

APIC-EM 1.3. - certificaatgeneratie - verwijdering via API

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Hoe ga je weten wat de huidige stand van het apparaat is?](#)

[Hoe zorgt u ervoor dat APIC-EM ook hetzelfde certificaat heeft of dat APIC-EM hetzelfde certificaat heeft begrepen of niet?](#)

[Hoe het certificaat van het apparaat te verwijderen?](#)

[Hoe wordt het certificaat van APIC - EM toegepast?](#)

[Soms heeft APIC-EM het certificaat maar het apparaat niet. Hoe kun je het oplossen?](#)

Inleiding

Dit document beschrijft hoe u de Cisco Application Policy Infrastructure Controller (APIC) - Extension Mobility (EM) API kunt gebruiken om het certificaat te maken - verwijderen. Met IWAN wordt dit allemaal automatisch ingesteld. Op dit moment heeft IWAN echter geen stroom om automatisch apparaat uit het verlopen certificaat te herstellen.

Het goede deel is dat er een soort van stroom in automatisering is in termen van RestAPI. Maar die automatisering is per apparaat en heeft wat informatie nodig over het apparaat. De RestAPI-stroom die buiten IWAN-stroom staat, gebruikt een mechanisme om het certificaat voor apparaat te automatiseren.

Achtergrondinformatie

Gebruikelijke klanttopologie.

SPOKE — HUB — APIC_EM [controller]

Dit zijn de drie situaties:

- Het certificaat is verlopen.
- Het certificaat vernieuwt niet.
- Het certificaat is helemaal niet beschikbaar.

Hoe ga je weten wat de huidige stand van het apparaat is?

Start de commando `Switch# sh hulpki 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

```

Als je ziet, zijn er twee certificaten en hier moet je Associated Trustpoint controleren.

De einddatum zal gewoonlijk één jaar zijn en moet langer zijn dan de aanvangsdatum.

Als het sdn-network-infra-iwan is, betekent het vanuit APIC-EM dat u zowel id als CA certificaat geregistreerd hebt.

Hoe zorgt u ervoor dat APIC-EM ook hetzelfde certificaat heeft of dat APIC-EM hetzelfde certificaat heeft begrepen of niet?

a. Versie van apparaat tonen en het serienummer verzamelen:

```

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

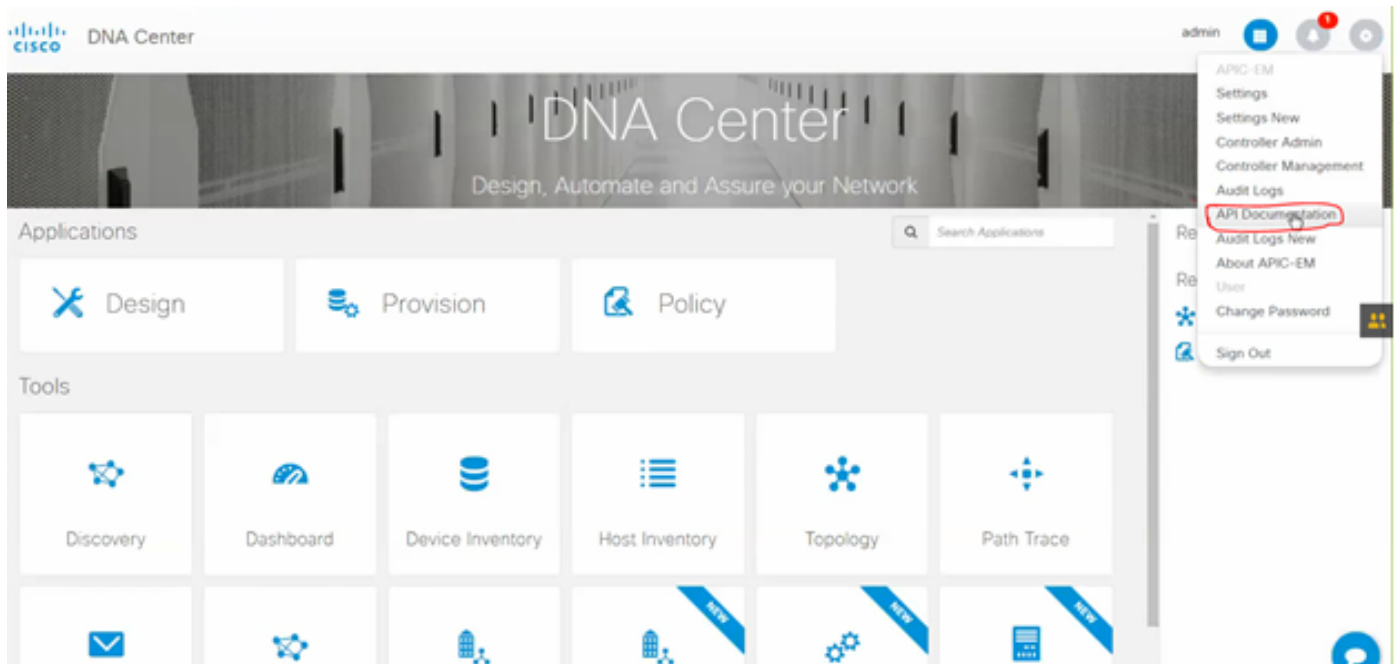
cisco ASR1001 (1RU) processor (revision 1RU) with 1062861K/6147K bytes of memory.
Processor board ID SSI161908CX
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7741439K bytes of eUSB flash at bootflash:.

Configuration register is 0x0

```

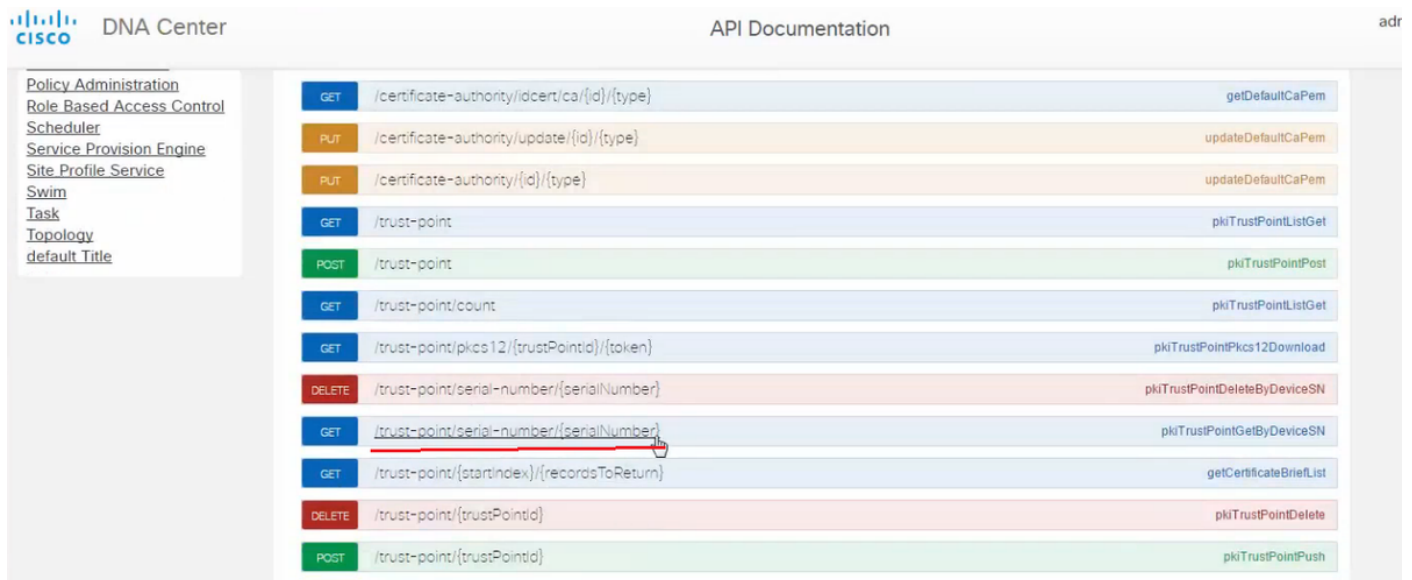
Met behulp van dit serienummer kunt u een APIC-EM query uitvoeren om uit te vinden wat APIC-EM denkt aan dit apparaat.

b. Navigeren in naar API-documentatie.



c. Klik op Public Key Infrastructure (PKI) Broker.

d. Klik op First API om de status van de API-kant te leren kennen.



Klik op **GET**.

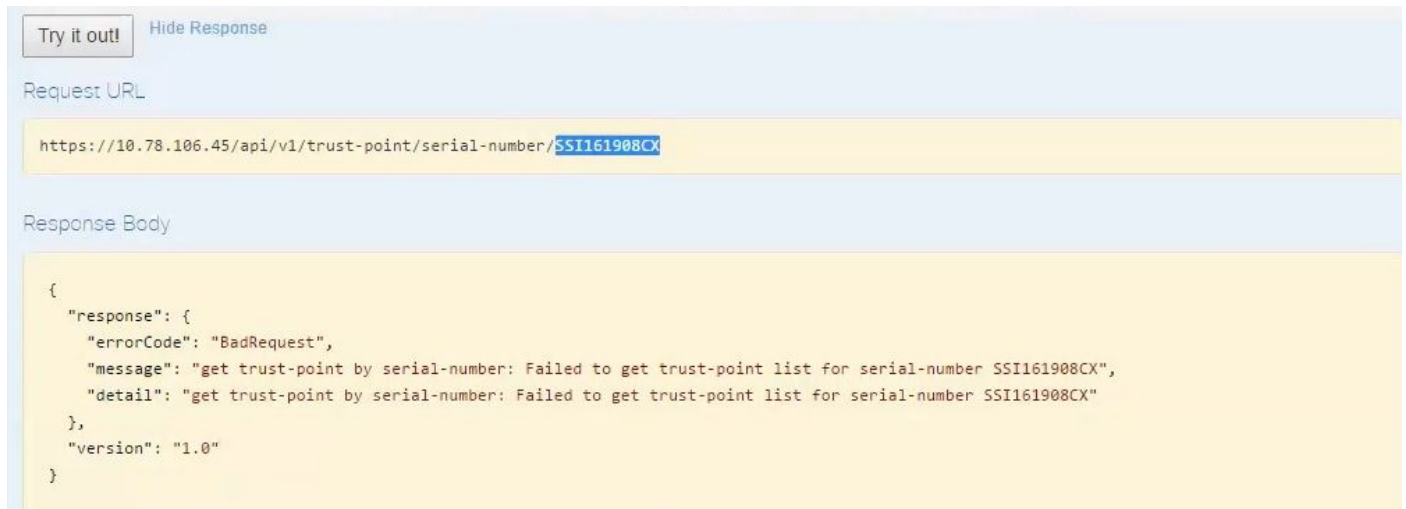
Klik in één selectieteken op het serienummer dat van de uitvoer van het apparaat wordt verzameld.

Klik op **Uitproberen!**.

Vergelijk de uitvoerwaarde met de **sh crp cert** uitvoer van het apparaat.

Hoe het certificaat van het apparaat te verwijderen?

Soms is het zo dat op het apparaat het certificaat aanwezig is en in de APIC-EM is het er niet. Daarom krijg je een foutmelding als je **Get API** runt.



The screenshot shows an API client interface. At the top, there are buttons for "Try it out!" and "Hide Response". Below that, the "Request URL" is displayed as `https://10.78.106.45/api/v1/trust-point/serial-number/SSI161908CX`. The "Response Body" section shows a JSON error response:

```
{
  "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"
}
```

De oplossing is slechts één en dat is het verwijderen van het certificaat van apparaat:

a. **Switch#** tonen run | Ik vertrouw op

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

Start commando **Switch#** op `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)#
```

Deze opdracht verwijdert alle certificaataanvraag op een apparaat dat is gekoppeld aan het geselecteerde trustpunt.

Controleer opnieuw of het certificaat is verwijderd.

Gebruik de opdracht: **Schakelaar... huil graf**.

Het zou geen sdn trustpunt moeten tonen dat is verwijderd.

b. Verwijdering van sleutel:

Start commando op apparaat: **Switch# sh huilen sleutel mypubkey.**

Hier zal je zien dat de Key name begint met **sdn-netwerk-infra**.

Opdracht om toets te verwijderen:

```
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. Zorg ervoor dat de APIC-EM interface die op het apparaat is aangesloten, Pingable is.

Het kan gebeuren dat APIC-EM twee interfaces heeft waarvan het ene openbaar is en het andere privé. In dat geval, zorg ervoor dat de APIC-EM interface die op het apparaat communiceert met elkaar pingt.

```
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#
```

Hoe wordt het certificaat van APIC - EM toegepast?

Onder APIC-EM, wanneer op API-documentatie wordt gedrukt en PKI Broker is geselecteerd, is deze optie beschikbaar.

[POST/trust-point](#)

- Hierdoor wordt een certificaat met APIC - EM gemaakt.

PKI Broker Service
 Policy Administration
 Role Based Access Control
 Scheduler
 Service Provision Engine
 Site Profile Service
 Swim
 Task
 Topology
 default Title

GET	/certificate-authority/ca/{id}/{type}	getDefaultCaPemChain
GET	/certificate-authority/ldcert/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

Vervolgens moet u informatie over het apparaat hebben en op de knop klikken om het uit te proberen.

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	<pre>{ "platformId": "ASR1001", "serialNumber": "SSI161908CX", "trustProfileName": "sdn-network-infra-iwan", "entityType": "router", "entityName": "HUB2" }</pre>	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. ASR1000, trustProfileName (string): Name of trust-profile (must already exist). Default: sdn-network-infra-iwan, entityType (string, optional): Available options: router.

Parameter content type: application/json

Voorbeeld:

```

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

- De gemarkeerde informatie is STATISCH en de rest is Dynamisch.
- Entiteitsnaam is Hostnaam van het apparaat.
- Serienummer dat je hebt van de show versie van het apparaat.
- Entiteitstype dat u kunt wijzigen op basis van het type apparaat.
- Deze informatie is nodig om APIC-EM te vertellen om het apparaat te configureren. Hier begrijpt APIC-EM het serienummer.

Uitvoer van probeer het uit!:

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"
}
```

Deze uitvoer betekent dat het bestand intern wordt aangemaakt door APIC-EM en is nu gereed om op het apparaat in te zetten. De volgende stap is om dit apparaat in de bundel te duwen. Om te duwen, moet je een vertrouwenspoint ID krijgen. Dit kan worden gedaan via Get API CALL.

[GET/trust-point/serienummer/ {serienummer}](#) - Query

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

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	551161908CX	Device serial-number	path	string

Error Status Codes

Het geeft je deze output. Het betekent dat APIC-EM het certificaat heeft om het apparaat aan te drukken.

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

Duw het certificaat op het apparaat.

[POST/trust-point/ {trustPointID}](#) // trustPointID moet worden gekopieerd van GET Serial Number Query

```

{"respons": {"platformID": "ASR1001", "serienummer": "SSI161908CX", "trustProfileName": "sdn-network-infra-iwan", "entitiesName": "HUB2", "entiteitType": "router", "certificaatAuthorityID": "f0bd5040-3f04-4e44-94d8-de97b8829e8d", "attribuutInfo": {}, "id": "c4c7d612-9752-4be5-88e5-e2b6f137ea13"}, "versie": "1.0"}

```

Dit zal het certificaat naar apparaat duwen - op voorwaarde dat er een goede connectiviteit is.

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).

Try it out!

Bericht van succes van respons:

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

Controleer het apparaat:

U ziet dat beide certificaten nu zijn geplakt:

```
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#
```

Soms heeft APIC-EM het certificaat maar het apparaat niet. Hoe kun je het oplossen?

Er is een bepaalde achtergrondtaak waarmee u het certificaat alleen kunt verwijderen uit APIC-EM. Soms schrapt de klant per ongeluk het certificaat van het apparaat maar in APIC-EM is het er nog. Klik op **VERWIJDEREN**.

[VERWIJDEREN/vertrouwen-punt/serienummer/ {serienummer}](#) - Verwijderen.

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

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)
}

Typ het serienummer en klik op **Probeer het!**.

Parameters

Parameter	Value	Description	Parameter Type	Data Type
serialNumber	<input type="text" value="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"
}
```