APIC-EM 1.3. - Génération de certificats - Suppression via API

Contenu

Introduction

Ce document décrit comment utiliser l'API Cisco APIC (Application Policy Infrastructure Controller) - Extension Mobility (EM) pour créer - supprimer le certificat. Avec IWAN, tout est configuré automatiquement. Cependant, pour le moment, IWAN n'a aucun flux pour récupérer automatiquement le périphérique à partir d'un certificat expiré.

Le bon côté est qu'il y a une sorte de flux dans l'automatisation en termes de RestAPI. Mais cette automatisation est par périphérique et elle nécessite des informations sur le périphérique. Le flux RestAPI qui se trouve en dehors du flux IWAN utilise un mécanisme pour automatiser le certificat du périphérique.

Informations générales

Topologie client habituelle.

SPOKE — HUB — APIC_EM [contrôleur]

Voici les trois situations :

- Le certificat a expiré.
- Le certificat n'est pas en cours de renouvellement.
- Le certificat n'est pas du tout disponible.

Comment allez-vous savoir quel est l'état actuel du périphérique ?

Exécutez la commande **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 vous voyez, il y a deux certificats et ici vous devez vérifier Associated Trustpoint .

La date de fin est généralement d'un an et doit être supérieure à la date de début.

S'il s'agit de sdn-network-infra-iwan, cela signifie à partir du module APIC-EM que vous avez un ID ainsi qu'un certificat CA enregistré.

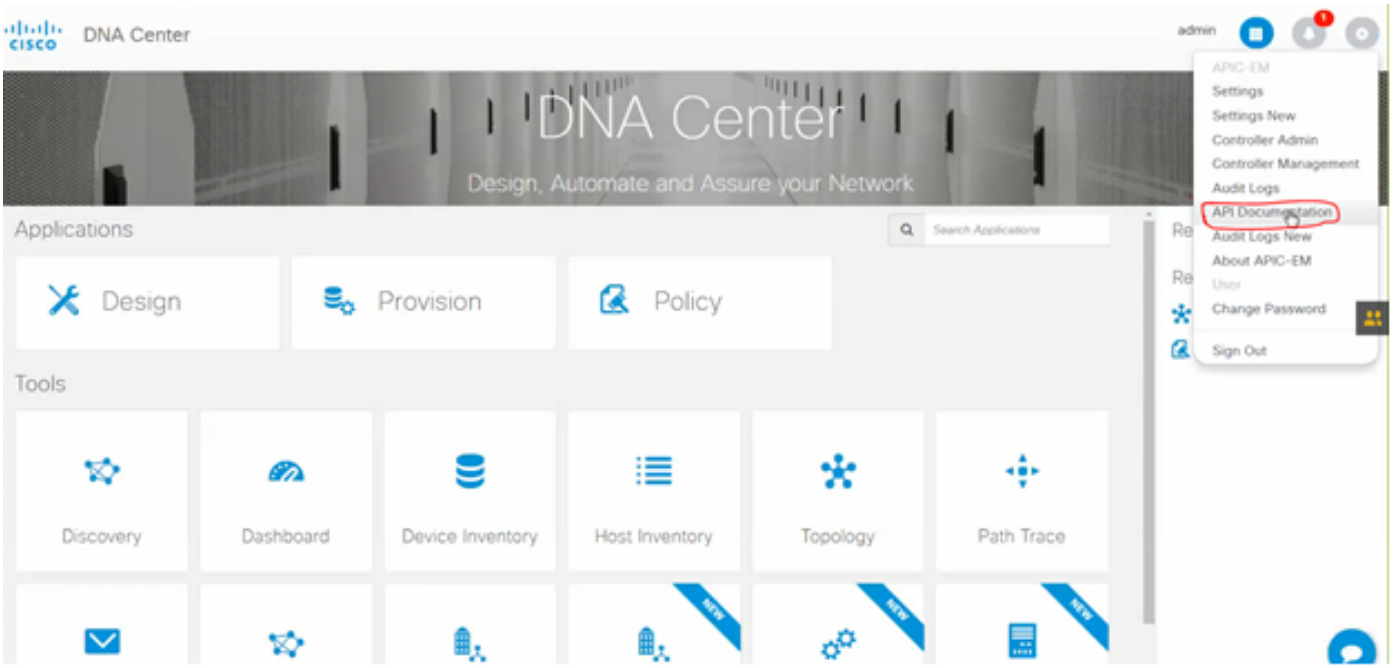
Comment vous assurer que le module APIC-EM a également le même certificat ou que le module APIC-EM a compris le même certificat ou non ?

a. Affichez la version à partir du périphérique et collectez le numéro 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
```

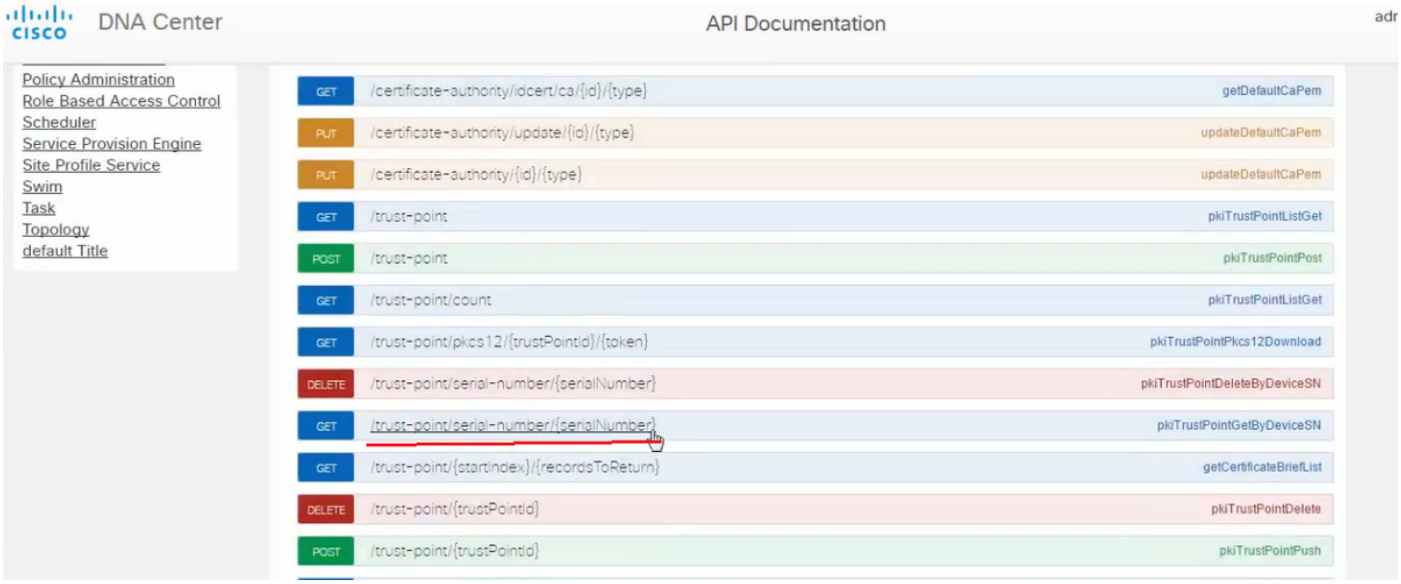
Àl'aide de ce numéro de série, vous pouvez effectuer une requête APIC-EM pour savoir ce que le module APIC-EM pense de ce périphérique.

b. Accédez à Documentation de l'API.



c. Cliquez sur Public Key Infrastructure (PKI) Broker.

d. Cliquez sur Première API pour connaître l'état du côté API.



Cliquez sur **GET.**

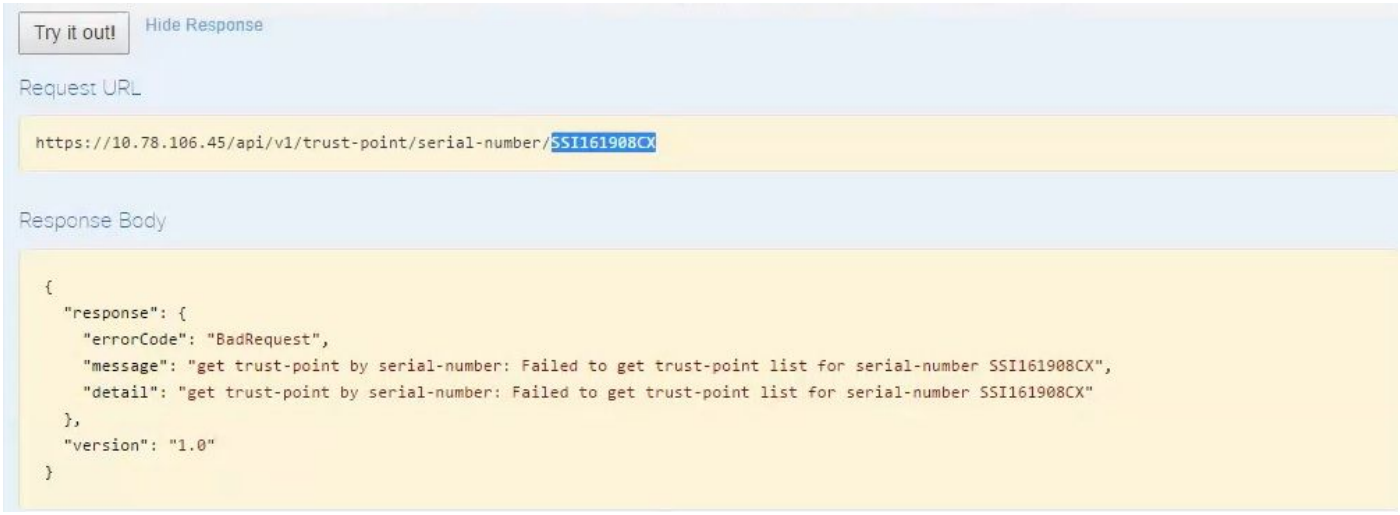
Sur une case à cocher, cliquez sur le numéro de série collecté à partir de la sortie show version of Device.

Cliquez sur **Try it out !**.

Comparez la valeur de sortie avec la sortie **sh crp pki cert** du périphérique.

Comment supprimer le certificat du périphérique ?

Il arrive parfois que sur le périphérique, le certificat est là et dans le module APIC-EM il n'est pas là. C'est pourquoi, lorsque vous exécutez **GET API**, vous recevez un message d'erreur.



La solution est la suivante : supprimer le certificat du périphérique :

a. **Switch# show run | J'ai confiance**

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

Exécutez la commande **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)#
```

Cette commande supprime tous les certificats sur le périphérique associé au point de confiance sélectionné.

Vérifiez à nouveau si le certificat est supprimé.

Utilisez la commande : **Switch# sh cry pki cert.**

Il ne doit pas afficher sdn trustpoint qui a été supprimé.

b. Suppression de la clé :

Exécuter la commande sur le périphérique : **Switch# sh cry key mypubkey all.**

Vous verrez que le nom de la clé commence par **sdn-network-infra**.

Commande permettant de supprimer la clé :

```
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. Assurez-vous que l'interface APIC-EM connectée au périphérique doit être Pingable.

Il se peut que le module APIC-EM ait deux interfaces à partir desquelles l'une est publique et l'autre privée. Dans ce cas, assurez-vous que l'interface APIC-EM qui communique avec le périphérique s'envoie des requêtes ping.

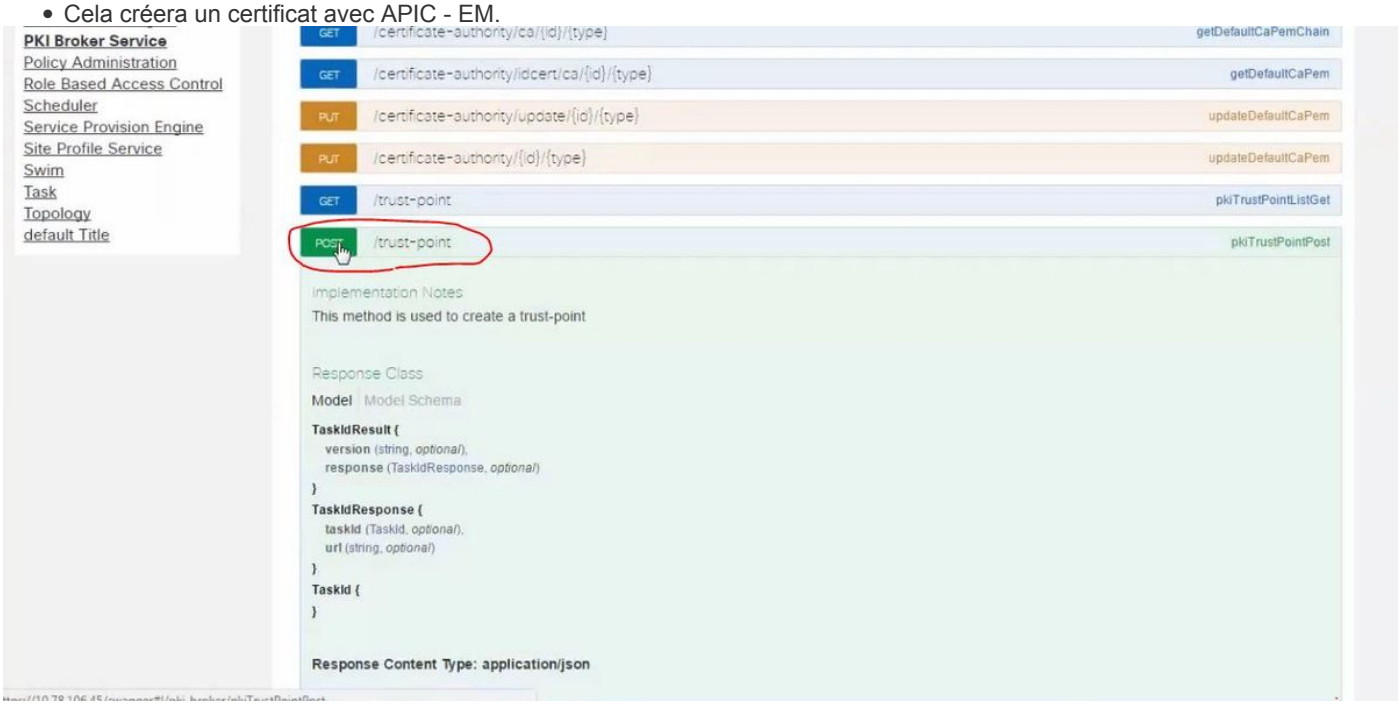
```
HUB2#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HUB2#
```

Comment faire une demande de certificat de l'APIC - EM?

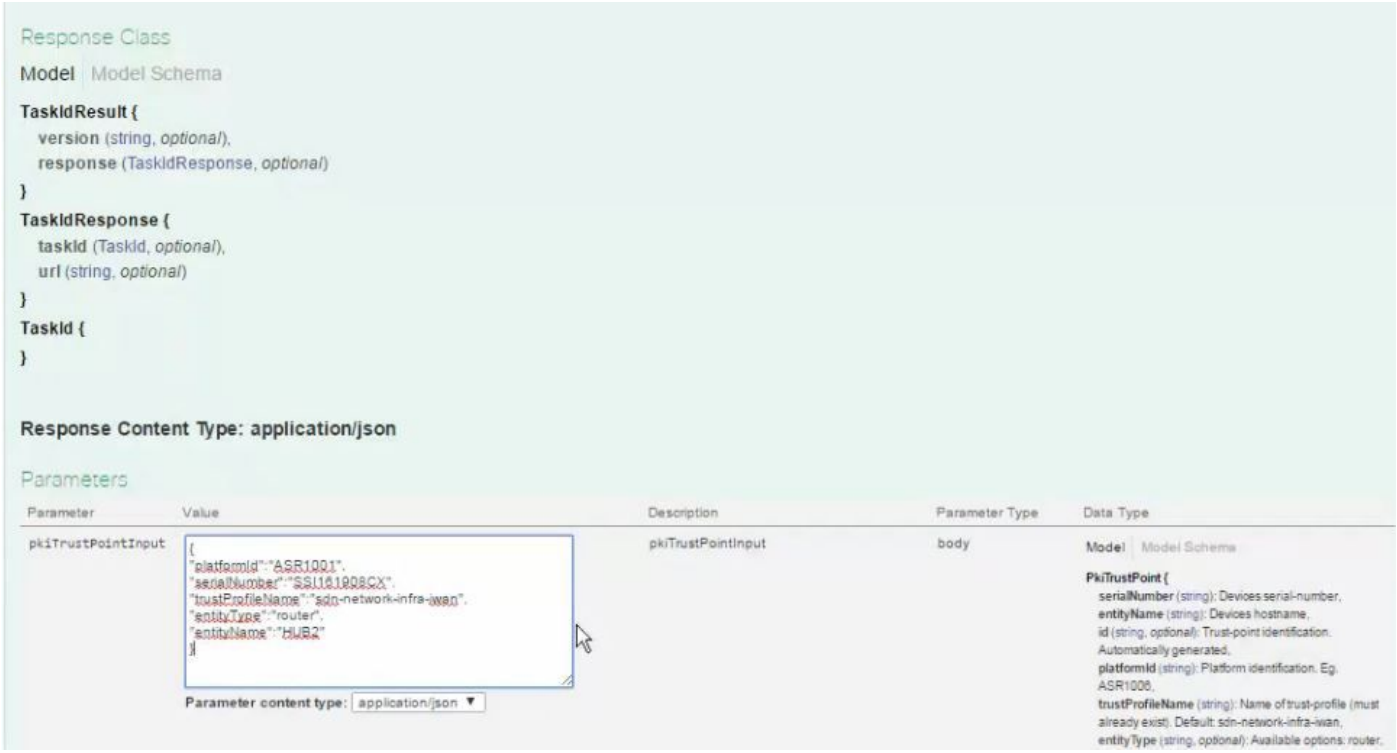
Sous APIC-EM, lorsque vous cliquez sur Documentation API et que PKI Broker est sélectionné, cette option est disponible.

POST/trust-point

- Cela créera un certificat avec APIC - EM.



Ensuite, vous avez besoin d'informations sur le périphérique et cliquez sur essayer.

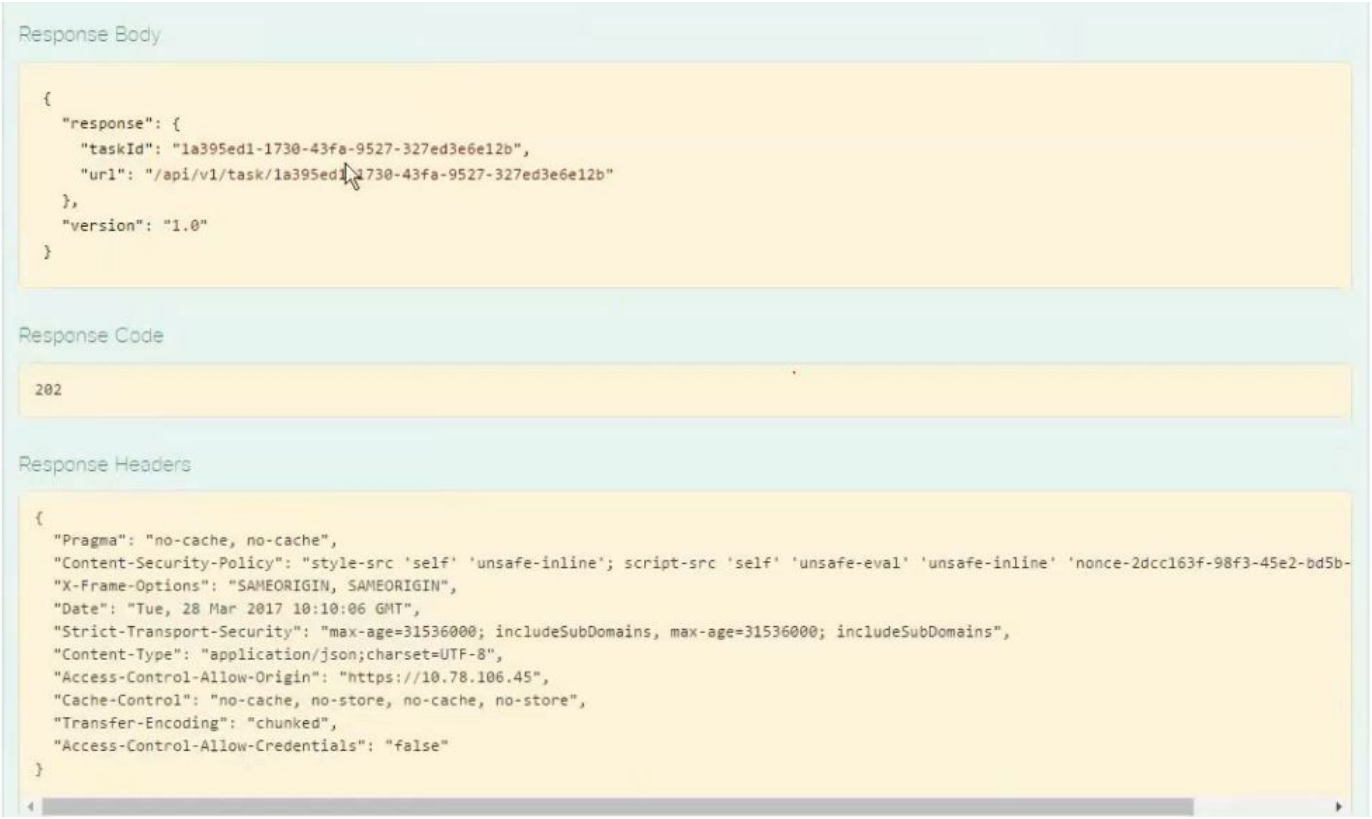


Exemple :

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

- Les informations mises en surbrillance sont STATIQUES et le reste est dynamique.
- Le nom d'entité est le nom d'hôte du périphérique.
- Numéro de série obtenu à partir de la version show du périphérique.
- Type d'entité que vous pouvez modifier en fonction du type de périphérique.
- Cette information est nécessaire pour indiquer au module APIC-EM de configurer le périphérique. Le module APIC-EM comprend le numéro de série.

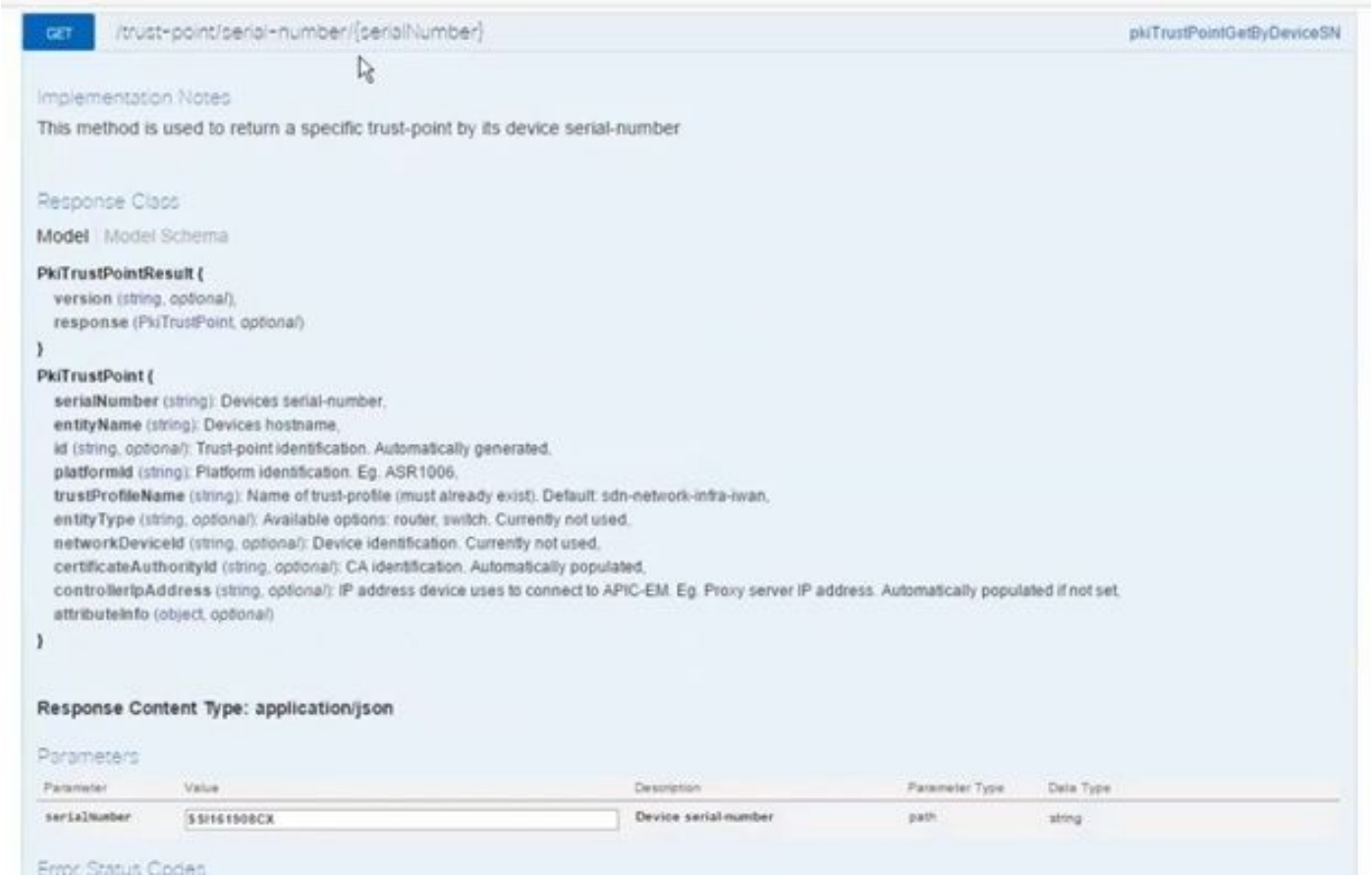
Résultat de Try it out :



Ce résultat signifie que le fichier est créé en interne par le module APIC-EM et est maintenant prêt à être déployé sur le périphérique.

L'étape suivante consiste à insérer ce périphérique dans le bundle. Pour pousser, vous devez obtenir l'ID du point de confiance. Ceci peut être fait via GET API CALL.

GET/trust-point/serial-number/{serialNumber} - Requête



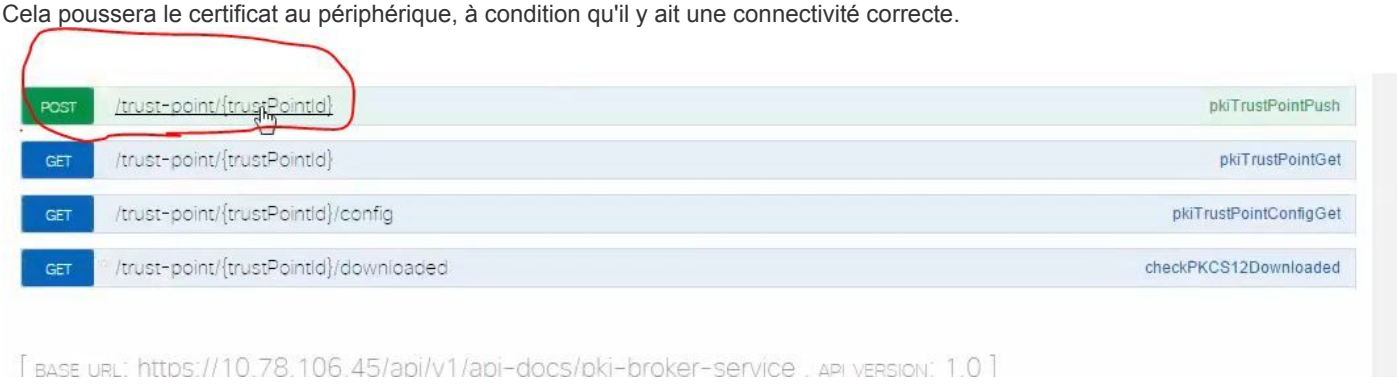
Cela vous donnera cette sortie. Cela signifie que le module APIC-EM possède le certificat avec lequel il peut être activé sur le périphérique.

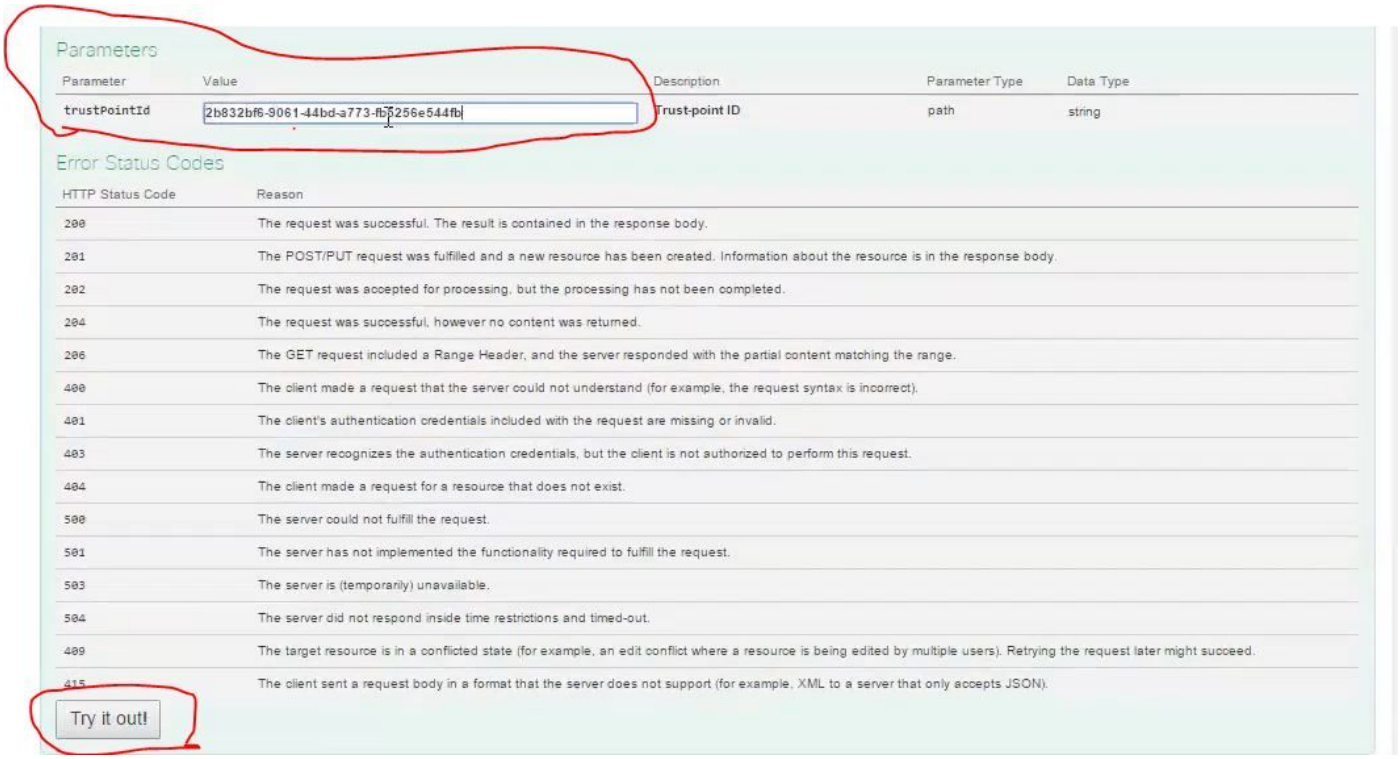
Poussez le certificat vers le périphérique.

POST/trust-point/{trustPointId} // trustPointId doit être copié à partir de la requête GET de numéro de série

{ « réponse » : { « 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 » }, « version » : « 1.0 » }

Cela poussera le certificat au périphérique, à condition qu'il y ait une connectivité correcte.





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!

Message de réussite de la réponse :

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"
}
```

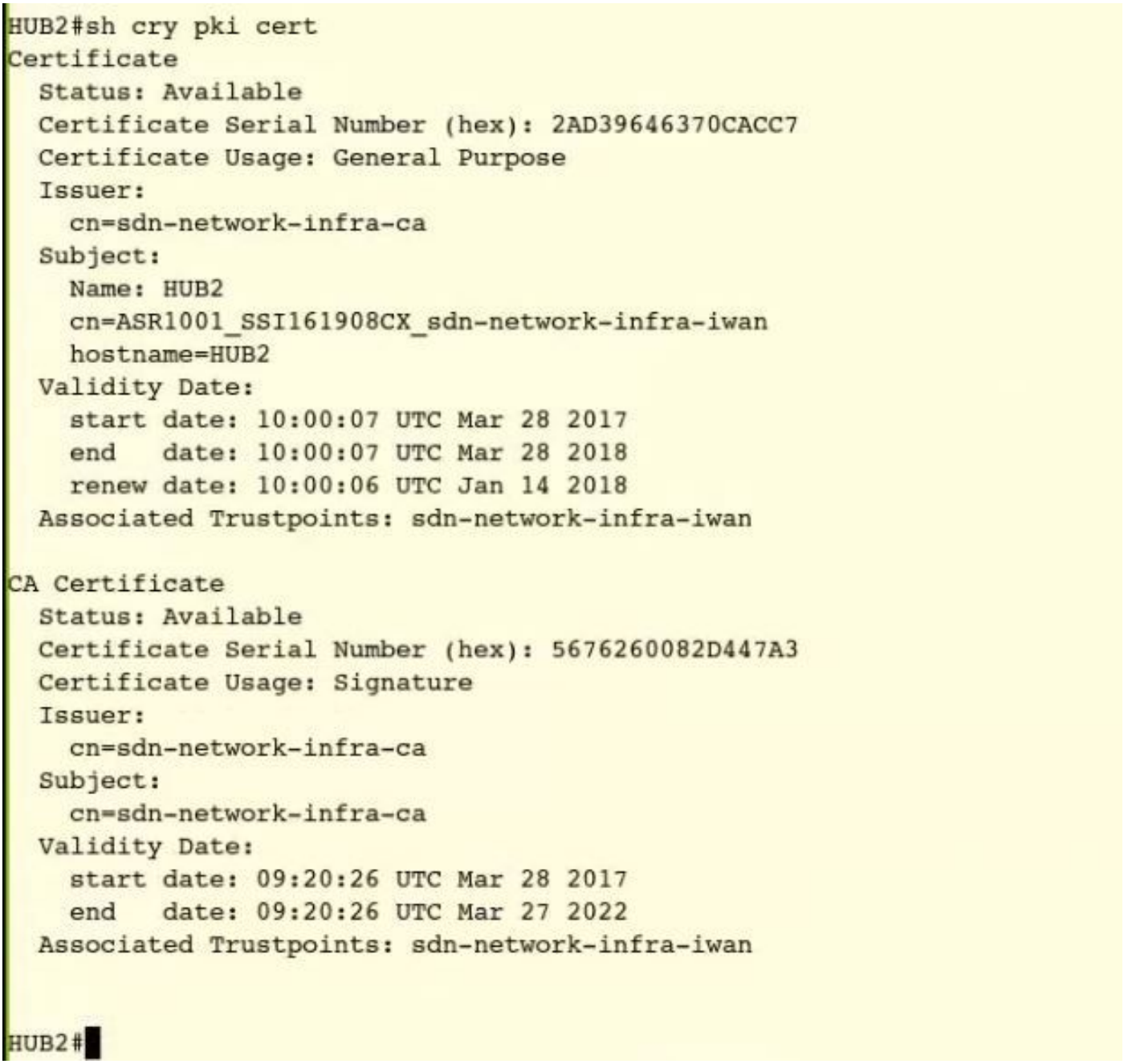
Response Code

```
202
```

Response Headers

Recheck on device :

Vous voyez que les deux certificats sont maintenant collés :



Le module APIC-EM possède parfois le certificat, mais pas le périphérique. Comment pouvez-vous le résoudre ?

Il existe une tâche en arrière-plan par laquelle vous pouvez supprimer le certificat de seulement APIC-EM.
Parfois, le client supprime par erreur le certificat du périphérique, mais dans le module APIC-EM, il est toujours présent.
Cliquez sur **SUPPRIMER.**

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

Entrez le numéro de série et cliquez sur **Try it out !**.