在WAP121和WAP321接入點上配置802.1X身份驗證

目標

在802.1X身份驗證中，當主機（也稱為請求方）嘗試連線到安全網路時，稱為身份驗證者的網路裝置會檢查支援安全協定RADIUS和可擴展身份驗證協定(EAP)的身份驗證伺服器，以驗證請求方的身份。這樣，網路裝置為網路提供了額外的安全層。

本文檔說明如何將WAP121和WAP321接入點配置為802.1X身份驗證的請求方。

適用裝置

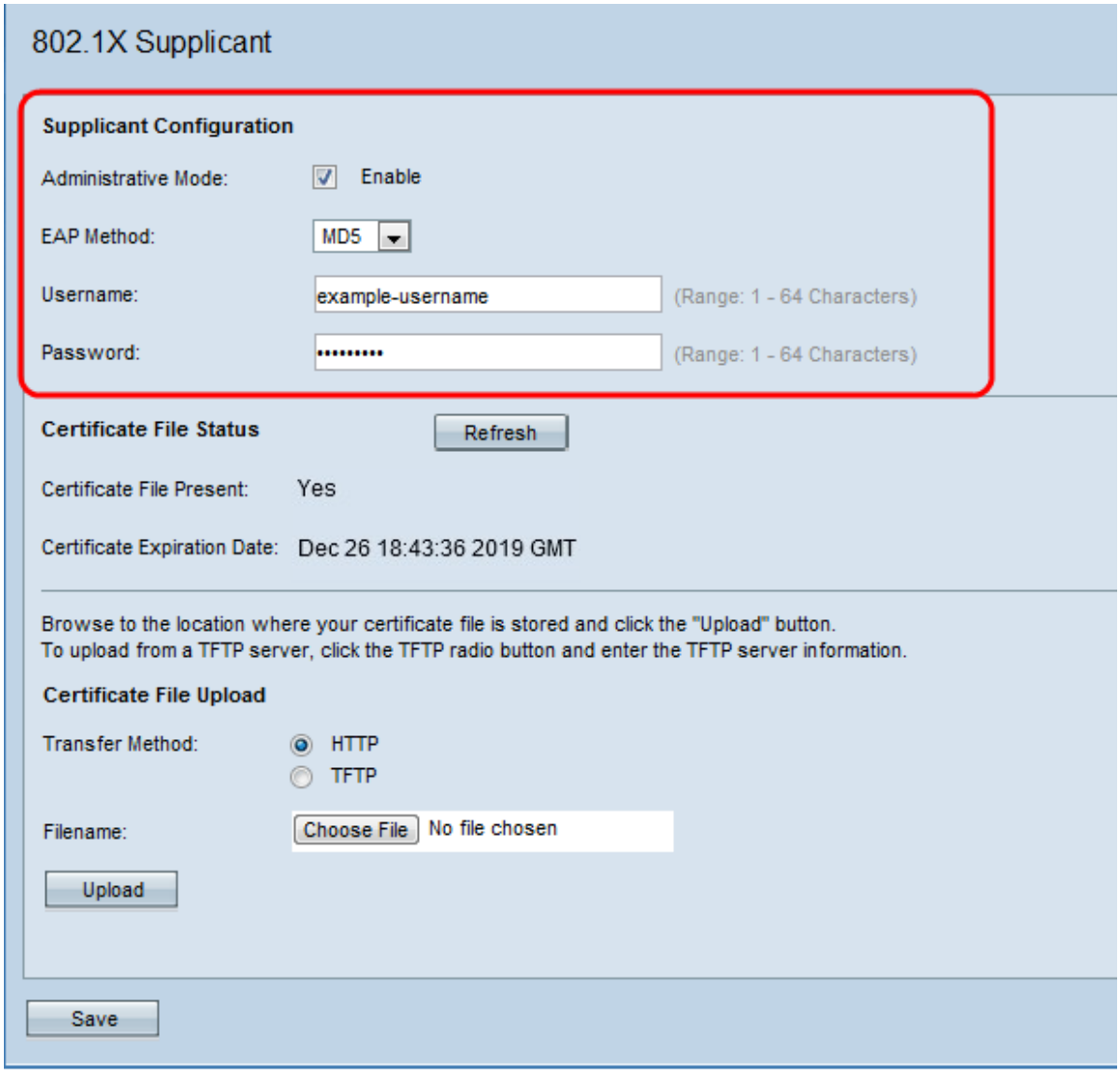
·WAP121
· WAP321

軟體版本

•1.0.3.4

802.1X請求方配置

步驟1.登入到Web配置實用程式並選擇**System Security > 802.1X Supplicant**。此時將開啟「*Supplicant Configuration*」頁：



步驟2.在「Administrative Mode」欄位中選中**Enable**，使裝置能夠充當802.1X身份驗證中的請求方。

步驟3.從「EAP方法」欄位的下拉選單中選擇適當型別的可擴展身份驗證協定(EAP)方法。

·MD5 — MD5是一種用於加密任意大小到128位的資料的演算法，MD5演算法使用公鑰加密系統加密資料。

·PEAP — 受保護的EAP是一種身份驗證方法，可提供增強的安全性，PEAP通過伺服器頒發的數位證書對無線LAN客戶端進行身份驗證，方法是在客戶端和身份驗證伺服器之間建立加密的SSL/TLS隧道。

·TLS — 傳輸層安全性(TLS)是一種加密協定，為Internet上的通訊提供安全性和資料完整性。當伺服器和客戶端通訊時，TLS確保沒有第三方篡改原始消息。MD5的大部分功能都用於TLS中。

步驟4.在「使用者名稱」和「密碼」欄位中輸入接入點用於從802.1X驗證器獲取身份驗證的使用者名稱和密碼。使用者名稱和密碼的長度必須介於1到64個字母數字和符號字元之間。

步驟5.按一下**Save**以儲存設定。

附註：Certificate File Status區域顯示證書檔案是否存在。SSL證書是由證書頒發機構數位簽章的證書，它允許Web瀏覽器與Web伺服器進行安全通訊。要管理和配置SSL證書，請參閱*WAP121和WAP321接入點上的安全套接字層(SSL)證書管理*文章。