APIC-EM 1.3. — 證書生成 — 通過API刪除

目錄

簡介
背景資訊
您將如何瞭解裝置的當前狀態？
如何確保APIC-EM是否也擁有相同的證書，或者APIC-EM是否瞭解相同的證書？
如何從裝置中刪除證書？
如何應用APIC - EM的證書？
有時APIC-EM有證書，但裝置沒有。您如何解決此問題？

簡介

本檔案介紹如何使用思科應用程式原則基礎架構控制器(APIC) — 延伸行動化(EM)API建立 — 刪除憑證。使用IWAN時，一切都自動配置。但是，目前IWAN沒有任何流量從過期證書中自動恢復裝置。

在RestAPI方面，自動化也有一些流程。但是，這種自動化是按裝置進行的，它需要裝置上的某些資訊。RestAPI流在IWAN流之外，它使用某種機制來自動化裝置的證書。

背景資訊

通常的客戶拓撲。

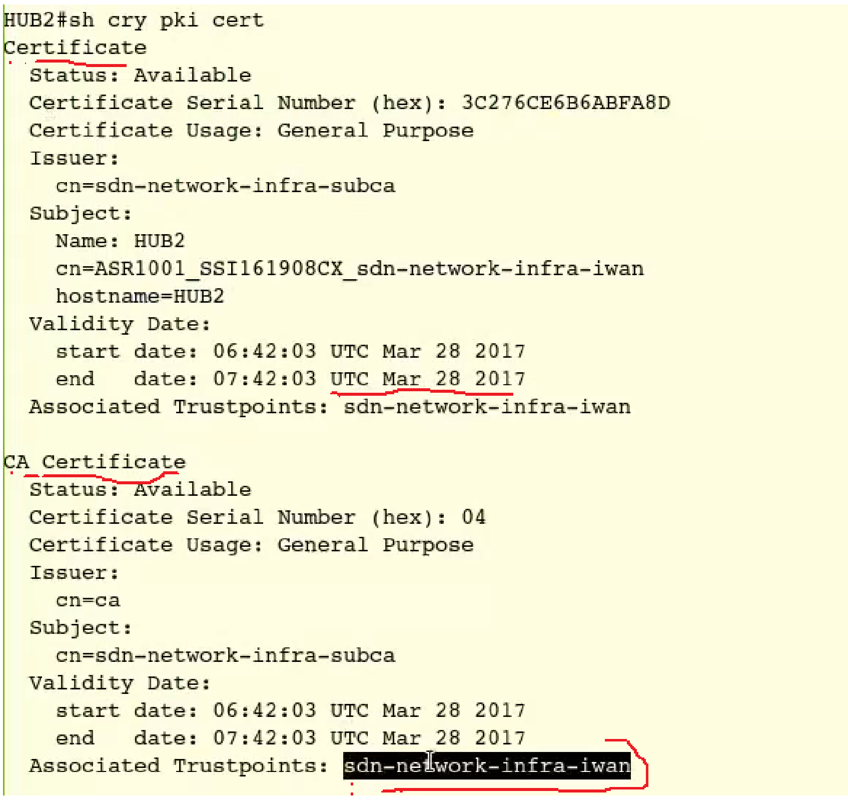
輻條 — 中心-----APIC_EM [控制器]

以下是三種情況：

- 證書已過期。
- 證書未續訂。
- 證書完全不可用。

您將如何瞭解裝置的當前狀態？

運行命令**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
```

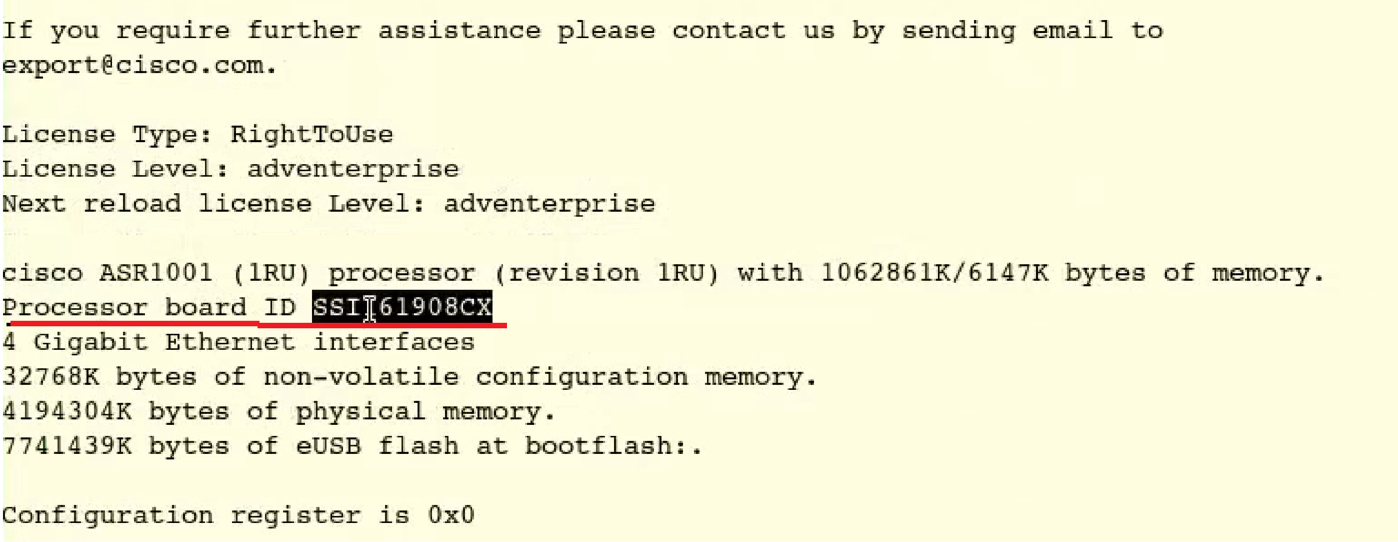
如果您看到，有兩個證書，此處您需要檢查關聯的信任點。

結束日期通常為一年且應大於開始日期。

如果是sdn-network-infra-iwan，則表示從APIC-EM中，您已註冊ID和CA證書。

如何確保APIC-EM是否也擁有相同的證書，或者APIC-EM是否瞭解相同的證書？

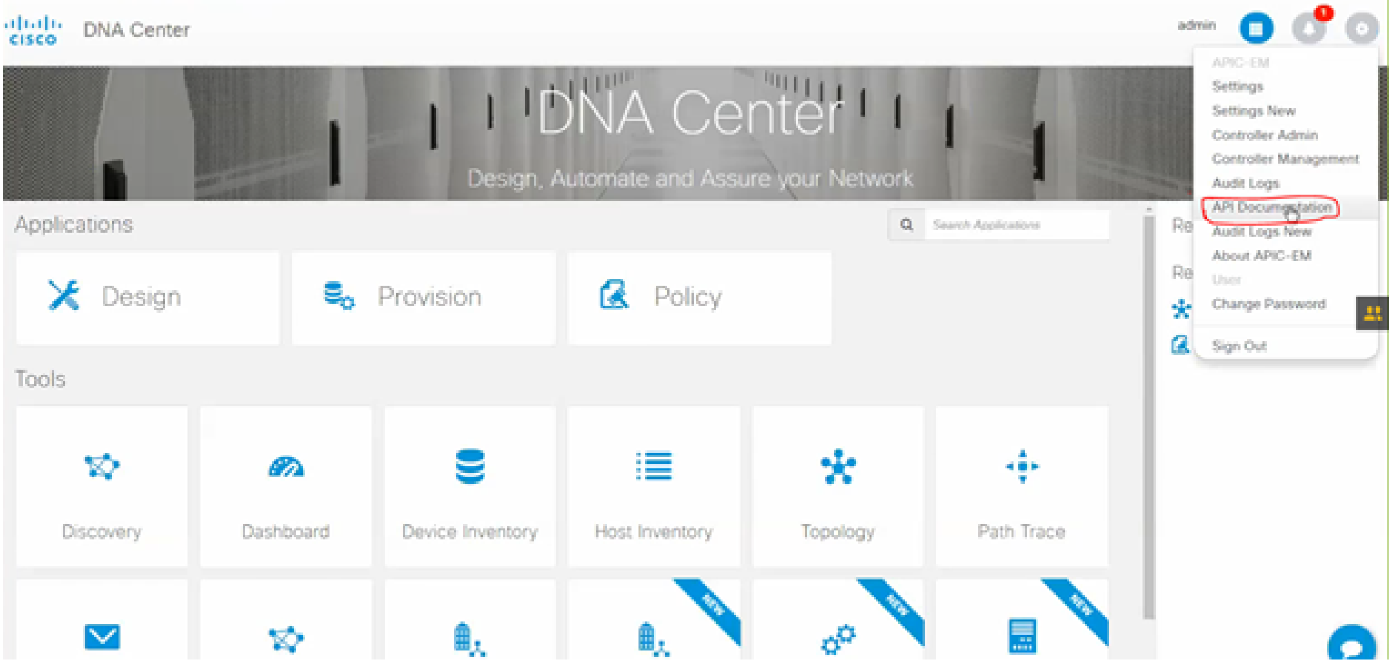
a.顯示裝置版本並收集序列號：



```
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
```

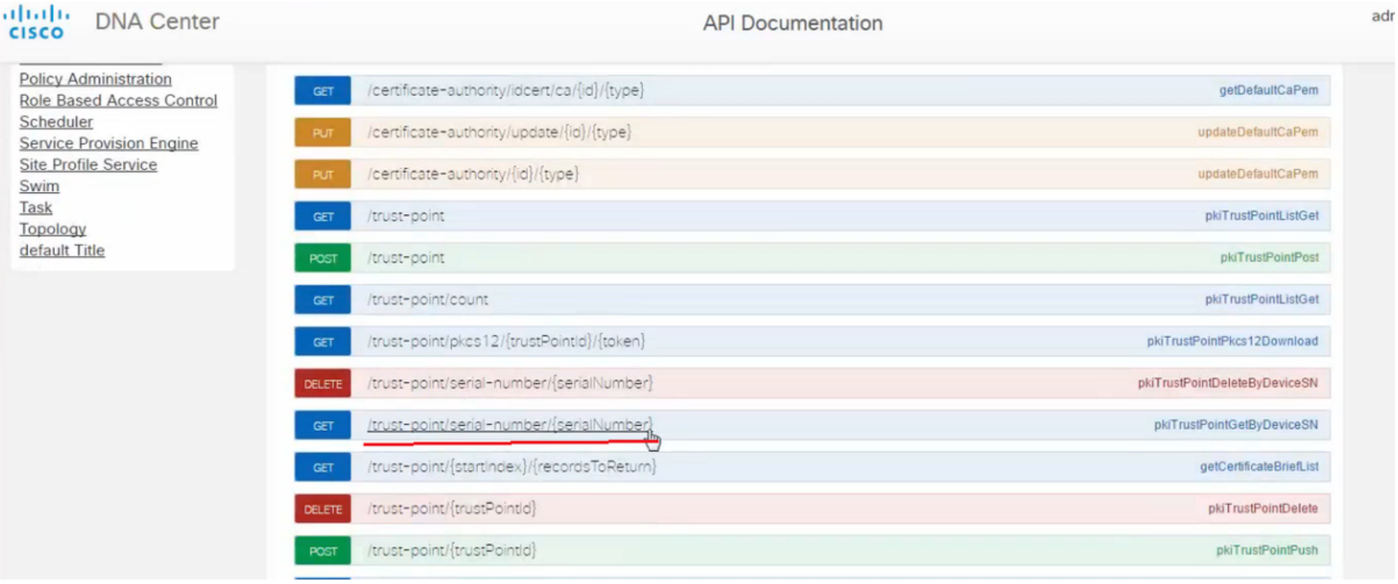
藉助此序列號，您可以執行APIC-EM查詢以瞭解APIC-EM對此裝置的看法。

b.導航到API文檔。



c.按一下Public Key Infrastructure(PKI)Broker。

d.按一下First API ，它將幫助我們從API端瞭解狀態。



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
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
GET	/trust-point/{startIndex}/{recordsToReturn}	getCertificateBriefList
DELETE	/trust-point/{trustPointId}	pkiTrustPointDelete
POST	/trust-point/{trustPointId}	pkiTrustPointPush

按一下**GET**。

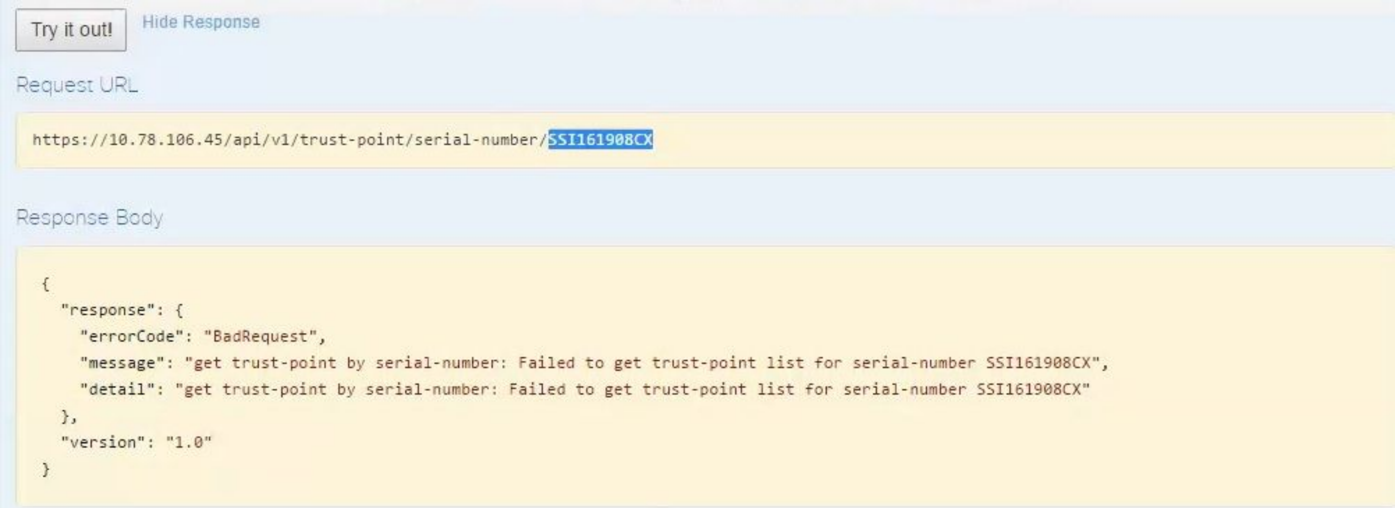
在一個覈取方塊中，點選從show version output of Device收集到的序列號。

按一下**Try it out!**。

將輸出值與裝置的**sh crp pki cert**輸出進行比較。

如何從裝置中刪除證書？

有時會發生以下情況：在裝置上，證書存在，而在APIC-EM中，證書不存在。因此，當您運行**GET API**時，會收到錯誤消息。



Request URL

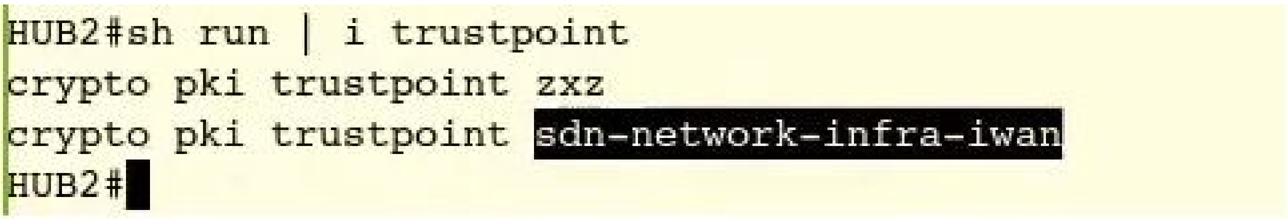
```
https://10.78.106.45/api/v1/trust-point/serial-number/SSI161908CX
```

Response Body

```
{
  "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"
}
```

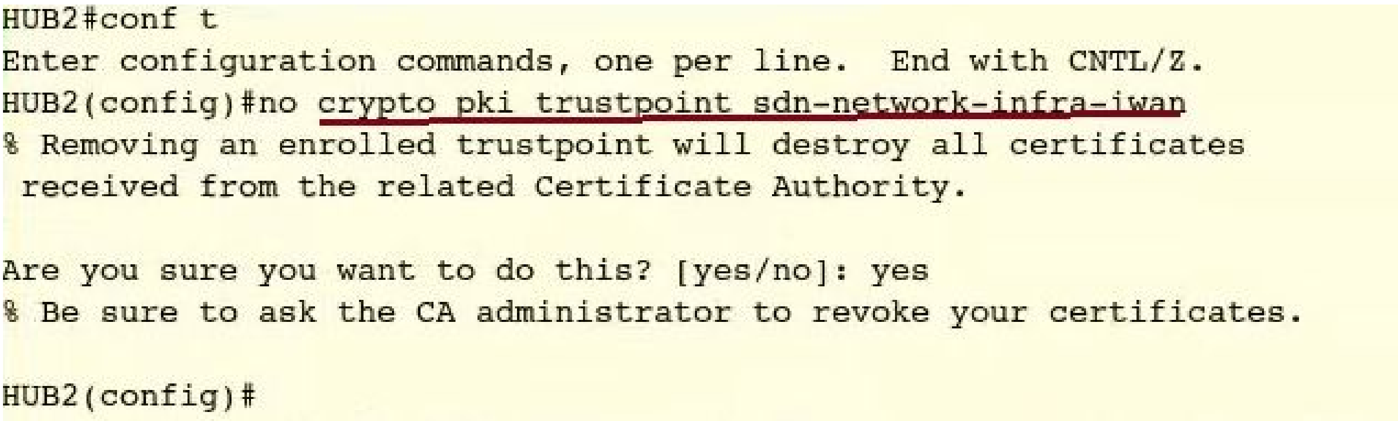
解決方案只有一個，即從裝置中刪除證書：

a.**Switch# show run | I信任點**



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

運行命令**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)#
```

此命令刪除與所選信任點關聯的裝置上的所有證書。

重新檢查證書是否已刪除。

使用命令:**Switch# sh cry pki cert。**

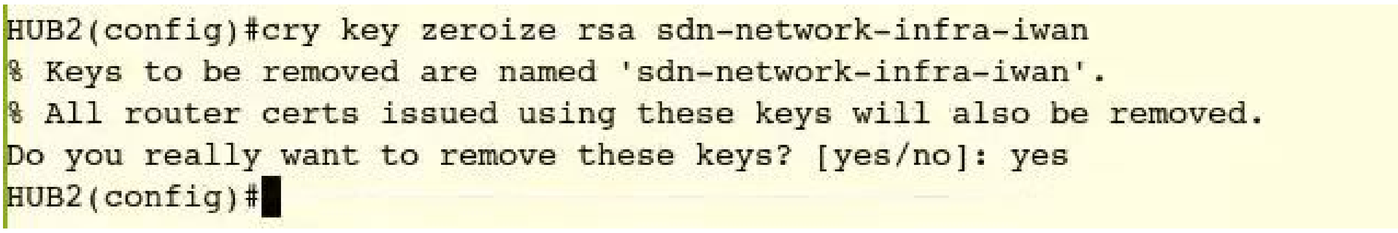
不應顯示已刪除的sdn信任點。

b.刪除金鑰：

在裝置上運行命令：**Switch# sh cry key mypubkey all。**

此處您會看到金鑰名稱以**sdn-network-infra**開頭。

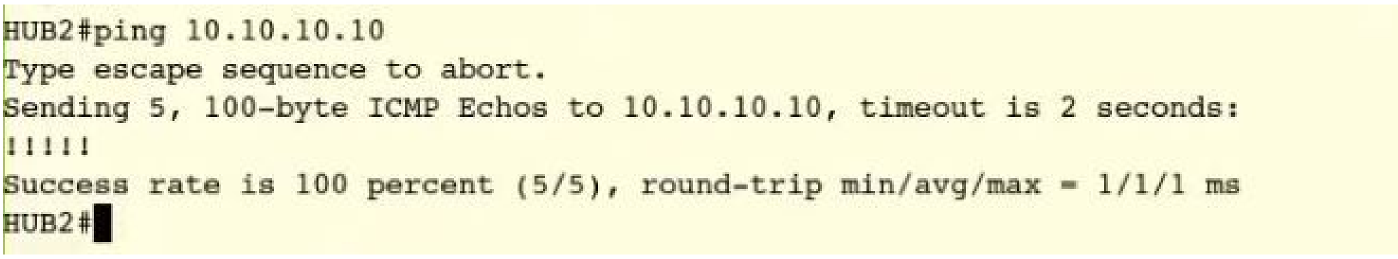
刪除金鑰的命令：



```
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.確保連線到裝置的APIC-EM介面應可執行Ping。

APIC-EM可能有兩個介面，其中一個是公共介面，另一個是專用介面。在這種情況下，請確保與裝置通訊的APIC-EM介面相互執行ping操作。



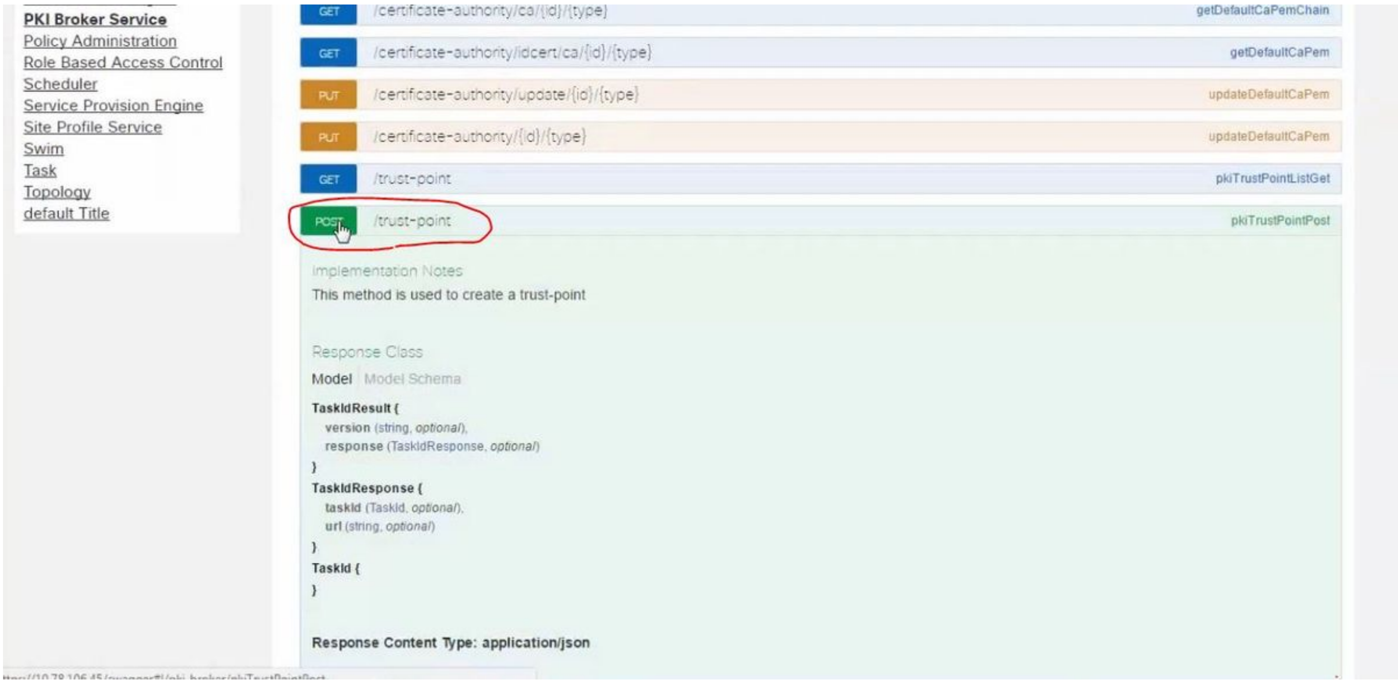
```
HUB2#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HUB2#
```

如何應用APIC - EM的證書？

在APIC-EM下，按一下API文檔並選擇PKI代理時，此選項可用。

POST/trust-point

- APIC - EM



```
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

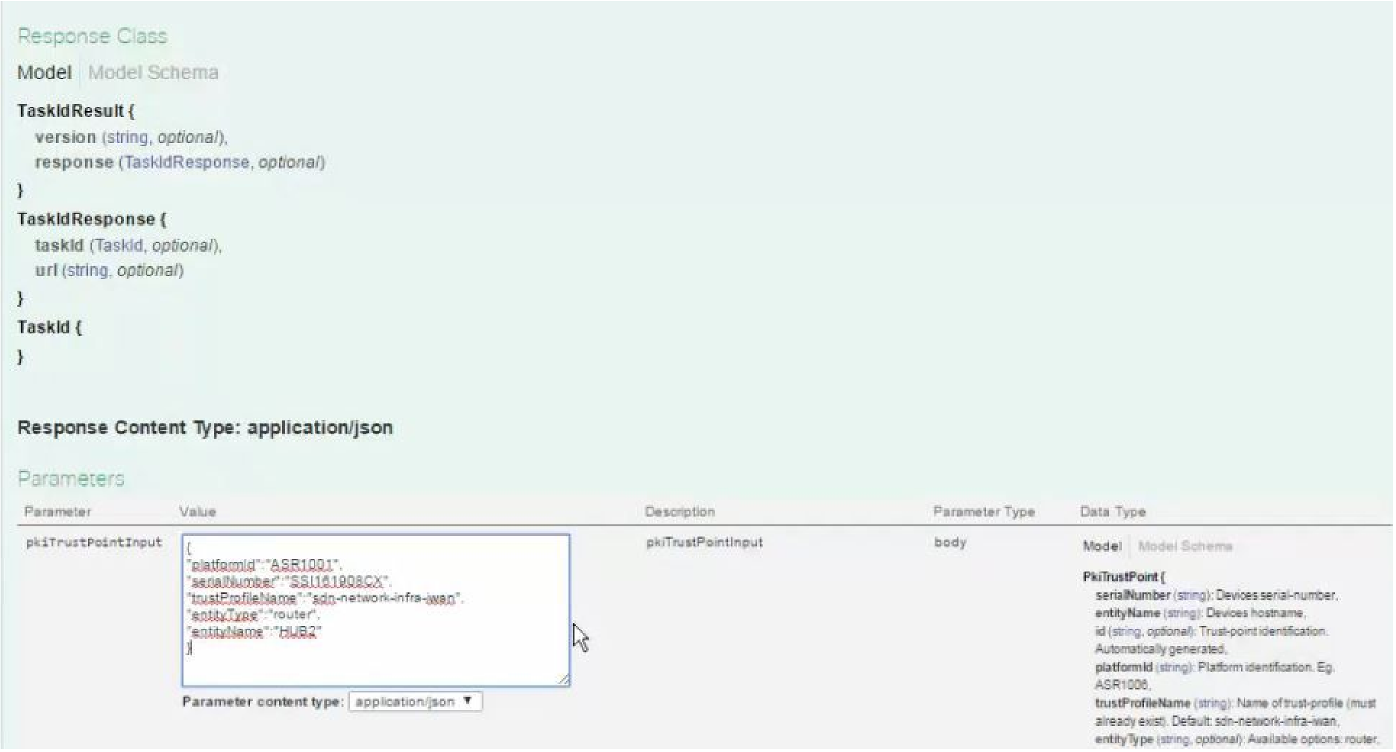
This method is used to create a trust-point

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



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

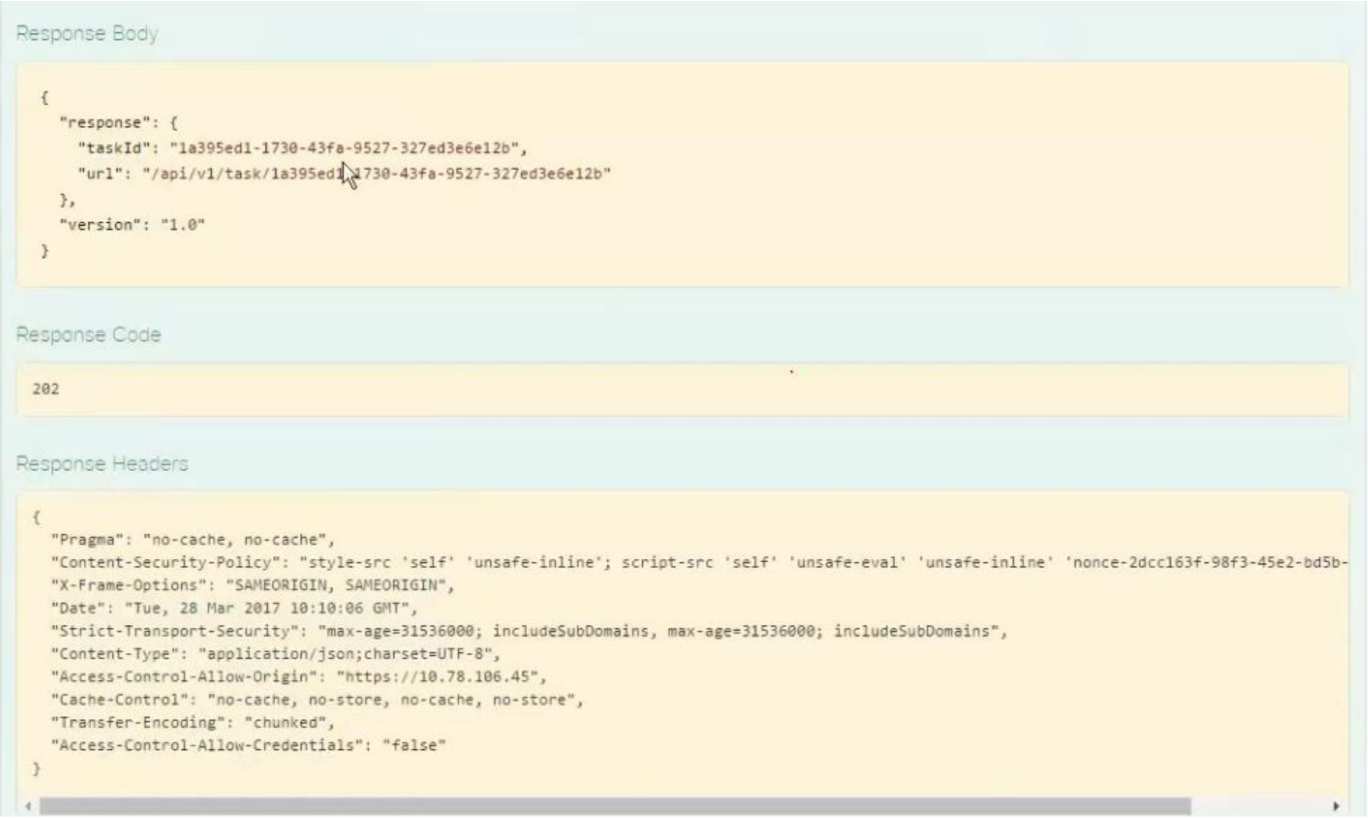
Parameter	Value	Description	Parameter Type	Data Type

pkiTrustPointInput	{
	"platformId":"ASR1001",
	"serialNumber":"SSI161908CX",
	"trustProfileName":"sdn-network-infra-iwan",
	"entityType":"router",
	"entityName":"HUB2"
	}
	Parameter content type: application/json ▼
		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. ASR1006,
				trustProfileName (string): Name of trust-profile (must already exist). Default: sdn-network-infra-iwan,
				entityType (string, optional): Available options: router,

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

- STATICDynamic
-
- show version of the device
-
- APIC-EMAPIC-EM

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

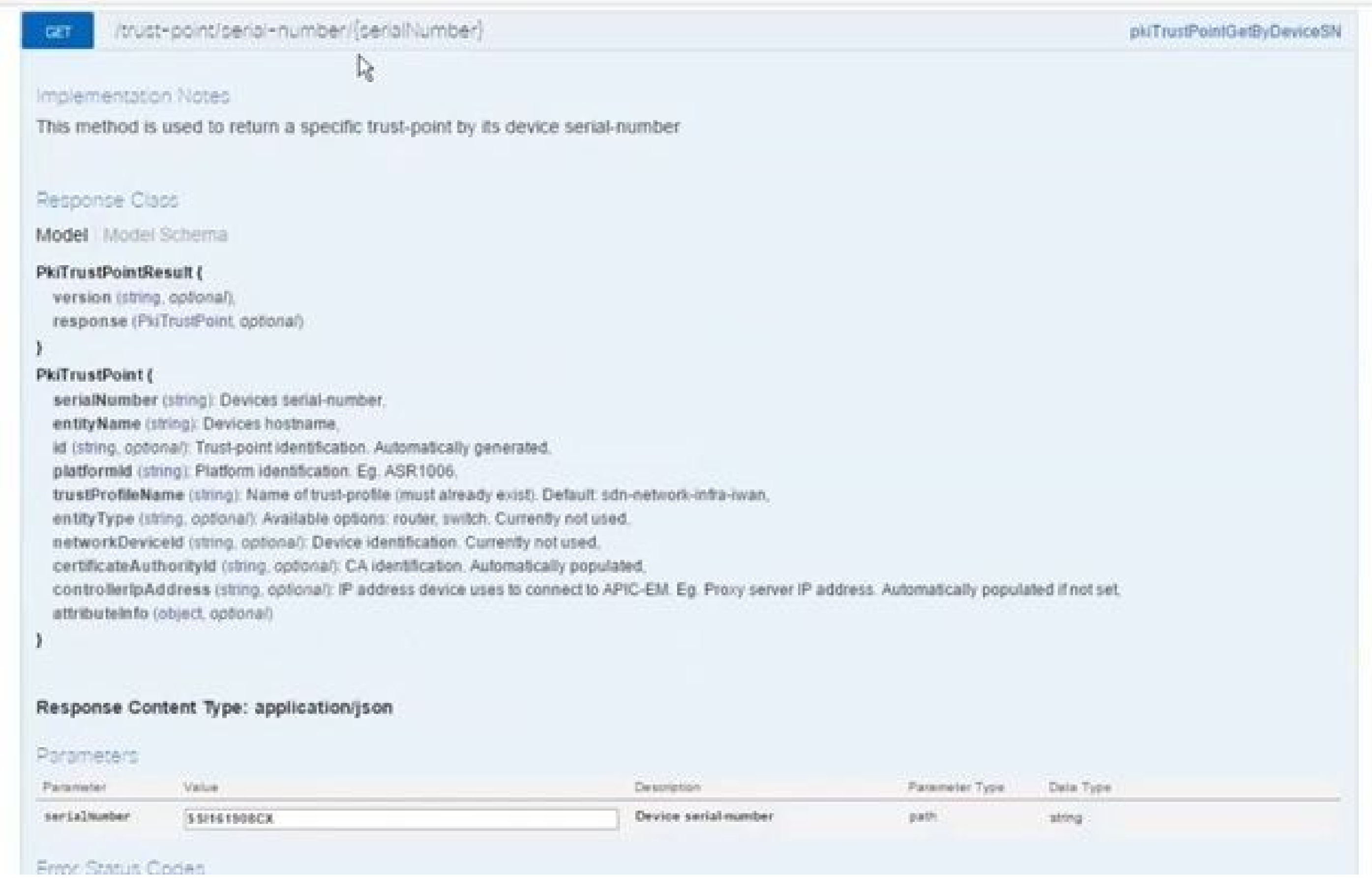
```
202
```

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"
}
```

APIC-EM
IDGET API CALL

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



/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)
}
```

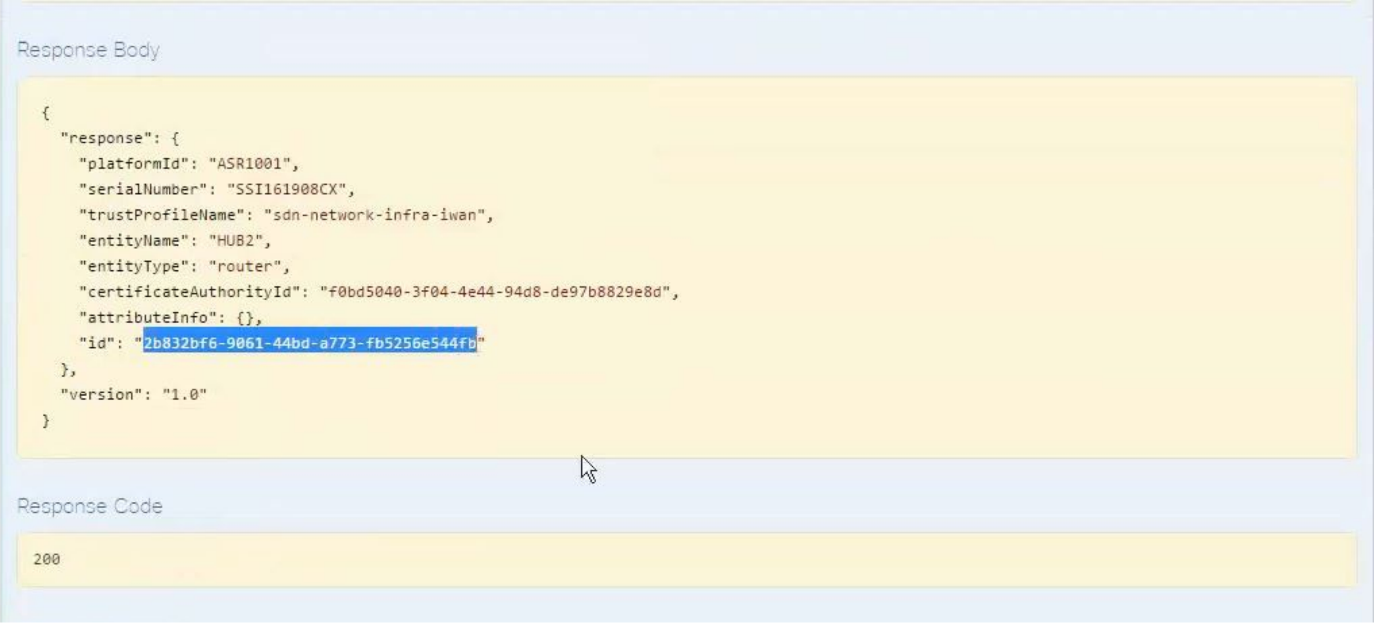
Response Content Type: application/json

Parameters

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

Error Status Codes

APIC-EM

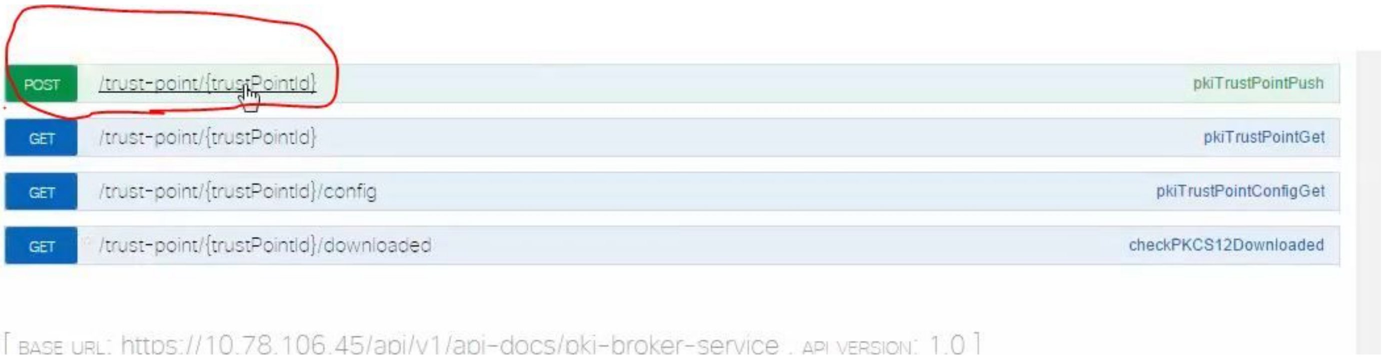


```
{
  "response": {
    "platformId": "ASR1001",
    "serialNumber": "SSI161908CX",
    "trustProfileName": "sdn-network-infra-iwan",
    "entityName": "HUB2",
    "entityType": "router",
    "certificateAuthorityId": "f0bd5040-3f04-4e44-94d8-de97b8829e8d",
    "attributeInfo": {},
    "id": "2b832bf6-9061-44bd-a773-fb5256e544fb"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

```
200
```

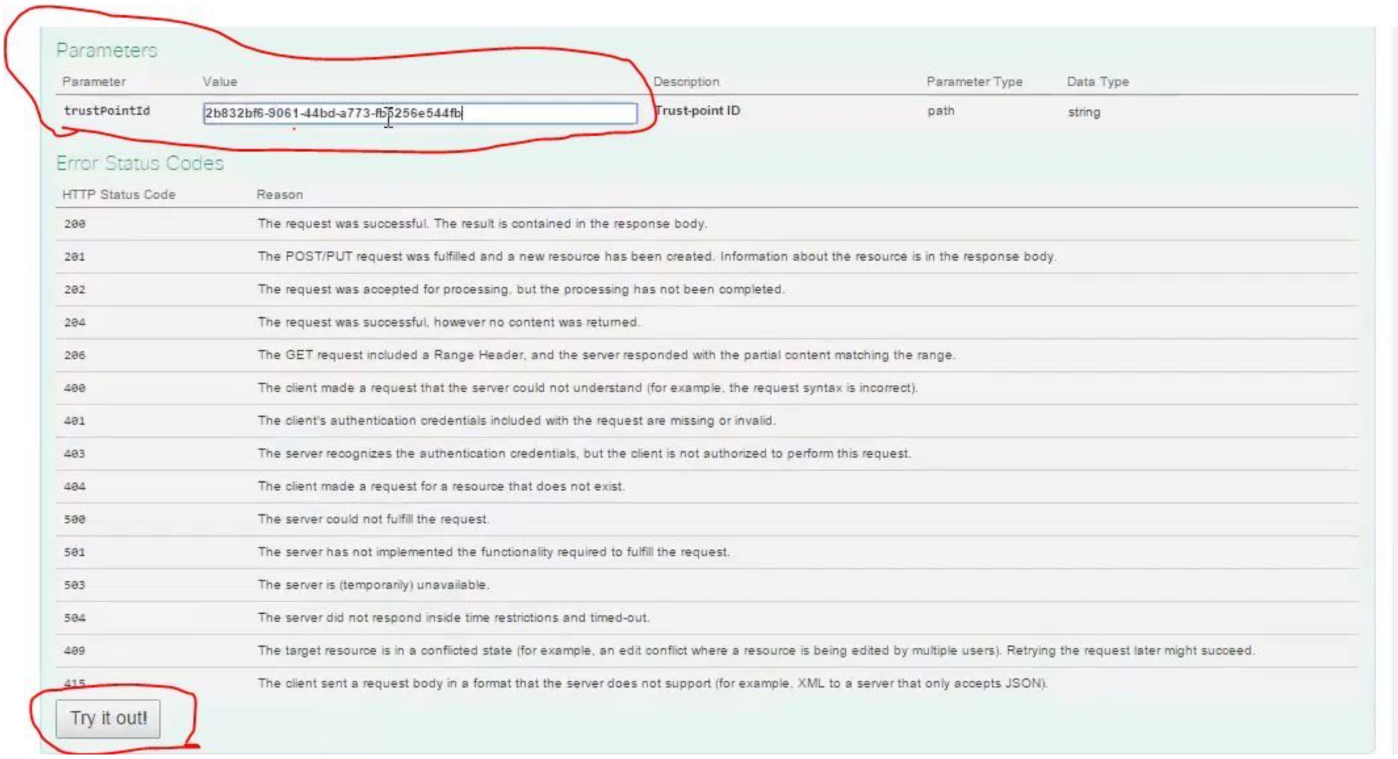
POST/trust-point/{trustPointId} // trustPointId需要從GET序列號查詢複製

{ "響應":{ "platformId":"ASR1001","序列號":"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" }



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]



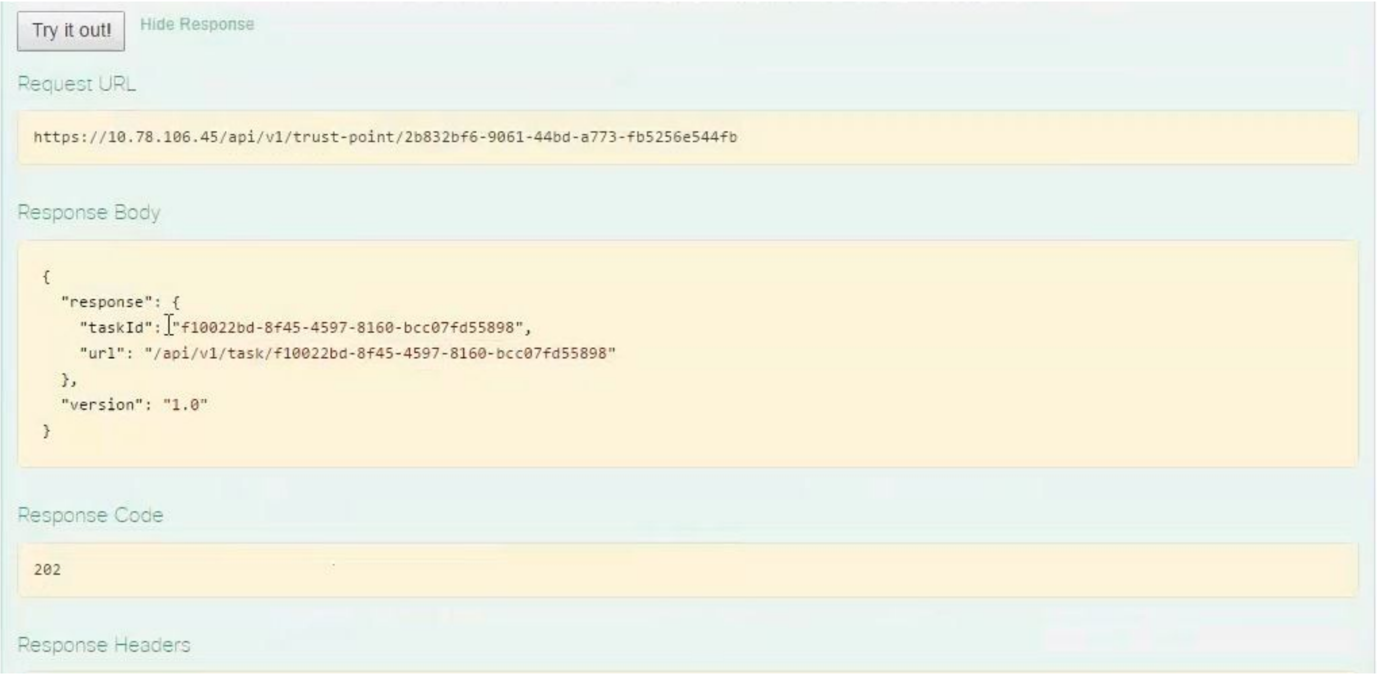
Parameters

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).

響應成功消息：



Request URL

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

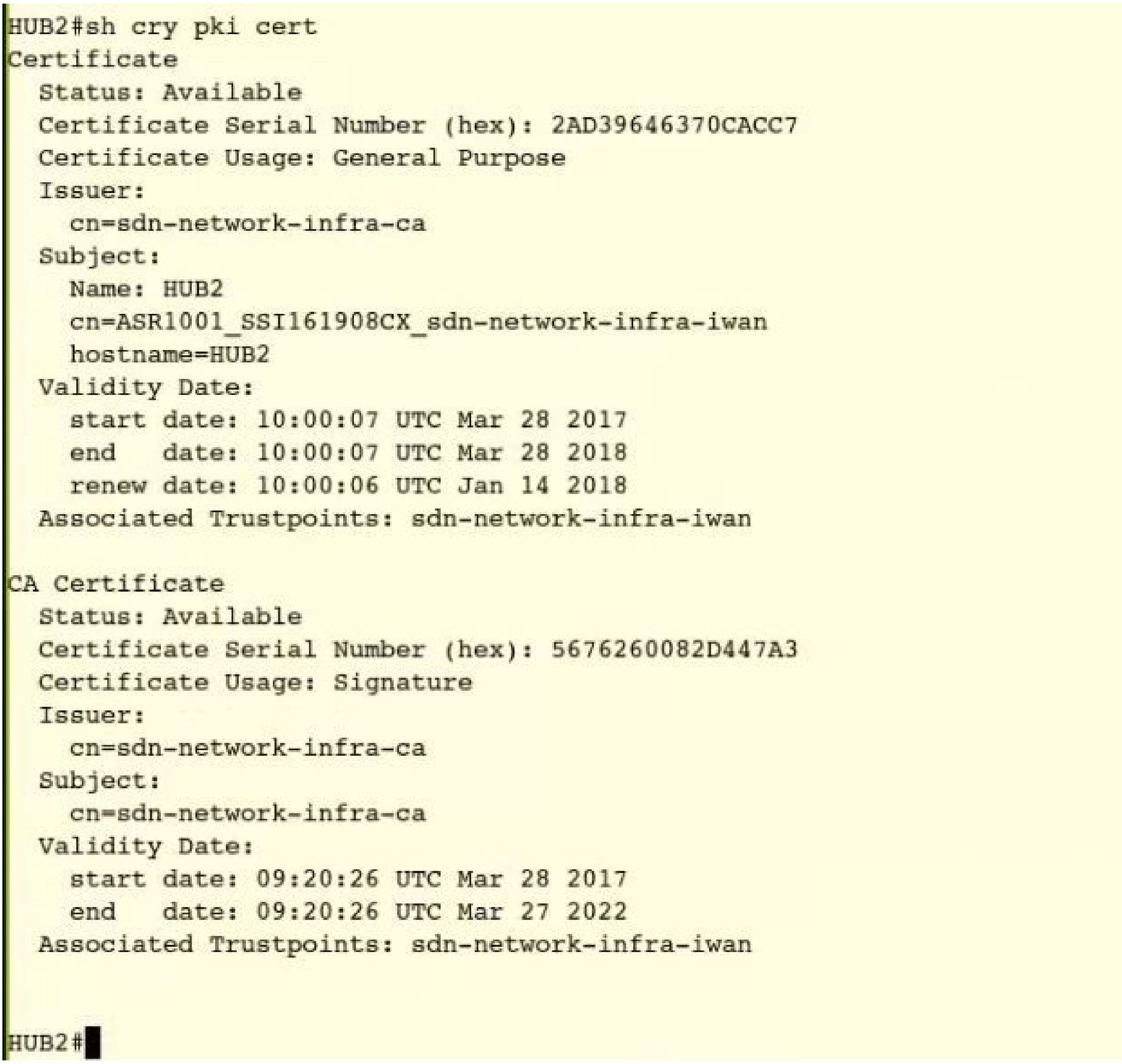
Response Body

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

Response Code

```
202
```

Response Headers

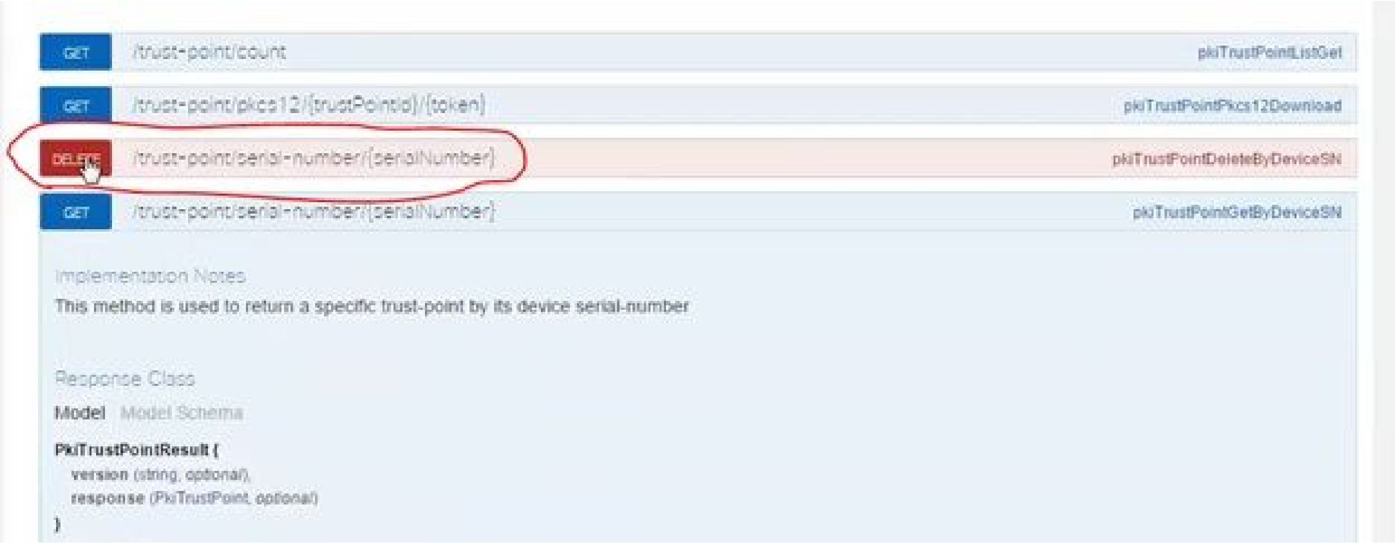


```
HUB2#sh cry pki cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 2AD39646370CACC7
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: HUB2
    cn=ASR1001_SSI161908CX_sdn-network-infra-iwan
    hostname=HUB2
  Validity Date:
    start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

有時APIC-EM有證書，但裝置沒有。您如何解決此問題？

APIC-EM
APIC-EM
DELETE

DELETE/trust-point/serial-number/{serialNumber} -刪除。



/trust-point/count

pkiTrustPointListGet

/trust-point/pkcs12/{trustPointId}/{token}

pkiTrustPointPkcs12Download

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

pkiTrustPointDeleteByDeviceSN

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

pkiTrustPointGetByDeviceSN

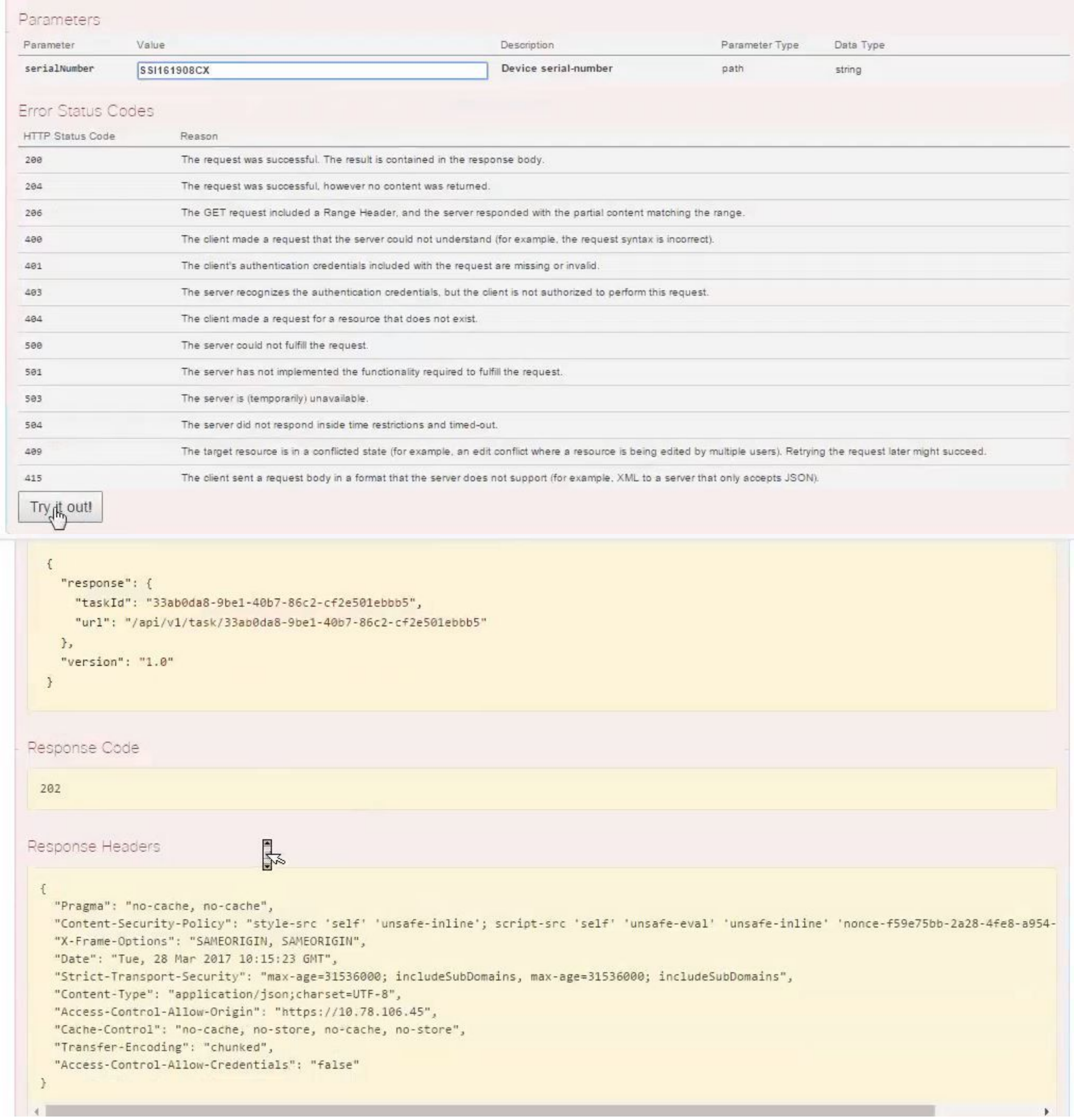
Implementation Notes

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

Response Class

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

Try it 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).

```
{
  "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"
}
```