Provisionar usuários e grupos para acesso seguro via OKTA

Contents

Introdução

Este documento descreve como provisionar grupos de usuários do OKTA para o Cisco Secure Access.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro da Cisco
- OKTA

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

- Painel do Cisco Secure Access

- OKTA

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 Cisco Secure Access suporta o provisionamento de usuários e grupos do OKTA.

Esse provisionamento permite que o Secure Access mantenha um diretório de usuários autorizados a:

- Inscreva-se no Zero Trust Access (ZTA).
- Conecte-se ao VPNaaS.
- Aplique políticas baseadas em identidade aos usuários do Umbrella Roaming.

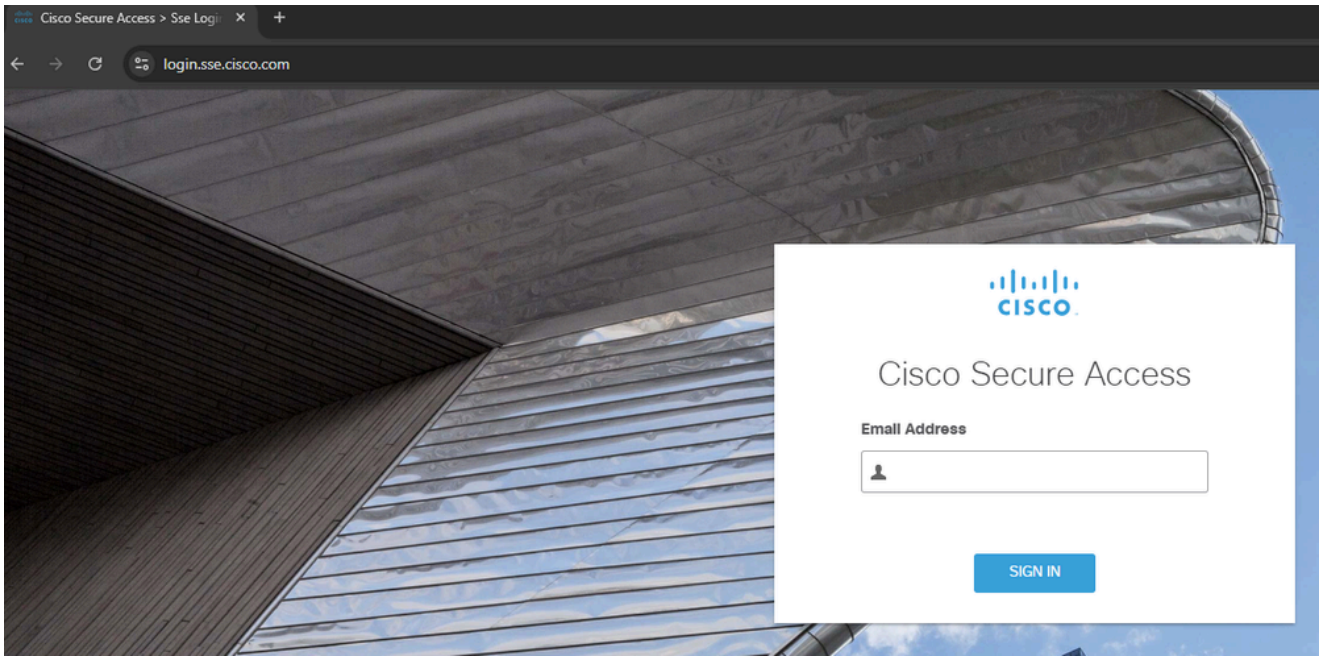
Note: Este documento se concentra especificamente no provisionamento de usuários e grupos do OKTA. A configuração de Entra ID ou outros Provedores de Identidade (IdP) para registro ZTA, autenticação VPNaaS ou configurações específicas de Umbrella Roaming está fora do escopo deste guia.

Configurar

Configurar o Cisco Secure Access

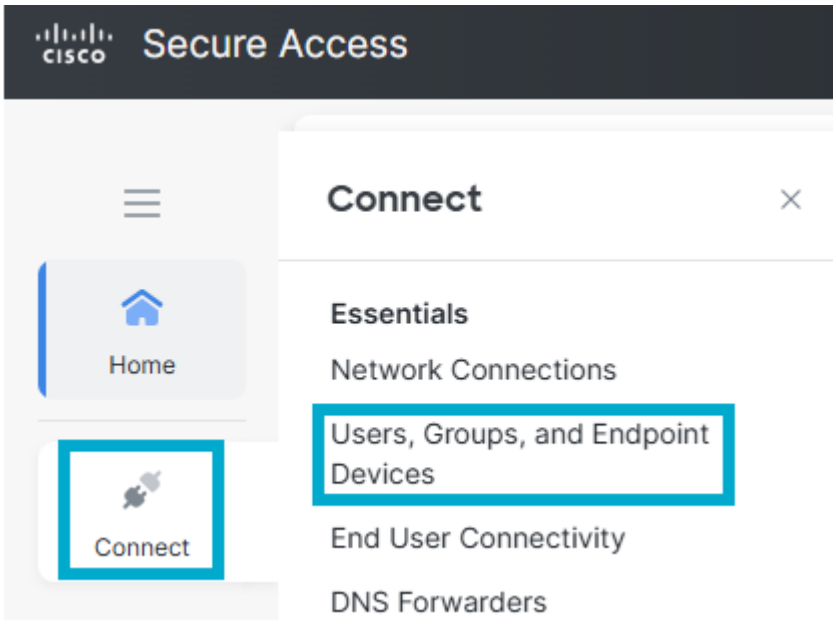
Para iniciar o processo de provisionamento, você deve primeiro configurar a integração de diretórios no painel do Cisco Secure Access. Esta etapa gera as credenciais necessárias e os parâmetros de configuração necessários para estabelecer uma conexão segura com o OKTA.

1. Inicie sessão no Cisco Secure Access Dashboard.



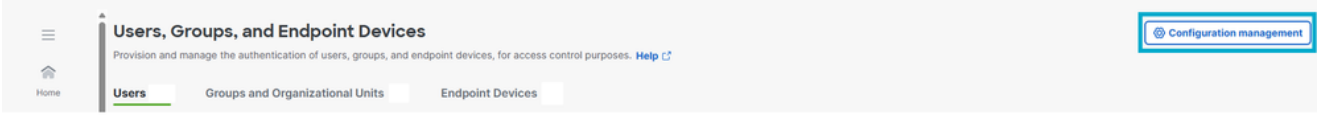
Entrar no CSA

2. Navegue até Connect > Users, Groups and Endpoint Devices.



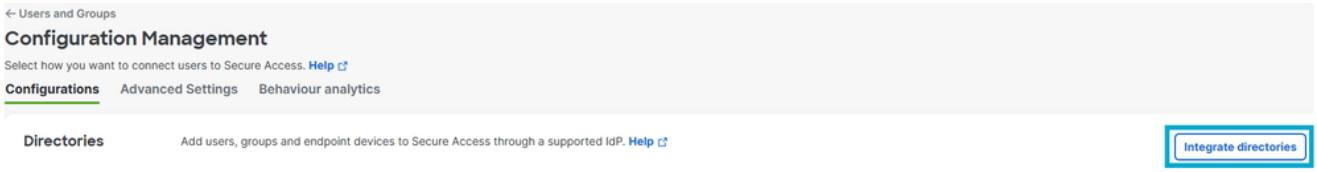
Usuários e grupos

3. Clique em Gerenciamento de configuração.



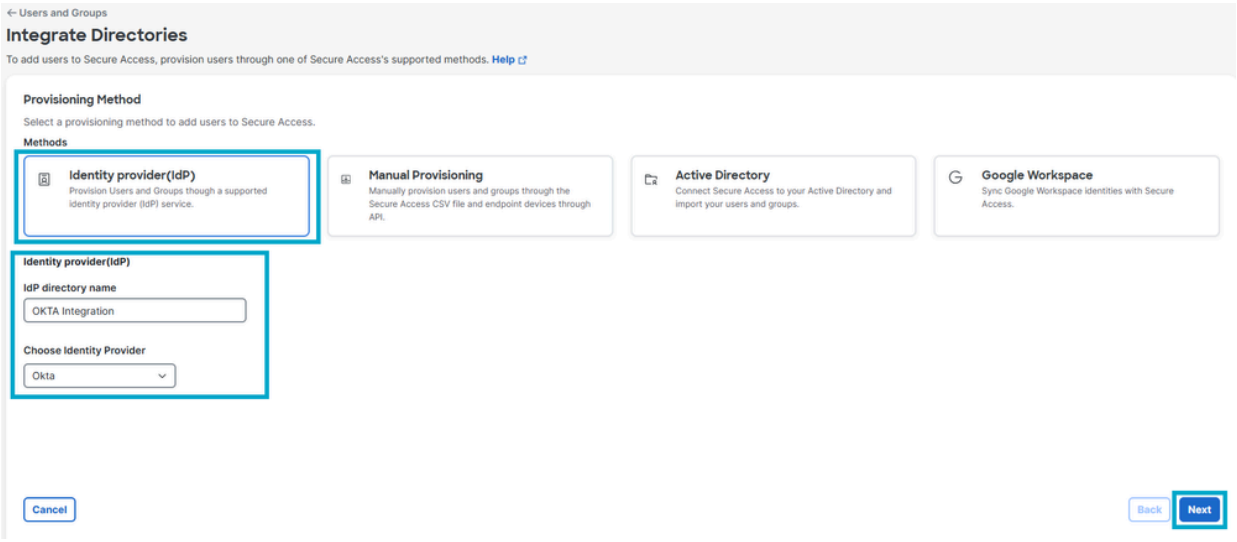
Gerenciamento de configuração

4. Clique em Integrar diretório.



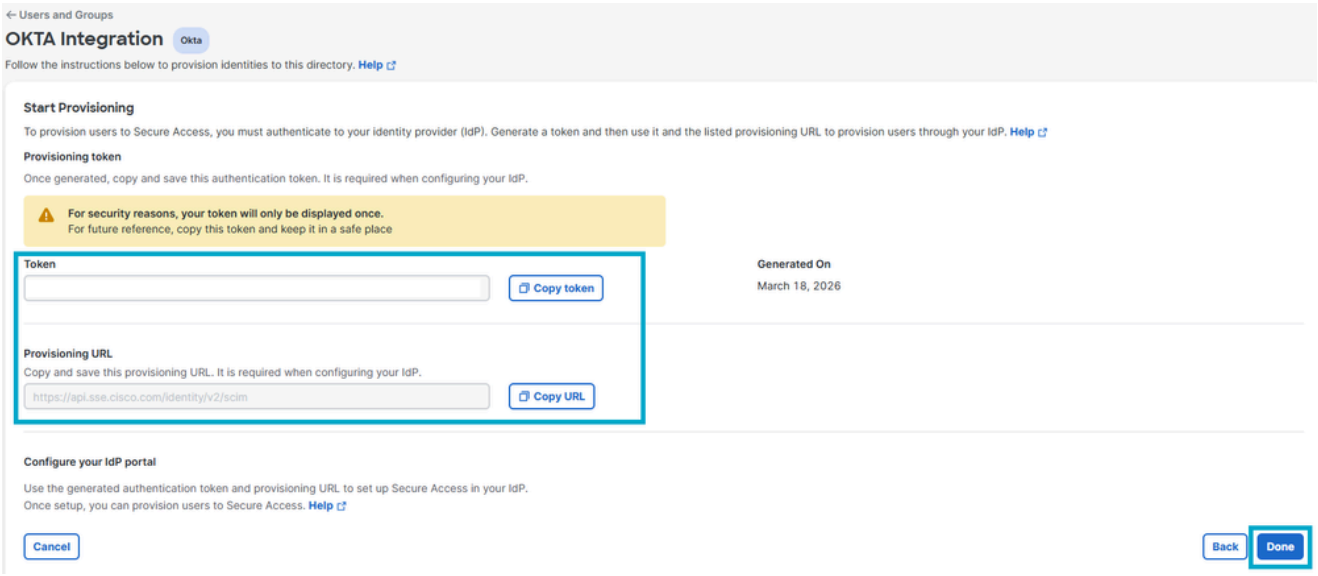
Diretório de integração

5. Em Método de provisionamento, clique em Provedor de identidade.
    - Nome do diretório IdP: Integração OKTA.
    - Escolher Provedor de Identidade: OKTA.
    - Clique em Next.



Directory Configuration

6. Clique em Gerar token. Salve o token gerado e o URL de provisionamento e clique em Concluído.

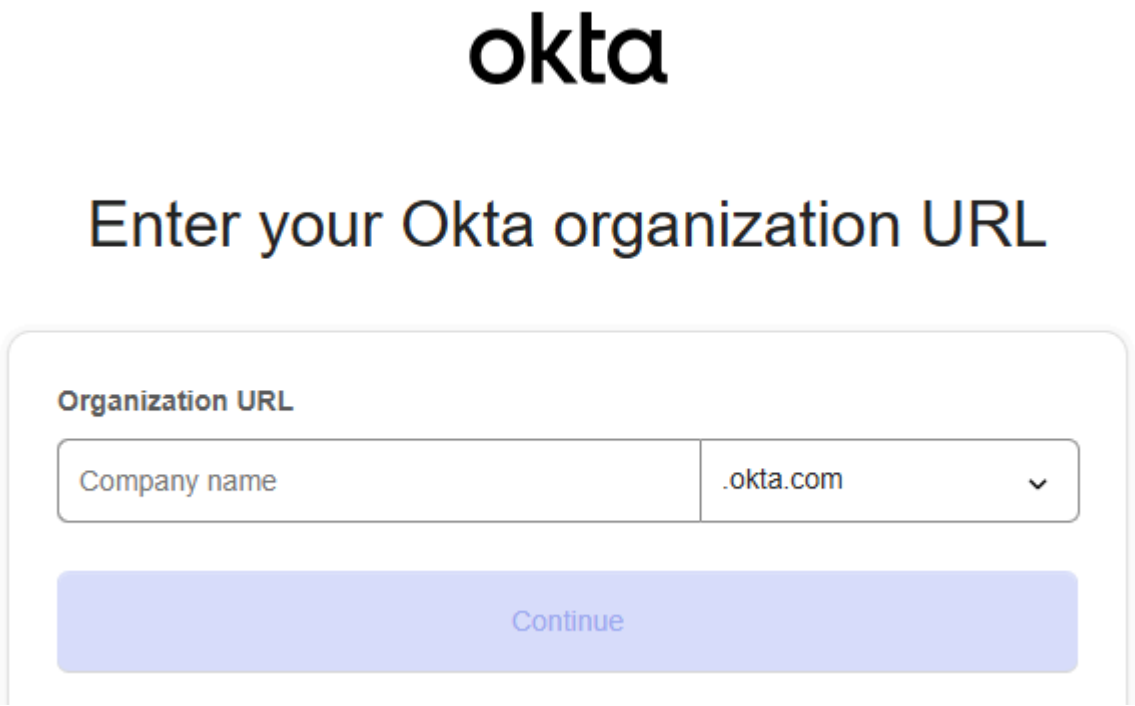


Gerar token

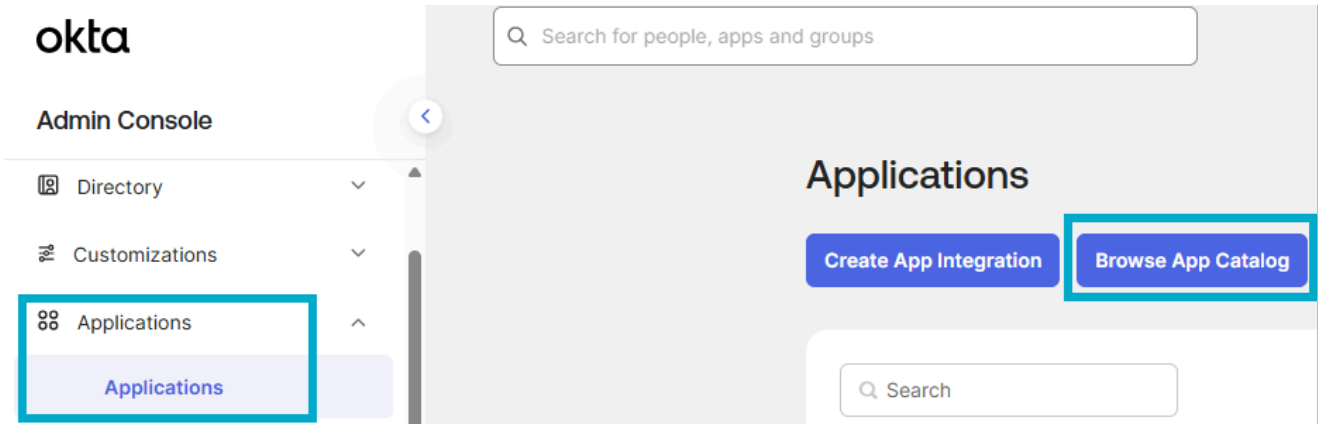
Configurar Provisionamento no OKTA

Depois de ter gerado suas credenciais no painel do Cisco Secure Access, você deve definir as configurações de provisionamento em seu locatário OKTA para habilitar a sincronização de usuários e grupos.

1. Entre no OKTA.

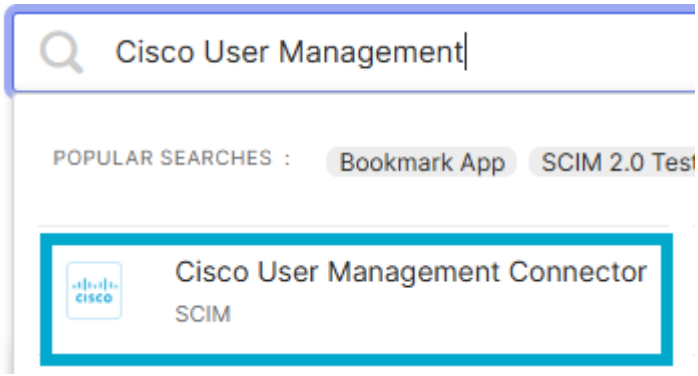


2. Navegue até Aplicativos > Catálogo de aplicativos do navegador.



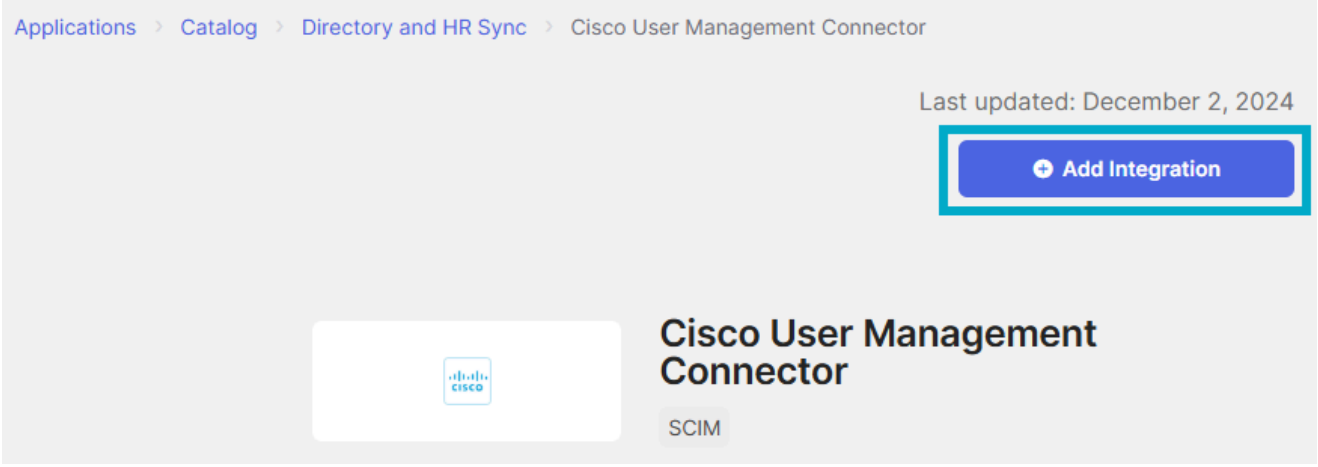
Procurar Catálogo de Aplicativos

3. Selecione o aplicativo Cisco User Management Connector.



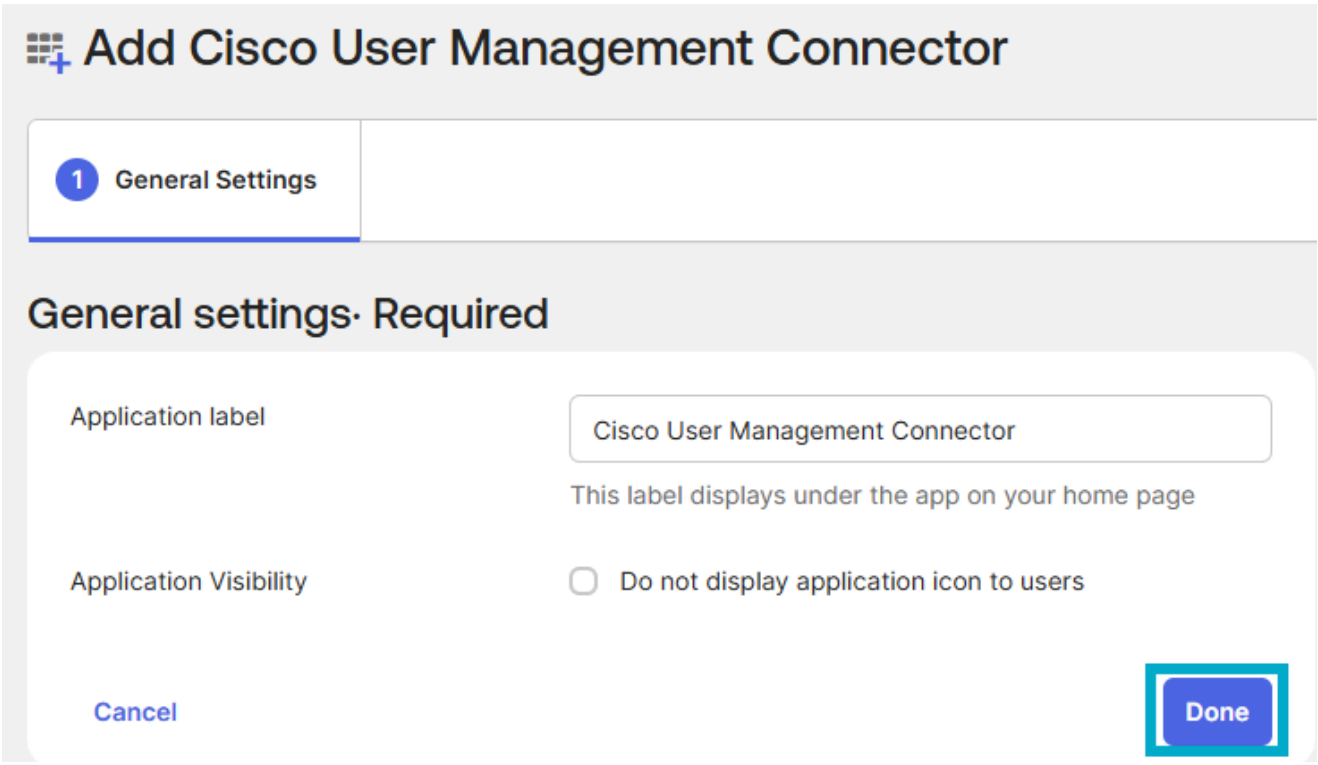
Aplicativo da Cisco

4. Clique em Add Integration.



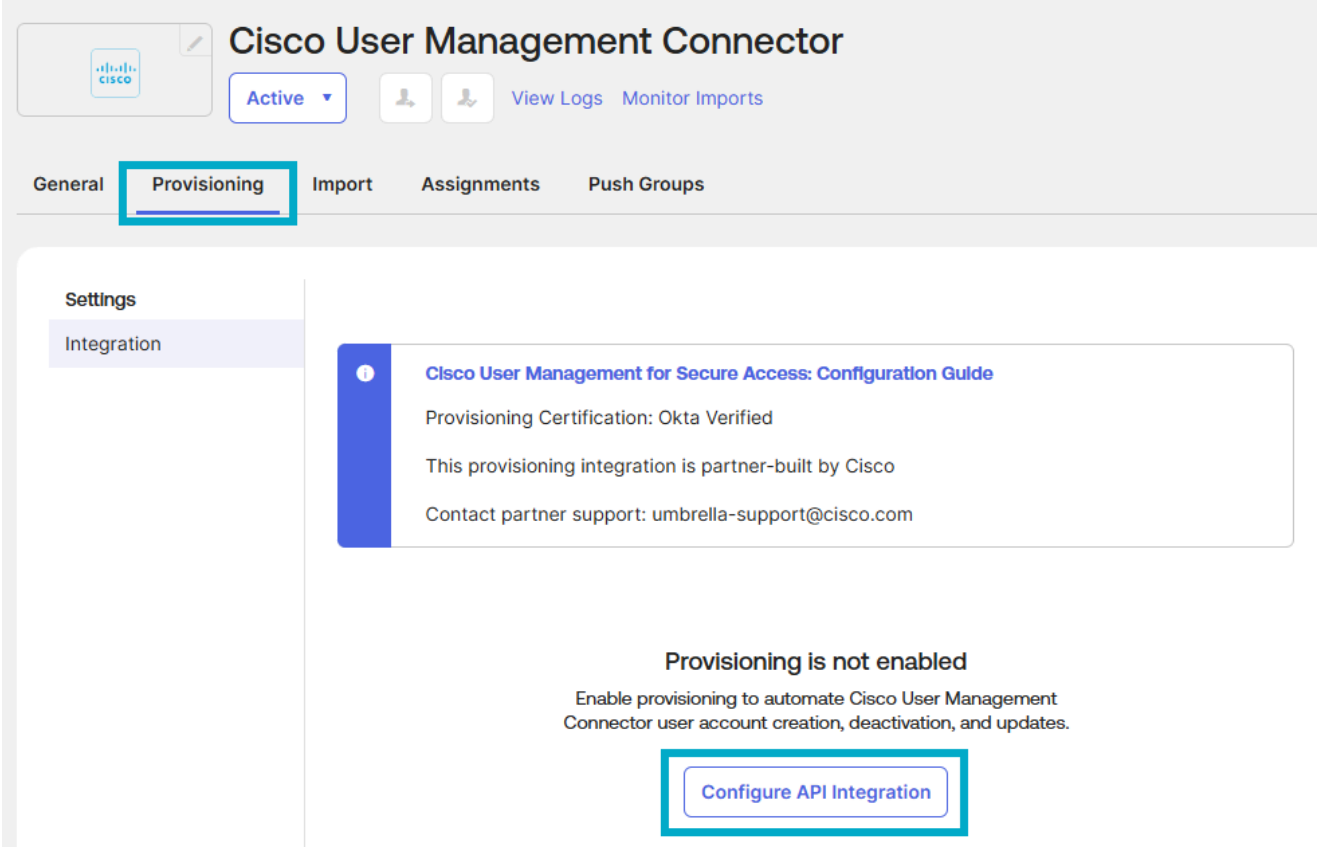
Adicionar integração

5. Clique em Concluído.



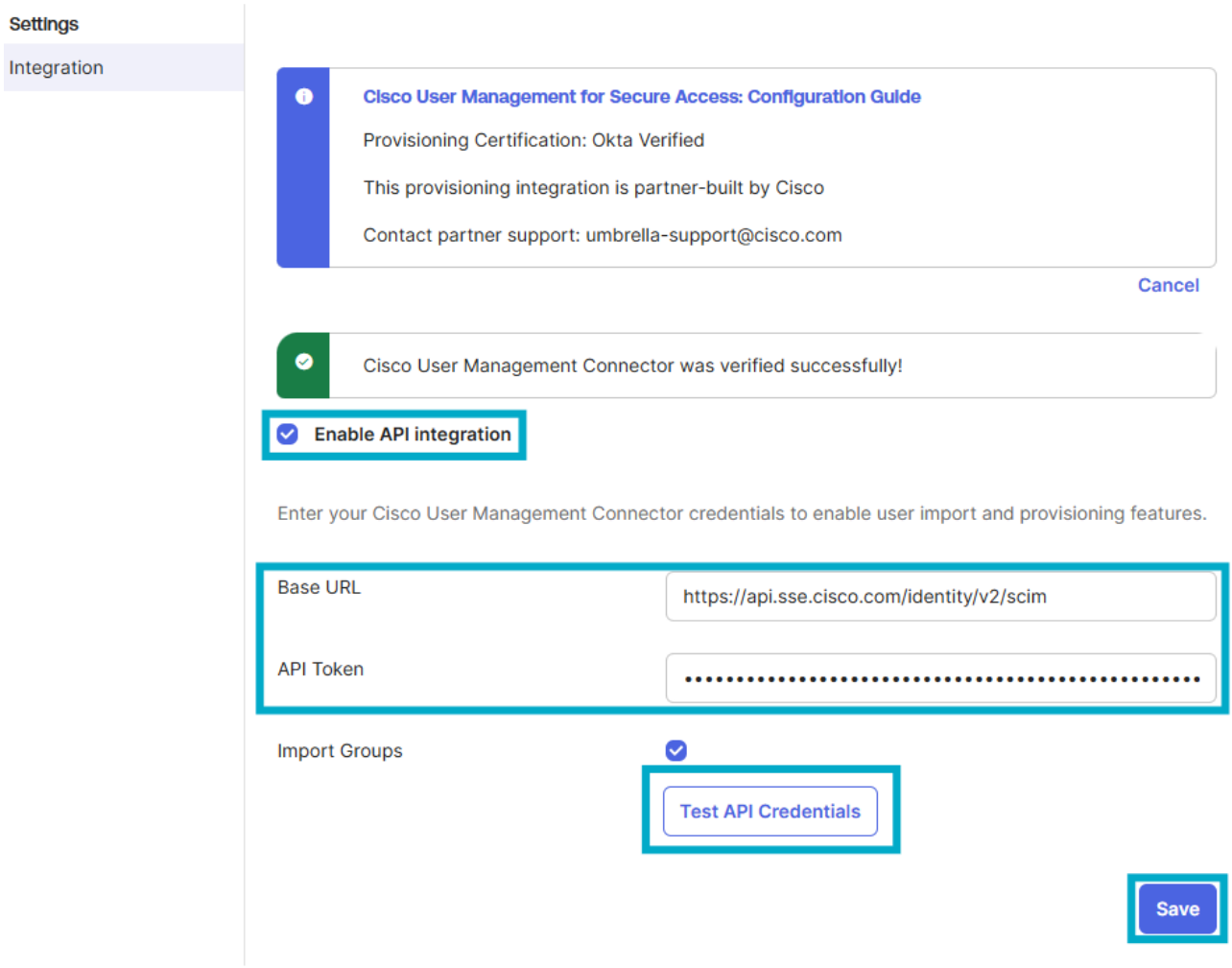
Adicionar aplicativo

6. Clique em Provisionamento > Configurar integração de API.



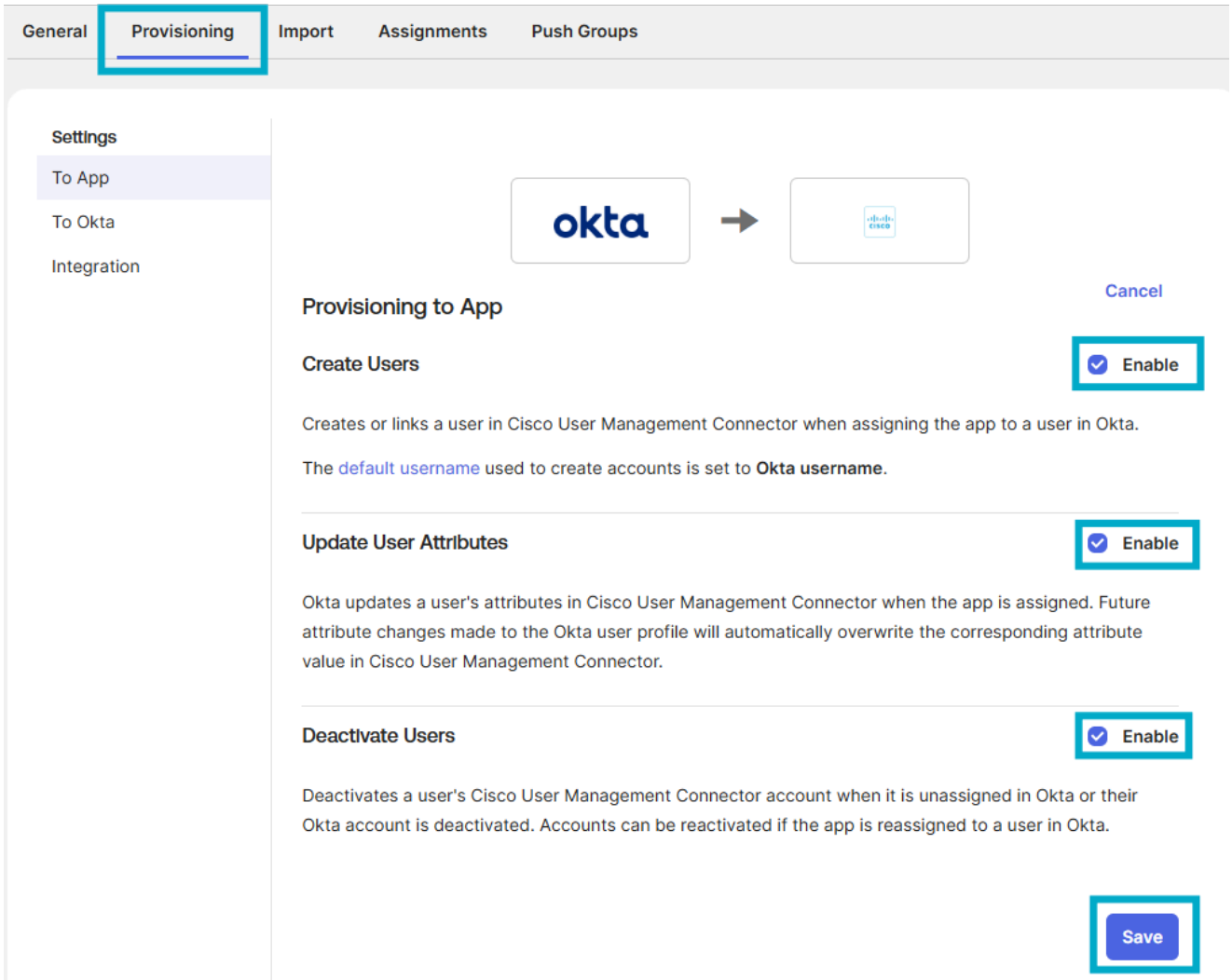
Configurar Integração de API

7. Clique em Enable API Integration e insira os tokens Based URL e API salvos da etapa #6 da Secure Access Configuration. Clique em Testar credenciais da API e em Salvar.



Teste de API

8. Navegue até Provisionamento > Para aplicativo. Ative as opções Criar usuários, Atualizar atributos do usuário e Desativar usuários e clique em Salvar.

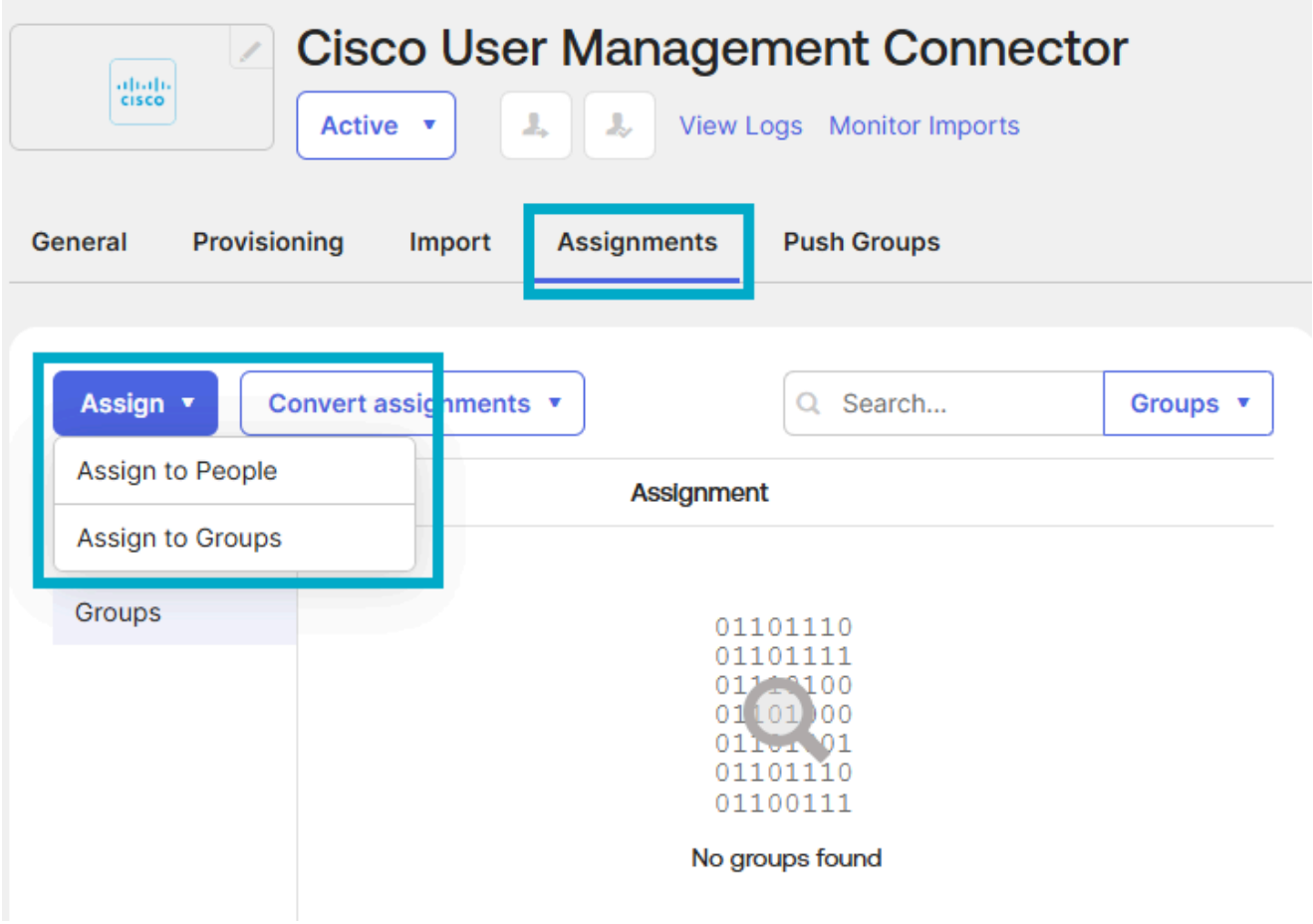


Provisionar para Aplicativo

Note: Verifique se você selecionou esses atributos para sincronização com o Secure Access. O Secure Access lista apenas os atributos Nome de exibição e Nome de usuário para usuários, não os atributos Nome fornecido e Nome da família: Nome de usuário, Nome fornecido, Família, Nome, Nome de exibição, Email

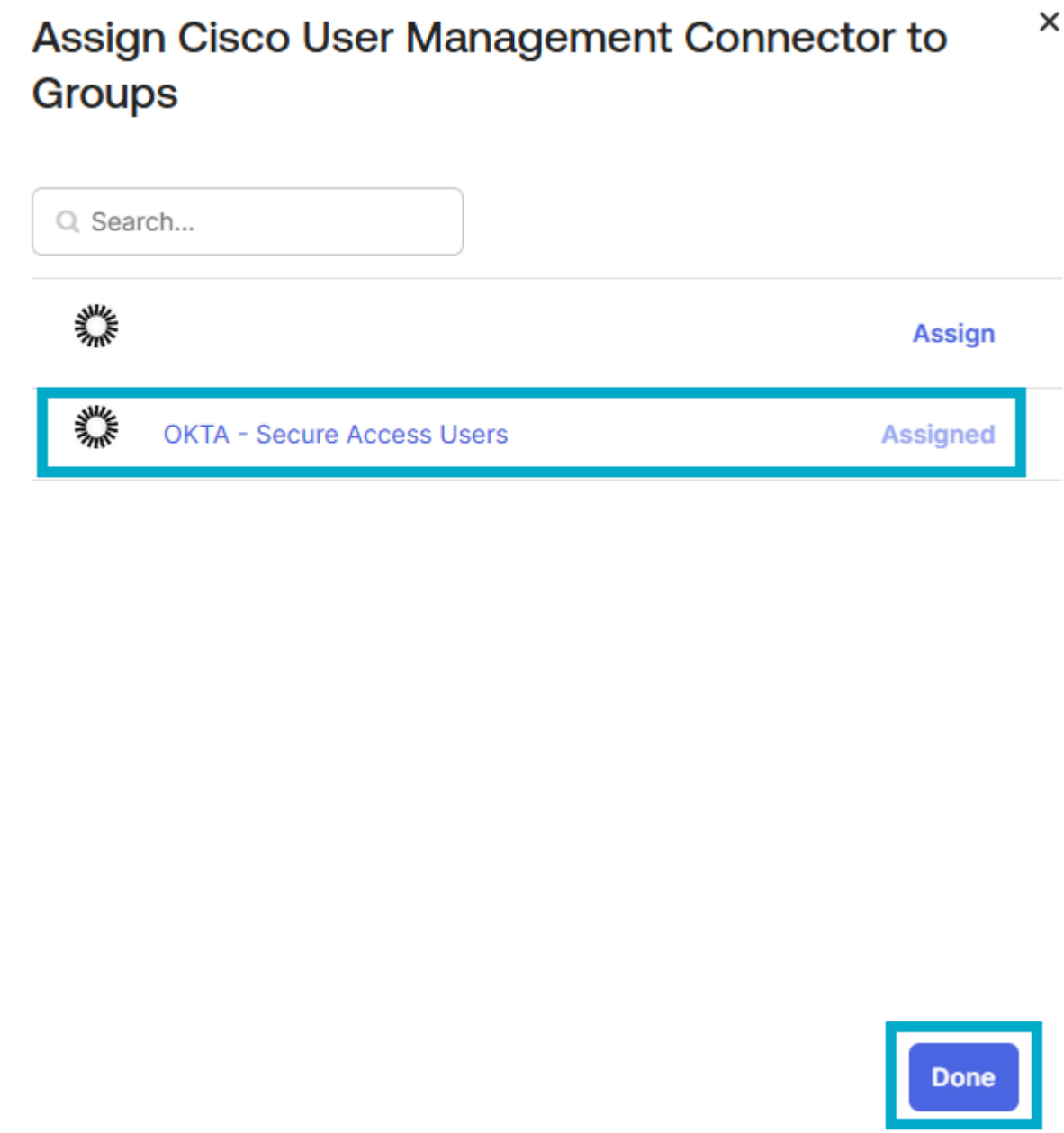
(Opcional) Adicione um Atributo objectGUID e crie o Mapeamento de Perfil de Usuário. Se precisar importar o atributo objectGUID para usuários, adicione um novo atributo e mapeie os atributos no mapeamento de perfil.

9. Para adicionar pessoas/grupos, clique em Atribuições > Atribuir > Atribuir a pessoas/Atribuir a grupos.



Atribuição

10. Selecione os grupos/pessoas que você deseja provisionar para o Secure Access e clique em Atribuir e em Concluído.

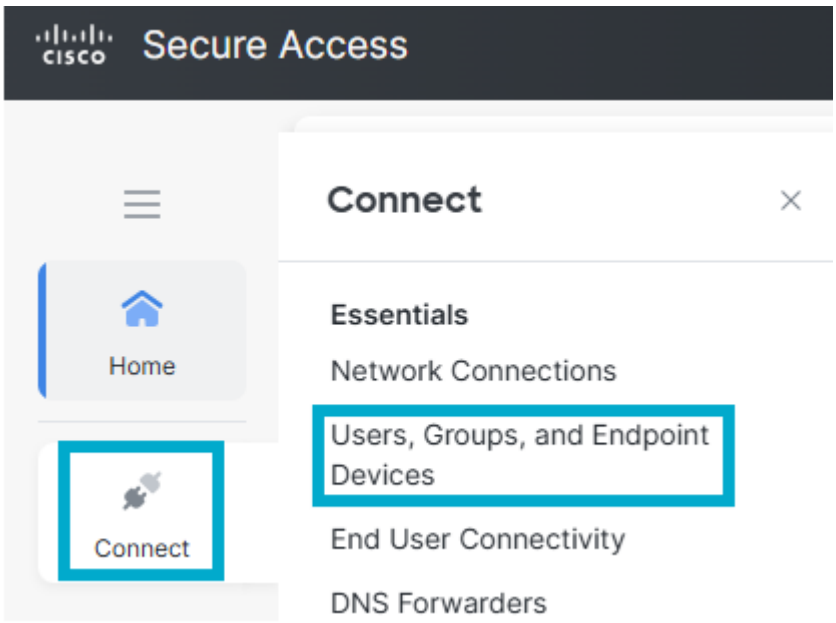


Atribuir grupos

Verificar

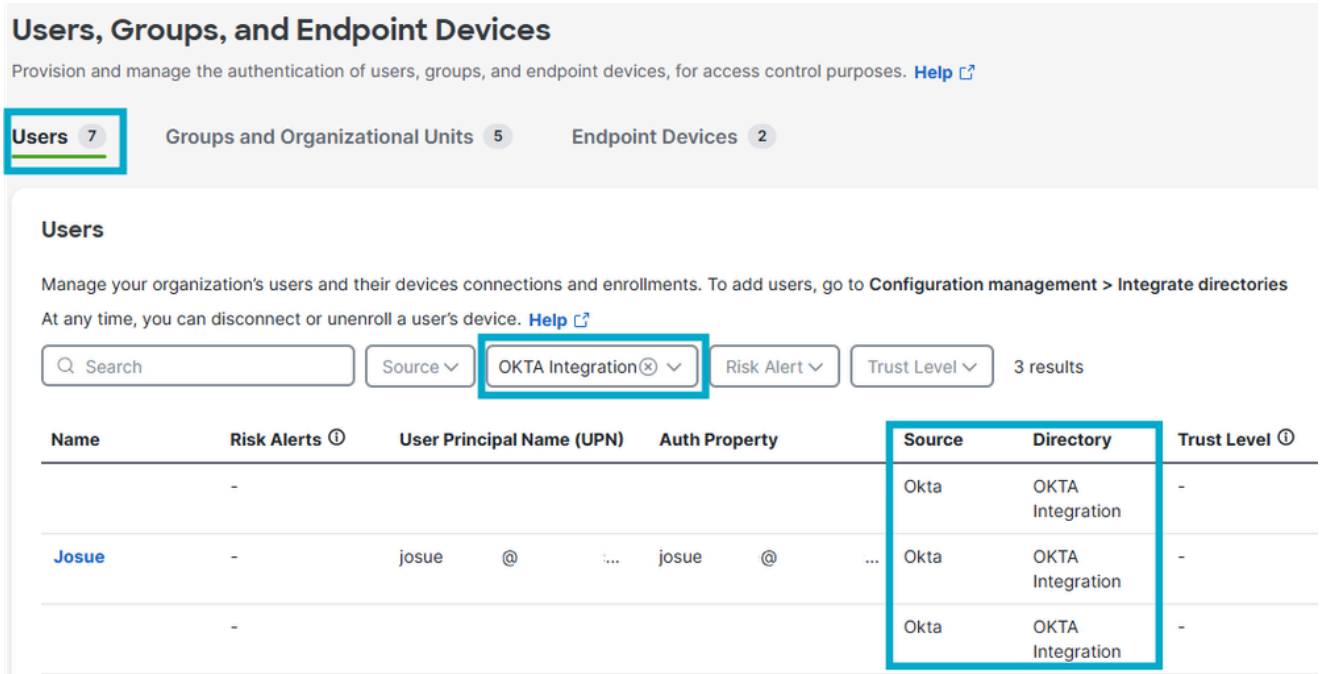
Verity no Cisco Secure Access

- Navegue para Connect > Users, Groups and Endpoint Devices.



Usuários e grupos no CSA

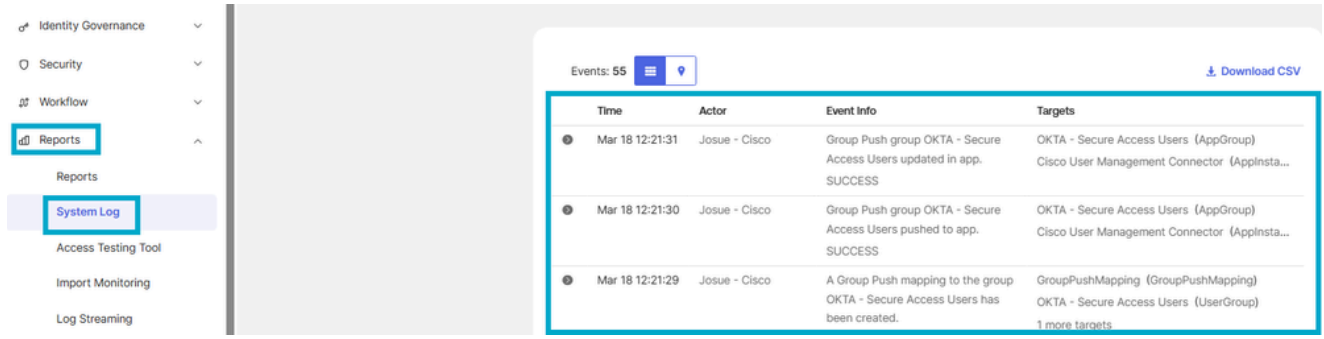
- Clique em Users.



Verificar usuários no CSA

Verity em OKTA

- Navegue até Relatórios > Log do sistema.



Logs OKTA

Informações Relacionadas

[Configurar Provedores de Identidade]

[Provisionar usuários e grupos do Okta]

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.