CBWアクセスポイントの個人用事前共有キー機能

目的

この記事では、Cisco Business Wireless(CBW)Access Point(AP)ファームウェアバージョン10.6.1.0のパーソナル事前共有キー(PSK)機能について説明します。

該当するデバイス |ソフトウェアバージョン

- Cisco Business Wireless 140ACアクセスポイント | 10.6.1.0 (最新のダウンロード)
- Cisco Business Wireless 145ACアクセスポイント | 10.6.1.0 (最新のダウンロード)
- Cisco Business Wireless 240ACアクセスポイント | 10.6.1.0 (最新のダウンロード)

概要

ネットワークにCBWギアがある場合は、ファームウェアバージョン10.6.1.0でパーソナルPSK機能を使用できます。

個人PSK(iPSK)とも呼ばれる個人PSKは、管理者が同じWi-Fi Protected Access II(WPA2)の個人無線ローカルエリアネットワーク(WLAN)の個々のデバイスに一意の事前共有キーを発行できるようにする機能です。 一意のPSKは、デバイスのMACアドレスに関連付けられます。これは、WPA3ポリシーが有効になっているWLANではサポートされていません。

この機能は、RADIUSサーバを使用してクライアントを認証します。これは通常、IoTデバイスや会社支給のラップトップやモバイルデバイスでの使用を目的としています。

目次

前提条件

- CBW APファームウェアを10.6.1.0にアップグレードしたことを確認します。ファームウェアの更新に関する手順を追加するには、クリックしてください。
- パーソナルPSKとデバイスのMACアドレスを設定する必要があるRADIUSサーバが必要です。
- このCBW機能は、3つの異なるRADIUSサーバ（FreeRADIUS、MicrosoftのNPS、およびシスコのISE）でサポートされています。設定は、使用するRADIUSサーバによって

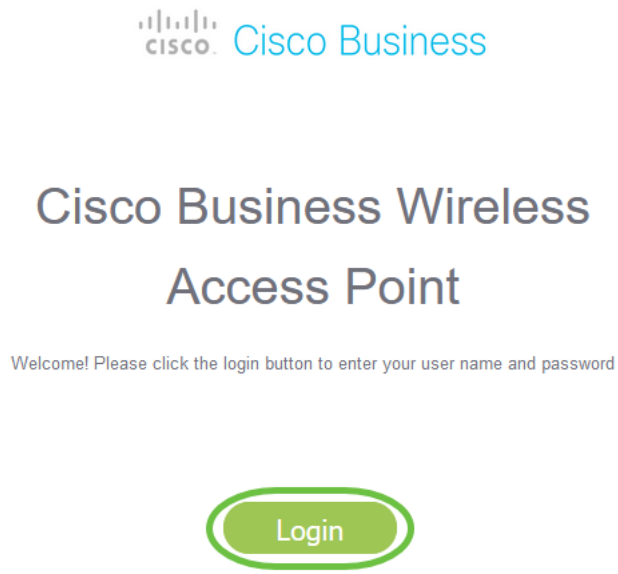
異なります。

CBW RADIUS設定の設定

CBW APでRADIUS設定を行うには、次の手順を実行します。

手順 1

CBW APのWebユーザインターフェイス(UI)にログインします。

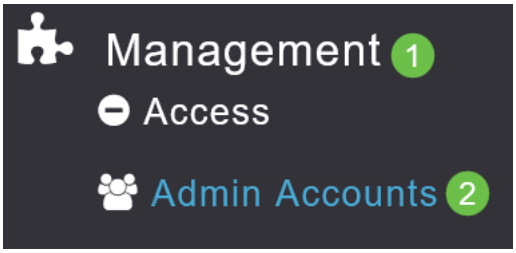


手順 2

双方向の矢印**記号をクリック**して、エキスパートビューに切り替えます。

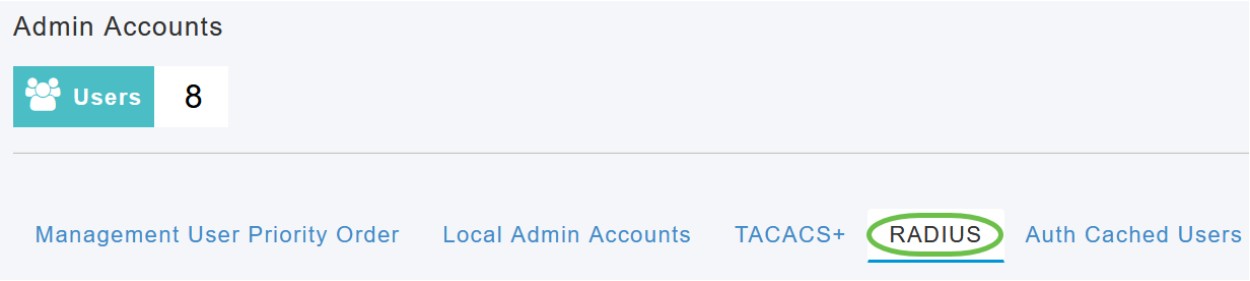
手順 3

[Management] > [Admin Accounts]に移動します。



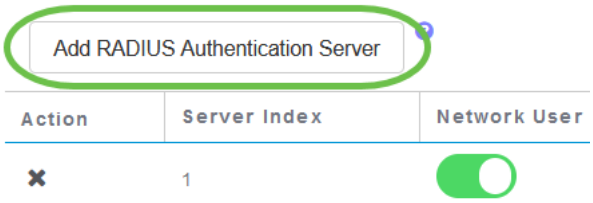
手順 4

[RADIUS]タブ**を選択**します。



手順 5

[Add RADIUS Authentication Server]をクリックします。

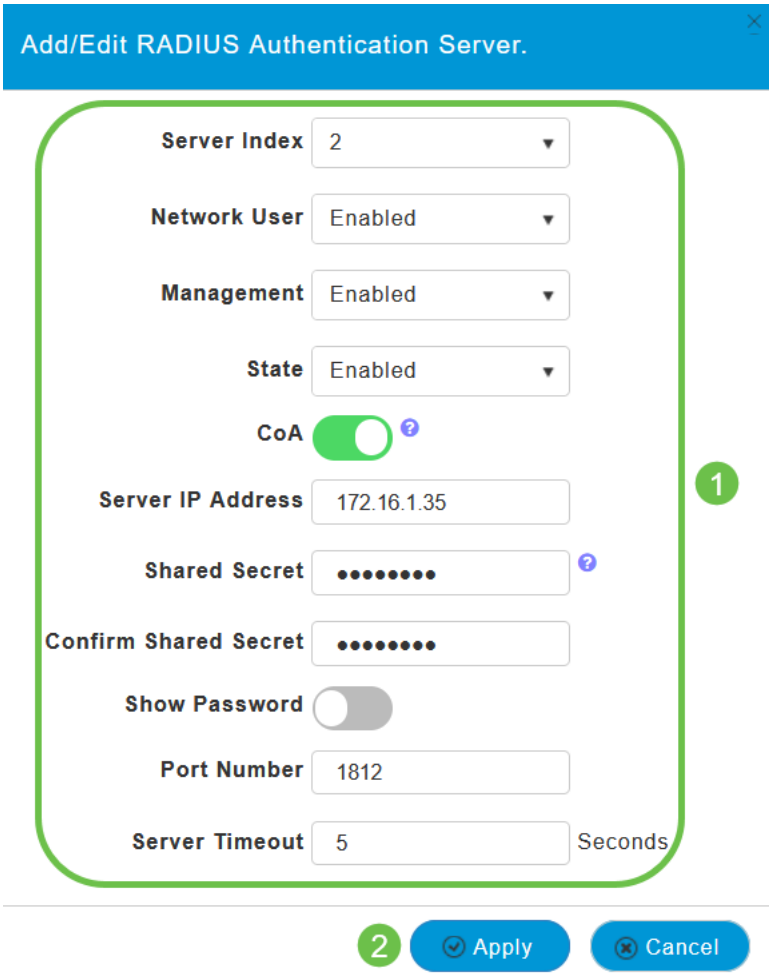


手順 6

次のように設定します。

- *サーバインデックス* – 1から6を選択
- *Network User* : 状態を有効にします。デフォルトでは[有効(Enabled)]です
- *管理* : 状態を有効にします。デフォルトでは[有効(Enabled)]です
- *State* : 状態を有効にします。デフォルトでは[有効(Enabled)]です
- *CoA*:Charge of authority(CoA)が有効になっていることを確認します。
- *Server IP Address*:RADIUSサーバのIPv4アドレスを入力します
- *Shared Secret* : 共有秘密キーを入力します
- *Port Number*:RADIUSサーバとの通信に使用されるポート番号を入力します。
- *Server Timeout* : サーバタイムアウトを入力します

[Apply] をクリックします。



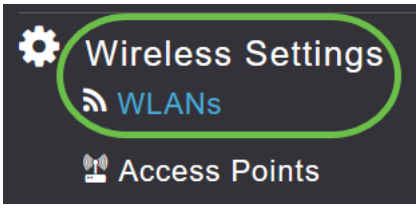
WLANの設定

標準のWPA2 Personal Secured WLANとしてWLANを作成します。

事前共有キーは、パーソナルPSKデバイスには使用されません。これは、RADIUSサーバで認証されていないデバイスにのみ使用されます。このWLANに接続するすべてのデバイスのMACアドレスを、このデバイスの許可リストに追加する必要があります。

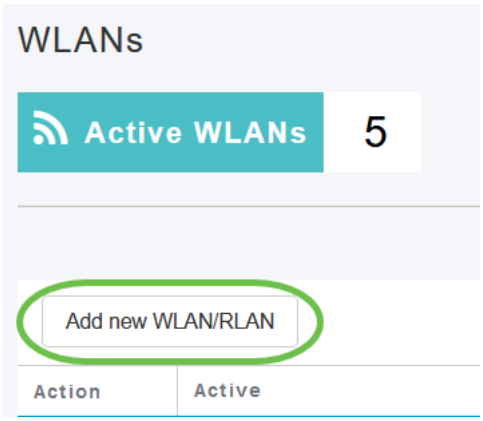
手順 1

[Wireless Settings] > [WLANs] に移動します。



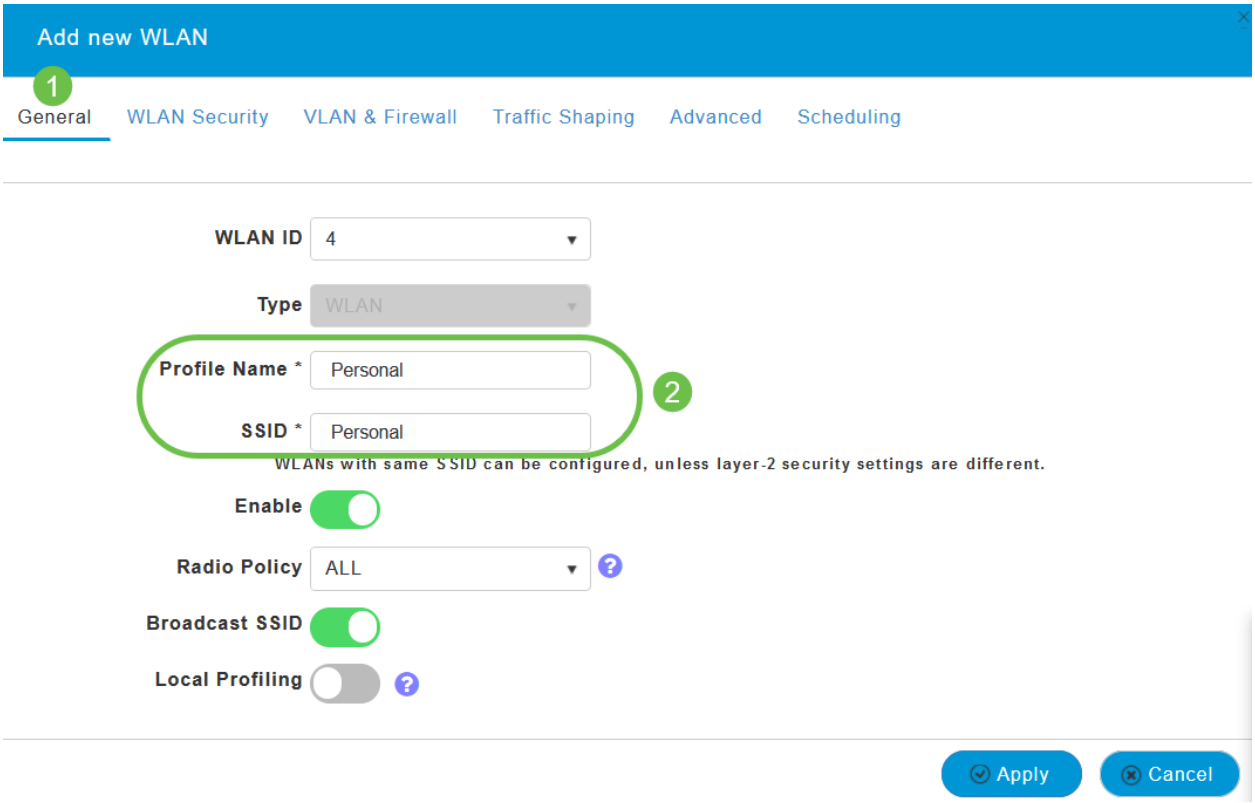
手順 2

Add new WLAN/RLANをクリックします。



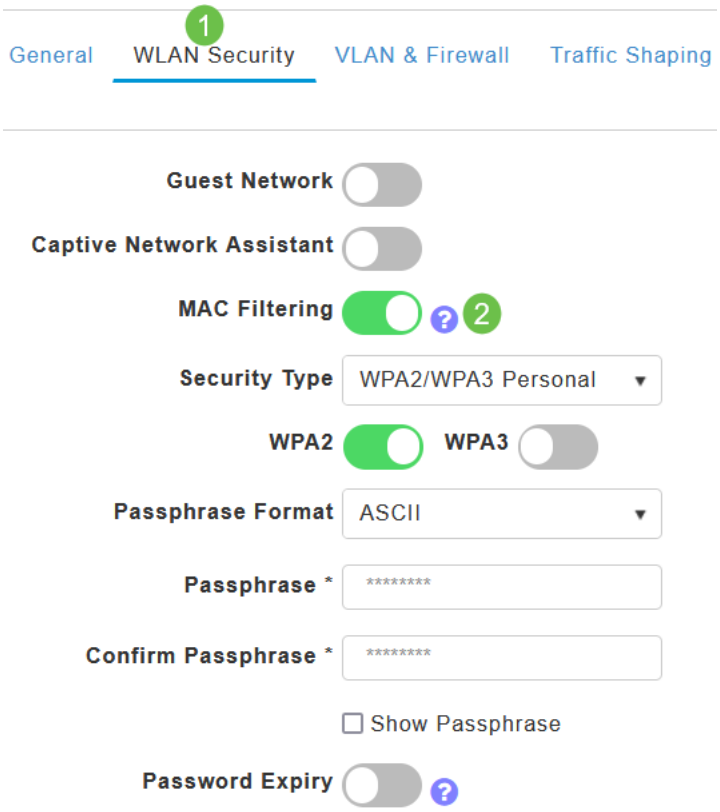
手順 3

[*General*]タブで、WLANの[*Profile Name*]を入力します。



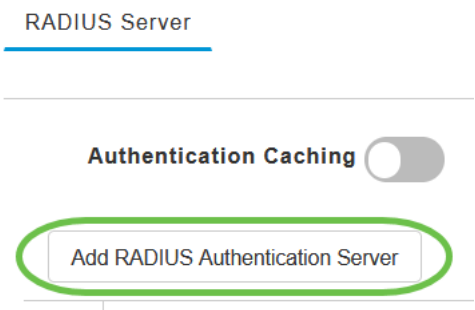
手順 4

[WLAN Security]タブに移動し、トグル**をスライド**させてMACフィルタリングを有効にします。



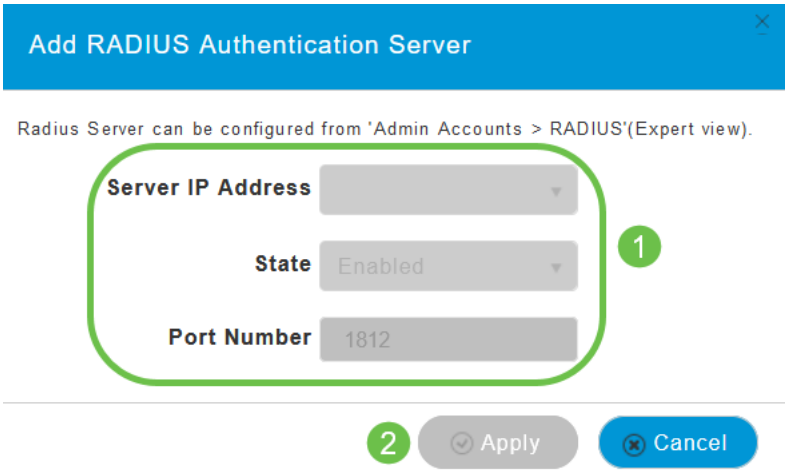
手順 5

[Add RADIUS Authentication Server] をクリックして、前のセクションで設定したRADIUSサーバを追加し、このWLANの認証を行います。



手順 6

ポップアップウィンドウが表示されます。サーバのIP*アドレス*、*状態*、*ポート番号*を*入力*します。[Apply] をクリックします。

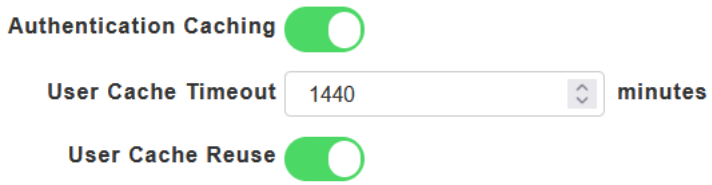


ステップ7

(オプション)

認証キャッシングを*有効*にします。このオプションを有効にすると、次のフィールドが表示されます。

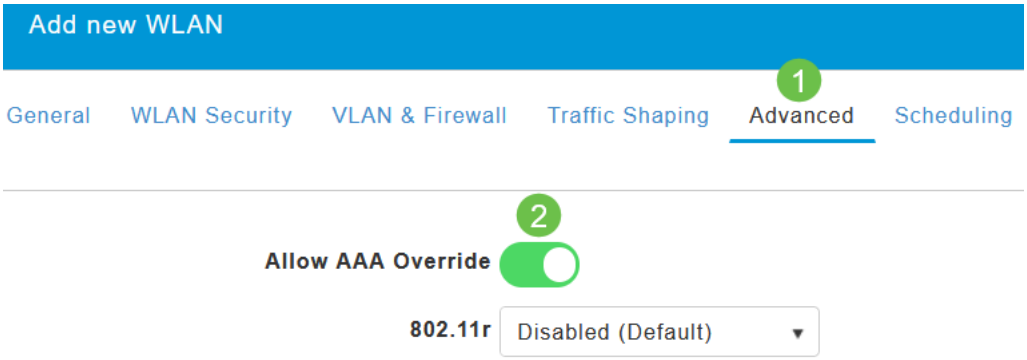
- *User Cache Timeout*：キャッシュ内の認証済みクレデンシャルの有効期限を指定します。
- *User Cache Reuse*：キャッシュタイムアウトの前に資格情報キャッシュ情報を使用します。デフォルトでは、無効になっています。



この機能が有効になっている場合、このサーバに対してすでに認証されているクライアントは、24時間以内にこのWLANに再接続するときに、RADIUSサーバにデータを渡す必要はありません。

手順 8

[Advanced] タブまで移動します。トグルを**スライドさせて**[Allow AAA Override]を有効にします。

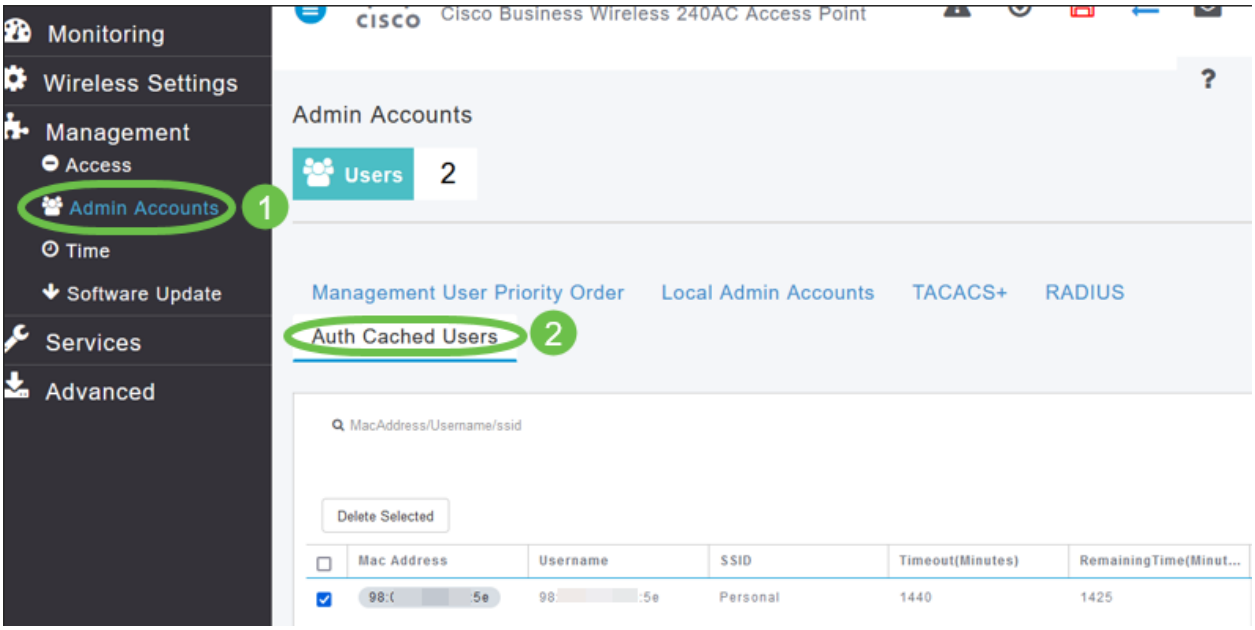


[詳細]タブは、エキスパートビューでのみ表示されます。

次のステップ

CBW APの設定とRADIUSサーバの設定が完了したら、デバイスを接続できるようになります。そのMACアドレスに設定されているカスタムPSKを入力すると、ネットワークに参加します。

認証キャッシングを設定している場合は、[Admin Accounts]の下の[*Auth Cached Users*]タブに移動して、WLANに参加しているデバイスを確認できます。必要に応じて、これを削除できます。



結論

行くぞ！これで、CBW APでパーソナルPSK機能の利点を享受できます。