

Cisco Business Wireless Access Pointでのカスタム証明書のアップロード

目的

このドキュメントの目的は、Cisco Business Wireless(CBW)Access Point(AP)にカスタム証明書をアップロードする方法を示すことです。

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
[ンロード](#))
- Cisco Business Wireless 240ACアクセスポイント | 10.6.1.0 (最新のダ
[ンロード](#))

概要

CBW APファームウェアバージョン10.6.1.0以降では、独自のWEBAUTH (キャプティブポータルページを処理する) またはWEBADMIN (CBWプライマリAP管理ページ) 証明書を、内部デバイスおよびシステムで信頼できるWebユーザーインターフェイス(UI)にインポートできます。デフォルトでは、WEBAUTHページとWEBADMINページは、通常は信頼されていない自己署名証明書を使用し、デバイスに接続しようとする
と証明書の警告が発生する可能性があります。

この新機能を使用すると、CBW APに簡単にカスタム証明書をアップロードできます。始めましょう。

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](#)**。
- CBWに必要なWEBAUTHまたはWEBADMIN証明書を発行するには、プライベートまたは内部の認証局(CA)が必要です。証明書は、CBW Web UIに接続できる管理PCにインストールできます。
- キャプティブポータルまたは管理アクセスにカスタム証明書を使用して、証明書の警告が表示されるのを防ぐために、対応するルートCA証明書をクライアントブラウザにインストールする必要があります。
- CBWは、キャプティブポータルリダイレクションに内部でリダイレクトされたIPアドレス192.0.2.1を使用します。したがって、これをWEBAUTH証明書のCommon Name(CN)またはSubject Alternative Name(SAN)として含めることをお勧めします。
- WEBADMIN証明書の命名要件は次のとおりです。CN-cisobusiness.cisco;SANはdns-cisobusiness.ciscoである必要があります。スタティックIPアドレスを使用する場合、SANにはdns=<ip address>も含まれます。

証明書のアップロード

手順 1

CBW APのWeb UIにログインします。



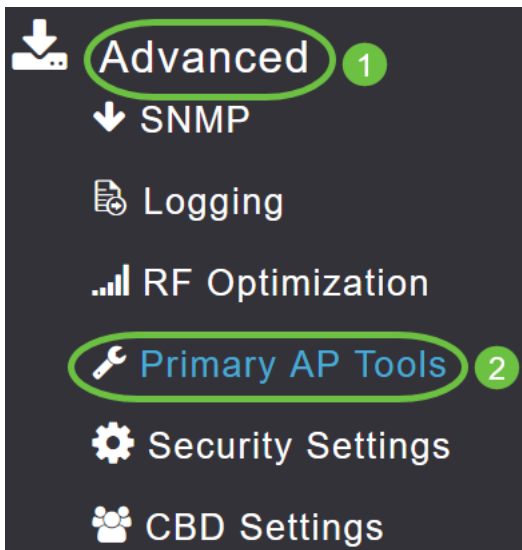
Cisco Business Wireless Access Point

Welcome! Please click the login button to enter your user name and password



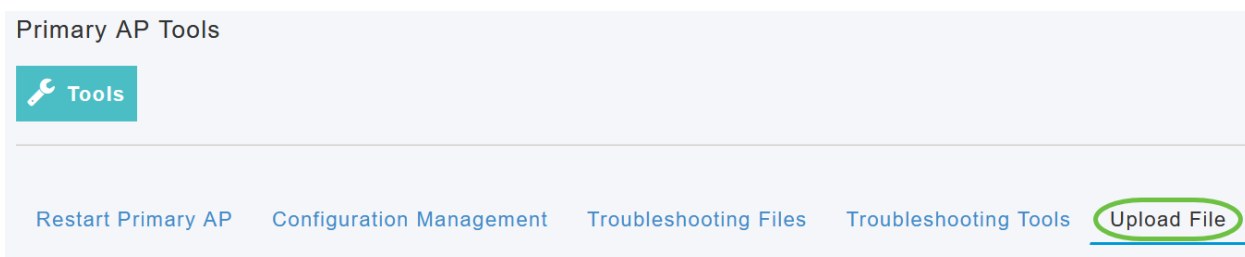
手順 2

証明書をアップロードするには、[Advanced] > [Primary AP Tools]に移動します。



手順 3

[ファイルのアップロード]タブを選択します。



手順 4

[ファイルタイプ]ドロップダウンメニューから、[WEBAUTH]または[WEBADMIN Certificate]を選択します。

Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT

File Type WEBAUTH Certificate

Transfer Mode

File Name* CCO ROOT CA Certificate

Certificate Password*

WEBAUTH Certificate

WEBADMIN Certificate

Browse

Apply settings and import

ファイルはPEM形式で、公開キーと秘密キーの両方を含む必要があります。パスワードも保護する必要があります。WEBAUTH証明書とWEBADMIN証明書の両方にciscobusiness.ciscoという共通名(CN)が必要です。したがって、証明書を発行するには内部CAを使用する必要があります。

手順 5

ドロップダウンメニューから転送モードを選択します。次のオプションがあります。

- HTTP (ローカルマシン)
- FTP
- TFTP

この例では、HTTPが選択されています。

File Type WEBAUTH Certificate

Transfer Mode HTTP (Local Machine)

File Name* HTTP (Local Machine)

Certificate Password*

FTP

TFTP

Browse

Apply settings and import

手順 6

[Browse] をクリックします。

Certificate Name `ciscobusiness.cisco` Valid up to `Jul 22 20:16:34 2023 GMT`

File Type

Transfer Mode

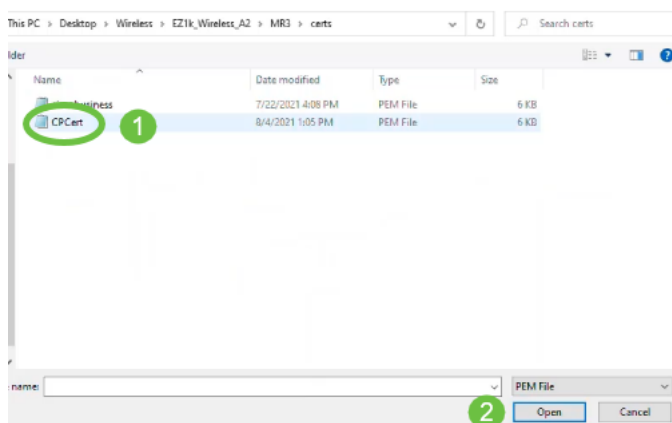
File Name*

Certificate Password*

転送モードがFTPまたはTFTPの場合は、サーバIPアドレス、ファイルパス、その他の必須フィールドを入力します。

ステップ7

カスタム証明書を含むフォルダに移動して、ローカルPCからファイルをアップロードします。証明書ファイルを選択し、[開く]をクリックします。



証明書はPEMファイルである必要があります。

手順 8

証明書のパスワードを入力します。

Certificate Name `192.0.2.1` Valid up to `Aug 4 17:50:50 2023 GMT`

File Type

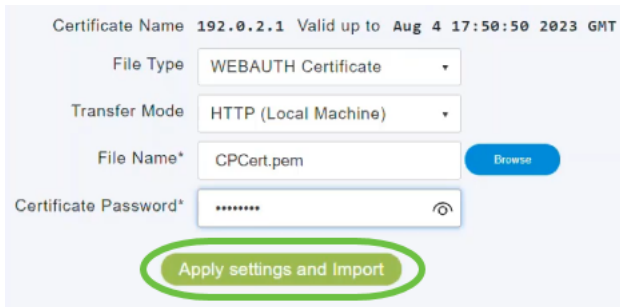
Transfer Mode

File Name*

Certificate Password

手順 9

[設定とインポートの適用]をクリックします。



Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT

File Type WEBAUTH Certificate

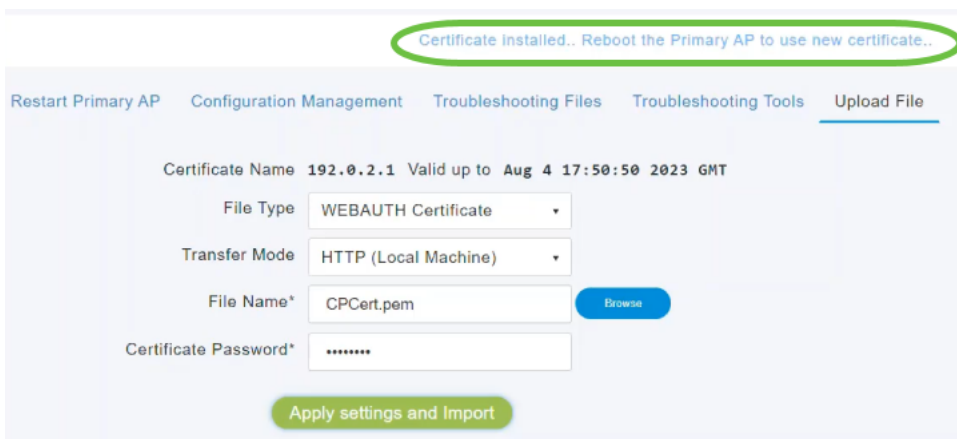
Transfer Mode HTTP (Local Machine)

File Name* CPCert.pem

Certificate Password*

手順 10

証明書が正常にインストールされると、通知が表示されます。プライマリAPをリブートします。



Certificate installed.. Reboot the Primary AP to use new certificate..

Restart Primary AP Configuration Management Troubleshooting Files Troubleshooting Tools Upload File

Certificate Name 192.0.2.1 Valid up to Aug 4 17:50:50 2023 GMT

File Type WEBAUTH Certificate

Transfer Mode HTTP (Local Machine)

File Name* CPCert.pem

Certificate Password*

証明書を変更するには、新しい証明書をアップロードするだけです。これにより、以前にインストールされた証明書が上書きされます。デフォルトの自己署名証明書に戻るには、プライマリAPを工場出荷時にリセットする必要があります。

結論

準備は万端！これで、カスタム証明書がCBW APに正常にアップロードされました。