

Cisco Business WirelessのプライマリAP設定のバックアップと復元

目的

この記事の目的は、Cisco Business Wireless(CBW)APを使用する場合に、プライマリアクセスポイント(AP)の設定をバックアップおよび復元するために必要な手順を示すことです。

該当するデバイス | ソフトウェアバージョン

140AC([データシート](#)) | 10.3.1.0 ([最新のダウンロード](#))

145AC([データシート](#)) | 10.3.1.0 ([最新のダウンロード](#))

240AC([データシート](#)) | 10.3.1.0 (最新の[ダウンロード](#))

概要

CBWには、バージョン10.3.1.0以降で利用可能な新機能が搭載されており、Webユーザインターフェイス(UI)でプライマリAP設定をエクスポートおよびインポートできます。

このコンフィギュレーションファイルには、無線、メッシュ、ロケーションの設定など、プライマリAPに関するすべての情報が含まれています。設定ファイルはXML形式で作成されます。

これは、工場出荷時のリセットを実行する必要がある場合に便利です。設定ファイルがある場合は、プライマリAPを最初から再設定する代わりにアップロードできます。コンフィギュレーションファイルが有用なもう1つのインスタンスは、新しいプライマリAPに同じ設定を設定する場合があります。

AP用のソフトウェアの最新バージョンがない場合は、開始する前に実行する必要があります。これらの手順は、アップデートなしでは実行できません。サポートが必要な場合は、[Cisco Business Wireless Access Pointのアップデートソフトウェアを確認してください](#)。

このドキュメントの用語に慣れていない場合は、[\[Cisco Business:新用語一覧\]](#)。

プライマリAPにログインします

手順 1

ネットワーク上のコンピュータを使用して、検索バーに[https://\[プライマリAPのIPアドレス\]](#)と入力して、プライマリAPのWeb UIにログインします。[https://](#)をプレフィックスとして使用することを確認してください。そうしないと、アクセスできなくなります。この例では、[https://192.168.1.124](#)が使用されていますが、使用するアドレスは異なります。アクセスに問題がある場合は、別のWebブラウザを試すことができます。

手順 2 (オプション)

セキュリティ証明書がない場合は、警告が表示されるポップアップが表示されることがあります。この警告は、Webブラウザによって異なる場合があります。クリックして先に進みます。



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.124** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve security on the web for everyone by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Advanced

Back to safety

2つ目のポップアップが表示され、クリックして続行できます。



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.124** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve security on the web for everyone by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Hide advanced

Back to safety

This server could not prove that it is **192.168.1.124**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.1.124 \(unsafe\)](#)

手順 3

[Login] をクリックする。

 Cisco Business

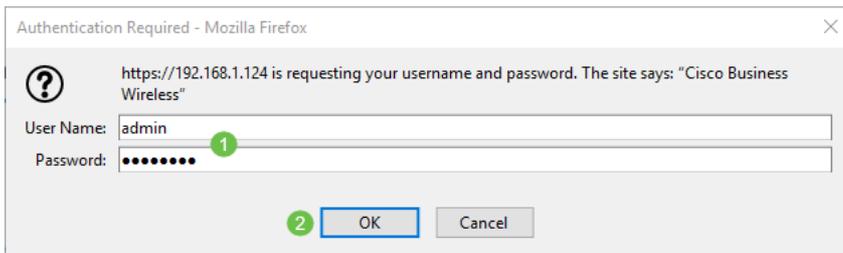
Cisco Business Wireless Access Point

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

Login

手順 4

ユーザ名とパスワードを入力します。[OK] をクリックします。



Authentication Required - Mozilla Firefox

https://192.168.1.124 is requesting your username and password. The site says: "Cisco Business Wireless"

User Name: admin 1

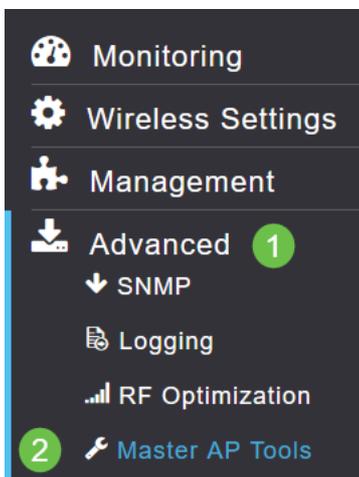
Password: ●●●●●● 1

2 OK Cancel

コンフィギュレーション ファイルのダウンロード

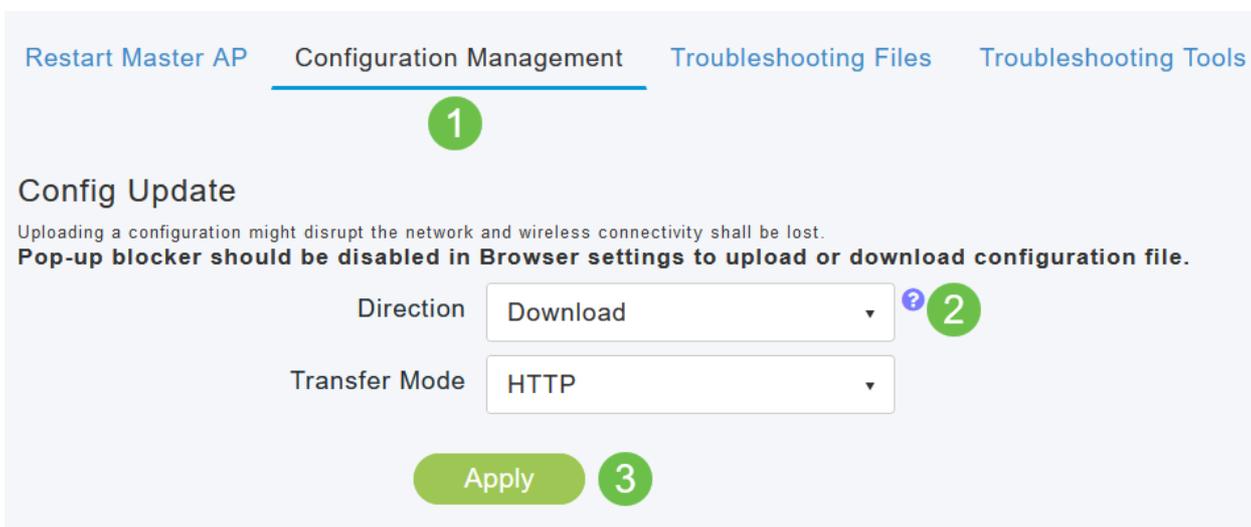
手順 1

[Advanced] > [Primary AP Tools] をクリックします。



手順 2

[構成管理] タブをクリックします。[方向] ドロップダウンメニューをクリックして、[ダウンロード] を選択します。転送モードはHTTPのままにしておきます。[Apply] をクリックします。



Restart Master AP Configuration Management Troubleshooting Files Troubleshooting Tools

1

Config Update

Uploading a configuration might disrupt the network and wireless connectivity shall be lost.
Pop-up blocker should be disabled in Browser settings to upload or download configuration file.

Direction Download 2

Transfer Mode HTTP

Apply 3

手順 3

ファイルをダウンロードするかどうかを確認するポップアップが表示されます。[Yes] をクリックします。

Download Configuration

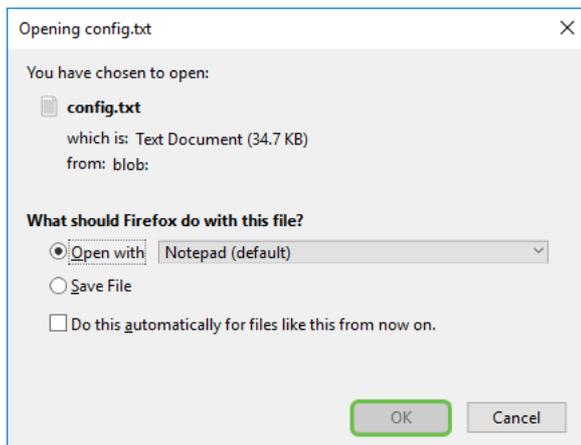
Are you sure you want to download this file.?

Yes

No

手順 4

ポップアップウィンドウに、いくつかのオプションが表示されます。この例では、[メモ帳で開く (既定)]を選択します。[OK]をクリックします。保存する前に表示しない場合は、[ファイルの保存]を選択して、この記事の[構成のアップロードセクションに移動](#)してください。



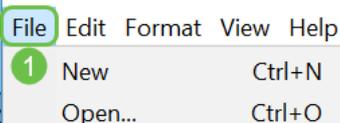
手順 5

これは、コンフィギュレーションファイルの1つのセクションの例です。

```
config.txt - Notepad
File Edit Format View Help
# WLC Config Begin <Fri Nov 13 09:34:09 2020>! Number of APs:
2! PID: CBW145AC-B, SN: FGL2418L84T ! Product Version:
10.3.1.0 ! ! ***** PORT SUMMARY
*****!
!          STP   Admin   Physical   Physical   Link   Link
! Pr  Type  Stat  Mode    Mode      Status  Status  Trap
! POE
! -----
! 1 Normal Forw Enable Auto      1000 Full Up    Enable
N/A      ! ! ***** CDP NEIGHBOUR SUMMARY
*****!
! Capability Codes: R - Router, T - Trans Bridge, B - Source
Route Bridge
!
!          S - Switch, H - Host, I - IGMP, r -
Repeater,
!
!          M - Remotely Managed Device
!
! Device ID      Local Intrfce   Holdtme   Capability
Platform Port ID
! c47d4fece352   wired0         152       S I
SG200-50P gi5config location expiry tags 5 config macfilter
add 6c:71:0d:55:73:c4 0 0 CBW145AC-73c4 config macfilter add
6c:71:0d:55:5d:a4 0 0 141ACM config countries-list add US
config rf-profile data-rates 802.11a disabled 6 High-Client-
Density-802.11a config rf-profile data-rates 802.11a disabled
9 High-Client-Density-802.11a config rf-profile data-rates
802.11a mandatory 12 High-Client-Density-802.11a config rf-
profile data-rates 802.11a supported 18 High-Client-Density-
802.11a config rf-profile data-rates 802.11a mandatory 24
High-Client-Density-802.11a config rf-profile data-rates
802.11a supported 36 High-Client-Density-802.11a config rf-
profile data-rates 802.11a supported 48 High-Client-Density-
802.11a config rf-profile data-rates 802.11a supported 54
High-Client-Density-802.11a config rf-profile data-rates
```

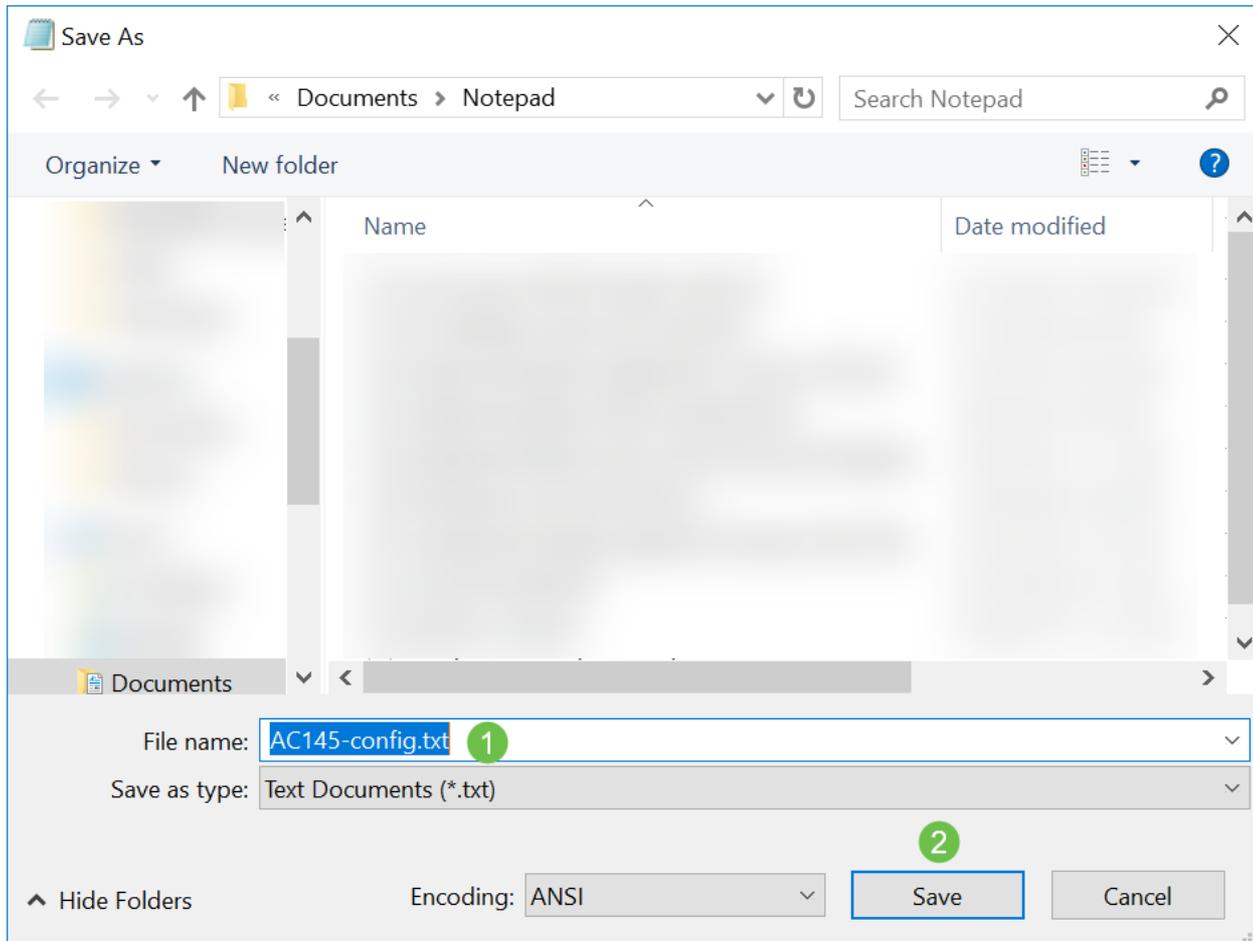
手順 6

[ファイル]をクリックし、ドロップダウンメニューから[名前を付けて保存...]を選択します。



ステップ7

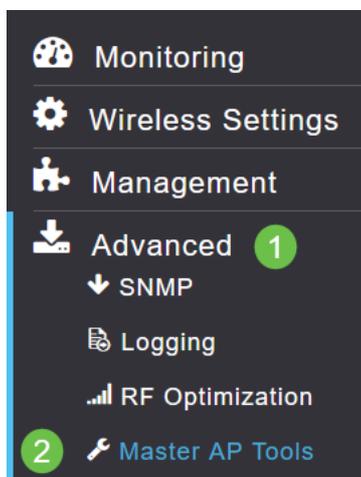
コンフィギュレーションファイルの名前を入力します。[Save] をクリックします。アップロードするファイルの場所をメモします。



コンフィギュレーション ファイルのアップロード

手順 1

[Advanced] > [Primary AP Tools]をクリックします。



手順 2

[構成管理]タブをクリックします。[方向]ドロップダウンメニューをクリックして、[アップロード

]を選択します。転送モードはHTTPのままにしておきます。[Apply] をクリックします。

Restart Master AP Configuration Management Troubleshooting Files Troubleshooting Tools Upload File

1

Config Update

Uploading a configuration might disrupt the network and wireless connectivity shall be lost.
Pop-up blocker should be disabled in Browser settings to upload or download configuration file.

Direction

Transfer Mode

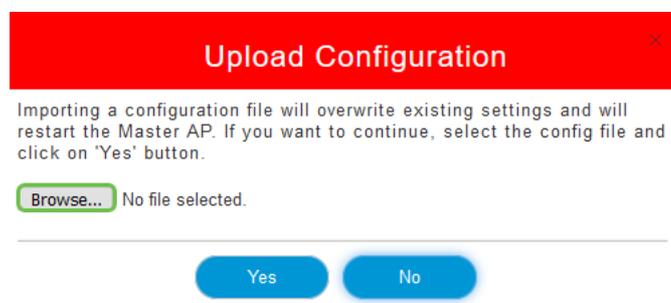
Apply

2

3

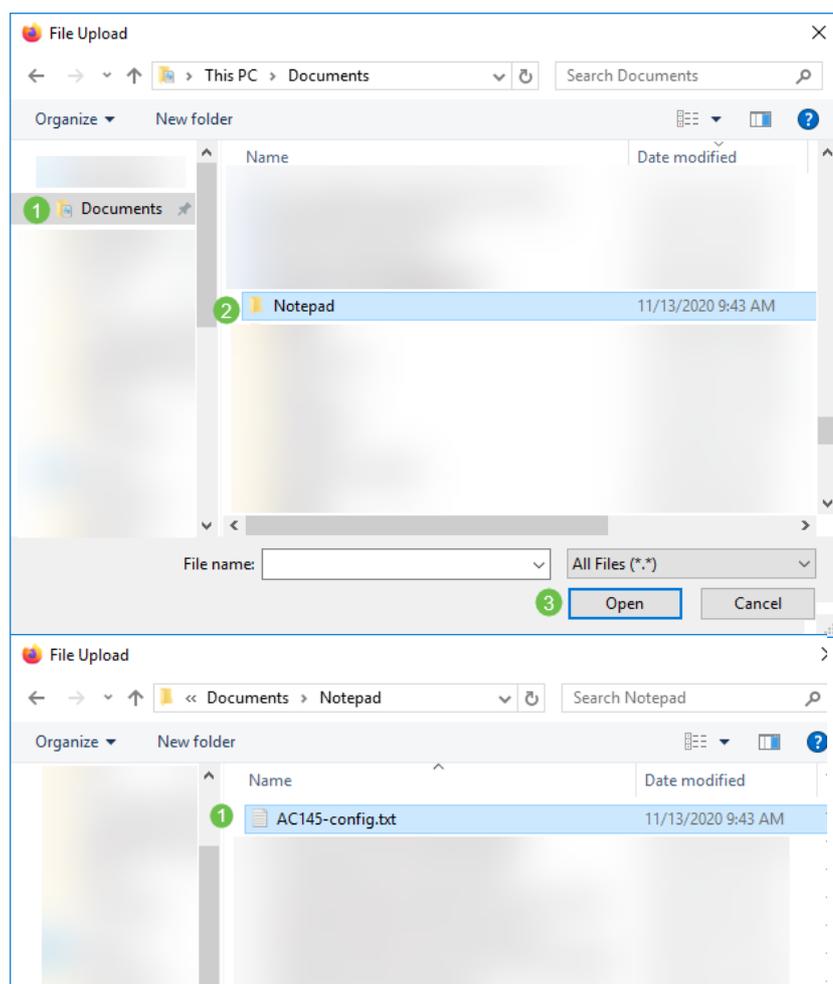
手順 3

ファイルをダウンロードするかどうかを確認するポップアップが表示されます。[Yes] をクリックします。



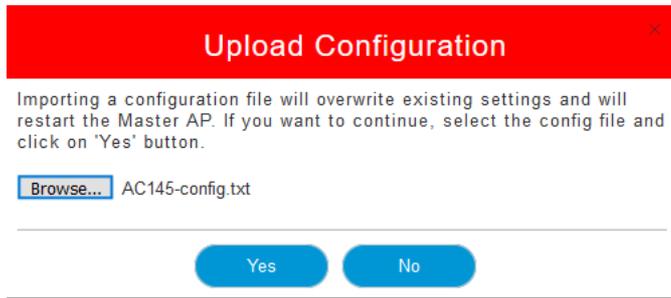
手順 4

最初のセクションでダウンロードした設定ファイルに移動します。[Open] をクリックします。



手順 5

設定ファイルをインポートすると既存の設定が上書きされ、プライマリAPが再起動されることを警告するメッセージが表示されます。[Yes] をクリックします。



手順 6

Web UIの上部に、次に示す更新プログラムが表示されます。

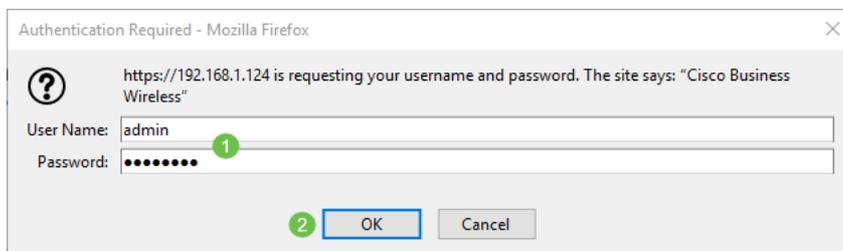
HTTP receive complete... updating configuration.

システムのリセットが確認されると、設定がアップロードされ、APがリブートします。しばらくお待ちください。これには最大10分かかることがあります。

System being reset.

ステップ7

リブートが完了すると、プライマリAPに再度ログインするように求められます。認証情報を入力し、[OK]をクリックします。



手順 8

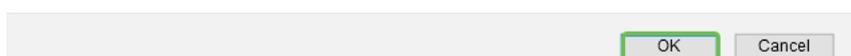
[保存]アイコンをクリックします。



手順 9

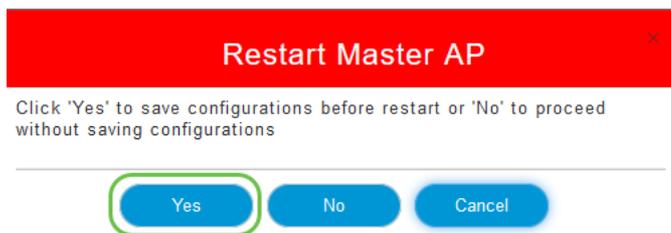
[OK] をクリックします。

Are you sure you want to save configuration to flash so that on a reboot the Master AP retains the configuration?



手順 10

再起動する前に設定を保存するには、[Yes]をクリックします。これには最大10分かかります。



結論

これで、コンフィギュレーションファイルをダウンロードしてアップロードするスキルが身に付きました。ベストプラクティスとして、コンフィギュレーションファイルを定期的にバックアップすることをお勧めします。

Cisco Business Wirelessのトピックの詳細については、次のいずれかをクリックしてください。

[シスコビジネスの新機能：機器および基本的なネットワーク用語集](#) [メッシュの概要](#) [メッシュFAQ](#) [Cisco Business Wireless Model Decoder](#) [再起動のヒント](#) [工場出荷時のデフォルトにリセット](#) [ゼロデイ：アプリ/Web経由で設定](#) [モバイルアプリとWeb UI](#) [シスコビジネスワイヤレスメッシュネットワークのベストプラクティス](#) [許可リスト](#) [ソフトウェアの更新](#) [CBWアプリケーションについて](#) [トラブルシューティング](#) [時間設定](#) [赤色LEDのトラブルシューティング](#) [ブリッジグループ名](#)