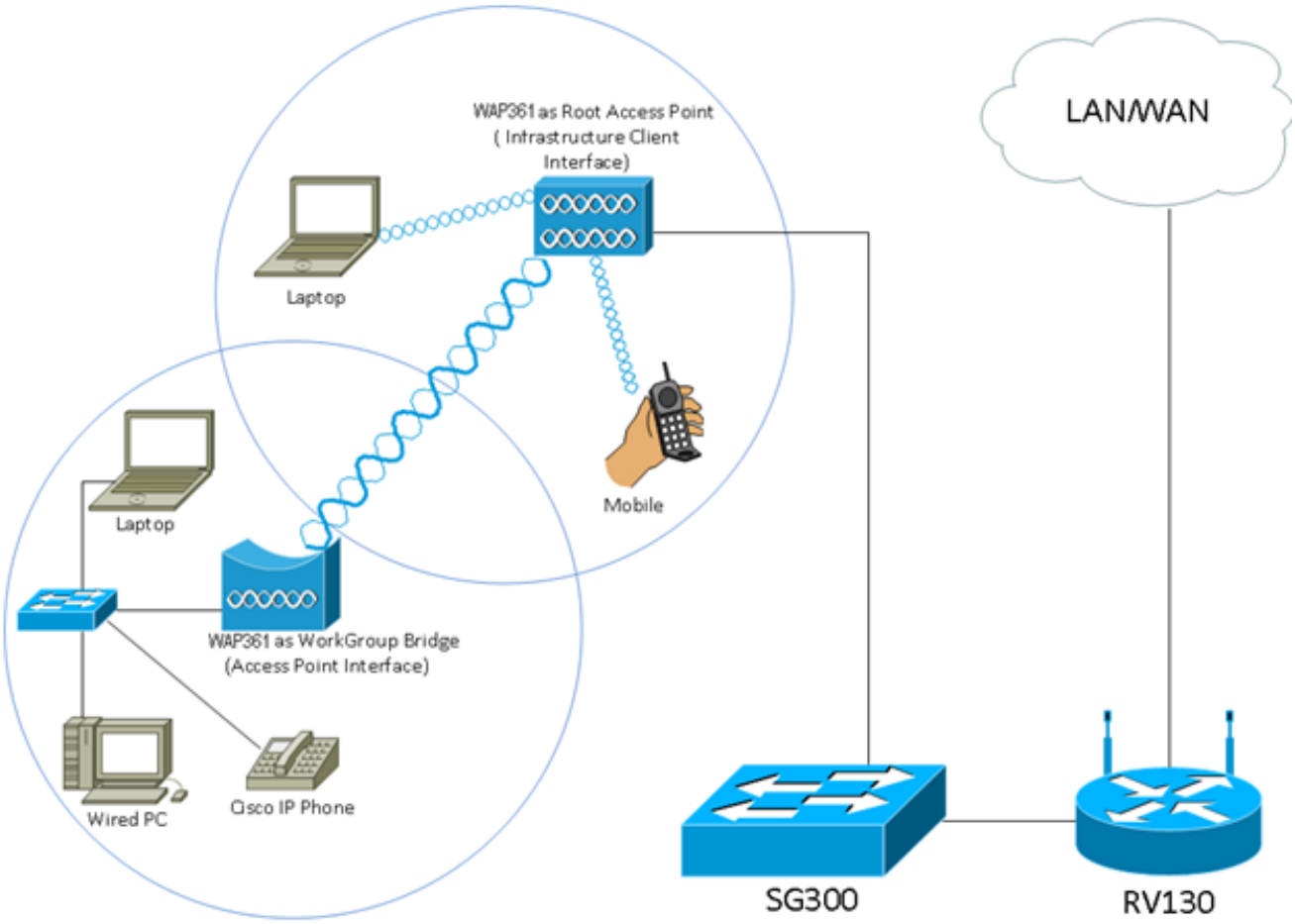
ワイヤレスアクセスポイント(WAP)でのワークグループブリッジの設定

目的

WorkGroup Bridge機能を使用すると、ワイヤレスアクセスポイント(WAP)は、リモートクライアントと、WorkGroup Bridgeモードに接続されているワイヤレスローカルエリアネットワーク(LAN)間でトラフィックをブリッジできます。リモートインターフェイスに関連付けられたWAPデバイスはアクセスポイントインターフェイスと呼ばれ、ワイヤレスLANに関連付けられたWAPデバイスはインフラストラクチャインターフェイスと呼ばれます。WorkGroup Bridgeを使用すると、有線接続のみのデバイスをワイヤレスネットワークに接続できます。Wireless Distribution System(WDS)機能が使用できない場合の代替手段として、WorkGroup Bridge Mode(WGB)が推奨されます。



注：上記のトポロジは、WorkGroup Bridgeモデルの例を示しています。有線デバイスは、WAPのLANインターフェイスに接続するスイッチに接続されます。WAPはアクセスポイントインターフェイスとして機能し、インフラストラクチャインターフェイスに接続します。

この記事では、2つのWAP間でWorkGroup Bridgeを設定する方法について説明します。

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]

- 1.0.0.17:WAP571、WAP571E
- 1.0.1.7 — WAP150、WAP361
- 1.0.2.5 — WAP131、WAP351
- 1.0.6.5 — WAP121、WAP321
- 1.2.1.3 — WAP551、WAP561
- 1.3.0.3 — WAP371

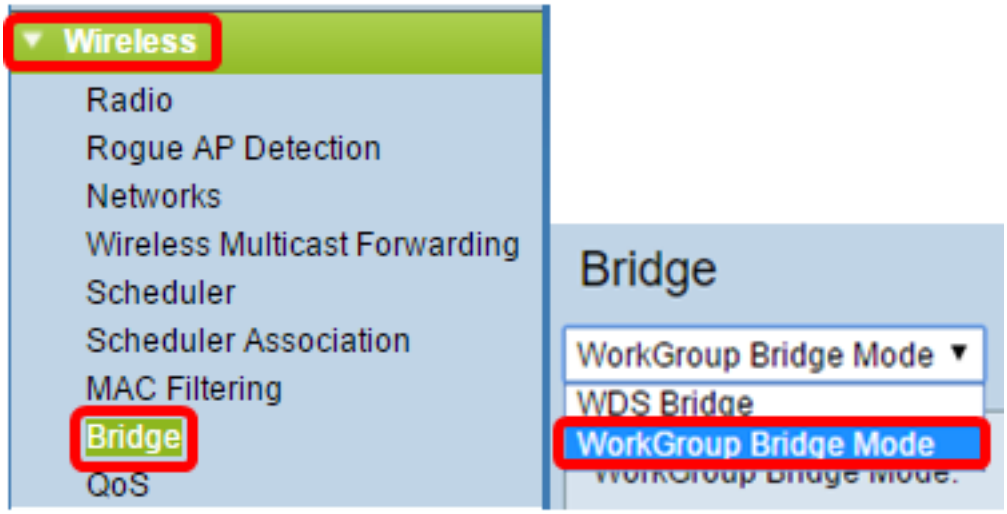
ワークグループブリッジの設定

インフラストラクチャクライアントインターフェイス

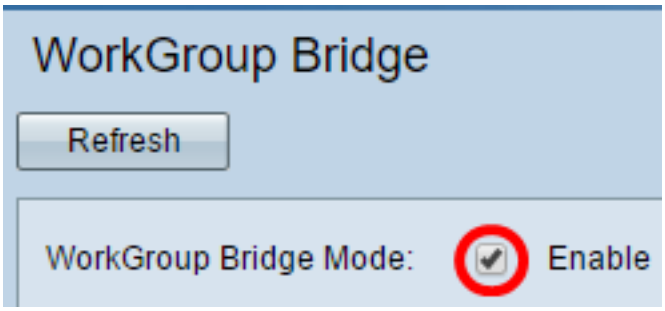
ステップ1:WAPのWebベースのユーティリティにログインし、**[Wireless] > [WorkGroup Bridge]を選択します。**

注：メニューオプションは、使用しているデバイスのモデルによって異なります。次の図は、特に明記されていない限り、WAP361から取得したものです。

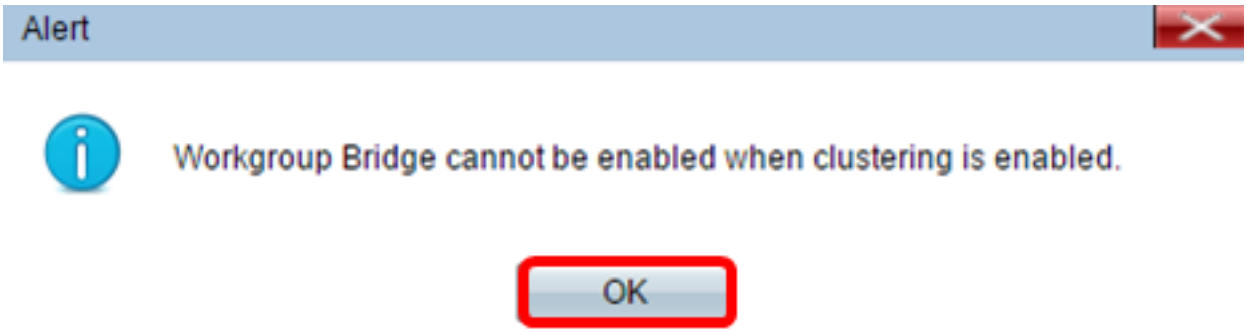
WAP571およびWAP571Eの場合は、**[Wireless] > [Bridge] > [WorkGroup Bridge Mode]を選択します。**



ステップ2:[Enable WorkGroup Bridge Mode]チェックボックスをオンにします。

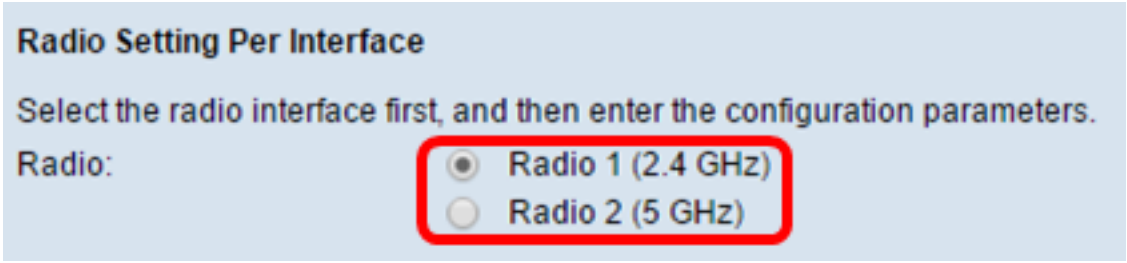


注：WAPでクラスタリングが有効になっている場合、WorkGroup Bridgeが動作するようにクラスタリングを無効にするようにポップアップから通知されます。[OK] をクリックして、次に進みます。クラスタリングを無効にするには、ナビゲーション・ペインから[Single Point Setup]を選択し、**[Access Points] > [Disable Single Point Setup]を選択します**。



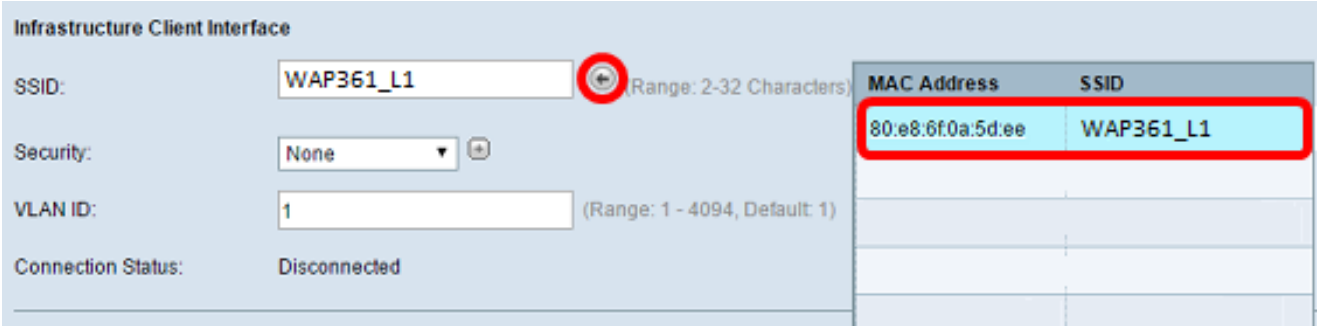
ステップ3：ワークグループブリッジの無線インターフェイスをクリックします。1つの無線をワークグループブリッジとして設定すると、もう1つの無線は引き続き動作します。無線インターフェイスは、WAPの無線周波数帯域に対応する。WAPは、2つの異なる無線インターフェイスでブロードキャストするように装備されています。1つの無線インターフェイスの設定は、もう1つの無線インターフェイスには影響しません。無線インターフェイスのオプションは、WAPモデルによって異なります。一部のWAPではRadio 1が2.4 GHzと表示され、一部のWAPではRadio 2が2.4 GHzと表示されます。

注：この手順は、デュアルバンドを使用する次のWAPにのみ適用されます。WAP131、WAP150、WAP351、WAP361、WAP371、WAP561、WAP571、WAP571E。この例では、Radio 1が選択されています。



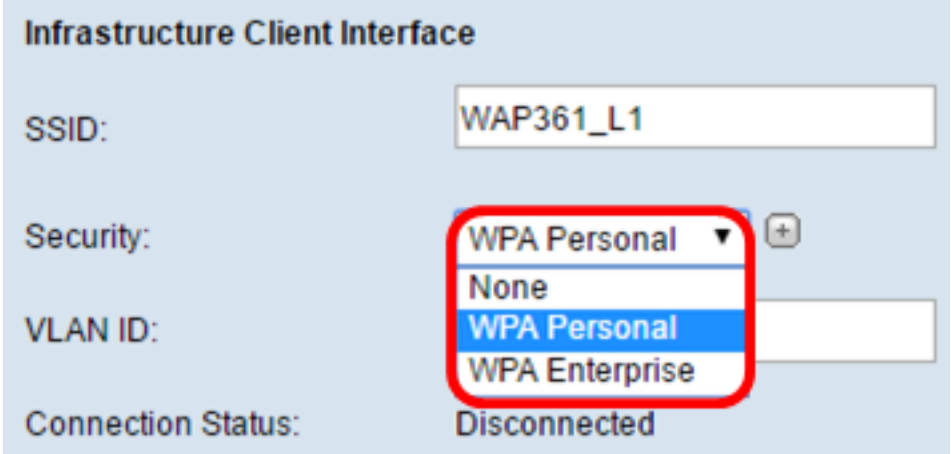
ステップ4:[SSID]フィールドにService Set Identifier(SSID)名を入力するか、フィールドの横にある矢印ボタンをクリックして、ネイバーをスキャンします。これは、デバイスとリモートクライアント間の接続として機能します。インフラストラクチャクライアントSSIDには、2 ~ 32文字を入力できます。

注：不正AP検出を有効にすることが重要です。この機能を有効にする方法の詳細については、ここをクリックしてください。この例では、矢印ボタンをクリックして、インフラストラクチャクライアントインターフェイスのSSIDとして[WAP361_L1]を選択します。



ステップ5:[Infrastructure Client Interface（インフラストラクチャクライアントインターフェイス）]領域で、[Security（セキュリティ）]ドロップダウンリストから、アップストリームWAPデバイスのクライアントステーションとして認証するセキュリティのタイプを選択します。次のオプションがあります。

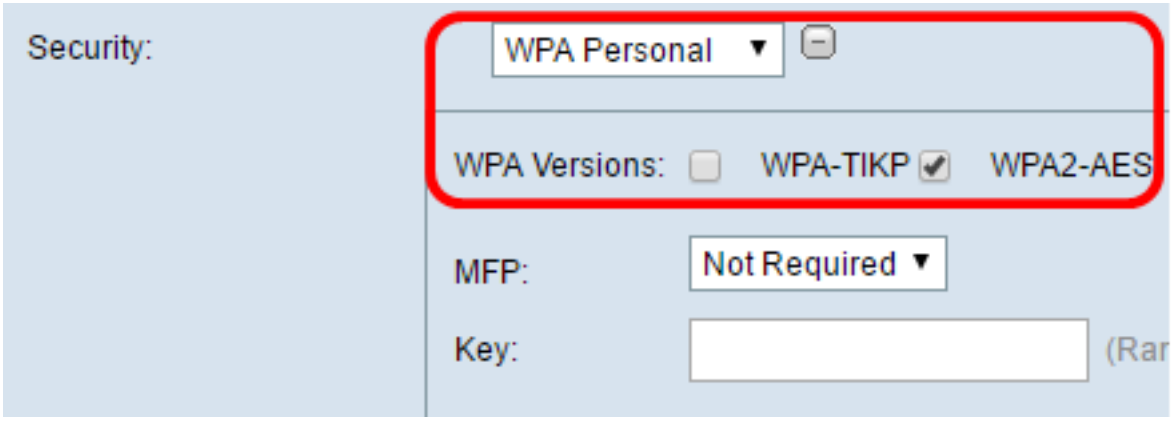
- [なし(None)]：セキュリティを開くか、なし。これはデフォルトです。これを選択した場合は、ステップ18に進みます。
- WPA Personal:WPA Personalは8 ~ 63文字の長さのキーをサポートできます。WPA2は、より強力な暗号化規格であるため、推奨されます。設定するにはステップ6に進んでください。
- WPA Enterprise:WPA EnterpriseはWPA Personalよりも高度で、認証に推奨されるセキュリティです。Protected Extensible Authentication Protocol(PEAP)およびTransport Layer Security(TLS)を使用します。 設定するにはステップ9に進んでください。このタイプのセキュリティは、オフィス環境でよく使用され、リモート認証ダイヤルインユーザサービス(RADIUS)サーバを設定する必要があります。ここをクリックして、RADIUSサーバの詳細を確認してください。



注：この例では、[WPA Personal]が選択されています。

ステップ6:[+]をクリックし、[WPA-TKIP]または[WPA2-AES]チェックボックスをオンにして、インフラストラクチャクライアントインターフェイスで使用するWPA暗号化の種類を決定します。

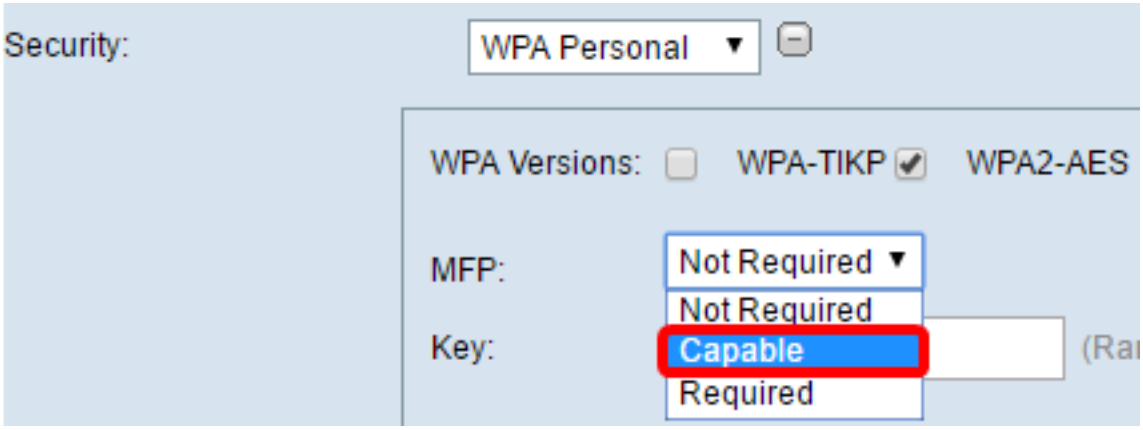
注：すべてのワイヤレス機器がWPA2をサポートしている場合は、インフラストラクチャクライアントのセキュリティをWPA2-AESに設定します。暗号化方式は、WPAの場合はRC4、WPA2の場合はAdvanced Encryption Standard(AES)です。WPA2はより強力な暗号化規格であるため、WPA2を推奨します。この例では、WPA2-AESが使用されています。



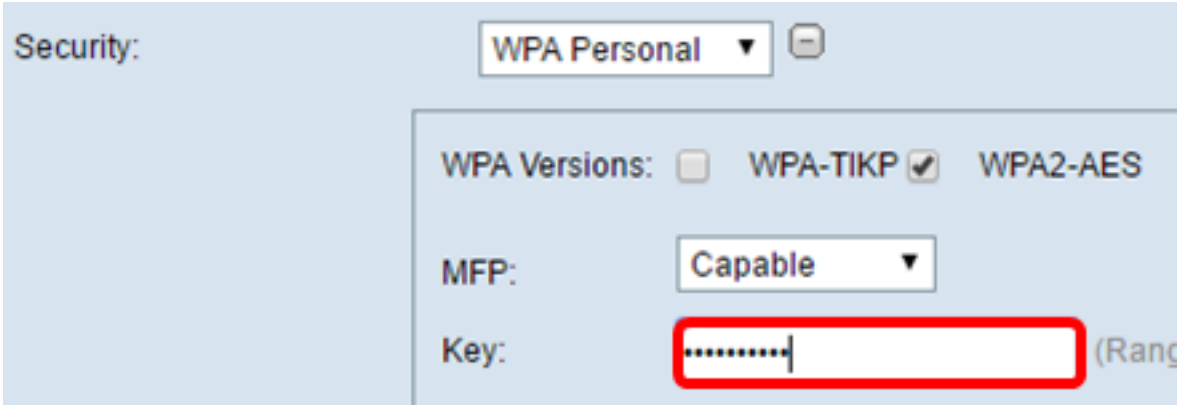
ステップ7:（オプション）ステップ6でWPA2-AESをオンにした場合、WAPで保護フレームを必要とするかどうかを選択するManagement Frame Protection(MFP)ドロップダウンリストからオプションを選択します。MFPの詳細については、ここをクリックしてください。次のオプションがあります。

- Not Required:MFPのクライアントサポートを無効にします。
- Capable:MFP対応クライアントとMFPをサポートしていないクライアントの両方がネットワークに参加できるようにします。これは、WAPのデフォルトのMFP設定です。
- 必須：クライアントは、MFPがネゴシエートされている場合にのみ関連付けを許可されます。デバイスがMFPをサポートしていない場合、ネットワークへの参加は許可されません。

注：この例では、[Capable]が選択されています。



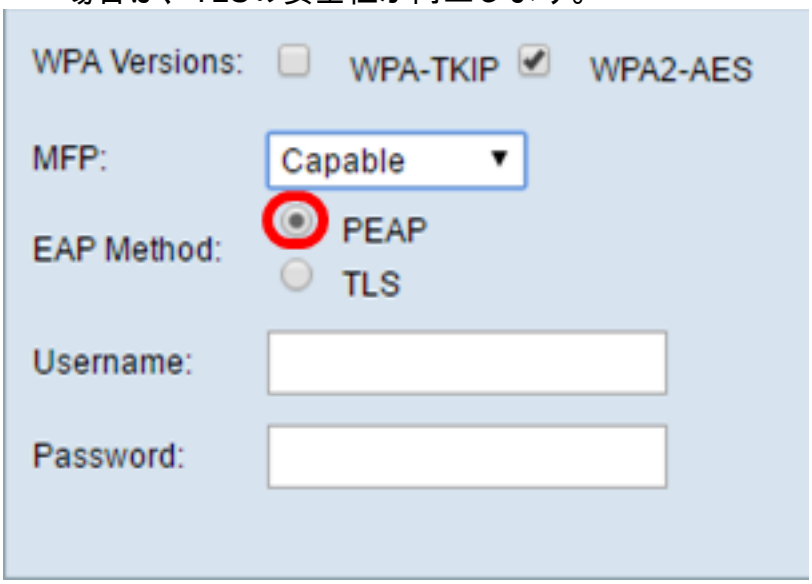
ステップ8:[Key]フィールドにWPA暗号化キーを入力します。キーの長さは8 ~ 63文字である必要があります。これは、文字、数字、特殊文字の組み合わせです。これは、ワイヤレスネットワークに初めて接続するときに使用されるパスワードです。次に、ステップ18に進みます。



ステップ9：ステップ5で[WPA Enterprise]を選択した場合は、[EAP Method]のオプションボタンをクリックします。

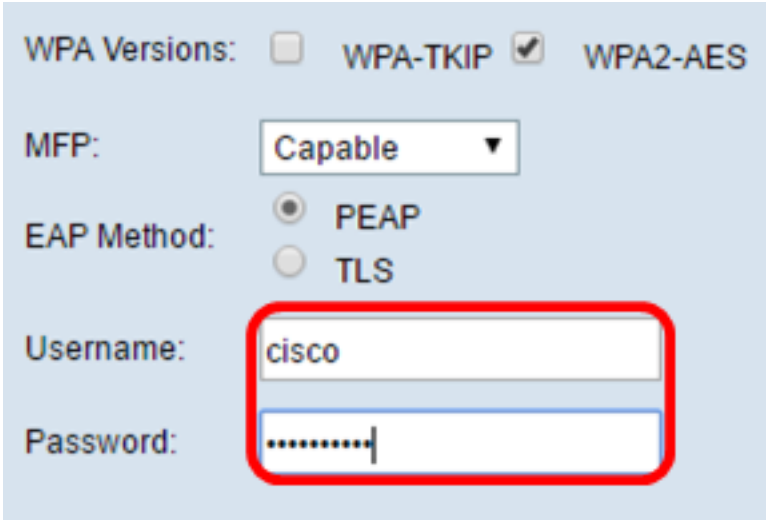
使用可能なオプションは次のように定義されます。

- PEAP：このプロトコルは、AES暗号化規格をサポートするWAPの個々のユーザ名とパスワードの下で各ワイヤレスユーザを提供します。PEAPはパスワードベースのセキュリティ方式であるため、Wi-Fiセキュリティはクライアントのデバイスクレデンシャルに基づいています。PEAPは、パスワードが脆弱な場合や、セキュリティで保護されていないクライアントがある場合に、重大なセキュリティ上のリスクを引き起こす可能性があります。これはTLSに依存しますが、すべてのクライアントにデジタル証明書をインストールすることを回避します。代わりに、ユーザ名とパスワードを使用して認証を行います。
- [TLS]:TLSでは、各ユーザに追加の証明書を持たせてアクセスを許可する必要があります。追加のサーバと、ユーザをネットワークに認証するために必要なインフラストラクチャがある場合は、TLSの安全性が向上します。

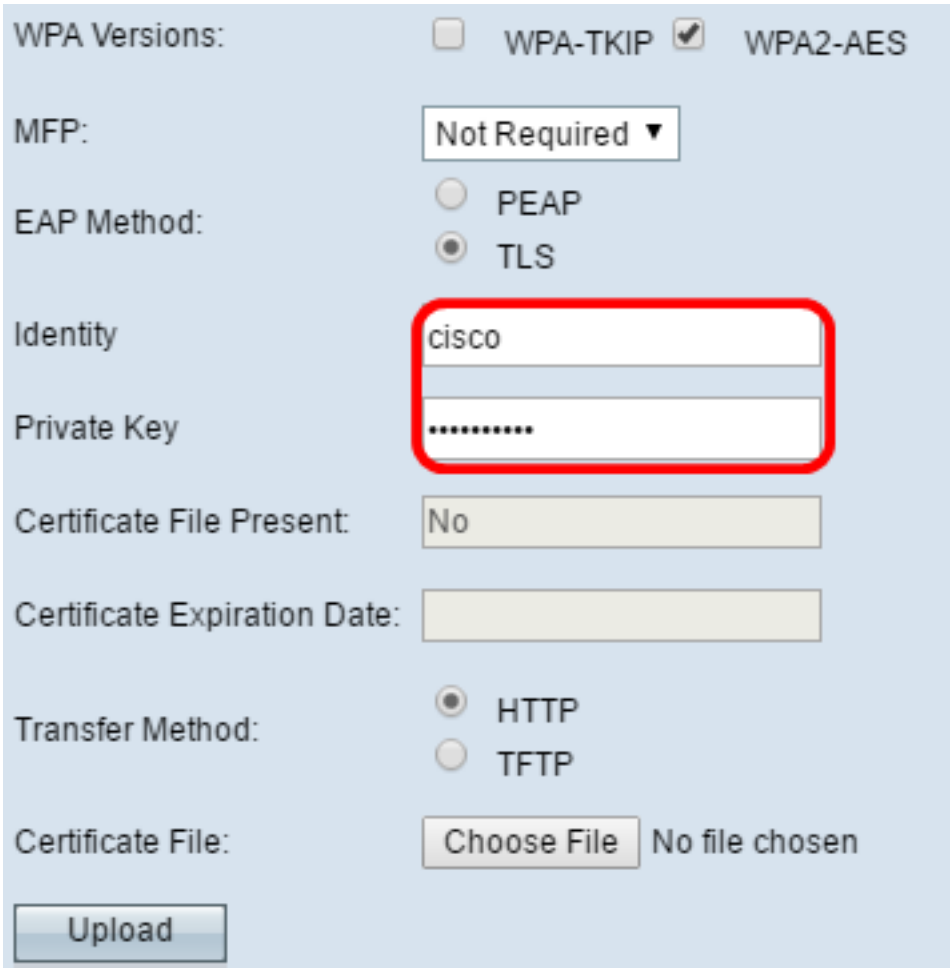


注：この例では、PEAPが選択されています。

ステップ10:[Username]フィールドと[Password]フィールドに、インフラストラクチャクライアントのユーザ名とパスワードを入力します。これは、インフラストラクチャクライアントインターフェイスへの接続に使用されるログイン情報です。この情報については、使用しているインフラストラクチャクライアントインターフェイスを参照してください。次に、ステップ18に進みます。

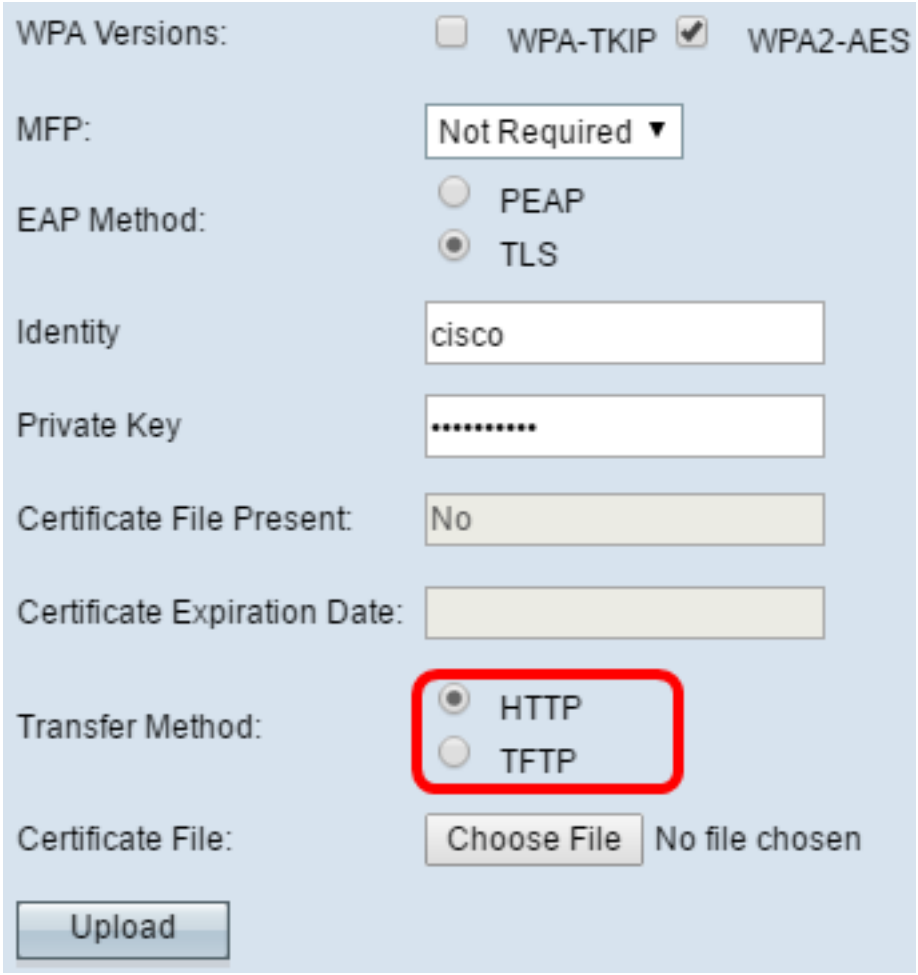


ステップ11：ステップ9でTLSをクリックした場合は、インフラストラクチャクライアントのIDと秘密キーを[ID]フィールドと*[秘密キー]フィールド*に入力します。



ステップ12：転送方法領域で、次のオプションのオプションボタンをクリックします。

- TFTP:Trivial File Transfer Protocol(TFTP)は、File Transfer Protocol(FTP)のセキュリティ保護されていない簡易バージョンです。 主に、ソフトウェアの配布や企業ネットワーク間でのデバイスの認証に使用されます。TFTPをクリックした場合は、ステップ15に進みます。
- HTTP:Hypertext Transfer Protocol（HTTP；ハイパーテキスト転送プロトコル）は、クライアントが認証フレームワークを提供するために使用できる、シンプルなチャレンジ/レスポンス認証フレームワークを提供します。

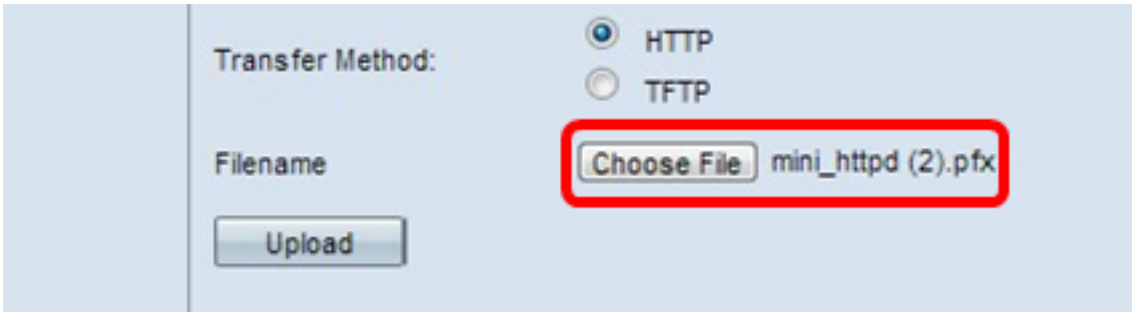


注：証明書ファイルがWAPに既に存在する場合は、[証明書ファイルの存*在(Certificate File Present)]*および[証明書の有効期限(*Certificate Expiration Date)]フィールド*には、すでに関連情報が入力されます。それ以外の場合は空白になります。

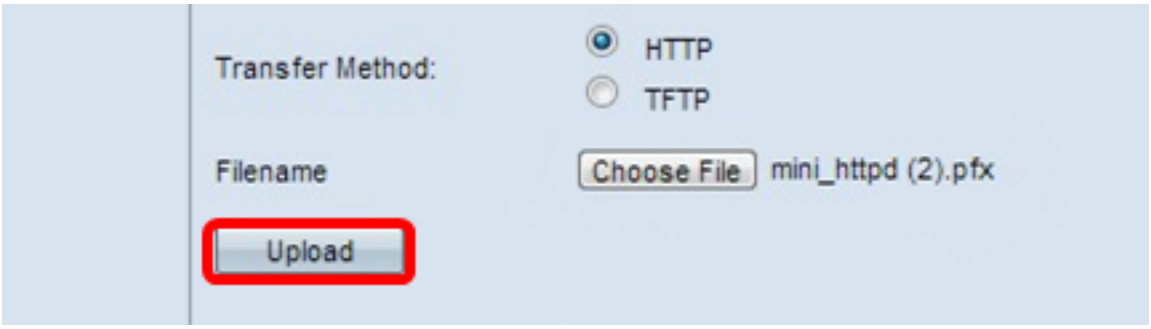
HTTP

ステップ13:[ファイルの選**択]ボタンをク**リックし、証明書ファイルを検索して選択します。ファイルに適切な証明書ファイル拡張子（.pemや.pfxなど）を付ける必要があります。そうしないと、ファイルは受け入れられません。

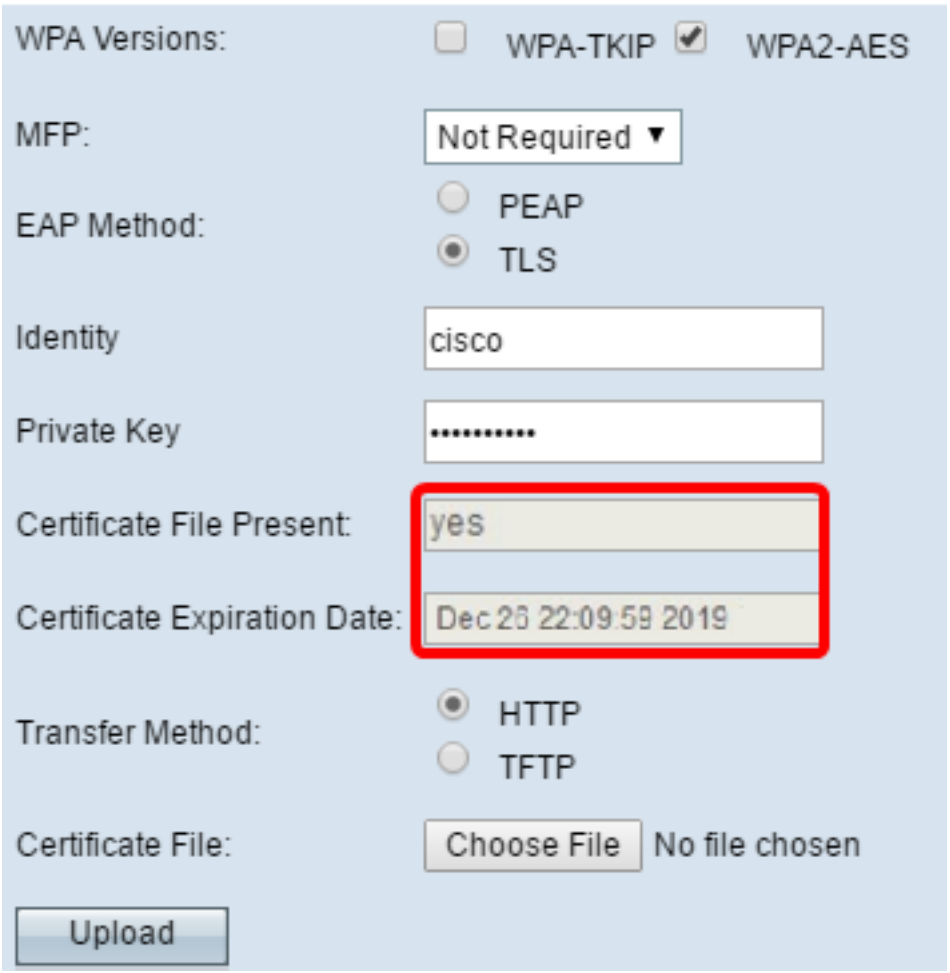
注：この例では、mini_httpd(2).pfxが選択されています。



ステップ14:[Upload]をクリックし、選択した証明書ファイルをアップロードします。ステップ 18 に進みます。



[証明書ファイルの存在]フィールドと[証明書の有効期限]フィールドは自動的に更新されます。



TFTP

ステップ15:ステップ12でTFTPをクリックした場合、証明書ファイルのファイル名を[ファイル名]フィールドに入力します。

注：この例では、mini_httpd.pemが使用されています。

ステップ16:[TFTP Server IPv4 Address]フィールドにTFTPサーバアドレスを入力します。

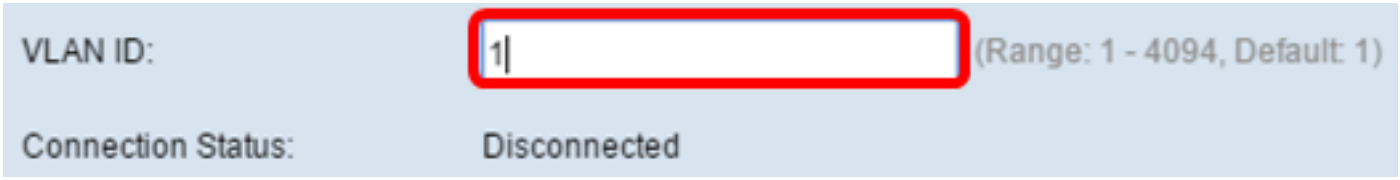
注：この例の場合は.TFTPサーバアドレスとして192.168.1.20が使用されます。

ステップ17:[アップロード]ボタンをクリックして、指定した証明書ファイルをアップロードします。

[証明書ファイルの存在]フィールドと[証明書の有効期限]フィールドは自動的に更新されます。

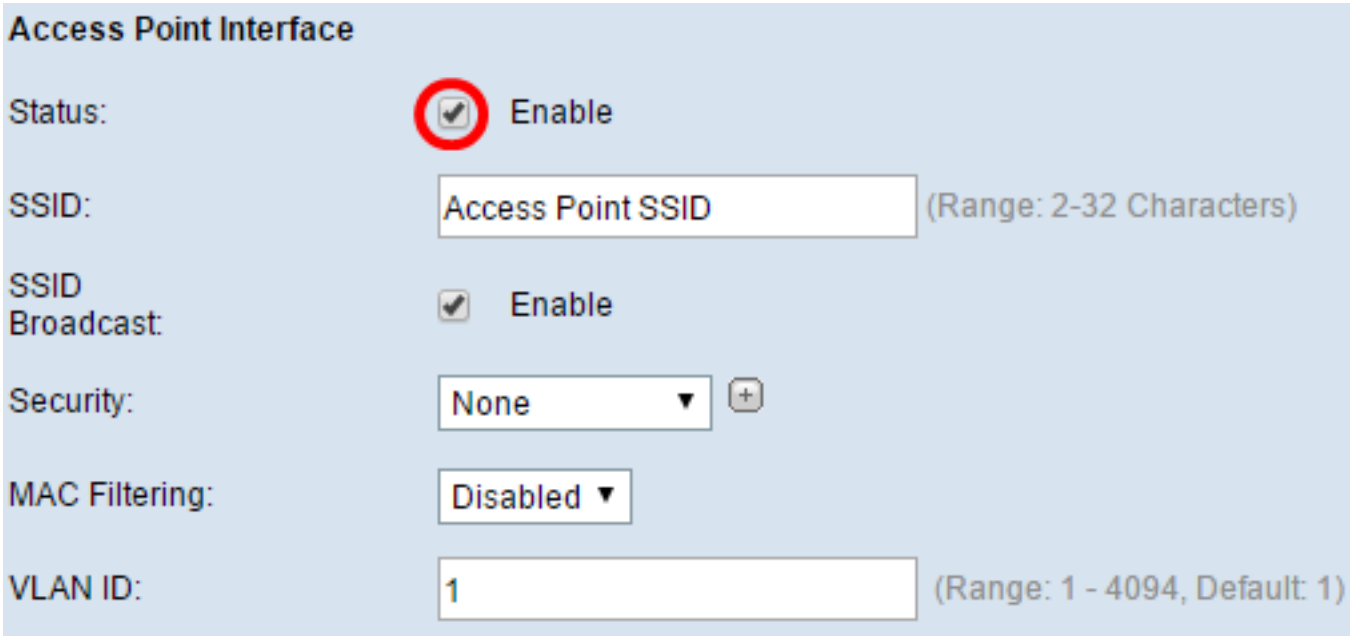
ステップ18：インフラストラクチャのクライアントインターフェイスのVLAN IDを入力します。デフォルトは 1 です。

注：この例では、デフォルトのVLAN IDが使用されます。



アクセスポイントインターフェイス

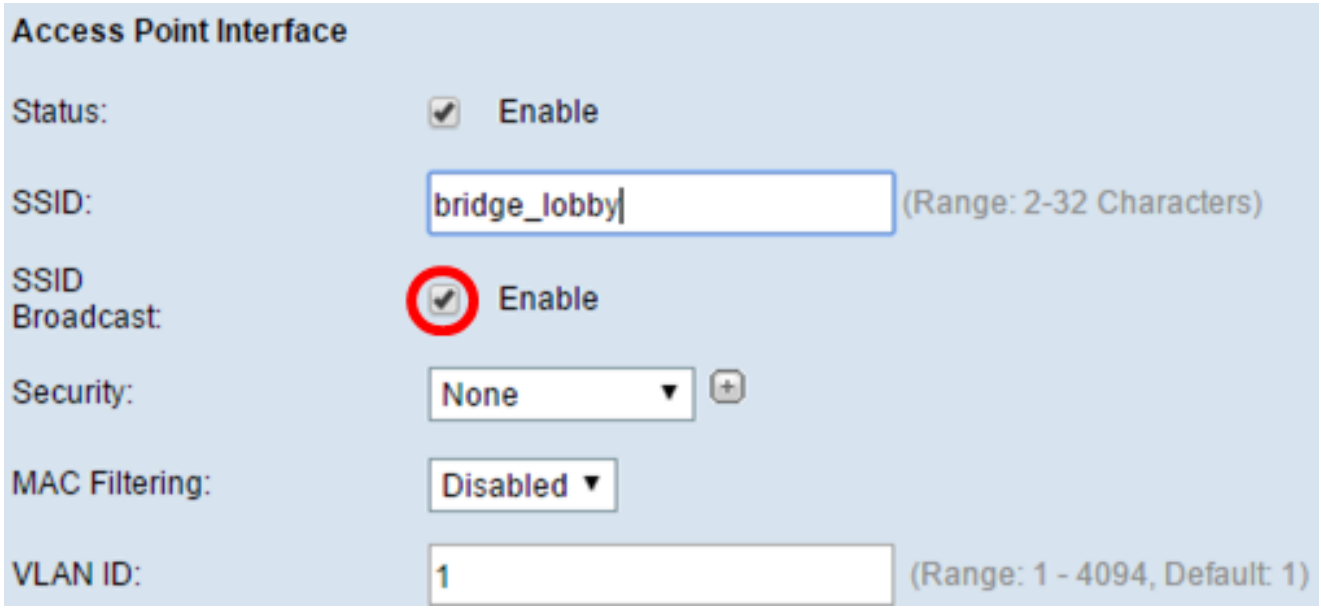
ステップ1：アクセスポイントインターフェイスでブリッジングを有効にするには、[Enable Status]チェックボックスをオンにします。



ステップ2:[SSID]フィールドにアクセスポイントのSSIDを入力します。SSIDの長さは2 ~ 32文字である必要があります。デフォルトはアクセスポイントのSSIDです。

注：この例では、使用するSSIDはbridge_lobbyです。

ステップ3:（オプション）SSIDをブロードキャストしない場合は、[SSIDブロードキャストを有効にする]チェックボックスをオフにします。これを行うと、アクセスポイントはワイヤレスアクセスポイントを検索するユーザからは見えなくなります。SSIDをすでに知っているユーザだけが接続できます。SSIDブロードキャストはデフォルトで有効になっています。

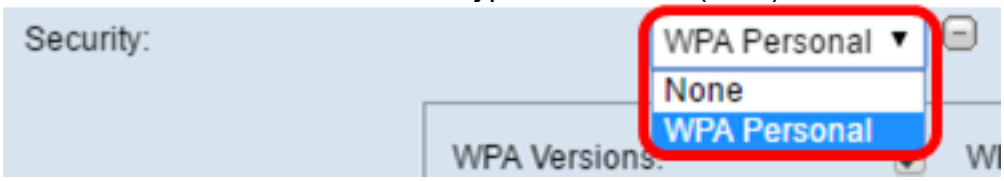


ステップ4:[Security]ドロップダウンリストから、ダウンストリームクライアントステーションをWAPに対して認証するセキュリティのタイプを選択します。

使用可能なオプションは次のように定義されます。

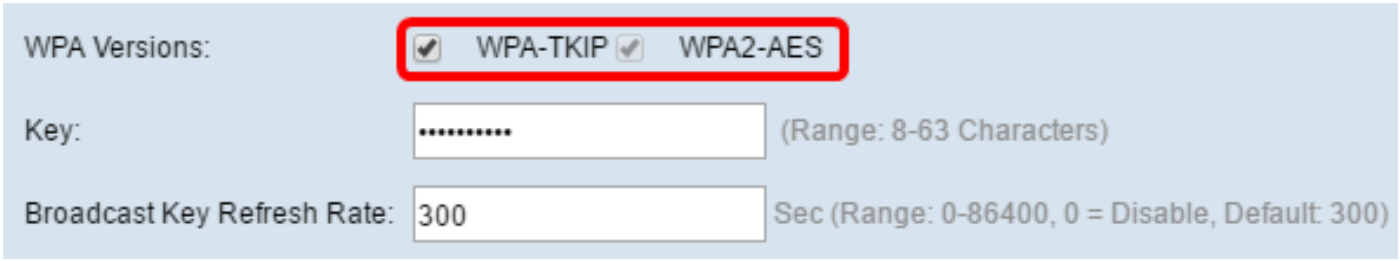
- [なし(None)]：セキュリティを開くか、なし。これがデフォルト値です。これを選択する場合は、ステップ10に進みます。
- WPA Personal:Wi-Fi Protected Access(WPA)Personalは8 ~ 63文字のキーをサポートできます。暗号化方式は、TKIPまたはCounter Cipher Mode with Block Chaining Message

Authentication Code Protocol(CCMP)のいずれかです。CCMPを使用するWPA2は、64ビットのRC4標準のみを使用するTemporal Key Integrity Protocol(TKIP)に比べて、より強力な暗号化規格であるAdvanced Encryption Standard(AES)を備えているため、推奨されます。

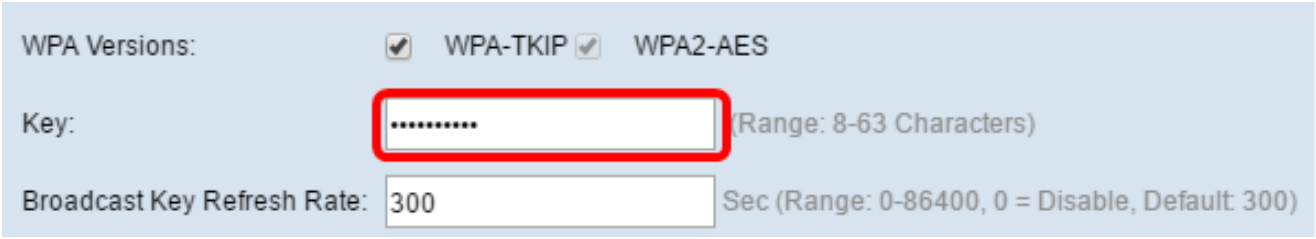


ステップ5:[**WPA-TKIP**]または[**WPA2-AES**]チェックボックスをオンにして、アクセスポイントインターフェイスが使用するWPA暗号化の種類を決定します。これらはデフォルトで有効になっています。

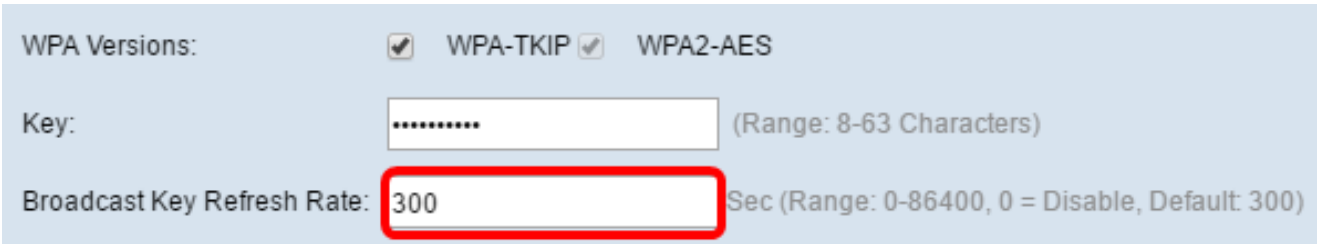
注：すべてのワイヤレス機器がWPA2をサポートしている場合は、インフラストラクチャクライアントセキュリティをWPA2-AESに設定します。暗号化方式は、WPAの場合はRC4、WPA2の場合はAdvanced Encryption Standard(AES)です。WPA2はより強力な暗号化規格であるため、WPA2を推奨します。この例では、WPA2-AESが使用されています。



ステップ6:[Key]フィールドに共有WPAキーを入力します。キーの長さは8 ~ 63文字で、英数字、大文字と小文字、特殊文字を使用できます。



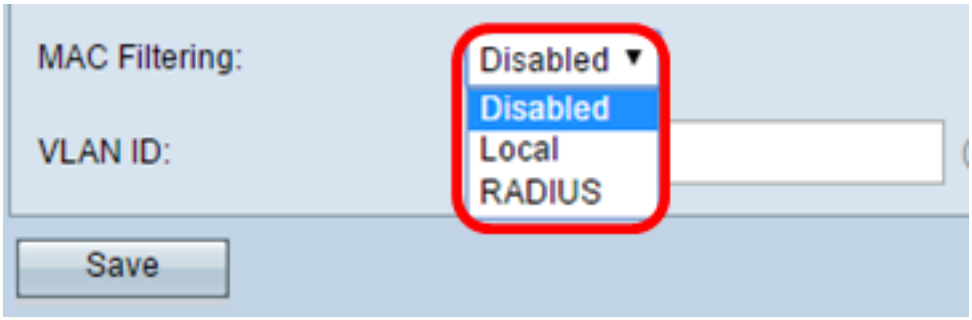
ステップ7:[Broadcast Key Refresh Rate]フィールドにレートを入力します。ブロードキャストキーリフレッシュレートは、このアクセスポイントに関連付けられているクライアントのセキュリティキーがリフレッシュされる間隔を指定します。レートは0 ~ 86400の範囲で、値0を指定すると機能が無効になります。デフォルト値は 300 です。



ステップ8:[MAC Filtering]ドロップダウンリストから、アクセスポイントインターフェイスに設定するMACフィルタリングのタイプを選択します。有効にすると、ユーザは、使用しているクライアントのMACアドレスに基づいて、WAPへのアクセスを許可または拒否されます。

使用可能なオプションは次のように定義されます。

- [Disabled]：すべてのクライアントがアップストリームネットワークにアクセスできます。これがデフォルト値です。
- Local：アップストリームネットワークにアクセスできるクライアントセットは、ローカルに定義されたMACアドレスリストで指定されたクライアントに制限されます。
- RADIUS：アップストリームネットワークにアクセスできるクライアントセットは、RADIUSサーバのMACアドレスリストで指定されたクライアントに制限されます。

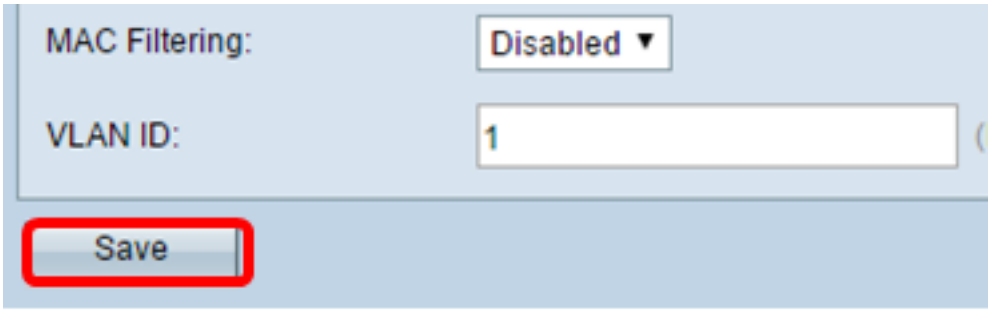


注：この例では、[Disabled]が選択されています。

ステップ9：アクセスポイントインターフェイスのVLAN ID*フィールド*にVLAN IDを入力します。

注：パケットのブリッジングを許可するには、アクセスポイントインターフェイスと有線インターフェイスのVLAN設定が、インフラストラクチャクライアントインターフェイスのVLAN設定と一致している必要があります。

ステップ10:[保存]を**クリック**して、変更を保存します。



これで、ワイヤレスアクセスポイントでWorkGroup Bridgeを正しく設定できました。