WAPでのワイヤレスセキュリティ設定の設定

概要

ワイヤレスアクセスポイント(WAP)でワイヤレスセキュリティを設定することは、ワイヤレスデバイスのプライバシーを侵害する可能性のある侵入者や、ワイヤレスネットワークを介して送信するデータからワイヤレスネットワークを保護するために非常に重要です。MACフィルタ、Wi-Fi Protected Access(WPA/WPA2) Personal、およびWPA/WPA2 Enterpriseを設定して、ワイヤレスネットワークのワイヤレスセキュリティを設定できます。

MACフィルタリングは、ワイヤレスクライアントがMACアドレスを使用してネットワークにアクセスするようにフィルタリングするために使用されます。クライアントリストは、設定に応じて、リスト上のアドレスがネットワークにアクセスすることを許可またはブロックするように設定されます。MACフィルタリングの詳細については、ここをクリックします。

WPA/WPA2 PersonalおよびWPA/WPA2 Enterpriseは、ワイヤレスネットワーク上で送信されるデータを暗号化してプライバシーを保護するために使用されるセキュリティプロトコルです。WPA/WPA2は、IEEE標準802.11Eおよび802.11iと互換性があります。Wired Equivalent Privacy(WEP)セキュリティプロトコルと比較して、WPA/WPA2は認証および暗号化機能を改善しました。

WPA/WPA2 Personalは家庭用で、WPA/WPA2 Enterpriseはビジネス規模のネットワーク用です。WPA/WPA2 Enterpriseは、WPA/WPA2 Personalと比較して、ネットワークのセキュリティと集中制御を強化します。

このシナリオでは、WPA/WPA2パーソナル設定とエンタープライズ設定を使用してネットワークを侵入者から保護するために、WAPでワイヤレスセキュリティを設定します。

目的

この記事では、ワイヤレスネットワークのセキュリティとプライバシーを向上させるために、WPA/WPA2パーソナルおよびエンタープライズセキュリティプロトコルを設定する方法を説明します。

注：この記事では、WAPでService Set Identifier(SSID)またはWireless Local Area Network(WLAN)がすでに作成されていることを前提としています。

該当するデバイス

- WAP100シリーズ
- WAP300シリーズ
- WAP500シリーズ

[Software Version]

- 1.0.2.14 - WAP131、WAP351
- 1.0.6.5 - WAP121、WAP321
- 1.3.0.4 - WAP371

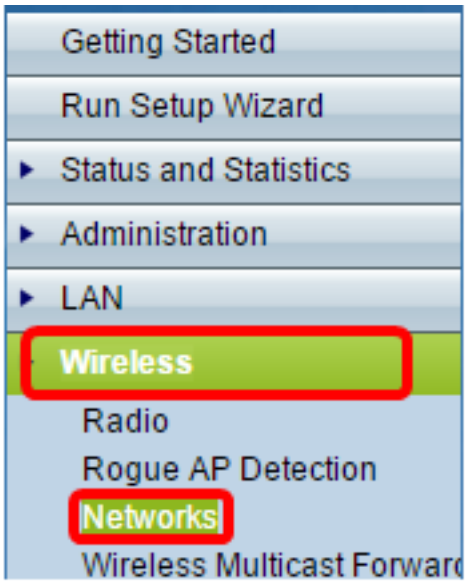
- 1.1.0.7 - WAP150、WAP361
- 1.2.1.5 - WAP551、WAP561
- 1.0.1.11 - WAP571、WAP571E

ワイヤレスセキュリティの設定

WPA/WPA2 Personalの設定

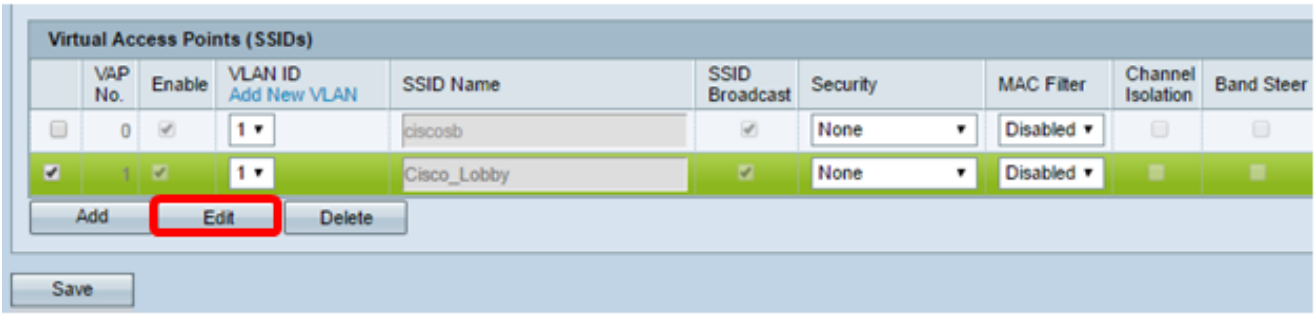
ステップ1：アクセスポイントのWebベースのユーティリティにログインし、[**Wireless**] > [**Networks**]を選択します。

注：次の図では、例としてWAP361のWebベースのユーティリティを使用しています。メニューのオプションは、デバイスのモデルによって異なります。

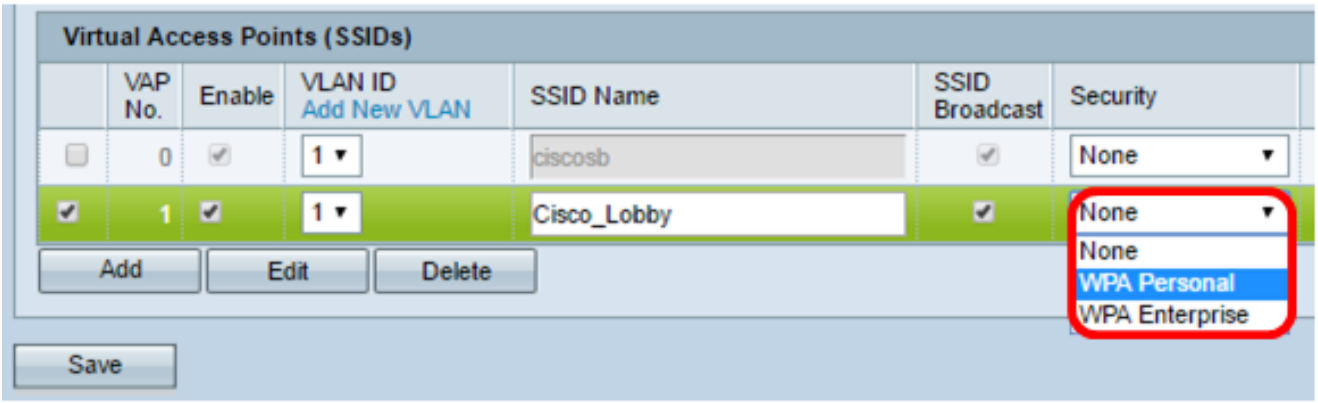


ステップ2:[Virtual Access Points (SSIDs)]領域で、設定するSSIDのチェックボックスをオンにし、[**Edit**]をクリックします。

注：この例では、VAP1が選択されています。



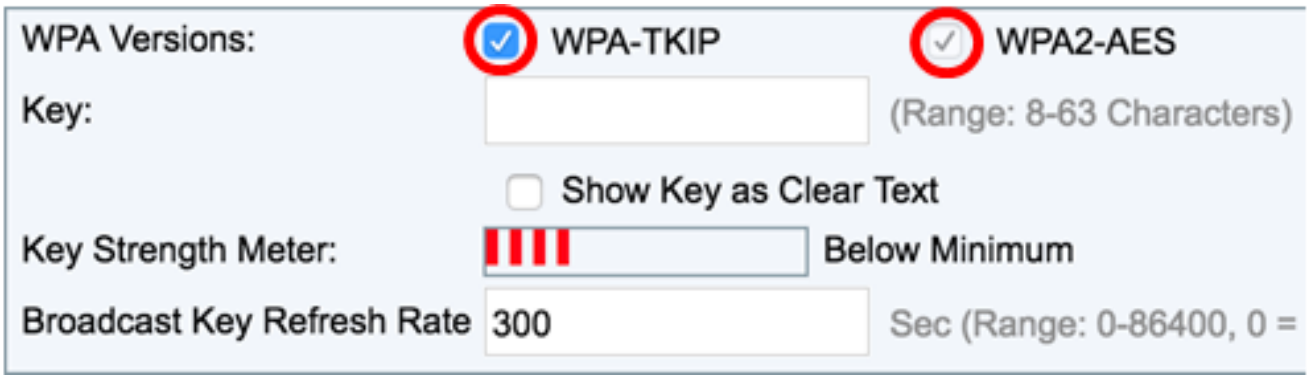
ステップ3:[セキュリティ]**ドロップダウン**リストから[WPA Personal]をクリックします。



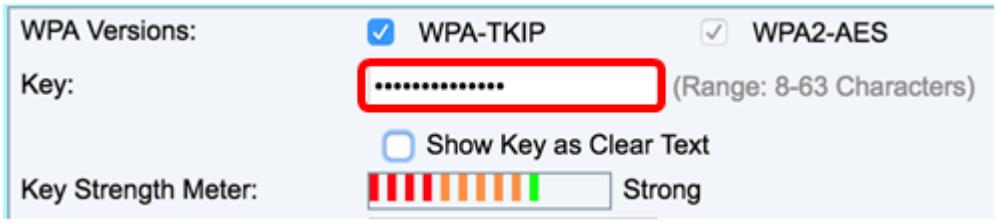
ステップ4：チェックボックスをオンにして、WPAバージョン（WPA-TKIPまたはWPA2-AES）を選択します。同時に二つ選ぶも可なり。

- WPA-TKIP:Wi-Fi Protected Access-Temporal Key Integrity Tool。ネットワークには、元のWPAおよびTKIPセキュリティプロトコルのみをサポートするクライアントステーションがあります。アクセスポイントにWPA-TKIPのみを選択することは、最新のWi-Fi Alliance要件に従って許可されないことに注意してください。
- WPA2-AES:Wi-Fi Protected Access-Advanced Encryption Standard。ネットワーク上のすべてのクライアントステーションは、WPA2およびAES-CCMP暗号化/セキュリティプロトコルをサポートします。このWPAバージョンは、IEEE 802.11i規格に準拠した最高のセキュリティを提供します。最新のWi-Fi Alliance要件に従って、WAPはこのモードを常にサポートする必要があります。

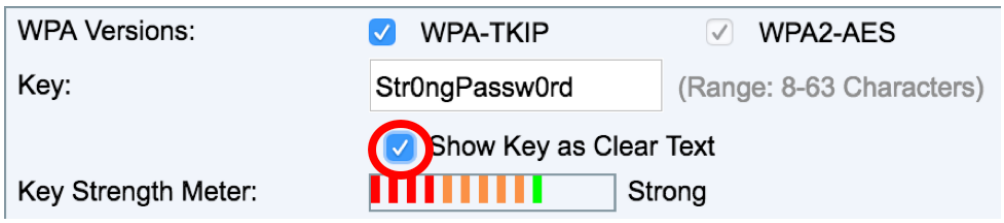
注：この例では、両方のチェックボックスがオンになっています。



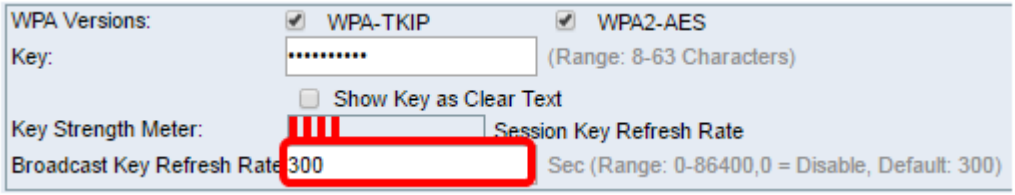
ステップ5:8 ~ 63文字で構成されるパスワードを作成し、[キー]フィールドに入力します。



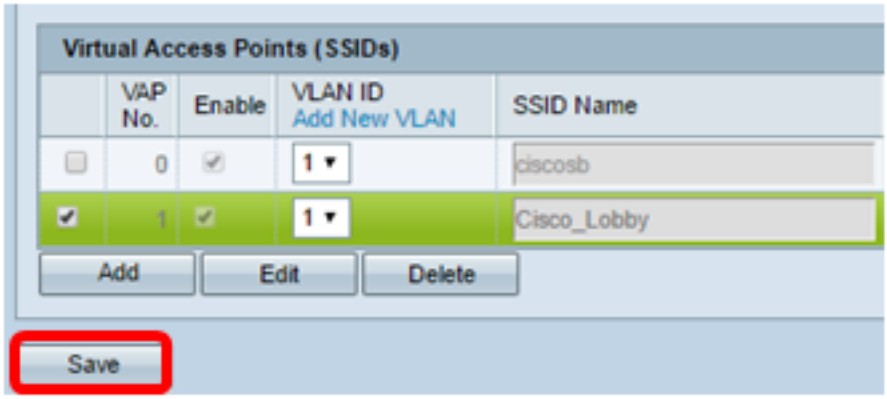
注：[クリアテキストとしてキーを表示]**ボックスをオンに**すると、作成したパスワードを表示できます。



ステップ6:（オプション）[*Broadcast Key Refresh Rate*]フィールドで、このVAPに関連付けられているクライアントのブロードキャスト（グループ）キーが更新される値または間隔を入力します。デフォルトは300秒で、有効な範囲は0 ~ 86400秒です。値0は、ブロードキャストキーが更新されていないことを示します。



ステップ7:[**Save**]をクリックします。

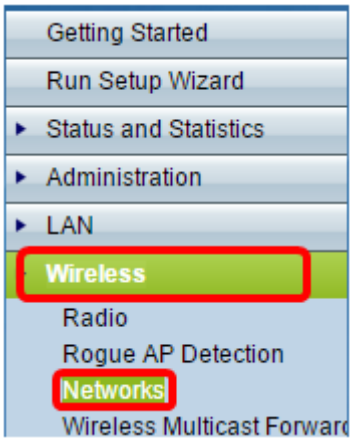


これで、WAPでWPA Personalが設定されました。

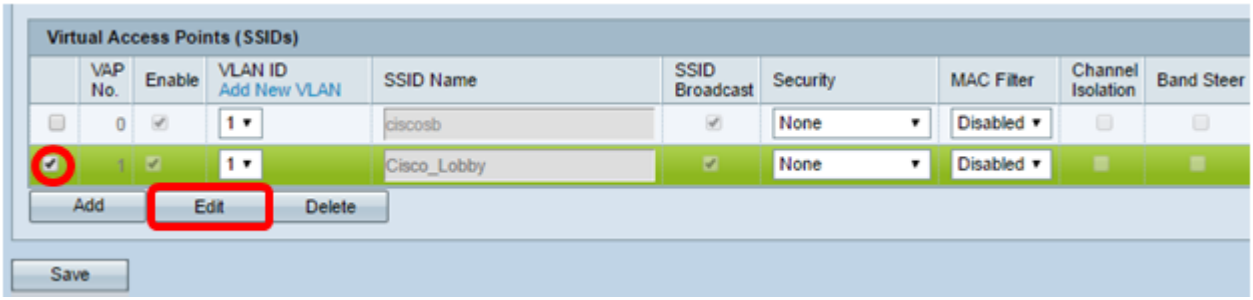
WPA/WPA2 Enterpriseの設定

ステップ1：アクセスポイントのWebベースのユーティリティにログインし、[**Wireless**] > [**Networks**]を選択します。

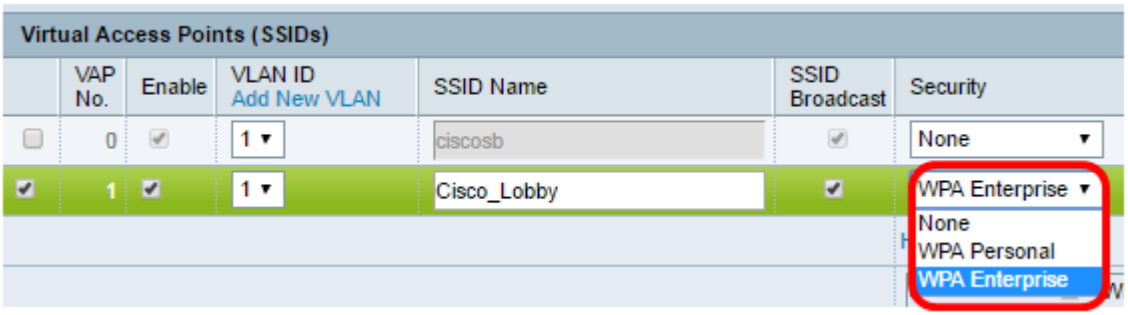
注：次の図では、例としてWAP361のWebベースのユーティリティを使用しています。



ステップ2:[Virtual Access Points (SSIDs)]領域で、設定するSSIDを確認し、その下の[**Edit**]ボタンをクリックします。



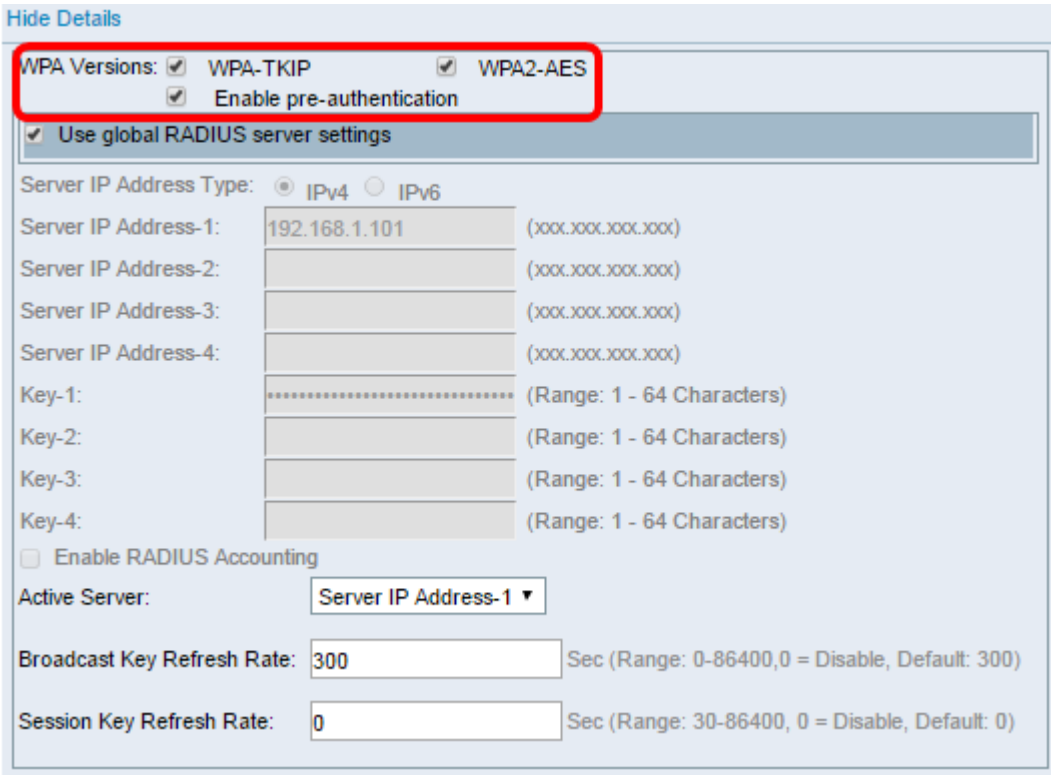
ステップ3:[セキュリティ]ドロップダウンリストから[WPA Enterprise]を選択します。



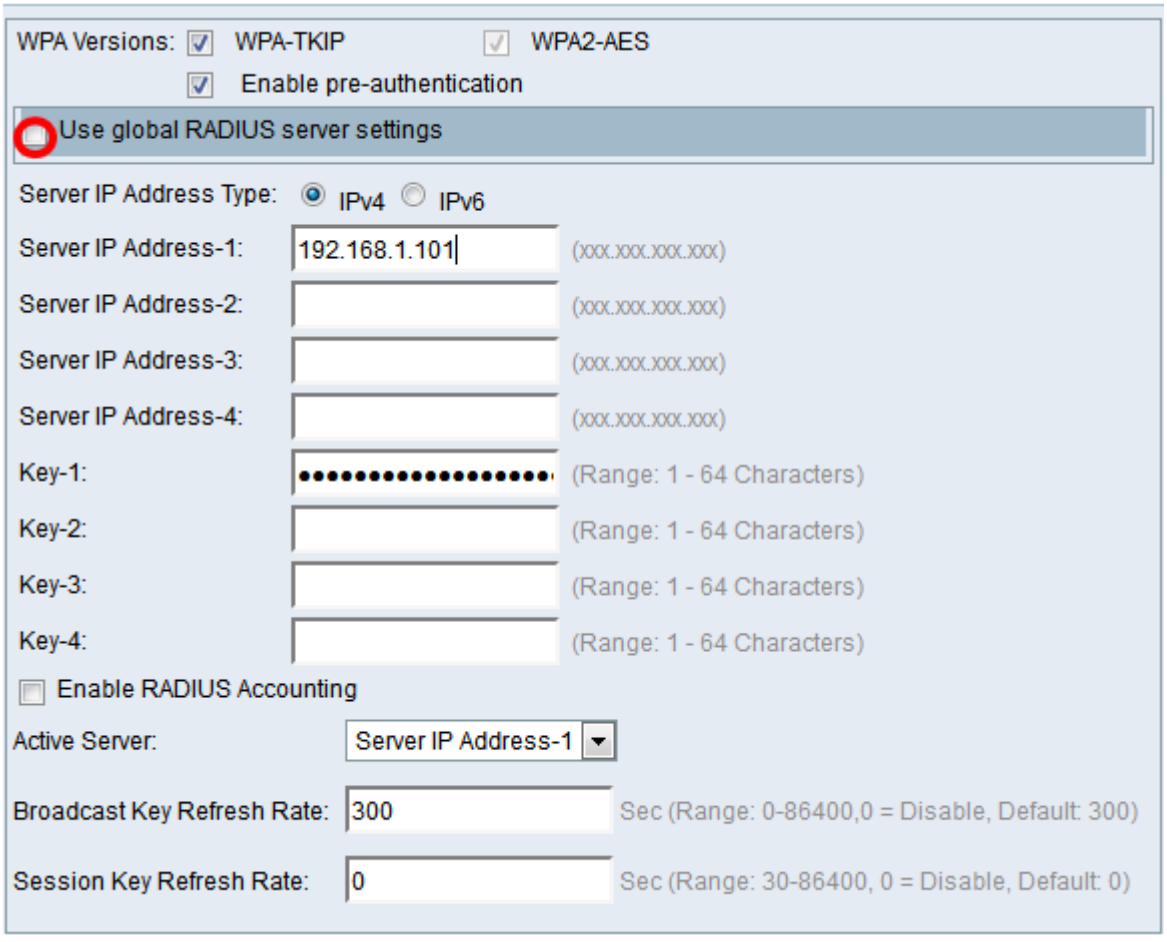
ステップ4:WPAバージョン（WPA-TKIP、WPA2-AES、および事前認証の有効化）を選択します。

- 事前認証の有効化：WPA2-AESのみ、またはWPAバージョンとしてWPA-TKIPとWPA2-AESの両方を選択した場合、WPA2-AESクライアントの事前認証を有効にできます。WPA2ワイヤレスクライアントが事前認証パケットを送信するようにするには、このオプションをオンにします。事前認証情報は、クライアントが現在使用しているWAPデバイスからターゲットWAPデバイスにリレーされます。この機能を有効にすると、複数のアクセスポイント(AP)に接続するローミングクライアントの認証を高速化できます。

注：WPA-TKIPをWPAバージョンに選択した場合、元のWPAはこの機能をサポートしていないため、このオプションは適用されません。

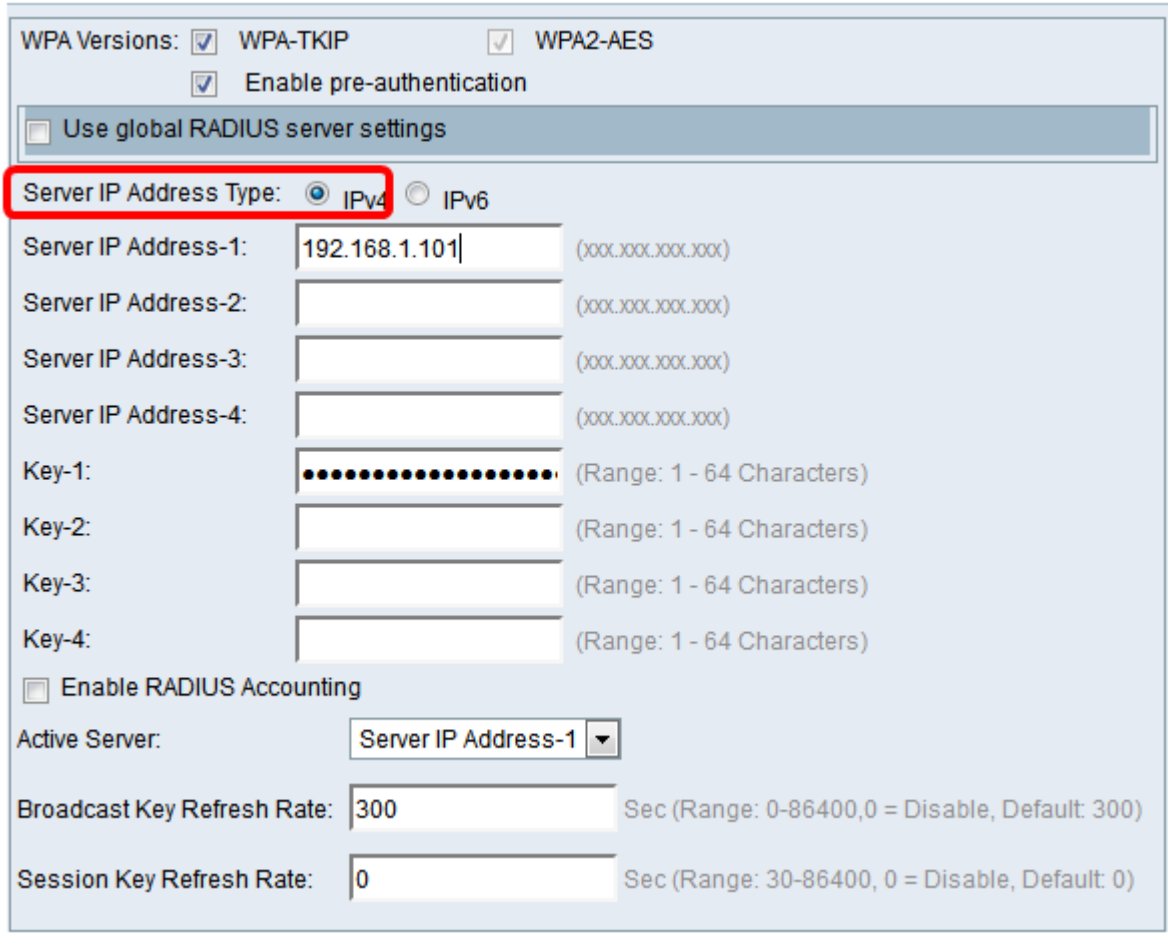


ステップ5:（オプション）[Use global RADIUS server settings]**チェックボックスをオフ**にして、設定を編集します。



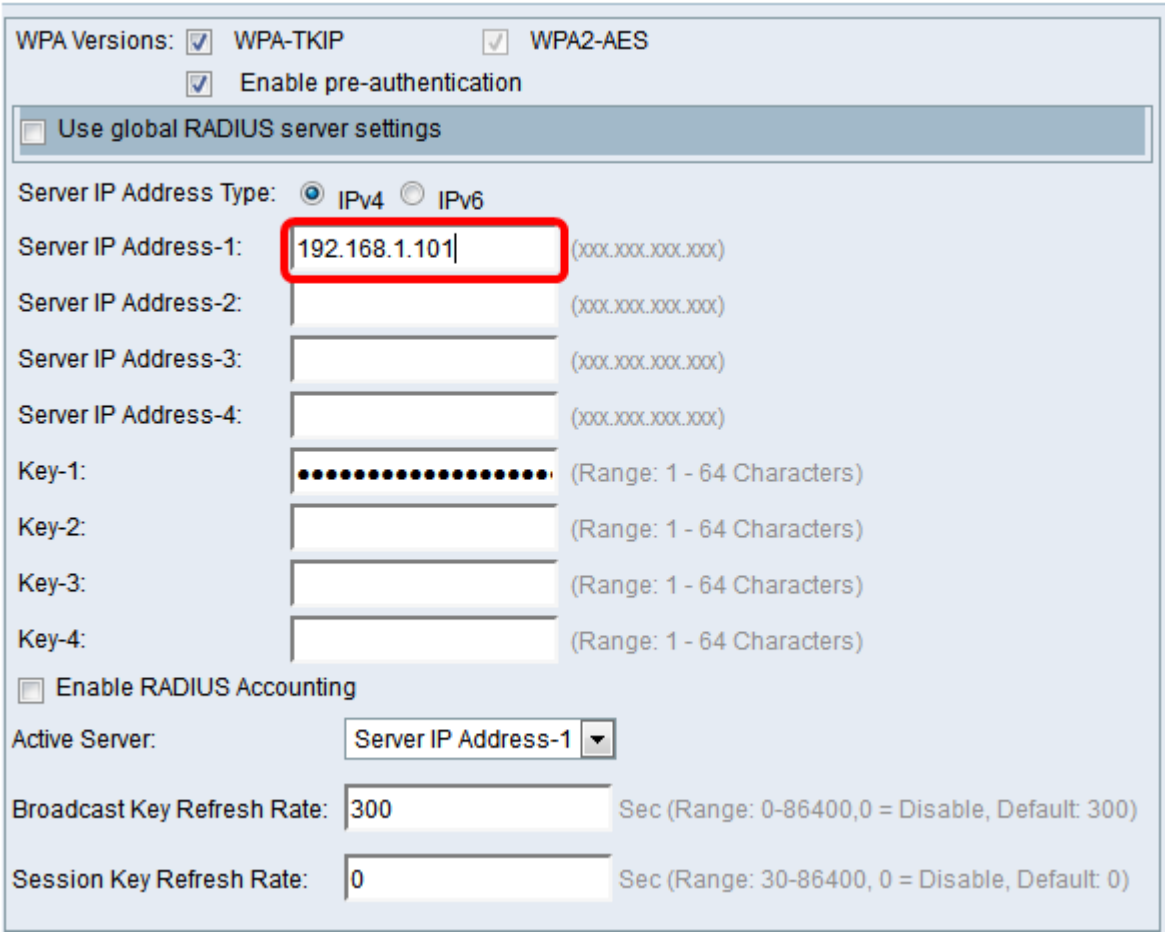
ステップ6:（オプション）正しいサーバーIPアドレスの種類のラジオボタンをクリックします。

注：この例では、IPv4が選択されています。



ステップ7:[Server IP Address]フィールドにRADIUSサーバのIPアドレスを入力します。

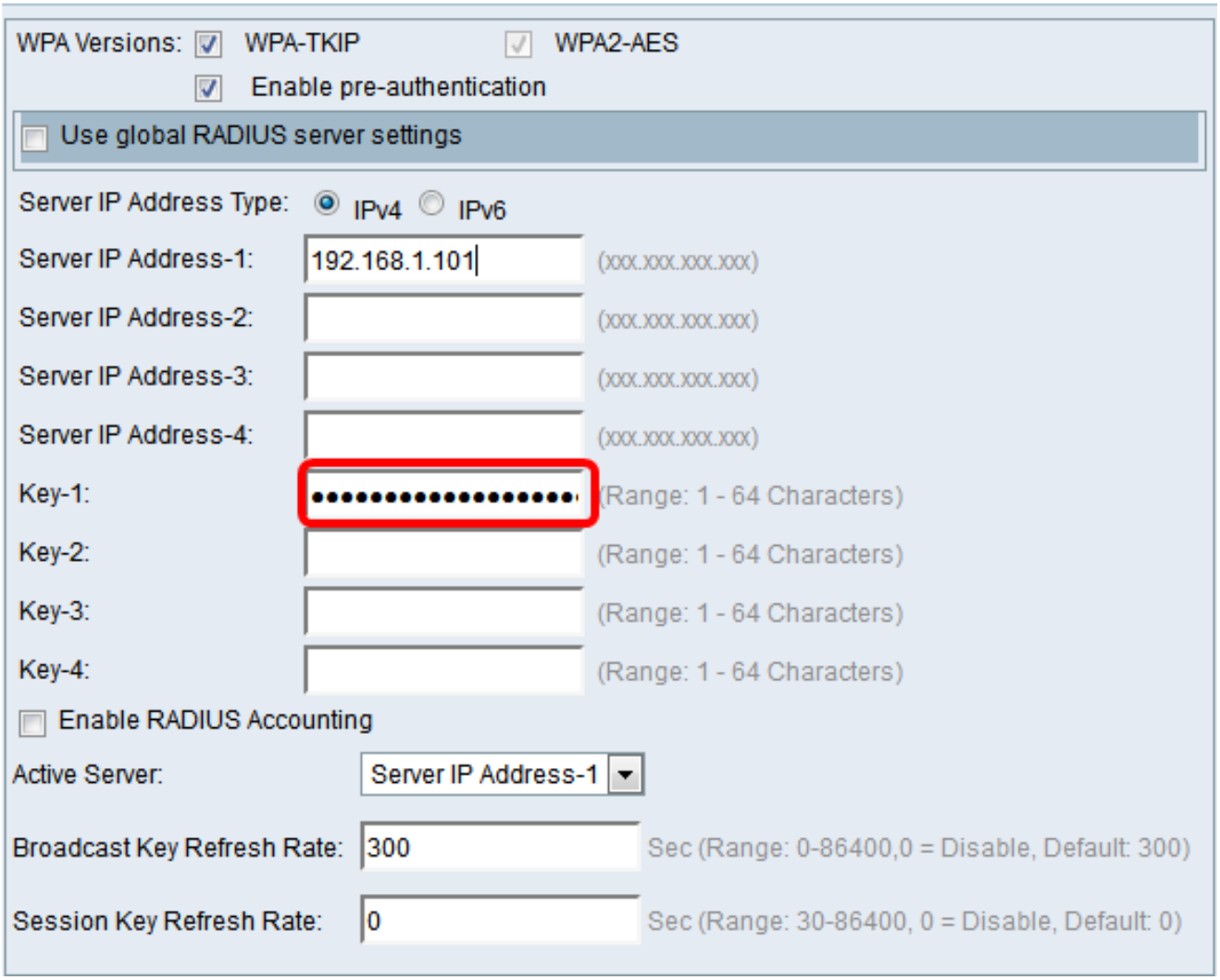
注： この例では、192.168.1.101を使用します。



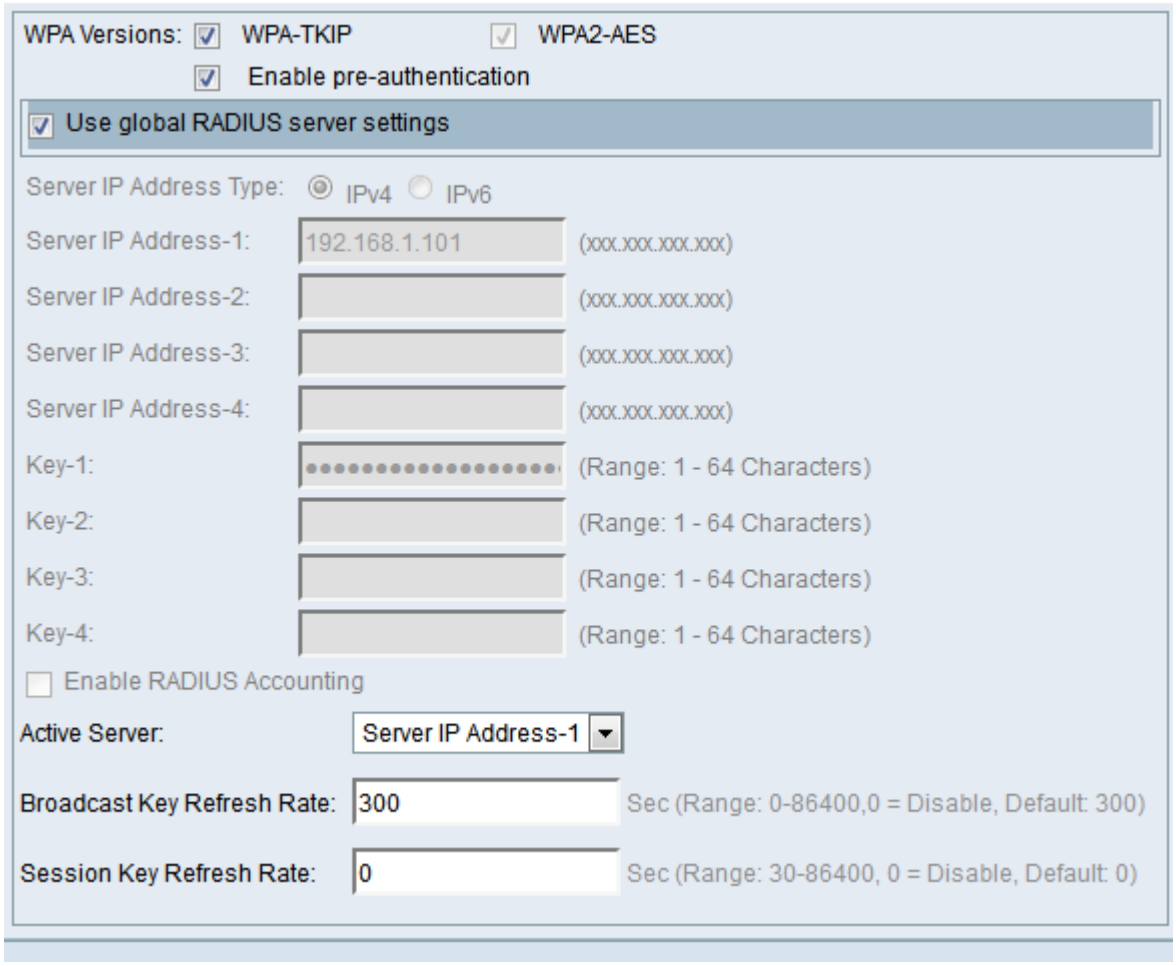
ステップ8:[Key] フィールドに、WAPがRADIUSサーバへの認証に使用するRADIUSサーバに対応するパスワードキーを入力します。1 ~ 64文字の英数字と特殊文字を使用できます。

注：キーは大文字と小文字が区別され、RADIUSサーバで設定されているキーと一致している必要があります。

ステップ9: (オプション) WAPと通信するネットワーク内のすべてのRADIUSサーバに対して、ステップ7 ~ 8を繰り返します。



ステップ10:（オプション）[EnableRADIUS Accounting] チェックボックスをオンにすると、ユーザが消費したリソース（システム時間、送信データ量）の追跡と測定が可能になります。 この機能を有効にすると、プライマリサーバとバックアップサーバの両方でRADIUSアカウンティングが可能になります。



ステップ11：をクリックします 

。

これで、WAPでWPA/WPA2 Enterpriseセキュリティが正しく設定されました。