

Configurazione delle impostazioni del richiedente 802.1X su un punto di accesso wireless

Obiettivo

Lo standard 802.1X è stato sviluppato per garantire la sicurezza nel layer 2 del modello OSI (Open System Interconnection). È costituito dai seguenti componenti: Supplicant, Authenticator e Authentication Server. Un supplicant è il client o il software che si connette a una rete in modo che possa accedere alle sue risorse. Deve fornire credenziali o certificati per ottenere un indirizzo IP e far parte di tale rete. Un supplicant non può accedere alle risorse di rete finché non è stato autenticato.

Configurare le impostazioni 802.1X Supplicant sul punto di accesso wireless (WAP) è utile per consentire ai dispositivi autorizzati dietro il punto di accesso wireless di far parte della rete e di accedere alle relative risorse. Allo stesso tempo, aggiunge un livello di sicurezza alla rete.

In questo articolo verrà illustrato come configurare le impostazioni del supporto 802.1X nel punto di accesso wireless.

Dispositivi interessati

- Serie WAP100
- Serie WAP300
- Serie WAP500

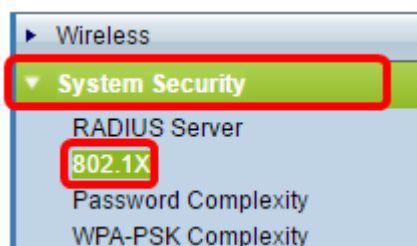
Versione del software

- 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

Configurare le impostazioni del supplicant 802.1X su un WAP

Passaggio 1. Accedere all'utility basata sul Web del punto di accesso e scegliere **System Security>802.1X**.

Nota: Il menu delle utilità basate sul Web può variare a seconda del modello di WAP in uso. Le immagini seguenti sono state acquisite da WAP361.



Nota: Se si utilizzano altri modelli di WAP, scegliere **System Security > 802.1X Supplicant**

quindi andare al [passo 3](#).

Passaggio 2. Selezionare la casella del numero di porta che si desidera configurare e fare clic su **Modifica**.

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

Passaggio 3. Selezionare la casella di controllo **Abilita**, quindi scegliere **Supplicant** dall'elenco a discesa. Questa è l'opzione predefinita.

Nota: Per gli altri modelli di WAP, selezionare la casella di controllo **Attiva** per la modalità amministrativa, quindi andare al [passaggio 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

Passaggio 4. Fare clic sul collegamento **Mostra dettagli** per consentire la modifica delle impostazioni.

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

Passaggio 5. Selezionare il tipo appropriato di metodo EAP (Extensible Authentication Protocol) dall'elenco a discesa Metodo EAP.

EAP Method: (Range: 1 - 64 Characters)

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Le opzioni sono:

- MD5 — MD5 è un algoritmo utilizzato per crittografare dati di qualsiasi dimensione in 128 bit. L'algoritmo MD5 utilizza un sistema di crittografia pubblico per crittografare i dati.
- PEAP: il protocollo PEAP (Protected Extensible Authentication Protocol) autentica i client LAN (Local Area Network) wireless tramite certificati digitali rilasciati dal server creando un tunnel SSL (Secure Sockets Layer) o TLS (Transport Layer Security) crittografato tra il client e il server di autenticazione.
- TLS: TLS è un protocollo che fornisce sicurezza e integrità dei dati per la comunicazione su Internet. Garantisce che nessuna terza parte manometta il messaggio originale.

Nota: Nell'esempio viene utilizzato MD5.

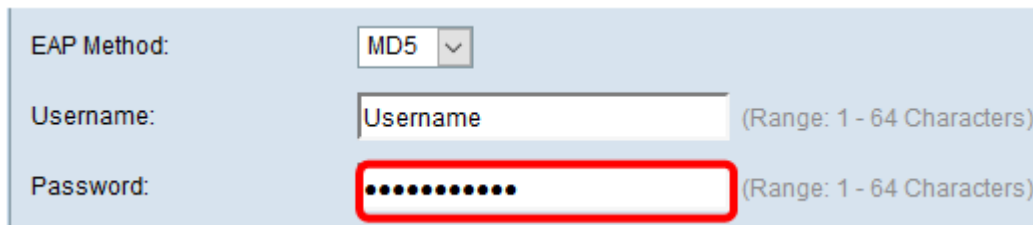
Passaggio 6. Inserire il nome utente desiderato nel campo *Nome utente*. Verrà utilizzato quando si risponde a un autenticatore 802.1X. Può contenere fino a 64 caratteri e può includere lettere maiuscole e minuscole, numeri e caratteri speciali, ad eccezione delle virgolette doppie.

EAP Method:

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

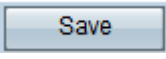
Passaggio 7. Inserire la password preferita nel campo *Password*. La password MD5 viene utilizzata quando si risponde a un autenticatore 802.1X. La password può contenere un massimo di 64 caratteri e può includere lettere maiuscole e minuscole, numeri e caratteri speciali, ad eccezione delle virgolette.



EAP Method: MD5

Username: Username (Range: 1 - 64 Characters)

Password: [Redacted] (Range: 1 - 64 Characters)

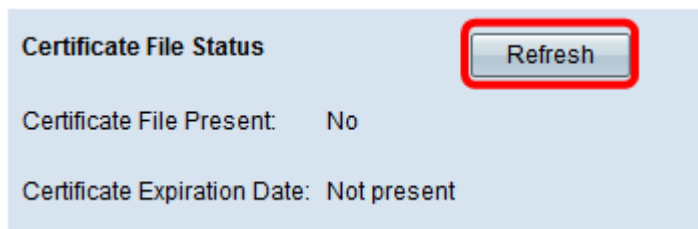
Passaggio 8. Fare clic sul  pulsante.

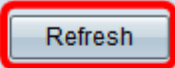
È ora necessario configurare le impostazioni 802.1X Supplicant sul WAP.

Visualizza impostazioni file certificato

Nell'area Stato file certificato viene indicato se il file di certificato è presente o meno. Il certificato SSL è un certificato firmato digitalmente da un'autorità di certificazione che consente al browser di comunicare in modo sicuro con il server Web.

Passaggio 1. Per visualizzare lo stato corrente del file di certificato, fare clic su **Aggiorna**.



Certificate File Status 

Certificate File Present: No

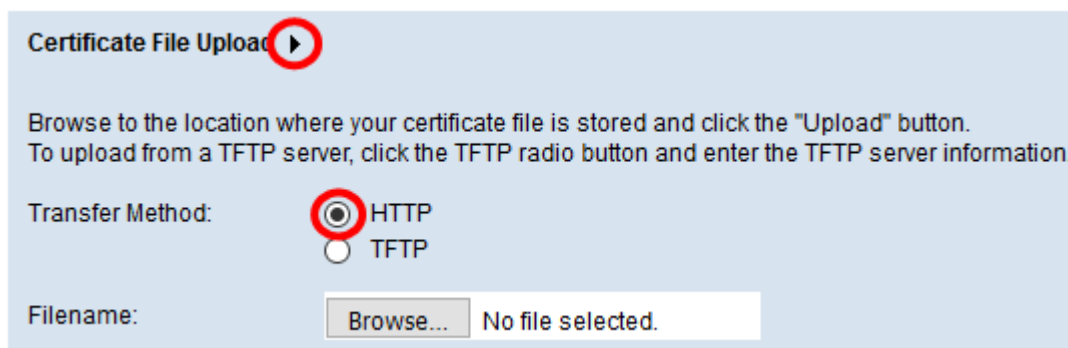
Certificate Expiration Date: Not present


L'area Stato file certificato contiene i campi riportati di seguito.

- File del certificato presente: indica se il file del certificato è presente o meno.
- Data scadenza certificato: visualizza la data di scadenza del file di certificato corrente.

Carica un file di certificato

Passaggio 1. Fare clic sulla freccia accanto a Caricamento file certificato, quindi scegliere il pulsante di opzione desiderato dal Metodo di trasferimento.



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.

Esistono due metodi per caricare il file:

- HTTP (Hypertext Transfer Protocol)
- Protocollo TFTP (Trivial File Transfer Protocol)

Nota: Nell'esempio viene scelto HTTP.

Passaggio 2. (Facoltativo) Se si sceglie HTTP, fare clic su **Sfoggia** per scegliere il file del

certificato dal computer, quindi andare al [Passaggio 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.

Passaggio 3. (Facoltativo) Se è stato scelto TFTP al passaggio 1, immettere il nome del file del certificato nel campo *Nome file*. Il server TFTP viene utilizzato per trasferire automaticamente i file di avvio all'interno dei dispositivi ed è molto semplice.

Nota: Nell'esempio, *mini_httpd.pem* viene usato come nome del file.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename: (Range: 1 - 256 Characters)

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

Passaggio 4. Immettere l'indirizzo IP del server TFTP nel campo *Indirizzo IPv4 server TFTP*.

Nota: Nell'esempio, l'indirizzo IPv4 del server TFTP è 10.10.11.

Transfer Method: HTTP
 TFTP

Filename: (Range: 1 - 256 Characters)

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

Passaggio 5. Fare clic su **Aggiorna**.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename: (Range: 1 - 256 Characters)

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

Nota: Se si utilizzano altri modelli di WAP, fare clic su **Carica**.

Passaggio 6. Fare clic sul pulsante per salvare le impostazioni.

A questo punto dovrebbe essere stato caricato correttamente un file di certificato sul WAP.