Using the Web-Browser Interface

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

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 9.0 and Mozilla Firefox version 17.

Note 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 IP address to browse to the management system. See the "Logging into the Access Point" section on page 4-3 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 IP address in the address bar of the and press **Enter**.
The Summary Status page appears.

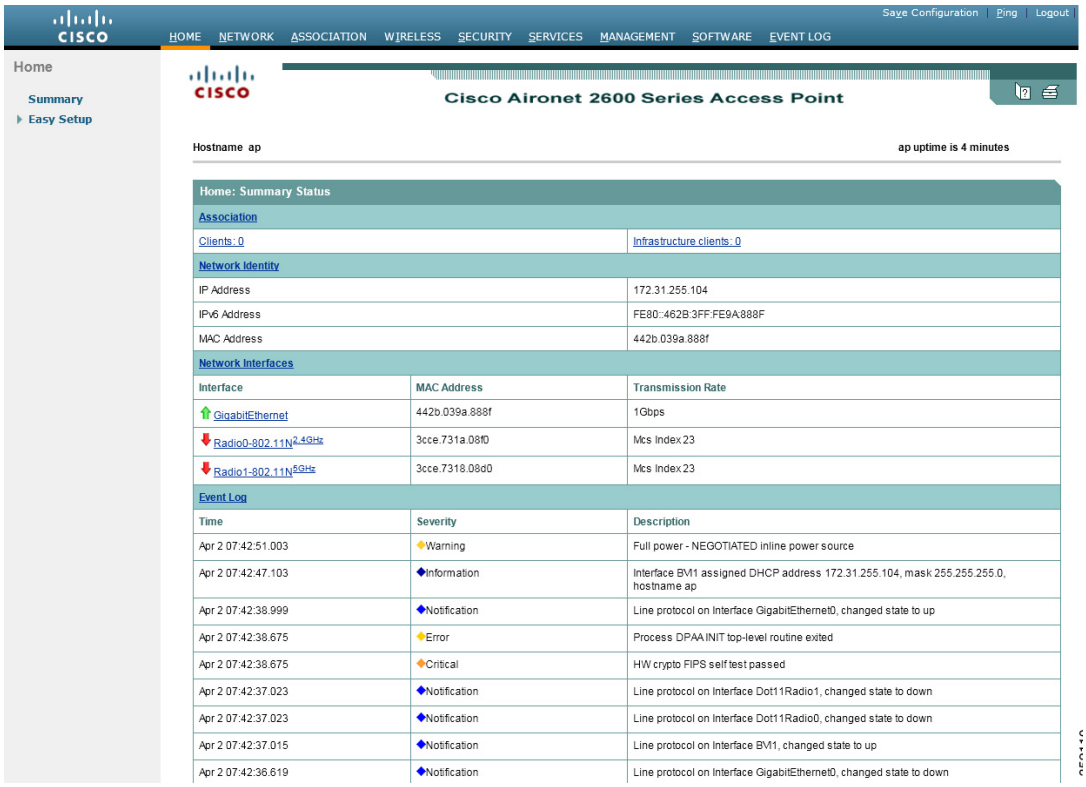
Using the Management Pages in the Web-Browser Interface

The system management pages use consistent techniques to present and save configuration information. You can use the navigation bar present at the top of a page to select the main menu options. Another navigation bar is present on the left side of the page, to use for navigating through the sub menus. You can use the navigation bar to browse to other management pages, and use the configuration action buttons to save or cancel changes to the configuration.

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

Figure 2-1 shows the web-browser interface home page.

Figure 2-1 Web-Browser Interface Home Page



Using Action Buttons

Table 2-1 lists the page links and buttons that appear on the management page.

Table 2-1 Buttons and Links on the Management Page

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.
Easy Setup	Displays the Easy Setup page that includes basic settings such as system name, IP address, and role in radio network.
Network	Displays a list of infrastructure devices on your wireless LAN. Provides configuration submenus for the access point interfaces (radio and Ethernet).
Association	Displays a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships.
Wireless	Displays a summary of wireless Domain services configuration and devices, and provides links to WDS configuration pages.
Security	Displays a summary of security settings and provides links to security configuration pages.

Table 2-1 Buttons and Links on the Management Page (continued)

Button/Link	Description
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.
Management	Displays a list of current guest users and provides links to configuration pages for guest users and web authentication pages.
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.
Configuration Action Buttons	
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.
Logout	Exits the AP configuration web interface without saving.
Ping	Pings an IPv4 or IPv6 address
Save Configuration	Saves the AP's current configuration to NVRAM.

Character Restrictions in Entry Fields

You cannot use the following characters in the entry fields on the web-browser interface. This is true for all access points using Cisco IOS software.

“

]

+

/

Tab

Trailing space

Enabling HTTPS for Secure Browsing

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

Note 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 address line from http://*ip_address* to **https://*ip_address*** and log into the access point again.

Note 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, create an FQDN for the access point as detailed in the following procedure.

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 Choose **Easy Setup > Network Configuration**.

The Network Configuration page appears.

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

Step 4 Choose **Services > DNS** page.

The Services: DNS - Domain Name Service page appears.

Step 5 In the **Domain Name System (DNS)** field, click the **Enable** radio button.

Step 6 In the **Domain Name** field, enter your company's domain name.

Step 7 Enter at least one IP address for your DNS server in the **Name Server IPv4/IPv6 Addresses** fields.

Step 8 Click **Apply**.

The access point FQDN is a combination of the system name and the domain name. For example, if your system name is *ap3600* and your domain name is *company.com*, the FQDN is *ap3600.company.com*.

Step 9 Enter the FQDN on your DNS server.

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

Step 10 Choose **Services > HTTP**.

The Services: HTTP - Web Server page is displayed.

Step 11 In the **Web-based Configuration Management** field, select the **Enable Secure (HTTPS) Browsing** check box.

Step 12 In the **Domain Name** field, enter a domain name, and then click **Apply**.

Note Enabling HTTPS automatically disables HTTP. To maintain HTTP access with HTTPS enabled, check the **Enable Secure (HTTPS) Browsing** check box, and then check the **Enable Standard (HTTP) Browsing** check box. Although you can enable both standard HTTP and HTTPS, we recommend that you enable only one.

A warning appears stating that you will now use secure HTTP to browse to the access point. The warning also displays the new URL containing *https*, which you will need to use to browse to the access point.

Step 13 In the warning box, click **OK**.

The address in your browser address line changes from *http://*<ip-address> to *https://*<ip-address>.

Step 14 Another warning appears stating that the access point security certificate was not issued by a trusted certificate authority. However, you can ignore this warning. Click **Continue to this Website (not recommended).**

Note The following steps assume that you are using Microsoft Internet Explorer. If you are not, please refer to your browser documentation for more information on how to access web sites using self signed certificates.

Step 15 The access point login window appears and you must log in to the access point again. The default username is *Cisco* (case-sensitive) and the default password is *Cisco* (case-sensitive).

Step 16 To display the access point's security certificate, click the **Certificate error** icon in the address bar.

Step 17 Click **View Certificates**.

Step 18 In the Certificate window, click **Install Certificate**.
The Microsoft Windows Certificate Import Wizard appears.

Step 19 Click **Next**.
The next screen asks where you want to store the certificate. We recommend that you use the default storage area on your system.

Step 20 Click **Next** to accept the default storage area.
You have now successfully imported the certificate.

Step 21 Click **Finish**.
A security warning is displayed.

Step 22 Click **Yes**.
A message box stating that the installation is successful is displayed.

Step 23 Click **OK**.

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 2-5:

```
AP# configure terminal
AP(config)# hostname ap3600
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 *ap3600*, 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 12.4. Click this link to browse to the master list of commands:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124htnml.htm

Deleting an HTTPS Certificate

The access point generates a certificate automatically when you enable HTTPS. However, if you need to change the fully qualified domain name (FQDN) for an access point, 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 Partial SSL certificate** to delete the certificate.

Step 4 Click **Apply**. The access point generates a new certificate using the new FQDN.

CLI Commands for Deleting an HTTPS Certificate

In the global configuration mode, use the following commands for deleting an HTTPS certificate.

	Command	Purpose
Step 1	**no ip http secure-server**	Disables HTTPS
Step 2	**crypto key zeroize rsa** *name-of-rsa-key*	Deletes the RSA key for the http server. Along with this all the router certificates (HTTPS certificates) issued using these keys will also be removed.

Using Online User Guides

In the web-browser interface, click the help icon at the top of the Home page to the online version of this guide (Cisco IOS Configuration Guide for Autonomous Cisco Aironet Access Points). You can choose view the guide online or you can also download a PDF version of the guide for offline reference. The online guide is periodically updated and hence will give you more up to date information.

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**.

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

```
ap(config)# ip http server
```