Configurar o SSO para SD-WAN usando a ID do Microsoft Entra

Contents

Introdução

Este documento descreve como configurar o Single Sign-On (SSO) para Cisco Catalyst Software-Defined Wide-Area Networks (SD-WAN) com o Microsoft Entra ID.

Pré-requisitos

Requisitos

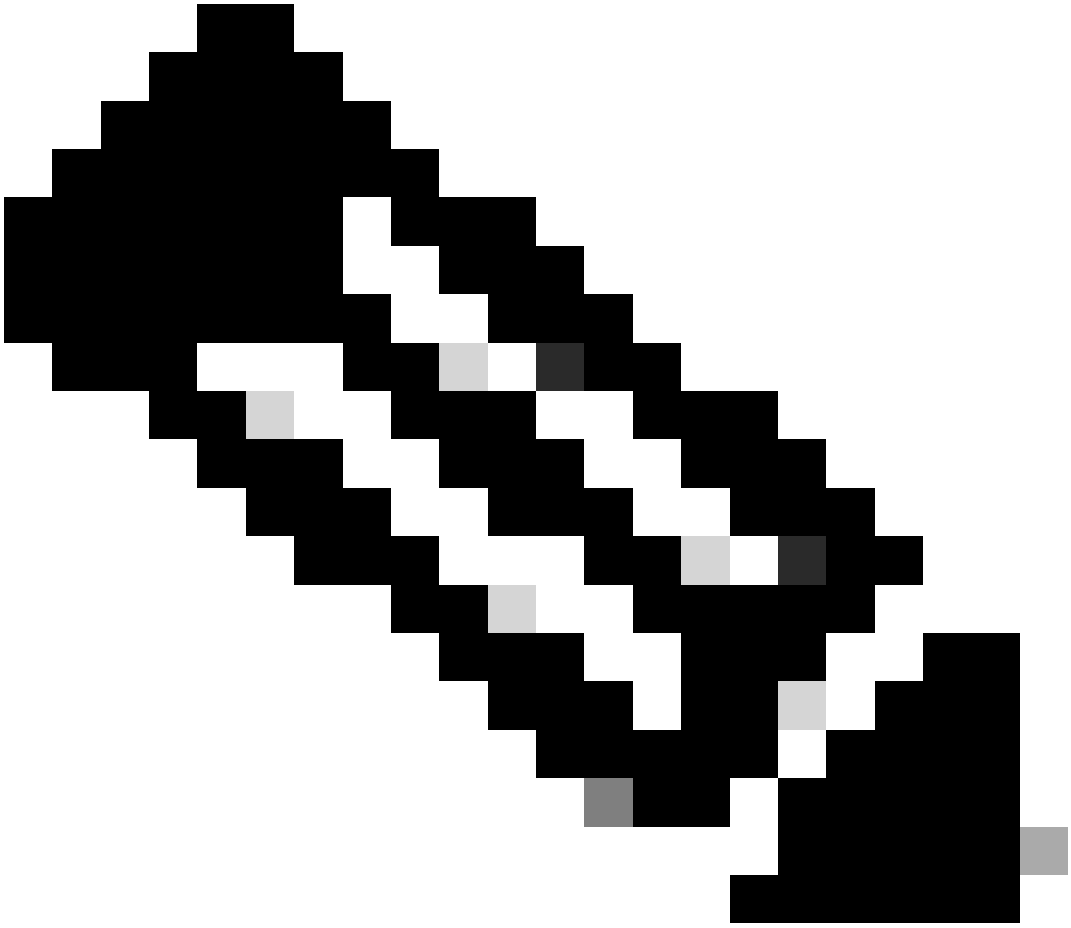
A Cisco recomenda que você tenha conhecimento geral sobre estes tópicos:

- Logon único
- Solução Cisco Catalyst SD-WAN

Componentes Utilizados

As informações neste documento são baseadas em:

- Cisco Catalyst SD-WAN Manager versão 20.15.3.1
- ID do Microsoft Entra



Note: A solução anteriormente conhecida como Azure Ative Diretory (Azure AD) agora é chamada de Microsoft Entra ID.

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 Logon Único é um método de autenticação que permite que os usuários acessem com segurança vários aplicativos ou sites independentes usando um único conjunto de credenciais. Com o SSO, os usuários não precisam mais entrar separadamente em cada aplicativo — depois de autenticados, eles podem acessar perfeitamente todos os recursos permitidos.

Uma maneira comum de implementar o SSO é por meio da federação, que estabelece a confiança entre um provedor de identidade (IdP) e um provedor de serviços (SP) usando

protocolos como SAML 2.0, WS-Federation ou OpenID Connect. A federação melhora a segurança, a confiabilidade e a experiência do usuário centralizando a autenticação.

O Microsoft Entra ID é um provedor de identidade baseado em nuvem amplamente usado que oferece suporte a esses protocolos de federação. Em uma configuração de SSO com o Cisco Catalyst SD-WAN, o ID do Microsoft Entra atua como o IdP e o Cisco SD-WAN Manager atua como o provedor de serviços.

A integração funciona da seguinte forma:

1. Um administrador de rede tenta fazer login no Cisco SD-WAN Manager.
2. O Cisco SD-WAN Manager envia uma solicitação de autenticação ao Microsoft Entra ID.
3. O Entra ID da Microsoft solicita que o administrador autentique com sua conta do Entra ID (Microsoft).
4. Quando as credenciais forem validadas, o Microsoft Entra ID enviará uma resposta segura de volta ao Cisco SD-WAN Manager confirmando a autenticação.
5. O Cisco SD-WAN Manager concede acesso sem exigir credenciais separadas.

Neste modelo:

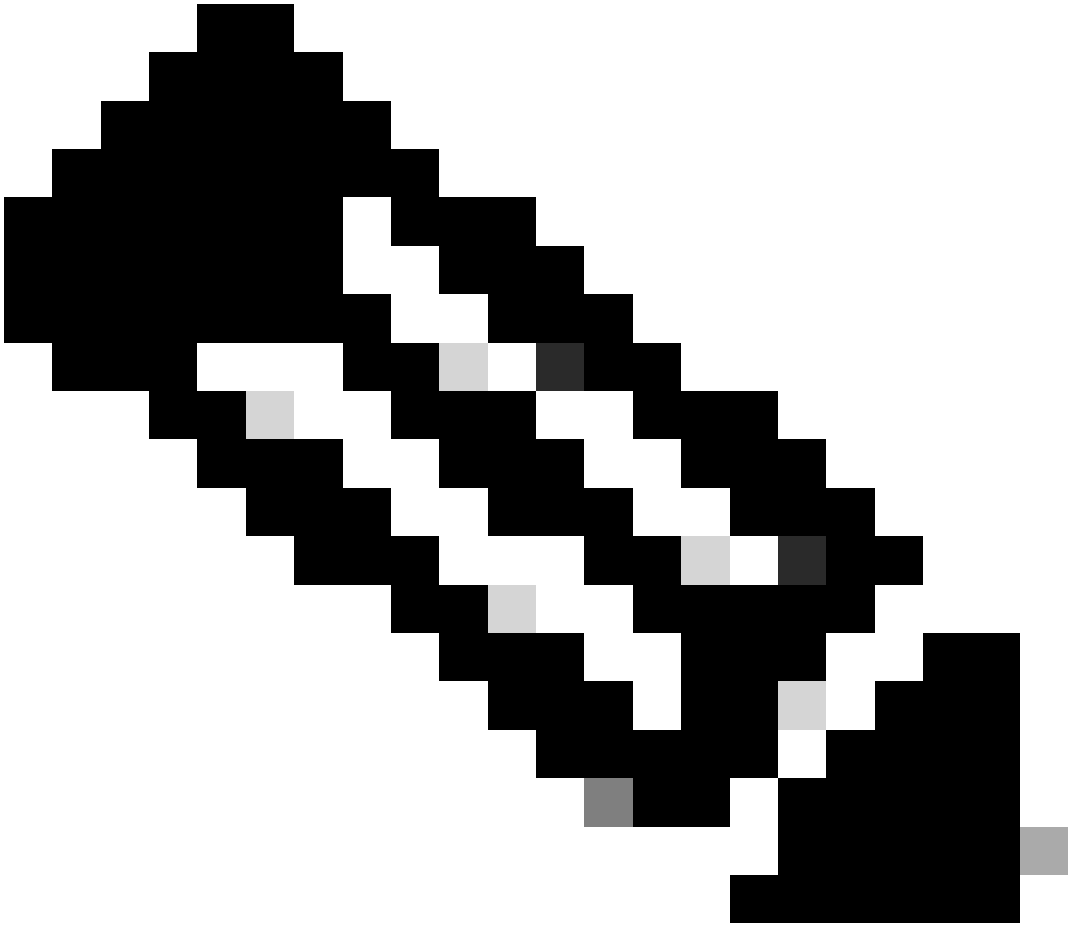
- Provedor de identidade (IdP) - Armazena dados do usuário, valida credenciais (por exemplo, Microsoft Entra ID, Okta, PingID, ADFS).
- Provedor de serviços - hospeda o aplicativo a ser acessado (por exemplo, Cisco SD-WAN Manager).
- Usuários - Possuem uma conta no diretório IdP e estão autorizados a acessar o provedor de serviços.

O Cisco Catalyst SD-WAN é compatível com qualquer IdP compatível com SAML 2.0 quando configurado de acordo com os padrões do setor.

Benefícios do uso do logon único

- Centraliza o gerenciamento de credenciais por meio do Provedor de identidade.
- Fortalece a segurança de autenticação, eliminando várias senhas fracas.
- Simplifica o acesso seguro para administradores.
- Permite o acesso com um clique ao Cisco Catalyst SD-WAN Manager e a outros aplicativos autorizados.

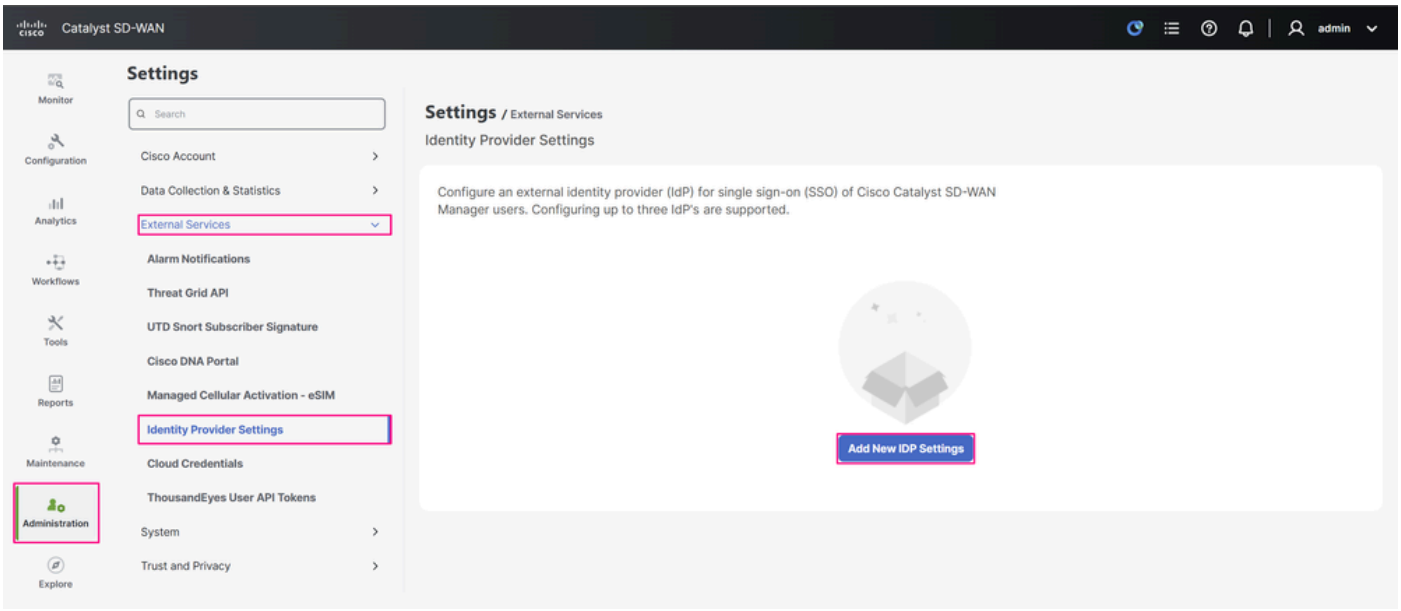
Configurar



Note: Versão mínima suportada: Cisco Catalyst SD-WAN Manager versão 20.8.1.

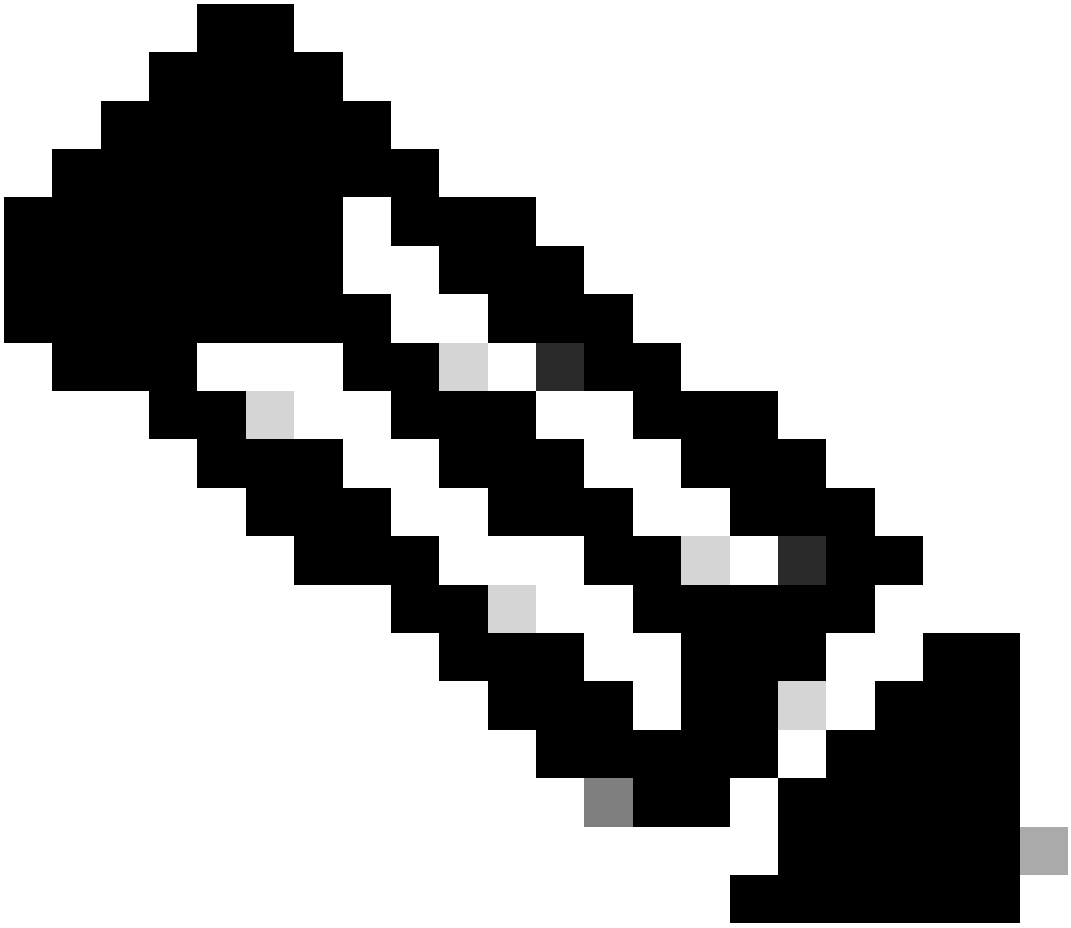
Etapa 1. Obter os metadados SAML do Cisco SD-WAN Manager

- No Cisco SD-WAN Manager, navegue para Administration > Settings > External Services > Identity Provider Settings e clique em Add New IDP Settings.



Interface do usuário do Cisco SD-WAN Manager

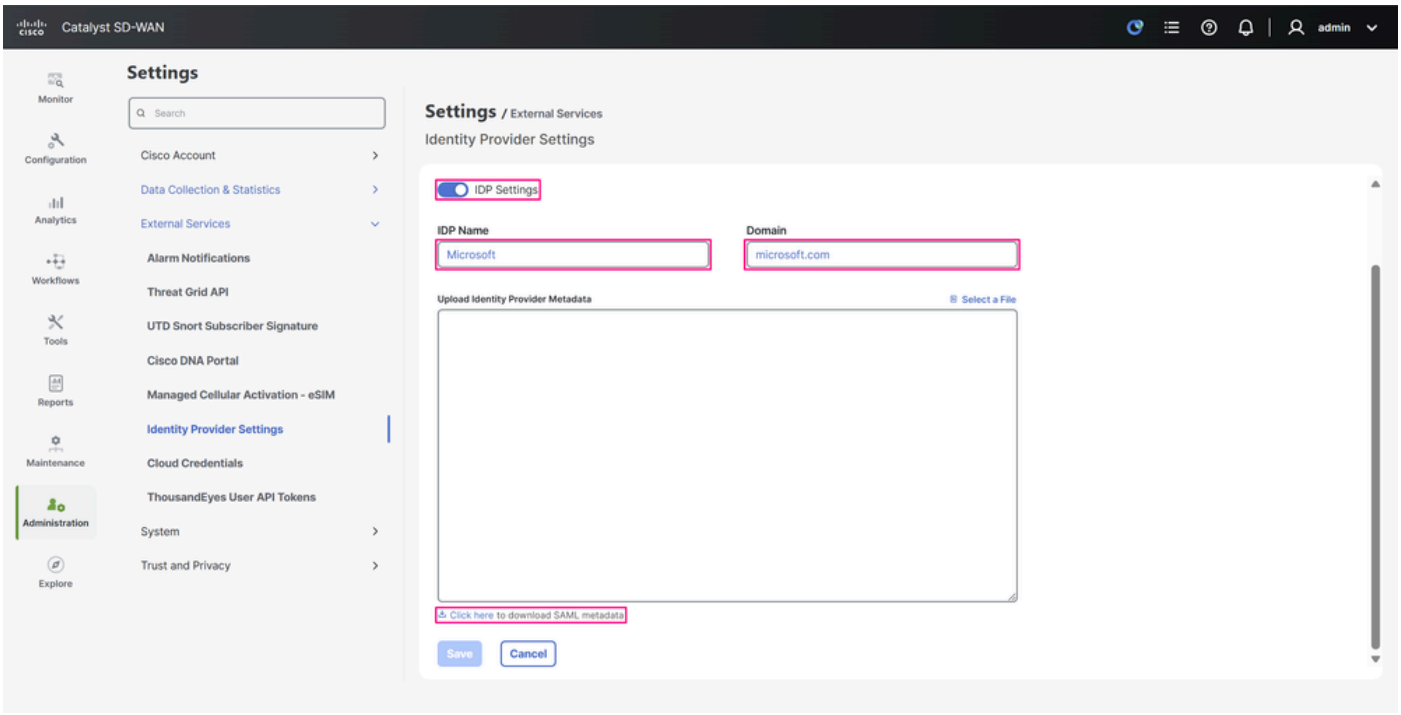
- Alterne Configurações de IDP para habilitar as configurações do provedor de identidade. No campo Nome do IDP, insira um nome que faça referência ao IdP que você está usando e, no campo Domínio, insira um domínio que corresponda aos nomes de domínio usados pelos usuários no aplicativo empresarial da sua organização. Clique em Clique aqui para baixar os metadados SAML e salvar o arquivo XML de metadados em seu computador. Esse arquivo é usado para configurar o SSO na ID do Microsoft Entra na próxima etapa.



Note: Neste exemplo, o arquivo XML de metadados aponta diretamente para o endereço IP do Cisco SD-WAN Manager, mas em muitos ambientes de produção, aponta para seu Fully Qualified Domain Name (FQDN). Para um Cisco SD-WAN Manager autônomo, a ID da entidade contida nos metadados corresponde à URL que você usa para fazer login no Cisco SD-WAN Manager no momento em que você faz o download. Isso significa que ele funciona com o endereço IP ou o FQDN, já que é uma configuração de nó único.

Para um cluster do Cisco SD-WAN Manager, o mesmo princípio se aplica ao fato de que o FQDN aponta para um dos nós do cluster, e os metadados incluem esse domínio como a ID da entidade. A diferença é que, quer você use metadados com o FQDN do cluster ou de um nó específico usando seu endereço IP, depois que a integração do SSO com a ID do Microsoft Entra for concluída com êxito, os outros nós também redirecionarão para o prompt de entrada do IdP.

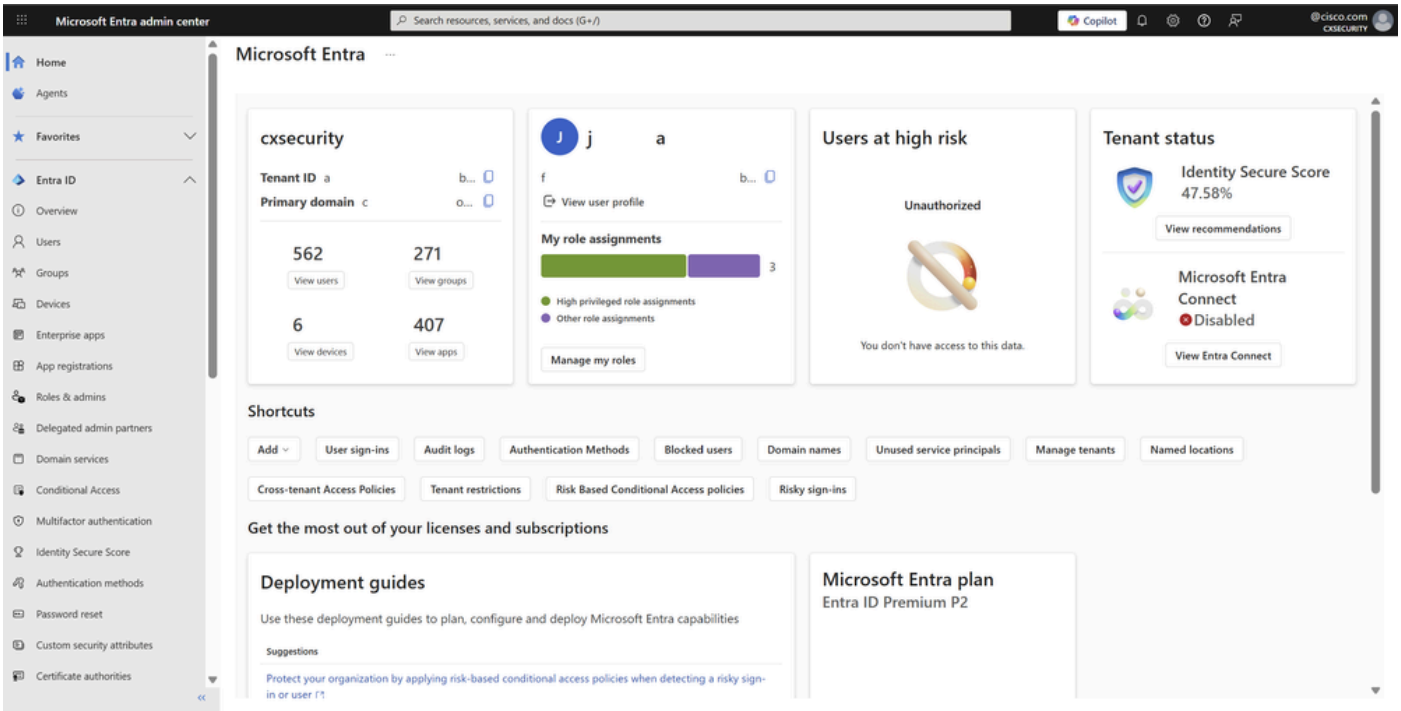
O principal requisito em ambos os cenários é que a ID da entidade que você usa no Cisco SD-WAN Manager, seja um endereço IP ou um FQDN, corresponda ao identificador configurado no lado do IdP.



Página Configuração de Definições de IdP

Etapa 2. Configurar um Aplicativo Corporativo para SSO no Microsoft Entra ID

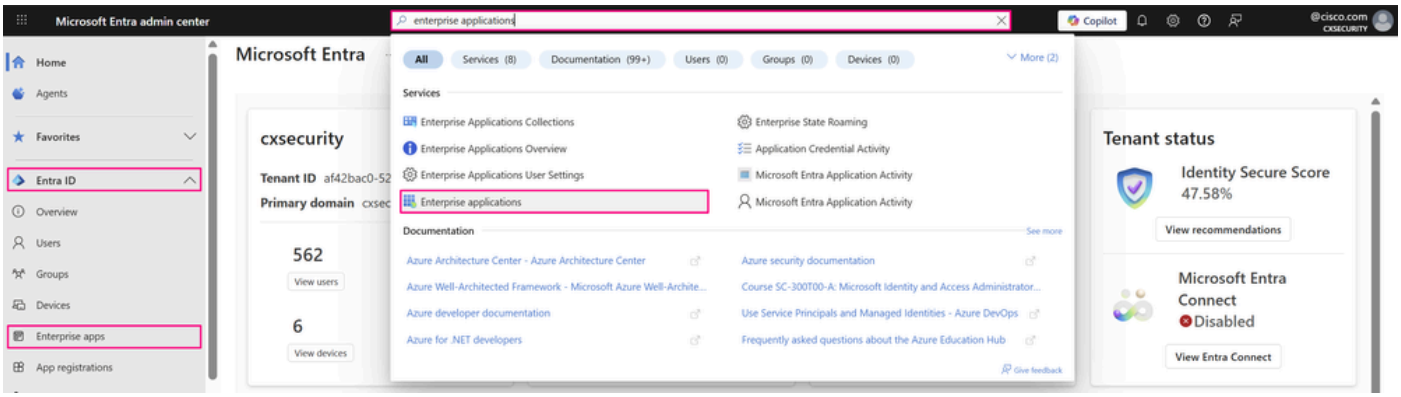
- Faça logon no portal do centro de administração do Microsoft Entra com uma destas funções: Administrador de aplicativos em nuvem, administrador de aplicativos ou proprietário da entidade de serviço.



Portal do Centro de Administração do Microsoft Entra

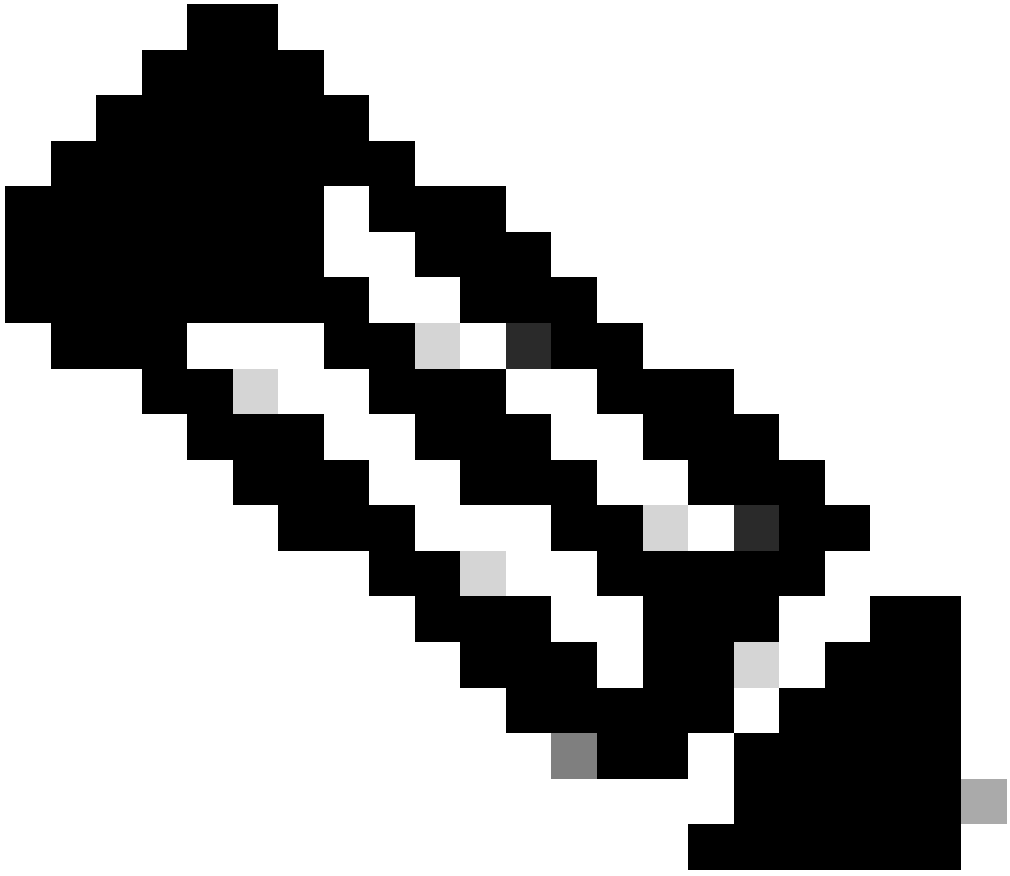
- Navegue para Entra ID > Enterprise apps, ou você também pode acessar este serviço ao inserir enterprise applications na barra de pesquisa na parte superior do portal e, em

seguida, escolha Enterprise Applications.



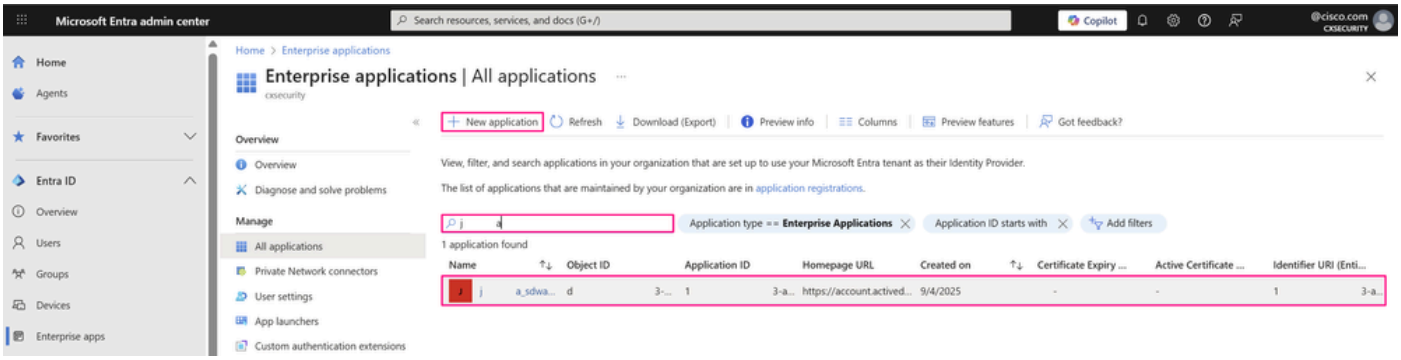
Portal do Centro de Administração do Microsoft Entra

- A página Todos os aplicativos é aberta. Insira o nome do aplicativo existente na caixa de pesquisa e escolha o aplicativo nos resultados da pesquisa.



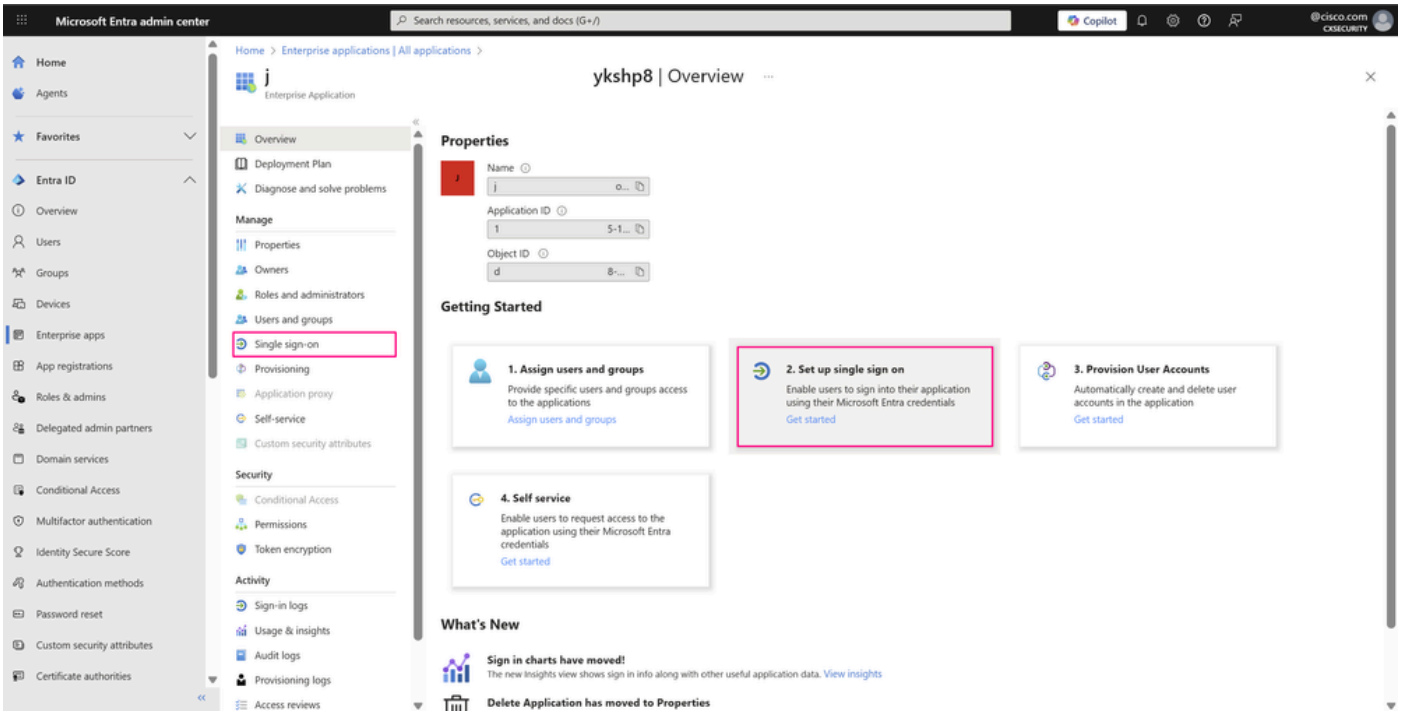
Note: Nessa mesma página, você pode criar um aplicativo empresarial personalizado com base nos requisitos da sua organização e configurá-lo com a

autenticação SSO, se ainda não tiver, ao clicar em Novo aplicativo.



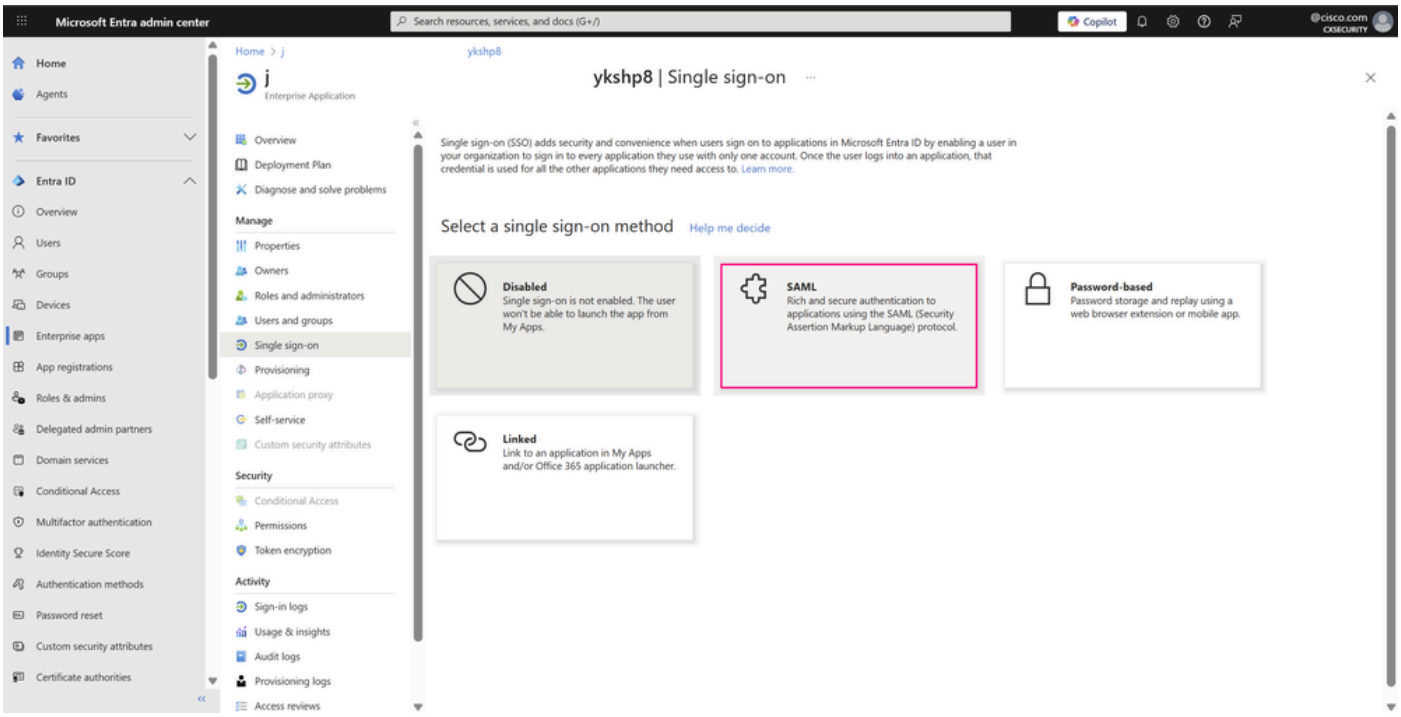
Painel de aplicativos corporativos

- Na seção Gerenciar do menu esquerdo, clique em Logon único ou, no painel Introdução na seção Visão geral, clique em2. Configure o logon único para abrir o painel Logon único para edição.



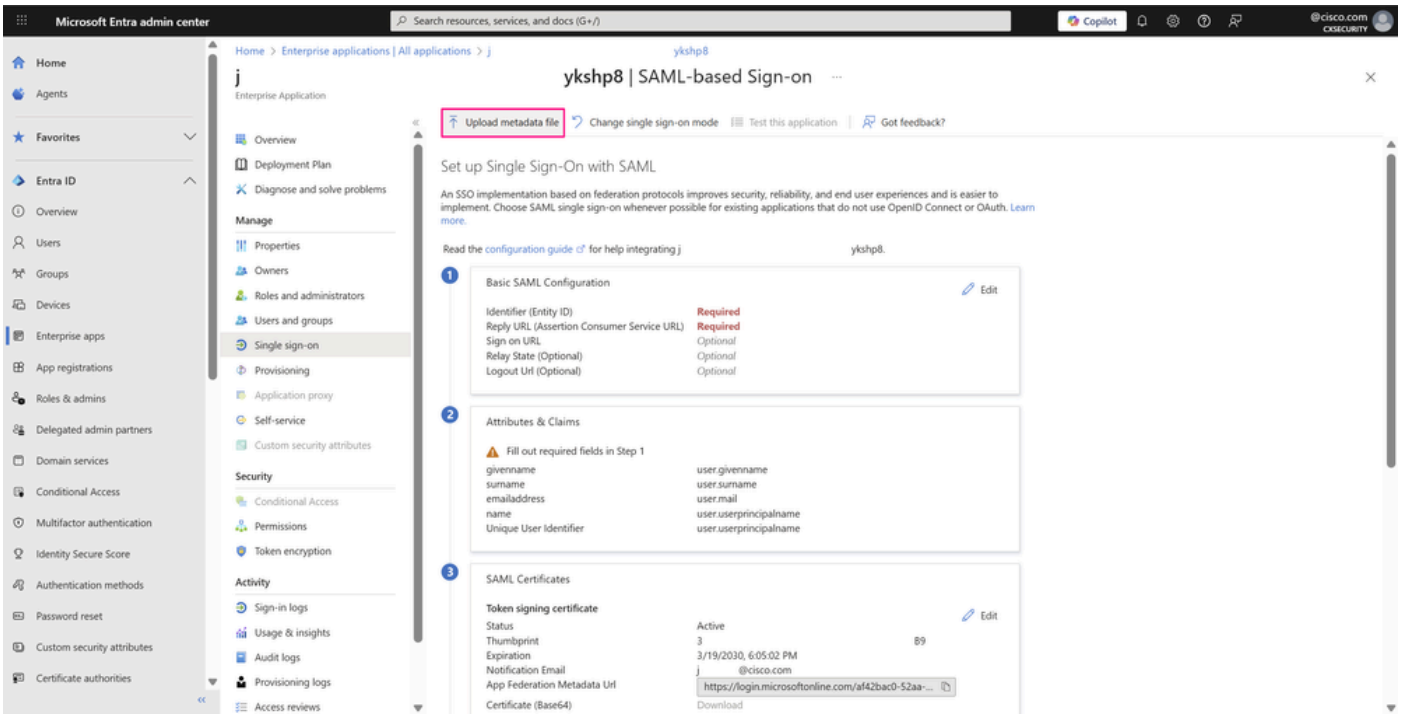
Visão geral dos aplicativos corporativos

- Selecione SAML para abrir a página de configuração de SSO.



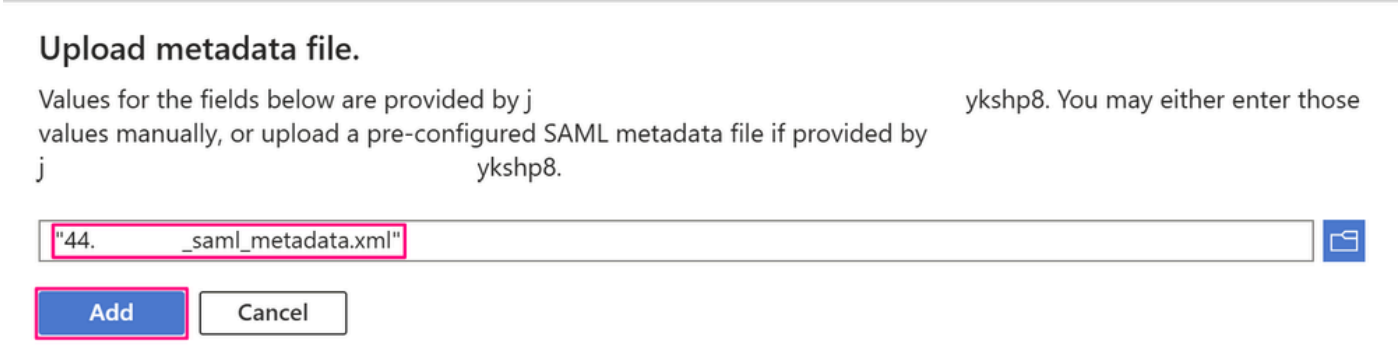
Painel de Logon Único

- Na página Configurar Single Sign-On com SAML, clique em Carregar arquivo de metadados.



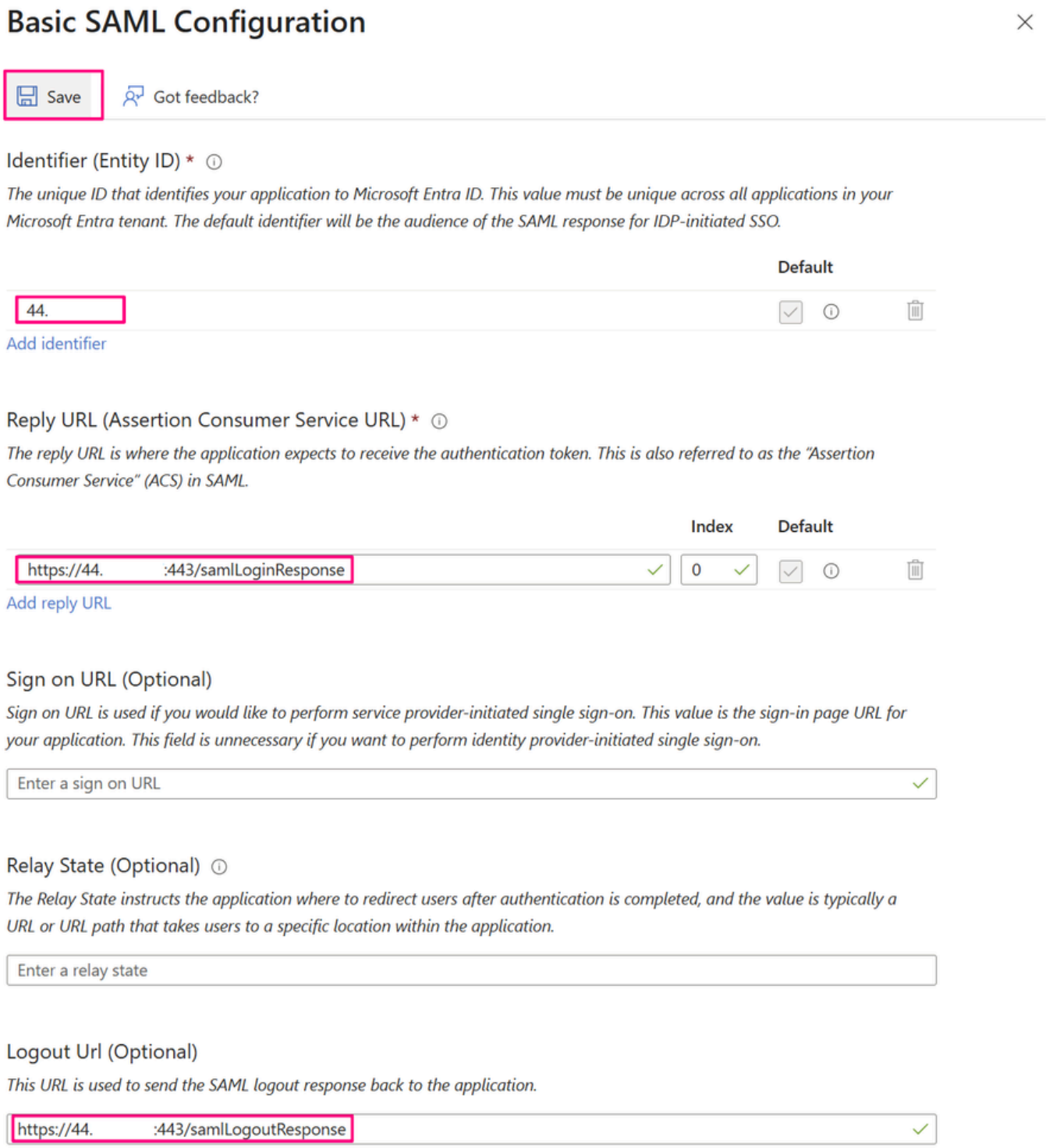
Página SSO com Configuração SAML

- Na janela Carregar arquivo de metadados, navegue e clique no arquivo XML de metadados baixado anteriormente e clique em Adicionar.



Janela Carregar Arquivo de Metadados

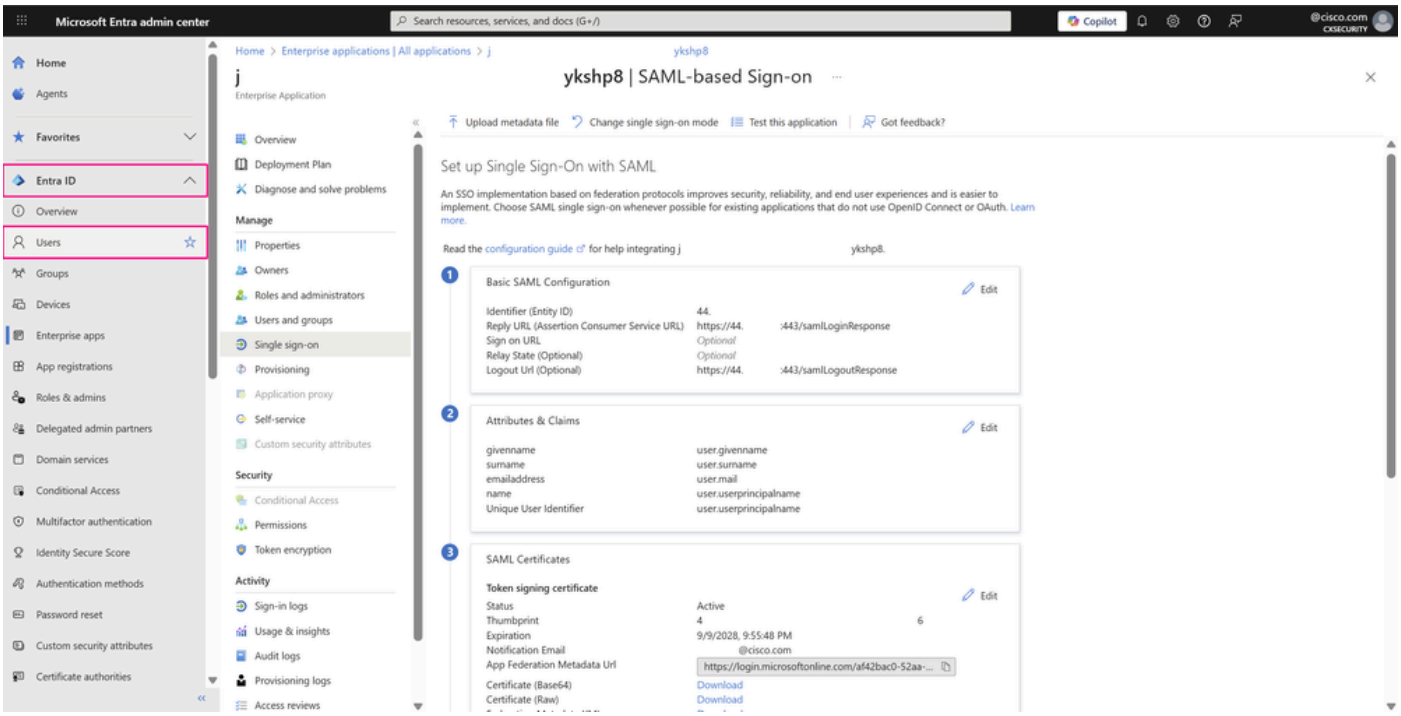
- Na janela Basic SAML Configuration, o Identifier (Entity ID) é geralmente o URL específico do aplicativo — neste caso, o Cisco SD-WAN Manager — com o qual você está se integrando (como explicado na etapa anterior). Os valores de URL de resposta e URL de logoff são preenchidos automaticamente quando o arquivo é carregado com êxito. Para continuar, clique em Salvar.



Janela Configuração SAML Básica

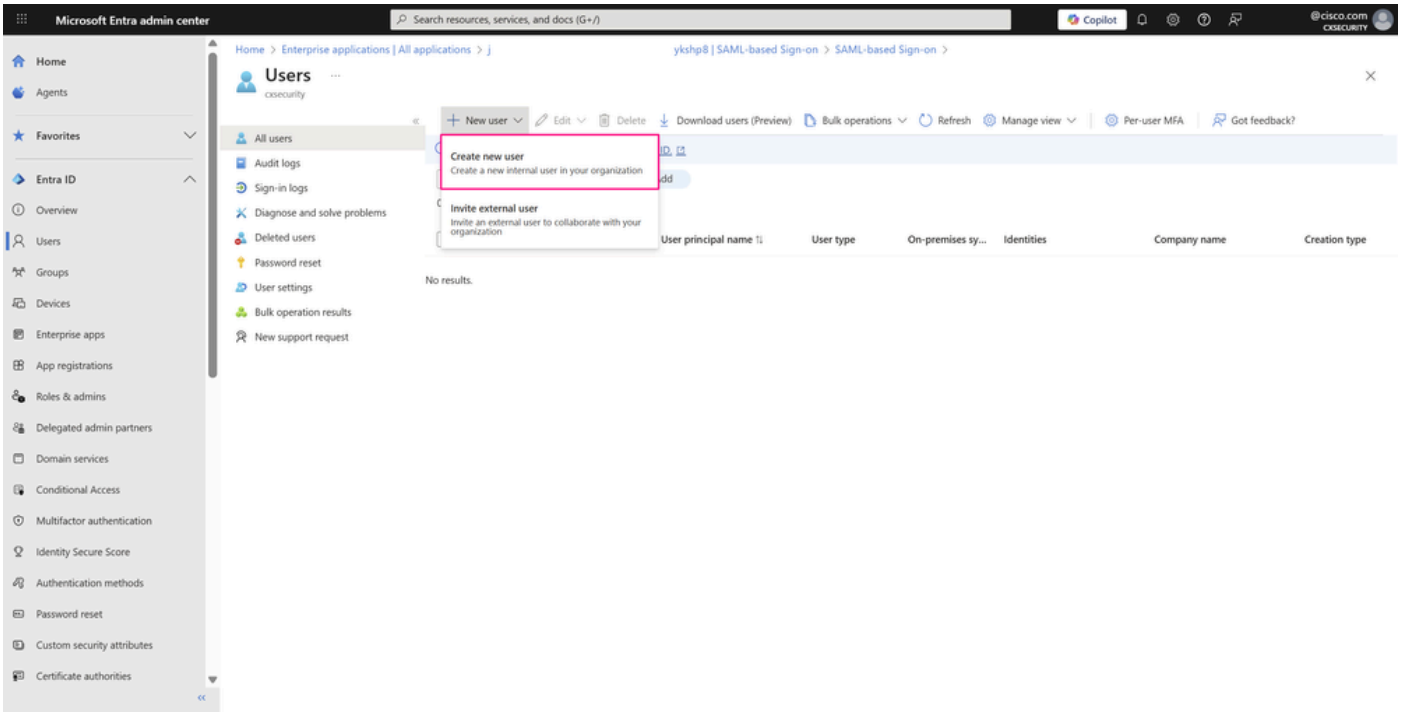
Etapa 3. Adicionar uma Conta de Usuário ou Grupo à Aplicação Enterprise

- Com os parâmetros de configuração SAML do aplicativo definidos, você continua a adicionar os usuários ou grupos no aplicativo empresarial que entram no aplicativo. Para fazer isso, primeiro navegue até Entra ID > Users, ou você também pode acessar esse serviço ao pesquisar o nome do serviço na barra de pesquisa na parte superior do portal, como mostrado em uma etapa anterior.



Página SSO com Configuração SAML

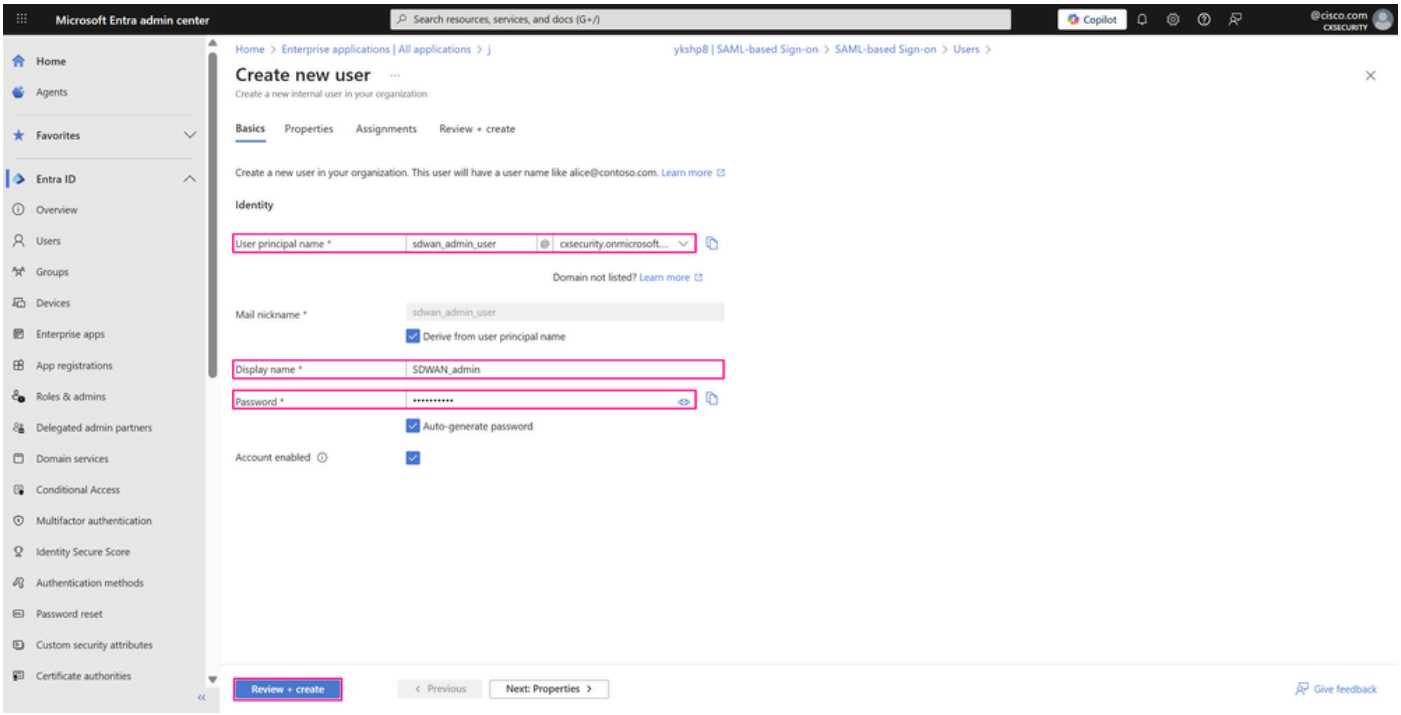
- Crie um usuário que você associe a um grupo para ilustrar a autenticação SSO com o Cisco SD-WAN Manager e um de seus grupos de usuários, netadmin, que é o mais comum em ambientes de produção. Para fazer isso, navegue até ID do Entra > Usuários. Em seguida, clique em Novo usuário e escolha Criar novo usuário.



Painel de usuários

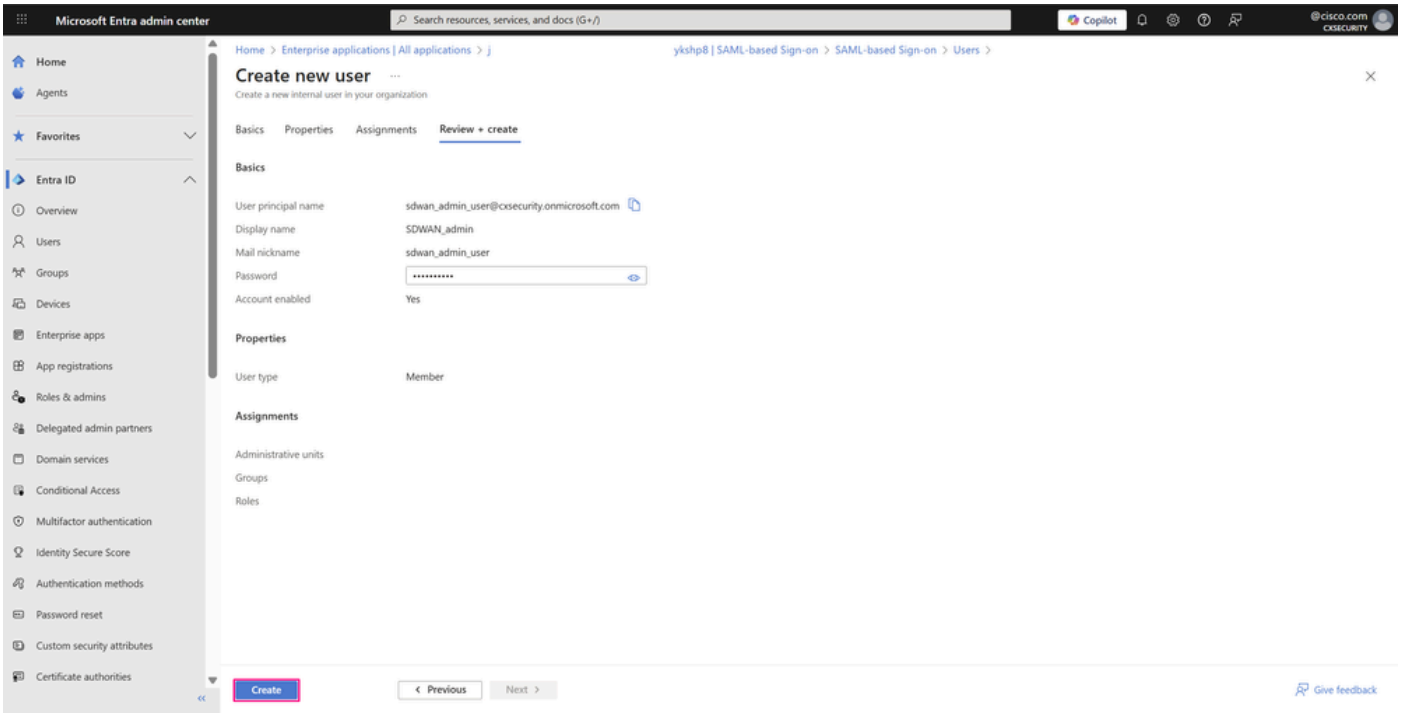
- A guia Basics contém os principais campos necessários para criar um novo usuário.
  - Para o Nome UPN, digite um nome de usuário exclusivo e escolha um domínio na lista suspensa de domínios disponíveis em sua organização.
  - Insira um nome de exibição para o usuário.

- Desmarque Gerar senha automaticamente se quiser inserir uma senha personalizada ou deixe esta opção marcada para que uma senha seja gerada automaticamente.
- Você pode adicionar o usuário a um grupo na guia Atribuições, mas como a associação de grupo ainda não foi criada, clique em Revisar + criar.



Página Criação de Usuário

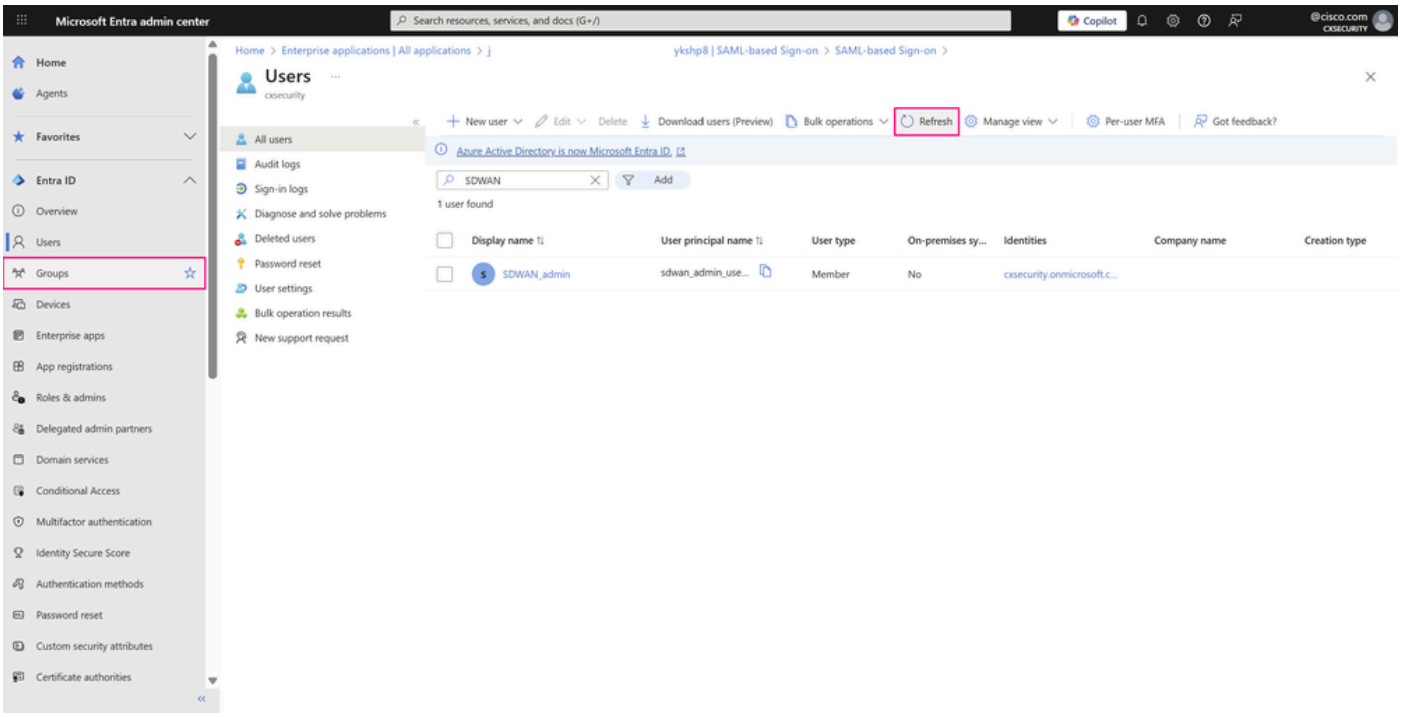
- A guia final mostra os principais detalhes do fluxo de trabalho de criação do usuário. Revise os detalhes e clique em Criar para concluir o processo.



Página Criação de Usuário

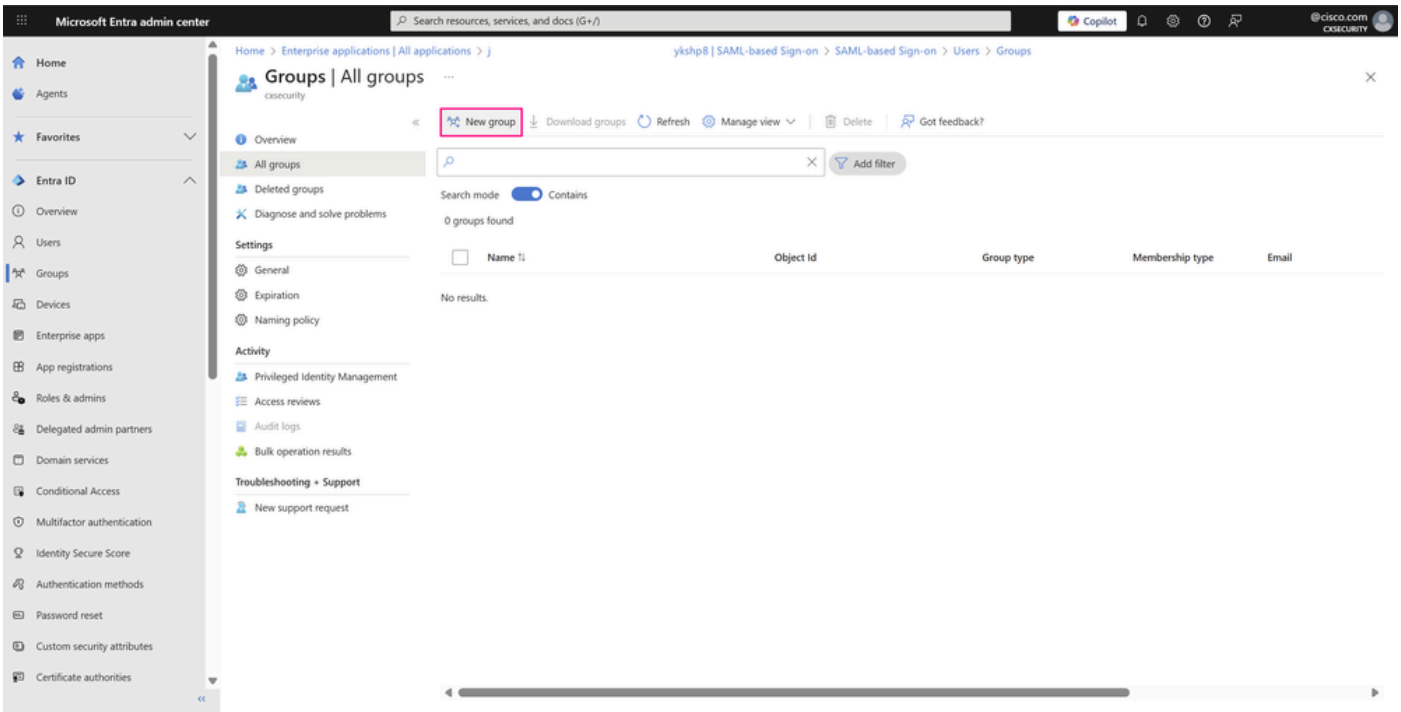
- O novo usuário aparece pouco depois. Se isso não acontecer, clique em Atualizar e procure

o usuário usando a barra de pesquisa no serviço. Em seguida, navegue até Entra ID > Groups > All groups para criar o novo grupo.



Painel de usuários

- Nesta página, você gerencia os diferentes grupos e suas permissões dentro da sua organização. Clique em Novo grupo para criar o grupo que tem privilégios de administrador de rede.

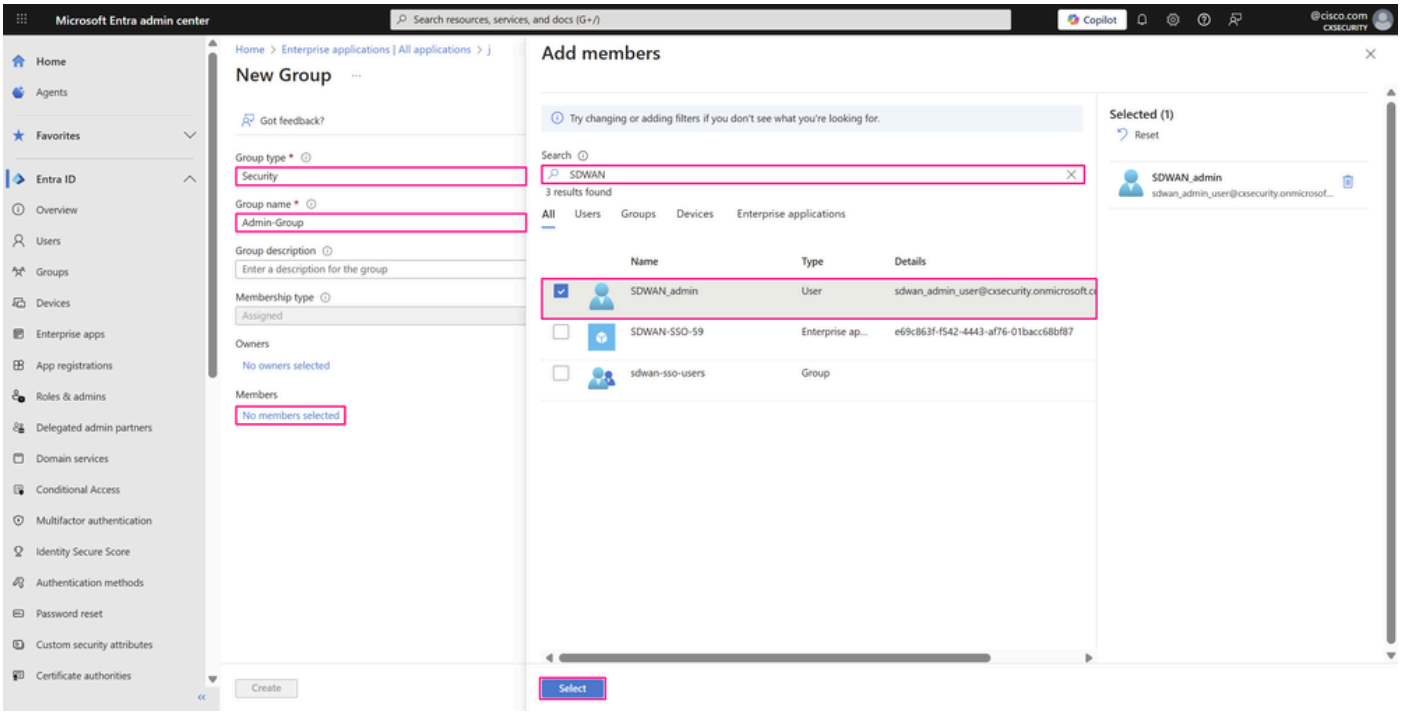


Página Todos os Grupos

- Escolha um Tipo de grupo na lista suspensa — nesse caso, Segurança, já que somente o acesso a recursos compartilhados é necessário. Insira um nome de grupo de sua escolha

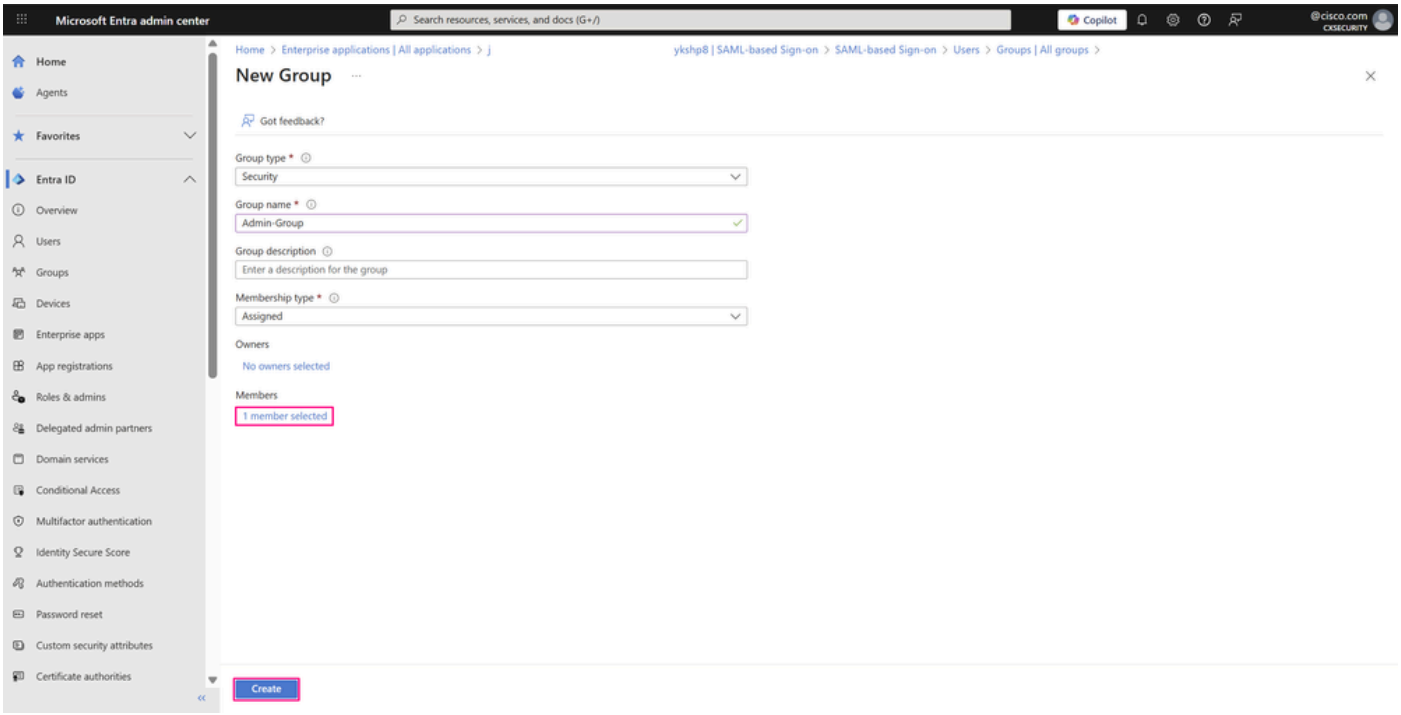
que faça referência à função ou às permissões do grupo. Nesse ponto, associe usuários ao grupo quando você clica nos membros selecionados no campo Membros.

- Na janela Adicionar membros, navegue e escolha os usuários que deseja adicionar — em nosso exemplo, o usuário que você acabou de criar — e clique em Selecionar.



Página Criação de Grupo

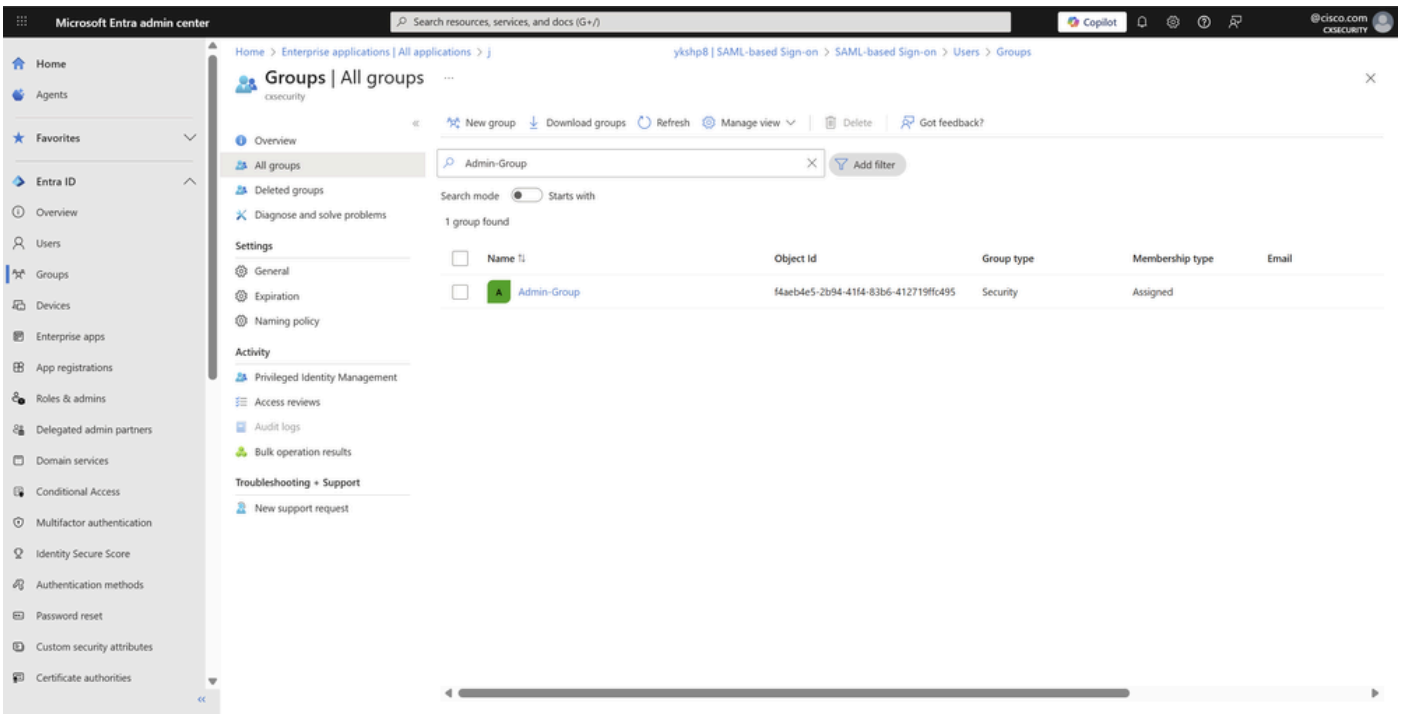
- Clique em Criar para criar o grupo.



Página Criação de Grupo

- O novo grupo aparece pouco depois. Se isso não acontecer, clique em Atualizar e procure o

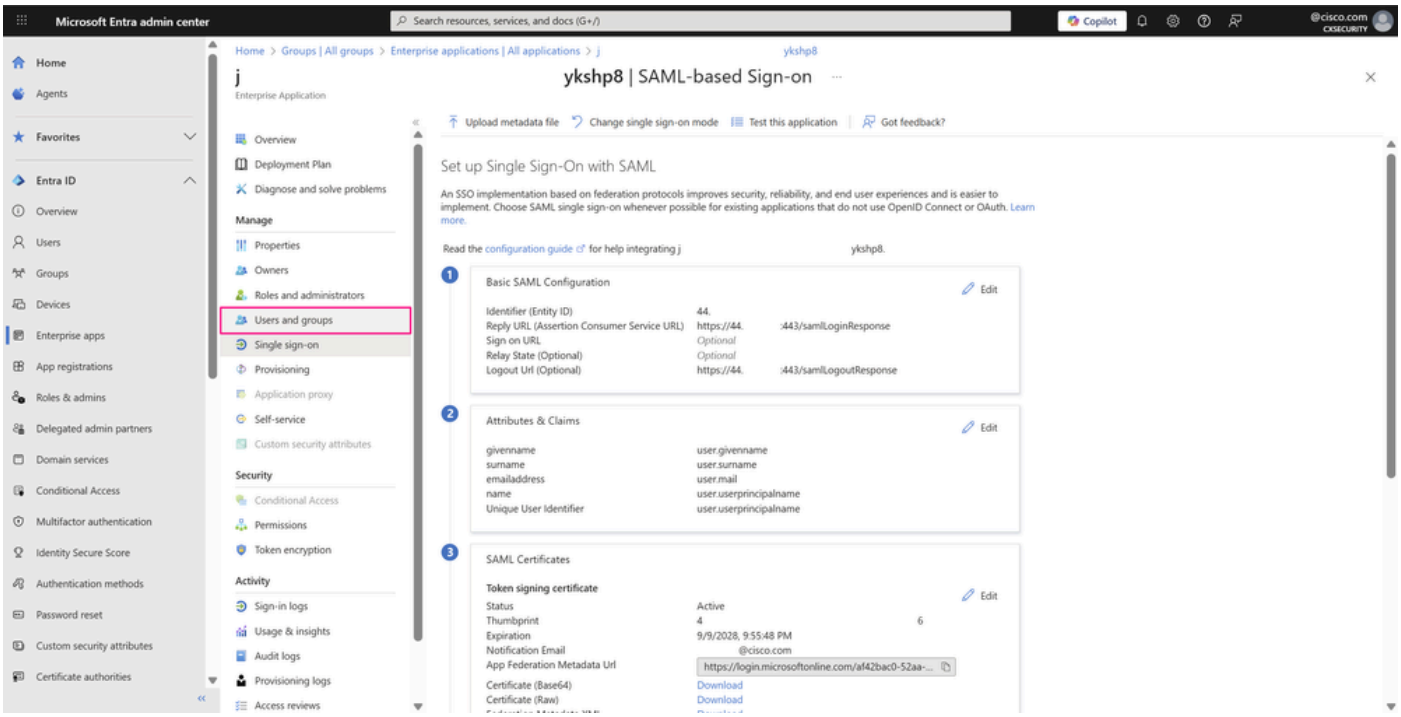
nome do grupo com a barra de pesquisa no serviço. Repita as etapas anteriores para criar outro usuário e adicioná-lo a uma associação de grupo diferente para validar o login do SSO com o aplicativo e um de seus outros grupos de usuários, como o operador.



Página Todos os Grupos

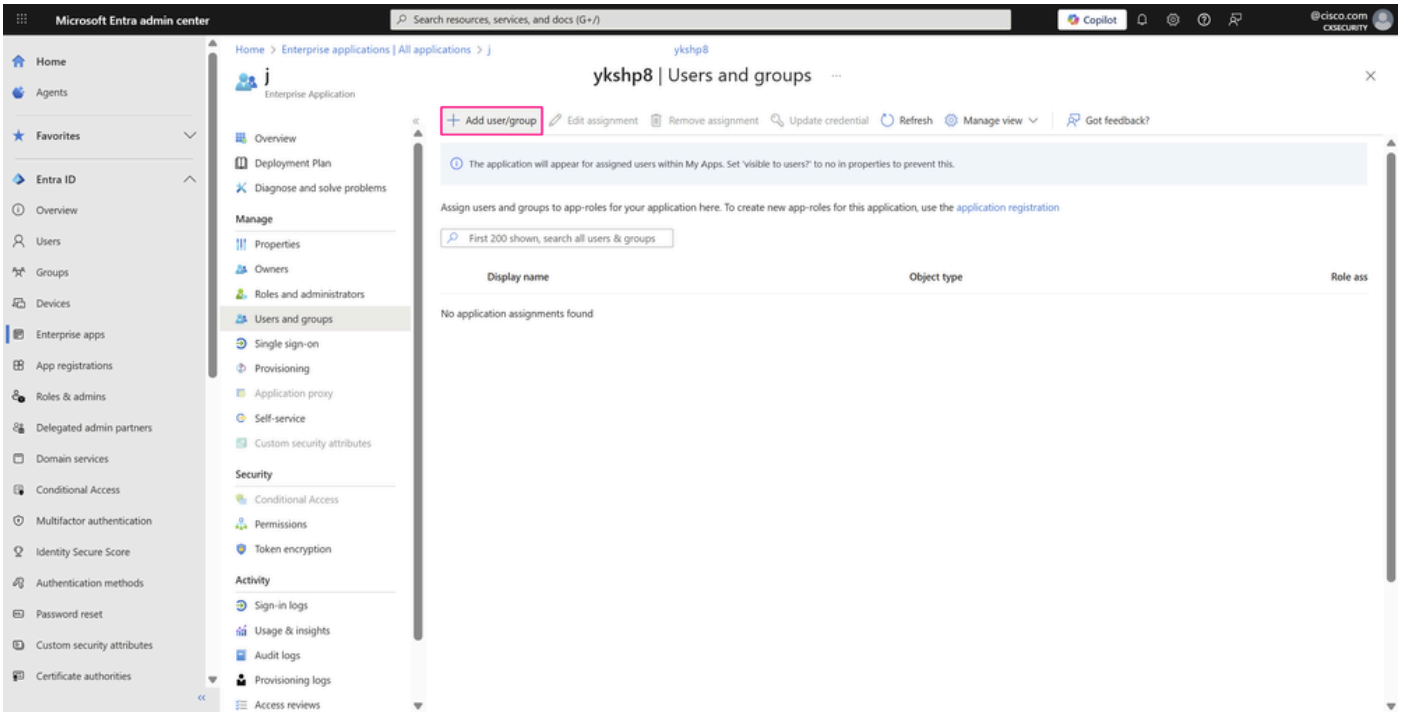
Etapa 4. Configurar Provisionamento de Grupo SAML para o Microsoft Entra ID

- Para provisionar os grupos ou os usuários associados a eles na configuração SAML, você precisa atribuí-los ao seu aplicativo empresarial para que eles tenham permissões de login para o seu aplicativo, por exemplo, o Cisco SD-WAN Manager. Navegue de volta para Entra ID > Enterprise apps e abra o aplicativo empresarial. Na seção Gerenciar do menu esquerdo, clique em Usuários e grupos.



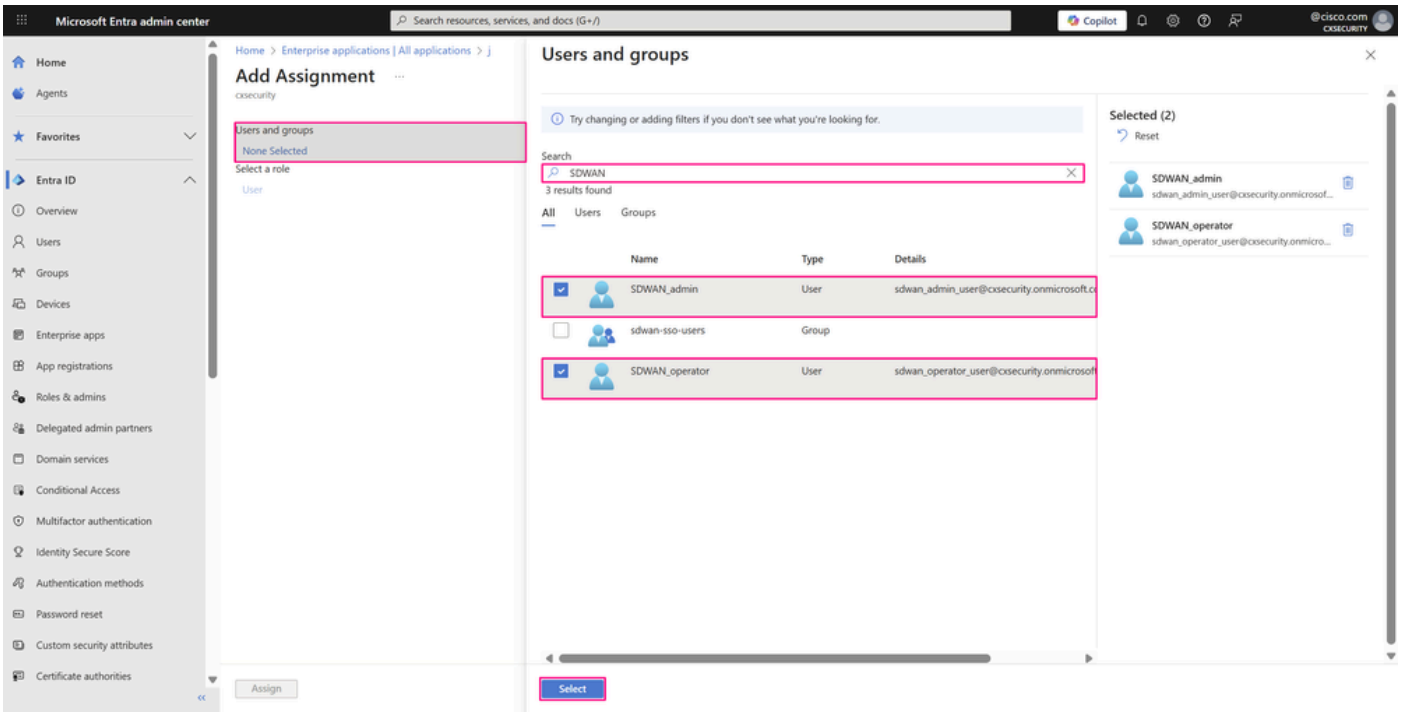
Página SSO com Configuração SAML

- Em seguida, clique em Adicionar usuário/grupo.



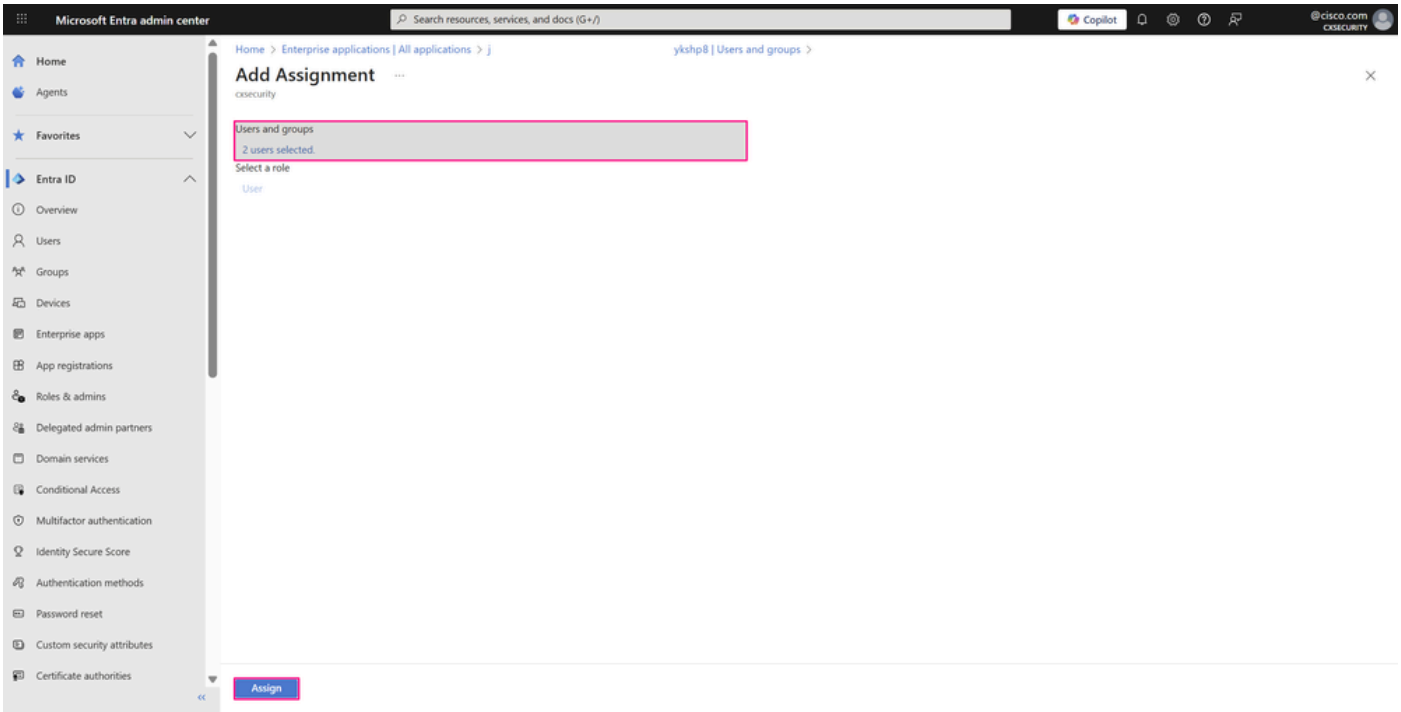
Página Usuário e Grupos

- No painel Adicionar tarefa, clique em Nenhum selecionado no campo Usuários e grupos. Procure e escolha o usuário ou grupo que deseja atribuir ao aplicativo — em nosso exemplo, os dois usuários criados nas etapas anteriores — e clique em Selecionar.



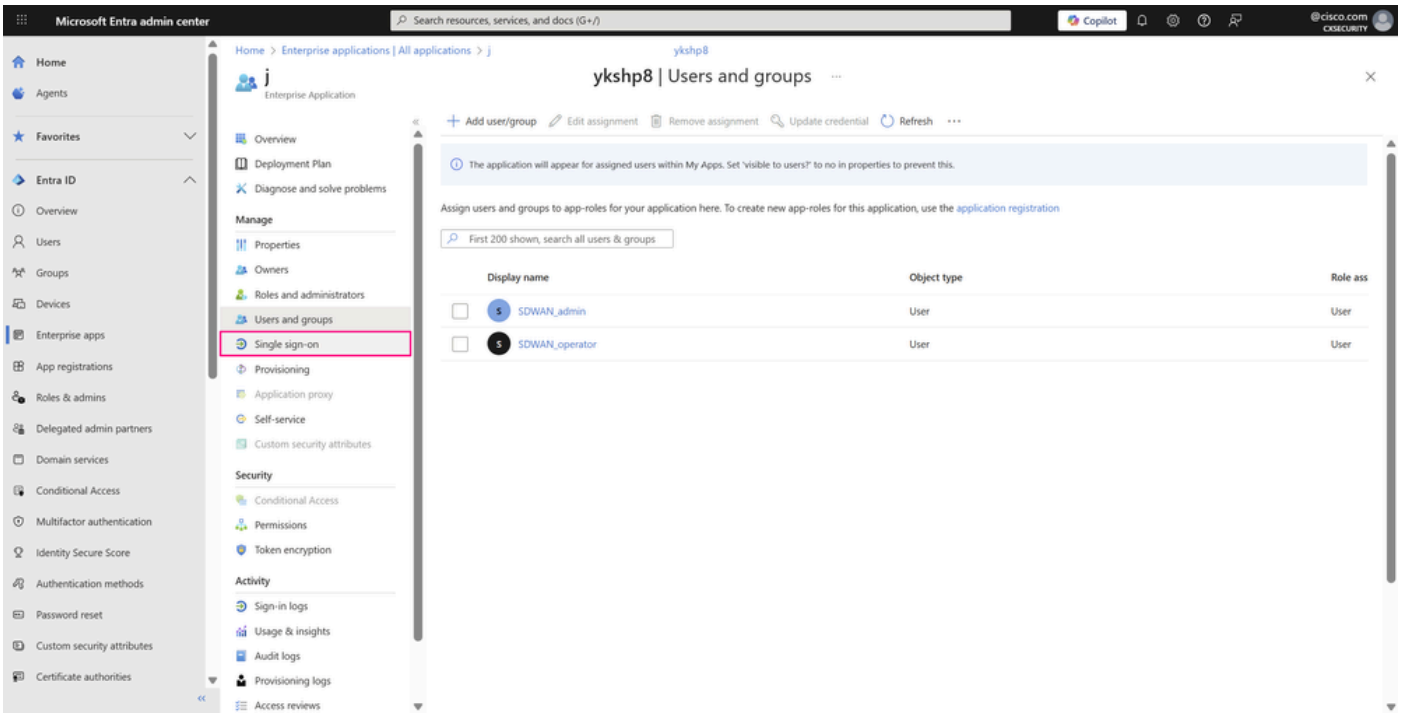
Painel Atribuição de usuário/grupo

- Clique em Atribuir para atribuir o usuário ou grupo ao aplicativo.



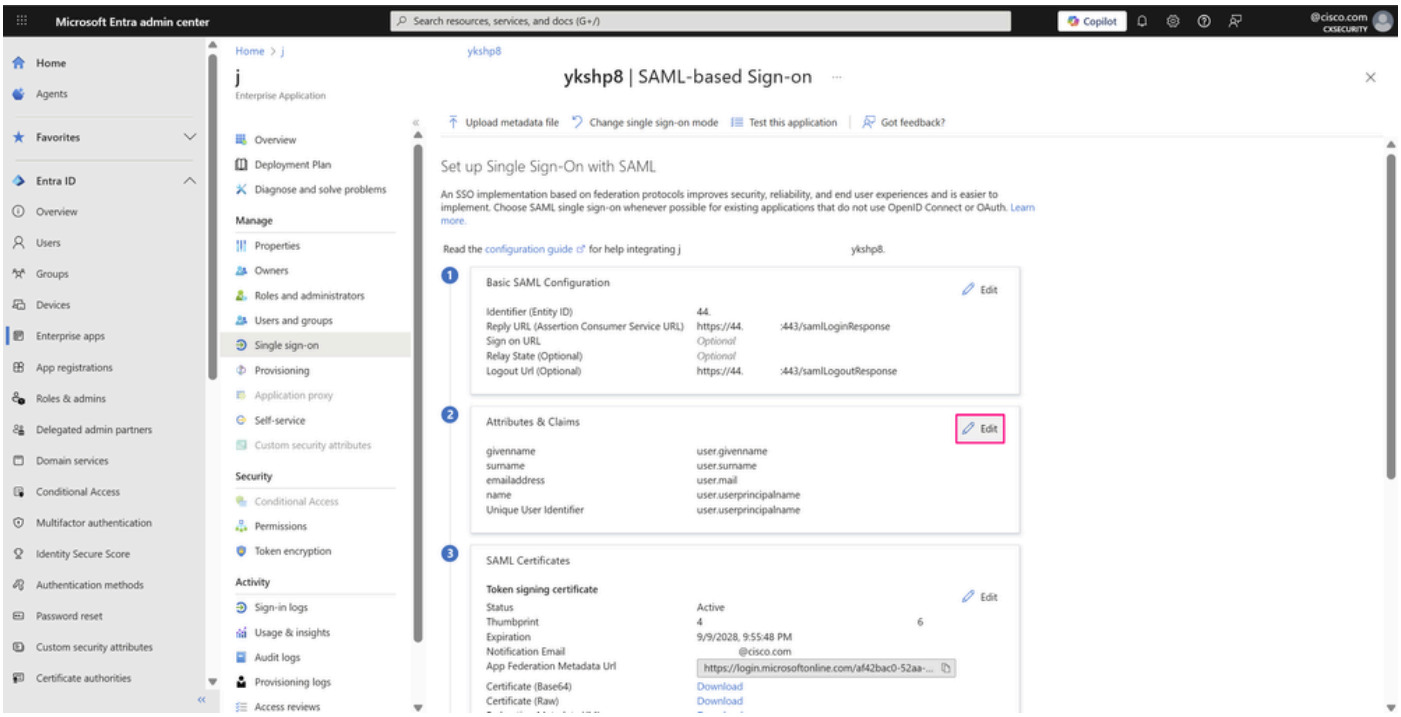
Painel Atribuição de usuário/grupo

- Os usuários atribuídos ao seu aplicativo empresarial são listados logo após a atribuição. Clique em Logon único na seção Gerenciar do menu esquerdo para acessar a configuração SSO SAML do seu aplicativo e concluir a configuração necessária restante.



Página Usuário e Grupos

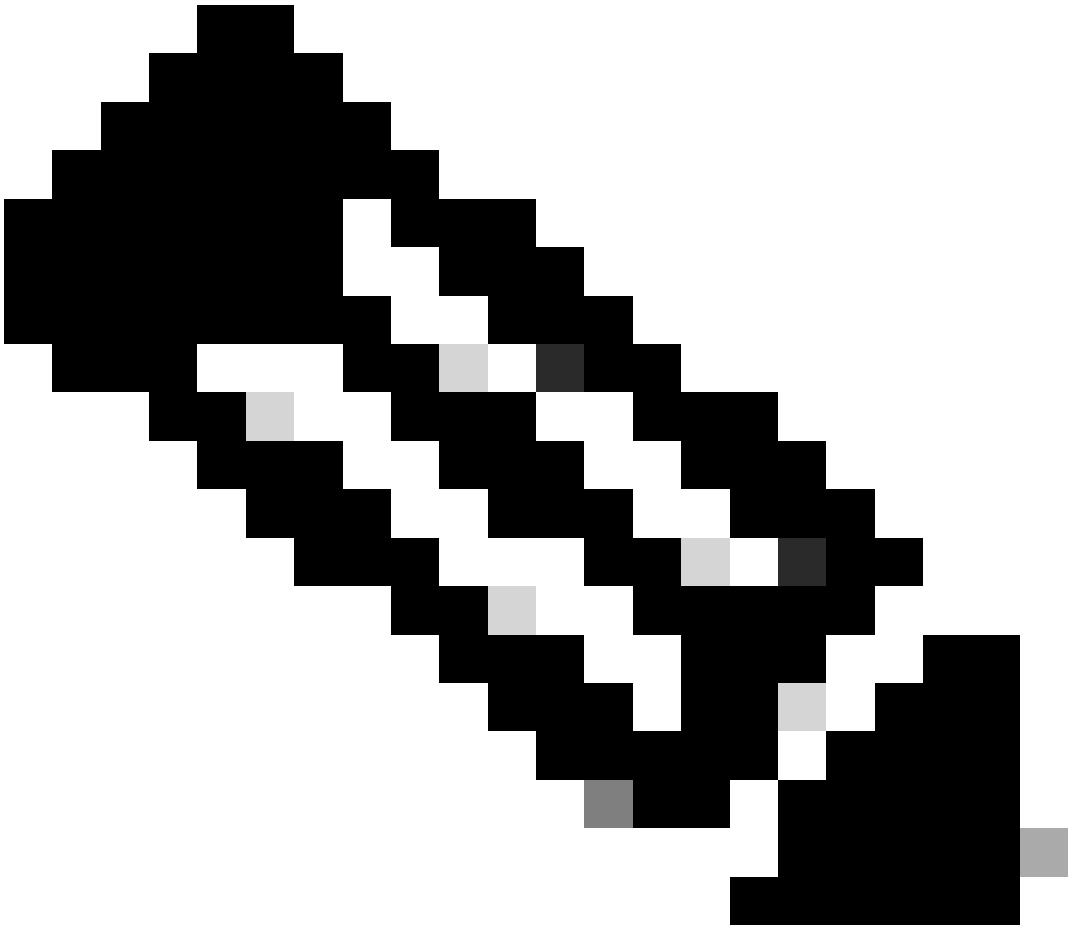
- Na página Configurar logon único com SAML, em Atributos e reivindicações, clique em Editar.



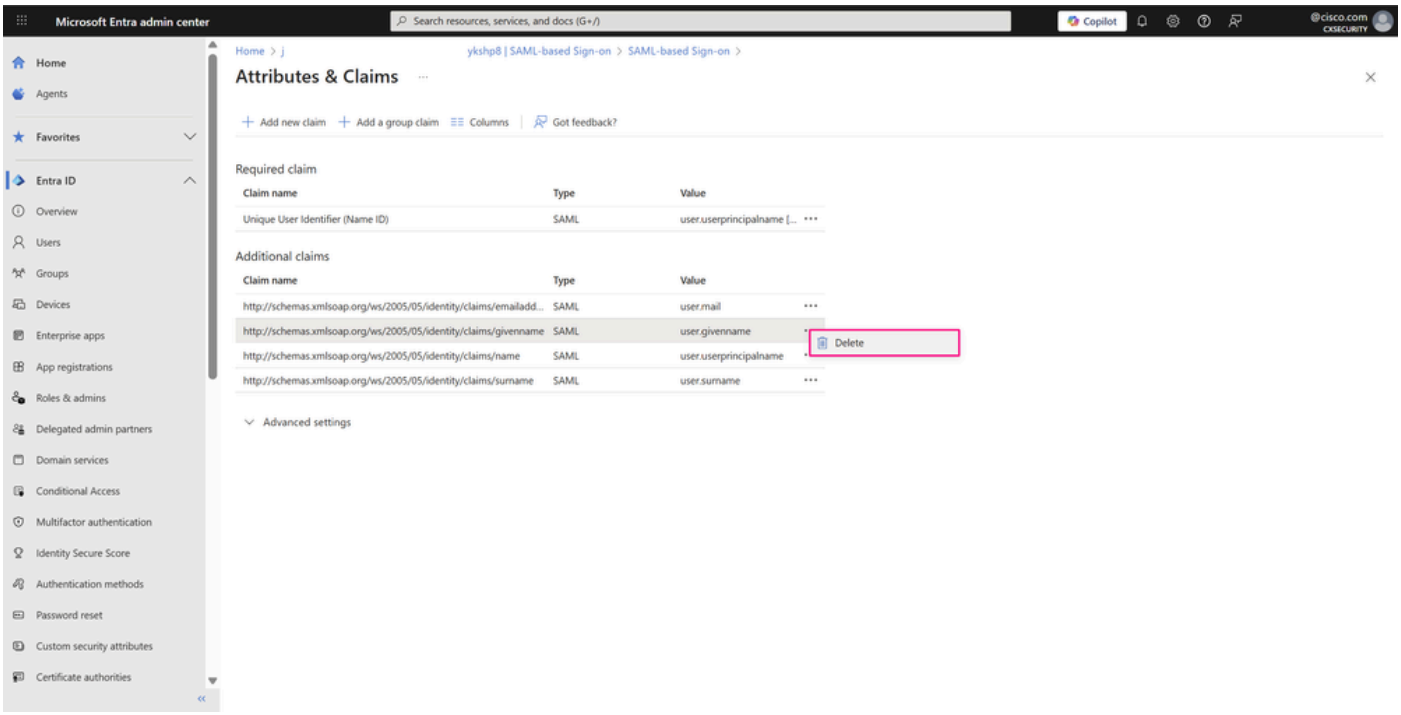
Página SSO com Configuração SAML

- Na página Atributos e reivindicações, clique no ícone de três pontos e em Excluir para remover a reivindicação com o valor user.givenname e a reivindicação com o valor user.surname, já que elas não são necessárias para este exemplo.Somente as próximas reivindicações são necessárias para a autenticação SSO básica com seu aplicativo:
    - Endereço de e-mail do usuário -user.mail

- Nome UPN do usuário -user.userprincipalname

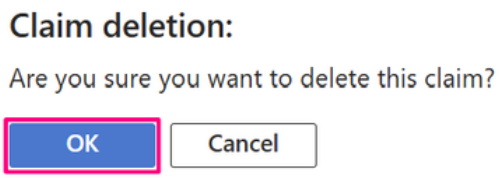


Note: Sua organização pode exigir reivindicações adicionais, dependendo de suas necessidades específicas.



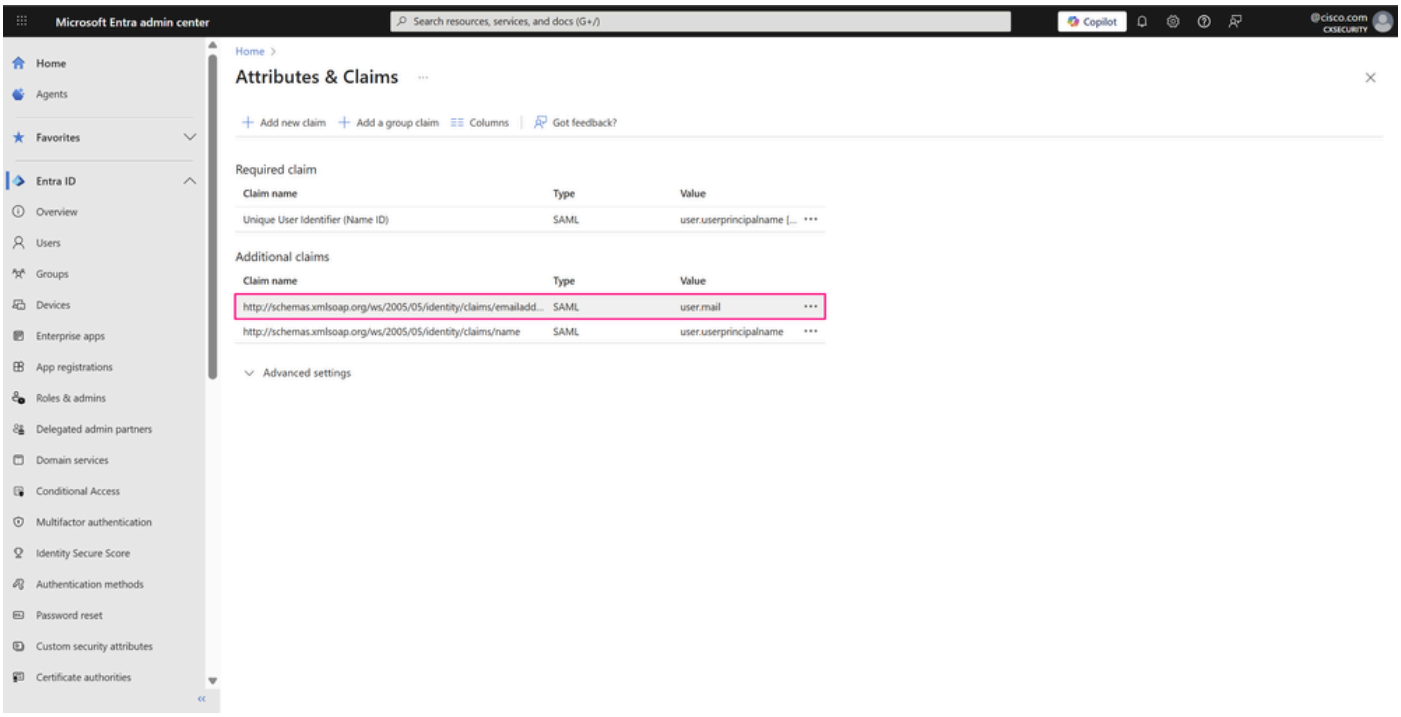
Página Atributos e Reivindicações

- Na janela Exclusão da reivindicação, clique em OK para excluir a reivindicação.



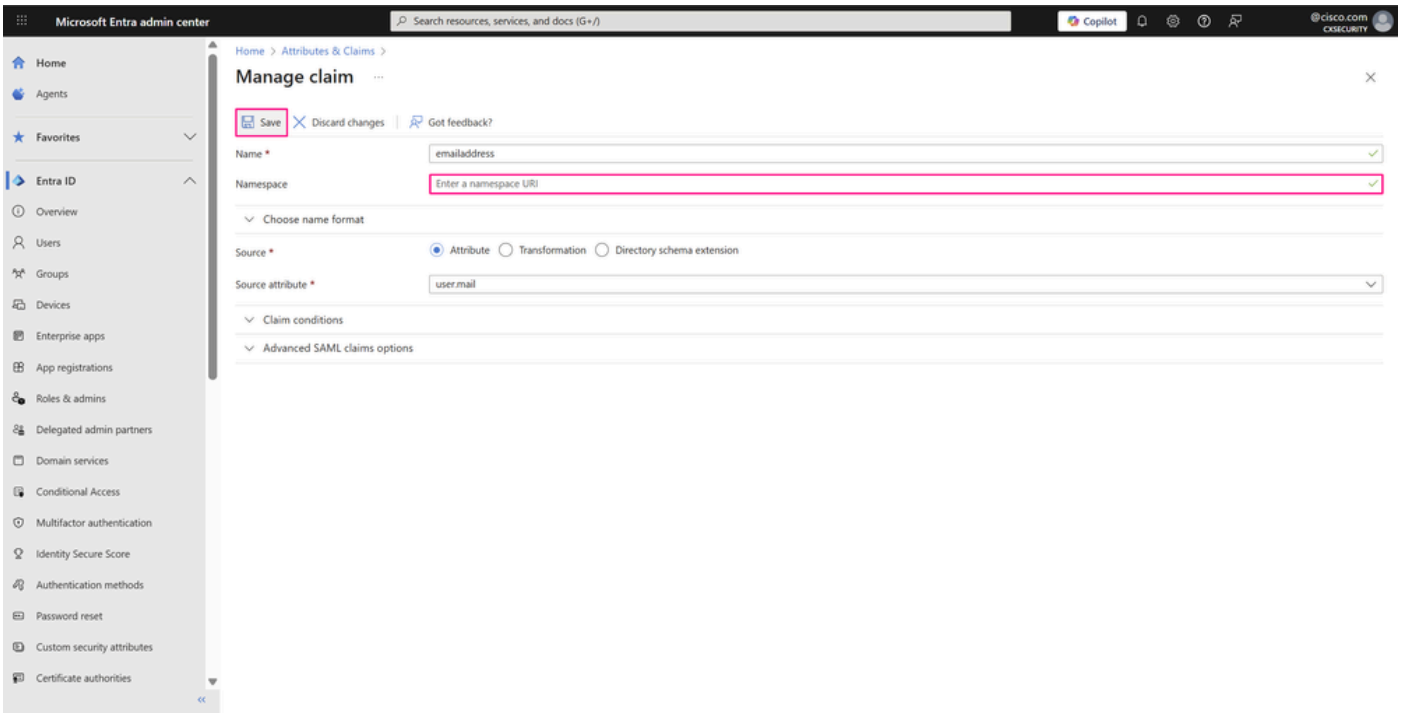
Janela Exclusão da reivindicação

- Em seguida, remova o namespace do Nome da reivindicação nas duas reivindicações restantes, pois esse campo é opcional. Essa alteração permite que o nome real de cada um seja exibido nessa página para facilitar a identificação. Passe o mouse sobre cada reivindicação e clique nela para acessar suas configurações.



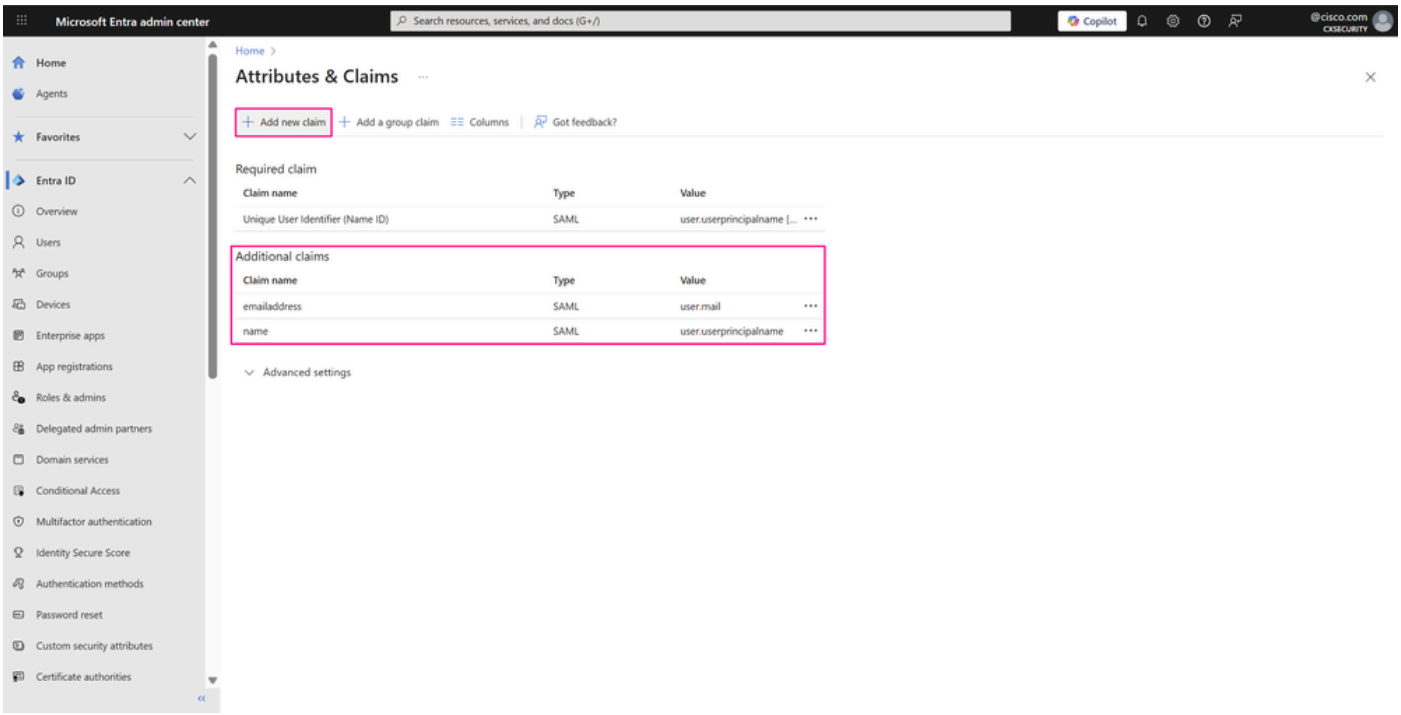
Página Atributos e Reivindicações

- Na página Gerenciar reivindicação, exclua o campo Namespace e clique em Salvar para aplicar as alterações.



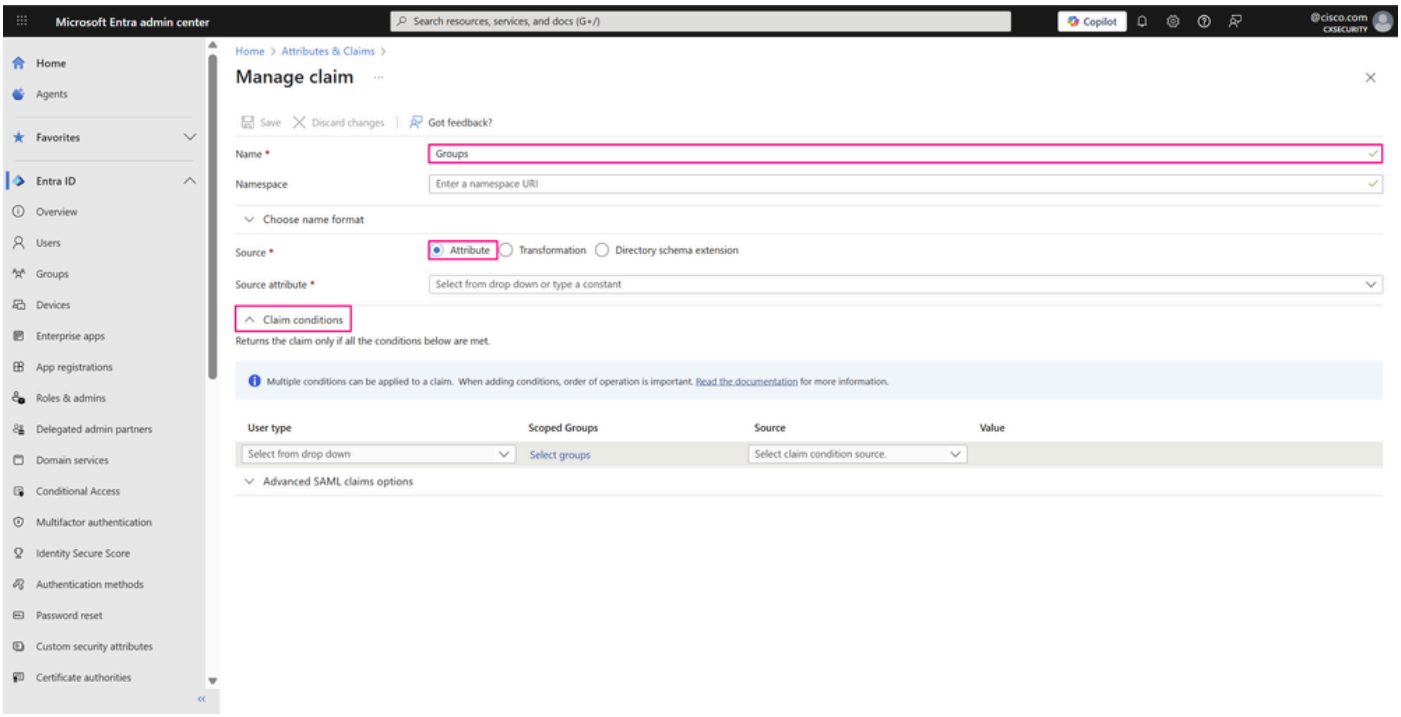
Página Gerenciar reivindicação

- Os nomes das duas asserções obrigatórias agora podem ser vistos. No entanto, mais uma reivindicação adicional ainda é necessária para definir os grupos aos quais os usuários pertencem e que estão autorizados a acessar os recursos do aplicativo. Para fazer isso, clique em Adicionar nova reivindicação.



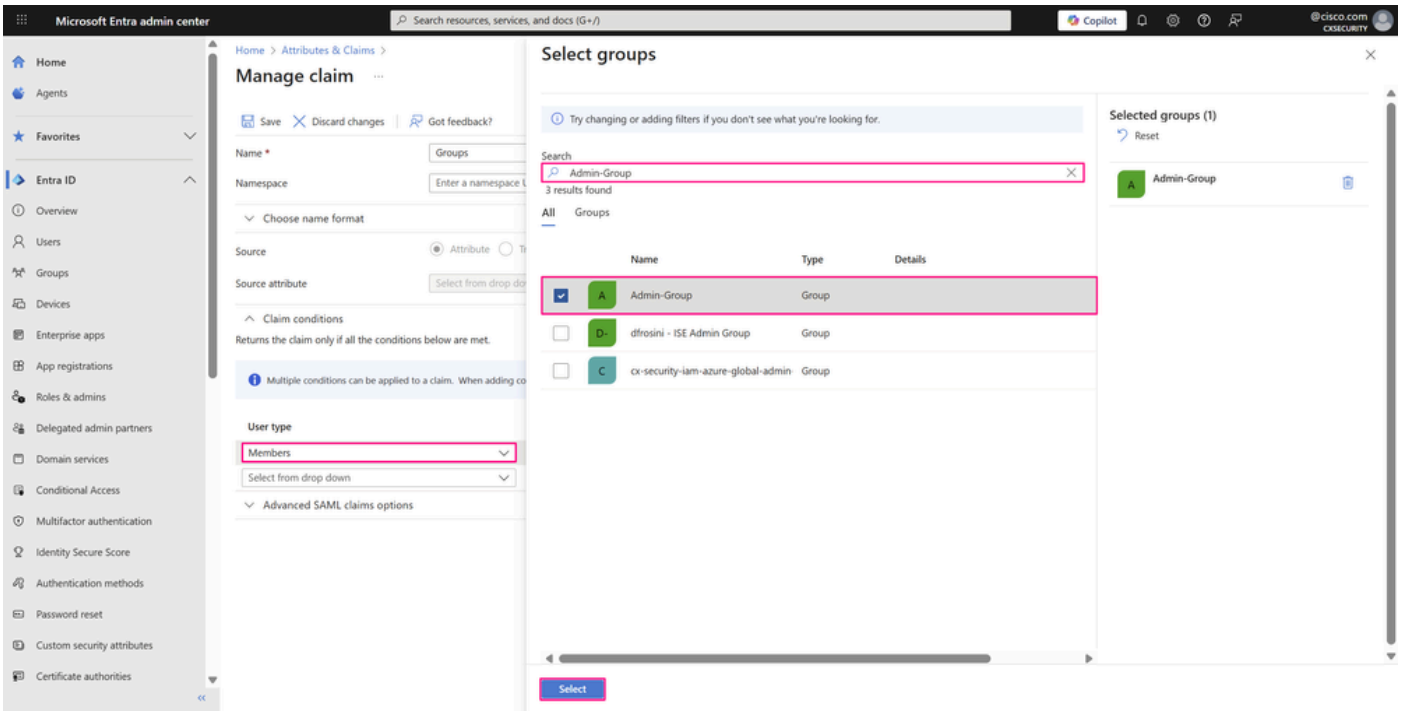
Página Atributos e Reivindicações

- Insira um Nome para identificar esta reivindicação. Ao lado de Source, selecione Attribute. Em seguida, clique em Claim conditions para expandir as opções e configurar várias condições.



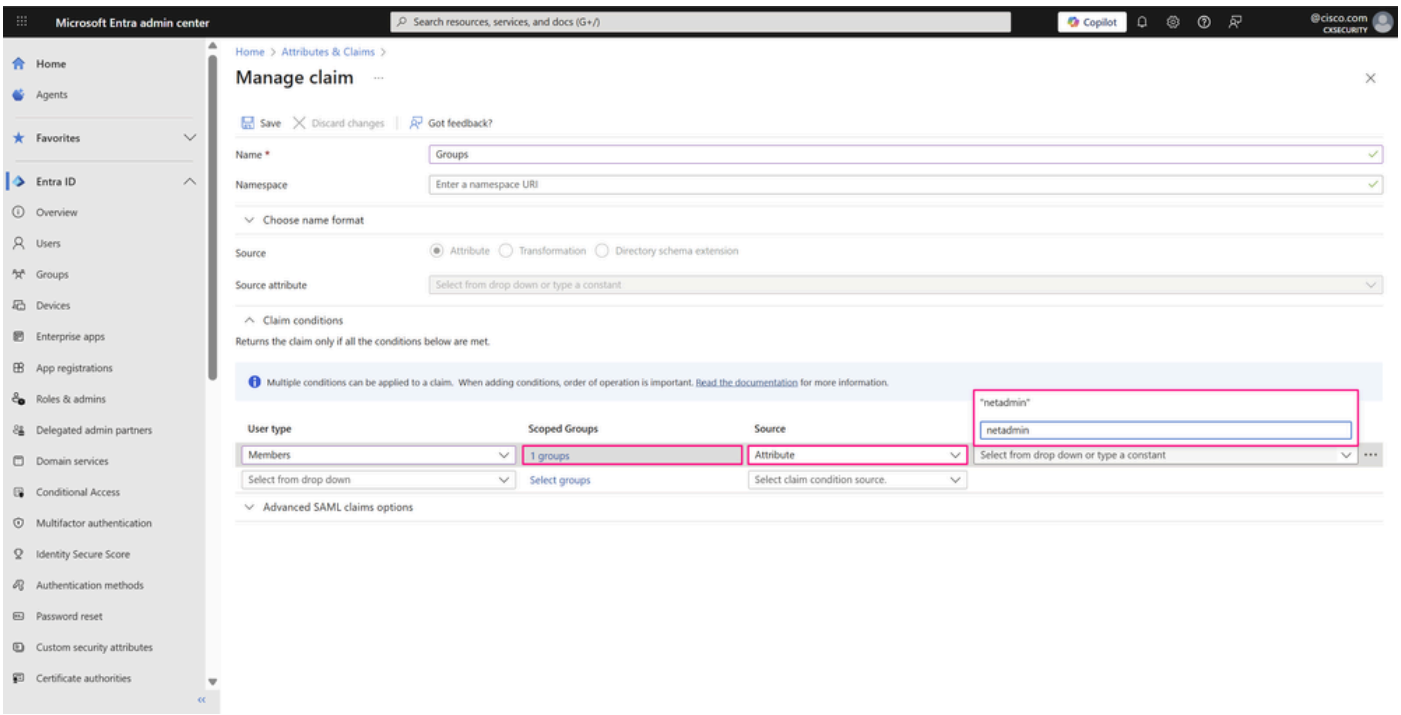
Página Gerenciar reivindicação

- Na condição de declaração, escolha Membros na lista suspensa Tipo de usuário e clique em Selecionar grupos para escolher o(s) grupo(s) ao(s) qual(is) o usuário deve pertencer e clique em Selecionar.



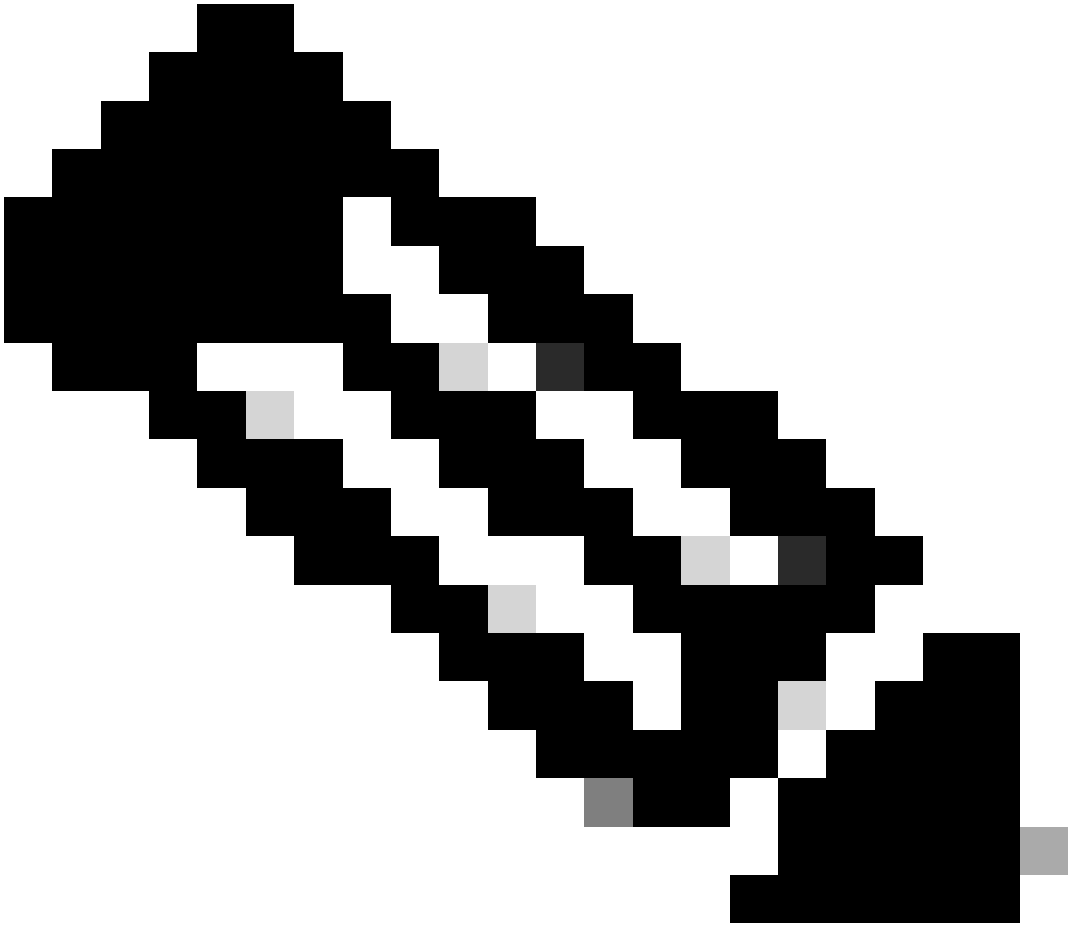
Página Gerenciar reivindicação

- Escolha Attribute na lista suspensa Source onde a reivindicação recupera seu valor. No campo Valor, insira o atributo personalizado do usuário que faz referência ao grupo de usuários definido em seu aplicativo. Neste exemplo, netadmin é um dos grupos de usuários padrão no Cisco SD-WAN Manager. Insira o valor do atributo sem aspas e pressione Enter.

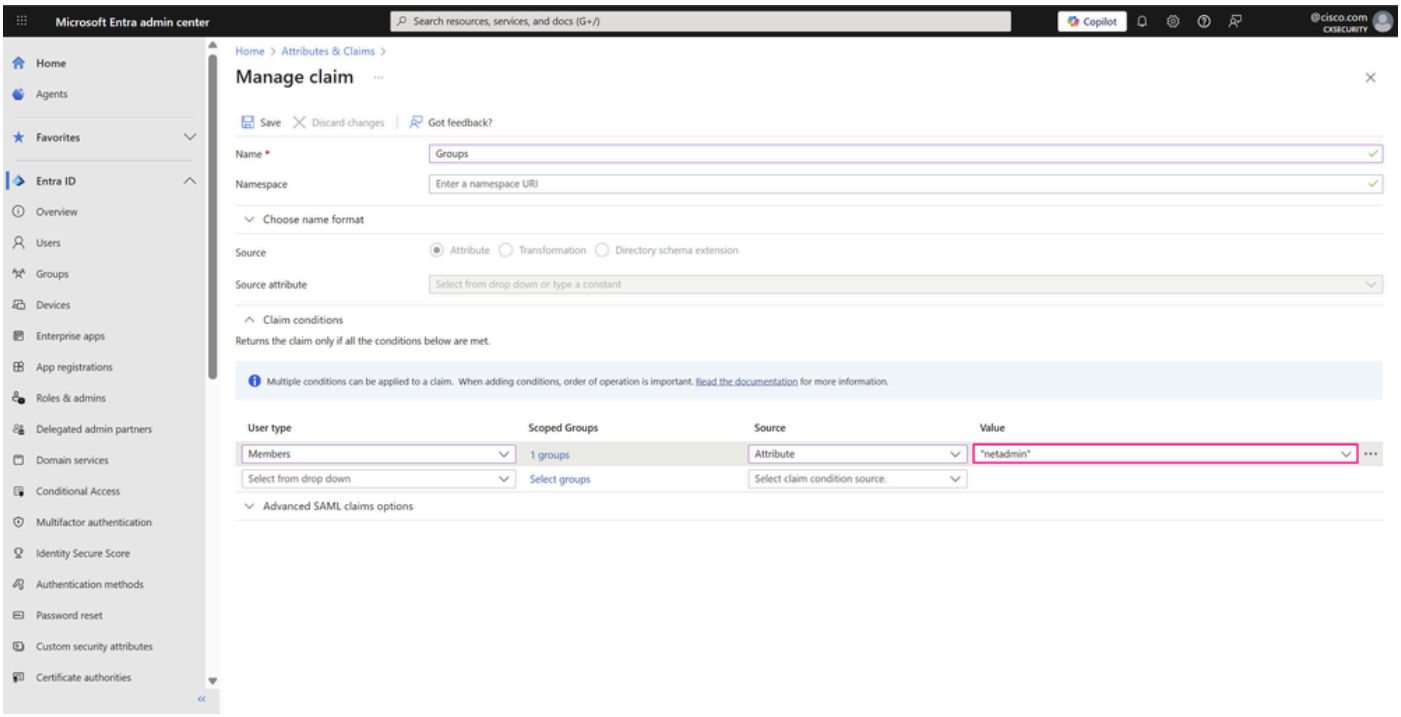


Página Gerenciar reivindicação

- Imediatamente depois, o valor do atributo aparece entre aspas, pois o Microsoft Entra ID trata esse valor como uma string.

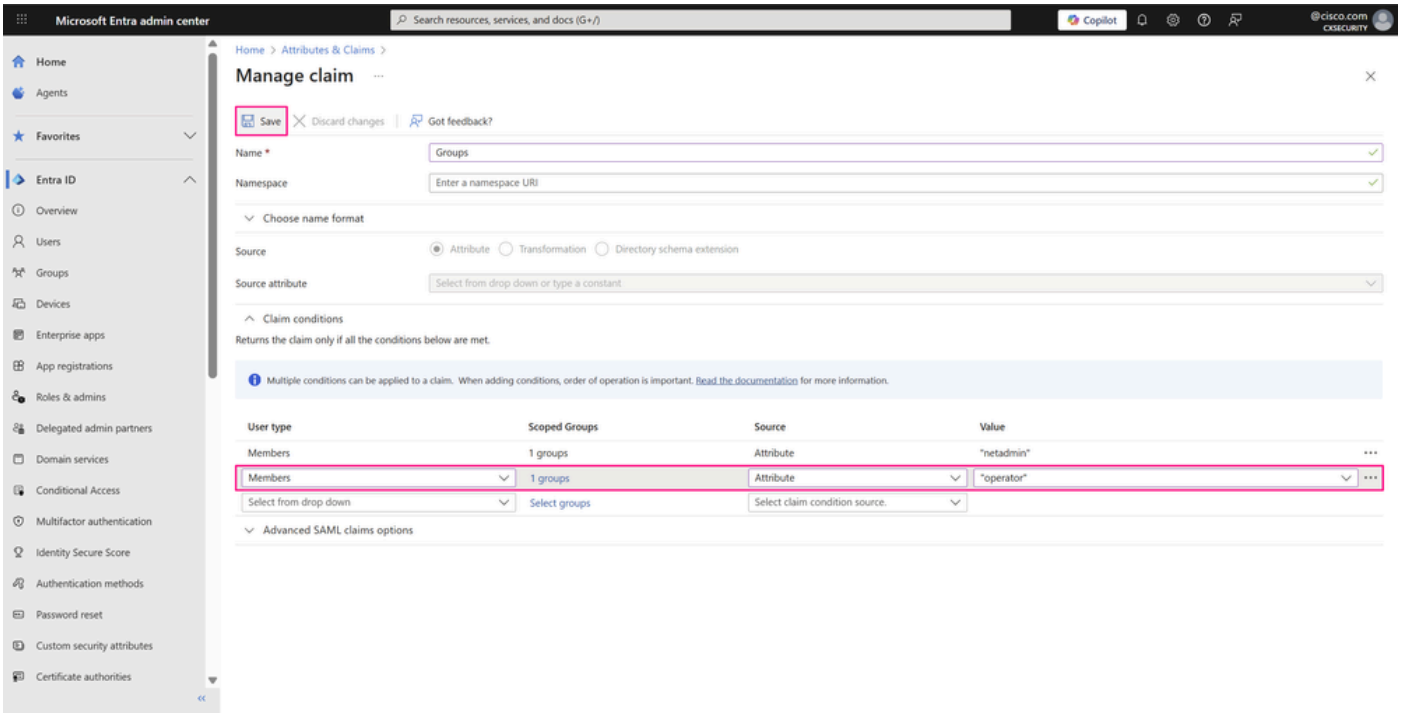


Note: Esses parâmetros nas condições de declaração são altamente relevantes na configuração SSO SAML do aplicativo empresarial, já que esses atributos personalizados devem sempre corresponder aos grupos de usuários definidos no Cisco SD-WAN Manager. Essa correspondência determina os privilégios ou permissões concedidos aos usuários com base no grupo ao qual eles pertencem na ID do Microsoft Entra.



Página Gerenciar reivindicação

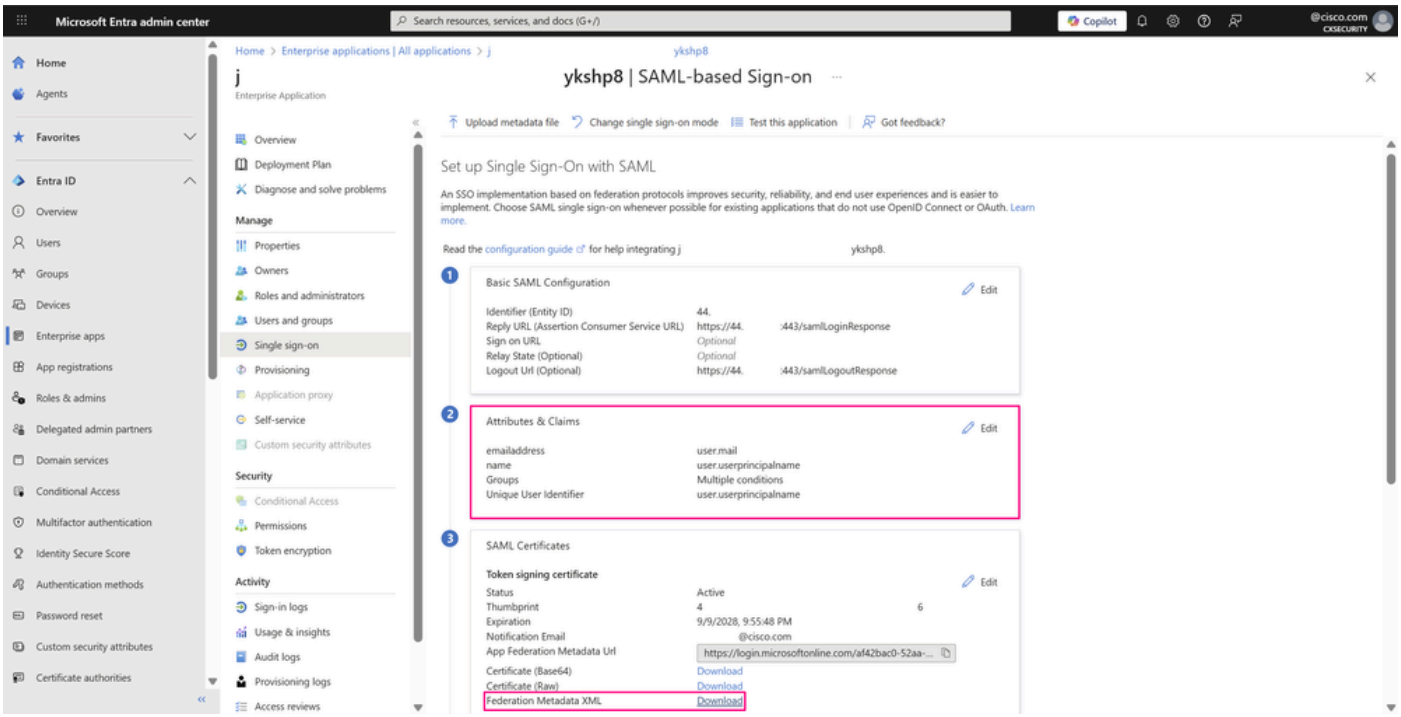
- Repita as mesmas etapas para uma segunda condição de declaração para o segundo grupo criado, que mapeia para o grupo de usuários do operador no Cisco SD-WAN Manager. Esse processo é necessário para cada grupo diferente com permissões específicas que você deseja que entre no aplicativo. Você também pode adicionar vários grupos em uma única condição. Clique em Save para salvar as alterações.



Página Gerenciar reivindicação

- Na página Configurar Single Sign-On com SAML, a seção Atributos e Reivindicações mostra as novas alterações feitas. Para concluir a configuração na ID do Microsoft Entra,

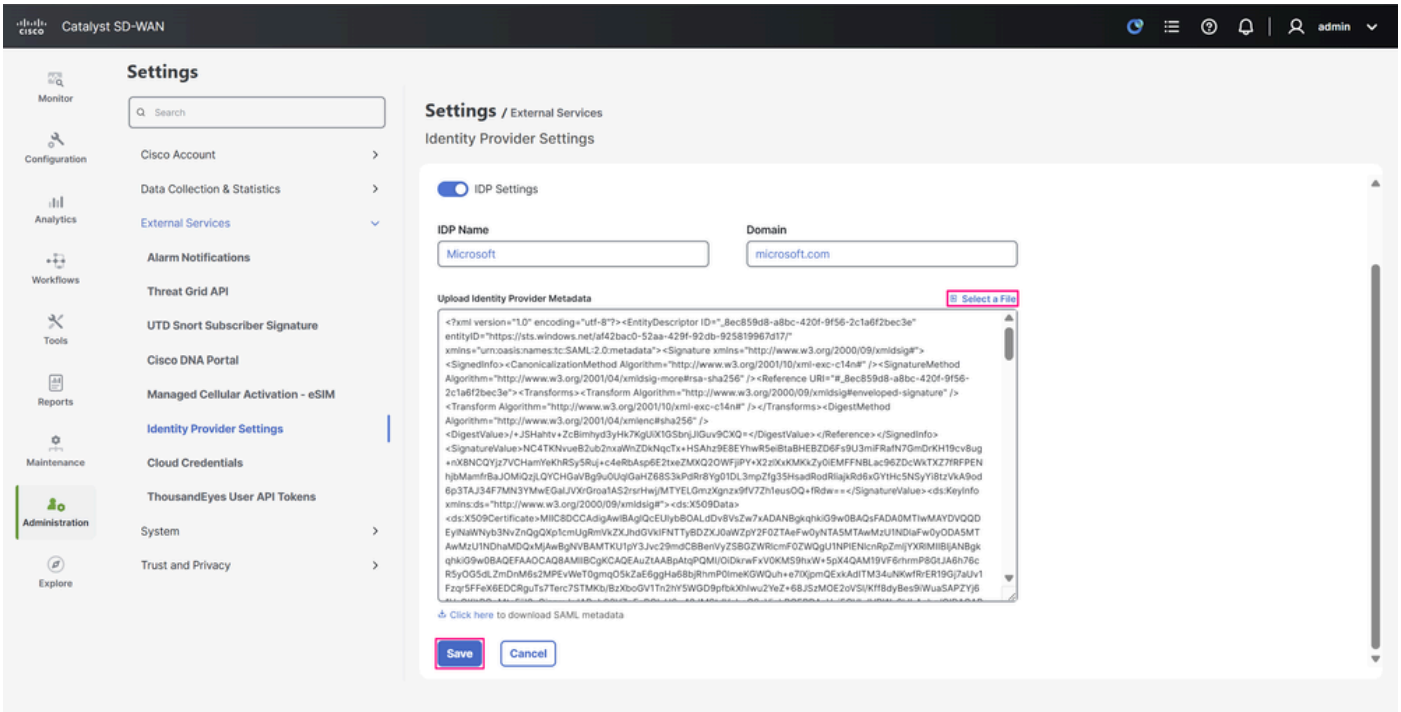
em Certificados SAML, clique em Download ao lado de XML de Metadados de Federação para baixar o arquivo XML que fornece serviços de identidade para o aplicativo.



Página SSO com Configuração SAML

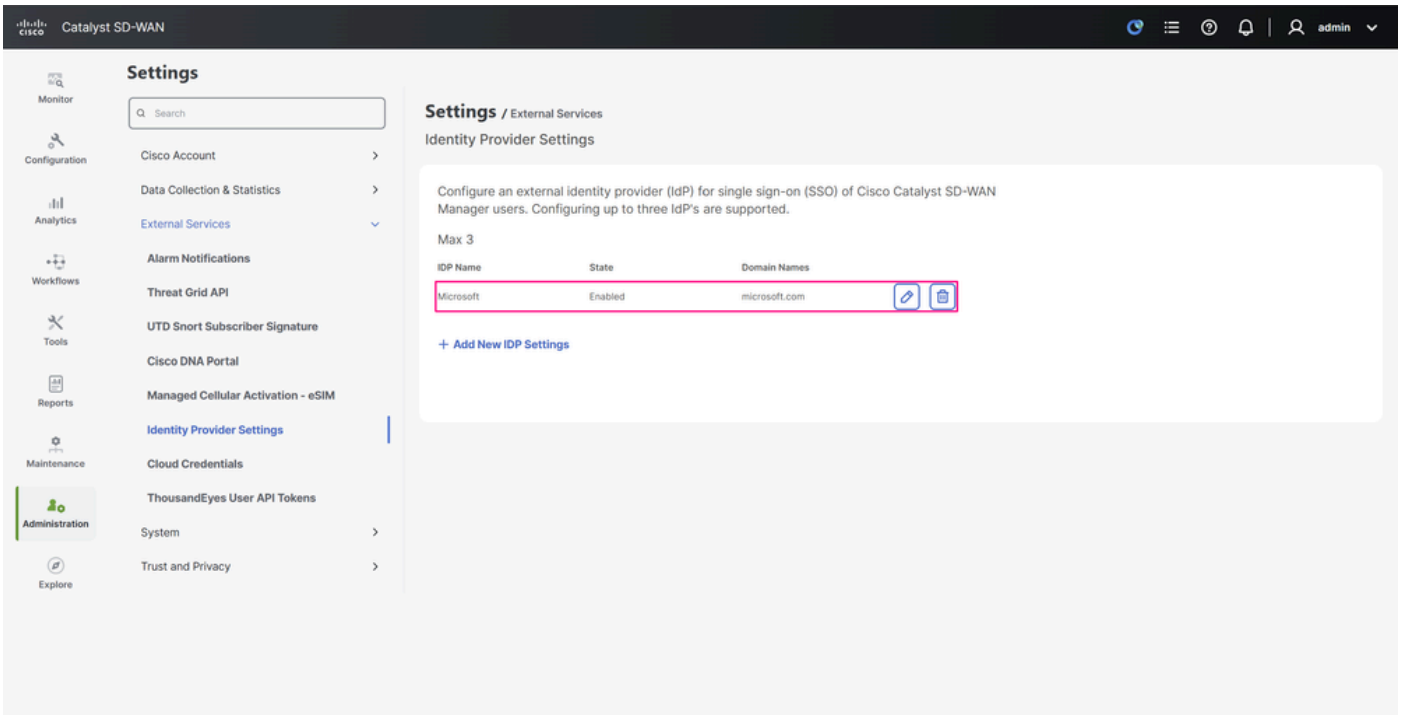
Etapa 5. Importar o arquivo de metadados do Microsoft Entra ID SAML para o Cisco SD-WAN Manager

- Para carregar os metadados de federação no Cisco SD-WAN Manager, navegue para Administração > Configurações > Serviços Externos > Configurações do Provedor de Identidade e clique em Selecionar um arquivo. Escolha o arquivo que você acabou de baixar do Microsoft Entra ID e clique em Salvar.



Página Configuração de Definições de IdP

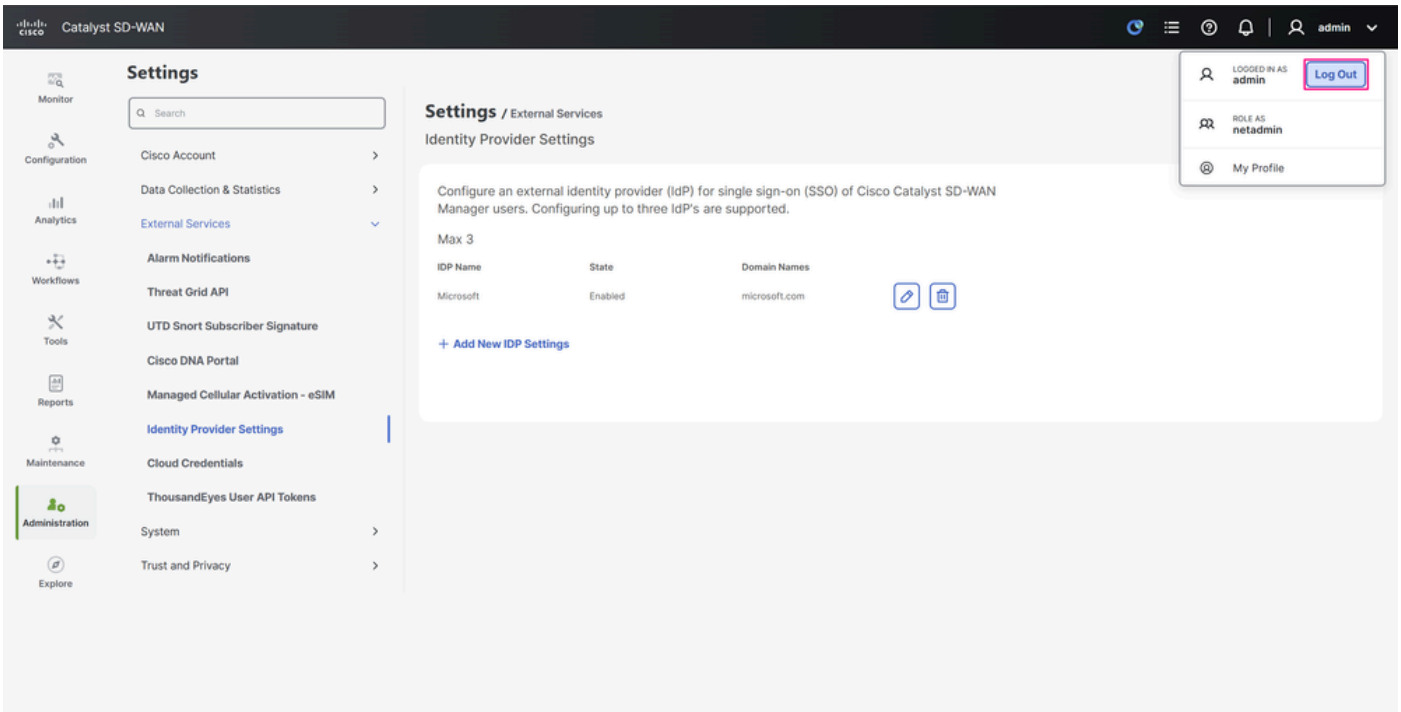
- As configurações de IdP e os metadados foram salvos.



Página Configuração de Definições de IdP

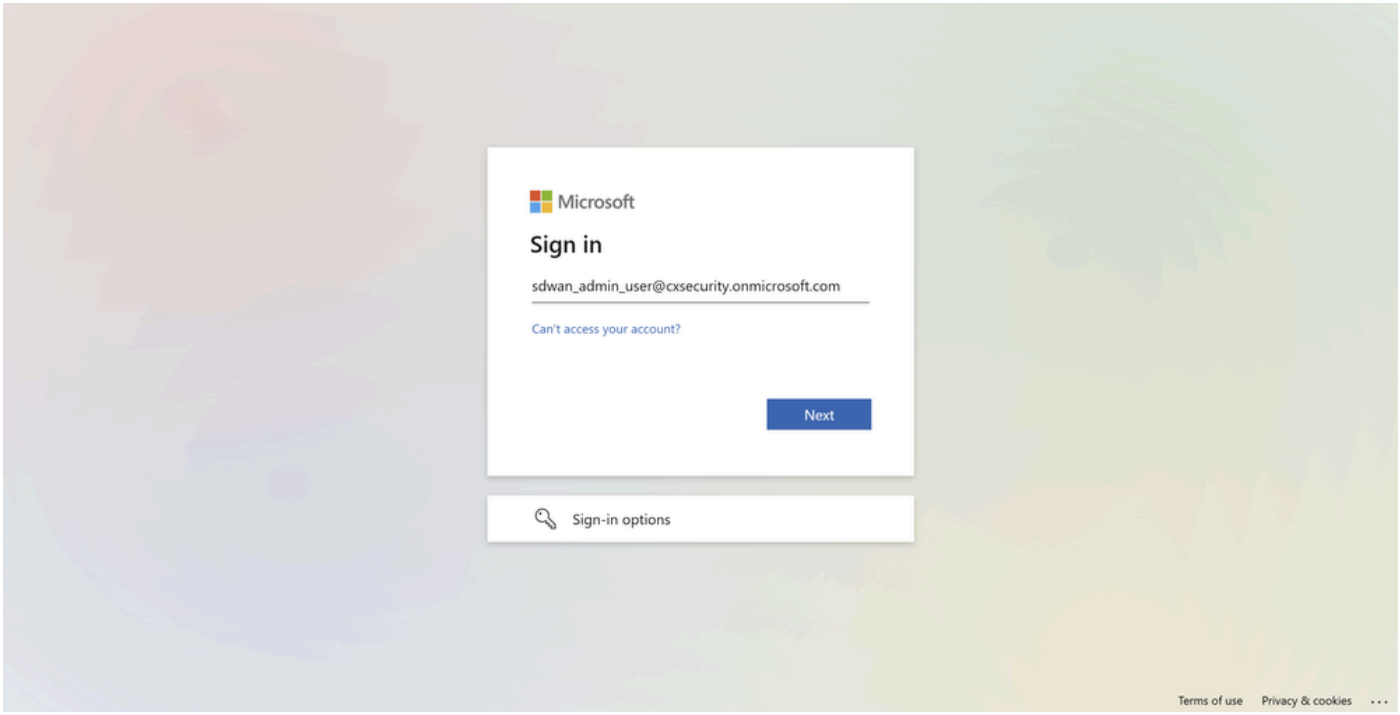
Verificar

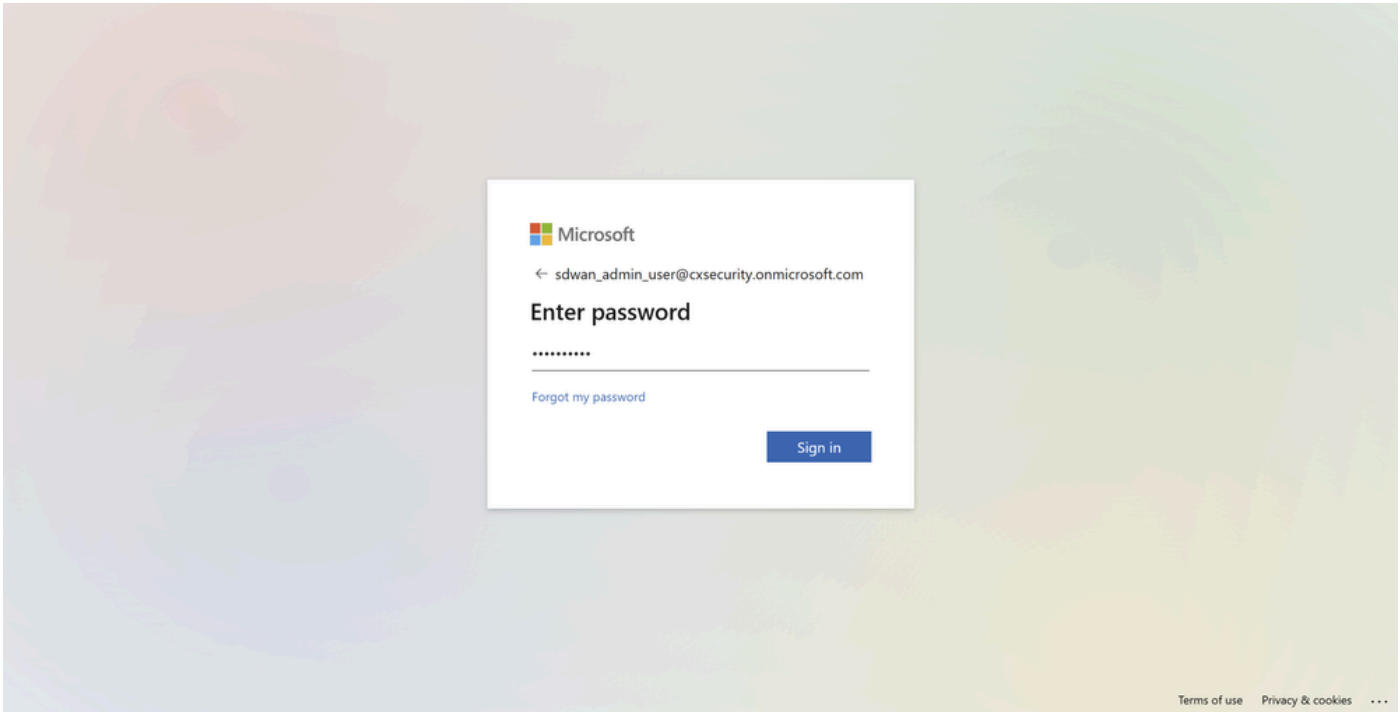
- Clique no nome do perfil no canto superior direito da interface do usuário para expandir as opções. Em seguida, clique em Logoff para sair do portal.



Menu Perfil

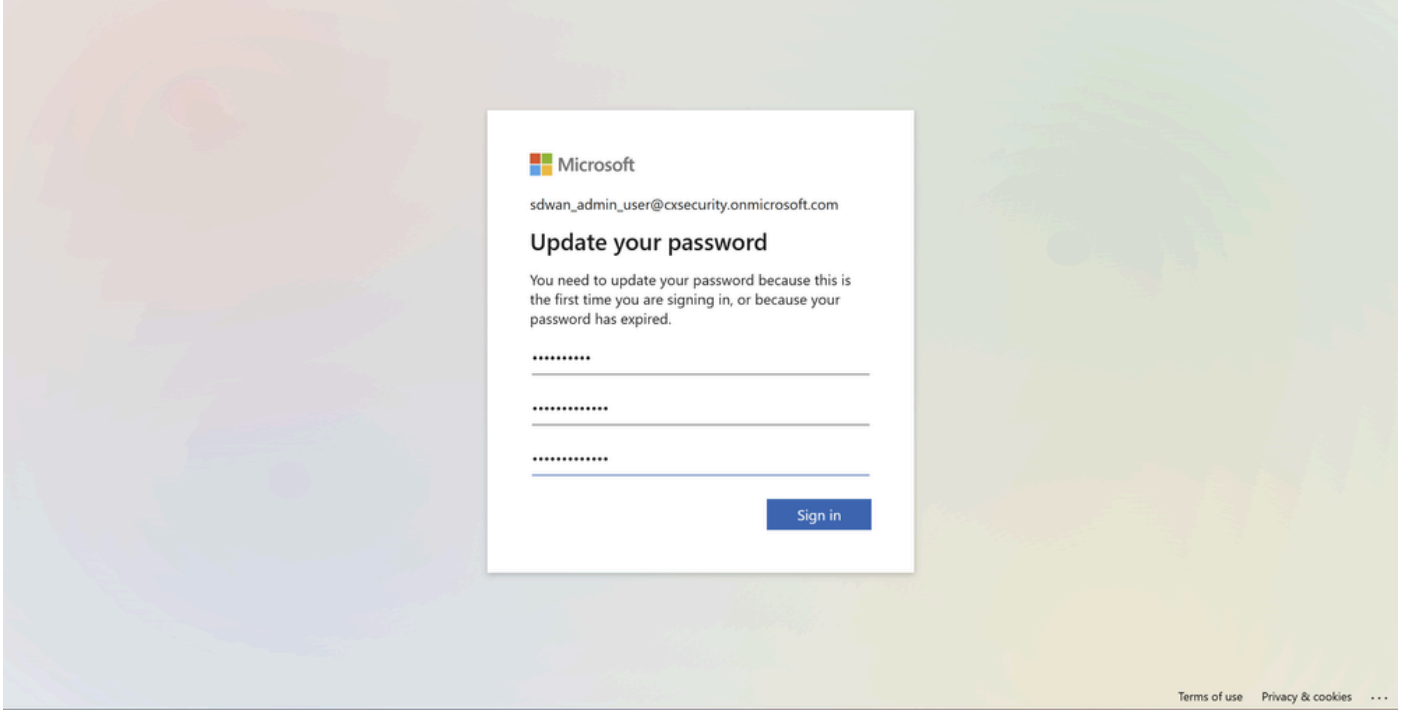
- Você será redirecionado imediatamente para a tela de autenticação da Microsoft, onde você entrará com as credenciais dos usuários do SSO da ID do Microsoft Entra.





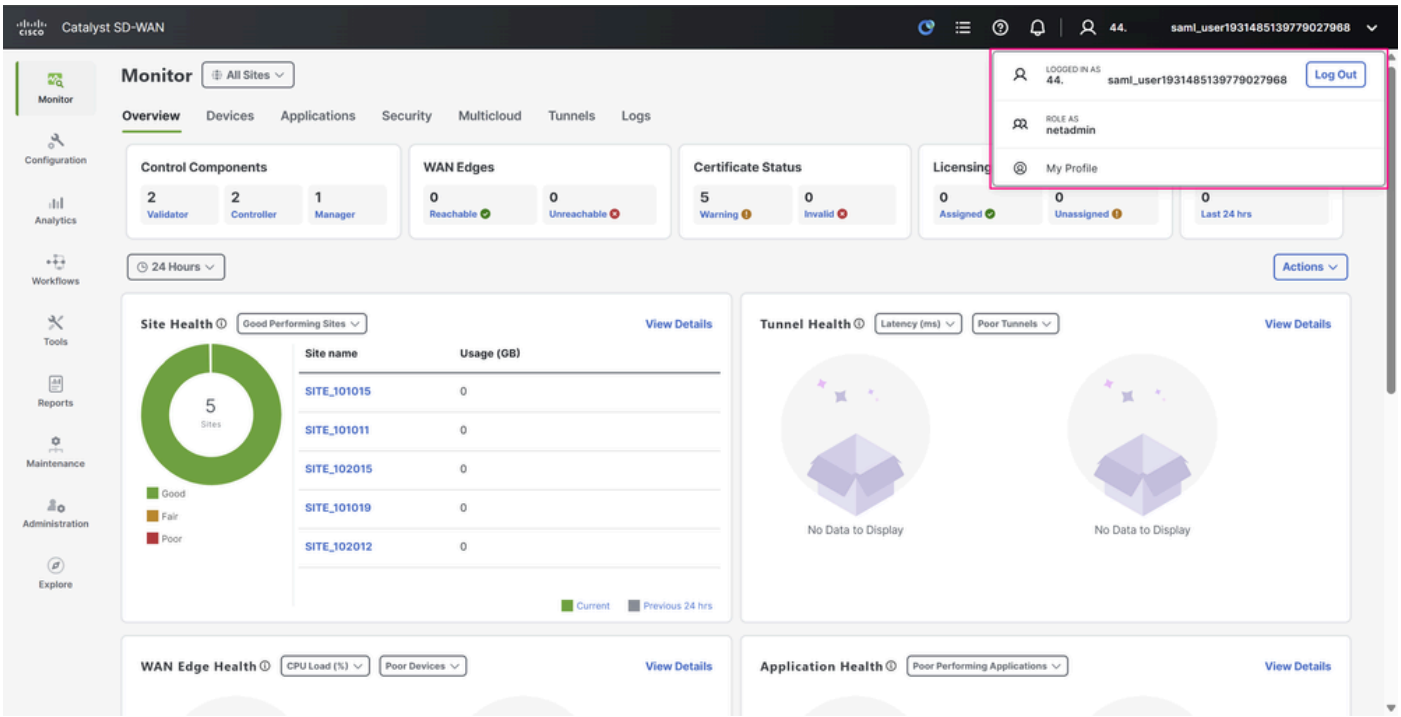
Tela de login da Microsoft

- Como esta é a primeira vez que o usuário do SSO efetua login, o prompt solicita uma alteração de senha.



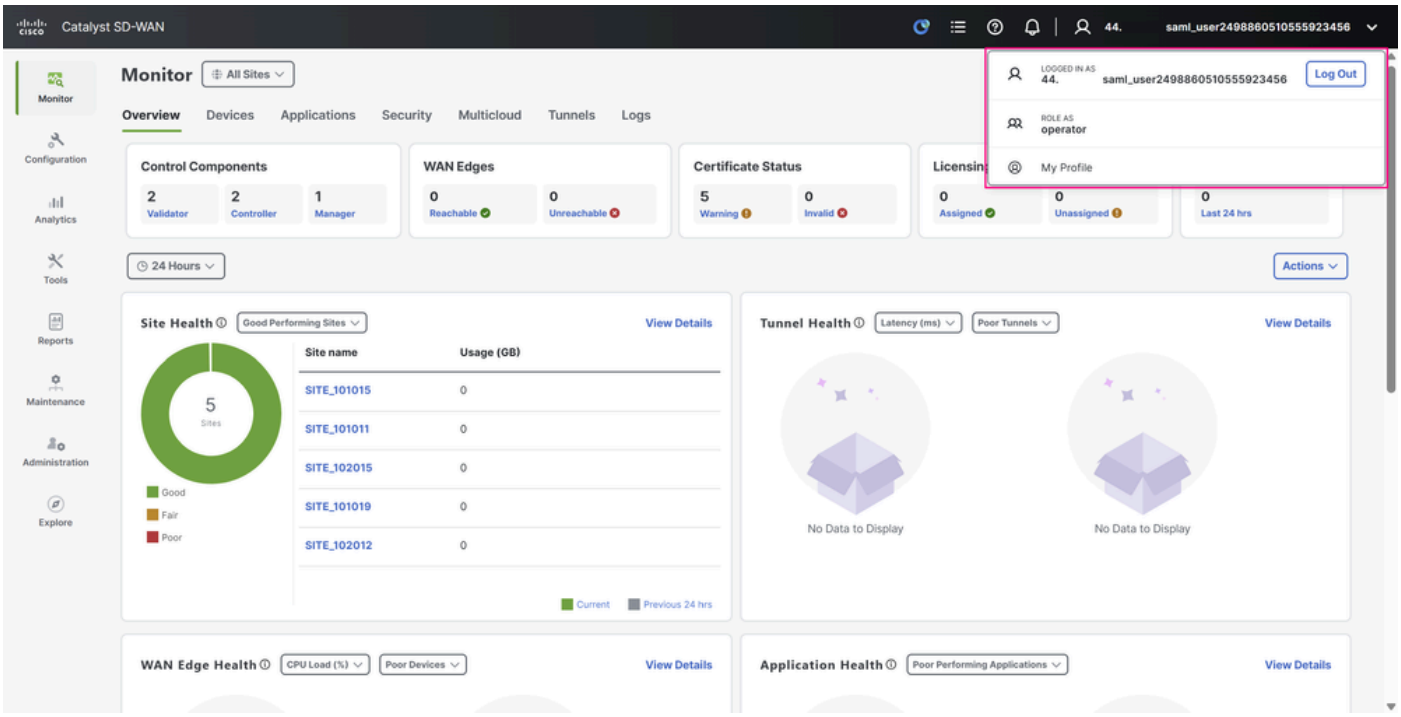
Tela de login da Microsoft

- Após uma entrada bem-sucedida, expanda os detalhes do seu perfil novamente no canto superior direito do painel e você poderá confirmar se o usuário foi detectado com uma função netadmin, exatamente como configurado no Microsoft Entra ID.



Interface do usuário do Cisco SD-WAN Manager

- Por fim, execute o mesmo teste de entrada com o outro usuário. Você vê o mesmo comportamento — o usuário agora é identificado com a função de operador.



Interface do usuário do Cisco SD-WAN Manager

Informações Relacionadas

- Configurar Single Sign-On no Cisco IOS XE Catalyst SD-WAN

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.