

# Configurazione di un VAP su WAP351, WAP131 e WAP371

## Obiettivo

I punti di accesso virtuali (VAP) segmentano la LAN wireless in più domini di broadcast equivalenti wireless di VLAN Ethernet. I VAP simulano più punti di accesso in un unico dispositivo WAP fisico. Su Cisco WAP131 sono supportati fino a quattro VAP e su Cisco WAP351 e WAP371 ne sono supportati fino a otto.

Lo scopo di questo documento è mostrare come configurare un VAP sui punti di accesso WAP351, WAP131 e WAP371.

## Dispositivi interessati

- WAP351
- WAP131
- WAP371

## Versione del software

- V1.0.0.39 (WAP351)
- V1.0.0.39 (WAP131)
- V1.2.0.2 (WAP371)

## Aggiunta e configurazione di un VAP

**Nota:** Ogni VAP è identificato da un SSID (Service Set Identifier) configurato dall'utente. Più VAP non possono avere lo stesso nome SSID.

**Nota:** Affinché la rete wireless funzioni correttamente, la radio a cui è associato il punto di accesso virtuale configurato deve essere abilitata e configurata correttamente. Per ulteriori informazioni, vedere [Configurazione delle impostazioni radio di base su WAP131 e WAP351](#) o [Configurazione delle impostazioni radio di base su WAP371](#).

Passaggio 1. Accedere all'utility di configurazione Web e selezionare **Wireless > Reti**. Viene visualizzata la pagina *Reti*:

Networks

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

Save

Passaggio 2. Nel campo *Radio*, selezionare il pulsante di opzione per la radio wireless su cui si desidera configurare i VAP.

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

Passaggio 3. Per aggiungere un nuovo VAP, fare clic su **Add** (Aggiungi). Nella tabella verrà visualizzato un nuovo VAP.

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

**Nota:** WAP131 supporta fino a 4 VAP, mentre WAP371 e WAP351 supportano fino a 8 VAP.

Passaggio 4. Per iniziare a modificare un punto di accesso virtuale, fare clic sulla casella di controllo all'estrema sinistra della voce della tabella, quindi scegliere **Modifica**. In questo modo sarà possibile modificare i campi disattivati del punto di accesso virtuale selezionato.

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		

Add Edit Delete

Passaggio 5. Per abilitare l'utilizzo del VAP, verificare che la casella di controllo *Abilita* sia selezionata.

Select the radio interface first, and then enter the configuration parameters.

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

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

Add Edit Delete

Passaggio 6. Nel campo *VLAN ID*, specificare l'ID VLAN da associare al VAP. Se si utilizza il protocollo WAP131 o WAP371, immettere l'ID della VLAN. Il valore massimo che è possibile immettere è 4094.

Select the radio interface first, and then enter the configuration parameters.

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

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

Add Edit Delete

**Nota:** L'ID VLAN immesso deve essere presente nella rete e configurato correttamente. Per ulteriori informazioni, vedere [Configurazione della VLAN sull'access point WAP351](#), [Gestione di ID VLAN con e senza tag su WAP131](#) o [Gestione di ID VLAN con e senza tag su WAP371](#).

Passaggio 7. Immettere il nome della rete wireless nel campo Nome SSID. Ogni VAP deve avere un nome SSID univoco.

Select the radio interface first, and then enter the configuration parameters.

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

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

Add Edit Delete

Passaggio 8. Se si desidera che il nome SSID venga trasmesso ai client, selezionare la casella di controllo *Trasmissione SSID*. Il nome SSID verrà visualizzato ai client nell'elenco delle reti disponibili.

Select the radio interface first, and then enter the configuration parameters.

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

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

Add Edit Delete

## Configurazione delle impostazioni di protezione

Passaggio 1. Selezionare il metodo di autenticazione richiesto per la connessione al VAP dall'elenco a discesa *Sicurezza*. Se è selezionata un'opzione diversa da **Nessuno**, verranno visualizzati campi aggiuntivi.

Select the radio interface first, and then enter the configuration parameters.

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

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/> 0	<input checked="" type="checkbox"/>	1	DISCO5B	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>

Buttons: Add, Edit, Delete, Save

Le opzioni disponibili sono le seguenti:

- Nessuna
- WEP statico
- WEP dinamico
- Personale WPA
- WPA Enterprise

**Nota:** WPA Personal e WPA Enterprise sono i tipi di autenticazione preferiti per la massima protezione. WEP statico e WEP dinamico devono essere utilizzati solo con apparecchiature legacy e richiedono l'impostazione della radio sulla modalità 802.11a o 802.11b/g. Per ulteriori informazioni, vedere [Configurazione delle impostazioni radio di base su WAP131 e WAP351](#) o [Configurazione delle impostazioni radio di base su WAP371](#).

## WEP statico

Il metodo di autenticazione WEP statico è il meno sicuro. I dati della rete wireless vengono crittografati in base a una chiave statica. È diventato semplice ottenere questa chiave statica in modo illegale, quindi l'autenticazione WEP deve essere utilizzata solo quando necessario con dispositivi legacy.

**Nota:** Quando si seleziona *Static WEP* come metodo di protezione, viene visualizzato un messaggio che indica che il metodo di protezione scelto non è sicuro.

Passaggio 1. Nell'elenco a discesa *Indice chiave di trasferimento*, selezionare l'indice della chiave WEP dall'elenco di chiavi sottostante che il dispositivo utilizzerà per crittografare i dati.

Transfer Key Index: 1

Key Length: 2, 3 bits, 4 bits

Key Type:  ASCII,  Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

Passaggio 2. Scegliere un pulsante di opzione nel campo *Lunghezza chiave* per specificare se la chiave è lunga 64 o 128 bit.

Transfer Key Index: 1

Key Length:  64 bits,  128 bits

Key Type:  ASCII,  Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

Passaggio 3. Nel campo *Tipo di chiave*, scegliere se immettere le chiavi in formato ASCII o esadecimale. Il codice ASCII include tutte le lettere, i numeri e i simboli presenti sulla tastiera, mentre il codice esadecimale deve utilizzare solo numeri o lettere da A a F.

Transfer Key Index: 1 ▾

Key Length:  64 bits  
 128 bits

Key Type:  ASCII  
 Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

Passaggio 4. Nel campo *Chiavi WEP*, immettere fino a 4 chiavi WEP diverse per il dispositivo. Ogni client da connettere a questa rete deve disporre di una delle stesse chiavi WEP nello stesso slot specificato dal dispositivo.

Transfer Key Index: 1 ▾

Key Length:  64 bits  
 128 bits

Key Type:  ASCII  
 Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

Passaggio 5. (Facoltativo) Fare clic sulla casella di controllo nel campo *Mostra chiave come testo non crittografato* se si visualizzano le stringhe di caratteri dei tasti.



essere associata al dispositivo WAP.

·Sistema aperto e chiave condivisa: se sono stati selezionati entrambi gli algoritmi di autenticazione, le stazioni client configurate per l'utilizzo di WEP in modalità chiave condivisa devono disporre di una chiave WEP valida da associare al dispositivo WAP. Inoltre, le stazioni client configurate per utilizzare WEP come sistema aperto (modalità chiave condivisa non abilitata) possono associarsi al dispositivo WAP anche se non dispongono della chiave WEP corretta.

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

## WEP dinamico

Dynamic WEP fa riferimento alla combinazione della tecnologia 802.1x e del protocollo EAP (Extensible Authentication Protocol). Per autenticare gli utenti, questa modalità richiede l'utilizzo di un server RADIUS esterno. Il dispositivo WAP richiede un server RADIUS che supporti EAP, ad esempio Microsoft Internet Authentication Server. Per utilizzare i client Microsoft Windows, il server di autenticazione deve supportare PEAP (Protected EAP) e MSCHAP v2. È possibile utilizzare uno qualsiasi dei diversi metodi di autenticazione supportati dalla modalità IEEE 802.1X, inclusi i certificati, Kerberos e l'autenticazione a chiave pubblica, ma è necessario configurare le stazioni client in modo che utilizzino lo stesso metodo di autenticazione utilizzato dal dispositivo WAP.

Passaggio 1. Per impostazione predefinita è selezionata l'opzione *Utilizza impostazioni globali del server RADIUS*. Deselezionare la casella di controllo se si desidera configurare il VAP per l'utilizzo di un set diverso di server RADIUS. In caso contrario, andare al passaggio 8.

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 2. Nel campo *Tipo di indirizzo IP server*, selezionare il tipo di indirizzo IP del server utilizzato dal dispositivo WAP. Le opzioni sono *IPv4* o *IPv6*. IPv4 utilizza numeri binari



a 32 bit rappresentati sotto forma di numeri decimali separati da punti. IPv6 utilizza numeri esadecimali e due punti per rappresentare un numero binario a 128 bit. Il dispositivo WAP contatta solo il server o i server RADIUS per il tipo di indirizzo selezionato in questo campo. Se si sceglie IPv6, andare al passaggio 4.

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 3. Se si è selezionato **IPv4** nel passaggio 2, immettere l'indirizzo IP del server RADIUS utilizzato da tutti i VAP per impostazione predefinita. Quindi andare al Passaggio 5.

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)

**Nota:** È possibile avere fino a tre indirizzi server RADIUS di backup IPv4. Se l'autenticazione non riesce con il server primario, ciascun server di backup configurato viene tentato in

sequenza.

Passaggio 4. Se è stato selezionato **IPv6** nel passaggio 2, immettere l'indirizzo IPv6 del server RADIUS globale primario.

The screenshot shows a configuration window for RADIUS server settings. At the top, there is a checkbox labeled "Use global RADIUS server settings" which is unchecked. Below this, the "Server IP Address Type" is set to "IPv6" (selected with a radio button). Four "Server IPv6 Address" fields are visible, each with a corresponding IPv6 address placeholder in parentheses. The first four fields are highlighted with a red rectangle. The addresses are: "2001:DB8:1234:abcd::", "2002:DB8:1234:abcd::", "2003:DB8:1234:abcd::", and "2004:DB8:1234:abcd::". Below these are four "Key" fields (Key-1 to Key-4), each with a range of 1-64 characters. Key-1 is filled with dots. There is also an "Enable RADIUS Accounting" checkbox which is unchecked. At the bottom, there are fields for "Active Server" (set to "Server IP Address-1"), "Broadcast Key Refresh Rate" (set to 300), and "Session Key Refresh Rate" (set to 0).

**Nota:** È possibile disporre di un massimo di tre indirizzi server RADIUS di backup IPv6. Se l'autenticazione non riesce con il server primario, ciascun server di backup configurato viene tentato in sequenza.

Passaggio 5. Nel campo *Chiave-1*, immettere la chiave segreta condivisa utilizzata dal dispositivo WAP per l'autenticazione al server RADIUS primario.

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (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: Server IP Address-1

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

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

Passaggio 6. Nei campi da *Chiave-2* a *Chiave-4* immettere la chiave RADIUS associata ai server RADIUS di backup configurati. L'indirizzo IP del server 2 utilizza Key-2, l'indirizzo IP del server 3 utilizza Key-3 e l'indirizzo IP del server 4 utilizza Key-4.

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (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: Server IP Address-1

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

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

Passaggio 7. (Facoltativo) Nel campo *Abilita accounting RADIUS* selezionare la casella di controllo se si desidera abilitare la registrazione e la misurazione delle risorse consumate da un utente specifico. L'attivazione dell'accounting RADIUS consente di tenere traccia dell'ora del sistema e della quantità di dati trasmessi e ricevuti. Le informazioni verranno memorizzate nel server Radius. Verrà attivata per il server RADIUS primario e tutti i server di backup.

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)

**Nota:** Se è stato attivato l'accounting RADIUS, verrà attivato per il server RADIUS primario e per tutti i server di backup

Passaggio 8. Scegliere il primo server attivo nel campo *Server attivo*. In questo modo è possibile selezionare manualmente il server RADIUS attivo anziché fare in modo che il dispositivo WAP tenti di contattare in sequenza ogni server configurato e scelga il primo server attivo.

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 9. Nel campo *Velocità di aggiornamento chiave trasmissione*, immettere l'intervallo di aggiornamento della chiave di trasmissione (gruppo) per i client associati a questo VAP. L'impostazione predefinita è 300 secondi.

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (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: Server IP Address-1

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

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

Passaggio 10. Nel campo *Session Key Refresh Rate* (Frequenza di aggiornamento chiavi sessione), immettere l'intervallo in base al quale il dispositivo WAP aggiorna la chiave di sessione (unicast) per ogni client associato al VAP. Il valore predefinito è 0.

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (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: Server IP Address-1

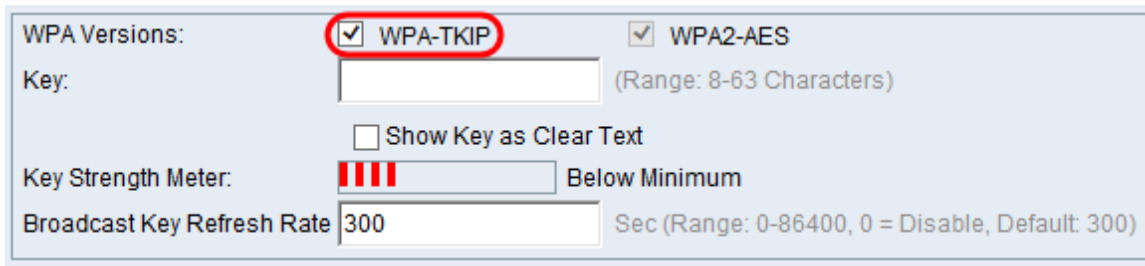
Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

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

## Personale WPA

WPA Personal è uno standard Wi-Fi Alliance IEEE 802.11i, che include la crittografia AES-CCMP e TKIP. WPA utilizza una chiave precondivisa (PSK) anziché IEEE 802.1X e EAP come nella modalità di protezione WPA aziendale. La chiave PSK viene utilizzata solo per un controllo iniziale delle credenziali. WPA è anche noto come WPA-PSK. Questa modalità di protezione è compatibile con le versioni precedenti per i client wireless che supportano WPA originale.

Passaggio 1. Nel campo *Versioni WPA*, selezionare la casella di controllo *WPA-TKIP* per abilitare WPA-TKIP. È possibile abilitare contemporaneamente WPA-TKIP e WPA2-AES. WAP supporta sempre WPA2-AES, pertanto non sarà possibile configurarlo.



The screenshot shows a configuration window for WPA security. At the top, under 'WPA Versions:', there are two checkboxes: 'WPA-TKIP' (checked and circled in red) and 'WPA2-AES' (checked). Below this is a 'Key:' field (empty) with '(Range: 8-63 Characters)' to its right. A 'Show Key as Clear Text' checkbox is unchecked. A 'Key Strength Meter' shows four red bars and the text 'Below Minimum'. At the bottom, 'Broadcast Key Refresh Rate' is set to '300' with '(Sec (Range: 0-86400, 0 = Disable, Default: 300))' to its right.

Le opzioni disponibili sono definite come segue:

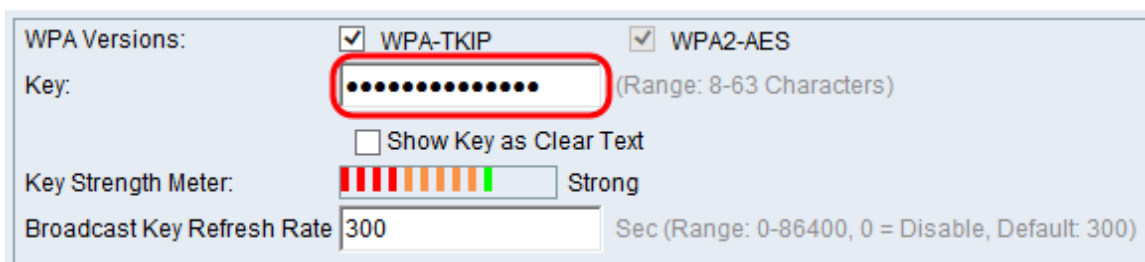
·WPA-TKIP: la rete dispone di alcune stazioni client che supportano solo il protocollo di sicurezza WPA e TKIP originale. In base ai più recenti requisiti di WiFi Alliance, non è consigliabile scegliere solo WPA-TKIP.

·WPA2-AES: 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 WiFi Alliance, l'access point deve supportare questa modalità in ogni momento.

·WPA-TKIP e WPA2-AES: se la rete dispone di una combinazione di client, alcuni dei quali supportano WPA2 e altri che supportano solo WPA originale, selezionare entrambe le caselle di controllo. Questa impostazione consente l'associazione e l'autenticazione delle stazioni client WPA e WPA2, ma utilizza la versione più affidabile di WPA2 per i client che la supportano. Questa configurazione WPA consente una maggiore interoperabilità al posto di una certa sicurezza.

**Nota:** I client WPA devono disporre di una di queste chiavi (una chiave TKIP valida o una chiave AES-CCMP valida) per poter essere associati al dispositivo WAP.

Passaggio 2. Nel campo *Chiave* immettere la chiave segreta condivisa per la protezione personale WPA. Immettere almeno 8 e un massimo di 63 caratteri.



The screenshot shows the same configuration window as above. The 'Key:' field now contains ten black dots, representing a hidden password. The 'Key Strength Meter' now shows five bars (four red, one green) and the text 'Strong'. The 'WPA-TKIP' checkbox remains circled in red.

**Nota:** I caratteri accettabili includono lettere maiuscole e minuscole, cifre numeriche e simboli speciali (?!\@#\$\$%^&\*).

Passaggio 3. (Facoltativo) Selezionare la casella di controllo *Mostra chiave come testo non crittografato* per rendere visibile il testo digitato. Per impostazione predefinita, la casella di controllo è deselezionata.

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Strong

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

**Nota:** quando si utilizza un firmware diverso su WAP351, WAP131 o WAP371, potrebbe mancare il campo *Mostra chiave come testo non crittografato*.

**Nota:** Il campo *Misuratore di forza chiave* indica dove il dispositivo WAP controlla la chiave in base a criteri di complessità quali il numero di tipi di caratteri diversi utilizzati e la lunghezza della chiave. Se la funzione di controllo della complessità WPA-PSK è attivata, la chiave viene accettata solo se soddisfa i criteri minimi. Per ulteriori informazioni sulla complessità di WPA-PSK, [consultare il documento sulla configurazione della complessità della password per WAP131, WAP351 e WAP371](#).

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Strong

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

Passaggio 4. Nel campo *Velocità di aggiornamento chiave trasmissione*, immettere l'intervallo di aggiornamento della chiave di trasmissione (gruppo) per i client associati a questo VAP. L'impostazione predefinita è 300 secondi.

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Strong

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

## WPA - Enterprise

WPA Enterprise con RADIUS è un'implementazione dello standard Wi-Fi Alliance IEEE 802.11i, che include CCMP (AES) e crittografia TKIP. La modalità Enterprise richiede l'utilizzo di un server RADIUS per autenticare gli utenti. La modalità di protezione è compatibile con i client wireless che supportano WPA originale.

**Nota:** La modalità VLAN dinamica è abilitata per impostazione predefinita e consente al server di autenticazione RADIUS di decidere quale VLAN utilizzare per le stazioni.

Passaggio 1. Nel campo *WPA Versions* (Versioni WPA), selezionare la casella di controllo relativa ai tipi di stazioni client da supportare. Per impostazione predefinita, sono tutti abilitati. L'access point deve supportare sempre WPA2-AES, quindi non sarà possibile configurarlo.

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)

Le opzioni disponibili sono definite come segue:

·WPA-TKIP: la rete dispone di alcune stazioni client che supportano solo il protocollo di sicurezza WPA e TKIP originale. Si noti che la selezione solo di WPA-TKIP per l'access point non è consentita in base al più recente requisito di WiFi Alliance.

·WPA2-AES: tutte le stazioni client della rete supportano la versione WPA2 e la cifratura/protocollo di sicurezza AES-CCMP. Questa versione WPA offre la migliore protezione dello standard IEEE 802.11i. In base all'ultimo requisito di Wi-Fi Alliance, il WAP deve supportare sempre questa modalità.

·Abilita preautenticazione: se si sceglie solo WPA2 o sia WPA che WPA2 come versione WPA, è possibile abilitare la preautenticazione per i client WPA2. 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 WAP. Questa opzione non è applicabile se è stata selezionata l'opzione WPA per le versioni WPA, in quanto la funzionalità WPA originale non è supportata.

**Nota:** Le stazioni client configurate per l'utilizzo di WPA con RADIUS devono avere uno degli indirizzi e delle chiavi seguenti: Un TKIP RADIUS valido o un indirizzo IP valido CCMP (AES) e una chiave RADIUS.

Passaggio 2. Per impostazione predefinita è selezionata l'opzione *Utilizza impostazioni globali del server RADIUS*. Deselezionare la casella di controllo se si desidera configurare il WAP per l'utilizzo di un set diverso di server RADIUS. In caso contrario, andare al passaggio 9.



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 3. Nel campo *Tipo di indirizzo IP server*, selezionare il tipo di indirizzo IP del server utilizzato dal dispositivo WAP. Le opzioni sono *IPv4* o *IPv6*. IPv4 utilizza numeri binari a 32 bit rappresentati sotto forma di numeri decimali separati da punti. IPv6 utilizza numeri esadecimali e due punti per rappresentare un numero binario a 128 bit. Il dispositivo WAP contatta solo il server o i server RADIUS per il tipo di indirizzo selezionato in questo campo.

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 4. Se nel passaggio 2 è stato selezionato **IPv4**, immettere l'indirizzo IP del server RADIUS utilizzato per impostazione predefinita da tutti i VAP. Quindi andare al passo 6.

The screenshot shows a configuration window for RADIUS server settings. At the top, there are checkboxes for WPA Versions:  WPA-TKIP,  WPA2-AES, and  Enable pre-authentication. Below this is a section with a checkbox  Use global RADIUS server settings. The main configuration area is titled 'Server IP Address Type:' with radio buttons for  IPv4 and  IPv6. There are four rows for 'Server IP Address-1' through 'Server IP Address-4', each with a text input field and a placeholder '(xxx.xxx.xxx.xxx)'. The first four IP addresses (192.168.10.23, 192.168.10.24, 192.168.10.25, and 192.168.10.26) are enclosed in a red rectangular box. Below these are four rows for 'Key-1' through 'Key-4', each with a text input field and a placeholder '(Range: 1-64 Characters)'. At the bottom, there is a checkbox  Enable RADIUS Accounting, an 'Active Server:' dropdown menu currently set to 'Server IP Address-1', and two more text input fields: 'Broadcast Key Refresh Rate:' with value '300' and 'Session Key Refresh Rate:' with value '0', both with placeholders 'Sec (Range: 0-86400, 0 = Disable, Default: 300)' and 'Sec (Range: 30-86400, 0 = Disable, Default: 0)' respectively.

**Nota:** È possibile avere fino a tre indirizzi server RADIUS di backup IPv4. Se l'autenticazione non riesce con il server primario, ciascun server di backup configurato viene tentato in sequenza.

Passaggio 5. Se è stato selezionato **IPv6** nel passaggio 2, immettere l'indirizzo IPv6 del server RADIUS globale primario.

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

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IPv6 Address-1:  (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX)

Server IPv6 Address-2:  (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX)

Server IPv6 Address-3:  (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX)

Server IPv6 Address-4:  (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX)

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)

**Nota:** È possibile disporre di un massimo di tre indirizzi server RADIUS di backup IPv6. Se l'autenticazione non riesce con il server primario, ciascun server di backup configurato viene tentato in sequenza.

Passaggio 6. Nel campo *Chiave-1* immettere la chiave segreta condivisa utilizzata dal dispositivo WAP per l'autenticazione al server RADIUS primario.

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. Nei campi da *Chiave-2* a *Chiave-4* immettere la chiave RADIUS associata ai server RADIUS di backup configurati. L'indirizzo IP del server 2 utilizza *Chiave-2*, l'indirizzo IP del server 3 utilizza *Chiave-3* e l'indirizzo IP del server 4 utilizza *Chiave-4*.

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. (Facoltativo) Nel campo *Abilita accounting RADIUS* selezionare la casella di controllo se si desidera abilitare la registrazione e la misurazione delle risorse consumate da

un utente specifico. L'attivazione dell'accounting RADIUS consente di tenere traccia dell'ora di sistema di un utente specifico e della quantità di dati trasmessi e ricevuti.

WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES	
<input checked="" type="checkbox"/> Enable pre-authentication	
<input type="checkbox"/> Use global RADIUS server settings	
Server IP Address Type:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Server IP Address-1:	<input type="text" value="192.168.10.23"/> (xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text" value="192.168.10.24"/> (xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text" value="192.168.10.25"/> (xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text" value="192.168.10.26"/> (xxx.xxx.xxx.xxx)
Key-1:	<input type="text" value="••••••••"/> (Range: 1-64 Characters)
Key-2:	<input type="text" value="••••••••"/> (Range: 1-64 Characters)
Key-3:	<input type="text" value="••••••~"/> (Range: 1-64 Characters)
Key-4:	<input type="text" value="••••••~"/> (Range: 1-64 Characters)
<input checked="" type="checkbox"/> Enable RADIUS Accounting	
Active Server:	<input type="text" value="Server IP Address-1"/> ▼
Broadcast Key Refresh Rate:	<input type="text" value="300"/> Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate:	<input type="text" value="0"/> Sec (Range: 30-86400, 0 = Disable, Default: 0)

**Nota:** Se è stato abilitato l'accounting RADIUS, questo verrà abilitato per il server RADIUS primario e per tutti i server di backup.

Passaggio 9. Scegliere il primo server attivo nel campo *Server attivo*. In questo modo è possibile selezionare manualmente il server RADIUS attivo anziché fare in modo che il dispositivo WAP tenti di contattare in sequenza ogni server configurato.

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: Server IP Address-1  
Server IP Address-2  
Server IP Address-3  
Server IP Address-4

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. Nel campo *Velocità di aggiornamento chiave trasmissione*, immettere l'intervallo di aggiornamento della chiave di trasmissione (gruppo) per i client associati al VAP. L'impostazione predefinita è 300 secondi.

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

Passaggio 11. Nel campo *Session Key Refresh Rate* (Frequenza di aggiornamento chiavi sessione), immettere l'intervallo in base al quale il dispositivo WAP aggiorna le chiavi di

sessione (unicast) per ogni client associato al VAP. Il valore predefinito è 0.

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication  
 Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)  
Server IP Address-2: 192.168.10.24 (xxx.xxx.xxx.xxx)  
Server IP Address-3: 192.168.10.25 (xxx.xxx.xxx.xxx)  
Server IP Address-4: 192.168.10.26 (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: Server IP Address-1

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

## Filtro MAC

Filtro MAC specifica se le stazioni che possono accedere a questo VAP sono limitate a un elenco globale configurato di indirizzi MAC.

Passaggio 1. Nell'elenco a discesa *MAC Filter*, scegliere il tipo di filtro MAC desiderato.

Select the radio interface first, and then enter the configuration parameters.

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

VAP No.	Enable	VLAN ID <a href="#">Add New VLAN</a>	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
0	<input checked="" type="checkbox"/>	1	DISCOFD	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled Local RADIUS	<input type="checkbox"/>

Add Edit Delete

Le opzioni disponibili sono definite come segue:

- Disabilitato — Non usa il filtro MAC.
- Locale: utilizza l'elenco di autenticazione MAC configurato nella sezione Filtro MAC. Per ulteriori informazioni sul filtro MAC, consultare il documento sulla [configurazione del filtro MAC su WAP351 e WAP131](#).
- RADIUS: utilizza l'elenco di autenticazione MAC su un server RADIUS esterno.

## Isolamento canali

Quando Isolamento canale è disattivato, i client wireless possono comunicare tra loro normalmente inviando traffico attraverso il dispositivo WAP. Quando è abilitato, il dispositivo

WAP blocca la comunicazione tra i client wireless sullo stesso VAP. Il dispositivo WAP consente ancora il traffico di dati tra i client wireless e i dispositivi cablati della rete, attraverso un collegamento WDS e con altri client wireless associati a un VAP diverso, ma non tra i client wireless.

Passaggio 1. Nel campo *Isolamento canale*, selezionare la casella di controllo se si desidera abilitare l'isolamento del canale.

Select the radio interface first, and then enter the configuration parameters.

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

VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discoSB	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>

Add Edit Delete

Passaggio 2. Fare clic su **Salva**.

**Nota:** Dopo il salvataggio delle nuove impostazioni, è possibile arrestare e riavviare i processi corrispondenti. Quando si verifica questa condizione, il dispositivo WAP potrebbe perdere la connettività. È consigliabile modificare le impostazioni del dispositivo WAP quando la perdita di connettività influisce meno sui client wireless.

## Banda sterzante

Band Steer è disponibile solo su WAP371. Band Steer utilizza in modo efficace la banda a 5 GHz guidando i client supportati dalla doppia banda dalla banda a 2,4 GHz alla banda a 5 GHz. In questo modo la banda a 2,4 GHz viene liberata per l'utilizzo con dispositivi legacy che non dispongono di supporto per doppia radio.

**Nota:** Le radio a 5 GHz e a 2,4 GHz devono essere abilitate all'uso di Band Steer. Per ulteriori informazioni sull'attivazione delle radio, consultare il documento sulla [configurazione delle impostazioni radio di base su WAP371](#).

Passaggio 1. La funzione Band Steer è configurata per VAP e deve essere abilitata su entrambe le radio. Se si desidera attivare il mandrino della banda, selezionare la casella di controllo nel campo Mandrino della banda.

Select the radio interface first, and then enter the configuration parameters.

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

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discoSB	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add Edit Delete

**Nota:** La funzione Band Steer non è consigliata sui VAP con traffico voce o video sensibile al tempo. Anche se la radio a 5 GHz utilizza meno larghezza di banda, cerca di indirizzare i client verso quella radio.

Passaggio 2. Fare clic su **Salva**.

## Eliminazione di un VAP

Passaggio 1. Selezionare la casella di controllo del VAP che si desidera eliminare.



Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
<a href="#">Show Details</a>									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
<a href="#">Show Details</a>									

Passaggio 2. Fare clic su **Elimina** per eliminare il VAP.

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
<a href="#">Show Details</a>									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
<a href="#">Show Details</a>									

Passaggio 3. Fare clic su **Salva** per salvare l'eliminazione in modo permanente.

Select the radio interface first, and then enter the configuration parameters.

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

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		