配置安全訪問，以使用帶Python的REST API

目錄

簡介

本文檔介紹配置API訪問並將其用於從Secure Access獲取資源資訊的步驟。

必要條件

思科建議您瞭解以下主題：

1. Python 3.x
2. REST API
3. Cisco Secure Access

需求

在繼續操作之前，必須滿足以下要求：

- 具有完整管理員使用者角色的Cisco Secure Access使用者帳戶。
- 思科安全雲單點登入(SCSO)帳戶用於登入安全訪問。

採用元件

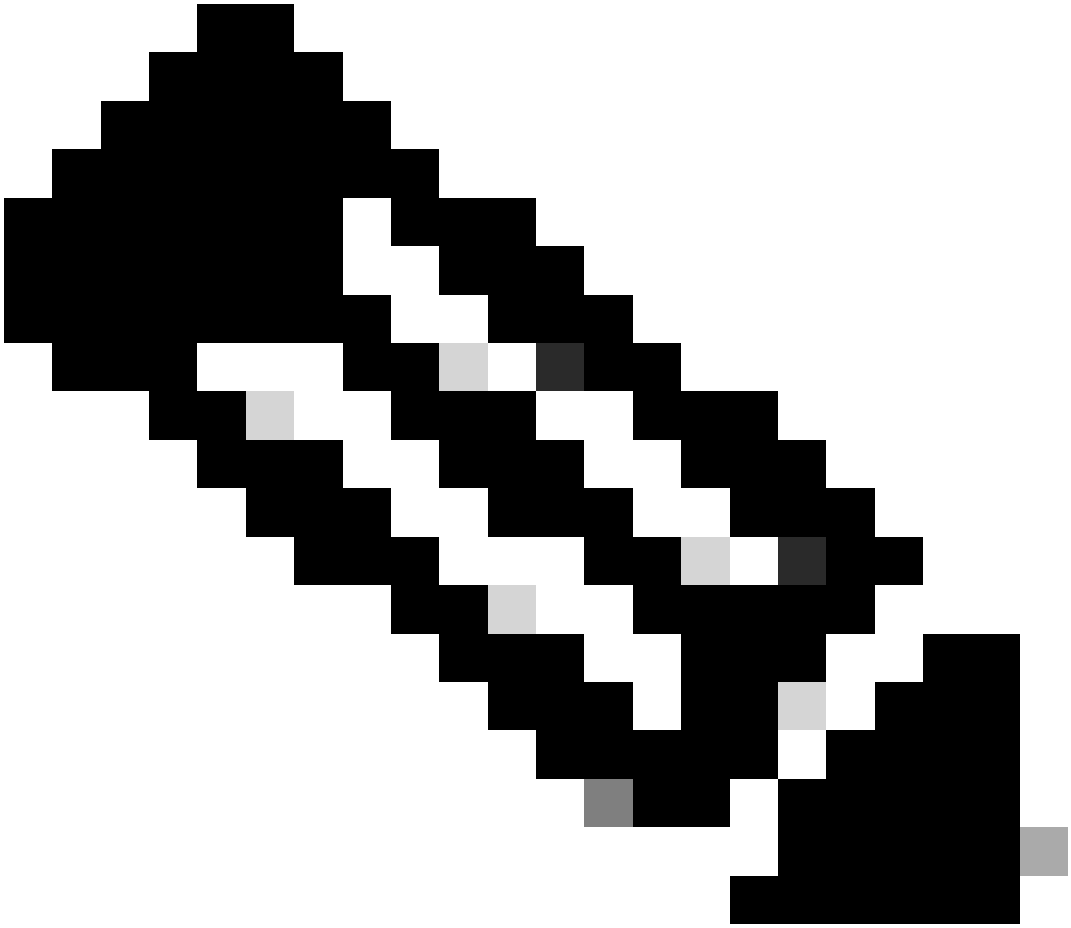
本文中的資訊係根據以下軟體和硬體版本：

- 安全訪問控制台
- Python

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。

設定

安全訪問API提供標準REST介面並支援OAuth 2.0客戶端憑證流。若要開始使用，請登入Secure Access並建立您的Secure Access API金鑰。然後，使用您的API憑證生成API訪問令牌。



> 注意：API金鑰、密碼、密碼和令牌允許訪問您的私有資料。您絕不能與其他使用者或組織共用您的認證。

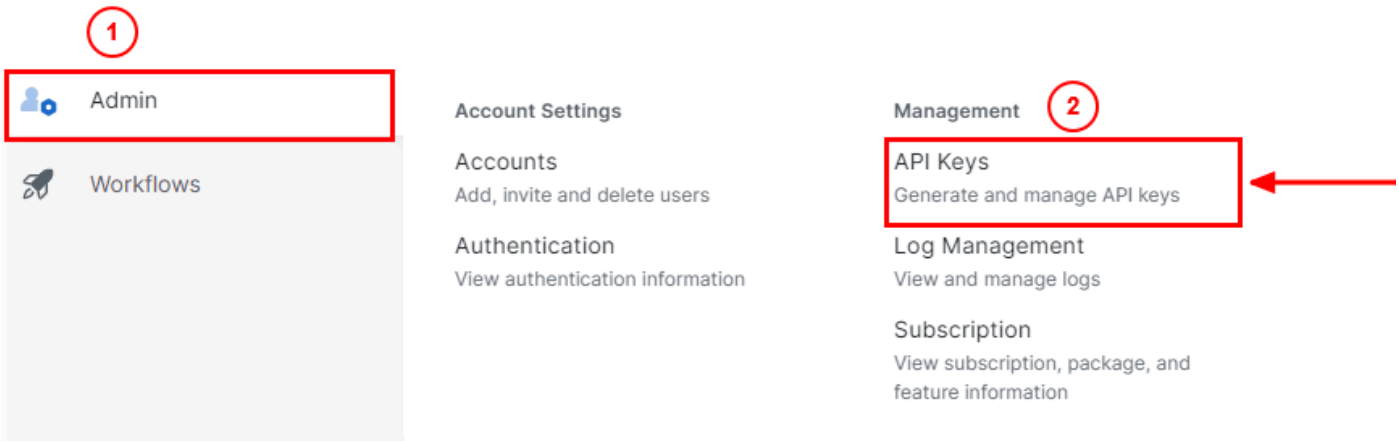
在執行本文中提到的指令碼之前，請從Secure Access Dashboard配置API金鑰。

建立API金鑰

使用以下步驟建立API金鑰和金鑰。使用URL登入安全訪問：安全訪問

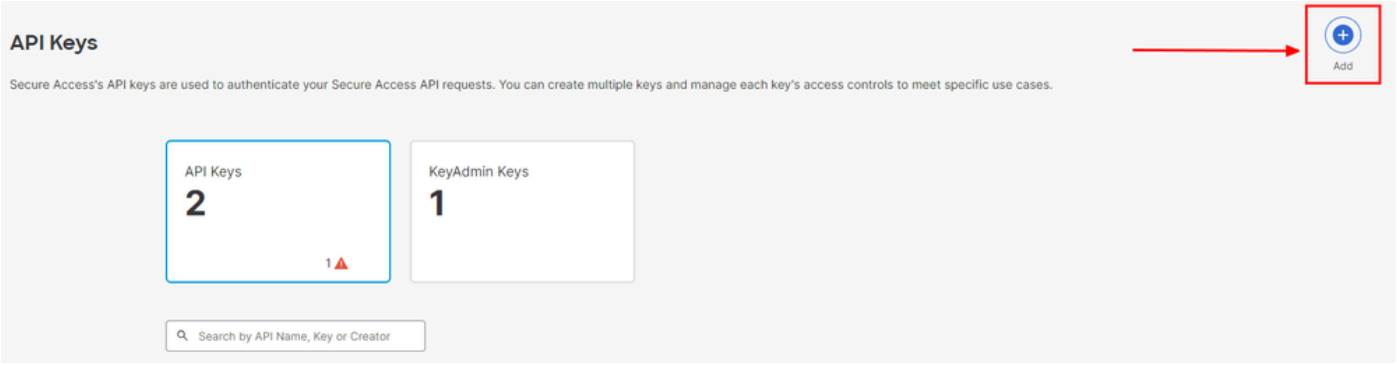
1. 從左側側邊欄中選擇選項Admin。

- 在Admin下選擇選項 **API Keys**:



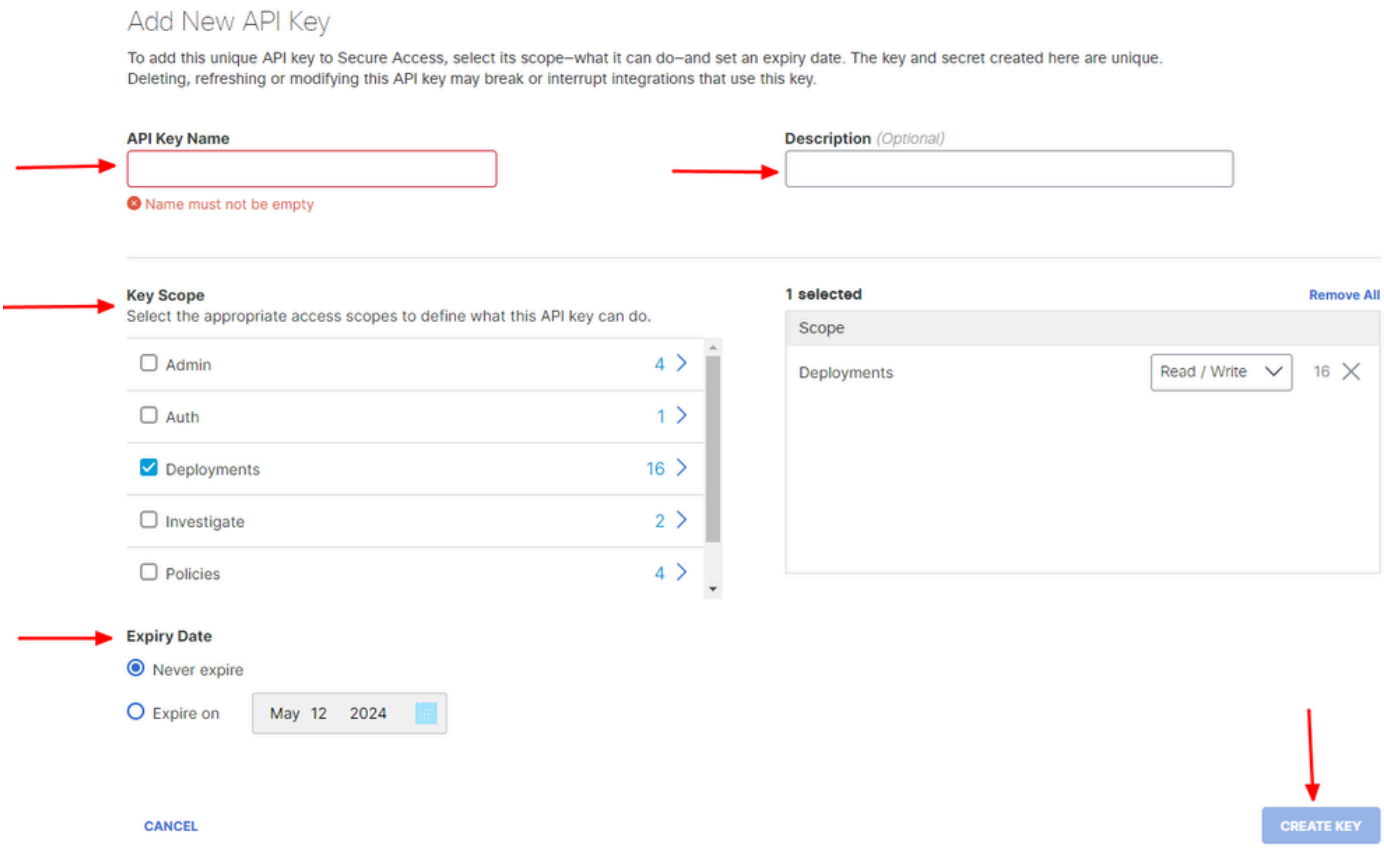
安全訪問控制台管理員- *API*金鑰

3. 在右上角，按一下+ 按鈕增加新的API金鑰：



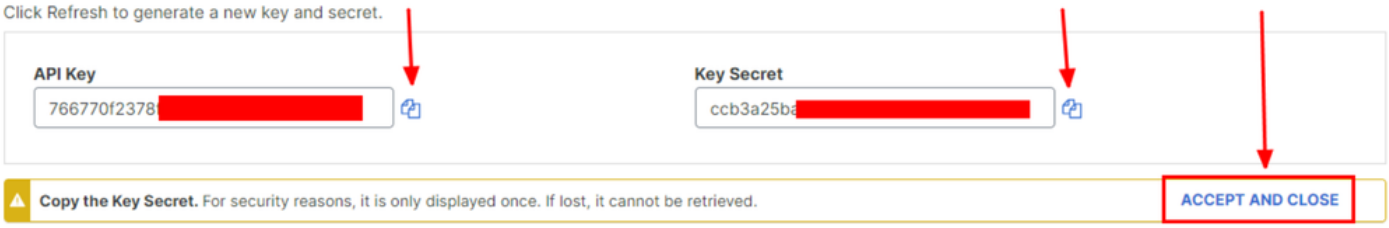
安全訪問-增加*API*金鑰

4. 提供 **API Key Name, Description**（可選），並根據您的要求選擇Key scope和Expiry date 。完成後，按一下 **Create**按鈕：

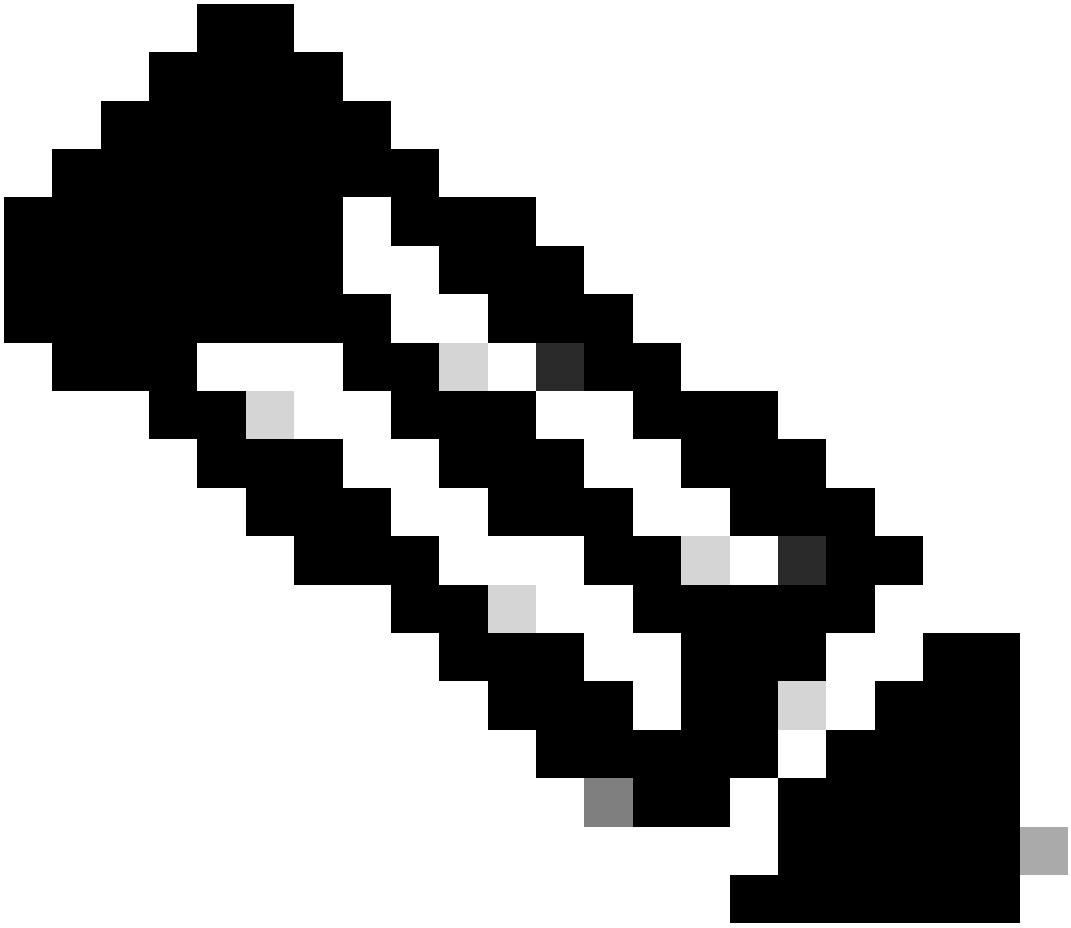


安全存取- *API*金鑰詳細資料

5. **複製**API Key**和 Key Secret** ，然後按一下ACCEPT AND CLOSE：



安全存取- *API*金鑰和密碼



注意：複製API機密的機會只有一個。Secure Access不會儲存您的API密碼，您無法在最初建立後檢索它。

Python代碼

考慮到生成的令牌的有效時間為3600秒（1小時），編寫此代碼的方式有多種。您可以建立兩個單獨的指令碼，第一個指令碼可用於生成持有者令牌，第二個指令碼可用於對感興趣的資源進行API呼叫（獲取/更新或刪除），或者編寫一個指令碼來同時執行這兩個操作，同時確保如果已經生成持有者令牌，則代碼中會保留一個條件，即在每次執行指令碼時不會生成新的持有者令牌。

為了使其在python中工作，請確保安裝以下庫：

```
pip install oauthlib pip install requests_oauthlib
```

指令碼1：

確保在此指令碼中提及正確的client_id和client_secret：

```
import requests from oauthlib.oauth2 import BackendApplicationClient from oauthlib.oauth2 import TokenE
```

輸出：

此指令碼的輸出必須類似於以下內容：

```
Token: {'token_type': 'bearer', 'access_token': 'eyJhbGciOiJSUzI1NiIsImtpZCI6IjcyNmI5MGUzLWxxxxxxxxxxxxx
```

access_token的長度非常長，包含數千個字元，因此，為了讓輸出保持可讀，它僅在以下示例中進行了縮短。

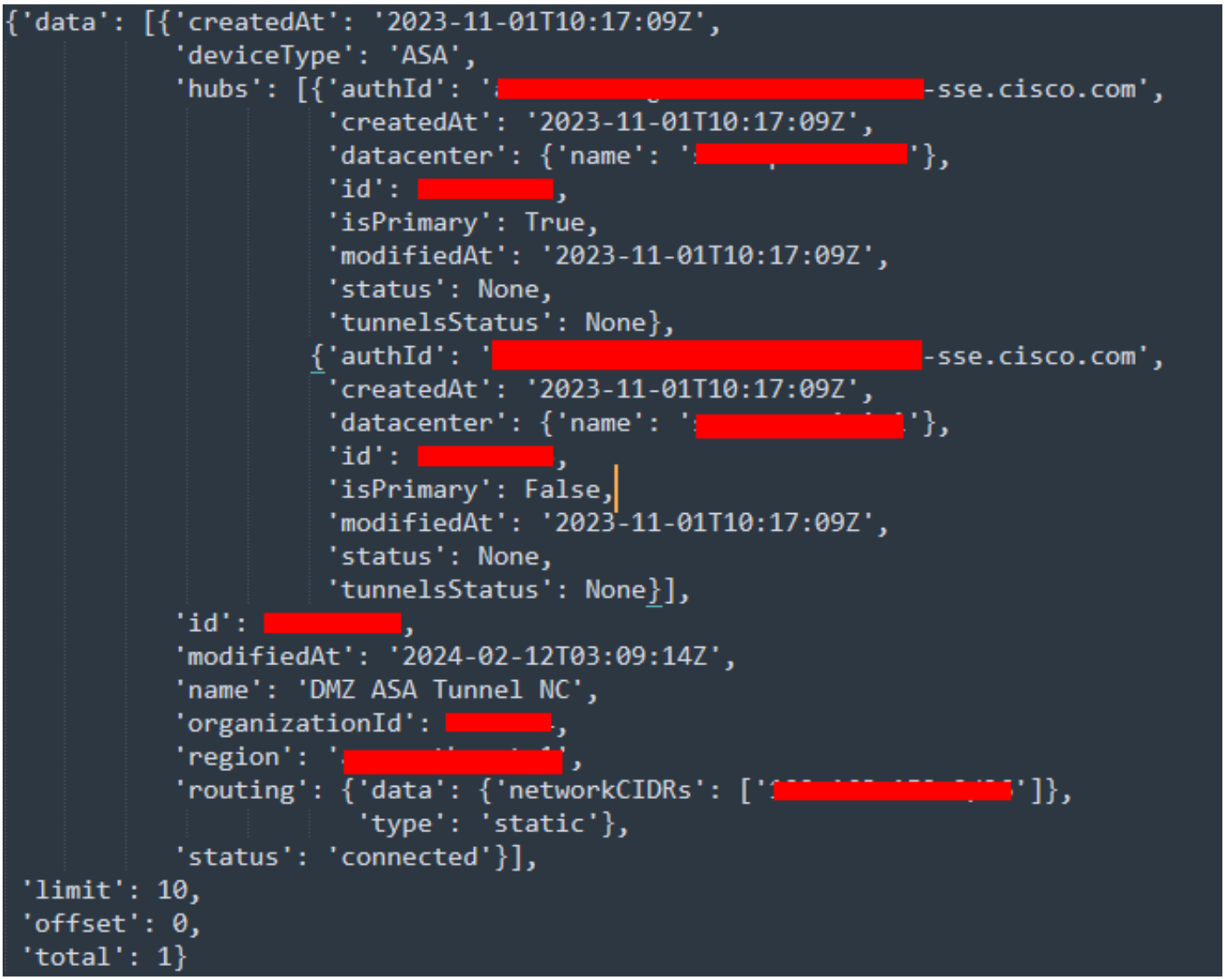
指令碼2：

然後，可以在此指令碼中使用Script 1中的access_token命令進行API呼叫。例如，使用指令碼2使用資源/deployments/v2/networktunnelgroups獲取有關網路隧道組的資訊：

```
import requests import pprint import json url = "https://api.sse.cisco.com/deployments/v2/networktunnel
```

輸出：

此指令碼的輸出必須類似於以下內容：



*Python*輸出-網路隧道組

您還可以透過安全訪問開發人員使用手冊獲取有關策略、漫遊電腦、報告等的資訊。

疑難排解

安全訪問API終端使用HTTP響應代碼表示API請求成功或失敗。一般而言，2xx範圍內的代碼表示成功，4xx範圍內的代碼表示由所提供資訊導致的錯誤，而5xx範圍內的代碼表示伺服器錯誤。解決問題的方法取決於收到的響應代碼：

200	**OK**	Success. Everything worked as expected.
201	**Created**	New resource created.
202	**Accepted**	Success. Action is queued.
204	**No Content**	Success. Response with no message body.
400	**Bad Request**	Likely missing a required parameter or malformed JSON. The syntax of your query may need to be revised. Check for any spaces preceding, trailing, or in the domain name of the domain you are trying to query.
401	**Unauthorized**	The authorization header is missing or the key and secret pair is invalid. Ensure your API token is valid.
403	**Forbidden**	The client is unauthorized to access the content.
404	**Not Found**	The requested resource doesn't exist. Check the syntax of your query or ensure the IP and domain are valid.
409	**Conflict**	The client requests that the server create the resource, but the resource already exists in the collection.
429	**Exceeded Limit**	Too many requests received in a given amount of time. You may have exceeded the rate limits for your organization or package.
413	**Content Too Large**	The request payload is larger than the limits defined by the server.

REST API -響應代碼1

500	**Internal Server Error**	Something wrong with the server.
503	**Service Unavailable**	Server is unable to complete request.

REST API -響應代碼2

相關資訊

- 思科安全訪問使用手冊
- Cisco技術支援和下載
- 增加安全訪問API金鑰
- 開發人員使用者指南

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）。