Ziellisten über Curl mit API für sicheren Zugriff verwalten

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Konfigurieren
  - 1.Erstellen Sie Ihren API-Schlüssel
  - 2.API-Zugriffstoken generieren
  - 3.Ziellisten verwalten
    - Alle Ziellisten abrufen
    - Abrufen aller Ziele in einer Zielliste
    - Erstellen einer neuen Zielliste
    - Hinzufügen von Zielen zu einer Zielliste
    - Löschen einer Zielliste
    - Ziele aus einer Zielliste löschen
- Fehlerbehebung
- Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Ziellisten mithilfe der API für sicheren Zugriff verwaltet werden.

Voraussetzungen

Anforderungen

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

- Sicherer Zugriff
- Sichere Zugriffs-API
- kräuseln
- Json

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Sicherer Zugriff
- APIs für sicheren Zugriff
- kräuseln
- Json

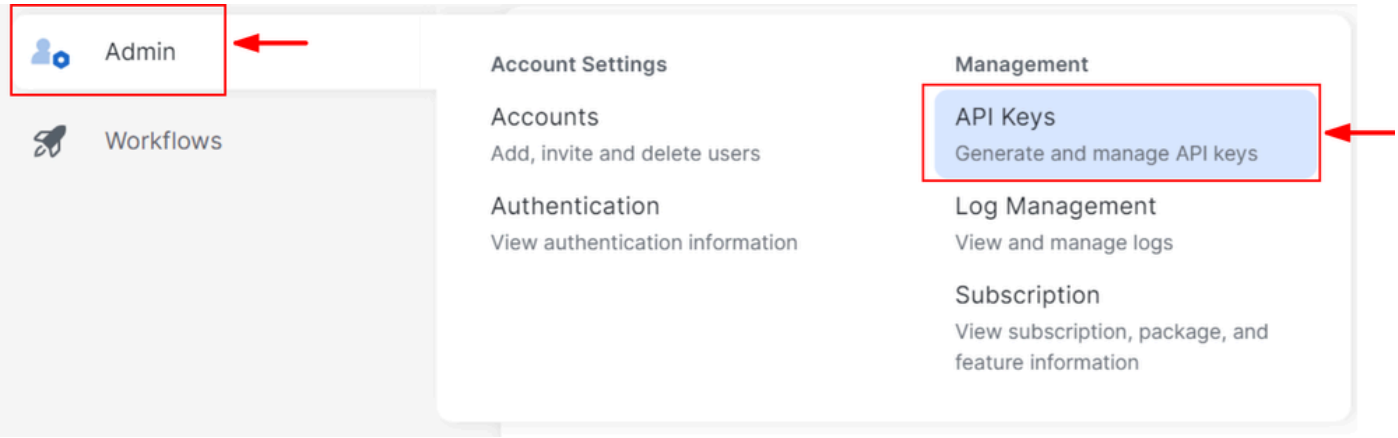
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfigurieren

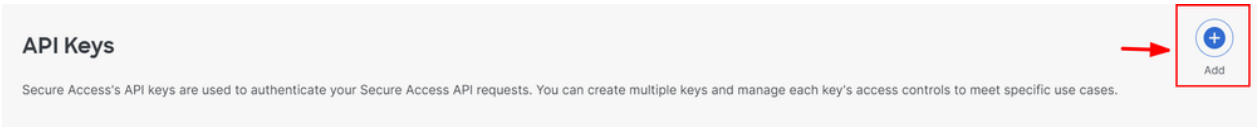
1.Erstellen Sie Ihren API-Schlüssel

Navigieren Sie zum [Dashboard für sicheren Zugriff.]

- Klicken Sie auf Admin > Api Keys > Add

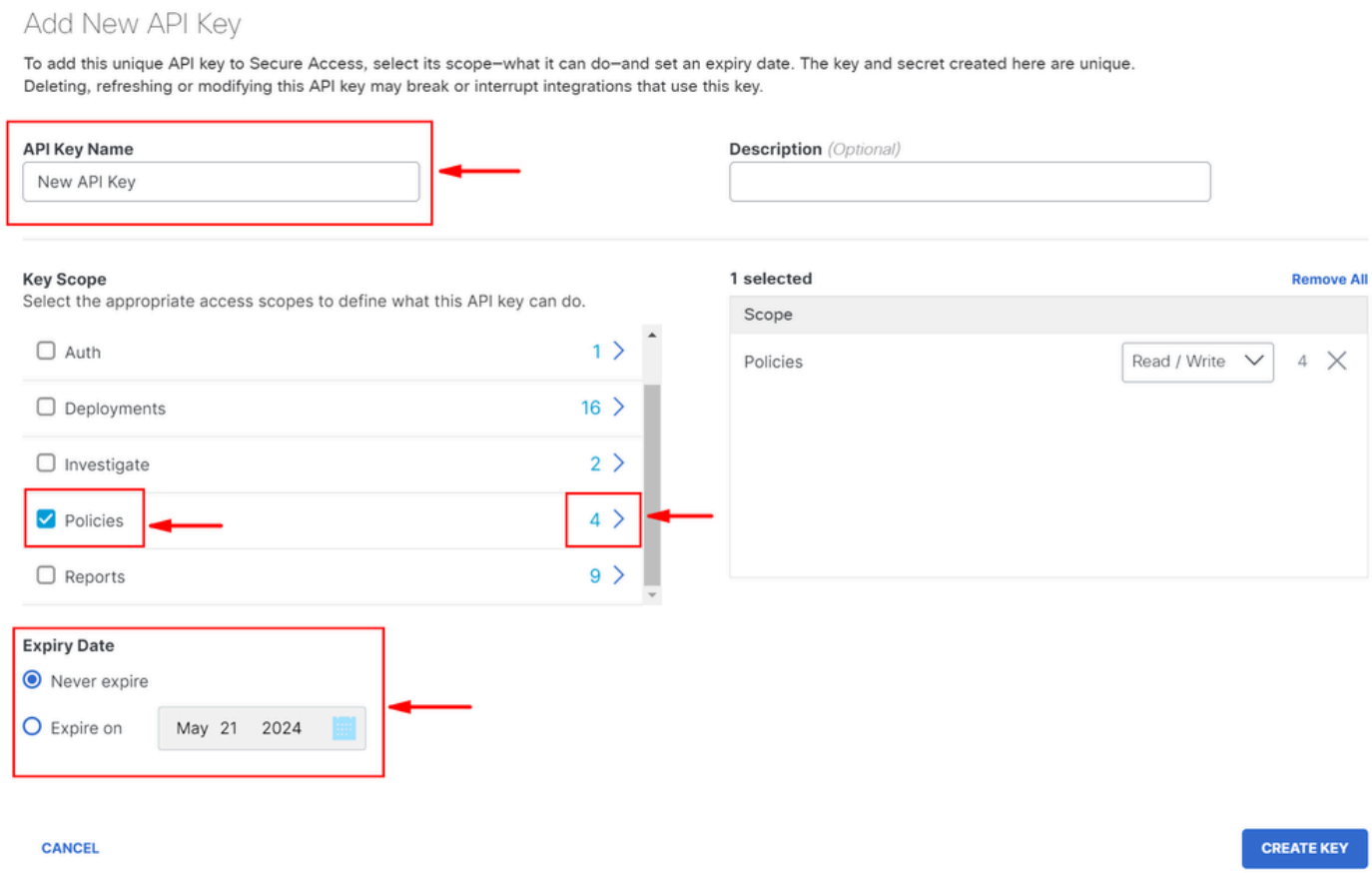


API-Schlüssel erstellen 1



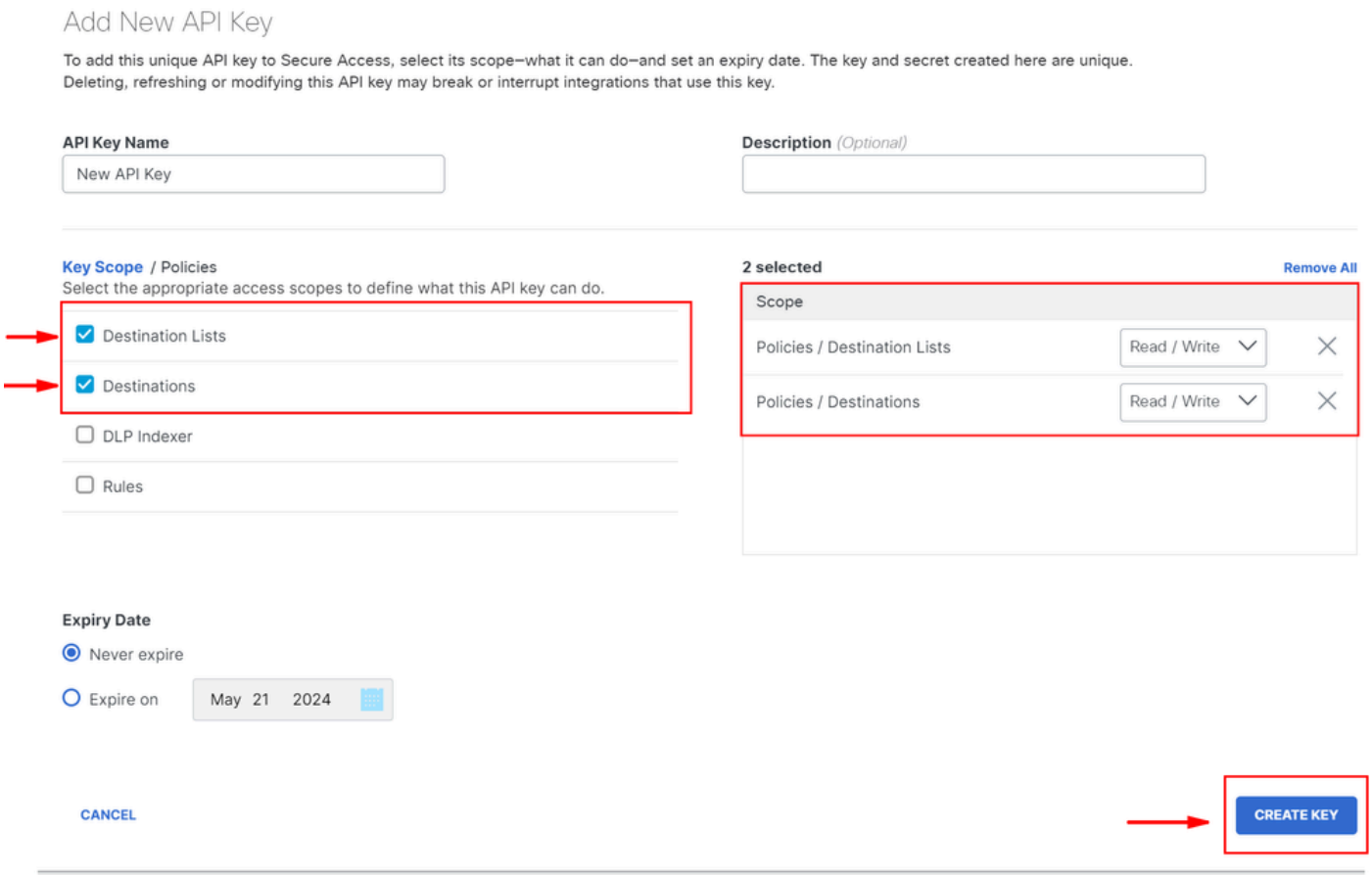
API-Schlüssel erstellen 2

- Fügen Sie die gewünschten API Key Name , Description (Optional) , nach BedarfExpiry Date hinzu.



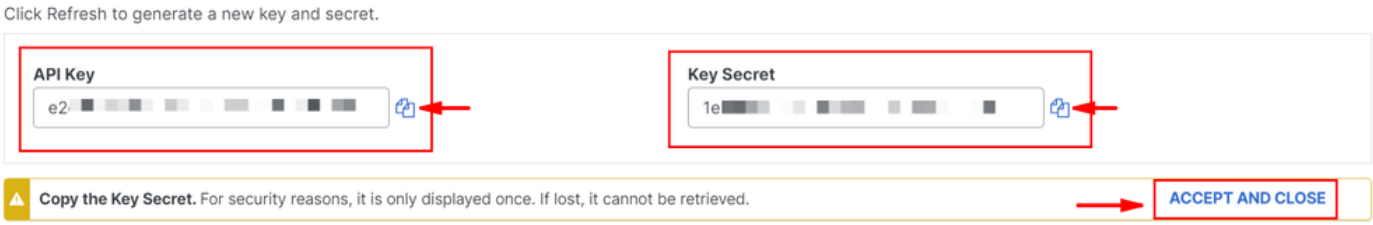
API-Schlüssel erstellen 3

- Wählen Key Scope Sie unter Richtlinien erweitern ausPolicies.
- Auswahl Destination Lists und Destinations
- Ändern Scope Sie diese nach Bedarf, andernfalls behalten Sie Read/Write
- Klicken Sie CREATE KEY

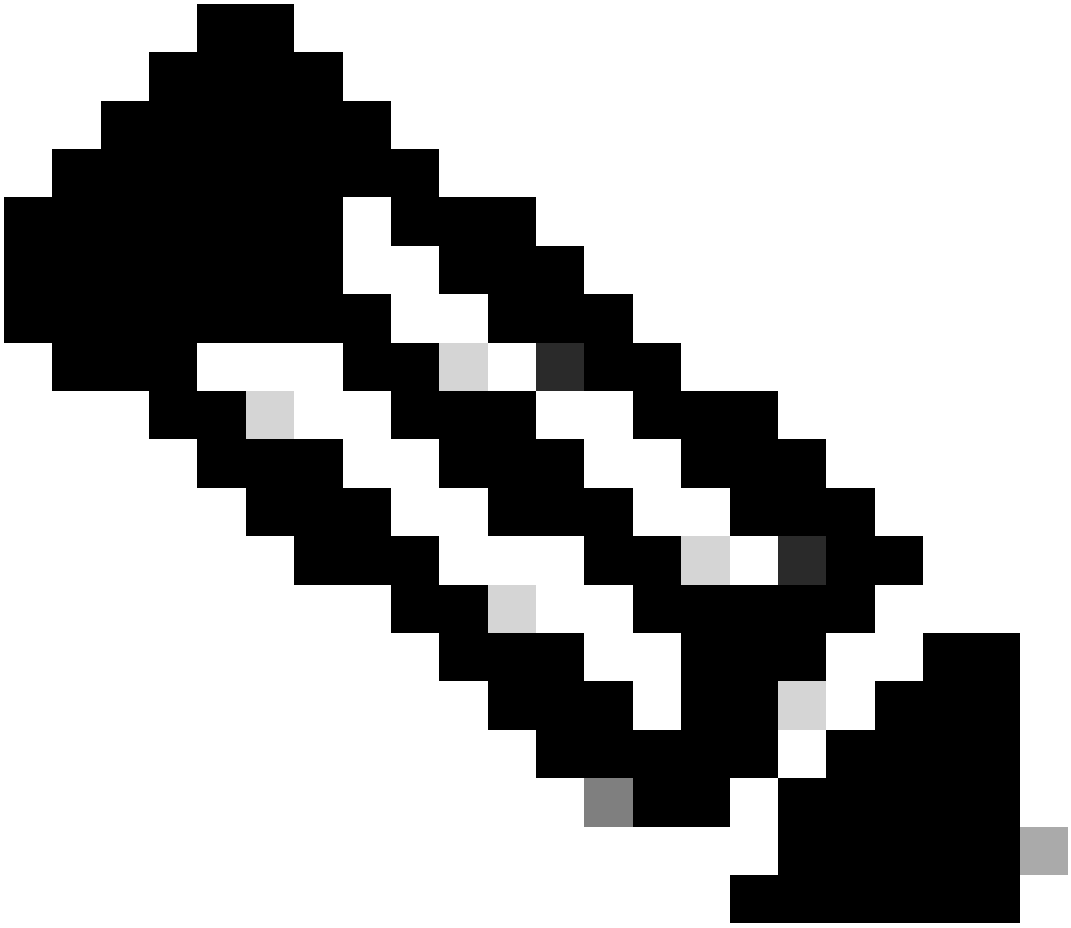


API-Schlüssel erstellen 4

- Kopieren Sie die API Keyund die **Key Secret** und klicken Sie dann auf ACCEPT AND CLOSE



API-Schlüssel erstellen 5



Hinweis: Es gibt nur eine Möglichkeit, Ihren API-Schlüssel zu kopieren. Secure Access speichert Ihren API-Schlüssel nicht, und Sie können ihn nach der ersten Erstellung nicht abrufen.

2.API-Zugriffstoken generieren

Um das API-Zugriffstoken zu generieren, stellen Sie eine Token-Autorisierungsanfrage:

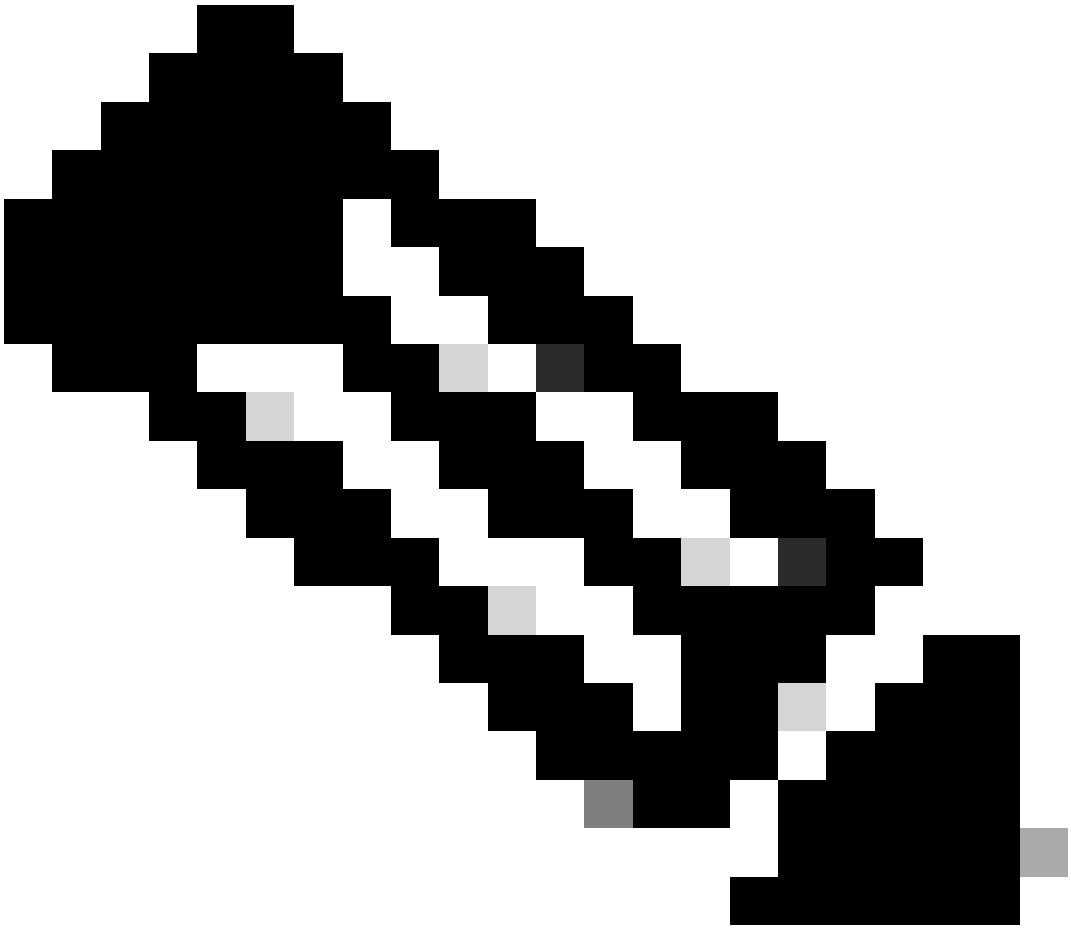
Anfrage für Tokenautorisierung

Verwenden Sie die API-Anmeldeinformationen für sicheren Zugriff, die Sie für Ihre Organisation erstellt haben, um ein API-Zugriffstoken zu generieren.

- Ersetzen Sie im curl-Beispiel den Schlüssel für die API für sicheren Zugriff durch einen geheimen Schlüssel.

```
curl --user key:secret --request POST --url https://api.sse.cisco.com/auth/v2/token -H Content-Type: ap
```

- Generiertes Träger-API-Token kopieren und speichern



Hinweis: Ein Secure Access OAuth 2.0-Zugriffstoken läuft in einer Stunde (3600 Sekunden) ab. Es wird empfohlen, ein Zugriffstoken erst zu aktualisieren, wenn das Token fast abgelaufen ist.

3.Ziellisten verwalten

Es gibt mehrere Möglichkeiten zur Verwaltung von Ziellisten:

Alle Ziellisten abrufen

Öffnen Sie die Windows-Eingabeaufforderung oder das Mac-Terminal, um den Befehl auszuführen:

```
curl -L --location-trusted --request GET --url https://api.sse.cisco.com/policies/v2/destinationlists -
```

Ausschnitt aus der Beispielausgabe:

```
{"id":23456789,"organizationId":1234567,"access":"none","isGlobal":false,"name":" Test Block list","thi
```

Notieren Sie sich die **destinationListId,** die im "**id**"-Feld der Ausgabe aufgeführt ist, die für GET-, POST- oder DELETE-Anforderungen speziell für diese Zielliste verwendet wird.

Abrufen aller Ziele in einer Zielliste

- Holen Sie sich die destinationListId mit diesem zuvor erwähnten Schritt, alle Ziellisten abrufen

Öffnen Sie die Windows-Eingabeaufforderung oder das Mac-Terminal, um den Befehl auszuführen:

```
curl -L --location-trusted --request GET --url https://api.sse.cisco.com/policies/v2/destinationlists/d
```

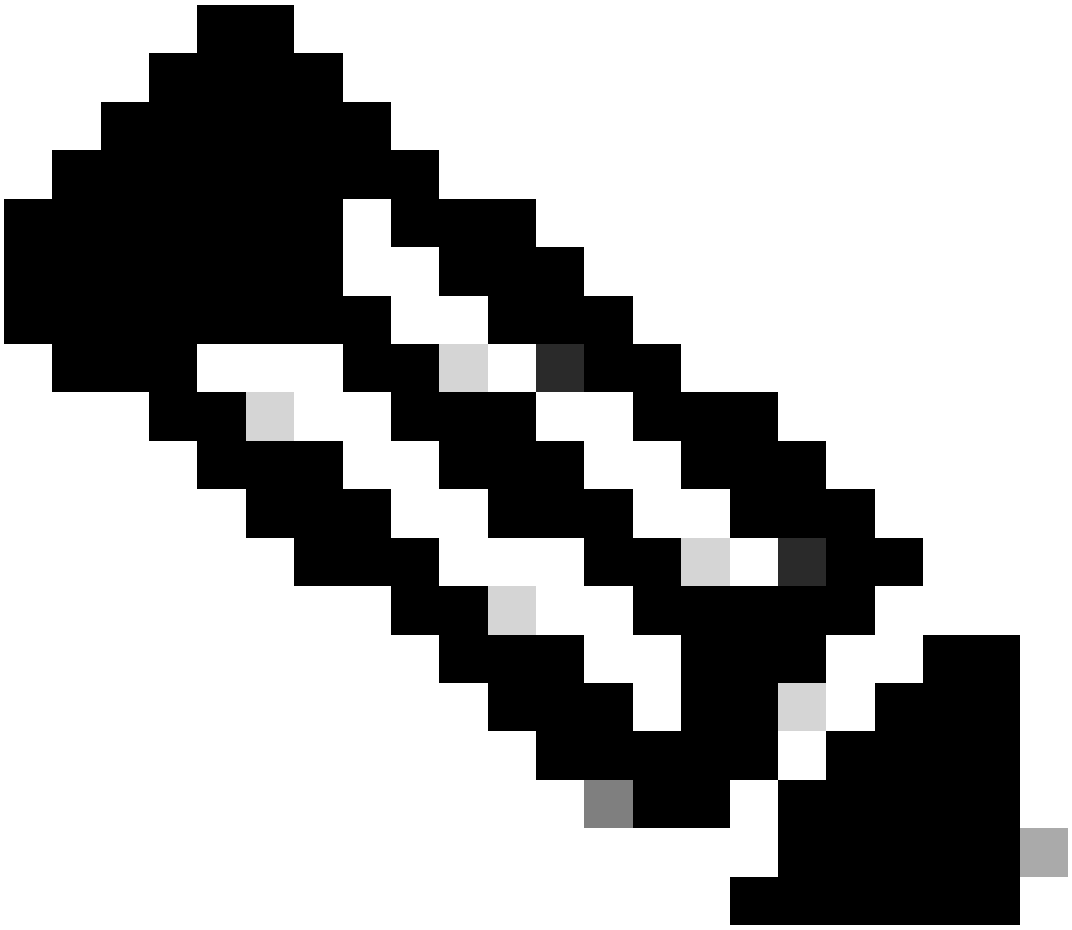
Beispiel für das Ergebnis:

```
{"status":{"code":200,"text":"OK"},"meta":{"page":1,"limit":100,"total":3},"data": [ {"id":"415214","de
```

Erstellen einer neuen Zielliste

Öffnen Sie die Windows-Eingabeaufforderung oder das Mac-Terminal, um den Befehl auszuführen:

```
curl -L --location-trusted --request POST --url https://api.sse.cisco.com/policies/v2/destinationlists
```



Hinweis: Ersetzen Sie 'Name der Zielliste' durch den gewünschten Namen.

Beispiel für das Ergebnis:

```
{"id":23456789,"organizationId":1234567,"access":"none","isGlobal":false,"name":"API List 1","thirdpart
```

Hinzufügen von Zielen zu einer Zielliste

- Holen Sie sich die destinationListId mit diesem zuvor erwähnten Schritt, alle Ziellisten abrufen

Öffnen Sie die Windows-Eingabeaufforderung oder das Mac-Terminal, um den Befehl auszuführen:

```
curl -L --location-trusted --request POST --url https://api.sse.cisco.com/policies/v2/destinationlists/
```

Beispiel für das Ergebnis:


```
{"status":{"code":200,"text":"OK"},"data":{"id":17804929,"organizationId":1234567,"access":"none","isGl
```


Löschen einer Zielliste

- Holen Sie sich die destinationListId mit diesem zuvor erwähnten Schritt, alle Ziellisten abrufen

Öffnen Sie die Windows-Eingabeaufforderung oder das Mac-Terminal, um den Befehl auszuführen:

```
curl -L --location-trusted --request DELETE --url https://api.sse.cisco.com/policies/v2/destinationlist
```

Beispiel für das Ergebnis:


```
{"status":{"code":200,"text":"OK"},"data":[]}
```


Ziele aus einer Zielliste löschen

- Holen Sie sich die destinationListId mit diesem zuvor erwähnten Schritt, alle Ziellisten abrufen
- Abrufen **id** des Ziels in der Liste, das mit diesem zuvor genannten Schritt gelöscht werden muss, Abrufen aller Ziele in einer Zielliste

Öffnen Sie die Windows-Eingabeaufforderung oder das Mac-Terminal, um den Befehl auszuführen:

```
curl -L --location-trusted --request DELETE --url https://api.sse.cisco.com/policies/v2/destinationlist
```

Beispiel für das Ergebnis:


```
{"status":{"code":200,"text":"OK"},"data":{"id":17804929,"organizationId":1234567,"access":"none","isGl
```


Fehlerbehebung

Die Endpunkte der API für sicheren Zugriff verwenden HTTP-Antwortcodes, um den Erfolg oder Misserfolg einer API-Anforderung anzuzeigen. Im Allgemeinen weisen Codes im 2xx-Bereich auf Erfolg hin, Codes im 4xx-Bereich auf einen Fehler hin, der sich aus den bereitgestellten Informationen ergibt, und Codes im 5xx-Bereich auf Serverfehler. Der Ansatz zur Behebung des Problems hängt vom empfangenen Antwortcode ab:

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 - Antwortcodes 1

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

REST-API - Antwortcodes 2

Zusätzlich zur Fehlerbehebung von API-bezogenen Fehlern oder Problemen sind hier die Ratenlimitierungen zu beachten:

- API-Beschränkungen für sicheren Zugriff

Zugehörige Informationen

- Cisco Secure Access Benutzerhandbuch
- Technischer Support und Downloads von Cisco

    - Hinzufügen von API-Schlüsseln für sicheren Zugriff

- Entwickler-Benutzerhandbuch

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.