Configuración del servicio HTTP/HTTPS y generación del certificado de capa de socket seguro (SSL) en los puntos de acceso WAP551 y WAP561

Objetivo

El punto de acceso se puede administrar a través de conexiones HTTP y HTTP Secure (HTTPS) cuando se configuran los servidores HTTP/HTTPS. El protocolo de transferencia de hipertexto seguro (HTTPS) es un protocolo de transferencia más seguro que HTTP. Un punto de acceso debe tener un certificado SSL válido para utilizar el servicio HTTPS. Un certificado SSL es un certificado firmado digitalmente por una autoridad certificadora que permite al navegador web tener una comunicación cifrada segura con el servidor web.

En este artículo se explica cómo configurar el servicio HTTP/HTTPS y cómo crear un certificado de capa de socket seguro (SSL) en los puntos de acceso WAP551 y WAP561.

Dispositivos aplicables

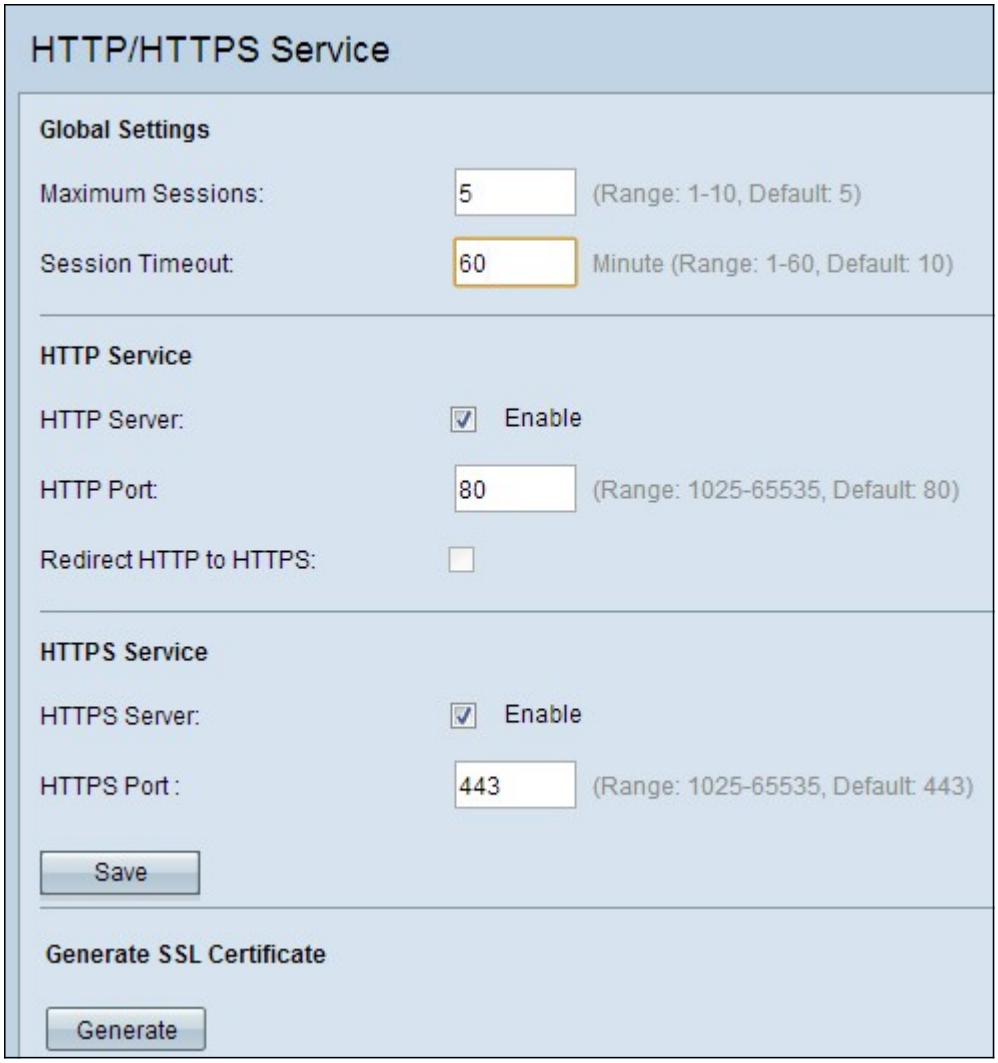
·WAP551
· WAP561

Versión del software

•1.1.0.4

Configuración del servicio HTTP/HTTPS

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Administration > HTTP/HTTPS Service**. Se abre la página *Servicio HTTP/HTTPS*:



Paso 2. Introduzca el número máximo de sesiones web en el campo Número máximo de sesiones. Esto significa el número máximo de usuarios que se pueden iniciar sesión en la utilidad de configuración web.

Paso 3. En el campo Session Timeout (Tiempo de espera de sesión), introduzca el tiempo máximo que un usuario inactivo puede permanecer conectado a la utilidad de configuración web de AP.

Paso 4. Marque la casilla de verificación **Enable** del servidor HTTP para habilitar el acceso web a través de HTTP. El servidor HTTP está habilitado de forma predeterminada.

Nota: Si el servidor HTTP está desactivado, las conexiones actuales que utilizan HTTP se desconectan.

Paso 5. En el campo Puerto HTTP, introduzca el número de puerto que se utilizará para las conexiones HTTP. El puerto número 80 se utiliza habitualmente para las conexiones HTTP.

Paso 6. (Opcional) Si desea redirigir los intentos de acceso HTTP de administración en el puerto HTTP al puerto HTTPS, marque la casilla de verificación **Redirigir HTTP a HTTPS**. Este campo solo está disponible para activarlo cuando el acceso HTTP está desactivado.

Paso 7. Marque la casilla de verificación **Enable** del servidor HTTPS para habilitar el acceso web a través de HTTPS. El servidor HTTPS está habilitado de forma predeterminada.

Nota: Si el servidor HTTPS está desactivado, las conexiones actuales que utilizan HTTPS se desconectan.

Paso 8. Introduzca el número de puerto que se utilizará para las conexiones HTTPS en el campo Puerto HTTPS. El número de puerto predeterminado 443 se utiliza normalmente con HTTPS.

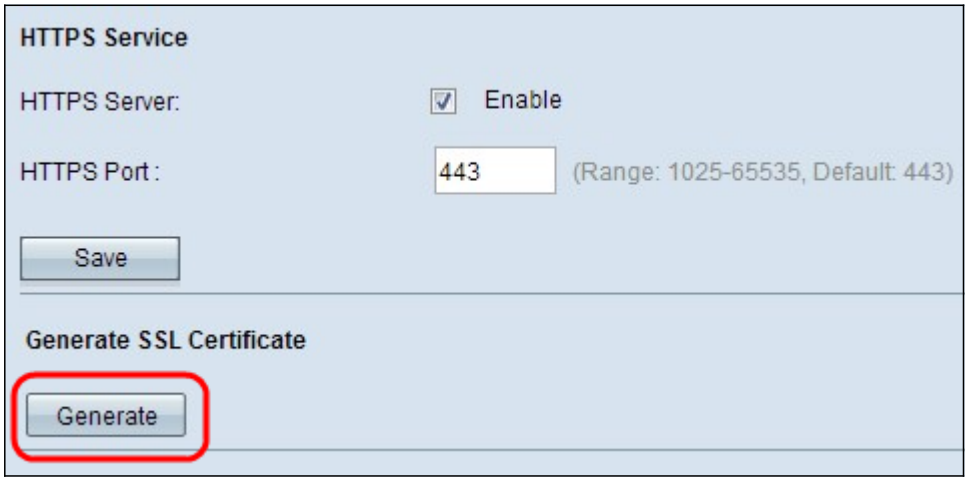
Paso 9. Haga clic en **Guardar para guardar la configuración.**

Configuración de certificados SSL

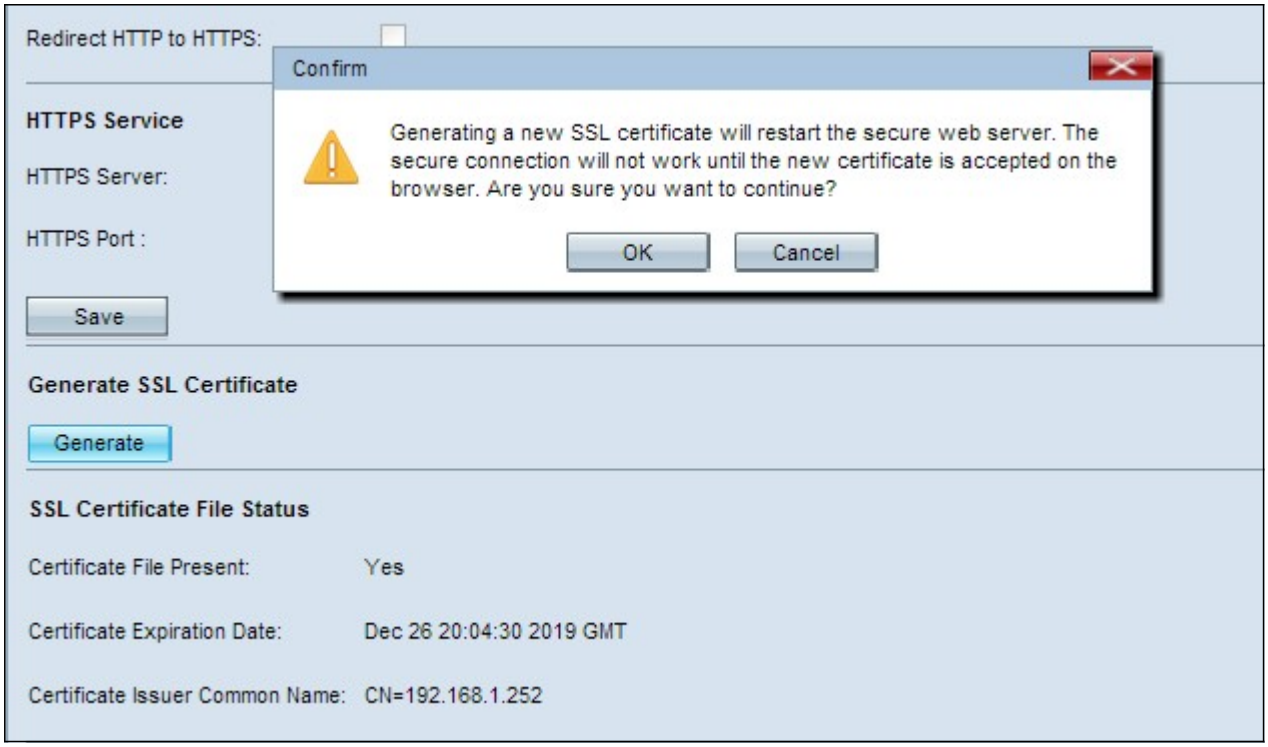
Puede descargar un certificado SSL a través de un navegador web HTTP/HTTPS o desde un servidor TFTP, utilizar el punto de acceso para generar un certificado SSL o cargar un certificado SSL desde su equipo. En esta sección, se describen los diferentes métodos para instalar un certificado SSL.

Generación de un certificado SSL

El nuevo certificado HTTP SSL para el servidor web seguro se debe generar después de que el punto de acceso (AP) haya adquirido una dirección IP de modo que el nombre común del certificado coincida con la dirección IP del AP. La generación de un nuevo certificado SSL reinicia el servidor web seguro. La conexión segura no funciona hasta que se acepte el nuevo certificado en el navegador.



Paso 1. Haga clic en **Generar** para generar un nuevo certificado SSL. Aparecerá una ventana de confirmación.



Paso 2. Haga clic en **Aceptar** para continuar con la generación del certificado SSL. Una vez generado el certificado, el área SSL Certificate File Status muestra la siguiente información:

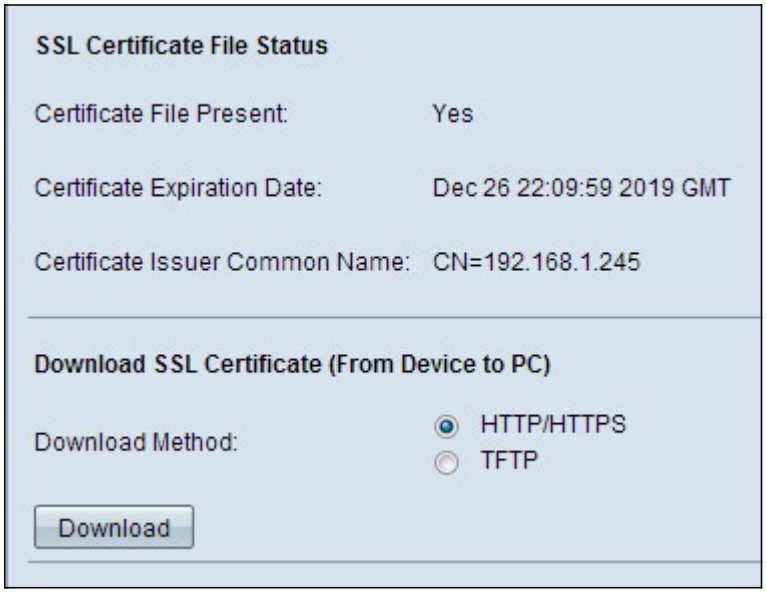
·archivo de certificado presente: indica si el archivo de certificado SSL HTTP está presente o no.

Fecha de vencimiento · certificado: muestra la fecha de vencimiento del certificado HTTP SSL actual.

Nombre común del emisor de certificados ·: muestra el nombre común del emisor de certificados actual.

Descargue el certificado SSL

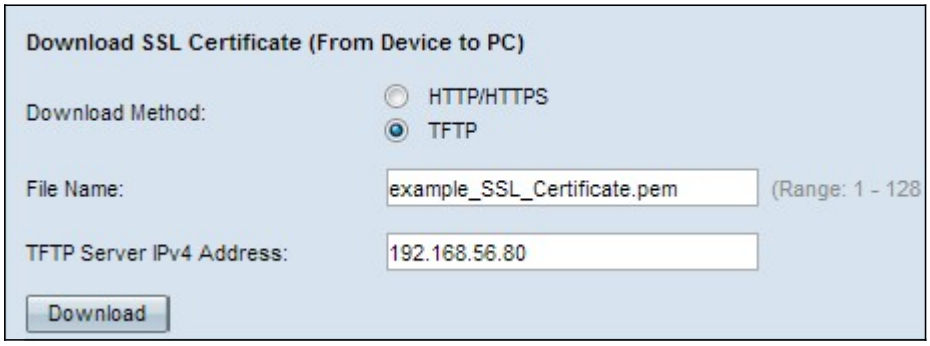
Los siguientes pasos describen cómo descargar el certificado SSL (un archivo .pem) del dispositivo al equipo como copia de seguridad.



Paso 1. Haga clic en el botón de opción correspondiente al método de descarga deseado en el área Descargar certificado SSL.

·HTTP/HTTPS: permite descargar el certificado SSL de un servidor web. Vaya al paso 4 si elige HTTP/HTTPS.

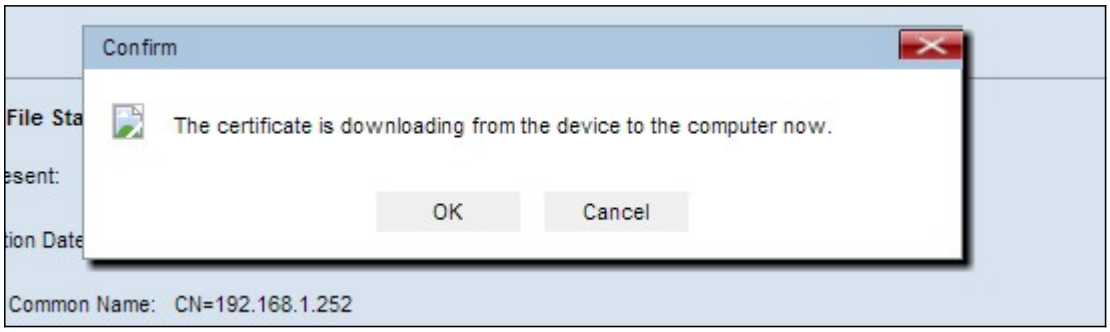
·TFTP: permite descargar el certificado SSL desde un servidor TFTP. Si elige esta opción, aparecen los campos Nombre de archivo y Dirección IPv4 del servidor TFTP.



Paso 2. Si selecciona TFTP en el Paso 1, introduzca el nombre de archivo en el campo Nombre de archivo. Se trata de un archivo de tipo de certificado con una extensión .pem.

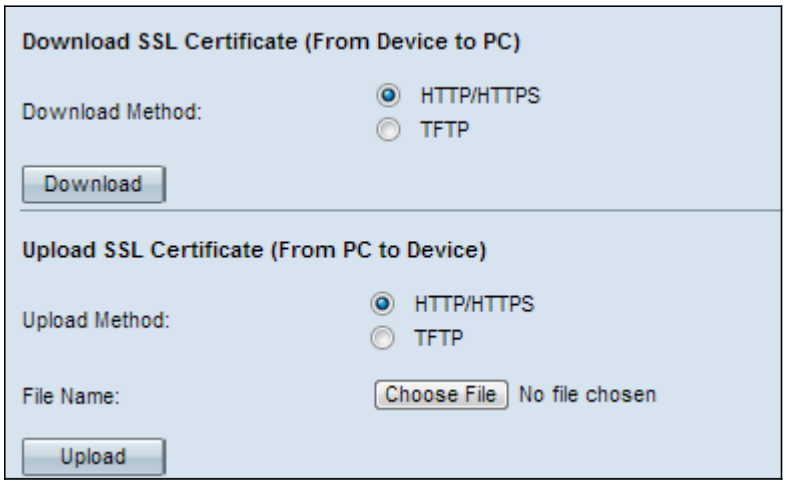
Paso 3. Si eligió TFTP en el Paso 1, ingrese la dirección IP del servidor TFTP en el campo TFTP Server IPv4 Address .

Paso 4. Haga clic en **Download** para descargar el archivo de certificado. Aparecerá una ventana de confirmación.



Paso 5. Haga clic en **Aceptar** para continuar con la descarga.

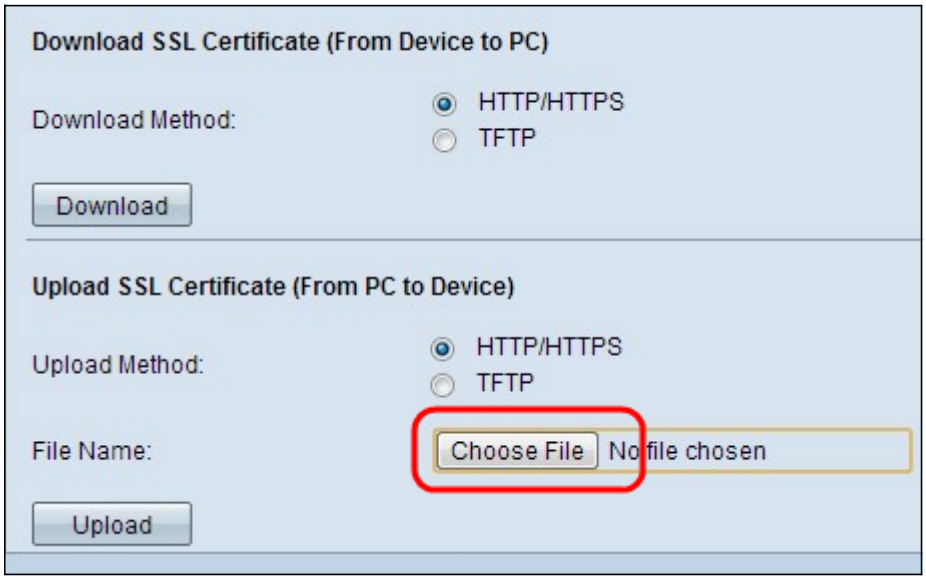
Cargar el certificado SSL



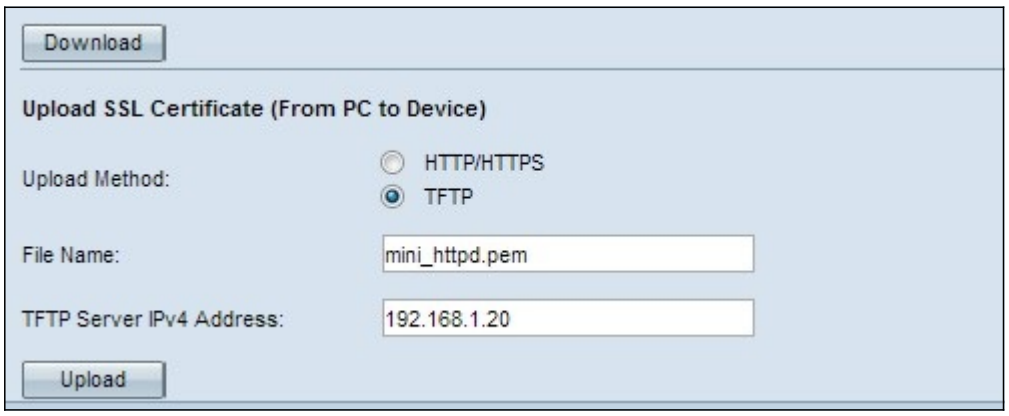
Paso 1. Haga clic en el botón de opción HTTP/HTTPS o TFTP para elegir el método de carga deseado en el área Cargar certificado SSL.

·HTTP/HTTPS: permite cargar el certificado con un servidor web. Si selecciona HTTP/HTTPS, complete el paso 2 y, a continuación, omita el paso 3.

·TFTP: Esto permite que el certificado SSL se cargue a través de un servidor TFTP. Si selecciona esta opción, aparecen los campos Nombre de archivo y Dirección IPv4 del servidor TFTP. Omita el paso 2 y realice el paso 3.

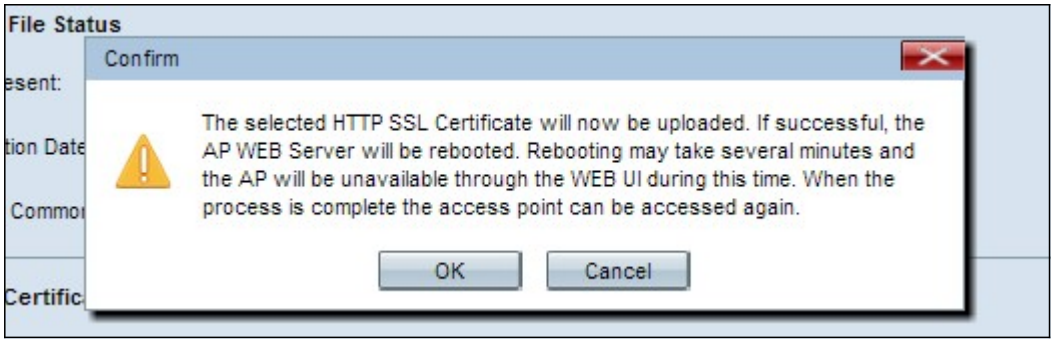


Paso 2. Haga clic en **Elegir archivo** para examinar y seleccionar el archivo.



Paso 3. Introduzca el nombre de archivo en el campo File Name (Nombre de archivo) y la dirección del servidor TFTP en el campo TFTP Server IPv4 Address (Dirección IPv4 del servidor TFTP).

Paso 4. Haga clic en **Cargar** para cargar el archivo de certificado. Aparecerá una ventana de confirmación.



Paso 5. Haga clic en **Aceptar** para continuar con la carga.