在WAP125或WAP581上配置802.1X請求方設定

目標

請求方是802.1X IEEE標準的三個角色之一。802.1X的開發目的是在OSI模型的第2層提供安全保護。它包括以下元件：Supplicant客戶端、身份驗證器和身份驗證伺服器。Supplicant客戶端是連線到網路以便訪問其資源的客戶端或軟體。它需要提供憑證或憑證以取得IP位址，並成為該特定網路的一部分。請求方在經過身份驗證之前不能訪問網路資源。

本文將向您展示如何將WAP125或WAP581接入點配置為802.1X請求方。

附註：若要瞭解如何配置交換機上的802.1X請求方憑據，請按一下此處。

適用裝置

- WAP125
- WAP581

軟體版本

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

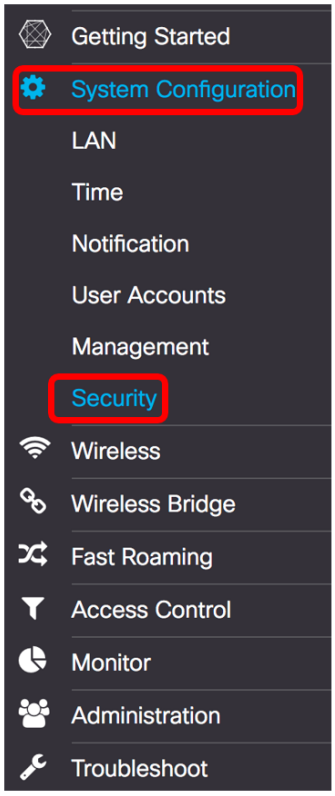
配置802.1X Supplicant客戶端

配置請求方憑據

步驟1.登入到WAP的基於Web的實用程式。預設使用者名稱和密碼為cisco/cisco。

附註：如果您已更改密碼或建立新帳戶，請輸入您的新憑據。

步驟2.選擇**System Configuration > Security**。

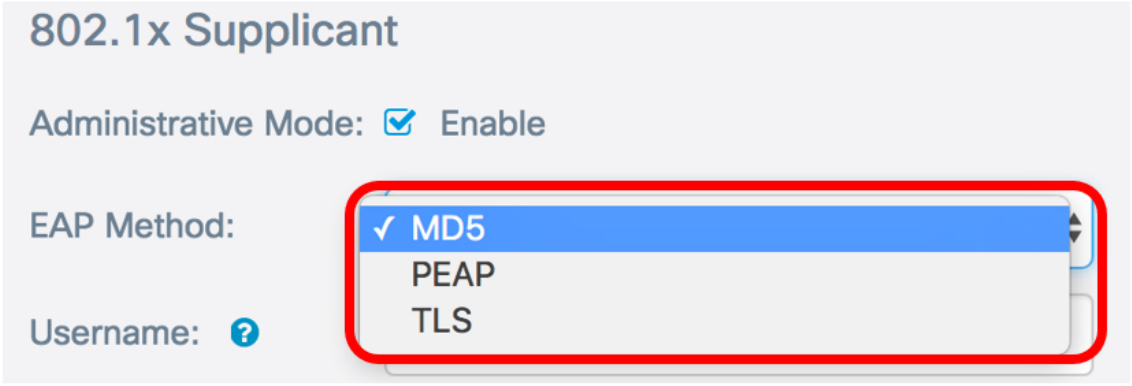


步驟3.勾選**Enable**覈取方塊以啟用管理模式。這使WAP能夠充當身份驗證器的請求方。

步驟4.從*EAP方法*下拉選單中選擇將用於加密使用者名稱和密碼的相應型別的可擴展身份驗證協定(EAP)方法。選項包括：

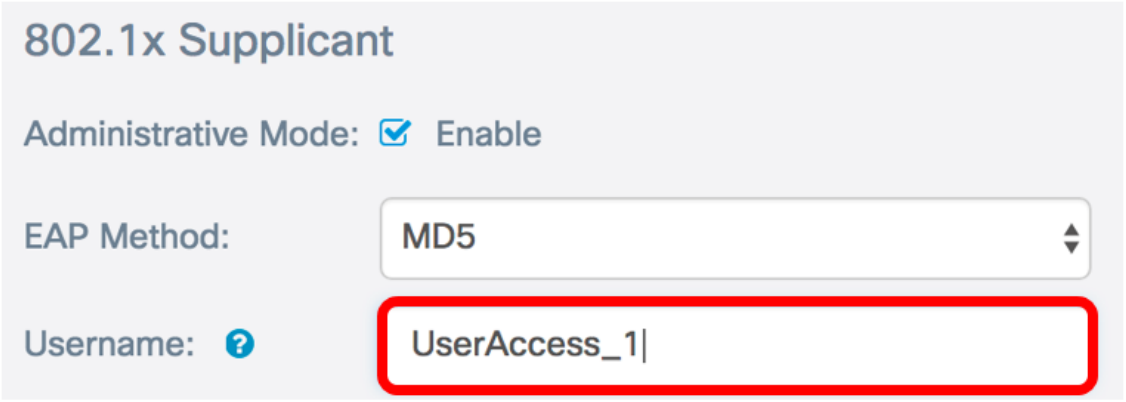
- MD5 — 使用128位加密方法。MD5演演算法使用公共加密系統加密資料。
- PEAP — 受保護的可擴展身份驗證協定(PEAP)通過在客戶端和身份驗證伺服器之間建立加密的SSL/TLS隧道，通過伺服器頒發的數位證書對無線LAN客戶端進行身份驗證。
- TLS — 傳輸層安全性(TLS)是一種協定，它為Internet上的通訊提供安全性和資料完整性。它確保沒有第三方篡改原始消息。

附註：本示例使用MD5。

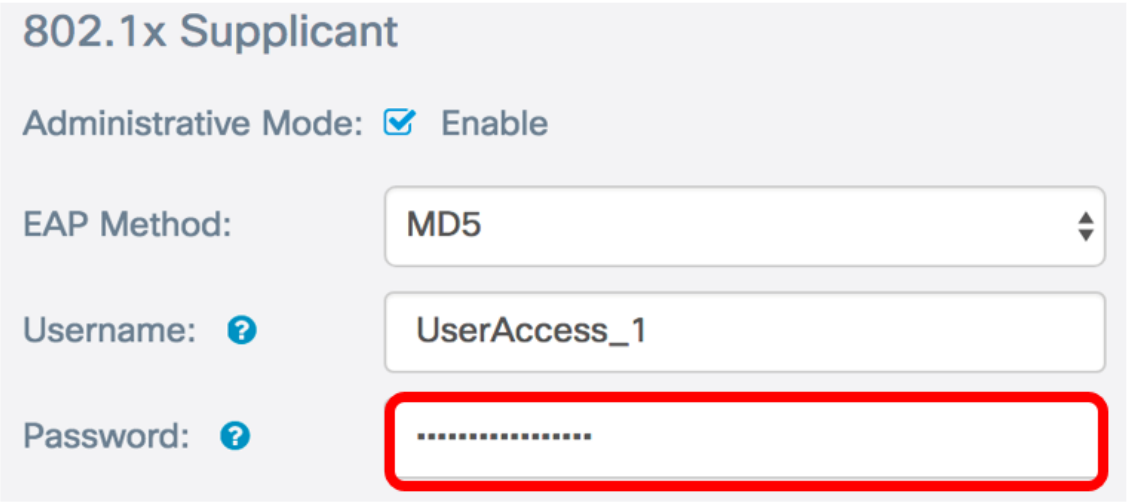


步驟5.在*Username*欄位中輸入使用者名稱。這是已在驗證器上配置的使用者名稱，用於響應802.1X驗證器。長度為1到64個字元，可以包含大寫字母、小寫字母、數字以及除雙引號之外的特殊字元。

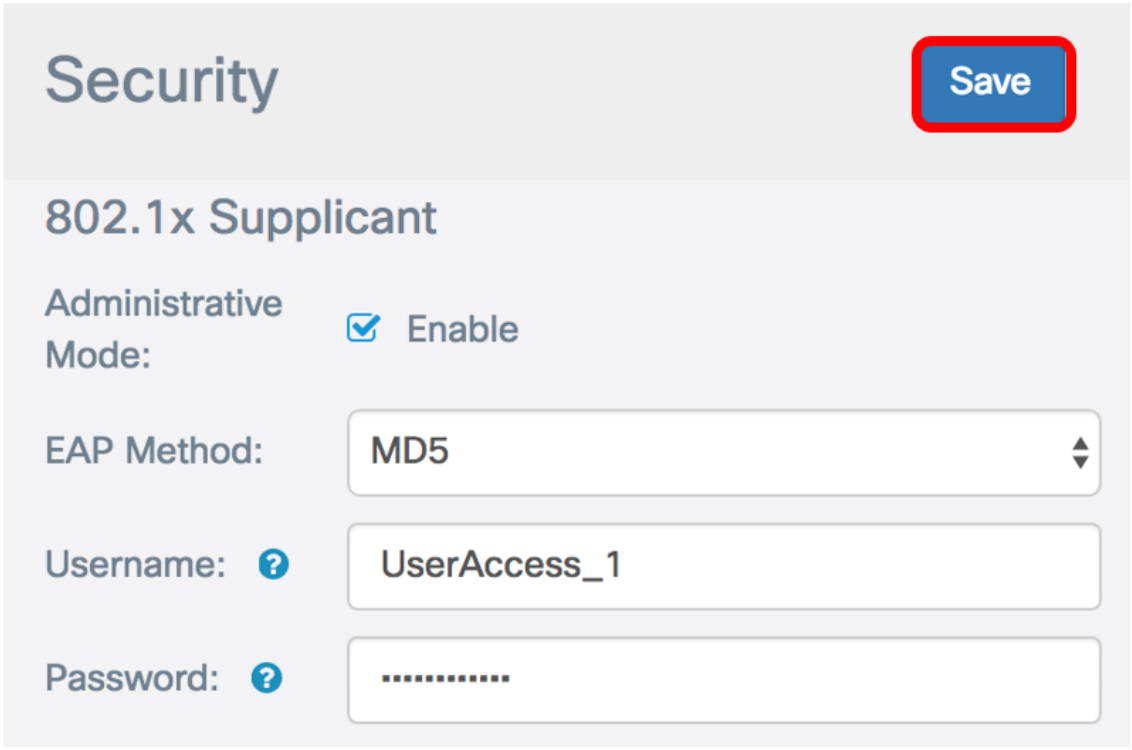
附註：本示例使用UserAccess_1。



步驟6.在*Password*欄位中輸入與Username關聯的密碼。此MD5密碼用於響應802.1X身份驗證器。密碼長度可以為1到64個字元，可以包含大寫和小寫字母、數字以及除引號之外的特殊字元。



步驟7.按一下**Save**按鈕以儲存已設定的設定。



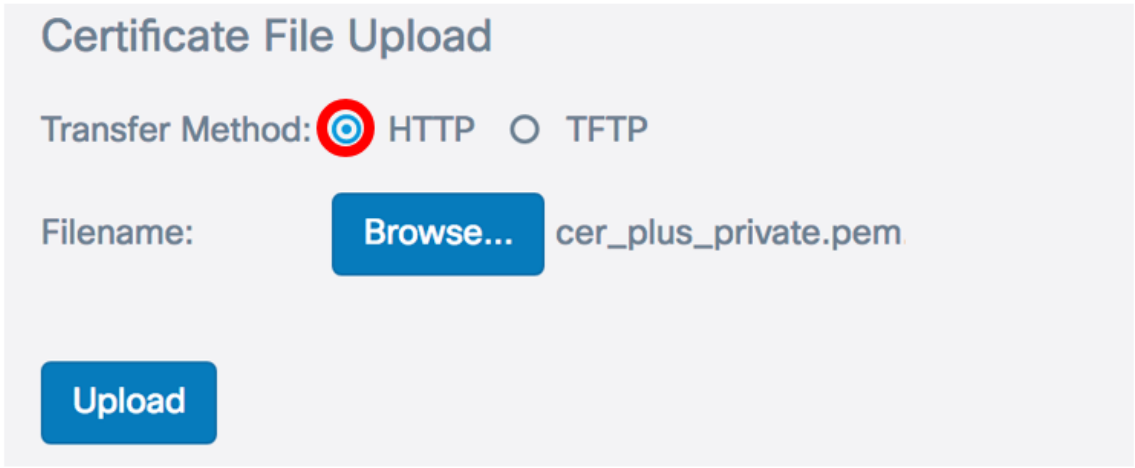
您現在應該已經在WAP上配置了802.1X Supplicant客戶端設定。

憑證檔案上傳

步驟1。從傳輸方法中選擇一種WAP將用於獲取SSL證書的方法。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。選項包括：

- HTTP — 憑證是通過超文字傳輸通訊協定(HTTP)或透過瀏覽器上傳。
- TFTP — 憑證透過簡單式檔案傳輸通訊協定(TFTP)伺服器上傳。如果選擇此選項，請跳至步驟3。您需要輸入檔名和TFTP地址。

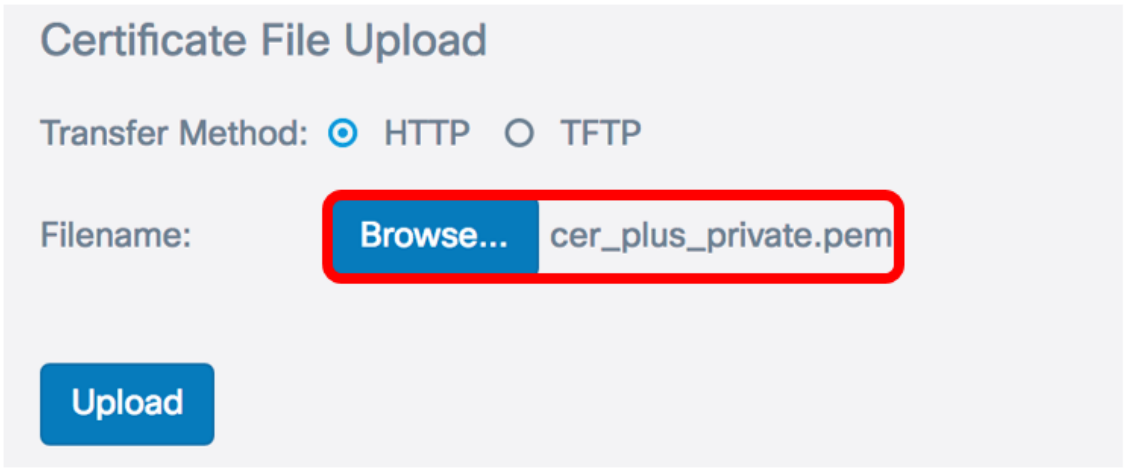
附註：在此範例中，選擇HTTP。



HTTP傳輸方法

步驟2.（可選）如果您已選擇HTTP，請按一下「Browse...」 並選擇SSL證書。

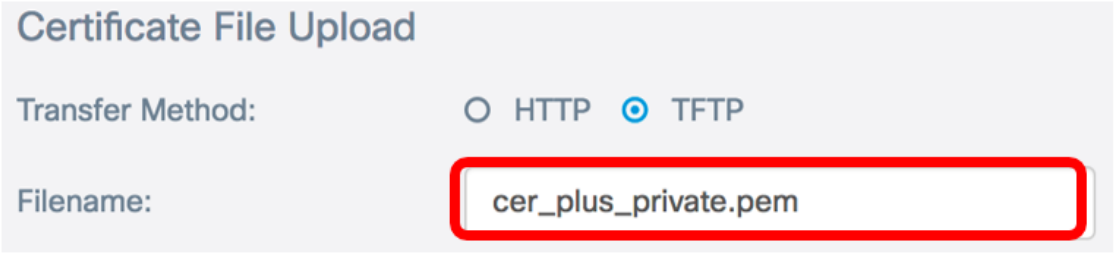
附註：在本示例中，使用了cer_plus_private.pem。



TFTP傳輸方法

步驟3.如果您在步驟1中選擇了TFTP，請在「Filename」欄位中輸入檔案的名稱。

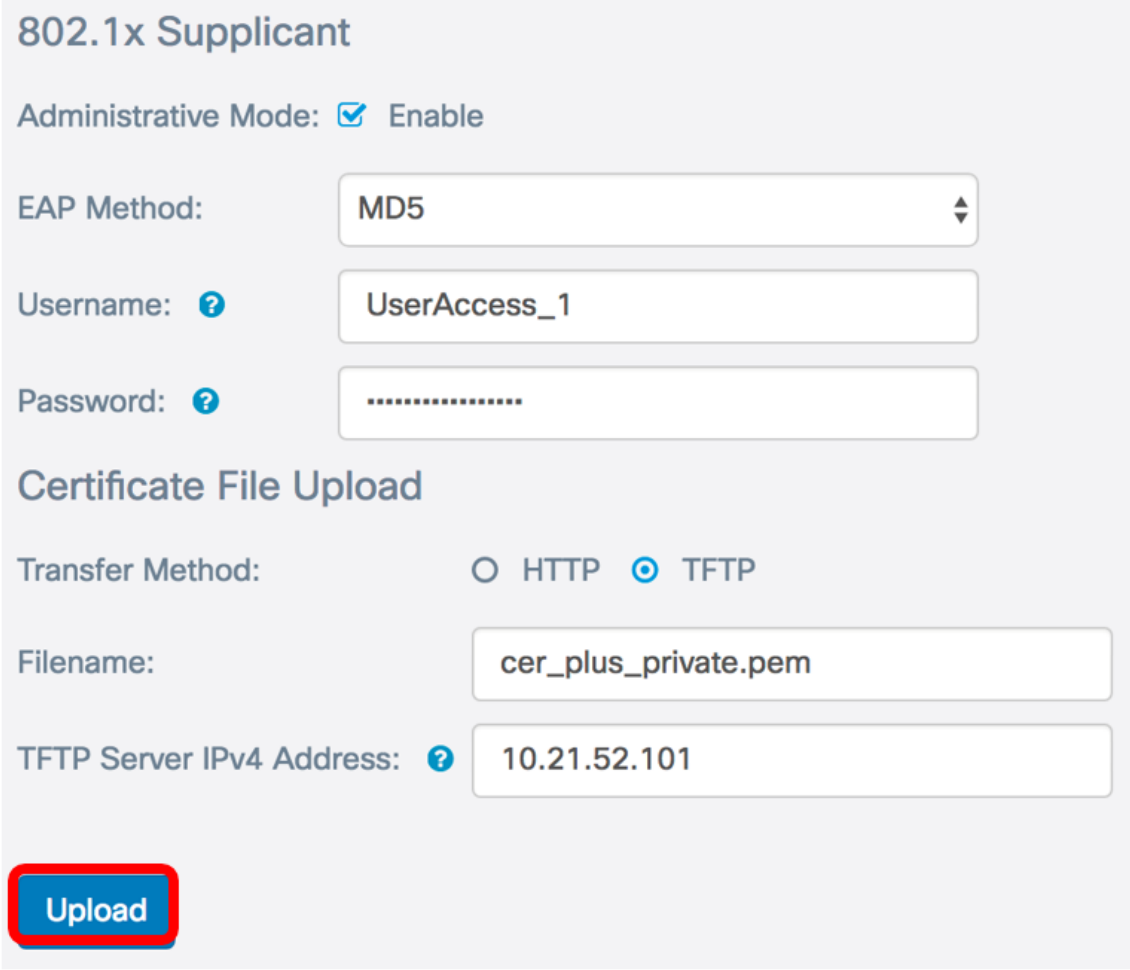
附註：在本示例中，使用了cer_plus_private.pem。



步驟4.（可選）如果選擇TFTP作為傳輸方法，請在「*TFTP伺服器IPv4地址*」欄位中輸入*TFTP伺服器的IPv4地*址。這是WAP將用於檢索證書的路徑。

附註：本例中使用的是10.21.52.101。

步驟5.按一下**Upload**。



您現在應該已經在WAP上成功上傳了證書。