在WAP131和WAP371上配置802.1X請求方設定

目標

IEEE 802.1X身份驗證使WAP裝置能夠訪問安全的有線網路。您可以將WAP裝置啟用為有線網路上的802.1X請求方（客戶端）。可以配置加密的使用者名稱和密碼以允許WAP裝置使用802.1X進行身份驗證。

在使用基於IEEE 802.1X埠的網路訪問控制的網路上，請求方無法訪問該網路，直到802.1X驗證方授予訪問許可權。如果您的網路使用802.1X，您必須在WAP裝置上設定802.1X驗證資訊，以便它能將其提供給驗證器。

本文檔的目的是向您展示如何在WAP131和WAP371上配置802.1X Supplicant設定。

適用裝置

·WAP131

·WAP371

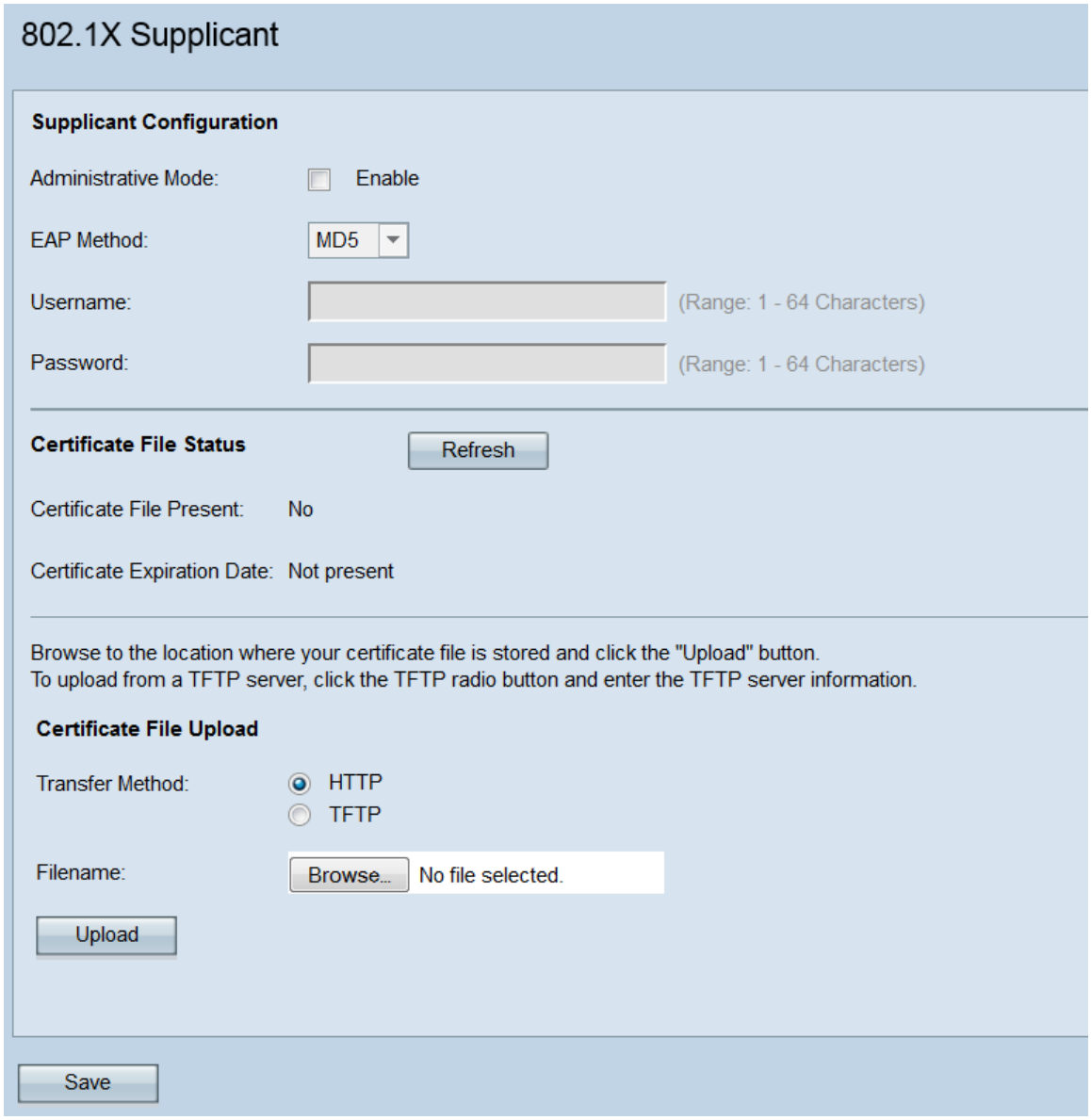
軟體版本

·v1.0.0.39(WAP131)

·v1.2.0.2(WAP371)

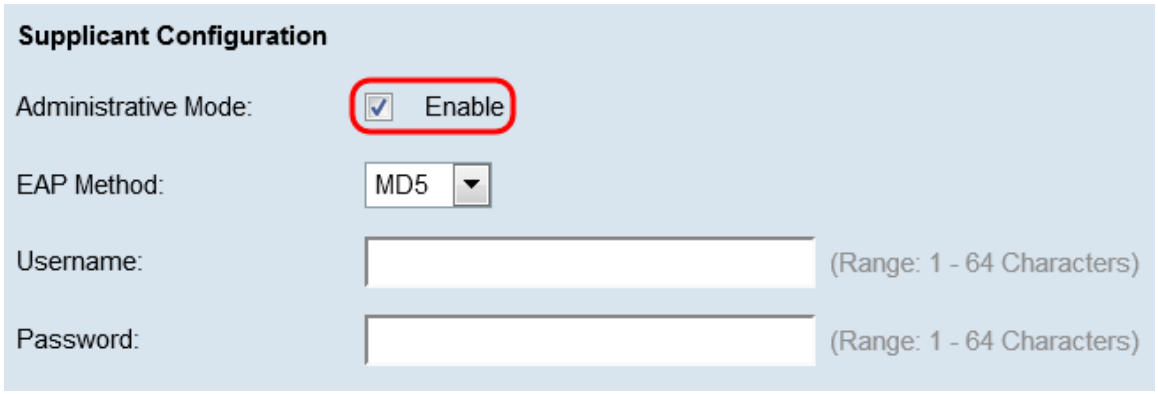
配置802.1X請求方設定

步驟1.登入到Web配置實用程式並選擇**System Security > 802.1X Supplicant**。*802.1X Supplicant*頁面開啟。

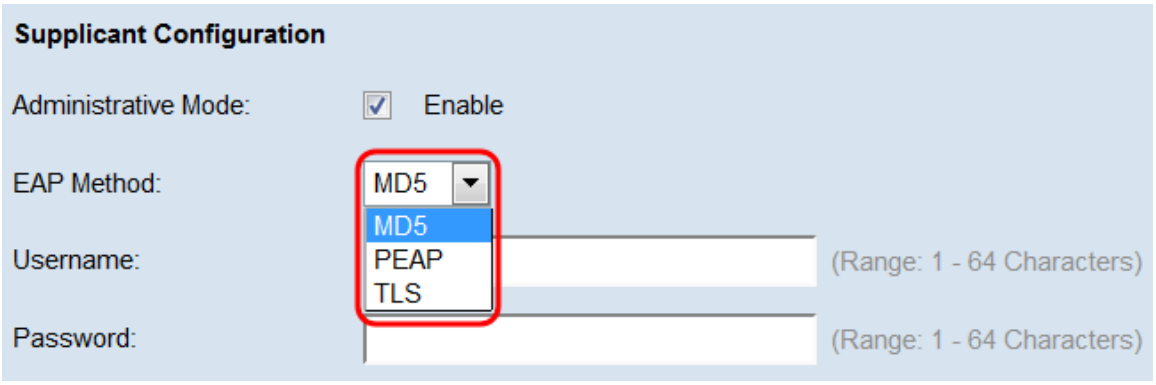


請求方配置

步驟1.導航到*Supplicant Configuration*區域。在*Administrative Mode*欄位中，勾選**Enable**覈取方塊以啟用802.1X請求方功能。



步驟2.在*EAP Method*下拉選單中，選擇用於加密使用者名稱和密碼的演算法。EAP代表可擴展身份驗證協定，並用作加密演算法的基礎。



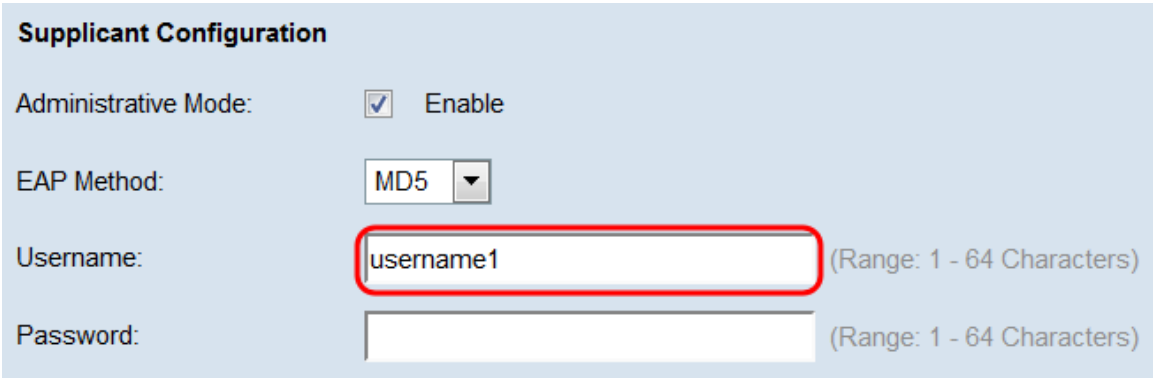
可用選項包括：

·MD5 - MD5消息摘要演算法利用雜湊函式來提供基本的安全性。不建議使用此演算法，因為其他兩個具有更高的安全性。

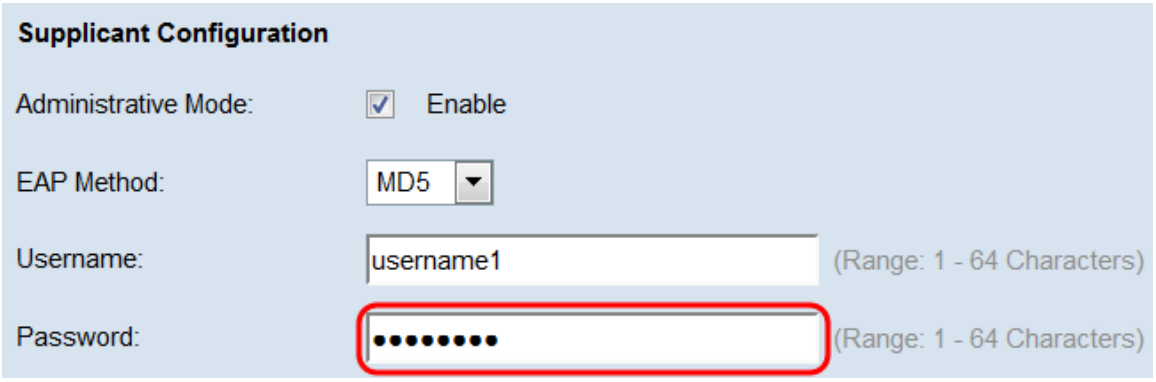
·PEAP - PEAP代表受保護的可擴展身份驗證協定。它封裝了EAP，通過使用TLS隧道傳輸資料，可提供比MD5更高的安全性。

·TLS — TLS代表傳輸層安全性，是提供高安全性的開放標準。

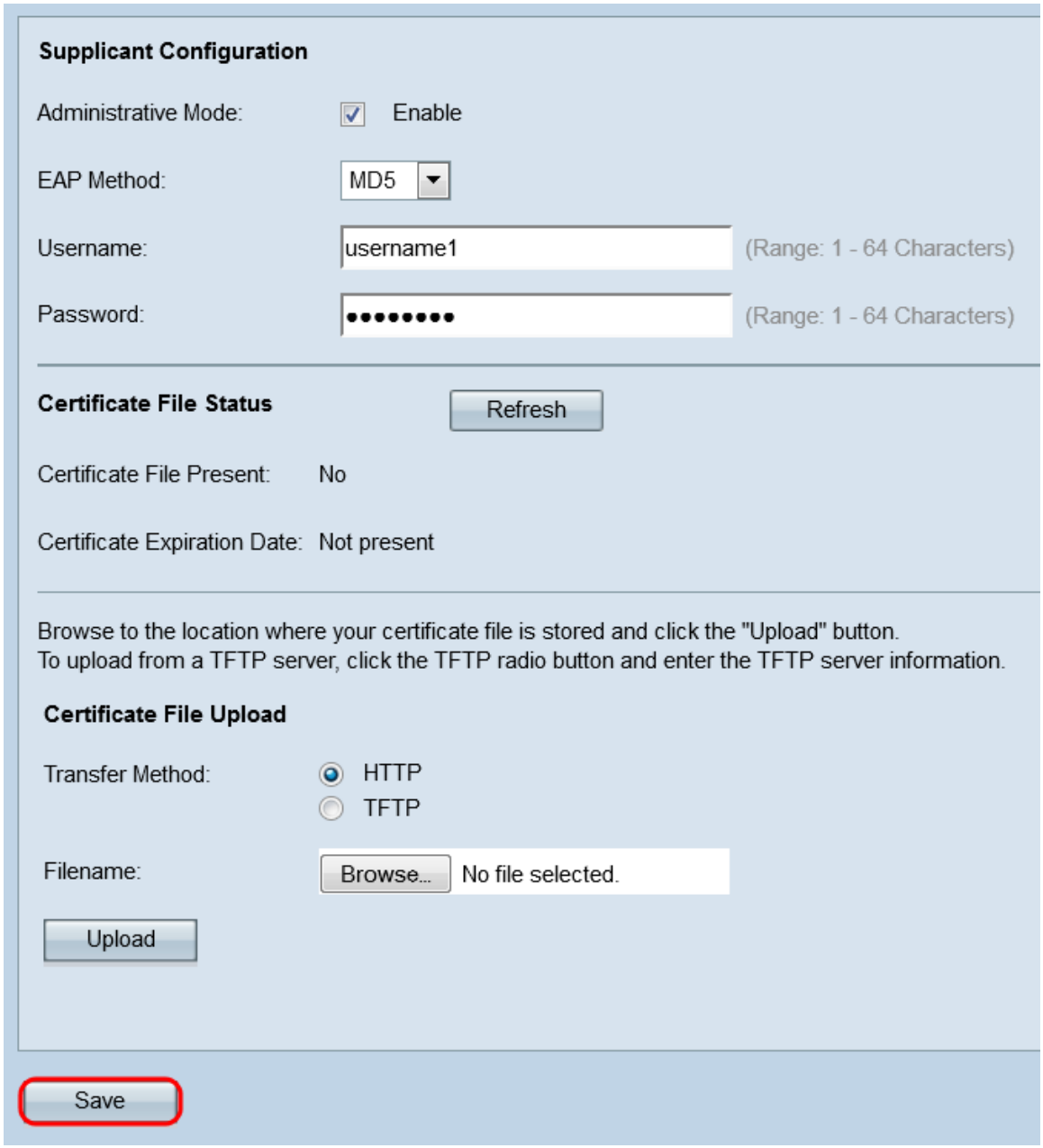
步驟3.在*Username*欄位中，輸入WAP裝置在回應802.1X驗證器要求時將使用的使用者名稱。使用者名稱長度必須為1到64個字元，並且可以包含字母數字字元和特殊字元。



步驟4.在*密碼*欄位中，輸入WAP裝置在回應802.1X驗證器要求時將使用的密碼。使用者名稱長度必須為1到64個字元，並且可以包含字母數字字元和特殊字元。

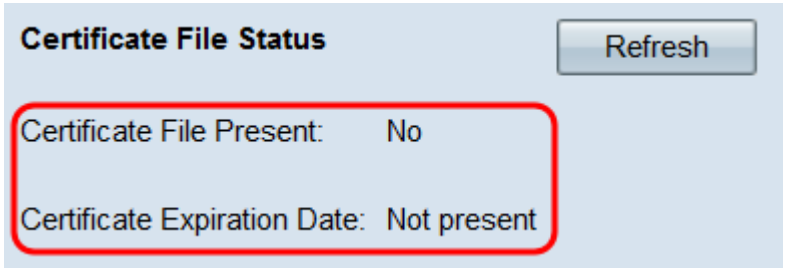


步驟5.按一下**Save**。

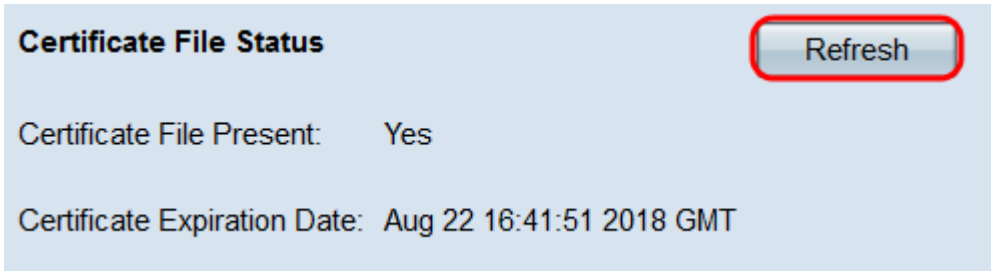


證書檔案狀態

步驟1。導覽至*Certificate File Status*區域。此區域顯示WAP裝置上是否存在HTTP SSL證書檔案。如果憑證存在，*Certificate File Present*欄位會顯示「Yes」；預設值為「No」。如果存在證書，則會顯示*證書到期日*;否則，預設值為「Not present」。

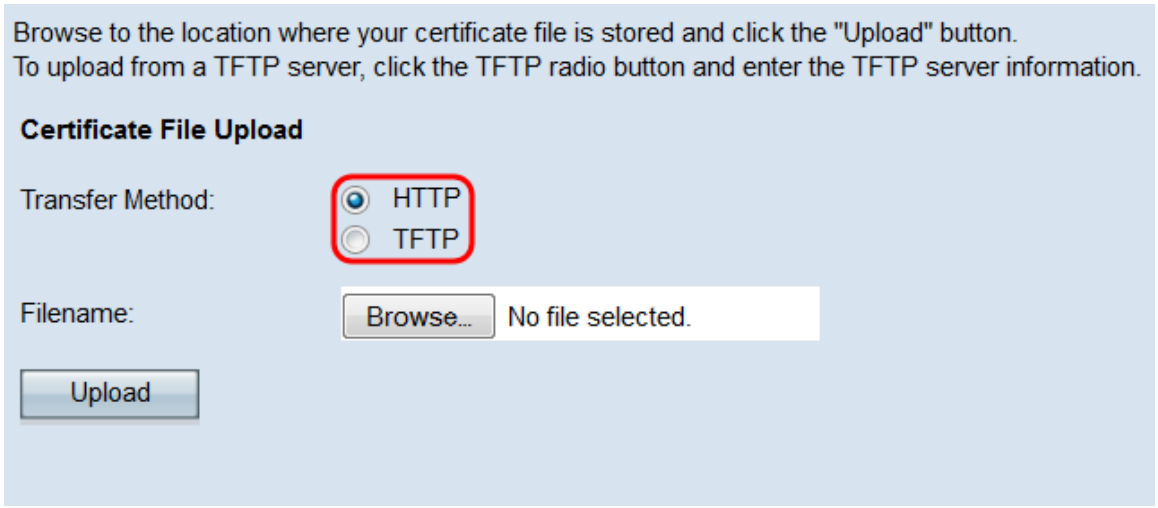


步驟2。若要顯示最新資訊，請按一下**Refresh**按鈕以取得最新的憑證資訊。

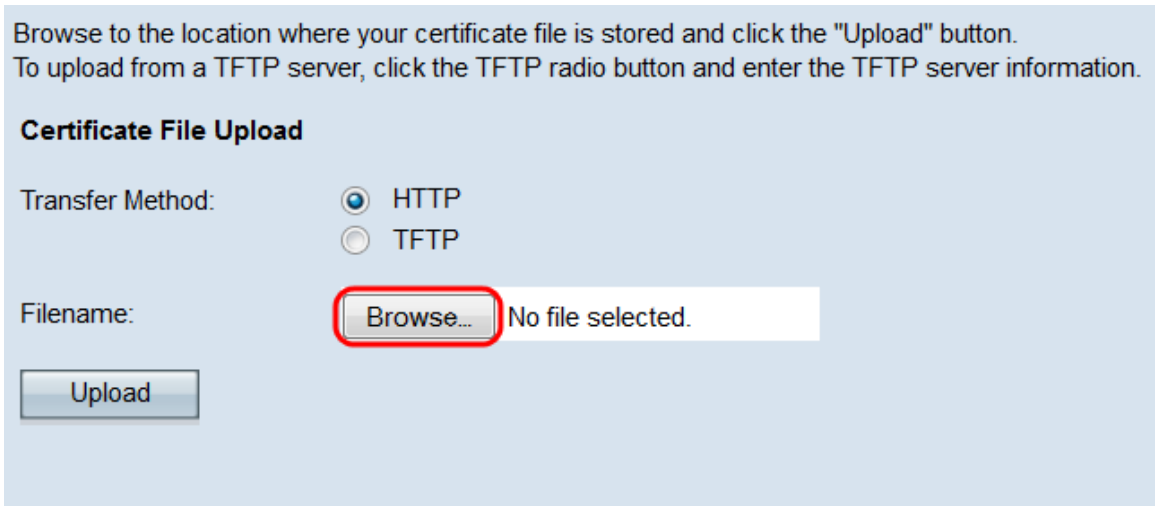


憑證檔案上傳

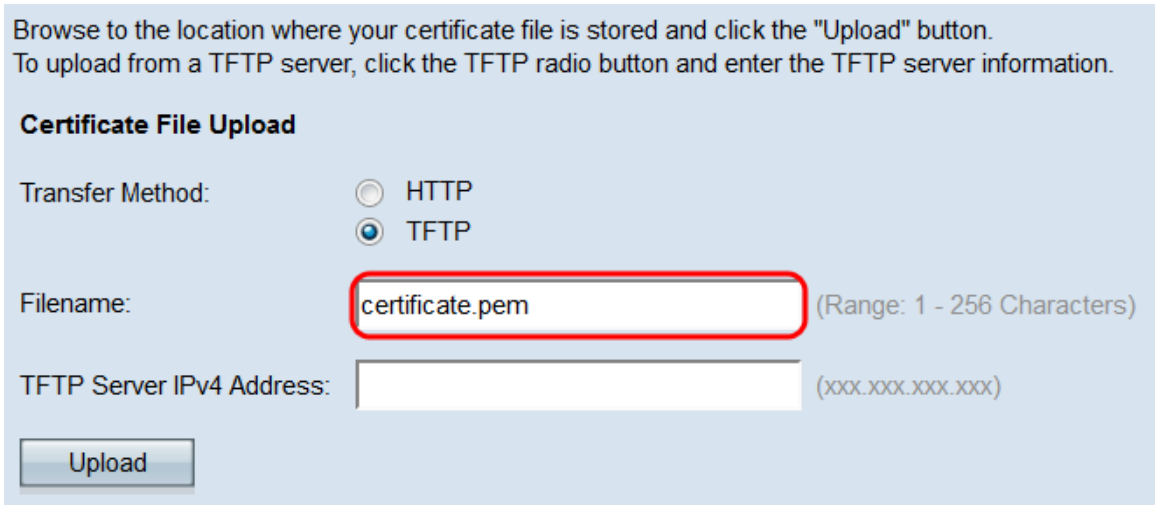
步驟1.導覽至*Certificate File Upload*區域將HTTP SSL憑證上傳到WAP裝置。在「*Transfer Method*」欄位中，選擇「**HTTP**」或「**TFTP**」單選按鈕，以選擇要用來上傳憑證的通訊協定。



步驟2.如果選擇**TFTP**，請繼續步驟3。如果選擇**HTTP**，請按一下**Browse...**按鈕在PC上查詢證書檔案。跳至步驟5。

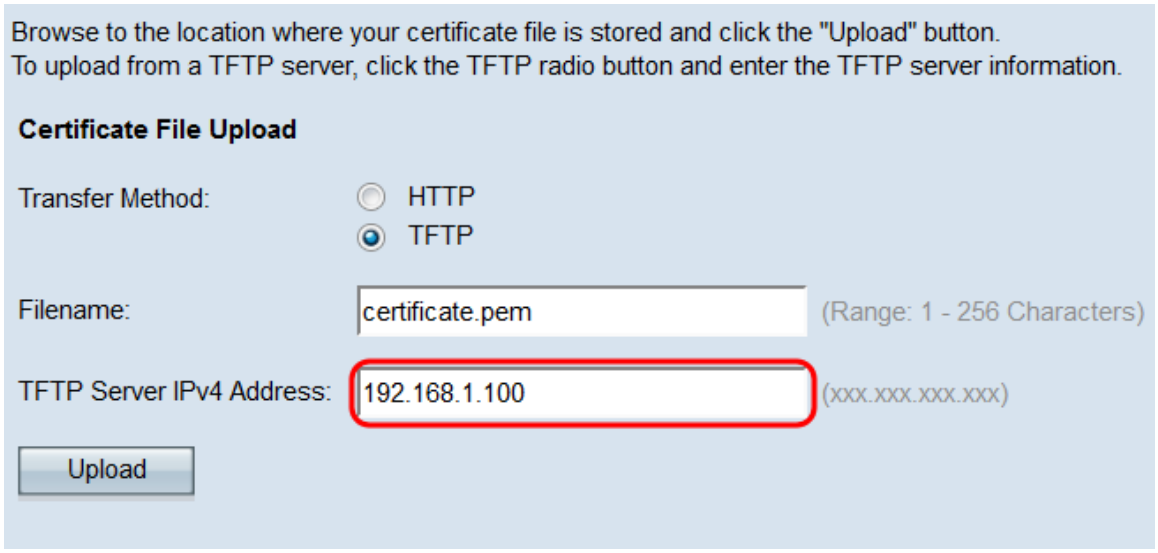


步驟3.如果您在*Transfer Method*欄位中選擇了**TFTP**，請在*Filename*欄位中輸入憑證的名稱。

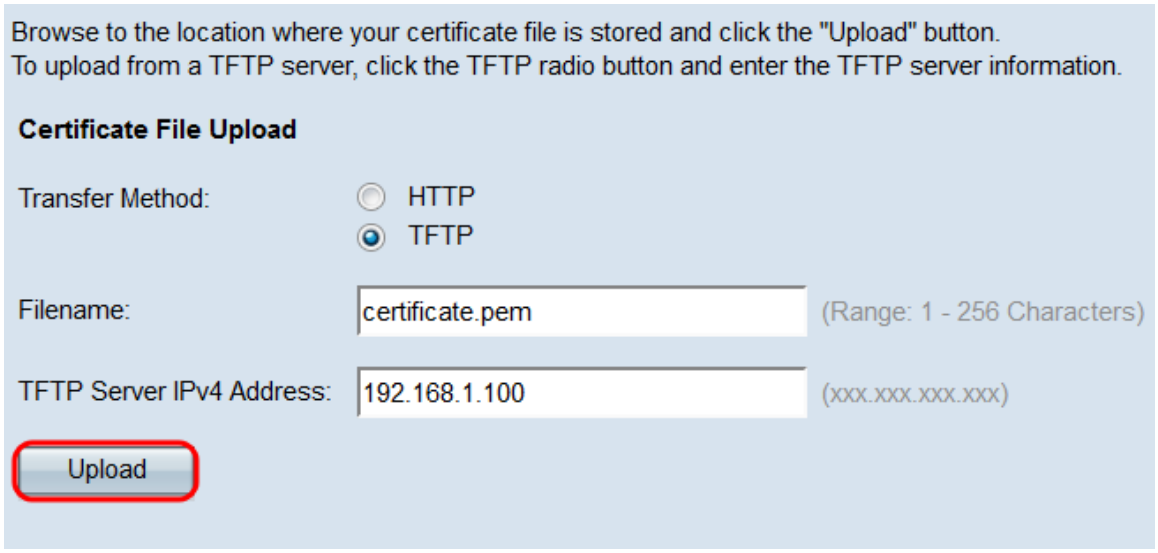


附註：檔案必須以.pem結尾。

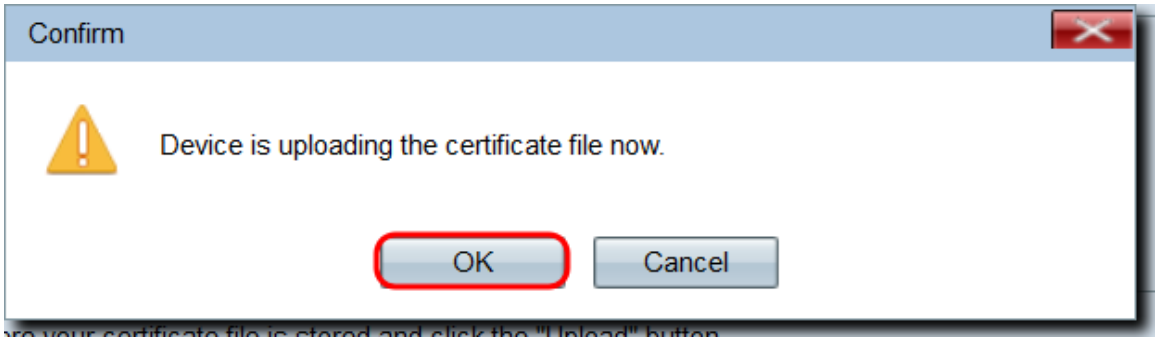
步驟4.在「*TFTP Server IPv4 Address*」欄位中輸入TFTP伺服器的IP地址。



步驟5.按一下**Upload**。



步驟6.出現確認視窗。按一下「**OK**」開始上傳。


Confirm
Device is uploading the certificate file now.
OK
Cancel

步驟7.按一下「**Save**」。