

Gestione degli elenchi di destinazione tramite Curl con l'API Secure Access

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[1. Creare la chiave API](#)

[2. Generare un token di accesso API](#)

[3. Gestisci elenchi destinazioni](#)

[Ottieni tutti gli elenchi di destinazione](#)

[Ottenere tutte le destinazioni all'interno di un elenco destinazioni](#)

[Crea un nuovo elenco destinazioni](#)

[Aggiungere destinazioni a un elenco destinazioni](#)

[Eliminare un elenco di destinazione](#)

[Eliminare le destinazioni da un elenco destinazioni](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come gestire gli elenchi di destinazione tramite curl con Secure Access API.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso sicuro
- API Secure Access
- ricciolo
- Json

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Accesso sicuro
- API Secure Access
- ricciolo
- Json

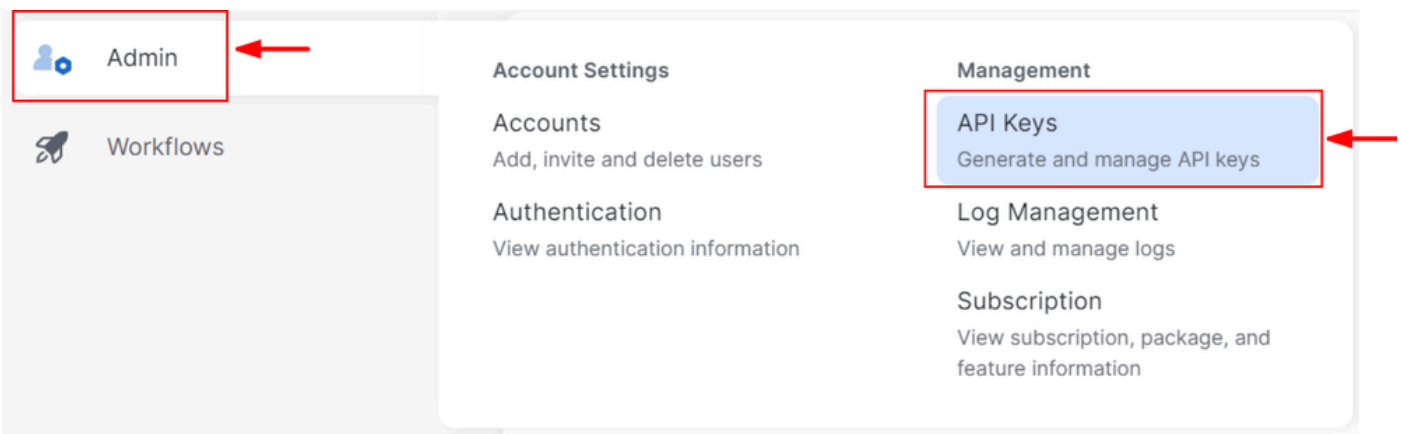
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

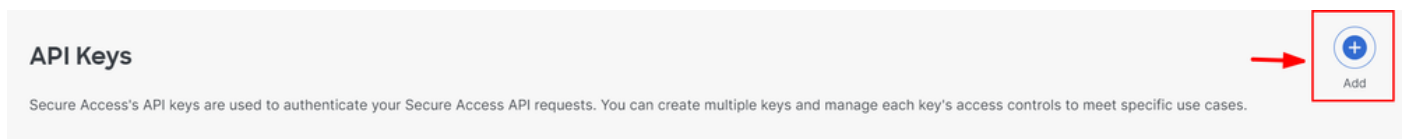
1. Creare la chiave API

Passare a [Dashboard di accesso protetto](#).

- Fare clic su Admin > Api Keys > Add



Creare la chiave API 1



Creare la chiave API 2

- Aggiungere API Key Name , Description (Optional) desiderato Expiry Date, se necessario

Add New API Key

To add this unique API key to Secure Access, select its scope—what it can do—and set an expiry date. The key and secret created here are unique. Deleting, refreshing or modifying this API key may break or interrupt integrations that use this key.

The screenshot shows the 'Add New API Key' form with several fields highlighted by red boxes and arrows:

- API Key Name:** A text input field containing 'New API Key'.
- Description (Optional):** An empty text input field.
- Key Scope:** A list of scopes with checkboxes and expandable options (indicated by blue chevrons):
 - Auth (1 >)
 - Deployments (16 >)
 - Investigate (2 >)
 - Policies (4 >)** - This row is highlighted with a red box, and a red arrow points to the '4 >' chevron.
 - Reports (9 >)
- Expiry Date:** A section with two radio buttons:
 - Never expire** (selected)
 - Expire on: May 21 2024 (with a calendar icon)
- Scope Selection Panel:** A panel titled '1 selected' with a 'Remove All' link. It shows a 'Scope' dropdown set to 'Policies' and a 'Read / Write' dropdown with a '4 X' indicator.
- Buttons:** 'CANCEL' and 'CREATE KEY' buttons.

Creare la chiave API 3

- In Key Scope, scegliere Policies quindi Espandi criteri
- Scegli Destination Lists e Destinations
- Modificare Scope se necessario, altrimenti conservare come Read/Write
- Fare clic su CREATE KEY

Add New API Key

To add this unique API key to Secure Access, select its scope—what it can do—and set an expiry date. The key and secret created here are unique. Deleting, refreshing or modifying this API key may break or interrupt integrations that use this key.

API Key Name

Description *(Optional)*

Key Scope / Policies

Select the appropriate access scopes to define what this API key can do.

 Destination Lists Destinations DLP Indexer Rules

2 selected

[Remove All](#)

Scope

Policies / Destination Lists

Read / Write



Policies / Destinations

Read / Write



Expiry Date

 Never expire Expire on

May 21 2024

[CANCEL](#)[CREATE KEY](#)

Creare la chiave API 4

- Copiare API Key **Key Secret** e quindi fare clic su ACCEPT AND CLOSE

Click Refresh to generate a new key and secret.

API Key

e2. [obscured]



Key Secret

1e [obscured]



Copy the Key Secret. For security reasons, it is only displayed once. If lost, it cannot be retrieved.

[ACCEPT AND CLOSE](#)

Creare la chiave API 5



Nota: esiste solo un'opportunità per copiare il segreto API. Secure Access non salva il segreto API e non è possibile recuperarlo dopo la creazione iniziale.

2. Generare un token di accesso API

Per generare il token di accesso API, creare una richiesta di autorizzazione token:

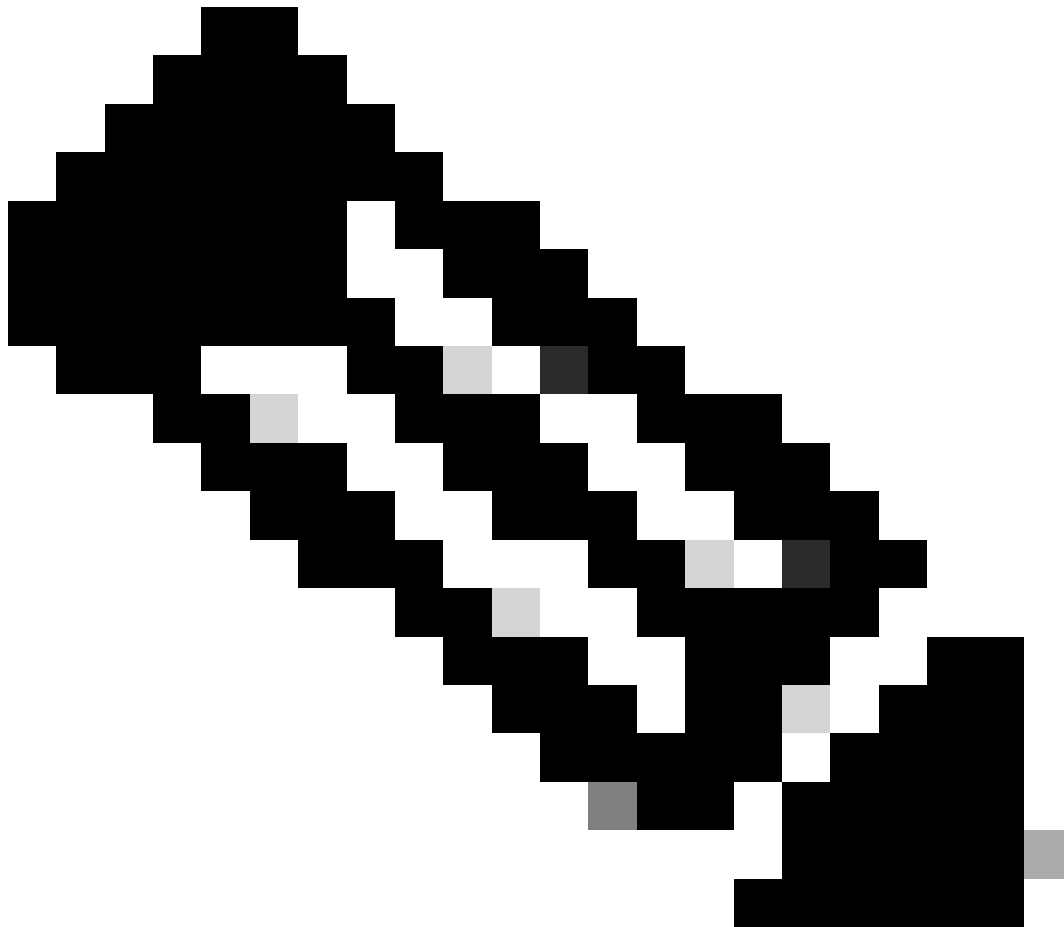
Richiesta di autorizzazione token

Utilizzare le credenziali dell'API Secure Access create per l'organizzazione per generare un token di accesso API.

- Nell'esempio di riciclo, sostituire la chiave e il segreto dell'API Secure Access

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

- Copiare e salvare il token Bearer API generato



Nota: un token di accesso Secure Access OAuth 2.0 scade tra un'ora (3600 secondi). È consigliabile non aggiornare un token di accesso fino a quando il token è quasi scaduto.

3. Gestisci elenchi destinazioni

Gli elenchi di destinazione possono essere gestiti in diversi modi, ad esempio:

Ottieni tutti gli elenchi di destinazione

Aprire il prompt dei comandi di Windows o il terminale Mac per eseguire il comando:

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

Frammento di codice da output di esempio:

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

Prendere nota dell'elemento **destinationListId** elencato nel campo **"id"** dell'output che viene utilizzato ulteriormente per le richieste GET, POST o DELETE specifiche di questo elenco di destinazione.

Ottenere tutte le destinazioni all'interno di un elenco destinazioni

- Ottieni il destinationListId utilizzando questo passaggio della citazione precedente, [Ottieni tutti gli elenchi di destinazione](#)

Aprire il prompt dei comandi di Windows o il terminale Mac per eseguire il comando:

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

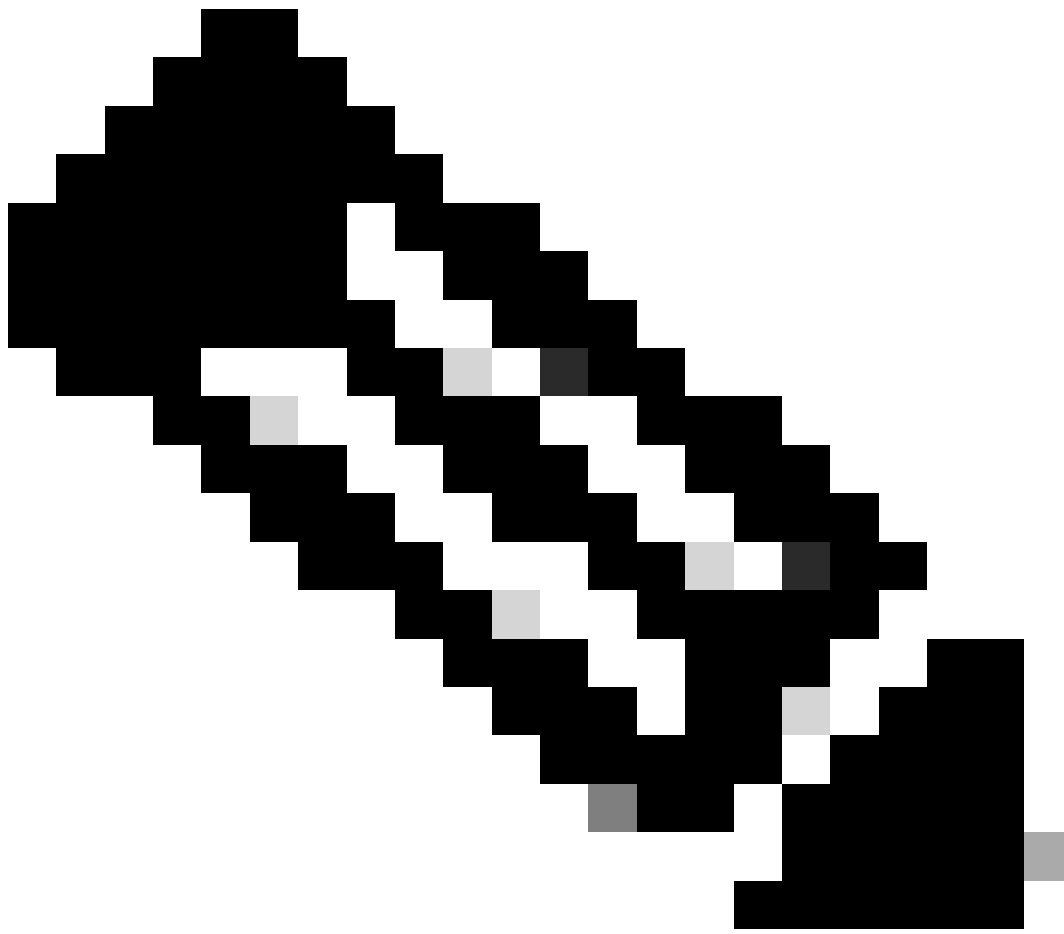
Output di esempio:

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

Crea un nuovo elenco destinazioni

Aprire il prompt dei comandi di Windows o il terminale Mac per eseguire il comando:

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



Nota: sostituire 'Nome elenco di destinazione' con il nome desiderato.

Output di esempio:

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

Aggiungere destinazioni a un elenco destinazioni

- Ottieni il destinationListId utilizzando questo passaggio della citazione precedente, [Ottieni tutti gli elenchi di destinazione](#)

Aprire il prompt dei comandi di Windows o il terminale Mac per eseguire il comando:

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

Output di esempio:

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

Eliminare un elenco di destinazione

- Ottieni il destinationListId utilizzando questo passaggio della citazione precedente, [Ottieni tutti gli elenchi di destinazione](#)

Aprire il prompt dei comandi di Windows o il terminale Mac per eseguire il comando:

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

Output di esempio:

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

Eliminare le destinazioni da un elenco destinazioni

- Ottieni il destinationListId utilizzando questo passaggio della citazione precedente, [Ottieni tutti gli elenchi di destinazione](#)
- Ottenere il nome **id** della destinazione specifica all'interno dell'elenco che deve essere eliminato utilizzando questo passaggio precedente, [Ottenerne tutte le destinazioni all'interno di un elenco di destinazione](#)

Aprire il prompt dei comandi di Windows o il terminale Mac per eseguire il comando:

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

Output di esempio:

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

Risoluzione dei problemi

Gli endpoint API di accesso sicuro utilizzano i codici di risposta HTTP per indicare l'esito positivo o negativo di una richiesta API. In generale, i codici nell'intervallo 2xx indicano un esito positivo, i codici nell'intervallo 4xx indicano un errore risultante dalle informazioni fornite e i codici nell'intervallo 5xx indicano errori del server. L'approccio per risolvere il problema dipende dal codice di risposta ricevuto:

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.

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

API REST - Codici di risposta 2

Inoltre, durante la risoluzione dei problemi relativi agli errori o ai problemi dell'API, è necessario conoscere i seguenti limiti di velocità:

- [Limiti dell'API Secure Access](#)

Informazioni correlate

- [Guida per l'utente di Cisco Secure Access](#)
- [Supporto tecnico Cisco e download](#)
- [Aggiungi chiavi API di accesso sicuro](#)
- [Guida per l'utente per gli sviluppatori](#)

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).