

Administración de listas de destino mediante Curl con API de acceso seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[1.Cree su clave de API](#)

[2.Generar un token de acceso API](#)

[3.Gestionar listas de destino](#)

[Obtener todas las listas de destino](#)

[Obtener todos los destinos de una lista de destinos](#)

[Crear una nueva lista de destino](#)

[Agregar destinos a una lista de destinos](#)

[Eliminar una lista de destino](#)

[Eliminar destinos de una lista de destino](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo administrar las listas de destino mediante curl con la API de Secure Access.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro
- API de acceso seguro
- rizar
- Json

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Acceso seguro
- API de acceso seguro
- rizar
- Json

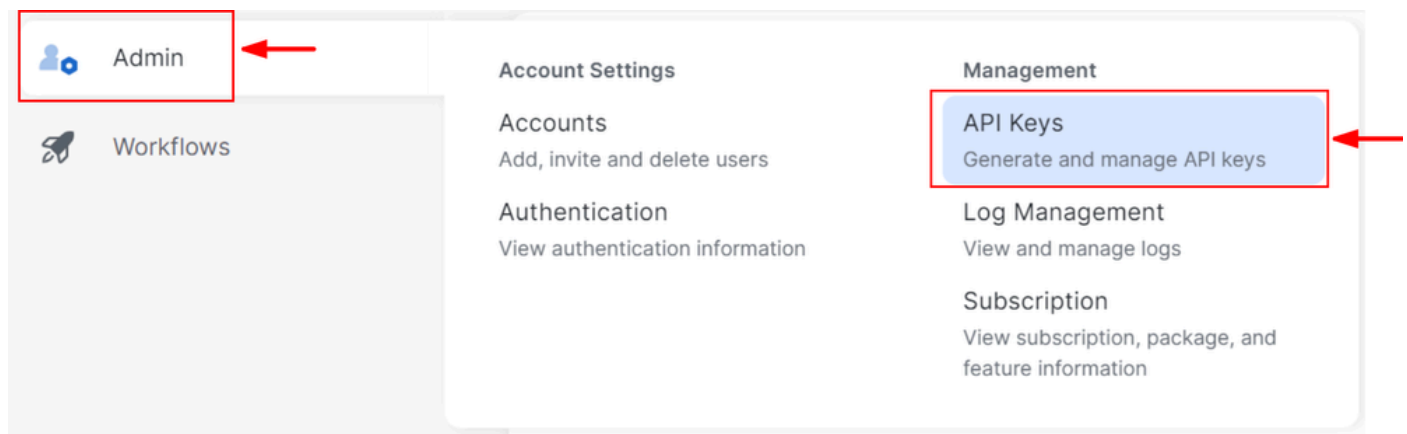
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

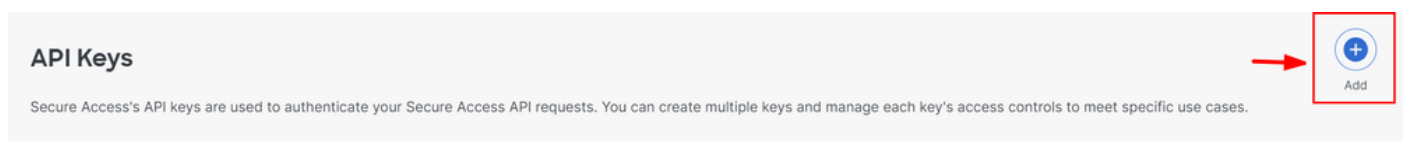
1. Cree su clave de API

Vaya a [Panel de acceso seguro](#).

- Haga clic en Admin > Api Keys > Add



Cree su API Key 1



Cree su API Key 2

- Añada los API Key Name , Description (Optional) , Expiry Date que desee según sea necesario

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. At the top, there is a text input for 'API Key Name' containing 'New API Key' and an optional 'Description' field. Below this is the 'Key Scope' section, which includes a list of scopes: Auth (1), Deployments (16), Investigate (2), Policies (4), and Reports (9). The 'Policies' scope is selected with a checkmark. To the right of the 'Policies' scope is a 'Scope' panel showing '1 selected' and 'Remove All'. The 'Scope' panel contains a dropdown menu set to 'Read / Write' and a count of '4'. At the bottom left, there is an 'Expiry Date' section with two options: 'Never expire' (selected) and 'Expire on' (with a date picker set to 'May 21 2024'). At the bottom right, there is a blue 'CREATE KEY' button and a 'CANCEL' link on the left.

Cree su clave de API 3

- En Key Scope, seleccione Políticas Expandir directivas
- Elija Destination Lists y Destinations
- Cambie Scope si es necesario; de lo contrario, siga el Read/Write
- Haga clic en 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
New API Key

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	Read / Write	
Policies / Destination Lists	Read / Write	×
Policies / Destinations	Read / Write	×

Expiry Date

Never expire

Expire on May 21 2024

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

Creación de la clave de API 4

- Copie el API Key el **Key Secret** y haga clic en **ACCEPT AND CLOSE**

Click Refresh to generate a new key and secret.

API Key
e2... [Copy]

Key Secret
1e... [Copy]

Copy the Key Secret. For security reasons, it is only displayed once. If lost, it cannot be retrieved. [ACCEPT AND CLOSE](#)

Creación de la clave de API 5



Nota: solo existe una oportunidad para copiar el secreto de la API. Secure Access no guarda el secreto de la API y no puede recuperarlo después de su creación inicial.

2. Generar un token de acceso API

Para generar el token de acceso API, realice una solicitud de autorización de token:

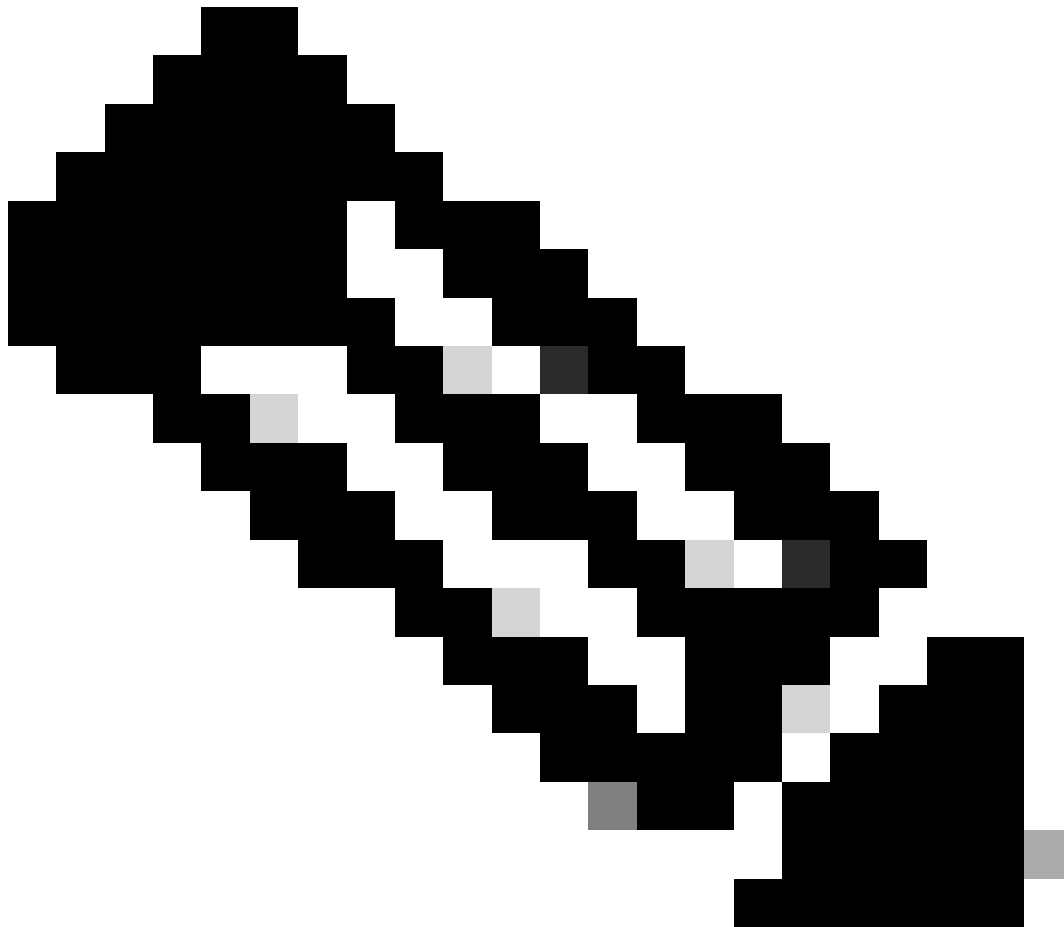
Solicitud de autorización de token

Utilice las credenciales de la API de acceso seguro que ha creado para su organización para generar un token de acceso a la API.

- En el ejemplo de rizo, sustituya su clave API Secure Access y secret

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

- Copie y guarde el token de la API portadora generado



Nota: Un token de acceso de OAuth 2.0 de Secure Access caduca en una hora (3600 segundos). Se recomienda no actualizar un token de acceso hasta que el token esté a punto de caducar.

3. Gestionar listas de destino

Existen varias formas de administrar listas de destinos, entre las que se incluyen:

Obtener todas las listas de destino

Abra el símbolo del sistema de Windows o el terminal Mac para ejecutar el comando:

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

Fragmento de salida de ejemplo:

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

Anote el **destinationListId** que aparece en el campo "id" del resultado, que se utiliza más adelante para las solicitudes GET, POST o DELETE específicas de esta lista de destino.

Obtener todos los destinos de una lista de destinos

- Obtenga el destinationListId uso de este paso de mención anterior, [Obtener todas las listas de destino](#)

Abra el símbolo del sistema de Windows o el terminal Mac para ejecutar el comando:

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

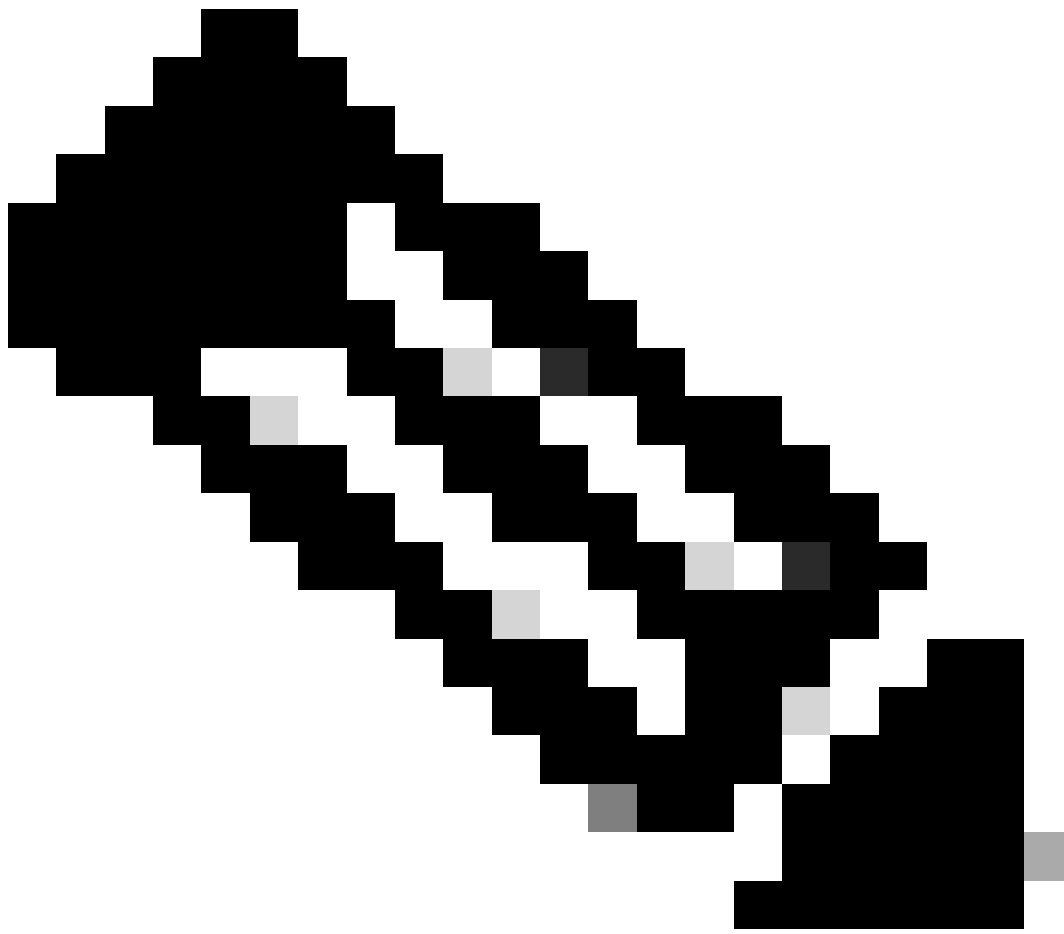
Ejemplo de Salida:

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

Crear una nueva lista de destino

Abra el símbolo del sistema de Windows o el terminal Mac para ejecutar el comando:

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



Nota: sustituya "Nombre de la lista de destino" por el nombre que desee.

Ejemplo de Salida:

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

Agregar destinos a una lista de destinos

- Obtenga el destinationListId uso de este paso de mención anterior, [Obtener todas las listas de destino](#)

Abra el símbolo del sistema de Windows o el terminal Mac para ejecutar el comando:

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

Ejemplo de Salida:

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

Eliminar una lista de destino

- Obtenga el destinationListId uso de este paso de mención anterior, [Obtener todas las listas de destino](#)

Abra el símbolo del sistema de Windows o el terminal Mac para ejecutar el comando:

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

Ejemplo de Salida:

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

Eliminar destinos de una lista de destino

- Obtenga el destinationListId uso de este paso de mención anterior, [Obtener todas las listas de destino](#)
- Obtenga la información **id** del destino específico dentro de la lista que debe eliminarse usando este paso mencionado anteriormente, [Obtenga todos los destinos dentro de una lista de destinos](#)

Abra el símbolo del sistema de Windows o el terminal Mac para ejecutar el comando:

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

Ejemplo de Salida:

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

Troubleshoot

Los terminales de la API de acceso seguro utilizan códigos de respuesta HTTP para indicar el éxito o el fracaso de una solicitud de la API. En general, los códigos de la gama 2xx indican éxito, los códigos de la gama 4xx indican un error derivado de la información proporcionada y los códigos de la gama 5xx indican errores del servidor. El enfoque para resolver el problema dependería del código de respuesta que se reciba:

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 - Códigos de respuesta 2

Además, mientras se solucionan los errores o problemas relacionados con API, aquí están los límites de velocidad que deben tenerse en cuenta:

- [Límites de API de acceso seguro](#)

Información Relacionada

- [Guía del usuario de Cisco Secure Access](#)
- [Soporte técnico y descargas de Cisco](#)
- [Agregar claves API de acceso seguro](#)
- [Guía del usuario para desarrolladores](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).