

在無線接入點上配置802.1X請求方設定

目標

802.1X標準的開發目的是在開放系統互聯(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。

在無線接入點(WAP)上配置802.1X Supplicant設定對於允許WAP背後的授權裝置成為網路的一部分並訪問其資源非常有用。同時，它還為網路新增了一層安全性。

本文將向您展示如何在無線接入點上配置802.1X請求方設定。

適用裝置

- WAP100系列
- WAP300系列
- WAP500系列

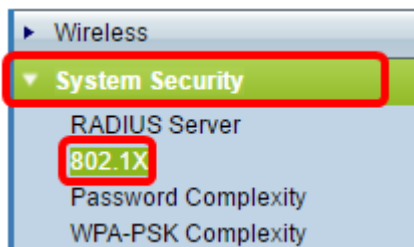
軟體版本

- 1.0.1.2 - WAP150、WAP361
- 1.0.6.2 - WAP121、WAP321
- 1.0.2.2 - WAP131、WAP351
- 1.2.1.3 - WAP551、WAP561、WAP371
- 1.0.0.17 - WAP571、WAP571E

在WAP上配置802.1X請求方設定

步驟1.登入到接入點的基於Web的實用程式，然後選擇**System Security>802.1X**。

附註：基於Web的實用程式選單可能因WAP型號而異。以下影象來自WAP361。



附註：如果您使用其他WAP型號，請選擇**System Security > 802.1X Supplicant**，然後跳至[步驟3](#)。

步驟2.選中您要配置的埠號的覈取方塊，然後按一下**Edit**。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

步驟3.選中Enable覆取方塊，然後從下拉選單中選擇Supplicant。這是預設選項。

附註：對於WAP的其他型號，請選中Enable覆取方塊以管理模式，然後跳至[步驟5](#)。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant Authenticator	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

步驟4.按一下Show Details連結以編輯設定。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

步驟5.從EAP方法下拉選單中選擇適當型別的可擴展身份驗證協定(EAP)方法。

EAP Method: MD5 ▼

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

選項包括：

- MD5 - MD5是一種演算法，用於加密任何大小的資料到128位。MD5演算法使用公共密碼系統加密資料。
- 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安全套接字層(SSL)或傳輸層安全(TLS)隧道，通過伺服器頒發的數位證書對無線區域網(LAN)客戶端進行身份驗證。
- TLS - TLS是一種協定，為通過Internet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6.在 *Username* 欄位中輸入您的首選使用者名稱。在響應802.1X身份驗證器時將使用此命令。長度最多為64個字元，可以包含大寫和小寫字母、數字以及除雙引號之外的特殊字元。

EAP Method: MD5 ▼

Username: Username (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

步驟7.在 *Password* 欄位中輸入您的首選密碼。在響應802.1X身份驗證器時使用此MD5密碼。密碼最長可為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。

EAP Method: MD5 ▼

Username: Username (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

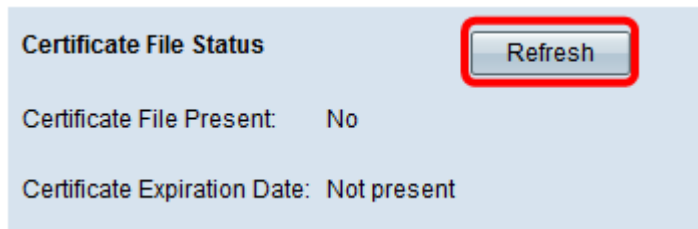
步驟8.按一下按  鈕。

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

檢視證書檔案設定

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。

步驟1。若要檢視憑證檔案的目前狀態，請按一下「Refresh」。



Certificate File Status

Refresh

Certificate File Present: No

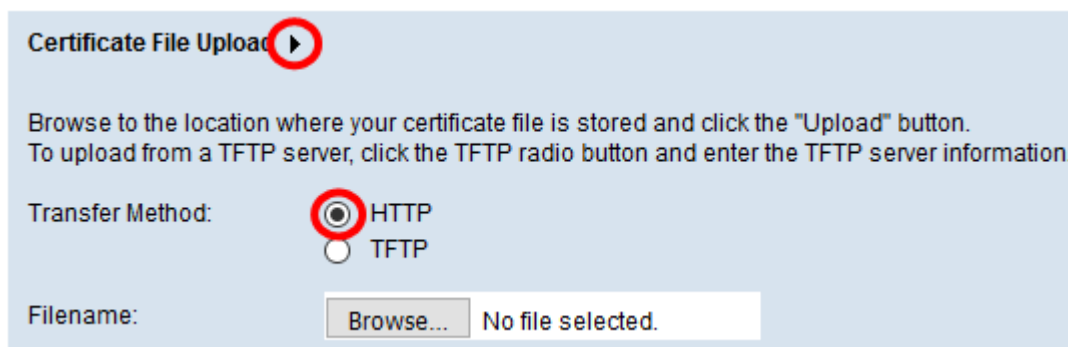
Certificate Expiration Date: Not present

Certificate File Status區域具有以下欄位：

- Certificate File Present — 顯示證書檔案是否存在。
- Certificate Expiration Date — 顯示當前證書檔案的到期日期。

上傳憑證檔案

步驟1。按一下Certificate File Upload旁邊的箭頭，然後從Transfer Method中選擇所需的單選按鈕。



Certificate File Upload ▶

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method: HTTP TFTP

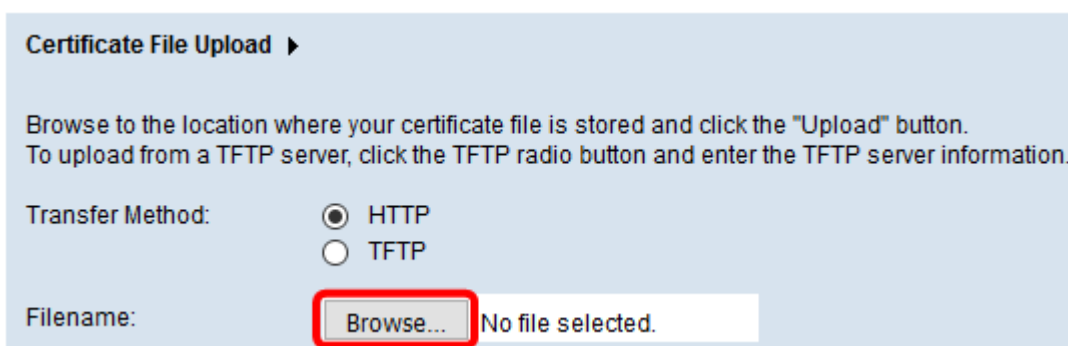
Filename: No file selected.

上傳檔案有兩種傳輸方式：

- 超文字傳輸通訊協定(HTTP)
- 簡單式檔案傳輸通訊協定(TFTP)

附註：在此範例中，選擇HTTP。

步驟2。(可選) 如果選擇HTTP，請按一下**Browse**，從您的電腦中選擇憑證檔案，然後跳至[步驟5](#)。



Certificate File Upload ▶

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method: HTTP TFTP

Filename: No file selected.

步驟3。(可選) 如果您在步驟1中選擇了TFTP，請在Filename欄位中輸入證書檔案的名稱。TFTP伺服器用於在裝置內自動傳輸引導檔案，非常簡單。

附註：在本例中，`mini_httpd.pem`用作檔名。

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

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

附註：在本示例中，10.10.10.11用作TFTP伺服器IPv4地址。

Transfer Method: HTTP
 TFTP

Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

步驟5.按一下Update。

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

附註：如果您使用的是其他WAP型號，請按一下Upload。

步驟6.按一下按 鈕儲存設定。

現在，您應該已經成功地在WAP上上傳了證書檔案。