

# Configurare le impostazioni di protezione wireless su WAP125 e WAP581

## Obiettivo

Protezione wireless consente di proteggere la rete wireless da accessi non autorizzati. I punti di accesso WAP125 e WAP581 supportano WEP (Static Wired Equivalent Protection), WPA (Wi-Fi Protected Access) Personal e WPA Enterprise. Queste impostazioni possono essere configurate per punto di accesso virtuale (VAP). L'implementazione di queste impostazioni fornisce la protezione di rete per VAP. Viene in genere configurato al momento della prima distribuzione del punto di accesso o quando vengono aggiornati le impostazioni di protezione wireless della rete.

In questo documento viene spiegato come configurare la sicurezza wireless su un access point WAP125 o WAP581.

## Dispositivi interessati

- WAP125
- WAP581

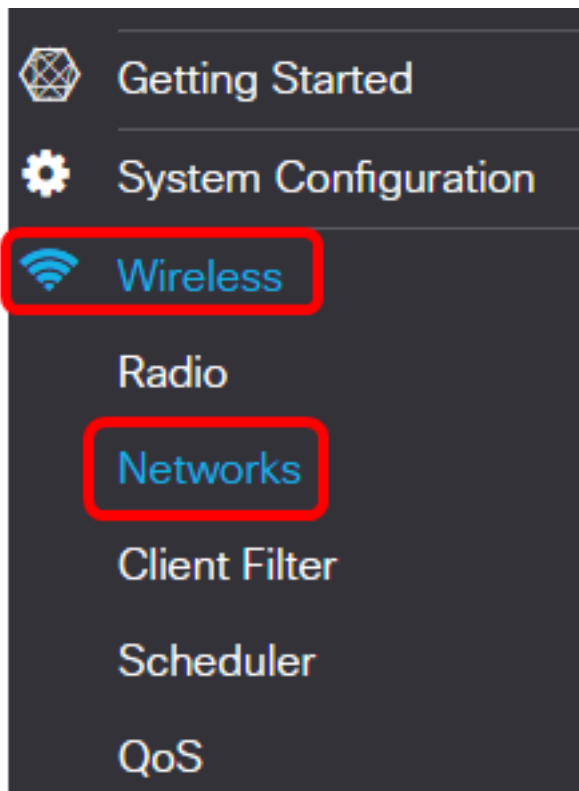
## Versione del software

- WAP125 - 1.0.0.3
- WAP581 - 1.0.0.4

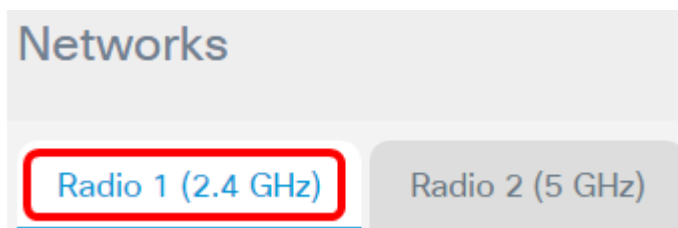
## Configurare le impostazioni di protezione wireless

### Configura protezione personale WPA

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

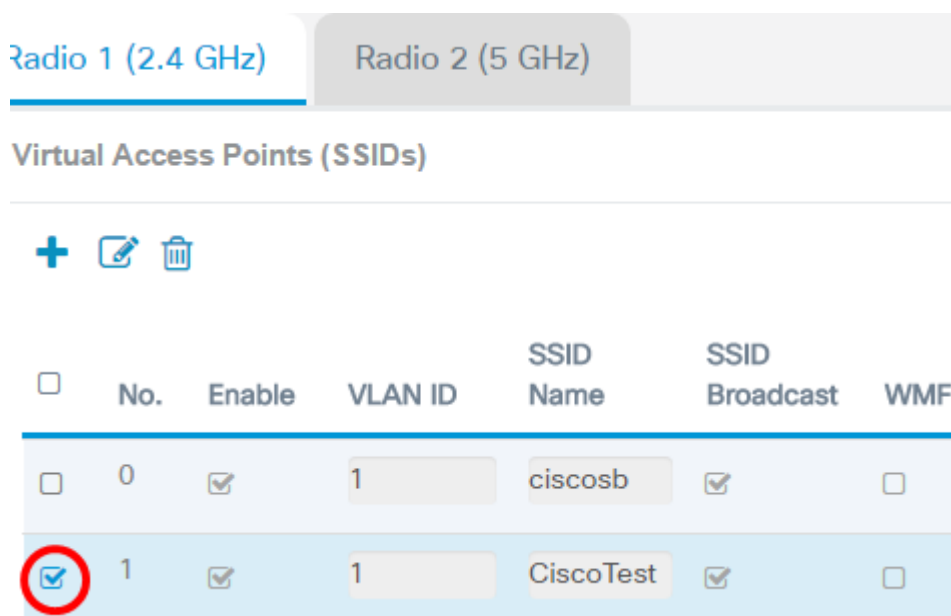


Passaggio 2. Scegliere la radio per la quale è necessario configurare le impostazioni di protezione wireless.



**Nota:** Nell'esempio, viene scelto Radio 1 (2,4 GHz).

Passaggio 3. Selezionare la casella di controllo del VAP di cui configurare le impostazioni di sicurezza wireless.



**Nota:** Nell'esempio, viene scelto VAP 1.

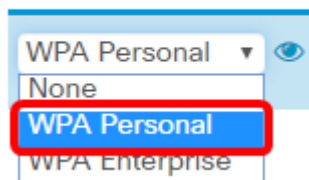
Passaggio 4. Fare clic su **Modifica**.

<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Passaggio 5. Scegliere una modalità di protezione dall'elenco a discesa Protezione. Le opzioni sono:

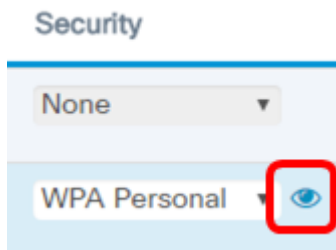
- Nessuna — questa opzione disattiva le impostazioni di sicurezza wireless del VAP selezionato. La disattivazione della modalità di protezione apre la rete wireless e consente a chiunque disponga di un dispositivo wireless di connettersi alla rete e alle relative risorse. Sebbene non sia consigliata, questa modalità può essere utile per le reti in posizioni remote.
- WPA Personal: questa opzione implementa la protezione WPA per la rete wireless. Consente di utilizzare gli algoritmi TKIP (Temporal Key Integrity Protocol) o AES (Advanced Encryption Standard). Se usato insieme, permette ai dispositivi che non supportano l'algoritmo AES di connettersi alla rete. WPA Personal consente di utilizzare una password alfanumerica con una lunghezza massima di 64 caratteri. WPA Personal viene in genere utilizzato negli uffici in cui non viene utilizzato un server RADIUS (Remote Authentication Dial-In User Service).
- WPA Enterprise: questa opzione consente di combinare le funzioni di sicurezza offerte da WPA, utilizzando anche un server RADIUS. Questa funzionalità viene in genere utilizzata negli ambienti in cui viene utilizzato un server RADIUS. Se si sceglie questa opzione, fare clic [qui](#).

#### Security



**Nota:** In questo esempio viene scelto WPA Personal.

Passaggio 6. Fare clic sul pulsante Visualizza per configurare i parametri personali di WPA.



Passaggio 7. Scegliere la versione WPA nell'area Versioni WPA. Le opzioni sono:

- WPA-TKIP: questa opzione implementa la protezione mista sulla rete wireless. È ideale per reti con client wireless misti. Questa opzione è disattivata per impostazione predefinita.
- WPA2-AES: questa opzione implementa la protezione WPA2-AES sulla rete. È ideale per reti wireless con client che supportano la sicurezza WPA2.

### Security Setting

WPA Versions:  WPA-TKIP  WPA2-AES

Key:

Show Key as Clear Text

Key Strength Meter:  Below Minimum

Broadcast Key Refresh Rate

**Nota:** Nell'esempio, viene controllato WPA-TKIP.

Passaggio 8. Immettere la password di rete nel campo *Chiave*. La chiave può essere costituita da una combinazione di lettere e numeri di lunghezza compresa tra 8 e 63 caratteri.

## Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&\*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

**Nota:** Nell'esempio, viene immesso Cisco!@#\$\$%^&\*().

Passaggio 9. (Facoltativo) Selezionare la casella di controllo **Mostra chiave come testo non crittografato** per visualizzare la chiave in testo normale.

## Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&\*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

**Nota:** In questo esempio è selezionata l'opzione Mostra chiave come testo non crittografato.

Passaggio 10. Immettere il numero di secondi che devono trascorrere prima che la chiave di protezione venga sostituita da una chiave appena generata nel campo *Velocità di aggiornamento chiave di trasmissione*. Il valore predefinito è 86400.

## Security Setting

---

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&\*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

Passaggio 11. Fare clic su **OK**.

## Security Setting

---

WPA Versions:

WPA-TKIP

WPA2-AES

Key: [?](#)

Cisco!@#\$\$%^&\*()

Show Key as Clear Text

Key Strength Meter:



Below Minimum

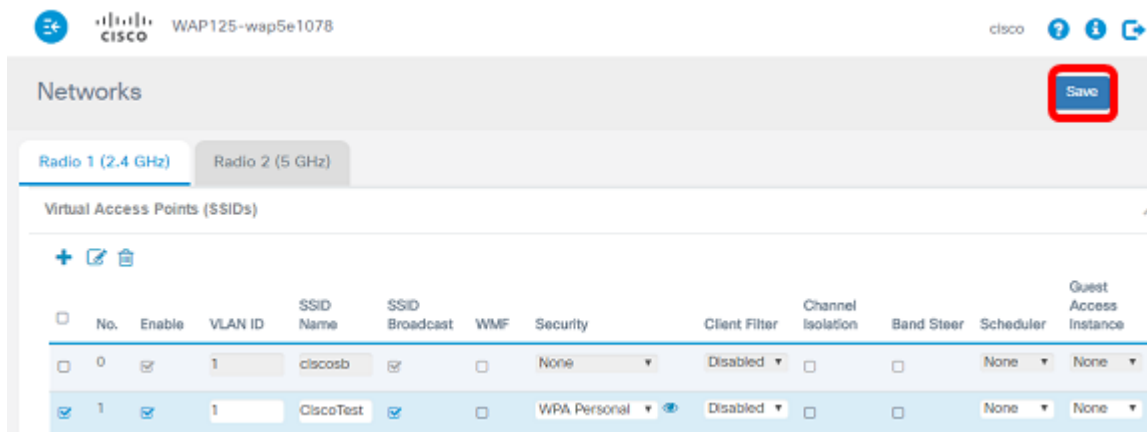
Broadcast Key Refresh Rate [?](#)

86400

OK

cancel

Passaggio 12. Fare clic su **Salva**.

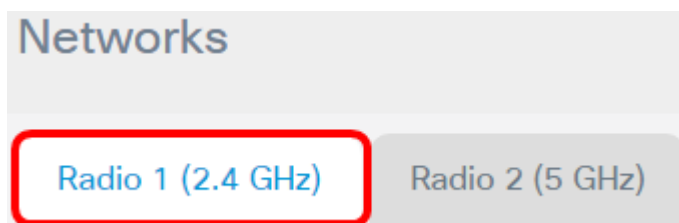


Passaggio 13. Fare clic su **OK**.

Le impostazioni di protezione wireless personale WPA sono state configurate su WAP125.

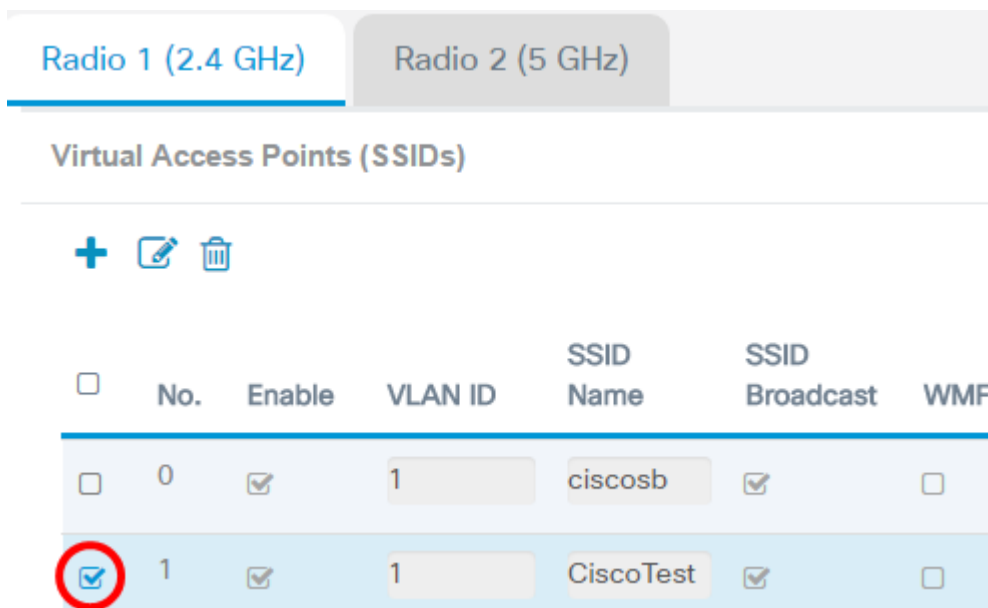
## Configura WPA Enterprise Security

Passaggio 1. Scegliere la radio per la quale è necessario configurare le impostazioni di protezione wireless.



**Nota:** Nell'esempio, viene scelto Radio 1 (2,4 GHz).

Passaggio 2. Selezionare la casella di controllo del VAP di cui configurare le impostazioni di sicurezza wireless.





**Nota:** Nell'esempio, viene scelto VAP 1.

Passaggio 3. Fare clic su **Modifica**.

Radio 1 (2.4 GHz) Radio 2 (5 GHz)

Virtual Access Points (SSIDs)


+  

<input type="checkbox"/>	No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Passaggio 4. Scegliere WPA Enterprise dall'elenco a discesa Sicurezza.

Security

None

WPA Enterprise 

None


WPA Personal

**WPA Enterprise**

[Passaggio 5.](#) Fare clic sul pulsante Visualizza per configurare i parametri WPA Enterprise.

Security

None

WPA Enterprise 

None

WPA Personal

WPA Enterprise

Passaggio 6. Scegliere la versione WPA nell'area Versioni WPA. Le opzioni sono:

- WPA-TKIP: questa opzione implementa la protezione mista sulla rete wireless. È ideale per reti con client wireless misti. Questa opzione è disattivata per impostazione predefinita.
- WPA2-AES: questa opzione implementa la protezione WPA2-AES sulla rete. È ideale per reti wireless con client che supportano la sicurezza WPA2.



## Security Setting

---



**Nota:** Nell'esempio, viene controllato WPA-TKIP.

Passaggio 7. (Facoltativo) Selezionare la casella di controllo **Abilita preautenticazione** per attivare la funzionalità. Se questa opzione è selezionata, le informazioni di preautenticazione vengono inoltrate dal WAP a cui il client wireless è attualmente connesso al 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. Quando la modalità di protezione è disattivata, anche questa opzione è disattivata e non può essere modificata.

## Security Setting

---



Passaggio 8. (Facoltativo) Deselezionare la casella di controllo Usa impostazioni globali server RADIUS per specificare un set diverso di server RADIUS. Per impostazione predefinita, ogni VAP utilizza le impostazioni globali RADIUS definite per il WAP.

## Security Setting

WPA Versions:

WPA-TKIP

WPA2-AES

Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:

IPv4  IPv6

Server IP Address-1: ?

192.168.1.1

Server IP Address-2: ?

Key-1: ?

.....

Key-2: ?

Enable RADIUS Accounting

Active Server:

Server IP Address-1 ▼

Broadcast Key Refresh Rate: ?

86400

Session Key Refresh Rate: ?

0

OK

cancel

**Nota:** In questo esempio, l'opzione Usa impostazioni globali del server RADIUS non è selezionata. Se questa opzione è selezionata, andare al [passo 17](#).

Passaggio 9. (Facoltativo) Scegliere un tipo di indirizzo IP del server. Le opzioni sono:

- IPv4 — Questa opzione consente al WAP di contattare il server RADIUS IPv4.
- IPv6 - Questa opzione consente al punto di accesso del punto di accesso del server RADIUS IPv6 di contattare il server RADIUS.

## Security Setting

WPA Versions:  WPA-TKIP  WPA2-AES

Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  Pv4  IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

OK

cancel

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

Passaggio 10. (Facoltativo) Immettere l'indirizzo IP primario del server RADIUS per il VAP nel campo *Indirizzo IP server -1*.

Server IP Address Type:

IPv4  IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

**Nota:** Nell'esempio, viene immesso 192.168.1.1.

Passaggio 11. (Facoltativo) Immettere l'indirizzo IP del server RADIUS di backup per il VAP nel campo *Indirizzo IP server -2*.

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

**Nota:** Nell'esempio, non viene immesso alcun indirizzo IP di backup.

Passaggio 12. (Facoltativo) Immettere una password per l'indirizzo del server principale nel campo *Key-1*.

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Passaggio 13. (Facoltativo) Immettere una password per l'indirizzo del server di backup nel campo *Chiave-2*.

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

**Nota:** Nell'esempio non viene immessa alcuna password.

Passaggio 14. (Facoltativo) Selezionare la casella di controllo **Abilita accounting RADIUS**. Questa opzione consente di tenere traccia e misurare le risorse utilizzate da un utente specifico, ad esempio il tempo di sistema e la quantità di dati trasmessi e ricevuti. Se attivata, verrà attivata per i server primario e di backup.

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

**Nota:** Nell'esempio, l'opzione Abilita accounting RADIUS è selezionata.

Passaggio 15. (Facoltativo) Scegliere un server attivo dall'elenco a discesa Server attivo.

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:

Server IP Address-2:

Key-1:

Key-2:

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

**Nota:** Nell'esempio, viene scelto Server IP Address-1.

Passaggio 16. (Facoltativo) Immettere il numero di secondi che devono trascorrere prima che la chiave di protezione venga sostituita da una chiave appena generata nel campo *Velocità di aggiornamento chiave di trasmissione*. Il valore predefinito è 86400.

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

---

**Nota:** In questo esempio, la velocità di aggiornamento della chiave di trasmissione viene mantenuta sul valore predefinito.

[Passaggio 17](#). Immettere l'intervallo in base al quale WAP aggiorna le chiavi di sessione per ogni client associato al VAP. Può essere di 30-86400 secondi.

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

---

Passaggio 18. Fare clic su **OK**.

Active Server:

Broadcast Key Refresh Rate:

Session Key Refresh Rate:

---

Passaggio 19. Fare clic su **Salva**.

The screenshot shows the Cisco Meraki Networks configuration interface for device WAP125-wap5e1078. The 'Virtual Access Points (SSIDs)' section is active, displaying a table with two SSIDs. The 'Save' button in the top right corner is highlighted with a red box.

No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input type="checkbox"/>	1	ciscosb	<input type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	1	CiscoTest	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None

È ora necessario configurare la protezione WPA Enterprise sulla rete wireless.

Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco](#)