

Gerenciar Listas de Destinos via Curl com API de Acesso Seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[1.Crie sua chave de API](#)

[2. Gerar um token de acesso à API](#)

[3.Gerenciar listas de destinos](#)

[Obter todas as listas de destino](#)

[Obter todos os destinos em uma lista de destinos](#)

[Criar uma nova lista de destinos](#)

[Adicionar destinos a uma lista de destinos](#)

[Excluir uma lista de destinos](#)

[Excluir destinos de uma lista de destinos](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como gerenciar listas de destino via curl com a API de Acesso Seguro.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro
- API de acesso seguro
- curva
- Json

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Acesso seguro
- APIs de acesso seguro

- curva
- Json

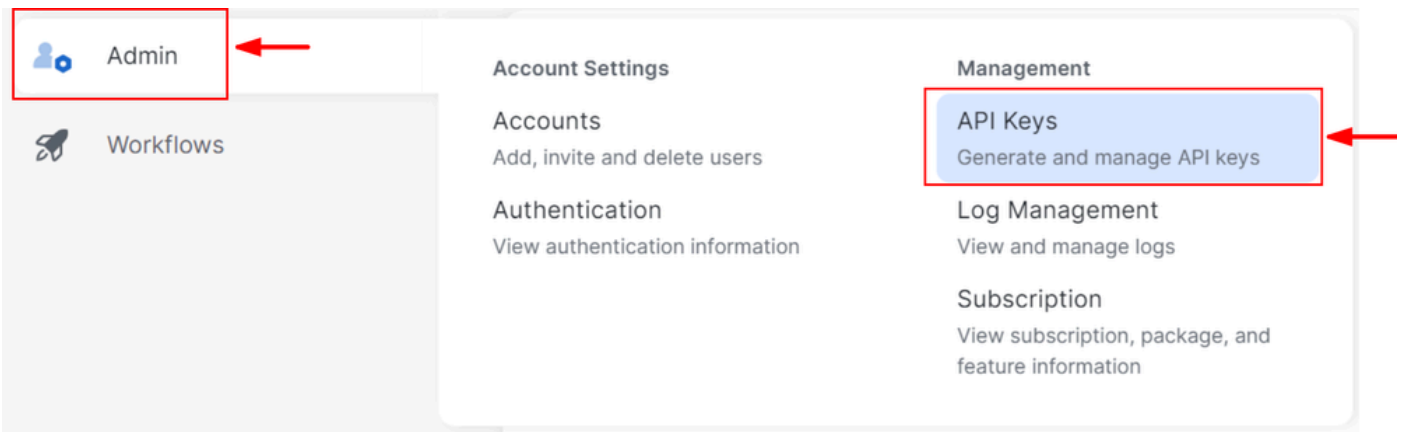
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

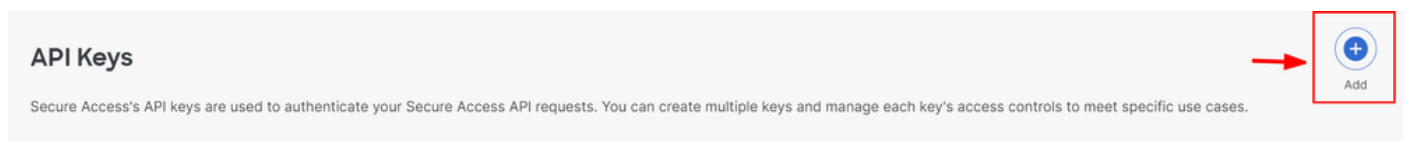
1. Crie sua chave de API

Navegue até [Painel de controle de acesso seguro](#).

- Clique em Admin > Api Keys > Add



Criar Chave de API 1



Criar Chave de API 2

- Adicione o API Key Name , Description (Optional) , Expiry Date desejado conforme necessário

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 section titled 'Key Scope' with the instruction 'Select the appropriate access scopes to define what this API key can do.' It contains a list of scopes: Auth (1 >), Deployments (16 >), Investigate (2 >), Policies (4 >), and Reports (9 >). The 'Policies' option is selected with a blue checkmark.
- Expiry Date:** A section titled 'Expiry Date' with two radio buttons: 'Never expire' (selected) and 'Expire on' (with a date picker set to 'May 21 2024').
- Scope Selection:** A panel on the right titled '1 selected' with a 'Remove All' link. It shows a 'Scope' dropdown set to 'Read / Write' and a count of '4' items.
- Buttons:** A 'CANCEL' button on the left and a 'CREATE KEY' button on the right.

Crie sua chave de API 3

- Em Key Scope, escolha Policies Expandir políticas
- Escolha Destination Lists e Destinations
- Alterar Scope se necessário, caso contrário, manter como Read/Write
- Clique em 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](#)

Crie sua chave de API 4

- Copie o e API Keyo **Key Secret** e clique em 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](#)

Crie sua chave de API 5



Observação: há apenas uma oportunidade para copiar o segredo da API. O Secure Access não salva o segredo da API e você não pode recuperá-lo após sua criação inicial.

2. Gerar um token de acesso à API

Para gerar o token de acesso à API, faça uma solicitação de autorização de token:

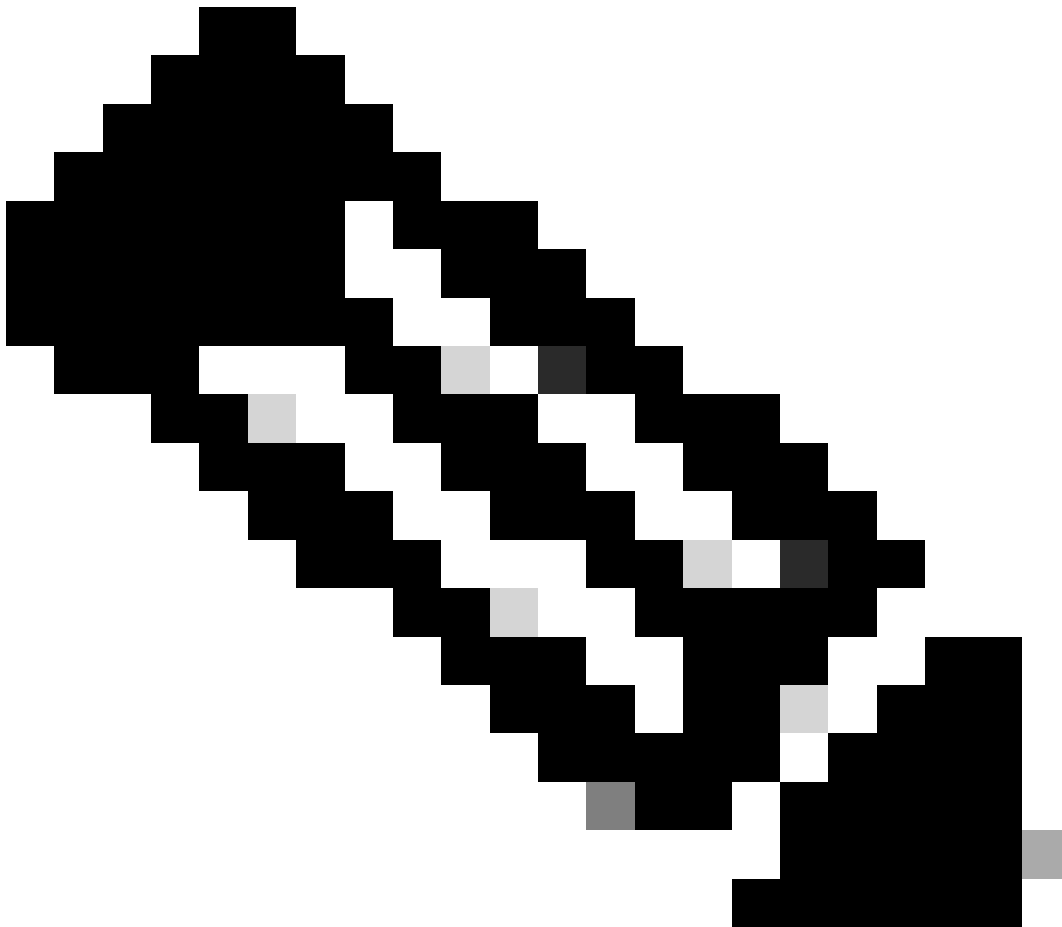
Solicitação de Autorização de Token

Use as credenciais de API de Acesso Seguro que você criou para sua organização para gerar um token de acesso à API.

- No exemplo de curl, substitua a chave e o segredo da API do Secure Access

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

- Copie e salve o token da API do portador gerado



Observação: um token de acesso OAuth 2.0 de acesso seguro expira em uma hora (3600 segundos). É recomendável que você não atualize um token de acesso até que ele esteja quase expirado.

3. Gerenciar listas de destinos

Há várias maneiras de gerenciar listas de destinos, que incluem:

Obter todas as listas de destino

Abra o prompt de comando do Windows ou o terminal Mac para executar o comando:

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

Trecho da saída de exemplo:

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

Anote a **destinationListId** que está listada no campo "id" da saída que é usada posteriormente para solicitações GET, POST ou DELETE específicas para essa lista de destinos.

Obter todos os destinos em uma lista de destinos

- **Obtenha** o destinationListId usando esta etapa de menção anterior, [Obter todas as listas de destino](#)

Abra o prompt de comando do Windows ou o terminal Mac para executar o comando:

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

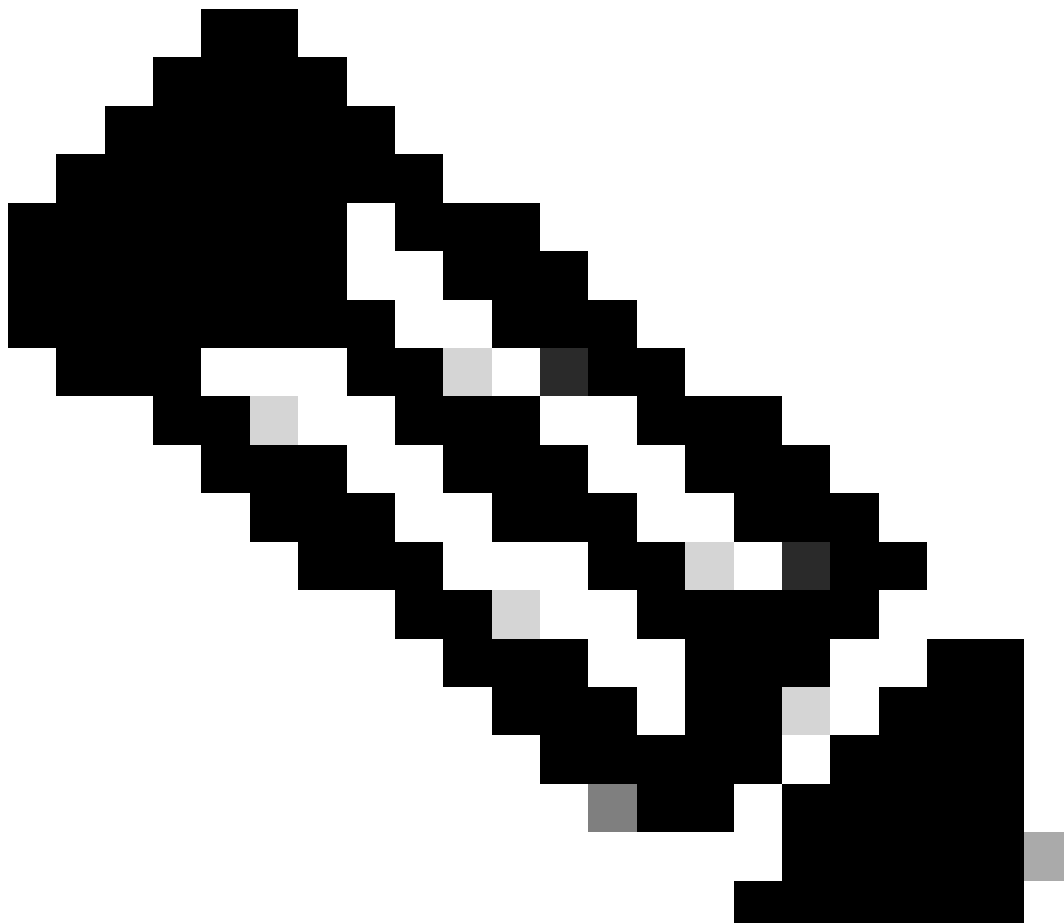
Saída de exemplo:

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

Criar uma nova lista de destinos

Abra o prompt de comando do Windows ou o terminal Mac para executar o comando:

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



Observação: substitua 'Nome da lista de destino' pelo nome desejado.

Saída de exemplo:

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

Adicionar destinos a uma lista de destinos

- Obtenha o destinationListId usando esta etapa de menção anterior, [Obter todas as listas de destino](#)

Abra o prompt de comando do Windows ou o terminal Mac para executar o comando:

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

Saída de exemplo:

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

Excluir uma lista de destinos

- **Obtenha o** destinationListId usando esta etapa de menção anterior, [Obter todas as listas de destino](#)

Abra o prompt de comando do Windows ou o terminal Mac para executar o comando:

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

Saída de exemplo:

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

Excluir destinos de uma lista de destinos

- Obtenha o destinationListId usando esta etapa de menção anterior, [Obter todas as listas de destino](#)
- Obtenha o **id** de um destino específico na lista que precisa ser excluída usando esta etapa mencionada anteriormente, [Obter todos os destinos em uma lista de destinos](#)

Abra o prompt de comando do Windows ou o terminal Mac para executar o comando:

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

Saída de exemplo:

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

Troubleshooting

Os pontos de extremidade da API Secure Access usam códigos de resposta HTTP para indicar o sucesso ou a falha de uma solicitação da API. Em geral, os códigos no intervalo 2xx indicam êxito, os códigos no intervalo 4xx indicam um erro resultante das informações fornecidas e os códigos no intervalo 5xx indicam erros de servidor. A abordagem para resolver o problema dependeria do código de resposta recebido:

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.

REST API - Códigos de resposta 2

Além disso, ao solucionar erros ou problemas relacionados à API, aqui estão os Limites de taxa a serem observados:

- [Limites de API de acesso seguro](#)

Informações Relacionadas

- [Guia do usuário do Cisco Secure Access](#)
- [Suporte técnico e downloads da Cisco](#)
- [Adicionar chaves de API de acesso seguro](#)
- [Guia do usuário para desenvolvedores](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.