

HTTP/HTTPS Service Configuration en Generation of Secure Socket Layer (SSL) certificaatcertificaat op WAP551 en WAP561 access points

Doel

Het access point kan worden beheerd via HTTP- en HTTP-beveiligde (HTTPS) verbindingen wanneer de HTTP/HTTPS-servers zijn geconfigureerd. Hyper-Text Transfer Protocol Secure (HTTPS) is een veiliger overdrachtprotocol dan HTTP. Een access point moet beschikken over een geldig SSL-certificaat om HTTPS-service te gebruiken. Een SSL-certificaat is een digitaal ondertekend certificaat door een certificeringsinstantie waarmee de webbrowser een beveiligde versleutelde communicatie met de webserver kan hebben.

Dit artikel legt uit hoe u de HTTP/HTTPS-service kunt configureren en hoe u een Secure Socket Layer (SSL)-certificaat kunt maken op de WAP551- en WAP561-access points.

Toepasselijke apparaten

- WAP551
- WAP561

Softwareversie

- 1.1.0.4

Configuratie van HTTP/HTTPS-service

Stap 1. Meld u aan bij het web-configuratieprogramma en kies **Beheer > HTTP/HTTPS-service**. De pagina *HTTP/HTTPS-service* wordt geopend:

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

Stap 2. Voer het maximale aantal websessies in het veld Maximum aantal sessies in. Dit geeft het maximale aantal gebruikers aan dat kan worden inlogd in het web configuratieprogramma.

Stap 3. In het veld Time-out voor sessie specificeert u de maximale tijd die een inactieve gebruiker kan inloggen op het AP-web configuratieprogramma.

Stap 4. Controleer het aanvinkvakje **Enable** of the HTTP Server om webtoegang via HTTP mogelijk te maken. De HTTP server is standaard ingeschakeld.

Opmerking: Als de HTTP Server uitgeschakeld is, worden alle huidige verbindingen die HTTP gebruiken losgekoppeld.

Stap 5. Voer in het veld HTTP-poort het te gebruiken poortnummer in voor HTTP-verbindingen. Poortnummer 80 wordt algemeen gebruikt voor HTTP-verbindingen.

Stap 6. (Optioneel) Als u de HTTP-toegangspogingen van het beheer wilt omleiden naar de HTTP-poort naar de HTTPS-poort, controleert u het aankruisvakje **HTTP naar HTTPS**. Dit veld is alleen beschikbaar voor het inschakelen van HTTP-toegang.

Stap 7. Controleer het aanvinkvakje voor **HTTPS**-server **inschakelen** om internettoegang via HTTPS mogelijk te maken. HTTPS-server is standaard ingeschakeld.

Opmerking: Als HTTPS Server uitgeschakeld is, worden alle huidige verbindingen die HTTPS gebruiken losgekoppeld.

Stap 8. Voer het te gebruiken poortnummer in voor HTTPS-verbindingen in het veld HTTPS-poort. Het standaardpoortnummer 443 wordt doorgaans gebruikt voor HTTPS.

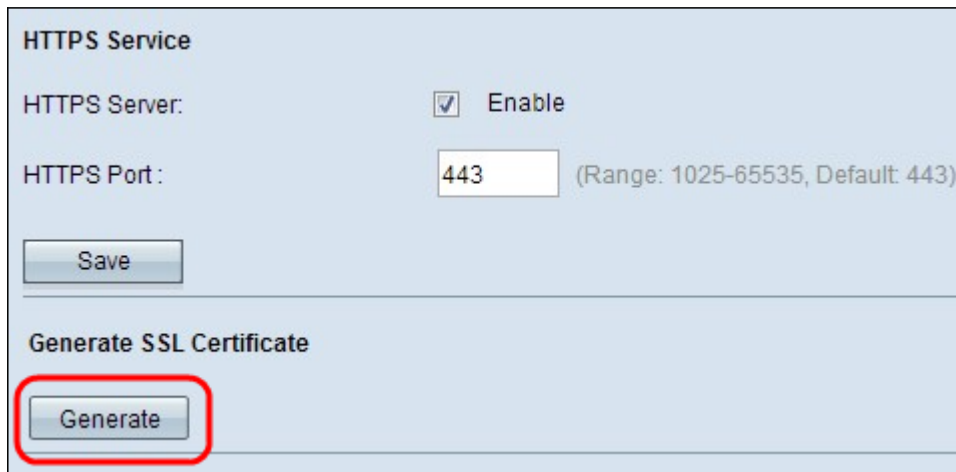
Stap 9. Klik op **Opslaan** om de instellingen op te slaan.

Configuratie van SSL-certificaten

U kunt een SSL-certificaat downloaden via een HTTP/HTTPS-webbrowser of van een TFTP-server, het toegangspunt gebruiken om een SSL-certificaat te genereren of een SSL-certificaat van uw computer te uploaden. In deze sectie worden alle verschillende methoden om een SSL-certificaat te installeren beschreven.

Generation of an SSL Certificate

Het nieuwe HTTP SSL-certificaat voor de beveiligde webserver moet worden gegenereerd nadat het Access Point (AP) een IP-adres heeft aangeschaft, zodat de gezamenlijke naam voor het certificaat overeenkomt met het IP-adres van het AP. Generation of a new SSL certificaat start de beveiligde webserver opnieuw. De beveiligde verbinding werkt niet totdat het nieuwe certificaat is geaccepteerd op de browser.



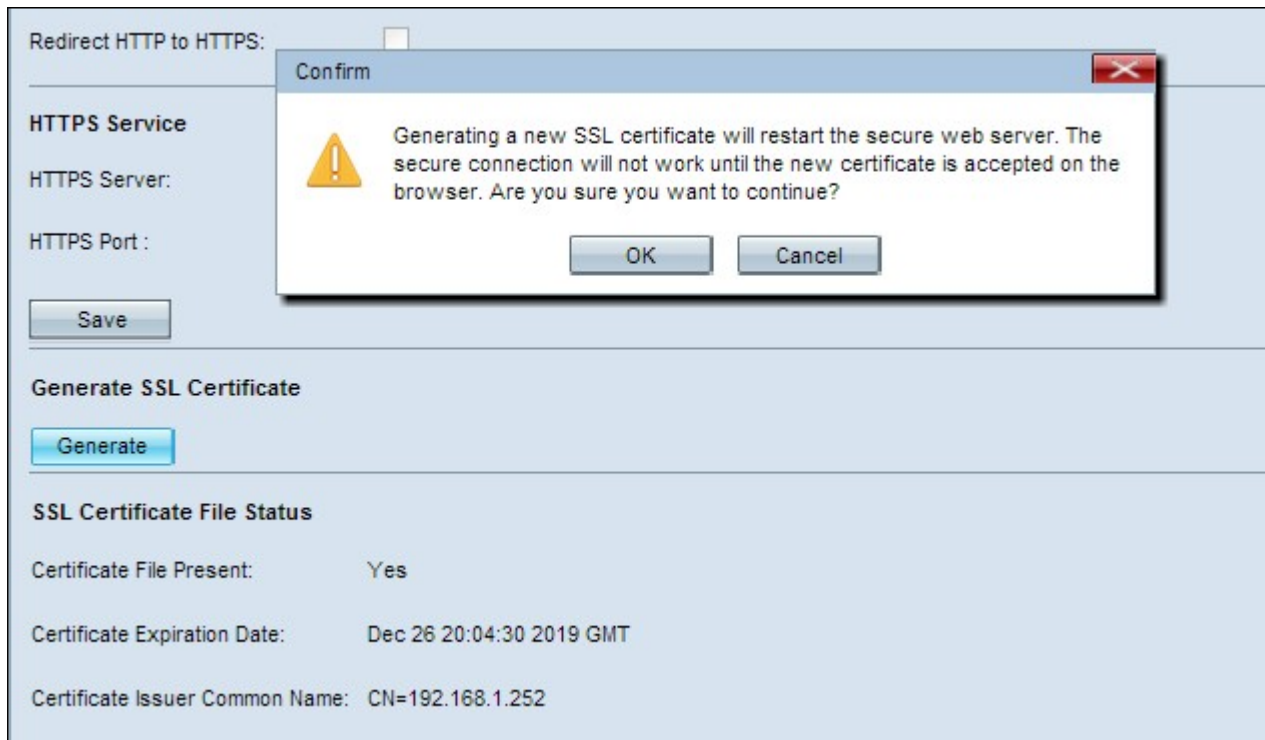
HTTPS Service

HTTPS Server: Enable

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

Generate SSL Certificate

Stap 1. Klik op **Generate** om een nieuw SSL certificaat te genereren. Er verschijnt een bevestigingsvenster.



Stap 2. Klik op **OK** om verder te gaan met de productie van het SSL-certificaat. Nadat het certificaat is gegenereerd, geeft het SSL-statusgebied van het certificaat de volgende informatie weer:

- certificaatbestand aanwezig — Geeft aan of het HTTP SSL-certificeringsbestand aanwezig is of niet.
- Vervaldatum certificaat — Hiermee wordt de verloopdatum van het huidige HTTP SSL-certificaat weergegeven.
- Gebruikelijke naam van de certificaathouder — Vermelding van de algemene naam van de huidige certificaathouder.

Download het SSL-certificaat

In de onderstaande stappen wordt beschreven hoe u het SSL-certificaat (een .pem-bestand) van een apparaat naar de pc als back-up kunt downloaden.

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

Stap 1. Klik op het radioknop dat overeenkomt met de gewenste downloadmethode onder het veld SSL-certificaat.

- HTTP/HTTPS — Hiermee kan SSL-certificaat worden gedownload van een webserver. Naar Stap 4 als u HTTP/HTTPS kiest.
- TFTP — Hiermee kan SSL-certificaat worden gedownload van een TFTP-server. Als u dit kiest, verschijnen de velden Bestandsnaam en TFTP Server IPv4-adres.

Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS
 TFTP

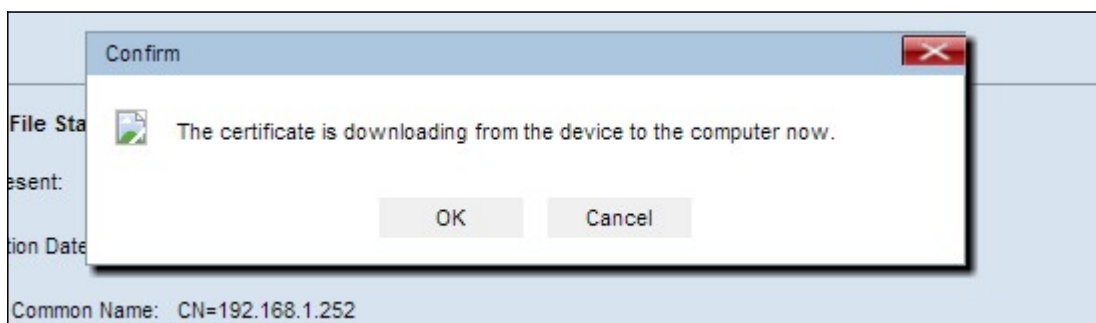
File Name: (Range: 1 - 128)

TFTP Server IPv4 Address:

Stap 2. Als u in Stap 1 TFTP hebt gekozen, voert u de bestandsnaam in het veld Bestandsnaam in. Dit is een certificaattype bestand met een .pem-extensie.

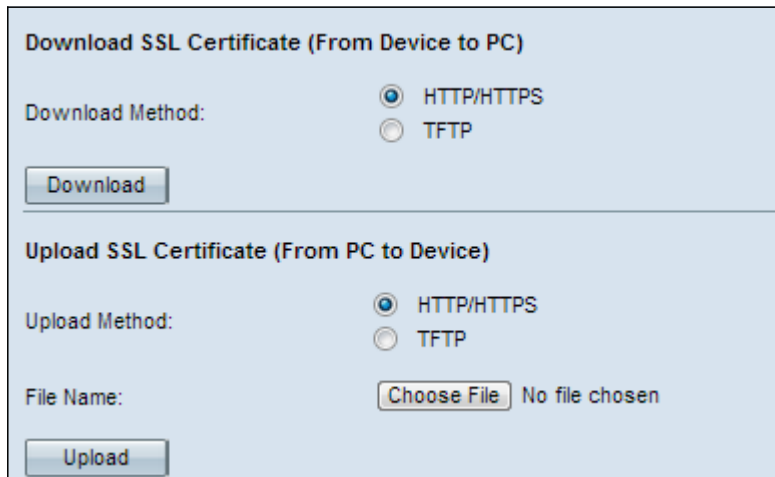
Stap 3. Als u in Stap 1 TFTP hebt gekozen, voert u het IP-adres van de TFTP-server in het veld IPv4-adres van de TFTP-server in.

Stap 4. Klik op **Download** om het certificaatbestand te downloaden. Er verschijnt een bevestigingsvenster.



Stap 5. Klik op **OK** om met de download verder te gaan.

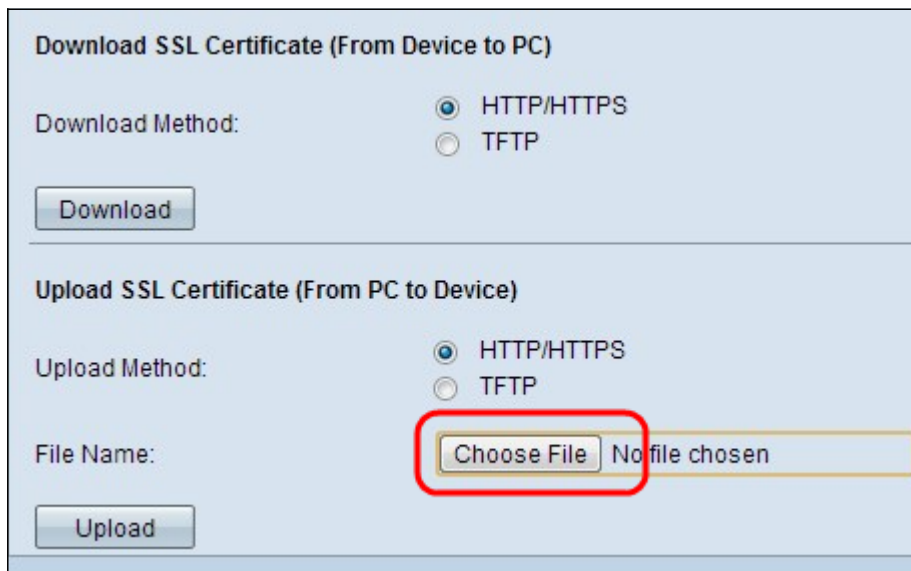
Het SSL-certificaat uploaden



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)'. In the 'Download' section, the 'Download Method' is set to 'HTTP/HTTPS' (selected with a radio button) and 'TFTP' (unselected). A 'Download' button is present. In the 'Upload' section, the 'Upload Method' is also set to 'HTTP/HTTPS' (selected) and 'TFTP' (unselected). Below this, there is a 'File Name:' label, a 'Choose File' button, and the text 'No file chosen'. An 'Upload' button is at the bottom of the section.

Stap 1. Klik op of de HTTP/HTTPS- of de TFTP-radioknop om de gewenste uploadmethode te kiezen onder het gebied met Upload SSL-certificaat.

- HTTP/HTTPS — Hiermee kan certificaat worden geüpload met een webserver. Als u HTTP/HTTPS kiest, volledige Stap 2 en dan slaan Stap 3 over.
- TFTP — Dit maakt het mogelijk SSL-certificaat te uploaden via een TFTP-server. Als u dit kiest, verschijnen de velden Bestandsnaam en TFTP Server IPv4 Adres. Stap 2 en voer Stap 3 uit.



This screenshot is identical to the one above, but with a red rectangular box highlighting the 'Choose File' button in the 'Upload' section. The text 'No file chosen' is visible to the right of the button.

Stap 2. Klik op **Kies bestand** om door te bladeren en selecteer het bestand.

Download

Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS
 TFTP

File Name:

TFTP Server IPv4 Address:

Upload

Stap 3. Voer de bestandsnaam in het veld Bestandsnaam en het TFTP-serveradres in het veld IPv4-adres van de TFTP-server in.

Stap 4. Klik op **Upload** om het certificaatbestand te uploaden. Er verschijnt een bevestigingsvenster.



Stap 5. Klik op **OK** om met het uploaden verder te gaan.