



Managing Firmware and Configurations

This section describes how to update the firmware version on the access point, how to distribute firmware to other access points, how to distribute the access point's configuration to other access points, and how to download, upload, and reset the access point configuration. You use the Cisco Services Setup page as a starting point for all these activities.

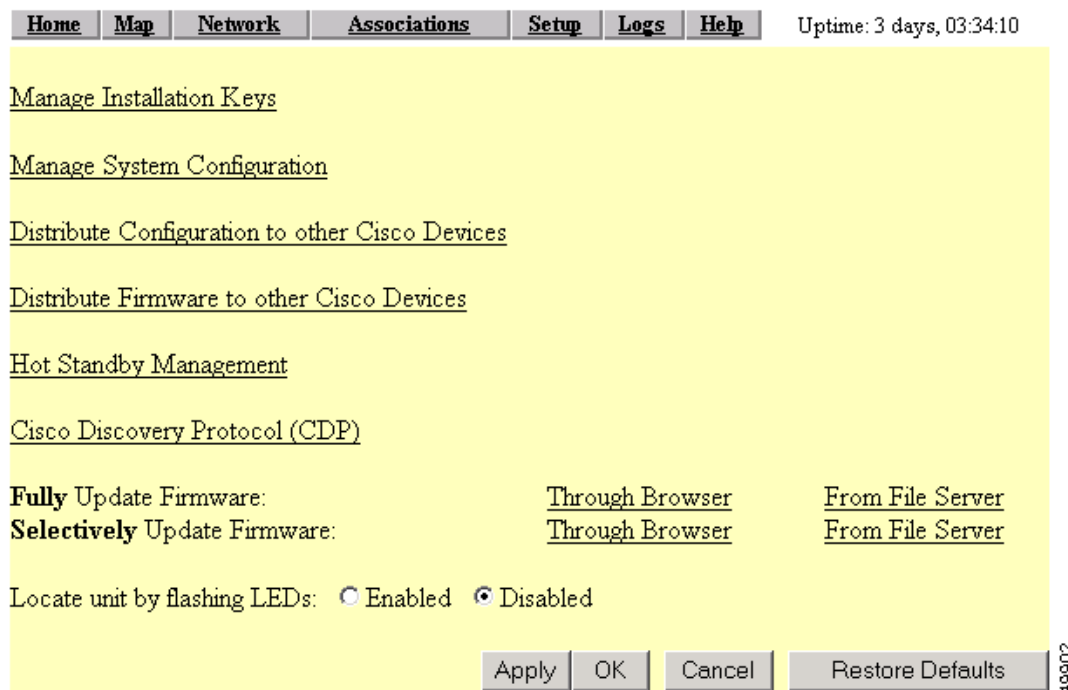
This chapter contains the following sections:

- [Updating Firmware, page 10-2](#)
- [Distributing Firmware, page 10-8](#)
- [Distributing a Configuration, page 10-9](#)
- [Downloading, Uploading, and Resetting the Configuration, page 10-10](#)

Updating Firmware

You use the Cisco Services Setup page to update the access point’s firmware. You can perform the update by browsing to a local drive or by using FTP to update the firmware from a file server. Figure 10-1 shows the Cisco Services Setup page.

Figure 10-1 Cisco Services Setup Page



Follow this link path in the browser interface to reach the Cisco Services Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.

Updating with the Browser from a Local Drive

When you update the firmware with your browser, you browse to your hard drive or to a mapped network drive for the new firmware. You can update the four firmware components—the management system firmware, the firmware web pages, and the radio firmware for both radios—individually or all at once. It is simplest to update all the components at once, but in some situations you might want to update them individually.

Full Update of the Firmware Components

To update all the firmware components at the same time, click **Through Browser** on the Fully Update Firmware line on the Cisco Services Setup page. The Update All Firmware Through Browser page appears. Figure 10-2 shows the Update All Firmware Through Browser page.

Figure 10-2 Update All Firmware Through Browser Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 3 days, 03:36:53
Current Version of System Firmware:						12.00	
Current Version of Web Pages:						12.00	
Current Version of Internal Radio Firmware:						5.02.03	
Current Version of Module Radio Firmware:						5.02.03	
Retrieve All Firmware Files							
New File for All Firmware:				<input type="text"/>		<input type="button" value="Browse..."/>	
						<input type="button" value="Browser Update Now"/>	
						<input type="button" value="Done"/>	

Follow these steps to update all three firmware components through the browser:

- Step 1** If you know the exact path and filename of the new firmware image file, type it in the New File for All Firmware entry field.
- If you aren't sure of the exact path to the new firmware image file, click **Browse...** next to the New File entry field. When the File Upload window appears, go to the directory that contains the firmware image file and select the file. Click **Open**.
- Step 2** When the filename for the new firmware appears in the New File entry field, click **Browser Update Now** to load and install the new firmware. When the update is complete, the access point automatically reboots.

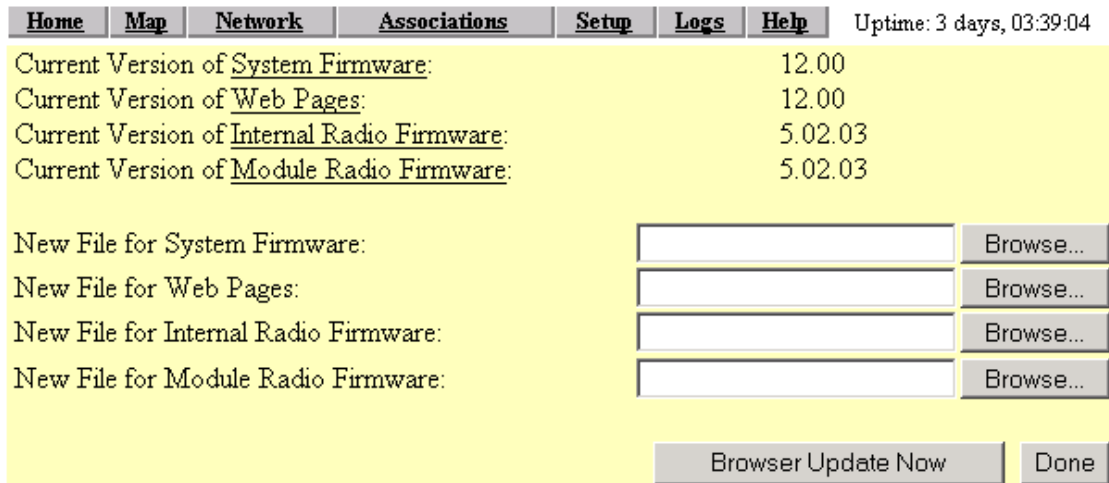


Note The access point only updates the radio firmware if the radio firmware version to be loaded is newer than the firmware in the radio.

Selective Update of the Firmware Components

To update firmware components individually, click **Through Browser** on the Selectively Update Firmware line on the Cisco Services Setup page. The Update Firmware Through Browser page appears. [Figure 10-3](#) shows the Update Firmware Through Browser page.

Figure 10-3 Update Firmware Through Browser Page



Follow these steps to update one of the firmware components through the browser:

- Step 1** If you know the exact path and filename of the new firmware component, type it in the New File for [component] entry field.
If you aren't sure of the exact path to the new component, click **Browse...** next to the component's New File entry field. When the File Upload window appears, go to the directory that contains the component and select the file. Click **Open**.
- Step 2** When the filename for the new component appears in the New File entry field, click **Browser Update Now** to load and install the new component. When the update is complete, the AP automatically reboots.

Updating from a File Server

When you update the firmware from a file server, you load new firmware through FTP or TFTP from a file server. You can update the four firmware components—the management system firmware, the firmware web pages, and the radio firmware for both radios—individually or all at once. It is simplest to update all the components at once, but in some situations you might want to update them individually.

Full Update of the Firmware Components

To update all the firmware components at the same time, click **From File Server** on the Fully Update Firmware line on the Cisco Services Setup page. The Update All Firmware From File Server page appears. Figure 10-4 shows the Update All Firmware From File Server page.

Figure 10-4 Update All Firmware From File Server Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 3 days, 03:41:09
Current Version of System Firmware:						12.00	
Current Version of Web Pages:						12.00	
Current Version of Internal Radio Firmware:						5.02.03	
Current Version of Module Radio Firmware:						5.02.03	
New File for All Firmware:						<input type="text"/>	
<u>File Server Setup</u>							
Update From Server			Save To Server			Done	Cancel

Follow these steps to update all three firmware components from a file server:

- Step 1** Click the File Server Setup link to enter the FTP settings. The FTP Setup page appears. [Figure 10-5](#) shows the FTP Setup page.

Figure 10-5 FTP Setup Page

Map	Help	Uptime: 02:37:33
File Transfer Protocol:	<input type="text" value="FTP"/>	
Default File Server:	<input type="text"/>	
FTP Directory:	<input type="text"/>	
FTP User Name:	<input type="text" value="anonymous"/>	
FTP User Password:	<input type="text" value="*****"/>	
Apply		OK
Cancel		Restore Defaults

- Step 2** Enter the FTP settings on the FTP Setup page.
- Select FTP or TFTP from the File Transfer Protocol pull-down menu. FTP (File Transfer Protocol) is the standard protocol that supports transfers of data between local and remote computers. TFTP (Trivial File Transfer Protocol) is a relatively slow, low-security protocol that requires no user name or password.
 - In the Default File Server entry field, enter the IP address of the server where the access point should look for FTP files.
 - In the FTP Directory entry field, enter the directory on the server where FTP files are located.
 - In the FTP User Name entry field, enter the user name assigned to the FTP server. If you selected TFTP, you can leave this field blank.

- e. In the FTP Password entry field, enter the password associated with the user name. If you selected TFTP, you can leave this field blank.
- f. Click **OK**. You return automatically to the Update All Firmware Through File Server page.

Step 3 On the Update All Firmware Through File Server page, type the filename of the new firmware image file in the New File for All Firmware entry field.

Step 4 Click **Browser Update Now** to load and install the new firmware. When the update is complete, the access point automatically reboots.

**Note**

The access point only updates the radio firmware if the radio firmware version to be loaded is newer than the firmware in the radio.

Selective Update of the Firmware Components

To update firmware components individually, click **From File Server** on the Selectively Update Firmware line on the Cisco Services Setup page. The Update Firmware From File Server page appears. Figure 10-6 shows the Update Firmware From File Server page.

Figure 10-6 Update Firmware From File Server Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 3 days, 03:43:05
Current Version of <u>System Firmware</u> :						12.00	
Current Version of <u>Web Pages</u> :						12.00	
Current Version of <u>Internal Radio Firmware</u> :						5.02.03	
Current Version of <u>Module Radio Firmware</u> :						5.02.03	
New File for System Firmware:						<input type="text"/>	
New File for Web Pages:						<input type="text"/>	
New File for Internal Radio Firmware:						<input type="text"/>	
New File for Module Radio Firmware:						<input type="text"/>	
<u>File Server Setup</u>							
Update From Server				Save To Server		Done	Cancel

To update one of the three firmware components from the file server, follow the steps listed in the “[Full Update of the Firmware Components](#)” section on page 10-4, but in **Step 3**, type the filenames of the firmware components you want to update in the components’ entry fields. Click **Browser Update Now** to load and install the new firmware. When the update is complete, the access point automatically reboots.

Retrieving Firmware and Web Page Files

You can retrieve and download the following files from an access point to your computer's hard drive:

- System firmware
- Web pages
- Internal radio firmware
- Module radio firmware

These files can be downloaded selectively or at one time, depending on which page you select from which to retrieve them. To retrieve all firmware and web page files, browse to the Update All Firmware Through Browser page and click **Retrieve All Firmware Files**. To selectively retrieve these files, browse to the Selectively Update Firmware Through Browser or From File Server and select the files you wish to retrieve.

Follow these steps to retrieve and download all files.

-
- Step 1** From the Services section of the setup page, click **Cisco Services**. The Cisco Services Setup page appears.
 - Step 2** On the Fully Update Firmware: line, click **Through Browser**. The Update All Firmware Through Browser page appears.
 - Step 3** Click **Retrieve All Firmware Files**. A file download window appears.
 - Step 4** Click **Save** to download the file to your computer. A Save As window appears.
 - Step 5** Browse to the drive and folder on your computer where you want to save the file.
 - Step 6** Click **Save**. A File Download window appears and provides the progress of the download operation.
 - Step 7** Click **Close** when the download is complete.
-

Follow these steps to retrieve and download selected files.

-
- Step 1** From the Selectively Update Firmware line on the Cisco Services Setup page, click **Through Browser** or **From File Server**. The Cisco Services Setup page appears.
 - Step 2** Click on the link for the file you wish to retrieve. A file download window appears.
 - Step 3** Click **Save** to download the file to your computer. A Save As window appears.
 - Step 4** Browse to the drive and folder on your computer where you want to save the file.
 - Step 5** Click **Save**. A File Download window appears and provides the progress of the download operation.
 - Step 6** Click **Close** when the download is complete.
-

Distributing Firmware

Use the Distribute Firmware page to distribute the access point's firmware to other Cisco Aironet access points. [Figure 10-7](#) shows the Distribute Firmware page.

The access point sends its firmware to all the access points on your network that:

- Are running access point firmware version 10.00 or newer
- Can detect the IP multicast query issued by the distributing access point (network devices such as routers can block multicast messages)
- Have their web servers enabled for external browsing (see the [“Entering Web Server Settings and Setting Up Access Point Help”](#) section on page 7-7).
- Have the same HTTP port setting as the distributing access point (the HTTP port setting is on the Web Server Setup page)
- Have a Default Gateway setting other than the default setting, which is 255.255.255.255 (the Default Gateway setting is on the Express Setup and Routing Setup pages)
- If they have User Manager enabled, contain in their User Lists a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing access point)

Follow the steps in the [“Limiting Distributions”](#) section on page 10-10 to limit the firmware distribution to certain access points.

Figure 10-7 Distribute Firmware Page

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 3 days, 03:44:42
Current User:						User Manager Not Enabled	
Distribute All Firmware:						<input checked="" type="radio"/> yes <input type="radio"/> no	
Current Version of System Firmware:				12.00		<input checked="" type="checkbox"/>	
Current Version of Web Pages:				12.00		<input checked="" type="checkbox"/>	
Current Version of Internal Radio Firmware:				5.02.03		<input checked="" type="checkbox"/>	
Current Version of Module Radio Firmware:				5.02.03		<input checked="" type="checkbox"/>	
						Start Abort	

Follow this link path in the browser interface to reach the Distribute Firmware page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Distribute Firmware to other Cisco Devices**.

Follow these steps to distribute firmware to other access points:

-
- Step 1** Follow the link path to reach the Distribute Firmware page.
- Step 2** To distribute all three firmware components at once, verify that *yes* is selected for Distribute All Firmware. This is the default setup for the Distribute Firmware page.

To distribute the firmware components individually, select **no** for Distribute All Firmware, and click the checkboxes for the components you want to distribute.

Step 3 Click **Start**. The access point's firmware is distributed to the access points on your network. To cancel the distribution, click **Abort**.

When the distribution is complete, the access points that received the firmware automatically reboot.

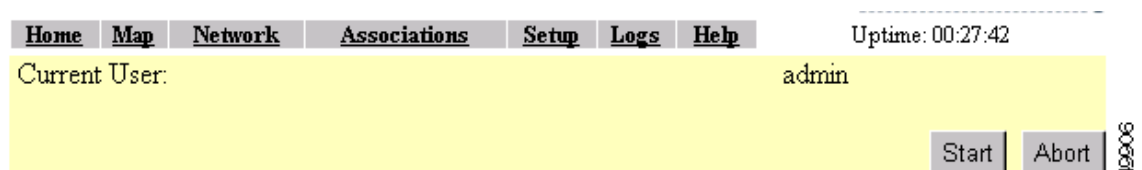
Distributing a Configuration

Use the Distribute Configuration page to distribute the access point's configuration to other Cisco Aironet access points. [Figure 10-8](#) shows the Distribute Configuration page.

The access point sends its entire system configuration except for its IP identity information and its User List. The configuration is sent and applied to all the access points on your network that:

- Are running access point firmware version 10.00 or newer
- Can detect the IP multicast query issued by the distributing access point (network devices such as routers can block multicast messages)
- Have their web servers enabled for external browsing (see the “[Entering Web Server Settings and Setting Up Access Point Help](#)” section on page 7-7)
- Have the same HTTP port setting as the distributing access point (the HTTP port setting is on the Web Server Setup page)
- Have a Default Gateway setting other than the default setting, which is 255.255.255.255 (the Default Gateway setting is on the Express Setup and Routing Setup pages)
- If they have User Manager enabled, contain in their User Lists a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing access point)

Figure 10-8 Distribute Configuration Page



Follow this link path in the browser interface to reach the Distribute Configuration page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Distribute Configuration to other Cisco Devices**.

Follow these steps to distribute the access point's configuration to other access points:

-
- Step 1** Follow the link path to reach the Distribute Configuration page.
 - Step 2** Click **Start**. The access point's configuration, except for its IP identity and its User List, is distributed to the access points on your network. To cancel the distribution, click **Abort**.
-

Limiting Distributions

You might need to distribute a configuration or firmware to certain access points but not to others. For example, if you distribute a configuration to several access points that use non-overlapping channels, the distributed configuration overwrites the channel settings and puts all the access points on the same channel. In this example, after the distribution you have to reconfigure all the access points to set up non-overlapping channels.

The simplest way to limit the distribution of a configuration or firmware is to create a unique user in the distributing and receiving access points' user management systems. An access point accepts distributed firmware and configurations only if its user manager contains a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing access point).

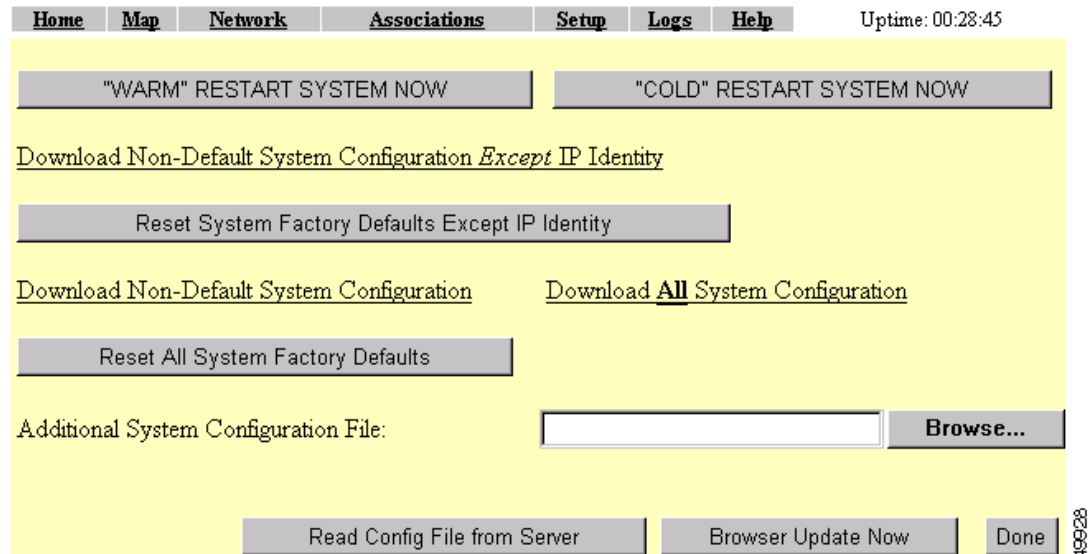
Follow these steps to limit distributions:

-
- Step 1** On the distributing access point, browse to the Security Setup page and create a new user, and then enable user manager protection. See the [“Creating a List of Authorized Management System Users” section on page 8-33](#) section for complete instructions on creating a new user.
 - Step 2** Create the same user with the same password and capabilities on each access point that should receive the distributed firmware or configuration. Make sure user manager protection is enabled on the access points.
 - Step 3** Log into the distributing access point using the new user name and perform the distribution. Only access points with matching users in their user manager systems receive the distribution.
-

Downloading, Uploading, and Resetting the Configuration

You use the System Configuration Setup page to download the current access point configuration to a local drive, upload a configuration from a local drive or file server, and reset the configuration to default settings. You can also use the System Configuration Setup page to restart the access point. [Figure 10-9](#) shows the System Configuration Setup page.

Figure 10-9 System Configuration Setup Page



Follow this link path in the browser interface to reach the System Configuration Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Manage System Configuration**.

Downloading the Current Configuration

Follow these steps to download the access point's current configuration to your hard drive or to a mapped network drive:

-
- Step 1** Follow the link path to the System Configuration Setup page.
- Step 2** If your web browser is Microsoft Windows Internet Explorer, use the download configuration links to save the configuration file:
- Click **Download System Configuration Except IP Identity** to save an .ini file containing the current configuration except for the access point's IP address.
 - To save the current non-default configuration including the access point's IP address, click **Download Non-Default System Configuration**.
 - To save the current default and non-default configuration including the access point's IP address, click **Download All System Configuration**.
- If your web browser is Netscape Communicator, use your right mouse button to click the download configuration links and select **Save link as** in the pop-up menu. If you click the links with your left mouse button, Netscape Communicator displays the text file but does not open the Save as window.
- Step 3** When the Save as window appears, select the drive and directory where you want to save the file, and provide a filename for the configuration file. Click **Save**.
-

Uploading a Configuration

You can upload a configuration file to the access point from your hard drive or a mapped network drive, or you can upload a configuration from a file server.

Uploading from a Local Drive

Follow these steps to upload a configuration file from your hard drive or a mapped network drive:

-
- Step 1** Follow the link path in the browser interface to reach the System Configuration Setup page.
- Step 2** If you know the exact path and filename of the configuration file, type it in the Additional System Configuration File entry field.
- If you aren't sure of the exact path to the configuration file, click **Browse...** next to the entry field. When the File Upload window appears, go to the directory that contains the configuration file and select the file. Click **Open**.
- Step 3** When the filename appears in the Additional System Configuration File entry field, click **Browser Update Now**.
- The configuration file is loaded and applied in the access point.
-

Uploading from a File Server

Follow these steps to upload a configuration file from a file server:

-
- Step 1** Before you load a configuration file from a server, you need to enter FTP settings for the server. If you have already entered the FTP settings, skip to [Step 3](#).
- Follow this link path in the browser interface to reach the FTP Setup page:
- On the Summary Status page, click **Setup**
 - On the Setup page, click **FTP**
- The FTP Setup page appears. [Figure 10-10](#) shows the FTP Setup page.

Figure 10-10 FTP Setup Page

Map Help Uptime: 02:37:33

File Transfer Protocol: FTP

Default File Server:

FTP Directory:

FTP User Name: anonymous

FTP User Password: *****

Apply OK Cancel Restore Defaults 40018

- Step 2** Enter the FTP settings on the FTP Setup page.
- Select FTP or TFTP from the File Transfer Protocol pull-down menu. FTP (File Transfer Protocol) is the standard protocol that supports transfers of data between local and remote computers. TFTP (Trivial File Transfer Protocol) is a relatively slow, low-security protocol that requires no user name or password.
 - In the Default File Server entry field, enter the IP address of the server where the access point should look for FTP files.
 - In the FTP Directory entry field, enter the directory on the server where FTP files are located.
 - In the FTP User Name entry field, enter the user name assigned to the FTP server. If you selected TFTP, you can leave this field blank.
 - In the FTP Password entry field, enter the password associated with the user name. If you selected TFTP, you can leave this field blank.
 - Click **OK**. You return automatically to the Setup page.
- Step 3** Follow the link path in the web browser to reach the System Configuration Setup page.
- Step 4** Click **Read Config File From Server**. The management system checks the server for several possible configuration filenames while attempting to load the configuration file. If the management system doesn't find the first filename, it continues to the next until it finds the file and loads it. It checks the server for the following names in the following order:
- [system name].ini
 - [IP address].ini
 - [boot file from DHCP/BOOTP server].ini
 - [boot file from DHCP/BOOTP server].ini by TFTP
-

Resetting the Configuration

You can reset the access point configuration to the default settings without resetting the access point's IP identity, or you can reset the configuration to the default settings including the IP identity. If you reset the access point's IP identity, however, you might lose your browser connection to the access point.

Two buttons on the System Configuration Setup page reset the configuration to defaults:

- **Reset System Factory Defaults Except IP Identity**—this button returns all access point settings to their factory defaults *except*:
 - The access point's IP address, subnet mask, default gateway, and boot protocol
 - The users in the User Manager list
 - The SNMP Administrator Community name
- **Reset All System Factory Defaults**—this button returns all access point settings to their factory defaults *except*:
 - The users in the User Manager list
 - The SNMP Administrator Community name



Note To completely reset all access point settings to defaults, follow the steps in the [“Resetting the Configuration” section on page 10-13](#).

Follow these steps to reset the configuration to default settings:

-
- Step 1** Follow the link path to reach the System Configuration Setup page. [Figure 10-9](#) shows the System Configuration Setup page. The link path is listed under [Figure 5-9](#).
- Step 2** Click **Reset System Factory Defaults Except IP Identity** to reset the access point configuration to the default settings without resetting the access point’s IP identity. Click **Reset All System Factory Defaults** to reset the configuration to the default settings including the IP identity.



Note If you reset the access point’s IP identity, you might lose your browser connection to the access point.

Restarting the Access Point

Use the System Configuration Setup page to restart the access point.

- Click **“Warm” Restart System Now** to perform a warm restart of the access point. A warm restart reboots the access point.
- Click **“Cold” Restart System Now** to perform a cold restart of the access point. A cold restart is the equivalent of removing and then reapplying power for the access point.