Caratteristica personale chiave già condivisa nel punto di accesso CBW

Obiettivo

In questo articolo viene illustrata la funzionalità PSK (Personal Pre-Shared Key) disponibile nel firmware dei Cisco Business Wireless (CBW) Access Point (AP) versione 10.6.1.0.

Dispositivi interessati | Versione software

- Access point Cisco Business Wireless 140AC | 10.6.1.0 (scarica la versione più recente)
- Access point Cisco Business Wireless 145AC | 10.6.1.0 (scarica la versione più recente)
- Access point Cisco Business Wireless 240AC | 10.6.1.0 (scarica la versione più recente)

Introduzione

Se nella rete è presente un dispositivo CBW, è ora possibile utilizzare la funzione PSK personale nella versione firmware 10.6.1.0!

La chiave PSK personale (iPSK), nota anche come chiave PSK individuale, è una funzione che consente a un amministratore di rilasciare chiavi precondivise univoche a singoli dispositivi per la stessa rete WLAN (Wireless Local Area Network) personale WPA2 (Wi-Fi Protected Access II). La chiave PSK univoca è legata all'indirizzo MAC del dispositivo. Questa funzionalità non è supportata nelle WLAN in cui è abilitato il criterio WPA3.

Questa funzionalità autentica il client utilizzando un server RADIUS. Generalmente è destinato all'uso da parte di dispositivi IoT e di notebook e dispositivi mobili forniti dall'azienda.

Sommario

Prerequisiti

- Accertarsi di aver aggiornato il firmware dell'access point CBW alla versione 10.6.1.0. Fare clic per istruzioni dettagliate sull'aggiornamento del firmware.
- Ènecessario un server RADIUS in cui configurare la chiave PAK personale e l'indirizzo MAC del dispositivo.
- Questa funzionalità CBW è supportata su tre diversi server RADIUS: FreeRADIUS,

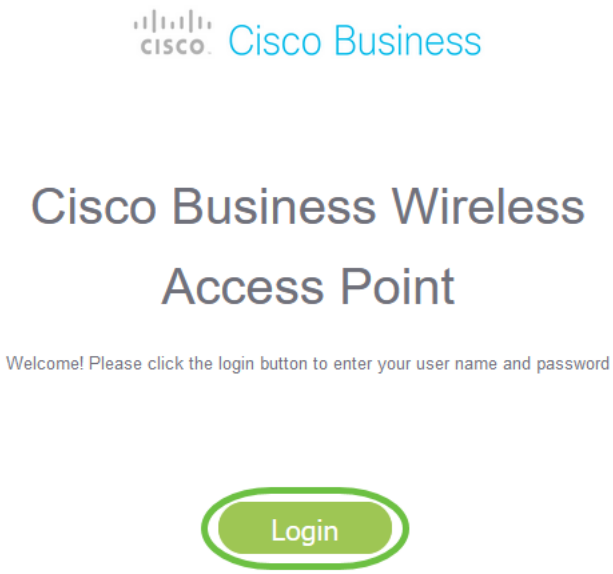
Server dei criteri di rete Microsoft e ISE di Cisco. La configurazione varia a seconda del server RADIUS utilizzato.

Configura impostazioni RADIUS CBW

Per configurare le impostazioni RADIUS sull'access point CBW, attenersi alla seguente procedura.

Passaggio 1

Accedere all'interfaccia utente Web dell'access point CBW.

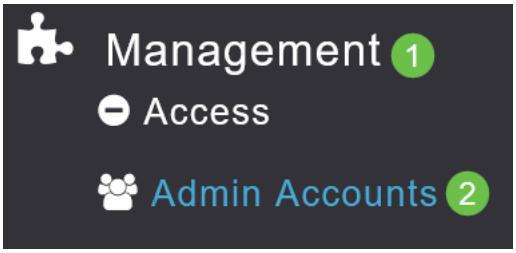


Passaggio 2

Fare clic sul simbolo della **freccia bidirezionale** per passare alla visualizzazione avanzata.

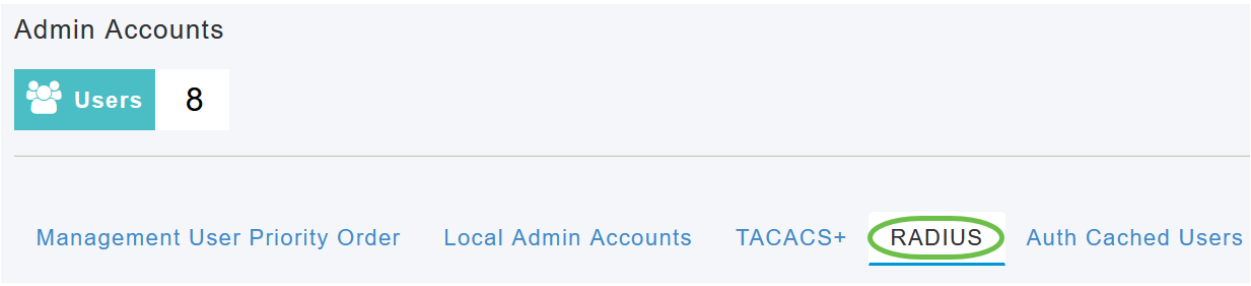
Passaggio 3

Passare a **Gestione > Account amministratore.**



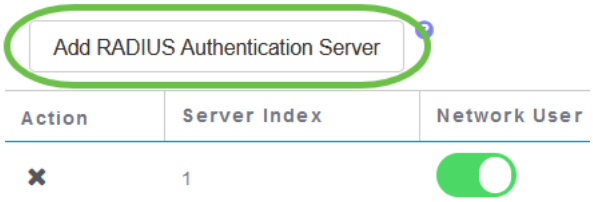
Passaggio 4

Selezionate la scheda **RADIUS**.



Passaggio 5

Fare clic su **Add RADIUS Authentication Server (Aggiungi server di autenticazione RADIUS)**.

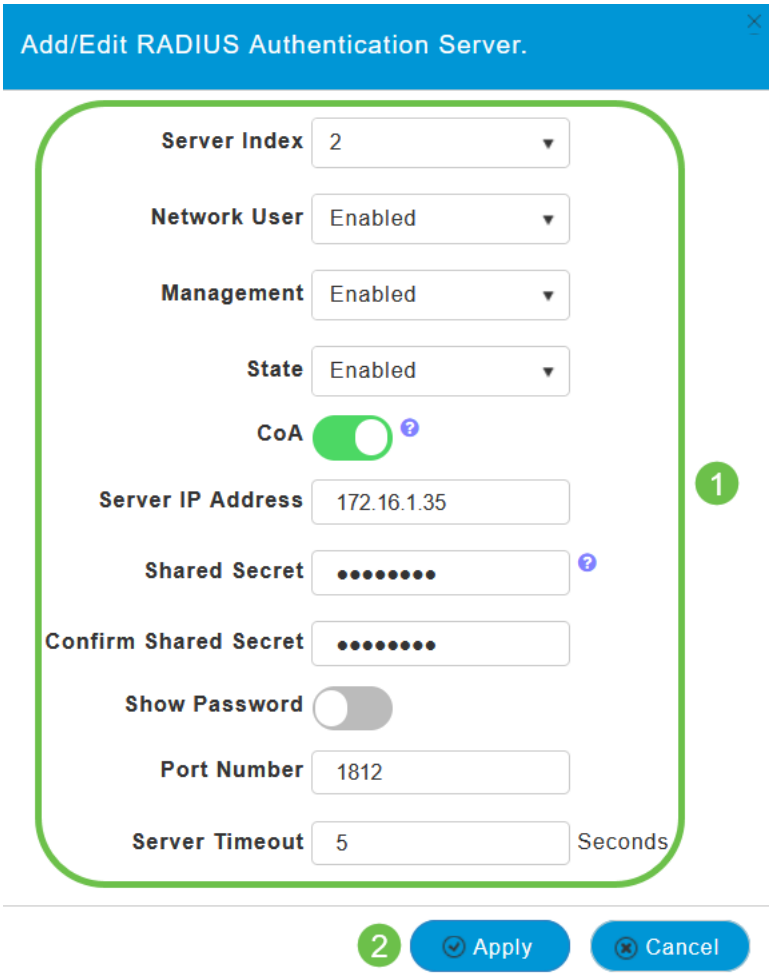


Passaggio 6

Configurare quanto segue:

- *Indice server* - Selezionare un valore compreso tra 1 e 6
- *Utente di rete* - Abilita lo stato. Per impostazione predefinita, è Attivato
- *Gestione* - Abilita lo stato. Per impostazione predefinita, è Attivato
- *State* - Attiva lo stato. Per impostazione predefinita, è Attivato
- *CoA* - Verificare che sia abilitata la funzione CoA (charge of authority).
- *Indirizzo IP server* - Immettere l'indirizzo IPv4 del server RADIUS
- *Segreto condiviso* - Immettere la chiave segreta condivisa
- *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).



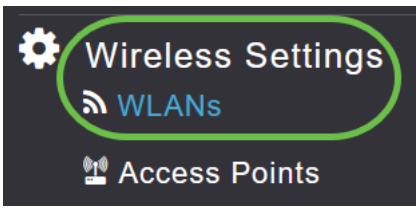
Configurazione delle impostazioni WLAN

Creare una WLAN come WPA2 Personal Secured WLAN standard.

La chiave già condivisa non verrà utilizzata per i dispositivi PSK personali. Questa opzione viene utilizzata solo per i dispositivi NON autenticati sul server RADIUS. Sarà necessario aggiungere gli indirizzi MAC di TUTTI i dispositivi che si connetteranno alla WLAN all'elenco dei dispositivi consentiti di questo dispositivo.

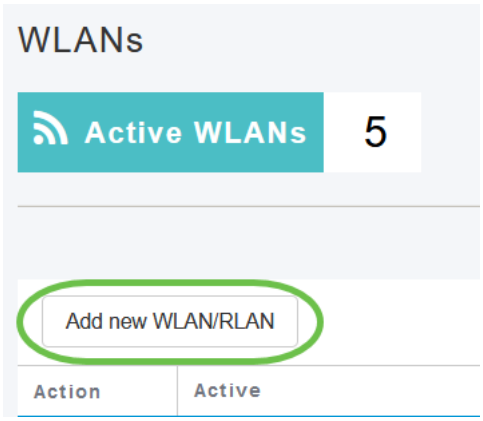
Passaggio 1

Selezionare **Impostazioni wireless > WLAN**.



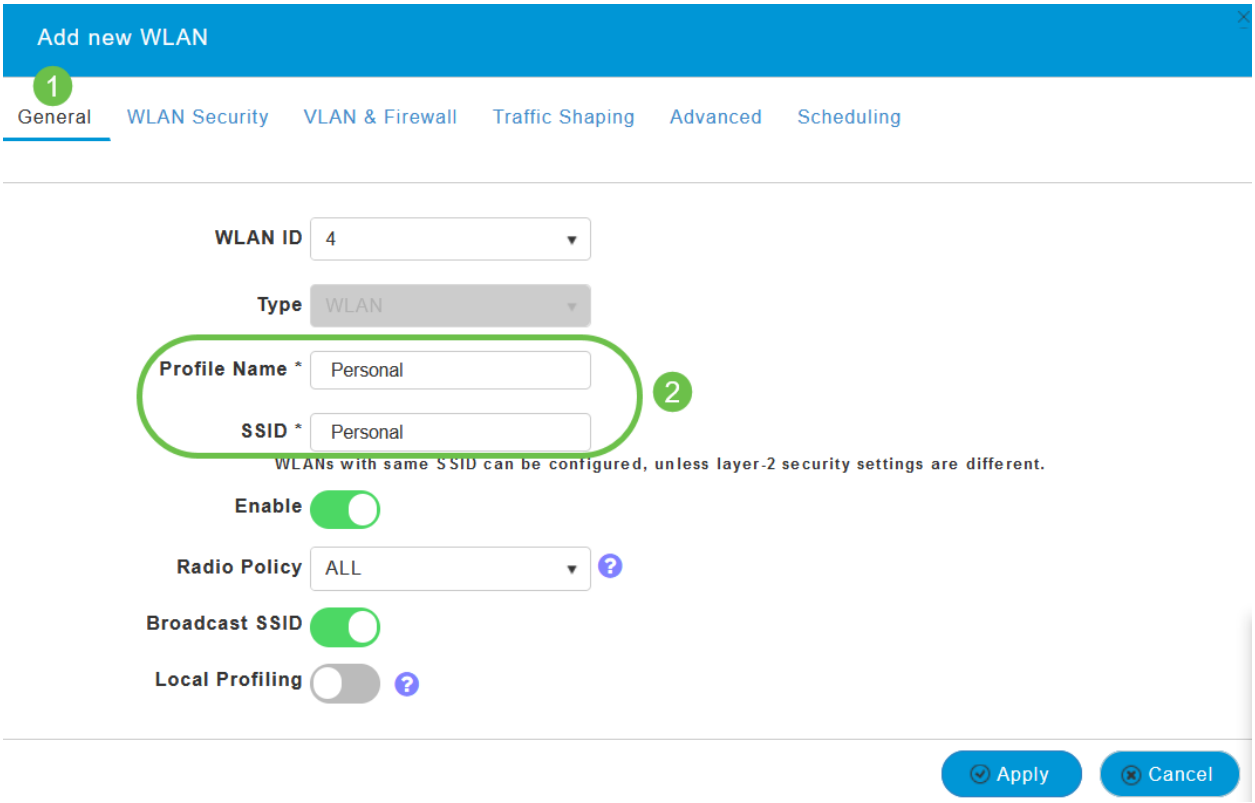
Passaggio 2

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



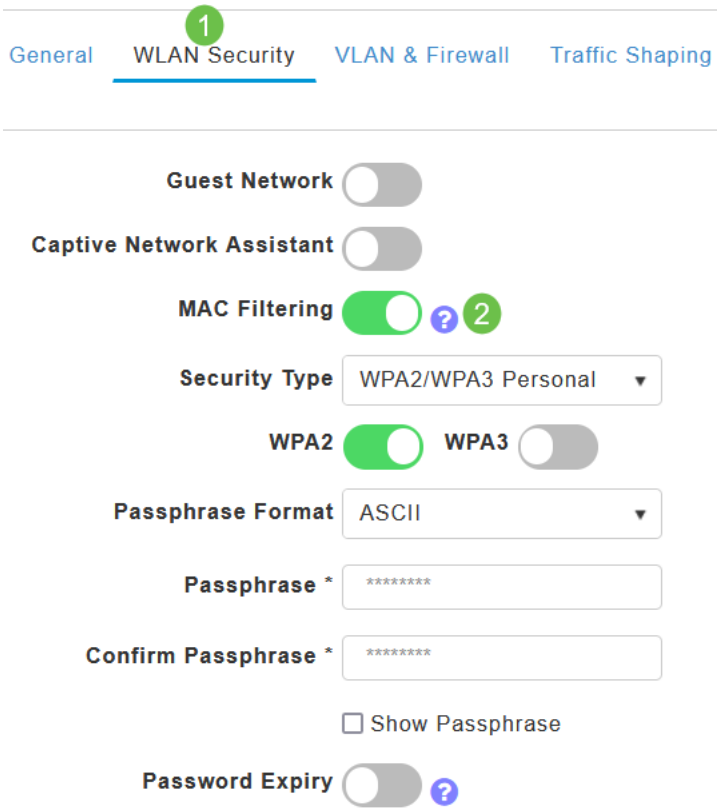
Passaggio 3

Nella scheda *General*, immettere il *nome* del *profilo* della WLAN.



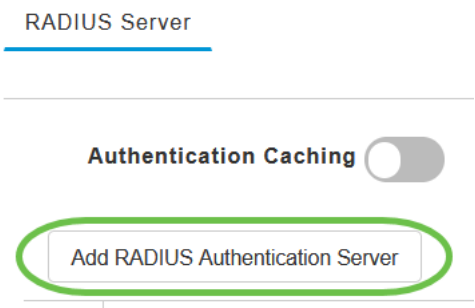
Passaggio 4

Passare alla scheda **Sicurezza WLAN** e abilitare il **filtro MAC** facendo scorrere l'interruttore.



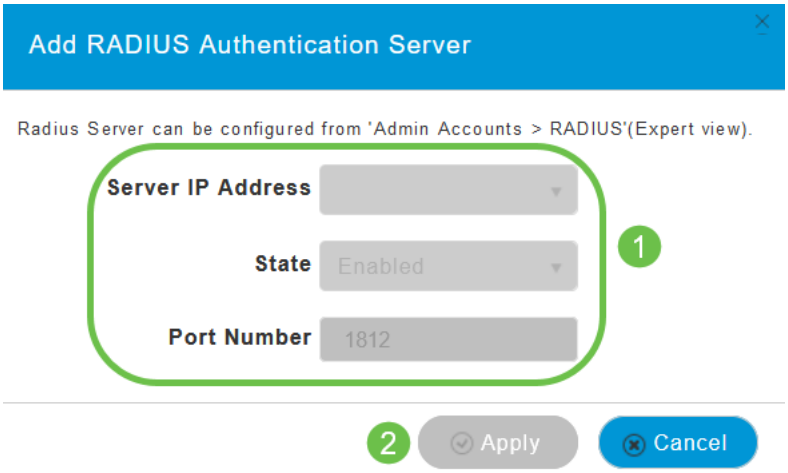
Passaggio 5

Fare clic su **Add RADIUS Authentication Server** (Aggiungi server di autenticazione RADIUS) per aggiungere il server RADIUS configurato nella sezione precedente per fornire l'autenticazione per la WLAN.



Passaggio 6

Viene visualizzata una finestra popup. Immettere l'*indirizzo IP, lo stato e il numero di porta del server*. Fare clic su **Apply** (Applica).

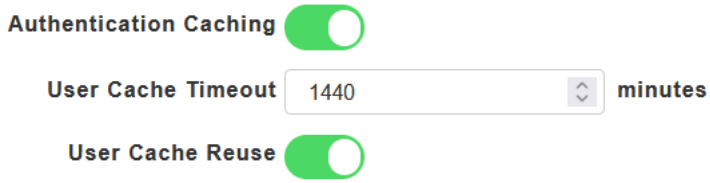


Passaggio 7

(Facoltativo)

Abilita *memorizzazione nella cache di autenticazione*. Quando si attiva questa opzione, vengono visualizzati i campi seguenti.

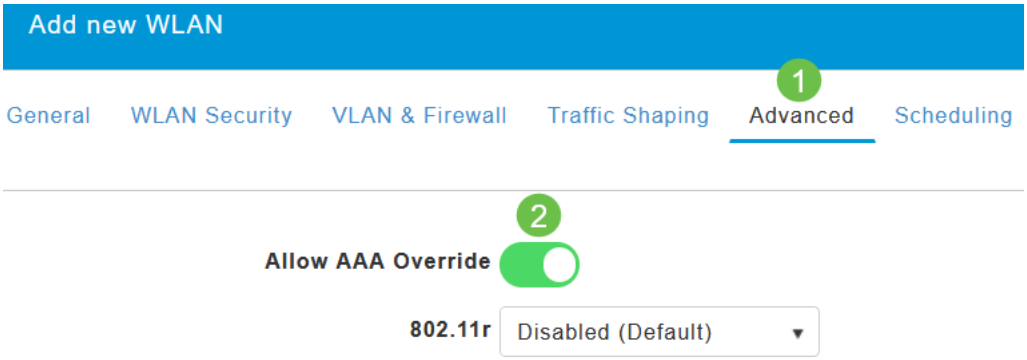
- *Timeout cache utente:* specifica il periodo di tempo in cui scadono le credenziali autenticate nella cache.
- *Riutilizzo cache utente*: utilizzare le informazioni della cache delle credenziali prima del timeout della cache. Per impostazione predefinita, questa è disattivato.



Se questa funzionalità è abilitata, un client che è già stato autenticato su questo server non dovrà passare i dati al server RADIUS quando si riconnetterà a questa WLAN entro le prossime 24 ore.

Passaggio 8

Passare alla scheda Avanzate. Abilitare l'opzione **Consenti sostituzione AAA** facendo scorrere l'interruttore.

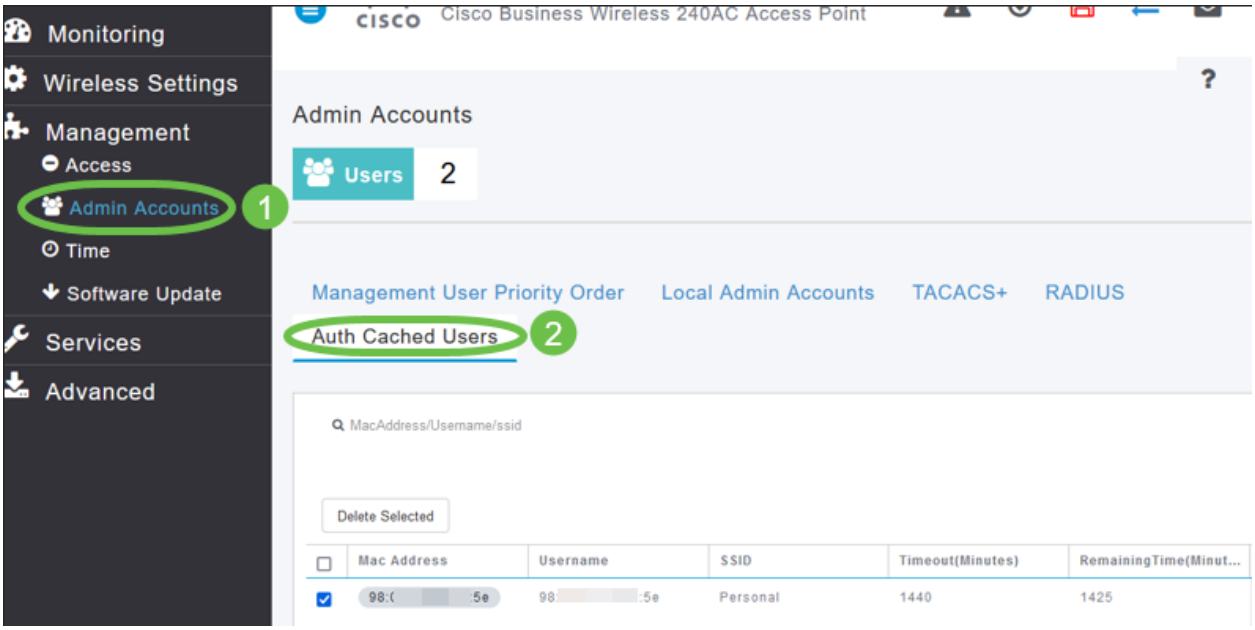


La scheda *Avanzate* sarà visibile solo in *Expert View*.

Fasi successive

Dopo aver configurato le impostazioni sull'access point CBW e configurato il server RADIUS, dovrebbe essere possibile connettere il dispositivo. Immettere la chiave PSK personalizzata configurata per l'indirizzo MAC e verrà aggiunta alla rete.

Se è stata configurata la memorizzazione nella cache di autenticazione, è possibile visualizzare i dispositivi che sono stati collegati alla WLAN andando alla scheda *Auth Cached Users* in *Admin Accounts*. Se necessario, è possibile eliminare questa voce.



Conclusioni

Ecco qua! È ora possibile usufruire dei vantaggi della funzione PSK personale sull'access point CBW.