

Configuração e gerenciamento de serviços HTTP/HTTPS do certificado SSL (Secure Socket Layer) nos access points WAP121 e WAP321

Objetivo

O ponto de acesso pode ser gerenciado através de conexões HTTP e HTTP Secure (HTTPS) quando os servidores HTTP/HTTPS estiverem configurados. O protocolo HTTPS é um protocolo de transferência mais seguro do que o HTTP. Alguns navegadores usam HTTP, enquanto outros usam HTTPS. Um ponto de acesso deve ter um certificado SSL válido para usar o serviço HTTPS. Um certificado SSL é um certificado assinado digitalmente por uma autoridade de certificado que permite que o navegador da Web tenha uma comunicação criptografada segura com o servidor da Web.

Este artigo explica como configurar o Serviço HTTP/HTTPS nos pontos de acesso WAP121 e WAP321.

Dispositivos aplicáveis

WAP121
WAP321

Versão de software

•1.0.3.4

Serviço HTTP/HTTPS

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Administration > HTTP/HTTPS Service**. A página *Serviço HTTP/HTTPS* é aberta:

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)

Etapa 2. Digite o número máximo de sessões da Web que inclui a sessão HTTP e HTTPS a serem usadas ao mesmo tempo no campo Máximo de sessões. Uma sessão é criada toda vez que um usuário faz logon no dispositivo. Se a sessão máxima for atingida, o próximo usuário que tentar fazer logon no dispositivo com o serviço HTTP ou HTTPS será rejeitado.

Etapa 3. Insira o tempo máximo em minutos durante o qual um usuário inativo permanece conectado à interface da Web do AP no campo Tempo limite da sessão.

The screenshot shows a configuration interface with three sections: Global Settings, HTTP Service, and HTTPS Service. In the Global Settings section, 'Maximum Sessions' is set to 8 and 'Session Timeout' is set to 45 minutes. In the HTTP Service section, the 'HTTP Server' is checked and labeled 'Enable', the 'HTTP Port' is set to 1025, and the 'Redirect HTTP to HTTPS' checkbox is unchecked. In the HTTPS Service section, the 'HTTPS Server' is checked and labeled 'Enable', and the 'HTTPS Port' is set to 65535. A 'Save' button is located at the bottom left of the configuration area.

Etapa 4. Marque a caixa de seleção **Habilitar** no campo Servidor HTTP para habilitar o acesso à Web via HTTP.

Note: Se o Servidor HTTP estiver desabilitado, todas as conexões atuais que usam HTTP serão desconectadas.

Etapa 5. Insira o número da porta a ser usada para conexões HTTP no campo Porta HTTP. O número da porta varia de 1025 a 65535.

Etapa 6. (Opcional) Para redirecionar as tentativas de acesso HTTP de gerenciamento na porta HTTP para a porta HTTPS, marque a caixa de seleção **Redirecionar HTTP para HTTPS**. Este campo está disponível somente quando o acesso HTTP está desativado.

Passo 7. Marque a caixa de seleção **Habilitar** do Servidor HTTPS para habilitar o acesso à Web via HTTPS.

Note: Se o servidor HTTPS estiver desabilitado, todas as conexões atuais que usam HTTPS serão desconectadas.

Etapa 8. Insira o número da porta a ser usada para conexões HTTPS no campo Porta HTTPS. O número da porta varia de 1025 a 65535.

Etapa 9. Clique em **Save (Salvar)** para salvar as configurações.

Geração de um certificado SSL

A geração de um novo certificado SSL HTTP para o servidor web seguro deve ser feita depois que o AP tiver adquirido um endereço IP. Isso garante que o nome comum do certificado corresponda ao endereço IP do AP. A geração de um novo certificado SSL reinicia o servidor Web seguro. A conexão segura não funciona até que o novo certificado seja aceito no navegador. Siga as etapas abaixo para gerar o certificado SSL.

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)

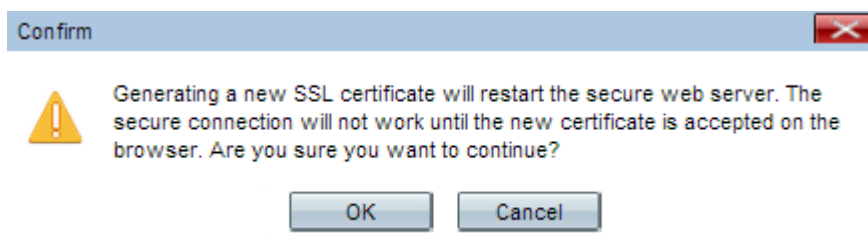
Generate SSL Certificate

SSL Certificate File Status

Certificate File Present: Yes

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

Etapa 1. Clique em **Gerar** para gerar um novo certificado SSL. A mensagem de alerta é exibida.



Etapa 2. Clique em **OK** para continuar com a geração do certificado SSL.

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

Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS
 TFTP

File Name: No file chosen

A área Status do arquivo de certificado SSL exibe as seguintes informações:

Arquivo de certificado presente — Indica se o arquivo de certificado SSL HTTP está presente ou não. O padrão é não.

Data de expiração do certificado — Exibe a data de expiração do certificado SSL HTTP.

Nome comum do emissor do certificado — Exibe o nome comum do emissor do certificado.

Fazer download do certificado SSL

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

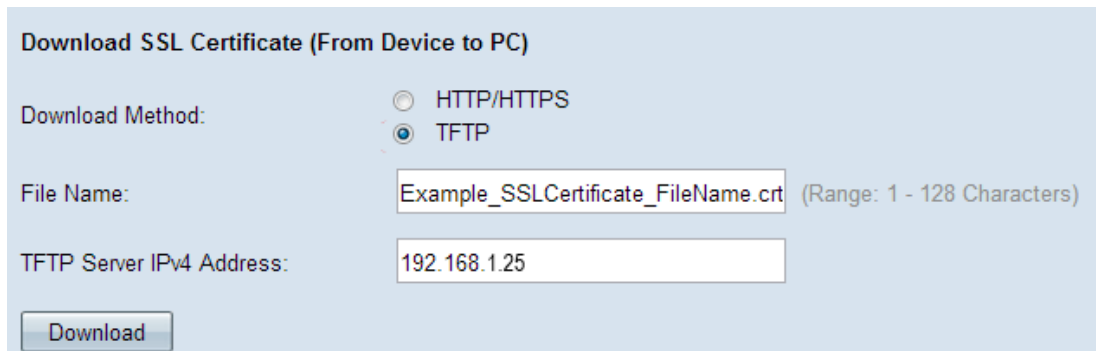
Etapa 1. Clique no arquivo de certificado SSL apropriado no botão de opção Download

Method na área Download SSL Certificate (From Device to PC).

HTTP/HTTPS — Clique neste botão de opção se o Certificado SSL deve ser baixado de um servidor Web.

TFTP — Clique neste botão de opção se o Certificado SSL deve ser baixado de um servidor TFTP.

Note: Vá para a etapa 4 se o HTTP/HTTPS for clicado na etapa anterior.



Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS TFTP

File Name: (Range: 1 - 128 Characters)

TFTP Server IPv4 Address:

Etapa 2. Se o TFTP for clicado na Etapa 2, insira o nome do arquivo no campo Nome do arquivo.

Etapa 3. Insira o endereço do servidor TFTP no campo Endereço IPv4 do servidor TFTP.

Etapa 4. Clique em **Download** para baixar o arquivo de certificado.

Fazer upload do certificado SSL

Siga as etapas abaixo para carregar o certificado SSL.



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

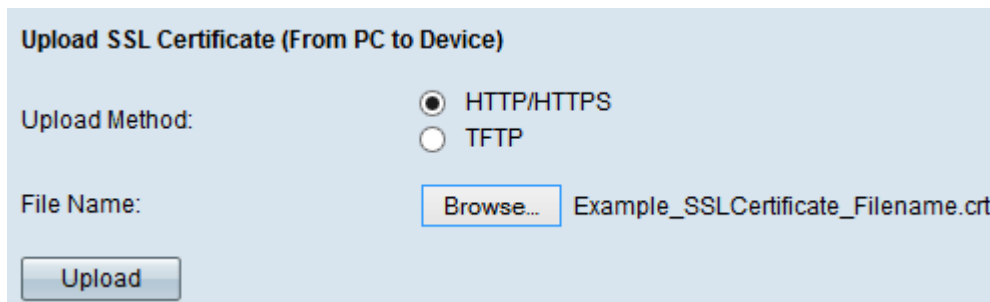
Etapa 1. Clique no botão de opção Método de upload apropriado na área Carregar certificado SSL (Do PC ao dispositivo).

HTTP/HTTPS — Clique neste botão de opção se o Certificado SSL deve ser carregado com um servidor Web.

TFTP — Clique neste botão de opção se o Certificado SSL deve ser carregado com um servidor TFTP.

Note: Vá para a etapa 4 se o TFTP for clicado na etapa anterior.

Etapa 2. Se o HTTP/HTTPS for clicado, clique em **Choose File** ou **Browse** baseado em seu navegador para procurar o arquivo.

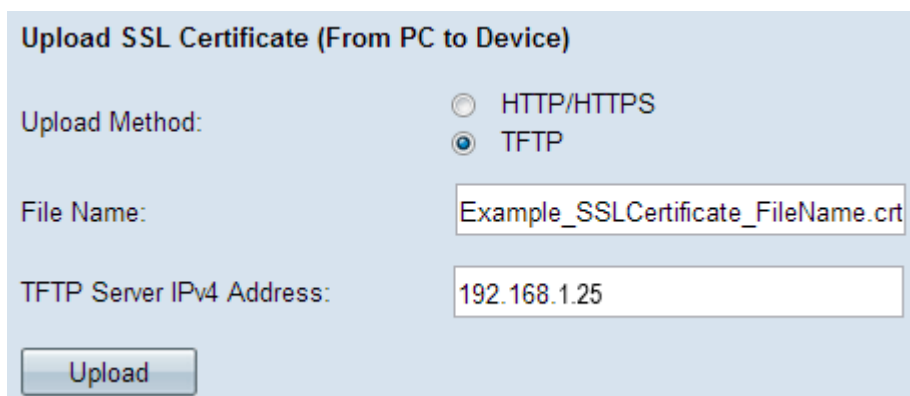


Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS
 TFTP

File Name: Example_SSLCertificate_Filename.crt

Etapa 3. Clique em **Carregar** para carregar o arquivo escolhido. Ignore as últimas etapas, pois essas etapas se aplicam somente ao TFTP.



Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS
 TFTP

File Name:

TFTP Server IPv4 Address:

Etapa 4. Se o TFTP for clicado na Etapa 2, insira o nome do arquivo no campo Nome do arquivo.

Etapa 5. Insira o endereço do servidor TFTP no campo Endereço IPv4 do servidor TFTP.

Etapa 6. Clique em **Carregar** para carregar o arquivo de certificado.