C H A P T E R **2**

Using the Web-Browser and CLI Interfaces

This chapter describes the web-browser and CLI interfaces that you use to configure the controller. 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 interface and disable the HTTP interface 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 later) or Windows 2000 SP4 (or later).

- The GUI is fully compatible with Microsoft Internet Explorer version 6.0 SP1 (or later) or Mozilla Firefox 2.0.0.11 (or later).

  > **Note**   Opera and Netscape are not supported.

  > **Note**   Internet Explorer 6.0 SP1 (or later) and Mozilla Firefox 2.0.0.11 (or later) are the only browsers supported for accessing the controller GUI and for using web authentication.

- You can use either the service port interface or the management interface to access the GUI. Cisco recommends that you use the service-port interface. Refer to Chapter 3 for instructions on configuring the service port interface.

- Click **Help** at the top of any page in the GUI to display online help. You might need to disable your browser's pop-up blocker to view the online help.

Opening the GUI

To open the GUI, enter the controller IP address in the browser's address line. For a secure connection, enter **https://*ip-address***. For a less secure connection, enter **http://*ip-address***. See the "Using the GUI to Enable Web and Secure Web Modes" section on page 2-2 for instructions on setting up HTTPS.

Enabling Web and Secure Web Modes

This section provides instructions for enabling the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can configure web and secure web mode using the controller GUI or CLI.

Using the GUI to Enable Web and Secure Web Modes

Follow these steps to enable web mode, secure web mode, or both using the controller GUI.

Step 1   Click **Management** > **HTTP** to open the HTTP Configuration page (see).

Figure 2-1   HTTP Configuration Page

Step 2   To enable web mode, which allows users to access the controller GUI using "http://*ip-address*," choose **Enabled** from the HTTP Access drop-down box. Otherwise, choose **Disabled**. The default value is Disabled. Web mode is not a secure connection.

Step 3   To enable secure web mode, which allows users to access the controller GUI using "https://*ip-address*," choose **Enabled** from the HTTPS Access drop-down box. Otherwise, choose **Disabled**. The default value is Enabled. Secure web mode is a secure connection.

Step 4   In the Web Session Timeout field, enter the amount of time (in minutes) before the web session times out due to inactivity. You can enter a value between 30 and 160 minutes (inclusive), and the default value is 30 minutes.

Step 5   Click **Apply** to commit your changes.

✎

Note   If desired, you can delete the current certificate by clicking **Delete Certificate** and have the controller generate a new certificate by clicking **Regenerate Certificate**.

Step 6   Click **Save Configuration** to save your changes.

Using the CLI to Enable Web and Secure Web Modes

Follow these steps to enable web mode, secure web mode, or both using the controller CLI.

Step 1   To enable or disable web mode, enter this command:

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

This command allows users to access the controller GUI using "http://*ip-address*." The default value is disabled. Web mode is not a secure connection.

Step 2   To enable or disable secure web mode, enter this command:

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

This command allows users to access the controller GUI using "https://*ip-address*." The default value is enabled. Secure web mode is a secure connection.

Step 3   To enable or disable secure web mode with increased security, enter this command:

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

This command allows users to access the controller GUI using "https://*ip-address*" but only from browsers that support 128-bit (or larger) ciphers. The default value is disabled.

Step 4   To enable or disable SSLv2 for web administration, enter this command:

config network secureweb cipher-option sslv2 {**enable** | **disable**}

If you disable SSLv2, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The default value is enabled.

Step 5   To verify that the controller has generated a certificate, enter this command:

show certificate summary

Information similar to the following appears:

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

Step 6   (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 has been generated.

Step 7   To save the SSL certificate, key, and secure web password to non-volatile RAM (NVRAM) so that your changes are retained across reboots, enter this command:

save config

Step 8   To reboot the controller, enter this command:

reset system

You can use a TFTP server to download an externally generated SSL certificate to the controller. 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, or you must create static routes on the controller. Also, if you load the certificate through the distribution system 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 key can vary from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you obtain a new certificate from a Certificate Authority, make sure that the RSA key embedded in the certificate is at least 768 bits long.

Using the GUI to Load an SSL Certificate

Follow these steps to load an externally generated SSL certificate using the controller GUI.

Step 1   On the HTTP Configuration page, check the **Download SSL Certificate** check box (see Figure 2-2).

Figure 2-2   HTTP Configuration Page

Step 2   In the Server IP Address field, enter the IP address of the TFTP server.

Step 3 In the Maximum Retries field, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 4 In the Timeout field, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 5 In the Certificate File Path field, enter the directory path of the certificate.

Step 6 In the Certificate File Name field, enter the name of the certificate (*webadmincert_name*.pem).

Step 7 (Optional) In the Certificate Password field, enter a password to encrypt the certificate.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Step 10 To reboot the controller for your changes to take effect, click **Commands** > **Reboot** > **Reboot** > **Save and Reboot**.

Using the CLI to Load an SSL Certificate

Follow these steps to load an externally generated SSL certificate using the controller CLI.

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 To view the current download settings, enter this command and answer **n** to the prompt:

transfer download start

Information similar to the following appears:

```
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 To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, enter this command:

transfer download certpassword *private_key_password*

Step 6 To confirm the current download settings and start the certificate and key download, enter this command and answer **y** to the prompt:

transfer download start

Information similar to the following appears:

```
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 To save the SSL certificate, key, and secure web password to NVRAM so that your changes are retained across reboots, enter this command:

save config

Step 8 To reboot the controller, enter this command:

reset system

Using the CLI

The Cisco UWN Solution command line interface (CLI) is built into each controller. The CLI allows you to use a VT-100 emulator to locally or remotely configure, monitor, and control individual controllers 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 *Cisco Wireless LAN Controller Command Reference* for information on specific commands.

> **Note** If you want to input any strings from the XML configuration into CLI commands, you must enclose the strings in quotation marks.

Logging into the CLI

You access the CLI using one 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 the 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 a remote Ethernet connection.

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 CLI 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 systemwide 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, click **Management > Mgmt Via Wireless** page and check the **Enable Controller Management to be accessible from Wireless Clients** check box.