

# Genere el CSR para los Certificados de tercera persona y descargue los Certificados encadenados al WLC

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requisitos](#)

[Componentes usados](#)

[Certificados encadenados](#)

[Ayuda para el certificado encadenado](#)

[Niveles del certificado](#)

[Paso 1. Genere un CSR](#)

[CSR de la opción A. con OpenSSL](#)

[Opción B. CSR Generated por el WLC](#)

[Paso 2. Consiga el certificado firmado](#)

[Opción A: Obtenga el fichero Final.pem de su empresa CA](#)

[Opción B: Obtenga el fichero Final.pem de un CA de tercera persona](#)

[Paso 3 CLI. Descargue el certificado de tercera persona al WLC con el CLI](#)

[Paso 3 GUI. Descargue el certificado de tercera persona al WLC con el GUI](#)

[Troubleshooting](#)

[Información Relacionada](#)

## 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 LAN de la Tecnología inalámbrica (red inalámbrica (WLAN)) (WLC).

## Prerequisites

### Requisitos

Antes de que usted intente esta configuración, usted debe tener conocimiento de estos temas:

- Cómo configurar el WLC, el Punto de acceso ligero (REVESTIMIENTO), y el indicador luminoso LED amarillo de la placa muestra gravedad menor del cliente de red inalámbrica para la operación básica
- Cómo utilizar la aplicación de OpenSSL
- Infraestructura y Certificados digitales de la clave pública

### Componentes usados

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

- Cisco 5508 WLC que funciona con la versión de firmware 8.3.102
- Aplicación de OpenSSL para Microsoft Windows
- Herramienta de la inscripción que es específica a las autoridades de certificación de tercera persona (CA)

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Certificados encadenados

Una Cadena de certificados es una secuencia de Certificados, donde cada certificado en el encadenamiento es firmado por el certificado subsiguiente. El propósito de una Cadena de certificados es establecer un encadenamiento de la confianza de un certificado de peer a un certificado CA de confianza. El CA atestigua para la identidad en el certificado de peer cuando la firma. Si el CA es uno que usted confía en, que es indicado por la presencia de una copia del certificado CA en su directorio del certificado raíz, éste le implica puede confiar en el certificado de peer firmado también.

A menudo, los clientes no validan los Certificados porque un CA sabido los no crearon. Del cliente los estados típicamente que la validez del certificado no puede ser verificada. Éste es el caso cuando el certificado es firmado por un CA intermedio, que no se sabe al buscador del cliente. En estos casos, es necesario utilizar un certificado SSL o un grupo encadenado del certificado.

### Ayuda para el certificado encadenado

El regulador permite para que el certificado del dispositivo sea descargado como certificado encadenado para la autenticación Web.

### Niveles del certificado

- Nivel 0 - Uso solamente de un certificado de servidor en el WLC
- Nivel 1 - Uso de un certificado de servidor en el WLC y un certificado raíz CA
- Nivel 2 - Uso de un certificado de servidor en el WLC, un solo certificado intermedio CA, y un certificado raíz CA
- Nivel 3 - Uso de un certificado de servidor en el WLC, dos Certificados intermedios CA, y un certificado raíz CA

El WLC no utiliza encadenado certifica más que 10KB de tamaño en el WLC. Sin embargo, esta restricción se ha quitado en la versión 7.0.230.0 WLC y más adelante.

**Note:** Los Certificados encadenados se utilizan para la autenticación Web solamente; no se utilizan para el certificado de la Administración.

**Note:** Los Certificados del comodín se utilizan completamente para EAP local, la Administración o el webauthentication

Los Certificados de la autenticación Web pueden ser ninguno de estos:

- Encadenado
- Soltado
- Auto-generado

**Note:** En la versión 7.6 y posterior WLC, solamente los Certificados encadenados se utilizan en el WLC para la autenticación Web.

Si usted está mirando para generar un certificado soltado para el fin de administración, usted puede seguir este documento e ignorar las piezas donde el certificado se combina con el certificado CA.

Este documento discute cómo instalar correctamente un certificado encadenado del Secure Socket Layer (SSL) a un WLC.

## Paso 1. Genere un CSR

Hay dos maneras de generar un CSR. Manualmente con OpenSSL (la única forma posible en software WLC pre-8.3) o usar el WLC sí mismo para generar el CSR (disponible después de 8.3.102).

### CSR de la opción A. con OpenSSL

**Note:** La versión 58 y posterior de Chrome no confía en el nombre común del certificado solamente y requiere el nombre alterno sujeto también estar presente. La sección siguiente explicará cómo agregar los campos SAN al CSR de OpenSSL que es un nuevo requisito para este navegador.

Complete estos pasos para generar un CSR con OpenSSL:

1. Instale y abra el [OpenSSL](#).

En Microsoft Windows, por abandono, openssl.exe está situado en C:\ > **el openssl > el compartimiento.**

**Note:** La versión 0.9.8 de OpenSSL es la versión recomendada para las viejas versiones WLC; sin embargo, a partir de la versión 7.5, la ayuda para la versión 1.0 de OpenSSL también fue agregada (refiera al ID de bug [CSCti65315 de Cisco](#) - ayuda de la necesidad para los Certificados generados usando OpenSSL v1.0) y es la versión recomendada a utilizar. OpenSSL 1.1 trabajos también fue probado y funciona increíble en 8.x y versiones posteriores WLC.

2. Localice su fichero de los config de OpenSSL y haga una copia de ella para corregirla para este CSR. Corrija la copia para agregar las secciones siguientes:

3.

```
[req]
req_extensions = v3_req
```

```
[ v3_req ]
```

```
# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = server1.example.com
DNS.2 = mail.example.com
DNS.3 = www.example.com
DNS.4 = www.sub.example.com
DNS.5 = mx.example.com
DNS.6 = support.example.com
```

Las líneas que comienzan con el "DNS.1", el "DNS.2" y así sucesivamente deben contener todos los nombres alternos que sus Certificados tendrán. Usted puede entonces escribir cualquier URL posible que usted esté utilizando para el WLC. Las líneas en antedicho intrépido no estaban presentes ni fueron comentadas en nuestra versión del openssl del laboratorio, puede variar grandemente dependiendo del sistema operativo y de la versión del openssl. Salvamos esta versión modificada de los config como **openssl-san.cnf** por este ejemplo.

4. Publique este comando para generar un nuevo CSR:

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem -config openssl-
san.cnf
```

**Note:** Ayuda de WLCs un tamaño de clave máximo de 2,048 bits.

5. Después de que usted publique el comando, hay un mensaje para una cierta información: Nombre del país, estado, ciudad, y así sucesivamente. Proporcione la información requerida.

**Note:** Es importante que usted proporciona al nombre común correcto. Asegúrese de que el nombre de host que se utiliza para crear el certificado (nombre común) haga juego la entrada de nombre de host del Domain Name System (DNS) para la dirección IP de la interfaz virtual en el WLC y de que el nombre existe en el DNS también. También, después de que usted realice el cambio IP virtual al interfaz (VIP), usted debe reiniciar el sistema para que este cambio tome el efecto.

Aquí está un ejemplo:

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem -config openssl-
san.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
```

State or Province Name (full name) [Some-State]:CA  
Locality Name (eg, city) []:San Jose  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC  
Organizational Unit Name (eg, section) []:CDE  
Common Name (eg, YOUR name) []:XYZ.ABC  
Email Address []:Test@abc.com

Please enter the following 'extra' attributes  
to be sent with your certificate request

A challenge password []:Test123

An optional company name []:OpenSSL>

6. Usted puede verificar el CSR (especialmente para el SAN atribuye la presencia) con el **req del openssl - texto - noout - en el csrfilename**
7. Después de que usted proporcione a todos los detalles requeridos, se generan dos ficheros:

una nueva clave privada que incluye el nombre **mykey.pem** un CSR que incluye el nombre **myreq.pem**

## Opción B. CSR Generated por el WLC

Si su WLC ejecuta la versión de software 8.3.102 o más adelante, más opción segura (y el más fáciles también) es utilizar el WLC para generar el CSR. La ventaja es que la clave está generada en el WLC y nunca sale del WLC; así nunca se expone en el mundo exterior.

A partir de ahora, este método no permite configurar el SAN en el CSR que pudo llevar a los problemas con ciertos navegadores que requiere la presencia de un atributo SAN. Algún CA permite insertar los campos SAN en el tiempo de firma, así que es una buena idea controlar con su CA.

**Note:** Si usted funciona con el comando de la generación csr y no instala el certificado resultante todavía, su WLC será totalmente inalcanzable en el HTTPS en la reinicialización siguiente, pues el WLC utilizará la clave nuevamente generada CSR después de que la reinicialización pero no tenga el certificado que va con ella.

Para generar un CSR para la autenticación Web, ingrese este comando:

**El certificado del >config (WLC) genera el csr-webauth SEA TAC de Cisco mywebauthportal.wireless.com tac@cisco.com de Bruselas del BR**

-----COMIENCIE LA SOLICITUD DE CERTIFICADO-----

```
MIICqjCCAZICAQAwwZTELMAkGA1UECAwCQlIxETAPBgNVBACMCEJydXNzZWxzMQ4w  
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVVEFDMSUwIwYDVQQDDDBxteXdIYmF1dGhw  
b3J0YWwud2lyZWxlc3MuY29tMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKc  
AQEAnssc0BxIj2ULa3xgJH5IAUtbD9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX  
JiaBbKMA27VJH1J2K2ycDMIhJyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK  
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NIZqg1hNemnhqVgbXEd90sgJmaF2  
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJial2JpbO0afRO3kSg  
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjiMzKT6OOjFGOGu  
yNkgYefrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K  
ZvEpAafoovphlcXIEIL2DSwVzjIbd9u7T5JRGgqri1I9/0wzxFjTymQofga427mj  
5dNqICWxRFmKhAmO0fGQkUoP1YhJRxidU+0T8O46s/stbhj9nuInmoTgPaA0s3YH  
tDdWgjmV2ASnroUV9oBNu3wR6RQtkDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd  
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqIPWYVQccvGyFacscA7L+nZK3SSITzGt9B2HAa  
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
```

Wkc/wH4DyYdH7x5jzHc=

-----TERMINE LA SOLICITUD DE CERTIFICADO-----

Para generar un CSR para el webadmin, el comando cambia descubierto:

**El certificado del >config (WLC) genera el csr-webadmin SEA TAC de Cisco mywebauthportal.wireless.com tac@cisco.com de Bruselas del BR**

**Note:** El CSR se imprime en la terminal después de que usted ingrese el comando. No hay otras maneras de extraerlo; no es posible cargarlo por teletratamiento del WLC ni es posible salvarlo. Usted debe copiar/goma él a un fichero en su ordenador después de que usted ingrese el comando. La clave generada permanece en el WLC hasta que se genere el CSR siguiente (la clave está sobregrabada así). Si usted tiene que cambiar nunca la dotación física WLC después (RMA), usted no podrá reinstalar el mismo certificado que una nuevos clave y CSR tendrán que ser generados en el nuevo WLC.

Usted entonces tiene que entregar este CSR a su autoridad de firma de tercera persona o a su Public Key Infrastructure (PKI) de la empresa.

## Paso 2. Consiga el certificado firmado

### Opción A: Obtenga el fichero Final.pem de su empresa CA

Este ejemplo muestra solamente una empresa existente CA (Servidor Windows 2012 en este ejemplo) y no cubre los pasos para poner a un Servidor Windows CA a partir de cero.

1. Va a su página del enterprise CA en el navegador (generalmente [https:// <CA-ip>/certsrv](https://<CA-ip>/certsrv)) y hace clic la **petición un certificado**.

#### Welcome

---

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

#### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

---

2. Solicitud de certificado avanzada del teclado.

# Request a Certificate

---

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

---

3. Ingrese el CSR que usted obtuvo del WLC o del OpenSSL. En la lista desplegable del Certificate Template plantilla de certificado, elija al **servidor Web**.

## **Submit a Certificate Request or Renewal Request**

---

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request into the Request box.

### **Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
5dNq1CWxRFmKhAm0fGQkUoP1YhJRxiDu+0T8046
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5Y
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWYVQccvGyFa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOn
Wkc/wH4DyYdH7x5jzHc=
-----END CERTIFICATE REQUEST-----
```

### **Certificate Template:**

---

Web Server

### **Additional Attributes:**

---

Attributes:

4. Haga clic el botón de radio **codificado base 64**.

## Certificate Issued

---

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

---

5. Si el certificado descargado es del tipo PKCS7 (.p7b), después usted necesita convertirlo al PEM (en el ejemplo abajo descargamos la Cadena de certificados como nombre de fichero el "All-certs.p7b"):

```
openssl pkcs7 - print_certs - in All-certs.p7b - hacia fuera All-certs.pem
```

6. Combine los Certificados de la Cadena de certificados (en este ejemplo, se nombra "All-certs.pem") con la clave privada que usted generó junto con el CSR (la clave privada del certificado del dispositivo, que es mykey.pem en este ejemplo) si usted fue con la opción A (es decir, usted utilizó OpenSSL para generar el CSR), y salva el fichero como final.pem. **Si usted generó el CSR directamente del WLC (opción B) usted puede saltar este paso.**

Publique estos comandos en la aplicación de OpenSSL para crear los ficheros All-certs.pem y final.pem:

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem  
-out All-certs.p12 -clcerts -passin pass:check123  
-passout pass:check123
```

```
openssl>pkcs12 -in All-certs.p12 -out final.pem  
-passin pass:check123 -passout pass:check123
```

**Note:** En este comando, usted debe ingresar una contraseña para los parámetros - **passin** y - **passout**. La contraseña que se configura para - parámetro del **passout** debe hacer juego el parámetro del **certpassword** que se configura en el WLC. En este ejemplo, la contraseña que se configura para - **passin** y - los parámetros del **passout** son **check123**.

Final.pem es el fichero que usted debe descargar al WLC si usted siguió el "CSR de la opción A. con OpenSSL". Si usted siguió el "CSR de la opción B. generado por el WLC sí mismo", después All-certs.pem es el fichero que usted debe descargar al WLC. El siguiente paso es descargar este fichero al WLC.

**Note:** Si la carga por teletratamiento del certificado al WLC falla, puede ser que usted no tenga el encadenamiento entero en el fichero PEM. Refiera al paso 2 de la opción B



(obtenga el final.pem de las de otras compañías CA) abajo para ver cómo deben parecer. Si usted ve solamente un certificado en el fichero, después usted necesidad de descargar manualmente todo el intermedio y certificado raíz CA ficheros y de añadirlos al final del fichero (por la goma de la copia sencilla) al fichero para crear el encadenamiento.

## Opción B: Obtenga el fichero Final.pem de un CA de tercera persona

1. La copia y pega la información CSR en cualquier herramienta de la inscripción CA.

Después de que usted presente el CSR al CA de tercera persona, el CA de tercera persona firma digitalmente el certificado y devuelve el encadenamiento de certificado firmado a través del correo electrónico. En el caso de los Certificados encadenados, usted recibe el encadenamiento entero de los Certificados del CA. Si usted tiene solamente un certificado intermedio como en este ejemplo, usted recibe estos tres Certificados del CA:

Raíz certificate.pem Certificate.pem intermedioDispositivo certificate.pem **Note:** Asegúrese de que el certificado sea Apache-compatible con el cifrado del algoritmo de troceo seguro 1 (SHA1).

2. Una vez que usted tiene tres Certificados, copie y pegue el contenido de cada fichero .pem en otro fichero en esta orden:

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem
-out All-certs.p12 -clcerts -passin pass:check123
-passout pass:check123
```

```
openssl>pkcs12 -in All-certs.p12 -out final.pem
-passin pass:check123 -passout pass:check123
```

3. Salve el fichero como **All-certs.pem**.
4. Combine el certificado All-certs.pem con la clave privada que usted generó junto con el CSR (la clave privada del certificado del dispositivo, que es mykey.pem en este ejemplo) si usted fue con la opción A (es decir, usted utilizó OpenSSL para generar el CSR), y salva el fichero como final.pem. **Si usted generó el CSR directamente del WLC (opción B) usted puede saltar este paso.**

Publique estos comandos en la aplicación de OpenSSL para crear los ficheros All-certs.pem y final.pem:

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem
-out All-certs.p12 -clcerts -passin pass:check123
-passout pass:check123
```

```
openssl>pkcs12 -in All-certs.p12 -out final.pem
-passin pass:check123 -passout pass:check123
```

**Note:** En este comando, usted debe ingresar una contraseña para los parámetros - **passin** y - **passout**. La contraseña que se configura para - parámetro del **passout** debe hacer juego el parámetro del **certpassword** que se configura en el WLC. En este ejemplo, la contraseña que

se configura para - **passin** y - los parámetros del **passout** son **check123.Final.pem** es el fichero que usted debe descargar al WLC si usted siguió el “CSR de la opción A. con OpenSSL”. Si usted siguió el “CSR de la opción B. generado por el WLC sí mismo”, después **All-certs.pem** es el fichero que usted debe descargar al WLC. El siguiente paso es descargar este fichero al WLC.

**Note:** SHA2 también se utiliza. El ID de bug [CSCuf20725 de](#) Cisco es un pedido la ayuda SHA512.

## Paso 3 CLI. Descargue el certificado de tercera persona al WLC con el CLI

Complete estos pasos para descargar el certificado encadenado al WLC con el CLI:

1. Mueva el **fichero final.pem** al directorio de valor por defecto en su servidor TFTP.
2. En el CLI, publique estos comandos para cambiar las configuraciones de la transferencia directa:

```
>transfer download mode tftp
>transfer download datatype webauthcert
>transfer download serverip <TFTP server IP address>
>transfer download path <absolute TFTP server path to the update file>
>transfer download filename final.pem
```

3. Ingrese la contraseña para el fichero .pem de modo que el sistema operativo pueda descryptar la clave y el certificado SSL.

```
>transfer download certpassword password
```

**Note:** Sea que el valor para el **certpassword** es lo mismo que - la contraseña segura del parámetro del **passout** que fue fijada en el paso 4 (o 5) de la [generación una](#) sección [CSR](#). En este ejemplo, el **certpassword** debe ser **check123**. Si usted había elegido la opción B (es decir, utilice el WLC sí mismo para generar el CSR) que usted puede dejar el espacio en blanco del campo del **certpassword**.

4. Publique el **comando transfer download start** para ver las configuraciones actualizadas. Entonces ingrese **y** en el pronto para confirmar las configuraciones actuales de la transferencia directa y comenzar la transferencia directa del certificado y de la clave. Aquí está un ejemplo:

```
(Cisco Controller) >transfer download start

Mode..... TFTP
Data Type..... Site Cert
TFTP Server IP..... 10.77.244.196
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
```

TFTP Path...../  
TFTP Filename..... final.pem

This might take some time.  
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

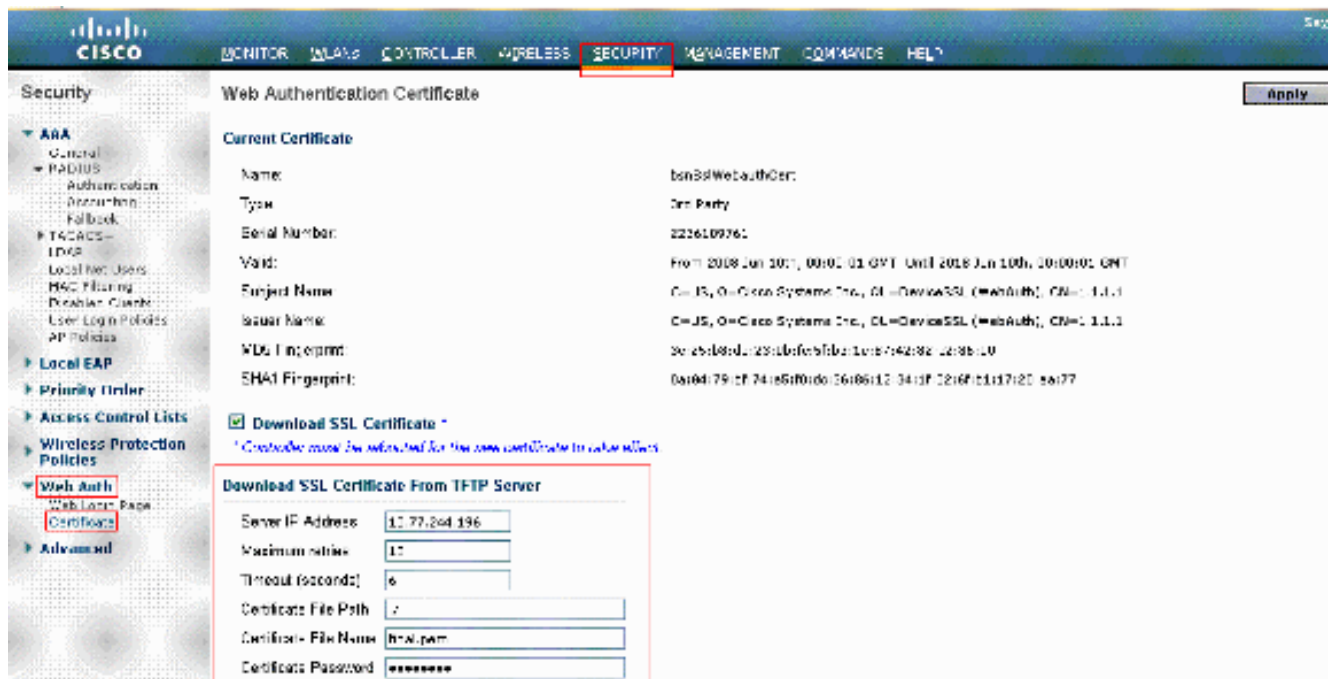
**Certificate installed.**  
Reboot the switch to use new certificate.

5. Reinicie el WLC para que los cambios tomen el efecto.

## Paso 3 GUI. Descargue el certificado de tercera persona al WLC con el GUI

Complete estos pasos para descargar el certificado encadenado al WLC con el GUI:

1. Copie el certificado final.pem del dispositivo al directorio de valor por defecto en su servidor TFTP.
2. Elija la **Seguridad > la red auténticas > CERT** para abrir la página del certificado de la autenticación Web.
3. Controle la casilla de verificación del **certificado de la transferencia directa SSL** para ver el certificado de la transferencia directa SSL de los parámetros del servidor TFTP.
4. En el campo del IP address, ingrese el IP address del servidor TFTP.



5. En el campo del trayecto del archivo, ingrese el trayecto del directorio del certificado.
6. En el campo de nombre del archivo, ingrese el nombre del certificado.

7. En el campo de contraseña del certificado, ingrese la contraseña que fue utilizada para proteger el certificado.
8. Haga clic en Apply (Aplicar).
9. Después de que la transferencia directa sea completa, elija los comandos > la **reinicialización > la reinicialización**.
10. Si está incitado para salvar sus cambios, haga clic la **salvaguardia y reinicie**.
11. Haga clic la **AUTORIZACIÓN** para confirmar su decisión para reiniciar el regulador.

## Troubleshooting

Qué presentará muy probablemente un problema es la instalación del certificado en el WLC. Para resolver problemas, abrir una línea de comando en el WLC y ingresar **ponga a punto la transferencia que toda activa y ponga a punto el pki P.M. activan** entonces completo el procedimiento del certificado de la transferencia directa.

```
(Cisco Controller) >transfer download start
```

```
Mode..... TFTP
Data Type..... Site Cert
TFTP Server IP..... 10.77.244.196
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /
TFTP Filename..... final.pem
```

This might take some time.

Are you sure you want to start? (y/N) **y**

TFTP EAP Dev cert transfer starting.

**Certificate installed.**

Reboot the switch to use new certificate.

Usted necesita verificar el formato del certificado y el encadenamiento después. Recuerde que WLCs que la versión 7.6 requiere más adelante el encadenamiento entero estar presente, así que usted puede no sólo cargar por teletratamiento su certificado WLC solamente. El encadenamiento hasta raíz CA debe estar presente en el fichero.

Aquí está un ejemplo de las depuraciones cuando el CA intermedio es incorrecto:

```
(Cisco Controller) >transfer download start
```

```
Mode..... TFTP
Data Type..... Site Cert
TFTP Server IP..... 10.77.244.196
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /
TFTP Filename..... final.pem
```

This might take some time.

Are you sure you want to start? (y/N) **y**

TFTP EAP Dev cert transfer starting.

**Certificate installed.**

Reboot the switch to use new certificate.

## Información Relacionada

- [Generación de CSR para Certificados de Terceros y Descarga de Certificados No Encadenados en el WLC](#)
- [Generación del pedido de firma de certificado \(CSR\) para un certificado de tercera persona en un sistema de control inalámbrico \(WCS\)](#)
- [Pedido de firma de certificado inalámbrico del sistema de control \(WCS\) \(CSR\) instalado en un ejemplo de la configuración de servidor Linux](#)
- [Soporte técnico y documentación - Cisco Systems](#)