ProCurve
Networking by HP

Installation and Configuration Guide

ProCurve Wireless Access Point 10ag

PoE

Power over Ethernet Devices

www.procurve.com

hp invent

ProCurve Wireless Access Point 10ag

Installation and Configuration Guide

Publication Number

5991-8615
May 2008

Applicable Products

ProCurve Wireless Access Point 10ag NA	(J9140A)
ProCurve Wireless Access Point 10ag WW	(J9141A)

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Open Source Software Acknowledgement

This software incorporates open source components that are governed by the GNU General Public License (GPL). In accordance with this license, ProCurve Networking will make available a complete, machine readable copy of the source code components covered by the GNU GPL upon receipt of a written request. Send a request to:

Hewlett-Packard Company, L.P.
ProCurve Access Point 10ag
GNU GPL Source Code
Attn: ProCurve Networking Support
MS: 5551
Roseville, CA 95747 USA

Safety

Before installing and operating these products, please read the "Installation Precautions" in Chapter 2 and "Safety Information" in Appendix C.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5552
Roseville, California 95747-5552
http://www.procurve.com

Contents

3 Getting Started With Access Point Configuration

4 Setting Up the Access Point

5 Managing the Access Point

6 Troubleshooting

A Specifications

B Access Point Port and Network Cables

C Safety and EMC Regulatory Statements

D Recycle Statements

E Open Source Licenses

Index

1

Introducing the ProCurve Wireless Access Point 10ag

The ProCurve Wireless Access Point 10ag is a dual-radio 802.11a and 802.11b/g access point that offers maximum flexibility in deployment and optimum throughput for high-density usage areas. Designed for small business networking environments, it provides high-speed, reliable wireless networking and comprehensive security and management features.

ProCurve Wireless Access Point 10ag NA (J9140A)
ProCurve Wireless Access Point 10ag WW (J9141A)

The Access Point 10ag has one 10/100Base-TX RJ-45 port. This port also supports Power over Ethernet (PoE) based on the IEEE 802.3af standard. The access point supports wireless connectivity at speeds up to 54 Mbps based on the IEEE 802.11a and IEEE 802.11g standards. It is designed to be used primarily for connecting wireless clients and devices to a wired primary network.

This chapter describes the Access Point 10ag, including:

- Package Contents
- Front of the Access Point
- Back of the Access Point
- Access Point Features

Throughout this manual, the ProCurve Access Point 10ag will be referred to as the ‘access point’.

Package Contents

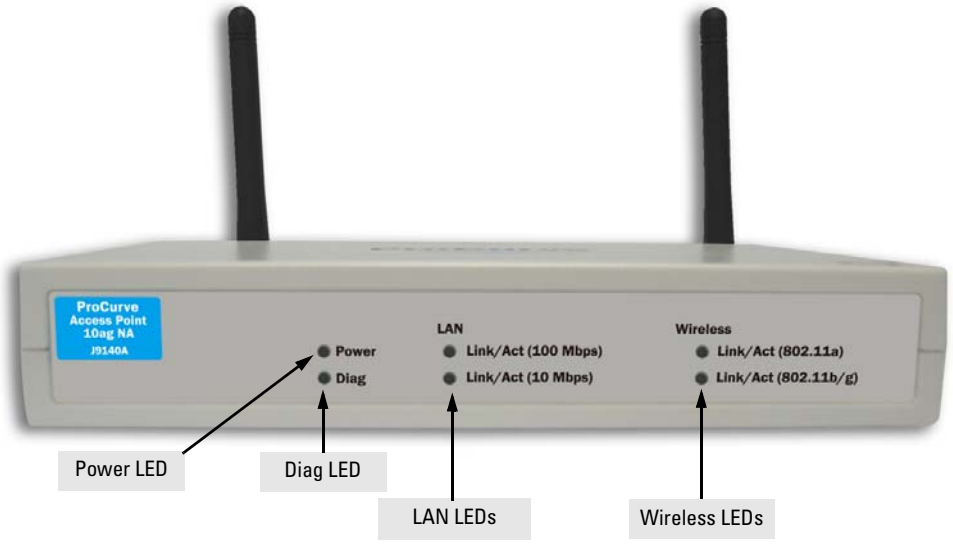
Before installing and using the access point, verify that the package you received is complete. A complete Access Point 10ag package includes the following items:

- *ProCurve Product Documentation CD-ROM*
  (contains PDF file copies of the documentation for the Access Point 10ag, including this *Installation and Configuration Guide*)
- *Read Me First*
- Ethernet cable
- AC power adapter

If any of the above items are damaged or missing, please contact the vendor from which you purchased the access point.

Front of the Access Point

ProCurve Wireless Access Point 10ag



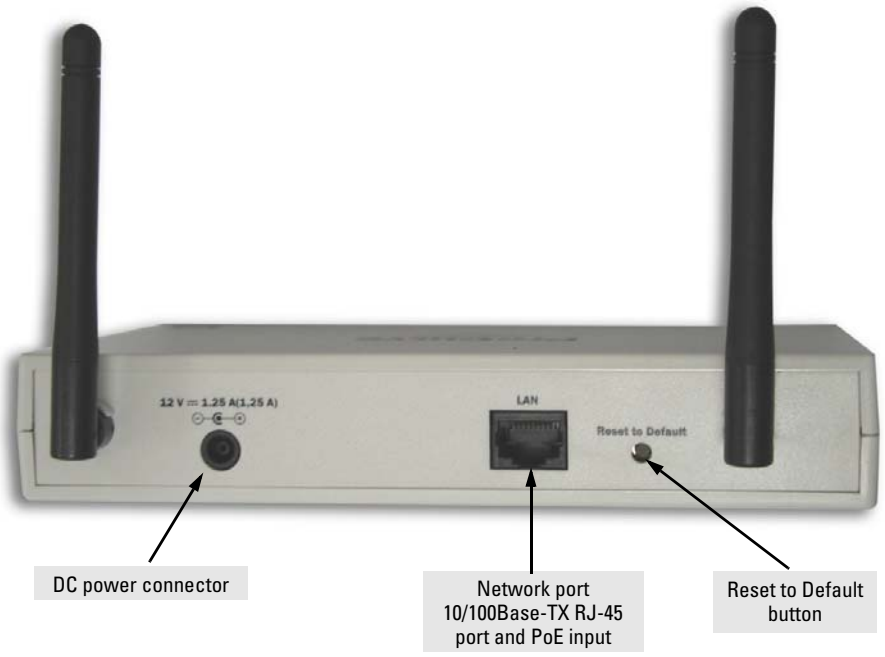
LEDs on the Front Panel

Table 1-1. Access Point LEDs

LED Label	State	Meaning
Power	Green	The access point is receiving power.
	Off	The access point is NOT receiving power. If the power adapter is connected to a power source, verify that the power jack is connected properly to the power connector on the back panel of the access point.
Diag	Blinking amber	Reset to factory default is in progress. Blinking stops when the access point has completed resetting to factory defaults and is about to reboot. For more information on resetting to factory default using the Reset to Default button, refer to "Restoring Factory Default Configuration" on page 6-6.
	Off	Normal state
LAN	Off	The RJ-45 port has no network cable connected, or is not receiving a link signal.
	Blinking or solid green	The RJ-45 port has a link indication from a 10 Mbps or 100 Mbps device and is transmitting or receiving traffic. The LED blinking rate is proportional to the traffic rate. If there is no traffic, the blinking rate will be once every five seconds. As the traffic rate increases, the blinking rate also increases until the LED is solid on, which indicates there no available bandwidth on the port.
Link/Act (802.11a) Link/Act (802.11b/g)	Blinking slowly	The wireless interface may be disabled. To verify, check the radio status on the Information page. For instructions on enabling the wireless interface, refer to "Configuring Advanced Settings" on page 4-25.
	Blinking fast or solid green	The wireless interface is enabled and transmitting or receiving traffic. The LED blinking rate is proportional to the traffic rate. If there is no traffic, the blinking rate will be once every second. As the traffic rate increases, the blinking rate also increases until the LED is solid green, which indicates there no available bandwidth on the interface.

Back of the Access Point

ProCurve Wireless Access Point 10ag



LAN Port

The access point includes one 10/100Base-TX port. This port uses Auto-MDIX, which means that you can use either a straight-through or a crossover twisted-pair cable to connect the access point to a switch, a hub, or a workstation.

Power Connector

The access point does not have a power switch. If the AC power adapter will be used, the access point is powered on when the AC power adapter is connected to the power connector, and the power adapter is connected to an active AC power source.

The access point's power adapter automatically adjusts to any voltage from 100 to 240 volts and either 50 or 60 Hz. There are no voltage range settings required.

CAUTION

Use only the AC power adapter supplied with the access point. Use of other adapters, including adapters that came with other ProCurve Networking products, may result in damage to the equipment.

The access point may also receive Power over Ethernet (PoE) from a switch or another network device that supplies power over the network cable based on the IEEE 802.3af standard.

Note that if the access point is connected to a PoE source device (through the LAN port) and a local power source (through the AC power adapter) at the same time, PoE will be disabled automatically.

Reset to Default Button

Use the Reset to Default button to reboot the access point or to restore the access point to factory default settings. To reach the button, you will need a pointed object, such as the tip of a ballpoint pen or a straightened paper clip.

- **Reboot the access point:** Rebooting the access point can help clear any temporary error conditions. To reboot the access point, press the Reset to Default button for one to three seconds. All the LEDs will go off (except the Power LED), then after another second, the LEDs will turn on and blink. Note that when the access point is rebooted, any associated wireless client will be disconnected temporarily. Connection will be restored automatically after the access point completes rebooting.

CAUTION

Do NOT press the Reset to Default button for more than five (5) seconds. Doing so will restore all access point settings to factory default.

- **Restore to factory settings:** Restoring the access point to factory settings will clear all configuration changes you have made through the Web interface, including the IP address, access control list, and other settings. Use this function only if you want to completely reconfigure the access point. For detailed information, see Restoring Factory Default Configuration in Chapter 6.

Antennas

The access point includes internal diversity antennas for wireless communications. A diversity antenna system uses two identical antennas to receive and transmit signals, helping to avoid multipath fading effects. When receiving, the access point checks both antennas and selects the one with the strongest signal. When transmitting, it uses the antenna previously selected for receiving. The access point never transmits from both antennas at the same time.

Access Point Features

The wireless features of the Access Point 10ag include:

- dual-radio design with IEEE 802.11a and IEEE 802.11b/g radios
- supports up to 54 Mbps data rate on the wireless interface
- supports 10/100Mbps data rate on the Ethernet interface with Auto-MDIX
- supports up to eight (8) Service Set IDentifier (SSID) interfaces
- independent security settings per SSID interface
- supports up to 128 wireless clients and devices
- advanced security through 64-bit and 128-bit WEP encryption, Wi-Fi Protected Access (WPA and WPA2), IEEE 802.1X, remote authentication via a RADIUS server, and MAC address filtering features to protect your sensitive data and authenticate only authorized users to your network
- access control list
- secured authentication of wireless clients through the client's Web browser
- dual power source options, including AC power adapter (included with device) and PoE (IEEE 802.3af)
- reset to factory default parameters

Other basic features of the Access Point 10ag include:

- one 10/100Base-TX RJ-45 port
- full-duplex operation for the 10/100 RJ-45 port
- easy management through a built-in graphical interface that can be accessed from common Web browsers
- RADIUS Accounting for logging user activity on the network
- download of new access point software for software updates
- backing up and restoring of configuration file

Notes

- Transmit power is regulated by international standards and users are forbidden to change its maximum limit.
- The AP10ag is compliant with IEEE 802.11d and will automatically limit the available channels and transmit-power level based on the Country/Region setting. Clients associating with the AP10ag will receive configuration information during the initial handshaking to enable compliant operation in the country/region of use.

Installing the Access Point

This chapter provides information on the requirements for installing the access point and guides you through the steps required for the proper installation of the device.

Topics covered include:

Before You Begin

Before starting with the installation, make sure that you have the required items for the installation ready. In addition, verify that the wireless clients and devices on the network have the required components for wireless communication with the access point.

Installation Requirements

To install the access point, you need the following:

- Access point
- Power adapter (included in the access point package) or PoE switch
- Ethernet cable

If the default IP address **192.168.1.14** is not compatible with your network settings, you will need to change it before you can set up the access point. To change the IP address, you will need to connect a computer with TCP/IP and a 10Mbps or 100Mbps network interface card directly to the access point.

The access point is managed through a browser-based interface. You will need a common Web browser to access the management interface.

The access point may receive power using either the power adapter or Power over Ethernet (PoE) from a switch or other network device that supplies power over the network cable based on the IEEE 802.3af standard. If you want to use PoE to supply power to the access point, you will also need IEEE 802.3af-compliant power sourcing equipment (PSE).

Wireless Client Requirements

For wireless clients and devices on the network to be able to communicate with the access point, they must have at least the following:

- An operating system that supports TCP/IP networking protocols (for example, Windows 2000/XP, UNIX, Mac OS 8.5 or later).
- An 802.11a, 802.11b, or 802.11g wireless network interface card

Safety Information

Before you continue, read Appendix C, "Safety and EMC Regulatory Statements".

Installation Precautions

Follow these precautions when installing the access point:

CAUTION

- Use only the AC power adapter supplied with the access point. Use of other adapters, including adapters that came with other ProCurve Networking products, may result in damage to the equipment.
- You can alternatively power the access point through a network connection to a switch or other network connection device that provides Power over Ethernet. However, note that if the access point is connected to a power source using its AC power adapter, Power over Ethernet is disabled.
- Make sure that the power source circuits are properly grounded, then use the power adapter supplied with the access point to connect it to the power source.
- When using the access point's AC power adapter, note that the AC outlet should be near the access point and should be easily accessible in case the access point must be powered off.
- Ensure that the access point does not overload the power circuits, wiring, and over-current protection. To determine the possibility of overloading the supply circuits, add together the ampere ratings of all devices installed on the same circuit as the access point, and then compare the total with the rating limit for the circuit. The maximum ampere ratings are usually printed on devices near the AC power connectors.
- When using either the AC power adapter or PoE power, do not install the access point in an environment where the operating ambient temperature might exceed 40° C (104° F).
- Make sure airflow around the sides of the access point is not restricted.

Summary of Installation Tasks

Follow these easy steps to install your access point. The rest of this chapter provides details on these steps.

1. **Preconfigure the access point** *(*page 2-5*)*. The access point ships with a default IP address of **192.168.1.14** and a subnet mask of **255.255.255.0**. If this IP address is already assigned to another device on the network or if the IP address settings are not compatible with your network, you will need to configure its IP address before installation.
2. **Prepare the installation site (**page 2-8**).** Make sure that the physical environment into which you will be installing the access point is properly prepared, including having the correct network cabling ready to connect to the access point and having an appropriate location for the access point.
3. **Verify that the access point completes its system initialization (**page 2-10**).** Before deployment, verify correct access point operation. Turn on the access point and observe the LEDs.
4. **Position the access point (**page 2-11**).** The access point can be installed on a flat surface, such as a desktop, or mounted on a wall (wall-mounting hardware is not provided; for mounting hardware, visit your local hardware vendor).
5. **Connect the power to the access point (**page 2-13**).** Once the access point is mounted, plug it into a nearby main power source using the supplied AC adapter, or connect it to a switch that provides Power over Ethernet.
6. **Connect to the network (**page 2-13**).** Using the appropriate network cable, connect the access point to a network port, such as a switch port. If PoE is used, this may have been completed in the prior step.

At this point, your access point is fully installed. See the rest of this chapter if you need detailed information on any of these installation steps.

Installation Procedures

Step 1. Preconfigure the Access Point

In its factory default configuration, the access point is assigned a static IP address of **192.168.1.14** and a subnet mask of **255.255.255.0** (the built-in DHCP client is disabled).

- If your network uses the same IP address class or range, and the IP address **192.168.1.14** is not assigned to any other network device, you do not need to change the IP address settings of your access point. Continue to the next step, "Step 2. Prepare the Installation Site" on page 2-8
- If your network uses a different IP address class or range, you will need to change the IP address settings of the access point so that it can work on your network. Refer to the instructions below.

a. Prepare the Management Computer

You will need to prepare a management computer that you want to use to preconfigure the access point. The management computer must have the following minimum specifications:

- Network interface card with TCP/IP installed
- A common Web browser

Note

The following instructions are for preparing a management computer running Microsoft Windows XP. If your computer is running a different version of Windows, the procedures may be slightly different.

To prepare the management computer:

1. Choose a computer on your local network that you want to use to access and manage the access point.
2. On this computer, click **Start** > **Connect to** > **Show all connections**. The Network Connections window appears.
3. Right-click **Local Area Connection**, and then click **Properties**. The Local Area Connection Properties window appears.
4. Click **Internet Protocol (IP)**, and then click **Properties**.

Note

Remember to write down your computer's current IP address settings. You will need to change them back after you configure the IP address settings of the access point.

5. On the General tab of the Internet Protocol (IP) Properties window, click **Use the following IP address**.
6. In **IP address**, type an IP address that is on the same range as the default IP address (**192.168.1.14**) of the access point. For example, you can type **192.168.1.123**.
7. In **Subnet mask**, type **255.255.255.0**.
8. Click **OK**.

You are now ready to connect the management computer to the access point.

b. Connect the Management Computer to the Access Point

In this step, you will physically connect the management computer to the access point to prepare for preconfiguration.

1. Connect one end of the Ethernet cable that is supplied with the access point to the LAN port on the management computer.
2. Connect the other end of the Ethernet cable to the LAN port on the back panel of the access point.
3. Connect the supplied power adapter to the power connector on the back of the access point.
4. Connect the other end of the power adapter to a power source.

The LEDs on the front panel of the access point flash as the device boots up. When it has completed booting up, check the LEDs again:

- The Power LED should be green.
- One LAN LED - either Link/Act (100Mbps) or Link/Act (10Mbps) - should be green.

c. Connect to the Web Interface and Change the IP Address

1. Start your Web browser.
2. In the address or location bar, enter **http://192.168.1.14**. The logon dialog box appears.
3. In **User Name**, type **admin**.

4. In **Password**, type **password**. The Web interface appears, showing the Information page.
5. On the menu, click **Basic Settings**.
6. Configure the IP address settings.
   - (Recommended) If you want to assign a fixed IP address to the access point, select **Disable** in DHCP Client, and then enter the IP Address, IP Subnet Mask, and Default Gateway that you want to assign to it. These settings must be compatible with your network to ensure that the access point can communicate with other network devices.
   - If you have a DHCP server on the network and you want the access point to automatically obtain an IP address from the DHCP server, click **Enable** in DHCP Client. You do not have to configure other settings, but you will need to check the DHCP server periodically to determine the IP address that the access point is using.
7. In **Country/Region**, select the country/region where you are operating the access point.

Note

You must select the correct country/region for the location in which you operate the access point, so that it uses only the authorized radio channels for wireless network devices.

8. Click **Apply**.

You have completed configuring your access point's IP address settings so that it can work on your network. Remember to return your computer's IP address settings to its original settings.

Disconnect the access point from the management computer. You are now ready to find a suitable location for the access point and to connect the access point to the network.

Step 2. Prepare the Installation Site

Cabling Infrastructure

Ensure that the cabling infrastructure meets the necessary network specifications. Refer to Table 2-1 for information on the cable type and length. For more information cabling, refer to Appendix B.

Table 2-1. Network Cable to Use With the Access Point

Port Type	Cable Type	Length Limit
	Twisted-Pair Cables	
10/100Base-TX	Category 5, 100-ohm unshielded twisted-pair (UTP)	100 meters **Note:** Since the 10Base-T operation is through the 10/100Base-TX port on the access point, if you ever want to upgrade the ports on other devices to 100Base-TX, it would be best to cable the 10/100Base-TX port on the access point initially with category 5 cable.

Installation Location

Before installing the access point, plan its location and orientation relative to other devices and equipment:

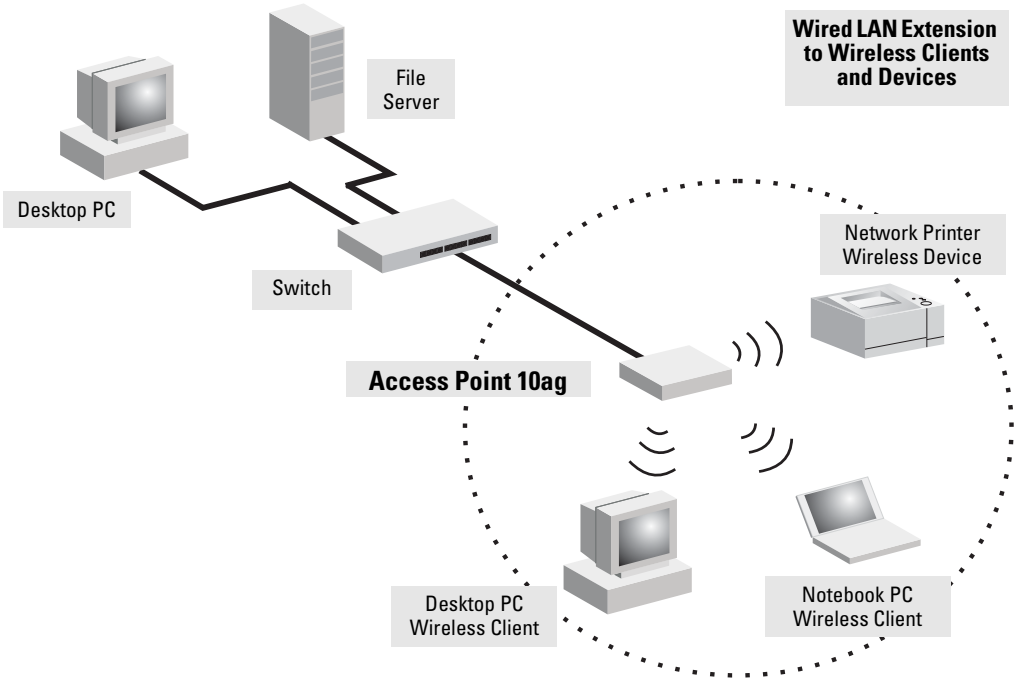
- Try to place the access point in the center of your wireless network. Normally, the higher you place the antennas, the better the performance. You may need to reposition the access point after testing the signal strength on several wireless clients and devices to ensure that the access point's location provides optimal reception throughout the service area.
- Choose a location that allows easy viewing of the front panel LEDs and access to the port and connector on the back panel.
- At the back of the access point, leave at least 7.6 cm (3 inches) of space for the twisted-pair cabling and the power cord.
- On the sides of the access point, leave at least 7.6 cm (3 inches) for cooling.

Network Topology

The Access Point 10ag is designed to provide wireless clients and devices access to a wired LAN. An integrated wired and wireless LAN is called an Infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users and an access point that is directly connected to the wired LAN. Each wireless PC in a BSS can communicate with any computer in its wireless group, or access other computers or network resources in the wired LAN through the access point.

The infrastructure configuration extends the accessibility of wireless PCs to the wired LAN and can be used for access to central network resources, or for connections between mobile workers, as shown in the following figure.

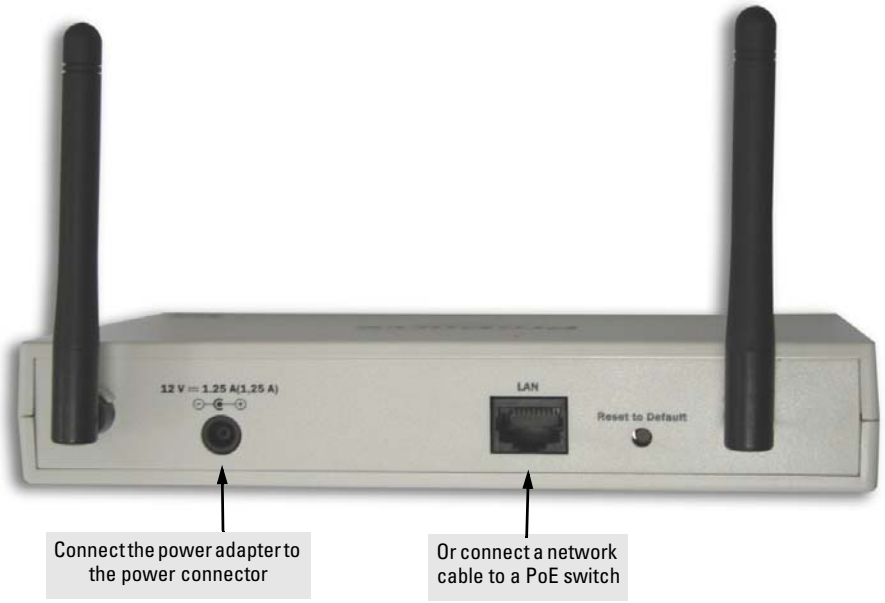
Figure 2-1. Infrastructure Wireless LAN



Step 3. Verify the Access Point Completes Initialization

Before deploying the access point to its network location, you should first verify that it is working properly by plugging in the AC adapter, or connecting it to a switch that provides Power over Ethernet, and verifying that it completes its system initialization.

1. Connect a network cable from a PoE source device (such as a switch) to the RJ-45 port on the back of the access point, or connect the supplied power adapter to the power connector on the back of the access point, and then into a properly grounded electrical outlet.



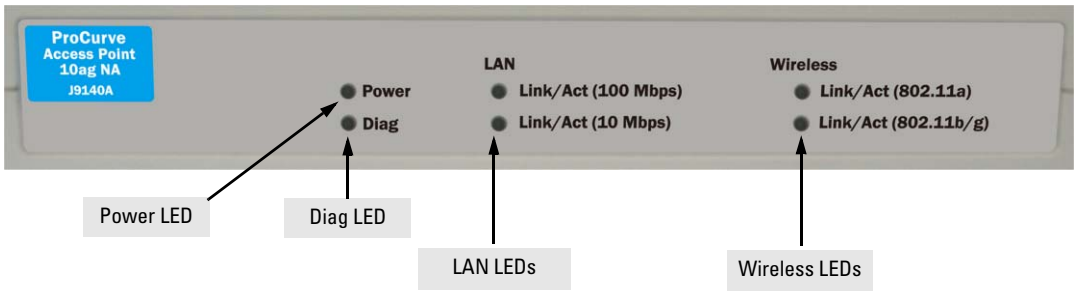
Note

The Access Point 10ag does not have a power switch. It is powered on when the power adapter is connected to the access point and to a power source, or when a network cable is connected to the access point and to a network device that provides Power over Ethernet.

For safety, when connecting to an electrical outlet, the power outlet should be located near the access point.

Use only the AC power adapter supplied with the access point. Use of other adapters, including adapters that came with other ProCurve Networking products, may result in damage to the equipment.

2. Check the LEDs on the access point as described below.



When the access point is powered on, it performs its system initialization. The system initialization takes between 30 seconds and one minute to complete.

LED Behavior

During the system initialization:

- The Power LED first turns on immediately, then both LAN LEDs blink once, then one LAN LED (depending on the speed of the connected device) turns on, and then the two Wireless LEDs turn on and off several times during the initialization phase.
- If RJ-45 port is not connected to any network device (for example, during predeployment), both LAN LEDs remain off before the two Wireless LEDs turn on and off.

When the system initialization completes successfully:

- The **Power** LED remains green.
- The **LAN** and **Wireless** LEDs on the front panel of the access point go into their normal operational mode:
  - If the RJ-45 network port and radio interfaces are connected to active network devices, the LEDs should be blinking at a rate proportional to the traffic rate. If there is no network activity, the LEDs should still be blinking at approximately one-second intervals.
  - If the RJ-45 network port is not connected to an active network device, the LEDs should be off.

If the LED display is different than what is described above, the system initialization has not completed correctly. Refer to Chapter 6, "Troubleshooting" for diagnostic help.

Step 4. Position the Access Point

Unplug the access point from its power source, and then place it in the network location that you have chosen. The access point can be installed on a flat surface (for example, on a desktop) or wall-mounted.

Note

Wall-mounting hardware is not provided. Visit your local hardware store for appropriate hardware. Mounting screws should be round or pan head, #6 or #7, of suitable type and length depending on your wall material and thickness. If necessary, use plastic conical anchors. Place two screws at a distance of 9.7 cm (~3 27/32 inches) apart, center-to-center. About 0.4 cm (~5/32 inch) of space between the wall and the bottom of each screw head is needed to mount the access point.

When deciding where to position the access point, choose a location that:

- Allows easy viewing of the front panel LED indicator lights, and access to the rear panel connectors, if necessary.
- Is centrally located to the wireless computers that will connect to the access point. A good location will optimize wireless connections to computers in both horizontal and vertical directions, allowing wider coverage.

When positioning the access point, ensure:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- There are no thick walls or metal shielding between the access point and the wireless clients and devices. In ideal conditions, the access point has a range of approximately 100 meters. If there are any obstructions between the wireless devices, the range is reduced and transmission speed is lower.
- Water or moisture cannot enter the case of the unit.
- Airflow around the unit and through the vents on the side of the case is not restricted. The access point should have a minimum of 25 mm (1 in.) clearance.

Step 5. Connect the Access Point to a Power Source

1. Plug the included power adapter into the access point's power connector and into a nearby AC power source.

   Alternatively, connect the Ethernet port on the access point to a switch or other network device that provides Power over Ethernet.

Note

If you connect the access point to an AC power source and a PoE power source at the same time, PoE will be disabled automatically.

2. Re-check the LEDs during the system initialization. See "LED Behavior" on page 2-11.

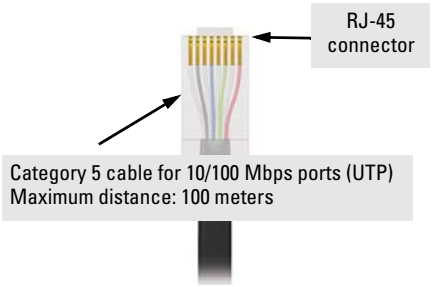
Step 6. Connect the Network Cable

Connect the network cable, described under ""Cabling Infrastructure" on page 2-8, from the network device or your patch panel to the LAN port on the access point.

Using the RJ-45 Connectors

To connect:
Push the RJ-45 plug into the LAN port until the tab on the plug clicks into place. When power is on, one of the two LAN LEDs should turn on to confirm a valid network connection.

If *neither* LAN LED turns on, see "Diagnosing with the LEDs" in Chapter 5.



Congratulations! You have completed installing your access point. You are now ready to start configuring your access point settings.

Please continue to Chapter 3, "Getting Started With Access Point Configuration" for an introduction of the Web interface and a summary of essential configuration tasks that you should perform.

Getting Started With Access Point Configuration

This chapter provides instructions for logging on to the Web interface and a summary of the essential configuration tasks you need to perform to get the access point up and running on your network.

Topics discussed include:

Introducing the Management Web Interface

The access point is managed through a Web browser-based interface that you can access from any PC or workstation on the same subnet as the access point. Open a compatible browser and type the access point's IP address as the URL. (See "Step 1. Preconfigure the Access Point" on page 2-5 for information on setting the IP address.)

Note

You can use the Web browser interface to access IP addressing only if the access point already has an IP address that is reachable through your network.

No additional software installation is required to make this interface available; it is included in the access point's onboard software.

You will need a common Web browser to access the management interface. The Web browser that you will use for management must have JavaScript enabled to support the interactive features of the Web interface. It must also support HTTP uploads to use the software update feature.

Note

To ensure proper screen refresh when using Internet Explorer with Windows XP, be sure that the browser options are configured as follows: Under the menu "**Tools** > **Internet Options** > **Temporary Internet Files** > **Settings**," the setting for item "**Check for newer versions of stored pages**" should be set to "**Automatically**."

s

Logging On to the Web Interface

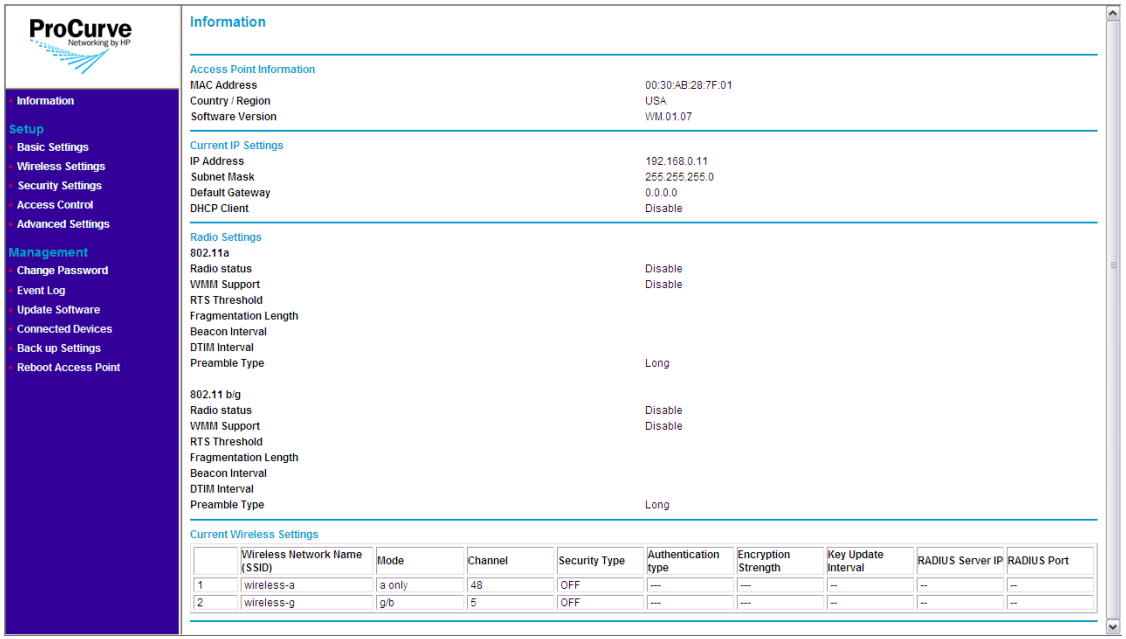
To log on to the Web interface:

1. Start your Web browser.
2. In the address or location bar, enter the IP address that you assigned to the access point when you preconfigured it in "Step 1. Preconfigure the Access Point" on page 2-5.

   A logon dialog box appears.
3. In **User name**, type **admin**.
4. In **Password**, type **password**.
5. Click **OK** to log on.

The ProCurve Access Point 10ag Web interface appears, showing the Information page.

Figure 3-1. Information Page (Web Interface Home Page)



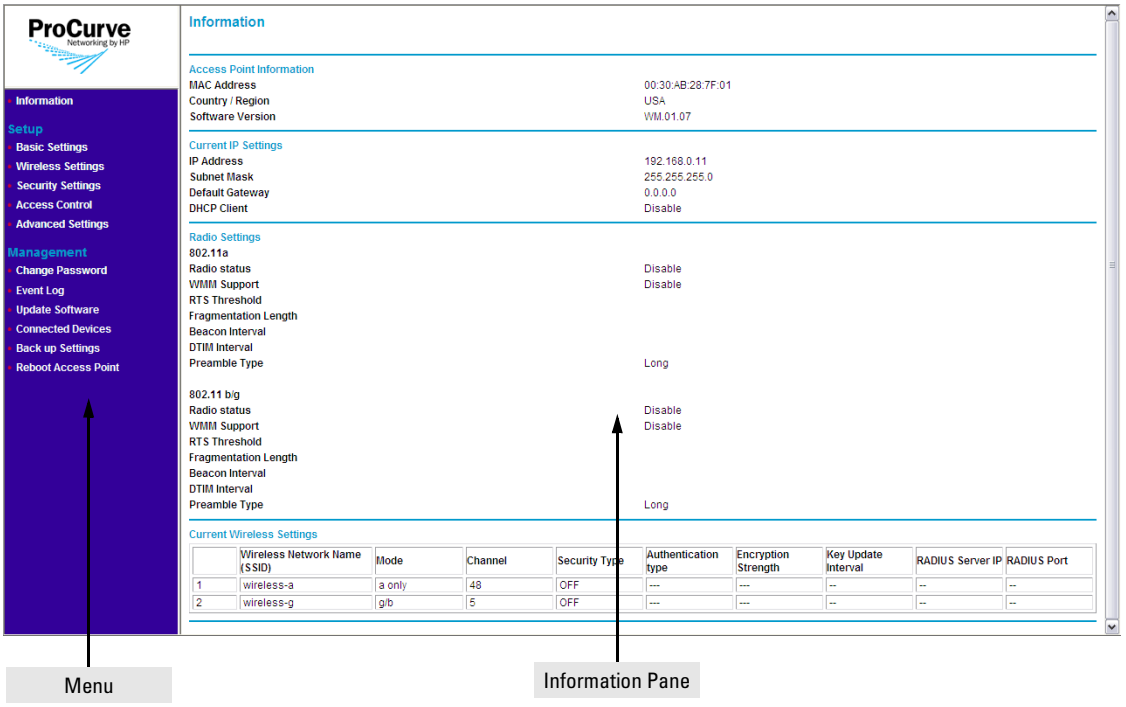
Note

The Web interface does not have a Log Off button. To end your Web interface session safely, close the Web browser.

Navigating Around the Web Interface

The Web interface provides logical window groups for easy access to common setup, management, and advanced configuration features. This section describes each of the logical window groups, submenus, screen elements and parameters.

Figure 3-2. Web Interface Elements



The Web interface has two primary sections:

- **The menu**: Located on the left-hand side of the page, the menu contains links to the primary configuration options on the Web interface. Menu items are grouped into three categories:
  - **Information** (default home page): Shows information about the access point, including the MAC address, software version, current IP address settings, and configured wireless networks.
  - **Setup**: Contains options for configuring the essential access point settings, such as basic IP address settings, basic wireless settings, security settings, and access control.
  - **Management**: Contains options for performing administrative tasks on the access point, including changing the password, updating the software, backing up and restoring settings, viewing the list of associated wireless clients and devices, and rebooting the access point.

- **The information pane**: Shows related configuration options for each item on the menu. For example, if you click **IP Settings** on the menu, the information pane loads the parameters that you can set or edit, and then save for your desired configuration change to take effect.

Tasks for Your First Web Browser Interface Session

The first time you access the Web browser interface, there are a number of basic tasks that you should perform. Table 3-1 lists these essential tasks. For specific instructions on the how perform the procedure, refer to the page number listed in the right column.

In setting up your access point for network installation, this manual covers many of the tasks that should be considered for proper security and management. Each of these tasks are detailed in their respective sections, however, this summary is provided as an aid for establishing your network.

Table 3-1. Basic Web Interface Tasks

To Learn How to Do This Task	Refer to
Change the default password	"Changing the Management Password" on page 5-3
Set the correct country/region code	"Configuring Basic Settings" on page 4-1
Control access to the wireless network	"Controlling Access to the Wireless Network" on page 4-22
Set wireless security from No Security (default) to at least WPA/WPA2	"Configuring Security Settings" on page 4-7

Default Configuration Parameters

Table 3-2 lists some of the default settings with which the access point is configured, including the basic IP address and wireless configuration parameters. Information on how to update each parameter is provided later in this guide.

Table 3-2. Default Parameters

Parameter	Default	Description
Username	admin	The name of the manager.
Password	password	The password for the manager.
IP Address	192.168.1.14	IP address compatible with your network.
Subnet Mask	255.255.255.0	Subnet mask compatible with your network.
Default Gateway	*not set*	IP address of the next-hop gateway node for network traffic that needs to be able to reach off-subnet destinations.
Radio Mode	802.11 b/g	The default radio mode.
Radios	Disabled	Both radios are disabled.
SSID	wireless-g	A pre-configured Service Set Identifier (SSID), also called a wireless network name.

Note: The IP address and subnet mask assigned to the access point must be compatible with the IP addressing used on your network. For more information on IP addressing, see "Configuring Basic Settings" on page 4-1.

Setting Up the Access Point

This chapter provides information on how configure the access point's network, wireless, and security settings to ensure its proper operation on the network. It also describes how to configure advanced options, such as the wireless radio settings and the built-in SNMP agent.

Topics discussed in this chapter include:

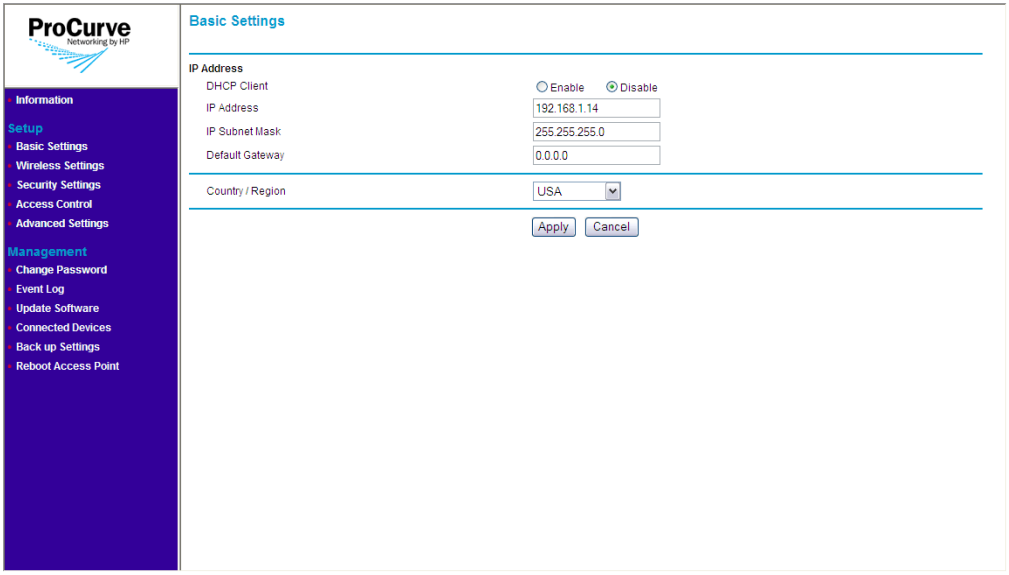
Configuring Basic Settings

Basic settings refer to the IP address settings and the country/region code assigned to the access point.

Note

If the access point's IP address settings are already compatible with your network, you do not need to change them.

Figure 4-1. Basic Settings Page



To configure the access point's basic settings:

1. On the menu, click **Basic Settings**.
2. Configure the IP address settings.
   - Assign an IP address (recommended) – If you want to assign a fixed IP address to the access point, select **Disable** for the DHCP Client, and then enter the IP Address, IP Subnet Mask, and Default Gateway that you want to assign to it. These settings must be compatible with your network to ensure that the access point can communicate with other network devices.
   - Enable the built-in DHCP client – If you have a DHCP server on the network and you want the access point to automatically obtain an IP address from the DHCP server, click **Enable** in DHCP Client. You do not have to configure other settings, but you will need to check the DHCP server from time to time to determine the IP address that the access point is using. You need this IP address to connect to the Web interface.

Note

If you enable the built-in DHCP client and the access point fails to obtain an IP address from the DHCP server after 10 seconds (for example, the DHCP server is unreachable), the access point will automatically use **192.168.1.14**, its default IP address.

3. In **Country/Region**, select the country or region where you are installing the access point (if you have not done so earlier).

Notes

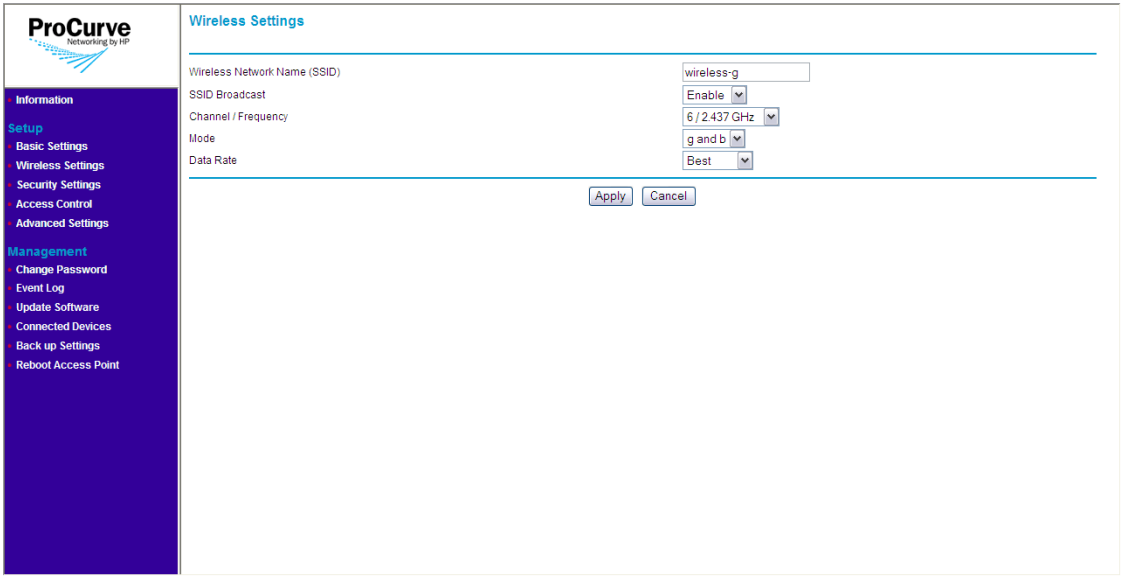
- You must select the correct country/region for the location in which you operate the access point, so that it uses only the authorized radio channels for wireless network devices.
- The radios are disabled if the Country/Region option is not set. Once this option is configured, the radios can be enabled.
- When resetting to factory defaults, the Access Point 10ag must have its Country/Region setting configured.

4. Click **Apply**.

Configuring Wireless Settings

Wireless settings define the SSID, wireless channel, wireless mode, and data rate that each wireless interface uses. The access point comes with one predefined wireless profile (SSID **wireless-g**), which allows 802.11b/g wireless clients to associate with it. You can edit this existing wireless profile, or you can create new ones.

Figure 4-2. Wireless Settings Page

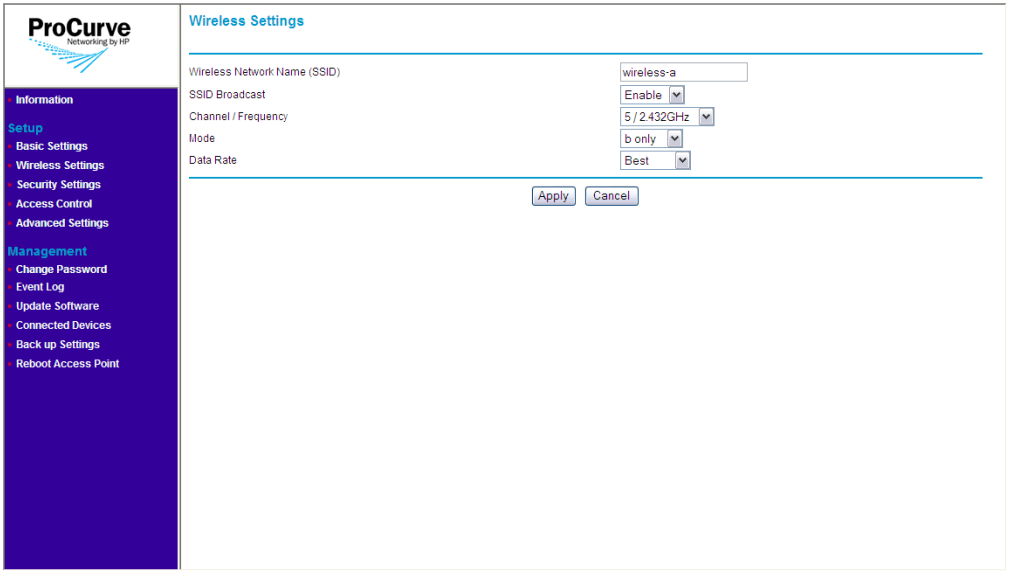


Creating a Wireless Profile

Note

The access point ships with one preconfigured wireless profile for 802.11b/g.

Figure 4-3. Add Wireless Profile Page



To create a new wireless profile:

1. On the menu, click **Wireless Settings**. The Wireless Settings page appears.
2. Click **Add**.
3. In **Wireless Network Name (SSID)**, type a unique SSID that you want to assign to the wireless profile.
4. In **SSID Broadcast**, click **Enable** if you want to allow all wireless clients and devices within the range of the access point to see the SSID. Otherwise, click **Disable**.
5. In **Channel/Frequency**, select the wireless channel and frequency that you want this wireless profile to use. The range of channels and frequencies available depends on the wireless mode that you selected.
6. In **Mode**, select the wireless mode that you want this wireless profile to use. Available options include:
   - **g and b**: Select to allow connections from 802.11g and 802.11b clients only.

- **g only:** Select to allow connections from 802.11g clients only.
- **a only**: Select to allow connections from 802.11a clients only.
- **b only:** Select to allow connections from 802.11b clients only.

7. In **Data Rate**, select the maximum speed at which the access point can transmit traffic for this wireless profile. If you want the access point to automatically use the optimum data rate for the associated wireless clients and devices, select **Best**.
8. Click **Apply**. A confirmation message appears.
9. Click **OK** to finish creating the wireless profile.

Note

For the access point to operate using this wireless profile, the radio interface configured for the SSID must be enabled. Check the radio status on the Information page. If the radio is disabled, refer to "Configuring Advanced Settings" on page 4-25 for instructions on how to enable it.

Editing a Wireless Profile

To edit an existing wireless profile:

1. On the menu, click **Wireless Settings**.
2. Click the option button for the wireless profile that you want to edit. For example, if you want to edit the **wireless-g** profile, click the option button next to it.
3. Click **Edit**.
4. Modify the following settings as required:
   - **Wireless Network Name (SSID)**
   - **SSID Broadcast**
   - **Channel/Frequency**
   - **Mode**
   - **Data Rate**
5. Click **Apply**.

Deleting a Wireless Profile

To delete a wireless profile:

1. On the menu, click **Wireless Settings** under **Setup**. The SSID List page appears.

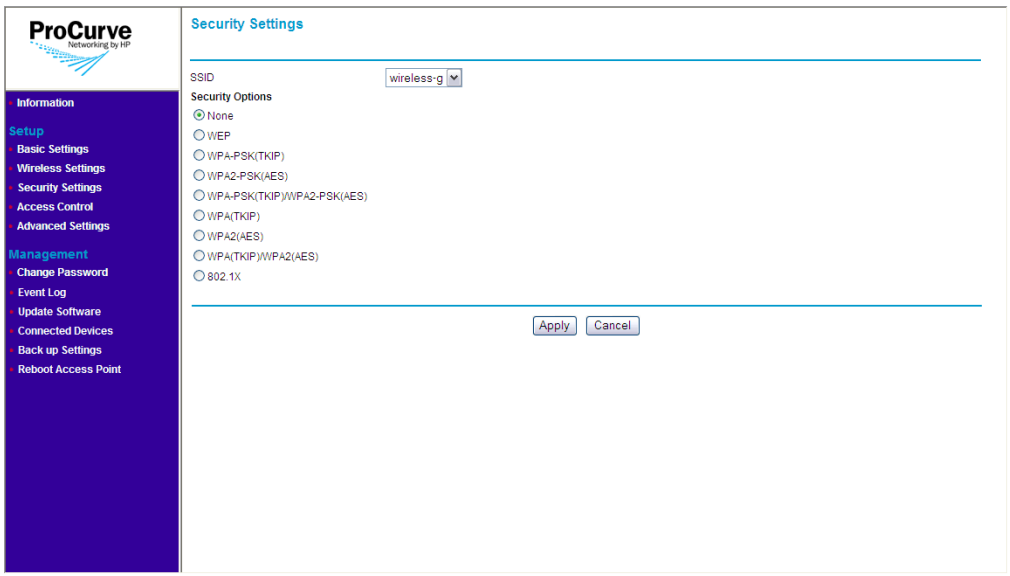
2. Select the option button for the wireless profile that you want to delete.
3. Click **Delete**.

The message **Please wait...** appears. After a few seconds, the SSID List refreshes and the wireless profile you chose to delete disappears from the list of SSIDs.

Configuring Security Settings

Unlike wired networks, anyone with a compatible wireless adapter can receive wireless data transmissions from your network well beyond your walls. To prevent outsiders from eavesdropping on your network traffic or from entering your network to access your computers and files, you should configure the security features of your access point.

Figure 4-4. Security Settings Page



Wireless Security Overview

By default, the access point is configured as an “open system,” with no security. This means that the access point broadcasts a beacon frame, advertising each configured wireless network (SSID). If a wireless client has a

configured WLAN of “any,” it can read the SSID from the beacon and use it to allow immediate connection to the access point. Wireless devices are permitted to connect with the access point without first verifying that users are authorized to access the network.

In addition, user data is transmitted over the air without being encrypted, and is subject to being intercepted by wireless devices anywhere within range that want to eavesdrop on the wireless network.

Configure your wireless network security to protect against eavesdroppers and to prevent unauthorized access to the wireless network. Wireless network security requires attention to three main areas:

- **Authentication**: Verifying that devices attempting to connect to the network are authorized users before granting them access.
- **Encryption**: Encrypting data that passes between the access point and devices (to protect against interception and eavesdropping).
- **Key Management:** Assigning unique data encryption keys to each wireless device session, and periodically changing the encryption keys to minimize risk of their potential discovery.

Authentication

The two ways of authenticating users on the Access Point 10ag are:

- MAC Authentication: Based on the user's wireless device MAC address.
- 802.1X Authentication: Based on the user credentials, such as; username/password, digital certificates, etc.

MAC Authentication. MAC authentication of users can be done either using a remote authentication server like a RADIUS server or by creating a local database on the access point itself. MAC authentication is not as secure as 802.1X authentication, as it is easy to decipher and spoof for unauthorized network access.

802.1X Authentication. User 802.1X authentication can be implemented using a remote authentication server, such as a RADIUS server. The user's credentials are exchanged with the servers using a mechanism called “Extensible Authentication Protocol (EAP)”. EAP is a public-key encryption system to ensure that only authorized network users can access the network. In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and sends back to the server to complete the authentication.

The Access Point 10ag supports all EAP types tested by the WiFi Alliance; TLS, TTLS, PEAP0/MSCHAPv2, PEAP1/GTC and SIM. EAP types that do not provide key management (like MD5) are not suitable for wireless networks. 802.1X authentication can be used with WEP, TKIP and AES encryption ciphers. It is possible to use a combination of both MAC authentication and 802.1X authentication simultaneously on the same WLAN.

Encryption

The access point supports three types of encryption:

- Wired Equivalent Privacy (WEP): Key lengths of 64 bits and 128 bits are possible. WEP provides the least secure method of encryption (static WEP is not secure, as it can be easily compromised).
- Temporal Key Integrity Protocol (TKIP): Intermediate security between WEP and AES with key length of 256 bits. Provides a more-secure method of encryption than WEP (security is much better than WEP, but not as robust as AES).
- Advanced Encryption Standard (AES): AES is a symmetric 128-bit block data encryption technique that works on multiple layers of the network. It is the most effective encryption system currently available for wireless networks.

Key Management

Keys for encrypting the data can be managed either dynamically using 802.1X authentication or statically using pre-shared keys between the access point and device. Dynamic key management provides significantly better security when compared to using static keys.

Deciding Which Security Profile to Use

Table 4-1 shows a summary of available security profiles. Use this table as a reference when deciding on which security profile best suits your network.

Remember that certain security profiles may require additional software or hardware. 802.1X, for example, requires a RADIUS server to be configured on the network. Additionally, not all wireless network cards support WPA.

Choose a security profile that provides the highest level of security while maintaining compatibility with most, if not all, existing wireless devices on the network.

Table 4-1. Summary of Wireless Security

Security Profile	Client Support	Implementation Considerations
None (NOT RECOMMENDED)	Built-in support on all 802.11a, 802.11b, and 802.11g devices	No key management, data encryption, or user authentication is used
WEP	Built-in support on all 802.11a, 802.11b, and 802.11g devices	• Provides only weak security • Requires manual key management
WPA-PSK (TKIP)	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	• Provides dynamically generated keys that are periodically refreshed • Provides similar shared key user authentication • Provides robust security in small networks
WPA2-PSK (AES)	Requires WPAs-enabled system and network card driver (native support provided in Windows XP)	• Provides robust security in small networks • Requires manual management of pre-shared key • Wireless devices may require hardware upgrade to be WPA2 compliant
802.1X (RECOMMENDED)	Requires WPA-enabled system and network card driver (native support provided in Windows XP)	• Provides dynamically generated keys that are periodically refreshed • Requires configured RADIUS server • Provides backward compatibility to the original WPA

When you have decided which security profile to implement on your network, refer to the next section, "Configuring the Access Point with Your Preferred Security Profile".

Configuring the Access Point with Your Preferred Security Profile

Wireless security options are available on the Security Settings page. By default, the Security Settings page shows **None** as the selected security profile. When you click other security options, the page refreshes, and then displays additional options for that security profile.

Note

The security profile for each SSID must be set separately. For example, if you set wireless-a to use **WPA2**, it will only be applied to wireless-a. If you want other SSIDs to use WPA2 as well, you need to configure each SSID separately.

CAUTION

When access point configuration parameters are changed, wireless clients and devices may be temporarily disconnected until the new configuration parameters are enabled. This includes any changes to a WLAN or radio parameter.

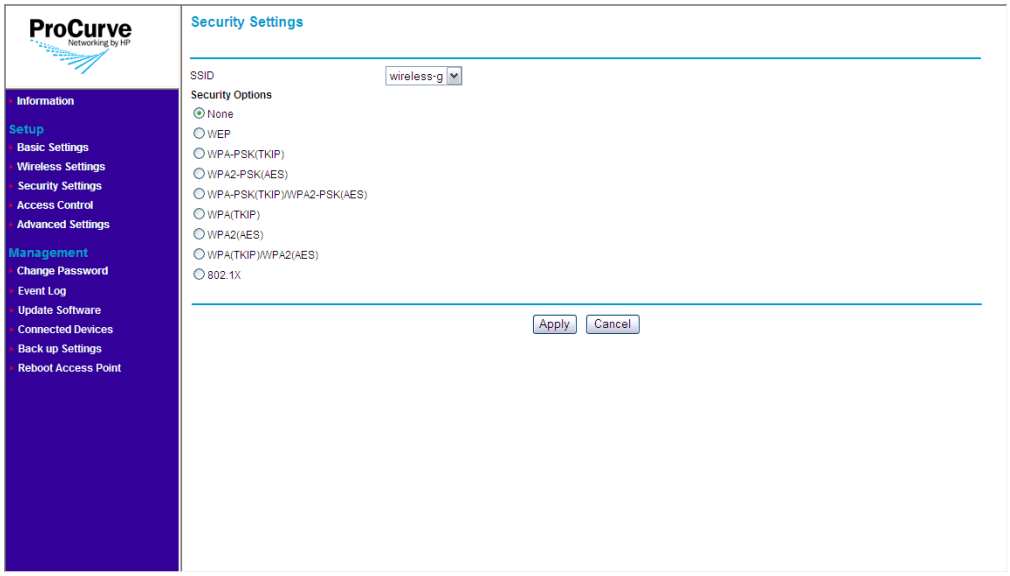
Using No Security

No security mode transmits data over the wireless connection without any form of encryption for data privacy. This mode may be appropriate for systems that provide simple internet and printer access, as on a guest network. It may also be appropriate where additional security is provided by the use of encrypted VPN tunnels between the wireless client device and a network VPN server. If this mode is used, it may be desirable to prevent advertising availability of the network to other devices by configuring the WLAN for closed-system operation.

CAUTION

Use this mode on a sensitive internal network only for: initial setup, testing, or problem solving; or where VPN connections are mandated to provide end-to- end security for the otherwise insecure wireless connection.

Figure 4-5. No Security (Default) Page



To use no security (not recommended):

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under Security Options, click **None**.
4. Click **Apply** to save your changes.

Repeat this procedure for every SSID that you want to use no security.

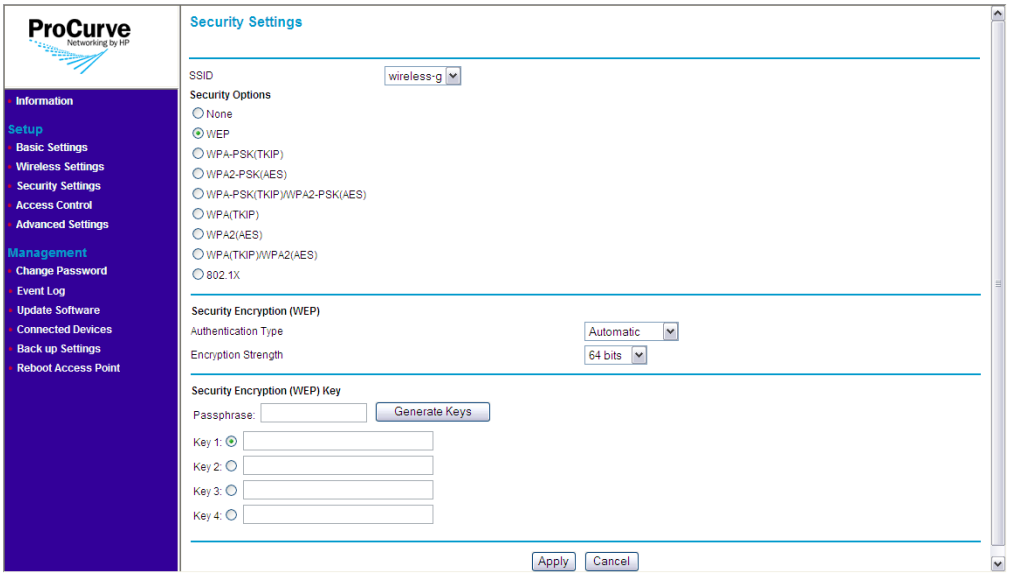
Configuring WEP

Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the access point. WEP uses static shared keys (fixed-length alphanumeric strings) that are manually distributed to all clients that want to use the network.

CAUTION

WEP has been found to be unreliable and is not be recommended for a high level of network security. For more robust wireless security, the access point provides Wi-Fi Protected Access (WPA or WPA2) for improved data encryption and user authentication.

Figure 4-6. WEP Options



To use WEP:

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under **Security Options**, click **WEP**.
4. Under **Security Encryption (WEP)**, configure the authentication type and encryption strength.
   - **Authentication**: Select **Open System** to allow association of wireless clients and devices without requiring authentication. Select **Shared Key** to establish a rudimentary form of user authentication. Select **Automatic** if Shared Key authentication is to be supported, but not required. Default is Automatic.

CAUTION

Shared Key mode is unreliable, in that it utilizes the static WEP encryption key (transmitted openly) for client authentication. This allows the WEP encryption key to be easily discovered by anyone who might eavesdrop on the wireless network. If static WEP is configured, it is recommended to select Open System authentication.

- **Encryption Strength**: Set the length of the encryption key that will be used. Select **64 bits** or **128 bits**. Note that the same size of encryption key must be supported on all wireless clients and devices. Default is **64 bits**.

5. Under **Security Encryption (WEP) Key**, enter up to four strings of character keys. The number of characters required updates automatically based on how you set Authentication and Encryption Strength.
6. Click **Apply** to save your changes.

Configuring WPA-PSK (TKIP)

Wi-Fi Protected Access (WPA) is an early version of the 802.11i security standard. Temporal key integrity protocol (TKIP) is designed for WPA to enhance WEP.

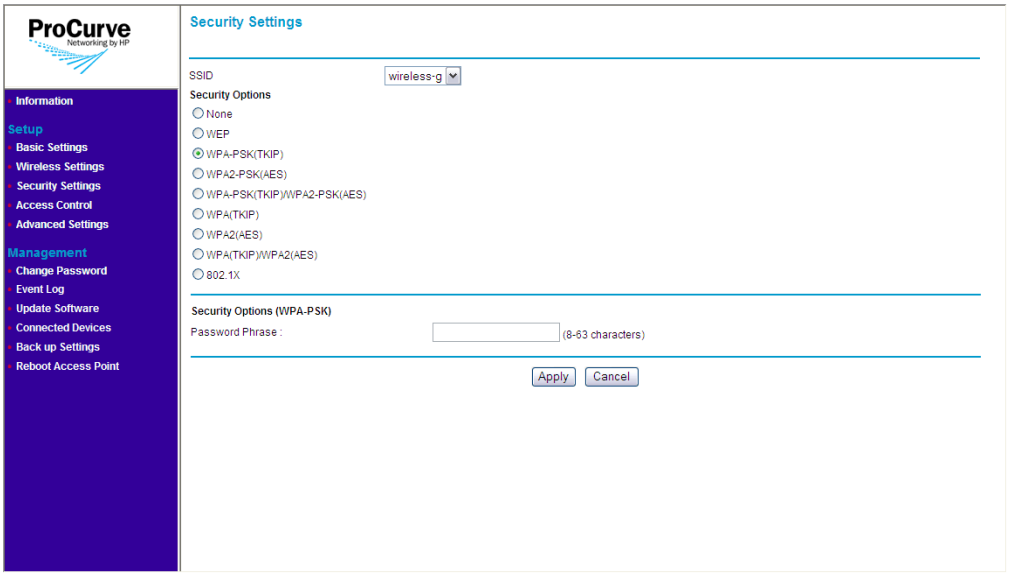
WPA-PSK (TKIP) employs a pre-shared key (PSK), which is used for an initial check of credentials and a 128-bit "temporal key", which combines the client's MAC address and a 16-octet initialization vector to produce the encryption key. This ensures unique key encryption. TKIP uses RC4 to perform the encryption and changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network.

To use this security profile, your wireless clients and devices must support WPA.

Note

If your wireless network has a mix of devices (some support WPA2 and others support the original WPA), you should use WPA-PSK (TKIP)/WPA2-PSK (AES). Refer to "Configuring WPA-PSK (TKIP) / WPA2-PSK (AES)" on page 4-16 for more information.

Figure 4-7. WPA-PSK (TKIP) Options



To use WPA-PSK (TKIP):

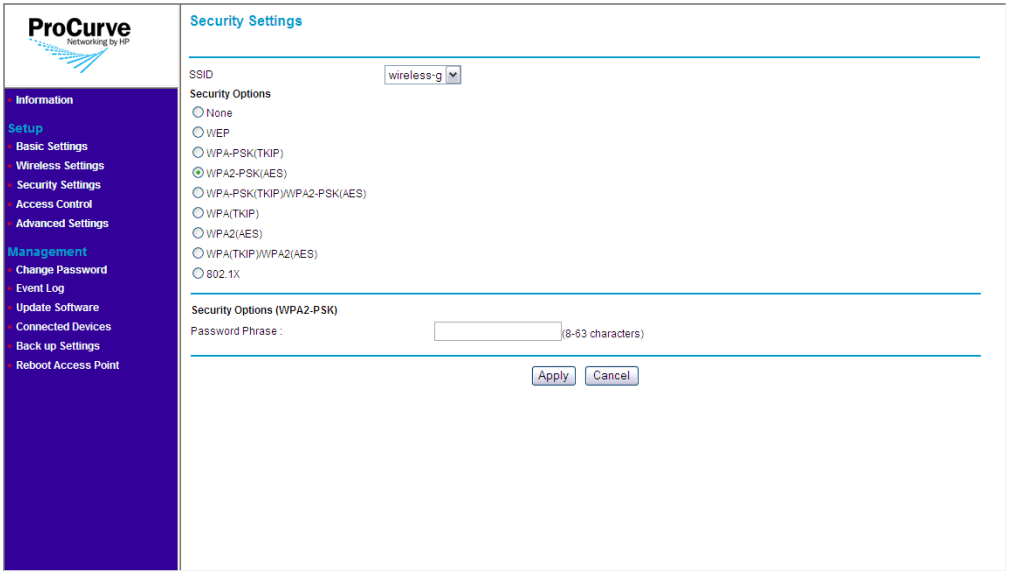
1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under **Security Options**, click **WPA-PSK (TKIP)**.
4. In the **Password Phrase** box under Security Options (WPA-PSK), enter a string of at least 8 characters to a maximum of 63 characters. The string that you enter here will be used as the shared secret key for WPA-PSK.
5. Click **Apply** to save your changes.

Configuring WPA2-PSK (AES)

WPA2-PSK (AES) employs a pre-shared key (PSK), which is used for an initial check of credentials, and CCMP, an IEEE802.1X encryption method that uses the Advanced Encryption Algorithm (AES).

To use this security profile, your wireless clients and devices must support WPA.

Figure 4-8. WPA2-PSK (AES) Options



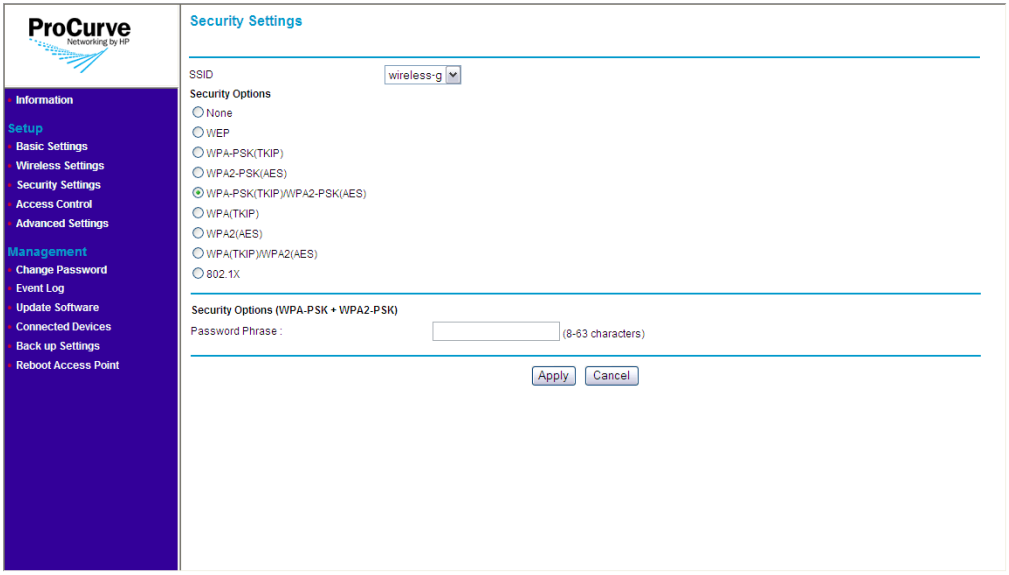
To use WPA2-PSK (AES):

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under **Security Options**, click **WPA2-PSK (AES)**.
4. In the **Password Phrase** box under Security Options (WPA-PSK), enter a string of at least 8 characters to a maximum of 63 characters. The string that you enter here will be used as the shared secret key for WPA-PSK.
5. Click **Apply** to save your changes.

Configuring WPA-PSK (TKIP) / WPA2-PSK (AES)

This security profile combines WPA-PSK (TKIP) and WPA2-PSK (AES). It uses a pre-shared key (PSK), which is used for an initial check of credentials, and a mixed cipher mode of TKIP and AES.

Figure 4-9. WPA-PSK (TKIP) / WPA2-PSK (AES) Options



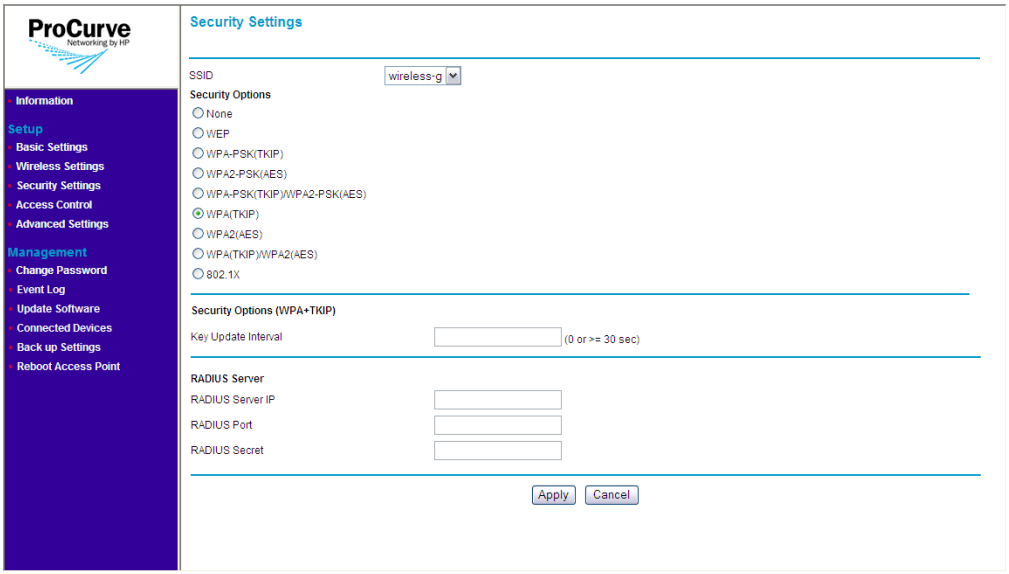
To use WPA-PSK (TKIP) / WPA2-PSK (AES):

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under Security Options, click **WPA-PSK (TKIP) / WPA2-PSK (AES)**.
4. In the **Password Phrase** box under Security Options (WPA-PSK), enter a string of at least 8 characters to a maximum of 63 characters. The string that you enter here will be used as the shared secret key for WPA-PSK.
5. Click **Apply** to save your changes.

Configuring WPA (TKIP)

This security profile uses TKIP as the encryption cipher and 802.1X as the authentication mechanism. In this way, each device is going to utilize a unique master key to derive the encryption between the access point and device.

Figure 4-10. WPA (TKIP) Options



To use WPA (TKIP):

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under Security Options, click **WPA (TKIP)**.
4. In the **Key Update Interval** box, define the time interval (in seconds) for regenerating a group key.
5. Under RADIUS Server, configure the RADIUS server settings:
   - **RADIUS Server IP**: Type the IP address of the RADIUS server on the network.
   - **RADIUS Port**: Type the User Datagram Protocol (UDP) port number used by the RADIUS server for accounting messages. Setting the port number to zero disables RADIUS authentication.

- **RADIUS Secret**: Type a shared text string used to encrypt messages between the access point and the RADIUS server. Make sure that the same text string is specified on the RADIUS Accounting server. Do not use blank spaces in the string. (Maximum length: 20 characters)

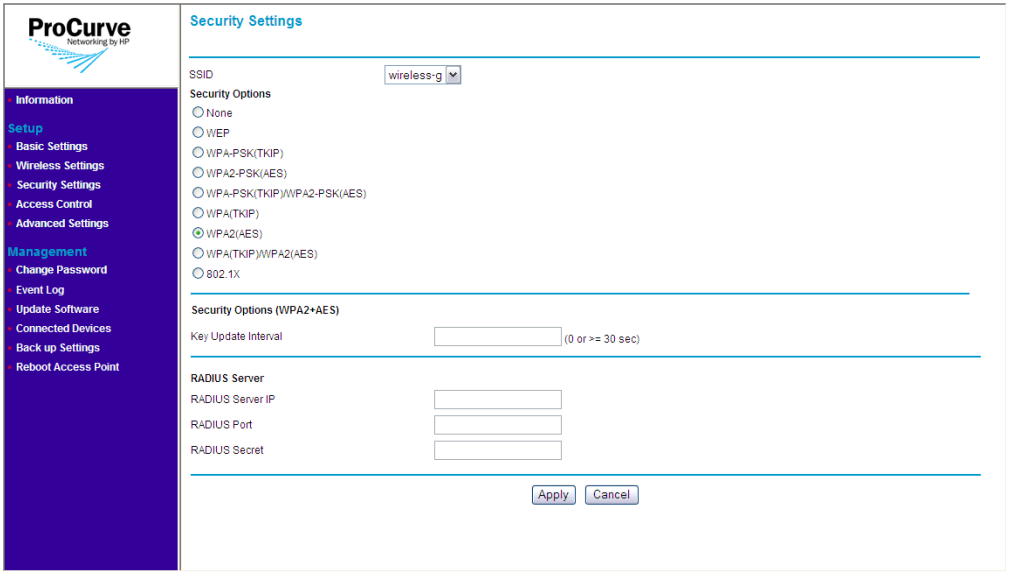
6. Click **Apply** to save your changes.

Repeat the same procedure for each SSID to which you want to assign WPA (TKIP) as its security profile.

Configuring WPA2 (AES)

This security profile uses AES as the encryption cipher and 802.1X as the authentication mechanism. In this way, each device is assigned a unique master key to derive the encryption between the access point and device, and the encryption keys can be automatically and periodically changed to further reduce the possibility of their discovery.

Figure 4-11. WPA2 (AES) Options



To use WPA2 (AES):

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.

3. In the **Key Update Interval** box, define the time interval (in seconds) for regenerating a group key.
4. Under RADIUS Server, configure the RADIUS server settings:
   - **RADIUS Server IP**: Type the IP address of the RADIUS server on the network.
   - **RADIUS Port**: Type the User Datagram Protocol (UDP) port number used by the RADIUS server for accounting messages. Setting the port number to zero disables RADIUS authentication.
   - **RADIUS Secret**: Type a shared text string used to encrypt messages between the access point and the RADIUS server. Make sure that the same text string is specified on the RADIUS Accounting server. Do not use blank spaces in the string. (Maximum length: 20 characters)
5. Click **Apply** to save your changes.

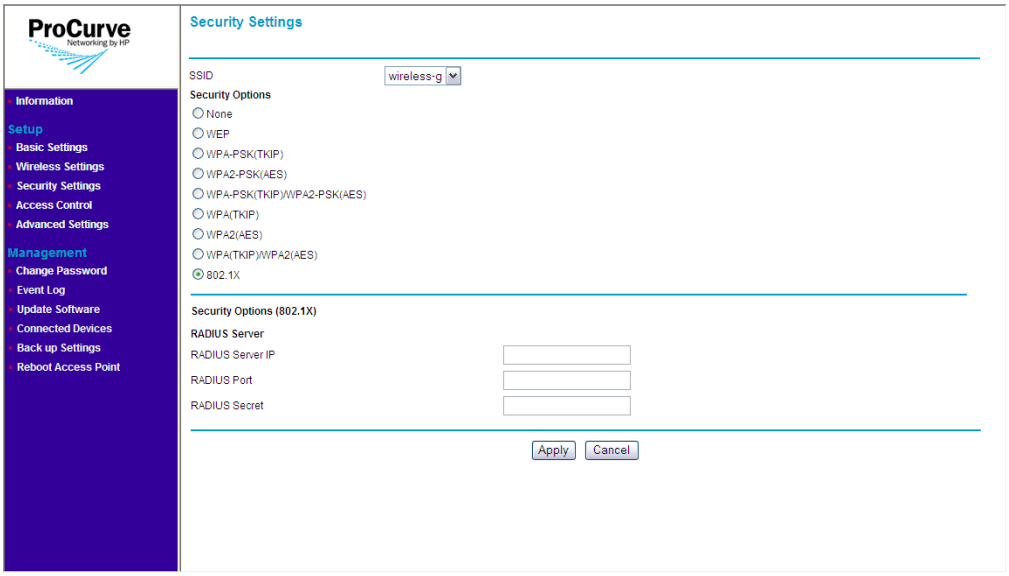
Repeat the same procedure for each SSID to which you want to assign WPA2 (AES) as its security profile.

Configuring 802.1X

802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication.

The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the access point grants the client access to the network.

Figure 4-12. 802.1X Options



To use 802.1X:

1. On the menu, click **Security Settings**. The Security Settings page appears.
2. In **SSID**, select the SSID for which you want to set the security profile.
3. Under Security Options, click **8021.X**.
4. Under Security Options (802.1X), configure the RADIUS server settings:
   - **RADIUS Server IP**: Type the IP address of the RADIUS server on the network.
   - **RADIUS Port**: Type the User Datagram Protocol (UDP) port number used by the RADIUS server for accounting messages. Setting the port number to zero disables RADIUS authentication.
   - **RADIUS Secret**: Type a shared text string used to encrypt messages between the access point and the RADIUS server. Make sure that the same text string is specified on the RADIUS Accounting server. Do not use blank spaces in the string. (Maximum length: 20 characters)
5. Click **Apply** to save your changes.

Repeat the same procedure for each SSID to which you want to assign 802.1X as its security profile.

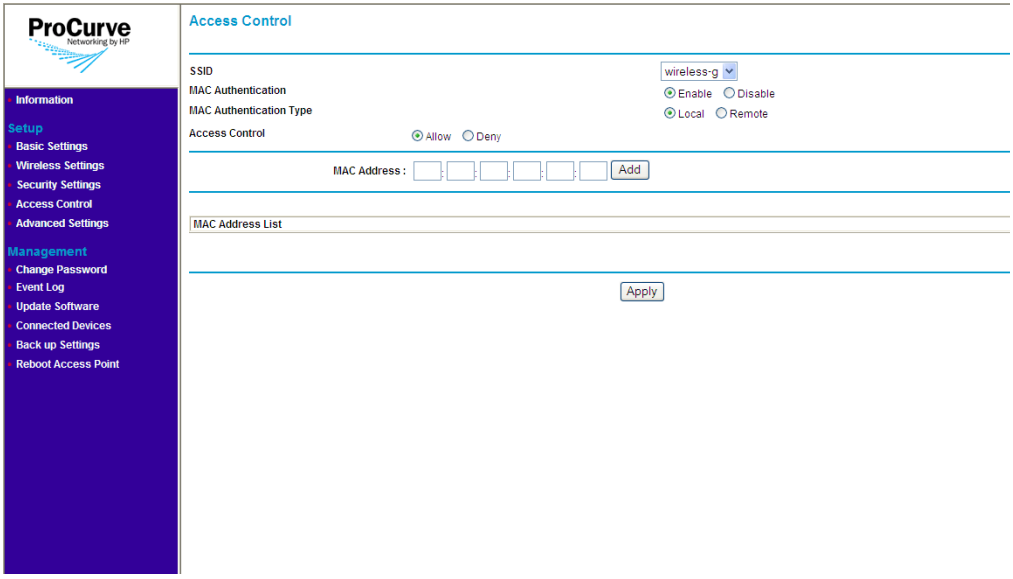
Controlling Access to the Wireless Network

You can configure the access point to authenticate client MAC addresses against a database stored locally on the access point or remotely on a RADIUS server. Client MAC addresses on the local database can be specified as allowed or denied access the network. This enables the access point to control which devices can associate with the access point.

Note

Access control settings for each SSID/wireless interface need to be configured separately. Enabling access control for one SSID will not enable access control for other SSIDs.

Figure 4-13. Access Control Page



There are two options for setting up access control on the wireless network:

- Local MAC authentication, and
- Remote MAC authentication

Note

You can only use one type of MAC authentication at any given time.

Before setting up either type of MAC authentication, you should list down the MAC addresses of the wireless clients and devices that you want to allow or deny access.

Setting Up Local MAC Authentication

Local MAC authentication allows you to add entries to the built-in MAC authentication database and to take certain actions based on a wireless client's MAC address. The MAC list can be configured to allow or deny network access to specific clients.

Note

You can add up to 16 MAC addresses per SSID to the local MAC authentication database.

To enable local MAC authentication:

1. On the menu, click **Access Control**.
2. In **SSID**, select the SSID to which you want to configure access.
3. In **MAC Authentication**, select **Enable**.
4. In **MAC Authentication Type**, select **Local**.
5. In **Access Control**, select the access option that you want to configure for the wireless device. Options include:
   - **Allow**: Click to permit access to all MAC addresses specified in the **[MAC Address List]** below.
   - **Deny**: Click to deny access to all MAC addresses specified in the **[MAC Address List]** below.
6. In the **MAC Address** box, enter the MAC or physical address of the wireless device that you want to allow or deny. A MAC address consists of six pairs of alphanumeric characters, for example, 00 11 AA 22 BB 33.
7. Click **Add**. The page refreshes and the MAC address that you entered appears under **MAC Address List**.

   Repeat steps 5 to 6 for each wireless device that you want to allow or deny.
8. Click **Apply** to save your changes.

The message **Please wait...** appears as the address is added to the list. When the access point has completed the process, the MAC address appears in the MAC Address List table.

To delete a MAC address from the list, click the **Delete** button next to it.

To disable local MAC authentication:

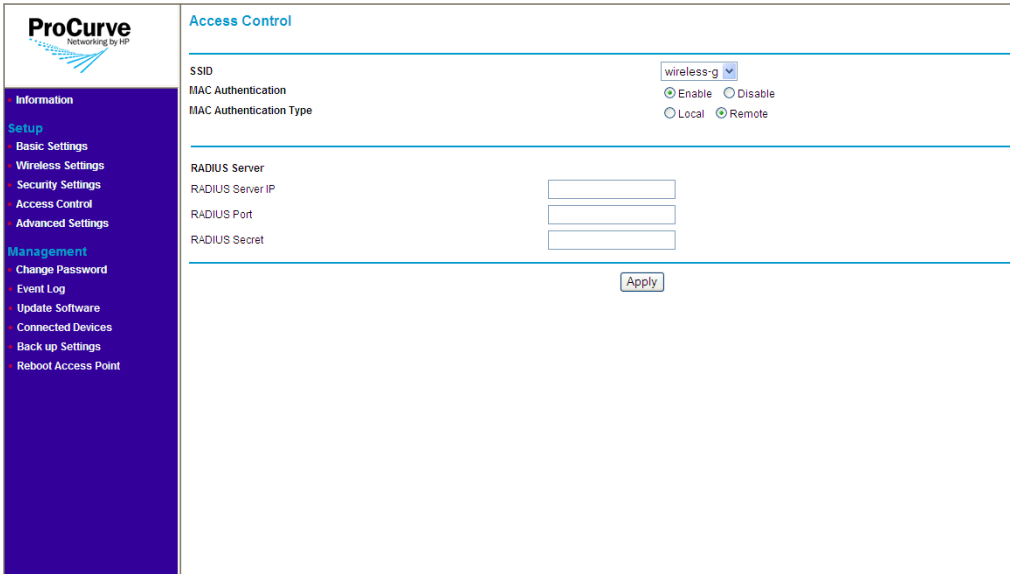
1. On the menu, click **Access Control**.
2. In **SSID**, select the SSID to which you want to configure access.
3. In **MAC Authentication**, select **Disable.**
4. Click **Apply** to save your changes.

Setting Up Remote MAC Authentication

Remote MAC Authentication makes use of a Remote Authentication Dial-in User Service (RADIUS) server to perform client authentication. RADIUS is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network. It is also used to implement IEEE 802.1X (802.1X) network access control and Wi-Fi Protected Access (WPA) wireless security.

If a RADIUS is available on the network, you can configure the access point to perform remote MAC authentication.

Figure 4-14. Remote MAC Authentication Page



Note

This guide assumes that you have already configured the RADIUS server(s) to support the access point. The configuration of RADIUS server software is beyond the scope of this guide. Refer to the documentation provided with the RADIUS server software.

To enable remote MAC authentication:

1. On the menu, click **Access Control**.
2. In **SSID**, select the SSID to which you want to configure access.
3. In **MAC Authentication**, select **Enable**.
4. In **MAC Authentication Type**, select **Remote**.
5. Under **RADIUS Server**, enter the following information:
   - **RADIUS Server IP**: The IP address of the RADIUS server on the network.
   - **RADIUS Port**: The port number used to communicate with the RADIUS server.
   - **RADIUS Secret**: The shared secret used to gain access to the RADIUS server.
6. Click **Apply** to save your changes.

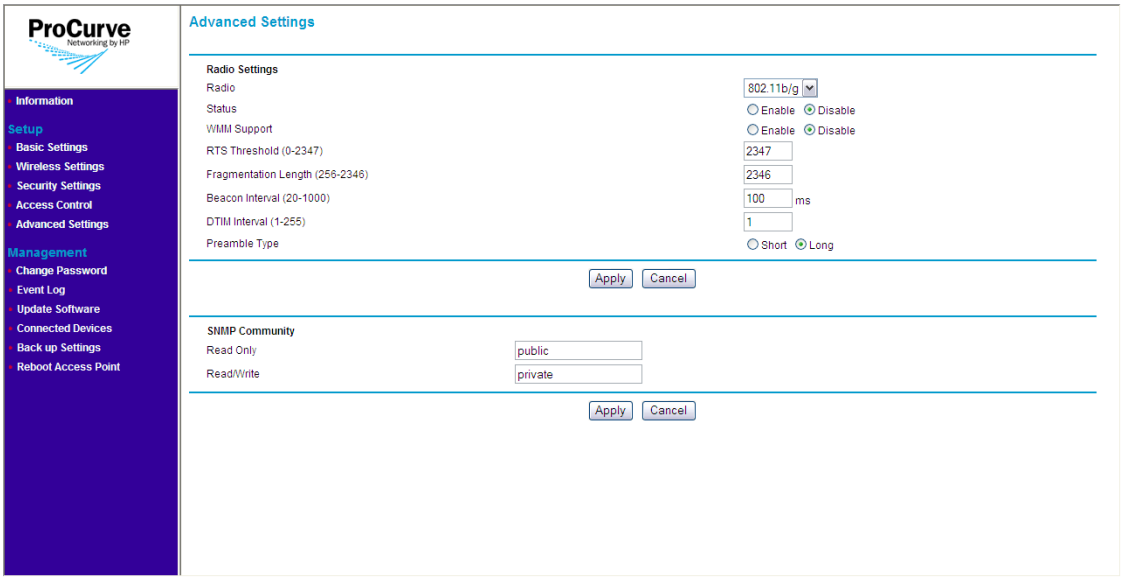
To disable remote MAC authentication:

1. On the menu, click **Access Control**.
2. In **SSID**, select the SSID to which you want to configure access.
3. In **MAC Authentication**, select **Disable.**
4. Click **Apply** to save your changes.

Configuring Advanced Settings

Advanced settings include options for enabling and disabling the wireless radios and Wi-Fi Multimedia (WMM), and for fine tuning the access point's radio operation.

Figure 4-15. Advanced Settings Page



To configure the advanced settings:

1. On the menu, click **Advanced Settings**.
2. In **Radio**, select the radio for which you want to configure the advanced settings. Available options are **802.11a** and **802.11b/g**.
3. In **Status**, click **Enable** if you want to turn on the radio interface that you selected in the previous step. Default is **Disable**.

Note

If you have SSIDs that are configured to use the selected radio, you need to enable the radio interface for the SSIDs to work.

4. In **WMM Support**, click **Enable** if you want the access point to prioritize certain types of traffic above other traffic. When enabled, WiFi Multimedia (WMM) provides basic Quality of Service (QoS) to wireless network. You should enable this option if your network requires prioritization for voice or video traffic (for example, if network users use Voice over IP applications).
5. Configure the following advanced settings for the SSID that you selected:
   - **RTS Threshold**: Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving device prior to the sending device starting communication. The access point sends RTS frames to a receiving device to negotiate the sending of a data frame.

After receiving an RTS frame, the device sends a CTS (clear to send) frame to notify the sending device that it can start sending data. (Default is 2347)

- **Fragmentation Length**: Configures the minimum packet size that can be fragmented when passing through the access point. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This speeds the retransmission of smaller frames. It is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. If set to 2346, this feature is disabled. Range: 256-2346, even numbers. (Default is 2346)
- **Beacon Interval**: The rate at which beacon frames are transmitted from the access point. The beacon frames allow wireless clients and devices to maintain contact with the access point. They may also carry power-management information. Range: 20-1000 ms (Default is 100)
- **DTIM Interval**: The Delivery Traffic Indication Message (DTIM) interval helps keep marginal clients connected by sending "wake up" frames. Range: 1- 255 (Default is 1).
- **Preamble Type:** Sets the length of the signal preamble used at the start of a data transmission. Using a short preamble can increase data throughput on the access point, but requires all connected devices be able to support a short preamble. (Default is Long)
  - **Long**: Sets the preamble to long. Using a long preamble ensures the access point can support all 802.11b and 802.11g devices
  - **Short**: Sets the preamble according to the capability of devices that are currently associated. Uses a short preamble if all associated devices can support it, otherwise a long preamble is used.

6. Click the **Apply** button right below the preamble type settings to save your changes.

Note

There are two **Apply** buttons on the Advanced Settings page: the first is for the advanced wireless settings and the second is for the SNMP community settings. Make sure you click the correct **Apply** button for the settings that you want to save.

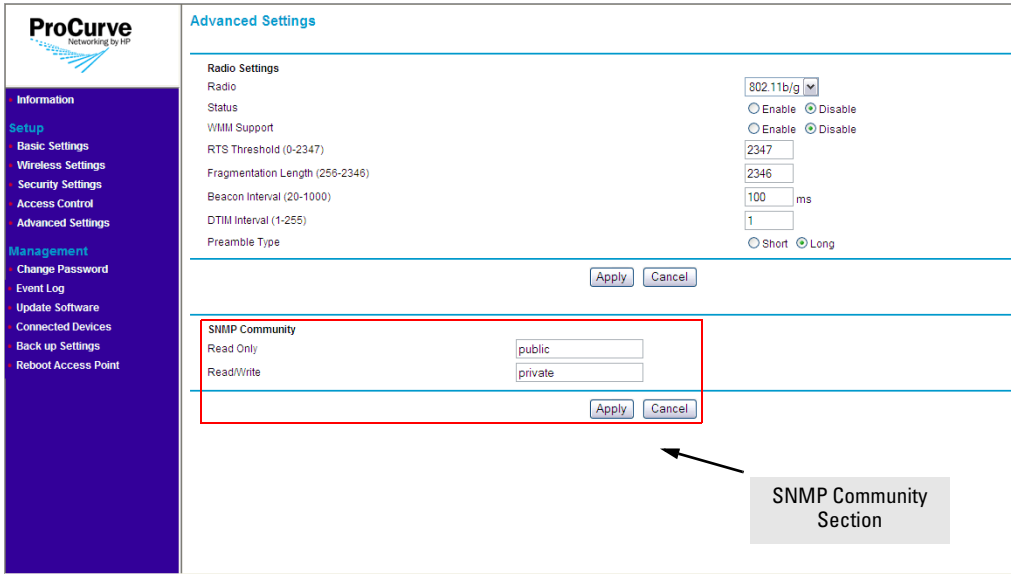
Setting the SNMP Community Names

You can manage the access point from a network management station running a Simple Network Management Protocol (SNMP) management application, such as ProCurve Manager.

The access point SNMP agent supports SNMP versions 1 and 2c. Management access from SNMP v1 or v2c stations is controlled by community names. To communicate with the access point, an SNMP v1 or v2c management station must first submit a valid community name for authentication.

The default community names are **public** for read-only access and **private** for read/write access. If you intend to support SNMP v1 or v2c managers, you should change the default community names to prevent unauthorized access.

Figure 4-16. SNMP Community Section on the Advanced Settings Page



To change the default SNMP community names:

1. On the menu, click **Advanced Settings** under **Setup**. The Advanced Settings page appears.
2. Configure the SNMP community settings under the **SNMP Community** section located at the lower portion of the page.

- To establish a public read-only SNMP community, type a **name** text string to replace the default community name (public) in the **Read Only** text field.
- To establish a private read-write SNMP community, type a **name** text string to replace the default community name (private) in the **Read/Write** text field.

3. Click the **Apply** button under the SNMP Community section to save your changes and activate the new SNMP community names.

Managing the Access Point

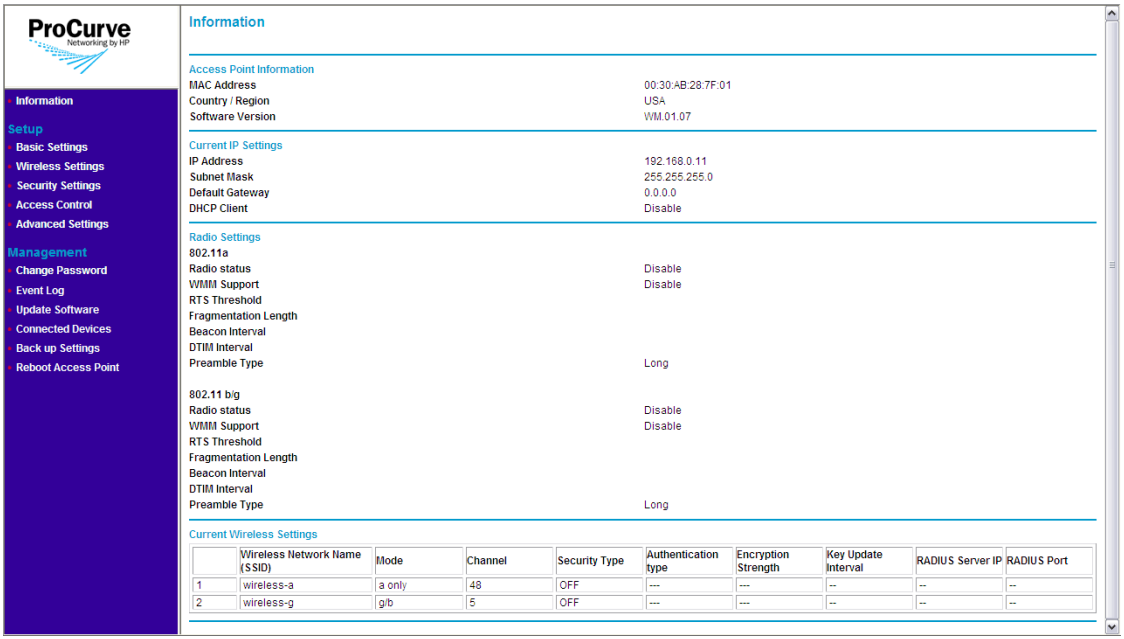
This chapter describes management tasks that you may periodically perform, including changing the management password and updating the software.

Topics discussed in this chapter include:

Viewing Device Information

Device information is available on the Information page, which is the default home page that loads after you log on to the Web interface. To access the Information page when you are already logged on, click **Information** on the menu.

Figure 5-1. Information Page



The Information page displays three types of device information:

- Access Point Information
  - **MAC Address**: The physical layer address for the Ethernet port interface
  - **Region**: Shows the country/region that was set on the Basic Settings page
  - **Software Version**: Shows the version number for the runtime software. Software version is shown as WM.XX.XX, where XX.XX is the version number (for example, WM.01.02).
- Current IP Settings
  - **IP Address**: Shows the IP address of the management interface for this device
  - **Subnet Mask**: Shows the subnet mask configured for the management interface
  - **Default Gateway**: Shows the IP address of the next-hop gateway node for network traffic that needs to be able to reach off-subnet destinations.Gateway address
  - **DHCP Client**: Shows whether the built-in DHCP client is Enabled or Disabled.

- Radio Settings: Shows the status of each radio interface and a summary of their configuration settings, including WMM Support, RTS Threshold, Beacon Interval, and other radio settings.
- Current Wireless Settings: Shows a table that lists all configured SSIDs on the access point and the wireless modes, channels, and security settings that they use.

Changing the Management Password

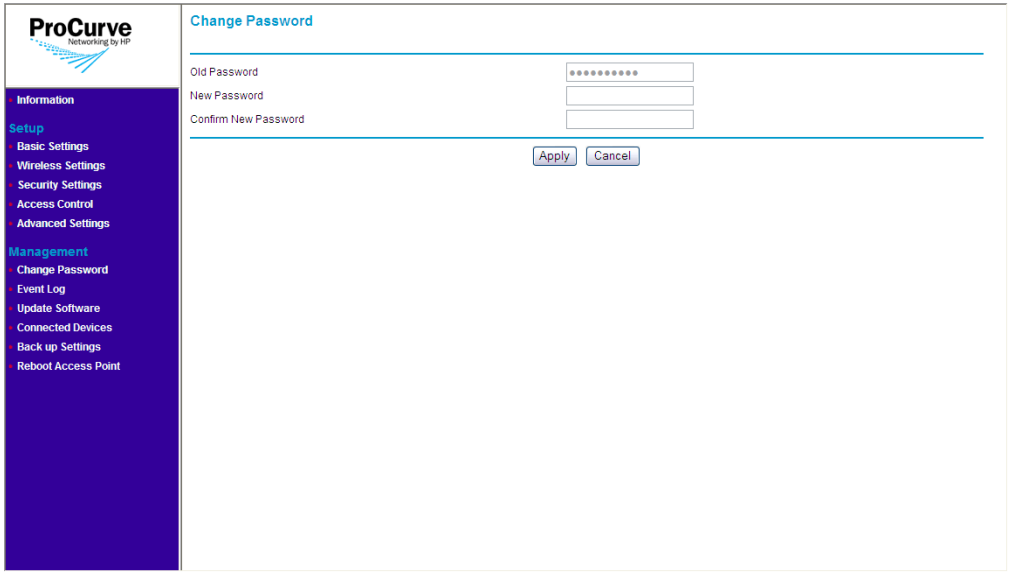
Management access to the Web interface is controlled through an administrator password. To prevent unauthorized users from accessing the Web interface and modifying the access point's settings, the interface is password-protected.

The default manager user name is **admin** and the default password is **password**.

CAUTION

You should change the default Web interface password *immediately* after your first logon. This will help prevent unauthorized users from logging on to the Web interface and changing the access point settings to compromise your network.

Figure 5-2. Change Password Page



To change the default Web interface password:

1. On the menu, click **Change Password**. The Change Password page appears.
2. In **Set Password**, type your new password.

Note

The password is case-sensitive and must be between 1 and 32 alphanumeric characters long.

3. In **Repeat New Password**, type your new password again to confirm.
4. In **Restore Default Password**, click **No**.
5. Click **Apply** to save your changes.

Your new password is instantly applied, and the logon dialog box appears after you save your new password. Enter your new password in the password box to log back onto the Web interface.

If You Forget Your Password

If you forget your password, you will need to reset the access point to factory default, and then log back on to the access point using the default user name (**admin**) and password (**password**).

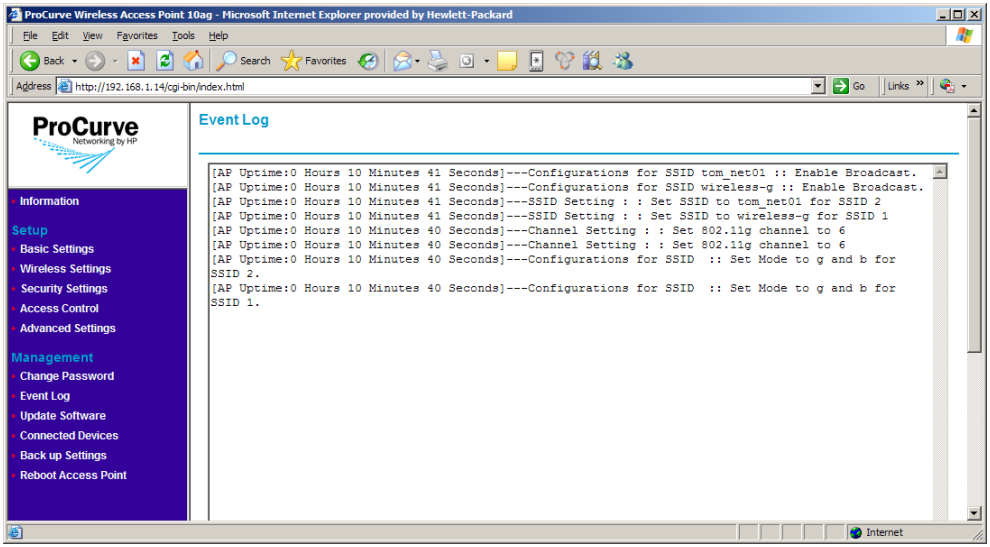
For detailed information, refer to "Restoring Factory Default Configuration" on page 6-6.

Viewing the Event Log

The event log contains a list of activity recorded by the access point. It may be useful for configuration review or troubleshooting.

To view the event log, click **Event Log** on the menu list. To clear the Event Log, scroll to the bottom of the page and click **Clear Log**.

Figure 5-3. Event Log Page



Updating the Access Point Software

The software update function allows you to install on the access point any new access point software that HP may release. To install the new software, you will first need to download the software from the HP Web site to the management computer.

Before performing a software update, take note of the current software version (shown on the Information page). The software version is shown as WM.XX.XX, where XX.XX is the version number (for example, WM.01.02). You need to know this to be able to verify that the update has been completed successfully.

Where to Download Software Updates

The ProCurve support site periodically provides access point software updates through the ProCurve Web site (*www.procurve.com*). At *www.procurve.com*, select **Customer Care** > **Support** > **Software**. In the list of product categories, select **Wireless access points**. Then check for available software updates for the ProCurve Wireless Access Point 10ag.

Update Precautions

CAUTION

Here are a few things that you can do to ensure that the software update process will be completed successfully:

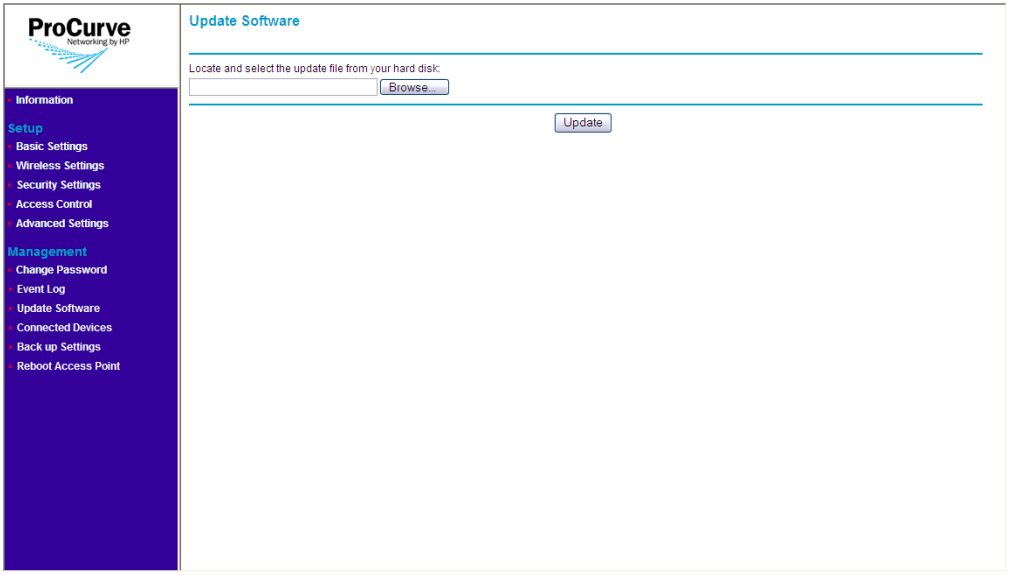
- Do not use your Web browser until the update process has completed.
- Do not interrupt the Web browser by closing the window, clicking a link, or loading a new page.
- Do not interrupt the software update by turning off your computer or the access point.

After a software update, the access point will automatically reboot and apply the updated code.

Note

Updating the software will not change the current configuration of the access point. The access point configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another access point of the same model. You should save a copy of the configuration file before updating your access point software. See "Backing Up and Restoring Configuration" on page 5-9 for information on saving the access point's configuration file.

Figure 5-4. Update Software Page



Software Update Procedure

To update the access point software:

1. On the menu, click **Update Software** under **Management**. The Update Software page appears.
2. Click **Browse**. The Choose File dialog box appears.
3. Go to the folder where you saved the software update file, select the file, and then click **Open**. The Choose File dialog box disappears.
4. Click **Update**. A progress bar appears.

   When the software update is complete, the access point reboots itself, and then redirects you to the Information page.
5. Check the value for **Software Version** and verify that it shows a later version than what was installed before the update.

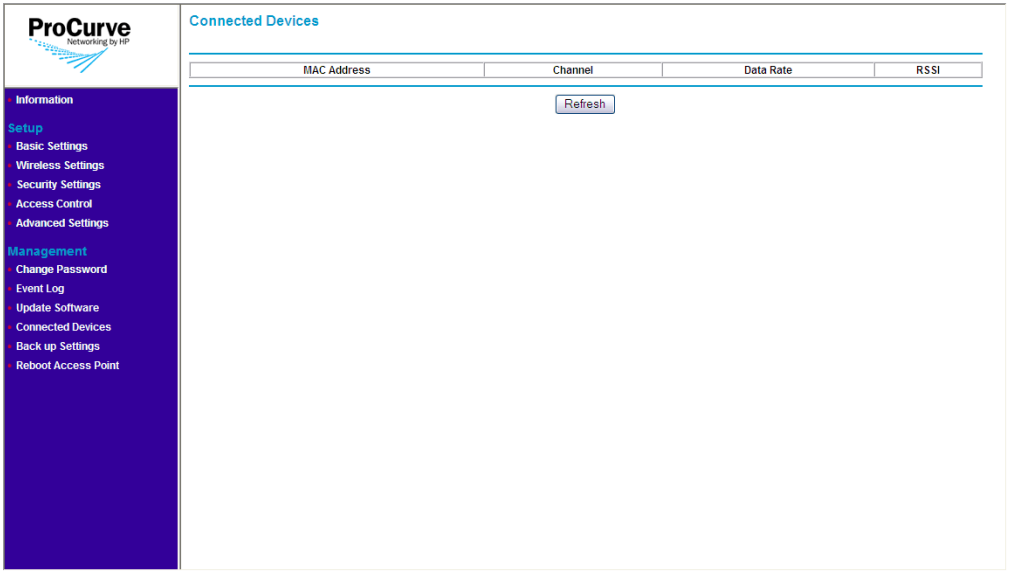
Viewing the List of Connected Devices

You can view which wireless devices are connected to the access point anytime by accessing the Connected Devices page on the Web interface.

To access the page, click **Connected Devices** on the menu. A table appears, which lists the following information about each associated wireless device:

- MAC address: Displays the MAC or physical address of the associated wireless device
- Channel: Displays the current radio channel on which the wireless device is receiving broadcast signal
- Data rate: Displays the transmission speed at which the wireless device is receiving data from the access point. Data rates shown on this page will depend on the type of associated wireless device. 802.11a and 802.11g devices can have data rates up to 54Mbps, while 802.11b devices can only have up to 11Mbps.
- RSSI: Displays the received signal strength of the wireless device on the current wireless channel. The higher the RSSI, the better the signal. The strongest signal will have an RSSI of 100.

Figure 5-5. Connected Devices Page



Backing Up and Restoring Configuration

To back up the current access point configuration:

1. On the menu, click **Back Up Settings**. The Back Up Settings page appears.
2. Click **Back Up** under Save a Copy of Current Settings. A browser dialog box appears, as your browser attempts to download the configuration file from the access point.
3. Click **Save**. The Save As dialog box appears.
4. Choose a location where to save the configuration file and, if you want, change the file name. The default file name is `AP10ag_backup.cfg`. If you are changing the file name, you should include the current date in the file name for ease of identification.
5. Click **Save**.
6. Start Windows Explorer, and then browse to the location where you save the configuration file, and then verify that it has been downloaded successfully.

To restore a backup configuration:

1. On the menu, click **Back Up Settings**. The Back Up Settings page appears.
2. Click **Browse** under Restore Saved Setting from a File.
3. When the Choose File dialog box appears, browse to the location where you saved the backup configuration file.
4. Select the backup file (default file name is `AP10ag_backup.cfg`), and then click **Open**.
5. Click **Restore**. A confirmation message appears.

CAUTION

Restoring settings from a backup configuration file will overwrite all current access point settings, including the IP address, password, and access control. Make sure that you are restoring the correct backup file.

6. Click **OK** to restore settings from the backup file and overwrite the current settings. The message **Please wait...** appears as the access point restores the backup configuration file. When the access point has completed the restore process, the following message appears:

   Access Point is rebooting.....

   PLEASE WAIT until re-directed to Information page.

The browser refreshes, and the Information page appears.

Rebooting the Access Point

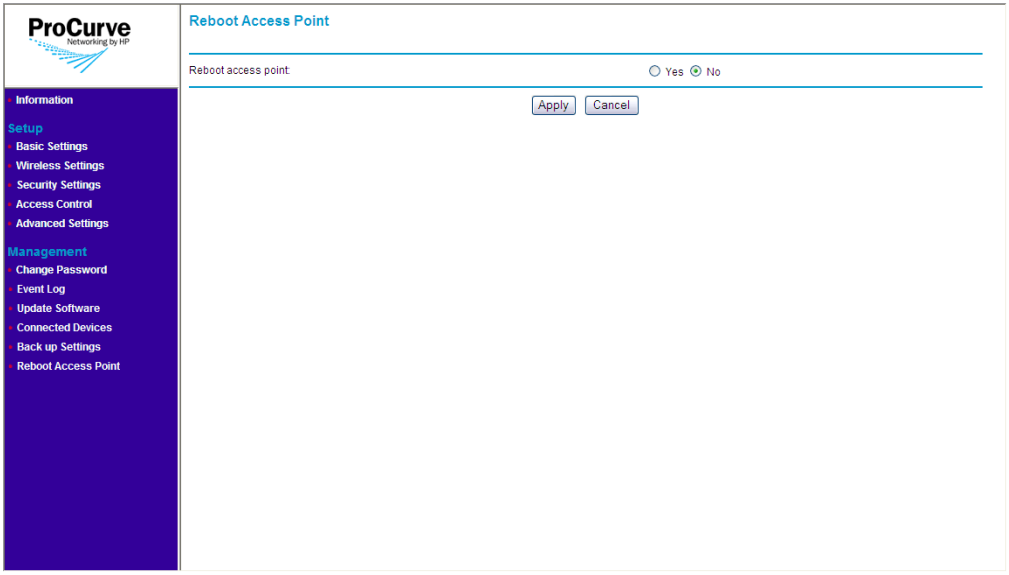
If you feel that the access point is not operating normally, try rebooting the device. This clears memory resources in use and can help restore normal operation.

Note that rebooting the access point will temporarily disconnect any wireless clients and devices that are connected to it. If you have users on the network that are connected to the Internet through the access point, they will be temporarily disconnected. Their connection will be restored as soon as the access point has completed rebooting.

You can reboot the access point by pressing the Reset to Default button (on the rear of the access) for one to three seconds. Alternatively, you can click **Reboot Access Point** on the Web interface to perform the same action.

Refer to the procedure below for instructions on how to reboot the access point from the Web interface.

Figure 5-6. Reboot Page



To reboot the access point:

1. On the menu, click **Reboot Access Point**.
2. In **Reboot access point**, click **Yes**.
3. Click **Apply**. A confirmation message appears.
4. Click **OK**. The following message appears:

Access Point is rebooting.....

PLEASE WAIT until re-directed to Information page.

When the access point has rebooted, the logon dialog box appears.

5. Enter your user name and password to log back on to the Web interface.

Troubleshooting

This chapter describes how to troubleshoot your ProCurve Wireless Access Point 10ag. Note that this document describes troubleshooting mostly from a hardware perspective.

This chapter describes the following:

Basic Troubleshooting Tips

Most problems are caused by the following situations. Check for these items first when starting your troubleshooting:

- **Connecting to devices that have a fixed full-duplex configuration.** By default, the RJ-45 port uses auto-negotiation to determine the duplex mode. That is, when connecting to attached devices, the access point will operate in one of two ways to determine the link speed and the communication mode (half duplex or full duplex):
  - If the connected device is also configured to use auto-negotiation, the access point will automatically negotiate both link speed and communication mode.
  - If the connected device has a fixed configuration, for example 100 Mbps, at half or full duplex, the access point will automatically sense the link speed, but will default to a communication mode of *half* duplex.

  Because the Access Point 10ag behaves in this way *(in compliance with the IEEE 802.3-2005 standard)*, if a device connected to the access point has a fixed configuration at *full* duplex, the device will not connect correctly to the access point. The result will be high error rates and very inefficient communications between the access point and the device.

All devices connected to the Access Point 10ag should be configured to auto-negotiate. To correct this problem you have to manually set the access point's RJ-45 port to match the duplex mode used by the attached device.

- **Faulty or loose cables.** Look for loose or obviously faulty connections. If the cables appear to be OK, make sure the connections are secure. If that does not correct the problem, try a different cable.
- **Non-standard cables.** Non-standard and miswired cables may cause network collisions and other network problems, and can seriously impair network performance. Use a new correctly-wired cable or compare your cable to the cable in Appendix B, Access Point Port and Network Cables for pinouts and correct cable wiring. A category 5 cable tester is a recommended tool for every 100Base-TX network installation.
- **Improper network topologies.** It is important to make sure you have a valid network topology. Common topology faults include excessive cable length and excessive repeater delays between end nodes. If you have network problems after recent changes to the network, change back to the previous topology. If you no longer experience the problems, the new topology is probably at fault. A sample network topology is shown at the end of Chapter 2.
- **Mobile users cannot connect to the network.** Make sure that the access point and wireless clients and devices are configured with compatible security settings. Check to ensure that the wireless device is within the maximum range supported by the access point. Also verify that the wireless device has been configured with an IP address compatible with the attached network, either manually or via DHCP.

For more information on possible network problems and their solutions, see **Customer Care** > **Support** > **Reference Library** at www.procurve.com.

Diagnosing with the LEDs

Table 6-1 shows LED patterns on the access point that indicate problem conditions.

1. Check in the table for the LED pattern that you see on your access point.
2. Refer to the corresponding diagnostic tip on the next few pages.

Table 6-1. LED Error Indicators

LED Pattern Indicating Problems			Diagnostic Tips
Power LED	**Radio LEDs**	**LAN LED**	
Off with power cord plugged in	*	*	**1**
Off without power cord plugged in, but linked to a PoE source	*	*	**2**
Prolonged on or off during initialization†	Prolonged on or off during initialization†	Prolonged on or off during initialization†	**3**
On	Off	*	**4**
On	*	Off with cable connected	**5**
On	*	On, but the port is not communicating	**6**

*** This LED is not important for the diagnosis.**
† Initialization takes between 30 seconds and one minute after a power on or reset.

Diagnostic Tips

Tip	Problem	Solution
1	The access point is not plugged into an active AC power source, or the access point's AC power adapter may have failed.	1. Verify that the power cord is plugged into an active power source and to the access point's AC power adapter. Make sure these connections are secure. 2. Try power-cycling the access point by unplugging and plugging the power cord back in. 3. If the Power LED is still not on, verify that the AC power source works by plugging another device into the outlet. Or try plugging the access point into a different outlet or try a different power cord. If the power source and power cord are OK and this condition persists, the access point's AC power adapter may have failed. Call your HP-authorized network reseller, or use the electronic support services from HP to get assistance.
2	The access point is not receiving power from the PoE source.	1. Verify that access point's 10/100Base-TX port is attached to a PoE source device. 2. Verify that the PoE source device is powered on, and that the PoE function has been administratively enabled on the source port attached to the access point.
3	The access point has experienced a software failure during initialization.	After a power on or reset, the LEDs indicate stages of the system initialization. If there is a software failure during initialization, the LED pattern indicates at which stage the failure occurred. The normal LED sequence during initialization is as follows: Stage 1. Power LED on. System initialization has started. Stage 2. Both LAN LEDs blink once. The boot ROM has successfully initialized. Stage 3. One LAN LED on. The operating system kernel has successfully loaded. Stage 4. LAN LED on only. The operating system is mounting the file system. Stage 5. LAN and 11a/b/g LEDs on. Radio drivers have been successfully loaded. Stage 6. LAN, 11a/b/g, and 11b/g LEDs on. The access point software is initializing. Stage 7. Normal LED operation. Initialization has completed successfully. The entire initialization sequence takes between 30 seconds (normal reset) and one minute (factory default reset). If one of the above LED patterns display longer than one minute, a failure has occurred. Do the following: 1. Reset the access point by power cycling the access point. 2. If the fault indication reoccurs, take note of the LED pattern and contact your HP-authorized network reseller, or use the electronic support services from HP to get assistance.
4	Wireless link has been administratively disabled.	Verify that the wireless port has not been disabled through an access point configuration change. You can use the Web browser interface to determine the state of the wireless port and re-enable the port if necessary. Also verify that the country/region code has been set.
5	The 10/100Base-TX network connection is not working properly.	Try the following procedures: • Verify that both ends of the cabling, at the access point and the connected device, are connected properly. • Verify the connected device and access point are both powered *on* and operating correctly. • Verify duplex operation (see page 6-1). • If these procedures don't resolve the problem, try using a different cable.

Hardware Diagnostic Tests

Testing the Access Point by Resetting It

If you believe that the access point is not operating correctly, you can reset the access point. To reset the access point, either:

- Unplug and plug in the power cord (power-cycling).
- Press the Reset to Default button on the back of the access point for one to three seconds (until the LEDs start to blink rapidly).

CAUTION

If you press the Reset to Default button for more than five seconds, you will reset the board and reload the factory default settings. See "Restoring Factory Default Configuration" on page 6-6.

Power-cycling the access point and pressing the Reset to Default (button for one to three seconds) both cause the access point to perform its system initialization, which normally resolves any temporary operational problems.

Checking the Access Point's LEDs

The system initialization is successful when the Power LED is on and the other LEDs are in a normal operating state after approximately one minute. If the LED pattern is different than this for longer than one minute, there may be a problem with the access point.

See "Diagnosing with the LEDs" on page 6-3 for information on interpreting the LED patterns.

Testing Twisted-Pair Cabling

Network cables that fail to provide a link or provide an unreliable link between the access point and the connected network device may not be compatible with the IEEE 802.3 Type 10Base-T, or 100Base-TX standards. The twisted-pair cables attached to the Access Point 10ag must be compatible with the appropriate standards. To verify that your cable is compatible with these standards, use a qualified cable test device.

Testing Access Point-to-Device Network Communications

You can perform the following communication test to verify that the network is operating correctly between the access point and any connected device that can respond correctly to the communication test.

- Ping Test -- a network layer test used on IP networks that sends test packets to any device identified by its IP address

Testing End-to-End Network Communications

Both the access point and the cabling can be tested by running an end-to-end communications test -- a test that sends known data from one network device to another through the access point. You can run a PING test to verify that the entire communication path between the two network devices is functioning correctly.

Restoring Factory Default Configuration

As part of your troubleshooting process on the Access Point 10ag, it may become necessary to return the access point's configuration to its factory default settings. This process momentarily interrupts the access point's operation and reboots the access point. When restoring the factory default configuration, all settings are cleared, including the manager password and any IP address.

CAUTION

Restoring factory defaults removes all access point configuration changes that you have made from the factory default settings. This includes the IP address, password, access control list, and radio interface settings. Returning the configuration of these features to their factory default settings may result in network connectivity issues.

If the access point has a valid configuration, and you are restoring the factory default settings for a reason other than configuration problems, you should save the access point configuration prior to performing the factory default reset. Then, after the reset and resolution of the original problem, you can restore the saved configuration to the access point.

You can restore factory default configuration either by pressing the Reset to Default button on the rear panel, or by clicking the **Erase** button on the Back Up Settings page.

To restore to factory default using the Reset to Default button:

1. Using a pointed object such as the tip of a ballpoint pen or a straightened clip, press the Reset to Default button for more than five seconds. The LEDs flash rapidly (about 10 times per second).
2. As soon as the LEDs (except the Power LED) shut off, release the Reset to Default button.

The access point resets to factory defaults and reboots.

To restore to factory default from the Web interface:

1. Log on to the Web interface.
2. On the menu, click **Back Up Settings**. The Back Up Settings page appears.
3. Under Revert to Factory Default Settings, click **Erase**. The following confirmation message appears:

   Loading the Factory Default Settings will erase all the current settings.

4. Click **OK** to continue.

   The following message appears:

   Please wait....
   Access Point is rebooting.....
   PLEASE WAIT until re-directed to Information page.

When the access point has completed restoring its settings to factory default, the Web interface refreshes and displays the Information page. If the access point was using an IP address other than the default, you may see a Page Not Found message in your browser. This is because the access point has already reverted to its default IP address, **192.168.1.14**, which may be incompatible with your current network settings.

HP Customer Care Services

If you are still having trouble with your access point, Hewlett-Packard offers support 24 hours a day, seven days a week through the use of a number of automated electronic services. The ProCurve Networking Web site, www.procurve.com, provides up-to-date support information under **Customer Care**.

Additionally, your HP-authorized network reseller can provide you with assistance, both with services that they offer and with services offered by HP.

Before Calling Support

To make the support process most efficient, before calling your networking dealer or HP Support, you first should retrieve the following information:

Information Item	Information Location
• product identification	• the front of the access point, Access Point 10ag (J9140A or J9141A)
• details about the access point's status including the software version and a copy of the access point configuration	• Web interface: Information page
• copy of your network topology map, including network addresses assigned to the relevant devices	• your network records

Specifications

Physical

Width:	178 mm
Depth:	103 mm
Height:	34 mm
Weight:	285 g

Electrical

Adapter	
AC voltage:	100-240 volts, 0.5A, 50/60 Hz
DC voltage:	12 volts, 1.25A (max)
Power consumption:	15 watts (max)

Note: Power can also be provided to the access point through the Ethernet port based on IEEE 802.3af Power over Ethernet (PoE) specifications. The access point is a Class 3 device, that is, the maximum power required is in the range of 6.49 to 12.95 watts. When both PoE is provided and the adapter is plugged in, PoE is turned off.

Japanese Power Cord Statement

製品には、同梱された電源コードをお使い下さい。
同梱された電源コードは、他の製品では使用出来ません。

Environmental

	Operating	Non-Operating
Temperature:	0°C to 40°C (32°F to 104°F) PoE mode	-40°C to 70°C (-40°F to 158°F)
Relative humidity: (non-condensing)	15% to 95%	10% to 90%
Maximum altitude:	3.05 Km (10,000 ft)	

Connectors

- The 10/100 Mbps RJ-45 twisted-pair port is compatible with the IEEE 802.3u 100Base-TX and IEEE 802.3 Type 10Base-T standards.

  Note: To provide Power over Ethernet to the access point, all 4 pairs of wires must be connected for any network cable attached to this port.

Safety

Complies with:

- IEC 60950-1: 2001
- EN 60950-1: 2002
- UL 60950-1 1st Ed.
- CAN/CSA-C22.2 No. 60950-1-03

EMC Compliance (Class B)

Complies with:

- FCC Part 15.107 and 15.109
- ICES-003 (Canada)
- VCCI

Radio Signal Certification

Complies with:

- FCC Part 15, Subpart C and E
- RSS-210 (Canada), Issue 7 (June 2007)
- EN300.328 v1.7.1 (2006-10)
- EN 301.893 V1.2.3 (2003-08)

- ARIB RCR STD-T66 (Ch 1~13), STD-33 (Ch 14), STD-71 (802.11a)
- DGT LP0002 (Taiwan)

Immunity

- EN 301.489-1 v1.6.1 (2005-09)
- EN 301.489-17 V1.2.1 (2002-08)
- EN 60601-1-2

Wireless

802.11a

Radio Standard:	IEEE 802.11a
Radio Technology:	Orthogonal Frequency Division Multiplexing (OFDM)
Data Rate:	6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel
Operating Frequency:	5.15 ~ 5.25 GHz (lower band) US, Canada, Japan, ETSI 5.25 ~ 5.35 GHz (middle band) Taiwan, Japan, ETSI 5.725~5.85 GHz (upper band) US, Canada, Taiwan 5.47 ~ 5.725 GHz ETSI
Maximum Channels:	FCC/IC/NCC: 9, ETSI: 19, MKK: 8
Modulation Type:	BPSK, QPSK, 16QAM, 64QAM
Media Access Protocol:	CSMA/CA with ACK
Transmit Output Power:	18 dBm (max)

802.11b/g

Radio Standard:	IEEE 802.11b/g
Radio Technology:	Direct Sequence Spread Spectrum (DSSS) Orthogonal Frequency Division Multiplexing (OFDM)
Data Rate:	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel
Operating Frequency:	2.4 ~ 2.4835 GHz (US, Canada, Taiwan, ETSI) 2.4 ~ 2.497 GHz (Japan)
Maximum Channels:	FCC/IC/NCC: 1-11, ETSI: 1-13, MKK: 1-13 (802.11g), 1-14 (802.11b)
Modulation Type:	BPSK, QPSK, 16QAM, 64QAM / OFDM, BPSK, QPSK, CCK / DSSS
Media Access Protocol:	CSMA/CA with ACK
Transmit Output Power:	18 dBm (max)

Antenna Type and Gain

Antenna Type: Dipole

Antenna Gain: 2.4GHz ~ 2.5GHz 1.78 (dBi)
5.15GHz ~ 5.25GHz 1.65 (dBi) FCC/IC/MKK/ETSI
5.25GHz ~ 5.35GHz 1.4 (dBi) ETIS/ECC/MKK
5.470GHz ~ 5.725GHz 2.28 (dBi) ETSI
5.725GHz ~ 5.85GHz 1.78 (dBi) FCC/IC/NCC

Receiver Sensitivity

Radio	ProCurve Access Point 10ag NA (J9140A)	ProCurve Access Point 10ag (J9141A)
802.11b (typical)	11Mbps @ -87dBm; 5.5Mbps @ -91dBm; 2Mbps @ -92dBm; 1Mbps @ -97dBm	11Mbps @ -87dBm; 5.5Mbps @ -89dBm; 2Mbps @ -91dBm; 1Mbps @ -94dBm
802.11g (typical)	54Mbps @ -74dBm; 48Mbps @ -75dBm; 36Mbps @-80dBm; 24Mbps @ -83dBm; 18Mbps @-86dBm; 12Mbps @ -88dBm; 9Mbps @ -90dBm; 6Mbps @ -91dBm	54Mbps @ -75dBm; 48Mbps @ -77dBm; 36Mbps @ -81dBm; 24Mbps @ -84dBm; 18Mbps @-87dBm; 12Mbps @ -88dBm; 9Mbps @ -89dBm; 6Mbps @ -90dBm
802.11a (typical)	54Mbps @ -70dBm; 48Mbps @ -72dBm; 36Mbps @-78dBm; 24Mbps @ -81dBm; 18Mbps @-85dBm; 12Mbps @ -87dBm; 9Mbps @ -89dBm; 6Mbps @ -90dBm	54Mbps @ -70dBm; 48Mbps @ -72dBm; 36Mbps @-78dBm; 24Mbps @ -81dBm; 18Mbps @-84dBm; 12Mbps @ -87dBm; 9Mbps @ -88dBm; 6Mbps @ -89dBm

Access Point Port and Network Cables

This appendix includes access point connector information and network cable information for cables that should be used with the Access Point 10ag, including minimum pin-out information and specifications for twisted-pair cables.

Note

Incorrectly wired cabling is the most common cause of problems for LAN communications. You should work with a qualified LAN cable installer for assistance with your cabling requirements.

Access Point Ports

The fixed RJ-45 10/100Base-TX port on the access point accepts 100-ohm unshielded twisted-pair cable with RJ-45 connectors as described on the next page.

Twisted-Pair Cables

10 Mbps Operation	Category 5 100-ohm unshielded twisted-pair (UTP), complying with IEEE 802.3 Type 10Base-T specifications, fitted with RJ-45 connectors
100 Mbps Operation	Category 5 100-ohm UTP cable, complying with IEEE 802.3u 100Base-TX specifications, fitted with RJ-45 connectors

Twisted-Pair Cable/Connector Pin-Outs

The access point includes one 10/100Base-TX port. This port uses Auto-MDIX, which means that you can use either straight-through or crossover twisted-pair cables to connect the access point to a switch.

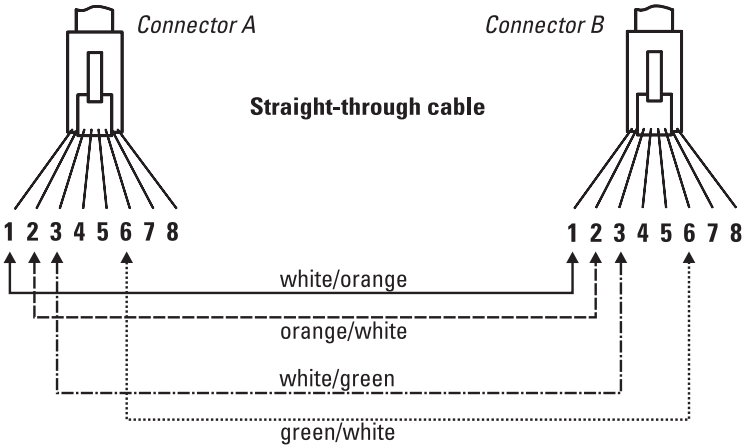
Other Wiring Rules:

- All twisted-pair wires used for 10 Mbps, and 100 Mbps operation must be twisted through the entire length of the cable. The wiring sequence must conform to EIA/TIA 568-B (not USOC). See "Twisted-Pair Cable Pin Assignments" later in this appendix for a listing of the signals used on each pin.
- For 10 Mbps connections to the ports, you can use Category 5 unshielded twisted-pair cable, as supported by the IEEE 802.3 Type 10Base-T standard.
- For 100 Mbps connections to the ports, use 100-ohm Category 5 UTP cable only, as supported by the IEEE 802.3u Type 100Base-TX standard.
- To provide Power over Ethernet to the access point, all 4 pairs must be connected for any network cable attached to this port; the cable must meet ISO/DIS 11801 Class D requirements and IEEE 802.3af requirements.

Straight-Through Twisted-Pair Cable for 10 Mbps or 100 Mbps Network Connections

Because the 10/100 port on the access point supports Auto-MDIX operation, you can use either a "straight-through" or "crossover" cable for network connections to PCs, servers, hubs, or switches.

Cable Diagram



Note

Pins 1 and 2 on connector "A" *must* be wired as a twisted pair to pins 1 and 2 on connector "B".
Pins 3 and 6 on connector "A" *must* be wired as a twisted pair to pins 3 and 6 on connector "B".
Pins 4, 5, 7, and 8 are not used for transmitting or receiving data, although they must be wired straight-through in the cable to support Power over Ethernet.

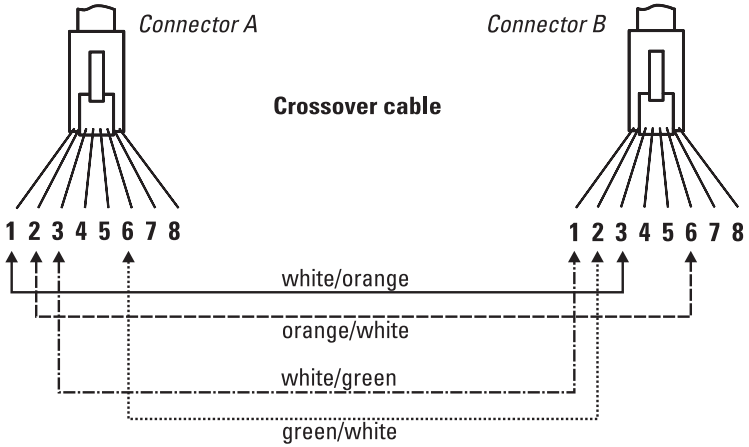
Pin Assignments

Access Point End (MDI)		**Hub or Switch Port, or Other MDI-X Port End**	
Signal	**Pins**	**Pins**	**Signal**
receive +	1 ←	1	transmit +
receive -	2 ←	2	transmit -
transmit +	3 →	3	receive +
transmit -	6 →	6	receive -

Crossover Twisted-Pair Cable for 10 Mbps or 100 Mbps Network Connection

Because the 10/100 port on the access point supports Auto-MDIX operation, you can use either a "straight-through" or "crossover" cable for network connections to PCs, servers, hubs, or switches.

Cable Diagram



Note

Pins 1 and 2 on connector "A" *must* be wired as a twisted pair to pins 3 and 6 on connector "B".
Pins 3 and 6 on connector "A" *must* be wired as a twisted pair to pins 1 and 2 on connector "B".
Pins 4, 5, 7, and 8 are not used for transmitting or receiving data, although they must be wired straight-through in the cable to support Power over Ethernet.

Pin Assignments

Access Point End (MDI)		**Computer, Transceiver, or Other MDI Port End**	
Signal	**Pins**	**Pins**	**Signal**
receive +	1	6	transmit -
receive -	2	3	transmit +
transmit +	3	2	receive -
transmit -	6	1	receive +

C

Safety and EMC Regulatory Statements

Safety Information

Documentation reference symbol. If the product is marked with this symbol, refer to the product documentation to get more information about the product.

WARNING — A WARNING in the manual denotes a hazard that can cause injury or death.

CAUTION — A CAUTION in the manual denotes a hazard that can damage the equipment or create a non-compliant condition.

Do not proceed beyond a WARNING or CAUTION notice until you have understood the hazardous conditions and have taken appropriate steps.

Grounding
Depending on the product model, your product will be classified either as a safety class I or safety class II compliant device. Class I devices require a connection to earth ground (3-terminal plug), while class II devices incorporate a 2-terminal plug.

Class I: There must be an uninterruptible safety earth ground from the main power source to the product's power cord or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

Class II: Safety class II-compliant devices include supplemental insulation to protect against electric shock, and do not require a connection to earth ground.

For LAN connections:

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.

- LAN cables may occasionally be subject to hazardous transient voltages (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.
- This product and all interconnected equipment must be installed indoors within the same building, including all associated LAN connections as described by Environment A of the IEEE 802.3af standard.

Servicing
There are no user-serviceable parts inside this product. Any servicing, adjustment, maintenance, or repair must be performed only by service-trained personnel.

This product does not have a power switch; it is powered on when the power cord is plugged in.

Informations concernant la sécurité

Symbole de référence à la documentation. Si le produit est marqué de ce symbole, reportez-vous à la documentation du produit afin d'obtenir des informations plus détaillées.

WARNING — Dans la documentation, un WARNING indique un danger susceptible d'entraîner des dommages corporels ou la mort.

CAUTION — Un texte de mise en garde intitulé CAUTION indique un danger susceptible de causer des dommages à l'équipement.

Ne continuez pas au-delà d'une rubrique WARNING ou CAUTION avant d'avoir bien compris les conditions présentant un danger et pris les mesures appropriées.

Bases
Suivant le modèle, votre produit sera classé comme un équipement conforme à la classe de sécurité I ou II. Les équipements de la classe I doivent être raccordés à la terre (fiche 3 broches), tandis que les équipements de la classe II intègrent une fiche 2 broches.

Classe I : La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entrée, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débranchez le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Classe II : Les équipements conformes à la classe II incluent une isolation supplémentaire pour la protection contre les chocs électriques et ne doivent pas forcément être raccordés à la terre.

Pour les connexions LAN :

- Si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité sont convenablement interconnectées.
- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précaution.
- Ce produit et tous les équipements interconnectés doivent être installés à l'intérieur, dans le même bâtiment, y compris toutes les connexions LAN, comme indiqué dans la norme IEEE 802.3af (Environnement A).

Dépannage
Aucune pièce à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

Cet appareil ne comporte pas de commutateur principal ; la mise sous tension est effectuée par branchement du cordon d'alimentation.

Hinweise zur Sicherheit

Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

WARNING	Eine WARNING in der Dokumentation symbolisiert eine Gefahr, die Verletzungen oder sogar Todesfälle verursachen kann.
CAUTION	CAUTION in der Dokumentation symbolisiert eine Gefahr, die dis Gerät beschädigen kann.
	Fahren Sie nach dem Hinweis WARNING oder CAUTION erst fort, nachdem Sie den Gefahrenzustand verstanden und die entsprechenden Maßnahmen ergriffen haben.

Erdung
Je nach Produktmodell wird Ihr Produkt als Gerät nach Sicherheitsklasse I oder Sicherheitsklasse II eingestuft. Für Geräte der Klasse I ist eine Verbindung mit Erdung (3-poliger Stecker) erforderlich, während Geräte der Klasse II einen 2-poligen Stecker enthalten.

Klasse I: Es muss eine ununterbrochene Sicherheitserdung von der Hauptstromquelle bis zum Stromversorgungskabel des Produkts oder dem mitgelieferten Stromversorgungskabel vorhanden sein. Wenn es wahrscheinlich ist, dass der Schutz nicht mehr besteht, trennen Sie das Stromkabel, bis die Erdung wiederhergestellt wurde.

Klasse II: Geräte gemäß Sicherheitsklasse II weisen eine Zusatzisolierung zum Schutz vor Stromschlägen auf und erfordern keine Erdungsverbindung.

Für LAN-Verbindungen:

- Wenn Ihr LAN ein Gebiet umfasst, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, dass die Sicherheitserdungen fest untereinander verbunden sind.
- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetzt werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponier-ter Metallbestandteile des Netzwerkes Vorsicht walten lassen.
- Dieses Produkt und sämtliche angeschlossene Ausrüstung einschließlich aller zugehörigen LAN-Verbindungen müssen in den Innenräumen desselben Gebäudes installiert werden, wie in der Norm IEEE 802.3af für Umgebung A beschrieben.

Wartung
Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedienungspersonal durchgeführt werden.

Dieses Gerät hat keinen Netzschalter; es wird beim Anschließen des Netzkabels eingeschaltet.

Considerazioni sulla sicurezza

Simbolo di riferimento alla documentazione. Se il prodotto è contrassegnato da questo simbolo, fare riferimento alla documentazione sul prodotto per ulteriori informazioni su di esso.

WARNING	La dicitura WARNING denota un pericolo che può causare lesioni o morte.
CAUTION	La dicitura CAUTION denota un pericolo che può danneggiare le attrezzature.
	Non procedere oltre un avviso di WARNING o di CAUTION prima di aver compreso le condizioni di rischio e aver provveduto alle misure del caso.

Messa a terra
A seconda del modello, il prodotto sarà classificato come dispositivo di sicurezza conforme alla classe I o alla classe II. I dispositivi di classe I richiedono una connessione alla messa a terra (connettore a 3 terminali), mentre quelli di classe II hanno un connettore a 2 terminali incorporato.

Classe I: deve essere presente una messa a terra di sicurezza di continuità dalla fonte di alimentazione principale al cavo di alimentazione del prodotto o al gruppo dei cavi di alimentazione. Se questa protezione non dovesse più sembrare accoppiata, scollegare il cavo di alimentazione fino a che non viene ripristinata la messa a terra.

Classe II: i dispositivi conformi alla sicurezza di classe II includono un isolamento supplementare per la protezione dalle scosse elettriche e non richiedono una connessione alla messa a terra.

Per le connessioni LAN:

- se la vostra LAN copre un'area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;
- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d'alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.
- Questo prodotto e tutti i dispositivi collegati, incluse le connessioni LAN associate, devono essere installati all'interno dello stesso edificio come descritto dallo standard IEEE 802.3af (Environment A).

Manutenzione
Nessun componente di questo prodotto può essere riparato dall'utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

Questo apparato non possiede un commutatore principale; si mette scotto tensione all'inserirsi il cavo d'alimentazione.

Consideraciones sobre seguridad

Símbolo de referencia a la documentación. Si el producto va marcado con este símbolo, consultar la documentación del producto a fin de obtener mayor información sobre el producto.

WARNING — Una WARNING en la documentación señala un riesgo que podría resultar en lesiones o la muerte.

CAUTION — Una CAUTION en la documentación señala un riesgo que podría resultar en averías al equipo.

No proseguir después de un símbolo de WARNING o CAUTION hasta no haber entendido las condiciones peligrosas y haber tomado las medidas apropiadas.

Toma de tierra
Dependiendo del modelo del producto, este aparecerá clasificado como dispositivo que cumple los requisitos de la categoría de seguridad I o de la categoría de seguridad II. Los dispositivos de categoría de seguridad I requieren una conexión a tierra (clavija de 3 terminales), mientras que los dispositivos de categoría de seguridad II incorporan una clavija de 2 terminales.

Categoría I: debe haber una puesta a tierra continua desde la fuente principal de energía hasta el cable de la corriente del producto o el grupo de cables proporcionado. Siempre que quepa la posibilidad de que la protección haya sido dañada, desconecte el cable de la corriente hasta que la toma de tierra haya sido restaurada.

Categoría II: los dispositivos de categoría de seguridad II incluyen un aislamiento adicional como protección contra descargas eléctricas y no requieren una conexión a tierra.

Para conexiones LAN:

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.
- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.
- Este producto y todos los equipos interconectados deben instalarse en interior, dentro del mismo edificio, incluyendo todas las conexiones LAN asociadas como se describe en Environment (entornos) A del estándar IEEE 802.3af.

Servicio
Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

Este producto no tiene interruptor de potencia; se activa cuando se enchufa el cable de alimentación.

Safety Information (Japan)

マニュアル参照記号。製品にこの記号がついている場 合は、マニュアルを参照し、注意事項等をご確認くだ さい。

WARNING　マニュアル中の「WARNING」は怪我や死亡事故の原因となる危険を示します。

CAUTION　マニュアル中の「CAUTION」は装置の破損または規定に準拠しない状況を招く原因となる危険を示します。

「WARNING」や「CAUTION」の項目は読み飛ばさず、危険性に関する記述を確実に理解し、適切な手順に従った上で次へ進んでください。

接地について

お使いの装置は、製品モデルによって安全性クラス I または安全性クラス II 準拠装置として分類されます。クラスI装置は3芯アース付プラグを使用して接続する必要があります。クラスII装置は2芯プラグを使用します。

クラス I : 主電源から装置の電源コードまたは付属の電 源コード セットの間には、連続かつ安全な接地が存在する必要があります。安全性が損なわれた可能性のある場合、電源コードを外し、安全性が確保されるまで再接続しないでください。

クラス II : 安全性クラス II に準拠している装置は電気ショックから装置を保護するための、補助的な絶縁材を使用しています。このため、接地は不要です。

LAN 接続について:

- お使いの LAN が複数の配電システムにより電力を受けている領域をカバーしている場合には、ぞれぞれのシステムの安全接地が確実に相互に結合されていることを確認してください。
- LAN ケーブルは雷、配電設備の電力網での障害など、危険な過渡電圧にさらされる場合があります。露出した金属部分の取り扱いには十分ご注意ください。
- 本製品およびすべての相互に接続されている機器は、IEEE 802.3af 標準の Environment A に規定されているとおり、LAN 接続を含め、同じ建物の室内に設置されている必要があります。

修理と点検

本製品の内部には、ユーザーが修理できる部品はありません。サービス、調整、保守、および修理は、サービス訓練を受けた専門家にお任せください。

本製品には主電源スイッチがありません。電源コードを接続すると、電源が入ります。

Safety Information (Korea)

설명서 참조 기호. 제품에 이 기호가 표시되어 있는 경우 제품 설명서를 참조하여 해당 제품에 대한 자세한 내용을 확인하십시오.

경고 — 이 설명서에 표시된 경고는 상해 또는 사망을 초래할 위험이 있음을 의미합니다.

주의 — 이 설명서에 표시된 주의는 장비를 손상하거나 호환되지 않는 상황을 발생시킬 수 있는 위험이 있음을 의미합니다.

반드시 경고 또는 주의 정보에서 설명한 위험 상황을 파악하고 적절한 절차를 수행한 후 진행해야 합니다.

접지

제품은 제품 모델에 따라 안전 1등급 또는 안전 2등급 호환 장치로 분류됩니다. 안전 1등급 장치에는 접지된 연결 장치(3터미널 플러그)를 사용해야 합니다. 안전 2등급 장치에는 2터미널 플러그가 포함되어 있습니다.

1등급: 주 전원과 제품 전원 코드 또는 공급된 전원 코드 세트를 연결하기 위한 무정전 안전 접지 장치가 반드시 있어야 합니다. 안전상의 위험이 있는 것으로 판단되는 경우 접지가 복구될 때까지 전원 코드를 분리해 둡니다.

2등급: 안전 2등급 호환 장치에는 감전을 예방하기 위한 추가 절연 장치가 포함되어 있으며 접지 연결 장치가 필요하지 않습니다.

LAN 연결 시:

- LAN이 하나 이상의 전원 분배 시스템에서 전원을 제공하는 영역에 걸쳐 있는 경우 접지가 제대로 연결되어 있는지 확인합니다.
- LAN 케이블에 번개 또는 전력망 장애와 같이 전압이 과도하게 공급되어 위험한 상황이 가끔 발생할 수 있습니다. 네트워크에서 노출된 금속 부품을 취급할 때 주의하십시오.
- 모든 LAN 연결을 포함한 이 제품 및 모든 관련 장비는 IEEE 802.3af 표준의 환경 A 조항에 명시된 대로 동일한 건물 내부에 설치해야 합니다.

서비스

이 제품에 있는 어떠한 부품도 사용자가 직접 다루어서는 안 됩니다. 모든 서비스, 조정, 유지 관리 및 수리는 전문 서비스 담당자가 수행해야 합니다.

이 제품에는 전원 스위치가 없고 전원 코드를 연결하면 전원이 켜집니다.

Safety Information (China)

HP网络产品使用安全手册

使用须知

欢迎使用惠普网络产品，为了您及仪器的安全，请您务必注意如下事项:

1. 仪器要和地线相接，要使用有正确接地插头的电源线，使用中国国家规定 的220V 电源。
2. 避免高温和尘土多的地方，否则易引起仪器内部部件的损坏。
3. 避免接近高温，避免接近直接热源，如直射太阳光、暖气等其它发热体。
4. 不要有异物或液体落入机内，以免部件短路。
5. 不要将磁体放置于仪器附近。

警告

为防止火灾或触电事故，请不要将该机放置于淋雨或潮湿处。

安装

安装辅助管理模块，请参看安装指南。

保修及技术支持

如果您按照以上步骤操作时遇到了困难，或想了解其它产品性能，请按以下 方式与我们联络。

如是硬件故障:

1. 与售出单位或当地维修机构联系。
2. 中国惠普有限公司维修中心地址:
   北京市海淀区知春路49号希格玛大厦
   联系电话: 010-62623888 转 6101
   邮政编码: 100080

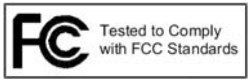
如是软件问题:

1. 惠普用户响应中心热线电话: 010-65645959
2. 传真自动回复系统: 010-65645735

EMC Regulatory Statements

Notice for U.S.A.

Manufacturer's FCC Declaration of Conformity Statement



Product No: J9140A

FCC ID No: B94RSVLC-0702

Regulatory Model No: RSVLC-0702

Manufacturer: Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185 USA

Phone:650-857-1501

For questions regarding this declaration, contact the Product Regulations Manager at the above address or phone number.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: 1) this device may not cause harmful interference, and 2) this device must accept any interference received, including interference that may cause undesired operation.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna

- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/television technician for help

The FCC requires the user to be notified that any changes or modifications made to the device that are not expressly approved by the Hewlett-Packard Company may void the user's authority to operate the equipment.

This device is restricted to **indoor** use when using the 5.15-5.25 GHz band (Channels 36, 40, 44 and 48).

Warning: Exposure to Radio Frequency Radiation

The radiated output power of this device is below the FCC radio exposure limits. Nevertheless, the device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antennas should not be less than 20 cm (8 inches) during normal operation.

Regulatory Model Identification Number

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is RSVLC-0702. The RMN should not be confused with the marketing name (Wireless Access Point 10ag) or the Product Number (J9140A, J9141A).

Notice for Canada

This device complies with the limits for a Class B digital device and conforms to Industry Canada standard ICES-003. Products that contain a radio transmitter comply with Industry Canada standard RSS210 and are labeled with an IC approval number.

Cet appareil numérique de la classe B est conforme à la norme ICES-003 d'Industry Canada. La radio sans fil de ce dispositif est conforme à la certification RSS 210 d'Industry Canada et est étiquetée avec un numéro d'approbation IC.

This device complies with the Class B limits of Industry Canada. Operation is subject to the following two conditions: 1) this device may not cause harmful interference, and 2) this device must accept interference received, including interference that may cause undesired operation.

This device is restricted to indoor use when using the 5.15-5.25GHz band (Channels 36, 40, 44 and 48) to reduce the potential for harmful interference to co-channel mobile satellite systems.

High-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and could cause interference and/or damage to LE-LAN devices.

Notice for European Community

This device complies with the EMC Directive 2004/108/EEC, Low Voltage Directive 2006/95/EC and R&TTE Directive 1999/5/EC. Compliance with these directives implies conformity to harmonized European standards (European Norms) that are listed on the EU Declaration of Conformity that has been issued by HP for this device.

Countries of Operation & Conditions of Use

This device may be used in the following EU and EFTA countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom. Restrictions for indoor vs. outdoor operation, licensing and allowed channels of operation apply in some countries as described below.

Note

The user must use the configuration utility provided with this device to ensure the channels of operation are in conformance with the spectrum usage rules for EU and EFTA countries as described below.

2.4 GHz Operation:

- This device may be operated indoors or outdoors in all EU and EFTA countries using the 2.4GHz band (Channels 1 - 13), except where noted below.
- In Italy, a license is required for outdoor use. Verify with your dealer or directly with the General Direction for Frequency Planning and Management (Direzione Generale Pianificazione e Gestione Frequenze).

  E'necessaria una concessione ministeriale anche per l'uso del prodotto. Verifici per favore con il proprio distributore o direttamente presso la Direzione Generale Pianificazione e Gestione Frequenze.
- In France, this device may use the entire 2400 - 2483.5 MHz band (Channels 1 through 13) for indoor applications. For outdoor use, only the 2400 - 2454 MHz frequency band (Channels 1 through 9) may be used. For the latest requirements, see http://www.art-telecom.fr.

  L'utilisation de cet équipement (LAN sans fil 2,4 GHz) est soumise à certaines restrictions : cet équipement peut être utilisé à l'intérieur d'un bâtiment en utilisant toutes les fréquences de 2400 à 2483,5 MHz (Chaîne 1-13). Pour une utilisation en environnement extérieur, vous devez utiliser les fréquences comprises entre 2400 et 2454 MHz (Chaîne 1-9). Pour les dernières restrictions, voir http://www.art-telecom.fr.

5 GHz Operation:

- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other systems. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document.
- This device employs a radar detection feature required for European Community and EFTA country operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community or EFTA country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.
- This device is restricted to indoor use when operated in EU and EFTA countries using the 5.15-5.35 GHz band (Channels 36, 40, 44, 48, 52, 56, 60 and 64). See the table below for the allowed 5 GHz channels in each band.

Operation Using 5 GHz Channels in the European Community

Frequency Band (MHz)	Allowed Channels	Usage	Maximum EIRP (mW)
5150 - 5250	36, 40, 44, 48	Indoor use only	200
5250 - 5350	52, 56, 60, 64	Indoor use only	200
5470 - 5725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor or outdoor use	1000

Note

In France, operation of this device is limited to 5150 - 5250 MHz (Channels 36, 40, 44 and 48).

En France, l'utilisation est limitée à la plage de fréquences 5150 - 5250 MHz (Canaux 36, 40, 44 et 48).

All ProCurve devices are designed to be compliant with the rules and regulations in locations they are sold and will be labeled as required. Any changes or modifications to ProCurve devices, not expressly approved by HP, could void the user's authority to operate this device.

EU Declaration of Conformity

DECLARATION OF CONFORMITY
according to ISO/IEC 17050-1 and EN 17050-1

DoC #: RSVLC-0702-01

Supplier's Name: Hewlett-Packard Company
Manufacturer's Address: 8000 Foothills Blvd., Roseville, CA 95747 U.S.A.

declares, that the product

Product Name: Procurve Wireless Access Point 10ag

Product Number(s): J9140A, J9141A

Regulatory Model No: RSVLC-0702

Product Options:

conforms to the following Product Specifications:

Safety: EN 60950-1:2001

EMC: EN 55022:2006 Class B
EN 61000-3-2:2006
EN 61000-3-3:1995 +A1:2001 +A2:2005
EN 60601-1-2:2001

Telecom: EN 300 328 V1.7.1
EN 301 893 V1.2.3
EN 301 489-1 V1.6.1
EN 301 489-17 V1.2.1
EN 50385:2002

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EEC and the R&TTE Directive 1999/5/EC and carries the CE marking accordingly.

For regulatory identification purposes, this product has been assigned a Regulatory Model Number (RMN). The RMN for your product is RSVLC-0702. The RMN should not be confused with the marketing name (Wireless Access Point 10ag) or the Product Number (J9140A, J9141A).

Roseville, September 18, 2007

Mike Avery, Regulatory Engineering Mgr.

Local contact for regulatory information:
EMEA: Hewlett-Packard GmbH, HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen, Germany
www.hp.com/go/certificates
U.S.: Hewlett-Packard, 3000 Hanover St., Palo Alto, CA 94304, U.S.A. 650-857-1501

Notice for Japan

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

1　この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。

2　万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等（例えば、パーティションの設置など）についてご相談して下さい。

3　その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：日本ヒューレット・パッカード株式会社　ＴＥＬ：０１２０－０１４１２１

Notice for Taiwan

DGT LPD (Low Power Device) Statement:

低功率電波輻射性電機管理辦法

第十四條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十七條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Recycle Statements

Waste Electrical and Electronic Equipment (WEEE) Statements

Disposal of Waste Equipment by Users in Private Household in the European Union

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

Likvidace zařízení soukromými domácími uživateli v Evropské unii

Tento symbol na produktu nebo balení označuje výrobek, který nesmí být vyhozen spolu s ostatním domácím odpadem. Povinností uživatele je předat takto označený odpad na předem určené sběrné místo pro recyklaci elektrických a elektronických zařízení. Okamžité třídění a recyklace odpadu pomůže uchovat přírodní prostředí a zajistí takový způsob recyklace, který ochrání zdraví a životní prostředí člověka. Další informace o možnostech odevzdání odpadu k recyklaci získáte na příslušném obecním nebo městském úřadě, od firmy zabývající se sběrem a svozem odpadu nebo v obchodě, kde jste produkt zakoupili.

Bortskaffelse af affald fra husstande i den Europæiske Union

Hvis produktet eller dets emballage er forsynet med dette symbol, angiver det, at produktet ikke må bortskaffes med andet almindeligt husholdningsaffald. I stedet er det dit ansvar at bortskaffe kasseret udstyr ved at aflevere det på den kommunale genbrugsstation, der forestår genvinding af kasseret elektrisk og elektronisk udstyr. Den centrale modtagelse og genvinding af kasseret udstyr i forbindelse med bortskaffelsen bidrager til bevarelse af naturlige ressourcer og sikrer, at udstyret genvindes på en måde, der beskytter både mennesker og miljø. Yderligere oplysninger om, hvor du kan aflevere kasseret udstyr til genvinding, kan du få hos kommunen, den lokale genbrugsstation eller i den butik, hvor du købte produktet.

Seadmete jäätmete kõrvaldamine eramajapidamistes Euroopa Liidus

See tootel või selle pakendil olev sümbol näitab, et kõnealust toodet ei tohi koos teiste majapidamisjäätmetega kõrvaldada. Teie kohus on oma seadmete jäätmed kõrvaldada, viies need elektri- ja elektroonikaseadmete jäätmete ringlussevõtmiseks selleks ettenähtud kogumispunkti. Seadmete jäätmete eraldi kogumine ja ringlussevõtmine kõrvaldamise ajal aitab kaitsta loodusvarasid ning tagada, et ringlussevõtmine toimub viisil, mis kaitseb inimeste tervist ning keskkonda. Lisateabe saamiseks selle kohta, kuhu oma seadmete jäätmed ringlussevõtmiseks viia, võtke palun ühendust oma kohaliku linnakantselei, majapidamisjäätmete kõrvaldamise teenistuse või kauplusega, kust Te toote ostsite.

Laitteiden hävittäminen kotitalouksissa Euroopan unionin alueella

Jos tuotteessa tai sen pakkauksessa on tämä merkki, tuotetta ei saa hävittää kotitalousjätteiden mukana. Tällöin hävitettävä laite on toimitettava sähkölaitteiden ja elektronisten laitteiden kierrätyspisteeseen. Hävitettävien laitteiden erillinen käsittely ja kierrätys auttavat säästämään luonnonvaroja ja varmistamaan, että laite kierrätetään tavalla, joka estää terveyshaitat ja suojelee luontoa. Lisätietoja paikoista, joihin hävitettävät laitteet voi toimittaa kierrätettäväksi, saa ottamalla yhteyttä jätehuoltoon tai liikkeeseen, josta tuote on ostettu.

Élimination des appareils mis au rebut par les ménages dans l'Union européenne

Le symbole apposé sur ce produit ou sur son emballage indique que ce produit ne doit pas être jeté avec les déchets ménagers ordinaires. Il est de votre responsabilité de mettre au rebut vos appareils en les déposant dans les centres de collecte publique désignés pour le recyclage des équipements électriques et électroniques. La collecte et le recyclage de vos appareils mis au rebut indépendamment du reste des déchets contribue à la préservation des ressources naturelles et garantit que ces appareils seront recyclés dans le respect de la santé humaine et de l'environnement. Pour obtenir plus d'informations sur les centres de collecte et de recyclage des appareils mis au rebut, veuillez contacter les autorités locales de votre région, les services de collecte des ordures ménagères ou le magasin dans lequel vous avez acheté ce produit.

Entsorgung von Altgeräten aus privaten Haushalten in der EU

Das Symbol auf dem Produkt oder seiner Verpackung weist darauf hin, dass das Produkt nicht über den normalen Hausmüll entsorgt werden darf. Benutzer sind verpflichtet, die Altgeräte an einer Rücknahmestelle für Elektro- und Elektronik-Altgeräte abzugeben. Die getrennte Sammlung und ordnungsgemäße Entsorgung Ihrer Altgeräte trägt zur Erhaltung der natürlichen Ressourcen bei und garantiert eine Wiederverwertung, die die Gesundheit des Menschen und die Umwelt schützt. Informationen dazu, wo Sie Rücknahmestellen für Ihre Altgeräte finden, erhalten Sie bei Ihrer Stadtverwaltung, den örtlichen Müllentsorgungsbetrieben oder im Geschäft, in dem Sie das Gerät erworben haben

Απόρριψη άχρηστου εξοπλισμού από χρήστες σε ιδιωτικά νοικοκυριά στην Ευρωπαϊκή Ένωση

Το σύμβολο αυτό στο προϊόν ή τη συσκευασία του υποδεικνύει ότι το συγκεκριμένο προϊόν δεν πρέπει να διατίθεται μαζί με τα άλλα οικιακά σας απορρίμματα. Αντίθετα, είναι δική σας ευθύνη να απορρίψετε τον άχρηστο εξοπλισμό σας παραδίδοντάς τον σε καθορισμένο σημείο συλλογής για την ανακύκλωση άχρηστου ηλεκτρικού και ηλεκτρονικού εξοπλισμού. Η ξεχωριστή συλλογή και ανακύκλωση του άχρηστου εξοπλισμού σας κατά την απόρριψη θα συμβάλει στη διατήρηση των φυσικών πόρων και θα διασφαλίσει ότι η ανακύκλωση γίνεται με τρόπο που προστατεύει την ανθρώπινη υγεία και το περιβάλλον. Για περισσότερες πληροφορίες σχετικά με το πού μπορείτε να παραδώσετε τον άχρηστο εξοπλισμό σας για ανακύκλωση, επικοινωνήστε με το αρμόδιο τοπικό γραφείο, την τοπική υπηρεσία διάθεσης οικιακών απορριμμάτων ή το κατάστημα όπου αγοράσατε το προϊόν.

Készülékek magánháztartásban történő selejtezése az Európai Unió területén

A készüléken, illetve a készülék csomagolásán látható azonos szimbólum annak jelzésére szolgál, hogy a készülék a selejtezés során az egyéb háztartási hulladéktól eltérő módon kezelendő. A vásárló a hulladékká vált készüléket köteles a kijelölt gyűjtőhelyre szállítani az elektromos és elektronikai készülékek újrahasznosítása céljából. A hulladékká vált készülékek selejtezéskori begyűjtése és újrahasznosítása hozzájárul a természeti erőforrások megőrzéséhez, valamint biztosítja a selejtezett termékek környezetre és emberi egészségre nézve biztonságos feldolgozását. A begyűjtés pontos helyéről bővebb tájékoztatást a lakhelye szerint illetékes önkormányzattól, az illetékes szemételtakarító vállalattól, illetve a terméket elárusító helyen kaphat.

Smaltimento delle apparecchiature da parte di privati nel territorio dell'Unione Europea

Questo simbolo presente sul prodotto o sulla sua confezione indica che il prodotto non può essere smaltito insieme ai rifiuti domestici. È responsabilità dell'utente smaltire le apparecchiature consegnandole presso un punto di raccolta designato al riciclo e allo smaltimento di apparecchiature elettriche ed elettroniche. La raccolta differenziata e il corretto riciclo delle apparecchiature da smaltire permette di proteggere la salute degli individui e l'ecosistema. Per ulteriori informazioni relative ai punti di raccolta delle apparecchiature, contattare l'ente locale per lo smaltimento dei rifiuti, oppure il negozio presso il quale è stato acquistato il prodotto.

Nolietotu iekārtu iznīcināšanas noteikumi lietotājiem Eiropas Savienības privātajās mājsaimniecībās

Šāds simbols uz izstrādājuma vai uz tā iesaiņojuma norāda, ka šo izstrādājumu nedrīkst izmest kopā ar citiem sadzīves atkritumiem. Jūs atbildat par to, lai nolietotās iekārtas tiktu nodotas speciāli iekārtotos punktos, kas paredzēti izmantoto elektrisko un elektronisko iekārtu savākšanai otrreizējai pārstrādei. Atsevišķa nolietoto iekārtu savākšana un otrreizējā pārstrāde palīdzēs saglabāt dabas resursus un garantēs, ka šīs iekārtas tiks otrreizēji pārstrādātas tādā veidā, lai pasargātu vidi un cilvēku veselību. Lai uzzinātu, kur nolietotās iekārtas var izmest otrreizējai pārstrādei, jāvēršas savas dzīves vietas pašvaldībā, sadzīves atkritumu savākšanas dienestā vai veikalā, kurā izstrādājums tika nopirkts.

Vartotojų iš privačių namų ūkių įrangos atliekų šalinimas Europos Sąjungoje

Šis simbolis ant gaminio arba jo pakuotės rodo, kad šio gaminio šalinti kartu su kitomis namų ūkio atliekomis negalima. Šalintinas įrangos atliekas privalote pristatyti į specialią surinkimo vietą elektros ir elektroninės įrangos atliekoms perdirbti. Atskirai surenkamos ir perdirbamos šalintinos įrangos atliekos padės saugoti gamtinius išteklius ir užtikrinti, kad jos bus perdirbtos tokiu būdu, kuris nekenkia žmonių sveikatai ir aplinkai. Jeigu norite sužinoti daugiau apie tai, kur galima pristatyti perdirbtinas įrangos atliekas, kreipkitės į savo seniūniją, namų ūkio atliekų šalinimo tarnybą arba parduotuvę, kurioje įsigijote gaminį.

Verwijdering van afgedankte apparatuur door privé-gebruikers in de Europese Unie

Dit symbool op het product of de verpakking geeft aan dat dit product niet mag worden gedeponeerd bij het normale huishoudelijke afval. U bent zelf verantwoordelijk voor het inleveren van uw afgedankte apparatuur bij een inzamelingspunt voor het recyclen van oude elektrische en elektronische apparatuur. Door uw oude apparatuur apart aan te bieden en te recyclen, kunnen natuurlijke bronnen worden behouden en kan het materiaal worden hergebruikt op een manier waarmee de volksgezondheid en het milieu worden beschermd. Neem contact op met uw gemeente, het afvalinzamelingsbedrijf of de winkel waar u het product hebt gekocht voor meer informatie over inzamelingspunten waar u oude apparatuur kunt aanbieden voor recycling.

Pozbywanie się zużytego sprzętu przez użytkowników w prywatnych gospodarstwach domowych w Unii Europejskiej

Ten symbol na produkcie lub jego opakowaniu oznacza, że produktu nie wolno wyrzucać do zwykłych pojemników na śmieci. Obowiązkiem użytkownika jest przekazanie zużytego sprzętu do wyznaczonego punktu zbiórki w celu recyklingu odpadów powstałych ze sprzętu elektrycznego i elektronicznego. Osobna zbiórka oraz recykling zużytego sprzętu pomogą w ochronie zasobów naturalnych i zapewnią ponowne wprowadzenie go do obiegu w sposób chroniący zdrowie człowieka i środowisko. Aby uzyskać więcej informacji o tym, gdzie można przekazać zużyty sprzęt do recyklingu, należy się skontaktować z urzędem miasta, zakładem gospodarki odpadami lub sklepem, w którym zakupiono produkt.

Descarte de Lixo Elétrico na Comunidade Européia

Este símbolo encontrado no produto ou na embalagem indica que o produto não deve ser descartado no lixo doméstico comum. É responsabilidade do cliente descartar o material usado (lixo elétrico), encaminhando-o para um ponto de coleta para reciclagem. A coleta e a reciclagem seletivas desse tipo de lixo ajudarão a conservar as reservas naturais; sendo assim, a reciclagem será feita de uma forma segura, protegendo o ambiente e a saúde das pessoas. Para obter mais informações sobre locais que reciclam esse tipo de material, entre em contato com o escritório da HP em sua cidade, com o serviço de coleta de lixo ou com a loja em que o produto foi adquirido.

Likvidácia vyradených zariadení v domácnostiach v Európskej únii

Symbol na výrobku alebo jeho balení označuje, že daný výrobok sa nesmie likvidovať s domovým odpadom. Povinnosťou spotrebiteľa je odovzdať vyradené zariadenie v zbernom mieste, ktoré je určené na recykláciu vyradených elektrických a elektronických zariadení. Separovaný zber a recyklácia vyradených zariadení prispieva k ochrane prírodných zdrojov a zabezpečuje, že recyklácia sa vykonáva spôsobom chrániacim ľudské zdravie a životné prostredie. Informácie o zberných miestach na recykláciu vyradených zariadení vám poskytne miestne zastupiteľstvo, spoločnosť zabezpečujúca odvoz domového odpadu alebo obchod, v ktorom ste si výrobok zakúpili.

Odstranjevanje odslužene opreme uporabnikov v zasebnih gospodinjstvih v Evropski uniji

Ta znak na izdelku ali njegovi embalaži pomeni, da izdelka ne smete odvreči med gospodinjske odpadke. Nasprotno, odsluženo opremo morate predati na zbirališče, pooblaščeno za recikliranje odslužene električne in elektronske opreme. Ločeno zbiranje in recikliranje odslužene opreme prispeva k ohranjanju naravnih virov in zagotavlja recikliranje te opreme na zdravju in okolju neškodljiv način. Za podrobnejše informacije o tem, kam lahko odpeljete odsluženo opremo na recikliranje, se obrnite na pristojni organ, komunalno službo ali trgovino, kjer ste izdelek kupili.

Eliminación de residuos de equipos eléctricos y electrónicos por parte de usuarios particulares en la Unión Europea

Este símbolo en el producto o en su envase indica que no debe eliminarse junto con los desperdicios generales de la casa. Es responsabilidad del usuario eliminar los residuos de este tipo depositándolos en un "punto limpio" para el reciclado de residuos eléctricos y electrónicos. La recogida y el reciclado selectivos de los residuos de aparatos eléctricos en el momento de su eliminación contribuirá a conservar los recursos naturales y a garantizar el reciclado de estos residuos de forma que se proteja el medio ambiente y la salud. Para obtener más información sobre los puntos de recogida de residuos eléctricos y electrónicos para reciclado, póngase en contacto con su ayuntamiento, con el servicio de eliminación de residuos domésticos o con el establecimiento en el que adquirió el producto.

Bortskaffande av avfallsprodukter från användare i privathushåll inom Europeiska Unionen

Om den här symbolen visas på produkten eller förpackningen betyder det att produkten inte får slängas på samma ställe som hushållssopor. I stället är det ditt ansvar att bortskaffa avfallet genom att överlämna det till ett uppsamlingsställe avsett för återvinning av avfall från elektriska och elektroniska produkter. Separat insamling och återvinning av avfallet hjälper till att spara på våra naturresurser och gör att avfallet återvinns på ett sätt som skyddar människors hälsa och miljön. Kontakta ditt lokala kommunkontor, din närmsta återvinningsstation för hushållsavfall eller affären där du köpte produkten för att få mer information om var du kan lämna ditt avfall för återvinning.

Open Source Licenses

Contents

Overview

This appendix includes the following information:

- Open Source licenses

GPL2 (GNU General Public License, v.2)

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute

them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have

received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.>Copyright (C) 19yy <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.
>
> <signature of Ty Coon>, 1 April 1989Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

LGPL (GNU Lesser General Public License)

GNU LESSER GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, “this License” refers to version 3 of the GNU Lesser General Public License, and the “GNU GPL” refers to version 3 of the GNU General Public License.

“The Library” refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A “Combined Work” is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the “Linked Version”.

The “Minimal Corresponding Source” for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The “Corresponding Application Code” for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information

is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

Index

Numerics

A

B

C

D

E

F

I

L

M

N

O

P

R

S

T

W

May 2008

Manual Part Number
5991-8615