Configurazione delle impostazioni del supporto 802.1X su WAP131 e WAP371

Obiettivo

L'autenticazione IEEE 802.1X consente al dispositivo WAP di accedere a una rete cablata protetta. È possibile abilitare il dispositivo WAP come supplicant 802.1X (client) sulla rete cablata. È possibile configurare un nome utente e una password crittografati per consentire l'autenticazione del dispositivo WAP utilizzando 802.1X.

Nelle reti che utilizzano il controllo degli accessi alla rete basato sulle porte IEEE 802.1X, un supplicant non può accedere alla rete finché l'autenticatore 802.1X non concede l'accesso. Se la rete utilizza 802.1X, è necessario configurare le informazioni di autenticazione 802.1X sul dispositivo WAP in modo che possa fornirle all'autenticatore.

L'obiettivo di questo documento è mostrare come configurare le impostazioni 802.1X Supplicant su WAP131 e WAP371.

Dispositivi interessati

·WAP131

·WAP371

Versione del software

·v1.0.0.39 (WAP131)

·v1.2.0.2 (WAP371)

Configurazione Delle Impostazioni Del Supplicant 802.1X

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Protezione sistema > Supplicant 802.1X**. Viene visualizzata la pagina *802.1X Supplicant*.

802.1X Supplicant		
Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5 💌	
Username:		(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)
Certificate File Status	Refresh	
Certificate File Present:	No	
Certificate Expiration Date:	Not present	
Browse to the location whe To upload from a TFTP ser	re your certificate file is stored and click the ver, click the TFTP radio button and enter t	e "Upload" button. he TFTP server information.
Certificate File Upload		
Transfer Method:	 HTTP TFTP 	
Filename:	Browse No file selected.	
Upload		
Save		

Configurazione supplicant

Passaggio 1. Passare all'area *Configurazione supplicant*. Nel campo *Modalità amministrativa* , selezionare la casella di controllo **Attiva** per abilitare la funzionalità 802.1X supplicant.

Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5 💌	
Username:		(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)

Passaggio 2. Nell'elenco a discesa *Metodo EAP*, scegliere l'algoritmo che verrà utilizzato per crittografare i nomi utente e le password. EAP è l'acronimo di Extensible Authentication Protocol ed è utilizzato come base per gli algoritmi di crittografia.

Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5 🔽	
Username:	MD5 PEAP	(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)

Le opzioni disponibili sono:

·MD5: l'algoritmo MD5 message-digest utilizza una funzione hash per fornire la sicurezza di base. Questo algoritmo non è consigliato, in quanto gli altri due hanno una protezione più elevata.

·PEAP: PEAP è l'acronimo di Protected Extensible Authentication Protocol. Incapsula il protocollo EAP e offre una sicurezza maggiore rispetto a MD5, utilizzando un tunnel TLS per trasmettere i dati.

·TLS: TLS è l'acronimo di Transport Layer Security ed è uno standard aperto che fornisce un alto livello di sicurezza.

Passaggio 3. Nel campo *Username*, immettere il nome utente che il dispositivo WAP utilizzerà per rispondere alle richieste di un autenticatore 802.1X. Il nome utente deve avere una lunghezza compresa tra 1 e 64 caratteri e può includere caratteri alfanumerici e speciali.

Supplicant Configuration		
Administrative Mode:	Enable	
EAP Method:	MD5	
Username:	username1	(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)

Passaggio 4. Nel campo *Password*, immettere la password che il dispositivo WAP utilizzerà per rispondere alle richieste di un autenticatore 802.1X. Il nome utente deve avere una lunghezza compresa tra 1 e 64 caratteri e può includere caratteri alfanumerici e speciali.

Supplicant Configuration		
Administrative Mode:	✓ Enable	
EAP Method:	MD5	
Username:	username1	(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)

Passaggio 5. Fare clic su Salva.

Supplicant Configuration			
Administrative Mode:	Enable		
EAP Method:	MD5 💌		
Username:	username1	(Range: 1 - 64 Characters)	
Password:	•••••	(Range: 1 - 64 Characters)	
Certificate File Status	Refresh		
Certificate File Present:	No		
Certificate Expiration Date:	Not present		
Browse to the location whe To upload from a TFTP ser	ere your certificate file is stored and click th ver, click the TFTP radio button and enter	e "Upload" button. the TFTP server information.	
Certificate File Upload			
Transfer Method:	HTTPTFTP		
Filename:	Browse No file selected.		
Upload			
Save			

Stato file certificato

Passaggio 1. Passare all'area *Stato file certificato*. In quest'area viene indicato se il dispositivo WAP contiene un file di certificato SSL HTTP. Nel campo *File certificato presente* verrà visualizzato "Sì" se è presente un certificato. il valore predefinito è "No". Se è presente un certificato, la *data di scadenza* del *certificato* sarà indicata al momento della scadenza; in caso contrario, il valore predefinito è "Not presence" (Non presente).

Certificate File Status		Refresh
Certificate File Present:	No	
Certificate Expiration Date:	Not present	

Passaggio 2. Per visualizzare le informazioni più recenti, fare clic sul pulsante **Aggiorna** per ottenere le informazioni più aggiornate sul certificato.

Certificate File Status		Refresh
Certificate File Present:	Yes	
Certificate Expiration Date:	Aug 22 16:41:51 2018 GMT	

Caricamento file di certificato

Passaggio 1. Passare all'area di *caricamento dei file di certificato* per caricare un certificato HTTP SSL nel dispositivo WAP. Nel campo *Metodo di trasferimento*, selezionare i pulsanti di opzione HTTP o TFTP per scegliere il protocollo da utilizzare per caricare il certificato.

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.		
Certificate File Upload		
Transfer Method:	 HTTP TFTP 	
Filename:	Browse No file selected.	
Upload		

Passaggio 2. Se è stato selezionato **TFTP**, passare al Passaggio 3. Se è stato selezionato **HTTP**, fare clic sul pulsante **Sfoglia...** per trovare il file del certificato sul PC. Andare al passo <u>5</u>.

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.		
Certificate File Upload		
Transfer Method:	 HTTP TFTP 	
Filename:	Browse No file selected.	
Upload		

Passaggio 3. Se è stato selezionato **TFTP** nel campo *Metodo di trasferimento*, immettere nel nome file del certificato il nome file nel campo *Nome file*.

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. Certificate File Upload Transfer Method:

HTTP
TFTP

Filename:

certificate.pem
(Range: 1 - 256 Characters)

TFTP Server IPv4 Address:

(xxx.xxx.xxx.xxx)

Nota: Il file deve terminare con .pem.

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

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.		
Certificate File Upload		
Transfer Method:	HTTPTFTP	
Filename:	certificate.pem	(Range: 1 - 256 Characters)
TFTP Server IPv4 Address:	192.168.1.100	(xxx.xxx.xxxx)
Upload		

Passaggio 5. Fare clic su 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.

Certificate File Upload		
Transfer Method:	HTTPTFTP	
Filename:	certificate.pem	(Range: 1 - 256 Characters)
TFTP Server IPv4 Address:	192.168.1.100	(xxx.xxx.xxx.xxx)
Upload		

Passaggio 6. Viene visualizzata una finestra di conferma. Fare clic su **OK** per avviare il caricamento.

Confirm	
	Device is uploading the certificate file now.
	OK Cancel

Passaggio 7. Fare clic su **Salva**.