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

Contents

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.

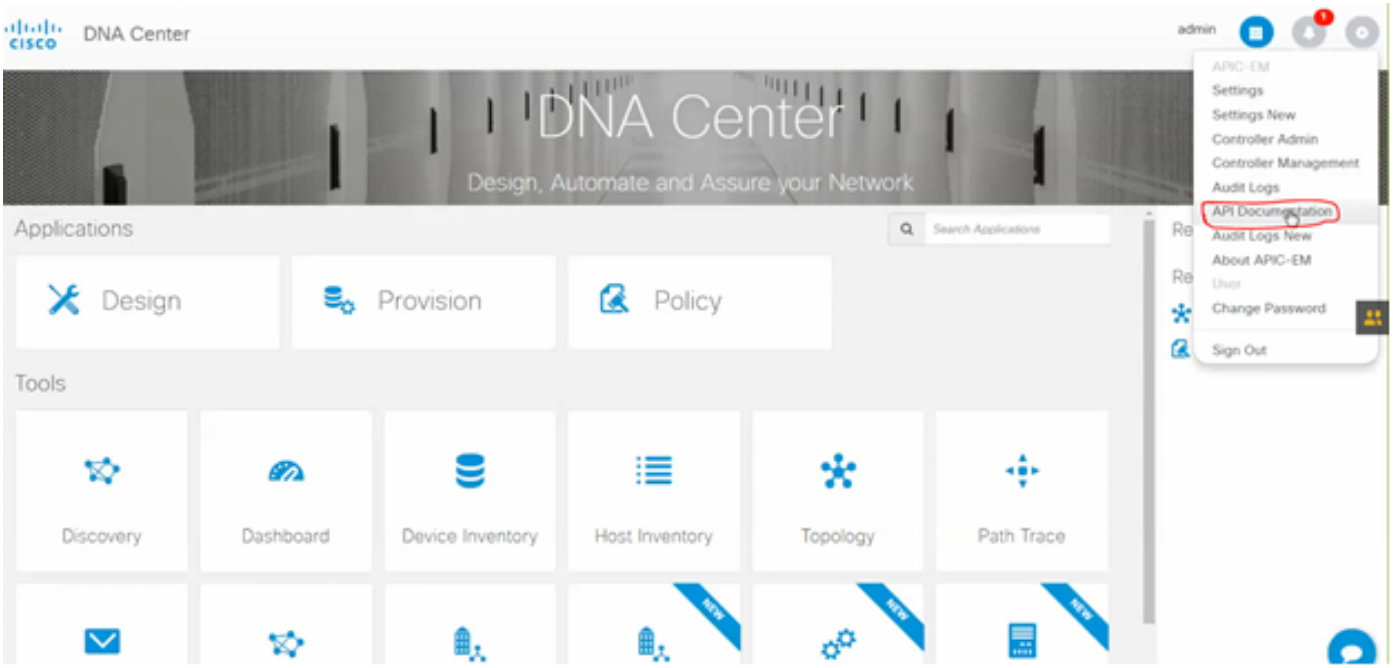
Como você garante se o APIC-EM também tem o mesmo certificado ou se o APIC-EM entendeu ou não o mesmo certificado?

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
```

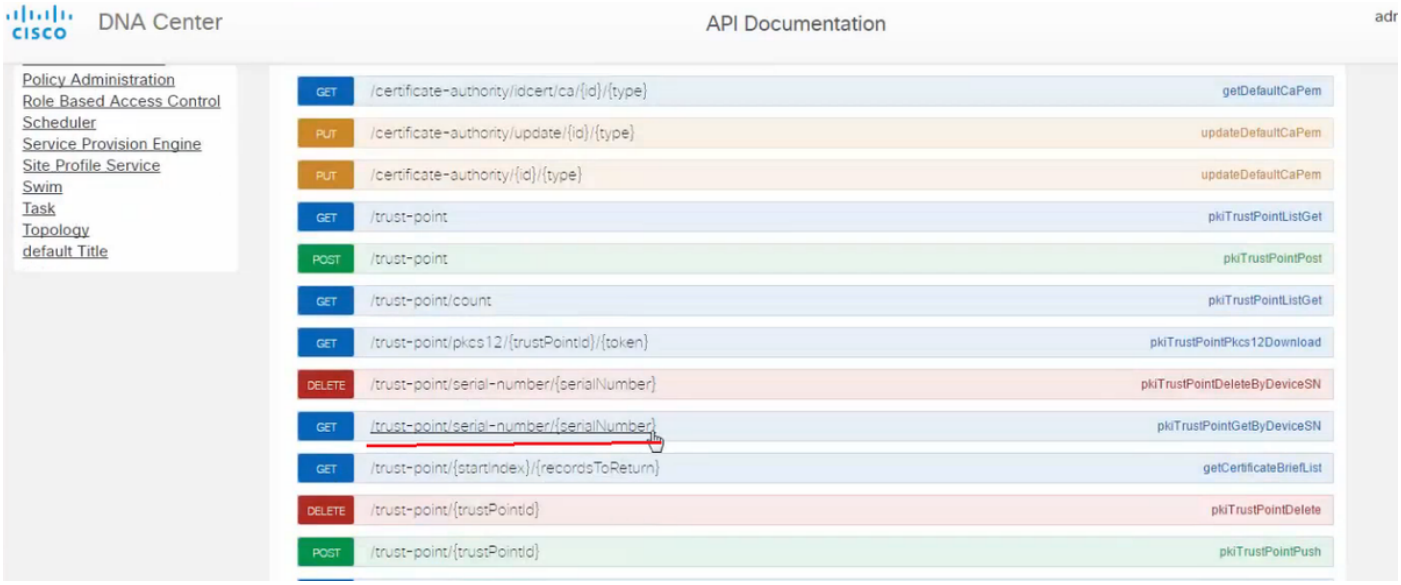
Com a ajuda desse número de série, você pode executar a consulta do APIC-EM para descobrir o que o APIC-EM pensa sobre esse dispositivo.

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.**

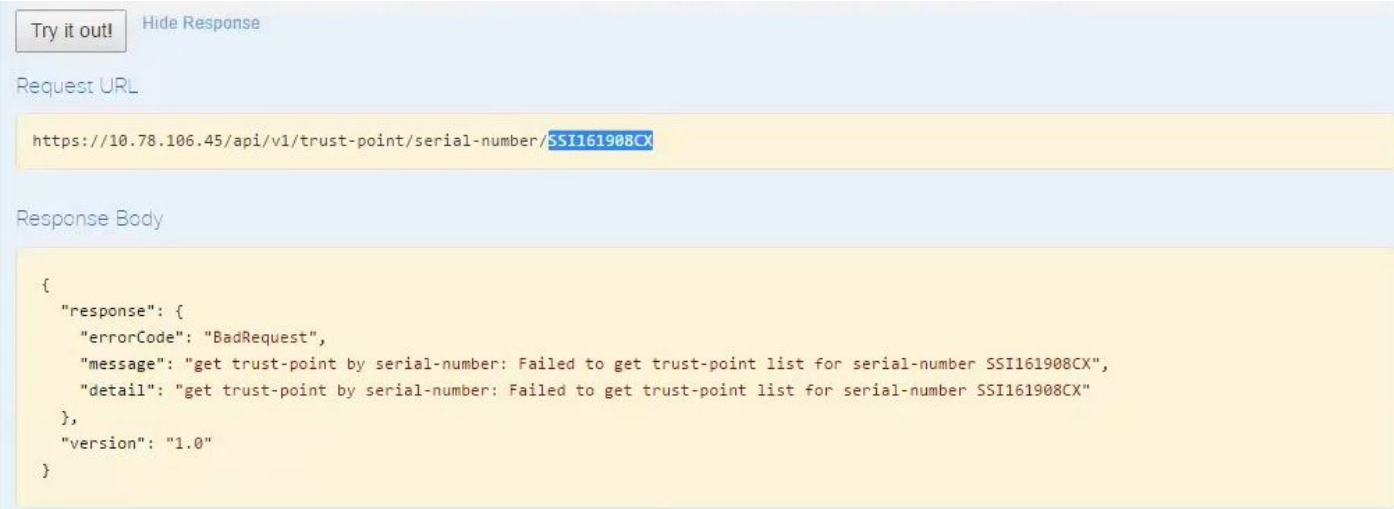
Em uma caixa de seleção, clique no número de série coletado da saída show version do dispositivo.

Clique em **Experimentar!**.

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

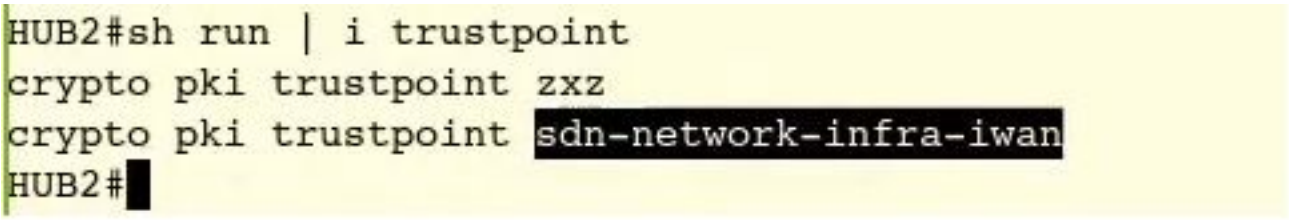
Como excluir o certificado do dispositivo?

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.

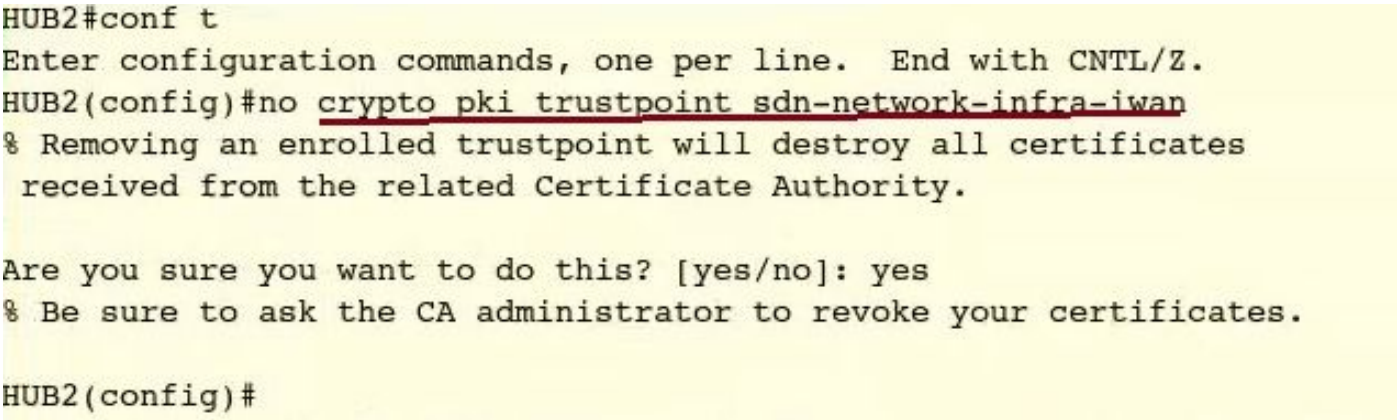


A solução é apenas uma e que consiste em excluir o certificado do dispositivo:

a. **Switch#show run | Ponto de confiança**



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



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.

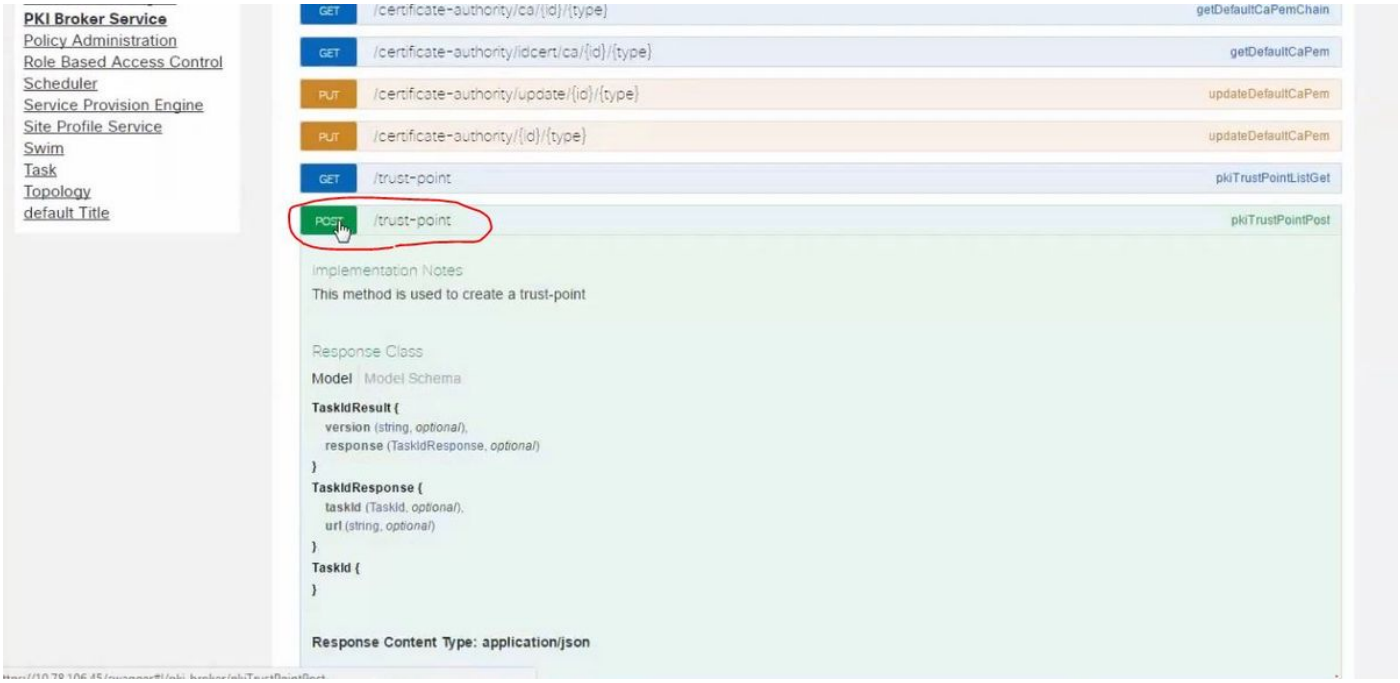
```
HUB2#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HUB2#
```

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.



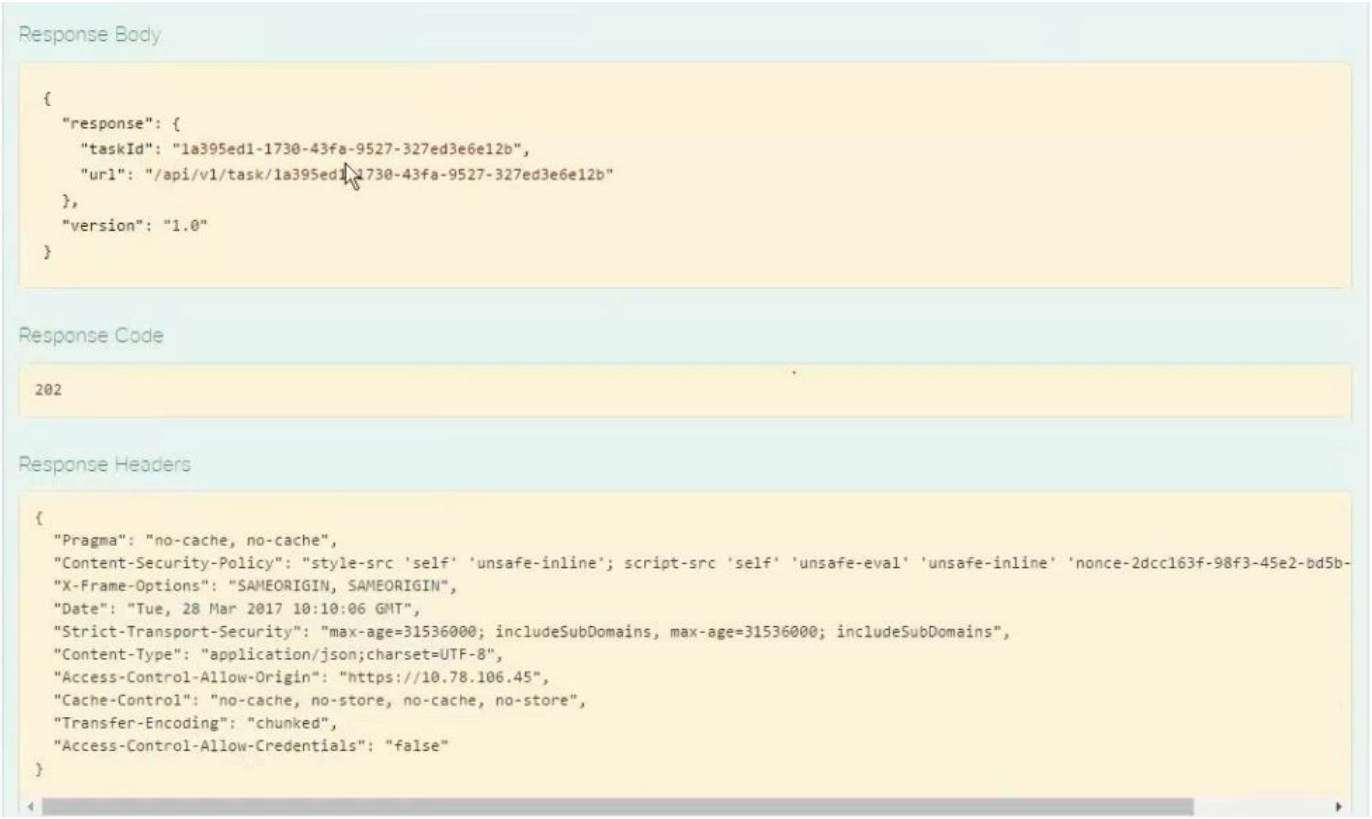
Em seguida, você precisa ter informações sobre o dispositivo e clicar em Tentar.

Exemplo:

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

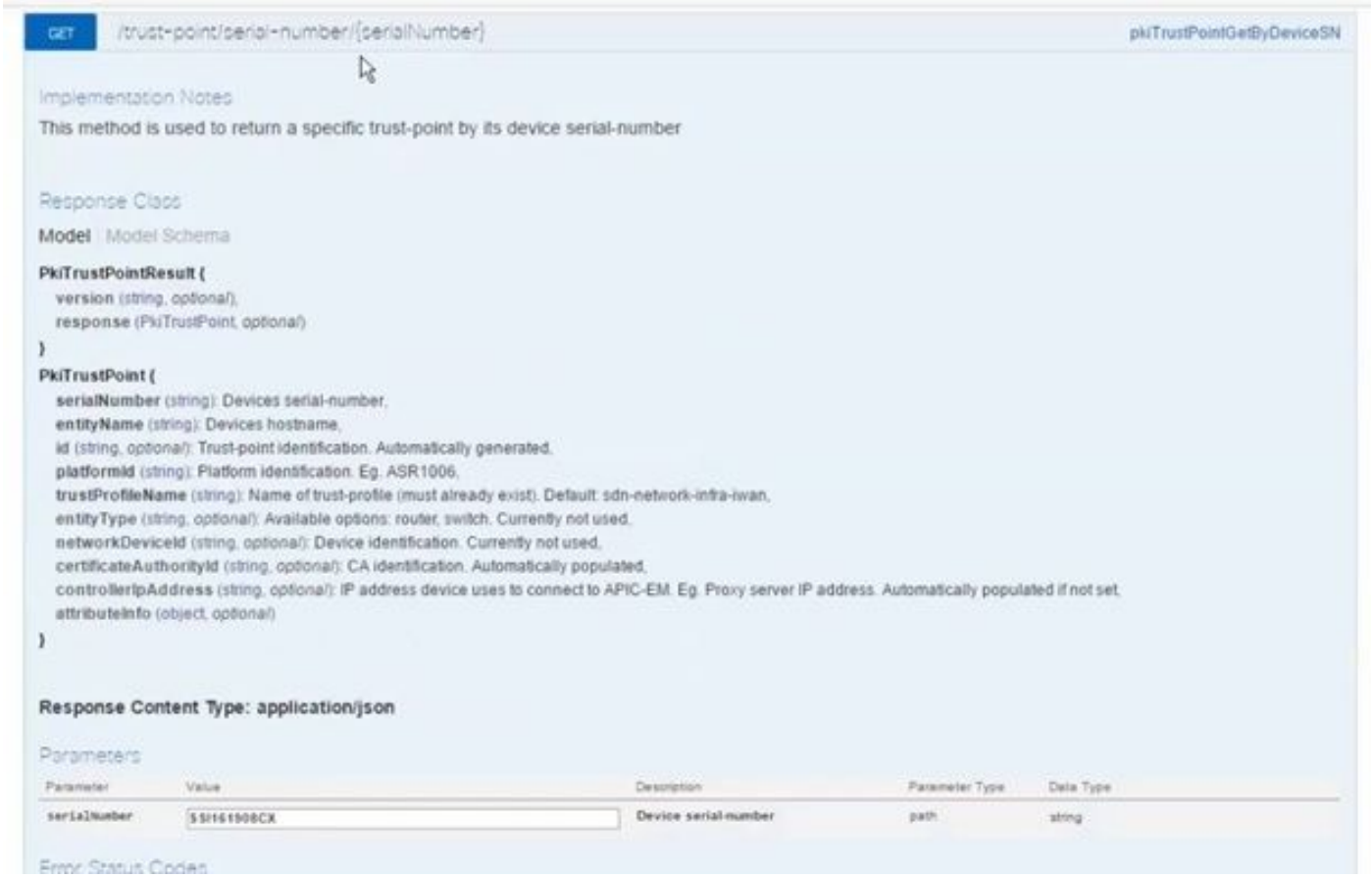
- As informações destacadas são ESTÁTICAS e o resto é dinâmico.
- O nome da entidade é Nome de host do dispositivo.
- Número de série obtido do comando show version do dispositivo.
- Tipo de entidade que você pode alterar com base no tipo de dispositivo.
- Essa informação é necessária para informar ao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

Resultado do teste!:



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



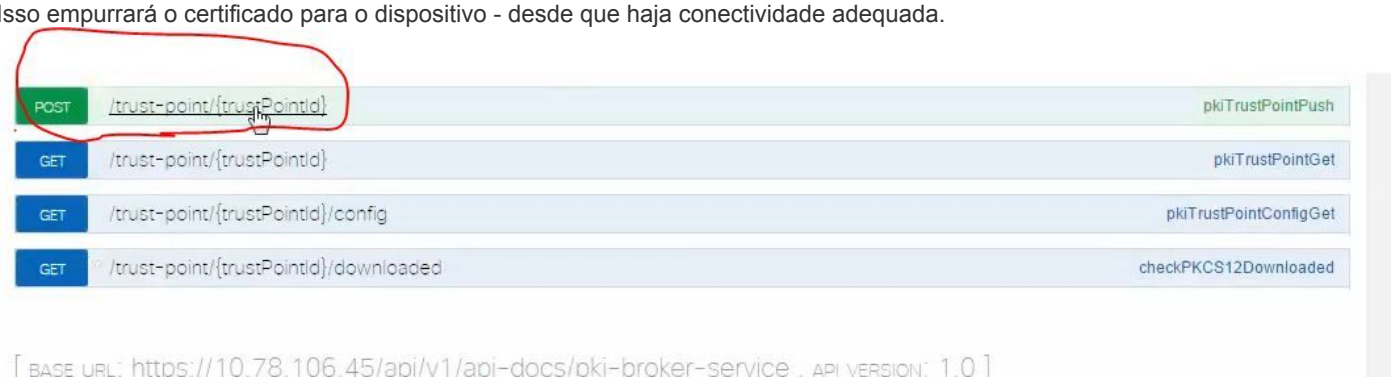
Ele fornecerá essa saída. Significa que o APIC-EM tem o certificado com isso para empurrar o dispositivo.

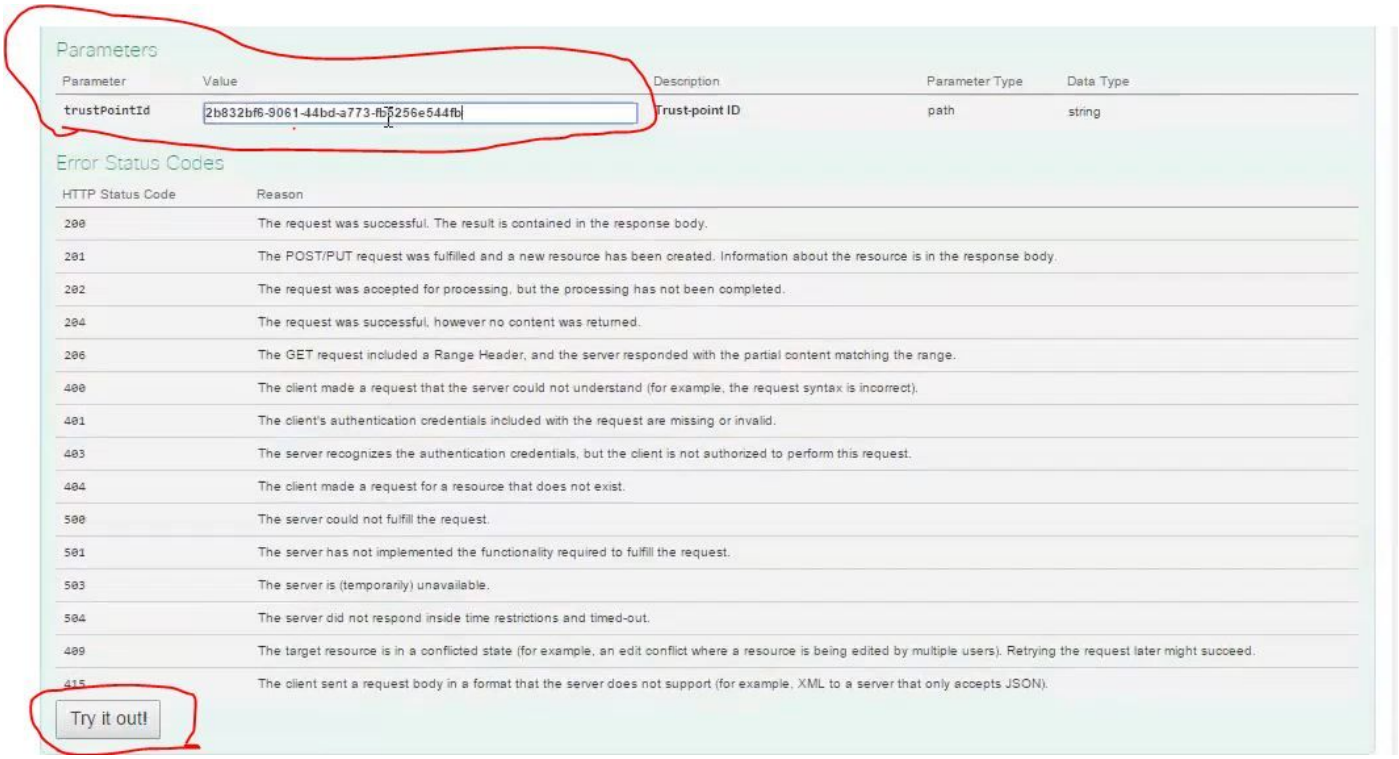
Empurre o certificado para o dispositivo.

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.





Mensagem de êxito da resposta:

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.

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