Configurazione delle impostazioni del supporto 802.1X su WAP131 e WAP371

Obiettivo

L'autenticazione IEEE 802.1X consente al dispositivo WAP di accedere a una rete cablata protetta. È possibile abilitare il dispositivo WAP come supplicant 802.1X (client) sulla rete cablata. È possibile configurare un nome utente e una password crittografati per consentire l'autenticazione del dispositivo WAP utilizzando 802.1X.

Nelle reti che utilizzano il controllo degli accessi alla rete basato sulle porte IEEE 802.1X, un supplicant non può accedere alla rete finché l'autenticatore 802.1X non concede l'accesso. Se la rete utilizza 802.1X, è necessario configurare le informazioni di autenticazione 802.1X sul dispositivo WAP in modo che possa fornirle all'autenticatore.

L'obiettivo di questo documento è mostrare come configurare le impostazioni 802.1X Supplicant su WAP131 e WAP371.

Dispositivi interessati

·WAP131

·WAP371

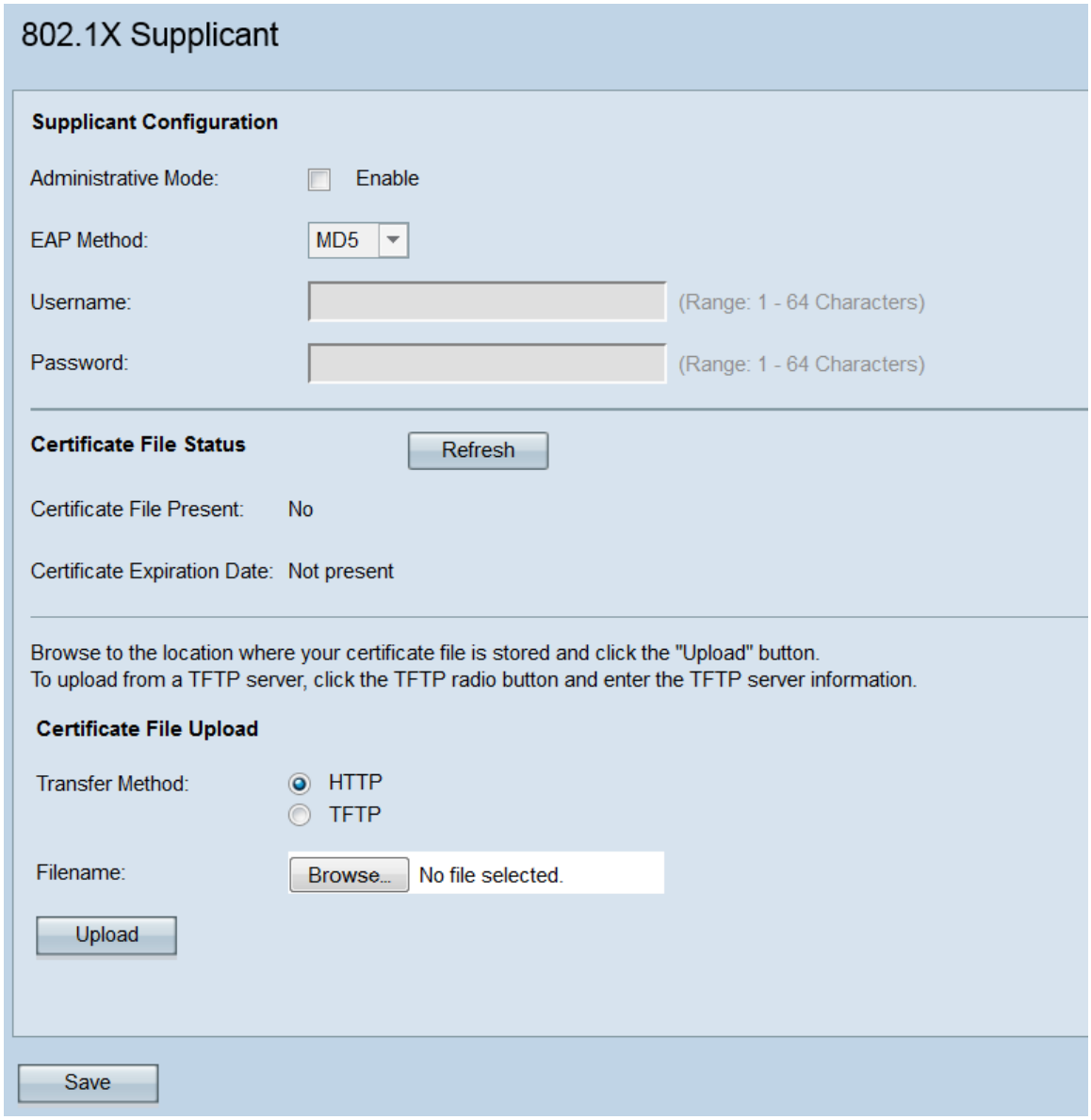
Versione del software

·v1.0.0.39 (WAP131)

·v1.2.0.2 (WAP371)

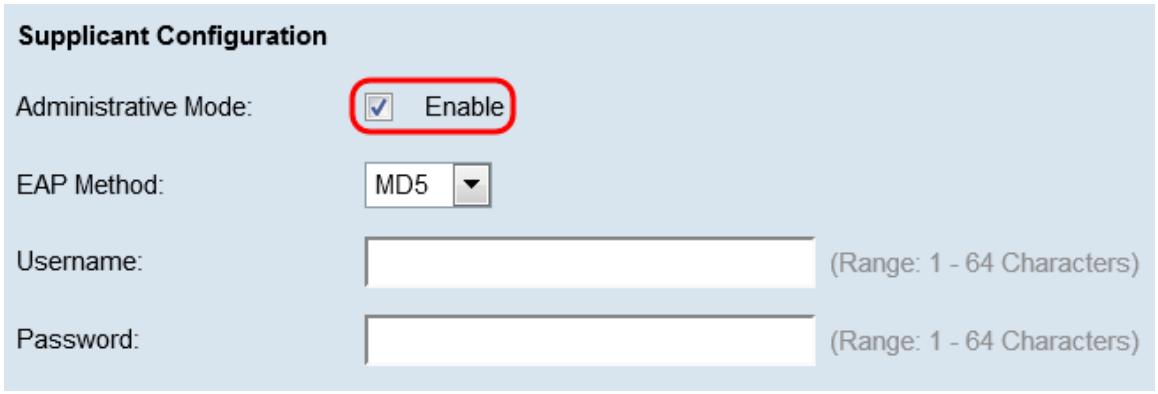
Configurazione Delle Impostazioni Del Supplicant 802.1X

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Protezione sistema > Supplicant 802.1X**. Viene visualizzata la pagina *802.1X Supplicant*.

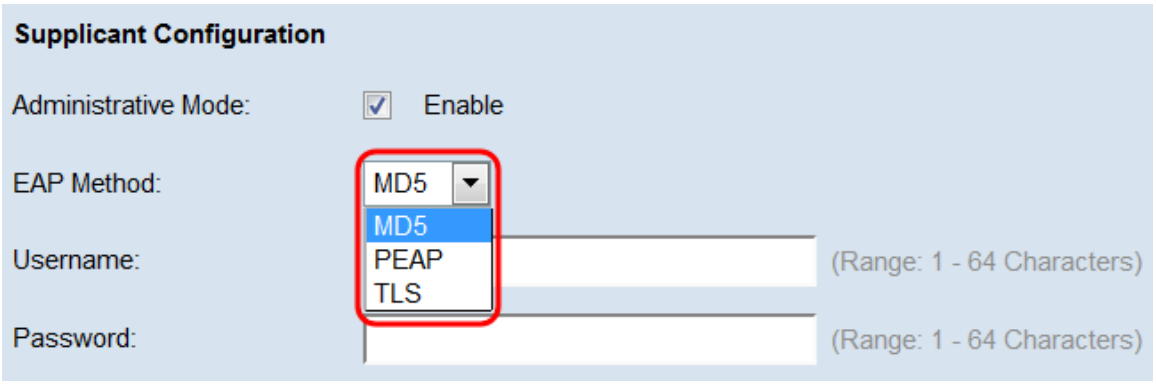


Configurazione supplicant

Passaggio 1. Passare all'area *Configurazione supplicant*. Nel campo *Modalità amministrativa* , selezionare la casella di controllo **Attiva** per abilitare la funzionalità 802.1X supplicant.



Passaggio 2. Nell'elenco a discesa *Metodo EAP*, scegliere l'algoritmo che verrà utilizzato per crittografare i nomi utente e le password. EAP è l'acronimo di Extensible Authentication Protocol ed è utilizzato come base per gli algoritmi di crittografia.



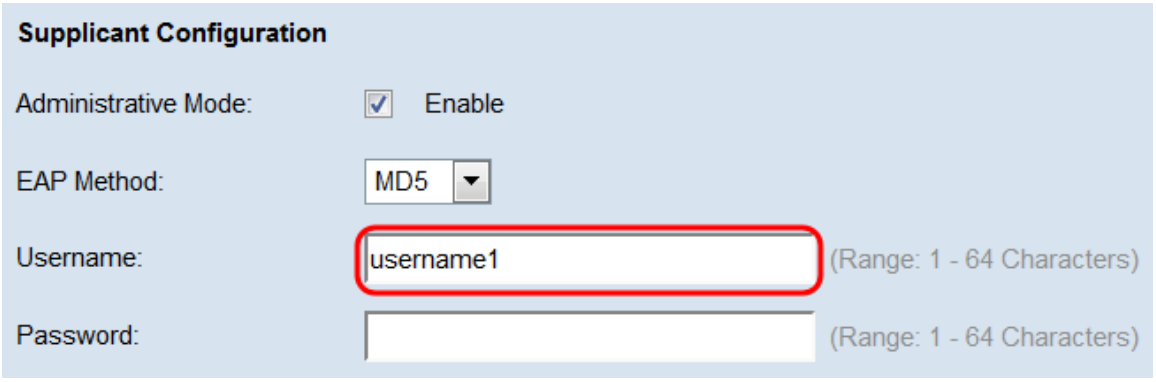
Le opzioni disponibili sono:

·MD5: l'algoritmo MD5 message-digest utilizza una funzione hash per fornire la sicurezza di base. Questo algoritmo non è consigliato, in quanto gli altri due hanno una protezione più elevata.

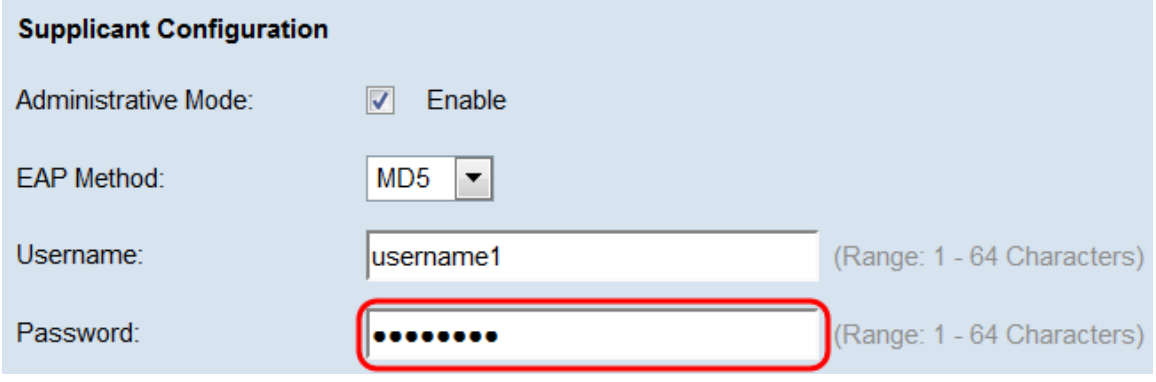
·PEAP: PEAP è l'acronimo di Protected Extensible Authentication Protocol. Incapsula il protocollo EAP e offre una sicurezza maggiore rispetto a MD5, utilizzando un tunnel TLS per trasmettere i dati.

·TLS: TLS è l'acronimo di Transport Layer Security ed è uno standard aperto che fornisce un alto livello di sicurezza.

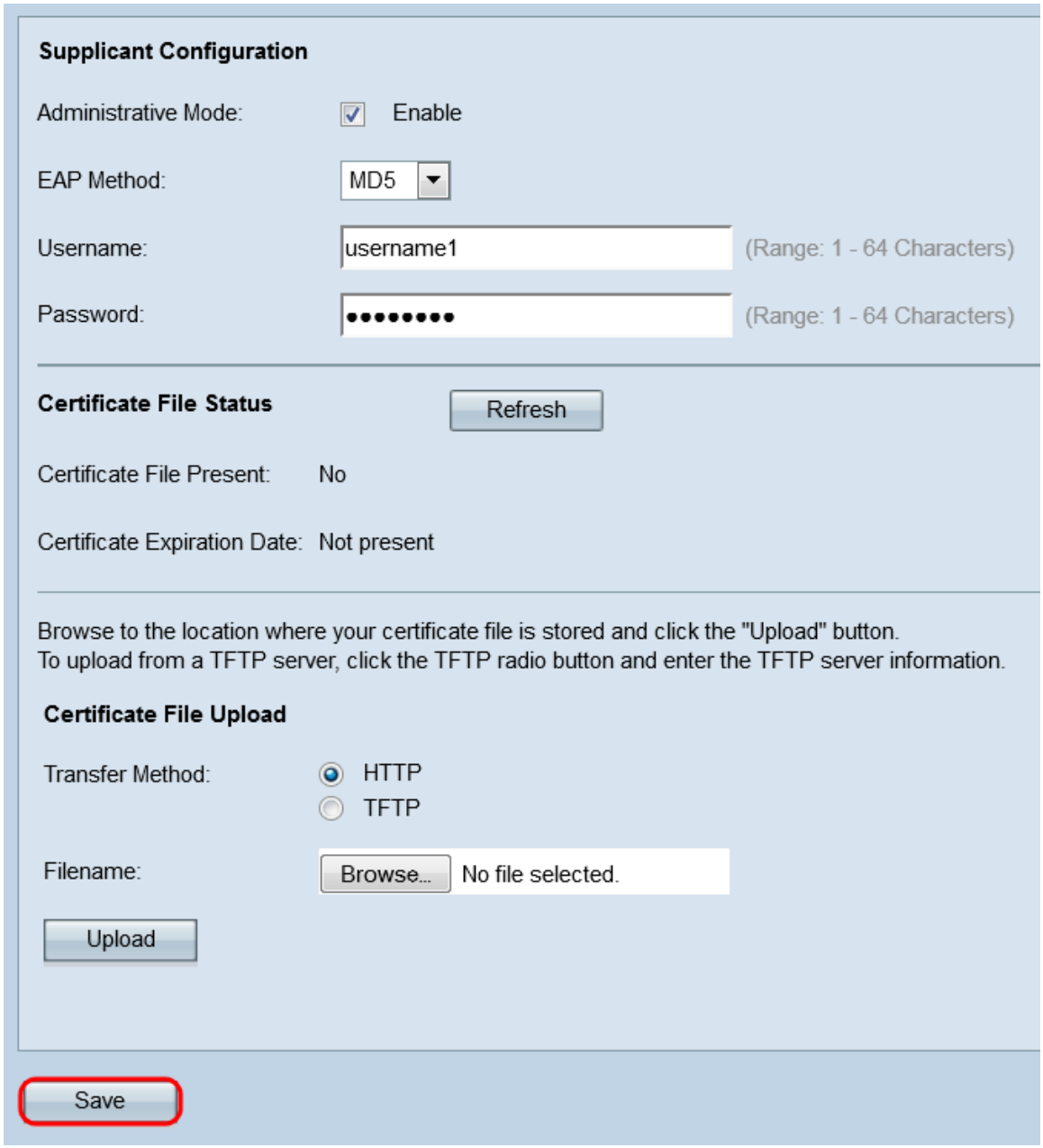
Passaggio 3. Nel campo *Username*, immettere il nome utente che il dispositivo WAP utilizzerà per rispondere alle richieste di un autenticatore 802.1X. Il nome utente deve avere una lunghezza compresa tra 1 e 64 caratteri e può includere caratteri alfanumerici e speciali.



Passaggio 4. Nel campo *Password*, immettere la password che il dispositivo WAP utilizzerà per rispondere alle richieste di un autenticatore 802.1X. Il nome utente deve avere una lunghezza compresa tra 1 e 64 caratteri e può includere caratteri alfanumerici e speciali.

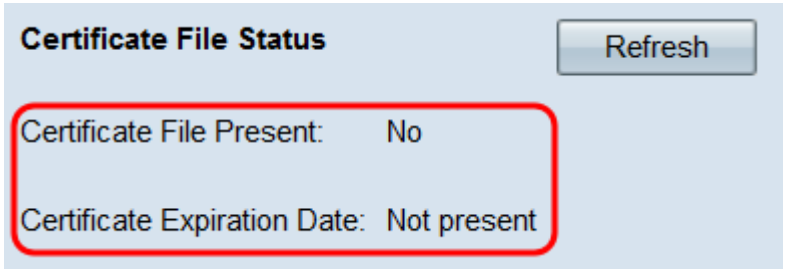


Passaggio 5. Fare clic su **Salva**.

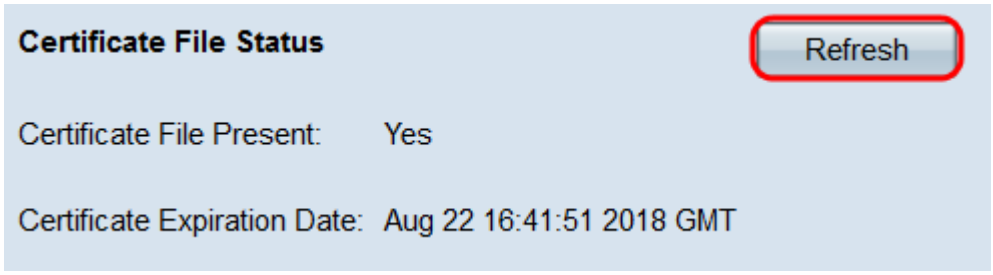


Stato file certificato

Passaggio 1. Passare all'area *Stato file certificato*. In quest'area viene indicato se il dispositivo WAP contiene un file di certificato SSL HTTP. Nel campo *File certificato presente* verrà visualizzato "Sì" se è presente un certificato. il valore predefinito è "No". Se è presente un certificato, la *data di scadenza* del *certificato* sarà indicata al momento della scadenza; in caso contrario, il valore predefinito è "Not presence" (Non presente).

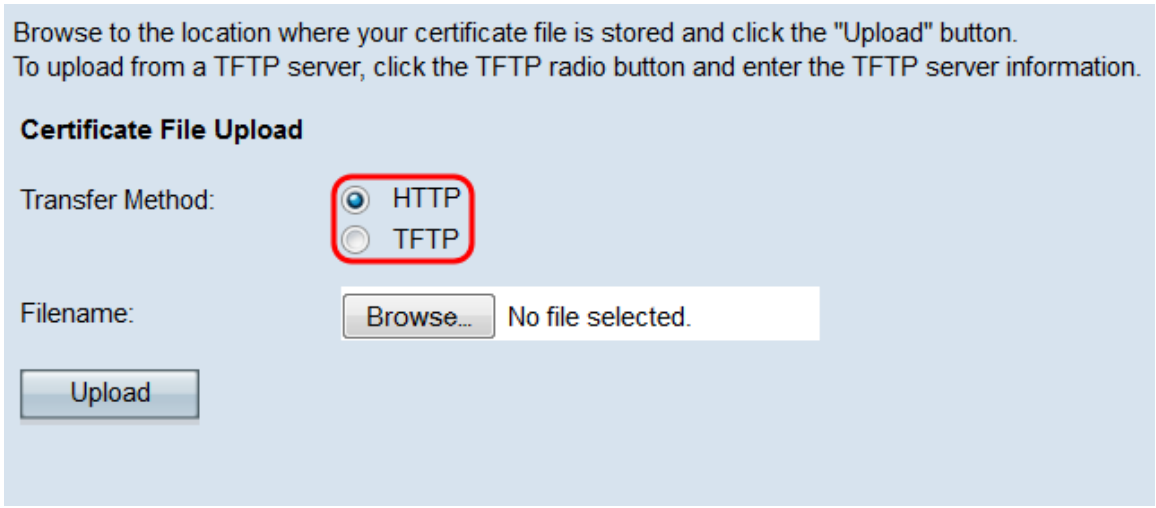


Passaggio 2. Per visualizzare le informazioni più recenti, fare clic sul pulsante **Aggiorna** per ottenere le informazioni più aggiornate sul certificato.

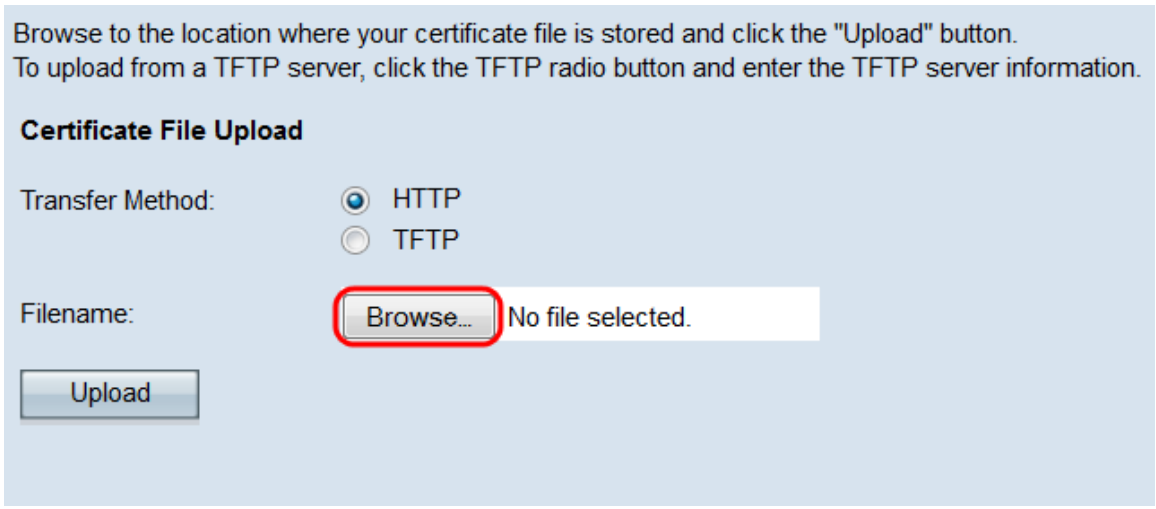


Caricamento file di certificato

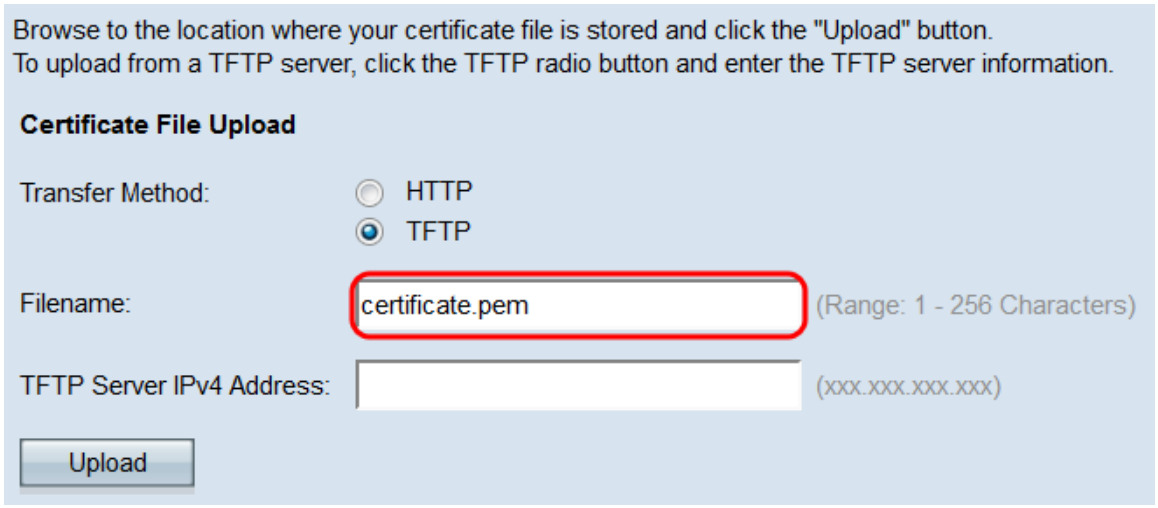
Passaggio 1. Passare all'area di *caricamento dei file di certificato* per caricare un certificato HTTP SSL nel dispositivo WAP. Nel campo *Metodo di trasferimento*, selezionare i pulsanti di opzione **HTTP** o **TFTP** per scegliere il protocollo da utilizzare per caricare il certificato.



Passaggio 2. Se è stato selezionato **TFTP**, passare al Passaggio 3. Se è stato selezionato **HTTP**, fare clic sul pulsante **Sfoglia...** per trovare il file del certificato sul PC. Andare al passo 5.

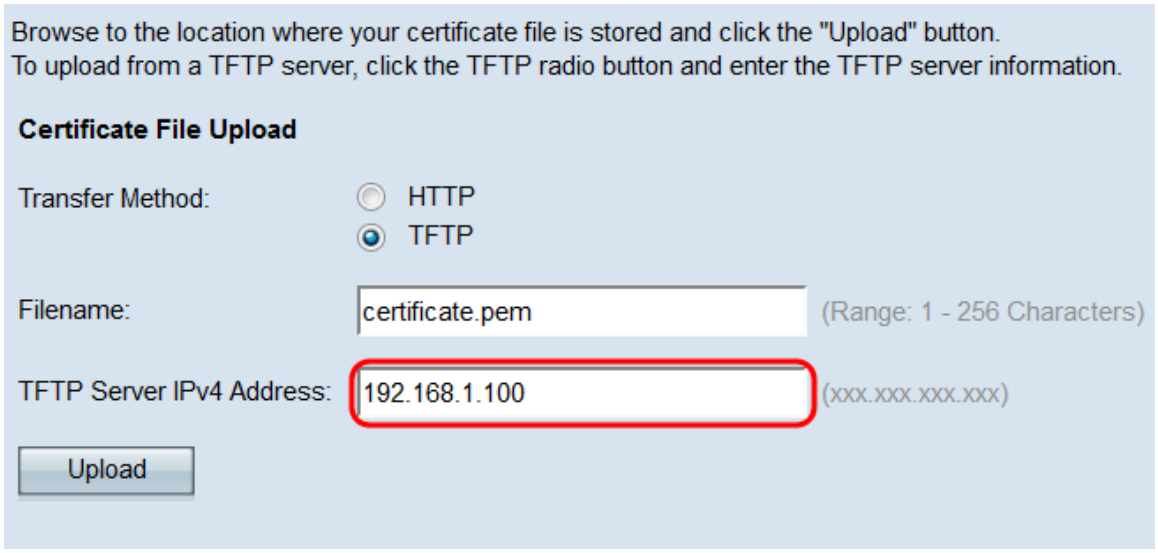


Passaggio 3. Se è stato selezionato **TFTP** nel campo *Metodo di trasferimento*, immettere nel nome file del certificato il nome file nel campo *Nome file*.

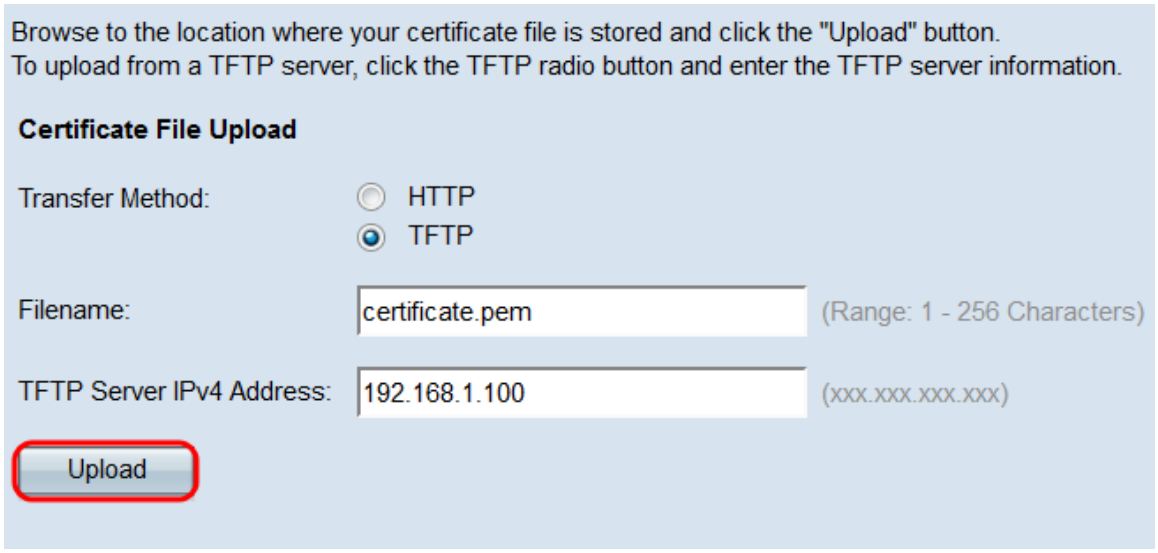


Nota: Il file deve terminare con .pem.

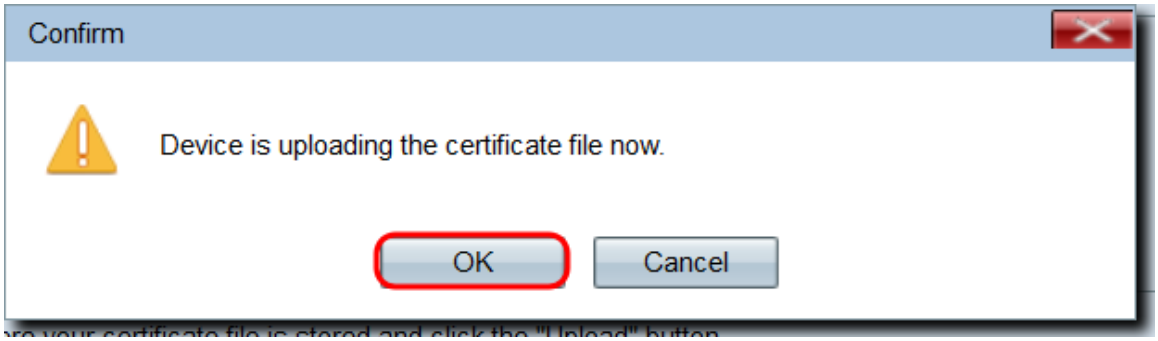
Passaggio 4. Immettere l'indirizzo IP del server TFTP nel campo *Indirizzo IPv4 server TFTP*.



Passaggio 5. Fare clic su **Upload**.



Passaggio 6. Viene visualizzata una finestra di conferma. Fare clic su **OK** per avviare il caricamento.



Passaggio 7. Fare clic su **Salva**.