PythonでREST APIを使用するためのセキュアアクセスの設定

内容

はじめに

このドキュメントでは、APIアクセスを設定し、これを使用してセキュアアクセスからリソース情報を取得する手順について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

1. Python 3.x
2. REST API
3. シスコセキュアアクセス

要件

次に進む前に、次の要件を満たす必要があります。

- Full Adminuserロールを持つCisco Secure Accessユーザアカウント。
- セキュアアクセスにサインインするためのCisco Security Cloudシングルサインオン(SCSO)アカウント。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

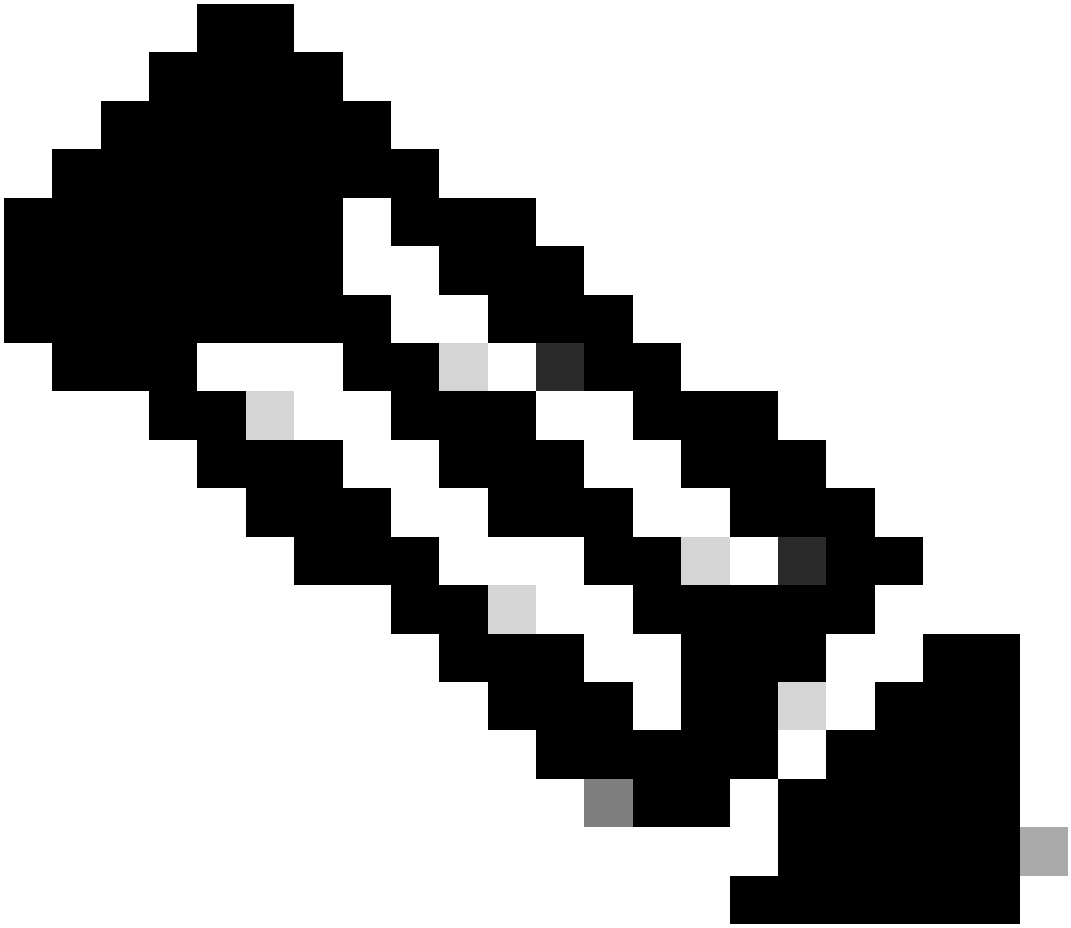
- セキュアアクセスダッシュボード

- Python

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

セキュアアクセスAPIは、標準のRESTインターフェイスを提供し、OAuth 2.0のクライアント資格情報フローをサポートします。開始するには、セキュアアクセスにサインインし、セキュアアクセスAPIキーを作成します。次に、APIクレデンシャルを使用してAPIアクセストークンを生成します。



注:APIキー、パスワード、シークレット、トークンを使用すると、プライベートデータにアクセスできます。他のユーザまたは組織と資格情報を共有することはできません。

この記事に記載されているスクリプトを実行する前に、セキュアアクセスダッシュボードからAPIキーを設定します。

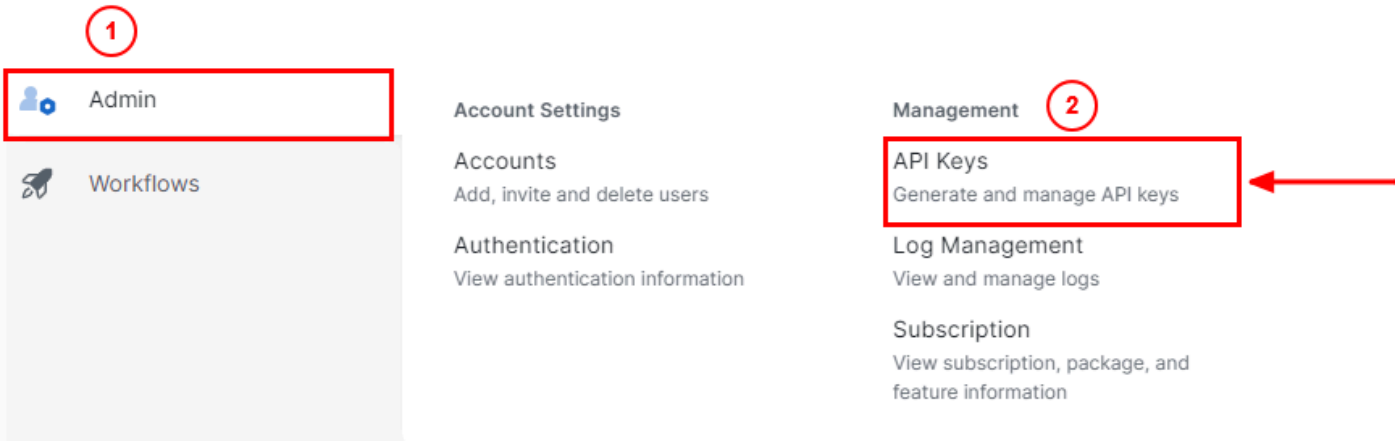
APIキーの作成

次の手順でAPIキーとシークレットを作成します。Secure AccessにURL:Secure Accessでサインインします。

1. 左側のサイドバーからAdminオプションを選択します。

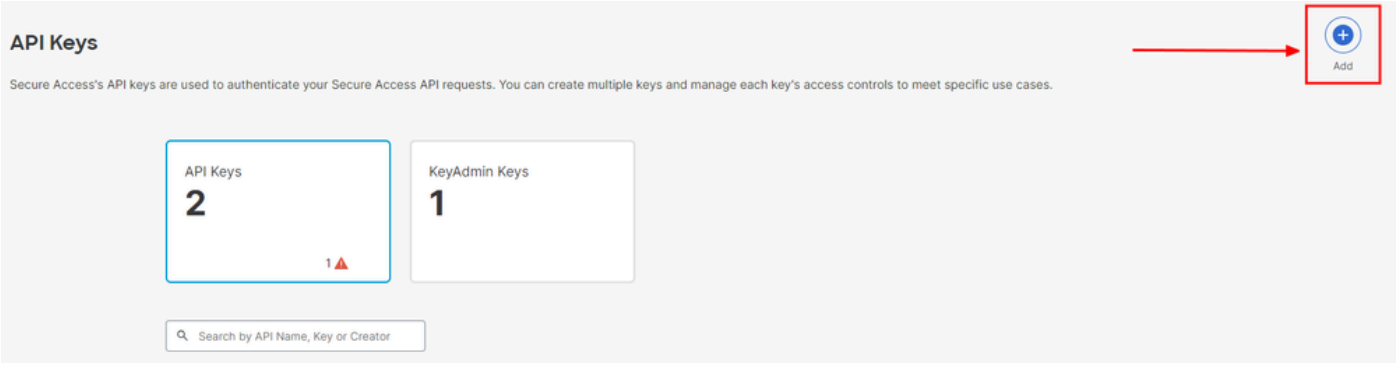
Admin

- でオプションを選択します。 **API Keys**:



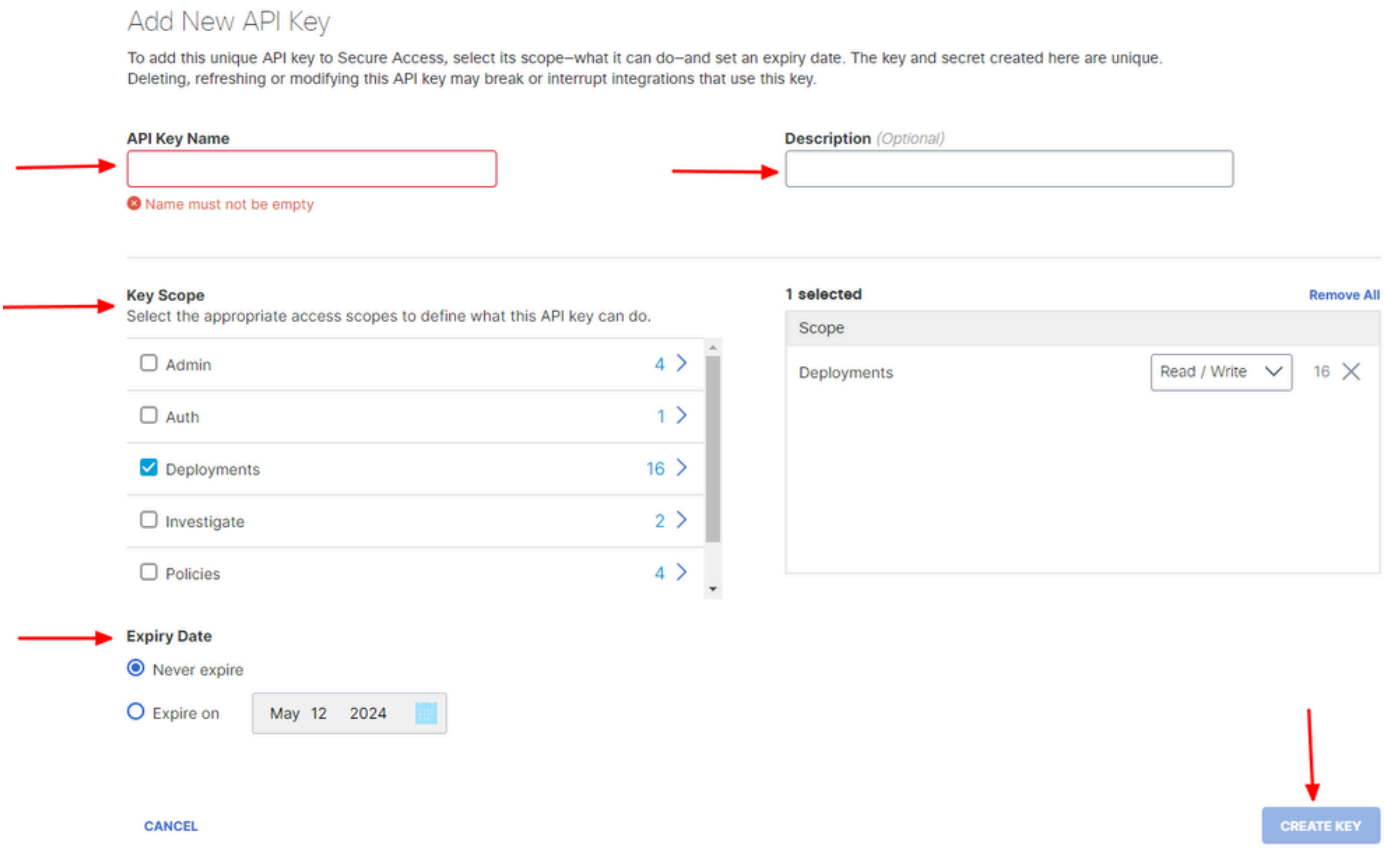
セキュアアクセスダッシュボードの管理者 – *API*キー

3. 右上隅の+ ボタンをクリックして、新しいAPIキーを追加します。



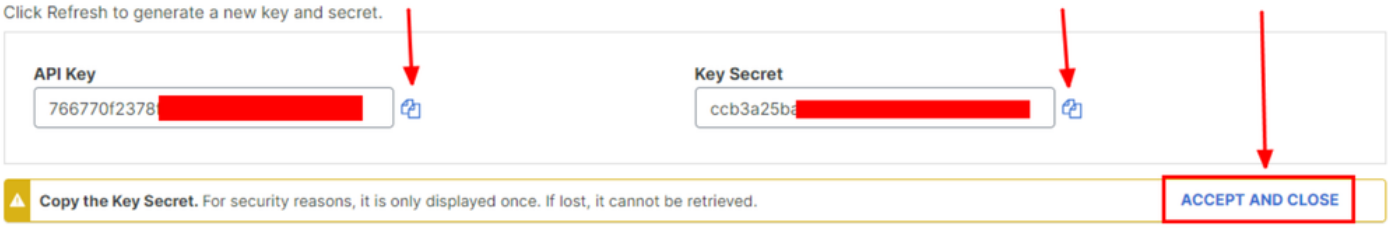
セキュアアクセス – *API*キーの追加

4. **API Key Name, Description**（オプション）を入力し、必要に応じてKey scopeとExpiry date を選択します。完了したら、**Create**のボタンをクリックします。

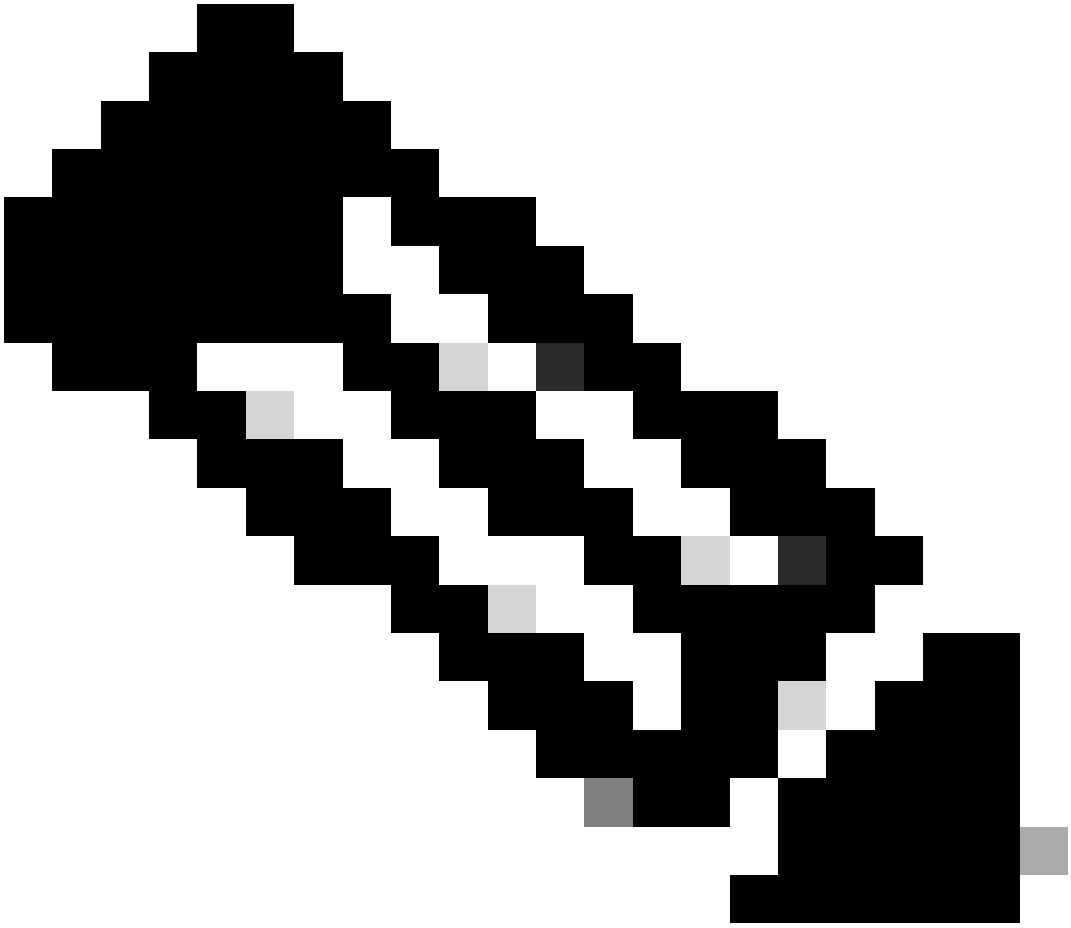


セキュアアクセス – *API*キーの詳細

5. API Keyと **Key Secret** をコピーし、ACCEPT AND CLOSE:をクリックします。



セキュアなアクセス：*API*キーとシークレット



注:APIシークレットをコピーする機会は1つだけです。Secure AccessはAPIシークレットを保存せず、最初の作成後は取得できません。

Pythonコード

生成されたトークンが3600秒（1時間）有効であることを考慮して、このコードを記述する方法は複数あります。最初のスクリプトを使用してBearer Tokenを生成し、次にBearer Tokenを使用して対象のリソースにAPIコール（フェッチ/更新または削除）を実行できる2つ目のスクリプトを作成するか、またはベアラトークンがすでに生成されている場合にスクリプトが実行されるたびに新しいベアラトークンが生成されないという条件をコードに記述して両方のアクションを実行します。

Pythonで動作させるには、以下のライブラリをインストールしてください。

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

スクリプト 1 :

このスクリプトで、client_idおよびclient_secretを正しく指定してください。

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

出力 :

このスクリプトの出力は次のようになります。

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

access_tokenは何千もの文字を扱うため非常に長いので、この例では出力を読みやすくするため、省略しています。

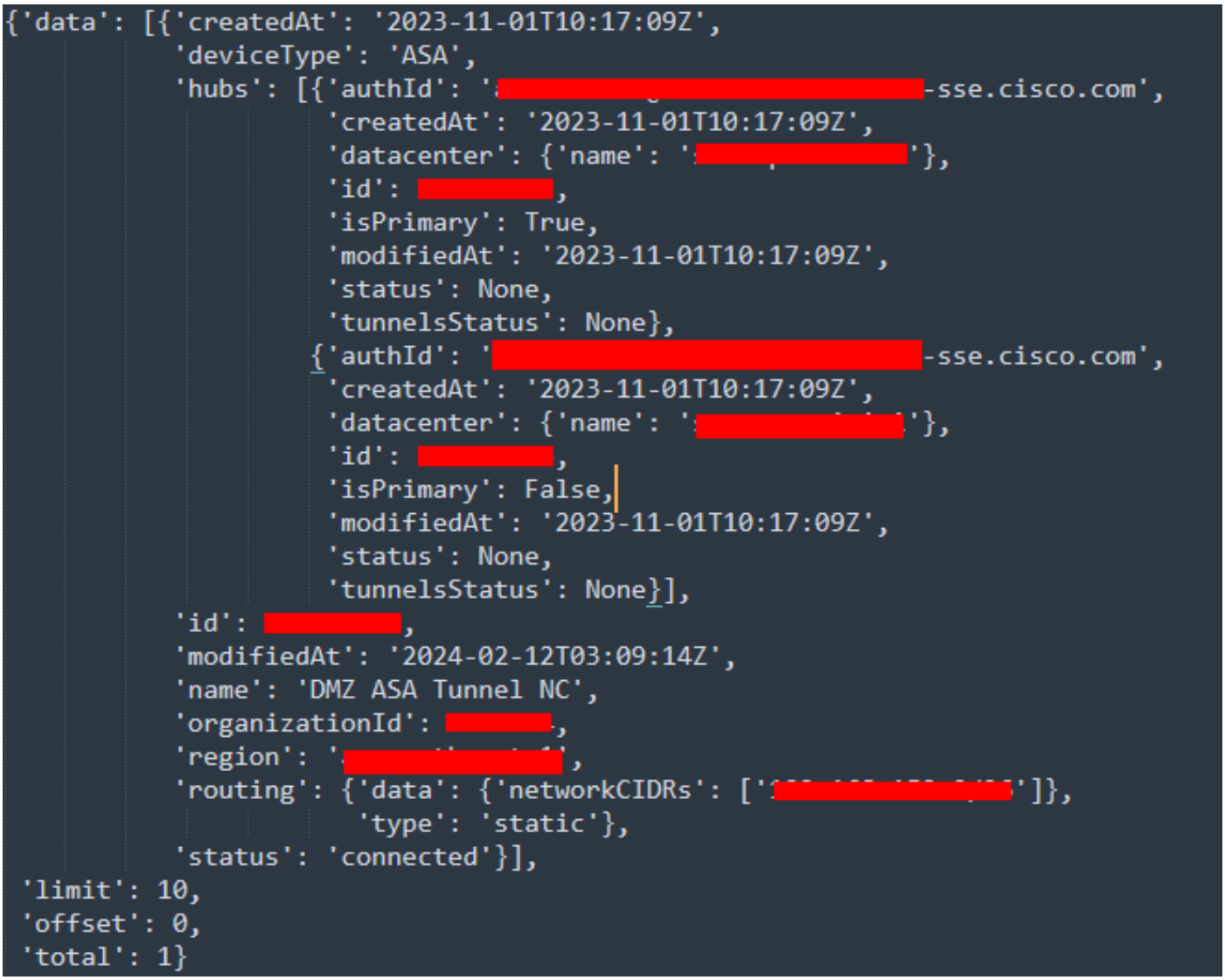
スクリプト 2 :

その後、このスクリプトでスクリプト1のaccess_tokenを使用してAPIを呼び出すことができます。たとえば、/deployments/v2/networktunnelgroupsというリソースを使用してネットワークトンネルグループに関する情報を取得するために、スクリプト2を使用します。

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

出力 :

このスクリプトの出力は次のようになります。



*Python*出力 – ネットワークトンネルグループ

また、『セキュアアクセス開発者ユーザガイド』を使用して、ポリシー、ローミングコンピュータ、レポートなどに関する情報を取得することもできます。

トラブルシュート

Secure Access APIエンドポイントは、HTTP応答コードを使用して、API要求の成功または失敗を示します。一般に、2xxの範囲のコードは成功を示し、4xxの範囲のコードは提供された情報に起因するエラーを示し、5xxの範囲のコードはサーバエラーを示します。問題を解決するアプローチは、受信した応答コードによって異なります。

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：応答コード1

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

REST API：応答コード2

関連情報

- Cisco Secure Accessユーザガイド
- シスコテクニカルサポートとダウンロード
- セキュアアクセスAPIキーの追加
- 開発者ユーザガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。