NetComm®
www.netcomm.com.au

Wireless Hotspot

(AG400-Optional extra)

# User Guide

# Table of Contents

# 1. Before You Start

## Preface

This manual is for Hotspot owners or network administrators to set up a network environment using the HS1100 system. It contains step-by-step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation. It also contains a Quick Start Guide for the NetComm AG400 Thermal Ticket Printer.

## Document Conventions

| | |
|---|---|
| ⚠ | Represents essential steps, actions, or messages that should not be ignored. |
| ⏩ **Note:** | Contains related information that corresponds to a topic. |
| 🏠 | Indicates that clicking this button will return to the homepage of this section. |
| ⬆ | Indicates that clicking this button will return to the previous page. |
| ✓ Apply | Indicates that clicking this button will apply all of your settings. |
| ✕ Clear | Indicates that clicking this button will clear what you have set before these settings are applied. |

# 2. System Overview

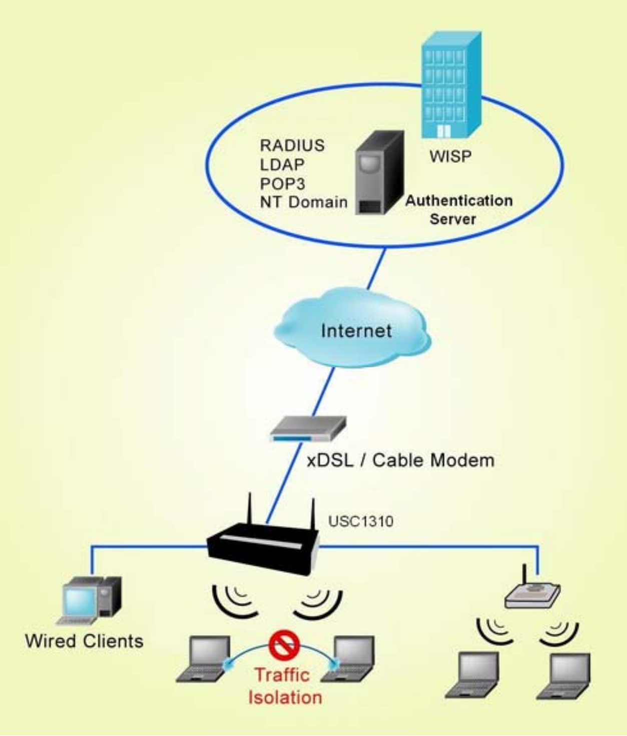
## Introduction of HS1100

HS1100 is an all-in-one product specially designed for small wireless/wired network environments. It integrates **"secure access control", "visitor account provisioning",** and **"high-speed secure wireless connection"** into one system to fulfill the needs in Hotspot locations. HS1100 supports 802.11b and 802.11g dual wireless transmission modes, and at the same time, incorporates **convenience, efficiency,** and **friendliness** for network services.

## System Concept

HS1100 is specially designed for user authentication, authorization and accounting management. The user account information is stored in the local database or a specified external databases server. The user authentication is processed via the SSL encrypted web interface. This interface is compatible to most desktop devices and palm computers. HS1100 manages network services for both wired and wireless network users.

The users located at the managed network will be unable to access network resources without permission. When a user attempts to connect to the Internet by opening a web browser on his computer, HS1100 will redirect the browser to the user login webpage of HS1100. The user must enter a username and password for authentication. After the identity is authenticated successfully, the user will gain proper access right defined on HS1100.



# *3. Installation*

## Hardware Installation

### System Requirements

- Standard 10/100BaseT including five network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

### Package Contents

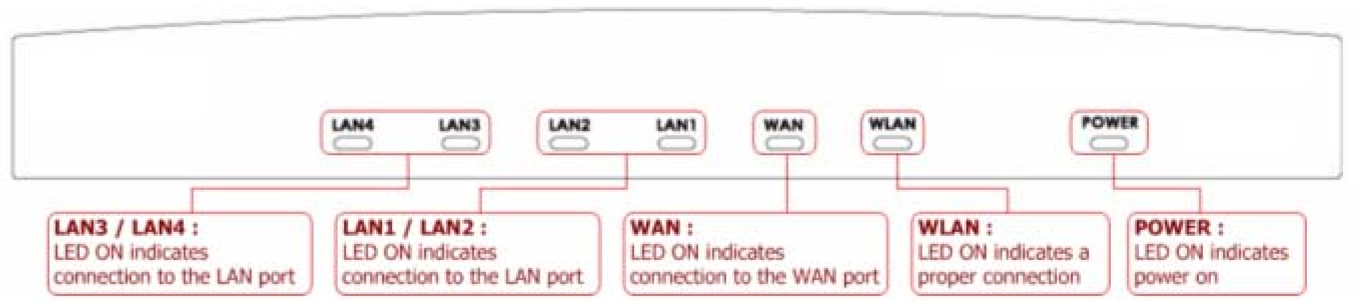
The standard package of HS1100 includes:

- HS1100 x 1
- CD-ROM x 1
- Power Adaptor (DC 12V) x 1
- Ethernet Cable x 1
- Console Cable x 1
- 2dbi Omni-antenna x 2

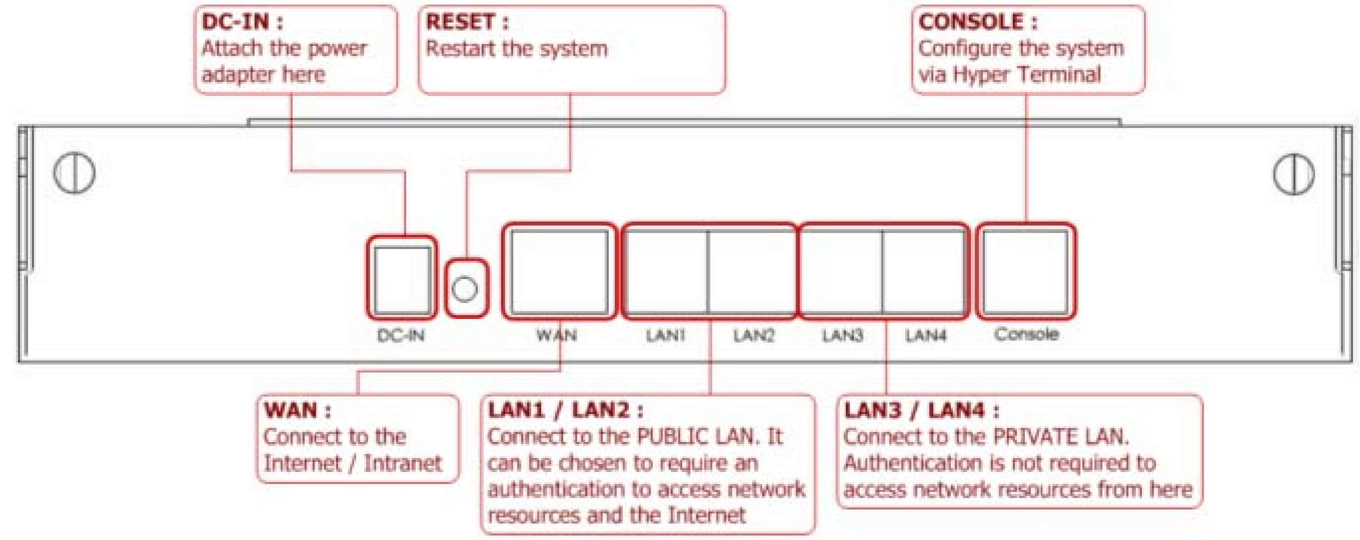
⚠ *It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.*

## Panel Function Descriptions

### Front Panel


LAN4
LAN3
LAN2
LAN1
WAN
WLAN
POWER
LAN3 / LAN4 : LED ON indicates connection to the LAN port
LAN1 / LAN2 : LED ON indicates connection to the LAN port
WAN : LED ON indicates connection to the WAN port
WLAN : LED ON indicates a proper connection
POWER : LED ON indicates power on

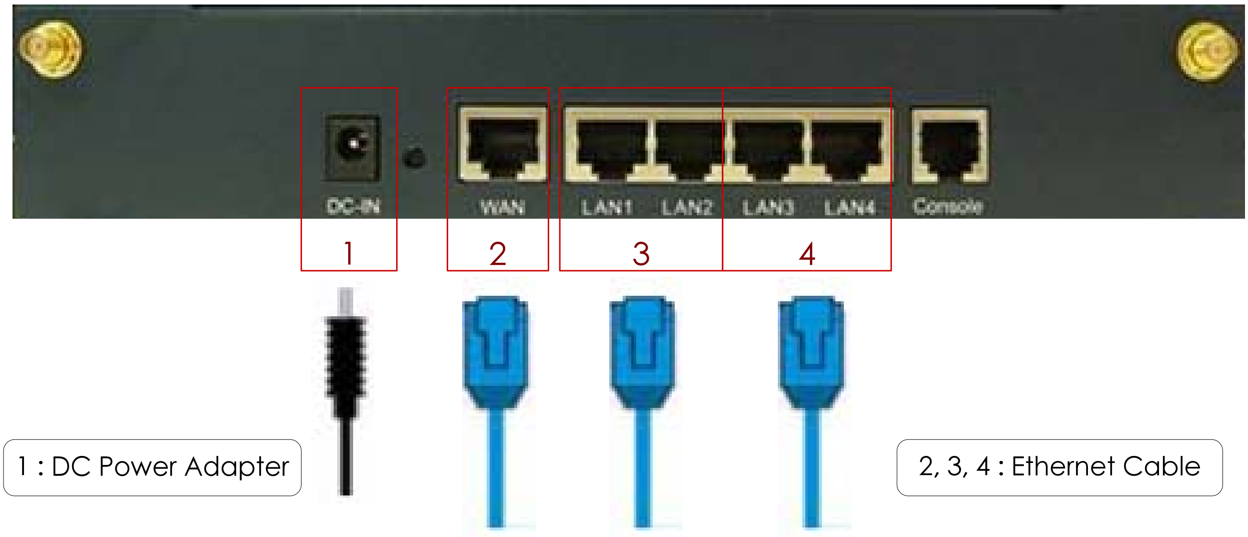
### Rear Panel


DC-IN : Attach the power adapter here
RESET : Restart the system
CONSOLE : Configure the system via Hyper Terminal
DC-IN
WAN
LAN1
LAN2
LAN3
LAN4
Console
WAN : Connect to the Internet / Intranet
LAN1 / LAN2 : Connect to the PUBLIC LAN. It can be chosen to require an authentication to access network resources and the Internet
LAN3 / LAN4 : Connect to the PRIVATE LAN. Authentication is not required to access network resources from here

- **DC IN:** The power adaptor plugs here.
- **RESET:** Press this button to restart/reboot the system (NOT reset back to factory default).
- **WAN:** The WAN port is used to connect to a network which is not managed by HS1100, and this port can be used to connect an xDSL/cable modem, or a switch/hub on a LAN of a company/organization.
- **LAN1/LAN2:** These two default authentication-demanding Public LAN ports are connected to the managed network or WLAN. They may be configured as authentication-demanding Public LAN or authentication-free Private LAN ports.
- **LAN3/LAN4:** These two default authentication-free Private LAN ports are connected to a trustful network, where the users can always access network resources without authentication. These ports may be connected to an external server such as a File Server or Database Server.
- **Console:** The system can be configured via HyperTerminal. For example, if you need to set the Administrator’s Password, you can connect a PC to this port as a Console Serial Port via a terminal connection program (such as the super terminal with the parameters of 9600, 8, N, 1, None flow control) to change the Administrator’s Password.

## Installation Steps

Please follow the steps below to install HS1100:



1. Connect the **power adapter** to the power socket on the rear panel. If the power supply and connection are normal, the Power LED will light up.

2. Connect an **Ethernet cable** to the WAN Port on the rear panel. Connect the other end of the Ethernet cable to an xDSL/cable modem, or a switch/hub on the LAN of a company/organization. The LED of this port should be on to indicate a proper connection.

3. Connect an **Ethernet cable** to the LAN1/LAN2 Port on the rear panel. Per your needs, connect the other end of the Ethernet cable to an AP for extending wireless coverage, a switch for connecting more wired clients, or a PC. The LED of LAN1/LAN2 should be on to indicate a proper connection.

⚠ *Authentication is required for the clients to access the network via LAN1/LAN2 Port. The LAN port with authentication function is referred to as **Public LAN**.*

4. Connect an **Ethernet cable** to the LAN3/LAN4 Port on the rear panel. Connect the other end of the Ethernet cable to a PC for configuring the HS1100 system. The LED of LAN3/LAN4 should be on to indicate a proper connection.

⚠ *Authentication is NOT required for the clients to access the network via the LAN3/LAN4 Port. The LAN port WITHOUT authentication function is referred to as **Private LAN**.*

**Note:** HS1100 supports Auto Sensing MDI/MDIX. You may use either a straight-through or a cross-over Ethernet cable to connect the Ethernet port.

After the hardware of HS1100 properly installed, follow the steps below to set up the HS1100 system.

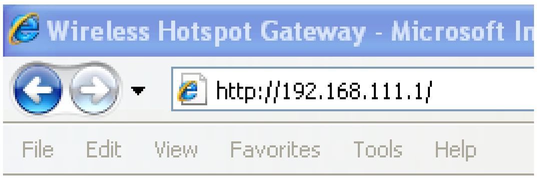
# Quick Software Configuration

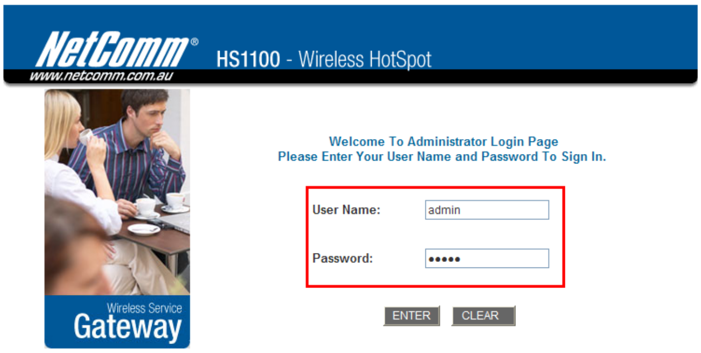
There are two ways to configure the HS1100 system: using the online **Configuration Wizard** or changing the settings by commands manually. The **Configuration Wizard** comprises of seven basic steps as follows. Follow the instructions of Configuration Wizard to enter the required information step by step, save your settings, and restart HS1100. The seven steps of Configuration Wizard are listed below:

**Step 1. Change Admin's Password**
**Step 2. Choose System's Time Zone**
**Step 3. Set System Information**
**Step 4. Select the Connection Type for WAN Port**
**Step 5. Set Authentication Methods**
**Step 6. Set Wireless – Access Point Connection**
**Step 7. Save and Restart HS1100**

Please follow the following steps to complete the quick configuration:

1. Use the network cable of the 10/100BaseT to connect a PC to the LAN3/LAN4 port, and then start a browser (such as Microsoft IE). Next, enter the gateway address for that port, the default is http://192.168.111.1. In the opened webpage, a login screen will appear. Enter ***"admin"***, the default username, and ***"admin"***, the default password, in the User Name and Password fields. Click ***Enter*** to log in.





Welcome To Administrator Login Page
Please Enter Your User Name and Password To Sign In.

User Name: admin
Password: •••••

> ⚠ *If you cannot get the login screen, your PC may have been set in DHCP to obtain an IP address automatically from another existing authentication LAN port, or the IP address used does not have the same subnet as the default URL of HS1100. Please use default IP address such as 192.168.111.xxx (xxx: 2~254) in your network and then try it again.*

You can log in as **admin**, **manager** or **operator**. The default usernames and passwords show as follows:

**Admin:** The administrator can access all configuration pages of HS1100.

User Name: **admin**

Password: **admin**

**Manager:** The manager can only access the configuration pages under ***User Authentication*** to manage the user accounts, but without the permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

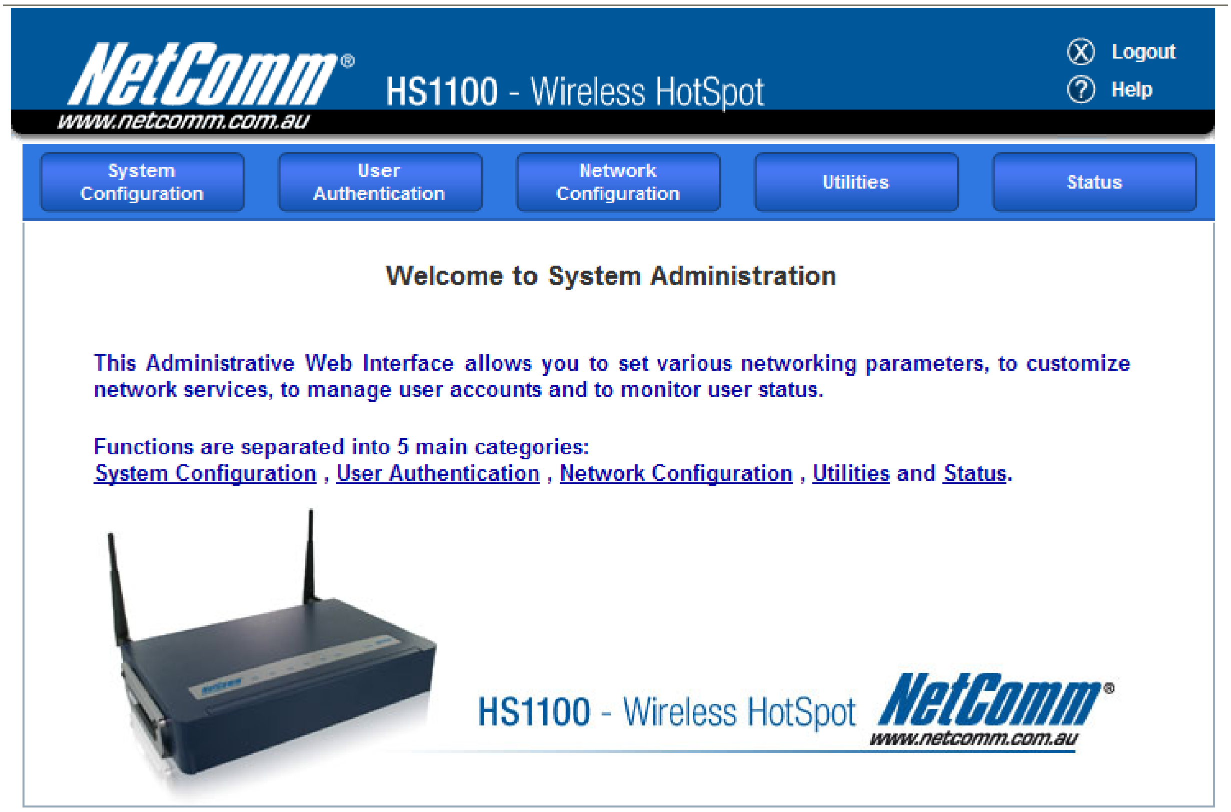
Password: **manager**

**Operator:** The operator can only access the configuration page of ***Create On-demand User*** to create new on-demand user accounts and print out the on-demand user account receipts.

User Name: **operator**

Password: **operator**

2. After successfully logging into HS1100, a web management interface with a welcome message will appear. There is a ***Logout*** button on the upper right corner to log out the system when finished.

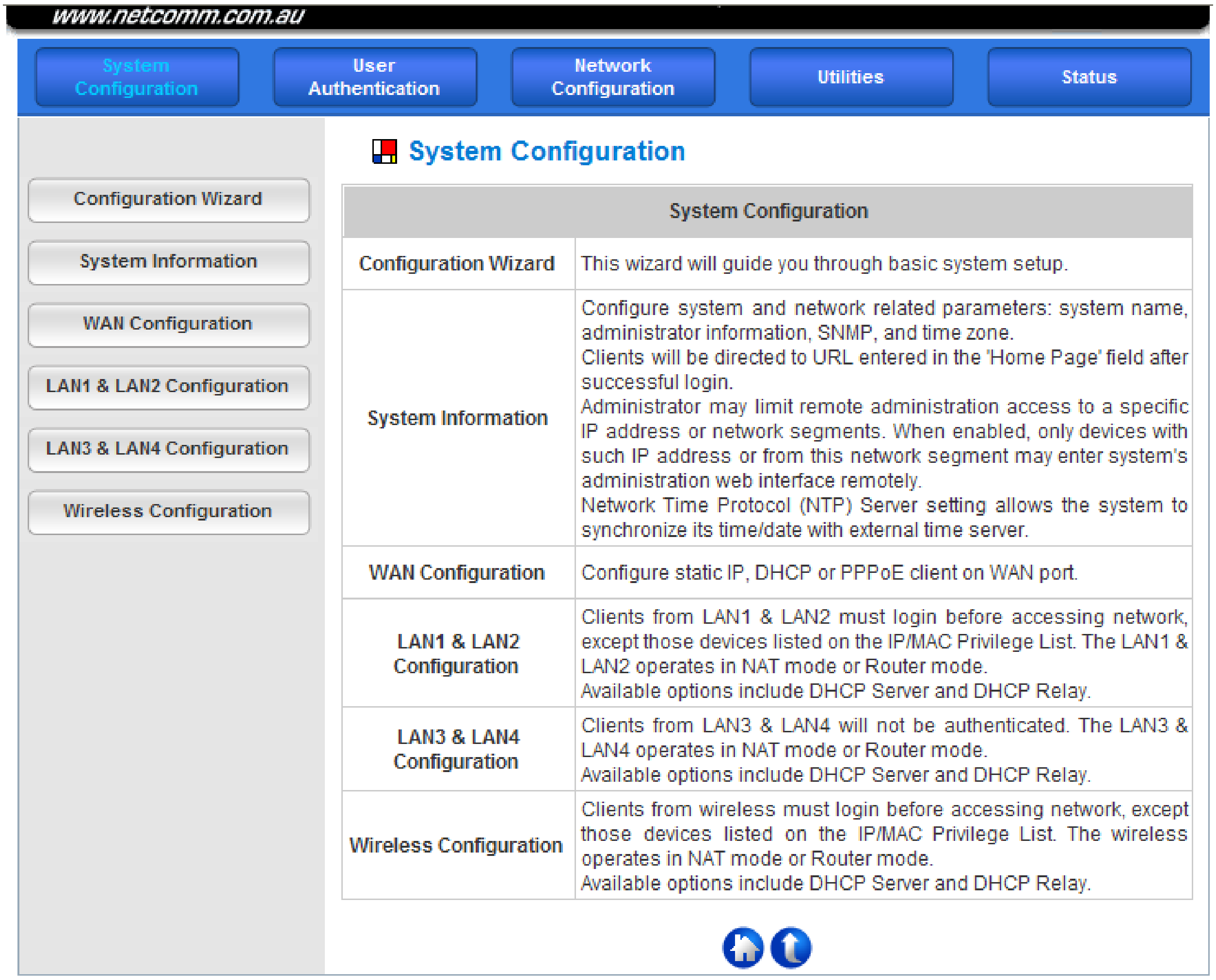


Welcome to System Administration

This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.

Functions are separated into 5 main categories:
System Configuration , User Authentication , Network Configuration , Utilities and Status.

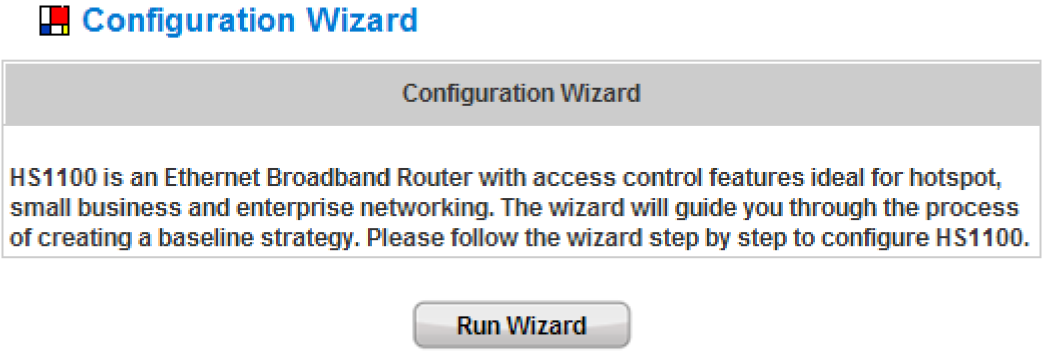
3. To quickly configure HS1100 by using the **Configuration Wizard**, click ***System Configuration*** to go to the **System Configuration** homepage.



System Configuration

| System Configuration | |
|---|---|
| Configuration Wizard | This wizard will guide you through basic system setup. |
| System Information | Configure system and network related parameters: system name, administrator information, SNMP, and time zone.<br>Clients will be directed to URL entered in the 'Home Page' field after successful login.<br>Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely.<br>Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server. |
| WAN Configuration | Configure static IP, DHCP or PPPoE client on WAN port. |
| LAN1 & LAN2 Configuration | Clients from LAN1 & LAN2 must login before accessing network, except those devices listed on the IP/MAC Privilege List. The LAN1 & LAN2 operates in NAT mode or Router mode.<br>Available options include DHCP Server and DHCP Relay. |
| LAN3 & LAN4 Configuration | Clients from LAN3 & LAN4 will not be authenticated. The LAN3 & LAN4 operates in NAT mode or Router mode.<br>Available options include DHCP Server and DHCP Relay. |
| Wireless Configuration | Clients from wireless must login before accessing network, except those devices listed on the IP/MAC Privilege List. The wireless operates in NAT mode or Router mode.<br>Available options include DHCP Server and DHCP Relay. |

4. Then, select ***Configuration Wizard*** and click the ***Run Wizard*** button to start the wizard.

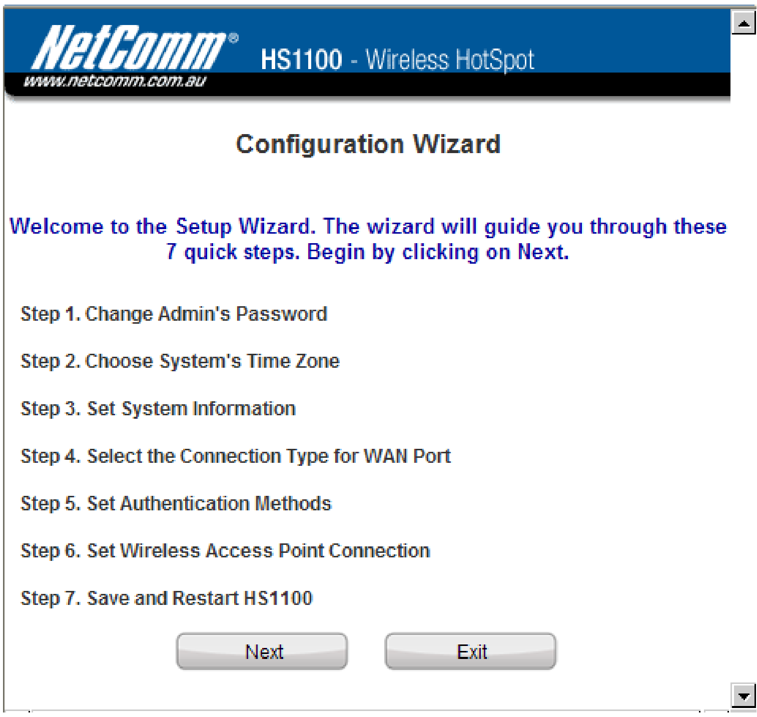


Configuration Wizard

| Configuration Wizard |
|---|
| HS1100 is an Ethernet Broadband Router with access control features ideal for hotspot, small business and enterprise networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure HS1100. |

5. **Configuration Wizard**

A welcome screen that briefly introduces the 7 steps will appear. Click ***Next*** to begin.



Configuration Wizard

Welcome to the Setup Wizard. The wizard will guide you through these 7 quick steps. Begin by clicking on Next.

Step 1. Change Admin's Password

Step 2. Choose System's Time Zone

Step 3. Set System Information

Step 4. Select the Connection Type for WAN Port

Step 5. Set Authentication Methods

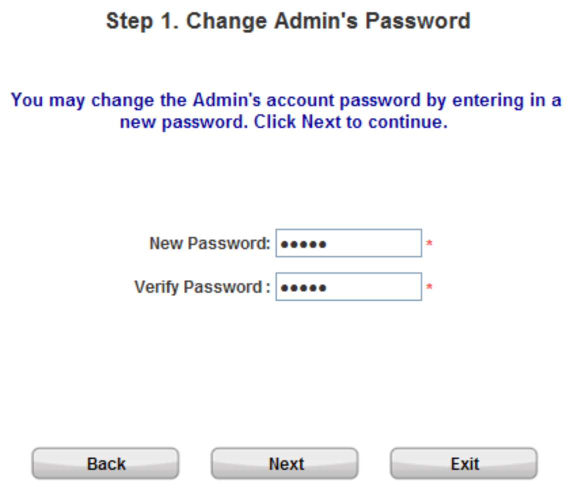
Step 6. Set Wireless Access Point Connection

Step 7. Save and Restart HS1100

- **Step 1. Change Admin's Password**

  Enter a new password for the admin account and retype it in the verify password field (maximum number of characters up to 20 and no spaces allowed).

  Click ***Next*** to continue.



Step 1. Change Admin's Password

You may change the Admin's account password by entering in a new password. Click Next to continue.

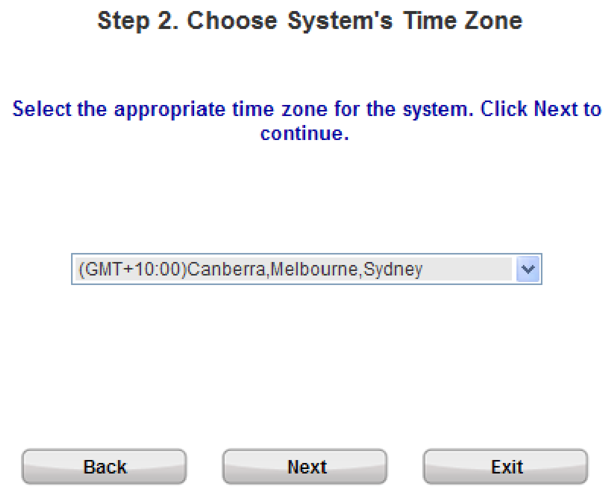
New Password: ●●●●● *

Verify Password : ●●●●● *

- **Step 2. Choose System's Time Zone**

  Select a proper time zone from the drop-down list box.

  Click ***Next*** to continue.



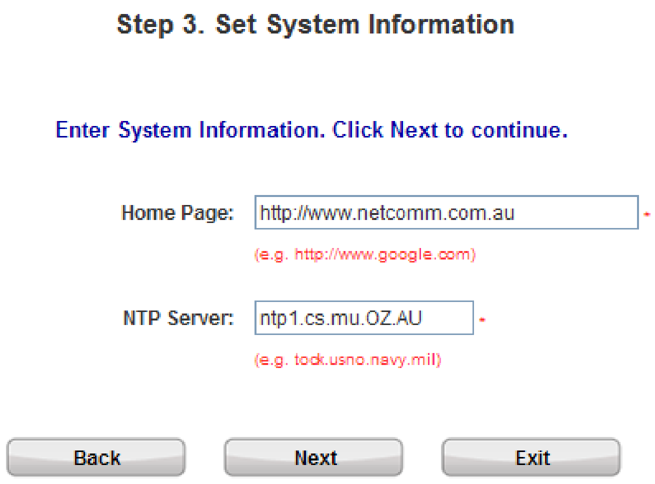
Step 2. Choose System's Time Zone

Select the appropriate time zone for the system. Click Next to continue.

(GMT+10:00)Canberra,Melbourne,Sydney

- **Step 3. Set System Information**
  - **Home Page:** Enter the URL to where the users should be directed when they are successfully authenticated.
  - **NTP Server:** Enter the URL of the external time server for HS1100 time synchronization or use the default setting.

  Click ***Next*** to continue.



Step 3. Set System Information

Enter System Information. Click Next to continue.

Home Page: http://www.netcomm.com.au *

(e.g. http://www.google.com)

NTP Server: ntp1.cs.mu.OZ.AU *

(e.g. tock.usno.navy.mil)

- **Step 4. Select the Connection Type for WAN Port**

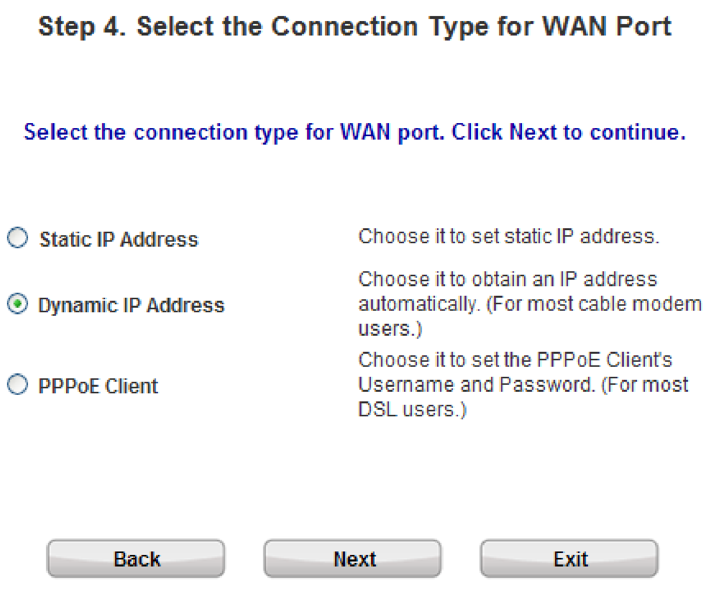
  Three are three types of WAN port to select from: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**.

  Select a proper Internet connection type and click ***Next*** to continue.

  ➢ **Dynamic IP Address**

  If this option is selected, an appropriate IP address and related information will automatically be assigned.

  Click ***Next*** to continue.



Step 4. Select the Connection Type for WAN Port

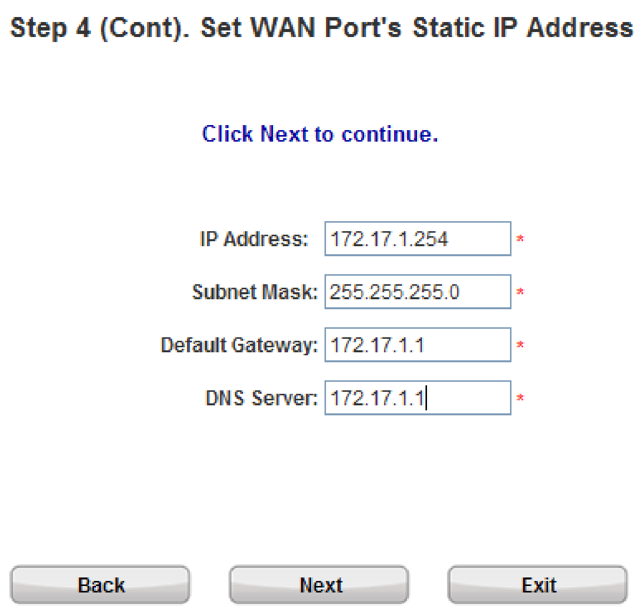
Select the connection type for WAN port. Click Next to continue.

| | |
|---|---|
| ○ Static IP Address | Choose it to set static IP address. |
| ● Dynamic IP Address | Choose it to obtain an IP address automatically. (For most cable modem users.) |
| ○ PPPoE Client | Choose it to set the PPPoE Client's Username and Password. (For most DSL users.) |

➢ **Static IP Address: Set WAN Port's Static IP Address**

Enter the **"IP Address"**, **"Subnet Mask"**, **"Default Gateway"** and **"DNS Server"** provided by your Internet Service Provider.

Click ***Next*** to continue.



Step 4 (Cont). Set WAN Port's Static IP Address

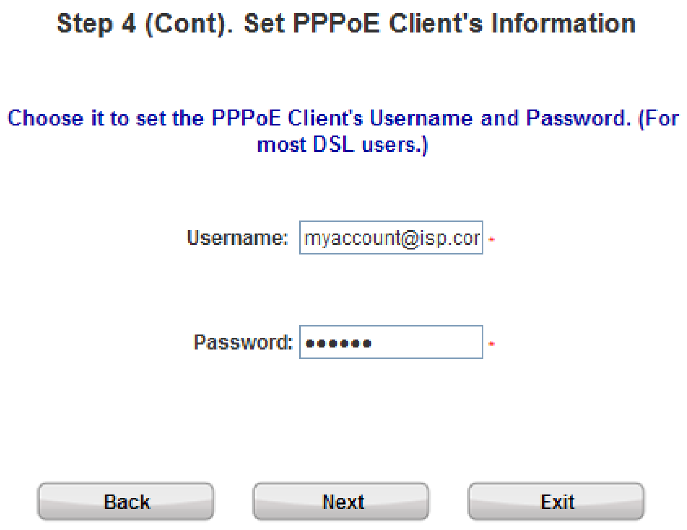
Click Next to continue.

| | |
|---|---|
| IP Address: | 172.17.1.254 * |
| Subnet Mask: | 255.255.255.0 * |
| Default Gateway: | 172.17.1.1 * |
| DNS Server: | 172.17.1.1 * |

➢ **PPPoE Client: Set PPPoE Client's Information**

Enter the **"Username"** and **"Password"** provided by your ISP.

Click ***Next*** to continue.



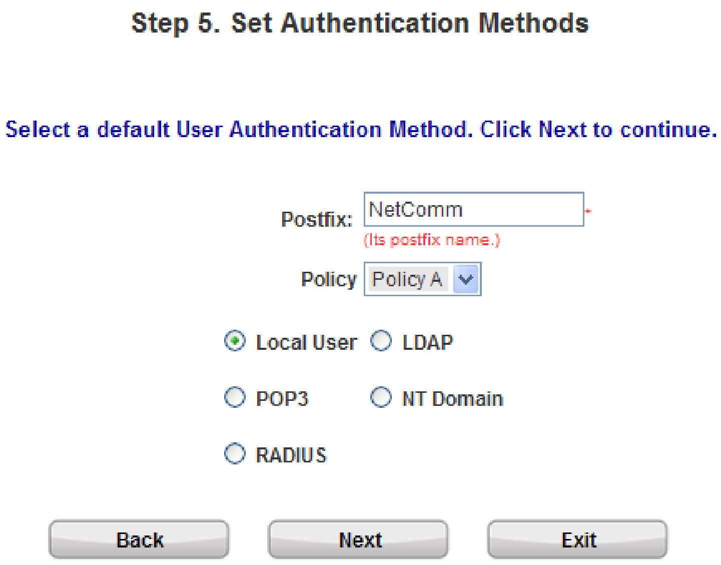
Step 4 (Cont). Set PPPoE Client's Information

Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

| | |
|---|---|
| Username: | myaccount@isp.cor * |
| Password: | •••••• * |

- **Step 5. Set Authentication Methods**
  - Set the user's information in advance. Enter an easily identified name as the postfix name in the **"Postfix"** field (e.g. test@Postfix1), select a **"Policy"** (or use the default value), and choose one authentication method from the 5 options appearing in this window.

    Click ***Next*** to continue.



Step 5. Set Authentication Methods

Select a default User Authentication Method. Click Next to continue.

Postfix: NetComm *
(Its postfix name.)

Policy: Policy A

● Local User ○ LDAP

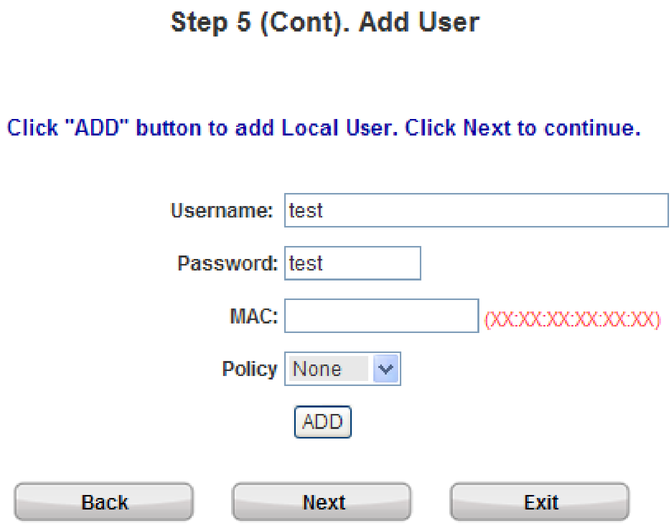
○ POP3 ○ NT Domain

○ RADIUS

  - **Local User: Add User**

    A new user can be added to the local user data base. To add a user here, enter the **"Username"** (e.g. test), **"Password"** (e.g. test), **"MAC"** (optional) and assign it a policy (or use the default). Upon completing adding a user, more users can be added to this authentication method by clicking the ***ADD*** button.

    Click ***Next*** to continue.



Step 5 (Cont). Add User

Click "ADD" button to add Local User. Click Next to continue.

Username: test

Password: test

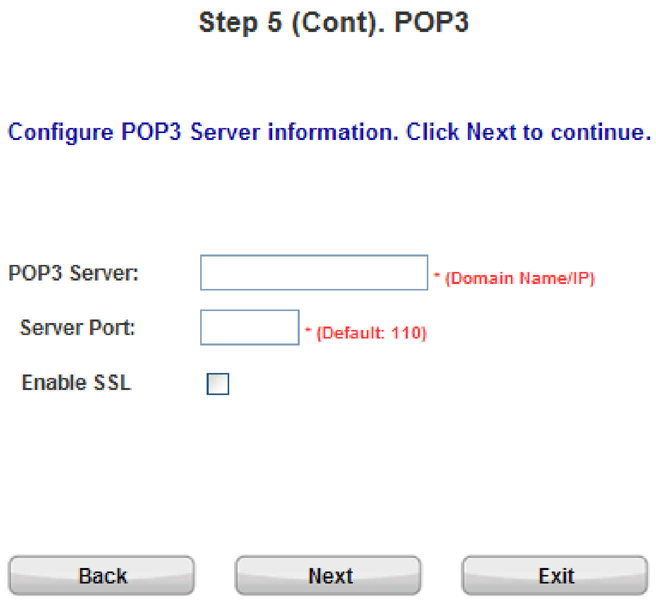
MAC: (XX:XX:XX:XX:XX:XX)

Policy: None

  - **POP3 User: POP3**

    Enter POP3 Server's **"Domain Name/IP"** and **"Server Port"**, and then choose **"Enable SSL"** or not.

    Click ***Next*** to continue.



Step 5 (Cont). POP3

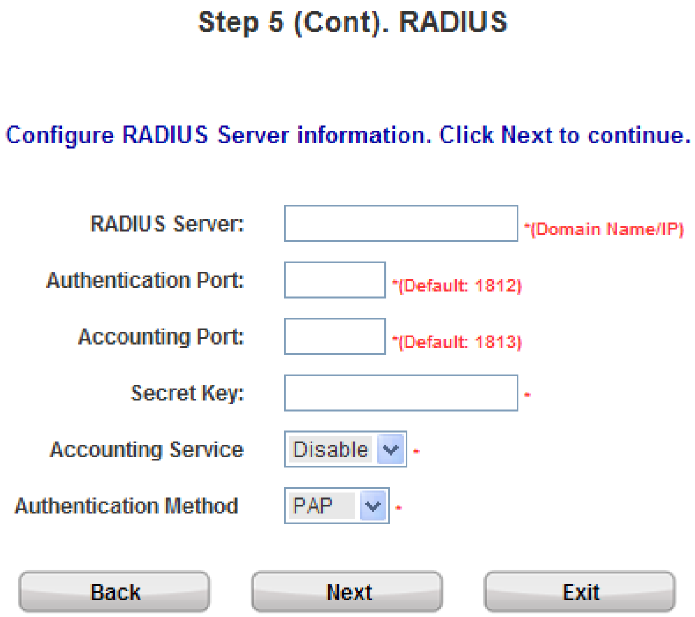
Configure POP3 Server information. Click Next to continue.

POP3 Server: * (Domain Name/IP)

Server Port: * (Default: 110)

Enable SSL □

- **RADIUS User: RADIUS**
  Enter RADIUS Server's **"Domain Name/IP"**, **"Accounting Port"** and **"Secret Key"**. Then choose to enable or disable **"Accounting Service"**, and select the desired **"Authentication Method"**.
  Click ***Next*** to continue.

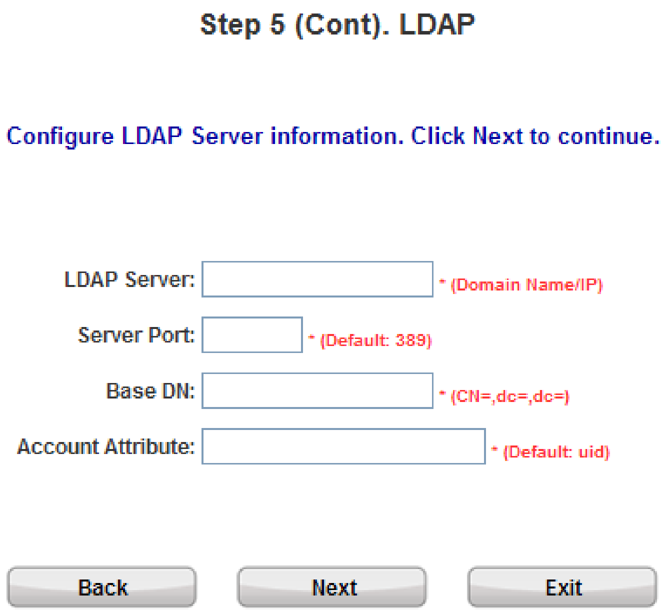


Step 5 (Cont). RADIUS

Configure RADIUS Server information. Click Next to continue.

| | | |
|---|---|---|
| RADIUS Server: | | *(Domain Name/IP) |
| Authentication Port: | | *(Default: 1812) |
| Accounting Port: | | *(Default: 1813) |
| Secret Key: | | * |
| Accounting Service | Disable | * |
| Authentication Method | PAP | * |

- **LDAP User: LDAP**
  Add a new user to the LDAP user data base if desired. Enter the LDAP Server's **"Domain Name/IP"**, **"Server Port"**, and **"Base DN"**.
  Click **Next** to continue.

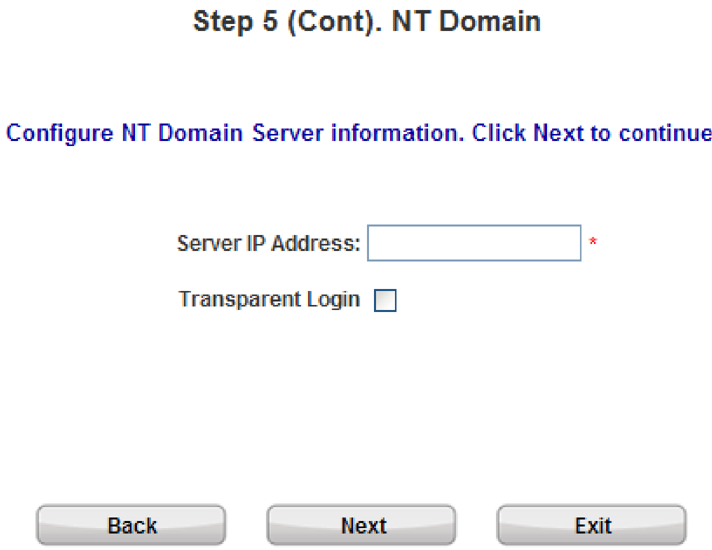


Step 5 (Cont). LDAP

Configure LDAP Server information. Click Next to continue.

| | | |
|---|---|---|
| LDAP Server: | | * (Domain Name/IP) |
| Server Port: | | * (Default: 389) |
| Base DN: | | * (CN=,dc=,dc=) |
| Account Attribute: | | * (Default: uid) |

- **NT Domain User: NT Domain**
  When NT Domain User is selected, enter the information for **"Server IP Address"**, and choose to enable/disable **"Transparent Login"**. If "Transparent Login" is enabled, users are logged in HS1100's NT Domain active directory and authenticated automatically when they log into their Windows OS domain.
  Click ***Next*** to continue.



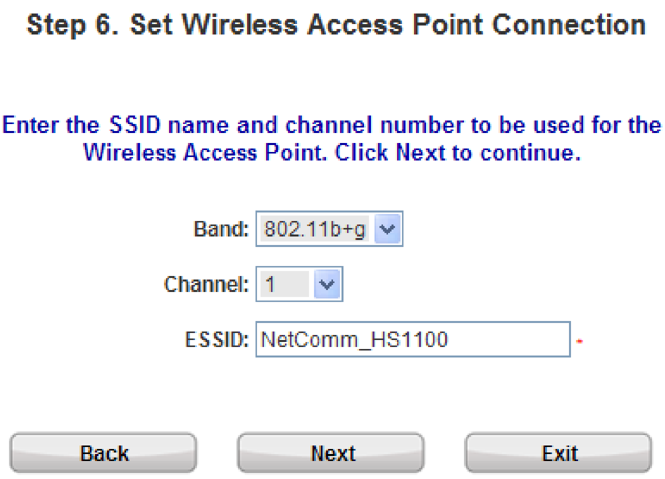
Step 5 (Cont). NT Domain

Configure NT Domain Server information. Click Next to continue

| | | |
|---|---|---|
| Server IP Address: | | * |
| Transparent Login | □ | |

- **Step 6. Set Wireless – Access Point Connection**
  - **Band:** HS1100 supports two transmission modes, **Disabled**, **802.11b**, **802.11g** and **802.11 (b+g)**. Select the appropriate transmission mode to work with the wireless clients in the network.
  - **Channel:** If the default channel has been used by many other access points, it is necessary to select another channel from the drop-down list box for a better performance.
  - **ESSID:** Enter a SSID (up to 32 characters) for the system. The default is ***HS1100***. **ESSID** is a unique identifier used for the wireless users' devices to associate with HS1100.

  Click ***Next*** to continue.



Step 6. Set Wireless Access Point Connection

Enter the SSID name and channel number to be used for the Wireless Access Point. Click Next to continue.

Band: 802.11b+g

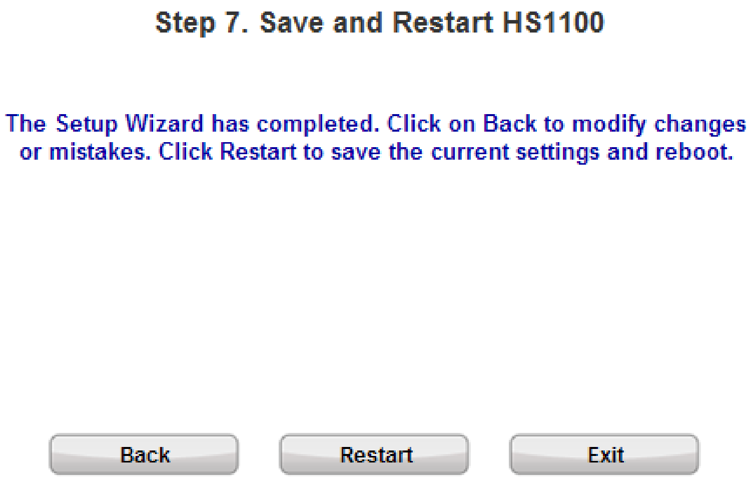
Channel: 1

ESSID: NetComm_HS1100

**Note:** *Available channels depend upon the region you are located. For instance, Channel 1~11 is available in North America, and Channel 1-13 in Europe*.

- **Step 7. Save and Restart HS1100**

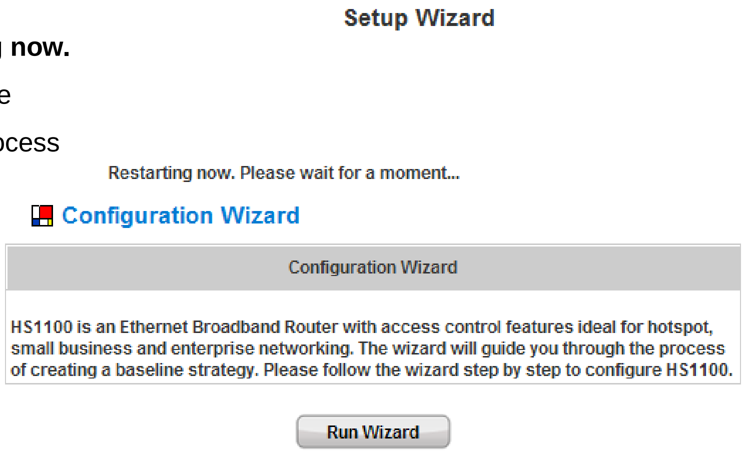
  Click ***Restart*** to save current settings and restart HS1100. The Setup Wizard is now completed.



Step 7. Save and Restart HS1100

The Setup Wizard has completed. Click on Back to modify changes or mistakes. Click Restart to save the current settings and reboot.

- **Setup Wizard.** During HS1100 restart, a **"Restarting now. Please wait for a while."** message will appear on the screen. Please do not interrupt HS1100 restarting process until the message has disappeared. This indicates that the entire restart process has been completed successfully.



Setup Wizard

Restarting now. Please wait for a moment...

Configuration Wizard

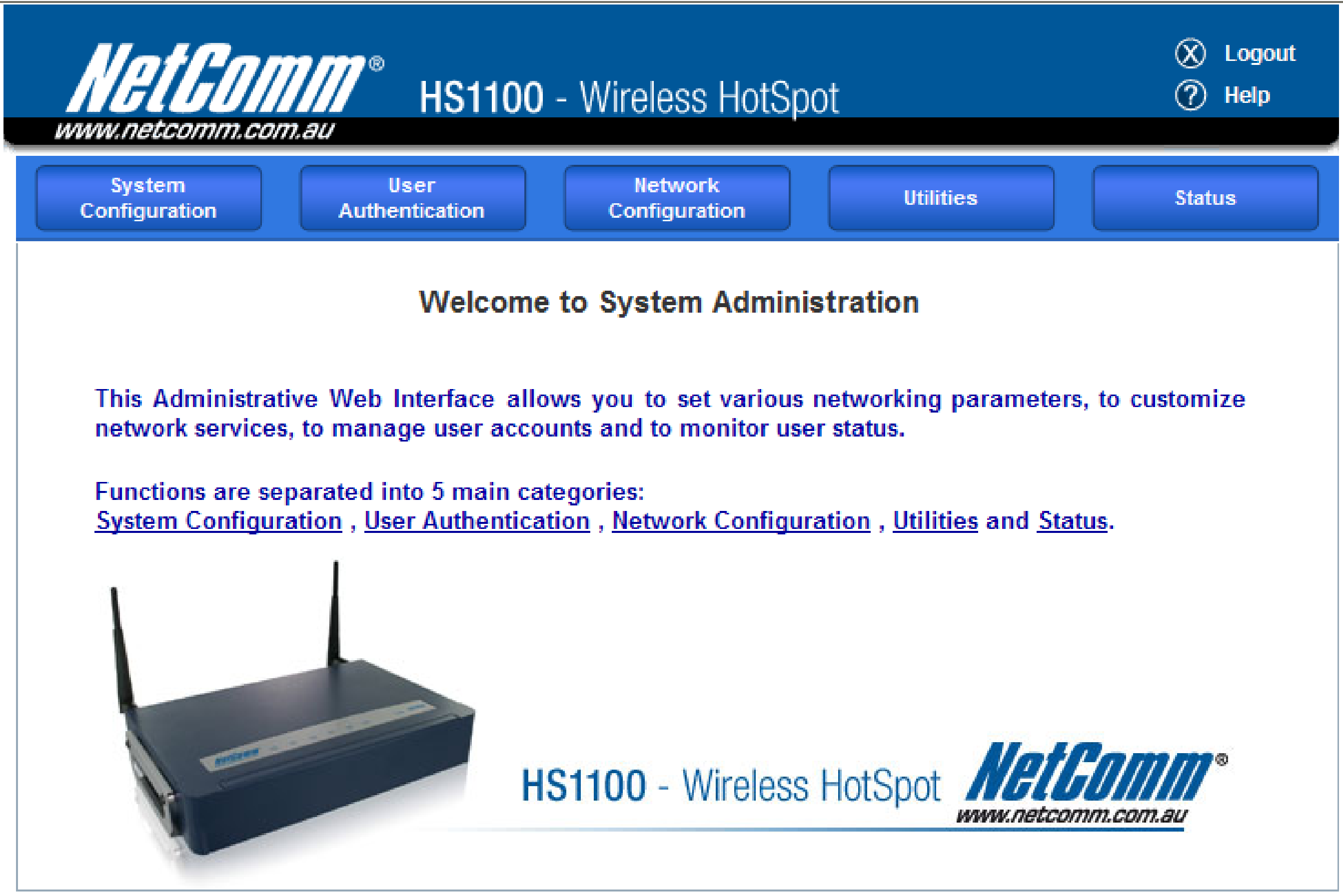
Configuration Wizard

HS1100 is an Ethernet Broadband Router with access control features ideal for hotspot, small business and enterprise networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure HS1100.

⚠ *During every step of the wizard, if you wish to go back to modify the settings, please click the **Back** button to go back to the previous step.*

# 4. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the functions of HS1100.



Welcome to System Administration

This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.

Functions are separated into 5 main categories:
System Configuration , User Authentication , Network Configuration , Utilities and Status.

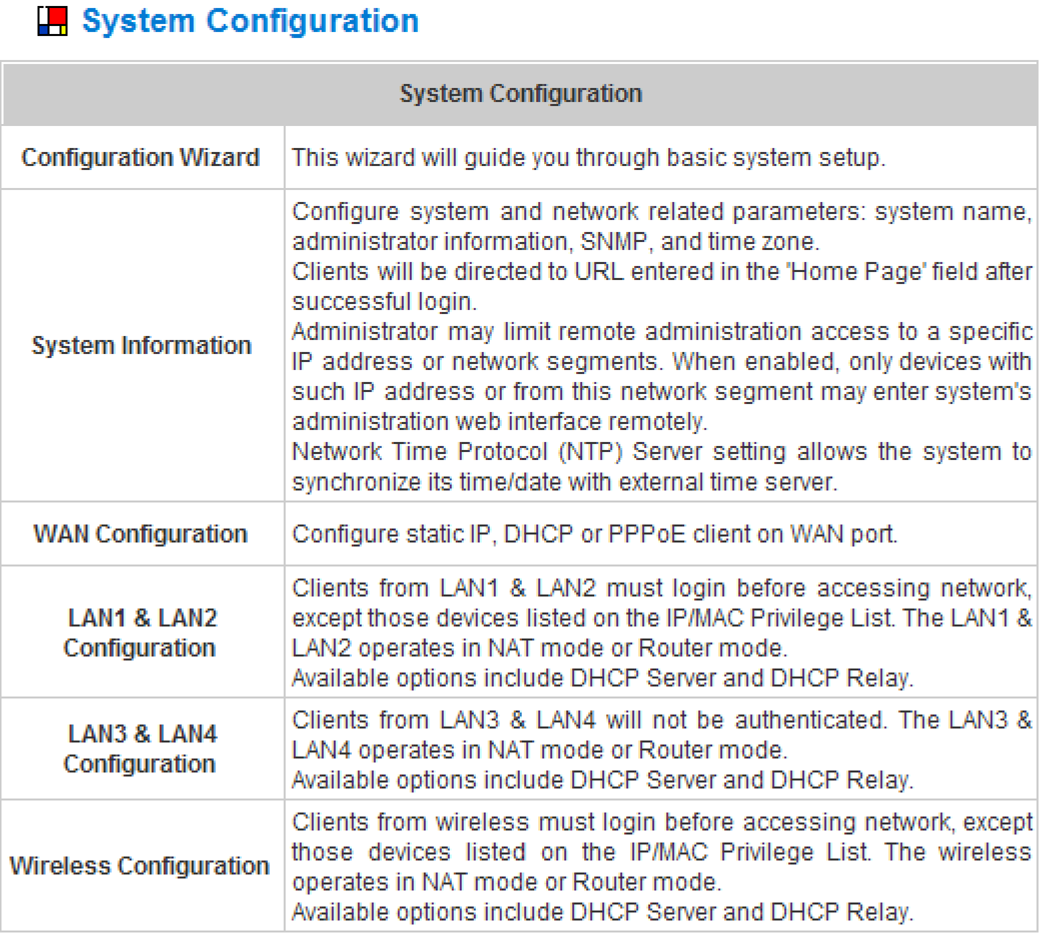
| OPTION | System Configuration | User Authentication | Network Configuration | Utilities | Status |
|---|---|---|---|---|---|
| FUNCTION | Configuration Wizard | Authentication Configuration | Network Address Translation | Network Utilities | System Status |
| | System Information | Black List Configuration | Privilege List | Change Password | Interface Status |
| | WAN Configuration | Policy Configuration | Monitor IP List | Backup/Restore Settings | Current Users |
| | LAN1 & LAN2 Configuration | Guest User Configuration | Walled Garden List | Firmware Upgrade | Traffic History |
| | LAN3 & LAN4 Configuration | Additional Configuration | Walled Garden AD List | Restart | Notify Configuration |

| | | | | | |
|---|---|---|---|---|---|
| | Wireless Configuration | | Proxy Server Properties | | |
| | | | Dynamic DNS | | |

⚠ *After finishing the configuration of the settings, please click **Apply** and pay attention to see if a RESTART message appears on the screen. If such message appears, the system must be restarted to allow the new settings to take effect. All on-line users will be disconnected during restart.*

# System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN Configuration**, **LAN1 & LAN2 Configuration**, **LAN3 & LAN4 Configuration** and **Wireless Configuration**.

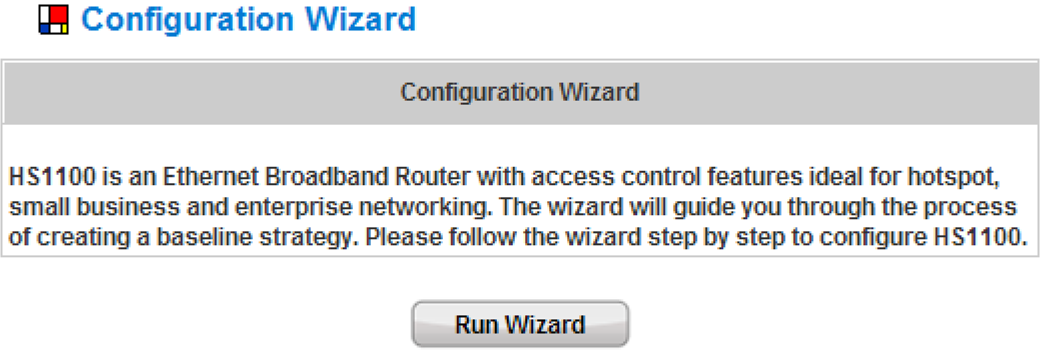


System Configuration

| System Configuration | |
|---|---|
| Configuration Wizard | This wizard will guide you through basic system setup. |
| System Information | Configure system and network related parameters: system name, administrator information, SNMP, and time zone.<br>Clients will be directed to URL entered in the 'Home Page' field after successful login.<br>Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely.<br>Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server. |
| WAN Configuration | Configure static IP, DHCP or PPPoE client on WAN port. |
| LAN1 & LAN2 Configuration | Clients from LAN1 & LAN2 must login before accessing network, except those devices listed on the IP/MAC Privilege List. The LAN1 & LAN2 operates in NAT mode or Router mode.<br>Available options include DHCP Server and DHCP Relay. |
| LAN3 & LAN4 Configuration | Clients from LAN3 & LAN4 will not be authenticated. The LAN3 & LAN4 operates in NAT mode or Router mode.<br>Available options include DHCP Server and DHCP Relay. |
| Wireless Configuration | Clients from wireless must login before accessing network, except those devices listed on the IP/MAC Privilege List. The wireless operates in NAT mode or Router mode.<br>Available options include DHCP Server and DHCP Relay. |

## Configuration Wizard

There are two ways to configure the HS1100 system: using the online **Configuration Wizard** or changing the settings by commands manually. The **Configuration Wizard** comprises of seven basic steps, providing a simple and easy way to go through the basic setups of HS1100 and is served as **Quick Configuration**.



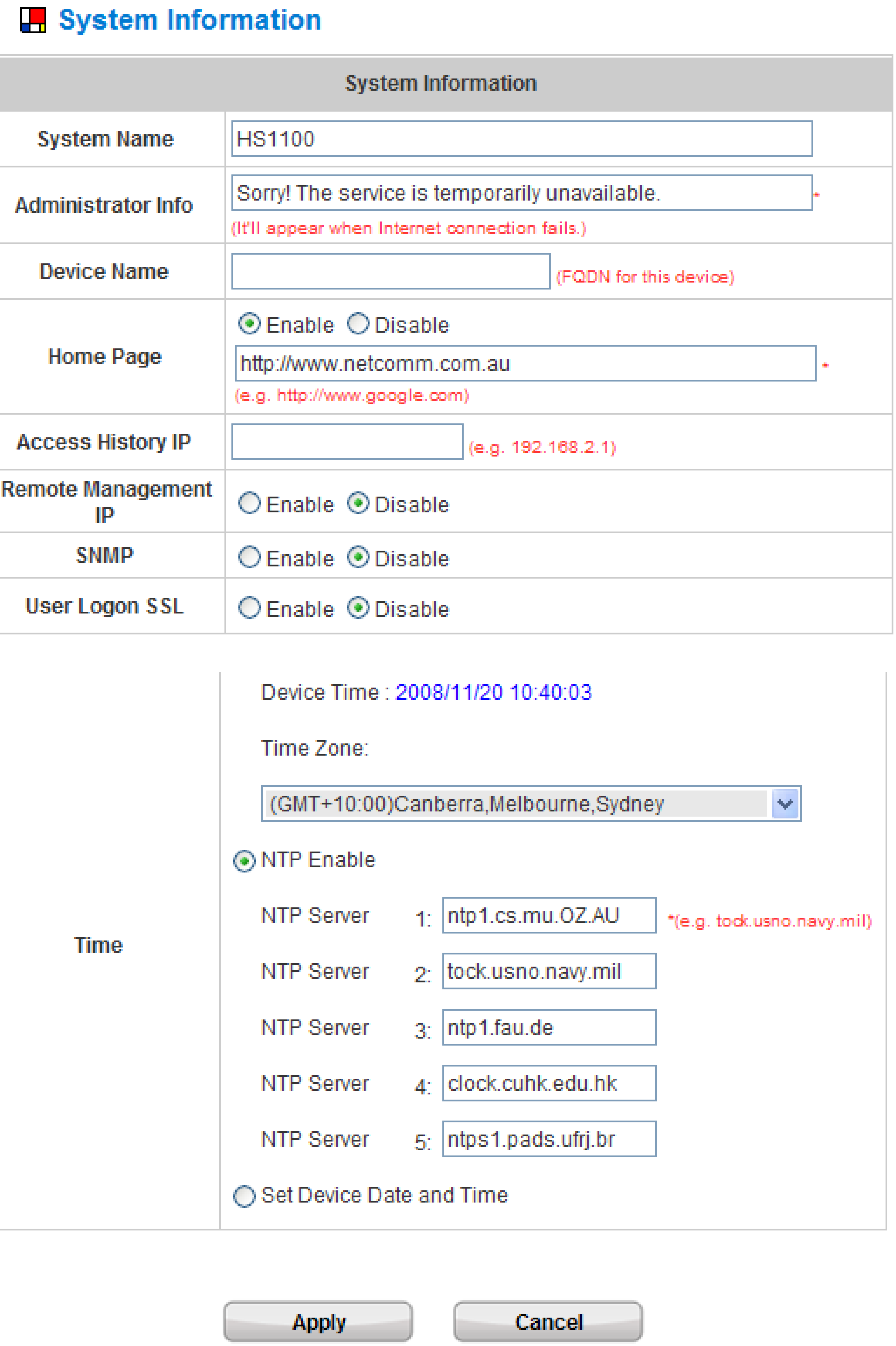
Configuration Wizard

Configuration Wizard

HS1100 is an Ethernet Broadband Router with access control features ideal for hotspot, small business and enterprise networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure HS1100.

## System Information

Main information about HS1100 is shown as follows:



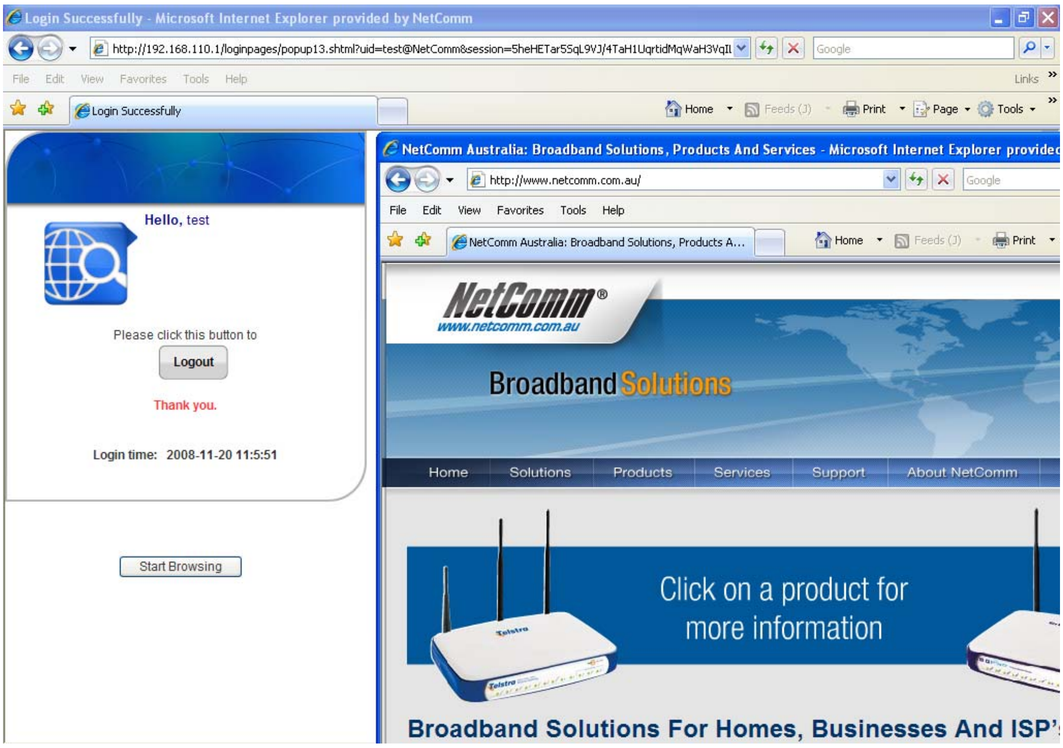
System Information

| System Information | |
|---|---|
| System Name | HS1100 |
| Administrator Info | Sorry! The service is temporarily unavailable. *<br>(It'll appear when Internet connection fails.) |
| Device Name | (FQDN for this device) |
| Home Page | ● Enable ○ Disable<br>http://www.netcomm.com.au *<br>(e.g. http://www.google.com) |
| Access History IP | (e.g. 192.168.2.1) |
| Remote Management IP | ○ Enable ● Disable |
| SNMP | ○ Enable ● Disable |
| User Logon SSL | ○ Enable ● Disable |
| Time | Device Time : 2008/11/20 10:40:03<br>Time Zone:<br>(GMT+10:00)Canberra,Melbourne,Sydney<br>● NTP Enable<br>NTP Server 1: ntp1.cs.mu.OZ.AU *(e.g. tock.usno.navy.mil)<br>NTP Server 2: tock.usno.navy.mil<br>NTP Server 3: ntp1.fau.de<br>NTP Server 4: clock.cuhk.edu.hk<br>NTP Server 5: ntps1.pads.ufrj.br<br>○ Set Device Date and Time |

- **System Name:** Set the system's name or use the default.
- **Administrator Info:** Enter the administrator's information here, such as the administrator's name, telephone

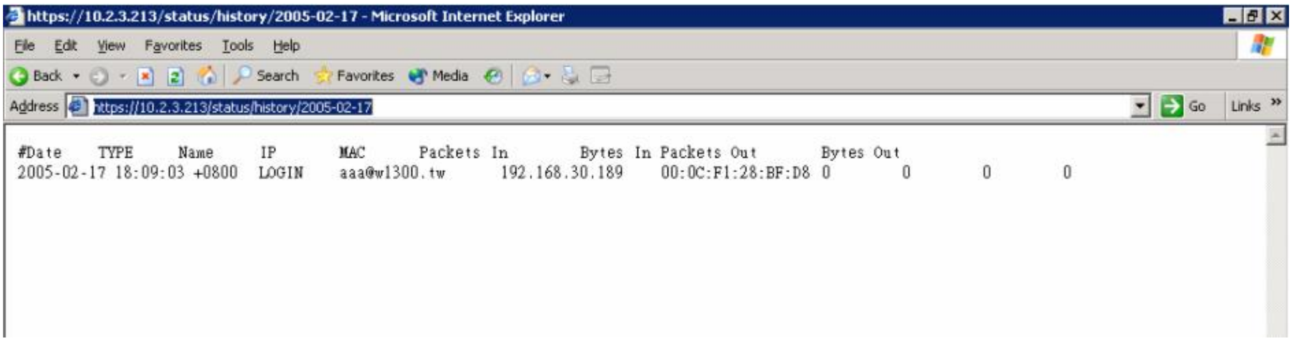
number, e-mail address, etc. If a user encounters problems while connecting to HS1100's WAN and can't get online, this information will appear on the user's login screen.

- **Home Page:** Enter the URL of a Web server as the homepage. Once logged in successfully, the users will be directed to this homepage, such as http://www.netcomm.com.au, regardless of the original homepage set in their computers.
  - ➢ **Homepage Redirect** is the system's special feature that would redirect client to your configured homepage right after the successful login. Your homepage appears after a successful login no matter what their browser's homepages are.


Login Successfully - Microsoft Internet Explorer provided by NetComm
http://192.168.110.1/loginpages/popup13.shtml?uid=test@NetComm&session=5heHETar5SqL9VJ/4TaH1UqrtidMqWaH3VqII
Login Successfully
Hello, test
Please click this button to
Logout
Thank you.
Login time: 2008-11-20 11:5:51
Start Browsing
NetComm Australia: Broadband Solutions, Products And Services - Microsoft Internet Explorer provided
http://www.netcomm.com.au/
NetComm
www.netcomm.com.au
Broadband Solutions
Home
Solutions
Products
Services
Support
About NetComm
Click on a product for more information
Broadband Solutions For Homes, Businesses And ISP'

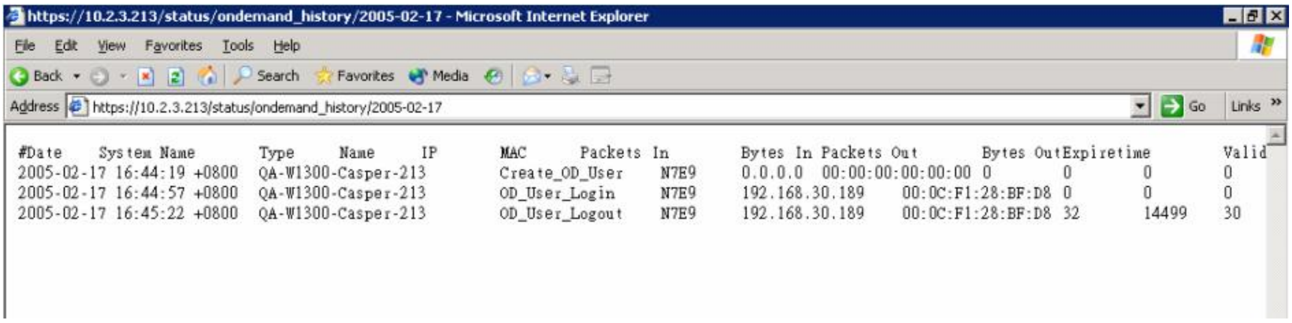
- **Access History IP:** Specify an IP address of the administrator's computer or a billing system to get billing history information of HS1100. An example is provided as follows ("10.2.3.213" is the WAN IP of HS1100).

Traffic History：https://10.2.3.213/status/history/2005-02-17


https://10.2.3.213/status/history/2005-02-17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.2.3.213/status/history/2005-02-17
Go Links

```
#Date      TYPE      Name       IP         MAC        Packets In          Bytes In Packets Out        Bytes Out
2005-02-17 18:09:03 +0800   LOGIN      aaa@w1300.tw       192.168.30.189     00:0C:F1:28:BF:D8 0          0          0          0
```

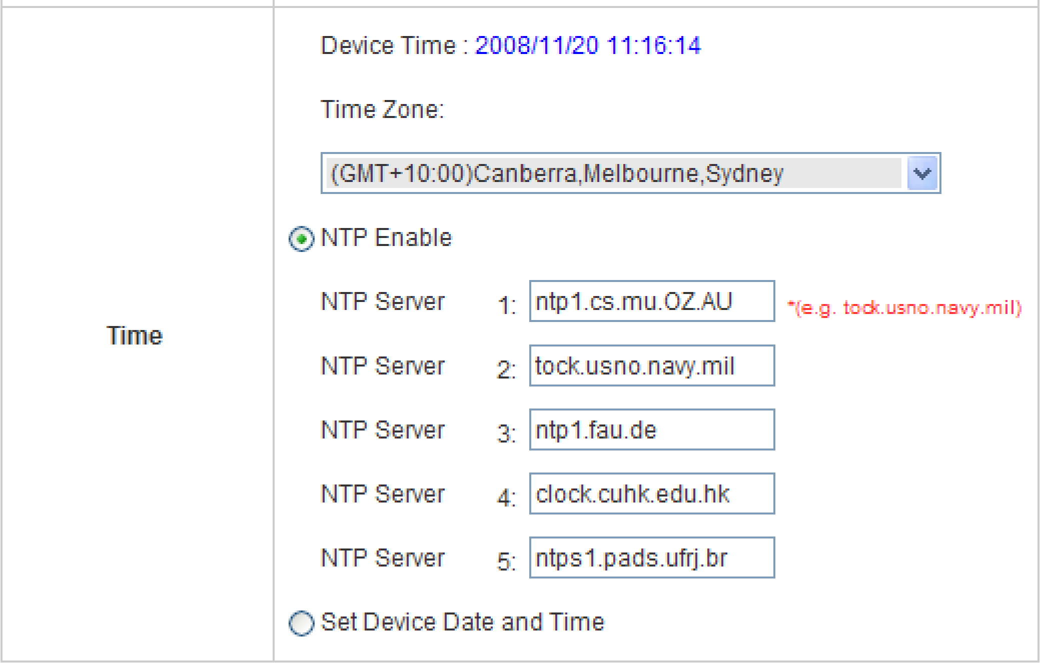
On-demand History：https://10.2.3.213/status/ondemand_history/2005-02-17



https://10.2.3.213/status/ondemand_history/2005-02-17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.2.3.213/status/ondemand_history/2005-02-17
Go
Links

```
#Date     System Name        Type      Name      IP        MAC       Packets In        Bytes In Packets Out       Bytes OutExpiretime        Valid
2005-02-17 16:44:19 +0800  QA-W1300-Casper-213        Create_OD_User     N7E9     0.0.0.0  00:00:00:00:00:00 0         0         0         0
2005-02-17 16:44:57 +0800  QA-W1300-Casper-213        OD_User_Login      N7E9     192.168.30.189     00:0C:F1:28:BF:D8 0         0         0
2005-02-17 16:45:22 +0800  QA-W1300-Casper-213        OD_User_Logout     N7E9     192.168.30.189     00:0C:F1:28:BF:D8 32        14499     30
```

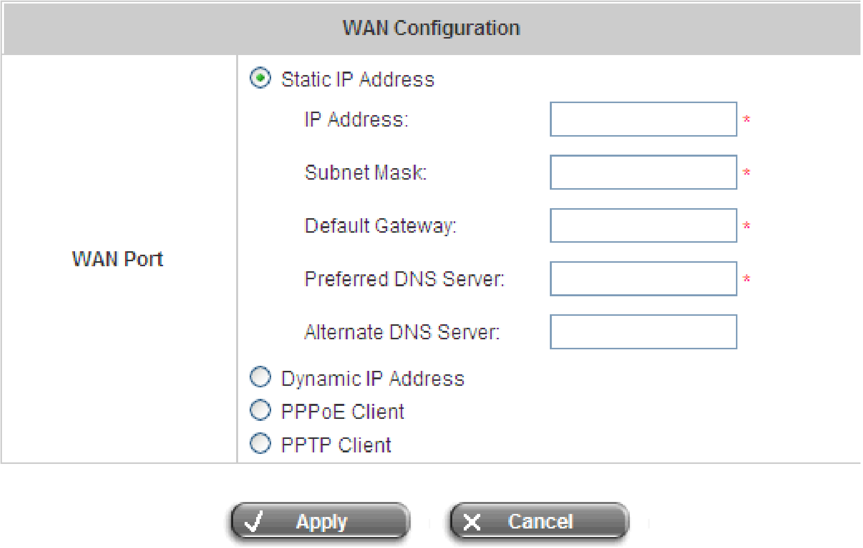
- **Remote Manage IP:** Set the IP range where the web management interface of HS1100 can be connected via the authenticated port (WAN or Public LAN). For example, 10.2.3.0/24 means that as long as you are within the IP range of 10.2.3.0/24, you can reach the management interface.
- **SNMP:** HS1100 supports SNMPv2. If this function is enabled, the administrator can assign the Manager IP address and the SNMP community name used to access the Management Information Base (MIB) of the system.
- **User logon SSL:** Enable to activate https (encryption) or disable to activate http (non encryption) login page.
- **Time:** HS1100 supports NTP (Network Time Protocol) communication protocol to synchronize the network time. Please specify the IP address of a NTP server to adjust the time automatically (Universal Time is Greenwich Mean Time, GMT). The time can also be set manually by selecting **"Set Device Date and Time"** and then entering the date and time in these fields.



| | |
|---|---|
| Time | Device Time : 2008/11/20 11:16:14<br>Time Zone:<br>(GMT+10:00)Canberra,Melbourne,Sydney<br>● NTP Enable<br>NTP Server 1: ntp1.cs.mu.OZ.AU *(e.g. tock.usno.navy.mil)<br>NTP Server 2: tock.usno.navy.mil<br>NTP Server 3: ntp1.fau.de<br>NTP Server 4: clock.cuhk.edu.hk<br>NTP Server 5: ntps1.pads.ufrj.br<br>○ Set Device Date and Time |

## WAN Configuration

There are 4 methods of obtaining IP address for the WAN Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE** and **PPTP Client**.



WAN Configuration

WAN Port

● Static IP Address

IP Address: *

Subnet Mask: *

Default Gateway: *

Preferred DNS Server: *

Alternate DNS Server:

○ Dynamic IP Address

○ PPPoE Client

○ PPTP Client

- **Static IP Address:** Manually specifying the IP address of the WAN Port is applicable for the network environment where the DHCP server is unavailable. The fields with red asterisks are required to be filled in.

  **IP Address:** The IP address of the WAN port.

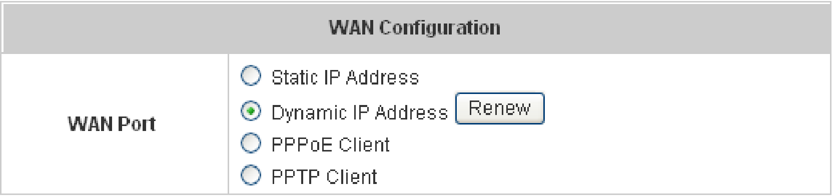
  **Subnet Mask:** The subnet mask of the WAN port.

  **Default Gateway:** The gateway of the WAN port.

  **Preferred DNS Server:** The primary DNS Server of the WAN port.

  **Alternate DNS Server:** The substitute DNS Server of the WAN port. This is not required.

- **Dynamic IP Address:** It is only applicable for the network environment where the DHCP server is available on the network. Click the ***Renew*** button to get an IP address automatically.



WAN Configuration

WAN Port

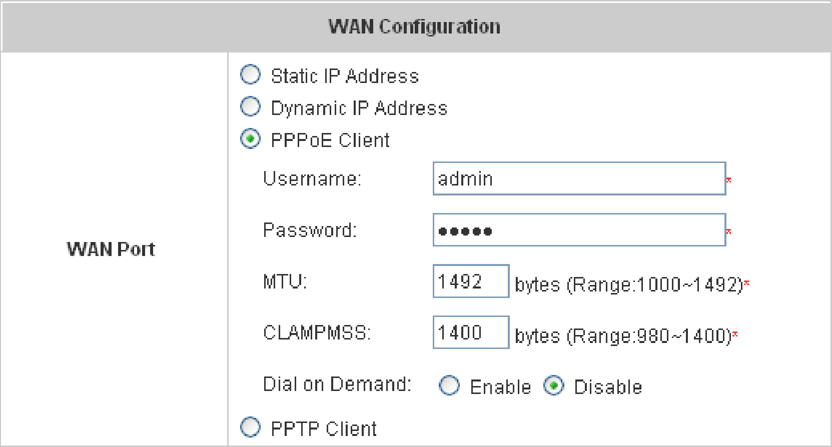
○ Static IP Address

● Dynamic IP Address

○ PPPoE Client

○ PPTP Client

- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the **“User Name”**, **“Password”**, **“MTU”** and **“CLAMPMSS”**. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.



WAN Configuration

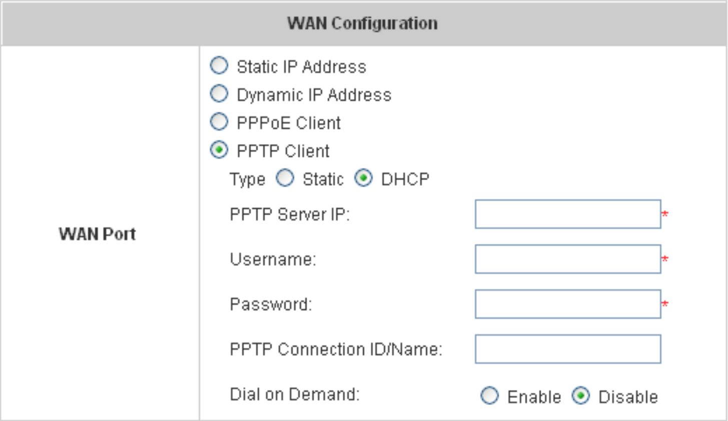
WAN Port

○ Static IP Address
○ Dynamic IP Address
● PPPoE Client

Username: admin *
Password: ●●●●● *
MTU: 1492 bytes (Range:1000~1492)*
CLAMPMSS: 1400 bytes (Range:980~1400)*
Dial on Demand: ○ Enable ● Disable

○ PPTP Client

- **PPTP Client:** Select **STATIC** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required to be filled in. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.



WAN Configuration

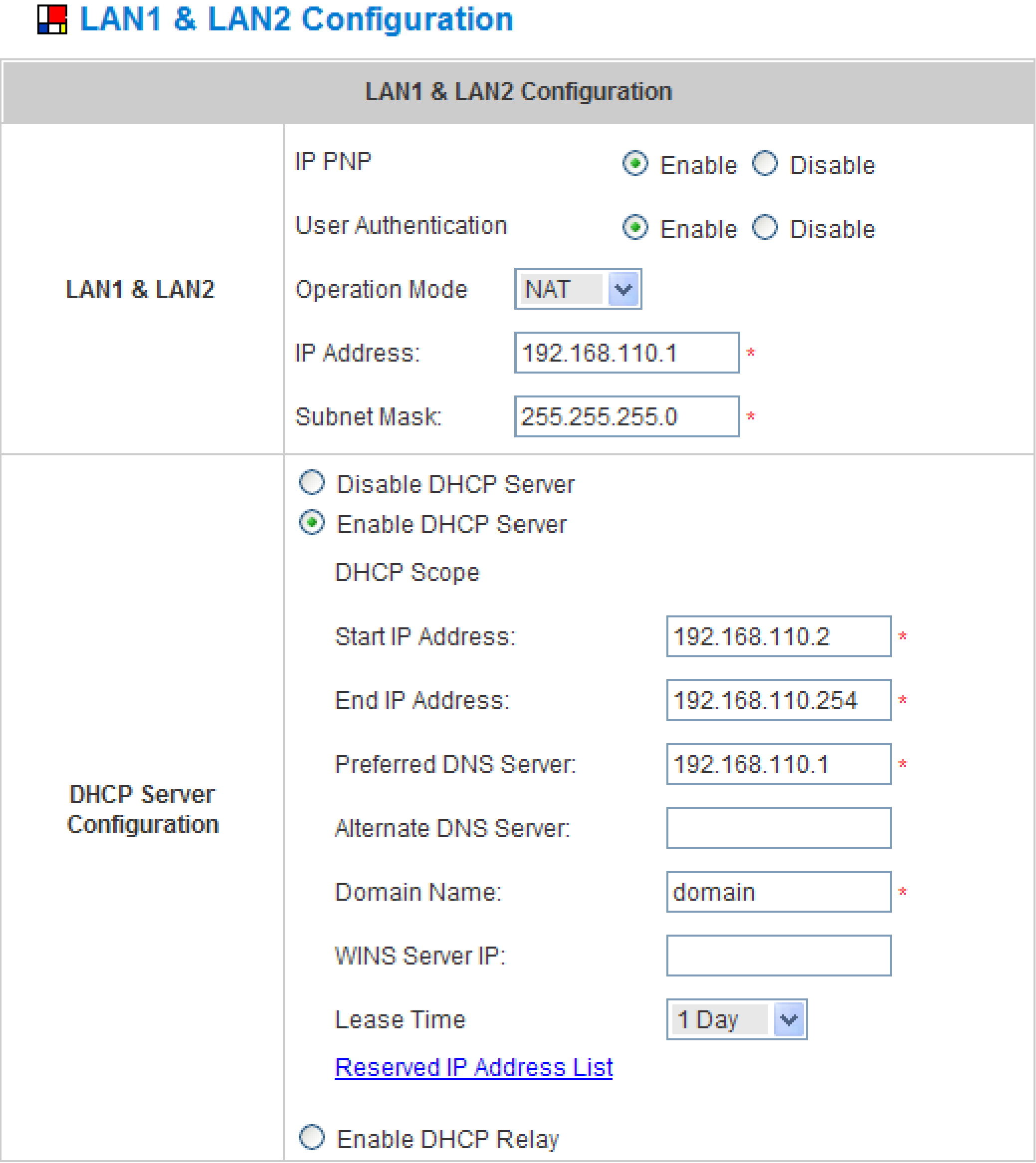
WAN Port

○ Static IP Address
○ Dynamic IP Address
○ PPPoE Client
● PPTP Client

Type ○ Static ● DHCP
PPTP Server IP: *
Username: *
Password: *
PPTP Connection ID/Name:
Dial on Demand: ○ Enable ● Disable

## LAN1 & LAN2 Configuration

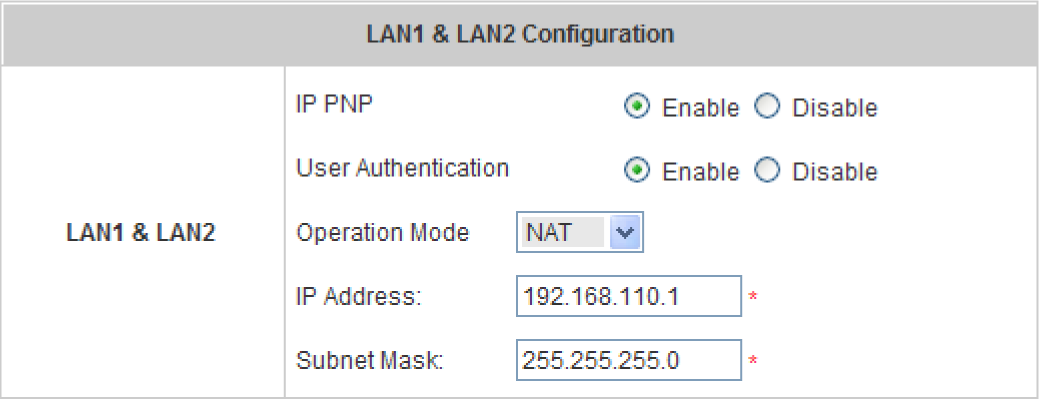
In this section, set the configuration for LAN1/LAN2 port and DHCP server. User authentication for LAN1/LAN2 port can be enabled or disabled.



LAN1 & LAN2 Configuration

| LAN1 & LAN2 Configuration | |
|---|---|
| LAN1 & LAN2 | IP PNP ● Enable ○ Disable<br>User Authentication ● Enable ○ Disable<br>Operation Mode NAT<br>IP Address: 192.168.110.1 *<br>Subnet Mask: 255.255.255.0 * |
| DHCP Server Configuration | ○ Disable DHCP Server<br>● Enable DHCP Server<br>DHCP Scope<br>Start IP Address: 192.168.110.2 *<br>End IP Address: 192.168.110.254 *<br>Preferred DNS Server: 192.168.110.1 *<br>Alternate DNS Server:<br>Domain Name: domain *<br>WINS Server IP:<br>Lease Time 1 Day<br>Reserved IP Address List<br>○ Enable DHCP Relay |

- **LAN1 & LAN2 Port**



| LAN1 & LAN2 Configuration | | |
|---|---|---|
| LAN1 & LAN2 | IP PNP | ● Enable ○ Disable |
| | User Authentication | ● Enable ○ Disable |
| | Operation Mode | NAT |
| | IP Address: | 192.168.110.1 * |
| | Subnet Mask: | 255.255.255.0 * |

**IP PNP:** Choose to enable or disable this function. If **"IP PnP"** is enabled, no matter what the IP address of the client device is – static or dynamic IP, users can access the network without changing the client IP address after being authenticated by HS1100.

**User Authentication:** Choose to enable or disable this function. If **"User Authentication"** is disabled, users can access the Internet without being authenticated.

**Operation Mode:** Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

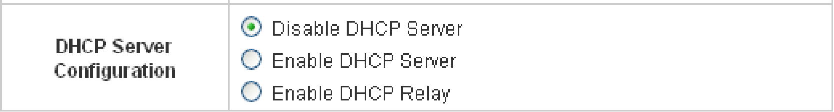
**IP Address:** Enter the desired IP address for the LAN1 & LAN2 port.

**Subnet Mask:** Enter the desired subnet mask for the LAN1 & LAN2 port.

- **DHCP Server Configuration**

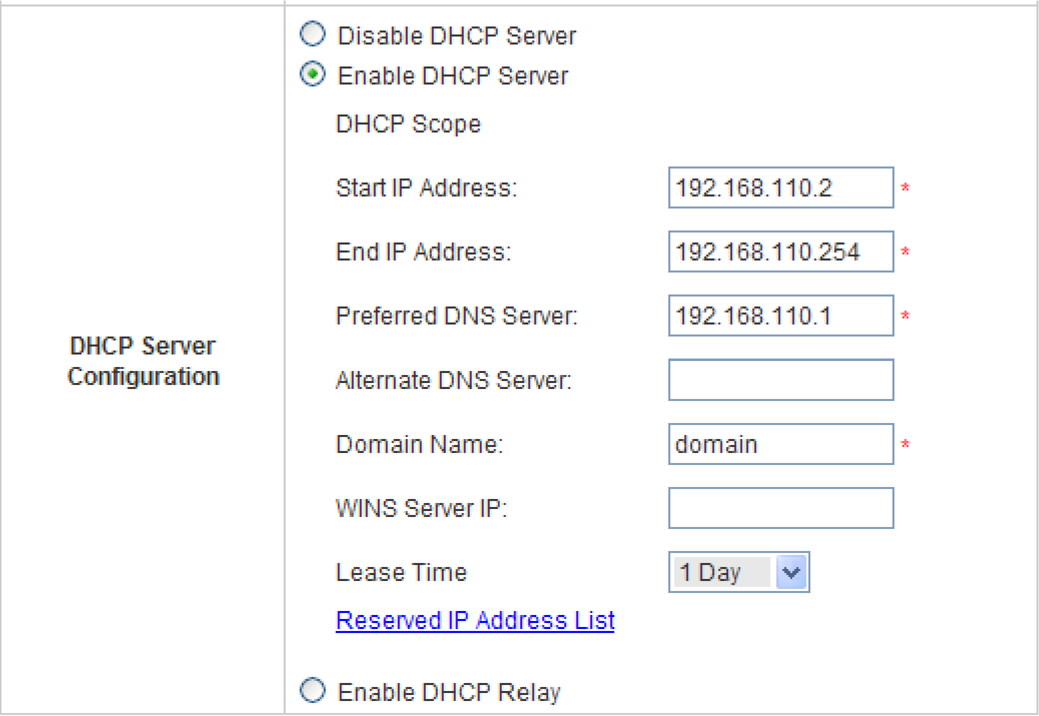
There are three methods to set the DHCP Server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable DHCP Server function.



| | |
|---|---|
| DHCP Server Configuration | ● Disable DHCP Server<br>○ Enable DHCP Server<br>○ Enable DHCP Relay |

2. **Enable DHCP Server:** Choose **"Enable DHCP Sever"** function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.



| | |
|---|---|
| **DHCP Server Configuration** | ○ Disable DHCP Server<br>● Enable DHCP Server<br>DHCP Scope<br>Start IP Address: 192.168.110.2 *<br>End IP Address: 192.168.110.254 *<br>Preferred DNS Server: 192.168.110.1 *<br>Alternate DNS Server:<br>Domain Name: domain *<br>WINS Server IP:<br>Lease Time: 1 Day<br>Reserved IP Address List<br>○ Enable DHCP Relay |

**DHCP Scope:** Enter the **"Start IP Address"** and the **"End IP Address"** of this DHCP block. These fields define the IP address range that will be assigned to the Public LAN clients.

**Preferred DNS Server:** The primary DNS server for the DHCP.

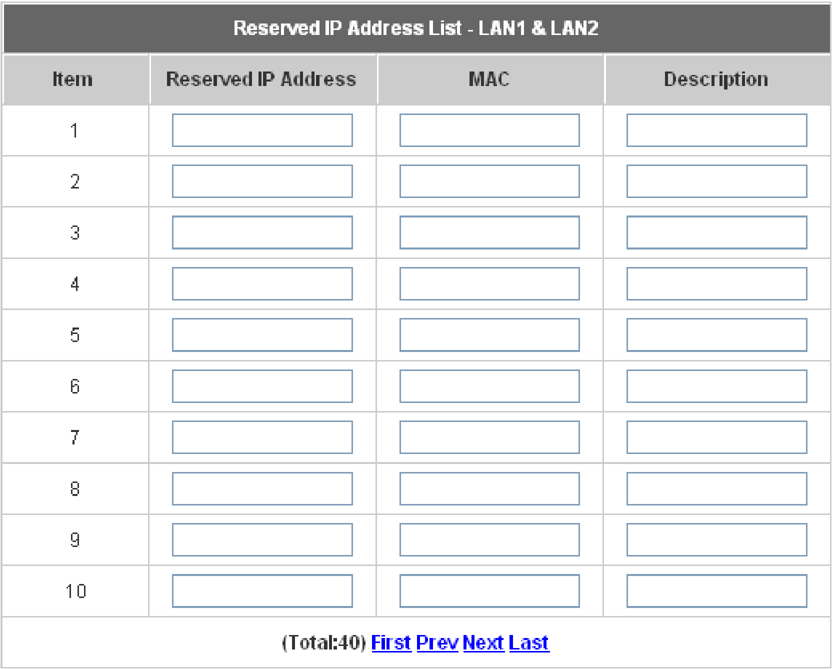
**Alternate DNS Server:** The substitute DNS server for the DHCP.

**Domain Name:** Enter the domain name.

**WINS IP Address:** Enter the IP address of WINS.

**Lease Time:** Choose the time interval to update DHCP IP addresses automatically.

**Reserved IP Address List:** To reserve an IP address for a specific client device via MAC, click the hyperlink of ***Reserved IP Address***. Then, the setup screen of the Reserved IP Address List as shown in the following figure will appear. Enter the related **"Reserved IP Address"**, **"MAC"**, and Description (not mandatory). Click ***Apply*** to save the settings.

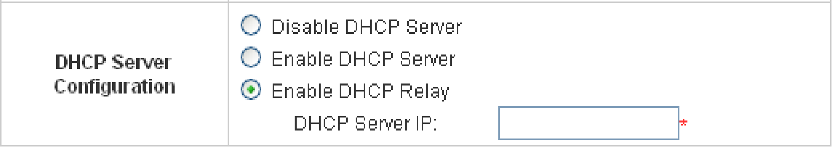


Reserved IP Address List - LAN1 & LAN2

| Item | Reserved IP Address | MAC | Description |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

(Total:40) First Prev Next Last

3. **Enable DHCP Relay:** If enabling this function is desired, the other DHCP Server IP address must be specified. See the following figure.

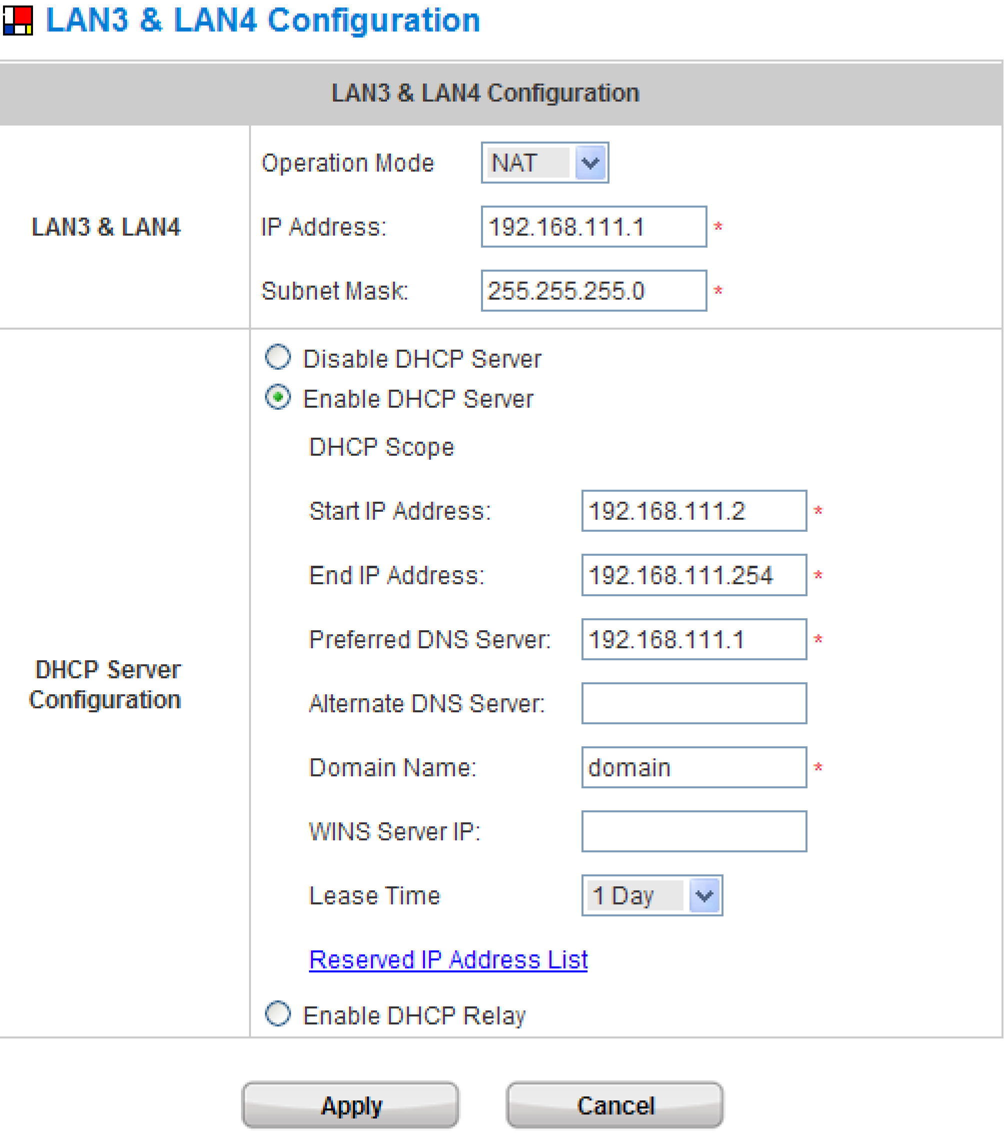


DHCP Server Configuration

○ Disable DHCP Server
○ Enable DHCP Server
● Enable DHCP Relay
DHCP Server IP: ______ *

## LAN3 & LAN4 Configuration

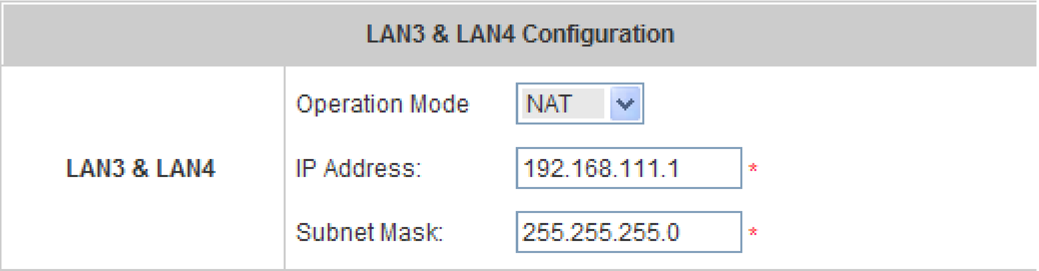
In this section, set the configuration for LAN3/LAN4 port and DHCP server.



LAN3 & LAN4 Configuration

| LAN3 & LAN4 Configuration | |
|---|---|
| LAN3 & LAN4 | Operation Mode: NAT<br>IP Address: 192.168.111.1 *<br>Subnet Mask: 255.255.255.0 * |
| DHCP Server Configuration | ○ Disable DHCP Server<br>● Enable DHCP Server<br>DHCP Scope<br>Start IP Address: 192.168.111.2 *<br>End IP Address: 192.168.111.254 *<br>Preferred DNS Server: 192.168.111.1 *<br>Alternate DNS Server:<br>Domain Name: domain *<br>WINS Server IP:<br>Lease Time: 1 Day<br>Reserved IP Address List<br>○ Enable DHCP Relay |

- **LAN3 & LAN4 Port**



| LAN3 & LAN4 Configuration | |
|---|---|
| LAN3 & LAN4 | Operation Mode: NAT<br>IP Address: 192.168.111.1 *<br>Subnet Mask: 255.255.255.0 * |

**Operation Mode:** Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

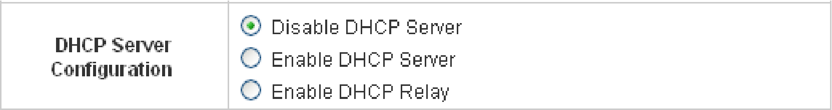
**IP Address:** Enter the desired IP address for the LAN3 & LAN4 port.

**Subnet Mask:** Enter the desired subnet mask for the LAN3 & LAN4 port.

- **DHCP Server Configuration**

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

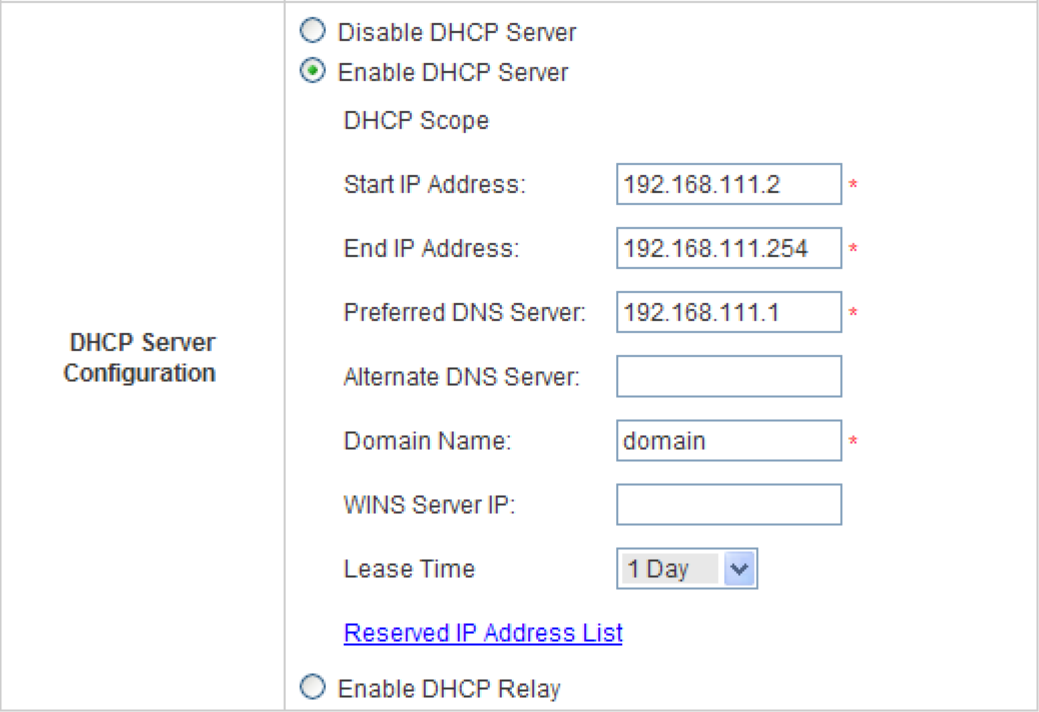
1. **Disable DHCP Server:** Disable DHCP Server function.



DHCP Server Configuration

● Disable DHCP Server
○ Enable DHCP Server
○ Enable DHCP Relay

2. **Enable DHCP Server:** Choose **"Enable DHCP Sever"** function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.



DHCP Server Configuration

○ Disable DHCP Server
● Enable DHCP Server

DHCP Scope

| | |
|---|---|
| Start IP Address: | 192.168.111.2 * |
| End IP Address: | 192.168.111.254 * |
| Preferred DNS Server: | 192.168.111.1 * |
| Alternate DNS Server: | |
| Domain Name: | domain * |
| WINS Server IP: | |
| Lease Time | 1 Day |

Reserved IP Address List

○ Enable DHCP Relay

**DHCP Scope:** Enter the **"Start IP Address"** and the **"End IP Address"** of this DHCP block. These fields define the IP address range that will be assigned to the Private LAN clients.

**Preferred DNS Server:** The primary DNS server for the DHCP.

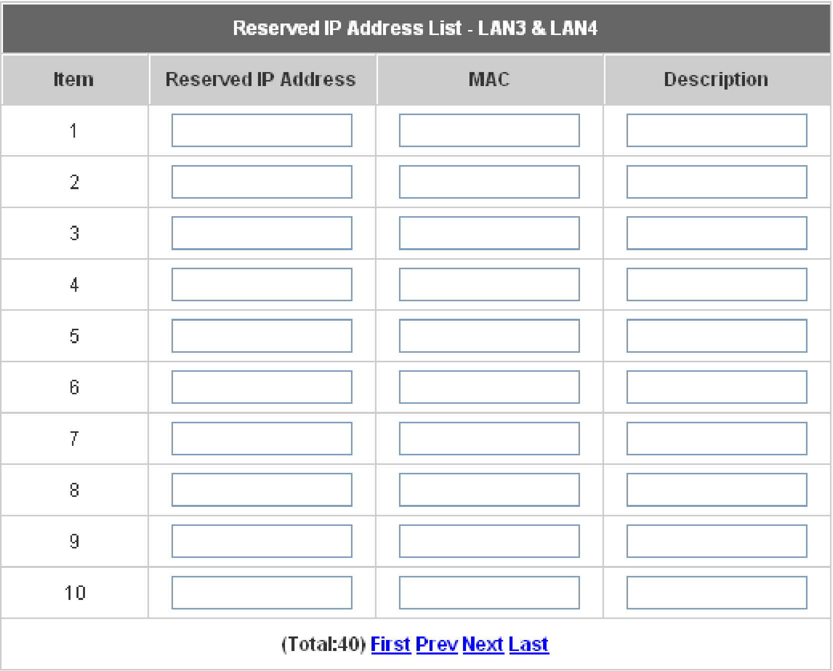
**Alternate DNS Server:** The substitute DNS server for the DHCP.

**Domain Name:** Enter the domain name.

**WINS IP Address:** Enter the IP address of WINS.

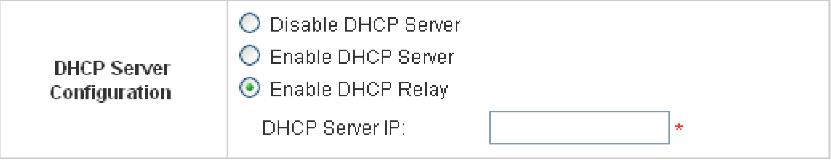
**Lease Time:** Choose the time interval to update DHCP IP addresses automatically.

**Reserved IP Address List:** To reserve an IP address for a specific client device via MAC, click the hyperlink of ***Reserved IP Address***. Then, the setup screen of the Reserved IP Address List as shown in the following figure will appear. Enter the related **"Reserved IP Address"**, **"MAC"**, and Description (not mandatory). Click ***Apply*** to save the settings.



| Reserved IP Address List - LAN3 & LAN4 | | | |
|---|---|---|---|
| Item | Reserved IP Address | MAC | Description |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| (Total:40) First Prev Next Last | | | |

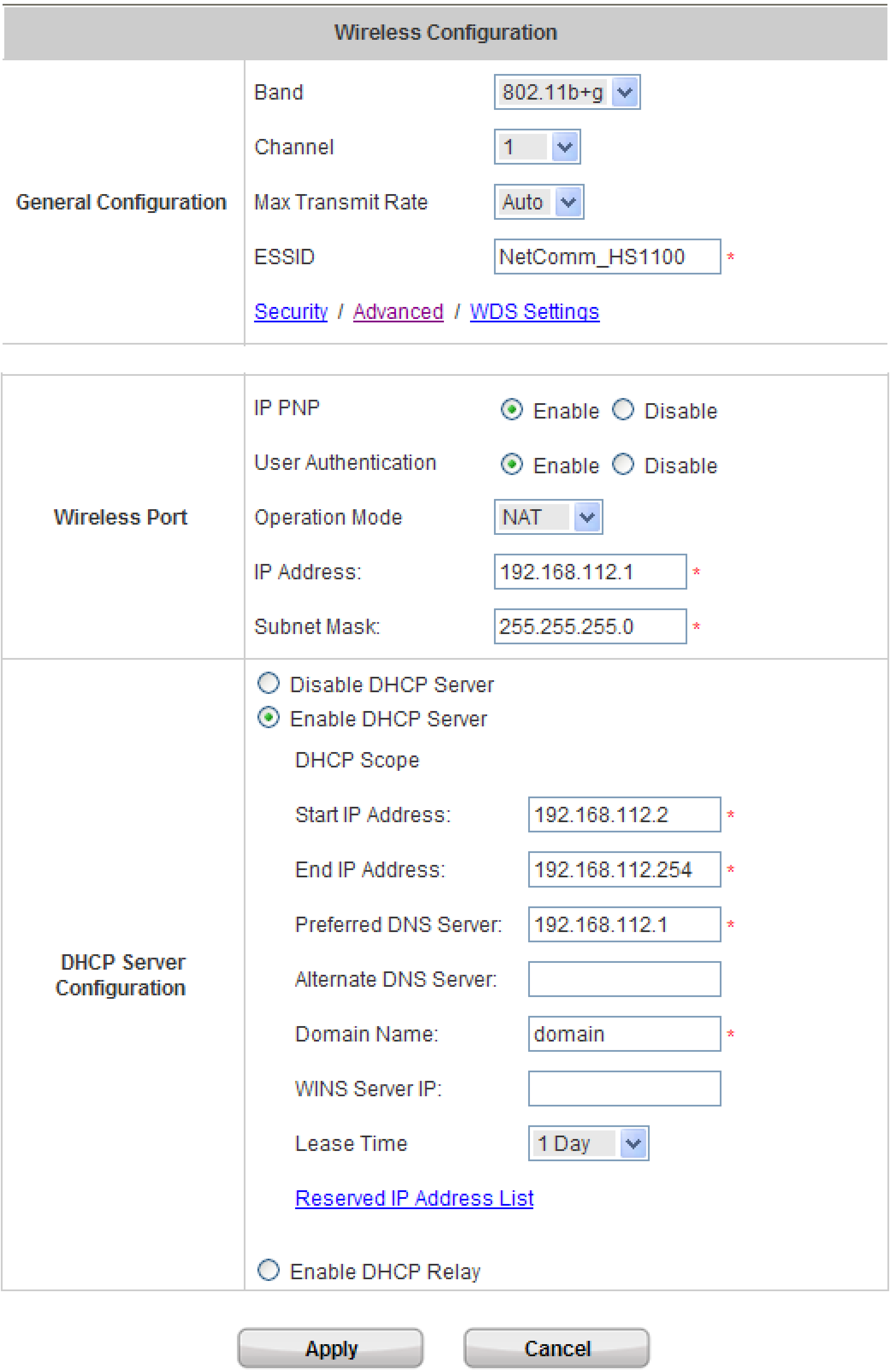
3. **Enable DHCP Relay:** If enabling this function is desired, the other DHCP Server IP address must be specified. See the following figure.



| | |
|---|---|
| DHCP Server Configuration | ○ Disable DHCP Server<br>○ Enable DHCP Server<br>● Enable DHCP Relay<br>DHCP Server IP: ____ * |

## Wireless Configuration

In this section, set the configuration for the wireless port.



Wireless Configuration

| | | |
|---|---|---|
| General Configuration | Band | 802.11b+g |
| | Channel | 1 |
| | Max Transmit Rate | Auto |
| | ESSID | NetComm_HS1100 * |
| | Security / Advanced / WDS Settings | |
| Wireless Port | IP PNP | ● Enable ○ Disable |
| | User Authentication | ● Enable ○ Disable |
| | Operation Mode | NAT |
| | IP Address: | 192.168.112.1 * |
| | Subnet Mask: | 255.255.255.0 * |
| DHCP Server Configuration | ○ Disable DHCP Server | |
| | ● Enable DHCP Server | |
| | DHCP Scope | |
| | Start IP Address: | 192.168.112.2 * |
| | End IP Address: | 192.168.112.254 * |
| | Preferred DNS Server: | 192.168.112.1 * |
| | Alternate DNS Server: | |
| | Domain Name: | domain * |
| | WINS Server IP: | |
| | Lease Time | 1 Day |
| | Reserved IP Address List | |
| | ○ Enable DHCP Relay | |

- **Wireless Configuration**

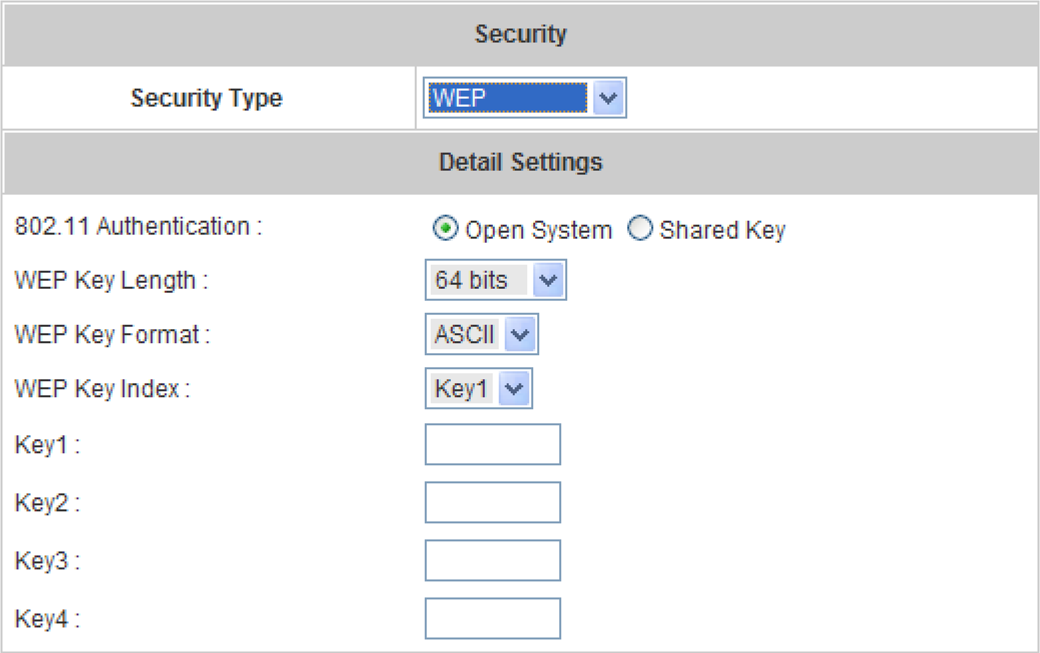
  **Band:** There are 4 modes to select from, **802.11b** (2.4G, 1~11Mbps) and **802.11 (b+g)** (2.4G, 1~11Mbps and 2.4G, 54Mbps).

**Channel:** Select the appropriate channel from the list to correspond to the network settings; for example, Channel 1~11 is available in the North America area. All access points on the same wireless network must use the same channel to ensure correct connection.

**Max Transmit Rate:** The default value is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of this particular wireless network.

**ESSID:** The SSID is a unique name shared among all devices in a wireless network. The SSID must be the same for all devices in the wireless network. The SSID must not exceed 32 characters and may be any character on the keyboard. The administrator can give a new name in this field or use the default name.

- **Security:** Configure **wireless encryption methods.** For security settings in detail, please click the hyperlink of ***Security*** to go into the **Security** page. Choose ***Security*** to configure the settings.



Security

Security Type: WEP

Detail Settings

802.11 Authentication : ● Open System ○ Shared Key

WEP Key Length : 64 bits

WEP Key Format : ASCII

WEP Key Index : Key1

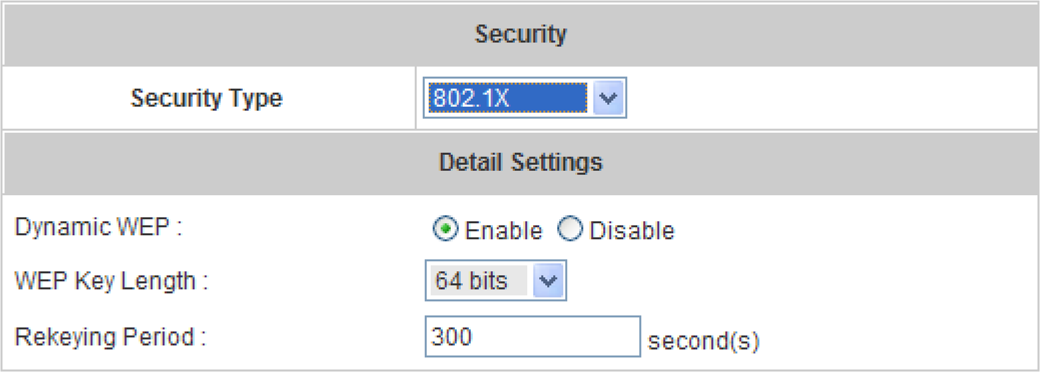
Key1 :

Key2 :

Key3 :

Key4 :

***WEP Type***



Security

Security Type: 802.1X

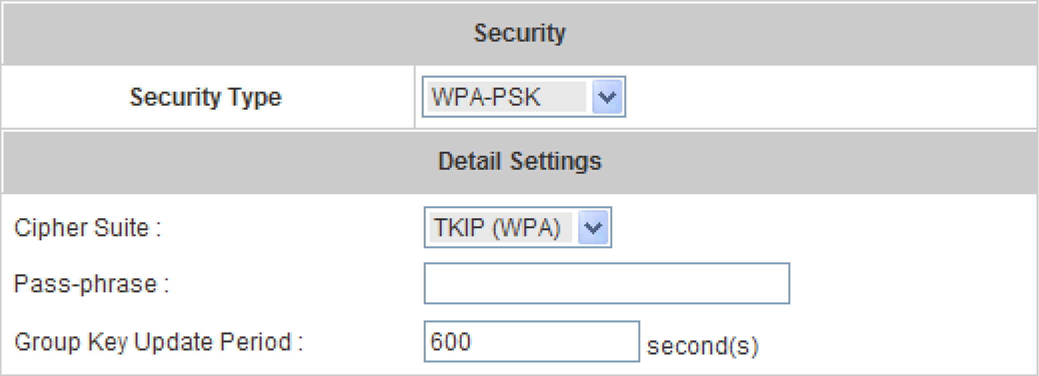
Detail Settings

Dynamic WEP : ● Enable ○ Disable

WEP Key Length : 64 bits

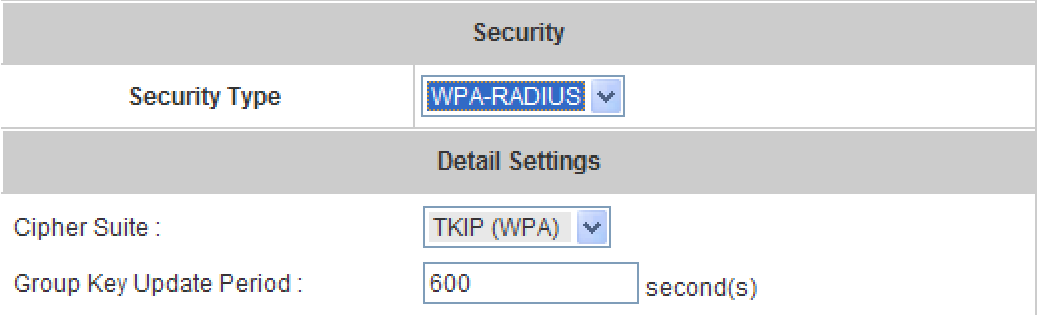
Rekeying Period : 300 second(s)

***802.1X Type***



| Security | |
|---|---|
| Security Type | WPA-PSK |
| Detail Settings | |
| Cipher Suite : | TKIP (WPA) |
| Pass-phrase : | |
| Group Key Update Period : | 600 second(s) |

***WPA-PSK Type***



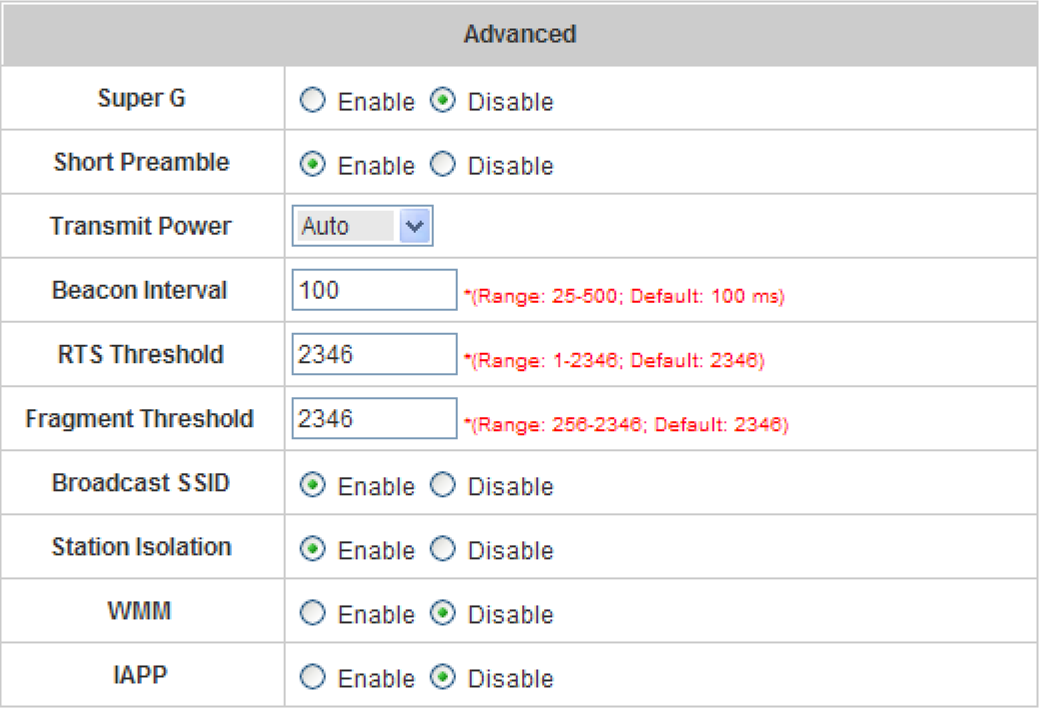
| Security | |
|---|---|
| Security Type | WPA-RADIUS |
| Detail Settings | |
| Cipher Suite : | TKIP (WPA) |
| Group Key Update Period : | 600 second(s) |

***WPA-RADIUS Type***

1. **Security Type:** There are disabled and 4 other security types to choose from, **WEP (Wired Equivalent Privacy)**, **802.1X**, **WPA-PSK** and **WPA-RADIUS**.
2. **Detail Settings**

- **802.11 Authentication:** Choose either Open System or encryption with static Shared Key.
- **WEP Key Length/Format/Index**: This is a data privacy mechanism based on a 64 bit or 128 bits shared key algorithm. There are types of encryption, HEX or ASCII.
- **Re-keying Period:** The default is 300 seconds.
- **Cipher Suite:** Choose among WPA, WPA2 or Mixed.
- **Pass-phrase:** Type the pass phrase for administrators.
- **Group Key Update Period:** The default is 600 seconds. Time for updated period.

- **Advanced:** Configure **wireless transmission data packet format** (for advanced users only, default recommended). Please click the hyperlink ***Advanced*** to go into the **Advanced** configuration page.



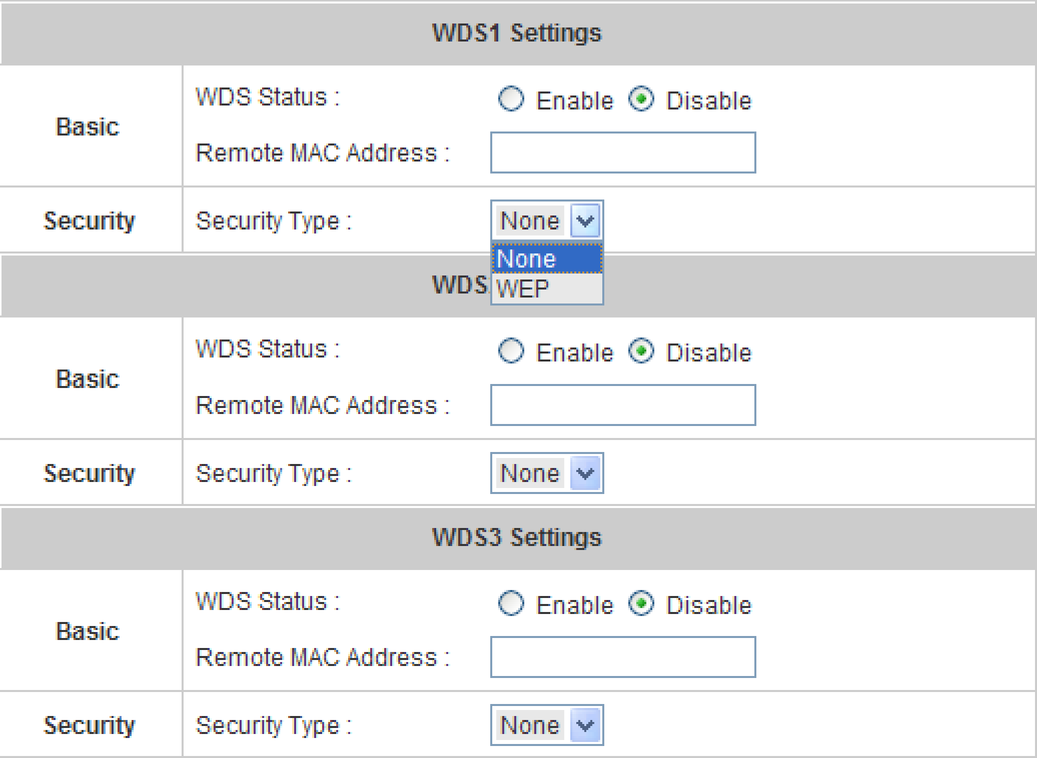
Advanced

| | |
|---|---|
| Super G | ○ Enable ● Disable |
| Short Preamble | ● Enable ○ Disable |
| Transmit Power | Auto |
| Beacon Interval | 100 *(Range: 25-500; Default: 100 ms) |
| RTS Threshold | 2346 *(Range: 1-2346; Default: 2346) |
| Fragment Threshold | 2346 *(Range: 256-2346; Default: 2346) |
| Broadcast SSID | ● Enable ○ Disable |
| Station Isolation | ● Enable ○ Disable |
| WMM | ○ Enable ● Disable |
| IAPP | ○ Enable ● Disable |

- **Super G:** Choose ***Enable*** or ***Disable*** this function.
- **Short Preamble:** Choose ***Enable*** or ***Disable*** this function.
- **Transmit Power:** The default value is **Auto**. Select a range of transmission speeds or use the default setting, **Auto**, to allow the access point to automatically use the fastest possible data rate.
- **Beacon Interval:** The default value is 100 milliseconds. The specified value represents the amount of time between access point beacon signal transmissions.
- **RTS Threshold: R**eady **T**o **S**end threshold. The range is from 256 to 2346 and the default is **OFF**. The administrator can set the value which is the amount of time between packet transmissions. It is recommended that the value remains in the range of 256 to 2346.
- **Fragment Threshold:** The range is from 256 to 2346 and the default is **OFF**. The value specifies the maximum size of a packet allowed before data is fragmented into multiple packets. It should be remained in the range of 256 to 2346. A smaller value results in smaller packets but allows a larger number of packets in transmission.
- **Broadcast SSID:** Enable or disable SSID broadcast. When disabled, clients cannot detect Access Point by its SSID broadcast, they must manually connect to Access Point by entering SSID on their devices.
- **Station Isolation:** When enabled, wireless client stations are isolated from each other. In other words, one PC on the wireless network is not able to see other PCs on the same wireless network.
- **WMM:** WMM (Wi-Fi Multimedia) provides basic Quality of service (QoS) features to Wi-Fi networks. When enabled, it prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background. However, it does not provide guaranteed throughput.
- **IAPP:** IAPP (Inter-Access Point Protocol) is to support smooth users' hand-over (roaming) from one access point to another. When enabled, it provides a better capability for wireless client stations to roam among APs with the same SSID.

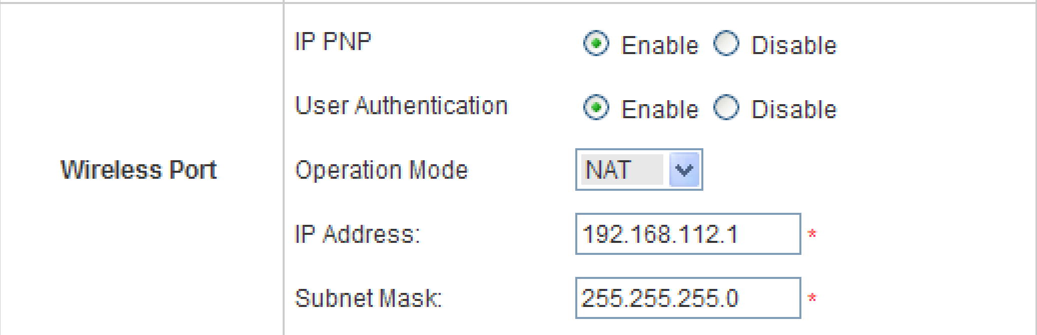
- **WDS Settings:**

Choose ***WDS Setting*** to configure the settings. This function can extend the range of accessing the network. When this function is enabled, please enter the MAC address of the repeater in the blank and choose Security Type.



| WDS1 Settings | | |
|---|---|---|
| Basic | WDS Status : | ○ Enable ● Disable |
| | Remote MAC Address : | |
| Security | Security Type : | None<br>None<br>WEP |
| WDS | | |
| Basic | WDS Status : | ○ Enable ● Disable |
| | Remote MAC Address : | |
| Security | Security Type : | None |
| WDS3 Settings | | |
| Basic | WDS Status : | ○ Enable ● Disable |
| | Remote MAC Address : | |
| Security | Security Type : | None |

- **Wireless Configuration**



| | | |
|---|---|---|
| Wireless Port | IP PNP | ● Enable ○ Disable |
| | User Authentication | ● Enable ○ Disable |
| | Operation Mode | NAT |
| | IP Address: | 192.168.112.1 * |
| | Subnet Mask: | 255.255.255.0 * |

**IP PNP:** Choose to enable or disable this function. If **"IP PnP"** is enabled, no matter what the IP address of the client device is – static or dynamic IP, users can access the network without changing the client IP address after being authenticated by HS1100.

**User Authentication:** If **"User Authentication"** is disabled, **"Specific Route Profile"** needs to be specified for users to access the Internet.

**Operation Mode:** Select one from the two modes, **NAT** mode and **Router** mode, by the requirements.

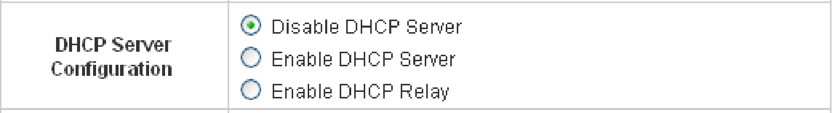
**IP Address:** Enter desired IP address for the wireless port.

**Subnet Mask:** Enter desired subnet mask for the wireless port.

- **DHCP Server configuration**

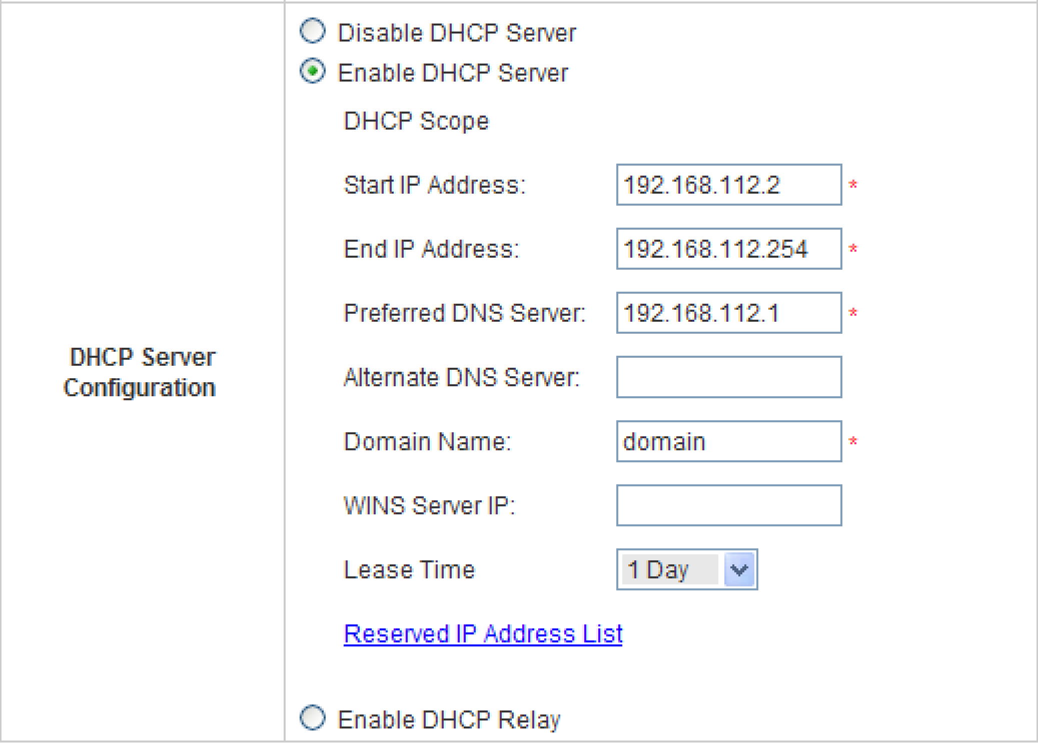
There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable the DHCP Server function.



| DHCP Server Configuration | ● Disable DHCP Server<br>○ Enable DHCP Server<br>○ Enable DHCP Relay |
|---|---|

2. **Enable DHCP Server:** Choose **"Enable DHCP Sever"** function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.



DHCP Server Configuration

○ Disable DHCP Server
● Enable DHCP Server

DHCP Scope

| | | |
|---|---|---|
| Start IP Address: | 192.168.112.2 | * |
| End IP Address: | 192.168.112.254 | * |
| Preferred DNS Server: | 192.168.112.1 | * |
| Alternate DNS Server: | | |
| Domain Name: | domain | * |
| WINS Server IP: | | |
| Lease Time | 1 Day | |

Reserved IP Address List

○ Enable DHCP Relay

**DHCP Scope:** Enter **"Start IP Address"** and **"End IP Address"** of this DHCP block. These fields define the IP address range that will be assigned to the Wireless LAN clients.

**Preferred DNS Server:** The primary DNS server for the DHCP.

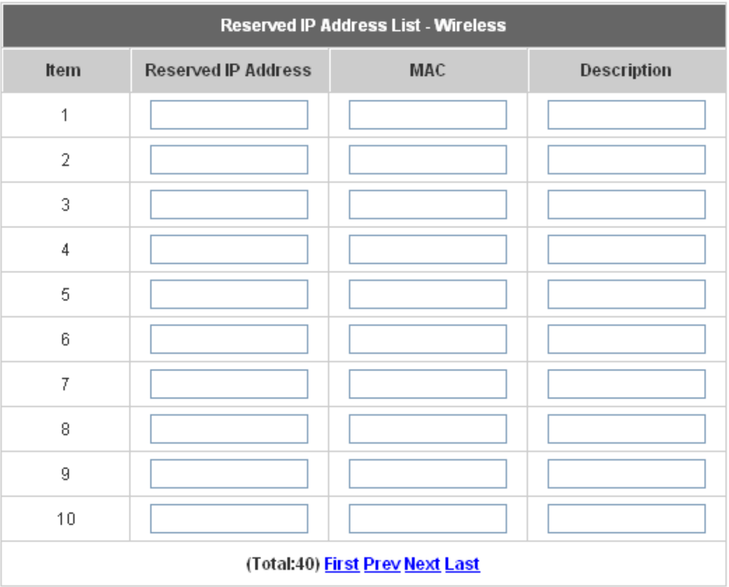
**Alternate DNS Server:** The substitute DNS server for the DHCP.

**Domain Name:** Enter the domain name.

**WINS IP Address:** Enter the IP address of WINS.

**Lease Time:** Choose the time interval to update DHCP IP addresses automatically.

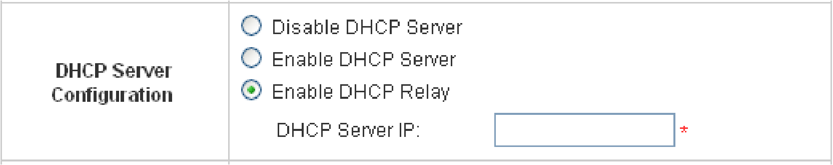
**Reserved IP Address List:** To reserve an IP address for a specific client device via MAC, click the hyperlink of ***Reserved IP Address***. Then, the setup screen of the Reserved IP Address List as shown in the following figure will appear. Enter the related **"Reserved IP Address"**, **"MAC"**, and Description (not mandatory). Click ***Apply*** to save the settings.



| Reserved IP Address List - Wireless | | | |
|---|---|---|---|
| Item | Reserved IP Address | MAC | Description |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

(Total:40) First Prev Next Last

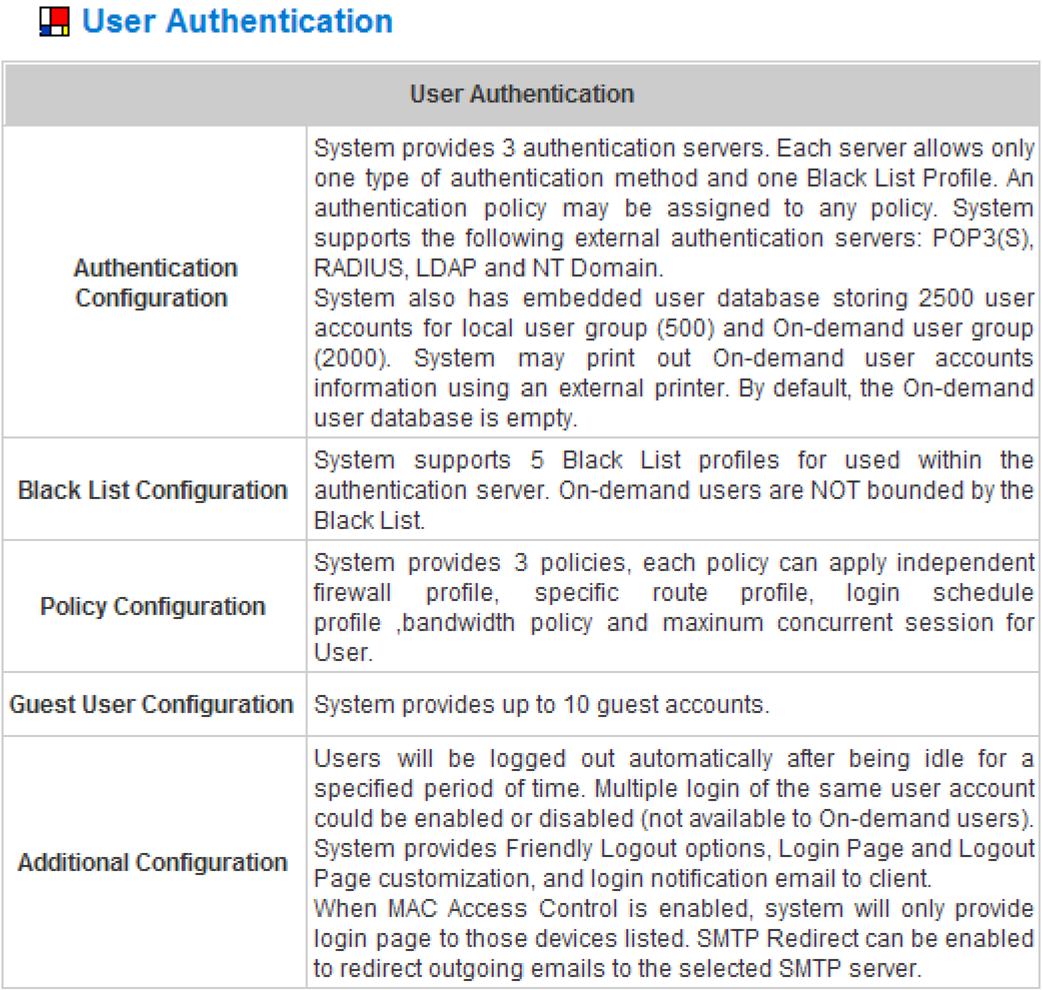
3. **Enable DHCP Relay:** If enabling this function is desired, the other DHCP Server IP address must be specified. See the following figure.



| | |
|---|---|
| DHCP Server Configuration | ○ Disable DHCP Server<br>○ Enable DHCP Server<br>● Enable DHCP Relay<br>DHCP Server IP: _____ * |

# User Authentication

This section includes the following functions: **Authentication Configuration**, **Black List Configuration**, **Policy Configuration**, **Guest User Configuration** and **Additional Configuration**.

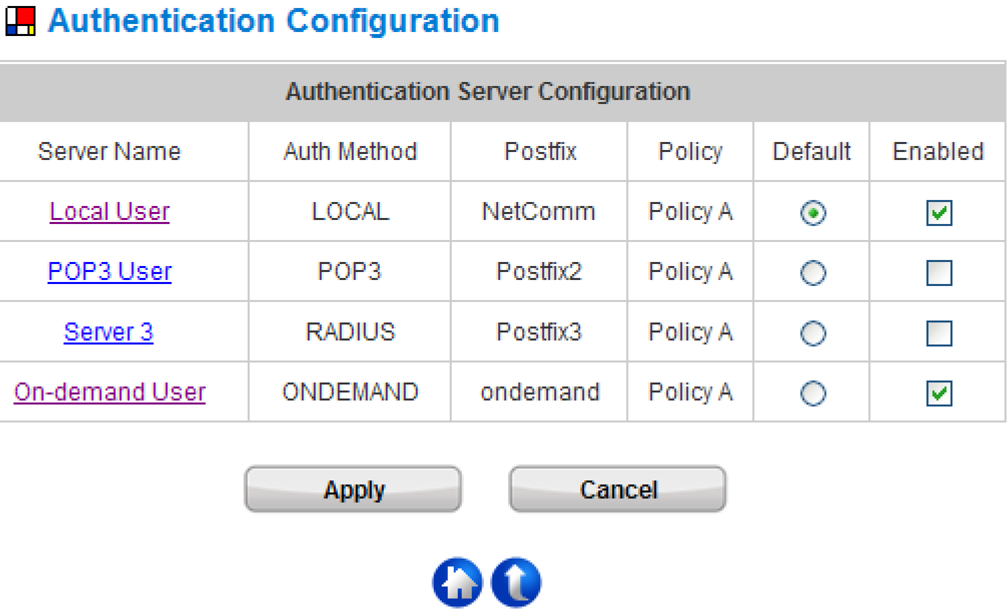


## User Authentication

| User Authentication | |
|---|---|
| Authentication Configuration | System provides 3 authentication servers. Each server allows only one type of authentication method and one Black List Profile. An authentication policy may be assigned to any policy. System supports the following external authentication servers: POP3(S), RADIUS, LDAP and NT Domain.<br>System also has embedded user database storing 2500 user accounts for local user group (500) and On-demand user group (2000). System may print out On-demand user accounts information using an external printer. By default, the On-demand user database is empty. |
| Black List Configuration | System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List. |
| Policy Configuration | System provides 3 policies, each policy can apply independent firewall profile, specific route profile, login schedule profile ,bandwidth policy and maxinum concurrent session for User. |
| Guest User Configuration | System provides up to 10 guest accounts. |
| Additional Configuration | Users will be logged out automatically after being idle for a specified period of time. Multiple login of the same user account could be enabled or disabled (not available to On-demand users). System provides Friendly Logout options, Login Page and Logout Page customization, and login notification email to client.<br>When MAC Access Control is enabled, system will only provide login page to those devices listed. SMTP Redirect can be enabled to redirect outgoing emails to the selected SMTP server. |

## Authentication Configuration

In this section, set the configuration for authentication servers, and on-demand user authentication. The **On-demand User** authentication is designed to create on-demand user accounts to provide temporary users with free or paid wireless Internet access.



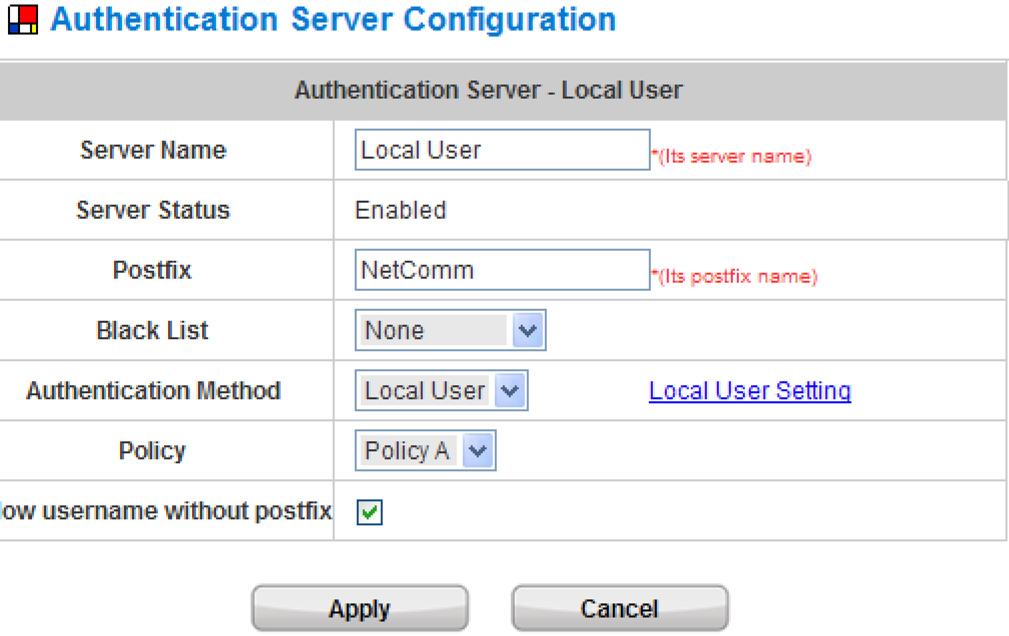
Authentication Configuration

| Authentication Server Configuration | | | | | |
|---|---|---|---|---|---|
| Server Name | Auth Method | Postfix | Policy | Default | Enabled |
| Local User | LOCAL | NetComm | Policy A | ● | ☑ |
| POP3 User | POP3 | Postfix2 | Policy A | ○ | □ |
| Server 3 | RADIUS | Postfix3 | Policy A | ○ | □ |
| On-demand User | ONDEMAND | ondemand | Policy A | ○ | ☑ |

- **Authentication Server Configuration**

  HS1100 provides three authentication servers and one on-demand server that the administrator can apply with different policy. Click on the server name to set the configuration for that particular server. After completing and clicking ***Apply*** to save the settings, go back to the previous page to select a server to be the default server and enable or disable any server on the list. Users can log into the default server without the postfix to allow faster login process.

  **Server 1~3: There are 5 authentication methods, Local User, POP3, RADIUS, LDAP and NTDomain, to select from.**



Authentication Server Configuration

| Authentication Server - Local User | |
|---|---|
| Server Name | Local User *(Its server name) |
| Server Status | Enabled |
| Postfix | NetComm *(Its postfix name) |
| Black List | None |
| Authentication Method | Local User  Local User Setting |
| Policy | Policy A |
| Allow username without postfix | ☑ |

**Server Name:** Set a name for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

**Sever Status:** The status shows that the server is enabled or disabled.

**Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

⚠ *The Policy Name cannot contain these words: MAC and IP.*

**Black List:** There are 5 sets of the black lists. Select from one of them or choose **"None"**. Please refer to **4.2.2 Black List Configuration**

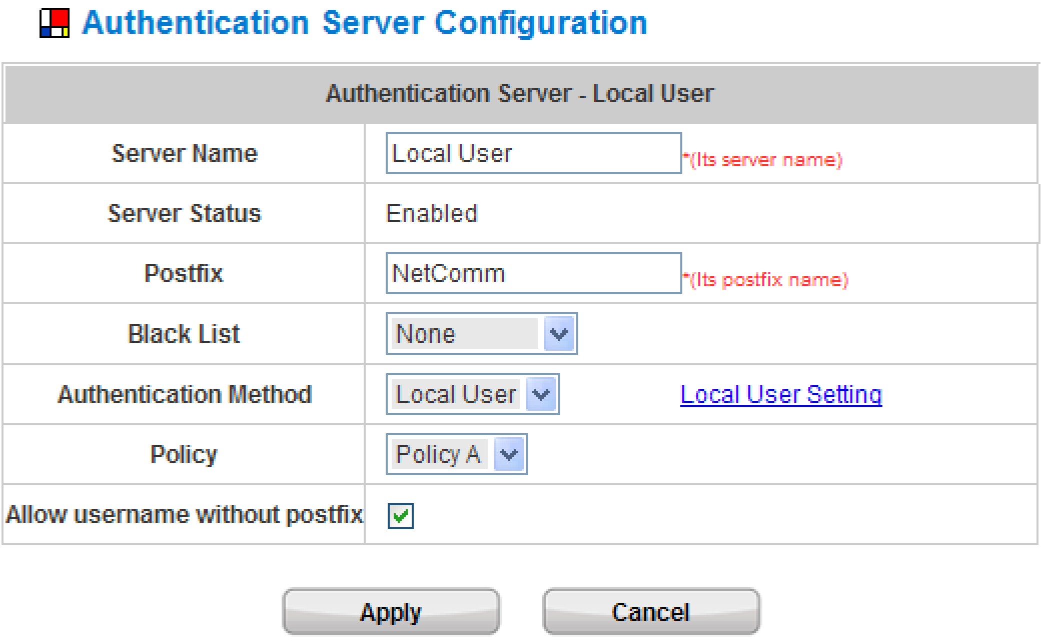
**Authentication Methods:** There are 5 authentication methods, **Local**, **POP3**, **RADIUS**, **LDAP** and **NT Domain** to select from for further configuration. Select the desired method and click the link besides the pull-down menu for the advanced configuration. For more details, please refer to **4.2.1.1~6 Authentication Method**.

⚠ *Enabling two or more servers of the same authentication method is NOT allowed.*

**Policy:** Select one from the 3 policies and apply it to this server.

**Authentication Method – Local User Setting**

Choose **"Local User"** from the **Authentication Method** field, the hyperlink besides the pull-down menu will become **"Local User Setting".**

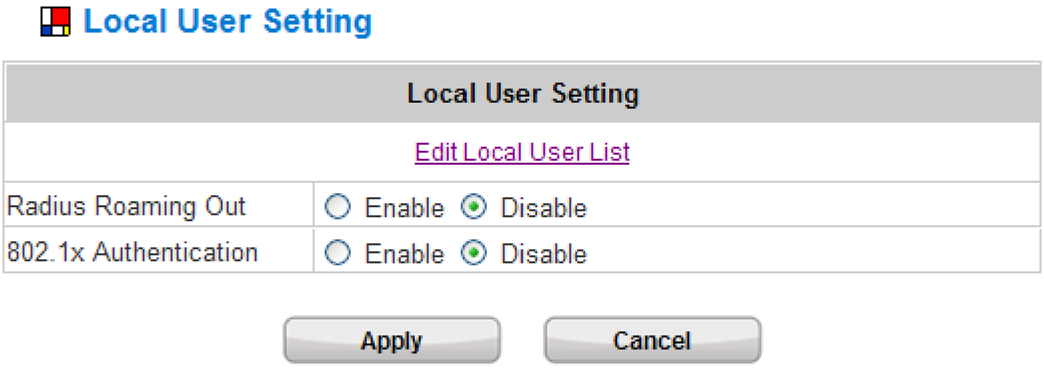


Authentication Server Configuration

| Authentication Server - Local User | |
|---|---|
| Server Name | Local User *(Its server name) |
| Server Status | Enabled |
| Postfix | NetComm *(Its postfix name) |
| Black List | None |
| Authentication Method | Local User    Local User Setting |
| Policy | Policy A |
| Allow username without postfix | ☑ |

*A. Local User Setting*

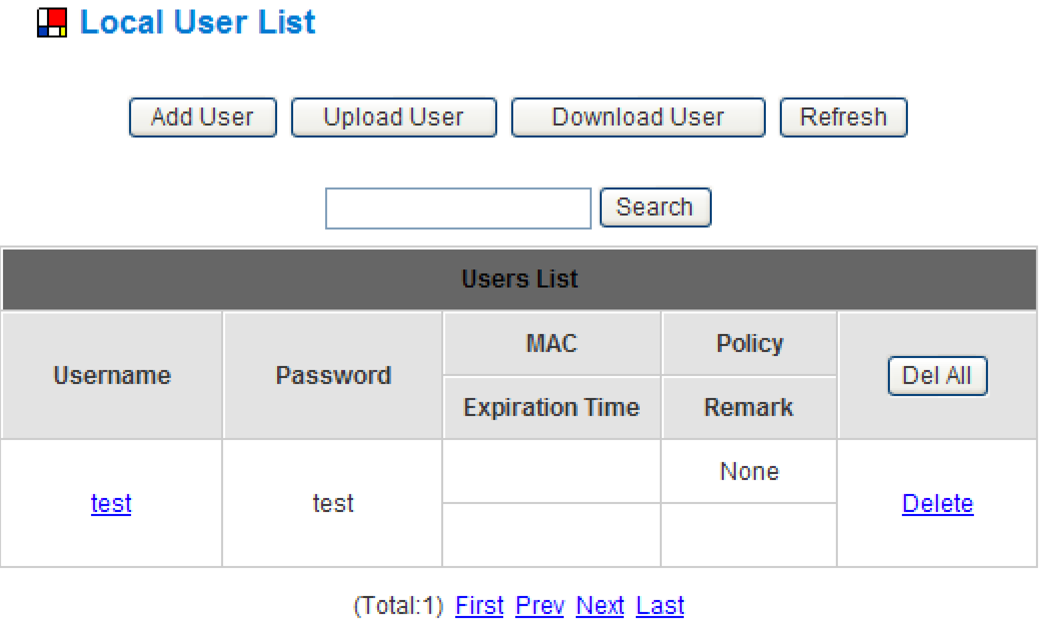
Click the hyperlink of ***Local User Setting*** for further configuration.



Local User Setting

| Local User Setting | |
|---|---|
| Edit Local User List | |
| Radius Roaming Out | ○ Enable ● Disable |
| 802.1x Authentication | ○ Enable ● Disable |

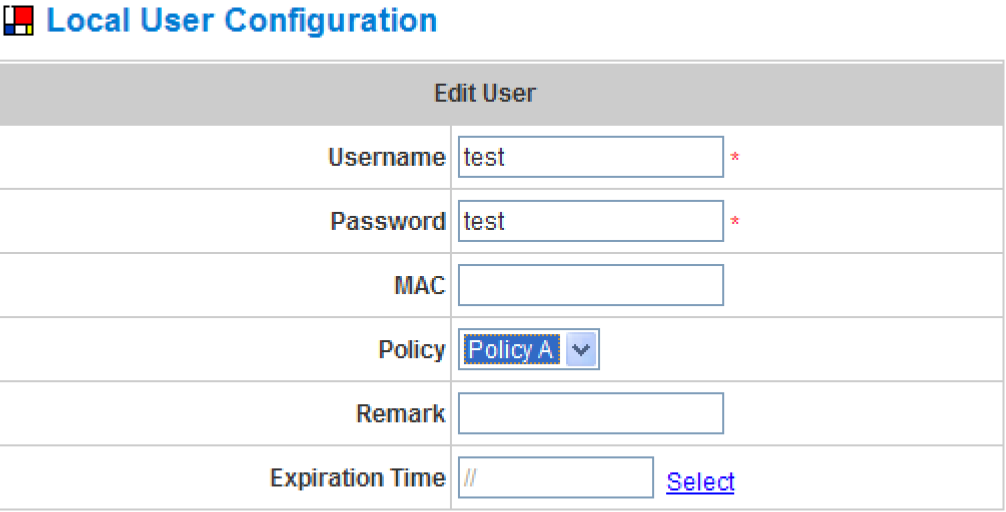
⇩



Local User List

| Users List | | | | |
|---|---|---|---|---|
| Username | Password | MAC | Policy | Del All |
| | | Expiration Time | Remark | |
| test | test | | None | Delete |
| | | | | |

(Total:1) First Prev Next Last

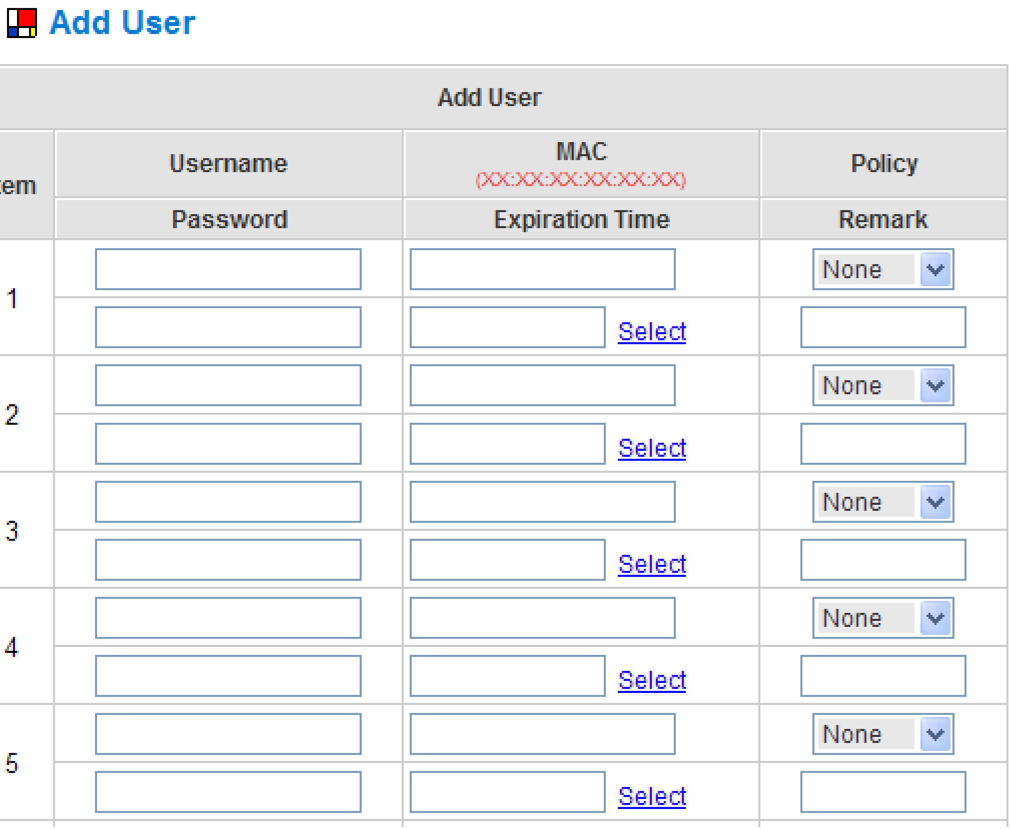


Local User Configuration

| Edit User | |
|---|---|
| Username | test * |
| Password | test * |
| MAC | |
| Policy | Policy A |
| Remark | |
| Expiration Time | // Select |

- **Edit Local User List:** Click this to enter the **"Local User List"** screen.

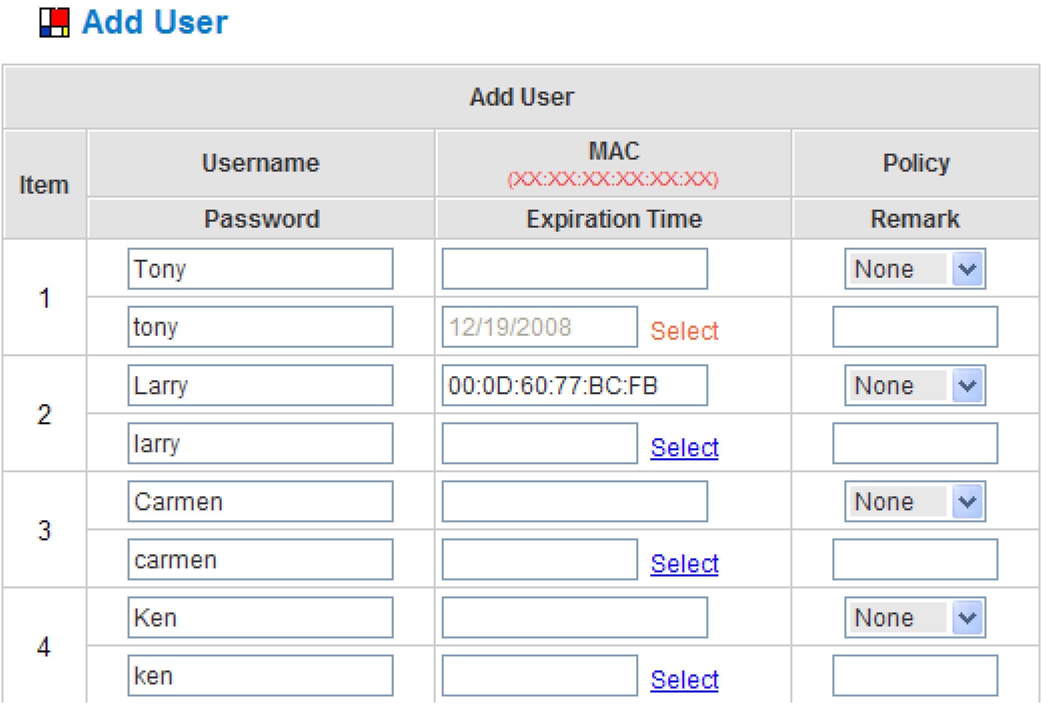
  **Add User:** Click the hyperlink of ***Add User*** to enter the **Add User** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC"** (optional) and **"Remark"** (optional). Then, select a desired **Policy** and click ***Apply*** to complete adding the user(s).



Add User

| Add User | | | |
|---|---|---|---|
| Item | Username | MAC<br>(XX:XX:XX:XX:XX:XX) | Policy |
| | Password | Expiration Time | Remark |
| 1 | | | None |
| | | Select | |
| 2 | | | None |
| | | Select | |
| 3 | | | None |
| | | Select | |
| 4 | | | None |
| | | Select | |
| 5 | | | None |
| | | Select | |

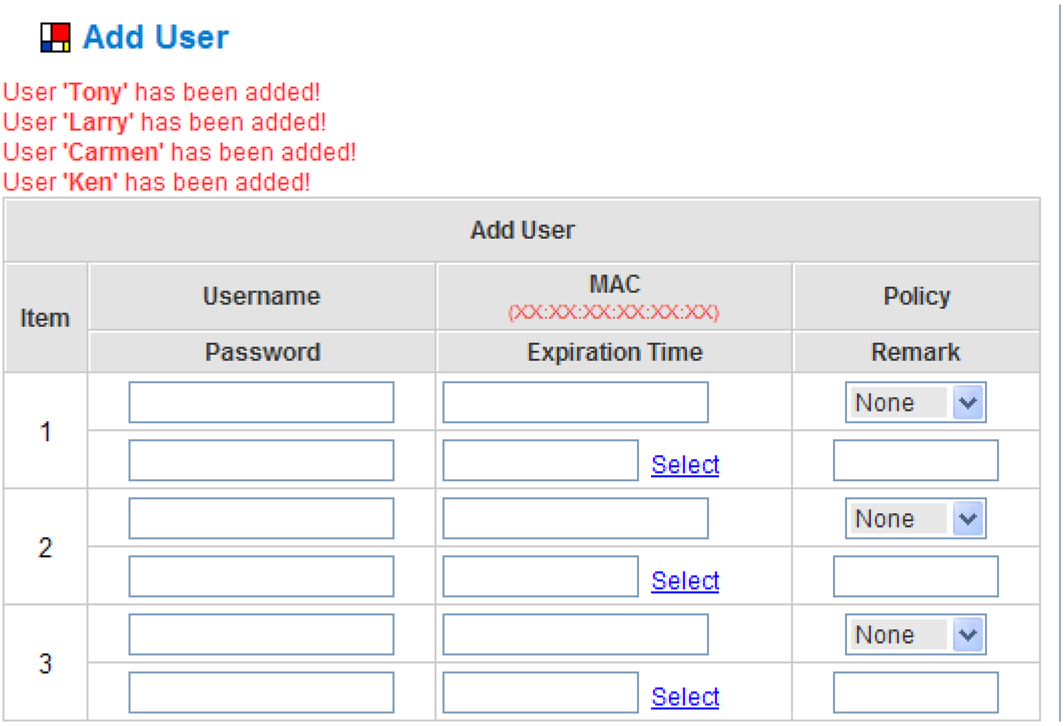
Add the user(s) and enter the necessary information.



Add User

| Add User | | | |
|---|---|---|---|
| Item | Username | MAC<br>(XX:XX:XX:XX:XX:XX) | Policy |
| | Password | Expiration Time | Remark |
| 1 | Tony | | None |
| | tony | 12/19/2008 Select | |
| 2 | Larry | 00:0D:60:77:BC:FB | None |
| | larry | Select | |
| 3 | Carmen | | None |
| | carmen | Select | |
| 4 | Ken | | None |
| | ken | Select | |

After adding the user(s) and all necessary information, click ***Apply***.

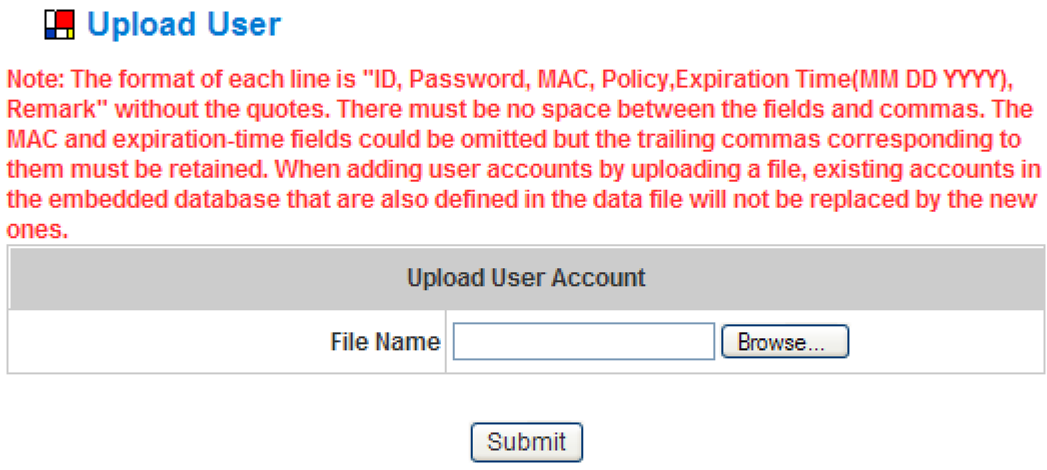


## Add User

User 'Tony' has been added!
User 'Larry' has been added!
User 'Carmen' has been added!
User 'Ken' has been added!

| Add User | | | |
|---|---|---|---|
| Item | Username | MAC<br>(XX:XX:XX:XX:XX:XX) | Policy |
| | Password | Expiration Time | Remark |
| 1 | | | None |
| | | Select | |
| 2 | | | None |
| | | Select | |
| 3 | | | None |
| | | Select | |

**Upload User:** Click this to enter the **Upload User** interface. Click the ***Browse*** button to select the text file for the user account upload. Then click ***Submit*** to complete the upload process.

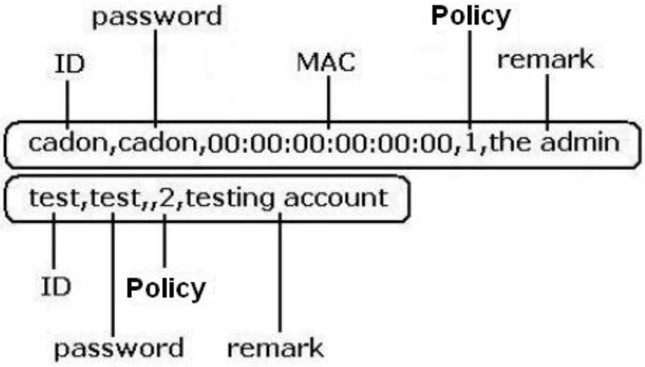


## Upload User

Note: The format of each line is "ID, Password, MAC, Policy,Expiration Time(MM DD YYYY), Remark" without the quotes. There must be no space between the fields and commas. The MAC and expiration-time fields could be omitted but the trailing commas corresponding to them must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.

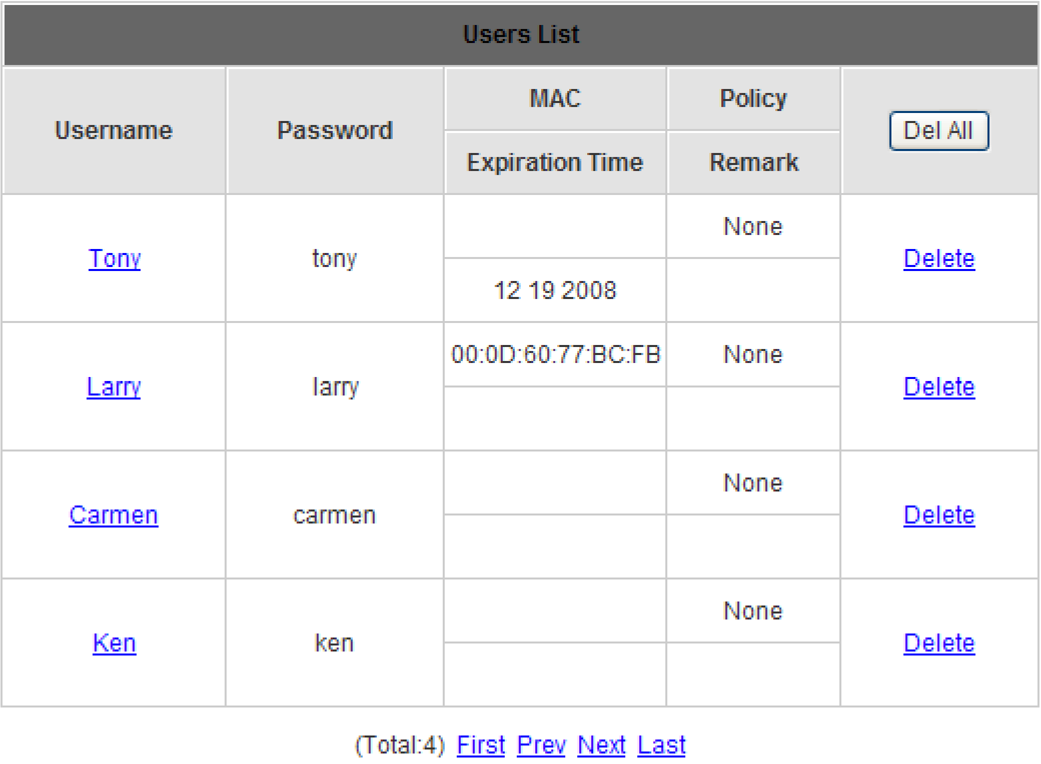
| Upload User Account | |
|---|---|
| File Name | Browse... |

The uploading file should be a text file and the format of each line is ***"ID, Password, MAC, Policy, Remark"*** without the quotes. There must be no spaces between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by new ones.



```
cadon,cadon,00:00:00:00:00:00,1,the admin
test,test,,2,testing account
```

**Download User:** Click this to enter the **Users List** page and the system will show a list of all created user accounts. Click ***Download*** to create a .txt file and then save it on disk.

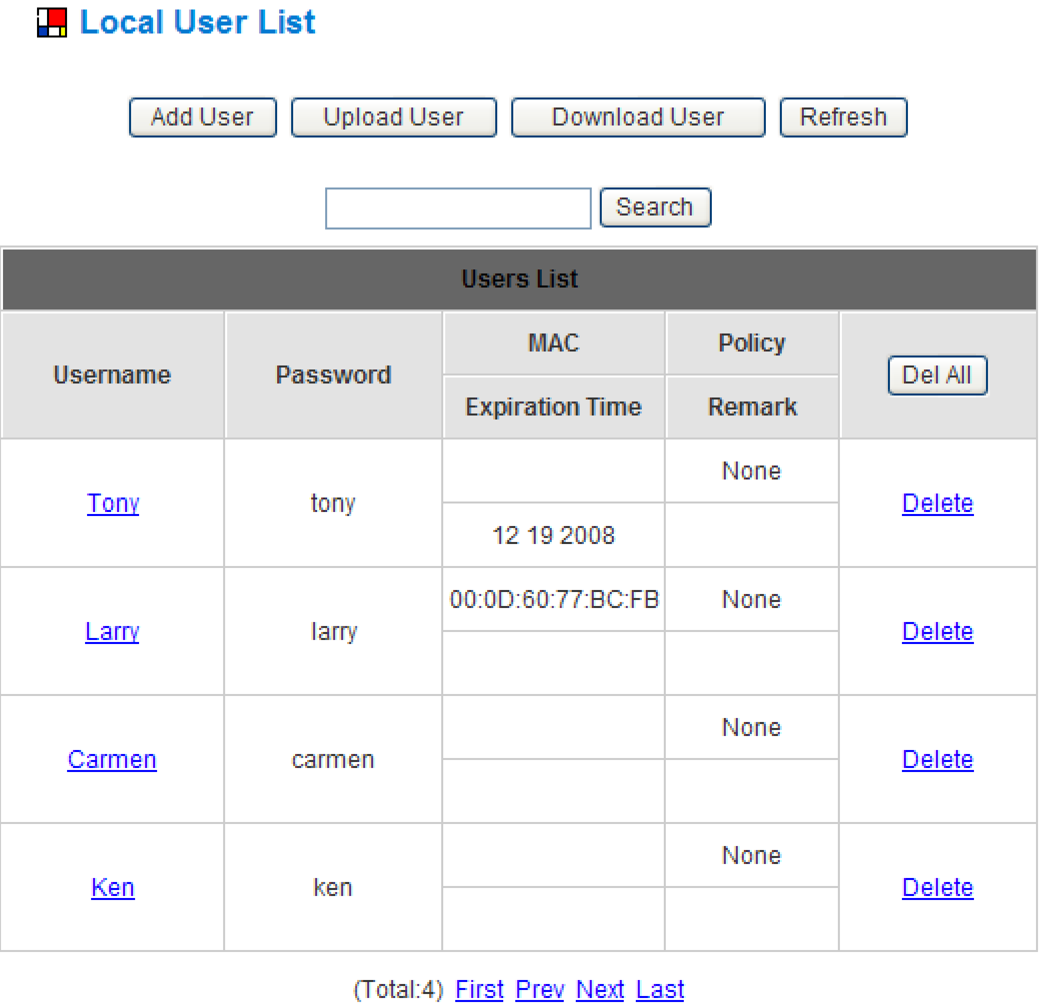


Users List

| Username | Password | MAC | Policy | Del All |
|---|---|---|---|---|
| | | Expiration Time | Remark | |
| Tony | tony | | None | Delete |
| | | 12 19 2008 | | |
| Larry | larry | 00:0D:60:77:BC:FB | None | Delete |
| | | | | |
| Carmen | carmen | | None | Delete |
| | | | | |
| Ken | ken | | None | Delete |
| | | | | |

(Total:4) First Prev Next Last

**Refresh:** Click ***Refresh*** to renew the user list.



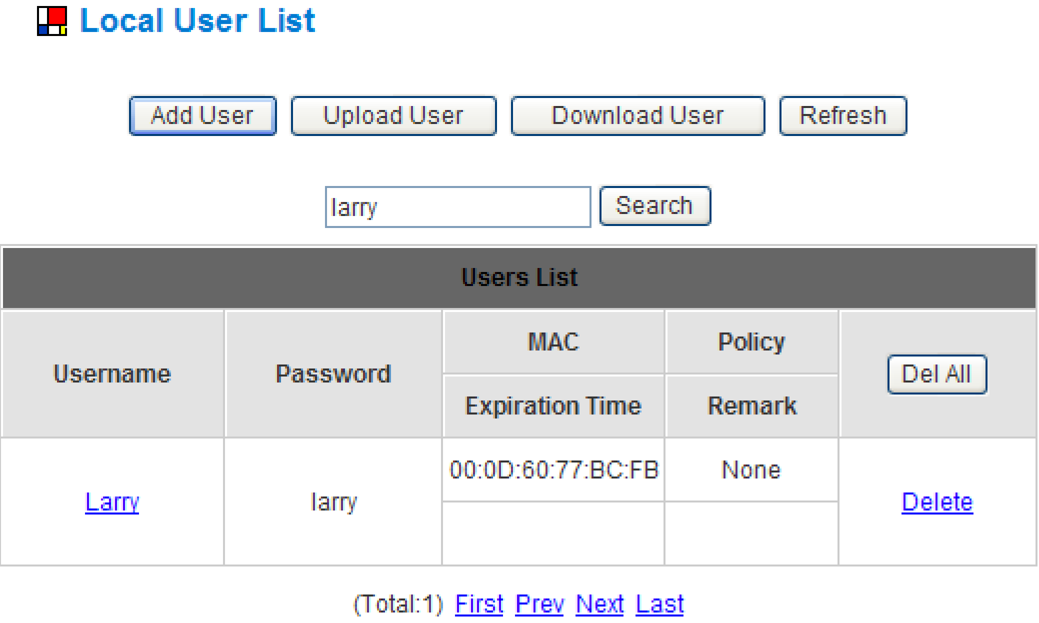
Local User List

Users List

| Username | Password | MAC | Policy | Del All |
|---|---|---|---|---|
| | | Expiration Time | Remark | |
| Tony | tony | | None | Delete |
| | | 12 19 2008 | | |
| Larry | larry | 00:0D:60:77:BC:FB | None | Delete |
| | | | | |
| Carmen | carmen | | None | Delete |
| | | | | |
| Ken | ken | | None | Delete |
| | | | | |

(Total:4) First Prev Next Last

**Search:** Enter a keyword of a username to be searched in the text field and click the ***Search*** button to perform the search. All usernames matching the keyword will be listed.


Local User List

larry

Users List

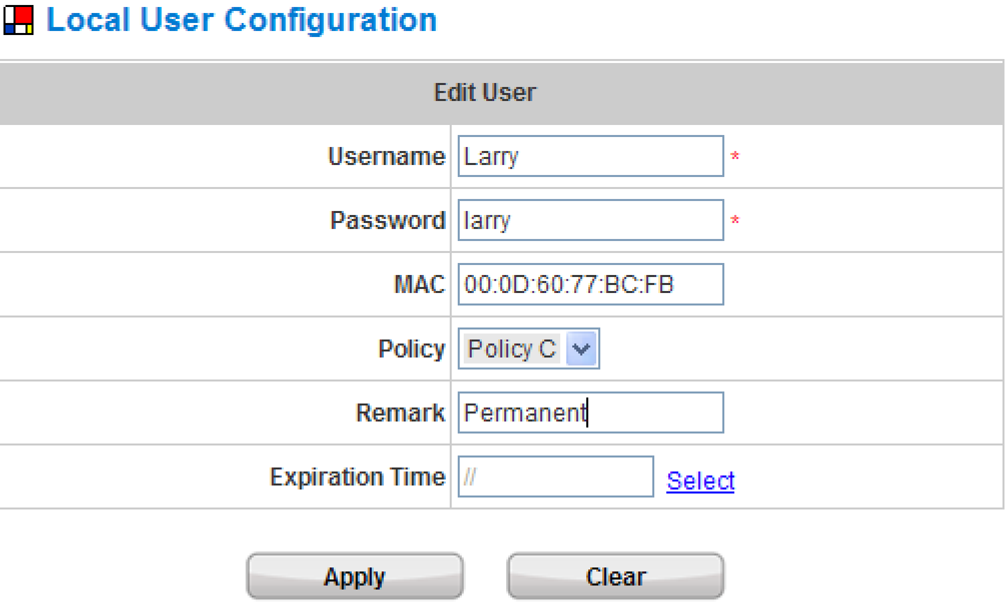
| Username | Password | MAC | Policy | Del All |
|---|---|---|---|---|
| | | Expiration Time | Remark | |
| Larry | larry | 00:0D:60:77:BC:FB | None | Delete |
| | | | | |

(Total:1) First Prev Next Last

**Del All:** This will delete all the users at once.

**Delete:** This will delete the user(s) one by one.

**Edit User:** If editing the content of any individual user account is desired, click the username of that desired user account to enter its **Edit User** Interface, and then modify or add any desired information such as **"Username"**, **"Password"**, **"MAC"** (optional) and **"Remark"** (optional). Then, click ***Apply*** to complete the modification.

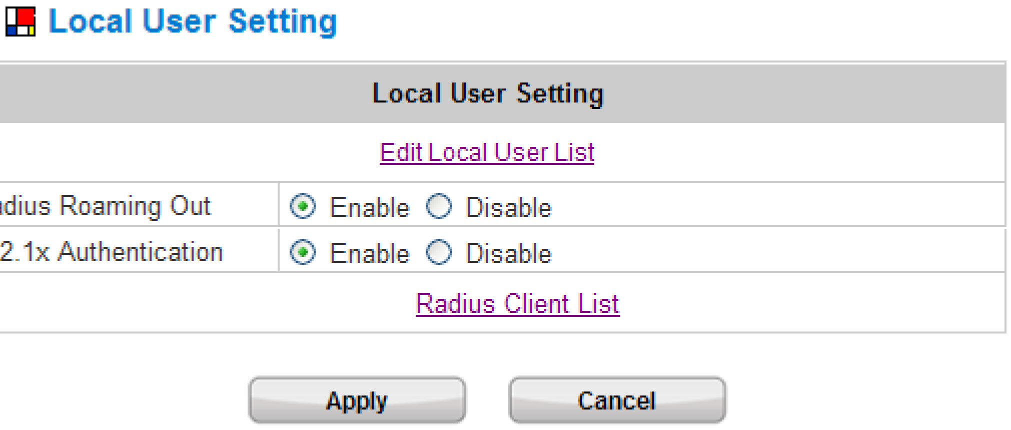

Local User Configuration

Edit User

| | |
|---|---|
| Username | Larry * |
| Password | larry * |
| MAC | 00:0D:60:77:BC:FB |
| Policy | Policy C |
| Remark | Permanent |
| Expiration Time | // Select |

***B. Radius Client Setting***

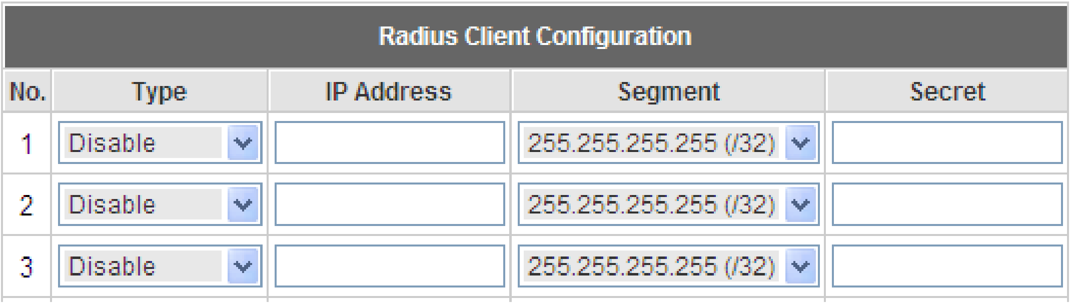
Click the hyperlink of ***Radius Client Setting*** for further configuration.



Local User Setting

| Local User Setting | |
|---|---|
| Edit Local User List | |
| Radius Roaming Out | ● Enable ○ Disable |
| 802.1x Authentication | ● Enable ○ Disable |
| Radius Client List | |

⇩



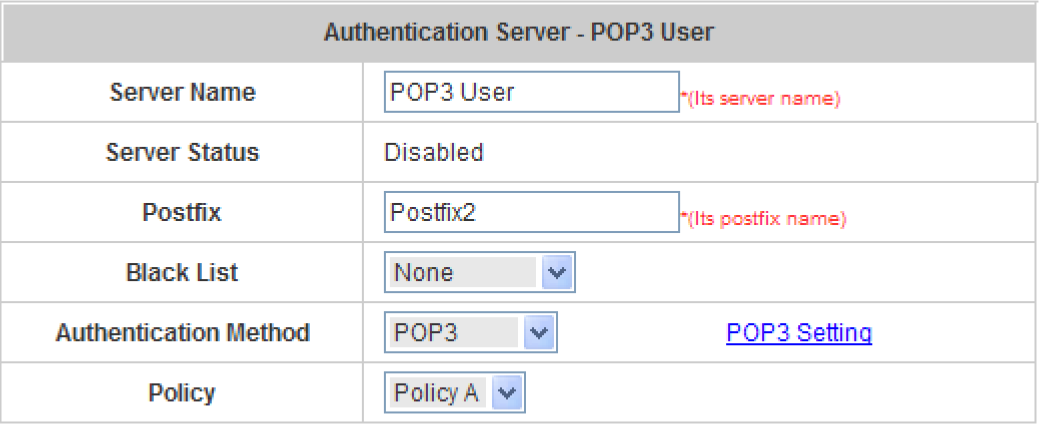
Radius Client Configuration

| No. | Type | IP Address | Segment | Secret |
|---|---|---|---|---|
| 1 | Disable | | 255.255.255.255 (/32) | |
| 2 | Disable | | 255.255.255.255 (/32) | |
| 3 | Disable | | 255.255.255.255 (/32) | |

**802.1X Authentication:** Enable this function and the hyperlink of **Radius Client List** will appear. Click the hyperlink of ***Radius Client List*** to get into the RADIUS Client Configuration list for further configuration. In the **Radius Client Configuration** table, depending on the Type to be selected (either Roaming Out or 802.1x), the client's IP address will be either another NAC's IP address (Roaming Out) or wireless AP/802.1x switch's IP addess (802.1x). The system will handle the authentication request from these clients accordingly.

### Authentication Method – POP3

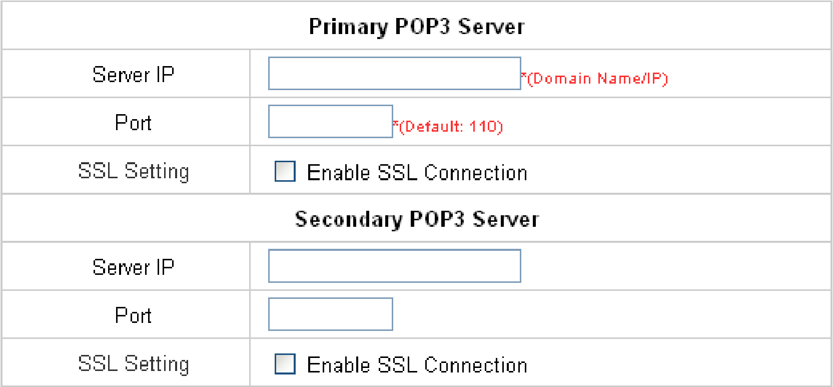
Choose **"POP3"** from the **Authentication Method** field, the hyperlink beside the pull-down menu will become **"POP3 Setting"**.



| Authentication Server - POP3 User | |
|---|---|
| Server Name | POP3 User *(Its server name) |
| Server Status | Disabled |
| Postfix | Postfix2 *(Its postfix name) |
| Black List | None |
| Authentication Method | POP3 POP3 Setting |
| Policy | Policy A |

Click the hyperlink of ***POP3 Setting*** for further configuration. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The fields with red asterisk are necessary information.

These settings will become effective immediately after clicking the ***Apply*** button.

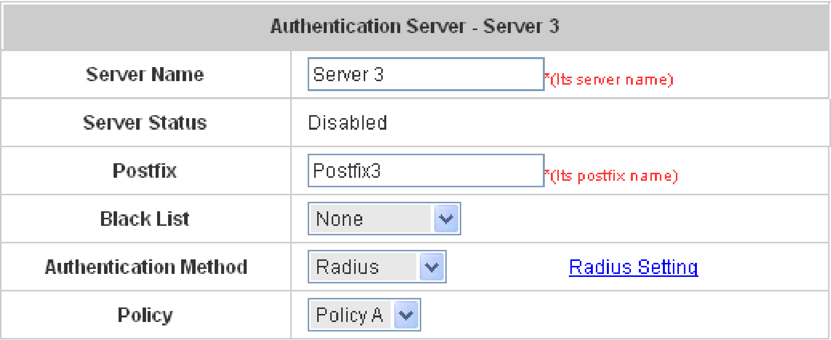


| | |
|---|---|
| **Primary POP3 Server** | |
| Server IP | *(Domain Name/IP) |
| Port | *(Default: 110) |
| SSL Setting | □ Enable SSL Connection |
| **Secondary POP3 Server** | |
| Server IP | |
| Port | |
| SSL Setting | □ Enable SSL Connection |

- **Server IP:** Enter the IP address/domain name given by your ISP.
- **Port:** Enter the Port. The default value is 100.
- **Enable SSL Connection:** If this option is enabled, the POP3 protocol will perform the authentication.

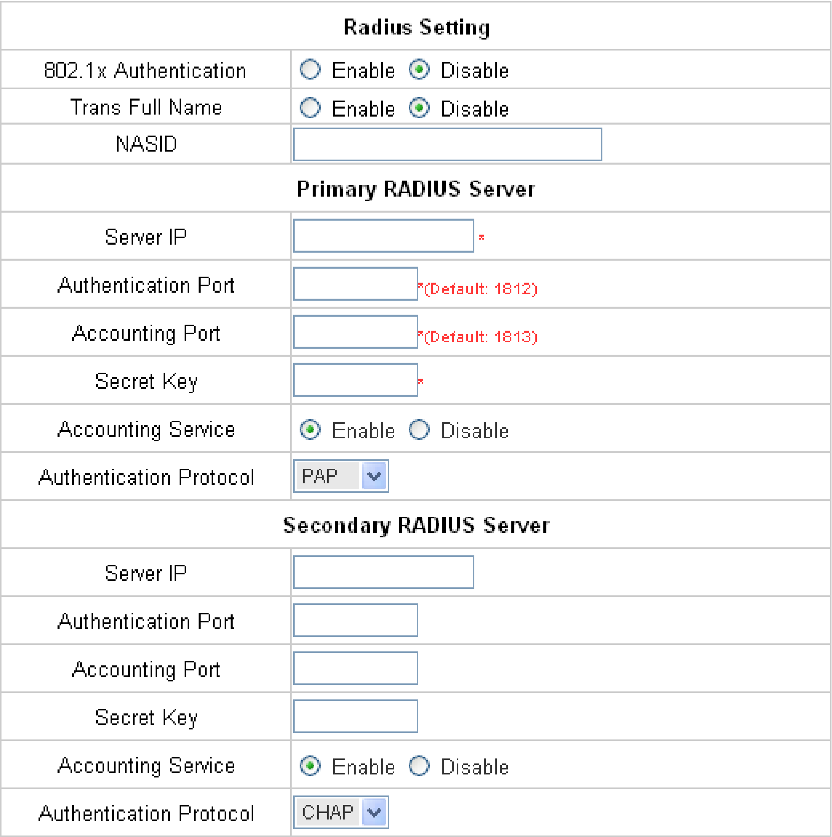
### Authentication Method – RADIUS

Choose **"RADIUS"** from the **Authentication Method** field, the hyperlink beside the pull-down menu will become **"Radius Setting"**.



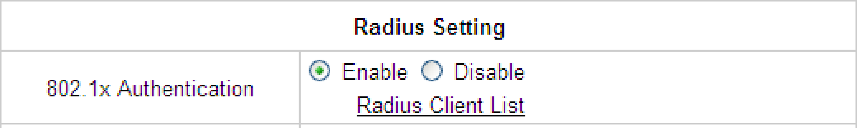
| Authentication Server - Server 3 | |
|---|---|
| Server Name | Server 3 *(Its server name) |
| Server Status | Disabled |
| Postfix | Postfix3 *(Its postfix name) |
| Black List | None |
| Authentication Method | Radius — Radius Setting |
| Policy | Policy A |

Click the hyperlink of ***Radius Setting*** for further configuration. The RADIUS server sets the external authentication for user accounts. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The fields with red asterisk are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.

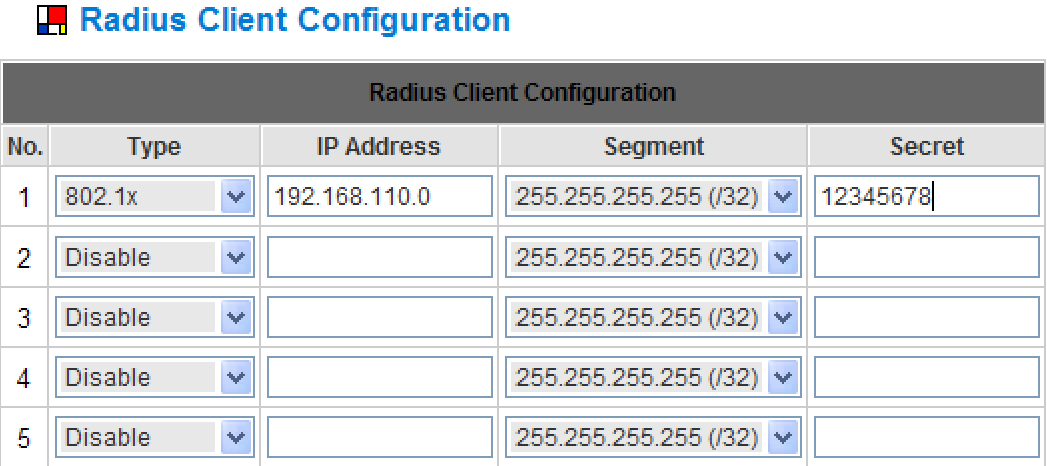


| Radius Setting | |
|---|---|
| 802.1x Authentication | ○ Enable ● Disable |
| Trans Full Name | ○ Enable ● Disable |
| NASID | |
| **Primary RADIUS Server** | |
| Server IP | * |
| Authentication Port | *(Default: 1812) |
| Accounting Port | *(Default: 1813) |
| Secret Key | * |
| Accounting Service | ● Enable ○ Disable |
| Authentication Protocol | PAP |
| **Secondary RADIUS Server** | |
| Server IP | |
| Authentication Port | |
| Accounting Port | |
| Secret Key | |
| Accounting Service | ● Enable ○ Disable |
| Authentication Protocol | CHAP |

- **802.1X Authentication:** Enable this function and the hyperlink of **Radius Client List** will appear. Click the hyperlink of ***Radius Client List*** to get into the RADIUS Client Configuration list for further configuration. In the **Radius Client Configuration** table, depending on the Type to be selected (either Roaming Out or 802.1x), the client's IP address will be either another NAC's IP address (Roaming Out) or wireless AP/802.1x switch's IP addess (802.1x). The system will handle the authentication request from these clients accordingly.



| Radius Setting | |
|---|---|
| 802.1x Authentication | ● Enable ○ Disable<br>Radius Client List |



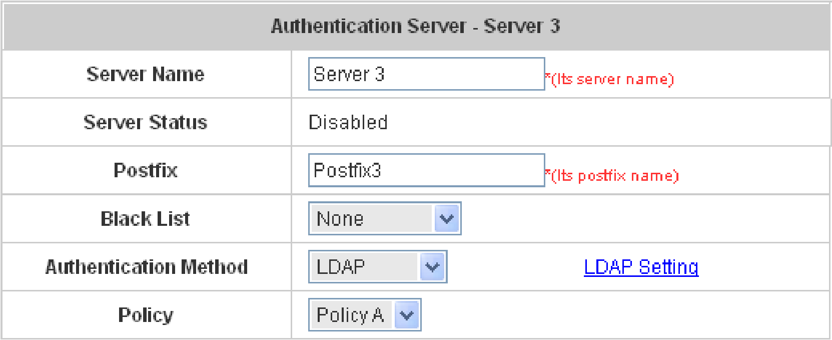
Radius Client Configuration

| No. | Type | IP Address | Segment | Secret |
|---|---|---|---|---|
| 1 | 802.1x | 192.168.110.0 | 255.255.255.255 (/32) | 12345678 |
| 2 | Disable | | 255.255.255.255 (/32) | |
| 3 | Disable | | 255.255.255.255 (/32) | |
| 4 | Disable | | 255.255.255.255 (/32) | |
| 5 | Disable | | 255.255.255.255 (/32) | |

- **Trans Full Name:** When enabled, the ID and postfix will be transferred to the RADIUS server for authentication. When disabled, only the ID will be transferred to the RADIUS server for authentication.
- **NASID:** Enter the NASID of HS1100 for the external RADIUS authentication server.
- **Server IP:** Enter the IP address/domain name of the RADIUS server.
- **Authentication Port:** Enter the authentication port for the RADIUS server and the default value is 1812.
- **Accounting Port:** Enter the accounting port for the RADIUS server and the default value is 1813.
- **Secret Key:** Enter the key for encryption and decryption.
- **Accounting Service:** Select this to enable or disable the **"Accounting Service"** for accounting capabilities.
- **Authentication Protocol:** There are two methods, CHAP and PAP for selection.

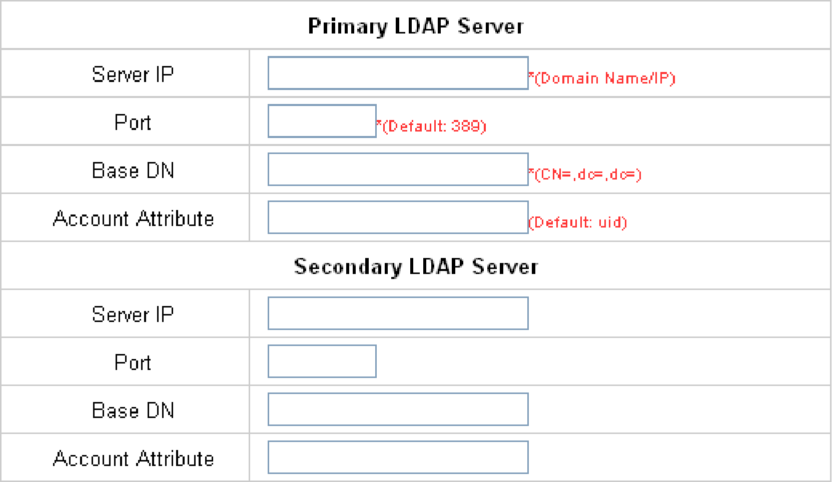
### Authentication Method – LDAP

Choose **“LDAP”** from the **Authentication Method** field, the hyperlink beside the pull-down menu will become **“LDAP Setting”**.



| Authentication Server - Server 3 | |
|---|---|
| Server Name | Server 3 *(Its server name) |
| Server Status | Disabled |
| Postfix | Postfix3 *(Its postfix name) |
| Black List | None |
| Authentication Method | LDAP LDAP Setting |
| Policy | Policy A |

Click the hyperlink of ***LDAP Setting*** for further configuration. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red asterisk are necessary information which should be filled in. These settings will become effective immediately after clicking the ***Apply*** button.

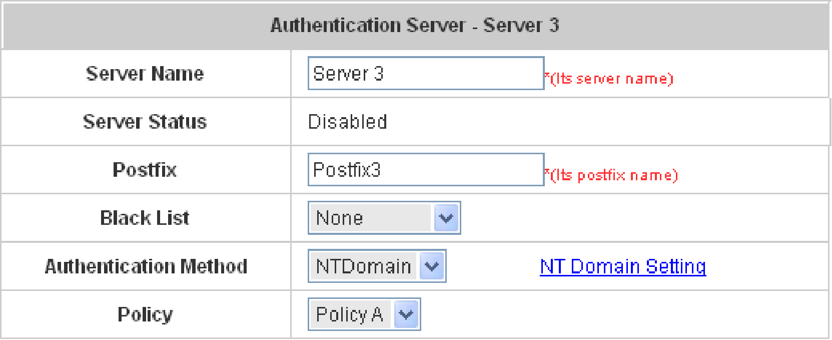


| Primary LDAP Server | |
|---|---|
| Server IP | *(Domain Name/IP) |
| Port | *(Default: 389) |
| Base DN | *(CN=,dc=,dc=) |
| Account Attribute | (Default: uid) |
| **Secondary LDAP Server** | |
| Server IP | |
| Port | |
| Base DN | |
| Account Attribute | |

- **Server IP:** Enter the IP address or domain name of the LDAP server.
- **Port:** Enter the Port for the LDAP server, and the default value is 389.
- **Base DN:** Enter the distinguished name for the LDAP server.
- **Account Attribute:** Enter the account attribute of the LDAP server.

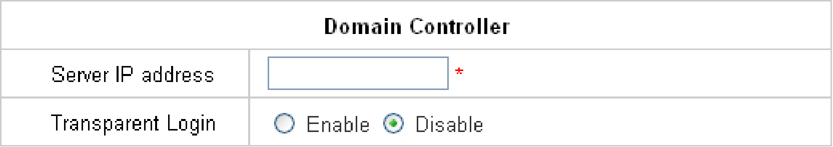
### Authentication Method – NTDomain

Choose **“NTDomain”** from the **Authentication Method** field, the hyperlink beside the pull-down menu will become **“NT Domain Setting”**.



| Authentication Server - Server 3 | |
|---|---|
| Server Name | Server 3 *(Its server name) |
| Server Status | Disabled |
| Postfix | Postfix3 *(Its postfix name) |
| Black List | None |
| Authentication Method | NTDomain NT Domain Setting |
| Policy | Policy A |

Click the hyperlink of ***NT Domain Setting*** for further configuration. Enter the server IP address and enable/disable the transparent login function. These settings will become effective immediately after clicking the ***Apply*** button.

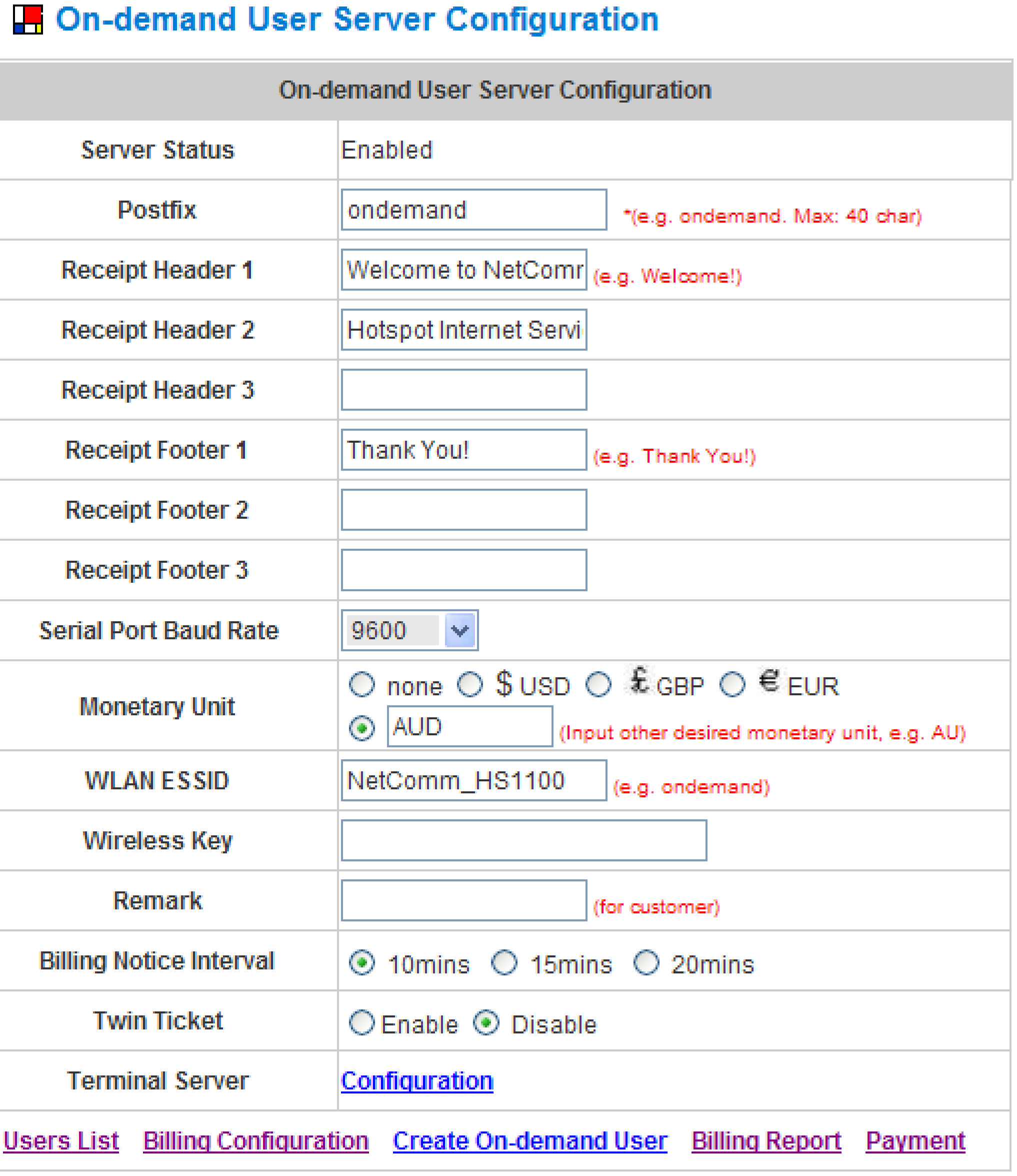


| Domain Controller | |
|---|---|
| Server IP address | * |
| Transparent Login | ○ Enable ● Disable |

- **Server IP address:** Enter the server IP address of the domain controller.
- **Transparent Login:** If the function is enabled, users will log into HS1100 automatically when they log into the Windows domain.

### Authentication Method – On-demand User

**On-demand User Server Configuration:** The administrator can enable and configure this authentication method to create on-demand user accounts. This function is designed for hotspot owners to provide temporary users with free or paid wireless Internet access in the hotspot environment. Major functions include accounts creation, users monitoring list, billing plan, billing report statistics, and external payment gateway support.



On-demand User Server Configuration

| On-demand User Server Configuration | |
|---|---|
| Server Status | Enabled |
| Postfix | ondemand *(e.g. ondemand. Max: 40 char) |
| Receipt Header 1 | Welcome to NetComr (e.g. Welcome!) |
| Receipt Header 2 | Hotspot Internet Servi |
| Receipt Header 3 | |
| Receipt Footer 1 | Thank You! (e.g. Thank You!) |
| Receipt Footer 2 | |
| Receipt Footer 3 | |
| Serial Port Baud Rate | 9600 |
| Monetary Unit | ○ none ○ $ USD ○ £ GBP ○ € EUR<br>● AUD (Input other desired monetary unit, e.g. AU) |
| WLAN ESSID | NetComm_HS1100 (e.g. ondemand) |
| Wireless Key | |
| Remark | (for customer) |
| Billing Notice Interval | ● 10mins ○ 15mins ○ 20mins |
| Twin Ticket | ○ Enable ● Disable |
| Terminal Server | Configuration |

Users List  Billing Configuration  Create On-demand User  Billing Report  Payment

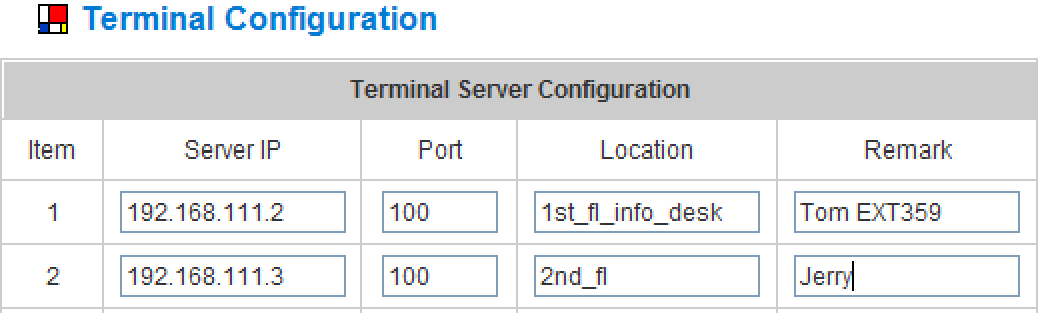
- **Server Status:** The status shows that the server is enabled or disabled.
- **Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.
- **Receipt Header 1~3:** Enter the receipt header message or use the default. When the administrator creates an On-demand User account, he/she can print out a receipt containing this On-demand User's information such as Username and Password.
- **Receipt Footer 1~3:** Enter the receipt footer message or use the default.
- **Serial Port Baud Rate:** Select the desired transmission baud rate. The default value is 9600.
- **Monetary Unit:** Select the desired monetary unit.
- **WLAN ESSID:** Enter the ESSID of the access point. The administrator can supply a new name or use the

default

- **Wireless Key:** Enter the Wireless key of the access point such as WEP or WPA.
- **Remark:** Enter any additional information that will appear at the bottom of the receipt.
- **Billing Notice Interval:** While the on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval defined here.
- **Twin Ticket:** Enable this function to print duplicate receipts.
- **Terminal Server**

  Terminal Configuration is a list of serial devices that communicate with the system only; never get online and no need to go through authentication.

  For customers making purchase at the front desk in a hotel, a receptionist uses an account generator (192.168.111.2) to create a guest account and print out receipts with account information. A client in the other floor can print the same receipt without going to the front desk on the lobby by using the second floor account generator (192.168.111.3). Both account generators work for the system on LAN side.



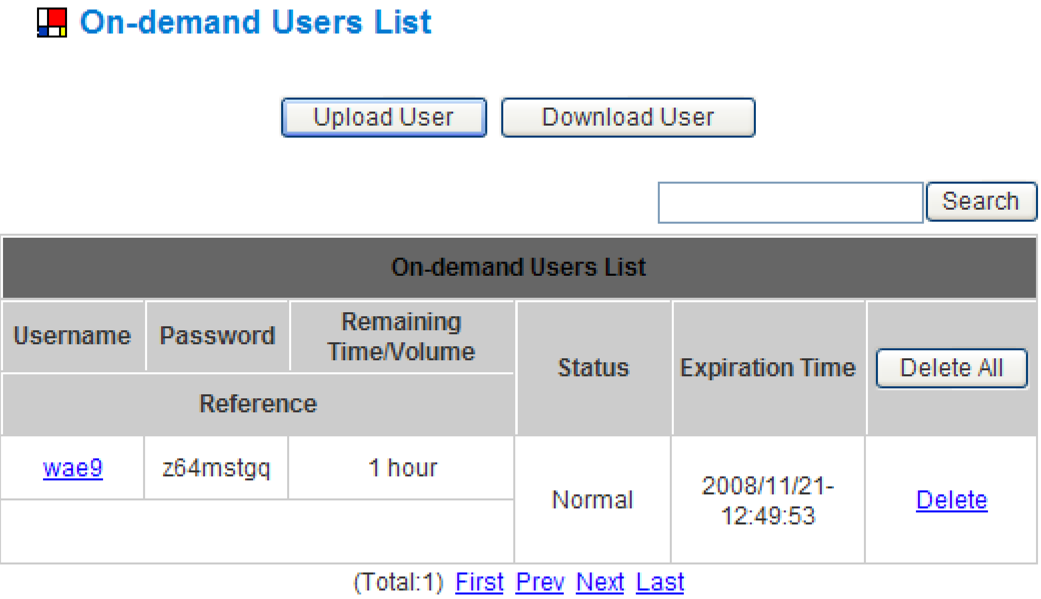
Terminal Configuration

Terminal Server Configuration

| Item | Server IP | Port | Location | Remark |
|---|---|---|---|---|
| 1 | 192.168.111.2 | 100 | 1st_fl_info_desk | Tom EXT359 |
| 2 | 192.168.111.3 | 100 | 2nd_fl | Jerry |

- ➢ **Server IP:** IP address of serial or converter devices.
- ➢ **Server Port:** Port number of serial or converter devices.
- ➢ **Location:** It will be displayed in on-demand users' log.
- ➢ **Remark:** it will be shown only here.

- **Users List:** Click to enter the **On-demand Users List** page. In the **On-demand Users List**, detailed information will be documented here. By default, the on-demand user database is empty.

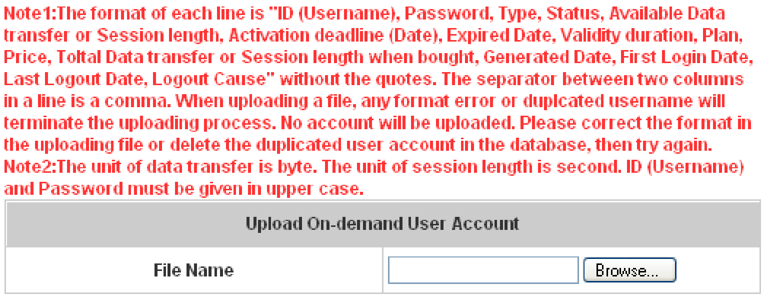


| On-demand Users List | | | | | |
|---|---|---|---|---|---|
| Username | Password | Remaining Time/Volume | Status | Expiration Time | Delete All |
| Reference | | | | | |
| wae9 | z64mstgq | 1 hour | Normal | 2008/11/21-<br>12:49:53 | Delete |

(Total:1) First Prev Next Last

- ➢ **Search:** Enter a keyword of a username which needs to be searched in the text field and click the ***Search*** button to perform the search. All usernames matching the keyword will be listed.
- ➢ **Username:** The login name of the on-demand user.
- ➢ **Password:** The login password of the on-demand user.
- ➢ **Remaining Time/Volume:** The total time/volume that the user can use currently.
- ➢ **Status:** The status of the account. **"Normal"** indicates that the account is not in-use and not overdue. **"Online"** indicates that the account is in-use and not overdue. **"Expire"** indicates that the account is overdue and cannot be used.
- ➢ **Expiration Time:** The expiration time of the account.
- ➢ **Del All:** Delete all the users at once.
- ➢ **Delete:** Delete the users one by one.

- **Upload User:** Click this to enter the **Upload User** interface. Click the ***Browse*** button to select the text file for the user account upload. Then click ***Submit*** to complete the upload process.



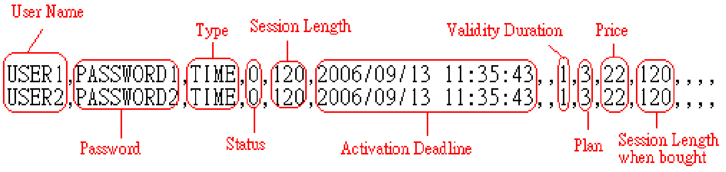
Note1:The format of each line is "ID (Username), Password, Type, Status, Available Data transfer or Session length, Activation deadline (Date), Expired Date, Validity duration, Plan, Price, Toltal Data transfer or Session length when bought, Generated Date, First Login Date, Last Logout Date, Logout Cause" without the quotes. The separator between two columns in a line is a comma. When uploading a file, any format error or duplcated username will terminate the uploading process. No account will be uploaded. Please correct the format in the uploading file or delete the duplicated user account in the database, then try again.
Note2:The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.

| Upload On-demand User Account | |
|---|---|
| File Name | Browse... |

The uploading file should be a text file and the format of each line is ***" ID (USERNAME), PASSWORD, Type, Status, Available Data Transfer or Session Length, Activation Deadline (Date), Expired Date, Validity Duration, Plan, Price, Total Data Transfer or Session Length when bought, Generated Date, First Login Date, Last Logout Date, Logout Cause"*** without the quotes. The separator between two columns in a line is a comma. When uploading a file, any format error or duplicated username will terminate the uploading process and no account will be uploaded. Please correct the format in the uploading file or delete the duplicated user account in the database, and then, try again. The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.

**>> Example 1: For Session Length type**

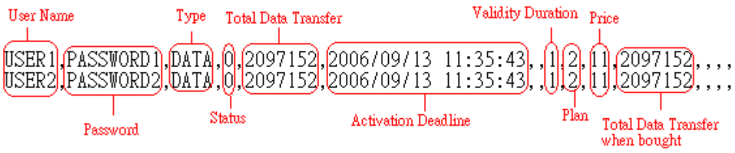
***Type*** must be written as **"TIME,"** and ***Status*** must be set as **"0"**. Set ***Session Length*** in seconds. ***Activation Deadline*** must be in the format of "yyyy/mm/dd hh:mm:ss". Set ***Validity Duration*** as **"1"**, and give a ***Plan*** that's already been generated and enabled from **Billing Configuration** page. Provide a price in any monetary unit defined in **On-demand User Server Configuration** page. Finally, set ***Session Length when bought*** the same as ***Session Length***. Leave other fields blank.



```
USER1,PASSWORD1,TIME,0,120,2006/09/13 11:35:43,,1,3,22,120,,,,
USER2,PASSWORD2,TIME,0,120,2006/09/13 11:35:43,,1,3,22,120,,,,
```

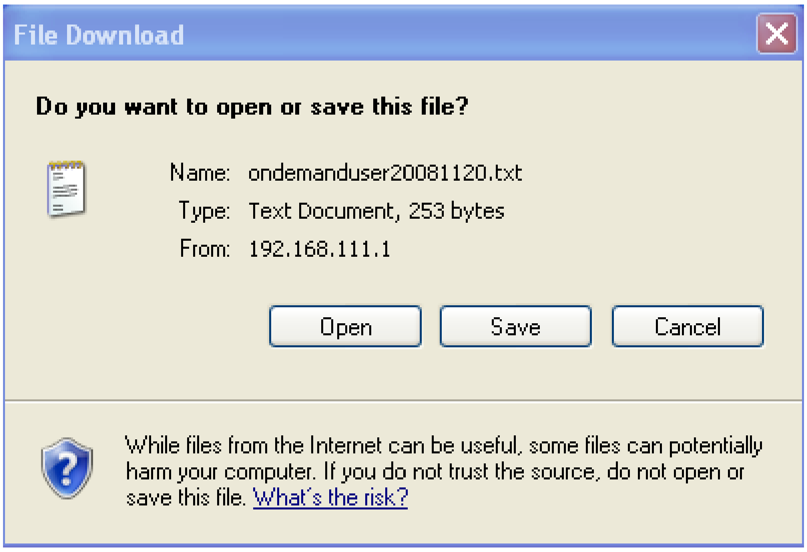
**>> Example 2: For Total Data Transfer type**

***Type*** must be written as **"DATA,"** and ***Status*** must be set as **"0"**. Set ***Total Data Transfer*** in bytes. ***Activation Deadline*** must be in the format of "yyyy/mm/dd hh:mm:ss". Set ***Validity Duration*** as **"1"**, and give a ***Plan*** that's already been generated and enabled from **Billing Configuration** page. Provide a price in any monetary unit defined in **On-demand User Server Configuration** page. Finally, set ***Total Data Transfer when bought*** the same as ***Session Length***. Leave other fields blank.



```
USER1,PASSWORD1,DATA,0,2097152,2006/09/13 11:35:43,,1,2,11,2097152,,,,
USER2,PASSWORD2,DATA,0,2097152,2006/09/13 11:35:43,,1,2,11,2097152,,,,
```

- **Download User:** Click this to create a .txt file and then save it on disk.



File Download

Do you want to open or save this file?

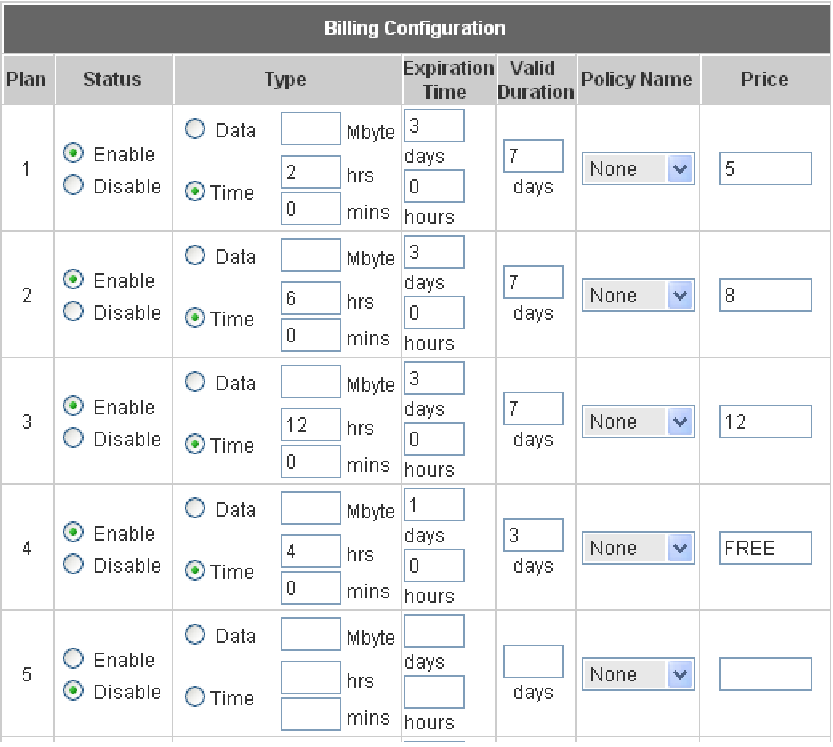
Name: ondemanduser20081120.txt

Type: Text Document, 253 bytes

From: 192.168.111.1

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

- **Billing Configuration:** The administrator can configure up to 10 billing plans.

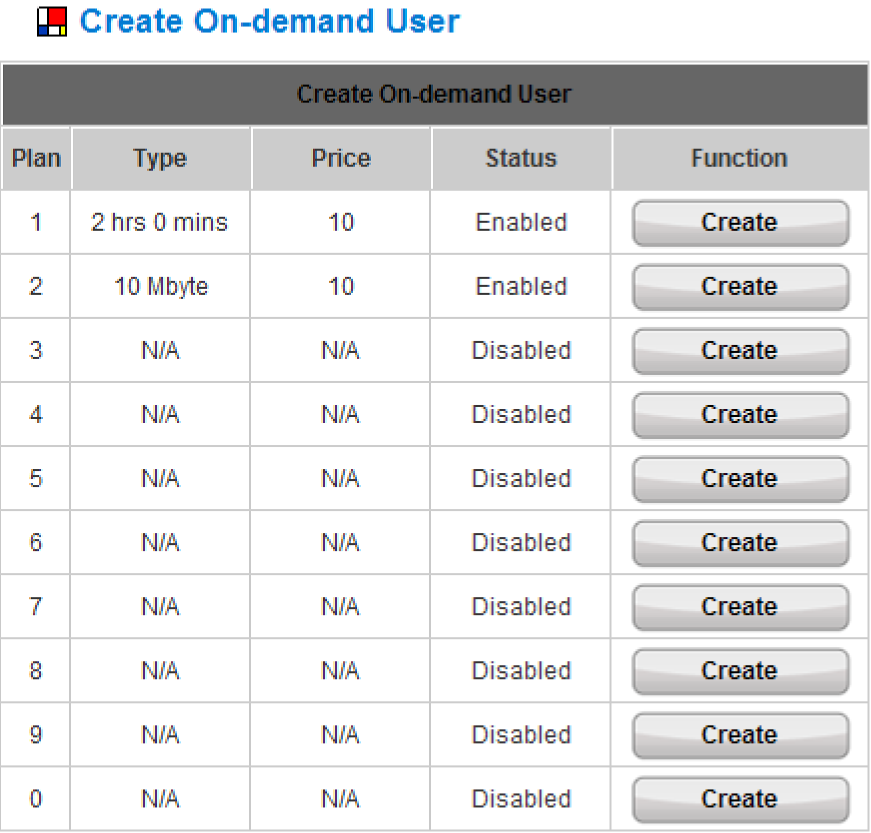


Billing Configuration

| Plan | Status | Type | Expiration Time | Valid Duration | Policy Name | Price |
|---|---|---|---|---|---|---|
| 1 | ● Enable<br>○ Disable | ○ Data [ ] Mbyte<br>● Time [2] hrs [0] mins | [3] days<br>[0] hours | [7] days | None | 5 |
| 2 | ● Enable<br>○ Disable | ○ Data [ ] Mbyte<br>● Time [6] hrs [0] mins | [3] days<br>[0] hours | [7] days | None | 8 |
| 3 | ● Enable<br>○ Disable | ○ Data [ ] Mbyte<br>● Time [12] hrs [0] mins | [3] days<br>[0] hours | [7] days | None | 12 |
| 4 | ● Enable<br>○ Disable | ○ Data [ ] Mbyte<br>● Time [4] hrs [0] mins | [1] days<br>[0] hours | [3] days | None | FREE |
| 5 | ○ Enable<br>● Disable | ○ Data [ ] Mbyte<br>○ Time [ ] hrs [ ] mins | [ ] days<br>[ ] hours | [ ] days | None | |

- **Status:** Select to enable or disable this billing plan.
- **Type:** Set the billing plan by **"Data"** (the maximum volume allowed is 9,999,999 Mbyte) or **"Time"** (the maximum days allowed is 999 days).
- **Expiration time:** This is the duration of time that the account must be activated after generating the account. After this duration, the account will self-expire
- **Valid Duration:** This is the duration of time that the user can use the Internet after activating the account. After this duration, the account will self-expire.
- **Policy Name:** Select policy to be applied upon login when user purchases this billing plan.
- **Price:** The price charged for this billing plan.

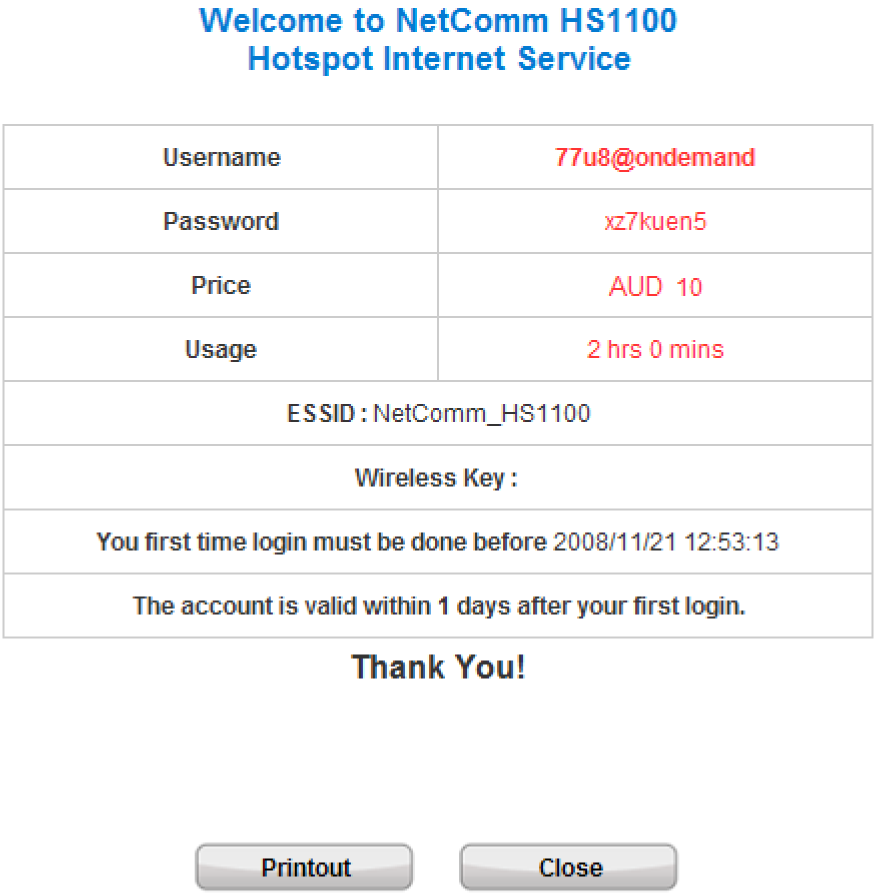
- **Create On-demand User:** The administrator can create on-demand user accounts.



Create On-demand User

| Plan | Type | Price | Status | Function |
|---|---|---|---|---|
| 1 | 2 hrs 0 mins | 10 | Enabled | Create |
| 2 | 10 Mbyte | 10 | Enabled | Create |
| 3 | N/A | N/A | Disabled | Create |
| 4 | N/A | N/A | Disabled | Create |
| 5 | N/A | N/A | Disabled | Create |
| 6 | N/A | N/A | Disabled | Create |
| 7 | N/A | N/A | Disabled | Create |
| 8 | N/A | N/A | Disabled | Create |
| 9 | N/A | N/A | Disabled | Create |
| 0 | N/A | N/A | Disabled | Create |

Click the ***Create*** button for the desired plan, an On-demand User account will be created. Then, click ***Printout*** to print a receipt containing this On-demand User's information.

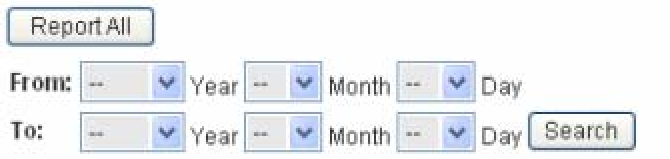


Welcome to NetComm HS1100
Hotspot Internet Service

| | |
|---|---|
| Username | 77u8@ondemand |
| Password | xz7kuen5 |
| Price | AUD 10 |
| Usage | 2 hrs 0 mins |
| ESSID : NetComm_HS1100 | |
| Wireless Key : | |
| You first time login must be done before 2008/11/21 12:53:13 | |
| The account is valid within 1 days after your first login. | |

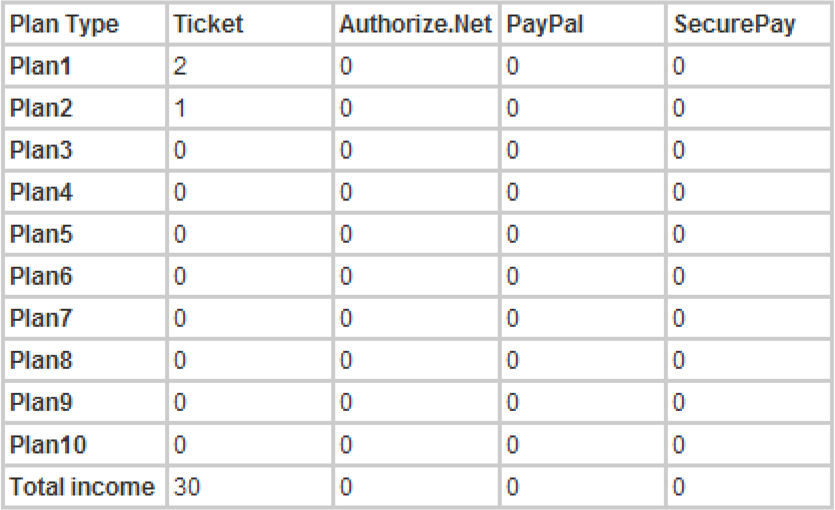
Thank You!

- **Billing Report:** The administrator can get a complete report or a report for a particular period.

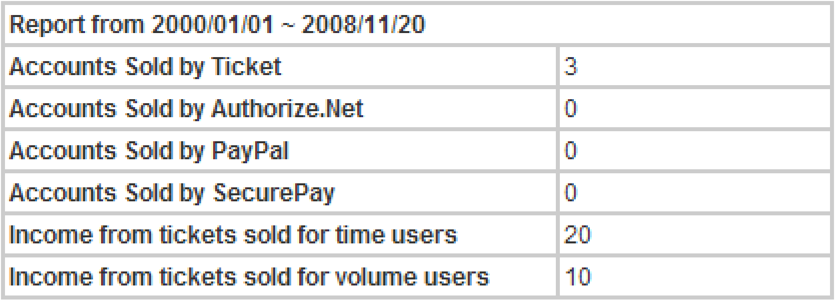


- **Report All:** Click to get a complete report including all the on-demand records. This report shows the total income as well as the individual accounting record of each plan for all plans available.

- **Search:** Select a time period to get a period report. This report shows the total income as well as the individual accounting record of each plan for all plans available for that period of time.

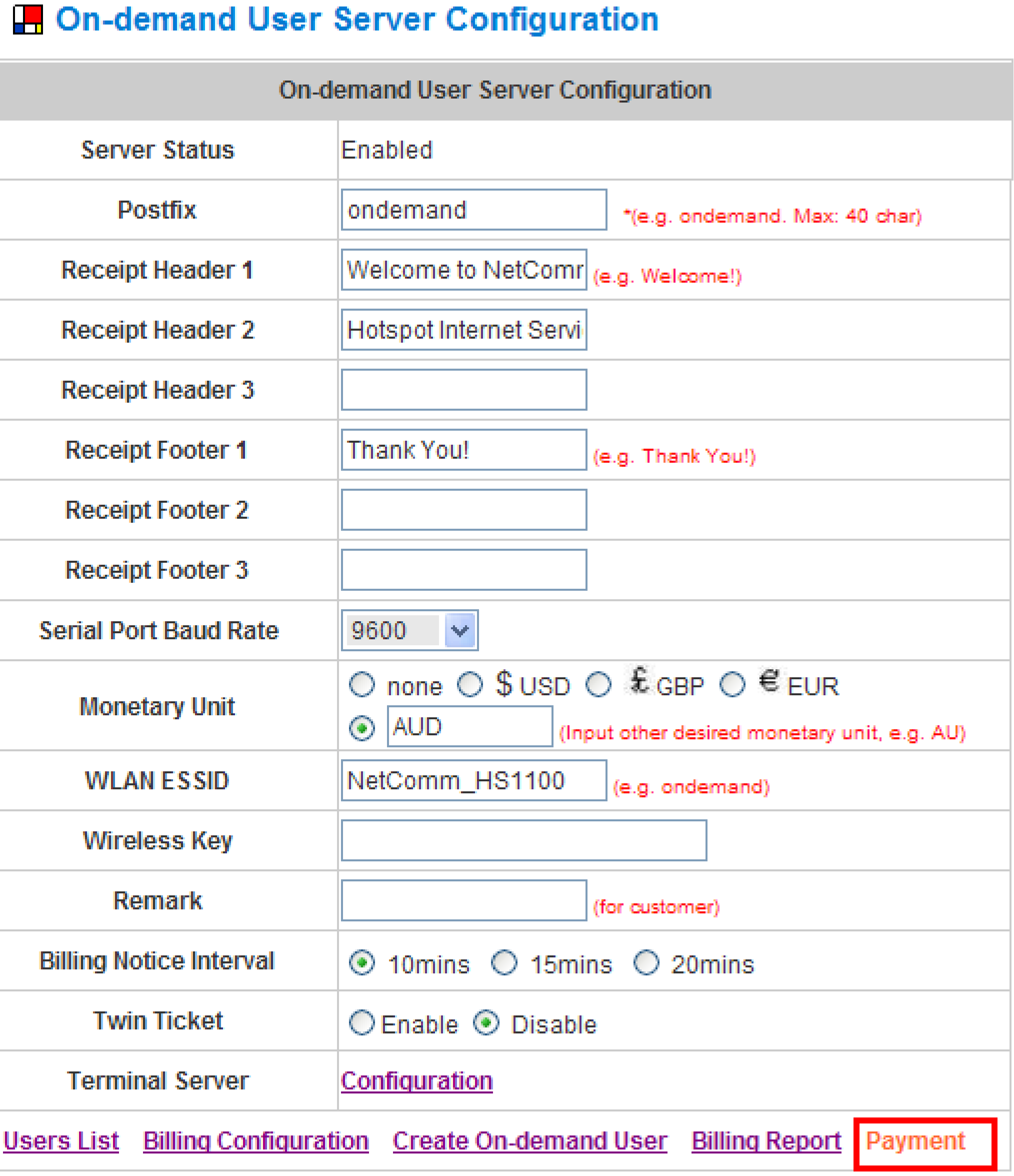


| Plan Type | Ticket | Authorize.Net | PayPal | SecurePay |
|---|---|---|---|---|
| Plan1 | 2 | 0 | 0 | 0 |
| Plan2 | 1 | 0 | 0 | 0 |
| Plan3 | 0 | 0 | 0 | 0 |
| Plan4 | 0 | 0 | 0 | 0 |
| Plan5 | 0 | 0 | 0 | 0 |
| Plan6 | 0 | 0 | 0 | 0 |
| Plan7 | 0 | 0 | 0 | 0 |
| Plan8 | 0 | 0 | 0 | 0 |
| Plan9 | 0 | 0 | 0 | 0 |
| Plan10 | 0 | 0 | 0 | 0 |
| Total income | 30 | 0 | 0 | 0 |



| Report from 2000/01/01 ~ 2008/11/20 | |
|---|---|
| Accounts Sold by Ticket | 3 |
| Accounts Sold by Authorize.Net | 0 |
| Accounts Sold by PayPal | 0 |
| Accounts Sold by SecurePay | 0 |
| Income from tickets sold for time users | 20 |
| Income from tickets sold for volume users | 10 |

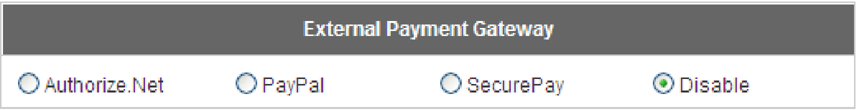
- **Payment:** This section is for hotspot owners to set up an external payment gateway to accept payments when providing wireless access service to end customers who wish to pay for the service on-line.



On-demand User Server Configuration

| On-demand User Server Configuration | |
|---|---|
| Server Status | Enabled |
| Postfix | ondemand *(e.g. ondemand. Max: 40 char) |
| Receipt Header 1 | Welcome to NetComr (e.g. Welcome!) |
| Receipt Header 2 | Hotspot Internet Servi |
| Receipt Header 3 | |
| Receipt Footer 1 | Thank You! (e.g. Thank You!) |
| Receipt Footer 2 | |
| Receipt Footer 3 | |
| Serial Port Baud Rate | 9600 |
| Monetary Unit | ○ none ○ $ USD ○ £ GBP ○ € EUR<br>● AUD (Input other desired monetary unit, e.g. AU) |
| WLAN ESSID | NetComm_HS1100 (e.g. ondemand) |
| Wireless Key | |
| Remark | (for customer) |
| Billing Notice Interval | ● 10mins ○ 15mins ○ 20mins |
| Twin Ticket | ○ Enable ● Disable |
| Terminal Server | Configuration |

Three payment selections include **Authorize.Net**, **PayPal, Secure Pay** and **Disable**. The default is ***Disable***.

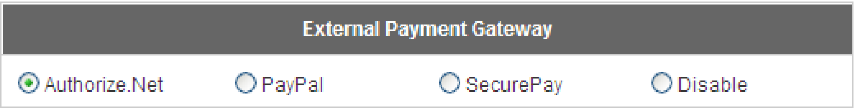


| External Payment Gateway | | | |
|---|---|---|---|
| ○ Authorize.Net | ○ PayPal | ○ SecurePay | ● Disable |

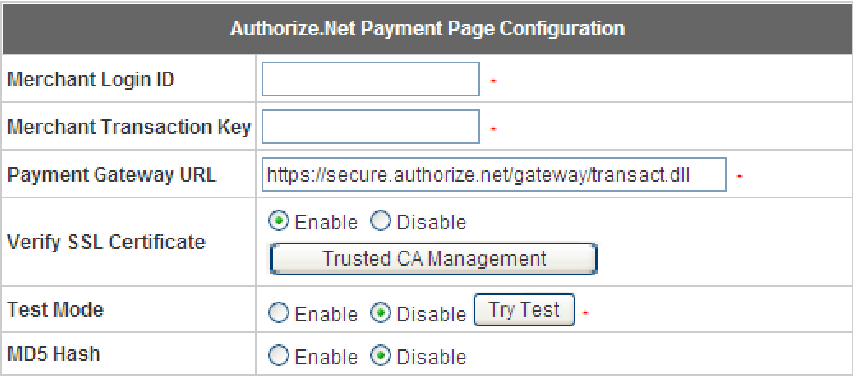
- **Authorize.Net**

Before setting up **"Authorize.Net"**, it is required that hotspot owners have a valid Authorize.Net account. Please see ***Appendix B. Accepting Payments via Authorize.Net*** for more information about opening an Authorize.Net account and its related maintenance functions.

➢ **External Payment Gateway / Authorize.Net Payment Page Configuration**



| External Payment Gateway | | | |
|---|---|---|---|
| ● Authorize.Net | ○ PayPal | ○ SecurePay | ○ Disable |



| Authorize.Net Payment Page Configuration | |
|---|---|
| Merchant Login ID | - |
| Merchant Transaction Key | - |
| Payment Gateway URL | https://secure.authorize.net/gateway/transact.dll - |
| Verify SSL Certificate | ● Enable ○ Disable<br>Trusted CA Management |
| Test Mode | ○ Enable ● Disable Try Test - |
| MD5 Hash | ○ Enable ● Disable |

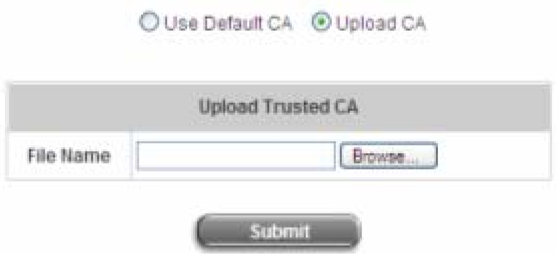
**Merchant ID:** The "Login ID" that comes with the Authorize.Net account

**Merchant Transaction Key:** The merchant transaction key is similar to a password and is used by Authorize.Net to authenticate transactions.

**Payment Gateway URL:** The default website address to post all transaction data.

**Verify SSL Certificate:** This is to help protect the system from accessing a website other than Authorize.Net.

- **Trusted CA Management:** Select the version of Trusted Certificate for the system.



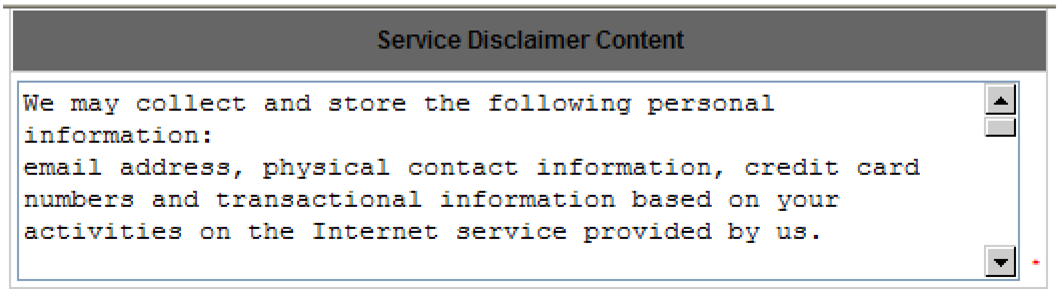
○ Use Default CA ● Upload CA

| Upload Trusted CA | |
|---|---|
| File Name | Browse... |

**Test Mode:** In this mode, hotspot owners can post **test** transactions **for free** to check if the payment function works properly.

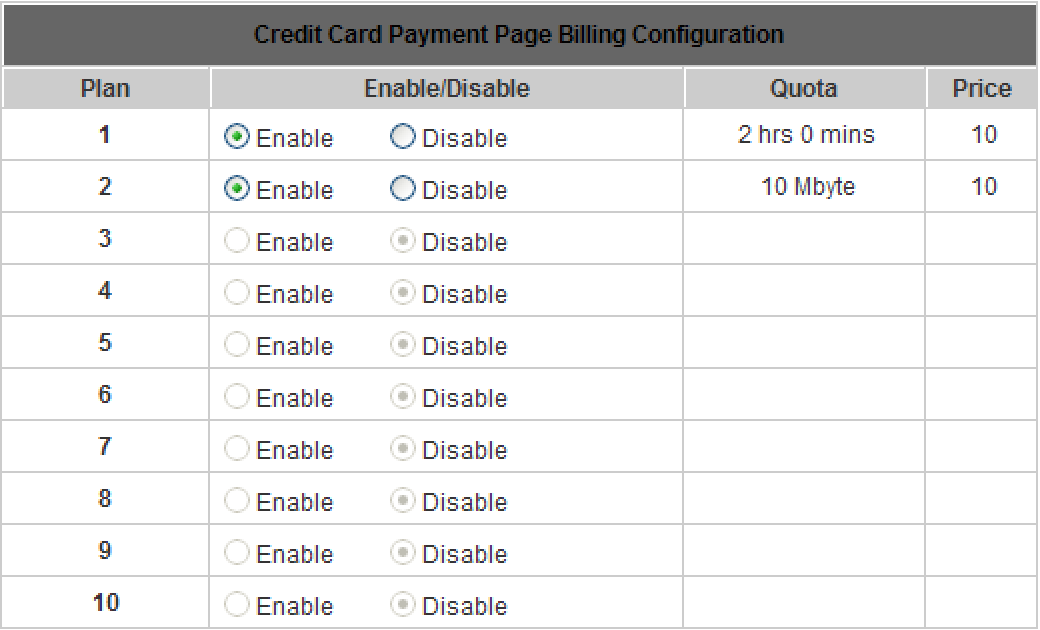
**MD5 Hash:** If transaction responses need to be encrypted by the Payment Gateway, enter and confirm a MD5 Hash value and select a reactive mode. The MD5 Hash security feature enables merchants to verify that the results of a transaction or transaction response received by their server were actually sent from the Authorize.Net.

- **Service Disclaimer Content / Credit Card Payment Page /Client's Purchasing Record**



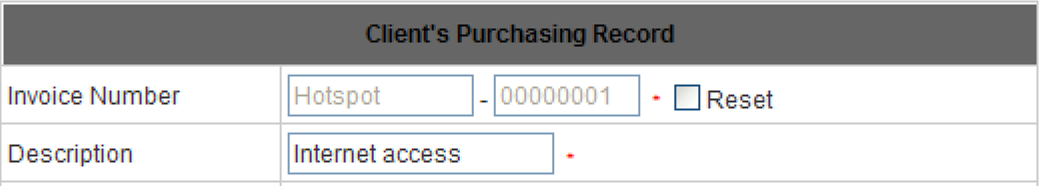
Service Disclaimer Content

We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.



Credit Card Payment Page Billing Configuration

| Plan | Enable/Disable | Quota | Price |
|---|---|---|---|
| 1 | ● Enable ○ Disable | 2 hrs 0 mins | 10 |
| 2 | ● Enable ○ Disable | 10 Mbyte | 10 |
| 3 | ○ Enable ● Disable | | |
| 4 | ○ Enable ● Disable | | |
| 5 | ○ Enable ● Disable | | |
| 6 | ○ Enable ● Disable | | |
| 7 | ○ Enable ● Disable | | |
| 8 | ○ Enable ● Disable | | |
| 9 | ○ Enable ● Disable | | |
| 10 | ○ Enable ● Disable | | |



Client's Purchasing Record

| | |
|---|---|
| Invoice Number | Hotspot - 00000001 * □ Reset |
| Description | Internet access * |

**Service Disclaimer Content:** View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

**Credit Card Payment Page Billing Configuration:** These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

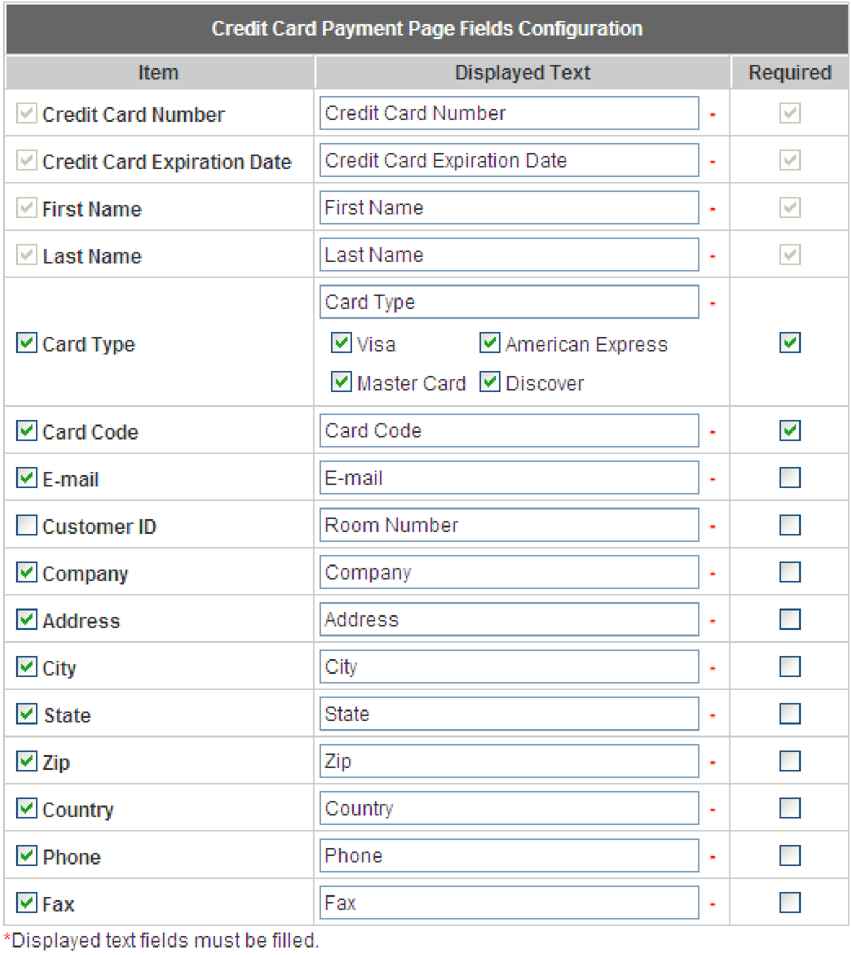
**Client's Purchasing Record:**

**Invoice Number:** An invoice number may be provided as additional information against a transaction. This is a reference field that may contain any kind of information.

**Description:** Enter the product/service description (e.g. wireless access service).

**Email Header:** Enter the information that will appear in the header of the invoice.

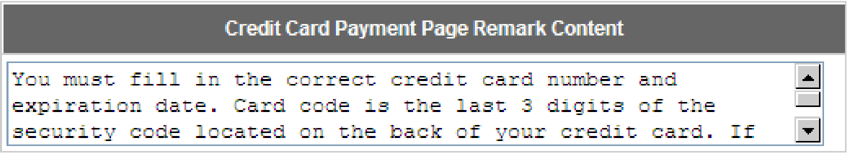
### ➢ Credit Card Payment Page Fields Configuration / Credit Card Page Remark Content



Credit Card Payment Page Fields Configuration

| Item | Displayed Text | Required |
|---|---|---|
| ☑ Credit Card Number | Credit Card Number * | ☑ |
| ☑ Credit Card Expiration Date | Credit Card Expiration Date * | ☑ |
| ☑ First Name | First Name * | ☑ |
| ☑ Last Name | Last Name * | ☑ |
| ☑ Card Type | Card Type *<br>☑ Visa ☑ American Express<br>☑ Master Card ☑ Discover | ☑ |
| ☑ Card Code | Card Code * | ☑ |
| ☑ E-mail | E-mail * | □ |
| □ Customer ID | Room Number * | □ |
| ☑ Company | Company * | □ |
| ☑ Address | Address * | □ |
| ☑ City | City * | □ |
| ☑ State | State * | □ |
| ☑ Zip | Zip * | □ |
| ☑ Country | Country * | □ |
| ☑ Phone | Phone * | □ |
| ☑ Fax | Fax * | □ |

*Displayed text fields must be filled.



Credit Card Payment Page Remark Content

You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If

***Item:*** *Check the box for the items that will show on the customer's online payment interface.*

***Displayed Text:*** *Enter what needs to be shown in this field.*

***Required:*** *Check the box for the items that will show as required fields.*

**Credit Card Number:** Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.

**Credit Card Expiration Date:** Expired date of the credit card. This should be entered in the format of MMYY (month & year). For example, if it is expired on July 2005, it should be entered as 0705.

**First Name:** The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's first name.

**Last Name:** The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's last name.

**Card Type:** This value indicates the level of match between the Card Code entered on a transaction and the value that is on file with a customer's credit card company. A code and narrative description are provided indicating the results returned by the processor.

**Card Code:** The three- or four-digit code assigned to a customer's credit card number (found either on the front of the card at the end of the credit card number or on the back of the card).

**E-mail:** An email address may be provided along with the billing information of a transaction. This is the customer's email address and should contain an "@" symbol.

**Customer ID:** This is an internal identifier for a customer that may be associated with the billing information of a transaction. This field may contain any kind of information.

**Company:** The name of the company associated with the billing or shipping information entered on a given transaction.

**Address:** The address entered either in the billing or shipping information of a given transaction.

**City:** The city is associated with either the billing address or shipping address of a transaction.

**State:** A state is associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.

**Zip:** The ZIP code represents the five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits - four digits.

**Country:** The country is associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full value.

**Phone:** A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all numbers or it may include parentheses ( ) or dashes (-) to separate the area code and number.

**Fax:** A fax number may be associated with the billing information of a transaction. This number may be entered as all numbers or contain parentheses ( ) and dashes (-) to separate the area code and number.

**Credit Card Payment Page Remark Content**

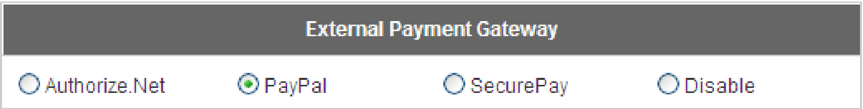
Enter additional details for the transaction such as Tax, Freight and Duty Amounts, Tax Exempt status, and a Purchase Order Number, if applicable.

- **PayPal**

Before setting up “PayPal”, it is required that the hotspot owners have a valid PayPal “Business Account”. Please see ***Appendix C. Accepting Payments via PayPal*** for more information about setting up a PayPal Business Account, relevant maintenance functions, and an example for clients.

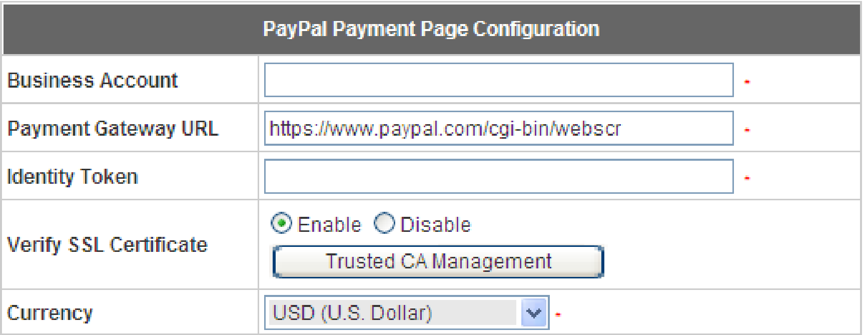
After opening a PayPal Business Account, the hotspot owners should find the **“Identity Token”** of this PayPal account to continue “PayPal Payment Page Configuration”.

➢ **External Payment Gateway / PayPal Payment Page Configuration**



External Payment Gateway

○ Authorize.Net ● PayPal ○ SecurePay ○ Disable



PayPal Payment Page Configuration

| | |
|---|---|
| Business Account | - |
| Payment Gateway URL | https://www.paypal.com/cgi-bin/webscr - |
| Identity Token | - |
| Verify SSL Certificate | ● Enable ○ Disable<br>Trusted CA Management |
| Currency | USD (U.S. Dollar) - |

**Business Account:** The “Login ID” (an email address) that is associated with the PayPal Business Account.

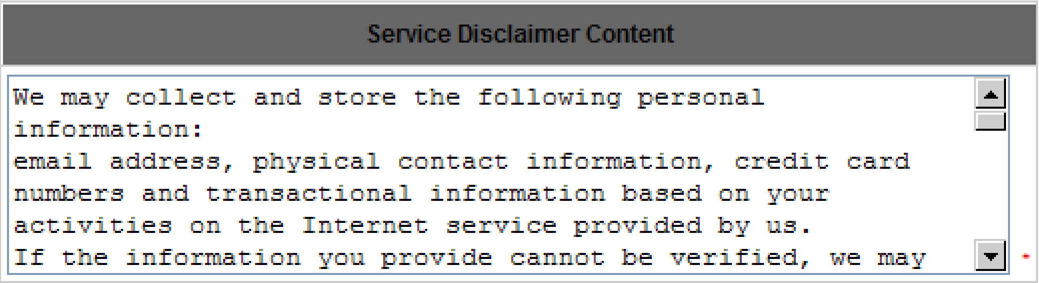
**Payment Gateway URL:** The default website address to post all transaction data.

**Identity Token:** This is the key used by PayPal to validate all the transactions.

**Verify SSL Certificate:** This is to help protect the system from accessing a website other than PayPal

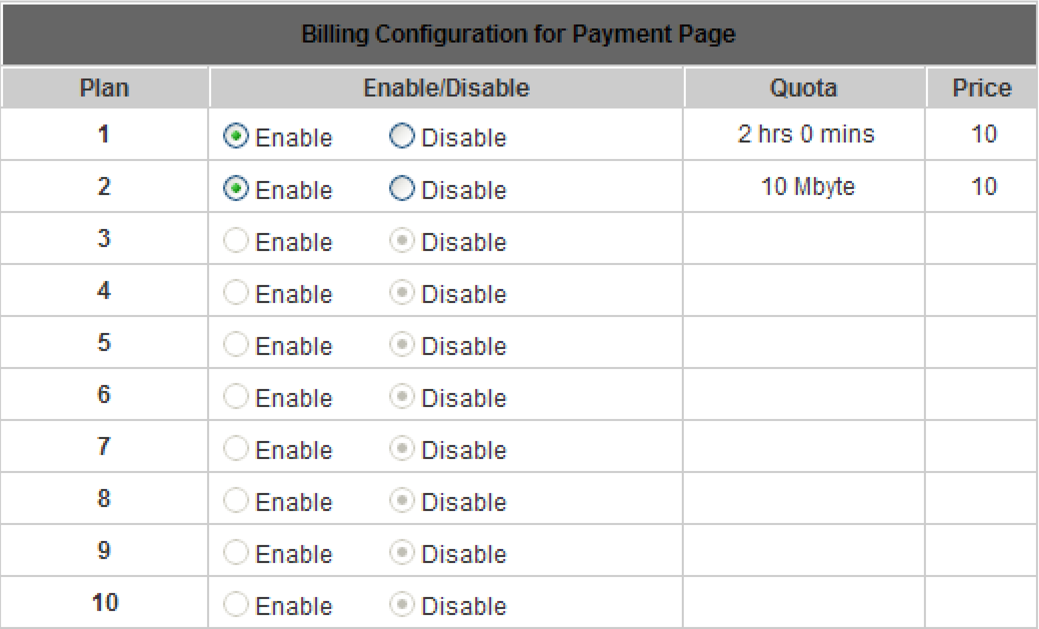
**Currency:** The currency to be used for the payment transactions.

- **Service Disclaimer Content / Billing Configuration for Payment Page**



Service Disclaimer Content

```
We may collect and store the following personal
information:
email address, physical contact information, credit card
numbers and transactional information based on your
activities on the Internet service provided by us.
If the information you provide cannot be verified, we may
```



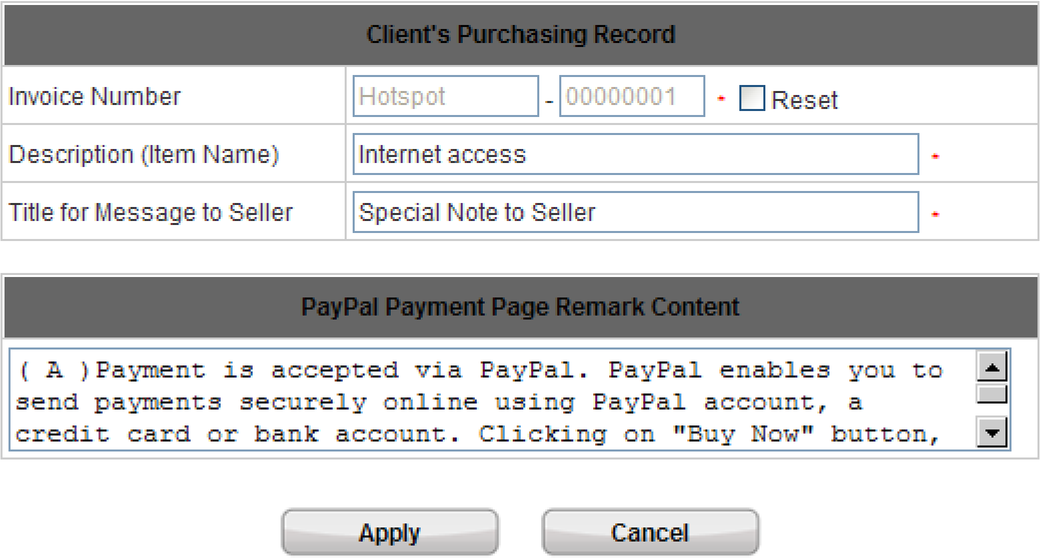
Billing Configuration for Payment Page

| Plan | Enable/Disable | Quota | Price |
|---|---|---|---|
| 1 | ● Enable ○ Disable | 2 hrs 0 mins | 10 |
| 2 | ● Enable ○ Disable | 10 Mbyte | 10 |
| 3 | ○ Enable ● Disable | | |
| 4 | ○ Enable ● Disable | | |
| 5 | ○ Enable ● Disable | | |
| 6 | ○ Enable ● Disable | | |
| 7 | ○ Enable ● Disable | | |
| 8 | ○ Enable ● Disable | | |
| 9 | ○ Enable ● Disable | | |
| 10 | ○ Enable ● Disable | | |

**Service Disclaimer Content:** View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

**Billing Configuration for Payment Page:** These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

- **Client's Purchasing Record / PayPal Payment Page Remark Content**



| Client's Purchasing Record | |
|---|---|
| Invoice Number | Hotspot - 00000001 * □ Reset |
| Description (Item Name) | Internet access * |
| Title for Message to Seller | Special Note to Seller * |

**PayPal Payment Page Remark Content**

```
( A )Payment is accepted via PayPal. PayPal enables you to
send payments securely online using PayPal account, a
credit card or bank account. Clicking on "Buy Now" button,
```

**Client's Purchasing Record:**

**Invoice Number:** An invoice number may be provided as additional information against a transaction. This is a reference field that may contain any kind of information.

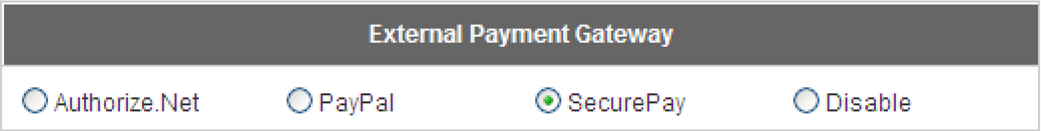
**Description:** Enter the product/service description (e.g. wireless access service).

**Title for Message to Seller:** Enter the information that will appear in the header of the PayPal payment page.

**PayPal Payment Page Remark Content:** The message content will be displayed as a special notice to end customers in the page of "Rate Plan". For example, it can describe the cautions for making a payment via PayPal.

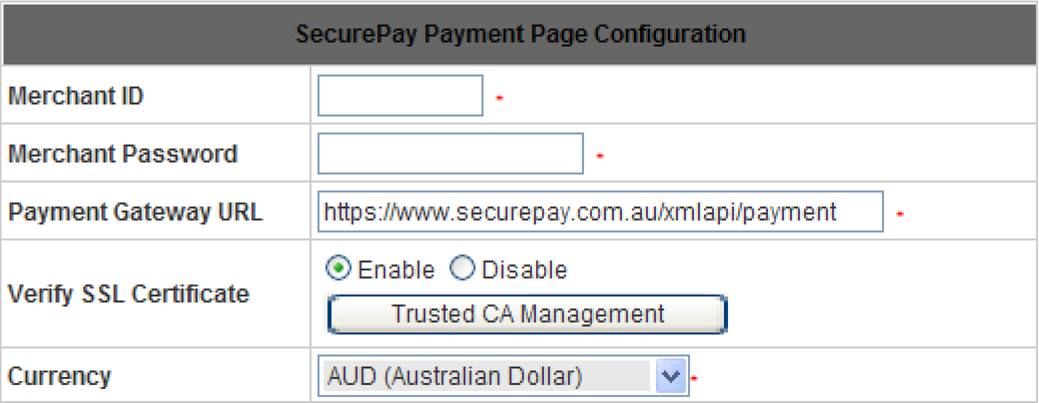
- **SecurePay**

Before setting up "SecurePay", it is required that the hotspot owners have a valid SecurePay "Merchant Account" from its official website. Please see ***Appendix D. Accepting Payments via SecurePay*** for more information about setting up a SecurePay Account, relevant maintenance functions, and an example for clients.



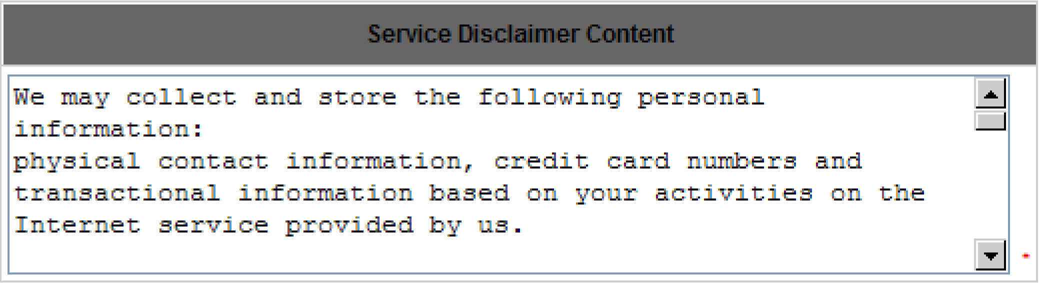
External Payment Gateway

○ Authorize.Net ○ PayPal ● SecurePay ○ Disable



SecurePay Payment Page Configuration

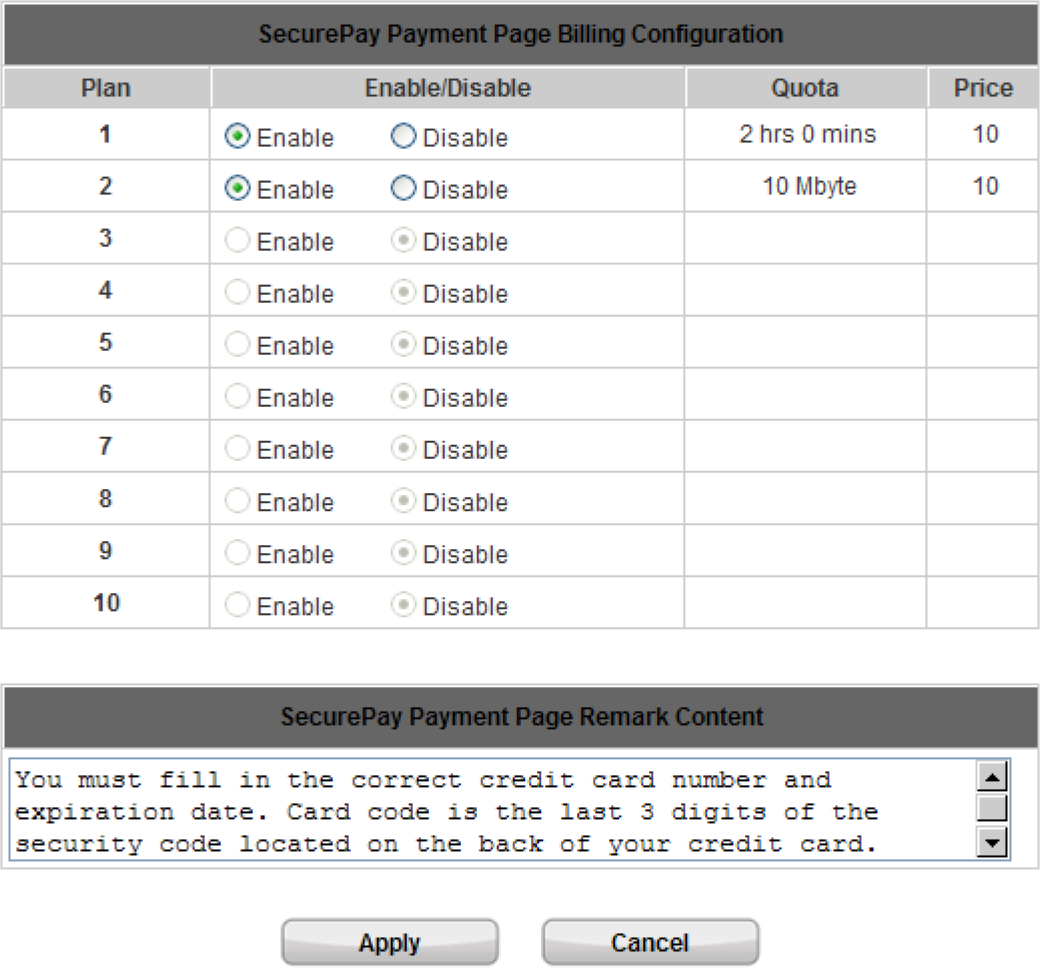
| | |
|---|---|
| Merchant ID | * |
| Merchant Password | * |
| Payment Gateway URL | https://www.securepay.com.au/xmlapi/payment * |
| Verify SSL Certificate | ● Enable ○ Disable<br>Trusted CA Management |
| Currency | AUD (Australian Dollar) * |



Service Disclaimer Content

```
We may collect and store the following personal
information:
physical contact information, credit card numbers and
transactional information based on your activities on the
Internet service provided by us.
```

*



SecurePay Payment Page Billing Configuration

| Plan | Enable/Disable | | Quota | Price |
|---|---|---|---|---|
| 1 | ● Enable | ○ Disable | 2 hrs 0 mins | 10 |
| 2 | ● Enable | ○ Disable | 10 Mbyte | 10 |
| 3 | ○ Enable | ● Disable | | |
| 4 | ○ Enable | ● Disable | | |
| 5 | ○ Enable | ● Disable | | |
| 6 | ○ Enable | ● Disable | | |
| 7 | ○ Enable | ● Disable | | |
| 8 | ○ Enable | ● Disable | | |
| 9 | ○ Enable | ● Disable | | |
| 10 | ○ Enable | ● Disable | | |

SecurePay Payment Page Remark Content

You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card.

- **Payment Page Configuration**

  **Merchant ID:** The ID that is associated with the Business Account.

  **Password:** This is the key used by Secure Pay to validate all the transactions.

  **Payment Gateway URL:** The default website address to post all transaction data.

  **Verify SSL Certificate:** This is to help protect the system from accessing a website other than Secure Pay.

  **Currency:** The currency to be used for the payment transactions.

- **Service Disclaimer Content**

  View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

- **SecurePay Payment Page Billing Configuration**

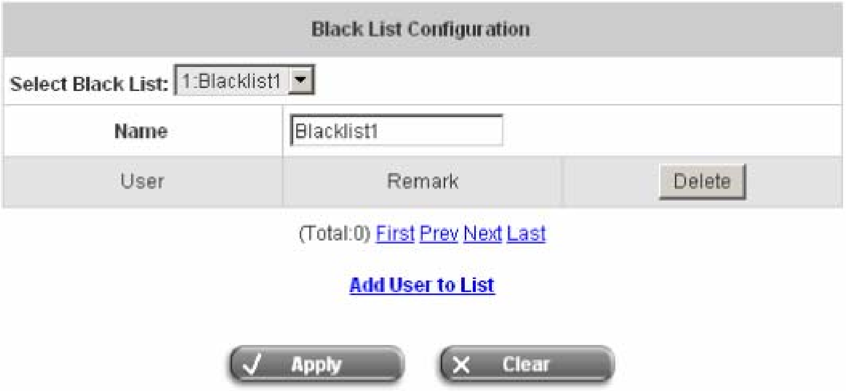
  These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

- **SecurePay Payment Page Remark Content**

  The message content will be displayed as a special notice to end customers.

## Black List Configuration

The administrator can add, delete, or edit the black list for user access control. Each black list can include 40 users at most. If a user in the black list wants to log into the system, the user's access will be denied. The administrator can use the pull-down menu to select the desired black list.



Black List Configuration

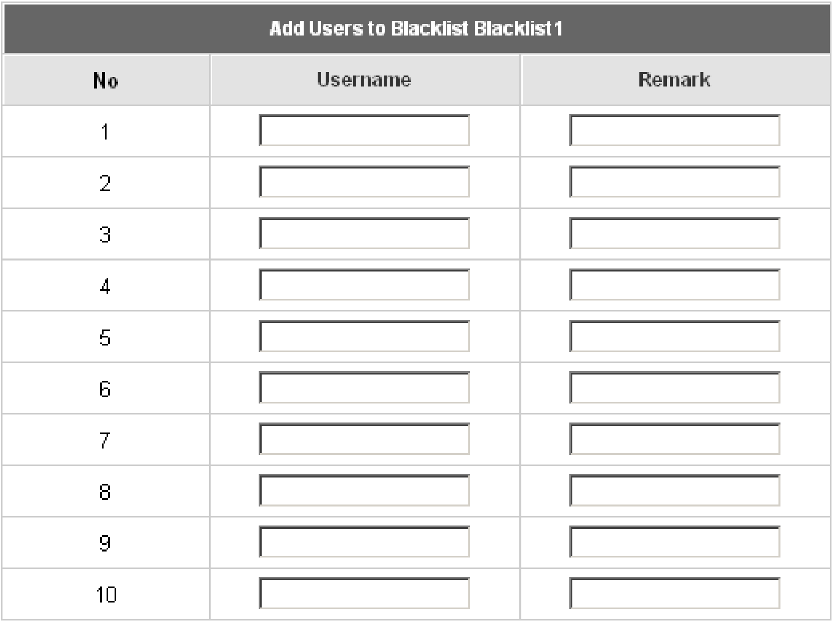
Select Black List: 1:Blacklist1

| | | |
|---|---|---|
| Name | Blacklist1 | |
| User | Remark | Delete |

(Total:0) First Prev Next Last

Add User to List

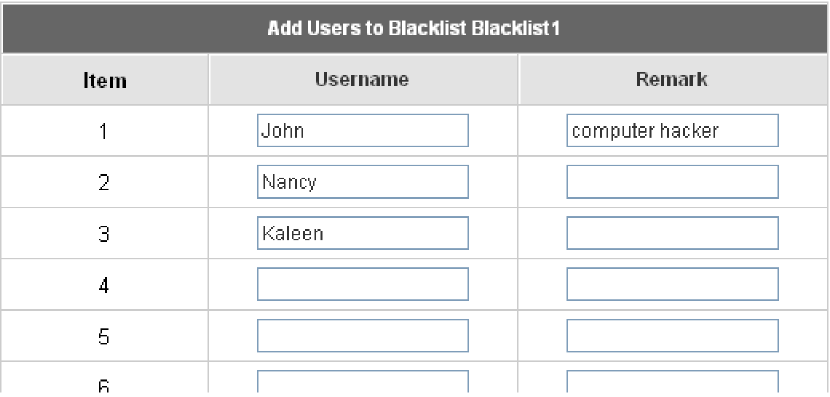
- **Select Black List:** There are 5 lists to select from for the desired black list.
- **Name:** Set the black list name and it will show on the pull-down menu above.
- **Add User to List:** Click the hyperlink of **"Add User to List"** to add users to the selected black list.



Add Users to Blacklist Blacklist1

| No | Username | Remark |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

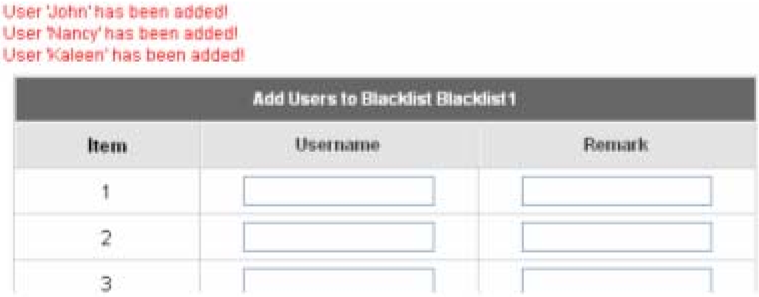
After entering the usernames in the **“Username”** fields and other information in the **“Remark”** field (not required).



Add Users to Blacklist Blacklist1

| Item | Username | Remark |
|---|---|---|
| 1 | John | computer hacker |
| 2 | Nancy | |
| 3 | Kaleen | |
| 4 | | |
| 5 | | |
| 6 | | |

Click ***Apply*** to add these users.

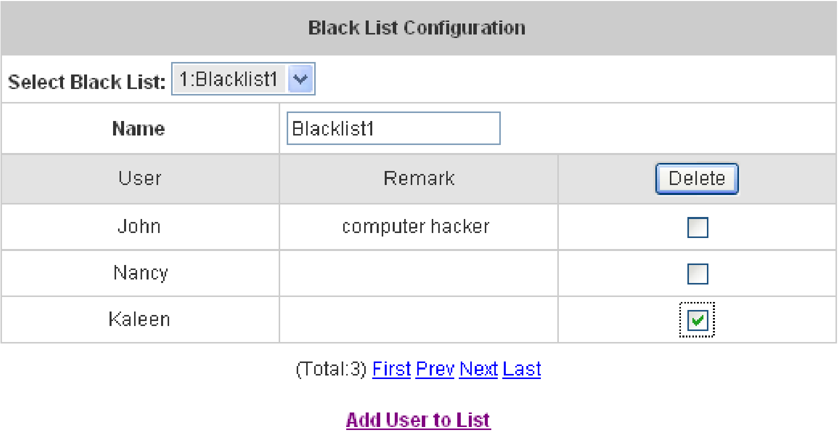


User 'John' has been added!
User 'Nancy' has been added!
User 'Kaleen' has been added!

Add Users to Blacklist Blacklist1

| Item | Username | Remark |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |

To remove a user from the black list, select the user’s **“Delete”** check box and then click the ***Delete*** button to remove that user from the black list.



Black List Configuration

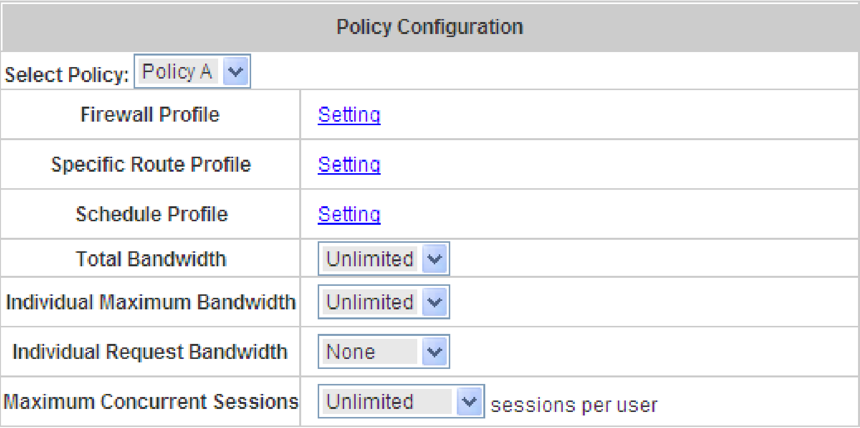
| | | |
|---|---|---|
| Select Black List: 1:Blacklist1 | | |
| Name | Blacklist1 | |
| User | Remark | Delete |
| John | computer hacker | □ |
| Nancy | | □ |
| Kaleen | | ☑ |

(Total:3) First Prev Next Last

Add User to List

## Policy Configuration

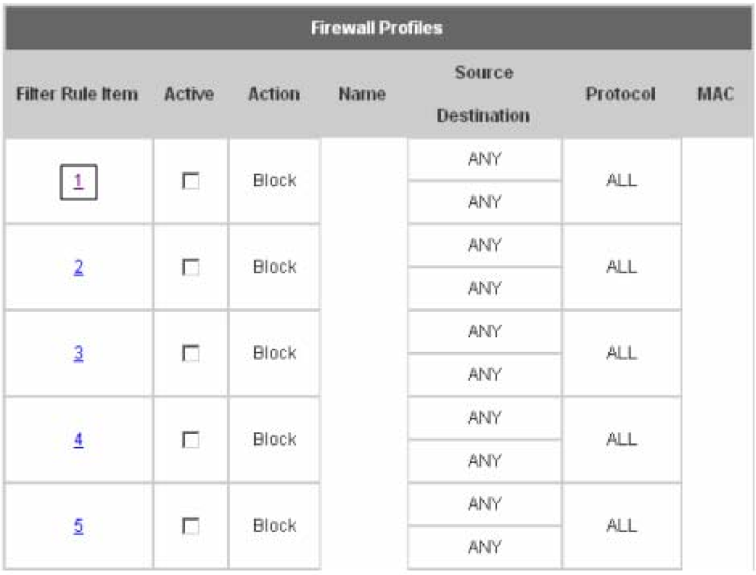
Every Policy has three profiles, **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** as well as one **Bandwidth** setting for that policy.



| Policy Configuration | |
|---|---|
| Select Policy: Policy A | |
| Firewall Profile | Setting |
| Specific Route Profile | Setting |
| Schedule Profile | Setting |
| Total Bandwidth | Unlimited |
| Individual Maximum Bandwidth | Unlimited |
| Individual Request Bandwidth | None |
| Maximum Concurrent Sessions | Unlimited sessions per user |

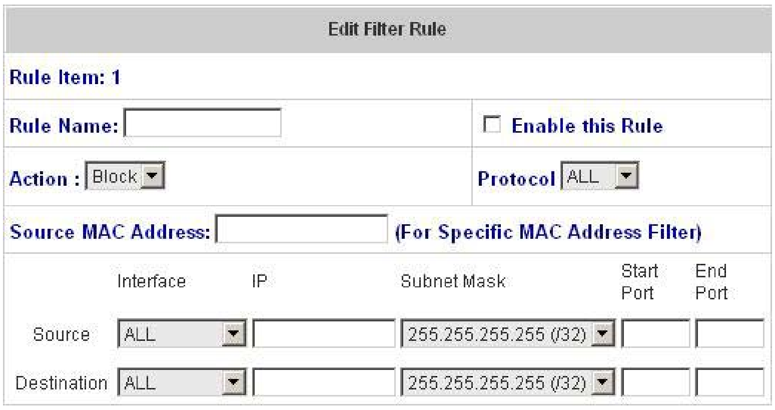
- **Firewall Profile**

  Click the hyperlink of ***Setting*** for **Firewall Profile**, the Firewall Profiles list will appear. Click the numbers of ***Filter Rule Item*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list. Check ***Active*** to enable that rule.



Firewall Profiles

| Filter Rule Item | Active | Action | Name | Source<br>Destination | Protocol | MAC |
|---|---|---|---|---|---|---|
| 1 | □ | Block | | ANY<br>ANY | ALL | |
| 2 | □ | Block | | ANY<br>ANY | ALL | |
| 3 | □ | Block | | ANY<br>ANY | ALL | |
| 4 | □ | Block | | ANY<br>ANY | ALL | |
| 5 | □ | Block | | ANY<br>ANY | ALL | |



Edit Filter Rule

Rule Item: 1

Rule Name: ______ □ Enable this Rule

Action : Block Protocol ALL

Source MAC Address: ______ (For Specific MAC Address Filter)

| | Interface | IP | Subnet Mask | Start Port | End Port |
|---|---|---|---|---|---|
| Source | ALL | | 255.255.255.255 (/32) | | |
| Destination | ALL | | 255.255.255.255 (/32) | | |

**Rule Item:** The rule selected.

**Rule Name:** The rule name can be changed here.

**Enable this Rule:** After checking this function, the rule will be enabled.

**Action:** There are two options, **Block** and **Pass**. **Block**. **"Block"** is to prevent packets from passing. **"Pass"** is to permit packets passing.

**Protocol:** There are three protocols to select from, **TCP**, **UDP** and **ICMP**. Or choose **ALL** to use all three protocols.

**Source MAC Address:** The MAC address of the source IP address. This is for specific MAC address filter.

**Source/Destination Interface:** There are five interfaces to choose from, **ALL, WAN**, **Wireless**, **Public LAN (LAN1/LAN2** by default**)** and **Private LAN (LAN3/LAN4** by default**)**.

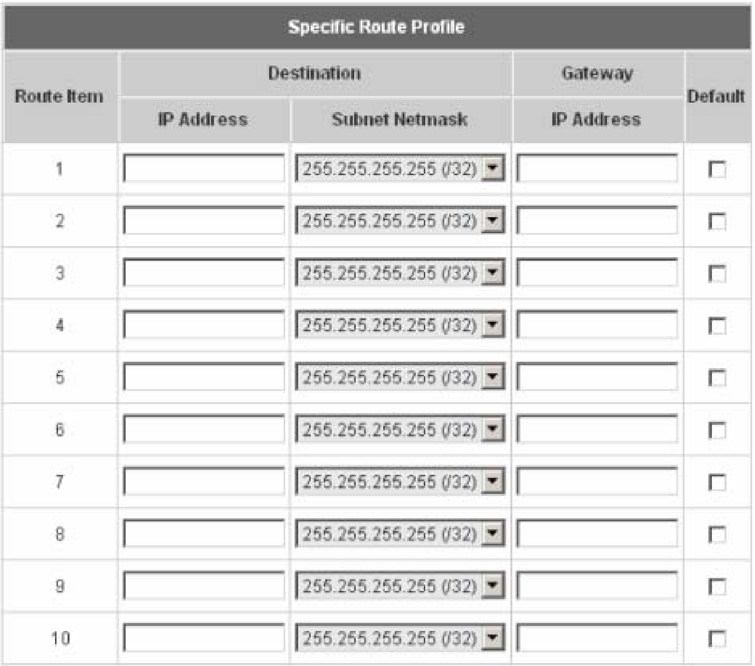
**Source/Destination IP:** Enter the source and destination IP addresses.

**Source/Destination Subnet Mask:** Enter the source and destination subnet masks.

**Source/Destination Start/End Port:** Enter the range of source and destination ports.

- **Specific Route Profile**

Click the hyperlink of ***Setting*** for **Specific Route Profile**, the Specific Route Profile list will appear.



Specific Route Profile

| Route Item | Destination | | Gateway | Default |
|---|---|---|---|---|
| | IP Address | Subnet Netmask | IP Address | |
| 1 | | 255.255.255.255 (/32) | | □ |
| 2 | | 255.255.255.255 (/32) | | □ |
| 3 | | 255.255.255.255 (/32) | | □ |
| 4 | | 255.255.255.255 (/32) | | □ |
| 5 | | 255.255.255.255 (/32) | | □ |
| 6 | | 255.255.255.255 (/32) | | □ |
| 7 | | 255.255.255.255 (/32) | | □ |
| 8 | | 255.255.255.255 (/32) | | □ |
| 9 | | 255.255.255.255 (/32) | | □ |
| 10 | | 255.255.255.255 (/32) | | □ |

**Profile Name:** The profile name can be changed here.

**IP Address:** The destination IP address of the host or the network.

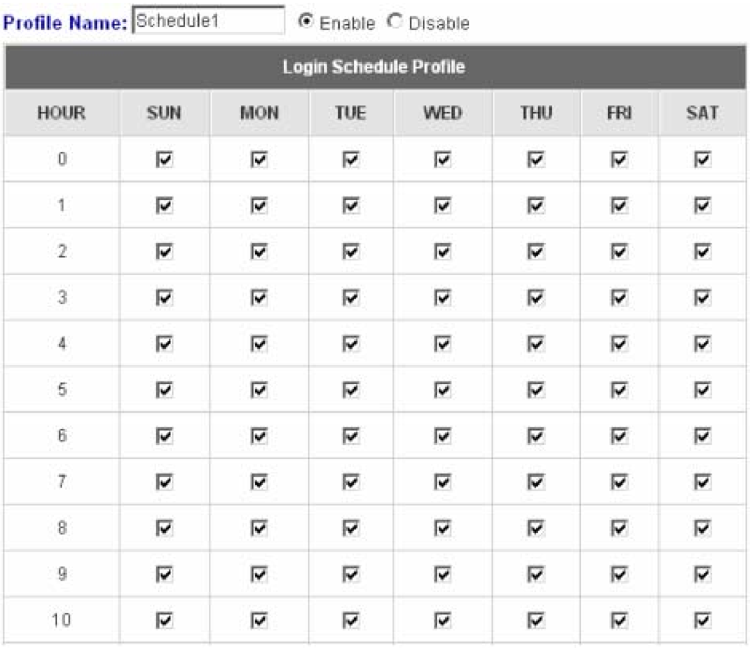
**Subnet Netmask:** Select a destination subnet netmask of the host or the network.

**IP Address:** The IP address of the next router to the destination.

**Default:** Check this option to apply the default value.

- **Schedule Profile**

  Click the hyperlink of ***Setting*** for **Schedule Profile** to enter the Schedule Profile list. Select **“Enable”** to show the list. This function is used to restrict the time that the users can log in. Please enable/disable the desired time slot(s) and click ***Apply*** to save the settings. These settings will become effective immediately after clicking the ***Apply*** button.



Profile Name: Schedule1 ● Enable ○ Disable

Login Schedule Profile

| HOUR | SUN | MON | TUE | WED | THU | FRI | SAT |
|---|---|---|---|---|---|---|---|
| 0 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 1 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 2 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 3 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 4 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 5 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 6 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 7 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 8 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 9 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 10 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

- **Total Bandwidth**

  Choose one bandwidth limit for that particular policy.

- **Individual Maximum Bandwidth**

  Choose one maximum bandwidth for that particular policy.

- **Individual Request Bandwidth**

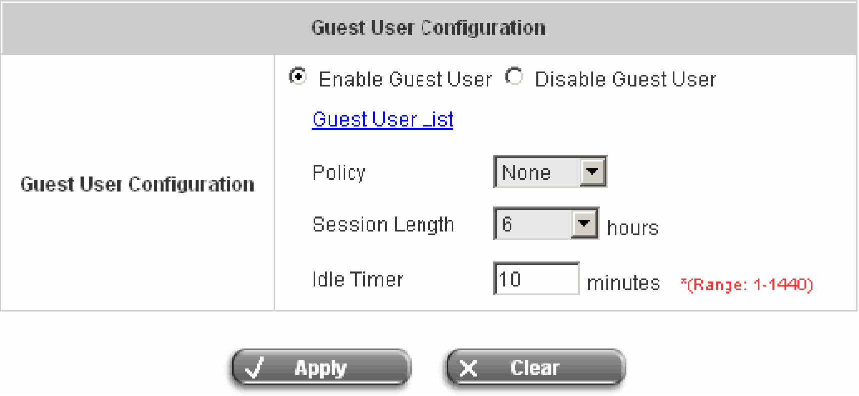
  Choose one individual bandwidth limit for that policy, from none to 54Mbps.

- **Maximum Concurrent Sessions**

  The concurrent sessions for each user, it can be restricted by administrator.

## Guest User Configuration

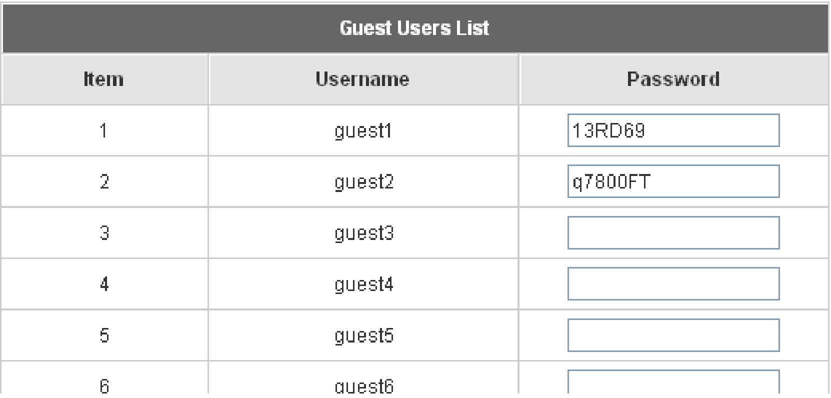
This function can permit guests to log into the system. Select **"Enable Guest User"** and click ***Apply*** to save the settings.



Guest User Configuration

| Guest User Configuration | ● Enable Guest User ○ Disable Guest User<br>Guest User List<br>Policy: None<br>Session Length: 6 hours<br>Idle Timer: 10 minutes *(Range: 1-1440) |
|---|---|

- **Guest User List:** HS1100 allows 10 guest users to log in. To activate a guest user, just enter the password in the corresponding **"Password"** field for that guest account. Guest accounts with blank password will not be activated.

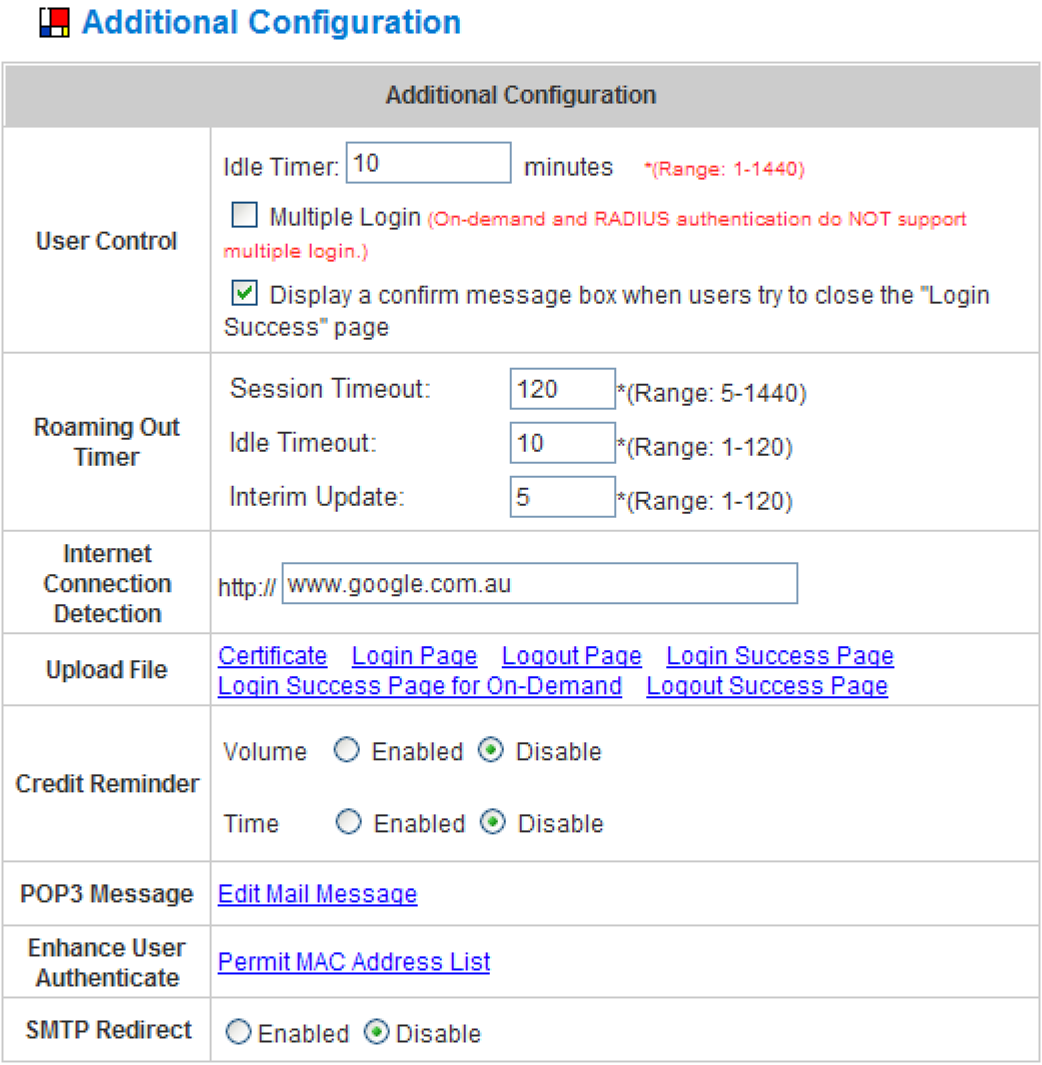


Guest Users List

| Item | Username | Password |
|---|---|---|
| 1 | guest1 | 13RD69 |
| 2 | guest2 | q7800FT |
| 3 | guest3 | |
| 4 | guest4 | |
| 5 | guest5 | |
| 6 | guest6 | |

- **Policy:** Select one policy to apply to.
- **Session Length:** This restricts the connection time of the guest users. The default session length is 6 hours and the available session time ranges from 1 to 12 hours or unlimited.
- **Idle Timer:** If a guest user has been idled with no network activities at all, the system will automatically kick out the user. The Idle timer can be set in the range of 1~1440 minutes, and the default idle timer is 10 minutes.

## Additional Configuration



Additional Configuration

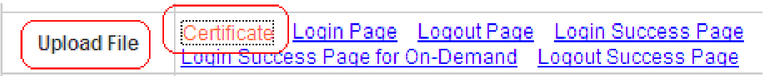
| Additional Configuration | |
|---|---|
| User Control | Idle Timer: 10 minutes *(Range: 1-1440)<br>☐ Multiple Login (On-demand and RADIUS authentication do NOT support multiple login.)<br>☑ Display a confirm message box when users try to close the "Login Success" page |
| Roaming Out Timer | Session Timeout: 120 *(Range: 5-1440)<br>Idle Timeout: 10 *(Range: 1-120)<br>Interim Update: 5 *(Range: 1-120) |
| Internet Connection Detection | http:// www.google.com.au |
| Upload File | Certificate Login Page Logout Page Login Success Page<br>Login Success Page for On-Demand Logout Success Page |
| Credit Reminder | Volume ○ Enabled ● Disable<br>Time ○ Enabled ● Disable |
| POP3 Message | Edit Mail Message |
| Enhance User Authenticate | Permit MAC Address List |
| SMTP Redirect | ○ Enabled ● Disable |

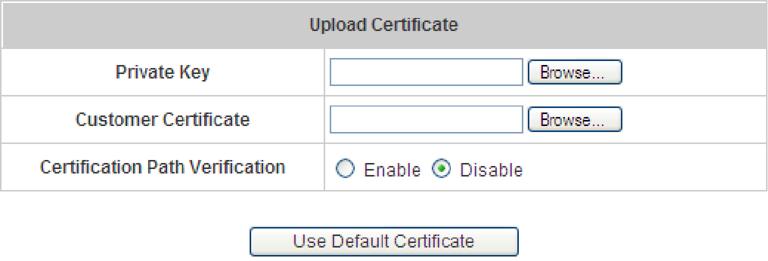
- **User Control:** Functions under this section applies for all general users.
    - **Idle Timer:** If a user has been idled with no network activities at all, the system will automatically kick out the user. The Idle timer can be set in the range of 1~1440 minutes, and the default idle timer is 10 minutes.
    - **Multiple Login:** When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS authentication method.)

- **Roaming Out Timer**
    - **Session Timeout:** Maximum session timeout.
    - **Idle Timeout:** Maximum idle timeout.
    - **Interim Update:** Constant records update time interval.

- **Internet Connection Detection:** Enter a specific URL or IP address to which HS1100 will send packets for detecting network connection status. If there is a problem in the connection in the WAN port of HS1100, and the URL or IP address specified cannot be reached, there will be a message appearing on users' login screen showing the **Administrator Info**, which can be set in *4.1.2 System Information* section.

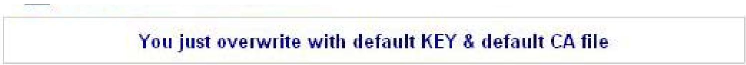
- **Upload File**
  - **Certificate:** The administrator can upload new private key and customer certification. Click the ***Browse*** button to select the file for the certificate upload. Then click ***Apply*** to complete the upload process; otherwise click ***Use Default Certificate*** to use the default one.





| Upload Certificate | |
|---|---|
| Private Key | Browse... |
| Customer Certificate | Browse... |
| Certification Path Verification | ○ Enable ● Disable |

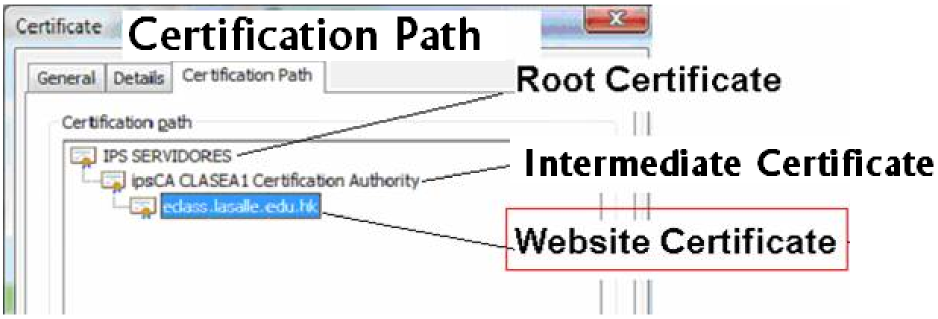
Click ***Use Default Certificate*** to use the default certificate and key.



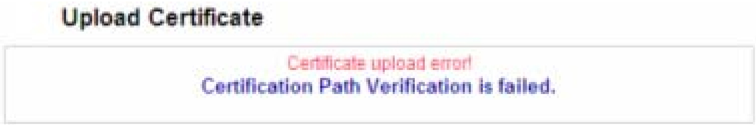
You just overwrite with default KEY & default CA file

1. ***Certification Pass Verification***

   It helps to verify validity of the entire



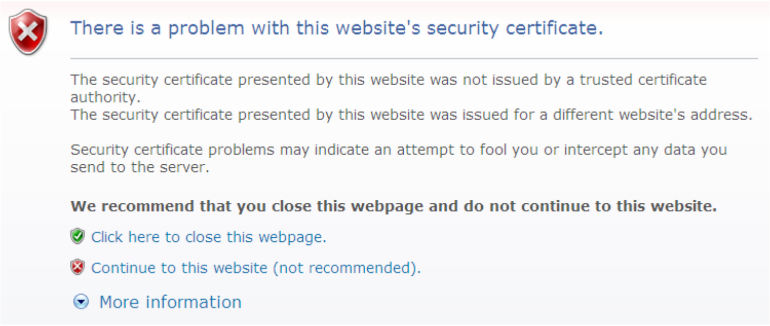
2. ***Alert Message***
   - Administrators' alert message is shown when any invalid certificate in the chain found.



Upload Certificate

Certificate upload error!
Certification Path Verification is failed.

   - Users' alert message is shown when any invalid certificate in the chain found.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

**We recommend that you close this webpage and do not continue to this website.**

Click here to close this webpage.

Continue to this website (not recommended).

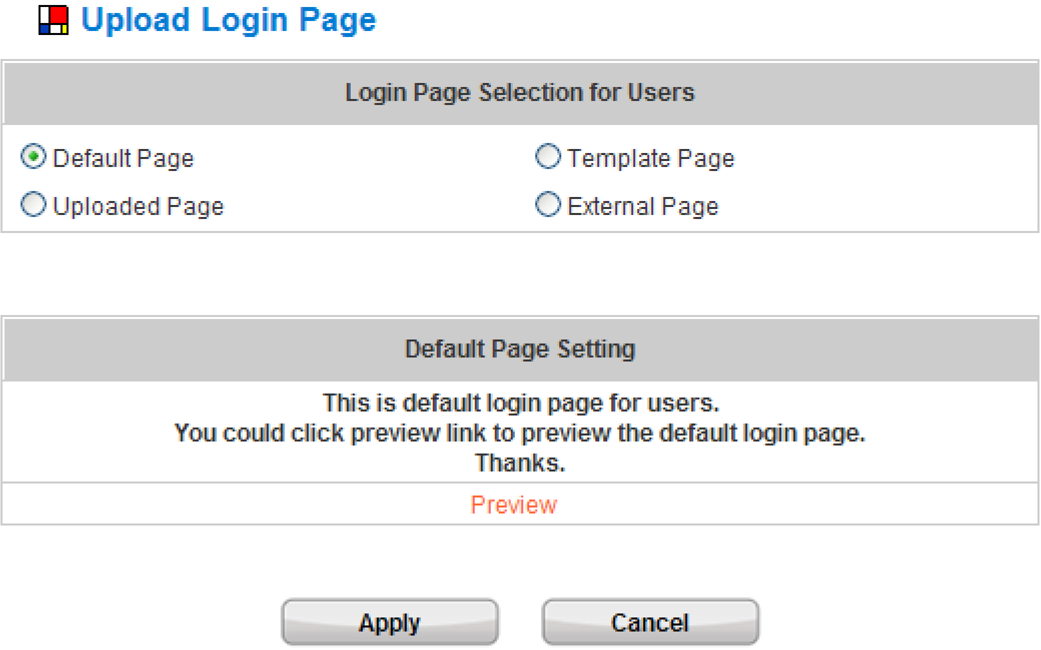
More information

***3. How to avoid Alert Message***

- For Clients, to install Root and Intermediate Certificates:
  1. Obtain ALL certificate files Offline and save them on your desktop.
  2. Click to Install Root CA and Intermediate certificates.
- For Administrators, to install Website Certificate:
  1. Go to “Additional Configuration >> Upload Files>> Certificate”
  2. Upload “Private Key” and “Customer Certificate” to HS1100

➢ **Login Page:** The administrator can use the default login page or get the customized login page by setting the template page, uploading an edited page, or downloading a specific page from the designated website. After finishing the setting, click ***Preview*** to see the login page.

a. Choose ***Default Page*** to use the default login page.



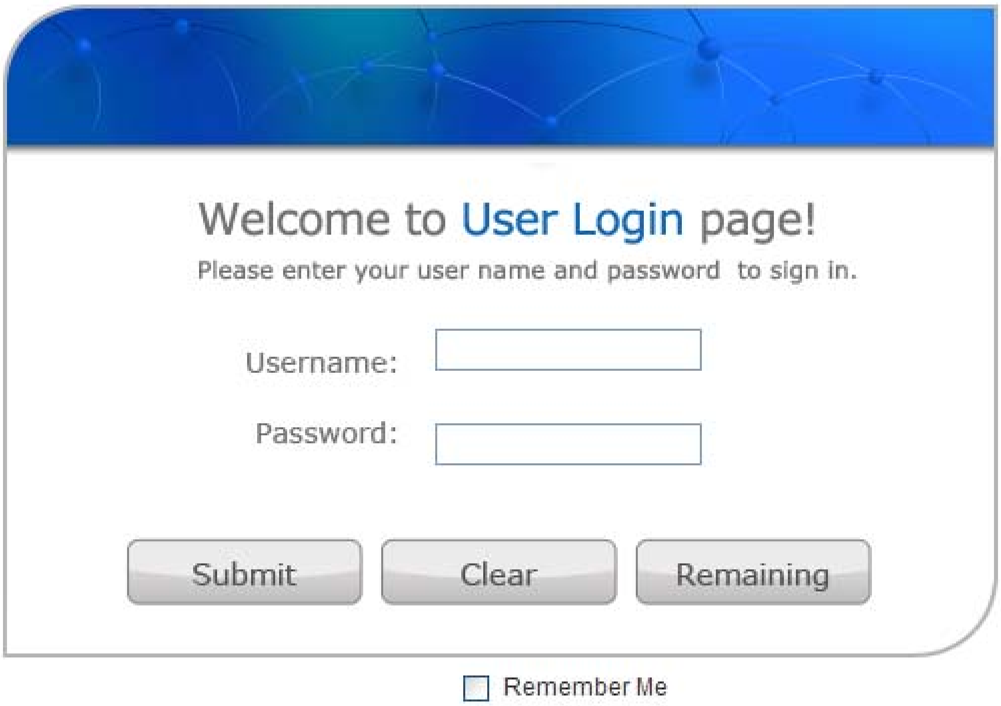
Upload Login Page

Login Page Selection for Users

| | |
|---|---|
| ● Default Page | ○ Template Page |
| ○ Uploaded Page | ○ External Page |

Default Page Setting

This is default login page for users.
You could click preview link to preview the default login page.
Thanks.



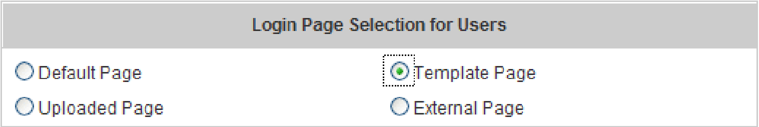
Welcome to User Login page!

Please enter your user name and password to sign in.

Username:

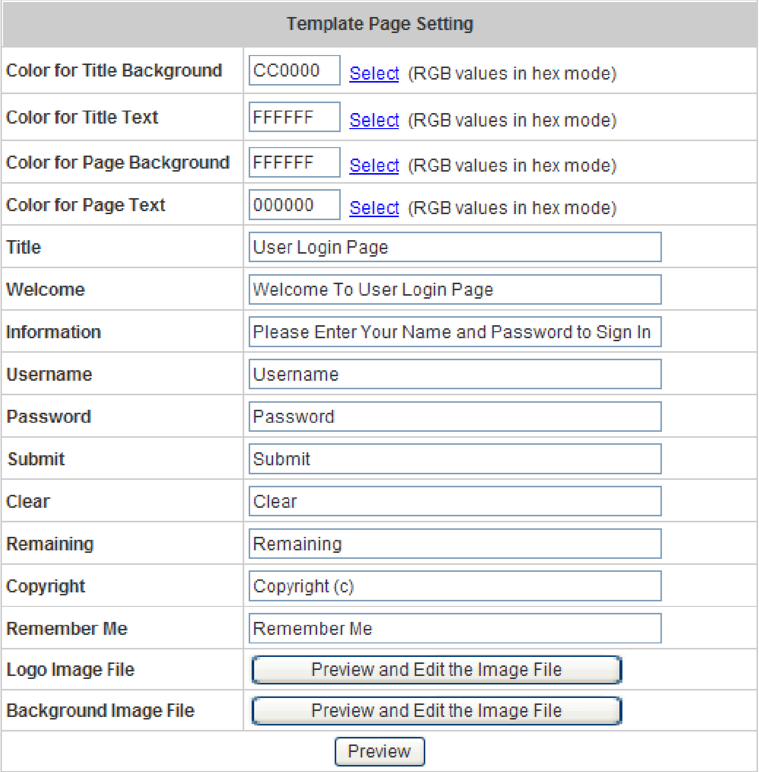
Password:

b. Choose ***Template Page*** to make a customized login page here. Click ***Select*** to pick a color and then fill in all of the blanks. Click ***Preview*** to see the result.



Login Page Selection for Users

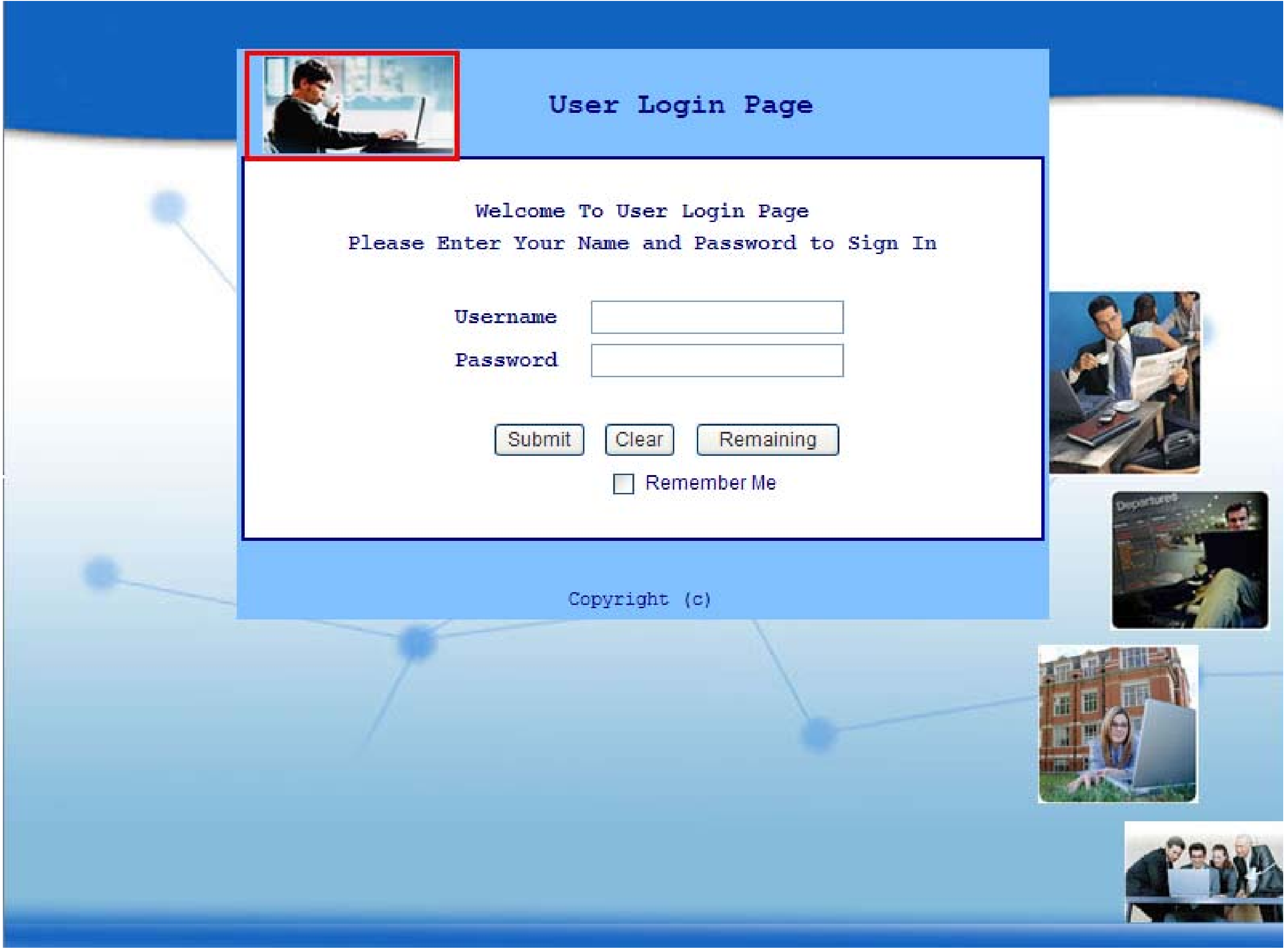
| | |
|---|---|
| ○ Default Page | ● Template Page |
| ○ Uploaded Page | ○ External Page |



Template Page Setting

| | |
|---|---|
| Color for Title Background | CC0000 Select (RGB values in hex mode) |
| Color for Title Text | FFFFFF Select (RGB values in hex mode) |
| Color for Page Background | FFFFFF Select (RGB values in hex mode) |
| Color for Page Text | 000000 Select (RGB values in hex mode) |
| Title | User Login Page |
| Welcome | Welcome To User Login Page |
| Information | Please Enter Your Name and Password to Sign In |
| Username | Username |
| Password | Password |
| Submit | Submit |
| Clear | Clear |
| Remaining | Remaining |
| Copyright | Copyright (c) |
| Remember Me | Remember Me |
| Logo Image File | Preview and Edit the Image File |
| Background Image File | Preview and Edit the Image File |

- ✓ **Logo Image File:** Customized logo can be edited with this function. The area circled in red in the following image is the position of Logo.



User Login Page

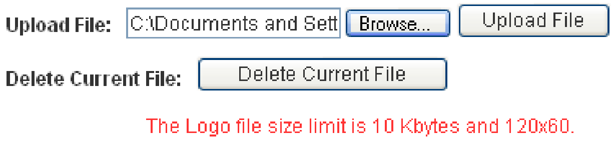
Welcome To User Login Page
Please Enter Your Name and Password to Sign In

Username
Password

Copyright (c)

Click on ***Preview and Edit the Image File*** to enter the editing interface as below.

Click on ***Browse*** to locate the desired image, and press ***Upload File*** to upload the file (the Logo file size limit is 10 Kbytes and 120x60).



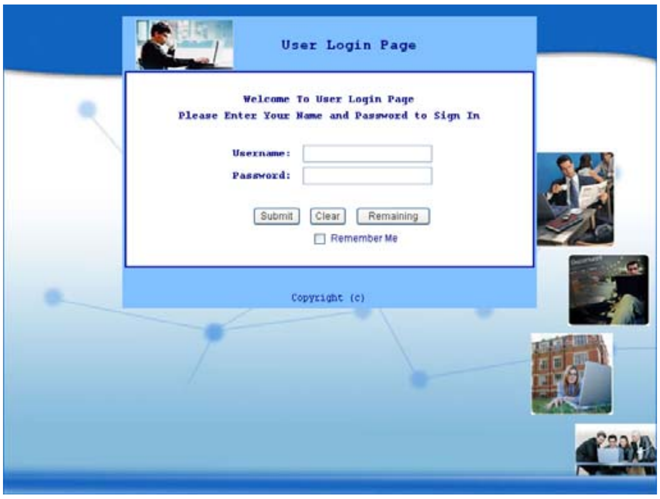
Upload File: C:\Documents and Sett

Delete Current File:

The Logo file size limit is 10 Kbytes and 120x60.

A warning message will appear. Click ***OK*** to complete the upload process.

✓ **Background and Image File:** Click on ***Preview and Edit the Image File*** to enter the editing interface. Repeat the steps of uploading logo image to upload the desired background image. After the logo and background image upload process is completed, the new login Template Page can be previewed by clicking ***Preview*** button at the bottom. The built-in login Template Page is shown as below.



User Login Page

Welcome To User Login Page

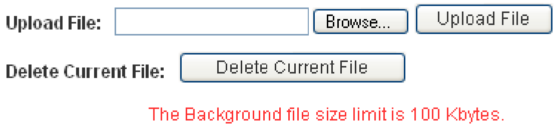
Please Enter Your Name and Password to Sign In

Username:

Password:

□ Remember Me

Copyright (c)

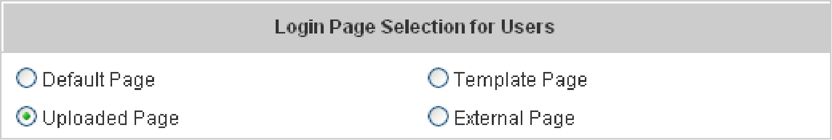


Upload File:

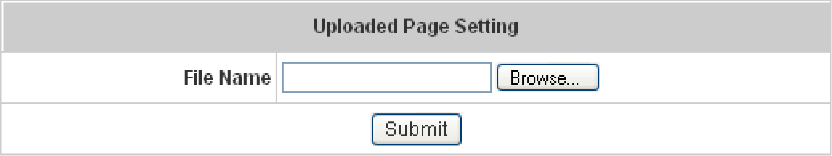
Delete Current File:

The Background file size limit is 100 Kbytes.

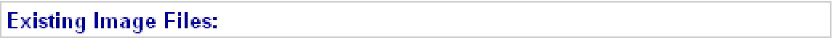
c. Choose ***Uploaded Page*** to upload a new/edited login page. Click the ***Browse*** button to select the file for uploading. Then, click ***Submit*** to complete the upload process.



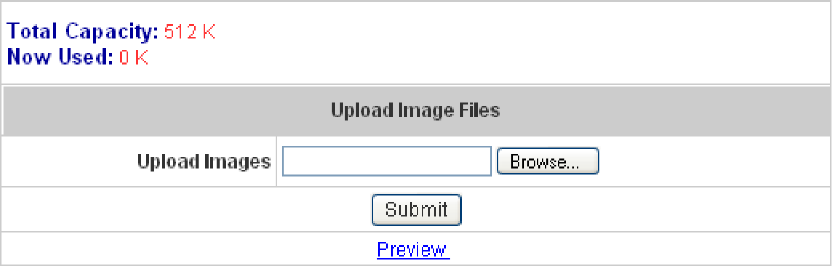
| Login Page Selection for Users | |
|---|---|
| ○ Default Page | ○ Template Page |
| ● Uploaded Page | ○ External Page |



| Uploaded Page Setting | |
|---|---|
| File Name | [ ] Browse... |
| Submit | |



Existing Image Files:

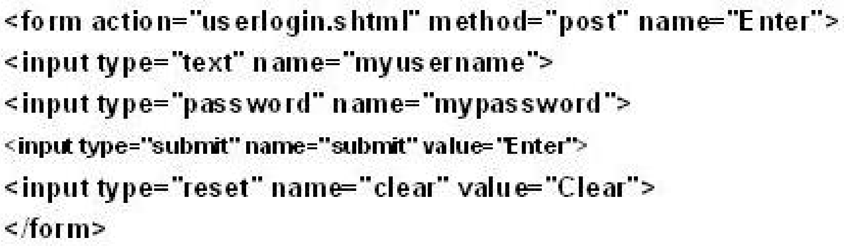


Total Capacity: 512 K
Now Used: 0 K

| Upload Image Files | |
|---|---|
| Upload Images | [ ] Browse... |
| Submit | |
| Preview | |

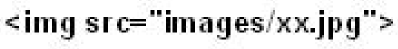
After the upload process is completed, the new login page can be previewed by clicking ***Preview*** button at the bottom.

The admin-defined login page must include the following HTML codes to provide the necessary fields for username and password.



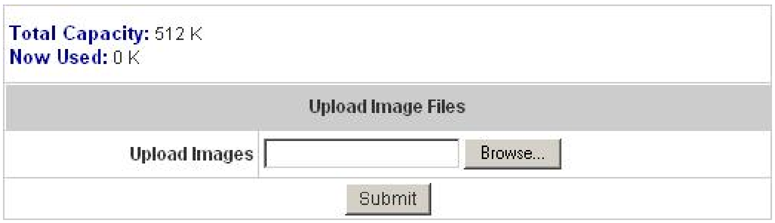
```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

If the admin-defined login page includes an image file, the image file path in the HTML codes must be the filename of the image file to be uploaded.



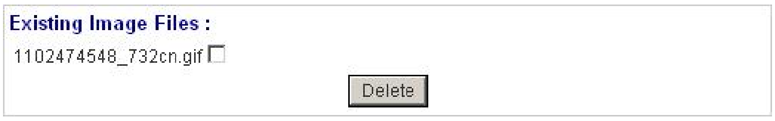
```
<img src="images/xx.jpg">
```

Then, enter or browse the filename of the images to upload in the **"Upload Images"** field on the **"Upload Images Files"** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login page, click the ***Use Default Page*** button to restore it to default.



Total Capacity: 512 K
Now Used: 0 K

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. The administrator can check the file and click ***Delete*** to delete that file.

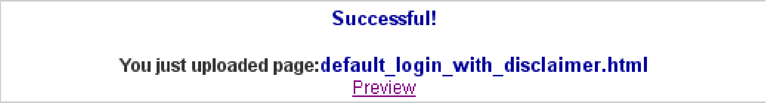


Existing Image Files :
1102474548_732cn.gif ☐

**>> How to edit "Terms of Use" or "Service Disclaimer" page:**

In HS1100, the client first gets a login page when he/she opens a web browser right after associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display "terms of use" or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking "I agree", users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

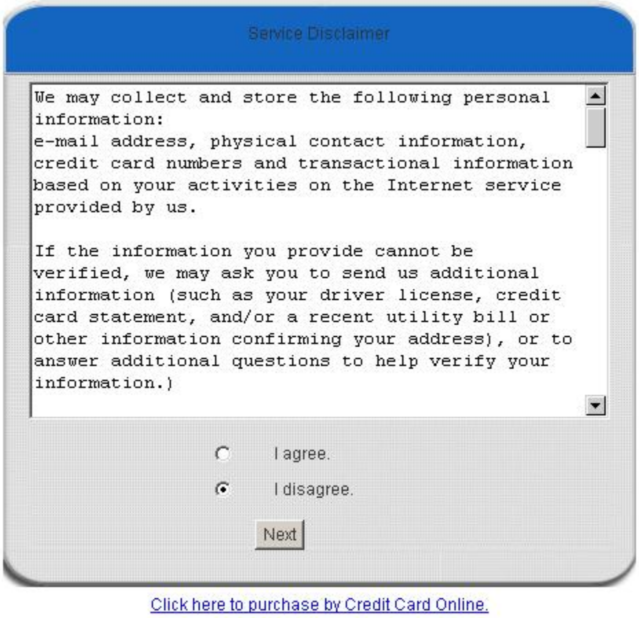
If the disclaimer page is successfully uploaded, an **upload success** page will show up.



Successful!

You just uploaded page:default_login_with_disclaimer.html

Click **"Preview"** to see the uploaded page.



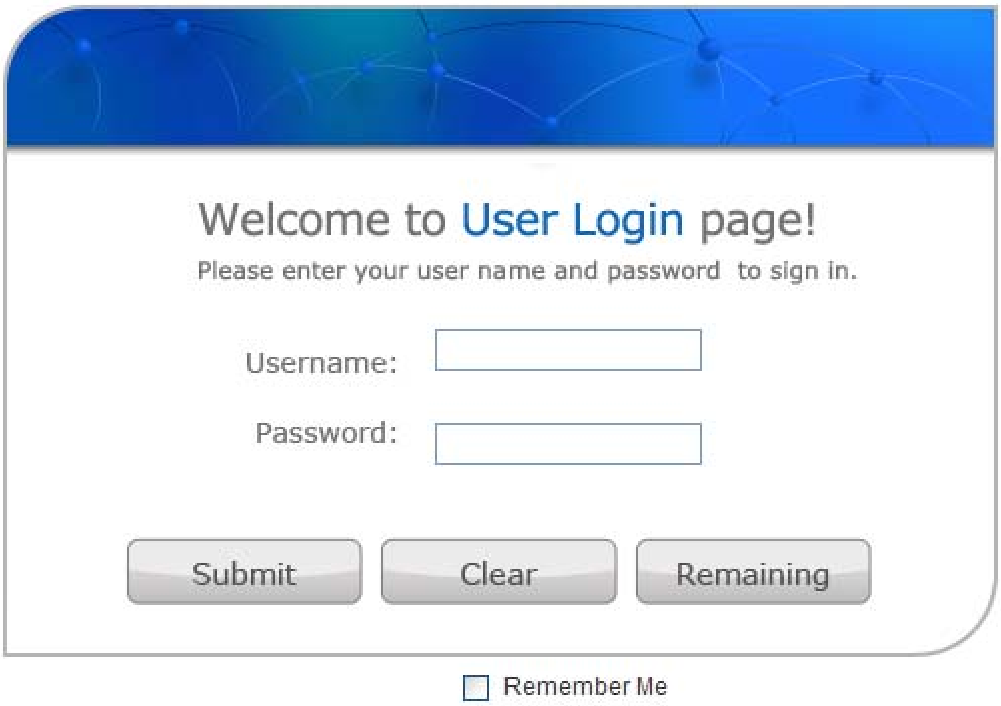
Service Disclaimer

```
We may collect and store the following personal
information:
e-mail address, physical contact information,
credit card numbers and transactional information
based on your activities on the Internet service
provided by us.

If the information you provide cannot be
verified, we may ask you to send us additional
information (such as your driver license, credit
card statement, and/or a recent utility bill or
other information confirming your address), or to
answer additional questions to help verify your
information.)
```

○ I agree.

● I disagree.

If the user checks **"I agree"** and clicks ***Next***, then he/she is prompted to fill in Login Name and Password.



Welcome to User Login page!

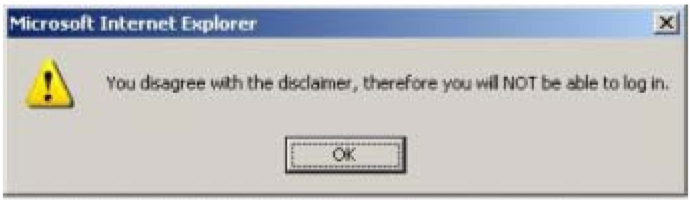
Please enter your user name and password to sign in.

Username:

Password:

□ Remember Me

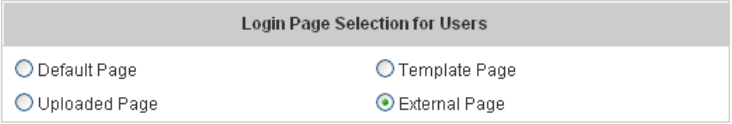
If the user checks **"I disagree"** and clicks ***Next***, a window shown as below will pop up to tell the user that he/she cannot log in.



Microsoft Internet Explorer

You disagree with the disclamer, therefore you will NOT be able to log in.

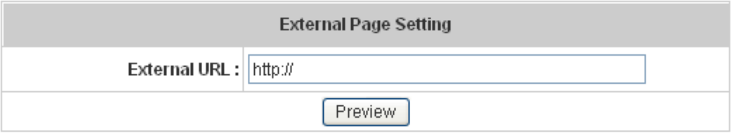
d. Choose ***External Page*** and get the login page from the designated website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***.



Login Page Selection for Users

○ Default Page ○ Template Page

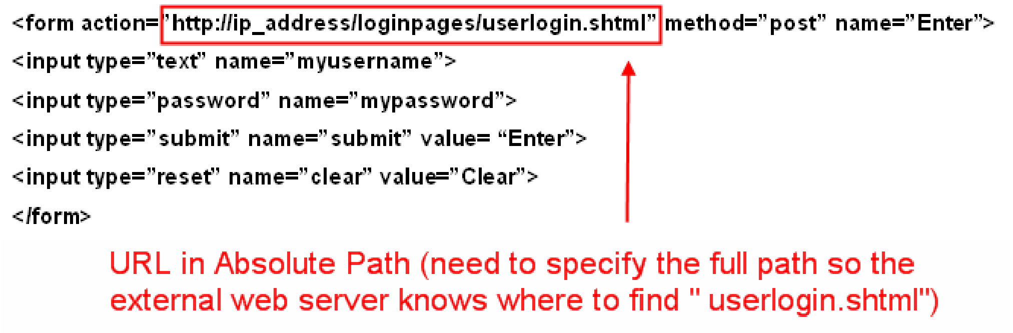
○ Uploaded Page ● External Page



External Page Setting

External URL : http://

The **External Page** prepared to be downloaded here must have the following HTML codes to ensure the system can work properly

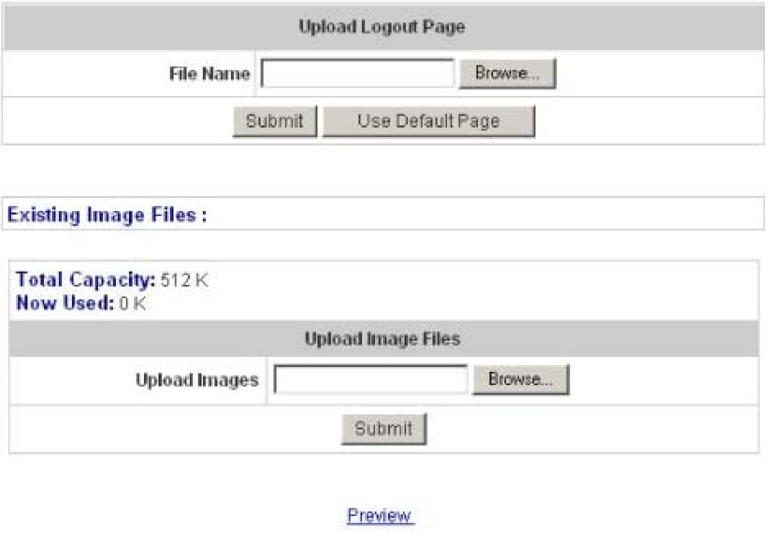


```
<form action="http://ip_address/loginpages/userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value= "Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

URL in Absolute Path (need to specify the full path so the external web server knows where to find " userlogin.shtml")

After applying the setting, the new login page can be previewed by clicking ***Preview*** button at the bottom of this page.

- **Logout Page:** The administrator can apply a new/edited logout page here. The process is similar to that of Login Page.



Upload Logout Page

File Name

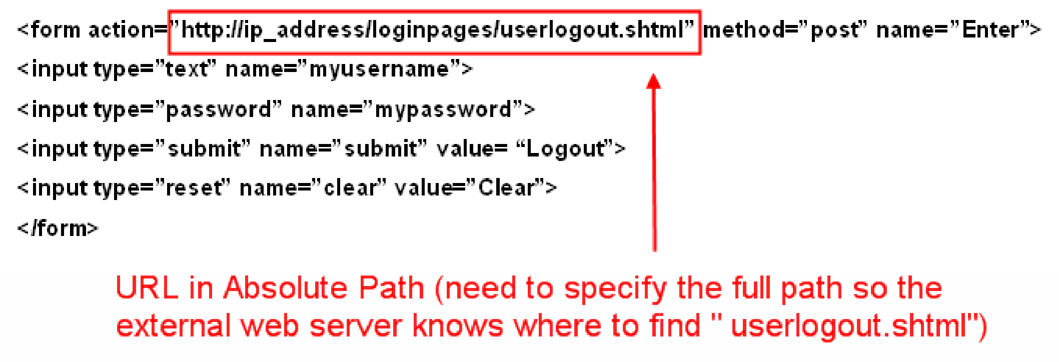
Existing Image Files :

Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

Upload Images

The different part is the HTML codes of the admin-defined logout page must include the following HTML codes to allow users to enter the username and password. After the upload is completed, the admin-defined logout page can be previewed by clicking ***Preview*** at the bottom of this page. If the administrator wants to restore the factory default setting of the logout interface, click the "**Use Default Page"** button.

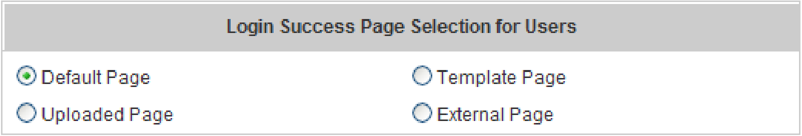


```
<form action="http://ip_address/loginpages/userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value= "Logout">
<input type="reset" name="clear" value="Clear">
</form>
```

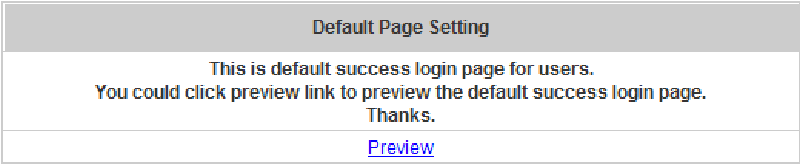
URL in Absolute Path (need to specify the full path so the external web server knows where to find " userlogout.shtml")

- **Login Success Page:** The administrator can use the default login success page or get the customized login success page by setting the template page, uploading an edited page or downloading a specific page from the designated website. After finishing the setting, click ***Preview*** to see the login success page.

a. Choose ***Default Page*** to use the default login success page.



| Login Success Page Selection for Users | |
|---|---|
| ● Default Page | ○ Template Page |
| ○ Uploaded Page | ○ External Page |

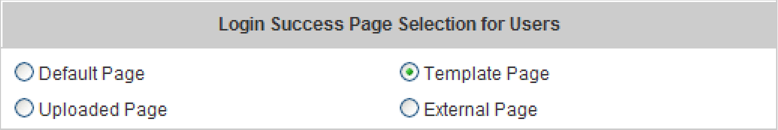


Default Page Setting

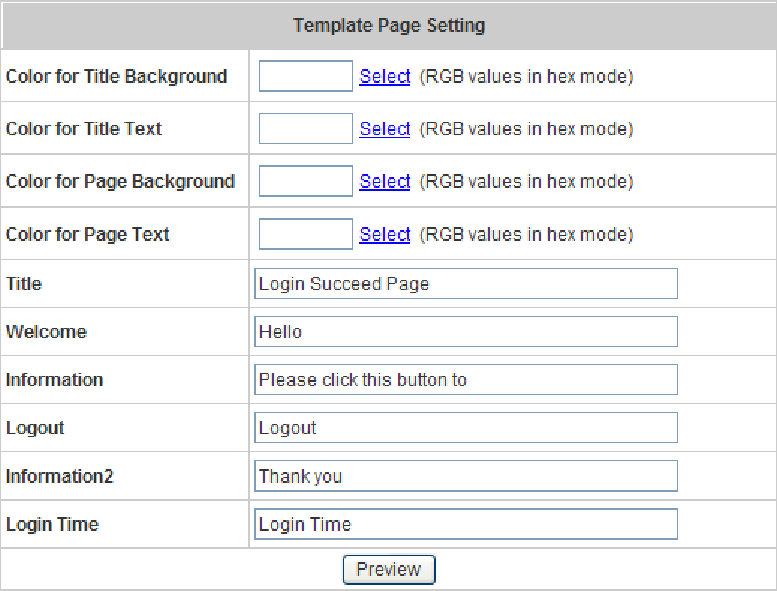
This is default success login page for users.
You could click preview link to preview the default success login page.
Thanks.

Preview

b. Choose ***Template Page*** to make a customized login success page here. Click ***Select*** to pick a color and then fill in all of the blanks. Click ***Preview*** to see the result first.

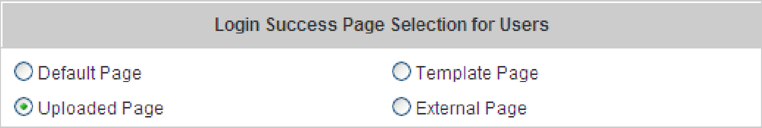


| Login Success Page Selection for Users | |
|---|---|
| ○ Default Page | ● Template Page |
| ○ Uploaded Page | ○ External Page |



| Template Page Setting | |
|---|---|
| Color for Title Background | Select (RGB values in hex mode) |
| Color for Title Text | Select (RGB values in hex mode) |
| Color for Page Background | Select (RGB values in hex mode) |
| Color for Page Text | Select (RGB values in hex mode) |
| Title | Login Succeed Page |
| Welcome | Hello |
| Information | Please click this button to |
| Logout | Logout |
| Information2 | Thank you |
| Login Time | Login Time |

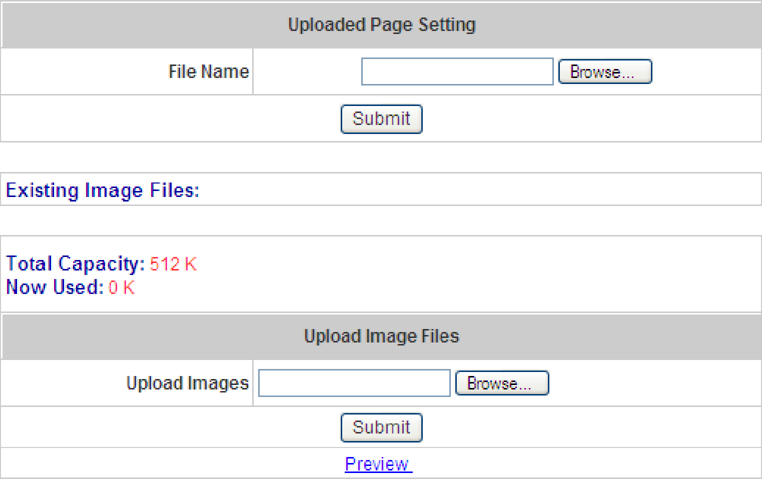
c. Choose ***Uploaded Page*** and upload a new/edited login success page. Click the ***Browse*** button to select the file for uploading. Then, click ***Submit*** to complete the upload process.



Login Success Page Selection for Users

○ Default Page ○ Template Page

● Uploaded Page ○ External Page



Uploaded Page Setting

File Name [ ] Browse...

Submit

Existing Image Files:

Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

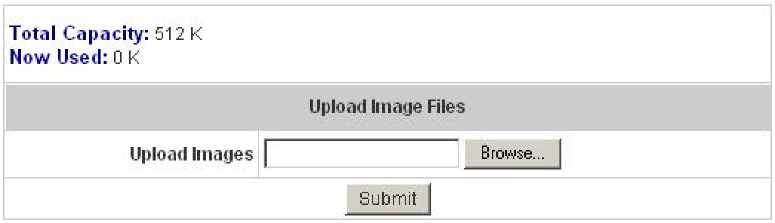
Upload Images [ ] Browse...

Submit

Preview

After the upload process is completed, the new login success page can be previewed by clicking ***Preview*** button at the bottom.

Enter or browse the filename of the images to upload in the **"Upload Images"** field on the **"Upload Images Files"** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login success page, click the ***Use Default Page*** button to restore it to default.



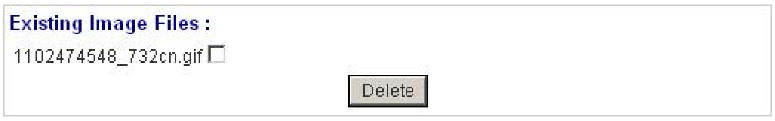
Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

Upload Images [ ] Browse...

Submit

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. The administrator can check the file and click ***Delete*** to delete the file.

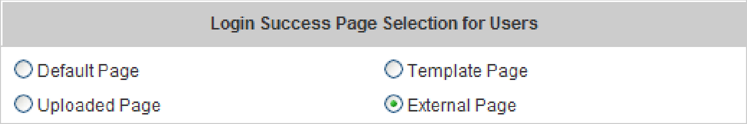


Existing Image Files :

1102474548_732cn.gif □

Delete

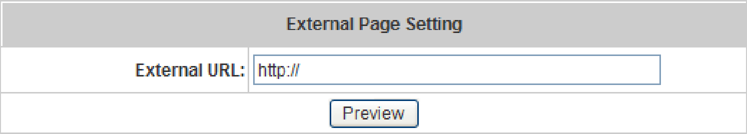
d. Choose ***External Page*** and down a specific login success page from the designated website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***. After applying the setting, the new login success page can be previewed by clicking ***Preview*** button at the bottom of this page.



Login Success Page Selection for Users

○ Default Page ○ Template Page

○ Uploaded Page ● External Page

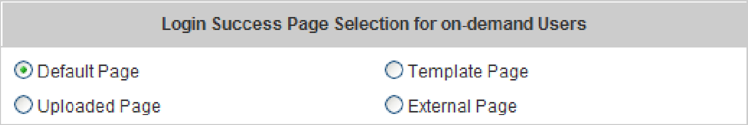


External Page Setting

External URL: http://

- ➢ **Login Success Page for On-Demand:** The administrator can use the default login success page for on-demand users or get the customized login success page by setting the template page, uploading an edited page or downloading a specific page from the designated website. After finishing the setting, click ***Preview*** to see the login success page for on-demand users.

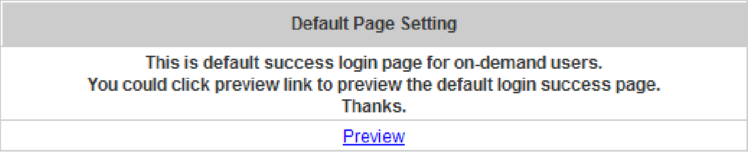
a. Choose ***Default Page*** to use the default login success page for on-demand users.



Login Success Page Selection for on-demand Users

● Default Page ○ Template Page

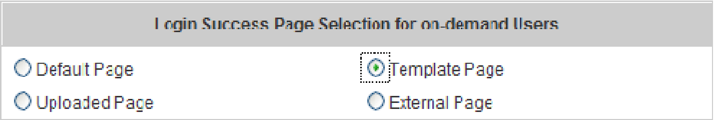
○ Uploaded Page ○ External Page



Default Page Setting

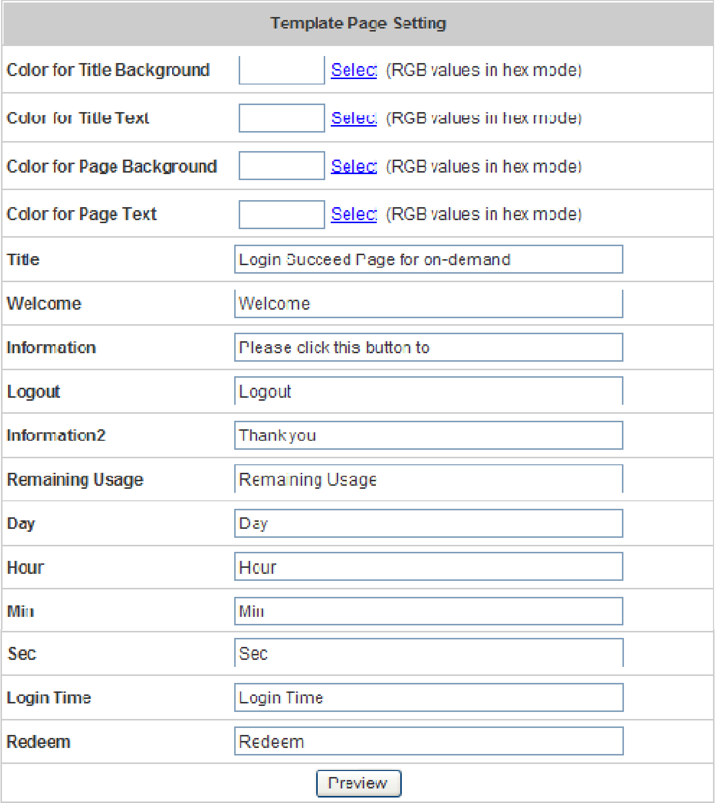
This is default success login page for on-demand users.
You could click preview link to preview the default login success page.
Thanks.

b. Choose ***Template Page*** to make a customized login success page for on-demand users here. Click ***Select*** to pick a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



Login Success Page Selection for on-demand Users

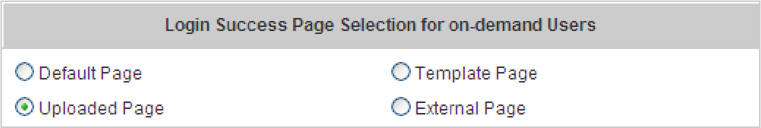
| | |
|---|---|
| ○ Default Page | ● Template Page |
| ○ Uploaded Page | ○ External Page |



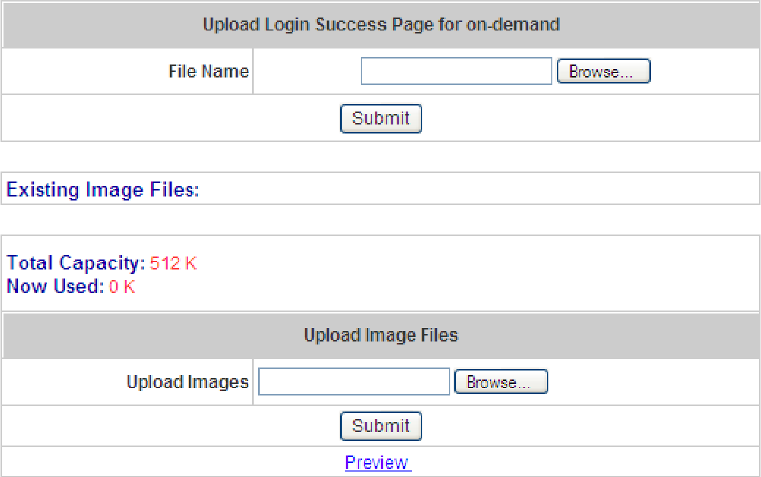
Template Page Setting

| | | |
|---|---|---|
| Color for Title Background | | Select (RGB values in hex mode) |
| Color for Title Text | | Select (RGB values in hex mode) |
| Color for Page Background | | Select (RGB values in hex mode) |
| Color for Page Text | | Select (RGB values in hex mode) |
| Title | Login Succeed Page for on-demand | |
| Welcome | Welcome | |
| Information | Please click this button to | |
| Logout | Logout | |
| Information2 | Thank you | |
| Remaining Usage | Remaining Usage | |
| Day | Day | |
| Hour | Hour | |
| Min | Min | |
| Sec | Sec | |
| Login Time | Login Time | |
| Redeem | Redeem | |

c. Choose ***Uploaded Page*** and click the ***Browse*** button to select the file for uploading. Then, click ***Submit*** to complete the upload process.



| Login Success Page Selection for on-demand Users | |
|---|---|
| ○ Default Page | ○ Template Page |
| ● Uploaded Page | ○ External Page |



| Upload Login Success Page for on-demand | |
|---|---|
| File Name | Browse... |
| Submit | |

Existing Image Files:

Total Capacity: 512 K
Now Used: 0 K

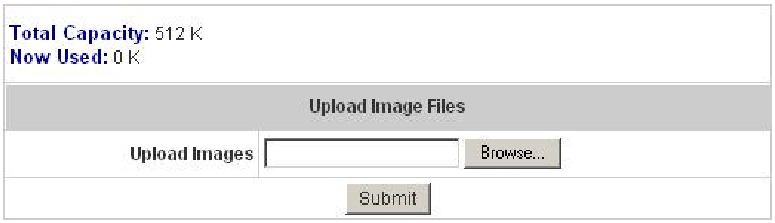
| Upload Image Files | |
|---|---|
| Upload Images | Browse... |
| Submit | |
| Preview | |

After the upload process is completed, the new login success page for on-demand users can be previewed by clicking ***Preview*** button at the bottom.

If the admin-defined login success page for on-demand users includes an image file, the image file path in the HTML codes must be the image file to be uploaded.

```
<img src="images/xx.jpg">
```

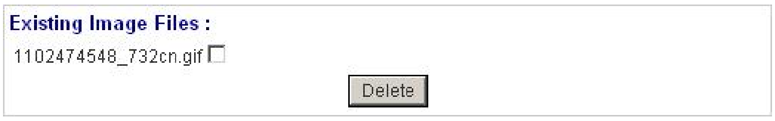
Enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login success page for on-demand users, click the ***Use Default Page*** button to restore it to default.



Total Capacity: 512 K
Now Used: 0 K

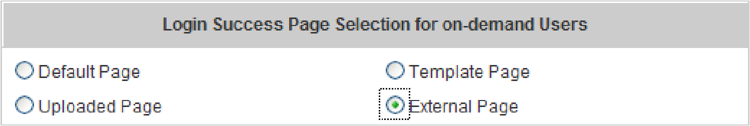
| Upload Image Files | |
|---|---|
| Upload Images | Browse... |
| Submit | |

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.



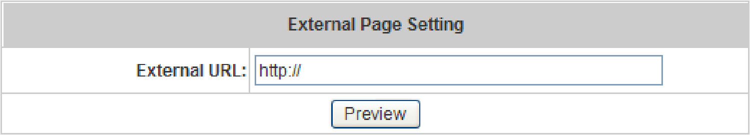
Existing Image Files :
1102474548_732cn.gif □
Delete

d. Choose the ***External Page*** selection and get the login success page for on-demand users from a specific website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***. After applying the setting, the new login success page for on-demand users can be previewed by clicking ***Preview*** button at the bottom of this page.



Login Success Page Selection for on-demand Users

| | |
|---|---|
| ○ Default Page | ○ Template Page |
| ○ Uploaded Page | ● External Page |



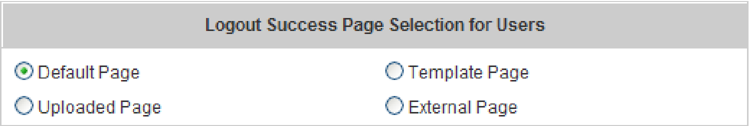
External Page Setting

| | |
|---|---|
| External URL: | http:// |

Preview

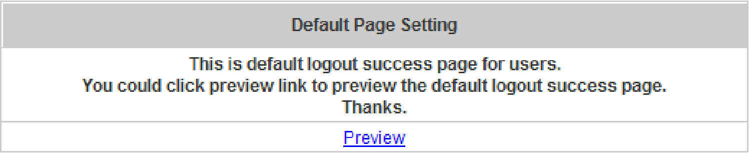
- **Logout Success Page:** The administrator can use the default logout success page or get the customized login success page by setting the template page, uploading the page or downloading from a specific website. After finishing the setting, click ***Preview*** to see the logout success page.

a. Choose ***Default Page*** to use the default logout success page.



Logout Success Page Selection for Users

| | |
|---|---|
| ● Default Page | ○ Template Page |
| ○ Uploaded Page | ○ External Page |

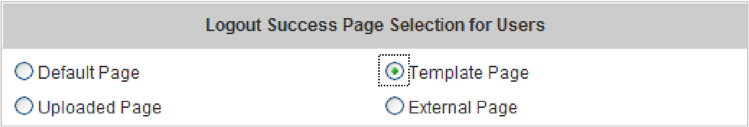


Default Page Setting

This is default logout success page for users.
You could click preview link to preview the default logout success page.
Thanks.

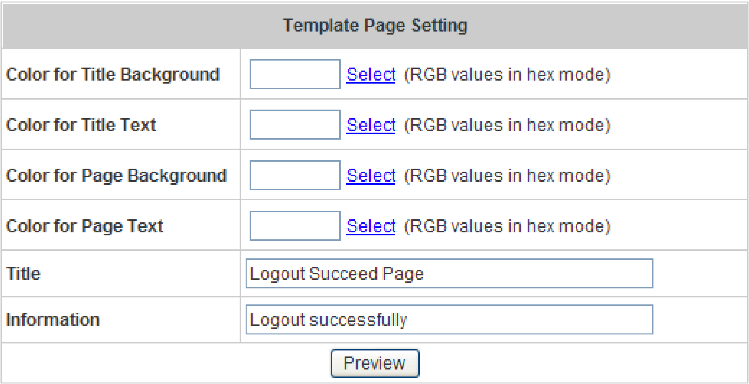
Preview

b. Choose ***Template Page*** to make a customized logout success page here. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



Logout Success Page Selection for Users

| | |
|---|---|
| ○ Default Page | ● Template Page |
| ○ Uploaded Page | ○ External Page |

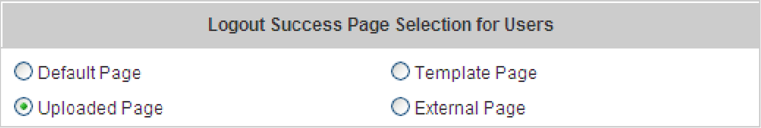


Template Page Setting

| | |
|---|---|
| Color for Title Background | Select (RGB values in hex mode) |
| Color for Title Text | Select (RGB values in hex mode) |
| Color for Page Background | Select (RGB values in hex mode) |
| Color for Page Text | Select (RGB values in hex mode) |
| Title | Logout Succeed Page |
| Information | Logout successfully |

Preview

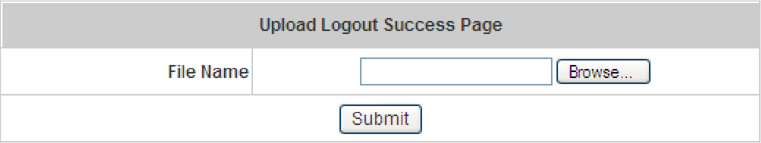
c. Choose ***Uploaded Page*** and click the ***Browse*** button to select the file for the logout success page upload. Then click ***Submit*** to complete the upload process.



Logout Success Page Selection for Users

○ Default Page ○ Template Page

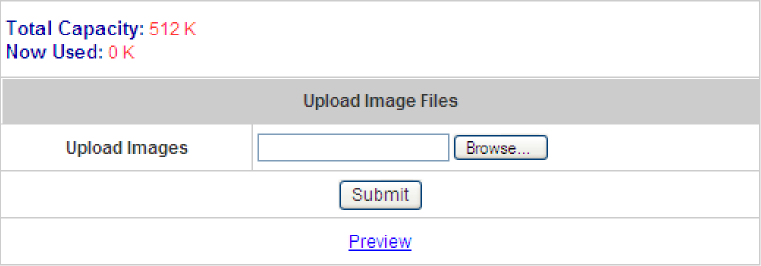
● Uploaded Page ○ External Page



Upload Logout Success Page

| | |
|---|---|
| File Name | Browse... |
| Submit | |

Existing Image Files:



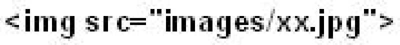
Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

| | |
|---|---|
| Upload Images | Browse... |
| Submit | |
| Preview | |

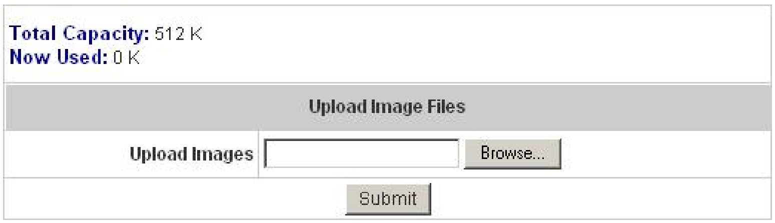
After the upload process is completed, the new logout success page can be previewed by clicking ***Preview*** button at the bottom.

If the user-defined logout success page includes an image file, the image file path in the HTML code must be the filename of the image file to be uploaded.



```
<img src="images/xx.jpg">
```

Enter or browse the filename of the images to upload in the **"Upload Images"** field on the **"Upload Images Files"** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the logout success page, click the ***Use Default Page*** button to restore it to default.

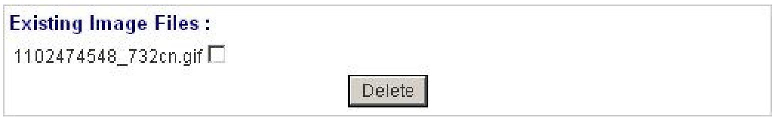


Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

| | |
|---|---|
| Upload Images | Browse... |
| Submit | |

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. The administrator can check the file and click ***Delete*** to delete it.

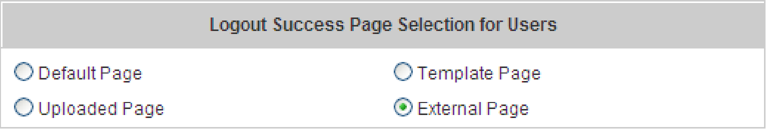


Existing Image Files :

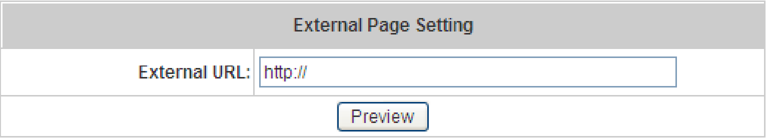
1102474548_732cn.gif □

Delete

d. Choose ***External Page*** and get a specific logout success page from the designated website. Enter the website address in the **"External Page Setting"** field and then click ***Apply***. After applying the setting, the new logout success page can be previewed by clicking ***Preview*** button at the bottom of this page.

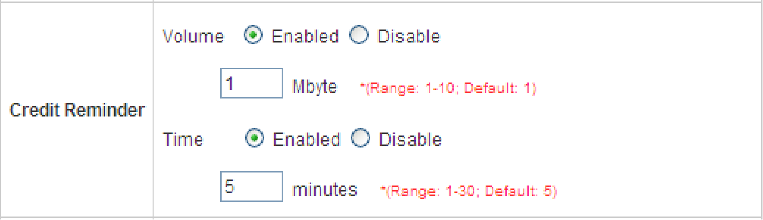


| Logout Success Page Selection for Users | |
|---|---|
| ○ Default Page | ○ Template Page |
| ○ Uploaded Page | ● External Page |



| External Page Setting | |
|---|---|
| External URL: | http:// |

- **Credit Reminder:** The administrator can enable this function to remind the on-demand users before their credit runs out. There are two kinds of reminder, **Volume** and **Time**. The default reminding trigger level for **Volume** is 1Mbyte and the level for **Time** is 5 minutes.



Credit Reminder

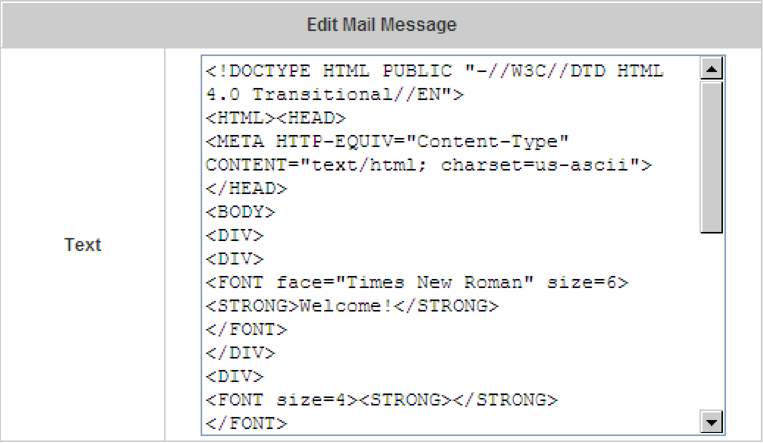
Volume ● Enabled ○ Disable

1 Mbyte *(Range: 1-10; Default: 1)

Time ● Enabled ○ Disable

5 minutes *(Range: 1-30; Default: 5)

- **POP3 Message:** Before users log into the network with their usernames and passwords, users will receive a welcome mail from HS1100. To edit the content, click the hyperlink of ***Edit Mail Message*** to enter the text edit page.

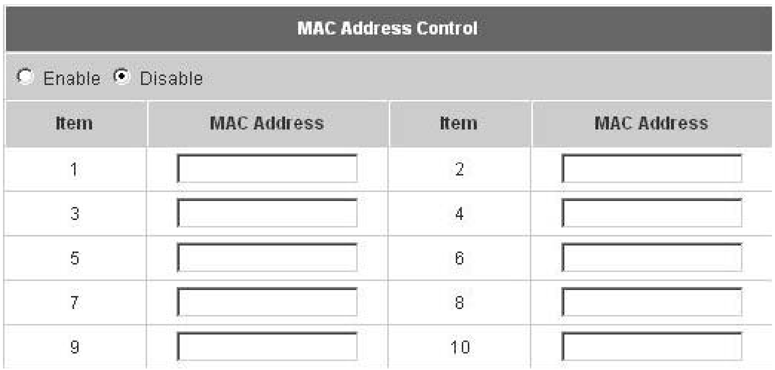


Edit Mail Message

Text

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML
4.0 Transitional//EN">
<HTML><HEAD>
<META HTTP-EQUIV="Content-Type"
CONTENT="text/html; charset=us-ascii">
</HEAD>
<BODY>
<DIV>
<DIV>
<FONT face="Times New Roman" size=6>
<STRONG>Welcome!</STRONG>
</FONT>
</DIV>
<DIV>
<FONT size=4><STRONG></STRONG>
</FONT>
```

- **Enhance User Authentication:** If enabled, only the users with their MAC addresses in this list can log into HS1100. However, user authentication is still required for these users. To specify the MAC addresses, click the hyperlink of ***Permit MAC Address List*** to enter the **"MAC Address Control"** page and fill in the MAC addresses. Select **Enable** and then click ***Apply***.



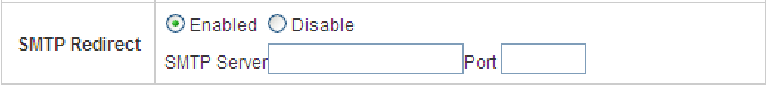
MAC Address Control

○ Enable ● Disable

| Item | MAC Address | Item | MAC Address |
|---|---|---|---|
| 1 | | 2 | |
| 3 | | 4 | |
| 5 | | 6 | |
| 7 | | 8 | |
| 9 | | 10 | |

*The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.*

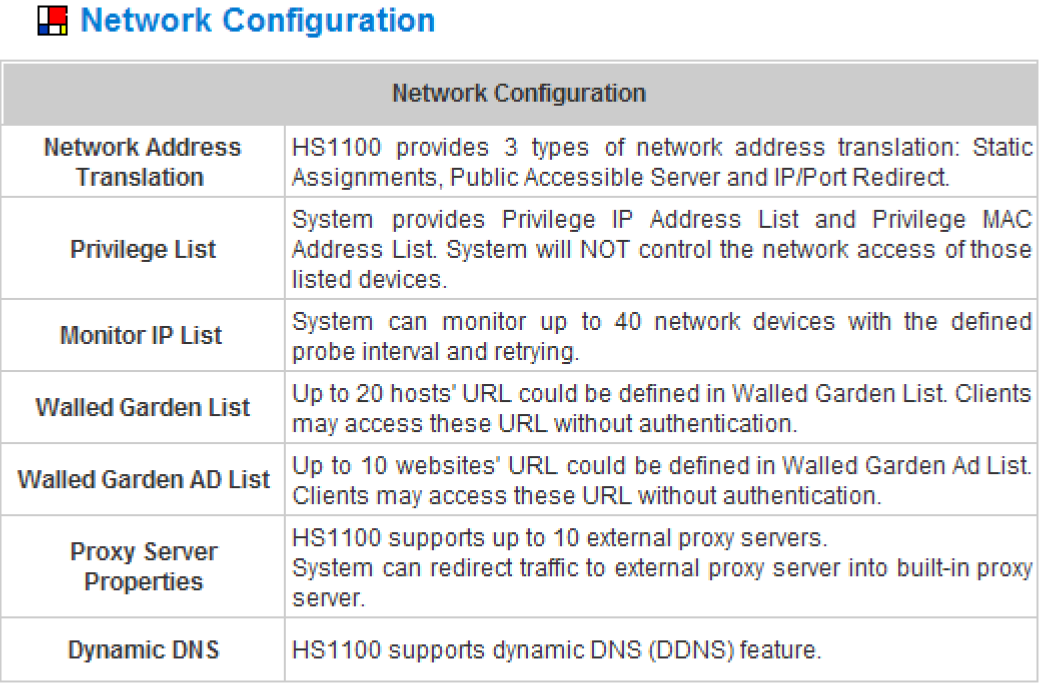
- **SMTP Redirect:** If enabled, please configure IP address of SMTP server and the port number of the SMTP server here.



| | |
|---|---|
| SMTP Redirect | ● Enabled ○ Disable<br>SMTP Server Port |

# Network Configuration

This section includes the following functions: **Network Address Translation**, **Privilege List**, **Monitor IP List**, **Walled Garden List**, **Walled Garden AD List**, **Proxy Server Properties** and **Dynamic DNS**.

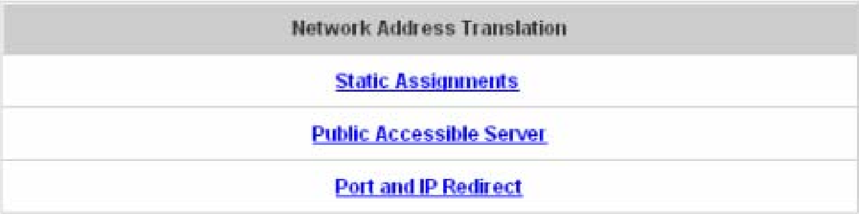


Network Configuration

| Network Configuration | |
|---|---|
| **Network Address Translation** | HS1100 provides 3 types of network address translation: Static Assignments, Public Accessible Server and IP/Port Redirect. |
| **Privilege List** | System provides Privilege IP Address List and Privilege MAC Address List. System will NOT control the network access of those listed devices. |
| **Monitor IP List** | System can monitor up to 40 network devices with the defined probe interval and retrying. |
| **Walled Garden List** | Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication. |
| **Walled Garden AD List** | Up to 10 websites' URL could be defined in Walled Garden Ad List. Clients may access these URL without authentication. |
| **Proxy Server Properties** | HS1100 supports up to 10 external proxy servers.<br>System can redirect traffic to external proxy server into built-in proxy server. |
| **Dynamic DNS** | HS1100 supports dynamic DNS (DDNS) feature. |

## Network Address Translation

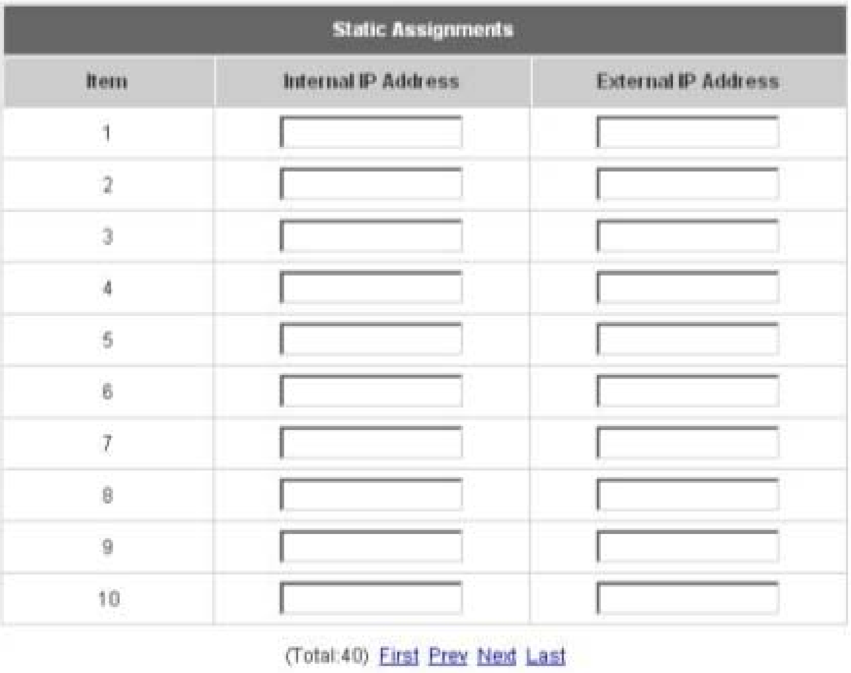
Set the configuration for **Static Assignments, Public Accessible Server** and **Port and Redirect**.



| Network Address Translation |
|---|
| Static Assignments |
| Public Accessible Server |
| Port and IP Redirect |

- **Static Assignments**

  The administrator can define mandatory external to internal IP mapping, so that a client on HS1100's WAN can access the managed machine (e.g. a PC, a system) on HS1100's LAN by accessing the external IP. There are 40 sets of static **Internal IP Address** and **External IP Address** available. Enter **Internal** and **External** IP Addresses as a set. After the setup, accessing the WAN will be mapped to access the Internal IP Address. These settings will become effective immediately after clicking the ***Apply*** button.



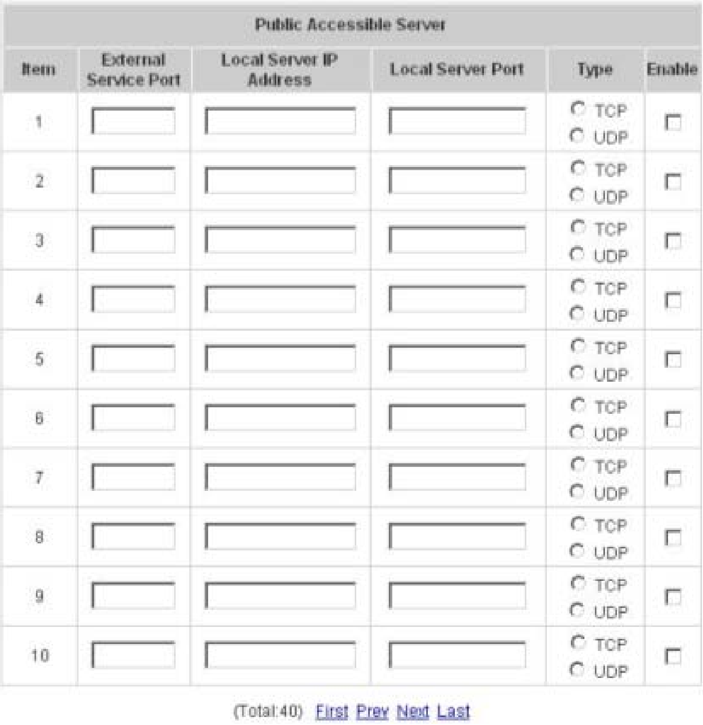
Static Assignments

| Item | Internal IP Address | External IP Address |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

(Total:40) First Prev Next Last

- **Public Accessible Server**

  This function allows the administrator to set 40 virtual servers at most, so that client devices outside the managed network can access these servers within the managed network. Different virtual servers can be configured for different sets of physical services, such as TCP and UDP services in general. Enter the **"External Service Port"**, **"Local Server IP Address"** and **"Local Server Port"**. Select **"TCP"** or **"UDP"** for the service's type. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the ***Apply*** button.

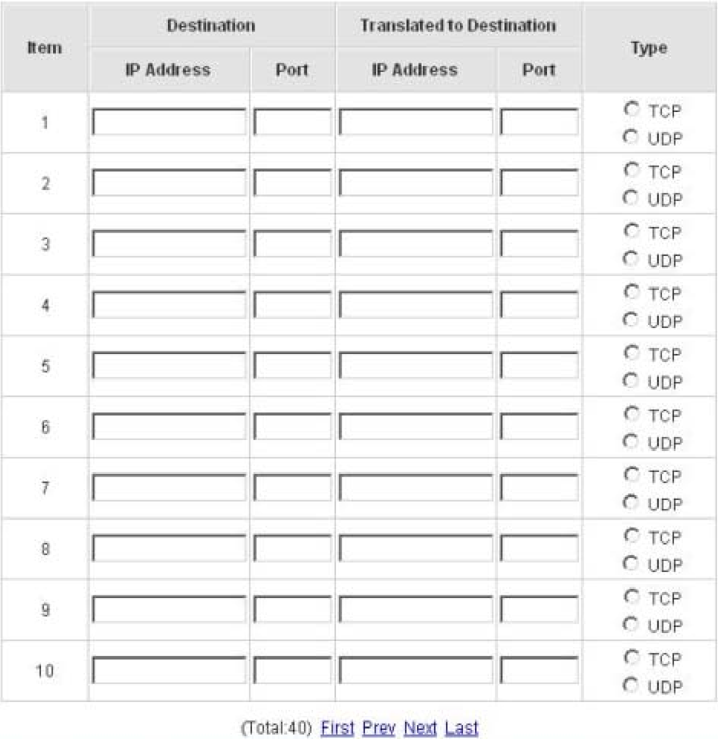


| Public Accessible Server | | | | | |
|---|---|---|---|---|---|
| Item | External Service Port | Local Server IP Address | Local Server Port | Type | Enable |
| 1 | | | | ○ TCP<br>○ UDP | □ |
| 2 | | | | ○ TCP<br>○ UDP | □ |
| 3 | | | | ○ TCP<br>○ UDP | □ |
| 4 | | | | ○ TCP<br>○ UDP | □ |
| 5 | | | | ○ TCP<br>○ UDP | □ |
| 6 | | | | ○ TCP<br>○ UDP | □ |
| 7 | | | | ○ TCP<br>○ UDP | □ |
| 8 | | | | ○ TCP<br>○ UDP | □ |
| 9 | | | | ○ TCP<br>○ UDP | □ |
| 10 | | | | ○ TCP<br>○ UDP | □ |

(Total:40) First Prev Next Last

- **Port and IP Redirect**

  This function allows the administrator to set 40 sets of the IP addresses at most for redirection purpose. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the **"IP Address"** and **"Port"** of **Destination**, and the **"IP Address"** and **"Port"** of **Translated to Destination**. Select **"TCP"** or **"UDP"** for the service's type. These settings will become effective immediately after clicking ***Apply***.

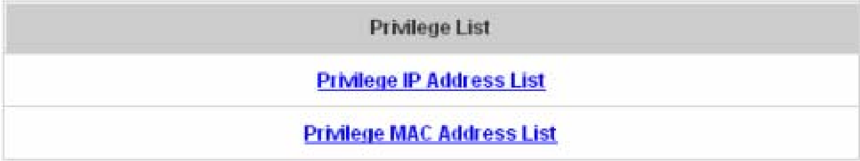


| Item | Destination | | Translated to Destination | | Type |
|---|---|---|---|---|---|
| | IP Address | Port | IP Address | Port | |
| 1 | | | | | ○ TCP<br>○ UDP |
| 2 | | | | | ○ TCP<br>○ UDP |
| 3 | | | | | ○ TCP<br>○ UDP |
| 4 | | | | | ○ TCP<br>○ UDP |
| 5 | | | | | ○ TCP<br>○ UDP |
| 6 | | | | | ○ TCP<br>○ UDP |
| 7 | | | | | ○ TCP<br>○ UDP |
| 8 | | | | | ○ TCP<br>○ UDP |
| 9 | | | | | ○ TCP<br>○ UDP |
| 10 | | | | | ○ TCP<br>○ UDP |

(Total:40) First Prev Next Last

## Privilege List

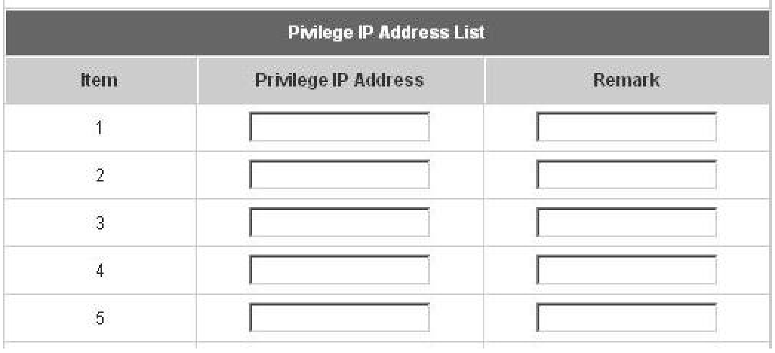
Set the configuration for **Privilege IP Address List** and **Privilege MAC Address List**.



| Privilege List |
|---|
| Privilege IP Address List |
| Privilege MAC Address List |

- **Privilege IP Address List**

  If there are workstations inside the managed network that need to access the network without authentication, enter the IP addresses of these workstations in the **"Privilege IP Address List"**. The **"Remark"** field is not necessary but is useful to keep track. HS1100 allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking ***Apply***.



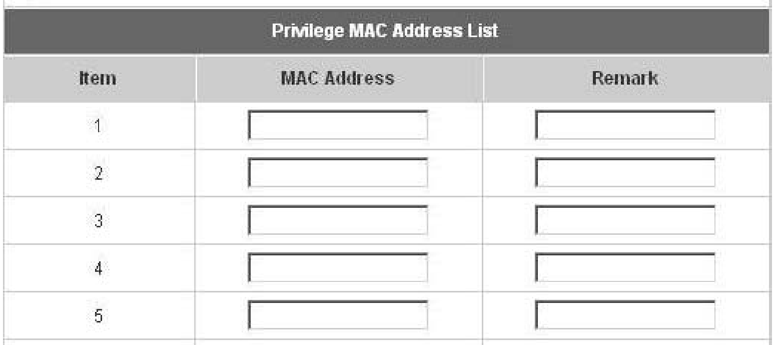
Pivilege IP Address List

| Item | Privilege IP Address | Remark |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

*Permitting specific IP addresses to have network access rights without going through standard authentication process at the Public LAN (LAN1/LAN2 by default) may cause security problems.*

- **Privilege MAC Address List**

  In addition to the IP address, the MAC address of the workstations that need to access the network without authentication can also be set in the **"Privilege MAC Address List"**. HS1100 allows 100 privilege MAC addresses at most. When manually creating the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (not necessary). These settings will become effective immediately after clicking ***Apply***.



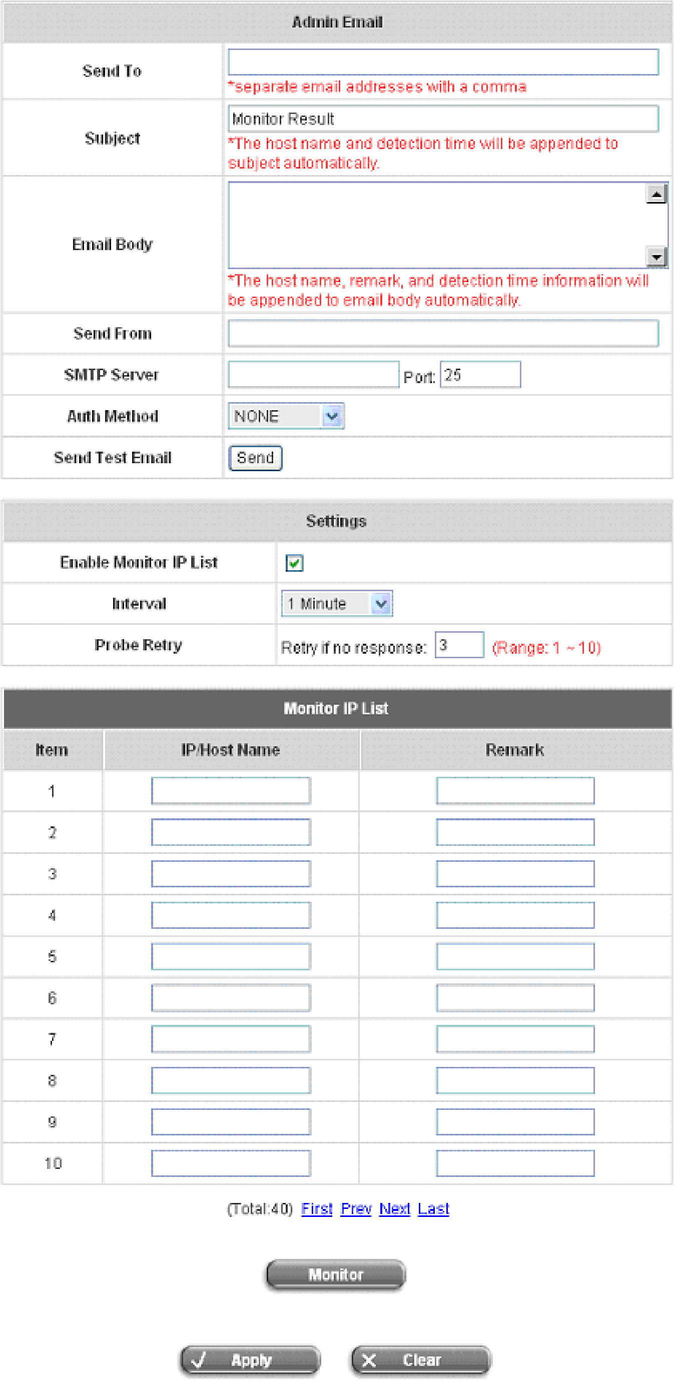
Privilege MAC Address List

| Item | MAC Address | Remark |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

*Permitting specific MAC addresses to have network access rights without going through standard authentication process at the Public LAN (LAN1/LAN2 by default) may cause security problems.*

## Monitor IP List

HS1100 will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the necessary information, click ***Apply*** to save the settings. Click ***Monitor*** to check the current status of all the monitored IP. The system supports monitoring on 40 IP addresses listed in the **"Monitor IP List"**.



| Admin Email | |
|---|---|
| Send To | *separate email addresses with a comma |
| Subject | Monitor Result<br>*The host name and detection time will be appended to subject automatically. |
| Email Body | *The host name, remark, and detection time information will be appended to email body automatically. |
| Send From | |
| SMTP Server | Port: 25 |
| Auth Method | NONE |
| Send Test Email | Send |

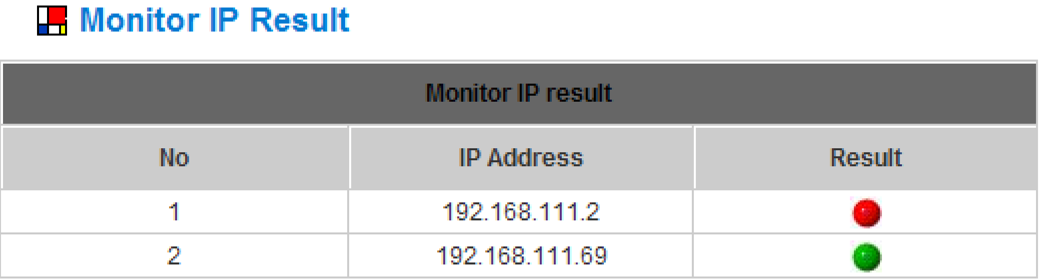
| Settings | |
|---|---|
| Enable Monitor IP List | ☑ |
| Interval | 1 Minute |
| Probe Retry | Retry if no response: 3 (Range: 1 ~ 10) |

Monitor IP List

| Item | IP/Host Name | Remark |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

(Total:40) First Prev Next Last

- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender’s e-mail.
- **Send To:** The e-mail address of the person to which the monitoring result is sent. This will be the receiver’s e-mail.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Server:** The IP address of the SMTP server.
- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **“None”** to use none of the above. Select one authentication method and enter the **Account Name**, **Password** and **Domain**.
- **Send Test Email:** To test if the settings are correct or not.
- **Monitor IP Address:** The IP addresses under monitoring.

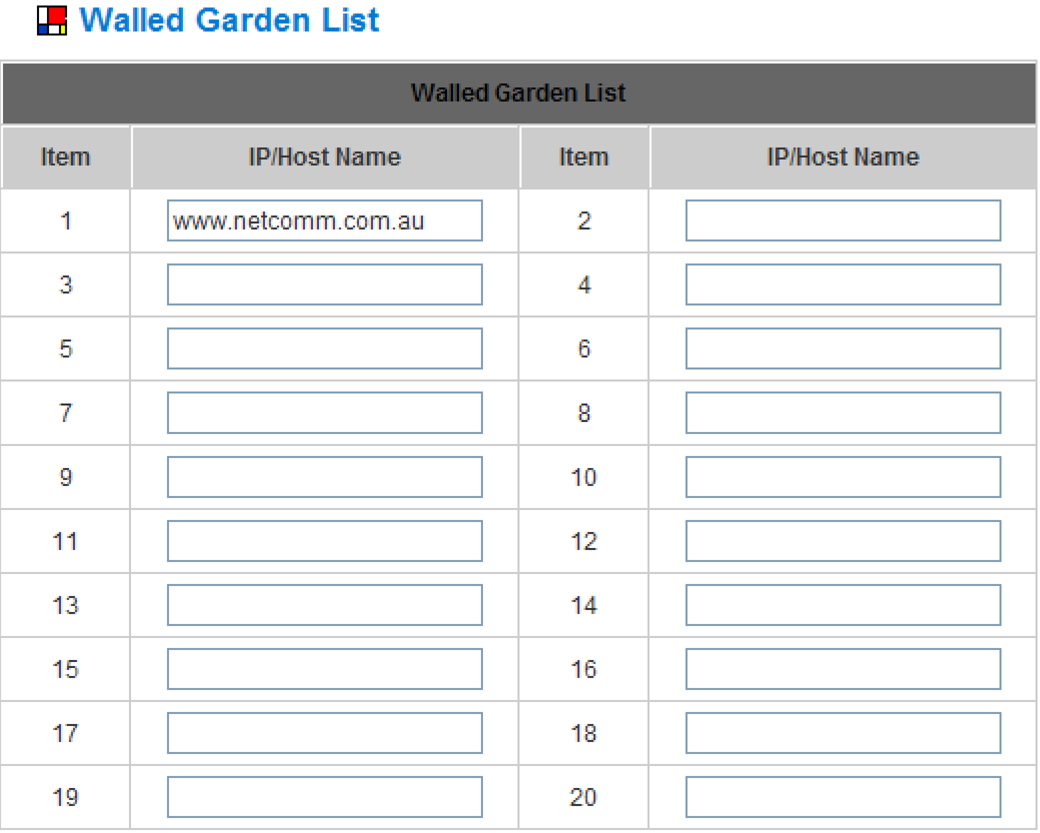


Monitor IP Result

| Monitor IP result | | |
|---|---|---|
| No | IP Address | Result |
| 1 | 192.168.111.2 | 🔴 |
| 2 | 192.168.111.69 | 🟢 |

## Walled Garden List

This function provides certain free services for users to access the websites listed here before login and authentication. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Enter the website **IP Address** or **Domain Name** in the list and click ***Apply*** to save the settings.

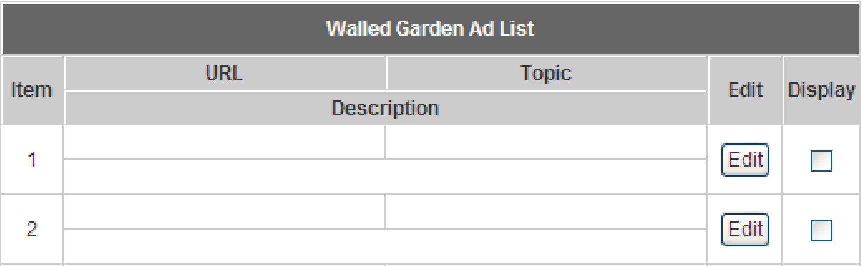


Walled Garden List

| Walled Garden List | | | |
|---|---|---|---|
| Item | IP/Host Name | Item | IP/Host Name |
| 1 | www.netcomm.com.au | 2 | |
| 3 | | 4 | |
| 5 | | 6 | |
| 7 | | 8 | |
| 9 | | 10 | |
| 11 | | 12 | |
| 13 | | 14 | |
| 15 | | 16 | |
| 17 | | 18 | |
| 19 | | 20 | |

## Walled Garden Ad List

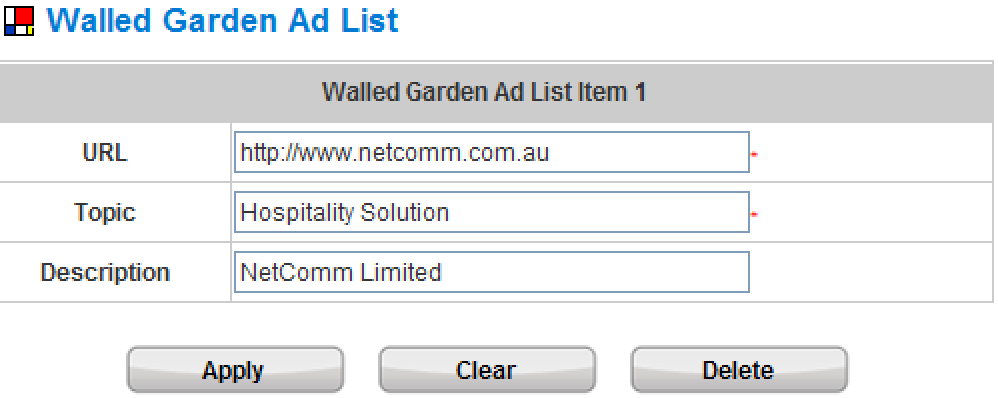
This function provides advertisement web pages for users to access free advertisement websites listed before login and authentication. Advertisement hyperlinks are displayed on the user's login page. Clients who click on it will be redirected to the listed advertisement websites.



Walled Garden Ad List

| Item | URL | Topic | Edit | Display |
|---|---|---|---|---|
| | Description | | | |
| 1 | | | Edit | □ |
| | | | | |
| 2 | | | Edit | □ |
| | | | | |

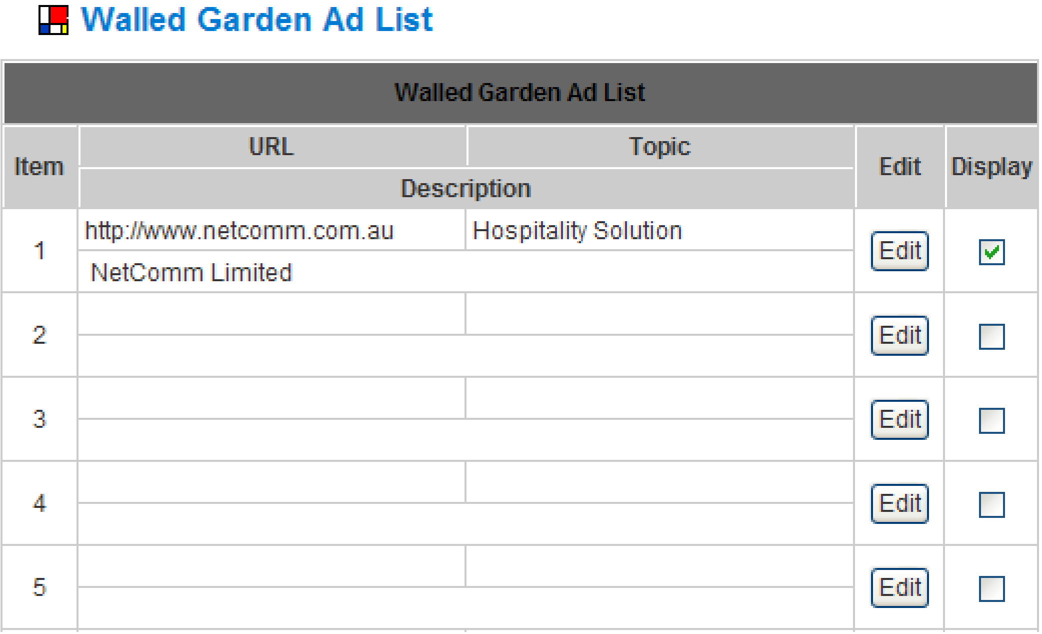
- **Edit:** Click ***Edit*** to add a new item or make changes. Click ***Apply***, the items will be added and shown in the list.
- **Display:** Choose ***Display*** to display advertisement hyperlinks on the login pages



Walled Garden Ad List

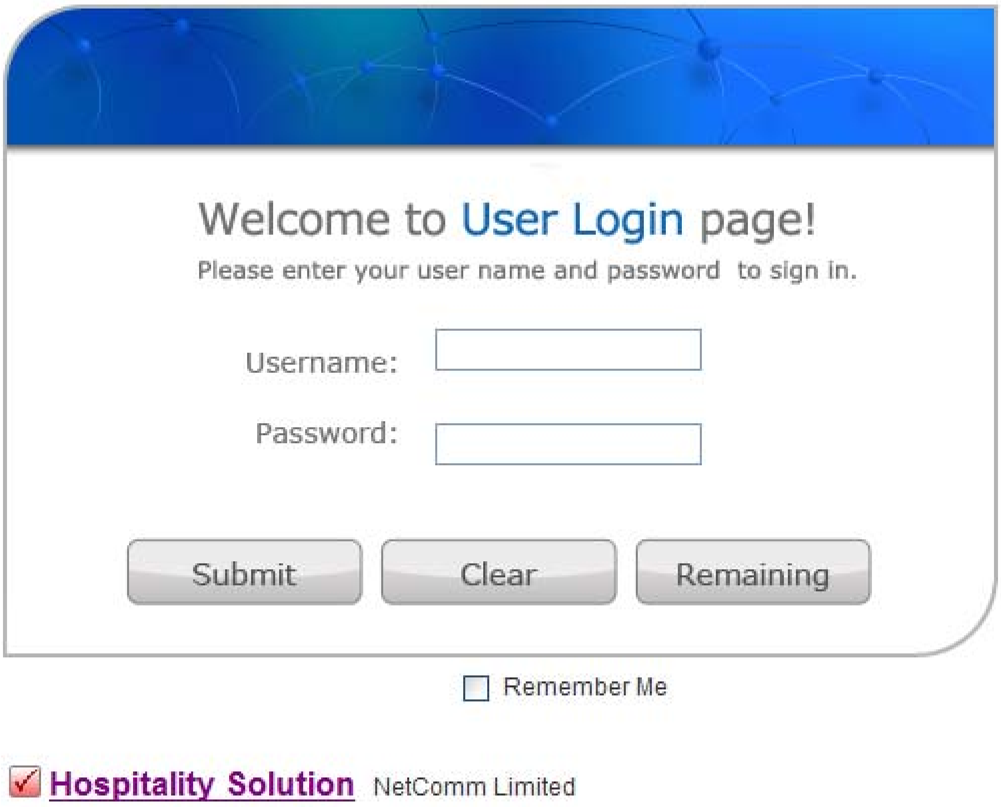
| Walled Garden Ad List Item 1 | |
|---|---|
| URL | http://www.netcomm.com.au * |
| Topic | Hospitality Solution * |
| Description | NetComm Limited |

⇩



Walled Garden Ad List

| Item | URL | Topic | Edit | Display |
|---|---|---|---|---|
| | Description | | | |
| 1 | http://www.netcomm.com.au | Hospitality Solution | Edit | ☑ |
| | NetComm Limited | | | |
| 2 | | | Edit | □ |
| | | | | |
| 3 | | | Edit | □ |
| | | | | |
| 4 | | | Edit | □ |
| | | | | |
| 5 | | | Edit | □ |
| | | | | |



Welcome to User Login page!

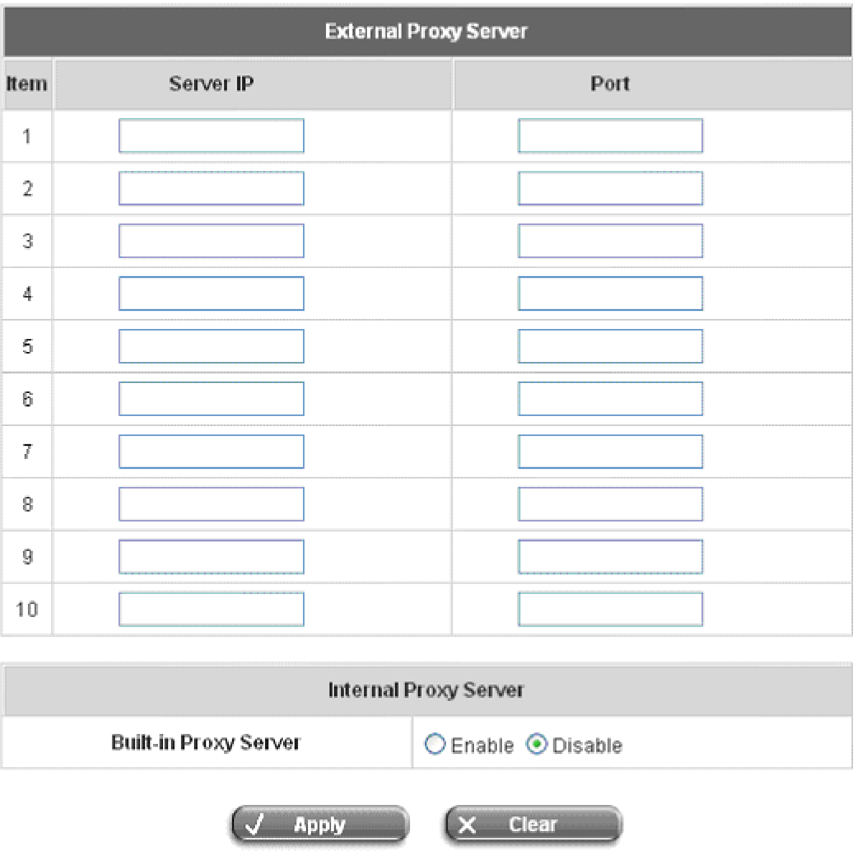
Please enter your user name and password to sign in.

Username:

Password:

## Proxy Server Properties

HS1100 supports Internal Proxy Server and External Proxy Server functions. Please select an **Access Gateway** and then set the necessary configurations.



External Proxy Server

| Item | Server IP | Port |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

Internal Proxy Server

| | |
|---|---|
| Built-in Proxy Server | ○ Enable ● Disable |

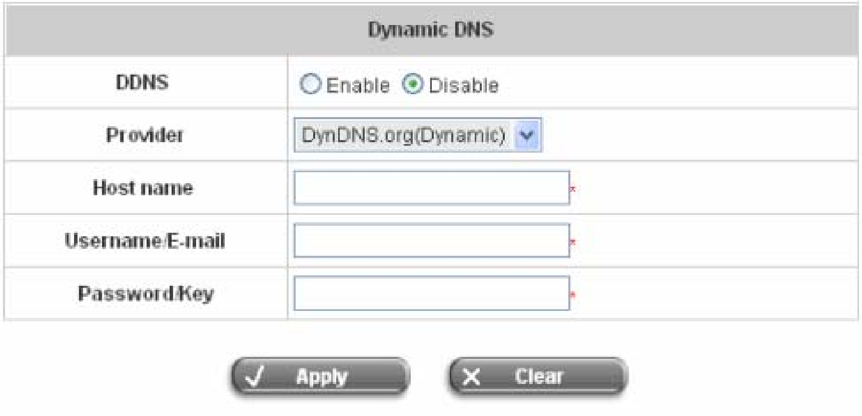
- **External Proxy Server:** Under the security management of HS1100, the system will match the External Proxy Server list to the clients' proxy settings. If there is not a match, the clients will not be able to reach the login page and thus unable to access the network. If there is a match, the clients will be directed to the system for authentication. After a successful authentication, the clients will be redirected back to the desired proxy servers depending on different situations.

- **Internal Proxy Server:** HS1100 has a built-in proxy server. If this function is enabled, the clients will be forced to treat HS1100 as the proxy server regardless of their original proxy settings.

**For more details about how to set up the proxy servers, please refer to *Appendix F. Proxy Setting*.**

## Dynamic DNS

Before activating this function, you must have your Dynamic DNS hostname registered with a Dynamic DNS provider. HS1100 supports DNS function to alias the dynamic IP address for the WAN port to a static domain name, allowing the administrator to easily access HS1100's WAN. If the dynamic DHCP is activated at the WAN port, it will update the IP address of the DNS server periodically. These settings will become effective immediately after clicking ***Apply***.



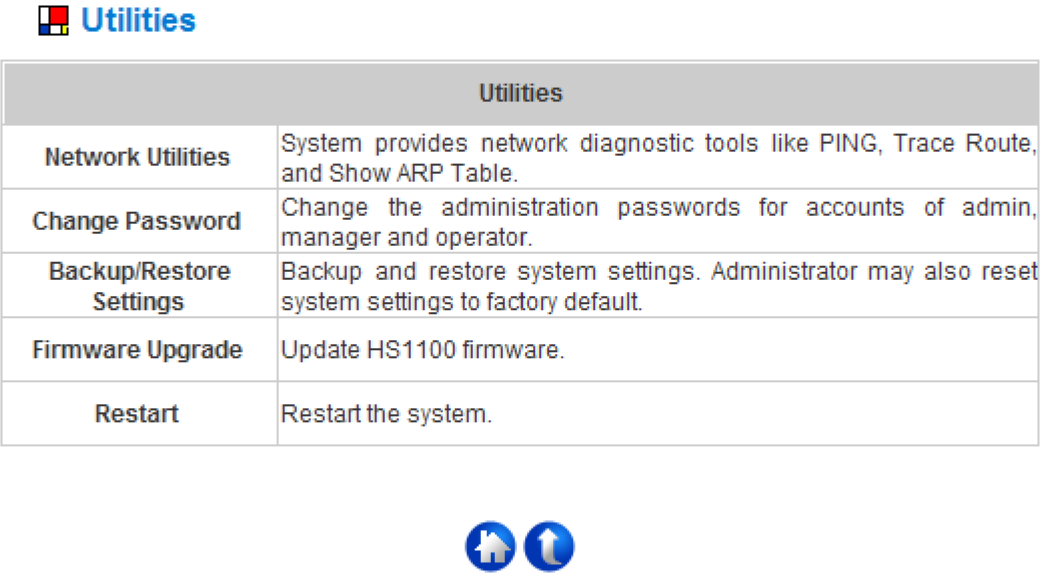
| Dynamic DNS | |
|---|---|
| DDNS | ○ Enable ● Disable |
| Provider | DynDNS.org(Dynamic) |
| Host name | * |
| Username/E-mail | * |
| Password/Key | * |

- **DDNS:** Enable or disable this function.
- **Provider:** Select the DNS provider.
- **Host name:** The IP address/domain name of the WAN port.
- **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- **Password/Key:** The register password for the DNS provider.

**Note:** To apply for free Dynamic DNS service, you may go to http://www.dyndns.com/services/dns/dyndns/howto.html

# Utilities

This section provides four utilities to customize and maintain the system including **Network Utilities**, **Change Password**, **Backup/Restore Setting**, **Firmware Upgrade** and **Restart**.

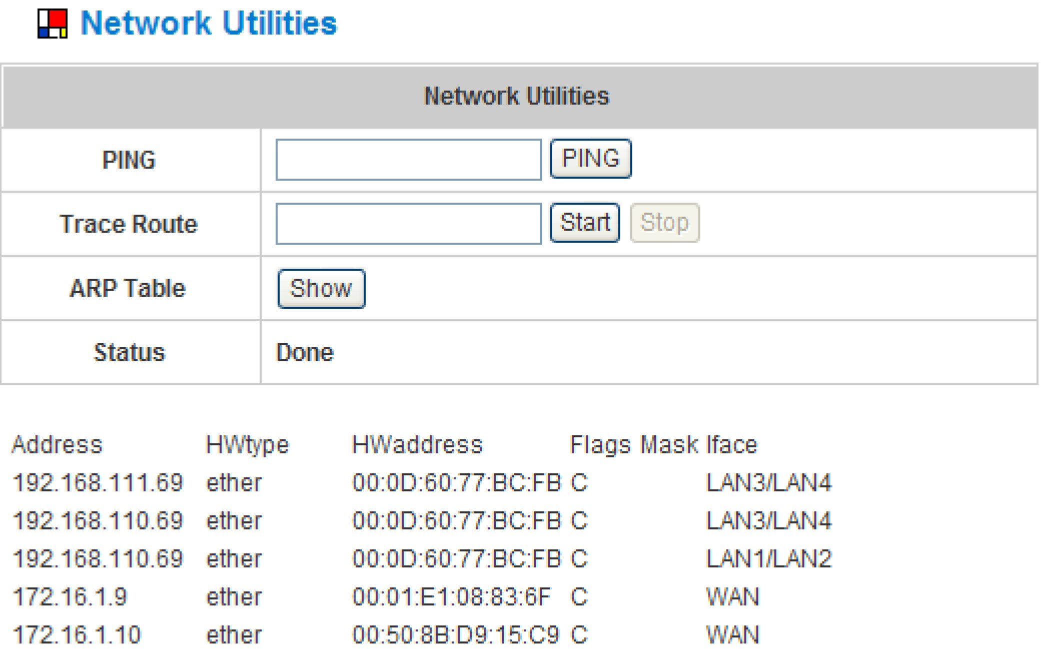


Utilities

| Utilities | |
|---|---|
| Network Utilities | System provides network diagnostic tools like PING, Trace Route, and Show ARP Table. |
| Change Password | Change the administration passwords for accounts of admin, manager and operator. |
| Backup/Restore Settings | Backup and restore system settings. Administrator may also reset system settings to factory default. |
| Firmware Upgrade | Update HS1100 firmware. |
| Restart | Restart the system. |

## Network Utilities

The system provides network diagnostic tools like **"PING"**, **"Trace Route"**, and **"ARP Table"**.



Network Utilities

| Network Utilities | |
|---|---|
| PING | PING |
| Trace Route | Start Stop |
| ARP Table | Show |
| Status | Done |

```
Address         HWtype    HWaddress         Flags Mask Iface
192.168.111.69  ether     00:0D:60:77:BC:FB C          LAN3/LAN4
192.168.110.69  ether     00:0D:60:77:BC:FB C          LAN3/LAN4
192.168.110.69  ether     00:0D:60:77:BC:FB C          LAN1/LAN2
172.16.1.9      ether     00:01:E1:08:83:6F C          WAN
172.16.1.10     ether     00:50:8B:D9:15:C9 C          WAN
```

## Change Password

There are three levels of authorities: **admin**, **manager** or **operator**. The default usernames and passwords are as follows:

**Admin:** The administrator can access all configuration pages of HS1100.

User Name: **admin**

Password: **admin**

**Manager:** The manager can only access the configuration pages under ***User Authentication*** to manage the user accounts, but without permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

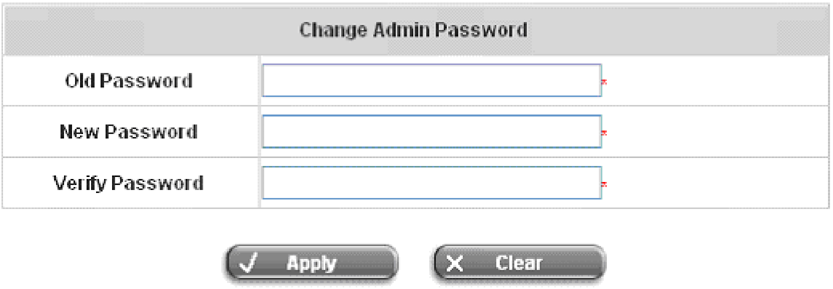
Password: **manager**

**Operator:** The operator can only access the configuration page of ***Create On-demand User*** to create new on-demand user accounts and print out the on-demand user account receipts.

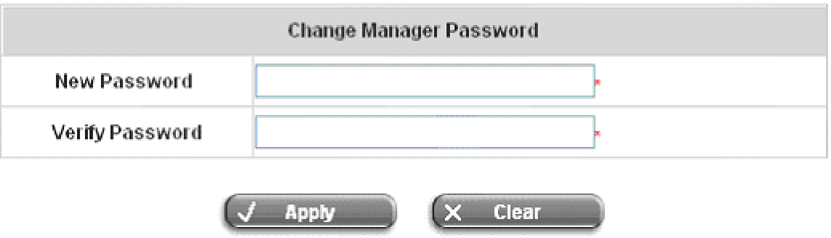
User Name: **operator**

Password: **operator**

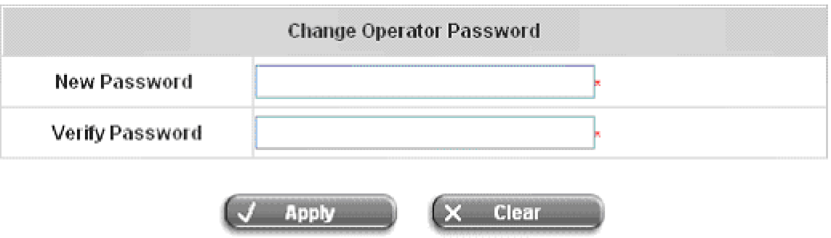
The administrator can change the passwords here. Please enter the current password and then enter the new password twice to verify. Click ***Apply*** to activate this new password.



| Change Admin Password | |
|---|---|
| Old Password | * |
| New Password | * |
| Verify Password | * |



| Change Manager Password | |
|---|---|
| New Password | * |
| Verify Password | * |

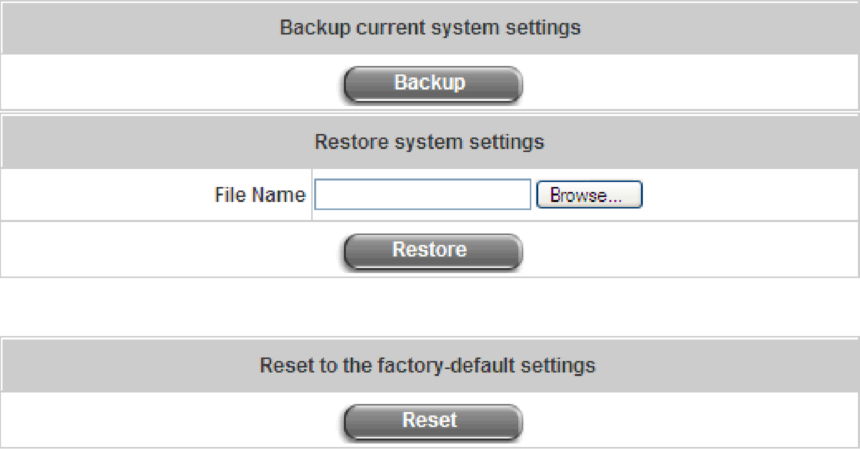


| Change Operator Password | |
|---|---|
| New Password | * |
| Verify Password | * |

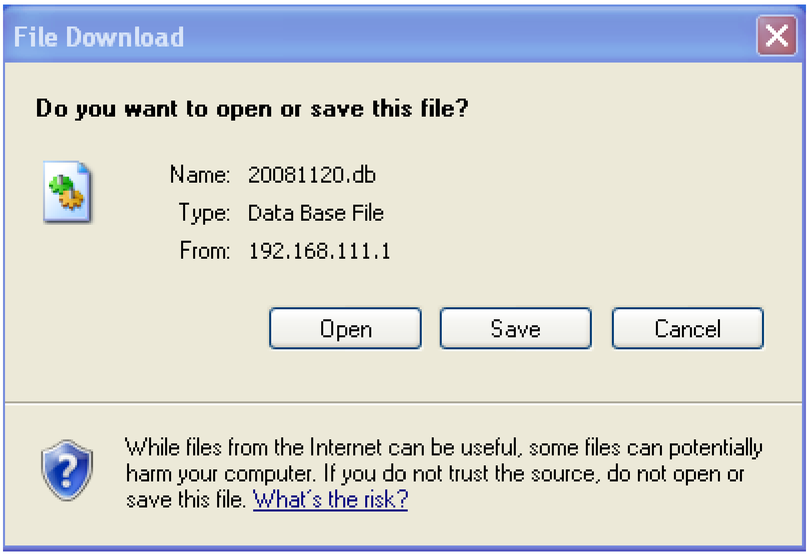
> *If the administrator’s password is lost, the administrator’s password still can be changed through the text mode management interface at the serial console port.*

## Backup/Restore Settings

This function is used to backup/restore the HS1100 settings. Also, HS1100 can be restored to the factory default settings here.


Backup current system settings
Backup
Restore system settings
File Name
Browse...
Restore
Reset to the factory-default settings
Reset

- **Backup current system settings:** Click ***Backup*** to create a .db database backup file and save it on disk.



Do you want to open or save this file?

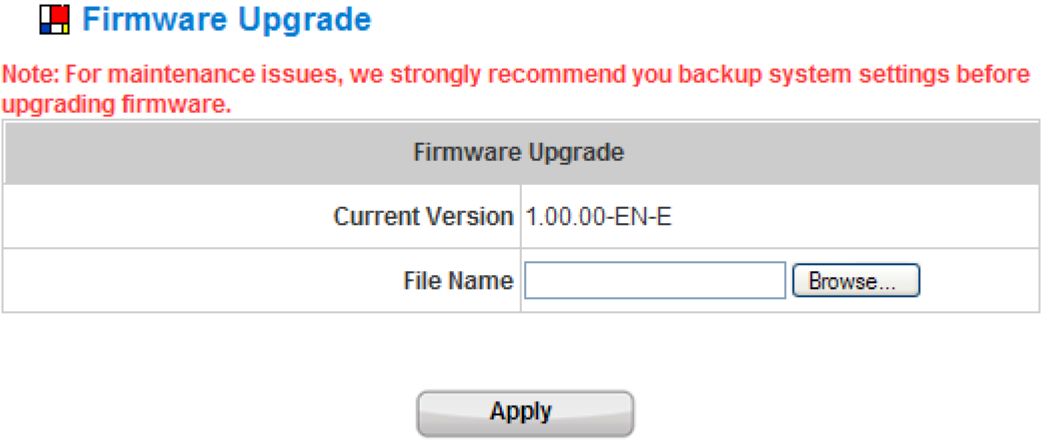
Name: 20081120.db
Type: Data Base File
From: 192.168.111.1

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

- **Restore system settings:** Click ***Browse*** to search for a .db database backup file created by HS1100 and click ***Restore*** to restore to the same settings at the time when the backup file was saved.
- **Reset to the factory-default settings:** Click ***Reset*** to load the factory default settings of HS1100.

## Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click ***Browse*** to search for the firmware file and click ***Apply*** for the firmware upgrade. It might take a few minutes before the upgrade process completes and the system needs to be restarted afterwards to activate the new firmware.



Firmware Upgrade

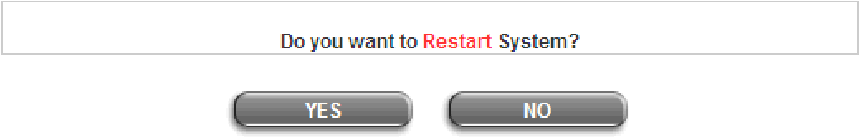
Note: For maintenance issues, we strongly recommend you backup system settings before upgrading firmware.

| Firmware Upgrade | |
|---|---|
| Current Version | 1.00.00-EN-E |
| File Name | |

1. *Firmware upgrade may cause the loss of some data. Please refer to the release notes for the limitation before upgrading.*
2. *Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or restart process. It may damage the system and cause malfunction.*

## Restart

This function allows the administrator to safely restart HS1100, and the process might take approximately three minutes. Click ***YES*** to restart HS1100; click ***NO*** to go back to the previous screen. If the power needs to be turned off, it is highly recommended to restart HS1100 first and then turn off the power after completing the restart process.

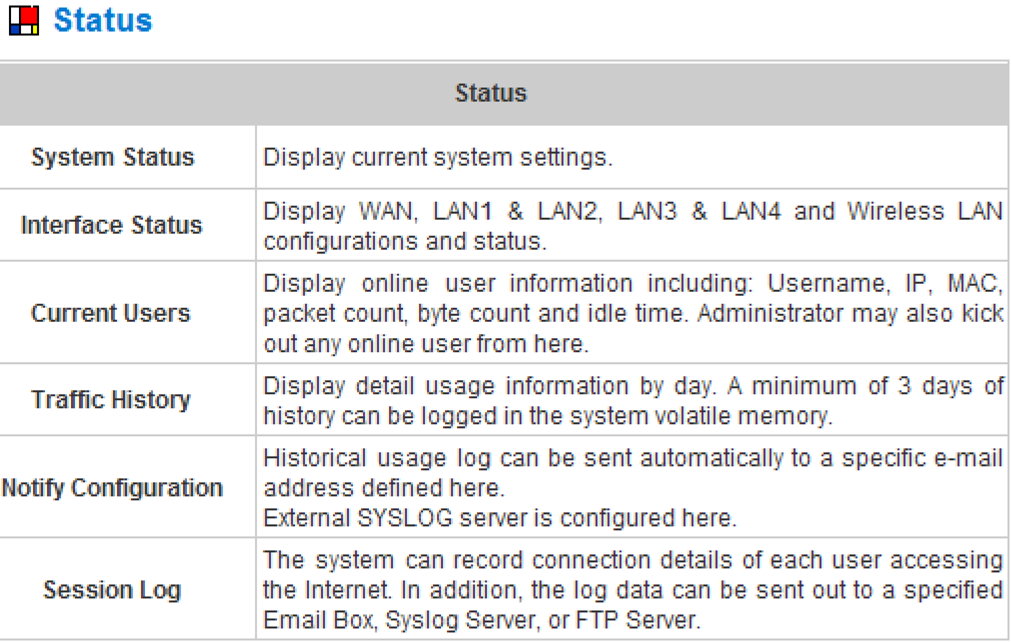


Do you want to Restart System?

⚠ *The connection of all online users of the system will be disconnected when system is in the process of restarting.*

# Status

This section includes **System Status**, **Interface Status**, **Current Users**, **Traffic History**, **Notification Configuration**, and **Session Log** to provide system status information and online user status.

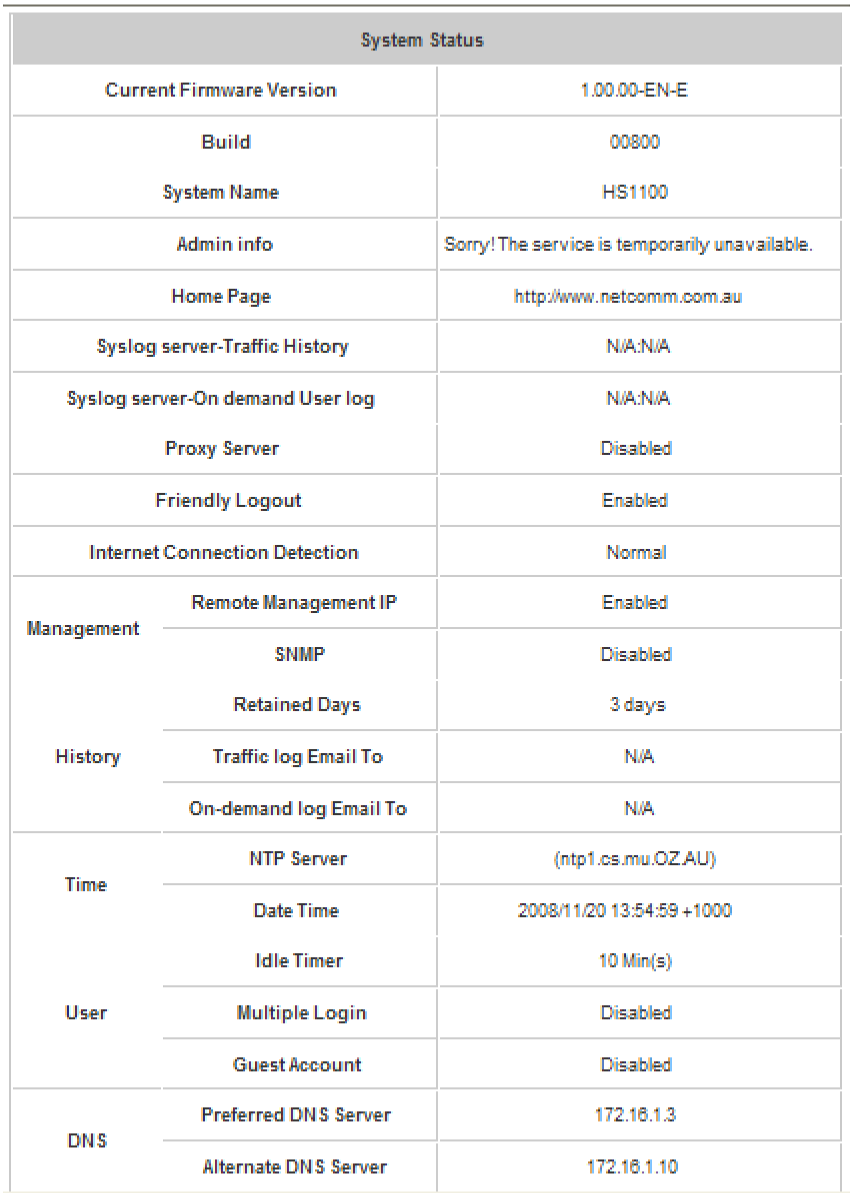


Status

| Status | |
|---|---|
| System Status | Display current system settings. |
| Interface Status | Display WAN, LAN1 & LAN2, LAN3 & LAN4 and Wireless LAN configurations and status. |
| Current Users | Display online user information including: Username, IP, MAC, packet count, byte count and idle time. Administrator may also kick out any online user from here. |
| Traffic History | Display detail usage information by day. A minimum of 3 days of history can be logged in the system volatile memory. |
| Notify Configuration | Historical usage log can be sent automatically to a specific e-mail address defined here.<br>External SYSLOG server is configured here. |
| Session Log | The system can record connection details of each user accessing the Internet. In addition, the log data can be sent out to a specified Email Box, Syslog Server, or FTP Server. |

## System Status

This section provides an overview of the system for the administrator.



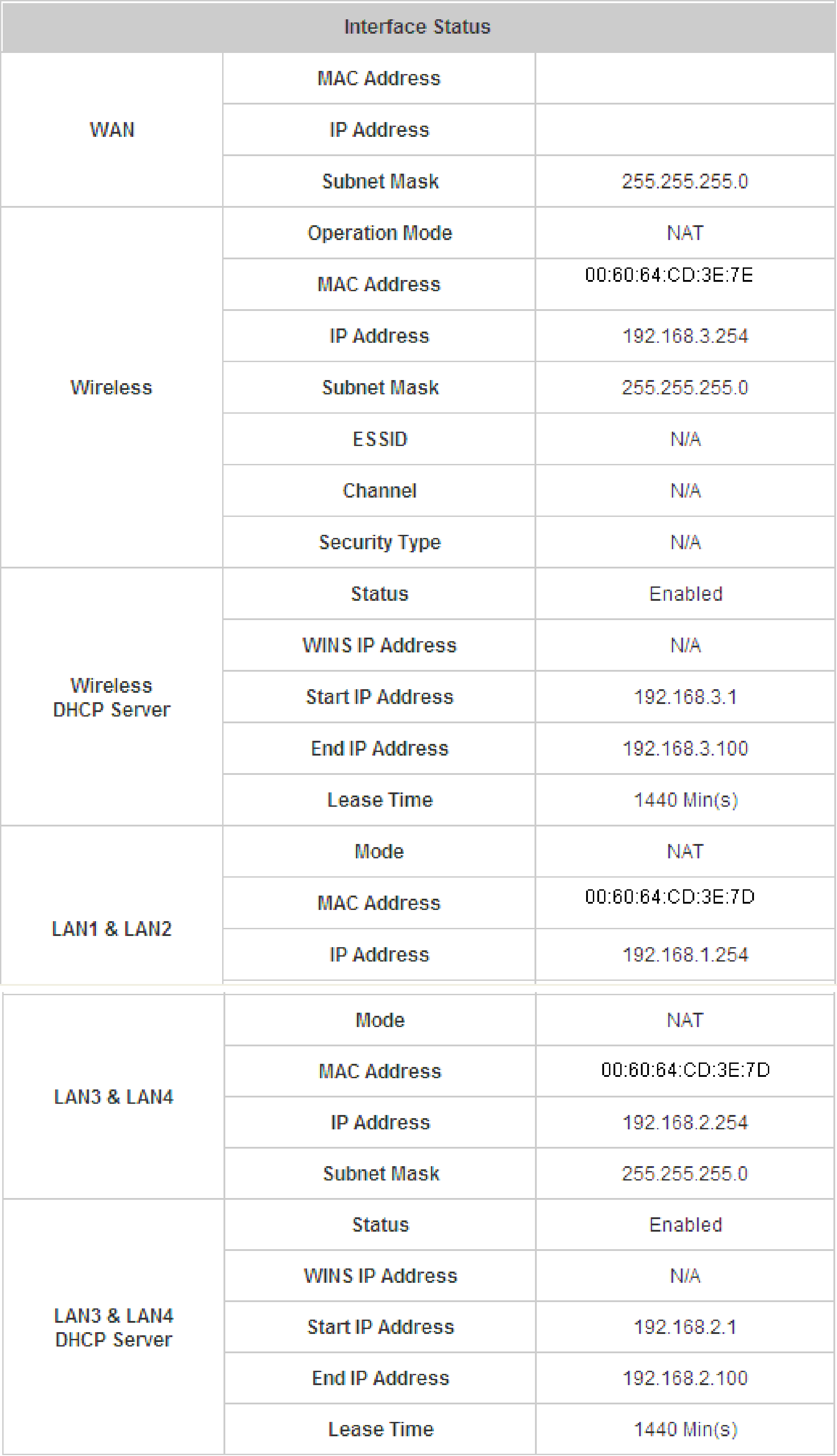
| System Status | | |
|---|---|---|
| Current Firmware Version | | 1.00.00-EN-E |
| Build | | 00800 |
| System Name | | HS1100 |
| Admin info | | Sorry! The service is temporarily unavailable. |
| Home Page | | http://www.netcomm.com.au |
| Syslog server-Traffic History | | N/A:N/A |
| Syslog server-On demand User log | | N/A:N/A |
| Proxy Server | | Disabled |
| Friendly Logout | | Enabled |
| Internet Connection Detection | | Normal |
| Management | Remote Management IP | Enabled |
| | SNMP | Disabled |
| History | Retained Days | 3 days |
| | Traffic log Email To | N/A |
| | On-demand log Email To | N/A |
| Time | NTP Server | (ntp1.cs.mu.OZ.AU) |
| | Date Time | 2008/11/20 13:54:59 +1000 |
| User | Idle Timer | 10 Min(s) |
| | Multiple Login | Disabled |
| | Guest Account | Disabled |
| DNS | Preferred DNS Server | 172.16.1.3 |
| | Alternate DNS Server | 172.16.1.10 |

The description of the above-mentioned table is as follows:

| ***Item*** | | ***Description*** |
|---|---|---|
| **Current Firmware Version** | | The present firmware version of HS1100 |
| **System Name** | | The system name. The default is HS1100 |
| **Admin Info** | | The information to be shown on the login window when a user has a connection problem. |
| **Home Page** | | The page to which the users are directed after successful login. |
| **Syslog server-Traffic History** | | The IP address and port number of the external Syslog Server. **N/A** means that it is not configured. |
| **Syslog server-On demand User log** | | The IP address and port number of the external Syslog Server. **N/A** means that it is not configured. |
| **Proxy Server** | | Enabled/disabled stands for that the system is currently using the proxy server or not. |
| **Friendly Logout** | | Enabled/disabled stands for the setting of hiding/displaying an extra confirmation window when users close the login succeed page. |
| **Internet Connection Detection** | | Enabled/Disabled stands for the connection at WAN is normal or abnormal (**Internet Connection Detection**) and all online users are allowed/disallowed to log in the network. |
| **Management** | **Remote Management IP** | The IP(s) that is allowed for accessing the management interface. |
| | **SNMP** | Enabled/disabled stands for the current status of the SNMP management function. |
| **History** | **Retained Days** | The maximum number of days for the system to retain the users' information. |
| | **Traffic log Email To** | The email address to which that the traffic history information will be sent. |
| | **On-demand log Email To** | The email address to which the history information about on-demand users is sent. |
| **Time** | **NTP Server** | The network time server that the system is set to align with. |
| | **Date Time(GMT+0:00)** | The system time is shown as the local time. |
| **User** | **Idle Timer** | The number of minutes before the system disconnects inactive users. |
| | **Multiple Login** | Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account. |
| | **Guest Account** | Enabled/disabled stands for the current status of allowing/disallowing Guest Accounts to log in. |
| **DNS** | **Preferred DNS Server** | IP address of the preferred DNS Server. |
| | **Alternate DNS Server** | IP address of the alternate DNS Server. |

## Interface Status

This section provides an overview of the interface for the administrator including **WAN**, **LAN1 & LAN2**, **LAN3 & LAN4,** and **Wireless Port**.



| Interface Status | | |
|---|---|---|
| WAN | MAC Address | |
| | IP Address | |
| | Subnet Mask | 255.255.255.0 |
| Wireless | Operation Mode | NAT |
| | MAC Address | 00:60:64:CD:3E:7E |
| | IP Address | 192.168.3.254 |
| | Subnet Mask | 255.255.255.0 |
| | ESSID | N/A |
| | Channel | N/A |
| | Security Type | N/A |
| Wireless DHCP Server | Status | Enabled |
| | WINS IP Address | N/A |
| | Start IP Address | 192.168.3.1 |
| | End IP Address | 192.168.3.100 |
| | Lease Time | 1440 Min(s) |
| LAN1 & LAN2 | Mode | NAT |
| | MAC Address | 00:60:64:CD:3E:7D |
| | IP Address | 192.168.1.254 |
| LAN3 & LAN4 | Mode | NAT |
| | MAC Address | 00:60:64:CD:3E:7D |
| | IP Address | 192.168.2.254 |
| | Subnet Mask | 255.255.255.0 |
| LAN3 & LAN4 DHCP Server | Status | Enabled |
| | WINS IP Address | N/A |
| | Start IP Address | 192.168.2.1 |
| | End IP Address | 192.168.2.100 |
| | Lease Time | 1440 Min(s) |

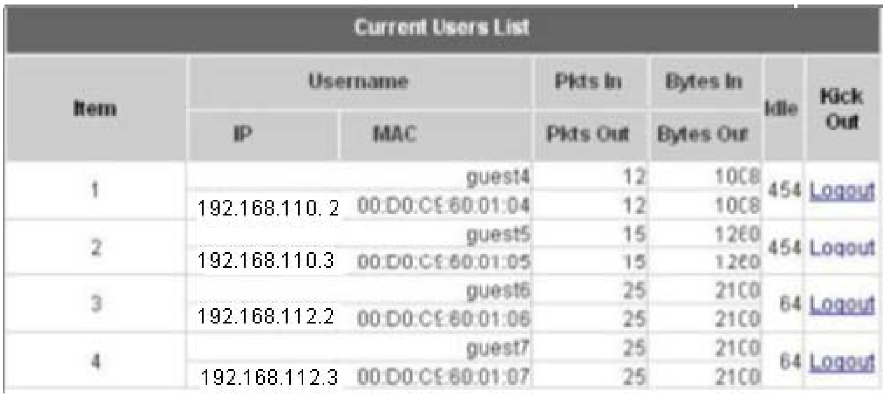
The description of the above-mentioned table is as follows:

| ***Item*** | | ***Description*** |
|---|---|---|
| **WAN** | **MAC Address** | The MAC address of the WAN port. |
| | **IP Address** | The IP address of the WAN port. |
| | **Subnet Mask** | The Subnet Mask of the WAN port. |
| **Wireless** | **Operation Mode** | The mode of the wireless port. |
| | **MAC Address** | The MAC address of the wireless port. |
| | **IP Address** | The IP address of the wireless port. |
| | **Subnet Mask** | The subnet mask of the wireless port. |
| | **ESSID** | The ESSID of the wireless port. |
| | **Channel** | The assigned Channel of the wireless port. |
| | **Security Type** | The security type of the wireless port. |
| **Wireless DHCP Server** | **Status** | Enable/disable stands for status of the DHCP server on the wireless port. |
| | **WINS IP Address** | The WINS server IP on DHCP server. **N/A** means that it is not configured. |
| | **Start IP Address** | The start IP address of the DHCP IP range. |
| | **End IP address** | The end IP address of the DHCP IP range. |
| | **Lease Time** | The number of minutes of the lease time of the IP address. |
| **LAN1 & LAN2** | **Mode** | The mode of the LAN1 & LAN2 port. |
| | **MAC Address** | The MAC address of the LAN1 & LAN2. |
| | **IP Address** | The IP address of the LAN1 & LAN2. |
| | **Subnet Mask** | The subnet mask of the LAN1 & LAN2. |
| **LAN1 & LAN2 DHCP Server** | **Status** | Enable/disable stands for status of the DHCP server on the LAN1 & LAN2. |
| | **WINS IP Address** | The WINS server IP on DHCP server. **N/A** means that it is not configured. |
| | **Start IP Address** | The start IP address of the DHCP IP range. |
| | **End IP address** | The end IP address of the DHCP IP range. |
| | **Lease Time** | The number of minutes of the lease time of the IP address. |
| **LAN3 & LAN4** | **Mode** | The mode of the LAN3 & LAN4. |
| | **MAC Address** | The MAC address of the LAN3 & LAN4. |
| | **IP Address** | The IP address of the LAN3 & LAN4. |
| | **Subnet Mask** | The subnet mask of the LAN3 & LAN4. |
| **LAN3 & LAN4 DHCP Server** | **Status** | Enable/disable stands for status of the DHCP server on the LAN3 & LAN4 port |
| | **WINS IP Address** | The WINS server IP on DHCP server. **N/A** means that it is not configured. |
| | **Start IP Address** | The start IP address of the DHCP IP range. |
| | **End IP address** | The end IP Address of the DHCP IP range. |
| | **Lease Time** | The number of minutes of the lease time of the IP address. |

## Current Users

In this function, each online user’s information can be obtained, including **Username**, **IP Address**, **MAC Address**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out, Idle** and **Kick Out**.

From the **“Current Users List”**, the administrator can force a specific online user to log out. Click the hyperlink of ***Logout*** next to the online user’s name to logout that particular user. Click ***Refresh*** to renew the Current Users List.

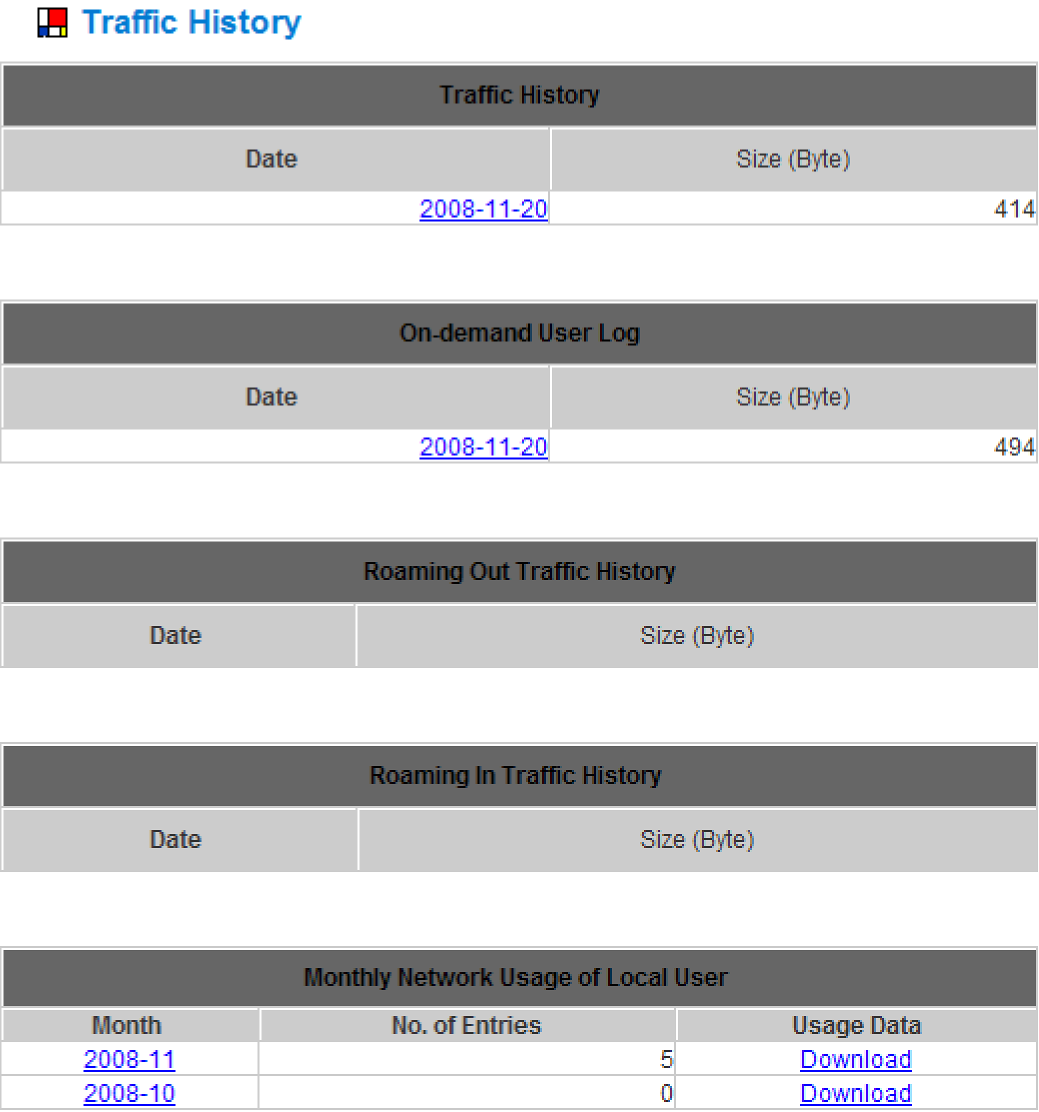


Current Users List

| Item | Username | | Pkts In | Bytes In | Idle | Kick Out |
|---|---|---|---|---|---|---|
| | IP | MAC | Pkts Out | Bytes Out | | |
| 1 | | guest4 | 12 | 10C8 | 454 | Logout |
| | 192.168.110. 2 | 00:D0:CE:60:01:04 | 12 | 10C8 | | |
| 2 | | guest5 | 15 | 12E0 | 454 | Logout |
| | 192.168.110.3 | 00:D0:CE:60:01:05 | 15 | 12E0 | | |
| 3 | | guest6 | 25 | 21C0 | 64 | Logout |
| | 192.168.112.2 | 00:D0:CE:60:01:06 | 25 | 21C0 | | |
| 4 | | guest7 | 25 | 21C0 | 64 | Logout |
| | 192.168.112.3 | 00:D0:CE:60:01:07 | 25 | 21C0 | | |

## Traffic History

This function is used to check the traffic history of HS1100. The history of each day will be saved separately in the DRAM for at least 3 days (72 full hours). The system also keeps a cumulated record of the traffic data generated by each user in the latest 2 calendar months.



Traffic History

| Traffic History | |
|---|---|
| Date | Size (Byte) |
| 2008-11-20 | 414 |

| On-demand User Log | |
|---|---|
| Date | Size (Byte) |
| 2008-11-20 | 494 |

| Roaming Out Traffic History | |
|---|---|
| Date | Size (Byte) |

| Roaming In Traffic History | |
|---|---|
| Date | Size (Byte) |

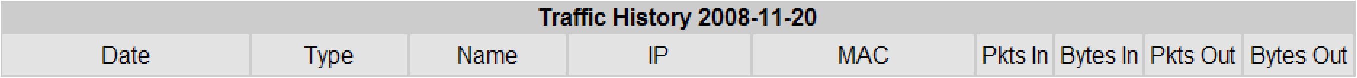
| Monthly Network Usage of Local User | | |
|---|---|---|
| Month | No. of Entries | Usage Data |
| 2008-11 | 5 | Download |
| 2008-10 | 0 | Download |

*Since the history is saved in the DRAM, if you need to restart the system, and at the same time, keep the history, please manually copy and save the traffic history information before restarting.*

If the **History Email** has been entered under the **Notify Configuration** page, the system will automatically send out the history information to that specified email address.

- **Traffic History**

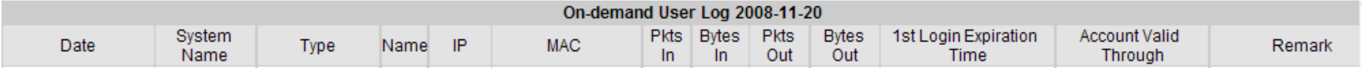
  All activities occur on the system within the nearest 72 hours are recorded; in date and time order. As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type, Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out** and **Bytes Out** of the user activities.



| Traffic History 2008-11-20 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | Type | Name | IP | MAC | Pkts In | Bytes In | Pkts Out | Bytes Out |

- **On-demand User Log**

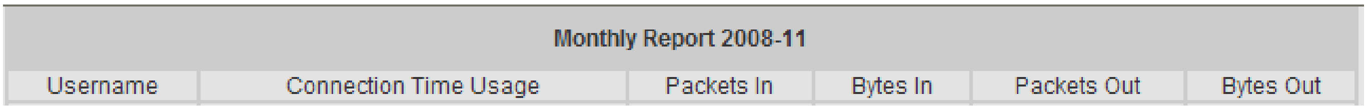
  All activities occur on the system within the nearest 72 hours are recorded; in date and time order. As shown in the following figure, each line is an on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, Expiretime**, **Validtime** and **Remark** of user activities.



| On-demand User Log 2008-11-20 | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Date | System Name | Type | Name | IP | MAC | Pkts In | Bytes In | Pkts Out | Bytes Out | 1st Login Expiration Time | Account Valid Through | Remark |

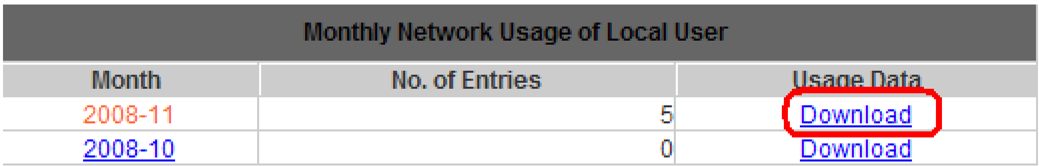
- **Monthly Network Usage of Local User**

  The system keeps a cumulated record of the traffic data generated by each user in the latest 2 calendar months. As shown in the following figure, each line in a monthly network usage of local user record consists of 6 fields, **System Name**, **Connection Time Usage**, **Packets In**, **Bytes In**, **Packets Out** and **Bytes Out** of user activities.



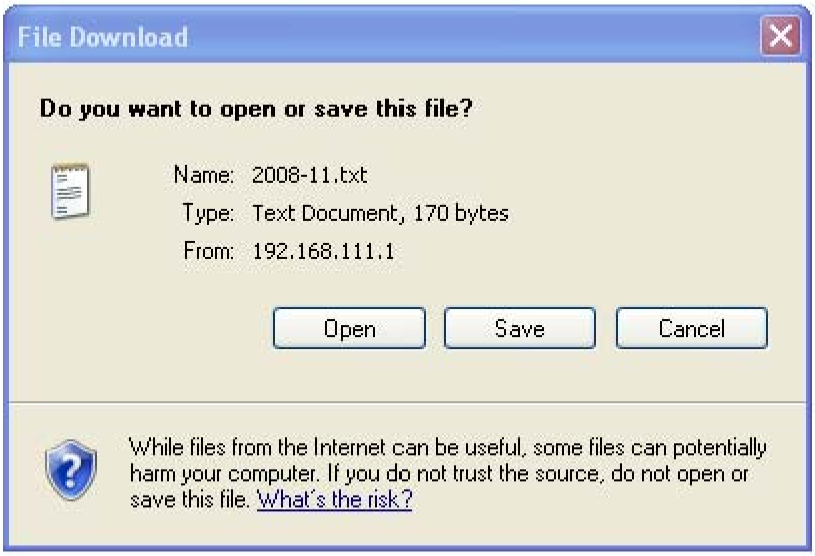
| Monthly Report 2008-11 | | | | | |
|---|---|---|---|---|---|
| Username | Connection Time Usage | Packets In | Bytes In | Packets Out | Bytes Out |

➢ **Download Monthly Network Usage of Local User:** Click on the ***Download*** button for outputting the report manually to a local database.



| Monthly Network Usage of Local User | | |
|---|---|---|
| Month | No. of Entries | Usage Data |
| 2008-11 | 5 | Download |
| 2008-10 | 0 | Download |

A warning message will then appear. Click ***Save*** to download the record into .txt format.



Do you want to open or save this file?

Name: 2008-11.txt

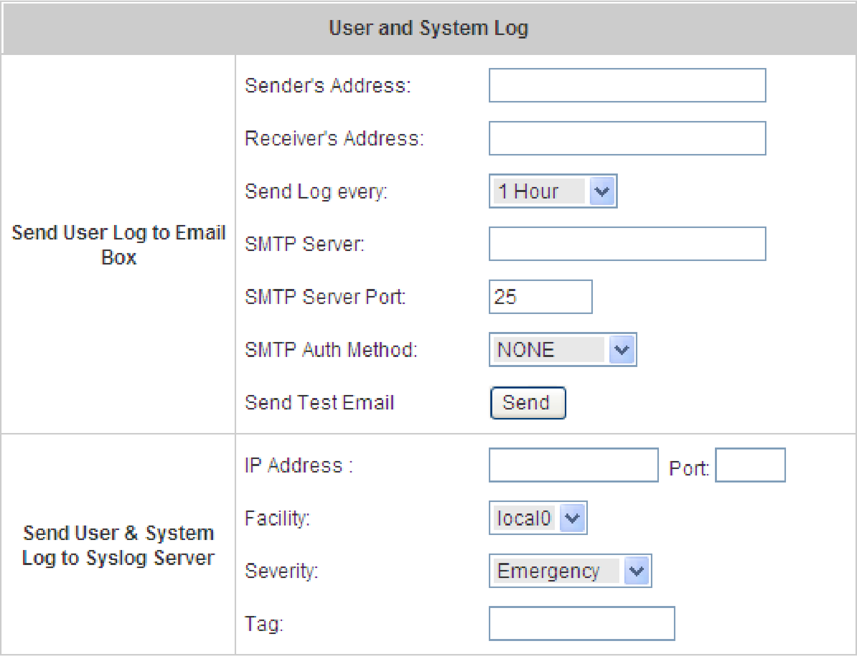
Type: Text Document, 170 bytes

From: 192.168.111.1

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

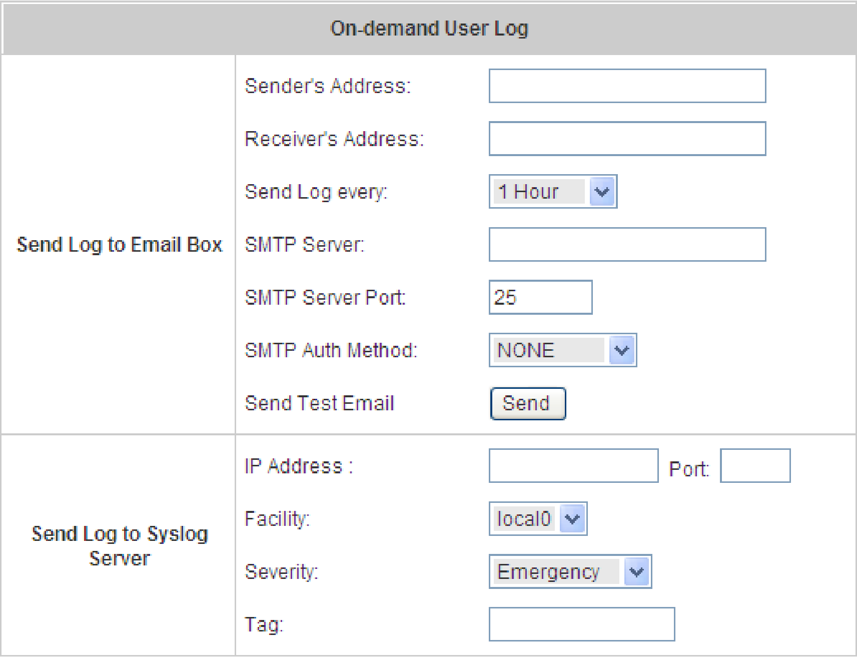
## Notify Configuration

HS1100 will save the traffic history into the internal DRAM. If the administrator wants the system to automatically send the history to a particular email address, enter the information shown as below.



User and System Log

| | | |
|---|---|---|
| Send User Log to Email Box | Sender's Address: | |
| | Receiver's Address: | |
| | Send Log every: | 1 Hour |
| | SMTP Server: | |
| | SMTP Server Port: | 25 |
| | SMTP Auth Method: | NONE |
| | Send Test Email | Send |
| Send User & System Log to Syslog Server | IP Address : | Port: |
| | Facility: | local0 |
| | Severity: | Emergency |
| | Tag: | |



On-demand User Log

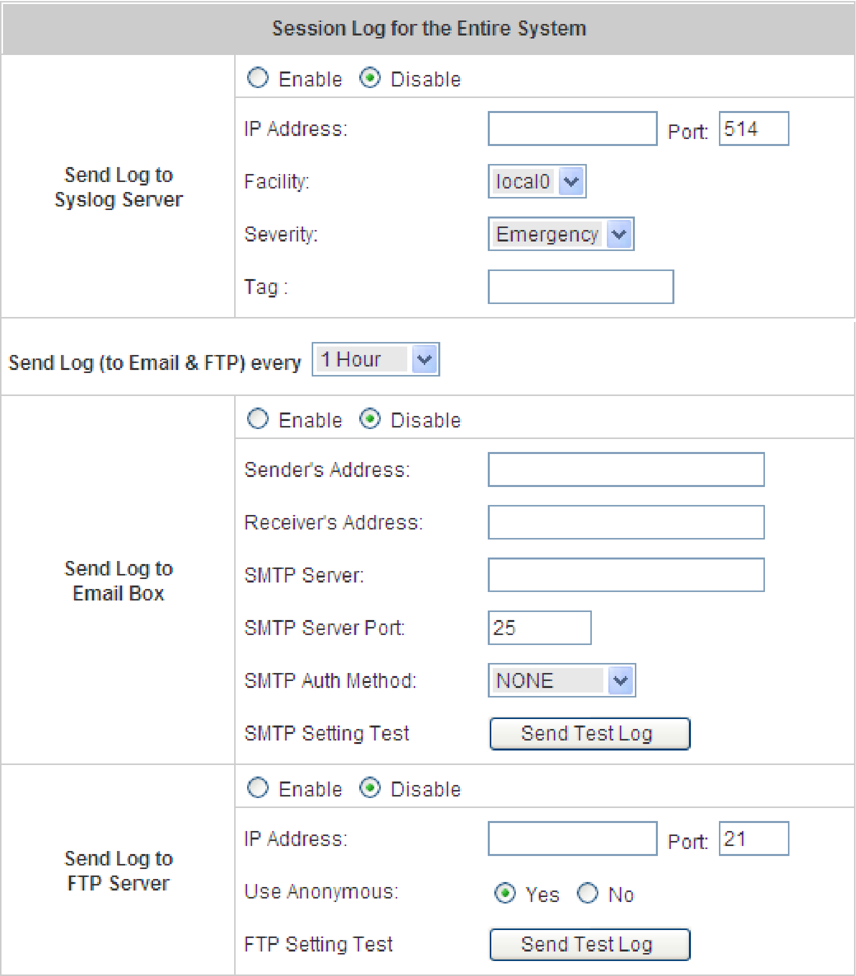
| | | |
|---|---|---|
| Send Log to Email Box | Sender's Address: | |
| | Receiver's Address: | |
| | Send Log every: | 1 Hour |
| | SMTP Server: | |
| | SMTP Server Port: | 25 |
| | SMTP Auth Method: | NONE |
| | Send Test Email | Send |
| Send Log to Syslog Server | IP Address : | Port: |
| | Facility: | local0 |
| | Severity: | Emergency |
| | Tag: | |

- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person to which the history email is sent to. This will be the receiver's e-mail.
- **Interval:** The time interval for sending the e-mail report of the traffic history.
- **SMTP Server:** The IP address of the SMTP server.
- **Auth Method:** The system provides four authentication methods, **PLAIN**, **LOGIN**, **CRAM-MD5** and **NTLMv1**, or **"NONE"** to use none of the above. Select one authentication method and enter the **Account Name**, **Password** and **Domain**.

  - **NTLMv1** is not currently available for general use.
  - **PLAIN** and **CRAM-MD5** are standard authentication mechanisms while **LOGIN** and **NTLMv1** are Microsoft proprietary mechanisms.
  - Only **PLAIN** and **LOGIN** can use the UNIX login password.
  - Netscape uses **PLAIN**.
  - Outlook and Outlook express use **LOGIN** as default, although they can be set to use **NTLMv1**.
  - Pegasus uses **CRAM-MD5** or **LOGIN** but the administrator cannot configure which method to be used.
- **Send Test Email:** To test the settings correct or not.
- **Syslog Server:** It specifies the IP and Port of the Syslog server.

## Session Log

Every connection created and activity executed on the Internet by users can be tracked if the **Session Log** function is enabled; the system will automatically report the connection details to a specified **Syslog Server**. Log files can also be sent out to an **Email Box** or uploaded to a particular **FTP Server** periodically when this function is enabled.



| Session Log for the Entire System | | |
|---|---|---|
| Send Log to Syslog Server | ○ Enable ● Disable | |
| | IP Address: | [ ] Port: 514 |
| | Facility: | local0 |
| | Severity: | Emergency |
| | Tag : | [ ] |
| Send Log (to Email & FTP) every 1 Hour | | |
| Send Log to Email Box | ○ Enable ● Disable | |
| | Sender's Address: | [ ] |
| | Receiver's Address: | [ ] |
| | SMTP Server: | [ ] |
| | SMTP Server Port: | 25 |
| | SMTP Auth Method: | NONE |
| | SMTP Setting Test | Send Test Log |
| Send Log to FTP Server | ○ Enable ● Disable | |
| | IP Address: | [ ] Port: 21 |
| | Use Anonymous: | ● Yes ○ No |
| | FTP Setting Test | Send Test Log |

- **Send Log to Syslog Server**

  Select *Enable*, and enter *IP Address* of the Syslog Server to be used.

  Select *Facility* and *Severity* from the drop-down list box.

  Enter a *Tag* description which will be included in session logs sent to the specified Syslog server.

  Click ***Apply*** to save the setting.

- **Send Log (to Email & FTP) every:**

  Select a time interval from the drop-down list box for sending session logs to an email box and/or FTP server.

  Click ***Apply*** to save the setting.

**Note:** The **"Send Log (to Email & FTP) every"** is applied only to **"Send Log to Email Box"**, and **"Send Log to FTP Server"** functions, but does not have any effect on **"Send Log to Syslog Server"** function.

- **Send Log to Email Box**

  Select *Enable*, and enter *Sender's* and *Receiver's Email Address*.

  Enter the domain name or IP address of the *SMTP Server*, and select an appropriate *SMTP Authentication Method* from the drop-down list box.

  Before applying the setting, you can send a test log to preview the setting by click ***Send Test Log*** button.

  Click ***Apply*** to save the setting.

- **Send Log to FTP Server**:

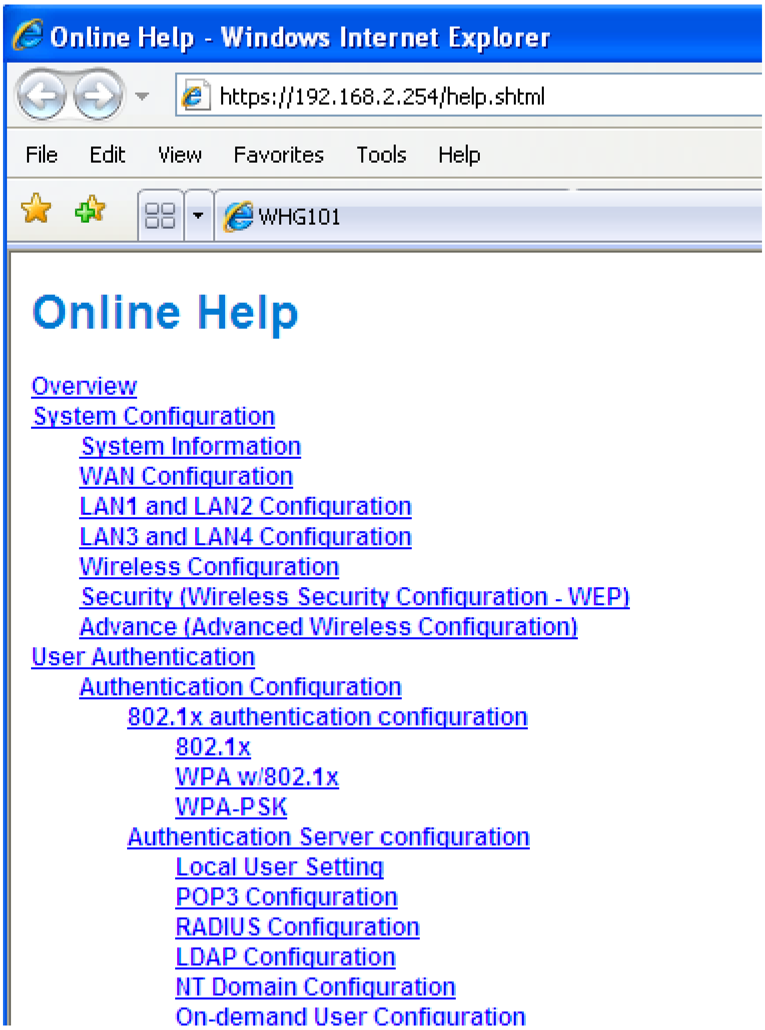
  Enter *IP Address* of the **FTP Server** to be used. When selecting *Anonymous*, specify the *Username* and *Password* for accessing the **FTP Server**.

  Before applying the setting, you can send a test log to preview the setting by click ***Send Test Log*** button..

  Click ***Apply*** to save the setting.

# Help

On the screen, the **Help** button is on the upper right corner. Click ***Help*** to the **Online Help** window and then click the hyperlink of the items for further information.



Online Help - Windows Internet Explorer
https://192.168.2.254/help.shtml
File Edit View Favorites Tools Help
WHG101

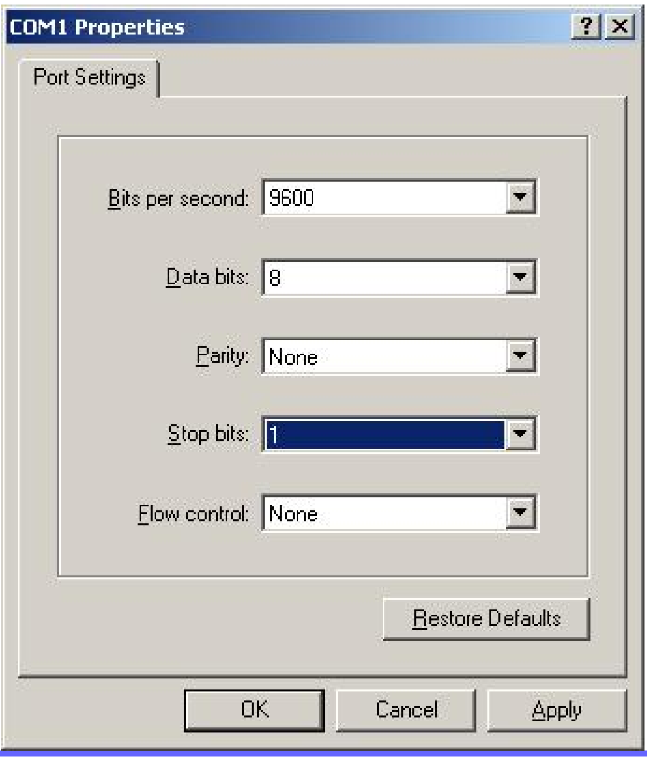
Online Help

- Overview
- System Configuration
  - System Information
  - WAN Configuration
  - LAN1 and LAN2 Configuration
  - LAN3 and LAN4 Configuration
  - Wireless Configuration
  - Security (Wireless Security Configuration - WEP)
  - Advance (Advanced Wireless Configuration)
- User Authentication
  - Authentication Configuration
    - 802.1x authentication configuration
      - 802.1x
      - WPA w/802.1x
      - WPA-PSK
    - Authentication Server configuration
      - Local User Setting
      - POP3 Configuration
      - RADIUS Configuration
      - LDAP Configuration
      - NT Domain Configuration
      - On-demand User Configuration

# *Appendix A. Console Interface*

Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. In order to connect to the console port of HS1100, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **9600,8,n,1**.



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

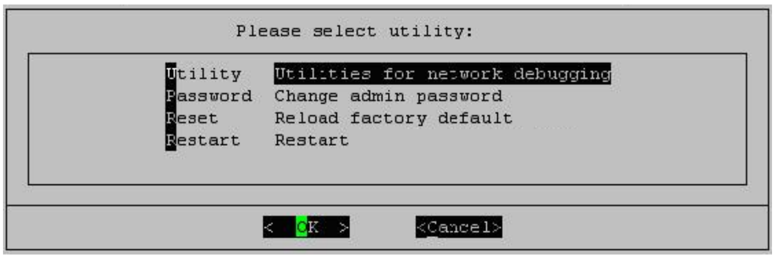
Parity: None

Stop bits: 1

Flow control: None

*The main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the* ***Enter*** *key to make selection or confirm what you enter.*

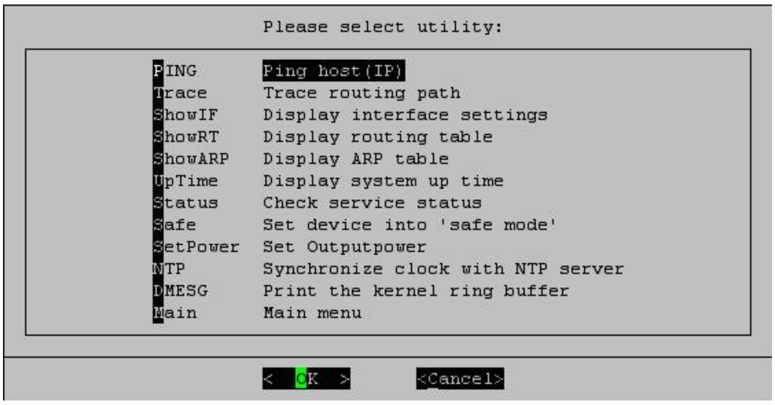
3. Once the console port of HS1100 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system, where the welcome screen or main menu should appear. If the welcome screen or main menu of the console still does not pop up, please check the connection of the cables and the settings of the terminal simulation program.



```
                    Please select utility:

             Utility    Utilities for network debugging
             Password   Change admin password
             Reset      Reload factory default
             Restart    Restart

                     <  OK  >      <Cancel>
```

- **Utilities for network debugging**

  The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follows:



```
                    Please select utility:

            PING       Ping host(IP)
            Trace      Trace routing path
            ShowIF     Display interface settings
            ShowRT     Display routing table
            ShowARP    Display ARP table
            UpTime     Display system up time
            Status     Check service status
            Safe       Set device into 'safe mode'
            SetPower   Set Outputpower
            NTP        Synchronize clock with NTP server
            DMESG      Print the kernel ring buffer
            Main       Main menu

                    <  OK  >      <Cancel>
```

- ➢ Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
- ➢ Trace routing path: Trace and inquire the routing path to a specific target.
- ➢ Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
- ➢ Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
- ➢ Display ARP table: The internal ARP table of the system is displayed.
- ➢ Display system up time: The system live time (time for system being turn on) is displayed.
- ➢ Check service status: Check and display the status of the system.
- ➢ Set device into “safe mode”: If the administrator is unable to use Web Management Interface via browser for the system failed inexplicitly. The administrator can choose this utility and set it into safe mode, which enables him to manage this device with browser again.
- ➢ Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.
- ➢ Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their boot-up messages instead of copying the messages by hand.
- ➢ Main menu: Go back to the main menu.

- **Change admin password**

  Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, we do not need to enter administrator's password to enter the console management interface. But connecting the system by SSH, we have to enter the username and password.

  The username is "admin" and the default password is also "admin", which is the same as for the web management interface. Password can also be changed here. If administrators forget the password and are unable to log in the management interface from the web or the remote end of the SSH, they can still use the null modem to connect the console management interface and set the administrator's password again.

> ⚠ *Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the HS1100 Admin username and password after logging in the system for the first time.*

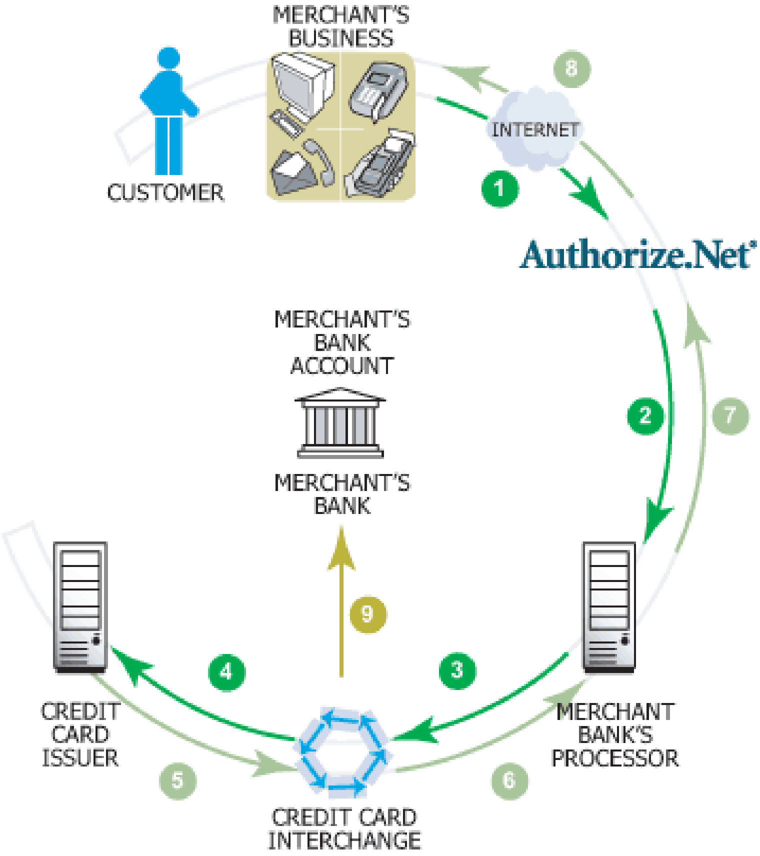
- **Reload factory default**

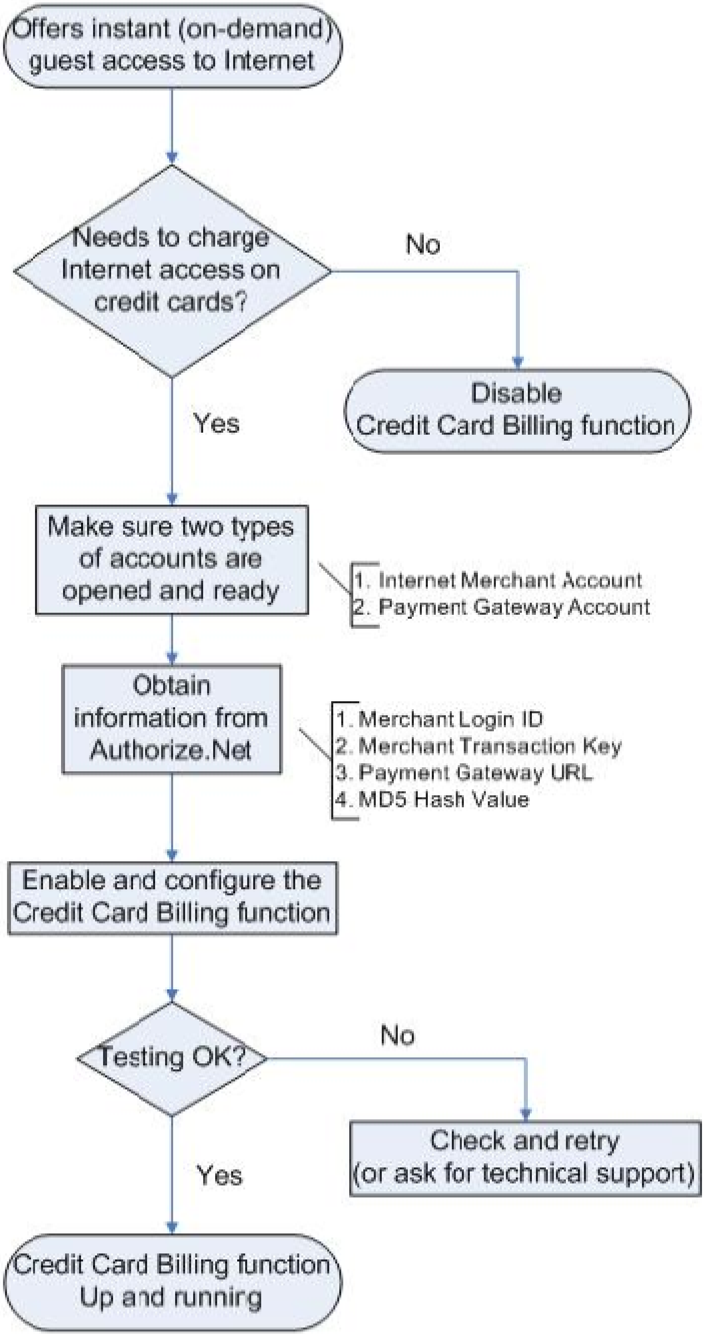
  Choosing this option will reset the system configuration to the factory defaults.
- **Restart HS1100**

  Choosing this option will restart HS1100.

# Appendix B. Accepting Payment via Authorize.Net

This section is to show independent Hotspot owners how to configure related settings in order to accept credit card payments via Authorize.Net, making the Hotspot an e-commerce environment for clients to pay for and obtain Internet access using their credit cards.



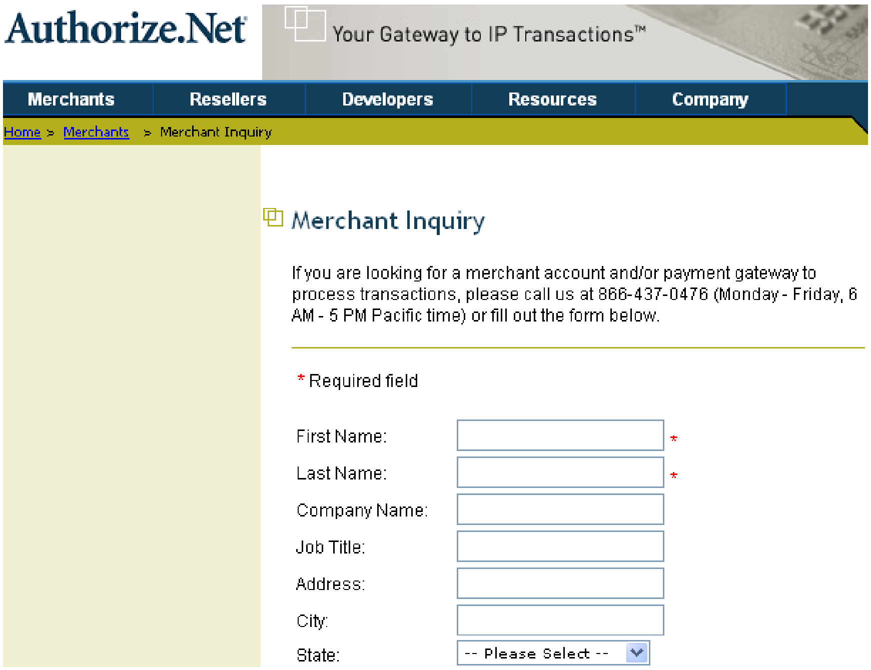

Offers instant (on-demand) guest access to Internet
Needs to charge Internet access on credit cards?
No
Disable Credit Card Billing function
Yes
Make sure two types of accounts are opened and ready
1. Internet Merchant Account
2. Payment Gateway Account
Obtain information from Authorize.Net
1. Merchant Login ID
2. Merchant Transaction Key
3. Payment Gateway URL
4. MD5 Hash Value
Enable and configure the Credit Card Billing function
Testing OK?
No
Check and retry (or ask for technical support)
Yes
Credit Card Billing function Up and running

# 1. Setting Up

## 1.1 Open Accounts

To set up HS1100 to process credit card billing, the merchant owner will need two accounts (Internet Merchant account and Authorize.Net account).

If you are looking for a merchant account or Internet payment gateway to process transactions, you can fill out the Inquiry Form on http://www.authorize.net/solutions/merchantsolutions/merchantinquiryform/.


Authorize.Net
Your Gateway to IP Transactions™
Merchants
Resellers
Developers
Resources
Company
Home > Merchants > Merchant Inquiry

Merchant Inquiry

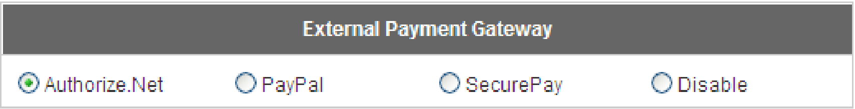
If you are looking for a merchant account and/or payment gateway to process transactions, please call us at 866-437-0476 (Monday - Friday, 6 AM - 5 PM Pacific time) or fill out the form below.

* Required field

| | |
|---|---|
| First Name: | * |
| Last Name: | * |
| Company Name: | |
| Job Title: | |
| Address: | |
| City: | |
| State: | -- Please Select -- |

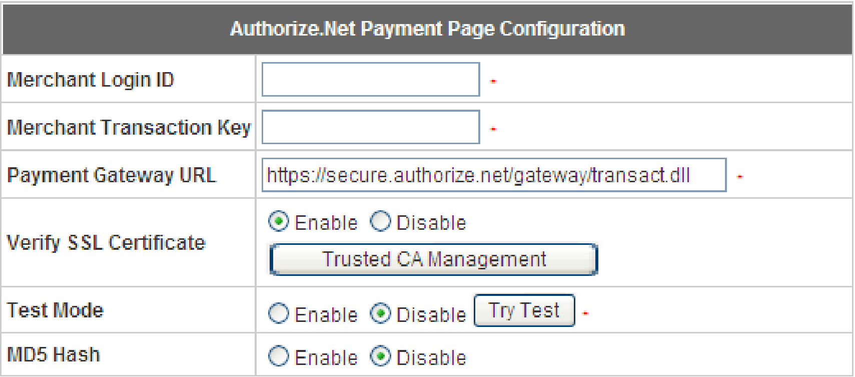
## 1.2 Configure HS1100 using an Authorize.Net account

Please log in HS1100. **User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> On-demand User Server Configuration >>** Click **Payment >> Payment Configuration >> External Payment Gateway >>** Select **Authorize.Net**



External Payment Gateway

● Authorize.Net ○ PayPal ○ SecurePay ○ Disable



| Authorize.Net Payment Page Configuration | |
|---|---|
| Merchant Login ID | * |
| Merchant Transaction Key | * |
| Payment Gateway URL | https://secure.authorize.net/gateway/transact.dll * |
| Verify SSL Certificate | ● Enable ○ Disable<br>Trusted CA Management |
| Test Mode | ○ Enable ● Disable Try Test * |
| MD5 Hash | ○ Enable ● Disable |

Some major fields are required:

| Setting | Description |
|---|---|
| **Merchant Login ID** | This is the "Login ID" that comes with the Authorize.Net account. |
| **Merchant Transaction Key** | To get a new key, please log in Authorize.Net **>>** Click **Settings and Profile >>** Go to the **"Security"** section **>>** Click **Obtain Transaction Key >>** Enter **"Secret Answer" >>** Click ***Submit***. |
| **Payment Gateway URL** | https://secure.authorize.net/gateway/transact.dll (default gateway address) |
| **MD5 Hash** | To enhance the transaction security, merchant owner can choose to enable this function and enter a value in the text box: **"MD5 Hash Value"**. |

⏩ **Note:** For detailed description, please see ***4.2.1.6 Authentication Method >> On-demand User >> Payment***

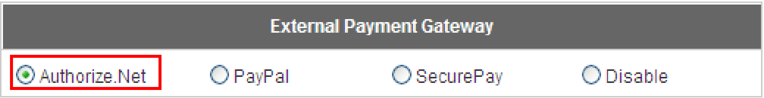
### 1.3 Configure the Authorize.Net Merchant Account to Match the Configuration of HS1100

Settings of the merchant account on Authorize.Net should be matched with the configuration of HS1100:

| Setting | Description |
|---|---|
| **MD5 Hash** | To configure **"MD5 Hash Value"**, please log in Authorize.Net **>>** Click **Settings and Profile >>** Go to the **"Security"** section **>>** Click **MD5 Hash >>** Enter **"New Hash Value"** & **"Confirm Hash Value" >>** Click ***Submit***. |
| **Required Card Code** | If the **"Card Code"** is set up as a required field, please log in Authorize.Net **>>** Click **Settings and Profile >>** Go to the **"Security"** section **>>** Click **Card Code Verification >>** Check the **Does NOT Match (N)** box **>>** Click ***Submit***. |
| **Required Address Fields** | After setting up the required address fields on the **"Credit Card Payment Page Billing Configuration"** section of HS1100, the same requirements must be set on Authorize.Net. To do so, please log in Authorize.Net **>>** Click **Settings and Profile >>** Go to the **"Security"** section **>>** Click **Address Verification System (AVS) >>** Check the boxes accordingly **>>** Click ***Submit***. |

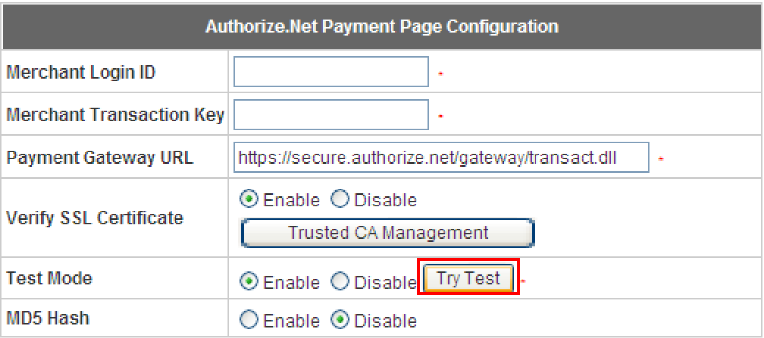
### 1.4 Test The Credit Card Payment via Authorize.Net

To test the connection between HS1100 and Authorize.Net, please log in HS1100. **>> User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> On-demand User Server Configuration >> Payment >> Payment Configuration >>** Select **Authorize.Net >>** Go to "**Authorize.Net Payment Page Configuration**" section **>>** Enable the **"Test Mode" >>** Click **Try Test** and follow the instructions



External Payment Gateway

● Authorize.Net ○ PayPal ○ SecurePay ○ Disable



| Authorize.Net Payment Page Configuration | |
|---|---|
| Merchant Login ID | * |
| Merchant Transaction Key | * |
| Payment Gateway URL | https://secure.authorize.net/gateway/transact.dll * |
| Verify SSL Certificate | ● Enable ○ Disable<br>Trusted CA Management |
| Test Mode | ● Enable ○ Disable Try Test * |
| MD5 Hash | ○ Enable ● Disable |

## 2. Basic Maintenance

In order to maintain the operation, merchant owners will have to manage the accounts and transactions via Authorize.Net as well as HS1100.

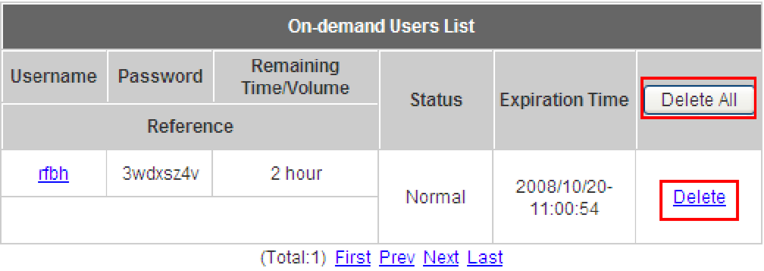
### 2.1 Void A Transaction and Remove the On-demand Account Generated on HS1100

Sometimes, a transaction (as well as the related user account on HS1100) may have to be canceled before it has been settled with the bank.

a. To void an unsettled transaction, please log in Authorize.Net. Click **Unsettled Transactions >>** Locate the specific transaction record on the **"List of Unsettled Transactions" >>** Click the **Trans ID** number **>>** Confirm and click **Void**.

**Note:** To find the on-demand account name, click ***Show Itemized Order Information*** on the **"Order Information"** page **>>** Username can be found in the **"Item Description"**.

b. To remove the specific account from HS1100, please log in HS1100. **>> User Authentication >> Authentication Configuration >>** Click the server **On-demand >> Users List >>** Click **Delete** on the record with the account name. Click ***Delete All*** to delete all users at once.



On-demand Users List

| Username | Password | Remaining Time/Volume | Status | Expiration Time | Delete All |
|---|---|---|---|---|---|
| Reference | | | | | |
| rfbh | 3wdxsz4v | 2 hour | Normal | 2008/10/20-11:00:54 | Delete |

(Total:1) First Prev Next Last

### 2.2 Refund A Settled Transaction and Remove the On-demand Account Generated on HS1100

a. To refund a credit card payment, please log in Authorize.Net. Click **Virtual Terminal >>** Select a Payment Method **>>** Click **Refund a Credit Card >> Payment/Authorization Information >>** Type information in at least three fields: **Card Number**, **Expiration Date**, and **Amount >>** Confirm and click ***Submit***.

b. To remove the specific account from HS1100, please log in HS1100. **>> User Authentication >>**

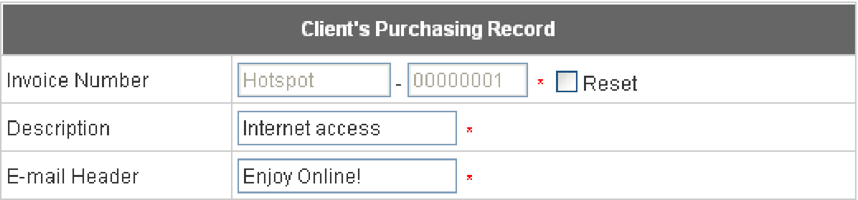
**Authentication Configuration >>** Click the server **On-demand User >> On-demand User Server Configuration >> Users List >>** Click **Delete** on the record with the account name.

### 2.3 Find the Username and Password for A Specific Customer

Please log in Authorize.Net. Click **Unsettled Transactions >>** Try to locate the specific transaction record on the **"List of Unsettled Transactions" >>** Click the **Trans ID** number **>>** Click **Show Itemized Order Information** in the **"Order Information"** section **>>** Username and Password can be found in the **"Item Description"**.

### 2.4 Send An Email Receipt to A Customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via Authorize.Net. To change the information on the receipt for customer, please log in HS1100. **>> User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> On-demand User Server Configuration >> Payment >> Payment Configuration >> External Payment Gateway >>** Select **Authorize.NET >>** Scroll down to **Client's Purchasing Record** section of the page **>>** Type in information in the text boxes: "**Description" and "E-mail Header" >>** Confirm and click ***Apply***.



| Client's Purchasing Record | |
|---|---|
| Invoice Number | Hotspot - 00000001 * □ Reset |
| Description | Internet access * |
| E-mail Header | Enjoy Online! * |

### 2.5 Send an Email Receipt for Each Transaction to the Merchant Owner

A copy of email receipt with payment details for each successful transaction will also be automatically sent to the merchant owner/administrator via Authorize.Net.

To configure the contact person who will receive a receipt for each transaction, please log in Authorize.Net. Click **Settings and Profile >>** Go to the **"General"** section **>>** Click **Manage Contacts >>** Click **Add New Contact** to **>>** Enter necessary contact information on this page **>>** Check the **"Transaction Receipt"** box **>>** Click ***Submit***.

## 3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

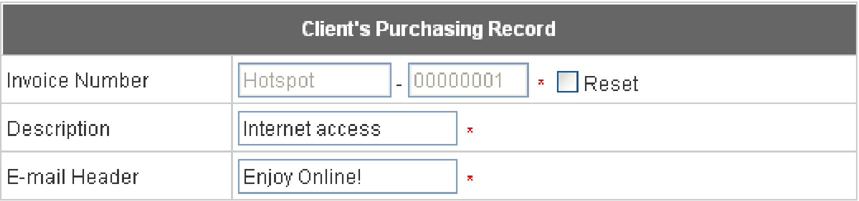
### 3.1 Transaction Statistics by Credit Card Type during the Period.

Please log in Authorize.Net. **>>** Click **Reports >>** Check **"Statistics by Settlement Date"** radio button **>>** Select **"Transaction Type"**, **"Start Date"**, and **"End Date"** as the criteria **>>** Click ***Run Report***.

### 3.2 Transaction Statistics by Different Location

a. To deploy more than one HS1100, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in HS1100. **>> User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> On-demand User Server**

**Configuration >> Payment >> Payment Configuration >> External Payment Gateway >>** Select **Authorize.NET >>** Scroll down to **"Client's Purchasing Record"** section of the page **>>** Check the **"Reset"** box **>>** A location-specific ID (for example, Hotspot-A) can be used as the first part of **"Invoice Number" >>** Confirm and click ***Apply***.



| Client's Purchasing Record | |
|---|---|
| Invoice Number | Hotspot - 00000001 * □ Reset |
| Description | Internet access * |
| E-mail Header | Enjoy Online! * |

b. Please log in Authorize.Net **>>** Click **Search and Download >>** Specify the transaction period (or ALL Settled, Unsettled) in **"Settlement Date"** section **>>** Go to **"Transaction"** section **>>** Enter the first part of invoice number plus an asterisk character (for example, Hotspot-A*) in the **"Invoice #"** text box **>>** Click ***Search* >>** If transaction records can be found, the number of accounts sold is the number of search results **>>** Or, click **Download To File** to download records and then use MS Excel to generate more detailed reports.

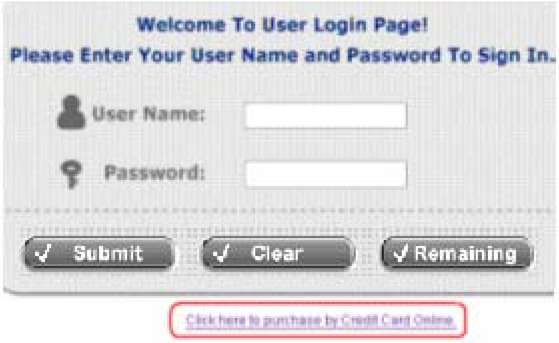
### 3.3 Search for The Transaction Details for A Specific Customer

Please log in Authorize.Net. Click **Search and Download >>** Enter the information for a specific customer as criteria **>>** Click ***Search* >>** Click the **Trans ID** number to view the transaction details.

⏩ **Note:** For more information about **Authorize.Net**, please see **http://www.authorize.net**.

## 4. Examples of Making Payment for Clients

**Step 1:** Click the link below the login window to pay for the service by credit card via Authorize.Net.



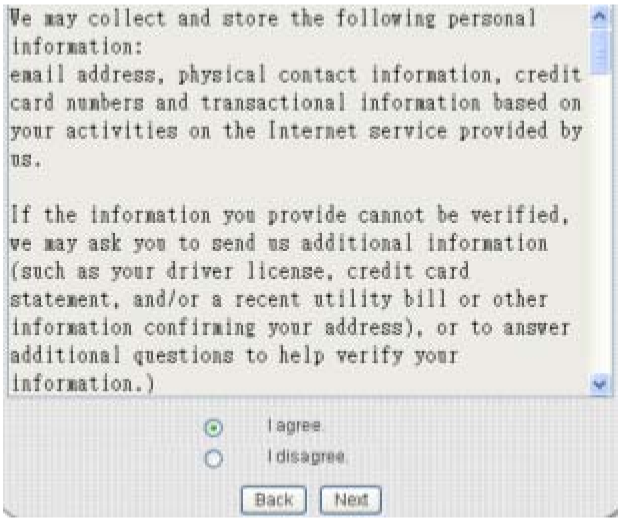
Welcome To User Login Page!

Please Enter Your User Name and Password To Sign In.

User Name:

Password:

**Step 2:** Choose ***I agree*** to accept the terms of use and click ***Next***.

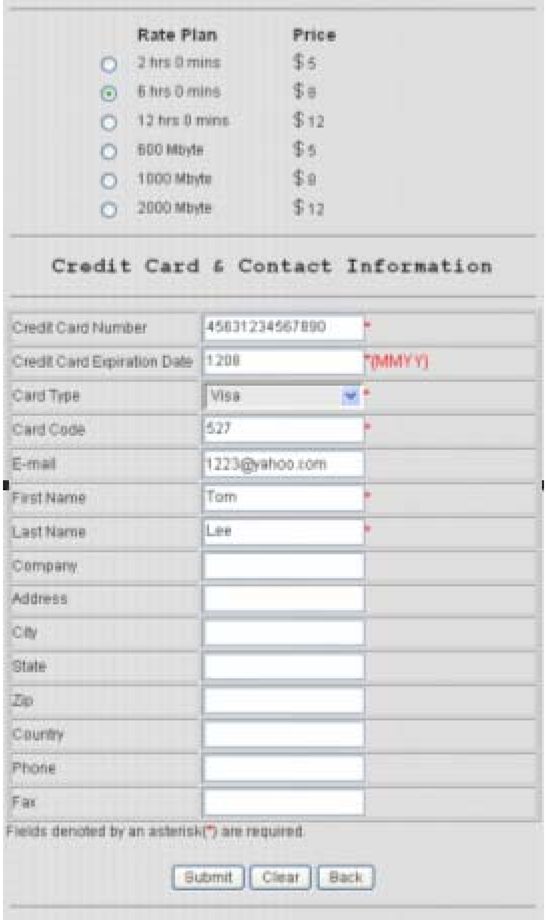


We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)

● I agree.
○ I disagree.

**Step 3:** Please fill out the form and Click ***Submit*** to send out this transaction. There will be a confirm dialog box.



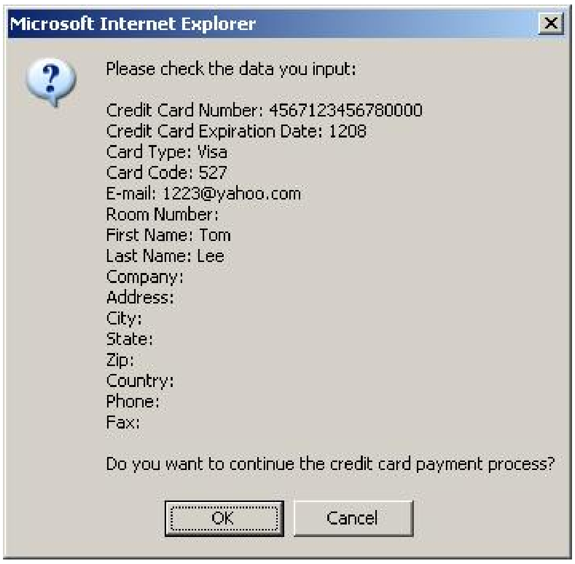
| | Rate Plan | Price |
|---|---|---|
| ○ | 2 hrs 0 mins | $5 |
| ● | 6 hrs 0 mins | $8 |
| ○ | 12 hrs 0 mins | $12 |
| ○ | 600 Mbyte | $5 |
| ○ | 1000 Mbyte | $8 |
| ○ | 2000 Mbyte | $12 |

Credit Card & Contact Information

| | | |
|---|---|---|
| Credit Card Number | 45631234567890 | * |
| Credit Card Expiration Date | 1208 | *(MMYY) |
| Card Type | Visa | * |
| Card Code | 527 | * |
| E-mail | 1223@yahoo.com | |
| First Name | Tom | * |
| Last Name | Lee | * |
| Company | | |
| Address | | |
| City | | |
| State | | |
| Zip | | |
| Country | | |
| Phone | | |
| Fax | | |

Fields denoted by an asterisk(*) are required.

**Step 4:** Please confirm the data and the click ***OK*** to go on the transaction or click ***Cance*l** to revise the data or cancel this transaction. After clicking OK, there will be another dialog box showing up to confirm this transaction again.



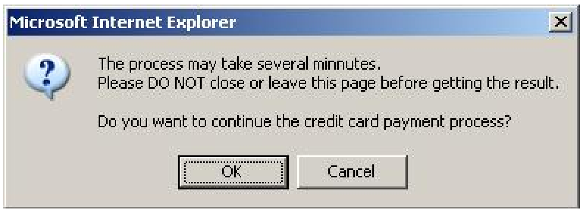
Microsoft Internet Explorer

Please check the data you input:

Credit Card Number: 4567123456780000
Credit Card Expiration Date: 1208
Card Type: Visa
Card Code: 527
E-mail: 1223@yahoo.com
Room Number:
First Name: Tom
Last Name: Lee
Company:
Address:
City:
State:
Zip:
Country:
Phone:
Fax:

Do you want to continue the credit card payment process?

**Step 5:** Click ***OK*** to complete the process or click ***Cancel*** to revise the data or cancel this transaction.

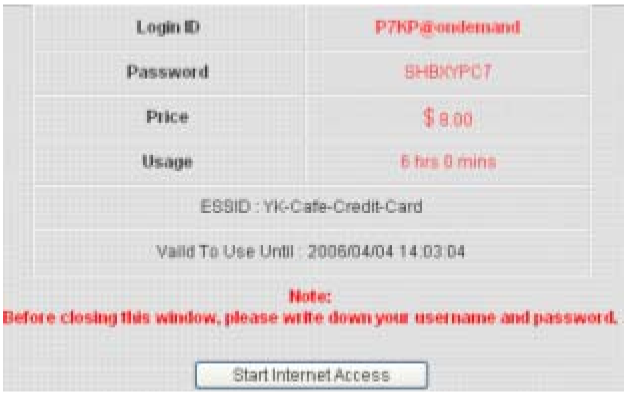


Microsoft Internet Explorer

The process may take several minnutes.
Please DO NOT close or leave this page before getting the result.

Do you want to continue the credit card payment process?

**Step 6:** Click ***Start Internet Access*** to use the Internet access service.



| | |
|---|---|
| Login ID | P7KP@ondemand |
| Password | SHBXYPC7 |
| Price | $ 8.00 |
| Usage | 6 hrs 0 mins |

ESSID : YK-Cafe-Credit-Card

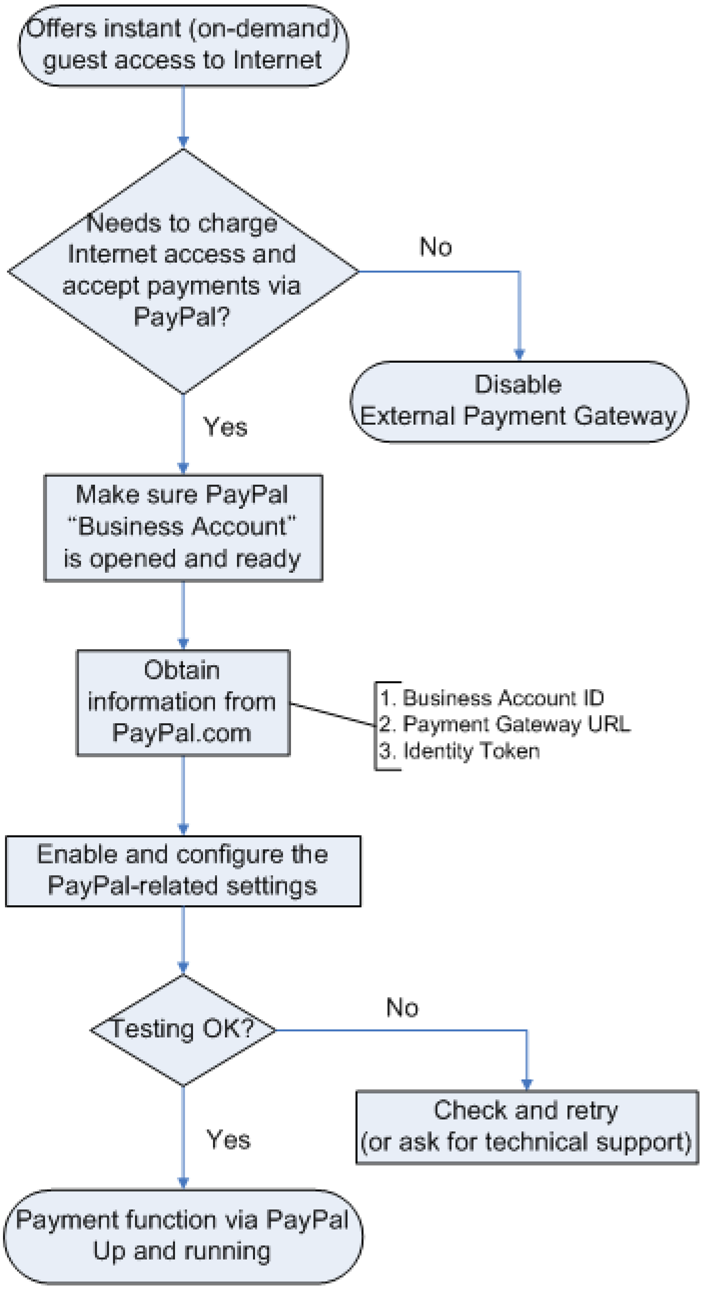
Valid To Use Until : 2006/04/04 14:03:04

**Note:**
**Before closing this window, please write down your username and password.**

⏩ **Note:** The clients must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If clients choose to enter the e-mail addresses, clients will receive confirmation letters for reference.

# Appendix C. Accepting Payment via PayPal

This section is to show independent Hotspot owners how to configure related settings in order to accept payments via PayPal, making the Hotspot an e-commerce environment for clients to pay for and obtain Internet access using their PayPal accounts or credit cards.


Offers instant (on-demand) guest access to Internet
Needs to charge Internet access and accept payments via PayPal?
No
Disable External Payment Gateway
Yes
Make sure PayPal "Business Account" is opened and ready
Obtain information from PayPal.com
1. Business Account ID
2. Payment Gateway URL
3. Identity Token
Enable and configure the PayPal-related settings
Testing OK?
No
Check and retry (or ask for technical support)
Yes
Payment function via PayPal Up and running

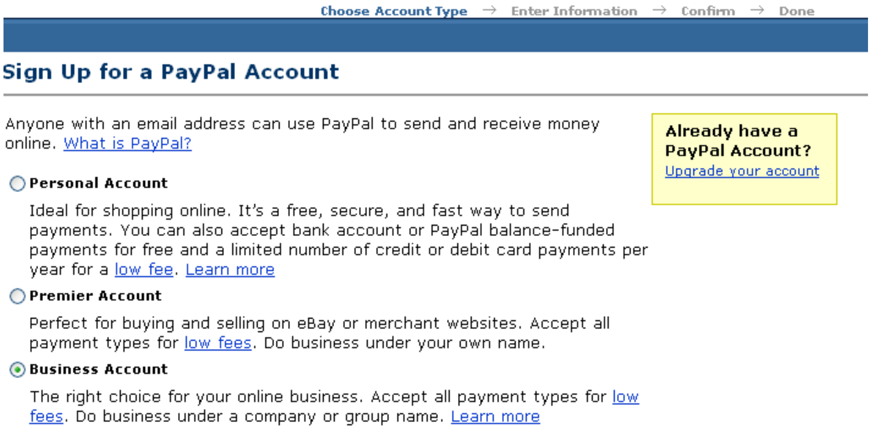
# 1. Setting Up

As follows are the basic steps to open and configure a “**Business Account**” on **PayPal**.

## 1.1 Open An Account

**Step 1: Sign up for a PayPal Business Account and login.**

Here is a link: https://www.paypal.com/cgi-bin/webscr?cmd=_registration-run



Choose Account Type → Enter Information → Confirm → Done

Sign Up for a PayPal Account

Anyone with an email address can use PayPal to send and receive money online. What is PayPal?

○ Personal Account

Ideal for shopping online. It’s a free, secure, and fast way to send payments. You can also accept bank account or PayPal balance-funded payments for free and a limited number of credit or debit card payments per year for a low fee. Learn more

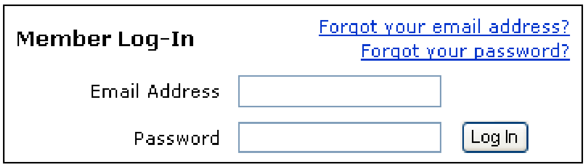
○ Premier Account

Perfect for buying and selling on eBay or merchant websites. Accept all payment types for low fees. Do business under your own name.

● Business Account

The right choice for your online business. Accept all payment types for low fees. Do business under a company or group name. Learn more

Already have a PayPal Account?
Upgrade your account



Member Log-In

Forgot your email address?
Forgot your password?

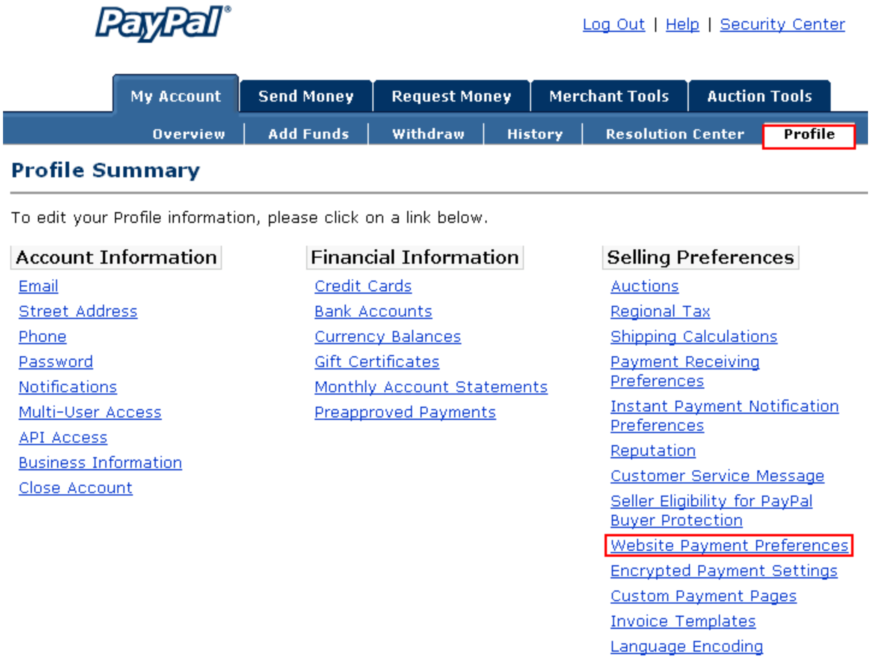
Email Address

Password

Log In

**Step 2: Edit necessary settings in “Website Payment Preferences”**

Click **Profile >>** Click **Website Payment Preferences** in the **Selling Preferences** section



Log Out | Help | Security Center

My Account | Send Money | Request Money | Merchant Tools | Auction Tools

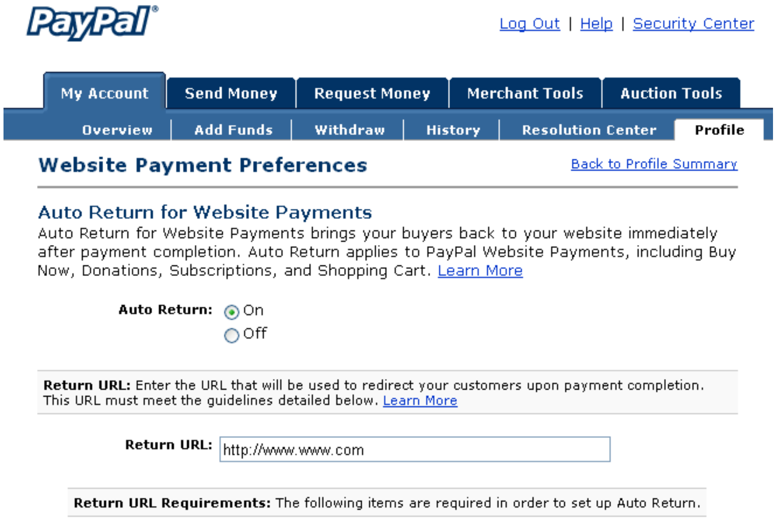
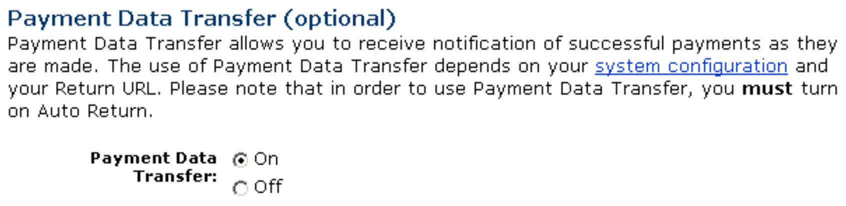
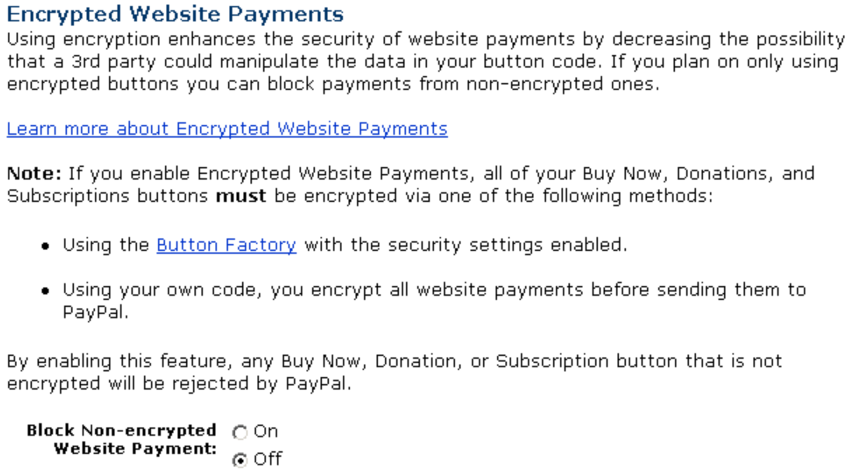
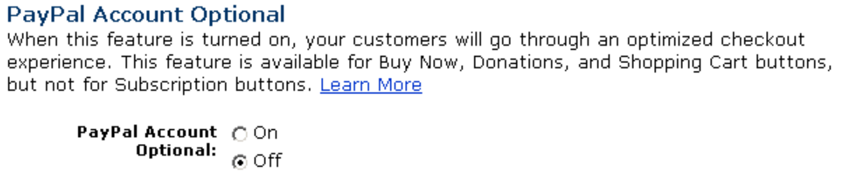
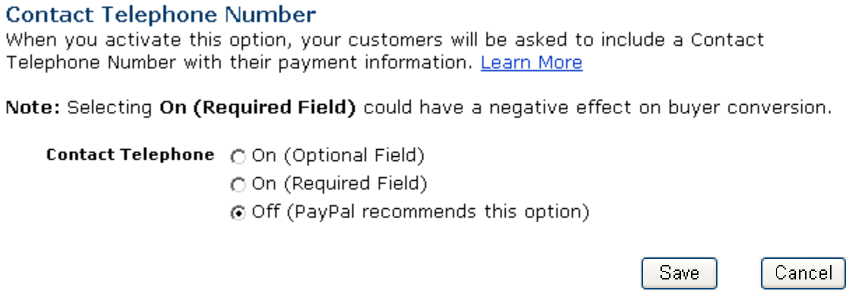
Overview | Add Funds | Withdraw | History | Resolution Center | Profile

Profile Summary

To edit your Profile information, please click on a link below.

| Account Information | Financial Information | Selling Preferences |
|---|---|---|
| Email | Credit Cards | Auctions |
| Street Address | Bank Accounts | Regional Tax |
| Phone | Currency Balances | Shipping Calculations |
| Password | Gift Certificates | Payment Receiving Preferences |
| Notifications | Monthly Account Statements | Instant Payment Notification Preferences |
| Multi-User Access | Preapproved Payments | Reputation |
| API Access | | Customer Service Message |
| Business Information | | Seller Eligibility for PayPal Buyer Protection |
| Close Account | | Website Payment Preferences |
| | | Encrypted Payment Settings |
| | | Custom Payment Pages |
| | | Invoice Templates |
| | | Language Encoding |

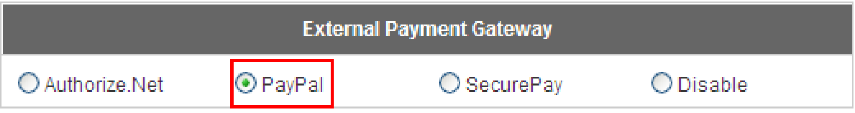
Administrators should scroll down to edit each setting as shown in the table below. To activate all the changes, please click ***Save*** at the end of the page.

| Settings | Screenshots |
|---|---|
| **Auto Return (On)**<br>**Return URL (Redirect Webpage)**<br>Type http://www.www.com or other URL. | <br> Log Out \| Help \| Security Center<br>My Account<br>Send Money<br>Request Money<br>Merchant Tools<br>Auction Tools<br>Overview<br>Add Funds<br>Withdraw<br>History<br>Resolution Center<br>Profile<br>Back to Profile Summary<br>**Website Payment Preferences**<br>**Auto Return for Website Payments**<br>Auto Return for Website Payments brings your buyers back to your website immediately after payment completion. Auto Return applies to PayPal Website Payments, including Buy Now, Donations, Subscriptions, and Shopping Cart. Learn More<br>**Auto Return:** ● On ○ Off<br>**Return URL:** Enter the URL that will be used to redirect your customers upon payment completion. This URL must meet the guidelines detailed below. Learn More<br>**Return URL:** http://www.www.com<br>**Return URL Requirements:** The following items are required in order to set up Auto Return. |
| **Payment Data Transfer (On)** | <br>**Payment Data Transfer (optional)**<br>Payment Data Transfer allows you to receive notification of successful payments as they are made. The use of Payment Data Transfer depends on your system configuration and your Return URL. Please note that in order to use Payment Data Transfer, you **must** turn on Auto Return.<br>**Payment Data Transfer:** ● On ○ Off |
| **Block Non-encrypted Website Payment (Off)** | <br>**Encrypted Website Payments**<br>Using encryption enhances the security of website payments by decreasing the possibility that a 3rd party could manipulate the data in your button code. If you plan on only using encrypted buttons you can block payments from non-encrypted ones.<br>Learn more about Encrypted Website Payments<br>**Note:** If you enable Encrypted Website Payments, all of your Buy Now, Donations, and Subscriptions buttons **must** be encrypted via one of the following methods:<br>• Using the Button Factory with the security settings enabled.<br>• Using your own code, you encrypt all website payments before sending them to PayPal.<br>By enabling this feature, any Buy Now, Donation, or Subscription button that is not encrypted will be rejected by PayPal.<br>**Block Non-encrypted Website Payment:** ○ On ● Off |
| **PayPal Account Optional (Off)** | <br>**PayPal Account Optional**<br>When this feature is turned on, your customers will go through an optimized checkout experience. This feature is available for Buy Now, Donations, and Shopping Cart buttons, but not for Subscription buttons. Learn More<br>**PayPal Account Optional:** ○ On ● Off |
| **Contact Telephone Number (Off)**<br>**Click *Save.*** | <br>**Contact Telephone Number**<br>When you activate this option, your customers will be asked to include a Contact Telephone Number with their payment information. Learn More<br>**Note:** Selecting **On (Required Field)** could have a negative effect on buyer conversion.<br>**Contact Telephone** ○ On (Optional Field)<br>○ On (Required Field)<br>● Off (PayPal recommends this option)<br> |

## 1.2 Configure HS1100 with a PayPal Business Account

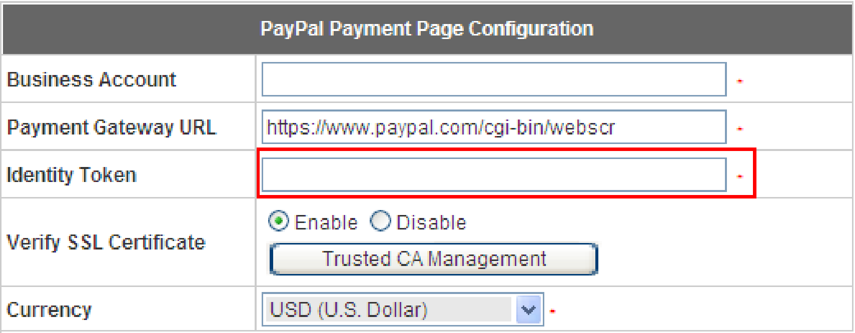
Please log in HS1100:

**User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> On-demand User Server Configuration >>** Click **Payment >> Payment Configuration >> External Payment Gateway >>** Select **PayPal**



External Payment Gateway

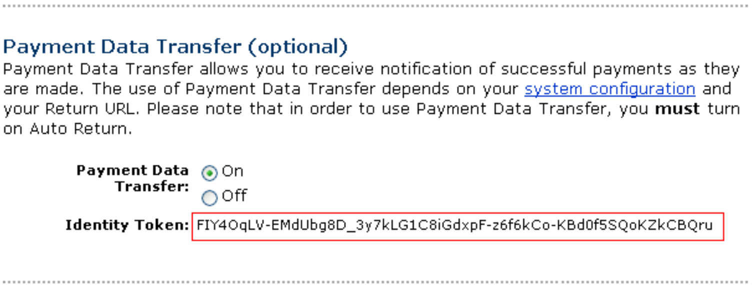
○ Authorize.Net ● PayPal ○ SecurePay ○ Disable

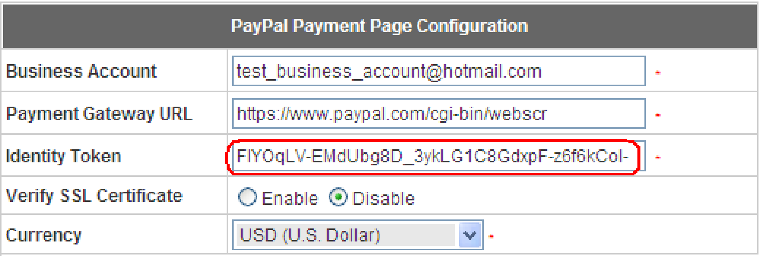


PayPal Payment Page Configuration

| | |
|---|---|
| Business Account | - |
| Payment Gateway URL | https://www.paypal.com/cgi-bin/webscr - |
| Identity Token | - |
| Verify SSL Certificate | ● Enable ○ Disable<br>Trusted CA Management |
| Currency | USD (U.S. Dollar) - |

Three fields are required:

| Setting | Description |
|---|---|
| **Business Account ID** | This is the "Login ID" (email address) that is associated with the PayPal Business Account. |
| **Payment Gateway URL** | https://www.paypal.com/cgi-bin/webscr (default URL for PayPal) |
| **Identity Token** | Please log in PayPal after saving the above settings **>>** Click **Profile >>** Click **Website Payment Preferences** in the **Selling Preferences** section **>>** Scroll down to the section, **Payment Data Transfer (optional)**.<br><br>Payment Data Transfer (optional)<br>Payment Data Transfer allows you to receive notification of successful payments as they are made. The use of Payment Data Transfer depends on your system configuration and your Return URL. Please note that in order to use Payment Data Transfer, you **must** turn on Auto Return.<br>**Payment Data Transfer:** ● On ○ Off<br>**Identity Token:** FIY4OqLV-EMdUbg8D_3y7kLG1C8iGdxpF-z6f6kCo-KBd0f5SQoKZkCBQru<br>Copy the **Identity Token** in the above page to the section "**PayPal Payment Page Configuration**" of HS1100. |

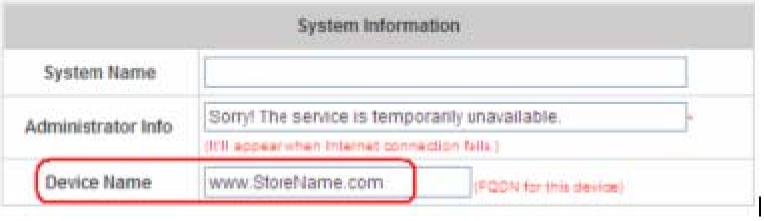


PayPal Payment Page Configuration

| | |
|---|---|
| Business Account | test_business_account@hotmail.com - |
| Payment Gateway URL | https://www.paypal.com/cgi-bin/webscr - |
| Identity Token | FIYOqLV-EMdUbg8D_3ykLG1C8GdxpF-z6f6kCol- - |
| Verify SSL Certificate | ○ Enable ● Disable |
| Currency | USD (U.S. Dollar) - |

### 1.3 Requirements for Building a Secure PayPal-based E-Commerce Site

To deploy the PayPal function properly, it is required that the merchant register an **Internet domain name** (for example, www.StoreName.com) for this subscriber gateway device.



System Information

| | |
|---|---|
| System Name | |
| Administrator Info | Sorry! The service is temporarily unavailable. -<br>(It'll appear when Internet connection fails.) |
| Device Name | www.StoreName.com (FQDN for this device) |

In addition, it is necessary to sign up for a **SSL certificate**, licensed from a "**Certificate Authority**" (for example, **VerSign**), for this registered Internet domain name.

Thus, by meeting these two requirements, it will allow end customers or subscribers to pay for the Internet access in a securer and convenient way.

## 2. Basic Maintenance

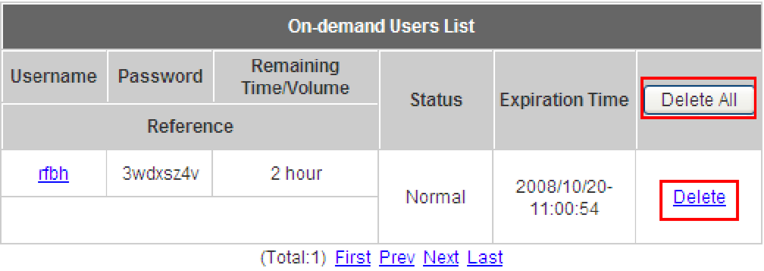
In order to maintain the operation, the merchant owner will have to manage the accounts and payment transactions on PayPal website as well as HS1100.

### 2.1 Refund a completed payment and remove the on-demand account generated on HS1100

(1) To refund a payment, please log in PayPal **>>** Click **History >>** Locate the specific payment listing in the activity history log **>>** Click **Details** of the payment listing **>>** Click **Refund Payment** at the end of the details page **>>** Type in information: **Gross Refund Amount** and/or **Optional Note to Buyer >>** Click ***Submit* >>** Confirm the details and click ***Process Refund***

(2) To remove the specific account from HS1100, please log in HS1100:

**User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> On-demand User Server Configuration >> Users List >>** Click **Delete** on the record with the account ID. Click ***Delete All*** to delete all users at once.



On-demand Users List

| Username | Password | Remaining Time/Volume | Status | Expiration Time | Delete All |
|---|---|---|---|---|---|
| Reference | | | | | |
| rfbh | 3wdxsz4v | 2 hour | Normal | 2008/10/20-11:00:54 | Delete |

(Total:1) First Prev Next Last

## 2.2 Find the username and password for a specific customer

(1) To find the username, please log in PayPal **>>** Click **History >>** Locate the specific payment listing in the activity history log **>>** Click **Details** of the payment listing **>>** Username can be found in the **"Item Title"** field

(2) To find the password associated with a specific username, please log in HS1100:

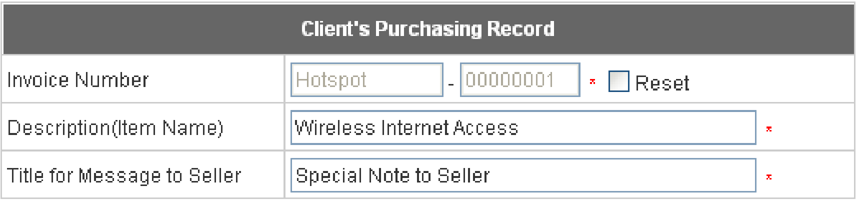
**User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> On-demand User Server Configuration >> Users List**. Search for the specific username. Password can be found in the same record

⏩ **Note:** As stated by PayPal, you can issue a full or partial refund for any reason and for **60 days** after the original payment was sent. To find the on-demand account name for a specific payment, click ***Details*** of the payment listing in the activity history log **>> Username** can be found in the **"Item Title"** field.

## 2.3 Send an email receipt to a customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via PayPal. To change the information on the receipt for customer, please log in HS1100:

**User Authentication >> Authentication Configuration >>** Click the server **On-demand User >> On-demand User Server Configuration >> Payment >> Payment Configuration >> External Payment Gateway>>** Select **PayPal >>** Go to "**Client's Purchasing Record**" section **>>** Type in information in the text boxes: **Invoice Number** and **Description (Item Name) >>** Confirm and click ***Apply***



Client's Purchasing Record

| | |
|---|---|
| Invoice Number | Hotspot - 00000001 * ☐ Reset |
| Description(Item Name) | Wireless Internet Access * |
| Title for Message to Seller | Special Note to Seller * |

## 2.4 Send an email receipt for each transaction to the merchant

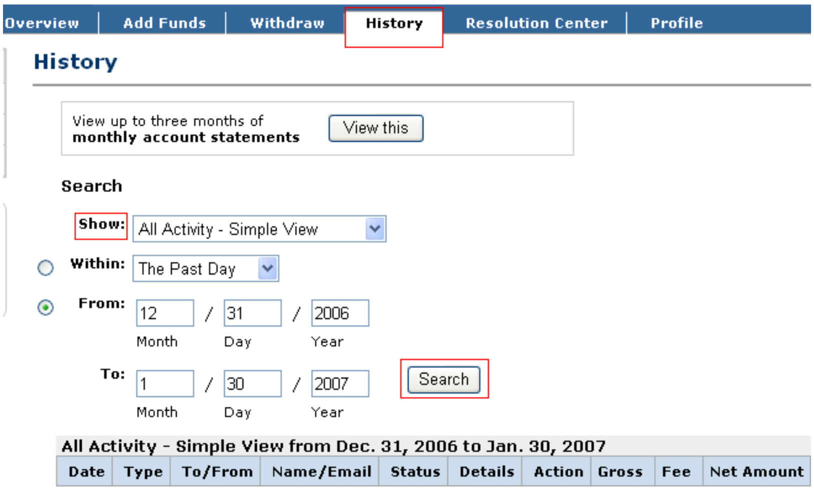
A copy of email receipt with payment details (including available message note from buyer) for each successful transaction will also be automatically sent to the merchant owner/administrator via PayPal.

# 3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

## 3.1 Transaction activity during a period

(1) Please log in PayPal **>>** Click **History >>** Choose activity type from the **Show** field as the search criteria **>>** Specify the dates (**From** and **To** fields) for the period **>>** Click ***Search***



History

View up to three months of **monthly account statements**

Search

Show: All Activity - Simple View

○ Within: The Past Day

● From: 12 / 31 / 2006 (Month / Day / Year)

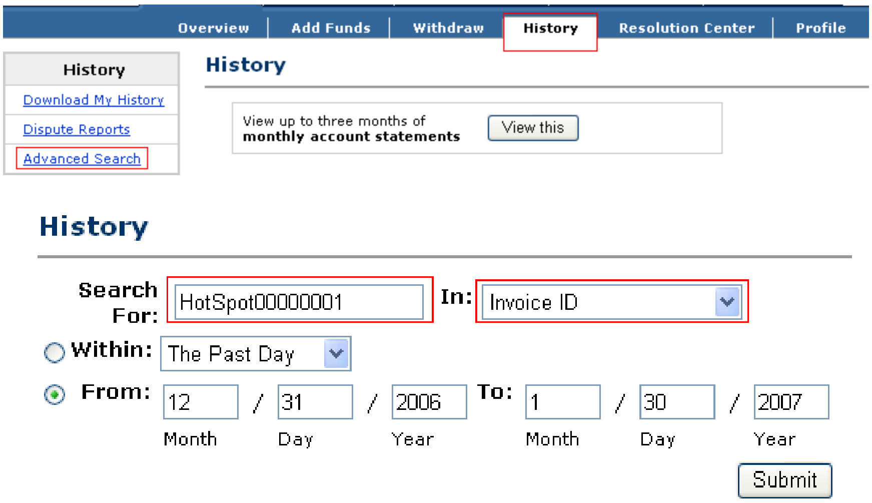
To: 1 / 30 / 2007 (Month / Day / Year)

All Activity - Simple View from Dec. 31, 2006 to Jan. 30, 2007

| Date | Type | To/From | Name/Email | Status | Details | Action | Gross | Fee | Net Amount |
|---|---|---|---|---|---|---|---|---|---|

## 3.2 Search for the transaction details for a specific customer

Please log in PayPal **>>** Click **History >>** Click **Advanced Search >>** Enter the name for a specific customer as criteria in the **Search For** field and Choose Last Name or First Name in the **In** field **>>** Specify the time period **>>** Click ***Submit* >>** Click **Details** to view the transaction details



History

View up to three months of **monthly account statements**

History

Search For: HotSpot00000001 In: Invoice ID

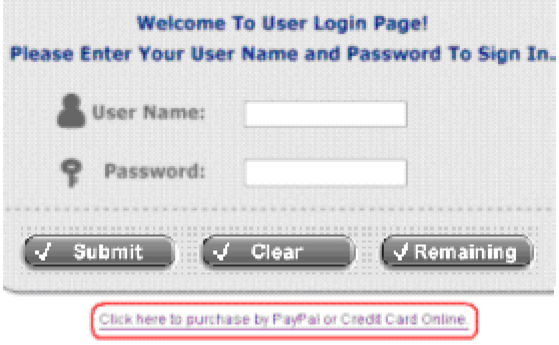
○ Within: The Past Day

● From: 12 / 31 / 2006 (Month / Day / Year) To: 1 / 30 / 2007 (Month / Day / Year)

⏩ **Note:** For more information about **PayPal**, please see **http://www.paypal.com**.

# 4. Examples of Making Payment for Clients

**Step 1:** Click the link below the login window to pay for the service via PayPal.

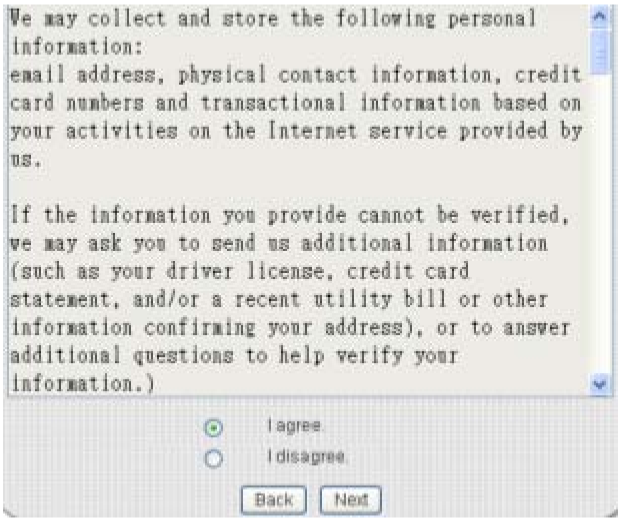


Welcome To User Login Page!
Please Enter Your User Name and Password To Sign In.

User Name:

Password:

**Step 2:** Choose ***I agree*** to accept the terms of use and click ***Next***.

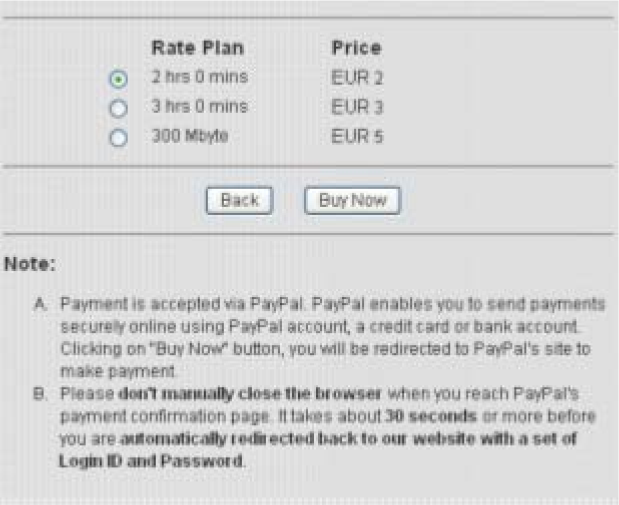


We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)

● I agree
○ I disagree

**Step 3:** Please fill out the form and Click ***Submit*** to send out this transaction. There will be a confirm dialog box.

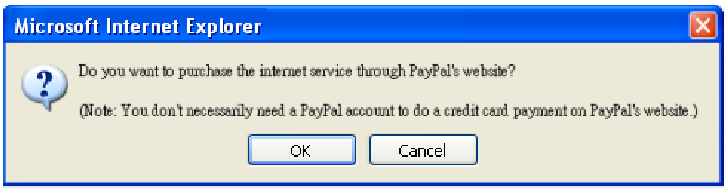


| | Rate Plan | Price |
|---|---|---|
| ● | 2 hrs 0 mins | EUR 2 |
| ○ | 3 hrs 0 mins | EUR 3 |
| ○ | 300 Mbyte | EUR 5 |

Note:

A. Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button, you will be redirected to PayPal's site to make payment.

B. Please **don't manually close the browser** when you reach PayPal's payment confirmation page. It takes about **30 seconds** or more before you are **automatically redirected back to our website with a set of Login ID and Password**.

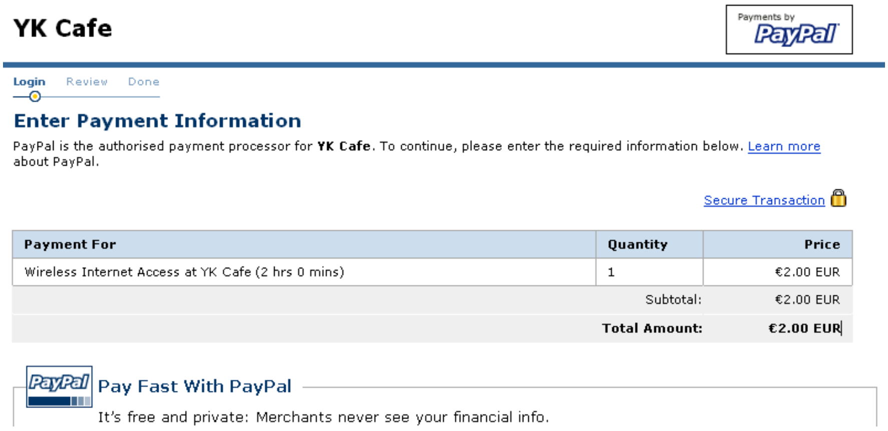


Microsoft Internet Explorer

Do you want to purchase the internet service through PayPal's website?

(Note: You don't necessarily need a PayPal account to do a credit card payment on PayPal's website.)

**Step 4:** You will be redirected to PayPal website to complete the payment process.



YK Cafe

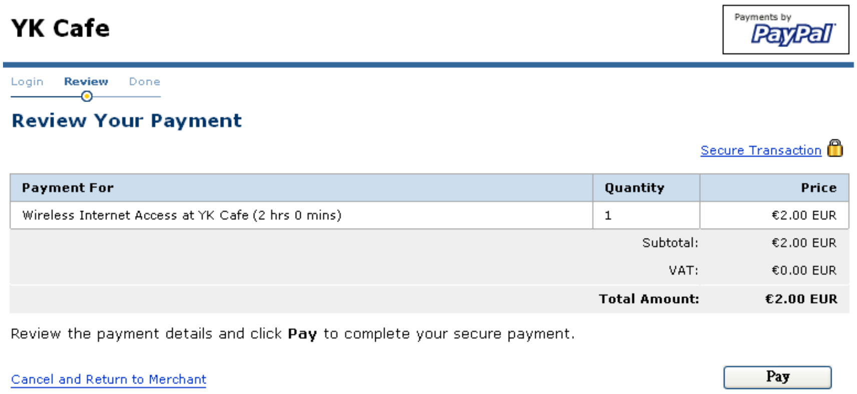
Enter Payment Information

PayPal is the authorised payment processor for **YK Cafe**. To continue, please enter the required information below. Learn more about PayPal.

Secure Transaction

| Payment For | Quantity | Price |
|---|---|---|
| Wireless Internet Access at YK Cafe (2 hrs 0 mins) | 1 | €2.00 EUR |
| | Subtotal: | €2.00 EUR |
| | **Total Amount:** | **€2.00 EUR** |

It's free and private: Merchants never see your financial info.



YK Cafe

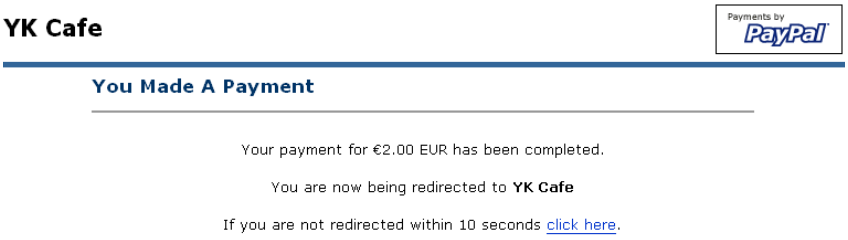
Review Your Payment

Secure Transaction

| Payment For | Quantity | Price |
|---|---|---|
| Wireless Internet Access at YK Cafe (2 hrs 0 mins) | 1 | €2.00 EUR |
| | Subtotal: | €2.00 EUR |
| | VAT: | €0.00 EUR |
| | **Total Amount:** | **€2.00 EUR** |

Review the payment details and click **Pay** to complete your secure payment.

Cancel and Return to Merchant



YK Cafe

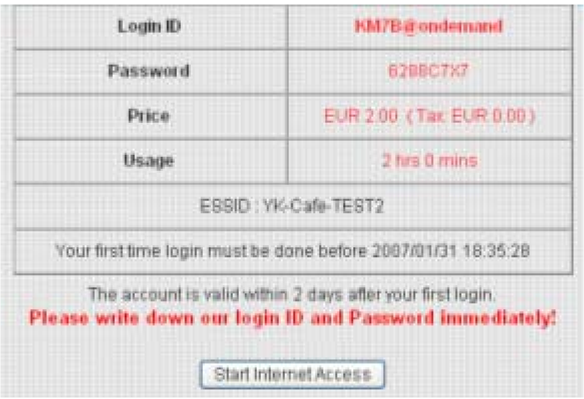
You Made A Payment

Your payment for €2.00 EUR has been completed.

You are now being redirected to **YK Cafe**

If you are not redirected within 10 seconds click here.

**Step 5:** Click ***Start Internet Access*** to use the Internet access service.



| | |
|---|---|
| Login ID | KM7B@ondemand |
| Password | 6288C7X7 |
| Price | EUR 2.00 ( Tax EUR 0.00 ) |
| Usage | 2 hrs 0 mins |
| ESSID : YK-Cafe-TEST2 | |
| Your first time login must be done before 2007/01/31 18:35:28 | |

The account is valid within 2 days after your first login.

**Please write down our login ID and Password immediately!**

|  |  |  |
|---|---|---|
| ⏩ **Note:** | *(a)* | Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on ***Buy Now*** button, you will be redirected to PayPal’s site to make payment. |
|  | *(b)* | Please **do not manually close the browser** when you reach PayPal’s payment confirmation page. It takes about 30 seconds or more before you are **automatically redirected back to our website with a set of Login ID and Password**. |

# *Appendix D. Accepting Payment via SecurePay*

## ▪ How to use SecurePay

SecurePay is another external online payment gateway compatible with HS1100. This section guides you how to get SecurePay working with HS1100 and how to check today's billing transactions, and teaches your clients how to purchase or renew different network-access plans online using their credit cards.

## ▪ For Administrators to get started

Before getting started, administrators need to apply for a "Merchant ID" and "Merchant Password" from the "SecurePay" official website.

In this example, merchant account one starting with plan one is

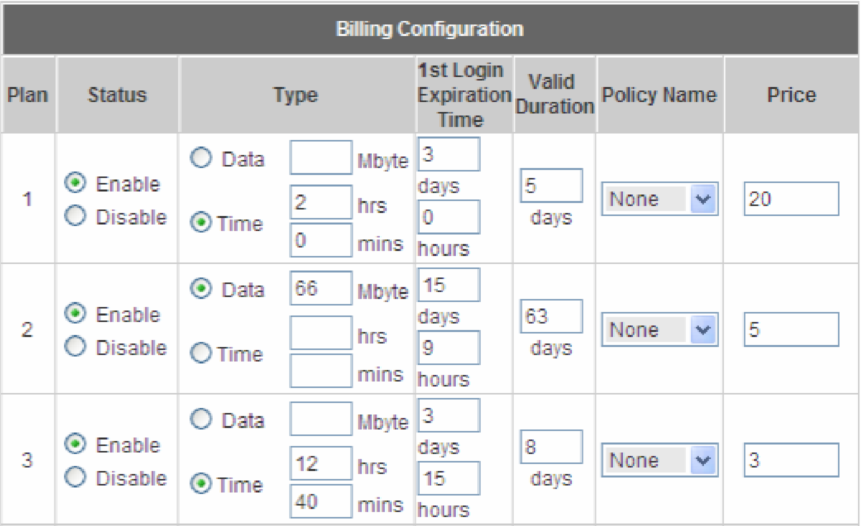
SecurePay Merchant *ID*: ABC0001

SecurePay Merchant *Password*: abc123

*1.* Create billing plans:

Administrators may come up with many ways to charge their clients. For example:

- Plan 2 (charged by Data): Each Plan 2 client has to make their first login within 15 days and 9 hours. He can transfer up to 66 Mbytes and this account is valid for 63 days. He's being charged 5 dollars for this plan.
- Plan 3 (charged by Time): Each Plan 3 client has to make their first login within 3 days and 15 hours. He can access the internet for 12 hour and 40 minutes and this account is valid for 8 days. He's being charged 3 dollars for this plan.



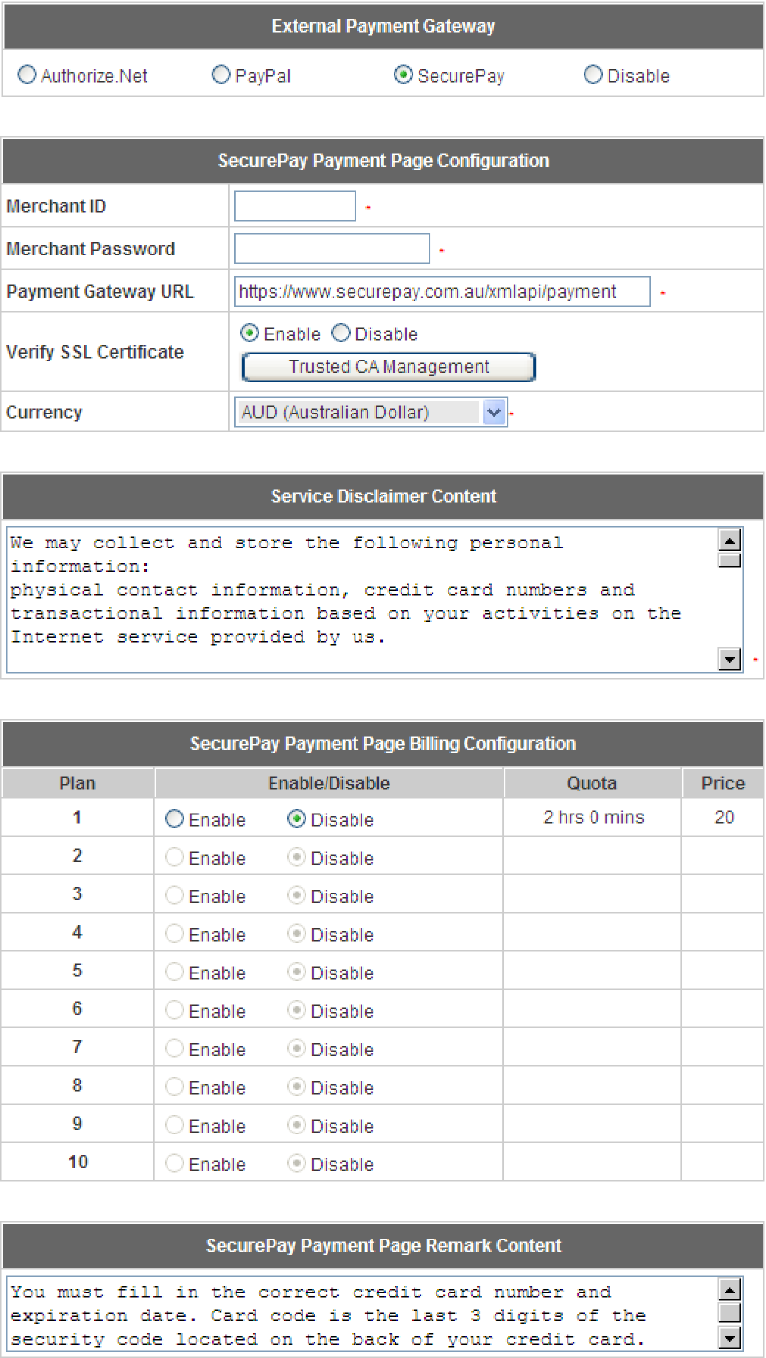
Billing Configuration

| Plan | Status | Type | 1st Login Expiration Time | Valid Duration | Policy Name | Price |
|---|---|---|---|---|---|---|
| 1 | ● Enable<br>○ Disable | ○ Data [ ] Mbyte<br>● Time 2 hrs<br>0 mins | 3 days<br>0 hours | 5 days | None | 20 |
| 2 | ● Enable<br>○ Disable | ● Data 66 Mbyte<br>○ Time [ ] hrs<br>[ ] mins | 15 days<br>9 hours | 63 days | None | 5 |
| 3 | ● Enable<br>○ Disable | ○ Data [ ] Mbyte<br>● Time 12 hrs<br>40 mins | 3 days<br>15 hours | 8 days | None | 3 |

*2.* Payment Configuration:

Select “Secure Pay” for your external payment gateway. Enter Merchant ID and Password. And Payment Gateway URL is one fixed URL: https://www.securepay.com.au/xmlapi/payment.

Finally, enable whichever plan(s) you’d like to apply to “SecurePay”.



| External Payment Gateway | | | |
|---|---|---|---|
| ○ Authorize.Net | ○ PayPal | ● SecurePay | ○ Disable |

| SecurePay Payment Page Configuration | |
|---|---|
| Merchant ID | ____ * |
| Merchant Password | ____ * |
| Payment Gateway URL | https://www.securepay.com.au/xmlapi/payment * |
| Verify SSL Certificate | ● Enable ○ Disable<br>Trusted CA Management |
| Currency | AUD (Australian Dollar) * |

**Service Disclaimer Content**

```
We may collect and store the following personal
information:
physical contact information, credit card numbers and
transactional information based on your activities on the
Internet service provided by us.
```

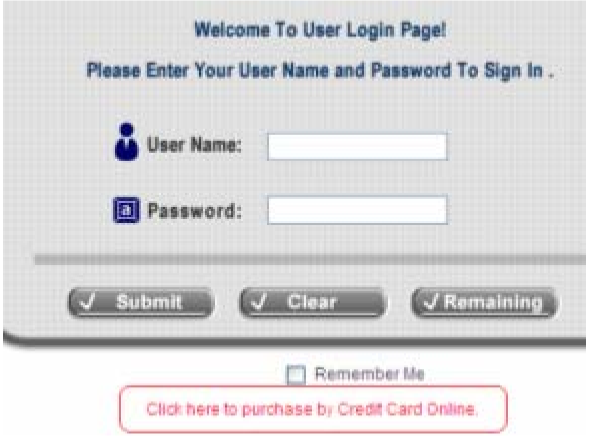
| SecurePay Payment Page Billing Configuration | | | | |
|---|---|---|---|---|
| Plan | Enable/Disable | | Quota | Price |
| 1 | ○ Enable | ● Disable | 2 hrs 0 mins | 20 |
| 2 | ○ Enable | ● Disable | | |
| 3 | ○ Enable | ● Disable | | |
| 4 | ○ Enable | ● Disable | | |
| 5 | ○ Enable | ● Disable | | |
| 6 | ○ Enable | ● Disable | | |
| 7 | ○ Enable | ● Disable | | |
| 8 | ○ Enable | ● Disable | | |
| 9 | ○ Enable | ● Disable | | |
| 10 | ○ Enable | ● Disable | | |

**SecurePay Payment Page Remark Content**

```
You must fill in the correct credit card number and
expiration date. Card code is the last 3 digits of the
security code located on the back of your credit card.
```

## ▪ How does your client purchase a plan?

*1.* Open a browser, it then shows a login page. And click "***Click here to purchase by Credit Card online***" to get started.



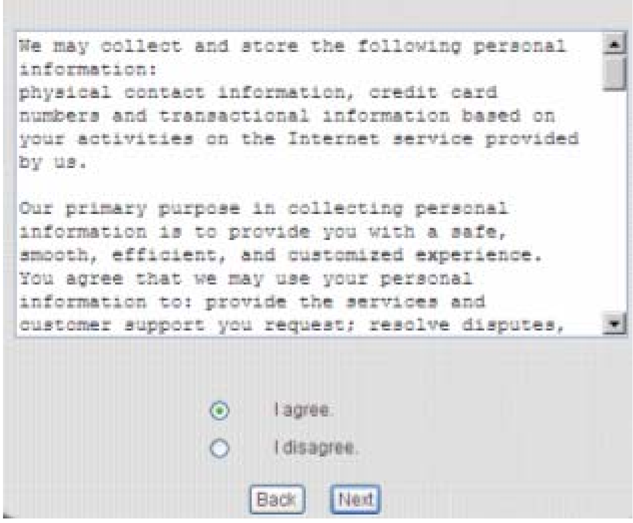
Welcome To User Login Page!

Please Enter Your User Name and Password To Sign In .

User Name:

Password:

*2.* Select "***I agree***" and click "***Next***".



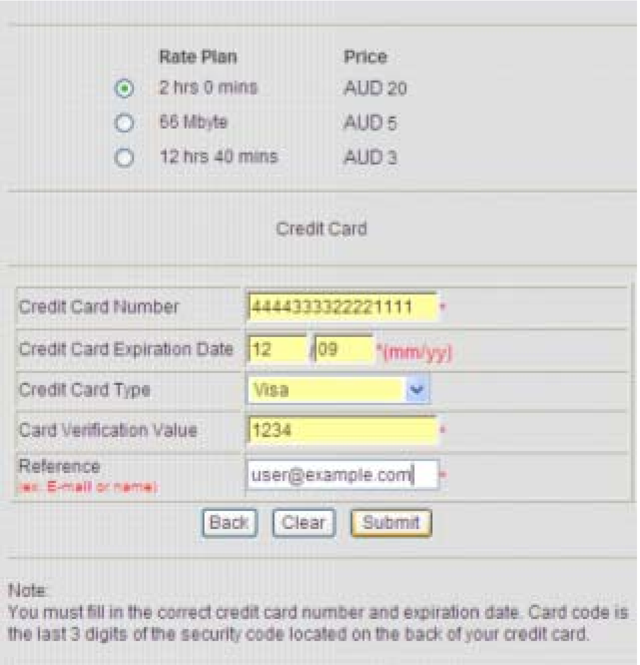
We may collect and store the following personal information:
physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

Our primary purpose in collecting personal information is to provide you with a safe, smooth, efficient, and customized experience. You agree that we may use your personal information to: provide the services and customer support you request; resolve disputes,

● I agree.

○ I disagree.

3. Select a billing plan to purchase; enter your credit card information and "***Submit***".



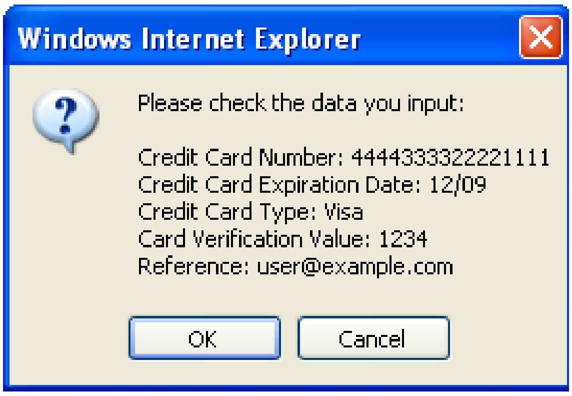
| | Rate Plan | Price |
|---|---|---|
| ● | 2 hrs 0 mins | AUD 20 |
| ○ | 66 Mbyte | AUD 5 |
| ○ | 12 hrs 40 mins | AUD 3 |

Credit Card

| | |
|---|---|
| Credit Card Number | 4444333322221111 * |
| Credit Card Expiration Date | 12 / 09 *(mm/yy) |
| Credit Card Type | Visa |
| Card Verification Value | 1234 * |
| Reference<br>(ex. E-mail or name) | user@example.com * |

Note:
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card.

4. Double confirm your credit card information.

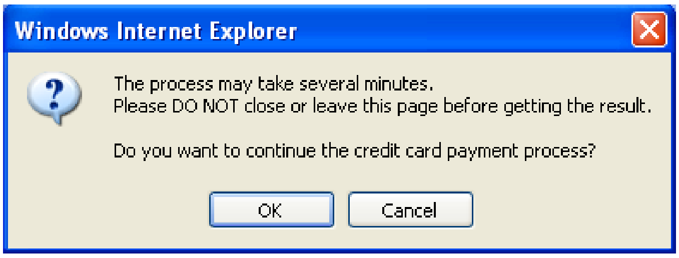


Windows Internet Explorer

Please check the data you input:

Credit Card Number: 4444333322221111
Credit Card Expiration Date: 12/09
Credit Card Type: Visa
Card Verification Value: 1234
Reference: user@example.com

5. Double confirm with your purchase. And wait for a couple minutes till you get your receipt.

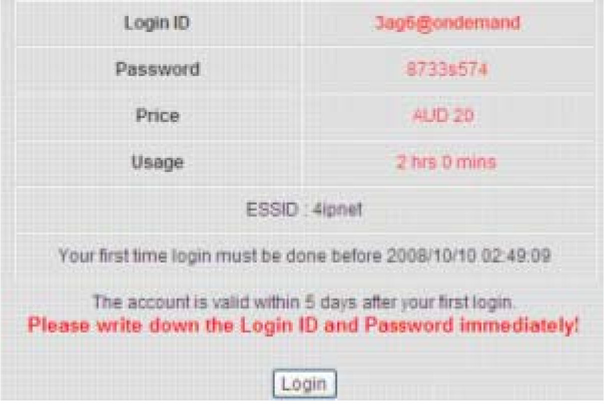


Windows Internet Explorer

The process may take several minutes.
Please DO NOT close or leave this page before getting the result.

Do you want to continue the credit card payment process?

6. Account has been successfully generated! Click "***Login***". And it's recommended not to close this page at all times in case you might re-login.



| | |
|---|---|
| Login ID | 3ag6@ondemand |
| Password | 8733s574 |
| Price | AUD 20 |
| Usage | 2 hrs 0 mins |

ESSID : 4ipnet

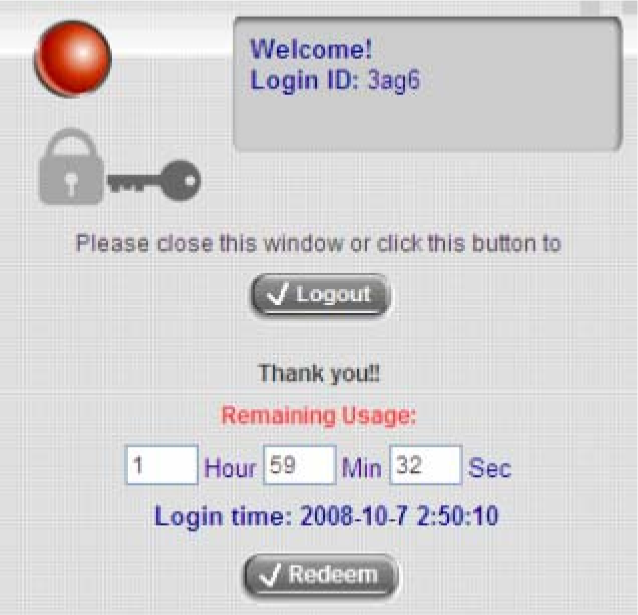
Your first time login must be done before 2008/10/10 02:49:09

The account is valid within 5 days after your first login.

Please write down the Login ID and Password immediately!

Login

7. The login successful box appears. Click "***Start Browsing***" to get online.



Welcome!
Login ID: 3ag6

Please close this window or click this button to

✓ Logout

Thank you!!

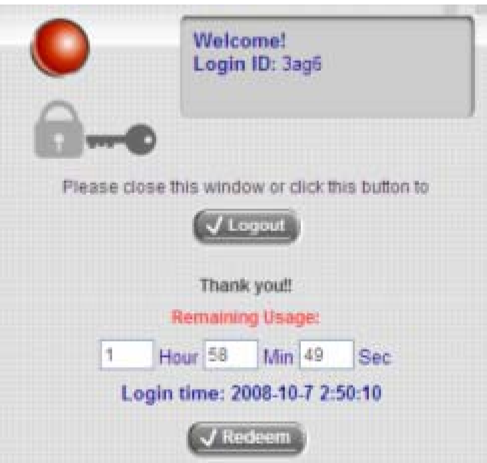
Remaining Usage:

1 Hour 59 Min 32 Sec

Login time: 2008-10-7 2:50:10

✓ Redeem

*8.* User is now redirected to YOUR homepage that URL you fill in the blank “**System Configuration >> Homepage**”.



Welcome!
Login ID: 3ag6

Please close this window or click this button to

Thank you!!

Remaining Usage:

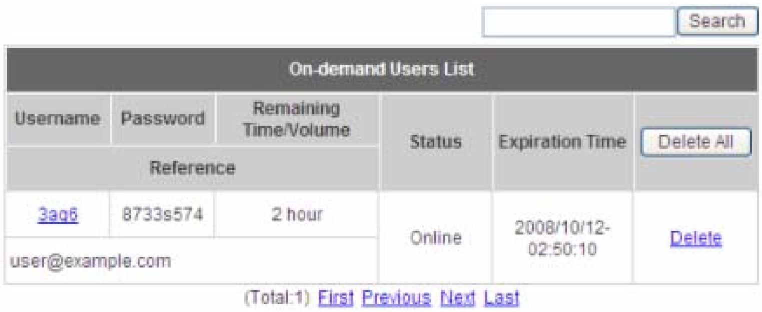
1 Hour 58 Min 49 Sec

Login time: 2008-10-7 2:50:10

## ▪ How does your client renew his service after running out of quota?

New username and password are needed to renew service. Client can either purchase a new account online (shown in the last section) or at the counter desk. The following example is to enter Web UI, manually generate an account and have your client renewed himself the service.

*1.* Go to On-demand Users List, the account being generated online (please see the last section) is shown.



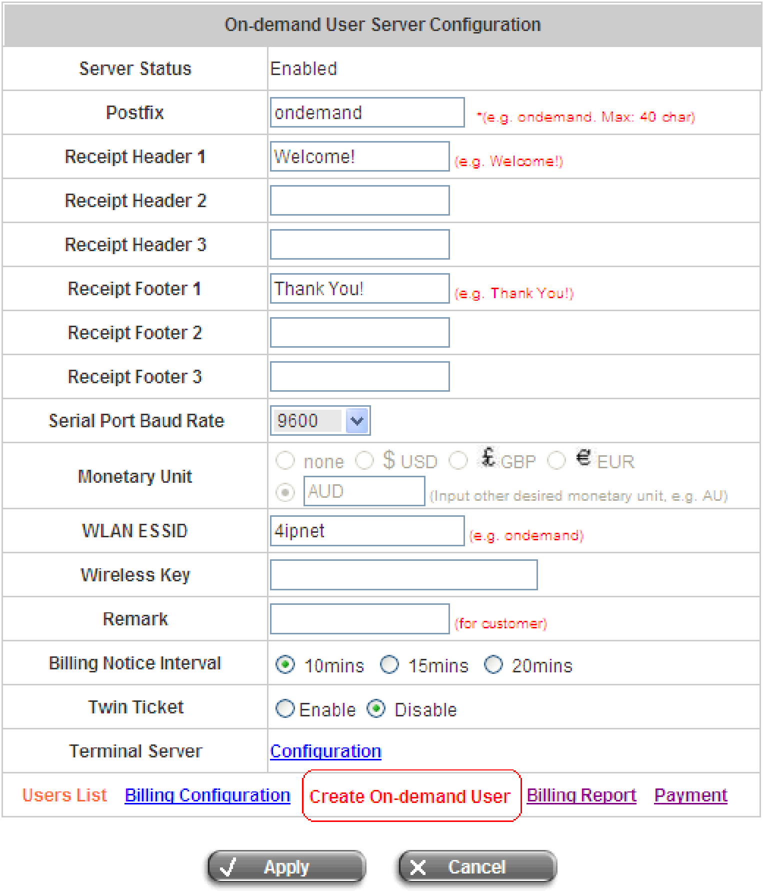
Search

On-demand Users List

| Username | Password | Remaining Time/Volume | Status | Expiration Time | Delete All |
|---|---|---|---|---|---|
| Reference | | | | | |
| 3ag6 | 8733s574 | 2 hour | Online | 2008/10/12-02:50:10 | Delete |
| user@example.com | | | | | |

(Total:1) First Previous Next Last

*2.* Create an on-demand user.

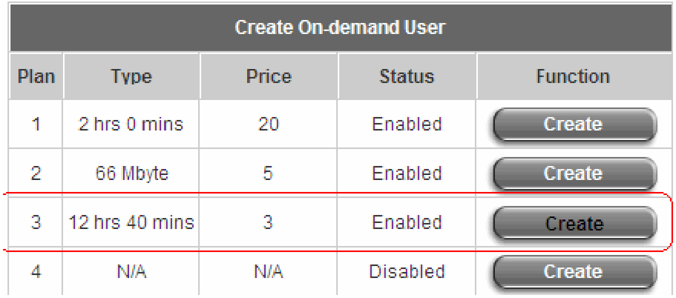


On-demand User Server Configuration

| | |
|---|---|
| Server Status | Enabled |
| Postfix | ondemand *(e.g. ondemand. Max: 40 char) |
| Receipt Header 1 | Welcome! (e.g. Welcome!) |
| Receipt Header 2 | |
| Receipt Header 3 | |
| Receipt Footer 1 | Thank You! (e.g. Thank You!) |
| Receipt Footer 2 | |
| Receipt Footer 3 | |
| Serial Port Baud Rate | 9600 |
| Monetary Unit | ○ none ○ $ USD ○ £ GBP ○ € EUR<br>● AUD (Input other desired monetary unit, e.g. AU) |
| WLAN ESSID | 4ipnet (e.g. ondemand) |
| Wireless Key | |
| Remark | (for customer) |
| Billing Notice Interval | ● 10mins ○ 15mins ○ 20mins |
| Twin Ticket | ○ Enable ● Disable |
| Terminal Server | Configuration |

Users List Billing Configuration Create On-demand User Billing Report Payment

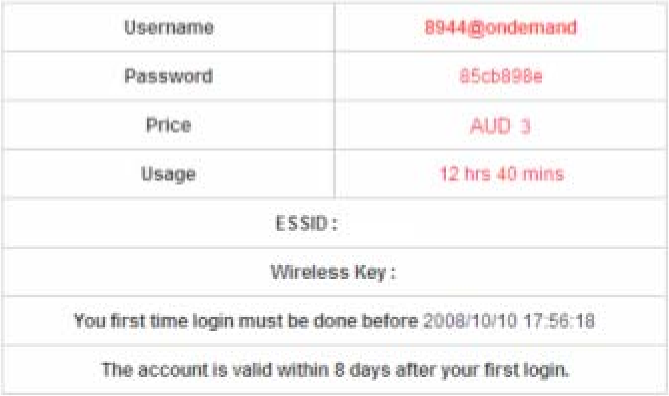
3. Choose a billing plan for this user and click “***Create***”.



Create On-demand User

| Plan | Type | Price | Status | Function |
|---|---|---|---|---|
| 1 | 2 hrs 0 mins | 20 | Enabled | Create |
| 2 | 66 Mbyte | 5 | Enabled | Create |
| 3 | 12 hrs 40 mins | 3 | Enabled | Create |
| 4 | N/A | N/A | Disabled | Create |

4. Give your client the print-out of this receipt with new account information.



| | |
|---|---|
| Username | 8944@ondemand |
| Password | 85cb898e |
| Price | AUD 3 |
| Usage | 12 hrs 40 mins |

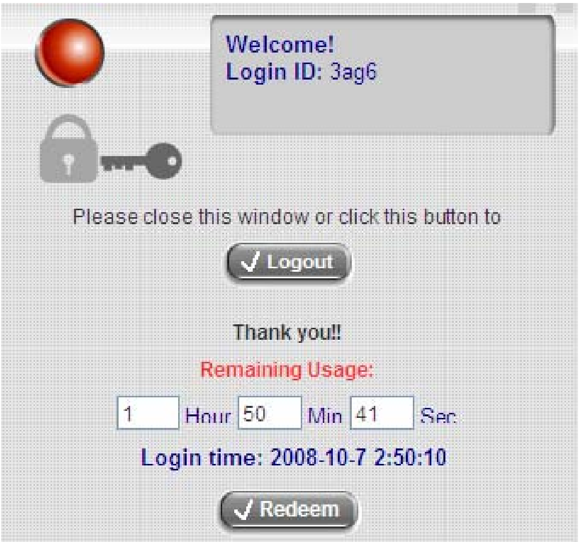
ESSID :

Wireless Key :

You first time login must be done before 2008/10/10 17:56:18

The account is valid within 8 days after your first login.

5. Have your client go back to the “Login successful page” and click “***Redeem***”. And enter new **User Name** and **Password**.



Welcome!
Login ID: 3ag6

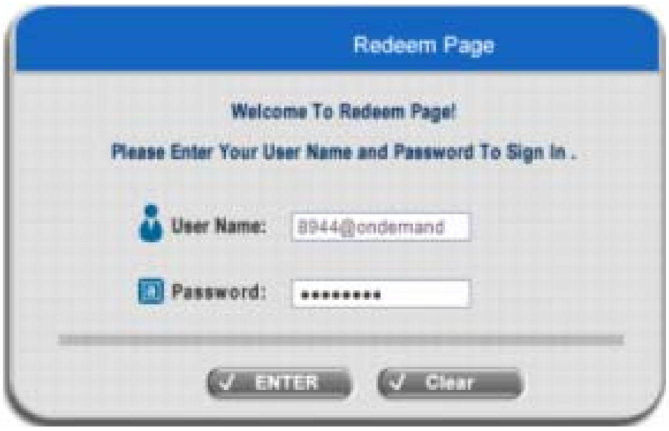
Please close this window or click this button to

Thank you!!

Remaining Usage:

1 Hour 50 Min 41 Sec

Login time: 2008-10-7 2:50:10



Redeem Page

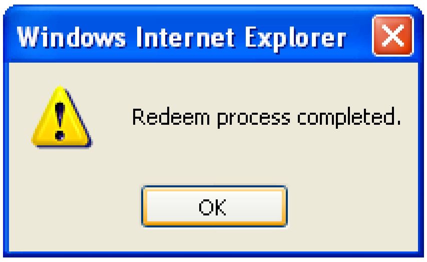
Welcome To Redeem Page!

Please Enter Your User Name and Password To Sign In .

User Name: 8944@ondemand

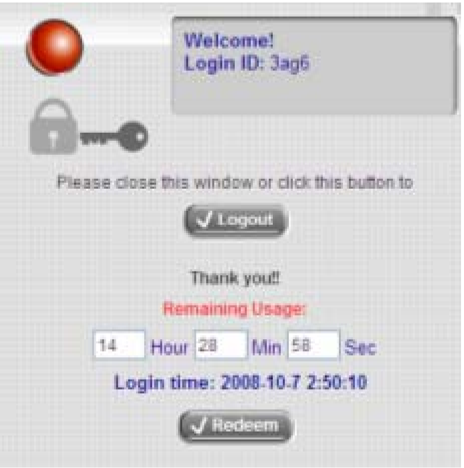
Password: •••••••••

*6.* Redeem is successful and you can see more quota for internet access.



Windows Internet Explorer

Redeem process completed.



Welcome!
Login ID: 3ag6

Please close this window or click this button to

Thank you!!

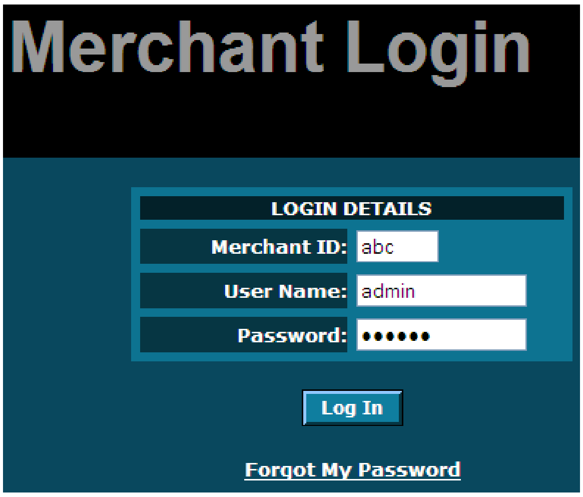
Remaining Usage:

14 Hour 28 Min 58 Sec

Login time: 2008-10-7 2:50:10

## ▪ How does Merchant check billing transactions?

1. Go to SecurePay Merchant Login Page at https://www.securepay.com.au/merchant/ and enter **Merchant ID**, Login **User Name** and **Password**.



Merchant Login

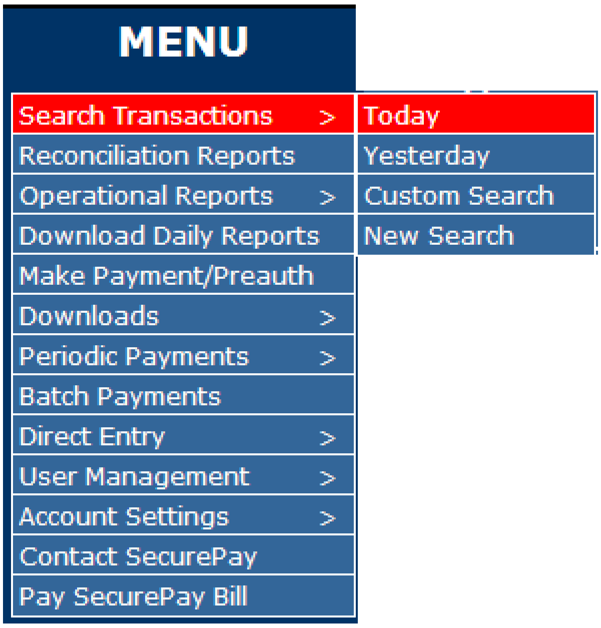
LOGIN DETAILS

Merchant ID: abc

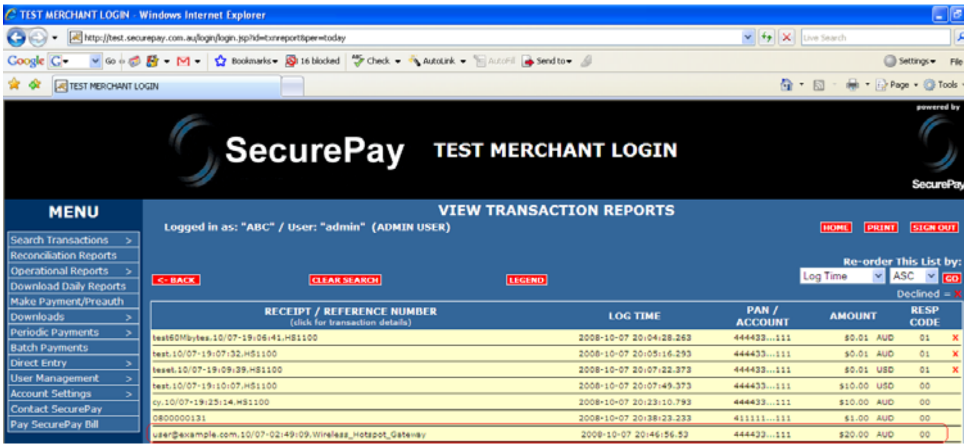
User Name: admin

Password: ••••••

2. Click “Search Transactions” and “Today” to check today’s transactions.



3. Today’s transaction is shown in table.



VIEW TRANSACTION REPORTS

Logged in as: "ABC" / User: "admin" (ADMIN USER)

Re-order This List by: Log Time ASC

Declined = ✗

| RECEIPT / REFERENCE NUMBER (click for transaction details) | LOG TIME | PAN / ACCOUNT | AMOUNT | RESP CODE | |
|---|---|---|---|---|---|
| test60Mbytes.10/07-19:06:41.HS1100 | 2008-10-07 20:04:28.263 | 444433...111 | $0.01 AUD | 01 | ✗ |
| test.10/07-19:07:32.HS1100 | 2008-10-07 20:05:16.293 | 444433...111 | $0.01 AUD | 01 | ✗ |
| teset.10/07-19:09:39.HS1100 | 2008-10-07 20:07:22.373 | 444433...111 | $0.01 USD | 01 | ✗ |
| test.10/07-19:10:07.HS1100 | 2008-10-07 20:07:49.373 | 444433...111 | $10.00 USD | 00 | |
| cy.10/07-19:25:14.HS1100 | 2008-10-07 20:23:10.793 | 444433...111 | $10.00 AUD | 00 | |
| 0800000131 | 2008-10-07 20:38:23.233 | 411111...111 | $1.00 AUD | 00 | |
| user@example.com.10/07-02:49:09.Wireless_Hotspot_Gateway | 2008-10-07 20:46:56.53 | 444433...111 | $20.00 AUD | 00 | |

# *Appendix E. RADIUS Accounting*

## ▪ How to create a user and add it into a group in Active Directory

*Step 1.* Open “Active Directory”

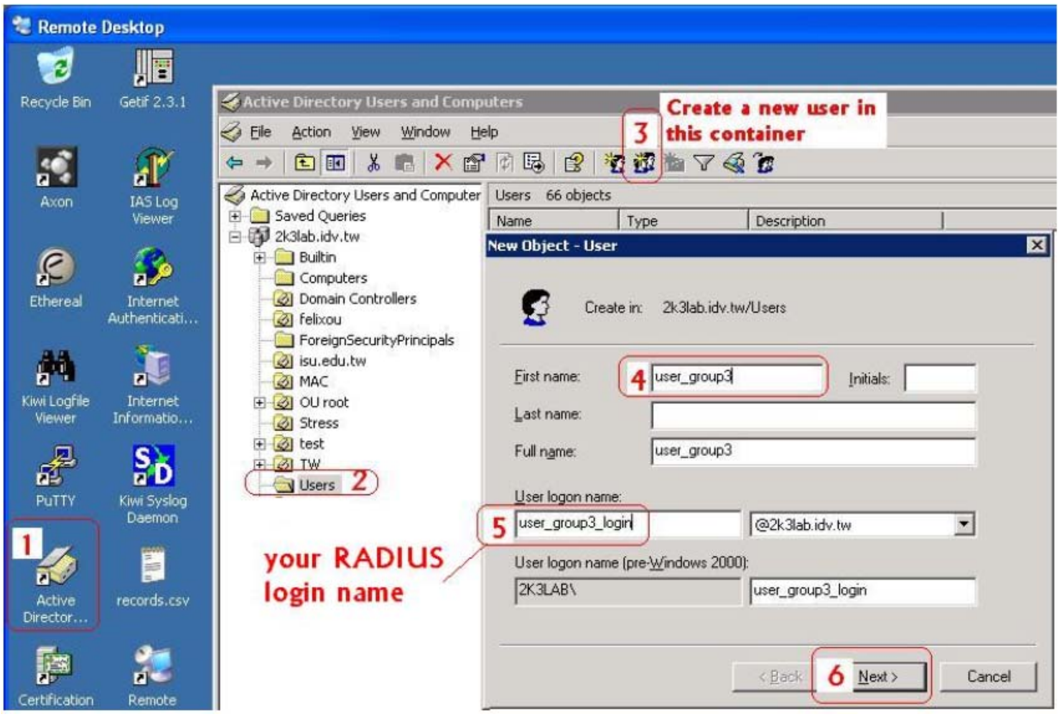
*Step 2.* Go to container “Users”

*Step 3.* Create a new user in this container.

*Step 4.* Enter the first name of this user.

*Step 5.* Enter User logon name which is the login name you will use in your RADIUS server.

*Step 6.* Click “Next” to continue.



Create a new user in this container

your RADIUS login name

New Object - User

Create in: 2k3lab.idv.tw/Users

First name: user_group3

Initials:

Last name:

Full name: user_group3

User logon name: user_group3_login @2k3lab.idv.tw

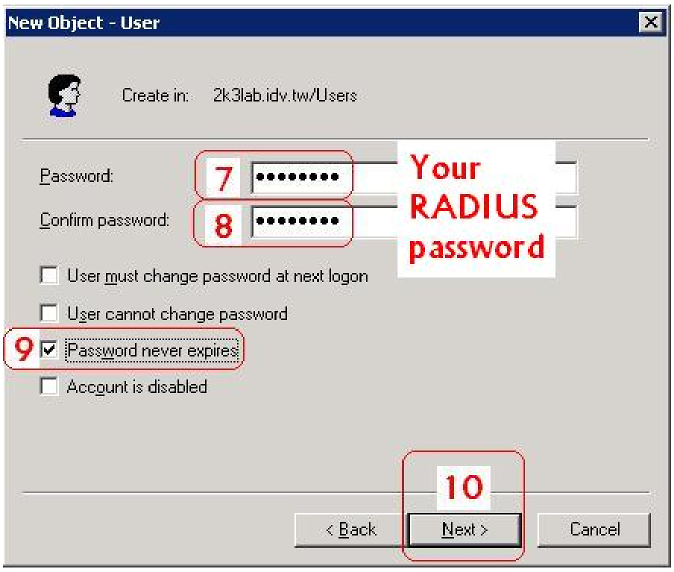
User logon name (pre-Windows 2000): 2K3LAB\ user_group3_login

*Step 7.* Enter your RADIUS password

*Step 8.* Re-enter your RADIUS password

*Step 9.* Check “Password never expires” so that this password lasts.

*Step 10.* Click Next to continue.



New Object - User

Create in: 2k3lab.idv.tw/Users

Password: •••••••••

Confirm password: •••••••••

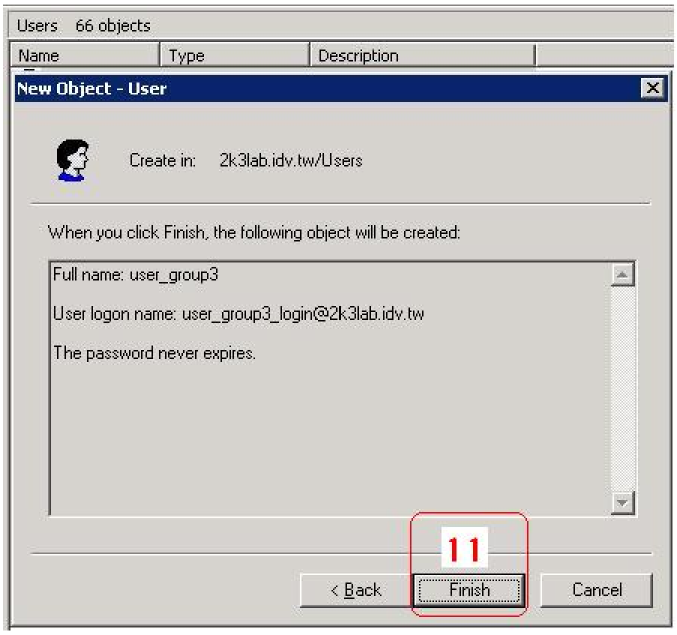
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

*Step 11.* Click finish to get done with account creation.



Users 66 objects

New Object - User

Create in: 2k3lab.idv.tw/Users

When you click Finish, the following object will be created:

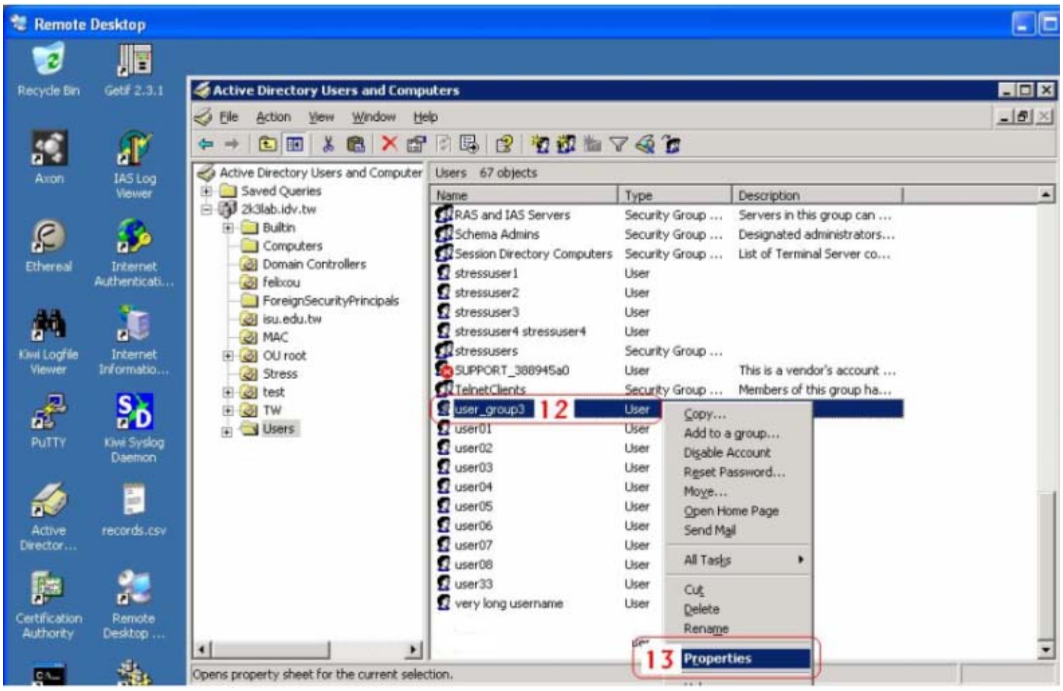
Full name: user_group3

User logon name: user_group3_login@2k3lab.idv.tw

The password never expires.

*Step 12.* It shows “user_group3” just created in the container “User”.

*Step 13.* Now let’s make this user “user_group3” a member of “group03”. Right click “user_group3” and scroll down to Properties.



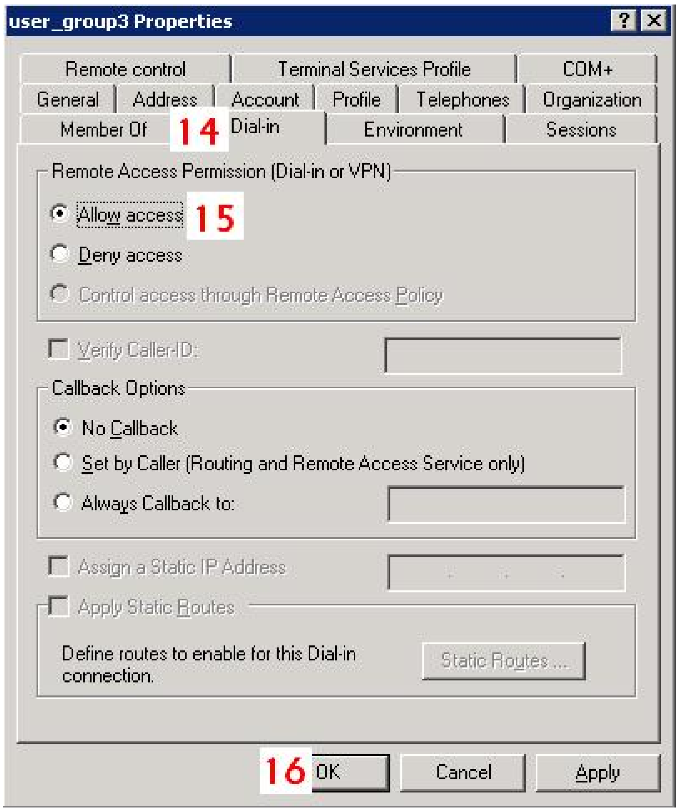
| Name | Type | Description |
|---|---|---|
| RAS and IAS Servers | Security Group ... | Servers in this group can ... |
| Schema Admins | Security Group ... | Designated administrators... |
| Session Directory Computers | Security Group ... | List of Terminal Server co... |
| stressuser1 | User | |
| stressuser2 | User | |
| stressuser3 | User | |
| stressuser4 stressuser4 | User | |
| stressusers | Security Group ... | |
| SUPPORT_388945a0 | User | This is a vendor's account ... |
| TelnetClients | Security Group ... | Members of this group ha... |
| user_group3 | User | |
| user01 | User | |
| user02 | User | |
| user03 | User | |
| user04 | User | |
| user05 | User | |
| user06 | User | |
| user07 | User | |
| user08 | User | |
| user33 | User | |
| very long username | User | |

Opens property sheet for the current selection.

*Step 14.* Select Dial-in

*Step 15.* Select "Allow access"

*Step 16.* Click OK



Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

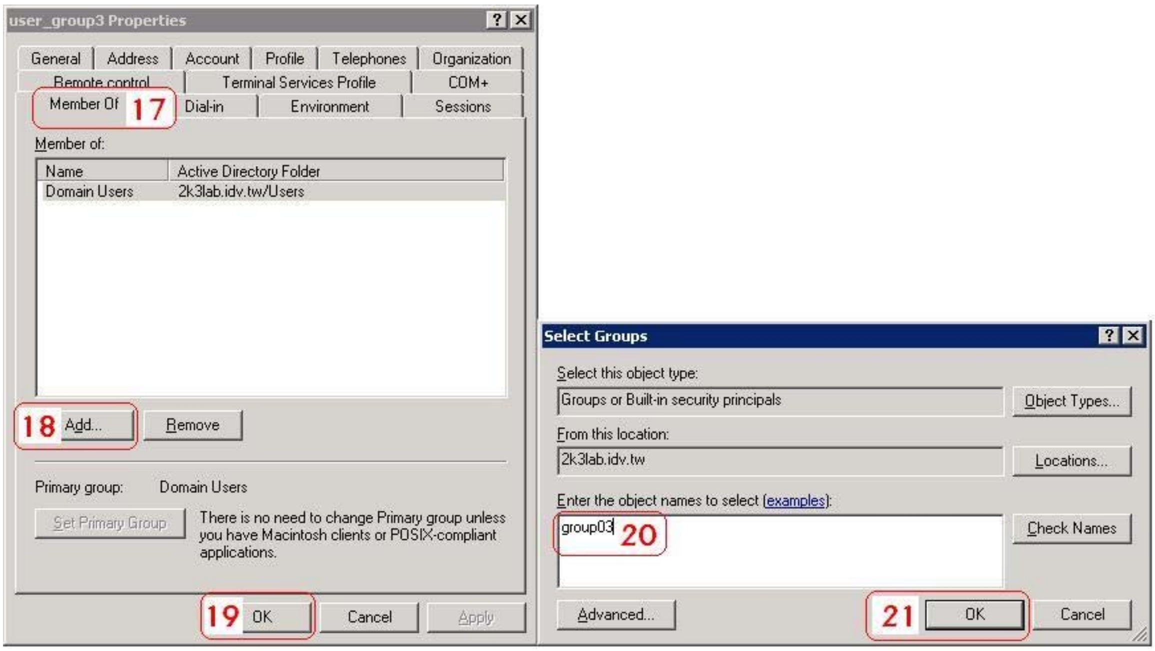
*Step 17.* Select “Member Of”

*Step 18.* Click “Add”

*Step 19.* Click “OK” to select Groups.

*Step 20.* Enter the object names “group03”

*Step 21.* Click “OK”



user_group3 Properties

Member of:

| Name | Active Directory Folder |
|---|---|
| Domain Users | 2k3lab.idv.tw/Users |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Select Groups

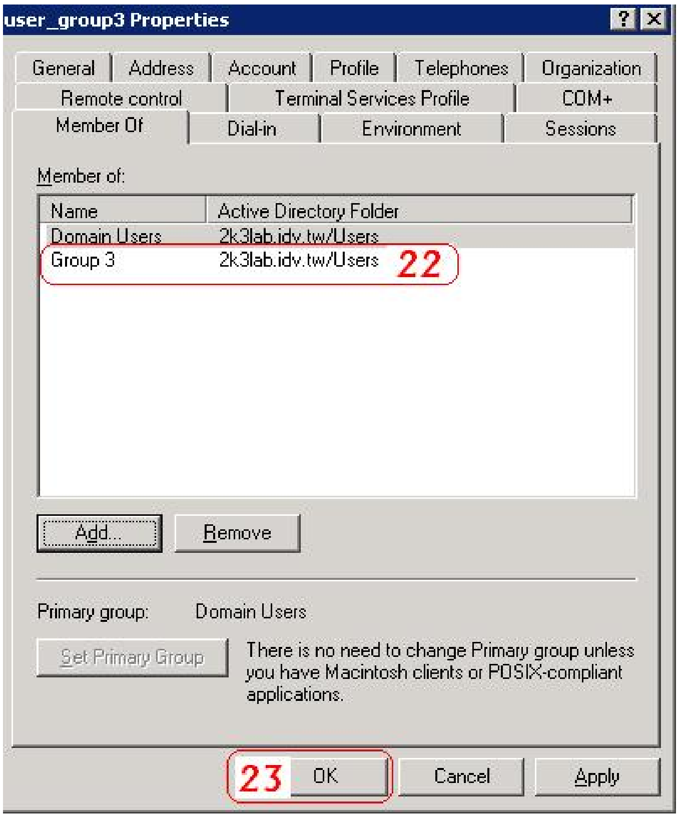
Select this object type: Groups or Built-in security principals

From this location: 2k3lab.idv.tw

Enter the object names to select (examples): group03

*Step 22.* Now this user is in “group3” under folder “2k3lab.idv.tw/Users”.

*Step 23.* Click “OK”



user_group3 Properties

Member of:

| Name | Active Directory Folder |
|---|---|
| Domain Users | 2k3lab.idv.tw/Users |
| Group 3 | 2k3lab.idv.tw/Users |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

## ▪ RADIUS accounting with VSA

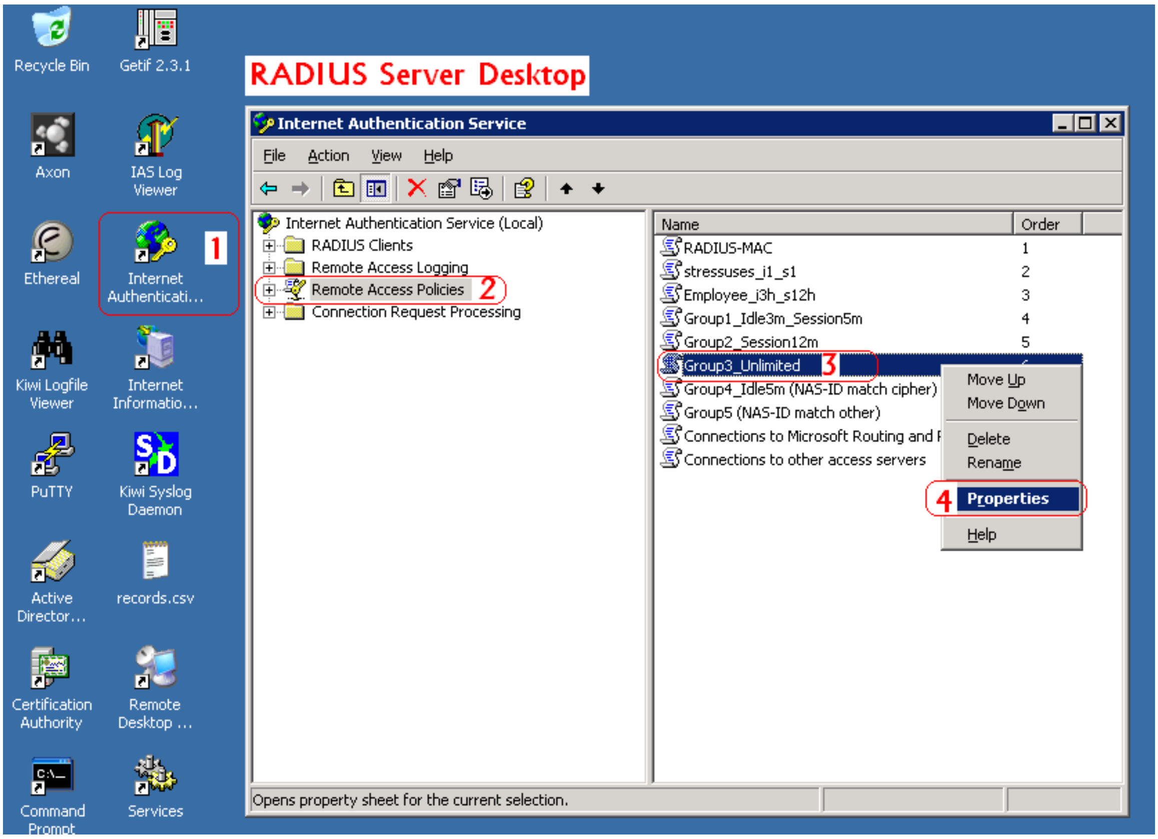
VSA stands for Vendor Specific Attributes. This VSA is a “value in bytes” sent by RADIUS server to gateway along with an Access-Accept packet. In other words, when your external RADIUS server accepts HS1100’s request, RADIUS not only replies with an “access-accept” but it also carries a maximum value in bytes that each client is allowed to transfer. This value is the maximum allowable summation of each client’s download plus upload traffic in bytes. Access-Accept packet and VSA are sent back to gateway in one session.

The bellowing shows the summary of this VSA format: (The fields are transmitted from left to right.)

| Vendor Specific Attribute Number | Vendor Code | Vendor Assigned Attribute Number | Attribute Value (the Max allowable download and upload transfer for each client in bytes) |
|---|---|---|---|
| By RADIUS Standard | By vendor | By vendor | By local administrator |
| 26 | 21920 | 10 | 0x100000 |

This section will guide you through a VSA configuration in your external RADIUS server. Before get started, go to or remotely connect to your external RADIUS server’s desktop.

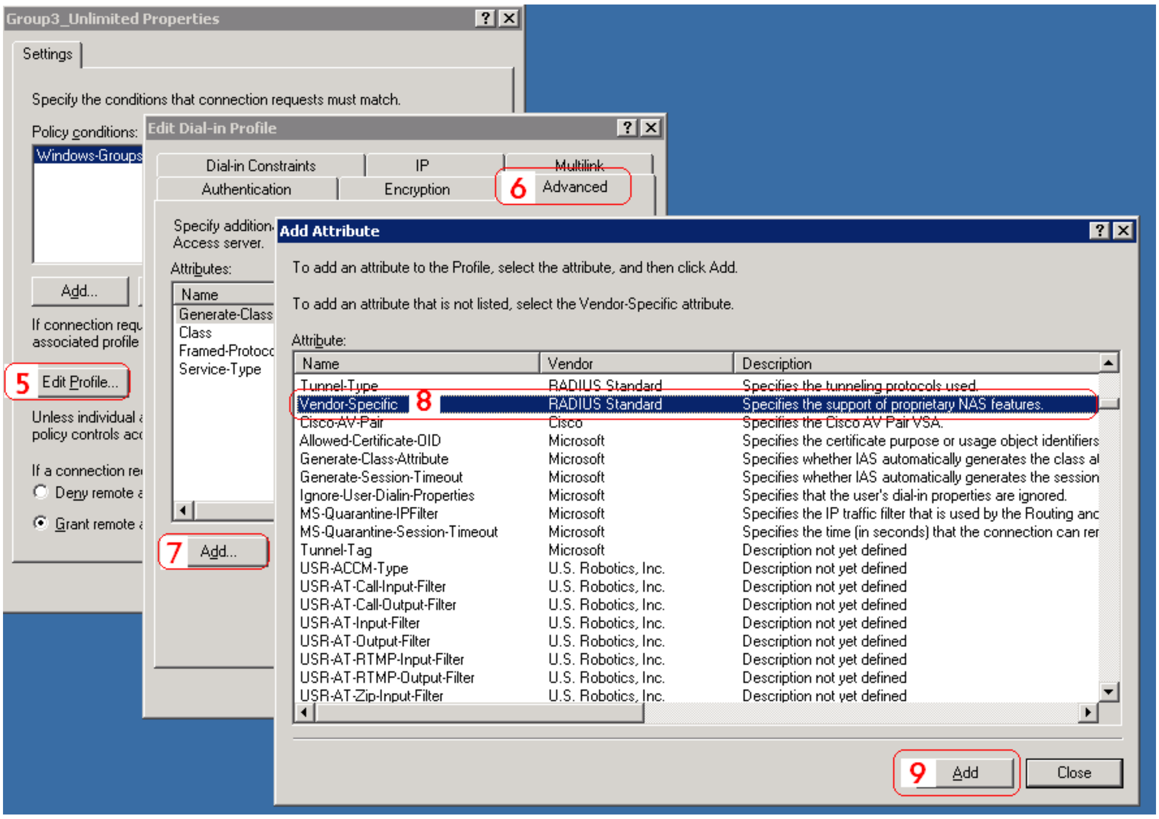
Step 1 to 4: Run “Internet Authentication Server”, open “Remote Access Policies” and select a policy. Right click and scroll down to its properties page.



| Name | Order |
|---|---|
| RADIUS-MAC | 1 |
| stressuses_i1_s1 | 2 |
| Employee_i3h_s12h | 3 |
| Group1_Idle3m_Session5m | 4 |
| Group2_Session12m | 5 |
| Group3_Unlimited | |
| Group4_Idle5m (NAS-ID match cipher) | |
| Group5 (NAS-ID match other) | |
| Connections to Microsoft Routing and R | |
| Connections to other access servers | |

Opens property sheet for the current selection.

Step 5 to 9: Steps 5 to 9 guides you through adding a “Vendor-Specific” attribute into properties of this selected policy.



Group3_Unlimited Properties

Specify the conditions that connection requests must match.

Policy conditions: Windows-Groups

If connection requ... associated profile

Unless individual ... policy controls acc...

If a connection re...

○ Deny remote ...

● Grant remote ...

Edit Dial-in Profile

Specify addition... Access server.

Attributes:

| Name |
|---|
| Generate-Class |
| Class |
| Framed-Protoco |
| Service-Type |

Add Attribute

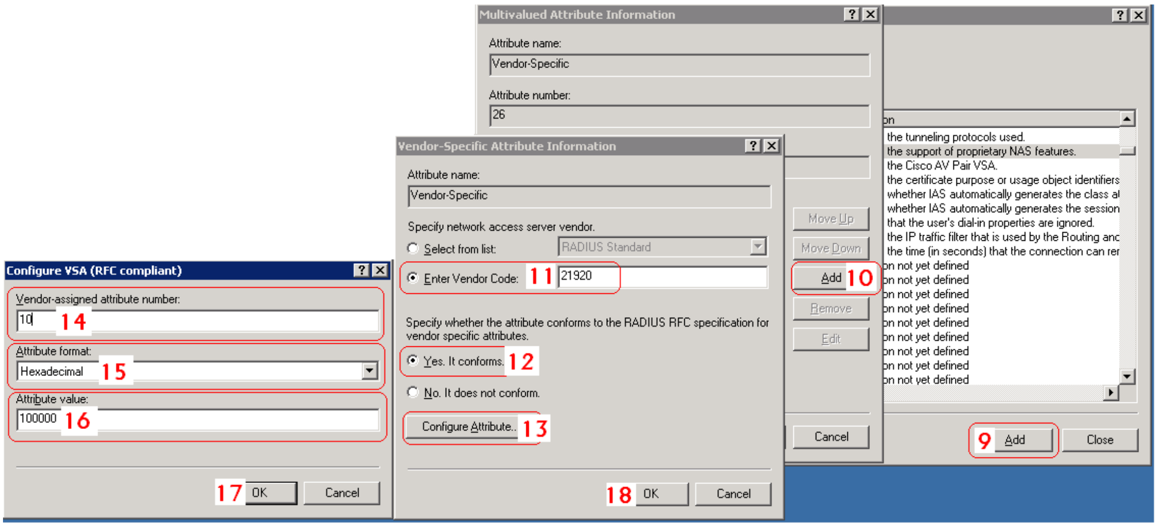
To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

| Name | Vendor | Description |
|---|---|---|
| Tunnel-Type | RADIUS Standard | Specifies the tunneling protocols used. |
| Vendor-Specific | RADIUS Standard | Specifies the support of proprietary NAS features. |
| Cisco-AV-Pair | Cisco | Specifies the Cisco AV Pair VSA. |
| Allowed-Certificate-OID | Microsoft | Specifies the certificate purpose or usage object identifiers |
| Generate-Class-Attribute | Microsoft | Specifies whether IAS automatically generates the class at |
| Generate-Session-Timeout | Microsoft | Specifies whether IAS automatically generates the session |
| Ignore-User-Dialin-Properties | Microsoft | Specifies that the user's dial-in properties are ignored. |
| MS-Quarantine-IPFilter | Microsoft | Specifies the IP traffic filter that is used by the Routing anc |
| MS-Quarantine-Session-Timeout | Microsoft | Specifies the time (in seconds) that the connection can rer |
| Tunnel-Tag | Microsoft | Description not yet defined |
| USR-ACCM-Type | U.S. Robotics, Inc. | Description not yet defined |
| USR-AT-Call-Input-Filter | U.S. Robotics, Inc. | Description not yet defined |
| USR-AT-Call-Output-Filter | U.S. Robotics, Inc. | Description not yet defined |
| USR-AT-Input-Filter | U.S. Robotics, Inc. | Description not yet defined |
| USR-AT-Output-Filter | U.S. Robotics, Inc. | Description not yet defined |
| USR-AT-RTMP-Input-Filter | U.S. Robotics, Inc. | Description not yet defined |
| USR-AT-RTMP-Output-Filter | U.S. Robotics, Inc. | Description not yet defined |
| USR-AT-Zip-Input-Filter | U.S. Robotics, Inc. | Description not yet defined |

Step 9 to 18: Step 9 to 18 guides you to add “Vendor Code = 21920”, “Vendor-assigned attribute number = 10”, and “Attribute Value = 100000 in Hexadecimal” into properties of this policy.



Multivalued Attribute Information

Attribute name: Vendor-Specific

Attribute number: 26

Vendor-Specific Attribute Information

Attribute name: Vendor-Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 21920

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms.

○ No. It does not conform.

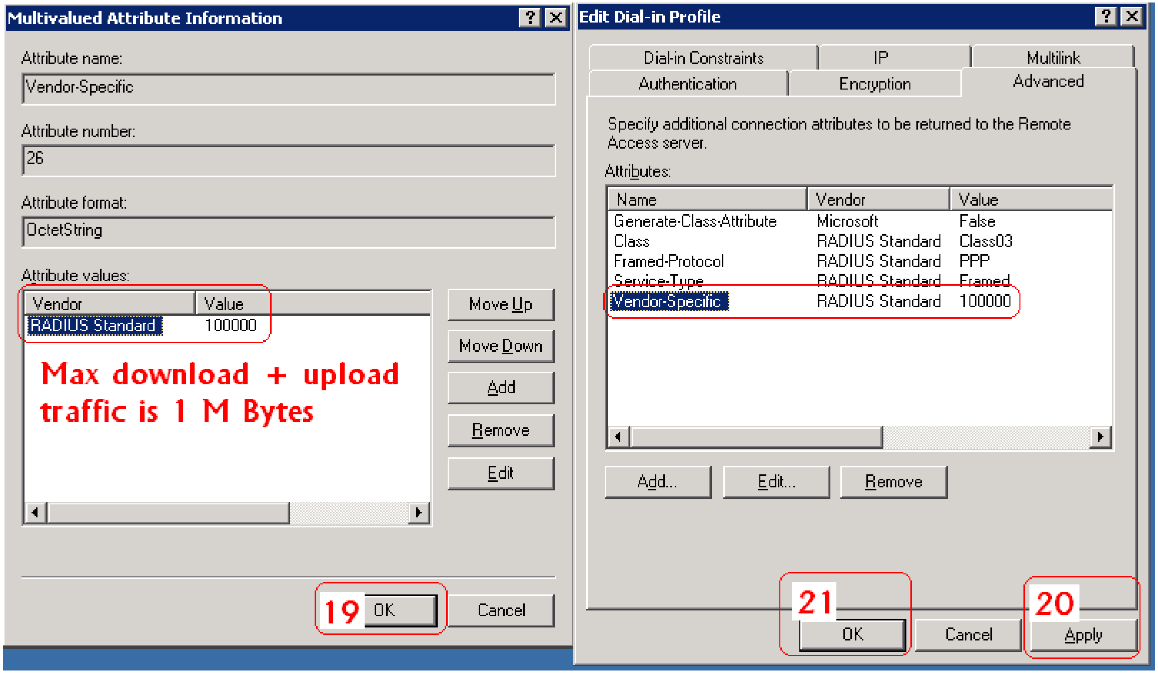
Configure VSA (RFC compliant)

Vendor-assigned attribute number: 10

Attribute format: Hexadecimal

Attribute value: 100000

Step 9 to 18: Step 19 to 21 shows that your Attribute Value has been added.



Multivalued Attribute Information

Attribute name: Vendor-Specific

Attribute number: 26

Attribute format: OctetString

Attribute values:

| Vendor | Value |
|---|---|
| RADIUS Standard | 100000 |

Max download + upload traffic is 1 M Bytes

Edit Dial-in Profile

Specify additional connection attributes to be returned to the Remote Access server.

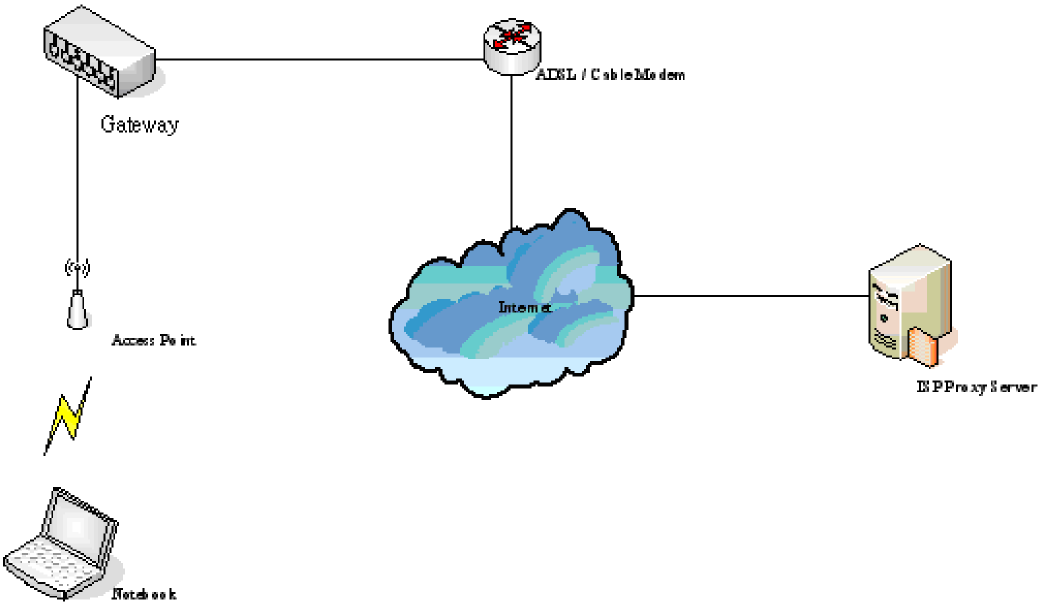
Attributes:

| Name | Vendor | Value |
|---|---|---|
| Generate-Class-Attribute | Microsoft | False |
| Class | RADIUS Standard | Class03 |
| Framed-Protocol | RADIUS Standard | PPP |
| Service-Type | RADIUS Standard | Framed |
| Vendor-Specific | RADIUS Standard | 100000 |

# Appendix F. Proxy Setting

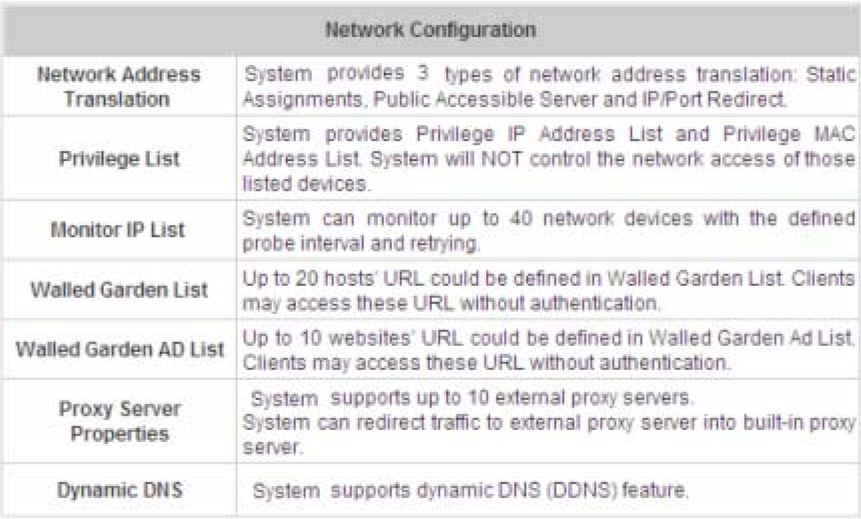
## 1. Proxy Setting for Hotspot

HotSpot is a place such as a coffee shop, hotel, or a public area where provides Wi-Fi service for mobile and temporary users. HotSpot is usually implemented without complicated network architecture and using some proxy servers provided by Internet Service Providers.



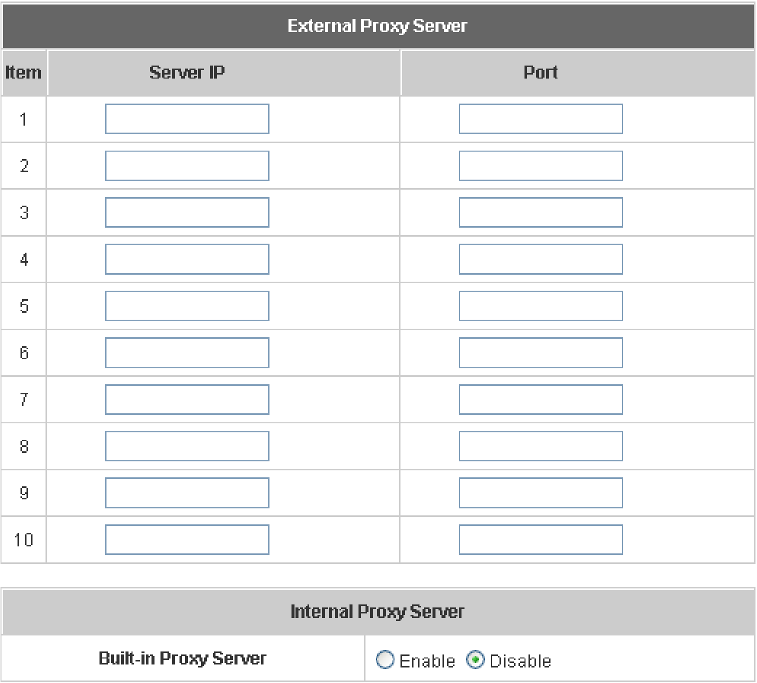
In Hotspots, users usually enable their proxy setting of the browsers such as IE and Firefox. Therefore, so we need to set some proxy configuration in the Gateway need to be set. Please follow the steps to complete the proxy configuration：

1. Login Gateway by using “***admin***”.
2. Click the ***Network Configuration from top menu*** and the homepage of the ***Network Configuration*** will appear.



| Network Configuration | |
|---|---|
| Network Address Translation | System provides 3 types of network address translation: Static Assignments, Public Accessible Server and IP/Port Redirect. |
| Privilege List | System provides Privilege IP Address List and Privilege MAC Address List. System will NOT control the network access of those listed devices. |
| Monitor IP List | System can monitor up to 40 network devices with the defined probe interval and retrying. |
| Walled Garden List | Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication. |
| Walled Garden AD List | Up to 10 websites' URL could be defined in Walled Garden Ad List. Clients may access these URL without authentication. |
| Proxy Server Properties | System supports up to 10 external proxy servers.<br>System can redirect traffic to external proxy server into built-in proxy server. |
| Dynamic DNS | System supports dynamic DNS (DDNS) feature. |

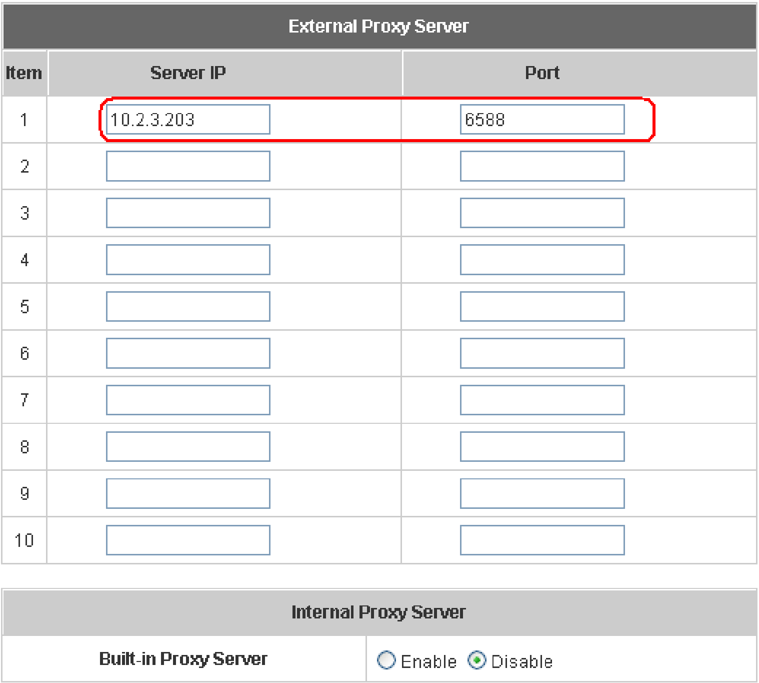
3. Click the ***Proxy Server Properties*** from left menu and the homepage of the **Proxy Server Properties** will appear.



| External Proxy Server | | |
|---|---|---|
| Item | Server IP | Port |
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

| Internal Proxy Server | |
|---|---|
| Built-in Proxy Server | ○ Enable ● Disable |

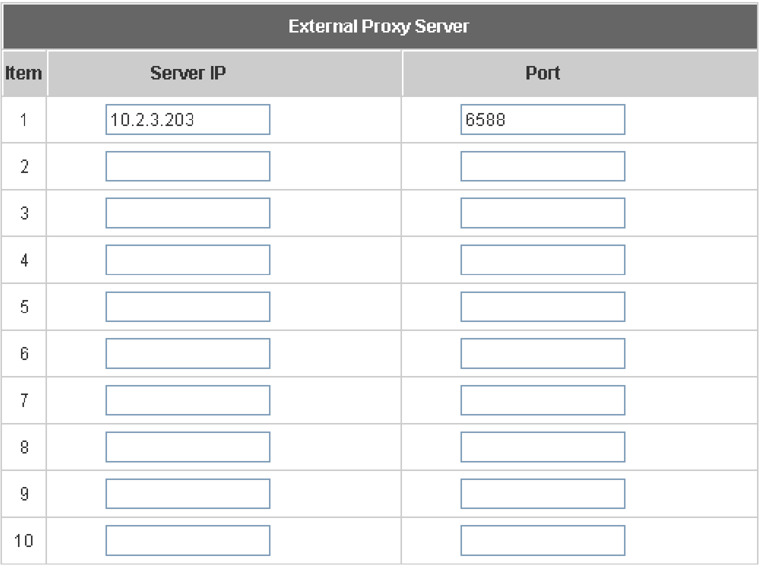
4. Add the ISP's proxy Server IP and Port into ***External Proxy Server*** Setting.



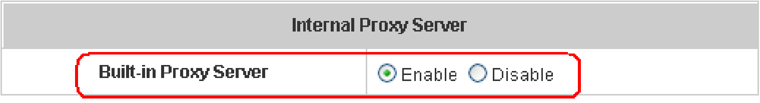
| External Proxy Server | | |
|---|---|---|
| Item | Server IP | Port |
| 1 | 10.2.3.203 | 6588 |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

| Internal Proxy Server | |
|---|---|
| Built-in Proxy Server | ○ Enable ● Disable |

5. ***Enable Built-in Proxy Server*** in ***Internal Proxy Server*** Setting.



| External Proxy Server | | |
|---|---|---|
| Item | Server IP | Port |
| 1 | 10.2.3.203 | 6588 |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

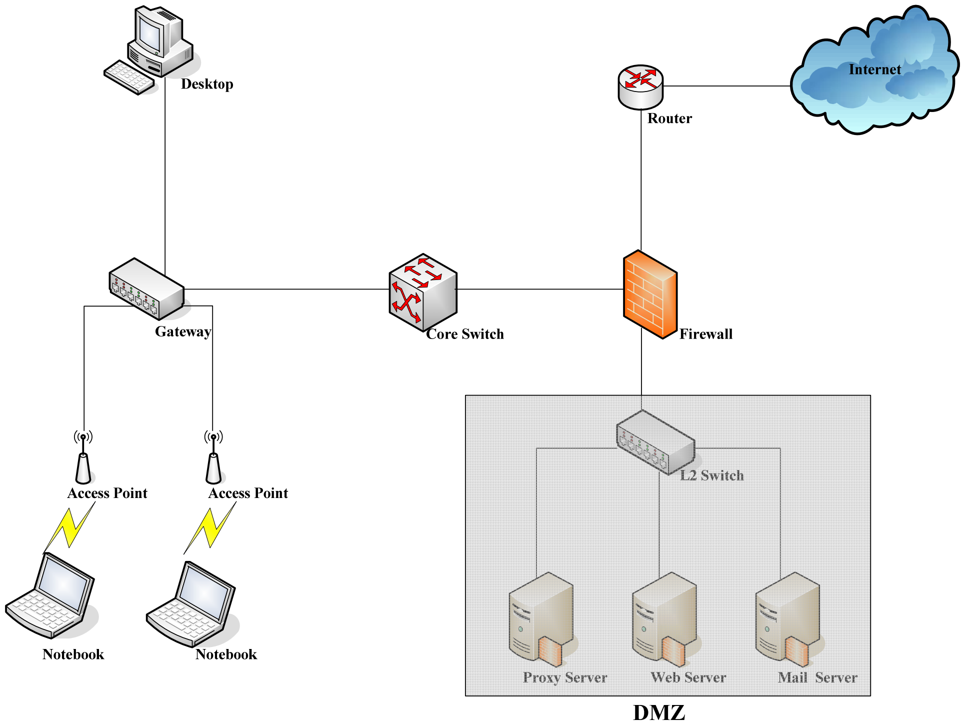


| Internal Proxy Server | |
|---|---|
| Built-in Proxy Server | ● Enable ○ Disable |

6. Click ***Apply*** to save the settings***.***

# 2. Proxy Setting for Enterprise

Enterprises usually isolate their intranet and internet by using more elaborated network architecture. Many enterprises have their own proxy server which is usually at intranet or DMZ under the firewall protection.



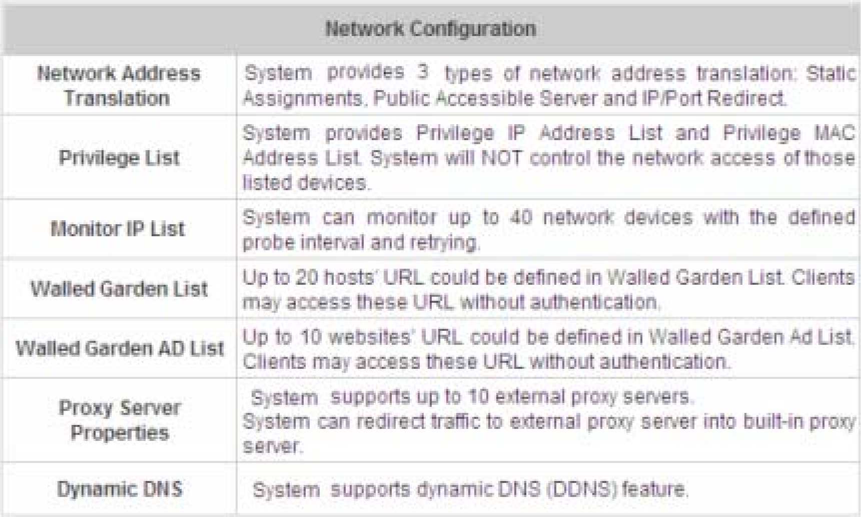
In enterprises, network managers or MIS staff may often ask their users to enable their proxy setting of the browsers such as IE and Firefox to reduce the internet access loading. Therefore some proxy configurations in the Gateway need to be set.

⚠ *Some enterprises will automatically redirect packets to proxy server by using core switch or Layer 7 devices. However, the clients do not need to enable the proxy settings of their browsers, and the administrator does not need to set any proxy configuration in the Gateway.*

Please follow the steps to complete the proxy configuration：

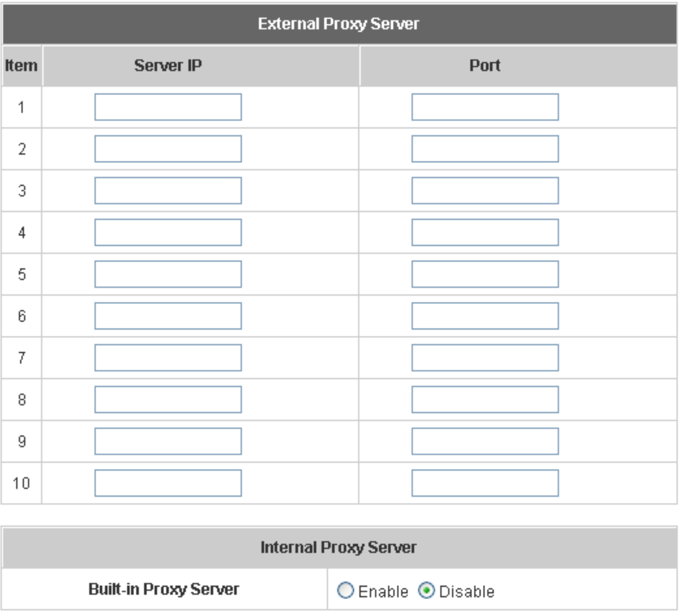
## ■ Gateway Setting

1. Login Gateway by using “***admin***”.
2. Click the ***Network Configuration from top menu,*** and the homepage of the ***Network Configuration*** will appear.



| Network Configuration | |
|---|---|
| Network Address Translation | System provides 3 types of network address translation: Static Assignments, Public Accessible Server and IP/Port Redirect. |
| Privilege List | System provides Privilege IP Address List and Privilege MAC Address List. System will NOT control the network access of those listed devices. |
| Monitor IP List | System can monitor up to 40 network devices with the defined probe interval and retrying. |
| Walled Garden List | Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication. |
| Walled Garden AD List | Up to 10 websites' URL could be defined in Walled Garden Ad List. Clients may access these URL without authentication. |
| Proxy Server Properties | System supports up to 10 external proxy servers.<br>System can redirect traffic to external proxy server into built-in proxy server. |
| Dynamic DNS | System supports dynamic DNS (DDNS) feature. |

3. Click the ***Proxy Server Properties*** from left menu, and the homepage of the ***Proxy Server Properties*** will appear.



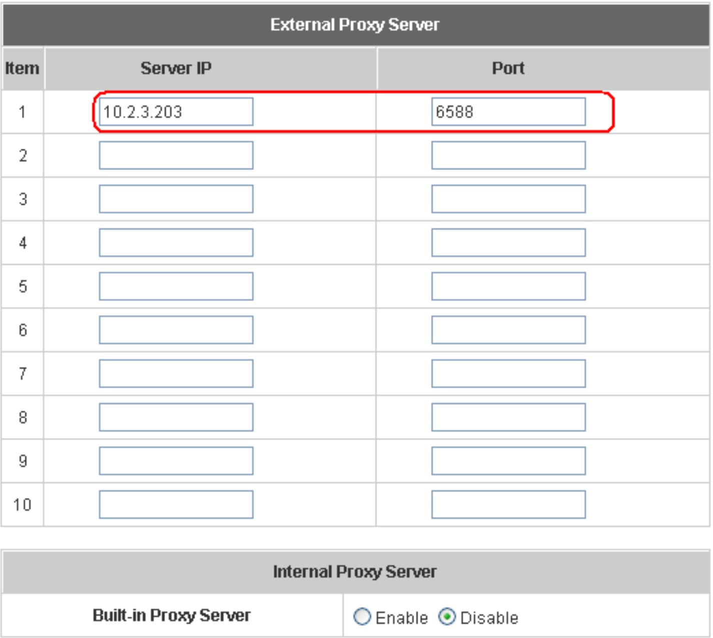
External Proxy Server

| Item | Server IP | Port |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

Internal Proxy Server

| | |
|---|---|
| Built-in Proxy Server | ○ Enable ● Disable |

4. Add your proxy Server IP and Port into ***External Proxy Server*** Setting.



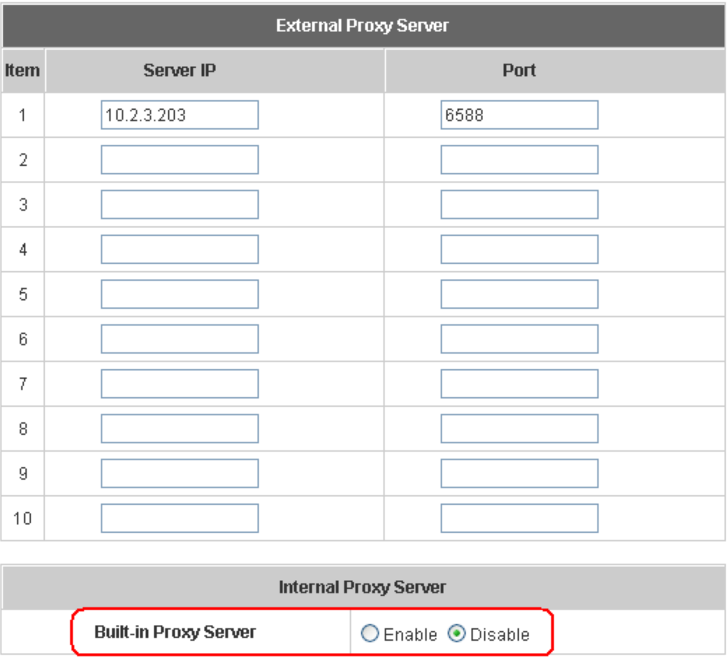
External Proxy Server

| Item | Server IP | Port |
|---|---|---|
| 1 | 10.2.3.203 | 6588 |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

Internal Proxy Server

| | |
|---|---|
| Built-in Proxy Server | ○ Enable ● Disable |

5. ***Disable Built-in Proxy Server*** in ***Internal Proxy Server*** Setting.



External Proxy Server

| Item | Server IP | Port |
|---|---|---|
| 1 | 10.2.3.203 | 6588 |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

Internal Proxy Server

| | |
|---|---|
| Built-in Proxy Server | ○ Enable ● Disable |

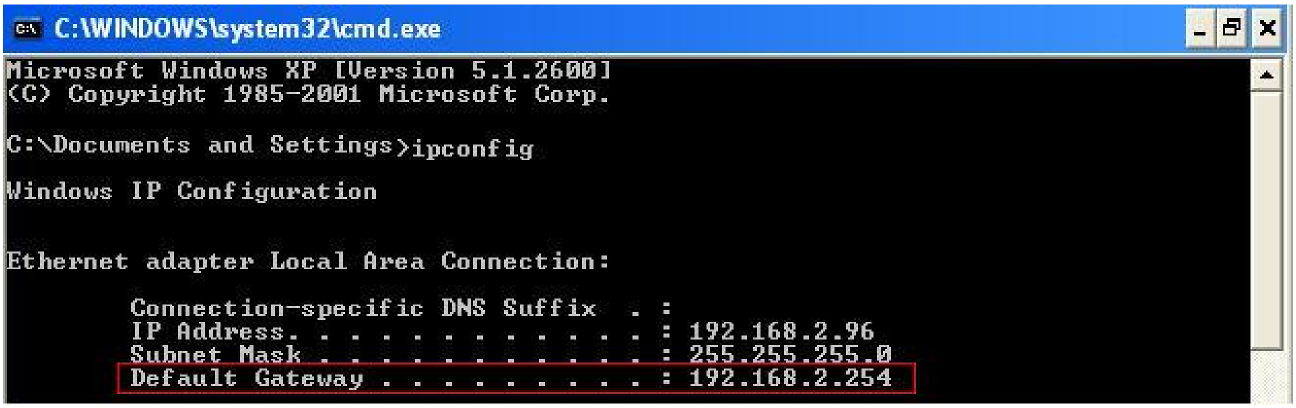
6. Click ***Apply*** to save the settings.

> ⚠ *If your proxy server is disabled, it will make the user authentication operation abnormal. When users open the browser, the login page will not appear because the proxy server is down. Please make sure that your proxy server is always available.*

## ■ Client Setting

It is necessary for clients to add default gateway IP address into proxy exception information so the user login successful page can show up normally.

1. Use command "***ipconfig***" to get Default Gateway IP Address.

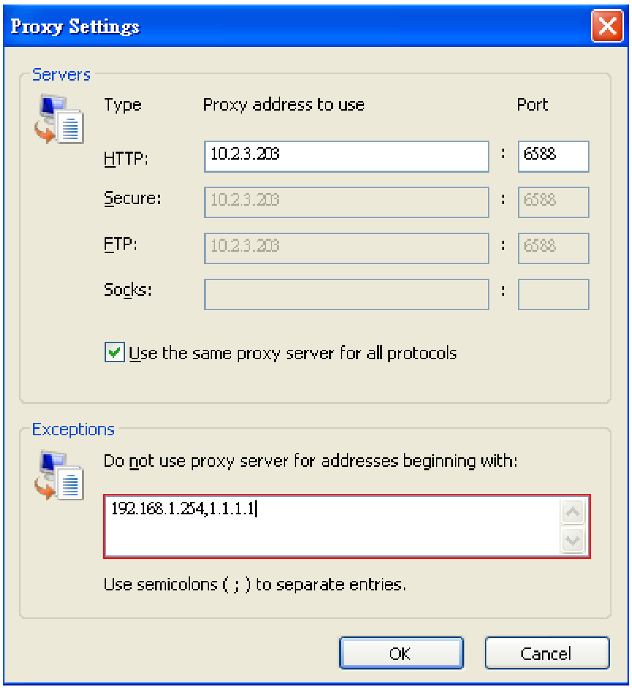


C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.96
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.254
```

2. Open browser to add ***default gateway IP address (e.g. 192.168.1.254)*** and ***logout page IP address "1.1.1.1"*** into proxy exception information.

- **For I.E**



Proxy Settings

Servers

| Type | Proxy address to use | | Port |
|---|---|---|---|
| HTTP: | 10.2.3.203 | : | 6588 |
| Secure: | 10.2.3.203 | : | 6588 |
| FTP: | 10.2.3.203 | : | 6588 |
| Socks: | | : | |

☑ Use the same proxy server for all protocols

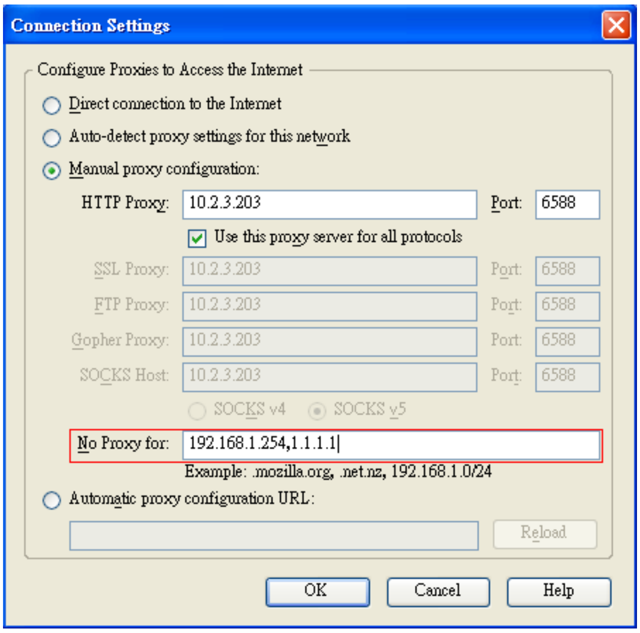
Exceptions

Do not use proxy server for addresses beginning with:

192.168.1.254,1.1.1.1

Use semicolons ( ; ) to separate entries.

- **For Firefox**



Connection Settings

Configure Proxies to Access the Internet

○ Direct connection to the Internet

○ Auto-detect proxy settings for this network

● Manual proxy configuration:

HTTP Proxy: 10.2.3.203 Port: 6588

☑ Use this proxy server for all protocols

SSL Proxy: 10.2.3.203 Port: 6588

FTP Proxy: 10.2.3.203 Port: 6588

Gopher Proxy: 10.2.3.203 Port: 6588

SOCKS Host: 10.2.3.203 Port: 6588

○ SOCKS v4 ● SOCKS v5

No Proxy for: 192.168.1.254,1.1.1.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

# Appendix G. Network Configuration & External Network Access

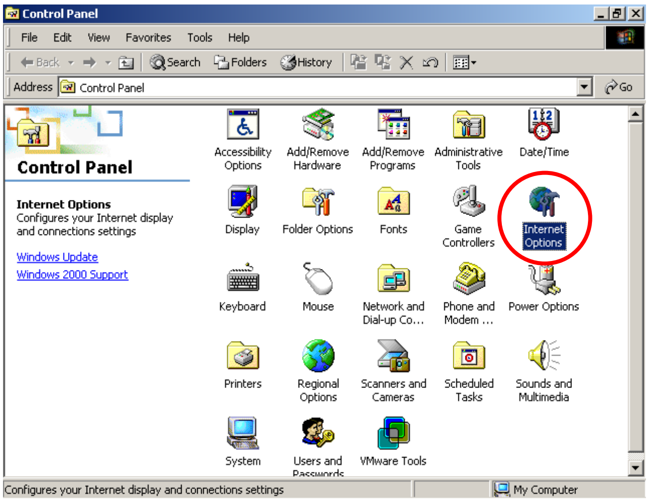
## 1. Network Configuration on PC

After HS1100 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**

◆ **Windows 9x/2000**

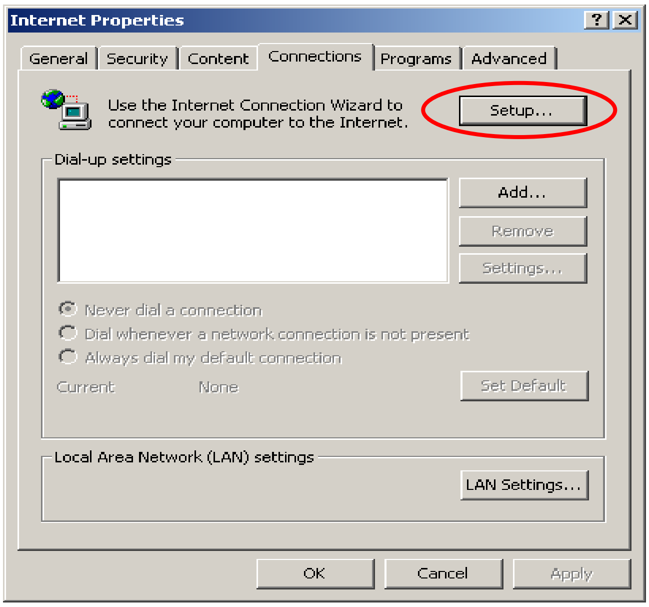
1) Choose **Start >> Control Panel >> Internet Options**.



Internet Options
Configures your Internet display and connections settings

Configures your Internet display and connections settings

2) Choose the **Connections** tab, and then click ***Setup***.



Use the Internet Connection Wizard to connect your computer to the Internet.

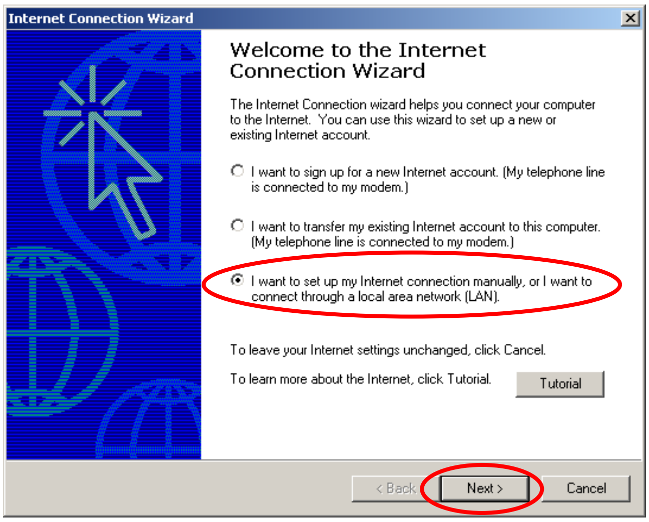
Dial-up settings

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

3) Choose **“I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)”**, and then click ***Next***.



Internet Connection Wizard

Welcome to the Internet Connection Wizard

The Internet Connection wizard helps you connect your computer to the Internet. You can use this wizard to set up a new or existing Internet account.

○ I want to sign up for a new Internet account. (My telephone line is connected to my modem.)

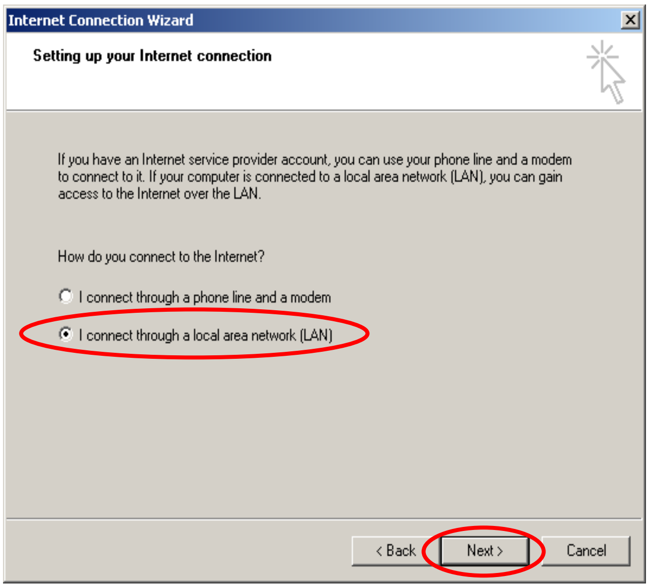
○ I want to transfer my existing Internet account to this computer. (My telephone line is connected to my modem.)

● I want to set up my Internet connection manually, or I want to connect through a local area network (LAN).

To leave your Internet settings unchanged, click Cancel.

To learn more about the Internet, click Tutorial.

4) Choose **“I connect through a local area network (LAN)”** and then click ***Next***.



Internet Connection Wizard

Setting up your Internet connection

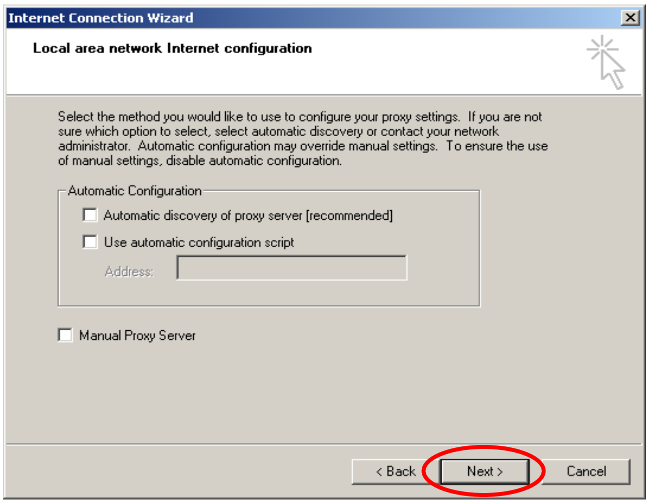
If you have an Internet service provider account, you can use your phone line and a modem to connect to it. If your computer is connected to a local area network (LAN), you can gain access to the Internet over the LAN.

How do you connect to the Internet?

○ I connect through a phone line and a modem

● I connect through a local area network (LAN)

5) **DO NOT** choose any option in the following LAN window for Internet configuration, and just click ***Next***.



Internet Connection Wizard

Local area network Internet configuration

Select the method you would like to use to configure your proxy settings. If you are not sure which option to select, select automatic discovery or contact your network administrator. Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

Automatic Configuration

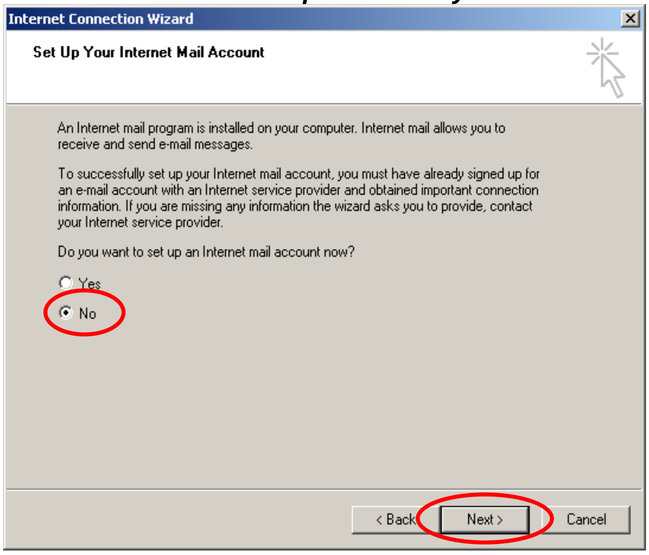
□ Automatic discovery of proxy server (recommended)

□ Use automatic configuration script

Address:

□ Manual Proxy Server

6) Choose **“No”** and then click ***Next***.



Internet Connection Wizard

**Set Up Your Internet Mail Account**

An Internet mail program is installed on your computer. Internet mail allows you to receive and send e-mail messages.

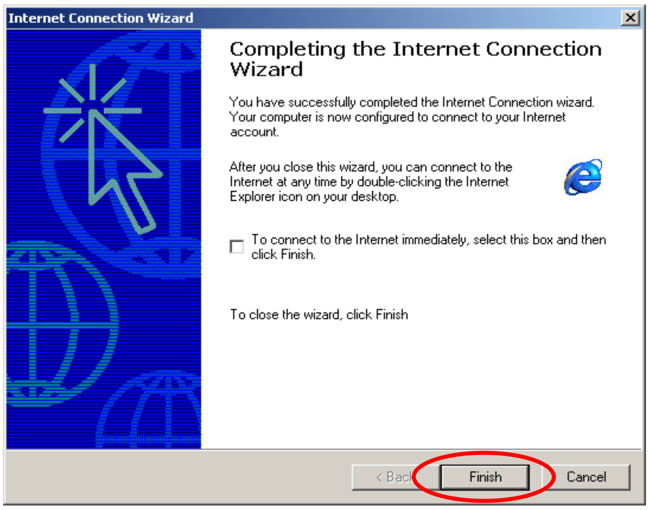
To successfully set up your Internet mail account, you must have already signed up for an e-mail account with an Internet service provider and obtained important connection information. If you are missing any information the wizard asks you to provide, contact your Internet service provider.

Do you want to set up an Internet mail account now?

○ Yes

● No

7) Finally, click ***Finish*** to exit the **Internet Connection Wizard**. Now, the set up is completed.



Internet Connection Wizard

Completing the Internet Connection Wizard

You have successfully completed the Internet Connection wizard. Your computer is now configured to connect to your Internet account.

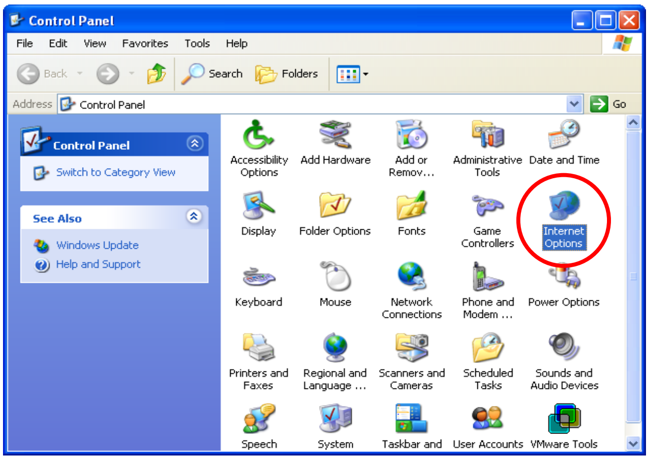
After you close this wizard, you can connect to the Internet at any time by double-clicking the Internet Explorer icon on your desktop.

□ To connect to the Internet immediately, select this box and then click Finish.

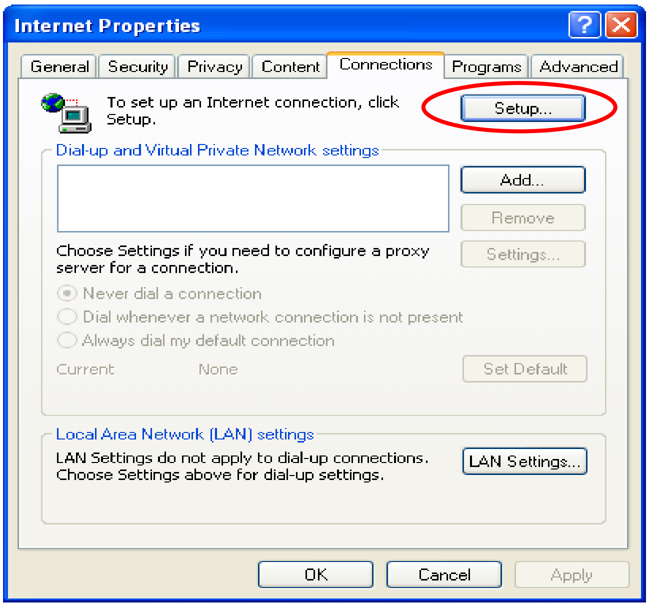
To close the wizard, click Finish

◆ **Windows XP**

1) Choose **Start >> Control Panel >> Internet Option**.



*2)* Choose the **Connections** tab, and then click ***Setup***.



Internet Properties

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

○ Never dial a connection

○ Dial whenever a network connection is not present

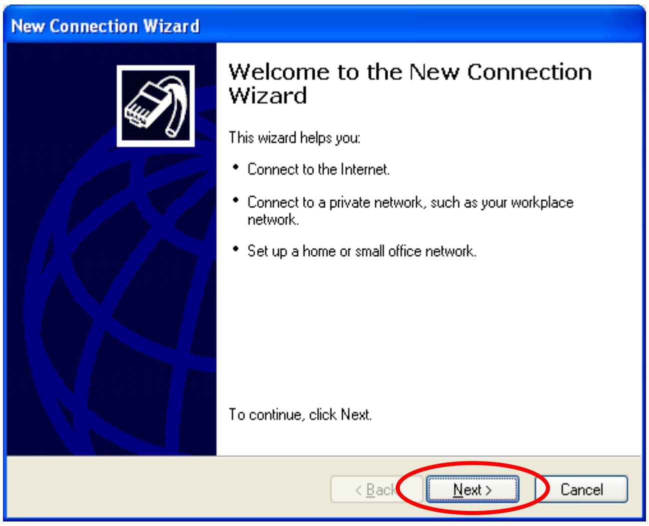
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

*3)* When the **Welcome to the New Connection Wizard** window appears, click ***Next***.



New Connection Wizard

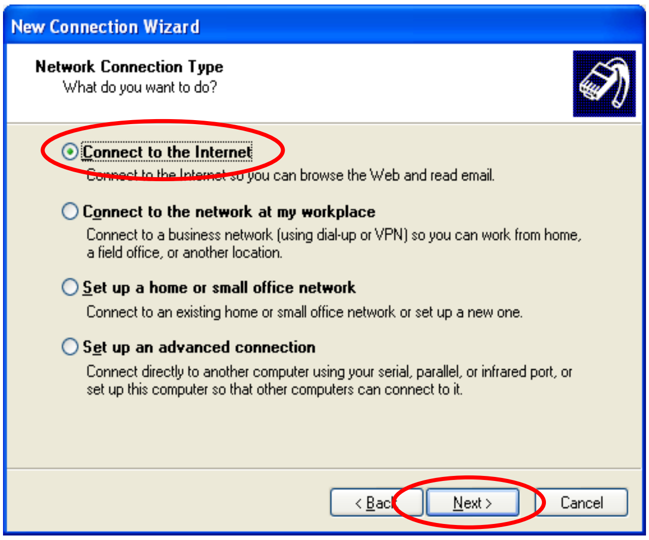
Welcome to the New Connection Wizard

This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To continue, click Next.

*4)* Choose **"Connect to the Internet"** and then click ***Next***.



New Connection Wizard

**Network Connection Type**
What do you want to do?

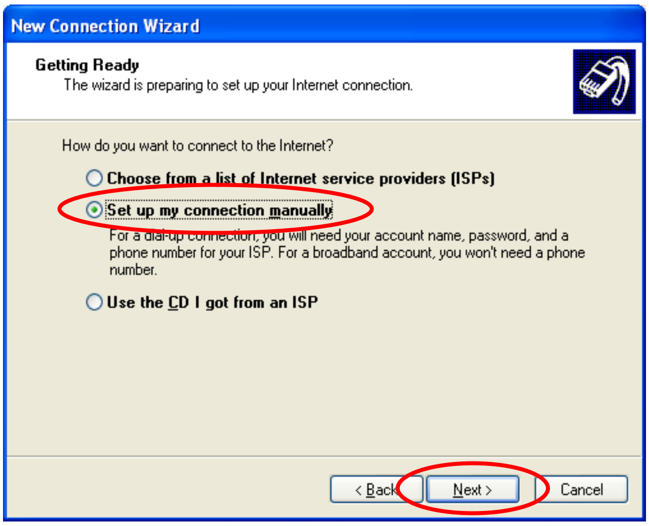
● **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

○ **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

*5)* Choose **“Set up my connection manually”** and then click ***Next***.



New Connection Wizard

**Getting Ready**

The wizard is preparing to set up your Internet connection.

How do you want to connect to the Internet?

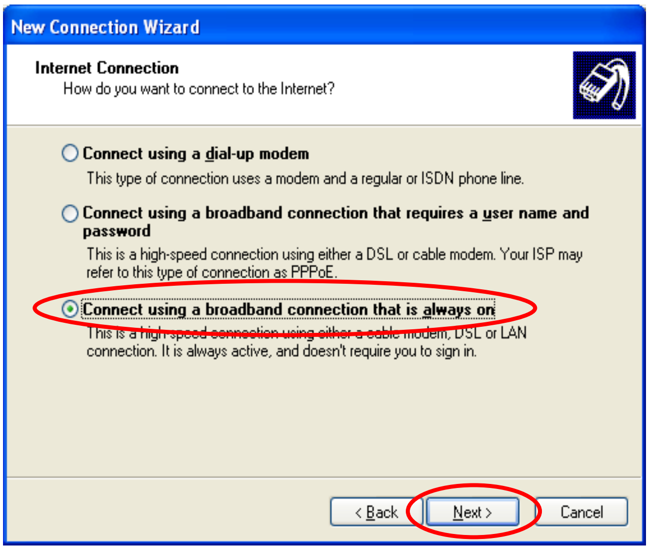
○ Choose from a list of Internet service providers (ISPs)

● Set up my connection manually

For a dial-up connection, you will need your account name, password, and a phone number for your ISP. For a broadband account, you won't need a phone number.

○ Use the CD I got from an ISP

*6)* Choose **“Connect using a broadband connection that is always on”** and then click ***Next***.



New Connection Wizard

**Internet Connection**

How do you want to connect to the Internet?

○ Connect using a dial-up modem

This type of connection uses a modem and a regular or ISDN phone line.

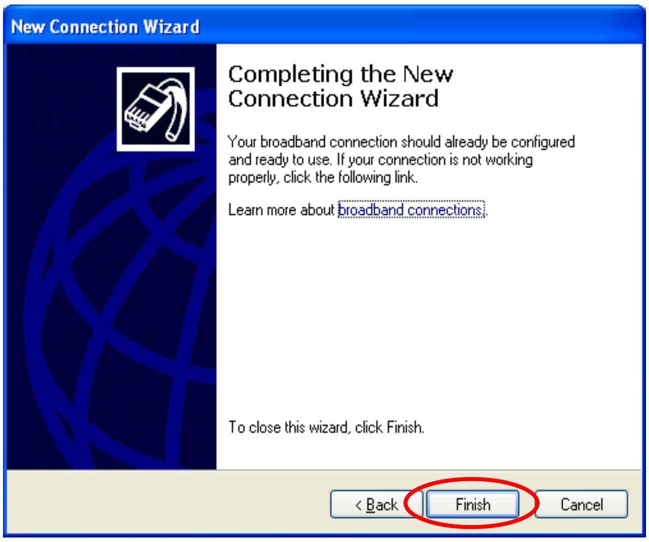
○ Connect using a broadband connection that requires a user name and password

This is a high-speed connection using either a DSL or cable modem. Your ISP may refer to this type of connection as PPPoE.

● Connect using a broadband connection that is always on

This is a high-speed connection using either a cable modem, DSL or LAN connection. It is always active, and doesn't require you to sign in.

*7)* Finally, click ***Finish*** to exit the **Connection Wizard**. Now, the setup is completed.



New Connection Wizard

Completing the New Connection Wizard

Your broadband connection should already be configured and ready to use. If your connection is not working properly, click the following link.

Learn more about broadband connections.

To close this wizard, click Finish.

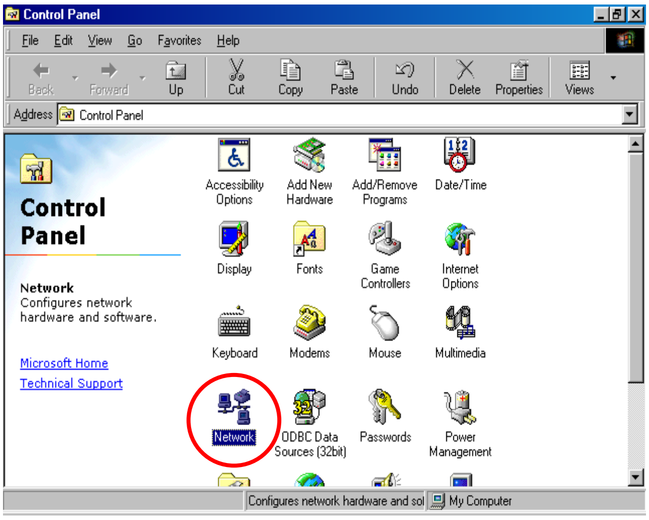
- **TCP/IP Network Setup**

If the operating system of the PC in use is Windows 95/98/ME/2000/XP, keep the default settings without any changes to directly start/restart the system. With the factory default settings, during the process of starting the system, HS1100 with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called **"Obtain an IP address automatically"**.

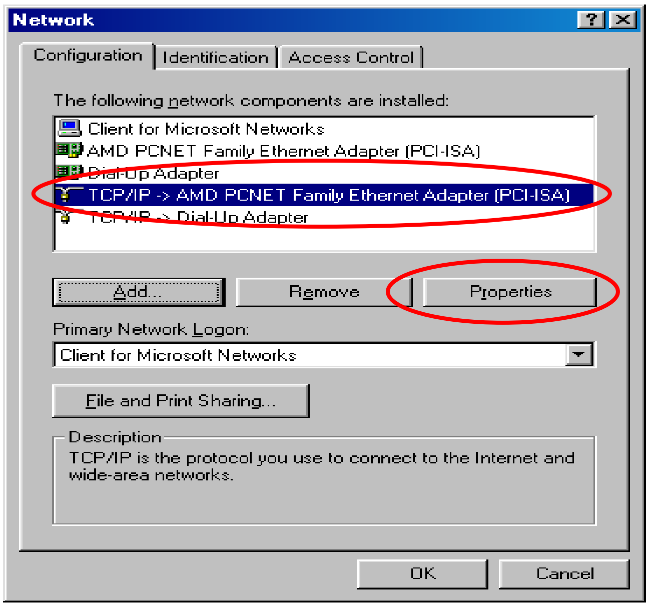
If checking the TCP/IP setup or using the static IP in the LAN1/LAN2 or LAN3/LAN4 section is desired, please follow these steps:

### ◆ Check the TCP/IP Setup of Window 9x/ME

*1)* Choose **Start >> Control Panel >> Network**.



*2)* Click on the **Configuration** tab and select **"TCP/IP > AMD PCNET Family Ethernet Adapter (PCI-ISA)"**, and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



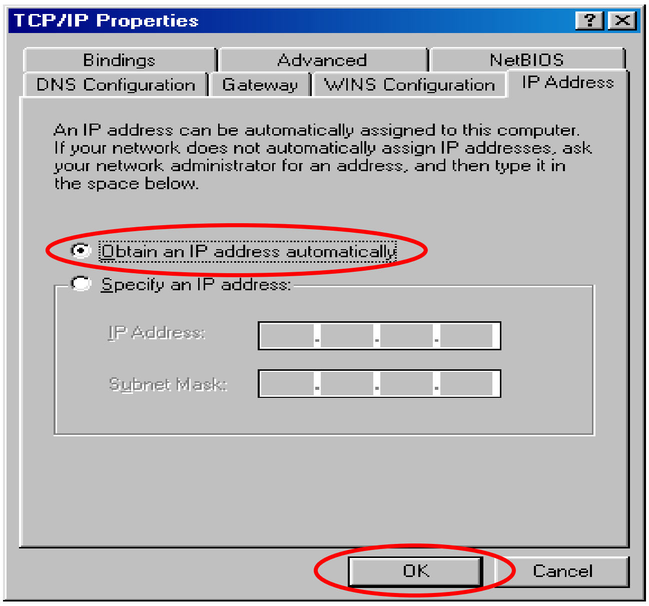
The following network components are installed:

Client for Microsoft Networks
AMD PCNET Family Ethernet Adapter (PCI-ISA)
Dial-Up Adapter
TCP/IP -> AMD PCNET Family Ethernet Adapter (PCI-ISA)
TCP/IP -> Dial-Up Adapter

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

*3)* **Using DHCP:** If you want to use DHCP, click on the **IP Address** tab and choose **"Obtain an IP address automatically"**, and then click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from HS1100.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

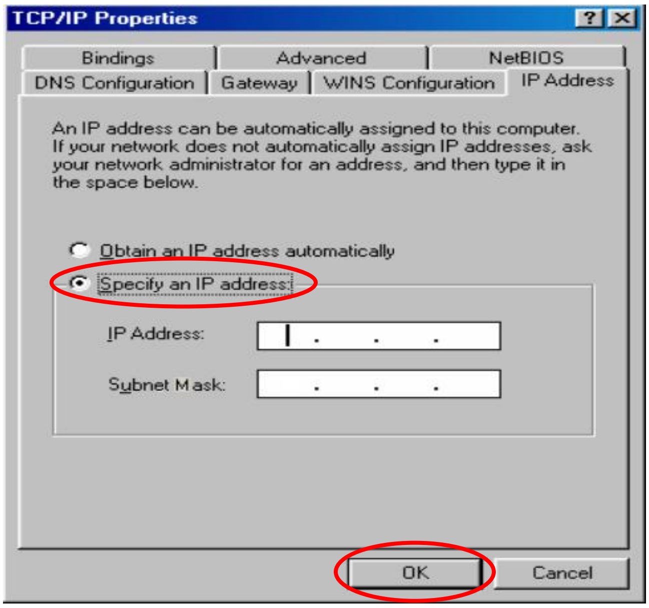
IP Address: . . .

Subnet Mask: . . .

*4)* **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of HS1100.

> *If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.*

4.1) Click on the **IP Address** tab and choose **"Specify an IP address"**. Enter the *IP Address*, *Subnet Mask* and then click ***OK***.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

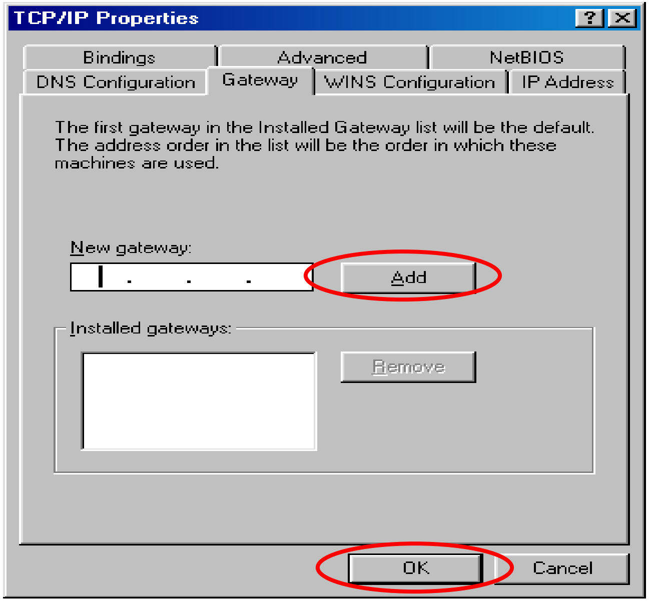
○ Obtain an IP address automatically

● Specify an IP address:

IP Address: . . .

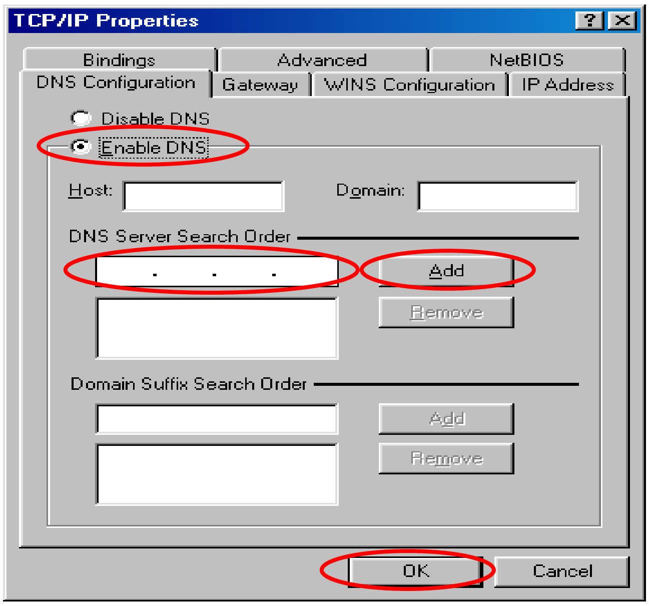
Subnet Mask: . . .

4.2) Click on the **Gateway** tab. Enter the gateway address of HS1100 in the **"New gateway"** field and click ***Add***. Then, click ***OK***.



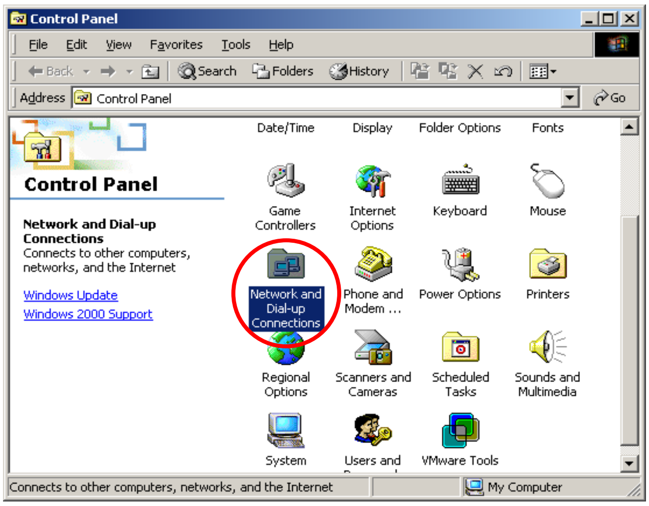
The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

4.3) Click on **DNS Configuration** tab. If the DNS Server field is empty, select **"Enable DNS"** and enter *DNS Server address*. Click ***Add***, and then click ***OK*** to complete the configuration.

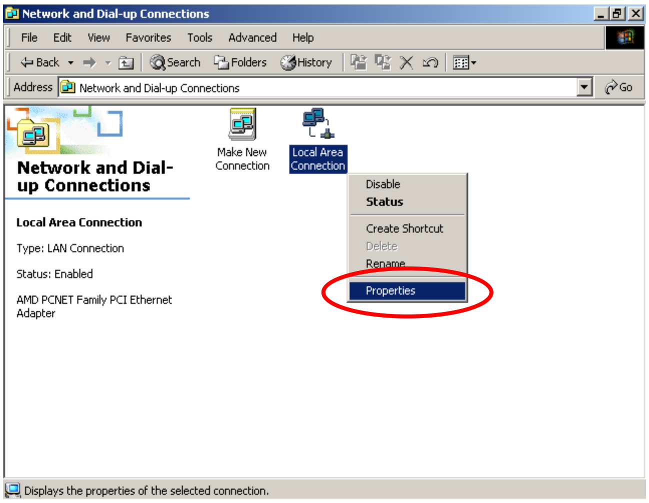


◆ **Check the TCP/IP Setup of Window 2000**

1) Select **Start >> Control Panel >> Network and Dial-up Connections**.



2) Right click on the **Local Area Connection** icon and select **"Properties"**.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Network and Dial-up Connections
Make New Connection
Local Area Connection
Disable
Status
Create Shortcut
Delete
Rename
Properties

Local Area Connection

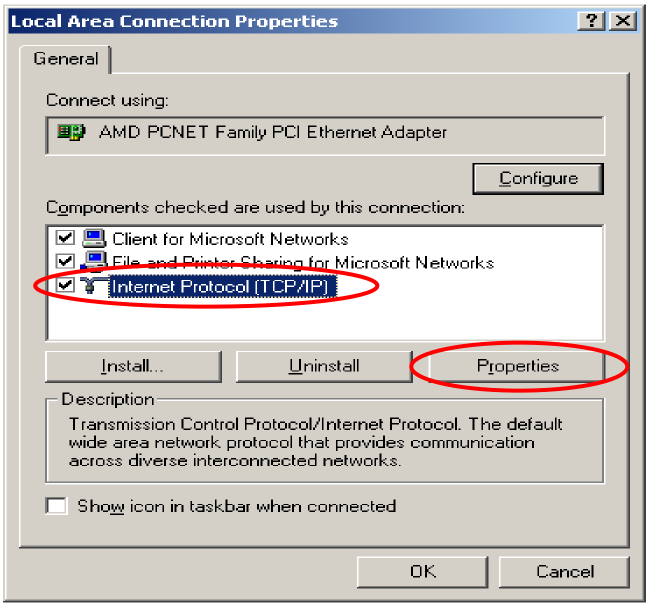
Type: LAN Connection

Status: Enabled

AMD PCNET Family PCI Ethernet Adapter

Displays the properties of the selected connection.

3) Select **"Internet Protocol (TCP/IP)"** and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



Connect using:

AMD PCNET Family PCI Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

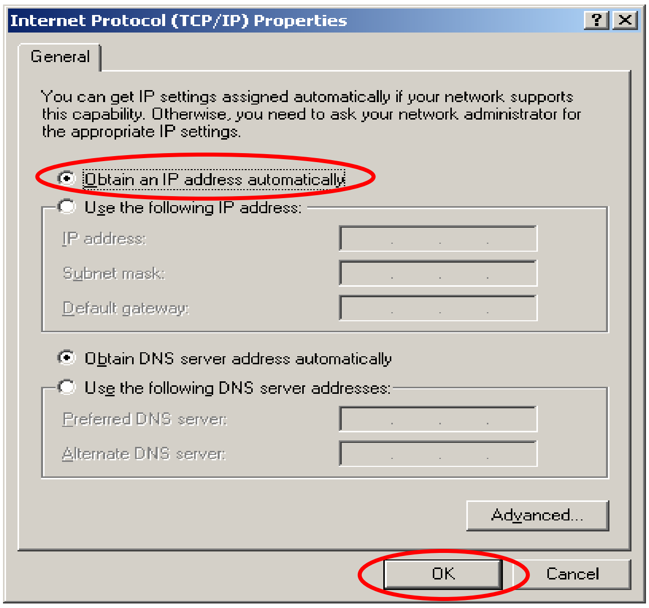
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

4) **Using DHCP:** If you want to use DHCP, choose **"Obtain an IP address automatically"**, and then click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from HS1100.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

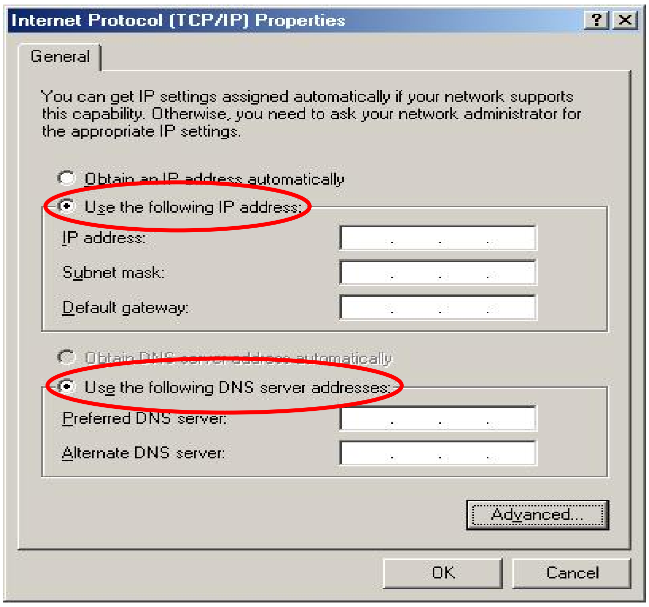
Alternate DNS server: . . .

5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of HS1100.

> ⚠ *If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.*

5.1) Choose **"Use the following IP address"** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **"Using the following DNS server addresses"** and enter the *DNS Server address*. Then, click ***OK***.

5.2) Click ***Advanced*** to enter the **Advanced TCP/IP Settings** window.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

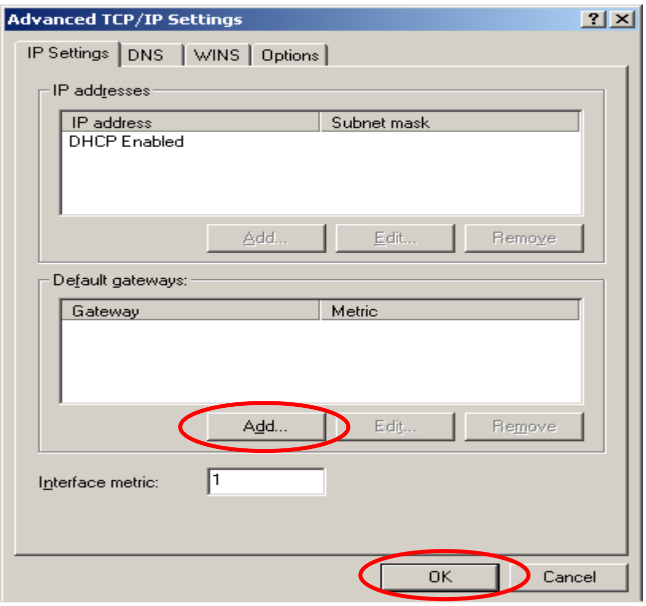
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5.3) Click on the **IP Settings** tab and click ***Add*** below the **"Default gateways"** column and the **TCP/IP Gateway Address** window will appear.



Advanced TCP/IP Settings

IP addresses

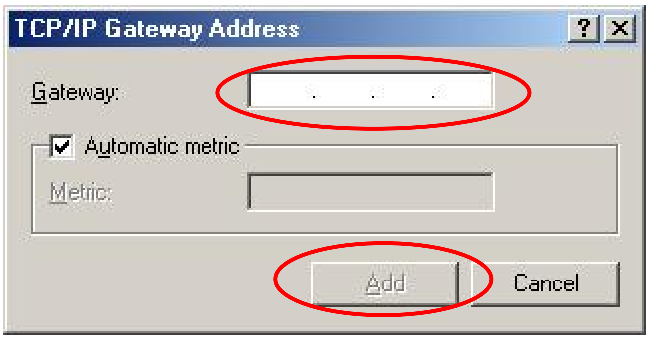
| IP address | Subnet mask |
|---|---|
| DHCP Enabled | |

Default gateways:

| Gateway | Metric |
|---|---|

Interface metric: 1

5.4) Enter the gateway address of HS1100 in the **"Gateway"** field, and then click ***Add***. After back to the **IP Settings** tab, click ***OK*** to complete the configuration.



TCP/IP Gateway Address

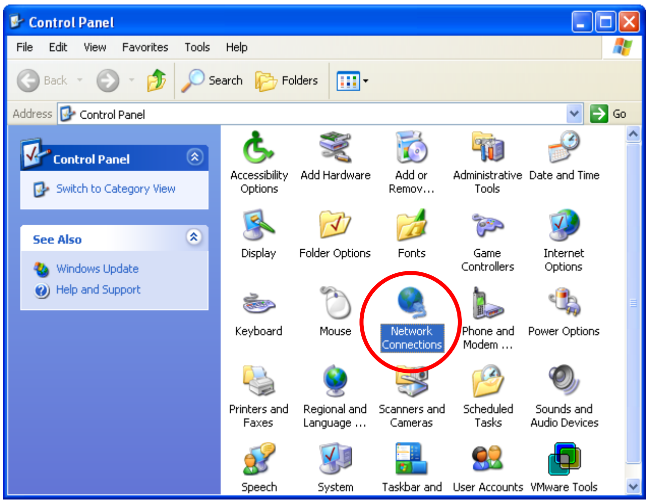
Gateway: . . .

☑ Automatic metric

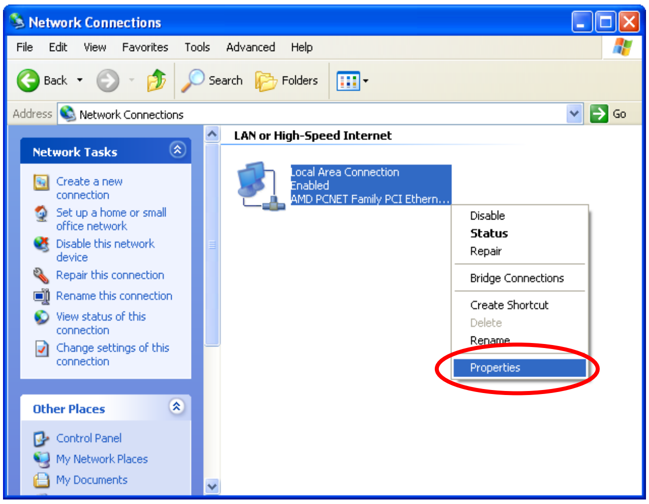
Metric:

◆ **Check the TCP/IP Setup of Window XP**

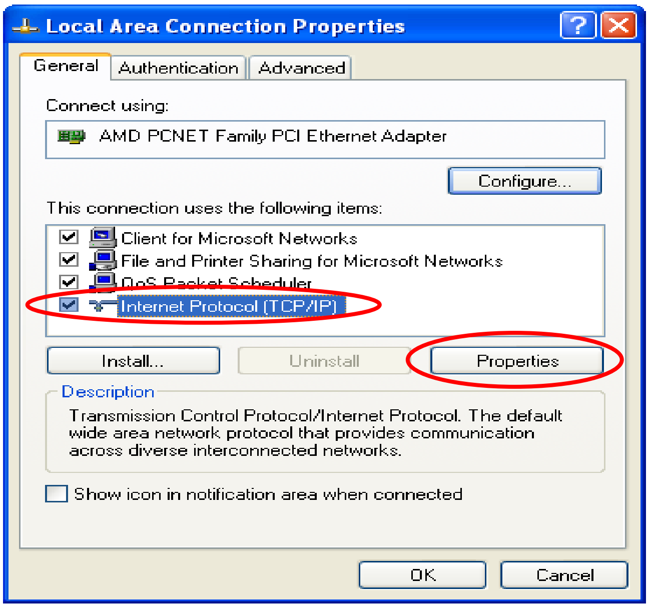
1) Select **Start >> Control Panel >> Network Connection**.



2) Right click on the **Local Area Connection** icon and select **"Properties"**.



3) Click on the **General** tab and choose **"Internet Protocol (TCP/IP)"**, and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



Connect using:

AMD PCNET Family PCI Ethernet Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

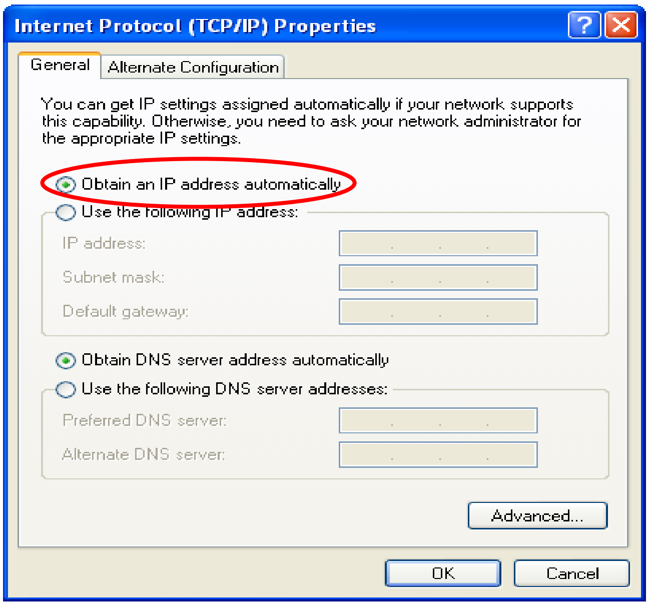
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

4) **Using DHCP:** If you want to use DHCP, choose **"Obtain an IP address automatically"** and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from HS1100.

5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of HS1100.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

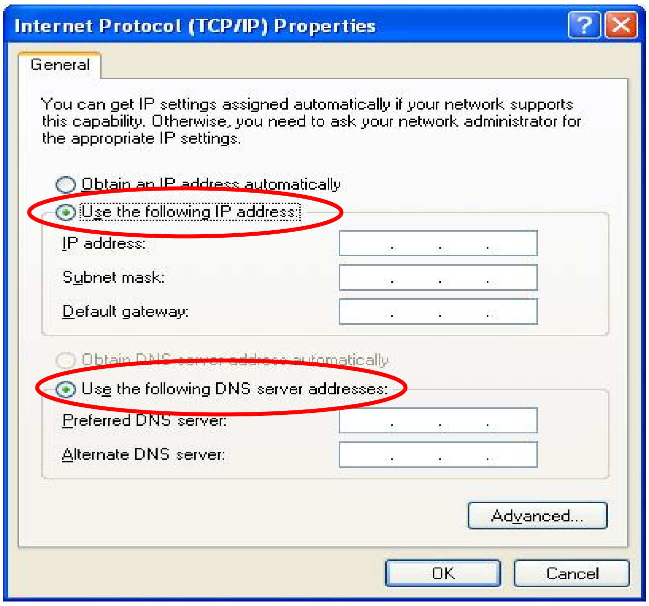
Preferred DNS server: . . .

Alternate DNS server: . . .

*If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.*

5.1) Choose **"Use the following IP address"** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **"Using the following DNS server addresses"** and enter the *DNS Server address*. Then, click ***OK***.

5.2) Click ***Advanced*** to enter the **Advanced TCP/IP Settings** window.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

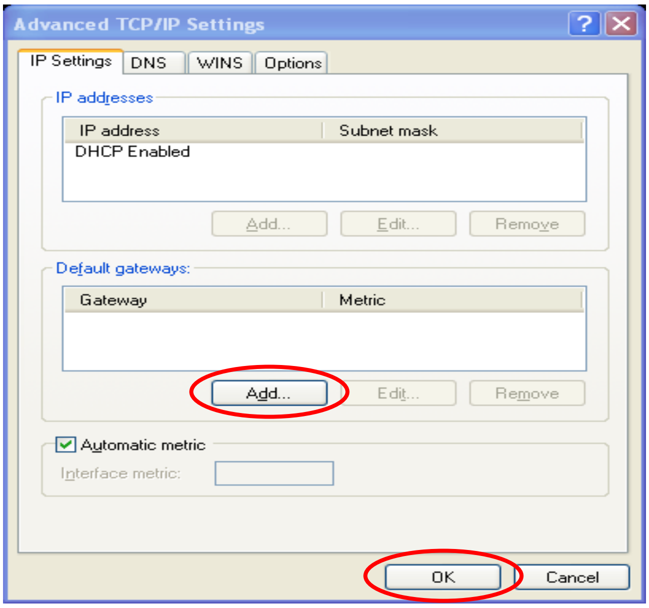
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

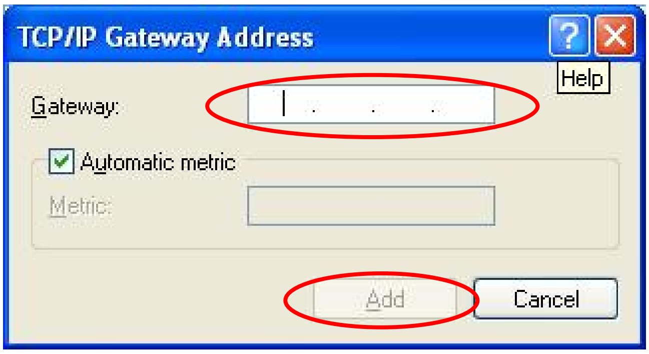
Preferred DNS server: . . .

Alternate DNS server: . . .

5.3) Click on the **IP Settings** tab and click ***Add*** below the **"Default gateways"** column and the **TCP/IP Gateway Address** window will appear.



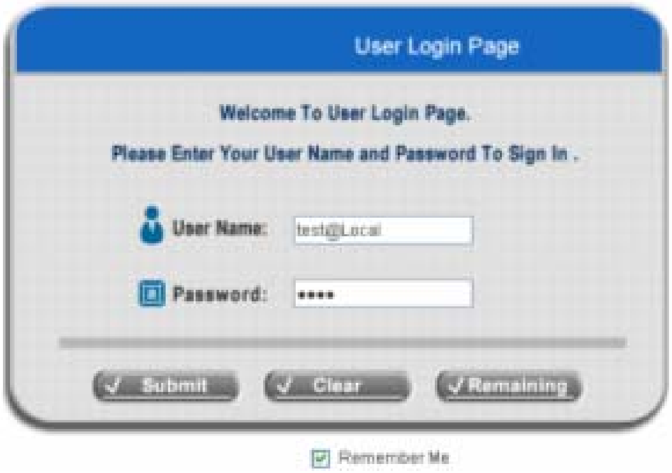
5.4) Enter the gateway address of HS1100 in the **"Gateway"** field, and then click ***Add***. After back to the **IP Settings** tab, click ***OK*** to finish the configuration.



# 2. External Network Access / User Login

If all the steps are set properly, HS1100 can be further connected to the managed network. Before connecting a client device (e.g. laptop, PC) to HS1100's Public LAN (LAN1/LAN2 by default), if eliminating the need for client IP configuration is desired, the administrator can enable the **"IP PnP"** function to support both static and dynamic IP. Otherwise, the client device must be set to use **DHCP** in TCP/IP to obtain an IP address automatically.

1. Open an Internet browser on a client device and the default **User Login Page** will be displayed.
2. Enter a username and password previously created in the Local User account database (e.g. **"test@postfix1"** for *Username* and **"test"** for *Password*). Check the ***Remember Me*** box to store the username and password on the current computer in order to automatically login to the system at next login. Then, click the ***Submit*** button.



User Login Page

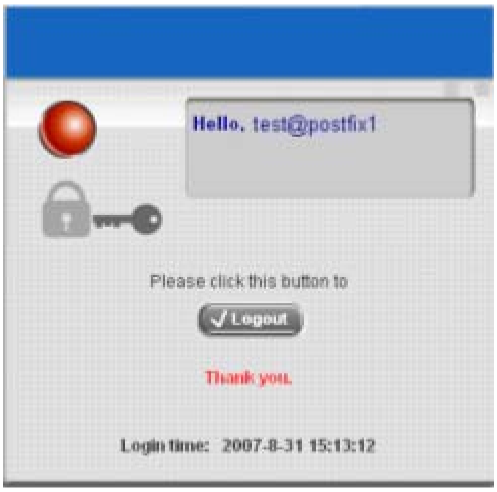
Welcome To User Login Page.

Please Enter Your User Name and Password To Sign In .

User Name: test@Local

Password: ••••

3. The **Login Successful** page appearing means HS1100 has been installed and configured successfully. Now, you are connected to the network and Internet!



Hello, test@postfix1

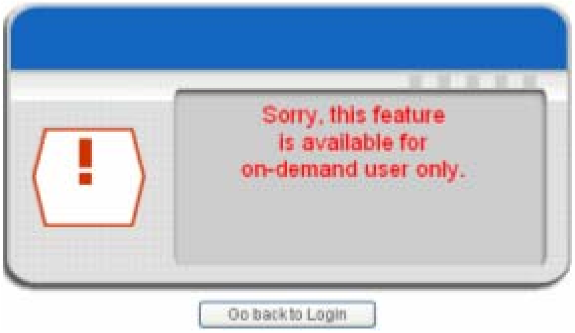
Please click this button to

Thank you.

Login time: 2007-8-31 15:13:12

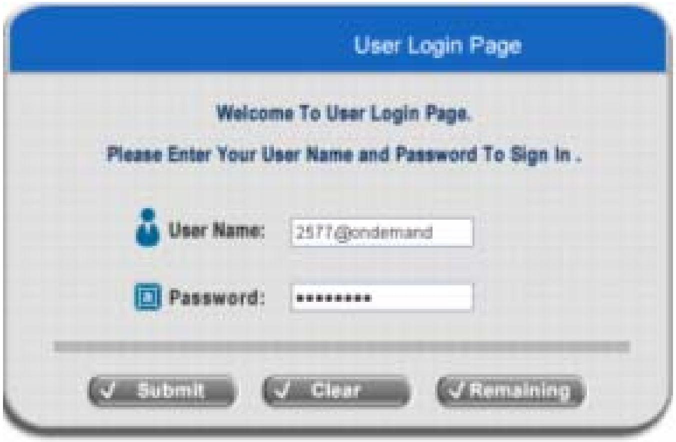
4. The ***Remaining*** button on the **User Login Page** is for on-demand users only, where they can check their Remaining Usage time. The notice shown as below will appear when non-on-demand users click the ***Remain***

button.



Sorry, this feature is available for on-demand user only.

5. An on-demand user can enter the username and password in the **User Login Page** and then click the ***Remaining*** button to check the Remaining Usage time.



User Login Page

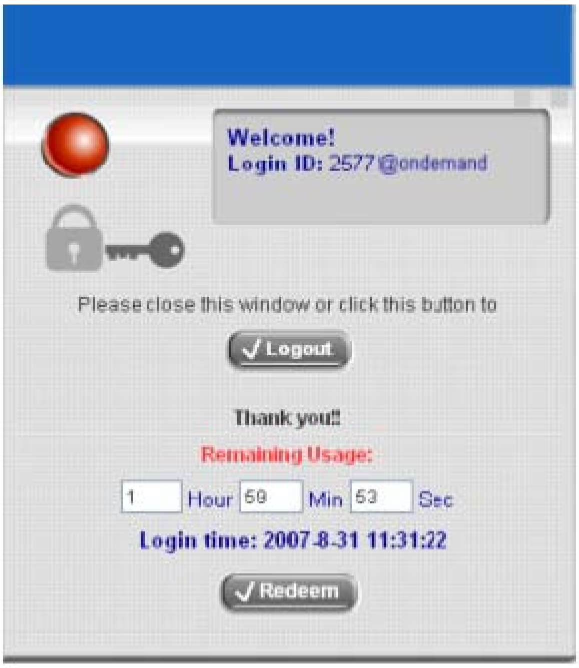
Welcome To User Login Page.

Please Enter Your User Name and Password To Sign In .

User Name: 2577@ondemand

Password: •••••••••

6. When an on-demand user logs in successfully, the **Login Successful** page shown as below will appear. The **Login Successful** page contains Remaining Usage time and a ***Redeem*** button.



Welcome!
Login ID: 2577@ondemand

Please close this window or click this button to

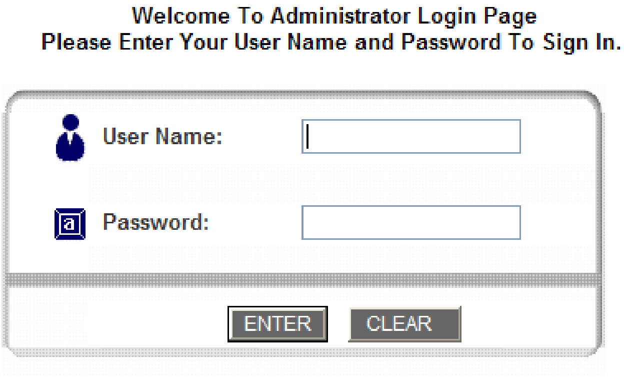
Thank you!!

Remaining Usage:

1 Hour 59 Min 53 Sec

Login time: 2007-8-31 11:31:22

- **Remaining usage:** Show the remaining time that the on-demand user can surf Internet.
- **Redeem:** When the remaining time or data size is insufficient, the user has to pay for adding credit at the counter, and then, the user will get a new username and password. After clicking the ***Redeem*** button, a login screen will appear. Please enter the new username and password obtained and click ***Redeem*** button. The total available use time and data size after adding credit will show up.



Welcome To Administrator Login Page
Please Enter Your User Name and Password To Sign In.

User Name:

Password:

⚠ *The system will automatically reject the redeem process when the redeem amount exceeds the maximum time/data volume provided by HS1100.*

# Appendix H. Session Limit and Session Log

## Session Limit

To prevent ill-behaved clients or malicious software from using up the system's connection resources, the administrator can restrict the number of concurrent sessions that a user can establish.

- ➢ The maximum number of concurrent sessions (TCP and UDP) for each user can be specified in the Global policy, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones.
- ➢ When the number of a user's sessions reaches the session limit (a choice of Unlimited, 10, 25, 50, 100, 200, 350 and 500), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to a Syslog server.
- ➢ Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in network deployment to maintain network operation.

## Session Log

The system can record connection details of each user accessing the Internet. In addition, the log data can be sent out to a specified Syslog Server, Email Box or FTP Server based on pre-defined interval time.

- ➢ The description of the fields of a session log record is shown as below:

| Field | Description |
|---|---|
| Date and Time | The date and time that the session is established |
| Session Type | [New]: This is a newly established session.<br>[Blocked]: This session is blocked by a Firewall rule. |
| Username | The account name (with postfix) of the user. When it shows "N.A.", it indicates that the user or device does not need to log in with a username, for example, the user or device is on a non-authenticated port or on the privileged MAC/IP list. Change the account name accordingly, if the name is not identifiable in the record.<br>⏩ **Note:** Only 31 characters are allowed for the combination of Session Type plus Username. |
| Protocol | The communication protocol of session: TCP or UDP |
| MAC | The MAC address of the user's computer or device |
| SIP | The source IP address of the user's computer or device |
| SPort | The source port number of the user's computer or device |
| DIP | The destination IP address of the user's computer or device |
| DPort | The destination port number of the user's computer or device |

- An example of session log data is shown as below:

```
31 Aug 12:35:05 2007    [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1626 DIP=203.125.164.132 DPort=80

31 Aug 12:35:05 2007    [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1627 DIP=203.125.164.132 DPort=80

31 Aug 12:35:06 2007    [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1628 DIP=203.125.164.142 DPort=80

31 Aug 12:35:06 2007    [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1629 DIP=203.125.164.142 DPort=80

31 Aug 12:35:07 2007    [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1630 DIP=67.18.163.154 DPort=80

31 Aug 12:35:09 2007    [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1631 DIP=202.43.195.52 DPort=80

31 Aug 12:35:10 2007    [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1632 DIP=203.84.196.242 DPort=80
```

# Appendix I: NetComm AG400 Thermal Ticket Printer Quick Start Guide

AG400 is a plug and play thermal ticket printer that connects to the NetComm HS1100 wireless hotspot gateway or IAC3000 internet access controller to print out ticket for on-demand user accounts. All billing profile configurations and settings are made in the HS1100 or IAC3000; no configurations are required to be made in the AG400. For detail explanation on how to configure billing profiles, please refer to the HS1100 or IAC3000 product user manual.

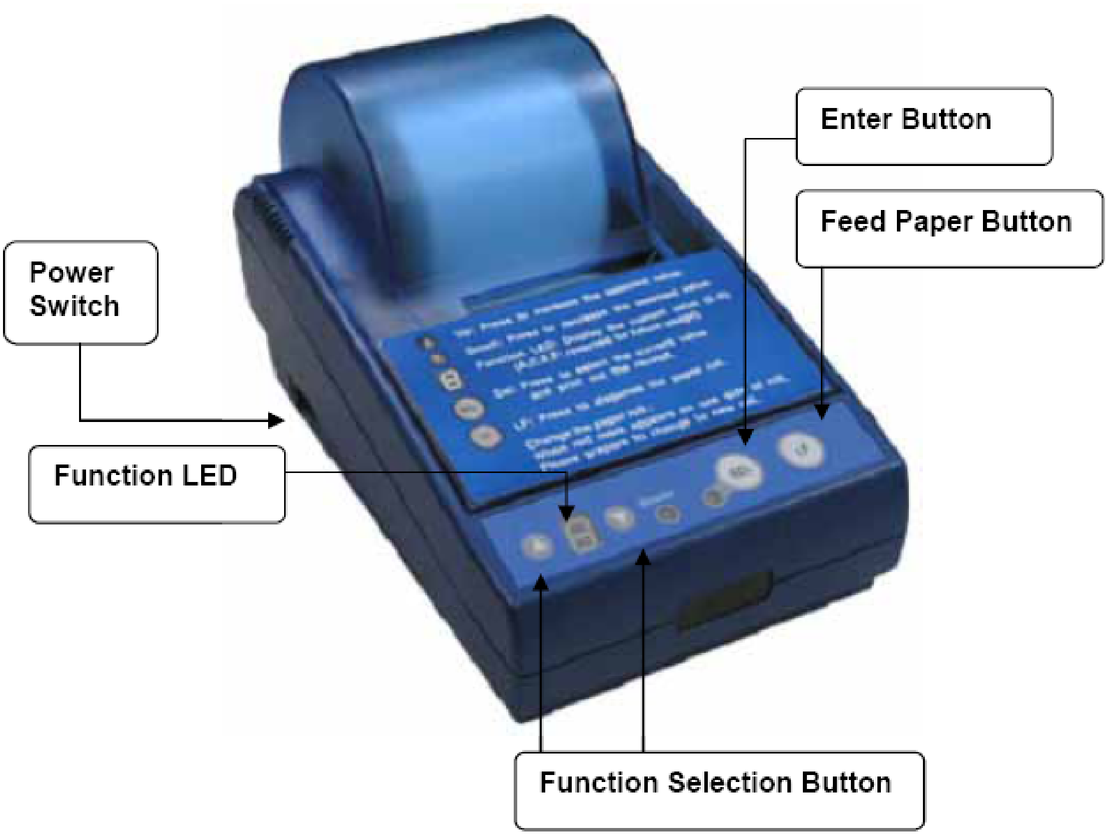
# 1. Package Contents

The standard package of the AG400 Thermal Ticket Printer includes:

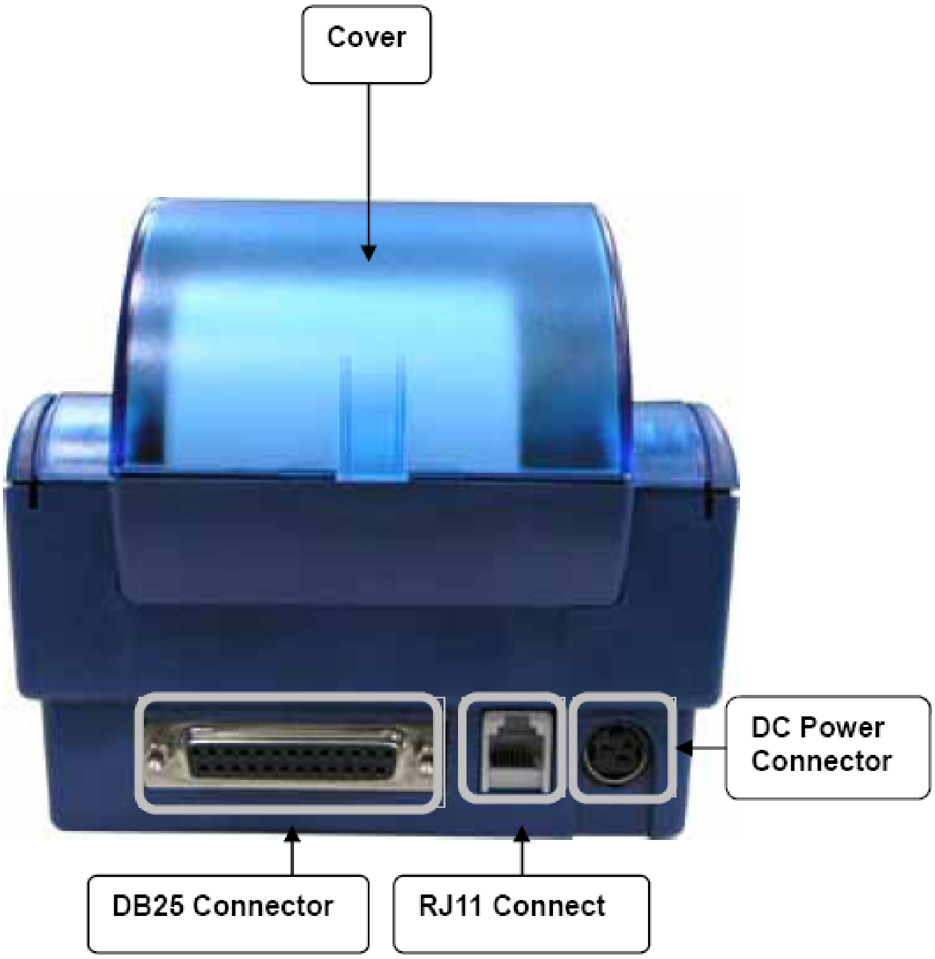
- AG400 Ticket Printer with paper x 1
- Power cable kit x 1 (AC Input: 100~240V / DC Output: 9~12V, 3A power adaptor)
- Thermal paper roll x 1
- RJ11 Cable x 1

# 2. Product Overview

(Front Side)



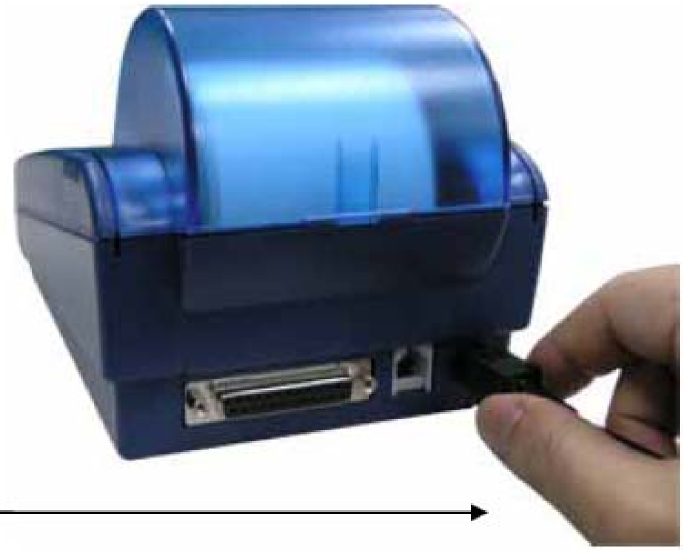
**(Back Side)**



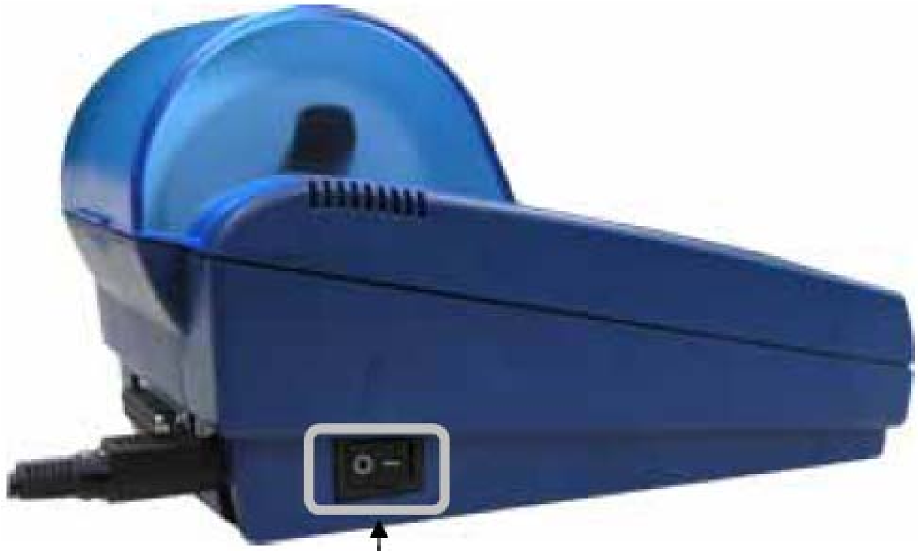
Please note:

DB25 and RJ11 connectors basically have the same function; they are used to connect to different model. The 'DB25 Connector' is not used in HS1100 or IAC3000 system. No connection is needed to this DB25 connector.

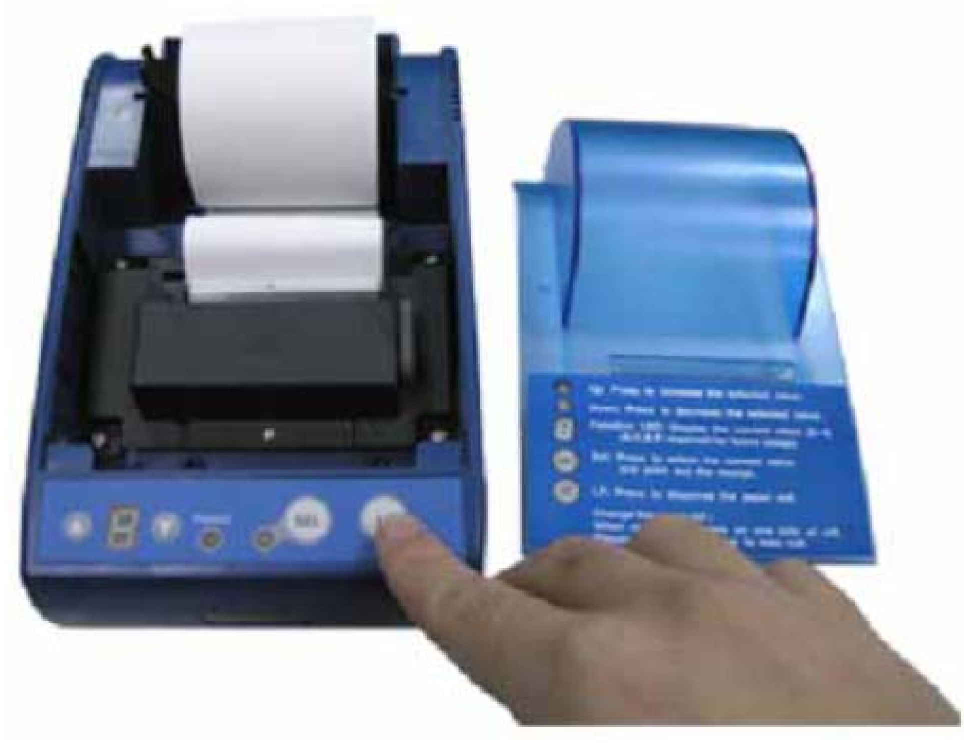
# 3. Installation



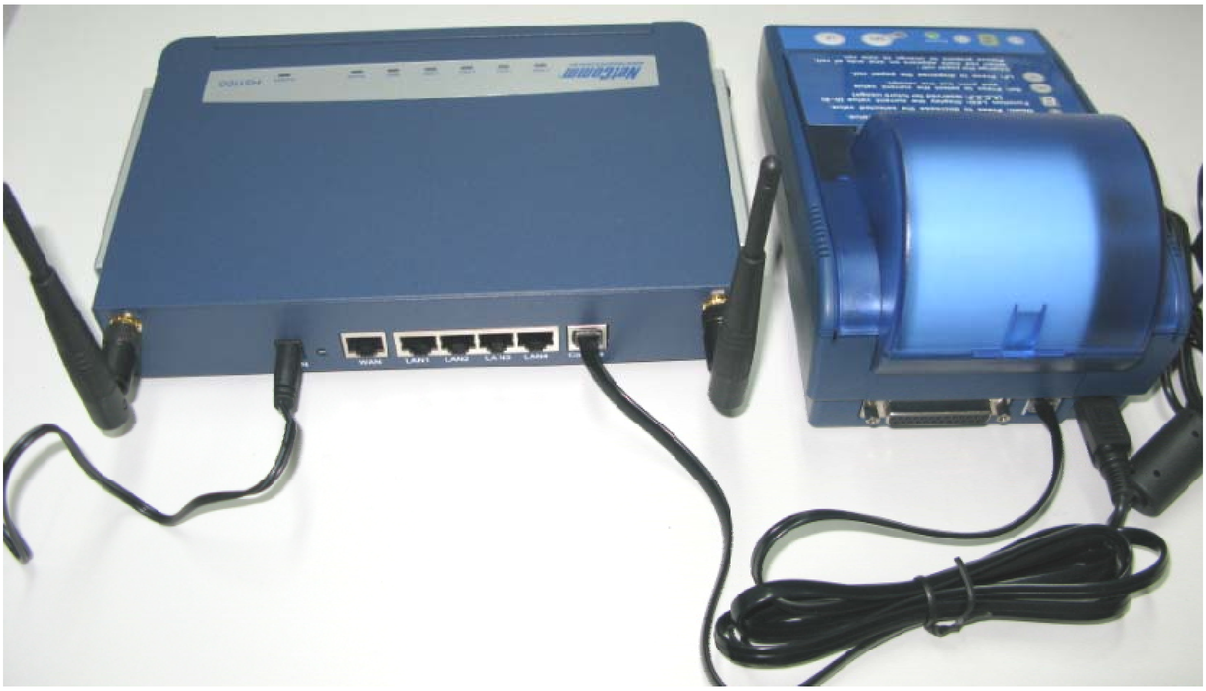
Plug in the power adapter into the back panel of the Ticket Printer



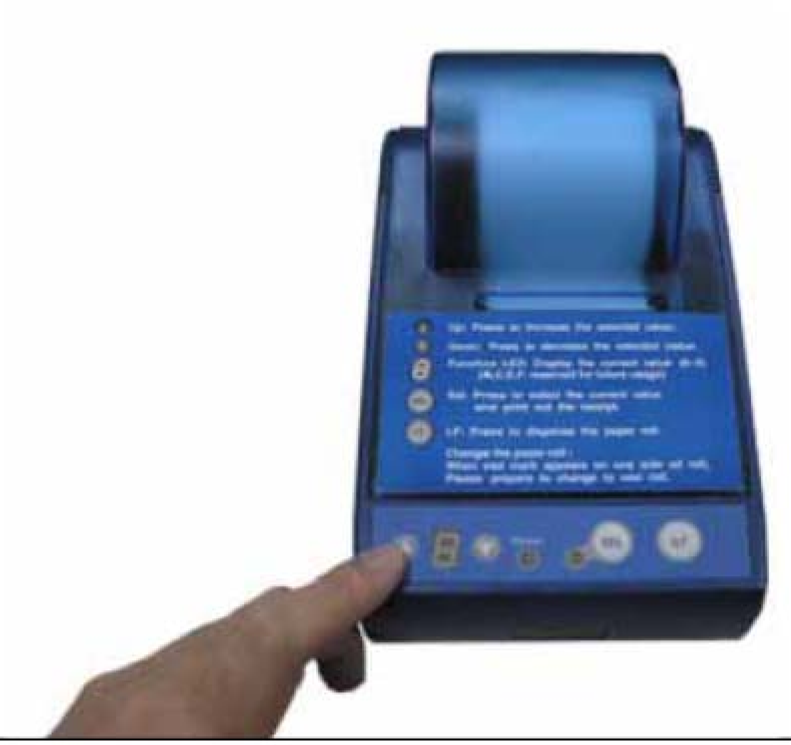
Turn on the power of Ticket Printer.



Remove the cover, then insert the paper roll and press "LF" to let the paper be drawn into the print mechanism. Then close the cover.



Connect the HS1100/IAC3000 to the AG400 Thermal Ticket Printer via the RJ11 cable provided.



Click on Function Selection button to choose the billing rule.

AG400 Thermal Ticket Printer quick installation completed

# Appendix J: Legal & Regulatory Information

NetComm Limited reserves the right to change the specifications and operating details of this product
without notice.

## Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

(1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.

(2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:

- Change the direction or relocate the receiving antenna.
- Increase the separation between this equipment and the receiver.
- Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
- Consult an experienced radio/TV technician for help.

(3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

### GNU General Public License

This product includes software code that is subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). This code is subject to the copyrights of one or more authors and is distributed without any warranty. A copy of this software can be obtained by contacting NetComm Limited on +61 2 9424 2059.

### Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;

2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

### Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

**All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at**

**www.netcomm.com.au**

www.netcomm.com.au

## Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website **www.netcomm.com.au**.

## Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

www.netcomm.com.au/support

Note: NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.

www.netcomm.com.au

**NETCOMM LIMITED** PO Box 1200, Lane Cove NSW 2066 Australia
**P:** 02 9424 2070 **F:** 02 9424 2010
**E:** sales@netcomm.com.au **W:** www.netcomm.com.au

www.dynalink.co.nz

**DYNALINK NZ** 224b Bush Road, Albany, Auckland, New Zealand
**P:** 09 448 5548 **F:** 09 448 5549
**E:** sales@dynalink.co.nz **W:** www.dynalink.co.nz