使用IOS XE PKI配置CA簽名證書

目錄

簡介

本文是設定由第三方憑證授權單位(CA)簽署的IOS XE憑證的通用指南。

本文將詳細介紹如何匯入多級CA簽名鏈結，以便裝置用作身份(ID)證書，以及如何匯入其他第三方證書以進行證書驗證。

必要條件

需求

使用IOS PKI功能時，必須配置NTP和時鐘時間。

如果管理員未配置NTP，則可能會在生成證書時產生未來日期/過去日期/時間的問題。日期或時間中的這種偏差可能會導致匯入問題和其他問題。

NTP配置示例：

```
ntp server 192.168.1.1
clock timezone EST -5
clock summer-time EDT recurring
```

採用元件

— 運行Cisco IOS® XE17.11.1a的Cisco路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

請注意，本檔案所詳述的某些功能可能在舊版IOS XE中無法使用。在可能的情況下，注意記錄何時引入或修改了命令或功能。

請始終參考指定版本IOS XE PKI功能的官方文檔，以瞭解可能與您的特定版本相關的任何限制或更改：

示例：

- IOS 15 M/T:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-pki-overview.html
- IOS XE 16.12.x:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-16-12/sec-pki-xe-16-12-book/sec-est-client-supp-pki.html
- IOS XE 17.x:https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-pki-overview-0.html

IOS XE PKI配置

在高級別，管理員在使用IOS XE PKI證書時必須執行下列操作：

1. 建立用於功能或服務的金鑰(加密金鑰生成)
2. 使用各種引數配置信任點並連結金鑰。(crypto pki trustpoint)
3. 生成證書簽名請求(CSR)(crypto pki enroll)
4. 將CSR提供給CA以供簽署(本檔案未涉及)
5. 驗證根和/或中繼CA證書(crypto pki authenticate)
6. 匯入裝置證書(crypto pki import)
7. 可選：驗證對等CA證書(crypto pki authenticate)

這些步驟將在後續章節中詳細介紹，這些章節將依據給定操作所需的命令進行分組。

crypto key generate

許多管理員輸入此命令以在路由器上啟用安全套接字外殼(SSH)，或作為某項功能的某些配置指南的一部分。但是，很少有人沒有剖析該命令的實際用途。

以以下命令為例：

```
crypto key generate rsa general-keys modulus 2048 label rsaKey exportable
crypto key generate ec keysize 521 exportable label ecKey
```

將這些命令細分為特定部分將詳細描述其用法：

- black(crypto key generate)命令的第一部分指示路由器我們將建立新金鑰。還有其它選項，例如加密金鑰匯出、加密金鑰匯入或加密金鑰零大小，這些選項將在稍後詳述。
- 命令的下一部分以綠色(rsa general-keys， ec)指示，路由器正在建立哪種型別的金鑰。在大多數情況下，將使用由公鑰/私鑰組成的Rivest-Shamir-Adleman(RSA)金鑰對，但管理員還可以配置橢圓曲線(EC)，以便使用需要ECDSA證書的功能或用於ECDHE握手的功能。
- 橙色命令定義了金鑰的大小。
    - 對於RSA，模數是術語和值，例如512-4096之間的可用選項。預設模數大小因版本而異，但建議遵循思科下一代加密的最佳實踐，並使用大於2048的金鑰。
    - 對於EC，需要key-size命令來指定金鑰中的位數。選項為256、384或512。
- 紫色命令定義此鍵的標籤。這一點非常重要，因為管理員可能需要在同一個IOS XE裝置上為各種用途定義多個金鑰。標籤用於指定與給定功能一起使用的確切金鑰。如果可能的話，始終使用標籤來區分正在使用的金鑰，並使為功能分配金鑰變得更容易。例如：標籤SSH、標籤CUBE、標籤HTTPS將建立兩個用於不同服務或功能的金鑰。
    - 金鑰的預設標籤是裝置hostname.domain。某些裝置可能會在首次啟動時生成RSA金鑰。如果不輸入標籤後修復，管理員可能面臨無意中覆蓋/重新生成錯誤金鑰的風險
- 最後一個藍色命令是可匯出的字尾。此命令詳細說明了金鑰可以與crypto pki export命令一起使用，以便匯出並用於其他系統。例如，可以匯入到對等高可用性裝置中，以便HA對的兩個成員都使用單個金鑰，或者在故障排除工具（如Wireshark）中使用單個金鑰來解密基於RSA的TLS會話。無論必須說明RSA金鑰只能從一開始就作為可匯出項建立的原因是什麼。如果管理員建立了一個不可匯出的RSA金鑰，如果不重新生成該金鑰，則無法將該金鑰設定為可匯出的，這可能會對其他功能產生漣漪效應，例如使使用該金鑰建立的所有證書失效。也就是說，通過使用命令crypto key move rsaKeyLabel non-exportable，可以將可匯出的金鑰降級為不可匯出的金鑰，而不用重新生成該金鑰

配置示例：

<#root>

```
Router(config)#
```

crypto key generate rsa general-keys modulus 2048 label rsaKey exportable

```
The name for the keys will be: rsaKey

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)

Router(config)#
```

```
crypto key generate ec keysize 521 exportable label ecKey
```

```
The name for the keys will be: ecKey
```

驗證示例：

<#root>

```
Router#
```

```
show crypto key mypubkey rsa rsaKey
```

```
% Key pair was generated at: 10:21:42 EDT Apr 14 2023
Key name: rsaKey
Key type: RSA KEYS      2048 bits
 Storage Device: not specified
 Usage: General Purpose Key
 Key is exportable. Redundancy enabled.
 Key Data:
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  [..truncated..]
  9F020301 0001

Router#
```

```
show crypto key mypubkey ec ecKey
```

```
% Key pair was generated at: 10:03:05 EDT Apr 14 2023
Key name: ecKey
Key type: EC KEYS      p521 curve
 Storage Device: private-config
 Usage: Signature Key
 Key is exportable. Redundancy enabled.
 Key Data:
  30819B30 1006072A 8648CE3D 02010605 2B810400 23038186 000401A2 A77FCD34
  [..truncated..]
  93FAC967 96ADA79E 4A245881 B2AD2F4A 279A362D F390A20F C06D5845 06DA
```

crypto pki trustpoint

信任點是「類似資料夾」的概念，用於在IOS XE中儲存和管理PKI證書。(命令語法)

高級別：

1. 每個IOS XE信任點可以包含通過crypto pki authenticate命令載入的單個根或中間CA證書。將經過身份驗證的信任點視為新增裝置現在信任的證書。
2. 每個IOS XE信任點還可以通過crypto pki import 命令匯入載入的單個身份(ID)證書。ID憑證是

這種裝置憑證，通常與某些服務或功能相關聯。
3. 管理員可以在同一信任點上使用authenticate和import命令（匯入ID證書需要該命令，稍後將對此進行討論。）使用身份驗證/匯入工作流時，信任點將包含兩個證書（根/中間+身份證書）。
4. 將信任點用於僅儲存受信任的對等根/中間CA證書時 crypto pki authenticate 命令為必填項。在這種情況下，信任點將僅包含由管理員驗證的單個證書。

注意：即將出現的有關crypto pki authenticate和crypto pki import的部分以及後面詳細介紹多級證書的身份驗證/匯入示例的部分將提供有關這四個專案的更多上下文。

信任點可以配置各種命令。這些命令可能會影響由裝置在信任點上使用crypto pki enroll 命令建立的證書簽名請求(CSR)中的值。

信任點可使用許多不同的命令（數量過多，本文檔中無法詳細說明），但下面的trustpoint示例和表中詳細列出了一些更常見的示例：

```
crypto pki trustpoint labTrustpoint
 enrollment terminal pem
 serial-number none
 fqdn none
 ip-address none
 subject-name cn=router.example.cisco.com
 subject-alt-name myrouter.example.cisco.com
 revocation-check none
 rsakeypair rsaKey
 hash sha256
```

指令	說明
crypto pki trustpoint labTrustpoint	此信任點的可讀配置標籤。用於在以後的命令中連結到功能或服務。
註冊終端pem	確定crypto pki enroll命令將執行的操作。 在此範例中，註冊終端pem表示憑證簽署請求(CSR)將以Base64 PEM格式文字輸出到終端。 其他選項(例如enrollment selfsigned)可用於建立自簽名證書，或者enrollment url可配置為定義HTTP URL並利用簡單證書註冊協定(SCEP)協定。這兩種方法都不在本檔案的範圍之內。
serial-number none	確定是否將IOS XE裝置串列新增到

	CSR。這也會在crypto pki enroll命令期間禁用提示。
fqdn none	確定是否將完全限定的域名(FQDN)新增到CSR。這也會在crypto pki enroll命令期間禁用提示。
ip-address none	確定是否將IOS XE裝置IP地址新增到CSR。這也會在crypto pki enroll命令期間禁用提示。
subject-name cn=router.example.cisco.com	指示將新增到CSR的X500已格式化。
subject-alt-name myrouter.example.cisco.com	從IOS XE 17.9.1開始，使用者替代名稱(SAN)值的逗號分隔清單可以新增到CSR。
revocation-check none	指示IOS XE裝置應如何檢查證書的有效性。如果選擇的證書頒發機構支援證書撤銷清單(CRL)、線上證書狀態協定(OCSP)等選項，則可以使用這些選項。這主要用於信任點被其他已配置的IOS XE功能或服務利用時。使用信任點對證書進行身份驗證時，也會檢查吊銷狀態。
rsakeypair rsaKey	指示命令使用具有此特定標籤的RSA金鑰對。 對於ECDSA證書，使用引用EC金鑰標籤的命令「eckeypair ecKey」
hash sha256	此命令會影響要使用的雜湊演算法的型別。選項包括SHA1、SHA256、SHA384、SHA512

crypto pki enroll

crypto pki enroll命令用於觸發給定信任點上的註冊命令。(命令語法)
對於先前顯示的示例信任點，命令crypto pki enroll labTrustpoint將以Base64 PEM文本格式向終端顯示證書簽名請求(CSR)，如下例所示。

現在，此證書簽名請求可以儲存在文本檔案中，也可以從命令列進行複製和貼上，以便提供給任何第三方CA進行驗證和簽名。

```
<#root>

Router(config)#

crypto pki enroll labTrustpoint

% Start certificate enrollment ..

% The subject name in the certificate will include: cn=router.example.cisco.com
```

```
% The fully-qualified domain name will not be included in the certificate
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwIzEhMB8GA1UEAxMYcm91dGVyLmV4YW1wbGUuY2lzY28uY29t
[..truncated..]
mGvBGUpn+cDIdFcNVzn8LQk=
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---
```

crypto pki authenticate

crypto pki authenticate命令用於將受信任CA證書新增到給定信任點。每個信任點可以進行一次身份驗證。也就是說，信任點只能包含一個CA根證書或中間證書。再次運行該命令並新增新證書將覆蓋第一個證書。

在配置了命令enrollment terminal pem後， crypto pki authenticate命令將提示路由器通過CLI上載Base64 PEM格式的證書。(命令語法)

管理員可以對信任點進行身份驗證，以便在證書鏈中新增根證書和可選的中間證書，以便以後匯入裝置的ID證書。

管理員還可以驗證信任點，以將其他受信任的根CA新增到IOS XE裝置，以便在與該對等裝置的協定握手期間啟用與對等裝置的信任關係。

為了進一步說明，對等裝置可能具有由「根CA 1」簽名的證書鏈。為了在IOS XE裝置和對等裝置之間的協定握手期間成功進行證書驗證，管理員可以使用crypto pki authenticate命令將CA證書新增到IOS XE裝置上的信任點。

需要記住的主要事項：使用crypto pki authenticate對信任點進行身份驗證始終用於將CA根或中間證書新增到信任點；而不是用於新增身份證書。請注意，此概念也應用於驗證來自其他對等裝置的自簽名證書。

以下示例顯示如何使用crypto pki authenticate命令從早期對信任點進行身份驗證：

<#root>

```
Router(config)#
```

crypto pki authenticate labTrustpoint

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
[..truncated..]
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
       Fingerprint MD5: C955FC74 7AABC184 D8A75DE7 3C9E7218
      Fingerprint SHA1: 3A99FF61 1E9E6C7B D0E567A9 96D882F5 2279C534

% Do you accept this certificate? [yes/no]:

yes

Trustpoint CA certificate accepted.
% Certificate successfully imported
```

crypto pki import

此命令用於將身份(ID)證書匯入信任點。單個信任點只能包含一個ID證書，再次發出命令將提示覆蓋以前匯入的證書。 (命令語法)

以下示例顯示如何使用crypto pki import命令將身份證書從早期的示例信任點匯入。

<#root>

```
Router(config)#

crypto pki import labTrustpoint certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
[..truncated..]
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

如果管理員在信任點驗證用於直接對此證書簽名的CA證書之前嘗試匯入證書，將會收到錯誤。

<#root>

```
Router(config)#

crypto pki import labTrustpoint certificate

% You must authenticate the Certificate Authority before
 you can import the router's certificate.
```

驗證對等CA證書

使用新增任何CA證書的相同方法將對CA證書新增到IOS XE。也就是說，使用crypto pki authenticate命令針對信任點對它們進行身份驗證。

以下命令顯示如何建立信任點和驗證對等第三方CA證書。

1. 首先使用一些描述性名稱建立一個信任點，用於儲存對等CA證書
2. 設定enrollment terminal pem，如此一來crypto pki authenticate指令就會透過指令行要求取得憑證。
3. 配置revocation-check none以在匯入過程中跳過CRL/OCSP檢查
4. 驗證信任點並提供證書
5. 根據對等CA證書的要求，對重複步驟1-4（每個信任點僅記住一個CA證書！）

<#root>

```
Router(config)#

crypto pki trustpoint PEER-ROOT

Router(ca-trustpoint)#

enrollment terminal pem

Router(ca-trustpoint)#

revocation-check none



Router(ca-trustpoint)#

crypto pki authenticate PEER-ROOT


Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
[..truncated..]
-----END CERTIFICATE-----

Certificate has the following attributes:
       Fingerprint MD5: 62D1381E 3E03D06A 912BAC4D 247EEF17
      Fingerprint SHA1: 3C97CBB4 491FC8D6 3D12B489 0C285481 64198EDB

% Do you accept this certificate? [yes/no]:

yes


Trustpoint CA certificate accepted.
% Certificate successfully imported
```

驗證一個或多個中間證書

前面的示例詳細介紹了如何使用crypto pki enroll生成CSR、使用crypto pki authenticate對根CA證書進行身份驗證，然後使用crypto pki import匯入身份證書。
但是，引入中間證書時，過程略有不同。別害怕，相同的概念和命令仍然適用！不同之處在於持有憑證的信任點的佈局方式。

請記住，每個信任點只能包含單個根或中間CA證書。因此，在我們具有如下所示的CA鏈的一個示例中，無法使用crypto pki authenticate命令新增多個CA證書：

<#root>

- Root CA

 - Intermediate CA 1

   - Identity Certificate

解決方案：

1. 建立一個信任點，該信任點將容納經過身份驗證的根CA。
2. 然後使用用於建立CSR的信任點驗證中間憑證
3. 最後將身份證書匯入到最終信任點。

使用下表可以說明使用與前一個鏈相對應的顏色的證書到命令到信任點的對映，以協助視覺化。

證書名稱	要使用的信任點	要使用的命令
根CA	crypto pki trustpoint ROOT-CA	crypto pki authenticate ROOT-CA
中繼CA 1	crypto pki trustpoint labTrustpoint	crypto pki authenticate labTrustpoint
身份證書	crypto pki trustpoint labTrustpoint	crypto pki import labTrustpoint certificate

相同的邏輯可應用於具有兩個中間CA憑證的憑證鏈結。同樣提供了顏色，以幫助直觀顯示新中間CA應用於IOS XE配置的位置。

<#root>

- Root CA

 - Intermediate CA 1

 - Intermediate CA 2

 - Identity Certificate

證書名稱	要使用的信任點	要使用的命令
根CA	crypto pki trustpoint ROOT-	crypto pki authenticate ROOT-CA

	CA	
中繼CA 1	crypto pki trustpoint INTER-CA	crypto pki authenticate INTER-CA
中繼CA 2	crypto pki trustpoint labTrustpoint	crypto pki authenticate labTrustpoint
身份證書	crypto pki trustpoint labTrustpoint	crypto pki import labTrustpoint certificate

仔細觀察就會發現兩種模式：

1. 所有根或中間證書都使用crypto pki authenticate（無論有多少個）載入到信任點。
2. 您還可以注意到，裝置身份證書（讀取直接簽署身份證書的證書）之前的最終證書始終在要匯入身份證書的同一信任點上進行身份驗證。
    - 與前面顯示的錯誤類似，IOS XE不會讓管理員在沒有先對用於直接對此證書簽名的CA證書進行驗證的情況下匯入證書。

以上兩種模式可用於兩個以上的任何數量的中間證書，儘管在大多數部署中，管理員在證書鏈中可能看到兩個以上的中間CA。

為完整起見，還提供了以下根/身份證書表：

<#root>

```
- Root CA
```

```
 - Identity Certificate
```

證書名稱	要使用的信任點	要使用的命令
根CA	crypto pki trustpoint labTrustpoint	crypto pki authenticate labTrustpoint
身份證書	crypto pki trustpoint labTrustpoint	crypto pki import labTrustpoint certificate

驗證

- 在身份驗證或匯入過程中，IOS XE會執行各種健全性檢查，以確保證書有效且格式正確。這些錯誤將列印到螢幕上，或者通過日誌(show logging)查詢以「CRYPTO_PKI」開頭的行

下面詳細介紹一些常見示例：

根據配置的時間與證書中找到的時間執行有效之前/之後檢查

<#root>

004458:

Aug 9

21:05:34.403: CRYPTO_PKI: trustpoint labTrustpoint authentication status = 0

%CRYPTO_PKI: Cert not yet valid or is expired -

start date: 05:54:04 EDT

Aug 29

2019
end   date: 05:54:04 EDT Aug 28 2022

如果未禁用revocation-check，則IOS XE將在匯入證書之前通過已配置的方法執行撤銷檢查

<#root>

003375: Aug 9 20:24:14:

%PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint ROOT failed

003376: Aug 9 20:24:14.121:

CRYPTO_PKI: enrollment url not configured

要檢視有關通過身份驗證或匯入的信任點配置的詳細資訊，請使用以下命令：

```
show crypto pki trustpoints trustpoint_name
show crypto pki certificates trustpoint_name
show crypto pki certificates verbose trustpoint_name
```

疑難排解

調試匯入問題或其他PKI問題時，使用以下調試。

```
debug crypto pki messages
debug crypto pki transactions
debug crypto pki validation
debug crypto pki api
debug crypto pki callback
!
debug ssl openssl error
debug ssl openssl msg
debug ssl openssl states
debug ssl openssl ext
```

高級IOS PKI概念

匯入PKCS12格式化的證書

某些CA提供程式可能會以PKCS#12格式(.pfx、.p12)提供回檔案。

PKCS#12是一種特殊型別的憑證格式，其中從根憑證到身分憑證的整個憑證鏈結與rsa key-pair捆綁在一起。

此格式非常便於使用IOS XE匯入，並且可以使用以下命令輕鬆匯入：

```
<#root>

Router(config)#

crypto pki import PKCS12-TP pkcs12 terminal password Cisco123


or
Router(config)#

crypto pki import PKCS12-TP pkcs12 ftp://cisco:cisco@192.168.1.1/certificate.pfx password Cisco123

% Importing pkcs12...
Address or name of remote host [192.168.1.1]?
Source filename [certificate.pfx]?
Reading file from ftp://cisco@192.168.1.1/certificate.pfx!
[OK - 2389/4096 bytes]
% You already have RSA keys named PKCS12.
% If you replace them, all router certs issued using these keys
% will be removed.
% Do you really want to replace them? [yes/no]:

yes

CRYPTO_PKI: Imported PKCS12 file successfully.
```

匯出PKCS12或PEM證書

管理員可以將證書以Base64純文字檔案PEM、Base64加密純文字檔案或PKCS12格式匯出到終端，以匯入到其他對等裝置。

這在啟動新的對等裝置時非常方便，管理員需要共用一個簽署裝置身份證書的根CA證書。

以下是一些範例語法：

```
<#root>

Router(config)#

crypto pki export labTrustpoint pem terminal
```

```
Router(config)#
crypto pki export labTrustpoint pem terminal 3des password Cisco!123
Router(config)#
crypto pki export labTrustpoint pkcs12 terminal password cisco!123
```

匯出RSA金鑰

可能需要匯出RSA金鑰，以便匯入到其他裝置或用於故障排除工作。假設金鑰對建立為可匯出的，則可以使用加密金鑰匯出命令以及加密方法(DES、3DES、AES)和密碼來匯出金鑰。

示例用法：

<#root>

```
Router(config)#
crypto key export rsa rsaKey pem terminal aes Cisco!123

% Key name: IOS-VG
   Usage: General Purpose Key
   Key data:
-----BEGIN PUBLIC KEY-----
[..truncated..]
-----END PUBLIC KEY-----

base64 len 1664-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,40E087AFF0886DA7C468D2084A0DECFB

[..truncated..]
-----END RSA PRIVATE KEY-----
```

如果金鑰無法匯出，將顯示錯誤。

<#root>

```
Router(config)#
crypto key export rsa kydavis.cisco.com pem terminal 3des mySecretPassword

% RSA keypair kydavis.cisco.com' is not exportable.
```

Import RSA Keys generated off-box

某些管理員可能會在機箱外執行RSA和證書建立，因此可以使用crypto key import命令匯入RSA金鑰，如下圖所示，使用密碼進行匯入。

<#root>

```
Router(config)#
```

crypto key import rsa rsaKey general-purpose exportable terminal mySecretPassword

```
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PUBLIC KEY-----
[..truncated..]
-----END PUBLIC KEY-----

% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9E31AAD9B7463502
[..truncated..]
-----END RSA PRIVATE KEY-----
quit
% Key pair import succeeded.
```

刪除RSA金鑰

使用命令crypto key zeroize rsa rsaKey刪除名為rsaKey的RSA金鑰對。

通過Trustpool匯入Cisco Trusted CA捆綁包

Trustpools與信任點略有不同，但核心用途相同。信任點通常包含單個CA證書時，信任池將包含多個受信任CA。

思科在https://www.cisco.com/security/pki/發佈CA捆綁包

一個常見用法是使用以下命令下載ios_core.p7b檔案：

<#root>

```
Router(config)#
```

crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_core.p7b

```
Reading file from http://www.cisco.com/security/pki/trs/ios_core.p7b
Loading http://www.cisco.com/security/pki/trs/ios_core.p7b
% PEM files import succeeded.
Router(config)#
```

常見問題

刪除信任點是否會使CSR或從給定CSR授予的證書鏈失效？

否，生成並儲存CSR後，可以在不使CSR無效的情況下刪除並重新新增信任點。

當驗證/匯入證書出錯時，思科技術支援經常使用此選項重新開始。

只要管理員或支援工程師不重新生成RSA金鑰，即可匯入CSR或簽名證書鏈。

重要事項！刪除信任點將刪除任何經過驗證/匯入的證書，如果某些服務或功能當前正在使用這些證書，則可能會產生更大的問題。

在信任點上生成CSR是否會使現有證書失效？

不，當證書即將到期時，這是常見情況。管理員可以執行crypto pki enroll命令以建立新的CSR，並在已經過身份驗證/匯入的現有證書仍在使用時開始使用CA進行證書簽名過程。管理員使用crypto pki authenticate/crypto pki import 替換證書的時間就是替換舊證書的時刻。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。