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

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Certificados encadenados
Soporte para el certificado encadenado
Niveles del certificado
Paso 1. Genere un CSR
Opción A. CSR con el OpenSSL
Opción B. CSR Generated por el WLC
Paso 2. Consiga el certificado firmado
Opción A: Obtenga el archivo Final.pem de su empresa CA
Opción B: Obtenga el archivo Final.pem de 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 del Wireless LAN (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 Lightweight Access Point (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 del OpenSSL
- Public Key Infrastructure y Certificados digitales

Componentes Utilizados

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

- WLC de Cisco 5508 que funciona con la versión de firmware 8.3.102
- Aplicación del OpenSSL para Microsoft Windows
- Herramienta de la inscripción que es específica al Certification Authority (CA) de tercera persona

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 de CA de confianza. CA atestigua para la identidad en el certificado de peer cuando la firma. Si CA es uno que usted confía en, que es indicado por la presencia de una copia del certificado de 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 CA conocido 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 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.

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

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

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

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

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

- Encadenado
- Soltado
- Automóvil generado

Note: En la versión 7.6 y posterior del WLC, solamente los Certificados encadenados se soportan 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 de 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 el 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).

Opción A. CSR con el OpenSSL

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

Complete estos pasos para generar un CSR con el 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 del OpenSSL es la versión recomendada para las viejas versiones del WLC; sin embargo, a partir de la versión 7.5, el soporte para la versión 1.0 del OpenSSL también fue agregado (refiera al Id. de bug Cisco CSCti65315 - soporte de la necesidad para los Certificados generados usando el v1.0 del OpenSSL) y es la versión recomendada a utilizar. El OpenSSL 1.1 trabajos también fue probado y funciona increíble en y posterior las versiones del WLC 8.x.
2. Localice su archivo de configuración del OpenSSL y haga una copia de ella para editarla para este CSR. Edite 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: Soporte del WLCs un tamaño de clave máximo de 2,048 bits.

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

Note: Es importante que usted proporciona el Common Name correcto. Asegúrese de que el nombre del host que se utiliza para crear el certificado (Common Name) haga juego la entrada de nombre del 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 a la interfaz (VIP), usted debe reiniciar el sistema para que este cambio tome el efecto.
Aquí tiene 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 todos los detalles requeridos, se generan dos archivos:

   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 marcar 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 certificate generate CSR-webauth del >config (del WLC) **SEA TAC de Cisco mywebauthportal.wireless.com tac@cisco.com de Bruselas del BR**

```
-----COMIENCE EL PEDIDO DE CERTIFICADO-----
MIICqjCCAZICAQAwZTELMAkGA1UECAwCQllxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDBxteXdlYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NlZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OOjFGOGu
yNkgYefrrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafoovphlcXIElL2DSwVzjlbd9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
```

Wkc/wH4DyYdH7x5jzHc=
-----TERMINE EL PEDIDO DE CERTIFICADO-----

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

El certificate generate CSR-webadmin del >config (del WLC) **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 del WLC ni es posible salvarlo. Usted debe copiar/goma él a un archivo 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 el hardware del WLC después (RMA), usted no podrá reinstalar el mismo certificado que una nuevos clave y CSR tendrán que ser generados en el nuevo WLC.

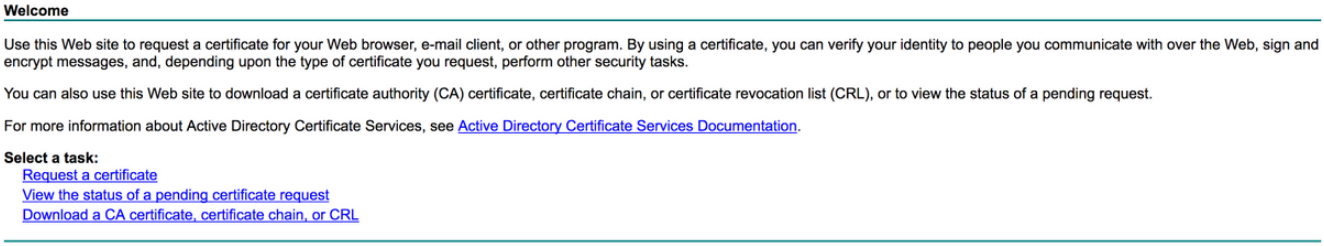
Usted entonces tiene que entregar este CSR a su autoridad de firma de tercera persona o a su Public Key Infrastructure (PKI) de la empresa.

Paso 2. Consiga el certificado firmado

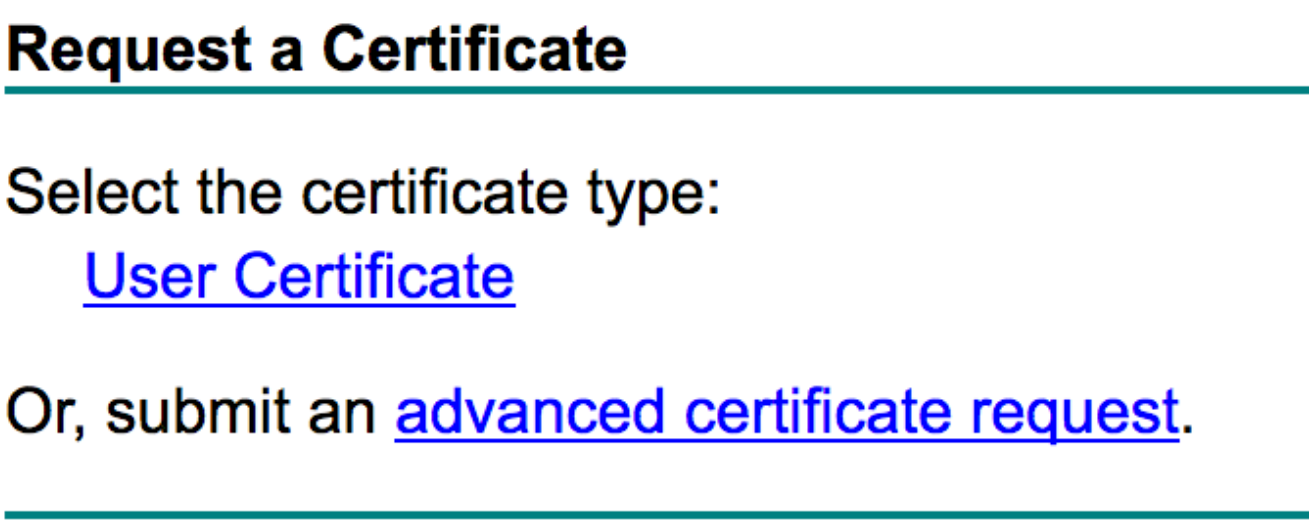
Opción A: Obtenga el archivo Final.pem de su empresa CA

Este ejemplo muestra solamente una empresa existente CA (Servidor Windows 2012 en este ejemplo) y no cubre los pasos para configurar a un Servidor Windows CA desde el principio.

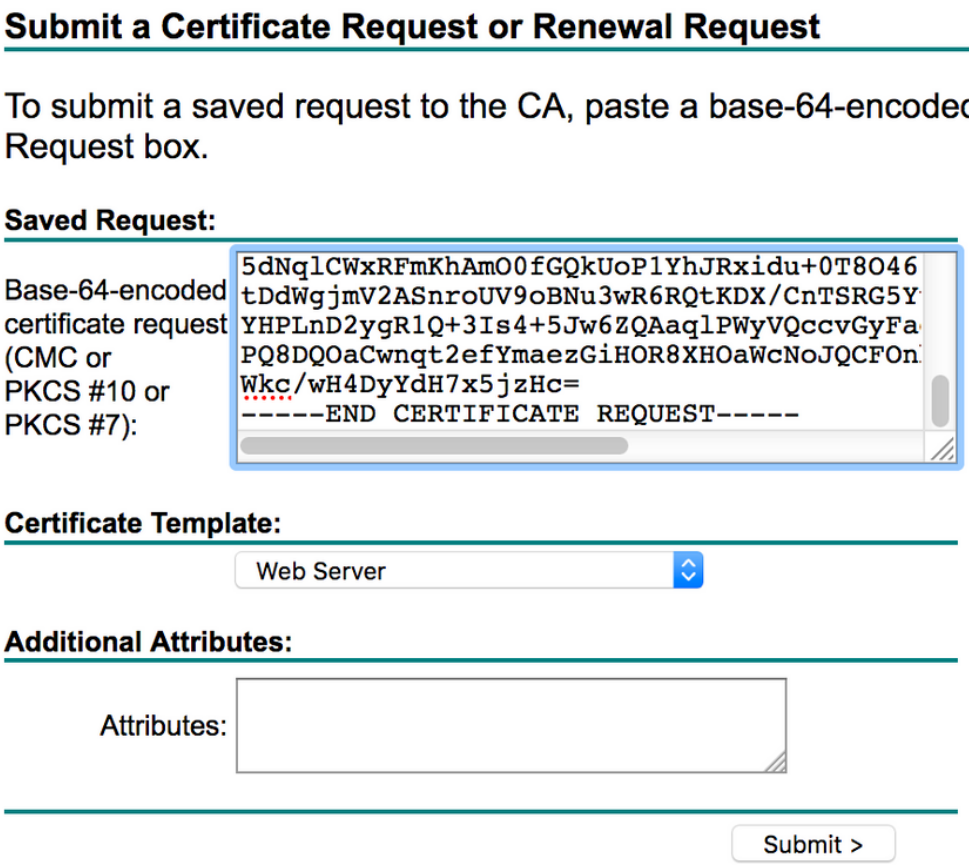
1. Va a su página de CA del enteprrise en el navegador (generalmente https:// <CA-ip>/certsrv) y hace clic la **petición un certificado**.



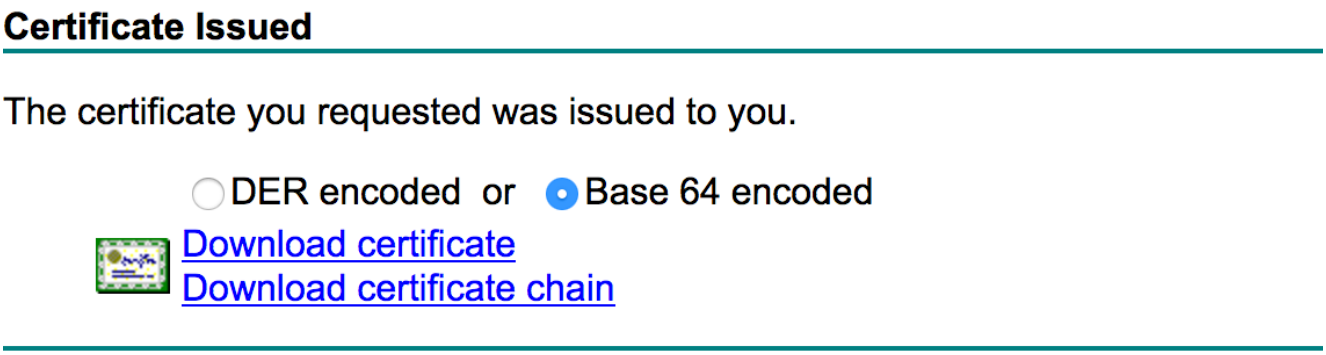
2. **Pedido de certificado avanzado del** tecleo.



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**.



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



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 - en 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 el OpenSSL para generar el CSR), y salva el archivo como final.pem**. Si usted** generó el CSR directamente del WLC (opción B) usted puede saltar este paso.

Publique estos comandos en la aplicación del OpenSSL para crear los archivos 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 archivo que usted debe descargar al WLC si usted siguió la “opción A. CSR con el OpenSSL”. Si usted siguió la “opción B. CSR generada por el WLC sí mismo”, después All-certs.pem es el archivo que usted debe descargar al WLC. El siguiente paso es descargar este archivo al WLC.

Note: Si la carga del certificado al WLC falla, puede ser que usted no tenga el encadenamiento entero en el archivo 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 archivo, después usted necesidad de descargar manualmente todo el intermedio y certificado raíz CA archivos y de añadirlos al final del fichero (por la goma de la copia sencilla) al archivo para crear el encadenamiento.

Opción B: Obtenga el archivo Final.pem de CA de tercera persona

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

   Después de que usted someta el CSR a CA de tercera persona, 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 de CA. Si usted tiene solamente un certificado intermedio como en este ejemplo, usted recibe estos tres Certificados de CA:

   Raíz certificate.pemCertificate.pem intermedioDispositivo certificate.pem**Note**: Aseegurese que el certificado es 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 archivo del .pem en otro archivo 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 archivo 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 el OpenSSL para generar el CSR), y salva el archivo como final.pem**. Si usted** generó el CSR directamente del WLC (opción B) usted puede saltar este paso.

   Publique estos comandos en la aplicación del OpenSSL para crear los archivos 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 archivo que usted debe descargar al WLC si usted siguió la “opción A. CSR con el OpenSSL”. Si usted siguió la “opción B. CSR generada por el WLC sí mismo”, después All-certs.pem es el archivo que usted debe descargar al WLC. El siguiente paso es descargar este archivo al WLC.

Note: SHA2 también se soporta. El Id. de bug Cisco CSCuf20725 es un pedido el soporte 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 **archivo final.pem al** directorio predeterminado en su servidor TFTP.
2. En el CLI, publique estos comandos para cambiar las configuraciones de la descarga:

```
    >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 archivo del .pem de modo que el sistema operativo pueda desencriptar 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 descarga y comenzar la descarga del certificado y de la clave. Aquí tiene 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

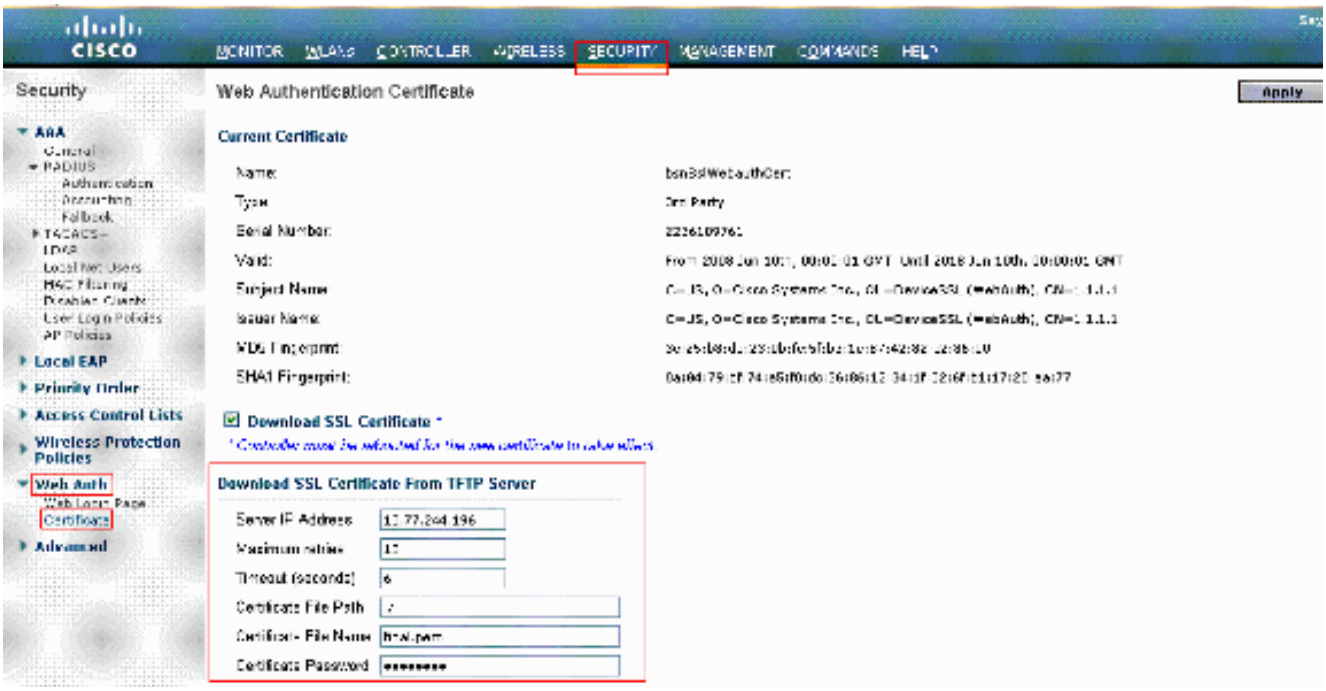
Complete estos pasos para descargar el certificado encadenado al WLC con el GUI:

1. Copie el certificado final.pem del dispositivo al directorio predeterminado en su servidor TFTP.

2. Elija el **auth de la Seguridad > de la red > el CERT** para abrir la página del certificado de la autenticación Web.

3. Marque la casilla de verificación del **certificado de la descarga SSL** para ver el certificado de la descarga 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 descarga sea completa, elija los **comandos > la reinicialización > la reinicialización**.

10. Si está indicado para salvar sus cambios, haga clic la **salvaguardia y reinicie**.

11. Haga Click en OK 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 la **transferencia toda del debug habilite** y el **pki del debug P.M. habilita** entonces completo el procedimiento del certificado de la descarga.

```
(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 el WLCs que la versión 7.6 requiere más adelante el encadenamiento entero estar presente, así que usted puede no sólo cargar su certificado del WLC solamente. El encadenamiento hasta raíz CA debe estar presente en el archivo.

Aquí está un ejemplo de los debugs cuando 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 configuración del servidor Linux
- Soporte Técnico y Documentación - Cisco Systems