

# Configurare le impostazioni di protezione wireless su un WAP

## Introduzione

La configurazione della protezione wireless sul punto di accesso wireless (WAP) è essenziale per proteggere la rete wireless da intrusioni che potrebbero compromettere la privacy dei dispositivi wireless e la trasmissione dei dati sulla rete wireless. È possibile configurare la protezione wireless sulla rete wireless configurando il filtro MAC, WPA/WPA2 (Wi-Fi Protected Access) Personal e WPA/WPA2 Enterprise.

Il filtro MAC viene utilizzato per filtrare i client wireless in modo da accedere alla rete utilizzando i relativi indirizzi MAC. Verrà configurato un elenco di client per consentire o bloccare gli indirizzi dell'elenco per accedere alla rete, a seconda delle preferenze. Per ulteriori informazioni sul filtro MAC, fare clic [qui](#).

WPA/WPA2 Personal e WPA/WPA2 Enterprise sono protocolli di sicurezza utilizzati per proteggere la privacy mediante la crittografia dei dati trasmessi sulla rete wireless. WPA/WPA2 è compatibile con gli standard IEEE 802.11E e 802.11i. Rispetto al protocollo di sicurezza WEP (Wired Equivalent Privacy), WPA/WPA2 ha migliorato le funzionalità di autenticazione e crittografia.

WPA/WPA2 Personal è per uso domestico e WPA/WPA2 Enterprise è per reti aziendali. WPA/WPA2 Enterprise offre maggiore sicurezza e controllo centralizzato sulla rete rispetto a WPA/WPA2 Personal.

In questo scenario, la protezione wireless verrà configurata sul server WAP per proteggere la rete da intrusi tramite le impostazioni personali ed aziendali di WPA/WPA2.

## Obiettivo

In questo articolo viene illustrato come configurare i protocolli di protezione WPA/WPA2 Personale ed Enterprise per migliorare la protezione e la privacy della rete wireless.

**Nota:** In questo articolo si presume che un SSID (Service Set Identifier) o una WLAN (Wireless Local Area Network) sia già stato creato sul WAP.

## Dispositivi interessati

- Serie WAP100
- Serie WAP300
- Serie WAP500

## Versione del software

- 1.0.2.14 - WAP131, WAP351
- 1.0.6.5 - WAP121, WAP321
- 1.3.0.4 - WAP371
- 1.1.0.7 - WAP150, WAP361

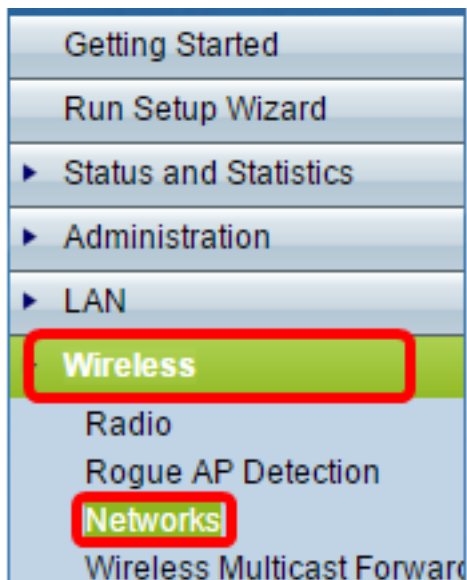
- 1.2.1.5 - WAP551, WAP561
- 1.0.1.11 - WAP571, WAP571E

## Configurare le impostazioni di protezione wireless

### Configura WPA/WPA2 Personal

Passaggio 1. Accedere all'utility basata sul Web del punto di accesso e scegliere **Wireless > Reti**.

**Nota:** Nell'immagine seguente, viene utilizzata l'utilità basata sul Web di WAP361. Le opzioni del menu possono variare a seconda del modello del dispositivo.



Passaggio 2. Nell'area dei punti di accesso virtuali (SSID), selezionare la casella di controllo dell'SSID che si desidera configurare e fare clic su **Modifica**.

**Nota:** Nell'esempio, viene scelto VAP1.

Virtual Access Points (SSIDs)										
	VAP No.	Enable	VLAN ID <a href="#">Add New VLAN</a>	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	Cisco_Lobby	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Passaggio 3. Fare clic su **WPA Personale** dall'elenco a discesa Protezione.

Virtual Access Points (SSIDs)						
VAP No.	Enable	VLAN ID <a href="#">Add New VLAN</a>	SSID Name	SSID Broadcast	Security	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	Cisco_Lobby	<input checked="" type="checkbox"/>	None	<div style="border: 2px solid red; padding: 2px;">           None            None            WPA Personal            WPA Enterprise         </div>

Passaggio 4. Selezionare la casella di controllo per scegliere la versione WPA (WPA-TKIP o WPA2-AES). Due possono essere scelti contemporaneamente.

- WPA-TKIP — Strumento di integrità della chiave temporale di accesso protetto Wi-Fi. La rete dispone di alcune stazioni client che supportano solo il protocollo di sicurezza WPA e TKIP originale. Si noti che la scelta solo di WPA-TKIP come punto di accesso non è consentita in base al più recente requisito di Wi-Fi Alliance.
- WPA2-AES — Wi-Fi Protected Access-Advanced Encryption Standard. Tutte le stazioni client della rete supportano il protocollo di cifratura/sicurezza WPA2 e AES-CCMP. Questa versione WPA offre la migliore protezione per lo standard IEEE 802.11i. In base all'ultimo requisito di Wi-Fi Alliance, il WAP deve supportare sempre questa modalità.

**Nota:** In questo esempio entrambe le caselle di controllo sono selezionate.

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Below Minimum

Broadcast Key Refresh Rate  Sec (Range: 0-86400, 0 =

Passaggio 5. Creare una password composta da 8-63 caratteri e immetterla nel campo *Chiave*.

WPA Versions:  WPA-TKIP  WPA2-AES

Key: ..... (Range: 8-63 Characters)

Show Key as Clear Text


Key Strength Meter:  Strong

**Nota:** È possibile selezionare la casella **Mostra chiave come testo non crittografato** per visualizzare la password creata.

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

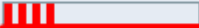
Key Strength Meter:  Strong

Passaggio 6. (Facoltativo) Nel campo *Velocità di aggiornamento chiave trasmissione* immettere un valore per l'intervallo di aggiornamento della chiave di trasmissione (gruppo) per i client associati al VAP. L'impostazione predefinita è 300 secondi e l'intervallo valido è compreso tra 0 e 86400 secondi. Il valore 0 indica che la chiave di trasmissione non viene aggiornata.

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Session Key Refresh Rate

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)

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

Virtual Access Points (SSIDs)				
	VAP No.	Enable	VLAN ID <a href="#">Add New VLAN</a>	SSID Name
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	Cisco_Lobby

A questo punto, è stato configurato WPA Personal su WAP.

## Configura WPA/WPA2 Enterprise

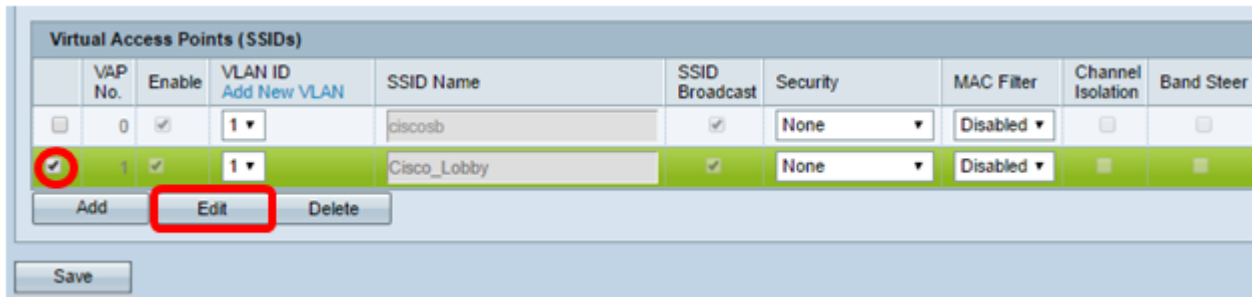
Passaggio 1. Accedere all'utilità basata sul Web del punto di accesso e scegliere **Wireless > Reti**.

**Nota:** Nell'immagine seguente, viene utilizzata l'utilità basata sul Web di WAP361.

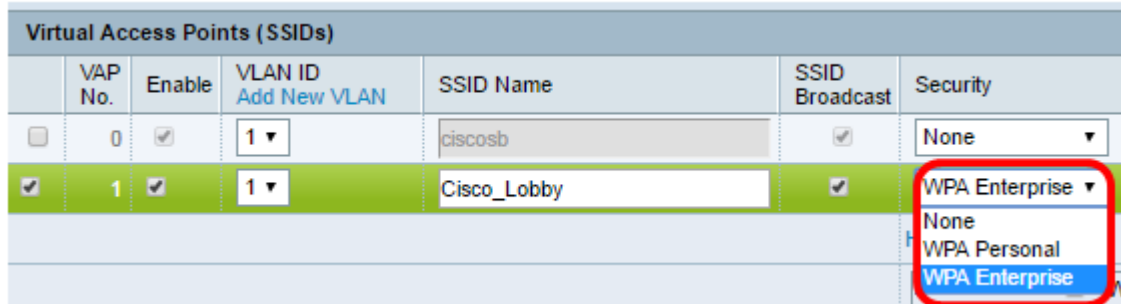
- Getting Started
- Run Setup Wizard
- ▶ Status and Statistics
- ▶ Administration
- ▶ LAN
- Wireless**
- Radio
- Rogue AP Detection
- Networks**
- Wireless Multicast Forwarding

Passaggio 2. Nell'area dei punti di accesso virtuali (SSID), selezionare l'SSID che si

desidera configurare e fare clic sul pulsante **Modifica** sottostante.



Passaggio 3. Scegliere **WPA Enterprise** dall'elenco a discesa Sicurezza.



Passaggio 4. Scegliere la versione WPA (WPA-TKIP, WPA2-AES e Abilita preautenticazione).

- **Abilita preautenticazione:** se si sceglie solo WPA2-AES o entrambe le versioni WPA-TKIP e WPA2-AES, è possibile abilitare la preautenticazione per i client WPA2-AES. Selezionare questa opzione se si desidera che i client wireless WPA2 inviino i pacchetti di preautenticazione. Le informazioni di preautenticazione vengono inoltrate dal dispositivo WAP attualmente utilizzato dal client al dispositivo WAP di destinazione. L'attivazione di questa funzionalità consente di velocizzare l'autenticazione per i client mobili che si connettono a più punti di accesso.

**Nota:** Questa opzione non è applicabile se è stata selezionata l'opzione WPA-TKIP per le versioni WPA, in quanto la WPA originale non supporta questa funzione.

Hide Details

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)  
 Server IP Address-2:  (xxx.xxx.xxx.xxx)  
 Server IP Address-3:  (xxx.xxx.xxx.xxx)  
 Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)  
 Key-2:  (Range: 1 - 64 Characters)  
 Key-3:  (Range: 1 - 64 Characters)  
 Key-4:  (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)  
 Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

Passaggio 5. (Facoltativo) Deselezionare la casella di controllo **Utilizza impostazioni globali del server RADIUS** per modificare le impostazioni.

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)  
 Server IP Address-2:  (xxx.xxx.xxx.xxx)  
 Server IP Address-3:  (xxx.xxx.xxx.xxx)  
 Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)  
 Key-2:  (Range: 1 - 64 Characters)  
 Key-3:  (Range: 1 - 64 Characters)  
 Key-4:  (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)  
 Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

Passaggio 6. (Facoltativo) Fare clic sul pulsante di opzione per il **tipo di indirizzo IP del server** corretto.

**Nota:** Nell'esempio, è stato scelto IPv4.

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)  
Server IP Address-2:  (xxx.xxx.xxx.xxx)  
Server IP Address-3:  (xxx.xxx.xxx.xxx)  
Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)  
Key-2:  (Range: 1 - 64 Characters)  
Key-3:  (Range: 1 - 64 Characters)  
Key-4:  (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:  ▼

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)  
Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

Passaggio 7. Immettere l'indirizzo IP del server RADIUS nel campo *Indirizzo IP server*.

**Nota:** nell'esempio viene usato 192.168.1.101.

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)  
 Server IP Address-2:  (xxx.xxx.xxx.xxx)  
 Server IP Address-3:  (xxx.xxx.xxx.xxx)  
 Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)  
 Key-2:  (Range: 1 - 64 Characters)  
 Key-3:  (Range: 1 - 64 Characters)  
 Key-4:  (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:  ▼

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)  
 Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

Passaggio 8. Nel campo *Chiave* immettere la chiave della password corrispondente al server RADIUS utilizzato da WAP per l'autenticazione al server RADIUS. È possibile utilizzare da 1 a 64 caratteri alfanumerici e speciali standard.

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

Passaggio 9. (Facoltativo) Ripetere i passaggi da 7 a 8 per ogni server RADIUS della rete con cui si desidera comunicare il WAP.



WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)  
Server IP Address-2:  (xxx.xxx.xxx.xxx)  
Server IP Address-3:  (xxx.xxx.xxx.xxx)  
Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)  
Key-2:  (Range: 1 - 64 Characters)  
Key-3:  (Range: 1 - 64 Characters)  
Key-4:  (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:  ▾

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)  
Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

Passaggio 10. (Facoltativo) Selezionare la casella di controllo **Abilita accounting RADIUS** per abilitare il rilevamento e la misurazione delle risorse utilizzate da un utente (tempo di sistema, quantità di dati trasmessi). L'attivazione di questa funzionalità consente l'accounting RADIUS sia per il server primario che per il server di backup.

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6


Server IP Address-1:  (xxx.xxx.xxx.xxx)  
Server IP Address-2:  (xxx.xxx.xxx.xxx)  
Server IP Address-3:  (xxx.xxx.xxx.xxx)  
Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)  
Key-2:  (Range: 1 - 64 Characters)  
Key-3:  (Range: 1 - 64 Characters)  
Key-4:  (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:  ▼

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)  
Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

Passaggio 11. Fare clic su .

Configurazione della protezione WPA/WPA2 Enterprise completata.