Aprovisionamiento de usuarios y grupos para un acceso seguro mediante OKTA

Contenido

Introducción

Este documento describe cómo proveer grupos de usuarios de OKTA a Cisco Secure Access.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro de Cisco
- OKTA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

- Panel de Cisco Secure Access

- OKTA

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

Cisco Secure Access admite el aprovisionamiento de usuarios y grupos de OKTA.

Este aprovisionamiento permite a Secure Access mantener un directorio de usuarios autorizados para:

- Inscríbase en Zero Trust Access (ZTA).
- Conéctese a VPNaaS.
- Aplique políticas basadas en identidad a los usuarios de Umbrella Roaming.

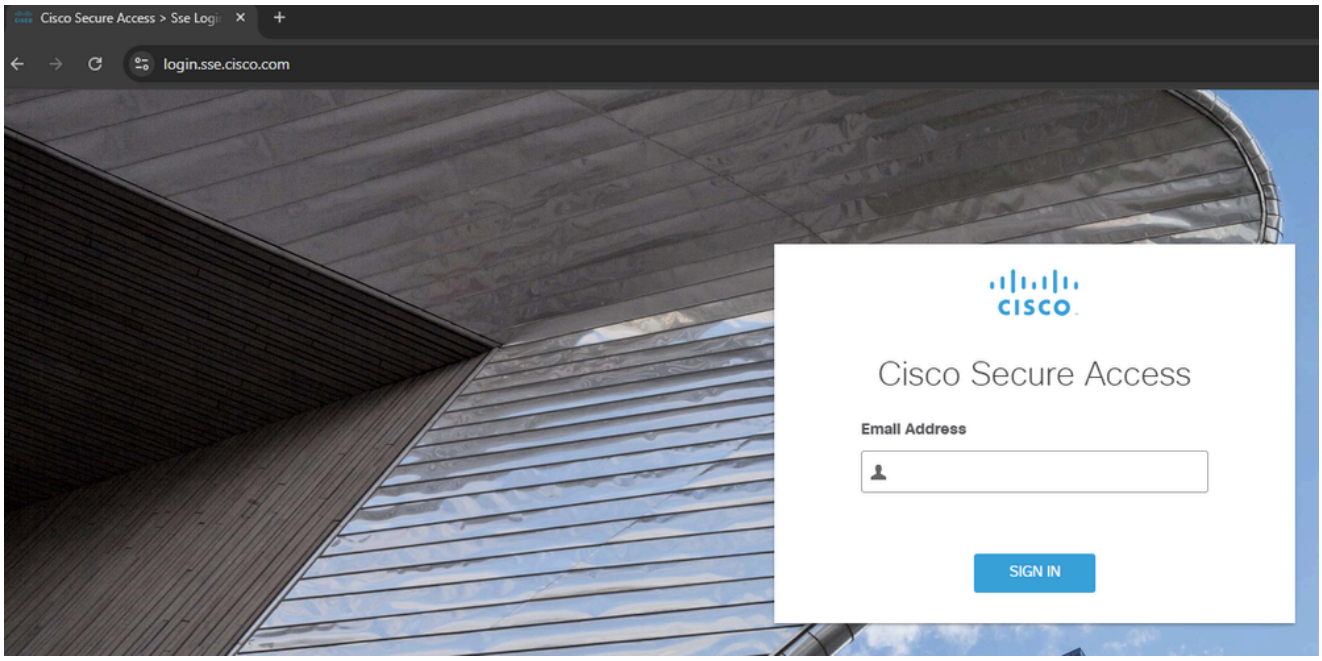
Nota: Este documento se centra específicamente en el aprovisionamiento de usuarios y grupos de OKTA. La configuración de la ID de entrada u otros proveedores de identidad (IdP) para la inscripción ZTA, la autenticación VPNaaS o los ajustes específicos de Umbrella Roaming está fuera del alcance de esta guía.

Configurar

Configuración de Cisco Secure Access

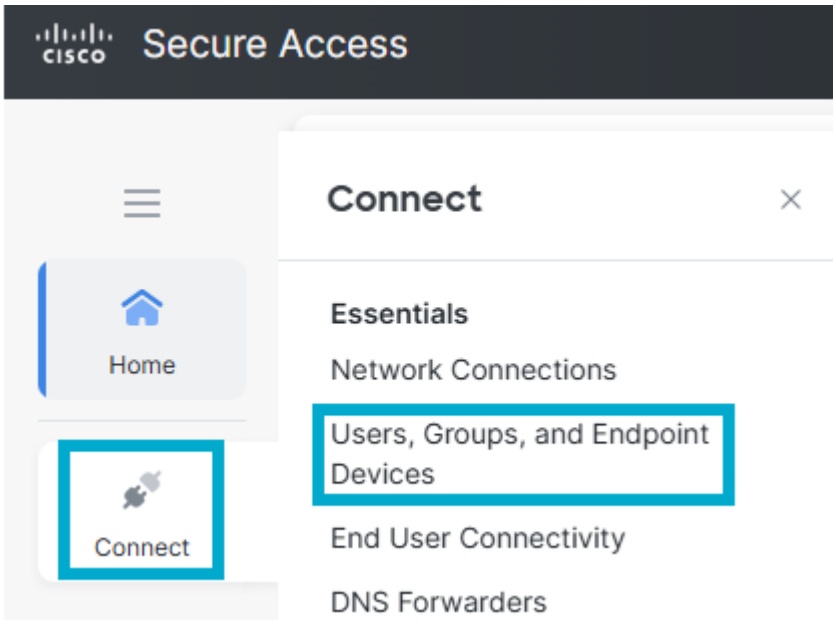
Para comenzar el proceso de aprovisionamiento, primero debe configurar la integración de directorios en el panel de Cisco Secure Access. Este paso genera las credenciales y los parámetros de configuración necesarios para establecer una conexión segura con OKTA.

1. Inicie sesión en el panel de Cisco Secure Access.



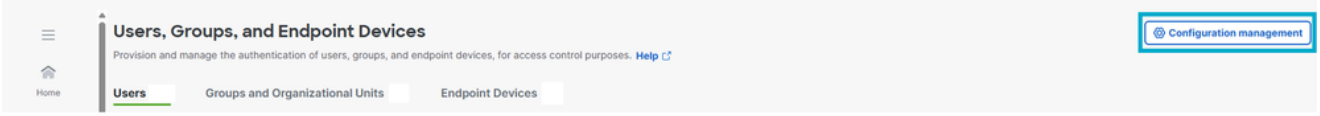
Iniciar sesión en CSA

2. Vaya a Connect > Users, Groups and Endpoint Devices.



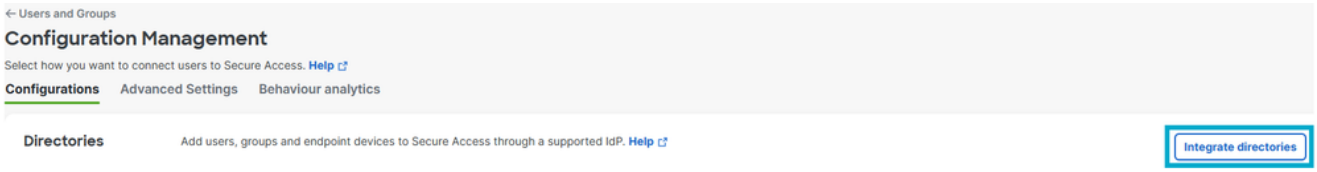
Usuarios y grupos

3. Haga clic en Configuration management.



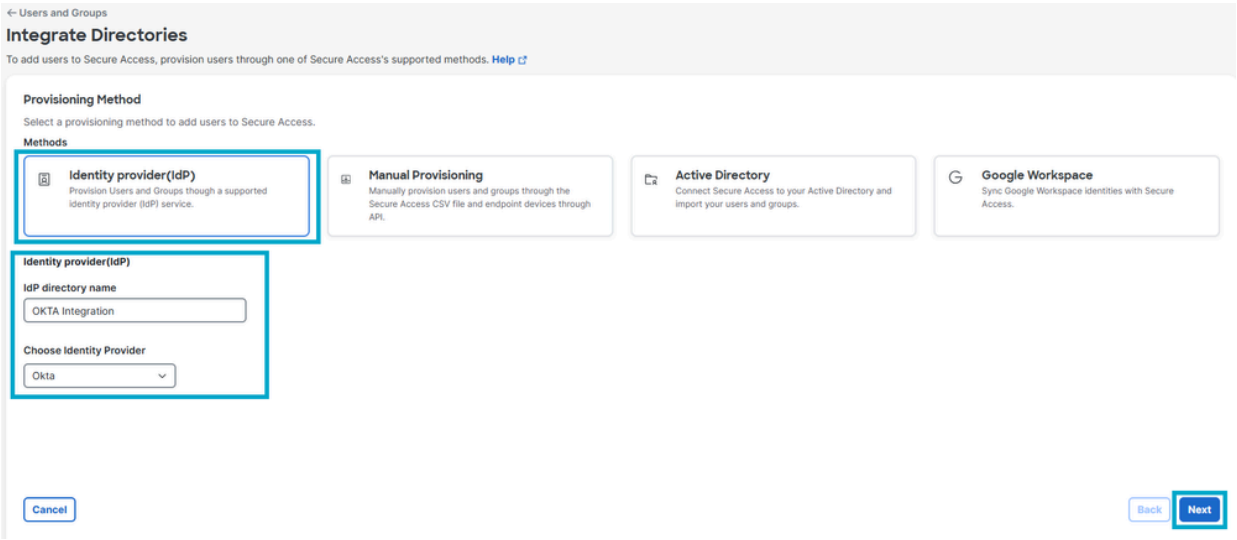
Administración de la Configuración

4. Haga clic en Integrar directorio.



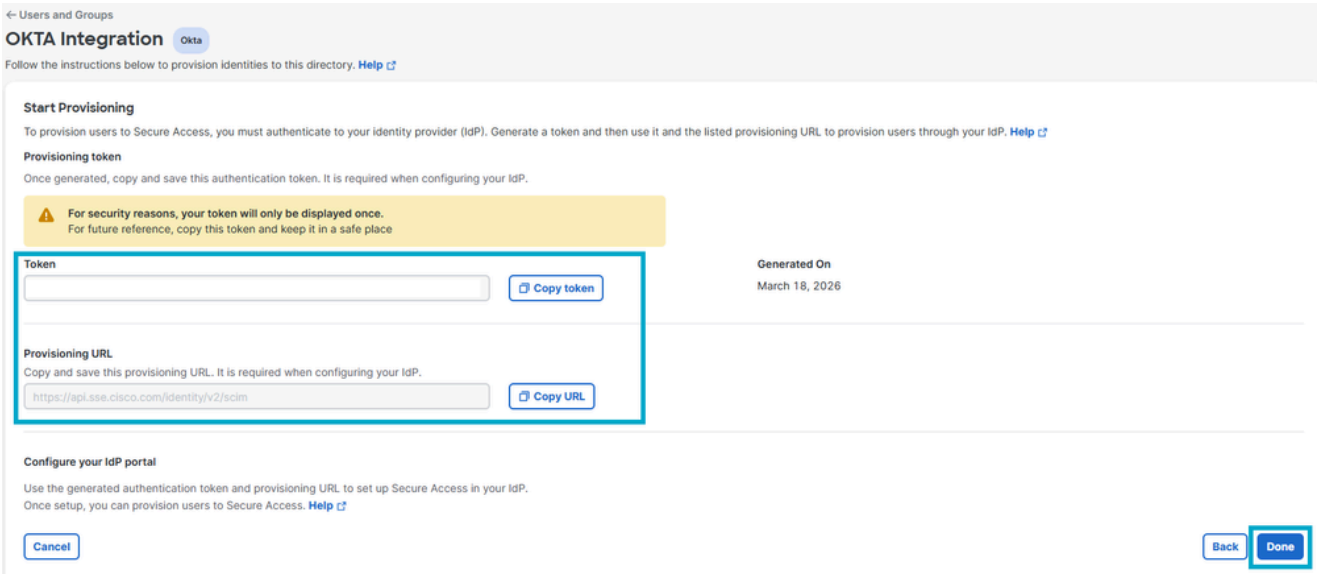
Directorio integrado

5. En Método de aprovisionamiento, haga clic en Proveedor de identidad.
    - Nombre del directorio IdP: Integración de OKTA.
    - Elija el proveedor de identidad: ESTÁ BIEN.
    - Haga clic en Next (Siguiente).



Directory Configuration

6. Haga clic en Generar token. Guarde el token generado y la URL de aprovisionamiento, luego haga clic en Finalizado.

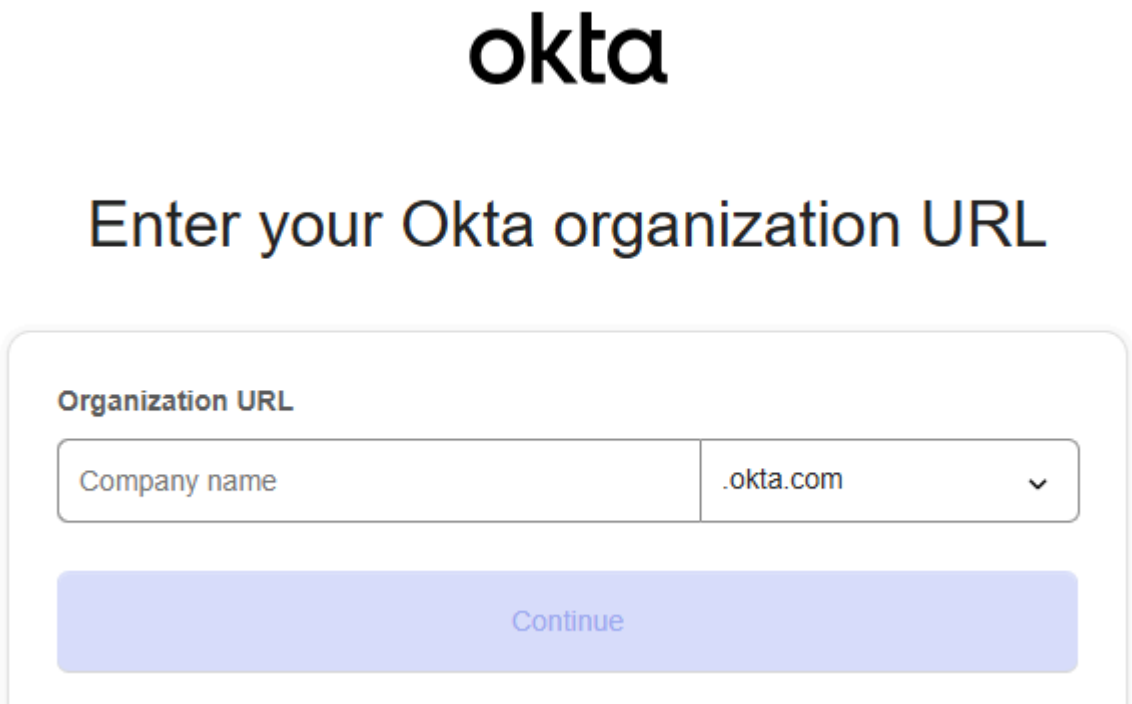


Generar token

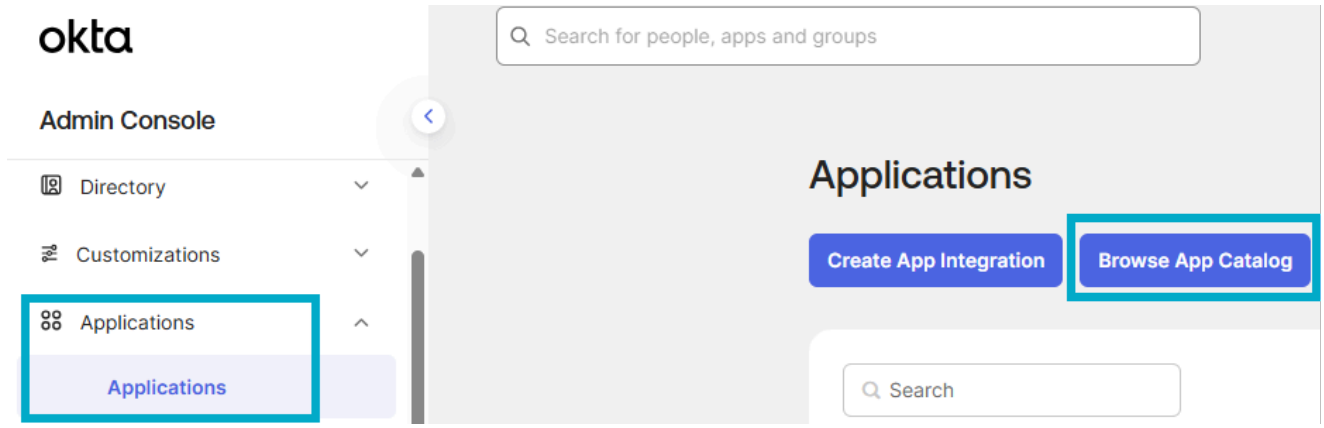
Configurar el aprovisionamiento en OKTA

Una vez que haya generado sus credenciales en el panel de Cisco Secure Access, debe configurar los ajustes de aprovisionamiento dentro de su arrendatario de OKTA para habilitar la sincronización de usuarios y grupos.

1. Inicie sesión en OKTA.

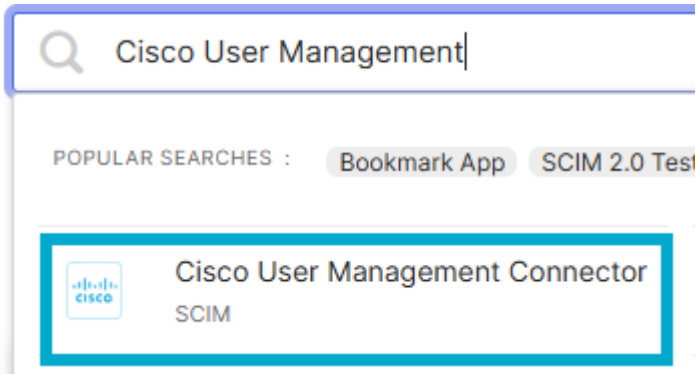


2. Vaya a Aplicaciones > Catálogo de aplicaciones del navegador.



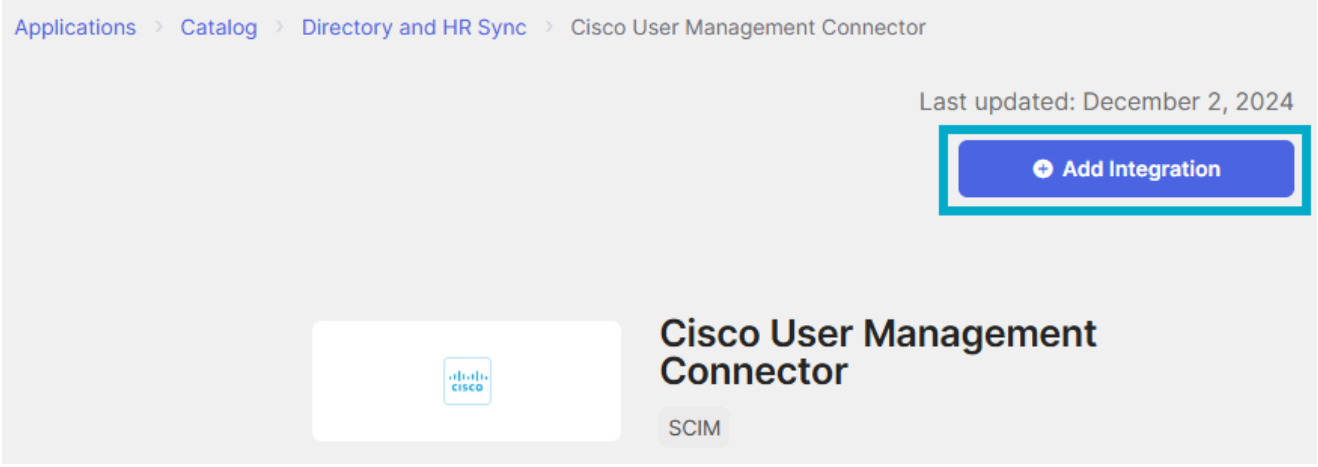
Examinar catálogo de aplicaciones

3. Seleccione la aplicación Cisco User Management Connector.



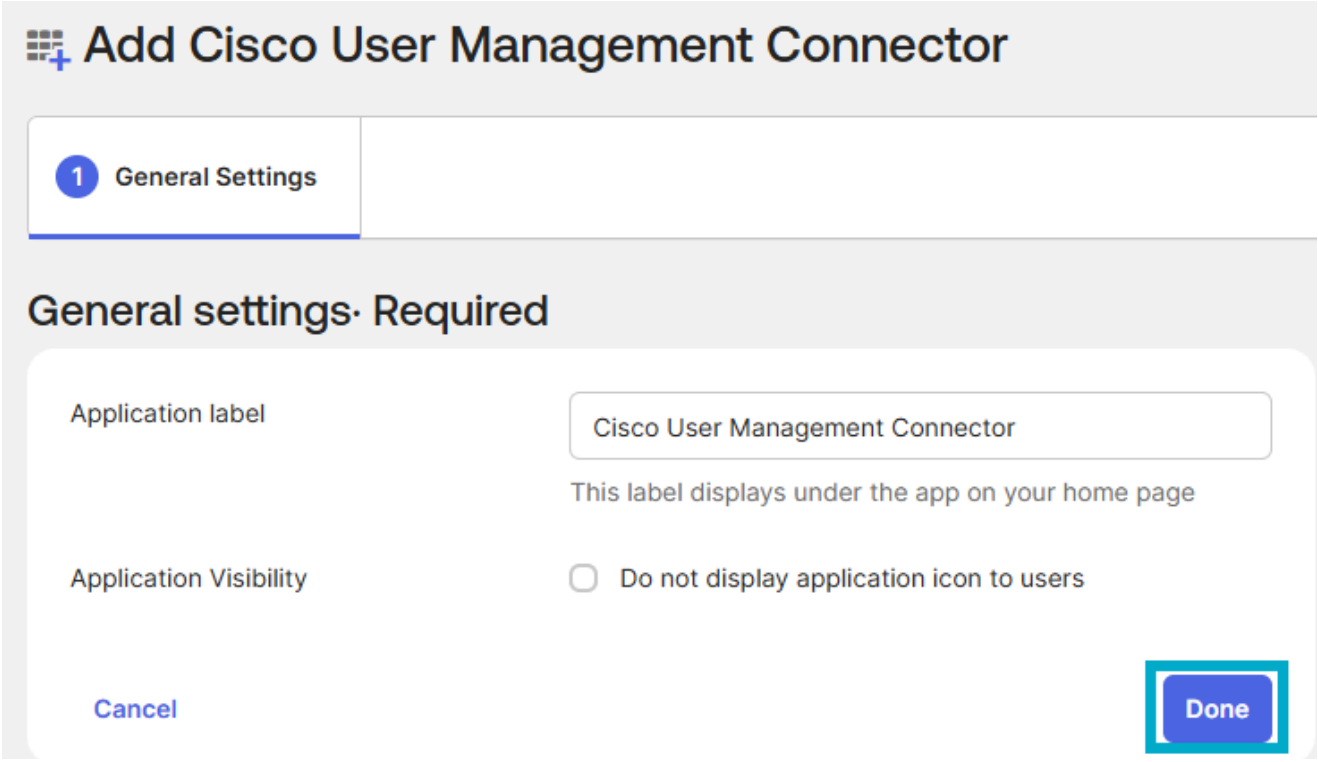
Aplicación de Cisco

4. Haga clic en Agregar integración.



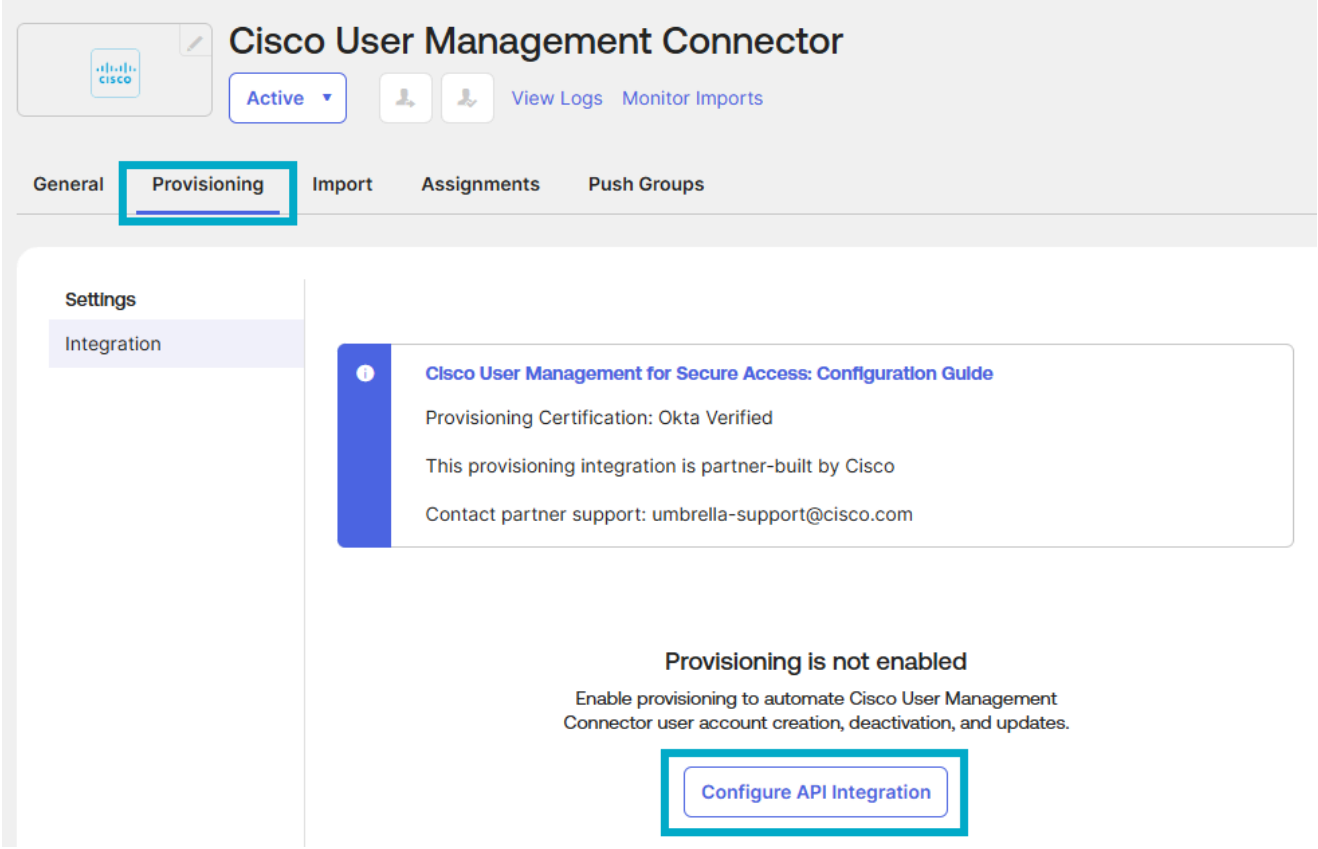
Agregar integración

5. Haga clic en Done (Listo).



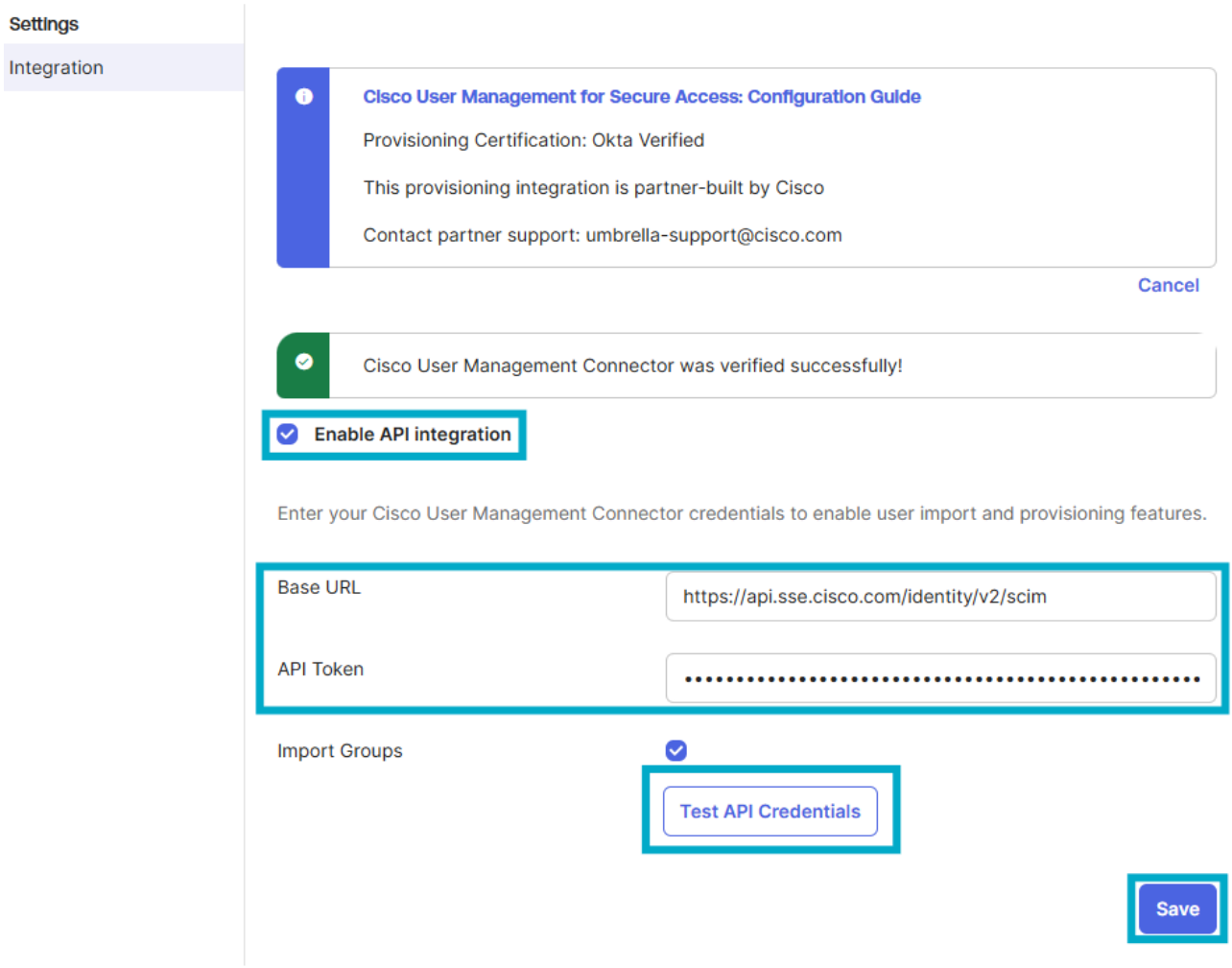
Agregar aplicación

6. Haga clic en Provisioning > Configure API Integration.



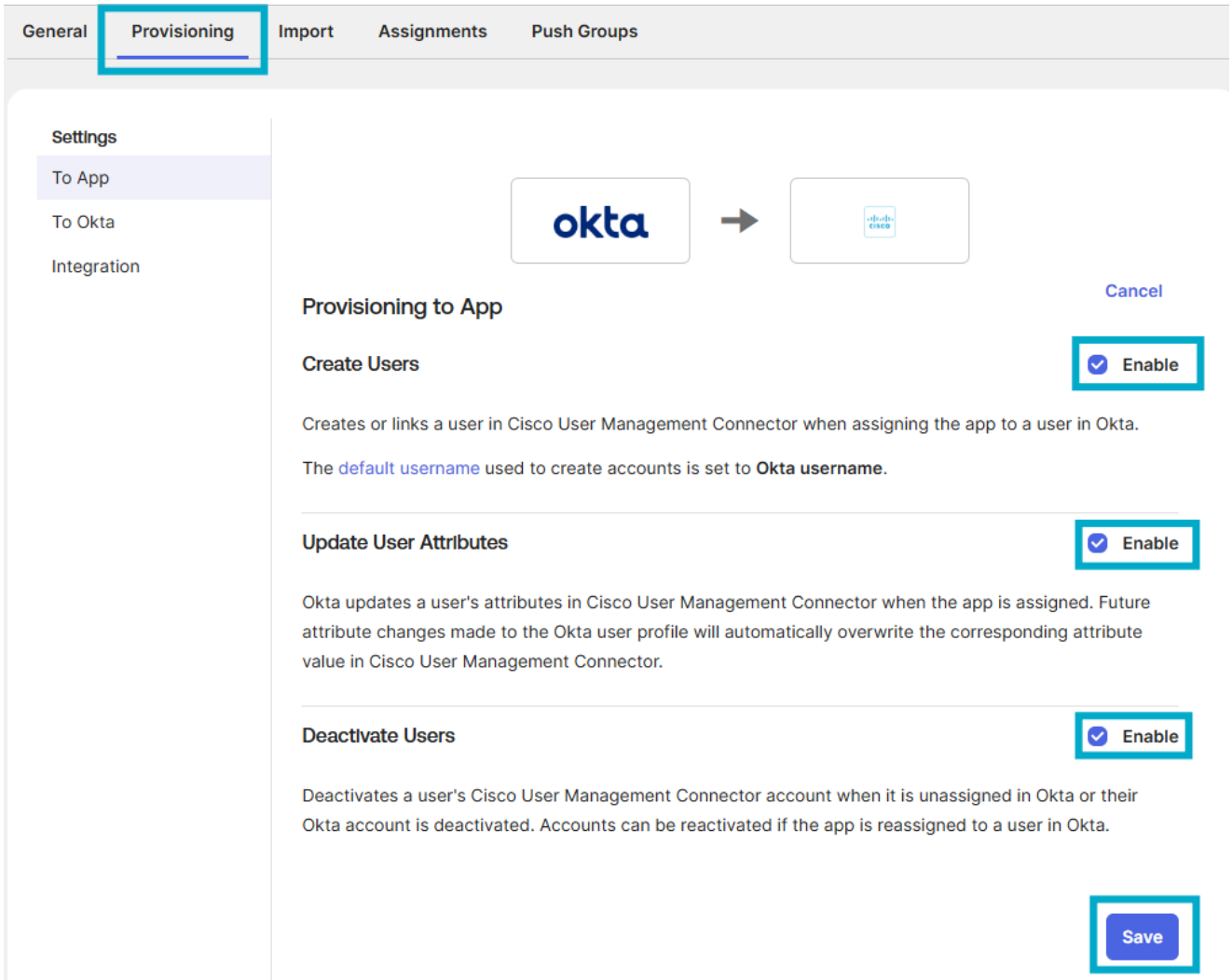
Configurar integración de API

7. Haga clic en Enable API Integration e ingrese los Tokens Based URL y API guardados del paso #6 de la Configuración de Secure Access. Haga clic en Test API Credentials y luego en Save.



Prueba de API

8. Vaya a Provisioning > To App. Active las opciones Create Users, Update User Attributes y Deactivate Users, y haga clic en Save.



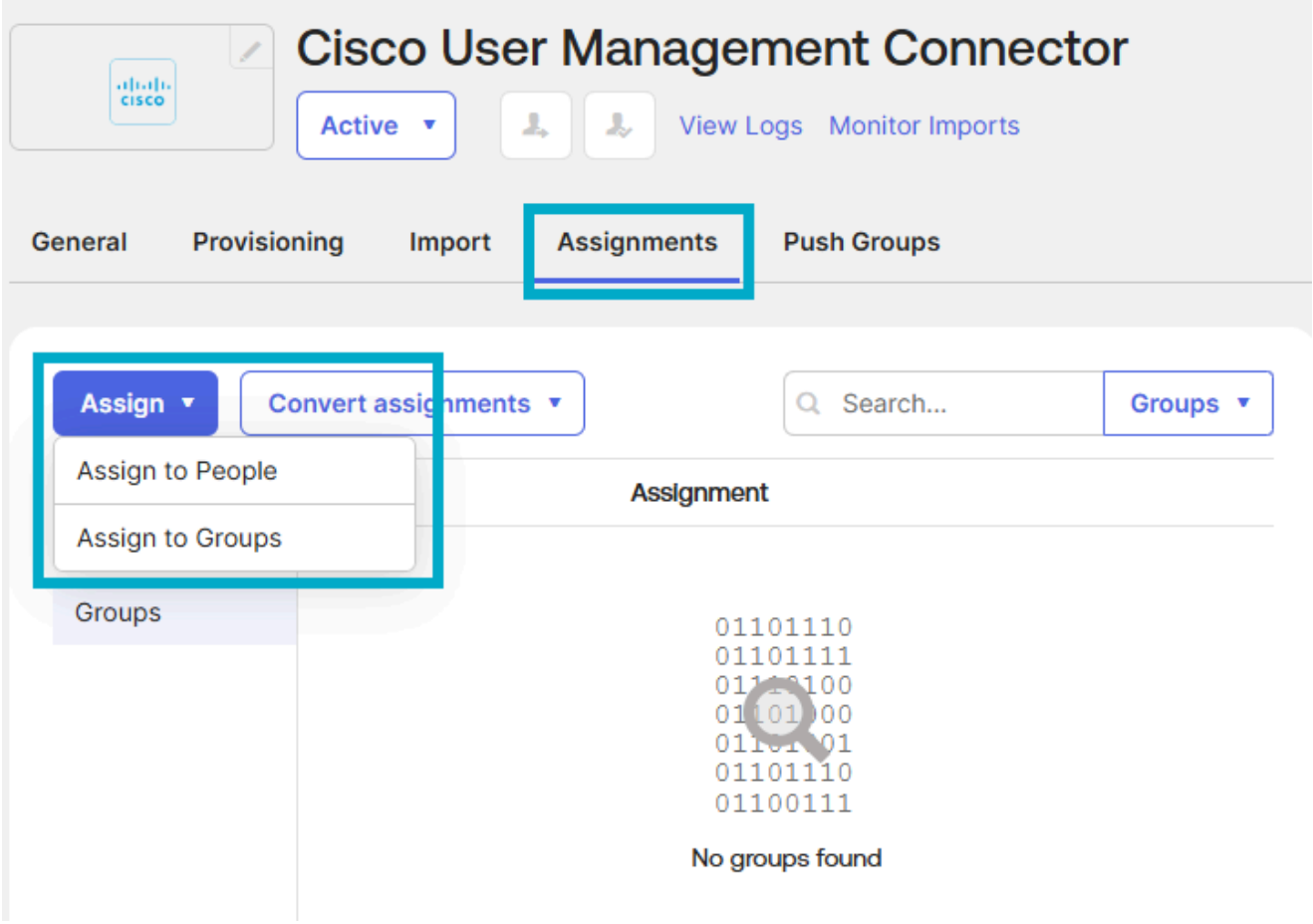
Aprovisionar a la aplicación

Nota: Compruebe que selecciona estos atributos para la sincronización con Secure Access. Secure Access sólo muestra los atributos Nombre mostrado y Nombre usuario para los usuarios, no los atributos Nombre dado y Nombre familiar: Nombre de usuario, Nombre, Familia, Nombre, Nombre para mostrar, Correo electrónico

(Opcional) Agregue un atributo objectGUID y cree la asignación de perfiles de usuario. Si necesita importar el atributo objectGUID para los usuarios, agregue un nuevo atributo y asigne los atributos en la asignación de perfiles.

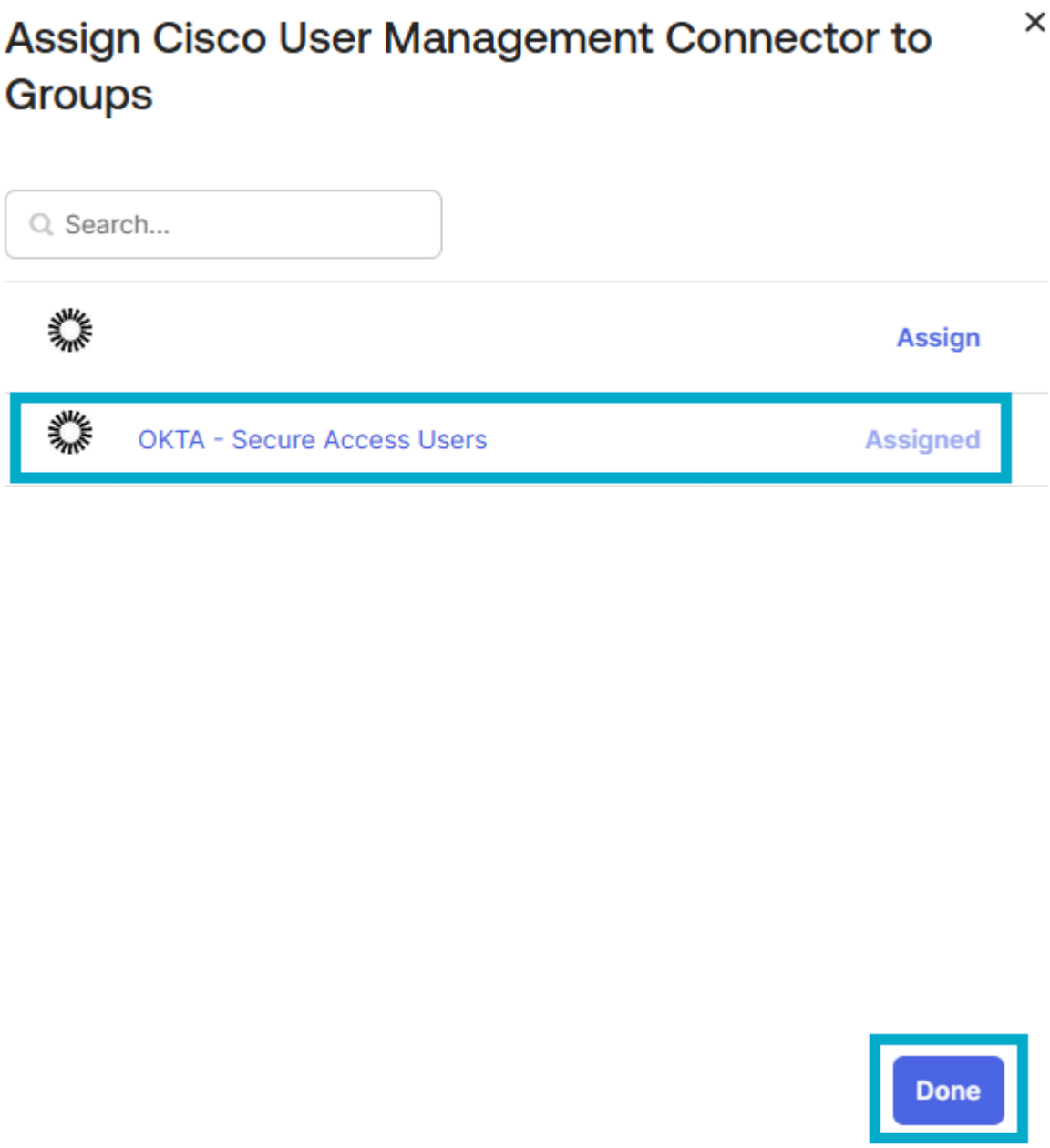
---

9. Para agregar personas/grupos, haga clic en Asignaciones > Asignar > Asignar a personas/Asignar a grupos.



Asignación

10. Seleccione los grupos o personas que desea aprovisionar para Secure Access, haga clic en Asignar y, a continuación, en Finalizado.

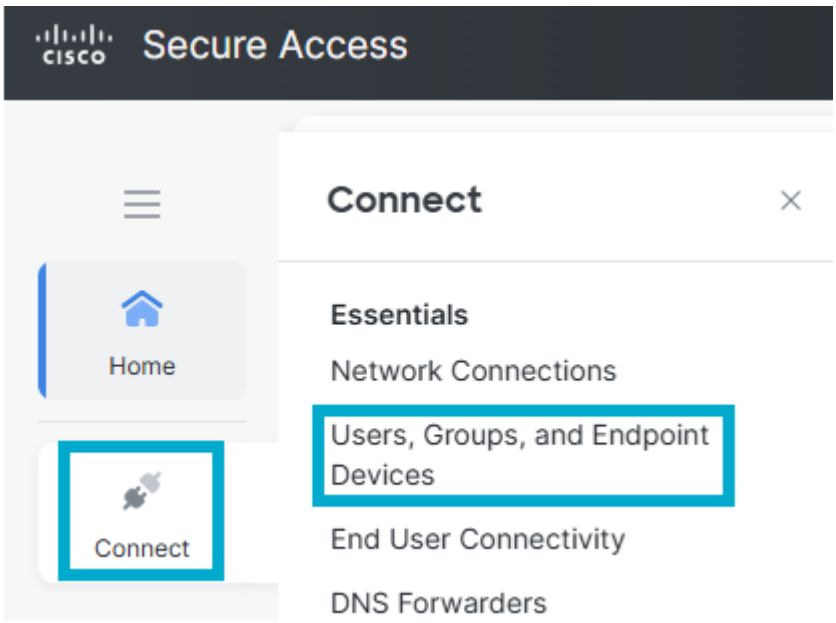


Asignar grupos

Verificación

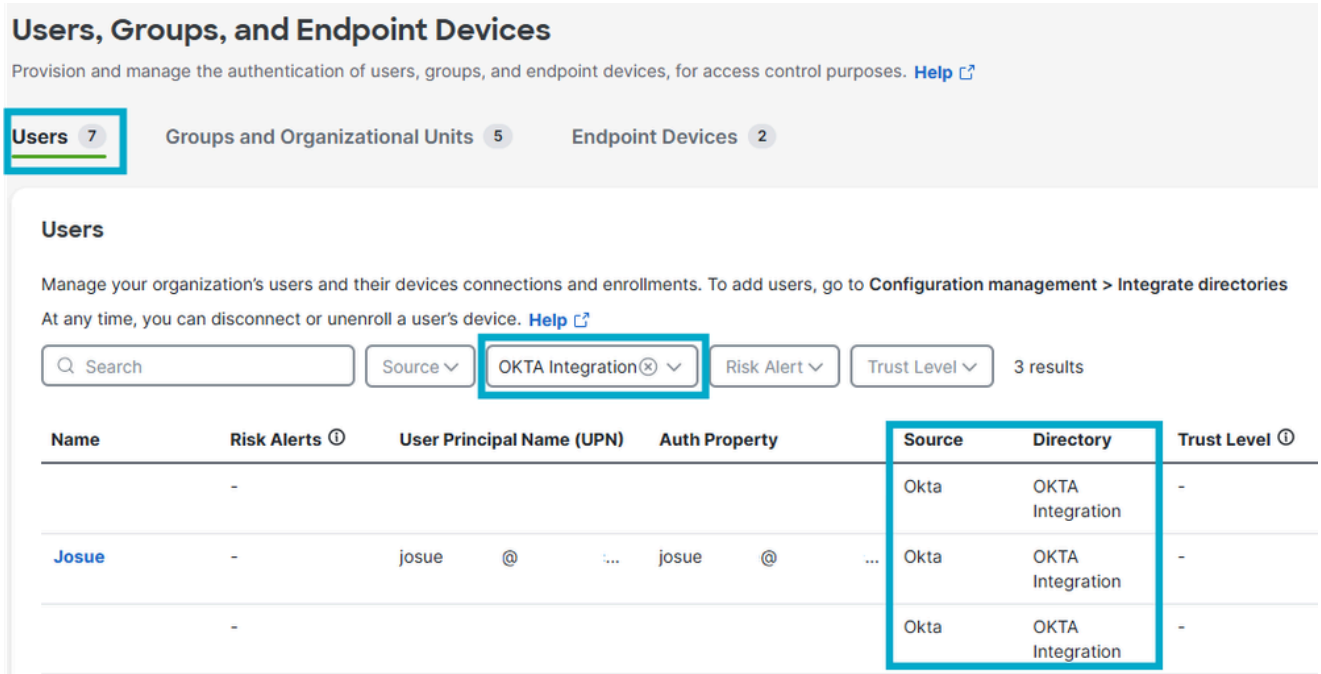
Veracidad en Cisco Secure Access

- Vaya a Connect > Users, Groups and Endpoint Devices.



Usuarios y grupos en CSA

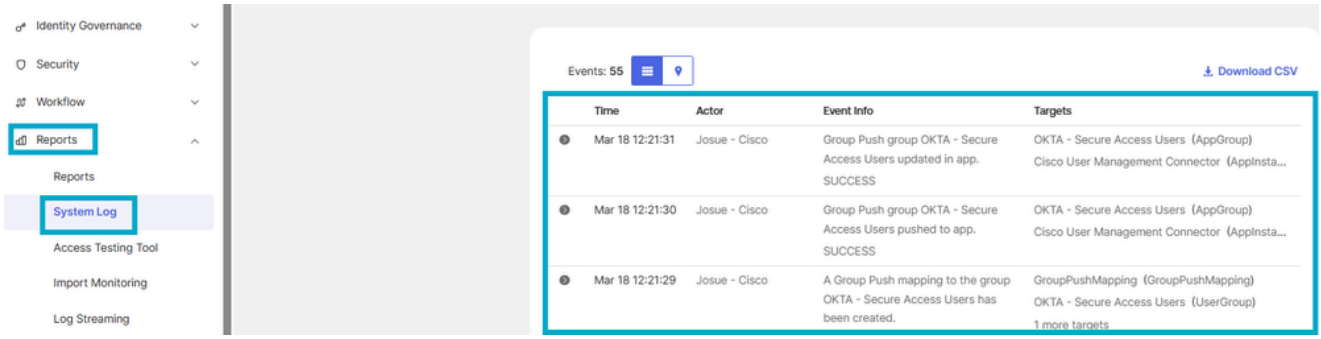
- Haga clic en Usuarios.



Verificar usuarios en CSA

Verity en OKTA

- Vaya a Informes > Registro del sistema.



Registros de OKTA

Información Relacionada

[Configurar proveedores de identidad]

[Aprovisionamiento de usuarios y grupos desde Okta]

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).