



## コントローラ CLI コマンド

- [Cisco Mobility Express CLI](#) (1 ページ)
- [CLI 初期設定ウィザードの使用](#) (1 ページ)
- [CLI での手順](#) (5 ページ)

### Cisco Mobility Express CLI

特定のCisco Mobility Express ソフトウェア リリースでサポートされている機能については、Cisco Mobility Express コントローラ ソフトウェアが 同じ Cisco Unified Wireless Network ソフトウェア リリース バージョン内の Cisco WLC によってサポートされているほとんどのコマンドをサポートしています。ただし、Cisco Mobility Express コントローラに特有のコマンドおよび手順や、異なる動作をするものがいくつかあります。これらの手順は、以降の各項で説明します。

Cisco Mobility Express コントローラ CLI でサポートされているコマンドの詳細なリストについては、<https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-reference-list.html> に示されている特定のリリースの『Cisco Mobility Express Command Reference』を参照してください。Cisco Mobility Express は、このドキュメントに記載されている AireOS コマンドのみをサポートしています。

WLC CLI 上で利用可能なコマンドについては、次の URL に記載されている Cisco Unified Wireless Network ソフトウェア リリース用の『Cisco Wireless Controller Command Reference』ガイドを参照してください。 <http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-command-reference-list.html>

### CLI 初期設定ウィザードの使用

#### 始める前に

- アクセス ポイントのコンソール ポートに接続して次の手順を実行します。
- 利用可能なオプションは、各設定パラメータの後の括弧内に示されます。デフォルト値は、すべて大文字で示されます。

- 入力した応答が正しくない場合は、「Invalid Response」などのエラーメッセージが表示され、ウィザードのプロンプトが再び表示されます。
- 前のコマンドラインに戻る必要があるときは、**ハイフン** キーを押してください。

**ステップ 1** 自動インストール プロセス (CLI 初期設定ウィザード) を終了するよう求められたら、30 秒待機します。CLI 初期設定ウィザードは 30 秒後に開始されます。

プロセスを終了するには、**yes** を入力します。

ウィザードが設定ファイルを TFTP サーバからダウンロードして、設定を自動的にコントローラにロードします。

**ステップ 2** このコントローラに割り当てる**管理者のユーザ名**および**パスワード**を入力します。それぞれ、24 文字までの ASCII 文字を入力できます。

パスワード ポリシーは次の通りです。

- パスワードには、次の中から少なくとも 3 つのクラスの文字を含める必要があります。
  - 小文字の英字
  - 大文字の英字
  - 数字
  - 特殊文字
- パスワードには同じ文字を連続して 4 回以上繰り返すことはできません。
- 新規のパスワードとして、関連するユーザ名と同じものやユーザ名を逆にしたものは使用できません。
- パスワードには、Cisco という語の大文字を小文字に変更したものや文字の順序を入れ替えたもの (cisco、ocsic など) を使用できません。また、i の代わりに 1、I、! を、o の代わりに 0 を、s の代わりに \$ を使用することはできません。

**ステップ 3** **システム名**を入力します。これは、コントローラに割り当てる名前です。ASCII 文字を最大 31 文字入力できます。

**ステップ 4** Mobility Express ネットワークが置かれる国のコードを入力します。

(注) 使用可能な Country Code の一覧を表示するには、**help** と入力します。

**ステップ 5** 電源投入時にコントローラの時間設定が外部ネットワーク タイムプロトコル (NTP) サーバから受信されるようにするには、「YES」と入力して NTP サーバを設定します。それ以外の場合は、**no** と入力します。

**YES** を入力した場合は、NTP サーバの IP アドレスを入力します。

**no** を入力した場合は、次に従って入力し、手動で日時を設定します。

- 日付を MM/DD/YY の形式で入力します。
- 時刻を HH:MM:SS の形式で入力します。

**ステップ 6** ゾーンの場所のインデックスを入力してタイムゾーンを設定します。 **help** を入力するとインデックス別のタイムゾーンのリストが表示されます。

**ステップ 7** 管理インターフェイスの IP アドレスを入力します。

(注) 管理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。

**ステップ 8** 管理インターフェイスの IP アドレスとサブネット マスクを入力します。

**ステップ 9** デフォルト ゲートウェイ ルータの IP アドレスを入力します。

**ステップ 10** 管理 DHCP スコープを有効にし、設定するには、「**yes**」と入力します。それ以外の場合は、「**No**」と入力します。

「**YES**」と入力した場合は、次を入力する必要があります。

1. DHCP Network IP address (DHCP ネットワーク IP アドレス)
2. DHCP Netmask (DHCP ネットマスク)
3. Router IP Address (ルータ IP アドレス)
4. IP アドレス範囲の [Start DHCP IP address] (開始 DHCP IP アドレス) と [Stop DHCP IP address] (終了 DHCP IP アドレス)
5. Domain Name (ドメイン名)
6. OpenDNS かユーザ DNS かの指定

**ステップ 11** [Employee Network] を有効にするには、**YES** を入力します。それ以外の場合は、**no** と入力します。

**YES** を入力した場合は、次のように入力します。

1. 社員ネットワーク名 (SSID)
2. 社員 VLAN ID (0 = タグなし)
3. 社員ネットワーク セキュリティ。 **PSK** または **enterprise** を入力できます。
4. 社員ネットワーク セキュリティを **enterprise** と入力した場合は、次を指定します。
  - RADIUS サーバのアドレス。
  - RADIUS サーバのポート。
  - RADIUS サーバのシークレット (パスワード)。
5. 社員ネットワーク セキュリティを **PSK** と入力した場合は、次を指定します。
  - PSK パス フレーズ (8~38 文字) を入力します。
  - PSK パス フレーズ (8~38 文字) を再入力します。

**ステップ 12** 従業員 DHCP スコープを有効にし、設定するには「**yes**」と入力します。それ以外の場合は、「**No**」と入力します。

「**YES**」と入力した場合は、次を入力する必要があります。

1. DHCP Network IP address (DHCP ネットワーク IP アドレス)
2. DHCP Netmask (DHCP ネットマスク)
3. Router IP Address (ルータ IP アドレス)
4. IP アドレス範囲の [Start DHCP IP address] (開始 DHCP IP アドレス) と [Stop DHCP IP address] (終了 DHCP IP アドレス)
5. Domain Name (ドメイン名)
6. OpenDNS かユーザ DNS かの指定

**ステップ 13** [Guest Network] を有効にするには、**YES** を入力します。それ以外の場合は、**no** と入力します。

**YES** を入力した場合は、次のように入力します。

1. ゲスト ネットワーク名 (SSID)。
2. ゲスト VLAN ID (0 = タグなし)。
3. ゲスト ネットワーク セキュリティ。 **WEB\_CONSENT** または **psk** を入力できます。
4. ゲスト ネットワーク セキュリティを **PSK** と入力した場合は、次を指定します。
  - ゲスト パス フレーズ (8 ~ 38 文字) を入力します。
  - ゲスト パス フレーズ (8 ~ 38 文字) を再入力します。

**ステップ 14** RF パラメータの最適化を有効にするには、**YES** を入力します。それ以外の場合は、**no** と入力します。

**YES** を入力した場合は、次のように入力します。

1. クライアント密度。必要に合わせて **TYPICAL**、**Low**、または **High** を入力できます。
2. 音声を含むトラフィック。必要に合わせて **NO** または **yes** を入力できます。

**ステップ 15** 設定が正しいかどうかをたずねるプロンプトが表示されたら、**yes** または **NO** と入力します。

**yes** と入力すると、コントローラは設定を保存してリポートし、ログオンプロンプトが表示されます。

---

## CLI での手順

### SNMPv3 ユーザのデフォルト値の変更

SNMPv3 ユーザのユーザ名、認証パスワード、およびプライバシーパスワードに対するコントローラのデフォルト値は、「default」が使用されています。これらの標準値を使用すると、セキュリティ上のリスクが発生します。したがって、これらの値を変更することを強く推奨します。

#### 始める前に

SNMPv3 は時間に依存しています。コントローラの時間および時間帯を正確に設定してください。

**ステップ 1** 次のコマンドを入力して、このコントローラに対する SNMPv3 ユーザの最新のリストを表示します。

```
show snmpv3user
```

**ステップ 2** [SNMPv3 User Name] カラムに「default」と表示されている場合は、次のコマンドを入力してこのユーザを削除します。

```
config snmp v3user delete username
```

*username* パラメータが SNMPv3 ユーザ名です（この場合は「default」）。

**ステップ 3** 次のコマンドを入力して、新しい SNMPv3 ユーザを作成します。

```
config snmp v3user create username {ro | rw} {none | hmacmd5 | hmacsha} {none | des | aescfb128} auth_key encrypt_key
```

値は次のとおりです。

- *username* は、SNMPv3 ユーザ名です。
- **ro** は読み取り専用モード、**rw** は読み取り/書き込みモードです。
- **none**、**hmacmd5**、および **hmacsha** は認証プロトコルのオプションです。
- **none**、**des**、および **aescfb128** はプライバシープロトコルのオプションです。
- *auth\_key* は、認証用の共有秘密キーです。
- *encrypt\_key* は、暗号化用の共有秘密キーです。

*username*、*auth\_key*、および *encrypt\_key* の各パラメータに「default」と入力しないでください。

**ステップ 4** **save config** コマンドを入力します。

ステップ 5 追加した SNMPv3 ユーザを有効にするために、**reset system** コマンドを入力して、コントローラを再起動します。

---

## 802.11r 高速移行の設定

---

- ステップ 1 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft {enable | disable} wlan-id** コマンドを使用します。
- デフォルトで、高速移行は無効です。
- ステップ 2 分散システム上の 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft over-the-dsconfig wlan security ft over-the-ds {enableenable | disabledisable} wlan-id** コマンドを使用します。
- デフォルトで、分散システム上の高速移行は無効です。
- ステップ 3 事前共有キー (PSK) を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft-psk {enable | disable} wlan-id** コマンドを使用します。
- デフォルトで、PSK を使用した認証キー管理は無効です。
- ステップ 4 802.1X を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft-802.1X {enable | disable} wlan-id** コマンドを使用します。
- デフォルトで、802.1X を使用した認証キー管理は無効です。
- ステップ 5 802.11r Fast Transition の再アソシエーション タイムアウトを有効または無効にするには、**config wlan security ft reassociation-timeoutconfig wlan security ft reassociation-timeout timeout-in-seconds wlan-id** コマンドを使用します。
- 有効範囲は 1 ~ 100 秒です。再アソシエーション タイムアウトのデフォルト値は 20 秒です。
- ステップ 6 分散システム上の高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft over-the-ds {enable | disable} wlan-id** コマンドを使用します。
- デフォルトで、分散システム上の高速移行の認証キー管理は無効です。
- ステップ 7 クライアントの高速移行の設定を表示するには、**show client detailed client-mac** コマンドを使用します。
- ステップ 8 WLAN の Fast Transition 設定を表示するには、**show wlanshow wlan wlan-id** コマンドを使用します。
- ステップ 9 高速移行イベントのデバッグを有効または無効にするには、**debug ft events {enable | disable}** コマンドを使用します。
- ステップ 10 高速移行のキー生成のデバッグを有効または無効にするには、**debug ft keys {enable | disable}** コマンドを使用します。
-

## CDP タイマーの設定



- 
- (注) CDP 保留時間の設定は、マスター AP のコントローラ コンソールからは行えません。コントローラの保留時間の設定は無視されます。これは、Cisco Mobility Express のマスター AP 上のコントローラと内部 AP がスイッチ上の同じインターフェイスを共有しているためです。
-

