Configuración de varios grupos de túnel con SAML en ASA

Contenido

Introducción

Este documento describe la autenticación SAML con Azure Identity Provider para varios grupos de túnel en Cisco ASA.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Adaptive Security Appliance (ASA)
- Lenguaje de marcado de aserción de seguridad (SAML)
- Certificados de capa de socket seguro (SSL)
- Microsoft Azure

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA 9.22(1)1

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Microsoft Azure puede admitir varias aplicaciones para el mismo Id. de entidad. Cada aplicación (asignada a un grupo de túnel diferente) requiere un certificado único. En ASA, se pueden configurar varios grupos de túnel para utilizar diferentes aplicaciones protegidas con el Proveedor de identidad de invalidación (IdP) debido a la Función de certificado IdP. Esta función permite a los administradores anular el certificado IdP principal en el objeto de servidor de inicio de sesión único (SSO) con un certificado IdP específico para cada grupo de túnel. Esta función se introdujo en ASA a partir de la versión 9.17.1.

SSO iniciado por SP de SAML

Cuando el usuario final inicia el inicio de sesión accediendo a ASA, el comportamiento de inicio de sesión continúa de la siguiente manera:

1. Cuando el usuario VPN accede o elige un grupo de túnel habilitado para SAML, el usuario final es redirigido al IdP de SAML para la autenticación. Se le solicita al usuario a menos que acceda directamente a la url del grupo, en cuyo caso la redirección es silenciosa.

2. El ASA genera una Solicitud de Autenticación SAML, que el navegador redirige al IdP SAML.

3. El IdP desafía al usuario final para obtener las credenciales y el usuario final se conecta. Las credenciales ingresadas deben satisfacer la configuración de autenticación IdP.

4. La respuesta de IdP se envía de vuelta al navegador y se publica en la URL de inicio de sesión de ASA. ASA verifica la respuesta para completar el inicio de sesión.

Configuraciones

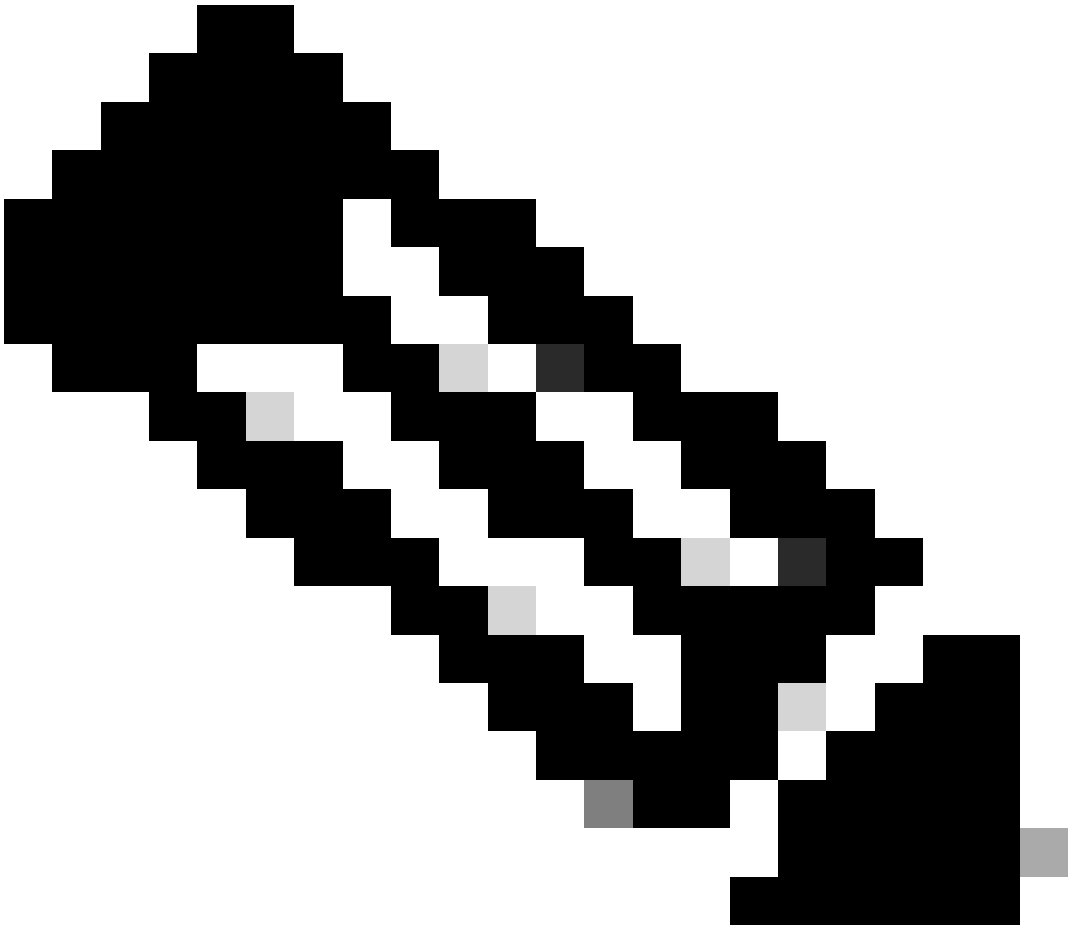
Adición de Cisco Secure Firewall - Secure Client desde la Galería

En este ejemplo, se agrega la integración de Microsoft Entra SSO con Cisco Secure Firewall - Secure Client en Azure para dos grupos de túnel configurados en ASA:

- SAML1
- SAML2

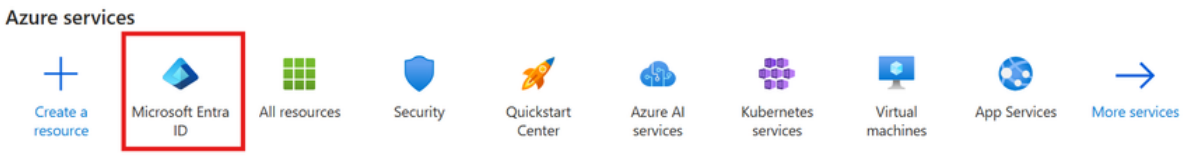
Para configurar la integración de Cisco Secure Firewall - Secure Client en Microsoft Entra ID,

debe agregar Cisco Secure Firewall - Secure Client de la galería a la lista de aplicaciones SaaS gestionadas.



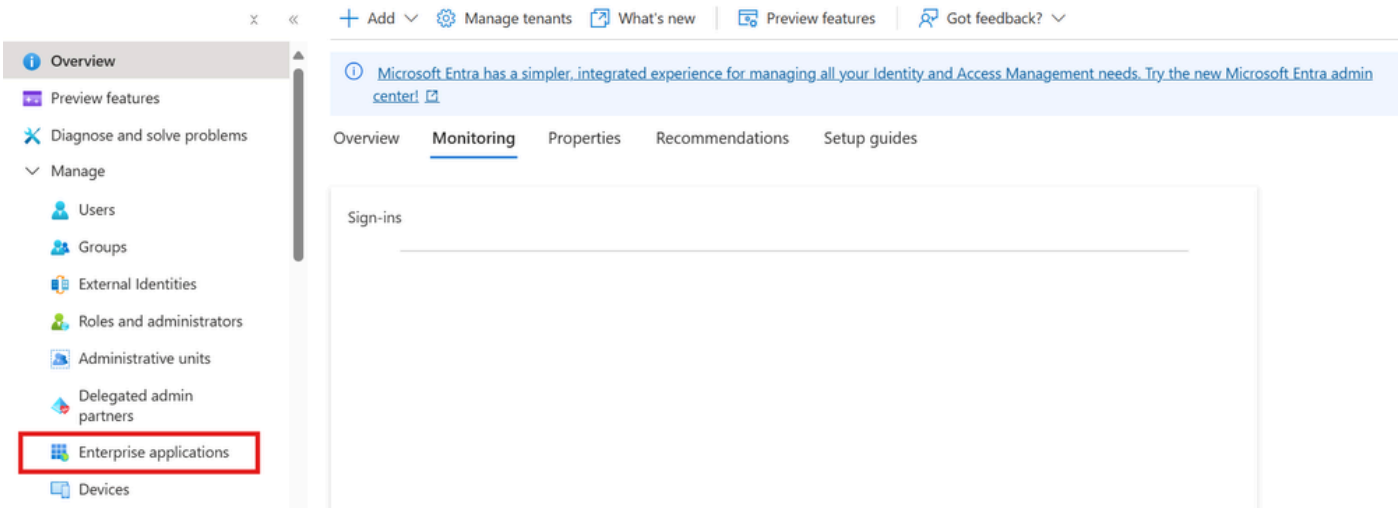
Nota: Estos pasos son para agregar Cisco Secure Firewall - Secure Client a la galería para el primer grupo de túnel, SAML1.

Paso 1. Inicie sesión en el Portal de Azure y elija Microsoft Entra ID.



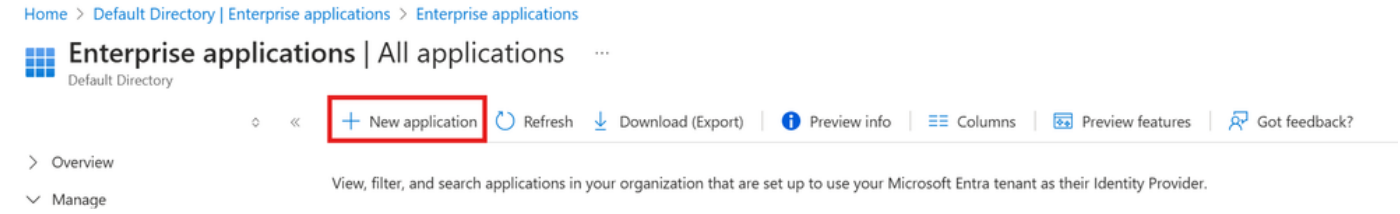
ID de Microsoft Entra

Paso 2. Como se muestra en esta imagen, seleccione Aplicaciones de Empresa.



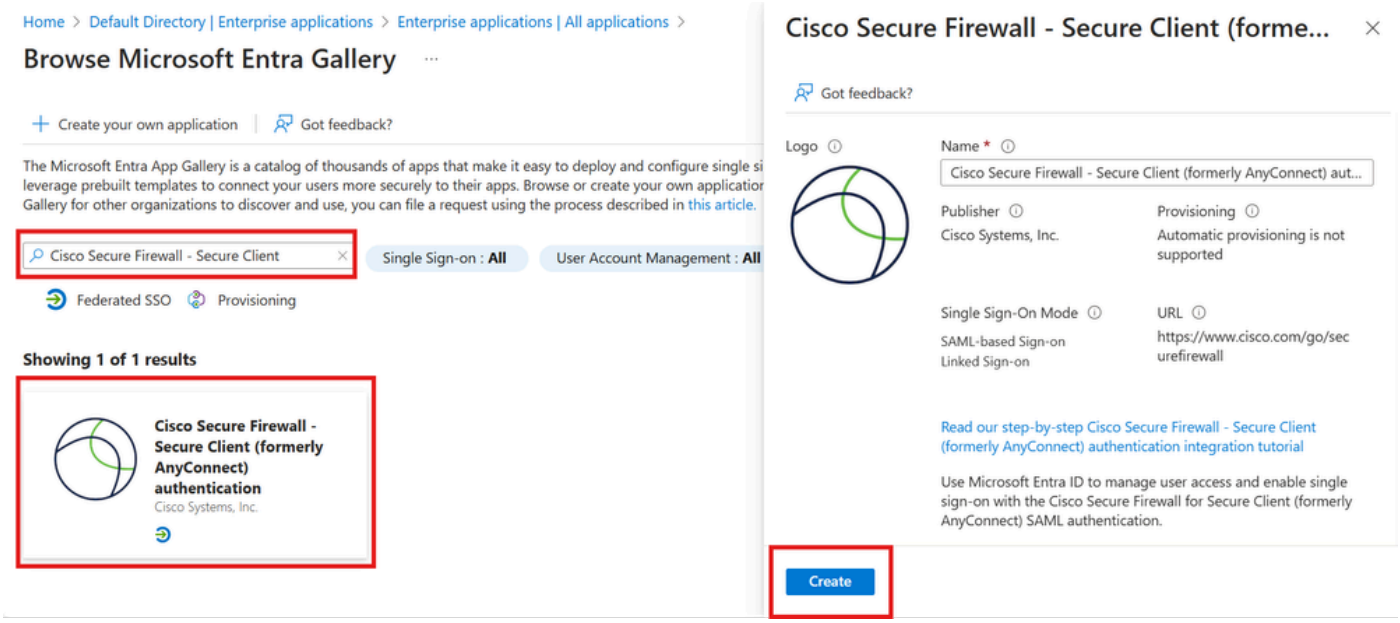
Aplicación empresarial

Paso 3. Ahora, elija Nueva aplicación, como se muestra en esta imagen.

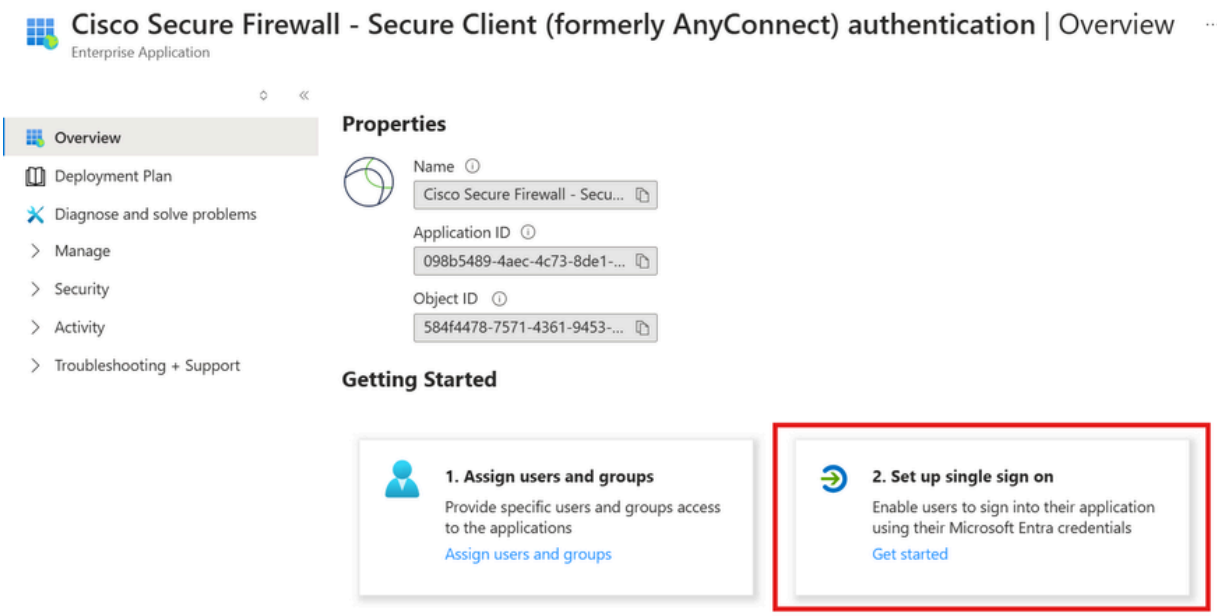


Nueva aplicación

Paso 4. En la sección Agregar de la galería, escriba Cisco Secure Firewall - Secure Client en el cuadro de búsqueda, elija Cisco Secure Firewall - Secure Client en el panel de resultados, y luego agregue la aplicación.

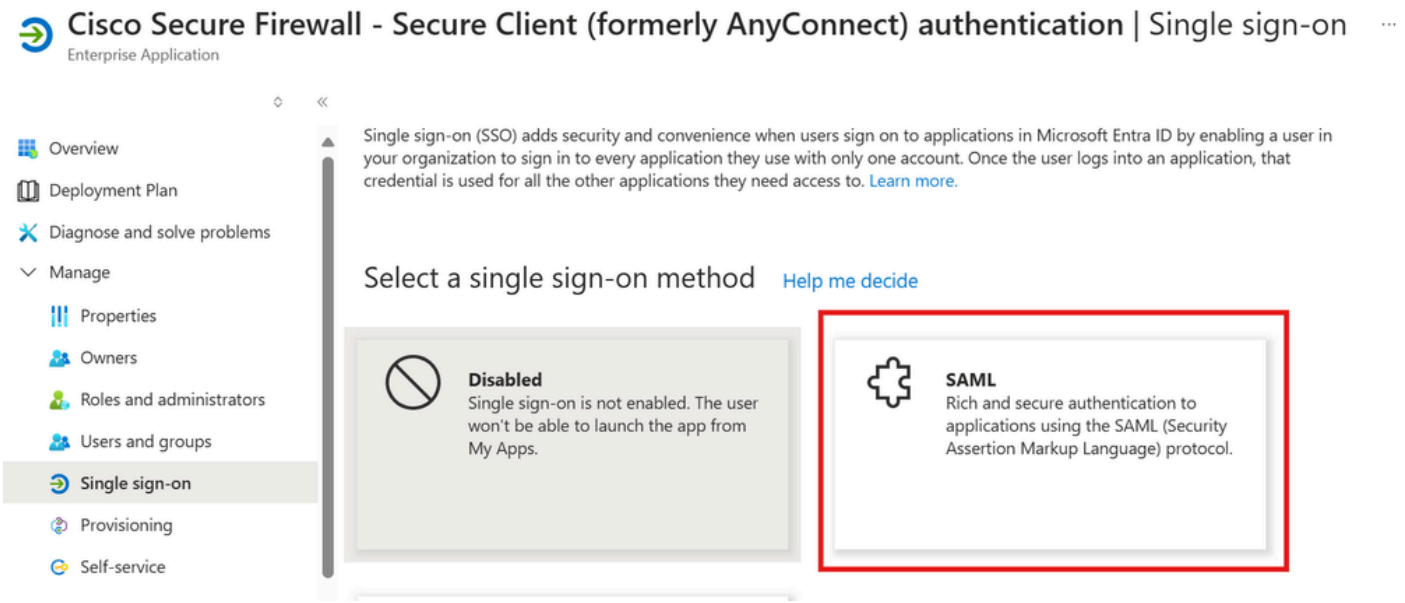


Paso 5. Elija Single Sign-on menu item, como se muestra en esta imagen.



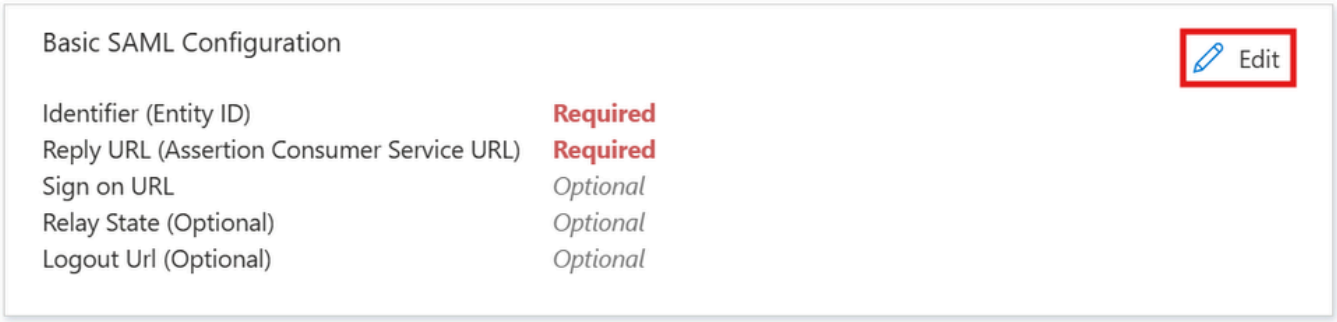
Configuración del inicio de sesión único

Paso 6. En la páginaSeleccione un método de inicio de sesión único, elijaSAML.



SAML

Paso 7. En la página Configurar inicio de sesión único con SAML, haga clic en el icono de edición/apertura de Configuración básica de SAML para editar los ajustes.



Configuración Saml Básica

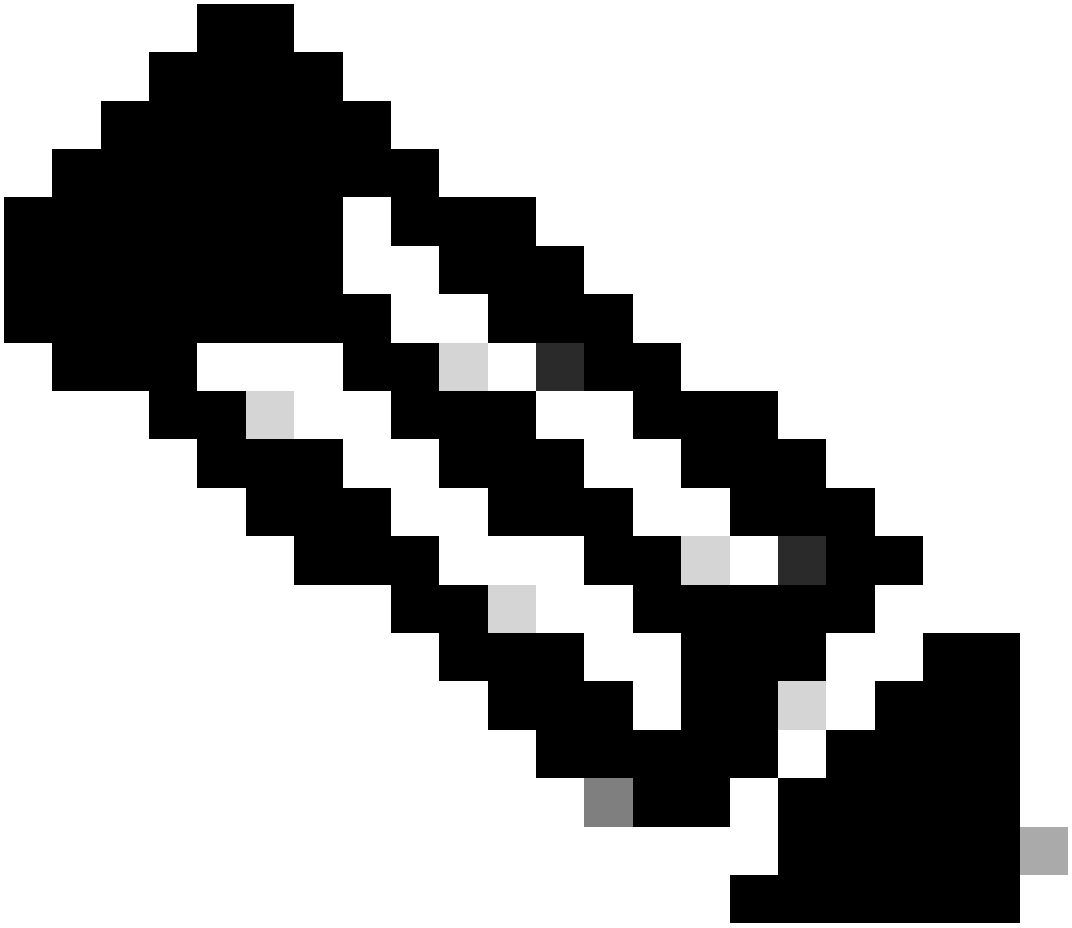
Paso 8. En la página Configurar el inicio de sesión único con SAML, introduzca los valores de estos campos:

a. En el cuadro de texto Identifiertext, escriba una dirección URL utilizando este patrón:

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

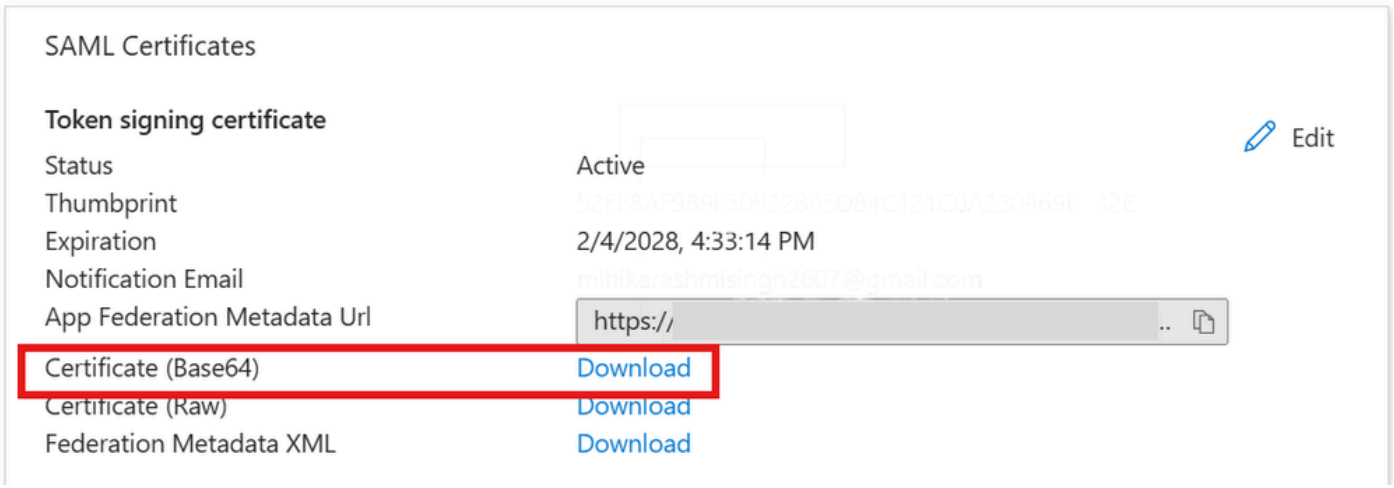
b. En el cuadro de texto URL de respuesta, escriba una dirección URL con este patrón:

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

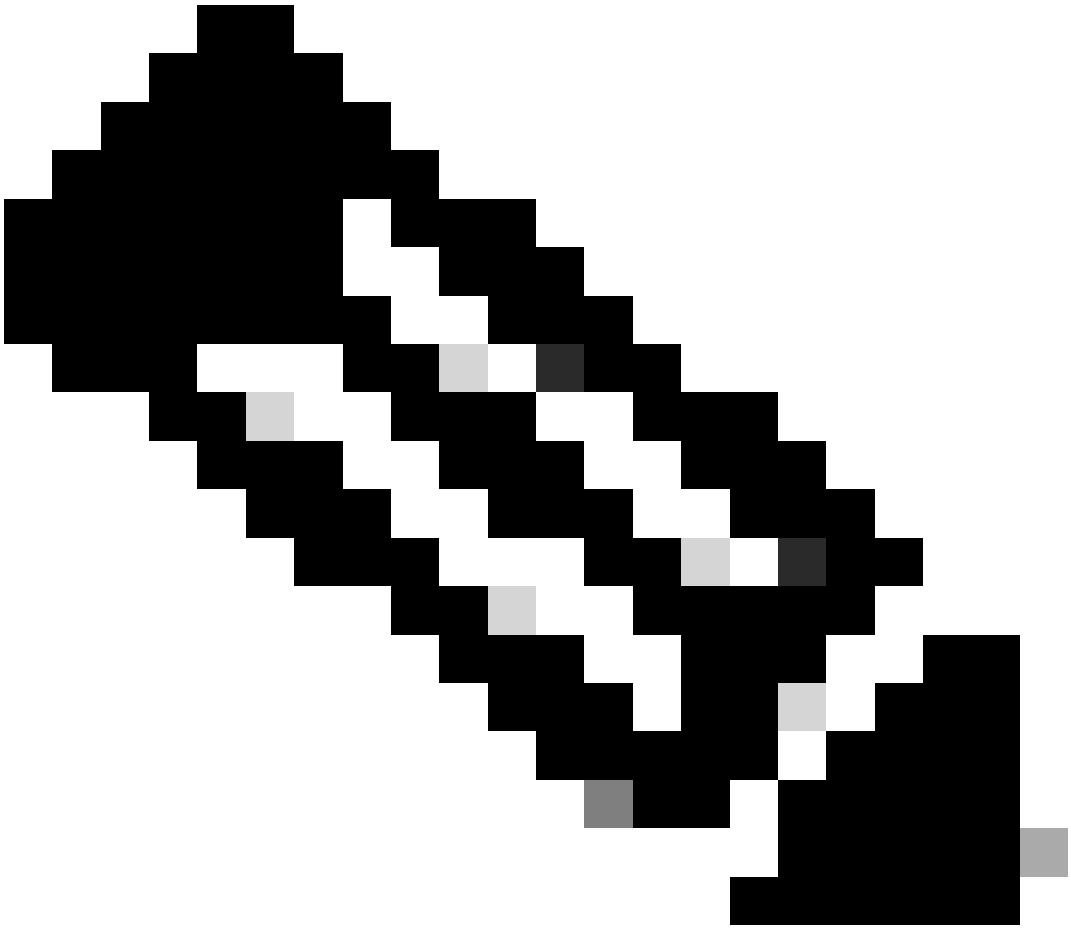


Nota: Tunnel_Group_Name distingue entre mayúsculas y minúsculas y el valor no debe contener puntos '.' y barras diagonales '/'.

Paso 9. En la página Configurar inicio de sesión único con SAML, en la sección Certificado de firma SAML, busque Certificado (Base64) y elija Descargar para descargar el archivo del certificado y guardarlo en su computadora.



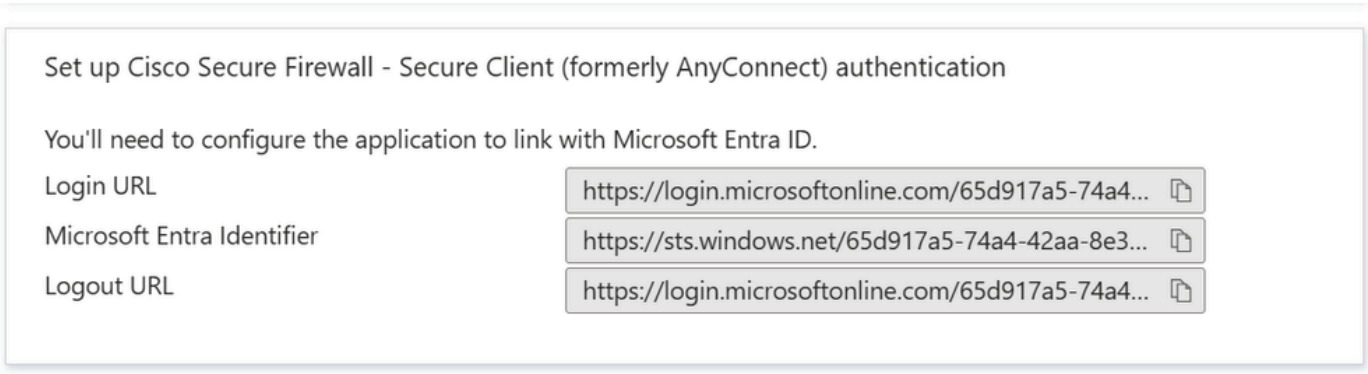
Descarga de certificado (Base64)



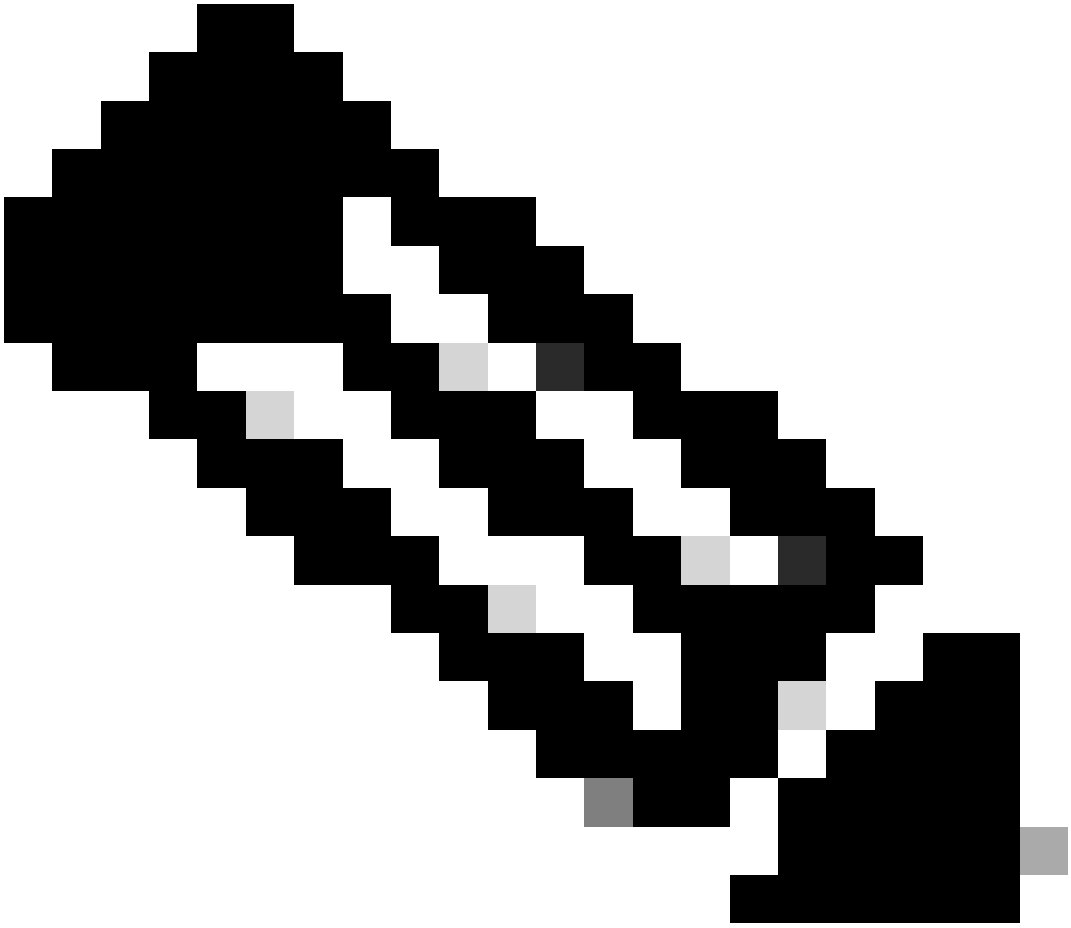
Nota: este certificado descargado se importa en el punto de confianza de ASA AzureAD-AC-SAML1. Consulte la sección Configuración de ASA para obtener más detalles.

Paso 10. En la sección Configuración de Cisco Secure Firewall - Secure Client, copie las URL apropiadas según sus requisitos. Estas URL se utilizan para configurar el objeto de servidor SSO en ASA.

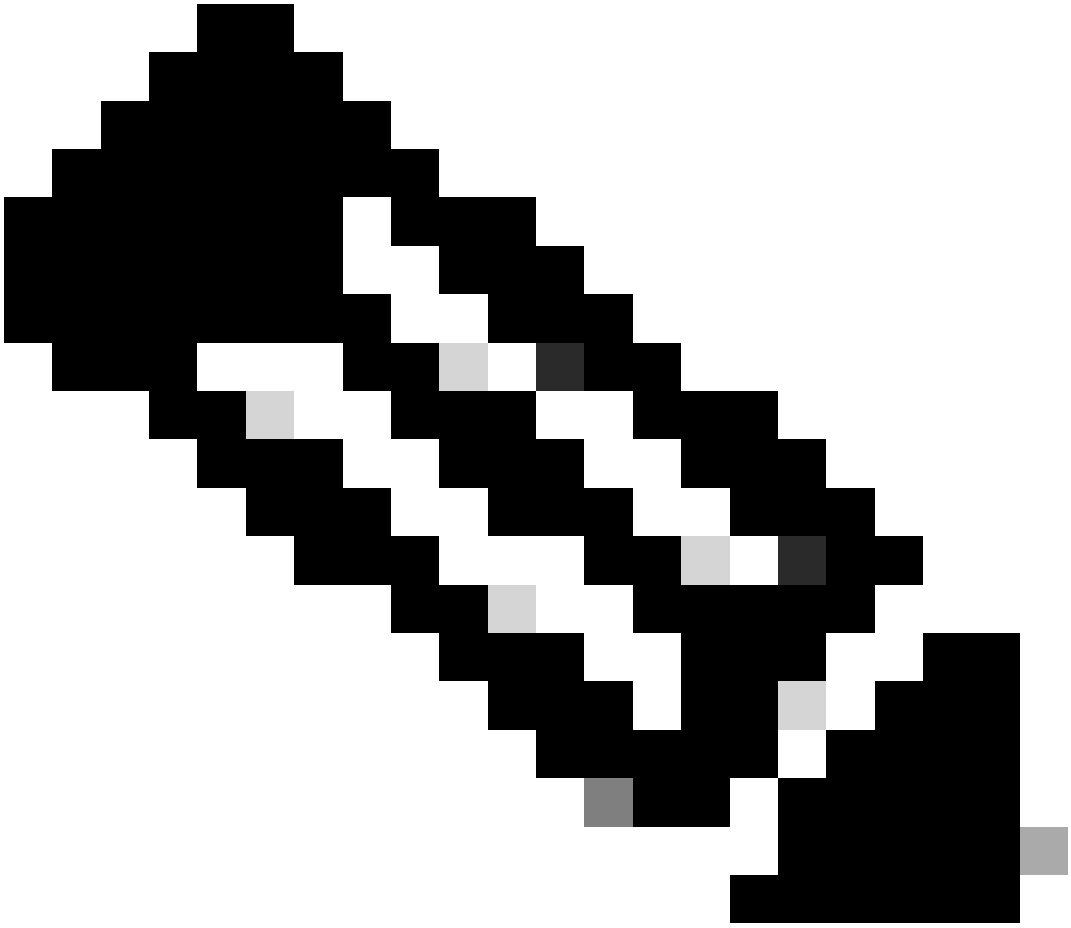
- Microsoft Entra Identifier - Este es el idp SAML en la configuración VPN.
- Login URL (URL de inicio de sesión): se trata del inicio de sesión de URL.
- Logout URL (URL de cierre de sesión): Se trata de la URL de cierre de sesión.



URL DE SSO



Nota: Repita los pasos de configuración anteriores para agregar la aplicación Cisco Secure Firewall - Secure Client desde la galería para el segundo grupo de túnel. El segundo nombre de grupo de túnel en este caso es SAML2.



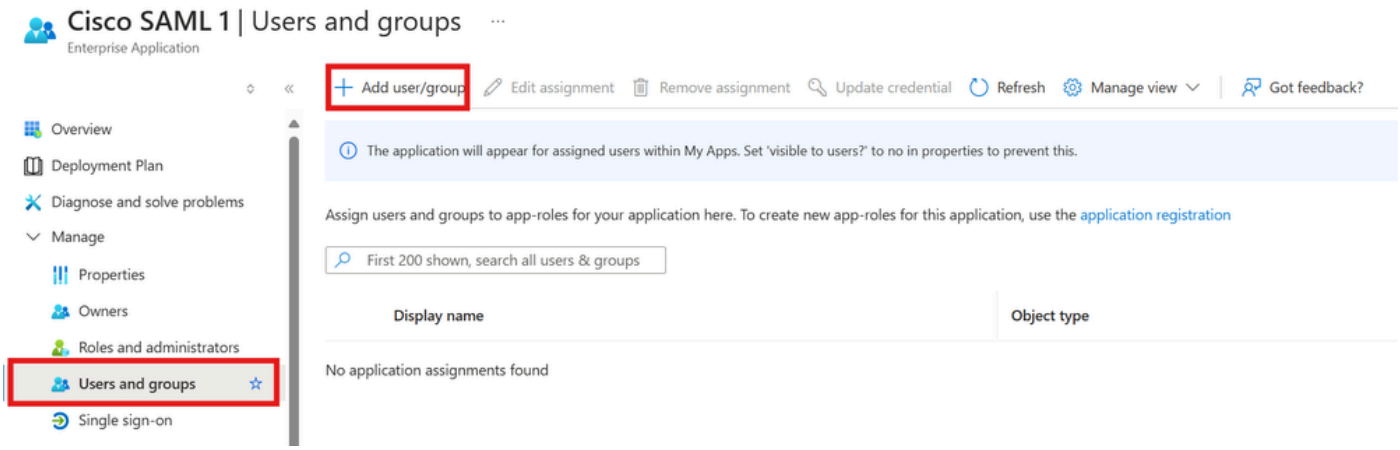
Nota: al agregar la aplicación Cisco Secure Firewall - Secure Client para el segundo grupo de túnel (SAML 2), el certificado de Azure descargado en el paso 8 se importa en el punto de confianza de ASA AzureAD-AC-SAML2.

Asignar usuarios de Azure AD a la aplicación

En esta sección, Test1 y Test2 están habilitados para utilizar Azure SSO, ya que otorga acceso a la aplicación Cisco Secure Client.

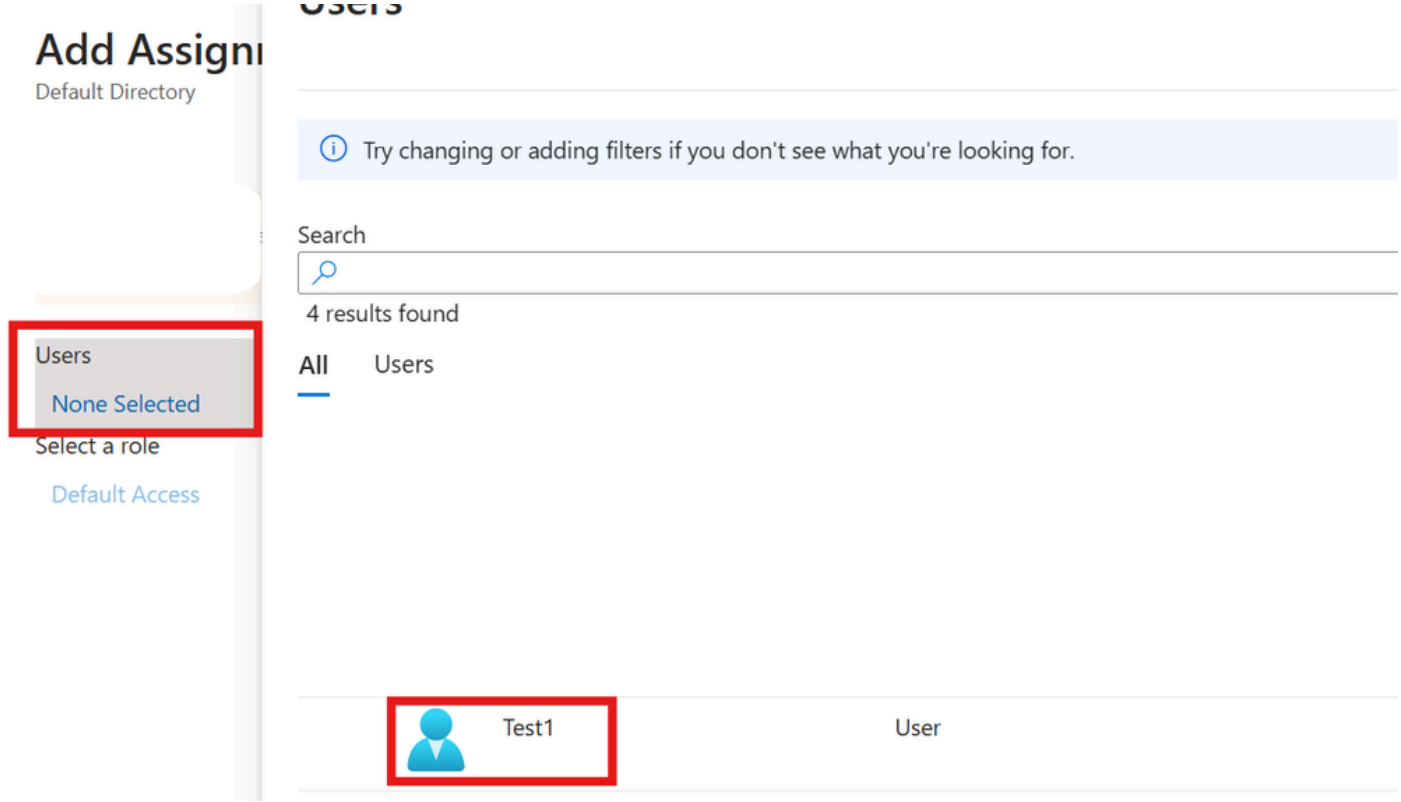
Para la primera aplicación IdP:

Paso 1. En la primera página de descripción general de la aplicación IdP, elija Usuarios y grupos, y luego Agregar usuario.



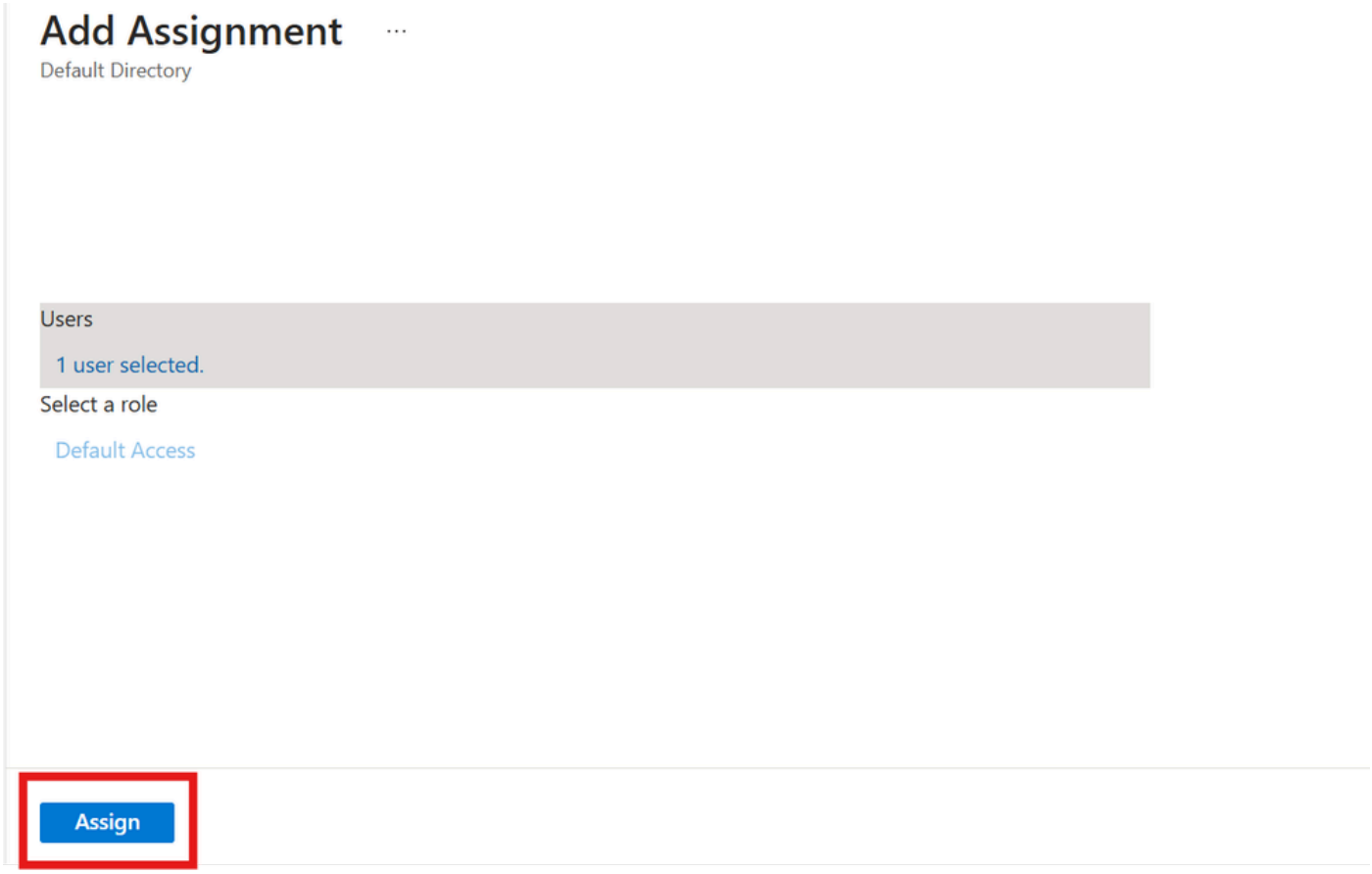
Usuario y grupos

Paso 2. Elija Usuarios o grupos en el diálogo Agregar asignación.



Agregar asignación 1

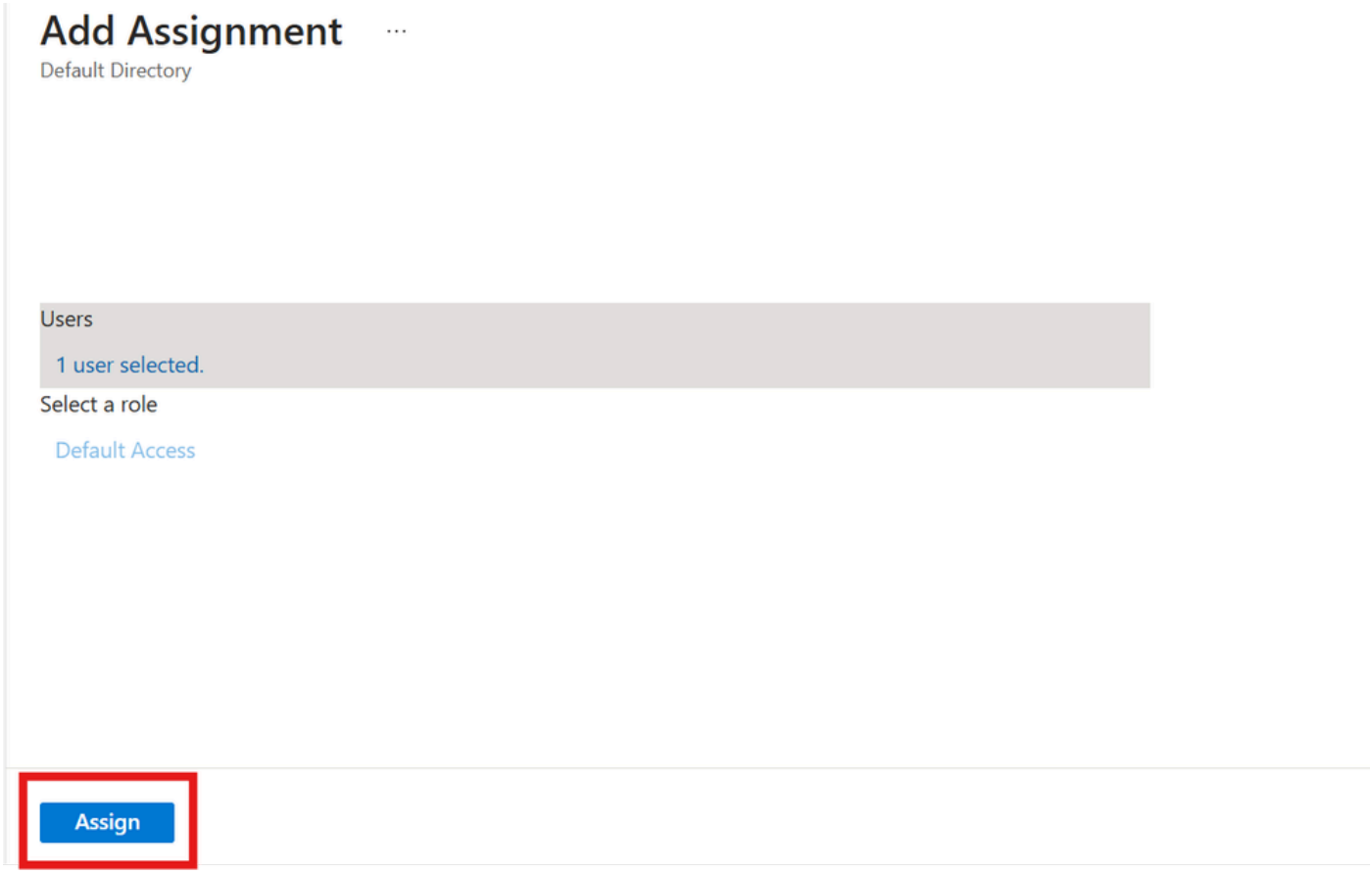
Paso 3. En el Añadir asignación diálogo, haga clic en Asignar botón.



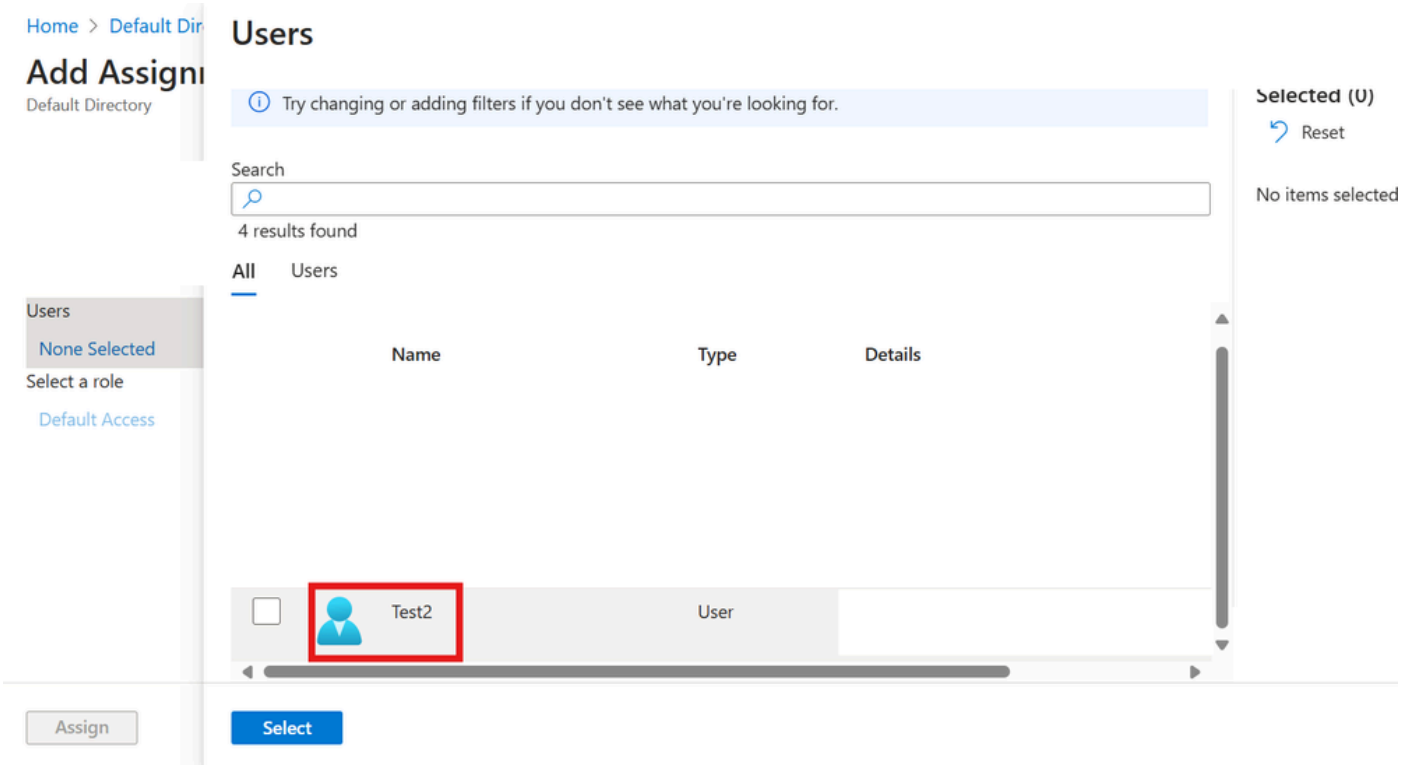
Asignación de usuario de Prueba1

Para la segunda aplicación IdP:

Repita los pasos anteriores para Second Idp Application (Segunda aplicación Idp) como se muestra en estas imágenes.

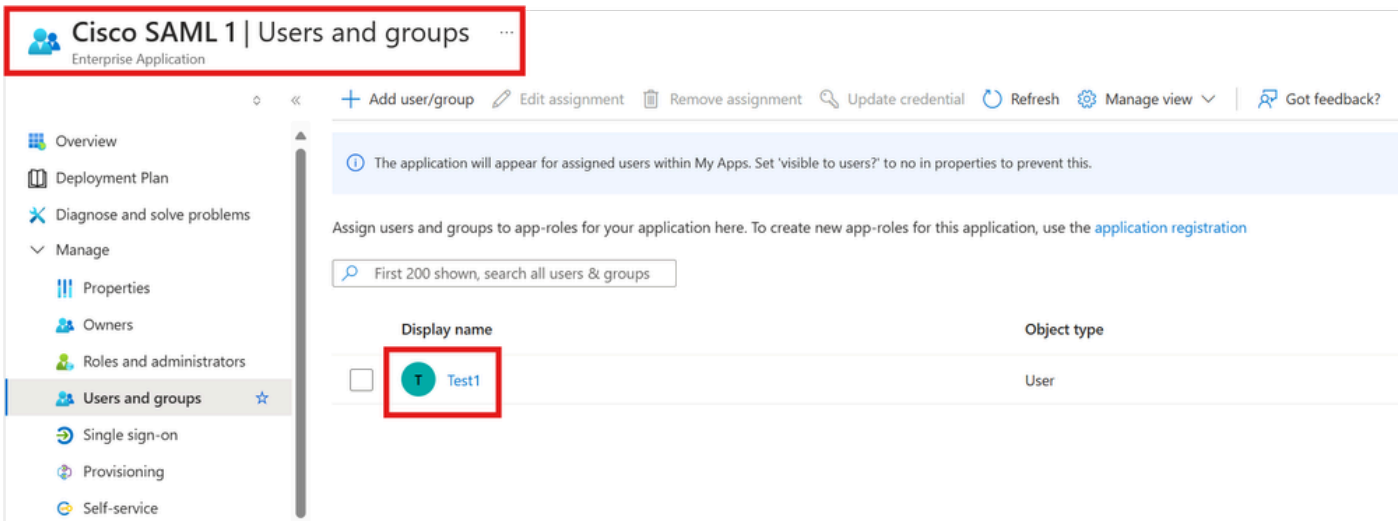


Agregar asignación 2



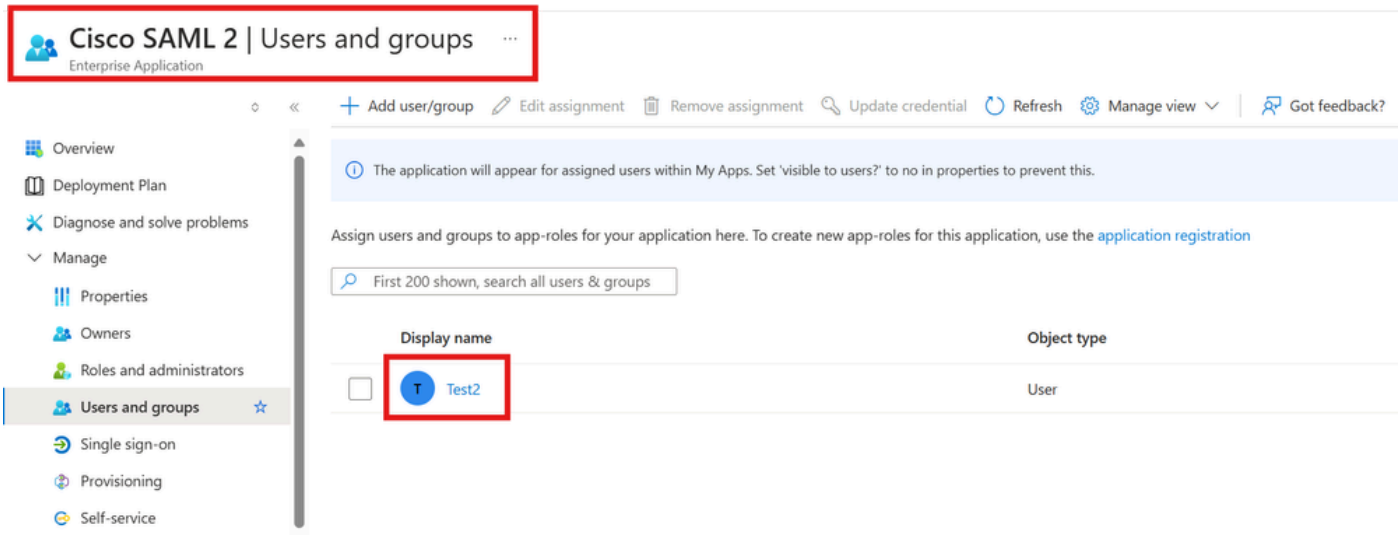
Asignación de usuario de prueba 2

Asignación de usuario de Test1:



Asignación de usuario de prueba 1

Asignación de usuario de Test2:



Asignación de usuario de prueba 2

Configuración de ASA mediante CLI

Paso 1. Crear puntos de confianza e importar certificados SAML.

Configure dos Trustpoints e importe los certificados SAML correspondientes para cada grupo de túnel.

<#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
```

Paso 2. Configure el IdP de SAML.

Utilice estos comandos para proveer la configuración de SAML IdP.

```
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
```

Paso 3. Aplique la autenticación SAML al primer grupo de túnel VPN.

Configure el grupo de túnel SAML1 con 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 (

Paso 4. Aplique la autenticación SAML al segundo grupo de túnel VPN.

Configure el grupo de túnel SAML2 con AzureAD-AC-SAML2 IdP trustpoint.

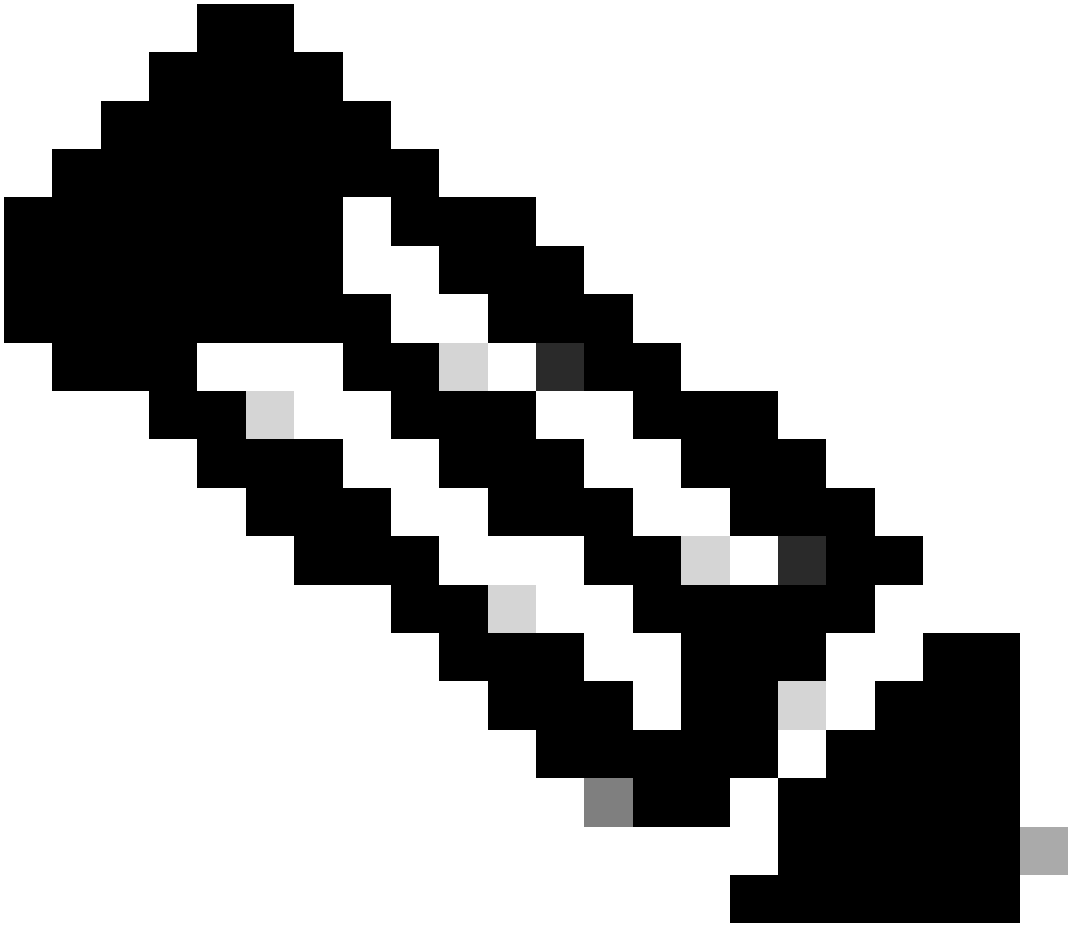
<#root>

```
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 (

Paso 5: Guarde la configuración.

```
write memory
```



Nota: Si realiza cambios en la configuración del IdP, debe quitar la configuración del proveedor de identidad SAML de su Grupo de Túnel y volver a aplicarla para que los cambios entren en vigencia.

Verificación

Pruebe AnyConnect con autenticación SAML.

Paso 1. Conéctese a la URL de VPN e ingrese sus datos de registro en Azure AD.

Paso 2. (Opcional) Aprobar solicitud de inicio de sesión.

Paso 3. AnyConnect está conectado.

Troubleshoot

La mayoría de los problemas de SAML implican un error de configuración que se puede encontrar cuando se verifica la configuración SAML o se ejecutan depuraciones. debug webvpn saml 255 se puede utilizar para resolver la mayoría de los problemas; sin embargo, en escenarios donde esta depuración no proporciona información útil, se pueden ejecutar depuraciones adicionales:

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

Información Relacionada

- Configuración de la VPN de AnyConnect de ASA con Microsoft Azure MFA a través de SAML
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).