Configurazione delle porte con RLAN in una rete CBW

Obiettivo

L'obiettivo di questo articolo è creare una rete RLAN (Remote Local Area Network) e assegnare porte e gruppi di punti di accesso a un punto di accesso primario (AP) Cisco Business Wireless (CBW).

Dispositivi interessati | Versione software

- 145AC (Scheda tecnica) | 10.4.1.0 (scarica la versione più recente)
- 240AC (Scheda tecnica) | 10.4.1.0 (scarica la versione più recente)

Introduzione

Gli access point CBW sono basati su 802.11 a/b/g/n/ac (Wave 2), con antenne interne. Questi access point supportano il più recente standard 802.11ac Wave 2 per prestazioni più elevate, maggiore accesso e reti a densità più elevata.

I access point serie 145AC e 240AC a cui si fa riferimento in questo articolo possono essere utilizzati in reti tradizionali o mesh. Questo articolo utilizza l'apparecchiatura per una rete wireless tradizionale.

Per informazioni sulle nozioni di base sulle reti mesh, consulta Cisco Business: Benvenuti nella sezione Wireless Mesh Networking.

Se si preferisce eseguire la configurazione delle porte in una rete mesh, consultare Configurazione delle porte Ethernet di Cisco Business Wireless Access Point in modalità Mesh.

In una rete wireless tradizionale, una RLAN viene utilizzata per autenticare i client cablati tramite l'access point primario. Una volta che il client cablato si è unito correttamente all'access point principale, le porte LAN spostano il traffico tra le modalità di switching centrale e locale. Il traffico proveniente dal client cablato viene considerato traffico client wireless.

L'RLAN invia la richiesta di autenticazione per autenticare il client cablato. L'autenticazione del client cablato in una RLAN è simile a quella del client wireless centralizzato autenticato.

Se è necessaria una sola VLAN (Virtual Local Area Network), non è necessario configurare una RLAN. Per impostazione predefinita, una RLAN viene fornita sull'access point, la VLAN nativa 1. Ha la sicurezza aperta e tutte le porte sono assegnate a questa RLAN per impostazione predefinita.

Se non conosci i termini usati, controlla Cisco Business: glossario dei nuovi termini.

Le RLAN non funzionano in una rete mesh. Mesh non è abilitato per impostazione predefinita, quindi se l'access point non era in esecuzione in modalità mesh, si è impostati per andare.

Procedura di configurazione

In questa sezione attivata/disattivata vengono evidenziati i suggerimenti per i principianti.

Accesso

Accedere all'interfaccia utente Web dell'access point primario. A tale scopo, aprire un browser Web e immettere https://ciscobusiness.cisco. È possibile che venga visualizzato un avviso prima di procedere. Immettere le credenziali.È inoltre possibile accedere all'access point primario immettendo https://[ipaddress] (dell'access point primario) in un browser Web.

Descrizione comandi

In caso di domande su un campo nell'interfaccia utente, cercare una descrizione comando simile alla seguente: 

Impossibile individuare l'icona Espandi menu principale.

Passare al menu sul lato sinistro dello schermo. Se il pulsante del menu non è visibile, fare clic su questa icona per aprire il menu della barra laterale. 

Cisco Business App

Questi dispositivi dispongono di app complementari che condividono alcune funzionalità di gestione con l'interfaccia utente Web. Non tutte le funzionalità nell'interfaccia utente Web saranno disponibili nell'app.

Scarica app iOS Scarica l'app Android

Domande frequenti

Se hai ancora domande a cui non hai risposto, puoi controllare il nostro documento delle domande frequenti. Domande frequenti

Passaggio 1

Accendere il punto di accesso se non è già acceso. Controllare lo stato delle spie. Quando la spia LED lampeggia in verde, procedere al passaggio successivo.

L'avvio del punto di accesso richiede circa 8-10 minuti. Il LED lampeggerà in verde a più tonalità, alternando rapidamente verde, rosso e giallo prima di tornare verde. Possono esserci piccole variazioni nell'intensità e nella tonalità dei LED.

Passaggio 2

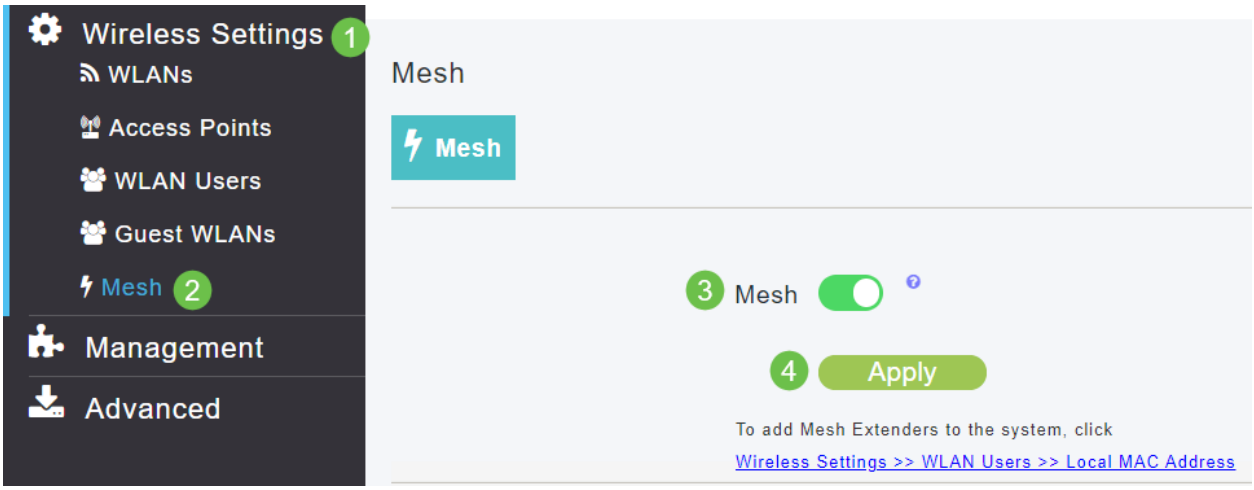
Accedere all'interfaccia utente Web dell'access point primario. Aprire un browser Web e immettere https://ciscobusiness.cisco Potrebbe essere visualizzato un avviso prima di procedere. Immettere le credenziali.

Èinoltre possibile accedervi immettendo l'indirizzo IP dell'access point primario in un browser Web.

Passaggio 3

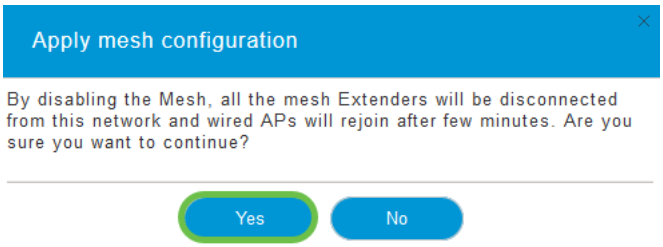
Affinché una RLAN funzioni, l'access point non può essere in modalità mesh. Per disattivare la

modalità mesh, selezionare **Wireless Settings > Mesh** (Impostazioni wireless > Mesh). Selezionate per disattivare la mesh. Se il punto di accesso è nuovo o si è certi che la modalità mesh non sia attiva, è possibile passare al punto 7.



Passaggio 4

Confermate di voler disattivare la modalità mesh facendo clic su **Sì**.

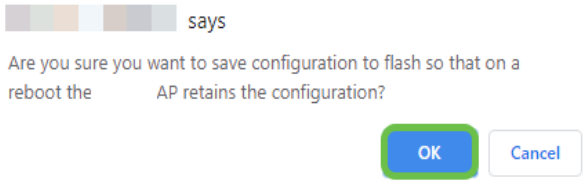


Passaggio 5

Assicurarsi di salvare le configurazioni facendo clic sull'**icona Salva** nel pannello superiore destro della schermata dell'interfaccia utente Web.

Passaggio 6

Confermare il salvataggio facendo clic su **OK**. L'access point verrà riavviato. Il completamento dell'operazione richiederà 8-10 minuti.

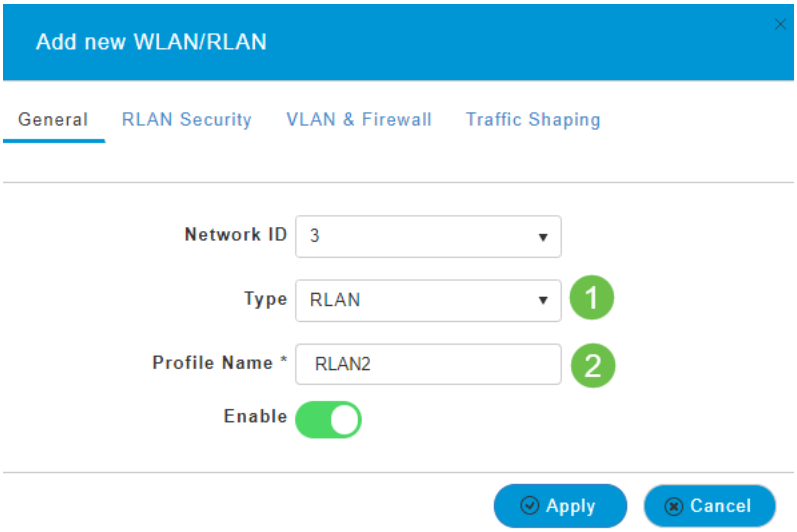


Passaggio 7

Per creare una RLAN, selezionare **Impostazioni wireless > WLAN**. Quindi selezionare **Add new WLAN/RLAN** (Aggiungi nuova WLAN/RLAN).

Passaggio 8

Selezionare **RLAN**. Creare un nome per il profilo.

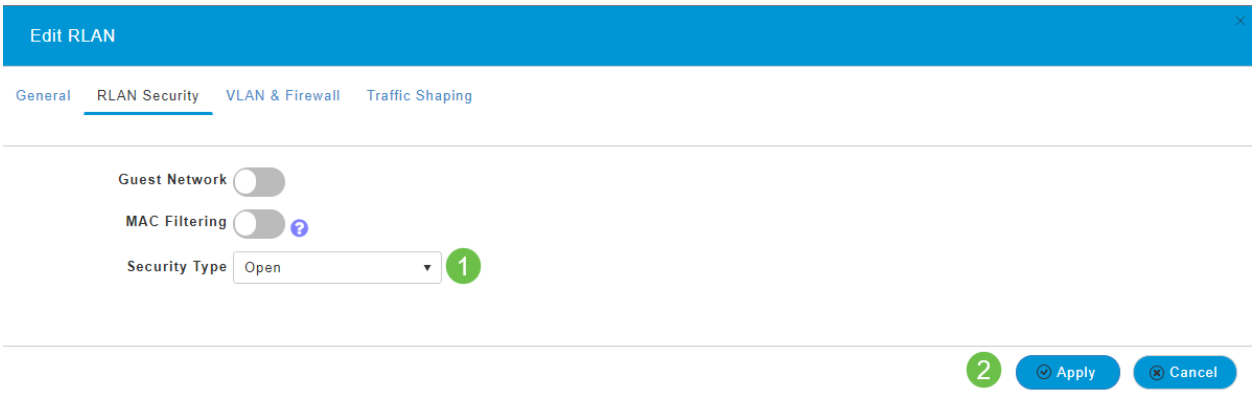


Passaggio 9 (Utilizzo della protezione aperta)

Nella scheda *Sicurezza RLAN*. In *Tipo di protezione* è possibile selezionare *Apri* o *802.1X*.

Nell'esempio, il *tipo di protezione* è stato lasciato come predefinito.

Fare clic su **Apply** (Applica). L'RLAN di sicurezza aperta verrà attivata automaticamente. Andare al passo 11.



Fase 10a (uso della sicurezza 802.1X)

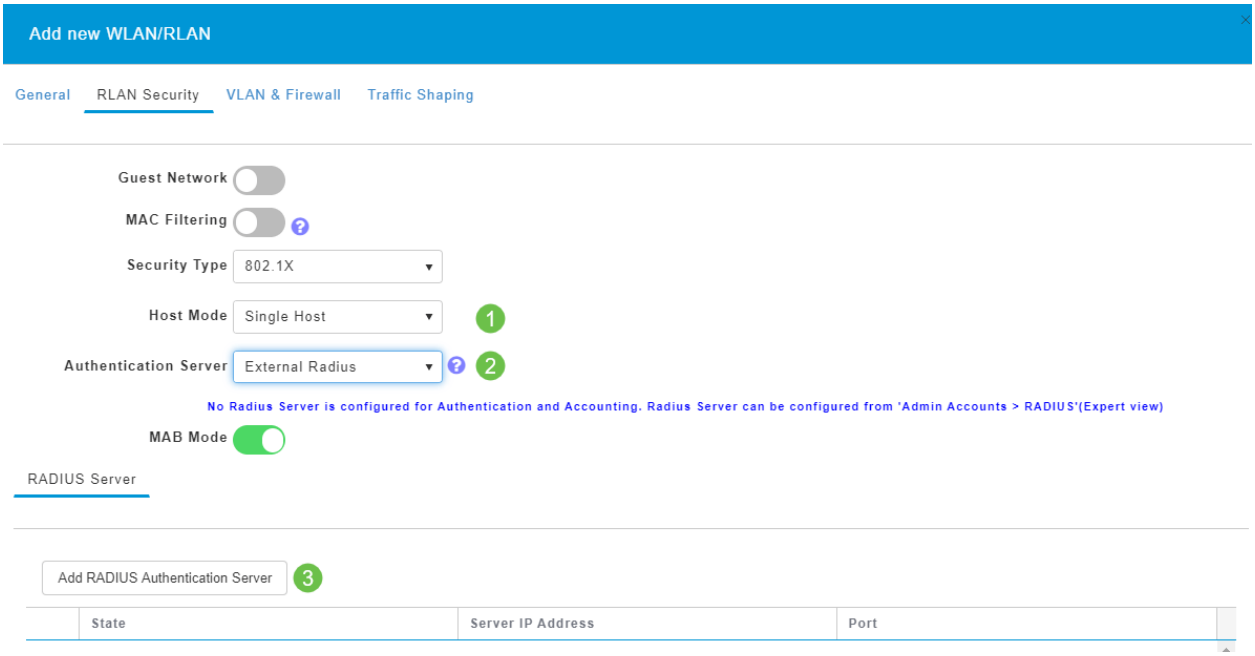
Per impostare un server Radius esterno, è necessario che il server Radius sia configurato in *Admin Accounts* in *RADIUS* in *Expert View*. Fare clic sull'**icona a forma di freccia** nel menu in alto a destra dell'interfaccia utente Web per passare alla *visualizzazione avanzata*. Per ulteriori informazioni sulla configurazione di un server RADIUS, consultare Radius

Fase 10b (uso della sicurezza 802.1X)

Se si sceglie 802.1X come Tipo di protezione, è necessario selezionare altre opzioni. Selezionare quanto segue:

- *Modalità host* - *Host singolo* o *multi-host*

- *Server di autenticazione - Radius* o *AP esterno*
- *Modalità MAB - Attivata* o *Disattivata.* Per aggiungere indirizzi MAC, seguire le istruzioni nel passaggio successivo.

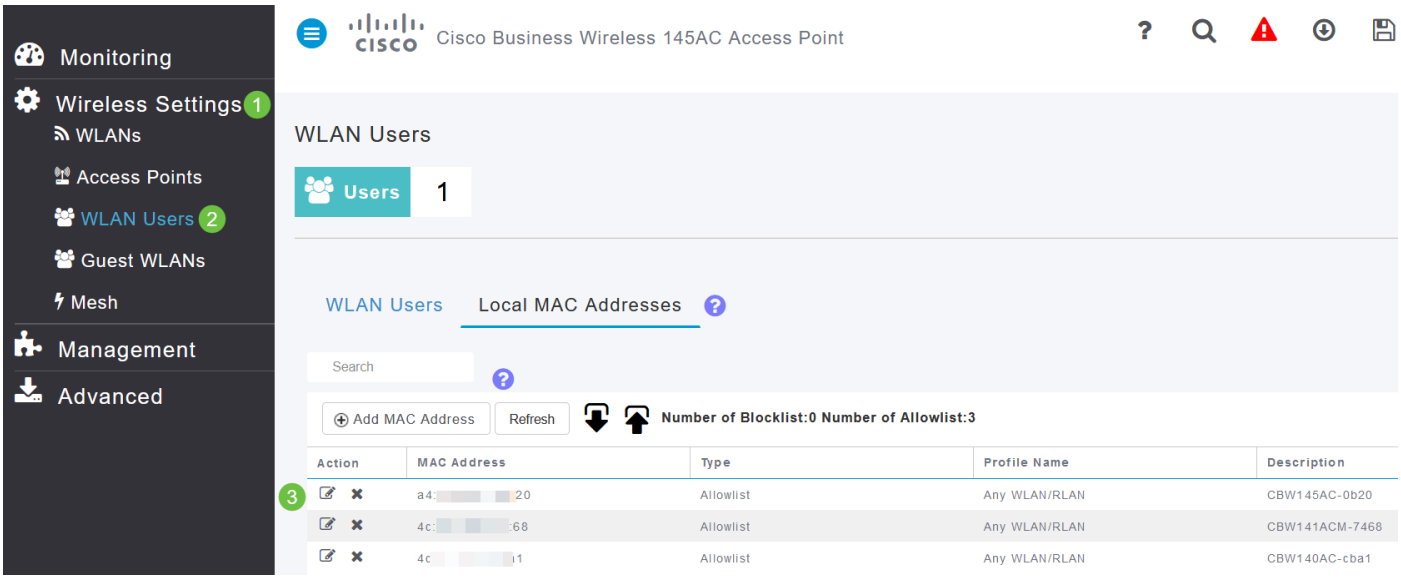


Passaggio 11 (facoltativo)

La modalità MAB (MAC Authentication Bypass) indica che se si dispone di un indirizzo MAC elencato in Utenti WLAN, il dispositivo non deve eseguire l'autenticazione. Gli indirizzi MAC elencati possono ignorare l'autenticazione per ottenere l'accesso automatico alla rete o il rifiuto automatico. Questa funzione è utile quando un telefono IP è collegato a una porta PoE di uno switch.

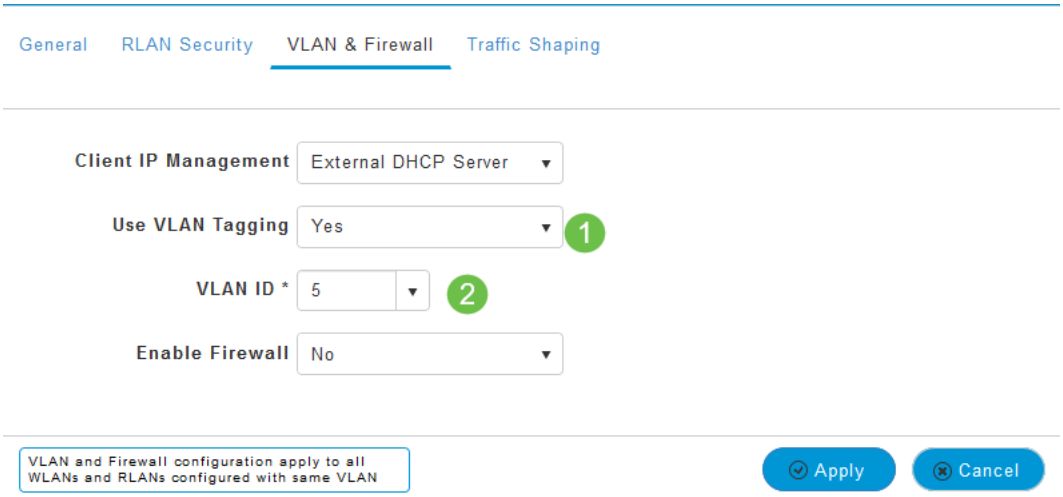
Èpossibile assegnare un'etichetta a ciascun indirizzo MAC in due modi:

1. *Allowlist* - Il dispositivo riceve l'accesso automatico.
2. *Blocklist* - Al dispositivo verrà automaticamente negato l'accesso.



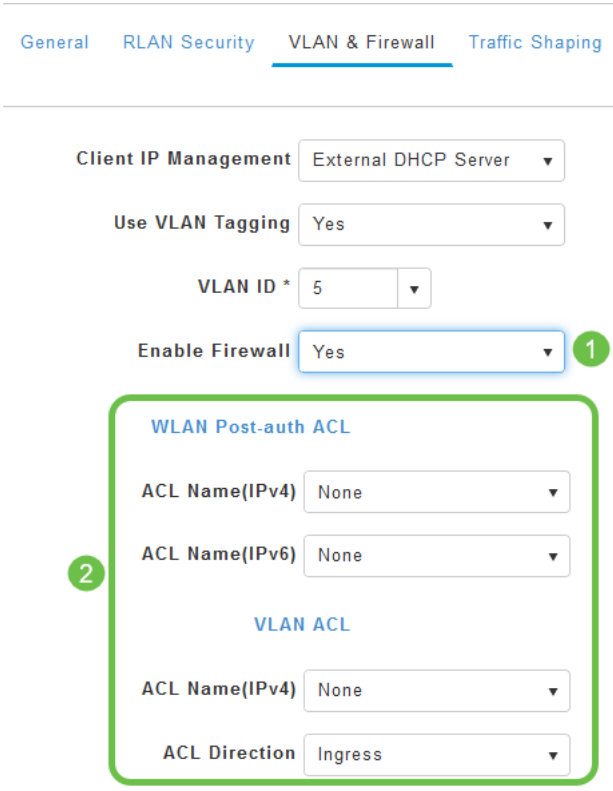
Passaggio 12

Nella scheda *VLAN e firewall*, è possibile selezionare Usa *tag VLAN* e selezionare un numero *ID VLAN*.



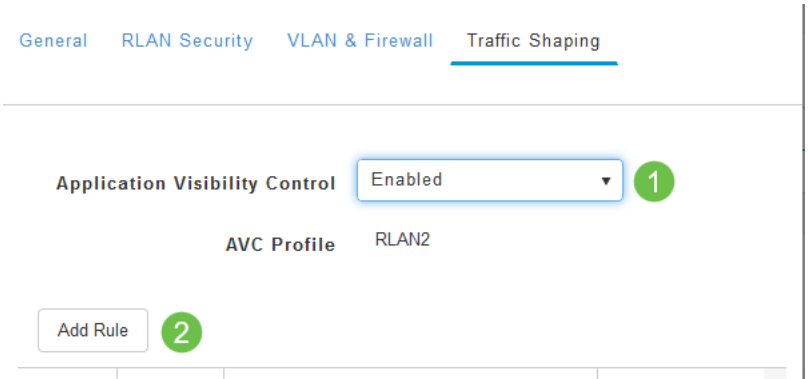
Passaggio 13 (facoltativo)

Èpossibile selezionare **Enable Firewall** (Abilita firewall) se si desidera configurare gli *Access Control Lists (ACL) (elenchi di controllo di accesso) in* modo da consentire o rifiutare l'accesso a specifici indirizzi IP o VLAN. Questa opzione viene utilizzata se un utente sta collegando il dispositivo della porta di rete per connettersi alla rete.



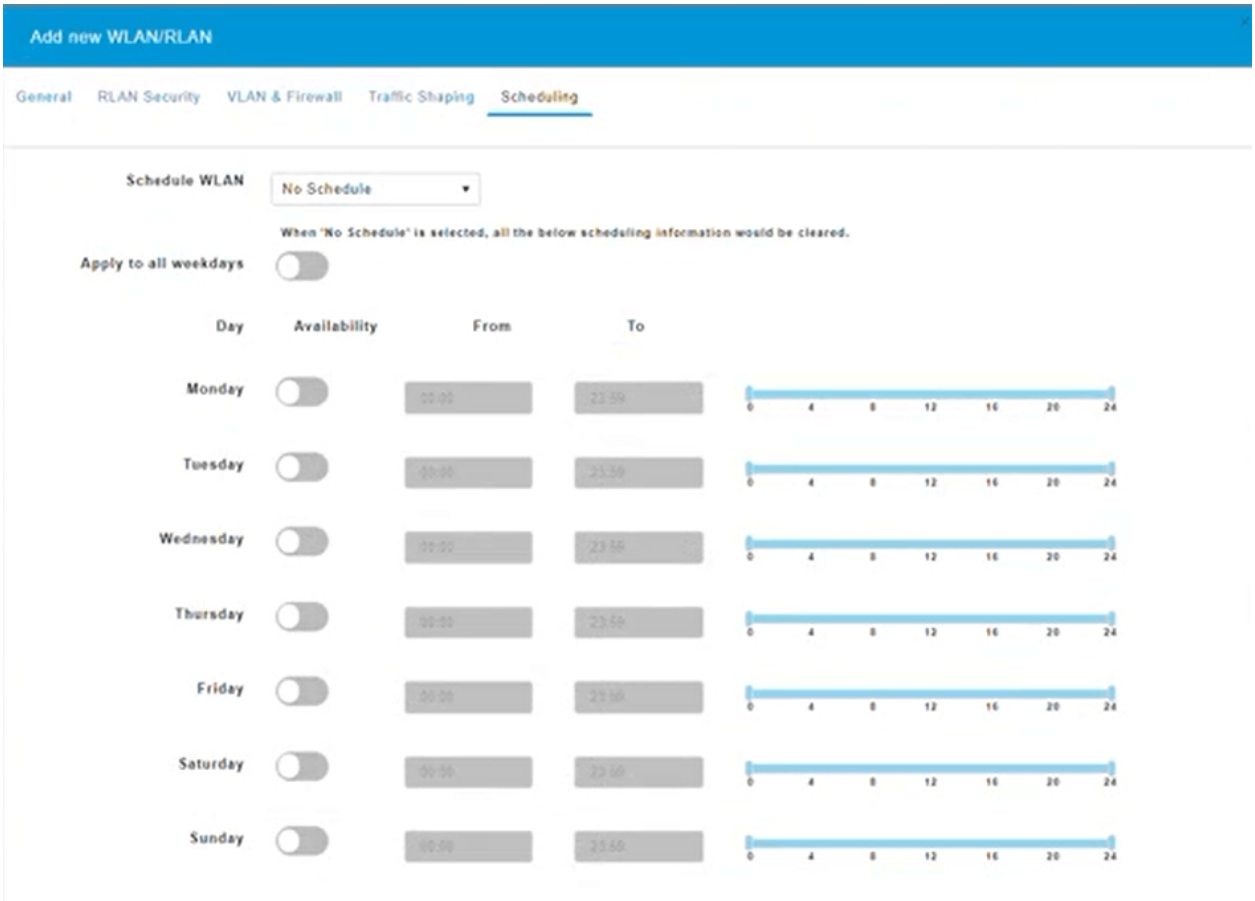
Passaggio 14 (facoltativo)

Nella scheda *Traffic Shaping* è possibile configurare il traffic shaping attivando **Application Visibility Control**. In questo modo viene impostata la priorità del traffico.



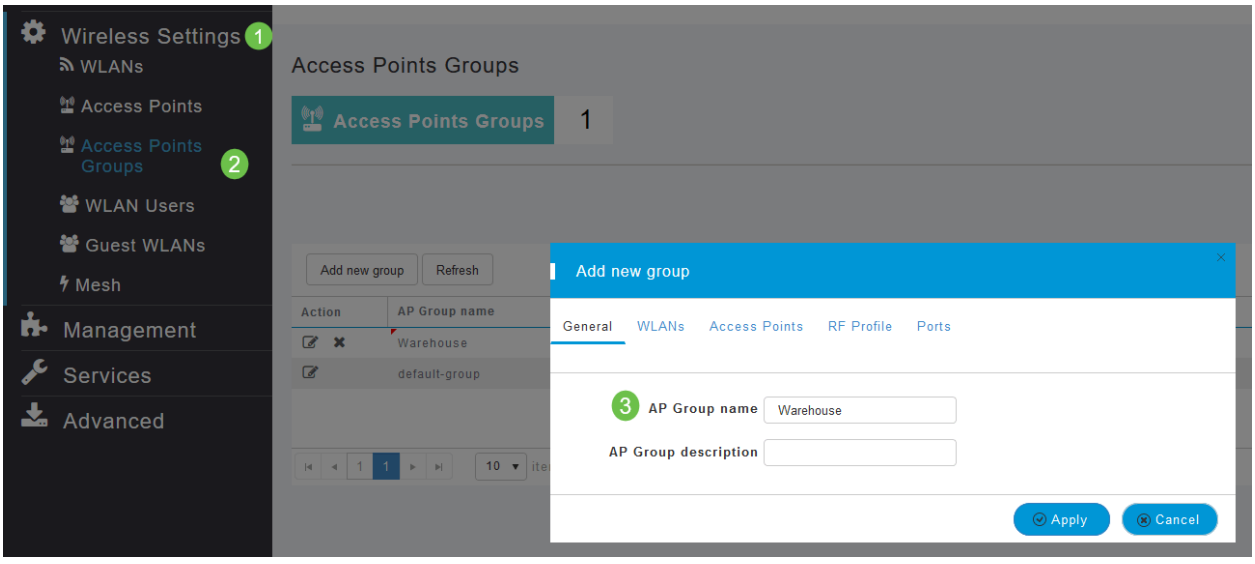
Passaggio 15 (facoltativo)

Nella scheda *Programmazione* è possibile selezionare una programmazione. Questa opzione imposta gli orari in cui la porta potrà essere connessa alla rete.



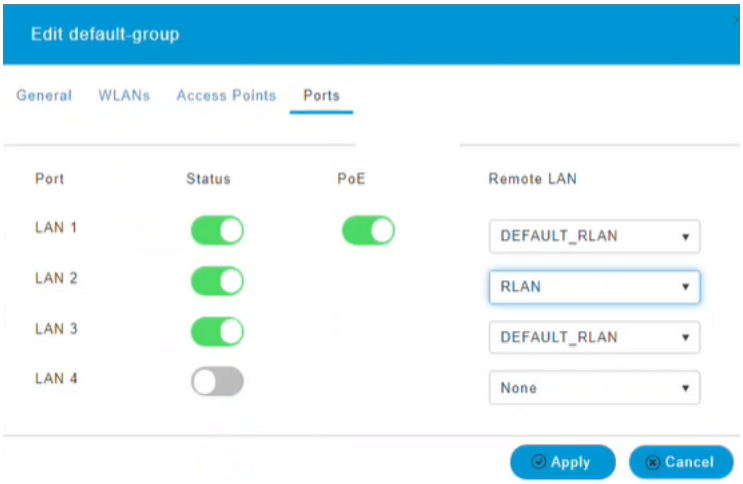
Passaggio 16 (facoltativo)

Una volta creata la RLAN, è possibile selezionare **Impostazioni wireless > Gruppi di punti di accesso**. Qui è possibile aggiungere o modificare i gruppi. Per visualizzare questa schermata, è necessario utilizzare la *visualizzazione Expert*, selezionata nel passaggio 10a.



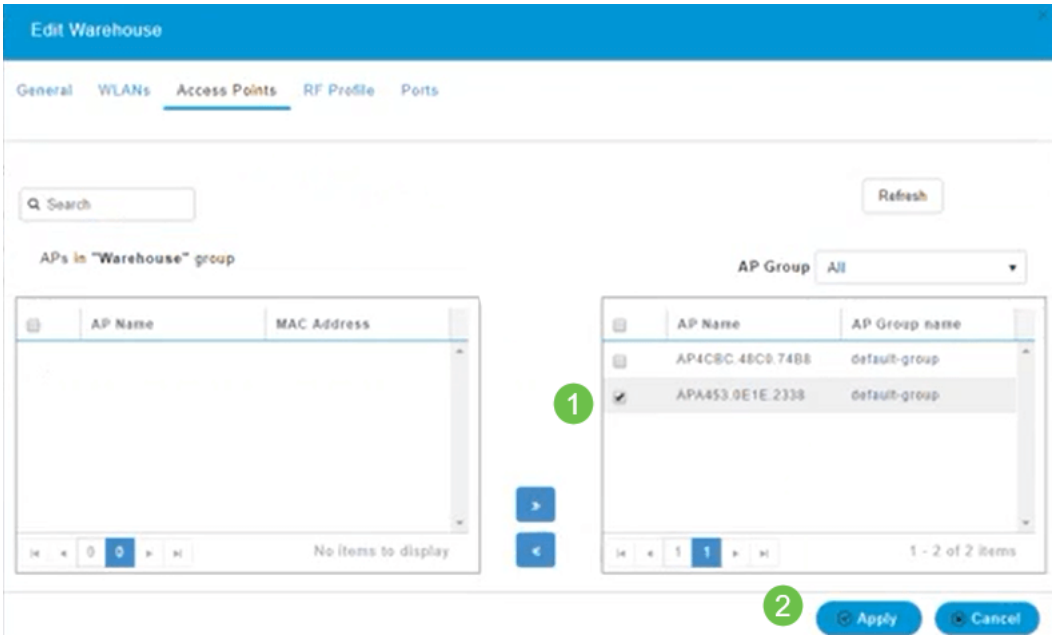
Passaggio 17

Nella scheda *Porte* è possibile assegnare le porte dell'access point a LAN remote specifiche.



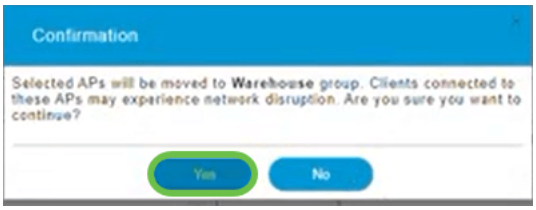
Passaggio 18

Nella scheda *Access Point* è necessario assegnare un punto di accesso specifico a tale gruppo di punti di accesso. Fare clic su **Apply** (Applica).



Passaggio 19

Selezionare **Sì** per confermare.



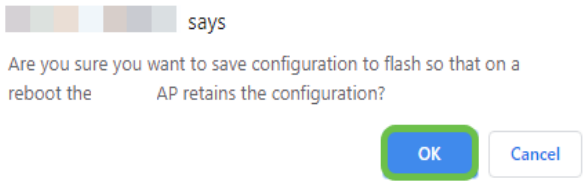
Passaggio 20

Assicurarsi di salvare le configurazioni facendo clic sull'**icona Salva** nel pannello superiore destro della schermata dell'interfaccia utente Web.

Passaggio 21

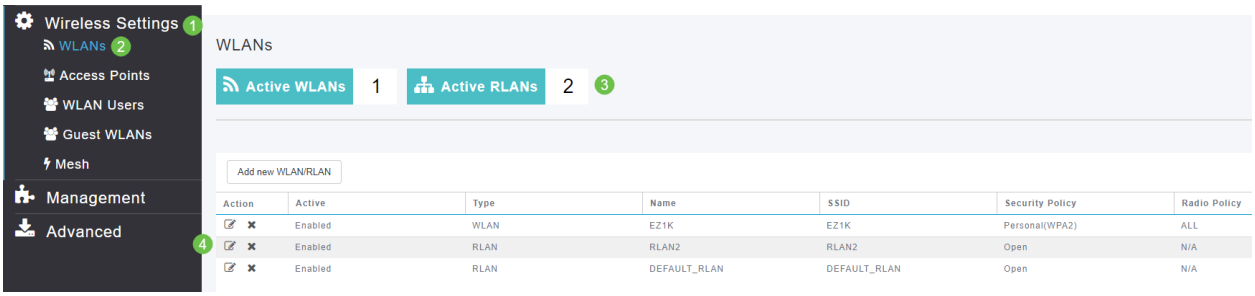
Confermare il salvataggio facendo clic su **OK**. L'access point verrà riavviato. Il completamento

dell'operazione richiederà 8-10 minuti.



Visualizzazione della RLAN

Per visualizzare l'RLAN creata, selezionare **Impostazioni wireless > WLAN**. Il numero di RLAN attive verrà aumentato a 2 e la nuova RLAN verrà elencata.

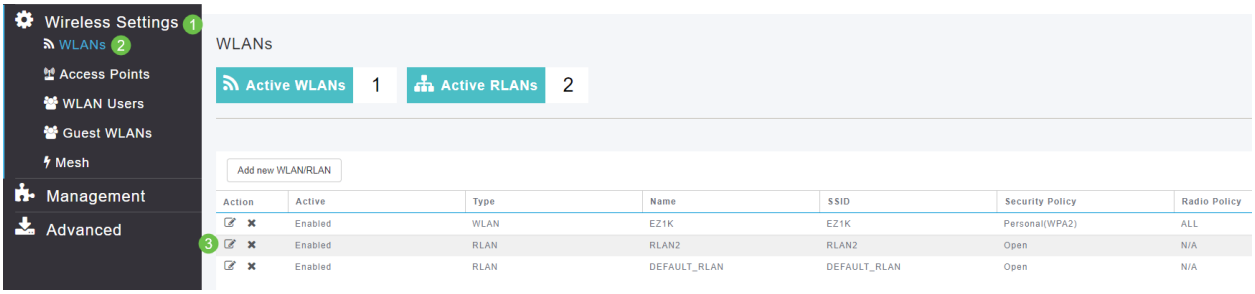


Modifica dell'RLAN

Quando si fa clic su **Apply** (Applica) al termine della configurazione dell'RLAN, l'RLAN viene attivata automaticamente. Per disabilitare la RLAN o apportare altre modifiche, attenersi alla seguente semplice procedura.

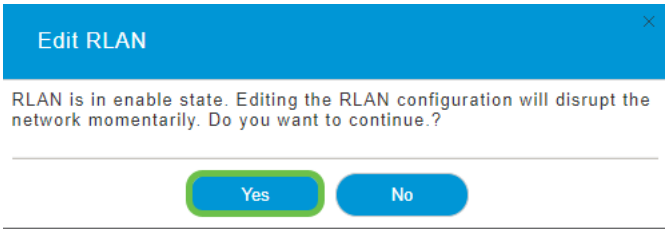
Passaggio 1

Selezionare **Wireless Settings > WLANs**. Fare clic sull'**icona Modifica**.



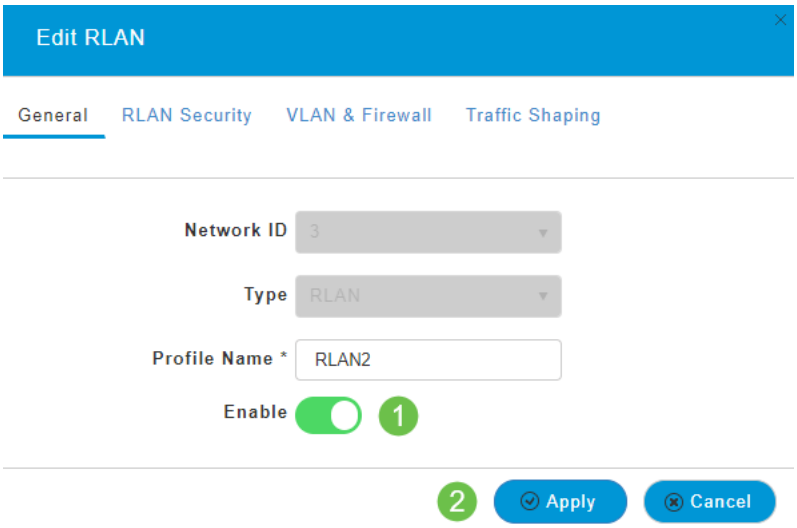
Passaggio 2

Viene visualizzata una schermata di popup che informa che la modifica dell'RLAN interromperà temporaneamente la rete. Confermare che si desidera continuare facendo clic su **Sì**.



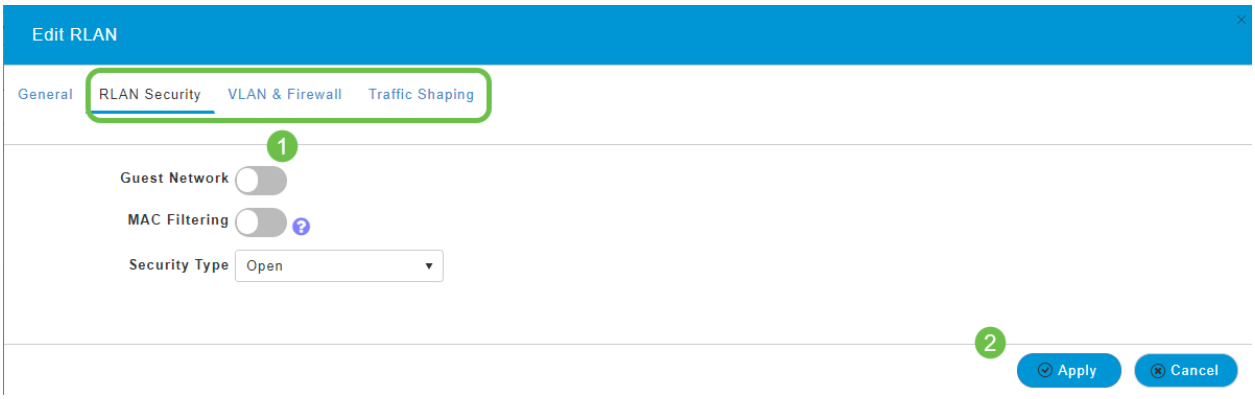
Passaggio 3 (Abilita/Disabilita)

Nella finestra **Edit WLAN/RLAN**, in **General**, selezionare ***Enabled*** (Abilitata) o ***Disabled (Disabilitata)*** per abilitare/disabilitare la RLAN. Fare clic su **Apply** (Applica).



Passaggio 4 (Modifica di altre impostazioni)

Per modificare le impostazioni, selezionare le schede *Sicurezza RLAN*, *VLAN e Firewall* o *Traffic Shaping*. Dopo aver apportato le modifiche, fare clic su **Applica**.



Passaggio 5

Assicurarsi di salvare le configurazioni facendo clic sull'**icona Salva** nel pannello superiore destro della schermata dell'interfaccia utente Web.

Conclusioni

Èstata creata una RLAN sulla rete CBW. Divertiti e potrai aggiungere altro se si adatta alle tue esigenze.

Domande frequenti Raggio Aggiornamento firmware RLAN Creazione profilo applicazione Creazione profilo client Strumenti AP primari Umbrella Utenti WLAN Registrazione Traffic Shaping Nemici Interferenti Gestione della configurazione Port Configuration Mesh Mode Benvenuti nella sezione CBW Mesh Networking Rete guest con autenticazione e-mail e accounting RADIUS Risoluzione dei problemi Uso di un router Draytek con CBW