APIC-EM 1.3. - Generazione certificato - Eliminazione tramite API

Sommario

Introduzione

Questo documento descrive come utilizzare l'API Cisco Application Policy Infrastructure Controller (APIC) - Extension Mobility (EM) per creare - eliminare il certificato. Con IWAN, è tutto configurato automaticamente. Tuttavia, al momento IWAN non dispone di alcun flusso per il recupero automatico del dispositivo dal certificato scaduto.

La parte buona è che c'è una sorta di flusso nell'automazione in termini di RestAPI. Tuttavia, tale automazione è per dispositivo e necessita di alcune informazioni sul dispositivo. Il flusso RestAPI che è esterno al flusso IWAN, utilizza un meccanismo per automatizzare il certificato per il dispositivo.

Premesse

Topologia cliente standard.

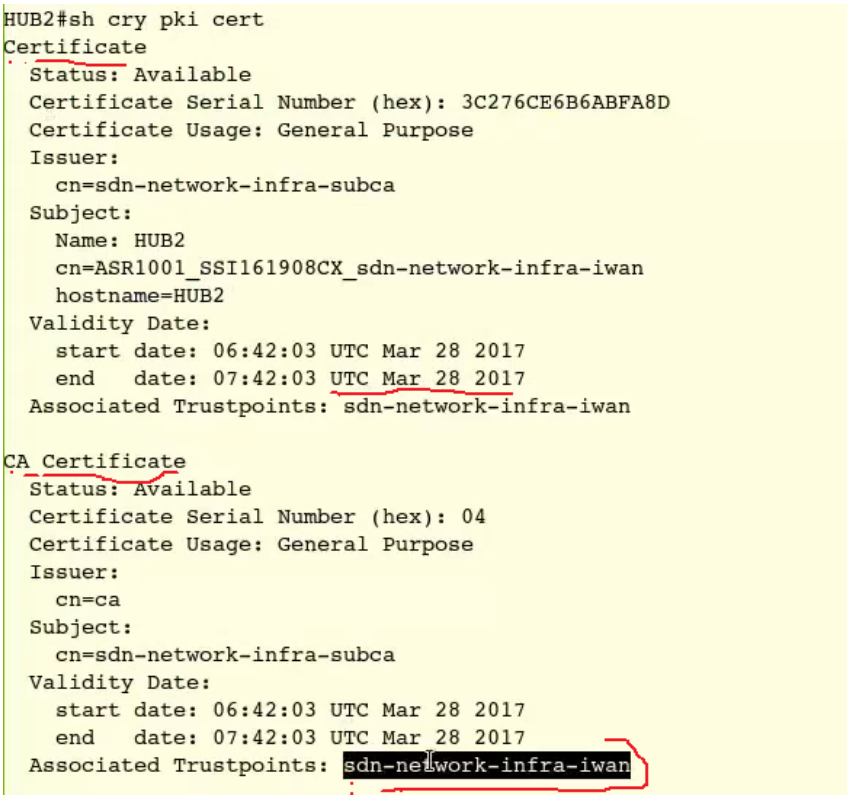
SPOKE — HUB — APIC_EM [Controller]

Queste sono le tre situazioni:

- Il certificato è scaduto.
- Il certificato non è in corso di rinnovo.
- Certificato non disponibile.

In che modo è possibile conoscere lo stato corrente del dispositivo?

Eseguire il 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
```

In questo caso sono presenti due certificati ed è necessario controllare il punto di attendibilità associato.

La data di fine è in genere un anno e deve essere successiva alla data di inizio.

Se si tratta di sdn-network-infra-iwan, significa da APIC-EM che si dispone di ID e certificato CA registrato.

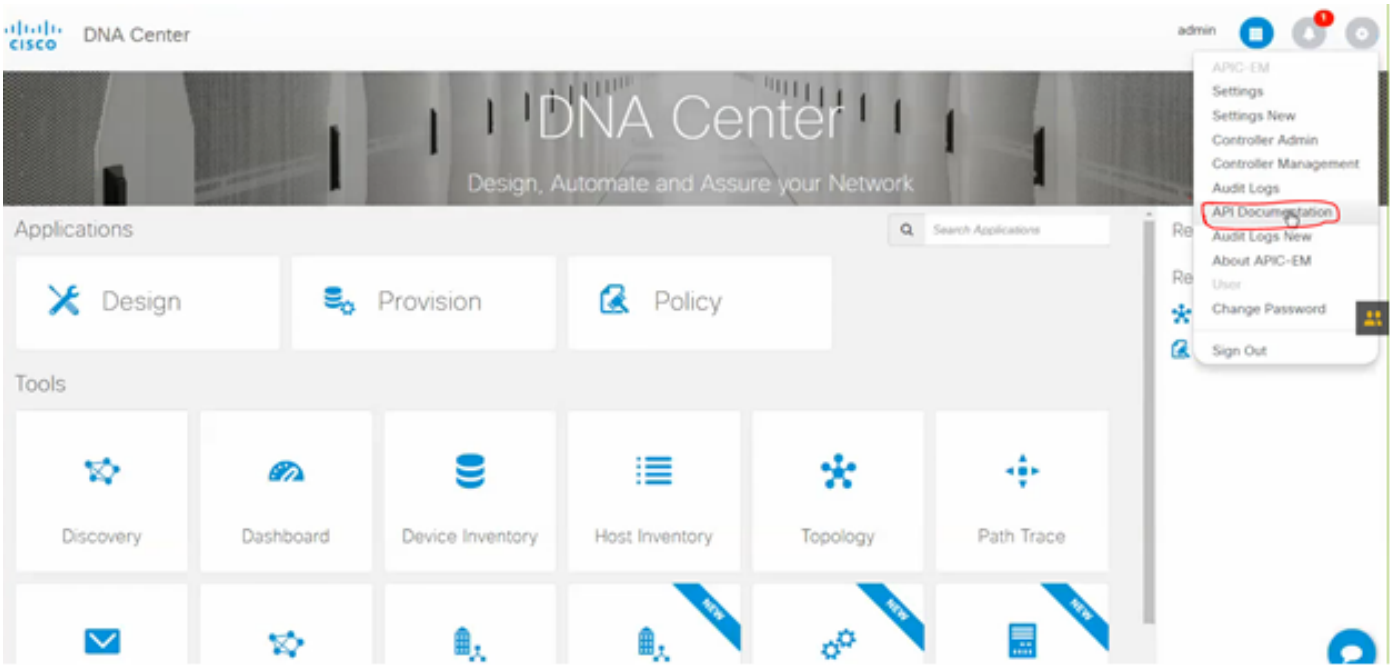
Come è possibile accertarsi che APIC-EM abbia lo stesso certificato o che APIC-EM abbia riconosciuto lo stesso certificato?

r. Mostra versione dal dispositivo e raccogli il numero di 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
```

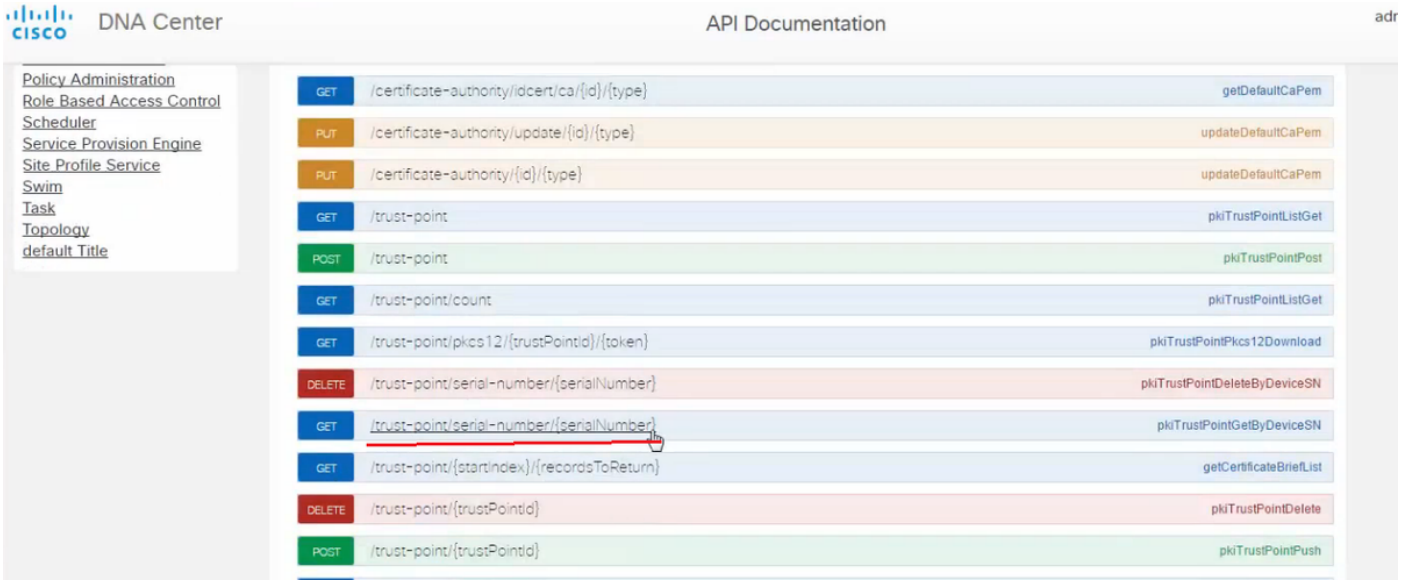
Con l'aiuto di questo numero di serie è possibile eseguire una query APIC-EM per scoprire cosa pensa APIC-EM di questo dispositivo.

b. Passare a Documentazione API.



c. Fare clic su Public Key Infrastructure (PKI) Broker.

d. Fare clic su First API (Prima API) per conoscere lo stato dal lato API.



Fare clic su **GET.**

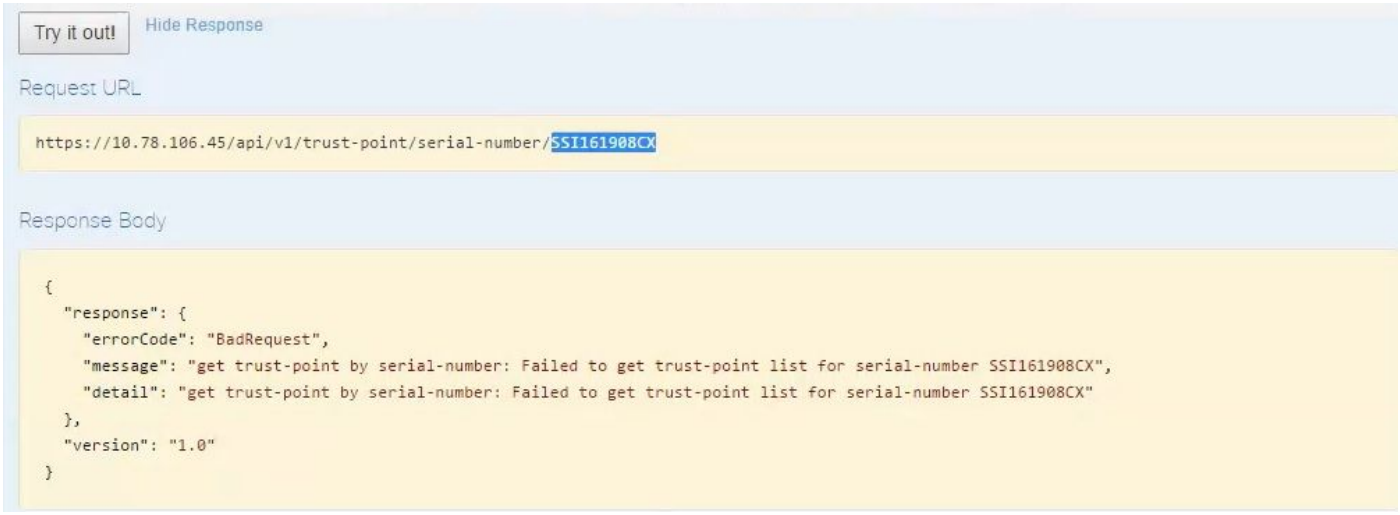
Selezionare una casella di controllo per selezionare il numero di serie raccolto dall'output show version del dispositivo.

Fai clic su **Prova!**.

Confrontare il valore di output con l'output del **certificato PKI crp sh** del dispositivo.

Come eliminare il certificato dal dispositivo?

A volte accade che sul dispositivo, il certificato sia presente e nell'APIC-EM non lo sia. Ecco perché, quando si esegue **GET API** viene visualizzato un messaggio di errore.



La soluzione è una sola, ovvero eliminare il certificato dal dispositivo:

r. **N. switch show run | I trustpoint**

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

Eseguire il comando **Switch# no crypto pki trustpoint <nome trust point>.**

```
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)#
```

Con questo comando vengono eliminati tutti i certificati nel dispositivo associati al trust point selezionato.

Ricontrolla se il certificato è stato eliminato.

Utilizzare il comando: **Switch# sh cry certificato pki.**

Non deve visualizzare il trust point sdn eliminato.

b. Eliminazione della chiave:

Esegui comando sul dispositivo: **Switch# sh cry key mypubkey all.**

In questo esempio il nome della chiave inizia con **sdn-network-infra**.

Comando per eliminare la chiave:

```
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. Accertarsi che l'interfaccia APIC-EM collegata al dispositivo sia di tipo Pingable.

Può succedere che APIC-EM abbia due interfacce, una pubblica e l'altra privata. In tal caso, verificare che l'interfaccia APIC-EM che comunica tra loro con il dispositivo esegua il ping.

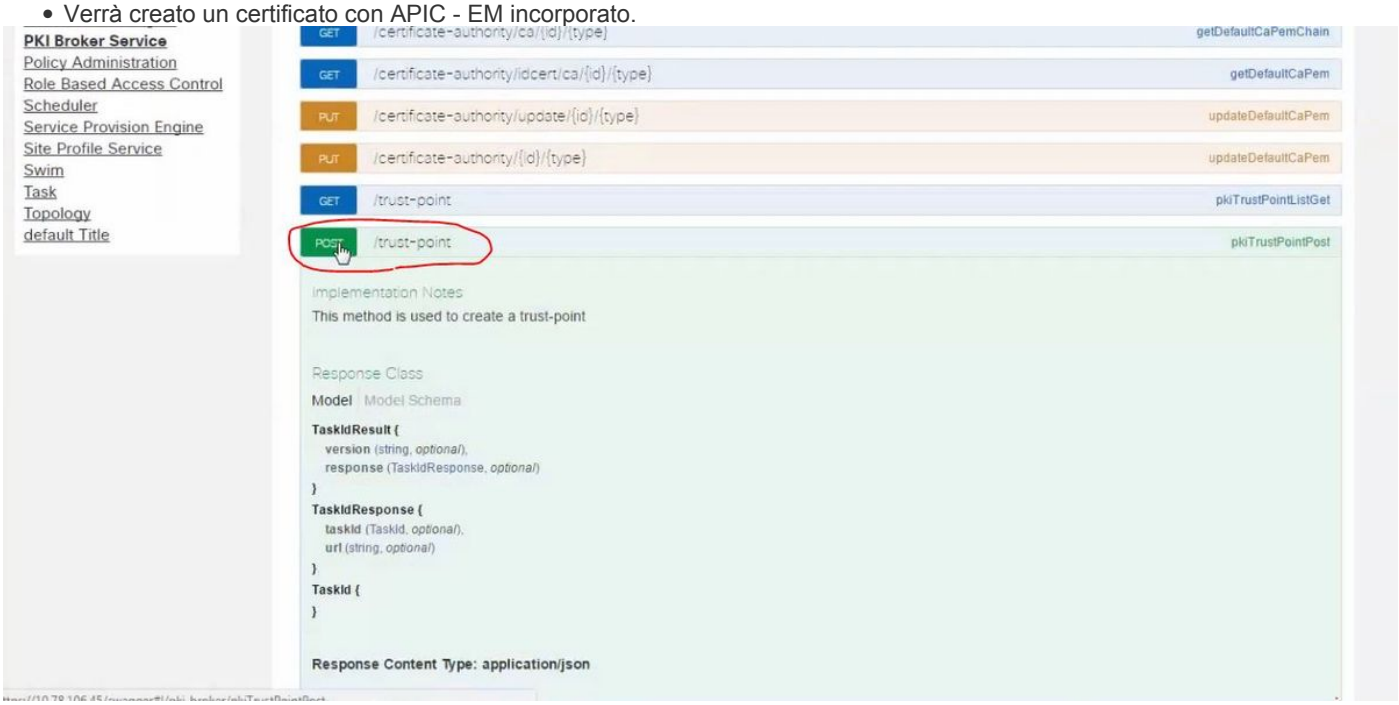
```
HUB2#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HUB2#
```

Come applicare un certificato da APIC - EM?

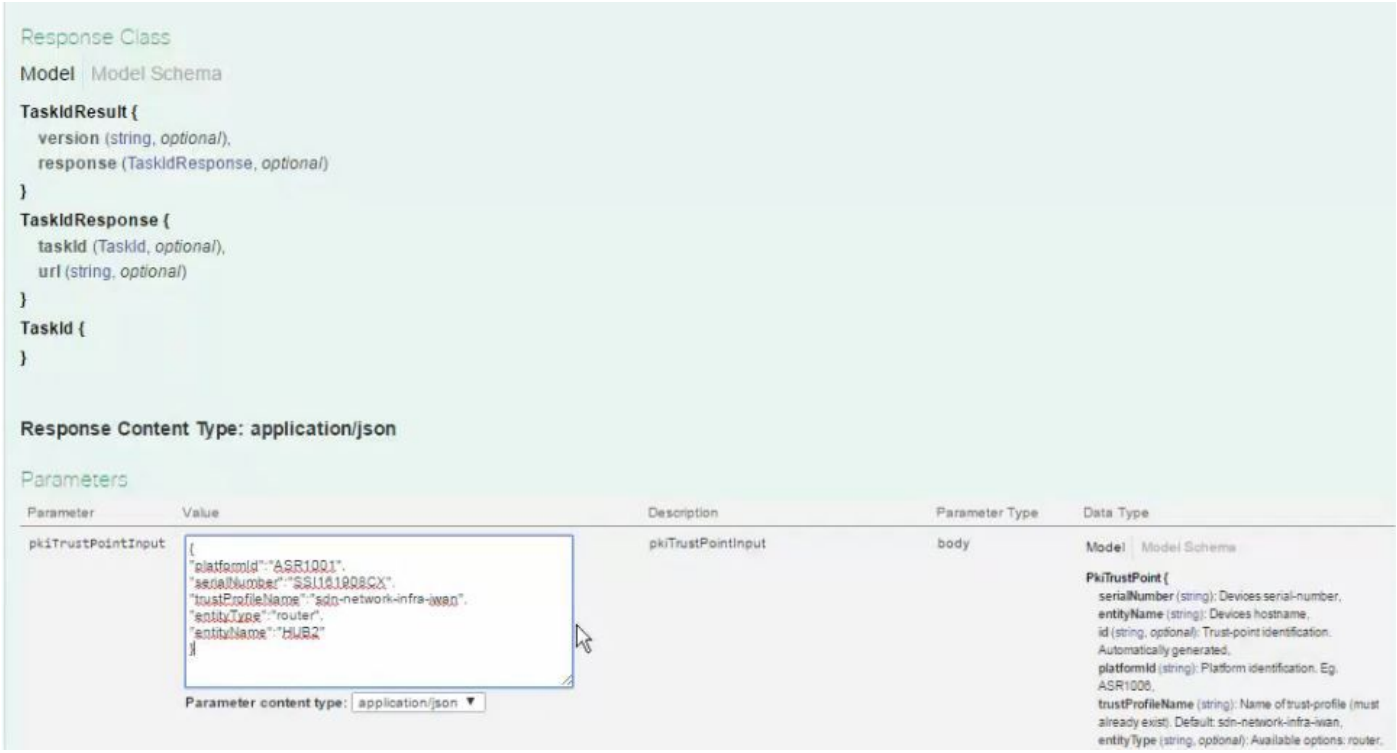
In APIC-EM questa opzione è disponibile quando si fa clic su Documentazione API e si seleziona Broker PKI.

POST/trust-point

- Verrà creato un certificato con APIC - EM incorporato.



Quindi è necessario avere le informazioni sul dispositivo e fare clic su prova.

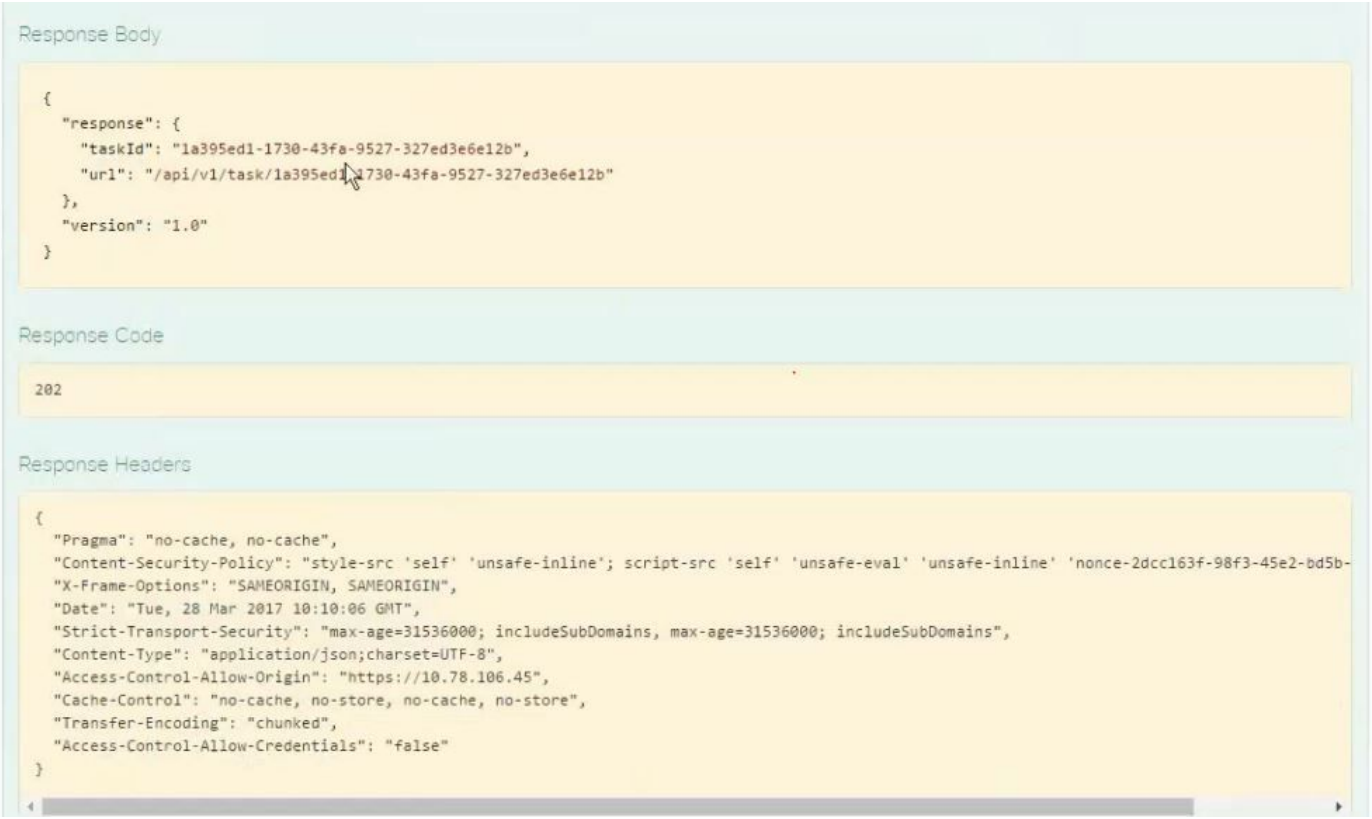


Esempio:

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

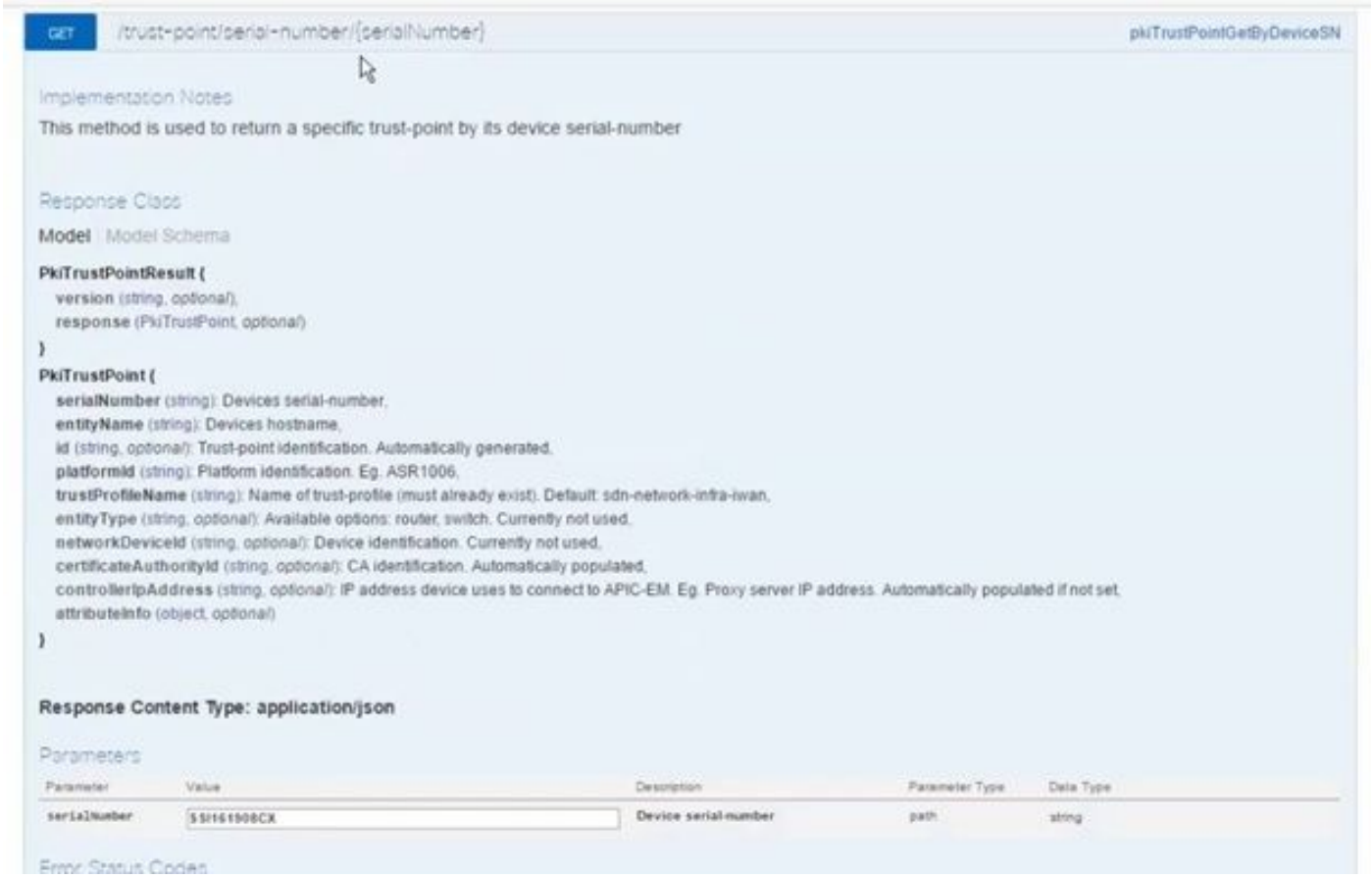
- Le informazioni evidenziate sono STATIC e il resto Dynamic.
- Il nome entità è il nome host del dispositivo.
- Numero di serie ottenuto dalla versione show del dispositivo.
- Tipo di entità che è possibile modificare in base al tipo di dispositivo.
- Queste informazioni sono necessarie per indicare ad APIC-EM di configurare il dispositivo. Qui APIC-EM comprende il numero di serie.

Output di Prova!:



Questo output indica che il file viene creato internamente da APIC-EM ed è pronto per essere distribuito sul dispositivo.
Il passo successivo è spingere questo dispositivo nel pacchetto. Per eseguire il push, è necessario ottenere l'ID del trust point. Questa operazione può essere eseguita tramite GET API CALL.

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



Vi darà questo output. Significa che l'APIC-EM ha il certificato con cui eseguire il push sul 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

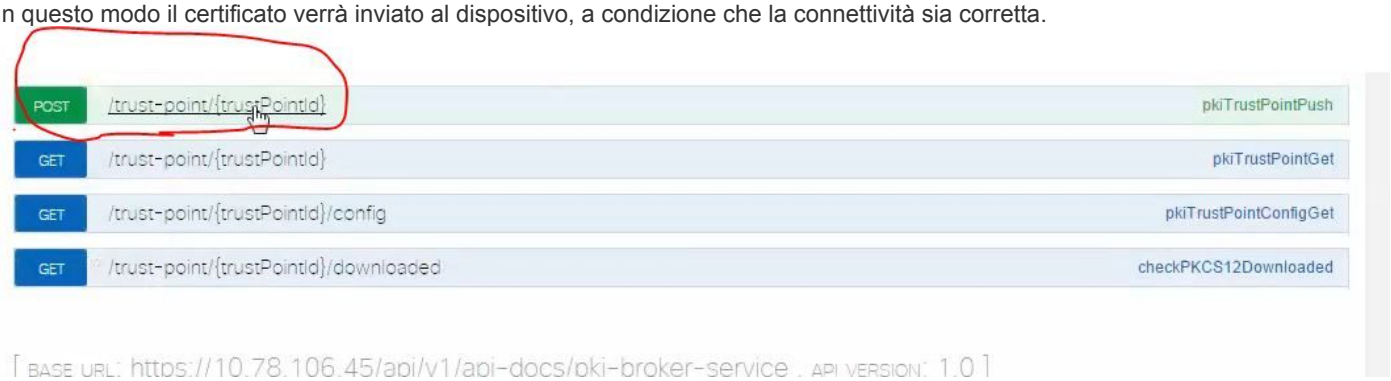
```
200
```

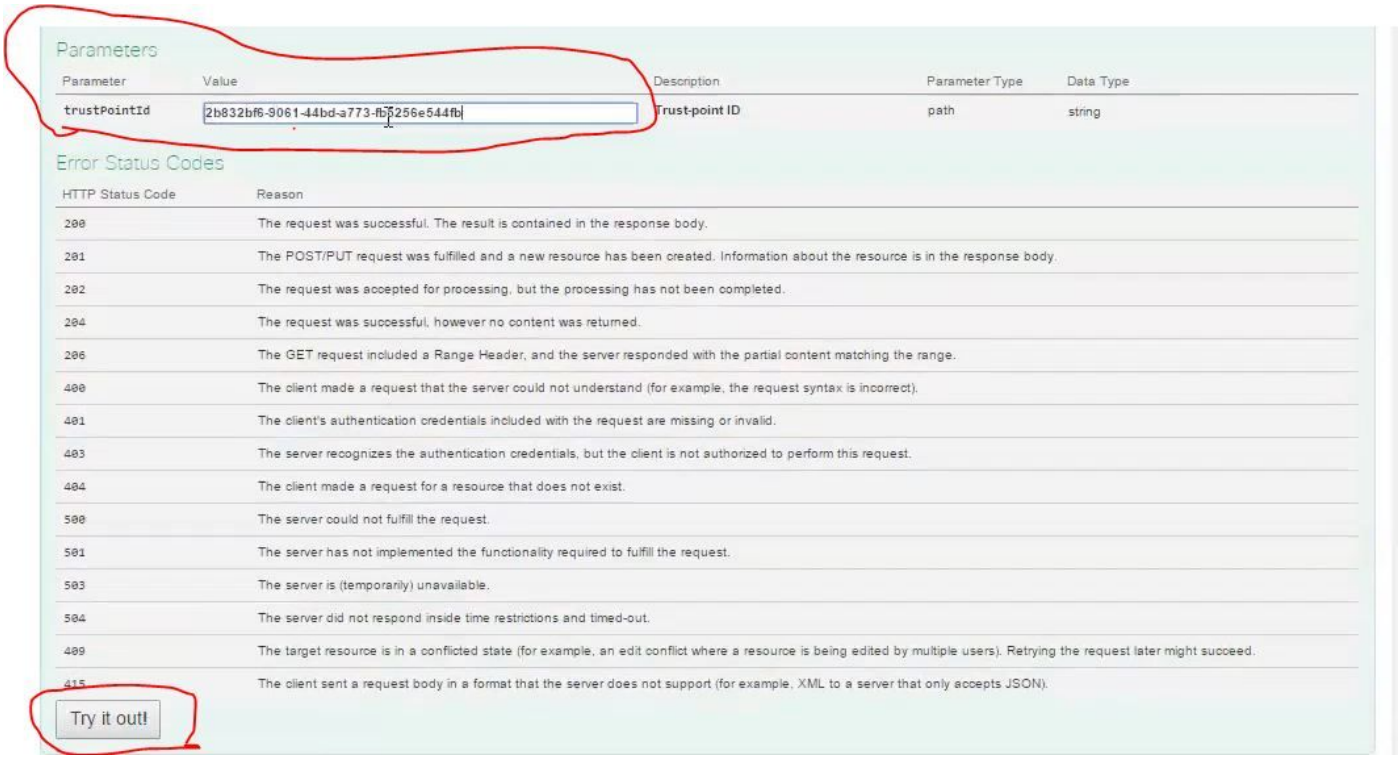
Eseguire il push del certificato nel dispositivo.

POST/trust-point/{trustPointId} // trustPointId deve essere copiato da GET Serial Number Query

{ "risposta": { "ID piattaforma": "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" }, "versione": "1,0" }

In questo modo il certificato verrà inviato al dispositivo, a condizione che la connettività sia corretta.





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!

Messaggio di risposta riuscita:

Try it out! Hide Response

Request URL

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

Response Body

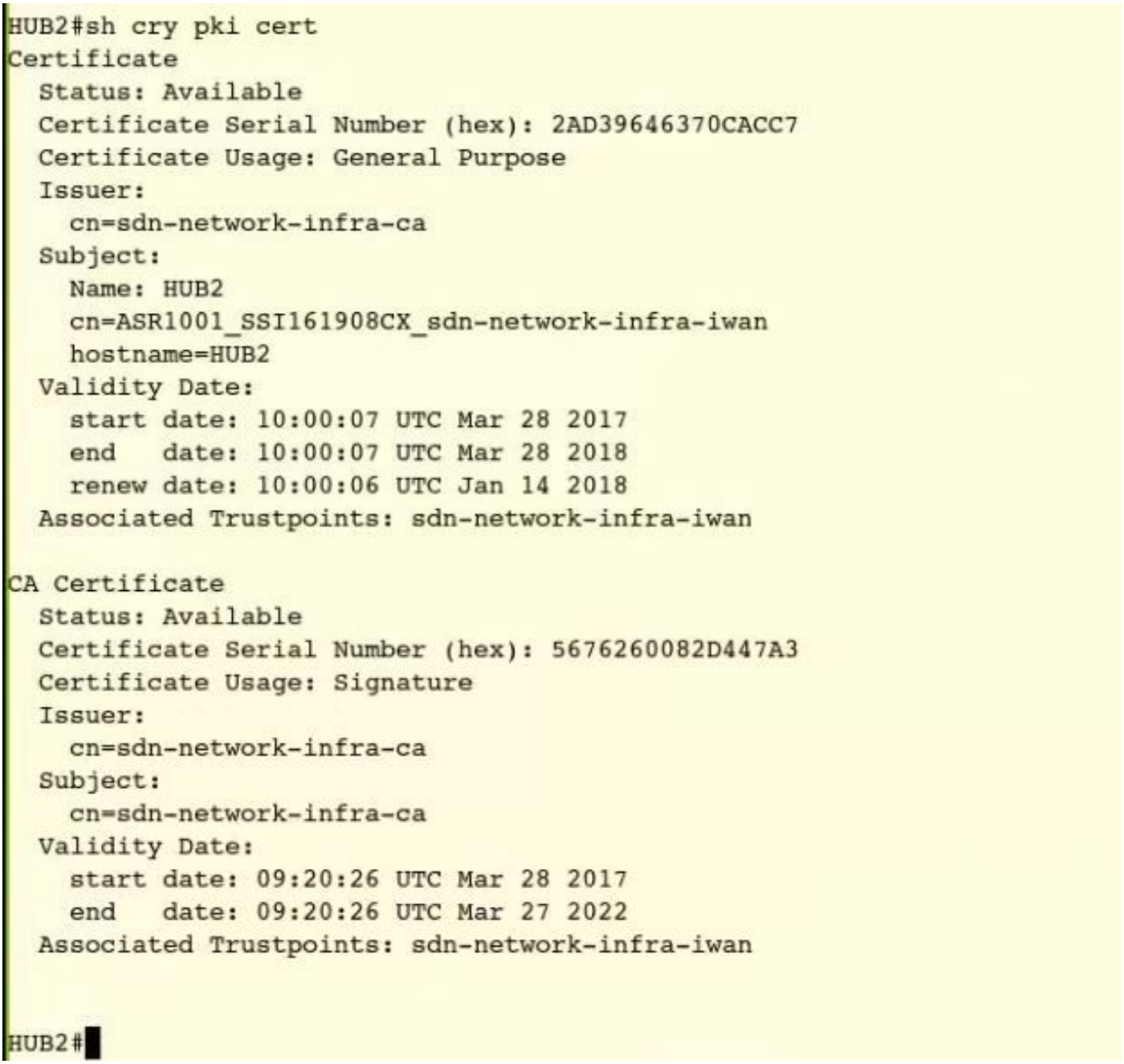
```
{
  "response": {
    "taskId": "f10022bd-8f45-4597-8160-bcc07fd55898",
    "url": "/api/v1/task/f10022bd-8f45-4597-8160-bcc07fd55898"
  },
  "version": "1.0"
}
```

Response Code

```
202
```

Response Headers

Ricontrolla sul dispositivo:
Entrambi i certificati vengono incollati:



A volte APIC-EM dispone del certificato, ma il dispositivo no. Come puoi risolverlo?

Èpresente un'attività in background attraverso la quale è possibile eliminare il certificato solo da APIC-EM.
Talvolta il cliente elimina per errore il certificato dal dispositivo, ma in APIC-EM è ancora presente.
Fare clic su **DELETE.**

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

Immettere il numero di serie e fare clic su **Prova!**.