



コントローラ ソフトウェアと設定の 管理

この章では、コントローラにおける設定とソフトウェア バージョンの管理方法について説明します。この章の内容は、次のとおりです。

- [コントローラ ソフトウェアのアップグレード \(P. 8-2\)](#)
- [コントローラとのファイルのやり取り \(P. 8-7\)](#)
- [設定の保存 \(P. 8-14\)](#)
- [コントローラ設定のクリア \(P. 8-14\)](#)
- [コントローラ設定の消去 \(P. 8-14\)](#)
- [コントローラのリセット \(P. 8-15\)](#)

コントローラ ソフトウェアのアップグレード

コントローラのソフトウェアをアップグレードすると、コントローラのアソシエート アクセス ポイントも自動的にアップグレードされます。アクセス ポイントがソフトウェアをロードしている場合、アクセス ポイントの各 LED は連続して点滅します。最大 10 個のアクセス ポイントをコントローラから同時にアップグレードできます。



注意

このプロセスの実行時に、コントローラまたは任意のアクセス ポイントの電源を切らないでください。電源を切ると、ソフトウェア イメージが破損する場合があります。多数のアクセス ポイントを含むコントローラをアップグレードするには、ネットワークのサイズにもよりますが、最大で 30 分かかる場合があります。アクセス ポイントの電源は入れたままにしておく必要があります。また、アップグレード時にコントローラをリセットしてはなりません。

コントローラ ソフトウェアのアップグレードに関するガイドライン

以前のリリースからソフトウェア リリース 4.1 にコントローラをアップグレードする前に、次のガイドラインに従ってください。

- ソフトウェアのアップグレードに TFTP サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。
 - コントローラ ソフトウェア リリース 4.1 は、32 メガバイト (MB) よりサイズが大きいので、TFTP サーバで 32 MB より大きいファイルがサポートされていることを確認する必要があります。このサイズのファイルをサポートする TFTP サーバとして、tftpd、Cisco tftp、および WCS 内の TFTP サーバがあります。4.1 コントローラ ソフトウェアをダウンロードする際に TFTP サーバでこのサイズのファイルがサポートされていない場合、次のエラーメッセージが表示されます。「TFTP failure while storing in flash.」
 - サービス ポート経由でアップグレードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
 - ディストリビューション システム ネットワーク ポートを経由してアップグレードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
 - サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。
- お使いのコントローラでソフトウェア リリース 3.2.195.10 以降の 3.2 リリース、または 4.0.206.04 以降の 4.0 リリースが動作している場合には、ソフトウェア リリース 4.1 に直接コントローラをアップグレードできます。お使いのコントローラで以前の 3.2 リリースまたは 4.0 リリースが動作している場合、コントローラを 4.1 にアップグレードする前に、中間リリースにアップグレードする必要があります。表 8-1 は、ソフトウェア リリース 4.1 をダウンロードする前に従う必要があるアップグレードパスを示します。



(注) お使いのコントローラで現在動作しているソフトウェア リリースを確認するには、**Monitor** をクリックして、コントローラ GUI 上の Controller Summary の下にある Software Version フィールドを見てください。

表 8-1 コントローラ ソフトウェア リリース 4.1 へのアップグレード パス

現在のソフトウェア リリース	4.1 ソフトウェアへのアップグレード パス
3.2.78.0	4.1 へアップグレードする前に、4.0.206.0 以降の 4.0 リリースへアップグレードします。
3.2.116.21	
3.2.150.10	
3.2.171.6	
3.2.193.5	コントローラが新規の J3 国コードで設定されている場合は、3.2.195.10 以降の 3.2 リリースにアップグレードします。コントローラが新規の J3 国コードに設定されていない場合は、3.2.195.10 以降の 3.2 リリースまたは 4.0.206.0 以降の 4.0 リリースにアップグレードできます。
3.2.195.10 以降の 3.2 リリース	4.1 へ直接アップグレードできます。
4.0.155.5	4.1 へアップグレードする前に、4.0.206.0 以降の 4.0 リリースへアップグレードします。
4.0.179.11	
3.2.195.10 以降の 4.0 リリース	4.1 へ直接アップグレードできます。



(注) 中間ソフトウェアリリースにコントローラをアップグレードする場合、4.1 ソフトウェアをインストールする前に、コントローラに接続されているすべてのアクセス ポイントが中間リリースにアップグレードされるまで待ってください。大規模なネットワークでは、各アクセス ポイントでソフトウェアをダウンロードするのに多少時間がかかる場合があります。

- 一部のコントローラのブートローダ ソフトウェアに加えられた拡張により、4.1 .aes ファイルをインストールする前またはインストールした後に、コントローラに Cisco Unified Wireless Network Controller Boot Software 4.1 _ER.aes image をインストールする必要があります。



(注) _ER.aes イメージが必要なコントローラについては、4.1 リリース向けのリリース ノートを参照してください。

- シスコでは、アップグレードを次の順序で実行することをお勧めします。
 - コントローラ設定ファイルをサーバにアップロードしてバックアップします。
 - 802.11a および 802.11b/g ネットワークを無効にします。
 - この項の手順に従って、お使いのコントローラを最新のソフトウェア リリースにアップグレードします。
 - 802.11a および 802.11b/g ネットワークを再度有効にします。
 - 必要な場合、最新の設定ファイルをコントローラにリロードします。



注意

あるリリースから別のリリースへダウングレードする必要がある場合、現在のリリースからの設定が失われる可能性があります。回避策として、バックアップ サーバに保存されている以前のコントローラ設定ファイルをリロードするか、コントローラを再設定する方法があります。

GUI を使用したコントローラ ソフトウェアのアップグレード

GUI を使用してコントローラ ソフトウェアをアップグレードする手順は、次のとおりです。

- ステップ 1** 次の Cisco.com のソフトウェア センターから必要なコントローラ ソフトウェア リリースを取得します。 <http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>
- ステップ 2** ソフトウェア ファイル (<ファイル名>.aes) を TFTP サーバ上のデフォルト ディレクトリに移動します。
- ステップ 3** **Commands > Download File** をクリックして、Download File to Controller ページにアクセスします (図 8-1 を参照)。

図 8-1 Download File to Controller ページ

The screenshot shows the Cisco GUI interface for downloading software to the controller. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' section is active, and the 'Download File' option is selected in the left sidebar. The main content area is titled 'Download file to Controller' and contains the following fields:

- File Type:** A dropdown menu set to 'Code'.
- TFTP Server:** A section containing:
 - IP Address:** A text input field containing '0.0.0.0'.
 - Maximum retries:** A text input field containing '10'.
 - Timeout (seconds):** A text input field containing '6'.
 - File Path:** An empty text input field.
 - File Name:** An empty text input field.

Buttons for 'Clear' and 'Download' are located at the top right of the form area. A vertical ID '230915' is visible on the right edge of the screenshot.

- ステップ 4** File Type ドロップダウン ボックスから、**Code** を選択します。
- ステップ 5** IP 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 6** Maximum Retries フィールドに、TFTP サーバによるソフトウェアのダウンロードの最大試行回数を入力します。
- ステップ 7** Timeout フィールドに、TFTP サーバがソフトウェアのダウンロードを試行する時間 (秒単位) を入力します。
- ステップ 8** File Path フィールドに、ソフトウェアのディレクトリ パスを入力します。
- ステップ 9** File Name フィールドに、ソフトウェア (<ファイル名>.aes) の名前を入力します。
- ステップ 10** **Download** をクリックして、ソフトウェアをコントローラへダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。
- ステップ 11** ダウンロードが完了した後、**Reboot** の順にクリックします。
- ステップ 12** 変更を保存するように求めるプロンプトが表示されたら、**Save and Reboot** をクリックします。
- ステップ 13** WLAN を無効にしてから、この手順を繰り返して _ER.aes ファイルをインストールします。

ステップ 14 WLAN を再度有効にします。

CLI を使用したコントローラ ソフトウェアのアップグレード

CLI を使用してコントローラ ソフトウェアをアップグレードする手順は、次のとおりです。

- ステップ 1** 次の Cisco.com のソフトウェア センターから必要なコントローラ ソフトウェア リリースを取得します。 <http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>
- ステップ 2** ソフトウェア ファイル (<ファイル名>.aes) を TFTP サーバ上のデフォルト ディレクトリに移動します。
- ステップ 3** コントローラの CLI にログインします。
- ステップ 4** **ping** <サーバの IP アドレス> を入力して、コントローラが TFTP サーバと通信できることを確認します。
- ステップ 5** **transfer download start** コマンドを入力し、プロンプトに **n** と応答して現在のダウンロード設定を表示します。次のような情報が表示されます。

```
Mode..... TFTP
Data Type..... Code
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... <directory path>
TFTP Filename..... xxx.aes

Are you sure you want to start?(y/n) n
Transfer Canceled
```

- ステップ 6** 次のコマンドを入力して、ダウンロードの設定を変更します。

```
transfer download mode tftp
transfer download datatype code
transfer download serverip <TFTP サーバの IP アドレス>
transfer download filename <ファイル名>
transfer download path tftp-server-path-to-file
```



(注) TFTP サーバ上のパス名は、サーバのデフォルト ディレクトリまたはルート ディレクトリに対して相対的です。たとえば、Solarwinds TFTP サーバの場合、このパスは "/" となります。

ステップ 7 `transfer download start` と入力して、更新後の設定を表示します。プロンプトに `y` と応答して、現在のダウンロード設定を確認し、ソフトウェアのダウンロードを開始します。次のような情報が表示されます。

```
Mode..... TFTP
Data Type..... Code
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... <directory path>
TFTP Filename..... xxx.aes

Are you sure you want to start? (y/n) y
TFTP Code transfer starting.
TFTP receive complete... extracting components.
Writing new bootloader to flash.
Making backup copy of RTOS.
Writing new RTOS to flash.
Making backup copy of Code.
Writing new Code to flash.
TFTP File transfer operation completed successfully.
  Please restart the switch (reset system) for update to complete.
```

ステップ 8 `reset system` と入力して不揮発性 NVRAM に対するコードのアップデートを保存し、コントローラをリブートします。コントローラのブートアッププロセスが完了します。

ステップ 9 (`config wlan disable<WLAN ID>` コマンドを使用して) WLAN を無効にしてから、この手順を繰り返して `_ER.aes` ファイルをインストールします。

ステップ 10 `config wlan enable<WLAN ID>` と入力して、WLAN を再度有効にします。

コントローラとのファイルのやり取り

コントローラには、さまざまなファイルをアップロードまたはダウンロードするための組み込みユーティリティがあります。コントローラ GUI または CLI を使用してファイルをインポートするには、次の項の指示に従ってください。

- [デバイスの証明書のダウンロード \(P. 8-7\)](#)
- [CA 証明書のダウンロード \(P. 8-9\)](#)
- [PAC のアップロード \(P. 8-12\)](#)

デバイスの証明書のダウンロード

各無線デバイス（コントローラ、アクセス ポイント、およびクライアント）には独自のデバイスの証明書があります。たとえば、コントローラには、Cisco によりインストールされたデバイスの証明書が付属しています。この証明書は、ローカル EAP 認証時に無線クライアントの認証を行うために、EAP-TLS および EAP-FAST（PAC を使用していない場合）により使用されます。ただし、ご自身のベンダー固有のデバイスの証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。



(注) ローカル EAP の設定の詳細は、「[ローカル EAP の設定](#)」の項 (P. 5-26) を参照してください。

この項の手順に従って、GUI または CLI のいずれかを介して、ベンダー固有のデバイスの証明書をコントローラにダウンロードします。ただし、開始する前に、証明書のダウンロードに TFTP サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。



(注) コントローラにダウンロードする証明書はすべて、PEM 形式でなければなりません。

GUI を使用したデバイスの証明書のダウンロード

GUI を使用してコントローラにデバイスの証明書をダウンロードする手順は、次のとおりです。

- ステップ 1** デバイスの証明書を TFTP サーバ上のデフォルト ディレクトリにコピーします。
- ステップ 2** **Commands > Download File** をクリックして、**Download File to Controller** ページにアクセスします (図 8-2 を参照)。

図 8-2 Download File to Controller ページ

The screenshot shows the Cisco GUI interface for downloading a certificate. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' tab is active. On the left, a sidebar lists 'Commands' with 'Download File' highlighted. The main content area is titled 'Download file to Controller' and contains the following fields:

- File Type:** A dropdown menu set to 'Vendor Device Certificate'.
- Certificate Password:** A text input field with masked characters (dots).
- TFTP Server:** A section with several input fields:
 - IP Address:** 10.10.10.4
 - Maximum retries:** 10
 - Timeout (seconds):** 60
 - File Path:** tftpboot/username
 - File Name:** devcert1.pem

Buttons for 'Clear' and 'Download' are located at the top right of the form area. A vertical label '230921' is visible on the right edge of the screenshot.

- ステップ 3** File Type ドロップダウン ボックスから、**Vendor Device Certificate** を選択します。
- ステップ 4** Certificate Password フィールドに、証明書を保護するために使用されたパスワードを入力します。
- ステップ 5** IP 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 6** Maximum Retries フィールドに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。
- ステップ 7** Timeout フィールドに、TFTP サーバが証明書のダウンロードを試行する時間 (秒単位) を入力します。
- ステップ 8** File Path フィールドに、証明書のディレクトリパスを入力します。
- ステップ 9** File Name フィールドに、証明書の名前を入力します。
- ステップ 10** **Download** をクリックして、デバイスの証明書をコントローラへダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。
- ステップ 11** ダウンロードが完了した後、**Commands > Reboot > Reboot** をクリックします。
- ステップ 12** 変更を保存するように求めるプロンプトが表示されたら、**Save and Reboot** をクリックします。

CLI を使用したデバイスの証明書のダウンロード

CLI を使用してコントローラにデバイスの証明書をダウンロードする手順は、次のとおりです。

- ステップ 1 コントローラの CLI にログインします。
- ステップ 2 `transfer download datatype eapdevcert` と入力します。
- ステップ 3 `transfer download certpassword` <パスワード> と入力します。
- ステップ 4 `transfer upload serverip` <TFTP サーバの IP アドレス> と入力します。
- ステップ 5 `transfer download filename` <ファイル名>.pem と入力します。
- ステップ 6 `transfer download start` と入力して更新した設定を表示し、現在のダウンロード設定を確認するプロンプトが表示されたら `y` と応答して、ダウンロードプロセスを開始します。このダウンロードコマンドの出力例は、次のとおりです。

```
Mode..... TFTP
Data Type..... Vendor Dev Cert
TFTP Server IP..... 10.10.10.4
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /tftpboot/username/
TFTP Filename..... filename.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
Reboot the switch to use the new certificate.
```

- ステップ 7 `reset system` と入力して、コントローラをリブートします。
- ステップ 8 コントローラがリブートしたら、`show certificates local-auth` と入力して証明書がインストールされていることを確認します。

CA 証明書のダウンロード

コントローラとアクセス ポイントには、デバイスの証明書の署名と確認に使用される Certificate Authority (CA; 認証局) の証明書があります。コントローラには、Cisco によりインストールされた CA 証明書が付属しています。この証明書は、ローカル EAP 認証時に無線クライアントの認証を行うために、EAP-TLS および EAP-FAST (PAC を使用していない場合) により使用される場合があります。ただし、ご自身のベンダー固有の CA 証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。



(注) ローカル EAP の設定の詳細は、「ローカル EAP の設定」の項 (P. 5-26) を参照してください。

この項の手順に従って、GUI または CLI のいずれかを介して、CA 証明書をコントローラにダウンロードします。ただし、開始する前に、証明書のダウンロードに TFTP サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。



(注)

コントローラにダウンロードする証明書はすべて、PEM 形式でなければなりません。

GUI を使用した CA 証明書のダウンロード

GUI を使用してコントローラに CA 証明書をダウンロードする手順は、次のとおりです。

- ステップ 1** CA 証明書を TFTP サーバ上のデフォルト ディレクトリにコピーします。
- ステップ 2** **Commands > Download File** をクリックして、Download File to Controller ページにアクセスします (図 8-3 を参照)。

図 8-3 Download File to Controller ページ

Download file to Controller	
File Type	Vendor CA Certificate
TFTP Server	
IP Address	10.10.10.4
Maximum retries	10
Timeout (seconds)	60
File Path	/tftpboot/username
File Name	ca.pem

- ステップ 3** File Type ドロップダウン ボックスから、**Vendor CA Certificate** を選択します。
- ステップ 4** IP 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 5** Maximum Retries フィールドに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。
- ステップ 6** Timeout フィールドに、TFTP サーバが証明書のダウンロードを試行する時間(秒単位)を入力します。
- ステップ 7** File Path フィールドに、証明書のディレクトリ パスを入力します。

- ステップ 8** File Name フィールドに、証明書の名前を入力します。
- ステップ 9** **Download** をクリックして、CA 証明書をコントローラへダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。
- ステップ 10** ダウンロードが完了した後、**Commands > Reboot > Reboot** をクリックします。
- ステップ 11** 変更を保存するように求めるプロンプトが表示されたら、**Save and Reboot** をクリックします。

CLI を使用した CA 証明書のダウンロード

CLI を使用してコントローラに CA 証明書をダウンロードする手順は、次のとおりです。

- ステップ 1** コントローラの CLI にログインします。
- ステップ 2** **transfer download datatype eapcert** と入力します。
- ステップ 3** **transfer upload serverip** <TFTP サーバの IP アドレス> と入力します。
- ステップ 4** **transfer download filename** <ファイル名>.pem と入力します。
- ステップ 5** **transfer download start** と入力して更新した設定を表示し、現在のダウンロード設定を確認するプロンプトが表示されたら **y** と応答して、ダウンロードプロセスを開始します。このダウンロードコマンドの出力例は、次のとおりです。

```
Mode..... TFTP
Data Type..... Vendor CA Cert
TFTP Server IP..... 10.10.10.4
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /tftpboot/username/
TFTP Filename..... filename.pem
```

```
This may take some time.
Are you sure you want to start? (y/N) y
```

```
TFTP EAP CA cert transfer starting.
```

```
Certificate installed.
Reboot the switch to use the new certificate.
```

- ステップ 6** **reset system** と入力して、コントローラをリブートします。
- ステップ 7** コントローラがリブートしたら、**show certificates local-auth** と入力して証明書がインストールされていることを確認します。

PAC のアップロード

Protected Access Credential (PAC) は、自動的または手動でプロビジョニングされる資格情報で、EAP-FAST 認証時にローカル EAP 認証で相互認証を実行するために使用されます。手動の PAC プロビジョニングが有効になっている場合、PAC ファイルはコントローラ上で手動で生成されます。



(注) ローカル EAP の設定の詳細は、「[ローカル EAP の設定](#)」の項 (P. 5-26) を参照してください。

この項の手順に従って、GUI または CLI のいずれかを使用して、コントローラから PAC を生成してロードします。ただし、開始する前に、PAC アップロードに TFTP サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービスポート経由でアップロードする場合、サービスポートはルーティングできないため、TFTP サーバはサービスポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポートを経由してアップロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

GUI を使用した PAC のアップロード

GUI を使用してコントローラから PAC をアップロードする手順は、次のとおりです。

ステップ 1 **Commands > Upload File** をクリックして、Upload File from Controller ページにアクセスします (図 8-4 を参照)。

図 8-4 Upload File from Controller ページ

The screenshot shows the Cisco GUI interface for uploading a PAC file. The page title is 'Upload file from Controller'. On the left, there is a sidebar with 'Commands' and 'Upload File' selected. The main content area contains the following fields:

- File Type:** A dropdown menu set to 'PAC (Protected Access Credential)'.
- User (Identity):** A text input field containing 'username'.
- Validity (in days):** A text input field containing '10'.
- Password:** A password input field with masked characters '...'.
- Confirm Password:** A password input field with masked characters '...'.
- TFTP Server:** A section with three input fields:
 - IP Address:** '10.10.10.4'
 - File Path:** 'tftpboot/username'
 - File Name:** 'test.pac'

At the top right of the form, there are 'Clear' and 'Upload' buttons. The Cisco logo and navigation tabs (MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP) are visible at the top.

ステップ 2 File Type ドロップダウン ボックスから、**PAC (Protected Access Credential)** を選択します。

ステップ 3 User フィールドに、PAC を使用するユーザ名を入力します。

ステップ 4 Validity フィールドに、PAC が有効である日数を入力します。デフォルトの設定は、ゼロ (0) です。

- ステップ 5** Password フィールドおよび Confirm Password フィールドに、PAC を保護するためのパスワードを入力します。
- ステップ 6** IP 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 7** File Path フィールドに、PAC のディレクトリ パスを入力します。
- ステップ 8** File Name フィールドに、PAC ファイルの名前を入力します。PAC ファイルには .pac 拡張子が付いています。
- ステップ 9** **Upload** をクリックして、コントローラから PCA をアップロードします。アップロードのステータスを示すメッセージが表示されます。
- ステップ 10** 無線クライアントの手順に従って、クライアント デバイス上に PAC をアップロードします。必ず上記で入力したパスワードを使用するようにしてください。
-

CLI を使用した PAC のアップロード

CLI を使用してコントローラから PAC をアップロードする手順は、次のとおりです。

- ステップ 1** コントローラの CLI にログインします。
- ステップ 2** **transfer upload datatype pac** と入力します。
- ステップ 3** **transfer upload pac** <ユーザ名に対する有効なパスワード> と入力します。
- ステップ 4** **transfer upload serverip** <TFTP サーバの IP アドレス> と入力します。
- ステップ 5** **transfer upload filename** *manual.pac* と入力します。
- ステップ 6** **transfer upload start** と入力して更新した設定を表示し、現在の設定を確認するプロンプトが表示されたら **y** と応答して、アップロードプロセスを開始します。このコマンドの出力例は、次のとおりです。

```
Mode..... TFTP
TFTP Server IP..... 10.10.10.4
TFTP Path...../tftpboot/username/
TFTP Filename..... manual.pac
Data Type..... PAC
PAC User..... username
PAC Validity..... 10 days
PAC Password..... password
```

```
Are you sure you want to start?(y/N) y
```

```
PAC transfer starting.
```

```
File transfer operation completed successfully.
```

- ステップ 7** 無線クライアントの手順に従って、クライアント デバイス上に PAC をアップロードします。必ず上記で入力したパスワードを使用するようにしてください。
-

設定の保存

コントローラには 2 種類のメモリが搭載されています。揮発性 RAM と NVRAM です。アクティブな揮発性 RAM の設定への変更は、次のコマンドのいずれかを使用することで、いつでも不揮発性 RAM に保存できます。

- **save config** コマンドを使用します。このコマンドにより、コントローラをリセットせずに、揮発性 RAM から NVRAM に設定を保存できます。
- **reset system** コマンドを使用します。CLI から、コントローラをリブートする前に、設定の変更を保存するかどうかを確認するプロンプトが表示されます。
- **logout** コマンドを使用します。CLI から、ログアウトの前に、設定の変更を保存するかどうかを確認するプロンプトが表示されます。

コントローラ設定のクリア

NVRAM のアクティブな設定をクリアする手順は、次のとおりです。

-
- ステップ 1** **clear config** と入力し、操作を確認するプロンプトが表示されたら、**y** と入力します。
 - ステップ 2** **reset system** と入力します。確認のプロンプトで **n** と入力すると、設定の変更を保存せずにリブートされます。コントローラをリブートすると、設定ウィザードが自動的に起動されます。
 - ステップ 3** 「設定 ウィザードの使用方法」の項 (P. 4-2) の指示に従って、初期設定を行います。
-

コントローラ設定の消去

コントローラ設定をデフォルト設定にリセットする手順は、次のとおりです。

-
- ステップ 1** **reset system** と入力します。確認のプロンプトで **y** と入力して、設定変更を NVRAM に保存します。コントローラがリブートします。
 - ステップ 2** ユーザ名の入力を求められたら、**recover-config** と入力してデフォルトの設定に戻します。コントローラをリブートすると、設定ウィザードが自動的に起動されます。
 - ステップ 3** 「設定 ウィザードの使用方法」の項 (P. 4-2) の指示に従って、初期設定を行います。
-

コントローラのリセット

次の 2 つの方法のいずれかを使用して、コントローラをリセットして、CLI コンソールにリブート処理を表示することができます。

- コントローラを一度オフにし、再びオンにします。
- CLI で **reset system** と入力します。確認のプロンプトで **y** と入力して、設定変更を NVRAM に保存します。コントローラがリブートします。

コントローラがリブートすると、CLI コンソールに次のリブート情報が表示されます。

- システムの初期化。
- ハードウェア設定の検証。
- マイクロコードのメモリへのロード。
- オペレーティング システム ソフトウェアのロードの検証。
- 保存されている設定による初期化。
- ログイン プロンプトの表示。

■ コントローラのリセット