

APIC-EM 1.3. - Geração de certificado - Exclusão via API

Contents

[Introduction](#)

[Informações de Apoio](#)

[Como você saberá qual é o estado atual do dispositivo?](#)

[Como você garante se o APIC-EM também tem o mesmo certificado ou se o APIC-EM entendeu ou não o mesmo certificado?](#)

[Como excluir o certificado do dispositivo?](#)

[Como aplicar o certificado do APIC - EM?](#)

[Às vezes, o APIC-EM tem o certificado, mas o dispositivo não. Como você pode resolver isso?](#)

Introduction

Este documento descreve como usar a API do Cisco Application Policy Infrastructure Controller (APIC) - Extension Mobility (EM) para criar - excluir o certificado. Com a IWAN, tudo é configurado automaticamente. No entanto, a IWAN neste momento não tem nenhum fluxo para recuperar automaticamente o dispositivo do certificado expirado.

A parte boa é que há algum tipo de fluxo na automação em termos de RestAPI. Mas essa automação é por dispositivo e precisa de algumas informações no dispositivo. O fluxo RestAPI, que está fora do fluxo de IWAN, usa algum mecanismo para automatizar o certificado para o dispositivo.

Informações de Apoio

Topologia normal do cliente.

SPOKE — HUB — APIC_EM [Controller]

Estas são as três situações:

- O certificado expirou.
- O certificado não está sendo renovado.
- O certificado não está disponível.

Como você saberá qual é o estado atual do dispositivo?

Execute o comando **Switch# sh cry pki cert.**

```
HUB2#sh cry pki cert
Certificate
Status: Available
Certificate Serial Number (hex): 3C276CE6B6ABFA8D
Certificate Usage: General Purpose
Issuer:
  cn=sdn-network-infra-subca
Subject:
  Name: HUB2
  cn=ASR1001_SSI161908CX_sdn-network-infra-iwan
  hostname=HUB2
Validity Date:
  start date: 06:42:03 UTC Mar 28 2017
  end   date: 07:42:03 UTC Mar 28 2017
Associated Trustpoints: sdn-network-infra-iwan

CA Certificate
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: General Purpose
Issuer:
  cn=ca
Subject:
  cn=sdn-network-infra-subca
Validity Date:
  start date: 06:42:03 UTC Mar 28 2017
  end   date: 07:42:03 UTC Mar 28 2017
Associated Trustpoints: sdn-network-infra-iwan
```

Se você vir, há dois certificados e aqui você precisa verificar o Ponto de confiança associado .

A data de término geralmente é de um ano e deve ser posterior à data de início.

Se for sdn-network-infra-iwan, significa, no APIC-EM, que você tem ID e certificado CA registrado.

Como você garante se o APIC-EM também tem o mesmo certificado ou se o APIC-EM entendeu ou não o mesmo certificado?

a. Mostrar versão do dispositivo e coletar o número de série:

```
If you require further assistance please contact us by sending email to
export@cisco.com.
```

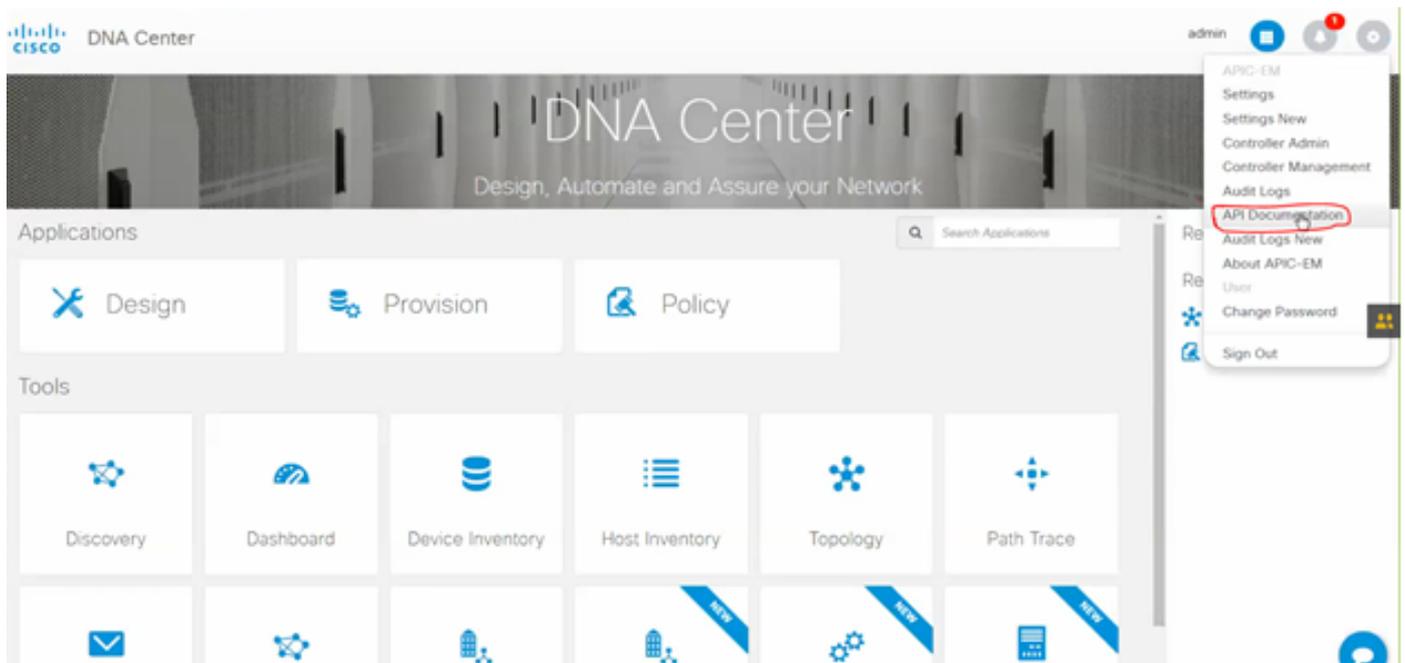
```
License Type: RightToUse
License Level: adventerprise
Next reload license Level: adventerprise
```

```
cisco ASR1001 (1RU) processor (revision 1RU) with 1062861K/6147K bytes of memory.
Processor board ID SSI161908CX
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7741439K bytes of eUSB flash at bootflash:.
```

```
Configuration register is 0x0
```

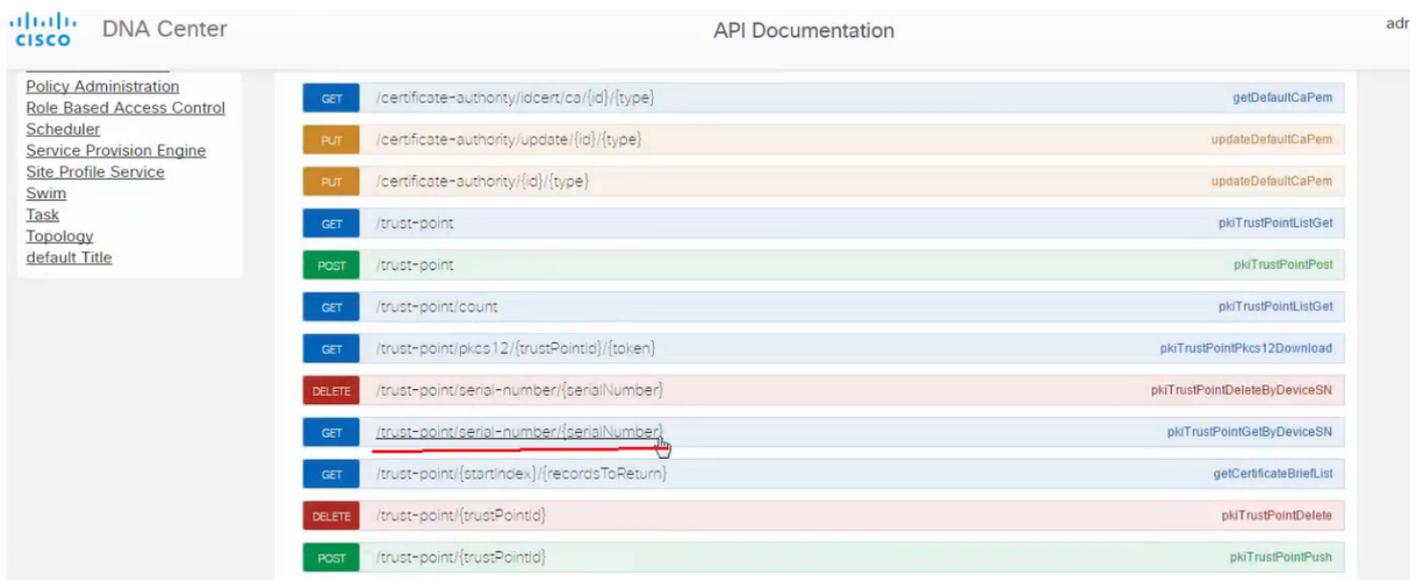
Com a ajuda desse número de série, você pode executar a consulta do APIC-EM para descobrir o que o APIC-EM pensa sobre esse dispositivo.

b. Navegue até Documentação da API.



c. Clique em Public Key Infrastructure (PKI) Broker.

d. Clique em First API (Primeira API), que nos ajudará a saber o status do lado da API.



Clique em **GET**.

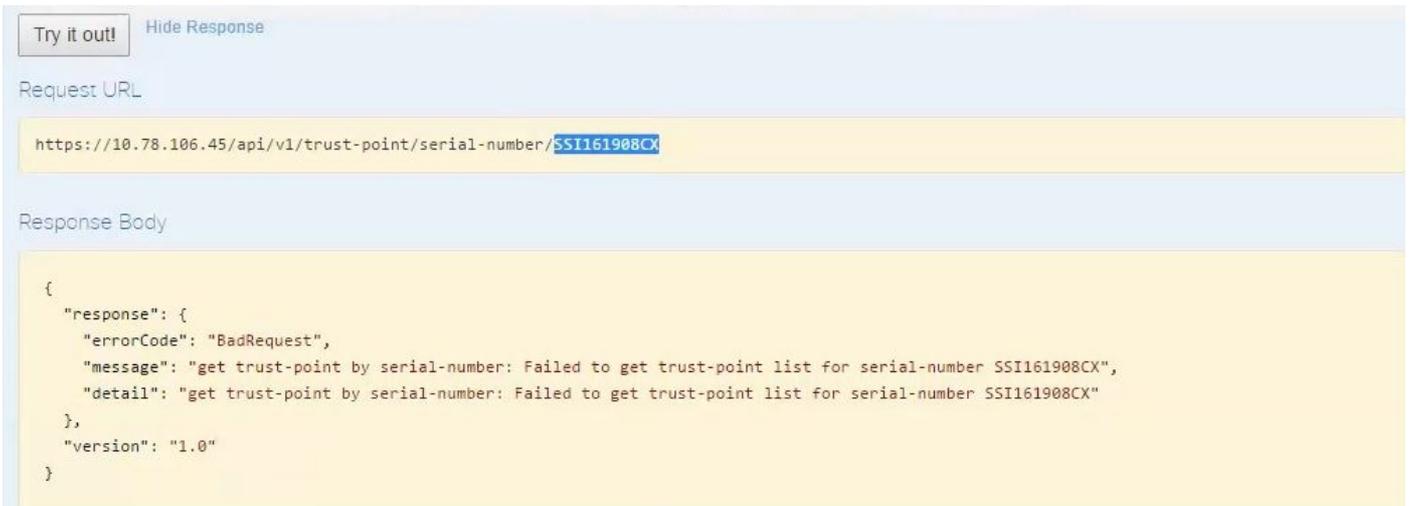
Em uma caixa de seleção, clique no número de série coletado da saída show version do dispositivo.

Clique em **Experimental!**.

Compare o valor de saída com a saída `sh crp pki cert` do dispositivo.

Como excluir o certificado do dispositivo?

Às vezes, acontece que no dispositivo, o certificado está lá e no APIC-EM não está lá. Por isso, quando você executa a **API GET**, você recebe uma mensagem de erro.



The screenshot shows an API client interface. At the top, there are buttons for "Try it out!" and "Hide Response". Below that, the "Request URL" is displayed as `https://10.78.106.45/api/v1/trust-point/serial-number/SSI161908CX`. The "Response Body" section shows the following JSON response:

```
{
  "response": {
    "errorCode": "BadRequest",
    "message": "get trust-point by serial-number: Failed to get trust-point list for serial-number SSI161908CX",
    "detail": "get trust-point by serial-number: Failed to get trust-point list for serial-number SSI161908CX"
  },
  "version": "1.0"
}
```

A solução é apenas uma e que consiste em excluir o certificado do dispositivo:

a. Switch#show run | Ponto de confiança

```
HUB2#sh run | i trustpoint
crypto pki trustpoint zxz
crypto pki trustpoint sdn-network-infra-iwan
HUB2#
```

Execute o comando **Switch#** no `crypto pki trustpoint <trustpoint name>`.

```
HUB2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
HUB2(config)#no crypto pki trustpoint sdn-network-infra-iwan
% Removing an enrolled trustpoint will destroy all certificates
received from the related Certificate Authority.

Are you sure you want to do this? [yes/no]: yes
% Be sure to ask the CA administrator to revoke your certificates.

HUB2(config)#
```

Esse comando exclui todo o certificado no dispositivo associado ao ponto de confiança selecionado.

Verifique novamente se o certificado foi excluído.

Use o comando: **Switch# sh cry pki cert.**

Ele não deve mostrar o ponto confiável de sdn que foi excluído.

b. Exclusão da chave:

Execute o comando no dispositivo: **Switch# sh cry key mypubkey all.**

Aqui você verá que o nome da chave começa com **sdn-network-infra.**

Comando para excluir a chave:

```
HUB2(config)#cry key zeroize rsa sdn-network-infra-iwan
% Keys to be removed are named 'sdn-network-infra-iwan'.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
HUB2(config)#
```

2. Certifique-se de que a interface APIC-EM conectada ao dispositivo seja Pingable.

Pode acontecer que o APIC-EM tenha duas interfaces das quais uma é pública e a outra é privada. Nesse caso, assegure-se de que a interface APIC-EM que se comunica com o dispositivo faça ping entre si.

```
HUB2#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HUB2#
```

Como aplicar o certificado do APIC - EM?

No APIC-EM, quando a documentação da API é clicada e o PKI Broker selecionado, essa opção está disponível.

[POST/trust-point](#)

- Isso criará um certificado com APIC - EM.

PKI Broker Service
 Policy Administration
 Role Based Access Control
 Scheduler
 Service Provision Engine
 Site Profile Service
 Swim
 Task
 Topology
 default Title

GET	/certificate-authority/ca/{id}/{type}	getDefaultCaPemChain
GET	/certificate-authority/idcert/ca/{id}/{type}	getDefaultCaPem
PUT	/certificate-authority/update/{id}/{type}	updateDefaultCaPem
PUT	/certificate-authority/{id}/{type}	updateDefaultCaPem
GET	/trust-point	pkitrustPointListGet
POST	/trust-point	pkitrustPointPost

Implementation Notes
 This method is used to create a trust-point

Response Class
 Model | Model Schema

```

TaskIdResult {
  version (string, optional),
  response (TaskIdResponse, optional)
}
TaskIdResponse {
  taskId (TaskId, optional),
  url (string, optional)
}
TaskId {
}
  
```

Response Content Type: application/json

Em seguida, você precisa ter informações sobre o dispositivo e clicar em Tentar.

Response Class
 Model | Model Schema

```

TaskIdResult {
  version (string, optional),
  response (TaskIdResponse, optional)
}
TaskIdResponse {
  taskId (TaskId, optional),
  url (string, optional)
}
TaskId {
}
  
```

Response Content Type: application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
pkitrustPointInput	<pre> { "platformId": "ASR1001", "serialNumber": "SSI161908CX", "trustProfileName": "sdn-network-infra-iwan", "entityType": "router", "entityName": "HUB2" } </pre>	pkitrustPointInput	body	Model Model Schema PkitrustPoint { serialNumber (string): Devices serial-number, entityName (string): Devices hostname, id (string, optional): Trust-point identification. Automatically generated, platformId (string): Platform identification. Eg. ASR1000, trustProfileName (string): Name of trust-profile (must already exist). Default: sdn-network-infra-iwan, entityType (string, optional): Available options: router.

Parameter content type: application/json

Exemplo:

```

{
  "platformId": "ASR1001",
  "serialNumber": "SSI161908CX",
  "trustProfileName": "sdn-network-infra-iwan",
  "entityType": "router",
  "entityName": "HUB2"
}
  
```

- As informações destacadas são ESTÁTICAS e o resto é dinâmico.
- O nome da entidade é Nome de host do dispositivo.
- Número de série obtido do comando show version do dispositivo.
- Tipo de entidade que você pode alterar com base no tipo de dispositivo.
- Essa informação é necessária para informar ao APIC-EM para configurar o dispositivo. Aqui, o APIC-EM compreende o número de série.

Resultado do teste!:

Response Body

```
{
  "response": {
    "taskId": "1a395ed1-1730-43fa-9527-327ed3e6e12b",
    "url": "/api/v1/task/1a395ed1-1730-43fa-9527-327ed3e6e12b"
  },
  "version": "1.0"
}
```

Response Code

202

Response Headers

```
{
  "Pragma": "no-cache, no-cache",
  "Content-Security-Policy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-2dcc163f-98f3-45e2-bd5b-...",
  "X-Frame-Options": "SAMEORIGIN, SAMEORIGIN",
  "Date": "Tue, 28 Mar 2017 10:10:06 GMT",
  "Strict-Transport-Security": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains",
  "Content-Type": "application/json;charset=UTF-8",
  "Access-Control-Allow-Origin": "https://10.78.106.45",
  "Cache-Control": "no-cache, no-store, no-cache, no-store",
  "Transfer-Encoding": "chunked",
  "Access-Control-Allow-Credentials": "false"
}
```

Essa saída significa que o arquivo é criado internamente pelo APIC-EM e agora está pronto para ser implantado no dispositivo. A próxima etapa é empurrar esse dispositivo para dentro do pacote. Para forçar, você precisa obter a ID do ponto de confiança. Isso pode ser feito via CHAMADA GET API.

[GET/trust-point/serial-number/{serialNumber}](#) - Consulta

The screenshot shows the REST API documentation for the endpoint `GET /trust-point/serial-number/{serialNumber}`. The implementation notes state: "This method is used to return a specific trust-point by its device serial-number". The response class is `PkiTrustPointResult`, which contains a `version` (optional string) and a `response` (optional `PkiTrustPoint`). The `PkiTrustPoint` class has several attributes: `serialNumber` (string), `entityName` (string), `id` (optional string), `platformId` (string), `trustProfileName` (string), `entityType` (optional string), `networkDeviceId` (optional string), `certificateAuthorityId` (optional string), `controllerIpAddress` (optional string), and `attributeInfo` (optional object). The response content type is `application/json`. The parameters section shows a table with one parameter: `serialNumber` (path, string).

Parameter	Value	Description	Parameter Type	Data Type
<code>serialNumber</code>	<input type="text" value="551161908CX"/>	Device serial-number	path	string

Ele fornecerá essa saída. Significa que o APIC-EM tem o certificado com isso para empurrar o dispositivo.

Response Body

```

{
  "response": {
    "platformId": "ASR1001",
    "serialNumber": "SSI161908CX",
    "trustProfileName": "sdn-network-infra-iwan",
    "entityName": "HUB2",
    "entityType": "router",
    "certificateAuthorityId": "f0bd5040-3f04-4e44-94d8-de97b8829e8d",
    "attributeInfo": {},
    "id": "2b832bf6-9061-44bd-a773-fb5256e544fb"
  },
  "version": "1.0"
}

```

Response Code

200

Empurre o certificado para o dispositivo.

[POST/trust-point/{trustPointId}](#) // trustPointId precisa ser copiado da consulta do número de série
GET

```

{"resposta": { "platformId": "ASR1001", "número de série": "SSI161908CX", "trustProfileName":
"sdn-network-infra-iwan", "nome da entidade": "HUB2", "EntityType": "router",
"certificateAuthorityId": "f0bd5040-3f04-4e44-94d8-de97b8829e8d", "attributeInfo": {}, "id":
"c4c7d612-9752-4be5-88e5-e2b6f137ea13" }, "versão": "1,0" }

```

Isso empurrará o certificado para o dispositivo - desde que haja conectividade adequada.

POST	/trust-point/{trustPointId}	pkiTrustPointPush
GET	/trust-point/{trustPointId}	pkiTrustPointGet
GET	/trust-point/{trustPointId}/config	pkiTrustPointConfigGet
GET	/trust-point/{trustPointId}/downloaded	checkPKCS12Downloaded

[BASE URL: https://10.78.106.45/api/v1/api-docs/pki-broker-service . API VERSION: 1.0]

Parameters

Parameter	Value	Description	Parameter Type	Data Type
trustPointId	2b832bf6-9061-44bd-a773-fb5256e544fb	Trust-point ID	path	string

Error Status Codes

HTTP Status Code	Reason
200	The request was successful. The result is contained in the response body.
201	The POST/PUT request was fulfilled and a new resource has been created. Information about the resource is in the response body.
202	The request was accepted for processing, but the processing has not been completed.
204	The request was successful, however no content was returned.
206	The GET request included a Range Header, and the server responded with the partial content matching the range.
400	The client made a request that the server could not understand (for example, the request syntax is incorrect).
401	The client's authentication credentials included with the request are missing or invalid.
403	The server recognizes the authentication credentials, but the client is not authorized to perform this request.
404	The client made a request for a resource that does not exist.
500	The server could not fulfill the request.
501	The server has not implemented the functionality required to fulfill the request.
503	The server is (temporarily) unavailable.
504	The server did not respond inside time restrictions and timed-out.
409	The target resource is in a conflicted state (for example, an edit conflict where a resource is being edited by multiple users). Retrying the request later might succeed.
415	The client sent a request body in a format that the server does not support (for example, XML to a server that only accepts JSON).

Try it out!

Mensagem de êxito da resposta:

Try it out! Hide Response

Request URL

```
https://10.78.106.45/api/v1/trust-point/2b832bf6-9061-44bd-a773-fb5256e544fb
```

Response Body

```
{
  "response": {
    "taskId": "f10022bd-8f45-4597-8160-bcc07fd55898",
    "url": "/api/v1/task/f10022bd-8f45-4597-8160-bcc07fd55898"
  },
  "version": "1.0"
}
```

Response Code

```
202
```

Response Headers

Verificar novamente no dispositivo:

Você vê que ambos os certificados agora estão colados:

```
HUB2#sh cry pki cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 2AD39646370CACC7
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: HUB2
    cn=ASR1001_SSI161908CX_sdn-network-infra-iwan
    hostname=HUB2
  Validity Date:
    start date: 10:00:07 UTC Mar 28 2017
    end   date: 10:00:07 UTC Mar 28 2018
    renew date: 10:00:06 UTC Jan 14 2018
  Associated Trustpoints: sdn-network-infra-iwan
```

```
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 5676260082D447A3
  Certificate Usage: Signature
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    cn=sdn-network-infra-ca
  Validity Date:
    start date: 09:20:26 UTC Mar 28 2017
    end   date: 09:20:26 UTC Mar 27 2022
  Associated Trustpoints: sdn-network-infra-iwan
```

```
HUB2#
```

Às vezes, o APIC-EM tem o certificado, mas o dispositivo não. Como você pode resolver isso?

Há alguma tarefa em segundo plano através da qual você pode excluir certificado somente do APIC-EM.
Às vezes, o cliente, por engano, exclui o certificado do dispositivo, mas no APIC-EM, ele ainda está lá.
Clique em **EXCLUIR**.

[DELETE/trust-point/serial-number/{serialNumber}](#) - Excluir.

GET	/trust-point/count	pkITrustPointListGet
GET	/trust-point/pkcs12/{trustPointId}/{token}	pkITrustPointPkcs12Download
DELETE	/trust-point/serial-number/{serialNumber}	pkITrustPointDeleteByDeviceSN
GET	/trust-point/serial-number/{serialNumber}	pkITrustPointGetByDeviceSN

Implementation Notes

This method is used to return a specific trust-point by its device serial-number

Response Class

Model Model Schema

PkiTrustPointResult {
 version (string, optional),
 response (PkiTrustPoint, optional)
}

Digite o número de série e clique em **Try out!**.

Parameters

Parameter	Value	Description	Parameter Type	Data Type
serialNumber	SSI161908CX	Device serial-number	path	string

Error Status Codes

HTTP Status Code	Reason
200	The request was successful. The result is contained in the response body.
204	The request was successful, however no content was returned.
206	The GET request included a Range Header, and the server responded with the partial content matching the range.
400	The client made a request that the server could not understand (for example, the request syntax is incorrect).
401	The client's authentication credentials included with the request are missing or invalid.
403	The server recognizes the authentication credentials, but the client is not authorized to perform this request.
404	The client made a request for a resource that does not exist.
500	The server could not fulfill the request.
501	The server has not implemented the functionality required to fulfill the request.
503	The server is (temporarily) unavailable.
504	The server did not respond inside time restrictions and timed-out.
409	The target resource is in a conflicted state (for example, an edit conflict where a resource is being edited by multiple users). Retrying the request later might succeed.
415	The client sent a request body in a format that the server does not support (for example, XML to a server that only accepts JSON).

Try it out!

```
{
  "response": {
    "taskId": "33ab0da8-9be1-40b7-86c2-cf2e501ebbb5",
    "url": "/api/v1/task/33ab0da8-9be1-40b7-86c2-cf2e501ebbb5"
  },
  "version": "1.0"
}
```

Response Code

202

Response Headers

```
{
  "Pragma": "no-cache, no-cache",
  "Content-Security-Policy": "style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-f59e75bb-2a28-4fe8-a954-",
  "X-Frame-Options": "SAMEORIGIN, SAMEORIGIN",
  "Date": "Tue, 28 Mar 2017 10:15:23 GMT",
  "Strict-Transport-Security": "max-age=31536000; includeSubDomains, max-age=31536000; includeSubDomains",
  "Content-Type": "application/json;charset=UTF-8",
  "Access-Control-Allow-Origin": "https://10.78.106.45",
  "Cache-Control": "no-cache, no-store, no-cache, no-store",
  "Transfer-Encoding": "chunked",
  "Access-Control-Allow-Credentials": "false"
}
```