Using the Web-Browser and CLI Interfaces

This chapter describes the web-browser and CLI interfaces that you use to configure the controllers. It contains these sections:

Using the Web-Browser Interface

The web-browser interface (hereafter called the GUI) is built into each controller. It allows up to five users to simultaneously browse into the controller http or https (http + SSL) management pages to configure parameters and monitor operational status for the controller and its associated access points.

Note Cisco recommends that you enable the https: and disable the http: interfaces to ensure more robust security for your Cisco UWN Solution.

Guidelines for Using the GUI

Keep these guidelines in mind when using the GUI:

- The GUI must be used on a PC running Windows XP SP1 or higher or Windows 2000 SP4 or higher.
- The GUI is fully compatible with Microsoft Internet Explorer version 6.0 SP1 or higher.

  Note Opera, Mozilla, and Netscape are not supported.

  Note Microsoft Internet Explorer version 6.0 SP1 or higher is required for using Web Authentication.

- You can use either the service port interface or the management interface to open the GUI. Cisco recommends that you use the service-port interface. Refer to Chapter 3, "Using the CLI to Configure the Service-Port Interface" for instructions on configuring the service port interface.
- You might need to disable your browser's pop-up blocker to view the online help.
- Before accessing the controller using the web browser interface verify the following items:
  - The IP address and network mask are configured correctly on the Management interface
  - The native vlan is configured correctly on the switch that connects to the WLC
  - The management interface and the AP management interface VLANs are configured correctly or the VLANS should be left at default settings, which is an untagged VLAN (VLAN 0 on the WLC)
- By default only https access is enabled. To enable http access, enter the following command from the controller CLI interface:

  config network webmode enable

Opening the GUI

To open the GUI, enter the controller IP address in the browser's address line. For an unsecure connection enter **http://***ip-address*. For a secure connection, enter **https://***ip-address*. See the "Configuring the GUI for HTTPS" section on page 2-3 for instructions on setting up HTTPS.

Enabling Web and Secure Web Modes

Use these commands to enable or disable the distribution system port as a web port or as a secure web port:

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

Web and secure web modes are enabled by default.

Configuring the GUI for HTTPS

Step 1 Enter **show certificate summary** to verify that the controller has generated a certificate:

```
>show certificate summary
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:.................... off
```

Step 2 (Optional) If you need to generate a new certificate, enter this command:

```
>config certificate generate webadmin
```

After a few seconds the controller verifies that the certificate is generated:

```
Web Administration certificate has been generated
```

Step 3 Enter this command to enable HTTPS:

```
>config network secureweb enable
```

Step 4 Save the SSL certificate, key, and secure web password to NVRAM (non-volatile RAM) so your changes are retained across reboots:

```
>save config
Are you sure you want to save? (y/n) y
Configuration Saved!
```

Step 5 Reboot the controller:

```
>reset system
Are you sure you would like to reset the system? (y/n) y
System will now restart!
```

The controller reboots.

You use a TFTP server to load the certificate. Follow these guidelines for using TFTP:

- If you load the certificate through the service port, the TFTP server must be on the same subnet as the controller because the service port is not routable. However, if you load the certificate through the distribution system (DS) network port, the TFTP server can be on any subnet.
- A third-party TFTP server cannot run on the same computer as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.

Note Every HTTPS certificate contains an embedded RSA Key. The length of the RSA key can vary from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you obtain a new certificate from a Certificate Authority, make sure the RSA key embedded in the certificate is at least 768 bits long.

Follow these steps to load an externally generated HTTPS certificate:

Step 1 Use a password to encrypt the HTTPS certificate in a .PEM-encoded file. The PEM-encoded file is called a Web Administration Certificate file (*webadmincert_name*.pem).

Step 2 Move the *webadmincert_name*.pem file to the default directory on your TFTP server.

Step 3 In the CLI, enter **transfer download start** and answer **n** to the prompt to view the current download settings:

```
>transfer download start
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
```

Step 4 Use these commands to change the download settings:

```
>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
```

Step 5 Enter the password for the .PEM file so the operating system can decrypt the Web Administration SSL key and certificate:

```
>transfer download certpassword private_key_password
>Setting password to private_key_password
```

Step 6 Enter **transfer download start** to view the updated settings, and answer **y** to the prompt to confirm the current download settings and start the certificate and key download:

```
>transfer download start
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.
```

Step 7 Enter this command to enable HTTPS:

```
>config network secureweb enable
```

Step 8 Save the SSL certificate, key, and secure web password to NVRAM (non-volatile RAM) so your changes are retained across reboots:

```
>save config
Are you sure you want to save? (y/n) y
Configuration Saved!
```

Step 9 Reboot the controller:

```
>reset system
Are you sure you would like to reset the system? (y/n) y
System will now restart!
```

The controller reboots.

Disabling the GUI

To prevent all use of the GUI, select the **Disable Web-Based Management** check box on the Services: HTTP-Web Server page and click **Apply**.

To re-enable the GUI, enter this command on theCLI:

```
>ip http server
```

Using Online Help

Click the help icon at the top of any page in the GUI to display online help. You might have to disable the browser pop-up blocker to view online help.

Using the CLI

The Cisco UWN Solution command line interface (CLI) is built into each controller. The CLI allows operators to use a VT-100 emulator to locally or remotely configure, monitor and control individual controllers, and to access extensive debugging capabilities. Because the CLI works with one controller at a time, the command line interface is especially useful when you wish to configure or monitor a single controller.

The controller and its associated lightweight access points can be configured and monitored using the command line interface (CLI), which consists of a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulators to simultaneously configure and monitor all aspects of the controller and associated lightweight access points.

The CLI allows you to use a VT-100 emulator to locally or remotely configure, monitor, and control a WLAN controller and its associated lightweight access points. The CLI is a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulators to access the controller.

Note Refer to the C*isco Wireless LAN Controller Command Reference* for information on specific commands.

Logging into the CLI

You access the CLI using either of two methods:

- A direct ASCII serial connection to the controller console port
- A remote console session over Ethernet through the pre-configured Service Port or through Distribution System Ports

Before you log into the CLI, configure your connectivity and environment variables based on the type of connection you use.

Using a Local Serial Connection

You need these items to connect to the serial port:

- A computer that has a DB-9 serial port and is running a terminal emulation program
- A DB-9 male-to-female null-modem serial cable

Follow these steps to log into the CLI through the serial port.

Step 1 Connect your computer to the controller using the DB-9 null-modem serial cable.

Step 2 Open a terminal emulator session using these settings:

- 9600 baud
- 8 data bits
- 1 stop bit
- no parity
- no hardware flow control

Step 3 At the prompt, log into the CLI. The default username is *admin*, and the default password is *admin*.

Note The controller serial port is set for a 9600 baud rate and a short timeout. If you would like to change either of these values, enter **config serial baudrate** *baudrate* and **config serial timeout** *timeout* to make your changes. If you enter **config serial timeout 0**, serial sessions never time out.

Using a Remote Ethernet Connection

You need these items to connect to a controller remotely:

- A computer with access to the controller over the Ethernet network
- The IP address of the controller
- A terminal emulation program or a DOS shell for the Telnet session

Note By default, controllers block Telnet sessions. You must use a local connection to the serial port to enable Telnet sessions.

Follow these steps to log into the CLI through the serial port:

Step 1 Verify that your terminal emulator or DOS shell interface is configured with these parameters:

- Ethernet address
- Port 23

Step 2 Use the controller IP address to Telnet to the CLI.

Step 3 At the prompt, log into the CLI. The default username is *admin* and the default password is *admin*.

Logging Out of the CLI

When you finish using the CLI, navigate to the root level and enter **logout**. The system prompts you to save any changes you made to the volatile RAM.

Navigating the CLI

The is organized around five levels:

Root Level

Level 2

Level 3

Level 4

Level 5

When you log into the CLI, you are at the root level. From the root level, you can enter any full command without first navigating to the correct command level. Table 2-1 lists commands you use to navigate the CLI and to perform common tasks.

Table 2-1 Commands for CLI Navigation and Common Tasks

Command	Action
help	At the root level, view system-wide navigation commands
?	View commands available at the current level
command **?**	View parameters for a specific command
exit	Move down one level
Ctrl-Z	Return from any level to the root level
save config	At the root level, save configuration changes from active working RAM to non-volatile RAM (NVRAM) so they are retained after reboot
reset system	At the root level, reset the controller without logging out

Enabling Wireless Connections to the Web-Browser and CLI Interfaces

You can monitor and configure controllers using a wireless client. This feature is supported for all management tasks except uploads from and downloads to the controller.

Before you can open the GUI or the CLI from a wireless client device you must configure the controller to allow the connection. Follow these steps to enable wireless connections to the GUI or CLI:

Step 1 Log into the CLI.

Step 2 Enter **config network mgmt-via-wireless enable**

Step 3 Use a wireless client to associate to a lightweight access point connected to the controller.

Step 4 On the wireless client, open a Telnet session to the controller, or browse to the controller GUI.

Tip To use the controller GUI to enable wireless connections, browse to the Management Via Wireless page and select the **Enable Controller Management to be accessible from Wireless Clients** check box.