Read This First

Note
If you purchased a 1242G access point, this quick start guide refers occasionally to an 802.11a radio. However, your 1242G access point does not contain an 802.11a radio; it only contains an 802.11b or 802.11g radio. Please disregard the sections in your quick start guide that refer specifically to an 802.11a radio.

You should review this table and the instructions for opening the top cover. The table contains important information that you need to know so that you can successfully configure your access point.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Cisco (case sensitive)</td>
</tr>
<tr>
<td>Password</td>
<td>Cisco (case sensitive)</td>
</tr>
<tr>
<td>IP address</td>
<td>Determined by DHCP server</td>
</tr>
<tr>
<td>Service Set Identifier (SSID)</td>
<td>See the “Radio and IP Address Configuration” section on page 2.</td>
</tr>
</tbody>
</table>
Radio and IP Address Configuration

The access point ships with its radio disabled and no assigned IP address or service set identifier (SSID). You must enable them when you configure the access point for the first time. The access point no longer is assigned an IP address. It is configured to obtain an IP address by using a DHCP server. If your network does not use a DHCP server, you must connect to the access point console port and assign a static IP address (See the “Assigning an IP Address Using the CLI” section on page 20.

<table>
<thead>
<tr>
<th>Status LED</th>
<th>Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Normal operating condition and at least one wireless client device is associated with the access point.</td>
</tr>
<tr>
<td>Light green</td>
<td>Normal operating condition, but no wireless client devices are associated with the access point.</td>
</tr>
<tr>
<td>Amber or red</td>
<td>Error condition. See the “Checking the Access Point LEDs” section on page 42.</td>
</tr>
</tbody>
</table>
Before You Start

Before you install the access point, make sure that you are using a computer connected to the same network as the access point, and obtain the following from your network administrator:

- A host name for the access point
- The case-sensitive SSID for your radio 802.11g and 802.11a radio networks
- A Simple Network Management Protocol (SNMP) community name and the SNMP file attribute (if SNMP is in use)
- The Media Access Control (MAC) address from the label on the bottom of the access point (such as 0016462584c), if you plan to use the Cisco IP Setup Utility to find an access point IP address.
- If you are not connected to a DHCP server, you can assign an IP address to the access point using the CLI. In this situation, obtain a unique IP address for your access point, a default gateway, and subnet mask from your network system administrator.
Safety Information

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper installation of this radio according to the instructions found in this manual will result in user exposure that is substantially below the FCC recommended limits.

- Do not hold any component containing a radio so that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.

Warnings

Translated versions of the following safety warnings are provided in Appendix A of the Cisco Aironet 1240AG Series Access Point Hardware Installation Guide.
Warning
Read the installation instructions before you connect the system to its power source. Statement 1004

Warning
This product must be connected to a power-over-ethernet (PoE) IEEE 802.3af compliant power source or an IEC60950 compliant limited power source. Statement 353

Warning
This product relies on the building’s installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 20A Statement 1005

Warning
Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use. Statement 245B
Overview

This guide is designed to help you minimally configure a Cisco Aironet 1240AG Series Access Point by using its GUI through your web browser. The GUI is the primary configuration tool. Configuration can also be performed by using the command-line interface (CLI). For instructions on using the CLI, see the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points.*
Configuring your access point by using Cisco’s Structured Wireless-Aware Network (SWAN) or Cisco’s Wireless LAN Solution Engine (WLSE) is not covered in this guide. Refer to the appropriate SWAN or WLSE documentation for configuration information. These documents are also available on Cisco.com.
This table lists documents related to the 1240AG series access point.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performing an advanced configuration</td>
<td><em>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points</em></td>
</tr>
<tr>
<td></td>
<td><em>Cisco Aironet Command Reference for Cisco Aironet Access Points and Bridges</em></td>
</tr>
<tr>
<td>Mounting the access point</td>
<td><em>Cisco Aironet 1240AG Series Access Point Hardware Installation Guide</em></td>
</tr>
<tr>
<td>System requirements, important notes, limitations, and last-minute updates</td>
<td><em>Release Notes for Cisco Aironet 1240AG Series Access Points for Cisco IOS Release 12.3(7)JA (or later)</em></td>
</tr>
</tbody>
</table>

These documents are on Cisco.com at the following URL:

Unpacking the Access Point

Follow these steps to unpack the access point:

1. Open the shipping container and carefully remove the contents.
2. Return all packing materials to the shipping container and save it.
3. Ensure that all items listed in the Package Contents section are included in the shipment. Check each item for damage. If any item is damaged or missing, notify your authorized Cisco sales representative.

Package Contents

Each access point package contains the following items:

• Cisco Aironet 1240AG Series Access Point
• Cisco Aironet 1240AG Series Power Module (universal power module)—optional
• Mounting hardware kit
• One mounting plate
  – Cable security bracket
  – Two suspended ceiling T-rail clips (accommodates standard and recessed T-rails)
  – One security hasp
  – Four 6 x 32 x ½ in. pan head Phillips machine screws
  – One 8 x 18 x ¾ in. pan head Phillips sheet metal screws
  – 2 #8 plastic wall anchors
  – One 10 x 24 nut (for ground stud on mounting bracket)
  – Four rubber foot pads
  – Two cable tie wraps

• Quick Start Guide: Cisco Aironet 1240AG Series Access Point
• Safety Warnings for Cisco Aironet 1240AG Series Access Points
• Cisco product registration and Cisco documentation feedback cards

The following illustrations show the access point with its external antennas connected.
Note

The 2.4-GHz and 5-GHz antennas pictured here are not supplied with the access point. Antennas must be ordered separately.
This illustration shows the connections and components on the 2.4-GHz end of the access point.

<table>
<thead>
<tr>
<th></th>
<th>2.4-Ghz antenna connector (left)</th>
<th></th>
<th>Console port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.4-Ghz antenna connector (left)</td>
<td>6</td>
<td>Console port</td>
</tr>
<tr>
<td>2</td>
<td>Ethernet status LED</td>
<td>7</td>
<td>Ethernet port</td>
</tr>
<tr>
<td>3</td>
<td>Radio status LED</td>
<td>8</td>
<td>48 VDC power port</td>
</tr>
<tr>
<td>4</td>
<td>Status LED</td>
<td>9</td>
<td>2.4-GHz antenna connector (right/primary)</td>
</tr>
<tr>
<td>5</td>
<td>Mode switch</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This illustration shows the connectors and components on the 5-GHz end of the access point.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5-GHz antenna connector (left)</td>
</tr>
<tr>
<td>2</td>
<td>5-GHz antenna connector (right/primary)</td>
</tr>
<tr>
<td>3</td>
<td>Security lock keyhole</td>
</tr>
</tbody>
</table>
Installation Summary

Installing the access point involves these operations:

- Mounting the access point
- Connecting power
- Obtaining and assigning an IP address
- Configuring power
- Configuring basic settings
- Enabling the radio interfaces
- Configuring security settings

Mounting the Access Point

Detailed mounting instructions are in the *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*. This document is available on Cisco.com at the following URL:

Connecting Power

The access point can be powered locally by using the AC power module or over Ethernet using power sourcing equipment (PSE). The following illustration shows the power options for the access point.
Warning

This product must be connected to a Power over Ethernet (PoE) IEEE 802.3af compliant power source or an IEC60950 compliant limited power source. Statement 353

The access point power options:

- **Option 1**—Switches with sufficient inline power:
  - An inline power capable switch, such as the Catalyst 3550 PWR XL, 3560-48PS, 3750-48PS, 4500 with 802.3af Power over Ethernet module, or the 6500 with 802.3af Power over Ethernet module
  - Other inline power switches supporting the IEEE 802.af inline power standard

- **Option 2**—Switches without sufficient inline power can use the power injector:
  - Cisco Aironet Power Injector (AIR-PWRINJ3 or AIR-PWRINJ-FIB)

- **Option 3**—Local power using a power module
Note

Some older switches and patch panels might not provide enough power to operate the access point. At power on, if the access point is unable to determine that the power source can supply sufficient power, the access point automatically deactivates both radios to prevent an over-current condition. The access point also activates a Status LED low power error indication and creates an error log entry. See the *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide* for more information.

When power is applied to the access point, it begins a routine power-up sequence that you can monitor by observing the three LEDs on the 2.4-GHz end of the access point. After all three LEDs turn green to show the starting of the Cisco IOS operating system, the Status LED blinks green to show that Cisco IOS is operational. When in an operational status, the Ethernet LED is steady green when no traffic is being passed and off when traffic is being passed. The sequence takes about 1 minute to complete. Refer to the “Checking the Access Point LEDs” section on page 42 for LED descriptions.

When the sequence is complete, you are ready to obtain the access point IP address and perform an initial configuration. Refer to “Configuring Basic Settings” section on page 25 for instructions on assigning basic settings to the access point.
If your access point is connected to inline power, do not connect the power module to the access point. Using two power sources on the access point might cause the access point to shut down to protect internal components and might cause the switch to shut down the port to which the access point is connected. If your access point shuts down, you must remove all power and reconnect only a single power source.

### Obtaining and Assigning an IP Address

To browse to the access point Express Setup page, you must either obtain or assign the access point IP address using these methods:

- Assign a static IP address by connecting to its console port and accessing the access point CLI.

- Use a DHCP server (if available) to automatically assign an IP address. You can find out the DHCP-assigned IP address by using one of the following methods:
Connect to the access point console port and use a Cisco IOS command to display the IP address, such as `show interface bvi1`.

Provide your organization’s network administrator with your access point MAC address. Your network administrator will query the DHCP server using the MAC address to identify the IP address. The MAC address is on a label attached to the bottom of the access point.

Use the CLI and serial port to identify the assigned IP address.

## Connecting to the Access Point Locally

If you need to configure the access point locally (without connecting it to a wired LAN), you can connect a PC to its console port by using a DB-9 to RJ-45 serial cable.

**Caution**

Be careful when handling the access point, the bottom plate might be hot.

Follow these steps to open the CLI by connecting to the access point console port:

1. Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 console port on the access point and to the COM port on a computer.
Note
The Cisco part number for the serial cable is AIR-CONCAB1200.

2. Set up a terminal emulator on your PC to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Assigning an IP Address Using the CLI

When you assign an IP address to the access point by using the CLI, you must assign the address to the BVI. Beginning in a privileged EXEC mode, follow these steps to assign an IP address to the access point BVI using the access point console port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>Interface bvi1</code></td>
<td>Enters interface configuration mode for the BVI.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip address address mask</code></td>
<td>Assigns an IP address and subnet mask address to the BVI.</td>
</tr>
</tbody>
</table>
**Note**  
If you are connected to the access point using a Telnet session, you lose your connection to the access point when you assign a new IP address to the BVI. If you need to continue configuring the access point using Telnet, use the new IP address to open another Telnet session to the access point.

**Using a Telnet Session to Access the CLI**

Follow these steps to browse to access the CLI using a Telnet session. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions.

1. Select **Start > Programs > Accessories > Telnet**.
   
   If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

2. When the Telnet window appears, click **Connect** and select **Remote System**.

3. In the Host Name field, type the access point IP address and click **Connect**.
Configuring Power

After connecting the access point to a power source, its status LED might be amber, which can indicate that the access point is unable to verify that the PSE is supplying sufficient power. In such cases, you need to configure settings on the access point or the switch to identify your power source.

Identify your power source and switch condition, and then make sure that your devices are configured as shown in the table on page 19.

Follow these steps to configure the system power settings using the GUI:

1. Open your browser and enter the access point IP address in the address field. A login and password screen appears.
2. Enter the username *Cisco* and password *Cisco*. The username and password are case sensitive.
3. When the access point does not receive enough power for full operations, it is in low power mode. If your access point is in low power mode, a warning message appears indicating that all radios are disabled due to insufficient power. Click **OK** to continue. The System Configuration page appears.
4. Scroll down to the System Power Settings section as shown in the following illustration.
5. Set the power settings and power injector fields, and verify your switch status as shown in the power settings table.

Note
To verify switch status, you need to use the switch CLI. See the Cisco IOS software configuration guide for your switch.

<table>
<thead>
<tr>
<th>Power Source</th>
<th>System Power Settings</th>
<th>Switch Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco PSE supporting Cisco Intelligent Power Management feature¹</td>
<td>Power Settings: Power Negotiation selected</td>
<td>power inline auto</td>
</tr>
<tr>
<td></td>
<td>Power Injector: Unchecked</td>
<td></td>
</tr>
<tr>
<td>Cisco PSE not supporting Cisco Intelligent Power Management feature¹</td>
<td>Power Settings: Prestandard Compatibility selected</td>
<td>power inline auto</td>
</tr>
<tr>
<td></td>
<td>Power Injector: Unchecked</td>
<td></td>
</tr>
<tr>
<td>Power Source</td>
<td>System Power Settings</td>
<td>Switch Status</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| Cisco Aironet Power Injector with a Cisco PSE supporting Intelligent Power Management feature¹ | Power Settings: Power Negotiation selected  
Power Injector: Unchecked | power inline never                                           |
| Cisco Aironet Power Injector with a Cisco PSE not supporting Cisco Intelligent Power Management feature¹ | Power Settings: Power Negotiation selected  
Power Injector: Checked  
MAC address² | power inline never                                           |
| Cisco Aironet Power Injector with a non-Cisco switch                       | No configuration requirement                                |                    |
| 802.3af-compliant switch that does not support Cisco inline power (non-Cisco switch) | No configuration requirement                                |                    |
| AC power adapter                                                          | No configuration requirement                                |                    |
6. Click **Apply**. The access point reboots configured with the power settings you specified.

Note: You might have to refresh your browser screen to see the current status indicating that the access point radios are enabled.

**Configuring Basic Settings**

Before you can configure basic settings, the access point and your PC needs an IP address. See the “Obtaining and Assigning an IP Address” section on page 18.

Follow these steps to configure basic settings for the access point using the GUI Express Setup page.

1. Open your browser, and enter the access point IP address in the address field. A username and password screen appears.
2. Enter the username *Cisco* and password *Cisco*. The username and password are case sensitive.

3. Press **Enter**. The Summary Status page appears.
4. If required, configure the power settings as described in the previous section. Otherwise, Click **Express Setup**. The Express Setup page appears.
5. Configure the settings using the following sections as a guide.
• Host Name—The host name (or system name) is a name for the access point that identifies it on your network. The system name appears in the titles of the management system pages.

• Configuration Server Protocol—This setting specifies how the access point obtains an IP address.
  – DHCP—IP address is automatically assigned by the network DHCP server.
  – Static IP—The access point uses a static IP address that you enter in the IP address field.

• IP Address—This setting assigns or changes the access point IP address. If DHCP is enabled, the access point obtains its IP address from your network DHCP server. You can assign a static IP address in this field.

• IP Subnet Mask—The IP subnet mask identifies the subnet on which the access point resides. This subnet is provided by your network administrator. If DHCP is enabled, leave this field blank.

• Default Gateway—The default gateway identifies the address the access point uses to access another network. This gateway is provided by your network administrator. If DHCP is enabled, leave this field blank.
• Web Server—This setting specifies the type of HTTP used to access the access point using a web browser.
  – Standard (HTTP)—Standard protocol used to transfer HTML using unencrypted traffic between web browsers.
  – Secure (HTTPS)—Protocol used to transfer secure data by using encrypted traffic to and from the user by means of a Secure Socket Layer (SSL).

• SNMP Community—The SNMP Community setting identifies and sets attributes for the Simple Network Management Protocol (SNMP) used to manage the network on which the access point resides.
  – Read-Only—Access point allows only SNMP read access.
  – Read-Write—Access point allows read and write access.

Note

The following radio settings must be applied separately to each radio: Radio0—802.11G and Radio1—802.11A.

• Role in Radio Network—Determines what function the access point performs in the wireless network.
  – Access Point—Specifies that the unit operates as an access point connected to the main Ethernet LAN network. In this mode, wireless clients associate to the access point.
– **Repeater**—Specifies that the unit operates as a repeater access point not connected to Ethernet LAN. In this mode, wireless clients associate to the access point.

– **Root Bridge**—Specifies that the unit operates as a root bridge and connects directly to the main Ethernet LAN. In this mode, the unit accepts associations from other Cisco Aironet non-root bridges and wireless client devices.

– **Non-Root Bridge**—Specifies that the unit operates as a nonroot bridge and connects to a remote LAN. In this mode, the unit must associate with a Cisco Aironet root bridge using the wireless interface. The nonroot bridge can support wireless client devices.

– **Workgroup Bridge**—Specifies that the unit operates as a workgroup bridge connected to a small wired Ethernet LAN network through an Ethernet hub or switch. The workgroup bridge must associate to a Cisco Aironet access point or bridge.

– **Scanner**—Specifies that the unit is configured by a Cisco WLSE and operates as a scanner and reports network traffic to the Cisco WLSE.

- **Optimize Radio Network For**—Optimizes the access point radio performance in the wireless network by adjusting data rates. This setting must match the setting on the clients.

  – **Throughput**—Maximizes data volume handled by the access point but might reduce its range.
– Range—Maximizes the access point range but might reduce throughput.

– Default—The access point uses its default data rate settings for the radio selected.

– Custom—The access point uses settings that you enter on the radio settings page. Clicking **Custom** takes you to the radio settings page.

- Aironet Extensions—By default, the access point uses Cisco Aironet 802.11 extensions to detect the capabilities of Cisco Aironet client devices and to support features that require specific interaction between the access point and associated client devices. Aironet extensions must be enabled to support features such as load balancing, Message Integrity Check (MIC), Temporal Key Integrity Check (TKIP), Repeater Mode, and World Mode. Disabling Aironet Extensions disables the features mentioned above, but it sometimes improves the ability of non-Cisco client devices to associate to the access point.
## Default Settings on the Express Setup Page

The following table lists the default settings on the Express Setup page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>ap</td>
</tr>
<tr>
<td>Configuration Server Protocol</td>
<td>DHCP</td>
</tr>
<tr>
<td>IP Address</td>
<td>Assigned by DHCP</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The access point does not have a default IP address.</td>
</tr>
<tr>
<td>IP Subnet Mask</td>
<td>Assigned by DHCP</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Assigned by DHCP</td>
</tr>
<tr>
<td>Role in Radio Network</td>
<td>Access point</td>
</tr>
<tr>
<td>Web Server</td>
<td>Standard (HTTP)</td>
</tr>
<tr>
<td>SNMP Community</td>
<td>default Community</td>
</tr>
<tr>
<td>Optimize Radio Network for</td>
<td>Throughput</td>
</tr>
<tr>
<td>Aironet Extensions</td>
<td>Enable</td>
</tr>
</tbody>
</table>
You can restore the access point to its factory defaults by unplugging the power jack and plugging it back in while holding the Mode button down until the Ethernet LED turns amber (approximately 2 to 3 seconds).

### Enabling the Radio Interfaces

In Cisco IOS Release 12.3(7)JA, the access point radios are disabled by default, and there is no default SSID. You must create an SSID and enable the radios before the access point allows wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points. Refer to the "Configuring Security Settings" section on page 33 for instructions on configuring the SSID.

Follow these steps to enable the radio interfaces:

1. Browse to your access point.

2. When the Summary Status page appears, click **Radio0-802.11G**. The 2.4-GHz radio status page appears.

3. Choose the **Settings** tab at the top of the page. The radio settings page appears.

4. Click **Enable** in the Enable Radio field.
5. Click **Apply**.

6. Click **Radio1-802.11A**. The 5-GHz radio status page appears.

7. Repeat Steps 3 to 5.

8. Close your web browser.

---

**Configuring Security Settings**

After you assign basic settings to your access point, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the access point can communicate beyond the physical boundaries of your work site.

Just as you use the Express Setup page to assign basic settings, you can use the Express Security page to create unique SSIDs and assign one of four security types to them. For detailed security information, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

---

**Configuring Basic Security Settings**

You can use the Express Security page to create unique SSIDs and assign one of four security types to them. This illustration shows the Express Security page.
### Express Security Set Up

#### SSID Configuration

1. **SSID**
   - [ ] Broadcast SSID in Beacon

2. **VLAN**
   - [ ] No VLAN
   - [ ] Enable VLAN ID: [ ] (1-4095)
   - [ ] Native VLAN

3. **Security**
   - [ ] No Security
   - [ ] Static WEP Key
     - Key 1: [ ] 128 bit
   - [ ] EAP Authentication
     - RADIUS Server: [ ] (Hostname or IP Address)
     - RADIUS Server Secret: [ ]
   - [ ] WPA
     - RADIUS Server: [ ] (Hostname or IP Address)
     - RADIUS Server Secret: [ ]

#### SSID Table

<table>
<thead>
<tr>
<th>SSID</th>
<th>VLAN</th>
<th>Encryption</th>
<th>Authentication</th>
<th>Key Management</th>
<th>Native VLAN</th>
<th>Broadcast SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Understanding Express Security Settings

When the access point configuration is set to factory defaults, the first SSID that you create by using the Express Security page overwrites the default SSID, which has no security settings. The SSIDs that you create appear in the SSID table at the bottom of the page. You can create up to 16 SSIDs on the access point.

Using VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs by using any of the four security settings on the Express Security page. However, if you do not use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because of the limited Express Security page encryption options. Without VLANs, encryption settings (WEP and ciphers) apply to an interface, such as the radio, and you cannot use more than one encryption setting on an interface. For example, when you create an SSID with static WEP with VLANs disabled, you cannot create additional SSIDs with WPA authentication because they use different encryption settings. If you find that the security setting for an SSID conflicts with another SSID, you can delete one or more SSIDs to eliminate the conflict.

If any VLANs are defined on the access point, the trunk port on the switch must be limited to allow only the VLANs defined on the access point.
Express Security Types

There are four security types you can assign to an SSID:

- **No security**—The least secure option. Use this option only for SSIDs used in a public space, and assign it to a VLAN that restricts access to your network.

- **Static WEP Key**—More secure than no security. Static WEP keys are vulnerable to attack. There are two different lengths for WEP keys: 40-bit and 128-bit (hexadecimal or ASCII characters). Cisco access points use hexadecimal characters. Client adapters can use either, depending on how the vendor chooses to configure them.

- **EAP Authentication**—Enables 802.1x authentication. Requires an IP address and shared secret from an authentication server on your network (server authentication port 1645). You do not need to enter a WEP key.

- **WPA**—Wi-Fi Protected Access (WPA) permits wireless access to users authenticated against a database through the services of an authentication server and encrypts their IP traffic with stronger algorithms than those used in WEP. As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).
Express Security Limitations

Because the Express Security page is designed for simple configuration of basic security, the options available are a subset of the access point security capabilities. Keep these limitations in mind when using the Express Security page:

- You cannot edit SSIDs. However, you can delete SSIDs and recreate them.
- You cannot assign SSIDs to specific radio interfaces. The SSIDs that you create are enabled on all radio interfaces. To assign SSIDs to specific radio interfaces, choose Security > SSID Manager.
- You cannot configure multiple authentication servers. To configure multiple authentication servers, click Security > Server Manager.
- You cannot configure multiple WEP keys. To configure multiple WEP keys, click Security > Encryption Manager.
- You cannot assign an SSID to a VLAN that is already configured on the access point. To assign an SSID to an existing VLAN, choose Security > SSID Manager.
- You cannot configure combinations of authentication types on the same SSID (such as MAC address authentication and EAP authentication). To configure combinations of authentication types, choose Security > SSID Manager.
Using the Express Security Page

Follow these steps to create an SSID using the Express Security page:

1. Type the SSID in the SSID entry field. The SSID can contain up to 32 alphanumeric characters.

   **Note**  
   These characters are not allowed in the SSID: +, ], /, “, TAB, and trailing SPACE.

2. To broadcast the SSID in the access point beacon, check the Broadcast SSID in Beacon check box.

   **Note**  
   When you broadcast the SSID, devices that do not specify an SSID can associate to the access point. This is a useful option for an SSID used by guests or client devices in public space. If you do not broadcast the SSID, client devices cannot associate to the access point unless their SSID matches this SSID, so only one SSID can be included in the access point beacon.

3. (Optional) Check the Enable VLAN ID check box and enter a VLAN number (1 through 4095) to assign the SSID to a VLAN. You cannot assign an SSID to an existing VLAN.
4. (Optional) Check the Native VLAN check box to mark the VLAN as the native VLAN.

5. Select the security setting for the SSID. The settings are listed in order of their robustness, from No Security to WPA, which is the most secure setting.

If you select Static WEP Key, choose the key number and encryption size and enter the encryption key (10 hexadecimal characters for 40-bit keys or 26 hexadecimal characters for 128-bit keys.

If you select EAP Authentication or WPA, enter the IP address and shared secret for the authentication server on your network.

Note If you do not use VLANS on your wireless LAN, the security options that you can assign to multiple SSIDs are limited. Refer to the Cisco IOS Software Configuration Guide for Cisco Aironet Access Points for VLAN details.

6. Click Apply. The SSID appears in the SSID table at the bottom of the page.
In Case of Difficulty

If you followed the instructions in previous sections of this guide, you should have had no trouble getting your access point installed and running. If you do experience difficulty, the following sections provide basic troubleshooting information.

Before contacting Cisco, look for a solution to your problem in this guide or the troubleshooting chapter of the *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*.

Follow this link to access Cisco Technical Support:


Checking the Access Point LEDs

If your access point is not working properly, check the Status LED on the 2.4-GHz end of the access point. You can use the LED colors to assess the unit status.

The LED meanings are in this table.
Regarding LED status colors, it is expected that there will be small variations in color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer’s specifications and is not a defect.

<table>
<thead>
<tr>
<th>Status LED</th>
<th>Ethernet LED</th>
<th>Radio LED</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>—</td>
<td>—</td>
<td>Normal operating condition; at least one wireless device associated.</td>
</tr>
<tr>
<td>Light green</td>
<td>—</td>
<td>—</td>
<td>Normal operating condition; no wireless device associated.</td>
</tr>
<tr>
<td></td>
<td>Blinking green</td>
<td>—</td>
<td>Sending or receiving Ethernet packets.</td>
</tr>
<tr>
<td></td>
<td>—</td>
<td>Blinking green</td>
<td>Sending or receiving radio packets.</td>
</tr>
<tr>
<td>Blinking dark blue</td>
<td>Green or blinking green</td>
<td>Blinking green or off</td>
<td>Software upgrade in progress.</td>
</tr>
<tr>
<td>Status LED</td>
<td>Ethernet LED</td>
<td>Radio LED</td>
<td>Meaning</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>-----------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Amber</td>
<td>Various</td>
<td>Various</td>
<td>Cisco IOS errors</td>
</tr>
<tr>
<td>Blinking red</td>
<td>Various</td>
<td>Various</td>
<td>Boot loader errors</td>
</tr>
</tbody>
</table>

For more details on these LED status codes, see the “Troubleshooting” chapter of the *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*.

**Checking Basic Settings**

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the access point does not communicate with client devices, check the following areas.

**SSID**

Wireless clients attempting to associate with the access point must use the same SSID as the access point. If a client device SSID does not match the SSID of an access point in radio range, the client device will not associate.
WEP Keys

The WEP keys that you use to transmit data must be set up exactly the same on your access point and any wireless devices with which it associates. For example, if you set WEP Key 3 on your client adapter to 0987654321 and select it as the transmit key, you must also set the same value for WEP Key 3 on the access point. However, the access point does not need to use WEP Key 3 as the transmit key.

Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on setting the access point WEP keys.

Security Settings

Wireless devices attempting to authenticate with your access point must support the same security options configured on the access point, such as EAP or LEAP, MAC address authentication, Message Integrity Check (MIC) WEP key hashing, and IEEE 802.1X versions.

If a wireless client cannot authenticate with your access point, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the access point settings.
Resetting to Default Configuration

If you forget your password that allows you to configure the access point, you might need to completely reset the configuration. You can use the MODE button on the access point to reset the configuration.

Note

These steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

Using the MODE Button

Follow these steps to delete the current configuration and return all access point settings to the factory defaults by using the MODE button:

1. Disconnect power from the access point (the power jack for external power or the Ethernet cable for in-line power).
2. Press and hold the MODE button while you reconnect power to the access point.
3. Continue pressing the MODE button until the Ethernet LED turns amber. (approximately 2 to 3 seconds). Then release the button.
4. After the access point reboots, you must reconfigure it using the web browser interface, the Telnet interface, or the access point console port.
Using the Web Browser Interface

Follow these steps to delete the current configuration and return all access point settings to factory defaults using the web browser interface:

1. Open your Internet browser. You must use Microsoft Explorer (version 5.x or later) or Netscape Navigator (version 4.x or later).

2. Enter the access point IP address in the browser address line, and press Enter. An Enter Network Password screen appears.

3. Enter the username Cisco in the User Name field.

4. Enter the password Cisco in the Password field and press Enter. The Summary Status page appears.

5. Click System Software. The System Software screen appears.

6. Click System Configuration. The System Configuration screen appears.

7. Click the Reset to Defaults button.

Note

If the access point is configured with a static IP address, the IP address does not change.

After the access point reboots, you must reconfigure it.
Compliance Information

This equipment has been tested and found to comply with the European Telecommunications Standard ETS 300.328. This standard covers Wideband Data Transmission Systems referred to in CEPT recommendation T/R 10.01.

This type-accepted equipment is designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed in accordance with the instruction manual, may cause harmful interference to radio communications.

The Declarations of Compliance for this product relevant to the European Union and other countries following EU Directive 1999/5/EC (R&TTE Directive) can be found in the Cisco Aironet 1240AG Series Access Point Hardware Installation Guide. This guide is available on Cisco.com.