APIC-EM 1.3. – 証明書の生成 – APIによる削除

内容

概要

このドキュメントでは、Cisco Application Policy Infrastructure Controller (APIC) - エクステンション モビリティ (EM) API を使用して証明書を作成または削除する方法について説明します。IWAN では、これがすべて自動的に設定されます。ただし、現時点では、期限切れの証明書からデバイスを自動的に復旧するためのフローが IWAN にはありません。

なお、RestAPI に関するある種の自動化フローが存在します。ただし、この自動化はデバイスごとに行われ、デバイスに関する情報が必要です。IWANフローの外部にあるRestAPIフローは、デバイスの証明書を自動化するメカニズムを使用します。

背景説明

標準的な顧客トポロジ。

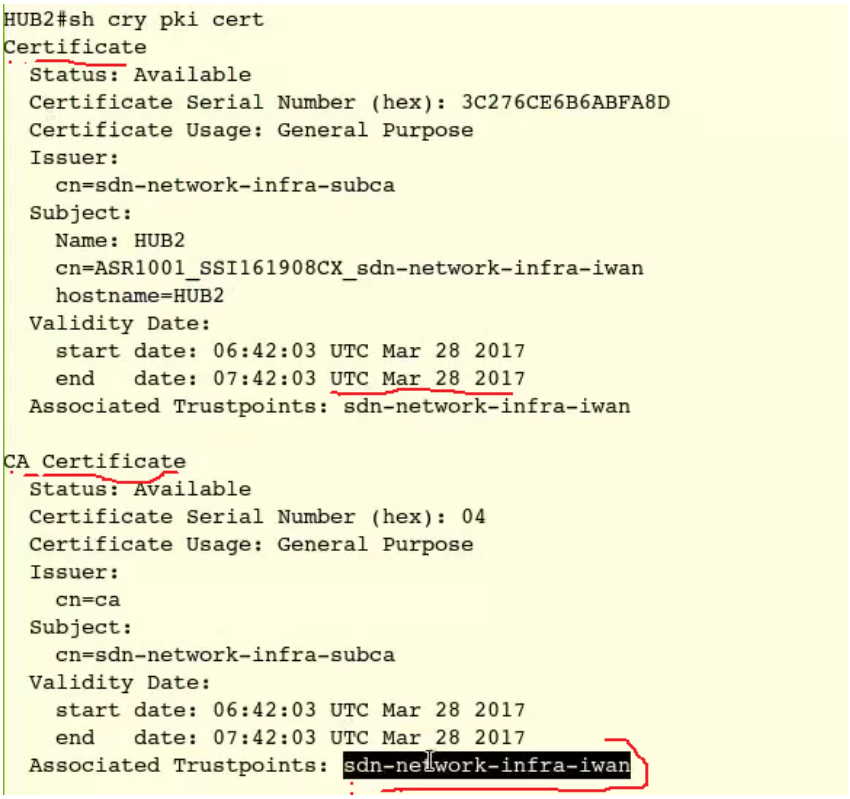
SPOKE — HUB — APIC_EM [コントローラ]

以下の 3 つの状況があります。

- 証明書の有効期限が切れている。
- 証明書が更新されない。
- 証明書をまったく使用できない。

デバイスの現在の状態を確認するには、どうすればよいですか。

コマンド **Switch# sh cry pki cert** を実行します。



```
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
```

結果を見ると 2 つの証明書があり、ここでは関連するトラストポイント（Associated Trustpoint）を確認する必要があります。

終了日は通常 1 年であり、開始日より後である必要があります。

これが sdn-network-infra-iwan である場合は、APIC-EM から、ID および CA 証明書が登録されていることを意味します。

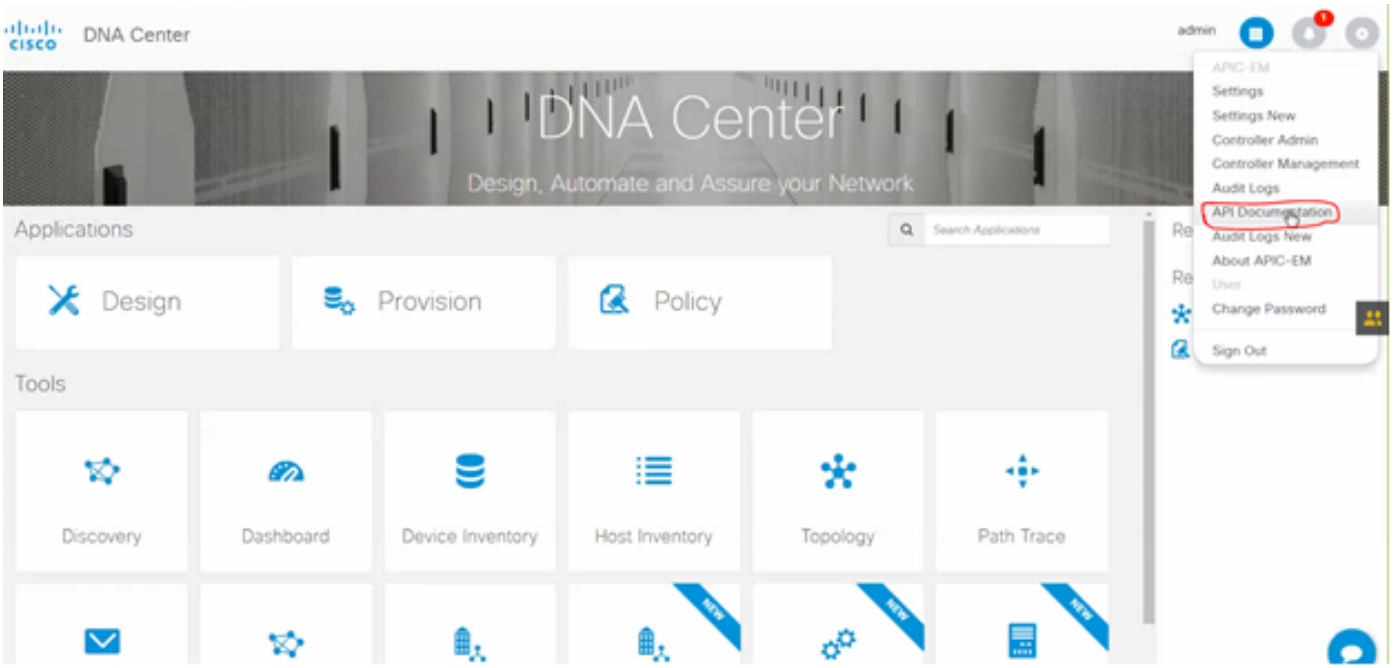
APIC-EM にも同じ証明書があるかどうか、または APIC-EM が同じ証明書を認識したどうかを確認するには、どうすればよいですか。

a.デバイスからバージョンを表示し、シリアル番号を次のように収集します。

```
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
```

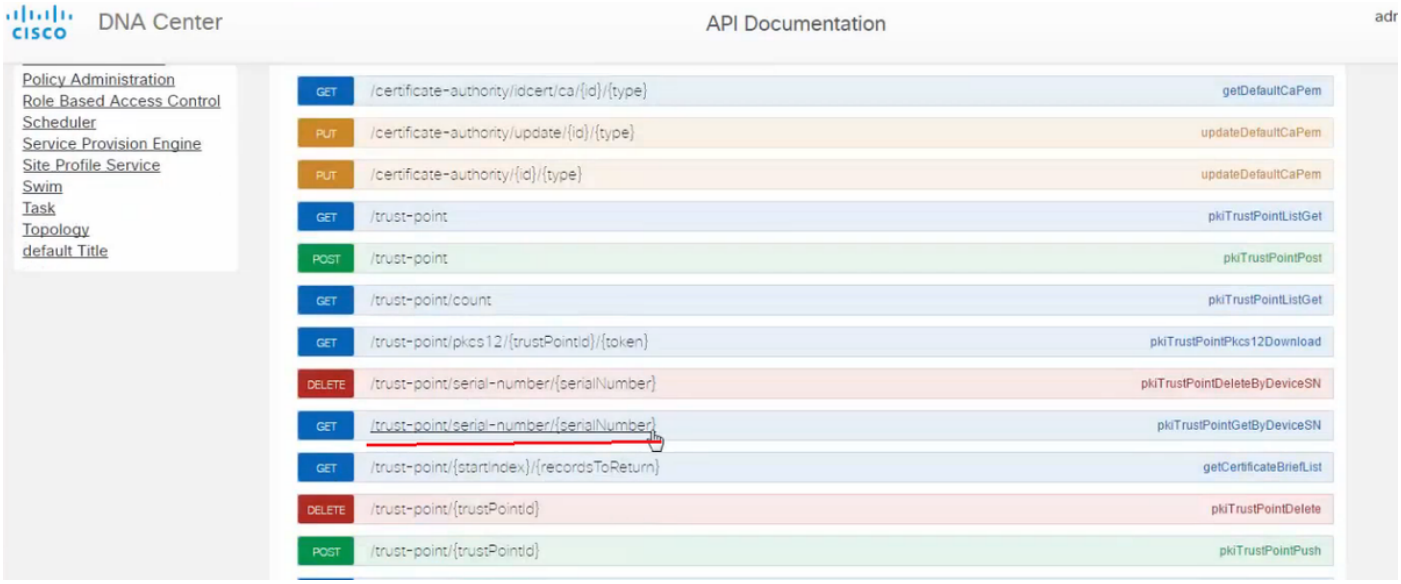
このシリアル番号を使って APIC-EM クエリを実行し、APIC-EM がこのデバイスをどのように認識しているかを確認できます。

b.API ドキュメントに移動します。



c. [Public Key Infrastructure (PKI) Broker]をクリックします。

d.最初の API をクリックします。これにより、API 側からのステータスを確認できます。



[GET] **をクリックします。**

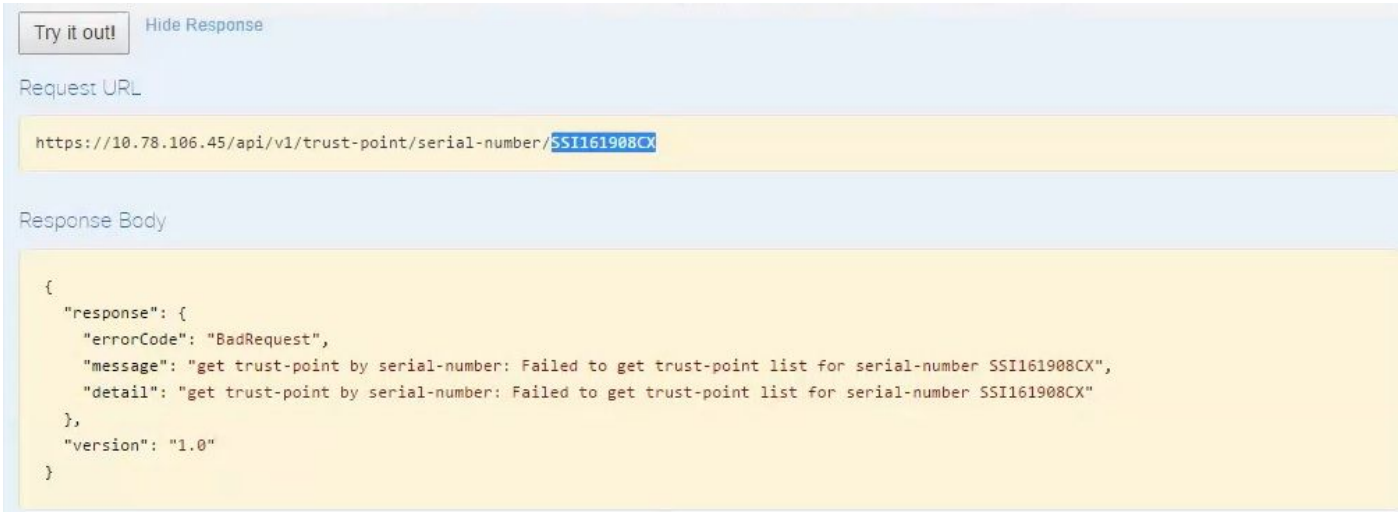
チェックボックスで、デバイスの show version の出力から収集されたシリアル番号をクリックします。

[Try it out!] をクリックします。

出力値を、デバイスの **sh crp pki cert 出力と比較します。**

デバイスから証明書を削除するには、どうすればよいですか。

デバイスには証明書があっても、APIC-EM には証明書がない場合があります。これが原因で、**GET API を実行すると工ラー メッセージが表示されます。**



解決法は 1 つのみ、つまりデバイスから証明書を削除することです。

a.**Switch# show run | I trustpoint**

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

コマンド **Switch# no crypto pki trustpoint <trustpoint name> を実行します。**

```
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)#
```

このコマンドは、選択したトラストポイントに関連付けられているデバイス上のすべての証明書を削除します。

証明書が削除されたことを再確認します。

コマンドを使用します**Switch# sh cry pki cert**

削除された sdn トラストポイントは表示されないはずです。

b.キーの削除：

デバイス上でコマンドを実行します。**Switch# sh cry key mypubkey all。**

ここで、キー名が **sdn-network-infra** で始まることが分かります。

キーを削除するコマンド：

```
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.デバイスに接続されているAPIC-EMインターフェイスがping可能であることを確認します。

APIC-EM に 2 つのインターフェイス (1 つは公開、もう 1 つは非公開) が存在する場合があります。この場合、デバイスと通信する APIC-EM インターフェイスが互いに ping 可能であることを確認してください。

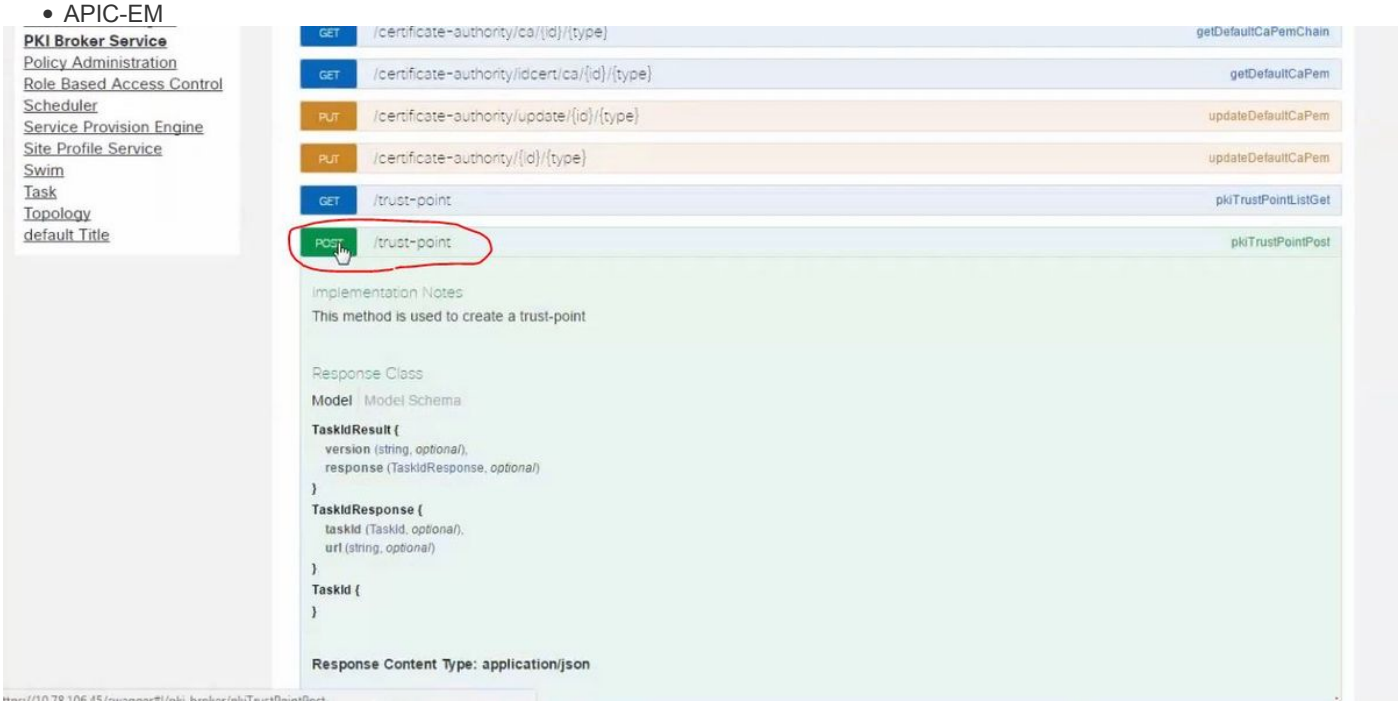
```
HUB2#ping 10.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HUB2#
```

APIC-EM から証明書を適用するには、どうすればよいですか。

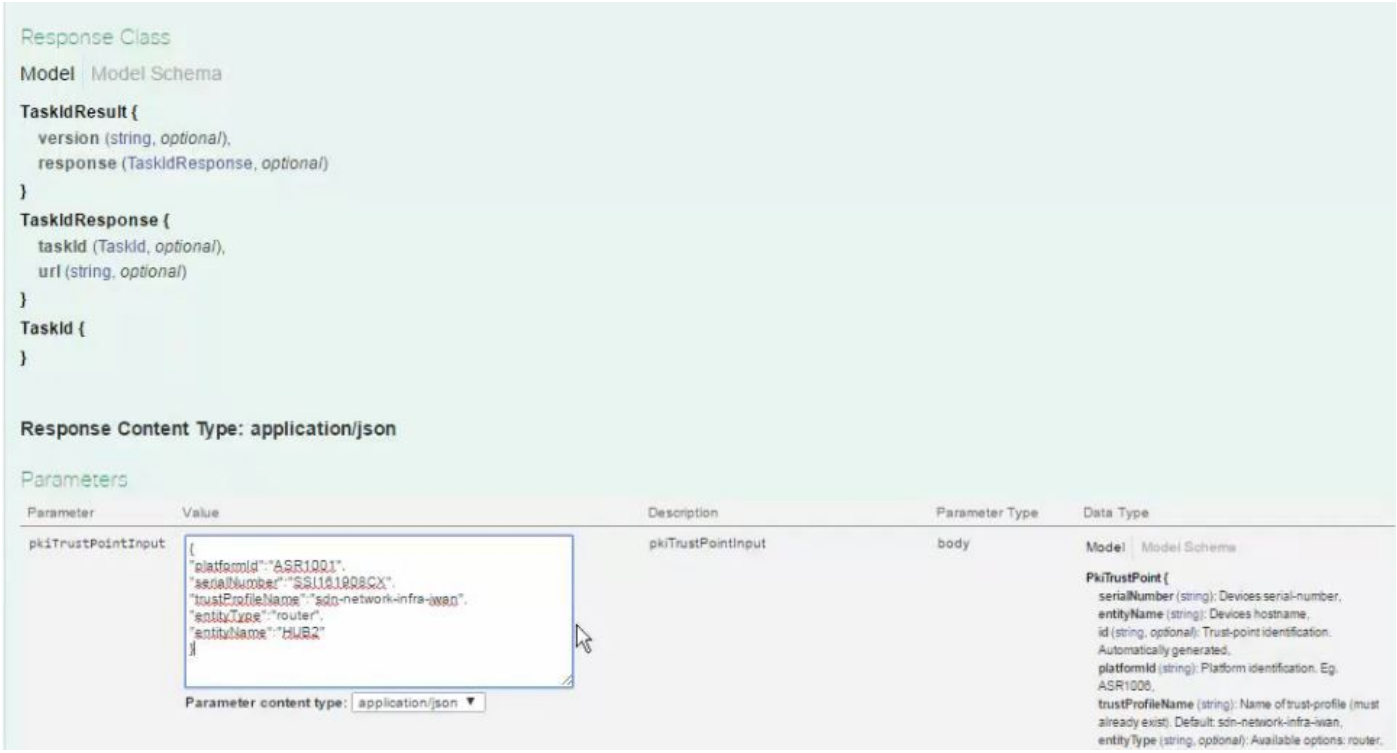
APIC-EM で [API Documentation] をクリックして [PKI Broker] を選択すると、このオプションが使用可能になります。

POST/trust-point

- APIC-EM



[try it out]



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

-
-
- show version
-
- APIC-EM APIC-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
ID GET API CALL

[GET/trust-point/serial-number/{serialNumber} - クエリ]

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

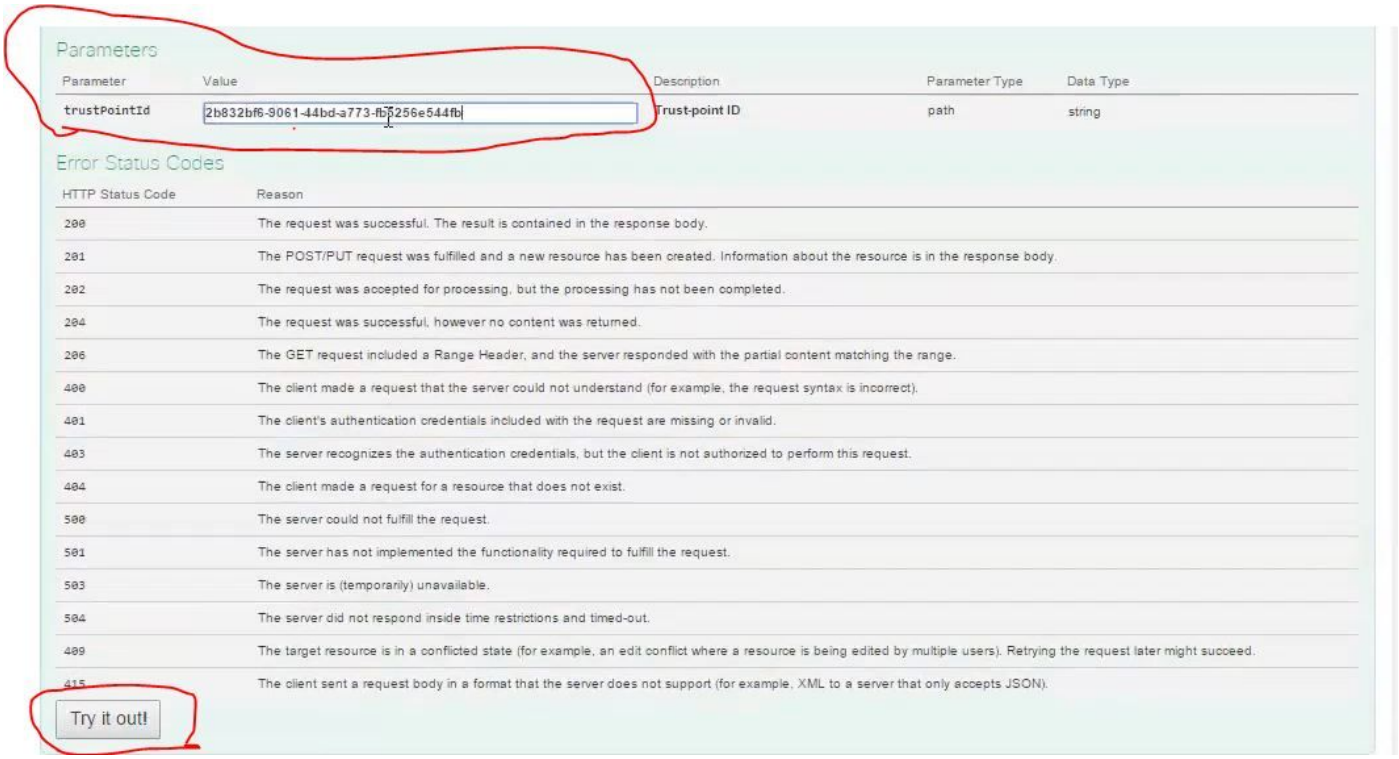
Parameter	Value	Description	Parameter Type	Data Type
serialNumber	SSI161908CX	Device serial-number	path	string

Error Status Codes

APIC-EM

[シリアル番号取得クエリから POST/trust-point/{trustPointId}　// trustPointId をコピーする必要があります。]

{ "response":{ "platformId":"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" }, "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!

成功応答メッセージ：


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#
```

APIC-EM には証明書があっても、デバイスにはない場合があります。これを解決するには、どうすればよいですか。

1　APIC-EM
APIC-EM
[DELETE]

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

[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"
}
```