

# HTTP/HTTPS-serviceconfiguratie en -beheer van Secure Socket Layer (SSL) Certificaat op WAP121 en WAP321 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. Sommige webbrowsers gebruiken HTTP terwijl anderen HTTPS gebruiken. 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 op de WAP121- en WAP321-access points.

## Toepasselijke apparaten

- WAP121
- WAP321

## Softwareversie

- 1.0.3.4

## 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)

Stap 2. Voer het maximale aantal websessies in dat de HTTP- en HTTPS-sessie bevat die tegelijkertijd in het veld Maximum aantal sessies moet worden gebruikt. Er wordt een sessie gemaakt telkens wanneer een gebruiker zich op het apparaat aanmeldt. Als de maximale sessie is bereikt wordt de volgende gebruiker die probeert in te loggen op het apparaat met HTTP of HTTPS-service, afgewezen.

Stap 3. Voer de maximale hoeveelheid tijd in minuten in die een inactieve gebruiker op de AP-webinterface in het veld Time-out sessie blijft inloggen.

**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)

Stap 4. Controleer het aanvinkvakje **Enable** in het veld HTTP Server om webtoegang via HTTP mogelijk te maken.

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

Stap 5. Voer het te gebruiken poortnummer in voor HTTP-verbindingen in het veld HTTP-poort. Het poortnummer varieert van 1025 tot 65535.

Stap 6. (Optioneel) Om de HTTP-toegangspogingen op de HTTP-poort naar de HTTPS-poort te richten, controleert u het aankruisvakje **HTTP naar HTTPS**. Dit veld is alleen beschikbaar als HTTP-toegang is uitgeschakeld.

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

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

Stap 8. Voer het te gebruiken poortnummer in voor HTTPS-verbindingen in het veld HTTPS-poorten. Het poortnummer varieert van 1025 tot 65535.

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

## Generation of an SSL Certificate

Het genereren van een nieuw HTTP SSL certificaat voor de beveiligde webserver moet gebeuren nadat het AP een IP adres heeft aangeschaft. Dit waarborgt dat de algemene 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. Volg de onderstaande stappen om het SSL-certificaat te genereren.

## 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**

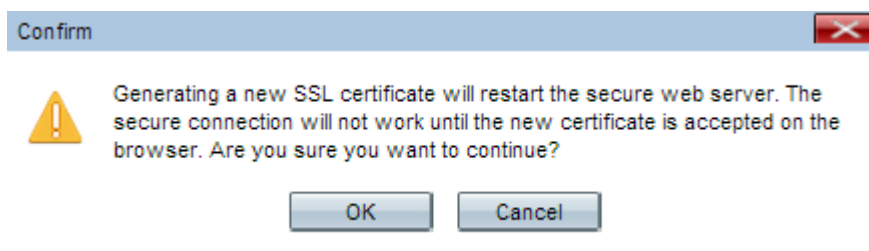
---

**SSL Certificate File Status**

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 20:00:03 2019 GMT

Stap 1. Klik op **Generate** om een nieuw SSL certificaat te genereren. Het waarschuwingsbericht verschijnt.



Stap 2. Klik op **OK** om verder te gaan met de productie van het SSL-certificaat.

### SSL Certificate File Status

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 20:00:03 2019 GMT

Certificate Issuer Common Name: CN=192.168.1.245

### Download SSL Certificate (From Device to PC)

Download Method:  HTTP/HTTPS  
 TFTP

Download

### Upload SSL Certificate (From PC to Device)

Upload Method:  HTTP/HTTPS  
 TFTP

File Name:  No file chosen

Upload

De SSL-bestandsstatus van het certificaat geeft de volgende informatie weer:

- certificaatbestand aanwezig — Geeft aan of het HTTP SSL-certificeringsbestand aanwezig is of niet. De standaardinstelling is nee.
- Vervaldatum certificaat — Hiermee wordt de verloopdatum van het HTTP SSL-certificaat weergegeven.
- Certificaatuitgevende instelling Gemeenschappelijke naam — Vermeld de algemene naam van de certificaathouder.

## Download het SSL-certificaat

### Download SSL Certificate (From Device to PC)

Download Method:  HTTP/HTTPS  
 TFTP

Download

### Upload SSL Certificate (From PC to Device)

Upload Method:  HTTP/HTTPS  
 TFTP

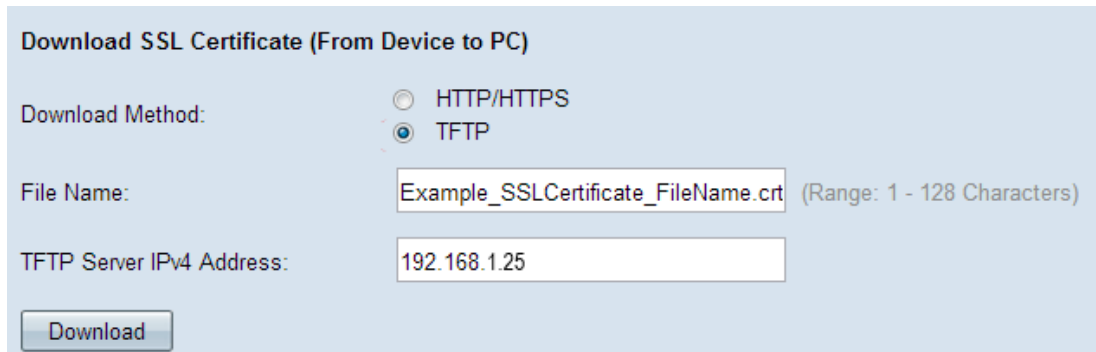
File Name:  No file chosen

Upload

Stap 1. Klik het juiste SSL-certificeringsbestand op de knop Downloadmethode in het gebied SSL-certificaat (Van apparaat naar pc).

- HTTP/HTTPS — Klik op deze radioknop als het SSL-certificaat moet worden gedownload van een webserver.
- TFTP — Klik op deze radioknop als het SSL-certificaat van een TFTP-server moet worden gedownload.

Opmerking: Naar Stap 4 als HTTP/HTTPS in de vorige stap is geklikt.



**Download SSL Certificate (From Device to PC)**

Download Method:  HTTP/HTTPS  
 TFTP

File Name:  (Range: 1 - 128 Characters)

TFTP Server IPv4 Address:

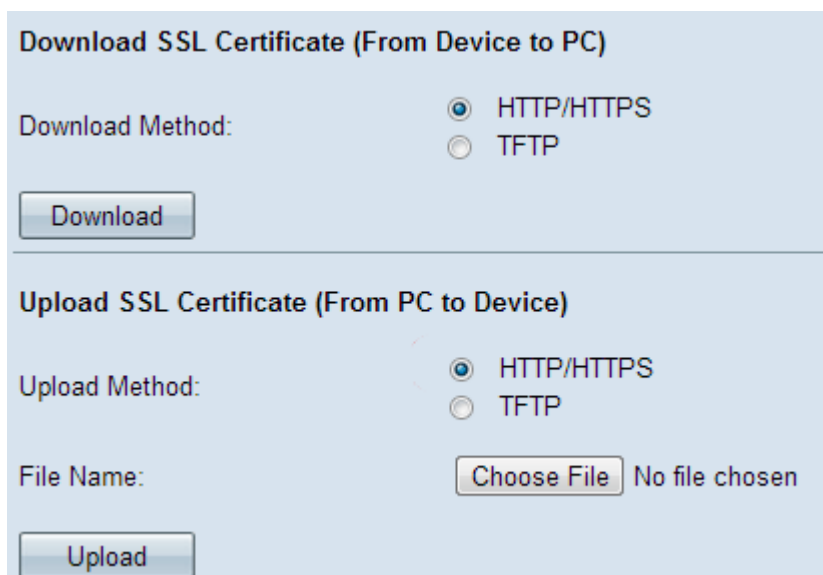
Stap 2. Als op TFTP in Stap 2 is gedrukt, voert u de bestandsnaam in het veld Bestandsnaam in.

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

Stap 4. Klik op **Download** om het certificaatbestand te downloaden.

## Het SSL-certificaat uploaden

Volg de onderstaande stappen om het SSL-certificaat te uploaden.



**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

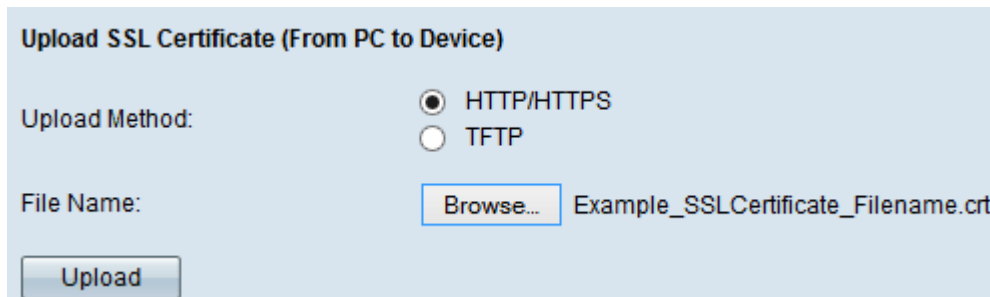
Stap 1. Klik het gewenste uploadmethode-keuzerondje in het gebied Upload SSL (Van pc naar apparaat).

- HTTP/HTTPS — Klik op deze radioknop als het SSL-certificaat met een webserver moet worden geüpload.
- TFTP — Klik op deze radioknop als het SSL-certificaat met een TFTP-server moet

worden geüpload.

Opmerking: Naar Stap 4 indien op TFTP is gedrukt in de vorige stap.

Stap 2. Als HTTP/HTTPS wordt geklikt, klik dan op **Kies Bestand** of **Bladeren** op basis van uw browser om naar het bestand te bladeren.

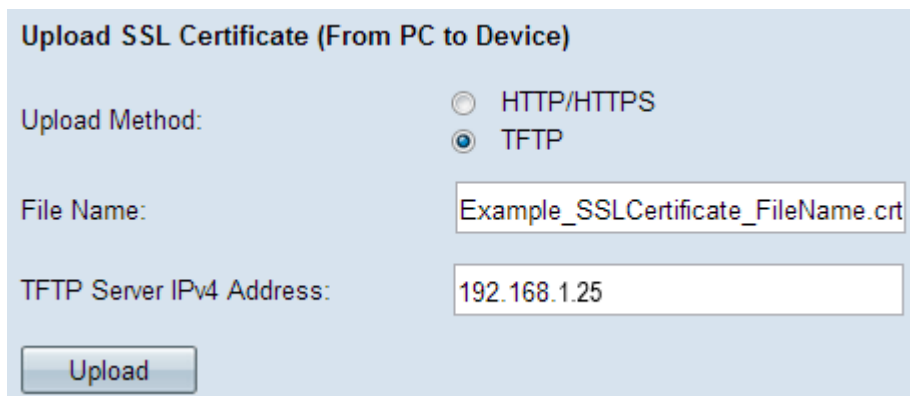


**Upload SSL Certificate (From PC to Device)**

Upload Method:  HTTP/HTTPS  
 TFTP

File Name:  Example\_SSLCertificate\_Filename.crt

Stap 3. Klik op **Upload** om het gekozen bestand te uploaden. Niet de laatste stappen omdat deze stappen alleen op TFTP van toepassing zijn.



**Upload SSL Certificate (From PC to Device)**

Upload Method:  HTTP/HTTPS  
 TFTP

File Name:

TFTP Server IPv4 Address:

Stap 4. Als op TFTP in Stap 2 is gedrukt, voert u de bestandsnaam in het veld Bestandsnaam in.

Stap 5. Voer het TFTP-serveradres in het veld IPv4-adres van de TFTP-server in.

Stap 6. Klik op **Upload** om het certificaatbestand te uploaden.