



CHAPTER 9

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.9-2)
- 「コントローラとのファイルのやり取り」(P.9-15)
- 「設定の保存」(P.9-32)
- 「設定ファイルの編集」(P.9-32)
- 「コントローラの設定のクリア」(P.9-34)
- 「コントローラ設定の消去」(P.9-34)
- 「コントローラのリセット」(P.9-34)

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) 5500 シリーズのコントローラは 6.0 ソフトウェアから最大 100 個のアクセス ポイントまでを同時にダウンロードできます。



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。



(注)

コントローラ ソフトウェア リリース 5.2 以降では、コントローラ GUI および CLI の両方から WLAN オーバーライド機能が削除されました。コントローラが、WLAN オーバーライドに対応し、コントローラ ソフトウェア リリース 5.2 以降にアップグレードするように設定されている場合、コントローラにより WLAN 設定が削除され、すべての WLAN がブロードキャストされます。アクセス ポイントグループを設定して、特定の WLAN のみを送信するように指定できます。各アクセス ポイントは、有効化されている WLAN のうち、そのアクセス ポイント グループに属する WLAN だけをアドバタイズします。

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

ソフトウェア リリース 6.0 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 または FTP サーバが使用できることを確認します。TFTP または FTP 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 6.0 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、tftpd32、および WCS 内の TFTP サーバがあります。6.0 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、「TFTP failure while storing in flash」というエラーメッセージが表示されます。
 - 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 または FTP 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ため、TFTP または FTP 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 または FTP サーバと WCS 内蔵型 TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは WCS と同じコンピュータ上で実行できません。
- 特定のリリース間のみでコントローラ ソフトウェアをアップグレードしたり、ダウングレードしたりすることができます。一部のインスタンスでは、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 6.0 にアップグレードする必要があります。表 9-1 に、ソフトウェア リリース 6.0 をダウンロードする前にアップグレードする必要があるパスが記載されています。

表 9-1 コントローラ ソフトウェア リリース 6.0 へのアップグレード パス

現在のソフトウェア リリース	6.0 ソフトウェアへのアップグレード パス
3.2.78.0 以降の 3.2 リリース	4.1 リリースにアップグレードしてから、4.2.176.0 にアップグレードし、さらに 6.0 にアップグレードします。
4.0.155.5 以降の 4.0 リリース	4.2.176.0 にアップグレードしてから、6.0 にアップグレードします。
4.1.171.0 以降の 4.1 リリース	4.2.176.0 にアップグレードしてから、6.0 にアップグレードします。
4.1.191.xM	4.1.192.35M にアップグレードしてから、6.0 にアップグレードします。
4.1.192.xM	6.0 へ直接アップグレードできます。
4.2.130.0 以降の 4.2 リリース	4.2.176.0 にアップグレードしてから、6.0 にアップグレードします。
4.2.173.0 以降の 4.2 リリース	6.0 へ直接アップグレードできます。
5.0.148.0 以降の 5.0 リリース	6.0 へ直接アップグレードできます。
5.1.151.0 以降の 5.1 リリース	6.0 へ直接アップグレードできます。
5.2.157.0 以降の 5.2 リリース	6.0 へ直接アップグレードできます。



(注) 5500 シリーズのコントローラは、コントローラ ソフトウェア リリース 6.0 以降のみを実行できます。



(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、コントローラに接続されているすべてのアクセス ポイントを中間リリースにアップグレードしてから 6.0 ソフトウェアをインストールしてください。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。

- ソフトウェア リリース 6.0.186.0 以降では、アップグレードイメージをコントローラにダウンロードしてから、ネットワークを稼動したままで、イメージをアクセス ポイントにダウンロードすることができます。新しい CLI およびコントローラ GUI 機能を使用すると、両方のデバイスのブートイメージを指定したり、コントローラのリセット時にアクセス ポイントをリセットしたりすることができます。両方のデバイスが稼動している場合は、アクセス ポイントでコントローラが検出され、再接続されます。アクセス ポイントへのイメージのプレダウンロードに関する詳細は、「アクセス ポイントへのイメージのプレダウンロード」(P.9-11) を参照してください。
- すべてのコントローラ プラットフォームに Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes ファイルをインストールすることを推奨します。このファイルは CSCsm03461 を解決するため、**show sysinfo** CLI コマンドの出力で ER.aes ファイルのバージョン情報を表示する際に必要となります。この ER.aes ファイルをインストールしないと、この欠陥の修正プログラムがコントローラによって取得されないため、このコマンドの出力にある [Field Recovery Image Version] または [Emergency Image Version] フィールドには「N/A」と表示されません。



(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 (5.2.157.0 ER.aes) をインストールすると、新旧ブート ソフトウェア ER.aes ファイルすべてに含まれるブート ソフトウェアの修正を確実にインストールできます。

**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。

メッシュ ネットワークのコントローラ ソフトウェア 6.0 のアップグレードに関するガイドライン

**注意**

メッシュ ネットワークでコントローラをソフトウェア リリース 6.0 をアップグレードする前に、次のルールに従う必要があります。

アップグレード互換性マトリクス

表 2 は、コントローラ メッシュのアップグレード互換性および非メッシュ リリースの概要を示し、アップグレードパスの一部として中間ソフトウェア リリースについて説明します。

ソフトウェア アップグレードの注意事項

- 設定ファイルを失うことなく、すべてのメッシュ リリースからコントローラ ソフトウェア リリース 6.0 にアップグレードできます。入手可能なアップグレードパスについては、表 2 を参照してください。



(注) メッシュ リリースにダウングレードする場合は、コントローラを再設定する必要があります。リリース 6.0 に初めてアップグレードする前に、メッシュ リリースの設定を保存しておくことを推奨します。さらに、ダウングレードする必要がある場合は、コントローラを再適用できます。

- コントローラ ソフトウェア リリース 6.0 からメッシュ リリース (4.1.190.5、4.1.191.22M、または 4.1.192.xxM) にダウンロードする場合には、必ず設定が失われます。
- メッシュ リリースからコントローラ ソフトウェア リリース 6.0 にアップグレードした直後の構成ファイルはバイナリ状態にあります。XML 構成ファイルは、リセット後に選択されます。
- XML ファイルは編集しないでください。
- 無効な値を含むフィールドはフィルタで除外され、XML 検証エンジンでデフォルトに設定されません。検証はブートアップ中に行われます。

表 2 コントローラ メッシュ リリースおよびコントローラ非メッシュ リリースのアップグレード互換性マトリクス

アップグレード先	6.0	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0	
アップグレード元																											
4.1.192.35M	Y	Y																									
4.1.192.22M	Y	Y	Y																								
4.1.191.24M			Y	-																							
4.1.190.5			Y ¹	Y	-																						
4.1.185.0				Y	Y ²	-																					
4.1.181.0					Y ²	Y ²																					
4.1.171.0					Y ²	Y ²	-																				
4.0.219.0						Y ²	Y ²	-																			
4.0.217.204				Y ²	Y ²	Y ²	Y ²	-																			
4.0.217.0					Y ²	Y ²	Y ²	Y ³	-																		
4.0.216.0					Y ²	Y ²	Y ²	Y ³	Y	-																	
4.0.206.0					Y ²	Y ²	Y ²	Y ³	Y		-																
4.0.179.11									Y	Y ⁴	-																
4.0.179.8									Y	Y ⁴	Y	-															
4.0.155.5									Y	Y ⁴	Y	Y	-														
4.0.155.0									Y	Y ⁴	Y	Y	Y	-													
3.2.195.10									Y	Y ⁴	Y	Y	Y		-												
3.2.193.5									Y	Y ⁴	Y	Y	Y		Y	-											
3.2.171.6									Y	Y ⁴	Y	Y	Y		Y		-										
3.2.171.5									Y	Y ⁴	Y	Y	Y		Y	Y	-										
3.2.150.10									Y	Y ⁴	Y	Y	Y		Y	Y		-									
3.2.150.6									Y	Y ⁴	Y	Y	Y		Y	Y		Y		-							
3.2.116.21									Y	Y ⁴	Y	Y	Y		Y	Y		Y		Y		-					
3.2.78.0									Y	Y ⁴	Y	Y	Y		Y	Y		Y	Y		Y		Y	-			
3.1.111.0																	Y	Y	Y	Y	Y	Y	Y	Y	-		
3.1.105.0																	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
3.1.59.24																	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

- ソフトウェア リリース 4.1.190.5 から 4.1.192.35M へは直接アップグレードできます。ただし、4.1.192.35M にアップグレードする前に、4.1.191.24M にアップグレードすることを強く推奨します。
- 動的周波数選択 (DFS) 機能を必要とするユーザは、このリリースを使用しないでください。このリリースには、リリース 4.0.217.204 で検出された DFS 機能の修正ファイルがありません。また、このリリースは ETSI 準拠の国およびシンガポールではサポートされていません。

■ コントローラ ソフトウェアのアップグレード

3. リリース 4.0.217.204 には、1510 シリーズのアクセス ポイント上にある DFS の修正ファイルが付属しています。この機能は、DFS 規制が適用されている国のみで必要です。
4. 次の国コードで、次のアクセス ポイントで動作している場合は 4.0.206.0 にアップグレードできません。オーストラリア (1505 および 1510)、ブラジル (1505 および 1510)、香港 (1505 および 1510)、インド (1505 および 1510)、日本 (1510)、韓国 (1505 および 1510)、メキシコ (1505 および 1510)、ニュージーランド (1505 および 1510)、およびロシア (1505 および 1510)。注: 1505 メッシュ アクセス ポイントはリリース 5.0 以降ではサポートされていません。1510 メッシュ アクセス ポイントはメッシュ リリース 4.1.190.5、4.1.191.22M、および 4.1.192.xxM のみでサポートされています。

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

コントローラ 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次の手順に従います。



(注)

6.0 コントローラ ソフトウェア ファイルと 5.2.157.0 ER.aes ブート ソフトウェア ファイルを同時にインストールしないでください。いずれかのファイルをインストールし、コントローラをリブートしてから、もう一方のファイルをインストールし、コントローラをリブートします。

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ことを強く推奨します。手順については、「[設定ファイルのアップロードおよびダウンロード](#)」(P.9-27) を参照してください。

ステップ 2

Cisco.com の Software Center から 6.0 コントローラ ソフトウェアおよび Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 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://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243>
- b. [Wireless Software] を選択します。
- c. [Wireless LAN Controllers] を選択します。
- d. [Standalone Controllers] または [Integrated Controllers and Controller Modules] を選択します。
- e. コントローラ シリーズを選択します。
- f. 必要に応じて、コントローラのモデルを選択します。
- g. ステップ d. で [Standalone Controllers] を選択する場合は、[Wireless LAN Controller Software] を選択します。
- h. ステップ e. で Cisco Catalyst 6500 Series/7600 Series Wireless Services Module WiSM を選択する場合は、[Wireless Services Modules (WiSM) Software] を選択します。
- i. コントローラ ソフトウェア リリースを選択します。ソフトウェア リリースには、ダウンロードするリリースを判断する際に役立つように、次のようなラベルが付いています。
 - **Early Deployment (ED)** : これらのソフトウェア リリースには、バグ修正ファイルだけでなく、新機能および新しいハードウェア プラットフォーム サポートが付属しています。
 - **Maintenance Deployment (MD)** : これらのソフトウェア リリースには、バグ修正ファイルおよび現時点のソフトウェア メンテナンスが付属しています。
 - **Deferred (DF)** : これらは延期されたソフトウェア リリースです。アップグレードしたリリースに移行することを推奨します。
- j. ソフトウェア リリース番号を選択します。

- k. ファイル名 (*filename.aes*) をクリックします。
- l. [Download] をクリックします。
- m. 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み、[Agree] をクリックします。
- n. お使いのハード ドライブにファイルを保存します。
- o. ステップ a. ~ n. を繰り返し、残りのファイル (6.0 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes ファイル) をダウンロードします。

- ステップ 3** 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 5.2.157.0 ER.aes ファイルを TFTP または FTP 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 4** 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 5** Cisco WiSM の場合、アクセス ポイントでソフトウェアのダウンロードが開始される前にコントローラでリポートできるように、Catalyst スイッチのコントローラ ポート チャネルをシャットダウンします。
- ステップ 6** コントローラ上のすべての WLAN を無効にします。
- ステップ 7** [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます (図 9-1 を参照してください)。

図 9-1 [Download File to Controller] ページ

The screenshot shows the 'Download File to Controller' configuration page in the Cisco Catalyst web interface. The page has a blue header with the Cisco logo and navigation tabs: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The 'COMMANDS' tab is active. On the left, there is a 'Commands' sidebar with links for Download File, Upload File, Reboot, Reset to Factory Default, and Set Time. The main content area is titled 'Download file to Controller' and contains several input fields and buttons. The 'File Type' dropdown is set to 'Code'. The 'Transfer Mode' dropdown is set to 'TFTP'. Under 'Server Details', the 'IP Address' field contains '1.2.3.4', 'Maximum retries' is '10', and 'Timeout (seconds)' is '6'. The 'File Path' field contains '/download' and the 'File Name' field contains 'sample.aes'. There are 'Clear' and 'Download' buttons at the top right of the form area. A vertical copyright notice '© 2006 Cisco' is visible on the right edge of the screenshot.

- ステップ 8** [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 9** [Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。
- ステップ 10** [IP Address] フィールドに、TFTP または FTP サーバの IP アドレスを入力します。
- ステップ 11** TFTP サーバを使用している場合は、[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、これらの値は変更できます。値を変更するには、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 12** [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 13** [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 14** FTP サーバを使用している場合は、次の手順に従います。
- a. [Server Login Username] フィールドにユーザ名を入力し、FTP サーバにログインします。
 - b. [Server Login Password] フィールドにパスワードを入力し、FTP サーバにログインします。
 - c. [Server Port Number] フィールドに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

- ステップ 15** [Download] をクリックして、ソフトウェアをコントローラに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 16** ダウンロードの完了後、[Reboot] をクリックします。
- ステップ 17** 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 18** [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。



(注) コントローラは、ただちにリブートしてください。ソフトウェアをダウンロードした直後にリブートします。すぐにリブートしない場合、ソフトウェアをコントローラで実行する前に、アクセス ポイントがソフトウェアのダウンロードを開始することがあります。

- ステップ 19** コントローラをリブートしたあとに、[ステップ 7](#) ~ [ステップ 18](#) を繰り返し、残りのファイル (6.0 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes ファイル) をダウンロードします。
- ステップ 20** WLAN を再度有効にします。
- ステップ 21** Cisco WiSM の場合、Catalyst スイッチのコントローラ ポート チャネルを再度有効にします。
- ステップ 22** 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 23** 必要に応じて、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 24** 6.0 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] を選択して [Controller Summary] の下の [Software Version] フィールドを見ます。
- ステップ 25** Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 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、[Monitor] を選択して [Summary] ページを開き、[Field Recovery Image Version] または [Emergency Image Version] フィールドを見ます。



(注) Cisco Unified Wireless Network Controller Boot Software ER.aes ファイルがインストールされていない場合、[Field Recovery Image Version] または [Emergency Image Version] フィールドには「N/A」と表示されます。

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

コントローラ 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次の手順に従います。



(注)

6.0 コントローラ ソフトウェア ファイルと 5.2.157.0 ER.aes ブート ソフトウェア ファイルを同時にインストールしないでください。いずれかのファイルをインストールし、コントローラをリブートしてから、もう一方のファイルをインストールし、コントローラをリブートします。

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ことを強く推奨します。手順については、「設定ファイルのアップロードおよびダウンロード」(P.9-27) を参照してください。

ステップ 2

Cisco.com の Software Center から 6.0 コントローラ ソフトウェアおよび Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 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://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243>
- b. [Wireless Software] を選択します。
- c. [Wireless LAN Controllers] を選択します。
- d. [Standalone Controllers]、[Wireless Integrated Routers]、または [Wireless Integrated Switches] を選択します。
- e. コントローラの名前を選択します。
- f. [Wireless LAN Controller Software] を選択します。
- g. コントローラ ソフトウェア リリースを選択します。
- 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み、[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. ステップ a. ~ k. を繰り返し、残りのファイル (6.0 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes ファイル) をダウンロードします。

ステップ 3

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 5.2.157.0 ER.aes ファイルを TFTP または FTP 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 4

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 5

Cisco WiSM の場合、アクセス ポイントでソフトウェアのダウンロードが開始される前にコントローラでリブートできるように、Catalyst スイッチのコントローラ ポート チャネルをシャットダウンします。

ステップ 6

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 7

コントローラの CLI にログインします。

ステップ 8

`ping server-ip-address` と入力して、コントローラが TFTP または FTP サーバと通信できることを確認します。

ステップ 9 `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 Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... <directory path>
TFTP Filename..... xxx.aes

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

ステップ 10 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 | ftp}`
- `transfer download datatype code`
- `transfer download serverip server-ip-address`
- `transfer download filename filename`
- `transfer download path server-path-to-file`



(注) TFTP または FTP 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 ディレクトリに対する相対パスです。たとえば、Solarwinds TFTP サーバの場合、このパスは "/" となります。

TFTP サーバを使用している場合は、次のコマンドを入力します。

- `transfer download tftpMaxRetries retries`
- `transfer download tftpPktTimeout timeout`



(注) 10 回の再試行および 6 秒のタイムアウト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、これらの値は変更できます。値を変更するには、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 `retries` パラメータ、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` パラメータに入力します。

FTP サーバを使用している場合は、次のコマンドも入力します。

- `transfer download username username`
- `transfer download password password`
- `transfer download port port`



(注) `port` パラメータのデフォルト値は 21 です。

ステップ 11 `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 Packet Timeout..... 6
TFTP Max Retries..... 10
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 12 **reset system** と入力して不揮発性メモリ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。



(注) コントローラは、ただちにリブートしてください。ソフトウェアをダウンロードした直後にリブートします。すぐにリブートしない場合、ソフトウェアをコントローラで実行する前に、アクセス ポイントがソフトウェアのダウンロードを開始することがあります。

ステップ 13 コントローラをリブートしたあとに、**ステップ 9** ~ **ステップ 12** を繰り返し、残りのファイル (6.0 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes ファイル) をダウンロードします。

ステップ 14 **config wlan enable wlan_id** と入力して、WLAN を再度有効にします。

ステップ 15 Cisco WiSM の場合、Catalyst スイッチのコントローラ ポート チャネルを再度有効にします。

ステップ 16 802.11a 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 17 必要に応じて、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 18 6.0 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 19 Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 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 [Field Recovery Image Version] または [Emergency Image Version] フィールドを見ます。



(注) Cisco Unified Wireless Network Controller Boot Software ER.aes ファイルがインストールされていない場合、[Field Recovery Image Version] または [Emergency Image Version] フィールドには「N/A」と表示されます。

アクセス ポイントへのイメージのプレダウンロード

ネットワークの停止を最小限に抑えるため、アクセス ポイントをリセットしたり、ネットワーク接続を切断したりせずに、アップグレード イメージをコントローラのアクセス ポイントにダウンロードできるようになりました。以前は、アップグレード イメージをコントローラにダウンロードし、コントローラ

をリセットすると、アクセス ポイントがディスカバリ モードに移行してしまいました。アクセス ポイントで新しいイメージを含むコントローラが検出されると、新しいイメージがダウンロードされ、アクセス ポイントがリセットされ、ディスカバリ モードに移行し、コントローラに再接続されます。

アップグレード イメージをコントローラにダウンロードしてから、ネットワークを稼動したままで、イメージをアクセス ポイントにダウンロードできるようになりました。さらに、指定の期間のあと、または特定の日に、コントローラおよびアクセス ポイントのリポートをスケジュールすることができます。両方のデバイスが稼動している場合は、アクセス ポイントによってコントローラが検出され、再接続されます。



(注)

このようなアクセス ポイント モデルは、イメージ 1120、1230、および 1310 のプレダウンロードをサポートしていません。

イメージのプレダウンロードのガイドラインおよび制限事項

イメージのプレダウンロードを使用するときには、次の点に留意してください。

- 最大プレダウンロード制限：4400 シリーズのコントローラでは、同時プレダウンロードの最大数は通常の同時イメージ ダウンロード数の半分に制限されます。5500 シリーズのコントローラでは、同時ダウンロード数は 25 に制限されます。この制限により、イメージのダウンロード中に、新しいアクセス ポイントのコントローラに接続が可能になります。

プレダウンロードの制限に達すると、イメージを取得できないアクセス ポイントはバック オフされ、180 ~ 600 秒間待機してから、プレダウンロードが再試行されます。

- プレダウンロードが有効である場合、アクセス ポイントが接続できるすべてのコントローラ（プライマリ、セカンダリ、およびターシャリ）では、プライマリ イメージとバックアップ イメージに同じイメージを使用する必要があります。たとえば、3 つのコントローラがある場合は、3 つのすべてのコントローラでは、プライマリ イメージとしてソフトウェア リリース x、バックアップ イメージとしてリリース y を使用する必要があります。コントローラの中には他のコントローラよりもリポートに時間がかかるものがあるため、イメージの一貫性を維持することが重要です。アクセス ポイントは、リポート後すぐにコントローラに再接続されます。5500 コントローラより先に 4400 コントローラがリポートされる場合は、アクセス ポイントがどちらか一方のコントローラに接続される場合に備え、両方のコントローラが同じイメージを実行している必要があります。
- プレダウンロード コマンドを入力する前に、アクティブなコントローラ ブート イメージをバックアップ イメージに変更することを推奨します。この手順を実行することで、コントローラが何らかの理由でリポートされた場合、アップグレード イメージが部分的にダウンロードされるのではなく、以前の実行イメージで確実にバックアップされます。
- アクセス ポイントの使用可能メモリの全容量が 16MB で（1130 および 1240 アクセス ポイント）、アップグレード イメージのダウンロードには空き容量が不足している場合、アクセス ポイントは、crash info ファイル、radio ファイル、およびすべてのバックアップ イメージを自動的に削除し、空き容量を増やします。ただし、プレダウンロード イメージはアクセス ポイントのバックアップ イメージに置き換えられるため、この制限はプレダウンロード プロセスには影響しません。

CLI を使用したアクセス ポイントへのイメージのプレダウンロード

CLI を使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントにイメージをプレダウンロードできます。プロセスの手順は、次のとおりです。

- アップグレード イメージをコントローラにプレダウンロードします。
- アップグレード イメージをアクセス ポイントにプレダウンロードします。
- コントローラおよびアクセス ポイントのイメージをアップグレードします。

- コントローラおよびアクセス ポイントのリブート時間を設定します。

コントローラへのアップグレード イメージのプレダウンロード

アップグレード イメージを取得するには、[ステップ 1](#) ~ [ステップ 10](#) (「[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](#)」(P.9-9)) に従います。

コントローラ CLI で **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 Packet Timeout..... 6
TFTP Max Retries..... 10
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.
```

コントローラで **show boot** と入力します。新しいイメージはプライマリ イメージ、古いイメージはバックアップ イメージとしてリストに表示されます。ただし、アップグレードの前または最中にコントローラをリセットする場合、ネットワークで既存のイメージが確実に検出されるように、コントローラプライマリ イメージとバックアップ イメージを切り替える必要があります。

config boot backup と入力して、コントローラのアクティブなブート イメージを既存のイメージ (ここではバックアップ イメージ) に変更します。

再度 **show boot** と入力し、イメージが正常にセットアップされたことを確認します。

アクセス ポイントへのイメージのプレダウンロード

イメージをアクセス ポイントのフラッシュ メモリにプレダウンロードするには、コントローラ CLI で次のコマンドを入力します。

```
config ap image predownload {primary | backup} {ap_name | all}
```

プライマリ イメージが新しいイメージ、バックアップ イメージが古いイメージです。アクセス ポイントは常にプライマリ イメージでブートされます。

アクセス ポイントのプライマリ イメージとバックアップ イメージを切り替えるには、次のコマンドを入力します。

```
config ap image swap {ap_name | all}
```

コントローラおよびアクセス ポイントでのイメージのアップグレード

プレダウンロード用に指定されたアクセス ポイントの詳細情報を表示するには、次のコマンドを入力します。

```
show ap image {all | ap-name}
```

コマンドの出力例は次のとおりです。

```
Total number of APs..... 7
Number of APs
  Initiated..... 4
  Predownloading..... 0
  Completed predownloading..... 3
  Not Supported..... 0
  Failed to Predownload..... 0
```

AP Name	Primary Image	Backup Image	Predownload Status	Predownload Version	Next Retry Time	Retry Count
AP1140-1	7.0.56.0	6.0.183.38	Complete	6.0.183.38	NA	NA
AP1140-2	7.0.56.0	6.0.183.58	Initiated	6.0.183.38	23:46:43	1
AP1130-2	7.0.56.0	6.0.183.38	Complete	6.0.183.38	NA	NA
AP1130-3	7.0.56.0	6.0.183.58	Initiated	6.0.183.38	23:43:25	1
AP1130-4	7.0.56.0	6.0.183.38	Complete	6.0.183.38	NA	NA
AP1130-5	7.0.56.0	6.0.183.58	Initiated	6.0.183.38	23:43:00	1
AP1130-6	7.0.56.0	6.0.183.58	Initiated	6.0.183.38	23:41:33	1

出力には、プレダウンドロード用に指定されたアクセスポイントがリストされ、各アクセスポイントについて、プライマリ イメージおよびセカンダリ イメージのバージョン、プレダウンドロード イメージのバージョン、プレダウンドロードの試行時間（必要な場合）、およびプレダウンドロードの試行回数が示されます。また、出力には、各デバイスのプレダウンドロードのステータスも示されます。ステータスには、次の種類があります。

- **None** : プレダウンドロード用のアクセスポイントはスケジュールされません。
- **Predownloading** : アクセスポイントがイメージをプレダウンドロードしています。
- **Not supported** : アクセスポイント（1120、1230、および1310）が、プレダウンドロードをサポートしていません。
- **Initiated** : 同時ダウンドロード制限に達したため、アクセスポイントはプレダウンドロード イメージを取得するために待機しています。
- **Failed** : アクセスポイントは64回、プレダウンドロードの試行に失敗しました。
- **Complete** : アクセスポイントがプレダウンドロードを完了しました。

リポート時間の設定

CLI を使用して、次のいずれかのコマンドを入力し、コントローラおよびアクセスポイントのリポートをスケジュールします。イメージ ダウンドロード フェーズに進まずに、ネットワークが元に戻ります。

- **reset system in HH:MM:SS image {swap | no-swap} reset-aps [save-config]**

このコマンドで、デバイスをリポートする前の遅延時間を指定できます。コントローラによってリセットメッセージがすべての接続アクセスポイントに送信されると、コントローラはリセットされます。**swap** キーワードを使用して、アクセスポイント上のプライマリ イメージとバックアップ イメージを切り替えます。

次のコマンドを入力すると、この出力がコンソールに表示されます。

```
System reset is scheduled for Jan 12 18:12:9 2010.
Current local time and date is Jan 12 12:53:35 2010.
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel.
Configuration will be saved before the system reset.
```

- **reset system at YYYY-MM-DD HH:MM:SS image {swap | no-swap} reset-aps [save-config]**

このコマンドで、デバイスをリブートする日時を指定できます。コントローラによってリセットメッセージがすべての接続アクセス ポイントに送信されると、コントローラはリセットされます。**swap** キーワードを使用して、アクセス ポイント上のプライマリ イメージとバックアップ イメージを切り替えます。

- **reset system notify-time minutes**

このオプションのコマンドは、次回のリセットを通知する SNMP トラップ メッセージをセットアップします。コントローラでは、リセット前に通知トラップの設定された分数が送信されます。次のコマンドを入力すると、この出力がコンソールに表示されます。

```
System reset is scheduled for Jan 12 18:12:9 2010.
Current local time and date is Jan 12 12:53:35 2010.
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel.
Configuration will be saved before the system reset.
```

スケジュールされたリブートをキャンセルするには、**reset system cancel** コマンドを入力します。



(注)

リセット時間を設定して **config time** コマンドを使用し、コントローラのシステム時間を変更する場合、任意のスケジュールされたリセット時間はキャンセルされるため、システムの設定後にその時間を設定する必要があることがコントローラによって通知されます。

show reset コマンドを使用して、スケジュールされたリセットを表示します。コマンドの出力例は次のとおりです。

```
System reset is scheduled for Oct 10 01:01:01 2009.
Current local time and date is Oct 07 02:57:44 2009.
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

スケジュールされたリセット時間にアクセス ポイントがコントローラからイメージをダウンロードしている場合、リセットはキャンセルされ、コントローラ コンソールに次のメッセージが表示されます。

```
%OSAPI-3-RESETSYSTEM_FAILED: osapi_task.c:4458 System will not reset as software is being upgraded.
```

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。

- 「ログイン バナー ファイルのダウンロード」 (P.9-16)
- 「デバイスの証明書のダウンロード」 (P.9-19)
- 「CA 証明書のダウンロード」 (P.9-22)
- 「PAC のアップロード」 (P.9-25)
- 「設定ファイルのアップロードおよびダウンロード」 (P.9-27)

ログイン バナー ファイルのダウンロード

コントローラ ソフトウェア リリース 6.0 以降では、GUI または CLI のいずれかを使用して、ログイン バナー ファイルをダウンロードできます。ログイン バナーとは、Telnet、SSH、およびコンソールポート接続を使用して、コントローラ GUI または CLI にアクセスしたときに、ユーザ認証の前に画面に表示されるテキストのことです。

ログイン バナー情報はテキスト ファイル (*.txt) で保存します。テキスト ファイルは 1500 バイト以下、テキストは 18 行以下でなければなりません。



(注) ASCII 文字セットには、印刷可能な文字と印刷不可能な文字があります。ログイン バナーでは、印刷可能な文字のみをサポートしています。

これはログイン バナーの一例です。

```
Welcome to the Cisco Wireless Controller!
Unauthorized access prohibited.
Contact sysadmin@corp.com for access.
```

この項の手順に従って、GUI または CLI を使用して、ログイン バナーをコントローラにダウンロードします。ただし、ダウンロードを開始する前に、ファイルのダウンロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP 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 または FTP 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。あるいは、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 または FTP 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 または FTP サーバと WCS 内蔵型 TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは WCS と同じコンピュータ上で実行できません。



(注) コントローラの設定をクリアしても、ログイン バナーは削除されません。コントローラ GUI または CLI を使用したログイン バナーのクリアに関する情報は、「[ログイン バナーのクリア](#)」(P.9-19) を参照してください。



(注) コントローラには、1 つのログイン バナー ファイルだけを含めることができます。別のログイン バナー ファイルをコントローラにダウンロードすると、最初のログイン バナー ファイルは上書きされません。

GUI を使用したバナー ファイルのダウンロード

コントローラの GUI を使用してログイン バナー 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** TFTP または FTP サーバ上にあるデフォルトのディレクトリにログイン バナー ファイルをコピーします。

ステップ 2 [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます (図 9-2 を参照してください)。

図 9-2 [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、[Login Banner] を選択します。

ステップ 4 [Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。

ステップ 5 [IP Address] フィールドに、TFTP または FTP サーバの IP アドレスを入力します。

ステップ 6 TFTP サーバを使用している場合は、[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、これらの値は変更できます。値を変更するには、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、ログイン バナー ファイルのディレクトリ パスを入力します。

ステップ 8 [File Name] フィールドに、ログイン バナー ファイル (*.txt) の名前を入力します。

ステップ 9 FTP サーバを使用している場合は、次の手順に従います。

- a. [Server Login Username] フィールドにユーザ名を入力し、FTP サーバにログインします。
- b. [Server Login Password] フィールドにパスワードを入力し、FTP サーバにログインします。
- c. [Server Port Number] フィールドに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

ステップ 10 [Download] をクリックして、ログイン バナー ファイルをコントローラに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。

CLI を使用したバナー ファイルのダウンロード

コントローラの CLI を使用してログイン バナー 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** コントローラの CLI にログインします。
- ステップ 2** `transfer download mode {tftp | ftp}` と入力します。
- ステップ 3** `transfer download datatype login-banner` と入力します。
- ステップ 4** `transfer download serverip server-ip-address` と入力します。
- ステップ 5** `transfer download path server-path-to-file` と入力します。

ステップ 6 `transfer download filename filename.txt` と入力します。

ステップ 7 TFTP サーバを使用している場合は、次のコマンドを入力します。

- `transfer download tftpMaxRetries retries`
- `transfer download tftpPktTimeout timeout`



(注) 10 回の再試行および 6 秒のタイムアウト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、これらの値は変更できます。値を変更するには、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 `retries` パラメータ、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` パラメータに入力します。

ステップ 8 FTP サーバを使用している場合は、次のコマンドを入力します。

- `transfer download username username`
- `transfer download password password`
- `transfer download port port`



(注) `port` パラメータのデフォルト値は 21 です。

ステップ 9 `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..... Login Banner
TFTP Server IP..... 10.10.10.10
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /
TFTP Filename..... banner.txt
```

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

```
TFTP Login Banner transfer starting.
```

```
TFTP receive complete... checking login banner.
```

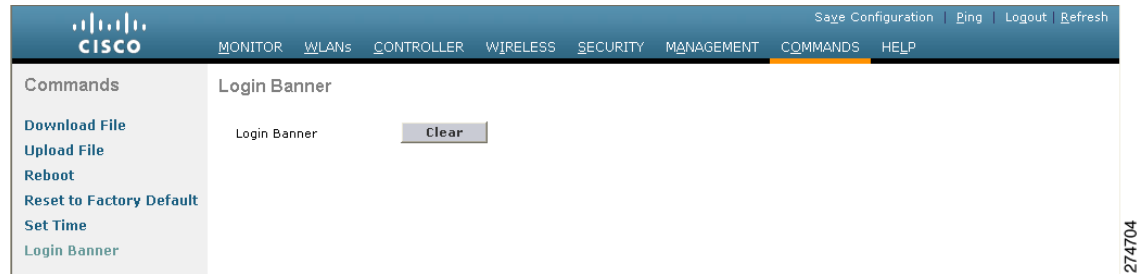
```
Successfully installed new login banner file
```

ログイン バナーのクリア

コントローラ GUI を使用して、次の手順に従い、コントローラからログイン バナーをクリアします。

- ステップ 1** [Commands] > [Login Banner] の順に選択して、[Login Banner] ページを開きます (図 9-3 を参照してください)。

図 9-3 [Login Banner] ページ



- ステップ 2** [Clear] ボタンをクリックします。
- ステップ 3** プロンプトが表示されたら、[OK] をクリックして、バナーをクリアします。

コントローラ CLI を使用してコントローラからログイン バナーをクリアするには、**clear login-banner** コマンドを入力します。

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 の設定の詳細については、「[ローカル EAP の設定](#)」(P.5-40) 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、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、ダウンロードを開始する前に、証明書のダウンロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP 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 または FTP 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。あるいは、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 または FTP 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 または FTP サーバと WCS 内蔵型 TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは 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

コントローラの GUI を使用してデバイスの証明書をコントローラに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 または FTP 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] の順に選択して、[Download File to Controller] ページを開きます (図 9-4 を参照してください)。

図 9-4 [Download File to Controller] ページ

- ステップ 3 [File Type] ドロップダウンリストから、[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 [Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。
- ステップ 6 [IP Address] フィールドに、TFTP または FTP サーバの IP アドレスを入力します。
- ステップ 7 TFTP サーバを使用している場合は、[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、これらの値は変更できません。値を変更するには、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 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 FTP サーバを使用している場合は、次の手順に従います。
 - a. [Server Login Username] フィールドにユーザ名を入力し、FTP サーバにログインします。
 - b. [Server Login Password] フィールドにパスワードを入力し、FTP サーバにログインします。
 - c. [Server Port Number] フィールドに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

- ステップ 11** [Download] をクリックして、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。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 12** ダウンロードの完了後、[Commands] > [Reboot] > [Reboot] の順に選択します。
- ステップ 13** 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 14** [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

コントローラの CLI を使用してデバイスの証明書をコントローラに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 mode {tftp | ftp}** と入力します。
- ステップ 3** **transfer download datatype eapdevcert** と入力します。
- ステップ 4** **transfer download certpassword password** と入力します。
- ステップ 5** **transfer download serverip server-ip-address** と入力します。
- ステップ 6** **transfer download path server-path-to-file** と入力します。
- ステップ 7** **transfer download filename filename.pem** と入力します。
- ステップ 8** TFTP サーバを使用している場合は、次のコマンドを入力します。
- **transfer download tftpMaxRetries retries**
 - **transfer download tftpPktTimeout timeout**



(注) 10 回の再試行および 6 秒のタイムアウト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、これらの値は変更できます。値を変更するには、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 *retries* パラメータ、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* パラメータに入力します。

- ステップ 9** FTP サーバを使用している場合は、次のコマンドを入力します。
- **transfer download username username**
 - **transfer download password password**
 - **transfer download port port**



(注) *port* パラメータのデフォルト値は 21 です。

- ステップ 10** **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 11 `reset system` と入力して、コントローラをリブートします。

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 の設定の詳細については、「[ローカル EAP の設定](#)」(P.5-40) 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、ダウンロードを開始する前に、証明書のダウンロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP 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 または FTP 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。あるいは、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 または FTP 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 または FTP サーバと WCS 内蔵型 TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは 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

コントローラの GUI を使用して CA 証明書をコントローラに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 または FTP 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] の順に選択して、[Download File to Controller] ページを開きます (図 9-5 を参照してください)。

図 9-5 [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 CA Certificate] を選択します。
- ステップ 4** [Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。
- ステップ 5** [IP Address] フィールドに、TFTP または FTP サーバの IP アドレスを入力します。
- ステップ 6** TFTP サーバを使用している場合は、[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、これらの値は変更できます。値を変更するには、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** FTP サーバを使用している場合は、次の手順に従います。
- [Server Login Username] フィールドにユーザ名を入力し、FTP サーバにログインします。
 - [Server Login Password] フィールドにパスワードを入力し、FTP サーバにログインします。
 - [Server Port Number] フィールドに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 10** [Download] をクリックして、CA 証明書をコントローラに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** ダウンロードの完了後、[Commands] > [Reboot] > [Reboot] の順に選択します。
- 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** [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

コントローラの CLI を使用して CA 証明書をコントローラに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 mode {tftp | ftp}` と入力します。
- ステップ 3** `transfer download datatype eapcert` と入力します。
- ステップ 4** `transfer download serverip server-ip-address` と入力します。
- ステップ 5** `transfer download path server-path-to-file` と入力します。
- ステップ 6** `transfer download filename filename.pem` と入力します。
- ステップ 7** TFTP サーバを使用している場合は、次のコマンドを入力します。
- `transfer download tftpMaxRetries retries`
 - `transfer download tftpPktTimeout timeout`



(注) 10 回の再試行および 6 秒のタイムアウト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、これらの値は変更できます。値を変更するには、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 `retries` パラメータ、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` パラメータに入力します。

- ステップ 8** FTP サーバを使用している場合は、次のコマンドを入力します。
- `transfer download username username`
 - `transfer download password password`
 - `transfer download port port`



(注) `port` パラメータのデフォルト値は 21 です。

- ステップ 9** `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 10** `reset system` と入力して、コントローラをリブートします。

PAC のアップロード

Protected Access Credential (PAC) は、自動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 の設定の詳細については、「[ローカル EAP の設定](#)」(P.5-40) 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 のアップロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP 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は、TFTP/FTP サーバが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。サービスポートはルーティングできないからです。同じサブネット上にない場合は、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は、TFTP/FTP 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。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だからです。
- サードパーティの TFTP または FTP サーバと WCS 内蔵型 TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは 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

コントローラ GUI を使用して PAC をコントローラから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] の順に選択して、[Upload File from Controller] ページを開きます (図 9-6 を参照)。

図 9-6 [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、[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** [Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。
- ステップ 7** [IP Address] フィールドに、TFTP または FTP サーバの IP アドレスを入力します。
- ステップ 8** [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 9** [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 10** FTP サーバを使用している場合は、次の手順に従います。
- [Server Login Username] フィールドにユーザ名を入力し、FTP サーバにログインします。
 - [Server Login Password] フィールドにパスワードを入力し、FTP サーバにログインします。
 - [Server Port Number] に、アップロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 11** [Upload] をクリックして、コントローラから PAC 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 12** 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

コントローラ CLI を使用して PAC をコントローラから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 mode {tftp | ftp}` と入力します。
- ステップ 3** `transfer upload datatype pac` と入力します。
- ステップ 4** `transfer upload pac username validity password` と入力します。
- ステップ 5** `transfer upload serverip server-ip-address` と入力します。
- ステップ 6** `transfer upload path server-path-to-file` と入力します。
- ステップ 7** `transfer upload filename manual.pac` と入力します。
- ステップ 8** FTP サーバを使用している場合は、次のコマンドを入力します。
- `transfer upload username username`
 - `transfer upload password password`
 - `transfer upload port port`



(注) `port` パラメータのデフォルト値は 21 です。

- ステップ 9** `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 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。

設定ファイルのアップロードおよびダウンロード

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バックアップすることを推奨します。一部の設定が失われた場合には、保存した設定をコントローラにダウンロードすることができます。



- (注)** 別のコントローラ プラットフォームからアップロードしたコントローラに設定ファイルをダウンロードしないよう注意してください。たとえば、5500 シリーズのコントローラは、4400 または 2100 シリーズのコントローラの設定ファイルをサポートしていません。

コントローラ ソフトウェア リリース 4.2 以降では、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、ソフトウェア リリース 4.2 以降が稼働しているコントローラにバイナリの設定ファイルを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 以降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)** コントローラ ソフトウェア リリース 5.2 以降を使用すると、設定ファイルを読み取ったり、修正したりすることができます。詳細は、「[設定ファイルの編集](#)」(P.9-32) を参照してください。5.2 以前のコントローラのソフトウェア リリースでは、設定ファイルを修正できません。4.2、5.0、または 5.1 設定ファイルに変更を試みてからファイルをコントローラにダウンロードすると、コントローラのレポート時に設定パラメータがデフォルト値に戻される際、コントローラにより巡回冗長検査 (CRC) エラーが表示されます。

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サーバに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] の順に選択して、[Upload File from Controller] ページを開きます (図 9-7 を参照)。

図 9-7 [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。
- ステップ 3** 設定ファイルを暗号化するには、[Configuration File Encryption] チェックボックスをオンにして [Encryption Key] フィールドに暗号化キーを入力します。
- ステップ 4** [Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。
- ステップ 5** [IP Address] フィールドに、TFTP または FTP サーバの IP アドレスを入力します。
- 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。
- ステップ 8** FTP サーバを使用している場合は、次の手順に従います。
- a. [Server Login Username] フィールドにユーザ名を入力し、FTP サーバにログインします。
 - b. [Server Login Password] フィールドにパスワードを入力し、FTP サーバにログインします。
 - c. [Server Port Number] に、アップロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 9** [Upload] をクリックし、設定ファイルを TFTP または FTP 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。アップロードに失敗すると、この手順が繰り返され、再試行されます。

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サーバにアップロードする手順は、次のとおりです。

- ステップ 1** 設定ファイルのダウンロードに使用する転送モードを指定するには、このコマンドを入力します。
- ```
transfer upload mode {tftp | ftp}
```
- ステップ 2** アップロードするタイプを指定するには、次のコマンドを入力します。

```
transfer upload datatype config
```

**ステップ 3** 設定ファイルを暗号化するには、次のコマンドを入力します。

  - **transfer encrypt enable**
  - **transfer encrypt set-key key**、ここで、*key* はファイルの暗号化に使用する暗号化キーです。

**ステップ 4** TFTP または FTP サーバの IP アドレスを指定するには、次のコマンドを入力します。

```
transfer upload serverip server-ip-address
```

**ステップ 5** 設定ファイルのディレクトリ パスを指定するには、次のコマンドを入力します。

**transfer upload path** *server-path-to-file*

**ステップ 6** アップロードする設定ファイルの名前を指定するには、次のコマンドを入力します。

**transfer upload filename** *filename*

**ステップ 7** FTP サーバを使用している場合、FTP サーバへのログインで使用するユーザ名およびパスワード、アップロードが発生するポート番号を指定するには、次のコマンドを入力します。

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*



(注) *port* パラメータのデフォルト値は 21 です。

**ステップ 8** アップロード プロセスを開始するには、次のコマンドを入力します。

**transfer upload start**

**ステップ 9** 現在の設定を確認するプロンプトが表示されたら、**y** と答えます。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.
```

アップロードに失敗すると、この手順が繰り返され、再試行されます。

## 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] の順に選択して、[Download File to Controller] ページを開きます (図 9-8 を参照してください)。

図 9-8 [Download File to 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。
- ステップ 3** 設定ファイルが暗号化されている場合は、[Configuration File Encryption] チェックボックスをオンにして、[Encryption Key] フィールドにファイルの暗号化解除に使用する暗号化キーを入力します。



(注) ここで入力するキーは、アップロードプロセス中に入力したキーと一致させる必要があります。

- ステップ 4** [Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。
- ステップ 5** [IP Address] フィールドに、TFTP または FTP サーバの IP アドレスを入力します。
- ステップ 6** TFTP サーバを使用している場合は、[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、これらの値は変更できます。値を変更するには、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 7** [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 8** [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 9** FTP サーバを使用している場合は、次の手順に従います。
- [Server Login Username] フィールドにユーザ名を入力し、FTP サーバにログインします。
  - [Server Login Password] フィールドにパスワードを入力し、FTP サーバにログインします。
  - [Server Port Number] フィールドに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 10** [Download] をクリックして、ファイルをコントローラに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、コントローラが自動的にリブートされます。ダウンロードに失敗すると、この手順が繰り返され、再試行されます。

## 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にダウンロードする手順は、次のとおりです。



(注) コントローラは差分設定のダウンロードをサポートしていません。設定ファイルには、ダウンロードが正常に完了するのに必要なすべての必須 CLI (すべてのインターフェイス アドレス CLI、読み取りおよび書き込み権限 CLI を持つ `mgmtuser`、およびインターフェイス ポートまたは LAG の有効または無効 CLI) が含まれています。たとえば、設定ファイルの一部として `config time ntp server index server_address` のみをダウンロードすると、ダウンロードは失敗します。設定ファイルに含まれる CLI コマンドだけがコントローラに適用されるため、ダウンロード前のコントローラの設定はすべて削除されます。

**ステップ 1** 設定ファイルのダウンロードに使用する転送モードを指定するには、次のコマンドを入力します。

**transfer download mode {tftp | ftp}**

**ステップ 2** ダウンロードするタイプを指定するには、次のコマンドを入力します。

**transfer download datatype config**

**ステップ 3** 設定ファイルが暗号化されている場合は、次のコマンドを入力します。

- **transfer encrypt enable**
- **transfer encrypt set-key key**、ここで、*key* はファイルの暗号化解除に使用する暗号化キーです。



(注) ここで入力するキーは、アップロードプロセス中に入力したキーと一致させる必要があります。

**ステップ 4** TFTP または FTP サーバの IP アドレスを指定するには、次のコマンドを入力します。

**transfer download serverip server-ip-address**

**ステップ 5** 設定ファイルのディレクトリ パスを指定するには、次のコマンドを入力します。

**transfer download path server-path-to-file**

**ステップ 6** ダウンロードする設定ファイルの名前を指定するには、次のコマンドを入力します。

**transfer download filename filename**

**ステップ 7** TFTP サーバを使用している場合は、次のコマンドを入力します。

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**



(注) 10 回の再試行および 6 秒のタイムアウト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、これらの値は変更できます。値を変更するには、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 *retries* パラメータ、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* パラメータに入力します。

**ステップ 8** FTP サーバを使用している場合、FTP サーバへのログインで使用するユーザ名およびパスワード、ダウンロードが発生するポート番号を指定するには、次のコマンドを入力します。

- **transfer download username username**
- **transfer download password password**
- **transfer download port port**



(注) *port* パラメータのデフォルト値は 21 です。

**ステップ 9** 更新された設定を表示するには、次のコマンドを入力します。

**transfer download start**

**ステップ 10** 現在の設定を確認し、ダウンロードプロセスを開始するプロンプトが表示されたら、**y** と答えます。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.
```

ダウンロードに失敗すると、この手順が繰り返され、再試行されます。

## 設定の保存

コントローラには、揮発性メモリと不揮発性メモリの2種類のメモリが搭載されています。次のコマンドのいずれかを使用して、アクティブな揮発性メモリから不揮発性メモリに設定の変更を随時保存できます。

- **save config** : コントローラをリセットせずに、揮発性メモリから不揮発性メモリに設定を保存できます。
- **reset system** : 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** : 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。

## 設定ファイルの編集

コントローラの設定を保存する場合、コントローラによりフラッシュメモリ内にXML形式で格納されます。コントローラソフトウェアリリース5.2以降では、設定ファイルをCLI形式に変換し、簡単に読み取ったり修正したりすることができます。設定ファイルをTFTPまたはFTPサーバにアップロードすると、コントローラではXMLからCLIへの変換が開始されます。さらに、サーバ上でCLI形式の設定ファイルを読み取ったり、編集したりすることができます。操作を完了したら、コントローラにファイルをダウンロードして、XML形式に再度変換し、保存します。

コントローラの設定ファイルを編集する手順は、次のとおりです。

**ステップ 1** 設定ファイルをTFTPまたはFTPサーバにアップロードするには、次のいずれかの手順を実行します。

- コントローラ GUI を使用してファイルをアップロードします。「[GUIを使用した設定ファイルのアップロード](#)」(P.9-27) の手順に従ってください。



- コントローラ CLI を使用してファイルをアップロードします。「[CLI を使用した設定ファイルのアップロード](#)」(P.9-28) の手順に従ってください。

**ステップ 2** サーバの設定ファイルを読み取るか、編集します。既存の CLI コマンドを修正または削除して、新しい CLI コマンドをファイルに追加できます。



(注) 設定ファイルを編集するには、Windows のメモ帳、ワードパッド、または Linux の VI エディタのいずれかを使用できます。

**ステップ 3** 変更をサーバ上の設定ファイルに保存します。

**ステップ 4** 設定ファイルをコントローラにダウンロードするには、次のいずれかを実行します。

- コントローラ GUI を使用してファイルをダウンロードします。「[GUI を使用した設定ファイルのダウンロード](#)」(P.9-29) の手順に従ってください。
- コントローラ CLI を使用してファイルをダウンロードします。「[CLI を使用した設定ファイルのダウンロード](#)」(P.9-30) の手順に従ってください。

コントローラでは、設定ファイルが XML 形式に変換されて、フラッシュ メモリに保存され、新しい設定を使用してリブートされます。既知のキーワードおよび正しい構文を持つ CLI コマンドは XML に変換されますが、不適切な CLI コマンドは無視されてフラッシュ メモリに保存されます。無効な値を持つすべての CLI コマンドはデフォルトの値に置き換えられます。無視されたコマンドおよび無効な設定値を確認するには、次のコマンドを入力します。

**show invalid-config**



(注) このコマンドは **clear config** または **save config** コマンドのあとには実行できません。

**ステップ 5** ダウンロードした設定に多数の無効な CLI コマンドが含まれている場合、分析のため、無効な設定を TFTP または FTP サーバにアップロードできます。無効な設定をアップロードするには、次のいずれかを実行します。

- コントローラ GUI を使用して無効な設定をアップロードします。「[GUI を使用した設定ファイルのアップロード](#)」(P.9-27) の手順に従いますが、**ステップ 2** の [File Type] ドロップダウン ボックスで [Invalid Config] を選択し、**ステップ 3** をスキップします。
- コントローラ CLI を使用して無効な設定をアップロードします。「[CLI を使用した設定ファイルのアップロード](#)」(P.9-28) の手順に従いますが、このコマンドを**ステップ 2: transfer upload datatype invalid-config** に入力し、**ステップ 3** をスキップします。

**ステップ 6** コントローラは、ポート設定 CLI コマンドのアップロードおよびダウンロードをサポートしていません。コントローラ ポートを設定する場合は、次のコマンドを入力します。

- **config port linktrap {port | all} {enable | disable}** : 特定のコントローラ ポートまたはすべてのポートでアップ リンク トラップおよびダウン リンク トラップを有効または無効にします。
- **config port adminmode {port | all} {enable | disable}** : 特定のコントローラ ポートまたはすべてのポートで管理モードを有効または無効にします。

**ステップ 7** 変更を保存するには、次のコマンドを入力します。

**save config**

## コントローラの設定のクリア

不揮発性メモリ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方法」(P.2-2) の指示に従って、初期設定を完了します。
- 

## 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、設定変更を不揮発性メモリに保存します。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します。
  - ステップ 3 「設定ウィザードの使用方法」(P.2-2) の指示に従って、初期設定を完了します。
- 

## コントローラのリセット

次の 2 つの方法のうちいずれかを使用して、コントローラをリセットし、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、設定変更を不揮発性メモリに保存します。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。