

### **Copyright Notice**

Copyright © 2005-2015 Handlink Technologies Inc. All rights reserved. No part of this document may be copied, reproduced, or transmitted by any means, for any purpose without prior written permission. Protected by TW patent 223184, JPN patent 3099924 and China patent ZL 03 2 04640.5.

### **Disclaimer**

We shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from furnishing this material, or the performance or use of this product. We reserve the right to change the product specification without notice. Information in this document may change without notice.

### **Trademarks**

Microsoft Win98, Windows 2000 , WinXP, Win Vista and Win7 are registered trademarks of Microsoft Corporation.

**General:** All other brand and product names mentioned herein may be registered trademarks of their respective owners. Customers should ensure that their use of this product does not infringe upon any patent rights. Trademarks mentioned in this publication are used for identification purposes only and are properties of their respective companies.

# Table of Contents

1	Introduction	4
1-1	Package Contents	4
1-2	Features	5
1-3	Precautions	5
1-4	Outlook	5
1-4-1	Top Panel	6
1-4-2	Rear Panel	7
1-5	Technical Specifications	7
1-5-1	Hardware Specifications	7
1-5-2	Software Specifications	9
2	Installation	11
2-1	Installation Requirements	12
2-2	Getting Start	14
3	Configuring the GuestWiFi	15
3-1	Setting Wizard	15
3-2	Advanced Setup	26
3-2-1	MANAGEMENT	27
3-2-3-1	Syslog	27
3-2-3-2	Session Trace	33
3-2-3-3	Bandwidth	35
3-2-3-4	SNMP	36
3-2-2	SECURITY	38
3-2-2-1	Pass Through	38
3-2-2-2	Secure Remote	40
3-2-3	SYSTEM	41
3-2-3-1	System	41
3-2-3-2	WAN/LAN	44
3-2-3-3	Server	51
3-2-3-4	Wireless	54

3-2-4	GUEST SETTING	55
3-2-4-1	Guest ESSID Settings	55
3-2-4-2	Authentication	57
3-2-4-3	Usage Time	59
3-2-4-4	Customization	60
3-2-5	EMPLOYEE ESSID SETTINGS	70
3-3	System Status	71
3-3-1	System	72
3-3-2	Account List	74
3-3-3	Account Log	75
3-3-4	Current User	76
3-3-5	DHCP Clients	77
3-3-6	Session List	77
3-4	System Tools	78
3-4-1	<i>Configuration</i>	79
3-4-2	<i>Firmware Upgrade</i>	80
3-4-3	<i>Boot Code</i>	82
3-4-4	<i>System Account</i>	82
3-4-5	<i>SSL Certificate</i>	84
3-4-6	<i>Pin Command</i>	85
3-4-7	<i>Restart</i>	86
3-4-8	<i>Logout</i>	86
Appendix A	Signal Connection Arrangements	87
Appendix B	Regulations/EMI Compliance	88
LIMITED WARRANTY		89

# 1 Introduction

The GW-1 guestWiFi account generator is designed as 300Mbps high speed wireless gateway for enterprises and schools to provide guests a secure Wi-Fi network in their meeting room, guest lobby, and library. It is deployed by MIS simply as adopting IP Plug and Play technology, all a guest has to do is to generate a guest account with a single click, and with a press of a button the guest ID will be shown on the display instantly. Guests can enjoy high-speed Internet connection and just follow four steps: press the key, find guest SSID, enter ID & WPA/WPA2 Per-Shared Key and Login to Internet; MIS have no need to re-configure any of their device IP settings including DHCP, DNS, Proxy, dynamic and static IP address assignments.

The GW-1 enables MIS to secure the Internet access in different network segments for guests and employees as it enhances security and firewall functionalities by utilizing WPA/WPA2 Encryption, Administration Access Control, Layer 2 Isolation, SSL Login page, VPN (IPSec/PPTP/L2TP), PPTP VPN Client, and IP/MAC/URL Address Pass through.

The GW-1 provides a customizable user-friendly management interface that supports Web-based Authentication, 20 simultaneous users and up to 256 account users, and marketing cooperation.

## 1-1 Package Contents

Please inspect your package. The following items should be included:

### © GW-1

- One guestWiFi
- One AC Power Adapter for guestWiFi
- One CD containing User's Manual
- Two screws for wall-mount
- One UTP Ethernet/Fast Ethernet cable (Cat.5 Twisted-pair)

If any of the above items are damaged or missing, please contact your dealer immediately.

## 1-2 Features

- Wireless data rates up to 300Mbps
- Supports 20 Simultaneous Users
- IP Plug and Play (iPnP)
- Comprehensive security
  - WPA encryption
  - WPA2 Encryption
- Intelligent Management
- Built-in AAA (Authentication/Accounting/Authorization) mechanism

---

**Note:** The "PnP" Function only can be used with TCP/IP-based Network.

---

## 1-3 Precautions

- Never remove or open the cover. You may suffer serious injury if you touch these parts.
- Never install the system in the wet locations.
- Use only the original fitting AC power adapter otherwise there is a danger of severe electrical shock.
- Avoid exposing the GuestWiFi to direct sunlight or another heat source.
- Choose a well-ventilated area to position your GuestWiFi.

## 1-4 Outlook



Figure 1 GuestWiFi Outlook

### 1-4-1 Top Panel

The top panel of the GuestWiFi is shown below.



Figure 2 GuestWiFi Top Panel

#### LEDs Indication

LED	State	Description
PWR	Off	The GuestWiFi is not receiving electrical power.
	Green	The GuestWiFi is receiving electrical power.
SYS	Off	The GuestWiFi status is defective.
	Green	The GuestWiFi status is complete.
	Green (Blinking)	During firmware upgrades, this system LED will blink.
WAN	Off	Port has not established any network connection.
	Green	A port has established a valid 10/100Mbps network connection.
	Green (Blinking)	10/100Mbps traffic is traversing the port.
LAN-1~ LAN-4	Off	Port has not established any network connection.
	Green	A port has established a valid 10/100Mbps network connection.
	Green (Blinking)	10/100Mbps traffic is traversing the port.
WLAN	Off	The Wireless is not ready.
	Green	The GuestWiFi has established a valid wireless connection.
	Green (Blinking)	The Wireless connection is active.

## 1-4-2 Rear Panel

The rear panel of the GuestWiFi is shown below.

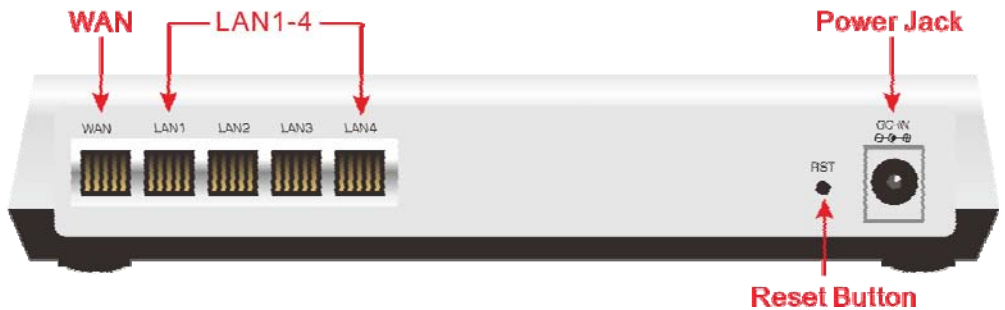


Figure 3 GuestWiFi Rear Panel

### 1. LAN (1-4):

The rear panel supports four auto-sensing RJ-45 ports and all ports can be auto-switched to MDI-II connections. The LAN ports used for linking hosts or other network devices. The individual port can be either connected to 100BaseTX networks or 10BaseT networks. When connecting to a 100BaseTX network, the ports operate at 100Mbps in half-duplex mode or 200Mbps in full-duplex mode. When connecting to a 10BaseT network, the ports operate at 10Mbps in half-duplex mode or 20Mbps in full-duplex mode.

**2. WAN:** One Ethernet port used for linking xDSL or Cable Modem.

### 3. Reset Button:

The GuestWiFi has a reset button at the rear panel of the device. Use this function to reset the system back to factory defaults.

**4. Power Jack:** Used to connect the external power supply with the GuestWiFi.

## 1-5 Technical Specifications

### 1-5-1 Hardware Specifications

#### Network Specification

IEEE802.3u 10BaseTx Ethernet

IEEE802.3u 100BaseTX Fast Ethernet

IEEE802.11b/g/n Wireless LAN

ANSI/IEEE 802.3 NWay auto-negotiation

Wi-Fi Compatible

#### Connectors

Four LAN Ports (10BaseT/100BaseTX Auto cross-over)

One WAN Port (10BaseT/100BaseTX Auto cross-over)

### **Encryption**

WPA (Wi-Fi Protected Access)

WPA2 (Wi-Fi Protected Access)

### **LED Indicators**

One POWER LED

One WAN 10/100M Link/Activity LED

Four LAN 10M/100M Link/Activity LEDs

One Wireless Link/Activity LED

One System LED

### **Power Requirement**

External Power Adapter

Input: 100-240 VAC, 50/60 Hz

Output: 12V, 1.5A

### **Environment Conditions**

Operating Temperature: 0 to 50°C

Storage Temperature: -10 to 60°C

Operating Humidity: 10~80% non-condensing

Storage Humidity: 10% to 90% non-condensing

### **Certifications**

FCC part 15 Class B, CE , C-Tick , Telec

### **Dimension**

Size: 223 (L) x 143 (W) x 36 (H) mm

Weight: About 500g (Net)

### **Mounting**

Desktop, Wall mounted



## **1-5-2 Software Specifications**

### **Networking**

- IEEE802.3u 10BaseTx Ethernet
- IEEE802.3u 100BaseTX Fast Ethernet
- IEEE802.11b Wireless LAN
- IEEE802.11g Wireless LAN
- IEEE802.11n Wireless LAN
- Supports 20 Simultaneous Users
- IP Plug and Play (iPnP)
- HTTP Proxy Support
- DHCP Server
- DHCP Relay
- Static IP WAN Client
- DHCP WAN Client
- PPPoE WAN Client
- PPTP WAN Client
- NAT
- NTP (Network Time Protocol) Support

### **Marketing Cooperation**

- Customizable log-on pages
- Portal Page

### **User Accounting and Authentication**

- Built-in Authentication
- Web-based Authentication
- User Authentication and Accounting
- Logout Window Timer Control

### **Security and Firewall**

- Layer 2 Isolation Security
- SSL User Login page/ Configuration Page
- SSL Administration
- VPN Pass through (IPSec/PPTP)
- Customize SSL Certificate
- Pass Through IP/MAC/URL Address
- Restricted Destination Filtering IP/URL
- VPN (IPSec/PPTP) Pass through
- PPTP VPN Client
- WPA
- WPA2

### **Management**

- Web-based Management Tool
- Firmware Upgrade via HTTP/TFTP
- Wizard setup for step-by-step Configuration
- Backup/Restore/Factory Default Setting
- Remote Authorized Management
- Real-time Session List
- Syslog (System/Subscriber/LAN device)
- E-mail logs
- SNMP v1/v2 (MIB II)
- System Information Table
- SSL certificate upload

## 2 Installation

The followings are instructions for setting up the GuestWiFi. Refer to the illustration and follow the simple steps below to quickly install your GuestWiFi.

### Wall-Mounting

The GuestWiFi can be wall-mounted on a wall by applying the two mounting brackets on screws.

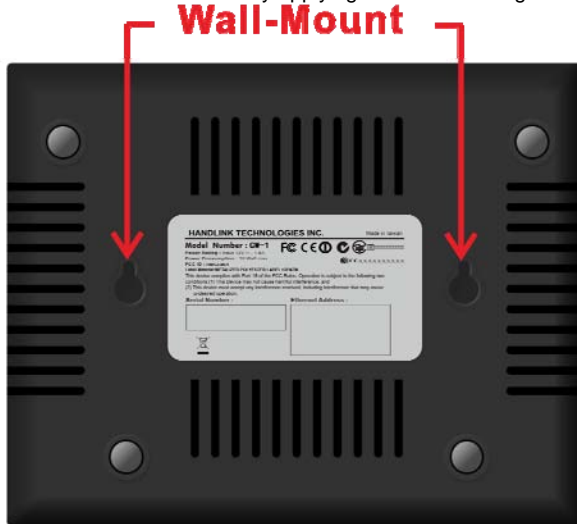


Figure 4 Wall-Mounting Bracket - Bottom of GuestWiFi

Please refer to the following instructions for mounting a GuestWiFi on a wall or other surface.

1. Install two screws on a wall according to the relative positions shown below.

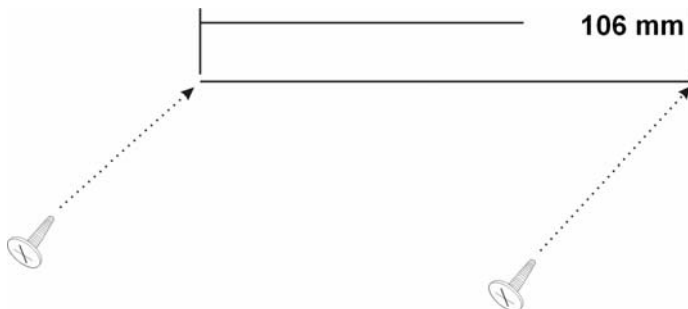


Figure 5

2. Hang GuestWiFi on the wall by sliding the two screws in the mounting brackets.

---

**Note:** If the screws are not properly anchored, the strain of the cables connected to the GuestWiFi rear panel connectors could pull out the GuestWiFi from the wall.

---

## 2-1 Installation Requirements

Before installing the GuestWiFi, make sure your network meets the following requirements.

### System Requirements

The GuestWiFi requires one of the following types of software:

- Windows 98 Second Edition/NT/2000/XP/Vista/7
- Red Hat Linux 7.3 or later version
- MAC OS X 10.2.4 or later version
- Any TCP/IP-enabled systems like Mac OS and UNIX (TCP/IP protocol installed)
- Standard phone line for xDSL modem Or Coaxial cable for Cable modem
- Web Browser Software (Microsoft I.E 5.0 or later version or Netscape Navigator 5.0 or later version)
- One computer with an installed 10Mbps, 100Mbps or 10/100Mbps Ethernet card
- UTP network Cable with a RJ-45 connection (Package contents)

---

**Note:** Prepare twisted-pair cables with RJ-45 plugs. Use Cat.5 cable for all connections. Make sure each cable not exceed 328 feet (Approximately 100 meters).

---

## ***ISP Requirements***

Verify whether your ISP use fixed or dynamic IP. If it is a fixed IP, be sure to get the IP from your ISP. For dynamic IP, which is mostly used, the PC will get the IP automatically whenever it hooks up on the modem.

### ***Dynamic IP***

- Dynamic IP Setting

### ***Fixed IP***

- Your fixed IP address for the GuestWiFi
- Your subnet mask for the GuestWiFi
- Your default gateway IP address
- Your DNS IP address

### ***PPPoE***

- Your user name from your ISP
- Your password from your ISP

### ***PPTP***

- PPTP Server IP Address from your ISP
- PPTP Local IP address from your ISP.
- PPTP Local IP subnet mask from your ISP.
- Your user name from your ISP
- Your password from your ISP
- Your PC Requirements

### **The Static IP settings for the PC**

- Your PC's fixed IP address
  - Your PC's subnet mask
  - Your PC's default gateway IP address
  - Your PC's primary DNS IP address
- 
- 

### ***Note:***

1. The gateway's default IP address setting is "10.59.1.1".
  2. The gateway's default subnet mask setting is "255.0.0.0".
- 

### **The Dynamic IP settings for the PC**

We recommend that you leave your IP settings as automatically assigned. By default, the GuestWiFi is a DHCP server, and it will give your PC the necessary IP settings.

## **2-2 Getting Start**

1. Connect the Ethernet cable to the guestWiFi's LAN port.
2. Ensure that your modem and computer are both switched on.
3. Use the supplied cable to connect the guestWiFi 's WAN port to the modem. Check that the Cable/xDSL Status LED lights.
4. Connect your computer to one of the 10/100 LAN ports on the guestWiFi. Check that the LAN Port Status LED lights.
5. Configure the further parameters via a Web browser.

## 3 Configuring the GuestWiFi

### 3-1 Setting Wizard

**Step 1:** Start your browser, and then enter the factory default IP address **10.59.1.1** in your browser's location box. Press **Enter**.

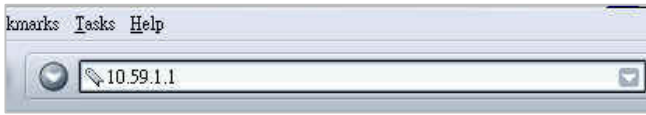


Figure 6 Web Browser Location Field (Factory Default)

**Step 2:** The GuestWiFi configuration tools menu will appear. In the Username and Password field, type the factory default user name **admin** and password **admin** and click **Login**. If you are first time setting the system, the wizard setup screen will appear. You will be guided, step-by-step, through a basic setup procedure.

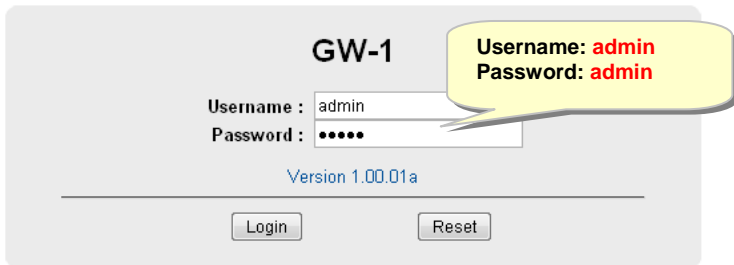


Figure 7 Configuration Tools Menu

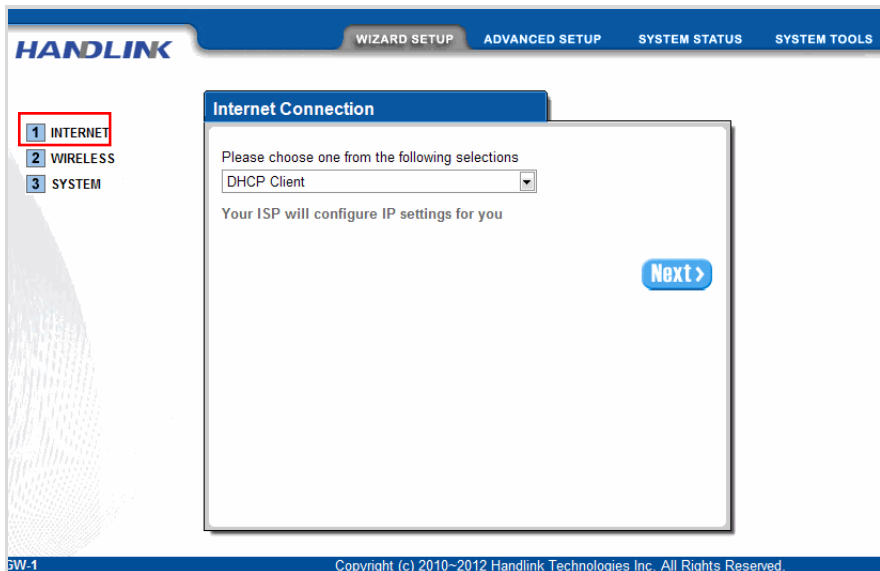


Figure 8 Wizard Setup Screen

## System Quick View

### System

System/Host Name		Firmware Version	1.07.06
Location Name		Domain Name	
System Time	2004/7/2 16:08:58	System Up Time	00D:00H:01M:11S
WAN MAC address	00:90:0E:00:60:C1	LAN MAC address	00:90:0E:00:60:C0
		WLAN MAC address	00:90:0E:00:60:C2

### Network

WAN Status	<b>Not Established</b>	WAN Type	DHCP Client
WAN IP Address	192.168.100.230	WAN Subnet Mask	255.255.255.0
Default Gateway	192.168.100.254	DNS	192.168.100.2
Guest LAN IP Address	10.59.1.1	Guest LAN Subnet Mask	255.255.255.0
Employee LAN IP Address	10.59.2.1	Employee LAN Subnet Mask	255.255.255.0

### Wireless

Wireless Service	OK	Guest ESSID	Guest
		Guest Secure Mode	Enable
Wireless Channel	10	Employee ESSID	Employee
		Secure Mode	Disable

### Traffic

WAN	TxData:10 RxData:0 TxError:0 RxError:0
LAN	TxData:83 RxData:77 TxError:0 RxError:0
Guest Wireless	TxData:2 RxData:0 TxError:0 RxError:0
Employee Wireless	TxData:2 RxData:0 TxError:0 RxError:0

Best View with Microsoft Internet Explorer 5.0 above

*Figure 9 System Quick View*

**Reset**

Click on reset button to clear the username and password data.

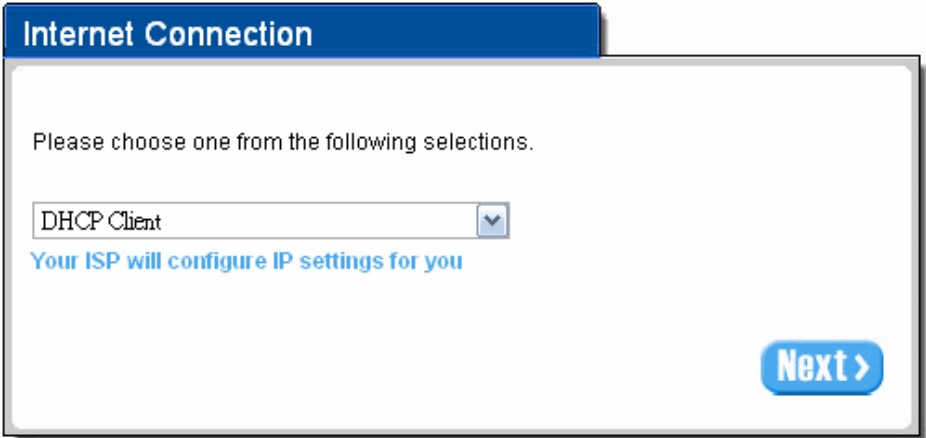
### Note:

- ☞ This Web agent is best viewed with IE 5.0 or Netscape 6.0 and above browsers.
- ☞ If you would like to change the password please see Step 10.
- ☞ Username and Password can consist of up to 20 alphanumeric characters and are case sensitive.
- ☞ If for some reason your password is lost or you cannot gain access to the GuestWiFi Configuration Program, please press the reset button to load the device to manufacturer defaults.
- ☞ If the GuestWiFi doesn't send packet in 5 minutes (default), the GuestWiFi will logout automatically.
- ☞ Proxy needs to set disable first when administrator accesses admin UI.



### Step 3: Internet Connection Setting

Select the appropriate Internet connection type to connect to your ISP.



**Internet Connection**

Please choose one from the following selections.

DHCP Client

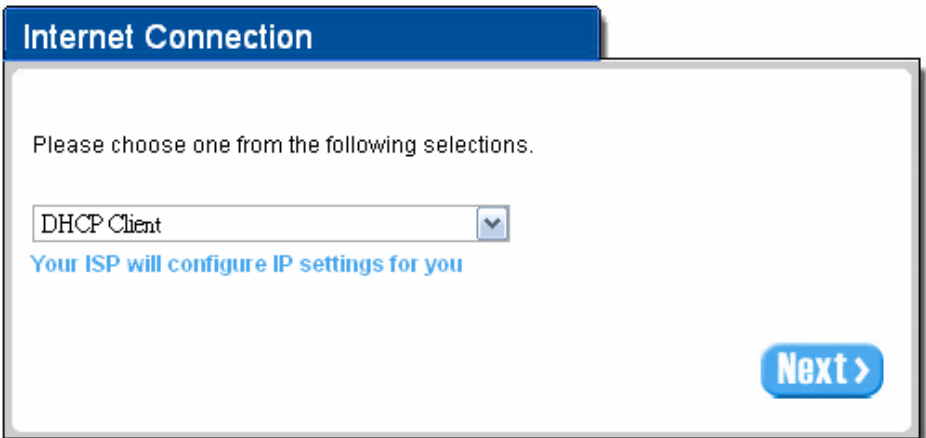
Your ISP will configure IP settings for you

Next >

Figure 10 Internet Connection Setting Screen

- **DHCP Client**

The device can work as a DHCP client. This allows the device to obtain the IP address and other TCP/IP settings from your ISP. If your xDSL/Cable comes with this feature, please enable Use DHCP Client.



**Internet Connection**

Please choose one from the following selections.

DHCP Client

Your ISP will configure IP settings for you

Next >

Figure 11 Internet Connection Setting Screen—DHCP Client Setting

- **Static IP Setting**

If **Static IP Setting** is selected, then this screen will appear. Enter the IP address information provided by your ISP.

Figure 12 Internet Connection Setting Screen—Static IP Setting

Item	Default	Description
IP Address	0.0.0.0	Enter the IP address provided by your ISP.
Subnet Mask	0.0.0.0	Enter the subnet mask for the IP address.
Gateway IP Address	0.0.0.0	Enter the Gateway IP Address provided by your ISP.
Primary DNS Server	Empty	Enter the primary DNS server IP address for the xDSL/Cable connection (provided by your ISP).
Secondary DNS Server	Empty	Enter the secondary DNS server IP address for the xDSL/Cable connection (provided by your ISP). If the primary DNS Server IP were not available, meanwhile, Secondary DNS Server IP would start in the same time.

- **PPPoE (Point-to-Point Protocol over Ethernet)**

If “PPPoE” is selected, then this screen will appear. Enter the username, password and other major fields.

Figure 13 Internet Connection Setting Screen—PPPoE Setting

Item	Default	Description
Username	Empty	Enter the user name provided by your ISP. The user name can consist of up to 80 alphanumeric characters and is case sensitive.
Password	Empty	Enter the user password provided by your ISP. The password can consist of up to 80 alphanumeric characters and is case sensitive.
PPP MTU Setting	1492	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.
TCP MSS Setting	1452	MSS (Maximum Segment Size) specifies maximum segment size.
Service Name	Empty	Enter the service name provided by your ISP. The service name can consist of up to 64 alphanumeric characters and is case sensitive.

Item	Default	Description
Connect on Demand and Max Idle Time		
Connect on Demand	Enable	You can configure your GuestWiFi to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your GuestWiFi to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain, click the radio button of keep alive. The Max Idle Time maximum value is 65535 minutes.
Max Idle Time	10 Minutes	
Keep alive and Redial Period		
Keep alive	Disable	This option keeps your PPPoE enabled Internet access connected indefinitely, even when it sits idle. The Redial Period maximum value is 65535 seconds.
Redial Period	30 Seconds	

- **PPTP Client (Point-to-Point Tunneling Protocol)**

If “PPTP” is selected, then this screen will appear. Fill out all the information provided by your ISP.

## Internet Connection

Please choose one from the following selections.

PPTP (Mostly for Europe ADSL modem users) ▾

**Your ISP requires you to input username / password / PPTP setting**

My IP Address:

My Subnet Mask:

Gateway IP address:

PPTP Server IP Address:

Username:

Password:

PPP MTU Setting:

TCP MSS Setting:

Connection ID/Name:

**Connect on Demand** Max Idle Time:  Min.

**Keep alive** Redial Period:  Sec.

Next >

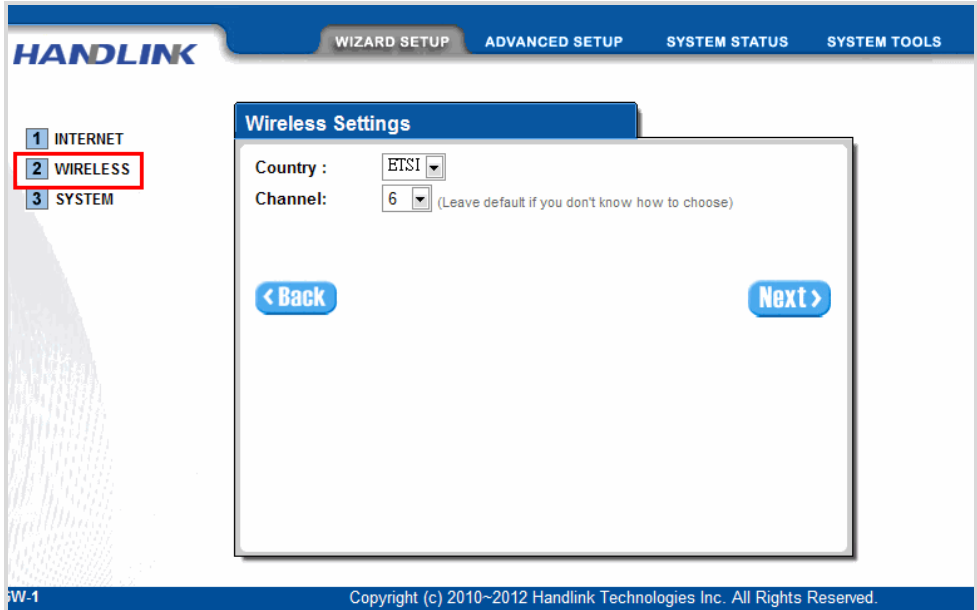
*Figure 14 Internet Connection Setting Screen—PPTP Client Setting*

Item	Default	Description
My IP Address	Empty	Enter the PPTP local IP address provided by your ISP.
My Subnet Mask	Empty	Enter the PPTP local Subnet Mask IP address for the IP address (My IP Address).

Item	Default	Description
Gateway IP Address	Empty	Enter the PPTP server Gateway IP address provided by your ISP.
PPTP Server IP Address	Empty	Enter the PPTP server IP address provided by your ISP.
Username	Empty	Enter the user name provided by your ISP. The user name can consist of up to 80 alphanumeric characters and is case sensitive.
Password	Empty	Enter the user password provided by your ISP. The password can consist of up to 80 alphanumeric characters and is case sensitive.
PPP MTU Setting	1460	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.
TCP MSS Setting	1400	MSS (Maximum Segment Size) specifies maximum segment size.
Connection ID/Name	Empty	Enter the connection ID or connection name. The connection ID/Name can consist of up to 81 alphanumeric characters and is case sensitive.
<b>Connect on Demand and Max Idle Time</b>		
Connect on Demand	Enable	You can configure your GuestWiFi to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your GuestWiFi to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain, click the radio button of keep alive. The Max Idle Time maximum value is 65535 minutes.
Max Idle Time	10 Minutes	
<b>Keep alive and Redial Period</b>		
Keep alive	Disable	This option keeps your PPTP enabled Internet access connected indefinitely, even when it sits idle. The Redial Period maximum value is 65535 seconds.

#### Step 4: Wireless Setting

This page allows you to define ESSID, Channel ID and WEP/WPA encryption for wireless connection.



The screenshot displays the 'Wireless Settings' configuration page. On the left, a vertical menu lists three steps: '1 INTERNET', '2 WIRELESS' (which is highlighted with a red rectangular border), and '3 SYSTEM'. The main content area is titled 'Wireless Settings' and contains two configuration fields: 'Country' with a dropdown menu showing 'ETSI', and 'Channel' with a dropdown menu showing '6'. A small text note next to the Channel dropdown reads '(Leave default if you don't know how to choose)'. At the bottom of the form area, there are two blue buttons: '< Back' on the left and 'Next >' on the right. The footer of the page shows 'W-1' on the left and 'Copyright (c) 2010~2012 Handlink Technologies Inc. All Rights Reserved.' on the right.

Figure 15 Wireless Setting Screen

Item	Default	Description
Country	ETSI	Select the Country code of the dropdown list.
Channel	6	Enter the channel ID for wireless connection.

Step 5: System Setting

**HANDLINK** WIZARD SETUP ADVANCED SETUP SYSTEM STATUS SYSTEM TOOLS

**System Setting**

Please be sure to change your password:

Username:

Password:  Confirm:

System date and time: Date: 2004/7/2 Time: 16:06:02

Server IP/Domain Name	<input type="text" value="time.nist.gov"/>
Time Zone	GMT +08:00
Update Time	<input type="text" value="24"/> hours
<input type="checkbox"/> Daylight Saving Time	Start Date: <input type="text" value="4"/> Month / <input type="text" value="1"/> Day
	End Date: <input type="text" value="10"/> Month / <input type="text" value="31"/> Day

Secure Administrator IP Address  All  Selected

**< Back** **FINISH**

GW-1 Copyright (c) 2010~2012 Handlink Technologies Inc. All Rights Reserved.

Figure 16 System Setting Screen



Item	Default	Description
Username	admin	Enter the user name. The user name can consist of up to 80 alphanumeric characters and is case sensitive.
Password	admin	Enter the user password. The password can consist of up to 80 alphanumeric characters and is case sensitive.
Confirm	Empty	Enter the password of administrator for confirmation.
<b>NTP Setting</b>		
Server IP/Domain Name	Empty	Enter the IP address/domain name of NTP server. The maximum allowed characters length is 100.
Time Zone	GMT+8:00	Select the appropriate time zone for your location.
Update Time	24 hours	Enter the number of hours for update time.
Daylight Saving Time	Disable	Enables or disables Daylight Saving Time (DST).
	Month/Day	Set the Daylight Saving Time (DST) on the Wireless Subscriber Gateway. Adjust the begin time and end time.

**FINISH**

*Click the button to save the settings then the system will restart.*

### 3-2 Advanced Setup

The Advanced Setting enables you to configure advanced settings related to accessing the Internet, including,

1. MANAGEMENT
  - SYSLOG
  - SESSION TRACE
  - BANDWIDTH
  - SNMP
2. SECURITY
  - PASS THROUGH
  - SECURE REMOTE
3. SYSTEM
  - SYSTEM
  - WAN/LAN
  - SERVER
  - WIRELESS
4. GUEST SETTING
  - ESSID SETTING
  - AUTHENTICATION
  - USAGE TIME
  - CUSTOMIZATION
5. EMPLOYEE SETTING
  - ESSID SETTING

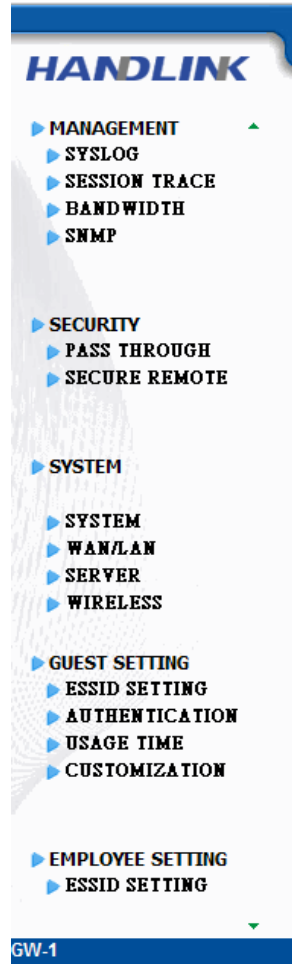


Figure 17 Advanced Setting Item Screen

---

**Note:** After change the settings of device, please click **apply** button to save the new settings.

---

## 3-2-1 MANAGEMENT

### 3-2-3-1 Syslog

The function allows the device to transmit event messages to your syslog server or your email address for monitoring and troubleshooting.

- **Syslog Setting**

SYSLOG
Syslog
Log Settings

**Send to Syslog Server**

**Disable**    **Enable**

Syslog Server on LAN:

Server IP Address :   
 Server MAC Address :

Syslog Server on WAN:

Server 1:   
 Server 2:

**Send to Email**

**Disable**    **Enable**

Email Server:

IP Address or Domain Name:   
 SMTP Port:

E-mail (SMTP) server needs to check my account

Username:

Password:

Email From:

Name:   
 Email Address:

Email To:

Email Address 1:   
 Email Address 2:

Apply

Figure 18 Syslog Setting Screen

Item	Default	Description
Syslog	Disable	Enables or disables the syslog server function.
<b>Syslog on LAN</b>		
Server IP Address	Empty	Enter syslog server's IP address. The GuestWiFi will send all of its logs to the specified syslog server.
Server MAC Address	Empty	Enter the syslog server's MAC address. The GuestWiFi will send all of its logs to the specified syslog server.

Item	Default	Description
<b>Syslog on WAN</b>		
Server 1 IP Address	Empty	Enter IP address of first syslog server.
Server 2 IP Address	Empty	Enter IP address of second syslog server.
<b>Send to Email</b>	Disable	Enables or disables the send to e-mail function.
<b>E-mail Server</b>		
IP Address or Domain Name	Empty	Enter the SMTP server IP address or domain name. The maximum allowed characters length is 50.
SMTP Port	25	The SMTP port allowed range is 25 or 2500 to 2599.
E-mail (SMTP) Server needs to check my account	Disable	If your SMTP server requires authentication before accepting e-mail, click on check box. These values (username and password) are supplied by your network administrator, SMTP server provider or ISP.
Username	Empty	Enter the username for the SMTP server. The maximum allowed characters length is 64.
Password	Empty	Enter the password for the SMTP server
<b>Email From</b>		
Name	Empty	Enter the name you would like to appear in the "message from" field of your outgoing message. The maximum allowed characters length is 20.
Email Address	Empty	Enter your e-mail address. This is the address others will use to send email to Email Address 1/Email Address 2.
<b>Email To</b>		
Email Address 1	Empty	Enter your first e-mail address to receive the logs.
Email Address 2	Empty	Enter your second e-mail address to receive the logs.

Apply

Click **Apply** button to save the new settings.

Click **Apply** button, the success dialog box appears. Click on **Back** to return to Syslog setting screen

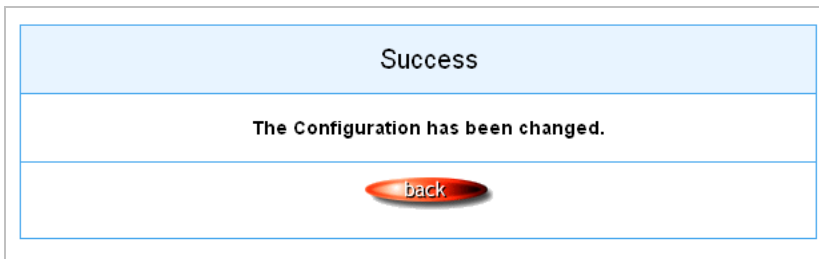


Figure 19 Success Dialog Box

● Log Categories

**SYSLOG**

Syslog		Log Settings		
<b>System</b>				
Syslog	Email	Syslog Name	Description	Interval Time
<input type="checkbox"/>	<input type="checkbox"/>	System Information	A log including the system information will be sent according to specified interval time	60 minute(s)
<input type="checkbox"/>	<input type="checkbox"/>	System Boot Notice	Once system reboots, the log will be sent	When system reboot
<input type="checkbox"/>	<input type="checkbox"/>	System Manager Activity Information	A log will be sent if system manager (Administrator, Supervisor or Account Manager) login to or logout from the device	When system manager login or logout
<input type="checkbox"/>	<input type="checkbox"/>	Wireless Association information	A log including wireless users information will be sent according to specified interval time.	60 minute(s)
<input type="checkbox"/>	<input type="checkbox"/>	Firmware Update Notice	A log will be sent if firmware update completed.	When firmware update completed
<b>User</b>				
Syslog	Email	Syslog Name	Description	Interval Time
<input type="checkbox"/>	<input type="checkbox"/>	User Login	A log including users information will be sent when user logged-in.	When user logged-in
<input type="checkbox"/>	<input type="checkbox"/>	User Logout	A log including users information will be sent when user logged-out.	When user logged-out
<input type="checkbox"/>	<input type="checkbox"/>	Current User List	A log including logged-in users information will be sent according to specified interval time.	60 minute(s)
<b>Account</b>				
Syslog	Email	Syslog Name	Description	Interval Time
<input type="checkbox"/>	<input type="checkbox"/>	Account information	A log will be sent once after an account is created..	When an account is created
				<a href="#">Apply</a>

Figure 20 Log Settings Screen

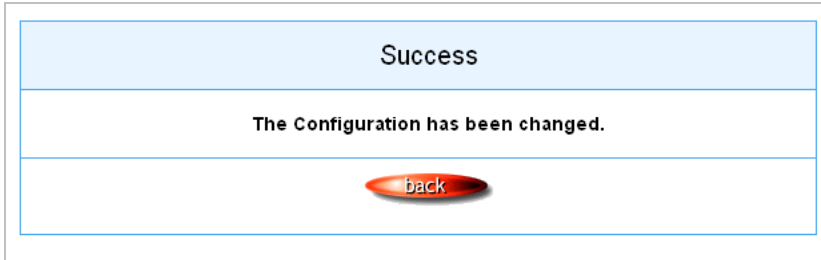
Item	Interval Time	Description
<b>System</b>		
System Information	5~60 minutes	<p>The log included system information would be sent according to specified interval time.</p> <p><b>Format:</b></p> <p>PRODUCT=GW-1;VER=2.00.00;LOGNAME=DVI;  DATE=07Mar26;TIME=11:30:00;  WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02;  WLANMAC=09-00-0e-00-00-03;  IP_ADDRESS=210.66.37.21;  SYS_UP_TIME=14D23H34M21S;WANTXOK=99999;  WANRXOK=99999;WANTXERROR=99999;WANRXERROR=99999;  LANTXOK=99999;LANRXOK=99999;LANTXERROR=99999;  LANRXERROR=99999;WIRELESSTXOK=99999;WIRELESSRXOK=99999;  WIRELESSTXERROR=99999;WIRELESSRXERROR=99999;</p>
System Boot Notice	When system rebooted	<p>If device have been rebooted or restarted, the log would be sent.</p> <p><b>Format:</b></p> <p>PRODUCT=GW-1;VER=2.00.00;LOGNAME=SUN;  DATE=07Mar26;TIME=15:23:32;  WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02;  WLANMAC=09-00-0e-00-00-03;  IP_ADDRESS=210.66.37.21;  SYS_NAME=Cafehotspot;LOCATION=East;CITY=Taipei;  COUNTRY=Taiwan; FIRMWARE=v1.01.02;MESSAGE=System_Up;  <b>Message</b> = System_Reboot</p>
System Manager Activity Information	When system manager login or logout	<p>A log will be sent if system manager (Administrator) login to or logout from the device.</p> <p><b>Format:</b></p> <p>PRODUCT=GW-1;VER=2.00.00;LOGNAME=SUN;  DATE=07Mar26;TIME=15:23:32;  WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02;  WLANMAC=09-00-0e-00-00-03;  IP_ADDRESS=210.66.37.21;  SYS_NAME=Cafehotspot;LOCATION=East;CITY=Taipei;  COUNTRY=Taiwan;  FIRMWARE=v1.01.02;MESSAGE=System_Up;  <b>Account Name</b> = Admin  <b>Status</b>= Login   Logout   Idle_Time_Out</p>
Wireless Association Information	5~60 minutes.	<p>A log including wireless users information will be sent according to specified interval time.</p> <p><b>Format:</b></p> <p>PRODUCT=GW-1;VER=2.00.00;LOGNAME=WAI;  DATE=07Mar26;TIME=15:23:32;  WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02;  WLANMAC=09-00-0e-00-00-03;  IP_ADDRESS=210.66.37.21;  USER_NUM=15;SEQ=1-5;USER_MAC=02-34-3e-01-00;</p>

Firmware Update Notice	When firmware update completed	<p>A log will be sent if firmware update completed</p> <p><b>Format:</b>  PRODUCT=GW-1;VER=2.00.00;LOGNAME=FUN;  DATE=07Mar26;TIME=15:23:32;  WANMAC=09-00-0e-00-00-01;LANMAC=09-00-0e-00-00-02;  WLANMAC=09-00-0e-00-00-03;  IP_ADDRESS=210.66.37.21;  MESSAGE=Success;OLD_FRIMWARE=v1.00.01;  NEW_FIRMWARE=v1.00.02</p> <p><b>Message</b> = Success   Fail</p>
<b>User</b>		
User Login	When user logged-in	<p>A log including users information will be sent when user logged –in</p> <p><b>Format:</b>  PRODUCT=GW-1;VER=2.00.00;LOGNAME=ULI;DATE=07Mar26;  TIME=15:23:32;WANMAC=09-00-0e-00-00-01;  LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03;  IP_ADDRESS=210.66.37.21;USER_NAME=asdfg12;USER_IP=10.59.1.1;  USER_MAC=02-34-3e-01-00;INTERFACE=Ethernet;  USER_TYPE=Dynamic;  <b>User Type</b> = Guest/ Employee</p>
User Logout	When user logged-out	<p>A log including users information will be sent when user logged –out</p> <p><b>Format:</b>  PRODUCT=GW-1;VER=2.00.00;LOGNAME=ULO;DATE=07Mar26;  TIME=15:23:32;WANMAC=09-00-0e-00-00-01;  LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03;  IP_ADDRESS=210.66.37.21;USER_NAME=asdfg12;USER_IP=10.59.1.1;  USER_MAC=02-34-3e-01-00;INTERFACE=Ethernet;  USER_TYPE=Dynamic;RXDATA=1234; TXDATA=1234;  USED_TIME=24:00:00;LOGOUT_TYPE=Time_Up;TIME_LEFT=24:00:00</p> <p><b>User Type</b> = Guest/ Employee</p>
Current User List	.5~60 minutes.	<p>A log including logged-in users information will be sent according to specified interval time</p> <p><b>Format:</b>  PRODUCT=GW-1;VER=2.00.00;LOGNAME=CUL;DATE=07Mar26;  TIME=15:23:32;WANMAC=09-00-0e-00-00-01;  LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03;  IP_ADDRESS=210.66.37.21;USER_NUM=0;SEQ=1-5;  USER_NAME=asdfg12,USER_IP=10.59.1.2,USER_MAC=02-34-3e-01-00,  INTERFACE=Ethernet,USER_TYPE=Dynamic,RXDATA=1234,  TXDATA=1234,USED_TIME=24:00:00,SESSION=100,WLAN_SIG=N/A;</p>
<b>Account and Billing</b>		
Account Information	When an account is created	<p>A log will be sent when an account is created</p> <p><b>Format:</b>  PRODUCT=GW-1;VER=2.00.00;LOGNAME=ACI;DATE=07Mar26;  TIME=15:23:32;WANMAC=09-00-0e-00-00-01;  LANMAC=09-00-0e-00-00-02; WLANMAC=09-00-0e-00-00-03;  IP_ADDRESS=210.66.37.21;USER_NAME=asdfg12;  ACCOUNT_TYPE=TimetoFinish; ACCOUNT_SERIAL=000002;</p>

A blue oval button with the word "Apply" in white text.

Click **Apply** button to save the new settings.

Click **Apply** button, the success dialog box appears. Click on **Back** to return to Logs setting screen.



*Figure 21 Success Dialog Box*



### 3-2-3-2 Session Trace

Session Trace is an intelligent function to help service provider to trace every user's access behavior. When "session trace" is enable , the system will collect information such like destination IP, destination port, source IP, source MAC, source port by every user and send the collected information in text format file to specified TFTP server or Email Server.

## SESSION TRACE

**Session Trace :** Disable

<b>TFTP Server</b>	<input type="checkbox"/> Enable Primary TFTP Server IP Address : <input style="width: 150px;" type="text"/> Secondary TFTP Server IP Address : <input style="width: 150px;" type="text"/>
<b>E-mail Server</b>	<input type="checkbox"/> Enable <div style="border: 1px solid gray; padding: 5px; margin-top: 5px;">                     IP Address or Domain Name : <input style="width: 150px;" type="text"/>                      SMTP Port : <input style="width: 50px;" type="text" value="25"/>  <input type="checkbox"/> E-mail (SMTP) server needs to check my account :                      Username : <input style="width: 100px;" type="text" value="admin"/>                      Password : <input style="width: 100px;" type="password" value="●●●●●●"/> </div> <div style="border: 1px solid gray; padding: 5px; margin-top: 5px;">                     Email From :                      Name : <input style="width: 150px;" type="text"/>                      Email address : <input style="width: 150px;" type="text"/> </div> <div style="border: 1px solid gray; padding: 5px; margin-top: 5px;">                     Email To :                      Email address 1 : <input style="width: 150px;" type="text"/>                      Email address 2 : <input style="width: 150px;" type="text"/> </div>

Send Session Trace log file every  minutes. (5~1440)  
(Note: Session Trace log file will be sent also when collected 50 logs)

Apply

Figure 22 Session Trace Setting Screen

Item	Default	Description
Session Trace	Disable	Disables or enables session trace function.
Primary TFTP Server IP Address	Empty	Enter the IP address of the primary TFTP server.
Secondary TFTP Server IP Address	Empty	Enter the IP address of the second TFTP server.
Send Session Trace log file every~ minutes.	10 minutes	The field means to send the session trace log file every interval minutes. The value range is 5 to 1440 (minutes).

Item	Default	Description
<b>Send to Email</b>	Disable	Enables or disables the send to e-mail function.
<b>E-mail Server</b>		
IP Address or Domain Name	Empty	Enter the SMTP server IP address or domain name. The maximum allowed characters length is 50.
SMTP Port	Empty	The SMTP port allowed range is 25 or 2500 to 2599.
E-mail (SMTP) Server needs to check my account	Disable	If your SMTP server requires authentication before accepting e-mail, click on check box. These values (username and password) are supplied by your network administrator, SMTP server provider or ISP.
Username	Empty	Enter the username for the SMTP server. The maximum allowed characters length is 64.
Password	Empty	Enter the password for the SMTP server
<b>Email From</b>		
Name	Empty	Enter the name you would like to appear in the "message from" field of your outgoing message. The maximum allowed characters length is 20.
Email Address	Empty	Enter your e-mail address. This is the address others will use to send email to Email Address 1/Email Address 2.
<b>Email To</b>		
Email Address 1	Empty	Enter your first e-mail address to receive the logs.
Email Address 2	Empty	Enter your second e-mail address to receive the logs.

### 3-2-3-3 Bandwidth

The function enables administrator to limit bandwidth usage on a per user basis (MAC address). That prevents users from consuming a disproportionately large amount of bandwidth so every user gets a fair share of the available bandwidth.

#### BANDWIDTH

**Bandwidth Management:**

The function enables administrator to limit bandwidth usage on a per user basis (MAC address). That prevents users from consuming a disproportionately large amount of bandwidth so every user gets a fair share of the available bandwidth.

Please setup the maximum Upstream/Downstream bandwidth

Maximum Upstream	<input checked="" type="radio"/> 64Kbps	<input type="radio"/> <input type="text"/> Kbps (64-5120)
Maximum Downstream	<input checked="" type="radio"/> 128Kbps	<input type="radio"/> <input type="text"/> Kbps (64-5120)

Figure 23 Bandwidth Setting Screen

Item	Default	Description
Bandwidth	Disable	Enables or disables Bandwidth Management.
Maximum Upstream	64Kbps	Specify the amount of upstream bandwidth.
Maximum Downstream	128Kbps	Specify the amount of downstream bandwidth.

### 3-2-3-4 SNMP

The SNMP Agent Configuration screen enables you to access to your device via Simple Network Management Protocol. If you are not familiar with SNMP, please consult your Network Administrator or consult SNMP reference material. You must first enable SNMP on the SNMP Agent Configuration screen.

**SNMP**

SNMP: Disable ▼

SNMP Port :  ( 161 or 16100 ~ 16199 )

Trap Port :  ( 162 or 16200 ~ 16299 )

No	Community Name	NMS Address	Privileges	Status
01	<input type="text" value="public"/>	<input type="text" value="ANY"/>	<span>Read</span> ▼	<span>Valid</span> ▼
02	<input type="text" value="private"/>	<input type="text" value="ANY"/>	<span>Write</span> ▼	<span>Valid</span> ▼
03	<input type="text"/>	<input type="text" value="ANY"/>	<span>All</span> ▼	<span>Invalid</span> ▼
04	<input type="text"/>	<input type="text" value="ANY"/>	<span>All</span> ▼	<span>Invalid</span> ▼
05	<input type="text"/>	<input type="text" value="ANY"/>	<span>All</span> ▼	<span>Invalid</span> ▼

Apply

Figure 24 SNMP Setting Screen

Item	Default	Description
SNMP	Disable	Disables or enables the SNMP management.
SNMP Port	161	If the SNMP enables, also allowed to specific the SNMP port number via NAT. The allowed SNMP port numbers are 161 (default), 16100-16199 and Trap port numbers are 162 (default), 16200-16299. This Port setting is useful for remote control via NAT network.
Trap Port	162	
Configuration		
Community Name	public/private	Every unit with SNMP enable must be configured to recognize one or more community names up to 20 characters. The default setting for the community of entry 1 is “public” and for the entry 2 is “private” and others are empty.
NMS Address	ANY	The address of the NMS. The default settings for the NMS Networking are “ANY”.

Item	Default	Description
Privileges	Read/Write	Choose "Read", "Write", "Trap Recipients" and "All" for different privileges. The default setting of the entry 2 is "write" and others are "read".
Status	Valid/Invalid	Chosen "Valid" or "Invalid". The default setting of entry 1, 2 are valid and others are invalid.

## 3-2-2 SECURITY

### 3-2-2-1 Pass Through

This function allow administrator to set some special devices pass through the GuestWiFi system. Because some network devices might be constructed under the GuestWiFi. However these devices needn't be checked and authorized. The GuestWiFi provides a pass through list and the administrator can control which devices can be pass through with authentication.

#### PASS THROUGH

Pass Through Disable

Pass Through Destination allows the subscribers to access specified internet websites without authentication, which is useful to promote selected services.Pass Through Subscriber is useful for VIP users without authentication.Pass Through LAN device is also useful for devices that do not have a web browser (cash registers, for example) or that are connected with LAN port (wireless access points, for example).

**Please enter new pass through for destination** (up to 50 entries)

URL or Website:

Start / End IP Address  ~

**Please enter new pass through for subscribers or LAN devices** (up to 50 entries)

Start / End IP Address  ~

IP Address:  Subnet Mask:

MAC Address:  Mask:

Description  (max 20 characters)

**Pass Through List**

No.	Active	Address List	Type	Description	Delete
-----	--------	--------------	------	-------------	--------

Figure 25 Pass through Setting Screen

Item	Default	Description
Pass Through	Disable	Enables or disables the pass through function.
Destination URL/IP Address Pass Through		
<input checked="" type="radio"/> URL or Website: <input type="text"/>		
URL or Website	Empty	Enter the URL Page; please use this format such like "http://www.yahoo.com". The maximum character of the URL Page is 50.
<input checked="" type="radio"/> Start / End IP Address: <input type="text"/> ~ <input type="text"/>		
Start IP Address	Empty	Enter the start IP address of you wants pass through.
End IP Address	Empty	Enter the end IP address of you wants pass through.
Subscriber IP/MAC Address or LAN Device Pass Through		
<input checked="" type="radio"/> Start / End IP Address: <input type="text"/> ~ <input type="text"/>		
Start IP Address	Empty	Enter the start IP address of you wants pass through.
End IP Address	Empty	Enter the end IP address of you wants pass through.
<input checked="" type="radio"/> IP Address: <input type="text"/> Subnet Mask: <input type="text"/>		
IP Address	Empty	Enter the IP address of you wants pass through.
Subnet Mask	Empty	Enter the subnet mask of you wants pass through.
<input checked="" type="radio"/> MAC address: <input type="text"/> Mask: <input type="text" value="FF-FF-FF-FF-FF-FF"/>		
MAC Address	Empty	Enter the MAC address of you wants pass through.
Mask	Empty	Enter the subnet mask of you wants pass through.
Pass Through List	Display the pass through Information of GuestWiFi.	
No.	-	The index number of pass through address.
Active	Disable	Click on check box, active or inactive the pass through address.
Address List	-	Display the pass through address(s).
Type	-	Display the type of pass through address.
Delete	Disable	Select the check boxes and click 'Delete' to delete the pass through address(s).

Add to List

Click **Add to List** button to add a new entry.

Apply

Click **Apply** button to save the new settings.

Delete All

Click **Delete All & Apply** button to delete all entries.

**Note:** The priority of "pass through" is higher than "Filtering".

### 3-2-2-2 Secure Remote

This feature allows you to create a secure connection to a remote site or back end system with VPN PPTP Client. If “Secure Remote” is enabled, the RADIUS packet/ syslog will be transferred to this secure connection.

**SECURE REMOTE**

Secure Remote: Disable ▾

This feature allows you to create a secure connection to a remote site or back end system with VPN PPTP Client. When this feature is enable, the RADIUS packet/syslog/HTTP/session trace will be transferred to this secure connection.

**PPTP Client**

Auto-connect at Start-up (Always connect)

PPTP Server IP address :

Username :

Password :

---

Status

VPN Tunnel : Offline

Client IP :

Figure 26 Secure Remote Setting Screen

Item	Default	Description
Auto-connect at Start-up (Always connect)	Disable	Enable the check box to automatically establish the PPTP connection.
PPTP Server IP address	Empty	Enter the PPTP server IP address provided by your ISP.
Username	Empty	Enter the user name provided by your ISP. The user name can consist of up to 80 alphanumeric characters and is case sensitive.
Password	Empty	Enter the user password provided by your ISP. The password can consist of up to 80 alphanumeric characters and is case sensitive.
<input type="button" value="Start connection"/>		Click on Start/Stop connection button to start/stop PPTP connection.
<input type="button" value="refresh↻"/>		Click on refresh button to update the status.
VPN Tunnel	Display the status.	
Client IP	Display the IP address.	



### 3-2-3 SYSTEM

#### 3-2-3-1 System

Define the GuestWiFi System configuration.

SYSTEM																					
<b>System/Host Name</b>	<input type="text"/> (Max.=50)																				
<b>Domain Name</b>	<input type="text"/> (Max.=50)																				
<b>Location Information</b>	<table border="1"><tr><td>Location Name:</td><td><input type="text"/> (Max.=50)</td></tr><tr><td>Address:</td><td><input type="text"/> (Max.=200)</td></tr><tr><td>City:</td><td><input type="text"/> (Max.=50)</td></tr><tr><td>State / Province:</td><td><input type="text"/> (Max.=50)</td></tr><tr><td>Zip / Postal Code:</td><td><input type="text"/> (Max.=10)</td></tr><tr><td>Country:</td><td><input type="text"/> (Max.=50)</td></tr><tr><td>Contact Name:</td><td><input type="text"/> (Max.=50)</td></tr><tr><td>Contact Telephone:</td><td><input type="text"/> (Max.=50)</td></tr><tr><td>Contact FAX:</td><td><input type="text"/> (Max.=50)</td></tr><tr><td>Contact Email:</td><td><input type="text"/> (Max.=50)</td></tr></table>	Location Name:	<input type="text"/> (Max.=50)	Address:	<input type="text"/> (Max.=200)	City:	<input type="text"/> (Max.=50)	State / Province:	<input type="text"/> (Max.=50)	Zip / Postal Code:	<input type="text"/> (Max.=10)	Country:	<input type="text"/> (Max.=50)	Contact Name:	<input type="text"/> (Max.=50)	Contact Telephone:	<input type="text"/> (Max.=50)	Contact FAX:	<input type="text"/> (Max.=50)	Contact Email:	<input type="text"/> (Max.=50)
Location Name:	<input type="text"/> (Max.=50)																				
Address:	<input type="text"/> (Max.=200)																				
City:	<input type="text"/> (Max.=50)																				
State / Province:	<input type="text"/> (Max.=50)																				
Zip / Postal Code:	<input type="text"/> (Max.=10)																				
Country:	<input type="text"/> (Max.=50)																				
Contact Name:	<input type="text"/> (Max.=50)																				
Contact Telephone:	<input type="text"/> (Max.=50)																				
Contact FAX:	<input type="text"/> (Max.=50)																				
Contact Email:	<input type="text"/> (Max.=50)																				
<b>Date/Time</b>	<p>Date: 2010 / 6 / 22 (Year/Month/Day)</p> <p>Time: 9 : 44 : 51 (Hour : Minute : Second)</p> <table border="1"><tr><td>Time Zone</td><td>GMT</td></tr><tr><td><input type="checkbox"/> Daylight Saving Time</td><td>Start Date: 4 Month / 1 Day End Date: 10 Month / 31 Day</td></tr></table> <p><input type="button" value="Get from my Computer"/> <input type="button" value="Get from NTP server"/></p> <p><input type="checkbox"/> <b>NTP Setting</b></p> <table border="1"><tr><td>Server IP/Domain Name</td><td><input type="text"/></td></tr><tr><td>Update Time</td><td>0 hours</td></tr></table>	Time Zone	GMT	<input type="checkbox"/> Daylight Saving Time	Start Date: 4 Month / 1 Day End Date: 10 Month / 31 Day	Server IP/Domain Name	<input type="text"/>	Update Time	0 hours												
Time Zone	GMT																				
<input type="checkbox"/> Daylight Saving Time	Start Date: 4 Month / 1 Day End Date: 10 Month / 31 Day																				
Server IP/Domain Name	<input type="text"/>																				
Update Time	0 hours																				

Figure 27 System Setting Screen

<b>IIAT (Network Address Translation)</b>	<input checked="" type="radio"/> <b>Enable</b> <input checked="" type="checkbox"/> IP Plug and Play <input type="radio"/> <b>Disable</b>																				
<b>Session Limit</b>	<input checked="" type="radio"/> <b>Enable</b> <input type="text" value="100"/> (1~1024) <input type="radio"/> <b>Disable</b>																				
<b>Layer 2 Isolation Security</b>	<input checked="" type="radio"/> <b>Enable</b> <input type="radio"/> <b>Disable</b>																				
<b>Secure administrator IP addresses</b>	<input checked="" type="radio"/> <b>Any</b> <input type="radio"/> <b>Specify</b> <table border="1"> <tr><td>1</td><td><input type="text"/></td><td>~</td><td><input type="text"/></td></tr> <tr><td>2</td><td><input type="text"/></td><td>~</td><td><input type="text"/></td></tr> <tr><td>3</td><td><input type="text"/></td><td>~</td><td><input type="text"/></td></tr> <tr><td>4</td><td><input type="text"/></td><td>~</td><td><input type="text"/></td></tr> <tr><td>5</td><td><input type="text"/></td><td>~</td><td><input type="text"/></td></tr> </table>	1	<input type="text"/>	~	<input type="text"/>	2	<input type="text"/>	~	<input type="text"/>	3	<input type="text"/>	~	<input type="text"/>	4	<input type="text"/>	~	<input type="text"/>	5	<input type="text"/>	~	<input type="text"/>
1	<input type="text"/>	~	<input type="text"/>																		
2	<input type="text"/>	~	<input type="text"/>																		
3	<input type="text"/>	~	<input type="text"/>																		
4	<input type="text"/>	~	<input type="text"/>																		
5	<input type="text"/>	~	<input type="text"/>																		
<b>Multicast Pass Through</b>	<input type="radio"/> <b>Enable</b> <input checked="" type="radio"/> <b>Disable</b>																				
<b>Allow remote user to ping the device</b>	<input checked="" type="radio"/> <b>Enable</b> <input type="radio"/> <b>Disable</b>																				
<b>SSL Certificate</b>	<input checked="" type="radio"/> <b>Default</b> <input type="radio"/> <b>Customer Certificate</b>																				
<input type="button" value="Apply"/>																					

Figure 28 System Setting Screen

Item	Default	Description
System/Host Name	Empty	The system name can consist of up to 40 alphanumeric characters.
Domain Name	Empty	The Domain name can consist of up to 80 alphanumeric characters.
Location Information	Empty	Enter your location information.
<b>Date/Time</b>		
Date (Year/Month/Day)	System Date	The system date of the GuestWiFi. The valid setting of year is from 2002 to 2035.
Time (Hour:Minute:Second)	System Time	The system time of the GuestWiFi.
<input type="button" value="Get from my Computer"/>	-	Click "Get from my Computer" button to correct the system date and time.
<input type="button" value="Get from NTP server"/>	-	Click "Get from NTP server" button to correct the system date and time.

Item	Default	Description
NTP Setting	Disable	Enables or disables NTP (Network Time Protocol) Time Server. Network Time Protocol can be utilized to synchronize the time on devices across a network. A NTP Time Server is utilized to obtain the correct time from a time source and adjust the local time.
Server IP/Domain Name	Empty	Enter the IP address/domain name of NTP server. The maximum allowed characters length is 100.
Time Zone	GMT-12:00	Select the appropriate time zone for your location.
Update Time	0 hours	Enter the number of hours for update time.
Daylight Saving Time	Disable	Enables or disables Daylight Saving Time (DST).
	Month/Day	Set the Daylight Saving Time (DST) on the GuestWiFi. Adjust the begin time and end time.
NAT (Network Address Translation)		
NAT	Enable	Enables or disables NAT Address Translation function.
User Session Limited	Enable,30	Enables or disables user session limit function. This feature provides you an ability to control a number of sessions allowed for particulars user(s) at the one time.
IP Plug and Play (iPnP Technology)	Enable	Enables or disables plug & play function. When enabled, the user needn't change their network configuration to access the Internet.
Layer 2 Isolation Security	Enable	If enable plug and play is selected, you can enable Layer 2 Isolation Security function. When the "Layer 2 Isolation Security" enabled, everyone cannot communicate with each other.
Secure administrator IP Addresses	Any	Options: Any and Specify. Administrator can specify 5 IP addresses or a range to allow remote control access from network.
Multicast Pass Through	Disable	This function allows for multiple transmissions to specific recipients at same time.
Allow remote user to ping the device	Enable	This function allows remote user to ping the GuestWiFi through Internet. Ping is normally used to test the physical connection between two devices, to ensure that everything is working correctly.

Item	Default	Description
SSL Certificate	Default	Option: default or customize certificate, These are two ways to create a certificate, one is purchase a certificate from a certificate authority (Ex. Verisign or Thawte), and another is creating a self-certificate (For example: Uses OpenSSL tool).

**Apply**

Click **Apply** button to save the new settings.

Click **Apply** button, then Restart dialog box will appear. Click **Apply** to restart the system.

## RESTART

**Do you want to restart the system ?**

**Apply**

Figure 29 Restart Dialog Box

### 3-2-3-2 WAN/LAN

## WAN / LAN

<b>LAN</b>	<p style="color: blue;"><b>The Device IP Address and Subnet mask settings</b></p> <p>IP Address: <input type="text" value="10.59.1.1"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p>
<b>WAN MAC Address</b>	<p><input checked="" type="radio"/> Default</p> <p><input type="radio"/> Change to: <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/></p>
<b>WAN MTU Setting</b>	<p>Wan Port Maximum Transmission Unit: <input type="text" value="1500"/></p>
<b>WAN Port Mode</b>	<p><input checked="" type="radio"/> <b>DHCP Clients</b> (Mostly for Cable modem users or Local Area Network )</p> <p><input type="radio"/> <b>Static IP</b> (Mostly for advanced Local Area Network environment )</p> <p><input type="radio"/> <b>PPPoE</b> (Mostly for ADSL modem users )</p> <p><input type="radio"/> <b>PPTP</b> (Mostly for Europe ADSL modem users )</p>

**Apply**

Figure 30 WAN/LAN Setting Screen

**Apply**

Click **Apply** button to save the new settings.

Click **Apply** button, then Restart dialog box will appear. Click **Apply** to restart the system.

## RESTART

Do you want to restart the system ?

Apply

Figure 31 Restart Dialog Box

### ● Device IP (LAN IP) Setting

## WAN / LAN

### LAN

#### The Device IP Address and Subnet mask settings

IP Address:

Subnet Mask:

Figure 32 Device IP (LAN IP) Setting

Item	Default	Description
IP Address	10.59.1.1	The internal LAN IP address of your Wireless Subscriber Server Gateway.
Subnet Mask	255.0.0.0	Enter the subnet mask for the IP address.

### ● WAN MAC Address

#### WAN MAC Address

Default

Change to:  :  :  :  :  :

Figure 33 WAN MAC Address Setting

Item	Description
IP Address	The default MAC address is set to the WAN physical interface on device.

### ● WAN Port Mode

#### WAN Port Mode

**DHCP Clients** ( Mostly for Cable modem users or Local Area Network

**Static IP** ( Mostly for advanced Local Area Network environment )

**PPPoE** ( Mostly for ADSL modem users )

**PPTP** ( Mostly for Europe ADSL modem users )

Figure 34 WAN Port Mode Setting

## DHCP Client

The device can work as a DHCP client. This allows the device to obtain the IP address and other TCP/IP settings from your ISP. If your xDSL/Cable comes with this feature, please enable Use DHCP Client.

**DHCP Clients** ( Mostly for Cable modem users or Local Area Network )

Figure 35 DHCP Client Setting Screen

## Static IP

**Static IP** ( Mostly for advanced Local Area Network environment )

You have static IP information from your ISP

IP Address:

Subnet Mask:

Gateway IP address:

Primary DNS Server:

Secondary DNS Server:

Figure 36 Static IP Setting Screen

Item	Description
IP Address	Enter the IP address for the xDSL/Cable connection (provided by your ISP).
Subnet Mask	Enter the subnet mask for the IP address.
Gateway IP Gateway	Enter the Gateway IP address for the xDSL/Cable connection (provided by your ISP).
Primary DNS Server	A primary DNS server IP address for the xDSL/Cable connection (provided by your ISP).
Secondary DNS Server	A secondary DNS server IP address for the xDSL/Cable connection (provided by your ISP). If the primary DNS Server IP were not available, meanwhile, Secondary DNS Server IP would start in the same time.

## PPPoE

**PPPoE** ( Mostly for ADSL modem users )

**Your ISP requires you to input username / password**

Username:

Password:

PPP MTU Setting:

TCP MSS Setting:

Service Name:

**Connect on Demand** Max Idle Time:  Min.

**Keep alive** Redial Period:  Sec.

Figure 37 PPPoE Setting Screen

Item	Default	Description
User Name	Empty	Enter your PPPoE account name. The user name can consist of up to 80 alphanumeric characters and is case sensitive.
Password	Empty	Enter your PPPoE password. The password can consist of up to 80 alphanumeric characters and is case sensitive.
PPP MTU Setting	1492	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.
TCP MSS Setting	1452	MSS (Maximum Segment Size) specifies maximum segment size.

Item	Default	Description
Service Name	Empty	Enter the service name provided by your ISP. The service name can consist of up to 64 alphanumeric characters and is case sensitive.
<b>Connect on Demand and Max Idle Time</b>		
Connect on Demand	Enable	You can configure your GuestWiFi to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your GuestWiFi to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain, click the radio button of keep alive. The Max Idle Time maximum value is 65535 minutes.
Max Idle Time	10 Minutes	
<b>Keep alive and Redial Period</b>		
Keep alive	Disable	This option keeps your PPPoE enabled Internet access connected indefinitely, even when it sits idle. The Redial Period maximum value is 65535 seconds.
Redial Period	30 Seconds	



## PPTP

**PPTP** ( Mostly for Europe ADSL modem users )

Your ISP requires you to input username / password / PPTP setting

My IP Address:

My Subnet Mask:

Gateway IP address:

PPTP Server IP Address:

Username:

Password:

PPP MTU Setting:

TCP MSS Setting:

Connection ID/Name:

**Connect on Demand**

Max Idle Time:  Min.

**Keep alive**

Redial Period:  Sec.

Figure 38 PPTP Setting Screen

Item	Default	Description
My IP Address	Empty	A PPTP local IP address for the xDSL/Cable connection (provided by your ISP).
My Subnet Mask	Empty	Enter the PPTP local IP address for the xDSL/Cable connection.
Gateway IP Address	Empty	A PPTP local default gateway for the xDSL/Cable connection (provided by your ISP).
PPTP Server IP Address	Empty	Enter the PPTP server IP address for the xDSL/Cable connection (provided by your ISP).
Username	Empty	Enter your PPTP account name. The user name can consist of up to 80 alphanumeric characters and is case sensitive.

Item	Default	Description
Password	Empty	Enter your PPTP password. The password can consist of up to 80 alphanumeric characters and is case sensitive.
PPP MTU Setting	1460	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.
TCP MSS Setting	1400	MSS (Maximum Segment Size) specifies maximum segment size.
Connection ID/Name	Empty	Enter the connection ID or connection name. The connection ID/Name can consist of up to 81 alphanumeric characters and is case sensitive.
<b>Connect on Demand and Max Idle Time</b>		
Connect on Demand	Enable	You can configure your GuestWiFi to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables your GuestWiFi to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain, click the radio button of keep alive. The Max Idle Time maximum value is 65535 minutes.
Max Idle Time	10 Minutes	
<b>Keep alive and Redial Period</b>		
Keep alive	Disable	This option keeps your PPTP enabled Internet access connected indefinitely, even when it sits idle. The Redial Period maximum value is 65535 seconds.

### 3-2-3-3 Server

## SERVER

Server

Static DHCP

<b>Web Server</b>	<input checked="" type="radio"/> HTTP Port: <input type="text" value="80"/> (80, 8010 - 8060) <input type="radio"/> HTTPS Port: <input type="text" value="443"/> (443, 4430 - 4440) Administrator Idle-Timeout: <input type="text" value="5"/> Min(s) (1 - 1440)										
<b>DHCP Server</b>	<input type="radio"/> DHCP Disable <input type="radio"/> DHCP Relay <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">                     DHCP Server IP Address: <input style="width: 100%;" type="text"/> </div> <input checked="" type="radio"/> DHCP Server <div style="border: 1px solid black; padding: 2px;">                     DHCP Server  <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="border-bottom: 1px solid black;">IP Pool Starting Address:</td> <td style="border-bottom: 1px solid black;"><input type="text" value="10.59.1.2"/></td> </tr> <tr> <td style="border-bottom: 1px solid black;">Pool Size:</td> <td style="border-bottom: 1px solid black;"><input type="text" value="253"/> (Max.=253)</td> </tr> <tr> <td style="border-bottom: 1px solid black;">Lease Time:</td> <td style="border-bottom: 1px solid black;"><input type="text" value="300"/> (Minutes)</td> </tr> <tr> <td style="border-bottom: 1px solid black;">Primary DNS Server:</td> <td style="border-bottom: 1px solid black;"><input type="text" value="10.59.1.1"/></td> </tr> <tr> <td style="border-bottom: 1px solid black;">Secondary DNS Server:</td> <td style="border-bottom: 1px solid black;"><input style="width: 100%;" type="text"/></td> </tr> </table> </div>	IP Pool Starting Address:	<input type="text" value="10.59.1.2"/>	Pool Size:	<input type="text" value="253"/> (Max.=253)	Lease Time:	<input type="text" value="300"/> (Minutes)	Primary DNS Server:	<input type="text" value="10.59.1.1"/>	Secondary DNS Server:	<input style="width: 100%;" type="text"/>
IP Pool Starting Address:	<input type="text" value="10.59.1.2"/>										
Pool Size:	<input type="text" value="253"/> (Max.=253)										
Lease Time:	<input type="text" value="300"/> (Minutes)										
Primary DNS Server:	<input type="text" value="10.59.1.1"/>										
Secondary DNS Server:	<input style="width: 100%;" type="text"/>										
<b>Email Server Redirect</b>	IP Address or Domain Name: <input style="width: 100%;" type="text"/> SMTP Port: <input type="text" value="25"/> (25, 2500 - 2599)										

Apply

*Figure 39 Server Setting Screen*

Item	Default	Description
<b>Web Server</b>		
HTTP Port	80	Enter the HTTP port number. The HTTP port allowed range is 80 or 8010 to 8060. For access the GuestWiFi system under NAT, please tab the "http://HTTP Port IP Address: Port Number".
HTTPS Port	443	Enter the HTTPS port number. The HTTPS port allowed range is 443 or 4430 to 4440. For access the GuestWiFi system, please tab the "https://HTTPS Port IP Address: Port Number".
Administrator Idle-Timeout	5 Minutes	The idle time out valid range is 1-1440. If the idle time out is set as 5 minutes, it means if the administrator doesn't send packet in 5 minutes, the administrator will logout automatically.

Item	Default	Description
DHCP Server	Enable	There are three types of DHCP Services. DHCP Disable—Disable the DHCP server function. DHCP Relay—Enable DHCP Relay function. DHCP Server—Enable DHCP server function.
DHCP Relay	To route DHCP through an external server, the administrator needs to enable the DHCP relay and assign a valid DHCP server IP address.	
DHCP Server IP Address	Empty	Enter the IP address of DHCP server.
DHCP Server	The GuestWiFi's DHCP server is turned on and running by default when you install it in your network.	
DHCP Pool Starting Address	10.59.1.2	Enter the DHCP Pool Starting IP address.
Pool Size	253	The DHCP pool size range is 1 to 512.
Lease Time	300 Minutes	The DHCP lease time. The DHCP lease time range is 1 to 71582788 minutes.
Primary DNS Server	168.95.1.1	Enter the IP address of the network's primary DNS server.
Secondary DNS Server	Empty	Enter the IP address of a second DNS server on the network.
Email Server Redirect	To prevent some subscriber's original Email server may protect by firewall or NAT network. GuestWiFi provides an extra Email server parameter to forward the subscriber's Email. The GuestWiFi not only forwards the subscribers' E-mail via other E-mail server but also changes the SMTP header. The recipient of your E-mail sees the message as if you sent it from your local Internet Service Provide, not form the hotel or other place. Note: Before setting this sever, please make sure the e-mail sever relay function is opened. It must not exceed 50 characters.	
IP Address or Domain Name	Empty	Enter the E-mail server IP address or domain name.
SMTP Port	25	Enter the SMTP port number for mail server. The SMTP port allowed range is 25 or 2500 to 2599.

Apply

Click **Apply** button to save the new settings.

## Static DHCP

This function allows subscriber to assign IP address on the LAN to specific individual computers based on their MAC Address.

**SERVER**

Server **Static DHCP**

NO.	IP Address	MAC Address	NO.	IP Address	MAC Address
1	<input type="text"/>	<input type="text"/>	26	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	27	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	28	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	29	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	30	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	31	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	32	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	33	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	34	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	35	<input type="text"/>	<input type="text"/>
24	<input type="text"/>	<input type="text"/>	49	<input type="text"/>	<input type="text"/>
25	<input type="text"/>	<input type="text"/>	50	<input type="text"/>	<input type="text"/>

Figure 40 Server Setting Screen

Item	Default	Description
IP Address	Empty	Enter the IP address that subscriber want to assign to the computer on LAN with the MAC address the subscriber will also specify
MAC Address	Empty	Enter the MAC address of a computer on your LAN

Click **Apply** button to save the new settings.

### 3-2-3-4 Wireless

#### WIRELESS

<b>General Setting</b>	Country: <input type="text" value="ESTI"/>
	Channel: <input type="text" value="6"/>
	802.11 Mode: <input type="text" value="802.11n + 802.11g + 802.11b"/>
	Channel Width: <input type="text" value="Auto 20/40 MHz"/>

Do not change any setting below unless you make sure you understand all the meaning of setting. You can press "DEFAULT" to restore the wireless factory default setting once you made setting changed to cause wireless not work.

<b>Beacon Interval</b>	<input type="text" value="100"/> (msec, range:1~1000, default:100)
<b>RTS Threshold</b>	<input type="text" value="2342"/> (range:256~2342, default:2342)
<b>Fragmentation Threshold</b>	<input type="text" value="2346"/> (range:256~2346, default:2346, even number only)
<b>Preamble Type</b>	<input type="radio"/> Short Preamble <input checked="" type="radio"/> Long Preamble <input type="radio"/> Dynamic Preamble

*Figure 41 Wireless Setting Screen*

Item	Default	Description
<b>General Settings</b>		
Country	ESTI	
Channel	6	Select the channel ID for wireless connection.
802.11 mode	802.11n+802.11g+802.11b	
Channel width	Auto 20/40MHz	
Beacon Interval	200	This value valid range is 1 to 1000 indicates the frequency interval of the beacon.
RTS Threshold	2347	This value valid range is 256-2342. This setting determines the packet size at which the GuestWiFi issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the GuestWiFi, or in areas where the clients are far apart and can detect only the GuestWiFi and not each other.
Fragmentation Threshold	2432	This setting determines the size at which packets are fragmented. Enter a setting ranging from 256 to 2432 bytes. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
Preamble Type	Long Preamble	The preamble type is a section of data at the head of a packet that contains information the GuestWiFi and client devices need when sending and receiving packets. The setting menu allows you to select a long, short or dynamic preamble type.

Apply

Click Apply button to save the new settings.

Click Apply button, the restart dialog box appears. Click on Apply to restart the system.

## RESTART

Do you want to restart the system ?

Apply

Figure 42 Restart Dialog Box

Default

This operation will load the default manufacturer configuration to the system. All this page (Wireless) configuration setup will be replaced by default settings.

### 3-2-4 GUEST SETTING

#### 3-2-4-1 Guest ESSID Settings

GUEST ESSID SETTINGS	
General Setting	<input checked="" type="radio"/> Active <input type="radio"/> Inactive ESSID <input type="text" value="Guest"/>
Security Setting	<input type="radio"/> Disable <input type="radio"/> WPA <input checked="" type="radio"/> WPA2 Group Key Rekeying: Per <input type="text" value="86400"/> Seconds <input checked="" type="radio"/> Use WPA with Pre-shared Key Pre-shared Key: <input type="text" value="8"/> (randomly generated; 8-10 characters) <input type="radio"/> Use WPA with RADIUS Server Server IP: <input type="text"/> Authentication Port: <input type="text"/> Shared Secret Key: <input type="text"/>
<p>Apply</p>	

Figure 43 Guest ESSID Settings Screen

Item	Default	Description
General Settings	Active	Active or inactive the wireless connection interface.
ESSID	Guest	The ESSID is the unique name that is shared among all points in a wireless network. It is case sensitive and must not exceed 32 characters.
Security	Enable	Select disable to allow wireless station to communicate with the device without any data encryption. Select enable to enable WPA or WPA2 data encryption.
WPA2 and WPA Encryption	Wi-Fi Protected Access Encryption	
Group Key Re-Keying	86400 Seconds	Enter a number in the field to set the force re-keying interval.
Pre-shared Key	Empty	The GW-1 will randomly to generating. (8-10 characters)
Use WPA with RADIUS	Disable	
Server IP	Empty	Enter the RADIUS server IP address or domain name. The maximum allowed characters length is 15.
Authentication Port	1812	Enter the authentication port number. The allowed numbers are from 0 to 65535.
Share Secret Key	Empty	Enter the RADIUS secret key



### 3-2-4-2 Authentication

#### AUTHENTICATION

Authentication Type	<input type="radio"/> No Authentication <input checked="" type="radio"/> Built-in Authentication <input type="radio"/> User Agreement <input type="radio"/> Redirect URL Link: <input style="width: 150px;" type="text"/> <a href="#">Code</a> <input type="radio"/> Standard User Agreement page
Current User Information Backup	<input style="width: 30px;" type="text"/> Min(s) (1 - 1440)
SSL Login Page	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

*Figure 44 Authentication Setting Screen*

Item	Default	Description
Authentication Type	No Authentication	<p>Option: No Authentication, Built-in Authentication or User Agreement.</p> <p><b>No Authentication—</b> Subscriber can direct access the Internet without enter username and password.</p> <p><b>Built-in Authentication—</b> Wireless Subscriber Gateway provides “Built-in Authentication” for service provider to build up an Internet service without any extra authentication software. If “Built-in Authentication” is selected, service provider can generate the subscriber account inside Wireless Subscriber Gateway, and the system will authenticate the subscriber login according to the generated account.</p> <p><b>User Agreement—</b> Subscriber must accept the service usage agreement before they can access the Internet.</p>

Item	Default	Description
Current User Information Backup	1 Min(s)	The system provides automatically backup account information and unused account to flash ROM. This function allow administrator to adjust the backup time. The default value is 1 minute. The Current User Information Backup valid range is 1 to 1440.
Redirect Login Page URL	Empty	The input format can be http://www.yahoo.com. The maximum character of the URL Link is 200.
Code	Copy and paste the following HTML Code into your home page to produce redirect subscriber login page.	

Copy and paste the following HTML Code into your home page to produce user agreement login page.

**Redirect Agreement Page Code**

```

<html>
<body>

<center>
<table width="100%" border="0">
<tr>
<td align="right" width="45%">

<form method="post" action="http://1.1.1.1/agree.cgi" name="agree">
<input type="submit" name="agree" value="Agree">
</form>
</td>
<td width="10%"> </td>
<td width="45%">
<form method="post" action="http://1.1.1.1/agree.cgi" name="disagree">
<input type="submit" name="disagree" value="Do not agree">
</form>
</td>
</tr>
</table>
</center>

</body>
</html>

```

Figure 45 Preview Redirect Login Page Code

Item	Default	Description
SSL Login Page	Disable	Enables or disables SSL security of login page.

**Apply**

Click **Apply** button to save the new settings.

### 3-2-4-3 Usage Time

This function allow service provider to generate the subscriber accounts.

#### USAGE TIME

Expiration	Un-used account will be deleted after <input style="width: 40px;" type="text" value="12"/> hours <input type="button" value="▼"/> automatically. (1~30)
Usage Time	<input style="width: 40px;" type="text" value="3"/> hours <input type="button" value="▼"/>
ID Length	<input style="width: 40px;" type="text" value="4"/> <input type="button" value="▼"/>

Figure 46 Accounting Setting Screen

Item	Default	Description
Expiration		
Un-used account will be deleted after ~hours automatically	12 hours	Enter the number of hours/days. The field maximum value is 30 hours/ days.
Usage Time		
The duration of the period. When this period expired, user account will be discontinued.	3 hours	Enter the number of hours/days. The field maximum value is 30 hours/ days.
ID Length	4	The field maximum value is 4-6.

### 3-2-4-4 Customization

- **Login Page**

The guestWiFi provides three different login page formats, including standard, redirect, advanced and frame format.

#### **Standard**

For some service providers, they may hope to have a customize subscriber's login page to the users. This function helps them to realize the ideal. The page elements are including login page title, background color, subtitle etc.

## CUSTOMIZATION

Login Page
Logo
Information Window
User Agreement

Please choose from the following login page types

**Standard**

Please enter the customizable message on the **standard** login page

<input type="checkbox"/> Logo	
Title	<input type="text" value="Welcome"/> (Max. 80 characters)
Subtitle	<input type="text" value="Guest WiFi"/> (Max. 80 characters)
Enter Button	<input type="text" value="Enter"/> (Max. 20 characters)
Cancel Button	<input type="text" value="Cancel"/> (Max. 20 characters)
<input type="checkbox"/> Footnote	<input type="text" value="Please contact us if you have any questio"/> (Max. 240 characters)
<input checked="" type="checkbox"/> Copyright	<input type="text" value="Copyright (c) 2010-2012 All Rights Reserv"/> (Max. 80 characters)
Background Color	<input type="text" value="FFFFFF"/> <a href="#">View Color Grid</a>

[Standard Login Page Preview](#)

*Figure 47 Standard Login Page Customization Setting Screen*

Item	Default	Description
Logo	Disable	Select the check box to display service provider's logo.
Title	Welcome	Enter the title name of subscriber login page. The maximum allowed characters length is 80.
Subtitle	Guest WiFi	Enter the subtitle name of subscriber login page. The maximum allowed characters length is 80.
Footnote	Disable	Allow the administrator to input the footnote such like "Please Contact to our Customer Service Center, EXT 141". The maximum character of the footnote is 240.

Item	Default	Description
Copyright	Enable	The copyright is allowed the administrator to input a paragraph in the subscriber login page for copyright information. The maximum character of the copyright is 80.
Background Color	FFFFFF	The background text color can be specified color. For the specified text color format please views the color grid. The allowed format is Hexadecimal.



Figure 48 Login Page Screen

Before you add logo to the login page, please make sure the logo image file is defined. For details, see section 3-2-4-4 Customization->Logo



Figure 49 Error Dialog Box

## Redirect

This allow service provider to redirect the subscriber's browser to a specified home page.

<input type="radio"/> <b>Redirect</b>	Redirect Login Page URL : <input type="text"/>	<b>Code</b>
---------------------------------------	--	-------------

Figure 50 Redirect Login Page Setting Screen

Copy and paste the following HTML Code into your home page to produce redirect subscriber login page.

Redirect Login Page Code
<pre>&lt;html&gt; &lt;body style="font-family: Arial" bgcolor="#FFFFFF"&gt; &lt;form method="post" action="http://1.1.1.1/login.cgi" name="apply"&gt; &lt;div align="center"&gt; &lt;table cellSpacing="0" borderColorDark="#FFFFFF" cellPadding="4" width="50%" bgColor="#F7F7F7" borderColorLight="#4aa9ee" border="1"&gt; &lt;tr&gt; &lt;td align="center" width="100%" bgcolor="#F7F7F7" colSpan="2"&gt; &lt;font size="2"&gt;&lt;b&gt;Welcome&lt;/b&gt;&lt;/font&gt; &lt;/td&gt; &lt;tr&gt; &lt;td align="right" width="35%" bgColor="#eaeaea"&gt; &lt;font color="#000080" size="2"&gt;&lt;b&gt;ID:&lt;/b&gt;&lt;/font&gt; &lt;/td&gt; &lt;td width="65%"&gt; &lt;input type="text" name="ID" size="25"&gt; &lt;/td&gt; &lt;tr&gt; &lt;td align="center" width="100%" colspan="2"&gt; &lt;input type="submit" name="apply" value="Enter" style="font-family: Arial"&gt; &lt;input type="reset" name="clear" value="Clear" style="font-family: Arial"&gt; &lt;/td&gt; &lt;/tr&gt; &lt;/table&gt; &lt;/div&gt; &lt;/form&gt; &lt;/body&gt; &lt;/html&gt;</pre>
<input type="button" value="Close"/>

Figure 51 Redirect Login Page Code Screen

## Advanced

This function allow user to design login page of Wireless Subscriber Gateway.

<input type="radio"/> Advanced	Welcome Slogan	<input type="text"/>
	Page Background	<input checked="" type="radio"/> None <input type="radio"/> Background Color <input type="text" value="FFFFFF"/> <a href="#">View Color Grid</a>
	Article	<div style="border: 1px solid black; height: 80px; width: 100%;"></div>
	Article Text Color	<input type="text" value="000000"/> <a href="#">View Color Grid</a>
	Article Background Color	<input checked="" type="radio"/> None <input type="radio"/> <input type="text" value="FFFFFF"/> <a href="#">View Color Grid</a>
	Information	<input type="text"/>
	Comments	<input type="text"/>

Figure 52 Advanced Login Page Setting Screen

Item	Default	Description
Welcome Slogan	Welcome	The maximum allowed characters length is 80.
Page Background	None	The page background can be none or specified color. For the background color format please views the color grid. The allowed format is Hexadecimal.
Article	Empty	The article is allowed the administrator to input a paragraph in the subscriber login page for advisement or announcement. The maximum character of the article is 1024.
Article Text Color	000000	The article text color can be specified color. For the specified text color format please views the color grid. The allowed format is Hexadecimal.
Article Background Color	None	The article background can be specified color. For the background color format please views the color grid. The allowed format is Hexadecimal.
Information	Empty	Allow the administrator to input the text information such like address, telephone number and fax information. The maximum character of the information is 80.
Comments	Empty	Allow the administrator to input the text comments such like "Please Contact to our Customer Service Center, EXT 141". The maximum character of the comment is 80.

Browser Set Background Colors by RGB					
000000	000080	000080	000080	0000CC	0000FF
003300	003333	003366	003399	0033CC	0033FF
006600	006633	006666	006699	0066CC	0066FF
009900	009933	009966	009999	0099CC	0099FF
00CC00	00CC33	00CC66	00CC99	00CCCC	00CCFF
00FF00	00FF33	00FF66	00FF99	00FFCC	00FFFF
800000	800033	800066	800099	8000CC	8000FF
803300	803333	803366	803399	8033CC	8033FF
806600	806633	806666	806699	8066CC	8066FF
809900	809933	809966	809999	8099CC	8099FF
80CC00	80CC33	80CC66	80CC99	80CCCC	80CCFF
80FF00	80FF33	80FF66	80FF99	80FFCC	80FFFF
C00000	C00033	C00066	C00099	C000CC	C000FF
C03300	C03333	C03366	C03399	C033CC	C033FF
C06600	C06633	C06666	C06699	C066CC	C066FF
C09900	C09933	C09966	C09999	C099CC	C099FF
C0CC00	C0CC33	C0CC66	C0CC99	C0CCCC	C0CCFF
C0FF00	C0FF33	C0FF66	C0FF99	C0FFCC	C0FFFF
E00000	E00033	E00066	E00099	E000CC	E000FF
E03300	E03333	E03366	E03399	E033CC	E033FF
E06600	E06633	E06666	E06699	E066CC	E066FF
E09900	E09933	E09966	E09999	E099CC	E099FF
E0CC00	E0CC33	E0CC66	E0CC99	E0CCCC	E0CCFF
E0FF00	E0FF33	E0FF66	E0FF99	E0FFCC	E0FFFF

Figure 53 Color Grid

**Frame**

If “Frame” is selected the subscriber login page will be separate into Top Frame and Bottom Frame. Bottom Frame is a default format for username and password input, Top Frame is allowed to be specified a URL to link.

**www.caesarpark.com**

<input type="radio"/> Frame	Top Frame	URL: <input type="text" value="http://"/> <input style="border: 2px solid magenta;" type="text" value="www.caesarpark.com"/>
	Bottom Frame	This frame will show the standard login page

Figure 54 Frame Login Page Setting Screen

Item	Default	Description
Top Frame URL Link	Empty	The input format can be http://www.yahoo.com. The maximum character of the URL Link is 200.
Bottom Frame	-	This frame will show the standard login page.



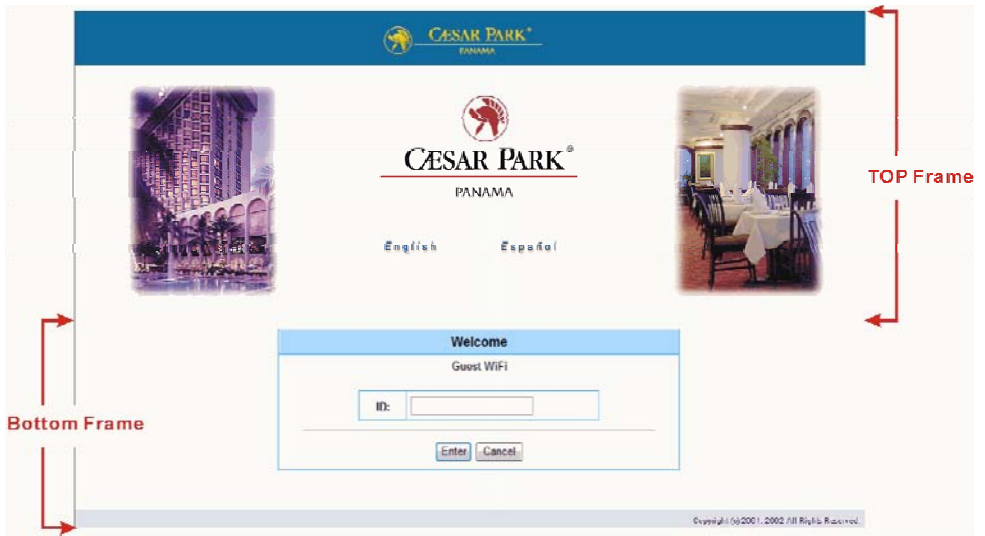


Figure 55 Example-Login Page Screen

- **Logo**

This function allows service provider to upload the customer's logo image file which can be shown on the standard login page and account printout of PC-connected printer.

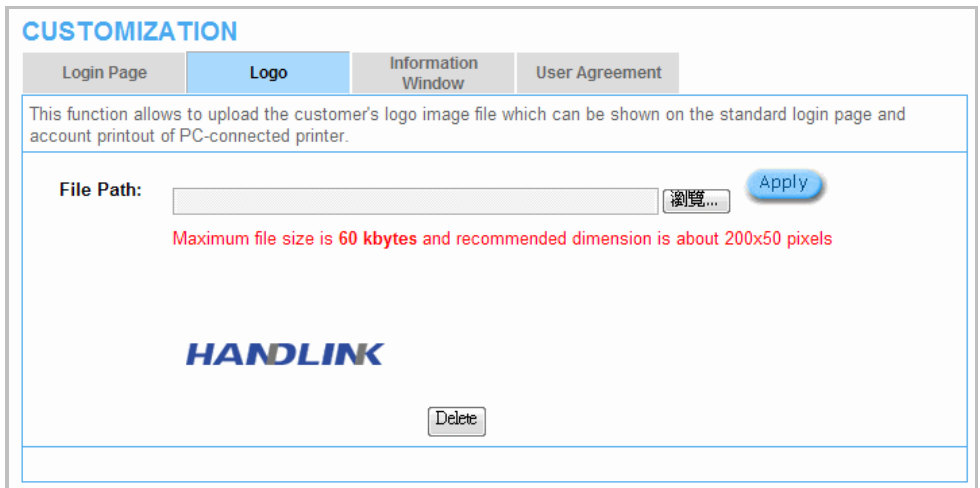




Figure 56 Logo Setting Screen



Figure 57 Login Page

Item	Default	Description
File Path	Empty	Enter the file pathname of the logo file in the File Path field.
		Click <b>Apply</b> button to save the logo file to system.
		Click <b>Delete</b> button to delete the logo file.

## Information Window

This function allow service provider can decide whether they want an “Information Window” pop-up on subscriber PC when authenticate successful or not and specified text of information window. Subscriber can type “http://1.1.1.1/info” to open the information window again or enter “http://1.1.1.1/logout” to logout immediately if accumulation billing selected.

### CUSTOMIZATION

Login Page	Logo	<b>Information Window</b>	User Agreement
------------	------	---------------------------	----------------

Information window is a pop-up window that is presented to subscribers with their browser once after subscriber login successfully. The subscriber can type http://1.1.1.1/info to open this window again.

**Display Information Window once after a subscriber logs in successfully**

Information Window Type	<input type="radio"/> Redirect <input checked="" type="radio"/> Pop Up
	<input checked="" type="checkbox"/> Allow to close the pop up window

#### Information Window Contents

Window Name	<input type="text" value="Information Window"/> (Max. 30 character)
Main message	<input type="text" value="You can use Internet now!"/> (Max. 30 character)
Message Description	<input type="text" value="This is an information window to sho"/> (Max. 150 character)
Time count label	Standard for pre-defined usage time
	<input type="text" value="Remaining Usage"/> (Max. 30 character)
	<input type="text" value="Post-Paid Billing"/> (Max. 30 character)
	<input type="text" value="Connecting Usage"/> (Max. 30 character)
<input type="checkbox"/> Warning/Alarm message	<input type="text" value="If you don't want to continue using In"/> (Max. 150 character)
<input type="checkbox"/> Notice Message	Notice Text 1
	<input type="text" value="Notice!"/> (Max. 150 character)
	Notice Text 2
	<input type="text" value="If you are going to use VPN connect"/> (Max. 150 character)
	<input type="text" value="Notice Text 3"/> (Max. 150 character)

[Preview](#)

Figure 58 Example-Login Page Screen

*Figure 59 Example-information windows Screen*

## User Agreement Page

This function allow user to design user agreement page of Internet Subscriber Server.

### CUSTOMIZATION

Login Page	Logo	Information Window	<b>User Agreement Page</b>
------------	------	--------------------	----------------------------

Title	<input type="text" value="User Agreement Page"/> (max. 100 Character)
Title Text Color	<input type="text" value="000000"/> <a href="#">View Color Grid</a>
Article	<div style="border: 1px solid #ccc; height: 60px;"></div> (max. 5000 Character)
Article Text Color	<input type="text" value="000000"/> <a href="#">View Color Grid</a>
Article Background Color	<input type="text" value="FFFFFF"/> <a href="#">View Color Grid</a>
Page Background Color	<input type="text" value="FFFFFF"/> <a href="#">View Color Grid</a>
Agree Button	<input type="text" value="Agree"/> (max. 50 character)
Disagree Button	<input type="text" value="Do not agree"/> (max. 50 character)


 [Standard User Agreement Page Preview](#)

Figure 60 User Agreement Page Setting Screen

## User Agreement Page

---

Figure 61 User Agreement Page

**3-2-5 EMPLOYEE ESSID SETTINGS**

### EMPLOYEE ESSID SETTINGS

<b>General Setting</b>	<input type="radio"/> Active <input checked="" type="radio"/> Inactive ESSID <input style="width: 100px;" type="text" value="Employee"/>
<b>Security Setting</b>	<input checked="" type="radio"/> Disable <input type="radio"/> WPA <input type="radio"/> WPA2 <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">                     Group Key Rekeying: Per <input style="width: 50px;" type="text" value="86400"/> Seconds  <input checked="" type="radio"/> Use WPA with Pre-shared Key                      Pre-shared Key: <input style="width: 150px;" type="text" value="1234567890"/> (8-63 characters)  <input type="radio"/> Use WPA with RADIUS Server                      Server IP: <input style="width: 100px;" type="text"/>                      Authentication Port: <input style="width: 100px;" type="text"/>                      Shared Secret Key: <input style="width: 100px;" type="text"/> </div>

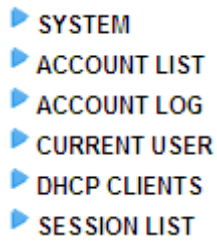
*Figure 62 Employee ESSID Setting Screen*

Item	Default	Description
General Settings	Active	Active or inactive the wireless connection interface.
ESSID	Guest	The ESSID is the unique name that is shared among all points in a wireless network. It is case sensitive and must not exceed 32 characters.
Security	Enable	Select disable to allow wireless station to communicate with the device without any data encryption. Select enable to enable WPA or WPA2 data encryption.
WPA2 and WPA Encryption	Wi-Fi Protected Access Encryption	
Group Key Re-Keying	86400 Seconds	Enter a number in the field to set the force re-keying interval.
Pre-shared Key	Empty	The GW-1 will randomly to generating. (8-10 characters)
Use WPA with RADIUS	Disable	
Server IP	Empty	Enter the RADIUS server IP address or domain name. The maximum allowed characters length is 15.
Authentication Port	1812	Enter the authentication port number. The allowed numbers are from 0 to 65535.
Share Secret Key	Empty	Enter the RADIUS secret key

### 3-3 System Status

Display GuestWiFi system basic status, including,

1. System
2. Account List
3. Account Log
4. Current User
5. DHCP Clients
6. Session List



*Figure 63 System Status Item Screen*

### 3-3-1 System

The System Information Menu displays current system basic information including the service connection message, host name, LAN, WAN, DHCP Configuration, DNS, SSL Certificate, network traffic Information and the system firmware version number.

#### SYSTEM

Display the detailed system information		
Service	Internet Connection	Fail
	Wireless Service	OK
System	Firmware Version	1.07.06
	Wireless Version	1.00a
	Bootrom Version	1.03
	Controller Firmware Version	1.00
	WAN MAC Address	00:90:0E:00:60:C1
	LAN MAC Address	00:90:0E:00:60:C0
	WLAN MAC Address	00:90:0E:00:60:C2
	System Time	2004/7/2 17:10:35
System Up Time	00D:01H:02M:48S	
LAN IP	Guest LAN IP Address	10.59.1.1
	Subnet Mask	255.255.255.0
	Employee LAN IP Address	10.59.2.1
	Subnet Mask	255.255.255.0
WAN IP	IP Port Mode	DHCP Client
	IP Address	None
	Subnet Mask	None
	Gateway IP address	None
DNS	Primary DNS Server	
	Secondary DNS Server	
Guest DHCP	DHCP Status	Server
	Start IP Address	10.59.1.2
	End IP Address:	10.59.1.254
	Lease Time	300

Figure 64 System Status Screen



<b>Employee DHCP</b>	DHCP Status	Server		
	Start IP Address	10.59.2.2		
	End IP Address:	10.59.2.254		
	Lease Time	300		
<b>Wireless</b>	Channel	10		
	ESSID	Guest:	Guest	
		Employee:	Employee	
	Secure Mode	Guest:	Enable	
		PSK:	a4s5d6f9e8	
		Employee:	Disable	
PSK:		1234567890		
<b>Network Traffic</b>	WAN Traffic	Tx Data: 500 Rx Data: 0 Tx Error: 0 Rx Error: 0		
	LAN Traffic	Tx Data: 4081 Rx Data: 3645 Tx Error: 0 Rx Error: 0		
	Wireless Traffic	Tx Data: 5 Rx Data: 0 Tx Error: 0 Rx Error: 0		

Figure 65 System Status Screen

### 3-3-2 Account List

You can display a list of all the account information on this device. This table includes the username, password, usage time, time created, login time, expiration time and status.

#### ACCOUNT LIST

List existing account's information. [refresh↻](#)

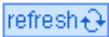
Status	PIN	Usage Time	Time Created	Login Time	Expiration Time	Delete
In-used	p2vy	10:00:00	2011-01-12 01:23:51	2011-01-12 01:24:06	2011-01-12 11:24:06	<input type="checkbox"/>
In-used	wsna	10:00:00	2011-01-12 01:24:29	2011-01-12 01:24:41	2011-01-12 11:24:41	<input type="checkbox"/>
In-used	hujq	10:00:00	2011-01-12 01:25:29	2011-01-12 01:25:35	2011-01-12 11:25:35	<input type="checkbox"/>
Un-used	nnaH	10:00:00	2011-01-12 03:42:31			<input type="checkbox"/>
Un-used	4rc3	10:00:00	2011-01-12 03:42:32			<input type="checkbox"/>
Un-used	uykf	10:00:00	2011-01-12 04:03:20			<input type="checkbox"/>

[Delete](#) [Delete All](#)

WIGO 1 PAGE

◀ First   Previous   Next   End ▶

Figure 66 Account List



Click on refresh button to update the account list page.



Click the column button to sort the column in ascending/descending order.



Select the check boxes and click 'Delete' to delete the accounts.



Delete all accounts in account list.

**Note:** This page will refresh automatically every 5 minutes.

### 3-3-3 Account Log

The account log shows the accounts' log information.

#### ACCOUNT LOG

List accounts log Export Clear Log refresh ↻

No.	PIN	Time Created	Login Time	Usage Time	Status
1	5vtr	2011-01-10 03:54:06	2011-01-10 03:54:32	01:00:00	Finished
17	ba44	2011-01-10 05:03:50	2011-01-10 09:30:03	01:00:00	Finished
18	653f	2011-01-10 05:03:51	2011-01-10 09:57:06	01:00:00	Delete
19	ixrr	2011-01-10 05:04:43		01:00:00	Delete
20	pxh2	2011-01-10 05:04:44		01:00:00	Expired
21	itss	2011-01-10 05:04:45	2011-01-10 10:47:41	01:00:00	Finished
7	4dyh	2011-01-10 04:08:06		01:00:00	Delete
8	bcyu	2011-01-10 04:08:08	2011-01-10 05:15:12	01:00:00	Finished
49	dymj	2011-01-10 05:05:25		01:00:00	Expired
50	as73	2011-01-10 05:05:26		01:00:00	Expired

IGO 1 PAGE

First Previous Next End

Figure 67 Account Log

#### Export

This allow you to export the account logs to a text file format. (export.log)

Clear Log

Click on **Clear Log** to remove all account log entries.

refresh ↻

Click on refresh button to update the account log page.

SN Username Time Created Login Time Usage Time Charge Status

Click the column button to sort the column in ascending/descending order.

### 3-3-4 Current User

Display the current logged-in subscribers' status. It allow service provider to disconnect any subscribers.

#### CURRENT USER

No.	Type	PIN	IP Address	MAC Address	Session	Delete
1	Guest	4wsz	10.59.1.3	B8:F9:34:1F:44:56	6	<input type="checkbox"/>
2	Guest	hujq	10.59.1.8	00:17:31:86:51:DB	0	<input type="checkbox"/>
3	Guest	wsna	10.59.1.5	00:0C:29:54:33:16	0	<input type="checkbox"/>
4	Guest	p2vy	10.59.1.2	00:23:6C:86:8B:18	0	<input type="checkbox"/>
5	Employee	****	10.59.2.2	20:CF:30:03:97:5B	24	<input type="checkbox"/>

MG0 1 PAGE

First Previous Next End

Delete Delete All

Figure 68 Current User List

No.	Type	IP Address	MAC Address	Session
1	No-Auth	10.59.1.2	00:30:1B:44:72:E1	2

MG0 1 PAGE

First Previous Next End

Figure 69 Current User List (No Authentication)



Click on refresh button to update the current user list page.

Type	Username	IP Address	MAC Address
------	----------	------------	-------------

Click the column button to sort the column in ascending/descending order.



Select the check boxes and click **'Disconnect'** to disconnect accounts.



Disconnect all accounts in current user list.

### 3-3-5 DHCP Clients

The DHCP client table shows the current DHCP users on the LAN.

#### DHCP CLIENTS

DHCP Clients Information, including assigned IP address and MAC address.

The DHCP Clients will be refresh every  minutes. (1~60 minute)

No.	MAC Address	IP Address
1	00:30:1B:44:72:E1	10.59.1.2

Figure 70 Current User Screen

### 3-3-6 Session List

The remote site administrator could monitor the real time usage status of GuestWiFi via this page.

#### SESSION LIST

List of sessions of Network events. Outgoing packet information, including source IP address, destination IP address, and port number.

The session list will be refresh every  minutes. (1~60 minute)

No.	TCP/UDP	Client IP	Client Port	Port Fake	Remote IP	Remote Port	Idle
1	tcp	10.59.1.2	2423	2423	207.46.124.106	1863	1185

PAGE

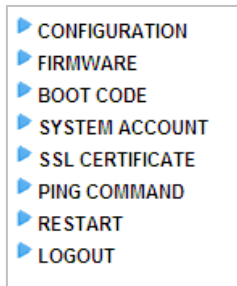
⏪ First    ◀ Previous    Next ▶    End ⏩

Figure 71 Session List Screen

### 3-4 System Tools

This allows service provider or administrator to process Firmware upgrade, change password and backup or restore configuration.

1. Configuration
2. Firmware
3. Boot Code
4. System Account
5. SSL Certificate
6. Ping Command
7. Restart
8. Logout



*Figure 72 System Tools Item*

### 3-4-1 Configuration

Use the Configuration item to save, restore or reset configuration parameters of the GuestWiFi.

**CONFIGURATION**

This feature can backup the system configuration from this device to your PC or restore your stored system configuration to this device.

<b>Backup</b>	Click Backup to backup the system configuration from this device to your computer or to the remote TFTP server. Remote TFTP Server IP Address: <input style="width: 150px;" type="text"/> File Name: <input style="width: 150px;" type="text"/>	<input type="button" value="Apply"/>
<b>Restore</b>	To restore your stored system configuration to this device.  Local PC File Path: <input style="width: 250px;" type="text"/> <input type="button" value="浏览..."/> Remote TFTP Server IP Address: <input style="width: 150px;" type="text"/> File Name: <input style="width: 150px;" type="text"/>	<input type="button" value="Apply"/>
<b>Reset the system back to factory defaults</b>	<input type="checkbox"/> Keep subscriber profile	<input type="button" value="Apply"/>

Figure 73 Configuration Setting Screen

Item	Default	Description
Backup		Click it to save the system configuration to your computer. (export.cfg)
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.
Restore		Click it to restore your system configuration.
Local PC File Path	Empty	Enter the file pathname of the system configuration file in the Local PC File Path field.
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.
Reset the system back to factory defaults		Erase all setting and back to factory setting.
Keep subscriber profile	Disable	Click the keep subscriber profile to change all the parameters into factory setting but still reserve the subscriber profiles.

### 3-4-2 Firmware Upgrade

The Firmware Upgrade menu loads updated firmware to be permanent in flash ROM. The download file should be a binary file from factory; otherwise the agent will not accept it. After downloading the new firmware, the agent will automatically restart it.

#### ● Manual Firmware Upgrade

**FIRMWARE**

Manual Firmware Upgrade | Scheduled Firmware Upgrade

To upgrade the firmware, click **Browse** to locate the firmware file or use remote TFTP server and click **Apply**.

Local PC File Path

Remote TFTP Server IP Address

File Name

Figure 74 Manual Firmware Upgrade Setting Screen

Item	Default	Description
<b>This allow administrator to upgrade the firmware via HTTP.</b>		
Local PC File Path	Empty	Enter the file name and location in the Local PC File Path field.
<b>This allows administrator use TFTP server to upgrade firmware.</b>		
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.

#### **Note:**

1. Before downloading the new firmware, users must save the configuration file for restore configuration parameters of the device.
2. Do not turn the power off during the upgrade process. This will damage the unit.



## ● Scheduled Firmware Upgrade

Scheduled Firmware Upgrade is a program that enables an automatic upgrade to the latest firmware version through the TFTP server.

### FIRMWARE

Figure 75 Scheduled Firmware Upgrade Setting Screen

Item	Default	Description
Disable/Enable	Disables or enables the scheduled firmware upgrade function.	
TFTP Server IP	Empty	Enter the IP address of TFTP Server.
File Synchronization	Empty	Enter the file name and location in the File Synchronization field.
<a href="#">View Sample File</a>	Click the button to display synchronization file example.	
Frequency	Weekly	Set the firmware upgrade time. The default value is “Weekly”.

Figure 76 Synchronization File Sample Code

---

**Note:** Do not turn the power off during the upgrade process. This will damage the unit.

---

### 3-4-3 Boot Code

**BOOT CODE**

To upgrade the Boot Code, click Browse to locate the file and click Apply.

Local PC File Path :

Figure 77 Boot Code Upgrade Setting Screen

### 3-4-4 System Account

Use the System Account screen to change the system accounts.

## SYSTEM ACCOUNT

**Administrator Account**

Administrator can fully control this system and modify all settings.

Username:

Password:

Confirm:

Figure 78 System Account Setting Screen

Item	Description
Username	The username can consist of up to 20 alphanumeric characters and is sensitive.
Password	The password can consist of up to 20 alphanumeric characters and is sensitive.
Confirm	The password for confirmation.

- **Administrator Account**

Step 1: Start your Web browser and enter the factory default IP address **10.59.1.1** in your browser's location box. Press Enter.



Figure 79 Web Browser Location Field (Factory Default)

Step 2: The GuestWiFi configuration main menu will appear. Enter **admin** (default) as the Username and **admin** (default) as the password and click **Login**. If you are first time setting the system, the wizard setup screen will appear.

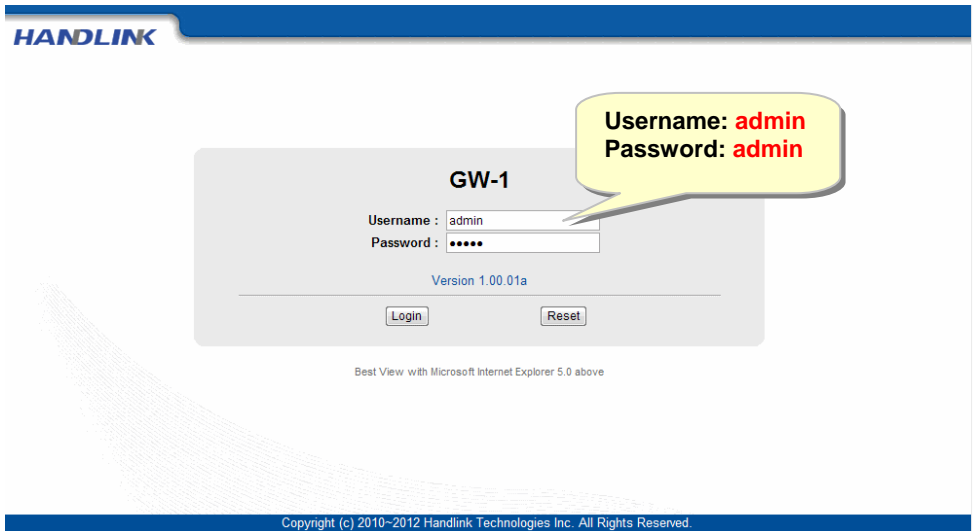


Figure 80 Administrator Account Login Screen (First Time)

## System Quick View

System			
System/Host Name		Firmware Version	1.07.06
Location Name		Domain Name	
System Time	2004/7/2 16:08:58	System Up Time	00D:00H:01M:11S
WAN MAC address	00:90:0E:00:60:C1	LAN MAC address	00:90:0E:00:60:C0
		WLAN MAC address	00:90:0E:00:60:C2

[refresh](#)

Network			
WAN Status	Not Established	WAN Type	DHCP Client
WAN IP Address	192.168.100.230	WAN Subnet Mask	255.255.255.0
Default Gateway	192.168.100.254	DNS	192.168.100.2
Guest LAN IP Address	10.59.1.1	Guest LAN Subnet Mask	255.255.255.0
Employee LAN IP Address	10.59.2.1	Employee LAN Subnet Mask	255.255.255.0

Wireless			
Wireless Service	OK	Guest ESSID	Guest
		Guest Secure Mode	Enable
Wireless Channel	10	Employee ESSID	Employee
		Secure Mode	Disable

Traffic	
WAN	TxData:10 RxData:0 TxError:0 RxError:0
LAN	TxData:83 RxData:77 TxError:0 RxError:0
Guest Wireless	TxData:2 RxData:0 TxError:0 RxError:0
Employee Wireless	TxData:2 RxData:0 TxError:0 RxError:0

[refresh](#)

Best View with Microsoft Internet Explorer 5.0 above

Figure 81 System Quick View

### 3-4-5 SSL Certificate

The function allows you to download the registered CA certificate into the GuestWiFi.

## SSL CERTIFICATE

This feature allows you to download the registered CA certificate into this device.

<b>Password for Private Key:</b>	<input type="text"/>
<b>Certificate File:</b>	<input type="text"/> <a href="#">瀏覽...</a>
<b>Private Key File:</b>	<input type="text"/> <a href="#">瀏覽...</a>

[Apply](#)

Figure 82 SSL Certificate Download Setting Screen

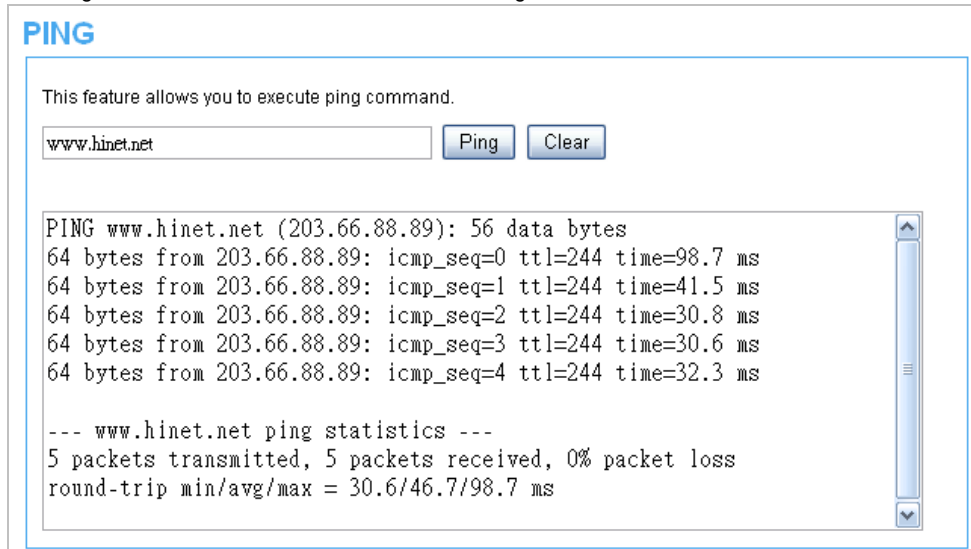
---

**Note:** The password field must be the same as the CA's registered password.

---

### 3-4-6 Pin Command

The Ping function can check the GuestWiFi networking connective or not.

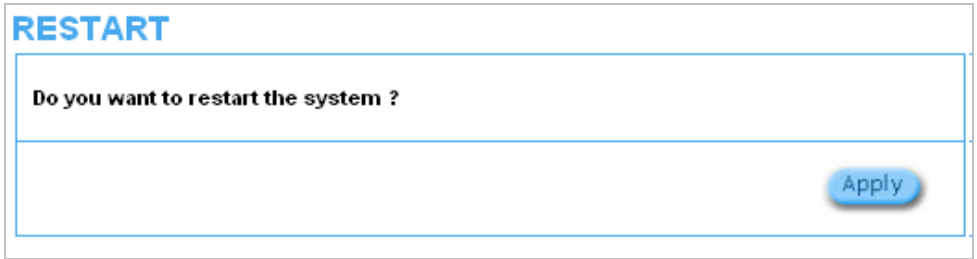


*Figure 83 Ping Command Screen*

Item	Description
IP or URL	Enter the IP address or the URL link.

### 3-4-7 Restart

If your GuestWiFi is not operating correctly, you can choose this option to display the restart GuestWiFi screen. Clicking the apply button restart the GuestWiFi, with all of your settings remaining intact.



**RESTART**

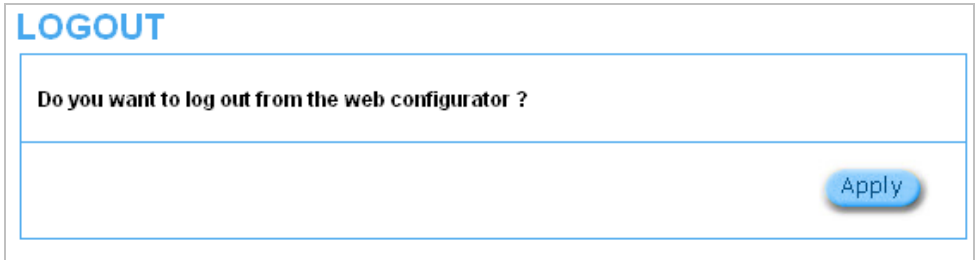
Do you want to restart the system ?

Apply

*Figure 84 Restart Screen*

### 3-4-8 Logout

If you would like to leave the configuration page, please click apply to exit.



**LOGOUT**

Do you want to log out from the web configurator ?

Apply

*Figure 85 Logout Screen*

## Appendix A Signal Connection Arrangements

### RJ-45 Ethernet Port

The GuestWiFi RJ-45 Ethernet port can connect to any networking devices that use a standard LAN interface, such as a Hub/Switch Hub or Router. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable to connect the networking device to the RJ-45 Ethernet port.

Depending on the type of connection, 10Mbps or 100Mbps, use the following Ethernet cable, as prescribed.

**10Mbps:** Use EIA/TIA-568-100-Category 3, 4 or 5 cable.

**100Mbps:** Use EIA/TIA-568-100-Category 5 cable.

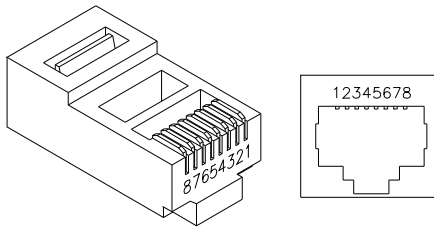


Figure 86 RJ-45 Connector and Cable Pins

---

**Note:** To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 meters.

---

## Appendix B Regulations/EMI Compliance

### FCC Statement

#### Federal Communication Commission 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 and, if not installed and used in accordance with the instructions, 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 to correct the interference by one of the following measures:

- Reorient or relocate 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/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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 and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

### IMPORTANT NOTE:

#### FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance **20cm** between the radiator & your body.



# LIMITED WARRANTY

## GuestWiFi

### **What the warranty covers:**

We warrant its products to be free from defects in material and workmanship during the warranty period. If a product proves to be defective in material or workmanship during the warranty period, we will at its sole option repair or replace the product with a like product with a like product. Replacement product or parts may include remanufactured or refurbished parts or components.

### **How long the warranty is effective:**

The Easy Hotspot Kit is warranted for one year for all parts and one year for all labor from the date of the first consumer purchase.

### **Who the warranty protects:**

This warranty is valid only for the first consumer purchaser.

### **What the warranty does not cover:**

1. Any product, on which the serial number has been defaced, modified or removed.
2. Damage, deterioration or malfunction resulting from:
  - a. Accident, misuse, neglect, fire, water, lightning, or other acts of nature, unauthorized product modification, or failure to follow instructions supplied with the product.
  - b. Repair or attempted repair by anyone not authorized by us.
  - c. Any damage of the product due to shipment.
  - d. Removal or installation of the product.
  - e. Causes external to the product, such as electric power fluctuations or failure.
  - f. Use of supplies or parts not meeting our specifications.
  - g. Normal wears and tear.
  - h. Any other cause that does not relate to a product defect.
3. Removal, installation, and set-up service charges.

### **How to get service:**

1. For information about receiving service under warranty, contact our **Customer Support**.
2. To obtain warranted service, you will be required to provide (a) the original dated sales slip, (b) your name, (c) your address (d) a description of the problem and (e) the serial number of the product.
3. Take or ship the product prepaid in the original container to your dealer, and our service center.
4. For additional information, contact your dealer or our **Customer Service Center**.

### **Limitation of implied warranties:**

THERE ARE NOWARRANTIED, EXPRESSED OR IMPLIED, WHICH EXTEND BEYOND THE DESCRIPTION CONTAINED HEREIN INCLUDING THE IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

### **Exclusion of damages:**

Our LIABILITY IS LIMITED TO THE COST OF REPAIR OR REPLACEMENT OF THE PRODUCT. We SHALL NOT BE LIABLE FOR:

1. DAMAGE TO OTHER PROPERTY CAUSED BY ANY DEFECTS IN THE PRODUCT, DAMAGES BASED UPON INCONVENIENCE, LOSS OF USE OF THE PRODUCT, LOSS OF TIME, LOSS OF PROFITS, LOSS OF BUSINESS OPPORTUNITY, LOSS OF GOODWILL, INTERFERENCE WITH BUSINESS RELATIONSHIPS, OR OTHER COMMERCIAL LOSS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
2. ANY OTHER DAMAGES, WHETHER INCIDENTAL, CONSEQUENTIAL OR OTHERWISE.
3. ANY CLAIM AGAINST THE CUSTOMER BY ANY OTHER PARTY.