Genere el CSR para los Certificados de tercera persona y descargue los Certificados encadenados a los reguladores inalámbricos del catalizador 9800

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Configurar](#)
[Consiga un certificado firmado](#)
[Cargue un certificado firmado PKCS12](#)
[Generación CSR 9800 WLC y carga por teletratamiento del certificado](#)
[Punta de Webadmin y de Webauth al nuevo certificado](#)
[Verificación](#)
[Troubleshooting](#)

Introducción

Este documento describe cómo generar un pedido de firma de certificado (CSR) para obtener un certificado de tercera persona y cómo descargar un certificado encadenado a un regulador elástico LAN de la Tecnología inalámbrica (9800 WLC) y al uso para el portal del webauth y del webadmin.

Prerrequisitos

Requisitos

Antes de que usted intente esta configuración, Cisco recomienda que usted tiene conocimiento de estos temas:

- Cómo configurar los 9800 WLC, el Punto de acceso ligero (REVESTIMIENTO) para la operación básica
- Cómo utilizar la aplicación de OpenSSL
- Infraestructura y Certificados digitales de la clave pública

Componentes Utilizados

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

- Versión 16.10 virtual 9800 WLC
- Aplicación de 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 su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Configurar

9800 ayudas de WLCs solamente un certificado de la autenticación Web, el certificado que usted marca para el trustpoint seguro HTTP serán tan la que está usada para los identificadores del conjunto de servicio de la autenticación Web (SSID) y para la Administración de la interfaz gráfica de usuario (GUI).

Consiga un certificado firmado

Hay la opción dos para conseguir un certificado para 9800 WLC.

1. Genere el pedido de firma de certificado (CSR) usando OpenSSL. Consiga un certificado PKCS12 firmado por su CA y cargúelo directamente a los 9800 WLC. Esto significa que la clave privada está liada con ese certificado. Para más información sobre cómo generar un CSR con OpenSSL usted puede controlar este link: CSR con OpenSSL
2. Utilice el comando line interface(cli) 9800 WLC de generar un pedido de firma de certificado (CSR), consígalo firmado por las autoridades de certificación y después cargue el certificado firmado

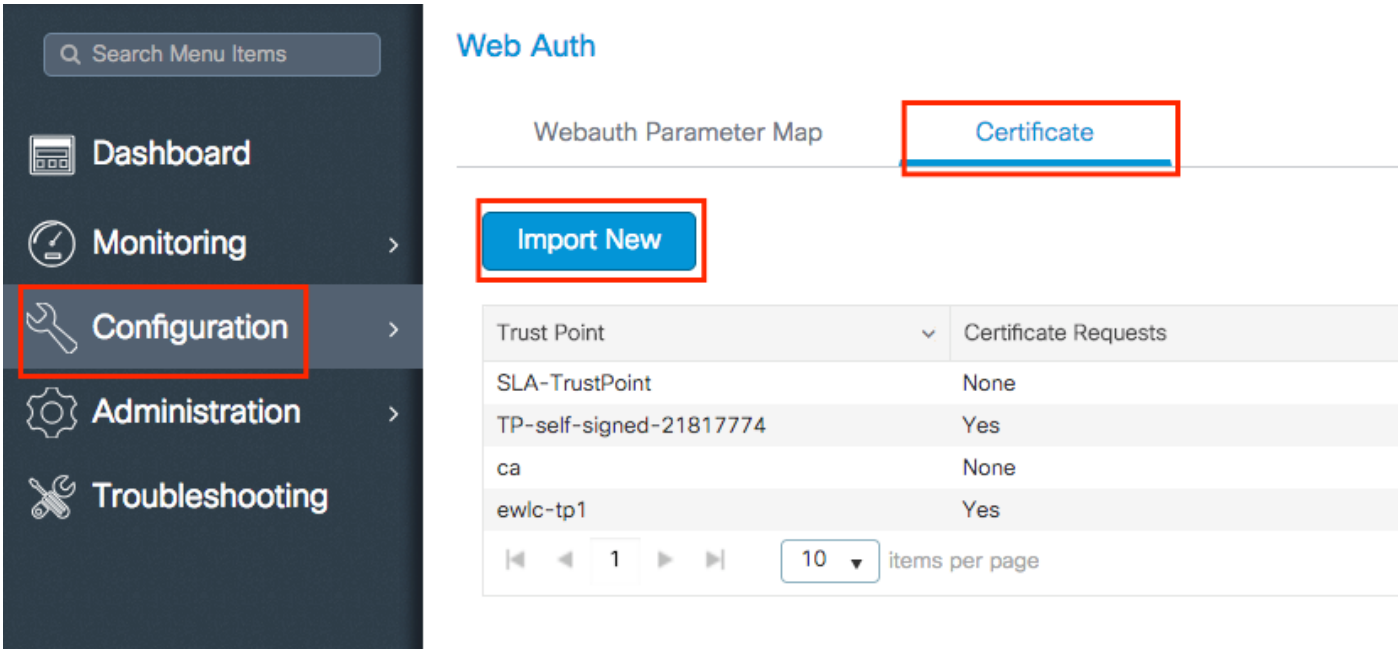
Utilice el que le cabe más.

Cargue un certificado firmado PKCS12

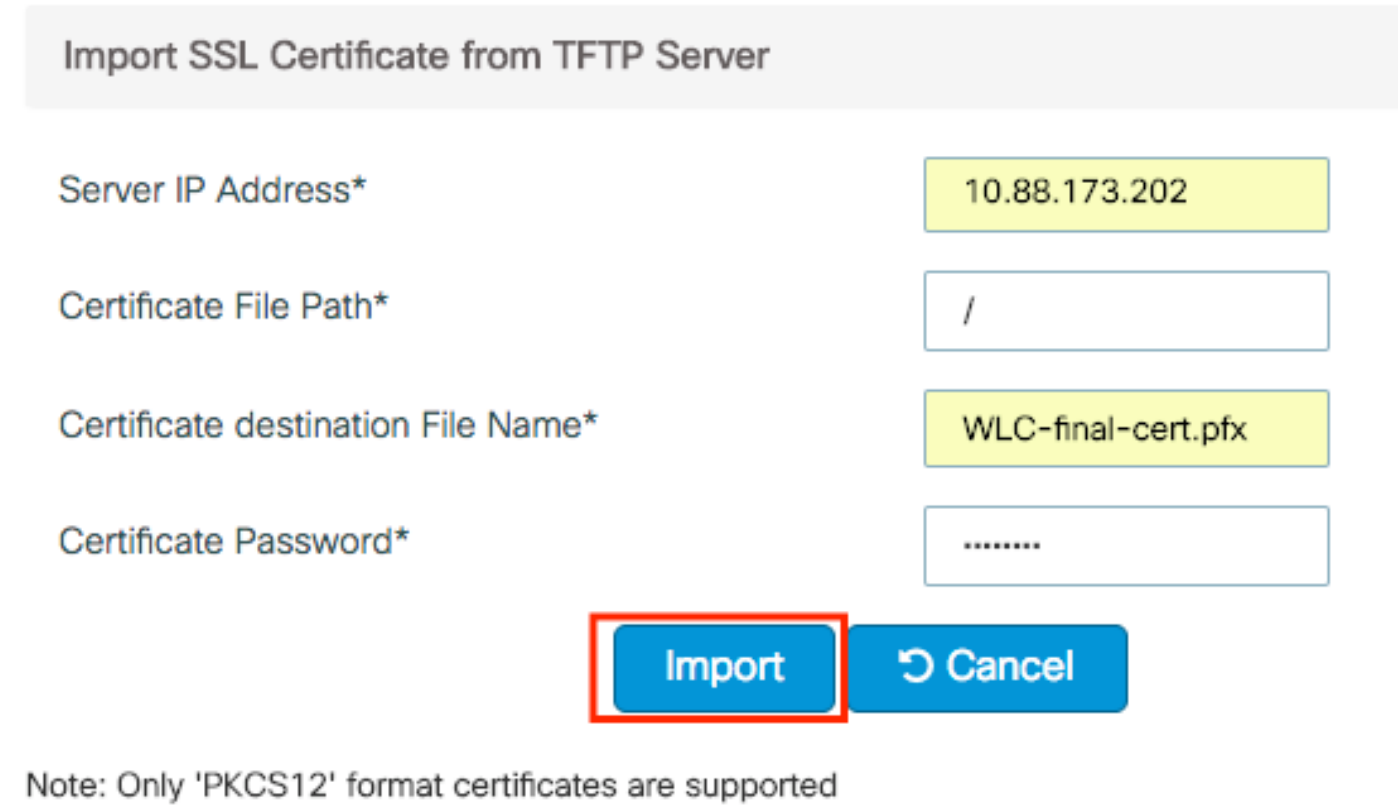
GUI:

Paso 1. Salve su certificado PKCS12 en un servidor del Trivial File Transfer Protocol (TFTP) que sea accesible de los 9800 WLC

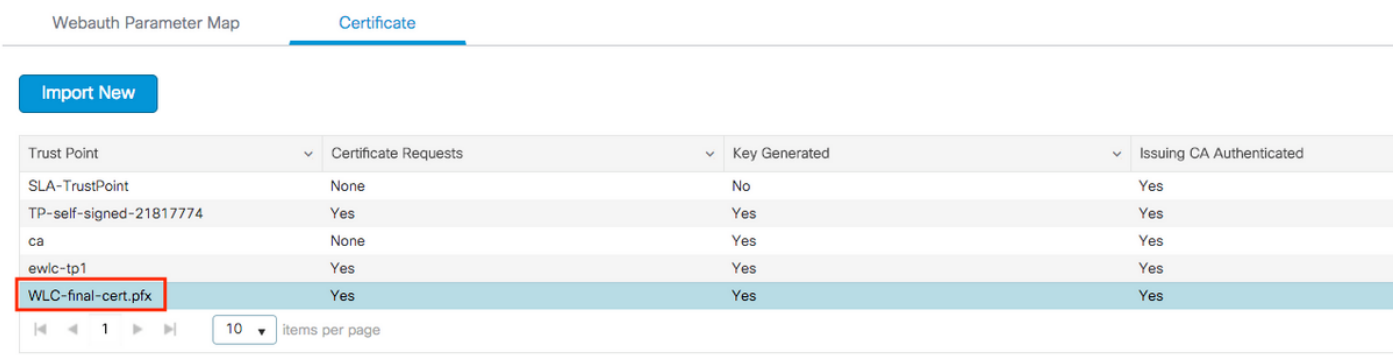
Paso 2. Abra el GUI sus 9800 WLC y navegue al **> Security (Seguridad) de la configuración > a la red auténticos > certificado** y haga clic la **importación nueva.**



Paso 3. Ingrese la información pedida y haga clic la **importación.**



Después que usted ve el nuevo certificado cargado.



CLI:

```
# config t
# crypto pki import <cert-name> pkcs12 tftp://<TFTP-IP>/<cert-name> password <cert-password>
```

Generación CSR 9800 WLC y carga por teletratamiento del certificado

Paso 1. Genere un par clave de fines generales RSA.

Ábrase una sesión por el Secure Shell (SSH) a sus 9800 WLC y publique estos comandos. Elegimos nombrar nuestras ewlc-**claves del** par clave, pero usted puede fijar el nombre que usted quiere:

```
# configure terminal
# crypto key generate rsa general-keys label ewlc-keys exportable

The name for the keys will be: ewlc-keys
Choose the size of the key modulus in the range of 360 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 [512]: 2048
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)
```

Paso 2. Genere un CSR para sus 9800 WLC virtuales. Asegure eligió un NC (y otras opciones del certificado) que haga juego el URL que será visitado (página del invitado, página del administrador Web, dependiendo de los casos del uso). Elegimos nombrar nuestro ewlc-**CERT del** certificado en este ejemplo pero usted puede eligió el nombre que usted prefiere distinguir sus Certificados.

```
# configure terminal
(config)#crypto pki trustpoint ewlc-cert
(ca-trustpoint)# enrollment terminal pem
(ca-trustpoint)# revocation-check none
(ca-trustpoint)# subject-name C=MX, ST=Nuevo Leon, L=Guadalupe, O=lab-wireless, OU=mex-wireless,
CN=public-guest.lab-kcg.com
(ca-trustpoint)# rsakeypair ewlc-keys
(ca-trustpoint)# exit

(config)#crypto pki enroll ewlc-cert
% Start certificate enrollment ..

% The subject name in the certificate will include: C=MX, ST=Nuevo Leon, L=Guadalupe, O=lab-
wireless, OU=mex-wireless, CN=public-guest.lab-kcg.com
% The subject name in the certificate will include: 9800 WLC-karlcisn-Public.lab-kcg.com
% 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-----
*9800 WLC CSR*
-----END CERTIFICATE REQUEST-----

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

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

C: País

ST: Un cierto estado, refiere al nombre del estado o de la provincia

L: El nombre de la ubicación, refiere a la ciudad

O: Nombre de la organización, referst a la compañía

OU: El nombre de la unidad organizacional, poder refiere a la sección.

NC: (Nombre común) refiere al tema al cual el certificado será publicado, usted debe especificar la dirección IP virtual de sus 9800 WLC, el hostname asociado a la dirección IP virtual de sus 9800 WLC, a la dirección IP de la Administración o al hostname asociado a la dirección IP de la Administración.

Paso 3. Consiga su CSR firmado por sus autoridades de certificación (el CA)

La cadena llena necesitará ser enviada a su CA para conseguirlo firmado.

```
# configure terminal
(config)#crypto pki trustpoint ewlc-cert
(ca-trustpoint)# enrollment terminal pem
(ca-trustpoint)# revocation-check none
(ca-trustpoint)# subject-name C=MX, ST=Nuevo Leon, L=Guadalupe, O=lab-wireless, OU=mex-wireless,
CN=public-guest.lab-kcg.com
(ca-trustpoint)# rsakeypair ewlc-keys
(ca-trustpoint)# exit

(config)#crypto pki enroll ewlc-cert
% Start certificate enrollment ..

% The subject name in the certificate will include: C=MX, ST=Nuevo Leon, L=Guadalupe, O=lab-
wireless, OU=mex-wireless, CN=public-guest.lab-kcg.com
% The subject name in the certificate will include: 9800 WLC-karlcisn-Public.lab-kcg.com
% 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-----
*9800 WLC CSR*
-----END CERTIFICATE REQUEST-----

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

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

Si usted utiliza a un Servidor Windows CA para firmar el certificado, descargue el certificado resultante en el formato Base64.

Paso 4. Haga su confianza 9800 WLC su CA

Usted debe conseguir el certificado raíz del CA que firmó el CSR sus 9800 WLC en el formato .pem.

Una vez que usted lo tiene, ábrase una sesión por SSH o Telnet a sus 9800 WLC y funcione con

estos comandos de copiar y de pegar el certificado raíz.

```
# config t
(config)# crypto pki authenticate ewlc-cert

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

-----BEGIN CERTIFICATE-----
*Root CA certificate*
-----END CERTIFICATE-----
quit
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 5. Cargue el certificado firmado en los 9800 WLC.

Ejecute éstos ordenan para cargar el certificado firmado que usted consiguió de su CA en los 9800 WLC.

```
# config t
(config)# crypto pki authenticate ewlc-cert

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

-----BEGIN CERTIFICATE-----
*Root CA certificate*
-----END CERTIFICATE-----
quit
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
```

> **Note**: La mayoría de los CAs sabidos proporcionan al certificado encadenado: raíz--> intermedio-->device. Si usted utiliza un CA que tenga la raíz y dispositivo intermedio usted tienen que especificar el dispositivo y el CERT intermedio.

Webadmin y Webauth señalan al nuevo certificado

Señale los portales web para utilizar el certificado firmado, salve la configuración y recargue los 9800 WLC para realizar el cambio tomar el efecto.

```
# config t
(config)# crypto pki authenticate ewlc-cert

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

```
-----BEGIN CERTIFICATE-----
*Root CA certificate*
-----END CERTIFICATE-----
quit
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
```

Si usted no quiere recargar los 9800 WLC, recomience al servidor Web puede hacer el truco:

```
# config t
(config)# crypto pki authenticate ewlc-cert

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

-----BEGIN CERTIFICATE-----
*Root CA certificate*
-----END CERTIFICATE-----
quit
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
```

Verificación

Usted puede utilizar estos comandos de verificar la configuración de los Certificados:

```
# show crypto pki certificates <cert-name>

Certificate
Status: Available
Certificate Serial Number (hex): 00A2020356CF31C818
Certificate Usage: General Purpose
Issuer:
cn=CA-KCG-lab
ou=lab-mex-wireless
o=mex-wireless
l=Guadalupe
st=Nuevo Leon
c=MX
Subject:
Name: *.lab-kcg.com
cn=*.lab-kcg.com
ou=lab-mex-wireless
o=mex-wireless
l=Benito Juarez
st=CDMX
c=MX
Validity Date:
start date: 17:14:54 UTC Feb 15 2018
end date: 17:14:54 UTC Mar 11 2023
```

```
Associated Trustpoints: cert-name
Storage: nvram:CA-KCG-lab#C818.cer

# 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: cert-name
HTTP secure server active session modules: ALL
```

Troubleshooting

Utilice este comando de resolver problemas.

```
# 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: cert-name
HTTP secure server active session modules: ALL
```