Configurazione del servizio HTTP/HTTPS e generazione del certificato SSL (Secure Sockets Layer) sui punti di accesso WAP551 e WAP561

Obiettivo

Il punto di accesso può essere gestito tramite connessioni HTTP e HTTP protetto (HTTPS) quando i server HTTP/HTTPS sono configurati. Il protocollo HTTPS (Hyper Text Transfer Protocol Secure) è un protocollo di trasferimento più sicuro del protocollo HTTP. Per utilizzare il servizio HTTPS, un punto di accesso deve disporre di un certificato SSL valido. Un certificato SSL è un certificato con firma digitale rilasciato da un'autorità di certificazione che consente al browser di comunicare con il server Web in modo protetto e crittografato.

In questo articolo viene illustrato come configurare il servizio HTTP/HTTPS e come creare un certificato SSL (Secure Sockets Layer) sui punti di accesso WAP551 e WAP561.

Dispositivi interessati

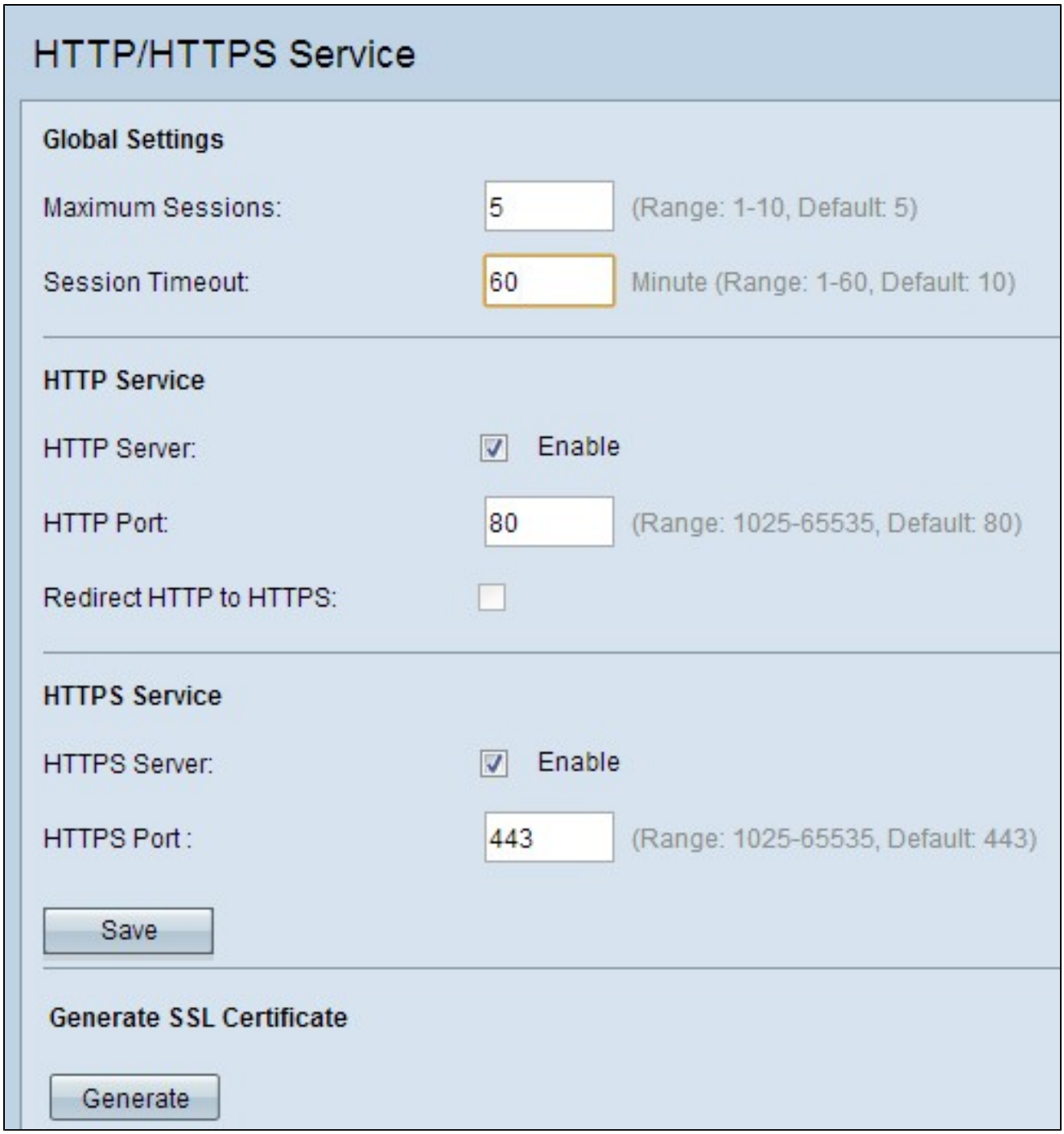
· WAP551
· WAP561

Versione del software

•1.1.0.4

Configurazione del servizio HTTP/HTTPS

Passaggio 1. Accedere all'utility di configurazione Web e scegliere Amministrazione > Servizio HTTP/HTTPS. Viene visualizzata la pagina Servizio HTTP/HTTPS:



Passaggio 2. Immettere il numero massimo di sessioni Web nel campo Numero massimo di sessioni. Indica il numero massimo di utenti che possono accedere all'utilità di configurazione Web.

Passaggio 3. Nel campo Timeout sessione, immettere il periodo di tempo massimo durante il quale un utente inattivo può rimanere connesso all'utility di configurazione Web dell'access point.

Passaggio 4. Selezionare la casella di controllo Abilita del server HTTP per abilitare l'accesso Web tramite HTTP. Il server HTTP è abilitato per impostazione predefinita.

Nota: se il server HTTP è disabilitato, tutte le connessioni correnti che utilizzano il protocollo HTTP verranno disconnesse.

Passaggio 5. Nel campo Porta HTTP immettere il numero di porta da utilizzare per le connessioni HTTP. Il numero di porta 80 è comunemente utilizzato per le connessioni HTTP.

Passaggio 6. (Facoltativo) Se si desidera reindirizzare i tentativi di accesso HTTP di gestione sulla porta HTTP alla porta HTTPS, selezionare la casella di controllo Reindirizza HTTP a HTTPS. Questo campo è disponibile per l'abilitazione solo quando l'accesso HTTP è disabilitato.

Passaggio 7. Selezionare la casella di controllo Abilita del server HTTPS per abilitare l'accesso Web tramite HTTPS. Il server HTTPS è abilitato per impostazione predefinita.

Nota: se il server HTTPS è disabilitato, tutte le connessioni correnti che utilizzano HTTPS vengono disconnesse.

Passaggio 8. Immettere il numero di porta da utilizzare per le connessioni HTTPS nel campo Porta HTTPS. Il numero di porta predefinito 443 viene in genere utilizzato con HTTPS.

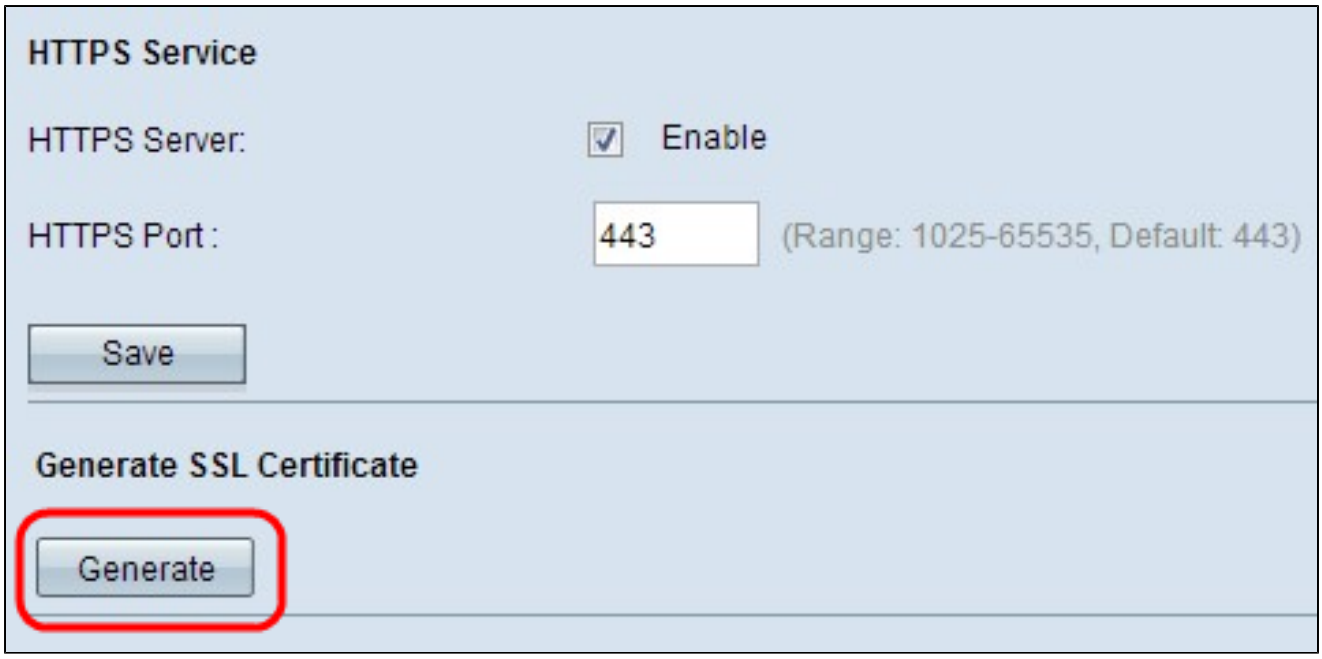
Passaggio 9. Fare clic su Save (Salva) per salvare le impostazioni.

Configurazione dei certificati SSL

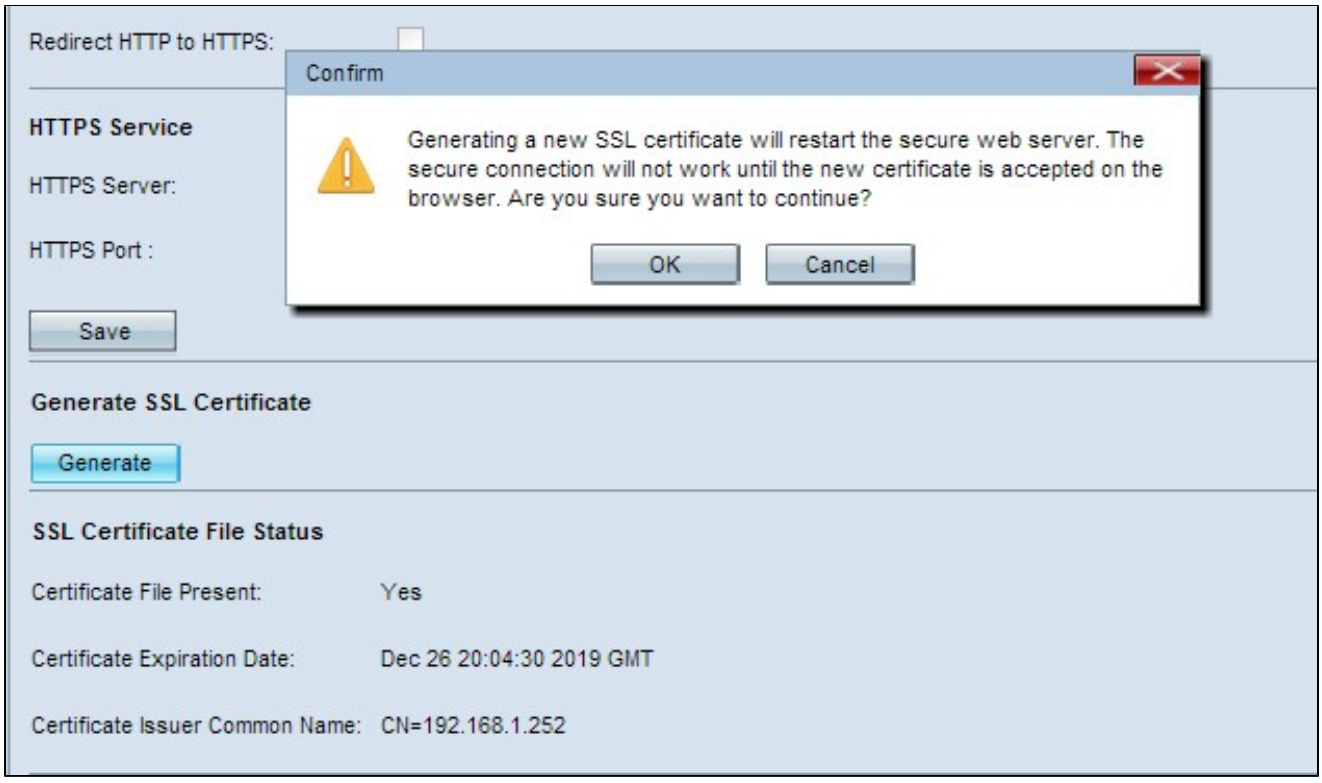
È possibile scaricare un certificato SSL tramite un browser Web HTTP/HTTPS o da un server TFTP, utilizzare il punto di accesso per generare un certificato SSL o caricare un certificato SSL dal computer. In questa sezione vengono descritti tutti i diversi metodi di installazione di un certificato SSL.

Generazione di un certificato SSL

Il nuovo certificato SSL HTTP per il server Web protetto deve essere generato dopo che il punto di accesso ha acquisito un indirizzo IP, in modo che il nome comune del certificato corrisponda all'indirizzo IP del punto di accesso. La generazione di un nuovo certificato SSL riavvia il server Web protetto. La connessione protetta non funziona finché il nuovo certificato non viene accettato nel browser.



Passaggio 1. Fare clic su Genera per generare un nuovo certificato SSL. Viene visualizzata una finestra di conferma.



Passaggio 2. Fare clic su OK per continuare la generazione del certificato SSL. Dopo la generazione del certificato, nell'area Stato file certificato SSL vengono visualizzate le informazioni seguenti:

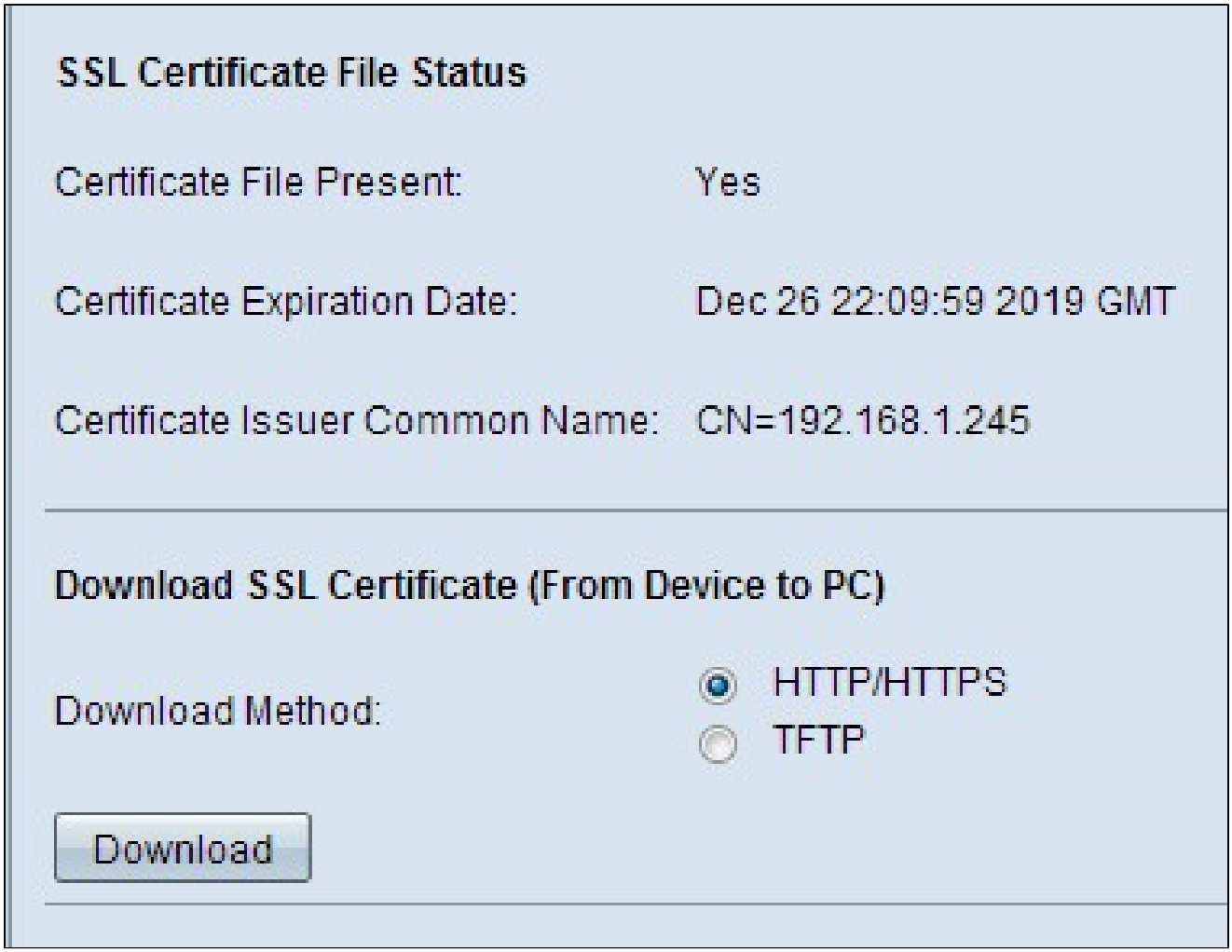
· File di certificato presente - indica se il file di certificato SSL HTTP è presente o meno.

· Data scadenza certificato: visualizza la data di scadenza del certificato SSL HTTP corrente.

· Nome comune autorità di certificazione - Visualizza il nome comune dell'autorità di certificazione corrente.

Scarica il certificato SSL

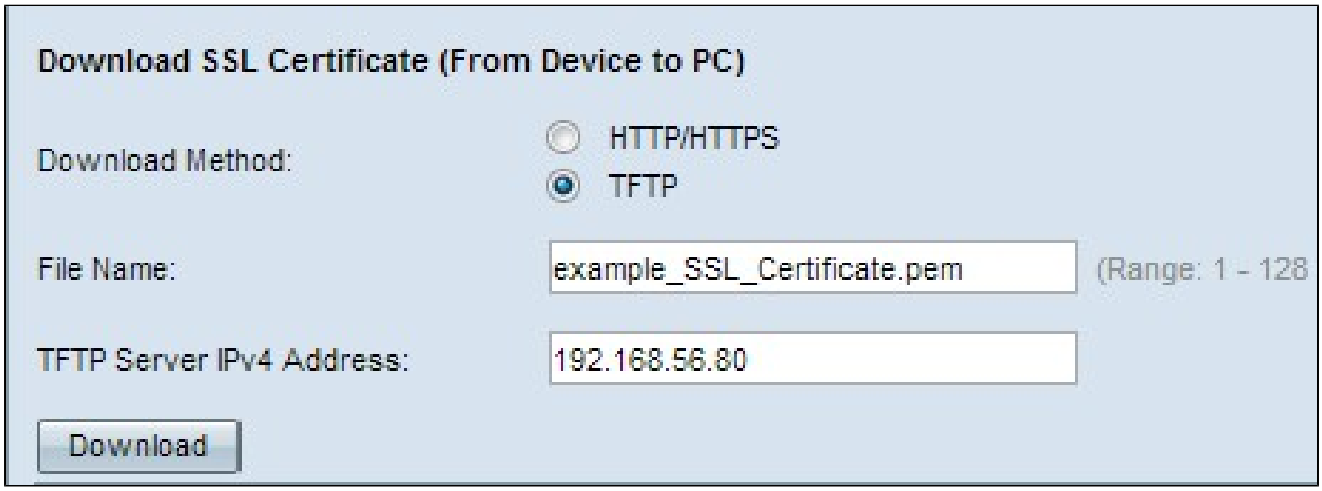
Di seguito viene descritto come scaricare il certificato SSL (un file con estensione pem) dal dispositivo al PC come backup.



Passaggio 1. Fare clic sul pulsante di opzione corrispondente al metodo di download desiderato nell'area Scarica certificato SSL.

· HTTP/HTTPS: consente di scaricare il certificato SSL da un server Web. Andare al passo 4 se si sceglie HTTP/HTTPS.

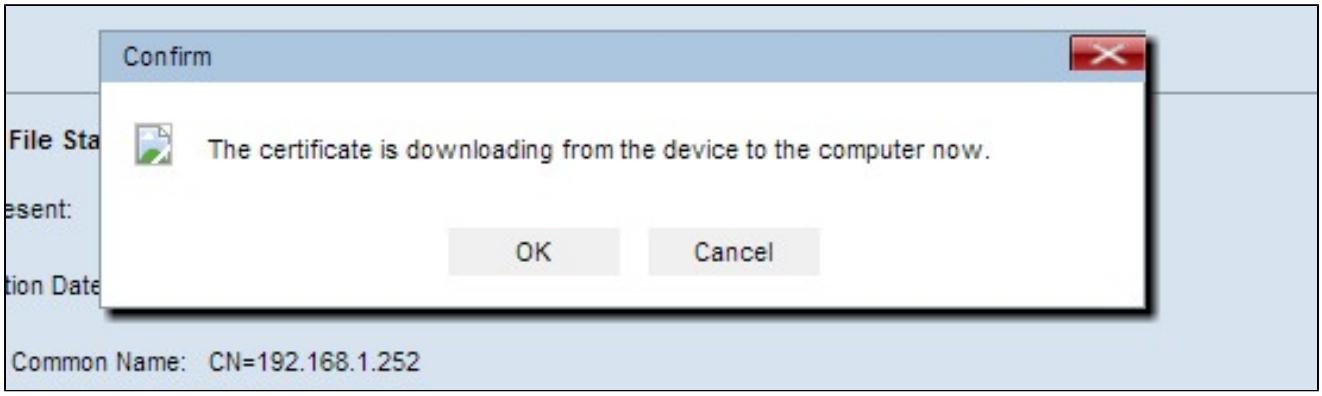
· TFTP: consente di scaricare il certificato SSL da un server TFTP. Se si sceglie questa opzione, vengono visualizzati i campi Nome file e Indirizzo IPv4 server TFTP.



Passaggio 2. Se nel passaggio 1 è stato scelto TFTP, immettere il nome del file nel campo Nome file. Si tratta di un file di tipo certificato con estensione pem.

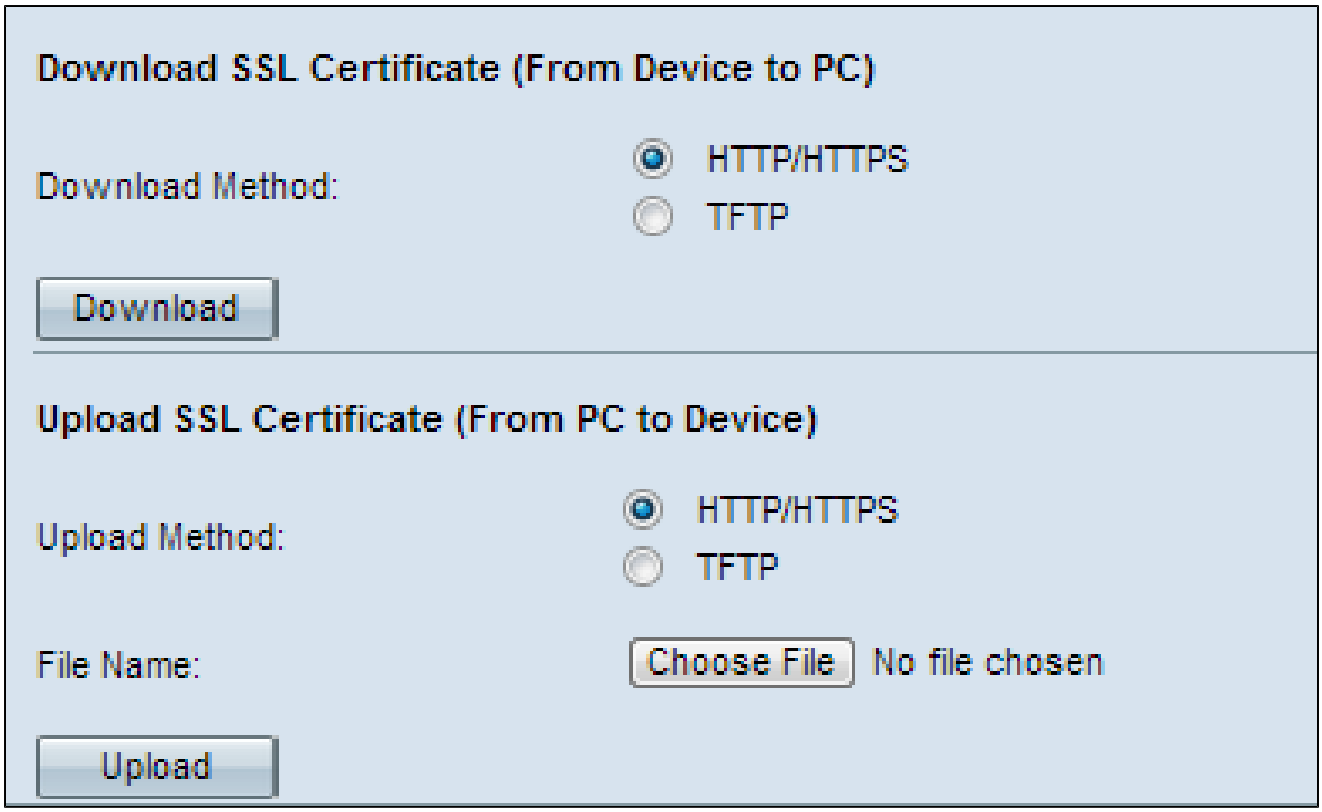
Passaggio 3. Se nel passaggio 1 è stato scelto TFTP, immettere l'indirizzo IP del server TFTP nel campo Indirizzo IPv4 server TFTP.

Passaggio 4. Fare clic su Download per scaricare il file del certificato. Viene visualizzata una finestra di conferma.



Passaggio 5. Fare clic su OK per continuare il download.

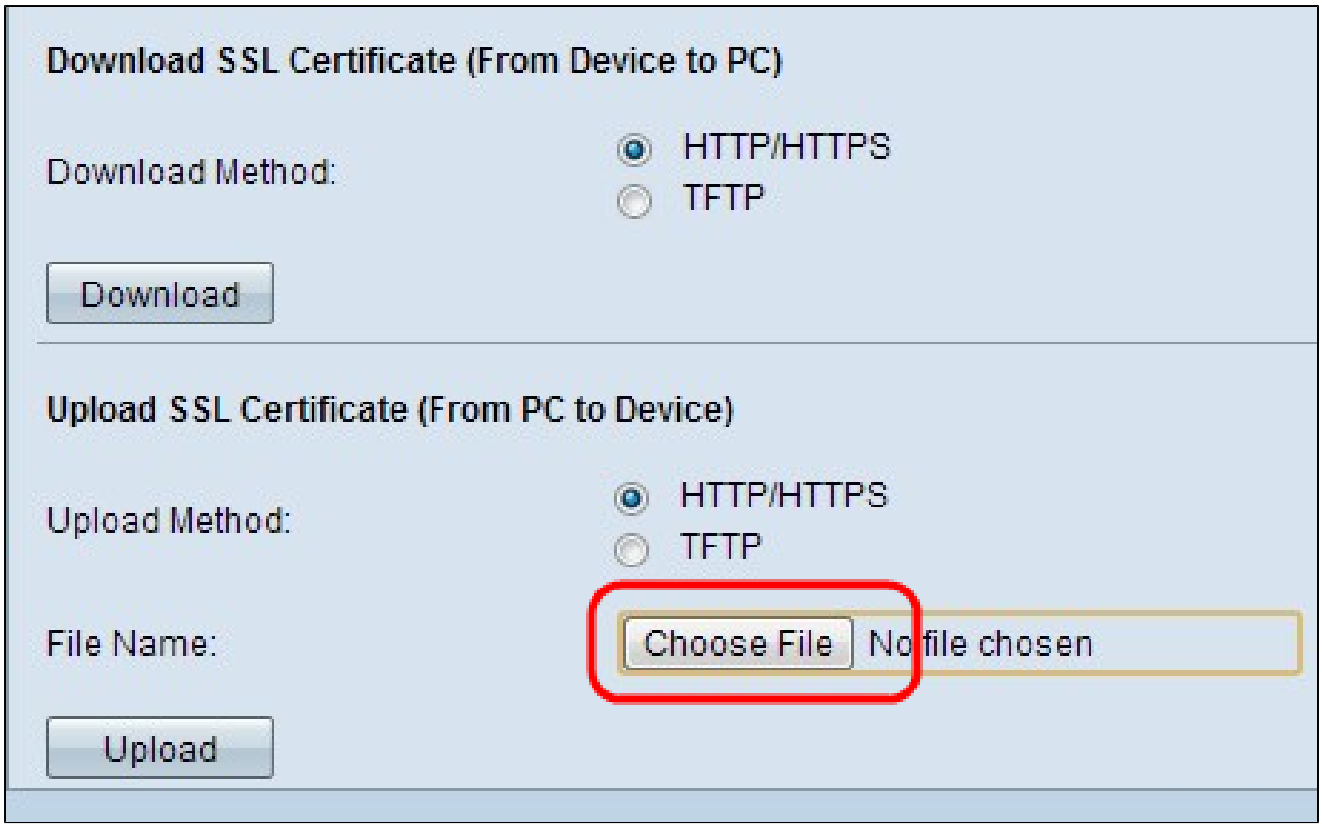
Carica il certificato SSL



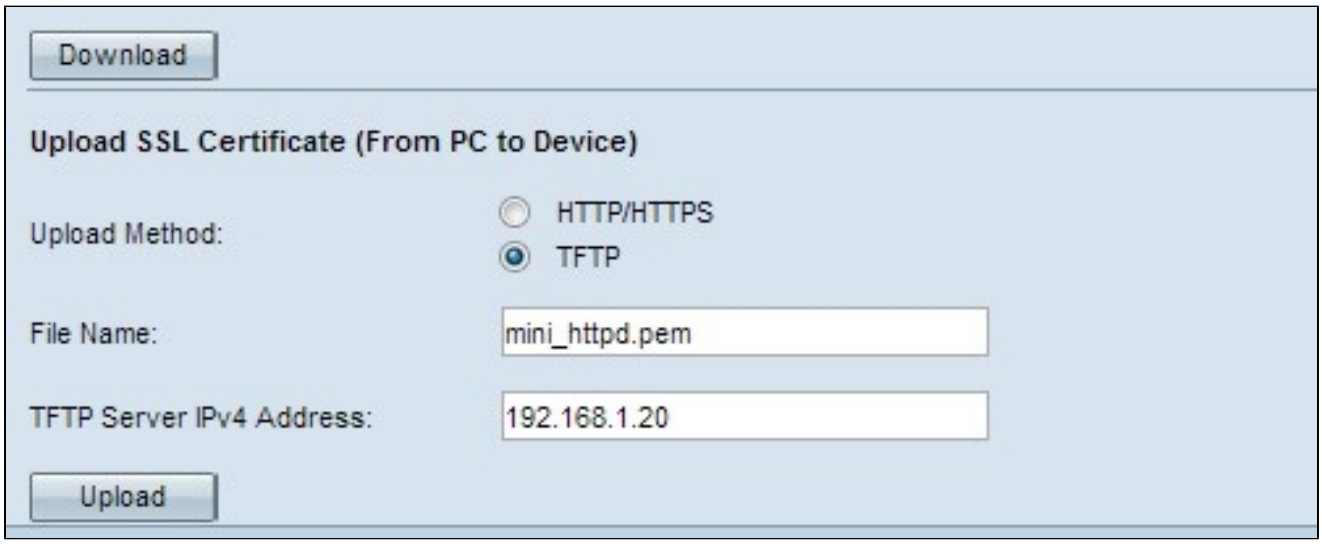
Passaggio 1. Fare clic sul pulsante di opzione HTTP/HTTPS o TFTP per scegliere il metodo di caricamento desiderato nell'area Carica certificato SSL.

· HTTP/HTTPS: consente il caricamento del certificato con un server Web. Se si sceglie HTTP/HTTPS, completare il passaggio 2 e quindi ignorare il passaggio 3.

· TFTP: consente di caricare il certificato SSL tramite un server TFTP. Se si sceglie questa opzione, vengono visualizzati i campi Nome file e Indirizzo IPv4 server TFTP. Ignorare il passaggio 2 ed eseguire il passaggio 3.

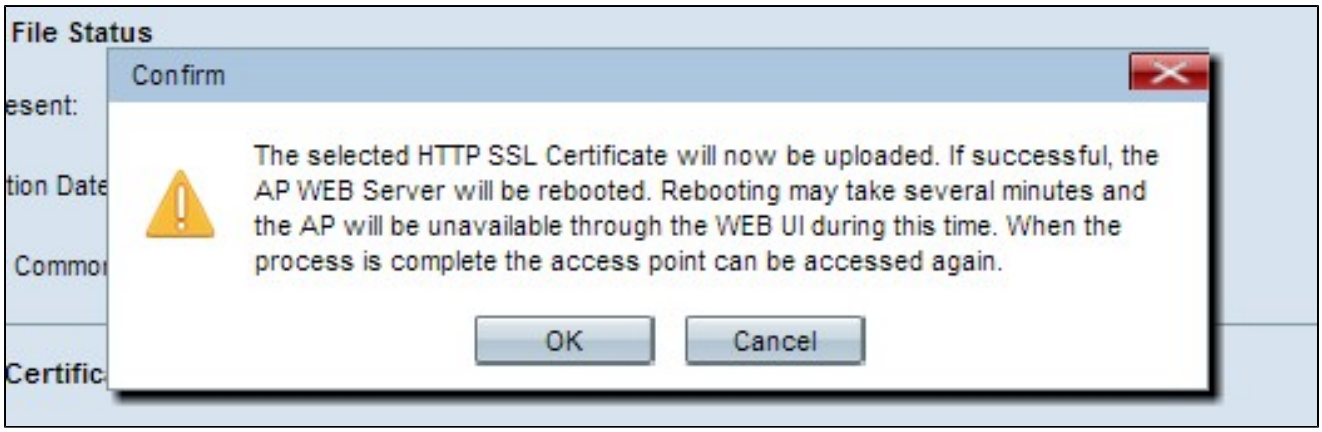


Passaggio 2. Fare clic su Scegli file per sfogliare e selezionare il file.



Passaggio 3. Immettere il nome del file nel campo Nome file e l'indirizzo del server TFTP nel campo Indirizzo IPv4 server TFTP.

Passaggio 4. Fare clic su Upload per caricare il file del certificato. Viene visualizzata una finestra di conferma.



Passaggio 5. Fare clic su OK per continuare il caricamento.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).