在Catalyst 9800 WLC上產生和下載CSR憑證

目錄

簡介

本檔案介紹在Catalyst 9800上產生、下載和安裝憑證的整體程式

必要條件

需求

思科建議您瞭解以下主題：

- 如何設定9800 WLC(存取點(AP))以達成基本操作
- 如何使用 OpenSSL 應用程式
- 公開金鑰基礎架構(PKI)和數位憑證

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 9800-L，Cisco IOS® XE版本17.3.3

- OpenSSL應用程式

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。

設定

在16.10.X上，9800s不支援Web驗證和Web管理的其他憑證。Web登入門戶始終使用預設證書。

在16.11.X上，可以為Web身份驗證配置專用證書，在全域性引數對映中定義信任點。

有兩個選項可取得9800 WLC的憑證。

1. 使用OpenSSL或任何其他的SSL應用程式產生憑證簽署請求(CSR)。取得您的憑證授權單位(CA)簽署的PKCS12憑證，並將其直接載入到9800 WLC。這表示私鑰與該憑證繫結。
2. 使用9800 WLC CLI產生 CSR，由CA簽署，然後手動將鏈結中的每個憑證載入到9800 WLC。

使用最符合您需求的產品。

選項1 — 載入預先存在的PKCS12簽名證書

定義簽名請求

如果您尚未獲得證書，則需要生成要授予您的CA的簽名請求。

從當前目錄（在安裝了OpenSSL的筆記型電腦上）編輯**openssl.cnf**檔案，複製並貼上這些行，以便在新建立的CSR中包括主題替代名稱(SAN)欄位。

```
[ req ]
default_bits       = 4096
distinguished_name = req_distinguished_name
req_extensions     = req_ext
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
stateOrProvinceName         = State or Province Name (full name)
localityName                = Locality Name (eg, city)
organizationName            = Organization Name (eg, company)
commonName                  = Common Name (e.g. server FQDN or YOUR name)
[ req_ext ]
subjectAltName = @alt_names
[alt_names]
DNS.1   = testdomain.com
DNS.2   = example.com
DNS.3   = webadmin.com
```

將DNS.X名稱替換為SAN。將主欄位替換為所需的證書詳細資訊。確保在SAN欄位(DNS.x)中重複公用名。Google Chrome要求URL中的名稱位於SAN欄位中才能信任憑證。

在Web管理的情況下，您還需要使用URL的變體填充SAN欄位(僅包括主機名，或者例如完全限定域名(FQDN))，以便無論瀏覽器位址列中的URL中的管理員型別是什麼，證書都匹配。

使用以下命令從OpenSSL產生CSR:

```
openssl req -out myCSR.csr -newkey rsa:4096 -nodes -keyout private.key -config openssl.cnf
```

除非向命令提供完整路徑，否則CSR會在執行OpenSSL的目錄中生成為**myCSR.csr**，其金鑰生成為**private.key**。

確保**private.key**檔案在用於加密通訊時是安全的。

可以使用以下內容驗證其內容：

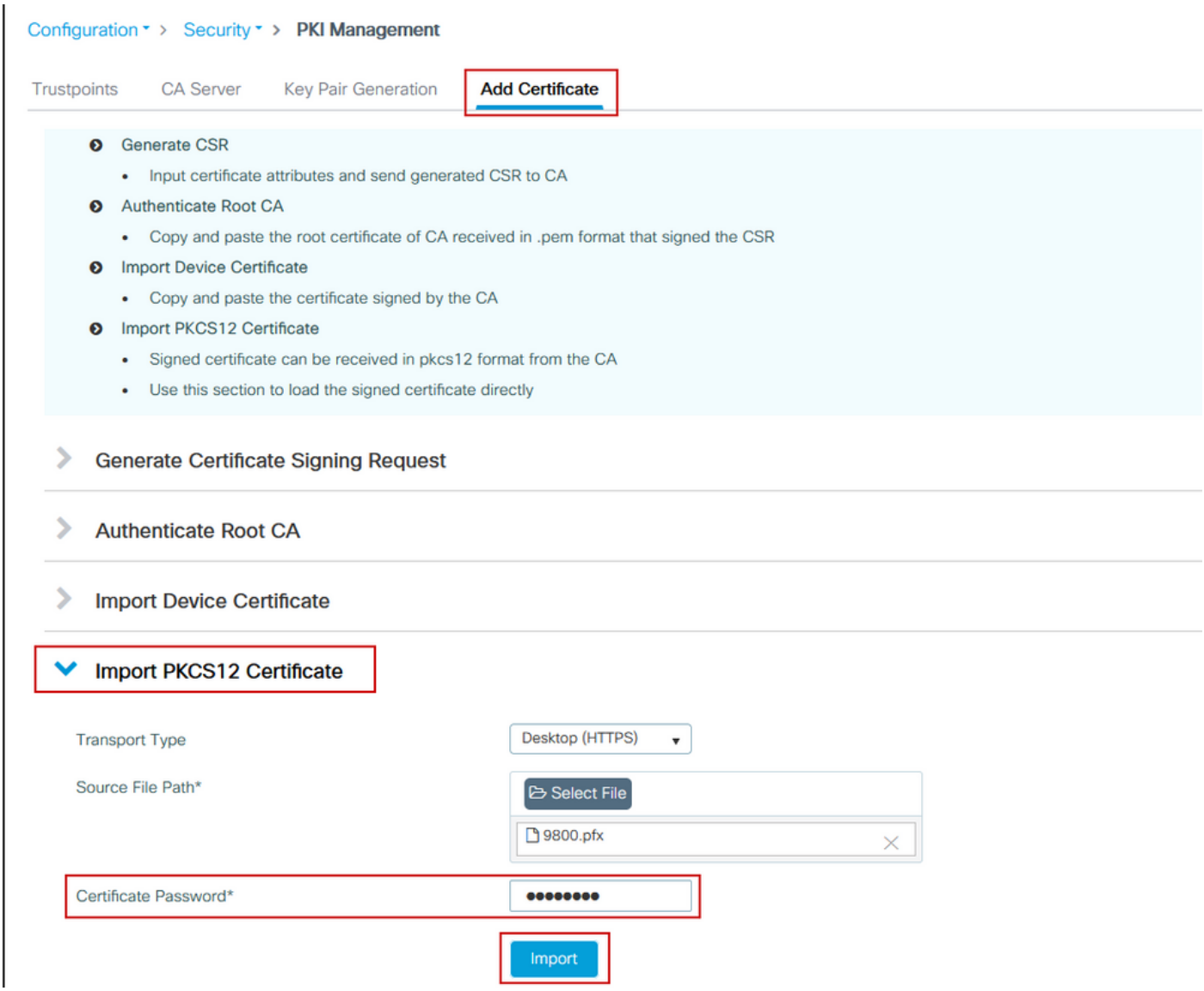
```
openssl req -noout -text -in myCSR.csr
```

然後，您可以向您的CA提供此CSR，以對其進行簽名並接收回證書。確保從CA下載完整鏈結，並確保憑證為Base64格式，以防需要進一步操作。

匯入證書

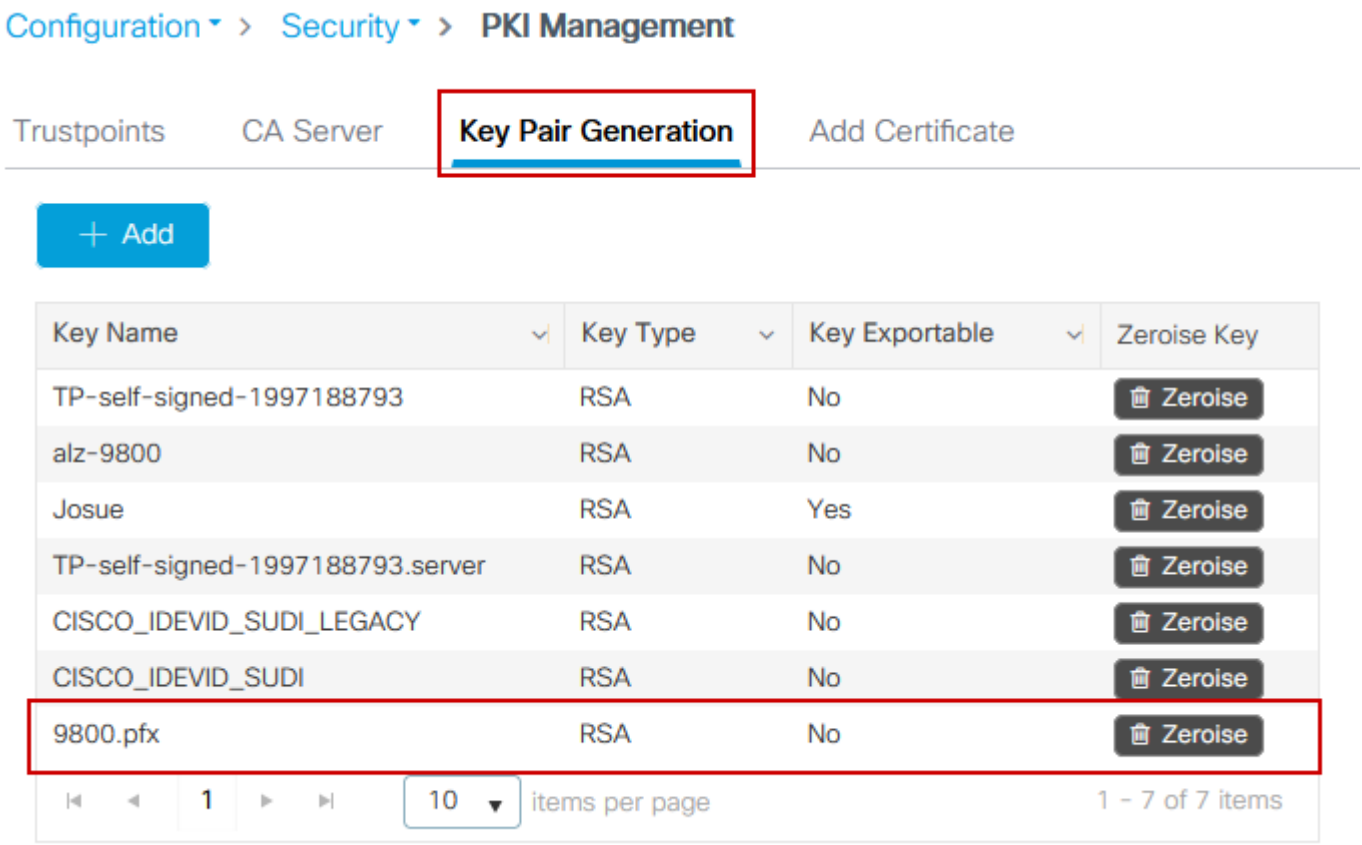
步驟1.在可從9800 WLC連線的簡單式檔案傳輸通訊協定(TFTP)伺服器上儲存PKCS12憑證。PKCS12證書必須包含私鑰以及直至根CA的證書鏈。

步驟2.開啟9800 WLC GUI並導航到**Configuration > Security > PKI Management**，然後點選**Add Certificate**頁籤。**展開Import PKCS12 Certificate**選單，並填寫TFTP詳細資訊。或者，**Transport Type**下拉清單中的**Desktop(HTTPS)**選項允許透過瀏覽器進行HTTP上傳。**Certificate Password**是指生成PKCS12證書時使用的密碼。



步驟3.驗證資訊是否正確，然後按一下**Import（匯入）。此後，您將在金鑰對生成**頁籤中看到為此新信任點安裝的新證書金鑰對。成功匯入後，9800 WLC還會為多級CA建立額外的信任點。

註：目前，每當特定信任點用於webauth或webadmin時，9800 WLC不會顯示完整的憑證鏈結，而是顯示裝置憑證及其直接頒發者。此追蹤專案使用思科錯誤ID CSCwa23606 ，已在Cisco IOS® XE 17.8中修正。



CLI:

```
9800# configure terminal
9800(config)#crypto pki import
```

註：證書檔名和信任點名稱必須與9800 WLC完全匹配，以便為多級CA建立任何其他信任點。

多級CA場景中的PKCS12格式轉換和證書鏈。

最後可能會遇到這樣的情況：您有一個PEM或CRT格式的私鑰檔案和證書，並且希望將它們組合成PKCS12(.pfx)格式，以便上傳到9800 WLC。若要執行此操作，請輸入以下命令：

```
openssl pkcs12 -export -in
```

如果您有一個憑證鏈結（一個或多個中繼CA和根CA）全部採用PEM格式，則需要將所有憑證合併到一個.pfx檔案中。

首先，手動將CA憑證合併到單一檔案中。將內容複製並貼上在一起（以.pem格式儲存檔案）：

```
----- BEGIN Certificate --------
<intermediate CA cert>
------END Certificate --------
-----BEGIN Certificate -----
<root CA cert>
-----END Certificate--------
```

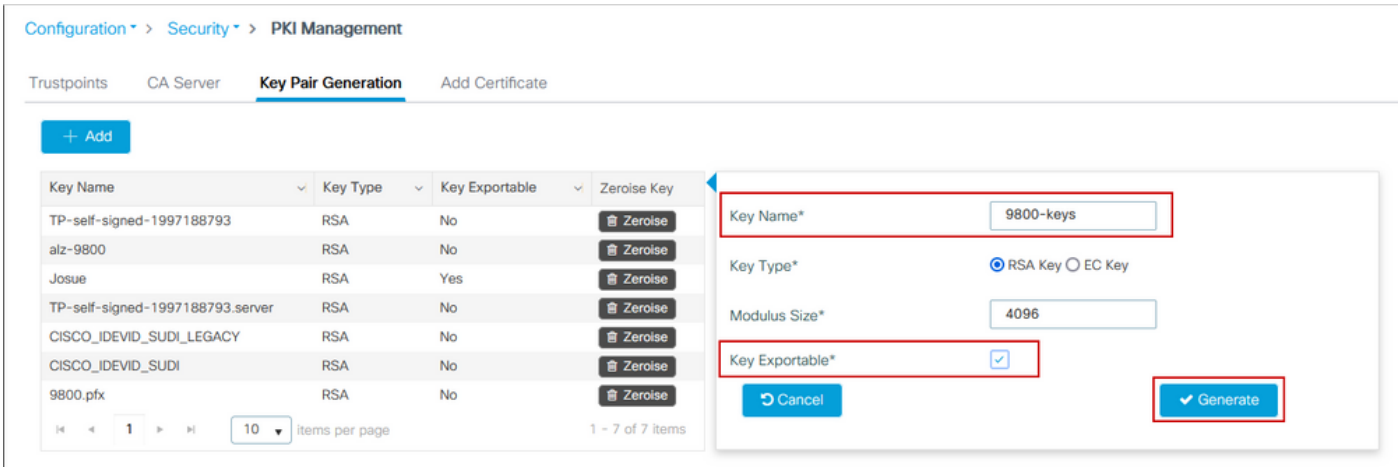
稍後，您可以將所有的PKCS12證書檔案與：

```
openssl pkcs12 -export -out chaincert.pfx -inkey
```

請參閱本文結尾的驗證一節，檢視最終證書的外觀。

選項2 — 在9800 WLC上定義金鑰和簽署請求(CSR)

步驟1.生成通用RSA金鑰對。導覽至**Configuration > Security > PKI Management**，選擇**Key Pair Generation**頁籤，然後按一下**+ Add**。輸入詳細資訊，確保選中**Key Exportable**覈取方塊，然後按一下**Generate**。



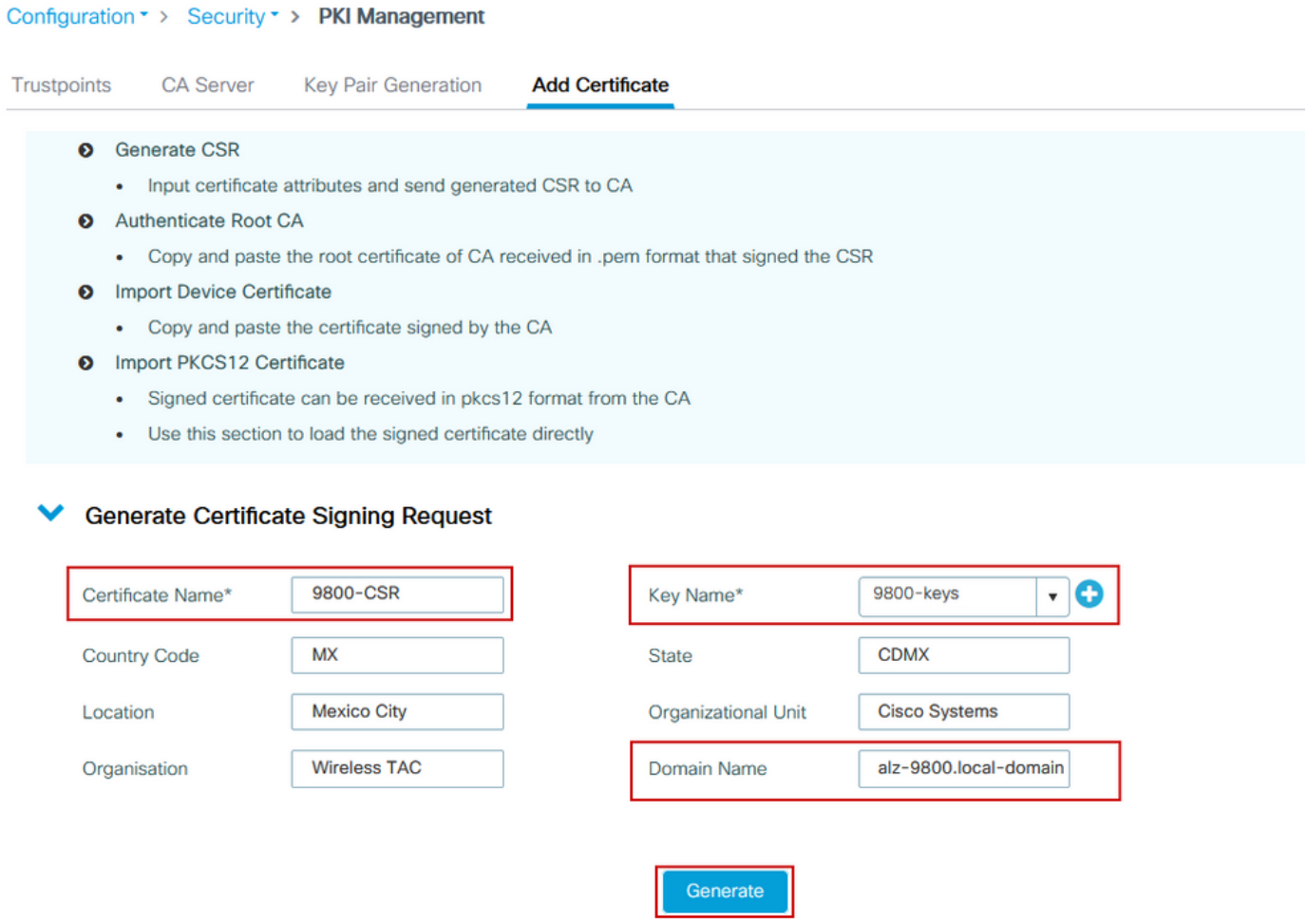
CLI配置：

```
9800(config)#crypto key generate rsa general-keys label 9800-keys exportable
The name for the keys will be: 9800-keys
Choose the size of the key modulus in the range of 512 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [1024]: 4096
```

```
% Generating 4096 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 9 seconds)
```

步驟2.產生9800 WLC的CSR。導航到**Add Certificate**頁籤，然後展開**Generate Certificate Signing Request**，填寫詳細資訊，並從下拉選單中選擇先前建立的金鑰對。**網域名稱**必須與9800 WLC上為使用者端存取定義的URL（Web管理頁面、Web驗證頁面等）相符，**Certificate Name**是信任點名稱，因此您可以根據信任點名稱的使用進行命名。

註:9800 WLC支援在其通用名稱中使用萬用字元引數的憑證。



確保資訊正確，然後按一下**Generate**。這會在原始表單旁邊的文本框中顯示CSR。

複製會將副本儲存到剪貼簿，以便您可以將其貼上到文本編輯器並儲存CSR。如果選擇「**Save to device**」，9800 WLC會建立CSR的副本並將其儲存在**bootflash:**/csr中。例如，運行以下命令：

```
9800#dir bootflash:/csr
Directory of bootflash:/csr/
```

```
1046531 -rw- 1844 Sep 28 2021 18:33:49 +00:00 9800-CSR1632856570.csr

26458804224 bytes total (21492699136 bytes free)
9800#more bootflash:/csr/9800-CSR1632856570.csr
-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----
```

CLI配置：

```
9800(config)#crypto pki trustpoint 9800-CSR
9800(ca-trustpoint)#enrollment terminal pem
9800(ca-trustpoint)#revocation-check none
9800(ca-trustpoint)#subject-name C=MX, ST=CDMX, L=Mexico City, O=Cisco Systems, OU=Wireless TaC,
CN=alz-9800.local-domain.com
9800(ca-trustpoint)#rsakeypair 9800-keys
9800(ca-trustpoint)#subject-alt-name domain1.mydomain.com,domain2.mydomain.com
9800(ca-trustpoint)#exit

(config)#crypto pki enroll 9800-CSR
% Start certificate enrollment ..

% The subject name in the certificate will include: C=MX, ST=CDMX, L=Mexico City, O=Cisco
Systems, OU=Wireless TaC, CN=alz-9800.local-domain.com
% The subject name in the certificate will include: alz-9800
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----

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

Redisplay enrollment request? [yes/no]: no
```

可用於使用者名稱配置的引數：

C：國家，只能是兩個大寫字母。

ST：某些州/省，是指州或省的名稱。

L:位置名稱，指城市。

O:組織名稱，是指公司。

OU：組織單位名稱，請參閱一節。

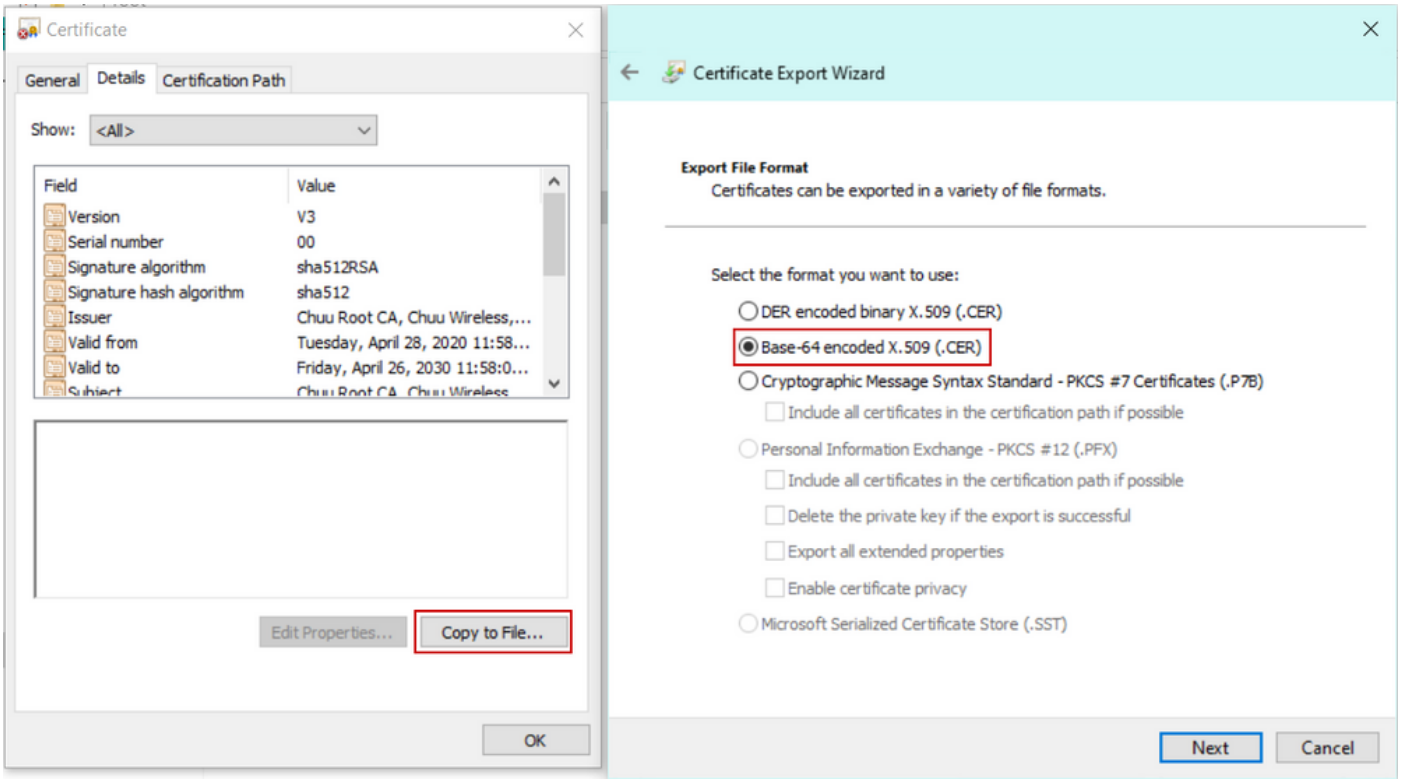
CN:(一般名稱)指將證書頒發到的主題，您必須指定要訪問的特定IP地址（無線管理IP、虛擬IP等）或使用FQDN配置的主機名。

> **註**：如果要新增使用者替代名稱，則在17.8.1之前的Cisco IOS XE版本上由於思科錯誤ID CSCvt15177而無法使用 .此案例可能由於SAN不存在而導致某些瀏覽器警報，為了避免出現這種情況，請在系統外建立登錄檔項和CSR，如選項1所示。

步驟3.讓您的憑證授權單位(CA)簽署您的CSR。需要將完整字串傳送到CA以對其進行簽名。

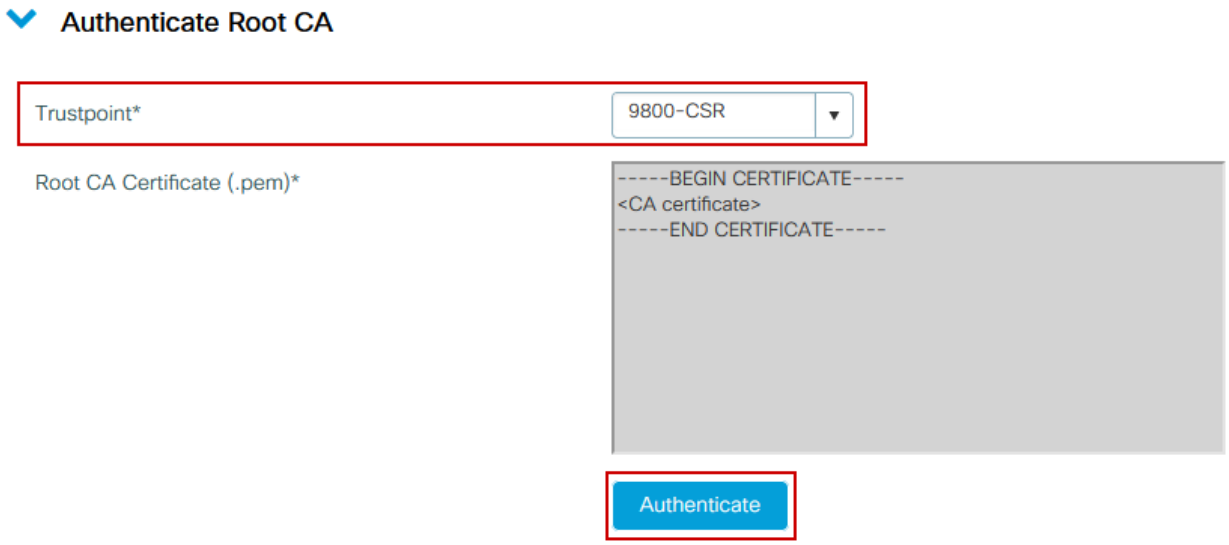
```
-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----
```

如果使用Windows Server CA對證書進行簽名，請以Base64格式下載已簽名的證書。否則，您需要使用Windows cert manager等實用程式進行匯出。



> **註**：信任點身份驗證過程取決於簽署CSR的CA數量。如果有單級CA，請檢查**步驟4a。**如果有多級CA，請轉至**步驟4b**。這是必需的，因為信任點一次只能儲存兩個證書（主題證書和頒發者證書）。

步驟4a.使9800信任頒發者CA。以.pem格式(Base64)下載頒發者CA證書。展開同一選單中的**Authentication Root CA**部分，從**Trustpoint**下拉選單中選擇先前定義的信任點，然後貼上頒發者CA證書。確保詳細資訊配置正確，然後按一下**Authenticate**。



CLI配置：

```
9800(config)# crypto pki authenticate 9800-CSR

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

-----BEGIN CERTIFICATE-----
```

```
Certificate has the following attributes: Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809 % Do you accept this certificate?
[yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

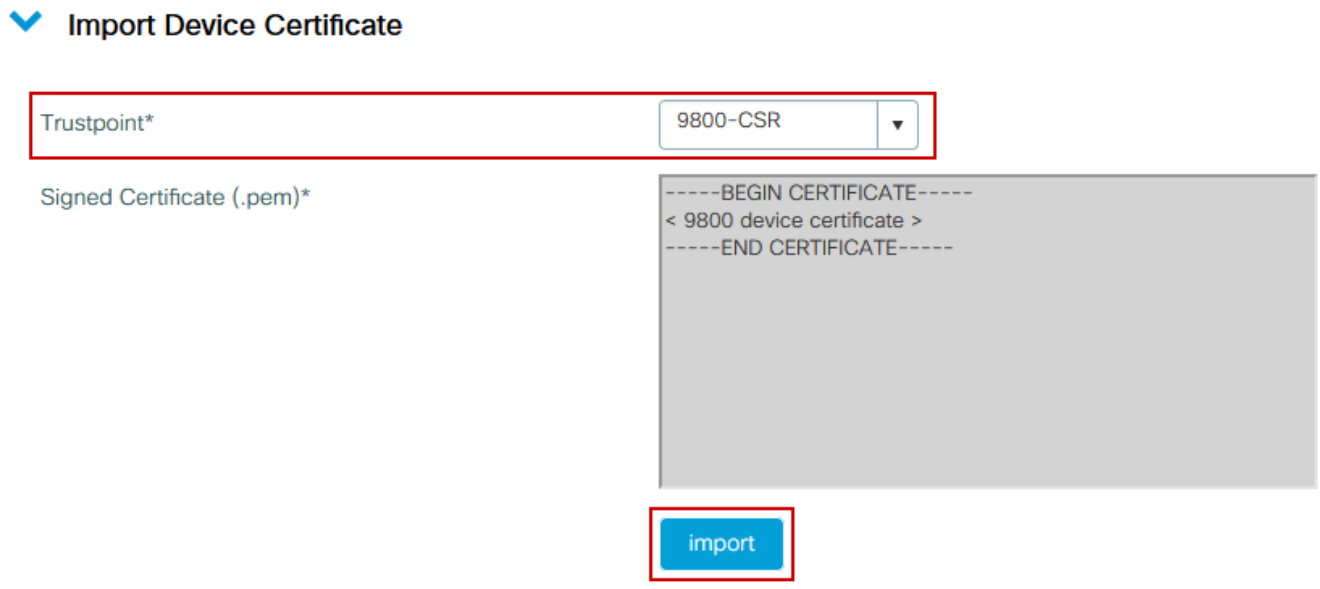
第4b步：在有多個授權級別的情況下，每個CA級別都需要一個新的信任點。這些信任點僅包含身份驗證證書並指向下一個身份驗證級別。此程式只在CLI中完成，在本範例中有一個中間CA和一個根CA:

```
9800(config)#crypto pki trustpoint root
9800(ca-trustpoint)#enrollment terminal
9800(ca-trustpoint)#chain-validation stop
9800(ca-trustpoint)#revocation-check none
9800(ca-trustpoint)#exit
9800(config)#crypto pki authenticate root

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

-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 6CAC00D5 C5932D01 B514E413 D41B37A8
Fingerprint SHA1: 5ABD5667 26B7BD0D 83BDFC34 543297B7 3D3B3F24

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

9800(config)#crypto pki trustpoint 9800-CSR
9800(ca-trustpoint)#chain-validation continue root
9800(config)#crypto pki authenticate 9800-CSR

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

-----BEGIN CERTIFICATE-----




-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809
Certificate validated - Signed by existing trustpoint CA certificate.

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

註：如果認證鏈中有多個中繼CA，則每個額外的認證級別必須生成一個新的信任點。此信任點必須使用**chain-validation continue <trustpoint-name>**命令引用包含下一級證書的信任點。

步驟5.將已簽名的憑證載入到9800 WLC。在同一選單中展開**Import Device Certificate**部分。選擇先前定義的**Trustpoint**，並貼上CA提供的已簽名的裝置證書。驗證憑證資訊後，按一下**import**。



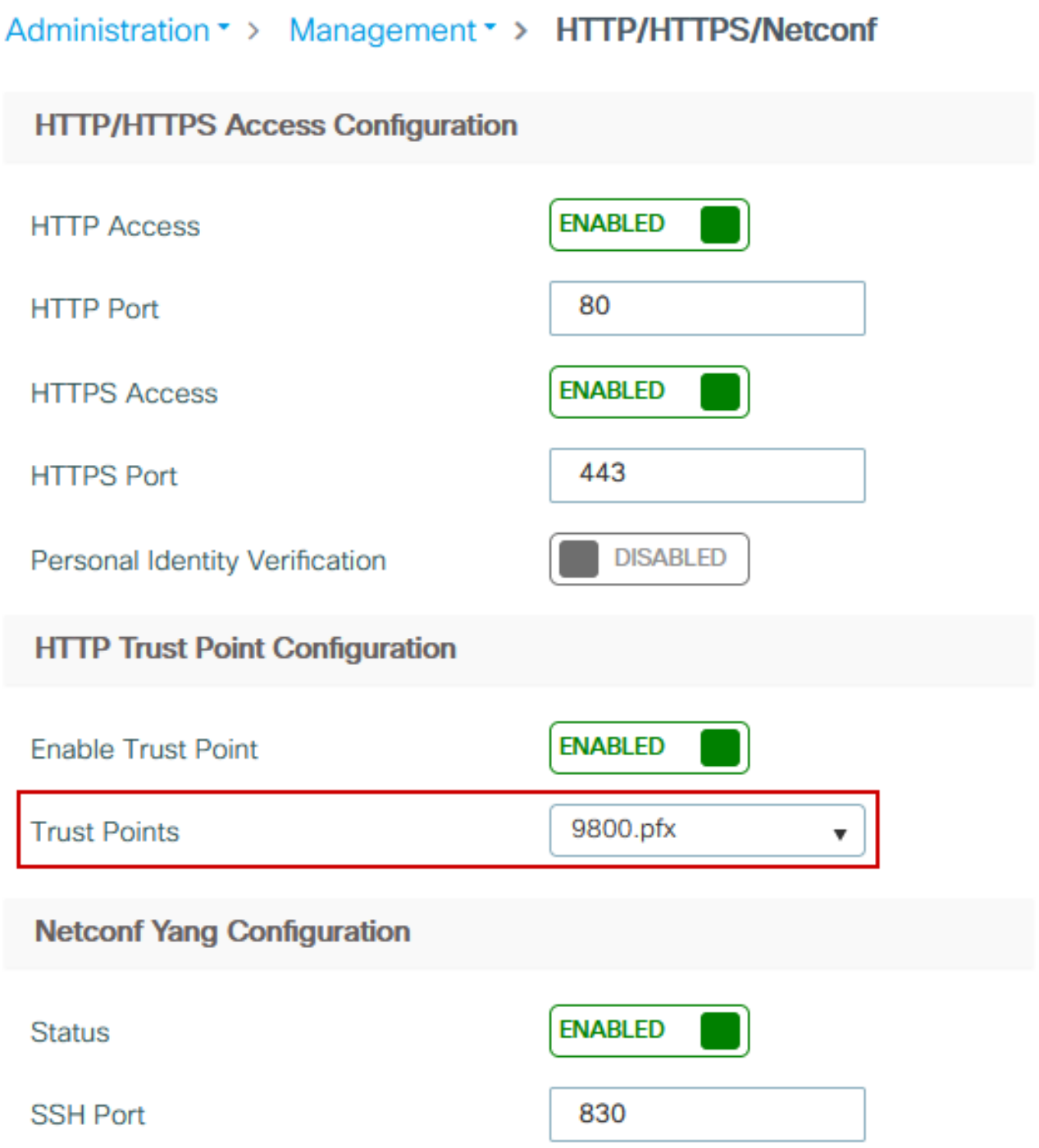
CLI配置：

```
9800(config)#crypto pki import 9800-CSR certificate

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

-----BEGIN CERTIFICATE-----
<9800 device certificate >
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

使用新證書

Web管理

導覽至Administration > Management > HTTP/HTTPS/Netconf，然後從Trust Points下拉式清單中選擇匯入的憑證。

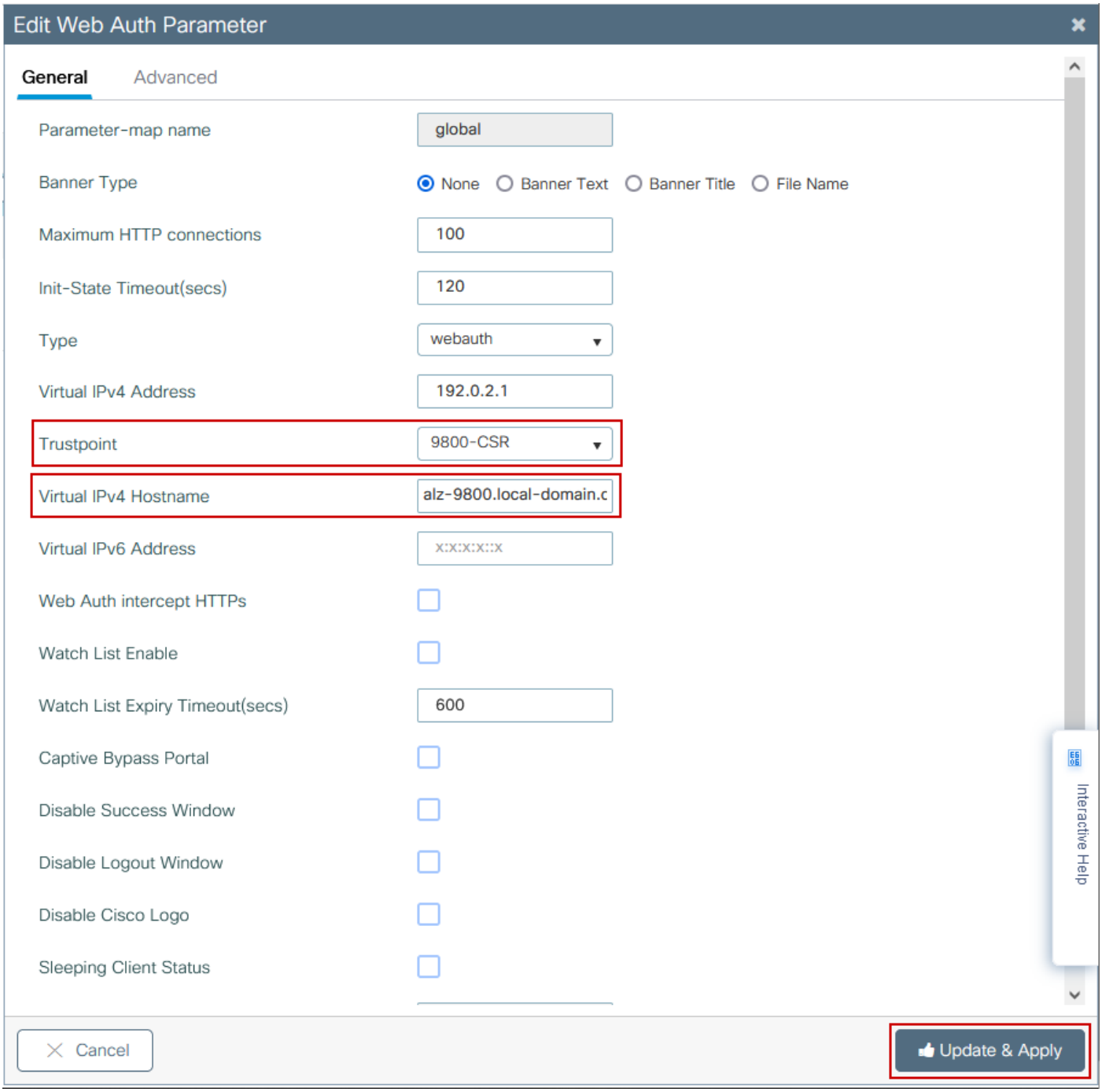


CLI配置：

```
9800(config)#ip http secure-trustpoint 9800.pfx
9800(config)#no ip http secure-server
9800(config)#ip http secure-server
```

本地Web驗證

導覽至Configuration > Security > Web Auth，選擇global引數貼圖，然後從Trustpoint下拉選單中選擇匯入的信任點。按一下「Update & Apply」以儲存變更。確保**虛擬IPv4主機名稱**與證書中的公用名匹配。



CLI配置：

```
9800(config)#parameter-map type webauth global
9800(config-params-parameter-map)#type webauth
9800(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1 virtual-host alz-9800.local-domain.com
9800(config-params-parameter-map)#trustpoint 9800-CSR
```

若要更新證書使用情況，請重新啟動HTTP服務：

```
9800(config)#no ip http server
9800(config)#ip http server
```

.

高可用性注意事項

在為狀態切換高可用性(HA SSO)配置的9800對上，所有證書在初始批次同步時從主證書複製到輔助證書。這包括私鑰在控制器上生成的證書，即使RSA金鑰配置為不可匯出。建立HA配對後，兩個控制器上都會安裝任何新的憑證，且系統會即時複製所有憑證。

失敗後，先前從輔助控制器現在處於活動狀態的控制器透明地使用從主控制器繼承的證書。

如何確保Web瀏覽器信任證書

確保Web瀏覽器信任證書有一些重要的注意事項：

- 其公用名（或SAN欄位）必須與瀏覽器訪問的URL匹配。
- 必須在有效期內。
- 必須由瀏覽器信任其根的CA或CA鏈頒發。為此，由Web伺服器提供的證書必須包含鏈中的所有證書，直到（不必包括）客戶端瀏覽器（通常是根CA）信任的證書為止。
- 如果它包含撤銷清單，瀏覽器需要能夠下載這些清單，並且必須不列出證書CN。

驗證

可以使用以下命令驗證證書配置：

```
9800#show crypto pki certificate 9800.pfx

Certificate
Status: Available
Certificate Serial Number (hex): 1236
Certificate Usage: General Purpose
Issuer:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Subject:
Name: alz-9800
e=user@example.com
cn=alz-9800
ou=Cisco Systems
o=Wireless TAC
l=CDMX
st=CDMX
c=MX
Validity Date:
start date: 17:54:45 Pacific Sep 28 2021
end date: 17:54:45 Pacific Sep 26 2031
Associated Trustpoints: 9800.pfx

CA Certificate
Status: Available
Certificate Serial Number (hex): 1000
Certificate Usage: Signature
Issuer:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
```

```
c=MX
Subject:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Validity Date:
start date: 05:10:34 Pacific Apr 29 2020
end date: 05:10:34 Pacific Apr 27 2030
Associated Trustpoints: 9800.pfx
```

```
9800#show ip http server secure status

HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha aes-128-cbc-sha
aes-256-cbc-sha dhe-aes-128-cbc-sha ecdhe-rsa-3des-ede-cbc-sha
rsa-aes-cbc-sha2 rsa-aes-gcm-sha2 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2
ecdhe-rsa-aes-cbc-sha2 ecdhe-rsa-aes-gcm-sha2
HTTP secure server TLS version: TLSv1.2 TLSv1.1 TLSv1.0
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: 9800.pfx
HTTP secure server active session modules: ALL
```

您可以在9800上驗證您的憑證鏈結。如果裝置證書是由中間CA簽發的，而中間CA本身是由根CA簽發的，則您有一個由兩個證書組成的組組成的信任點，因此每個級別都有自己的信任點。在這種情況下，9800 WLC的9800.pfx包含裝置憑證（WLC憑證）及其核發CA（中繼CA）。然後是另一個信任點，該信任點具有發出該中間CA的根CA。

```
9800#show crypto pki certificate 9800.pfx
Certificate
Status: Available
Certificate Serial Number (hex): 1236
Certificate Usage: General Purpose
Issuer:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Subject:
Name: alz-9800
e=user@example.com
cn=alz-9800
ou=Cisco Systems
o=Wireless TAC
l=CDMX
st=CDMX
c=MX
Validity Date:
start date: 17:54:45 Pacific Sep 28 2021
end date: 17:54:45 Pacific Sep 26 2031
Associated Trustpoints: 9800.pfx

CA Certificate
Status: Available
Certificate Serial Number (hex): 1000
Certificate Usage: Signature
Issuer:
cn=Chuu Root CA
ou=Chuu Wireless
```

```
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Subject:
cn=Chuu Intermediate CA
ou=Chuu Wireless
o=Chuu Inc
st=CDMX
c=MX
Validity Date:
start date: 05:10:34 Pacific Apr 29 2020
end date: 05:10:34 Pacific Apr 27 2030
Associated Trustpoints: 9800.pfx

9800#show crypto pki certificate 9800.pfx-rrr1
CA Certificate
Status: Available
Certificate Serial Number (hex): 00
Certificate Usage: Signature
Issuer:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Subject:
cn=Chuu Root CA
ou=Chuu Wireless
o=Chuu Inc
l=Iztapalapa
st=CDMX
c=MX
Validity Date:
start date: 04:58:05 Pacific Apr 29 2020
end date: 04:58:05 Pacific Apr 27 2030
Associated Trustpoints: 9800-CSR 9800.pfx-rrr1
```

使用OpenSSL的憑證驗證

OpenSSL在驗證憑證本身或執行某些轉換作業方面可能會很有用。

若要顯示使用OpenSSL的憑證：

```
openssl x509 -in
```

若要顯示CSR的內容：

```
openssl req -noout -text -in
```

如果您想驗證9800 WLC上的終端憑證，但希望使用瀏覽器以外的其他用途，OpenSSL可以執行此

操作並提供許多詳細資訊。

```
openssl s_client -showcerts -verify 5 -connect
```

您可以使用9800的WebAdmin的URL或訪客輸入網站的URL（虛擬IP）替換<wlcURL>。您還可以將IP地址放在此處。它會告訴您收到的證書鏈，但是使用IP地址代替主機名時，證書驗證永遠不能100%正確。

要檢視內容並驗證PKCS12(.pfx)證書或證書鏈：

```
openssl pkcs12 -info -in
```

以下是憑證鏈結上的此命令範例，其中裝置憑證是由名為「intermediate.com」的中間CA（其本身由名為「root.com」的根CA核發）核發給技術協助中心(TAC):

```
openssl pkcs12 -info -in chainscript2.pfx
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
localKeyID: 1D 36 8F C2 4B 18 0B 0D B2 57 A2 55 18 96 7A 8B 57 F9 CD FD
subject=/C=BE/ST=Diegem/L=Diegem/O=Cisco/CN=TAC
issuer=/C=BE/ST=Diegem/O=Cisco/OU=TAC/CN=intermediate.com/emailAddress=int@int.com
-----BEGIN CERTIFICATE-----
<Device certificate >
-----END CERTIFICATE-----
Certificate bag
Bag Attributes: <No Attributes>
subject=/C=BE/ST=Diegem/O=Cisco/OU=TAC/CN=intermediate.com/emailAddress=int@int.com
issuer=/C=BE/ST=Diegem/L=Diegem/O=Cisco/OU=TAC/CN=RootCA.root.com/emailAddress=root@root.com
-----BEGIN CERTIFICATE-----
<Intermediate certificate >
-----END CERTIFICATE-----
Certificate bag
Bag Attributes: <No Attributes>
subject=/C=BE/ST=Diegem/L=Diegem/O=Cisco/OU=TAC/CN=RootCA.root.com/emailAddress=root@root.com
issuer=/C=BE/ST=Diegem/L=Diegem/O=Cisco/OU=TAC/CN=RootCA.root.com/emailAddress=root@root.com
-----BEGIN CERTIFICATE-----
<Root certificate >
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
localKeyID: 1D 36 8F C2 4B 18 0B 0D B2 57 A2 55 18 96 7A 8B 57 F9 CD FD
Key Attributes: <No Attributes>
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

```
<Private key >
-----END ENCRYPTED PRIVATE KEY-----
```

疑難排解

使用以下命令進行疑難排解。如果在遠端會話（SSH或telnet）上完成，則需要terminal monitor來顯示輸出：

```
9800#debug crypto pki transactions
```

成功的方案調試輸出

此輸出顯示了在9800上成功匯入證書時的預期輸出。使用此命令作為參考並確定故障狀態：

```
Sep 28 17:35:23.242: CRYPTO_PKI: Copying pkcs12 from bootflash:9800.pfx
Sep 28 17:35:23.322: CRYPTO_PKI: Creating trustpoint 9800.pfx
Sep 28 17:35:23.322: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: 9800.pfx created succesfully
Sep 28 17:35:23.324: CRYPTO_PKI: examining cert:
Sep 28 17:35:23.324: CRYPTO_PKI: issuerName=cn=Chuu Intermediate CA,ou=Chuu Wireless,o=Chuu
Inc,st=CDMX,c=MX
Sep 28 17:35:23.324: CRYPTO_PKI: subjectname=e=user@example.com,cn=alz-9800,ou=Cisco
Systems,o=Wireless TAC,l=CDMX,st=CDMX,c=MX
Sep 28 17:35:23.324: CRYPTO_PKI: adding RSA Keypair
Sep 28 17:35:23.324: CRYPTO_PKI: bitValue of ET_KEY_USAGE = 140
Sep 28 17:35:23.324: CRYPTO_PKI: Certificate Key Usage = GENERAL_PURPOSE
Sep 28 17:35:23.324: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named 9800.pfx has been generated or
imported by pki-pkcs12
Sep 28 17:35:23.331: CRYPTO_PKI: adding as a router certificate.Public key in cert and stored
public key 9800.pfx match

Sep 28 17:35:23.333: CRYPTO_PKI: examining cert:
Sep 28 17:35:23.333: CRYPTO_PKI: issuerName=cn=Chuu Root CA,ou=Chuu Wireless,o=Chuu
Inc,l=Iztapalapa,st=CDMX,c=MX
Sep 28 17:35:23.333: CRYPTO_PKI: subjectname=cn=Chuu Intermediate CA,ou=Chuu Wireless,o=Chuu
Inc,st=CDMX,c=MX
Sep 28 17:35:23.333: CRYPTO_PKI: no matching private key presents.

[...]

Sep 28 17:35:23.335: CRYPTO_PKI: Setting the key_type as RSA
Sep 28 17:35:23.335: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Sep 28 17:35:23.335: CRYPTO_PKI:Peer's public inserted successfully with key id 21
Sep 28 17:35:23.336: Calling pkiSendCertInstallTrap to send alert
Sep 28 17:35:23.337: CRYPTO_PKI: Deleting cached key having key id 31
Sep 28 17:35:23.337: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Sep 28 17:35:23.337: CRYPTO_PKI:Peer's public inserted successfully with key id 32
Sep 28 17:35:23.338: CRYPTO_PKI: (A0323) Session started - identity selected (9800.pfx)
Sep 28 17:35:23.338: CRYPTO_PKI: Rcvd request to end PKI session A0323.
Sep 28 17:35:23.338: CRYPTO_PKI
alz-9800#: PKI session A0323 has ended. Freeing all resources.
Sep 28 17:35:23.338: CRYPTO_PKI: unlocked trustpoint 9800.pfx, refcount is 0
Sep 28 17:35:23.338: CRYPTO_PKI: Expiring peer's cached key with key id 32Public key in cert and
stored public key 9800.pfx match

Sep 28 17:35:23.341: Calling pkiSendCertInstallTrap to send alert
Sep 28 17:35:23.341: CRYPTO_PKI: cert verified and inserted.
Sep 28 17:35:23.402: CRYPTO_PKI: Creating trustpoint 9800.pfx-rrr1
Sep 28 17:35:23.402: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: 9800.pfx-rrr1 created succesfully
```

```
Sep 28 17:35:23.403: CRYPTO_PKI: Setting the key_type as RSA
Sep 28 17:35:23.404: CRYPTO_PKI: Attempting to insert the peer's public key into cache
Sep 28 17:35:23.404: CRYPTO_PKI:Peer's public inserted successfully with key id 22
Sep 28 17:35:23.405: Calling pkiSendCertInstallTrap to send alert
Sep 28 17:35:23.406: CRYPTO_PKI: no CRLs present (expected)
Sep 28 17:35:23.406: %PKI-6-PKCS12_IMPORT_SUCCESS: PKCS #12 import in to trustpoint 9800.pfx
successfully imported.
```

嘗試匯入沒有CA的PKCS12證書

如果您匯入證書並收到錯誤：「未找到CA證書。」，則表示.pfx檔案不包含整個鏈或一個CA不存在。

```
9800(config)#crypto pki import pkcs12.pfx pkcs12 bootflash:pks12.pfx password
```

```
% Importing pkcs12...
Source filename [pks12.pfx]?
Reading file from bootflash:pks12.pfx
% Warning: CA cert is not found. The imported certs might not be usable.
```

如果運行命令openssl pkcs12 -info -in <path to cert>，但只會顯示一個具有一個私鑰的憑證，則表示CA不存在。根據經驗法則，此命令理想地列出您的整個憑證鏈結。如果客戶端瀏覽器已經知道頂部根CA，則不需要包含它。

解決此問題的一種方法是將PKCS12解構為PEM並正確重建該鏈。在下一個示例中，我們有一個.pfx檔案，該檔案只包含裝置(WLC)證書及其金鑰。它是由一個中間CA（在PKCS12檔案中不存在）發出的，而中間CA又由已知的根CA簽名。

步驟1。將私鑰匯出出去。

```
openssl pkcs12 -in
```

步驟2.將憑證匯出為PEM。

```
openssl pkcs12 -in
```

步驟3.將中間CA憑證下載為PEM。

CA的來源取決於其性質。如果它是公共CA，則聯機搜尋足以查詢儲存庫。否則，CA管理員必須提供Base64格式(.pem)的證書。如果有多個級別的CA，請將其分組到一個檔案中，與選項1匯入過程結束時所顯示的**檔案**類似。

步驟4.從金鑰、裝置證書和CA證書重建PKCS 12。

```
openssl pkcs12 -export -out fixedcertchain.pfx -inkey cert.key -in certificate.pem -certfile CA.pem
```

我們現在有「fixedcertchain.pfx」，可以方便地將其匯入Catalyst 9800!

註釋和限制

- Cisco IOS® XE不支援有效期超過2099的CA證書：思科錯誤ID CSCvp64208
- Cisco IOS® XE不支援SHA256 message digest PKCS 12套件（支援SHA256證書，但如果PKCS12套件本身已使用SHA256簽名，則不支援）：Cisco錯誤ID CSCvz41428
- 如果WLC需要攜帶使用者證書，並且可以通過網際網路訪問NAC/ISE裝置（例如，在SD-WAN部署中），則可以看到分段。憑證幾乎一律大於1500位元組（這表示傳送憑證訊息時會傳送多個RADIUS封包），如果網路路徑中有多個不同的MTU，則可能會發生RADIUS封包本身的過度分段。在這種情況下，我們建議您透過相同路徑傳送用於WLC流量的所有UDP資料包，以避免網際網路天氣可能導致的延遲/抖動等問題

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）。