



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 \(P. 8-1\)](#)
- [コントローラとのファイルのやり取り \(P. 8-8\)](#)
- [設定の保存 \(P. 8-18\)](#)
- [コントローラ設定のクリア \(P. 8-19\)](#)
- [コントローラ設定の消去 \(P. 8-19\)](#)
- [コントローラのリセット \(P. 8-19\)](#)

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。ただし、ソフトウェア リリース 4.0.206.0 以降でサポートされている場合、同時にアップグレードされるアクセス ポイント数が増加したため、アップグレードの時間が大幅に短縮されました。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 4.2 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 ソフトウェアのアップグレード

- コントローラ ソフトウェア リリース 4.2 は、32MB よりサイズが大きいので、TFTP サーバで 32MB 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、および WCS 内の TFTP サーバがあります。4.2 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。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- 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、4.0.206.04 以降の 4.0 リリース、または 4.1.171.0 (以降の 4.1 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 4.2 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 または 4.0 リリースが動作している場合には、コントローラを中間リリースにアップグレードしてから 4.2 にアップグレードしてください。表 8-1 には、ソフトウェア リリース 4.2 をダウンロードする前にアップグレードする必要のあるパスが記載されています。



- (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、コントローラの GUI 上で **Controller Summary** の下にある **Software Version** フィールドを見るか、コントローラの CLI に **show sysinfo** と入力してください。

表 8-1 コントローラ ソフトウェア リリース 4.2 へのアップグレード パス

現在のソフトウェア リリース	4.2 ソフトウェアへのアップグレード パス
3.2.78.0	4.2 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	
3.2.195.10 以降の 3.2 リリース	4.2 へ直接アップグレードできます。
4.0.155.5	4.2 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	
4.0.206.0 以降の 4.0 リリース	4.2 へ直接アップグレードできます。
4.1.171.0 以降の 4.1 リリース	4.2 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、4.2 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。

- コントローラに Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイルもインストールすることをお勧めします。ブートローダの欠陥はこのファイルにより解決され、このファイルはコントローラが適切に動作していることを確認する際に必要です。ER.aes ファイルはすべてのコントローラのプラットフォームに必要です。



(注) ブートローダは、2106 コントローラではアップグレードできません。



(注) ER.aes ファイルは、コントローラ ソフトウェア ファイルに依存しません。どのコントローラ ソフトウェア ファイルも、すべての ER.aes ファイルで動作させることができます。ただし、最新のブートソフトウェア ファイル (4.2 ER.aes) をインストールすると、ブートソフトウェア ER.aes ファイルの新旧すべてのファイルでブートローダの修正をインストールしてあることが確認されます。

**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 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。



(注) コントローラの設定ファイルをバックアップしてから、コントローラ ソフトウェアをアップグレードするよう強くお勧めします。バックアップしない場合には、コントローラを手動で設定してください。

ステップ 2 802.11a および 802.11b/g ネットワークを無効にします。

ステップ 3 コントローラ上のすべての WLAN を無効にします。

ステップ 4 Software Center on Cisco.com から 4.2 コントローラ ソフトウェアおよび Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイルを取得する手順は、次のとおりです。

- a. 次の URL をクリックして、Software Center にアクセスします。
<http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>
- b. **Wireless Software** をクリックします。
- c. **Wireless LAN Controllers** をクリックします。
- d. **Standalone Controllers**、**Wireless Integrated Routers**、または **Wireless Integrated Switches** をクリックします。
- e. コントローラの名前をクリックします。

- f. **Wireless LAN Controller Software** をクリックします。
- g. コントローラ ソフトウェア リリースをクリックします。
- h. ファイル名 (*filename.aes*) をクリックします。
- i. **Download** をクリックします。
- j. シスコのエンド ユーザ ソフトウェアのライセンス契約を読んでから、**Agree** をクリックします。
- k. お使いのハード ドライブにファイルを保存します。
- l. 手順 a. ~ k. を繰り返し、残りのファイル (4.2 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイル) をダウンロードします。

ステップ 5 コントローラ ソフトウェア ファイル (*filename.aes*) および Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイルを TFTP サーバのデフォルト ディレクトリにコピーします。

ステップ 6 **Commands > Download File** の順にクリックして、Download File to Controller ページを開きます (図 8-1 を参照)。

図 8-1 Download File to Controller ページ

ステップ 7 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 8 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 9 Maximum Retries フィールドの 10 回の再試行および Timeout フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、必要に応じてその値を変更できます。そのためには、TFTP サーバがソフトウェアのダウンロードを試行する最大回数を Maximum Retries フィールドに、ソフトウェアのダウンロードを試行する時間の合計 (秒単位) を Timeout フィールドに入力します。

ステップ 10 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 11 File Name フィールドに、コントローラ ソフトウェア ファイル (*filename.aes*) の名前を入力します。

ステップ 12 **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 13 **ステップ 6 ~ ステップ 12** を繰り返し、残りのファイル (4.2 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイル) をダウンロードします。

- ステップ 14** 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 15** 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 16** **OK** をクリックし、変更内容を確定してコントローラをリブートします。
- ステップ 17** コントローラのリブート後、**WLAN** を再び有効にします。
- ステップ 18** 802.11a および 802.11b/g ネットワークを再度有効にします。
- ステップ 19** 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。
- ステップ 20** 4.2 コントローラ ソフトウェアがコントローラにインストールされたことを確認するには、コントローラの GUI の **Monitor** をクリックして **Controller Summary** の下の **Software Version** フィールドを見ます。
- ステップ 21** Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイルがコントローラにインストールされていることを確認するには、コントローラの CLI に **show sysinfo** コマンドを入力して **Bootloader Version** フィールドを見ます。



(注) このコマンドを使用して 2106 を除くすべてのコントローラのブート ソフトウェアのバージョンを確認できます。2106 コントローラでは、ブートローダをアップグレードできません。

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** 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。



(注) コントローラの設定ファイルをバックアップしてから、コントローラ ソフトウェアをアップグレードするよう強くお勧めします。バックアップしない場合には、コントローラを手動で設定してください。

- ステップ 2** 802.11a および 802.11b/g ネットワークを無効にします。
- ステップ 3** コントローラ上のすべての WLAN を無効にします (**config wlan disable wlan_id** コマンドを使用)。
- ステップ 4** Software Center on Cisco.com から 4.2 コントローラ ソフトウェアおよび Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイルを取得する手順は、次のとおりです。
- 次の URL をクリックして、Software Center にアクセスします。
<http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>
 - Wireless Software** をクリックします。

- c. **Wireless LAN Controllers** をクリックします。
- d. **Standalone Controllers**、**Wireless Integrated Routers**、または **Wireless Integrated Switches** をクリックします。
- e. コントローラの名前をクリックします。
- f. **Wireless LAN Controller Software** をクリックします。
- g. コントローラ ソフトウェア リリースをクリックします。
- h. ファイル名 (*filename.aes*) をクリックします。
- i. **Download** をクリックします。
- j. シスコのエンド ユーザ ソフトウェアのライセンス契約を読んでから、**Agree** をクリックします。
- k. お使いのハード ドライブにファイルを保存します。
- l. 手順 a. ~ k. を繰り返し、残りのファイル (4.2 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイル) をダウンロードします。

ステップ 5 コントローラ ソフトウェア ファイル (*filename.aes*) および Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイルを TFTP サーバのデフォルト ディレクトリにコピーします。

ステップ 6 コントローラの CLI にログインします。

ステップ 7 `ping server-ip-address` 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 8 `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 9 必要に応じて、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-server-ip-address
transfer download filename filename
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 10 `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 11 **ステップ 8** ~ **ステップ 11** を繰り返し、残りのファイル(4.2 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイル) をダウンロードします。

ステップ 12 `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 13 `config wlan enable wlan_id` と入力して、WLAN を再度有効にします。

ステップ 14 802.11a および 802.11b/g ネットワークを再度有効にします。

ステップ 15 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。

ステップ 16 4.2 コントローラ ソフトウェアがコントローラにインストールされたことを確認するには、`show sysinfo` と入力して Product Version フィールドを見ます。

ステップ 17 Cisco Unified Wireless Network Controller Boot Software 4.2 ER.aes ファイルがコントローラにインストールされていることを確認するには、`show sysinfo` と入力して Bootloader Version フィールドを見ます。



(注) このコマンドを使用して 2106 を除くすべてのコントローラのブート ソフトウェアのバージョンを確認できます。2106 コントローラでは、ブートローダをアップグレードできません。

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. 8-8)
- CA 証明書のダウンロード (P. 8-10)
- PAC のアップロード (P. 8-12)
- 設定ファイルのアップロードおよびダウンロード (P. 8-15)

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-FAST（PAC を使用していない場合）、EAP-TLS、PEAP-GTC、および PEAP-MSCHAPv2 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。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- 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** の順にクリックして、Download File to Controller ページを開きます (図 8-2 を参照)。

図 8-2 Download File to Controller ページ

- 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 フィールドの 10 回の再試行および Timeout フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、必要に応じてその値を変更できます。そのためには、TFTP サーバが証明書のダウンロードを試行する最大回数を Maximum Retries フィールドに、証明書のダウンロードを試行する時間の合計（秒単位）を Timeout フィールドに入力します。
- 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、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 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。
- ステップ 12** **OK** をクリックし、変更内容を確定してコントローラをリブートします。

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 password` と入力します。

ステップ 4 `transfer upload serverip tftp-server-ip-address` と入力します。

ステップ 5 `transfer download filename filename.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-FAST (PAC を使用していない場合)、EAP-TLS、PEAP-GTC、および PEAP-MSCHAPv2 により使用できます。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。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- 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** の順にクリックして、Download File to Controller ページを開きます (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 フィールドの 10 回の再試行および Timeout フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、必要に応じてその値を変更できます。そのためには、TFTP サーバが証明書のダウンロードを試行する最大回数を Maximum Retries フィールドに、証明書のダウンロードを試行する時間の合計 (秒単位) を Timeout フィールドに入力します。
- ステップ 6** 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 7** File Name フィールドに、証明書の名前を入力します。
- ステップ 8** **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 9** 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 10** 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 11 OK をクリックし、変更内容を確定してコントローラをリブートします。

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 download serverip` *tftp-server-ip-address* と入力します。

ステップ 4 `transfer download filename` *filename.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。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- 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 ページを開きます (図 8-4 を参照)。

図 8-4 Upload File from Controller ページ

The screenshot shows the Cisco GUI for uploading a PAC. The 'Commands' menu is open, and 'Upload File' is selected. The 'Upload file from Controller' page is displayed with the following fields:

- File Type:** PAC (Protected Access Credential) (dropdown menu)
- User (Identity):** username
- Validity (in days):** 10
- Password:** [masked]
- Confirm Password:** [masked]
- TFTP Server:**
 - IP Address:** 10.10.10.4
 - File Path:** tftpboot/username
 - File Name:** test.pac

Buttons for 'Clear' and 'Upload' are visible at the top right of the form.

- 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 username validity password` と入力します。
- ステップ 4** `transfer upload serverip tftp-server-ip-address` 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。

設定ファイルのアップロードおよびダウンロード

お使いのコントローラのソフトウェアをアップグレードする前に、コントローラの設定ファイルをサーバにアップロードして保存することをお勧めします。その上で新しいコントローラ ソフトウェアをインストールすると、設定ファイルをコントローラにダウンロードできます。



(注)

コントローラの設定ファイルをコントローラのソフトウェアのアップグレード前に保存していない場合は、手動でコントローラを再設定する必要があります。

コントローラ ソフトウェア リリース 4.2 では、コントローラのブートアップ設定ファイルがバイナリ形式ではなく、Extensible Markup Language (XML; 拡張マークアップ言語) 形式で保存されます。したがって、バイナリの設定ファイルを、ソフトウェア リリース 4.2.61.0 を稼動しているコントローラにダウンロードできません。ただし、以前のソフトウェア リリースを 4.2.61.0 にアップグレードする際には、設定ファイルが移行されて XML に変換されます。



(注)

設定ファイルを変更しないようにしてください。設定ファイルを変更してからそのファイルをコントローラへダウンロードすると、コントローラがリブートしながら設定パラメータをデフォルト値に戻す際に、コントローラは巡回冗長検査 (CRC) エラーを表示します。

設定ファイルのアップグレード

GUI または CLI のいずれかを使用して、設定ファイルをアップロードできます。

GUI を使用した設定ファイルのアップロード

コントローラ GUI を使用して設定ファイル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** の順にクリックして、Upload File from Controller ページを開きます (図 8-5 を参照)。

図 8-5 Upload File from Controller ページ

- ステップ 2** File Type ドロップダウン ボックスから **Configuration** を選択します。

■ コントローラとのファイルのやり取り

ステップ 3 暗号化を有効にするには、**Configuration File Encryption** チェックボックスをオンにして暗号キーを入力します。

ファイルの暗号化により、設定ファイルが TFTP サーバを介してアップロードされる際に、データは確実に暗号化されます。

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 File Path フィールドに、設定ファイルのディレクトリパスを入力します。

ステップ 6 File Name フィールドに、設定ファイルの名前を入力します。

ステップ 7 **Upload** をクリックし、設定ファイルを TFTP サーバに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。

CLI を使用した設定ファイルのアップロード

コントローラ CLI を使用して設定ファイル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 config** と入力します。

ステップ 3 設定ファイルを暗号化する手順は、次のとおりです。

a. **transfer encrypt enable** と入力します。

b. **transfer encrypt set-key key** と入力します。

ステップ 4 **transfer upload serverip tftp-server-ip-address** と入力します。

ステップ 5 **transfer upload path path** と入力します。

ステップ 6 **transfer upload filename filename** と入力します。

ステップ 7 **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..... Config/
TFTP Filename..... AS_4402_4_2_55_8_Config.xml
Data Type..... Config File
Encryption..... Disabled
```

```
*****
*** WARNING: Config File Encryption Disabled ***
*****
```

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

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

設定ファイルのダウンロード

GUI または CLI のいずれかを使用して、設定ファイルをダウンロードできます。

GUI を使用した設定ファイルのダウンロード

コントローラの GUI を使用して設定ファイルをダウンロードする手順は、次のとおりです。

- ステップ 1** **Commands > Download File** の順にクリックして、**Download File to Controller** ページを開きます (図 8-6 を参照)。

図 8-6 Download File to Controller ページ

Download file to Controller	
File Type	Configuration
Configuration File Encryption Key	*****
TFTP Server	
IP Address	10.10.10.4
Maximum retries	10
Timeout (seconds)	6
File Path	tftpboot/username/
File Name	AS_4402_4_55

- ステップ 2** File Type ドロップダウン ボックスから **Configuration** を選択します。
- ステップ 3** Configuration File Encryption Key フィールドに、ファイルがダウンロードされる際に設定ファイルのデータを暗号化する暗号キーを入力します。
- 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 フィールドの 10 回の再試行および Timeout フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、必要に応じてその値を変更できます。そのためには、TFTP サーバが設定ファイルのダウンロードを試行する最大回数を Maximum Retries フィールドに、設定ファイルのダウンロードを試行する時間の合計 (秒単位) を Timeout フィールドに入力します。
- ステップ 6** File Path フィールドに、設定ファイルのディレクトリパスを入力します。
- ステップ 7** File Name フィールドに、設定ファイルの名前を入力します (*filename*)。
- ステップ 8** **Download** をクリックして、ファイル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したメッセージが表示され、コントローラが自動的にリポートされます。

CLI を使用した設定ファイルのダウンロード

コントローラの CLI を使用して 設定ファイルをコントローラへ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 config` と入力します。
- ステップ 3** 設定ファイルを暗号化する手順は、次のとおりです。
- a. `transfer encrypt enable` と入力します。
 - b. `transfer encrypt set-key key` と入力します。
- ステップ 4** `transfer download serverip tftp-server-ip-address` と入力します。
- ステップ 5** `transfer download path path` と入力します。
- ステップ 6** `transfer download filename filename` と入力します。
- ステップ 7** `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
TFTP Server IP..... 10.10.10.4
TFTP Path..... Config/
TFTP Filename..... AS_4402_4_2_55_8_Config.xml
Data Type..... Config File
Encryption..... Disabled

*****
*** WARNING: Config File Encryption Disabled ***
*****

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

File transfer operation completed successfully.
```

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 からの不揮発性 RAM への設定の変更は、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ポートされます。コントローラをリポートすると、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。コントローラがリポートします。
 - 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。コントローラをリポートすると、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 コンソールにリポ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。コントローラがリポートします。

コントローラがリポートすると、CLI コンソールに次のリポ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