

# Configurazione delle impostazioni del supporto 802.1X su un WAP125 o WAP581

## Obiettivo

Il supplicant è uno dei tre ruoli dello standard 802.1X IEEE. Lo standard 802.1X è stato sviluppato per garantire la sicurezza nel layer 2 del modello OSI. 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.

In questo documento viene spiegato come configurare l'access point WAP125 o WAP581 come supplicant 802.1X.

**Nota:** per informazioni su come configurare le credenziali del richiedente 802.1X sullo switch, fare clic [qui](#).

## Dispositivi interessati

- WAP125
- WAP581

## Versione del software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

## Configurazione del supplicant 802.1X

### Configura credenziali richiedente

Passaggio 1. Accedere all'utilità basata sul Web di WAP. Il nome utente e la password predefiniti sono cisco/cisco.



## Wireless Access Point

cisco

.....|

English

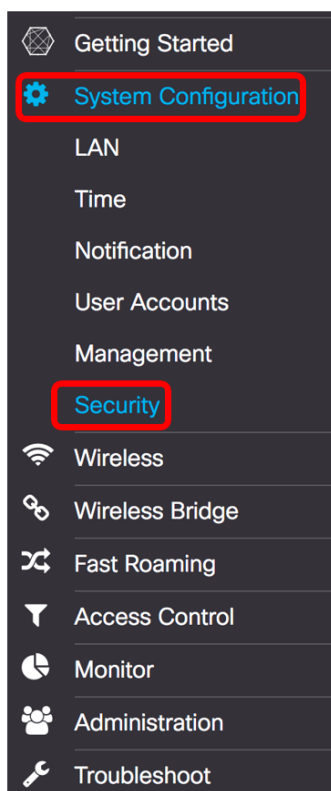
Login

©2017 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

**Nota:** Se la password è già stata modificata o è stato creato un nuovo account, immettere le nuove credenziali.

Passaggio 2. Scegliere **Configurazione di sistema > Sicurezza**.



Passaggio 3. Selezionare la casella di controllo **Abilita** per abilitare la modalità amministrativa. In questo modo il WAP può fungere da supplicant per l'autenticatore.

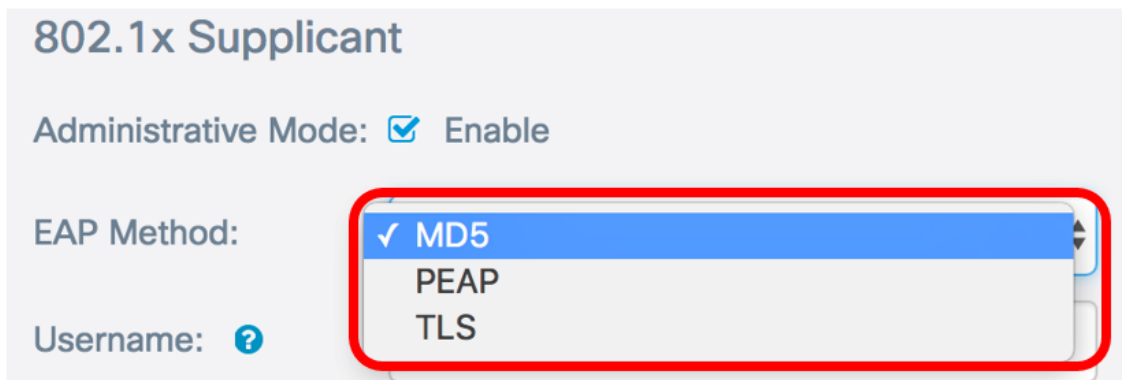
# 802.1x Supplicant

Administrative Mode:  Enable

Passaggio 4. Selezionare il tipo appropriato di metodo EAP (Extensible Authentication Protocol) da utilizzare per crittografare nomi utente e password dall'elenco a discesa *Metodo EAP*. Le opzioni sono:

- MD5: utilizza il metodo di crittografia a 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 wireless tramite certificati digitali rilasciati dal server creando un tunnel SSL/TLS crittografato tra il client e il server di autenticazione.
- TLS — Transport Layer Security (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.



802.1x Supplicant

Administrative Mode:  Enable

EAP Method: ✓ MD5  
PEAP  
TLS

Username: 

Passaggio 5. Inserire un nome utente nel campo *Nome utente*. Questo è il nome utente configurato sull'autenticatore e utilizzato per rispondere all'autenticatore 802.1X. Può contenere da uno a 64 caratteri e può includere lettere maiuscole e minuscole, numeri e caratteri speciali ad eccezione delle virgolette doppie.

**Nota:** Nell'esempio viene utilizzato UserAccess\_1.

### 802.1x Supplicant

Administrative Mode:  Enable

EAP Method: MD5

Username:

Passaggio 6. Immettere una password associata al nome utente nel campo *Password*. Questa password MD5 viene utilizzata per rispondere all'autenticatore 802.1X. La password può contenere da uno a 64 caratteri e può includere lettere maiuscole e minuscole, numeri e caratteri speciali ad eccezione delle virgolette.

### 802.1x Supplicant

Administrative Mode:  Enable

EAP Method: MD5

Username:

Password:

Passaggio 7. Fare clic sul pulsante **Salva** per salvare le impostazioni configurate.

# Security

**Save**

## 802.1x Supplicant

Administrative Mode:  Enable

EAP Method:

Username:

Password:

A questo punto, è necessario configurare le impostazioni di Supplicant 802.1X nel WAP.

### Caricamento file di certificato

Passaggio 1. Dal metodo di trasferimento, scegliere un metodo che WAP utilizzerà per ottenere il certificato SSL. 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. Le opzioni sono:

- HTTP: il certificato viene caricato tramite il protocollo HTTP (Hyper Text Transfer Protocol) o il browser.
- TFTP: il certificato viene caricato tramite un server TFTP (Trivial File Transfer Protocol). Se si sceglie questo comando, andare al [passo 3](#). Sarà necessario immettere il nome del file e l'indirizzo TFTP.

**Nota:** Nell'esempio viene scelto HTTP.

## Certificate File Upload

Transfer Method:  HTTP  TFTP

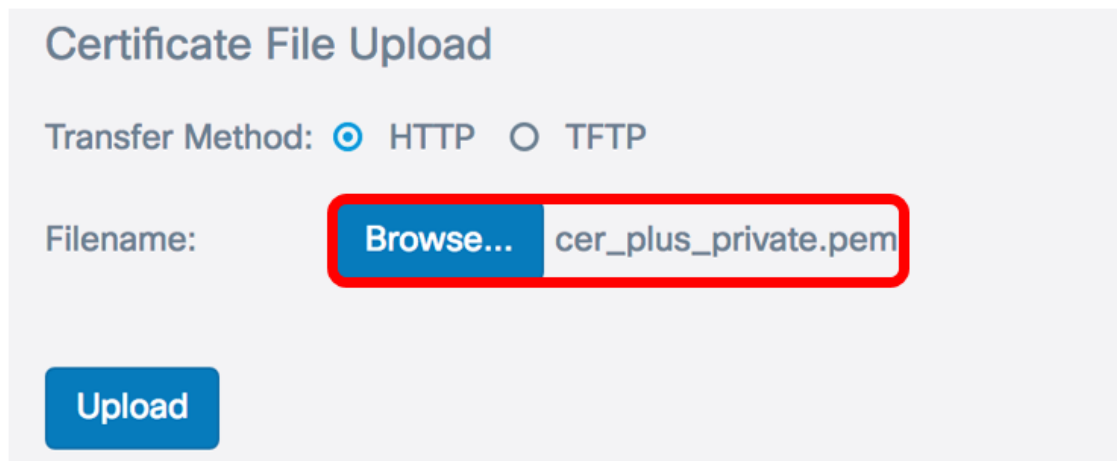
Filename:  cer\_plus\_private.pem

**Upload**

### Metodo di trasferimento HTTP

Passaggio 2. (Facoltativo) Se è stato scelto HTTP, fare clic su **Sfoggia...** e scegliere il certificato SSL.

**Nota:** Nell'esempio viene utilizzato cer\_plus\_private.pem.

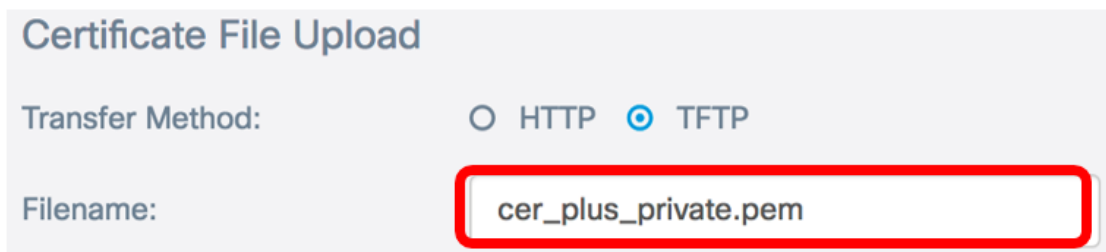


The screenshot shows the 'Certificate File Upload' form. The 'Transfer Method' is set to 'HTTP' (selected with a blue radio button). The 'Filename' field contains 'cer\_plus\_private.pem' and is highlighted with a red box. A blue 'Browse...' button is visible to the left of the filename. A blue 'Upload' button is located at the bottom left of the form.

## Metodo di trasferimento TFTP

[Passaggio 3](#). Se nel passaggio 1 è stato scelto TFTP, immettere il nome del file nel campo Nome file.

**Nota:** Nell'esempio viene utilizzato cer\_plus\_private.pem.



The screenshot shows the 'Certificate File Upload' form. The 'Transfer Method' is set to 'TFTP' (selected with a blue radio button). The 'Filename' field contains 'cer\_plus\_private.pem' and is highlighted with a red box.

Passaggio 4. (Facoltativo) Se si sceglie TFTP come metodo di trasferimento, immettere l'indirizzo IPv4 del server TFTP nel campo *Indirizzo IPv4 server TFTP*. Percorso utilizzato dal punto di accesso Windows per recuperare il certificato.

**Nota:** nell'esempio viene usato 10.21.52.101.



The screenshot shows the 'Certificate File Upload' form. The 'Transfer Method' is set to 'TFTP' (selected with a blue radio button). The 'Filename' field contains 'cer\_plus\_private.pem'. The 'TFTP Server IPv4 Address' field contains '10.21.52.101' and is highlighted with a red box.

Passaggio 5. Fare clic su **Upload**.

## 802.1x Supplicant

Administrative Mode:  Enable

EAP Method:

Username:

Password:

## Certificate File Upload

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

A questo punto, è necessario aver caricato correttamente un certificato nel WAP.