802.11g Wireless LAN Access Point

User Guide

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

·On board of airplanes, or

·In an explosive environment, or

·In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

USA-FCC (Federal Communications Commission) statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause interference, and

2. This device must accept any interference, including interference that may cause undesired operation of this device.

FCC Radio Frequency Exposure statement

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65 and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices.

The radiated output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When nearby persons has to be kept to ensure RF exposure compliance, in order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antennas and the user should not be less than 20 cm.

FCC Interference Statement

This equipment 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. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications.

However, there is no guarantee that 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 and correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.

2. Increase the distance between the equipment and the receiver.

3. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

4. Consult the dealer or an experienced radio/TV technician for help.

Export restrictions

This product or software contains encryption code that may not be exported or transferred from the US of Canada without an approved US Department of Commerce export license.

Safety Information

Your device contains a low power transmitter. When device is transmitted it sends out radio frequency (RF) signal.

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328-2 has been conducted. These are considered relevant and sufficient.

CE in which Countries where the product may be used freely:

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.

France: The use of other channels that the channel 10 through 13 is prohibited by law.

TABLE OF CONTENT

ABOUT THIS GUIDE

Congratulations on your purchase of this IEEE 802.11g Wireless LAN Access Point. This manual helps to features the innovating wireless technology that can help you build a wireless network easily! This manual contains detailed instructions in operation of this product. Please keep this manual for future reference.

With a WLAN (IEEE 802.11g) Access Point, a mobile computer can share data with another mobile computer in a wireless way. Easy-to-use utilities are bundled with WLAN Access Point for configuration and monitoring purposes.

WLAN networking can wirelessly transmit and receive data, minimizing the need for wired connections, at a speed of up to Fifty-four megabit per second. With WLAN networking, you can locate your PC wherever you want without wires and cables.

WLAN networking provides users with an access to real-time information anywhere in their organization. The mobility provides productivity and service, which are not available under wired networks.

Purpose

This manual discusses how to install the WLAN Access Point.

Overview of this User's Guide

Introduction. Describes the WLAN Access Point and its features.

Unpacking and Setup. Helps you get started with the basic installation of the WLAN Access Point.

Hardware Installation. Describes the LED indicators of the AP.

Software Installation. Tells how to setup the driver and the utility setting.

Technical Specifications. Lists the technical (general, physical and environmental) specifications of the WLAN Access Point.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Access Point.

Unpacking

Open the box of the Access Point and carefully unpack it. The box should contain the following items:

- One Wireless Access Point
- One external power adapter
- One CD-Rom (User's guide)

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the Wireless Access Point can be performed using the following steps:

- Locate an optimum location for the Wireless LAN Access Point (AP). The best place for your AP is usually the center of your wireless network, with line of sight to all of your mobile stations.
- Visually inspect the Ethernet RJ45 port connector and make sure that it is fully plugged in to the system's Ethernet switch/hub port.
- Fix the direction of the antennas. Try to place the AP in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.
- Visually inspect if the Power Adapter was fully plugged to the device power jack.

HARDWARE INSTALATION

LED Indicator

The figure below shows the LED Indicator of the Wireless LAN Access Point.

PWR/Power

This indicator lights green when the Access Point receives power. Otherwise, it turns off.

LAN (Link/ACT)

The indicator lights green when the LAN port is connected to a 100Mbps Ethernet station, the indicator blinks green while transmitting or receiving data on the 100Mbps Ethernet network.

WLAN (Link)

The indicator always blinks green while the wireless AP is always broadcasting packets.

Rear Panel

The figure below shows the rear panel of the Access Point

Rear Panel
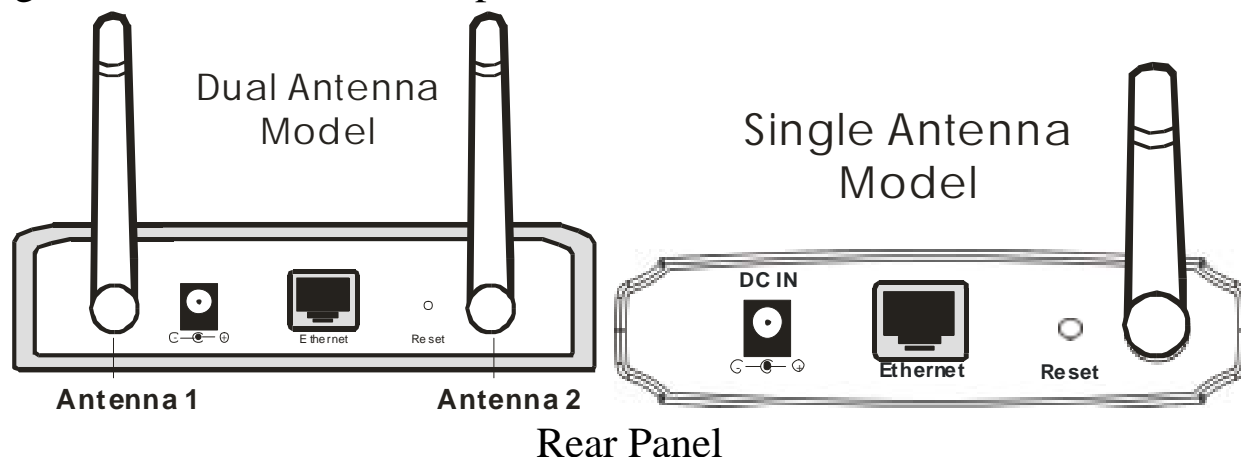
Ethernet

Ethernet uplink port with 10/100Mbps Fast Ethernet connections, connect this port to switch/hub.

Reset

The Reset function is to reset the setting back to factory default setting, once you press the "RESET" button within 10 seconds, the LED of the WLAN will turn off. And when the Access Point is ready, the WLAN LED will start blinking.

And the other function is when the AP is locked, press the reset button to unlock it.
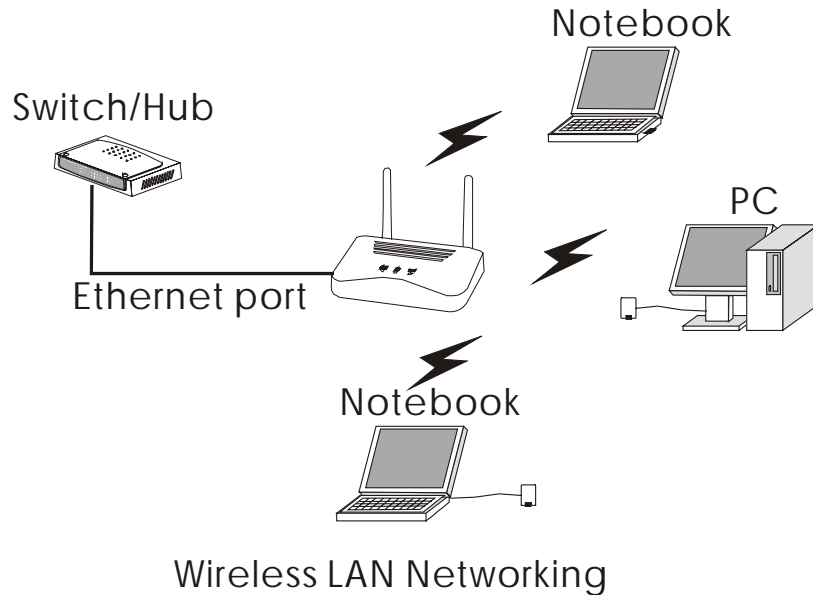
DC Power

Connect the Power Adapter DC plug to the AP's power jack.

Antenna

There are two antennas in the rear panel, when you need to connect extended Antenna, connect to Antenna 2 for the extended antenna. When you are using one antenna model, connect the extended antenna directly to the antenna screw in the rear panel.

Hardware connections

Wireless LAN Networking

Connect to the Switch/Hub

1. Plug in one end of the RJ45 network cable to the Switch/Hub port,
2. Plug in the other end of the RJ45 network cable to the Wireless Access Point.

Check the installation

The control LEDs of the Access Point are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected, the Power, LAN and WLAN port link LEDs of the Internet Broadband Router will light up indicating a normal status.
2. If the LAN Port's Link indicator does not light up then check the RJ-45 cable if it is firmly feed to the RJ45 port, while the LAN is link up to the Switch/Hub, the LAN port's LED will light up.

CONFIGURING THE WIRELESS LAN ACCESS POINT

The Wireless Access Point has a Web GUI interface for the configuration. The AP can be configured through the Web Browser. A network manager can manage, control and monitor the AP from the local LAN. This section indicates how to configure the AP to enable its functions.

Login to the Wireless AP through WLAN

Before configuring the Wireless AP through WLAN, make sure that the SSID, Channel and the WEP was set properly.

The default setting of the Wireless AP that you will use:

SSID: default

Channel: 6

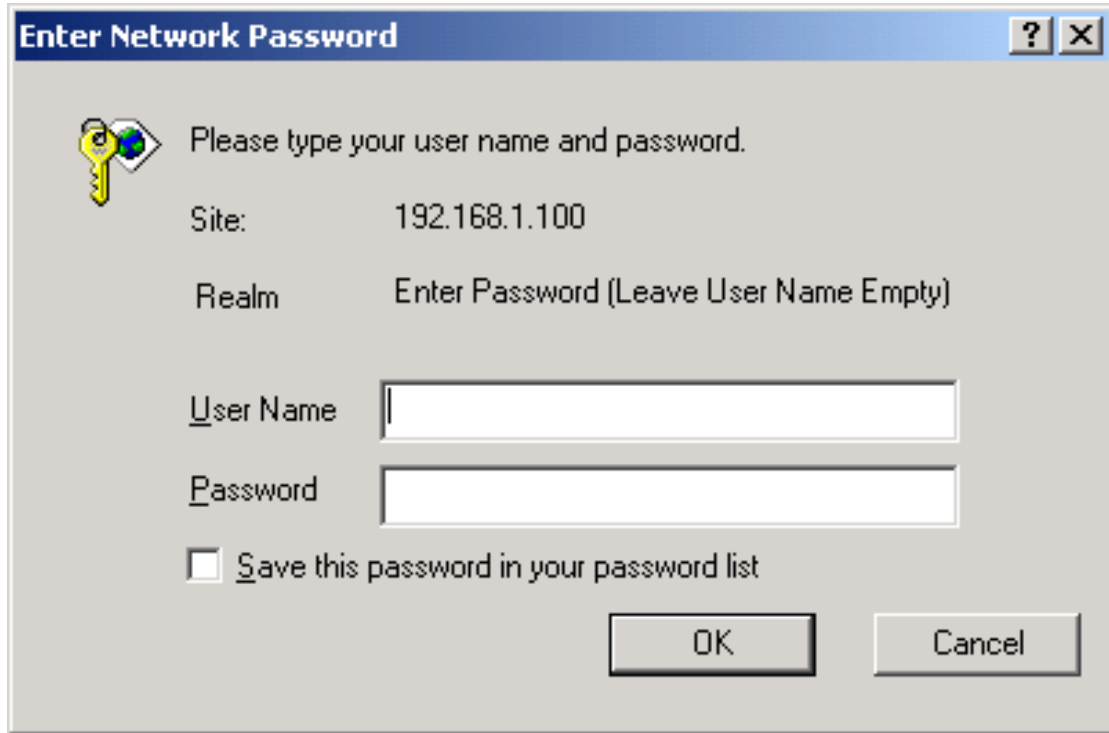WEP Encryption: disable

Login

Before you configure this device, note that when the AP is configured through an Ethernet connection, make sure the manager PC must be set on same the **IP network**. For example, when the default network address of the default IP address of the AP is ***192.168.1.100***, then the manager PC should be set at 192.168.1.x (where x is a number between 1 and 254), and the default subnet mask is 255.255.255.0.

Open Internet Explorer 5.0 or above Web browser.

Enter IP address ***http://192.168.1.100*** (the factory-default IP address setting) to the address location.

When there is a screen needs to enter the Network password, it means that there is a password settle, type in the password you entered before. There is no need to enter any password when you first login the AP, the default setting is without password.

Type a name or leave the username dialog box empty to login, the system will check only the password that was set in the system before.
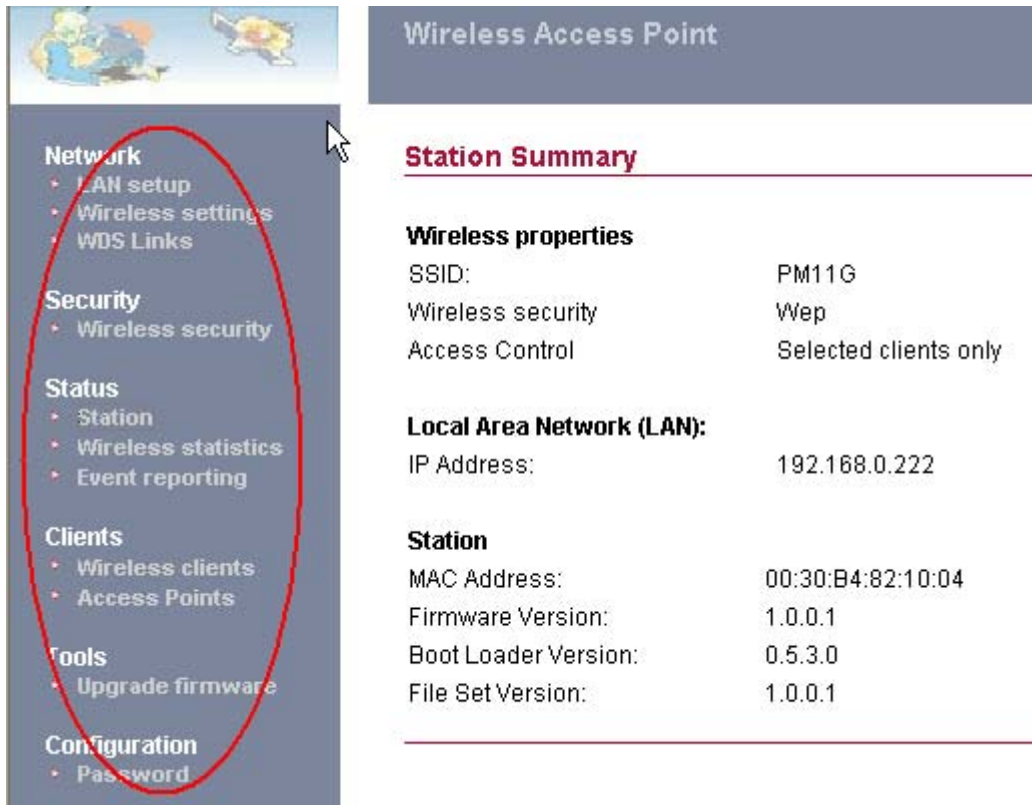
Main Screen of the Access Point

The screen will show the station summary of the AP when you login to the AP.

There are six main functions included in the left side of the main screen: Network, Security, Status, Clients, Tools and Configuration. Point the selections in the left side of the menu screen.

Network

The Network Function can configure the LAN Setup, Wireless settings and WDS Links of the Access Point.

I. LAN Setup

The LAN Setup function can configure the basic LAN setting:

Dynamic (DHCP Client): Click on the Dynamic for dynamic IP address allocation from the Server PCs.

Static IP: Click on the Static IP to fill up the IP Address, Subnet Mask and Gateway from the Networking Manager.

Local Area Network (LAN)

Primary Address Selection

- ◉ Dynamic
- ○ Static IP

IP Address	192.168.1.100
Subnet mask	255.255.255.0
Gateway	0.0.0.0

II. Wireless Settings

The Wireless Settings contain two settings, Radio Setting and Wireless LAN Setting.

Wireless Settings

Radio settings:

Regulatory Domain: FCC change region...

Wireless LAN:

Wireless network name (SSID):   default

Band: 2.4 GHz (Mixed)   change policy...

Radio Channel: 6

Broadcast SSID: ☑

Cancel   Apply

**Radio Settings:** to configure the Regulatory Domain settings.

➢ **Regulatory Domain:** this is the channel selection of each country regulatory domain, select the country where you are using this Wireless Device, users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of these countries.

Radio settings:

Regulatory Domain:　　　　　ETS change region...

Click on the "change region" button and a window will pop out, select the region in which you are using this AP.
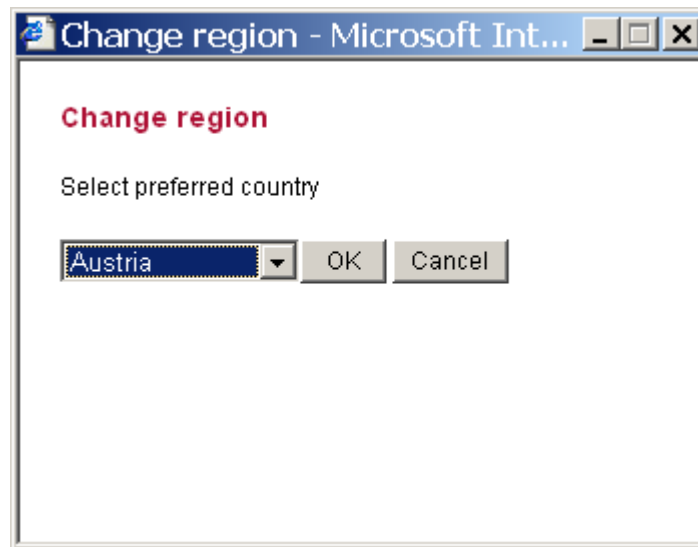

Wireless LAN Settings: to configure the wireless networking settings.

➢ **Wireless Network Name (SSID):** It is an ASCII string up to 32 characters used to identify a WLAN that prevents the unintentional merging of two co-located WLANs. The SSID value must be the same in all stations and AP in the extended WLAN.

➢ **Band:** you can select to change the radio band to mixed mode, G-only or B-only, a window will pop out to change the policy, it may result in a loss of the connection when you are using wireless connection.

Mixed mode: choosing this mode may allow users using both 802.11g and 802.11b.

G-only: choosing this mode may allow users using only 802.11g.

B-only: choosing this mode may allow users using only 802.11b.

➢ **Radio Channel:** there are 14 channels available due to different Regulatory Domain. The channels differ from country to country; select the channel to be used.

➢ **Broadcast SSID:** when enable this function, this AP will broadcast the SSID to the stations; if the function was disable, the stations must know the AP SSID in advance.

III. WDS Links

WDS (Wireless Distribution System) uses wireless media to communicate with other APs. When you enter the screen of the WDS, there are list of other APs will appear, click enable in the left side of the screen and click apply to add the AP to your WDS Link, or click the "Add WDS Link" button to add the APs that you need to add.
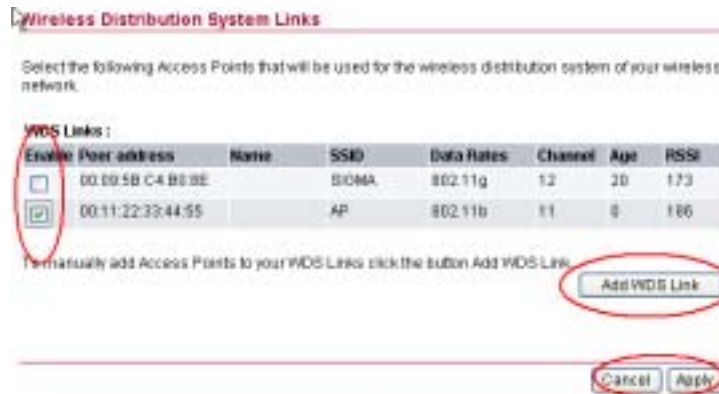
This WDS Link will scan only other APs channel within the range of 3 channels among your AP radio channel, two other ways to connect to the APs that are not listed in the WDS Link.

1. Click the "Add WDS Link" button, a window will pop out, type in the MAC address of the AP that you need to communicate.
2. Change your AP radio channel within the range of 3 channels to scan the AP that you want to connect.

To remove an AP in the WDS Link list, unclick the enable dialog box to remove the WDS Link where you set before.

In Addition, make sure you configure all WDS APs to work on the same radio channel and in the same WEP key.

Security

This function is used to protect wireless communication from eavesdropping. A secondary function of encryption is to prevent unauthorized access to a wireless network, and it can be achieved by using the Encryption function.

This AP provides three modes for Security Encryption, WPA, 802.1x and WEP.

When there are security function enable, it will show check sign or numbers on the left side of the screen.

➢ Check sign means that the function is enable.

➢ The numbers shows that how many Radius servers were set.

I.   Access Control List

Access Control function allows clients whose MAC addresses in the list will be able to connect to this Access Point. When this function is activate, there is no wireless clients will be able to connect to the Access Point unless they are listed in the Access Control list.

➢ **Default Access:** select the Accept will allows the clients on the list to connect to this AP, and select Reject to disable the clients on the list to connect to the AP.

➢ **Specific Clients:** add the MAC address list of the clients that the manager want to control, the manager can control the specific clients in the list to enable or disable accessing with the AP.

II. Radius Server

A RADIUS server is used to authenticate the connection for clients and return authentication key parameters to the users to connect to the wireless networking.

RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

Re-authentication Time: type in how long the seconds that you want to re-authentication with the client.

Click "Add" button to add the Radius Server IP Address, Server UDP port and Secret. The secret is a key between the AP and the Radius Server.

III. Wired Equivalent Privacy (WEP)

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

When choose the encryption to WEP mode, click the "Use WEP Security" to enable the WEP security function, some setting as follow:

- ◆ **64-bits:** selecting the 64bit, you must type 10 values in the following range (0~F, hexadecimal).
- ◆ **128-**bits: selecting the 128bit, you must type 26 values in the following range (0~F, hexadecimal).

Wired Equivalent Privacy (WEP)

☑ Use WEP security
　 Pre-shared Key:
　 ⦿　64-bits　　*********
　 ○　128-bits

IV. 802.1x Security

To address the shortcomings of WEP for authentication, the industry is working towards solutions based on the 802.1x specification, which is based on the Extensible Authentication Protocol (EAP). EAP was designed with flexibility in mind, and it has been used as the basis for a number of network authentication extensions.

Click to enable the 802.1x security function.

802.1X Security

☑ Use 802.1X security
Key Size
○ 64-bits
⦿ 128-bits
Group Key Rekey Settings
⦿ No rekeying
○ Rekey every　60　　minutes
○ Rekey every　10　　x 1000 packets

- ◆ **Key Size:** selecting the 64bit or 128-bit for the key size of the 802.1x security.
- ◆ **Group Key Setting:**
   No Rekeying: the clients will not need to re-key the password to authenticate with the Radius Server.

Rekeying Time: type in the time for when the manager want clients to re-keying the password for authentication and security.

Rekeying packets: type in the numbers of packets in which the manager want to control every client to re-key the password when the number of every 1000 packets was transmitted.

V. Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption.

➢ **Disable WPA Security:** to disable the WPA security.

➢ **Use WPA with Pre-Shared Key:** type in 8 ~ 63 characters inside the dialog box to have the WPA password between the AP and the clients.

➢ **Use WPA with Radius Server:** the authentication between the Radius Server, the AP and the clients using the Group Key Re-key Settings.

No Rekeying: the clients will not need to re-key the password to authenticate with the Radius Server.

Rekeying Time: type in the time for when the manager want clients to re-keying the password for authentication and security.

Rekeying packets: type in the numbers of packets in which the manager want to control every client to re-key the password when the number of every 1000 packets was transmitted.

➢ **Update Group Key:** to update the password when the station or the client leaves the Networking Group (BSS, Basic Service Set).

Wi-Fi Protected Access (WPA)

○ Disable WPA security

○ Use WPA with pre-shared key

Password Phrase   ********   (8-63 characters)

◉ Use WPA with RADIUS server

Group Key Rekey settings:

◉ No rekeying

○ Rekey every   60   minutes

○ Rekey every   10   x 1000 packets

☐ Update Group Key if station leaves BSS

Status

This function will show the statistics of the Station, Wireless Statistics and Event Reporting.

I. Station

This screen will show the status summary of the system.

Station Summary

Wireless properties

SSID:	PM11G
Wireless security	Wep
Access Control	Any client

Local Area Network (LAN):

IP Address:	169.254.16.4
	172.16.5.145

Station

MAC Address:	00:30:B4:82:10:04
Firmware Version:	1.0.0.1
Boot Loader Version:	0.5.3.0
File Set Version:	1.0.0.1

II. Wireless Statistics

This screen shows the statistics of the wireless AP.

Wireless Statistics

	Wireless LAN
Transmitted Fragments	0
Transmitted Multicasts	0
Transmitted Frame Count	903450
Failed Packets	0
Retry Count	0
Multiple Retry Count	0
Duplicate Frames	0
RTS Success Count	0
RTS Failure Count	0
ACK Failure Count	0
Received Fragment Count	0
Received Multicasts	118
FCS Errors	2843990
WEP Undecryptable	0

III. Event Report

This screen shows the event happened on the AP, press "Reset Event Log" to clear the record of the event happened.

Event reporting

The following events are reported by the Access Point:

[Reset eventlog]

Report level	Facility	ID	Description	Count	Occurence
Info	System	102	802.1x authenticator started	1	00m 00d 14:15:12
Notice	System	109	Respawning paed	1	00m 00d 14:15:12
Info	System	104	802.1x authenticator stopped	1	00m 00d 14:15:07
Alert	Kernel	10C	Kernel: <1>offset in paed: 0x0033e8c4	1	00m 00d 14:15:07
Alert	Kernel	10C	Kernel: <1>Brk: 0x0 - 0x0	1	00m 00d 14:15:07
Alert	Kernel	10C	Kernel: <1>Bss: 0x0 - 0x0	1	00m 00d 14:15:07

Clients

This function shows the list of the wireless surrounded this AP.

I. Wireless Clients

This function shows the list of the wireless clients that connected to this AP.

Wireless Clients

Wireless clients

Address	Rate	Quality	RSSI	State	Age
00:05:4E:46:70:BF	24		-38	Forwarding	1

II. Access Points

This function shows the list of the Wireless Access Point that this AP can connect with, this is the list that you can use for WDS Links, refer for the WDS Links on page 10.

Access Points

Detected Access Points

| BSSID	SSID	Data Rates	Channel	Age	RSSI
00:40:F4:82:12:50	default	11 5.5 2 1	6	0	176
00:40:F4:82:1E:6D	SALES	11 5.5 2 1	7	0	163
00:40:F4:AB:CD:EF	CalvinAP	11 5.5 2 1	9	0	168
00:10:91:00:44:2A	default	11 5.5 2 1	6	33	170

Tools

This function will help you to upgrade the firmware of the AP, press the "Upgrade Firmware" button in the left side of the menu screen and a window will pop out.
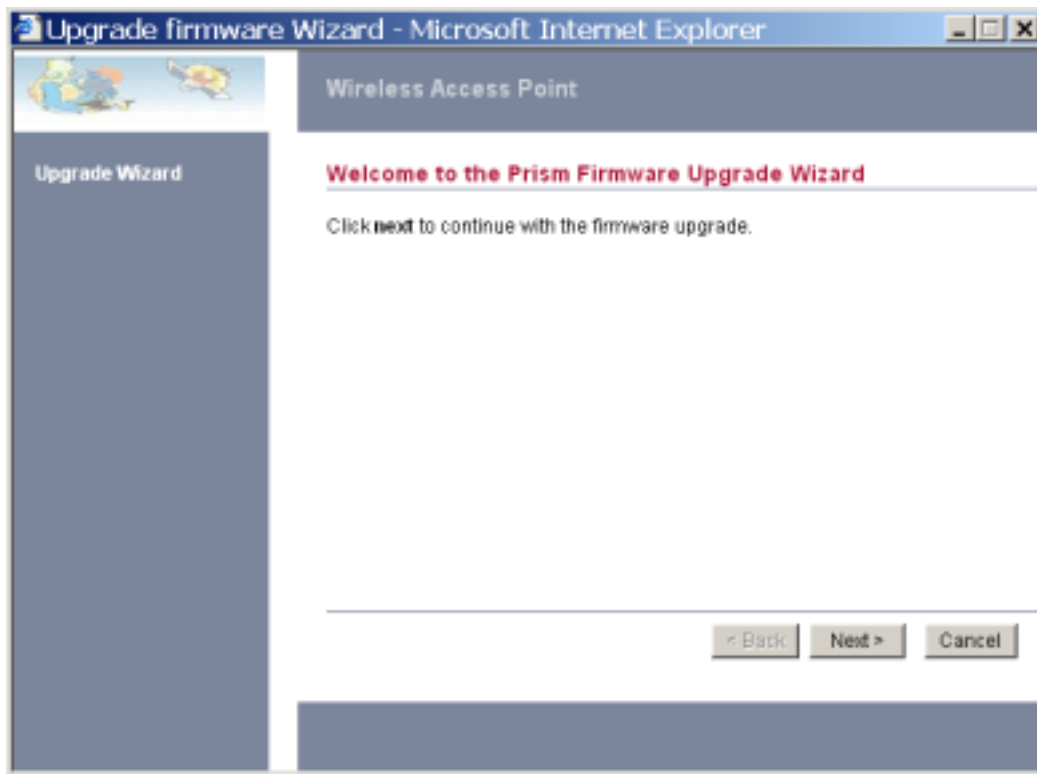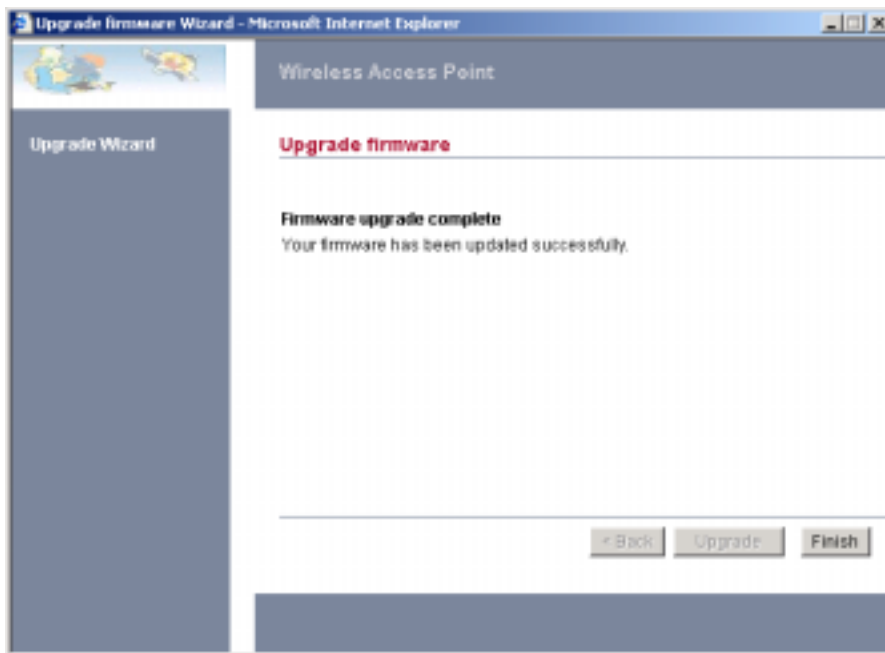

Press "Next ".

Type the firmware file that you need to upgrade inside the dialog box, or press the "Browse" button to find the firmware file location.
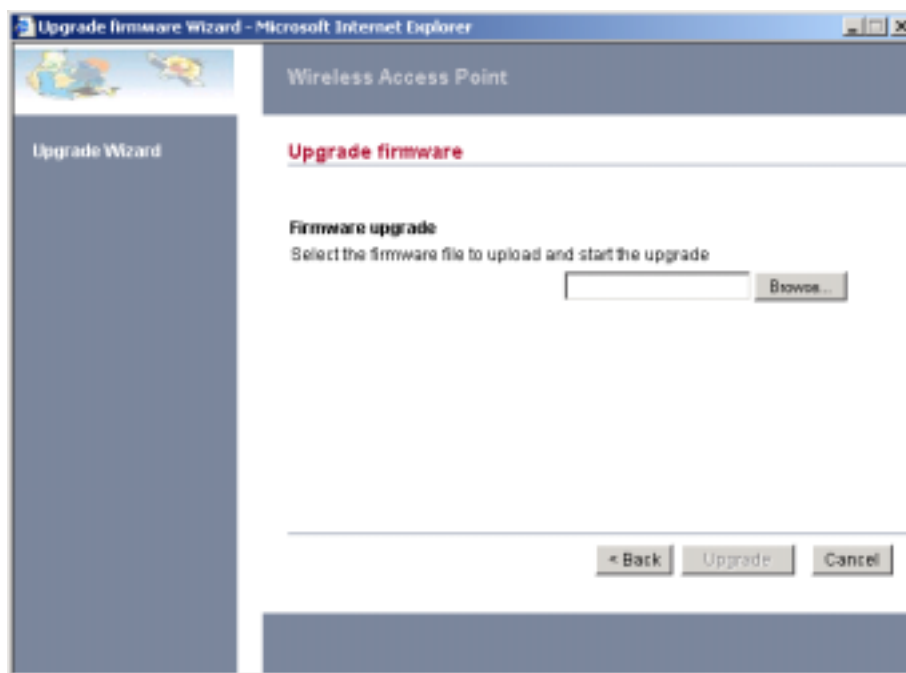
Press "Upgrade" button to proceed the upgrade procedure.

When finish uploading the file to the AP, *do not power off the AP until the "Firmware Upgrade Complete" screen appears.*

Press the "Reset" button on the rear panel of the AP, to set back to factory default setting.

Configuration

I.   Change Password

This function will help you to configure the password of the AP, type in the new password inside the New password and Confirm password dialog box, press the "Change password" button to activate this function.

Security Against Unauthorized Configuration

Change password
Set the password needed to access and configure your Access Point.

New password: _____ (3-16 characters)
Confirm password: _____

[Change password...]

II. Lock Access Point

Lock the Access Point to deny configuration changes to it. You need to have physical access to the Access Point to unlock it, press the reset button on the rear panel of the AP to unlock.

Lock Access Point
Lock the Access Point to deny configuration changes to it. You need to have physical access to the Access Point to unlock it.

[Lock Access Point]

TECHNICAL SPECIFICATIONS

General	
Standards	Standard: IEEE 802.11g IEEE 802.3u 10/100BASE-TX Fast Ethernet
Signal Type:	OFDM (Orthogonal Frequency Division Multiplexing)
Modulation:	QPSK / BPSK / CCK / OFDM
LED Indicators:	Power, LAN (Link/Activity), WLAN (Link)
Frequency Range	2412 ~ 2484 MHz ISM band (channels 1 ~ 14)
Frequency Band:	2.4 GHz
Channel:	1 ~ 11 Channels (US, Canada, China) 1 ~ 13 Channels (Europe) 1 ~ 14 Channels (Japan)
Data Encryption:	64 bit / 128 bit WEP Encryption, WPA
Data Transfer Rate	Fast Ethernet: 100Mbps Wireless: Up to 54Mbps (with Automatic Scale Back)
Receiver Sensitivity	54Mbps: Typical -68dBm @10% PER 11Mbps: Typical -81dBm @8% PER
Transmit Power	802.11g: Minimum 12dBm typically 802.11b: Minimum 15dBm typically
Transmission Range:	Outdoor: 100~300M (depends on environment) Indoor: 50~100M (depends on environment)
Network Cables	10BASET: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA- 568 100-ohm STP (100 m)
Interface	1 x 10/100Mbps RJ45 port
Antenna:	2 x 2dBi Dipole Antenna or 1 x 1dBi Dipole + Printed Antenna
Physical and Environmental	
DC inputs	DC 5V /1.2A
Power Consumption	3W (Max)
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	140 x 98 x 30 mm (W x H x D) without Antenna
EMI:	FCC Class B, CE Mark B,