Configurazione delle impostazioni 802.1X su WAP351

Obiettivo

L'autenticazione IEEE 802.1X consente al dispositivo WAP di accedere a una rete cablata protetta. È possibile configurare il dispositivo WAP come supplicant 802.1X (client) sulla rete cablata. WAP351 può anche essere configurato come autenticatore. 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 del supporto 802.1X su WAP351.

Dispositivi interessati

·WAP351

Versione del software

·v1.0.1.3

Configurazione Delle Impostazioni Del Supplicant 802.1X

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

802.1X					
Port Table					
	Port No.	Enable	Role		
	1		Supplicant -	Show Details	
	2		Supplicant -	Show Details	
	3		Supplicant 🔻	Show Details	
	4		Supplicant 💌	Show Details	
	5		Supplicant 🔻	Show Details	
	Edit				
Sa	ve				

Passaggio 2. La *tabella delle porte* mostra cinque interfacce LAN che possono essere configurate per l'autenticazione 802.1X. Selezionare le caselle di controllo corrispondenti alle porte che si desidera modificare.

302.1X					
Port	Table				
	Port No.	Enable	Role		
			Supplicant 🔹	Show Details	
	2		Supplicant -	Show Details	
	3		Supplicant -	Show Details	
	4		Supplicant -	Show Details	
5 Supplicant Show Details					
Edit					
Save					

Passaggio 3. Fare clic sul pulsante **Modifica**. Le porte selezionate saranno disponibili per la modifica.

802.1X						
Port	t Table					
	Port No.	Enable	Role			
V			Supplicant	•	Show Details	
	2		Supplicant	•	Show Details	
	3		Supplicant	•	Show Details	
	4		Supplicant	•	Show Details	
	5		Supplicant	•	Show Details	
	Edit					
Sa	ve					

Passaggio 4. Nel campo *Enable*, selezionare le caselle di controllo delle porte su cui si desidera abilitare le impostazioni 802.1X.

8	802.1X						
	Port Table						
		Port No.	Enable	Role			
	V			Supplicant	•	Show Details	
		2		Supplicant	•	Show Details	
		3		Supplicant	•	Show Details	
		4		Supplicant	•	Show Details	
		5		Supplicant	•	Show Details	
	Edit						
	Save						

Passaggio 5. Nell'elenco a discesa *Ruolo* selezionare se la porta corrispondente verrà configurata come **Supplicant** o come **Authenticator**. Se si sceglie Supplicant, passare alla sezione *Configurazione impostazioni supplicant*. Se si sceglie Autenticatore, andare alla sezione *Configurazione delle impostazioni dell'autenticatore*. Un autenticatore si trova tra il client (supplicant) che desidera accedere alla rete e il server RADIUS stesso. È responsabile della gestione di tutte le comunicazioni tra i due. Un richiedente fornisce le credenziali a un autenticatore per accedere alla rete. In un'impostazione tipica sul modello WAP351, la porta WAN è Supplicant (in modo che il WAP possa accedere alla rete) e le porte LAN sono

Authenticator (in modo che il WAP possa autorizzare i dispositivi sottostanti).

8	802.1X					
	Port Table					
		Port No.	Enable	Role		
	V		V	Supplicant 💌	Show Details	
		2		Supplicant Authenticator	Show Details	
		3		Supplicant 💌	Show Details	
		4		Supplicant 🔻	Show Details	
		5		Supplicant 💌	Show Details	
	Edit					
	Save					

Configurazione impostazioni supplicant

Passaggio 1. Fare clic su **Mostra dettagli** per visualizzare le informazioni sulle impostazioni del supplicant.

Port	Table		
	Port No.	Enable	Role
<		V	Supplicant Hidden Details
	1		Supplicant Hitdlen Details EAP Method: MD5 Username: (Range: 1 - 64 Characters) Password: Password: (Range: 1 - 64 Characters) Certificate File Status Refresh Certificate File Present: No Certificate Expiration Date: Not Present 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
	2		Filename Browse No file selected.

Nota: Queste informazioni potrebbero aprirsi automaticamente dopo aver effettuato una selezione nel campo *Modalità*.

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.

EAP Method: MD5						
Username: PEAP TLS	(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 where your certificate file is stored and cli To upload from a TFTP server, click the TFTP radio button and e	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						

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.

EAP Method:	MD5 💌						
Username:	username1	(Range: 1 - 64 Characters)					
Password:		(Range: 1 - 64 Characters)					
Certificate File Status Certificate File Present:	Certificate File Status Refresh Certificate File Present: No						
Certificate Expiration Da	te: Not Present						
Browse to the location v To upload from a TFTP	where your certificate file is stored and cli server, click the TFTP radio button and e	ick the "Upload" button. nter the TFTP server information.					
Certificate File Upload	I						
Transfer Method: H T 	ITTP FTP						
Filename Bro	wse No file selected.						
Upload							

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.

EAP Method:	MD5 •	
Username:	username1	(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)
Certificate File Statu	Is Refresh	
Certificate File Preser	it: No	
Certificate Expiration I	Date: Not Present	
Browse to the locatior To upload from a TFT	where your certificate file is stored and P server, click the TFTP radio button an	click the "Upload" button. d enter the TFTP server information.
Certificate File Uplo	ad	
Transfer Method:	HTTP TFTP	
Filename	rowse No file selected.	
Upload		

Passaggio 5. Nell'area *Stato file certificato* viene indicato se nel dispositivo WAP esiste 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). Per visualizzare le informazioni più recenti, fare clic sul pulsante **Aggiorna** per ottenere le informazioni più aggiornate sul certificato.

EAP Method:	MD5 <				
Username:	username1	(Range: 1 - 64 Characters)			
Password:	•••••	(Range: 1 - 64 Characters)			
Certificate File Status	Refresh				
Certificate File Present:	No				
Certificate Expiration Da	te: Not Present				
Browse to the location w To upload from a TFTP s	where your certificate file is stored and cl server, click the TFTP radio button and e	ick the "Upload" button. Inter the TFTP server information.			
Certificate File Upload	I				
Transfer Method: HTTP TFTP 					
Filename Bro	wse No file selected.				
Upload					

Passaggio 6. Se non si desidera caricare un file di certificato SSL HTTP, andare al passaggio 12. In caso contrario, selezionare i pulsanti di opzione HTTP o TFTP nel campo *Metodo di trasferimento* per scegliere il protocollo da utilizzare per caricare il certificato.

EAP Method:	MD5 💌	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Status	Refresh	
Certificate File Present:	No	
Certificate Expiration Da	te: Not Present	
Browse to the location w To upload from a TFTP s	here your certificate file is stored and cli server, click the TFTP radio button and e	ck the "Upload" button. hter the TFTP server information.
Certificate File Upload		
Transfer Method: 💿 H 🔘 T	TTP FTP	
Filename	wse No file selected.	
Upload		

Passaggio 7. Se è stato selezionato **TFTP**, andare al Passaggio 8. Se è stato selezionato **HTTP**, fare clic sul pulsante **Sfoglia...** per trovare il file del certificato sul PC. Andare al <u>passo 10</u>.

MD5 💌					
username1	(Range: 1 - 64 Characters)				
•••••	(Range: 1 - 64 Characters)				
Refresh					
No					
e: Not Present					
here your certificate file is stored and c erver, click the TFTP radio button and	lick the "Upload" button. enter the TFTP server information.				
Transfer Method: HTTP TFTP 					
vse No file selected.					
	MD5 username1 Refresh No Refresh No Refresh No Refresh No TTP TP TP Nse No file selected.				

Passaggio 8. Se è stato selezionato **TFTP** nel campo *Metodo di trasferimento*, immettere il nome file del certificato nel campo *Nome file*.

EAP Method:	MD5 💌	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Status Certificate File Present:	Refresh	
Certificate Expiration Da	te: Not Present	
Browse to the location w To upload from a TFTP s	where your certificate file is stored and cli server, click the TFTP radio button and e	ck the "Upload" button. nter the TFTP server information.
Transfer Method:	HTTPTFTP	
Filename	certificate.pem	(Range: 1 - 256 Characters)
TFTP Server IPv4 Addre	ss:	(XXX.XXX.XXX.XXX)
Upload		

Nota: Il file deve terminare con .pem.

Passaggio 9. Immettere l'indirizzo IP del server TFTP nel campo Indirizzo IPv4 server TFTP.

EAP Method:	MD5 -	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Status	Refresh	
Certificate File Present:	No	
Certificate Expiration Da	te: Not Present	
Browse to the location w To upload from a TFTP s	where your certificate file is stored and clic server, click the TFTP radio button and er	ck the "Upload" button. Inter the TFTP server information.
Certificate File Upload	I	
Transfer Method:	HTTPTFTP	
Filename	certificate.pem	(Range: 1 - 256 Characters)
TFTP Server IPv4 Addre	ess: 192.0.2.100	(xxx.xxx.xxx)
Upload		

Passaggio 10. Fare clic su Upload.

EAP Method:	MD5 -	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Stat	us Refresh	
Certificate File Prese	nt: No	
Certificate Expiration	Date: Not Present	
Browse to the location To upload from a TFT	n where your certificate file is stored and o P server, click the TFTP radio button and	lick the "Upload" button. enter the TFTP server information.
Certificate File Uplo	bad	
Transfer Method: ()	HTTP TFTP	
Filename	Browse certificate.pem	
Upload		

Passaggio 11. Viene visualizzata una finestra di conferma. Fare clic su **OK** per avviare il caricamento.

Devic	e is uploading the certificate file now.
	OK Cancel
Certificate File	Present: No
Certificate Exp	ration Date: Not Present
Browse to the To upload from	ocation where your certificate file is stored and click the "Upload" button. a TFTP server, click the TFTP radio button and enter the TFTP server information
Browse to the To upload from Certificate Fil	ocation where your certificate file is stored and click the "Upload" button. a TFTP server, click the TFTP radio button and enter the TFTP server information e Upload
Browse to the To upload from Certificate Fil Transfer Metho	ocation where your certificate file is stored and click the "Upload" button. a TFTP server, click the TFTP radio button and enter the TFTP server information e Upload d: O HTTP TFTP
Browse to the To upload from Certificate Fil Transfer Metho Filename	 a TFTP server, click the TFTP radio button and enter the TFTP server informatie e Upload d: HTTP TFTP Browse certificate.pem

Passaggio 12. Ripetere questa sezione per ciascuna porta che si desidera configurare come supplicant 802.1X. Quindi, fare clic su **Salva**.

8	802.1X							
	Port	Table						
		Port No.	Enable	Role				
	✓		V	Supplicant	•	Show Details		
		2		Supplicant	•	Show Details		
		3		Supplicant	•	Show Details		
		4		Supplicant	•	Show Details		
		5		Supplicant	-	Show Details		
(Edit							
C	Save							

Configurazione impostazioni autenticatore

Passaggio 1. Fare clic su **Mostra dettagli** per visualizzare le informazioni sulle impostazioni dell'autenticatore.

Port	Table							
	Port No.	Enable	Role					
V			Authenticator Hidden Details					
			 ✓ Use global RADIUS server settings Server IP Address Type: IPv4 IPv6 ✓ IPv6 					
			No. Server IP Address (xxx.xxx.xxx.xxx) Key (Range: 1 - 64 Characters) Authentication Port (Range: 0 - 65535, Default: 1812)					
			1 0.0.0.0 1812					
			2 1812					
			3 1812					
			4 1812					
			Enable RADIUS Accounting Active Server: Server IP Address-1 Periodic Reauthentication: Enable Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)					
	2		Supplicant Show Details					

Nota: Queste informazioni potrebbero aprirsi automaticamente dopo aver effettuato una selezione nel campo *Modalità*.

Passaggio 2. Selezionare la casella di controllo *Utilizza impostazioni globali del server RADIUS* se si desidera che la porta utilizzi le impostazioni globali RADIUS durante l'autenticazione. Se si desidera che la porta utilizzi uno o più server RADIUS diversi, deselezionare questa casella di controllo; in caso contrario, andare al <u>passaggio 8</u>.

Use global RADIUS server settings						
00110		IPv6				
No.	Server IP Address (XXXX.XXXX.XXXX)	Key (Range: 1 - 6	4 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)		
1	0.0.0.0			1812		
2				1812		
3				1812		
4				1812		
E	Enable RADIUS Accou	unting				
Active Server: Server IP Address-1						
Periodic Reauthentication: Enable						
Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)						

Nota: Per ulteriori informazioni, vedere l'articolo Configurazione delle impostazioni globali del

server RADIUS su WAP131 e WAP351.

Passaggio 3. Nel campo *Tipo di indirizzo IP server*, selezionare il pulsante di opzione per la versione IP utilizzata dal server RADIUS. Le opzioni disponibili sono **IPv4** e **IPv6**.

Use global RADIUS server settings Server IP Address Type: IPv4 IPv6								
No.	Server IP Address (xxx.xxx.xxx)		Key (Range: 1 - 64	Characters)	Aut (Ra	hentication Port ange: 0 - 65535, Default: 1812)		
1	0.0.0.0				ſ	1812		
2					ſ	1812		
3					ſ	1812		
4					ſ	1812		
E	Enable RADIUS Accou	unting						
Active	Server:	Server IP	Address-1					
Period	lic Reauthentication:	Enab	le					
Reaut	hentication Period:	3600		sec. (Range: 3	300 - 4	4294967295, Default: 3600)		

Nota: È possibile passare da un tipo di indirizzo all'altro per configurare le impostazioni degli indirizzi RADIUS IPv4 e IPv6, ma il dispositivo WAP contatta solo il server o i server RADIUS con il tipo di indirizzo selezionato in questo campo. Non è possibile che più server utilizzino tipi di indirizzo diversi in un'unica configurazione.

Passaggio 4. Nel campo *Indirizzo IP server 1* o *Indirizzo IPv6 server 1* immettere un indirizzo IPv4 o IPv6 per il server RADIUS a seconda del tipo di indirizzo scelto nel passaggio 3.

Use global RADIUS server settings Server IP Address Type: IPv4 IPv6							
No.	Server IP Address (XXX.XXX.XXX.XXX)	Key (Range: 1 - 64 Cl	Authentication Port (Range: 0 - 65535, Default: 1812)				
1	192.0.2.1		1812				
2			1812				
3			1812				
4			1812				
E	Enable RADIUS Accou	inting					
Active	Server:	Server IP Address-1					
Period	lic Reauthentication:	Enable					
Reaut	hentication Period:	3600 se	c. (Range: 300 - 4294967295, Default: 3600)				

Nota: L'indirizzo immesso in questo campo designerà il server RADIUS primario della porta. Gli indirizzi immessi nei campi successivi (*Indirizzo IP server da 2* a *4*) designeranno i server RADIUS di backup che verranno eseguiti in sequenza se l'autenticazione non riesce con il server primario.

Passaggio 5. Nel campo *Chiave* immettere la chiave segreta condivisa corrispondente al server RADIUS primario utilizzato dal dispositivo WAP per l'autenticazione al server RADIUS. È possibile utilizzare da 1 a 64 caratteri alfanumerici e speciali standard. Ripetere questo passaggio per ogni server RADIUS successivo configurato per la porta nei campi da *Key 2* a *4*.

Serve	 Use global RADIUS server settings Server IP Address Type: IPv4 IPv6 							
No.	Server IP Address (XXXX.XXXX.XXXX)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)					
1	192.0.2.1		1812					
2			1812					
3			1812					
4			1812					
E	Enable RADIUS Accou	inting						
Active	Server:	Server IP Address-1						
Period	lic Reauthentication:	Enable						
Reaut	hentication Period:	3600 sec. (Range:	300 - 4294967295, Default: 3600)					

Nota: Le chiavi fanno distinzione tra maiuscole e minuscole e devono corrispondere alla chiave configurata nel server RADIUS.

Passaggio 6. Nel campo *Authentication Port* (Porta di autenticazione), immettere la porta che verrà utilizzata da WAP per connettersi al server RADIUS. Ripetere questo passaggio per ogni server RADIUS di backup configurato nei campi da *Porta di autenticazione 2* a *4*. Il valore predefinito è 1812.

Use global RADIUS server settings Server IP Address Type: IPv4 IPv6							
No.	Server IP Address (XXXX.XXXX.XXXX)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)				
1	192.0.2.1		1812				
2			1812				
3			1812				
4			1812				
E	Enable RADIUS Accou	unting					
Active	Server:	Server IP Address-1					
Period	lic Reauthentication:	Enable					
Reaut	hentication Period:	3600 sec. (Range	e: 300 - 4294967295, Default: 3600)				

Passaggio 7. Selezionare la casella di controllo Abilita accounting RADIUS per abilitare la

registrazione e la misurazione delle risorse utilizzate da un utente (tempo di sistema, quantità di dati trasmessi e così via). Selezionando questa casella di controllo verrà attivato l'accounting RADIUS per i server primario e di backup.

Use global RADIUS server settings Server IP Address Type: IPv4 IPv6								
No.	Server IP Address (XXX.XXX.XXXX)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)					
1	192.0.2.1	•••••	1812					
2	192.0.2.2	•••••	2500					
3			1812					
4			1812					
E	Enable RADIUS Accou	unting	,					
Active Server: Server IP Address-1								
Periodic Reauthentication: Enable								
Reaut	hentication Period:	3600 sec. (Range:	300 - 4294967295, Default: 3600)					

Passaggio 8. Nell'elenco a discesa *Server attivo* scegliere uno dei server RADIUS configurati da impostare come server attivo. Questa impostazione consente a WAP di tentare immediatamente di contattare il server attivo, anziché tentare di contattare ciascun server in sequenza e scegliendo il primo disponibile.

 Use global RADIUS server settings Server IP Address Type: IPv4 IPv6 						
No.	Server IP Address (XXXX.XXXX.XXXX)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)			
1	192.0.2.1	•••••	1812			
2	192.0.2.2	•••••	2500			
3			1812			
4			1812			
Enable RADIUS Accounting						
Active Server: Server IP Address-1						
Periodic Reauthentication: Server IP Address-1 Server IP Address-2 Server IP Address-3 Server IP Address-4 Server IP Address-4 Server IP Address-4 Server IP Address-4						

per attivare la riautenticazione EAP. Se non si desidera abilitare la riautenticazione EAP, andare al <u>passaggio 11</u>.

Use global RADIUS server settings Server IP Address Type: IPv4 IPv6						
No.	Server IP Address (XXXXXXXXXXXXXXXX)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)			
1	192.0.2.1	•••••	1812			
2	192.0.2.2	•••••	2500			
3			1812			
4			1812			
Enable RADIUS Accounting						
Active Server: Server IP Address-1						
Periodic Reauthentication: 🗵 Enable						
Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)						

Passaggio 10. Se è stata selezionata la casella di controllo **Abilita** nel campo *Riautenticazione periodica*, immettere il periodo di riautenticazione EAP in secondi nel campo *Periodo di riautenticazione*. Il valore predefinito è 3600. L'intervallo valido è compreso tra 300 e 4294967295 secondi.

 Use global RADIUS server settings Server IP Address Type: IPv4 IPv6 						
No.	Server IP Address (xxxxxxxxxxxxxxxxxxxxxxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)			
1	192.0.2.1	•••••	1812			
2	192.0.2.2	•••••	2500			
3			1812			
4			1812			
Enable RADIUS Accounting Active Server: Server IP Address-1						
Periodic Reauthentication: 🗹 Enable						
Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)						

Passaggio 11. Ripetere questa sezione per ciascuna porta che si desidera configurare come autenticatore 802.1X. Quindi, fare clic su **Salva**.

802.1X							
Port Table							
	Port No.	Enable	Role				
✓		✓	Authenticator	•	Show Details		
	2		Supplicant	•	Show Details		
	3		Supplicant	•	Show Details		
	4		Supplicant	•	Show Details		
	5		Supplicant	•	Show Details		
Edit							
Save							