Konfigurieren der 802.1X-Komponenteneinstellungen auf dem WAP131 und WAP371

Ziel

Die IEEE 802.1X-Authentifizierung ermöglicht dem WAP-Gerät den Zugriff auf ein sicheres kabelgebundenes Netzwerk. Sie können das WAP-Gerät als 802.1X-Komponente (Client) im kabelgebundenen Netzwerk aktivieren. Ein verschlüsselter Benutzername und ein verschlüsseltes Kennwort können so konfiguriert werden, dass das WAP-Gerät mithilfe von 802.1X authentifiziert werden kann.

In Netzwerken, die IEEE 802.1X-Port-basierte Netzwerkzugriffskontrolle verwenden, kann eine Komponente erst dann auf das Netzwerk zugreifen, wenn der 802.1X-Authentifizierer Zugriff gewährt. Wenn Ihr Netzwerk 802.1X verwendet, müssen Sie 802.1X-Authentifizierungsinformationen auf dem WAP-Gerät konfigurieren, damit es es dem Authentifizierer zur Verfügung stellen kann.

In diesem Dokument wird erläutert, wie Sie die 802.1X-Komponenteneinstellungen auf dem WAP131 und dem WAP371 konfigurieren.

Anwendbare Geräte

WAP131

WAP371

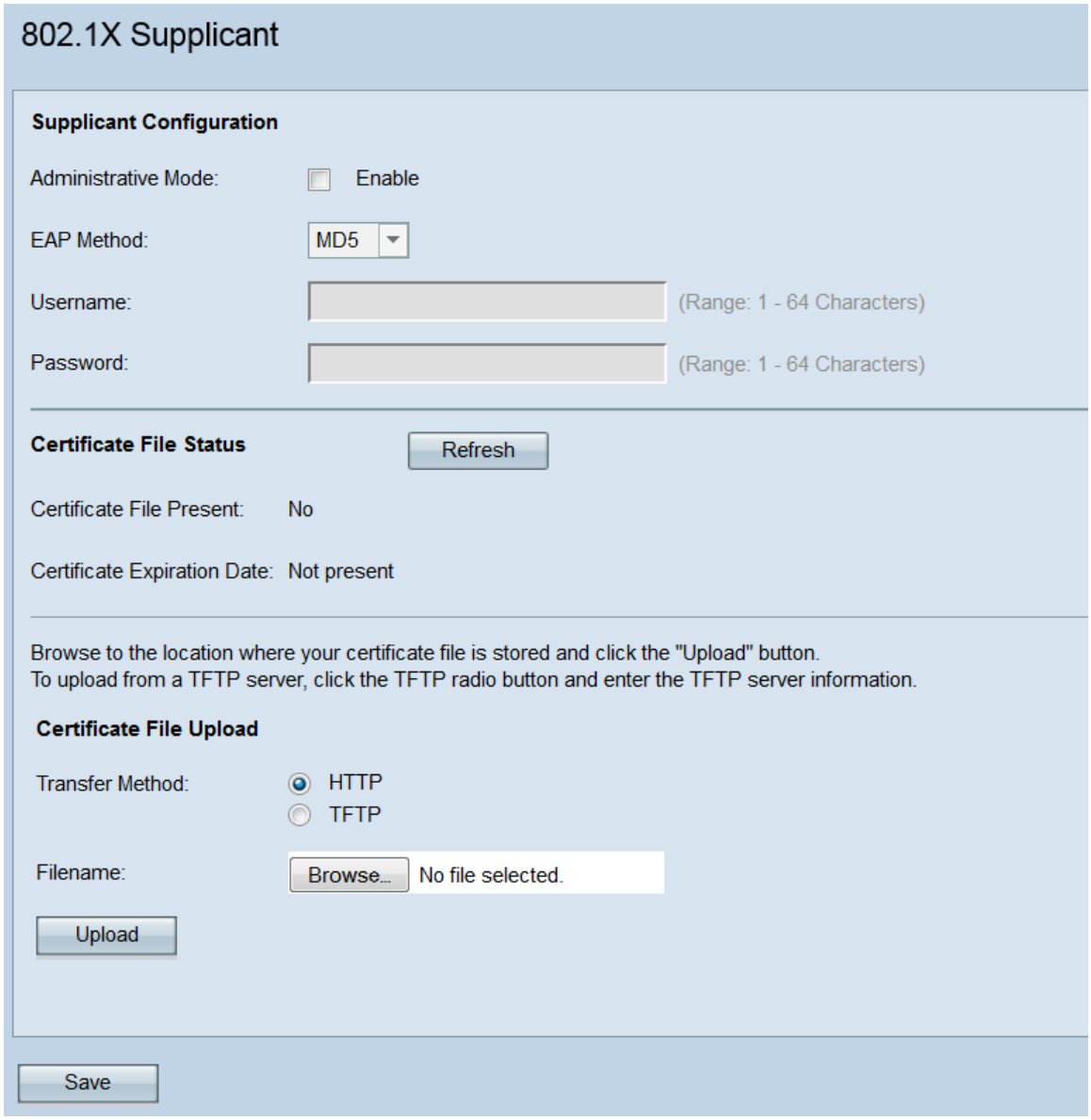
Softwareversion

·v1.0.0.39 (WAP131)

·v1.2.0.2 (WAP371)

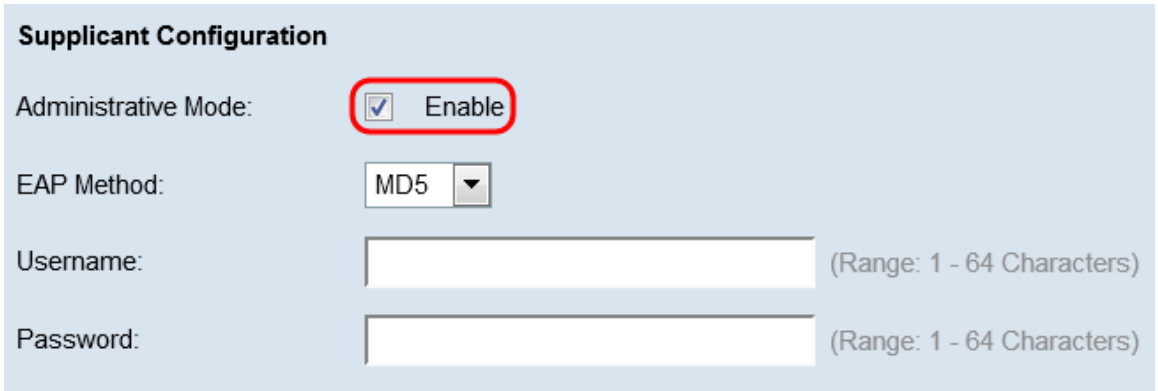
Konfigurieren der 802.1X-Komponenteneinstellungen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Systemsicherheit > 802.1X Supplicant aus**. Die Seite *802.1X Supplicant* wird geöffnet.

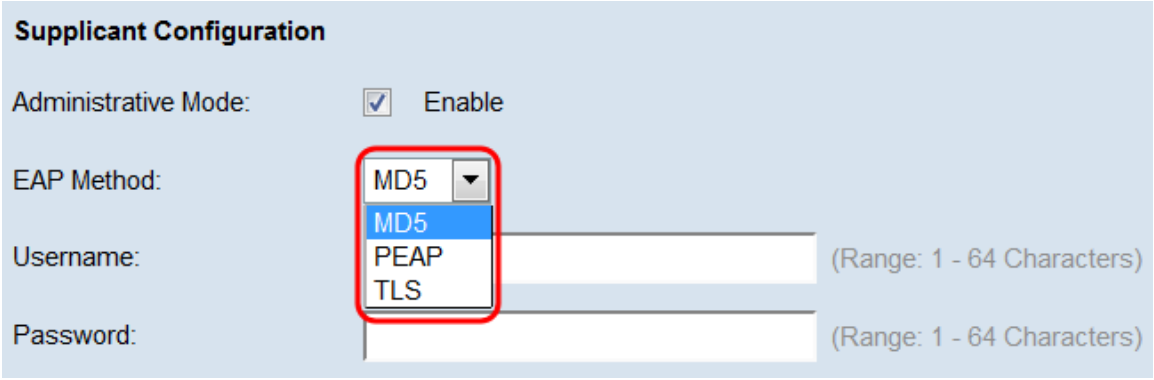


Supplicant-Konfiguration

Schritt 1: Navigieren Sie zum Bereich *Supplicant Configuration* (Komponentenkonfiguration). Aktivieren Sie im Feld *Verwaltungsmodus das* **Kontrollkästchen Aktivieren**, um die 802.1X-Komponentenfunktion zu aktivieren.



Schritt 2: Wählen Sie in der Dropdown-Liste *EAP Method* den Algorithmus aus, der zur Verschlüsselung von Benutzernamen und Kennwörtern verwendet wird. EAP steht für Extensible Authentication Protocol und wird als Grundlage für Verschlüsselungsalgorithmen verwendet.



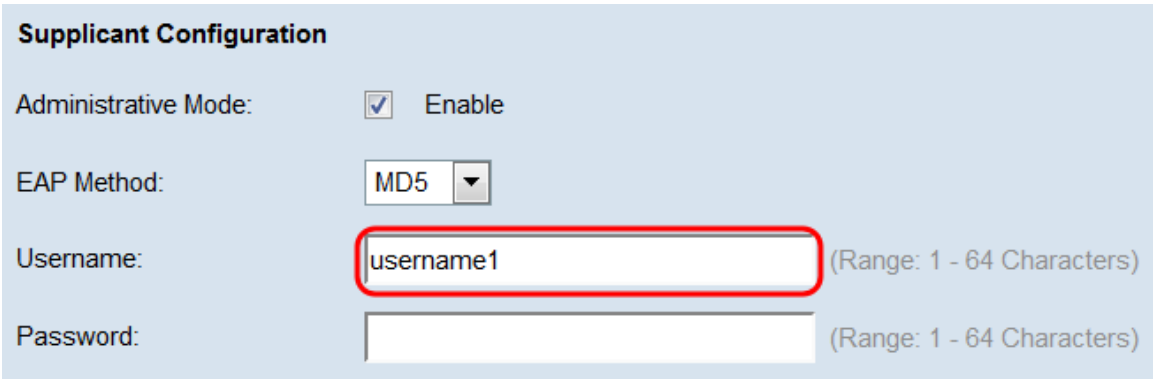
Folgende Optionen stehen zur Verfügung:

·MD5 - Der MD5-Message-Digest-Algorithmus verwendet eine Hash-Funktion, um grundlegende Sicherheit zu gewährleisten. Dieser Algorithmus wird nicht empfohlen, da die anderen beiden höhere Sicherheit bieten.

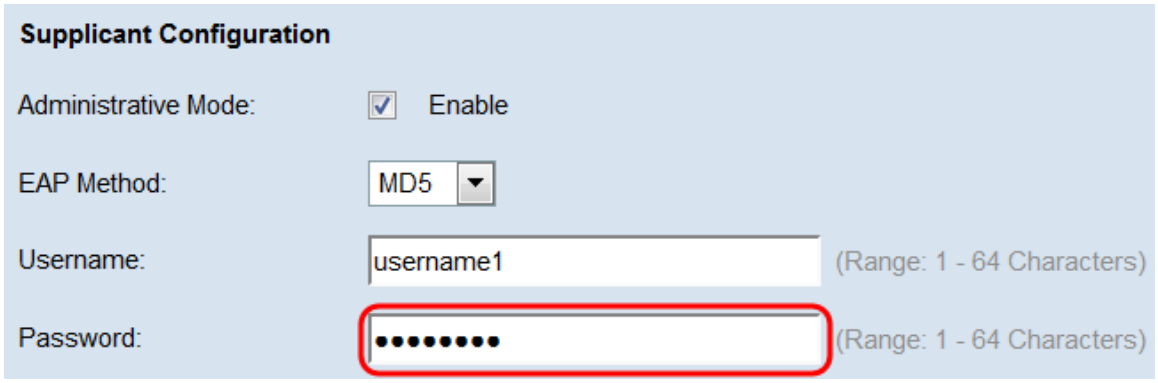
·PEAP - PEAP steht für Protected Extensible Authentication Protocol. Sie kapselt EAP und bietet eine höhere Sicherheit als MD5, indem sie einen TLS-Tunnel für die Datenübertragung verwendet.

·TLS - TLS steht für Transport Layer Security und ist ein offener Standard, der hohe Sicherheit bietet.

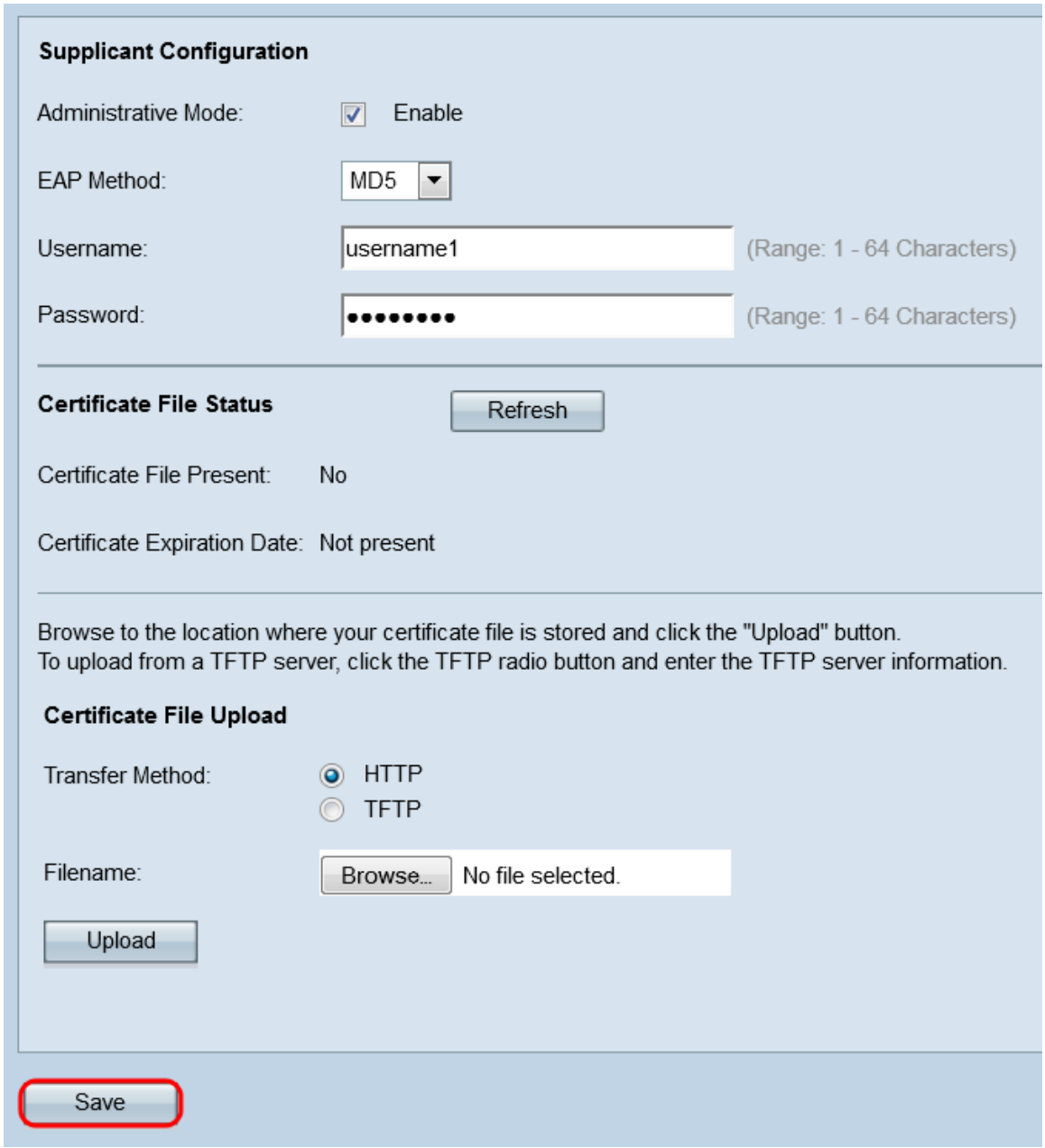
Schritt 3: Geben Sie im Feld *Benutzername* den Benutzernamen ein, den das WAP-Gerät bei der Beantwortung von Anfragen eines 802.1X-Authentifizierers verwenden wird. Der Benutzername muss 1-64 Zeichen lang sein und kann alphanumerische und Sonderzeichen enthalten.



Schritt 4: Geben Sie im Feld *Password (Kennwort*) das Kennwort ein, das das WAP-Gerät bei der Beantwortung von Anfragen eines 802.1X-Authentifizierers verwenden wird. Der Benutzername muss 1-64 Zeichen lang sein und kann alphanumerische und Sonderzeichen enthalten.

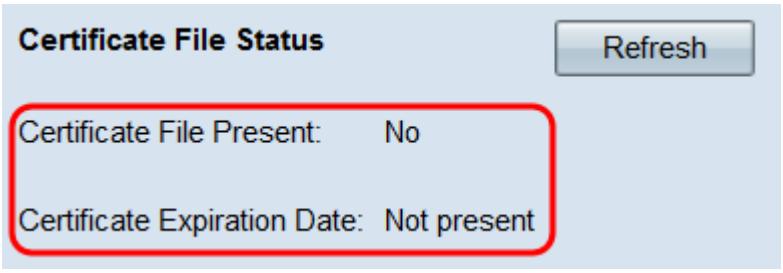


Schritt 5: Klicken Sie auf **Speichern**.

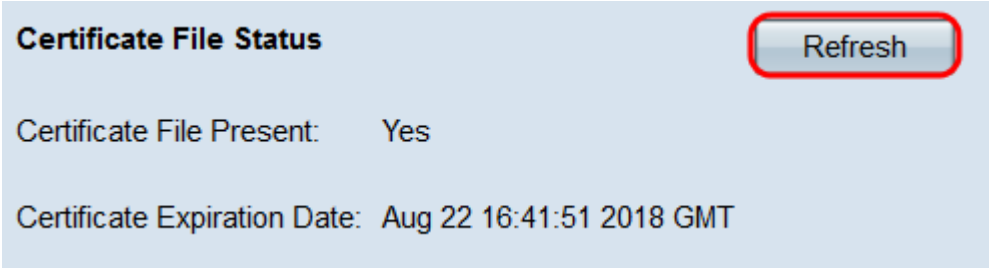


Status der Zertifikatsdatei

Schritt 1: Navigieren Sie zum Bereich *Status der Zertifikatsdatei*. Dieser Bereich zeigt an, ob eine HTTP-SSL-Zertifikatsdatei auf dem WAP-Gerät vorhanden ist. Im Feld *Zertifikatdatei* vorhanden wird "Ja" angezeigt, wenn ein Zertifikat vorhanden ist. Der Standardwert ist "Nein". Wenn ein Zertifikat vorhanden ist, wird das *Ablaufdatum* des Zertifikats angezeigt, wenn es abläuft. Andernfalls ist die Standardeinstellung "Nicht vorhanden".

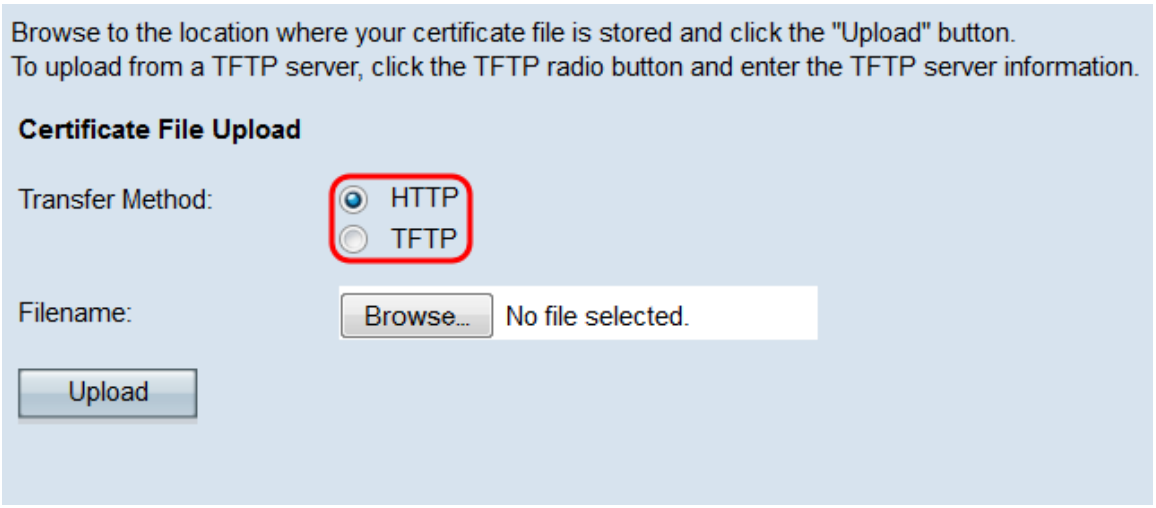


Schritt 2: Um die neuesten Informationen anzuzeigen, klicken Sie auf die Schaltfläche **Aktualisieren**, um die aktuellsten Zertifikatinformationen abzurufen.

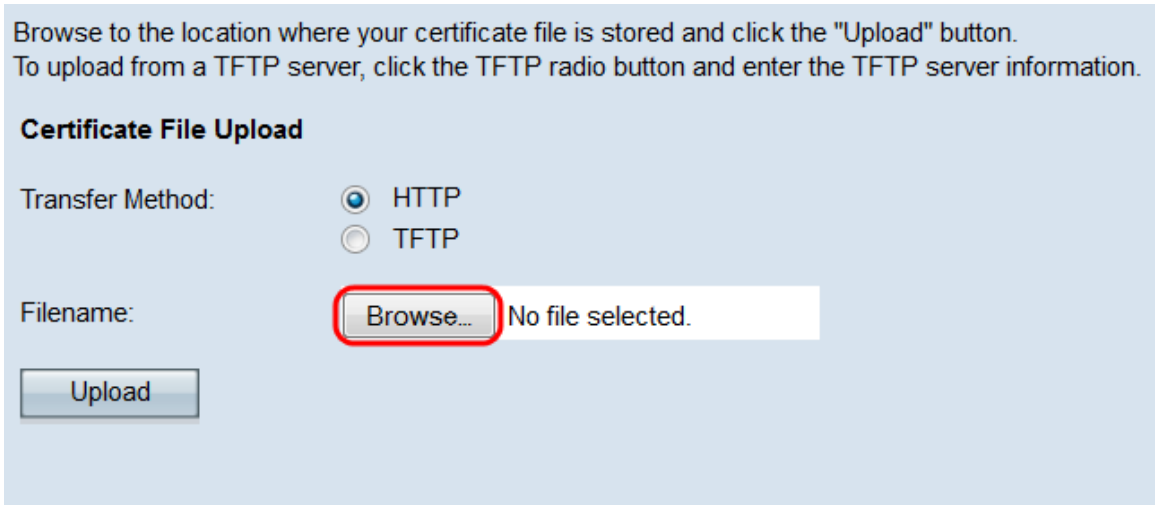


Hochladen der Zertifikatsdatei

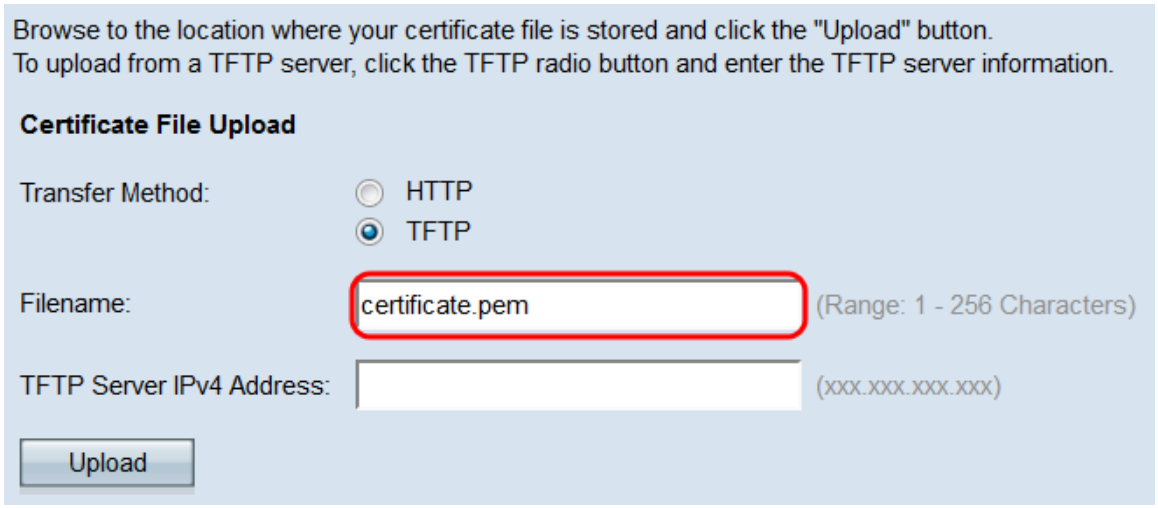
Schritt 1: Navigieren Sie zum Bereich *Zertifikatsdatei-Upload*, um ein HTTP-SSL-Zertifikat auf das WAP-Gerät hochzuladen. Wählen Sie im Feld *Transfer Method (Übertragungsmethode)* entweder die Optionsschaltflächen **HTTP** oder **TFTP** aus, um das Protokoll auszuwählen, das Sie zum Hochladen des Zertifikats verwenden möchten.



Schritt 2: Wenn Sie **TFTP** ausgewählt haben, fahren Sie mit Schritt 3 fort. Wenn Sie **HTTP** ausgewählt haben, klicken Sie auf die Schaltfläche **Durchsuchen**, um die Zertifikatsdatei auf Ihrem PC zu suchen. Fahren Sie mit Schritt 5 fort.

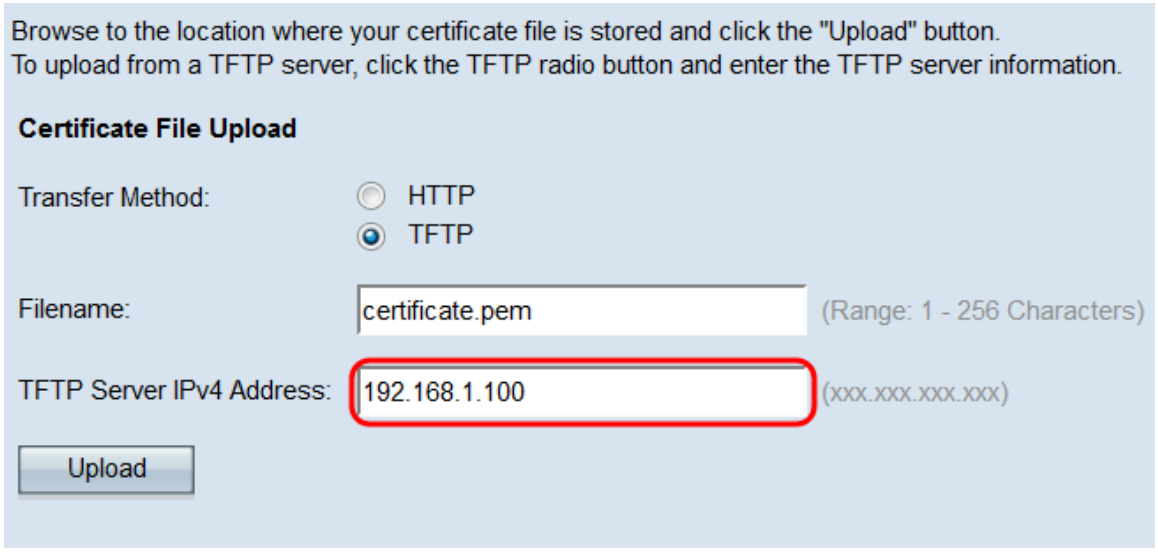


Schritt 3: Wenn Sie **TFTP** im Feld *Übertragungsmethode* ausgewählt haben, geben Sie den Dateinamen des Zertifikats im Feld *Dateiname ein*.

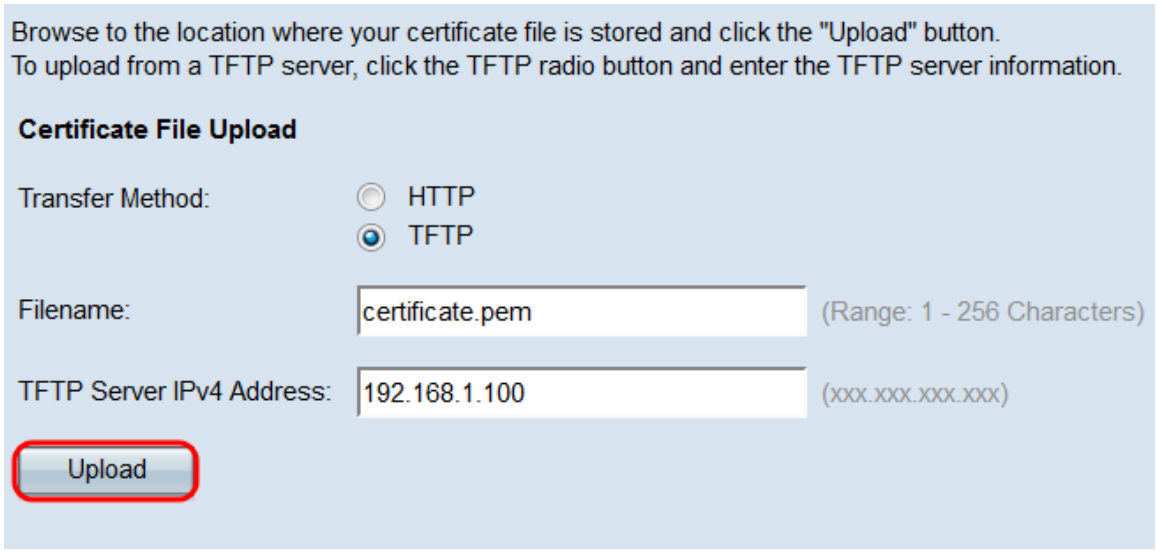


Hinweis: Die Datei muss in .pem enden.

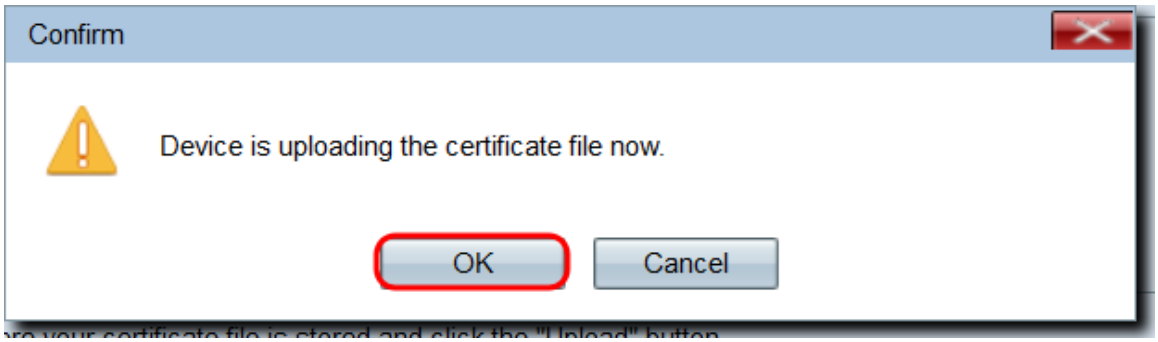
Schritt 4: Geben Sie die IP-Adresse des TFTP-Servers in das Feld *IPv4-Adresse* des *TFTP-Servers ein*.



Schritt 5: Klicken Sie auf **Hochladen**.



Schritt 6: Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **OK**, um den Upload zu starten.



Schritt 7: Klicken Sie auf **Speichern**.