

Configuración de servicio HTTP/HTTPS y generación de certificado del Secure Socket Layer (SSL) en los Puntos de acceso WAP551 y WAP561

Objetivo

El Punto de acceso se puede manejar a través de las conexiones seguras HTTP y HTTP (HTTPS) cuando se configuran los servidores HTTP/HTTPS. El protocolo hyper text transfer seguro (HTTPS) es un protocolo transfer más seguro que el HTTP. Un Punto de acceso debe tener un certificado válido SSL para utilizar el servicio HTTPS. Un certificado SSL es un certificado firmado digitalmente por una autoridad de certificación que permita que el buscador Web tenga una comunicación encriptada segura con el servidor Web.

Este artículo explica cómo configurar el servicio HTTP/HTTPS y cómo crear un certificado del Secure Socket Layer (SSL) en los Puntos de acceso WAP551 y WAP561.

Dispositivos aplicables

- WAP551
- WAP561

Versión de software

- 1.1.0.4

Configuración del servicio HTTP/HTTPS

Paso 1. Ábrase una sesión a la utilidad de configuración de la red y elija la **administración > el servicio HTTP/HTTPS**. La página del *servicio HTTP/HTTPS* se abre:

HTTP/HTTPS Service

Global Settings

Maximum Sessions: (Range: 1-10, Default: 5)

Session Timeout: Minute (Range: 1-60, Default: 10)

HTTP Service

HTTP Server: Enable

HTTP Port: (Range: 1025-65535, Default: 80)

Redirect HTTP to HTTPS:

HTTPS Service

HTTPS Server: Enable

HTTPS Port: (Range: 1025-65535, Default: 443)

Generate SSL Certificate

Paso 2. Ingrese el número máximo de sesiones de la red en el campo de las sesiones máximas. Esto significa la cantidad máxima de usuario que se puede abrir una sesión a la utilidad de configuración de la red.

Paso 3. En el campo del tiempo de espera de la sesión, ingrese la cantidad máxima de tiempo que un usuario inactivo puede seguir abierto una sesión a la utilidad de configuración de la red AP.

Paso 4. Controle la casilla de verificación del **permiso del** servidor HTTP para activar el Acceso Web vía el HTTP. El servidor HTTP se activa por abandono.

Nota: Si se inhabilita el servidor HTTP, cualquier conexión actual que utilice el HTTP es disconnected.

Paso 5. En el campo de puerto HTTP, ingrese el número del puerto para utilizar para las conexiones HTTP. El número del puerto 80 es de uso general para las conexiones HTTP.

Paso 6. (opcional) si usted desea reorientar los intentos de acceso de la Administración HTTP en el puerto HTTP al control del puerto HTTPS la **reorientación HTTP a casilla de verificación HTTPS**. Este campo está disponible activar solamente cuando se inhabilita el acceso HTTP.

Paso 7. Controle la casilla de verificación del **permiso del** servidor HTTPS para activar el Acceso Web vía el HTTPS. Activan al servidor HTTPS por abandono.

Nota: Si inhabilitan al servidor HTTPS, cualquier conexión actual que utilice el HTTPS es

disconnected.

Paso 8. Ingrese el número del puerto para utilizar para las conexiones HTTPS en el campo de puerto HTTPS. El puerto predeterminado número 443 se utiliza típicamente con el HTTPS.

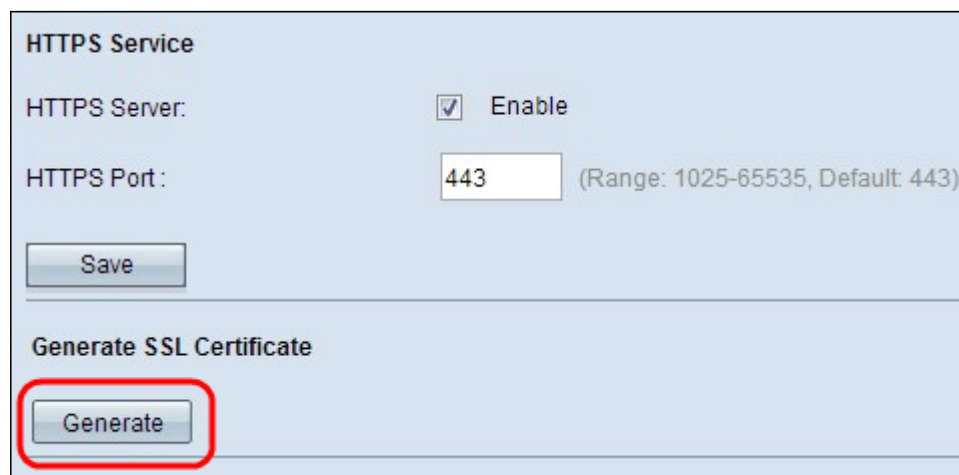
Paso 9. **Salvaguardia del teclado** para salvar las configuraciones.

Configuración de los Certificados SSL

Usted puede descargar un certificado SSL vía un buscador Web HTTP/HTTPS o de un servidor TFTP, utilizar el Punto de acceso para generar un certificado SSL, o cargar por teletratamiento un certificado SSL de su ordenador. En esta sección, todos los métodos distintos para instalar un certificado SSL se describen.

Generación de un certificado SSL

El nuevo certificado HTTP SSL para el servidor Web seguro debe ser generado después de que el punto de acceso haya adquirido una dirección IP de modo que el nombre común para el certificado haga juego la dirección IP del AP. La generación de un nuevo certificado SSL recomienza al servidor Web seguro. La conexión segura no funciona hasta que el nuevo certificado se valide en el navegador.



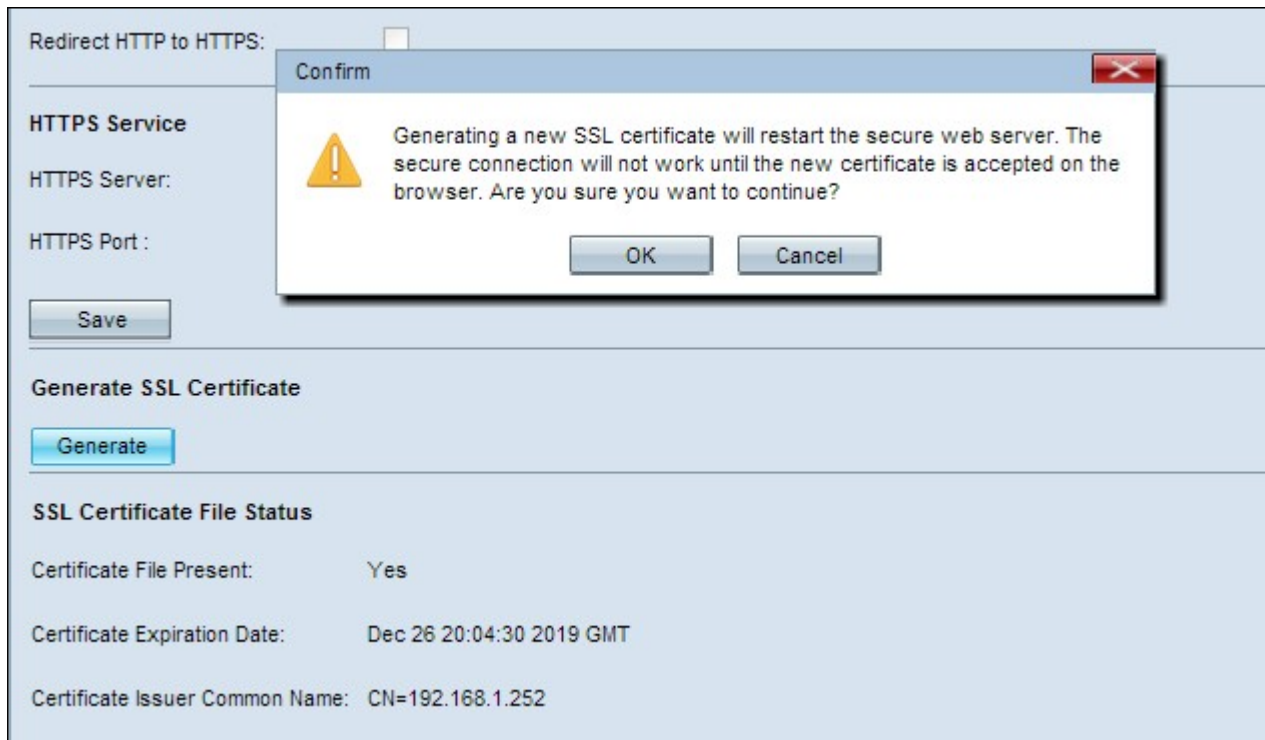
HTTPS Service

HTTPS Server: Enable

HTTPS Port: (Range: 1025-65535, Default: 443)

Generate SSL Certificate

Paso 1. El teclado **genera** para generar un nuevo certificado SSL. Una ventana de confirmación aparece.



Paso 2. Haga clic la **AUTORIZACIÓN** para continuar con la generación del certificado SSL. Después de que se haya generado el certificado, el área del estatus del archivo de certificado SSL visualiza la siguiente información:

- Archivo de certificado presente — Indica si el archivo de certificado HTTP SSL está presente o no.
- Fecha de caducidad del certificado — Visualiza la fecha de caducidad del certificado actual HTTP SSL.
- Nombre común del emisor del certificado — Visualiza el nombre común del emisor actual del certificado.

Descargue el certificado SSL

Los pasos abajo describen cómo descargar el certificado SSL (un fichero .pem) del dispositivo a la PC como salvaguardia.

SSL Certificate File Status

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 22:09:59 2019 GMT

Certificate Issuer Common Name: CN=192.168.1.245

Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS
 TFTP

Paso 1. Haga clic el botón de radio que corresponde con el método deseado de la transferencia directa bajo área del certificado de la transferencia directa SSL.

- HTTP/HTTPS — Permite que el certificado SSL sea descargado de un servidor Web. Salte al paso 4 si usted elige el HTTP/HTTPS.
- TFTP — Permite que el certificado SSL sea descargado de un servidor TFTP. Si usted elige esto, el nombre del archivo y los campos de direccionamiento del servidor IPv4 TFTP aparecen.

Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS
 TFTP

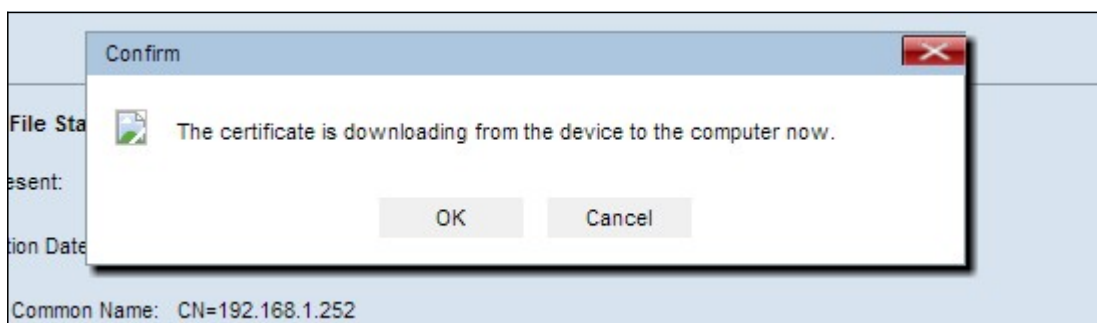
File Name: (Range: 1 - 128)

TFTP Server IPv4 Address:

Paso 2. Si usted eligió TFTP en el paso 1, ingrese el nombre del archivo en el campo de nombre del archivo. Esto es un fichero del tipo de certificado con una extensión .pem.

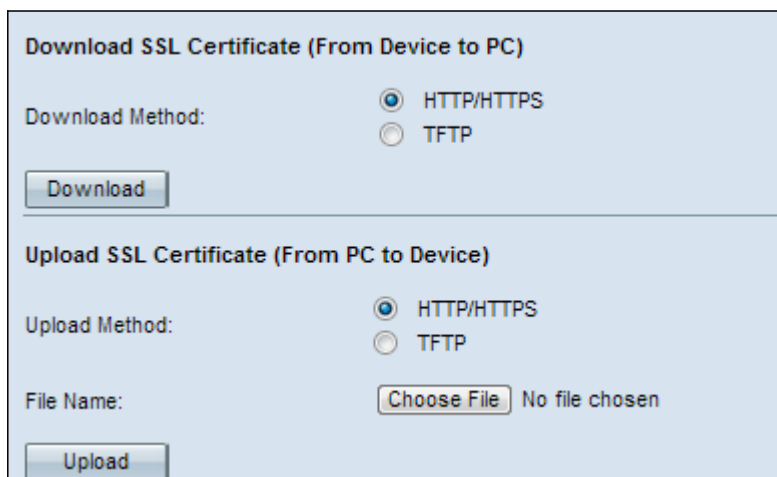
Paso 3. Si usted eligió TFTP en el paso 1, ingrese el IP address del servidor TFTP en el campo de direccionamiento del servidor IPv4 TFTP.

Paso 4. **Transferencia directa del teclado** para descargar el archivo de certificado. Una ventana de confirmación aparece.



Paso 5. **AUTORIZACIÓN** del teclado a continuar con la transferencia directa.

Cargue por teletratamiento el certificado SSL



The screenshot shows a web interface for managing SSL certificates. It is divided into two main sections: 'Download SSL Certificate (From Device to PC)' and 'Upload SSL Certificate (From PC to Device)'. Both sections have radio buttons for 'HTTP/HTTPS' (selected) and 'TFTP'. The 'Upload' section also includes a 'File Name:' field with a 'Choose File' button and the text 'No file chosen'. Both sections have a corresponding 'Download' or 'Upload' button.

Paso 1. Haga clic el HTTP/HTTPS o el botón de radio TFTP para elegir el método deseado de la carga por teletratamiento bajo área del certificado de la carga por teletratamiento SSL.

- HTTP/HTTPS — Esto permite que el certificado sea cargado por teletratamiento con un servidor Web. Si usted eligió el HTTP/HTTPS, el paso completo 2 y entonces salta el paso 3.
- TFTP — Esto permite que el certificado SSL sea cargado por teletratamiento a través de un servidor TFTP. Si usted elige esto el nombre del archivo y los campos de direccionamiento del servidor IPv4 TFTP aparecen. Salte el paso 2 y realice el paso 3.



This screenshot is identical to the one above, but with a red rectangular box highlighting the 'Choose File' button in the 'Upload' section. The 'File Name:' field is also highlighted with a yellow border.

Paso 2. Haga clic **eligen el fichero** para hojear y para seleccionar el fichero.

Download

Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS
 TFTP

File Name:

TFTP Server IPv4 Address:

Upload

Paso 3. Ingrese el nombre del archivo en el campo de nombre del archivo y a la dirección del servidor TFTP en el campo de direccionamiento del servidor IPv4 TFTP.

Paso 4. **Carga por teletratamiento del teclado** para cargar por teletratamiento el archivo de certificado. Una ventana de confirmación aparece.

File Status

Confirm

esent:

tion Date

Common

Certific

The selected HTTP SSL Certificate will now be uploaded. If successful, the AP WEB Server will be rebooted. Rebooting may take several minutes and the AP will be unavailable through the WEB UI during this time. When the process is complete the access point can be accessed again.

OK Cancel

Paso 5. **AUTORIZACIÓN del teclado** a continuar con la carga por teletratamiento.