WAP125 または WAP581 の 802.1X サプリカント設定を設定して下さい

目標

サプリカントは 802.1X IEEE規格の 3 つの口ールの 1 つです。 802.1X は OSI モデルのレイヤ2のセキュリティを提供するために開発されました。 それは次のコンポーネントで構成されています: サプリカント、オーセンティケータおよび認証サーバ。 サプリカントはリソースにアクセスできるようにネットワークに接続するソフトウェアまたはクライアントです。 それは IP アドレスを得、その特定のネットワークの一部であるために資格情報か証明書を提供する必要があります。 サプリカントはネットワークリソースに認証されるまでアクセスできることができません。

この技術情報は 802.1X サプリカントで WAP125 か WAP581 アクセス ポイントを設定する方法を示します。

注: 学ぶためにスイッチの 802.1X サプリカント 資格情報を設定する方法をここをクリックして下さい。

適当なデバイス

- WAP125
- WAP581

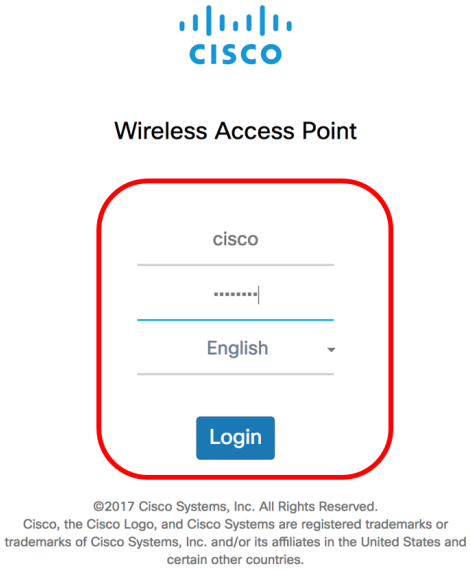
[Software Version]

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

802.1X サプリカントを設定して下さい

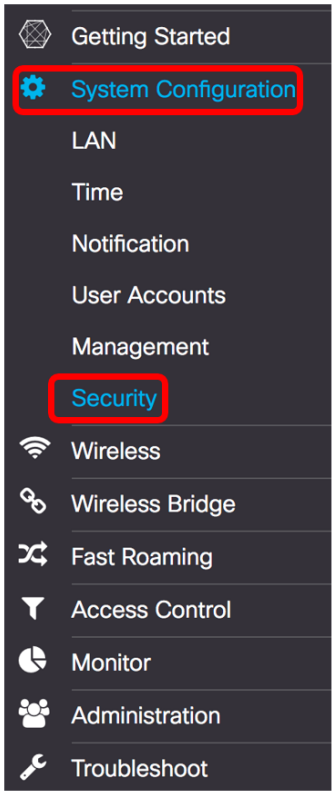
サプリカント 資格情報を設定して下さい

ステップ 1. WAP の Webベース ユーティリティへのログイン。 デフォルトのユーザ名およびパスワードは cisco/cisco です。



注: 既にパスワードを変更するか、または新しいアカウントを作成している場合、新しい資格情報を代りに入力して下さい。

ステップ 2. **> Security を**『System Configuration』 を選択 して下さい。

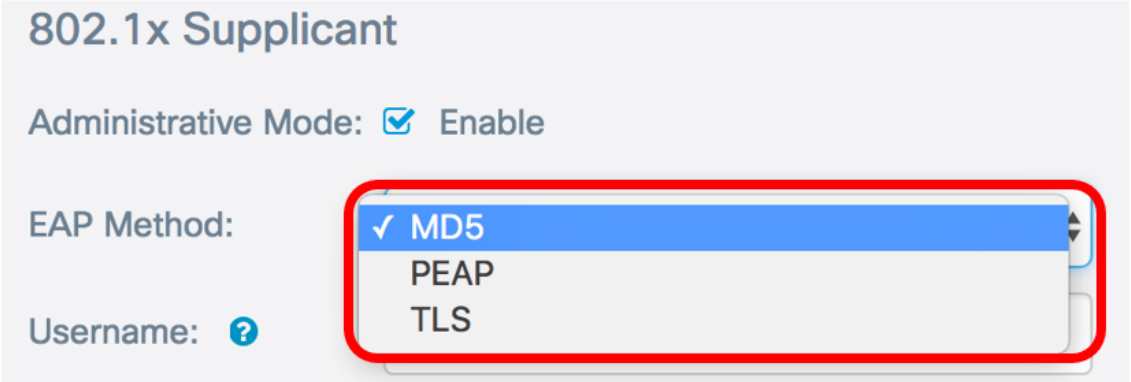


ステップ 3 管理モードを有効に するために **Enable チェックボックスを**チェックして下さい。 これはオーセンティケータにサプリカントとして機能することを WAP が可能にします。

ステップ 4. *EAP 方式* ドロップダウン リストからのユーザ名 および パスワードを暗号化するのに使用する Extensible Authentication Protocol（EAP） 方式の適切な型を選択して下さい。 次のオプションがあります。

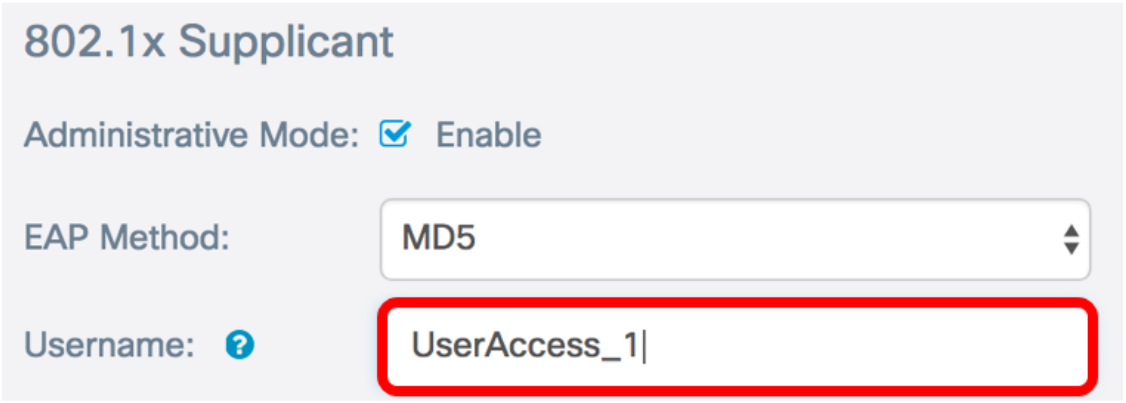
- MD5 — 128 ビット 暗号化の方法を使用します。 MD5 アルゴリズムは公共暗号システムをデータを暗号化するのに使用します。
- PEAP — Protected Extensible Authentication Protocol （PEAP）はクライアントと認証サーバ間の暗号化された SSL/TLS トンネルの作成によるサーバによって発行されるデジタル証明書を通して Wireless LAN クライアントを認証します。
- TLS： Transport Layer Security （TLS）はプロトコルですインターネット上の通信にセキュリティおよびデータ統合を提供する。 サード パーティが元のメッセージを不正変更しないようにします。

注: この例では、MD5 は使用されます。

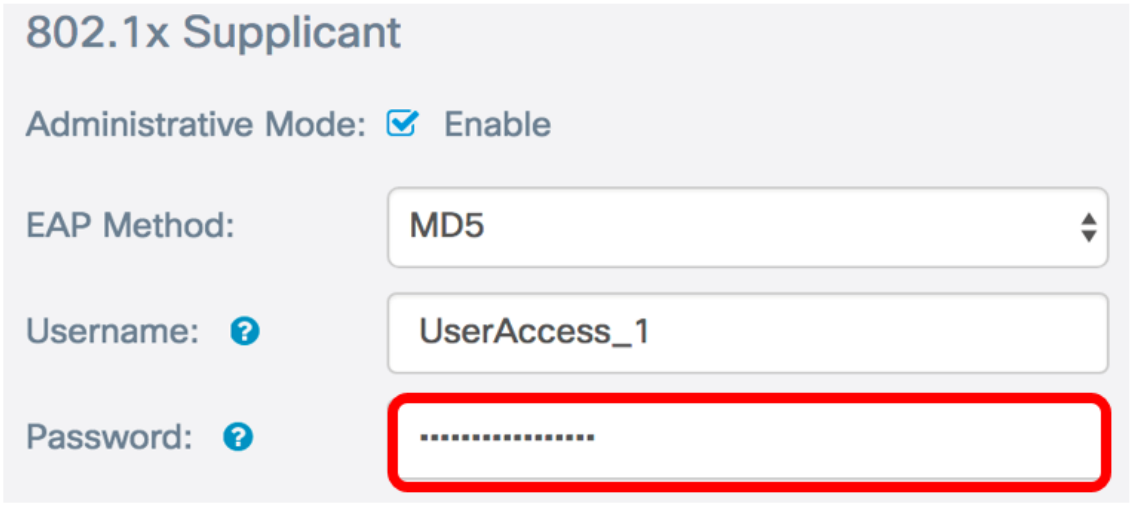


ステップ 5. *Username フィールド*でユーザ名を入力して下さい。 これはオーセンティケータで設定されたで、802.1X オーセンティケータに応答するのに使用されていますユーザ名。 それは長く 1 から 64 文字である場合もありましたり二重引用符を除く大文字および小文字、数および特殊文字含むかもしれません。

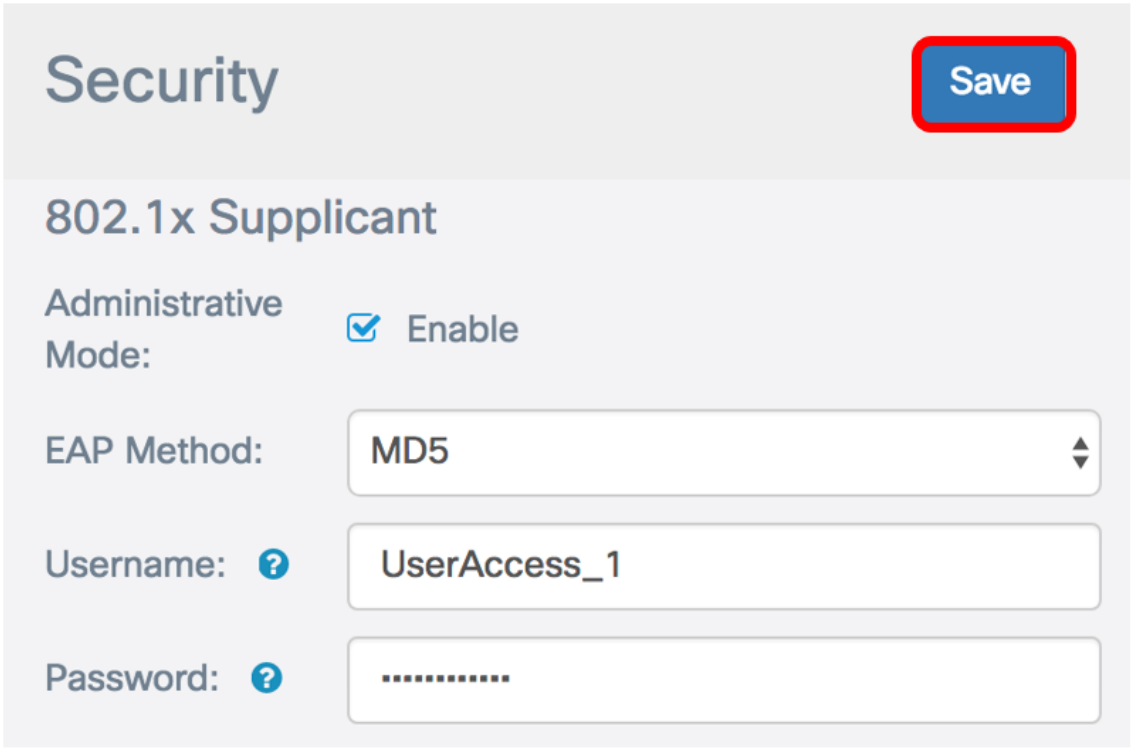
注: この例では、UserAccess_1 は使用されます。



ステップ 6.ユーザ名と関連付けられる *Password フィールド*でパスワードを入力して下さい。802.1X オーセンティケータに応答するのにこの MD5 パスワードが使用されています。 パスワードは長く 1 から 64 文字である場合もありましたり引用符を除く大文字および小文字、数および特殊文字含むかもしれません。



ステップ 7.行われた設定を保存するために **SAVE ボタンを**クリックして下さい。



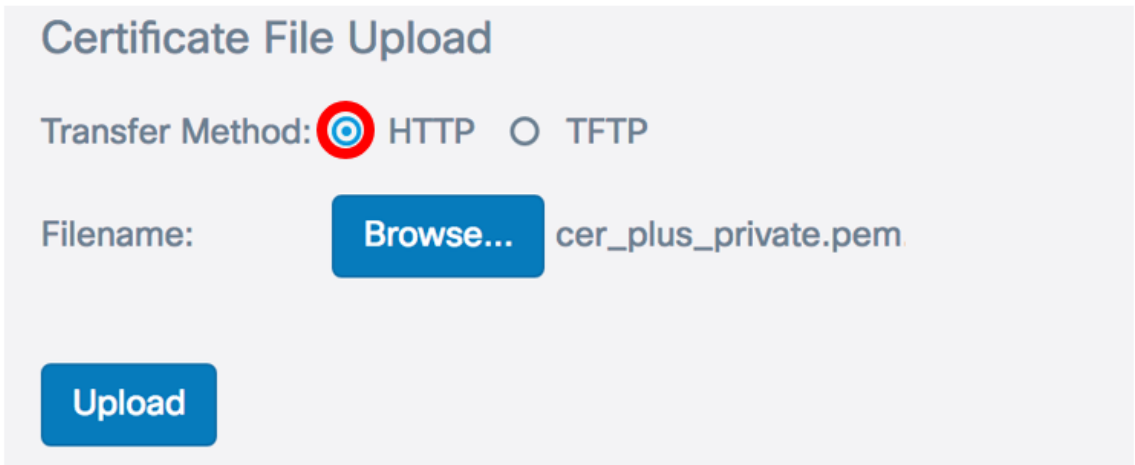
今 WAP の 802.1X サプリカント設定を行う必要があります。

証明書ファイル アップ ロード

ステップ 1： 転送方式から、SSL 証明書を得るのに WAP が使用する方式を選択して下さい。 SSL 証明書は認証局によって Webブラウザが Webサーバのセキュアコミュニケーションがあるようにするデジタルで 署名入り認証行います。 次のオプションがあります。

- HTTP： 証明書は Hyper Text Transfer Protocol （ HTTP ）によってまたはブラウザによってアップ ロードされます。
- TFTP - 証明書はトリビアル ファイル転送プロトコル（ TFTP ） サーバによってアップ ロードされます。 これが選択される場合、ステップ 3.にスキップして下さい。 ファイル名および TFTP アドレスを入力するために必要となります。

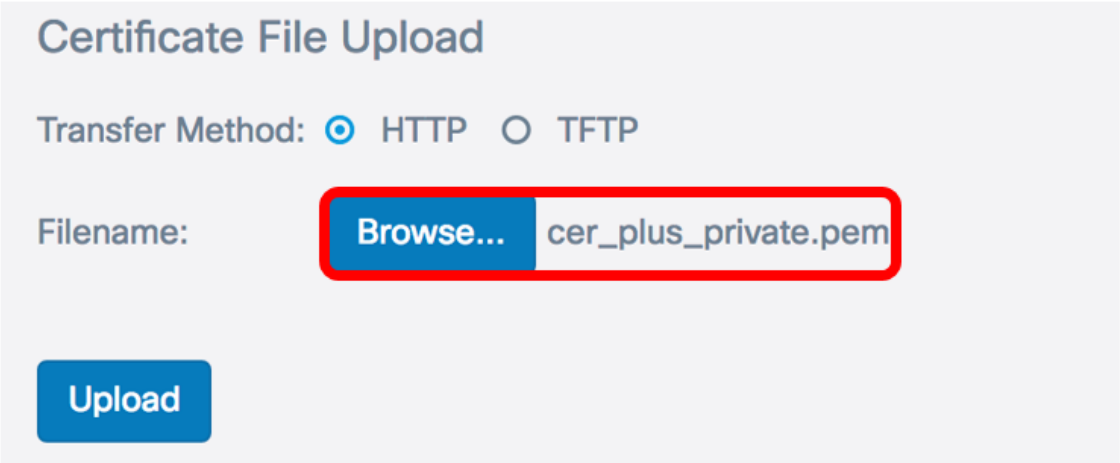
注: この例では、HTTP は選択されます。



HTTP 転送方式

『HTTP』 を選択 する場合ステップ 2.（ オプションの ）は、... 『Browse』 をクリック し、SSL 証明書を選択します。

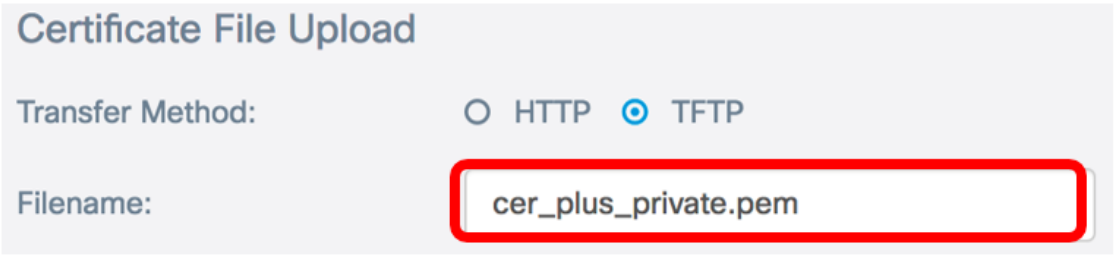
注: この例では、cer_plus_private.pem は使用されます。



TFTP 転送 方式

ステップ 3 ステップ 1 の TFTP を選択する場合、Filename フィールドでファイルの名前を入力して下さい。

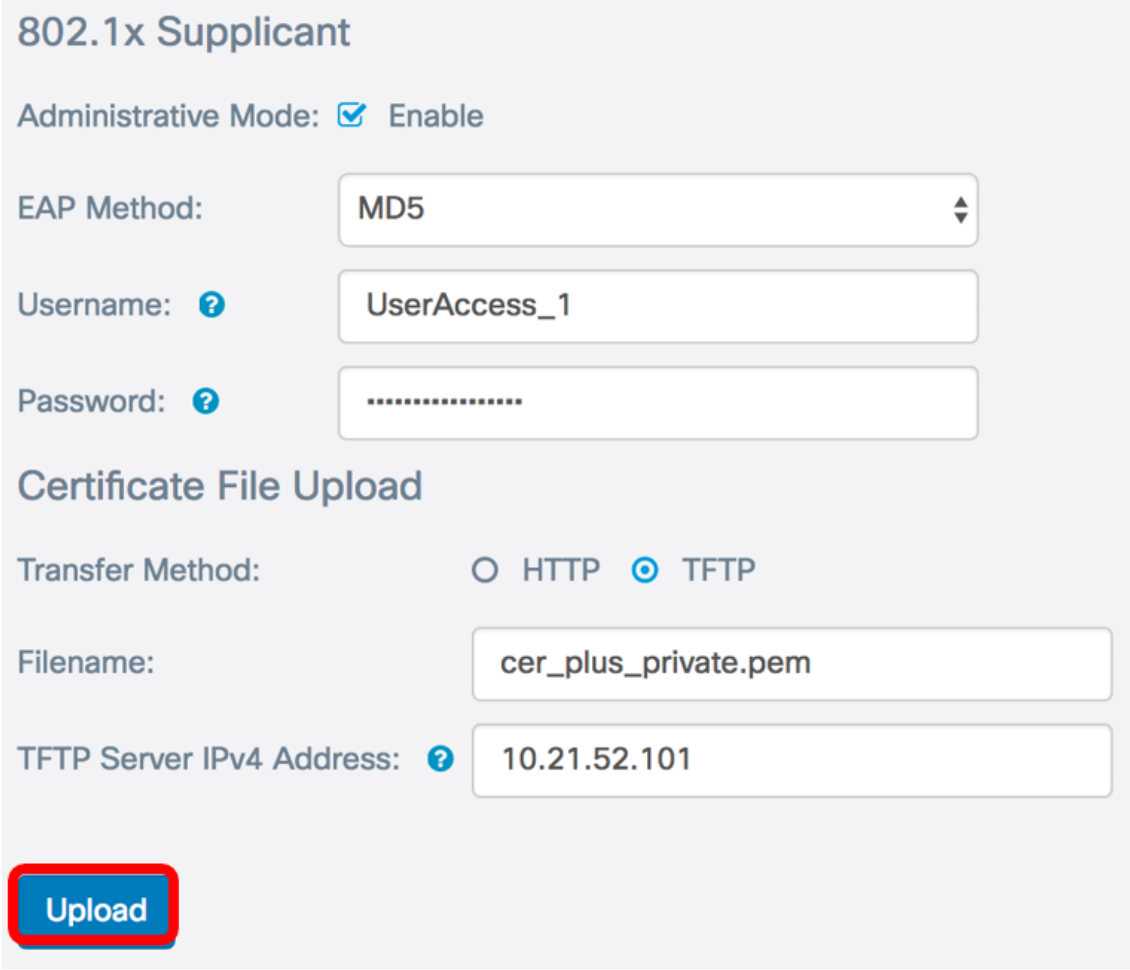
注: この例では、cer_plus_private.pem は使用されます。



TFTP が転送方式として選択される場合ステップ 4.（ オプションの ）は *TFTPサーバ IPv4 Address フィールド*で、TFTPサーバの IPv4 アドレスを入力します。 これは証明書を取得するのに WAP が使用するパスです。

注: この例では、10.21.52.101 は使用されます。

ステップ 5. 『Upload』 をクリック して下さい。



今正常に WAP の証明書をアップ ロードする必要があります。