Configurar vários grupos de túnel com SAML no ASA

Contents

Introdução

Este documento descreve a Autenticação SAML com o Provedor de Identidade do Azure para vários grupos de túneis no Cisco ASA.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Adaptive Security Appliance (ASA)
- SAML (Security Assertion Markup Language, Linguagem de marcação de asserção de segurança)
- Certificados SSL
- Microsoft Azure

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 9.22(1)1

- ID do Microsoft Azure Entra com SAML 2.0
- Cisco Secure Client 5.1.7.80

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Microsoft Azure pode oferecer suporte a vários aplicativos para a mesma ID de entidade. Cada aplicativo (mapeado para um grupo de túneis diferente) requer um certificado exclusivo. No ASA, vários grupos de túneis podem ser configurados para usar diferentes aplicativos protegidos por IdP (Override Identity Provider) devido ao recurso de certificado IdP. Este recurso permite que os administradores substituam o certificado IdP primário no objeto do Servidor de Signon Único (SSO) por um certificado IdP específico para cada grupo de túneis. Esse recurso foi introduzido no ASA a partir da versão 9.17.1.

SSO Iniciado por SP SAML

Quando o usuário final inicia o login acessando o ASA, o comportamento de login continua como:

1. Quando o usuário da VPN acessa ou escolhe um grupo de túneis habilitado para SAML, o usuário final é redirecionado para o SAML IdP para autenticação. O usuário é avisado, a menos que acesse a url do grupo diretamente, caso em que o redirecionamento é silencioso.

2. O ASA gera uma Solicitação de Autenticação SAML, que o navegador redireciona para o IdP SAML.

3. O IdP desafia o usuário final quanto à credencial e o usuário final faz login. As credenciais inseridas devem atender à configuração de autenticação do IdP.

4. A Resposta IdP é enviada de volta ao navegador e publicada na URL de entrada do ASA. O ASA verifica a resposta para concluir o login.

Configurações

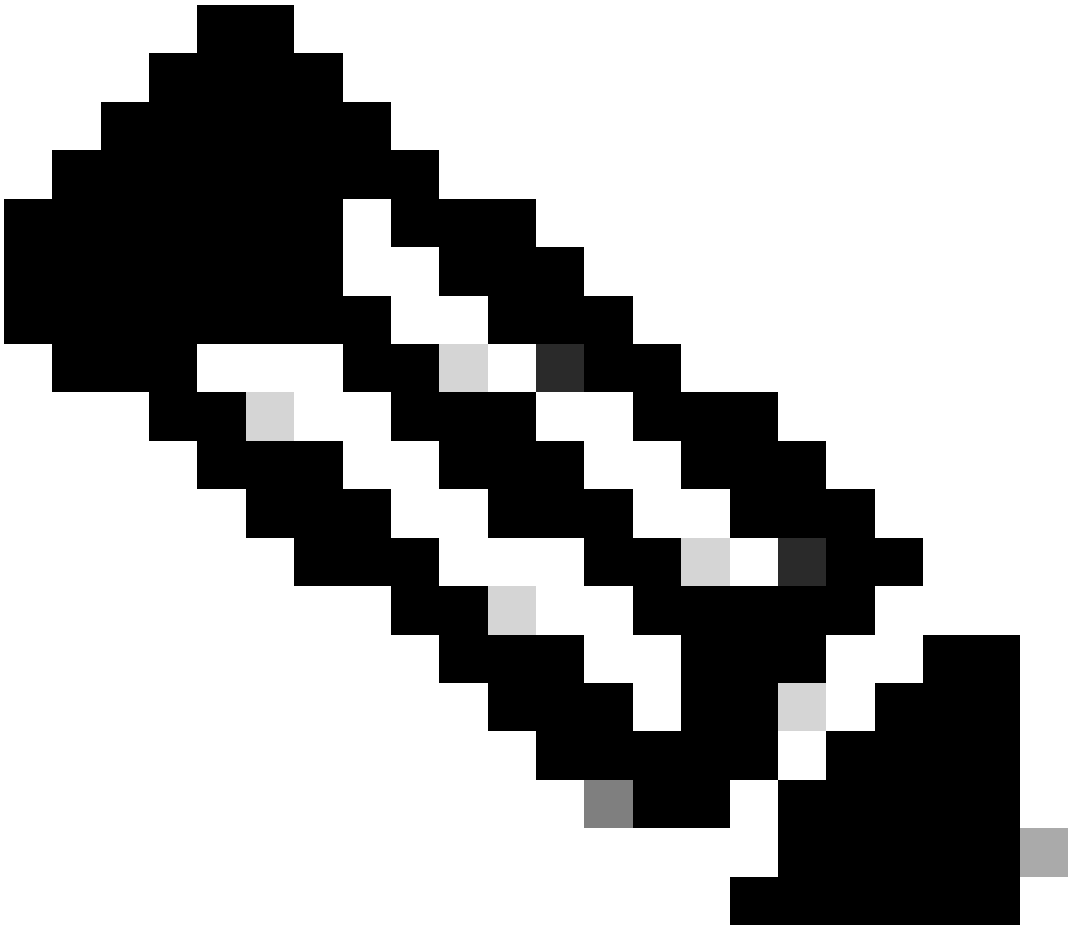
Adicione o Cisco Secure Firewall - Secure Client da galeria

Neste exemplo, a integração do Microsoft Entra SSO com o Cisco Secure Firewall - Secure Client no Azure foi adicionada para dois grupos de túneis configurados no ASA:

- SAML1
- SAML2

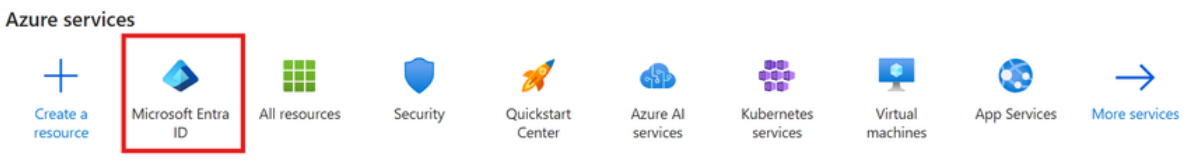
Para configurar a integração do Cisco Secure Firewall - Secure Client no Microsoft Entra ID, você

precisa adicionar o Cisco Secure Firewall - Secure Client da galeria à sua lista de aplicativos SaaS gerenciados.



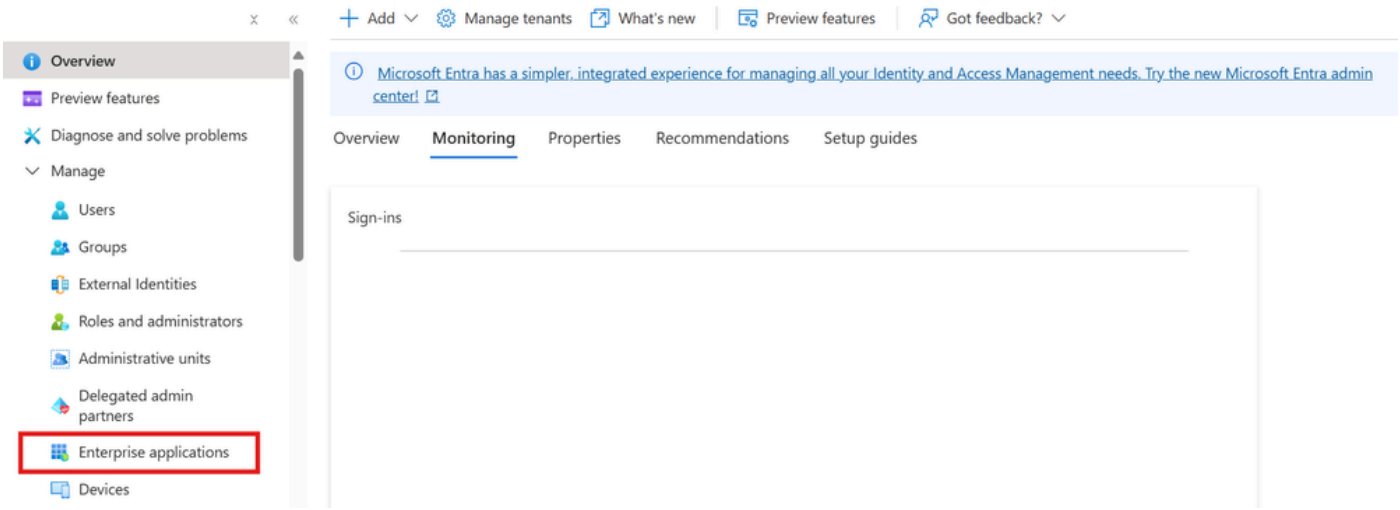
Note: Estas etapas destinam-se a adicionar o Cisco Secure Firewall - Secure Client à galeria para o primeiro grupo de túneis, SAML1.

Etapa 1. Faça logon no Portal do Azure e escolha a ID do Microsoft Entra.



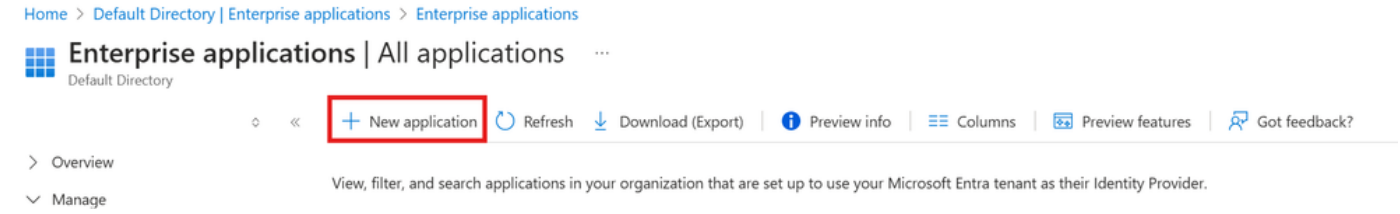
ID do Microsoft Entra

Etapa 2. Como mostrado nesta imagem, escolha Aplicações Empresariais.



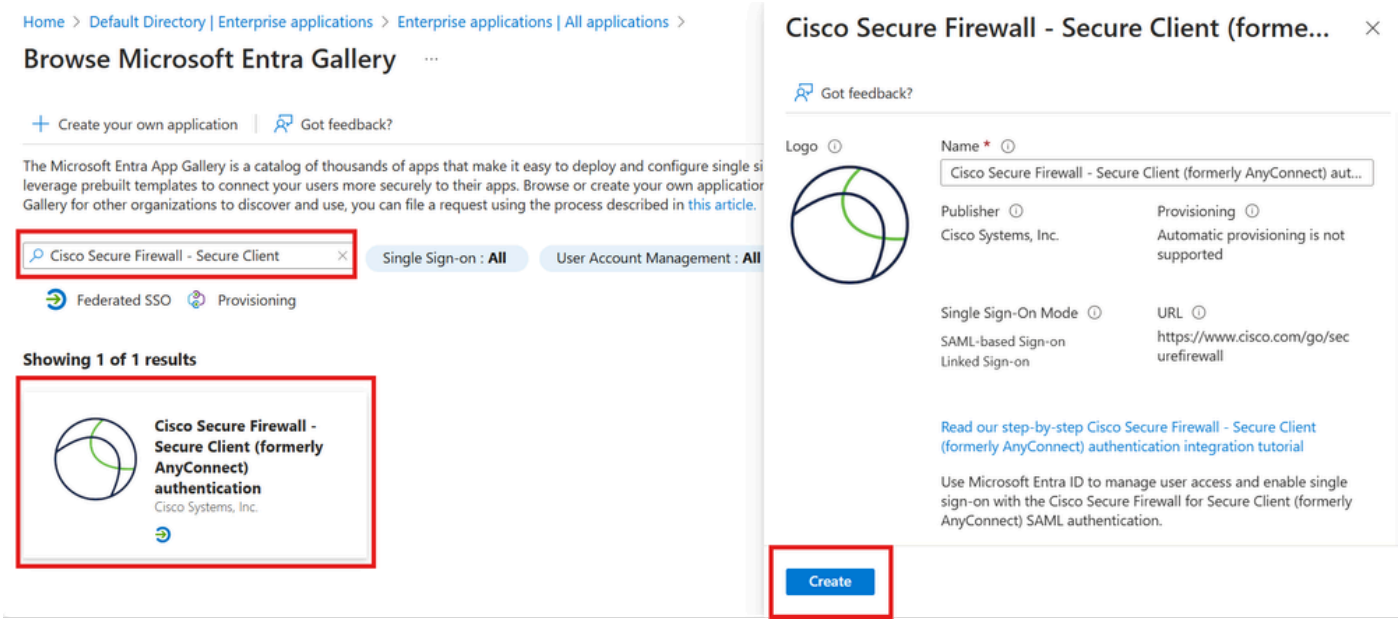
Aplicativo empresarial

Etapa 3. Agora, escolha New Application, como mostrado nesta imagem.

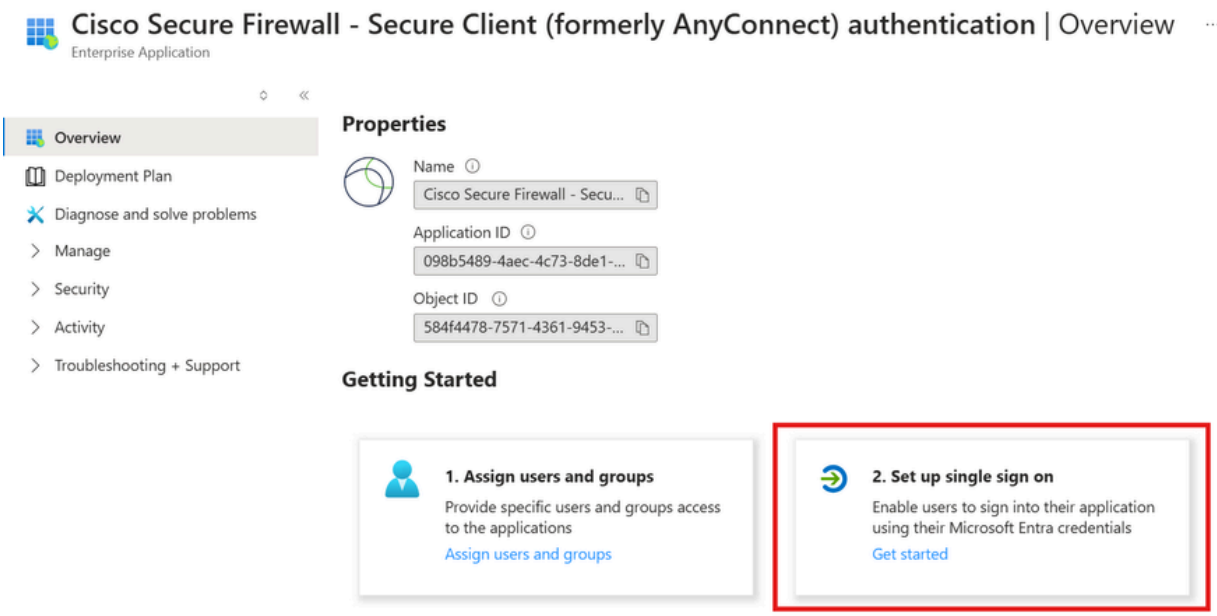


Novo aplicativo

Etapa 4. Na seção Add from the gallery, digite Cisco Secure Firewall - Secure Client na caixa de pesquisa, escolha Cisco Secure Firewall - Secure Client no painel de resultados e, em seguida, adicione o aplicativo.

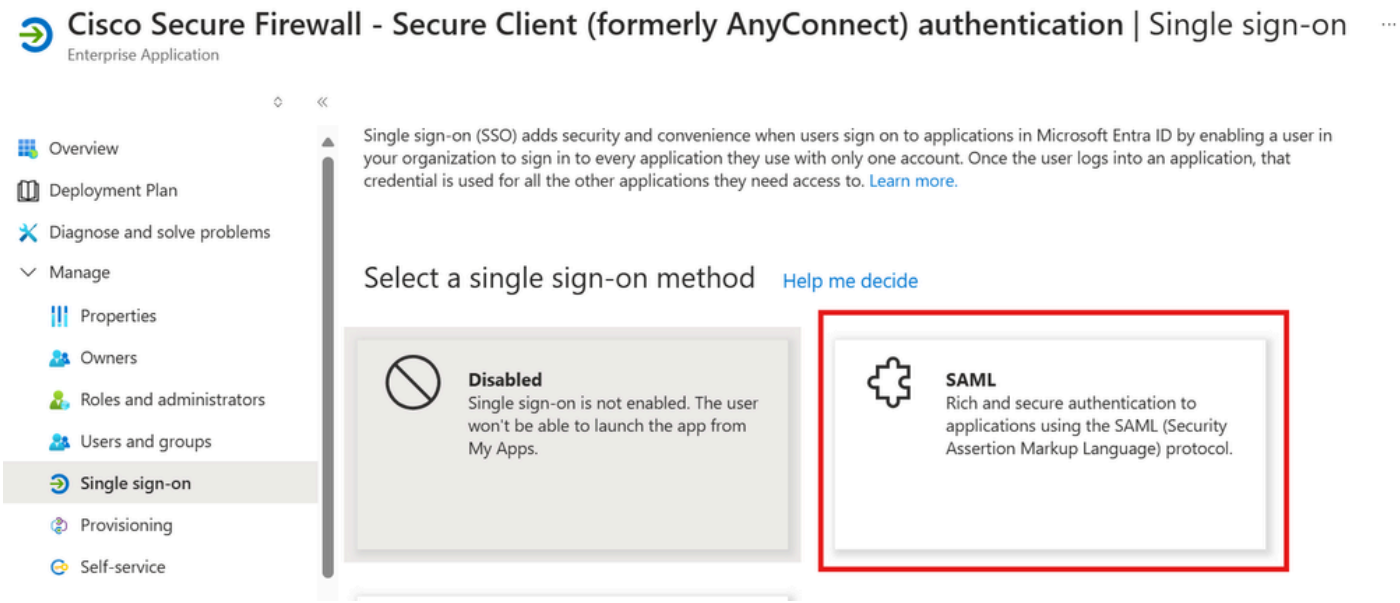


Etapa 5. Escolha o item de menu Sign-on único, como mostrado nesta imagem.



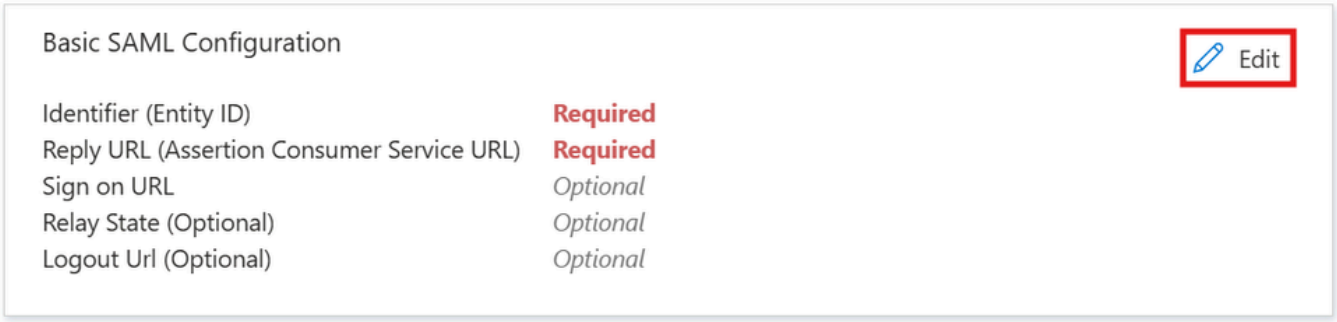
Configurar Logon Único

Etapa 6. Na página Selecionar um método de logon único, escolhaSAML.



SAML

Etapa 7. Na página Configurar logon único com SAML, clique no ícone editar/abrir da Configuração SAML Básica para editar as configurações.



Configuração Saml Básica

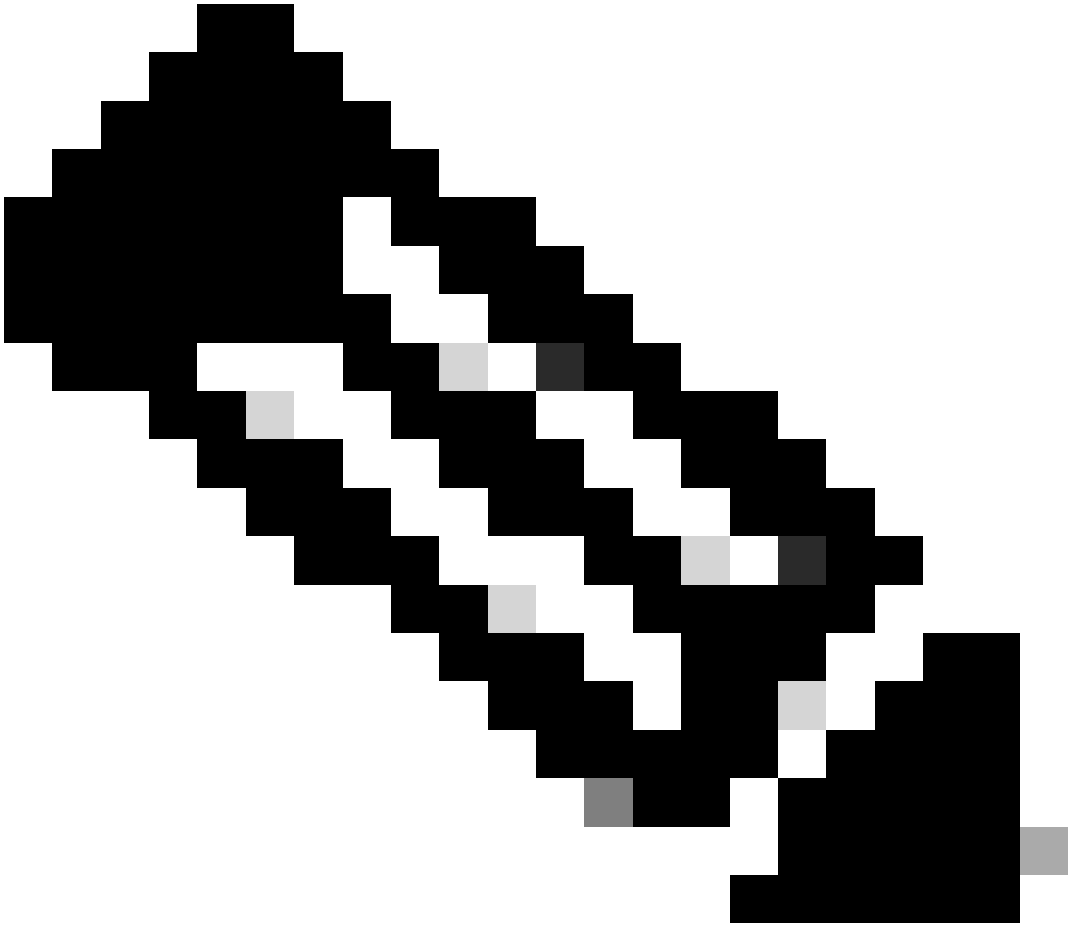
Etapa 8. Na página Configurar logon único com SAML, digite os valores para estes campos:

a. Na caixa de textoIdentificador, digite um URL usando este padrão:

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

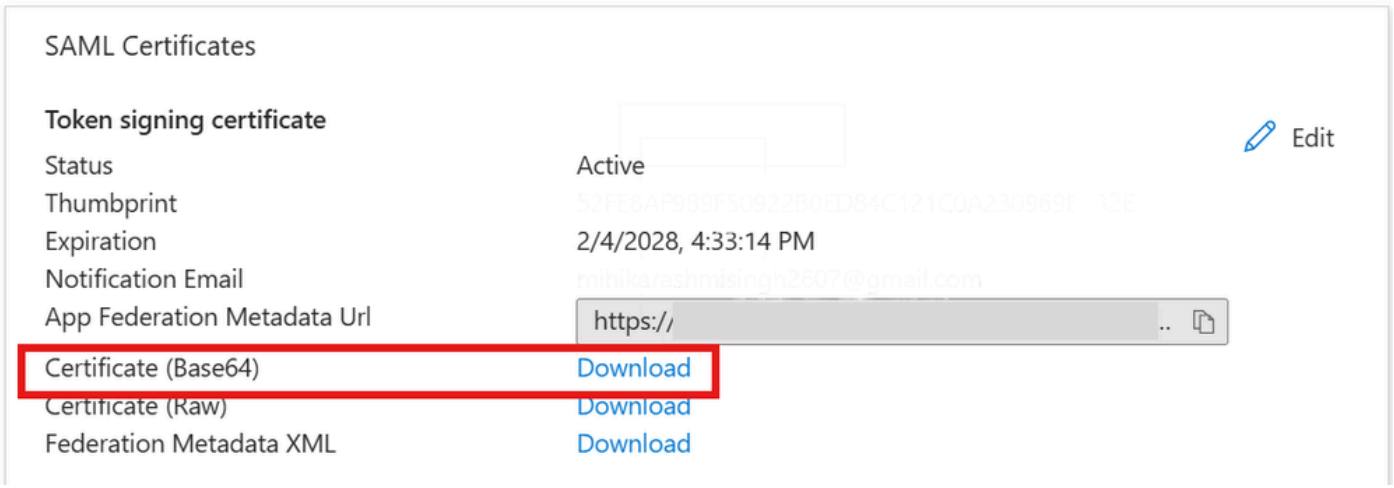
b. Na caixa de texto URL de resposta, digite uma URL usando este padrão:

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

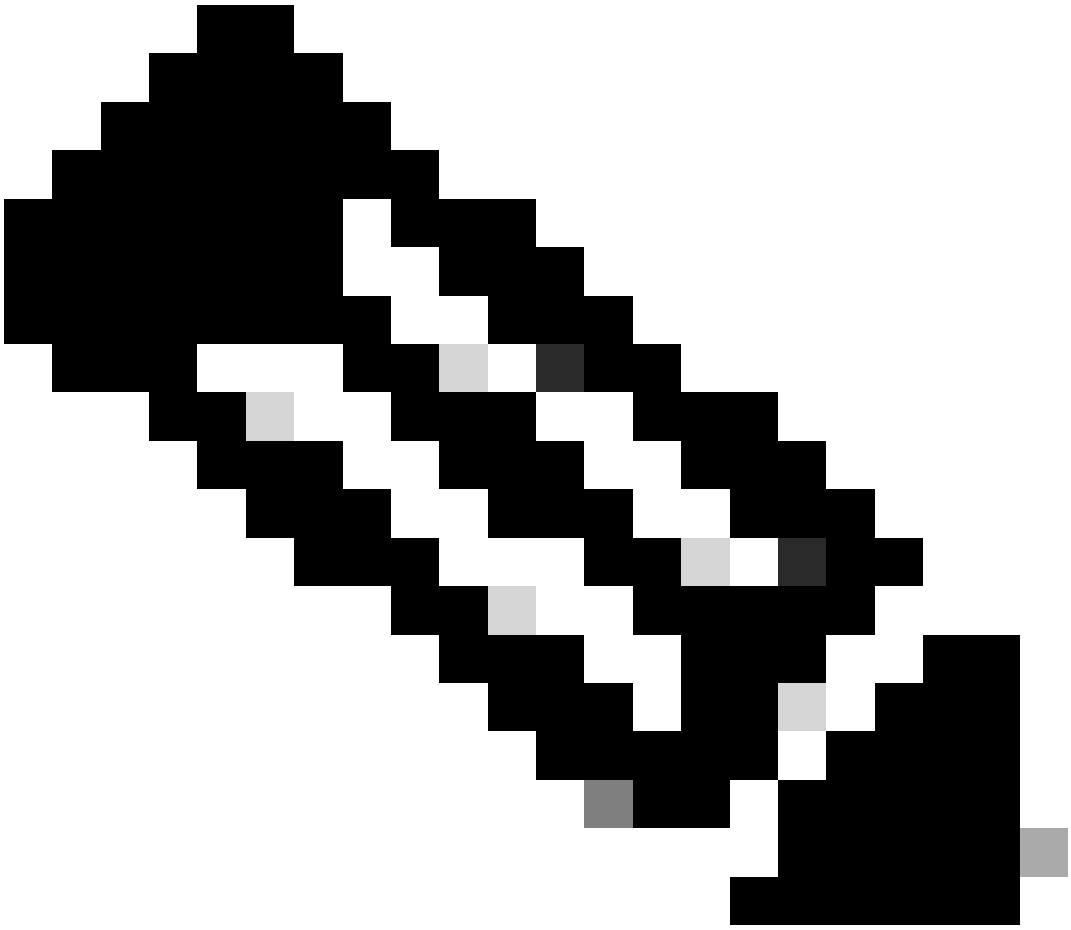


Note: Tunnel_Group_Name diferencia maiúsculas de minúsculas e o valor não deve conter pontos '.' e barras '/'.

Etapa 9. Na página Configurar logon único com SAML, na seção Certificado de assinatura SAML, localize Certificado (Base64) e escolha Download para baixar o arquivo de certificado e salvá-lo no computador.



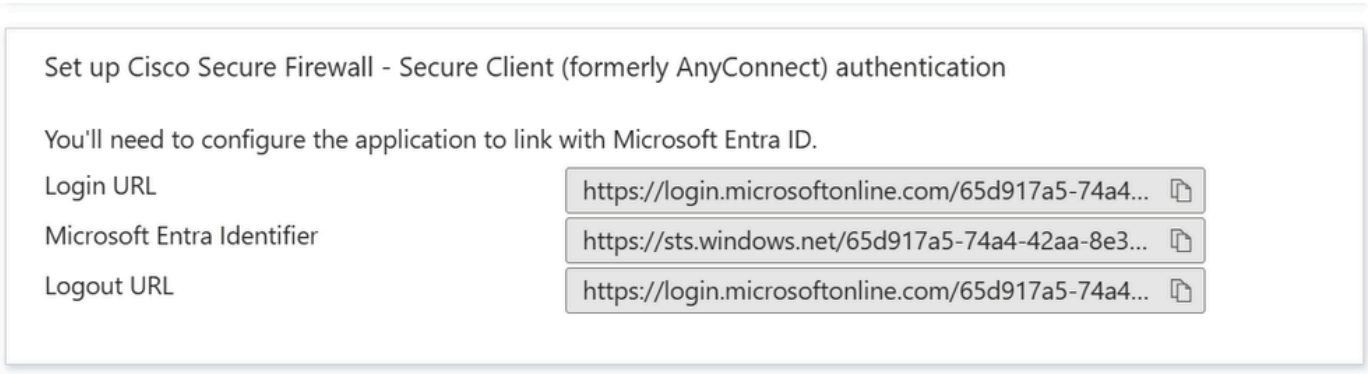
Download do certificado (Base64)



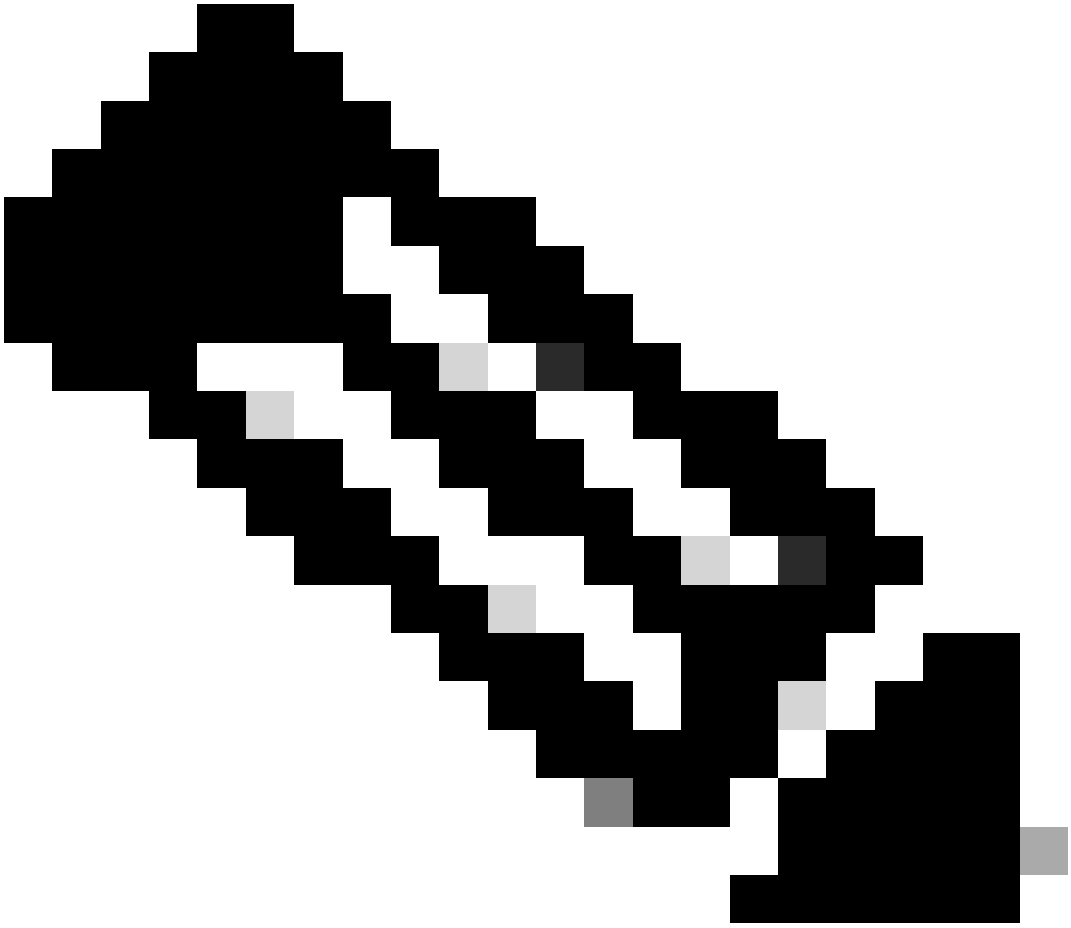
Observação: este certificado baixado é importado para o ponto confiável do ASA AzureAD-AC-SAML1. Consulte a seção Configuração do ASA para obter mais detalhes.

Etapa 10. Na seção Configuração do Cisco Secure Firewall - Cliente Seguro, copie os URLs apropriados com base em seu requisito. Esses URLs são usados para configurar o objeto do Servidor SSO no ASA.

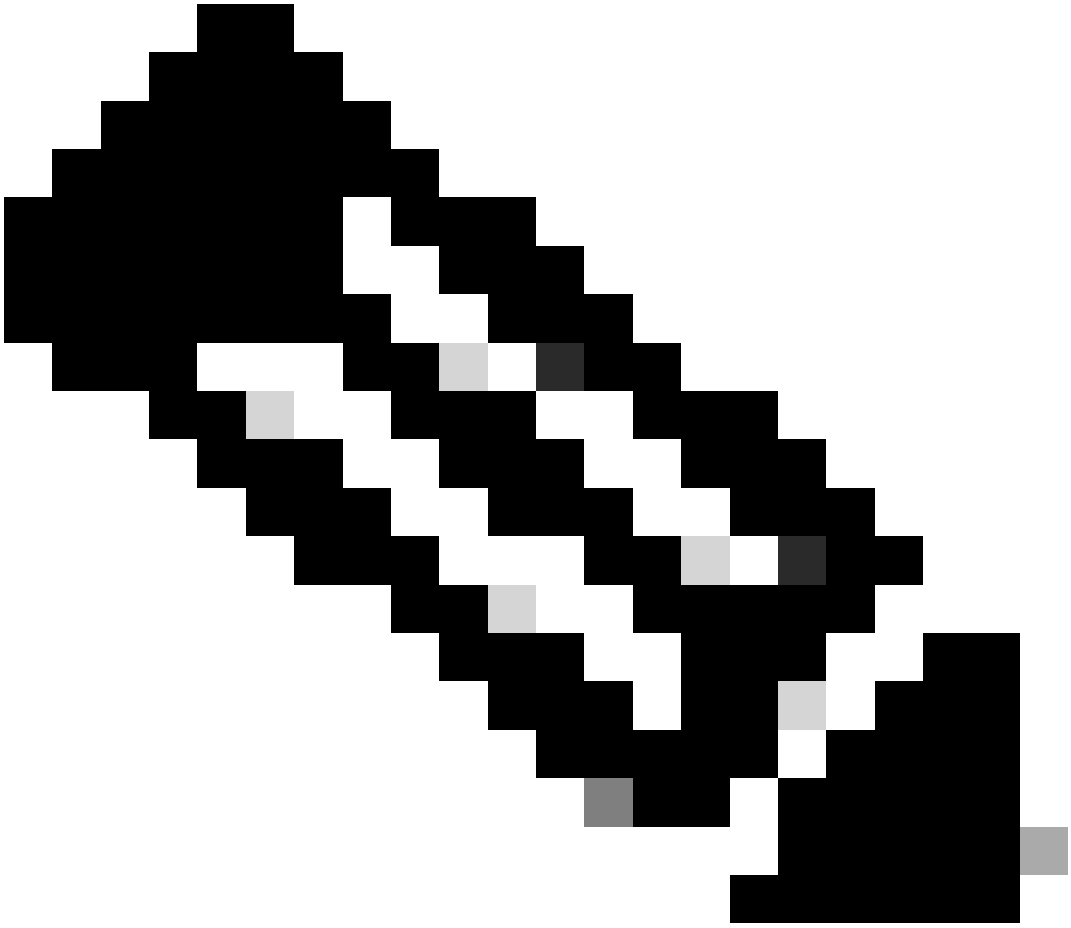
- Microsoft Entra Identifier - Este é o IDP SAML na configuração da VPN.
- URL de login - É a URL de entrada.
- URL de logoff - É o URL de saída.



URL SSO



Note: Repita as etapas de configuração anteriores para adicionar o aplicativo Cisco Secure Firewall - Secure Client da galeria para o segundo grupo de túnel. O segundo nome do grupo de túneis, nesse caso, é SAML2.



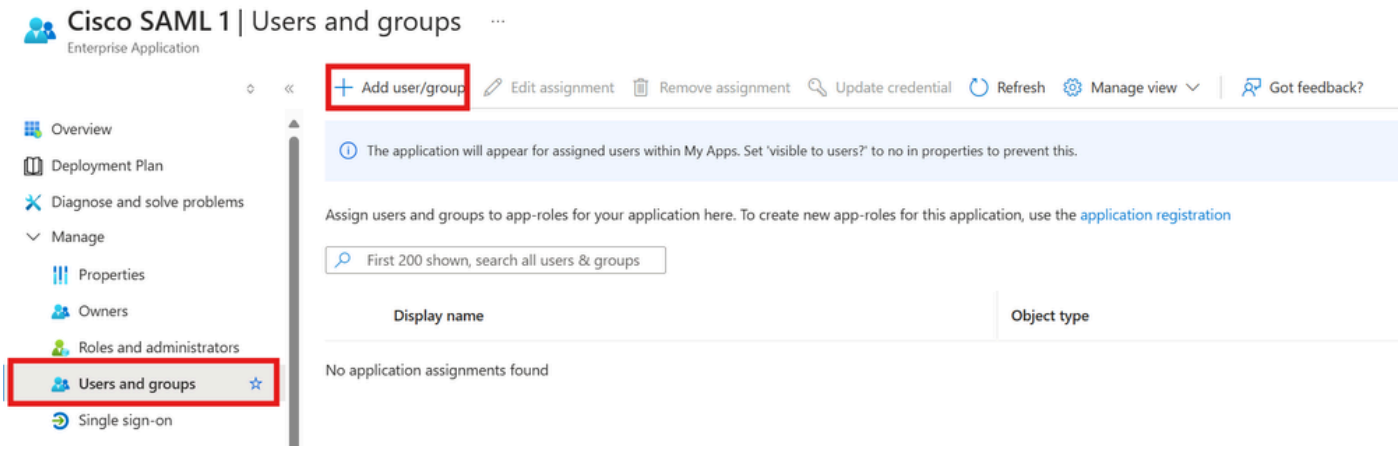
Observação: ao adicionar o aplicativo Cisco Secure Firewall - Secure Client para o segundo grupo de túneis (SAML 2), o certificado do Azure baixado na Etapa 8. é importado para o ASA trustpoint AzureAD-AC-SAML2.

Atribuir usuários do Azure AD ao aplicativo

Nesta seção, Test1 e Test2 está habilitado para usar o SSO do Azure, à medida que você concede acesso ao aplicativo Cisco Secure Client.

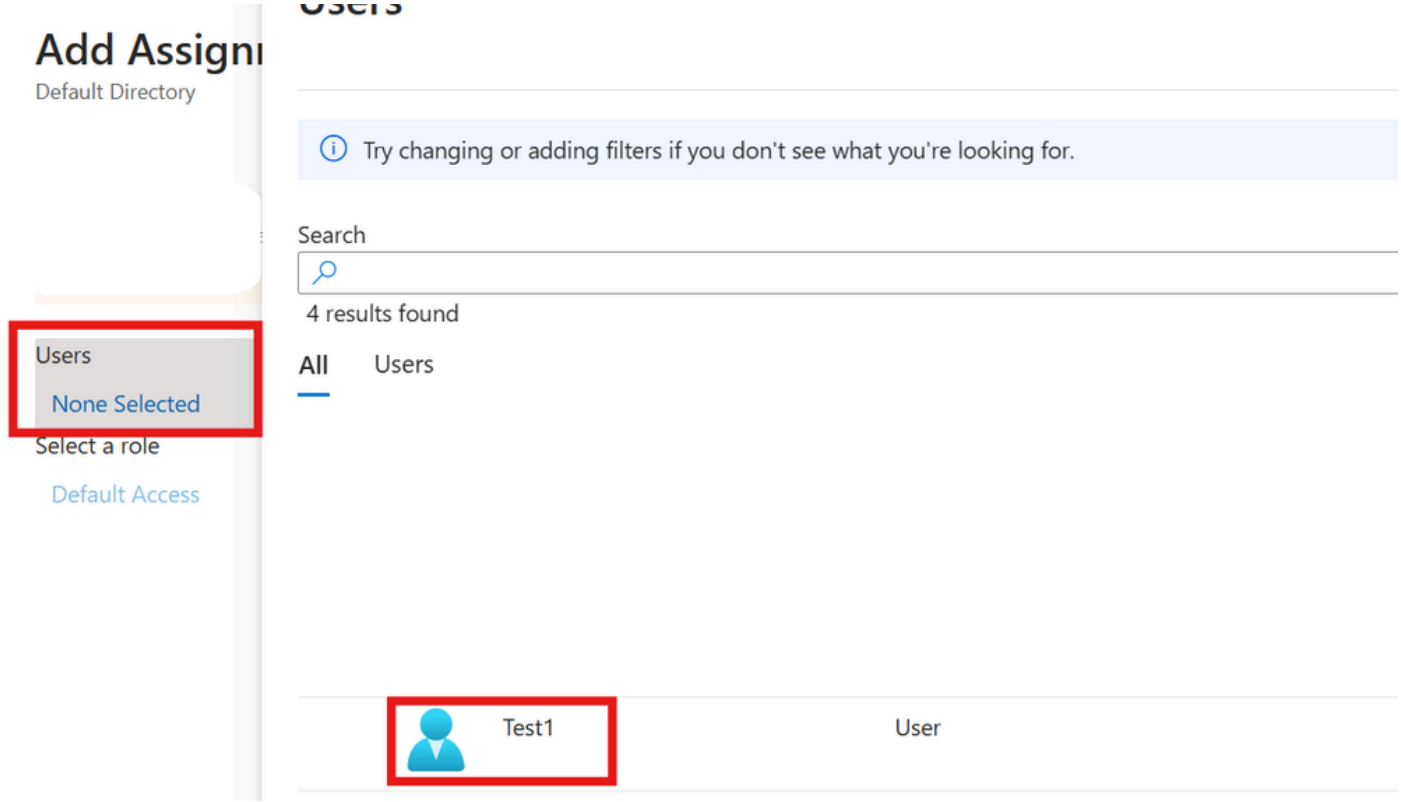
Para o primeiro aplicativo IdP:

Etapa 1. Na primeira página de visão geral do aplicativo IdP, escolha Users and groups e, em seguida, Add user.



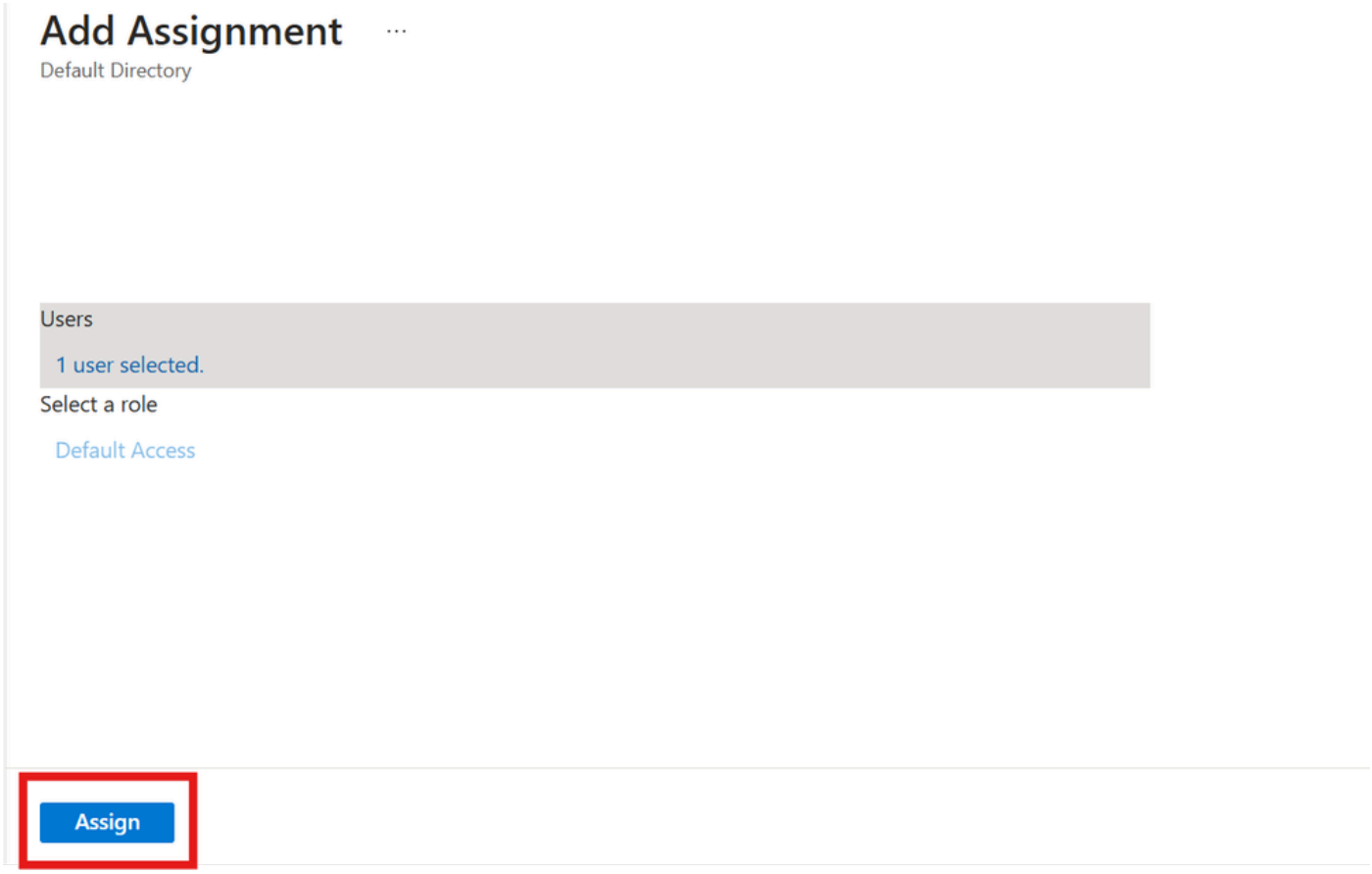
Usuário e Grupos

Etapa 2. Escolha Usuários ou grupos na caixa de diálogo Adicionar tarefa.



Adicionar tarefa 1

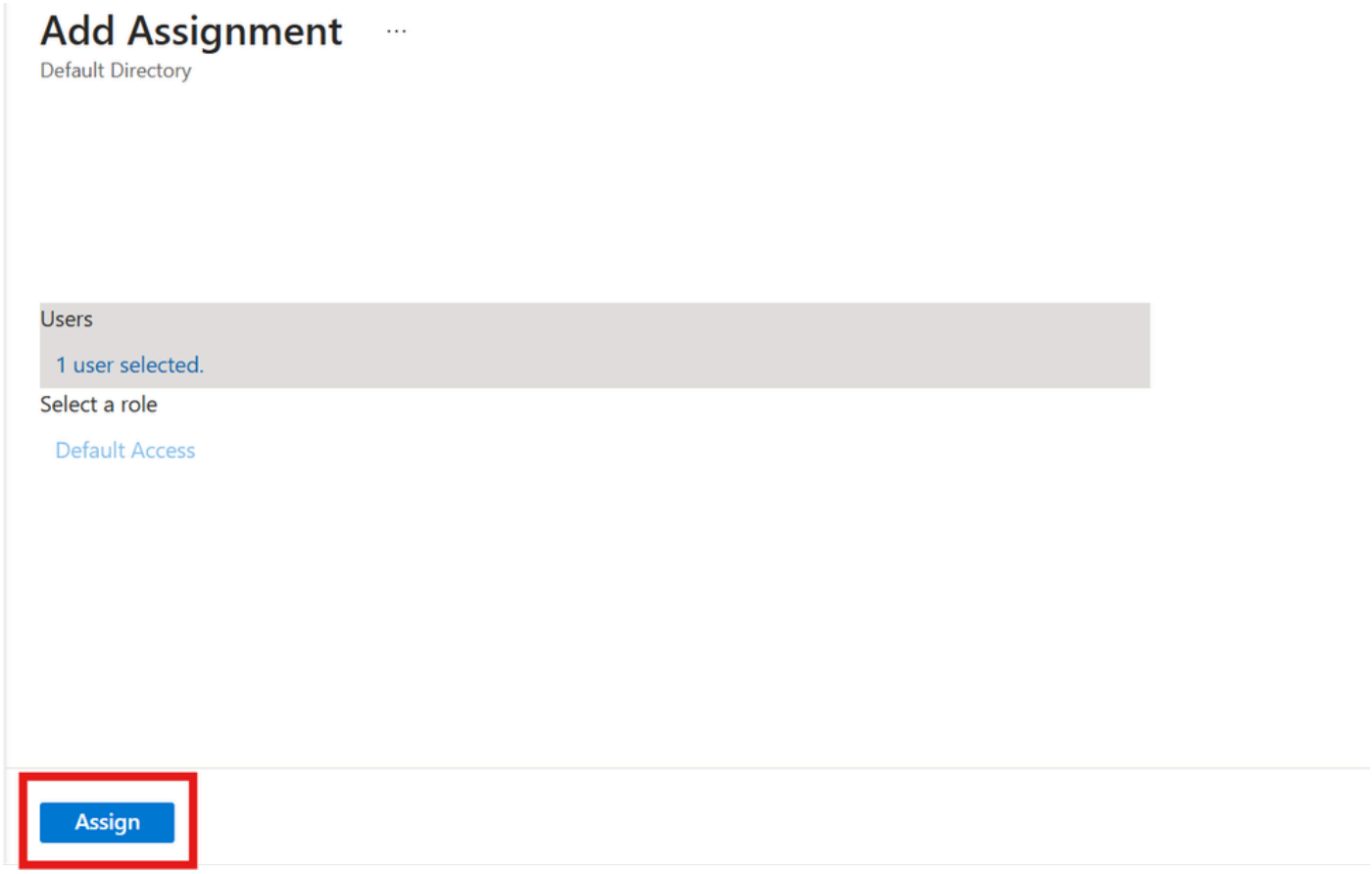
Etapa 3. Na caixa de diálogo Add Assignment, clique no botão Assign.



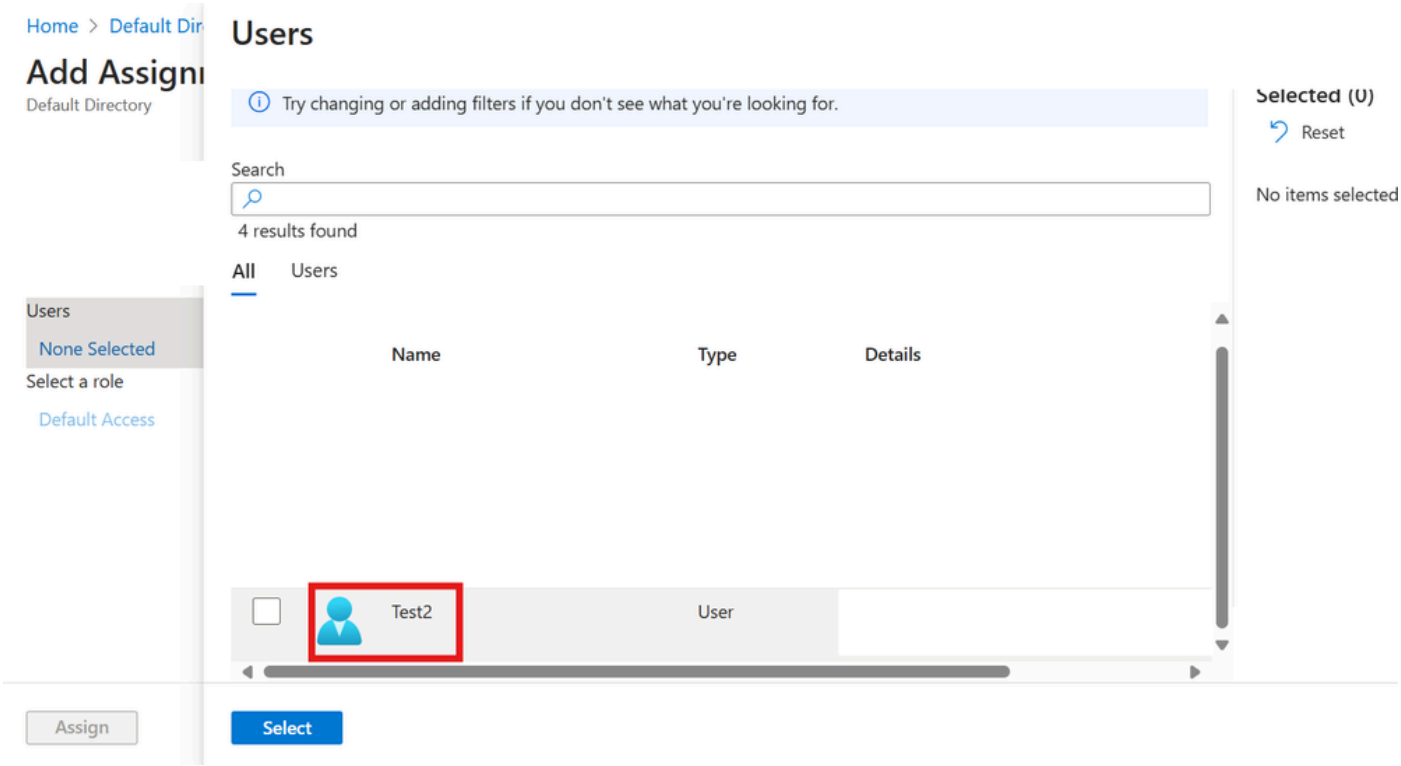
Atribuição de Usuário Test1

Para o segundo aplicativo IdP:

Repita as etapas anteriores para o Second Idp Application conforme mostrado nessas imagens.

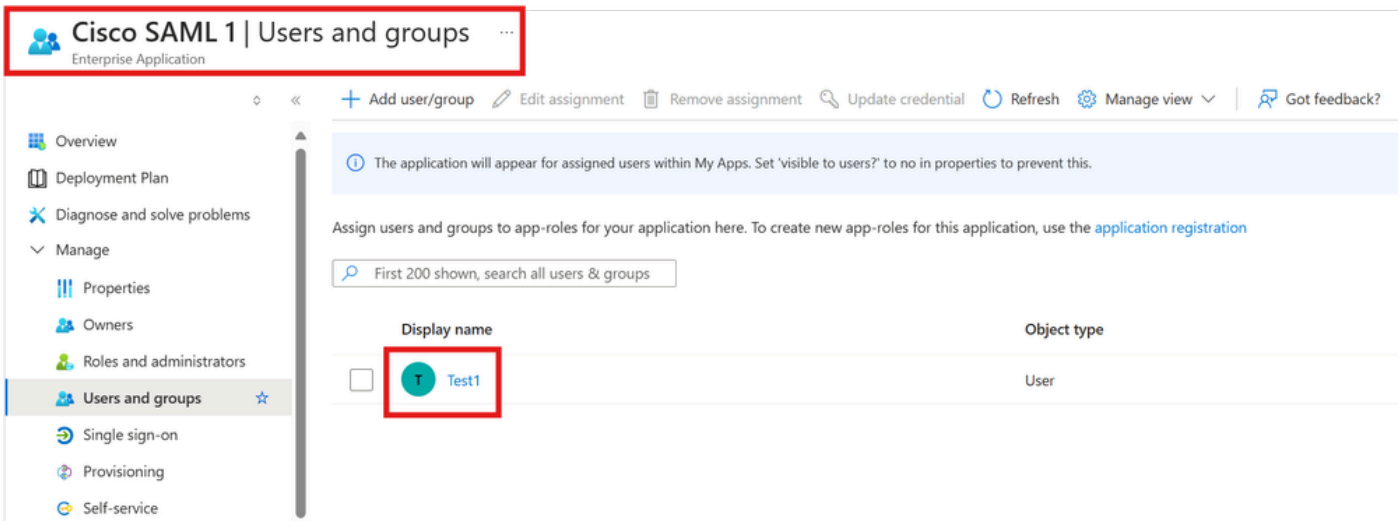


Adicionar tarefa 2



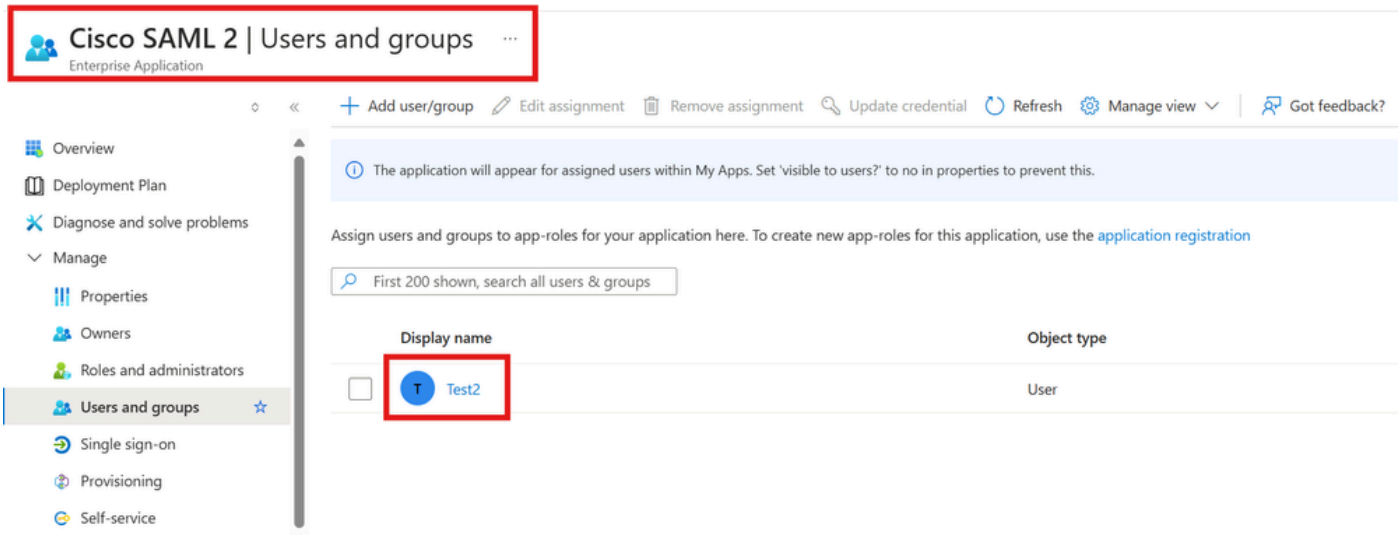
Atribuição de Usuário Test2

Atribuição de usuário de Test1:



Teste 1 atribuição de usuário

Atribuição de Usuário de Teste2:



Atribuição de usuário do teste 2

Configuração do ASA via CLI

Etapa 1. Criar pontos confiáveis e importar certificados SAML.

Configure dois pontos confiáveis e importe os respectivos certificados SAML 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
```

Etapa 2. Configurar o SAML IdP.

Use estes comandos para provisionar as configurações de IdP 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
```

Etapa 3. Aplique a autenticação SAML ao primeiro grupo de túneis VPN.

Configure o grupo de túneis SAML1 com o ponto de confiança IdP do AzureAD-AC-SAML1.

<#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 (

Etapa 4. Aplicar a autenticação SAML ao segundo grupo de túneis VPN.

Configure o grupo de túneis SAML2 com o ponto de confiança IdP do AzureAD-AC-SAML2.

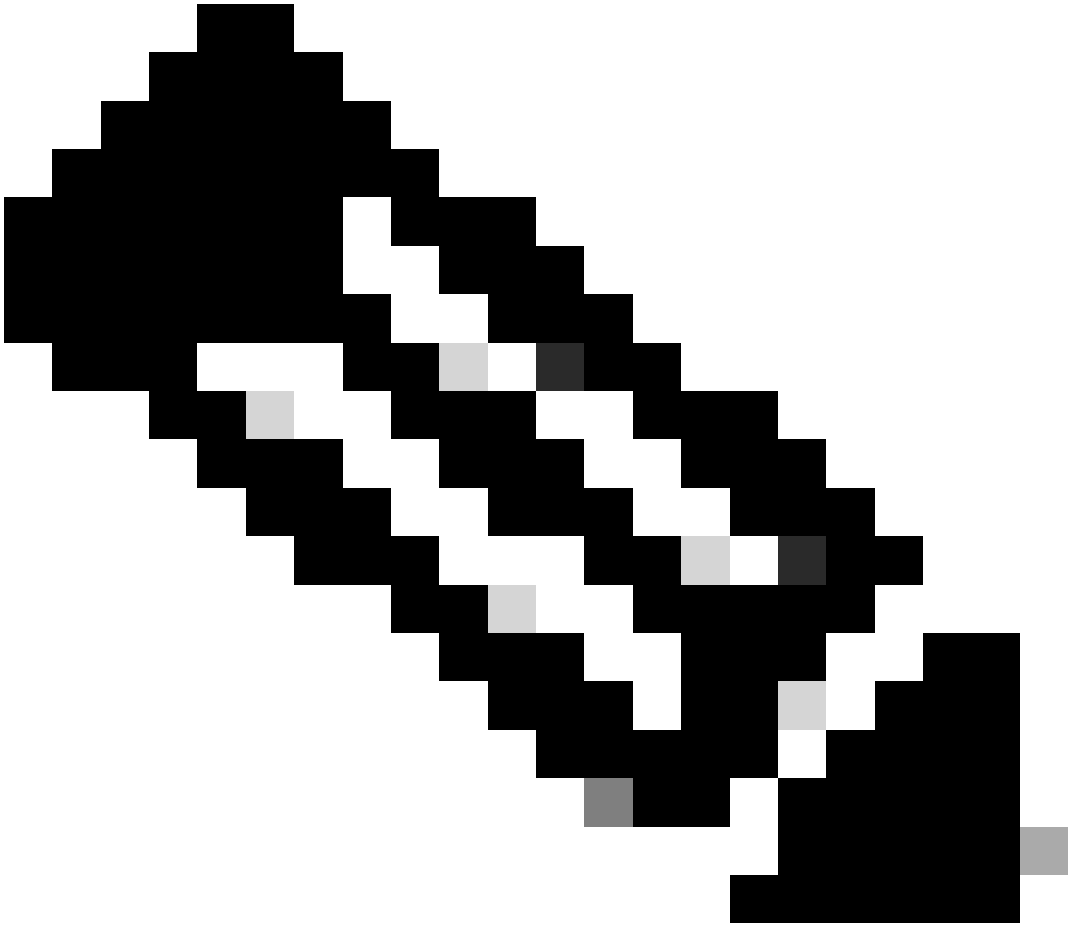
<#root>

```
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 (

Passo 5: Salve a configuração.

```
write memory
```



Note: Se você fizer alterações na configuração do IdP, precisará remover a configuração do provedor de identidade SAML do Grupo de Túneis e reaplicá-la para que as alterações entrem em vigor.

Verificar

Teste o AnyConnect com autenticação SAML.

Etapa 1. Conecte à sua URL VPN e insira seu log em detalhes do Azure AD.

Etapa 2. (Opcional) Aprovar solicitação de entrada.

Etapa 3. O AnyConnect está conectado.

Troubleshooting

A maioria das soluções de problemas SAML envolve uma configuração incorreta que pode ser encontrada quando a configuração SAML é verificada ou quando depurações são executadas. debug webvpn saml 255 pode ser usado para solucionar a maioria dos problemas, no entanto, em cenários onde essa depuração não fornece informações úteis, depurações adicionais podem ser executadas:

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

Informações Relacionadas

- Configurar ASA AnyConnect VPN com Microsoft Azure MFA usando o SAML
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.