



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, page 2-2](#)
- [Enabling Web and Secure Web Modes, page 2-3](#)
- [Using the CLI, page 2-5](#)
- [Enabling Wireless Connections to the Web-Browser and CLI Interfaces, page 2-9](#)

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

You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Socket Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local Web Administration SSL certificate and automatically applies it to the GUI.

You can also load an externally generated certificate. Follow the instructions in the [“Loading an Externally Generated HTTPS Certificate”](#) section on page 2-4 for instructions on loading an externally generated certificate.

Using the CLI, follow these steps to enable 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.
-

Loading an Externally Generated HTTPS Certificate

- 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*).

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

In the CLI, enter `transfer download mode tftp` and answer `y` to the prompt to view the current download settings:

```
>
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)
Transfer Canceled
```

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
```

```
transfer download certpassword private_key_password
private_key_password
```

- Step 6**

```
TFTP Filename..... webadmincert_name
Are you sure you want to start? (y/n)
TFTP Webadmin cert transfer starting.
```

Step 7

Step 8

Step 9

Disabling the GUI

Disable Web-Based Management
Apply

Using Online Help

Using the CLI



Note

isco Wireless LAN Controller Command Reference

Logging into the CLI

-
-

Using a Local Serial Connection

-
-

Step 1

Step 2

-
-
-
-
-

Step 3



Note

```
config serial timeout 0 baudrate timeout
```

Using a Remote Ethernet Connection

-
-
-



Note

Navigating the CLI

Table 2-1 Commands for CLI Navigation and Common Tasks

Command	Action
?	
?	
exit	
Ctrl-Z	
save config	
reset system	

config network mgmt-via-wireless enable



Enable Controller Management to be accessible from Wireless Clients

