Generación de CSR para certificados de terceros y descarga de certificados encadenados al WLC

Contenido

Introducción

Este documento describe cómo generar e importar certificados en WLC de AireOS.

Prerequisites

Requirements

Antes de intentar esta configuración, debe tener conocimiento de estos temas:

- Cómo configurar el WLC, el Lightweight Access Point (LAP) y la tarjeta cliente inalámbrica para el funcionamiento básico
- Cómo utilizar la aplicación OpenSSL
- Infraestructura de clave pública y certificados digitales

Componentes Utilizados

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

hardware.

- Cisco 5508 WLC que ejecuta la versión de firmware 8.3.102
- Aplicación OpenSSL para Microsoft Windows
- Herramienta de inscripción específica para la entidad emisora de certificados (CA) de terceros

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Certificados en cadena

Una cadena de certificados es una secuencia de certificados en la que cada certificado de la cadena está firmado por el certificado subsiguiente.

El propósito de una cadena de certificados es establecer una cadena de confianza de un certificado de peer a un certificado de CA de confianza. La CA realiza los vales para la identidad en el certificado de par cuando se firma.

Si la CA es de confianza (indicada por la presencia de una copia del certificado de CA en el directorio de certificados raíz), esto implica que también puede confiar en el certificado de peer firmado.

A menudo, los clientes no aceptan los certificados porque no fueron creados por una CA conocida. Normalmente, el cliente afirma que no se puede verificar la validez del certificado.

Este es el caso cuando el certificado está firmado por una CA intermedia, que no es conocida por el navegador cliente. En tales casos, es necesario utilizar un certificado SSL encadenado o un grupo de certificados.

Compatibilidad con certificado en cadena

El controlador permite que el certificado del dispositivo se descargue como certificado encadenado para la autenticación web.

Niveles de certificado

- Nivel 0 - Uso de solamente 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 único 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 certificados encadenados de más de 10KB de tamaño en el WLC. Sin embargo, esta restricción ha sido eliminada en la versión 7.0.230.0 del WLC y posterior.

> **Nota:** Los certificados en cadena son compatibles y se requieren de hecho para la autenticación web y el administrador web

Nota: Los certificados comodín son totalmente compatibles con EAP local, administración o autenticación web

Los certificados de autenticación Web pueden ser cualquiera de los siguientes:

- Encadenado
- Sin encadenar
- Generado automáticamente

Nota: En WLC versión 7.6 y posteriores, sólo se admiten certificados encadenados (y por lo tanto se requieren)

Para generar un certificado sin encadenar con fines de administración, este documento y ignorar las partes donde el certificado se combina con el certificado CA.

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

Paso 1. Generar una CSR

Existen dos formas de generar una CSR. Ya sea manualmente con OpenSSL (la única manera posible en el software WLC previo a 8.3) o en el propio WLC para generar el CSR (disponible después de 8.3.102).

Opción A. CSR con OpenSSL

Nota: Chrome versión 58 y posteriores no confía solamente en el Nombre común del certificado y requiere que el Nombre alternativo del sujeto también esté presente. En la siguiente sección se explica cómo agregar campos SAN a la CSR 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, de forma predeterminada, openssl.exe se encuentra en **C:\ > openssl > bin**.

   Nota: La versión 0.9.8 de OpenSSL es la versión recomendada para las versiones anteriores del WLC; sin embargo, a partir de la versión 7.5, también se agregó soporte para la versión 1.0 de OpenSSL (refiérase a Cisco bug ID CSCti65315 - Necesita soporte para los certificados generados con OpenSSL v1.0) y es la versión recomendada para usar. OpenSSL 1.1 también se probó y funciona en versiones 8.x y posteriores del WLC.
2. Busque su archivo de configuración de OpenSSL y haga una copia de él para editarlo para este CSR. Edite la copia para agregar las siguientes secciones :
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 por "DNS.1", "DNS.2" (etc.) deben contener todos los nombres alternativos de los certificados. Luego escriba cualquier URL posible utilizada para el WLC. Las líneas en negrita del ejemplo anterior no estaban presentes o se comentaron en nuestra versión de laboratorio openSSL. Puede variar considerablemente con la versión de sistemas operativos y de OpenSl. Guardamos esta versión modificada de la configuración como **openssl-san.cnf** para este ejemplo.

4. Ingrese este comando para generar una nueva CSR:

```
OpenSSL>req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
```

Nota: Los WLC soportan un tamaño máximo de clave de 4096 bits a partir de la versión de software 8.5

5. Hay un mensaje para obtener información: nombre del país, estado, ciudad, etc. Proporcione la información requerida.

Nota: Es importante proporcionar el nombre común correcto. Asegúrese de que el nombre de host que se utiliza para crear el certificado (Nombre común) coincida con la entrada de nombre de host del Sistema de nombres de dominio (DNS) para la dirección IP de la interfaz virtual en el WLC y que el nombre también exista en el DNS. Además, después de realizar el cambio a la interfaz IP virtual (VIP), debe reiniciar el sistema para que este cambio surta efecto.

Aquí tiene un ejemplo:

```
OpenSSL>req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
Loading 'screen' into random state - done
Generate a 1024 bit RSA private key
.....................................................................++++++
.................................................++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that is 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 is a default value,
If you enter '.', the field is 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 []:(email address)

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Test123
An optional company name []:OpenSSL>
```

6. Puede verificar el CSR (especialmente para los atributos SAN presencE) con **openssl req -text -noout -in csrfilename**
7. Después de proporcionar todos los detalles necesarios, se generan dos archivos:

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

Opción B. CSR generado por el WLC

Si su WLC ejecuta la versión de software 8.3.102 o posterior, la opción más segura es utilizar el WLC para generar el CSR. La ventaja es que la clave se genera 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 SAN en el CSR, lo que se sabe que conduce a problemas con ciertos exploradores que requieren la presencia de un atributo SAN. Algunas CA permiten insertar campos SAN en el momento de la firma, por lo que es una buena idea consultar con su CA.

La generación CSR por el propio WLC utiliza un tamaño de clave de 2048 bits y el tamaño de clave ecdsa es de 256 bits.

> **Nota:** Si usted ejecuta el comando de generación csr y no instala el certificado subsiguiente todavía, su WLC se representa completamente inalcanzable en HTTPS en el siguiente reinicio, ya que el WLC utiliza la clave CSR recién generada después del reinicio pero no tiene el certificado que lo acompaña.

Para generar una CSR para la autenticación web, ingrese este comando:

(WLC) >**El certificado de configuración genera csr-webauth BE BR Bruselas Cisco TAC mywebauthportal.wireless.com tac@cisco.com**
—INICIAR SOLICITUD DE CERTIFICADO—
MIICqjCCAZICAQAwZTELMAkGA1UECAwCQlIxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDBxteXdlYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdiI0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NlZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OOjFGOGu
NkgYefrrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K

ZvEpAafoovphlcXIElL2DSwVzjlbd9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc=
—SOLICITUD DE CERTIFICADO FINAL—

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

(WLC) **>El certificado de configuración genera csr-webadmin BE BR Bruselas Cisco TAC mywebauthportal.wireless.com tac@cisco.com**

> **Nota:** El CSR se imprime en el terminal después de ingresar el comando. No hay otras maneras de recuperarlo; no es posible cargarlo desde el WLC ni es posible guardarlo. Debe copiarlo/pegarlo en un archivo del equipo después de ingresar el comando. La clave generada permanece en el WLC hasta que se genera la próxima CSR (la clave se sobrescribe). Si alguna vez tiene que cambiar el hardware del WLC más adelante (RMA), no podrá reinstalar el mismo certificado que una nueva clave y CSR se genera en el nuevo WLC.

a

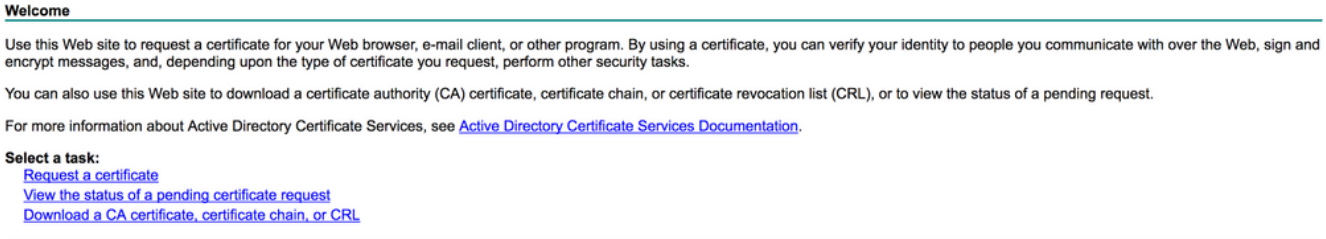
A continuación, debe entregar esta CSR a su autoridad de firma de terceros o a su infraestructura de clave pública (PKI) empresarial.

Paso 2. Obtener el certificado firmado

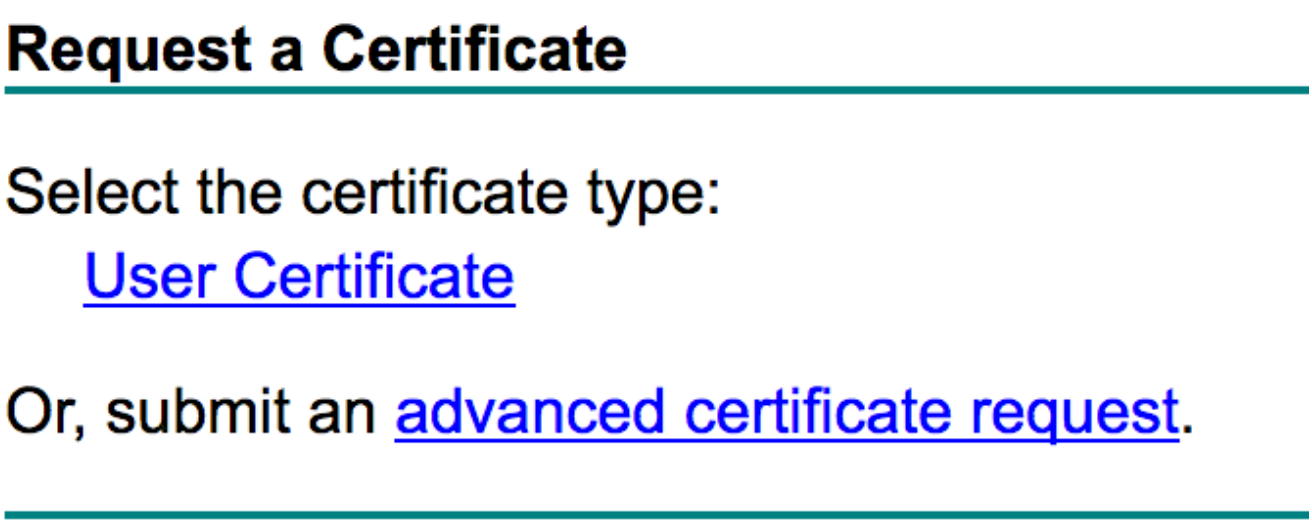
Opción A: Obtenga el archivo Final.pem de su CA empresarial

Este ejemplo sólo muestra una CA empresarial actual (Windows Server 2012 en este ejemplo) y no describe los pasos para configurar una CA de Windows Server desde el principio.

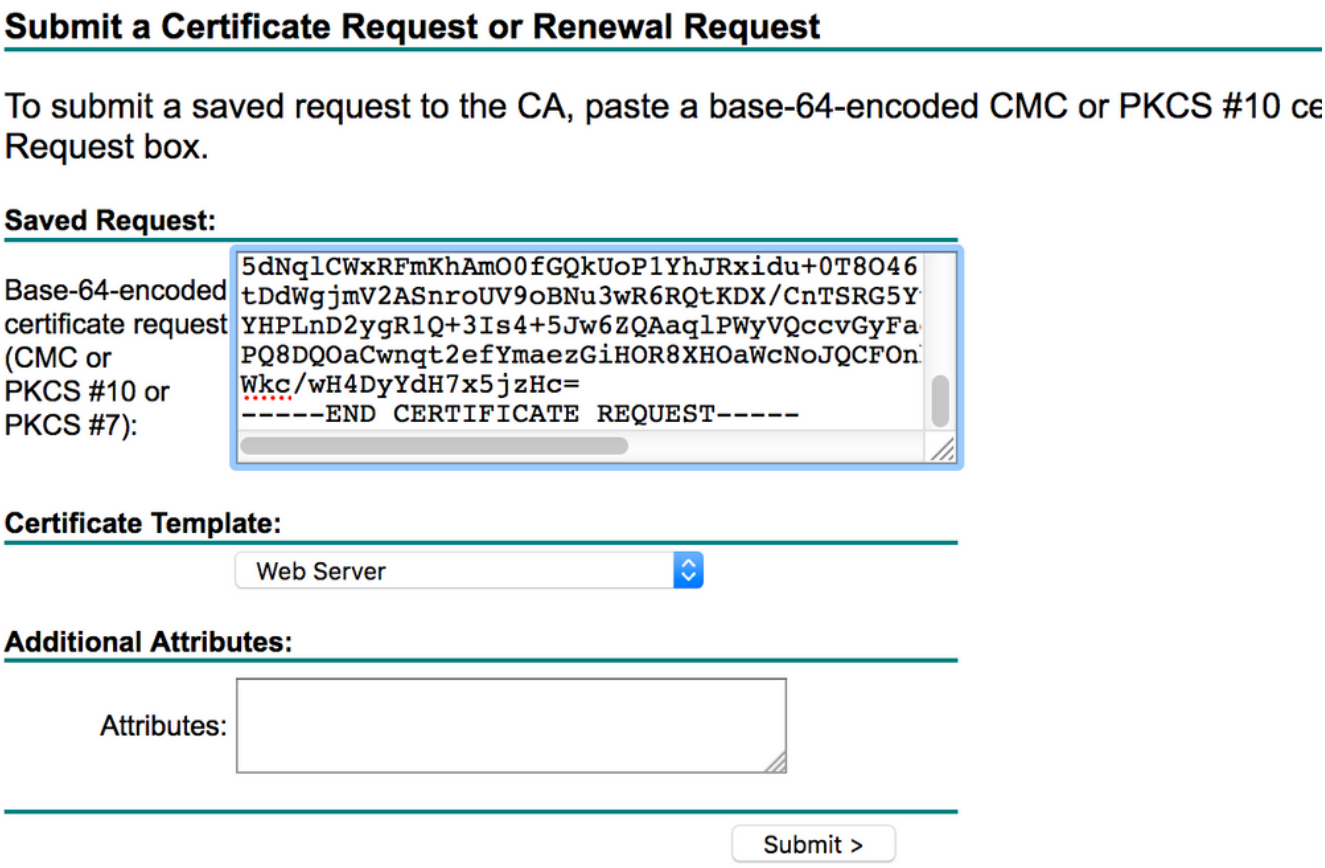
1. Vaya a la página de CA de su empresa en el explorador (normalmente https://<CA-ip>/certsrv) y haga clic en **Request a certificate**.



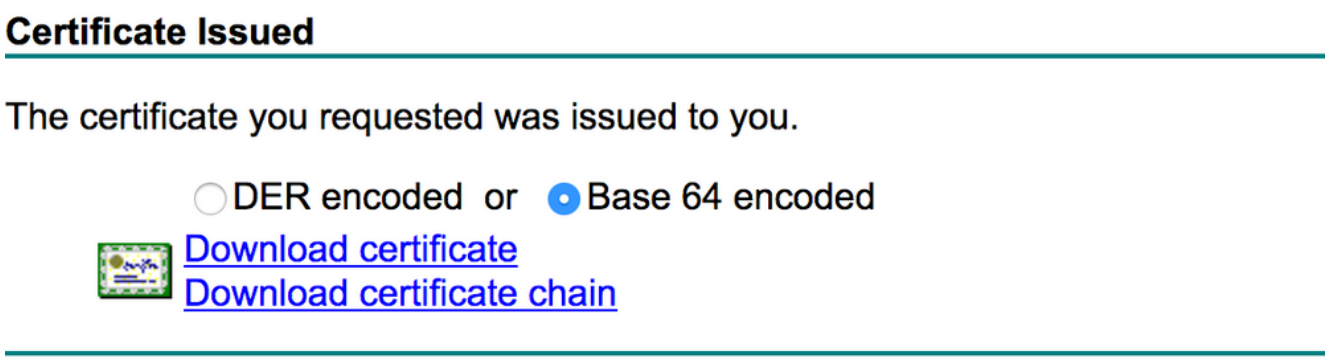
2. Haga clic **advanced certificate request**.



3. Introduzca la CSR que obtuvo del WLC o OpenSSL. En la lista desplegable Plantilla de certificado, elija **Web Server**.



4. Haga clic en el **Base 64 encoded**botón de opción.



5. Si el certificado descargado es del tipo PKCS7 (.p7b), conviértalo a PEM (en el siguiente ejemplo, la cadena de certificados se descargó como nombre de archivo "All-certs.p7b"):

openssl pkcs7 -print_certs -in All-certs.p7b -out All-certs.pem

6. Combine los certificados de cadena de certificados (en este ejemplo, se denomina "All-certs.pem") con la clave privada que se generó junto con la CSR (la clave privada del certificado del dispositivo, que es mykey.pem en este ejemplo) si se utilizó la opción A (OpenSSL para generar la CSR), y guarde el archivo como **final.pem**. Si generó el CSR directamente desde el WLC (opción B), omita este paso.

Ingrese estos comandos en la aplicación 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
```

> **Nota:** En este comando, debe ingresar una contraseña para los parámetros **-passin** y **-passout**. La contraseña que se configura para el parámetro **-passout debe coincidir con el parámetro certpassword** que se configura en el WLC. En este ejemplo, la contraseña que se configura para los parámetros **-passin** y **-passout es check123**.

Final.pem es el archivo que se descargará al WLC si siguió "Opción A. CSR con OpenSSL".

Si siguió la opción B. CSR generado por el propio WLC", luego All-certs.pem es el archivo para descargar al WLC. El siguiente paso es descargar este archivo al WLC.

> **Nota:** Si la carga del certificado al WLC falla, verifique que haya toda la cadena en el archivo pem. Consulte el paso 2 de la opción B (obtenga el archivo final.pem de una CA de terceros) para ver cómo debe ser. Si sólo ve un certificado en el archivo, debe descargar manualmente todos los archivos de certificados de CA intermedia y raíz y anexarlos

(mediante copia simple y pegar) al archivo para crear la cadena.

Opción B: Obtenga el archivo Final.pem de una CA de terceros

1. Copie y pegue la información de CSR en cualquier herramienta de inscripción de CA.

   Después de enviar el CSR a la CA de terceros, la CA de terceros firma digitalmente el certificado y devuelve la cadena de certificados firmada por correo electrónico. En el caso de los certificados encadenados, recibe toda la cadena de certificados de la CA. Si sólo tiene un certificado intermedio como en este ejemplo, recibe estos tres certificados de la CA:

   Root certificate.pemCertificado intermedio.pemDevice certificate.pem**Nota:** Asegúrese de que el certificado es compatible con Apache con el cifrado Secure Hash Algorithm 1 (SHA1).
2. Una vez que tenga los tres certificados, copie y pegue el contenido de cada archivo .pem en otro archivo en este orden:

```
------BEGIN CERTIFICATE------
*Device cert*
------END CERTIFICATE------
------BEGIN CERTIFICATE------
*Intermediate CA cert *
------END CERTIFICATE--------
------BEGIN CERTIFICATE------
*Root CA cert *
------END CERTIFICATE------
```

3. Guarde el archivo como **All-certs.pem**.

4. Combine el certificado All-certs.pem con la clave privada que se generó junto con el CSR (la clave privada del certificado del dispositivo, que es mykey.pem en este ejemplo) si utilizó la opción A (OpenSSL para generar el CSR) y guarde el archivo como **final.pem**. Si generó el CSR directamente desde el WLC (opción B), omita este paso.

   Ingrese estos comandos en la aplicación 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
```

   Nota: En este comando, debe ingresar una contraseña para los parámetros **-passin** y **-passout**. La contraseña que se configura para el parámetro **-passout debe coincidir con el parámetro certpassword** que se configura en el WLC. En este ejemplo, la contraseña que se configura para los parámetros **-passin** y **-passout es check123**.Final.pem es el archivo que se descargará al WLC si siguió "Opción A. CSR con OpenSSL". Si siguió la opción B. CSR generado por el propio WLC", luego All-certs.pem es el archivo que debe descargar al WLC. El siguiente paso es descargar este archivo al WLC.

Nota: También se admite SHA2. El Id. de bug Cisco CSCuf20725 es una solicitud para el soporte de SHA512.

Paso 3 CLI. Descargue el certificado de terceros al WLC con la CLI

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

1. Mueva el archivo **final.pem** al directorio predeterminado en su servidor TFTP.

2. En la CLI, ingrese estos comandos para cambiar la configuración de descarga:

```
    >transfer download mode tftp
>transfer download datatype webauthcert
>transfer download serverip
```

```
>transfer download path
```

```
>transfer download filename final.pem
```

3. Introduzca la contraseña del archivo .pem para que el sistema operativo pueda descifrar la clave SSL y el certificado.

```
>transfer download certpassword password
```

Nota: Asegúrese de que el valor para **certpassword** sea el mismo que la contraseña del parámetro **-passout establecida en el Paso 4 (o 5) de la** sección Generar un CSR. En este ejemplo, la **certpassword** debe ser **check123**. Si ha elegido la opción B (es decir, use el WLC mismo para generar el CSR), deje el campo certpassword en blanco.

4. Ingrese el comando **transfer download start** para ver la configuración actualizada. Luego ingrese **y** en el prompt para confirmar la configuración de descarga actual e iniciar la descarga del certificado y 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 start.

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

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

GUI del paso 3. Descargue el certificado de terceros al WLC con la GUI

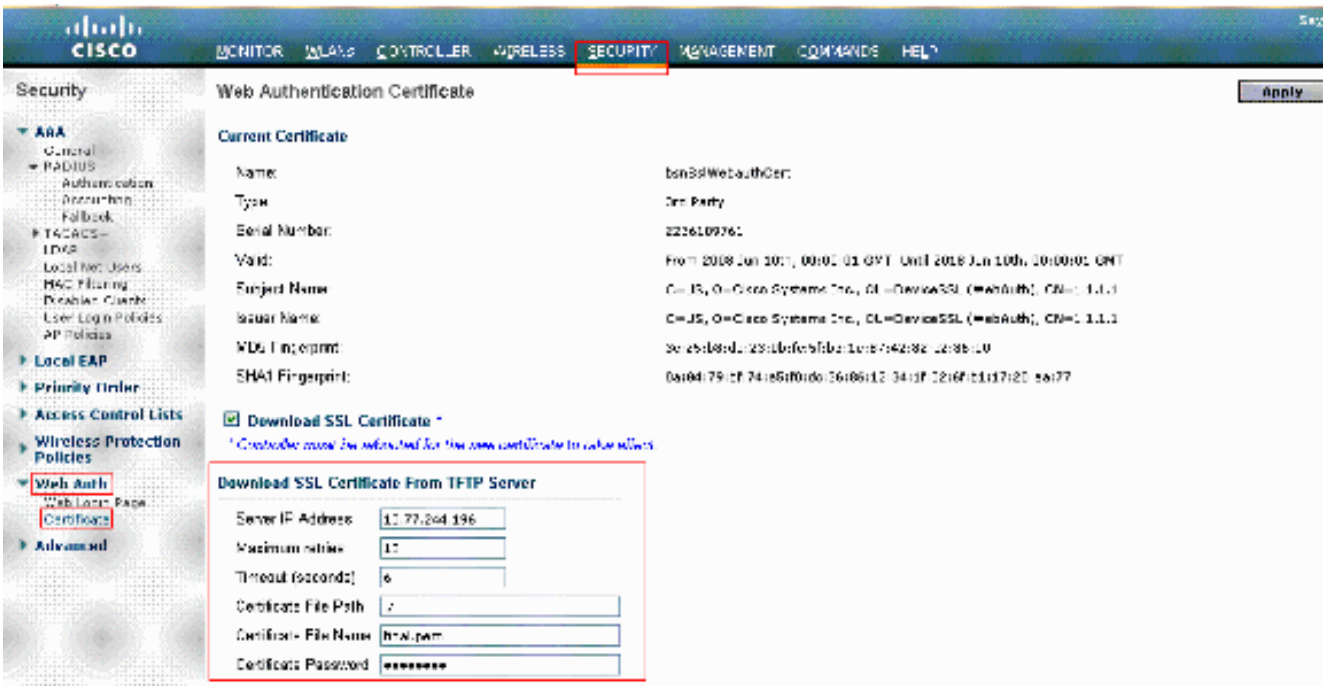
Complete estos pasos para descargar el certificado encadenado al WLC con la GUI:

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

2. Elegir **Security > Web Auth > Cert** para abrir la página Certificado de autenticación Web.

3. Compruebe el **Download SSL Certificate**para ver los parámetros Download SSL Certificate From TFTP Server.

4. En el campo IP Address (Dirección IP), introduzca la dirección IP del servidor TFTP.



5. En el campo Ruta de archivo, introduzca la ruta de acceso del directorio del certificado.

6. En el campo Nombre de archivo, introduzca el nombre del certificado.

7. En el campo Contraseña del certificado, introduzca la contraseña que se utilizó para proteger el certificado.

8. Haga clic **Apply**.

9. Una vez finalizada la descarga, seleccione **Commands > Reboot > Reboot**.

10. Si se le solicita que guarde los cambios, haga clic en **Save and Reboot**.

11. Haga clic en **Aceptar** para confirmar su decisión de reiniciar el controlador.

Troubleshoot

Para resolver el problema de la instalación del certificado en el WLC, abra una línea de comandos en el WLC e ingrese **debug transfer all enable** y **debug pm pki enable** luego complete el procedimiento del certificado de descarga.

```
In some cases, the logs only say that the certificate installation failed:
*TransferTask: Sep 09 08:37:17.415: RESULT_STRING: TFTP receive complete... Installing
Certificate.
*TransferTask: Sep 09 08:37:17.415: RESULT_CODE:13

TFTP receive complete... Installing Certificate.
*TransferTask: Sep 09 08:37:21.418: Adding cert (1935 bytes) with certificate key password.
*TransferTask: Sep 09 08:37:21.421: RESULT_STRING: Error installing certificate.
```

Verifique el formato y la cadena del certificado. Recuerde que los WLC posteriores a la versión 7.6 requieren que toda la cadena esté presente, por lo que no puede cargar su certificado WLC solo. La cadena hasta la CA raíz debe estar presente en el archivo.

Este es un ejemplo de depuraciones cuando la CA intermedia es incorrecta :

```
*TransferTask: Jan 04 19:08:13.338: Add WebAuth Cert: Adding certificate & private key using
password check123
*TransferTask: Jan 04 19:08:13.338: Add ID Cert: Adding certificate & private key using password
check123
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Adding certificate (name:
bsnSslWebauthCert) to ID table using password check123
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Decoding PEM-encoded Certificate
(verify: YES)
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking
string length instead
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length 7148 & VERIFY
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification return
code: 0
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification result
text: unable to get local issuer certificate
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: Error in X509 Cert Verification at
0 depth: unable to get local issuer certificate
*TransferTask: Jan 04 19:08:13.343: Add Cert to ID Table: Error decoding (verify: YES) PEM
certificate
*TransferTask: Jan 04 19:08:13.343: Add ID Cert: Error decoding / adding cert to ID cert table
(verifyChain: TRUE)
*TransferTask: Jan 04 19:08:13.343: Add WebAuth Cert: Error adding ID cert
```

Consideraciones sobre alta disponibilidad (HA SSO)

Como se explica en la guía de implementación de SSO HA del WLC, los certificados no se replican del controlador primario al secundario en un escenario de SSO HA.

Esto significa que debe importar todos los certificados al secundario antes de formar el par HA.

Otra advertencia es que esto no funciona si generó la CSR (y por lo tanto creó la clave localmente) en el WLC primario porque esa clave no se puede exportar.

La única manera es generar el CSR para el WLC primario con OpenSSL (y por lo tanto tener la clave conectada al certificado) e importar esa combinación de certificado/clave en ambos WLC.

Información Relacionada

- Generación de CSR para Certificados de Terceros y Descarga de Certificados No Encadenados en el WLC
- Generación de solicitud de firma de certificado (CSR) para un certificado de terceros en un sistema de control inalámbrico (WCS)
- Ejemplo de Configuración de la Solicitud de firma de certificados (CSR) de Wireless Control System (WCS) instalado en un servidor Linux
- Soporte Técnico y Documentación - Cisco Systems
- Guía WLC HA SSO