APIC-EM 1.3. - 인증서 생성 - API를 통한 삭제

목차

소개

이 문서에서는 Cisco APIC(Application Policy Infrastructure Controller) - EM(Extension Mobility) API를 사용하여 인증서를 생성하고 삭제하는 방법에 대해 설명합니다.IWAN에서는 모두 자동으로 구성됩니다.그러나 현재 IWAN에는 만료된 인증서에서 자동으로 디바이스를 복구하는 흐름이 없습니다.

좋은 점은 RestAPI와 관련하여 자동화에 일종의 흐름이 있다는 것입니다.그러나 이러한 자동화는 장치별로 이루어지며 장치에 대한 일부 정보가 필요합니다. IWAN 흐름 외부에 있는 RestAPI 흐름에서는 일부 메커니즘을 사용하여 장치용 인증서를 자동화합니다.

배경 정보

일반적인 고객 토폴로지.

스포크 — 허브 — APIC_EM [컨트롤러]

다음은 세 가지 상황입니다.

- 인증서가 만료되었습니다.
- 인증서가 갱신되지 않습니다.
- 인증서를 사용할 수 없습니다.

디바이스의 현재 상태를 어떻게 알 수 있습니까?

Switch **# sh cry pki cert 명령을 실행합니다.**

```
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
```

표시되는 경우 두 개의 인증서가 있으며 여기서 Associated Trustpoint를 확인해야 합니다.

종료 날짜는 일반적으로 1년이며 시작 날짜보다 커야 합니다.

sdn-network-infra-iwan인 경우 APIC-EM에서 ID와 CA 인증서가 등록되었음을 의미합니다.

APIC-EM이 동일한 인증서를 가지고 있는지 아니면 APIC-EM이 동일한 인증서를 알고 있는지 여부를 어떻게 확인합니까?

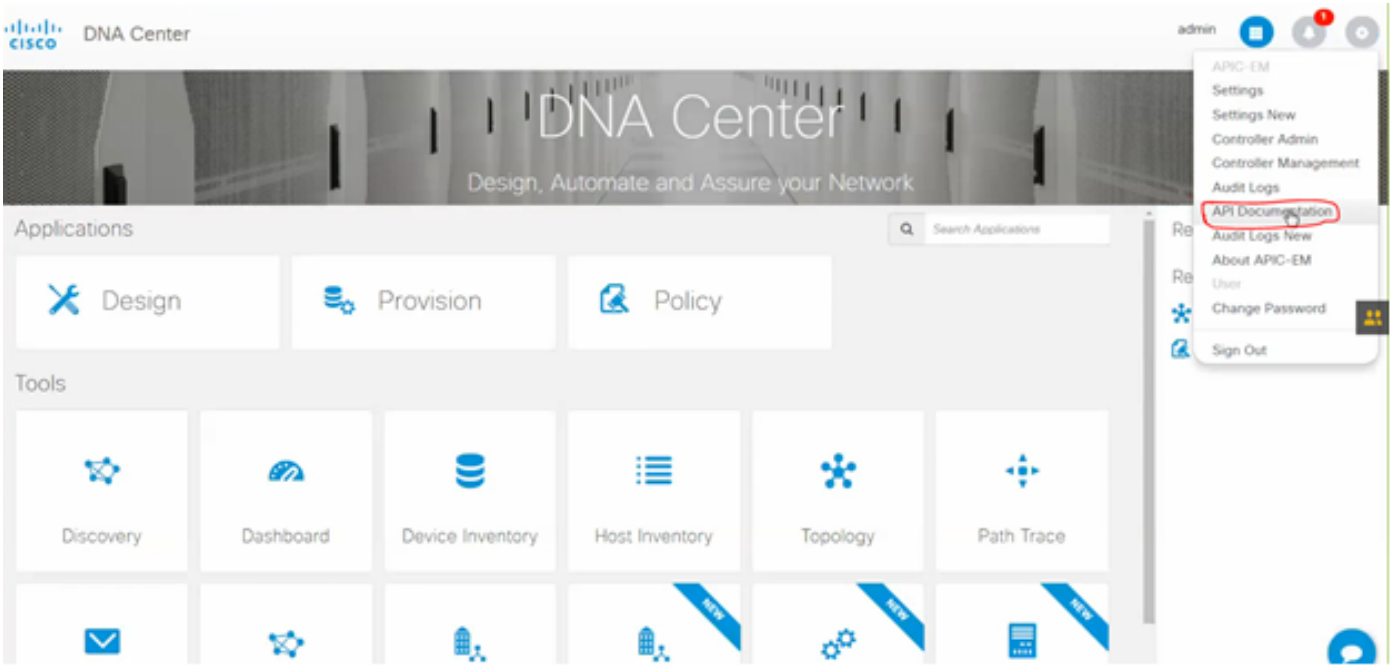
a.디바이스의 버전을 표시하고 일련 번호를 수집합니다.

```
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
```

이 일련 번호의 도움을 받아 APIC-EM 쿼리를 수행하여 APIC-EM이 이 장치에 대해 어떻게 생각하

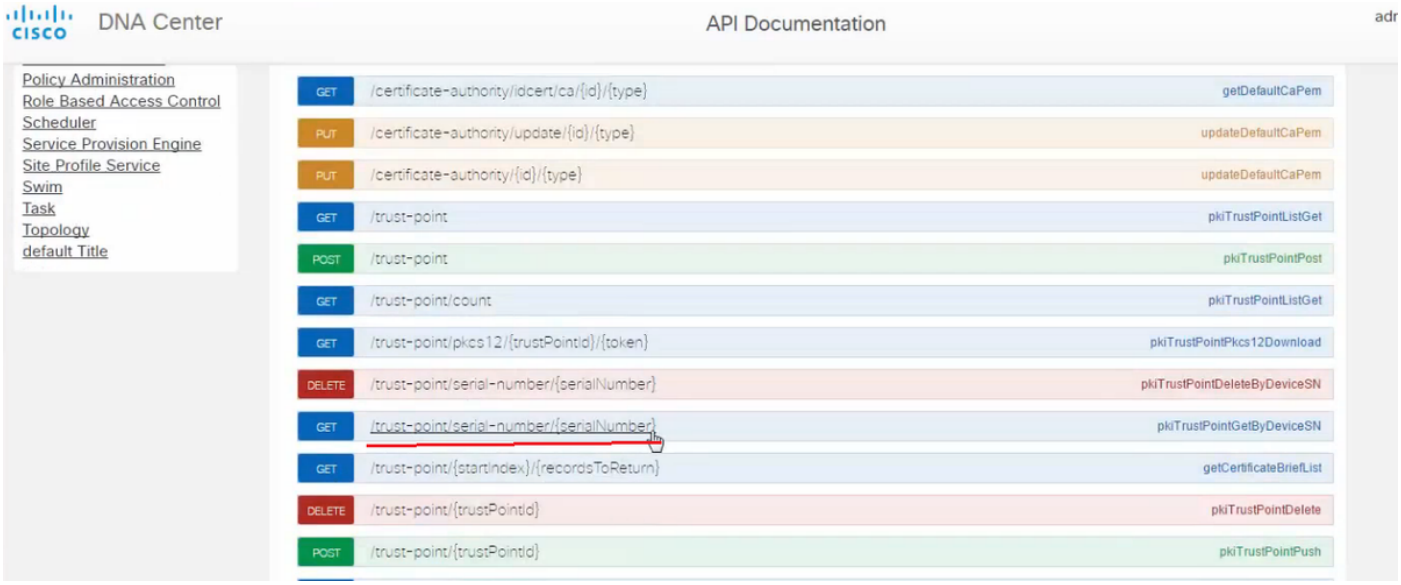
는지 알아볼 수 있습니다.

b.API 설명서로 이동합니다.



c. PKI(Public Key Infrastructure) Broker를 클릭합니다.

d.API 측의 상태를 파악하는 데 도움이 될 First API를 클릭합니다.



GET을 클릭합니다.

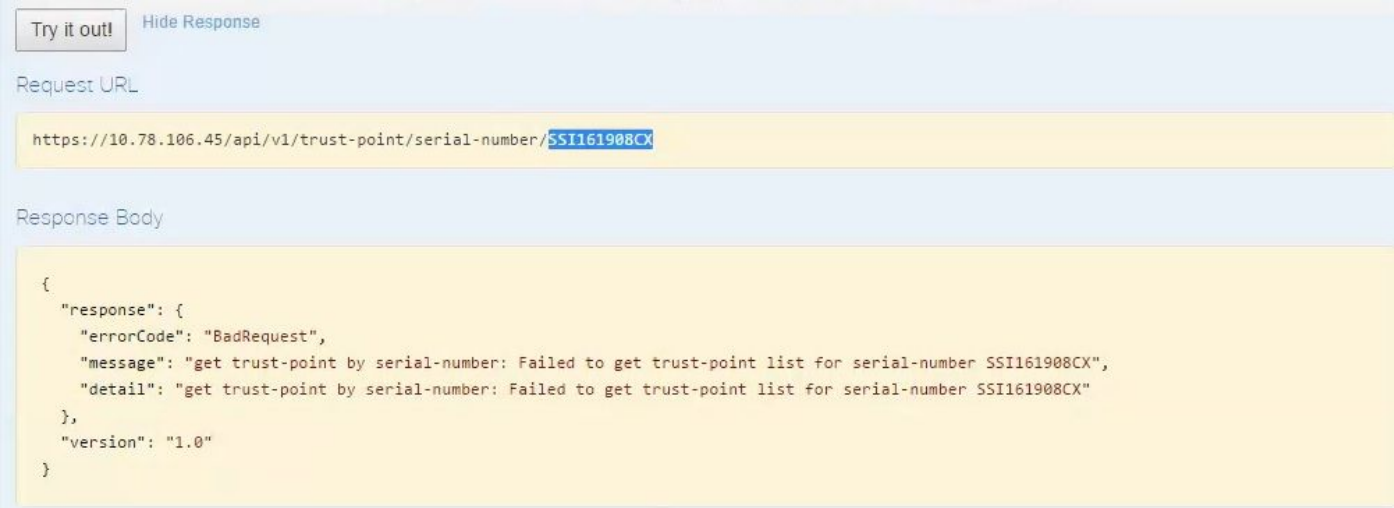
하나의 확인란을 선택하면 디바이스의 show version 출력에서 수집된 일련 번호를 클릭합니다.

Try **it out!을 클릭합니다**.

출력 값을 디바이스의 **sh crp pki 인증서** 출력과 비교합니다.

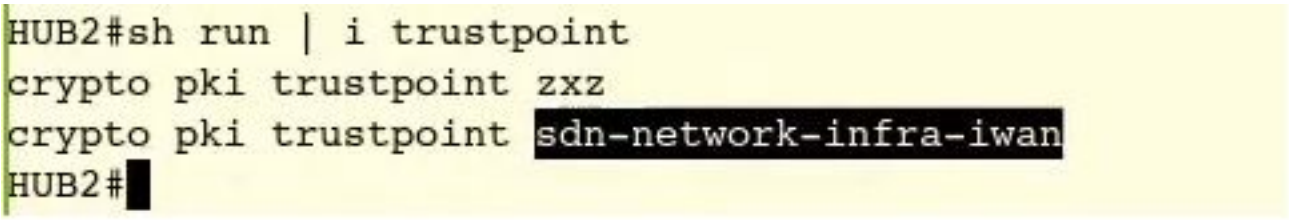
디바이스에서 인증서를 삭제하는 방법

때로는 디바이스에서 인증서가 있고 APIC-EM에 인증서가 없는 경우가 있습니다.따라서 **GET API**를 실행하면 오류 메시지가 표시됩니다.

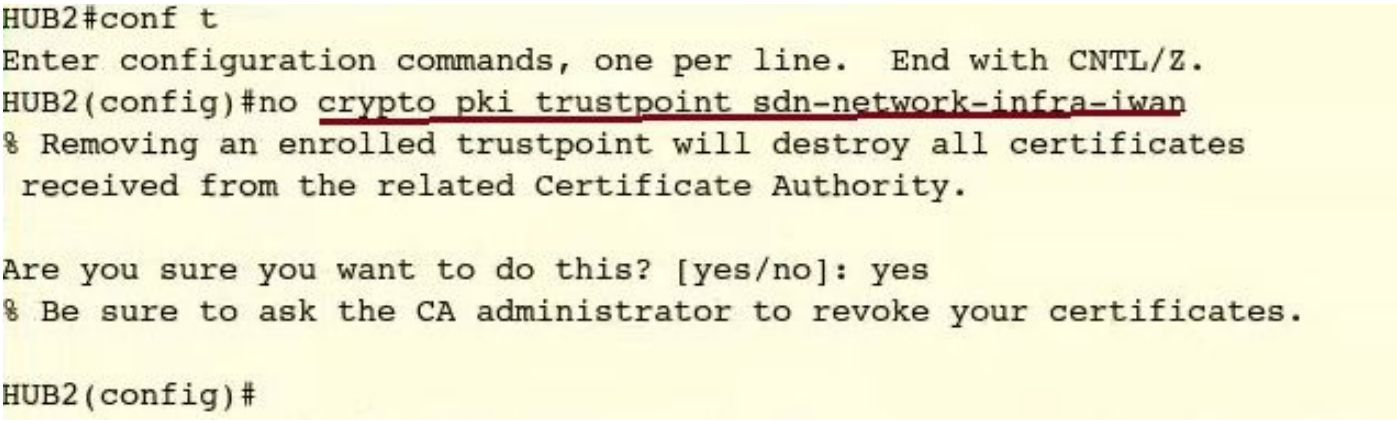


이 솔루션은 디바이스로부터 인증서를 삭제하는 데 사용되는 유일한 솔루션입니다.

a.**Switch# show run | I 신뢰 지점**



crypto **pki trustpoint <trustpoint name> 없이 Switch# 명령을 실행합니다.**



이 명령은 선택한 신뢰 지점과 연결된 디바이스의 모든 인증서를 삭제합니다.

인증서가 삭제되었는지 다시 확인합니다.

다음 명령을 사용합니다.**스위치# sh cry pki cert.**

삭제된 sdn 신뢰 지점을 표시하지 않아야 합니다.

b.키 삭제:

디바이스에서 명령 실행: **Switch# sh cry key mypubkey all.**

여기서 키 이름은 sdn-network-infra로 시작합니다.

키를 삭제하는 명령:

```
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. 디바이스에 연결된 APIC-EM 인터페이스가 ping이 가능해야 합니다.

APIC-EM에는 두 개의 인터페이스가 있는데 그중 하나는 퍼블릭이고 다른 하나는 비공개입니다.이 경우 디바이스와 통신하는 APIC-EM 인터페이스가 서로 ping하는지 확인합니다.

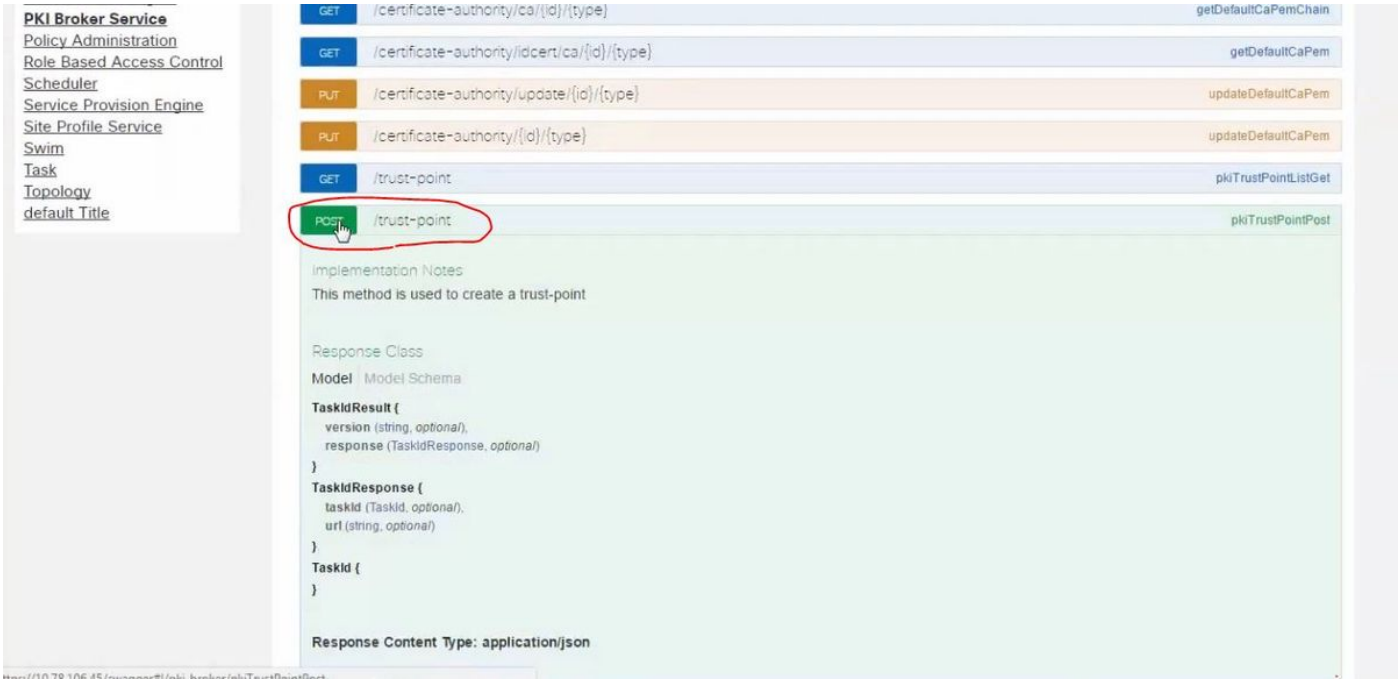
```
HUB2#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HUB2#
```

APIC에서 인증서를 적용하는 방법 - EM?

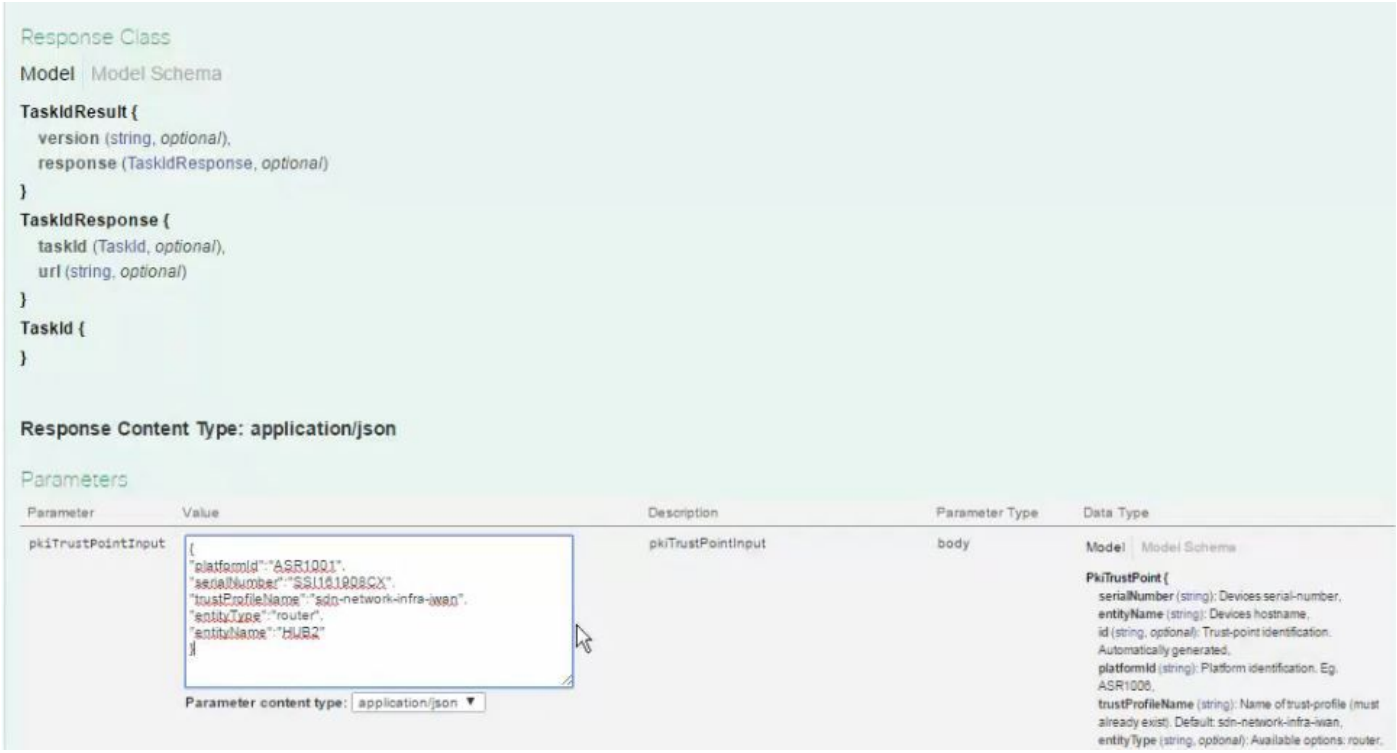
APIC-EM에서 API Documentation을 클릭하고 PKI Broker를 선택한 경우 이 옵션을 사용할 수 있습니다.

POST/trust-point

- APIC - EM .



.



:

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

- STATIC Dynamic.
- .
- show .
- .
- APIC-EM . APIC-EM .

:

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 .

. ID . GET API CALL .

[GET/trust-point/serial-number/{serialNumber}](#) - 쿼리

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

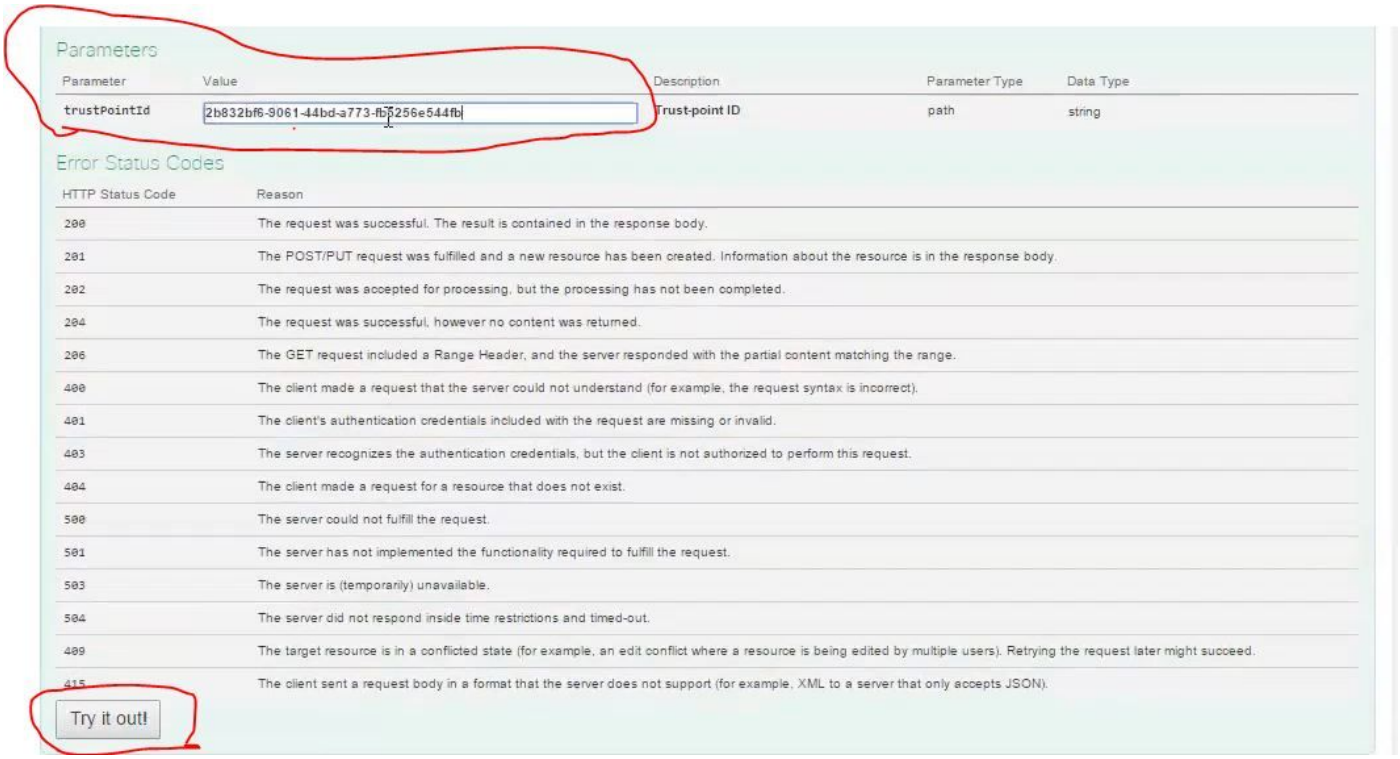
., APIC-EM .

.

[GET 일련 번호 쿼리에서 POST/trust-point/{trustPointId}](#) // trustPointId를 복사해야 합니다.

{ "응답":{ "platformId":"ASR1001", "일련 번호":"SSI161908CX", "trustProfileName":"sdn-network-infra-iwan", "entityName":"HUB2", "entityType":"router", "certificateAuthorityId":"f0bd5040-3f04-4e44-94d8-de97b8829e8d", "attributeInfo":{}, "id":"c4c7d612-9752-4be5-88e5-e2b6f137ea13" }, "버전":"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).
Try it out!

응답 성공 메시지:


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

:

.

```
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#
```

때때로 APIC-EM에 인증서가 있지만 디바이스는 인증서를 가지고 있지 않습니다.어떻게 해결할 수 있습니까?

APIC-EM .
APIC-EM .
DELETE .

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

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).

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"
}
```