

WAP551およびWAP561アクセスポイントでのHTTP/HTTPSサービスの設定とSecure Socket Layer(SSL)証明書の生成

目的

アクセスポイントは、HTTP/HTTPSサーバが設定されている場合、HTTP接続とHTTPセキュア(HTTPS)接続の両方で管理できます。Hyper Text Transfer Protocol Secure(HTTPS)は、HTTPよりも安全な転送プロトコルです。HTTPSサービスを使用するには、アクセスポイントに有効なSSL証明書が必要です。SSL証明書は、WebブラウザがWebサーバとセキュアで暗号化された通信を行うことを可能にする、認証局によるデジタル署名付き証明書です。

この記事では、HTTP/HTTPSサービスを設定する方法と、WAP551およびWAP561アクセスポイントでSecure Socket Layer(SSL)証明書を作成する方法について説明します。

適用可能なデバイス

- WAP551
- WAP561

[Software Version]

- 1.1.0.4

HTTP/HTTPSサービスの設定

ステップ 1 : Web設定ユーティリティにログインし、Administration > HTTP/HTTPS Serviceの順に選択します。HTTP/HTTPSサービスページが開きます。

HTTP/HTTPS Service

Global Settings

Maximum Sessions: (Range: 1-10, Default: 5)

Session Timeout: Minute (Range: 1-60, Default: 10)

HTTP Service

HTTP Server: Enable

HTTP Port: (Range: 1025-65535, Default: 80)

Redirect HTTP to HTTPS:

HTTPS Service

HTTPS Server: Enable

HTTPS Port: (Range: 1025-65535, Default: 443)

Generate SSL Certificate

ステップ 2 : Maximum SessionsフィールドにWebセッションの最大数を入力します。これは、Web設定ユーティリティにログインできるユーザの最大数を示します。

ステップ 3 : Session Timeoutフィールドに、非アクティブなユーザがAP Web設定ユーティリティにログオン状態を維持できる最大時間を入力します。

ステップ 4 : HTTP経由のWebアクセスをイネーブルにするには、HTTPサーバのEnableチェックボックスにチェックマークを付けます。HTTPサーバはデフォルトで有効になっています。

注：HTTPサーバが無効になっている場合は、HTTPを使用する現在の接続はすべて切断されます。

ステップ 5：HTTPポートフィールドに、HTTP接続に使用するポート番号を入力します。ポート番号80は通常、HTTP接続に使用されます。

ステップ6: (オプション) HTTPポートでの管理HTTPアクセス試行をHTTPSポートにリダイレクトする場合は、Redirect HTTP to HTTPSチェックボックスにチェックマークを付けます。このフィールドは、HTTPアクセスが無効な場合にのみ有効にできます。

手順 7：HTTPSサーバのEnableチェックボックスにチェックマークを入れて、HTTPS経由のWebアクセスを有効にします。HTTPSサーバはデフォルトで有効になっています。

注：HTTPSサーバが無効になっている場合、HTTPSを使用する現在の接続はすべて切断されます。

ステップ 8：HTTPS接続に使用するポート番号をHTTPS Portフィールドに入力します。通常、デフォルトポート番号443はHTTPSで使用されます。

ステップ 9：[Save] をクリックして、設定を保存します。

SSL証明書の設定

SSL証明書は、HTTP/HTTPS WebブラウザまたはTFTPサーバからダウンロードするか、アクセスポイントを使用してSSL証明書を生成するか、コンピュータからアップロードできます。このセクションでは、SSL証明書をインストールするさまざまな方法について説明します。

SSL証明書の生成

セキュアWebサーバ用の新しいHTTP SSL証明書は、証明書の共通名がAPのIPアドレスに一致するように、アクセスポイント(AP)がIPアドレスを取得した後に生成する必要があります。新しいSSL証明書を生成すると、セキュアWebサーバが再起動します。セキュリティで保護された接続は、新しい証明書がブラウザで受け入れられるまで機能しません。

HTTPS Service

HTTPS Server: Enable

HTTPS Port: (Range: 1025-65535, Default: 443)

Generate SSL Certificate

ステップ 1 : Generateをクリックして、新しいSSL証明書を生成します。確認ウィンドウが表示されます。

Redirect HTTP to HTTPS:

HTTPS Service

HTTPS Server:

HTTPS Port :

Generate SSL Certificate


SSL Certificate File Status

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 20:04:30 2019 GMT

Certificate Issuer Common Name: CN=192.168.1.252

Confirm

 Generating a new SSL certificate will restart the secure web server. The secure connection will not work until the new certificate is accepted on the browser. Are you sure you want to continue?

ステップ 2 : OKをクリックして、SSL証明書の生成を続行します。証明書が生成されると、SSL Certificate File Status領域に次の情報が表示されます。

- ・ Certificate File Present:HTTP SSL証明書ファイルが存在するかどうかを示します。

- ・ Certificate Expiration Date : 現在のHTTP SSL証明書の有効期限が表示されます。
- ・ Certificate Issuer Common Name : 現在の証明書発行者の共通名を表示します。

SSL証明書のダウンロード

次の手順では、SSL証明書 (.pemファイル) をデバイスからバックアップとしてPCにダウンロードする方法について説明します。

SSL Certificate File Status

Certificate File Present:	Yes
Certificate Expiration Date:	Dec 26 22:09:59 2019 GMT
Certificate Issuer Common Name:	CN=192.168.1.245

Download SSL Certificate (From Device to PC)

Download Method:

HTTP/HTTPS
 TFTP

ステップ 1 : Download SSL Certificate領域で、目的のダウンロード方法に対応するオプションボタンをクリックします。

- ・ HTTP/HTTPS — SSL証明書をWebサーバーからダウンロードできるようにします。HTTP/HTTPSを選択する場合は、ステップ4に進みます。
- ・ TFTP:SSL証明書をTFTPサーバからダウンロードできるようにします。これを選択すると、File NameフィールドとTFTP Server IPv4 Addressフィールドが表示されます。

Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS
 TFTP

File Name: (Range: 1 - 128)

TFTP Server IPv4 Address:

ステップ 2 : ステップ1でTFTPを選択した場合は、File Nameフィールドにファイル名を入力します。これは、.pem拡張子を持つ証明書タイプのファイルです。

手順 3 : ステップ1でTFTPを選択した場合は、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。

ステップ 4 : Downloadをクリックして、証明書ファイルをダウンロードします。確認ウィンドウが表示されます。



ステップ 5 : OKをクリックしてダウンロードを続行します。

SSL証明書のアップロード

Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS
 TFTP

Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS
 TFTP

File Name: No file chosen

ステップ 1 : HTTP/HTTPSまたはTFTPオプションボタンをクリックして、Upload SSL Certificate領域で目的のアップロード方法を選択します。

- ・ HTTP/HTTPS:Webサーバで証明書をアップロードできます。HTTP/HTTPSを選択した場合は、ステップ2を完了してからステップ3をスキップしてください。
- ・ TFTP:SSL証明書をTFTPサーバ経由でアップロードできるようにします。これを選択すると、File NameフィールドとTFTP Server IPv4 Addressフィールドが表示されます。ステップ2を省略し、ステップ3を実行します。

Download SSL Certificate (From Device to PC)

Download Method: HTTP/HTTPS
 TFTP

Upload SSL Certificate (From PC to Device)

Upload Method: HTTP/HTTPS
 TFTP

File Name: No file chosen

ステップ 2 : Choose Fileをクリックし、ファイルを参照して選択します。

Upload SSL Certificate (From PC to Device)

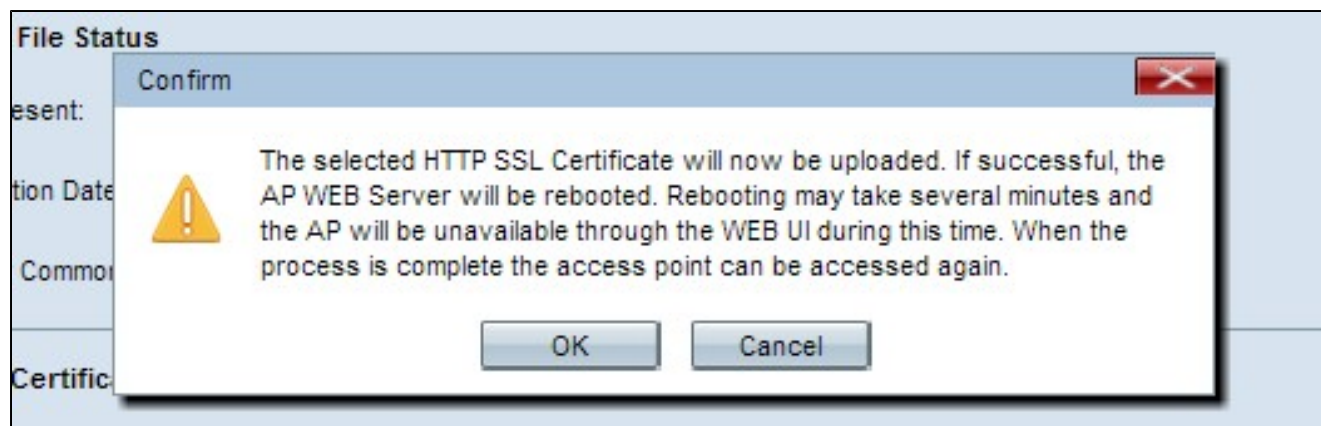
Upload Method: HTTP/HTTPS
 TFTP

File Name:

TFTP Server IPv4 Address:

ステップ 3 : File Nameフィールドにファイル名を入力し、TFTP Server IPv4 AddressフィールドにTFTPサーバアドレスを入力します。

ステップ 4 : Uploadをクリックして、証明書ファイルをアップロードします。確認ウィンドウが表示されます。



ステップ 5 : OKをクリックして、アップロードを続行します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。