Meervoudige tunnelgroepen configureren met SAML op ASA

Inhoud

Inleiding

Dit document beschrijft SAML-verificatie met Azure Identity Provider voor meerdere tunnelgroepen op Cisco ASA.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Adaptieve security applicatie (ASA)
- Security Assertion Markup Language (SAML)
- Secure Socket Layer (SSL)-certificaten
- Microsoft Azure

Gebruikte componenten

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

- ASA 9.22(1)1
- Microsoft Azure Entra ID met SAML 2.0

- Cisco Secure-client 5.1.7.80

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

Microsoft Azure kan meerdere toepassingen ondersteunen voor dezelfde entiteit-ID. Elke toepassing (in kaart gebracht aan een verschillende tunnelgroep) vereist een uniek certificaat. Bij ASA kunnen meerdere tunnelgroepen worden geconfigureerd om verschillende door Identity Provider (IDP) beschermde toepassingen te gebruiken vanwege de functie voor IDP-certificaat. Deze eigenschap staat beheerders toe om het primaire IDp certificaat in het Single Sign-On (SSO) Server-object met een specifiek IDP-certificaat voor elke tunnelgroep met voeten te treden. Deze functie werd vanaf versie 9.17.1 op ASA geïntroduceerd.

Door SAML SP geïnitieerde SSO

Wanneer de eindgebruiker inlogt door toegang te krijgen tot de ASA, gaat het inloggedrag als volgt te werk:

1. Wanneer de VPN-gebruiker een tunnelgroep met SAML-enabled benadert of kiest, wordt de eindgebruiker omgeleid naar de SAML IDP voor verificatie. De gebruiker wordt gevraagd, tenzij de gebruiker de groep-url direct benadert, in welk geval de omleiding stil is.

2. De ASA genereert een SAML-verificatieaanvraag, die door de browser wordt doorgestuurd naar de SAML-idP.

3. De IDp daagt de eindgebruiker uit voor referenties en de eindgebruiker inlogt. De ingevoerde referenties moeten voldoen aan de configuratie van de IDp-verificatie.

4. De IDp-respons wordt teruggestuurd naar de browser en gepost aan de ASA aanmelding-URL. ASA verifieert de reactie om de login te voltooien.

Configuraties

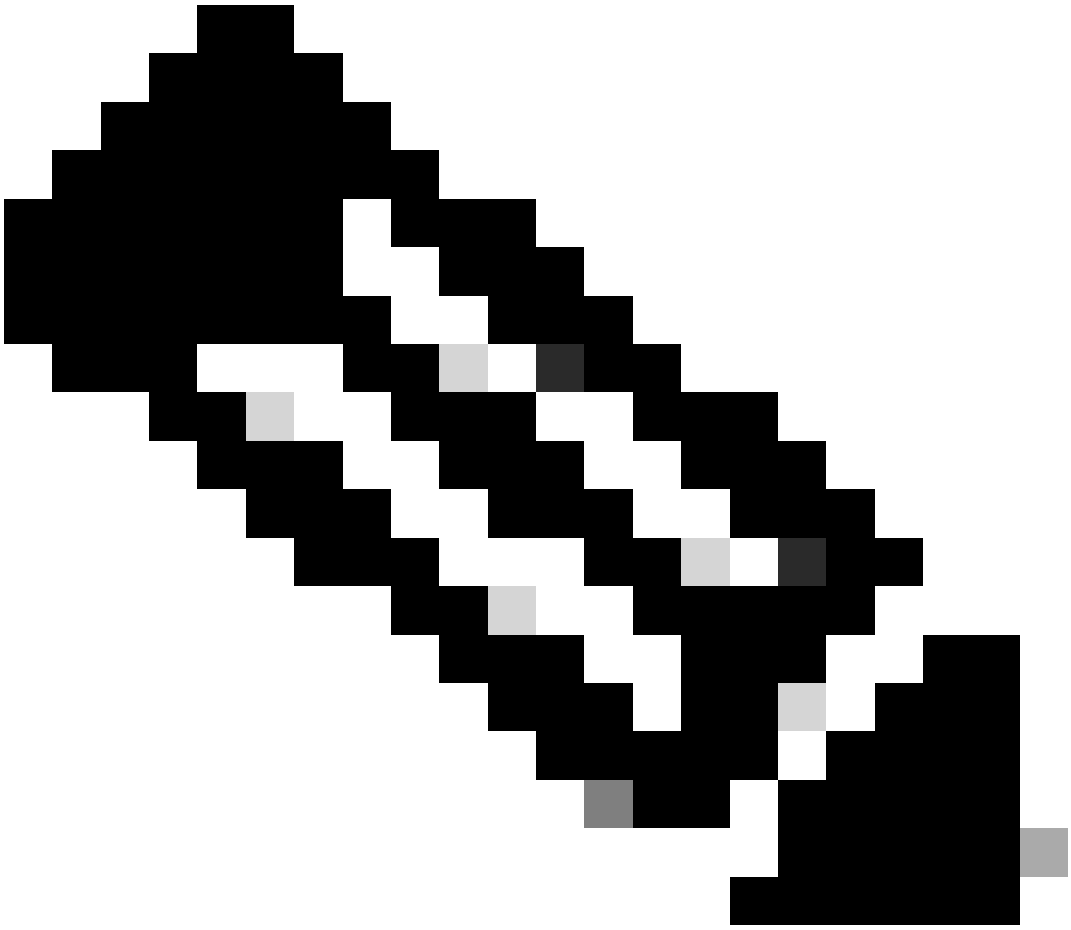
Cisco Secure Firewall toevoegen - beveiligde client uit de galerij

In dit voorbeeld wordt de integratie van Microsoft Entra SSO met Cisco Secure Firewall - Secure Client on Azure toegevoegd voor twee tunnelgroepen die op ASA zijn geconfigureerd:

- SAML1
- SAML2

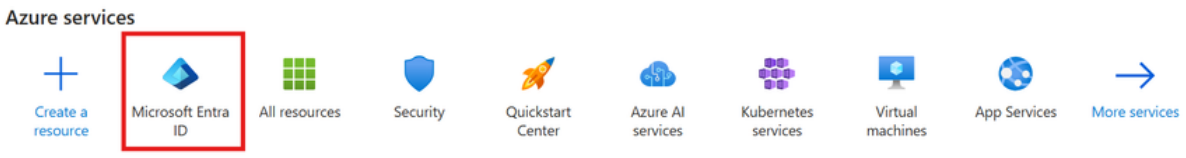
Om de integratie van Cisco Secure Firewall - Secure Client in Microsoft Entra ID te kunnen

configureren, moet u Cisco Secure Firewall - Secure Client uit de galerij toevoegen aan uw lijst met beheerde SaaS-apps.



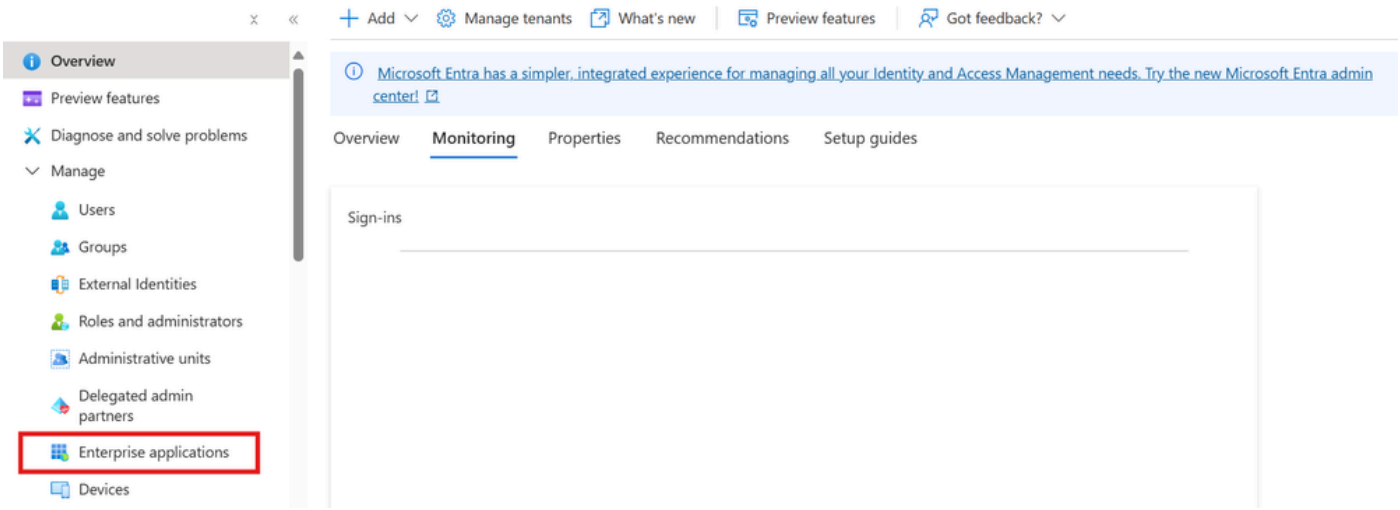
Opmerking: Deze stappen zijn voor het toevoegen van Cisco Secure Firewall - Secure Client aan de galerij voor de eerste tunnelgroep, SAML1.

Stap 1. Meld u aan bij Azure Portal en kies Microsoft Entra ID.



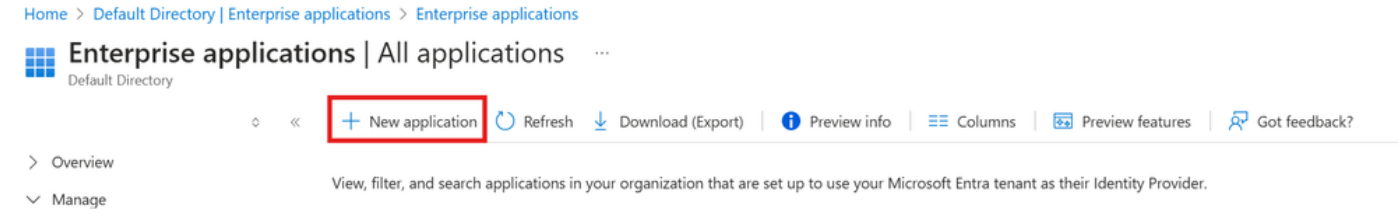
Microsoft Entra ID

Stap 2. Kies Enterprise Application zoals in deze afbeelding wordt getoond.



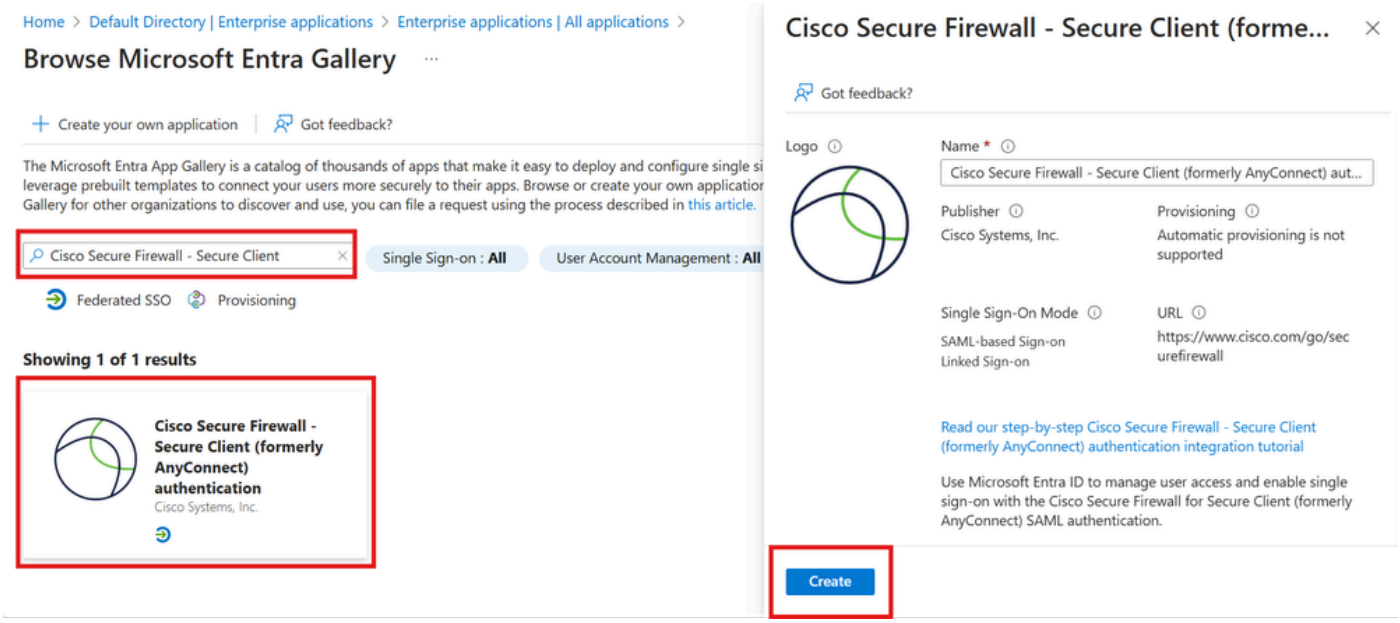
Enterprise-toepassing

Stap 3. Kies nu Nieuwe toepassing, zoals in deze afbeelding.

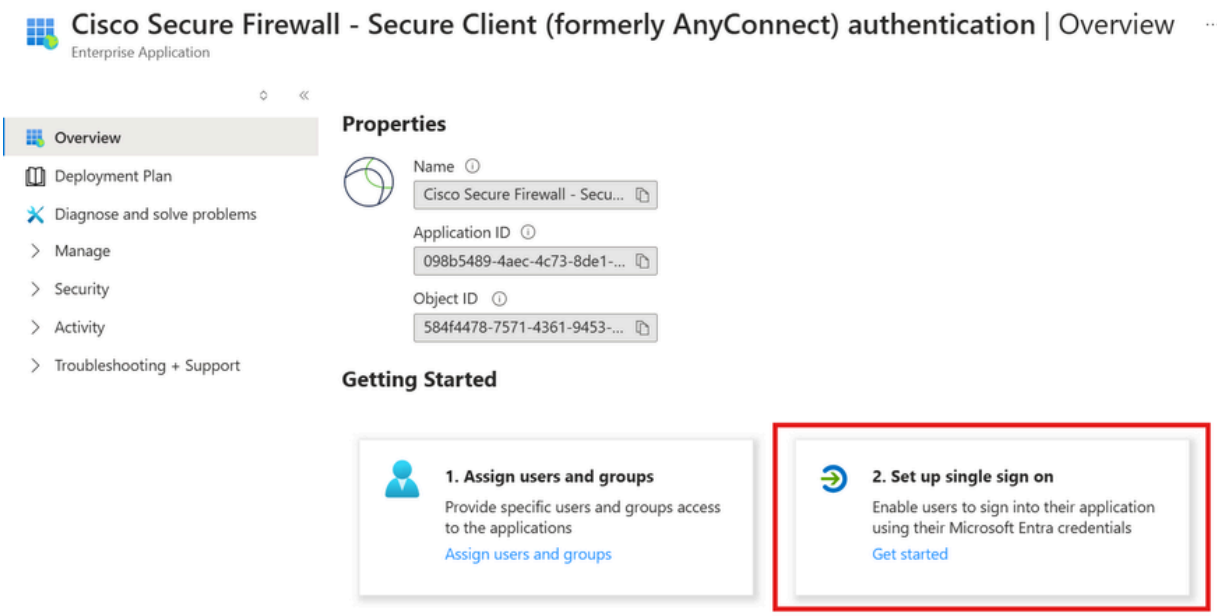


Nieuwe toepassing

Stap 4. In de sectie Toevoegen uit de galerij typt u Cisco Secure Firewall - Secure Client in het zoekvak, kiest u Cisco Secure Firewall - Secure Client in het resultatenpaneel en voegt u de app toe.

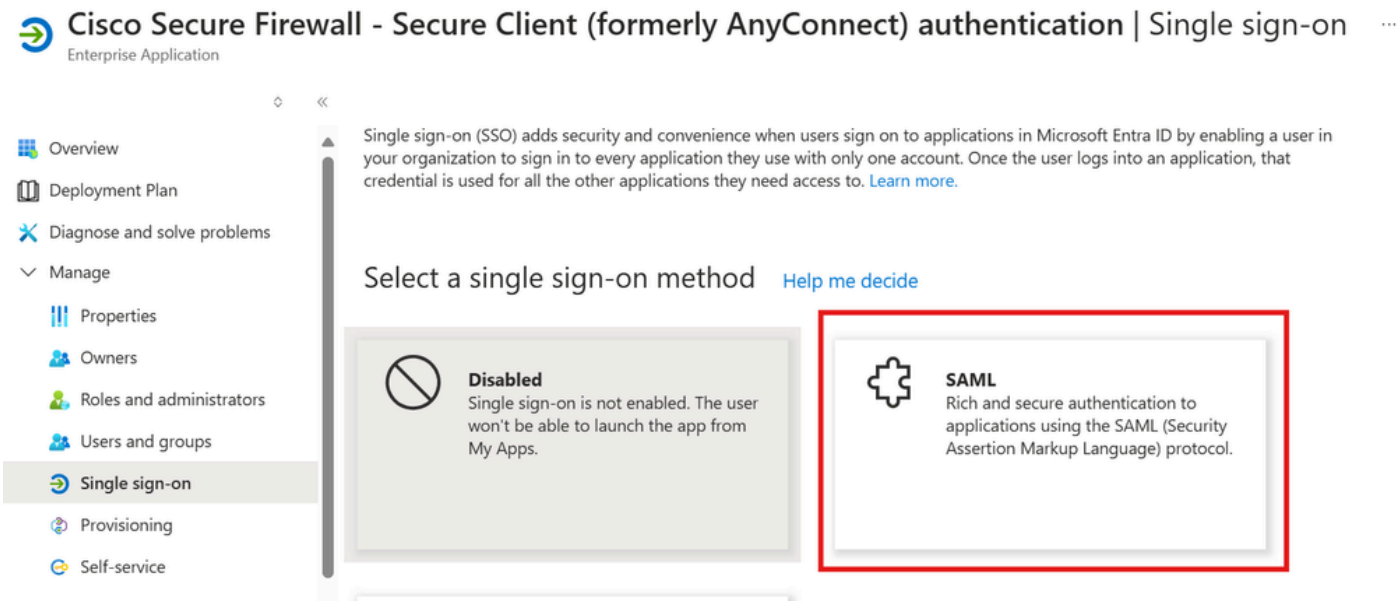


Stap 5. Kies Single Sign-on menuoptie, zoals in deze afbeelding wordt getoond.



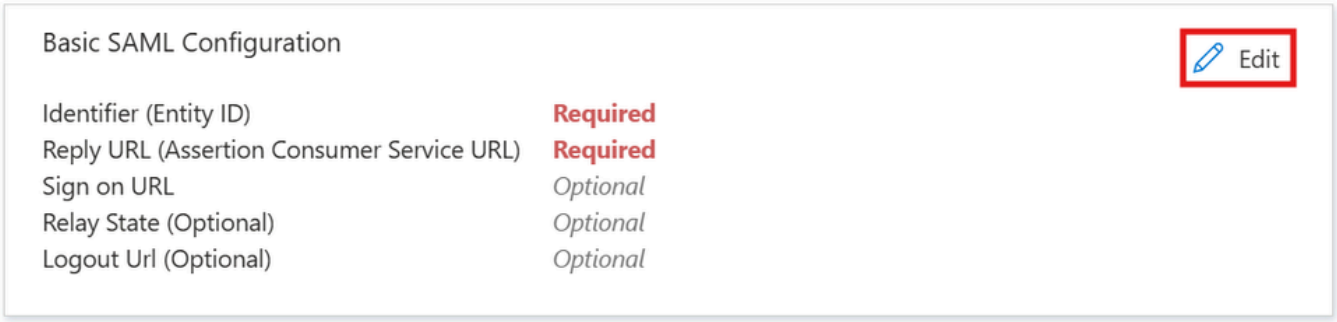
Single Sign On instellen

Stap 6. Kies op de methodpagina Selecteer één aanmelding. SAML.



SAML

Stap 7. Op de eenmalige aanmelding met SAML-pagina instellen, klikt u op het pictogram bewerken/openen voor Basic SAML Configuration om de instellingen te bewerken.



Basisconfiguratie van staal

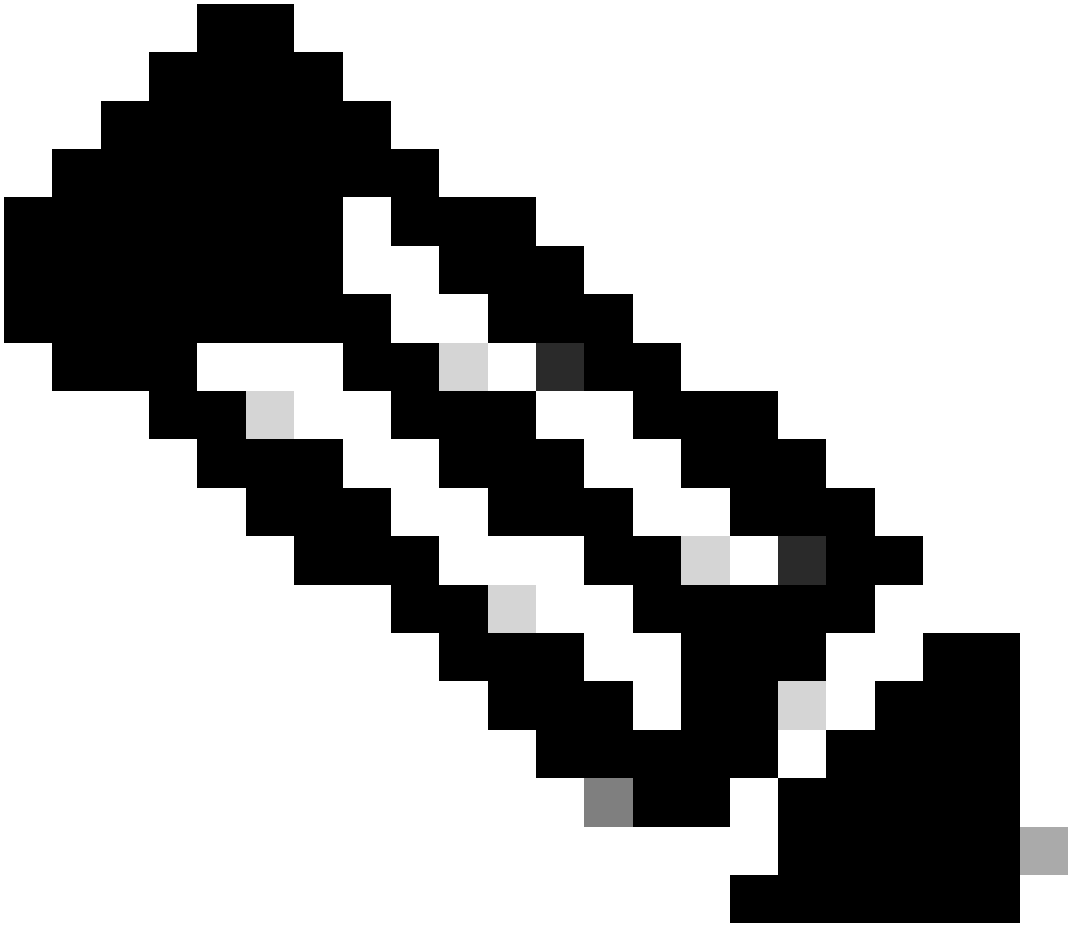
Stap 8. Voer in de eenmalige aanmelding met SAML-pagina de waarden voor deze velden in:

a. Typ in het vak Identifier-tekst een URL met dit patroon:

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

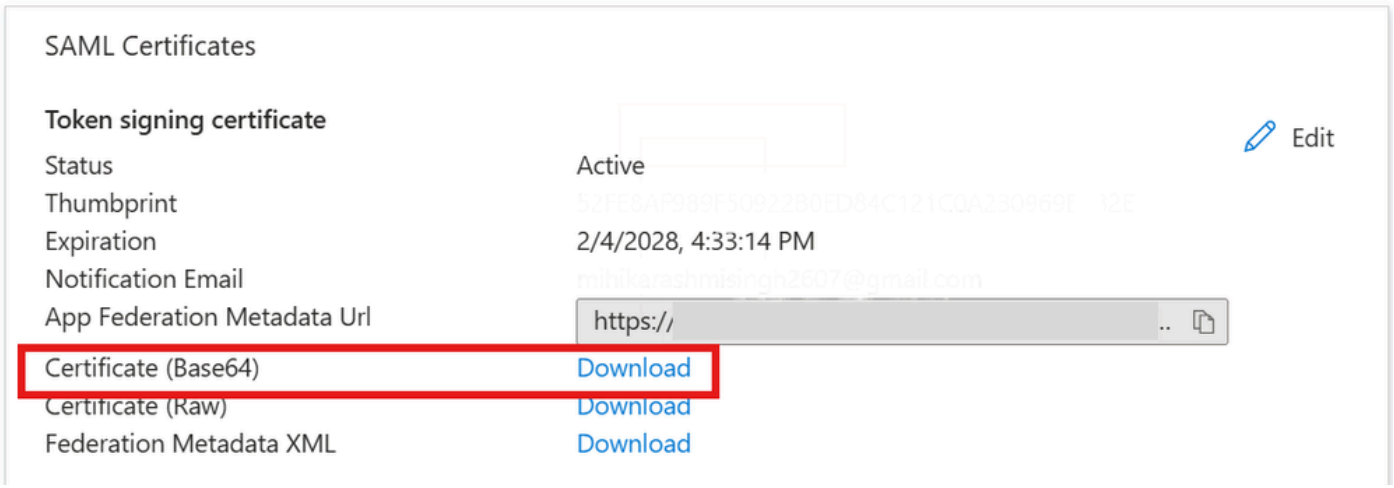
b. Typ in het tekstvak URL voor antwoord een URL met dit patroon:

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

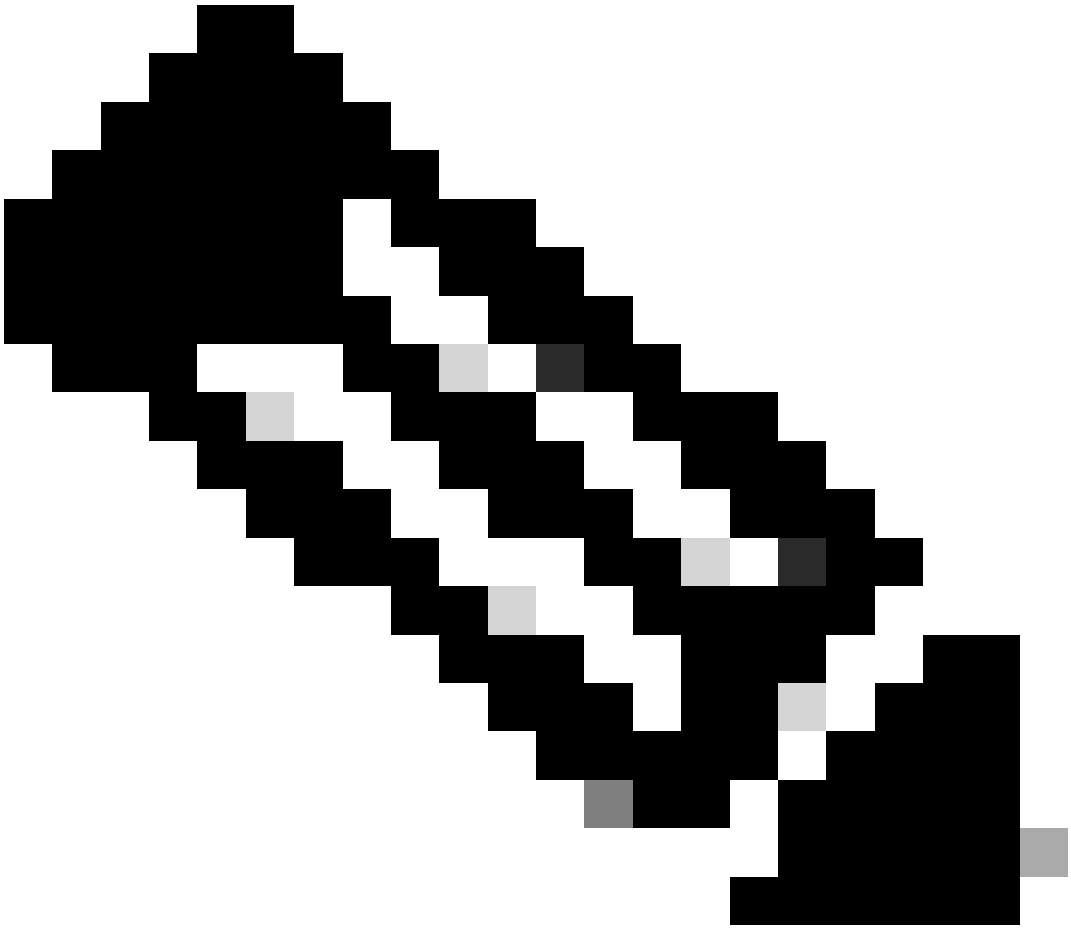


Opmerking: Tunnel_Group_Name is hoofdlettergevoelig en de waarde mag geen punten bevatten '.' en schuine strepen '/'.

Stap 9. Op de enkele aanmelding met SAML-pagina instellen, in het gedeelte SAML Signing Certificate, vind je Certificate (Base64) en kies Download om het certificaatbestand te downloaden en op je computer op te slaan.



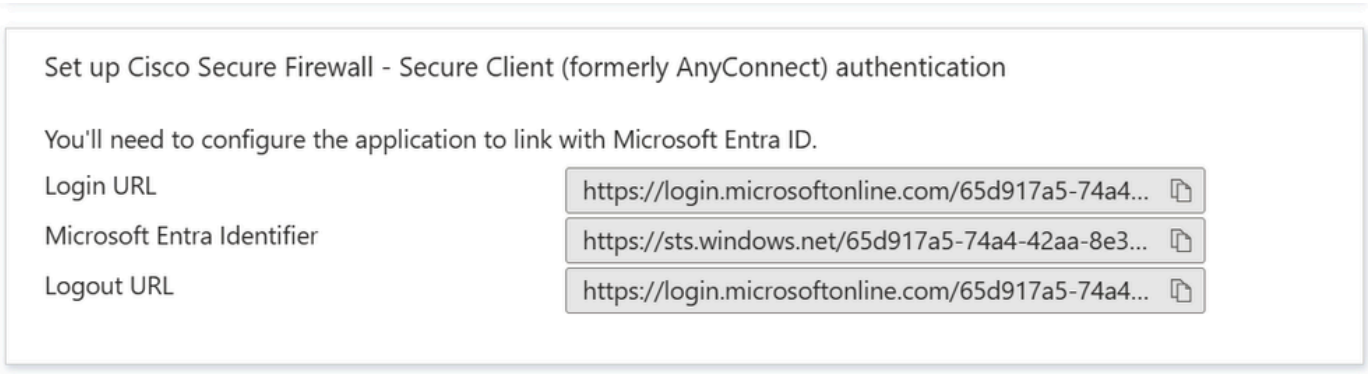
Certificaat (Base64) downloaden



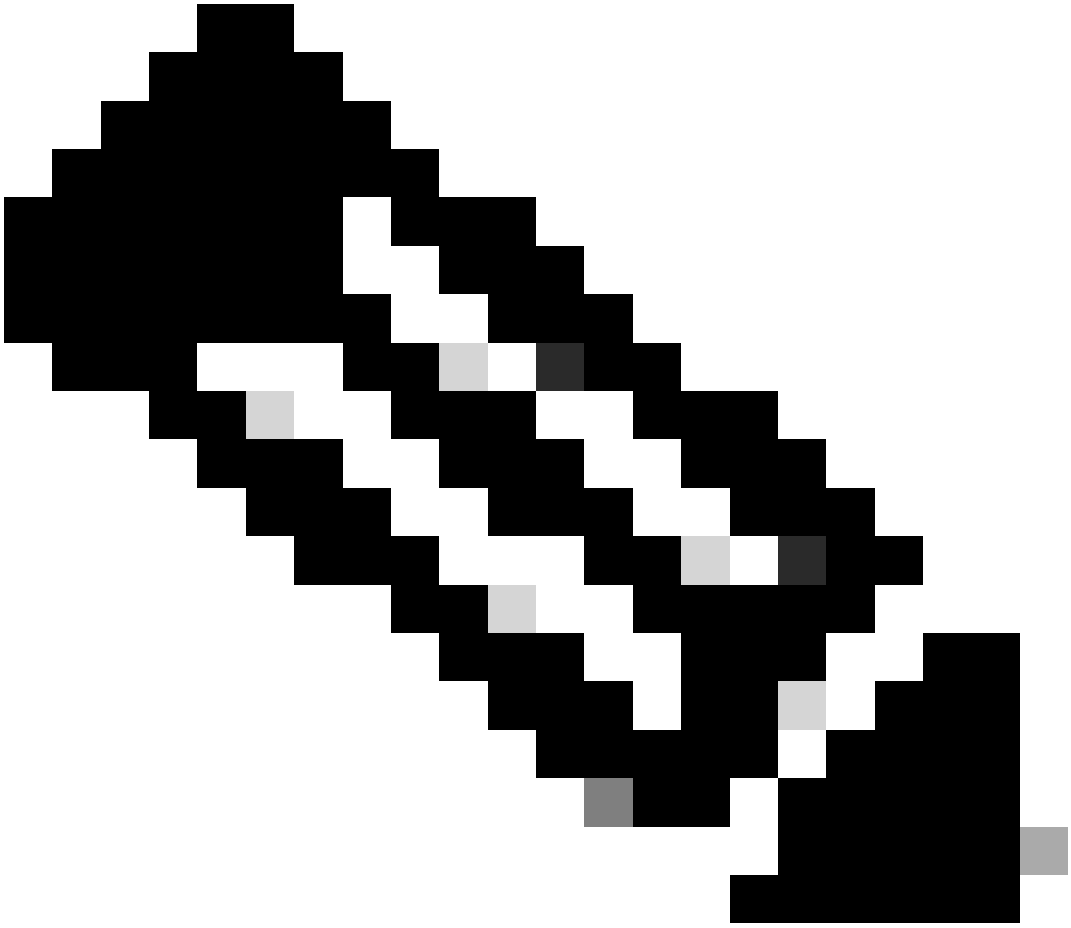
Opmerking: dit gedownloade certificaat wordt geïmporteerd in het ASA trustpoint AzureAD-AC-SAML1. Raadpleeg de sectie ASA Configuration voor meer informatie.

Stap 10. Kopieer in het gedeelte Cisco Secure Firewall - Secure Client (Beveiligde client) instellen de juiste URL(s) die op uw vereiste is (zijn) gebaseerd. Deze URL(s) worden gebruikt om een SSO Server-object op ASA te configureren.

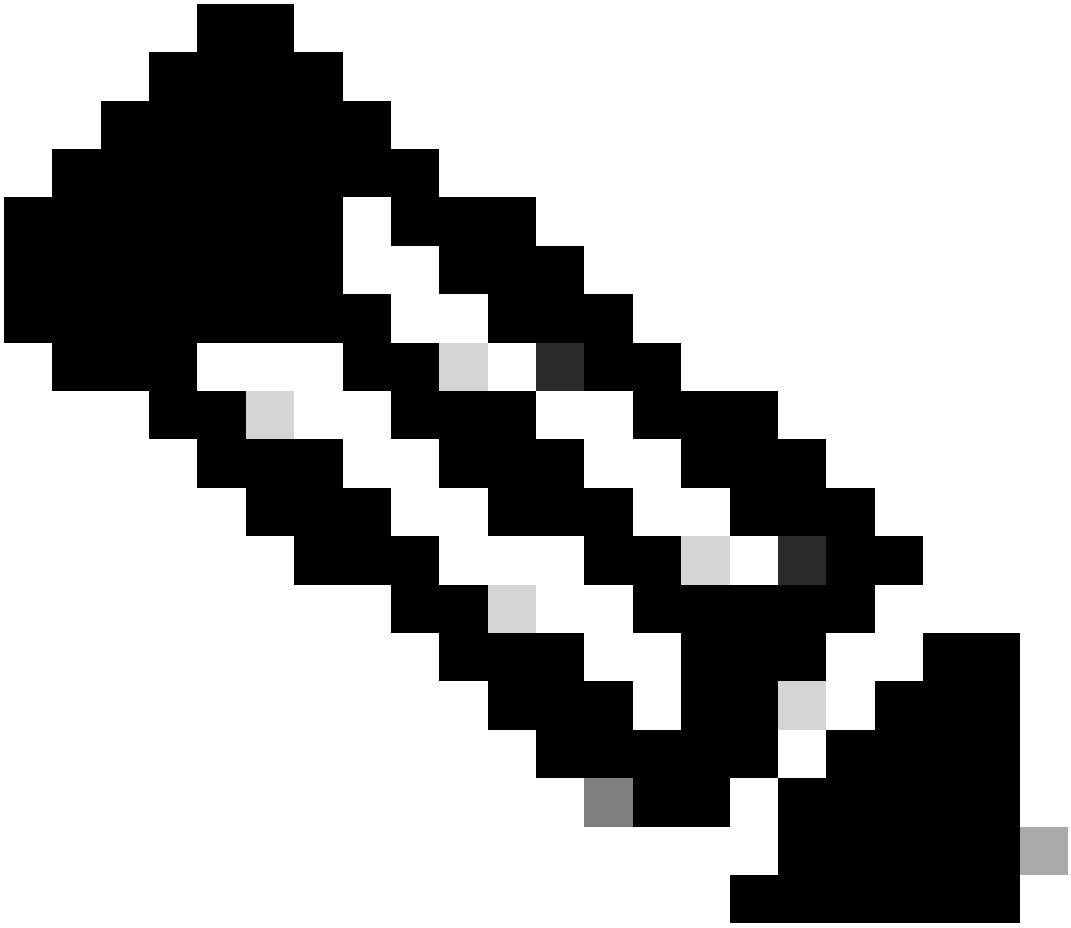
- Microsoft Entra Identifier - Dit is de SAML idp in de VPN-configuratie.
- Aanmeldings-URL: dit is de URL voor aanmelden.
- Afmeldings-URL: dit is de URL voor afmelden.



DSB-URL



Opmerking: Herhaal de eerdere configuratiestappen om de Cisco Secure Firewall - Secure Client-app toe te voegen vanuit de galerij voor de tweede tunnelgroep. De tweede tunnelgroepnaam in dit geval is SAML2.



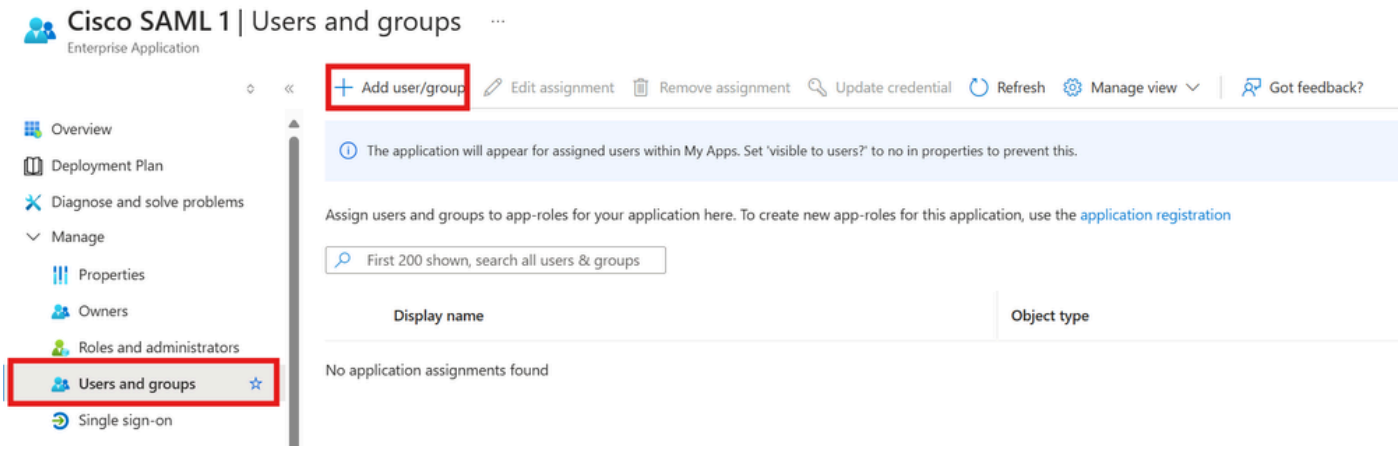
Opmerking: bij het toevoegen van de Cisco Secure Firewall - Secure Client-app voor de tweede tunnelgroep (SAML 2), wordt het azuurcertificaat dat is gedownload in stap 8. geïmporteerd in het ASA-betrouwbaarheidspunt AzureAD-AC-SAML2.

Azure AD-gebruikers toewijzen aan de app

In deze sectie zijn Test1 en Test2 ingeschakeld om Azure SSO te gebruiken, aangezien u toegang verleent tot de Cisco Secure Client-app.

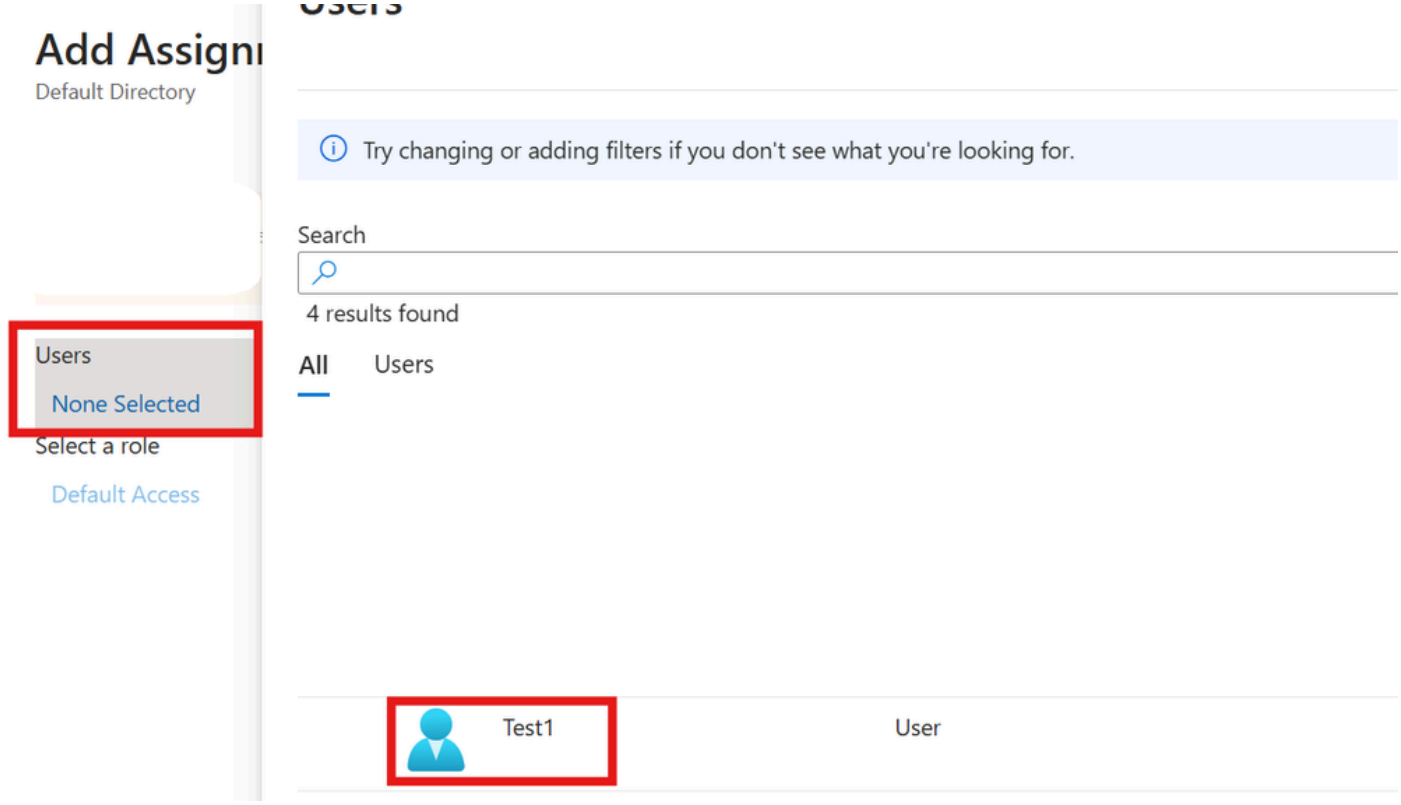
Voor de eerste IDp-toepassing:

Stap 1. Kies Gebruikers en groepen in de eerste overzichtspagina van de IDp-toepassing en voeg gebruiker toe.



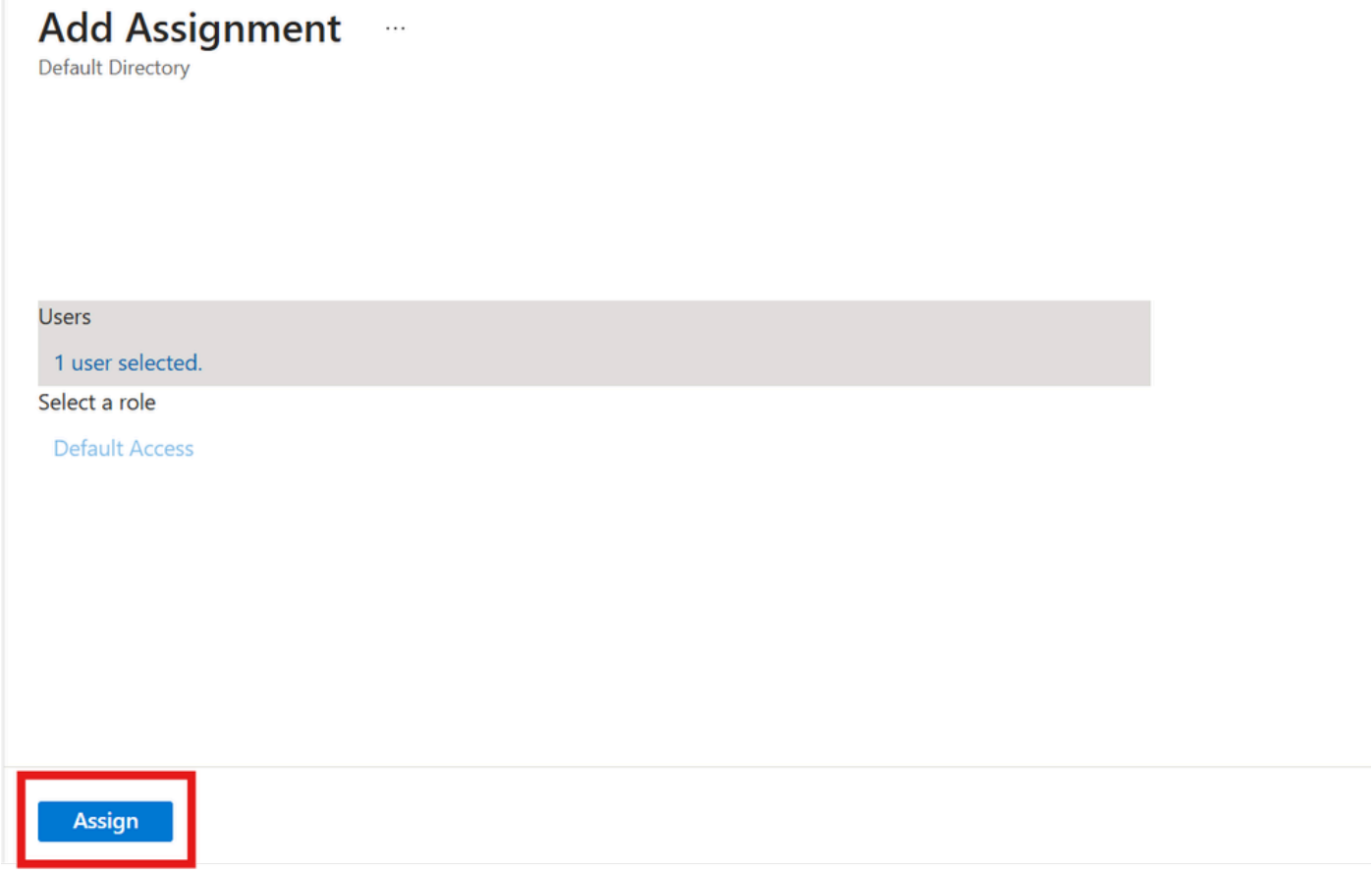
Gebruikers en groepen

Stap 2. Kies Gebruikers of groepen in het dialoogvenster Toewijzing toevoegen.



Toewijzing toevoegen 1

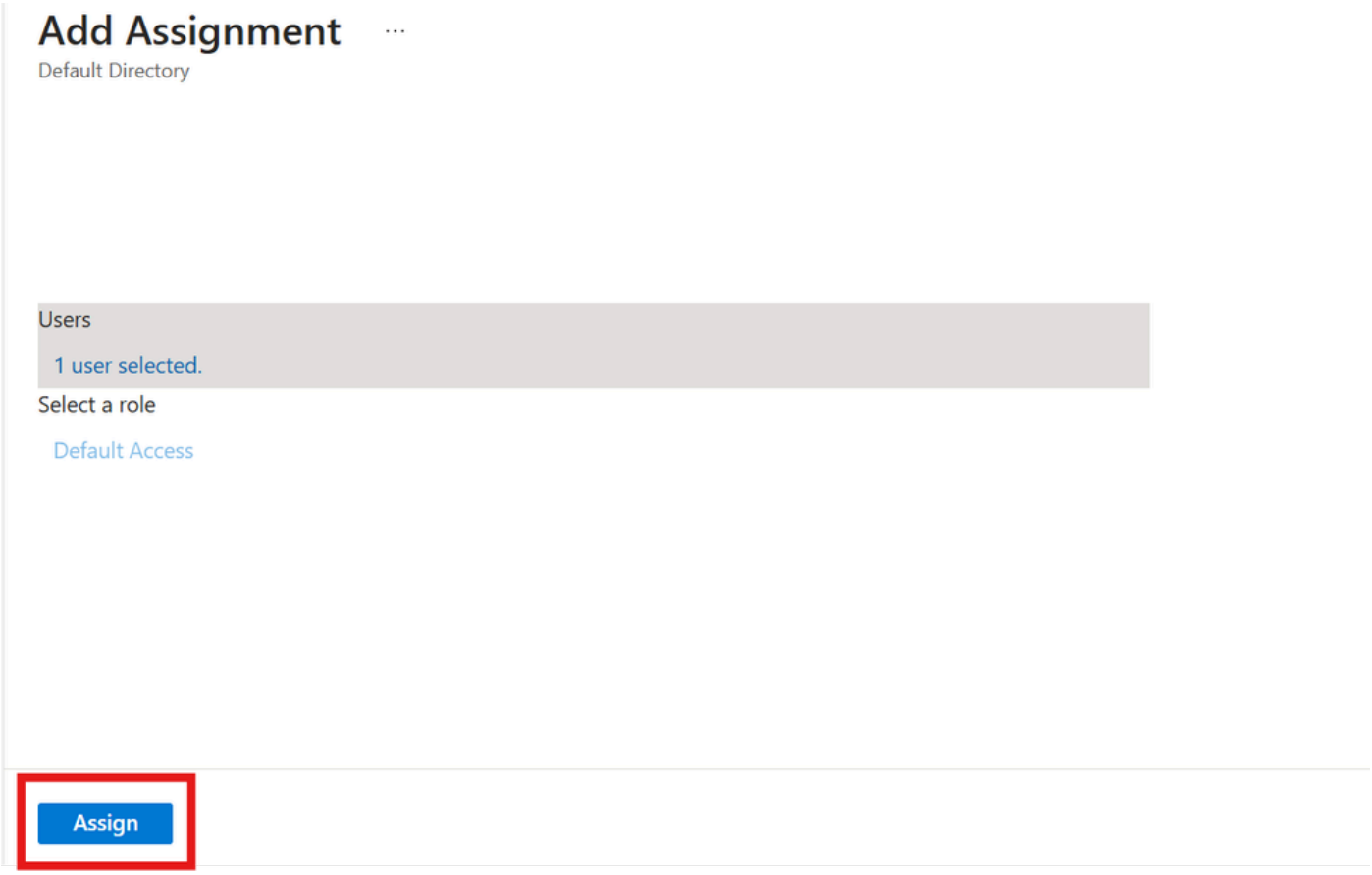
Stap 3. Klik in het dialoogvenster Add Assignment (Toewijzing toevoegen) op de knop Assign (Toewijzen).



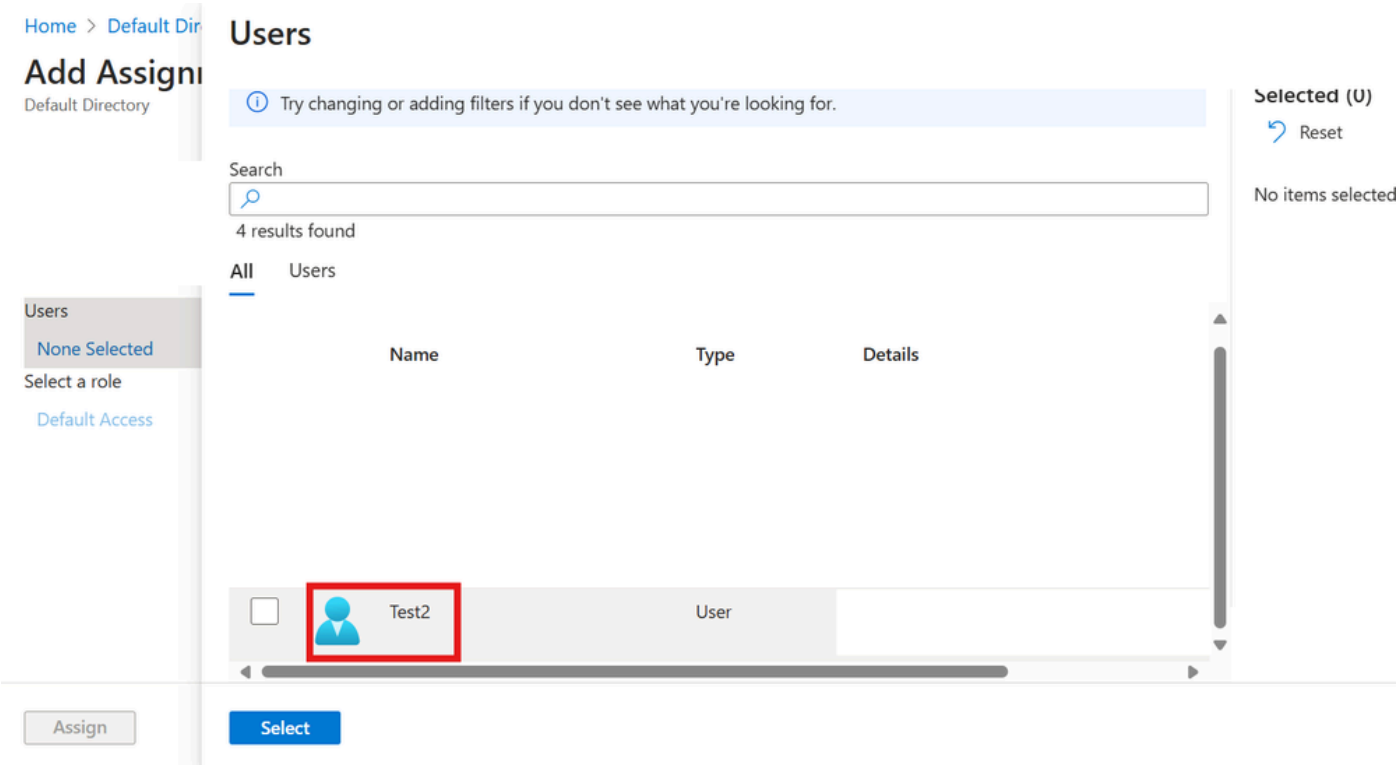
Test 1 gebruikerstoewijzing

Voor de tweede IDp-toepassing:

Herhaal de vroegere stappen voor Tweede Idp Toepassing zoals getoond in deze beelden.

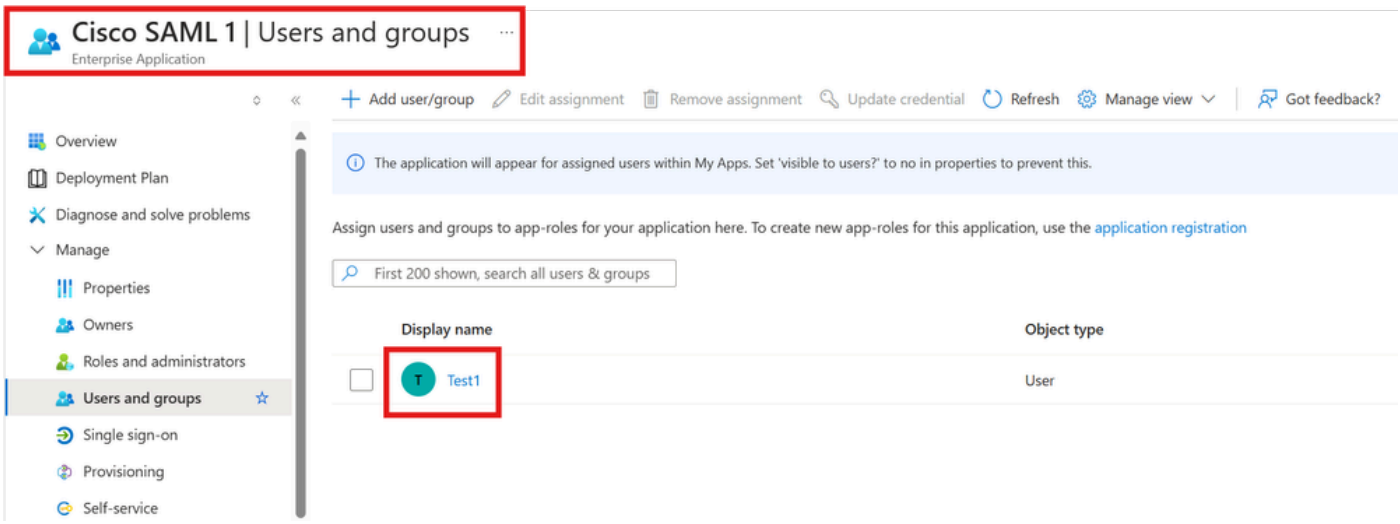


Toewijzing toevoegen 2



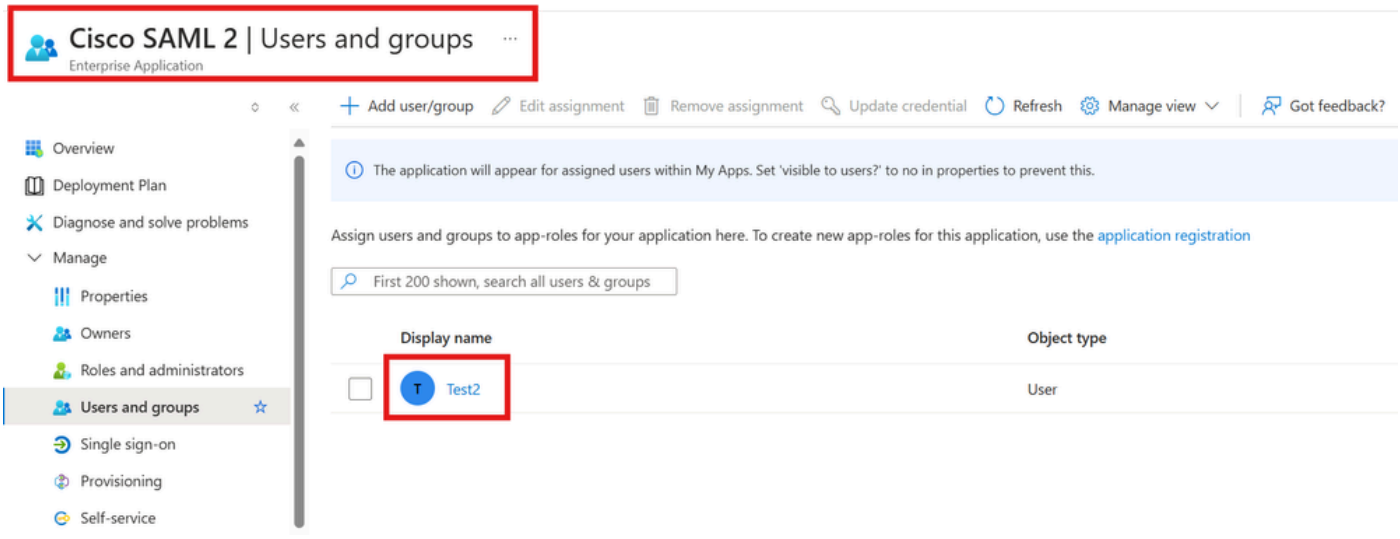
Test2 gebruikerstoewijzing

Test1 Gebruikerstoewijzing:



Test 1 gebruikerstoewijzing

Test2 Gebruikerstoewijzing:



Test 2 gebruikerstoewijzing

ASA-configuratie via CLI

Stap 1. Maak vertrouwen aan en importeer SAML-certificaten.

Configureer twee Trustpoints en importeer de respectieve SAML-certificaten voor elke tunnelgroep.

<#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
```

Stap 2. Configureer de SAML IDP.

Gebruik deze opdrachten om de SAML IDp-instellingen te provisioneren.

```
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
```

Stap 3. Pas SAML-verificatie toe op de eerste VPN-tunnelgroep.

Configureer de SAML1 tunnelgroep met AzureAD-AC-SAML1 IDP trustpoint.

<#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 (

Stap 4. Pas SAML-verificatie toe op de tweede VPN-tunnelgroep.

Configureer de SAML2 tunnelgroep met AzureAD-AC-SAML2 IDP trustpoint.

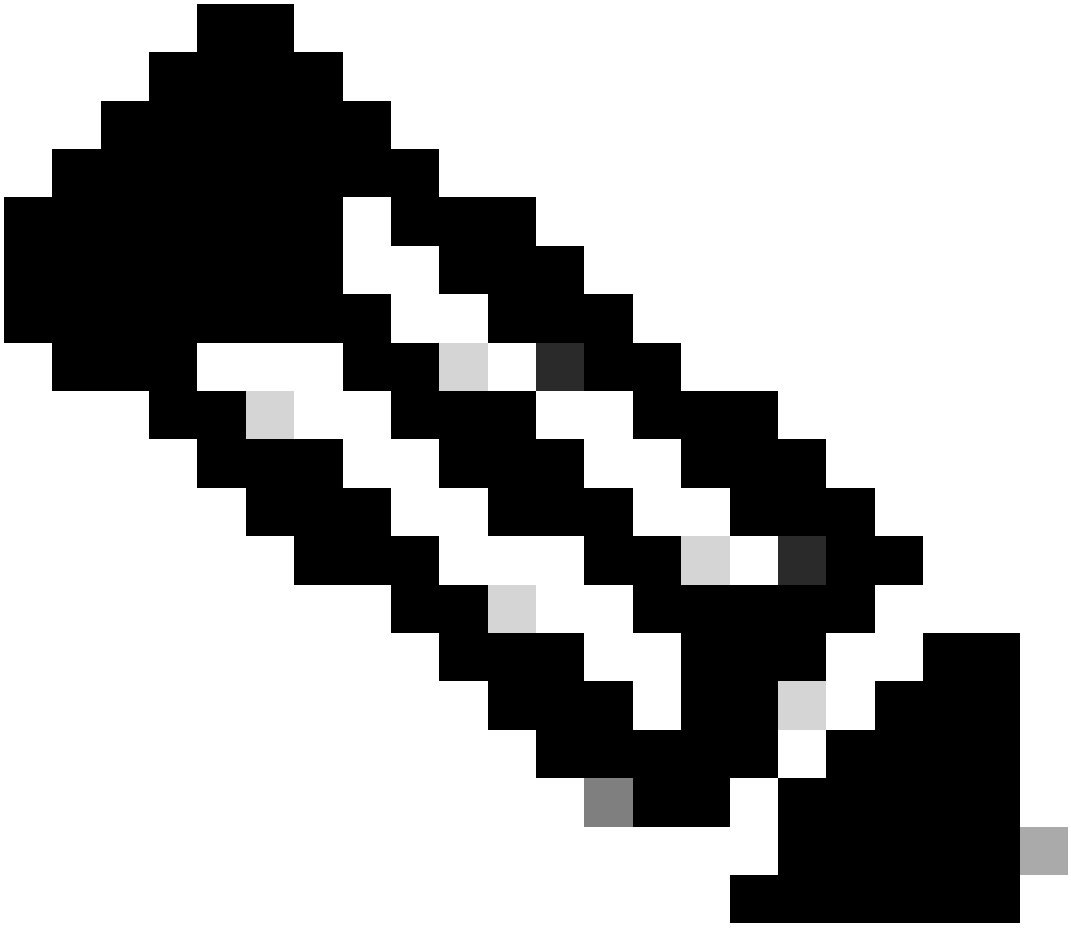
<#root>

```
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 (

Stap 5: Sla de configuratie op.

```
write memory
```



Opmerking: Als u wijzigingen aanbrengt in de IDp-configuratie, moet u de SAML Identity-Provider-configuratie uit uw Tunnel Group verwijderen en opnieuw toepassen voor de wijzigingen om effectief te worden.

Verifiëren

Test AnyConnect met SAML-verificatie.

Stap 1. Maak verbinding met uw VPN-URL en voer uw login in Azure AD details.

Stap 2. (optioneel) Goedkeuring van inlogaanvraag.

Stap 3. AnyConnect is verbonden.

Problemen oplossen

De meeste problemen met SAML hebben betrekking op een foutieve configuratie die kan worden gevonden wanneer de SAML-configuratie is ingeschakeld of wanneer debugs worden uitgevoerd. debug webvpn saml 255 kan worden gebruikt om de meeste problemen op te lossen, echter, in scenario's waar dit debug geen nuttige informatie biedt, kunnen extra debugs worden uitgevoerd:

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

Gerelateerde informatie

- ASA AnyConnect VPN met Microsoft Azure MFA configureren via SAML
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.