

# **Using the Web-Browser Interface**

This chapter describes the web-browser interface that you can use to configure the wireless device. This chapter contains these sections:

- Using the Web-Browser Interface for the First Time, page 3-2
- Using the Management Pages in the Web-Browser Interface, page 3-2
- Enabling HTTPS for Secure Browsing, page 3-5
- Using Online Help, page 3-14
- Disabling the Web-Browser Interface, page 3-16

The web-browser interface contains management pages that you use to change the wireless device settings, upgrade firmware, and monitor and configure other wireless devices on the network.

Note

The wireless device web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98 and 2000 platforms, and with Netscape version 7.0 on Windows 98, Windows 2000, and Solaris platforms.



Avoid using both the CLI and the web-browser interfaces to configure the wireless device. If you configure the wireless device using the CLI, the web-browser interface might display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the wireless device is misconfigured.

# Using the Web-Browser Interface for the First Time

Use the wireless device's IP address to browse to the management system. See the "Obtaining and Assigning an IP Address" section on page 2-3 for instructions on assigning an IP address to the wireless device. Follow these steps to begin using the web-browser interface:

- **Step 1** Start the browser.
- **Step 2** Enter the wireless device's IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer) and press **Enter**. The Summary Status page appears.

# Using the Management Pages in the Web-Browser Interface

The system management pages use consistent techniques to present and save configuration information. A navigation bar is on the left side of the page, and configuration action buttons appear at the bottom. You use the navigation bar to browse to other management pages, and you use the configuration action buttons to save or cancel changes to the configuration.



It is important to remember that clicking your web-browser's **Back** button returns you to the previous page without saving any changes you have made. Clicking **Cancel** cancels any changes you made on the page and keeps you on that page. Changes are only applied when you click **Apply**.

Figure 3-1 shows the web-browser interface home page.

| Hostname ap                          |                                  | ap uptime is 1 day, 1 hour, 36 mir                          |
|--------------------------------------|----------------------------------|---|
| SS SET-UP                            |                                  |   |
| RKMAP + Home: Summary S              | tatus                            |   |
| ATION + Association                  |                                  |   |
| ACES + Clients: 0                    |                                  | Repeaters: 0  |
| TY +<br>ES + <u>Network Identity</u> |                                  |   |
| SS SERVICES + IP Address             |                                  | 10.91.104.91  |
| ISOFTWARE +<br>LOG + MAC Address     |                                  | 0005.9a38.42c0  |
| Network Interfaces                   |                                  |   |
|                                      | MAC Address                      | Transmission Rate   |
|                                      | MAC Address                      |   |
| 1 <u>FastEthernet</u>                | 0005.9a38.42c0                   | 100Mb/s   |
| 1 Radio0-802.11B                     | 0001.6445.b9e6                   | 11.0Mb/s  |
| 1 Radio1-802.11A                     | 0005.9a39.2451                   | 54.0Mb/s  |
| Event Log                            |                                  |   |
| Time                                 | Severity                         | Description   |
| Mar 1 00:00:58.231                   | <ul> <li>Notification</li> </ul> | Line protocol on Interface Dot11Radio0, changed state to up |
| Mar 1 00:00:57.250                   | ◆Error                           | Interface Dot11Radio0, changed state to up                  |
| Mar 1 00:00:57.231                   | ◆Information                     | Interface Dot11Radio0, frequency 2447 selected              |
| Mar 1 00:00:57.231                   | ◆Information                     | Interface Dot11Radio0, frequency 2457 is in use             |
| Mar 1 00:00:57.231                   | ◆Information                     | Interface Dot11Radio0, frequency 2437 is in use             |
| Mar 1 00:00:57.231                   | Information                      | Interface Dot11Radio0, frequency 2427 is in use             |
| Mar 1 00:00:57.230                   | Information                      | Interface Dot11Radio0, frequency 2422 is in use             |
| Mar 1 00:00:57.230                   | ◆Information                     | Interface Dot11Radio0, frequency 2417 is in use             |
| Mar 1 00:00:57.230                   | ◆Information                     | Interface Dot11Radio0, frequency 2412 is in use             |
| Mar 1 00:00:55.232                   | Notification                     | Line protocol on Interface Dot11Radio1, changed state to up |
|                                      |                                  |   |

Figure 3-1 Web-Browser Interface Home Page

## **Using Action Buttons**

Table 3-1 lists the page links and buttons that appear on most management pages.

Table 3-1 Common Buttons on Management Pages

| Button/Link                    | Description   |
|--------------------------------|---|
| Navigation Links               |   |
| Home                           | Displays wireless device status page with information on the number of radio devices associated to the wireless device, the status of the Ethernet and radio interfaces, and a list of recent wireless device activity. |
| Express Setup                  | Displays the Express Setup page that includes basic settings such as system name, IP address, and role in radio network.  |
| Express Security               | Displays the Express Security page that you use to create SSID and assign security settings to them.  |
| Network Map                    | Displays a list of infrastructure devices on your wireless LAN.   |
| Association                    | Displays a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships.  |
| Network Interfaces             | Displays status and statistics for the Ethernet and radio interfaces and provides links to configuration pages for each interface.  |
| Security                       | Displays a summary of security settings and provides links to security configuration pages.   |
| Services                       | Displays status for several wireless device features and links to configuration pages for Telnet/SSH, CDP, domain name server, filters, QoS, SNMP, SNTP, and VLANs.   |
| Wireless Services              | Displays a summary of wireless services used with CCKM and provides links to WDS configuration pages.   |
| System Software                | Displays the version number of the firmware that the wireless device is running and provides links to configuration pages for upgrading and managing firmware.  |
| Event Log                      | Displays the wireless device event log and provides links to configuration pages where you can select events to be included in traps, set event severity levels, and set notification methods.                          |
| <b>Configuration Action Bu</b> | ttons   |
| Apply                          | Saves changes made on the page and remains on the page.   |
| Refresh                        | Updates status information or statistics displayed on a page.   |
| Cancel                         | Discards changes to the page and remains on the page.   |
| Back                           | Discards any changes made to the page and returns to the previous page.   |

## **Character Restrictions in Entry Fields**

Because the 1200 series access point uses Cisco IOS software, there are certain characters that you cannot use in the entry fields on the web-browser interface. You cannot use these characters in entry fields:

" ] + / Tab

**Trailing space** 

# **Enabling HTTPS for Secure Browsing**

You can protect communication with the access point web-browser interface by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Socket Layer (SSL) protocol.



When you enable HTTPS, your browser might lose its connection to the access point. If you lose the connection, change the URL in your browser's address line from http://ip\_address to https://ip\_address and log into the access point again.



When you enable HTTPS, most browsers prompt you for approval each time you browse to a device that does not have a fully qualified domain name (FQDN). To avoid the approval prompts, complete Step 2 through Step 9 in these instructions to create an FQDN for the access point. However, if you do not want to create an FQDN, skip to Step 10.

Follow these steps to create an FQDN and enable HTTPS:

- Step 1 If your browser uses popup-blocking software, disable the popup-blocking feature.
- **Step 2** Browse to the Express Setup page. Figure 3-2 shows the Express Setup page.

|                                    | name AP1100                   | A                        | P1100 uptime is 3 days, 23 hours, 33 min | utes   |
|------------------------------------|-------------------------------|--------------------------|--|--------|
| EXPRESS SET-UP<br>EXPRESS SECURITY |                               |                          |  |        |
|                                    | press Set-Up                  |                          |  |        |
| ASSOCIATION +                      |                               |                          |  |        |
|                                    | ost Name:                     | AP1100                   |  |        |
| INTERFACES MA                      | AC Address:                   | 0005.9a39.2110           |  |        |
| SECURITY +                         |                               | 0000.0400.2110           |  |        |
| WIRELESS SERVICES +                |                               |                          |  |        |
| SYSTEM SOFTWARE + Co               | onfiguration Server Protocol: | O DHCP 💿 Static IP       |  |        |
| EVENTLOG + IP                      | Address:                      | 10.91.107.18             |  |        |
| IP                                 | Subnet Mask:                  | 255.255.255.192          |  |        |
| De                                 | efault Gateway:               | 10.91.107.1              |  |        |
|                                    |                               |                          |  |        |
| SN                                 | IMP Community:                | defaultCommunity         |  |        |
|                                    |                               | Read-Only C Read-Write   |  |        |
|                                    |                               | ,                        |  |        |
| Det                                | dio0-802.11B                  |                          |  |        |
| Rad                                | a100-002.11D                  |                          |  |        |
| Ro                                 | ole in Radio Network: 🦷       | Access Point Root O Repe | ater Non-Root                            |        |
|                                    | 0                             | ි Workgroup Bridge       |  |        |
| Ор                                 | otimize Radio Network for: 🤇  | ා Throughput             | Custom                                   |        |
| Air                                | ronet Extensions: (           | 🖲 Enable 🔿 Disable       |  |        |
|                                    |                               |                          |  |        |
|                                    |                               |                          |  | 38     |
|                                    |                               |                          | Apply Car                                | ncel a |

Figure 3-2 Express Setup Page

**Step 3** Enter a name for the access point in the System Name field and click **Apply**.

**Step 4** Browse to the Services – DNS page. Figure 3-3 shows the Services – DNS page.

21643

| HOME                      | Hostname AP1100                              | AP1100 uptime is 4 days, 18 hours, 3 minutes |
|---------------------------|--|--|
| EXPRESS SET-UP            |  |  |
| EXPRESS SECURITY          |  |  |
| NETWORK MAP +             | Services: DNS - Domain Name Service          |  |
| ASSOCIATION +             | Domain Name System (DNS): 💿 Enable 🔿 Disable |  |
| NETWORK +<br>INTERFACES + | Domain Name System (DNS): C Enable C Disable |  |
| SECURITY +                | Domain Name (optional):                      |  |
| SERVICES                  |  |  |
| Telnet/SSH                |  |  |
| Hot Standby               | Name Server IP Addresses:                    |  |
| CDP                       | 1.   |  |
| DNS                       |  |  |
| Filters                   | 2.   |  |
| HTTP                      | 3.   |  |
| Proxy Mobile IP           | 3.   |  |
| QoS                       |  |  |
| SNMP                      |  |  |
| NTP                       |  |  |
| VLAN                      |  |  |
| ARP Caching               |  |  |
| WIRELESS SERVICES +       |  |  |
| SYSTEM SOFTWARE +         |  |  |
| EVENTLOG +                |  |  |

Figure 3-3 Services – DNS Page

- **Step 5** Select **Enable** for Domain Name System.
- **Step 6** In the Domain Name field, enter your company's domain name. At Cisco Systems, for example, the domain name is *cisco.com*.
- Step 7 Enter at least one IP address for your DNS server in the Name Server IP Addresses entry fields.
- **Step 8** Click **Apply**. The access point's FQDN is a combination of the system name and the domain name. For example, if your system name is *ap1100* and your domain name is *company.com*, the FQDN is *ap1100.company.com*.
- **Step 9** Enter the FQDN on your DNS server.

<u>}</u> Tip

If you do not have a DNS server, you can register the access point's FQDN with a dynamic DNS service. Search the Internet for *dynamic DNS* to find a fee-based DNS service.

**Step 10** Browse to the Services: HTTP Web Server page. Figure 3-4 shows the HTTP Web Server page:

Figure 3-4 Services: HTTP Web Server Page

| HOME              | Hostname AP1100                                  | AP1100 uptime is 5 days, 41 minu |
|-------------------|--|----------------------------------|
| EXPRESS SET-UP    |  |                                  |
| EXPRESS SECURITY  |  |                                  |
| NETWORK MAP +     | + Services: HTTP- Web Server                     |                                  |
| ASSOCIATION +     | Web-based Configuration Management:              |                                  |
|                   | +  | Enable Standard (HTTP) Browsing  |
| NTERFACES         | +  | Enable Secure (HTTPS) Browsing   |
| ERVICES           |  |                                  |
| Teinet/SSH        |  | 🗖 Disable Web-based Management   |
| Hot Standby       | -  |                                  |
| CDP               | HTTP Port:                                       | 80 (1025-65535 or default 80)    |
| DNS               |  | 80 (1025-65535 or default 80)    |
| Filters           | HTTPS Port:                                      | 443 (1025-65535 or default 443)  |
| HTTP              | _  |                                  |
|                   | _  |                                  |
| Proxy Mobile IP   | Help Root URL: (Set to default by clearing text) | ox)                              |
| QoS               | http://www.cisco.com/warp/public/779/smbiz/pr    | adoarfia/holp/opa                |
| SNMP              |  | ouconlightelpreag                |
| NTP               | Target Help URL:                                 |                                  |
| VLAN              | http://www.cisco.com/warp/public/779/smbiz/pro   | deenfig/holp/opg/123.02_LA/1100  |
| ARP Caching       | http://www.cisco.com/warp/public///o/sinbiz/pro  | dconing/help/eag/123-02.0//1100  |
| VIRELESS SERVICES | +  |                                  |
| SYSTEM SOFTWARE   | +  |                                  |
| EVENT LOG +       | +  |                                  |

**Step 11** Select the Enable Secure (HTTPS) Browsing check box and click **Apply**.

Note

Although you can enable both standard HTTP and HTTPS, Cisco recommends that you enable one or the other.

A warning window appears stating that you will use HTTPS to browse to the access point. The window also instructs you to change the URL that you use to browse to the access point from *http* to *https*. Figure 3-5 shows the warning window:

Figure 3-5 HTTPS Warning Window

| Microsoft | Internet Explorer  |        |
|-----------|--|--------|
|           | WARNING:<br>Web-based configuration will now employ secure HTTP.<br>To access the browser using secure HTTP, use the URL https://10.91.104.92. |        |
|           | OK   | 101030 |

Step 12 Click OK. The address in your browser's address line changes from http://ip-address to https://ip-address.

**Step 13** Another warning window appears stating that the access point's security certificate is valid but is not from a known source. However, you can accept the certificate with confidence because the site in question is your own access point. Figure 3-6 shows the certificate warning window:

Figure 3-6 Certificate Warning Window

| Security | Aler   | t 🛛 🗵  |        |
|----------|--|--|--------|
| ß        | Information you exchange with this site cannot be viewed or<br>changed by others. However, there is a problem with the site's<br>security certificate. |  |        |
|          | ⚠  | The security certificate was issued by a company you have<br>not chosen to trust. View the certificate to determine whether<br>you want to trust the certifying authority. |        |
|          | 0  | The security certificate date is valid.  |        |
|          | ⚠  | The name on the security certificate is invalid or does not<br>match the name of the site  |        |
|          | Doy  | ou want to proceed?  |        |
|          |  | Yes View Certificate   | 121631 |

**Step 14** Click **View Certificate** to accept the certificate before proceeding. (To proceed without accepting the certificate, click **Yes**, and skip to Step 23 in these instructions.) Figure 3-7 shows the Certificate window.

| Certificate   | ? ×  |
|---|------|
| General Details Certification Path  | 1    |
| Certificate Information   |      |
| This CA Root certificate is not trusted. To enable trust,<br>install this certificate in the Trusted Root Certification<br>Authorities store. |      |
|   |      |
| Issued to: IOS-Self-Signed-Certificate-2587435280   | -    |
| Issued by: IOS-Self-Signed-Certificate-2587435280   |      |
| <b>Valid from</b> 3/1/2002 <b>to</b> 12/31/2019   |      |
| Issuer State  | ment |
|   | ОК   |

Figure 3-7 Certificate Window

**Step 15** On the Certificate window, click **Install Certificate**. The Microsoft Windows Certificate Import Wizard appears. Figure 3-8 shows the Certificate Import Wizard window.



Figure 3-8 Certificate Import Wizard Window

**Step 16** Click **Next**. The next window asks where you want to store the certificate. Cisco recommends that you use the default storage area on your system. Figure 3-9 shows the window that asks about the certificate storage area.

Figure 3-9 Certificate Storage Area Window

| Certificate Import Wizard   | ×     |
|---|-------|
| Certificate Store   |       |
| Certificate stores are system areas where certificates are kept.                    |       |
| Windows can automatically select a certificate store, or you can specify a location | for   |
| Automatically select the certificate store based on the type of certificate         |       |
| O Place all certificates in the following store                                     |       |
| Certificate store;  |       |
| Browse,   | ,     |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
| < <u>B</u> ack <u>N</u> ext > C   | ancel |
|   |       |

**Step 17** Click **Next** to accept the default storage area. A window appears that states that you successfully imported the certificate. Figure 3-10 shows the completion window.

Figure 3-10 Certificate Completion Window

| Certificate Import Wizard |   | ×  |
|---------------------------|---|--|
|                           | Completing the (<br>Wizard<br>You have successfully comp<br>wizard.<br>You have specified the follo |  |
|                           |   | Automatically determined by t<br>Certificate |
|                           | < <u>B</u> ack  | Finish Cancel                                |

**Step 18** Click **Finish**. Windows displays a final security warning. Figure 3-11 shows the security warning.

Figure 3-11 Certificate Security Warning

| Security | Warning   |        |
|----------|---|--------|
|          | You are about to install a certificate from a certification authority (CA) claiming to represent:   | l      |
| -        | IOS-Self-Signed-Certificate-2587435280  | l      |
|          | Windows cannot validate that the certificate is actually from "IOS-Self-Signed-Certificate-2587435280". You should<br>confirm its origin by contacting "IOS-Self-Signed-Certificate-2587435280". The following number will assist you in this<br>process: |        |
|          | Thumbprint (sha1): 55235875 C306F1DA 1DC55CD0 40E54735 CFB0B036   | l      |
|          | Warning:<br>If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a<br>certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.        |        |
|          | Do you want to install this certificate?  | l      |
|          | <u>Y</u> es   | 101000 |

**Step 19** Click **Yes**. Windows displays another window stating that the installation is successful. Figure 3-12 shows the completion window.

Figure 3-12 Import Successful Window

| Certificat | e Import Wizard 🛛 🔀        |        |
|------------|----------------------------|--------|
| ٩          | The import was successful. |        |
|            | OK                         | 121633 |

- Step 20 Click OK.
- Step 21 On the Certificate window shown in Figure 3-7, which is still displayed, click OK.
- Step 22 On the Security Alert window shown in Figure 3-6, click Yes.
- **Step 23** The access point login window appears and you must log into the access point again. The default user name is *Cisco* (case-sensitive) and the default password is *Cisco* (case-sensitive).

### **CLI Configuration Example**

This example shows the CLI commands that are equivalent to the steps listed in the "Enabling HTTPS for Secure Browsing" section on page 3-5:

```
AP# configure terminal
AP(config)# hostname ap1100
AP(config)# ip domain name company.com
AP(config)# ip name-server 10.91.107.18
AP(config)# ip http secure-server
AP(config)# end
```

In this example, the access point system name is *ap1100*, the domain name is *company.com*, and the IP address of the DNS server is 10.91.107.18.

For complete descriptions of the commands used in this example, consult the Cisco IOS Commands Master List, Release 12.3. Click this link to browse to the master list of commands: http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products\_product\_indices\_list.html

### **Deleting an HTTPS Certificate**

The access point generates a certificate automatically when you enable HTTPS. However, if you need to change the access point's fully qualified domain name (FQDN) or you need to add an FQDN after enabling HTTPS, you might need to delete the certificate. Follow these steps:

- Step 1 Browse to the Services: HTTP Web Server page.
- Step 2 Uncheck the Enable Secure (HTTPS) Browsing check box to disable HTTPS.
- **Step 3** Click **Delete Certificate** to delete the certificate.
- **Step 4** Re-enable HTTPS. The access point generates a new certificate using the new FQDN.

# **Using Online Help**

Click the help icon at the top of any page in the web-browser interface to display online help. Figure 3-13 shows the help and print icons.

Figure 3-13 Help and Print Icons



When a help page appears in a new browser window, use the Select a topic drop-down menu to display the help index or instructions for common configuration tasks, such as configuring VLANs.

### **Changing the Location of Help Files**

Cisco maintains up-to-date HTML help files for access points on the Cisco web site. By default, the access point opens a help file on Cisco.com when you click the help button on the access point web-browser interface. However, you can install the help files on your network so your access points can access them there. Follow these steps to install the help files locally:

**Step 1** Download the help files from the Software Center on Cisco.com. Click this link to browse to the Software Center's Wireless Software page:

http://www.cisco.com/cisco/software/navigator.html

Select the help files that match the software version on your access point.

**Step 2** Unzip the help files on your network in a directory accessible to your access point. When you unzip the help files, the HTML help pages are stored in a folder named according to the help version number and access point model number.

**Step 3** Browse to the Services: HTTP Web Server page in the access point web-browser interface. Figure 3-14 shows the HTTP Web Server page:

| Figure 3-14 H | ITTP Web | Server Page |
|---------------|----------|-------------|
|---------------|----------|-------------|

| HOME                       | Hostname AP1100                                    | AP1100 uptime is 5 days, 41 minut |
|----------------------------|--|-----------------------------------|
| EXPRESS SET-UP             |  |                                   |
| EXPRESS SECURITY           |  |                                   |
| NETWORK MAP +              | Services: HTTP- Web Server                         |                                   |
| ASSOCIATION +              | Web-based Configuration Management:                |                                   |
| NETWORK +                  | web-based Computation Management.                  | 🗹 Enable Standard (HTTP) Browsing |
| INTERFACES '<br>SECURITY + |  | Enable Secure (HTTPS) Browsing    |
| SERVICES                   |  |                                   |
| Telnet/SSH                 |  | Disable Web-based Management      |
| Hot Standby                |  |                                   |
| CDP                        | HTTP Port:   | 80 (1025-65535 or default 80)     |
| DNS                        |  |                                   |
| Filters                    | HTTPS Port:  | 443 (1025-65535 or default 443)   |
| HTTP                       |  |                                   |
| Proxy Mobile IP            | Help Root URL: (Set to default by clearing textbo  | <b>1</b> /1                       |
| QoS                        | Theip Root DRE. (Det to deladit by cleaning textor | ,,<br>,,                          |
| SNMP                       | http://www.cisco.com/warp/public/779/smbiz/pro     | odconfig/help/eag                 |
| NTP                        | Tanuat Hala UDL                                    |                                   |
| VLAN                       | Target Help URL:                                   |                                   |
| ARP Caching                | http://www.cisco.com/warp/public/779/smbiz/proc    | lconfig/help/eag/123-02.JA/1100   |
| WIRELESS SERVICES +        |  |                                   |
| SYSTEM SOFTWARE +          |  |                                   |
| EVENTLOG +                 |  |                                   |

**Step 4** In the Default Help Root URL entry field, enter the complete path to the location where you unzipped the help files. When you click the access point help button, the access point automatically appends the help version number and model number to the path that you enter.

S, Note

Do not add the help version number and device model number to the Default Help Root URL entry. The access point automatically adds the help version and model number to the help root URL.

If you unzip the help files on your network file server at *//myserver/myhelp*, your Default Help Root URL looks like this:

#### http://myserver/myhelp

Table 3-2 shows an example help location and Help Root URL for an 1100 series access point.

Table 3-2 Example Help Root URL and Help Location

| Files Unzipped at This Location | Default Help Root URL  | Actual Location of Help Files    |
|---------------------------------|------------------------|----------------------------------|
| //myserver/myhelp               | http://myserver/myhelp | //myserver/myhelp/123-02.JA/1100 |

### Step 5 Click Apply.

# **Disabling the Web-Browser Interface**

To prevent all use of the web-browser interface, select the **Disable Web-Based Management** check box on the Services: HTTP-Web Server page and click **Apply**. Figure 3-15 shows the Services: HTTP-Web Server page.

Figure 3-15 Services: HTTP-Web Server Page

|                       | · · · · · · · · · · · · · · · · · · ·      |                                       |
|-----------------------|--|---------------------------------------|
| HOME                  | Hostname AP1100                            | AP1100 uptime is 5 days, 41 minutes   |
| EXPRESS SET-UP        |  |                                       |
| EXPRESS SECURITY      | Services: HTTP- Web Server                 |                                       |
| NETWORK MAP +         | ·  |                                       |
| ASSOCIATION +         | Web-based Configuration Management:        | :                                     |
| NETWORK<br>INTERFACES | r  | • Enable Standard (TTTP) browsing     |
|                       | +  | Enable Secure (HTTPS) Browsing        |
| SERVICES              | -  | Disable Web-based Management          |
| Telnet/SSH            |  | Lisable web-based wanagement          |
| Hot Standby           | T  |                                       |
| CDP                   | HTTP Port:                                 | 80 (1025-65535 or default 80)         |
| DNS                   |  |                                       |
| Filters               | HTTPS Port:                                | 443 (1025-65535 or default 443)       |
| HTTP                  |  |                                       |
| Proxy Mobile IP       | Help Root URL: (Set to default by clearing | textbox)                              |
| QoS                   |  | ,                                     |
| SNMP                  | http://www.cisco.com/warp/public/779/smb   | piz/prodconfig/help/eag               |
| NTP                   | Target Help URL:                           |                                       |
| VLAN                  |  |                                       |
| ARP Caching           | http://www.cisco.com/warp/public/779/smbi  | iz/prodconfig/help/eag/123-U2.JAV11UU |
| WIRELESS SERVICES     | f  |                                       |
| SYSTEM SOFTWARE       | -  |                                       |
| EVENT LOG +           | F  |                                       |

To re-enable the web-browser interface, enter this global configuration command on the access point CLI:

ap(config)# ip http server