

APIC-EM 1.3 - Zertifikatgenerierung - Löschung über API

Inhalt

[Einführung](#)

[Hintergrundinformationen](#)

[Wie können Sie den aktuellen Status des Geräts ermitteln?](#)

[Wie stellen Sie sicher, dass das APIC-EM auch über dasselbe Zertifikat verfügt oder das APIC-EM dasselbe Zertifikat verstanden hat?](#)

[Wie wird das Zertifikat vom Gerät gelöscht?](#)

[Anwenden des Zertifikats des APIC - EM](#)

[Manchmal verfügt das APIC-EM über das Zertifikat, das Gerät jedoch nicht. Wie können Sie dieses Problem beheben?](#)

Einführung

Dieses Dokument beschreibt die Verwendung der API von Cisco Application Policy Infrastructure Controller (APIC) - Extension Mobility (EM) zum Erstellen - Löschen des Zertifikats. Mit IWAN wird alles automatisch konfiguriert. Derzeit verfügt das IWAN jedoch nicht über einen Datenfluss, um das Gerät automatisch aus einem abgelaufenen Zertifikat wiederherzustellen.

Der Vorteil ist, dass es eine Art von Fluss in der Automatisierung in Bezug auf RestAPI. Diese Automatisierung ist jedoch auf jedem Gerät möglich und erfordert einige Informationen auf dem Gerät. Der RestAPI-Fluss außerhalb des IWAN-Datenflusses verwendet Mechanismen zur Automatisierung des Zertifikats für das Gerät.

Hintergrundinformationen

Gewöhnliche Kundentopologie.

SPOKE - HUB - APIC_EM [Controller]

Dies sind die drei folgenden Situationen:

- Das Zertifikat ist abgelaufen.
- Das Zertifikat erneuert nicht.
- Zertifikat ist überhaupt nicht verfügbar.

Wie können Sie den aktuellen Status des Geräts ermitteln?

Führen Sie den Befehl **Switch# sh cry pki cert** aus.

```
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
```

Wenn Sie sehen, gibt es zwei Zertifikate und hier müssen Sie Associated Trustpoint überprüfen.

Das Enddatum beträgt in der Regel ein Jahr und sollte größer als das Startdatum sein.

Wenn es sich um "sdn-network-infra-iwan" handelt, bedeutet dies, dass Sie im APIC-EM sowohl ID als auch CA-Zertifikat registriert haben.

Wie stellen Sie sicher, dass das APIC-EM auch über dasselbe Zertifikat verfügt oder das APIC-EM dasselbe Zertifikat verstanden hat?

a) Version vom Gerät anzeigen und Seriennummer erfassen:

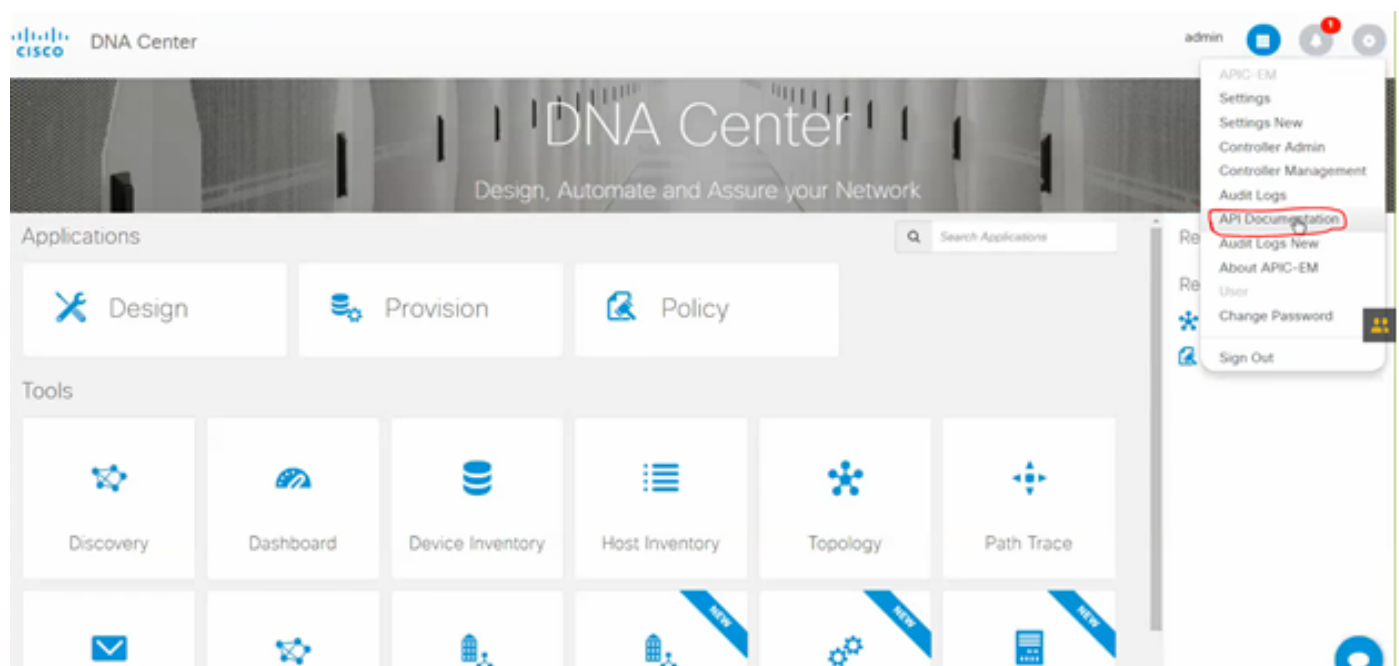
If you require further assistance please contact us by sending email to export@cisco.com.

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 SSI61908CX  
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
```

Mithilfe dieser Seriennummer können Sie eine APIC-EM-Abfrage durchführen, um herauszufinden, was das APIC-EM über dieses Gerät denkt.

b) Navigieren Sie zur API-Dokumentation.



c) Klicken Sie auf Public Key Infrastructure (PKI) Broker.

d) Klicken Sie auf First API (Erste API), um den Status von API zu erfahren.

Policy Administration	GET	/certificate-authority/ dcert/ca/{id} {type}	getDefaultCaPem
Role Based Access Control	PUT	/certificate-authority/update/{id} {type}	updateDefaultCaPem
Scheduler	PUT	/certificate-authority/{id} {type}	updateDefaultCaPem
Service Provision Engine	GET	/trust-point	pkiTrustPointListGet
Site Profile Service	POST	/trust-point	pkiTrustPointPost
Swim	GET	/trust-point/count	pkiTrustPointListGet
Task	GET	/trust-point/pkcs12/{trustPointId} {token}	pkiTrustPointPkcs12Download
Topology	DELETE	/trust-point/serial-number/{serialNumber}	pkiTrustPointDeleteByDeviceSN
default Title	GET	/trust-point/serial-number/{serialNumber}	pkiTrustPointGetByDeviceSN
	GET	/trust-point/{startIndex} {recordsToReturn}	getCertificateBriefList
	DELETE	/trust-point/{trustPointId}	pkiTrustPointDelete
	POST	/trust-point/{trustPointId}	pkiTrustPointPush

Klicken Sie auf **GET**.

Klicken Sie in einem Kontrollkästchen auf die Seriennummer, die aus der Ausgabe der Geräteversion angezeigt wird.

Klicken Sie auf **Versuchen Sie es heraus!**

Vergleichen Sie den Ausgabewert mit der **sh crp pki cert**-Ausgabe des Geräts.

Wie wird das Zertifikat vom Gerät gelöscht?

Manchmal ist das Zertifikat auf dem Gerät vorhanden und im APIC-EM nicht vorhanden. Aus diesem Grund erhalten Sie beim Ausführen der **GET-API** eine Fehlermeldung.

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"
}

```

Die Lösung ist die einzige, die das Löschen des Zertifikats vom Gerät ermöglicht:

a) **Switch# show run | I Trustpoint**

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

Führen Sie den Befehl **Switch# no crypto pki trustpoint <trustpoint name>** aus.

```
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)#
```

Mit diesem Befehl werden alle Zertifikate auf einem Gerät gelöscht, die ausgewählten Trustpoints zugeordnet sind.

Überprüfen Sie erneut, ob das Zertifikat gelöscht wurde.

Verwenden Sie den Befehl: **Switch# sh cry pki cert.**

Es sollte kein sdn trustpoint angezeigt werden, der gelöscht wurde.

b) Löschen des Schlüssels:

Befehl auf Gerät ausführen: **Switch# sh cry key mypubkey all.**

Hier sehen Sie, dass der Schlüsselname mit **sdn-network-infra** beginnt.

Befehl zum Löschen des Schlüssels:

```
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. Stellen Sie sicher, dass die mit dem Gerät verbundene APIC-EM-Schnittstelle Pingable sein muss.

Es kann vorkommen, dass das APIC-EM über zwei Schnittstellen verfügt, von denen eine Public und die andere Private ist. Stellen Sie in diesem Fall sicher, dass die APIC-EM-Schnittstelle, die mit dem Gerät kommuniziert, einander 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#
```

Anwenden des Zertifikats des APIC - EM

Wenn unter APIC-EM auf API Documentation (API-Dokumentation) geklickt und PKI Broker ausgewählt ist, ist diese Option verfügbar.

[POST/trust-point](#)

- Dadurch wird ein Zertifikat mit dem APIC - EM erstellt.

The screenshot displays the API Documentation for the PKI Broker Service. The left sidebar lists various services, with 'PKI Broker Service' selected. The main area shows a list of API endpoints. The 'POST /trust-point' endpoint is highlighted with a red circle. The detailed view for this endpoint includes the following information:

- 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

Dann benötigen Sie Informationen zum Gerät, und klicken Sie auf "Probieren Sie es aus".

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 ▼

Beispiel:

```

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

```

- Die hervorgehobenen Informationen sind STATIC und der Rest ist Dynamic.
- Der Entitätsname ist der Hostname des Geräts.
- Die Seriennummer, die Sie von der show version des Geräts erhalten haben.
- Der Entitätstyp kann je nach Gerätetyp geändert werden.
- Diese Informationen werden benötigt, um dem APIC-EM die Konfiguration des Geräts mitzuteilen. Hier versteht das APIC-EM die Seriennummer.

Ausgabe of 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"
}
```

Diese Ausgabe bedeutet, dass die Datei intern vom APIC-EM erstellt wird und jetzt auf dem Gerät bereitgestellt werden kann. Der nächste Schritt besteht darin, dieses Gerät in das Paket zu schieben. Um dies zu bewerkstelligen, benötigen Sie eine Vertrauenspunkt-ID. Dies kann über GET API CALL erfolgen.

[GET/Trust-Point/Seriennummer/{Seriennummer}](#) - Abfrage

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	551161908CX	Device serial-number	path	string

Error Status Codes

Sie wird Ihnen diese Ausgabe geben. Das bedeutet, dass das APIC-EM über das entsprechende Zertifikat verfügt, um das Gerät anzuschließen.

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

Schieben Sie das Zertifikat zum Gerät.

[POST/Trust-Point/{trustPointId}](#) // trustPointId muss aus der Abfrage der GET-Seriennummer kopiert werden

{"Antwort": { "PlatformId": "ASR1001", "Seriennummer": "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" }

Dadurch wird das Zertifikat an das Gerät übertragen - vorausgesetzt, es besteht eine ordnungsgemäße Verbindung.

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!

Meldung zum Erfolg der Antwort:

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

Gerät erneut überprüfen:

Sie sehen, dass jetzt beide Zertifikate eingefügt wurden:

```
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#
```

Manchmal verfügt das APIC-EM über das Zertifikat, das Gerät jedoch nicht. Wie können Sie dieses Problem beheben?

Es gibt einige Hintergrundaufgaben, bei denen Sie Zertifikate nur aus dem APIC-EM löschen können. Manchmal löscht der Kunde aus Versehen das Zertifikat vom Gerät, aber im APIC-EM ist es immer noch vorhanden. Klicken Sie auf **LÖSCHEN**.

[LÖSCHEN/Vertrauenspunkt/Seriennummer/{Seriennummer}](#) - Löschen.

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)
}

Geben Sie die Seriennummer ein und klicken Sie auf **Try It out!**.

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"
}
```