

調配使用者和組以通過OKTA安全訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[配置思科安全訪問](#)

[在OKTA中配置調配](#)

[驗證](#)

[思科安全訪問中的真實性](#)

[奧克塔的維里蒂](#)

[相關資訊](#)

簡介

本檔案介紹如何將使用者群組從OKTA布建到Cisco Secure Access。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure Access
- OKTA

採用元件

本文件所述內容不限於特定軟體和硬體版本。

- Cisco Secure Access控制面板
- OKTA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco Secure Access支援從OKTA調配使用者和組。

此設定使Secure Access能夠維護授權以下使用者的目錄：

- 註冊零信任訪問(ZTA)。
- 連線到VPNaaS。
- 將基於身份的策略應用於Umbrella漫遊使用者。



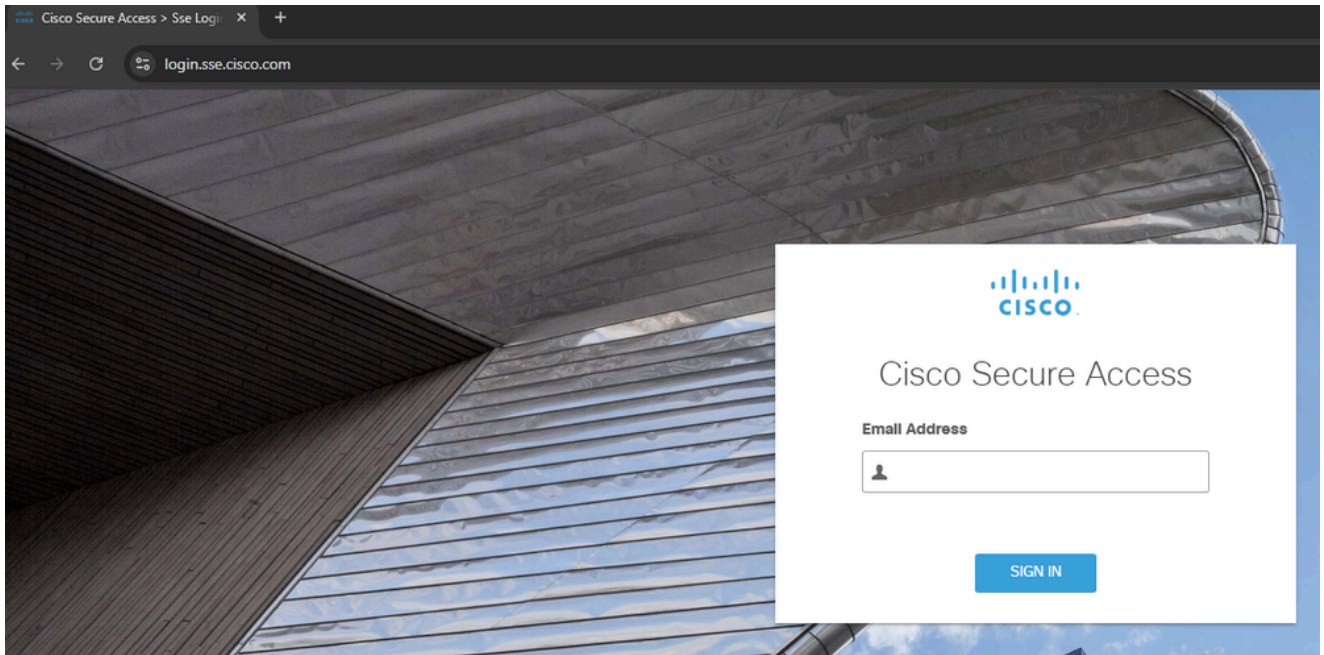
附註：本文檔專門介紹如何從OKTA調配使用者和組。為ZTA註冊、VPNaaS身份驗證或特定Umbrella漫遊設定配置Entra ID或其他身份提供程式(IdP)不在本指南範圍內。

設定

配置思科安全訪問

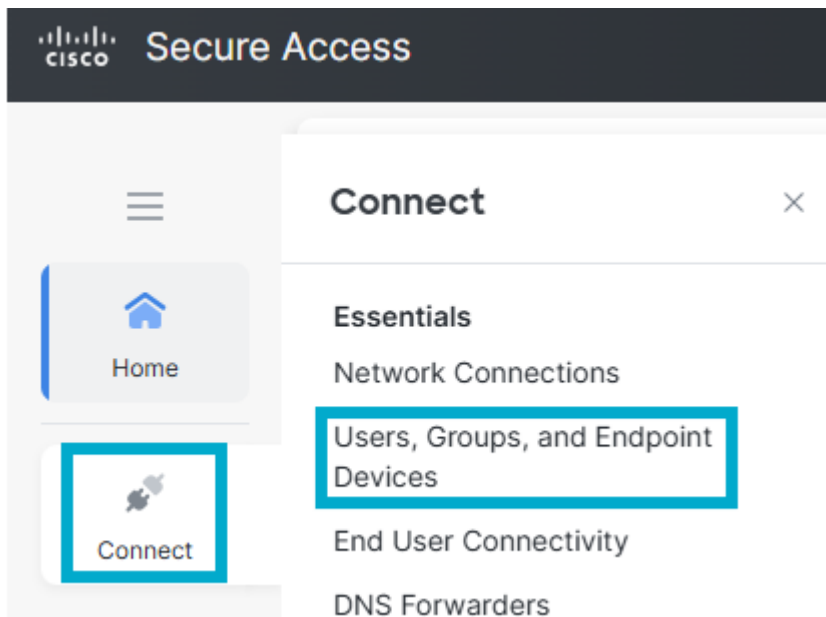
要開始調配流程，您必須首先在Cisco Secure Access控制面板中配置目錄整合。此步驟生成與OKTA建立安全連線所需的必要憑證和配置引數。

1. 登入到Cisco Secure Access [Dashboard](#)。



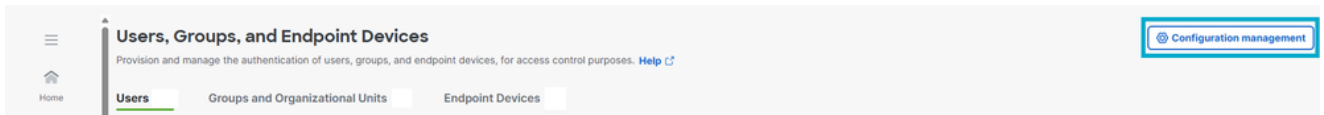
登入到CSA

2. 導覽至Connect > Users , Groups and Endpoint Devices。



使用者和組

3. 按一下「Configuration management」。



組態管理

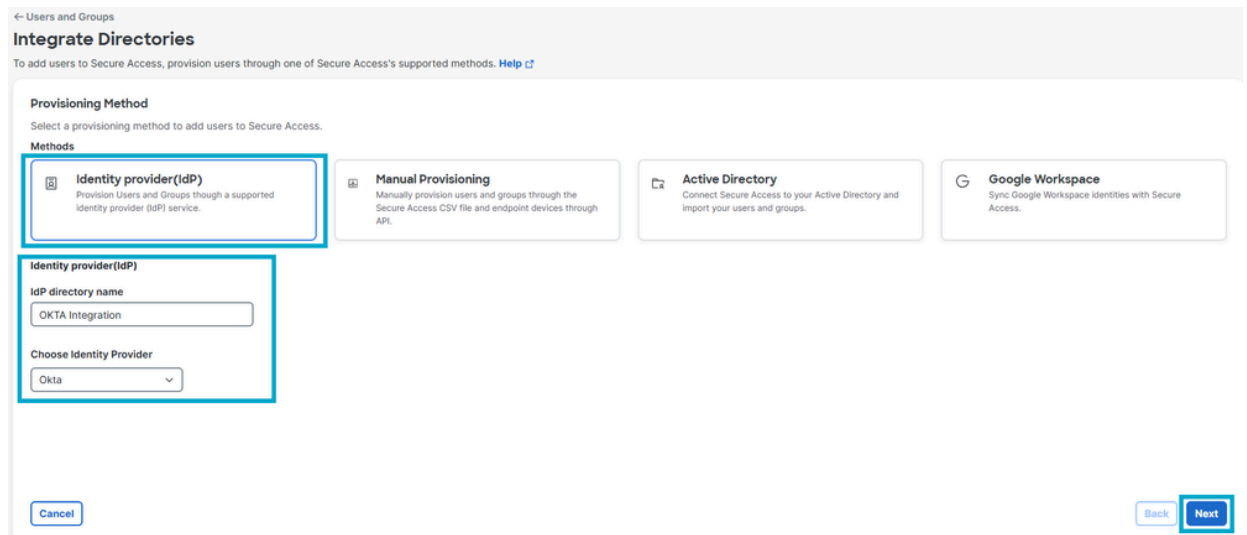
4. 按一下Integrate Directory。



整合目錄

5. 在Provision Method下，按一下Identity Provider。

- IdP目錄名稱：OKTA整合。
- 選擇Identity Provider:好吧。
- 按「Next」（下一步）。



Directory Configuration

6. 按一下Generate Token。儲存生成的令牌和預配URL，然後按一下Done。

← Users and Groups

OKTA Integration Okta

Follow the instructions below to provision identities to this directory. [Help](#)

Start Provisioning

To provision users to Secure Access, you must authenticate to your identity provider (IdP). Generate a token and then use it and the listed provisioning URL to provision users through your IdP. [Help](#)

Provisioning token

Once generated, copy and save this authentication token. It is required when configuring your IdP.

⚠ For security reasons, your token will only be displayed once. For future reference, copy this token and keep it in a safe place

Token <input type="text"/> Copy token	Generated On March 18, 2026
--	---------------------------------------

Provisioning URL

Copy and save this provisioning URL. It is required when configuring your IdP.

<input type="text" value="https://api.sse.cisco.com/identity/v2/scim"/> Copy URL

Configure your IdP portal

Use the generated authentication token and provisioning URL to set up Secure Access in your IdP. Once setup, you can provision users to Secure Access. [Help](#)

[Cancel](#) [Back](#) [Done](#)

生成令牌

在OKTA中配置調配

在Cisco Secure Access控制面板中生成憑證後，必須在OKTA租戶中配置調配設定，以啟用使用者和組的同步。

1. 登入到[OKTA](#)。

okta

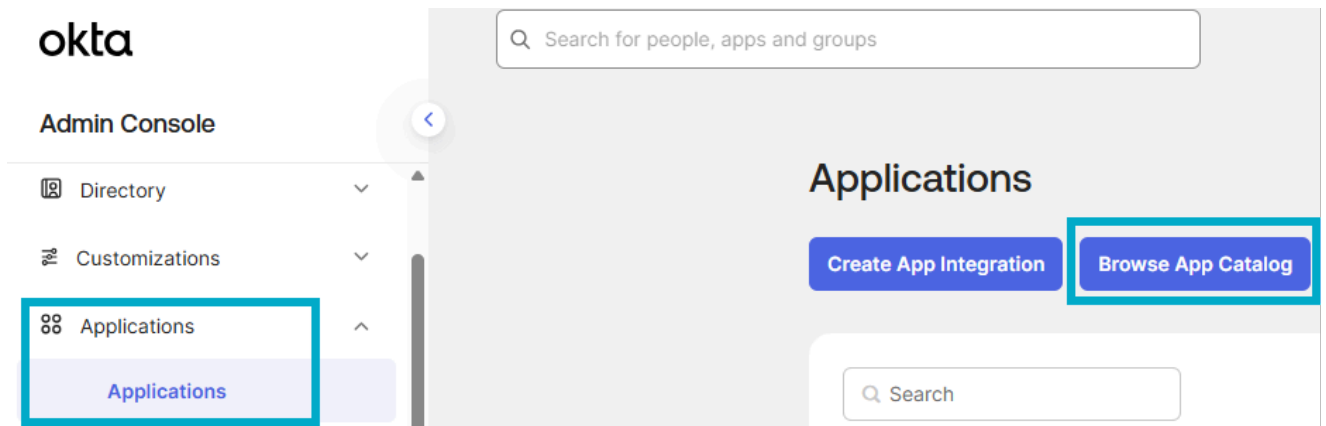
Enter your Okta organization URL

Organization URL

<input type="text" value="Company name"/>	<input type="text" value=".okta.com"/> ▼
---	---

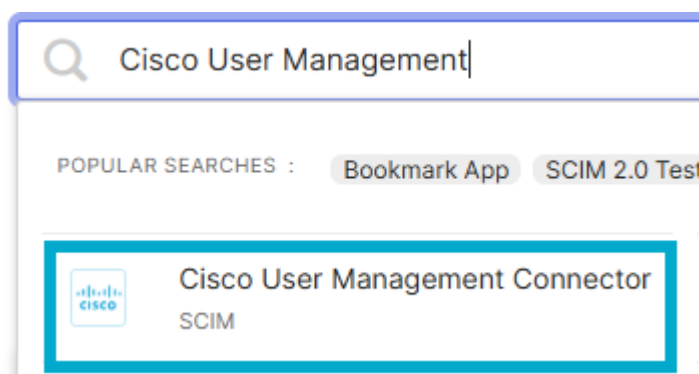
[Continue](#)

2. 導航到Applications > Browser App Catalog。



瀏覽應用目錄

3. 選擇Cisco User Management Connector應用程式。



思科應用程式

4. 按一下Add Integration。

Last updated: December 2, 2024

+ Add Integration



Cisco User Management Connector

SCIM

新增整合

5. 按一下「完成」。

+ Add Cisco User Management Connector

1 General Settings

General settings · Required

Application label

Cisco User Management Connector

This label displays under the app on your home page

Application Visibility

Do not display application icon to users

Cancel

Done

新增應用

6. 按一下 Provisioning > Configure API Integration。

Cisco User Management Connector

Active ▾

View Logs Monitor Imports

General **Provisioning** Import Assignments Push Groups

Settings

Integration

1 [Cisco User Management for Secure Access: Configuration Guide](#)

Provisioning Certification: Okta Verified

This provisioning integration is partner-built by Cisco

Contact partner support: umbrella-support@cisco.com

Provisioning is not enabled

Enable provisioning to automate Cisco User Management Connector user account creation, deactivation, and updates.

[Configure API Integration](#)

配置API整合

7. 按一下Enable API Integration，然後輸入Based URL 和API 標籤，它們儲存在安全訪問配置的步驟#6。按一下Test API Credentials，然後按一下Save。

Settings

Integration

Cisco User Management for Secure Access: Configuration Guide
Provisioning Certification: Okta Verified
This provisioning integration is partner-built by Cisco
Contact partner support: umbrella-support@cisco.com

Cancel

Cisco User Management Connector was verified successfully!

Enable API integration

Enter your Cisco User Management Connector credentials to enable user import and provisioning features.

Base URL	<input type="text" value="https://api.sse.cisco.com/identity/v2/scim"/>
API Token	<input type="password" value="....."/>

Import Groups

Test API Credentials

Save

API測試

8. 導航到調配>到應用。啟用選項Create Users、Update User Attributes和Deactivate Users，然後按一下Save。

General **Provisioning** Import Assignments Push Groups

Settings
To App
To Okta
Integration

okta → Cisco

Provisioning to App Cancel

Create Users Enable

Creates or links a user in Cisco User Management Connector when assigning the app to a user in Okta.
The [default username](#) used to create accounts is set to **Okta username**.

Update User Attributes Enable

Okta updates a user's attributes in Cisco User Management Connector when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Cisco User Management Connector.

Deactivate Users Enable

Deactivates a user's Cisco User Management Connector account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

Save

調配到應用



附註：驗證是否選擇這些屬性以同步到Secure Access。「安全訪問」僅列出使用者的「顯示名稱」和「使用者名稱」屬性，而不列出「指定名稱」和「姓氏」屬性：使用者名稱、指定名稱、系列、名稱、顯示名稱、電子郵件

(可選) 新增 [objectGUID 屬性](#) 並建立使用者配置檔案對映。如果需要匯入使用者的 objectGUID 屬性，請新增新的屬性並對映配置檔案對映中的屬性。

9. 要新增人員/組，請按一下「分配」>「分配」>「分配給人員/分配給組」。

The screenshot shows the Cisco User Management Connector interface. At the top, there is a header with the Cisco logo, a status indicator 'Active', and navigation links for 'View Logs' and 'Monitor Imports'. Below the header, there are tabs for 'General', 'Provisioning', 'Import', 'Assignments', and 'Push Groups'. The 'Assignments' tab is selected and highlighted with a red box. In the main content area, there is a search bar and a 'Groups' dropdown menu. A red box highlights the 'Assign' dropdown menu, which is open and shows two options: 'Assign to People' and 'Assign to Groups'. Below the search bar, there is a list of binary strings under the heading 'Assignment':



```
01101110
01101111
01101100
01101100
01101101
01101110
01100111
```

Below the list, it says 'No groups found'.

分配

10. 選擇要設定為Secure Access的組/人員，然後按一下Assign，然後按一下Done。

Assign Cisco User Management Connector to Groups ×

		Assign
	OKTA - Secure Access Users	Assigned

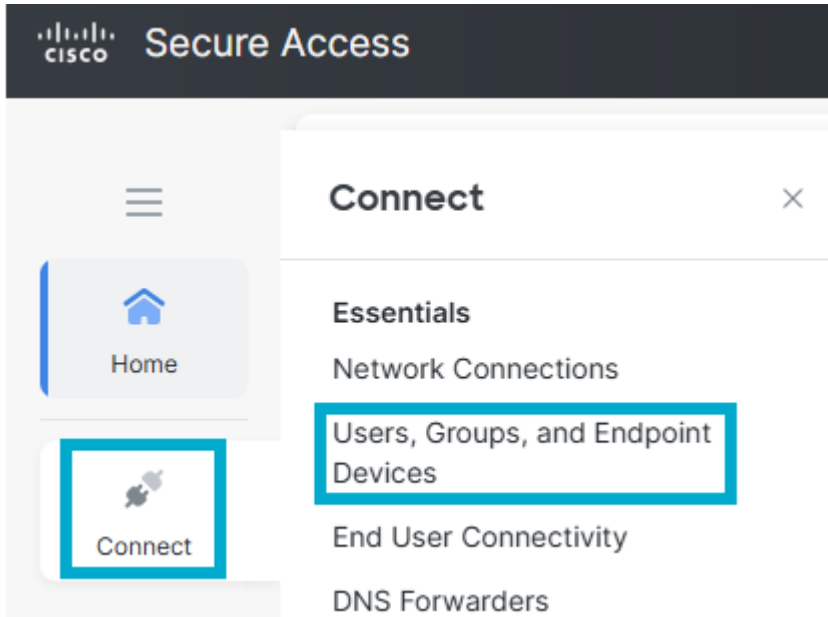
[Done](#)

分配組

驗證

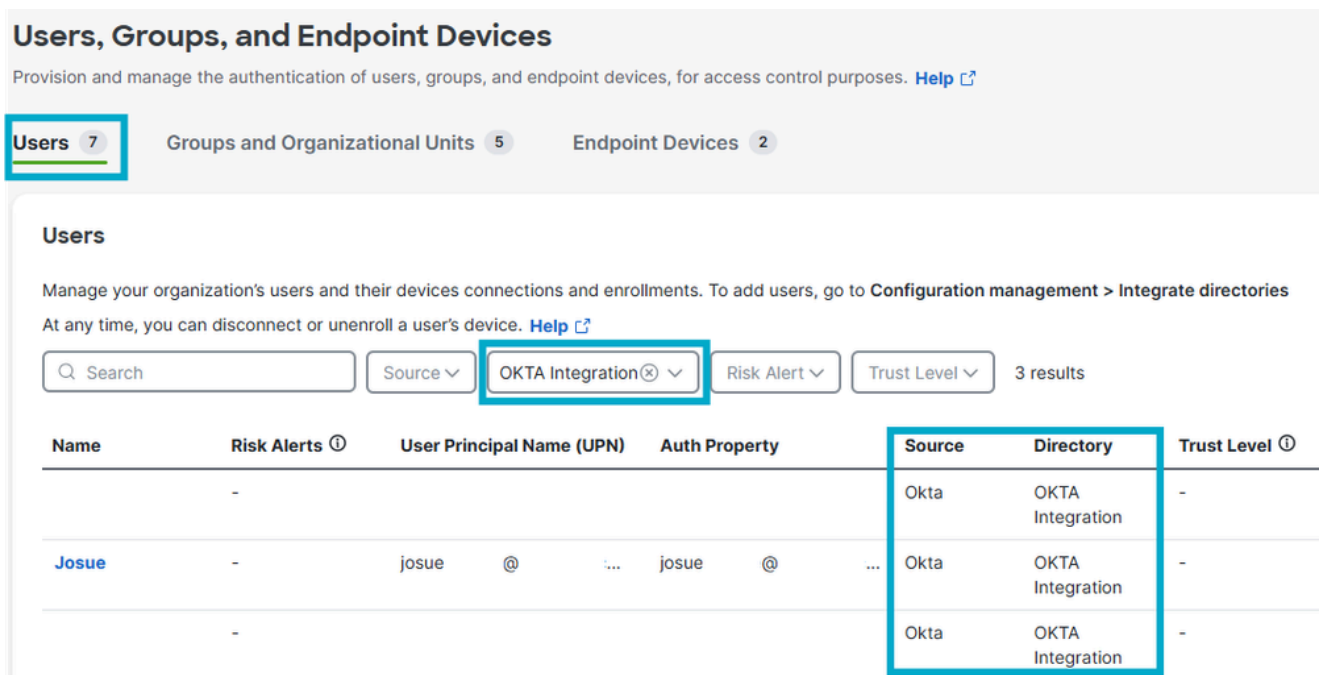
思科安全訪問中的真實性

- 導覽至Connect > Users , Groups and Endpoint Devices。



CSA中的使用者和組

- 按一下「Users」。



驗證CSA中的使用者

奧克塔的維里蒂

- 導航到Reports > System Log。

Time	Actor	Event Info	Targets
Mar 18 12:21:31	Josue - Cisco	Group Push group OKTA - Secure Access Users updated in app. SUCCESS	OKTA - Secure Access Users (AppGroup) Cisco User Management Connector (AppInsta...
Mar 18 12:21:30	Josue - Cisco	Group Push group OKTA - Secure Access Users pushed to app. SUCCESS	OKTA - Secure Access Users (AppGroup) Cisco User Management Connector (AppInsta...
Mar 18 12:21:29	Josue - Cisco	A Group Push mapping to the group OKTA - Secure Access Users has been created.	GroupPushMapping (GroupPushMapping) OKTA - Secure Access Users (UserGroup) 1 more targets

OKTA日誌

相關資訊

[配置身份提供程式](#)

[從Okta調配使用者和組](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。