APIC-EM 1.3. — 证书生成 — 通过API删除

目录

简介

本文档介绍如何使用思科应用策略基础设施控制器(APIC) — 分机移动(EM)API创建 — 删除证书。使用IWAN时，它都会自动配置。但是，IWAN目前没有任何流从过期的证书中自动恢复设备。

好的部分是，在RestAPI方面，自动化有某种流。但是，该自动化是按设备进行的，并且它需要有关设备的一些信息。IWAN流之外的RestAPI流使用一些机制来自动执行设备的证书。

背景信息

常见客户拓扑。

辐条 — 中心 — APIC_EM [控制器]

以下是三种情况：

- 证书已过期。
- 证书未续约。
- 证书完全不可用。

您如何了解设备的当前状态？

运行命令**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，有两个证书，您需要在此处检查关联信任点。

结束日期通常为一年，应晚于开始日期。

如果它是sdn-network-infra-iwan，则表示从APIC-EM注册了ID和CA证书。

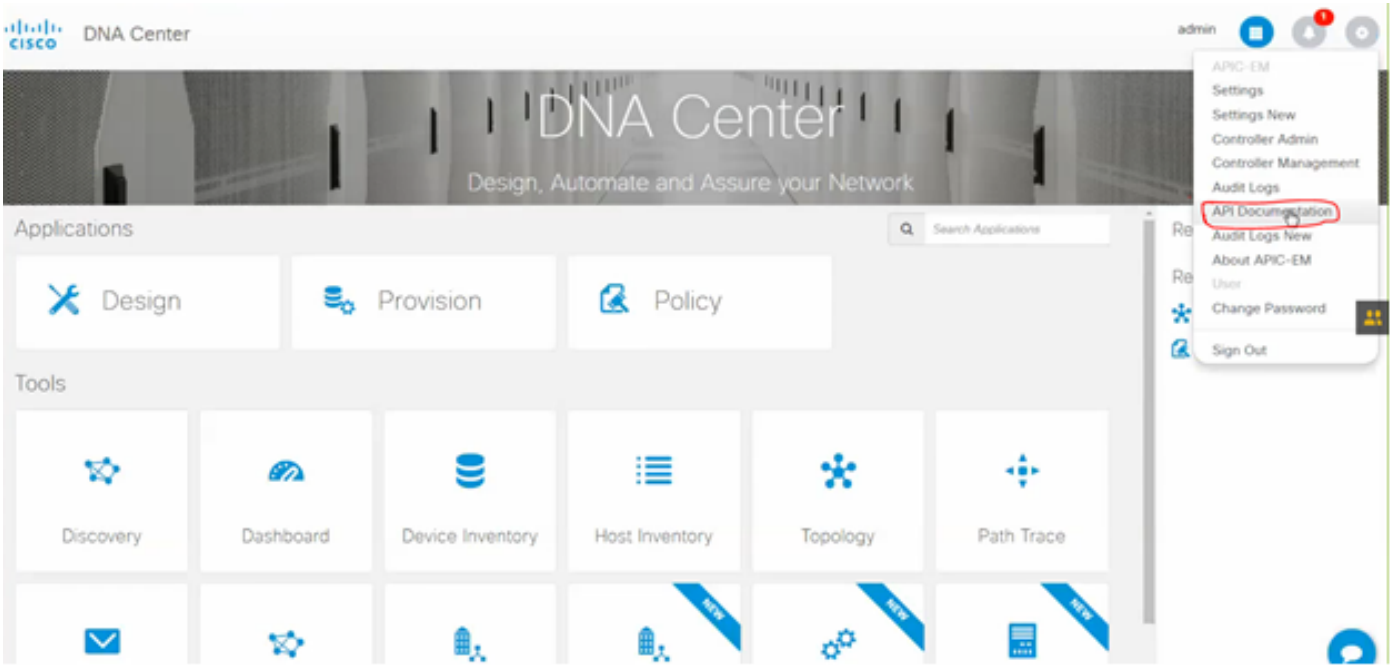
您如何确保APIC-EM是否也具有相同的证书，或者APIC-EM是否理解相同的证书？

a.从设备显示版本并收集序列号：

```
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
```

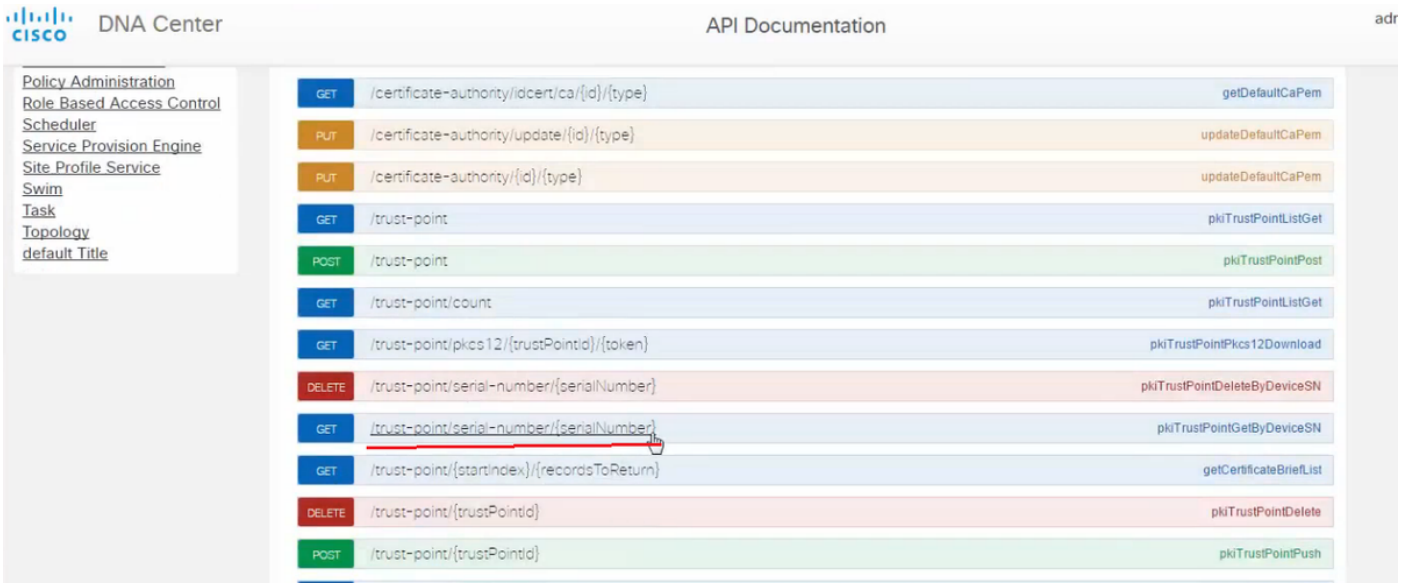
借助此序列号，您可以执行APIC-EM查询，以了解APIC-EM对此设备的看法。

b.导航至API文档。



c.点击公钥基础设施(PKI)代理。

d.点击First API（第一个API），这将帮助我们从API端了解状态。



单击“GET(**获取**)”。

在一个复选框上，点击从设备的show version输出收集的序列号。

单击“**Try out！（试用！）**”。

将输出值与设备**的sh crp pki cert**输出进行比较。

如何从设备中删除证书？

有时，在设备上，证书存在，而在APIC-EM中，证书不存在。因此，运行GET API**时**会收到错误消息。

Try it out! Hide Response

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"
}
```


解决方案只有一个，即从设备中删除证书：

a.**Switch# show run |我信任点**

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

运行命**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)#
```

此命令删除与所选信任点关联的设备上的所有证书。

重新检查证书是否已删除。

使用下列命令：**Switch# sh cry pki cert。**

它不应显示已删除的sdn信任点。

b.删除密钥：

在设备上运行命令：**Switch# sh cry key mypubkey all。**

您将看到密钥名称以**sdn-network-infra**开头。

删除密钥的命令：

```
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.确保连接到设备的APIC-EM接口应为Ping。

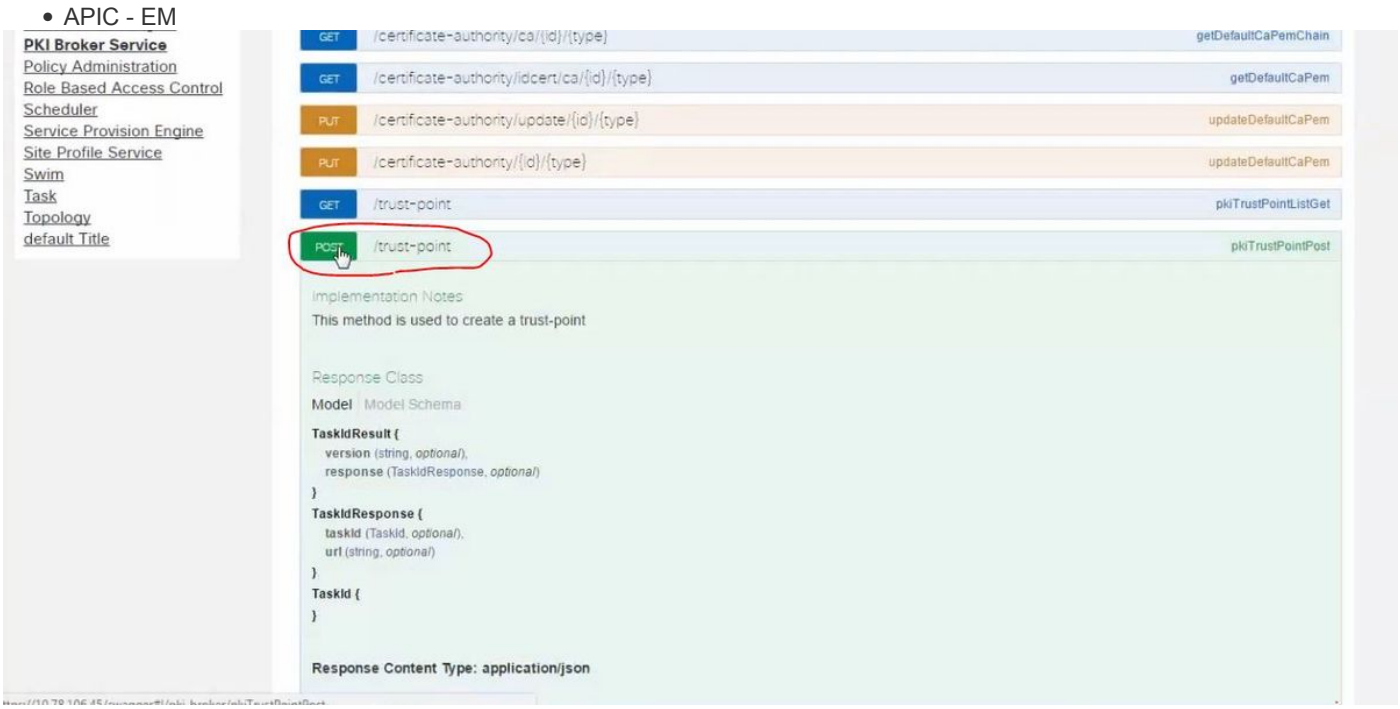
APIC-EM可能有两个接口，一个是公共接口，另一个是私有接口。在这种情况下，请确保与设备通信的APIC-EM接口彼此ping。

```
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#
```

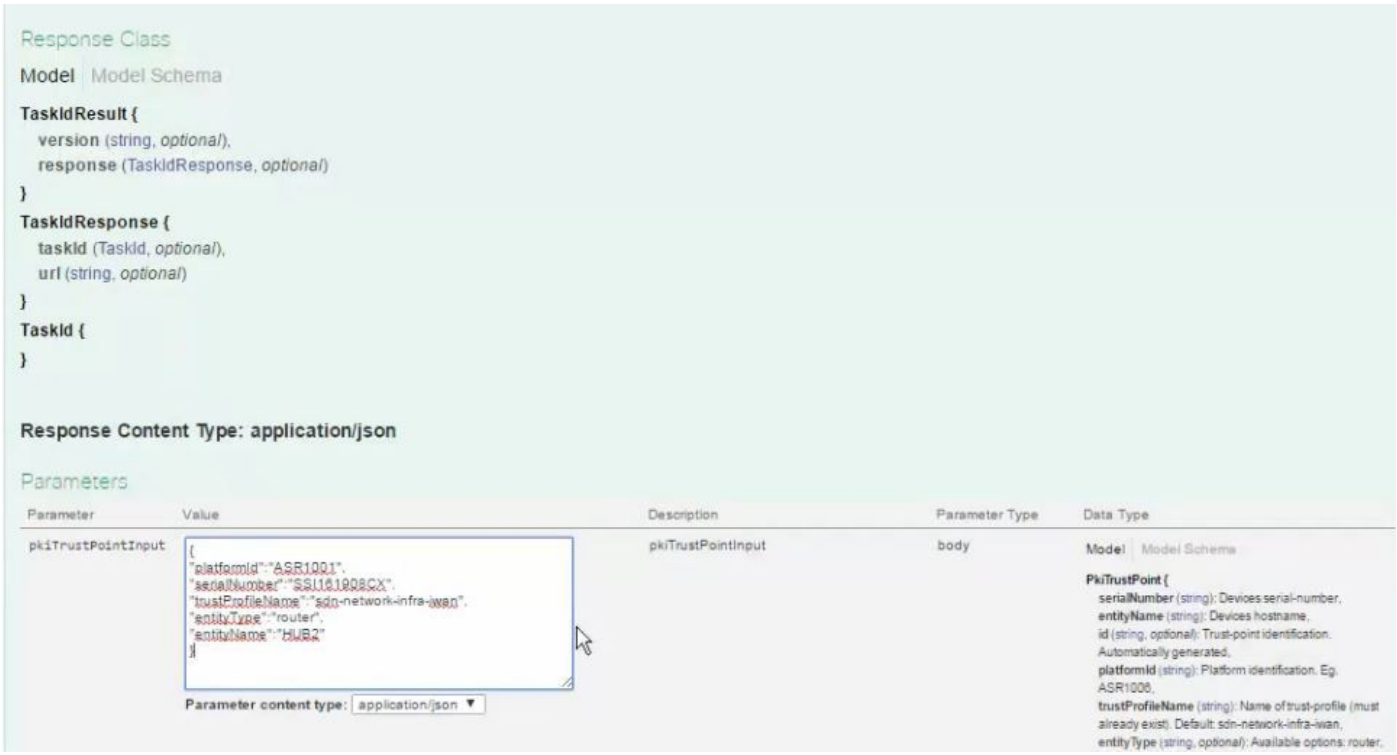
如何从APIC - EM应用证书？

在APIC-EM下，点击API文档并选择PKI代理后，此选项可用。

POST/trust-point



“”



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

- “”“”
-
- show version
-
- 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} — 查询

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

Response Body

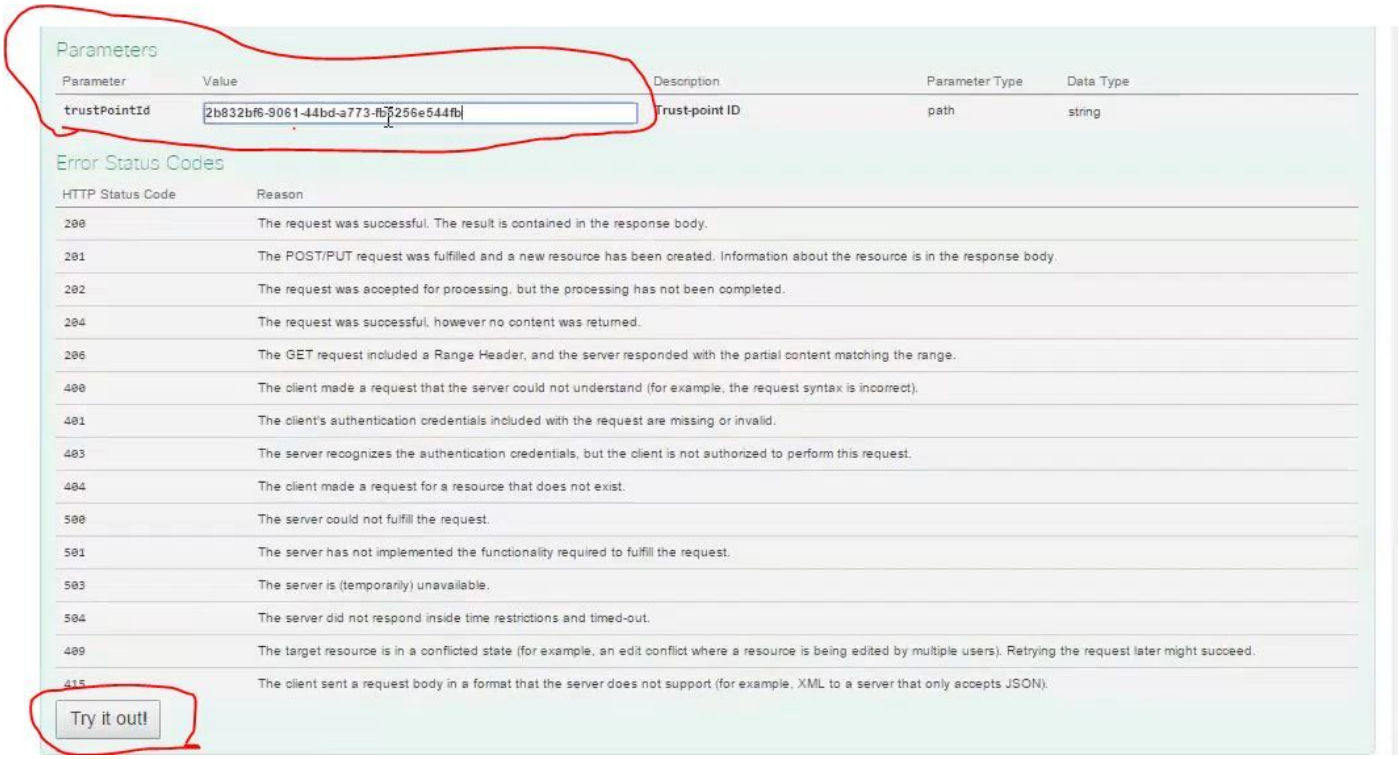

```
{
  "response": {
    "platformId": "ASR1001",
    "serialNumber": "SSI161908CX",
    "trustProfileName": "sdn-network-infra-iwan",
    "entityName": "HUB2",
    "entityType": "router",
    "certificateAuthorityId": "f0bd5040-3f04-4e44-94d8-de97b8829e8d",
    "attributeInfo": {},
    "id": "2b832bf6-9061-44bd-a773-fb5256e544fb"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


Response Code

```
200
```

POST/trust-point/{trustPointId} // trustPointId需要从GET序列号查询复制

{“响应”：{ "platformId":“ASR1001”、“序列号”："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" }


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!

响应成功消息：


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#
```

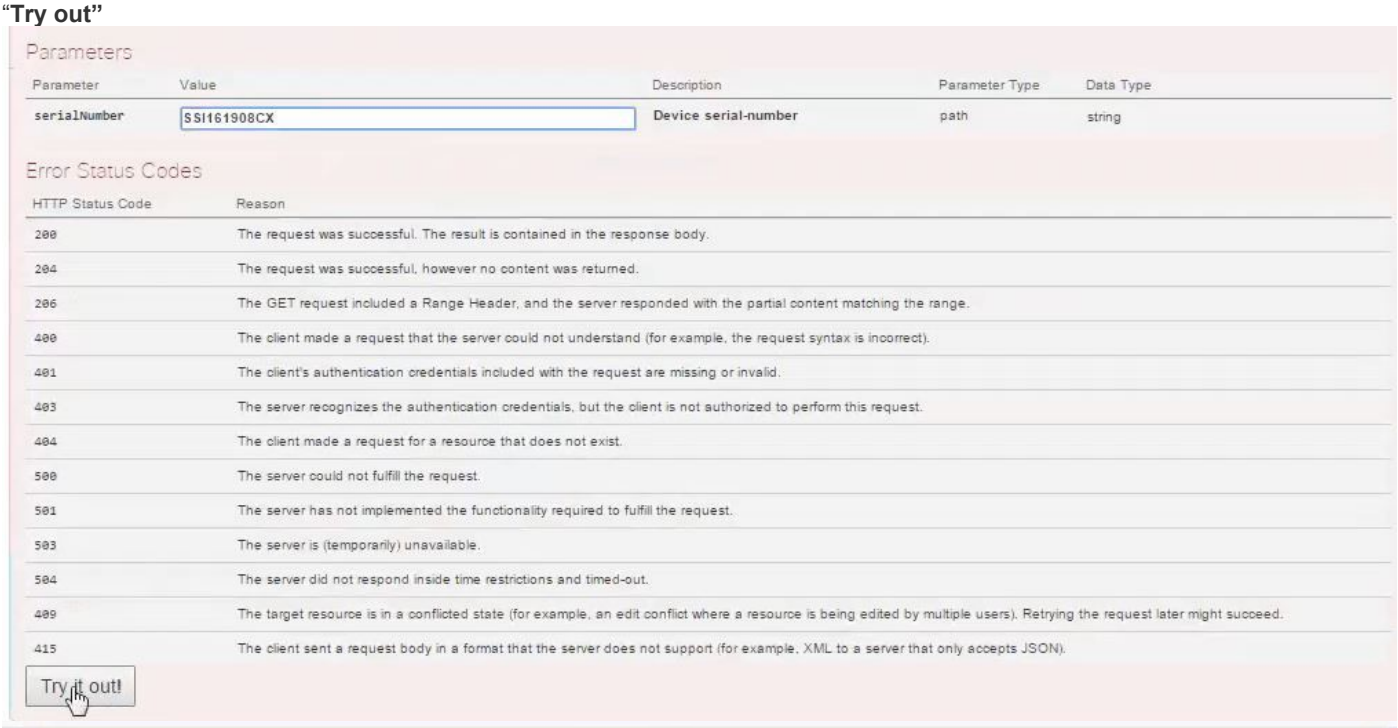
有时，APIC-EM有证书，但设备没有。您如何解决它？

APIC-EM
APIC-EM
“”

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


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)
}

"Try 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"
}