# Assegnazione dell'accesso sicuro a utenti e gruppi tramite OKTA

## Sommario



## Introduzione

In questo documento viene descritto come eseguire il provisioning dei gruppi di utenti da OKTA a Cisco Secure Access.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Access
- OKTA

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

- Cisco Secure Access Dashboard

- OKTA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

Cisco Secure Access supporta il provisioning di utenti e gruppi da OKTA.

Questo provisioning consente l'accesso sicuro per la gestione di una directory di utenti autorizzati a:

- Registrarsi in Zero Trust Access (ZTA).
- Connessione a VPNaaS.
- Applicazione di criteri basati sull'identità agli utenti di Umbrella Roaming.

---

Nota: Questo documento si concentra in modo specifico sul provisioning di utenti e gruppi da OKTA. La configurazione dell'ID Entra o di altri provider di identità (IdP) per la registrazione ZTA, l'autenticazione VPNaaS o impostazioni di roaming Umbrella specifiche esula dall'ambito di questa guida.

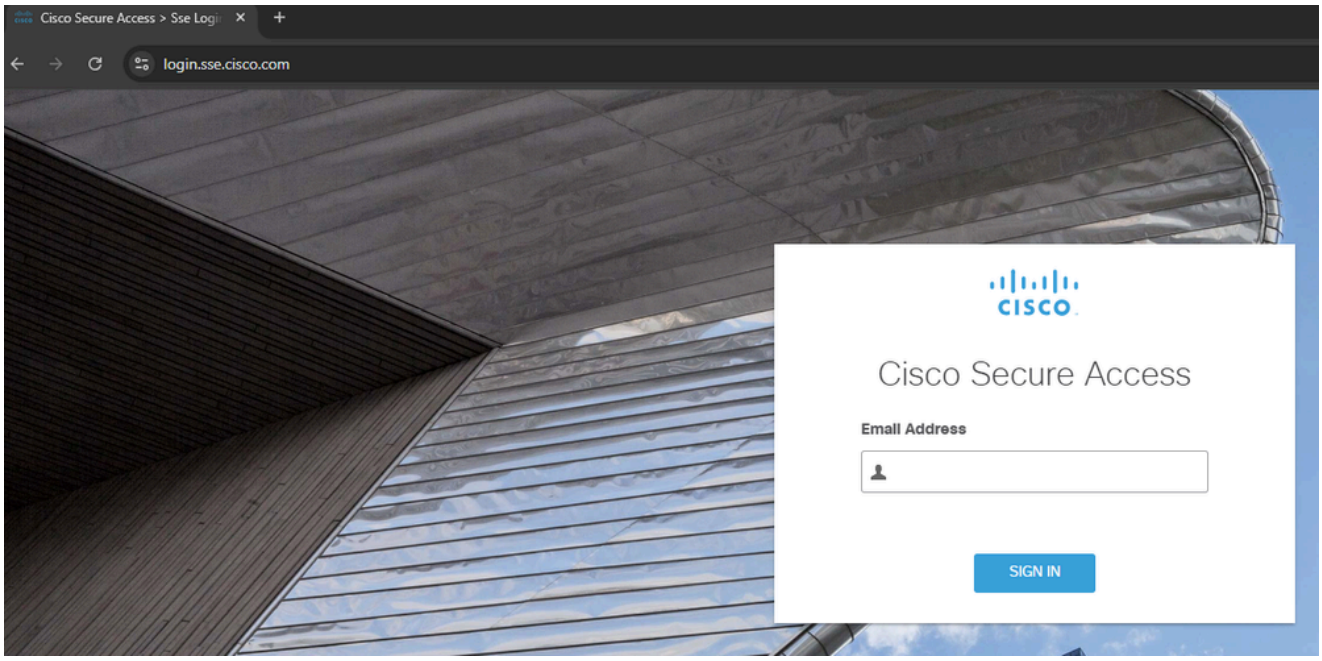
---

# Configurazione

## Configurazione di Cisco Secure Access

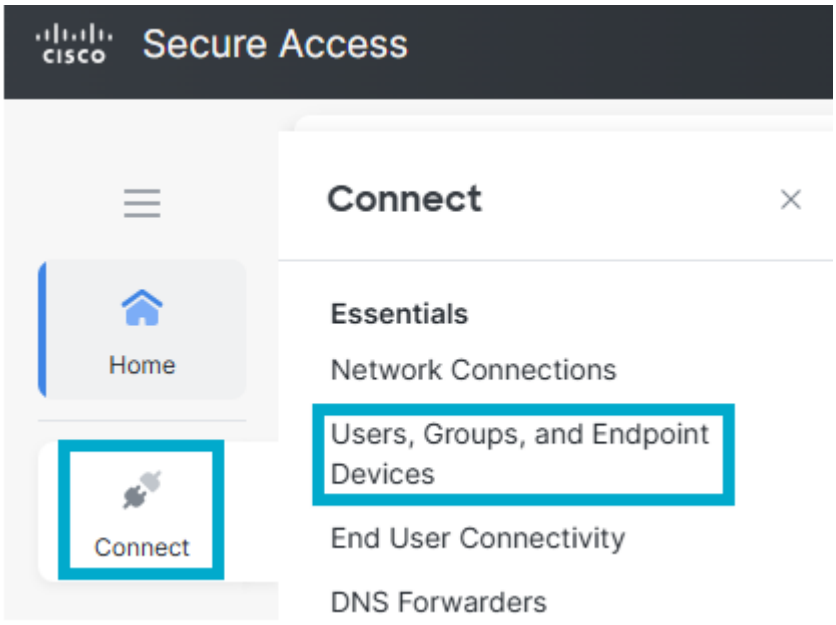
Per avviare il processo di provisioning, è necessario innanzitutto configurare l'integrazione delle directory nel dashboard Cisco Secure Access. Questo passaggio genera le credenziali e i parametri di configurazione necessari per stabilire una connessione protetta con OKTA.

1. Accedere a Cisco Secure Access Dashboard.



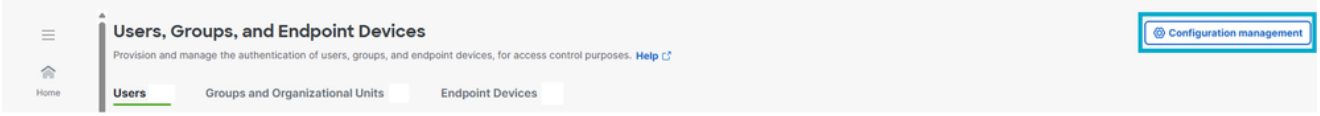

Accedi a CSA

2. Passare a Connetti > Utenti, gruppi e dispositivi endpoint.



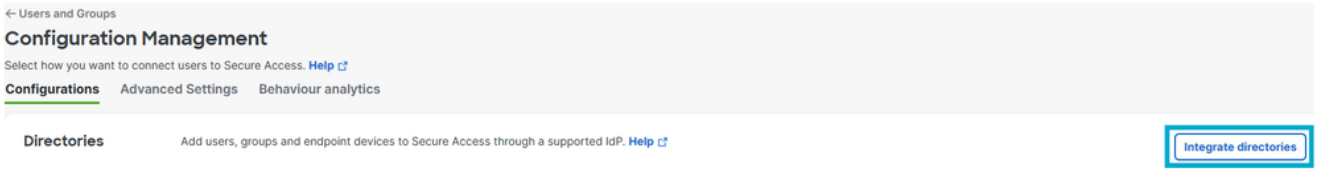

Utenti e gruppi

3. Fare clic su Gestione configurazione.



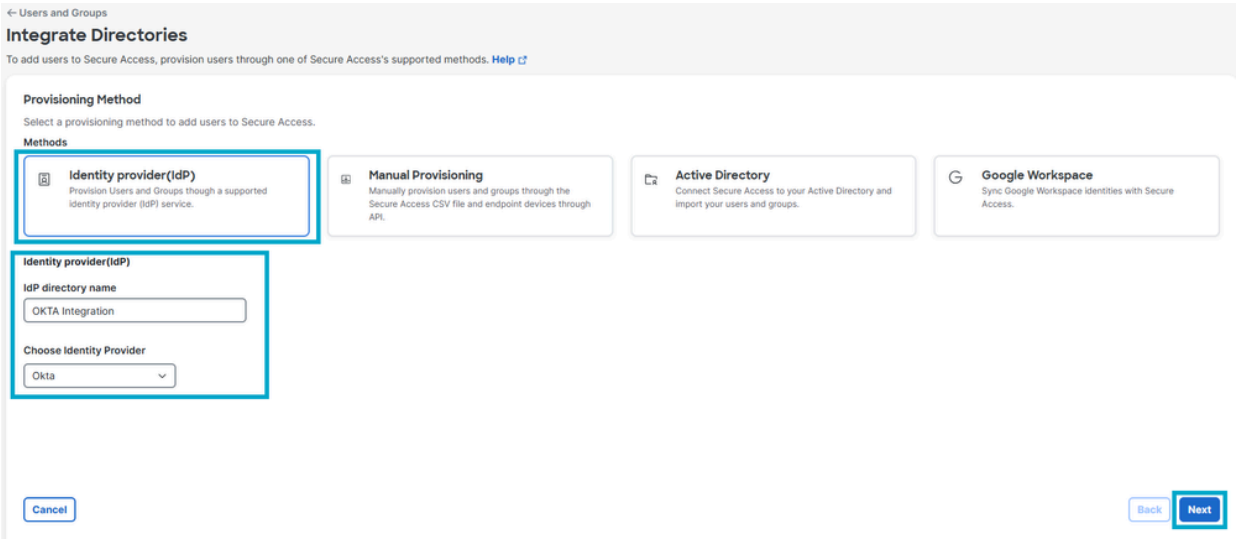

Gestione della configurazione

4. Fate clic su Integra directory (Integrate Directory).



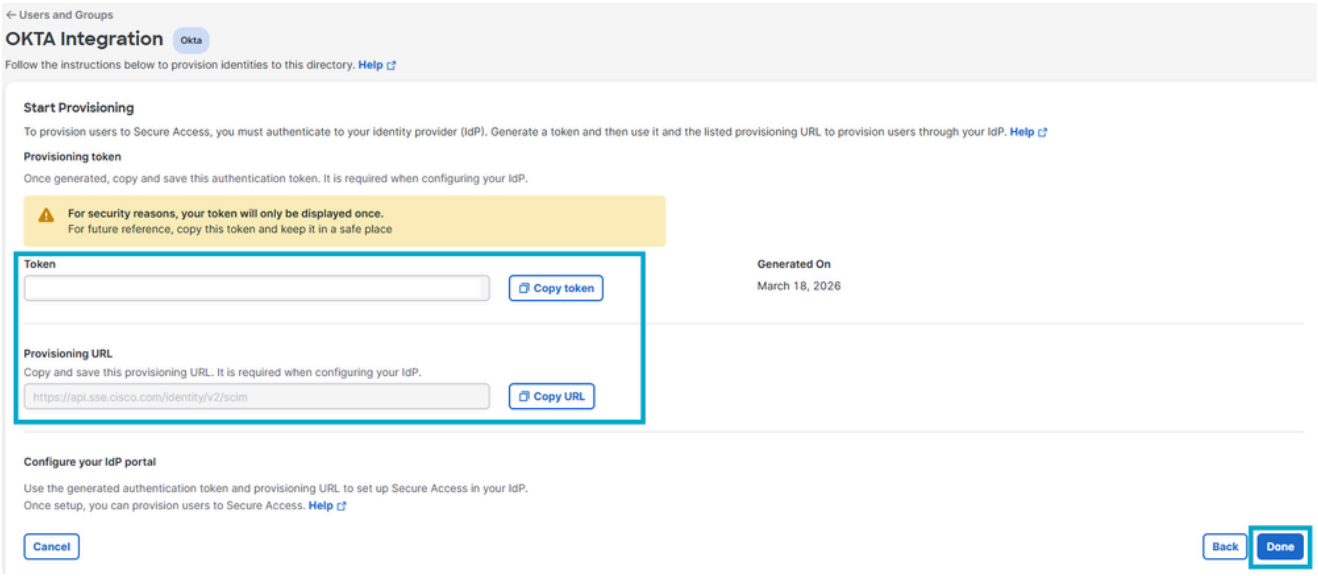

Directory di integrazione

5. In Metodo di provisioning fare clic su Provider di identità.
    - Nome directory IdP: Integrazione OKTA.
    - Scegli provider di identità: OK.
    - Fare clic su Next (Avanti).




*Directory Configuration*

6. Fare clic su Generate Token. Salvare il token generato e l'URL di provisioning, quindi fare clic su Done.

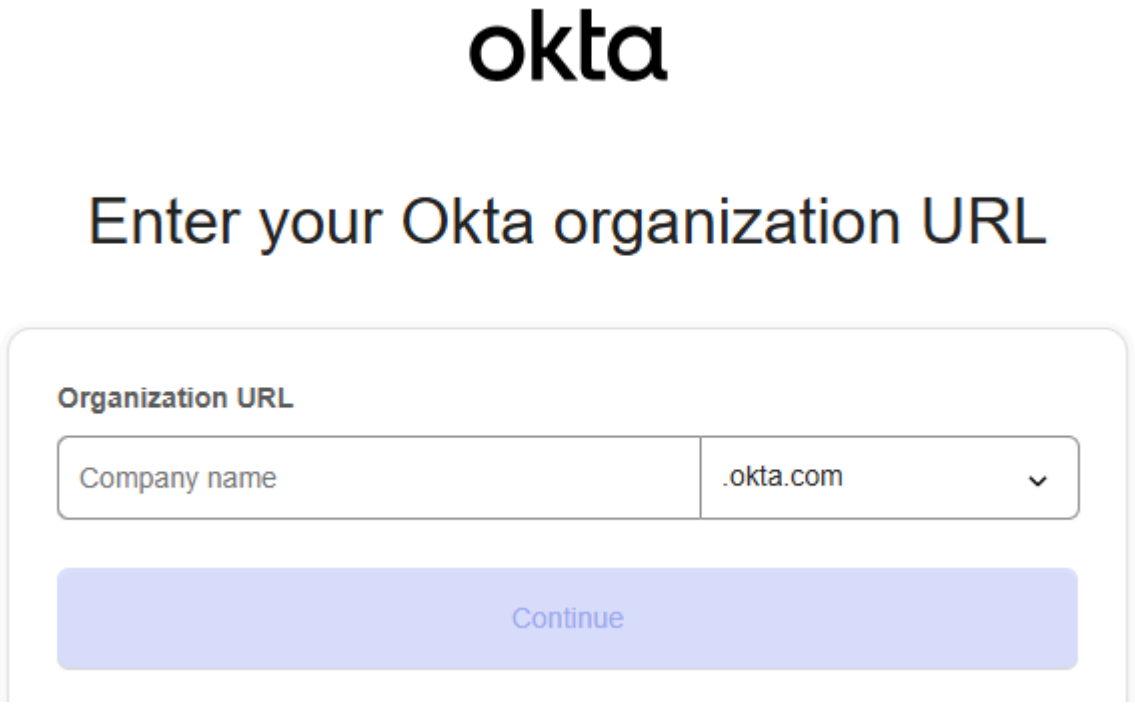



Genera token

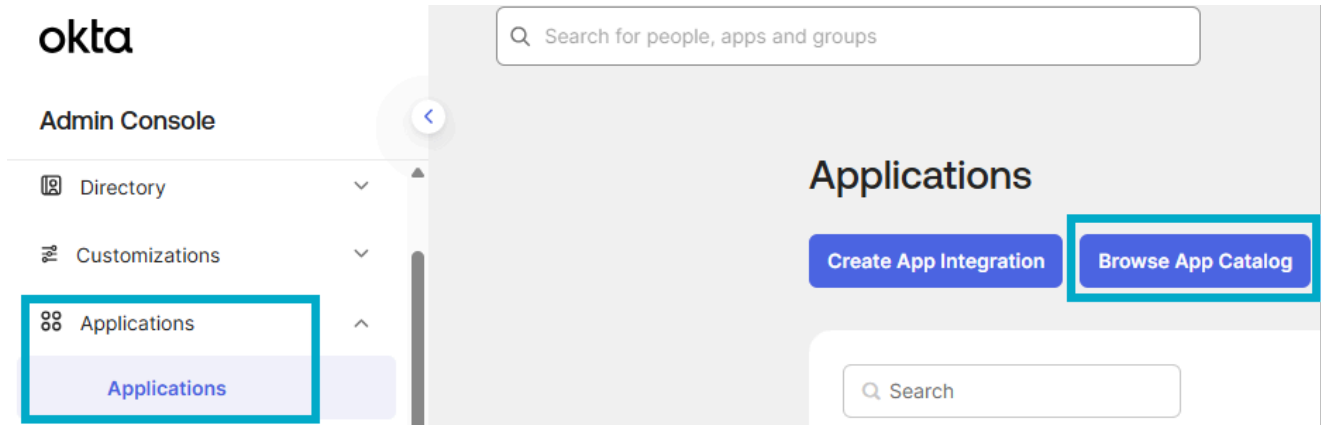
## Configura provisioning in OKTA

Dopo aver generato le credenziali nel dashboard Cisco Secure Access, è necessario configurare le impostazioni di provisioning nel tenant OKTA per abilitare la sincronizzazione di utenti e gruppi.

1. Accedere a OKTA.

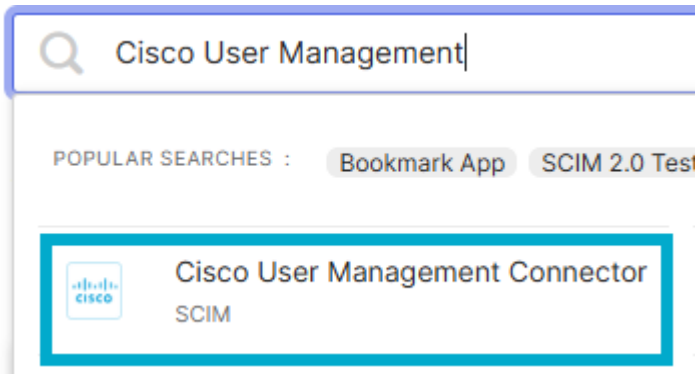


2. Passare a Applicazioni > Catalogo app browser.



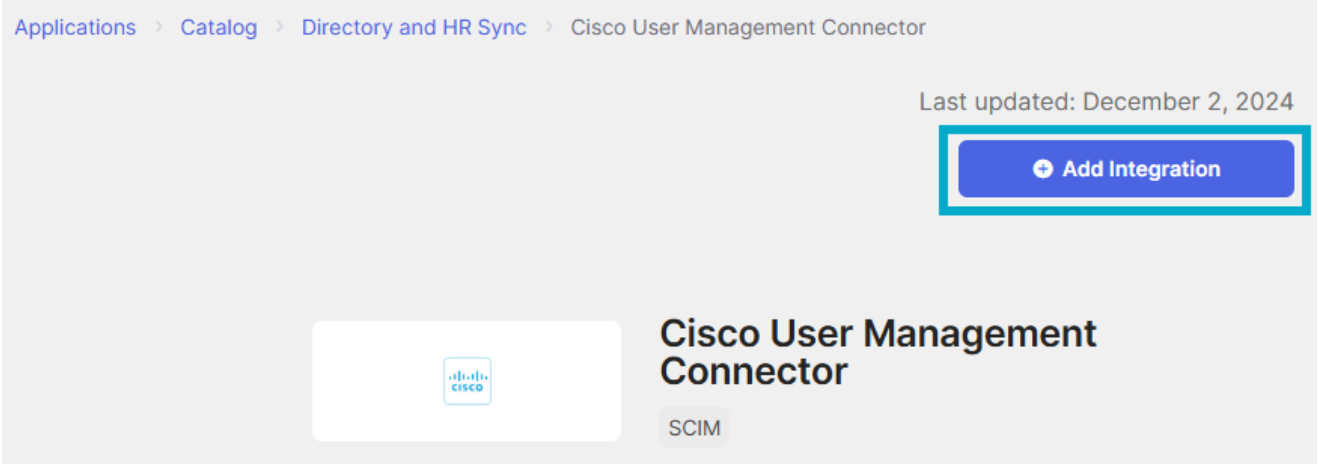

Sfoglia catalogo app

3. Selezionare l'app Cisco User Management Connector.



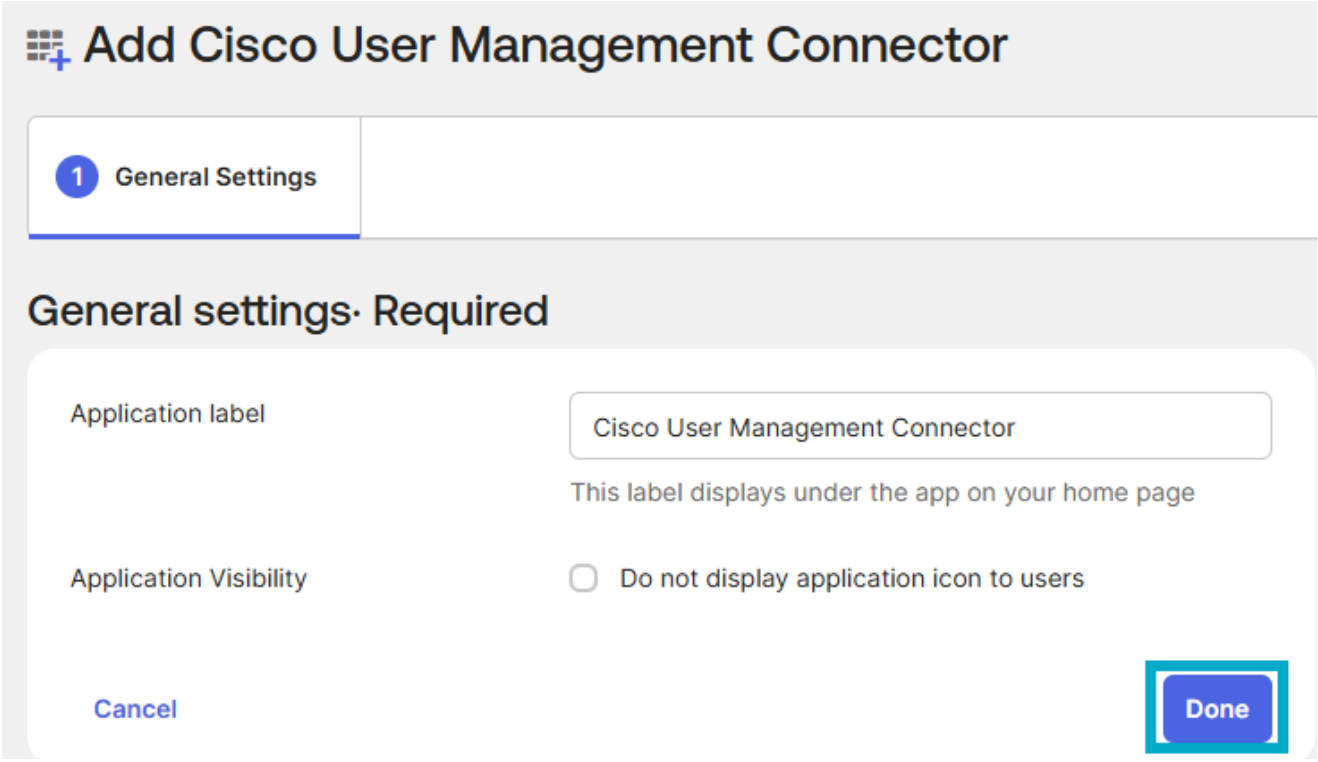

App Cisco

4. Fare clic su Aggiungi integrazione.



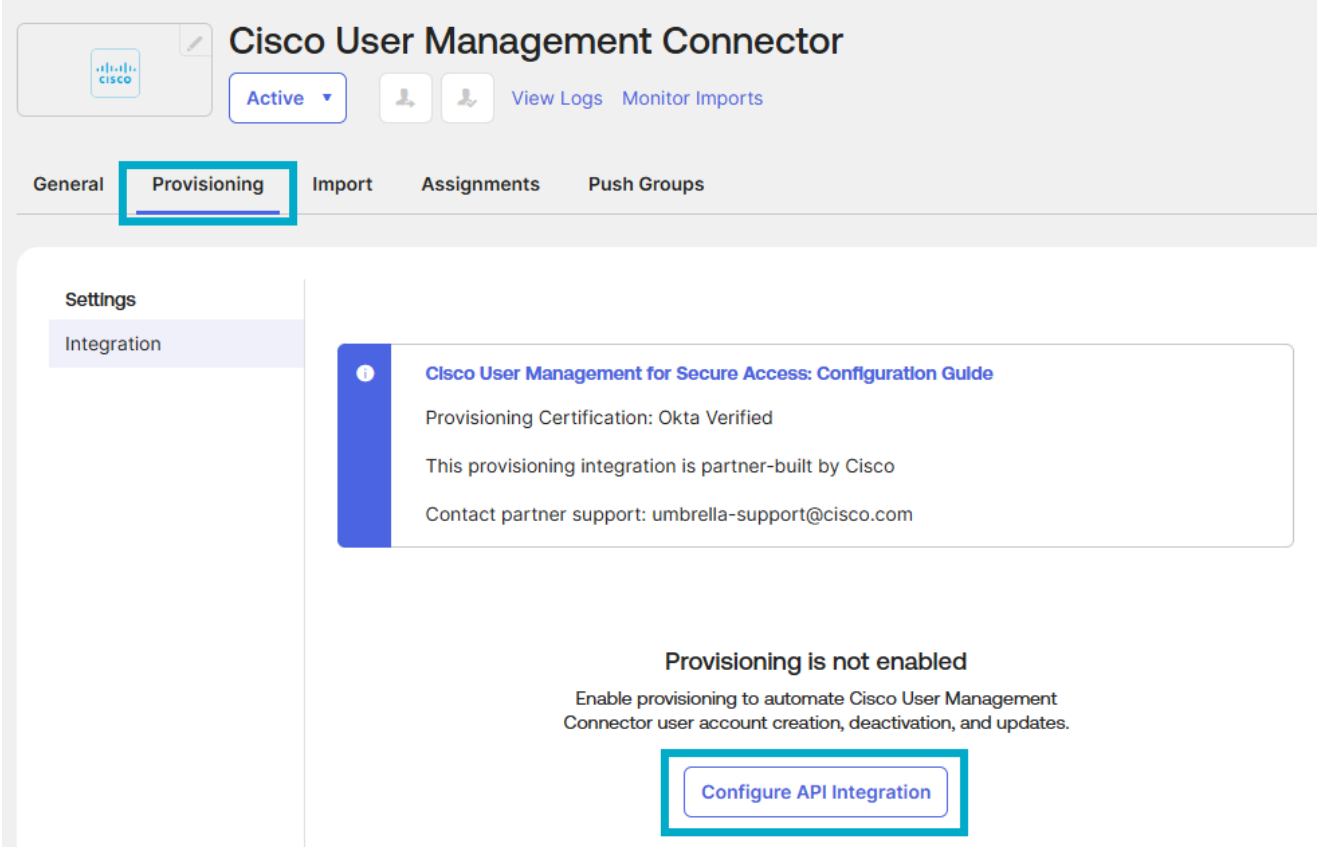

Aggiungi integrazione

5. Selezionate Fatto (Done).



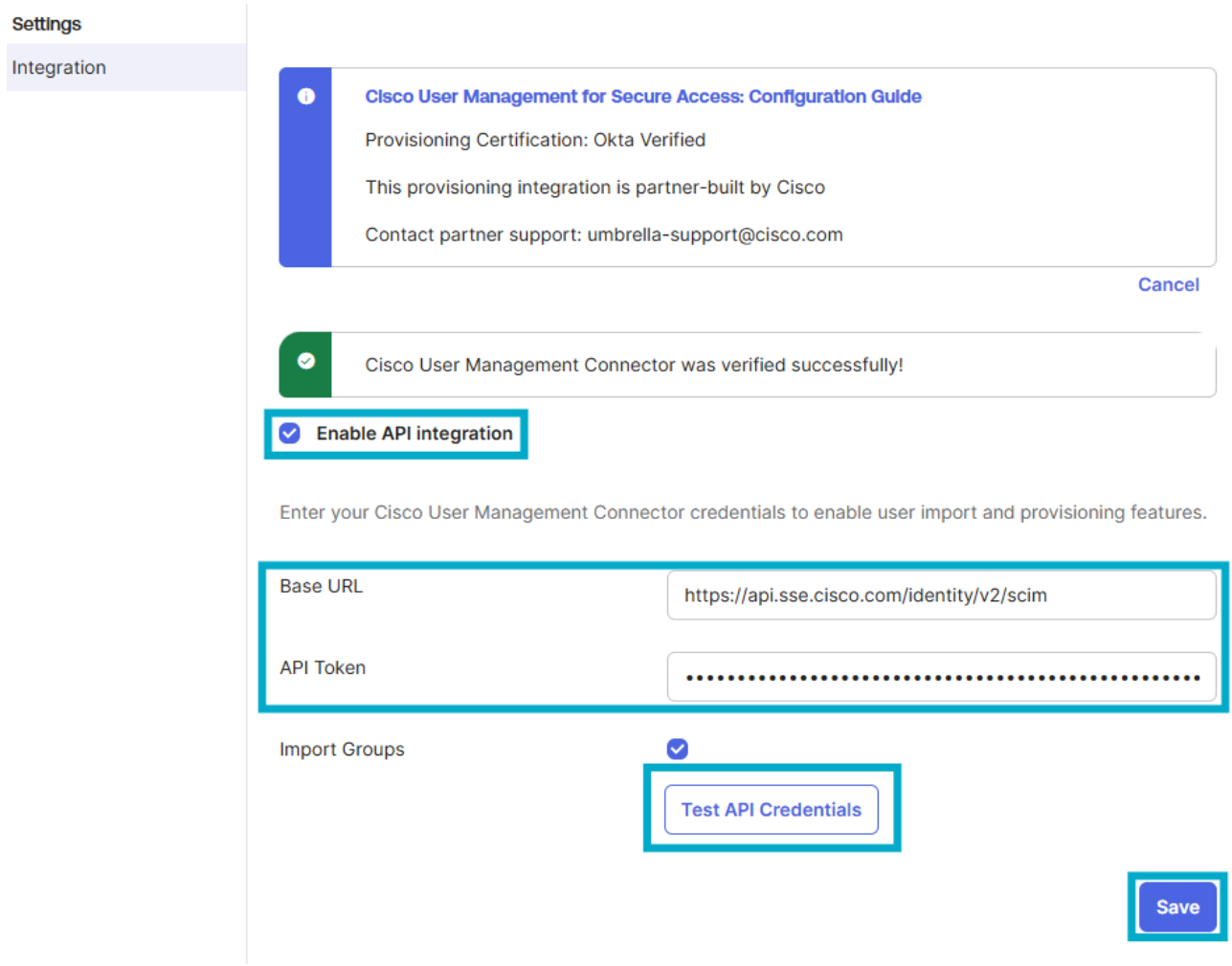

Aggiungi app

6. Fare clic su Provisioning > Configura integrazione API.

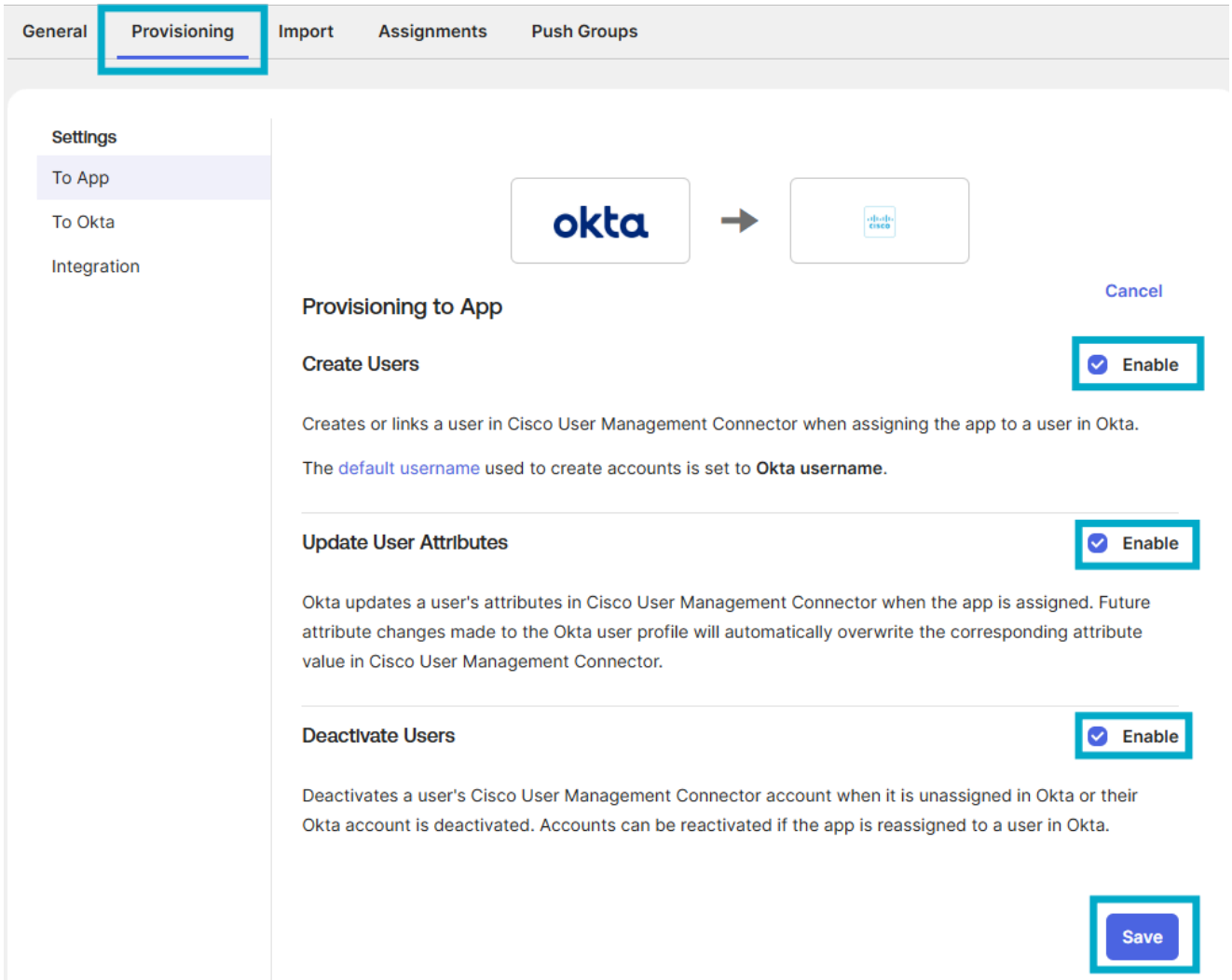



Configura integrazione API

7. Fare clic su Enable API Integration (Abilita integrazione API) e immettere l'URL basato e il token API salvati nel passaggio 6 della configurazione Secure Access. Fare clic su Prova credenziali API e quindi su Salva.




8. Passare a Provisioning > All'applicazione. Abilitare le opzioni Crea utenti, Aggiorna attributi utente e Disattiva utenti e fare clic su Salva.




Provisioning per app

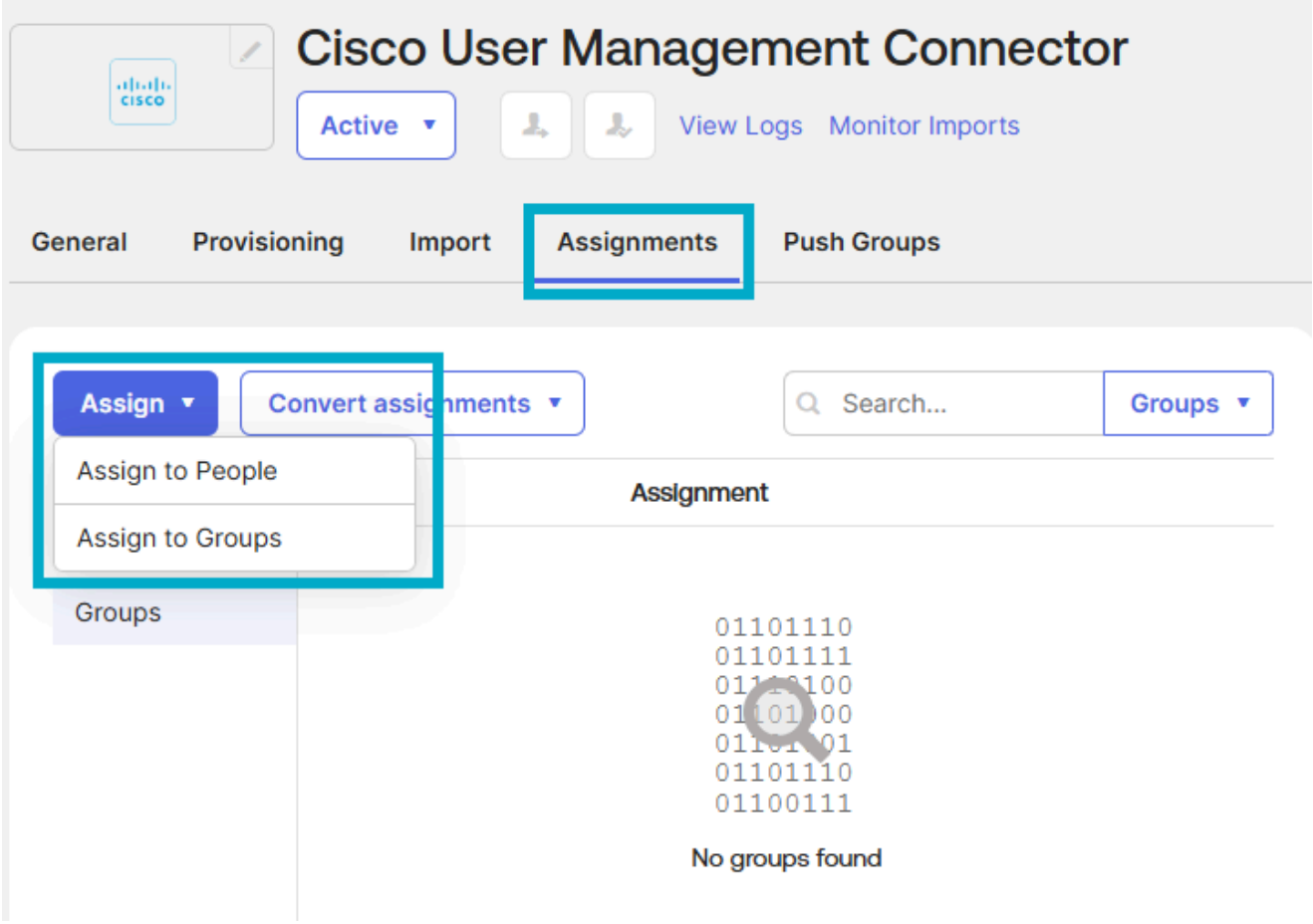
---

Nota: Verificare di aver selezionato questi attributi per la sincronizzazione con Secure Access. Secure Access elenca solo gli attributi Nome visualizzato e Nome utente per gli utenti, non gli attributi Nome specificato e Nome famiglia: Nome utente, Nome, Famiglia, Nome, Nome visualizzato, E-mail

(Facoltativo) Aggiungere un attributo objectGUID e creare il mapping del profilo utente. Se è necessario importare l'attributo objectGUID per gli utenti, aggiungere un nuovo attributo e mappare gli attributi nel mapping del profilo.

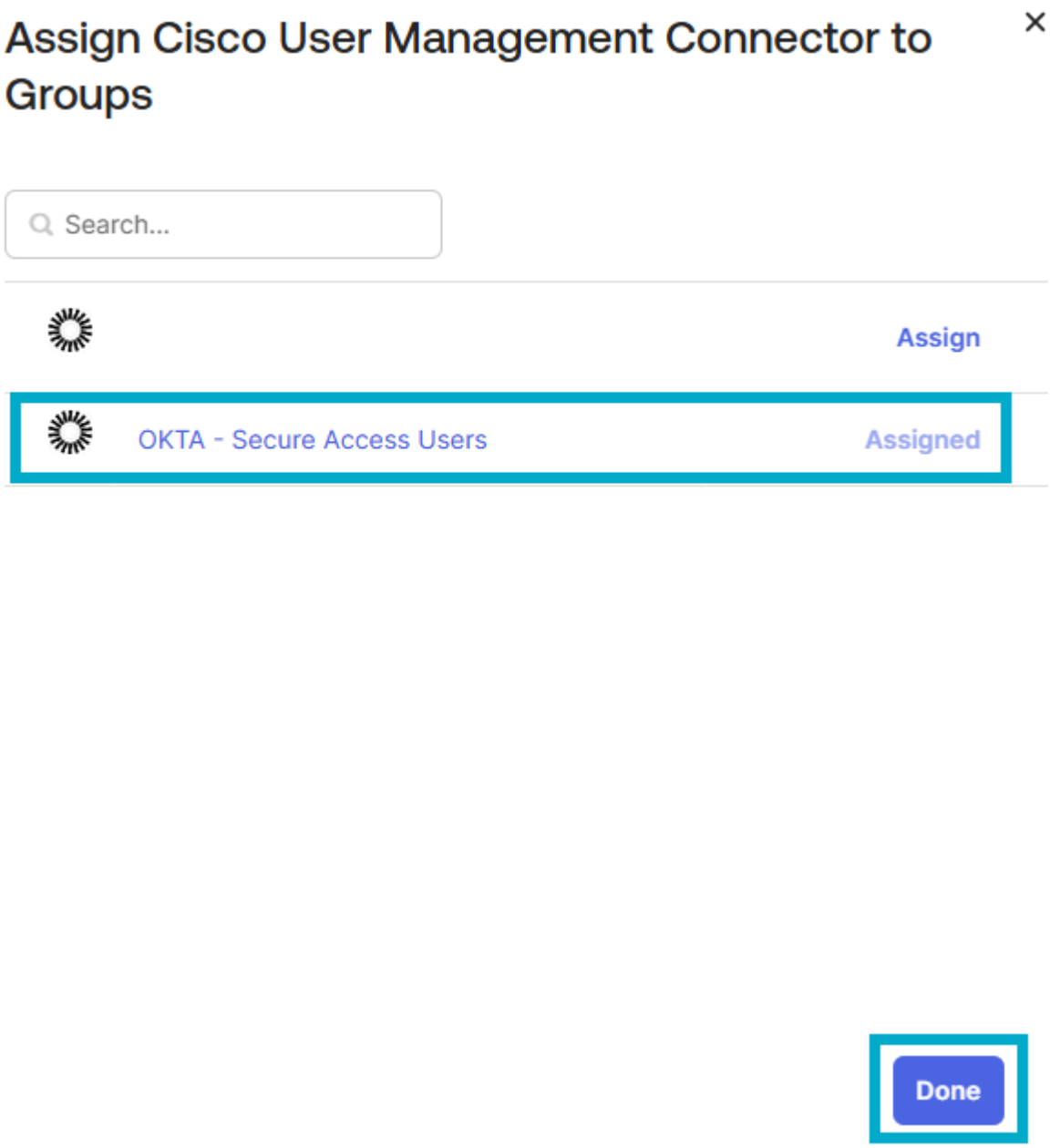
---

9. Per aggiungere persone/gruppi, fare clic su Assegnazioni > Assegna > Assegna a persone/Assegna a gruppi.




Assegnazione

10. Selezionare i gruppi/le persone che si desidera attivare per Accesso sicuro e fare clic su Assegna e quindi su Fine.

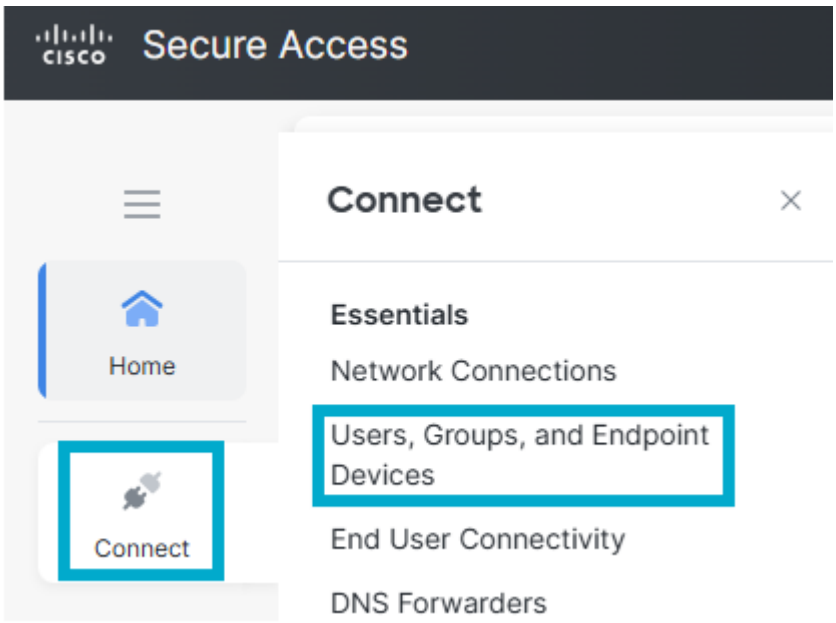



Assegna gruppi

## Verifica

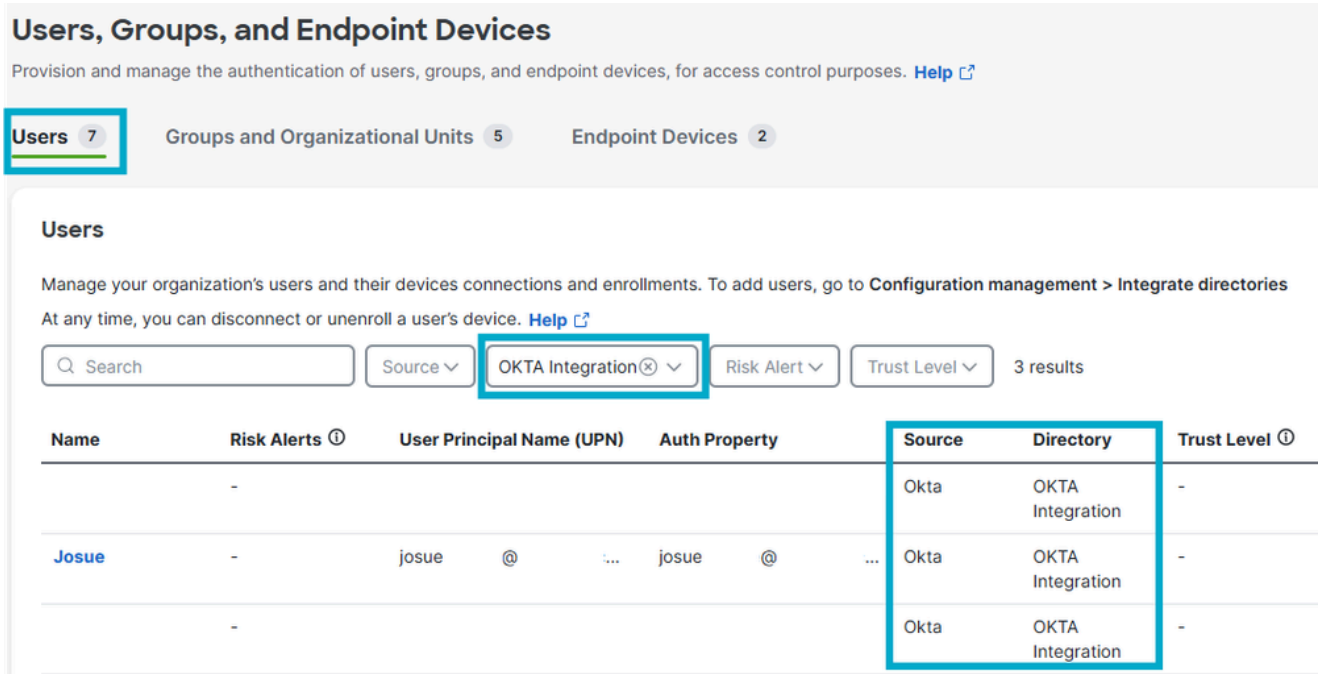
Verity in Cisco Secure Access

- Passare a Connetti > Utenti, gruppi e dispositivi endpoint.




Utenti e gruppi in CSA

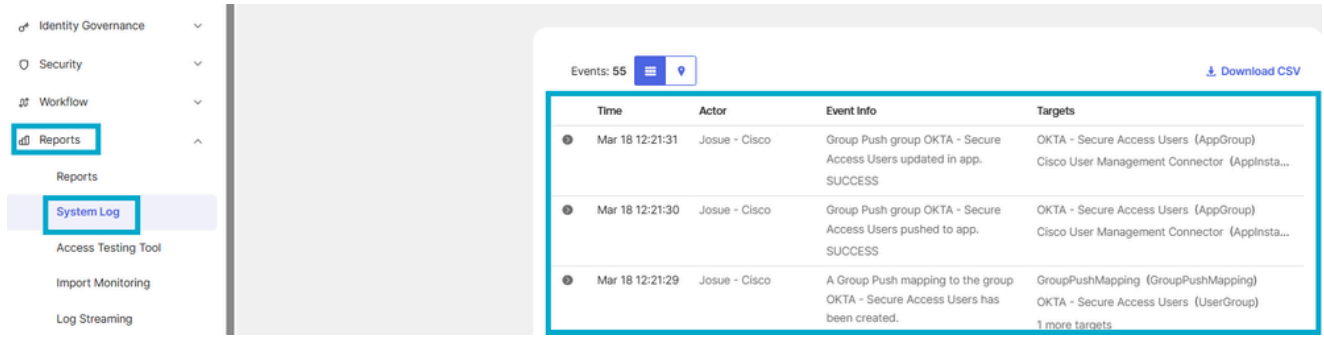
- Fare clic su Utenti.




Verifica degli utenti in CSA

Verity in OKTA

- Passare a Rapporti > Log di sistema.




Log OKTA

## Informazioni correlate

[Configura provider di identità]

[Assegna ruoli a utenti e gruppi da Okta]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).