Bereitstellung von Benutzern und Gruppen für den sicheren Zugriff über OKTA

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Benutzergruppen von OKTA für Cisco Secure Access bereitgestellt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff von Cisco
- OKTA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

- Cisco Secure Access Dashboard

- OKTA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco Secure Access unterstützt die Bereitstellung von Benutzern und Gruppen von OKTA.

Diese Bereitstellung ermöglicht Secure Access die Verwaltung eines Verzeichnisses von Benutzern, die autorisiert sind,

- Registrieren Sie sich für Zero Trust Access (ZTA).
- Herstellen einer Verbindung mit VPNaaS
- Anwendung identitätsbasierter Richtlinien auf Umbrella Roaming-Benutzer

---

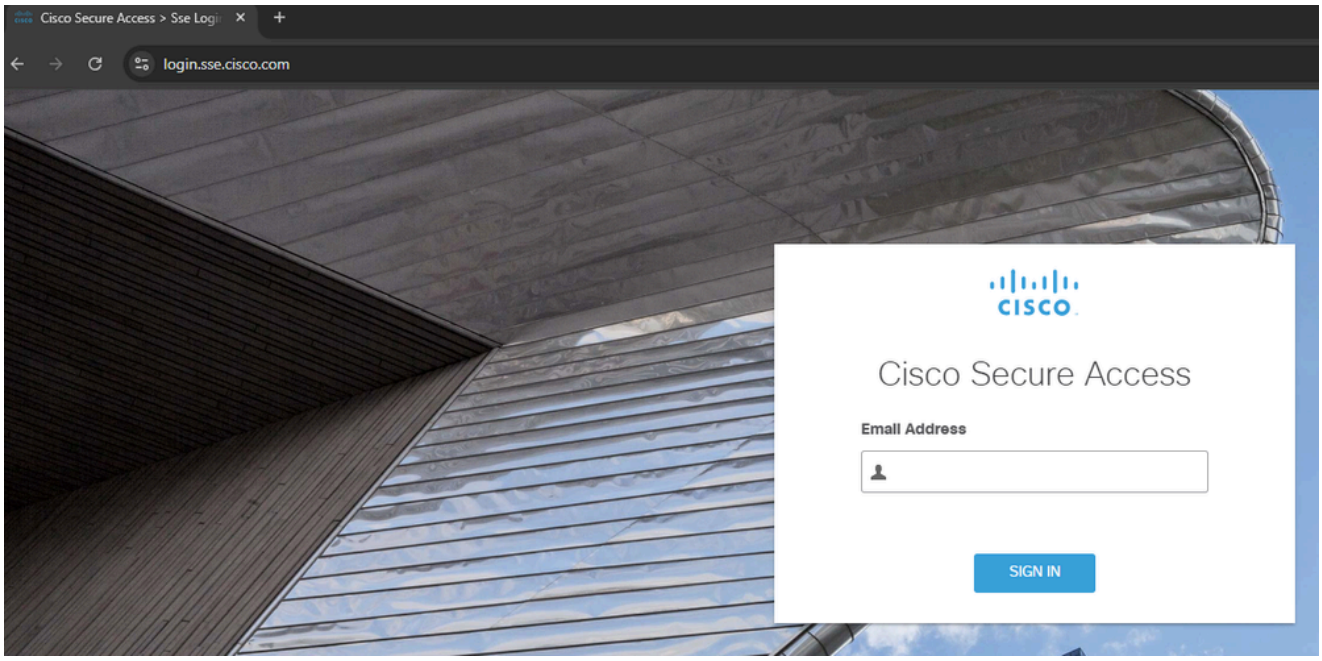
Anmerkung: Dieses Dokument konzentriert sich speziell auf die Bereitstellung von Benutzern und Gruppen von OKTA. Die Konfiguration der Entra-ID oder anderer Identitätsanbieter (IdP) für die ZTA-Registrierung, die VPNaaS-Authentifizierung oder bestimmte Umbrella Roaming-Einstellungen wird in diesem Leitfaden nicht behandelt.

Konfigurieren

Konfigurieren von Cisco Secure Access

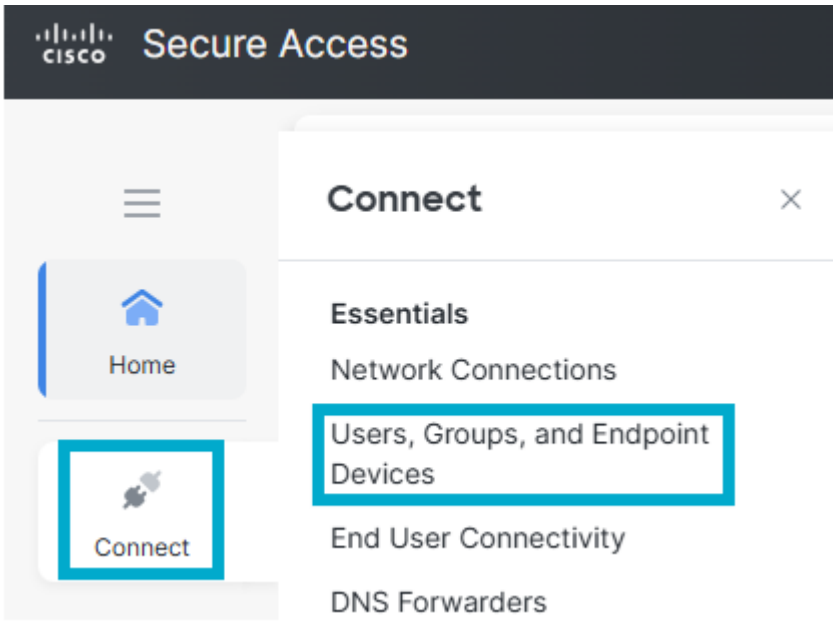
Um mit der Bereitstellung zu beginnen, müssen Sie zunächst die Verzeichnisintegration im Cisco Secure Access Dashboard konfigurieren. In diesem Schritt werden die erforderlichen Anmeldeinformationen und Konfigurationsparameter für den Aufbau einer sicheren Verbindung mit OKTA generiert.

1. Melden Sie sich beim Cisco Secure Access Dashboard an.



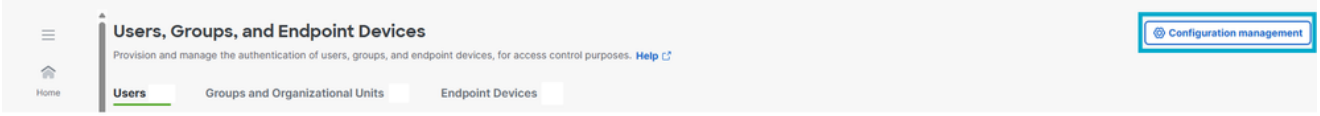
Bei CSA anmelden

2. Navigieren Sie zu Verbinden > Benutzer, Gruppen und Endgeräte.



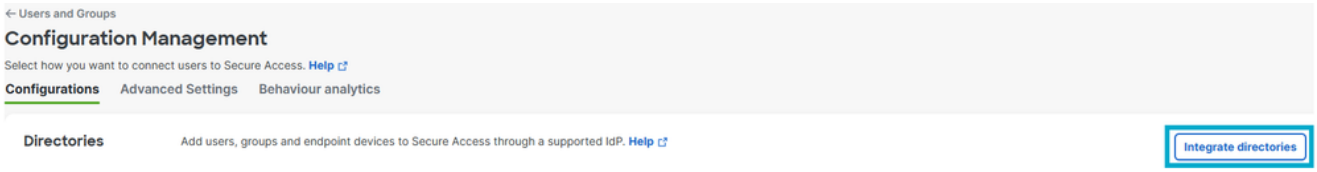
Benutzer und Gruppen

3. Klicken Sie auf Konfigurationsmanagement.



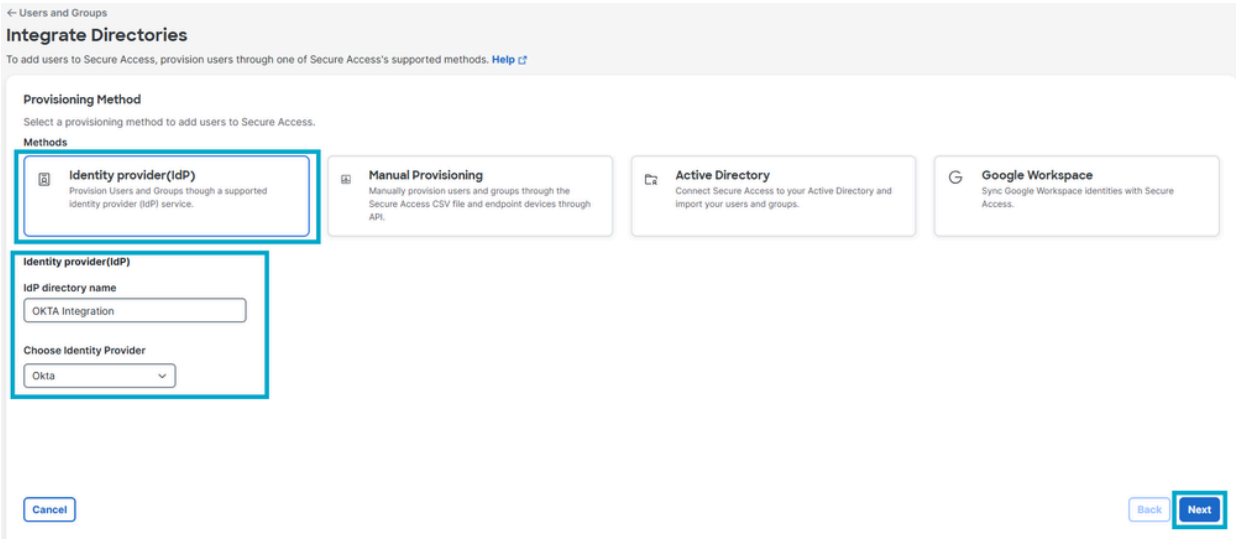
Konfigurationsverwaltung

4. Klicken Sie auf Verzeichnis integrieren.



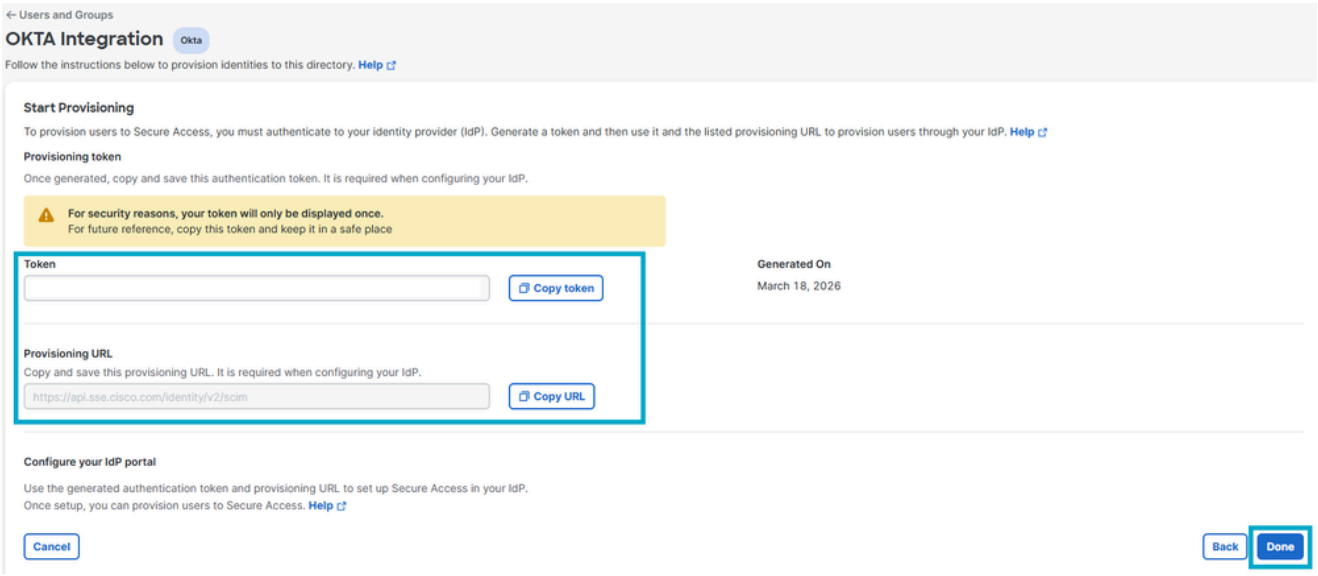
Verzeichnis integrieren

5. Klicken Sie unter Bereitstellungsmethode auf Identitätsanbieter.
    - IdP-Verzeichnisname: OKTA-Integration.
    - Identitätsanbieter auswählen: OKTA.
    - Klicken Sie auf Next (Weiter).



Directory Configuration

6. Klicken Sie auf Token generieren. Speichern Sie das generierte Token und die Bereitstellungs-URL, und klicken Sie dann auf Fertig.

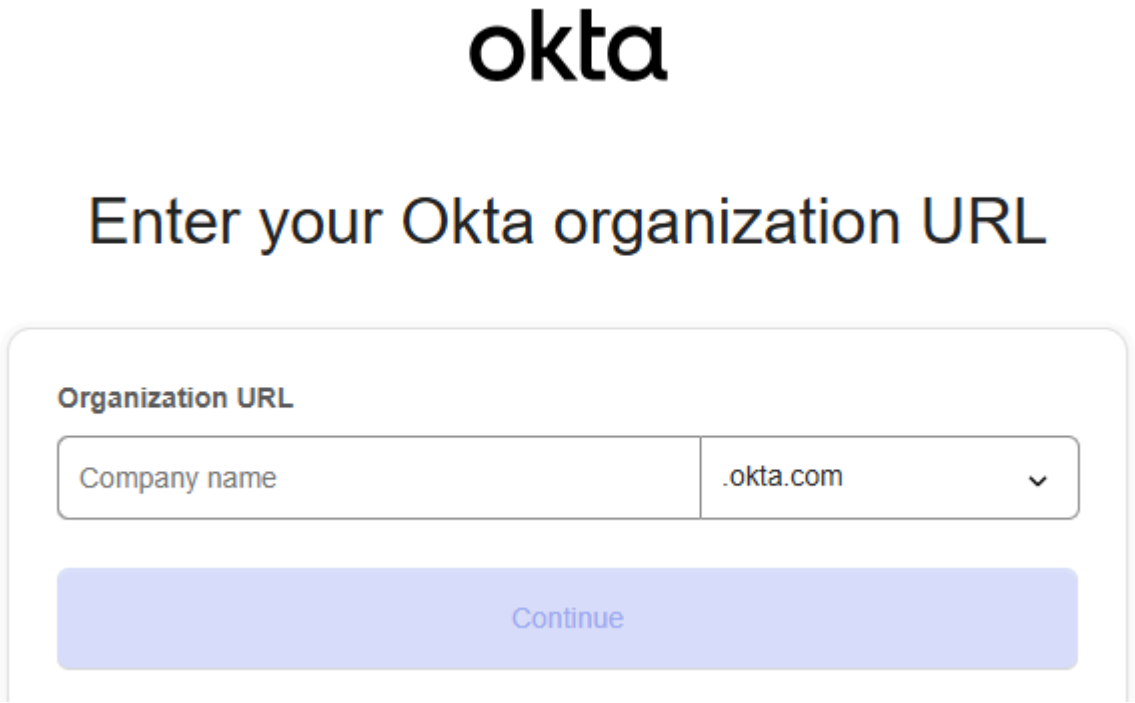


Token generieren

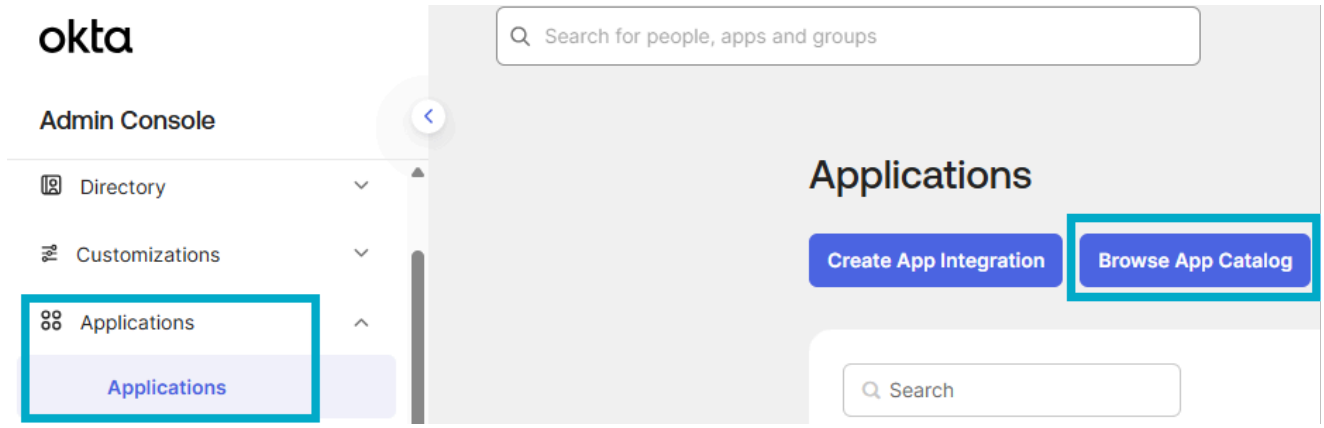
Konfiguration der Bereitstellung in OKTA

Nachdem Sie Ihre Anmeldeinformationen im Cisco Secure Access Dashboard generiert haben, müssen Sie die Bereitstellungseinstellungen in Ihrem OKTA-Tenant konfigurieren, um die Synchronisierung von Benutzern und Gruppen zu ermöglichen.

1. Melden Sie sich bei OKTA an.

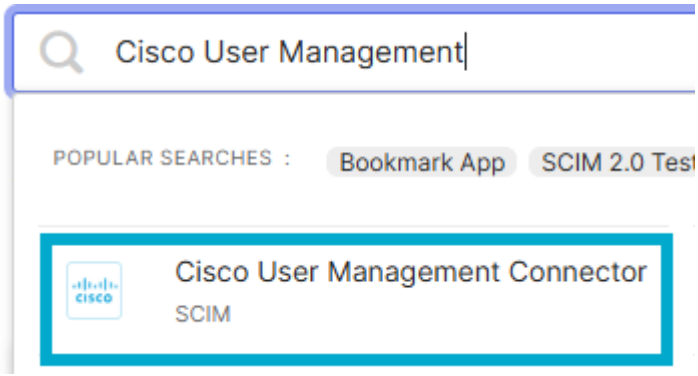


2. Navigieren Sie zu Anwendungen > Browser App Catalog.



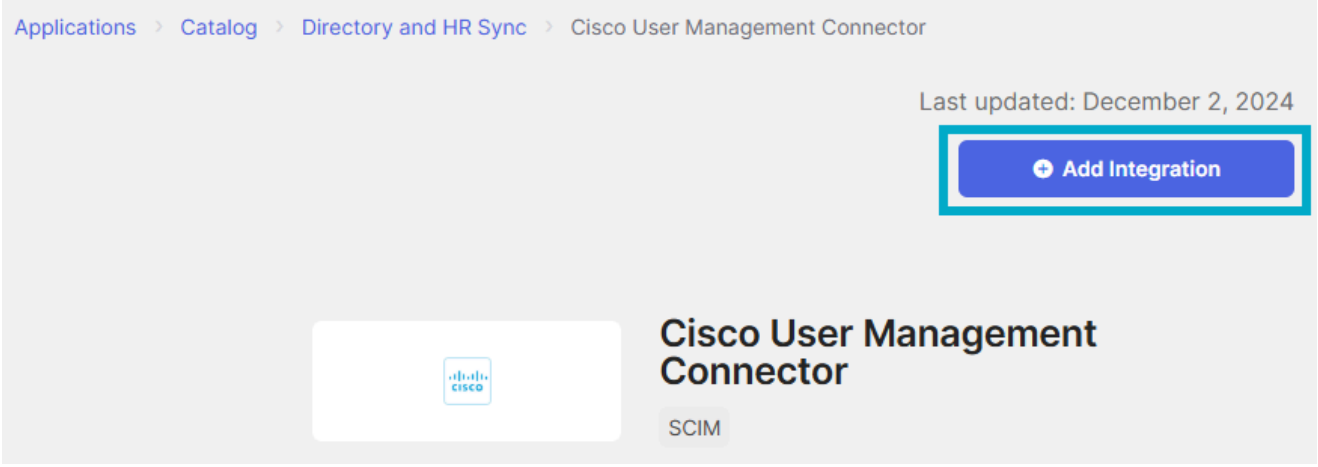
Katalog durchsuchen

3. Wählen Sie die Cisco User Management Connector-App aus.



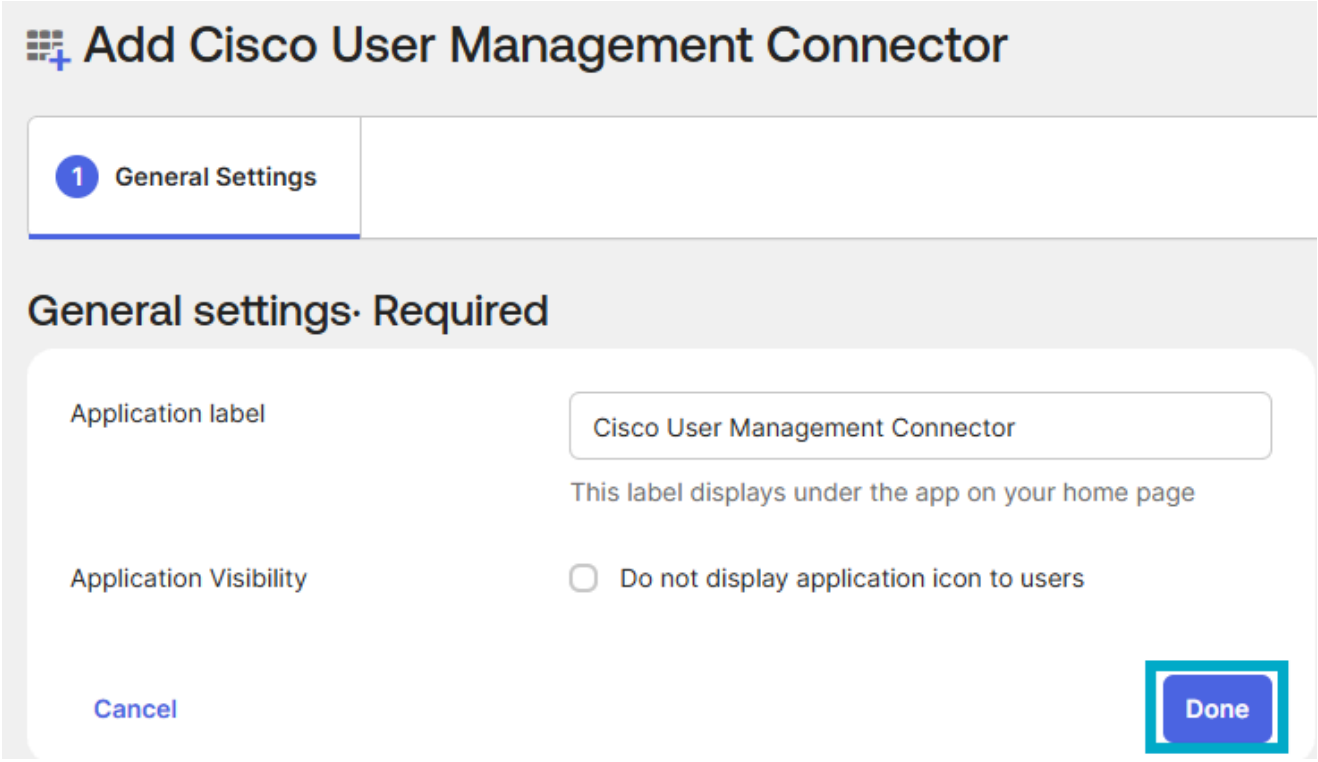
Cisco Anwendung

4. Klicken Sie auf Integration hinzufügen.



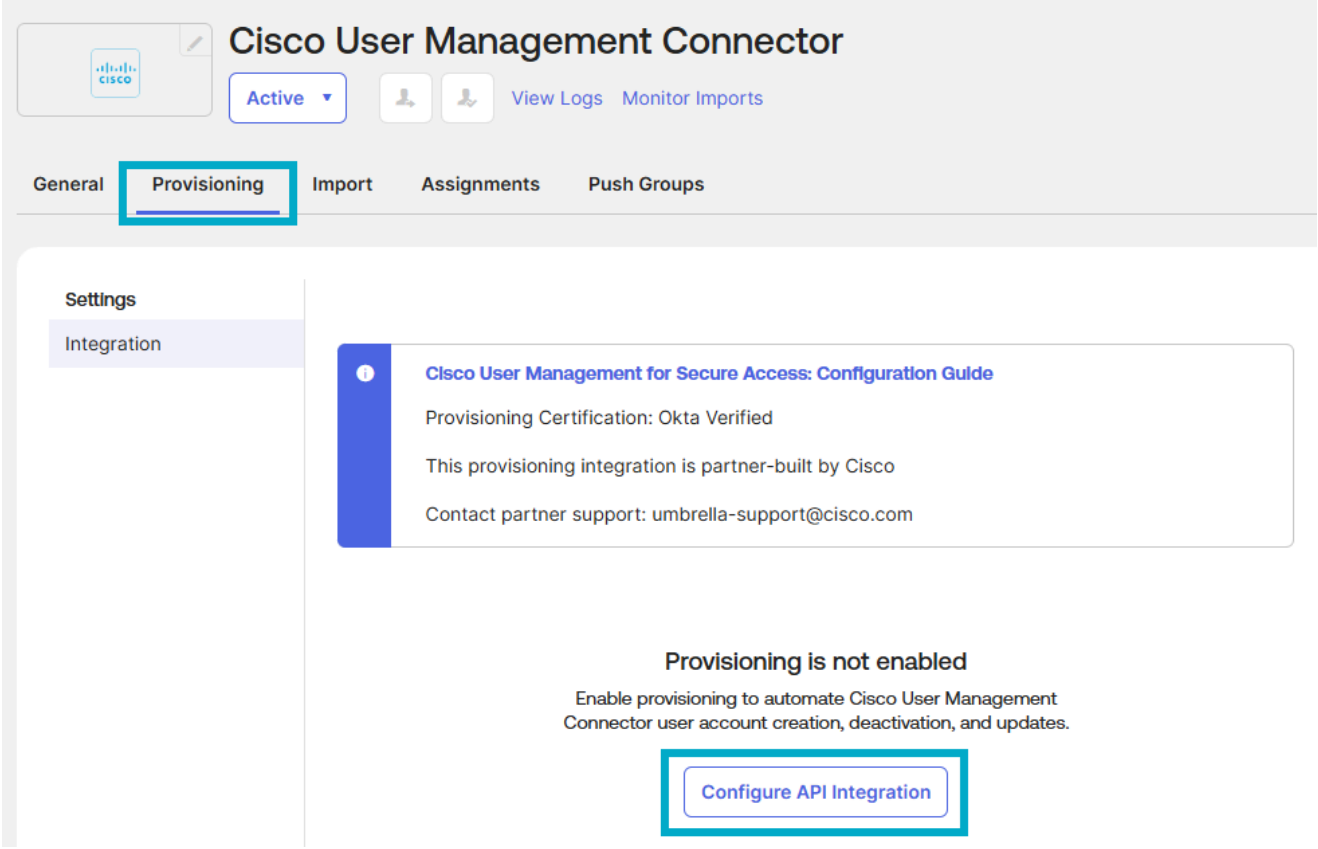
Integration hinzufügen

5. Klicken Sie auf Done (Fertig).



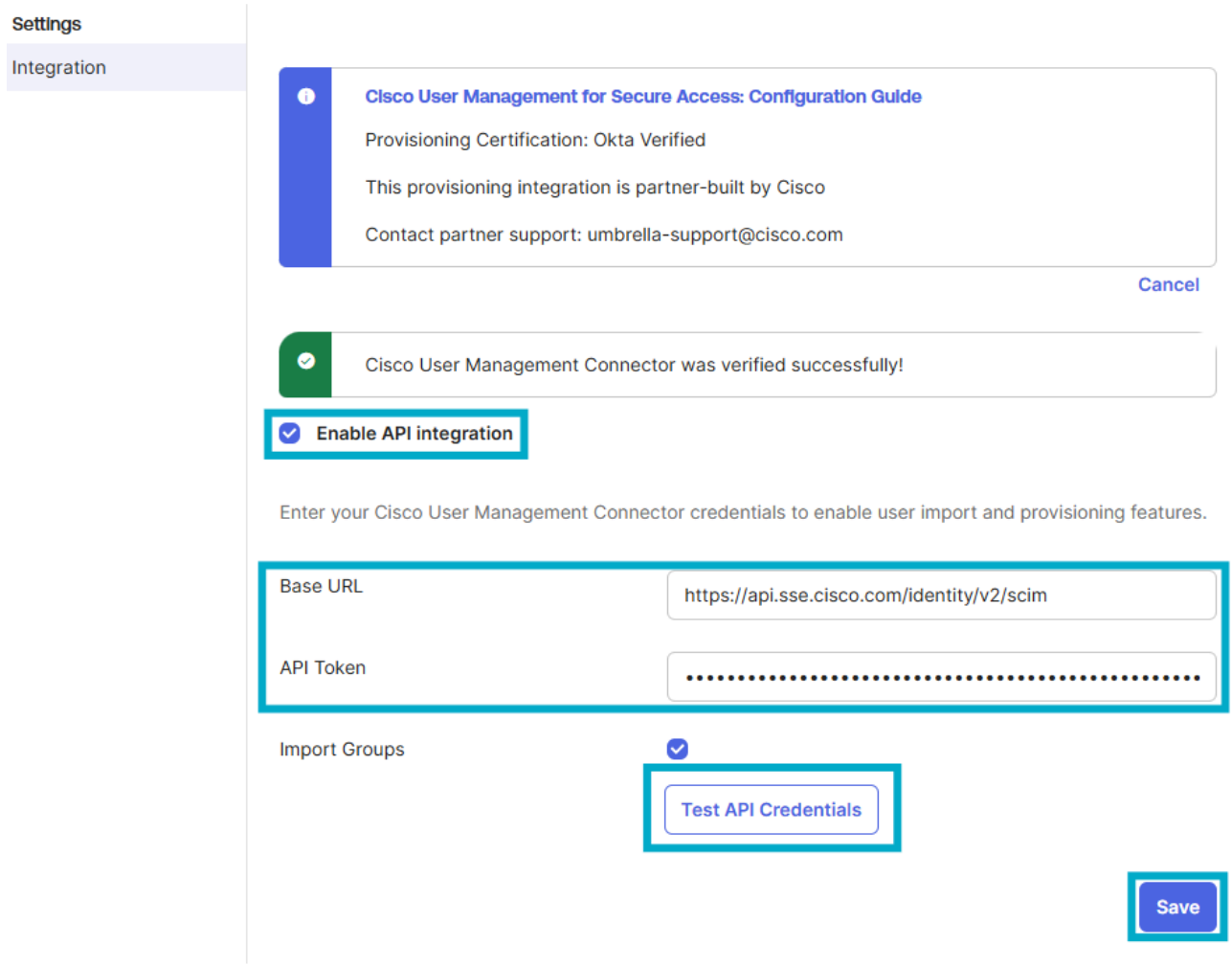
App hinzufügen

6. Klicken Sie auf Provisioning > Configure API Integration.



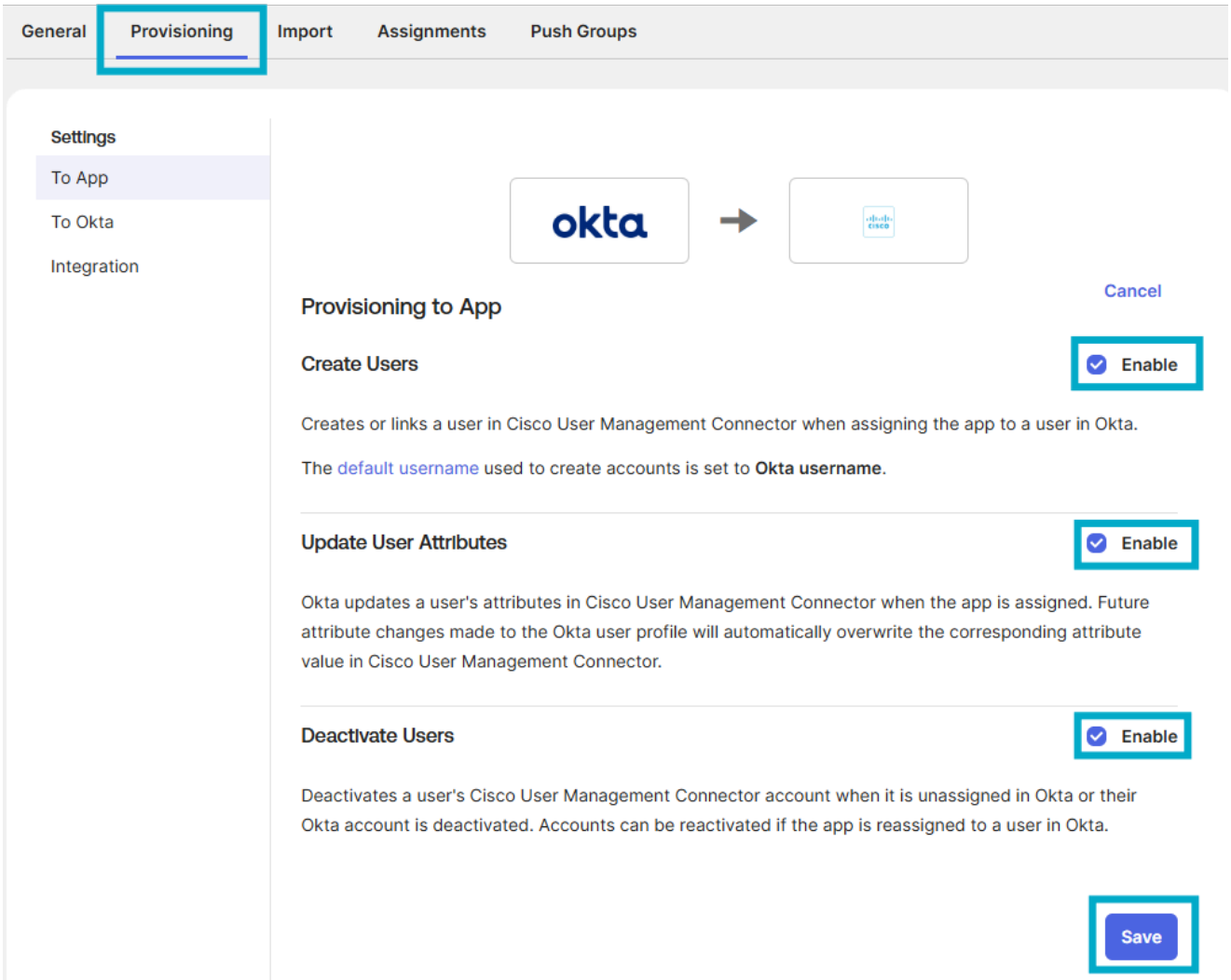
API-Integration konfigurieren

7. Klicken Sie auf API-Integration aktivieren, und geben Sie die Based URL und API Token ein, die in Schritt #6 der Secure Access Configuration gespeichert sind. Klicken Sie auf Test API Credentials (API-Anmeldeinformationen testen) und dann auf Save.



API-Test

8. Navigieren Sie zu Provisioning > To App. Aktivieren Sie die Optionen Benutzer erstellen, Benutzerattribute aktualisieren und Benutzer deaktivieren, und klicken Sie auf Speichern.



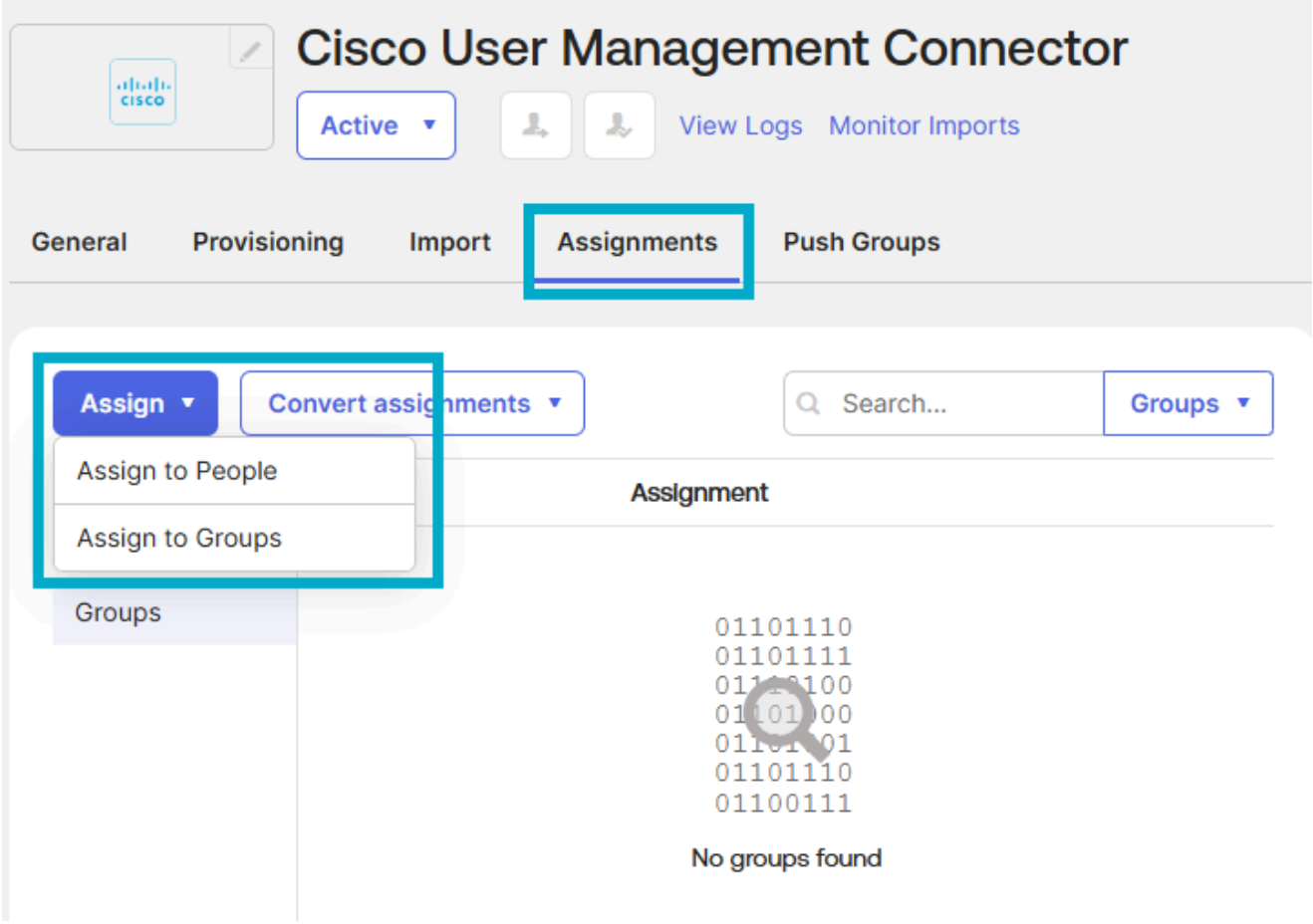
Bereitstellung für Anwendung

Anmerkung: Überprüfen Sie, ob Sie diese Attribute für die Synchronisierung mit Secure Access ausgewählt haben. In Secure Access werden nur die Attribute "Anzeigename" und "Benutzername" für Benutzer aufgeführt, nicht die Attribute "Vorname" und "Nachname": Benutzername, Vorname, Familie, Name, Anzeigename, E-Mail

(Optional) Fügen Sie ein objectGUID-Attribut hinzu, und erstellen Sie die Benutzerprofilzuordnung. Wenn Sie das objectGUID-Attribut für Benutzer importieren müssen, fügen Sie ein neues Attribut hinzu, und ordnen Sie die Attribute in der Profilzuordnung zu.

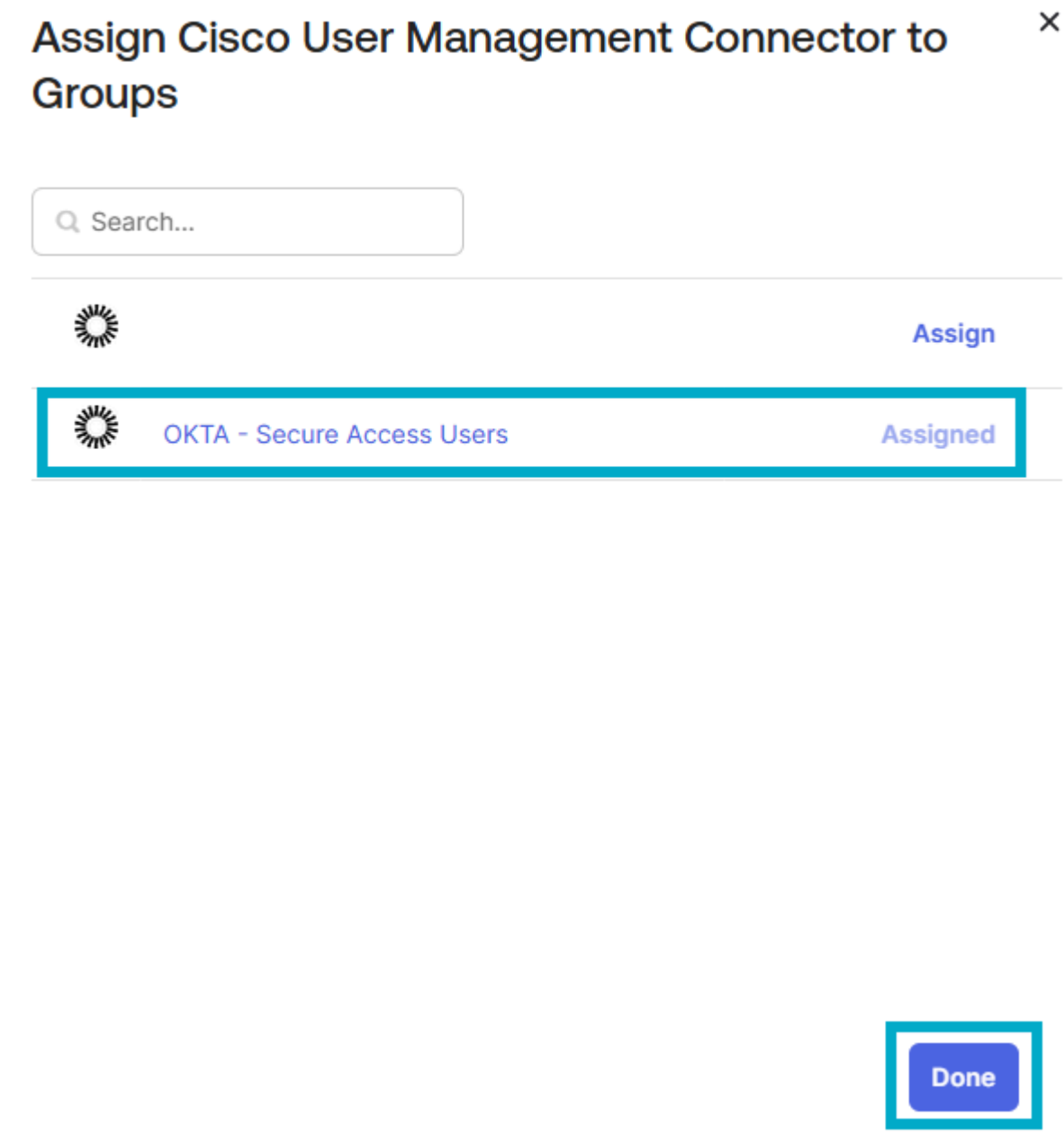
---

9. Um Personen/Gruppen hinzuzufügen, klicken Sie auf Assignments > Assign > Assign to People/Assign to Groups.



Zuweisung

10. Wählen Sie die Gruppen/Personen aus, die Sie für den sicheren Zugriff bereitstellen möchten, und klicken Sie auf Zuweisen und dann auf Fertig.

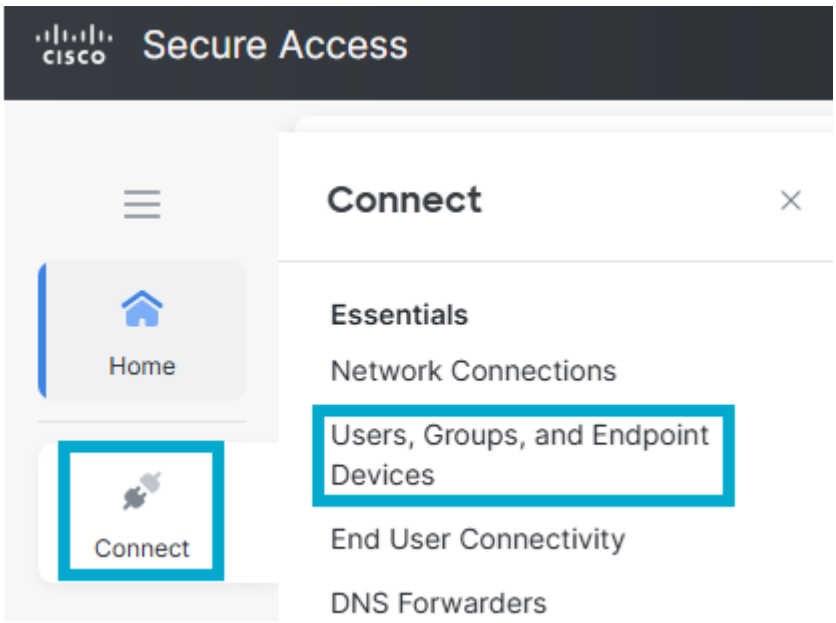


Gruppen zuweisen

Überprüfung

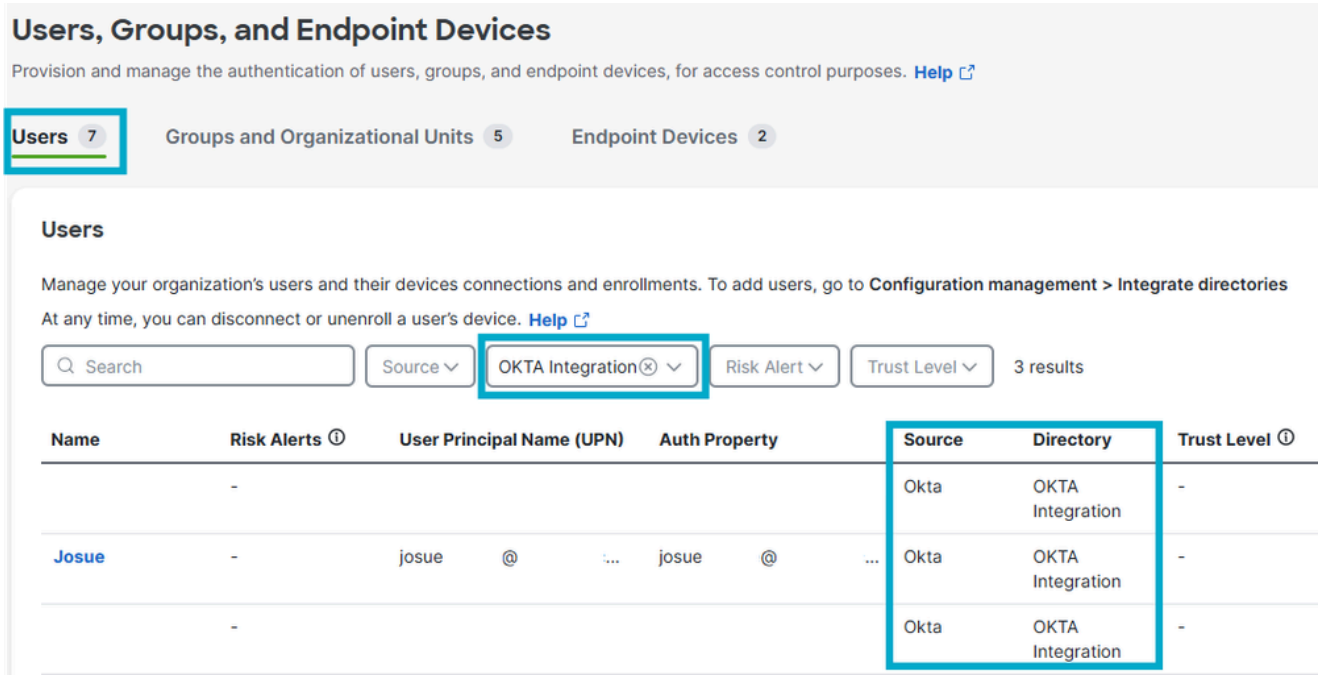
Verity in Cisco Secure Access

- Navigieren Sie zu Verbinden > Benutzer, Gruppen und Endgeräte.



Benutzer und Gruppen in CSA

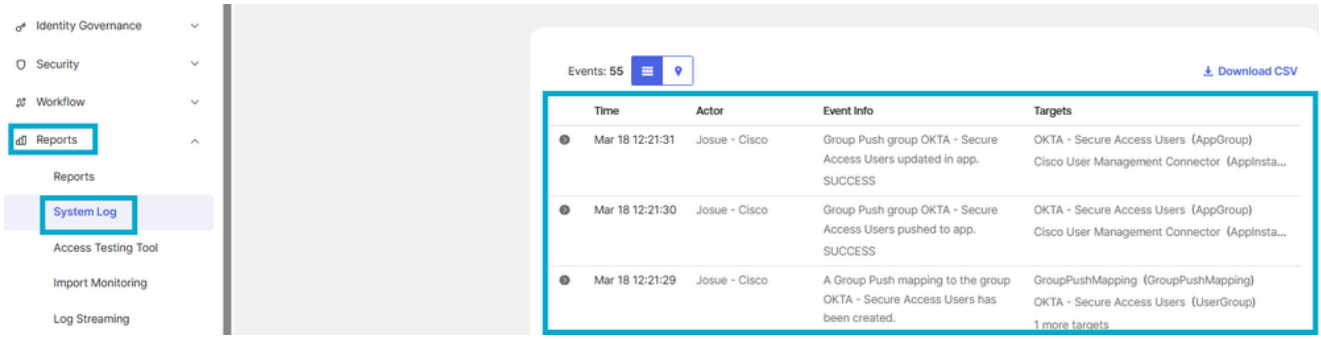
- Klicken Sie auf Benutzer.



Benutzer in CSA überprüfen

Veritas in OKTA

- Navigieren Sie zu Berichte > Systemprotokoll.



OKTA-Protokolle

Zugehörige Informationen

Identitätsanbieter konfigurieren

Bereitstellung von Benutzern und Gruppen von Okta aus

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.