

# ワイヤレスアクセスポイントでの802.1Xサブリカントの設定

## 目的

802.1X規格は、オープンシステム相互接続(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。次のコンポーネントで構成されています。サブリカント、オーセンティケータ、および認証サーバ。サブリカントは、ネットワークに接続してリソースにアクセスできるクライアントまたはソフトウェアです。IPアドレスを取得し、その特定のネットワークの一部となるクレデンシャルまたは証明書を提供する必要があります。サブリカントは、認証されるまでネットワークリソースにアクセスできません。

ワイヤレスアクセスポイント(WAP)で802.1Xサブリカント設定を設定すると、WAPの背後にある許可デバイスがネットワークの一部になり、そのリソースにアクセスできるようになります。同時に、ネットワークにセキュリティのレイヤも追加します。

この記事では、ワイヤレスアクセスポイントで802.1Xサブリカント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

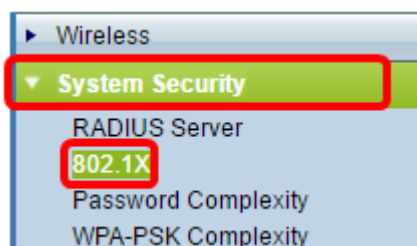
## [Software Version]

- 1.0.1.2 - WAP150、WAP361
- 1.0.6.2 - WAP121、WAP321
- 1.0.2.2 - WAP131、WAP351
- 1.2.1.3 - WAP551、WAP561、WAP371
- 1.0.0.17 - WAP571、WAP571E

## WAPでの802.1Xサブリカントの設定

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、[System Security] > [802.1X]を選択します。

注：Webベースのユーティリティメニューは、WAPのモデルによって異なる場合があります。次の画像は、WAP361から取得したものです。



注：WAPの他のモデルを使用している場合は、System Security > 802.1X Supplicantの順に選択し、[Step 3に進みます](#)。

ステップ2：設定するポート番号のチェックボックスをオンにし、[Edit]をクリックします。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

ステップ3:[Enable]チェックボックスをオンにし、ドロップダウンリストから[Supplicant]を選択します。これはデフォルトのオプションです。

注：WAPの他のモデルの場合は、管理モードのEnableチェックボックスをオンにし、ステップ5に進みます。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼ Supplicant	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Authenticator	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

ステップ4:[詳細の表示]リンクをクリックして、設定を編集できます。

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

ステップ5:[EAP Method]ドロップダウンリストから、適切なタイプのExtensible Authentication Protocol(EAP)方式を選択します。

EAP Method:  (Range: 1 - 64 Characters)

Username:  (Range: 1 - 64 Characters)

Password:  (Range: 1 - 64 Characters)

次のオプションがあります。

- MD5:MD5は、任意のサイズのデータを128ビットに暗号化するために使用されるアルゴリズムです。MD5アルゴリズムは、公開暗号システムを使用してデータを暗号化します。
- PEAP:Protected Extensible Authentication Protocol(PEAP)は、クライアントと認証サーバ間に暗号化されたSecure Sockets Layer(SSL)またはTransport Layer Security(TLS)トンネルを作成して、サーバが発行するデジタル証明書を使用して無線LAN(WLAN)クライアントを認証します。
- TLS:TLSは、インターネット上の通信にセキュリティとデータの整合性を提供するプロトコルです。これにより、元のメッセージを第三者に改ざんされることがなくなります。

注：この例では、MD5が使用されています。

ステップ6:[ユーザ名]フィールドに希望のユーザ名を入力します。これは、802.1X Authenticatorに応答するとき使用されます。最大64文字まで使用でき、大文字と小文字、数字、および二重引用符を除く特殊文字を使用できます。

EAP Method:  (Range: 1 - 64 Characters)

Username:  (Range: 1 - 64 Characters)

Password:  (Range: 1 - 64 Characters)

ステップ7:[Password]フィールドに優先パスワードを入力します。このMD5パスワードは、802.1Xオーセンティケータに応答するとき使用されます。パスワードは最大64文字で、大文字と小文字、数字、および引用符を除く特殊文字を含めることができます。

EAP Method:  (Range: 1 - 64 Characters)

Username:  (Range: 1 - 64 Characters)

Password:  (Range: 1 - 64 Characters)

ステップ8：ボタンをクリック  クします。

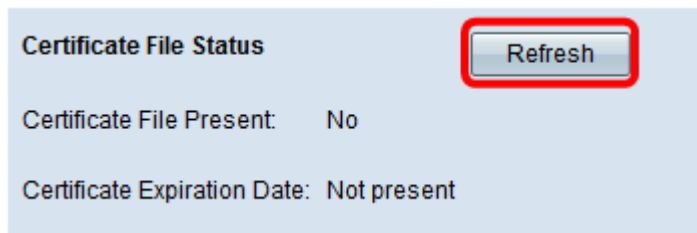
これで、WAPで802.1Xサブクライアントの設定が完了したはずですが。

証明書ファイル設定の表示

[Certificate File Status]領域には、証明書ファイルが存在するかどうかが表示されます。SSL証明書は、WebブラウザがWebサーバと安全に通信できるようにする認証局によってデジタル署名された証明書です。

ステップ1：証明書ファイルの現在のステータスを表示するには、[更新]をクリックします

。



Certificate File Status

Refresh

Certificate File Present: No

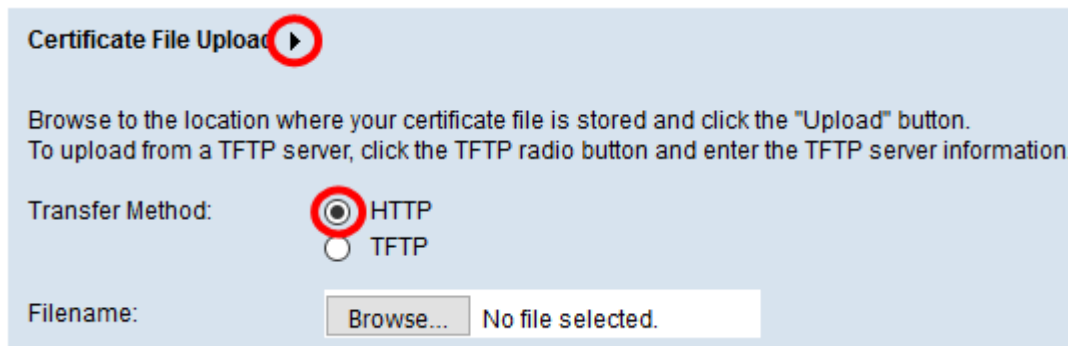
Certificate Expiration Date: Not present

[Certificate File Status]領域には、次のフィールドがあります。

- Certificate File Present : 証明書ファイルが存在するかどうかを表示します。
- [証明書の有効期限(Certificate Expiration Date)] : 現在の証明書ファイルの有効期限が表示されます。

### 証明書ファイルのアップロード

ステップ1:[Certificate File Upload]の横にある矢印をクリックし、[Transfer Method]から目的のオプションボタンを選択します。



Certificate File Upload ▶

Browse to the location where your certificate file is stored and click the "Upload" button.  
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method:  HTTP  TFTP

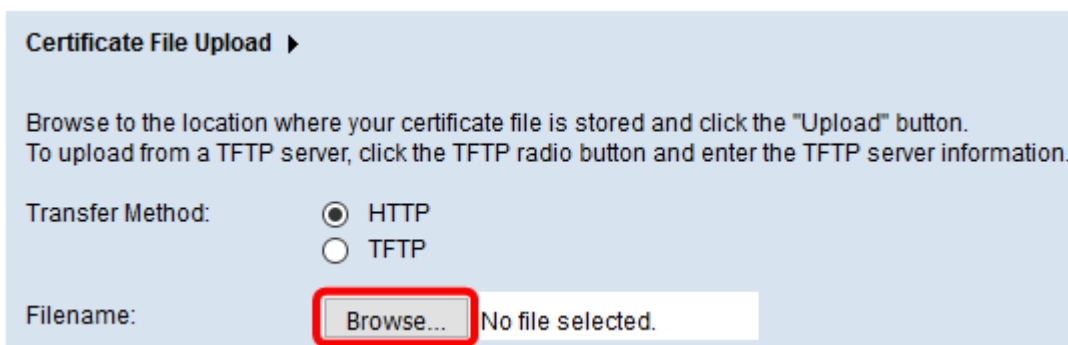
Filename:  No file selected.

ファイルのアップロードには、次の2つの転送方法があります。

- ハイパーテキスト転送プロトコル ( HTTP )
- Trivial File Transfer Protocol ( TFTP )

注 : この例では、HTTPが選択されています。

ステップ2: ( オプション ) HTTPが選択されている場合は、[参照]をクリックしてコンピュータから証明書ファイルを選択し、ステップ5に進みます。



Certificate File Upload ▶

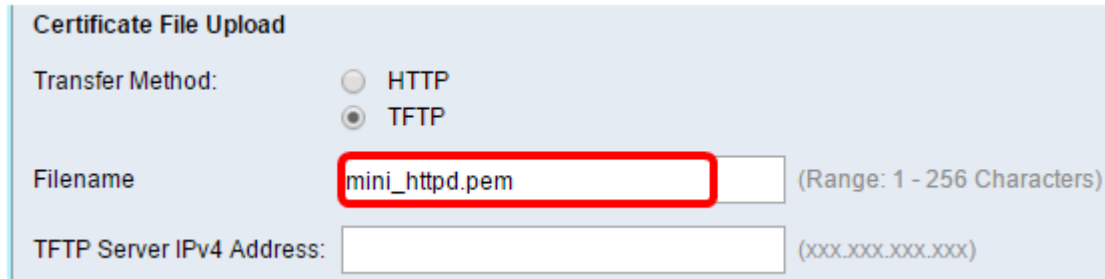
Browse to the location where your certificate file is stored and click the "Upload" button.  
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method:  HTTP  TFTP

Filename:  No file selected.

ステップ3: ( オプション ) ステップ1でTFTPを選択した場合は、[ファイル名]フィールドに証明書ファイルの名前を入力します。TFTPサーバは、デバイス内でブートファイルを自動的に転送するために使用され、非常にシンプルです。

注：この例では、ファイル名として`mini_httpd.pem`が使用されています。



Certificate File Upload

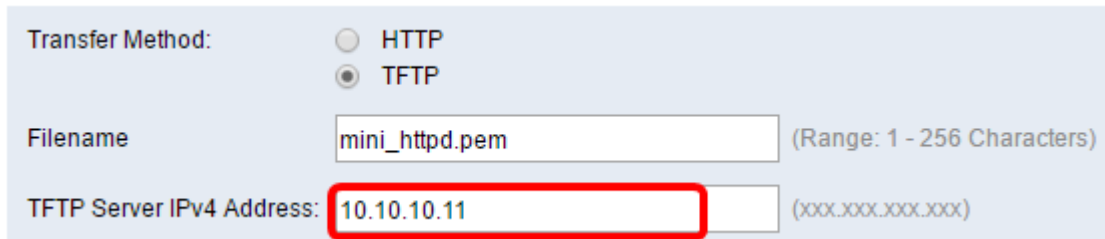
Transfer Method:  HTTP  
 TFTP

Filename:  (Range: 1 - 256 Characters)

TFTP Server IPv4 Address:  (xxx.xxx.xxx.xxx)

ステップ4:[TFTP Server IPv4 Address]フィールドにTFTPサーバのIPアドレスを入力します。

注：この例では、TFTPサーバのIPv4アドレスとして`10.10.10.11`が使用されています。

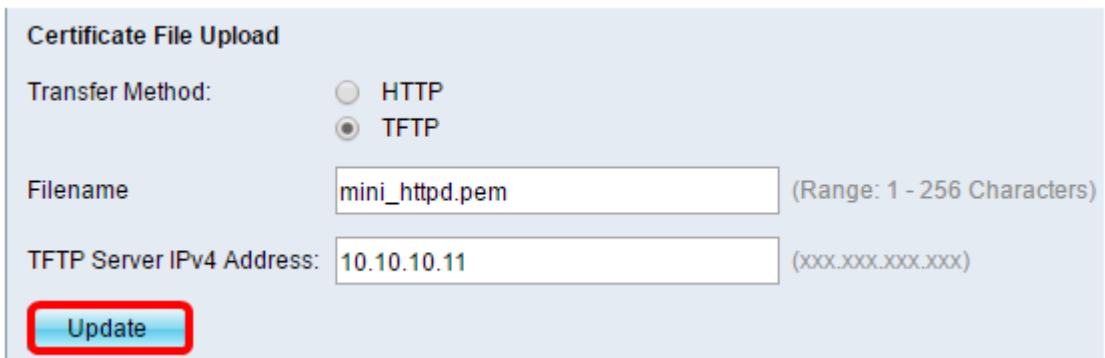


Transfer Method:  HTTP  
 TFTP

Filename:  (Range: 1 - 256 Characters)

TFTP Server IPv4 Address:  (xxx.xxx.xxx.xxx)

ステップ5:[Update]をクリックします。



Certificate File Upload

Transfer Method:  HTTP  
 TFTP

Filename:  (Range: 1 - 256 Characters)

TFTP Server IPv4 Address:  (xxx.xxx.xxx.xxx)

注：WAPの他のモデルを使用している場合は、[アップロード]をクリックします。

ステップ6：ボタンをクリックし  て、設定を保存します。

これで、WAPに証明書ファイルが正常にアップロードされたはずです。