HTTP/HTTPS Service Configuration and Generation of Secure Socket Layer (SSL) Certificate on WAP551 and WAP561 Access Points

Objective

The access point can be managed through both HTTP and HTTP Secure (HTTPS) connections when the HTTP/HTTPS servers are configured. Hyper Text Transfer Protocol Secure (HTTPS) is a more secure transfer protocol than HTTP. An Access Point must have a valid SSL certificate to use HTTPS service. A SSL certificate is a digitally signed certificate by a certificate authority that allows the web browser to have a secure encrypted communication with the web server.

This article explains how to configure the HTTP/HTTPS Service and how to create a Secure Socket Layer (SSL) certificate on the WAP551 and WAP561 access points.

Applicable Devices

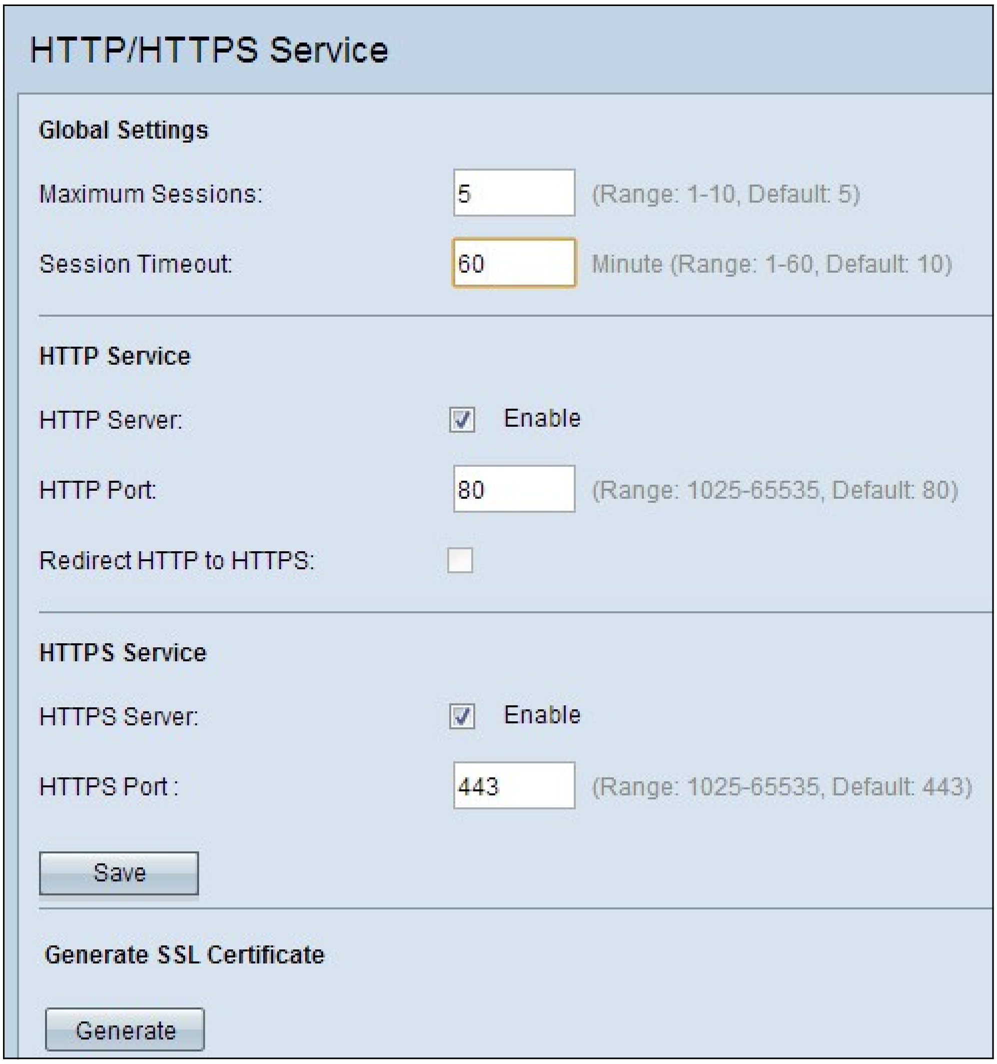
- WAP551
- WAP561

Software Version

- 1.1.0.4

Configuration of HTTP/HTTPS Service

Step 1. Log in to the web configuration utility and choose **Administration > HTTP/HTTPS Service**. The *HTTP/HTTPS Service* page opens:



HTTP/HTTPS Service

Global Settings

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

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

HTTP Service

HTTP Server: ☑ Enable

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

Redirect HTTP to HTTPS: □

HTTPS Service

HTTPS Server: ☑ Enable

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

Generate SSL Certificate

Step 2. Enter the maximum number of web sessions in the Maximum Sessions field. This signifies the maximum number of user that can be logged in to the web configuration utility.

Step 3. In the Session Timeout field, enter the maximum amount of time that an inactive user can remain logged on to the AP web configuration utility.

Step 4. Check the **Enable** check box of the HTTP Server to enable web access via HTTP. The HTTP server is enabled by default.

Note: If the HTTP Server is disabled, any current connections that use HTTP are disconnected.

Step 5. In the HTTP Port field, enter the port number to use for HTTP connections. Port number 80 is commonly used for HTTP connections.

Step 6. (Optional) If you wish to redirect management HTTP access attempts on the HTTP port to the HTTPS port check the **Redirect HTTP to HTTPS** check box. This field is available to enable only when HTTP access is disabled.

Step 7. Check the **Enable** check box of the HTTPS Server to enable web access via HTTPS. The HTTPS server is enabled by default.

Note: If the HTTPS Server is disabled, any current connections that use HTTPS are disconnected.

Step 8. Enter the port number to use for HTTPS connections in the HTTPS Port field. The default port number 443 is typically used with HTTPS.

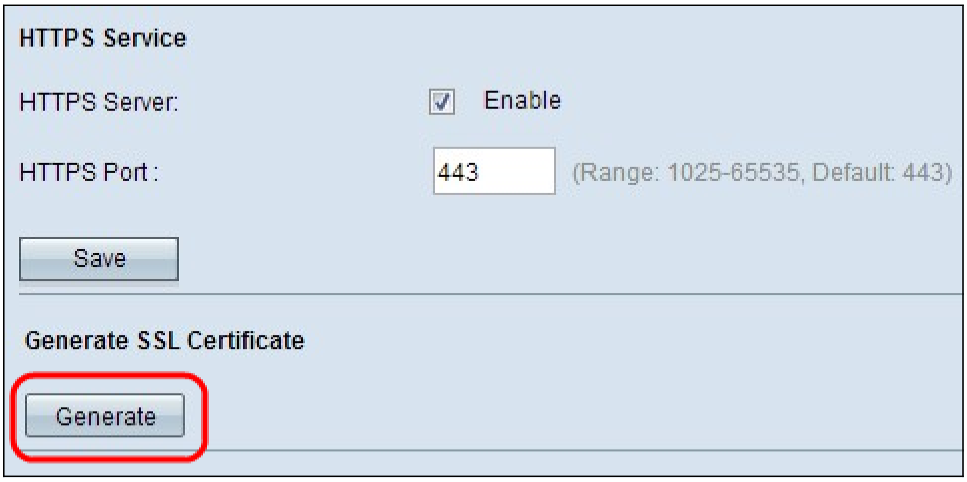
Step 9. Click **Save** to save the settings.

Configuration of SSL Certificates

You can download an SSL Certificate via an HTTP/HTTPS web browser or from a TFTP server, use the access point to generate an SSL certificate, or upload an SSL Certificate from your computer. In this section, all the different methods to install an SSL certificate are described.

Generation of an SSL Certificate

The new HTTP SSL certificate for the secure web server should be generated after the Access Point (AP) has acquired an IP address so that the common name for the certificate matches the IP address of the AP. Generation of a new SSL certificate restarts the secure web server. The secure connection does not work until the new certificate is accepted on the browser.



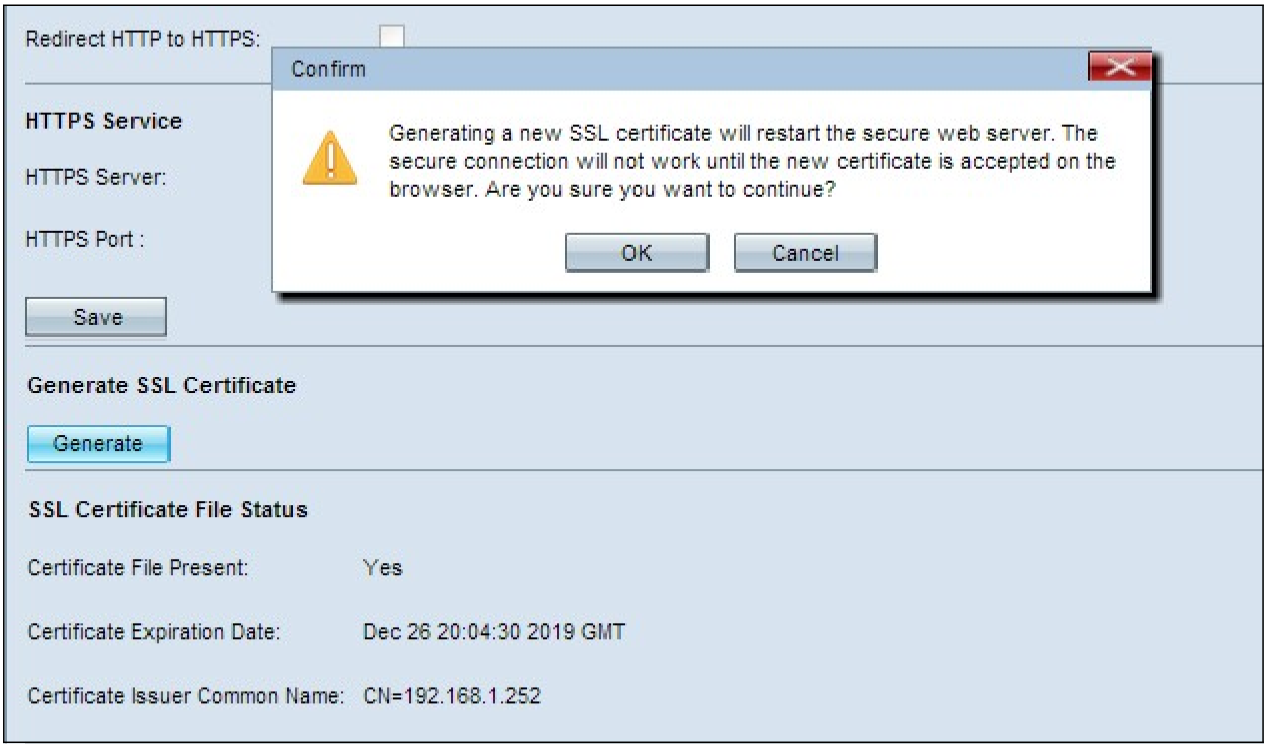
HTTPS Service

HTTPS Server: ☑ Enable

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

Generate SSL Certificate

Step 1. Click **Generate** to generate a new SSL certificate. A confirmation window appears.


Redirect HTTP to HTTPS: □

HTTPS Service

HTTPS Server:

HTTPS Port :

Confirm

Generating a new SSL certificate will restart the secure web server. The secure connection will not work until the new certificate is accepted on the browser. Are you sure you want to continue?

Generate SSL Certificate

SSL Certificate File Status

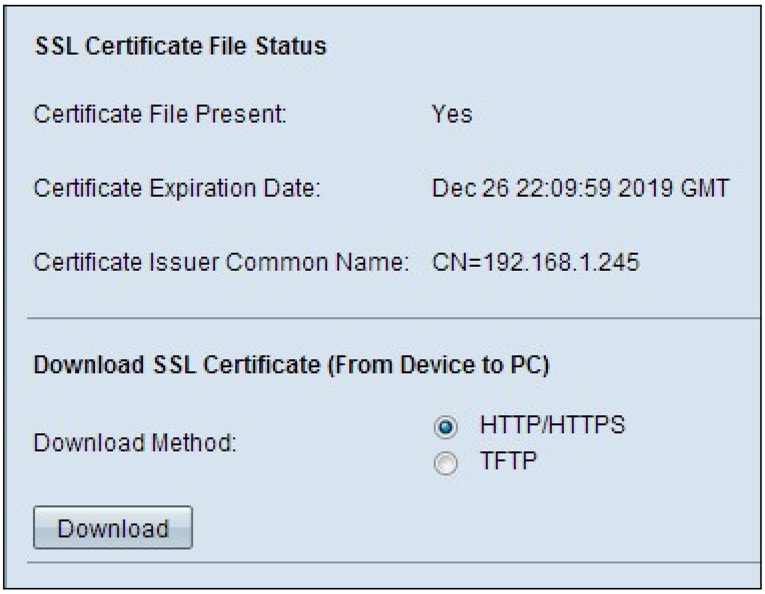
Certificate File Present:	Yes
Certificate Expiration Date:	Dec 26 20:04:30 2019 GMT
Certificate Issuer Common Name:	CN=192.168.1.252

Step 2. Click **OK** to continue with the generation of the SSL certificate. After the certificate has been generated, the SSL Certificate File Status area displays the following information:

- Certificate File Present — Indicates whether the HTTP SSL certificate file is present or not.
- Certificate Expiration Date — Displays the expiration date of the current HTTP SSL certificate.
- Certificate Issuer Common Name — Displays the common name of the current certificate issuer.

Download the SSL Certificate

The steps below describe how to download the SSL certificate (a .pem file) from device to the PC as a backup.


SSL Certificate File Status

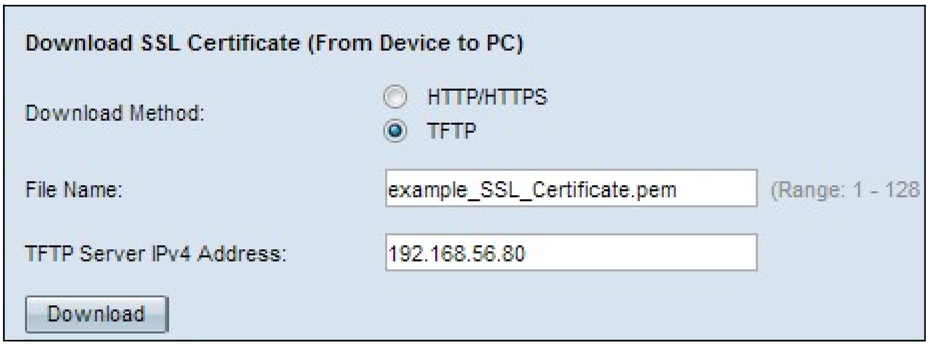
Certificate File Present:	Yes
Certificate Expiration Date:	Dec 26 22:09:59 2019 GMT
Certificate Issuer Common Name:	CN=192.168.1.245

Download SSL Certificate (From Device to PC)

Download Method: ● HTTP/HTTPS ○ TFTP

Step 1. Click the radio button that corresponds with the desired download method under the Download SSL Certificate area.

- HTTP/HTTPS — Allows SSL Certificate to be downloaded from a web server. Skip to Step 4 if you choose HTTP/HTTPS.
- TFTP — Allows SSL Certificate to be downloaded from a TFTP server. If you choose this, the File Name and TFTP Server IPv4 Address fields appear.



Download SSL Certificate (From Device to PC)

Download Method: ○ HTTP/HTTPS ● TFTP

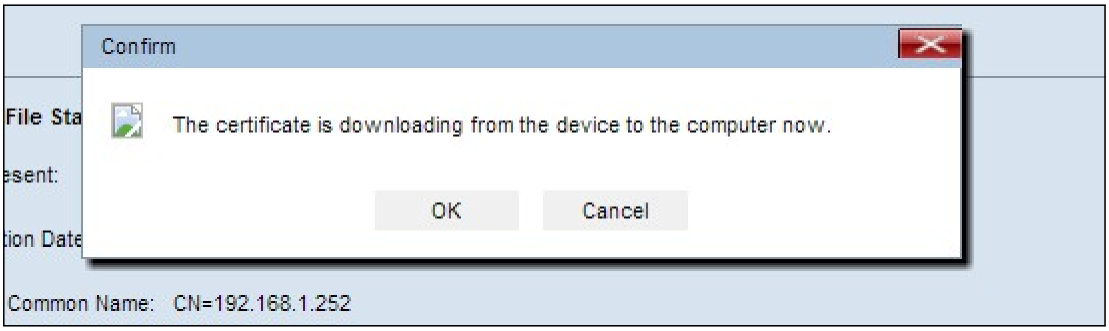
File Name: example_SSL_Certificate.pem (Range: 1 - 128

TFTP Server IPv4 Address: 192.168.56.80

Step 2. If you chose TFTP in Step 1, enter the file name in the File Name field. This is a certificate type file with a .pem extension.

Step 3. If you chose TFTP in Step 1, enter the IP address of the TFTP server in the TFTP Server IPv4 Address field.

Step 4. Click **Download** to download the certificate file. A confirmation window appears.



Confirm

The certificate is downloading from the device to the computer now.

File Sta

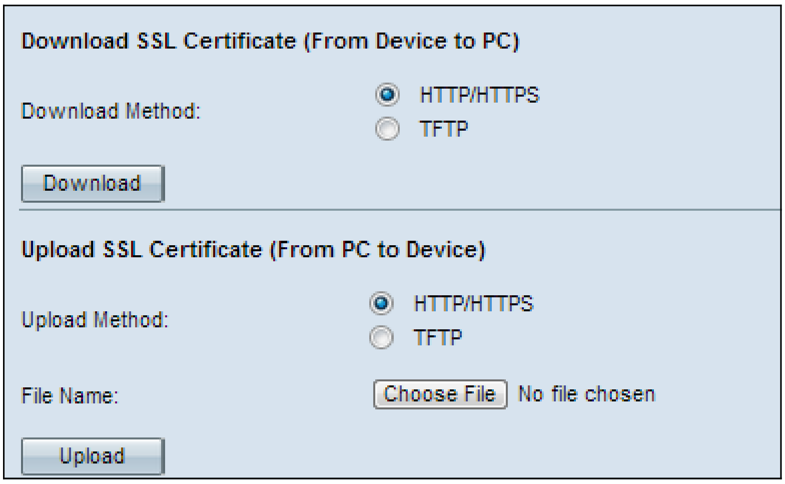
esent:

ion Date

Common Name: CN=192.168.1.252

Step 5. Click **OK** to continue with the download.

Upload the SSL Certificate



Download SSL Certificate (From Device to PC)

Download Method: ● HTTP/HTTPS ○ TFTP

Upload SSL Certificate (From PC to Device)

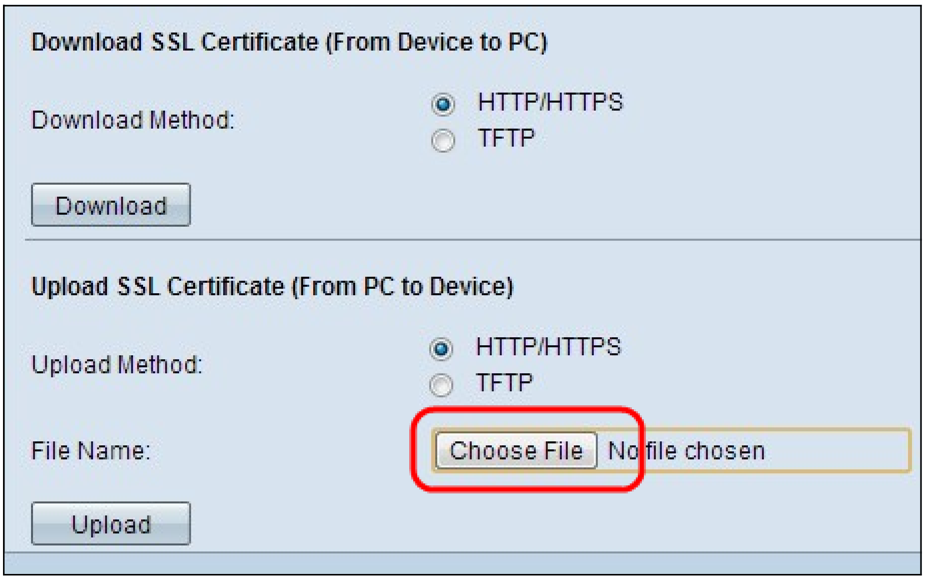
Upload Method: ● HTTP/HTTPS ○ TFTP

File Name: No file chosen

Step 1. Click either the HTTP/HTTPS or the TFTP radio button to choose desired upload method under the Upload SSL Certificate area.

- HTTP/HTTPS — This allows certificate to be uploaded with a web server. If you chose HTTP/HTTPS, complete Step 2 and then skip Step 3.

- TFTP — This allows SSL Certificate to be uploaded through a TFTP server. If you choose this the File Name and TFTP Server IPv4 Address fields appear. Skip Step 2 and perform Step 3.



Download SSL Certificate (From Device to PC)

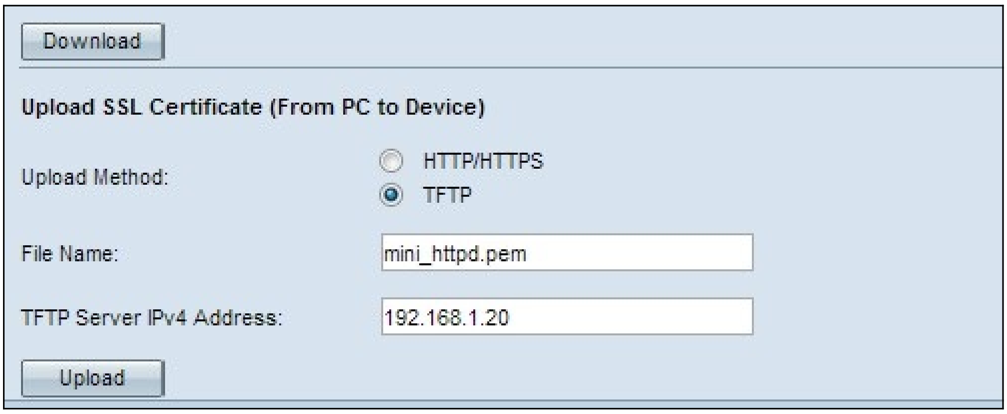
Download Method: ● HTTP/HTTPS ○ TFTP

Upload SSL Certificate (From PC to Device)

Upload Method: ● HTTP/HTTPS ○ TFTP

File Name: No file chosen

Step 2. Click **Choose File** to browse and select the file.



Upload SSL Certificate (From PC to Device)

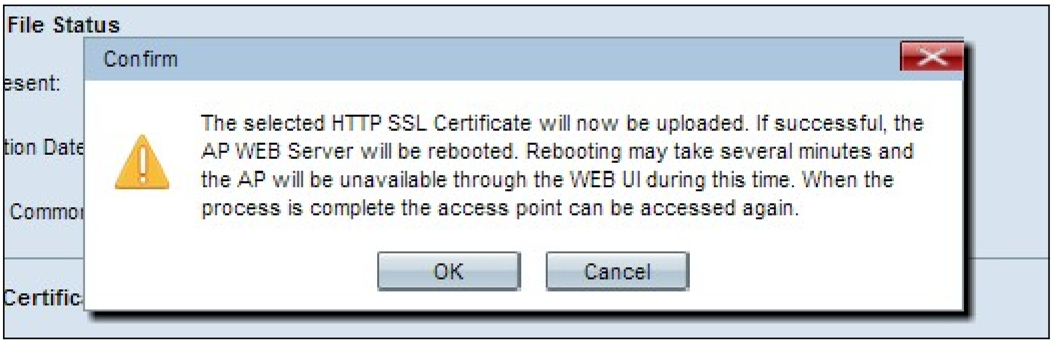
Upload Method: ○ HTTP/HTTPS ● TFTP

File Name: mini_httpd.pem

TFTP Server IPv4 Address: 192.168.1.20

Step 3. Enter the file name in the File Name field and the TFTP server address in the TFTP Server IPv4 Address field.

Step 4. Click **Upload** to upload the certificate file. A confirmation window appears.



File Status

Confirm

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.

Step 5. Click **OK** to continue with the upload.