WAP125 アクセス ポイントの設定ゲスト アクセス例表

目標

WAP125 アクセス ポイントのゲスト アクセス機能はデバイスの範囲内の一時無線クライアントにワイヤレス接続を提供します。 それはアクセス ポイント ブロードキャスト 2 異なるサービス セット ID （SSID）を持っていることによってはたらきます: ゲスト ネットワークの主要なネットワークのための 1 つ、および他。 ゲストは資格情報を入力するために必要となる捕虜ポータルにそれからリダイレクトされます。 事実上、これはまだゲストにインターネットへのアクセスを可能にしている間主要なネットワークをセキュア保存します。

セッション タイムアウトおよびリダイレクト Uniform Resource Locator （URL）のような捕虜ポータルの設定は WAP125 の Webベース ユーティリティのゲスト アクセス例表で行われます。 ゲスト アクセス機能はホテルおよびオフィス ロビー、レストランおよびずっとモールで特に役立ちます。

この技術情報は WAP125 アクセス ポイントのゲスト アクセス例表を設定する方法を示すことを向けます。 ウェブ ポータル ロケール表およびゲスト グループ表の設定が既に行われていると仮定します。 両方の設定を行うことの手順に関しては、ここをクリックして下さい。

適当なデバイス

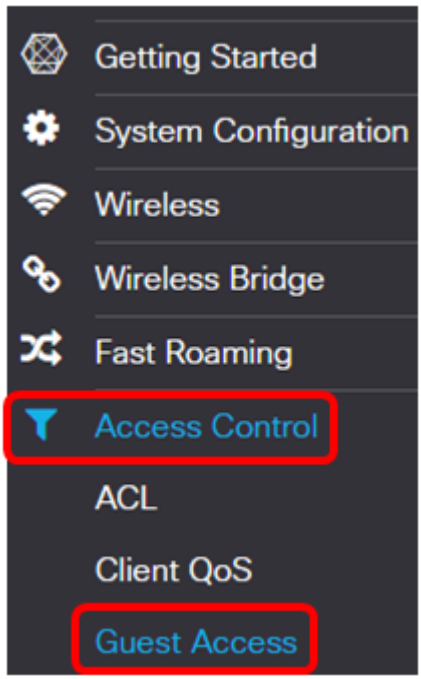
- WAP125

[Software Version]

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

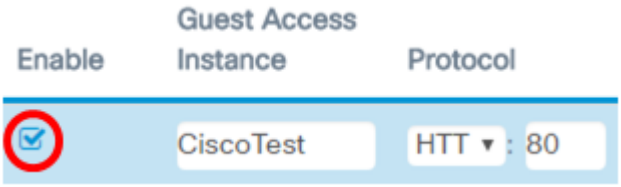
設定ゲスト アクセス例表

ステップ 1. WAP125 の Webベース ユーティリティへのログインは**アクセスコントロール > ゲスト アクセス**を選択し。

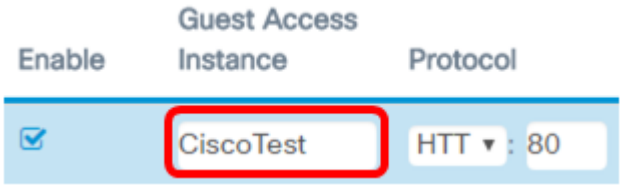


注: この技術情報のイメージは WAP125 から撮られます。 メニュー オプションはデバイスのモデルによって変わるかもしれません。

ステップ 2.ゲスト アクセスがアクティブであることを確認するためにゲスト アクセス例 **Enable チェックボックスが**チェックされることを確認して下さい。



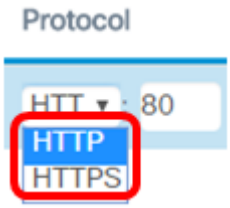
ステップ 3.*ゲスト アクセス インスタンス フィールド*で例の名前を入力して下さい。 これは 32 までの英数字である場合もあります。



注: この例では、CiscoTest は入ります。

ステップ 4.ゲスト アクセス例のためのプロトコルを選択して下さい。 次のオプションがあります。

- HTTP： このオプションは別名ハイパーテキスト転送プロトコル（HTTP）です。 それは要求された Web ページの確認の間に暗号化を提供しません。
- HTTPS — このオプションは別名 Hypertext Transfer Protocol（HTTP）セキュアです（HTTPS）。 これはによって暗号化される接触している Webサイトとコンピュータ間のすべての通信ことを意味します。



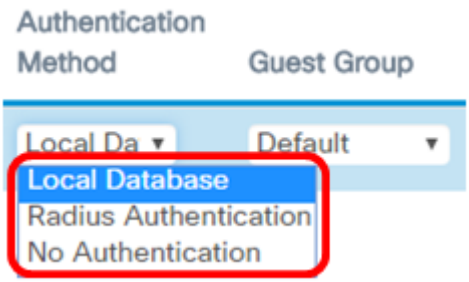
注: この例では、HTTP は選択されます。

ステップ 5. Protocol フィールドの側のポート番号を入力して下さい。 ポート番号ヘルプはそれがサーバに達するときプロトコルを確認します。

注: この例では、80 は入ります。

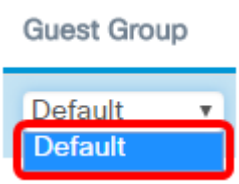
ステップ 6.認証方式 ドロップダウン リストから認証方式を選択して下さい。 これはアクセス ポイント時捕虜ポータルを通したクライアント認証する使用されます。 次のオプションがあります。

- ローカルは database —このオプション WAP デバイスがローカルで保存されるファイルからのユーザの資格情報を確認するようにします。 このオプションが選択される場合、ステップ 7 からステップ 10 に終え、次にゲスト グループ表を設定することを続行して下さい。
- RADIUS認証—このオプションはアクセス ポイントがリモート認証ダイヤルイン ユーザ サービス (RADIUS) サーバによってユーザを確認するようにします。 このオプションが選択される場合、ステップ 7 からステップ 10 に終え、次に RADIUS認証を設定することを続行して下さい。
- 認証無し—このオプションは認証を無効に し、無線クライアントが資格情報を入力しないでゲスト ネットワークに接続するようにします。 このオプションが選択される場合、ステップ 11.にスキップして下さい。



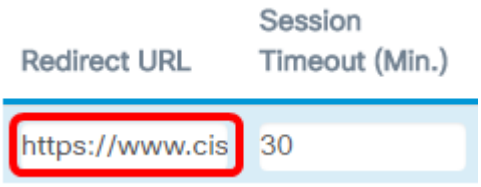
注: この例では、ローカル データベースは選択されます。

ステップ 7.ゲスト グループ ドロップダウン リストからグループを選択して下さい。



注: この例では、デフォルトは自動的に選択されます。

ステップ 8.*リダイレクト URL フィールド*の資格情報を入力した後リダイレクトされるべきアドレスを入力して下さい。

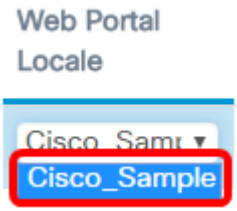


注: アドレスは HTTP か HTTPS から開始する必要があります。 この例では、https://www.cisco.com は入ります。

ステップ 9.*セッション タイムアウト (最少)* フィールドでの前に分の数をセッションタイム入力して下さい。

注: この例では、30 は入ります。

ステップ 10.ウェブ ポータル ロケール ドロップダウン リストからウェブ ポータル プロファイルを選択して下さい。



注: この例では、Cisco_Sample は自動的に選択されます。 ウェブ ポータル ロケールを設定する方法に関する説明に関してはここをクリックして下さい。

ゲスト アクセス例表は今設定する必要があります。

設定ゲスト グループ表

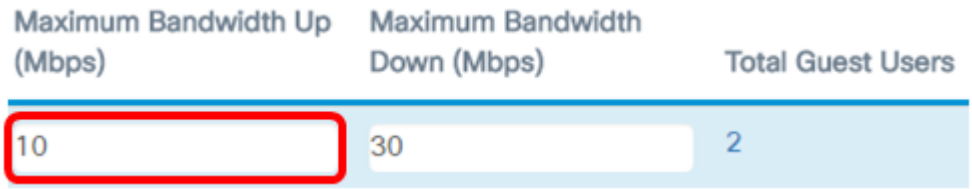
ステップ 7.ゲスト *Group Name フィールド*でゲスト グループの名前を入力して下さい。 ゲスト グループ名は長く 32 文字までである場合もあります。

注: この例では、CiscoGuests は入ります。

ステップ 8.*アイドル状態のタイムアウト (最少)* フィールドで敏速な時の前に分の数を入力して下さい。

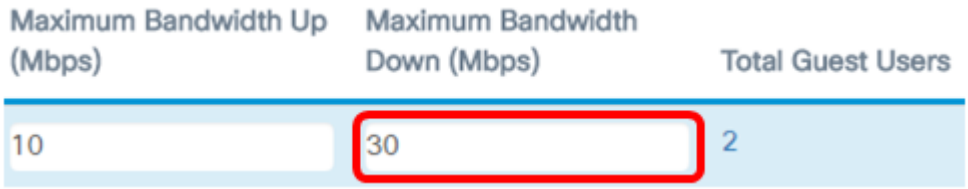
注: この例では、5 つは入ります。

ステップ 9.*最大帯域幅アップ (Mbps)* フィールドで最大アップロード速度を入力して下さい。 これは最大帯域幅、送信 無線クライアントができる Mbps でです、捕虜ポータルを使用するとき。 最大帯域幅は 0 がデフォルト値であるところに 0 から 300 からのどれである場合もあります。



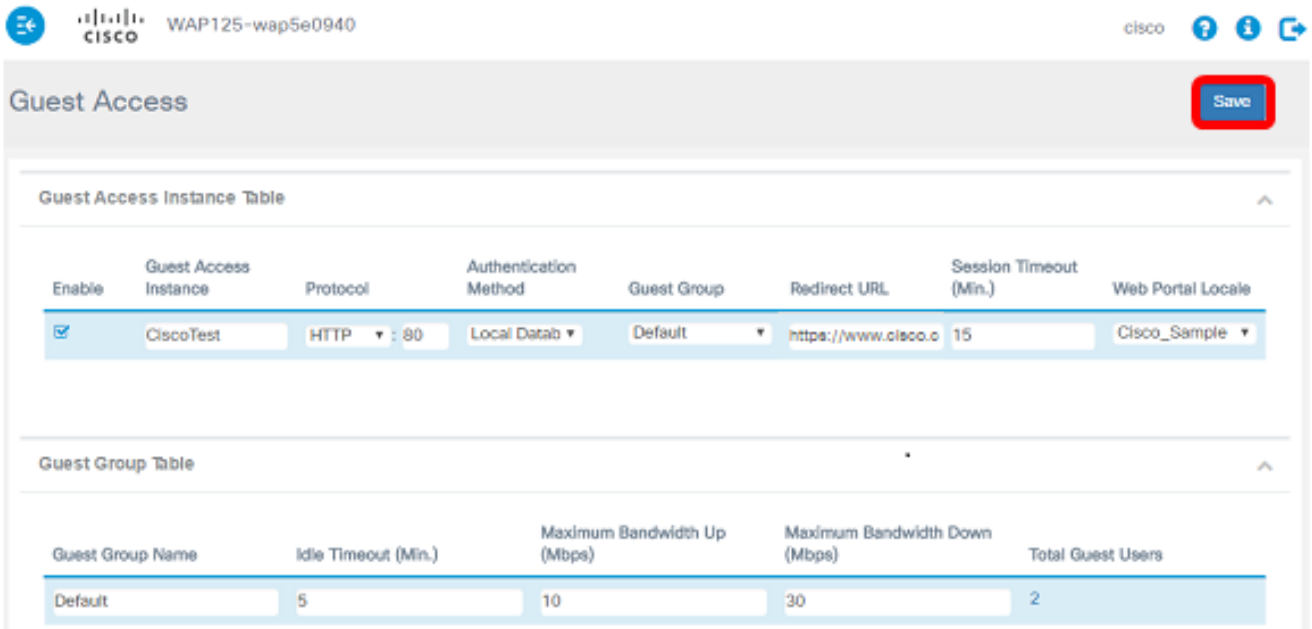
注: この例では、10 は入ります。

ステップ 10.*最大帯域幅 (Mbps)* フィールドで最大ダウンロード速度を入力して下さい。 これは最大帯域幅、受け取る無線クライアントがことができる Mbps でです、捕虜ポータルを使用するとき。 最大帯域幅は 0 がデフォルト値であるところに 0 から 300 からのどれである場合もあります。



注: この例では、30 は入ります。

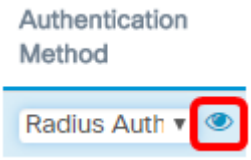
ステップ 11. 『SAVE』 をクリック して下さい。



ゲスト アクセス例表はローカル データベース認証で今設定する必要があります。

RADIUS 認証

ステップ 1. View ボタンをクリックして下さい。

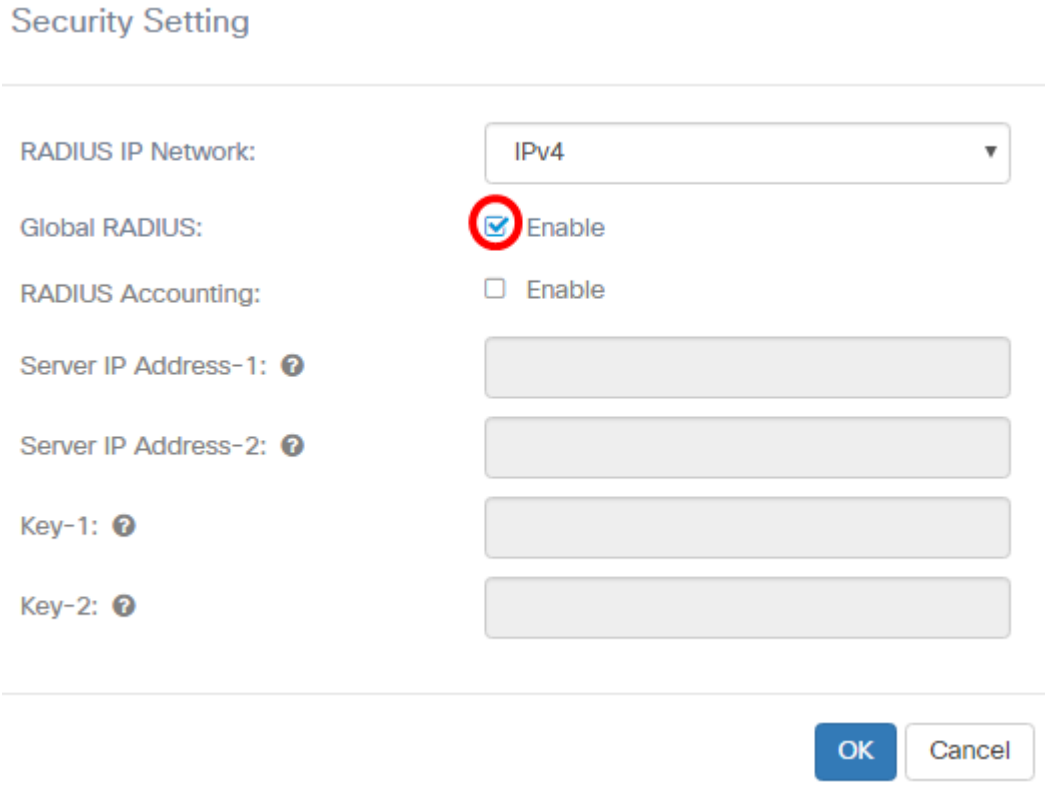


呼び出します。 セキュリティ設定ポップアップ ウィンドウで、RADIUS IP ネットワーク ドロップダウン リストから半径 IP ネットワークを選択して下さい。 次のオプションがあります。

- IPv4 —このオプションはネットワークの IP アドレッシングの最も広く使われた形式です。 それはネットワークのホストを識別するのに 32ビット形式を使用します。
- IPv6 —このオプションは IPv4 形式を取り替えるように意図されている次世代 IP アドレス規格です。 IPv6 は IPv4 で使用される 32ビットの代りに 128 ビット アドレス 指定方式の使用におけるアドレス欠乏問題を解決します。

注: この例では、IPv4 は選択されます。

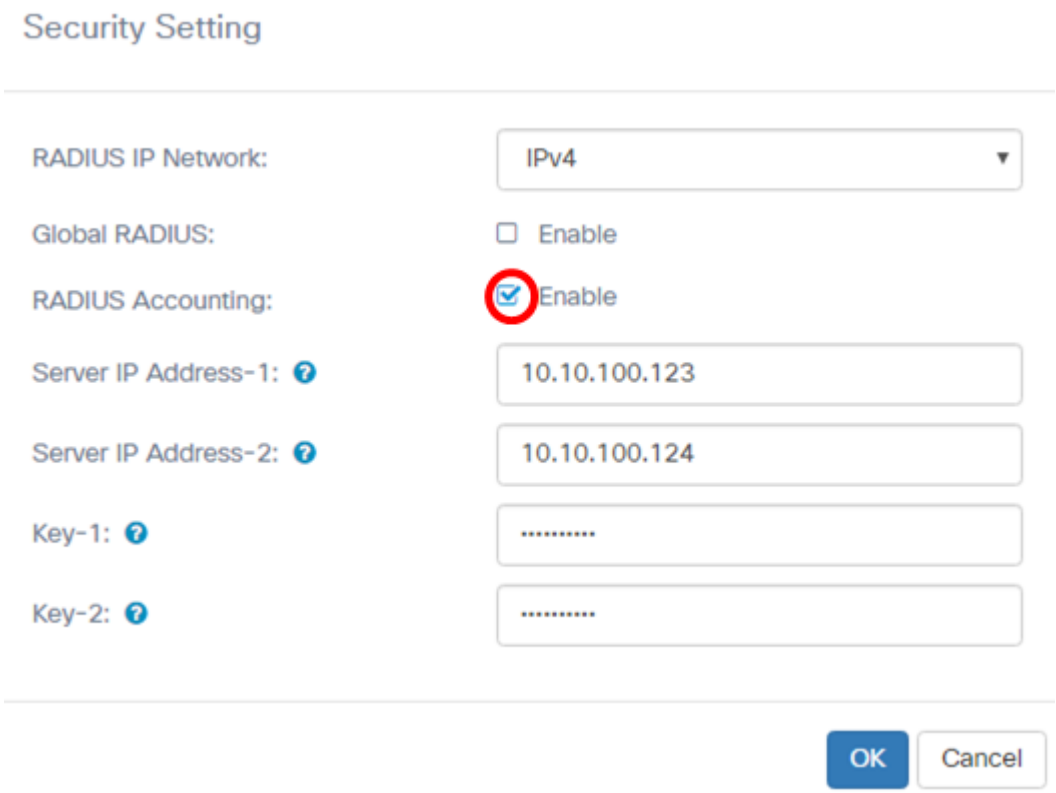
ステップ 3. (オプションの) チェック捕虜門脈使用を許可するグローバル な Radius enable チェックボックス別の一組の RADIUSサーバ。



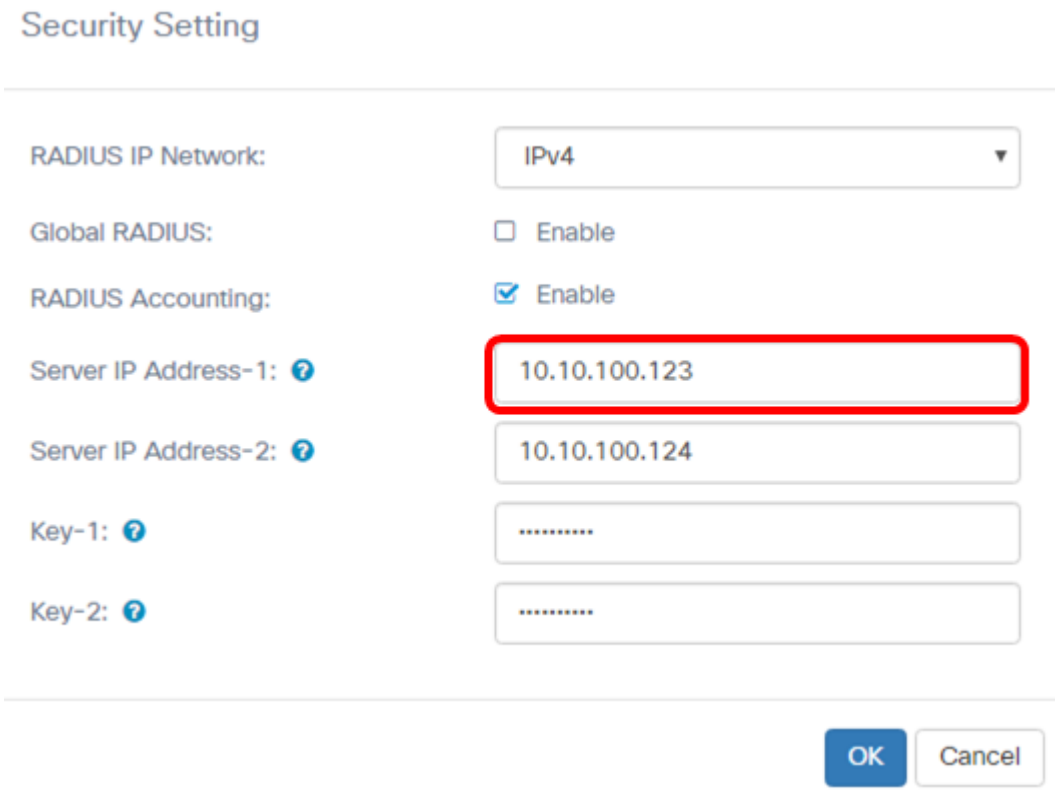
注: 有効に されたとき、セキュリティ設定エリアのための他の設定は設定される必要がありません。 ステップ 9.に進んで下さい。 この例では、グローバル な RADIUS は有効に なり

ます。

ステップ 4.（オプションの）チェック特定のユーザが消費したデータのシステムの時刻および送受信される量のようなリソースを、トラッキングし、測定するようにアクセス ポイントがする RADIUS 説明 **Enable チェックボックス**。

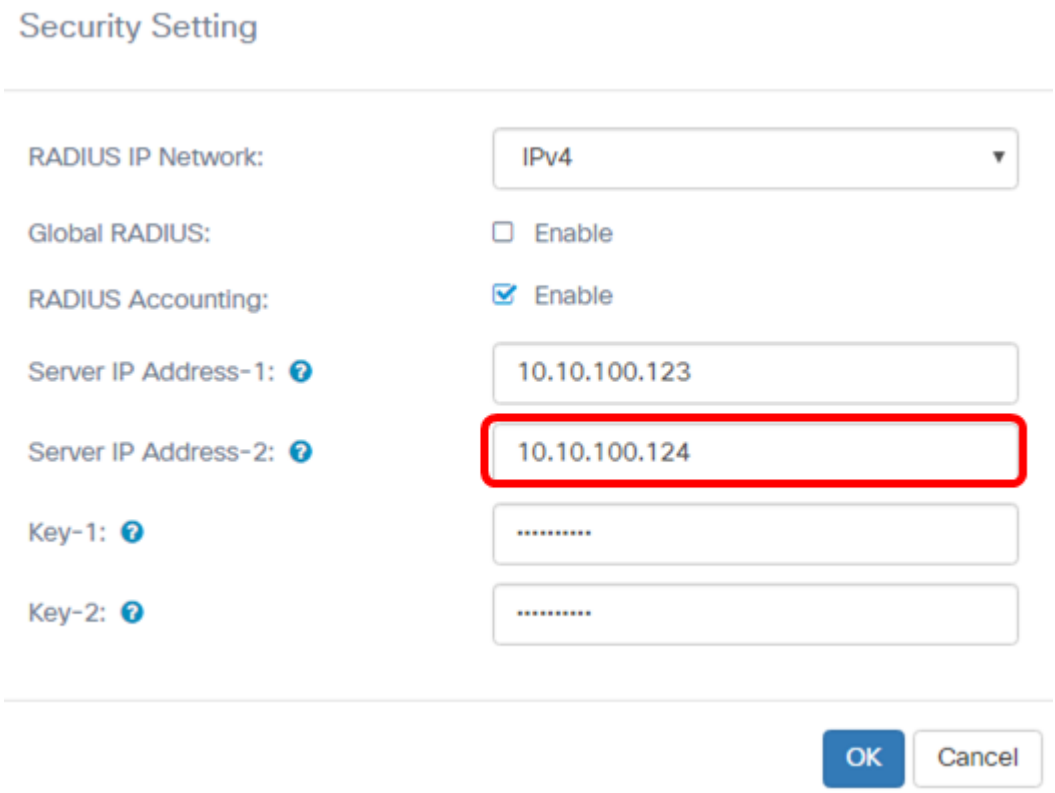


ステップ 5.（オプションの）は *サーバIP Address-1* フィールドでプライマリ RADIUSサーバの IPv4 または IPv6 アドレスを入力します。



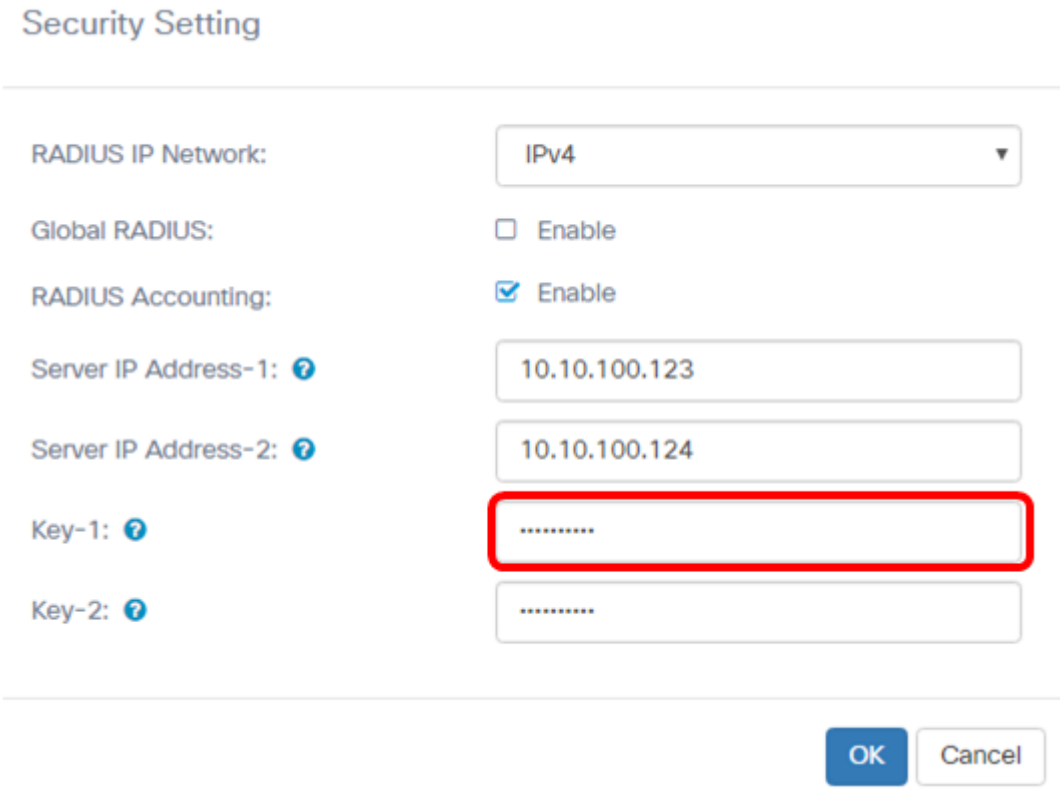
注: この例では、10.10.100.123 は入ります。

ステップ 6.（オプションの）はサーバ*IP Address-2* フィールドでバックアップ RADIUSサーバの IPv4 または IPv6 アドレスを入力します。



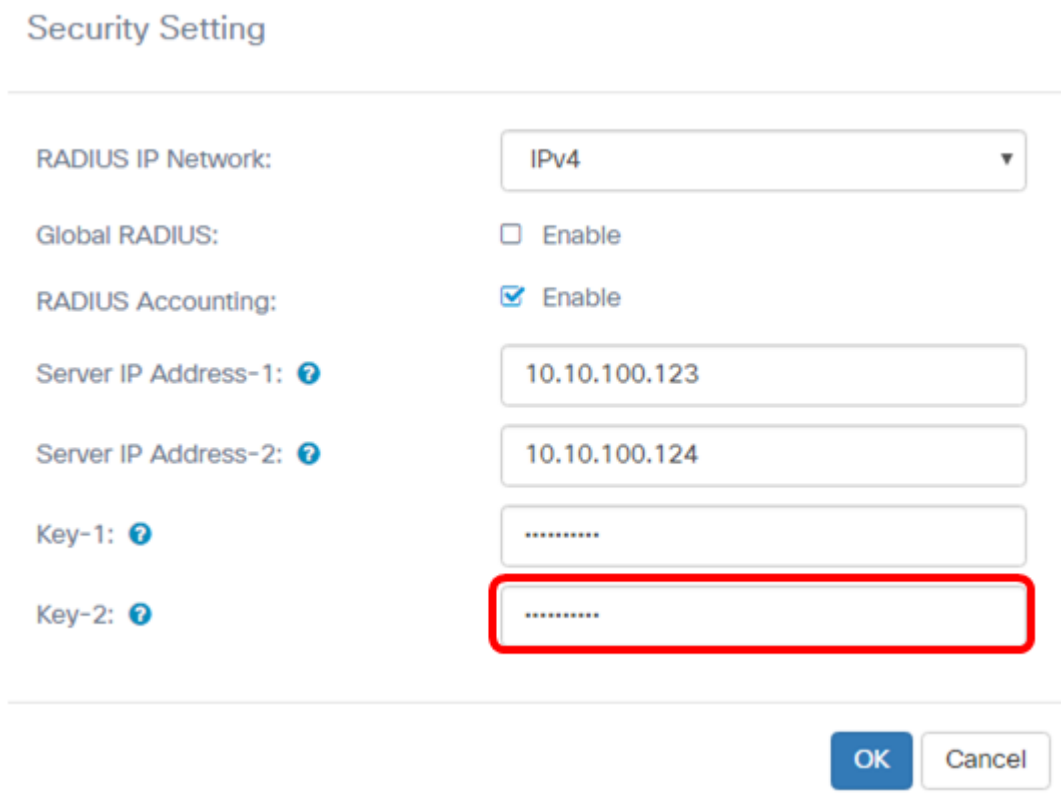
注: この例では、10.10.100.124 は入ります。

ステップ 7.（オプションの）はアクセス ポイントが *Key-1* フィールドのプライマリ RADIUSサーバを認証するのに使用するパスワードを入力します。 このフィールドのエントリは大文字/小文字の区別があり、プライマリ RADIUSサーバで設定されるエントリを一致する必要があります。 キーは 63 までの英数字である場合もあります。

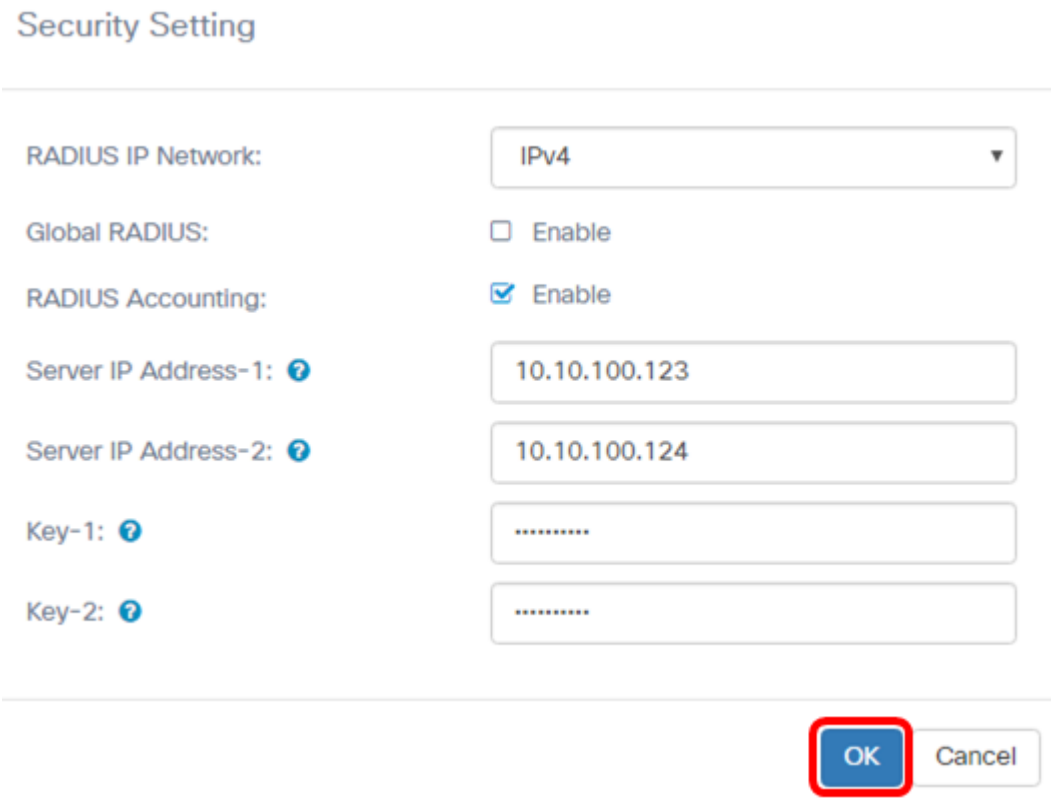


ステップ 8.（オプションの）はアクセス ポイントが *Key-2* フィールドのセカンダリ

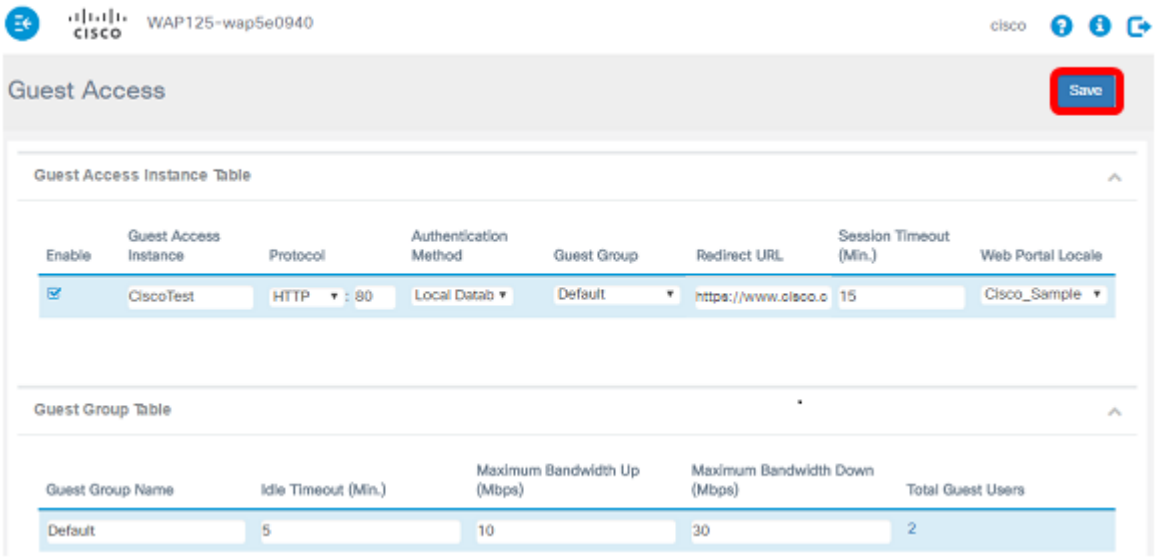
RADIUSサーバを認証するのに使用するパスワードを入力します。 このフィールドのエントリは大文字/小文字の区別があり、プライマリ RADIUSサーバで設定されるエントリを一致する必要があります。 キーは 63 までの英数字である場合もあります。



ステップ 9. 『OK』 をクリック して下さい。



ステップ 10. 『SAVE』 をクリック して下さい。



ゲスト アクセス例表は RADIUS認証認証方法で今設定する必要があります。