# APIC-EM 1.3 - Generación de certificados: eliminación mediante API

## Contenido



## Introducción

Este documento describe cómo utilizar la API Cisco Application Policy Infrastructure Controller (APIC) - Extension Mobility (EM) para crear y eliminar el certificado. Con IWAN, todo se configura automáticamente. Sin embargo, IWAN en este momento no tiene ningún flujo para recuperar automáticamente el dispositivo del certificado caducado.

Lo bueno es que hay algún tipo de flujo en la automatización en términos de RestAPI. Sin embargo, la automatización se realiza por dispositivo y necesita cierta información sobre el dispositivo. El flujo RestAPI que está fuera del flujo IWAN, utiliza algún mecanismo para automatizar el certificado para el dispositivo.

## Antecedentes

Topología habitual del cliente.

SPOKE — HUB — APIC_EM [Controller]

Estas son las tres situaciones:

- El certificado ha caducado.
- El certificado no se está renovando.
- El certificado no está disponible en absoluto.

## ¿Cómo sabrá cuál es el estado actual del dispositivo?

Ejecute el 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
```

Si ve, hay dos certificados y aquí debe marcar el punto de confianza asociado .

La fecha de finalización será normalmente de un año y debe ser posterior a la fecha de inicio.

Si se trata de sdn-network-infra-iwan, significa desde APIC-EM que tiene ID y certificado CA registrados.

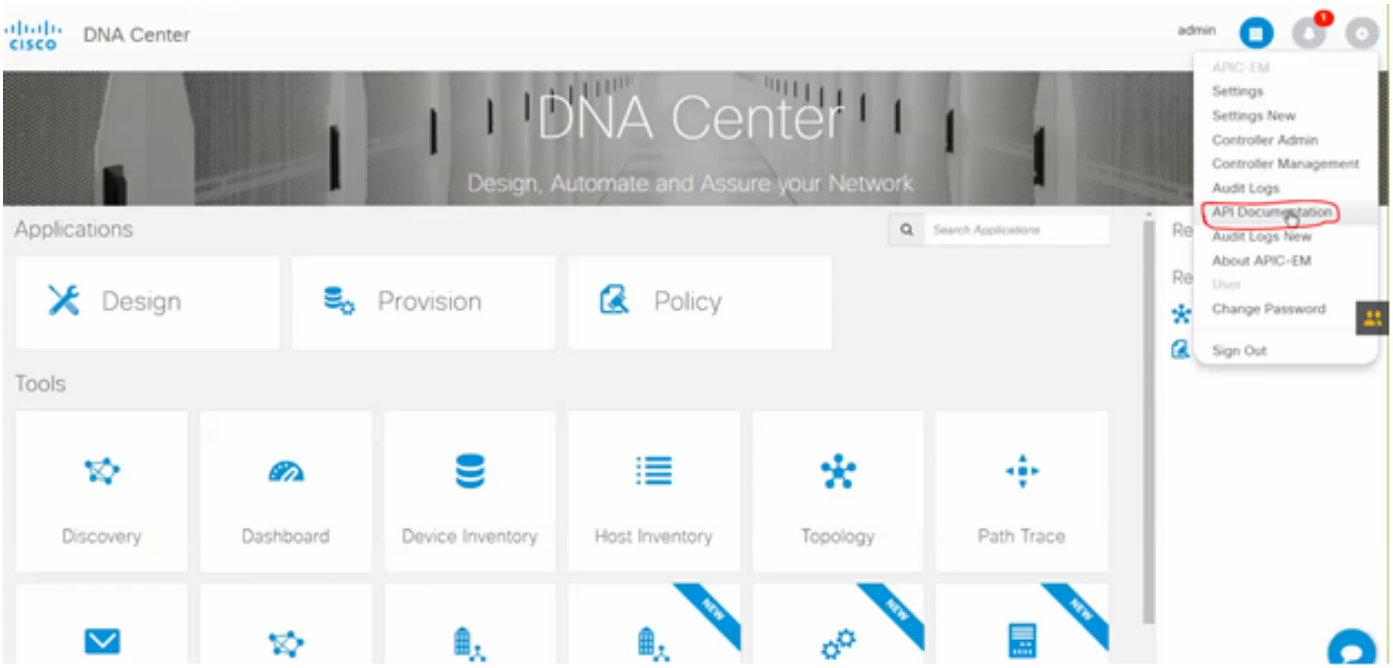
## ¿Cómo se asegura de que APIC-EM también tenga el mismo certificado o de que APIC-EM haya entendido o no el mismo certificado?

a. Mostrar la versión del dispositivo y recopilar el número de serie:

```
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 SSI[61908CX
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
```

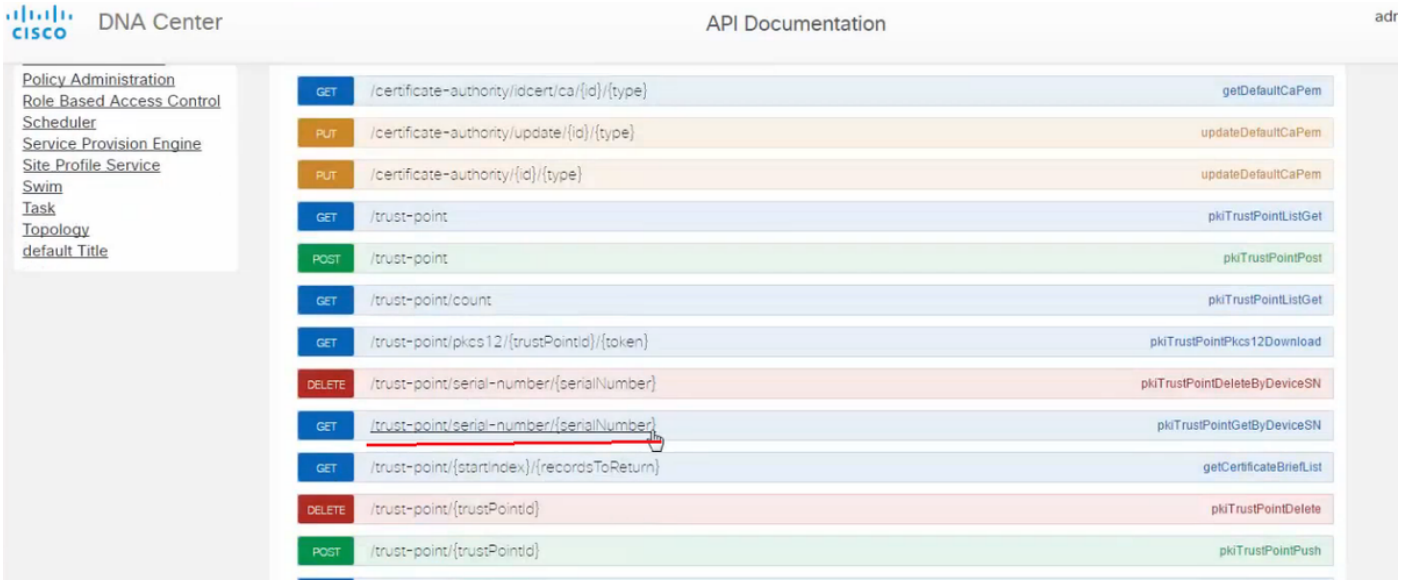
Con la ayuda de este número de serie, puede realizar una consulta APIC-EM para averiguar qué piensa APIC-EM sobre este dispositivo.

b. Vaya a Documentación de API.




c. Haga clic en Agente de infraestructura de clave pública (PKI).

d. Haga clic en First API (Primera API), que nos ayudará a conocer el estado desde el lado de la API.




Haga clic en **GET.**

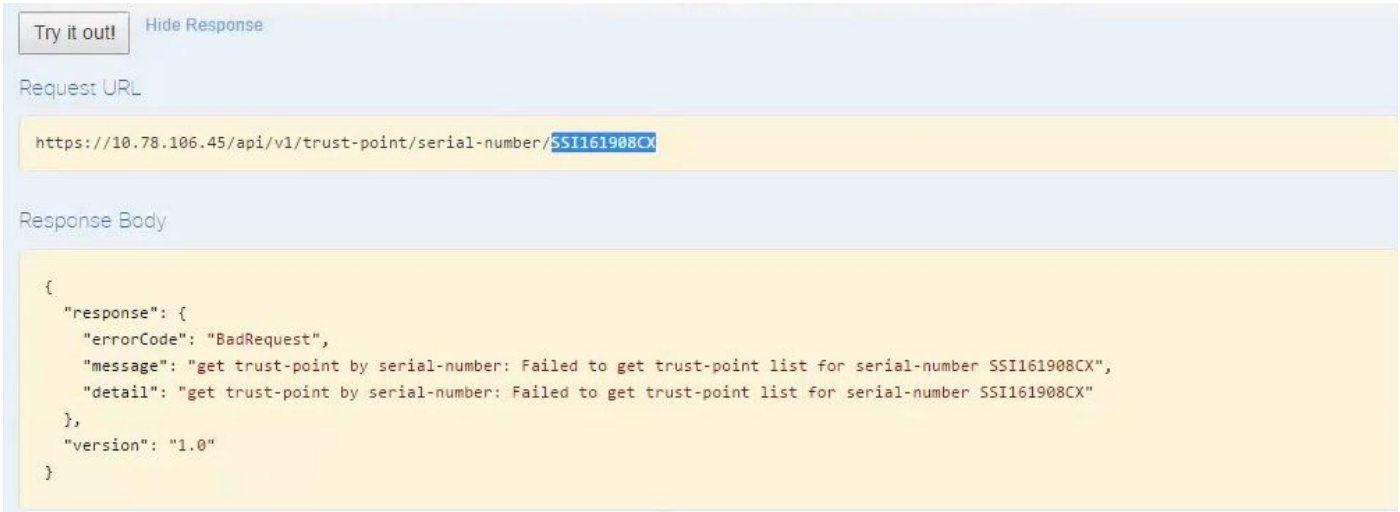
En una casilla de verificación, haga clic en el número de serie recopilado de la salida show version del Dispositivo.

Haga clic en **Prueba!**.

Compare el valor de salida con el resultado **sh crp pki cert** del dispositivo.

# ¿Cómo se elimina el certificado del dispositivo?

A veces ocurre que en el dispositivo, el certificado está ahí y en el APIC-EM no está ahí. Por eso, cuando ejecuta **GET API** obtiene un mensaje de error.




La solución es sólo una y es eliminar el certificado del dispositivo:

a. **Switch# show run | I trustpoint**

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

Ejecute el 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)#
```

Este comando elimina todo el certificado en el dispositivo asociado con el punto de confianza seleccionado.

Vuelva a comprobar si se elimina el certificado.

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

No debe mostrar el punto de confianza sdn que se eliminó.

b. Eliminación de clave:

Ejecute el comando en el dispositivo: **Switch# sh cry key mypubkey all.**

Aquí verá que el nombre de la clave comienza con **sdn-network-infra**.

Comando para eliminar la clave:

```
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. Asegúrese de que la interfaz APIC-EM conectada al dispositivo sea Pingable.

Puede ocurrir que APIC-EM tenga dos interfaces de las cuales una es pública y la otra es privada. En ese caso, asegúrese de que la interfaz APIC-EM que se comunica con el dispositivo haga ping entre sí.

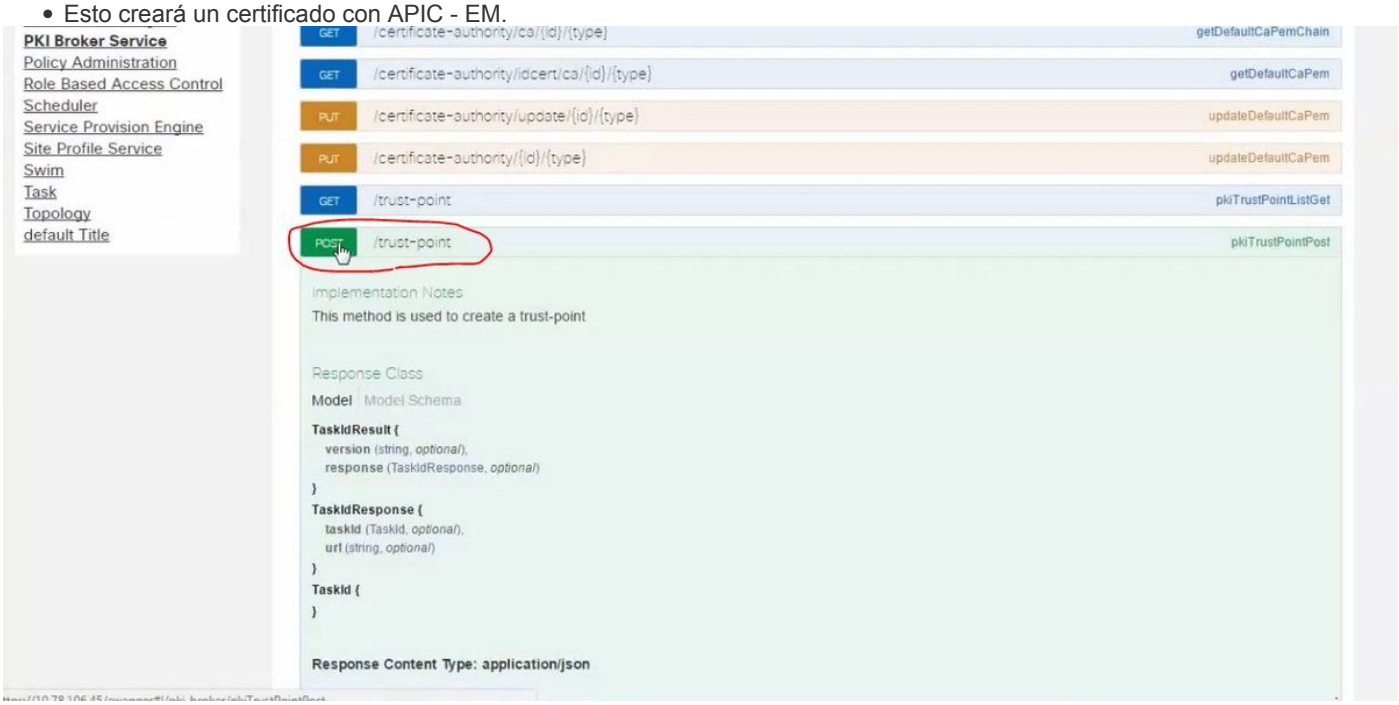
```
HUB2#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HUB2#
```

# ¿Cómo se aplica el certificado de APIC - EM?

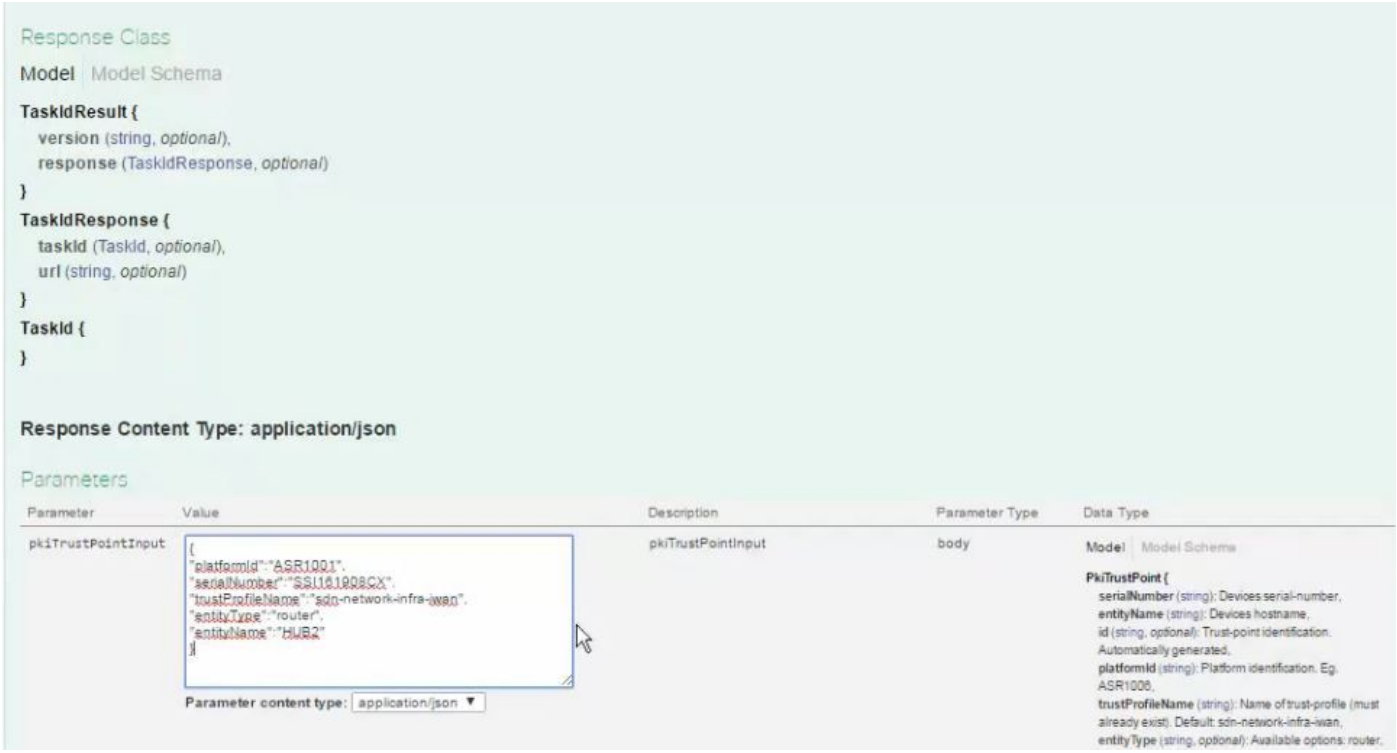
En APIC-EM, cuando se hace clic en Documentación de API y se selecciona Agente PKI, esta opción está disponible.

POST/trust-point

- Esto creará un certificado con APIC - EM.




A continuación, debe tener información sobre el dispositivo y hacer clic en la opción de probarlo.




Ejemplo:

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

- La información resaltada es ESTÁTICA y el resto es Dinámica.
- El nombre de entidad es el nombre de host del dispositivo.
- Número de serie que obtuvo de la versión show del dispositivo.
- Tipo de entidad que puede cambiar en función del tipo de dispositivo.
- Esta información es necesaria para indicar a APIC-EM que configure el dispositivo. Aquí APIC-EM comprende el número de serie.

Salida de Try it out!:

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"
}
```


Esta salida significa que APIC-EM crea el archivo internamente y que ahora está listo para implementarlo en el dispositivo.
El siguiente paso es introducir este dispositivo en el paquete. Para pulsar, necesita obtener una ID de punto de confianza. Esto se puede hacer a través de GET API CALL.

## GET/trust-point/serial-number/{serialNumber} - Consulta

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)
**)**
**PkiTrustPoint (**
  **serialNumber** (string): Devices serial-number,
  **entityName** (string): Devices hostname,
  **id** (string, optional): Trust-point identification. Automatically generated,
  **platformId** (string): Platform identification. Eg. ASR1006,
  **trustProfileName** (string): Name of trust-profile (must already exist). Default: sdn-network-infra-iwan,
  **entityType** (string, optional): Available options: router, switch. Currently not used,
  **networkDeviceId** (string, optional): Device identification. Currently not used,
  **certificateAuthorityId** (string, optional): CA identification. Automatically populated,
  **controllerIpAddress** (string, optional): IP address device uses to connect to APIC-EM. Eg. Proxy server IP address. Automatically populated if not set,
  **attributeInfo** (object, optional)
**)**

**Response Content Type: application/json**

Parameters

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

Error Status Codes

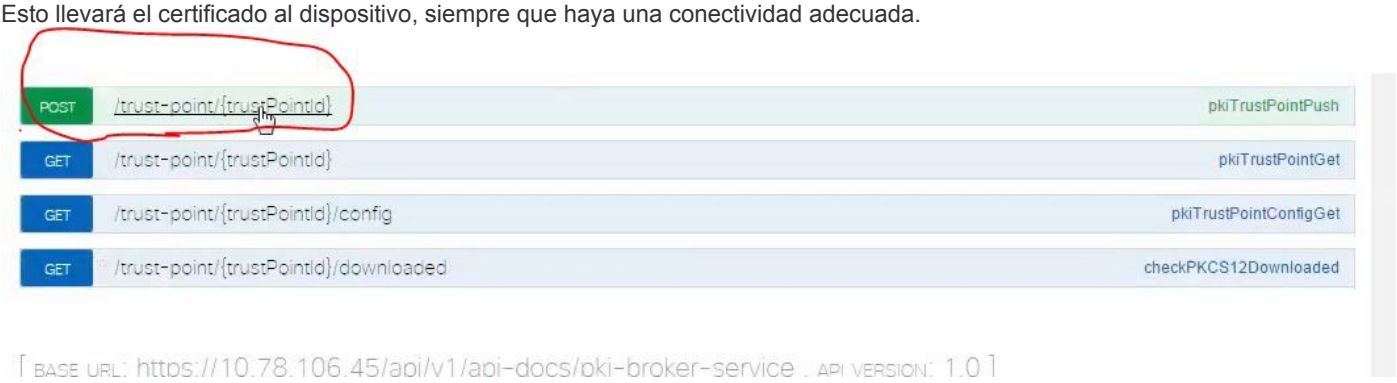
Le dará este resultado. Significa que el APIC-EM tiene el certificado con esto para presionar el dispositivo.

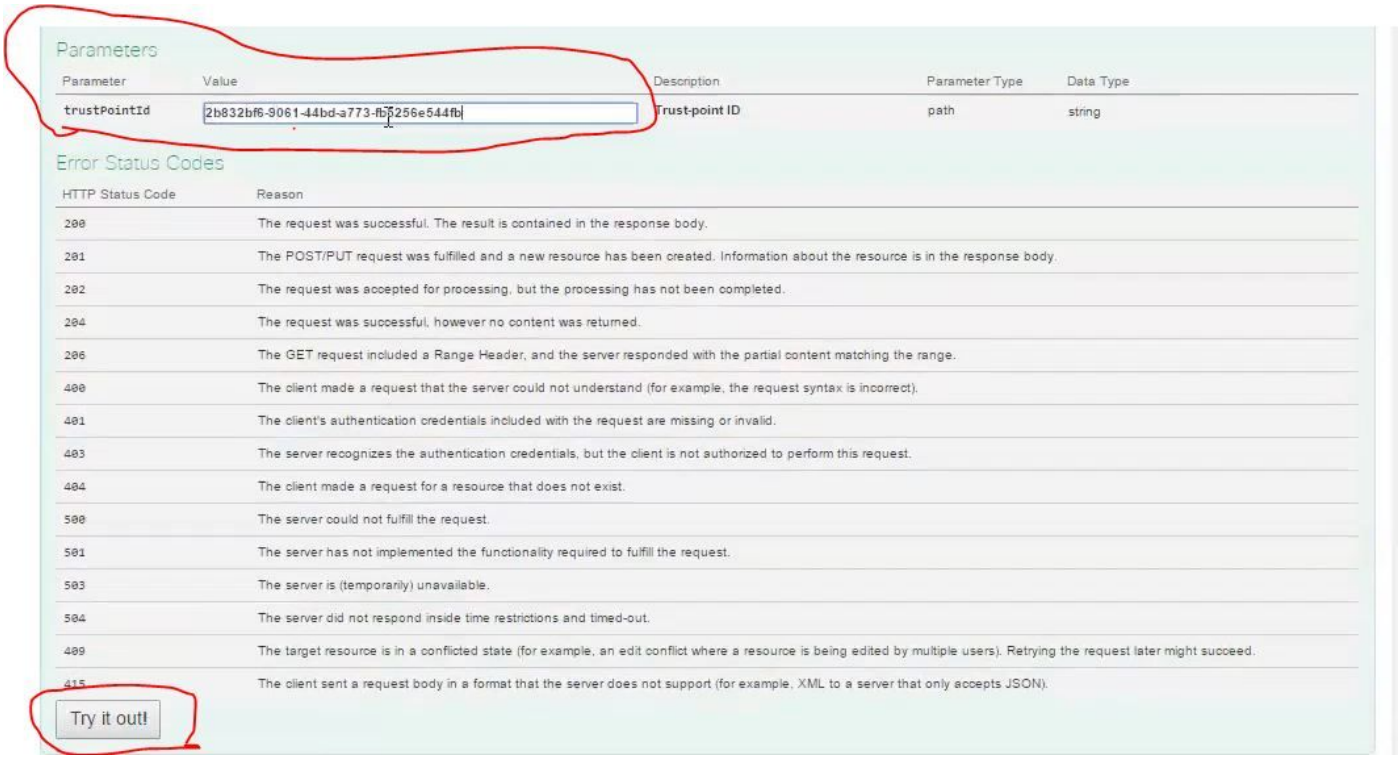

Empuje el certificado al dispositivo.

POST/trust-point/{trustPointId} // trustPointId debe copiarse de la consulta del número de serie de GET

{"response": { "platformId": "ASR1001", "serialNumber": "SSI161908CX", "trustProfileName": "sdn-network-infra-iwan", "entityName": "HUB2", "EntityType": "router", "certificateAuthorityId": "f0bd5040-3f04-4e44-94d8-de97b8829e8d", "attributeInfo": {}, "id": "c4c7d612-9752-4be5-88e5-e2b6f137ea13" }, "versión": "1.0" }

Esto llevará el certificado al dispositivo, siempre que haya una conectividad adecuada.





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!

Mensaje de respuesta correcta:

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

Vuelva a comprobar el dispositivo:
Ya ve que ambos certificados se han pegado:

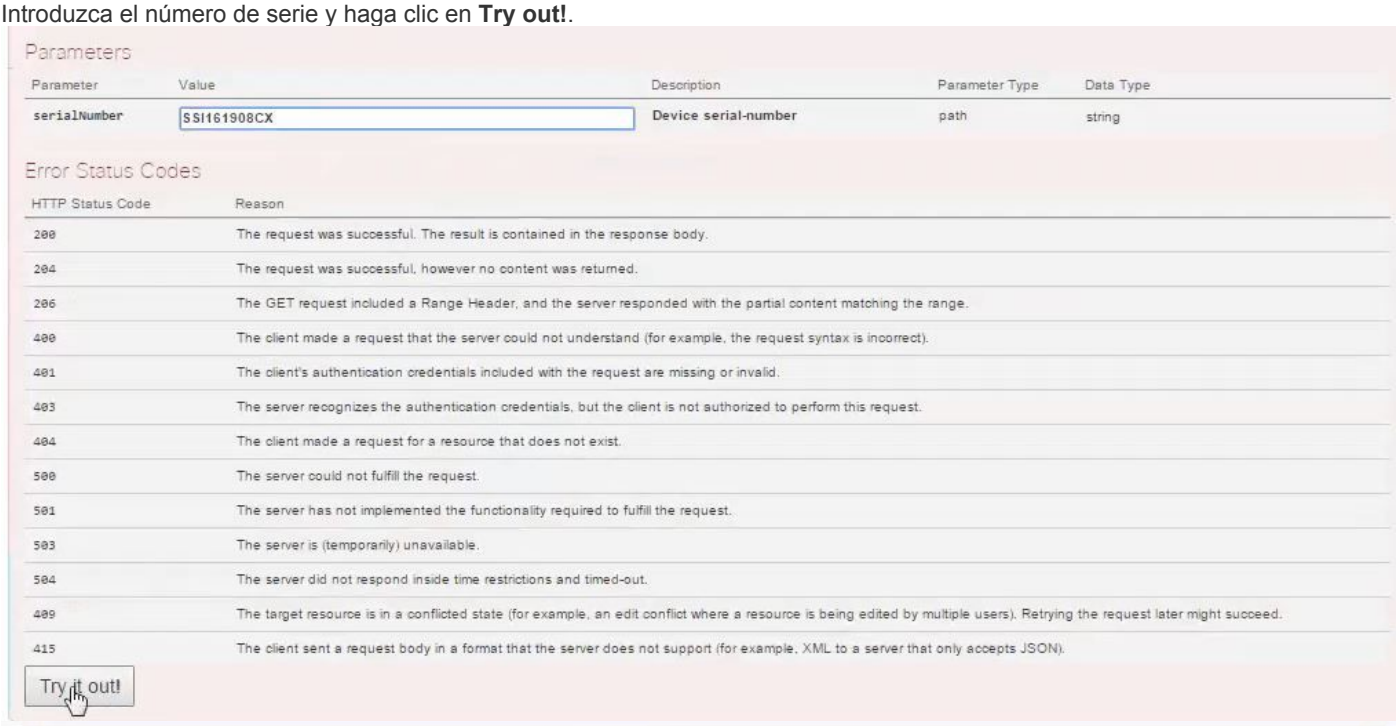
```
HUB2#sh cry pki cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 2AD39646370CACC7
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: HUB2
    cn=ASR1001_SSI161908CX_sdn-network-infra-iwan
    hostname=HUB2
  Validity Date:
    start 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#
```

# A veces APIC-EM tiene el certificado pero el dispositivo no. ¿Cómo puede resolverlo?

Hay una tarea en segundo plano a través de la cual sólo puede eliminar el certificado de APIC-EM.
A veces, el cliente elimina por error el certificado del dispositivo, pero en APIC-EM, sigue ahí.
Haga clic en **ELIMINAR.**

DELETE/trust-point/serial-number/{serialNumber} - Eliminar.


Introduzca el número de serie y haga clic en **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"
}
```