Erstellen und Herunterladen von CSR-Zertifikaten auf Catalyst 9800 WLCs

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[Option 1 - Laden eines vorhandenen signierten PKCS12-Zertifikats](#)
[Signierungsanforderung definieren](#)
[Zertifikat importieren](#)
[PKCS12-Formatumwandlung und Zertifikatkette in Szenarien mit mehrstufigen Zertifizierungsstellen.](#)
[Option 2 - Definieren eines Key and Signing Request (CSR) auf dem 9800 WLC](#)
[Neues Zertifikat verwenden](#)
[Webverwaltung](#)
[Lokale Webauthentifizierung](#)
[Überlegungen zur Hochverfügbarkeit](#)
[Sicherstellen, dass das Zertifikat von Webbrowsern als vertrauenswürdig eingestuft wird](#)
[Überprüfung](#)
[Zertifikatsverifizierung mit OpenSSL](#)
[Fehlerbehebung](#)
[Erfolgreiche Szenario-Debug-Ausgabe](#)
[Versuchen Sie, ein PKCS12-Zertifikat zu importieren, das keine Zertifizierungsstelle besitzt.](#)
[Hinweise und Einschränkungen](#)

Einleitung

Dieses Dokument beschreibt den gesamten Prozess zum Generieren, Herunterladen und Installieren von Zertifikaten auf dem Catalyst 9800.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfigurieren des 9800 WLC, des Access Points (AP) für den Basisbetrieb
- Verwendung der OpenSSL-Anwendung
- Public Key Infrastructure (PKI) und digitale Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 9800-L, Cisco IOS® XE Version 17.3.3
- OpenSSL-Anwendung

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Am 16.10.X unterstützen 9800s kein anderes Zertifikat für die Webauthentifizierung und Webadministration. Das Portal für die Webanmeldung verwendet immer das Standardzertifikat.

Auf 16.11.X können Sie ein dediziertes Zertifikat für die Webauthentifizierung konfigurieren und den Vertrauenspunkt in der globalen Parameterzuordnung definieren.

Es gibt zwei Optionen, um ein Zertifikat für einen 9800 WLC zu erhalten.

1. Erstellen Sie eine CSR-Anforderung (Certificate Signing Request) mit OpenSSL oder einer anderen SSL-Anwendung. Holen Sie sich ein PKCS12-Zertifikat, das von Ihrer Zertifizierungsstelle (Certificate Authority, CA) signiert wurde, und laden Sie es direkt auf den 9800 WLC. Das bedeutet, dass der private Schlüssel mit diesem Zertifikat gebündelt ist.
2. Verwenden Sie die Kommandozeile des 9800 WLC, um eine CSR: Lassen Sie es von einer Zertifizierungsstelle signieren, und laden Sie dann jedes Zertifikat in der Kette manuell auf den 9800 WLC.

Verwenden Sie die Lösung, die Ihren Anforderungen am besten entspricht.

Option 1 - Laden eines vorhandenen signierten PKCS12-Zertifikats

Signierungsanforderung definieren

Wenn Sie noch nicht über das Zertifikat verfügen, müssen Sie eine Signierungsanfrage generieren, die Sie an Ihre Zertifizierungsstelle weitergeben möchten.

Bearbeiten Sie die Datei **openssl.cnf** aus Ihrem aktuellen Verzeichnis (auf einem Laptop mit OpenSSL installiert), kopieren Sie diese Zeilen, und fügen Sie sie ein, um das Feld Subject Alternate Names (SAN) in neu erstellte CSRs aufzunehmen.

```
[ 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
```

Ersetzen Sie die DNS.X-Namen durch Ihr SAN. Ersetzen Sie die Hauptfelder durch die erforderlichen Zertifikatdetails. Stellen Sie sicher, dass Sie den Common Name in den SAN-Feldern (DNS.x) wiederholen. Um dem Zertifikat zu vertrauen, muss sich der in der URL enthaltene Name in den SAN-Feldern befinden.

Im Fall von Web-Admin müssen Sie SAN-Felder auch mit Variationen der URL (nur Hostname oder vollständiger vollqualifizierter Domänenname (FQDN)) füllen, damit das Zertifikat unabhängig von den Admin-Typen in der URL in der Adressleiste des Browsers übereinstimmt.

Generieren Sie den CSR von OpenSSL mit dem folgenden Befehl:

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

Der CSR generiert **myCSR.csr** und seinen Schlüssel als **private.key** im Verzeichnis, aus dem OpenSSL ausgeführt wird, es sei denn, der vollständige Pfad wird für den Befehl angegeben.

Stellen Sie sicher, dass die Datei **private.key** sicher ist, da sie zum Verschlüsseln von Kommunikation verwendet wird.

Sie können den Inhalt überprüfen mit:

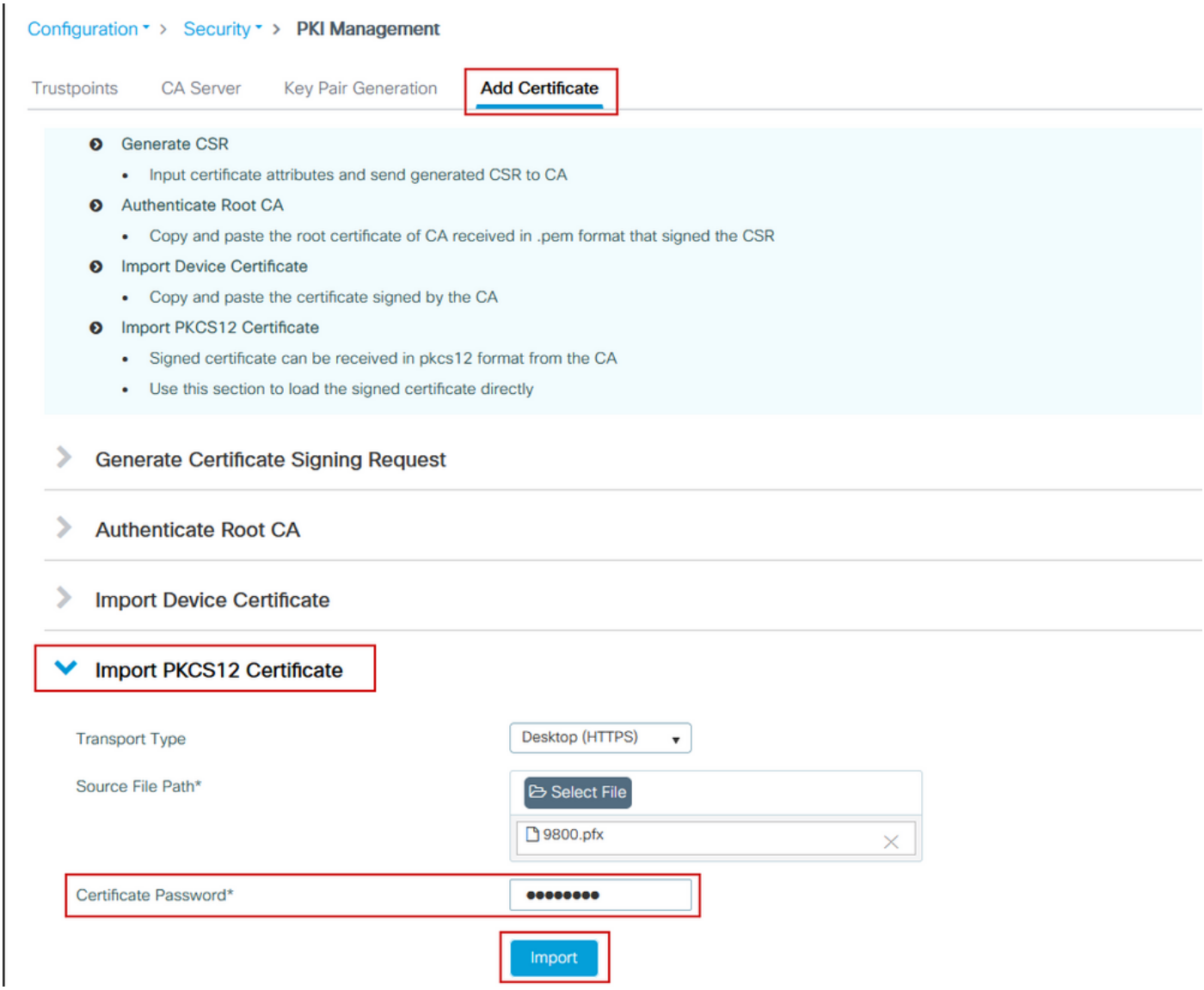
```
openssl req -noout -text -in myCSR.csr
```

Sie können diese CSR-Anfrage dann an Ihre Zertifizierungsstelle senden, damit diese signiert wird und ein Zertifikat zurückerhält. Stellen Sie sicher, dass die gesamte Kette von der Zertifizierungsstelle heruntergeladen wird und dass das Zertifikat im Base64-Format vorliegt, falls weitere Änderungen erforderlich sind.

Zertifikat importieren

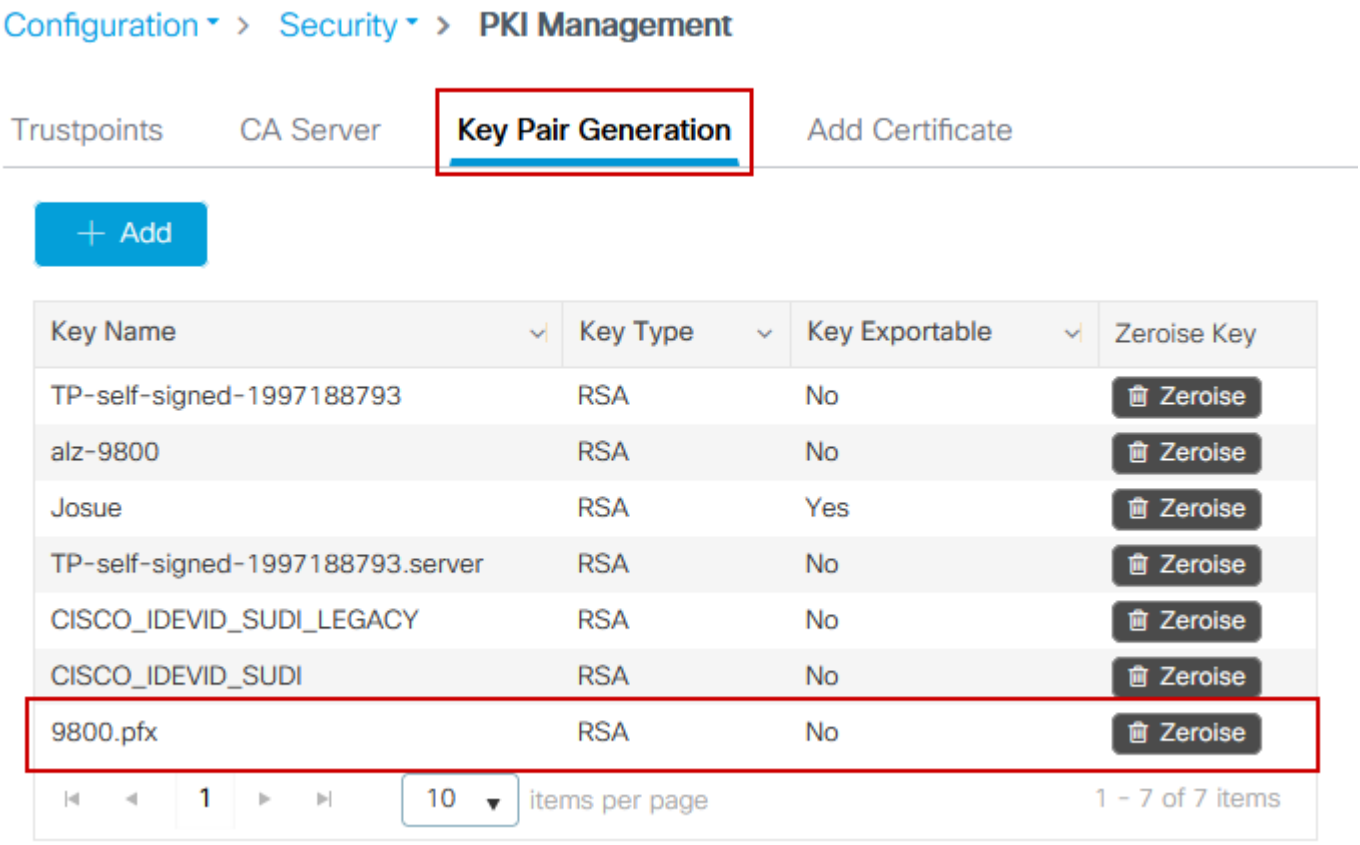
Schritt 1: Speichern Sie Ihr PKCS12-Zertifikat auf einem TFTP-Server (Trivial File Transfer Protocol), der über den 9800 WLC erreichbar ist. Das PKCS12-Zertifikat muss den privaten Schlüssel sowie die Zertifikatkette bis zur Stammzertifizierungsstelle enthalten.

Schritt 2: Öffnen Sie die Benutzeroberfläche des 9800 WLC, und navigieren Sie zu **Configuration > Security > PKI Management**, und klicken Sie auf die Registerkarte **Add Certificate.** Erweitern Sie das Menü **PKCS12-Zertifikat importieren**, und geben Sie die TFTP-Details ein. Alternativ können Sie über die Option **Desktop (HTTPS**) in der Dropdown-Liste **Transporttyp** HTTP-Upload über den Browser zulassen. **Das Zertifikatkennwort** bezieht sich auf das Kennwort, das beim Generieren des PKCS12-Zertifikats verwendet wurde.



Schritt 3: Überprüfen Sie die Informationen, und klicken Sie auf **Importieren.** Anschließend wird das neue Zertifikatschlüsselpaar für diesen neuen Vertrauenspunkt auf der Registerkarte **Schlüsselpaarerzeugung** installiert. Nach dem erfolgreichen Import erstellt der 9800 WLC außerdem einen zusätzlichen Vertrauenspunkt für mehrstufige Zertifizierungsstellen.

> **Hinweis**: Derzeit stellt der 9800 WLC nicht die vollständige Zertifikatkette dar, wenn ein bestimmter Vertrauenspunkt für Webauth oder Webadmin verwendet wird, sondern das Gerätezertifikat und seinen direkten Aussteller. Diese wird mit der Cisco Bug-ID CSCwa23606 verfolgt. , behoben in Cisco IOS® XE 17.8.



CLI:

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

Hinweis: Es ist wichtig, dass sowohl der Name der Zertifikatsdatei als auch der Name des Vertrauenspunkts für den 9800 WLC exakt übereinstimmen, damit zusätzliche Vertrauenspunkte für mehrstufige Zertifizierungsstellen erstellt werden können.

PKCS12-Formatumwandlung und Zertifikatkette in Szenarien mit mehrstufigen Zertifizierungsstellen.

Es ist möglich, in eine Situation zu gelangen, in der Sie eine private Schlüsseldatei und ein Zertifikat im PEM- oder CRT-Format haben und diese in einem PKCS12-Format (PFX) kombinieren möchten, um sie auf den 9800 WLC hochzuladen. Geben Sie dazu den folgenden Befehl ein:

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

Wenn Sie eine Zertifikatkette (eine oder mehrere Zwischen-CA und Root-CA) im PEM-Format haben, müssen Sie alle in einer einzigen PFX-Datei kombinieren.

Kombinieren Sie die Zertifizierungsstellenzertifikate manuell in einer Datei. Kopieren Sie den Inhalt, und fügen Sie ihn zusammen (speichern Sie die Datei im PEM-Format):

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

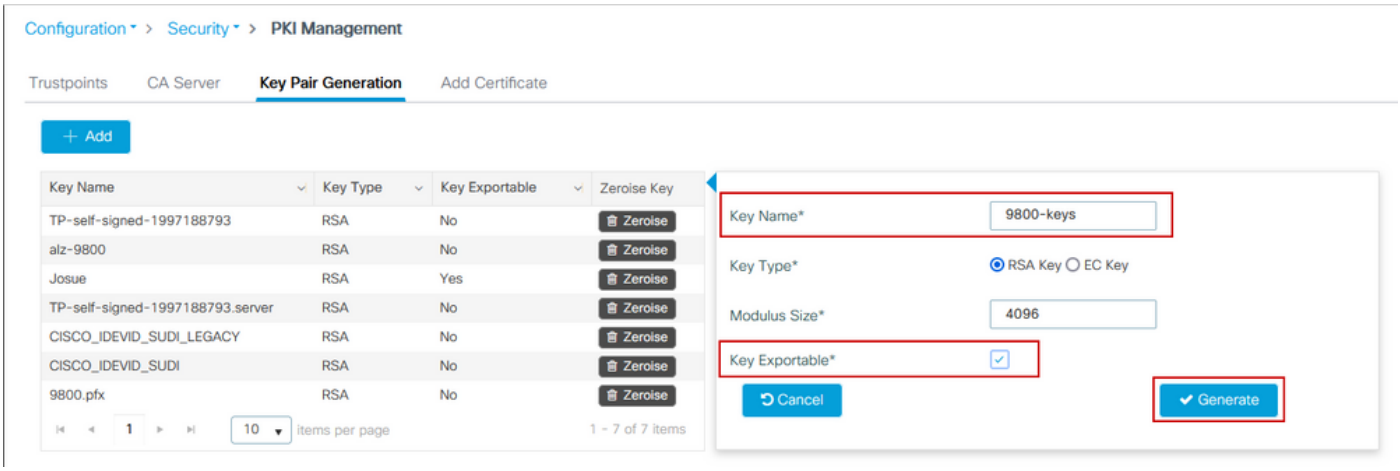
Später können Sie dann alle in einer PKCS12-Zertifikatsdatei kombinieren mit:

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

Lesen Sie den Verifizierungsabschnitt am Ende des Artikels, um zu sehen, wie das endgültige Zertifikat aussieht.

Option 2 - Definieren eines Key and Signing Request (CSR) auf dem 9800 WLC

Schritt 1: Generieren Sie ein RSA-Schlüsselpaar für allgemeine Zwecke. Navigieren Sie zu **Configuration > Security > PKI Management**, wählen Sie die Registerkarte **Key Pair Generation** aus, und klicken Sie dann auf **+ Add**. Geben Sie die Details ein, stellen Sie sicher, dass das Kontrollkästchen **Exportfähiger Schlüssel** aktiviert ist, und klicken Sie dann auf **Generieren**.



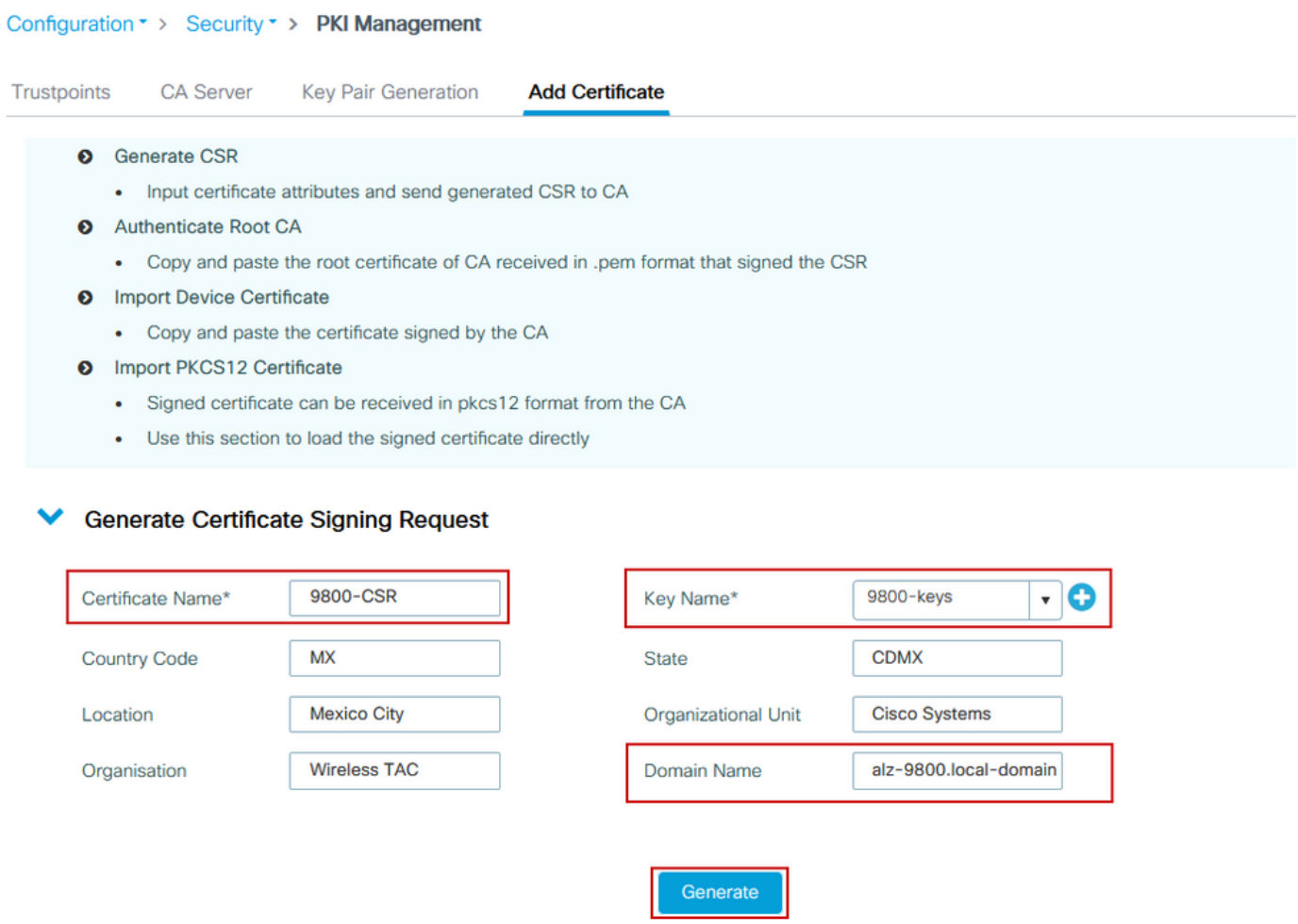
CLI-Konfiguration:

```
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)
```

Schritt 2: Erstellen Sie eine CSR-Anfrage für Ihren 9800 WLC. Navigieren Sie zur Registerkarte **Zertifikat hinzufügen,** und erweitern Sie die Option **Zertifikatsignierungsanfrage generieren,** geben Sie die Details ein, und wählen Sie das zuvor erstellte Schlüsselpaar aus der Dropdown-Liste aus. Es ist wichtig, dass der **Domänenname** mit der URL übereinstimmt, die für den Clientzugriff auf dem 9800 WLC definiert ist (Webadministratorseite, Webauthentifizierungsseite usw.). Der **Zertifikatsname** ist der Name des Vertrauenspunkts, sodass Sie ihn basierend auf seiner Verwendung benennen können.

> **Hinweis**: Die 9800 WLCs unterstützen Zertifikate mit Platzhalterparametern innerhalb ihres Common Name.



Stellen Sie sicher, dass die Informationen korrekt sind, und klicken Sie dann auf **Generate (Generieren)**. Der CSR wird in einem Textfeld neben dem ursprünglichen Formular angezeigt.

Kopieren speichert eine Kopie in der Zwischenablage, sodass Sie sie in einen Texteditor einfügen und den CSR speichern können. Wenn **Save to device** (Auf Gerät speichern) ausgewählt ist,

erstellt der 9800 WLC eine Kopie des CSR und speichert sie im **Bootflash:**/csr. Führen Sie beispielsweise die folgenden Befehle aus:

```
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-Konfiguration:

```
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
```

Verfügbare Parameter für die Konfiguration des Betreffnamens:

C: Land, es müssen nur zwei Großbuchstaben sein.

ST: "Some State" (Bestimmter Staat) bezieht sich auf den Namen des Staates oder der Provinz.

L: Standortname, bezieht sich auf die Stadt.

O: Name der Organisation, bezieht sich auf das Unternehmen.

OU: Name der Organisationseinheit, siehe Abschnitt.

CN: (Common Name)Bezieht sich auf das Subjekt, für das das Zertifikat ausgestellt wird. Sie müssen entweder die spezifische IP-Adresse angeben, auf die zugegriffen werden soll (Wireless-

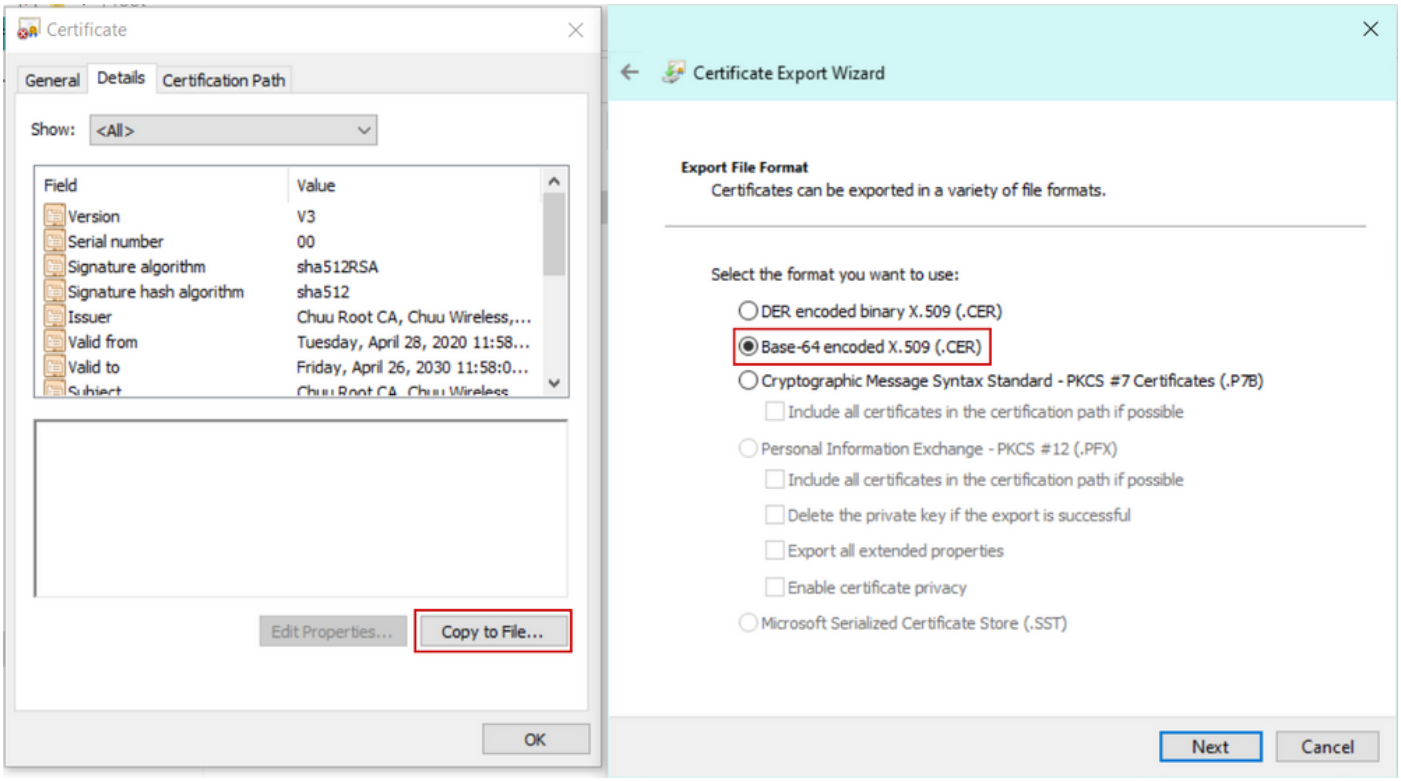
Management-IP, virtuelle IP usw.), oder den konfigurierten Hostnamen mit FQDN.

> **Hinweis**: Wenn Sie einen alternativen Antragstellernamen hinzufügen möchten, ist dies in Cisco IOS XE-Versionen vor 17.8.1 aufgrund des Cisco Bug-ID CSCvt15177 nicht möglich. . Dieses Szenario kann dazu führen, dass einige Browser-Warnungen aufgrund des Fehlens von SAN ausgegeben werden. Um dies zu vermeiden, erstellen Sie dann den Schlüssel und den CSR-Off-Box, wie in Option 1 gezeigt.

Schritt 3: Lassen Sie Ihren CSR von Ihrer Zertifizierungsstelle (Certification Authority, CA) unterzeichnen. Die vollständige Zeichenfolge muss an die Zertifizierungsstelle gesendet werden, damit sie signiert wird.

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

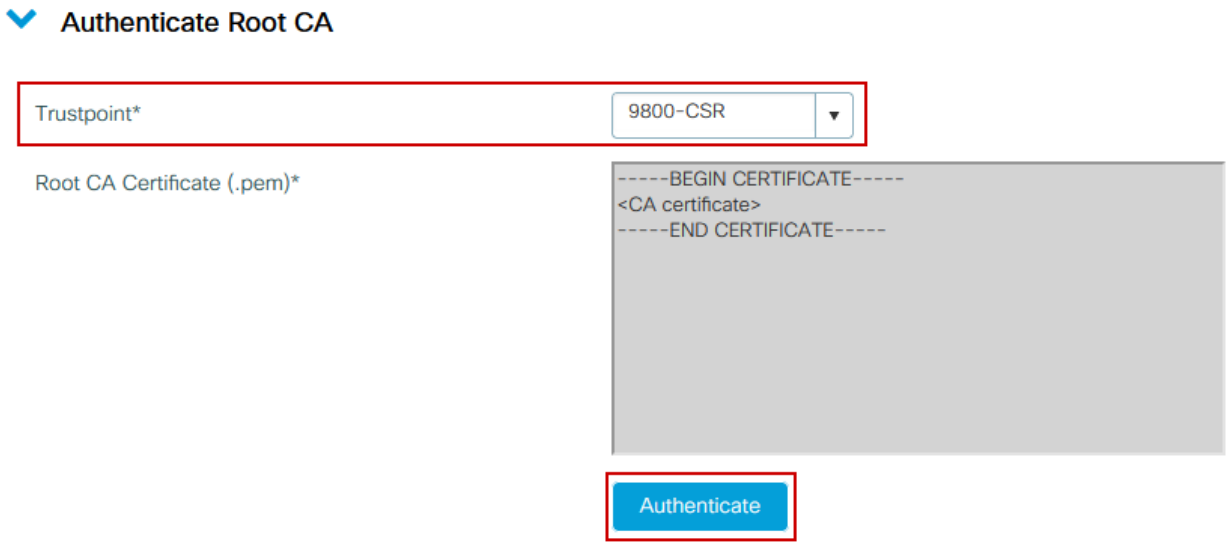
Wenn Sie das Zertifikat mit einer Windows Server-Zertifizierungsstelle signieren, laden Sie das signierte Zertifikat im Base64-Format herunter. Andernfalls müssen Sie mit Dienstprogrammen wie dem Windows-Zertifikatsmanager exportieren.



> **Hinweis**: Der Authentifizierungsprozess für Vertrauenspunkte hängt von der Anzahl der Zertifizierungsstellen ab, die den CSR signiert haben. Wenn eine einstufige Zertifizierungsstelle vorhanden ist, überprüfen Sie **Schritt 4a.** Wenn eine mehrstufige Zertifizierungsstelle vorhanden ist, fahren Sie mit **Schritt 4b fort**. Dies ist erforderlich, da ein Vertrauenspunkt jeweils nur zwei Zertifikate speichern kann (das entsprechende Zertifikat und das Ausstellerzertifikat).

Schritt 4a: 9800 der ausstellenden Zertifizierungsstelle vertrauen. Laden Sie das Zertifikat der Herausgeberzertifizierungsstelle im PEM-Format herunter (Base64). Erweitern Sie den Abschnitt **Authentication Root CA** im selben Menü, wählen Sie den zuvor definierten Vertrauenspunkt aus

der Dropdown-Liste Vertrauenspunkt aus, und fügen Sie das Zertifikat der Ausstellerzertifizierungsstelle ein. Stellen Sie sicher, dass die Details ordnungsgemäß konfiguriert sind, und klicken Sie auf **Authenticate (Authentifizieren)**.



CLI-Konfiguration:

```
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
```

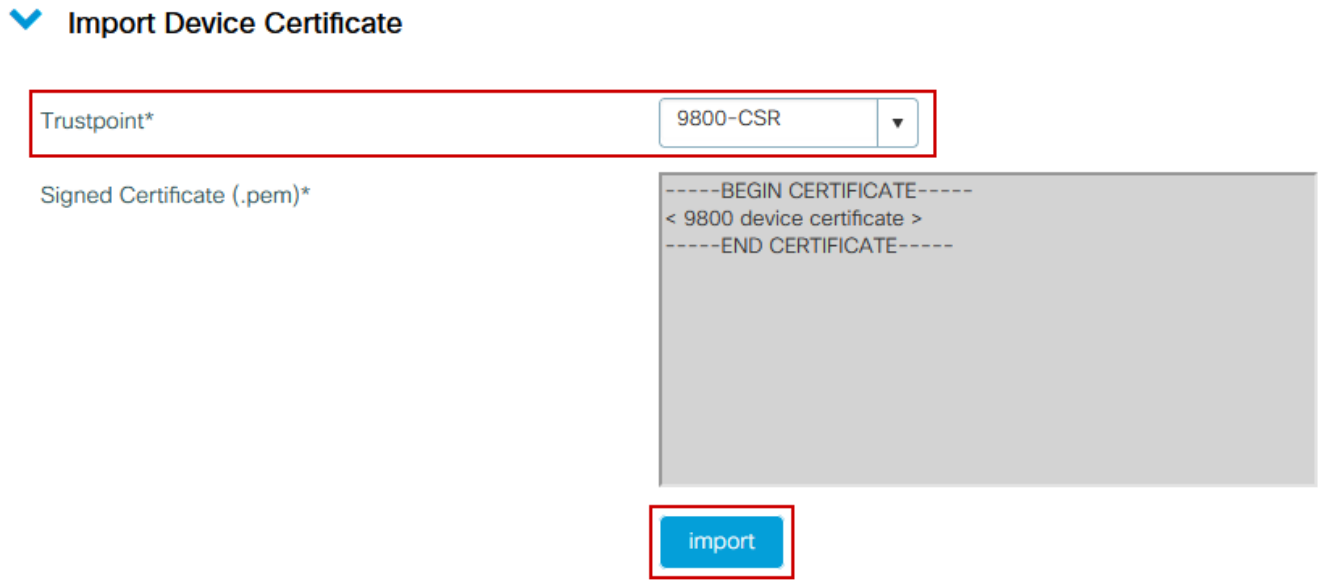
Schritt 4b: Wenn mehrere Autorisierungsebenen vorhanden sind, ist für jede Zertifizierungsstellenebene ein neuer Vertrauenspunkt erforderlich. Diese Vertrauenspunkte enthalten nur das Authentifizierungszertifikat und verweisen auf die nächste Authentifizierungsebene. Dieser Prozess wird nur in der CLI durchgeführt. In diesem Beispiel gibt es eine zwischengeschaltete Zertifizierungsstelle und eine Stamm-Zertifizierungsstelle:

```
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
```

> **Hinweis**: Wenn mehr als eine Zertifizierungsstelle der Zwischenzeit in der Zertifizierungskette vorhanden ist, muss pro zusätzlicher Zertifizierungsstufe ein neuer Truspoint generiert werden. Diese Prüfpunkte müssen auf den Prüfpunkt verweisen, der die nächste Zertifizierungsstufe mit dem Befehl **chain-validation continue <Prüfpunktname> enthält**.

Schritt 5: Laden Sie das signierte Zertifikat in den 9800 WLC. Erweitern Sie im gleichen Menü den Abschnitt **Gerätezertifikat importieren**. Wählen Sie den zuvor definierten **Vertrauenspunkt aus**, und fügen Sie das von der Zertifizierungsstelle bereitgestellte signierte Gerätezertifikat ein. Klicken Sie anschließend auf **Importieren**, sobald die Zertifikatinformationen überprüft wurden.



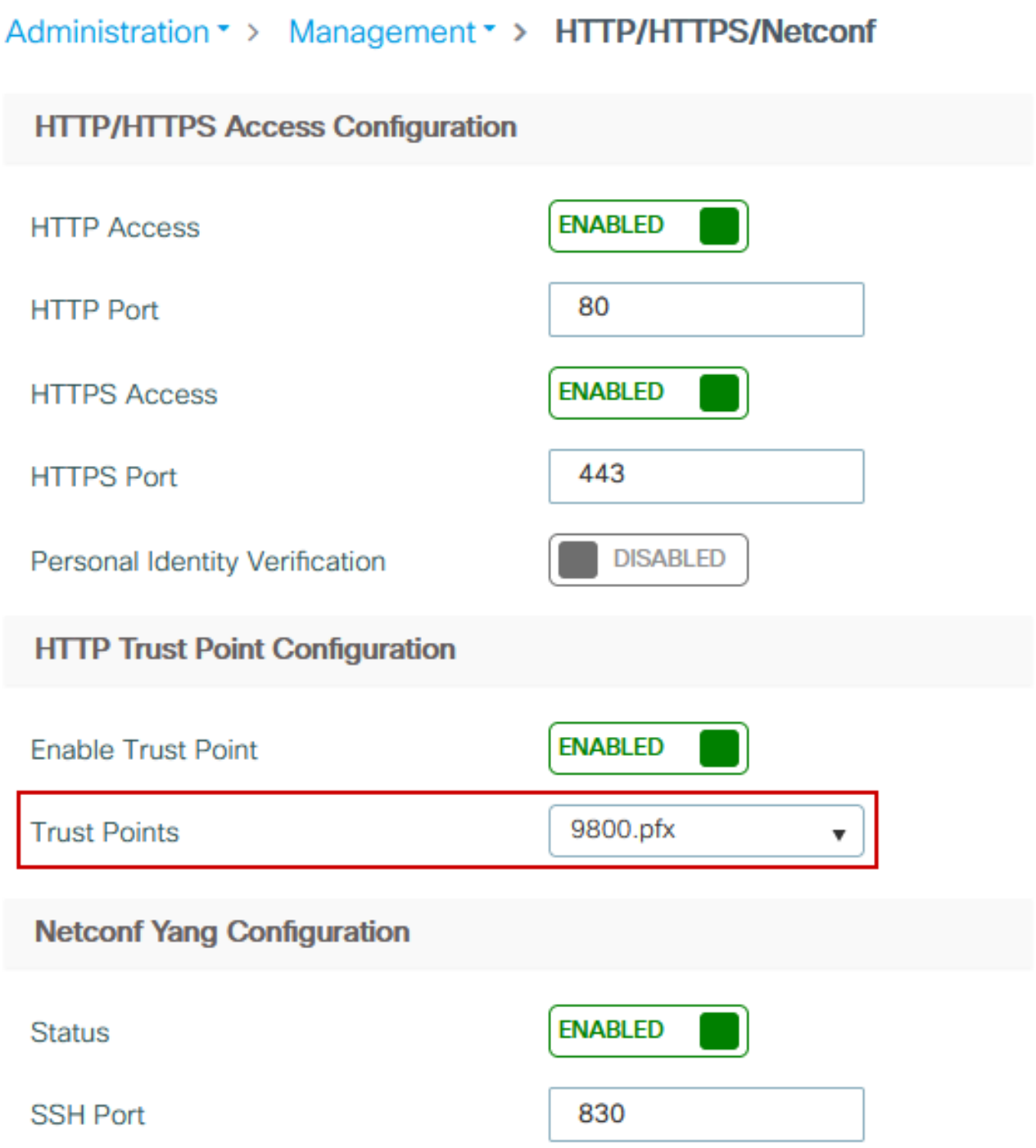
CLI-Konfiguration:

```
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
```

Neues Zertifikat verwenden

Webverwaltung

Navigieren Sie zu **Administration > Management > HTTP/HTTPS/Netconf,** und wählen Sie das importierte Zertifikat aus der Dropdown-Liste **Trust Points (Vertrauenspunkte**) aus.

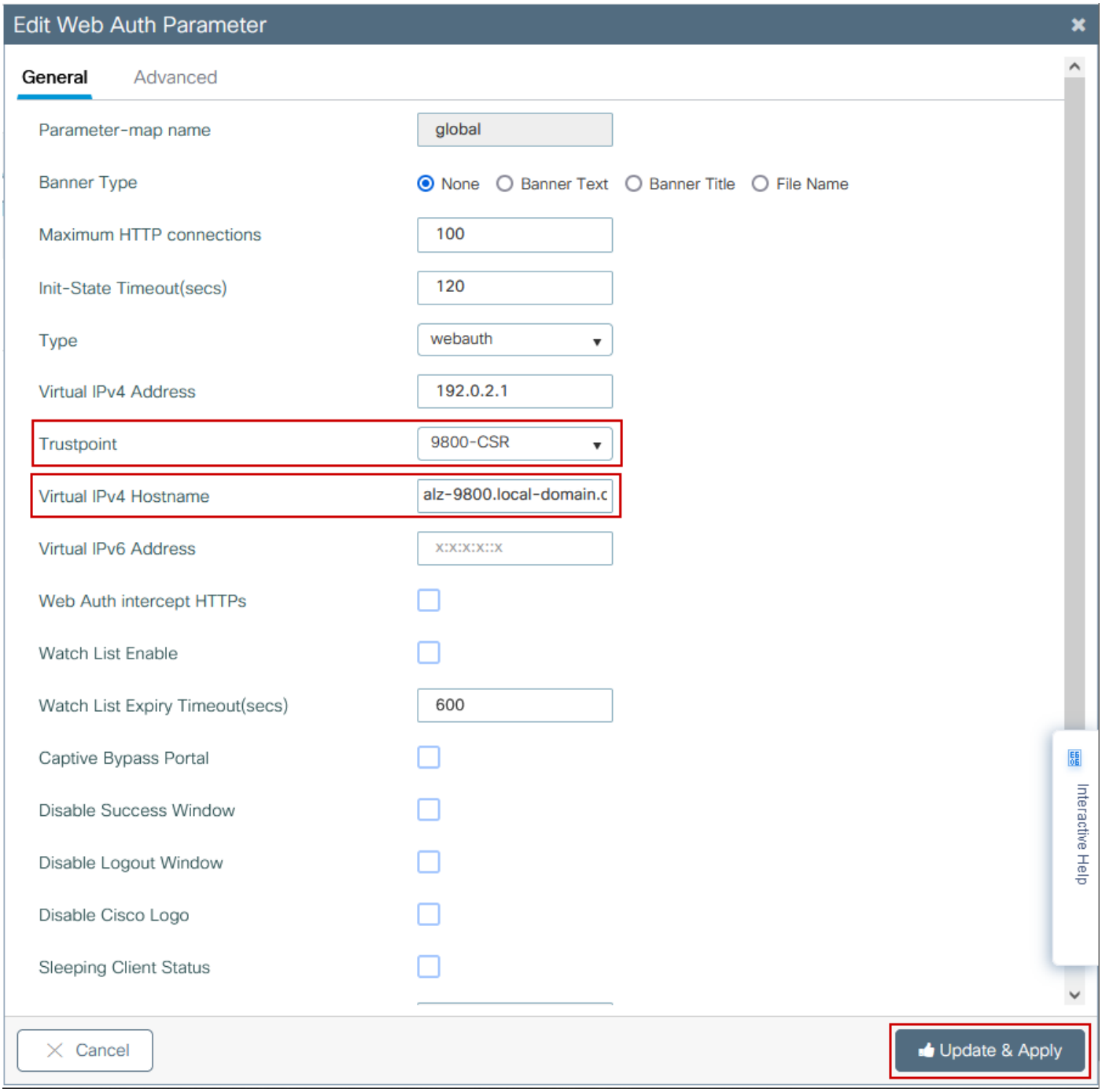


CLI-Konfiguration:

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

Lokale Webauthentifizierung

Navigieren Sie zu **Configuration > Security > Web Auth**, wählen Sie die **globale** Parameterzuordnung aus, und wählen Sie den importierten Vertrauenspunkt aus der **Vertrauenspunkt**-Dropdown-Liste aus. Klicken Sie auf **Aktualisieren und anwenden**, um die Änderungen zu speichern. Stellen Sie sicher, dass der **virtuelle IPv4-Hostname** mit dem Common Name im Zertifikat übereinstimmt.



CLI-Konfiguration:

```
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
```

Starten Sie die HTTP-Dienste neu, um die Zertifikatverwendung zu aktualisieren:

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

.

Überlegungen zur Hochverfügbarkeit

Auf einem 9800-Paar, das für Stateful Switchover High Availability (HA SSO) konfiguriert ist, werden alle Zertifikate bei der ersten Bulk-Synchronisierung vom primären zum sekundären Switch repliziert. Dies umfasst Zertifikate, bei denen der private Schlüssel auf dem Controller selbst generiert wurde, auch wenn der RSA-Schlüssel so konfiguriert ist, dass er nicht exportierbar ist. Nachdem das HA-Paar eingerichtet wurde, werden alle neu installierten Zertifikate auf beiden Controllern installiert, und alle Zertifikate werden in Echtzeit repliziert.

Nach einem Ausfall verwendet der ehemalige sekundäre Controller die vom primären Controller geerbten Zertifikate transparent.

Sicherstellen, dass das Zertifikat von Webbrowsern als vertrauenswürdig eingestuft wird

Es gibt einige wichtige Überlegungen, um sicherzustellen, dass ein Zertifikat von Webbrowsern als vertrauenswürdig eingestuft wird:

- Der Common Name (oder ein SAN-Feld) muss mit der vom Browser besuchten URL übereinstimmen.
- Sie muss innerhalb ihrer Gültigkeitsdauer liegen.
- Sie muss von einer Zertifizierungsstelle oder einer Kette von Zertifizierungsstellen ausgestellt werden, deren Root vom Browser als vertrauenswürdig eingestuft wird. Dazu muss das vom Webserver bereitgestellte Zertifikat alle Zertifikate der Kette enthalten, bis (nicht notwendigerweise) ein vom Client-Browser vertrauenswürdiges Zertifikat (in der Regel die Root-CA) vorhanden ist.
- Wenn er Sperrlisten enthält, muss der Browser diese herunterladen können, und die Zertifikats-CN darf nicht aufgeführt werden.

Überprüfung

Sie können die folgenden Befehle verwenden, um die Zertifikatkonfiguration zu überprüfen:

```
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
```

Sie können Ihre Zertifikatskette auf dem 9800 überprüfen. Im Fall eines Gerätezertifikats, das von einer zwischengeschalteten Zertifizierungsstelle ausgestellt wird, die ihrerseits von einer Stammzertifizierungsstelle ausgestellt wird, verfügen Sie über einen Vertrauenspunkt nach Gruppen von zwei Zertifikaten, sodass jede Stufe über einen eigenen Vertrauenspunkt verfügt. In diesem Fall hat der 9800 WLC **9800.pfx** mit dem Device Certificate (WLC Certificate) und seiner ausstellenden CA (Intermediate CA). Dann ein weiterer Vertrauenspunkt mit der Stammzertifizierungsstelle, die die zwischengeschaltete Zertifizierungsstelle ausgestellt hat.

```
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
```

Zertifikatsverifizierung mit OpenSSL

OpenSSL kann nützlich sein, um das Zertifikat selbst zu überprüfen oder einige Konvertierungsoperationen durchzuführen.

Um ein Zertifikat mit OpenSSL anzuzeigen:

openssl x509 -in

So zeigen Sie den Inhalt eines CSR an:

openssl req -noout -text -in

Wenn Sie das Endzertifikat auf dem 9800 WLC überprüfen möchten, aber etwas Anderes als Ihren Browser verwenden möchten, kann OpenSSL dies tun und Ihnen eine Menge Details geben.

openssl s_client -showcerts -verify 5 -connect

Sie können **<**wlcURL**>** durch die URL des Webadministrators des 9800 oder die URL des Gastportals (virtuelle IP) ersetzen. Sie können dort auch eine IP-Adresse angeben. Es teilt Ihnen mit, welche Zertifikatskette empfangen wird, aber die Zertifikatvalidierung kann niemals zu 100 % korrekt sein, wenn eine IP-Adresse anstelle eines Hostnamens verwendet wird.

So zeigen Sie den Inhalt an und überprüfen ein PKCS12-Zertifikat (PFX-Zertifikat) oder eine Zertifikatskette:

openssl pkcs12 -info -in

Der folgende Befehl in einer Zertifikatskette zeigt ein Beispiel, in dem das Gerätezertifikat vom Technical Assistance Center (TAC) von einer zwischengeschalteten Zertifizierungsstelle mit der Bezeichnung "intermediär.com" ausgestellt wird, die ihrerseits von der Stamm-Zertifizierungsstelle mit der Bezeichnung "root.com" stammt:

```
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-----
```

Fehlerbehebung

Verwenden Sie diesen Befehl zur Fehlerbehebung. Wenn dies auf einer Remote-Sitzung (SSH oder Telnet) erfolgt, wird ein **Terminalmonitor** benötigt, um die folgenden Ausgaben anzuzeigen:

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

Erfolgreiche Szenario-Debug-Ausgabe

Diese Ausgabe zeigt die erwartete Ausgabe an, wenn ein erfolgreicher Zertifikatimport auf einem 9800 erfolgt. Verwenden Sie diese als Referenz, und identifizieren Sie den Fehlerstatus:

```
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.
```

Versuchen Sie, ein PKCS12-Zertifikat zu importieren, das keine Zertifizierungsstelle besitzt.

Wenn Sie ein Zertifikat importieren und die Fehlermeldung "CA cert is not found." (Zertifizierungsstellenzertifikat wurde nicht gefunden) erhalten, bedeutet dies, dass Ihre PFX-Datei nicht die gesamte Kette enthält oder keine Zertifizierungsstelle vorhanden ist.

```
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.
```

Wenn Sie den Befehl openssl pkcs12 -info -in <path to cert> ausführen und nur ein Zertifikat mit einem privaten Schlüssel angezeigt wird, bedeutet dies, dass die Zertifizierungsstelle nicht vorhanden ist. Als Faustregel gilt, dass dieser Befehl idealerweise Ihre gesamte Zertifikatskette auflistet. Es ist nicht erforderlich, die oberste Stammzertifizierungsstelle einzuschließen, wenn diese bereits von den Clientbrowsern bekannt ist.

Eine Möglichkeit, dies zu beheben, besteht darin, das PKCS12 in PEM zu dekonstruieren und die Kette ordnungsgemäß neu aufzubauen. Im nächsten Beispiel hatten wir eine PFX-Datei, die nur das Device-Zertifikat (WLC) und den zugehörigen Schlüssel enthielt. Sie wurde von einer zwischengeschalteten Zertifizierungsstelle ausgegeben (die in der PKCS12-Datei nicht vorhanden

war), die ihrerseits von einer bekannten Stammzertifizierungsstelle signiert wurde.

Schritt 1: Exportieren Sie den privaten Schlüssel.

```
openssl pkcs12 -in
```

Schritt 2: Exportieren Sie das Zertifikat als PEM.

```
openssl pkcs12 -in
```

Schritt 3: Zwischenzertifikat als PEM herunterladen.

Die Quelle der CA hängt von ihrer Art ab. Wenn es sich um eine öffentliche CA handelt, reicht eine Online-Suche aus, um das Repository zu finden. Andernfalls muss der CA-Administrator die Zertifikate im Base64-Format (.pem) bereitstellen. Wenn es mehrere Ebenen von CA gibt, gruppieren Sie diese in einer einzigen Datei, wie sie am Ende des Importprozesses für **Option 1** dargestellt wird.

Schritt 4: Erstellen Sie das PKCS 12 mithilfe des Schlüssels, des Gerätezertifikats und des Zertifizierungsstellenzertifikats neu.

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

Jetzt haben wir "fixedcertchain.pfx", das wir mit Vergnügen auf den Catalyst 9800 importieren können!

Hinweise und Einschränkungen

- Cisco IOS® XE unterstützt keine CA-Zertifikate mit einer Gültigkeit über 2099 hinaus: Cisco Bug-ID CSCvp64208
- Cisco IOS® XE unterstützt kein SHA256 Message Digest PKCS 12-Paket (SHA256-Zertifikate werden unterstützt, jedoch nicht, wenn das PKCS12-Paket selbst mit SHA256 signiert ist): Cisco Bug-ID CSCvz41428
- Die Fragmentierung wird angezeigt, wenn der WLC Benutzerzertifikate übertragen muss und die NAC/ISE-Appliance über das Internet erreichbar ist (z. B. in einer SD-WAN-Bereitstellung). Zertifikate sind fast immer größer als 1500 Byte (d. h. mehrere RADIUS-Pakete werden gesendet, um die Zertifikatsnachricht zu übertragen). Wenn Sie über mehrere unterschiedliche MTUs im Netzwerkpfad verfügen, kann es zu einer Fragmentierung der RADIUS-Pakete selbst kommen. In solchen Fällen empfehlen wir, dass Sie alle UDP-Datagramme für den WLC-Datenverkehr über den gleichen Pfad senden, um Probleme wie Verzögerungen/Jitter zu vermeiden, die durch das Internetwetter verursacht werden können.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.