# Configurazione dei VAP (Virtual Access Point) sui WAP121 e WAP321

## Obiettivo

I VAP (Virtual Access Point) simulano più percorsi di accesso in un unico dispositivo WAP fisico. I VAP sono simili alle VLAN (Virtual Local Area Network) Ethernet. Ogni VAP può essere abilitato o disabilitato in modo indipendente ed è identificato da un SSID (Service Set Identifier) configurato dall'utente o noto anche come nomi di rete. È possibile configurare fino a quattro VAP su Cisco WAP121 e fino a otto VAP su Cisco WAP321.

L'obiettivo di questo documento è mostrare come configurare i Virtual Access Point sui Cisco WAP121 e WAP321 Access Point.

## Dispositivi interessati

- WAP121
- WAP321

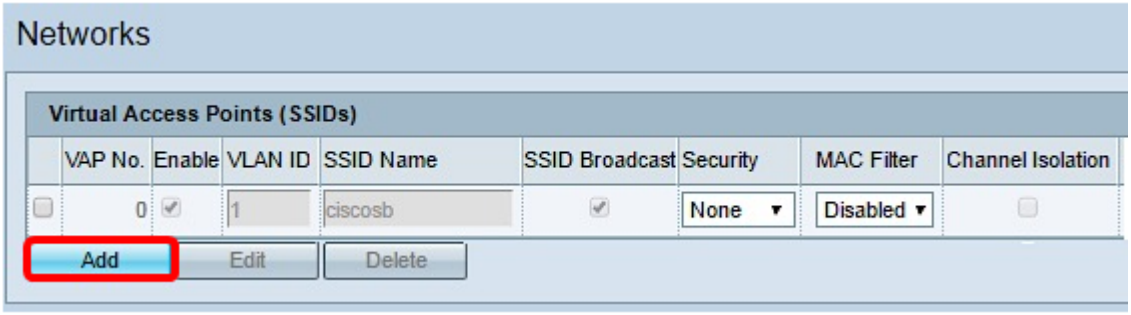
## Versione del software

- 1.0.6.5

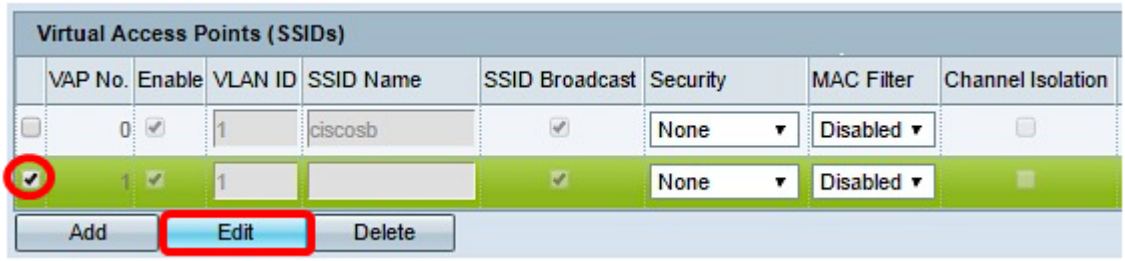
Passaggio 1. Accedere all'utility basata sul Web Access Point e scegliere **Wireless > Reti**.


Passaggio 2. Nella tabella dei punti di accesso virtuali (SSID), fare clic sul pulsante **Aggiungi** .

**Nota:** VAP No. 0 è l'interfaccia radio fisica predefinita e può essere modificata a seconda delle preferenze. Questo VAP non può essere eliminato e rimane abilitato finché la radio è abilitata.

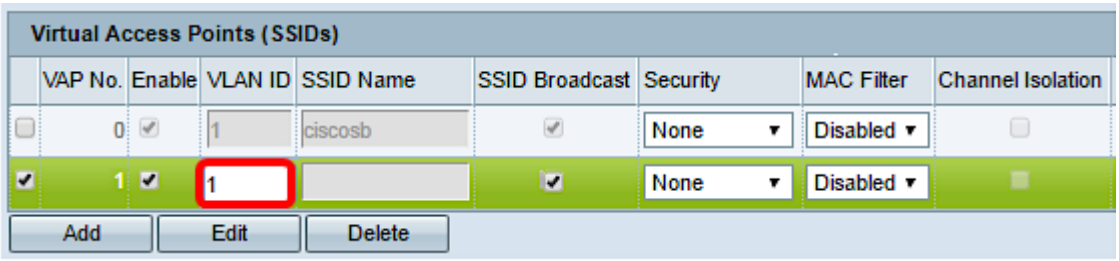



Passaggio 3. Selezionare la casella di controllo accanto al numero VAP, quindi fare clic su **Modifica**.



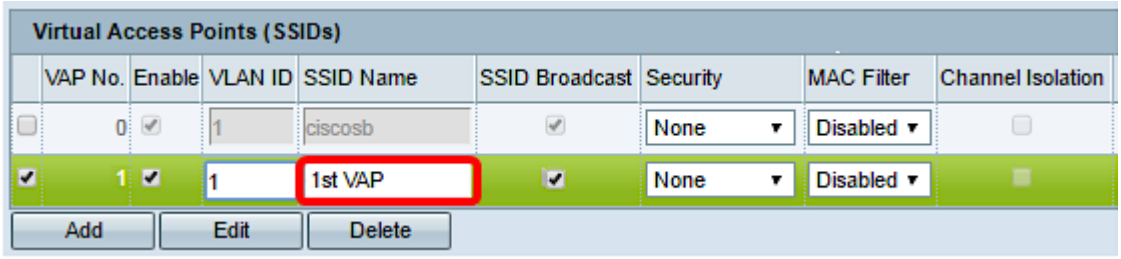

Passaggio 4. Nel campo *VLAN ID*, immettere l'ID VLAN a cui associare il VAP in fase di creazione. Un ID VLAN può essere un valore compreso tra 1 e 4094.

**Nota:** verificare che l'ID VLAN sia configurato correttamente sulla rete. Se il VAP comunica con i client wireless su una VLAN configurata in modo errato, possono verificarsi errori di rete. La scheda WAP121 supporta cinque VLAN attive (quattro WLAN più una VLAN di gestione), mentre la scheda WAP321 supporta nove VLAN attive (otto WLAN più una VLAN di gestione).




**Nota:** nell'esempio, viene usato l'ID VLAN 1. Si tratta dell'impostazione predefinita.

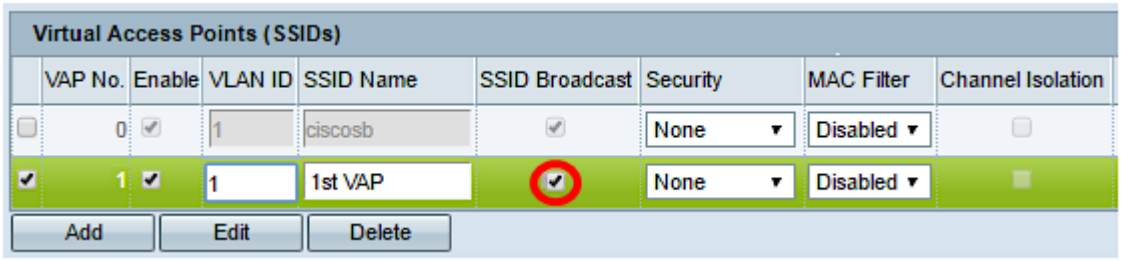
Passaggio 5. Nel campo *SSID Name* (Nome SSID), creare un nome per il VAP. Lo SSID può contenere qualsiasi voce alfanumerica con distinzione tra maiuscole e minuscole compresa tra 2 e 32 caratteri.




Passaggio 6. Selezionare la casella di controllo Trasmissione SSID. In questo modo il VAP sarà visibile a tutti i dispositivi wireless nel suo campo di copertura.

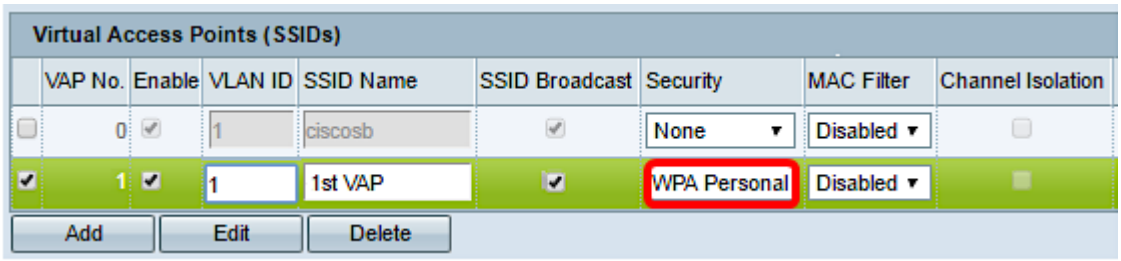
**Nota:** La trasmissione SSID è abilitata per impostazione predefinita. La disattivazione della

trasmissione SSID impedisce ai client wireless di connettersi alla rete poiché il VAP non sarà visibile. Offre tuttavia un livello di protezione minimo e non impedisce le minacce alla sicurezza per la connessione o il monitoraggio del traffico non crittografato. Le trasmissioni SSID possono essere abilitate o disabilitate in modo indipendente su ciascun VAP.



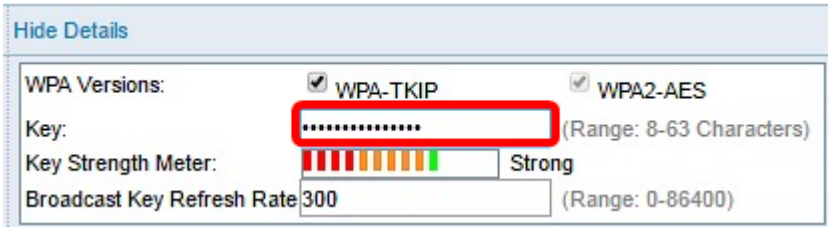

Passaggio 7. Selezionare un'opzione dall'elenco a discesa Sicurezza a seconda del tipo di sicurezza che si desidera utilizzare nel VAP. Le opzioni sono:

- Nessuno — Aprire o non proteggere. Questa è l'opzione predefinita. Se si sceglie questa opzione, andare al passaggio 10.
- WPA Personal: protezione più avanzata rispetto a WEP e in grado di supportare chiavi di lunghezza compresa tra 8 e 63 caratteri.
- WPA Enterprise: il metodo di protezione più avanzato. Utilizza il protocollo PEAP (Protected Extensible Authentication Protocol), in cui ogni utente wireless in WAP è autorizzato con nomi utente e password individuali. Queste password possono supportare AES (Advanced Encryption Standard). Utilizza anche Transport Layer Security (TLS) oltre a PEAP, in cui ogni utente deve fornire un certificato aggiuntivo per ottenere l'accesso.



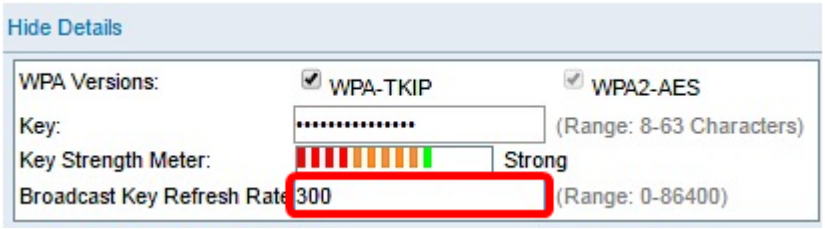

**Nota:** In questo esempio viene scelto WPA Personal.

Passaggio 8. Nel campo *Key*, creare una password per il VAP. Questa sarà la password che ogni client wireless dovrà immettere per connettersi alla rete wireless.




**Nota:** L'indicatore di livello chiave indica la complessità della password creata.

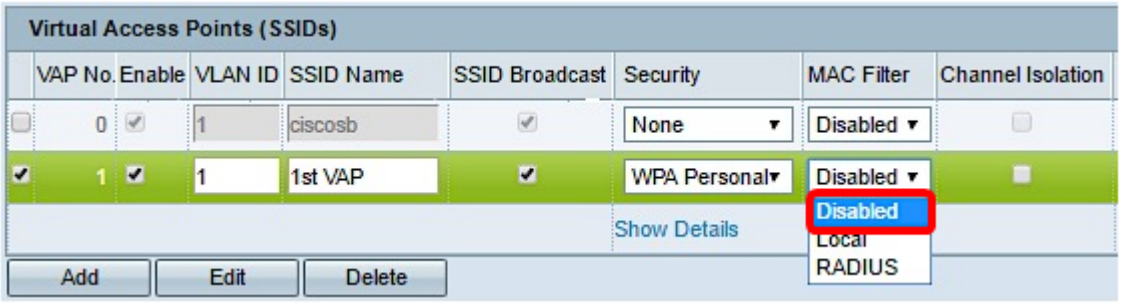
Passaggio 9. Inserire un valore in Velocità di aggiornamento chiave trasmissione. Intervallo di aggiornamento della chiave di trasmissione (gruppo) per i client associati al VAP. L'intervallo valido è compreso tra 0 e 86400 secondi.




**Nota:** Nell'esempio viene utilizzato il valore predefinito 300.

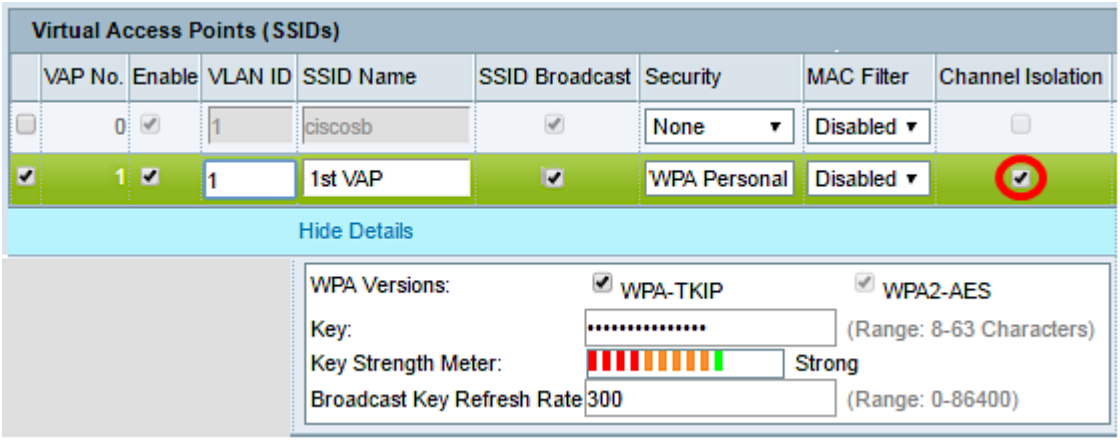
Passaggio 10. Scegliere un'opzione dall'elenco a discesa Filtro MAC per specificare se i client che possono accedere al VAP sono limitati a un elenco globale configurato di indirizzi MAC. Le opzioni sono:

- Disabilitato: tutti i client possono accedere alla rete a monte.
- Impostazioni locali — l'insieme di client che possono accedere alla rete a monte è limitato ai client specificati in un elenco indirizzi MAC definito localmente.
- Radius: l'insieme di client che possono accedere alla rete a monte è limitato ai client specificati in un elenco indirizzi MAC su un server RADIUS.




**Nota:** In questo esempio, viene scelta l'impostazione predefinita Disabilitato.

Passaggio 11. (Facoltativo) Selezionare la casella di controllo **Isolamento canali** se si desidera che il dispositivo WAP blocchi 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 12. Ripetere i passaggi da 2 a 11 per ogni access point che si desidera aggiungere. È possibile configurare fino a quattro VAP su Cisco WAP121 e fino a otto VAP su Cisco WAP321.

Passaggio 13. Fare clic sul  pulsante.

A questo punto è necessario configurare correttamente i punti di accesso virtuali ai punti di accesso WAP121 e WAP321.