Generar y descargar certificados CSR en WLC Catalyst 9800

Contenido

Introducción

Este documento describe el proceso general para generar, descargar e instalar certificados en el Catalyst 9800

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo configurar el 9800 WLC, el punto de acceso (AP) para el funcionamiento básico
- Cómo utilizar la aplicación OpenSSL
- Infraestructura de clave pública (PKI) y certificados digitales

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 9800-L, Cisco IOS® XE versión 17.3.3
- aplicación OpenSSL

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

En 16.10.X, los 9800 no admiten un certificado diferente para la autenticación y administración web. El portal de inicio de sesión web siempre utiliza el certificado predeterminado.

En 16.11.X, puede configurar un certificado dedicado para la autenticación web y definir el punto de confianza dentro del mapa de parámetros global.

Hay dos opciones para obtener un certificado para un WLC 9800.

1. Generar solicitud de firma de certificado (CSR) con OpenSSL o cualquier otra aplicación SSL. Obtenga un certificado PKCS12 firmado por su autoridad de certificación (CA) y cárguelo directamente en el WLC 9800. Esto significa que la clave privada se incluye con ese certificado.
2. Utilice la CLI de 9800 WLC para generar una CSR, consígala firmada por una CA y luego carga cada certificado en la cadena manualmente al WLC 9800.

Utilice el que mejor se adapte a sus necesidades.

Opción 1: cargar un certificado firmado PKCS12 preexistente

Definir una solicitud de firma

Si aún no tiene el certificado, debe generar una solicitud de firma para entregarlo a la CA.

Edite el archivo **openssl.cnf** desde el directorio actual (en un equipo portátil que tenga instalado OpenSSL), copie y pegue estas líneas para incluir el campo Nombres alternativos de asunto (SAN) en los CSR recién creados.

```
[ 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
```

Reemplace los nombres DNS.X por su SAN. Reemplace los campos principales por los detalles del certificado que necesite. Asegúrese de repetir el nombre común dentro de los campos de SAN (DNS.x). Google Chrome requiere que el nombre presente en la URL esté en los campos SAN para confiar en el certificado.

En el caso del administrador web, también debe rellenar los campos SAN con variaciones de la URL (solo el nombre de host o el nombre de dominio completo (FQDN), por ejemplo) para que el certificado coincida con cualquier tipo de administrador en la URL de la barra de direcciones del navegador.

Genere el CSR desde OpenSSL con este comando:

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

El CSR genera como **myCSR.csr** y su clave como **private.key** en el directorio desde donde se ejecuta OpenSSL, a menos que se proporcione la ruta completa al comando.

Asegúrese de mantener el archivo **private.key** seguro mientras se utiliza para cifrar las comunicaciones.

Puede verificar su contenido con:

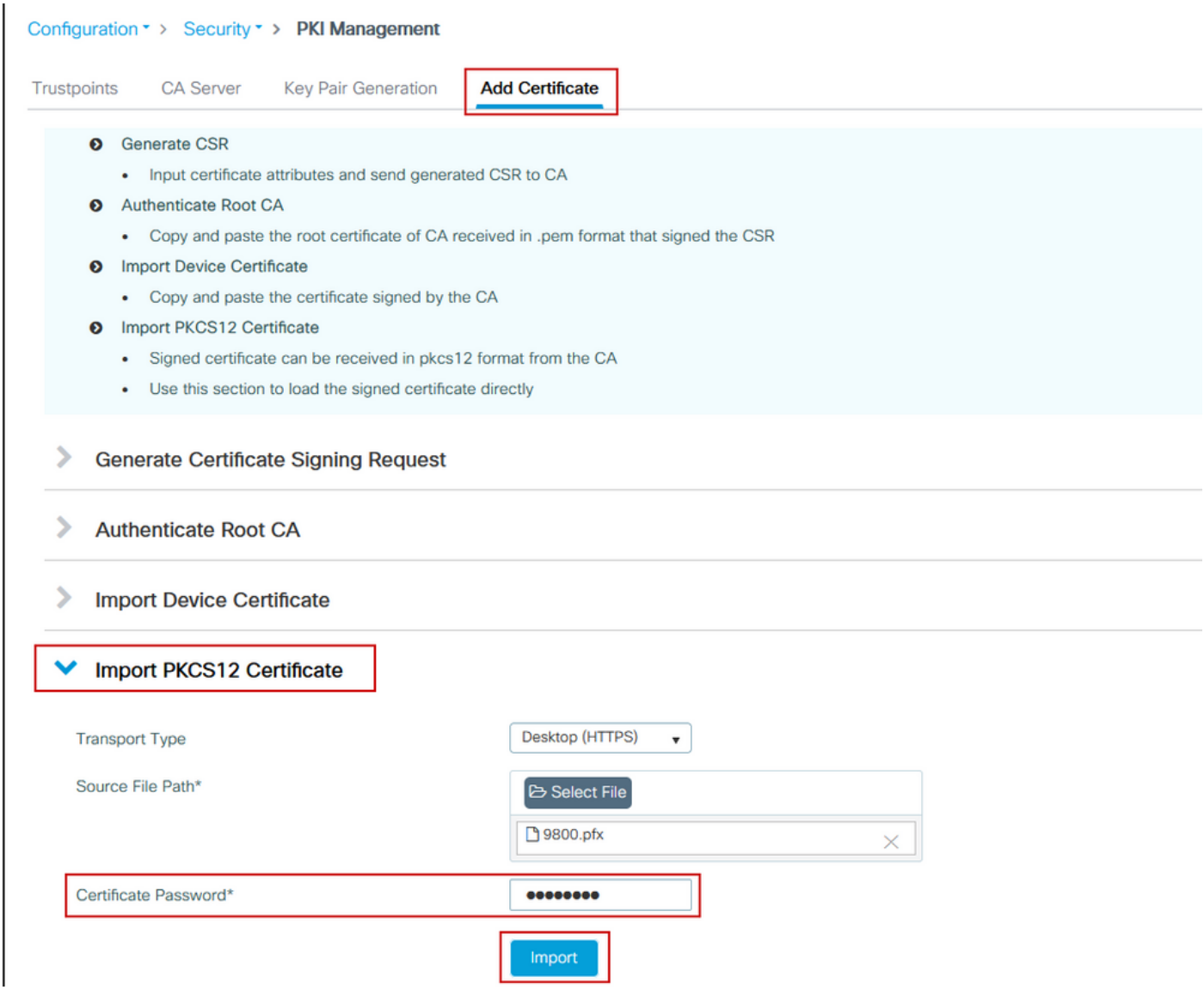
```
openssl req -noout -text -in myCSR.csr
```

A continuación, puede proporcionar esta CSR a la CA para que la firme y reciba un certificado de vuelta. Asegúrese de que la cadena completa se descarga de la CA y que el certificado está en formato Base64 en caso de que necesite manipulación adicional.

Importar el certificado

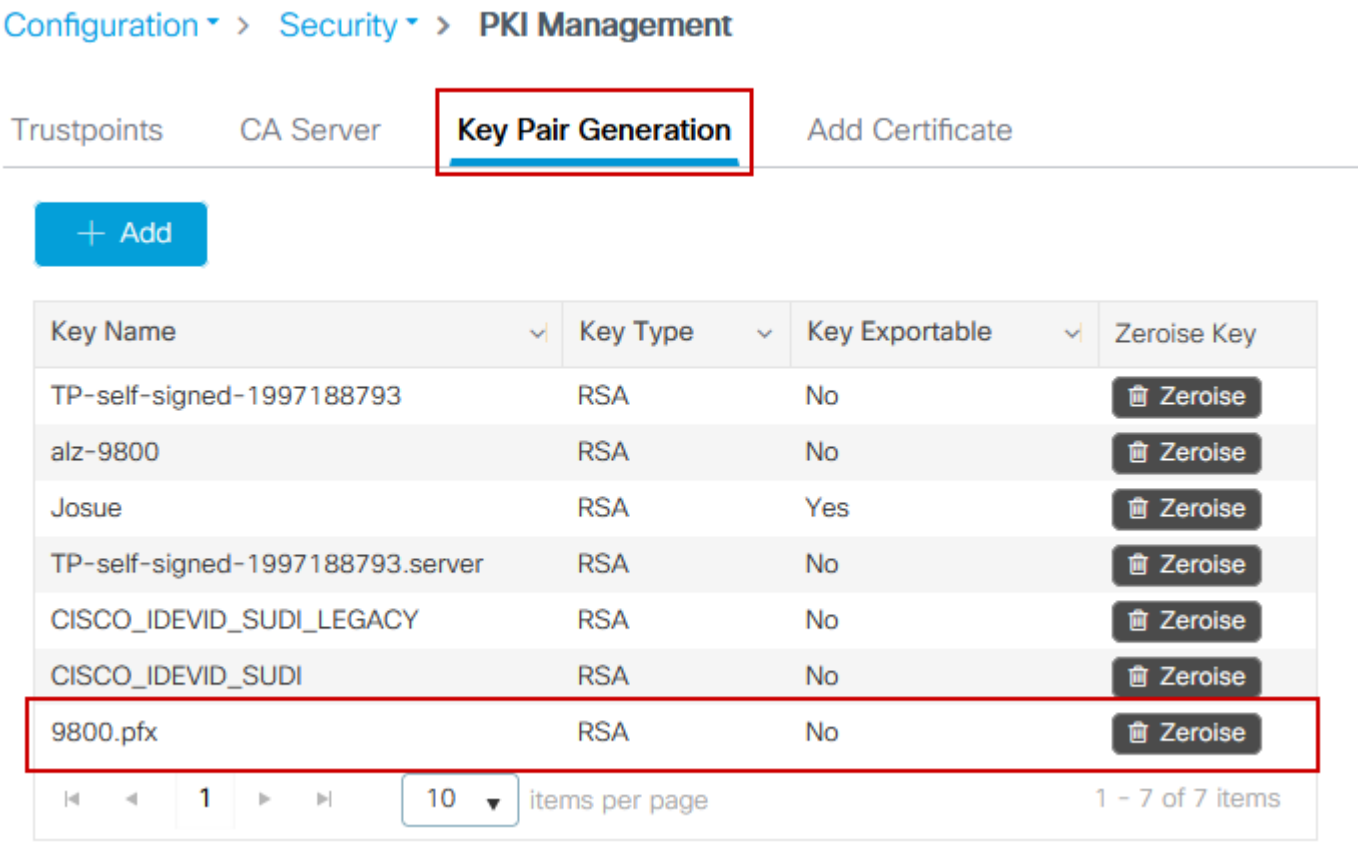
Paso 1. Guarde el certificado PKCS12 en un servidor TFTP (protocolo trivial de transferencia de archivos) al que se puede acceder desde el WLC 9800. El certificado PKCS12 debe contener la clave privada y la cadena de certificados hasta la CA raíz.

Paso 2. Abra su GUI de 9800 WLC y navegue hasta **Configuration > Security > PKI Management**, haga clic en la pestaña **Add Certificate**. **Expanda el menú Import PKCS12 Certificate** y complete los detalles de TFTP. Como alternativa, la opción **Desktop (HTTPS)** de la lista desplegable **Transport Type** permite la carga de HTTP a través del navegador. **La contraseña del certificado** hace referencia a la contraseña que se utilizó cuando se generó el certificado PKCS12.



Paso 3. Verifique que la información sea correcta y haga clic en **Importar. Después de esto, verá el nuevo par de claves de certificado para este nuevo punto de confianza instalado en la ficha Generación de pares de claves**. Después de una importación exitosa, el WLC 9800 también crea un punto de confianza adicional para las CA multinivel.

> **Nota**: Actualmente, el WLC 9800 no presenta la cadena completa del certificado cada vez que se utiliza un punto de confianza específico para webauth o webadmin, en lugar de presentar el certificado del dispositivo y su emisor inmediato. Se realiza un seguimiento de esto con el ID de bug de Cisco CSCwa23606 , corregido en Cisco IOS® XE 17.8.



CLI:

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

Nota: Es importante que tanto el nombre de archivo del certificado como el nombre del punto de confianza coincidan exactamente con el WLC 9800 para crear cualquier punto de confianza adicional para CA de varios niveles.

Conversión de Formato PKCS12 y Cadena de Certificados en Escenarios de CA Multinivel.

Es posible terminar en una situación donde usted tiene un archivo de clave privada y un certificado en formato PEM o CRT y desea combinarlos en un formato PKCS12 (.pfx) para cargar al WLC 9800. Para hacerlo, ingrese este comando:

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

En el caso de que tenga una cadena de certificados (una o varias CA intermedias y CA raíz) en formato PEM, deberá combinar todas en un único archivo .pfx.

En primer lugar, combine manualmente los certificados de CA en un único archivo como tal. Copie y pegue el contenido (guarde el archivo en formato .pem):

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

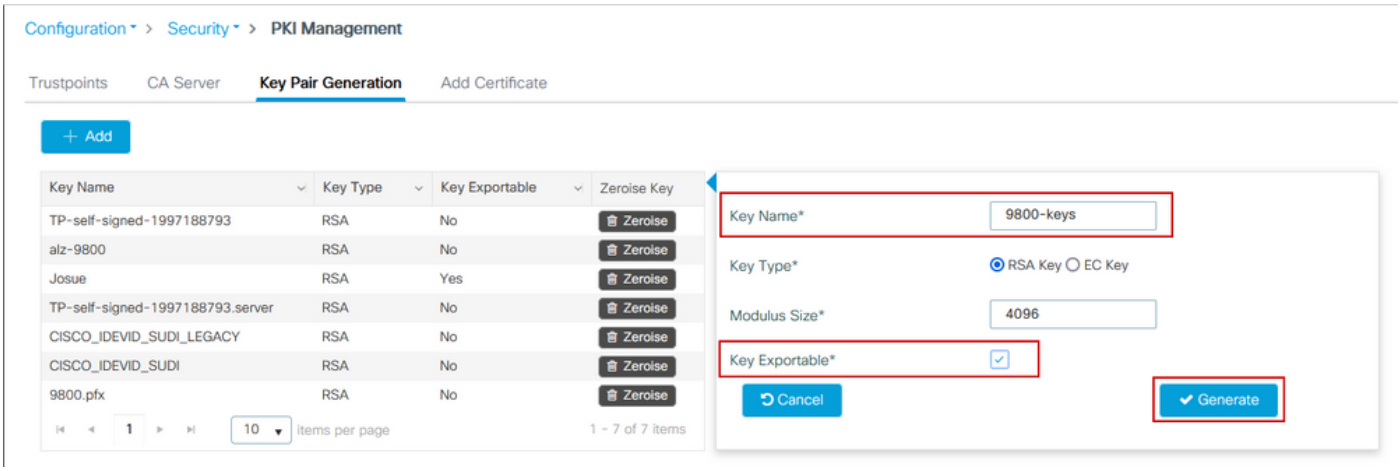
Posteriormente, puede combinar todo en un archivo de certificado PKCS12 con :

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

Consulte la sección Verificación al final del artículo para ver el aspecto del certificado final.

Opción 2 - Defina una llave y una petición de la firma (CSR) en el WLC 9800

Paso 1. Genere un par de claves RSA de uso general. Navegue hasta **Configuration > Security > PKI Management**, elija la pestaña **Key Pair Generation** y luego haga clic en **+ Add**. Introduzca los detalles, asegúrese de que la casilla de verificación **Clave exportable** está activada y, a continuación, haga clic en **Generar**.



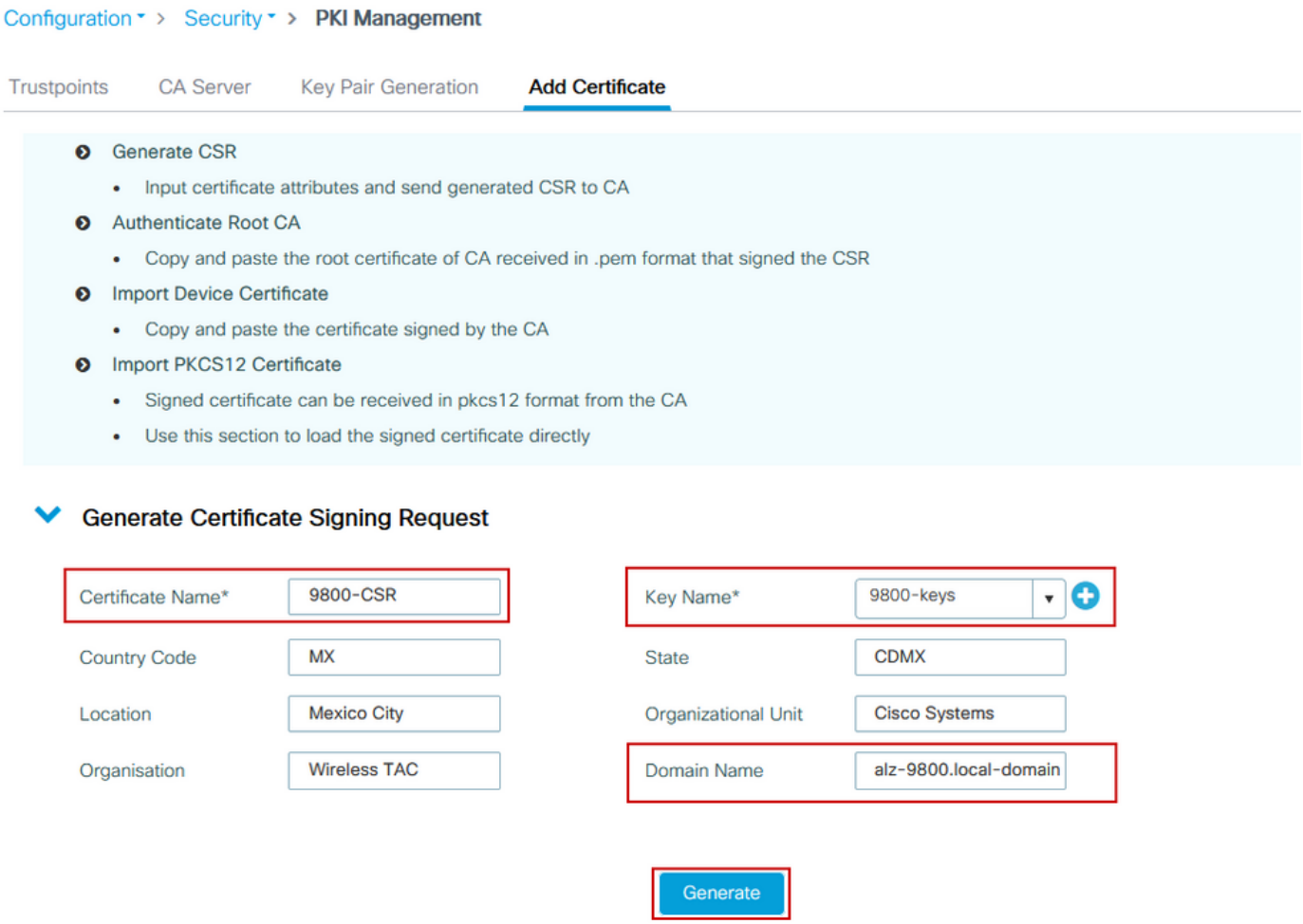
Configuración de CLI:

```
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)
```

Paso 2. Genere un CSR para su 9800 WLC. Vaya a la pestaña **Add Certificate** y expanda **Generate Certificate Signing Request**, rellene los detalles y elija el par de claves creado anteriormente de la lista desplegable. Es importante que **Domain Name** coincida con la URL que

se define para el acceso del cliente en el WLC 9800 (página de administración web, página de autenticación web, etc.), **Certificate Name** es el nombre de trustpoint para que pueda asignar un nombre basado en su uso.

> **Nota**: Los 9800 WLC soportan certificados con parámetros comodín dentro de su nombre común.



Asegúrese de que la información es correcta y, a continuación, haga clic en **Generar**. Esto muestra la CSR en un cuadro de texto junto al formulario original.

Copiar guarda una copia en el portapapeles para que pueda pegarla en un editor de texto y guardar el CSR. Si se selecciona **Save to device**, el WLC 9800 crea una copia del CSR y la almacena en **bootflash:**/csr. Por ejemplo, ejecute estos comandos:

```
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-----
```

Configuración de CLI:

```
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
```

Parámetros disponibles para la configuración del nombre del sujeto:

C: País, sólo debe tener dos letras mayúsculas.

ST: Algún estado, se refiere al nombre del estado o provincia.

L: Nombre de la ubicación, se refiere a la ciudad.

O: Nombre de la organización, se refiere a la empresa.

OU: Nombre de la unidad organizativa, puede consultar la sección.

CN: (nombre común)Se refiere al asunto para el que se emite el certificado. Debe especificar la dirección IP específica a la que se va a acceder (IP de administración inalámbrica, IP virtual, etc.) o el nombre de host configurado con FQDN.

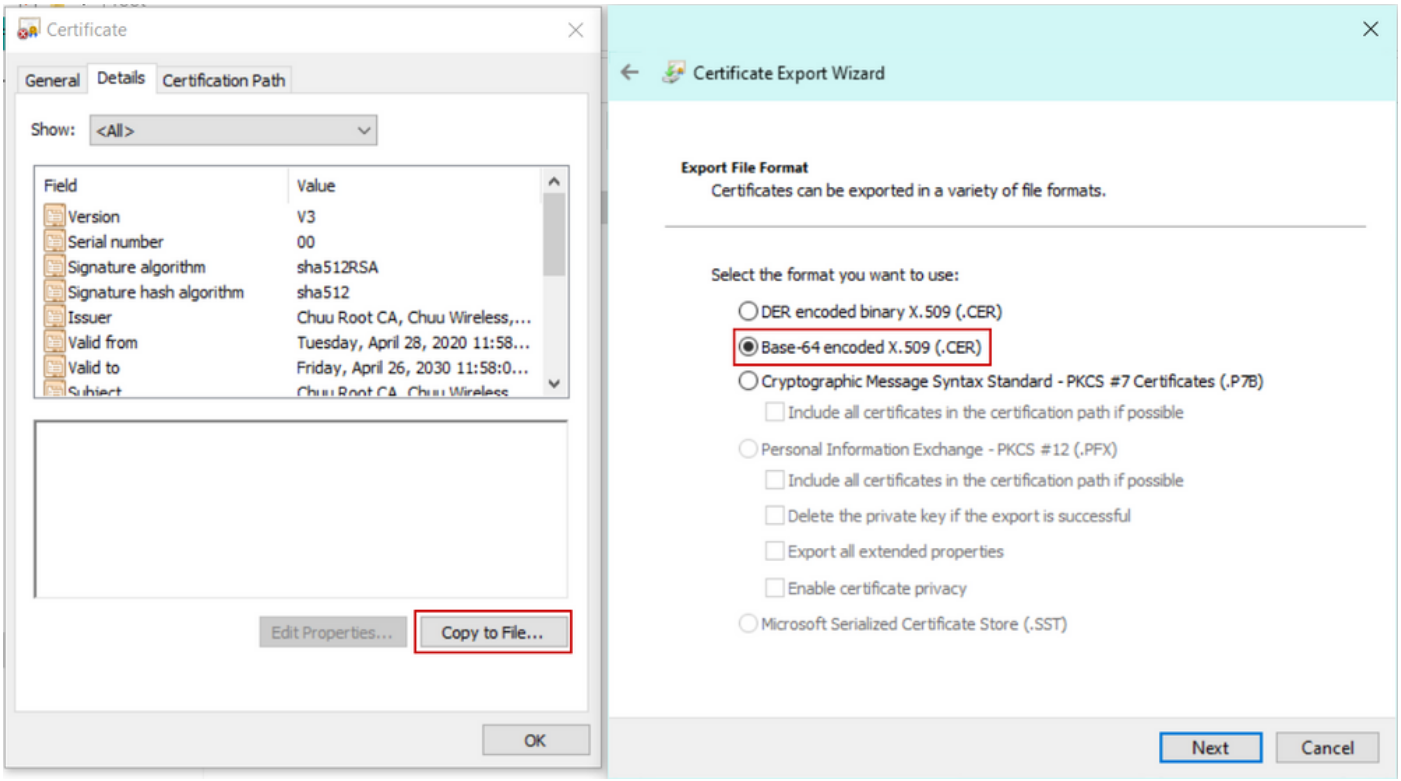
> **Nota**: Si desea agregar un nombre alternativo de asunto, no es posible en las versiones de Cisco IOS XE anteriores a la 17.8.1 debido al ID de bug de Cisco CSCvt15177 . Esta situación puede dar lugar a que algunas alertas del navegador no estén presentes debido a

la SAN. Para evitarlo, cree la clave y la CSR fuera de la caja, como se muestra en la opción 1.

Paso 3. Consiga que su CSR esté firmado por su entidad de certificación (CA). La cadena completa debe enviarse a la CA para que la firme.

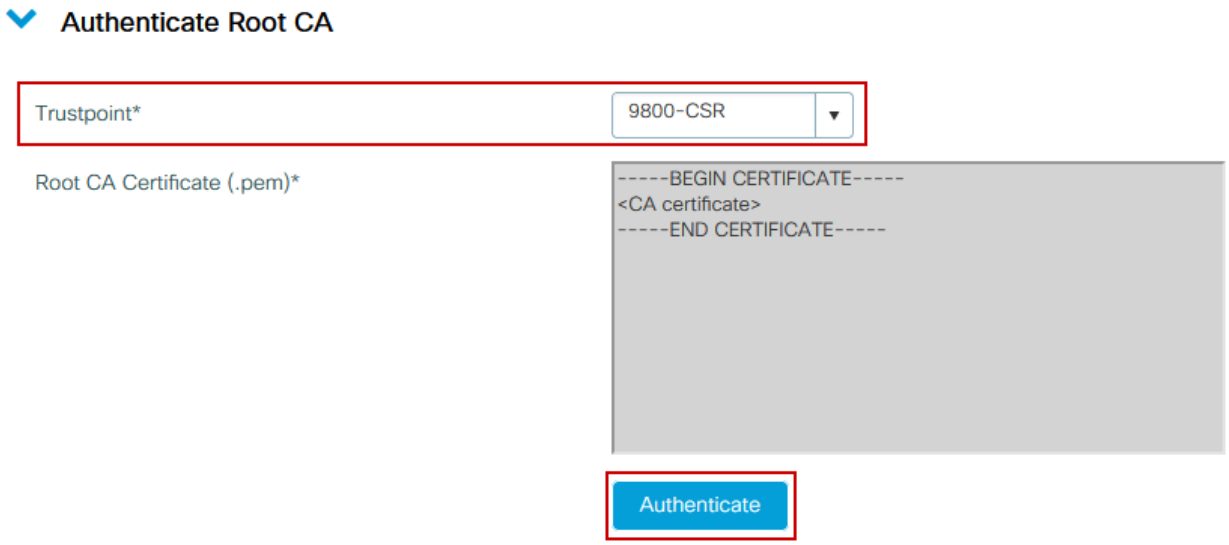
```
-----BEGIN CERTIFICATE REQUEST-----
<Certificate Request>
-----END CERTIFICATE REQUEST-----
```

Si utiliza una CA de Windows Server para firmar el certificado, descargue el certificado firmado en formato Base64. De lo contrario, tendrá que exportar con utilidades como Windows cert manager.



Nota: El proceso de autenticación de punto de confianza depende del número de CA que firmaron su CSR. Si hay una CA de un solo nivel, verifique el **Paso 4a.** Si hay una CA multinivel, vaya al **paso 4b**. Esto es necesario porque un punto de confianza sólo puede almacenar dos certificados a la vez (el certificado del sujeto y el certificado del emisor).

Paso 4a. Haga que 9800 confíe en la CA del emisor. Descargue el certificado de CA del emisor en formato .pem (Base64). Expanda la sección **Autenticación de CA raíz** dentro del mismo menú, elija el punto de confianza definido previamente de la lista desplegable **Punto de confianza** y pegue el certificado de CA del emisor. Asegúrese de que los detalles estén correctamente configurados y haga clic en **Authenticate**.



Configuración de CLI:

```
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
```

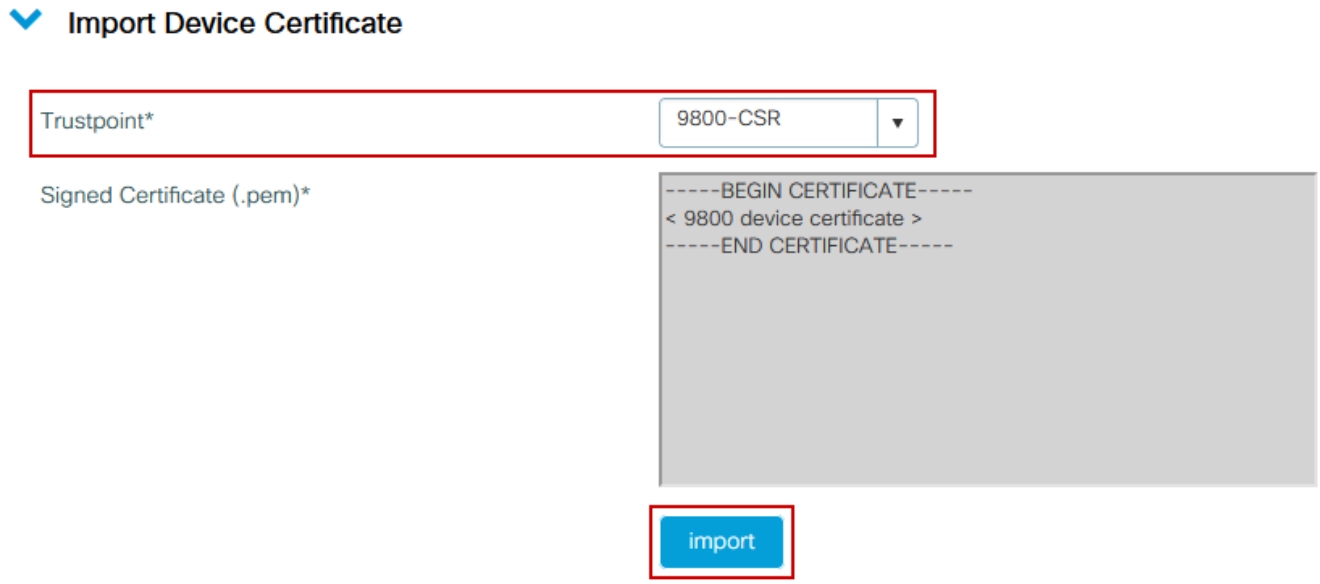
Paso 4b. En el escenario donde existen varios niveles de autorización, se requiere un nuevo punto de confianza para cada nivel de CA. Estos puntos de confianza sólo contienen el certificado de autenticación y apuntan al siguiente nivel de autenticación. Este proceso se realiza solamente en la CLI y en este ejemplo hay una CA intermedia y una CA raíz:

```
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
```

> **Nota**: si hay más de una CA intermedia en la cadena de certificación, se debe generar un nuevo punto de confianza por cada nivel de certificación adicional. Estos puntos de confianza deben hacer referencia al punto de confianza que contiene el siguiente nivel de certificación con el comando **chain-validation continue <trustpoint-name>**.

Paso 5. Cargue el certificado firmado en el WLC 9800. Expanda la sección **Importar certificado de dispositivo** dentro del mismo menú. Elija el **Trustpoint** definido anteriormente y pegue el certificado de dispositivo firmado proporcionado por la CA. A continuación, haga clic en **importar** una vez verificada la información del certificado.



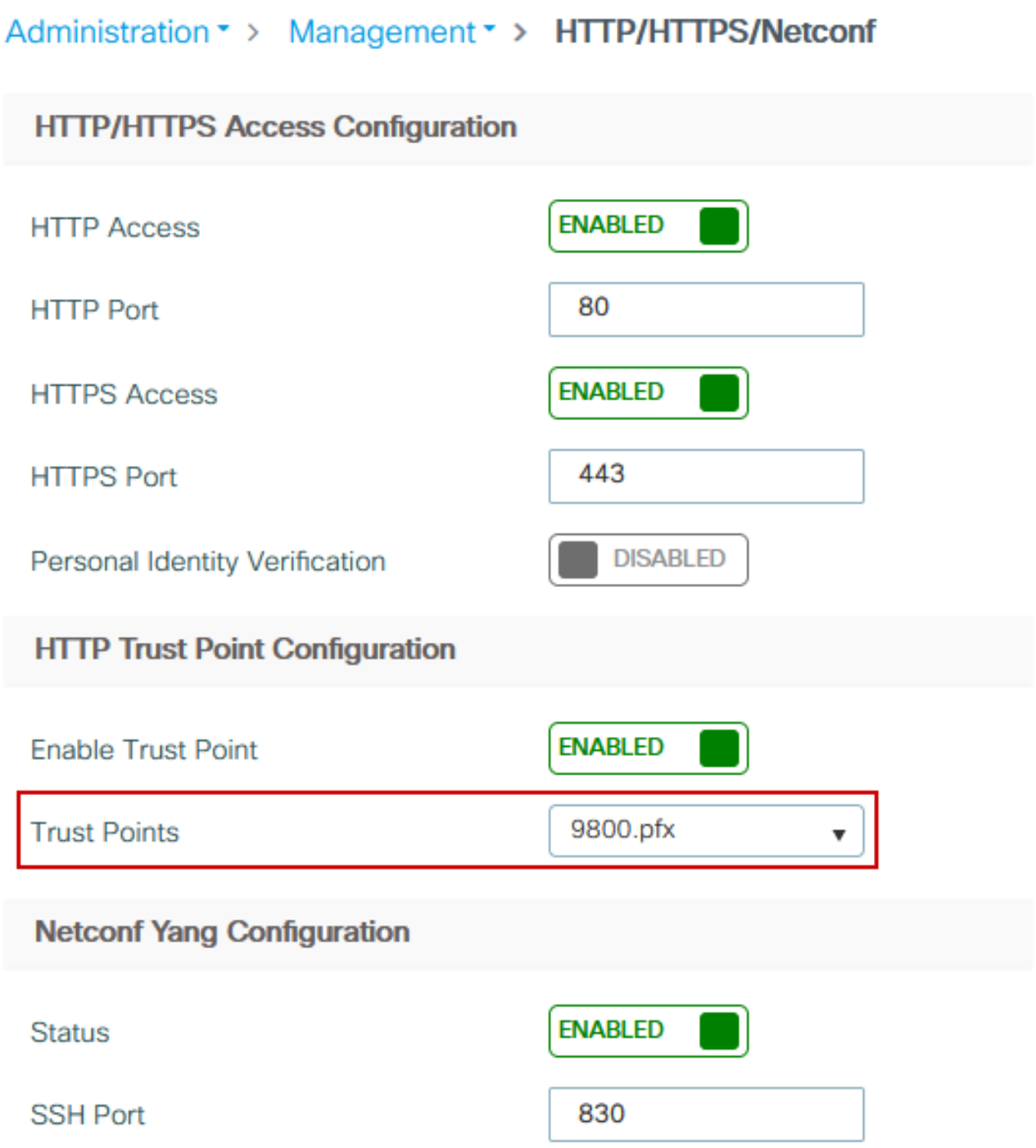
Configuración de CLI:

```
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
```

Utilizar el nuevo certificado

Administración web

Navegue hasta **Administration > Management > HTTP/HTTPS/Netconf** y elija el certificado importado de la lista desplegable **Trust Points**.

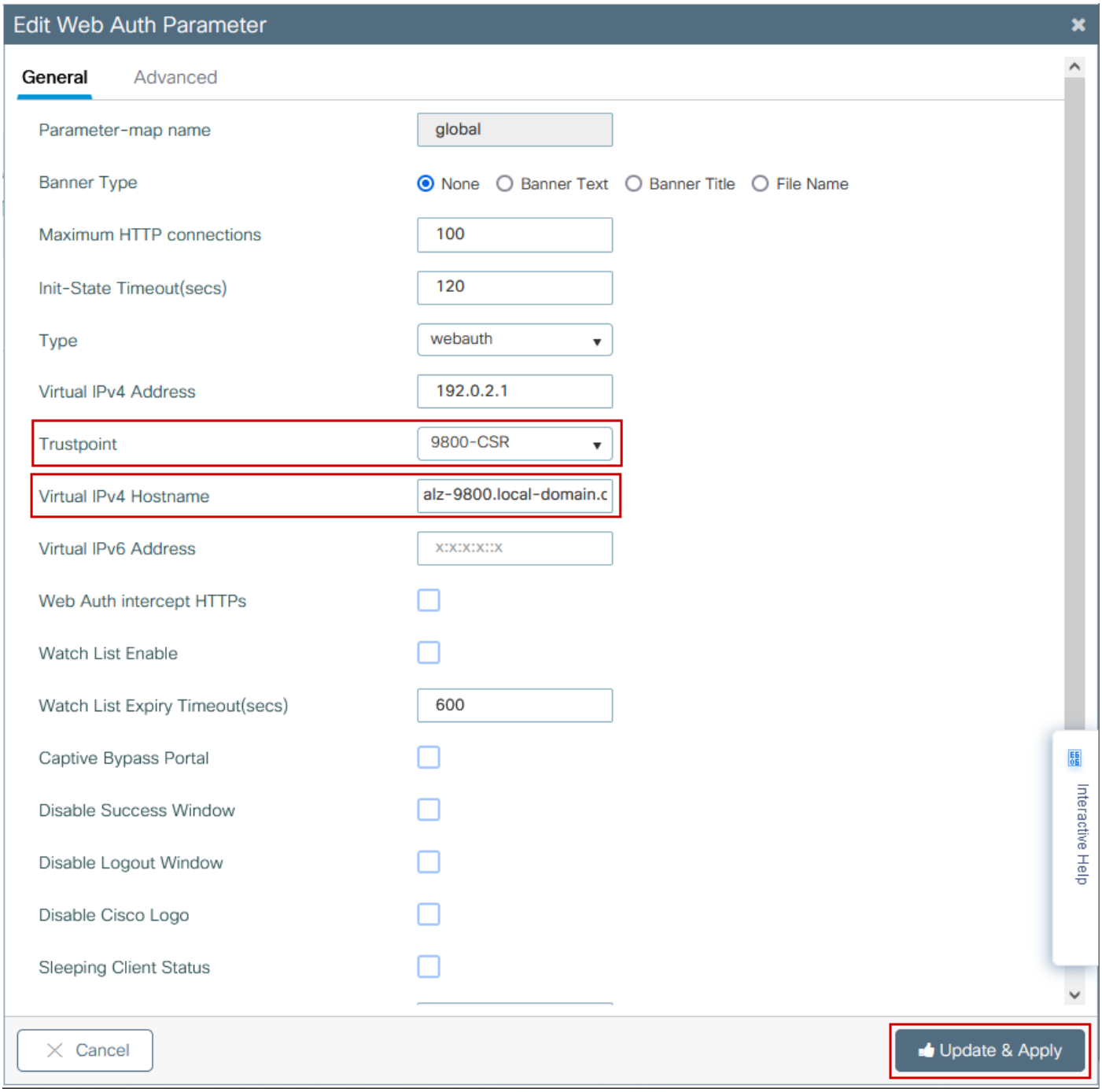


Configuración de CLI:

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

Autenticación web local

Navegue hasta **Configuration > Security > Web Auth**, elija el mapa de parámetro **global** y elija el punto de confianza importado de la lista desplegable **Trustpoint**. Haga clic en **Update & Apply** para guardar los cambios. Asegúrese de que **Virtual IPv4 Hostname** coincida con el Common Name en el certificado.



Configuración de CLI:

```
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
```

Para actualizar el uso del certificado, reinicie los servicios HTTP:

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

.

Consideraciones sobre alta disponibilidad

En un par 9800 configurado para Stateful Switchover High Availability (HA SSO), todos los certificados se replican del principal al secundario en la sincronización masiva inicial. Esto incluye los certificados en los que la clave privada se generó en el propio controlador, incluso si la clave RSA está configurada como no exportable. Una vez establecido el par HA, cualquier certificado nuevo instalado se instala en ambos controladores y todos los certificados se replican en tiempo real.

Después de la falla, el controlador anterior-secundario-ahora-activo utiliza los certificados heredados del primario de manera transparente.

Cómo garantizar que los exploradores web confían en el certificado

Hay algunas consideraciones importantes para garantizar que los exploradores web confían en un certificado:

- Su nombre común (o un campo SAN) debe coincidir con la URL visitada por el navegador.
- Debe estar dentro de su período de validez.
- Debe ser emitido por una CA o cadena de CA cuya raíz sea de confianza para el explorador. Para ello, el certificado proporcionado por el servidor web debe contener todos los certificados de la cadena hasta que (no necesariamente incluido) un certificado de confianza para el explorador cliente (normalmente la CA raíz).
- Si contiene listas de revocación, el explorador debe poder descargarlas y el certificado CN no debe aparecer en la lista.

Verificación

Puede utilizar estos comandos para verificar la configuración de los certificados:

```
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
```

Puede verificar la cadena de certificados en el 9800. En el caso de un certificado de dispositivo emitido por una CA intermedia, a su vez emitido por una CA raíz, tiene un punto de confianza por grupos de dos certificados, por lo que cada nivel tiene su propio punto de confianza. En este caso, el WLC 9800 tiene 9800.pfx con el certificado del dispositivo (certificado del WLC) y su CA que emite (CA intermedia). Luego, otro punto de confianza con la CA raíz que emitió esa CA intermedia.

```
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
```

Verificación de certificados con OpenSSL

OpenSSL puede ser útil para verificar el certificado en sí o para realizar algunas operaciones de conversión.

Para mostrar un certificado con OpenSSL :

```
openssl x509 -in
```

Para mostrar el contenido de una CSR:

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

Si desea verificar el certificado final en el WLC 9800 pero desea utilizar algo más que su navegador, OpenSSL puede hacer esto y darle muchos detalles.

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

Puede sustituir **<**wlcURL**>** por la URL del webadmin del 9800 o la URL del portal de invitados (IP virtual). También puede poner una dirección IP allí. Indica qué cadena de certificados se recibe, pero la validación de certificados nunca puede ser 100% correcta cuando se utiliza una dirección IP en lugar del nombre de host.

Para ver el contenido y verificar un certificado PKCS12 (.pfx) o una cadena de certificados :

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

Este es un ejemplo de este comando en una cadena de certificado donde el certificado del dispositivo es emitido al Technical Assistance Center (TAC) por una CA intermedia llamada "mediana.com", a su vez emitida por una CA raíz llamada "raíz.com" :

```
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-----
```

Troubleshoot

Utilice este comando para solucionar problemas. Si se realiza en una sesión remota (SSH o telnet), se necesita **terminal monitor** para mostrar las salidas:

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

Resultado de depuración de escenario exitoso

Este resultado muestra el resultado esperado cuando se realiza una importación de certificado correcta en un 9800. Utilice esto como referencia e identifique el estado de falla:

```
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.
```

Intente importar un certificado PKCS12 que no tenga una CA

Si importa un certificado y obtiene el error: "No se encuentra el certificado de CA", significa que el archivo .pfx no contiene toda la cadena o que no hay una CA presente.

```
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.
```

Si ejecuta el comando **openssl pkcs12 -info -in <path to cert>** y sólo se muestra un certificado con una clave privada, significa que la CA no está presente. Como regla general, este comando enumera idealmente toda la cadena de certificados. No es necesario incluir la CA raíz superior si ya la conocen los exploradores cliente.

Una manera de solucionar esto es deconstruir el PKCS12 en PEM y reconstruir la cadena correctamente. En el siguiente ejemplo, teníamos un archivo .pfx que contenía solamente el certificado del dispositivo (WLC) y su clave. Fue emitido por una CA intermedia (que no estaba presente en el archivo PKCS12) que, a su vez, estaba firmado por una CA raíz conocida.

Paso 1. Exporte la clave privada hacia fuera.

```
openssl pkcs12 -in
```

Paso 2. Exporte el certificado como PEM.

```
openssl pkcs12 -in
```

Paso 3. Descargue el certificado de la CA intermedia como PEM.

El origen de la CA depende de la naturaleza de la misma. Si es una CA pública, basta con realizar una búsqueda en línea para encontrar el repositorio. De lo contrario, el administrador de la CA debe proporcionar los certificados en formato Base64 (.pem). Si hay varios niveles de CA, agrúpelos en un solo archivo como el que se presenta al final del proceso de importación de la **opción 1**.

Paso 4. Reconstruya el PKCS 12 a partir de la clave, el certificado del dispositivo y el certificado de la CA.

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

Ahora tenemos "fixedcertchain.pfx" que podemos importar gustosamente al Catalyst 9800.

Notas y limitaciones

- Cisco IOS® XE no admite certificados de CA con una validez superior a 2099: Id. de error de Cisco CSCvp64208
- Cisco IOS® XE no es compatible con el paquete PKCS 12 de resumen de mensajes SHA256 (se admiten los certificados SHA256, pero no si el paquete PKCS12 en sí está firmado con SHA256): Id. de error de Cisco CSCvz41428
- Puede ver la fragmentación si el WLC necesita llevar certificados de usuario, y el dispositivo NAC/ISE es accesible a través de Internet (por ejemplo, en una implementación SD-WAN). Los certificados son casi siempre mayores que 1500 bytes (lo que significa que se envían varios paquetes RADIUS para transportar el mensaje del certificado) y si tiene varias MTU diferentes a través de la trayectoria de red, puede ocurrir una fragmentación excesiva de los paquetes RADIUS en sí. En tales casos, recomendamos que envíe todos sus datagramas UDP para el tráfico WLC por la misma ruta para evitar problemas como retraso/fluctuación que pueden ser causados por el clima de Internet

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).