Configurazione di RADIUS in Cisco Business Wireless Access Point

Obiettivo

L'obiettivo di questo documento è mostrare come configurare RADIUS in un Cisco Business Wireless (CBW) Access Point (AP).

Dispositivi interessati | Versione firmware

- 140AC (Scheda tecnica) | 10.4.1.0 (scarica la versione più recente)
- 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

Se si desidera configurare RADIUS nell'access point CBW, è possibile trovare la soluzione giusta. I CBW AP supportano l'ultimo standard 802.11ac Wave 2 per prestazioni più elevate, accesso più ampio e reti a densità più elevata. Offrono prestazioni all'avanguardia con connessioni wireless sicure e affidabili, per un'esperienza utente mobile e affidabile.

RADIUS (Remote Authentication Dial-In User Service) è un meccanismo di autenticazione che consente ai dispositivi di connettersi e utilizzare un servizio di rete. Viene utilizzato per l'autenticazione, l'autorizzazione e la contabilità centralizzate. Un server RADIUS regola l'accesso alla rete verificando l'identità degli utenti tramite le credenziali di accesso immesse. Ad esempio, una rete Wi-Fi pubblica è installata in un campus universitario. Solo gli studenti che dispongono della password possono accedere a queste reti. Il server RADIUS controlla le password immesse dagli utenti e concede o nega l'accesso alla rete WLAN (Wireless Local Area Network) in base alle esigenze.

Per configurare RADIUS sull'access point CBW, iniziare.

Sommario

Configurare RADIUS sull'access point CBW

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.

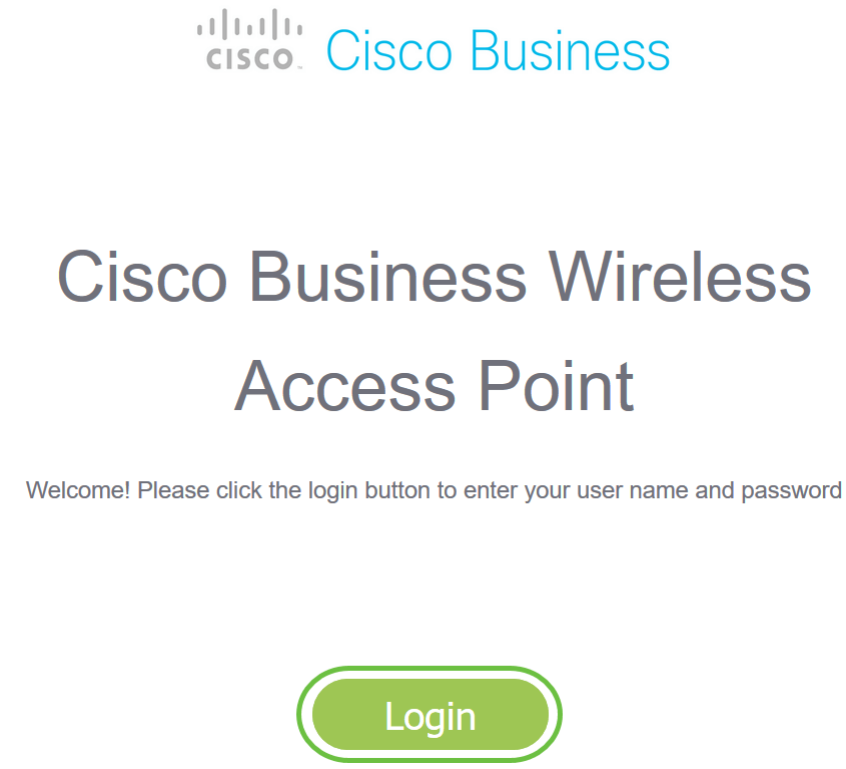
Scarica app iOS Scarica l'app Android

Domande frequenti

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

Passaggio 1

Accedere all'access point CBW utilizzando un nome utente e una password validi.

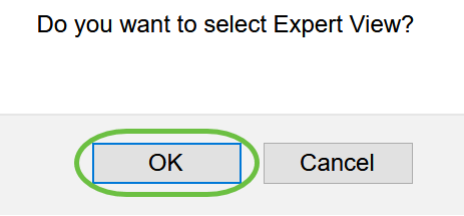


Passaggio 2

Fare clic sul simbolo della **freccia bidirezionale** nella parte superiore dell'interfaccia utente Web

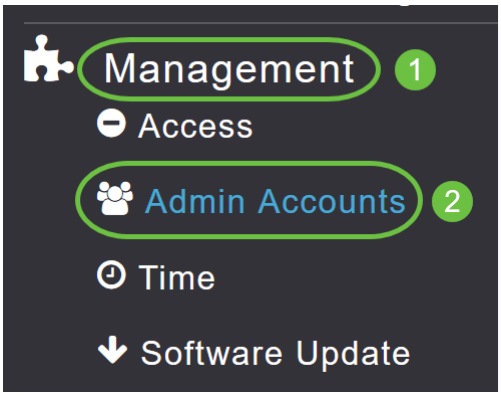
per *passare alla visualizzazione avanzata*.

Verrà visualizzata la seguente schermata a comparsa. Fare clic su **OK** per continuare.



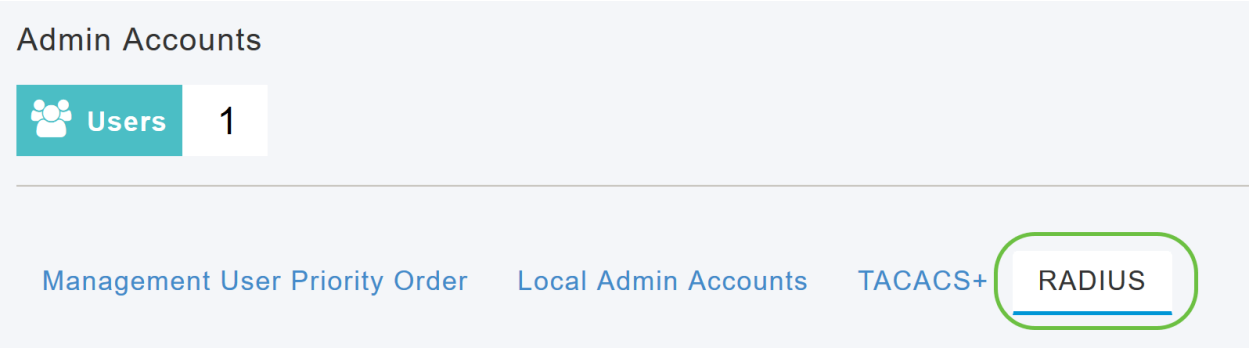
Passaggio 3

Passare a **Gestione > Account amministratore**.



Passaggio 4

Per aggiungere i server RADIUS, fare clic sulla scheda **RADIUS**.

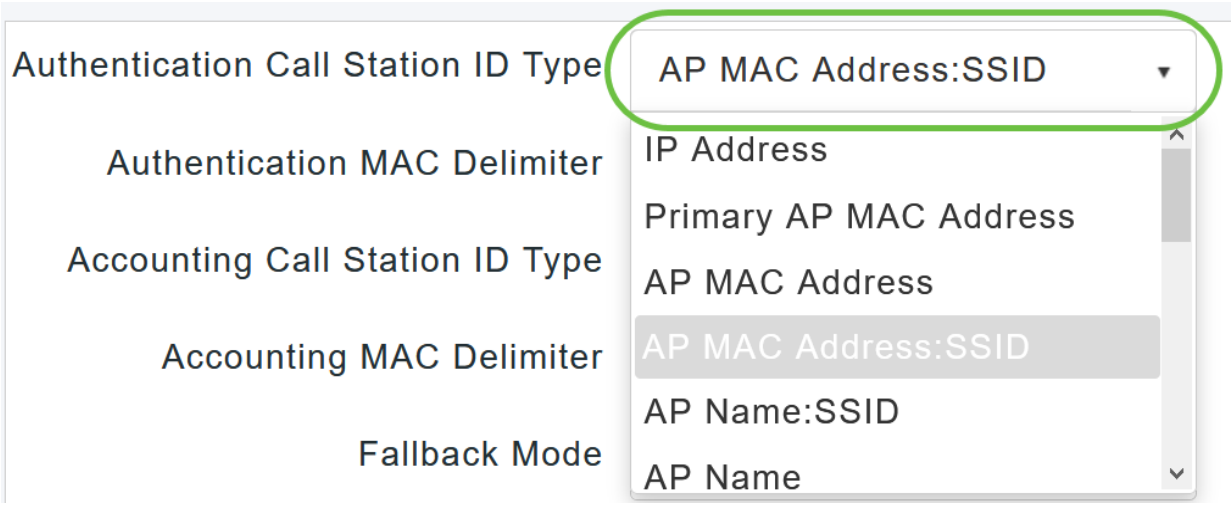


Passaggio 5

Dall'elenco a discesa *Authentication Call Station ID Type* (Tipo di ID stazione di chiamata autenticazione), selezionare l'opzione inviata al server RADIUS nel messaggio Access-Request (Richiesta di accesso). Sono disponibili le seguenti opzioni:

- *Indirizzo IP*

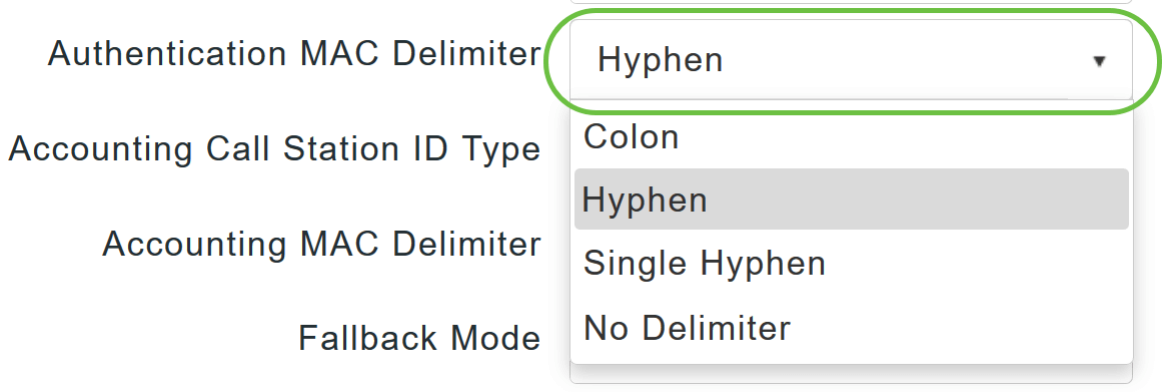
- *Indirizzo MAC AP primario*
- *Indirizzo MAC AP*
- *Indirizzo MAC AP:SSID*
- *Nome AP:SSID*
- *Nome punto di accesso*
- *Gruppo AP*
- *Flex Group*
- *Posizione punto di accesso*
- *ID VLAN*
- *Indirizzo MAC Ethernet AP*
- *Indirizzo MAC Ethernet AP:SSID*
- *Indirizzo etichetta AP*
- *Etichetta punto di accesso: SSID*
- *MAC AP:Gruppo AP SSID*
- *AP Eth MAC:SSID Gruppo AP*



Passaggio 6

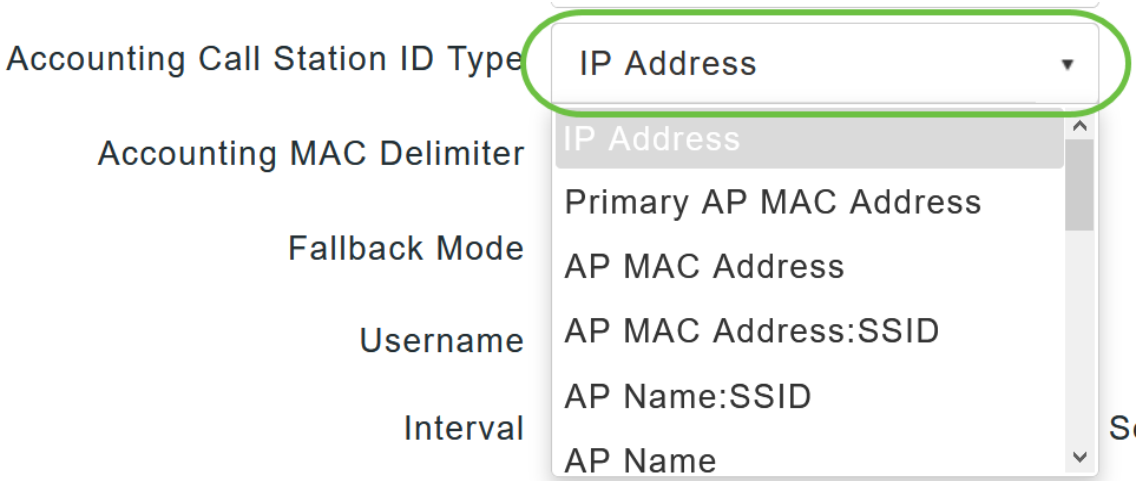
Selezionare il *delimitatore MAC di autenticazione* dall'elenco a discesa. Le opzioni sono:

- *Due punti*
- *Segno meno*
- *Trattino singolo*
- *Nessun delimitatore*



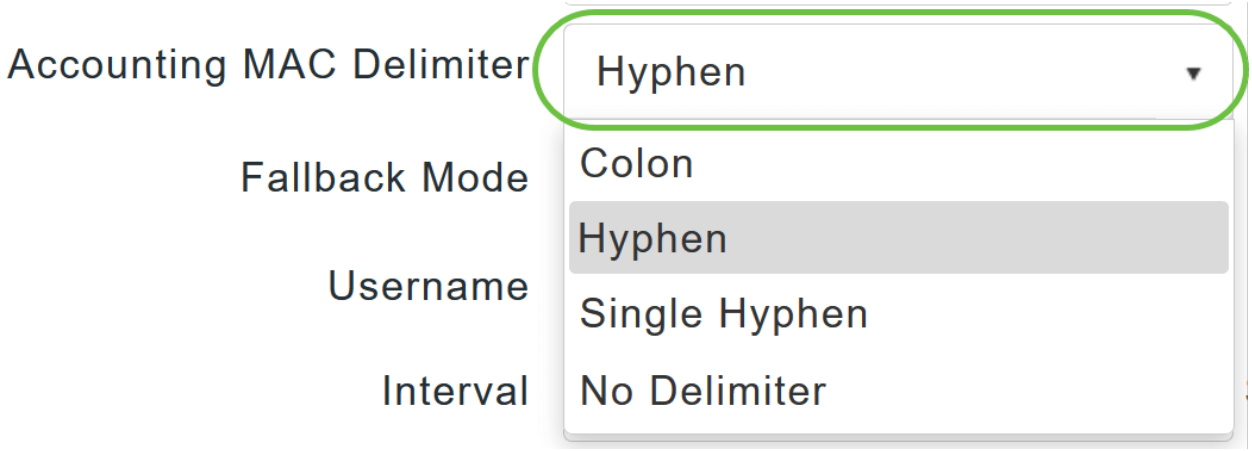
Passaggio 7

Scegliere il *tipo di ID stazione di chiamata contabile* dall'elenco a discesa.



Passaggio 8

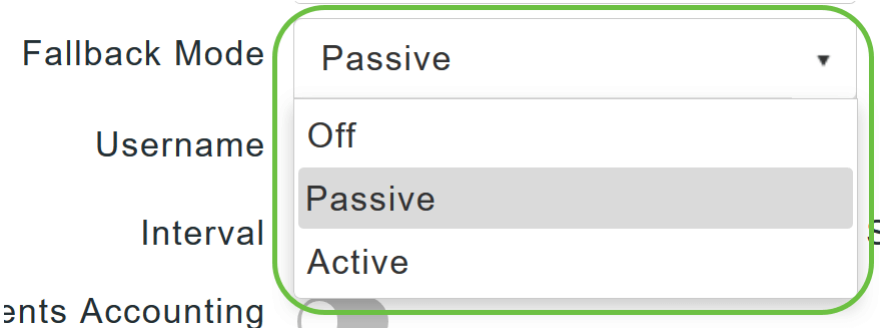
Scegliere il *delimitatore MAC di accounting* dall'elenco a discesa.



Passaggio 9

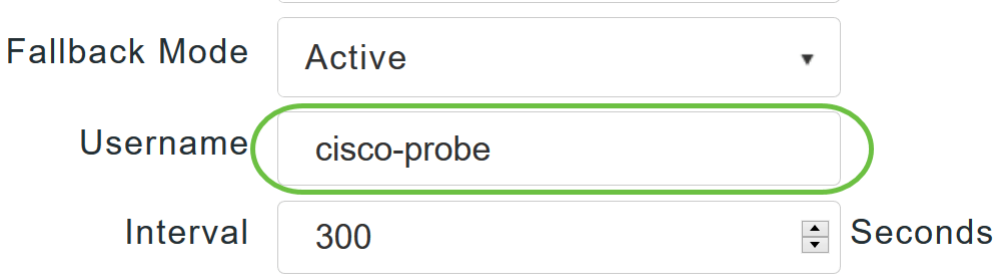
Specificare la *modalità di fallback* del server RADIUS dall'elenco a discesa. Può essere uno dei seguenti:

- *Off* - Disattiva il fallback del server RADIUS. Questo è il valore predefinito.
- *Passivo*: determina il ripristino dell'access point primario a un server con priorità inferiore rispetto ai server di backup disponibili senza utilizzare messaggi di probe estranei. L'access point primario ignora tutti i server inattivi per un determinato periodo di tempo e riprova in seguito quando è necessario inviare un messaggio RADIUS.
- *Attivo* - Consente al punto di accesso primario di tornare a un server con priorità inferiore dai server di backup disponibili utilizzando i messaggi di richieste RADIUS per determinare in modo proattivo se un server contrassegnato come inattivo è di nuovo in linea. Il punto di accesso primario ignora tutti i server inattivi per tutte le richieste RADIUS attive. Quando il server primario riceve una risposta dal server ACS ripristinato, il server RADIUS di fallback attivo non invia più messaggi di probe al server che richiede l'autenticazione probe attiva.



Passaggio 10

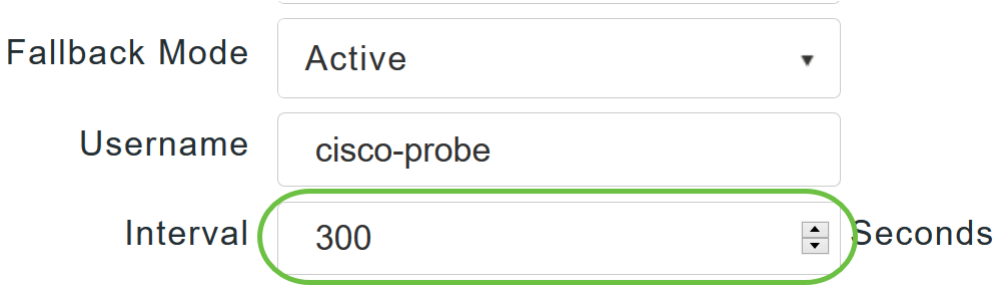
Se è stata abilitata la *modalità di fallback attivo*, immettere il nome da inviare nelle richieste server inattive nel campo *Nome utente*.



Èpossibile immettere fino a 16 caratteri alfanumerici. Il valore predefinito è **cisco-probe**.

Passaggio 11

Se è stata attivata la *modalità Active Fallback*, immettere il valore dell'intervallo di sonda (in secondi) nel campo Intervallo. L'intervallo serve come tempo di inattività in modalità passiva e come intervallo di probe in modalità attiva.

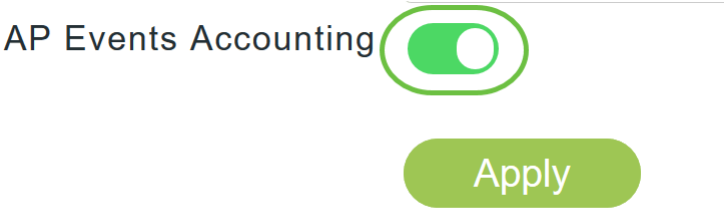


L'intervallo valido è compreso tra 180 e 3600 secondi e il valore predefinito è **300** secondi.

Passaggio 12

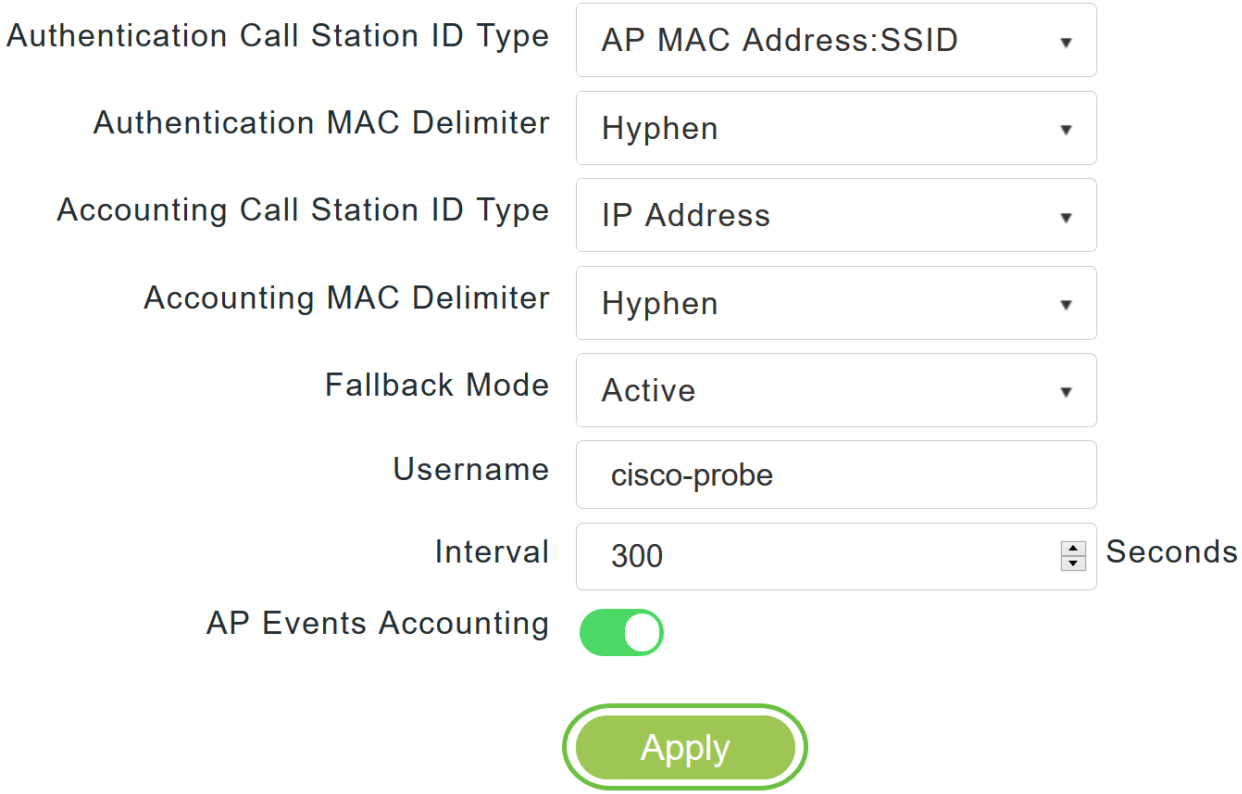
Abilitare il pulsante di scorrimento *Accounting eventi AP* per attivare l'invio di richieste di accounting al server RADIUS.

Durante i problemi di rete, gli access point si uniscono/si disconnettono dall'access point primario. L'attivazione di questa opzione garantisce il monitoraggio di questi eventi e l'invio delle richieste di accounting al server RADIUS per rilevare i problemi di rete.



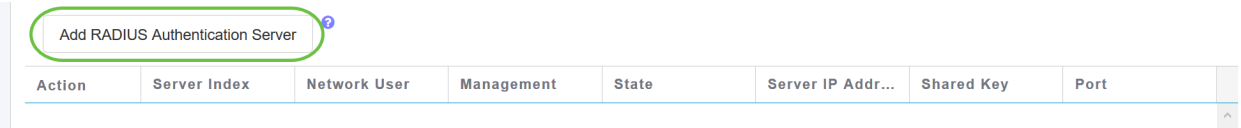
Passaggio 13

Fare clic su **Apply** (Applica).



Passaggio 14

Per configurare il server di autenticazione RADIUS, fare clic su **Add RADIUS Authentication Server**.



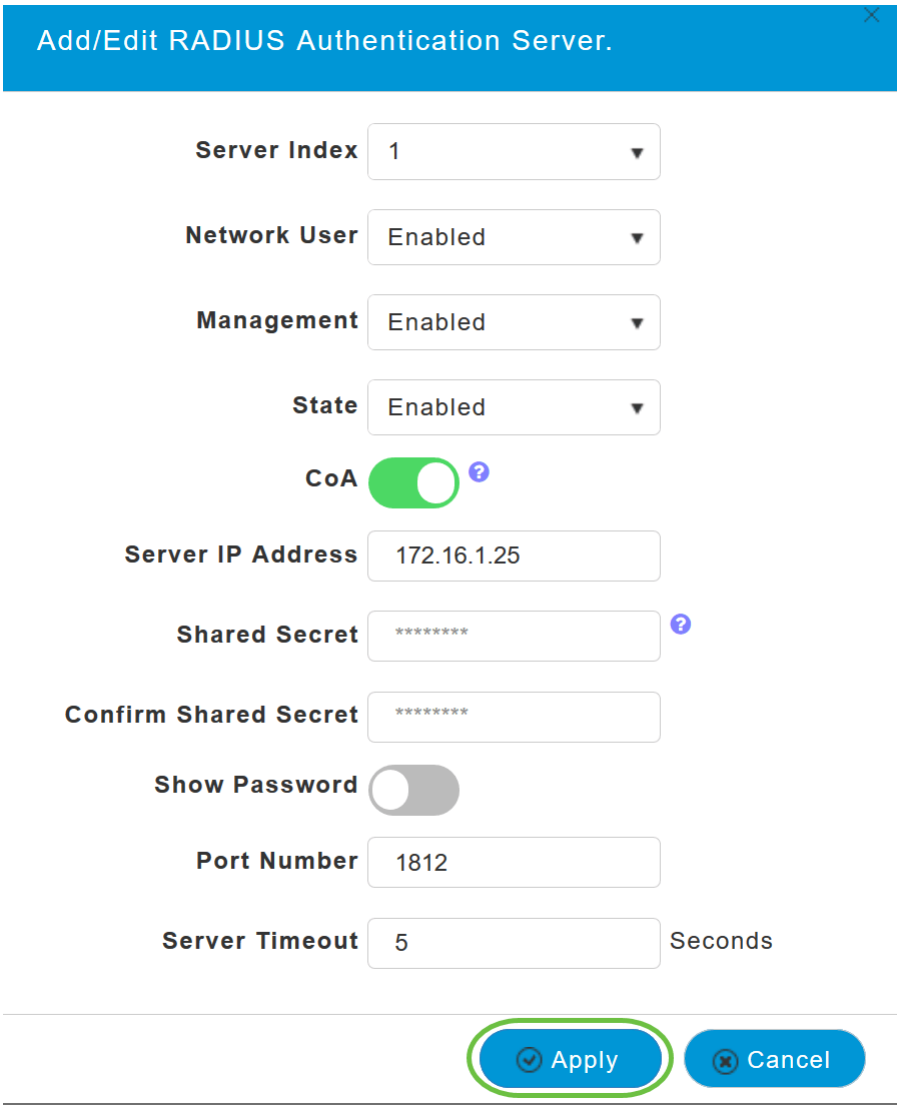
Passaggio 15

Nella finestra popup *Aggiungi/Modifica autenticazione RADIUS*, configurare quanto segue:

- *Indice server* - Selezionare un valore compreso tra 1 e 6
- *Utente di rete* - Abilita lo stato. Per impostazione predefinita, questa opzione è attivata
- *Gestione* - Abilita lo stato. Per impostazione predefinita, questa opzione è attivata
- *State* - Attiva lo stato. Per impostazione predefinita, questa opzione è attivata
- *CoA* - È possibile attivare questa opzione spostando il tasto di scorrimento
- *Indirizzo IP server* - Immettere l'indirizzo IPv4 del server RADIUS

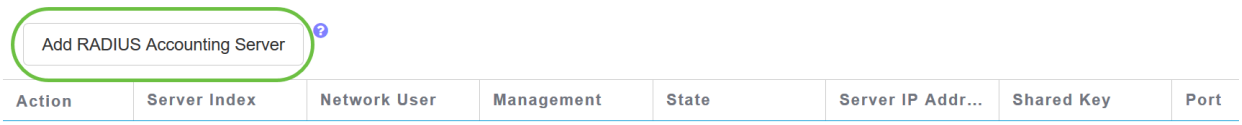
- *Segreto condiviso* - Immettere il segreto condiviso
- *Numero porta*: immettere il numero di porta utilizzato per la comunicazione con il server RADIUS.
- *Timeout server* - Immettere il timeout del server

Fare clic su **Apply** (Applica).



Passaggio 16

Per aggiungere il *server di accounting RADIUS*, eseguire la stessa procedura descritta nel passaggio 15, in quanto la pagina contiene campi simili.

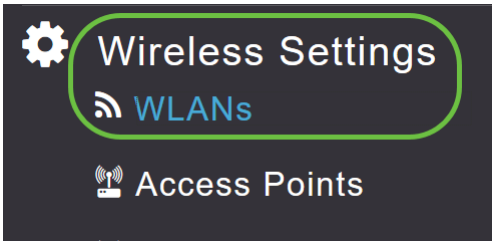


Configurazione WLAN

Passaggio 1

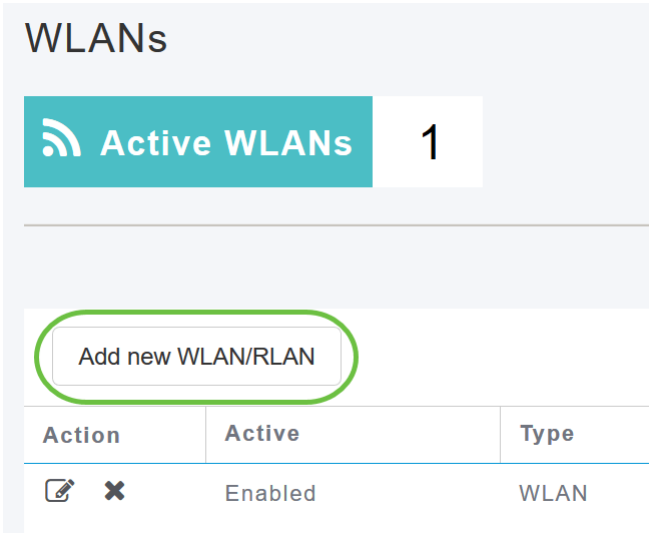
Per configurare la WLAN che gestirà l'autenticazione WPA2 con RADIUS, selezionare

Impostazioni wireless > WLAN.



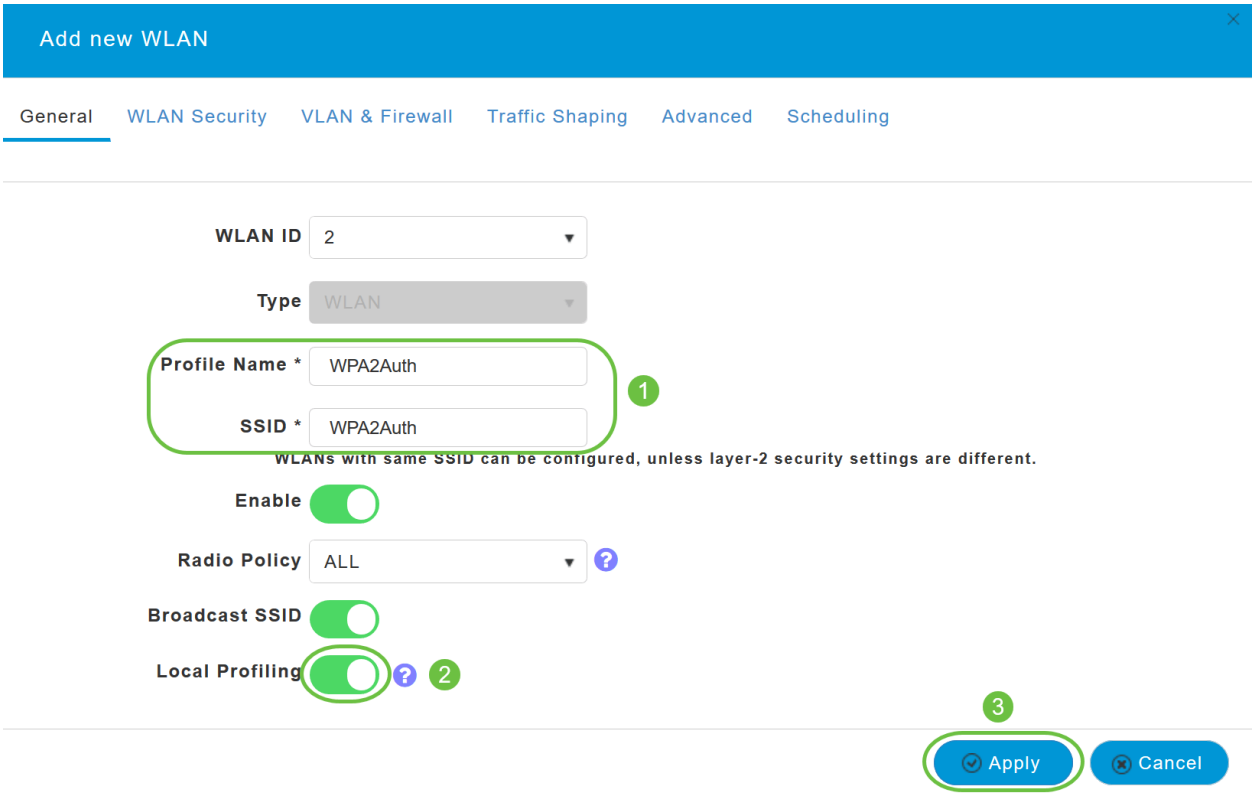
Passaggio 2

Fare clic su **Add New WLAN/RLAN**.



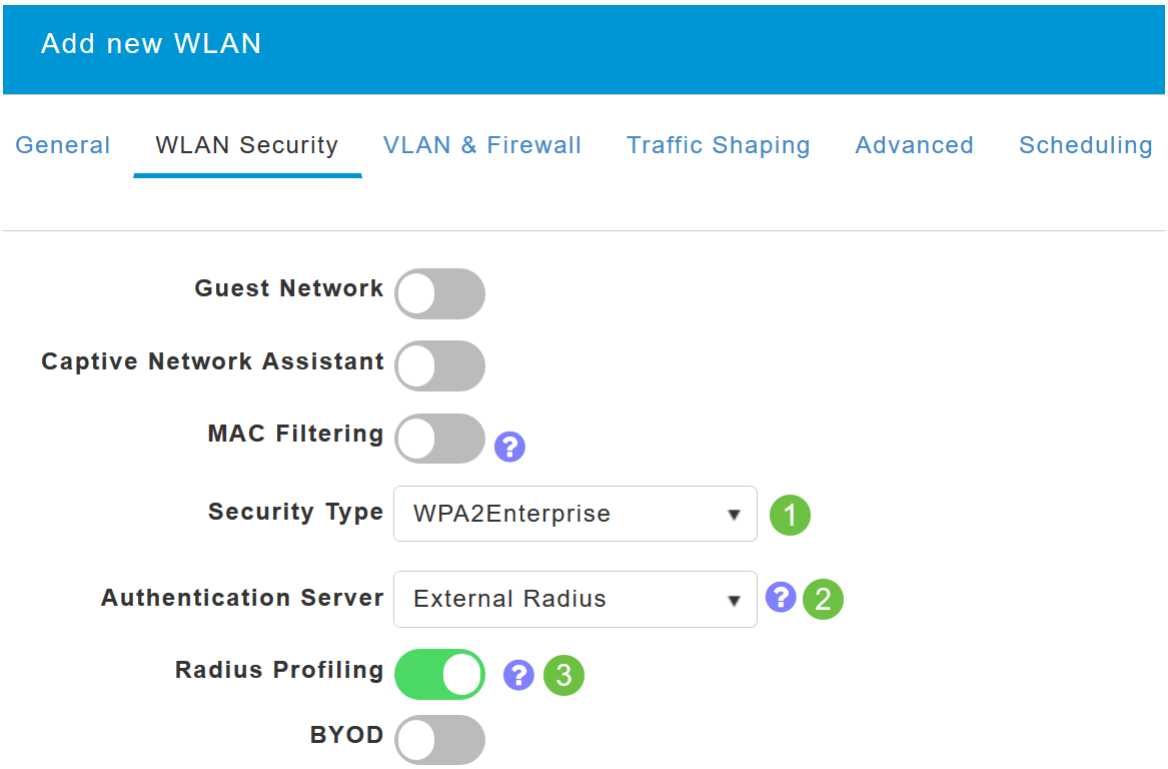
Passaggio 3

Nella scheda *Generale*, immettere il *Nome profilo*. Il campo *SSID* verrà compilato automaticamente. È possibile scegliere di abilitare la *profilatura locale*. Fare clic su **Apply** (Applica).



Passaggio 4

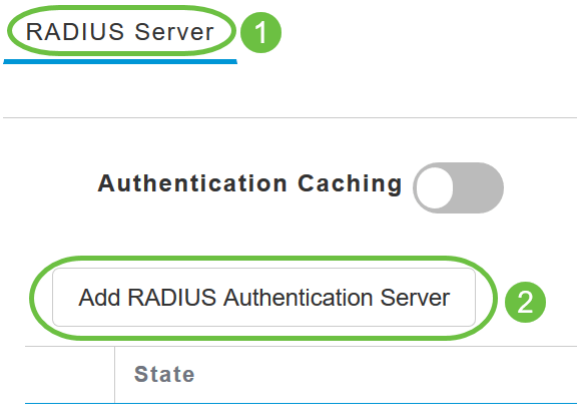
Passare alla scheda *Sicurezza WLAN*. Dal menu a discesa *Tipo di protezione*, scegliere **WPA2Enterprise**. Selezionare **Raggio esterno** come *server* di *autenticazione*. È possibile scegliere di attivare la *profilatura dei raggi*.



Passaggio 5

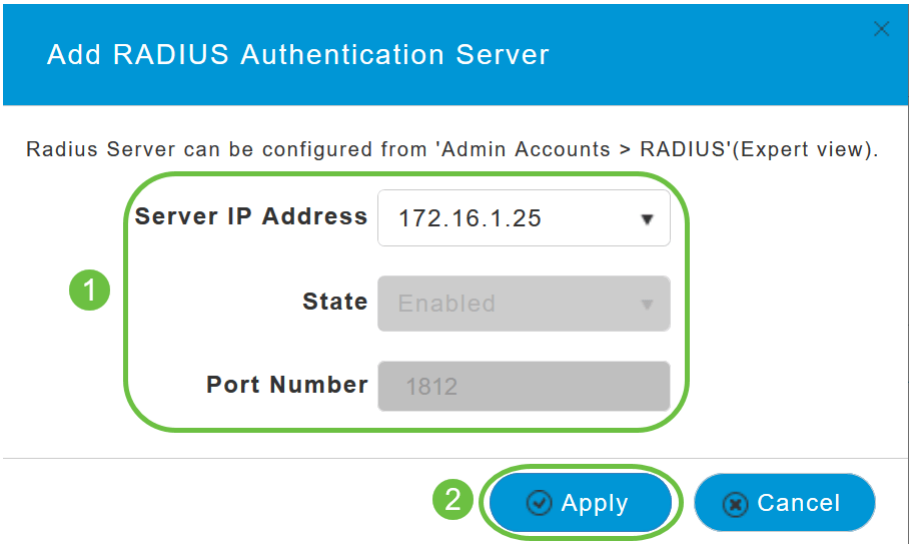
Passare alla sezione *Server RADIUS*. Fare clic su **Add RADIUS Authentication Server (Aggiungi**

server di autenticazione RADIUS).



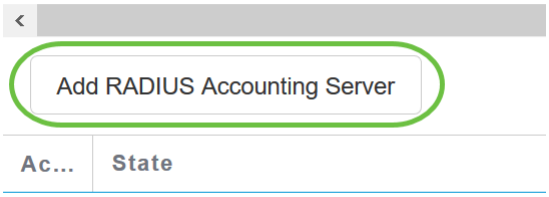
Passaggio 6

Verificare i dettagli del server di autenticazione RADIUS configurato e fare clic su **Applica**.



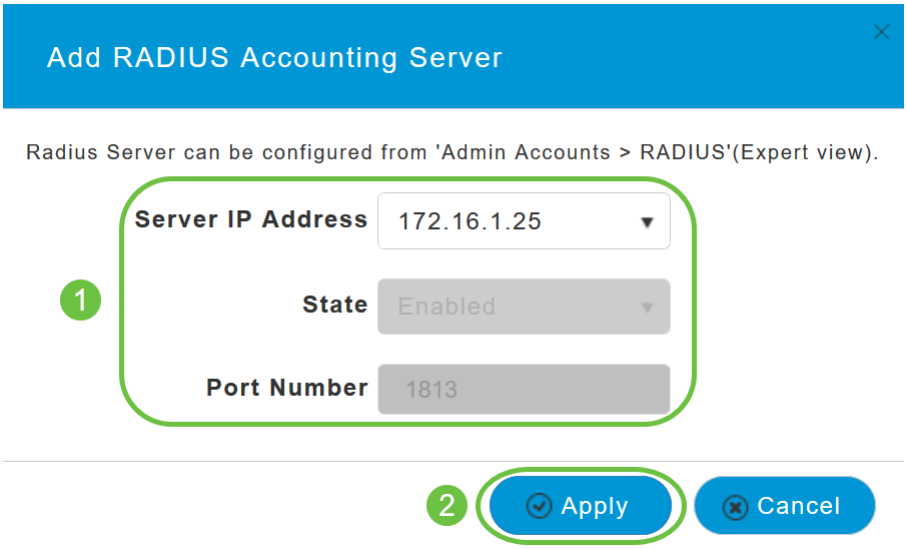
Passaggio 7

Fare clic su **Add RADIUS Accounting Server**.



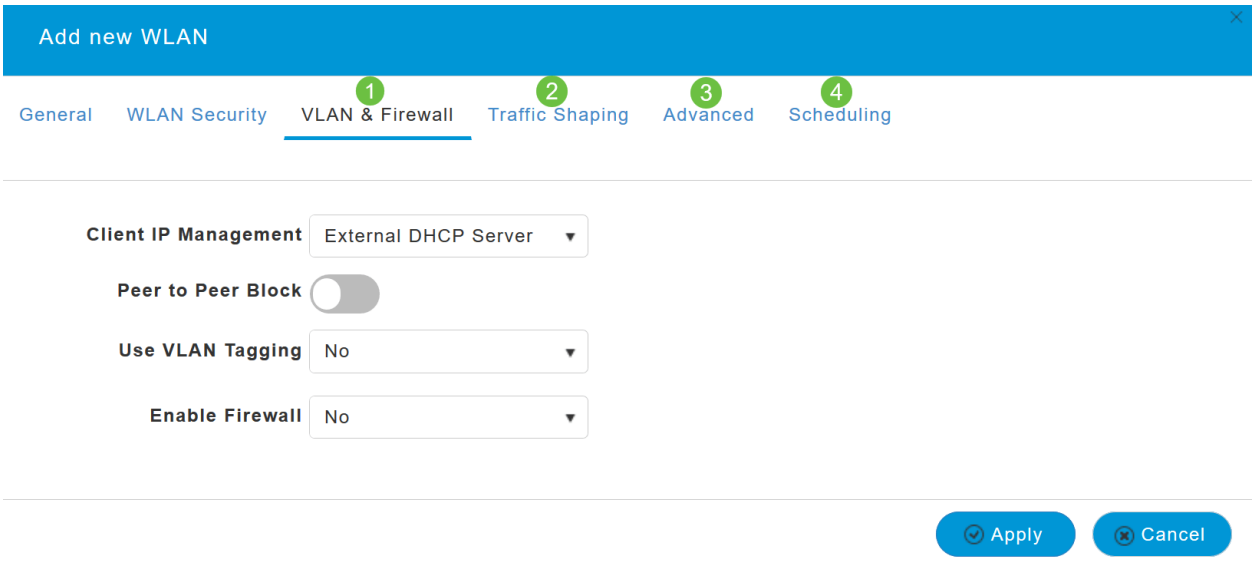
Passaggio 8

Verificare i dettagli del server di accounting RADIUS configurato e fare clic su **Applica**.



Passaggio 9

Passare alle schede *VLAN e firewall*, *Traffic Shaping*, *Advanced* e *Scheduling* per configurare le impostazioni in base alle preferenze di rete. Fare clic su **Apply** (Applica).

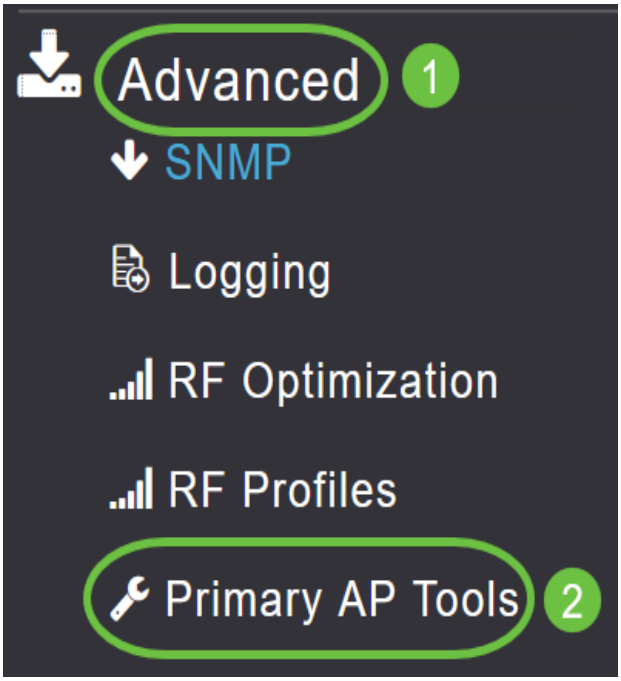


Verifica

Per verificare l'autenticazione RADIUS, eseguire le operazioni seguenti:

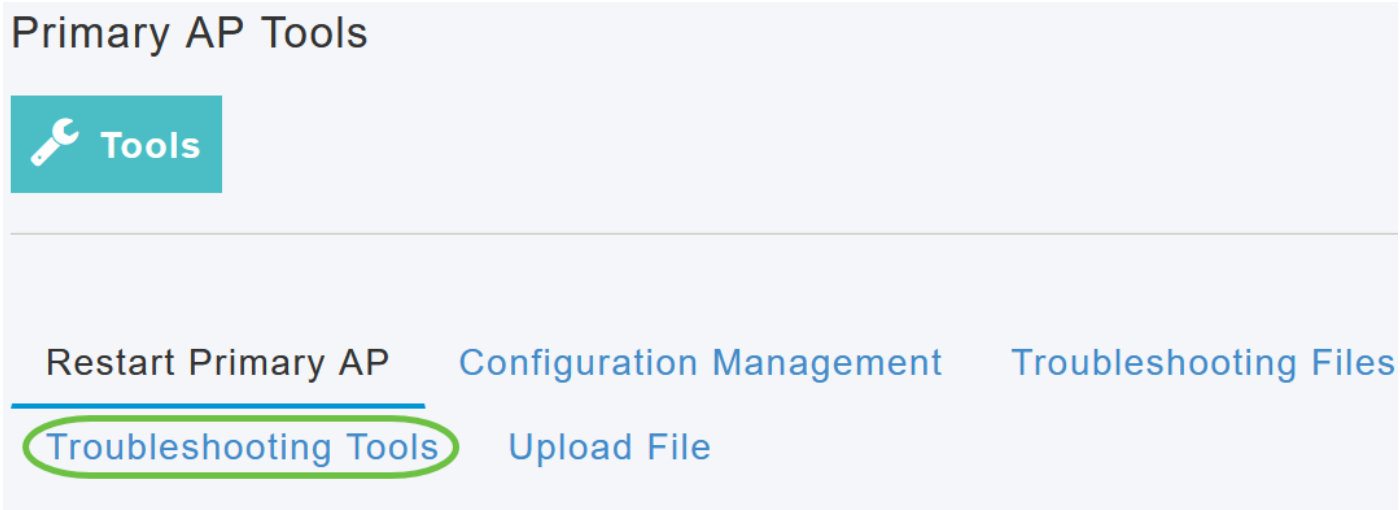
Passaggio 1

Passare a **Avanzate > Strumenti principali PA**.



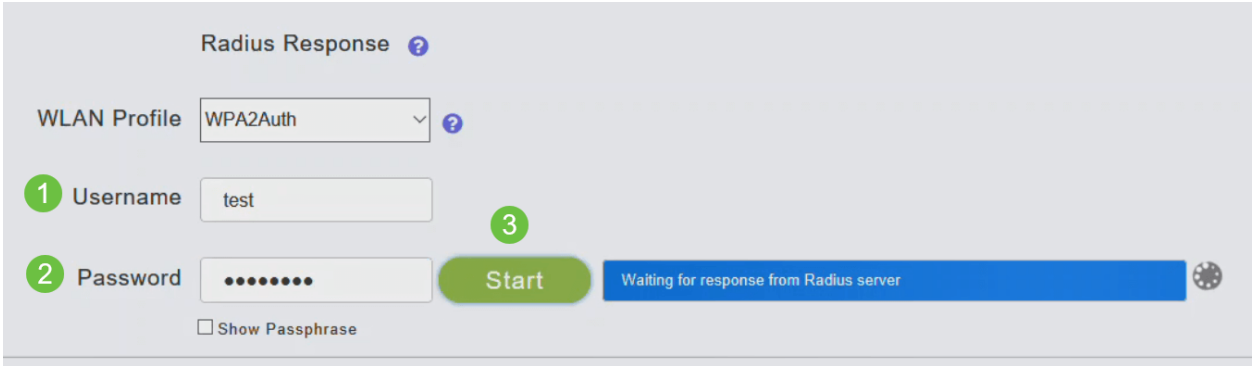
Passaggio 2

Fare clic su **Troubleshooting Tools (Strumenti di risoluzione problemi)**.



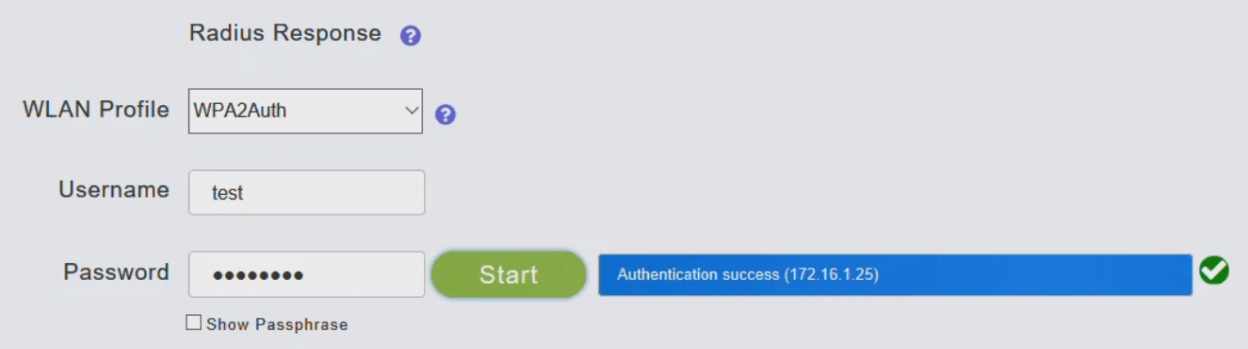
Passaggio 3

Nella sezione *Risposta Radius*, immettere il *nome utente* e la *password* per il profilo WLAN configurato in precedenza e fare clic su **Start**.



Passaggio 4

Una volta completata la verifica, verrà visualizzata la seguente notifica.



Conclusioni

Ecco qua! A questo punto, sono stati descritti i passaggi per configurare RADIUS sull'access point CBW. Per configurazioni più avanzate, fare riferimento al *manuale Cisco Business Wireless Access Point Administration Guide (in lingua inglese).*

Domande frequenti 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