CHAPTER 2

Web ブラウザと CLI インターフェイスの使用方法

この章では、コントローラの設定に使用する Web ブラウザと CLI インターフェイスについて説明します。この章の内容は、次のとおりです。

Web ブラウザ インターフェイスの使用方法

Web ブラウザ インターフェイス（以降、GUI）は、すべてのコントローラに組み込まれています。最大 5 名のユーザが、コントローラ http または https（http + SSL）管理ページを同時に閲覧して、パラメータを設定し、コントローラとそのアソシエートされているアクセス ポイントの動作ステータスを監視することができます。

（注） Cisco UWN Solution のセキュリティを強化するために、HTTPS インターフェイスを有効にし、HTTP インターフェイスを無効にすることをお勧めします。

GUI を使用する際の注意事項

GUI を使用するときは、次の点に留意してください。

- GUI は、Windows XP SP1 以上または Windows 2000 SP4 以上が動作するコンピュータで使用してください。
- この GUI は、Microsoft Internet Explorer バージョン 6.0 SP1 以上と完全に互換性があります。

（注） Opera、Mozilla、および Netscape はサポートされていません。

（注） Web 認証を使用するには、Microsoft Internet Explorer バージョン 6.0 SP1 以上が必要です。

- サービス ポート インターフェイスまたは管理インターフェイスを使用して GUI にアクセスできますが、サービス ポート インターフェイスの使用をお勧めします。サービス ポート インターフェイスの設定方法については、第 3 章を参照してください。
- GUI のページ上部にある **Help** をクリックすると、オンライン ヘルプが表示されます。オンライン ヘルプを表示するには、ブラウザのポップアップ ブロックを無効にする必要があります。

GUI の表示

GUI を開くには、ブラウザのアドレス行にコントローラの IP アドレスを入力します。セキュリティで保護されている接続の場合は、**https://**<IP アドレス> と入力します。セキュリティの保護が十分でない接続の場合は、**http://**<IP アドレス> と入力します。HTTPS をセットアップする手順は、「GUI を使用した Web およびセキュア Web モードの有効化」の項（P. 2-2）を参照してください。

Web モードおよびセキュア Web モードの有効化

この項では、ディストリビューション システム ポートを Web ポート（HTTP を使用）またはセキュア Web ポート（HTTPS を使用）として有効にする手順について説明します。HTTPS を有効化すると、GUI との通信を保護できます。HTTPS では、SSL（Secure Socket Layer）プロトコルを使用することによって、HTTP ブラウザのセッションを保護します。HTTPS を有効にすると、コントローラは独自の Web アドミニストレーション SSL 証明書を生成して、自動的に GUI に割り当てます。また、外部で生成された証明書をダウンロードすることもできます。

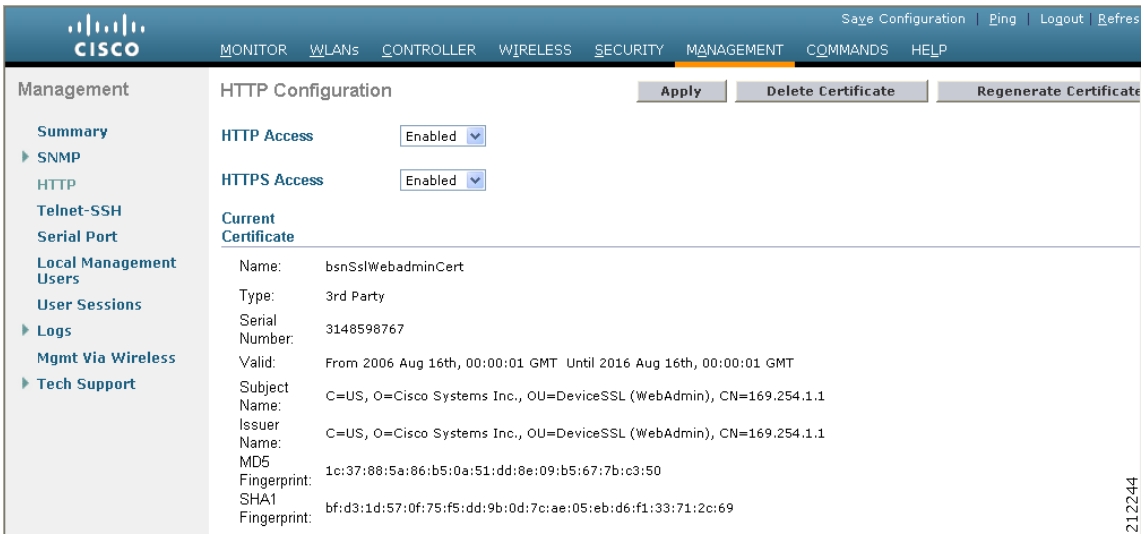
コントローラ GUI または CLI を使用して、Web およびセキュア Web モードを設定できます。

GUI を使用した Web およびセキュア Web モードの有効化

コントローラの GUI を使用して、Web モード、セキュア Web モード、またはその両方を有効にする手順は、次のとおりです。

ステップ 1　**Management** > **HTTP** の順にクリックして、HTTP Configuration ページを開きます（図 2-1 を参照）。

図 2-1　HTTP Configuration ページ



ステップ 2　Web モードを有効にすると、ユーザが「http://<IP アドレス >」を使用してコントローラ GUI にアクセスできるようになります。そのためには、HTTP Access ドロップダウン ボックスから **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。Web モードの接続は、セキュリティで保護されていません。

ステップ 3　セキュア Web モードを有効にすると、ユーザが「https://<IP アドレス >」を使用してコントローラ GUI にアクセスできるようになります。そのためには、HTTPS Access ドロップダウン ボックスから **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。セキュア Web モードの接続は、セキュリティで保護されています。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　ステップ 3 でセキュア Web モードを有効にすると、コントローラはローカル Web アドミニストレーション SSL 証明書を生成して自動的に GUI に適用します。現在の証明書の詳細は、HTTP Configuration ページの中央に表示されます（図 2-1 を参照）。

（注）　独自の SSL 証明書をコントローラにダウンロードする場合は、「外部で生成した SSL 証明書のロード」の項（P. 2-5）の手順を参照してください。

（注）　必要に応じて、**Delete Certificate** をクリックして現在の証明書を削除し、**Regenerate Certificate** をクリックして新しい証明書を生成するようコントローラで指定できます。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した Web およびセキュア Web モードの有効化

コントローラの CLI を使用して、Web モード、セキュア Web モード、またはその両方を有効にする手順は、次のとおりです。

ステップ 1　Web モードを有効または無効にするには、次のコマンドを入力します。

config network webmode {**enable** | **disable**}

このコマンドにより「http://<IP アドレス >」を使用してコントローラの GUI にアクセスできるようになります。デフォルト値は、Disabled です。Web モードの接続は、セキュリティで保護されていません。

ステップ 2　セキュア Web モードを有効または無効にするには、次のコマンドを入力します。

config network secureweb {**enable** | **disable**}

このコマンドにより「https://<IP アドレス >」を使用してコントローラの GUI にアクセスできるようになります。デフォルト値は、Enabled です。セキュア Web モードの接続は、セキュリティで保護されています。

ステップ 3　セキュア Web モードのセキュリティの強化を有効または無効にするには、次のコマンドを入力します。

config network secureweb cipher-option high {**enable** | **disable**}

このコマンドにより、「https://<IP アドレス >」を使用してコントローラの GUI にアクセスできます。ただし、128 ビット（またはそれ以上）の暗号をサポートするブラウザ以外からは、アクセスできません。デフォルト値は無効（disable）です。

ステップ 4　コントローラが証明書を生成したことを確認するには、次のコマンドを入力します。

show certificate summary

次のような情報が表示されます。

```
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:.................... off
```

（注）　独自の SSL 証明書をコントローラにダウンロードする場合は、「外部で生成した SSL 証明書のロード」の項（P. 2-5）の手順を参照してください。

ステップ 5　（オプション）新しい証明書を生成する場合は、次のコマンドを入力します。

config certificate generate webadmin

数秒後、コントローラでは、証明書が生成されたことが確認されます。

ステップ 6　リブート後も変更内容が維持されるように、SSL 証明書、キー、セキュア Web パスワードを NVRAM（不揮発性 RAM）に保存するには、次のコマンドを入力します。

save config

ステップ 7　コントローラ をリブートするには、次のコマンドを入力します。

reset system

外部で生成した SSL 証明書のロード

TFTP サーバを使用して、外部で生成された SSL 証明書をコントローラにダウンロードできます。TFTP を使用する際の注意事項は次のとおりです。

- サービス ポート経由で証明書をロードする場合、サービス ポートはルーティングできないため、TFTP サーバはコントローラ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。また、証明書を Distribution System（DS; ディストリビューション システム）のネットワーク ポートでロードすると、TFTP サーバを任意のサブネット上におくこともできます。
- 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。

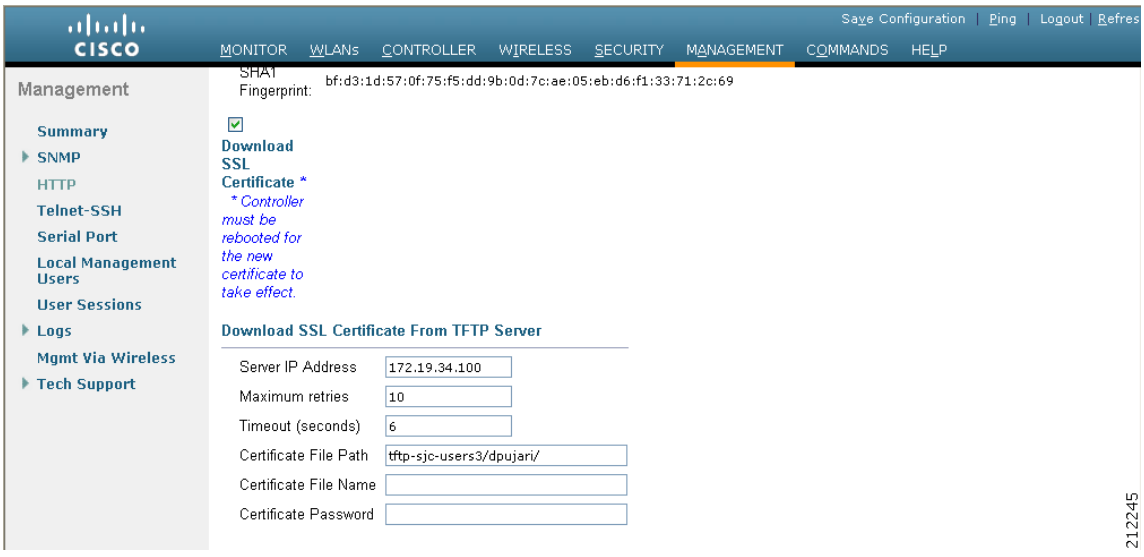
（注）　各 HTTPS 証明書には RSA キーが組み込まれています。キーの長さは、比較的安全性の低い 512 ビットから、非常に安全性の高い数千ビットまで対応しています。認証局から新しい証明書を取得する際、証明書に組み込まれた RSA キーの長さが 768 ビットより長いことを確認してください。

GUI を使用した SSL 証明書のロード

コントローラの GUI を使用して、外部で生成された SSL 証明書をロードする手順は、次のとおりです。

ステップ 1　HTTP Configuration ページで、**Download SSL Certificate** チェックボックスをオンにします（図 2-2 を参照）。

図 2-2　HTTP Configuration ページ



ステップ 2　Server 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 3　Maximum Retries フィールドに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 4　Timeout フィールドに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 5　Certificate 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 6　Certificate File Name フィールドに、証明書の名前を入力します（*webadmincert_name*.pem）。

ステップ 7　（オプション）Certificate Password フィールドに、パスワードを入力して証明書を暗号化します。

ステップ 8　**Apply** をクリックして、変更を適用します。

ステップ 9　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 10　コントローラをリブートして変更内容を有効化するには、**Commands** > **Reboot** > **Reboot** > **Save and Reboot** の順にクリックします。

CLI を使用した SSL 証明書のロード

コントローラの CLI を使用して、外部で生成された SSL 証明書をロードする手順は、次のとおりです。

ステップ 1　パスワードを使用して、.PEM エンコード ファイルで HTTPS 証明書を暗号化します。PEM エンコード ファイルは、Web アドミニストレーション証明書ファイル（*webadmincert_name*.pem）と呼ばれます。

ステップ 2　*webadmincert_name*.pem ファイルを TFTP サーバ上のデフォルト ディレクトリに移動します。

ステップ 3　現在のダウンロードの設定を表示するには、次のコマンドを入力してプロンプトに **n** と応答します。

transfer download start

次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Admin Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename.............................
Are you sure you want to start? (y/n) n
Transfer Canceled
```

ステップ 4　次のコマンドを使用して、ダウンロード設定を変更します。

transfer download mode tftp

transfer download datatype webauthcert

transfer download serverip *TFTP_server IP_address*

transfer download path *absolute_TFTP_server_path_to_the_update_file*

transfer download filename *webadmincert_name.pem*

ステップ 5　オペレーティング システムが Web アドミニストレーション SSL キーおよび証明書の暗号化を解除できるように、.PEM ファイルのパスワードを設定するには、次のコマンドを入力します。

transfer download certpassword *private_key_password*

ステップ 6　現在のダウンロードの設定を確認して証明書とキーのダウンロードを開始するには、次のコマンドを入力して、プロンプトに **y** と応答します。

transfer download start

次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ directory path
TFTP Filename............................ webadmincert_name
Are you sure you want to start? (y/n) y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

ステップ 7　リブート後も変更内容が維持されるように、SSL 証明書、キー、セキュア Web パスワードを NVRAM に保存するには、次のコマンドを入力します。

save config

ステップ 8　コントローラをリブートするには、次のコマンドを入力します。

reset system

CLI の使用方法

Cisco UWN Solution のコマンドライン インターフェイス（CLI）は、すべてのコントローラに組み込まれています。CLI では、VT-100 エミュレータを使用して、個々のコントローラおよび各コントローラにアソシエートされた Lightweight アクセス ポイントをローカルまたはリモートで設定、監視、制御することができます。CLI は簡単なテキスト ベースのツリー構造のインターフェイスで、Telnet 対応ターミナル エミュレータを使用して最大 5 名のユーザがコントローラにアクセスできます。

（注）　特定のコマンドの情報は、『Cisco Wireless LAN Controller Command Reference』を参照してください。

CLI へのログイン

CLI には、次の 2 つのいずれかの方法でアクセスします。

- コントローラ コンソール ポートへの ASCII シリアル直接接続
- 事前設定されたサービス ポートやディストリビューション システム ポートを使用したイーサネット上のリモート コンソール セッション

CLI にログインする前に、使用する接続の種類に基づいて接続および環境変数を設定しておく必要があります。

ローカル シリアル接続の使用方法

シリアル ポートに接続するには以下が必要です。

- DB-9 シリアル ポートを備えており、ターミナル エミュレーション プログラムを実行しているコンピュータ
- DB-9 オス対メスのヌルモデム シリアル ケーブル

シリアル ポートで CLI にログインする手順は、次のとおりです。

ステップ 1　DB-9 ヌルモデム シリアル ケーブルを使用して、コンピュータをコントローラに接続します。

ステップ 2　以下の設定を使用して、ターミナル エミュレータ セッションを開きます。

- 9600 ボー
- データ ビット 8
- ストップ ビット 1
- パリティなし
- ハードウェア フロー制御なし

ステップ 3　プロンプトで CLI にログインします。デフォルトのユーザ名は *admin*、デフォルトのパスワードは *admin* です。

（注）　コントローラのシリアル ポートは、9600 ボー レートおよび短いタイムアウト用に設定されています。これらの値のいずれかを変更するには、**config serial baudrate** *baudrate* コマンドおよび **config serial timeout** *timeout* コマンドを使用します。**config serial timeout 0** と入力すると、シリアル セッションはタイムアウトしなくなります。

リモート イーサネット接続の使用方法

リモートでコントローラに接続するには、以下が必要です。

- イーサネット ネットワーク上でコントローラにアクセスできるコンピュータ
- コントローラの IP アドレス
- Telnet セッション用のターミナル エミュレーション プログラムまたは DOS シェル

（注）　デフォルトでは、コントローラは Telnet セッションをブロックします。Telnet セッションを有効にするには、シリアル ポートへのローカル接続を使用する必要があります。

リモート イーサネット接続で CLI にログインする手順は、次のとおりです。

ステップ 1　ターミナル エミュレータまたは DOS シェル インターフェイスが、次のパラメータを使用して設定されていることを確認します。

- イーサネット アドレス
- ポート 23

ステップ 2　コントローラの IP アドレスを使用して Telnet を CLI に接続します。

ステップ 3　プロンプトで CLI にログインします。デフォルトのユーザ名は *admin*、デフォルトのパスワードは *admin* です。

CLI からのログアウト

CLI での作業が終わったら、ルート レベルに移動して、**logout** と入力します。揮発性 Random-Access Memory（RAM; ランダムアクセス メモリ）へ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。

CLI のナビゲーション

CLI のナビゲーションは、5 つのレベルに分かれています。

ルート レベル

レベル 2

レベル 3

レベル 4

レベル 5

CLI にログインしたときは、ルート レベルです。ルート レベルでは、正しいコマンド レベルに移動することなくすべてのコマンドを入力できます。表 2-1 は、CLI のナビゲーションを使用し、共通タスクを実行するためのコマンドの一覧です。

表 2-1　CLI のナビゲーションと共通タスクのコマンド

コマンド	操作
help	ルート レベルの場合、システム全体のナビゲーション コマンドが表示されます。
?	現在のレベルで使用できるコマンドが表示されます。
< コマンド > **?**	指定したコマンドのパラメータが表示されます。
exit	1 つ下のレベルに移動します。
Ctrl+Z	ルート レベルに戻ります。
save config	ルート レベルの場合、使用中のアクティブな RAM への変更を、リブート後も維持されるように不揮発性 RAM（NVRAM）に保存します。
reset system	ルート レベルの場合、ログアウトせずにコントローラをリセットします。

Web ブラウザと CLI インターフェイスの無線接続の有効化

無線クライアントを使用してコントローラを監視および設定できます。この機能は、コントローラとの間のアップロードおよびダウンロード以外のすべての管理タスクでサポートされています。

無線クライアント デバイスから GUI や CLI を開く前に、接続が許可されるようにコントローラを設定する必要があります。GUI や CLI への無線接続を有効にする手順は、次のとおりです。

ステップ 1　CLI にログインします。

ステップ 2　**config network mgmt-via-wireless enable** と入力します。

ステップ 3　無線クライアントを使用して、コントローラに接続されている Lightweight アクセス ポイントにアソシエートします。

ステップ 4　無線クライアントで、コントローラの Telnet セッションを開くか、コントローラの GUI を参照します。

ヒント　コントローラの GUI を使用して無線接続を有効にするには、**Management** > **Mgmt Via Wireless** ページをクリックして、**Enable Controller Management to be accessible from Wireless Clients** チェックボックスをオンにします。