



## ネットワークの管理

---

- [管理アクセスインターフェイスの設定](#) (1 ページ)
- [Admin アカウントの管理](#) (2 ページ)
- [ロビー管理者アカウントを使用したゲスト ユーザの管理](#) (4 ページ)
- [日時の設定](#) (6 ページ)
- [Cisco Mobility Express ソフトウェアの更新](#) (9 ページ)
- [設定管理](#) (18 ページ)

### 管理アクセス インターフェイスの設定

管理アクセス インターフェイスは、コントローラのインバンド管理やエンタープライズ サービスへの接続に使用されるデフォルトインターフェイスです。また、コントローラとアクセスポイント (AP) 間の通信にも使用されます。管理インターフェイスには、唯一常時 ping 可能な、コントローラのインバンドインターフェイス IP アドレスが設定されています。コントローラの Web インターフェイスにアクセスするには、ブラウザのアドレス バーに、コントローラの管理インターフェイスの IP アドレスを入力します。

AP の場合、ポートの数に関係なく、このコントローラには、コントローラ間の全通信を制御する管理インターフェイスが1つと、コントローラとアクセスポイント間の全通信を制御する AP マネージャ インターフェイスが1つ必要です。

以下の操作を行って、コントローラへの管理アクセスのタイプを有効または無効にします。

---

**ステップ 1** [Management] > [Access] を選択します。

[Management Access] ウィンドウが表示されます。有効にした管理タイプの数が、ウィンドウの上部に表示されます。

**ステップ 2** コントローラへの管理アクセスのタイプを有効または無効にするには、ドロップダウンリストから該当するオプションを選択します。

- **HTTP Access** : HTTP アクセス モードを有効にして、Web ブラウザで `http://<ip-address>` を使用してコントローラの GUI にアクセスできるようにするには、[HTTP Access] ドロップダウン リストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。

デフォルト値は [Disabled] です。

(注) HTTP アクセス モードの接続は、セキュリティで保護されません。

- **HTTPS Access** : HTTPS アクセス モードを有効にして、Web ブラウザで `http://ip-address` を使用してコントローラの GUI にアクセスできるようにするには、[HTTPS Access] ドロップダウンリストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。

デフォルト値は [Enabled] です。

(注) HTTPS アクセス モードの接続は、セキュリティで保護されます。

- **Telnet Access** : Telnet アクセス モードを有効にして、ラップトップのコマンドプロンプトを使用してコントローラの CLI へのリモート アクセスを可能にするには、[Telnet Access] ドロップダウン リストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。

デフォルト値は [Disabled] です。

(注) Telnet アクセス モードの接続は、セキュリティで保護されません。

- **SSHv2 Access** : Secure Shell バージョン 2 (SSHv2) アクセス モードを有効にするには、[SSHv2 Access] ドロップダウン リストから [Enabled] を選択します。このアクセス モードは、Telnet のセキュリティを強化したもので、データ暗号化およびセキュアチャネルを使用してデータを転送します。有効にしない場合は、[Disabled] を選択します。

デフォルト値は [Enabled] です。

(注) SSHv2 アクセス モードの接続は、セキュリティで保護されます。

ステップ 3 [Apply] をクリックして変更内容を保存します。

## Admin アカウントの管理

Cisco Mobility Express は、ユーザアカウントに割り当てられている権限に基づいて、Cisco Mobility Express コントローラの GUI から管理できます。これにより、権限のないユーザがコントローラにアクセスしたり、コントローラを設定したりするのを防ぐことができます。

Cisco Mobility Express の GUI へは、次のアクセス タイプのいずれかを持つ管理者アカウントを使用してログインできます。

- **読み取り/書き込み** : この管理アカウントには、コントローラ コンフィギュレーションを表示および変更するためのすべてのアクセス権があります。
- **読み取り専用** : この制限付きアクセスの管理アカウントでは、ユーザはコントローラ コンフィギュレーションの表示のみを行えます。このユーザは、設定に変更を加えることはできません。
- **ロビー アンバサダー** : この制限付きの管理アカウントでは、ユーザはゲスト ユーザアカウントの作成および管理のみを行なえます。また、ロビー アンバサダーはゲスト ユーザアカウントのクレデンシャルを印刷または電子メールすることができます。

ゲストユーザアカウントの作成については、「[ゲストユーザアカウントの作成](#)」を参照してください。

## 管理者アカウントの追加

**ステップ 1** [Management] > [Admin Accounts] の順に選択します。

Cisco Mobility Express コントローラの管理者アカウントの総カウントがこのウィンドウの上部に表示され、利用可能なすべての管理者アカウントの詳細なリストがテーブルに表示されます。

[Admin Accounts] ウィンドウが表示されます。

**ステップ 2** [Add New User] をクリックして、新規管理者ユーザを追加します。  
新しい編集可能な行エントリがテーブルに表示されます。

**ステップ 3** 必要に応じて、次のパラメータを設定します。

- **Account name** : 管理者ユーザが使用するログイン ユーザ名。管理者アカウント名は一意でなければなりません。
- **Access** : 管理者のアクセス権限を次のいずれかに設定します。
  - **Read Only**
  - **Read/Write**
  - **Lobby Ambassador**
- **[Password]** : パスワードは大文字と小文字が区別され、次のガイドラインに基づいて作成する必要があります。
  - 8 文字以上で、大文字および小文字と、数字、特殊文字を組み合わせて使用します。
  - Cisco という語や管理ユーザ名を含めることはできず、次の方法で取得したこれらの語の変形も使用できません。
    - これらの語の文字を反転させる
    - 文字の大文字と小文字を変更する
    - 次のように置き換える
      - i の代わりに 1、|、または!
      - o の代わりに 0
      - s の代わりに \$
  - パスワード内で同じ文字を 4 回以上続けて繰り返すことはできません。

ステップ4 [Apply] をクリックして変更内容を保存します。

---

## 管理者アカウントの編集

---

ステップ1 [Management] > [Admin Accounts] の順に選択します。

[Admin Accounts] ページが表示され、Cisco Mobility Express コントローラ上のすべての管理者アカウントがリストされます。コントローラ上の管理者アカウントの総数がページの上部に表示されます。

ステップ2 編集するアカウントの横にある [Edit] アイコンをクリックします。

ステップ3 管理者アカウントパラメータを必要に応じて変更します。これらのパラメータの詳細については、[管理者アカウントの追加 \(3 ページ\)](#) を参照してください。

ステップ4 [Apply] をクリックします。

---

## 管理者アカウントの削除

---

ステップ1 [Management] > [Admin Accounts] の順に選択します。

[Admin Accounts] ウィンドウが表示され、Cisco Mobility Express コントローラ上のすべての管理者アカウントがリストされます。コントローラ上の管理者アカウントの総数がページの上部に表示されます。

ステップ2 削除するアカウントの横にある [Delete] アイコンをクリックします。

ステップ3 確認ダイアログ ボックス内の [Ok] をクリックします。

---

## ロビー管理者アカウントを使用したゲストユーザの管理

ネットワークに一時的にアクセスできるようにするためにゲスト ユーザ アカウントを作成します。このネットワーク アクセスは、ゲスト アカウントのクレデンシャルが正常に認証された後に与えられます。

ロビー アンバサダー管理者アカウントを使用して、ゲスト ユーザ アカウントを作成、管理できます。ロビー アンバサダー アカウントの詳細については、[Admin アカウントの管理 \(2 ページ\)](#) を参照してください。

## ゲストユーザアカウントの作成

### 始める前に

ゲストユーザアカウントを作成する前に、1つ以上のロビーアンバサダーユーザアカウントを所有している必要があります。ロビーアンバサダーアカウントの作成については、[管理者アカウントの追加 \(3 ページ\)](#) を参照してください。

**ステップ 1** ブラウザで Cisco Mobility Express の GUI まで移動します。

**ステップ 2** ロビーアンバサダー クレデンシャルを使用してログインします。

[Lobby Ambassador Guest Management] ウィンドウが表示されます。

**ステップ 3** [Add Guest User] をクリックします。

[Add Guest User] ダイアログボックスが表示されます。

**ステップ 4** ゲストユーザアカウントの次の詳細を入力します。

- **[ユーザ名 (User Name)]**

- **[Wireless Network]** : ネットワークへのゲストアクセス用にすでに設定されている特定のゲスト WLAN を選択します。ゲスト WLAN が設定されていないか、またはゲスト WLAN を選択しなかった場合は、デフォルトで [All Guest WLANs] が選択されます。

(注) ゲスト WLAN の作成の詳細については、[WLAN の追加](#) を参照してください。

- **[Permanent User]** : このゲストユーザアカウントが時間制限なくネットワークにアクセスできるようにするには、このチェックボックスを選択します。

- **[Expiry Date & Time]** : カレンダーとクロックアイコンをそれぞれクリックして、日時を指定します。ゲストユーザアカウントは指定した日時に無効になり、ゲストネットワークへのアクセスを防ぎます。

(注) [Permanent User] チェックボックスがオンになっている場合は、このフィールドはダイアログボックスに表示されません。

- **[Generate Password]** : 作成中のゲストユーザアカウントにパスワードを自動的に生成するには、このオプションボタンをクリックします。

ゲストユーザアカウントのパスワードを手動で指定する場合は、[Password] フィールドと [Confirm Password] フィールドにそのパスワードを入力します。

- **Password**

(注) [Generate Password] オプションボタンをクリックすると、このフィールドはダイアログボックスに表示されなくなります。

- **[Confirm Password]** : このエントリが [Password] フィールドの入力と一致していることを確認します。

- **Description**

ステップ 5 [Update] をクリックします。

アカウントのクレデンシャルは電子メールを介して、または印刷することでゲスト ユーザと共有できません。

[Guest User Credentials] ポップアップが表示されるとともに、[Guest Users List] テーブルが更新され、この新しいゲスト ユーザ アカウントのエントリが含まれます。

## 日時の設定

Cisco Mobility Express コントローラの日時は最初、コントローラの初期設定セットアップ ウィザードを実行したときに設定されます。日時は手動で入力することも、日時を設定する Network Time Protocol (NTP) サーバを指定することもできます。

### 自動的に日時を設定するための NTP サーバの使用

コントローラが自動的に同期して日時を設定するための Network Time Protocol (NTP) サーバを 3 つまで指定できます。

デフォルトで 3 つの NTP サーバが自動的に作成されます。NTP サーバのデフォルトの完全修飾ドメイン名 (FQDN) は次のとおりです。

- 0.ciscome.pool.ntp.org (NTP のインデックス値 1)
- 1.ciscome.pool.ntp.org (NTP のインデックス値 2)
- 2.ciscome.pool.ntp.org (NTP のインデックス値 3)

初期設定ウィザードで NTP サーバの IPv4 アドレスまたは FQDN 名を指定できます。これは NTP インデックス 1 を持つサーバに適用されてそのデフォルトの FQDN である *0.ciscome.pool.ntp.org* を上書きします。

NTP サーバの詳細を追加および編集するには、[Management] > [Time] に進みます。これにより、[Time Settings] ページが開きます。

### NTP サーバの追加と編集

コントローラが自動的に日時を設定するための Network Time Protocol (NTP) サーバを 3 つまで指定できます。

ステップ 1 [Management] > [Time] の順に選択します。

[Time Settings] ウィンドウが表示され、設定されているタイムゾーンがページ上部に表示されます。現在の日時は [Set Time Manually] フィールドに表示されます。既存の NTP サーバがある場合、[NTP Index] 値の順に表示されます。

**ステップ 2** [NTP Polling Interval] フィールドに、ポーリング間隔（秒単位）を指定します。

**ステップ 3** 既存の NTP サーバを編集するには、その隣の [Edit] アイコンをクリックします。新しい NTP サーバを追加するには、[Add NTP Server] をクリックします。

**ステップ 4** NTP サーバの次の値を追加、編集できます。

- a) NTP サーバのプライオリティを設定するには、[NTP Index] ボックスで NTP のインデックス値を指定します。NTP のインデックス値は、プライオリティが高いものから順に 1 から 3 まで設定できます。コントローラは、最初にプライオリティが最も高いものから、指定されたポーリング間隔の時間の終わりまで NTP サーバと同期を試みます。同期が完了すると、コントローラは続けて残りの NTP サーバとの同期を試みます。同期が失敗した場合、コントローラは次の NTP サーバとの同期を試みます。
- b) [NTP Server] ボックスで、NTP サーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を指定します。FQDN を指定すると、DNS ルックアップが実行されます。ルックアップに失敗すると、エラーのログが `syslog` サーバに記録されます。コントローラは、NTP の設定を変更するかまたは有効な FQDN を指定するまでこの FQDN の解決を継続し、エラーがログに記録されます。
- c) すべての AP（内部と外部の両方）をコントローラが同期するのと同じ NTP サーバと同期させる場合は、[AP に適用 (Apply for APs)] オプションを有効にします。
  - [Apply for APs] オプションでは、一度に 1 つの NTP サーバのみ設定できます。このオプションで 1 つの NTP サーバを設定すると、他のすべての設定済み NTP サーバは冗長になり、これらの冗長サーバへは接続されません。また、NTP サーバのフォールバックもありません。
  - このオプションを有効にすると、NTP サービスがコントローラで再起動されます。
  - [Apply for APs] オプションをサポートしていないリリースからサポートしているリリースにアップグレードすると、デフォルトでは [Apply for APs] オプションによって NTP サーバは設定されません。
  - [Apply for APs] オプションをサポートしているリリースから、サポートしていない旧リリースにダウングレードすると、ダウングレード後に [Apply for APs] の設定は失われます。
  - 高可用性シナリオでは、[Apply for APs] オプションの設定はスタンバイユニットと同期されます。

**ステップ 5** [Apply] をクリックします。

---

## グローバル NTP サーバの設定 (CLI)

---

**ステップ 1** 次のコマンドを入力して、グローバル NTP サーバを設定します。この設定は、コントローラが時間に関する情報を取得して、外部 AP に送信するために使用します。

```
config advanced apgroup-global-ntp add ntp-server-index
```

**ステップ 2** （任意）次のコマンドを入力して、グローバル NTP サーバを削除します。

```
config advanced apgroup-global-ntp delete
```

**ステップ 3** 次のコマンドを入力して、1 つまたはすべての AP のグローバル NTP サーバに関する情報を表示します。

```
show ap ntp-server-info {all | cisco-ap}
```

**ステップ 4** 次のコマンドを入力して、AP グループに設定されているグローバル NTP サーバに関する情報を表示します。

```
show advanced apgroup-global-ntp
```

## NTP サーバステータスの更新

[Time Settings] ページの NTP サーバ テーブルの [NTP Status] 列には、各 NTP サーバへの接続のステータスが表示されます。ステータスは次のいずれかになります。

- [Not Tried] : 同期はまだ試行されていません。
- [In Sync] : コントローラの時間は NTP サーバと同期されている状態です。
- [Not Synched] : コントローラ的时间は NTP サーバと同期されていません。
- [In Progress] : 現在、同期の試行中です。

[Refresh] をクリックすると、更新された NTP の状態をいつでも確認することができます。

## NTP サーバの削除と無効化

NTP サーバを削除するには、[Management] > [Time] の順に選択します。表示される [Time Settings] ページで、削除する NTP サーバの隣の [Delete] アイコンをクリックします。確認ダイアログで [OK] をクリックし、次に [Apply] をクリックします。

NTP サーバによる日時の設定を無効にするには、上記の手順に従って、すべての設定済み NTP サーバを削除する必要があります。

## 日時の手動設定

**ステップ 1** [Management] > [Time] の順に選択します。

[Time Settings] ウィンドウが表示され、設定されているタイムゾーンがページ上部に表示されます。現在の日時が [Set Time Manually] フィールドに表示されます。

(注) これらのフィールドは、[NTP State] が [Enable] に設定されている場合は編集できません。

**ステップ 2** [NTP State] ドロップダウンリストから [Disable] を選択します。

**ステップ 3** [Time Zone] ドロップダウンリストからローカルタイムゾーンを選択します。

Daylight Saving Time (DST; 夏時間) を使用する時間帯を選択すると、DST の発生時の時間変更を反映してコントローラが自動的にそのシステムクロックを設定します。米国では、DST は 3 月の第 2 日曜日始まり、11 月の第 1 日曜日で終わります。

**ステップ 4** [Set Time Automatically from Current Location] チェックボックスをオンにして、指定したタイムゾーンに基づいて時刻を設定します。

**ステップ 5** [Set Time Manually] フィールドで次の操作を行います。

- カレンダーアイコンをクリックし、月、日、年を選択します。
- 時計アイコンをクリックし、時刻（時と分）を指定します。

ステップ 6 [Apply] をクリックします。

## Cisco Mobility Express ソフトウェアの更新

以下の操作を行って、Cisco Mobility Express コントローラの現在のソフトウェアバージョンを表示します。

- Web インターフェイスの右上隅にある歯車アイコンをクリックしてから、[System Information] をクリックします。
- [Management] > [Software Update] の順に選択します。

これにより [Software Update] ウィンドウが表示され、その上部に現在のソフトウェアのバージョン番号が表示されます。

コントローラの Web インターフェイスを使用して Cisco Mobility Express コントローラ ソフトウェアを更新できます。Cisco Mobility Express コントローラ上の現在の設定は削除されません。

次の表に、利用可能なソフトウェア アップデート方法を示します。

方法	方法へのリンク
HTTP を使用したソフトウェア アップデート (注) この方法は (ap1g4 および ap3g3 イメージをサポートする) Cisco Aironet 1830、1850、2800、および 3800 アクセスポイントだけでネットワークが構成されている場合にのみ使用できます。	<a href="#">HTTP を使用したソフトウェア アップデート (11 ページ)</a> を参照してください。
TFTP を使用したソフトウェア アップデート	<a href="#">TFTP を使用したソフトウェア アップデート (13 ページ)</a> を参照してください。
SFTP を使用したソフトウェア アップデート	<a href="#">SFTP を使用したソフトウェア アップデート (15 ページ)</a> を参照してください。
Cisco.com からのソフトウェア直接アップデート	<a href="#">Cisco.com からのソフトウェア直接アップデート (16 ページ)</a> を参照してください。

ソフトウェアを更新すると、内部コントローラソフトウェアが更新されるだけでなく、関連付けられているすべての AP 上の AP ソフトウェアも更新されます。AP 上の Cisco Mobility Express AP ソフトウェアのバージョンが古い場合、ソフトウェア アップグレード後にマスター AP に

join すると、Cisco Mobility Express AP ソフトウェアが自動的にアップグレードされて、最新のソフトウェアになります。これは、ソフトウェアのアップデートプロセス中に、コントローラに関連付けられているすべての Cisco Mobility Express サポート対象 AP 用の最新の Cisco Mobility Express ソフトウェアもダウンロードされるためです。コントローラに join する AP が、Cisco Mobility Express ソフトウェアのバージョンとマスター AP 上のバージョンを比較し、不一致が検出されると、新しい AP がソフトウェアのアップグレードを要求します。マスター AP が、TFTP サーバまたは HTTP パスから新しい AP への新しいソフトウェアの転送を支援します。

ソフトウェアのダウンロードはバックグラウンドで実行されるため、ネットワークには影響がありません。ソフトウェアアップデートがネットワークのパフォーマンスに影響しないようにするため、アップグレードは自動的に順次実行されます。



(注) 5 つまでのアクセス ポイントのソフトウェアを同時に更新できます。

## 異種ネットワークに対応するための AP の効率的な接続

効率的な AP の参加機能では、新しい AP がネットワークに参加すると、AP はネットワーク ファイル サーバからではなく、イメージ マスター AP からイメージをダウンロードします。新しい AP がネットワークに参加し、同じイメージ タイプの別の AP がすでにネットワークに存在している場合、新しい AP は既存の AP (イメージ マスター) からイメージをダウンロードします。その結果、WAN ネットワーク上のトラフィックが減少します。

効率的な AP 参加イメージのダウンロードのシーケンスは次のとおりです。

- 新しい AP (スレーブ AP) が Mobility Express (ME) ネットワークに参加すると、ME はまず、効率的な AP の参加機能が有効であるか、AP のタイプが Cisco Wave 2 AP であるか、およびイメージのバージョンが 8.8 またはそれ以降であるかをチェックします。
- ME は、マスターおよびスレーブの設定メッセージを選択したマスターに送信します。トリガーのメッセージは、加入メッセージへの応答として、スレーブに送信されます。
- その後、スレーブ AP は、TFTP 経由でイメージをダウンロードするイメージのマスター AP を問い合わせます。イメージのマスター AP からの応答がないと、スレーブ AP はイメージ マスター AP に TFTP 要求を継続的に送信し、再試行回数を超過した場合、ディスカバリ モードに戻ります。
- スレーブ AP がイメージ マスターからイメージを正常にダウンロードすると、スレーブ AP は再起動し、新しいイメージで ME に参加します。



(注) システムに十分なメモリがない場合は、フォールバック機能により、外部サーバから新しく参加した AP にイメージがストリーミングされます。

転送モードを HTTP に設定している場合、このフォールバック機能はサポートされません。

## AP の効率的な参加の設定

### 始める前に

効率的な AP の参加機能をサポートするには、Cisco Wireless リリースのバージョンは 8.8 以降である必要があります。

**ステップ 1** [Management] > [Software Update] に移動します。

**ステップ 2** [効率的な参加 (Efficient Join) ] オプションを有効にし、[適用 (Apply) ] ボタンをクリックします。

[効率的な参加 (Efficient Join) ] 機能を有効または無効にするには、次のコマンドを使用します。デフォルトでは、この機能は有効です。

```
(Cisco Controller) > config flexconnect group default-flexgroup efficient-join {enable | disable}
```

## AP の効率的な参加のステータスを確認

ME での AP の効率的な参加機能のステータスを確認するには、次の **show** コマンドを使用します。

```
(Cisco Controller) > show flexconnect group detail default-flexgroup
```

ダウンロードの進捗状況を確認するには、次 **show** コマンドを使用します。

```
(Cisco Controller) > show ap image all
```

```
(Cisco Controller) > show flexconnect efficient-upgrade aps
```

## HTTP を使用したソフトウェア アップデート

### 始める前に

ネットワークが (ap1g4 および ap3g3 イメージをサポートする) 1830、1850、2800、および 3800 アクセス ポイントのみで構成されている場合にのみ、HTTP を介してソフトウェア アップデートを実行できます。ネットワーク内にサポートされている他の AP モデルがある場合は、TFTP を使用するか、または Cisco.com から直接更新します。

**ステップ 1** 以下のステップに従って、コントローラ ソフトウェアのイメージを入手します。

- コンピュータを使用して、[Cisco Download Software] ページ (URL : <http://www.cisco.com/cisco/software/navigator.html>) にアクセスします。
- AP モデルに移動し、[Mobility Express Software] をクリックすると、現在使用可能なソフトウェアのリストが最新リリースから順に表示されます。
- ソフトウェア リリース番号を選択します。
- ZIP ファイルに対応する [Download] をクリックします。
- 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。

- f) ZIP ファイルをコンピュータのハード ドライブに保存し、その内容をコンピュータのディレクトリに抽出します。

**ステップ 2** Cisco Mobility Express コントローラの Web インターフェイスから [Management] > [Software Update] を選択します。

[Software Update] ウィンドウが表示され、現在のソフトウェアのバージョン番号が表示されます。

**ステップ 3** [Transfer Mode] ドロップダウンリストから [HTTP] を選択します。

**ステップ 4** [File] フィールドの横にある [Browse] ボタンをクリックし、展開された ZIP ファイルの内容が含まれているフォルダを参照し、次の表に示すようにソフトウェア ファイルを選択します。

Cisco Mobility Express コントローラの Cisco AP シリーズ	選択するソフトウェア ファイル
1830、1850	ap1g4
2800、3800	ap3g3

(注) ここで開くファイルエクスプローラは、オペレーティングシステム固有のエクスプローラで、コンピュータの OS によって異なります。

**ステップ 5** イメージの事前ダウンロードの完了後にコントローラを自動的にリブートするように設定するには、[Auto Restart] チェック ボックスをオンにします。

また、[Advanced] > [Controller Tools] を選択し、[Restart Controller] を選択することで、アップグレード後にコントローラを手動でリブートできます。

**ステップ 6** [Apply] をクリックして、指定したパラメータを保存します。

これらのパラメータは、今後変更しない限り、保存されたままになります。次回のソフトウェア アップデート時に、これらのパラメータを再度入力する必要はありません。

**ステップ 7** [Update Now] をクリックし、確認ダイアログで [Ok] をクリックします。

ページトップのセクションに、ダウンロードのステータスが表示されます。このプロセスの実行中に、コントローラまたは AP の電源を手動で切ったり、リセットしたりしないでください。電源を切ったり、リセットしたりすると、ソフトウェア イメージが破損する場合があります。

ページの [Image Pre-Download Status] セクションに、ネットワーク内の AP にダウンロードされるプリイメージのステータスが表示されます。

進行中のソフトウェア アップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることで中止できます。

**ステップ 8** イメージの事前ダウンロードの完了後、ソフトウェア アップグレードを完了するにはコントローラを再起動（またはリブート）する必要があります。[Auto Restart] チェック ボックスをオンにしていない場合は、アップグレード後に [Advanced] > [Controller Tools] を選択し、[Restart Controller] をクリックすることで、コントローラを手動でリブートできます。

イメージの事前ダウンロード機能の詳細については、[アクセスポイントへのイメージのプレダウンロード](#)を参照してください。

進行中のソフトウェア アップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることで中止できます。

**ステップ 9** コントローラにログインし、[Software Update] ウィンドウでコントローラ ソフトウェアのバージョンを確認します。

## TFTP を使用したソフトウェア アップデート

### 始める前に

- Cisco Mobility Express ソフトウェア ファイルをホストするために、次のガイドラインに従って TFTP サーバを準備します。
  - TFTP サーバが 32 MB より大きいサイズのファイルに対して拡張 TFTP をサポートすることを確認します。このサイズのファイルをサポートする TFTP サーバには、tftpd32 や Cisco Prime Infrastructure 内の TFTP サーバがあります。
  - コントローラ ソフトウェアをダウンロードするときに 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と、TFTP failure while storing in flash というエラー メッセージが表示されます。
  - 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であるため、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。
- Cisco.com および TFTP サーバにアクセスできるコンピュータを利用可能にしておきます。



(注) TFTP サーバには、マスター AP 上にあるものと同じ Cisco Mobility Express ソフトウェア バンドルか、Cisco.com 上の最新のソフトウェア バンドルのいずれかが常に存在していることを確認します。

**ステップ 1** 以下のステップに従って、コントローラ ソフトウェアのイメージを入手します。

- a) コンピュータを使用して、[Cisco Download Software] ページにアクセスします。
- b) 特定の AP モデルに移動し、[Mobility Express Software] をクリックすると、現在使用可能なソフトウェアのリストが最新リリースから順に表示されます。
- c) 特定のソフトウェア リリース番号を選択します。
- d) ファイル名をクリックします。
- e) ZIP ファイルに対応する [Download] をクリックします。
- f) 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。
- g) ファイルをコンピュータのハード ドライブに保存します。

- h) コンピュータのハード ドライブからファイルをコピーし、解凍してコンテンツ全体を TFTP サーバ上のデフォルト ディレクトリに抽出します。

**ステップ 2** Cisco Mobility Express コントローラの Web インターフェイスから [Management] > [Software Update] を選択します。

[Software Update] ウィンドウが表示され、現在のソフトウェアのバージョン番号が表示されます。

**ステップ 3** [Transfer Mode] ドロップダウンリストから [TFTP] を選択します。

**ステップ 4** [IP Address (Ipv4)] 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、ソフトウェア ファイルの TFTP サーバディレクトリ パスを入力します。

**ステップ 6** イメージの事前ダウンロードの完了後にコントローラを自動的にリブートするように設定するには、[Auto Restart] チェック ボックスをオンにします。

また、[Advanced] > [Controller Tools] を選択し、[Restart Controller] を選択することで、アップグレード後にコントローラを手動でリブートできます。

**ステップ 7** [Apply] をクリックして、指定したパラメータを保存します。

これらのパラメータは、今後変更しない限り、保存されたままになります。次のソフトウェア アップデート時に、これらのパラメータを再度入力する必要はありません。

**ステップ 8** 更新を即時に実行するか、後から実行するようにスケジュールします。

- 更新をただちに実行するには、[Update Now] をクリックし、確認ダイアログで [OK] をクリックします。
- 更新を後から実行するには、[Set Update Time] フィールドに現在の日付から 5 日間以内の日時を指定してから、[Schedule Update] をクリックします。

ページ トップのセクションに、ダウンロードのステータスが表示されます。このプロセスの実行中に、コントローラまたは AP の電源を手動で切ったり、リセットしたりしないでください。電源を切ったり、リセットしたりすると、ソフトウェア イメージが破損する場合があります。

ページの [Image Pre-Download Status] セクションに、ネットワーク内の AP にダウンロードされるプリイメージのステータスが表示されます。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることで中止できます。

**ステップ 9** イメージの事前ダウンロードの完了後、ソフトウェア アップグレードを完了するにはコントローラを再起動（またはリブート）する必要があります。[Auto Restart] チェック ボックスをオンにしていない場合は、アップグレード後に [Advanced] > [Controller Tools] を選択し、[Restart Controller] をクリックすることで、コントローラを手動でリブートできます。

イメージの事前ダウンロード機能の詳細については、[アクセス ポイントへのイメージのプレダウンロード](#)を参照してください。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることで中止できます。

**ステップ 10** コントローラにログインし、[Software Update] ウィンドウでコントローラ ソフトウェアのバージョンを確認します。

## SFTP を使用したソフトウェア アップデート

SFTP 転送モードによるソフトウェア アップデートは、Cisco Mobility Express 導入でサポートされているすべてのアクセスポイントに有効です。このアップグレード方法を使用するには、マスターアクセスポイントと通信できる SFTP サーバが必要です。この更新方法はコントローラ WebUI および CLI からサポートされます。

**ステップ 1** 以下のステップに従って、コントローラ ソフトウェアのイメージを入手します。

- a) コンピュータを使用して、[Cisco Download Software] ページにアクセスします。
- b) 特定の AP モデルに移動し、[Mobility Express Software] をクリックすると、現在使用可能なソフトウェアのリストが最新リリースから順に表示されます。
- c) 特定のソフトウェア リリース番号を選択します。
- d) ファイル名をクリックします。
- e) ZIP ファイルに対応する [Download] をクリックします。
- f) 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。
- g) ファイルをコンピュータのハード ドライブに保存します。
- h) コンピュータのハード ドライブからファイルをコピーし、解凍してコンテンツ全体を SFTP サーバ上のデフォルト ディレクトリに抽出します。

**ステップ 2** Cisco Mobility Express コントローラの Web インターフェイスから [Management] > [Software Update] を選択します。

[Software Update] ウィンドウが表示され、現在のソフトウェアのバージョン番号が表示されます。

**ステップ 3** [Transfer Mode] ドロップダウンリストから [SFTP] を選択します。

**ステップ 4** [IP Address (Ipv4)/Name] フィールドに、SFTP サーバの IP アドレスまたはドメイン名を入力します。

**ステップ 5** [ポート (Port)] フィールドにポート番号を入力します。デフォルトは 22 です。

**ステップ 6** [File Path] フィールドに、ソフトウェア ファイルの SFTP サーバ ディレクトリ パスを入力します。

**ステップ 7** SFTP サーバにログインする [ユーザ名 (Username)] と [パスワード (Password)] を入力します。

**ステップ 8** 更新を即時に実行するか、後から実行するようにスケジュールします。

- 更新をただちに実行するには、[更新 (Update)] をクリックし、確認ダイアログで [OK] をクリックします。
- 更新を後から実行するには、[更新時間の設定 (Set Update Time)] フィールドで現在の日付から 5 日間以内の日時を指定してから、[更新をスケジュール (Schedule Update)] をクリックします。

**ステップ 9** イメージの事前ダウンロードの完了後にコントローラを自動的にリブートするように設定するには、[Auto Restart] チェック ボックスをオンにします。

また、[Advanced]>[Controller Tools] を選択し、[Restart Controller] を選択することで、アップグレード後にコントローラを手動でリブートできます。

**ステップ 10** [Apply] をクリックして、指定したパラメータを保存します。

これらのパラメータは、今後変更しない限り、保存されたままになります。次のソフトウェアアップデート時に、これらのパラメータを再度入力する必要はありません。

**ステップ 11** イメージの事前ダウンロードの完了後、ソフトウェア アップグレードを完了するにはコントローラを再起動（またはリブート）する必要があります。[Auto Restart] チェック ボックスをオンにしていない場合は、アップグレード後に [Advanced]>[Controller Tools] を選択し、[Restart Controller] をクリックすることで、コントローラを手動でリブートできます。

イメージの事前ダウンロード機能の詳細については、[アクセス ポイントへのイメージのプレダウンロード](#)を参照してください。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることで中止できます。

**ステップ 12** コントローラにログインし、[Software Update] ウィンドウでコントローラ ソフトウェアのバージョンを確認します。

---

## Cisco.com からのソフトウェア直接アップデート

### 始める前に

- マスター AP のシリアル番号は、サービス契約に記載されているものである必要があります。これは、Cisco.com サイトからは実行できません。シスコカスタマーサービスに連絡し、シリアル番号をサービス契約に追加する必要があります。

ただし、返品保証（Return to Manufacturer Authorization : RMA）を行っている場合、シリアル番号はデバイスを交換するチームによってサービス契約に追加されます。また、Cisco Services Contract Center データベースへのアクセスを持つ特定のシスコパートナーも、サービス契約にシリアル番号を追加できます。

- 有効な Cisco.com ユーザ クレデンシャルが必要です。
- Cisco Mobility Express コントローラが Cisco.com に到達できる必要があります。

---

**ステップ 1** [Software Update Mode] ドロップダウンリストから [Cisco.com] を選択します。

**ステップ 2** Cisco.com アカунトの Cisco.com ユーザ名とパスワードを入力します。

以前使用していた既存のクレデンシャルをクリアするには、新しいクレデンシャルを入力する前に [Clear Credentials] をクリックします。

**ステップ3** ソフトウェア アップデートを自動的に確認するようにコントローラを設定するには、[Automatically Check for Updates] ドロップダウンリストの [Enabled] を選択します。この設定はデフォルトでイネーブルになっています。

ソフトウェアの確認が実行され、新しい最新のソフトウェアアップデートまたは推奨ソフトウェアアップデートが Cisco.com で入手できる場合は、次のようになります。

- GUI の右上隅にある [Software Update Alert] アイコンが緑色になります（それ以外の場合はグレー）。このアイコンをクリックすると [Software Update] ページが表示されます。
- [Software Update] ページの下部にある [Update] ボタンが有効になります

**ステップ4** [Apply] をクリックします。

これにより、ソフトウェア アップデート モード、Cisco.com のクレデンシャル、[Automatically Check For Updates] のフィールドで行ったエントリまたは変更が保存されます。

コントローラは30日ごとに自動確認を実行し、Cisco.comでのダウンロードに利用可能な最新のソフトウェアや推奨ソフトウェアバージョンをチェックします。この情報は、[Latest Software Release] フィールドと [Recommended Software Release] フィールドに表示されます。表示されたリリースのリリース ノートを表示するには、横にある [?] をクリックします。

[Last Software Check] フィールドには、ソフトウェアを最後に自動または手動で確認したときのタイムスタンプが表示されます。

Cisco.com のユーザ名かパスワードまたはその両方が有効でない場合、ソフトウェアの確認は失敗してソフトウェア アップデートを実行できなくなります。

**ステップ5** [Check Now] をクリックし、ソフトウェア確認を手動で実行します。

ソフトウェア確認は、[Check Now] をクリックすることでいつでも手動で実行できます。

**ステップ6** ソフトウェア アップデートを進めるには、[Update] をクリックします。

[Software Update] ウィザードが表示されます。このウィザードは、次の3つのタブでの作業を順次実行します。

- [Release] タブ：推奨ソフトウェア リリースか、または最新ソフトウェア リリースのどちらにアップデートするかを指定します。
- [Update] タブ：APをいつリセットするかを指定します。すぐに実行するか、後から実行するためにスケジュールを設定するかを選択できます。  
イメージの事前ダウンロードの完了後にコントローラを自動的にリブートするように設定するには、[Auto Restart] チェック ボックスをオンにします。
- [Confirm] タブ：選択を確認します。

ウィザードの指示に従います。[Confirm] をクリックするまでは、どのタブにもいつでも戻ることができます。[Confirm] をクリックすると、シスコ ソフトウェア使用許諾契約書 (EULA) が表示されます。

**ステップ7** EULA に同意して更新を開始するには、[Agree] をクリックします。EULA に同意しないと、更新が中止されてエラーが表示されます。

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることで中止できます。

### 次のタスク

更新のステータスおよび進捗状況は [Software Update] ページでモニタできます。更新が進むにつれて、次のデータが表示されます。

- ネットワーク内の AP の総数
- 次の AP の数
  - 現在更新中
  - 更新待機中
  - リブート中
  - 更新失敗

さらに、各 AP について、次のデータを使用して更新の進捗状況も表示されます。

- [AP Name]
- [State] : [Waiting to be updated] (更新待機中)、[Pre-downloading software] (ソフトウェアの事前ダウンロード中)、[Rebooting] (リブート中)、[Failed] (失敗)
- ダウンロード率の色分け
- 更新試行
- 最終更新エラー

進行中のソフトウェアアップデートは、コントローラがリブートを完了するまではいつでも [Abort] をクリックすることで中止できます。

## 設定管理

### 設定管理の拡張機能

リリース 8.10 では、次の設定管理の拡張機能を使用できるようになりました。

- コンフィギュレーションファイルのダウンロードのスケジューリング：リリース 8.10 では、コンフィギュレーションファイルのダウンロードをスケジュールできます。1回限りのダウンロードまたは定期的なダウンロードのスケジュールを設定できます。

リリース 8.10 より前では、コンフィギュレーションファイルの即時ダウンロードがサポートされていませんでした。

この拡張機能には、次のオプションがあります。

- **1回限りのダウンロード**：コンフィギュレーションファイルをダウンロードする絶対時間を設定できます。この設定は再起動後も保持されます。
- **定期的ダウンロード**：間隔（時間単位、週単位、月単位）を指定し、コンフィギュレーションファイルの定期的ダウンロードをスケジュールできます。
- **FQDNをサーバアドレスのオプションとして使用**：リリース8.10より前では、即時ダウンロード機能を使用して、IPアドレスのみをサーバアドレスとして設定できました。リリース8.10では、FQDNをサーバアドレスとして設定し、コンフィギュレーションファイルをダウンロードすることも可能です。
- **コンフィギュレーションファイルのダウンロード後にコントローラを再起動**：リリース8.10より前は、コンフィギュレーションファイルをダウンロードしてMEに展開した後、ユーザがMEを再起動して新しい設定を有効にする必要がありました。MEの起動が完了するのに長い時間を要するため、ネットワークのダウンタイムが増加します。リリース8.10では、完全なMEプラットフォームを再起動する代わりに、ME上で実行中のコントローラサービスのみが再起動されます。
- **エラー発生時に以前の設定にロールバック**：新しいコンフィギュレーションファイルのダウンロードや展開プロセスで何らかのエラーが発生した場合、システムが自動的に以前のコンフィギュレーションファイルにロールバックします。

## 注意事項および制約事項

- 1つのダウンロードポリシーのみを設定すると、ポリシーをさらに強化できます。
- 設定データタイプに限定してダウンロードをスケジュールできます。
- 手動で設定したシステム時刻は再起動後に経過しないため、ダウンロードポリシーを設定する際にNTPを有効にすることをお勧めします。

## 設定の更新（GUI）

- ステップ1** Cisco Mobility Express コントローラの Web インターフェイスから、**[Advanced]** > **[Controller Tools]** を選択します。
- ステップ2** **[Configuration Management]** タブをクリックします。
- ステップ3** **[Direction]** ドロップダウンリストから、設定ファイルの **[Upload]** または **[Download]** を選択します。
  - **アップロード (Upload)**：外部ソースからコントローラに設定を転送します。
  - **ダウンロード (Download)**：コントローラから外部ソースに設定を転送します。
- ステップ4** **[Transfer Mode]** ドロップダウンリストで、次のオプションから選択します。

- FTP
- HTTP
- SFTP
- TFTP

**ステップ 5** [IP Address(IPv4)/FQDN] ボックスに、サーバの完全修飾ドメイン名の IPv4 アドレスを入力します。

**ステップ 6** [Port Number] ボックスで、ポート番号を指定します。

**ステップ 7** [File Path] ボックスに、設定ファイルのパスを入力します。

(注) パスとファイル名には、\、:、\*、?の文字は使用できません。また、"、<、>、|は、パスとファイル名には使用できません。スラッシュ「/」は、パス区切り記号として使用します。

**ステップ 8** [File Name] ボックスに、設定ファイル名を入力します。

**ステップ 9** ユーザ名とパスワードを指定します。

**ステップ 10** コンフィギュレーションファイルのダウンロードをスケジュールするには、[Schedule Update] を有効に設定します。

**ステップ 11** コンフィギュレーションファイルのダウンロードのスケジューリングを有効にするには、[Active] を有効に設定します。

**ステップ 12** コンフィギュレーションファイルのダウンロード頻度を指定します。

**ステップ 13** コンフィギュレーションファイルをダウンロードする日時を指定します。

**ステップ 14** [Schedule Window] ボックスには、転送スケジュールの間隔を設定します。有効な範囲は 5 ~ 180 分です。

**ステップ 15** [Apply] をクリックします。

## 設定の更新 (CLI)

**ステップ 1** 次のコマンドを入力して、新しいダウンロードポリシーを作成するか、またはコンフィギュレーションファイルをダウンロードするために既存のポリシーを削除します。

```
transfer schedule {create | delete} policy-name
```

**ステップ 2** 次のコマンドを入力して、ダウンロードポリシーをアクティブ化または非アクティブ化します。

```
transfer schedule {start | stop} policy-name
```

**ステップ 3** 次のコマンドを入力して、特定のプロファイルに対して転送ダウンロード関連の各種パラメータを設定します。

```
transfer schedule parameter policy-name
```

次のパラメータオプションを使用できます。

パラメータ	説明
<b>datatype</b>	ファイルタイプを設定
<b>direction</b>	スケジュールポリシーの方向を設定
<b>filename</b>	サーバ上のファイル名を設定
<b>mode</b>	転送モードを設定
<b>password</b>	サーバのログインパスワードを設定
<b>path</b>	サーバ上のファイルパスを設定
<b>port</b>	デフォルトのサーバポートを変更
<b>serverIP</b>	サーバの IP アドレスまたは FQDN を設定
<b>tftpMaxRetries</b>	許可される TFTP パケットの最大再試行回数。有効な範囲は 1 ~ 254 です。
<b>tftpPktTimeout</b>	TFTP パケットのタイムアウト (秒単位)。有効な範囲は 1 ~ 254 です。
<b>username</b>	サーバのログインユーザ名を設定
<b>window</b>	転送スケジュールの間隔を設定
<b>frequency</b>	ダウンロードポリシーの頻度を設定。時間単位、日単位、週単位、月単位で設定できます。

**ステップ 4** 次のコマンドを入力して、スケジュール済みポリシーの概要 (ポリシー名、データタイプ、スケジュールステータスなど) を表示します。

**show transfer-schedule summary**

**ステップ 5** 次のコマンドを入力して、ダウンロードポリシーの詳細情報を表示します。

**show transfer-schedule detailed *policy-name***

