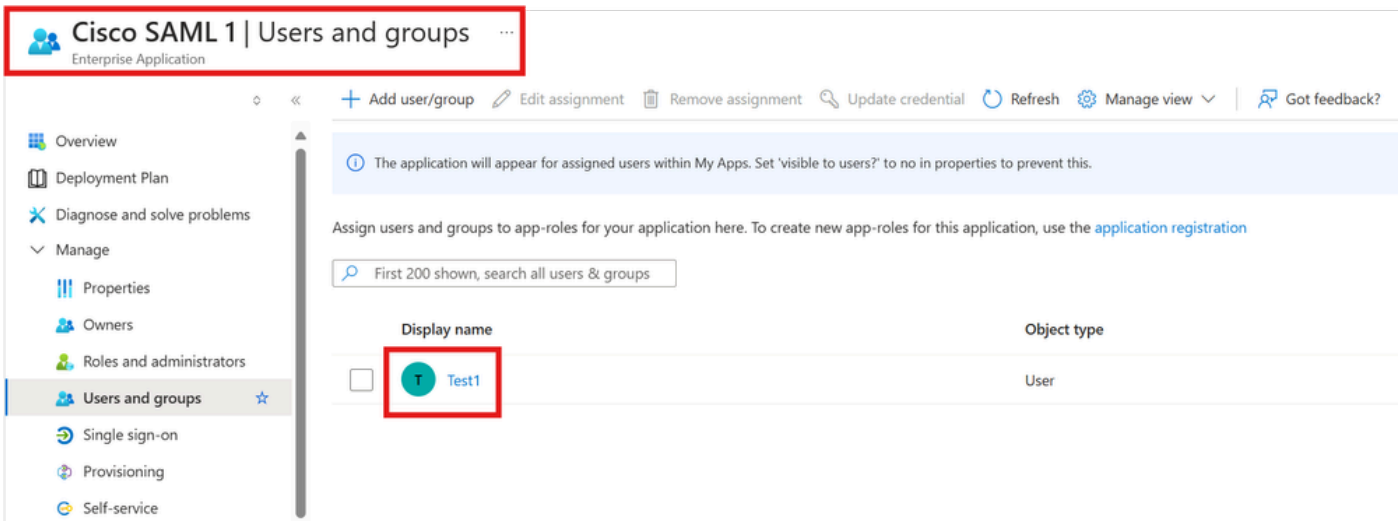


Aggiungi assegnazione 2



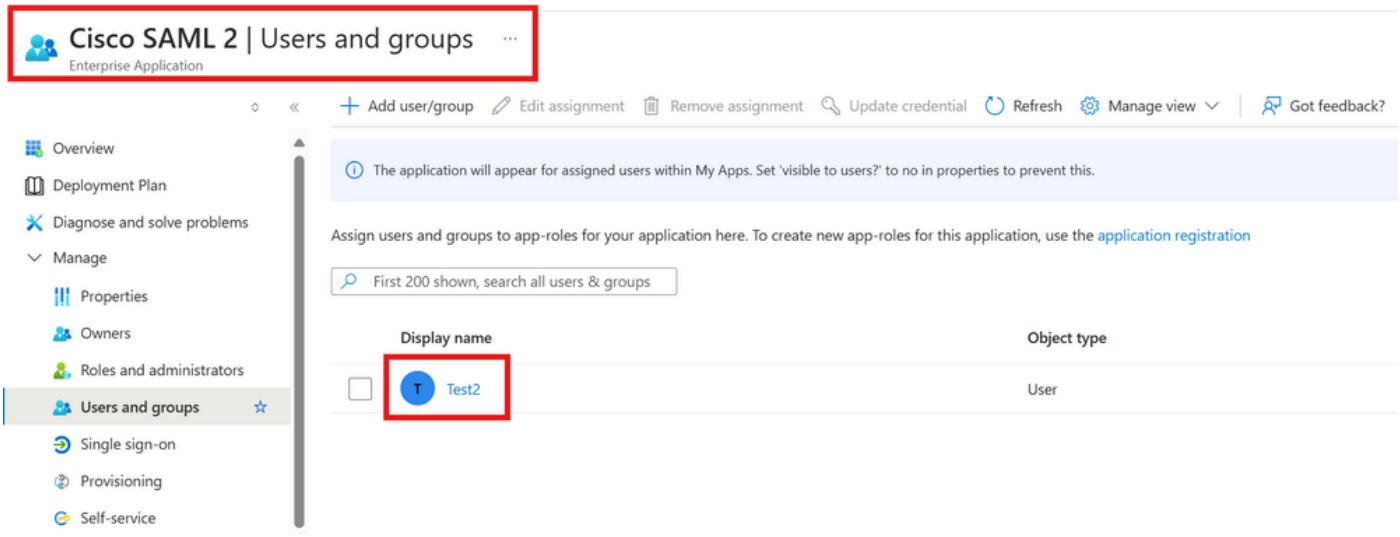
Test2 Assegnazione utente

Assegnazione utente Test1:



Test 1 assegnazione utente

Assegnazione utente Test2:



Test 2 assegnazione utenti

Configurazione ASA tramite CLI

Passaggio 1. Creare punti di fiducia e importare certificati SAML.

Configurare due trust point e importare i rispettivi certificati SAML per ogni gruppo di tunnel.

<#root>

```
config t

 crypto ca trustpoint
```

AzureAD-AC-SAML1

```
   revocation-check none
   no id-usage
   enrollment terminal
```

```
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML1

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit

!
!

crypto ca trustpoint
```

AzureAD-AC-SAML2

```
   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML2

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit
```

Passaggio 2. Configurare il provider di identità SAML.

Utilizzare questi comandi per eseguire il provisioning delle impostazioni del provider di identità SAML.

```
webvpn

 saml idp https://xxx.windows.net/xxxxxxxxxxxx/ - [Azure AD Identifier]
 url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
 url sign-out https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2  - [Logout URL]
 trustpoint idp AzureAD-AC-SAML1 - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

Passaggio 3. Applicare l'autenticazione SAML al primo gruppo di tunnel VPN.

Configurare il gruppo di tunnel SAML1 con il trust point AzureAD-AC-SAML1 IdP.

<#root>

```
tunnel-group SAML1 webvpn-attributes
authentication saml
group-alias SAML1 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML1 <---- Overrides the primary IDP certificate in the Single Sign-On (

Passaggio 4. Applicare l'autenticazione SAML al secondo gruppo di tunnel VPN.

Configurare il gruppo di tunnel SAML2 con il trust point AzureAD-AC-SAML2 IdP.

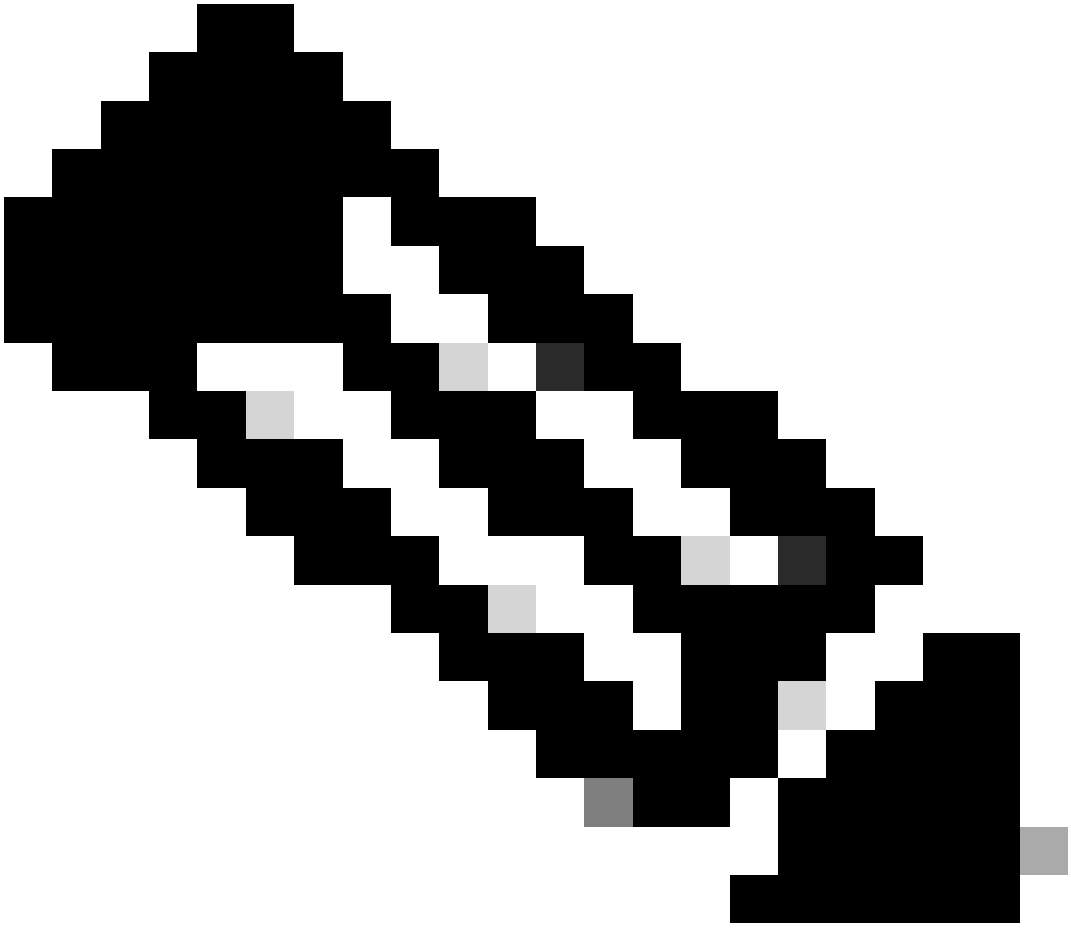
<#root>

```
tunnel-group SAML2 webvpn-attributes
authentication saml
group-alias SAML2 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML2 <---- Overrides the primary IDP certificate in the Single Sign-On (

Passaggio 5: Salvare la configurazione.

```
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 il log nei dettagli di Azure AD.

Passaggio 2. (Facoltativo) Approvare la richiesta di accesso.

Passaggio 3. AnyConnect è connesso.

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 quando vengono eseguiti i debug. debug webvpn saml 255 può essere usato per risolvere la maggior parte dei problemi. tuttavia, negli 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

- Configurazione di ASA AnyConnect VPN con l'autenticazione a più fattori (MFA) di Microsoft Azure tramite SAML
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).