Configurazione della tabella delle istanze di accesso guest nel punto di accesso WAP125

Obiettivo

La funzionalità Guest Access del punto di accesso WAP125 fornisce connettività wireless ai client wireless temporanei entro la portata del dispositivo. Il punto di accesso trasmette due SSID (Service Set Identifier) diversi: uno per la rete principale e l'altro per la rete guest. Gli ospiti vengono quindi reindirizzati a un Portale vincolato in cui è necessario immettere le credenziali. In questo modo, infatti, la rete principale rimane protetta e gli ospiti possono accedere a Internet.

Le impostazioni di Captive Portal, ad esempio il timeout della sessione e l'URL (Uniform Resource Locator) di reindirizzamento, vengono configurate nella tabella delle istanze di accesso guest dell'utility basata sul Web di WAP125. La funzione di accesso guest è stata particolarmente utile nelle hall di hotel e uffici, ristoranti e centri commerciali.

In questo articolo viene illustrato come configurare la tabella delle istanze di accesso guest del punto di accesso WAP125. Si presuppone che le impostazioni per le tabelle locali del portale Web e del gruppo di guest siano già configurate. Per istruzioni su come configurare entrambe le impostazioni, fare clic qui.

Dispositivi interessati

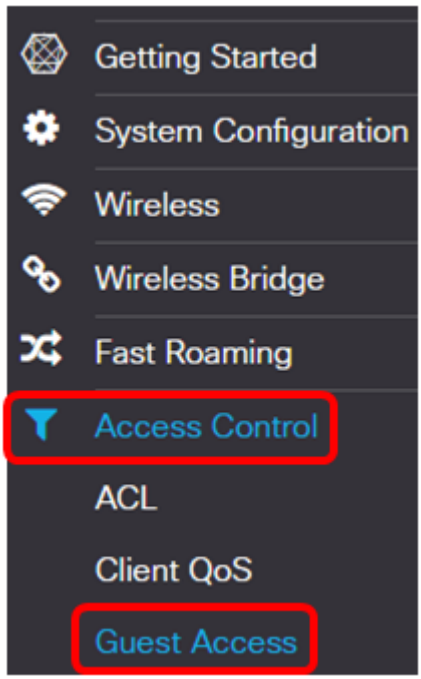
- WAP125

Versione del software

- 1.0.0.4 - WAP581
- 1.0.0.5 — WAP125

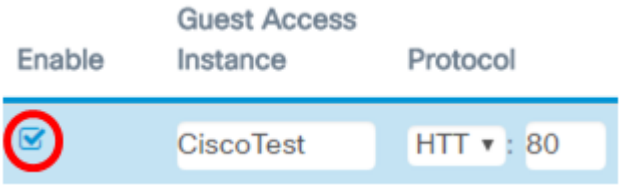
Configura tabella istanza di accesso guest

Passaggio 1. Accedere all'utility basata sul Web di WAP125 e scegliere **Controllo accesso > Accesso guest**.

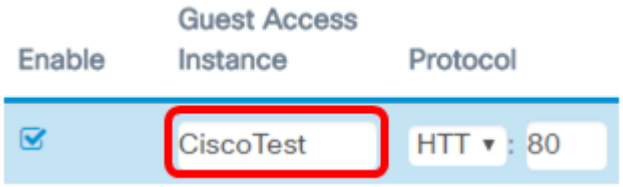


Nota: Le immagini in questo articolo sono prese da WAP125. Le opzioni di menu possono variare a seconda del modello del dispositivo.

Passaggio 2. Verificare che la casella di controllo **Abilita** istanza di accesso guest sia selezionata per assicurarsi che Accesso guest sia attivo.



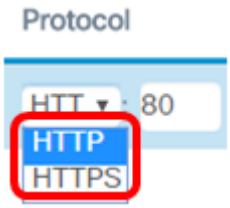
Passaggio 3. Immettere un nome per l'istanza nel campo *Istanza di accesso guest*. Può contenere fino a 32 caratteri alfanumerici.



Nota: Nell'esempio, viene immesso CiscoTest.

Passaggio 4. Scegliere un protocollo per l'istanza di accesso guest. Le opzioni sono:

- HTTP: questa opzione è nota anche come HTTP (HyperText Transfer Protocol). Non fornisce la crittografia durante la verifica della pagina Web richiesta.
- HTTPS — questa opzione è nota anche come HTTPS (HyperText Transfer Protocol Secure). Ciò significa che tutte le comunicazioni tra il computer e il sito Web che sta contattando sono crittografate.



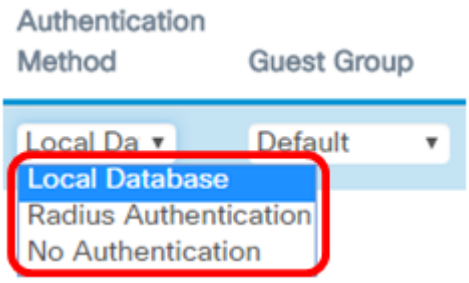
Nota: Nell'esempio viene scelto HTTP.

Passaggio 5. Inserire un numero di porta accanto al campo Protocollo. Il numero di porta consente di identificare il protocollo quando raggiunge un server.

Nota: nell'esempio, viene immesso 80.

Passaggio 6. Scegliere un metodo di autenticazione dall'elenco a discesa Metodo di autenticazione. Verrà utilizzato dal punto di accesso quando i client eseguiranno l'autenticazione tramite il portale vincolato. Le opzioni sono:

- Database locale - Questa opzione consente al dispositivo WAP di verificare le credenziali dell'utente da un file archiviato localmente. Se si sceglie questa opzione, completare i passaggi da 7 a 10 e quindi configurare la tabella del gruppo guest.
- Autenticazione RADIUS: questa opzione consente al punto di accesso di verificare gli utenti tramite un server RADIUS (Remote Authentication Dial-In User Service). Se si sceglie questa opzione, completare i passaggi da 7 a 10 e quindi configurare l' autenticazione RADIUS.
- Nessuna autenticazione: questa opzione disabilita l'autenticazione e consente ai client wireless di connettersi alla rete guest senza immettere le credenziali. Se si sceglie questa opzione, andare al passaggio 11.

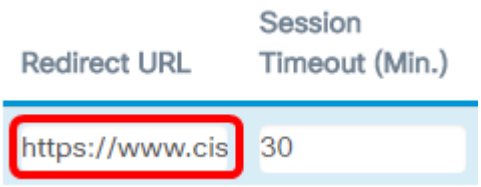


Nota: In questo esempio viene scelto Database locale.

Passaggio 7. Scegliere un gruppo dall'elenco a discesa Gruppo guest.

Nota: In questo esempio viene selezionato automaticamente Predefinito.

Passaggio 8. Inserire l'indirizzo da reindirizzare dopo aver immesso le credenziali nel campo *Redirect URL*.

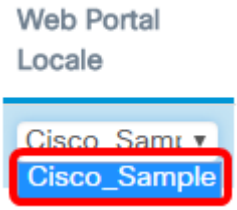


Nota: L'indirizzo deve iniziare con HTTP o HTTPS. Nell'esempio viene immesso https://www.cisco.com.

Passaggio 9. Immettere il numero di minuti prima del timeout di una sessione nel campo *Timeout sessione (min)*.

Nota: nell'esempio, viene immesso 30.

Passaggio 10. Scegliere un profilo di portale Web dall'elenco a discesa Impostazioni internazionali del portale Web.



Nota: Nell'esempio, Cisco_Sample viene scelto automaticamente. Per istruzioni su come configurare le impostazioni locali del portale Web, fare clic qui.

È ora necessario configurare la tabella delle istanze di accesso guest.

Configura tabella gruppo guest

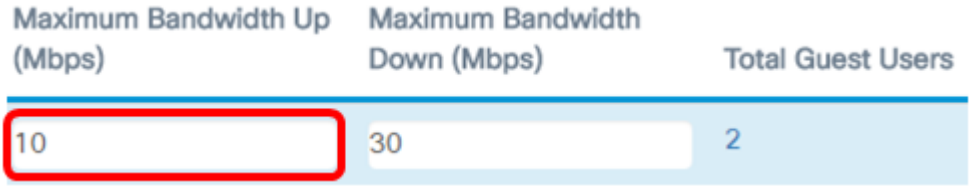
Passaggio 7. Inserire un nome per il gruppo di ospiti nel campo *Nome gruppo di ospiti*. Il nome del gruppo di ospiti può avere una lunghezza massima di 32 caratteri.

Nota: Nell'esempio, viene immesso CiscoGuests.

Passaggio 8. Immettere il numero di minuti prima del timeout del prompt nel campo *Timeout di inattività (min)*.

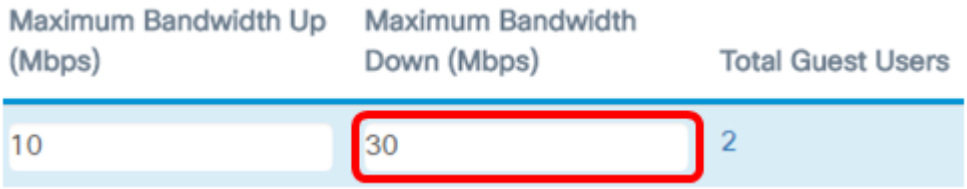
Nota: Nell'esempio viene immesso 5.

Passaggio 9. Immettere la velocità massima di caricamento nel campo *Aumento larghezza di banda massima (Mbps)*. Si tratta della larghezza di banda massima, in Mbps, che un client wireless può inviare quando utilizza il Captive Portal. La larghezza di banda massima può essere compresa tra 0 e 300, dove 0 è il valore predefinito.



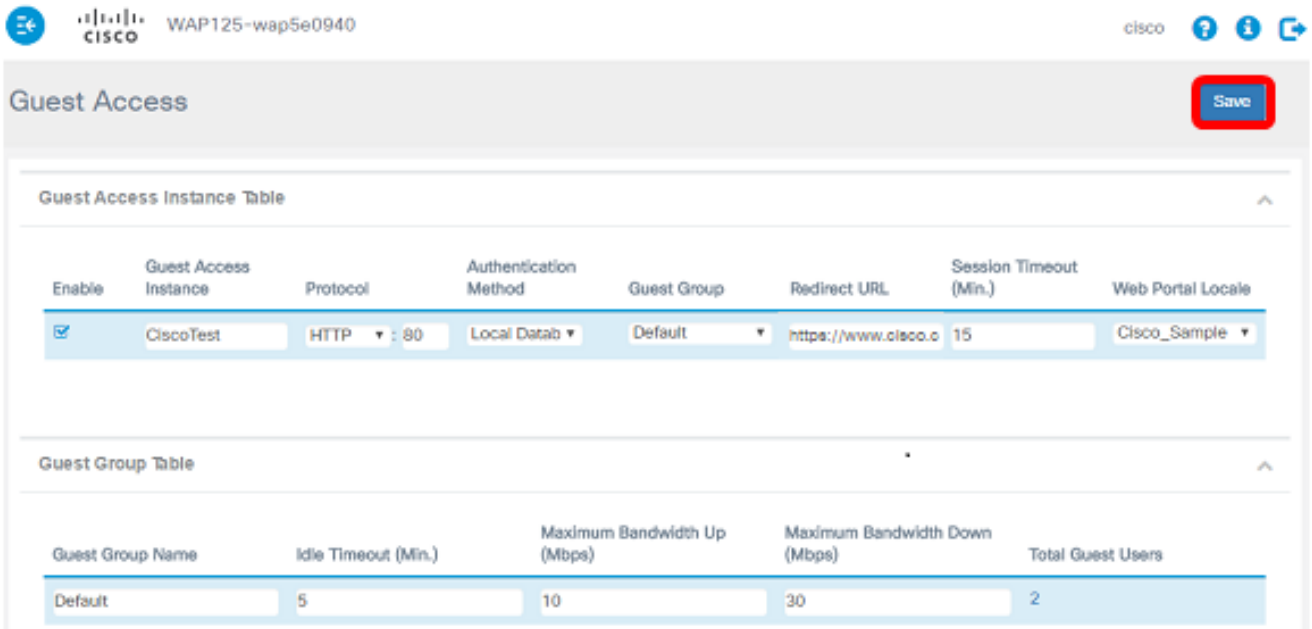
Nota: Nell'esempio, viene immesso 10.

Passaggio 10. Immettere la velocità massima di download nel campo *Maximum Bandwidth Down (Mbps)* . Si tratta della larghezza di banda massima, in Mbps, che un client wireless può ricevere quando utilizza il Captive Portal. La larghezza di banda massima può essere compresa tra 0 e 300, dove 0 è il valore predefinito.



Nota: nell'esempio, viene immesso 30.

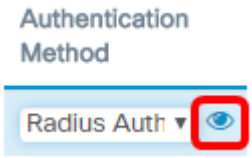
Passaggio 11. Fare clic su **Salva**.



La tabella dell'istanza di accesso guest deve essere ora configurata con Autenticazione database locale.

Autenticazione RADIUS

Passaggio 1. Fare clic sul pulsante Visualizza.

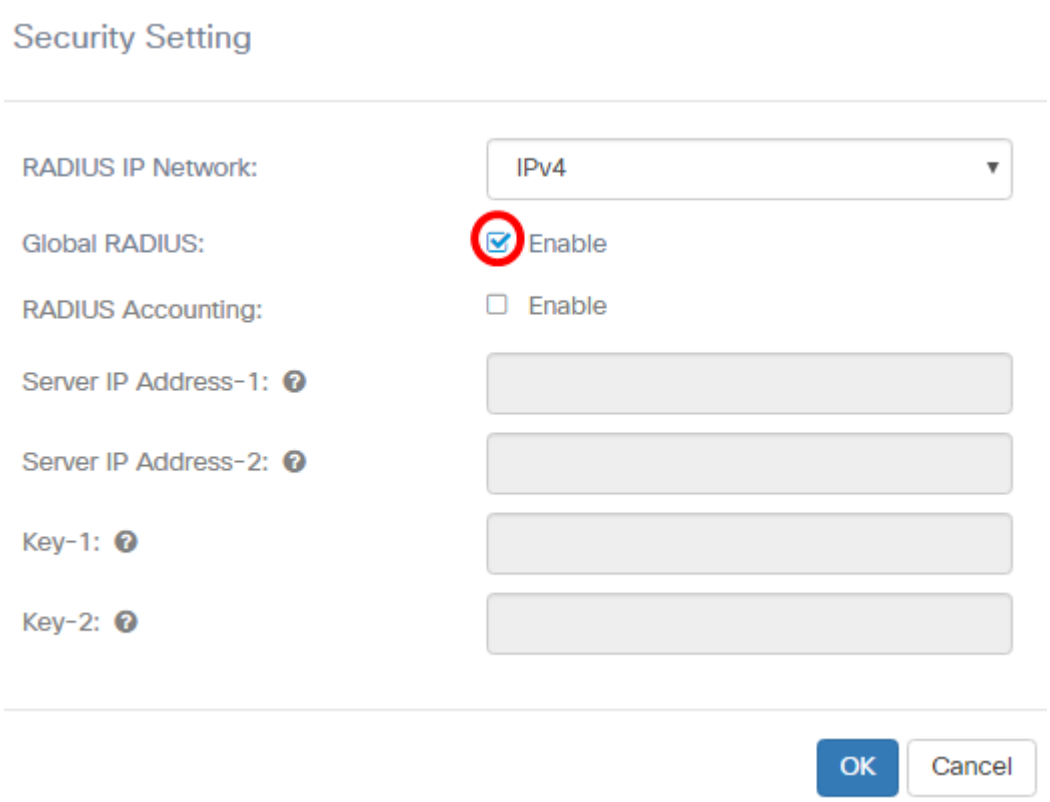


Passaggio 2. Nella finestra popup Security Setting (Impostazioni di sicurezza), selezionare la rete RADIUS IP dall'elenco a discesa RADIUS IP Network (Rete RADIUS IP). Le opzioni sono:

- IPv4: questa opzione è il tipo di indirizzamento IP più comunemente utilizzato in una rete. Utilizza un formato a 32 bit per identificare gli host su una rete.
- IPv6 — Questa opzione è lo standard di indirizzi IP di nuova generazione destinato a sostituire il formato IPv4. Il protocollo IPv6 risolve il problema della scarsità di indirizzi con l'utilizzo di un sistema di indirizzamento a 128 bit anziché a 32 bit utilizzato nel protocollo IPv4.

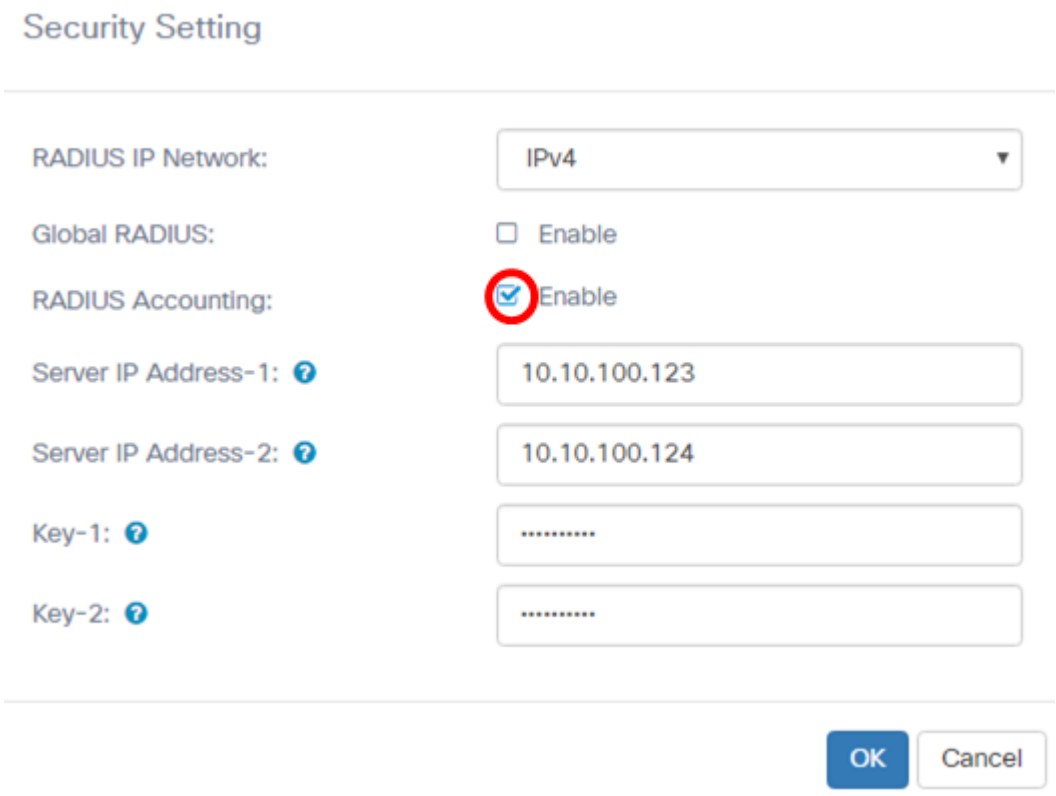
Nota: Nell'esempio, è stato scelto IPv4.

Passaggio 3. (Facoltativo) Selezionare la casella di controllo **Abilita** RADIUS globale per consentire al portale vincolato di utilizzare un set diverso di server RADIUS.

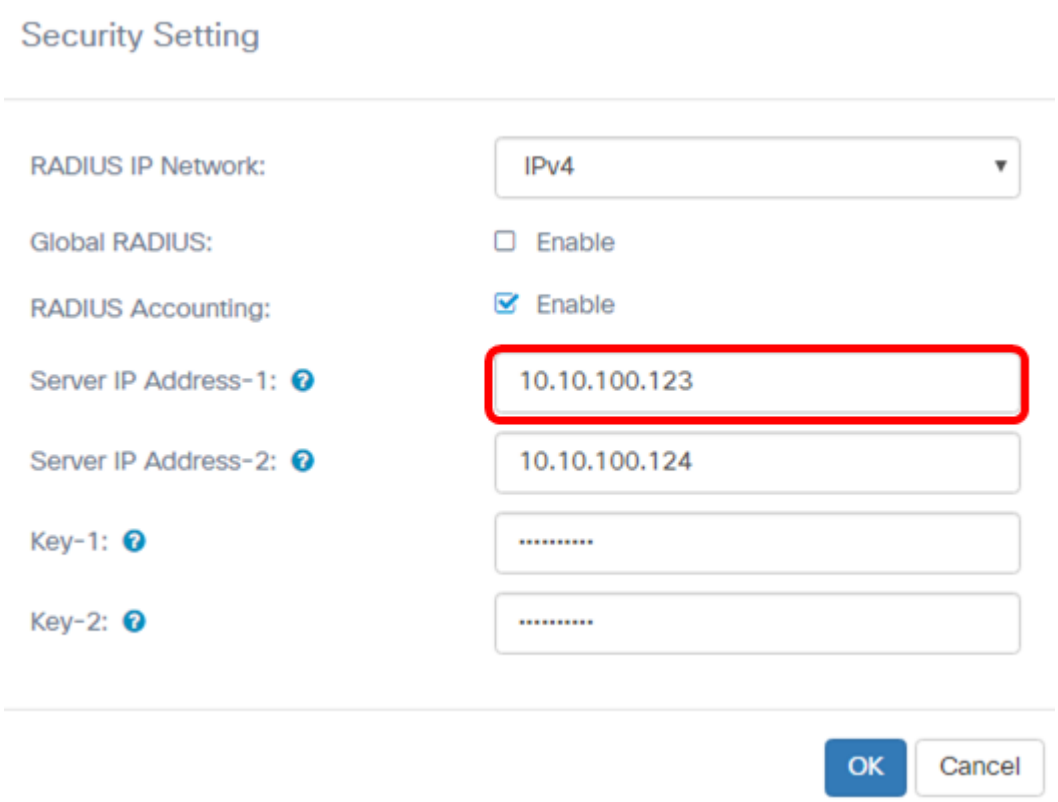


Nota: Quando è attivata, non è necessario configurare altre configurazioni per l'area Impostazioni protezione. Procedere al passo 9. In questo esempio, Global RADIUS è abilitato.

Passaggio 4. (Facoltativo) Selezionare la casella di controllo **Abilita** accounting RADIUS per consentire al punto di accesso di tenere traccia e misurare le risorse utilizzate da un utente specifico, ad esempio il tempo di sistema e la quantità di dati trasmessi e ricevuti.

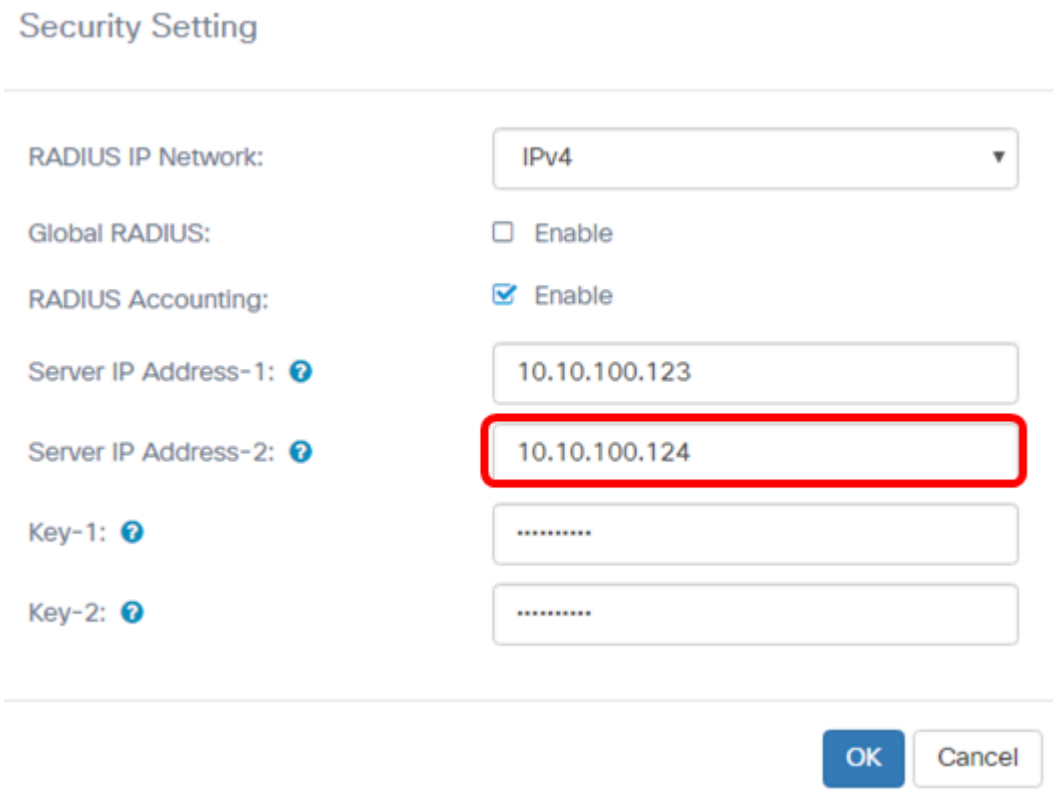


Passaggio 5. (Facoltativo) Immettere l'indirizzo IPv4 o IPv6 del server RADIUS primario nel campo *Indirizzo IP server-1*.



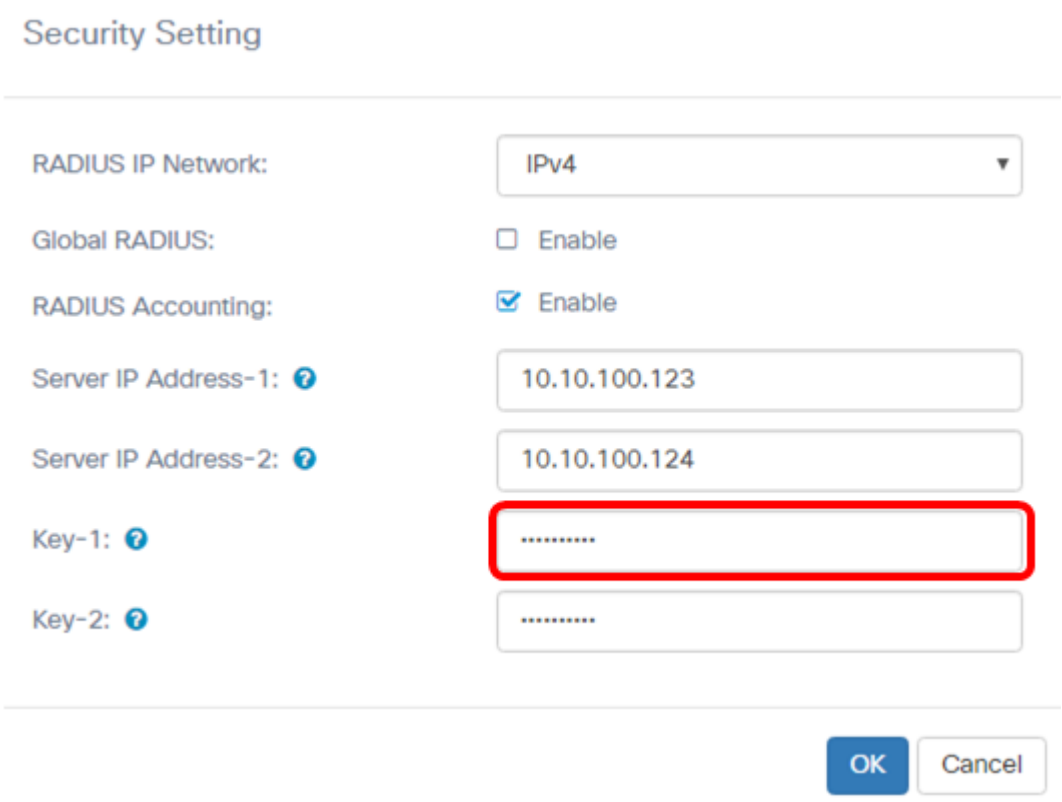
Nota: Nell'esempio, viene immesso 10.10.100.123.

Passaggio 6. (Facoltativo) Immettere l'indirizzo IPv4 o IPv6 del server RADIUS di backup nel campo *Indirizzo IP server-2*.

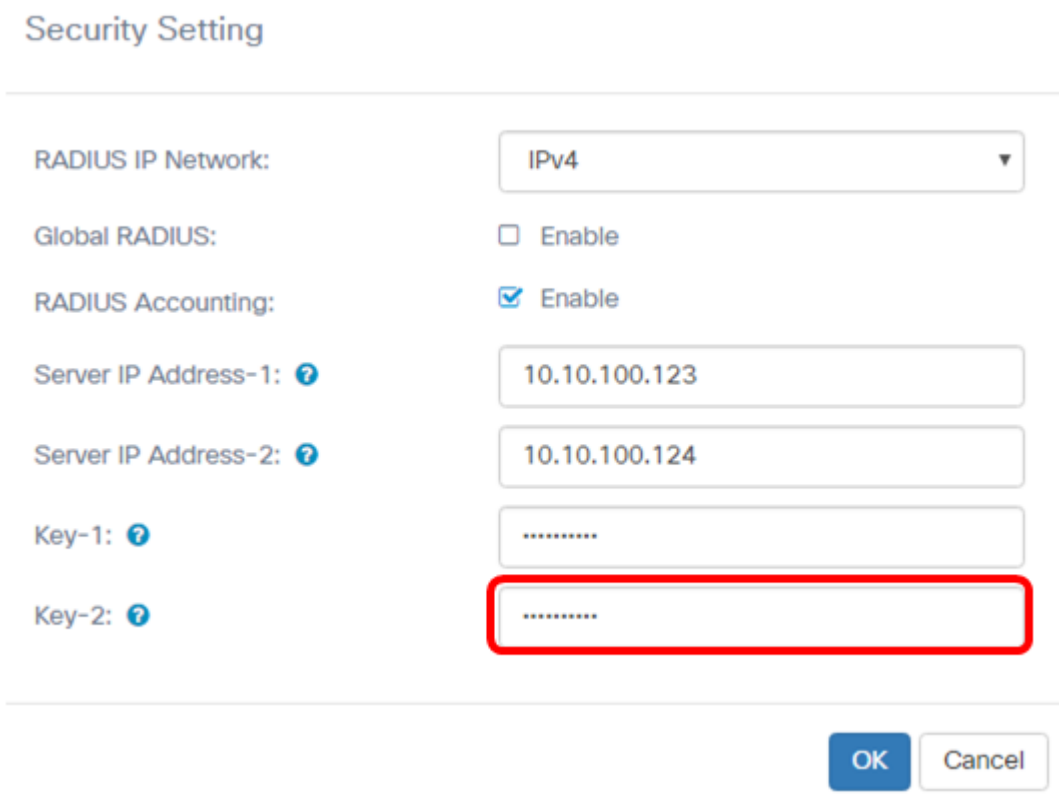


Nota: nell'esempio, viene immesso 10.10.100.124.

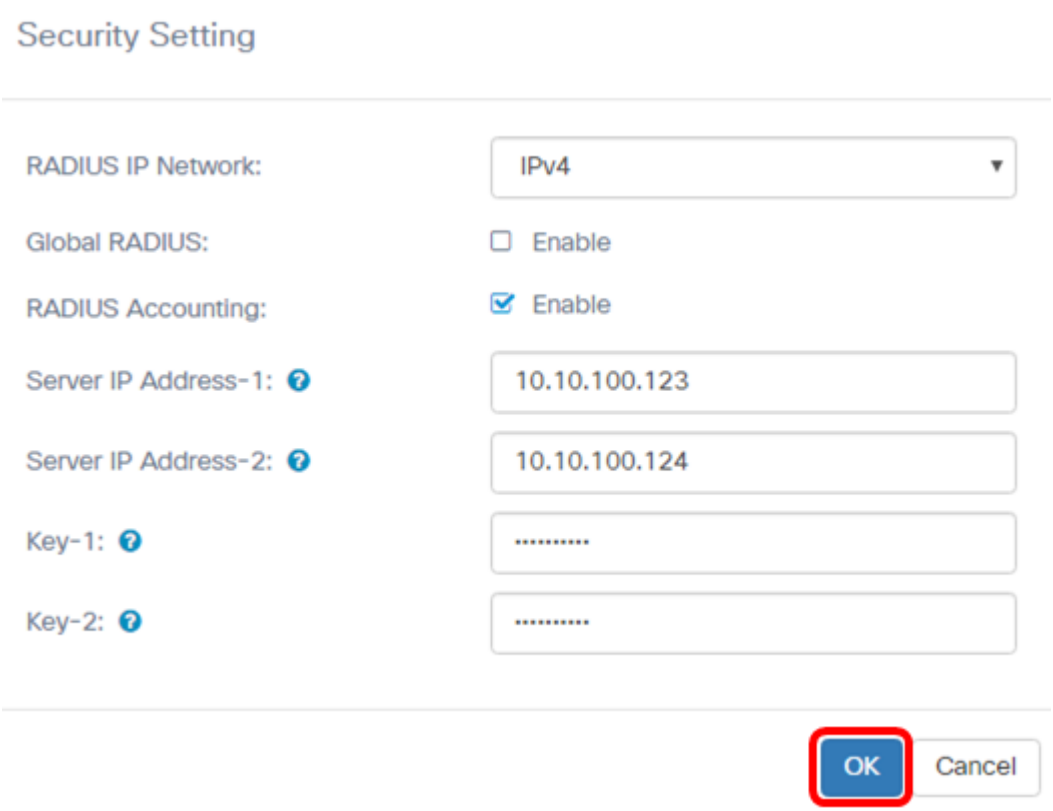
Passaggio 7. (Facoltativo) Immettere la password utilizzata dal punto di accesso per autenticare il server RADIUS primario nel campo *Chiave-1*. La voce di questo campo fa distinzione tra maiuscole e minuscole e deve corrispondere alla voce configurata nel server RADIUS primario. La chiave può contenere un massimo di 63 caratteri alfanumerici.



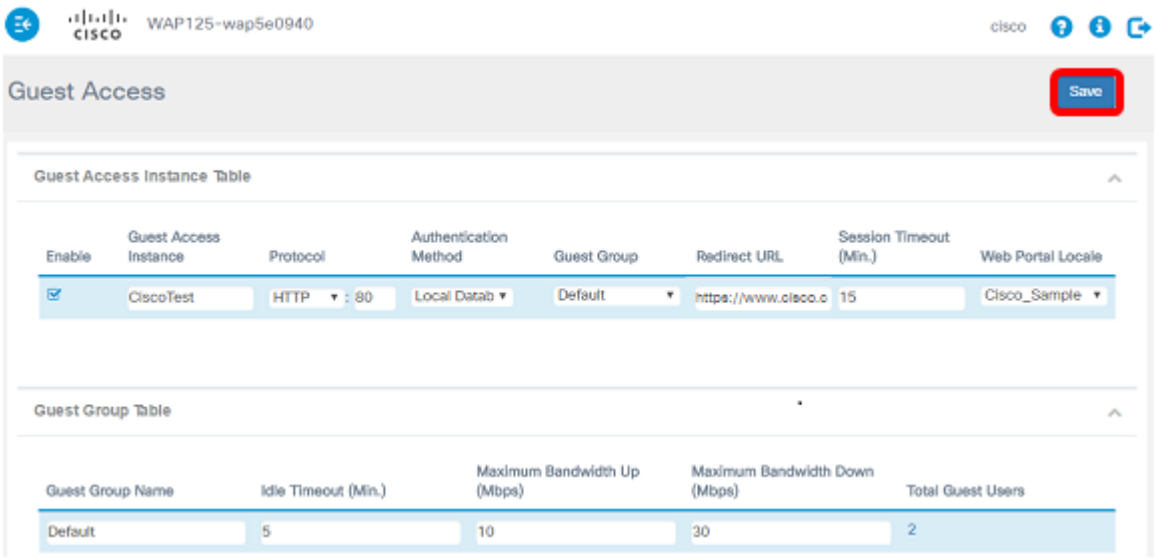
Passaggio 8. (Facoltativo) Immettere la password utilizzata dal punto di accesso per autenticare il server RADIUS secondario nel campo *Chiave-2*. La voce di questo campo fa distinzione tra maiuscole e minuscole e deve corrispondere alla voce configurata nel server RADIUS primario. La chiave può contenere un massimo di 63 caratteri alfanumerici.



Passaggio 9. Fare clic su **OK**.



Passaggio 10. Fare clic su **Salva**.



La tabella Istanza di accesso guest deve essere ora configurata con il metodo di autenticazione RADIUS.