Configuring 802.1X Supplicant Settings on the WAP131 and WAP371

Objective

IEEE 802.1X authentication enables the WAP device to gain access to a secured wired network. You can enable the WAP device as an 802.1X supplicant (client) on the wired network. An encrypted user name and password can be configured to allow the WAP device to authenticate using 802.1X.

On the networks that use IEEE 802.1X port-based network access control, a supplicant cannot gain access to the network until the 802.1X authenticator grants access. If your network uses 802.1X, you must configure 802.1X authentication information on the WAP device, so that it can supply it to the authenticator.

The objective of this document is to show you how to configure 802.1X Supplicant settings on the WAP131 and WAP371.

Applicable Devices

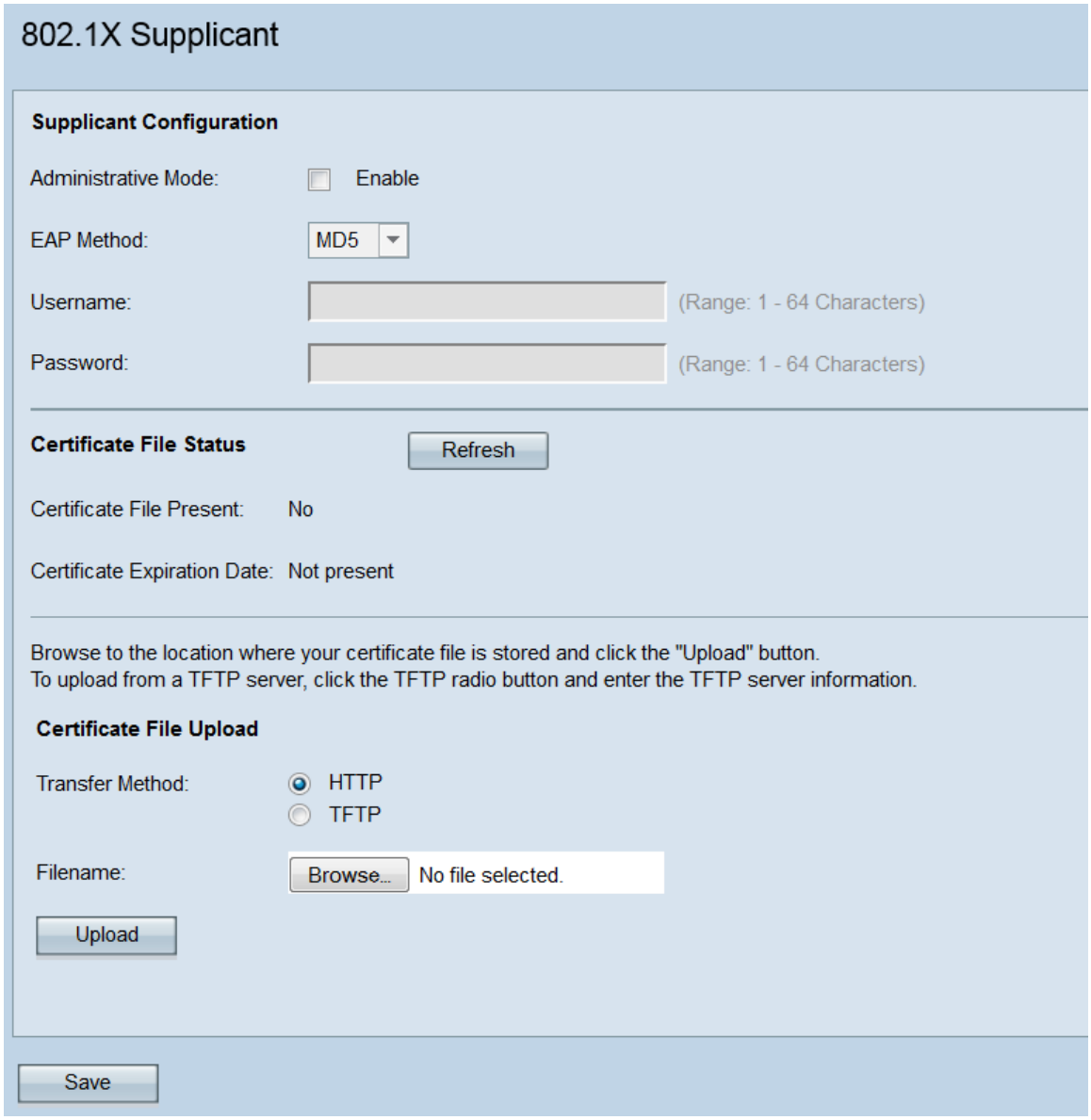
- WAP131
- WAP371

Software Version

- v1.0.0.39 (WAP131)
- v1.2.0.2 (WAP371)

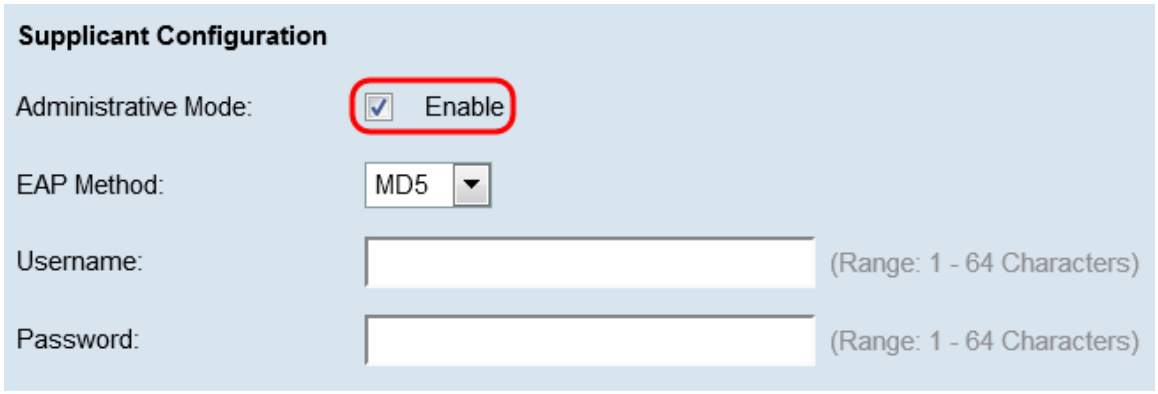
Configuring 802.1X Supplicant Settings

Step 1. Log in to the web configuration utility and choose **System Security > 802.1X Supplicant**. The *802.1X Supplicant* page opens.

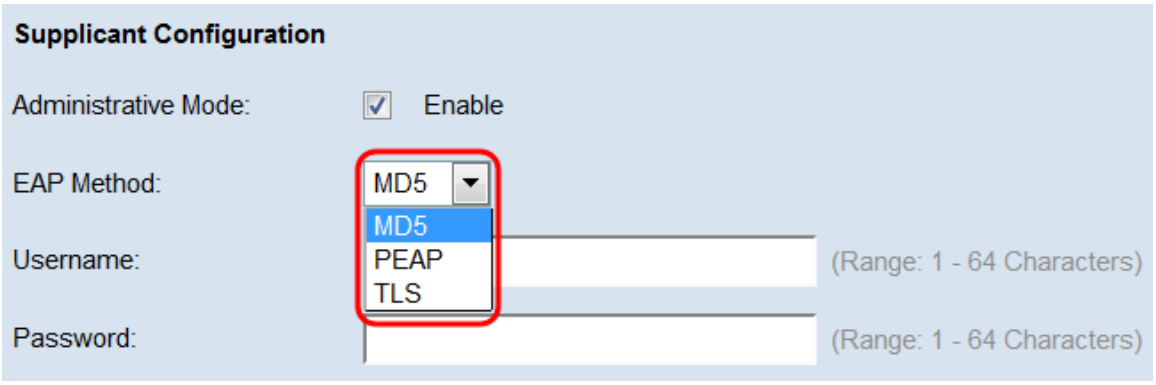


Supplicant Configuration

Step 1. Navigate to the *Supplicant Configuration* area. In the *Administrative Mode* field, check the **Enable** checkbox to enable 802.1X supplicant functionality.



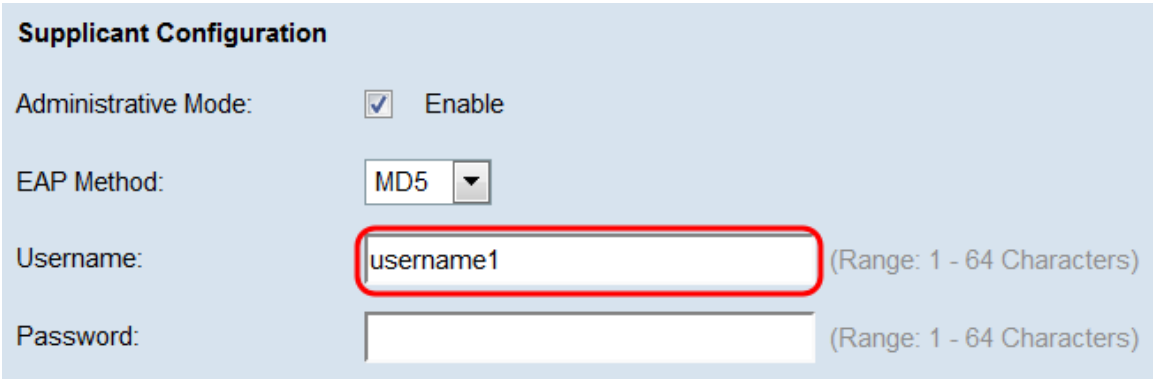
Step 2. In the *EAP Method* drop-down list, choose the algorithm that will be used to encrypt usernames and passwords. EAP stands for Extensible Authentication Protocol, and is used as a basis for encryption algorithms.



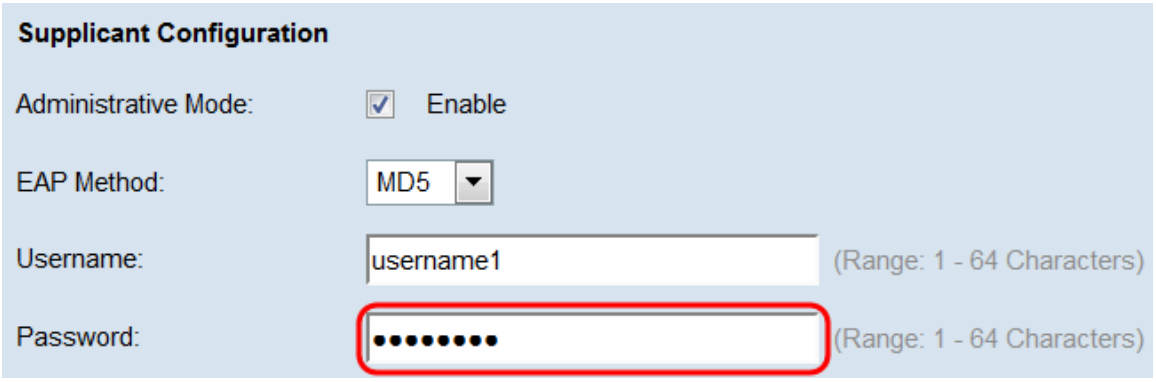
The available options are:

- MD5 — The MD5 message-digest algorithm utilizes a hash function to provide basic security. This algorithm is not recommended, as the other two have higher security.
- PEAP — PEAP stands for Protected Extensible Authentication Protocol. It encapsulates EAP and provides higher security than MD5 by using a TLS tunnel to transmit data.
- TLS — TLS stands for Transport Layer Security, and is an open standard that provides high security.

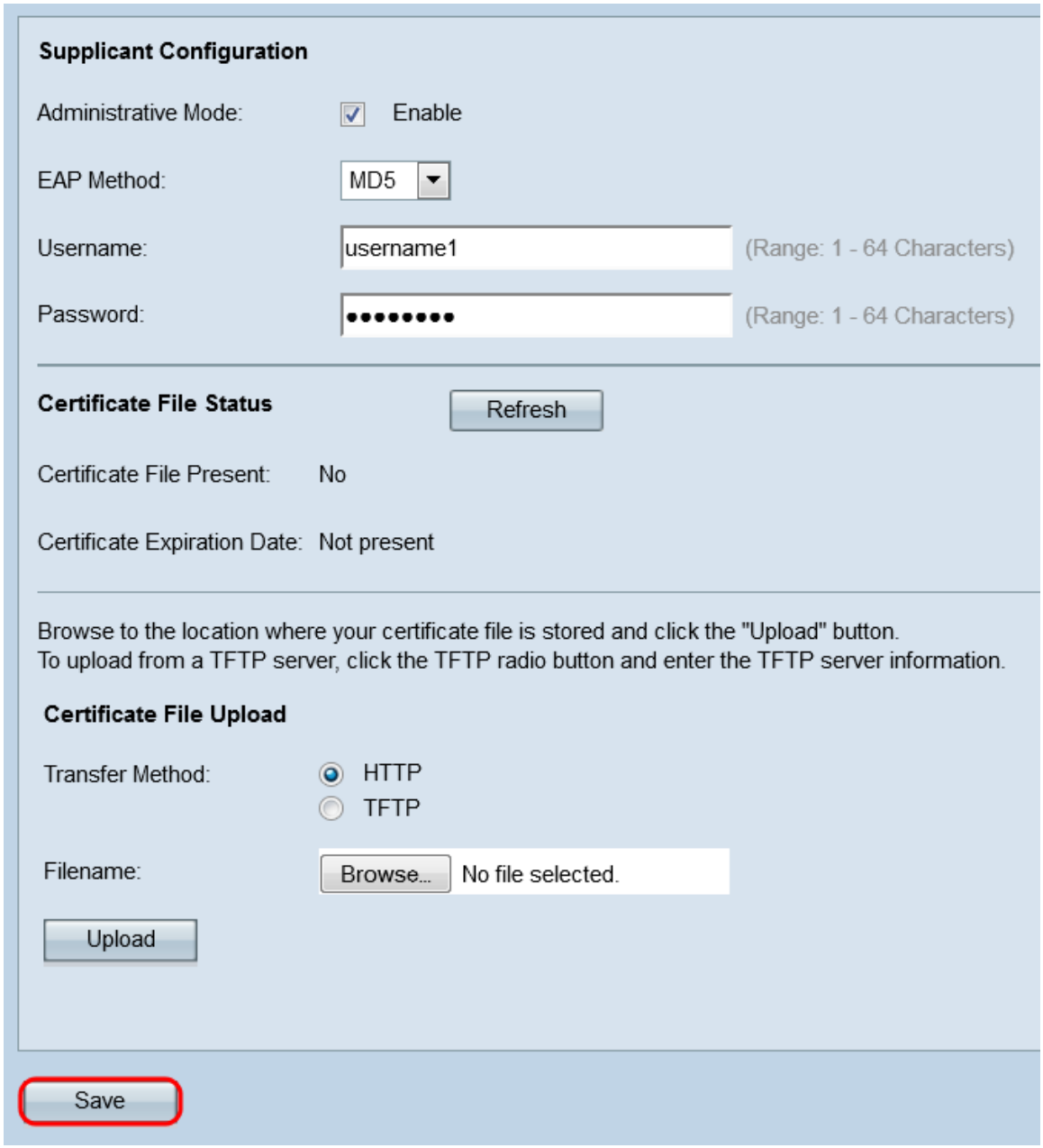
Step 3. In the *Username* field, enter in the username that the WAP device will use when responding to requests from an 802.1X authenticator. The username must be 1 – 64 characters long, and can include alphanumeric and special characters.



Step 4. In the *Password* field, enter in the password that the WAP device will use when responding to requests from an 802.1X authenticator. The username must be 1 - 64 characters long, and can include alphanumeric and special characters.

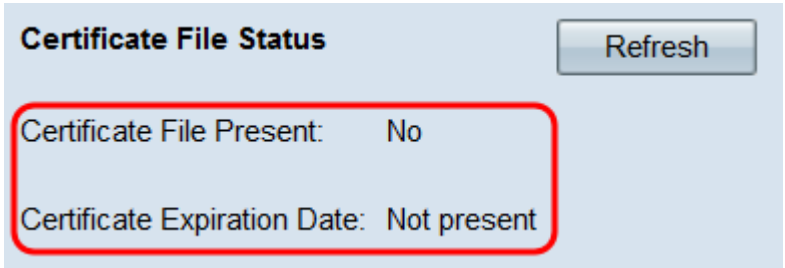


Step 5. Click **Save**.

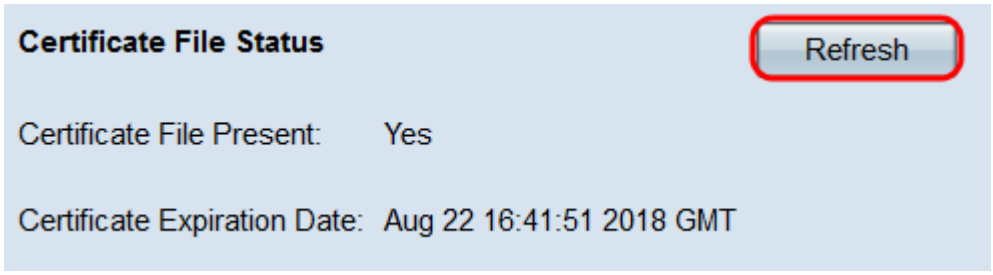


Certificate File Status

Step 1. Navigate to the *Certificate File Status* area. This area shows whether an HTTP SSL certificate file exists on the WAP device. The *Certificate File Present* field will show “Yes” if a certificate is present; the default is “No”. If a certificate is present, the *Certificate Expiration Date* will show when it expires; otherwise, the default is “Not present”.

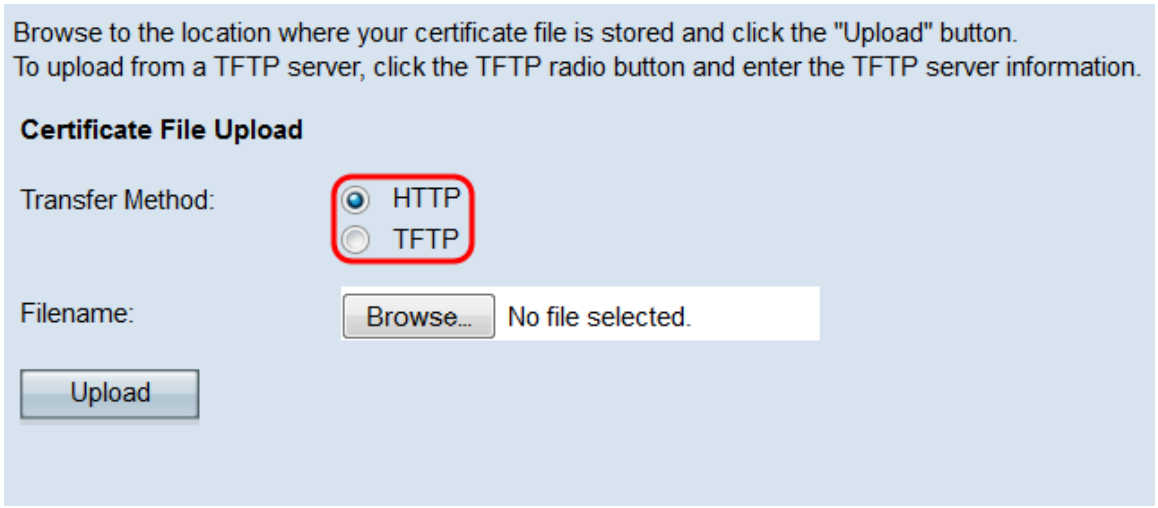


Step 2. To display the latest information, click the **Refresh** button to get the most current certificate information.

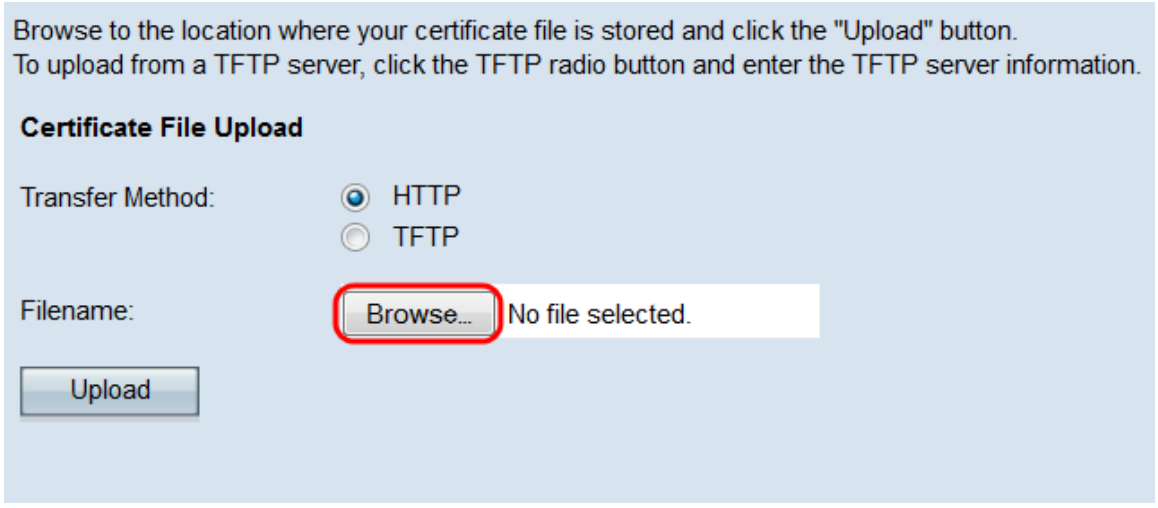


Certificate File Upload

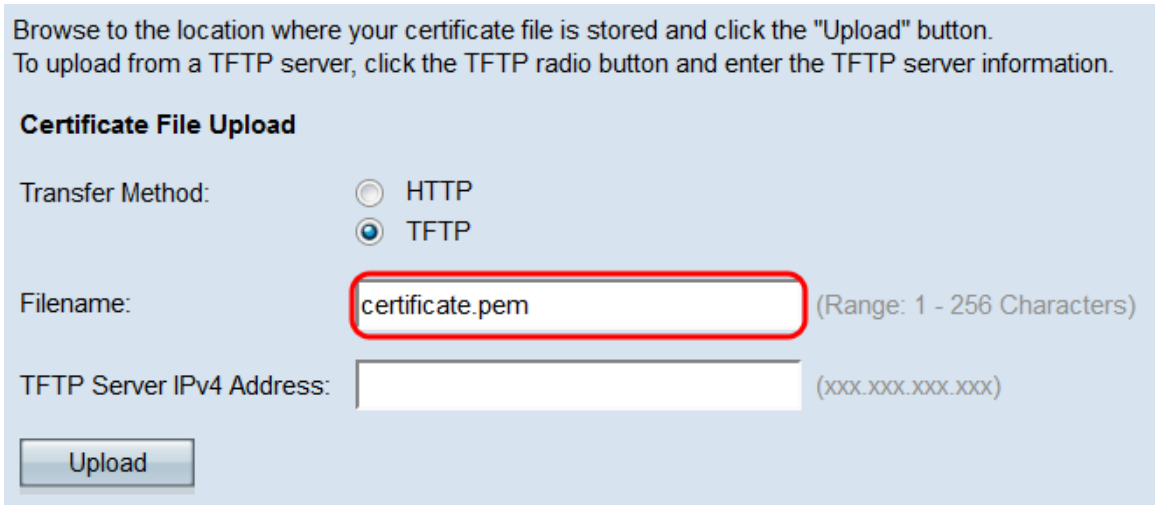
Step 1. Navigate to the *Certificate File Upload* area to upload an HTTP SSL certificate to the WAP device. In the *Transfer Method* field, select either the **HTTP** or **TFTP** radio buttons to choose which protocol you want to use to upload the certificate.



Step 2. If you selected **TFTP**, continue to Step 3. If you selected **HTTP**, click the **Browse…** button to find the certificate file on your PC. Skip to Step 5.

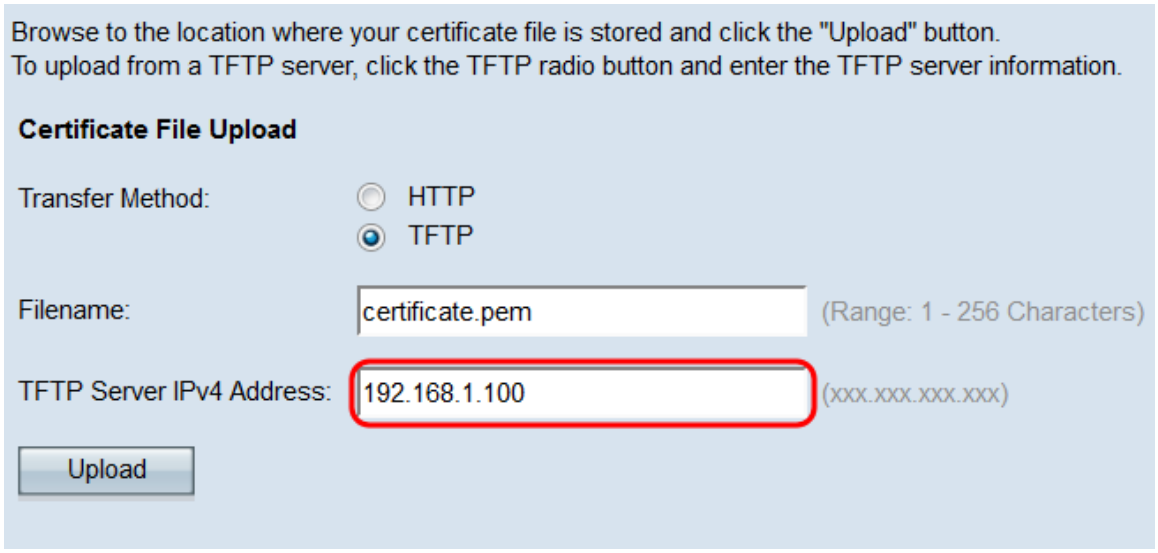


Step 3. If you selected **TFTP** in the *Transfer Method* field, enter in the filename of the certificate in the *Filename* field.

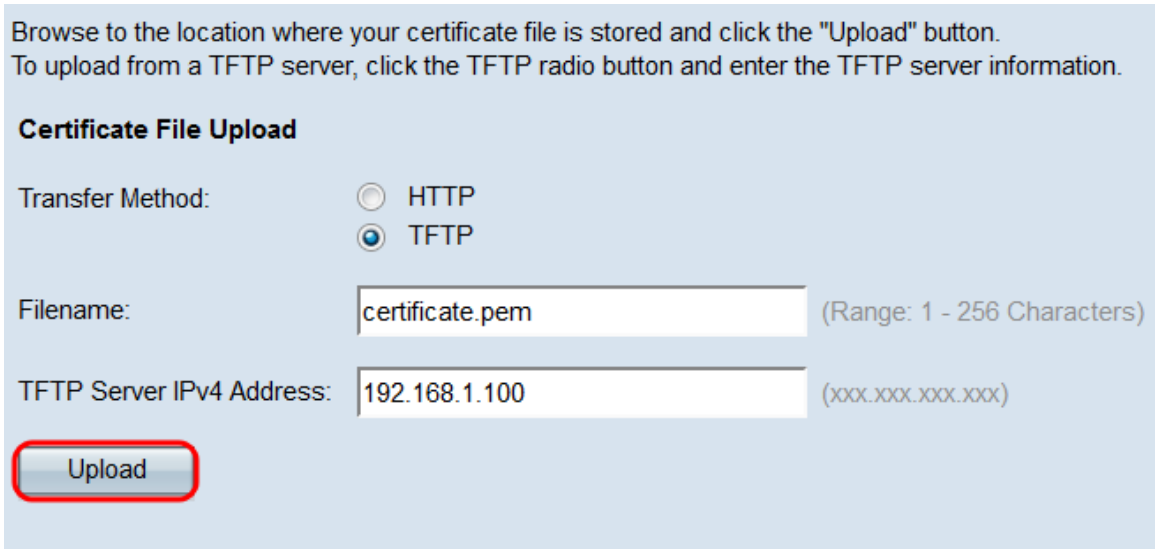


Note: The file must end in .pem.

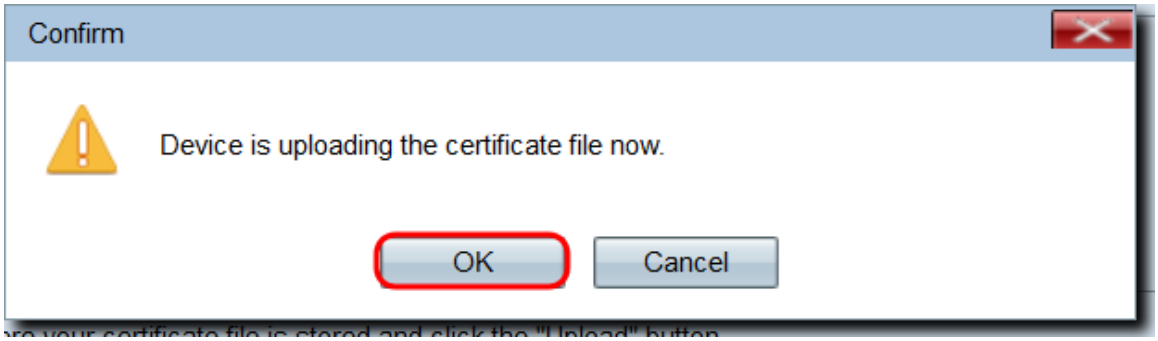
Step 4. Enter the IP address of the TFTP server in the *TFTP Server IPv4 Address* field.



Step 5. Click **Upload**.



Step 6. A confirmation window appears. Click **OK** to begin the upload.



Step 7. Click **Save**.