NetComm®

Wireless N Hotspot

User Guide

Revision History

Revision	Date
1.0 – Initial Release	July 2011

Table of Contents

1 Before You Start

1.1 Preface

This manual is for wireless service providers or network administrators to set up a network environment using the HS1100N system. It contains step-by-step procedures and graphic examples to guide IT staff or individuals with some network system knowledge to complete the installation.

1.2 Document Conventions

Caution:	Represents essential steps, actions, or messages that should not be ignored.
Note:	Contains related information that corresponds to a specific topic.
	Indicates that clicking this button will apply all of your settings.
	Indicates that clicking this button will clear any changed settings.
	Indicates that clicking this button will save the changes you made. **Please note:** *You must reboot the system upon the completion of the configuration for these changes to take effect.*
*	The red asterisk indicates that information in this field is compulsory.

1.3 Package Checklist

The standard package of The HS1100N includes:

- HS1100N x 1
- Quick Installation Guide (QIG) x 1
- Console Cable x 1
- Ethernet Cable x 1
- Power Adapter (DC 12V) x 1
- Rubber Antenna x 2
- Mounting Kit x 1
- Ground Cable x 1

Caution:
It is highly recommended to use the original parts supplied instead of substituting components by other suppliers in order to guarantee the best performance possible.

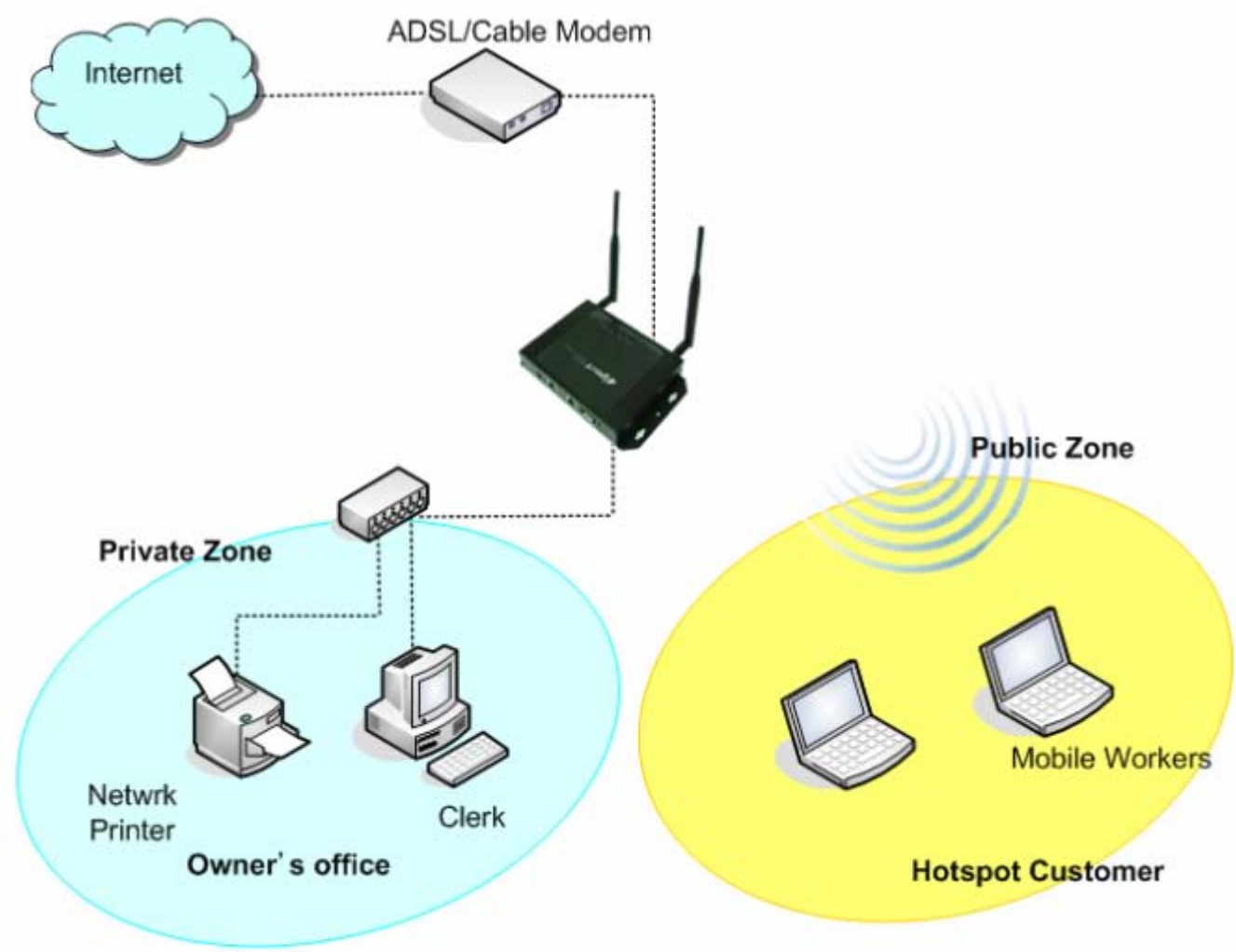
2 System Overview and Getting Started

2.1 Introduction to the HS1100N

The **HS1100N** is an economical and feature rich **Wireless Hotspot Gateway.** Feature-packed for hotspot operation, the HS1100N comes with a **built-in wireless 802.11 n/b/g MIMO access point, web server and web pages for clients to login, simple user/visitor account management tool, payment plans, multiple credit card gateways, traffic logs, and IP sharing**. The HS1100N also includes the extra advantage of being wall-mountable and dust-proof with a (IP50) metal housing.

2.2 System Concept

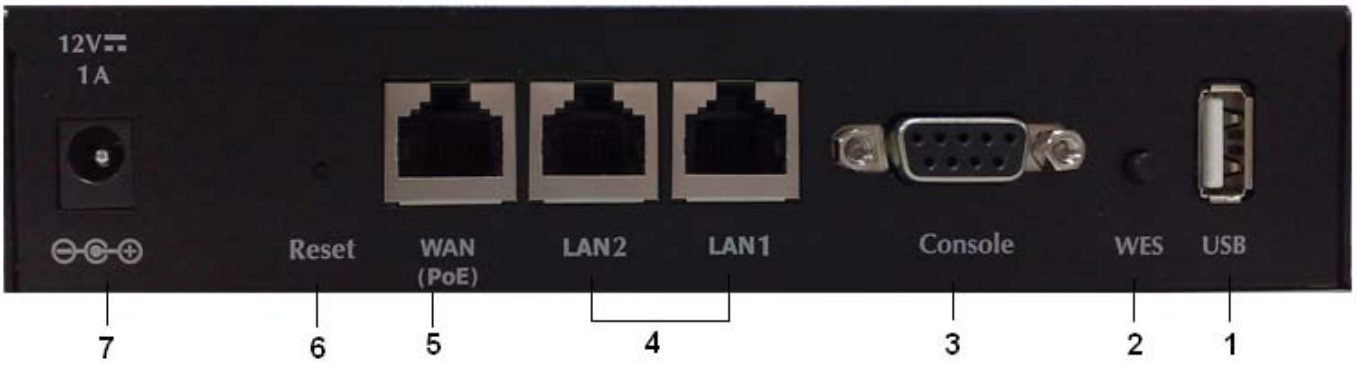
The HS1100N is capable of managing user authentication, authorisation and accounting. The user account information is stored in the local database or a specified external RADIUS database server. Featuring user authentication and integrated with external payment gateway, the HS1100N allows users to easily pay the applicable fee and enjoy the Internet service using credit cards through a variety of payment gateways including Authorize.Net, PayPal, SecurePay, and WorldPay. Furthermore, the HS1100N introduces the concept of Zones – a Private Zone and Public Zone, each with its own definable access control profiles. The Private Zone means clients are not required to be authenticated before using the network services. On the other hand, clients in the Public Zone are required to be authenticated before using the network services. This enables hotspot owners to deploy wireless network services for clients and then to manage the network as well. The following diagram is an example of the HS1100N set to manage the Internet and access to network services in a typical deployment scenario.



【*Example: A typical Hotspot network*】

2.3 Hardware Descriptions

Front Panel

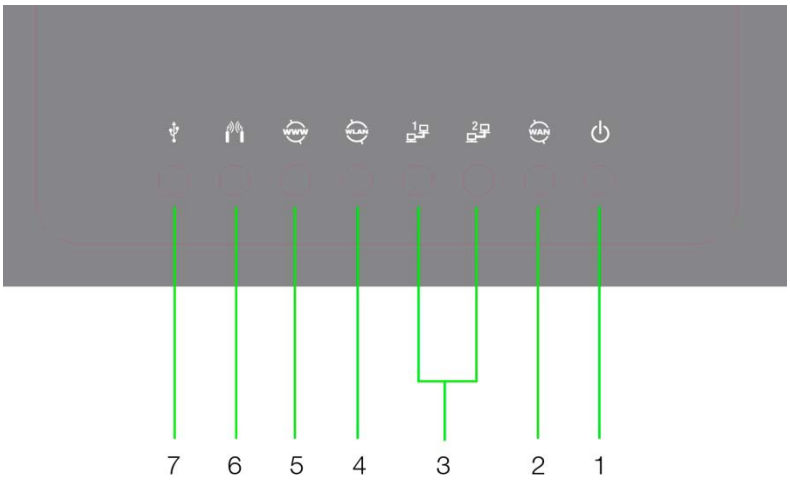


1	**USB**	For future usage only.
2	**WES**	Press to start running WES (WDS Easy Setup) process.
3	**Console**	Attach the RS-232 console cable here, for management use only.
4	**LAN1/LAN2**	Attach Ethernet cables here for connecting to the wired local network. LAN1 maps to Private Zone and requires no user authentication, LAN2 maps to Public Zone and by default requires user authentication.
5	**WAN (PoE)**	Attach the wired external network here. This port supports Power over Ethernet (PoE) for flexible installation.
6	**Reset**	Hardware reset button, press once to restart the system.
7	**Power Socket (12VDC/1A)**	For connecting to external power supply via the power adapter.

Rear Panel

1 **2**	**Antenna Connector**	Attach antennas here. The HS1100N supports 1 RF interface with 2 SMA connectors.

Top LED Panel



1		LED ON indicates power on; OFF indicates power off.
2	WAN	LED ON indicates WAN connection; OFF indicates no connection; BLINKING indicates transmitting data.
3		LED ON indicates LAN1/LAN2 connection; OFF indicates no connection; BLINKING indicates transmitting data.
4	WLAN	LED ON indicates wireless ready.
5	WWW	LED ON indicates outbound internet connection is alive; LED OFF indicates that outbound internet connection is down. The detection interval is 1 minute; hence it reflects the connection status within the last minute.
6		For indicating WES status during WES setup:
7		For future usage only.

	Master	Slave
WES Start	LED BLINKING SLOWLY	LED BLINKING QUICKLY
WES Negotiate	LED BLINKING SLOWLY	LED BLINKING QUICKLY
WES Fail (Negotiate Timeout)	LED OFF	LED OFF
WES Success	LED ON for over 5 seconds	LED ON for over 5 seconds (after Master displays WES Success)

2.4 System Requirement

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

2.5 Installation Steps

Please follow the steps below to install the HS1100N:

1. **Place the HS1100N in the best location possible.**
   The best location for The HS1100N is usually at the centre of your wireless network.
2. **There are two ways to supply power over to the HS1100N.**
   (a) Connect the **DC power adapter** to the HS1100N power socket on the front panel.

   (b) The HS1100N is capable of receiving DC current via its WAN PoE port. Connect an IEEE 802.3af-compliant PSE device, e.g. a PoE-switch, to the WAN port of The HS1100N with the Ethernet cable.
3. **Connect the HS1100N to your outbound network device.**
   Connect one end of the **Ethernet cable** to the WAN port of the HS1100N on the front panel. Depending on the type of internet service provided by your ISP, connect the other end of the cable to an ADSL/ cable modem, a switch or a hub. The WAN LED indicator should be ON to indicate a proper connection.
4. **Connect the HS1100N to your network device.**
   Connect one end of the **Ethernet cable** to the LAN1 port of The HS1100N on the front panel. Connect the other end of the cable to a PC for configuring the system. The LAN1 LED indicator should be ON to indicate a proper connection.

   Note:

   The HS1100N has two virtual zones **Private** and **Public** which are mapped to LAN1(192.168.110.254) and LAN2(192.168.11.254) respectively.

The hardware installation is now complete.

Caution:
Only use the power adapter supplied with the HS1100N. Using a different power adapter may damage the unit.

2.6 Access Web Management Interface

The HS1100N supports Web Management Interface (WMI) configuration. Upon the completion of hardware installation, the HS1100N can be configured via web browsers with JavaScript enabled such as Internet Explorer version 6.0 and above or Firefox.

Default LAN interface IP address:

LAN1 (192.168.110.1) is mapped to Private Zone with no authentication required for users.

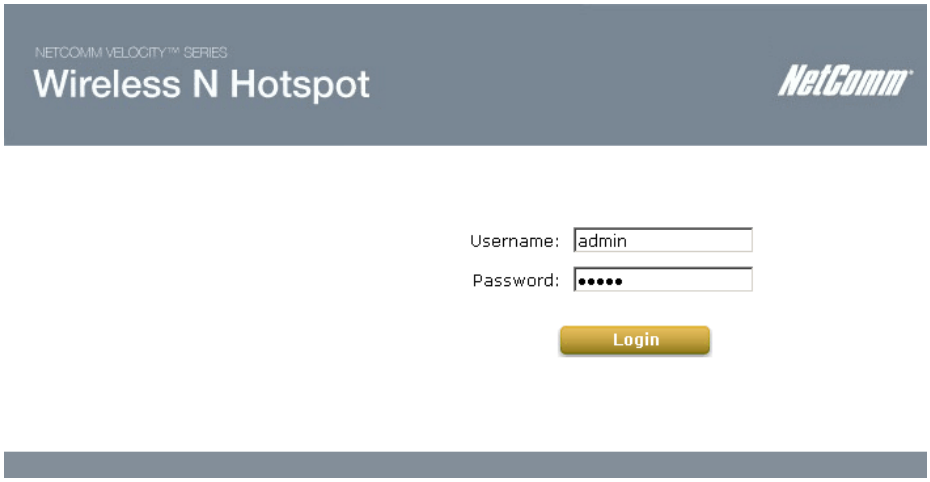
LAN2 (192.168.11.254) is mapped to Public Zone, by default authentication is required for users.

Note: The instructions below are illustrated with the administrator PC connected to LAN1.

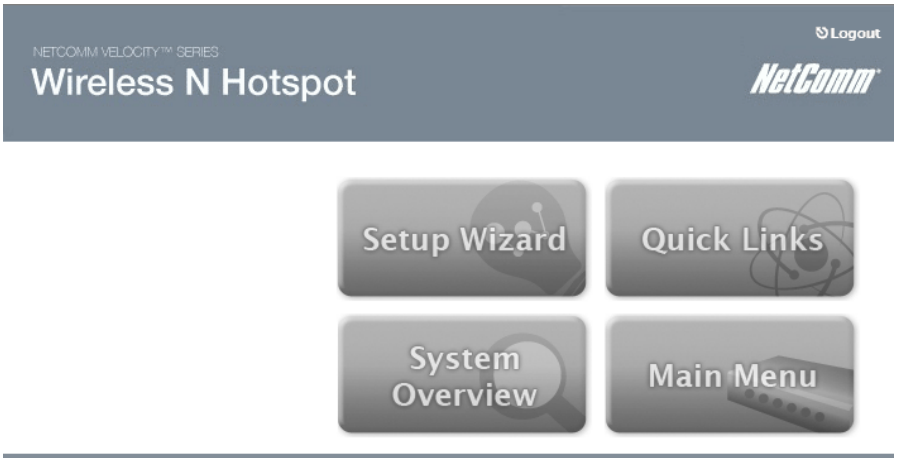
To access the web management interface, connect a PC to **LAN1 Port**, and then launch a browser. **Make sure you have set your computer to "Obtain an IP address automatically"**. The default gateway IP address should be the default gateway IP address of the Private Zone: "192.168.110.1".

Next, enter the gateway IP address of The HS1100N at the address field. The default gateway IP address of **LAN1 Port** is***"https://192.168.110.1"*** (**"https"** is used for a secured connection).

The administrator login page will appear. Enter ***"admin"***, the default username, and ***"admin"***, the default password, in the **User Name** and **Password** fields. Click ***LOGIN*** to log in.



After a successful login, the "Home" page with four main buttons will appear on the screen.



For the first time, if the HS1100N is not using a **trusted SSL certificate**, there will be a **"Certificate Error"**, because the browser treats the HS1100N as an illegal website. Please press **"Continue to this website"** to continue.

Caution:
If you are unable to see the login screen verify your computer is configured to obtain an IP address automatically. You can also try using a static IP address such as 192.168.110.xxx (where xxx is a number between 2 and 254) and then try loading the page again.

For assistance configuring your computer, please refer to Appendix A: Network Configuration on a Computer.

3 Adding the HS1100N to the Network

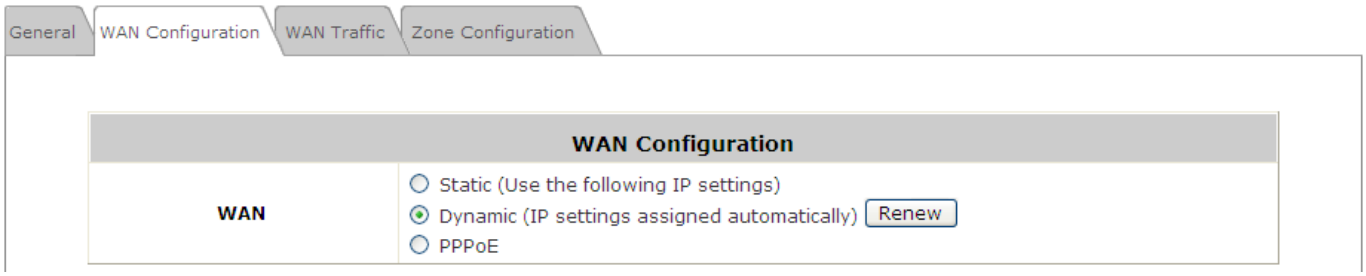
3.1 Network Requirement

In typical network environment, the main role of the HS1100N is a gateway that manages all the network access from the internal network to the Internet. Thus, the first step is to prepare an Internet connection from your ISP (Internet Service Provider) and connect it to the WAN port of The HS1100N.

3.2 Configuring the WAN Port

There are 3 connection types for the WAN Port: **Static**, **Dynamic** and **PPPoE**.

To configure the WAN port, go to: ***System >> WAN Configuration***.

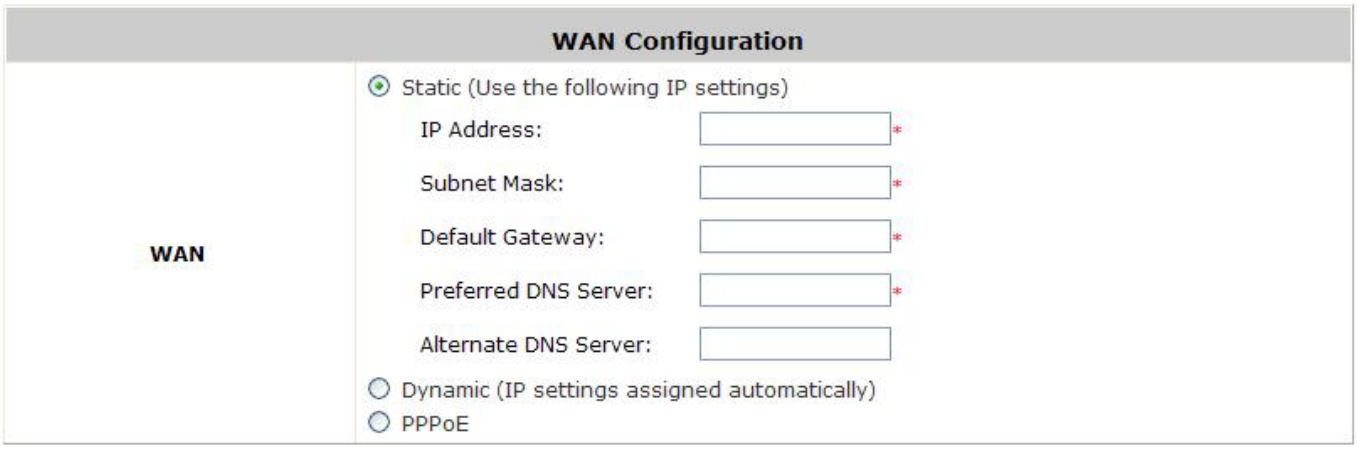


The parameters related to each connection method are described in the following page.

3.2.1 Static IP

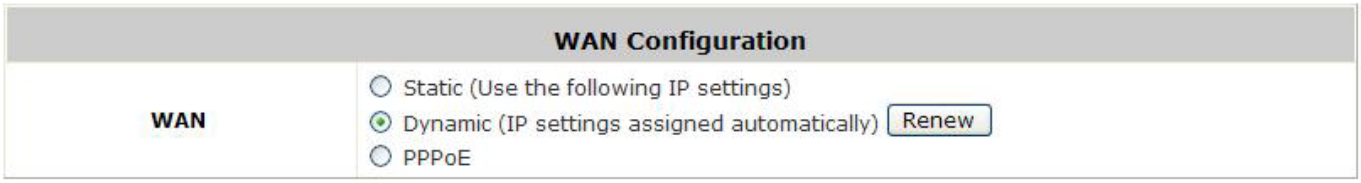
Static: Manually specifying the IP address of the WAN Port. The fields with red asterisks are mandatory.

- **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 system.
- **Alternate DNS Server:** The substitute DNS Server of the system. This is an optional field.



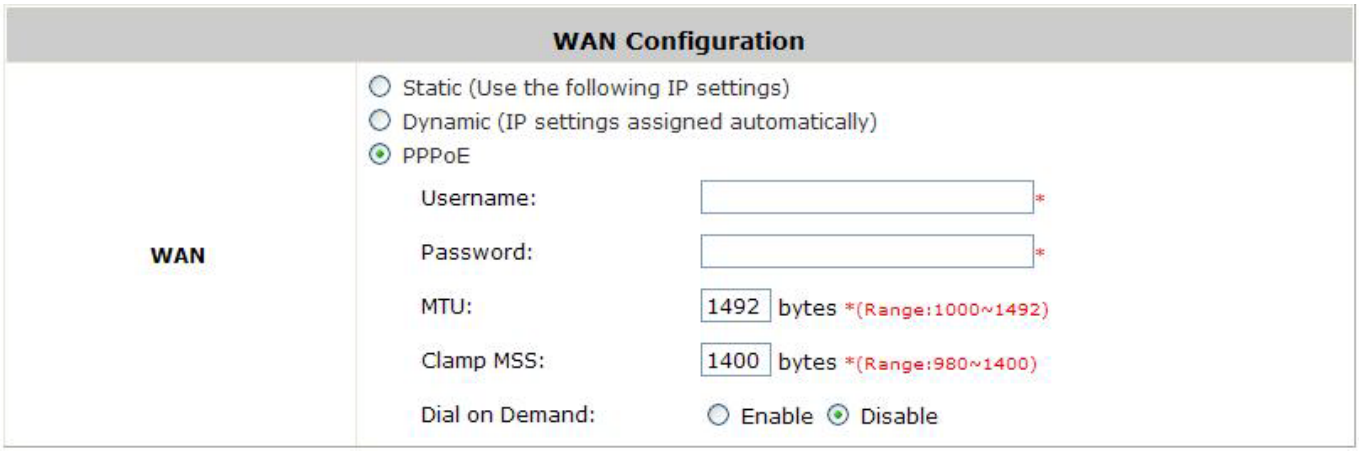
3.2.2 Dynamic

Dynamic: This options is only applicable for a network environment where the DHCP server is available upstream (i.e. – Available from your ISP) of the HS1100N. Click the ***Renew*** button to get an IP address automatically.



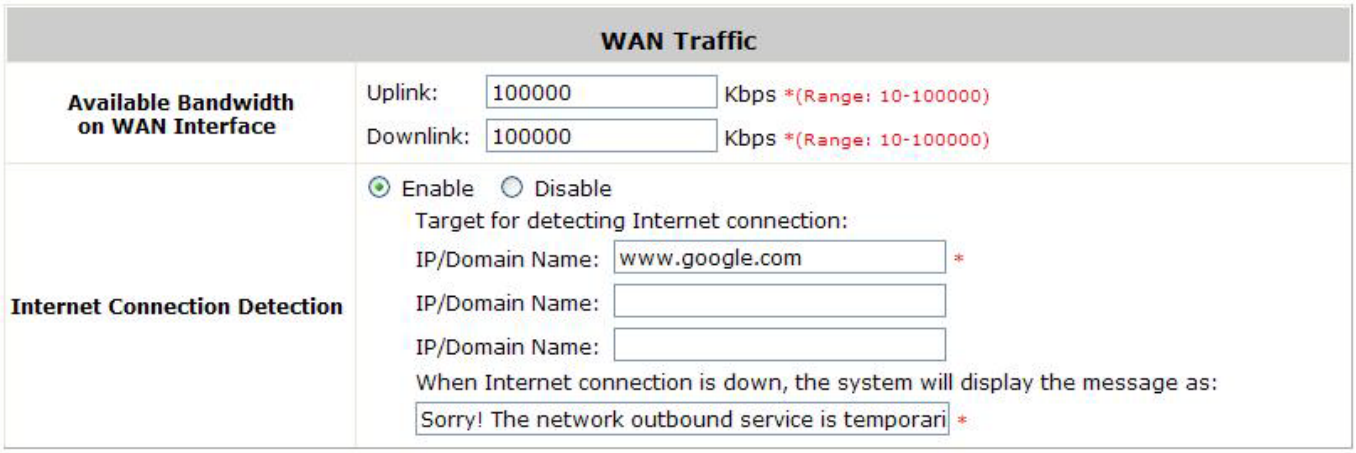
3.2.3 PPPoE

PPPoE: When selecting PPPoE to connect to the network, enter the **"Username"**, **"Password"**, **"MTU"** and **"Clamp MSS"** as supplied by your ISP. There is also a **Dial on demand** function under PPPoE. If this function is enabled, the **Maximum Idle Time** field becomes available. When the idle time is reached, the system will automatically disconnect itself.



3.3 Internet Connection Detection

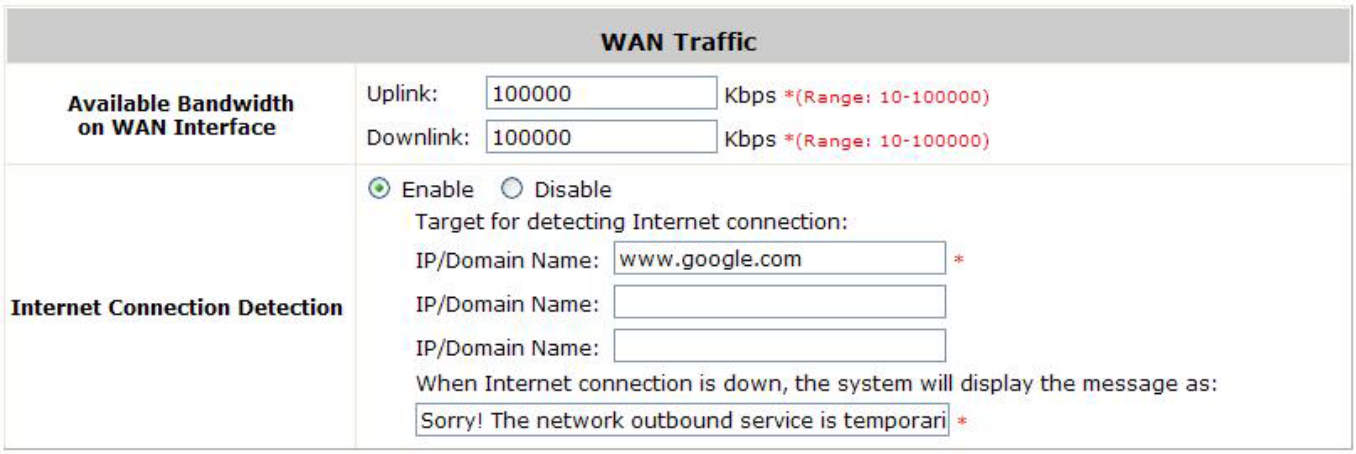
To configure Internet Connection Detection, go to: ***System >> WAN Traffic***.



- **Internet Connection Detection:** When enabled, the system will try to access the listed IP/Domain addresses. If the system can reach these IP/Domain address, it means that the outbound Internet connection is in a normal state. There is also a text box available for the administrator to enter a message. This message will appear on clients' screens when the Internet connection is down.

3.4 WAN Bandwidth Control

To configure WAN Bandwidth Control, go to: ***System >> WAN Traffic***.



The feature gives administrators control over the entire system's traffic though the WAN interface. These parameters set here should not exceed the real bandwidth coming from your ISP. For example, if your xDSL connection is 8Mbs/640kbs, you may input these two values here.

Available Bandwidth on WAN Interface:

- **Uplink:** Specifies the maximum uplink bandwidth that can be shared by clients of the system.
- **Downlink:** Specifies the maximum downlink bandwidth that can be shared by clients of the system.

3.5 What is a Zone?

To configure Zones, go to: ***System >> Zone Configuration***.

A *Zone* is a logical network area that covers wired or wireless networks, or both of them. By associating to the unique ESSID of a Zone, the wireless network is divided into different logical zones. Clients attempting to access the resources within a particular Zone will be controlled based on the access control profile of that Zone, such as authentication, security feature, wireless encryption method and traffic control, etc.

There are two Zones that can be utilised by The HS1100N – A Private Zone and a Public Zone, as shown in the table below. Using the Private Zone means clients are not required to be authenticated before using the network services. On the other hand, clients in the Public Zone are required to get authentication before using the network services.

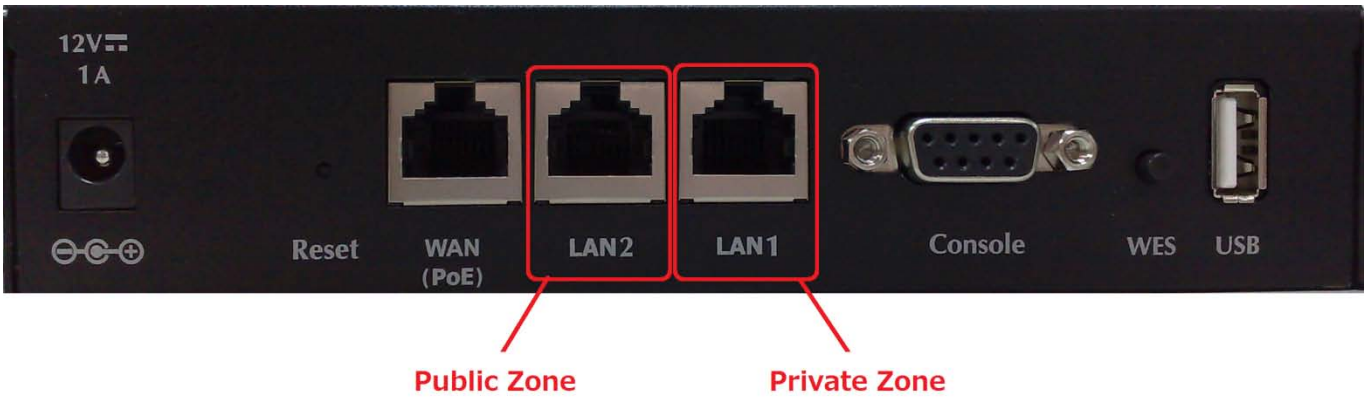
Zone Settings				
Name	**ESSID**	**Wireless Security**	**Default Authen Option**	**Details**
Private	NetComm_HS1100N_2	WPA-PSK	N/A	Configure
Public	NetComm_HS1100N	None	On-demand User	Configure

- **Name:** The mnemonic name of the Zone.
- **ESSID:** The SSID that is associated with the Zone.
- **Wireless Security:** Data encryption method for wireless networks within the Zone.
- **Default Authen Option:** Default authentication method/server that is used within the Zone.
- **Details:** Configurable, detailed settings for each Zone.

Click the ***Configure*** button to configure each Zone: **Basic Settings**, **Authentication Settings (Public Zone only)**, **Wireless Settings**, and **WDS Settings (Public Zone only)**.

3.5.1 Port Role Assignment

The Zone and Port mappings are shown below, LAN1 and LAN2 maps to Private Zone and Public Zone respectively.

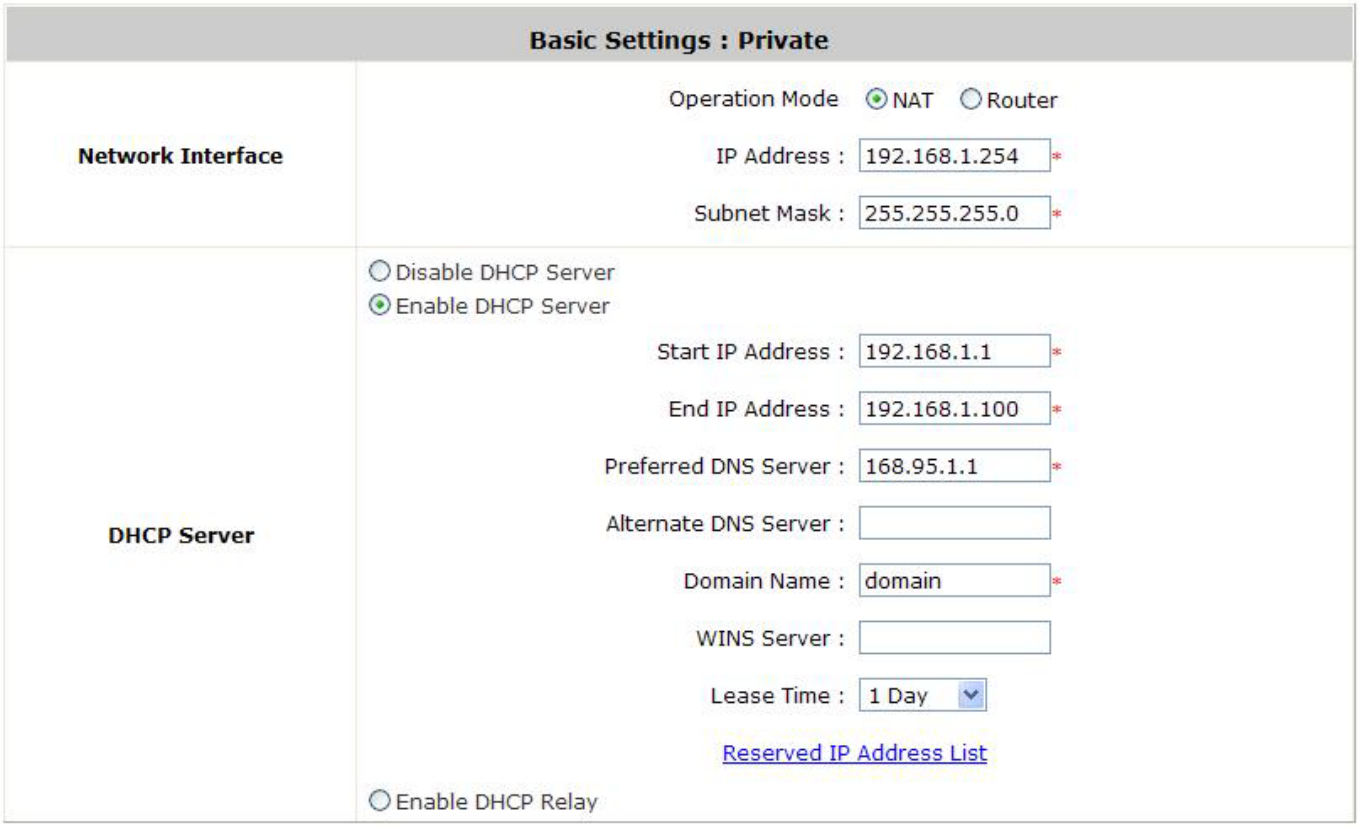


Note:

The system's WMI can also be accessed via the WAN port as long as the administrator uses an IP address listed in **Management IP Address List** setting. If both WAN and LAN ports are unable to reach WMI, please use the console interface to resolve this issue.

3.5.2 Configure the Zone Network

To configure the Zone network; go to: ***System >> Zone Configuration***. Click the ***Configure*** *button* of Private zone for further configuration. The parameter descriptions for the Basic Settings in the Private and Public Zones are the same. The wireless settings under each zone will be covered in the next section.



- **Network Interface:**
  - **Operation Mode:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, the service zone runs in NAT mode. When Router mode is chosen, this zone runs in Router mode.
  - **IP Address:** The IP Address of this zone.
  - **Subnet Mask:** The subnet Mask of this zone.
- **DHCP Server:** Related information needed on setting up the DHCP Server is listed here. Please note that when "*Enable DHCP Relay"* is enabled, the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this zone.
  - **Start IP Address / End IP Address:** A range of IP addresses that the built-in DHCP server will assign to clients.

    Note: Please remember to change the Management IP Address List accordingly (in the *System >> General >> Management IP Address List section of the WMI*) to permit the administrator to access the HS1100N admin page after the default IP address of the network interface is changed.
  - **Preferred DNS Server:** The primary DNS server that is used by this Zone.
  - **Alternate DNS Server:** The substitute DNS server that is used by this Zone.
  - **Domain Name:** Enter the domain name for this zone.

- **WINS Server:** The IP address of the WINS (Windows Internet Naming Service) server if WINS server is applicable to this zone.
- **Lease Time:** This is the period of time that the IP addresses issued from the DHCP server are valid and available.
- **Reserved IP Address List:** Each zone can reserve up to 40 IP addresses from a predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. The administrator can reserve a specific IP address for a special device with a certain MAC address.

4 Enabling the Wireless Network

4.1 General Wireless Settings

To configure the System's General Wireless Settings, go to: ***System >> Zone Configuration***.

Wireless General Settings	
Band	802.11g+802.11n
Short Preamble	Enable / Disable
Short Guard Interval	Enable / Disable
Channel Width	20 MHz
Channel	1
Max Transmit Rate	Auto
Transmit Power	Auto
DTIM Period	1 (1-255ms)
ACK Timeout	100 (0-255ms)

Wireless General Settings:

- **Band:** There are 4 modes to select, **802.11b** (2.4G, 1~11Mbps), **802.11g** (2.4G, 54Mbps), **802.11b+g**, and **802.11g+n**.
- **Short Preamble:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select **Enable** for **Short Preamble** or **Disable** for **Long Preamble**.
- **Short Guard Interval (802.11g+n only):** The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. With 802.11n, short guard interval is half of what it is used to be to increase throughput. Select *Enable* to use Short Guard Interval or *Disable* to use normal Guard Interval.
- **Channel Width (802.11g+n only):** For 802.11n, double channel bandwidth up to 40 MHz is supported to enhance throughput.
- **Channel:** Select the appropriate channel from the drop-down menu to correspond with your network settings, for example, Channel 1-11 is available in North American and Channel 1-13 in Europe, or choose the default *Auto*.
- **Max Transmit Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **Transmit Power:** Select from the range, or keep the default setting as applicable for your environment.
- **DTIM Period:** Enter the DTIM Interval that is generated within the periodic beacon at a specified frequency. A Higher DTIM interval will enable the wireless client to save power, but the throughput will be effected.

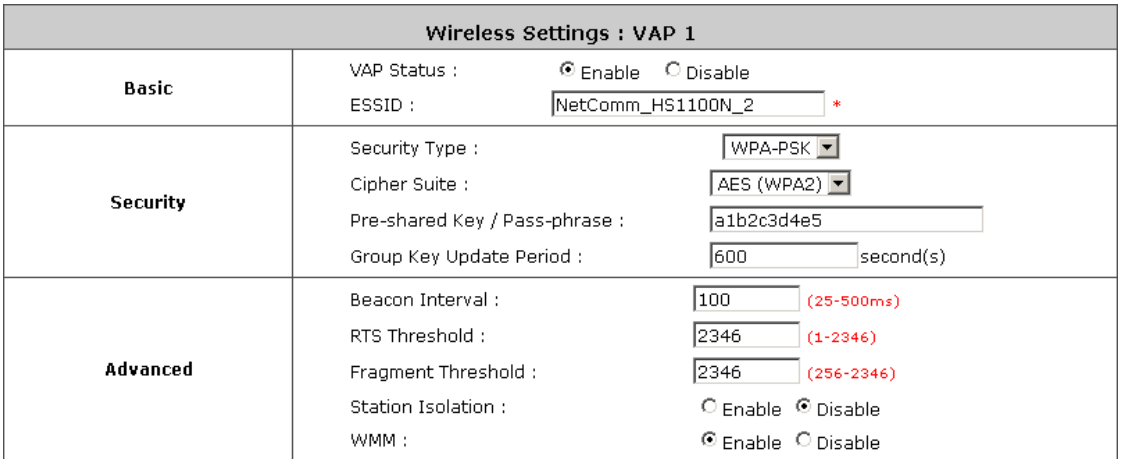
- **ACK Timeout:** The time interval for waiting the "**ACK**nowledgement frame". If the ACK is not received within that timeout period then the packet will be re-transmitted. Setting a higher ACK Timeout will decrease the packet loss, but the throughput will be effected.

4.2 Zone Wireless Settings

Each zone has its own VAP (Virtual Access Point) and this corresponds to one SSID. In the Private zone, it's VAP1 and the SSID is hidden, so public users cannot scan this SSID in the air, for privilege users who already know this SSID, they can manually associate to the SSID of Private zone. On the other hand, the SSID of VAP2 under Public zone by default is enabled with SSID Broadcast feature, allowing public users to scan this SSID in the air.

After the general wireless settings are done, use the parameters in the Wireless Settings under each zone to fine tune the wireless network configuration.

To configure the Private Zone's Wireless Settings, go to: ***System >> Zone Configuration***, click the **Configure** button for the Private zone



- **Wireless Settings: VAP1 (Wireless Settings Private Zone)**
  - **Basic:** Enable the VAP Status if you wish to provide wireless service under this zone. Assign an ESSID for VAP1 under the Private Zone or use default "HS1100N-1", the ESSID of the Private Zone will not be broadcasted and internal staff will need to associate to Private Zone's VAP1 manually.
  - **Security:** Configure the wireless network under Private Zone with security encryption to prevent unauthorized wireless association if necessary. The encryption standards supported are WEP and WPA-PSK.By default, WPA-PSK is selected for use.
  - **Advanced:** The parameters in advanced are wireless settings that allow customization of data transmission, enhanced security and wireless roaming.

    Beacon Interval: The entered amount of time indicates how often the beacon signal will be sent from the VAP.

    RTS Threshold: Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the frame to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the HS1100N or in areas where the clients are far apart and can detect only the HS1100N but not each other.

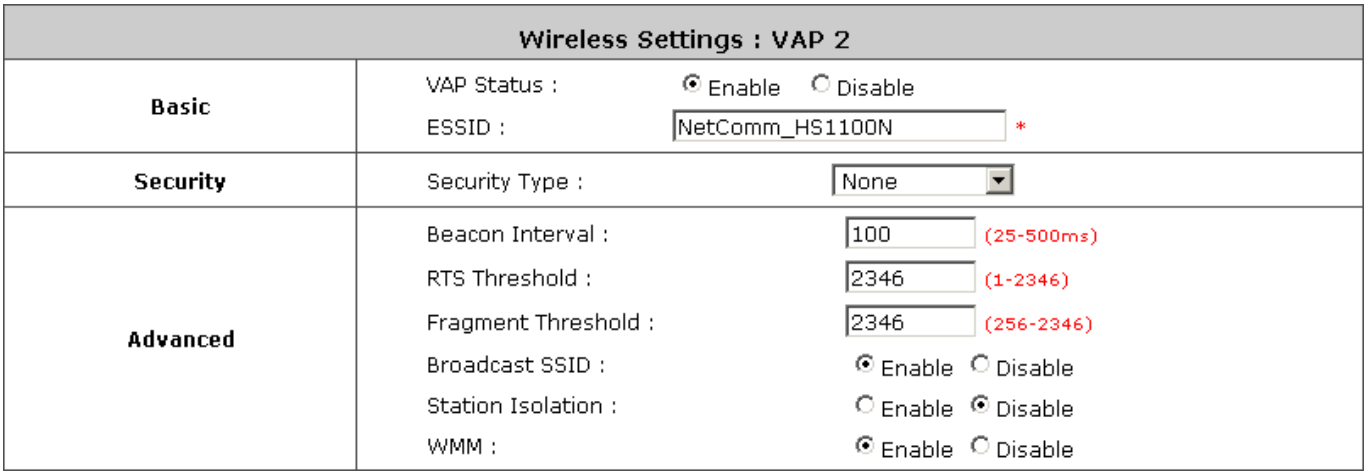
    Fragment Threshold: Enter a value between 256 and 2346. The default is 2346. A packet size

larger than this threshold will be fragmented (split into several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

Station Isolation: By enabling this function, all stations wirelessly associated to this zone are isolated from each other and can only communicate with the system.

WMM: The default is *Enable.* Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.

Normally we use VAP2, the VAP under Public Zone to provide wireless service to public clients in a hotspot environment. To configure the Public Zone's Wireless Settings, go to: ***System >> Zone Configuration***, click the **Configure** button for the Public zone



- **Wireless Settings: VAP2 (Wireless Settings for Public Zone)**
  - **Basic:** Enable the VAP Status if you wish to provide wireless service under this zone. Assign an ESSID for VAP2 under the Public Zone or use the default setting of "HS1100N-2", the ESSID of Public Zone will be broadcasted by default to allow it to be scanned in the air.
  - **Security:** Configure the wireless network under Public Zone with security encryption to prevent unauthorized wireless association if necessary. The encryption standards supported are WEP, 802.1X, WPA-PSK and WPA-RADIUS.
  - **Advanced:** The parameters in advanced are wireless settings that allow customization of data transmission, enhanced security and wireless roaming.

    Beacon Interval: The entered amount of time indicates how often the beacon signal will be sent from the VAP.

    RTS Threshold: Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the frame to prevent the hidden node problem. The RTS mechanism will be activated if the data size

exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the HS1100N or in areas where the clients are far apart and can detect only the HS1100N but not each other.

Fragment Threshold: Enter a value between 256 and 2346. The default is 2346. A packet size larger than this threshold will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

Broadcast SSID: Enable to broadcast VAP2's SSID in the air, Disable to hide VAP's SSID so that it cannot be scanned.

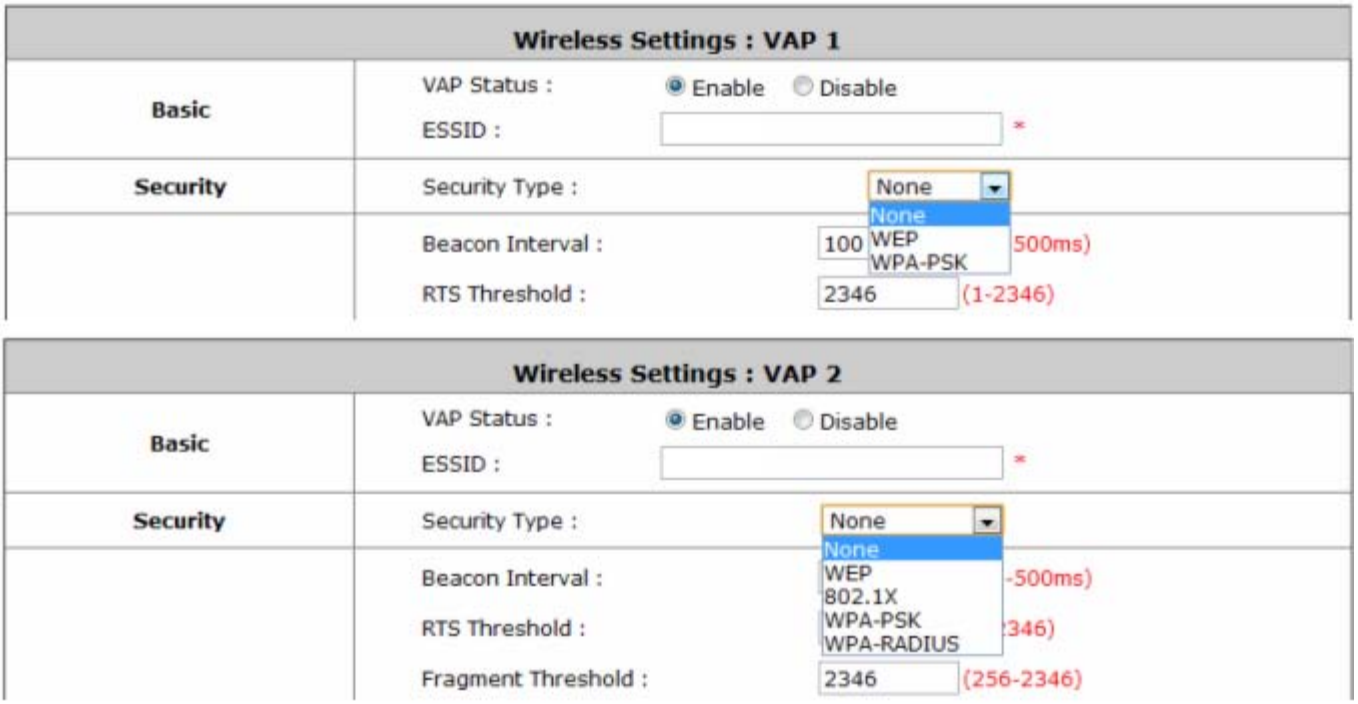
Station Isolation: By enabling this function, all stations wirelessly associated to this zone are isolated from each other and can only communicate with the system.

WMM: The default is *Enable.* Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.

4.3 Zone Wireless Security

To configure a Zones' Wireless Security, go to: ***System >> Zone Configuration***, click the ***Configure*** *button for the* Private zone or click the ***Configure*** *button* for the Public zone.

Please note: Ensure a wireless security key is set to protect your wireless network.



- **Security:**

For each zone, administrators can set up a different wireless security profile, it include **WEP**, **802.1x** (for **Public Zone** only), **WPA-PSK** or **WPA-RADIUS** (for **Public Zone** only).

- **WEP:**
  - **802.11 Authentication:** Select from **Open System** or **Shared Key**.
  - **WEP Key Length:** Select from **64-bit**, **128-bit**, **152-bit** key length.
  - **WEP Key Format:** Select from **ASCII** or **Hex** format for the WEP key.
  - **WEP Key Index:** Select a key index from **1~4**. The WEP key index is a number that specifies which WEP key will be used for the encryption of wireless frames during data transmission.
  - **WEP Keys:** Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.

- **802.1X:**
  - **Dynamic WEP:** For 802.1X security type, Dynamic WEP is always enabled to automatically generate WEP keys for encryption.
  - **WEP Key Length:** Select from **64-bit** or **128-bit** key length.
  - **Re-keying Period:** The time interval for the dynamic WEP key to be updated; the time unit specified is in seconds.
- **WPA-PSK:**
  - **Cipher Suite:** Select an encryption method from **TKIP (WPA)**, **AES (WPA)**, **TKIP (WAP2)**, **AES**

(WAP2), or **Mixed**.

- **Pre-shared Key / Passphrase:** Enter the key value for the pre-shared key or passphrase.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.

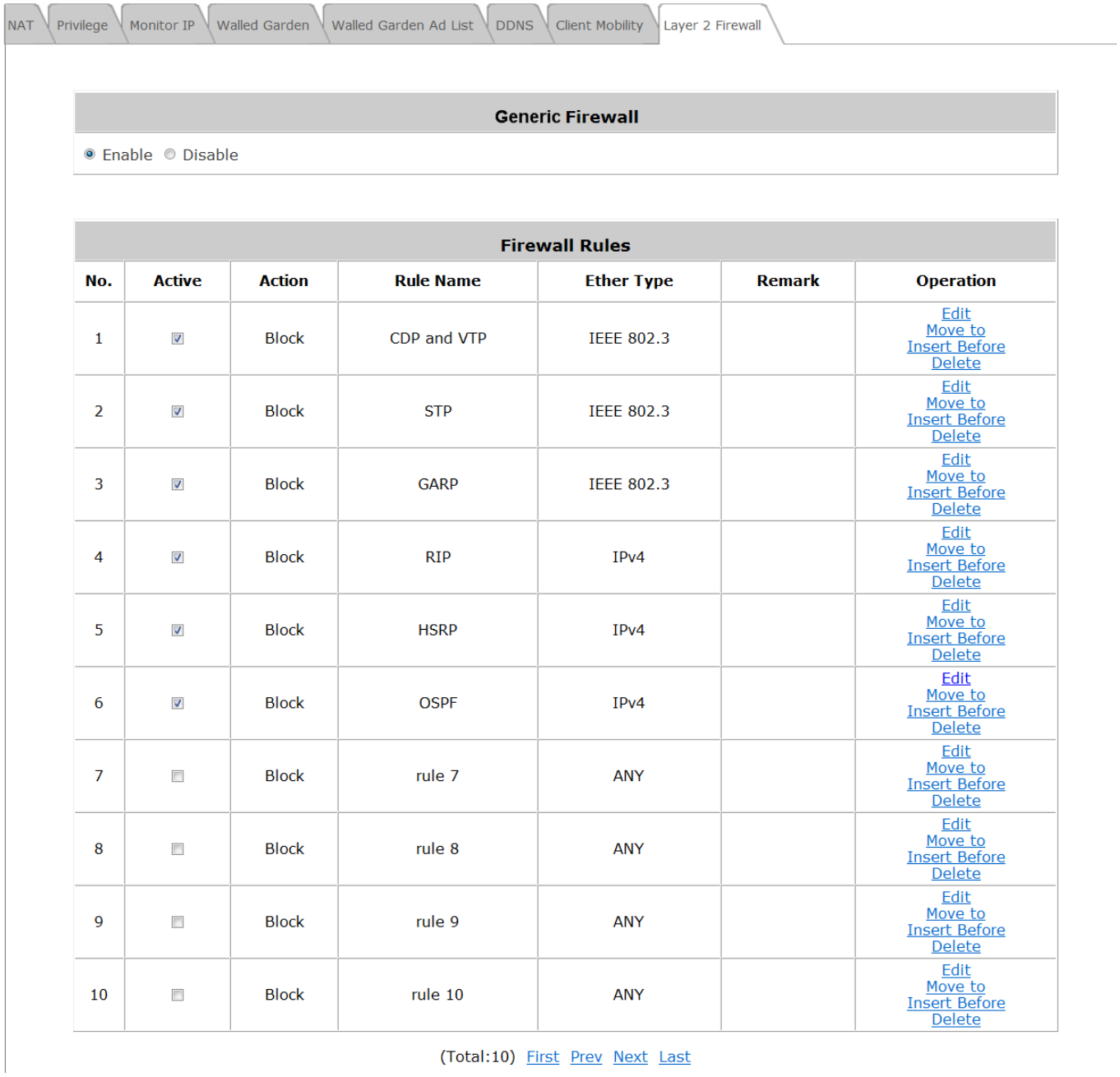
- **WPA-RADIUS:** Same as **802.1X**, when it is selected, it is combined with *TKIP*, *AES* or *Mixed* mode.
  - **Cipher Suite:** Select an encryption method from *TKIP (WPA)*, *AES (WPA)*, *TKIP(WAP2)*, *AES (WAP2)*, or *Mixed*.
  - **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.

4.4 Wireless Layer 2 firewall

The system provides an additional security feature, a Layer2 Firewall, in addition to standard wireless security. Layer2 Firewall offers a firewall function that is tailored specifically for Layer2 traffic, providing another choice of shield against possible security threats coming from/going to the WLAN (AP interfaces); hence, besides firewall policies configured in Policies, this extra security feature will assist to mitigate possible security breaches. This section provides information in the following functions: **Generic Firewall Rules**, **Predefined and Custom Service Protocols** and **Advanced**.

4.4.1 Generic Firewall Rules

You can choose to enable or disable the wireless Generic Firewall. This section provides an overview of firewall rules for the system's wireless interface; 6 default rules with up to a total of 20 firewall rules are available for configuration.

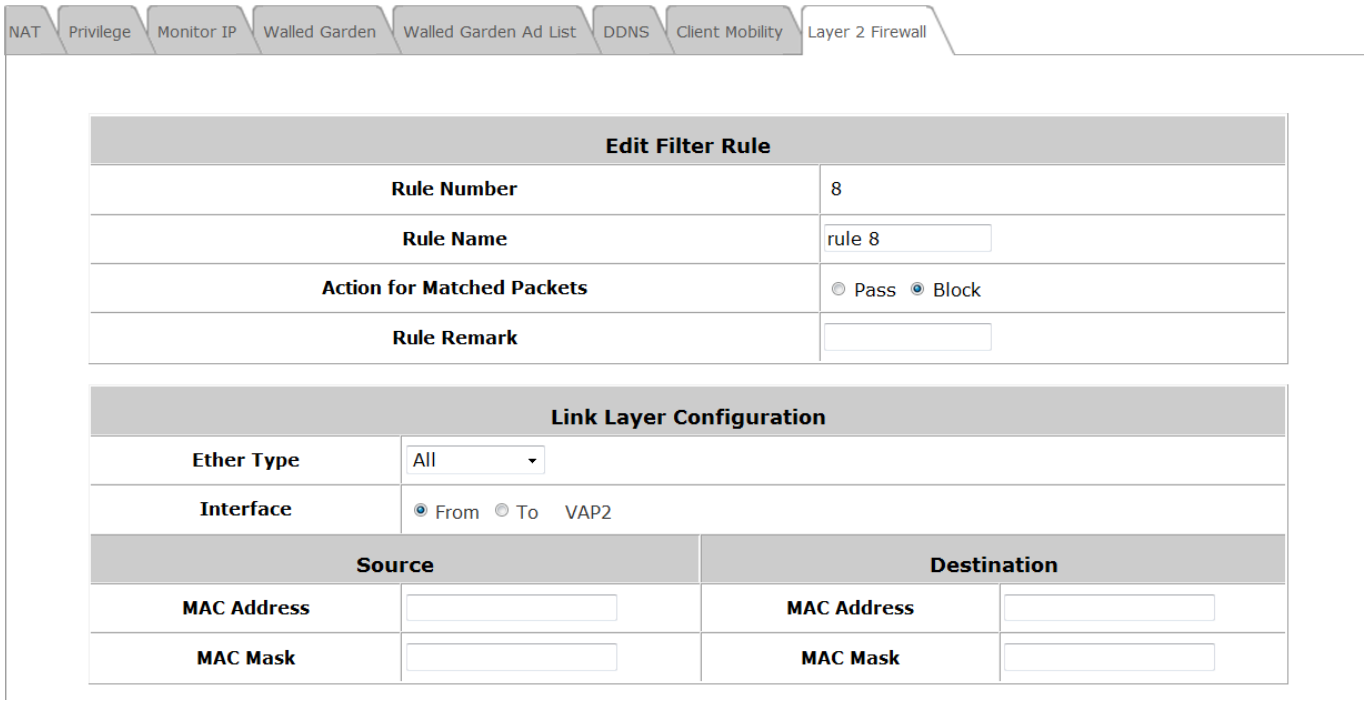


From the overview table, each rule is designated with the following field;

- **No.:** The numbering decides the priority of the firewall rules in the table.
- **Active:** Checking this field will mark the rule as active which means this rule will be enforced.
- **Action: Block** denotes a block rule; **PASS** denotes a pass rule.
- **Name:** This is the unique name of the rule.
- **EtherType:** It denotes the type of traffic subject to this rule.
- **Remark:** It shows the additional reference information of this rule.
- **Operation:** 4 actions are available; ***Edit*** denotes to edit the rule details, ***Move to*** denotes to move the rule to a specified rule number, ***Insert Before*** denotes to insert a rule before the current rule, and ***Delete*** denotes to delete the rule.

>>To edit a specific rule,

Clicking the ***Edit*** in the **Operation** column of firewall rules will lead to the following page for detailed configuration. From this page, an existing rule can be revised.



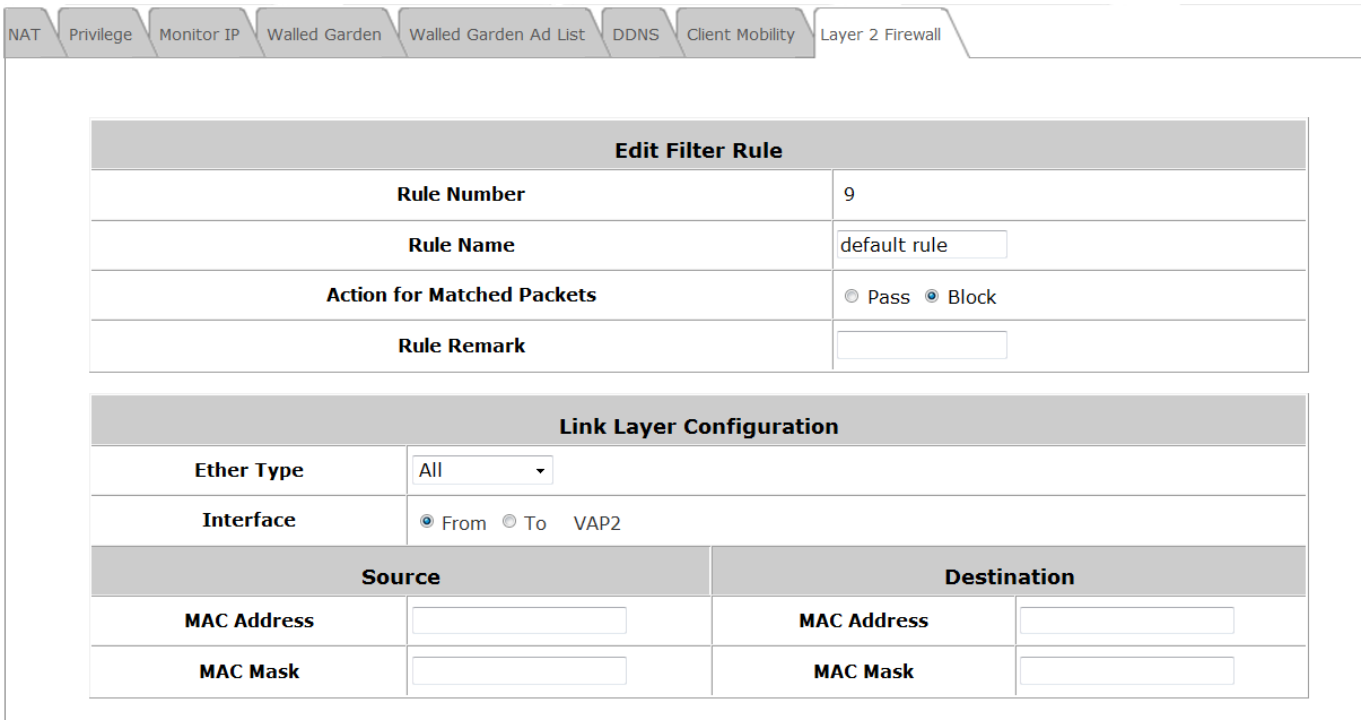
- **Rule Number:** The numbering of this specific rule will decide its priority among available firewall rules in the list.
- **Rule name:** The rule name can be specified here.
- **Action for Matched Packets:** The rule can be chosen to be **Block** or **Pass** packets that match the rule criteria.
- **Rule Remark:** The additional reference note of this rule can be specified here.
- **EtherType:** The drop-down list will provide the available types of traffics subject to this rule.
- **Interface:** For specifying the traffic direction (To or From VAP2) subjected to this rule.
- **IPv4 Service** (when EtherType is **IPv4**)**:** Select the available upper layer protocols/services from the drop-down list.

- **DSAP/SSAP** (when EtherType is **IEEE 802.3**)**:** The value can be further specified for the fields in an 802.2 LLC frame header.
- **SNAP Type** (when EtherType is **IEEE802.3**)**:** The field can be used to indicate the type of encapsulated traffic.
- **VLAN ID** (when EtherType is **VLAN**)**:** The VLAN ID is provided to associate with certain VLAN-tagging traffic.
- **VLAN Priority** (when EtherType is **VLAN**)**:** It denotes the priority level with associated VLAN traffics.
- **VLAN Type** (when EtherType is **VLAN**)**:** It can be used to indicate the type of encapsulated traffics.
- **Opcode** (when EtherType is **ARP/RARP**)**:** This list can be used to specify the ARP Opcode in an ARP header.
- **Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields (when EtherType is **ARP**).
- **Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields (when EtherType is **ARP**).

When you have finished configuring these settings, please click ***Apply*** to load the firewall rules.

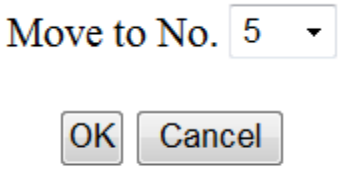
>>To insert a specific rule,

*The **Insert Before*** in the **Operation** column of firewall list will lead to the following page for detailed configuration of the rule ID for the rule currently being inserted.

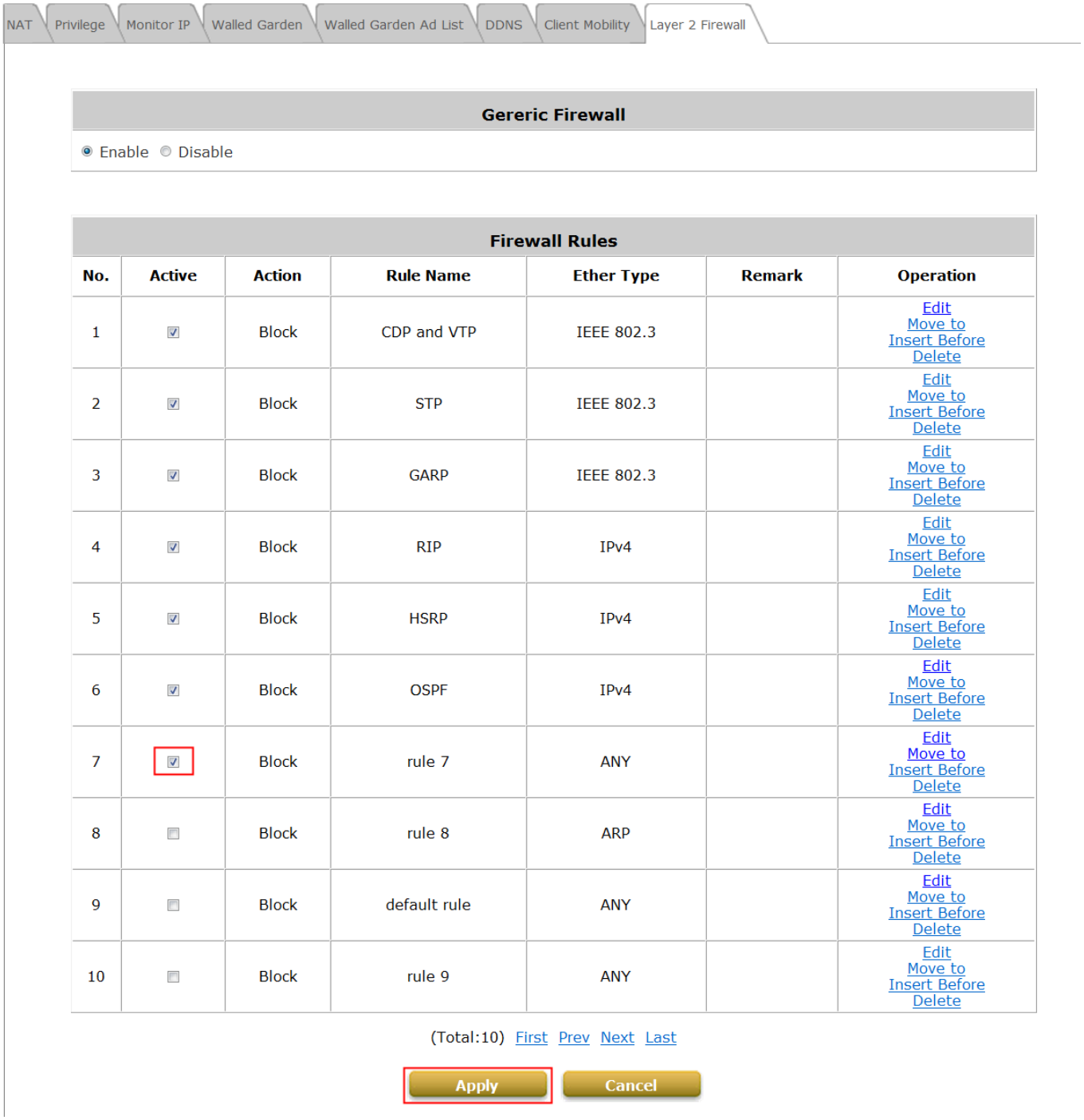


>>To move a specific rule,

The ***Move to*** in the **Operation** column of firewall rules will lead to the following page for reordering confirmation. Click ***OK*** to save the changes made.



Please make sure all desired rules are checked as Active and applied in the overview page.

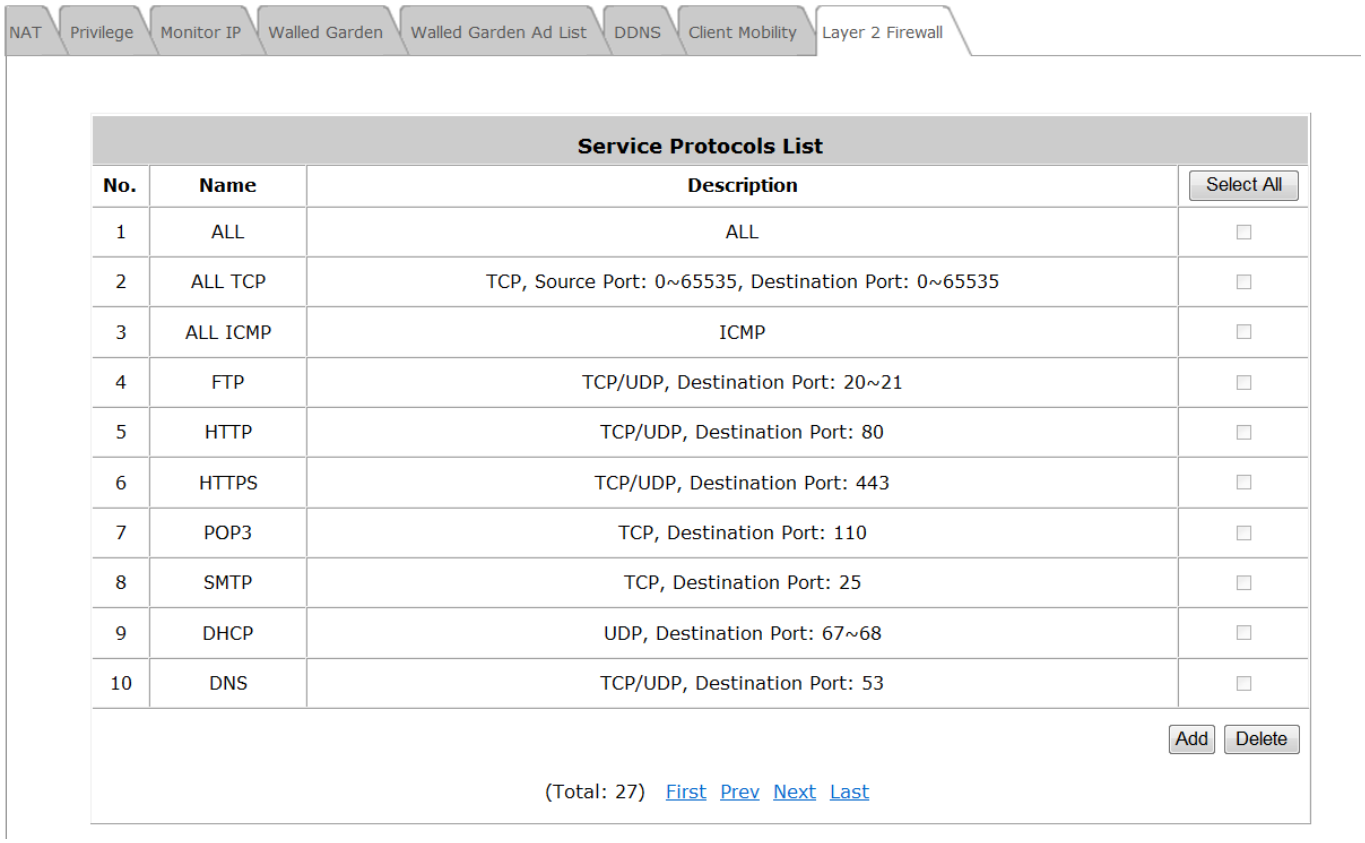


4.4.2 Predefined and Custom Service Protocols

The administrator can add or delete firewall service protocols here; the services in this list will become available drop-down options to choose from in firewall rule (when EtherType is IPv4).

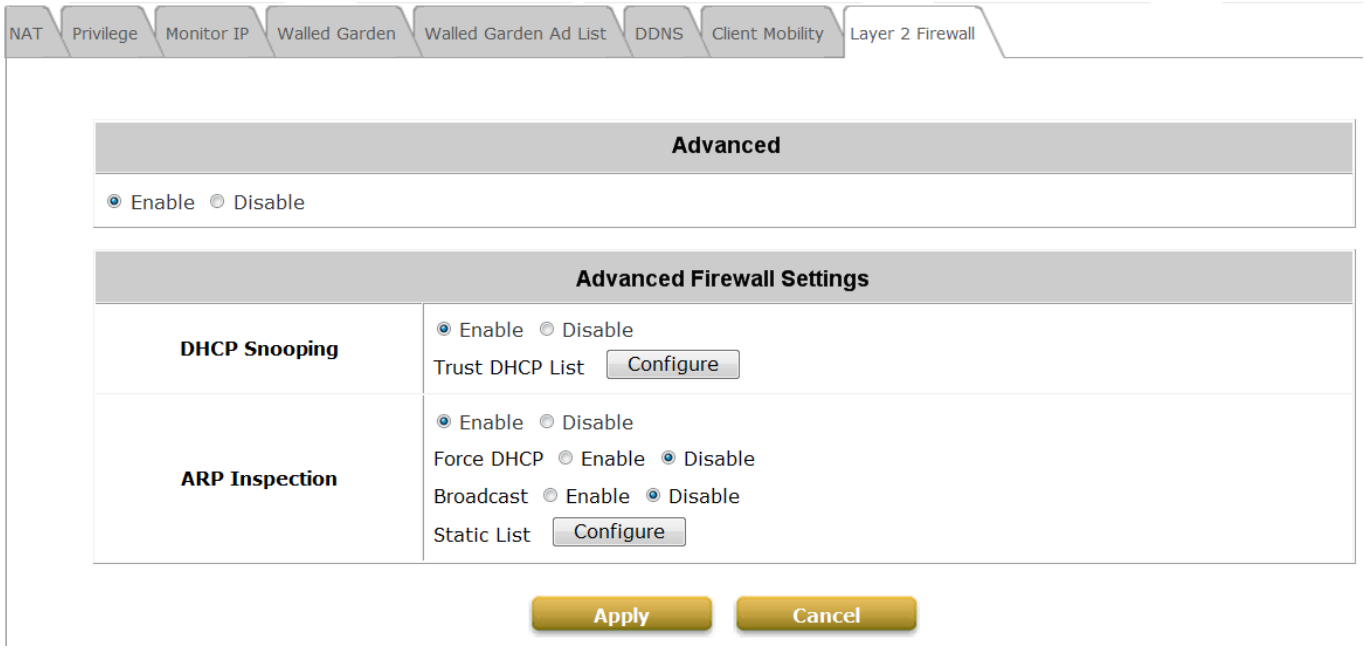
The first 27 entries are default services and the administrator can add any extra desired services.

The 27 default firewall services cannot be deleted but can be disabled.



4.4.3 Advanced

Advanced Firewall Settings can be enabled to supplement the firewall rules, providing extra security enhancement against DHCP and ARP traffics traversing the available interfaces of system.



- **DHCP Snooping**: When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack; in addition, the **Trust DHCP List** (IP/MAC) can be used to specify legitimate DHCP servers to prevent an unauthorised DHCP server.
- **ARP Inspection**: When enabled, ARP packets will be validated against ARP spoofing.
    - **Force DHCP** option when enabled, the AP only learns MAC/IP pair information through DHCP packets. Devices configured with static IP address does not accept DHCP traffic, therefore any clients with static IP address will be blocked from internet access unless its MAC/IP pair is listed and enabled on the **Static List.**
    - **Broadcast** can be enabled to let another AP (with L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests.
    - **Static List** can be used to add MAC or MAC/IP pairs of devices that are trusted to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears in the static list (with a different MAC), their ARP requests will be dropped to prevent eavesdropping.

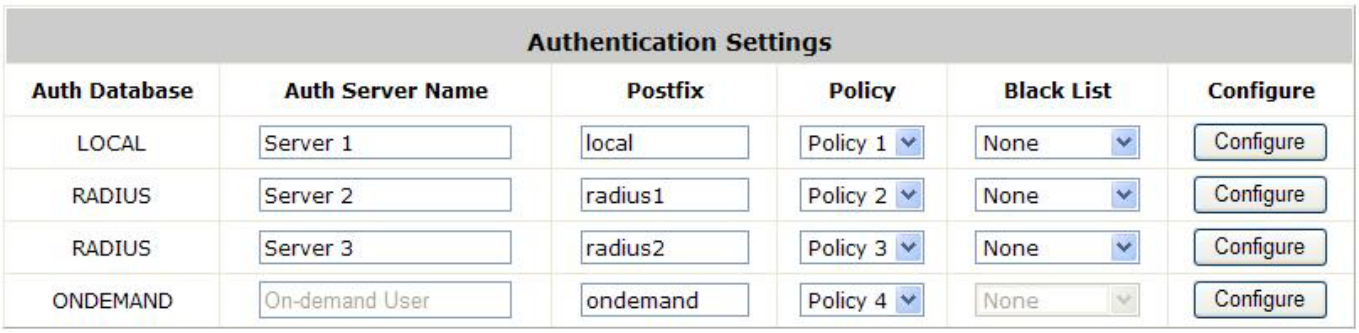
If any changes are made to the settings, please click ***Apply*** to save the new configuration before leaving this page.

5 Who Can Access the Network

5.1 Type of Users

To configure Users, go to: ***Users >> Authentication***.

This section is for administrators to pre-configure authentication servers for the entire system. Concurrently up to three servers can be selected and pre-configured for static user authentication, one server uses a built-in LOCAL database while the other two servers uses an external RADIUS database. In addition, another server called On-demand can be configured for temporary user authentication.



Authentication Settings					
Auth Database	**Auth Server Name**	**Postfix**	**Policy**	**Black List**	**Configure**
LOCAL	Server 1	local	Policy 1	None	Configure
RADIUS	Server 2	radius1	Policy 2	None	Configure
RADIUS	Server 3	radius2	Policy 3	None	Configure
ONDEMAND	On-demand User	ondemand	Policy 4	None	Configure

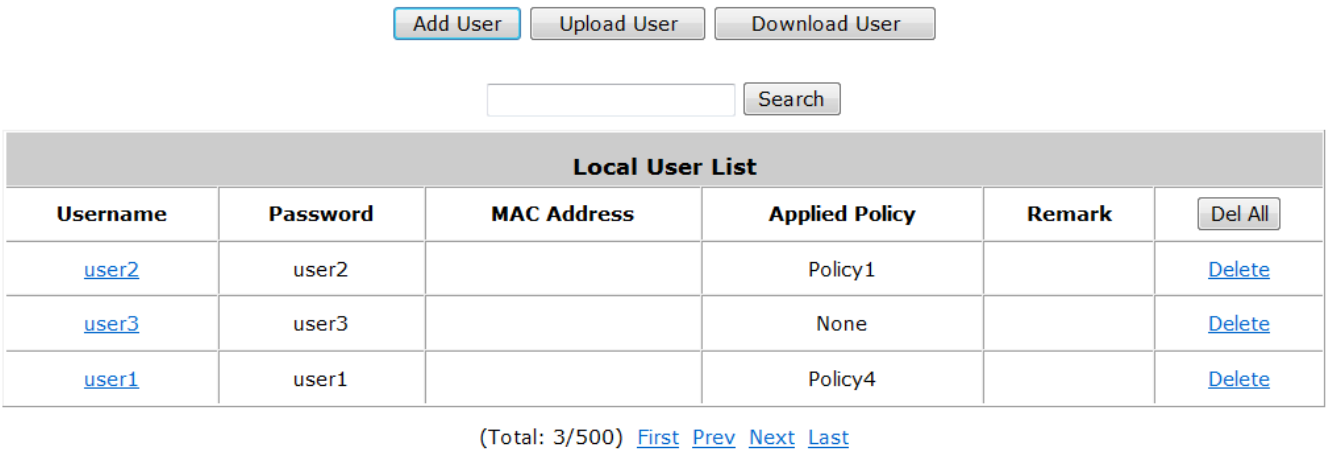
- **Auth Database:** There are four different authentication options in the HS1100N that uses databases: **LOCAL**, **RADIUS1**, **RADIUS2** and **ONDEMAND**.
- **Auth Server Name:** Set a name for the authentication databases by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_), space and dot (.) only. This name is used for the administrator to identify the authentication options easily such as HQ-RADIUS.
- **Postfix:** A postfix represents the authentication server in a complete username. For example, **user1@local** means that this user (user1) will be authenticated against the LOCAL authentication database.
- **Policy:** Select one Policy from the drop-down list box for this specific authentication option.
- **Black List:** There are 5 sets of black lists provided by the system. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one (or None) black list from the drop-down menu and this black list will be applied to this specific authentication option.
- **Configure:** Click ***Configure*** button to display the specific authentication page. For example, if you want to edit the *Local* authentication database, please click ***Configure*** button of **Local**.

5.1.1 Local

Click the ***Configure*** button in the **Local** section for further configuration options.

Local User Database Settings	
Local User List	
Account Roaming Out	○ Enable ◉ Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	○ Enable ◉ Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)

- **Local User List:** Lets the administrator view, add or delete a local user account. The ***Upload User*** button is for importing a list of user account from a text file. The ***Download User*** button is for exporting all local user accounts into a text file. Clicking on each user account leads to a page for configuring the individual local account.



Add User | Upload User | Download User

Search

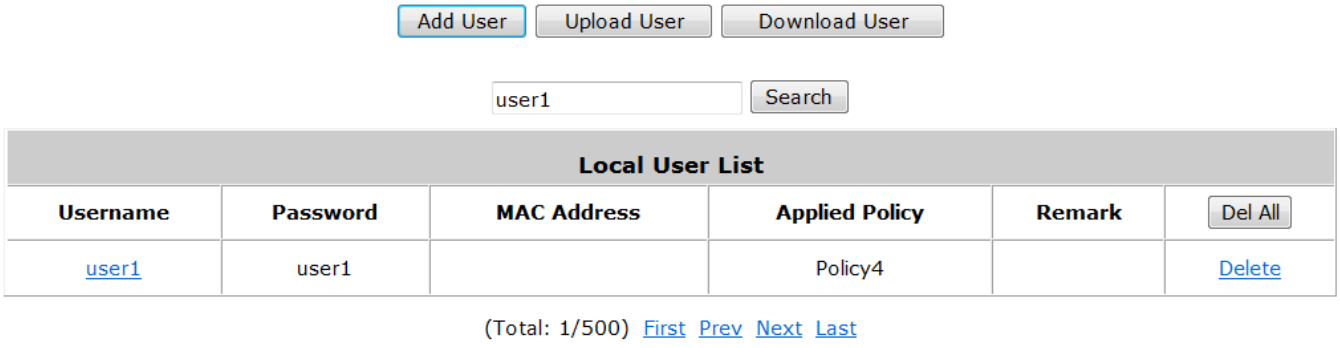
Local User List					
Username	**Password**	**MAC Address**	**Applied Policy**	**Remark**	Del All
user2	user2		Policy1		Delete
user3	user3		None		Delete
user1	user1		Policy4		Delete

(Total: 3/500) First Prev Next Last

Add User*:** Click this button to enter into the **Adding User(s) to the List** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC Address"**, and **"Remark"**. Select a desired **Policy** to classify local users. Click ***Apply to complete adding the user(s). The MAC address of a networking device can be bound with a local user as well. It means this user must login to system with a networking device (PC) that has the corresponding MAC address, so this user can not login with other networking devices.

Adding User(s) to the List					
No.	Username*	Password*	MAC Address (XX:XX:XX:XX:XX:XX)	Policy	Remark
1				None	
2				None	
3				None	
4				None	
5				None	
6				None	
7				None	
8				None	
9				None	
10				None	

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

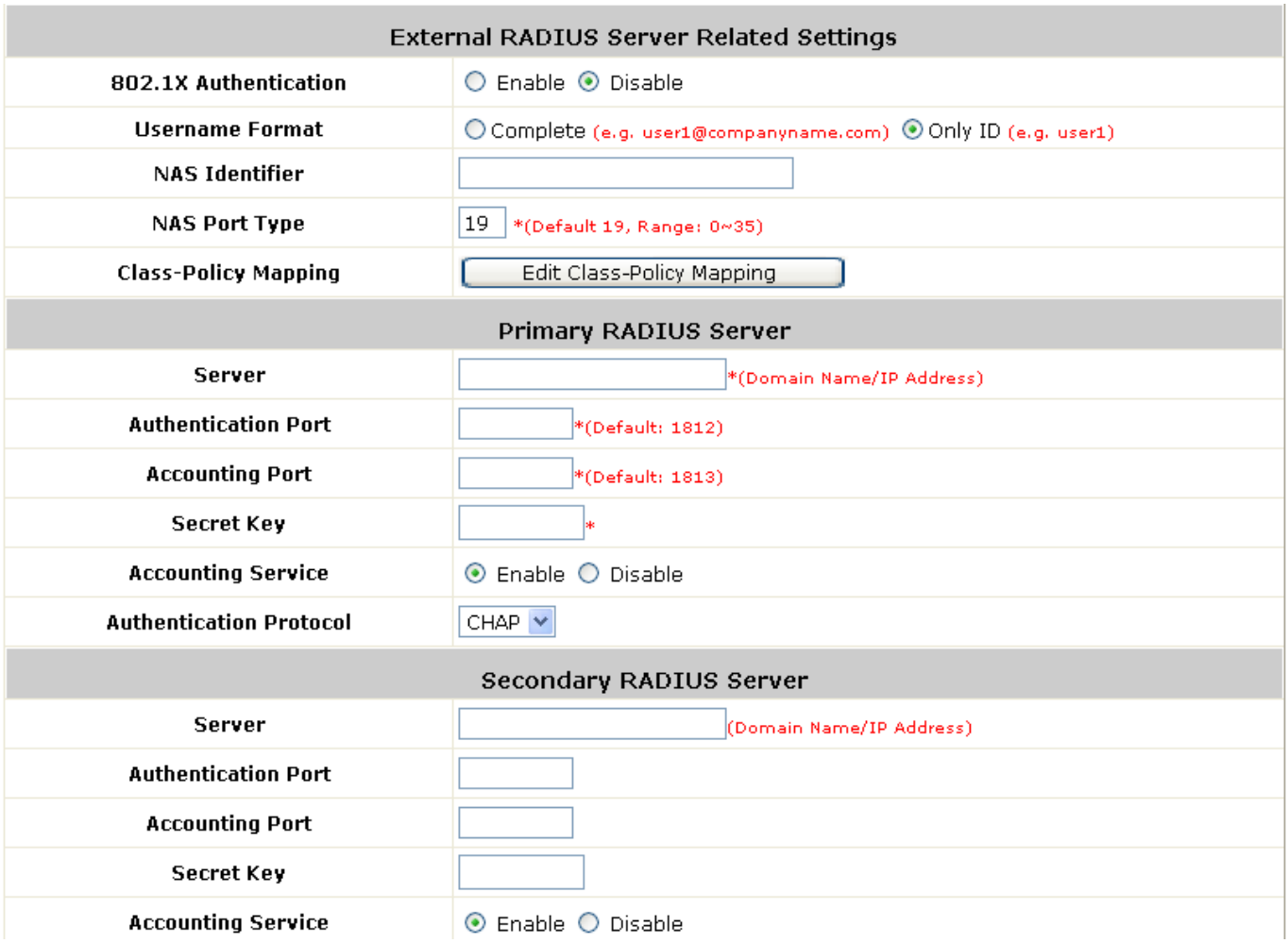


- ***Del All***: Click on this button to delete all the users at once or click on the ***Delete*** hyperlink to delete a specific user individually.

- **Edit User:** If editing the content of individual user account is needed, click the username of the desired user account in **Local User List** to enter the **User Profile** Interface for that particular user, and then modify or add any desired information such as *Username*, *Password*, *MAC Address* (optional), *Applied Policy* (optional) and *Remark* (optional). Click ***Apply*** to complete the modification.

5.1.2 RADIUS

There are two RADIUS authentication databases for configuration. Click the ***Configure*** button of any one of **RADIUS** servers for further configuration options. 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 mandatory). The fields with red asterisk are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.



➢ **External RADIUS Related Settings**

- **802.1X Authentication:** Enable /Disable 802.1X authentication for users authenticating through this Server.
- **Username Format:** Select the format which the user login information is sent to the external RADIUS Server. You may choose to send username in **Complete** (userID + Postfix), **Only ID** or **Leave Unmodified**.

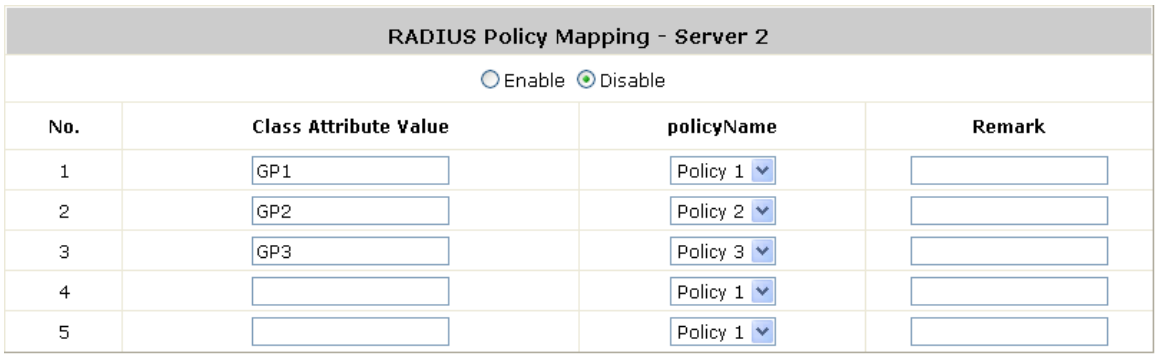
Please note: If the Leave Unmodified option is selected, the system will send the username to the **Default Auth Server** set in the **802.1X** configuration page for authentication.

- **NAS Identifier:** This attribute is the string identifying the NAS originating the access request. The

System will send this value to the external RADIUS server, if the external RADIUS server is configured to need this.

- **NAS Port Type:** Indicates the type of physical port the network access server is using to authenticate the user. System will send this value to the external RADIUS server, if the external RADIUS server is configured to need this.

- **Class-Policy Mapping:** This function is to assign a Policy to a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes logs into the system via the RADIUS server, each client will be mapped to an assigned Policy.



➢ **Primary / Secondary RADIUS Server**

- **Server:** Enter the domain name or IP address of your RADIUS Server.
- **Authentication Port:** Enter the Port number used for authentication.
- **Accounting Port:** Enter the Port number used for accounting.
- **Secret Key:** Secret Key used for authentication.
- **Accounting Service:** Enable / Disable RADIUS accounting.
- **Authentication Protocol:** Select Challenge-Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).

5.1.3 On-Demand Users

On-demand User Server Configuration: The administrator can 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 and external payment gateway support.

Authentication Server - On-demand User		
General Settings	WLAN ESSID	NetComm_HS1100N
	Wireless Key	
	Currency	None $ USD £ GBP € EUR (Input other desired currency, e.g. AU)
	Remaining Reminder	Time: Enable Disable Volume: Enable Disable
	Sync Interval	10min(s) 15min(s) 20min(s)
Ticket Customization		Configure
Billing Plans		Configure
External Payment Gateway		Configure
Terminal Server		Configure
On-demand Account Creation		Create
On-demand Account Batch Creation		Create
On-demand Account List		View

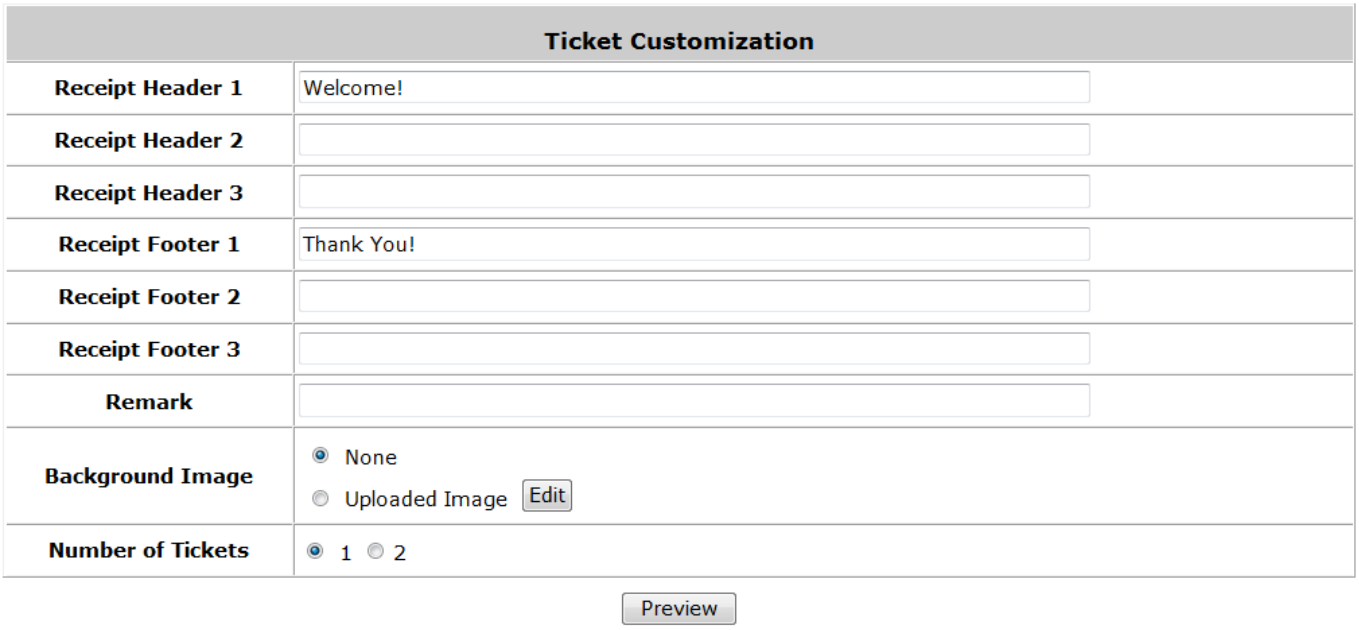
1) General Settings

These are the common settings for the On-demand User authentication option.

- **WLAN ESSID:** It will show the ESSID of Public Zone.
- **Wireless Key:** It will show the wireless key that was configured in Public Zone settings.
- **Currency:** Select the desired currency unit for charged internet access.
- **Remaining Reminder:** Enable it and input the count-down minute, system will remind users that their quota will run out soon when their quota reaches this time. The remaining message will not show up if the Remaining Reminder time is configured longer than the quota of billing plans.
- **Sync Interval:** Select the desired interval for on-demand user quota update. The quota information, i.e. remaining time or remaining quota displayed on the on-demand user login success page will be refreshed according to the time interval configured here.

2) Ticket Customization

The On-demand account ticket can be customized here and previewed on the screen.



- **Receipt Header:** There are 3 receipt headers supported by the system. The entered content will be printed on the receipt. These headers are optional.
- **Receipt Footer:** There are 3 receipt footers supported by the system. The entered content will be printed on the receipt. These footers are optional.
- **Remark:** Enter any additional information that will appear at the bottom of the receipt.
- **Background Image:** You can choose to customize the ticket by uploading your own background image for the ticket, or choose none. Click **Edit** to select the image file and then click **Upload**. The background image file size limit is 100 Kbytes. No limit for the dimensions of the image is set, but a 460x480 image is recommended.
- **Number of Tickets:** Enable this function to print duplicate receipts. Another Remark field will appear when the Number of Ticket is selected to 2 and the content will appear at the bottom of the 2nd duplicate receipt.
- **Preview:** Click ***Preview*** button, the ticket will be shown including the username and password information with the selected background. You can also print the ticket here.

3) Billing Plans

Administrators can configure several billing plans. Click ***Edit*** button to enter the page of **Editing Billing Plan**. Configure billing plans with desired account type, expiration date, price, etc. Click ***Apply*** to save the plan. Go back to the screen of **Billing Plans**, check the ***Enable*** checkbox or click **Select all** button, and then click **Apply.** The plan(s) will then be activated.

Billing Plans					
Plan	**Account Type**	**Quota**	**Price**	**Enable**	**Function**
1	Usage-time	15 min(s) connection time quota with expiration	10.91	☑	Edit
2	Usage-time	11 min(s) connection time quota	1	☑	Edit
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	☑	Edit
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	☑	Edit
5	N/A			☐	Edit
6	N/A			☐	Edit
7	N/A			☐	Edit
8	N/A			☐	Edit
9	N/A			☐	Edit
0	N/A			☐	Edit

- **Plan:** The number of the specific plan.
- **Type:** This is the type of the plan which defines how the account can be used including Usage-time, Volume, Hotel Cut-off and Duration-time.
- **Quota:** The limit on how On-demand users are allowed to access the network.
- **Price:** The unit price charged for buying an account from this billing plan.
- **Enable:** Check the checkbox to activate the plan.
- **Function:** Click the button ***Edit*** to add one billing plan. For detailed information regarding on-demand accounts and billing plan configuration, please refer to ***Appendix E, On-demand Account types & Billing Plan***.

4) External Payment Gateway

This section is for merchants to set up an external payment gateway to accept payments in order to provide wireless access services to end customers who wish to pay for the service on-line.

The options are **Authorize.Net**, **PayPal**, **SecurePay**, **WorldPay** or **Disable**. For detailed parameter descriptions please refer to ***Appendix F, External Payment Gateways.***

External Payment Gateway				
○ Authorize.Net	○ PayPal	○ SecurePay	○ WorldPay	◉ Disable

5) Terminal Server

Terminal Server Configuration is a list of serial-to-Ethernet devices that communicate with the system only; they never go online and have no need to go through the authentication process. Enter the device IP into server IP field.

Please note: The SDS-AG1100 (Smart Device Server) is the terminal server device used to connect the PRT-AG1100 POS Network Ticket printer to the HS1100N in order to generate tickets.

Terminal Server Configuration				
Item	Server IP	Port	Location	Remark
1				

6) On-demand Account Creation

After at least one billing plan is enabled, the administrator can generate single on-demand user accounts here. Click this to enter the On-demand Account Creation page. Click on the ***Create*** button of the desired plan to create an on-demand account. The username and password to be created by an on-demand account is configurable. Select ***Manual created*** in Username/Password Creation and then administrator can enter desired username and password for the on-demand account. In addition, an External ID (such as a student's school ID) can be entered together with account creation.

After the account is created, you can click ***Printout*** to print a receipt which will contain the on-demand user's information, including the username and password to a network printer. Alternatively, you can click ***Send to POS*** to print a receipt by a POS device.

Note:

If no Billing plan is enabled, accounts cannot be created by clicking ***Create*** button. Please go back to Billing Plans to activate at least one Billing plan by clicking ***Edit*** button and ***Apply*** the setting to activate the plan. The printer used by ***Print*** is a pre-configured printer connected to the administrator's computer.

On-demand Account Creation					
Plan	**Account Type**	**Quota**	**Price**	**Status**	**Function**
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create
5	N/A	N/A	N/A	Disabled	Create
6	N/A	N/A	N/A	Disabled	Create
7	N/A	N/A	N/A	Disabled	Create
8	N/A	N/A	N/A	Disabled	Create
9	N/A	N/A	N/A	Disabled	Create
0	N/A	N/A	N/A	Disabled	Create

- **Plan:** The number of a specific plan.
- **Account Type:** Show account type of the plan in Usage-time. Duration-time or Hotel Cut-off.
- **Quota:** The total amount of time or period of time that On-demand users are allowed to access the network. For Time users, it is the total time. For Volume users, it is the total amount of traffic.
- **Price:** For each plan, this is the unit price charged for an account.

- **Status:** Show the status in enabled or disabled.
- **Function:** Press ***Create*** button for the desired plan and the Creating an On-demand Account page will appear.

On-demand Account Creation

Plan	Account Type	Quota	Price	Status	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create

Creating an On-demand Account

Plan : Account Type	2 : Usage-time
Quota	11 min(s) connection time quota
Username/Password Creation	System created
Account Activation	First time login must be done within 1 hour(s)
Total Price	1
Reference	this is a ref Add a reference related to this account (for example, the customer's name)
External ID	Enter an external ID such as Library ID No.
Please confirm the information and press Create button to create an account.	

Create Cancel

7) **On-demand Account Batch Creation**

After at least one billing plan is enabled, the administrator can generate multiple on-demand user accounts at once with batch creation. Click ***Create*** button to enter the On-demand Account Batch Creation. Enter the desired number of accounts of enabled plans to create a batch of on-demand accounts together. The Number of Accounts field of disabled plans will not be able to enter any number. The sum of all Number of Accounts will be constrained and will not accept a number over the available account limits in database. Click ***Create*** button to start batch creation. Next page will show Success or Failed message to indicate the batch creation status. Once creation is successful, all created accounts can be exported to a text file for extended usage. Moreover, you can click ***Send to POS*** to print a receipt to a POS device via Serial or Ethernet network.

Please note: It can take some time if you create lots of on-demand accounts by a batch creation.

On-demand Account Batch Creation				
Plan	**Account Type**	**Quota**	**Price**	**Number of Accounts**
1	Usage-time	15 min(s) connection time quota with expiration	10.91	
2	Usage-time	11 min(s) connection time quota	1	
3	Hotel Cut-off	Valid until 12:00 the following day	5	
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	
5	N/A			
6	N/A			
7	N/A			
8	N/A			
9	N/A			
0	N/A			

- **Plan:** The number of a specific plan.
- **Account Type:** Show account type of the plan in Usage-time, Duration-time or Hotel Cut-off.
- **Quota:** The total time amount, interval or traffic volume on how On-demand users are allowed to access the network.
- **Price:** For each plan, this is the unit price charged for an account.
- **Number of Accounts:** The desired number of accounts to be created from the plan.

8) On-demand Account List

All created On-demand accounts are listed and related information on is also provided.

Search

Upload User | Download User

On-demand Account List						
Username	**Password**	**Remaining Quota**	**Status**	**External ID**	**Reference**	Delete All
7k3t	g3x5fum4	11 min(s)	Normal		New York branch	Delete
gcz9	6ey68m44	Until 2010/06/16-12:30	Normal		Boston Branch	Delete

(Total:2) First Prev Next Last

- **Search:** Enter a keyword of a username, External ID, or reference, to be searched in the text filed and click this button to perform the search. All usernames, External ID, or reference, matching the keyword will be listed.
- **Username:** The login name of the account.
- **Password:** The login password of the account.
- **Remaining Quota:** The remaining time or volume, or the cut-off time that the account can continue to use to access the network.

- **Status:** The status of the account.
  - **Normal:** the account is not currently in use and has not exceeded the quota limit.
  - **Online:** the account is currently in use.
  - **Expired:** the account is not valid any more, even if there is remaining quota left.
  - **Out of Quota:** the account has exceeded the quota limit.
  - **Redeemed:** the account has applied for an account renewal.
- **External ID:** This is an additional information field for combined with a unique account only, for example the customer's name or social security number etc.
- **Reference:** Any other additional information, for example venue where the account is generated etc.
- **Delete All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

9) Redeem On-demand Accounts

For Usage-time accounts, when the remaining quota is insufficient or if they are almost out of quota, they can use redeem function to extend their quota. After the user has got, or bought a new account, they just need to click the **Redeem** button in the login success page to enter Redeem Page, input the new account **Username** and **Password** and then click **Submit**. This new account's quota will be extended to the original account. However, the Redeem function can only be used with an account of the same billing type, i.e. Volume accounts can only be redeemed with another Volume account and so on.

Note:

The maximum quota is 365dys 23hrs 59mins 59secs even after redeem. If the redeem amount exceeds this number, the system will automatically reject the redeem process.

Note:

Duration-time and Hotel Cut-off type do not support the redeem function.

5.2 User Login

5.2.1 Default Authentication

There are different types of authentication database (LOCAL, RADIUS and ONDEMAND) that are supported by the system. Only the Public Zone can set authentication.
A postfix is used to inform the system which authentication option is to be used for authenticating an account (e.g. Bob@local or Tim@radius1 etc.) when multiple options are concurrently in use. One of the authentication options can be assigned as default. For the default authentication assigned, the postfix can be omitted. For example, if "local" is the postfix of the default option, then user with username Bob can login as "Bob" without having to type in "Bob@local".

Authentication Settings					
Authentication Required For the Zone	◉ Enable ○ Disable				
Authentication Options	**Auth Server**	**Auth Database**	**Postfix**	**Default**	**Enabled**
	Server 1	LOCAL	local	◉	☑
	Server 2	RADIUS	radius1	○	☑
	Server 3	RADIUS	radius2	○	☑
	On-demand User	ONDEMAND	ondemand	○	☑

5.2.2 Login with Postfix

For each authentication option, set a postfix that is easy to distinguish (e.g. Local) user login with the appropriate authentication server. The acceptable characters are numbers (0~9), alphabet (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. No other characters are allowed.

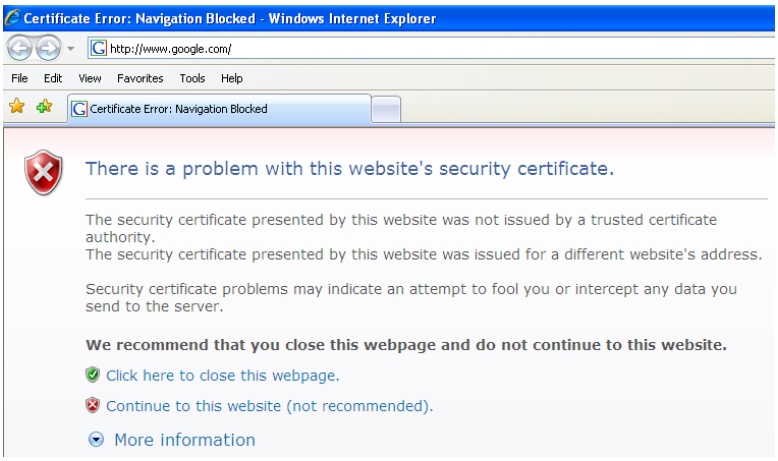
Beside the Default Authentication, all other authentication server users logging into to system, the username must contain the postfix to identify the authentication option this user belongs to.

Authentication Settings					
Auth Database	**Auth Server Name**	**Postfix**	**Policy**	**Black List**	**Configure**
LOCAL	Server 1	local	Policy 1	None	Configure
RADIUS	Server 2	radius1	Policy 2	None	Configure
RADIUS	Server 3	radius2	Policy 3	None	Configure
ONDEMAND	On-demand User	ondemand	Policy 4	None	Configure

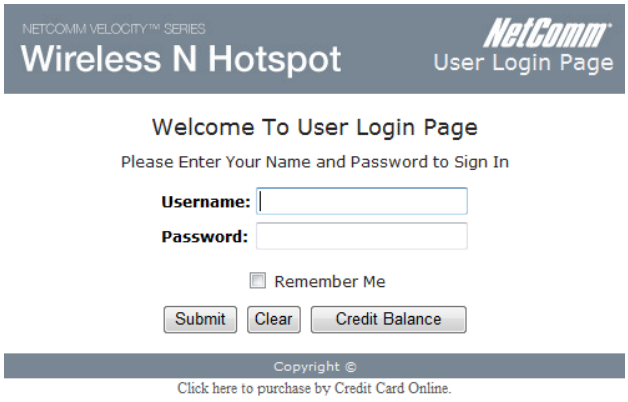
5.2.3 An Example of User Login

Normally, users will be authenticated before they get network access through the HS1100N. This section presents the basic authentication flow for end users. Please make sure that the HS1100N is configured properly and that the network related settings are done.

1. Connect a client PC to Public Zone of The HS1100N. Open an Internet browser and try to connect to any website (in this example, we try to connect to www.google.com).
   a) For the first time, if the HS1100N is not using a trusted SSL certificate, there will be a “Certificate Error”, because the browser treats the HS1100N as an illegal website.

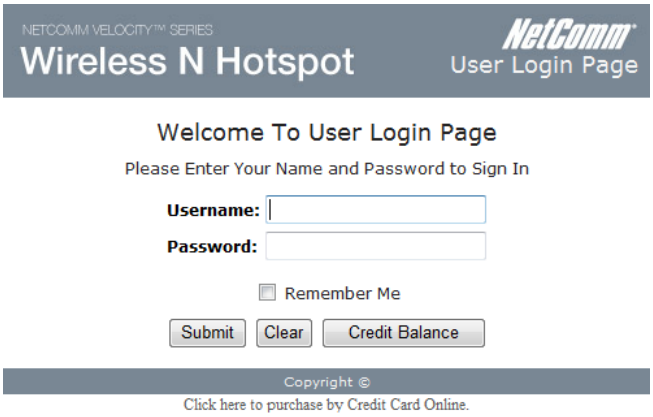


   b) Please press “Continue to this website” to continue.
   c) The default user login page will appear in the browser.

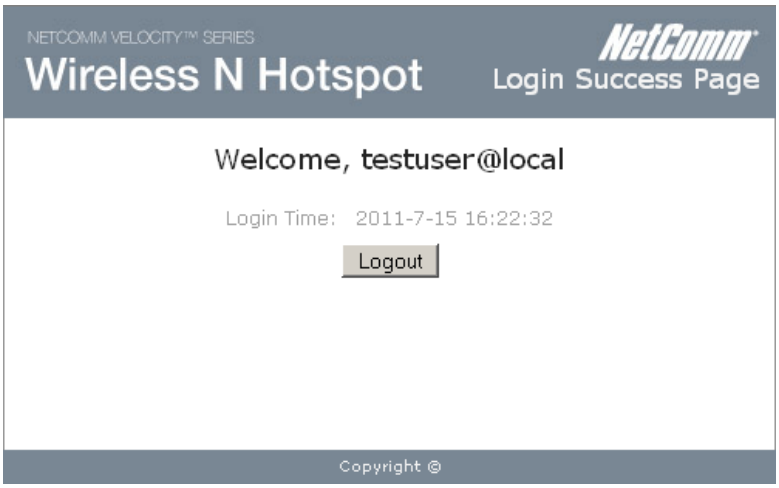


2. Enter the username and password (for example, we use a local user account: **test@local** here) and then click ***Submit*** button. If the ***Remember Me*** check box is checked, the browser will store the username and password on the current computer in order to automatically login to the system at the next login. Then, click the ***Submit*** button.

   The ***Credit Balance*** button on the **User Login Page** is for on-demand users only, they can check their Remaining quota here.



3. Successful! The **Login Success Page** means you are now connected to the network and Internet!

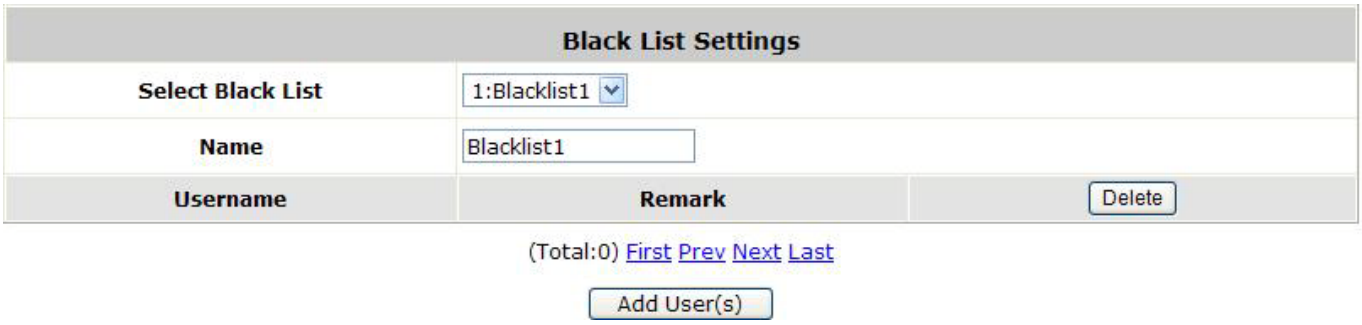


6 Restrain the Users

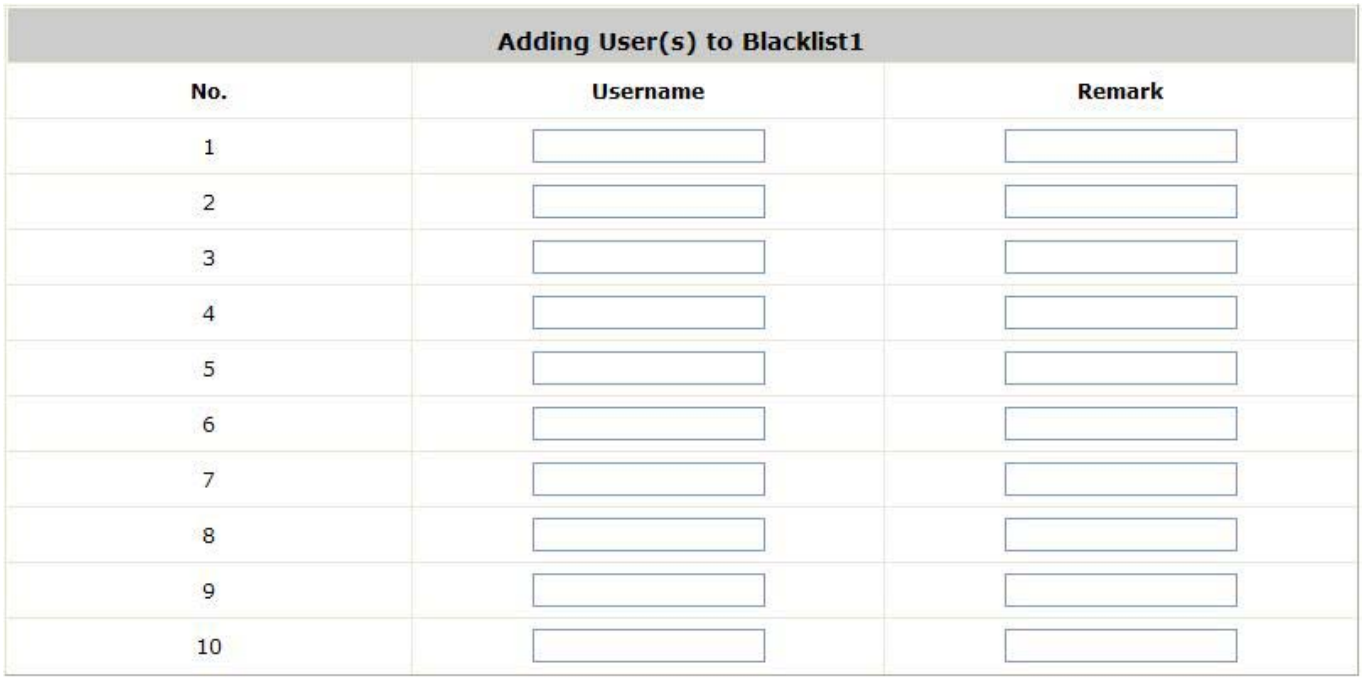
6.1 Black List

To configure Black Lists, go to: ***Users >> Black List***.

The administrator can add, delete, or edit the black list for user access control. Users' accounts that appear in the black list will be denied network access. The administrator can use the pull-down menu to select the desired black list.

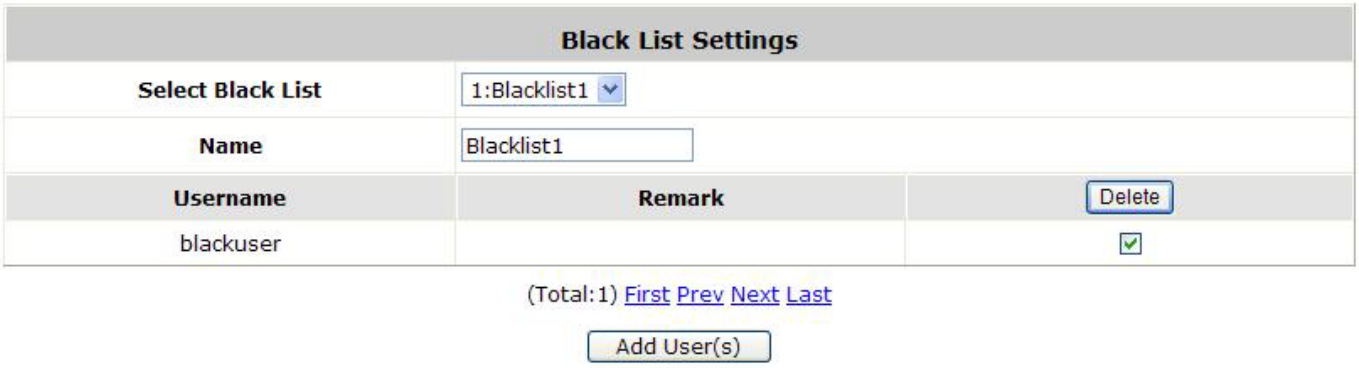


- **Select Black List:** There are 5 black list profiles available for utilization.
- **Name:** Set the black list name and it will show on the pull-down menu above.
- **Add User(s):** Click the ***Add User(s)*** button to add users to the selected black list.

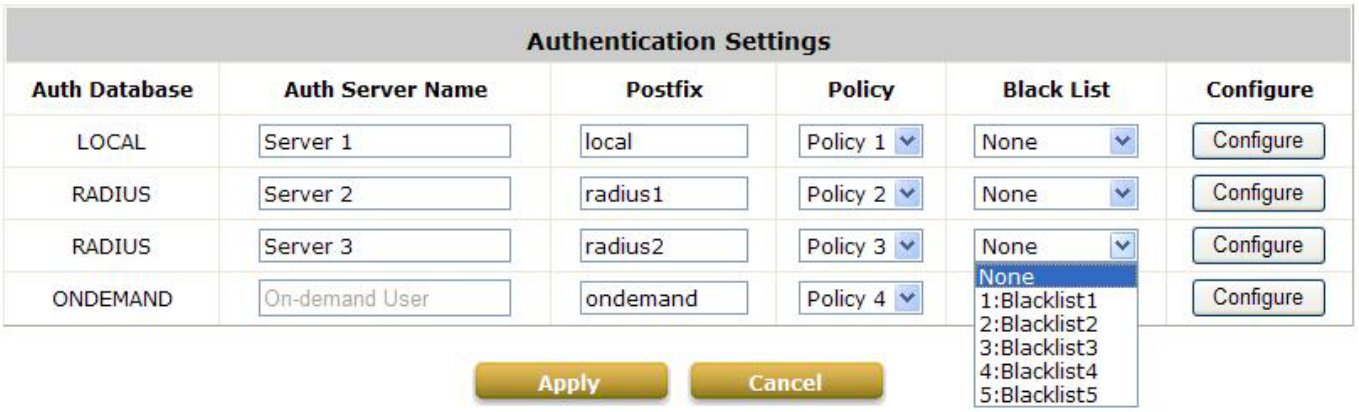


After entering the usernames in the **"Username"** field and the related information in the **"Remark"** blank (not required), click ***Apply*** to add the users.

If removing a user from the black list is desired, select the user's **"Delete"** check box and then click the ***Delete*** button to remove that user from the black list.

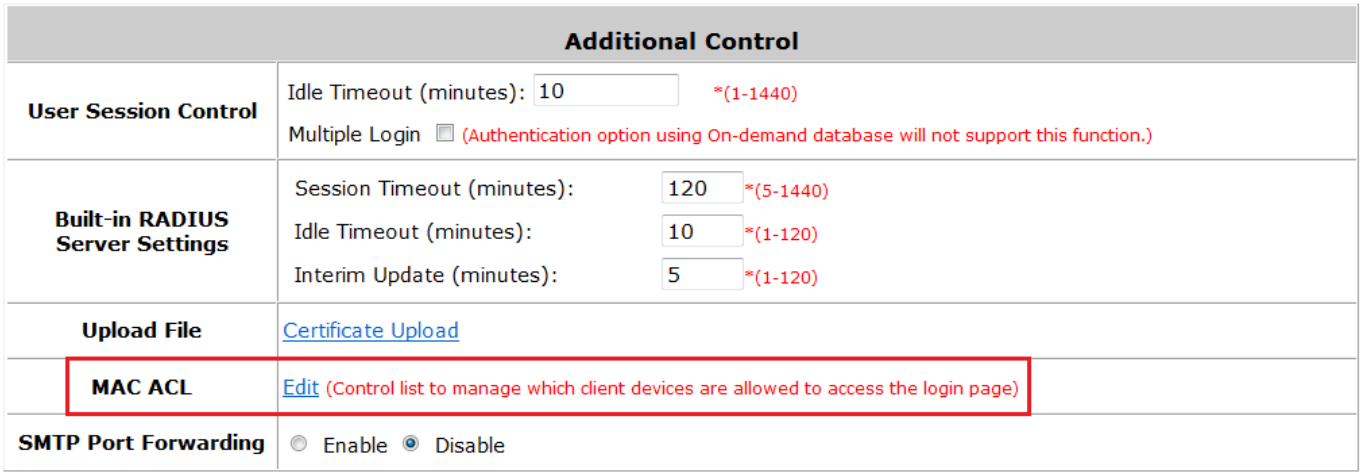


After the Black List editing is completed. You can select the appropriate Black List in each Authentication Server type to enable it.

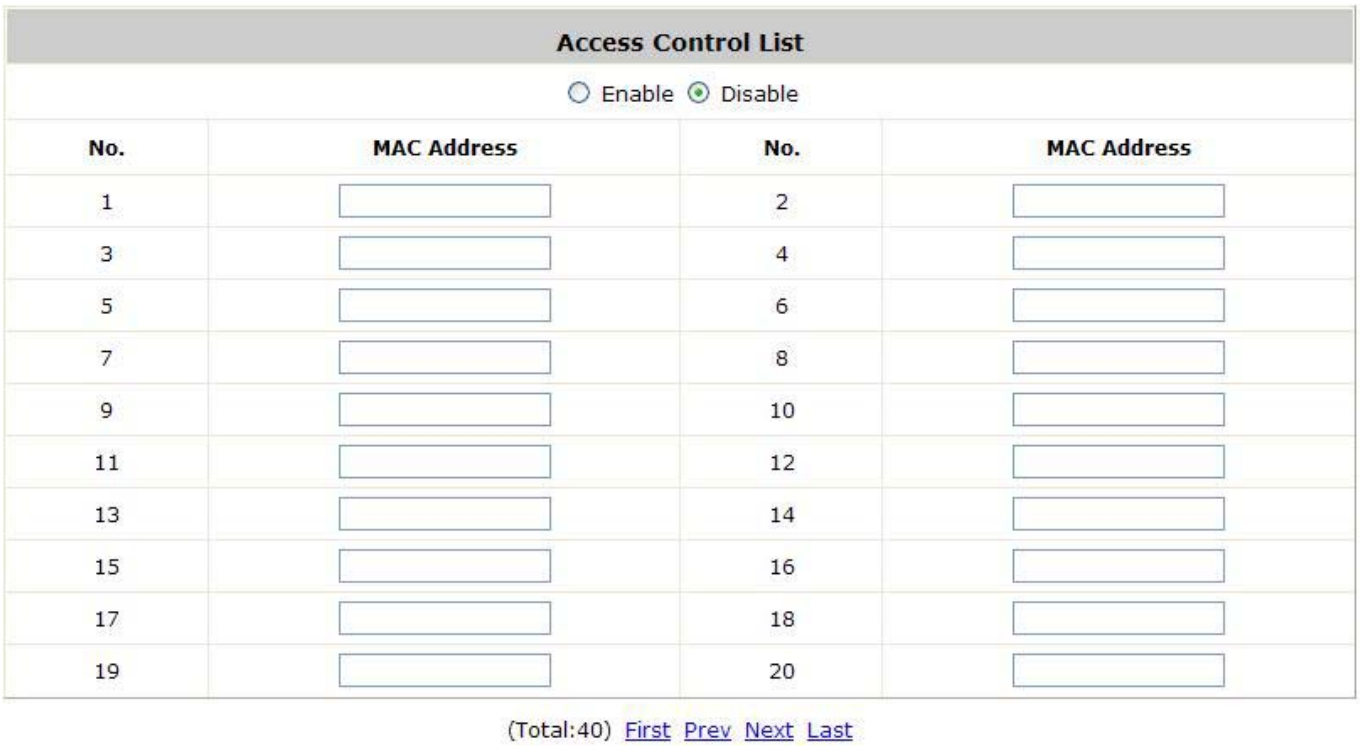


6.2 MAC Address Control

To configure MAC Address Control, go to: ***Users >> Additional Control***.



MAC ACL: With this function, only the users with their MAC addresses in this list can login to the HS1100N. There are 40 users maximum allowed in this MAC address list. User authentication is still required for these users. Click ***Edit*** to enter the **MAC Address Control** list. Fill in these MAC addresses, select **Enable**, and then click ***Apply***.



Caution:

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

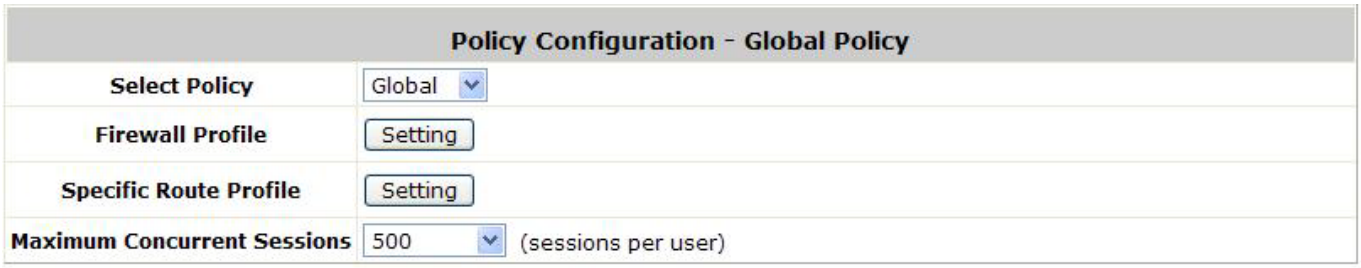
6.3 Policy

To configure Policy, go to: ***Users >> Policy***.

The HS1100N supports multiple Policies, including one **Global Policy** and 5 individual **Policy** types.
Global Policy is the system's universal policy and applied to all clients unless they are bounded by another policy. Individual Policy can be defined and applied to different authentication server. The client login with this authentication server will be bound by the corresponding Policy, if for an authentication server no policy is applied, its users will be governed by the Global Policy.
When the type of authentication database is **RADIUS**, the **Class-Policy Mapping** function will be available to allow the administrator to assign a Policy for a RADIUS class attribute; therefore, a Policy will be mapped to a user of a RADIUS class attribute.

Global Policy

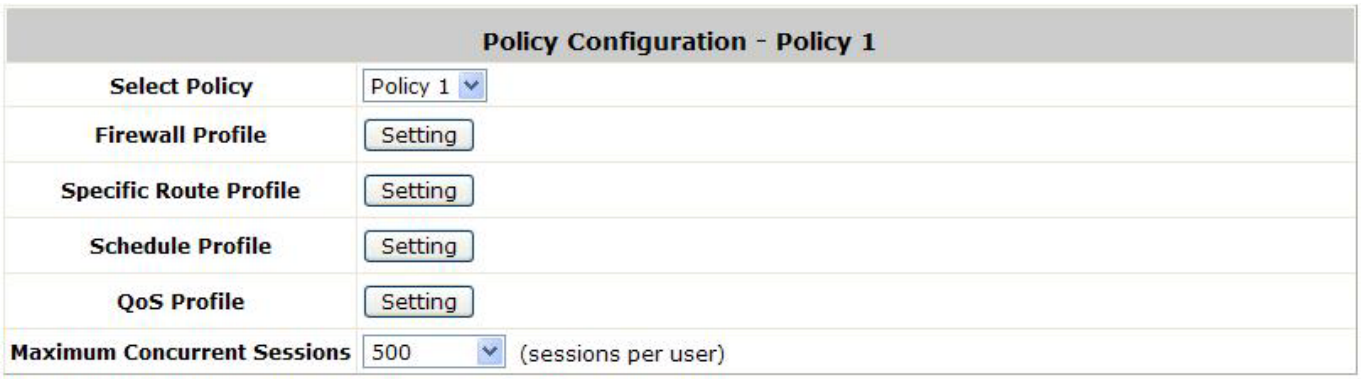
Global policy is the system's universal policy containing **Firewall Rules**, **Specific Routes Profile** and **Maximum Concurrent Sessions** which will be applied to all users unless the user has been regulated and applied with another individual Policy.



- **Select Policy:** Select the desired policy profile to configure.
- **Firewall Profile:** Global policy and policy 1 ~ 5 all have a firewall service list and a set of firewall profiles which is composed of firewall rules.
- **Specific Route Profile:** When Specific Routes are configured here, all clients effected by this policy will access the specific destination through these gateway settings.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client belonging to this group.

Policy 1 ~ Policy 5

Beside **Global Policy**, **Policy1** to **Policy5**, each consists of access control profiles that can be configured respectively and applied to a certain authentication server or user.



- **Select Policy:** Select the desired policy profile to configure.
- **Firewall Profile:** Each Policy has a firewall service list and a set of firewall profiles consisting of firewall rules.
- **Specific Route Profile:** The default gateway of a desired IP address can be defined in a policy. When Specific Routes are configured here, all clients applied with this policy will access the specific destination through these gateway settings.
- **Schedule Profile:** The Schedule table in a 7X24 format is used to control the clients' login time. When Schedule is enabled, clients applied with this policy are only allowed to login the system at the time which is checked in Schedule profile settings.
- **QoS Profile:** QoS profile defines the traffic class for the users governed by this Policy.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client belonging to this group.

6.3.1 Firewall

Firewall Profile: Click ***Setting*** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules.

Policy 1 - Firewall Configuration
Predefined and Custom Service Protocols
Firewall Rules

1) Predefined Protocols

Predefined and Custom Service Protocols: There are predefined service protocols available for firewall rules editing.

Policy 1 - Service Protocols List

No.	Name	Description	Select All
1	ALL	ALL	☐
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	☐
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	☐
4	ALL ICMP	ICMP; Type: Any, Code: Any	☐
5	FTP	TCP/UDP; Destination Port: 20;21	☐
6	HTTP	TCP/UDP; Destination Port: 80	☐
7	HTTPS	TCP/UDP; Destination Port: 443	☐
8	POP3	TCP; Destination Port: 110	☐
9	SMTP	TCP; Destination Port: 25	☐
10	DHCP	UDP; Destination Port: 67;68	☐

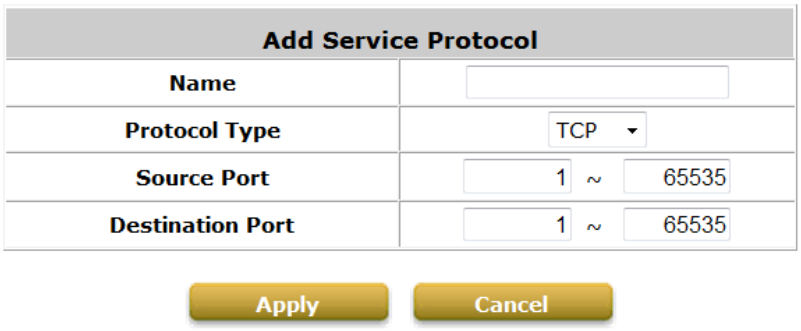
Add Delete

(Total: 27) First Prev Next Last

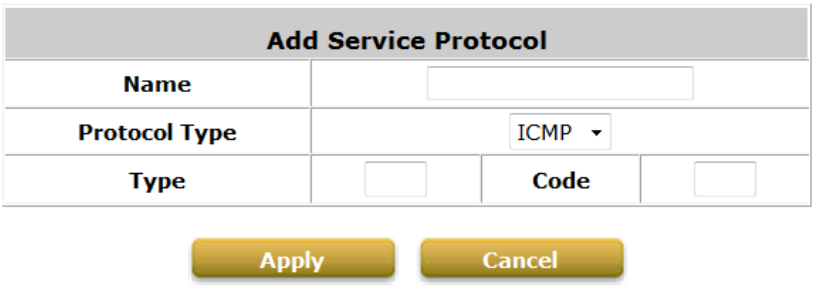
The administrator is able to add new custom service protocols by clicking ***Add***, and delete the added protocols individually or with ***Select All*** followed by ***Delete*** operation.

Caution:
The Predefined Service Protocols cannot be deleted.

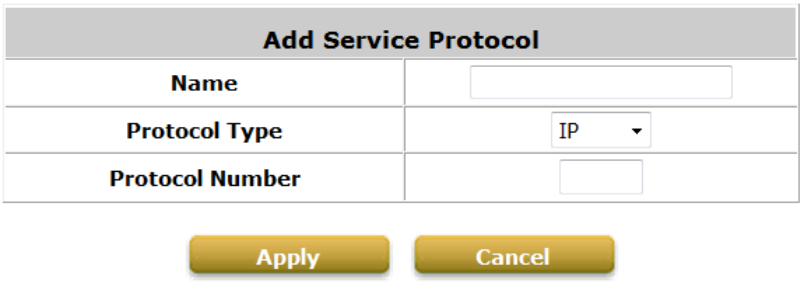
Click **Add** to add a custom service protocol. The **Protocol Type** can be defined from a list of service by protocols (*TCP/UDP/ICMP/IP*); and then define the **Source Port** (range) and **Destination Port** (range); click ***Apply*** to save this protocol.



If the **Protocol Type** is **ICMP**, define the **Type** and **Code**.



If the **Protocol Type** is **IP**, define the **Protocol Number**.



2) Firewall Rules

After the custom protocol is defined or just use the **Predefined Service Protocols**, you will need to enable the **Firewall Rule** to apply these protocols.

- **Firewall Rules:** Click the number of filter ***Rule No.*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list. Check **"Active"** checkbox and click ***Apply*** to enable that rule.

  Rule No.1 has the highest priority; Rule No.2 has the second priority and so on. Each firewall rule is defined by Source, Destination and Pass/Block action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to **Always**, **Recurring** or **One Time**.

Policy 1 - Firewall Rules						
No.	Active	Action	Rule Name	Source / Destination	Service	Schedule
1	☐	Block		ANY / ANY	ALL	Always
2	☐	Block		ANY / ANY	ALL	Always

Selecting the Filter Rule Number 1 as an example:

Policy 1 - Edit Filter Rule			
Rule Number	1		
Rule Name			
Source		**Destination**	
Interface/Zone	ALL	Interface/Zone	ALL
IP Address	0.0.0.0	IP Address	0.0.0.0
Subnet Mask	0.0.0.0 (/0)	Subnet Mask	0.0.0.0 (/0)
MAC Address			
Service Protocol	ALL		
Schedule	Always / Recurring / One Time		
Action for Matched Packets	Block / Pass		

- **Rule Number:** This is the rule selected “1”. Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on.
- **Rule Name:** The rule name can be changed here.
- **Source/Destination – Interface/Zone:** There are choices of **ALL, WAN**, **Public** and **Private** to be applied for the traffic interface.
- **Source/Destination – IP Address/Domain Name:** Enter the source and destination IP addresses. Domain Name filtering is supported but Domain Host filtering is not.
- **Source/Destination – Subnet Mask:** Select the source and destination subnet masks.
- **Source- MAC Address:** The MAC Address of the source IP address. This is for specific MAC address filter.
- **Service Protocol:** These are the defined protocols in the **service protocols list** to be selected.
- **Schedule:** When schedule is selected, clients assigned with this policy are applied the firewall rule only within the time specified. There are three options, **Always**, **Recurring** and **One Time. Recurring** is set with the hours within a week.
- **Action for Matched Packets:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets through.

6.3.2Routing

Specific Route Profile: Click the Setting button for **Specific Route Profile**, the Specific Route Profile list will

appear.

1) Specific Route

- **Specific Route Profile:** The Specific Default Route is use to control clients to access some specific IP segment by the specified gateway.

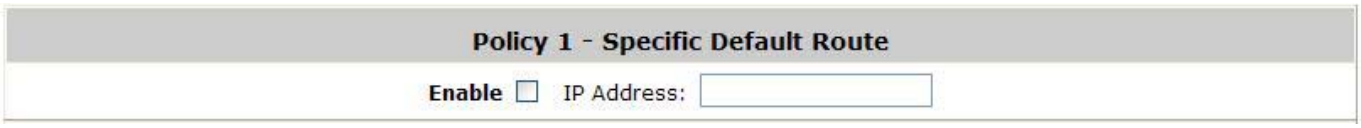
Global Policy - Specific Routes			
Route No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1		255.255.255.255 (/32)	
2		255.255.255.255 (/32)	
3		255.255.255.255 (/32)	
4		255.255.255.255 (/32)	

Policy 1 - Specific Default Route			
Enable ☐ IP Address:			
Policy 1 - Specific Routes			
Route No.	Destination		Gateway
	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)	

- **Destination / IP Address:** The destination network address or IP address of the destination host. Please note that, if applicable, the system will calculate and display the appropriate value based on the combination of Network/IP Address and Subnet Mask that have just been entered and applied.
- **Destination / Subnet Netmask:** The subnet mask of the destination network. Select *255.255.255.255(/32)* if the destination is a single host.
- **Gateway / IP Address:** The IP address of the gateway or next router to the destination.

2) Default Gateway

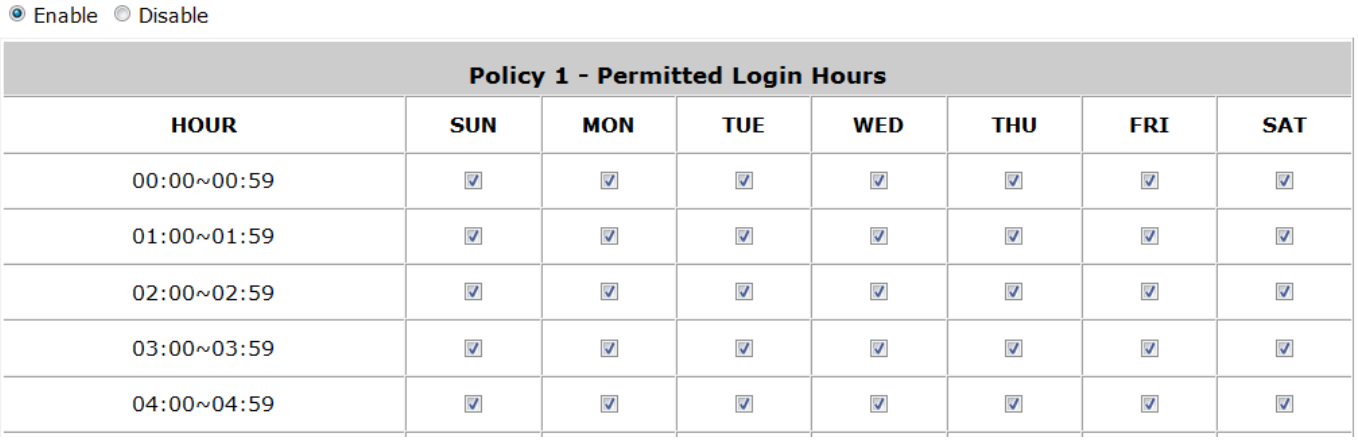
- **Default Gateway:** The default gateway of a desired IP address can be defined in each Policy except **Global Policy**. When Specific Default Route is enabled, all clients applied with this Policy will access the Internet through this default gateway.



  - **Enable:** Check ***Enable*** box to activate this function or uncheck to disable it.
  - **Default Gateway IP Address**: You may need to enter the IP address of the default gateway.

6.3.3 Schedule

- **Schedule Profile:** Click ***Setting*** of *Schedule Profile* to enter the configuration page. Select ***Enable*** to show the **Permitted Login Hours** list. This function is used to limit the time when clients can log in. Check the desired time slots checkbox and click ***Apply*** to save the settings. These settings will become effective immediately after clicking ***Apply***.



6.3.4 QoS Profile

For certain applications or users that need stable bandwidth or traffic priority, Policy 1 to 5 allows defining the QoS profile for the users governed by this Policy.

Policy 1 - Traffic Configuration	
Traffic Class	Best Effort
Total Downlink	Unlimited
Individual Maximum Downlink	Unlimited
Individual Request Downlink	None
Total Uplink	Unlimited
Individual Maximum Uplink	Unlimited
Individual Request Uplink	None

- **Traffic Class:** A Traffic Class can be chosen for a Group of users. There are four traffic classes: ***Voice***, ***Video***, ***Best-Effort*** **and** ***Background***. **Voice** and **Video** traffic will be placed in the high priority queue. When **Best-Effort** or **Background** is selected, more bandwidth management options such as Downlink and Uplink Bandwidth will appear.
- **Total Downlink:** Defines the maximum bandwidth allowed to be shared by clients.
- **Individual Maximum Downlink:** Defines the maximum downlink bandwidth allowed for an individual client. The Individual Maximum Downlink cannot exceed the value of Total Downlink.
- **Individual Request Downlink:** Defines the guaranteed minimum downlink bandwidth allowed for an individual client. The Individual Request Downlink cannot exceed the value of Total Downlink and Individual Maximum Downlink.
- **Total Uplink:** Defines the maximum uplink bandwidth allowed to be shared by clients.
- **Individual Maximum Uplink:** Defines the maximum uplink bandwidth allowed for an individual client. The Individual Maximum Uplink cannot exceed the value of Total Uplink.
- **Individual Request Uplink:** Defines the guaranteed minimum bandwidth allowed for an individual client. The Individual Request Uplink cannot exceed the value of Total Uplink and Individual Maximum Uplink.

6.3.5 Session Limit

To prevent ill-behaved clients or malicious software from taking up the system's connection resources, the administrator can restrict the number of concurrent sessions that a user can establish.

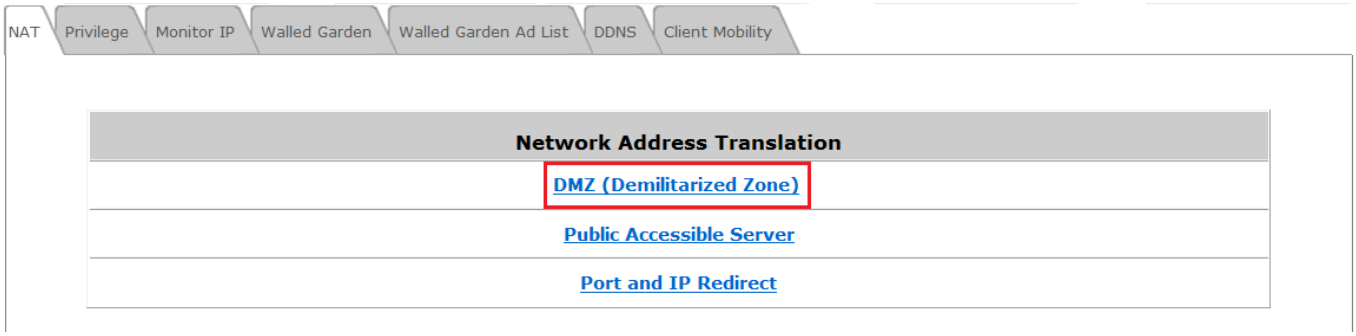
Policy Configuration - Policy 1	
Select Policy	Policy 1
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Maximum Concurrent Sessions	500 (sessions per user)

- The maximum number of concurrent sessions including 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. This can also be specified in the other policies to apply to the authenticated users.
- 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.

7 Access Network without Authentication

7.1 DMZ

To configure the DMZ, go to: ***Network >> Network Address Translation >> DMZ (Demilitarized Zone)***.



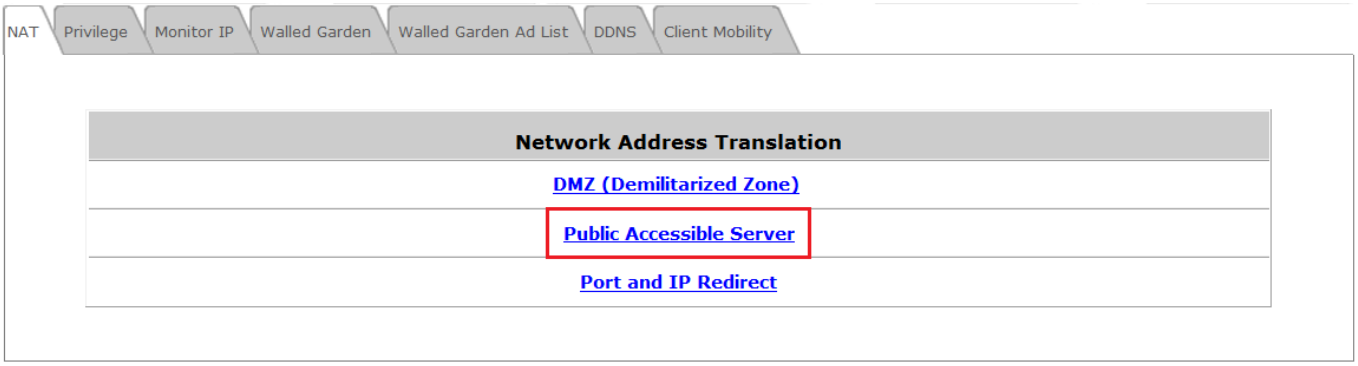
There are 20 sets of static Internal IP Address and External IP Address available. Enter the **Internal** and **External** IP Address as a set. After the setup, accessing the External IP address listed in DMZ will be mapped to accessing the corresponding Internal IP Address. These settings will become effective immediately after clicking the ***Apply*** button. The External IP Address of the Automatic WAN IP Assignment is the IP address of External Interface (WAN) that will change dynamically if WAN Interface is Dynamic. When **Automatic WAN IP Assignments** is enabled, the entered Internal IP Address of Automatic WAN IP Assignment will be bound with the WAN interface.

Automatic WAN IP Assignment		
Enable	**External IP Address**	**Internal IP Address**
☐	10.2.3.70	

DMZ (Demilitarized Zone)		
Item	**External IP Address**	**Internal IP Address**
1		
2		
3		
4		
5		

7.2 Virtual Server

To configure the Virtual Server, go to: ***Network >> Network Address Translation >> Public Accessible Server***.



This function allows the administrator to set 20 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

No.	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				TCP UDP	
2				TCP UDP	
3				TCP UDP	
4				TCP UDP	
5				TCP UDP	
6				TCP UDP	
7				TCP UDP	
8				TCP UDP	
9				TCP UDP	
10				TCP UDP	

(Total:20) First Prev Next Last

7.3 Privilege List

To configure the Privilege List, go to: ***Network >> Privilege***

Setup the **Privilege IP Address List** and **Privilege MAC Address List**. The clients accessing the internet via IP addresses and/or networking devices in the list can access the network without any authentication.

7.3.1 Privilege IP

Privilege IP Address List

To configure a Privilege IP Address List, go to: ***Network Configuration >> 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 **"Granted Access by IP Address"**. The **"Remark"** field is not necessary but is useful to keep track of each entry. The HS1100N allows 100 privilege IP addresses at most.

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

Granted Access by IP Address		
No.	**IP Address**	**Remark**
1		
2		
3		
3		
4		
5		
8		
9		
10		

(Total: 100) First Prev Next Last

Caution:

Permitting specific IP addresses to have network access rights without going through standard authentication process under Public zone may cause security problems.

7.3.2 Privilege MAC

Privilege MAC Address List

In addition to the Privilege IP List, the MAC address List allows the MAC address of the workstations that need to access the network without authentication to be set in the **"Granted Access by MAC Address"**. The HS1100N 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***.

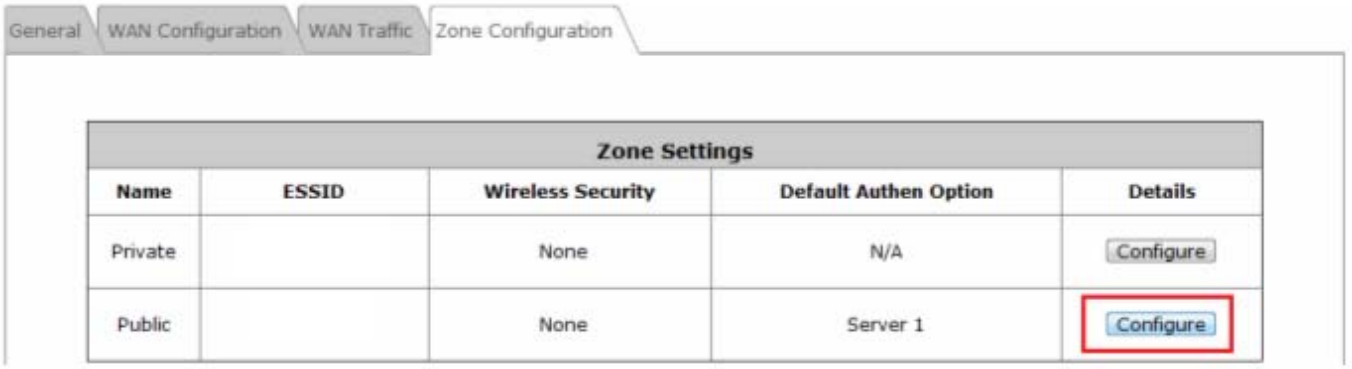
Granted Access by MAC Address		
No.	**MAC Address**	**Remark**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

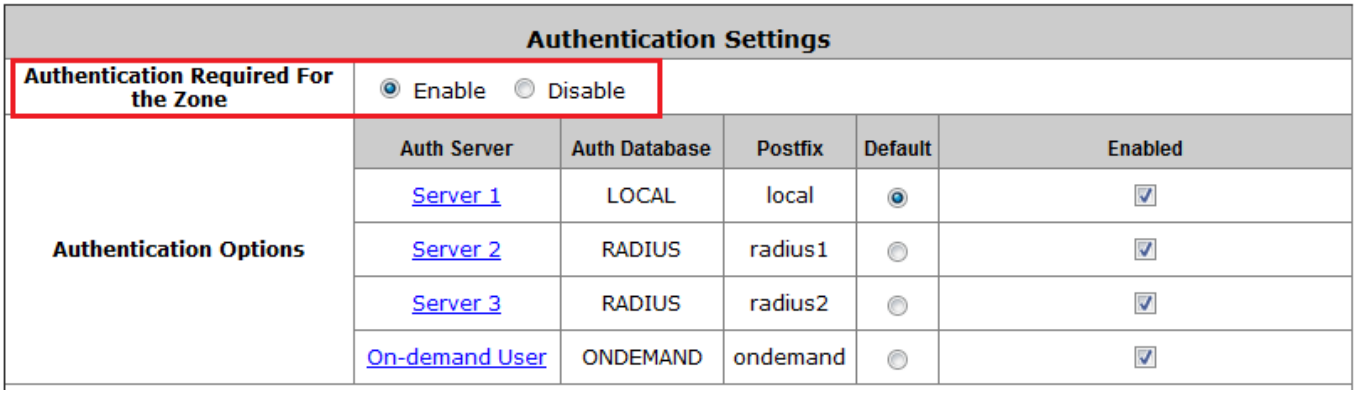
(Total: 100) First Prev Next Last

Caution:
Permitting specific MAC addresses to have network access rights without going through standard authentication process under Public zone may cause security problems

7.4 Disable Authentication in Public Zone

Configure Disable Authentication in Public Zone, go to: ***System >> Zones Configuration,*** *click* ***Configure*** *in* ***Public Zone***.





- **Authentication Required For the Zone:** When it is disabled, users will not need to authenticate before they get access to the network within Public Zone.

8 User Login and Logout

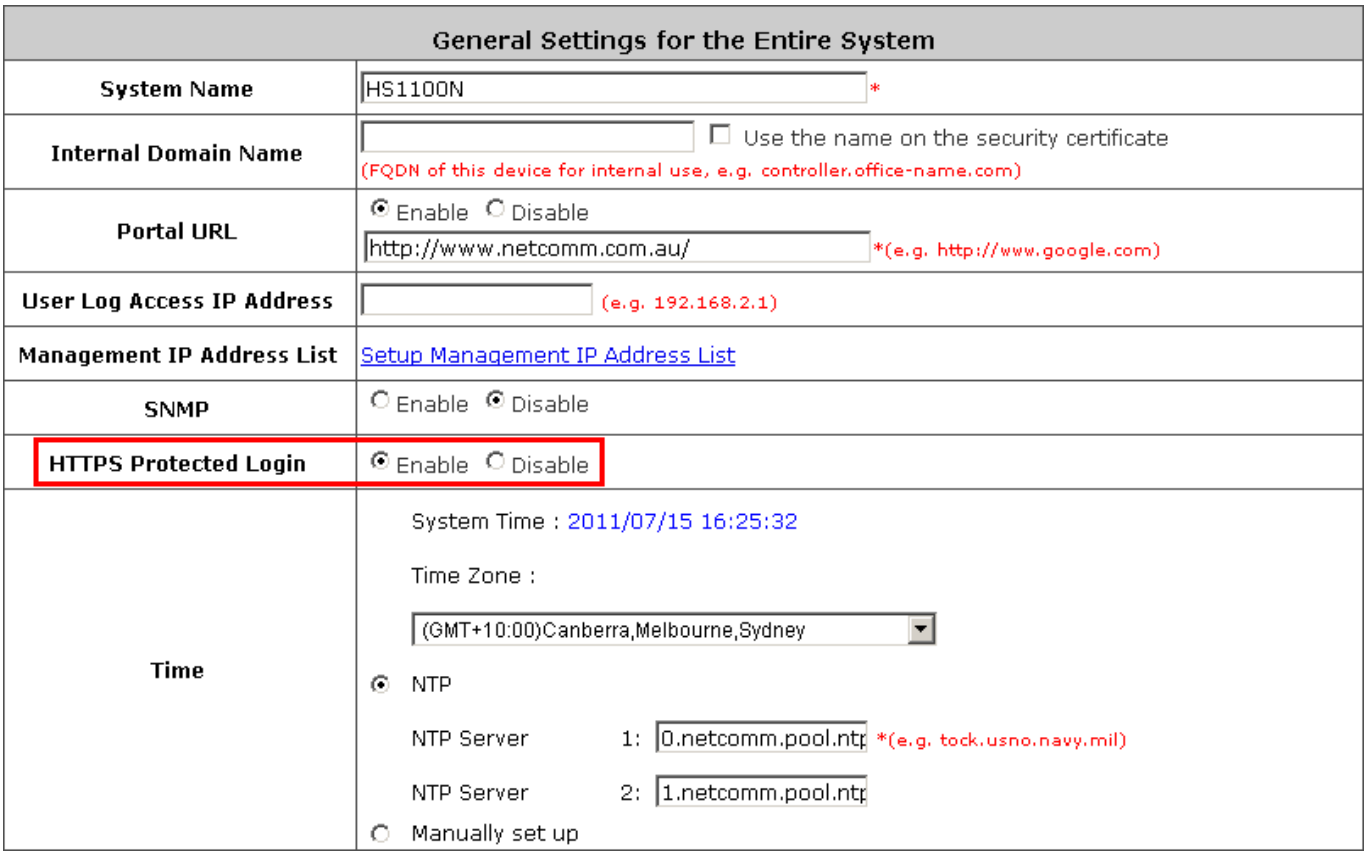
8.1 Before User Login

8.1.1 Login with SSL

Configure HTTPS, go to: ***System >> General***.

HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sub-layer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

HTTP Protected Login function will let the client's login with https for more security. Enable to activate https (encryption) or disable to activate http (non encryption) login page.



8.1.2 Internal Domain Name with Certificate

To configure the Internal Domain Name, go to: ***System >> General***.

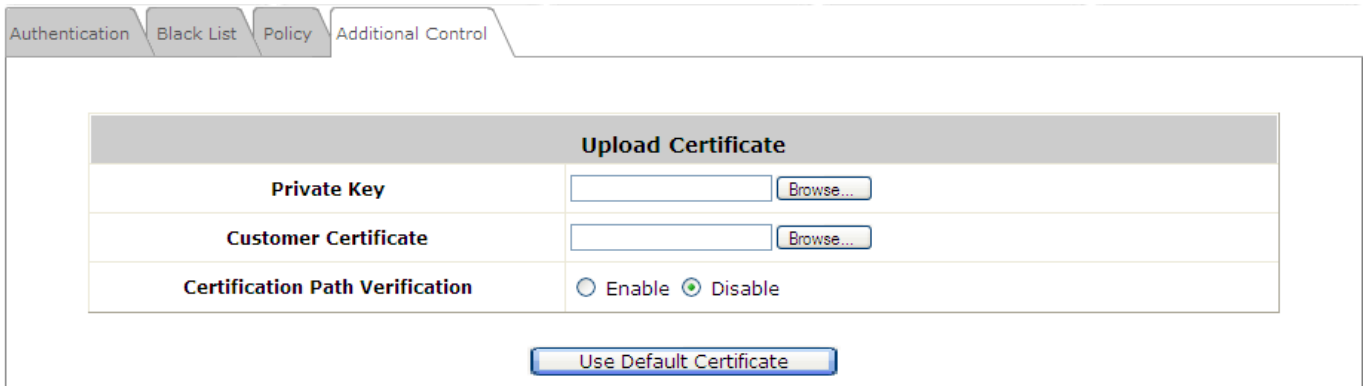
Internal Domain Name is the domain name of the HS1100N as seen on client machines connected under zone. It must conform to the FQDN (Fully-Qualified Domain Name) standard. A user on client machine can use this domain name to access the HS1100N instead of its IP address.
In addition, when "***Use the name on the security certificate***" option is checked, the system will use the CN (Common Name) value of the uploaded SSL certificate as the domain name.

General Settings for the Entire System	
System Name	HS1100N *
Internal Domain Name	☐ Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)

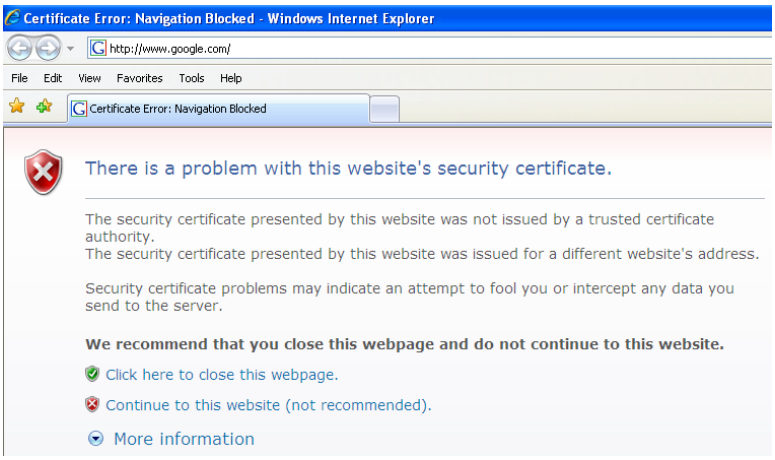
To configure a Certificate, go to: ***Users >> Additional Control >> Upload File***.

Certificate: A data record used for authenticating network entities such as a server or a client. A certificate contains X.509 information pieces about its owner (called the subject) and the signing Certificate Authority (called the issuer), plus the owner's public key and the signature made by the CA. Network entities verify these signatures using CA certificates. You can apply for a SSL certificate at CAs such as VeriSign.

If you already have a SSL Certificate, please Click Browse to select the file and upload it. Click ***Apply*** to complete the upload process. If you do not have a valid SSL Certificate, use the system default certificate.

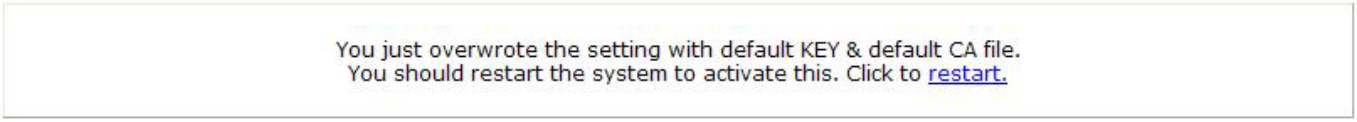


Without a valid certificate, users may encounter the following problem in IE7 when they try to open the login page.



Click "Continue to this website" to access the user login page.

Use Default Certificate: Click ***Use Default Certificate*** to use the default certificate and key. Click **restart** to validate the changes.



8.1.3 Walled Garden

To configure the Walled Garden, go to: ***Network >> Walled Garden***.

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 network access can still have a chance to utilise the network free of charge. Enter the website **IP Address** or **Domain Name** in the list and click ***Apply*** to save the settings.

Walled Garden List			
No.	**Domain Name/IP Address**	**No.**	**Domain Name/IP Address**
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

8.1.4 Walled Garden AD List

To configure the Walled Garden AD List, go to: ***Network >> Walled Garden AD List***.

This function provides advertisement links to web pages for users to access free of charge 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	Description	Display
1				☐
2				☐
3				☐
4				☐
5				☐
6				☐
7				☐
8				☐
9				☐
10				☐

- Enter all items or make changes, click ***Apply***, the items will be added and shown in the list.
- **URL:** Enter the URL of the advertisement website.
- **Topic:** Enter the content of the hyperlink, for instance if you enter Google in this field, on the user login page a hyperlink Google will be displayed.
- **Description:** Any additional message for administrator's reference.
- **Display:** Choose ***Display*** to display advertisement hyperlinks on the login pages

8.2 After User Login

8.2.1 Portal URL after successful login

To configure the Portal URL shown after a successful user login, go to: ***System >> General***.

When this function is enabled, enter the URL of a Web server as the Portal page. Once logged in successfully, users will be directed to this URL, such as *http://www.google.com*, regardless of the original homepage set in their browsers.

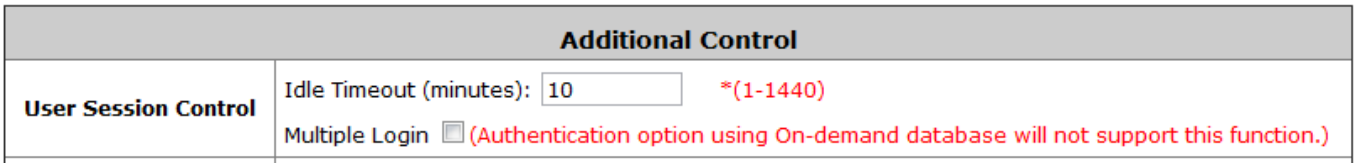
General Settings for the Entire System	
System Name	HS1100N *
Internal Domain Name	Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Portal URL	Enable Disable http://www.netcomm.com.au/ *(e.g. http://www.google.com)
User Log Access IP Address	(e.g. 192.168.2.1)

When this function is disabled, after users logged in successfully, users will be directed to the original homepage set in their browsers.

8.2.2 Idle Timer

To configure the Idle Timer, go to: ***Users >> Additional Control***.

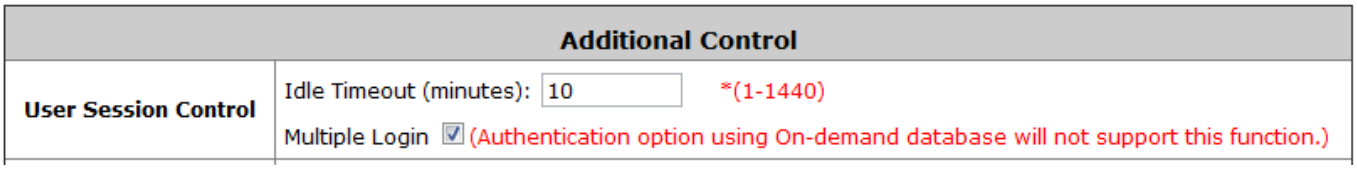
If a user is idle, with no network activity, the system will automatically disconnect the user. The logout timer can be set between 1~1440 minutes, and the default idle time is 10 minutes.



8.2.3 Multiple Login

To configure Multiple Login, go to: ***Users >> Additional Control***.

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.)



9 Networking Features of a Gateway

9.1 IP Plug and Play

To configure IP Plug and Play, go to: ***Network >> Client Mobility***.

The HS1100N supports the IP PNP function. User can login and access network with any IP address setting. This function is disabled in default settings.

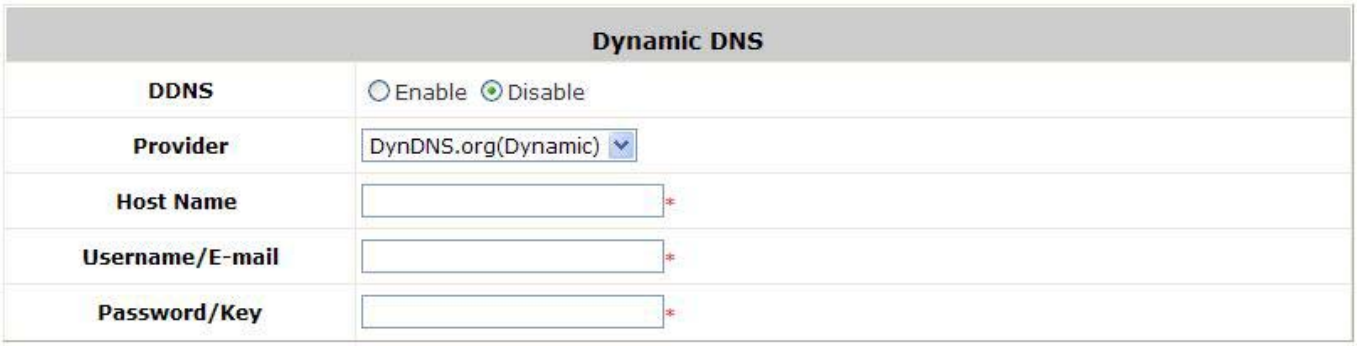
Client Mobility	
IP PNP	○ Enable ◉ Disable

When **IP PNP** is enabled, at the user end, a static IP address can be used to connect to the system. Regardless of what the IP address at the user end is using, authentication can still be performed through the HS1100N.

9.2 Dynamic Domain Name Service (DDNS)

To configure the Dynamic Domain Name Service, go to: ***Network >> DDNS***.

Before activating this function, you must have your Dynamic DNS hostname registered with a Dynamic DNS provider. The HS1100N supports DNS functions to alias the dynamic IP address for the WAN port to a static domain name, allowing the administrator to easily access the HS1100N'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***.



- **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.

9.3 Port and IP Redirect

To configure Port and IP Redirect, go to: ***Network >> NAT >> Port and IP Redirect***.

This function allows the administrator to set 40 sets of IP address redirection. 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***.

Port and IP Redirect					
No.	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1					TCP UDP
2					TCP UDP
3					TCP UDP
4					TCP UDP
5					TCP UDP
6					TCP UDP
7					TCP UDP
8					TCP UDP
9					TCP UDP
10					TCP UDP

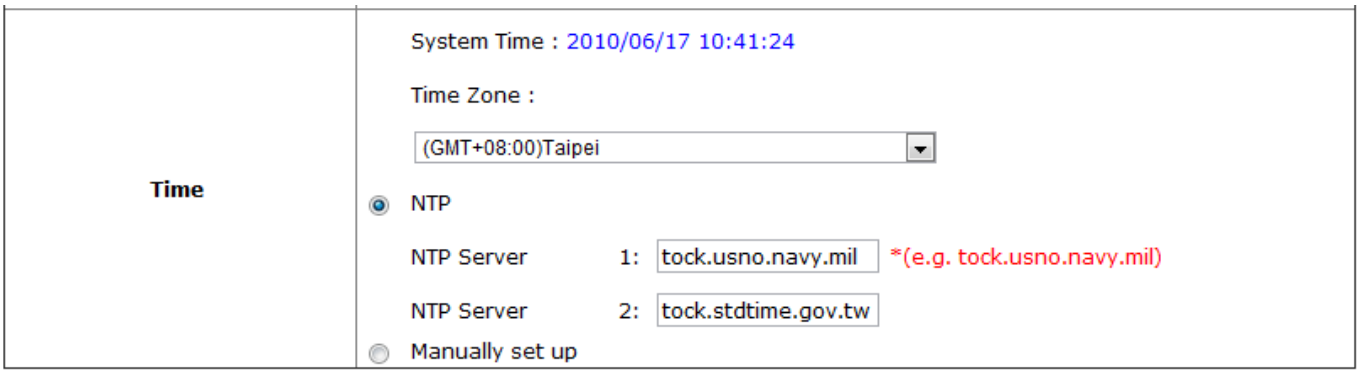
(Total:40) First Prev Next Last

10 System Management and Utilities

10.1 System Time

To configure the System Time, go to: ***System >> General***.

The **NTP** (Network Time Protocol) communication protocol can be used to synchronize the system time with a remote time server. Please specify the local time zone and the IP address of at least one NTP server for adjusting the time automatically (Universal Time is Greenwich Mean Time, GMT).
Manually set up is another option to setup system time, if you choose to setup system time manually, please enter the Year, Month, Day, the current time and click Apply to activate the changes.



Note:
When system cannot sync the time with the specified NTP server, clients will not be allowed to login to system. On-demand accounts are also unable to be created.

10.2 Management IP

To configure Management IP, go to: ***System >> General***.

General Settings for the Entire System	
System Name	HS1100N *
Internal Domain Name	Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Portal URL	Enable Disable http://www.netcomm.com.au/ *(e.g. http://www.google.com)
User Log Access IP Address	(e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List
SNMP	Enable Disable

Only PCs within the Management IP range on the list are allowed to access the system's web management interface. For example, 10.2.3.0/24 means that as long as an administrator is using a computer with the IP address range of 10.2.3.0/24, he or she can access the web management page. Another example is 10.0.0.3: if an administrator is using a computer with the IP address of 10.0.0.3, he or she can access the web management page.

Management IP Address List			
No.	**IP Address/Segment**	**No.**	**IP Address/Segment**
1	0.0.0.0/0.0.0.0	2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

The default value is “0.0.0.0/0.0.0.0”. It means that the WMI can be accessed by any IP address, for security reasons, please change this value before the system provides network services.

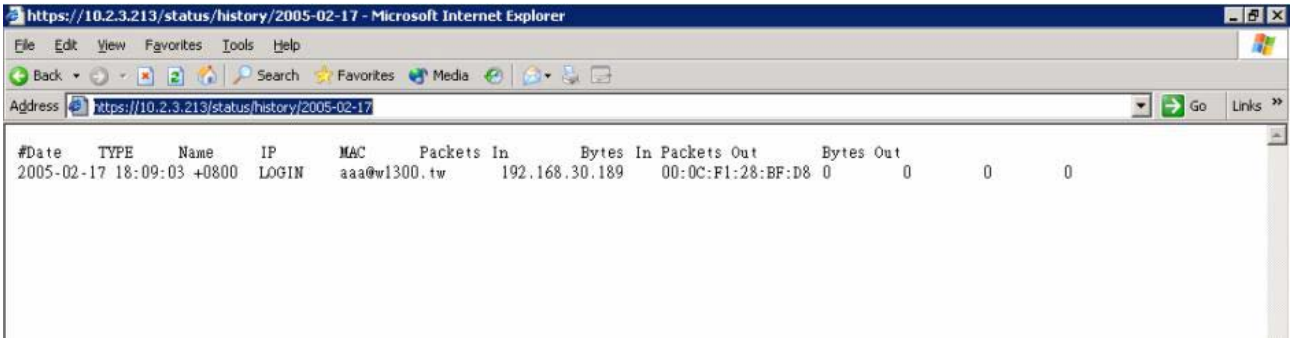
10.3 User Log Access IP Address

To configure User Log Access IP History, go to: ***System >> General***.

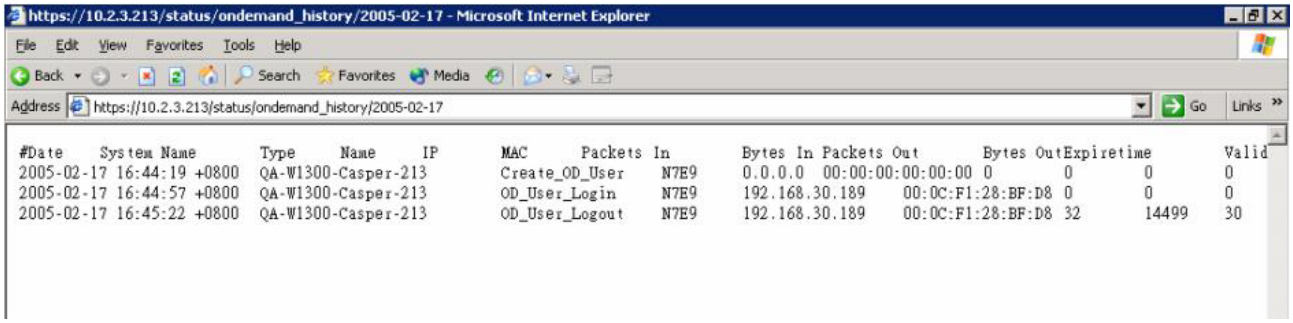
General Settings for the Entire System	
System Name	HS1100N *
Internal Domain Name	Use the name on the security certificate (FQDN of this device for internal use, e.g. controller.office-name.com)
Portal URL	Enable Disable http://www.netcomm.com.au/ *(e.g. http://www.google.com)
User Log Access IP Address	(e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List

Specify an IP address of the administrator's computer or a billing system to get billing history information of the HS1100N with the predefined URLs. The file name format is "yyyy-mm-dd". An example is provided as follows:

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



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



10.4 SNMP

To configure SNMP, go to: ***System >> General***. The HS1100N supports SNMP v1/v2c.

If this function is enabled, the SNMP Management IP and the Community string can be assigned for SNMP access to the system.

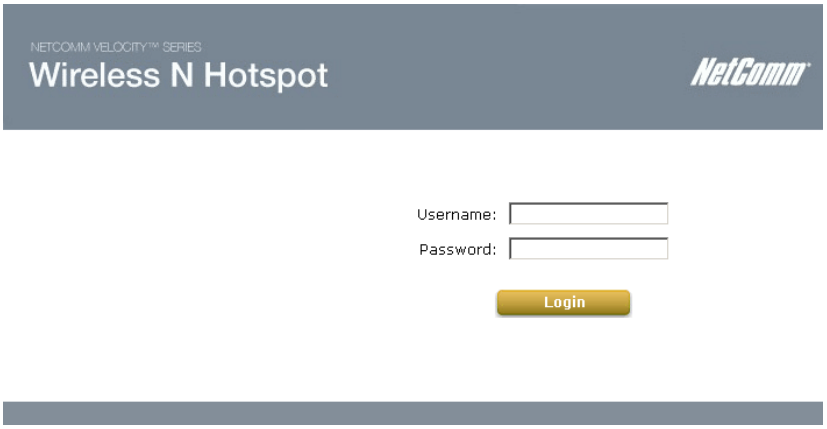
10.5 Three-Level Administration

The HS1100N supports three kinds of account interface. You can log in as **admin**, **manager** or **operator**. The default usernames and passwords show as follows:

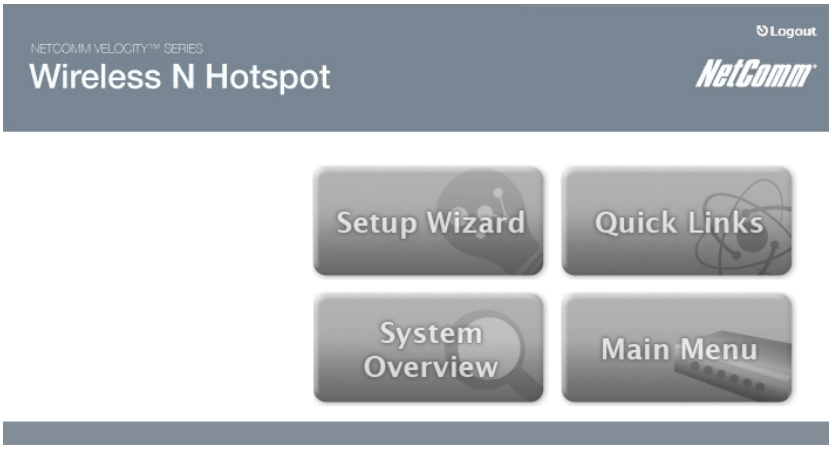
Admin: The administrator can access all configuration pages of the HS1100N.

Username: **admin**

Password: **admin**



After a successful login to the HS1100N, a web management interface with a Home page will appear.



Manager: The manager can only access the configuration pages under **User Authentication** to manage the user accounts.

User Name: **manager**

Password: **manager**

Authentication Settings					
Auth Database	**Auth Server Name**	**Postfix**	**Policy**	**Black List**	**Configure**
LOCAL	Server 1	local	Policy 1	None	Configure
RADIUS	Server 2	radius1	Policy 2	None	Configure
RADIUS	Server 3	radius2	Policy 3	None	Configure
ONDEMAND	On-demand User	ondemand	Policy 4	None	Configure

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**

On-demand Account Creation					
Plan	**Type**	**Quota**	**Price**	**Status**	**Function**
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Cut-off	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create

Note:

To logout, simply click the ***Logout*** icon on the upper right corner of the WMI to return to the login screen.

10.6 Change the Password

To Change the Password, go to: ***Utilities >> Password Change***.

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 the HS1100N.

User Name: **admin**

Password: **admin**

Manager: The manager can only access the configuration pages under ***User Authentication*** to manage the user accounts.

User Name: **manager**

Password: **manager**

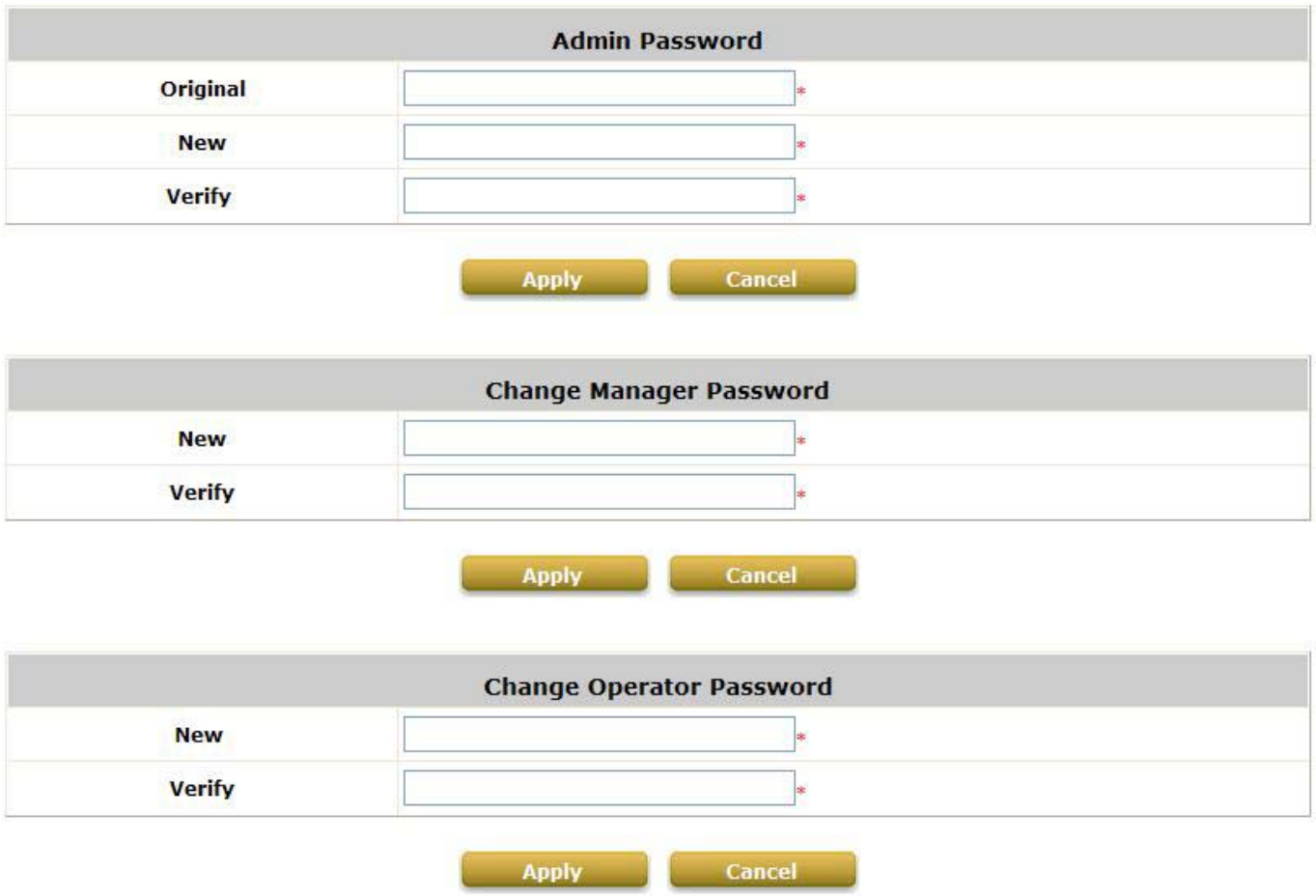
Operator: The operator can only access the configuration page of ***Create On-demand User*** to create new on-demand user accounts and print out the on-demand user account receipts.

User Name: **operator**

Password: **operator**

The administrator can change the passwords here. Click ***Apply*** to activate this new password.

Note:
Only **admin** account can change passwords.



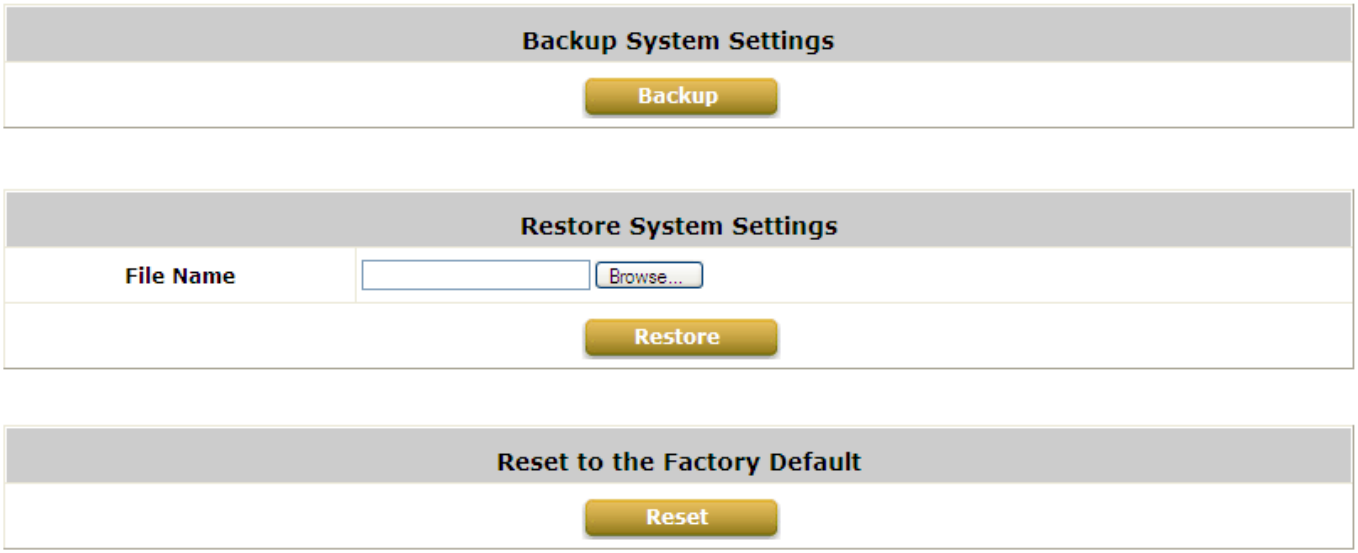
Caution:

If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface via the serial console port.

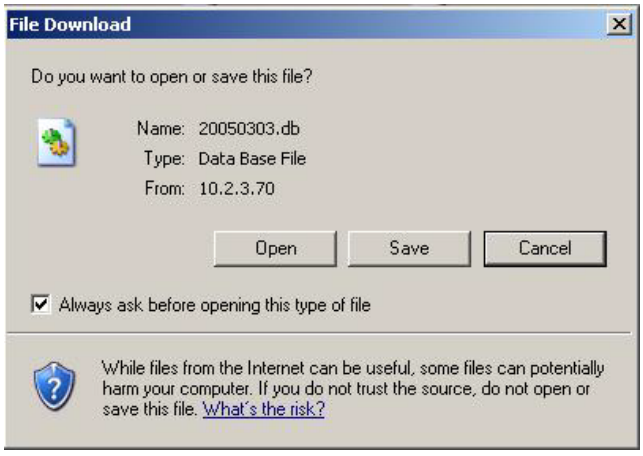
10.7 Backup / Restore and Reset to Factory

To configure Backup / Restore and Reset to Factory Default, go to: ***Utilities >> Backup & Restore***.

This function is used to backup/restore the HS1100N settings. Also, the HS1100N can be restored to the factory default settings here.



- **Backup System Settings:** Click ***Backup*** to create a .db database backup file and save it on disk.

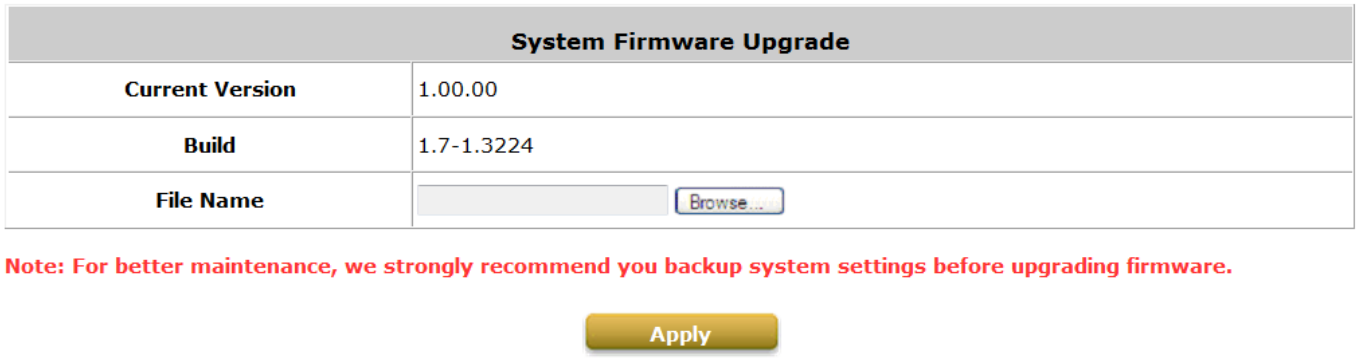


- **Restore System Settings:** Click ***Browse*** to search for a .db database backup file created by the HS1100N and click ***Restore*** to restore to the same settings at the time when the backup file was saved.
- **Reset to Factory Default:** Click ***Reset*** to load the factory default settings of the HS1100N.

10.8 Firmware Upgrade

To perform a Firmware Upgrade, go to: ***Utilities*** >> ***System Upgrade***.

The administrator can download the latest firmware from the NetComm website and upgrade the system here. Select the latest firmware with ***Browse*** button, then click ***Apply***, the system will upload the file and restart to perform the upgrade process. It might take a few minutes before the upgrade process completes and the new firmware's WMI interface appears.



Note:

*After clicking **Apply**, the system will begin uploading the chosen firmware into the system. Once the upload process is complete system will restart to activate the new firmware. The entire process may take a few minutes until the new firmware WMI appears. When restart is complete, the system will not lease IP addresses. Use a static IP configured computer to upgrade the system firmware.*

Caution:

1. *Firmware upgrade may cause the loss of some data. You may need to manually backup user account information, please refer to the release notes for any limitations before upgrading.*
2. *Do not power on/off the system during the upgrade or restart process. It may damage the system and cause malfunction.*

10.9 Restart

To perform a system restart, go to: ***Utilities >> Restart***.

This function allows the administrator to safely restart the HS1100N, and the process takes approximately three minutes. Click ***YES*** to restart the HS1100N; click ***NO*** to go back to the previous screen. Do NOT power off the power during system restart as this might damage the system. If the power needs to be turned off, it is highly recommended to restart the HS1100N first and then turn off the power after completing the restart process.

Caution:
All online users will be disconnected when system is in the process of restarting.

10.10 Network Utility

To use the Network Utilities, go to: ***Utilities >> Network Utilities***.

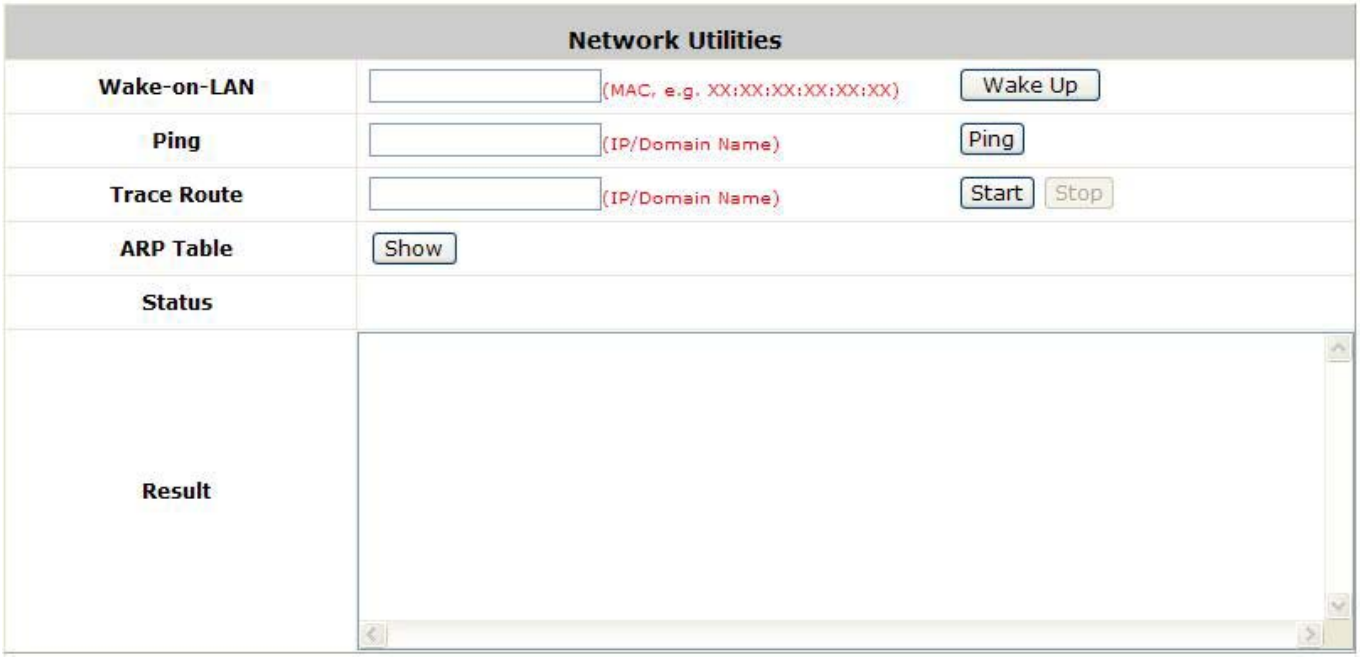
The System provides some network utilities to allow administrators to use.

Wake-on-LAN is for waking up remote devices that supports Wake-on-LAN feature by entering the MAC address of the target device and then press ***Wake Up*** button.

Ping is to see whether a destination host is reachable and alive by entering the destination host's domain name or IP address and then press ***Ping*** button.

Trace Route displays the actual route taken to reach the destination host by entering the destination host's domain name or IP address and then press ***Start*** button.

ARP Table is for displaying ARP information stored on the system.



10.10.1 Wake-on-LAN

This allows the system to remotely boot up a powered-down computer with the Wake-On-LAN feature enabled in its BIOS while it is connected to a LAN port. Enter the MAC Address of the desired device and click ***Wake Up*** button to execute this function.

10.10.2 Ping

It allows the administrator to detect a device using IP address or Host domain name to see if it is responding to network traffic or not.

10.10.3 Trace Route

It allows the administrator to find out the real path of packets from the gateway to a destination using IP address or Host domain name.

10.10.4 Show ARP Table

It allows the administrator to view the IP-to-Physical address translation tables used by the address resolution protocol (ARP).

10.11 Monitor IP Link

To Monitor the IP Link, go to: ***Network*** >> ***Monitor IP***.

The HS1100N will send out a packet periodically to monitor the connection status of the IP addresses on the list. On each monitored item with a WEB server running, administrators may add a link for the easy access by entering the IP, select the **Protocol** to *http* or *https* and then click ***Create***. After clicking ***Create*** button, the IP address will become a hyperlink, and administrators can easily access the host by clicking the hyperlink remotely. Click the ***Delete*** button to remove the hyperlink if desired.

Monitor IP List				
No.	**Protocol**	**IP Address**	**Hyperlink**	**Remark**
1	http		Create	
2	http		Create	
3	http		Create	
4	http		Create	
5	http		Create	
6	http		Create	
7	http		Create	
8	http		Create	
9	http		Create	
10	http		Create	

(Total: 40) First Prev Next Last

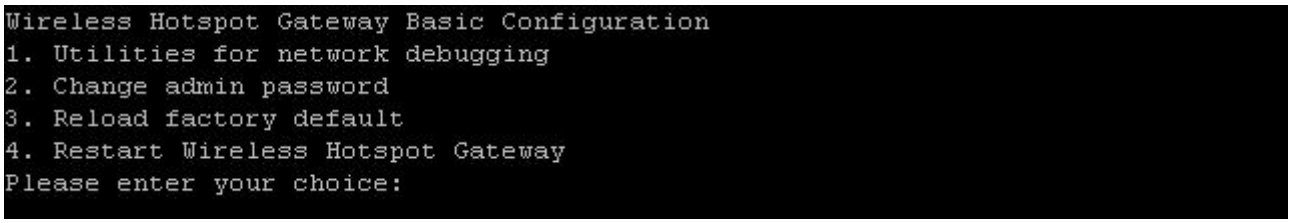
10.12 Console Interface

Via the console port, administrators can enter the console interface for handling problems and situations which may occur during normal operation.

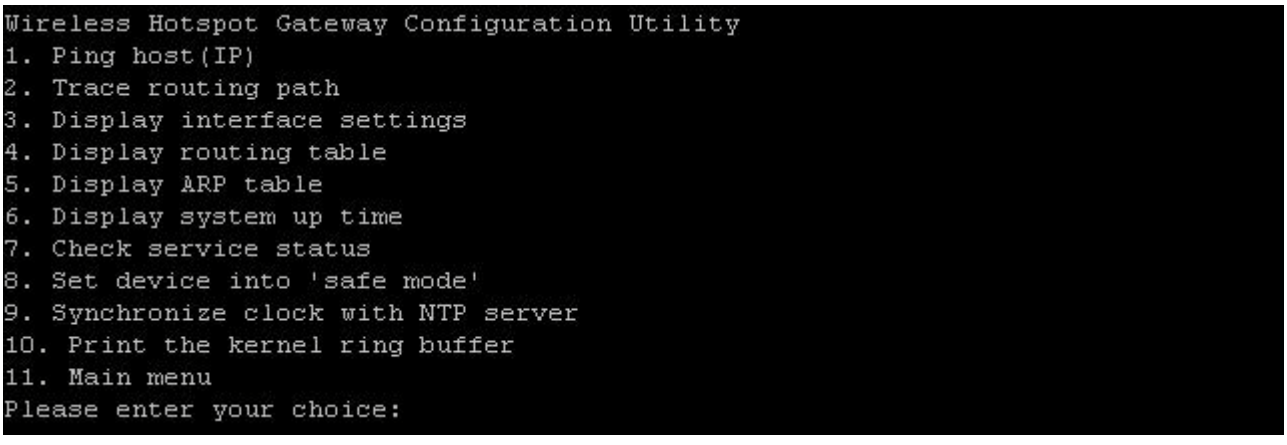
1. In order to connect to the console port of the HS1100N, a console, modem cable and a terminal emulation program, such as the Hyper Terminal are needed.
2. If a Terminal emulator is used, please set the parameters as **9600, 8, None, 1, None.**

Caution:
*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 the HS1100N is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal emulation program automatically, please try to press the arrow keys, so that the terminal emulation program will send some messages to the system, and 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 for the terminal emulation program.



- **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:



  - Ping host (IP): By sending ICMP echo requests to a specified host and wait for the response to test the network status.
  - Trace routing path: Trace and display the routing path to a specific target.
  - Display interface settings: It displays the information for each network interface 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 since the system was powered 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 the Web Management Interface via a browser, the administrator can choose this utility and set it into safe mode. This enables them to manage this device with a web 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, the internal clock is reset 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 cable, the system also supports SSH connections for 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 when connecting to the system by SSH, the username and password are required.

  The username is “admin” and the default password is also “admin”. The 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.

Caution:

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 HS1100N 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 The HS1100N**

  Choosing this option will restart the HS1100N.

11 System Status and Reports

11.1 View the Status

This section includes **System**, **Interface**, **Routing Table**, **Online Users**, **User Log** and **E-mail & SYSLOG** to provide system status information and online user status.

11.1.1 System Status

To view the System Status, go to: ***Status >> System***.

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

System Setting Overview		
Firmware Version		1.00.01
Build		1.5-1.4418.2.7
Site		EN-AU
System Name		HS1100N
Portal URL		http://www.netcomm.com.au/
Primary SYSLOG Server		N/A:N/A
Secondary SYSLOG Server		N/A:N/A
Warning of Internet Disconnection		Normal
User Log	**Retained Days**	3 days
	Receiver E-mail Address(es)	N/A
System Time	**NTP Server**	0.netcomm.pool.ntp.org
	Time	2011/07/15 16:38:11 +1000
User Session Control	**Idle Time Out**	10 Min(s)
	Multiple Login	Disabled
DNS	**Preferred DNS Server**	
	Alternate DNS Server	

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

Item		***Description***
Firmware Version		The present firmware version of the HS1100N
System Name		The system name. The default is HS1100N
Portal URL		The page the users are directed to after initial login success.
SYSLOG server- System Log		The IP address and port number of the external SYSLOG Server. **N/A** means that it is not configured.
SYSLOG server- On-demand Users Log		The IP address and port number of the external SYSLOG Server. **N/A** means that it is not configured.
Warning of Internet Disconnection		Show whether the status for the WAN connection is normal or disconnected (**Internet Connection Detection**) and whether online users are allowed/disallowed to log in the network.
User Log	**Retained Days**	The maximum number of days for the system to retain the users' information.
	Receiver Email Address (es)	The email address to which the user log information will be set.
System Time	**NTP Server**	The network time server that the system is set to synchronise against.
	Time	The system time is shown as the local time.
User Session Control	**Idle Time Out**	The minutes allowed for the users to be inactive before their account expires automatically.
	Multiple Login	Enabled/disabled stands for the current setting to allow/disallow multiple login from the same local account.
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

11.1.2 Interface Status

To view the Interface Status, go to: ***Status >> Interface***.

This section provides an overview of the interface for the administrator including **WAN**, **Zone Wireless General Settings**, **Zone - Private** and **Zone - Public**.

WAN		
General	MAC Address	00:1F:D4:00:7E:62
	IP Address	
	Subnet Mask	255.255.255.0
	Packets Out	3251
	Bytes Out	502256
	Packets In	17940
	Bytes In	3162100
	Number of Sessions	23

Zone Wireless General Settings		
General	MAC Address	00:1F:D4:00:7E:64
	Band	11ng
	Channel	6
	Transmit Power	14 dBm

Zone - Private		
General	Mode	NAT
	MAC Address	00:1F:D4:00:7E:63
	IP Address	192.168.110.1
	Subnet Mask	255.255.255.0
DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.110.2
	End IP Address	192.168.110.100
	Lease Time	1440 Min(s)
VAP 1	BSSID	00:1F:D4:00:7E:64
	ESSID	NetComm_HS1100N_2
	Security Type	WPA-PSK
	Associated Clients	0

Zone - Public		
General	Mode	NAT
	MAC Address	00:1F:D4:00:7E:63
	IP Address	192.168.11.254
	Subnet Mask	255.255.255.0
DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.11.1
	End IP Address	192.168.11.100
	Lease Time	1440 Min(s)
VAP 2	BSSID	06:1F:D4:00:7E:64
	ESSID	NetComm_HS1100N
	Security Type	None
	Associated Clients	0

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.
	Packets Out/In	The total accumulated packets in/out through this WAN port since the gateway was booted up. The delta shows the difference between the numbers from last time this Interface Status page was visited.
	Bytes Out/In	The total accumulated bytes in/out through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
	Number of Sessions	The number of concurrent WAN port sessions.
Zone Wireless General Settings	**MAC Address**	The MAC address of the Wireless interface.
	Band	The current Band setting of Wireless interface.
	Channel	The current Channel setting of Wireless interface.
	Transmit Power	The current Transmit Power setting of Wireless interface.
Zone - General	**Mode**	The operation mode of the zone.
	MAC Address	The MAC address of the zone.
	IP Address	The IP address of the zone.
	Subnet Mask	The Subnet Mask of the zone.
Zone - DHCP	**Status**	Enable/disable stands for status of the DHCP server in this zone
	WINS IP Address	The WINS server IP from the 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	Minutes of the lease time for the DHCP IP address.
Zone - VAP	**BSSID**	The BSSID of this zone.
	ESSID	The ESSID of this zone.
	Security Type	The current security type of this zone.
	Associated Clients	The number of associated clients in this zone.

11.1.3 Routing Table

To view the System Status, go to: ***Status >> Routing Table***.

All the **Policy** Route rules and **Global Policy** Route rules will be listed here. Also it will show the **System** Route rules specified by each interface.

Policy 1			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Policy 2			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Policy 3			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Policy 4			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Policy 5			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Global Policy			
Destination	**Subnet Mask**	**Gateway**	**Interface**

System			
Destination	**Subnet Mask**	**Gateway**	**Interface**
192.168.110.0	255.255.255.0	0.0.0.0	Private
192.168.11.0	255.255.255.0	0.0.0.0	Public
10.22.0.0	255.255.0.0	0.0.0.0	WAN
0.0.0.0	0.0.0.0	10.22.0.1	WAN

- **Policy 1~5:** Shows the information of the individual Policy from 1 to 5.
- **Global Policy:** Shows the information of the Global Policy.
- **System:** Shows the current system routing table.
  - **Destination:** The Destination IP address.
  - **Subnet Mask:** The Subnet Mask of the IP address range.
  - **Gateway**: The Gateway IP address of the interface.
  - **Interface:** Including **WAN**, **Private** and **Public**.

11.1.4 Current Users

To view the Current Users, go to: ***Status >> Online Users***.

In this page, each online user's information including **Username**, **IP Address**, **MAC Address**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Idle** and **Kick Out** will be shown. Administrators can disconnect a specific online user by clicking the **Kick Out** hyperlink. Click **Refresh** to update the current users list.

11.1.5 User Log

To view the User Log, go to: ***Status >> User Log***.

This page is used to check the traffic history of the HS1100N. The history of each day will be saved separately in memory 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 last 2 calendar months.

User Log	
Date	**Size (Byte)**
2009-04-22	65
2009-04-23	65

On-demand User Log	
Date	**Size (Byte)**
2009-04-22	105
2009-04-23	254

Roaming Out User Log	
Date	**Size (Byte)**
2009-04-22	106
2009-04-23	106

Roaming In User Log	
Date	**Size (Byte)**
2009-04-22	112
2009-04-23	112

Monthly Network Usage of Local User		
Month	**No. of Entries**	**Usage Data**
2009-04	1	Download

Caution:
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 **Receiver E-mail Address(es)** has been entered under the **E-mail & SYSLOG** page, the system will automatically send this historicalinformation to that specified email address.

- **Primary User Log**

  All user activities occuring on the system within the last 72 hours excluding other user logs such as on-demand user log are recorded; in date and time order. 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 users' activities.

- **On-demand User Log**

  Each line is an on-demand user log record consisting of 14 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, Activation Time, 1st Login Expiration Time**, and **Remark**, of on-demand users' activities.

- **Roaming Out User Log**

  Each line is a roaming out traffic history record consisting of 14 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of users' activities.

- **Roaming In User Log**

  Each line is a roaming in traffic history record consisting of 15 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of users' activities.

11.1.6 Local User Monthly Network Usage

To view the Local User Monthly Network Usage, go to: ***Status >> User Log***.

- **Monthly Network Usage of Local User**

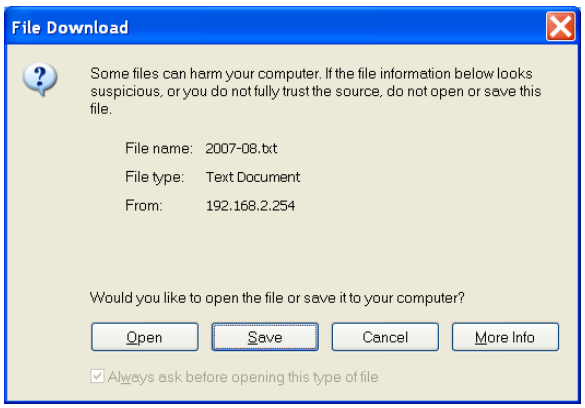
  The system keeps a cumulated record of the traffic generated by each Local user in the last 2 calendar months. Each line in a monthly network usage of local user record consists of 6 fields, **Username**, **Connection Time Usage**, **Packets In**, **Bytes In**, **Packets Out** and **Bytes Out** of users' activities.

  - **Username:** Username of the local user account.
  - **Connection Time Usage:** The total time used by the user.
  - **Pkts In/ Pkts Out:** The total number of packets received and sent by the user.
  - **Bytes In/ Bytes Out:** The total number of bytes received and sent by the user.

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

Monthly Network Usage of Local User		
Month	**No. of Entries**	**Usage Data**
2009-04	1	Download

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



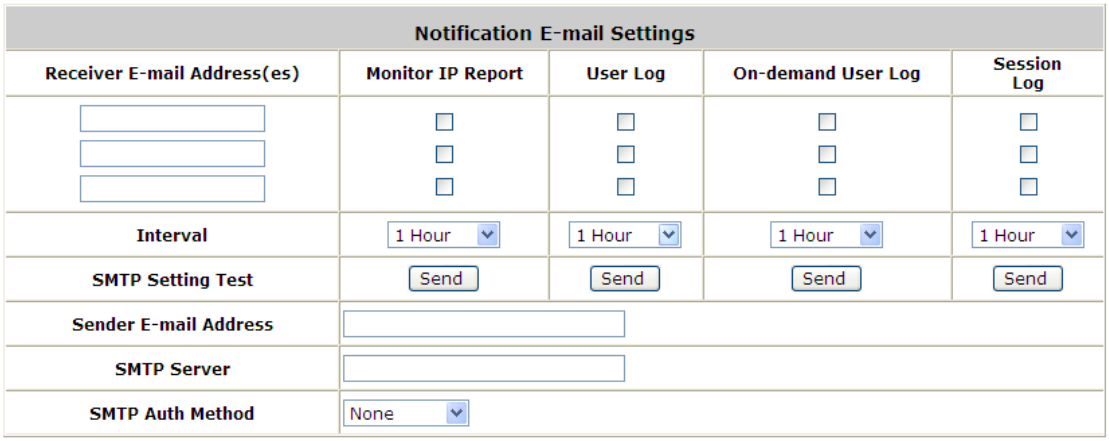
11.2 Notification

Configure Notification, go to: ***Status >> E-mail & SYSLOG***.

The HS1100N can automatically send the notification of **Monitor IP Report**, **Users Log**, **On-demand User Log** and **Session Log** to up to 3 particular e-mail addresses. A trial email is provided by the system for validation. Secondly, the system supports recording of **System Log**, **On-demand Users Log**, **Session Log** and **HTTP Web Log** via external SYSLOG servers.
Thirdly **Session Log** and **HTTP Web Log** can also be configured to be sent to an external FTP server. In addition, **Event Log** section on WMI displays of clients associate and disassociate messages.

11.2.1 E-Mail

To configure Email Notification, go to: ***Status >> E-mail & SYSLOG***.



- **Notification E-mail Settings:**
  - **Receiver Email Address (es):** Up to 3 e-mail address can be set up to receive the notification. These are the receiver's e-mail addresses. There are four kinds of notification to selection -- Monitor IP Report, Users Log, On-demand Users Log and Session Log, check the selection box to choose the type of notification to be sent.
  - **Interval:** The time interval to send the e-mail report.
  - **SMTP Setting Test:** To test the settings immediately.
  - **Sender Email Address:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
  - **SMTP Server:** The IP address of the sender's SMTP server.
  - **SMTP Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method selected, enter the **Account Name**, **Password** and **Domain**.
    - **NTLMv1** is not currently available for general use.
    - **Plain** and **CRAM-MD5** are standardized 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 which method to be used cannot be configured.

Notification E-mail Settings				
Receiver E-mail Address(es)	**Monitor IP Report**	**User Log**	**On-demand User Log**	**Session Log**
Interval	1 Hour	1 Hour	1 Hour	1 Hour
SMTP Setting Test	Send	Send	Send	Send
Sender E-mail Address				
SMTP Server				
SMTP Auth Method	None			

11.2.2 SYSLOG

- **SYSLOG Server Settings:** There are 4 types of SYSLOG supported: **System Log**, **On-demand User Log**, **Session Log**, and **HTTP Web Log**. Enter the IP address and Port number to specify the SYSLOG server where the report should be sent to.

  Except for System Log, each supported log may be assigned *Tag* info as well as SYSLOG standard attributes *Severity* and *Facility* to meet the filtering requirements on the SYSLOG Server. HTTP Web Log can further select which Service Zone Web interface information to log. For each type of log information, whenever an incident occurs and data is updated, the updated log will be immediately sent to the configured SYSLOG server.

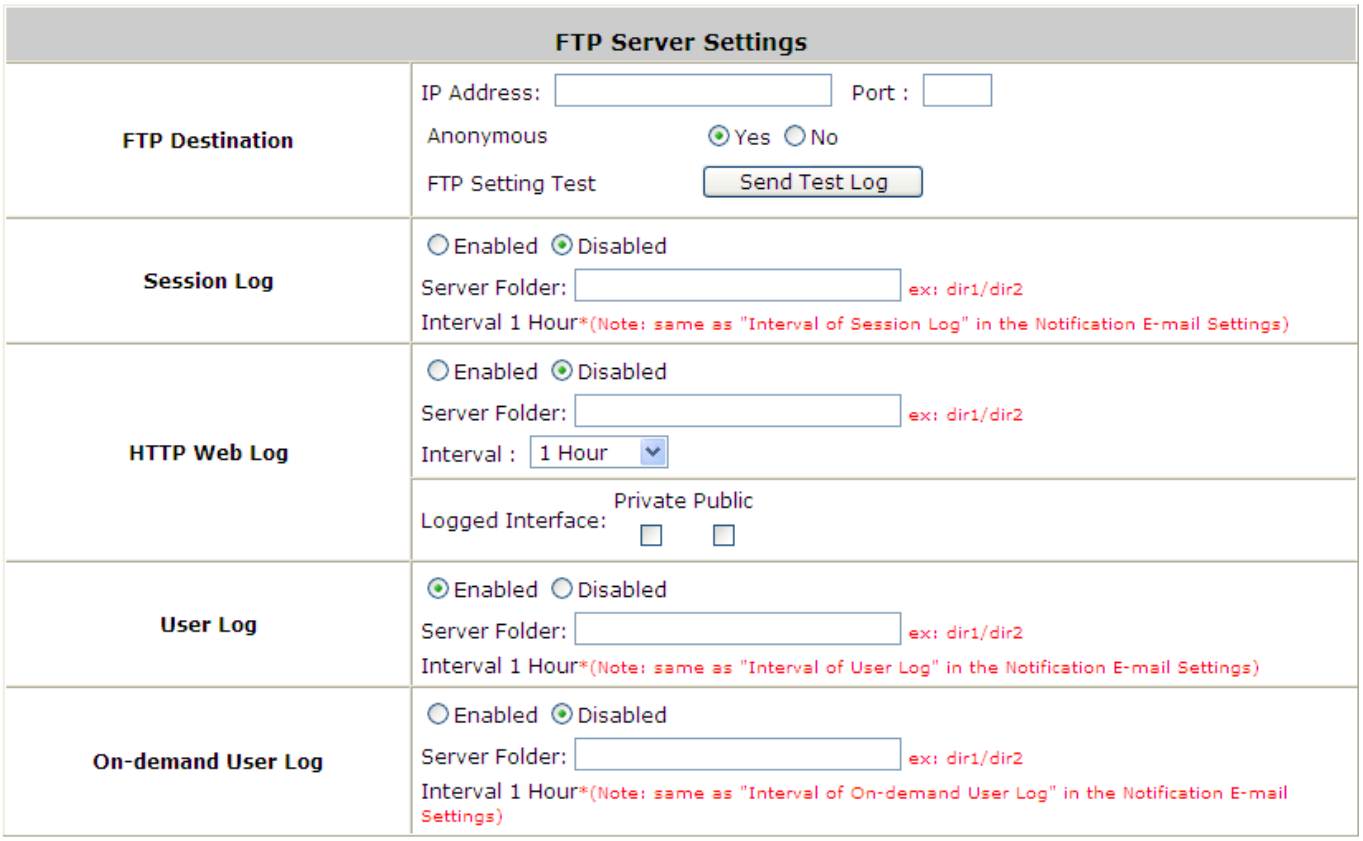
SYSLOG Server Settings	
SYSLOG Destinations	SYSLOG Server 1 IP Address: Port : SYSLOG Server 2 IP Address: Port :
System Log	Enabled Disabled
On-demand User Log	Enabled Disabled Tag: Severity: Emergency Facility: local0
Session Log	Enabled Disabled Tag: Severity: Emergency Facility: local0
HTTP Web Log	Enabled Disabled Tag: Severity: Emergency Facility: local0
	Logged Interface: Private Public

Note:

When the number of a user's session (TCP and UDP) reaches the session limit specified in the policy, a record will be logged to this SYSLOG server.

11.2.3 FTP

This configuration page allows the setting of FTP Server to send, including the types of Session Log, HTTP Web Log, User Log or On-demand User Log based on Server Folder and Interval.



- **FTP Server Settings**

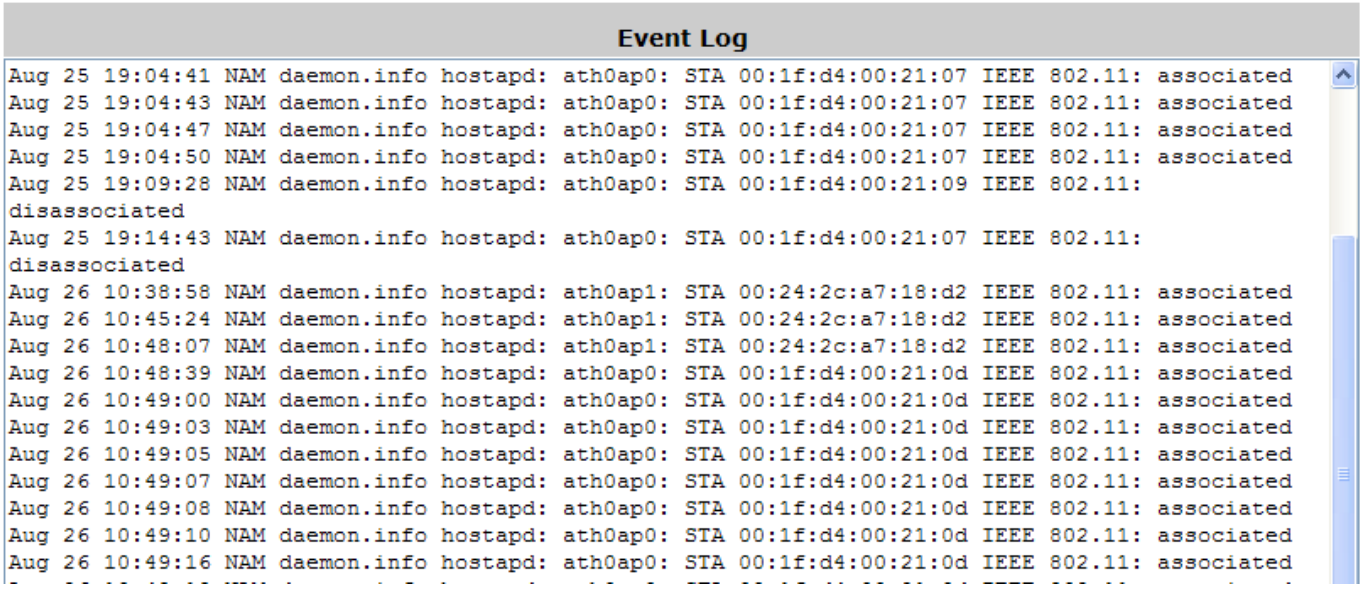
  FTP Destination: Configures the common settings of the FTP server that the logs will be sent to which includes the following:

  - **IP Address/Port:** IP address and port number of FTP server.
  - **Anonymous:** Check option “Yes” if the FTP server does not need ID credentials, otherwise check option “No” and fill in the necessary *Username* and *Password*.
  - **FTP Setting Test:** To test the FTP settings correct or not.
  - **Session Log:** Log each connection created by users and tracking the source IP/Port and destination IP/Port. Session Log will be sent to the FTP server automatically during every defined interval in Session Log email notification. Session Log allows uploading the log file to a FTP server periodically. The maximum log file size is 256K. The log file also will be sent to the FTP server once the file size reaches its maximum size.
  - **Enable:** Decide whether or not to send Session Log file to the FTP Server configured in **FTP Destination**.
  - **Server Folder:** The folder in the configured FTP Server in which the sent Log will be placed.
  - **HTTP Web Log:** Records the URL of websites visited by users accessing the internet via The HS1100N to a specific FTP server.

- **Enable:** Decide whether or not to send HTTP Web Log file to the FTP Server configured in **FTP Destination**.
- **Server Folder:** The folder in the configured FTP Server in which the sent Log will be placed.
- **Interval:** The time interval at which the Log will be sent.
- **Logged Interface:** The check box of Public or Private shall be checked to enable logging the HTTP Web Log of this interface.
- **User Log:** Records the User Log of the system to a specific FTP server.
- **Enable:** Decide whether or not to send User Log file to the FTP Server configured in **FTP Destination**.
- **Server Folder:** The folder in the configured FTP Server in which the sent Log will be placed.
- **On-demand User Log:** Records the On-demand User Log of the system to a specific FTP server.
- **Enable:** Decide whether or not to send On-demand User Log to the FTP Server configured in **FTP Destination**.
- **Server Folder:** The folder in the configured FTP Server in which the sent Log will be placed.

11.2.4 Event Log

Event Log: The Event Log provides the system activities records. The administrator can monitor the system status by checking this log.



In the log, normally, each line represents an event record which includes these fields:

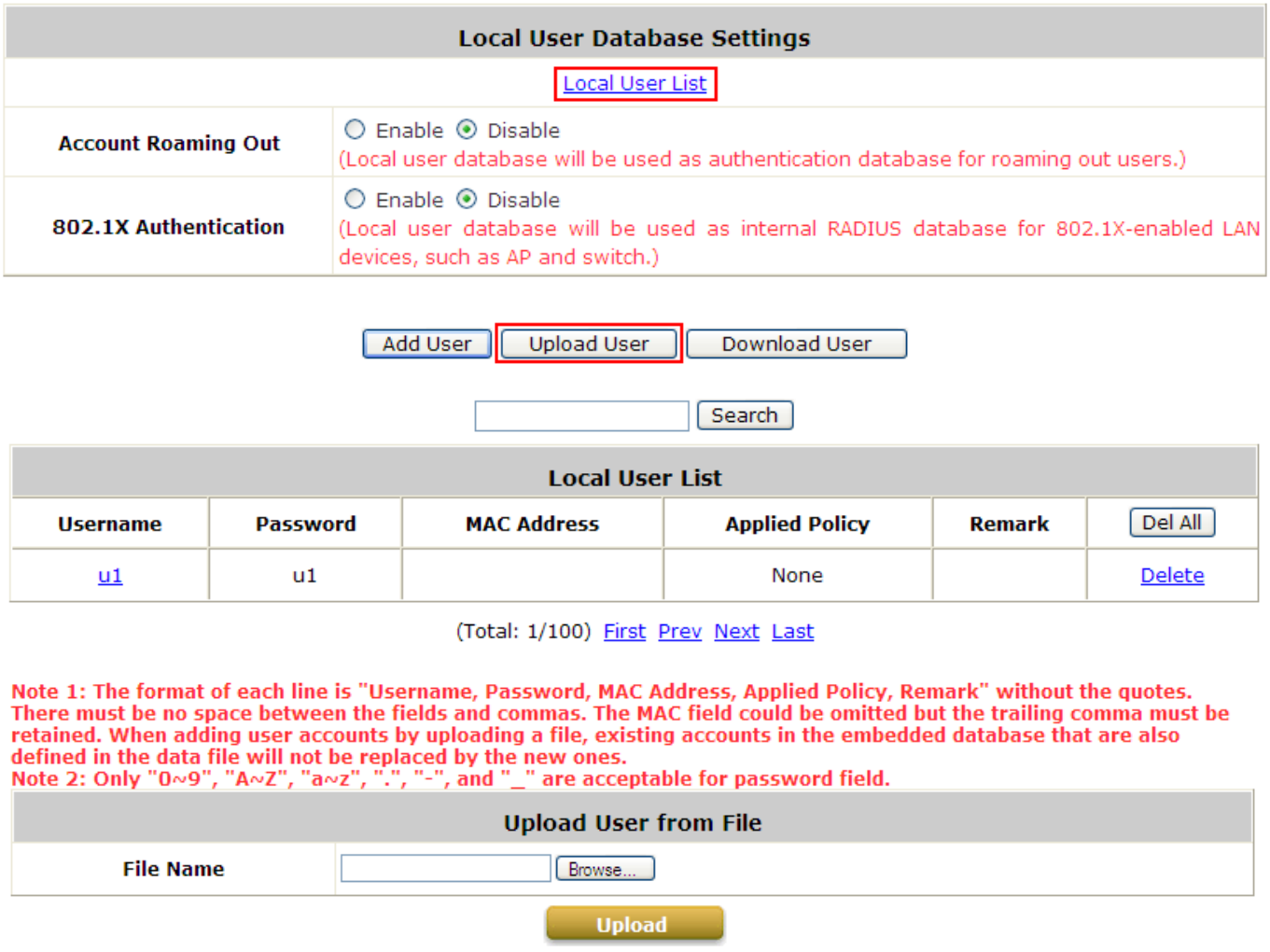
- **Date/Time:** The time & date when the event happened
- **Hostname:** Indicate which host records this event. Note that all events in this page are local event, so the hostname in this field are all the same.
- **Process name:** Indicate the event generated by the running instance.
- **Description:** Description of this event.

12 Advanced Applications

12.1 Upload/Download Local Users Accounts

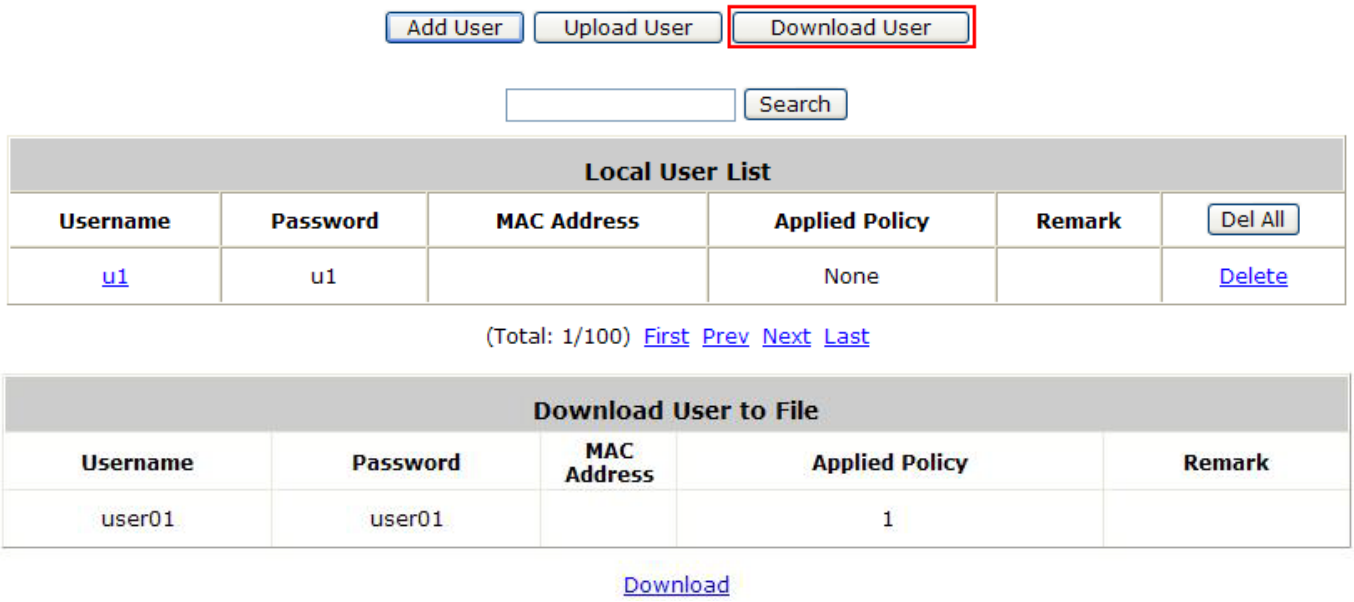
To Upload / Download Local Users Accounts, go to: ***Users >> Authentication,*** click ***Configure*** button of ***Local***. Or click ***Quick Links >> Local User Management*** from system Home page.

- **Upload User:** Click **Upload User** to enter the **Upload User from File** interface. Click the ***Browse*** button to select the text file for uploading user accounts, then click **Upload** to complete the upload process.



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.

- **Download User:** Use this function to create a .txt file with all ***Local*** user account information and then save it on disk.



12.2 RADIUS Advanced Settings

To configure RADIUS Advanced Settings, go to: ***Users >> Authentication***. Click ***Configure*** of ***RADIUS***.

- **Complete vs. Only ID**

For RADIUS authentication, there is an option to send the complete username with postfix or username only.

Username Format: When **Complete** option is checked, both the username and postfix will be transferred to the RADIUS server for authentication. On the other hand, when **Only ID** option is checked, only the username will be transferred to the external RADIUS server for authentication.

- **NAS Identifier**

System will send this value to the external RADIUS server, if the external RADIUS server needs this.

- **NAS Port Type**

System will send this value to the external RADIUS server, if the external RADIUS server needs this.

- **Class-Policy Mapping**

This function is to assign a *Policy* to a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes log into the system via the RADIUS server, each client will be mapped to its assigned Policy.

RADIUS Policy Mapping - Server 2

○ Enable ◉ Disable

No.	Class Attribute Value	policyName	Remark
1		Policy 1	
2		Policy 1	
3		Policy 1	
4		Policy 1	
5		Policy 1	

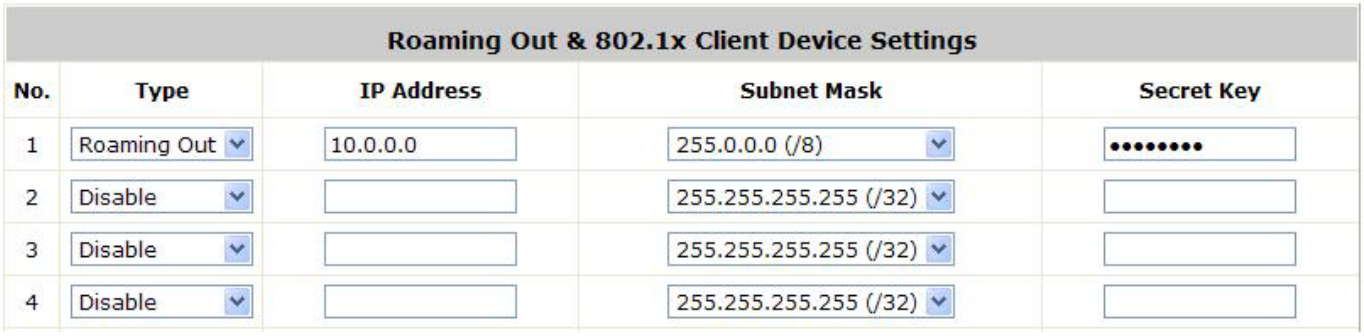
12.3 Roaming Out

To configure local user Roaming Out, go to: ***Users >> Authentication,*** *click* ***configure*** *of* ***Local***.

Under certain configurations, The HS1100N can act as a RADIUS server for Roaming Out local user logged from other system. The Local User database will act as the RADIUS user database.

- **Account Roaming Out & 802.1X Authentication:** When Account Roaming Out is enabled; the link of *Roaming Out & 802.1X Client Device Settings* will be available to define the client device authorized to roam by entering the IP address, Subnet Mask, and Secret Key.

Local User Database Settings	
Local User List	
Account Roaming Out	◉ Enable ○ Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	○ Enable ◉ Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
Roaming Out & 802.1X Client Device Settings	



Roaming Out & 802.1x Client Device Settings				
No.	**Type**	**IP Address**	**Subnet Mask**	**Secret Key**
1	Roaming Out	10.0.0.0	255.0.0.0 (/8)	••••••••
2	Disable		255.255.255.255 (/32)	
3	Disable		255.255.255.255 (/32)	
4	Disable		255.255.255.255 (/32)	

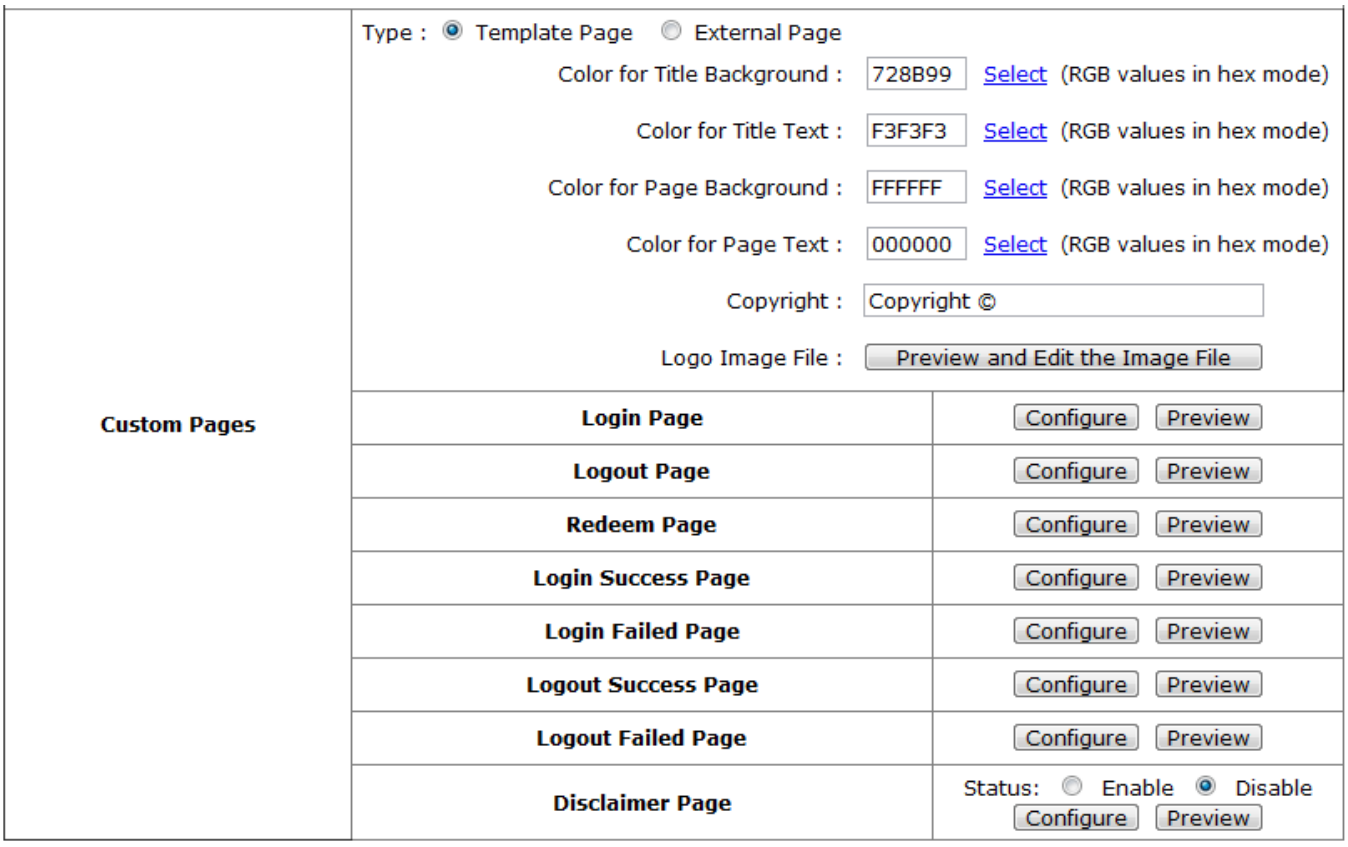
Click the hyperlink ***Roaming Out & 802.1x Client Device Settings*** to enter the ***Roaming Out & 802.1X Client Device Settings*** interface. Choose **Roaming Out** and key in the Roaming Out client's IP address and network mask and then click ***Apply*** to complete the settings.

In the other system, such as another The HS1100N, setup it's RADIUS server to this HS1100N with same postfix, then the local user in this HS1100N can login success from another HS1100N by RADIUS authentication.

12.4 Customizable Pages

Configure Custom Pages, go to: ***System >> Zone Configuration,*** *click* ***Configure*** *in* ***Public*** *zone*.

There are several user login and logout pages that can be customized by the administrator.
You can select **Template Page** or **External Page**.



- **Template Page:**
  To utilise the template user pages stored locally in the system, choose ***Template Page*** and configure the necessary settings as follows. Click ***Select*** hyperlink to pick up a colour for each item and then fill in your copyright message. You can also upload a Logo image file for your template with the ***Preview and Edit the Image File*** button. Click the button of ***Configure***, the setup page will appear for the corresponding page where you can change the text displayed as you wish. After finishing the setting, click ***Preview*** to see the result. If you are happy with the customized pages, click ***Apply*** to activate the changes made.

- **Disclaimer Page**:

  The **Disclaimer Page** is for the hotspot owner or IT staff who want to display a ‘terms of use” or an announcement before the user login page. Click the button for ***Configure*** *and* the setup page will appear. An unauthorized client will receive a disclaimer page once opening the web browser. If a client selects “I agree” and clicks “Next,” then he or she will proceed to the User Login Page for client to login with username and password.

- **External Page:**

  Choose the ***External Page*** option if you wish to use other pages located on a designated website. Click the button to ***Configure*** for each custom pages and enter the URL of its’ corresponding external login page and then click ***Apply***.

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

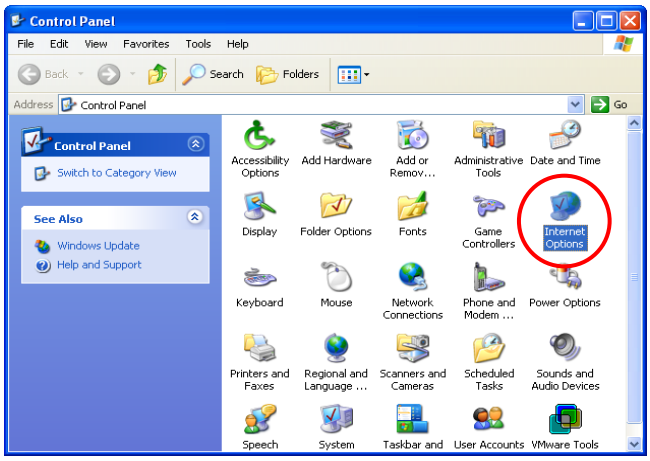
Appendix A. Network Configuration on PC & User Login

▪ Network Configuration on PC

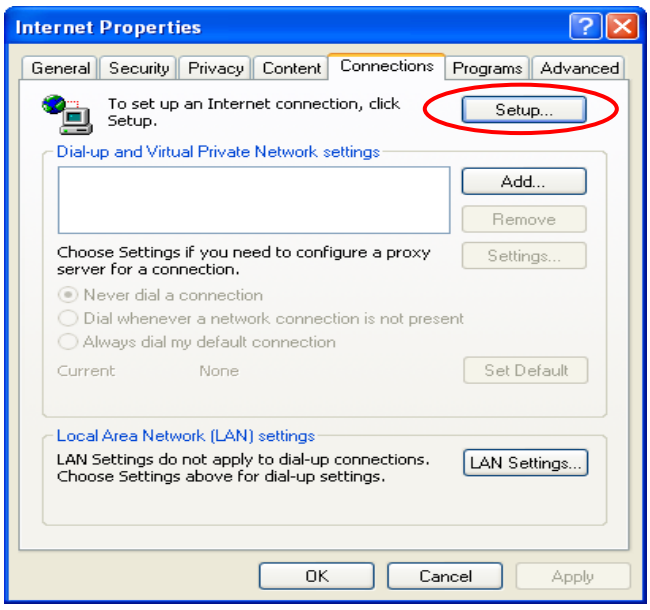
After The HS1100N is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**
  - **Windows XP**

1) Choose **Start** >> **Control Panel** >> **Internet Option**.

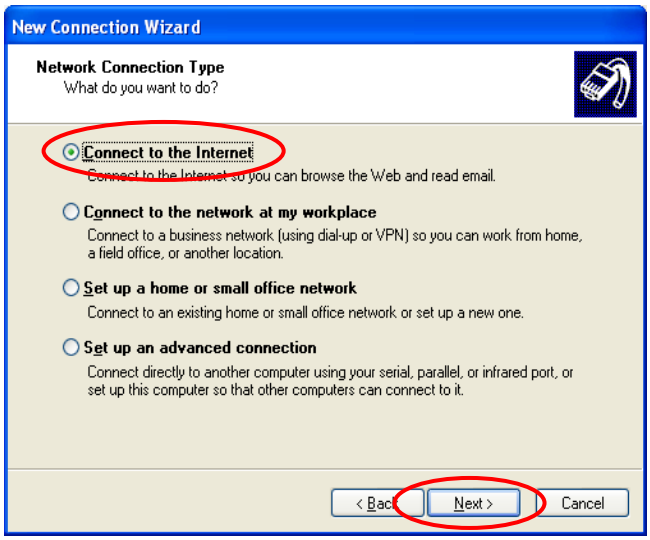


2) Choose the **Connections** tab, and then click ***Setup***.

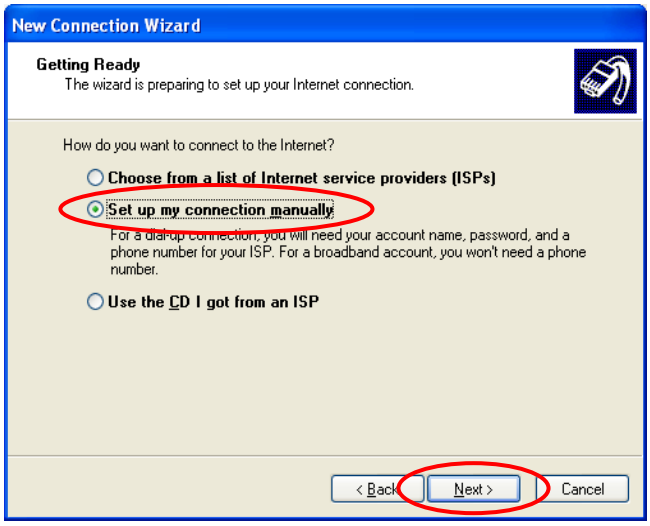


3) When the **Welcome to the New Connection Wizard** window appears, click ***Next***.

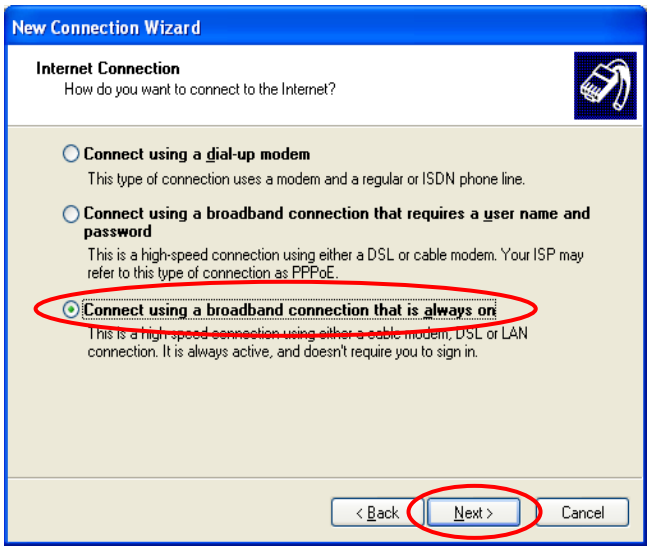
4) Choose **"Connect to the Internet"** and then click ***Next***.



5) Choose **"Set up my connection manually"** and then click ***Next***.



6) Choose **"Connect using a broadband connection that is always on"** and then click ***Next***.



7) Finally, click ***Finish*** to exit the **Connection Wizard**. Now, the setup is completed.

- **TCP/IP Network Setup**

  If the operating system of the computer 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, the HS1100N DHCP function will automatically assign an appropriate IP address and related information for each PC.

Appendix B. Policy Priority

▪ Global Policy, Authentication Policy and User Policy

The HS1100N supports multiple Policies, including one **Global Policy** and 5 individual **Policies** which can be assigned to different **Authentication Servers**. The **Global Policy** is the system's universal policy and is applied to all clients, while other individual Policy can be selected and defined to be applied to any Authentication Server. For some authentication, such as Local and RADIUS, users can be assigned to different Policy individually. So one user may be applied different policies at the same time. Which policy is actually then applied to this user?

The Policy Priority are enforced as follows:

User Policy >> Authentication Policy >> Global Policy

Now, let us discus different user policy type:

- For Local and RADIUS, the users can be assigned to different Policy individually. For example, a Local user, user01, is assigned to Policy1 and the Local Authentication is assigned to Policy2. Then user01 login to Public Zone will get Policy1. This is a common case for users that can assign Policy individually.
- For Local and RADIUS, if these users are not assigned any User Policy individually, they will be the same as other users within the same authentication server. For example, a Local user, user01, the Local Authentication is assigned to Policy3. Then user01 login to Public Zone will get Policy3. This is another common case for users that is assigned Policy by the authentication server.
- If User is not assigned a Policy individually and the authentication server is also not assigned a Policy, then the users will be applied the Global Policy. For example, a Local user, user01, is assigned to *None* Policy and the Local Authentication is also assigned to *None Policy* in User list. Then user01 logging to Public Zone will be applied with the Global Policy.

As a conclusion, the Global Policy has the lowest policy priority; on the other hand, the User Policy has the highest one.

Appendix C. WDS Management

The Public Zone of the HS1100N supports up to 2 WDS links. WDS (Wireless Distribution System) is a function used to connect APs (Access Points) wirelessly to extend wireless coverage. The WDS management function of the system can help administrators to setup two WDS links.

To configure WDS, go to: ***System >> Zone Configuration,*** *click* ***Configure*** *in* ***Public*** *zone*.

Zone Settings				
Name	**ESSID**	**Wireless Security**	**Default Authen Option**	**Details**
Private	NetComm_HS1100N_2	WPA-PSK	N/A	Configure
Public	NetComm_HS1100N	None	On-demand User	Configure

WDS (Wireless Distribution System) is a function used to connect **AP**s (Access Points) wirelessly. The WDS management function of the system can help administrators to setup two WDS links.

WDS1 Settings : Public		
Basic	WDS Status :	Enable Disable
	MAC Address of Remote AP :	
Security	Security Type :	None

WDS2 Settings : Public		
Basic	WDS Status :	Enable Disable
	MAC Address of Remote AP :	
Security	Security Type :	None

- **WDS Status:** Select ***Enable*** to active this WDS link.
- **MAC Address of Remote AP:** Enter the MAC of the remote AP that create WDS link with The HS1100N.
- **Security Type:**
  - **WEP: WEP Key Length** may be *64 bits*, *128 bits* or *152 bits*; and **WEP Key Format** can be *ASCII* or *HEX*. Lastly, enter the **WEP Key**.
  - **WPA-PSK:** Select the preferred ciphering method, *TKIP* or *AES* and enter the **PSK / Pass-phrase**.

Appendix D. RADIUS Accounting

This section will briefly introduce the basic configuration of RADIUS server to work with VSA for the purpose to control the maximum client volume usage (upload; download or upload + download traffic).

This **VSA** will be sent from RADIUS server to gateway along with an **Access-Accept** packet. In other words, when the external RADIUS server accepts the request, it will reply not only an **Access-Accept** but also a maximum value in bytes each user is allowed to transfer. This value can be the maximum upload traffic, the maximum download traffic, or the sum of the download and upload traffics in bytes per user. Gateway will check this value every minute; if the user traffics reach this value, gateway will stop the session of this user and send a “Stop” to RADIUS server.

1. Description

VSA is designed to allow vendors to support their own extended Attributes not covered in common attributes. It MUST not affect the operation of the RADIUS protocol.

The **Attribute Type** of VSA is “26” and the “**Vendor ID**” should be determined before proceeding to RADIUS configuration; in this example; the **Vendor ID** is “21920”. “**Attribute Number**” and “**Attribute Value**” can then be designed to provide additional control over RADIUS.

Attribute Name	Attribute Number	Attribute Value
HS1100N-Byte-Amount	10	To be defined by administrator for different user group
HS1100N-MaxByteIn	11	To be defined by administrator for different user group
HS1100N-MaxByteOut	12	To be defined by administrator for different user group
HS1100N-Byte-Amount-4GB	20	To be defined by administrator for different user group
HS1100N-MaxByteIn-4GB	21	To be defined by administrator for different user group
HS1100N-MaxByteOut-4GB	22	To be defined by administrator for different user group

If the amount of traffics is larger than 4 GB, the attributes of “XXXX-4GB” will be used. For example, if the amount is 5 GB, the following settings should be set: “HS1100N-Byte-Amount = 1048576” and “HS1100N-Byte-Amount-4GB = 1”.

On the other hand, when the administrator fills in all attributes, the user will be kicked out from system if any condition is reached. For example, if the administrator sets “HS1100N-Byte-Amount = 1048576”; “HS1100N - MaxByteIn = 1048576” and “HS1100N- MaxByteOut = 1048576”, the user will be kicked out from system when the downlink, uplink, or total traffic exceeds the limit.

2. VSA configuration in RADIUS server (IAS Server)

This section will guide you through a VSA configuration in your external RADIUS server. Before getting started, please access your external RADIUS server’s desktop directly or remotely from other PC.

Step 1

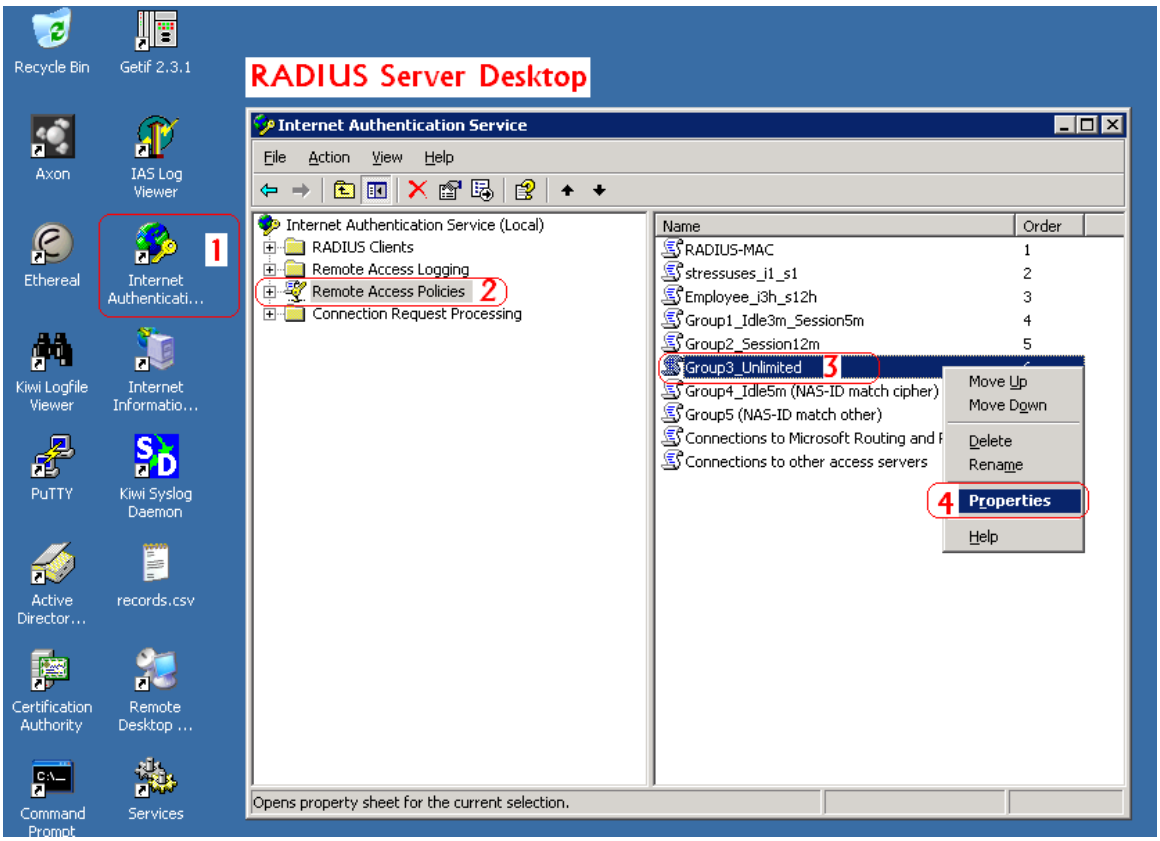
Confirm the following key elements in RADIUS server: users, groups, and policies.

- Verify whether there are already **users** in RADIUS Server.
- Verify whether there are already **Groups** and assigned **users** belonging to these **Groups** in RADIUS Server.
- Verify whether there are already **Policies** and assigned **Groups** belonging to these **Policies** in RADIUS Server.

Step 2

Run “Internet Authentication Server” and open “Remote Access Policies”

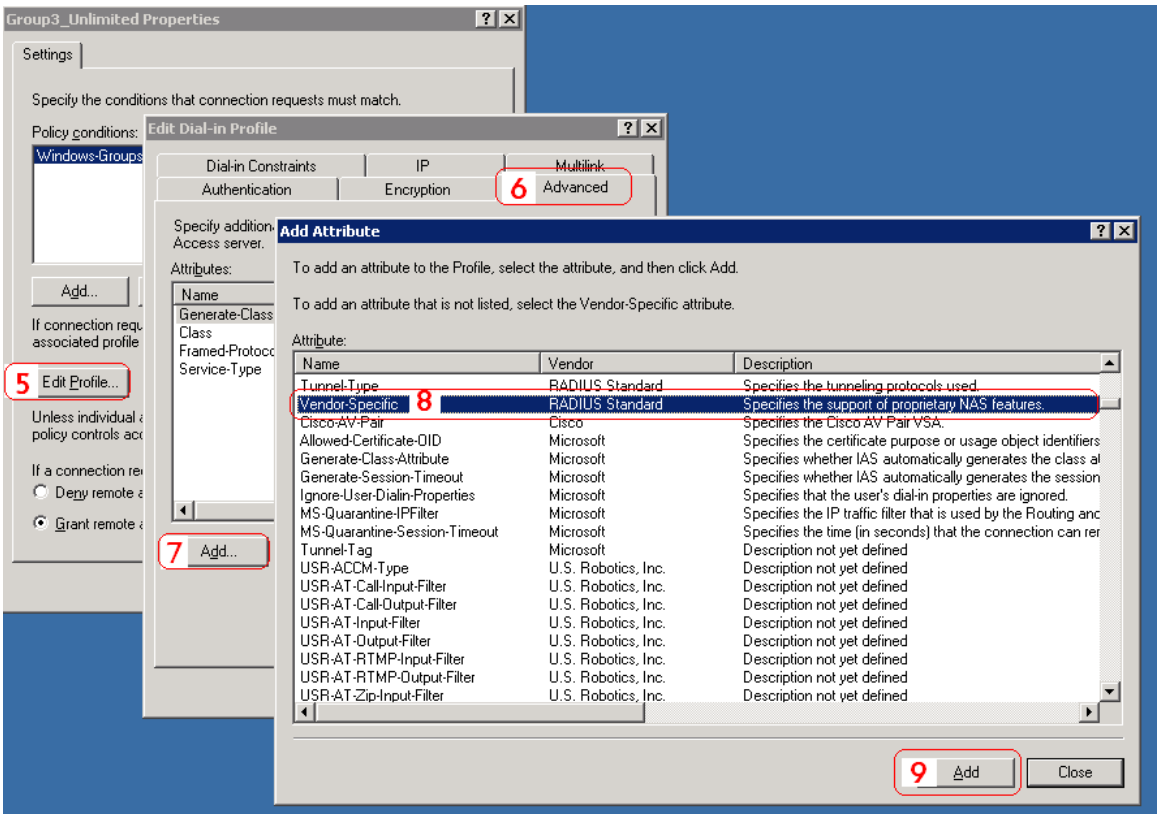
Select a **Policy** with right click and scroll down to its **Properties** page



Step 3

Click **Edit Profile and** select the **Advanced** Tag.

Click **Add** to add a new **Vendor-specific** attribute.



Step 4

Add a new attribute under **Vendor-specific**

Set “**Vendor Code = 21920**”.

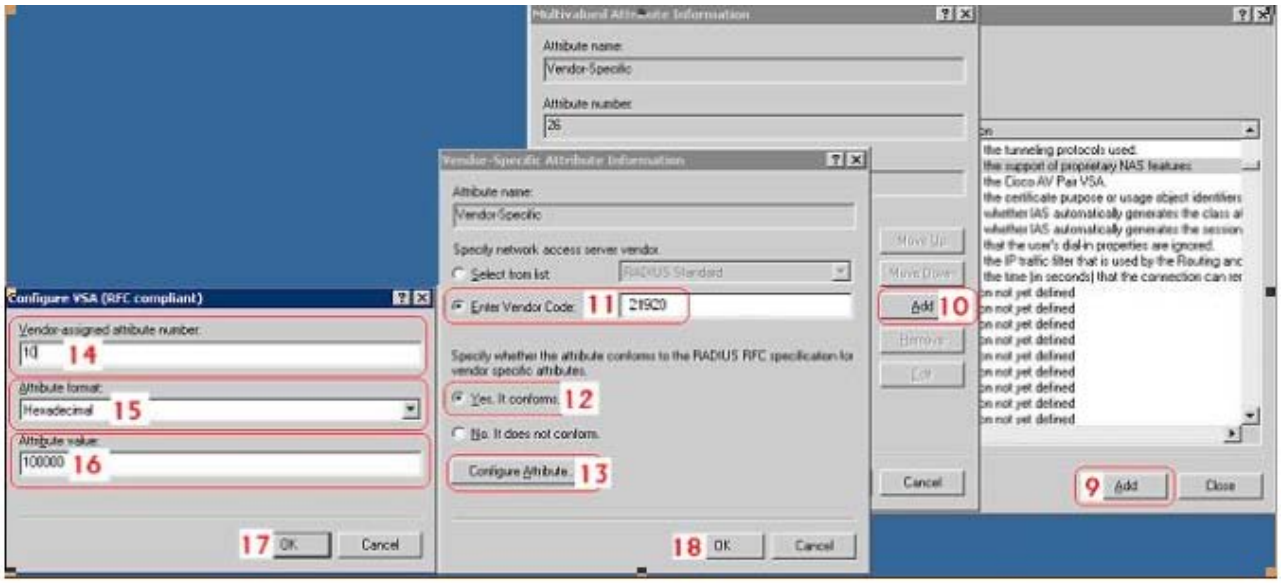
Check **Yes** to conform to the RADIUS RFC.

Click **Configure Attribute** to proceed.

Set **“Vendor-assigned attribute number = 10”**

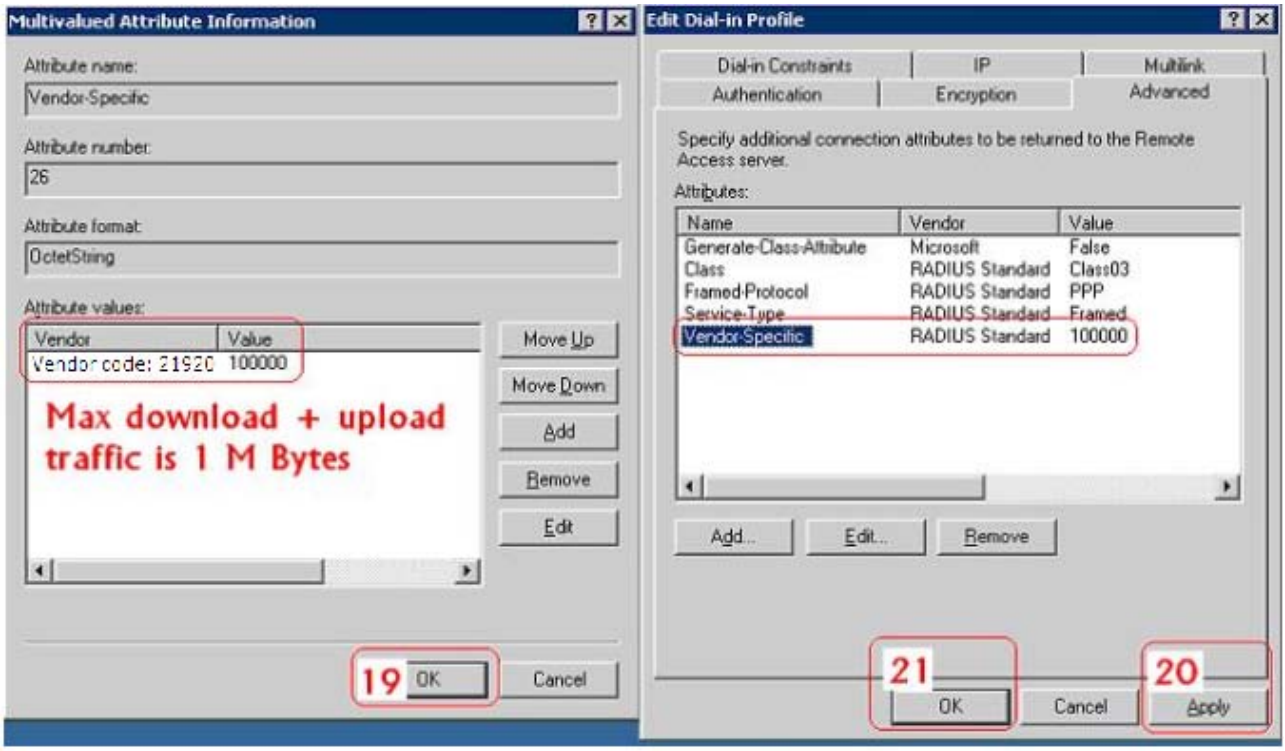
Select **“Attribute format = Hexadecimal”**

Set **“Attribute Value = 1000000”**



Step 5

Confirm whether the **Vendor-specific Attribute** has been added successfully

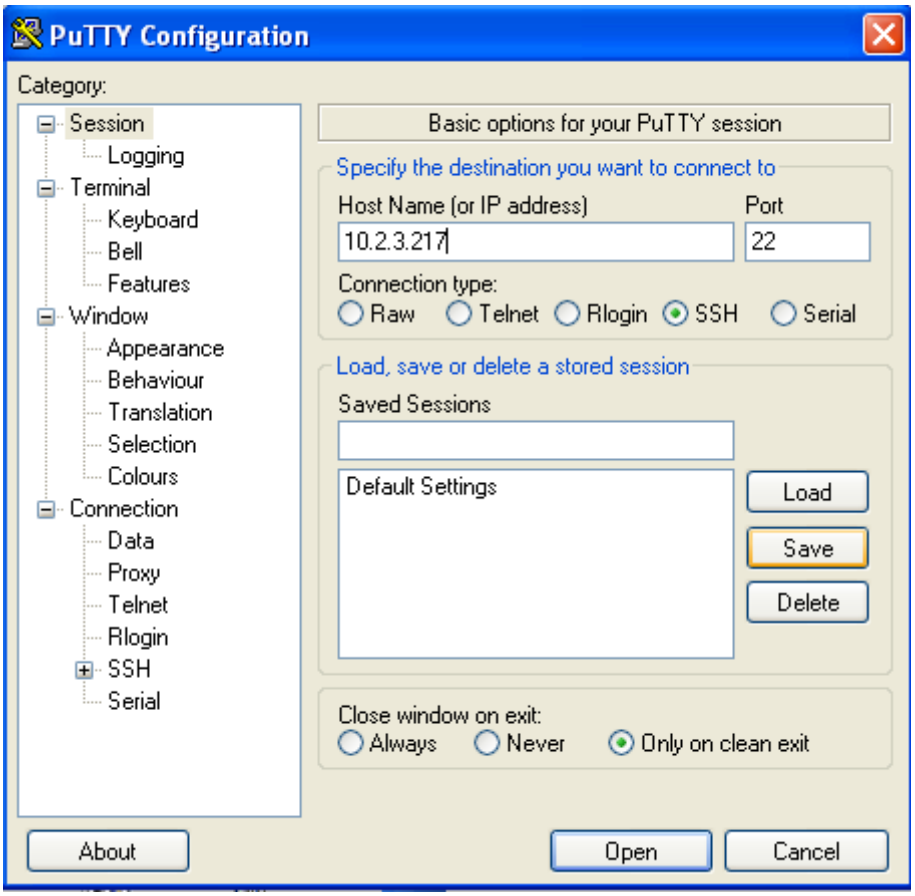


Step 6

Follow the same steps to create another **Vendor-specific Attribute** if needed.

3. VSA configuration in RADIUS server (FreeRADIUS)

This section will guide you through **VSA** configuration with FreeRADIUS v1.0.5 running on “Fedora”. Before getting started, open the shell of RADIUS server; for example, use *Putty* to access the Linux host:



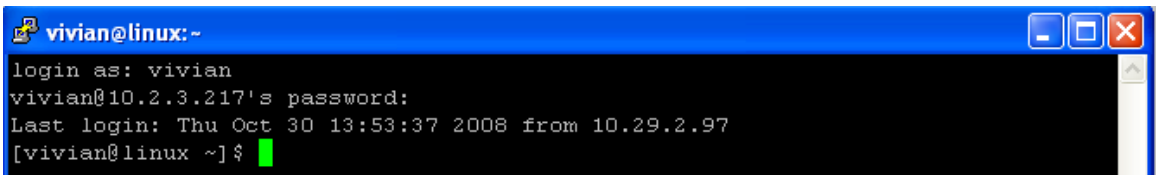
Step 1

Confirm the following key elements in RADIUS server: users, groups

- Verify whether there are already **users** in RADIUS Server.
- Verify whether there are already **Groups** and assigned **users** belonging to these **Groups** in RADIUS Server.

Step 2

Log in the Linux host of the RADIUS server.



Step 3

Create a file “dictionary.HS1100N” under the “freeradius” folder.

```
[vivian@linux ~]$ vi /usr/share/freeradius/dictionary.
```

Step 4

Edit and save the contents of the file “dictionary.HS1100N” as follows:

```
VENDOR                          21920

#
#       Standard attribute
#
ATTRIBUTE             -Byte-Amount              10      interger
```

Administrator can also add other attributes as the table stated in Section 2 with the same format.

```
VENDOR                          21920

#
#       Standard attribute
#
ATTRIBUTE             -Byte-Amount              10    interger
ATTRIBUTE             -MaxByteIn                11    interger
ATTRIBUTE             -MaxByteIn                12    interger
ATTRIBUTE             -Byte-Amount-4GB          20    interger
ATTRIBUTE             -MaxByteIn-4GB            21    interger
ATTRIBUTE             -MaxByteIn-4GB            22    interger
```

Step 5

Edit the file “dictionary” under the folder “freeradius”.

```
[vivian@linux ~]$ vi /usr/share/freeradius/dictionary
```

Step 6

To include “dictionary.HS1100N” in the dictionary of RADIUS server, insert it in an incremental position as follows.

```
$INCLUDE dictionary.ascend
$INCLUDE dictionary.bay
$INCLUDE dictionary.bintec
$INCLUDE dictionary.cabletron
$INCLUDE dictionary.
$INCLUDE dictionary.cisco
#
#  This is the same as the altiga dictionary.
#
#$INCLUDE dictionary.cisco.vpn3000
$INCLUDE dictionary.cisco.vpn5000
$INCLUDE dictionary.cisco.bbsm
$INCLUDE dictionary.colubris
$INCLUDE dictionary.erx
```

Step 7

Open the “radius” database.

```
[vivian@linux ~]$ mysql -u root -p radius
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 98 to server version: 5.0.27

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

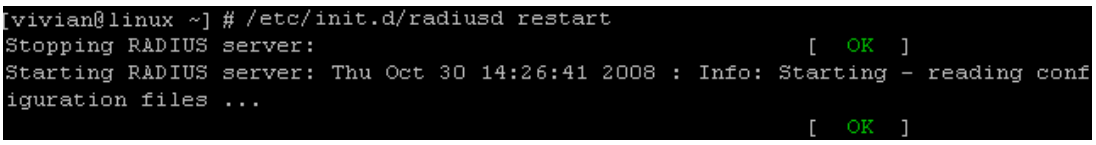
Step 8

Insert **VSA** into RADIUS response. In this example, the maximum download and upload traffics in bytes for **group03 users** is 1MBytes.

```
mysql> INSERT INTO radgroupreply (GroupName,Attribute,op,Value)
VALUES ('group03', cipherium-Byte-Amount',':=','1048576')
Query OK, 1 row affected (0.00 sec);
mysql> exit
Bye
```

Step 9

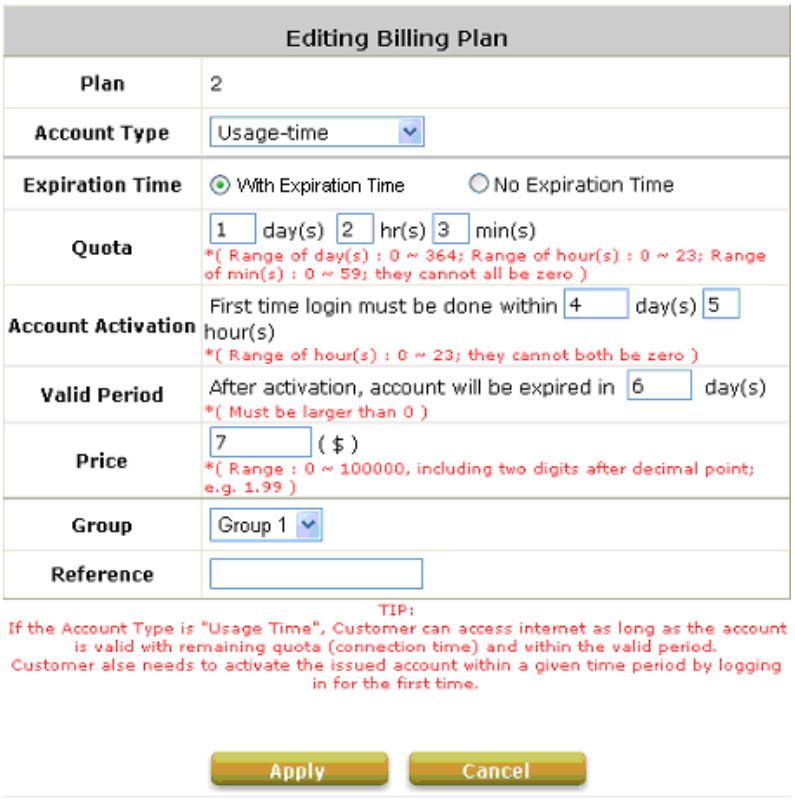
Restart RADIUS daemon to get your settings activated.

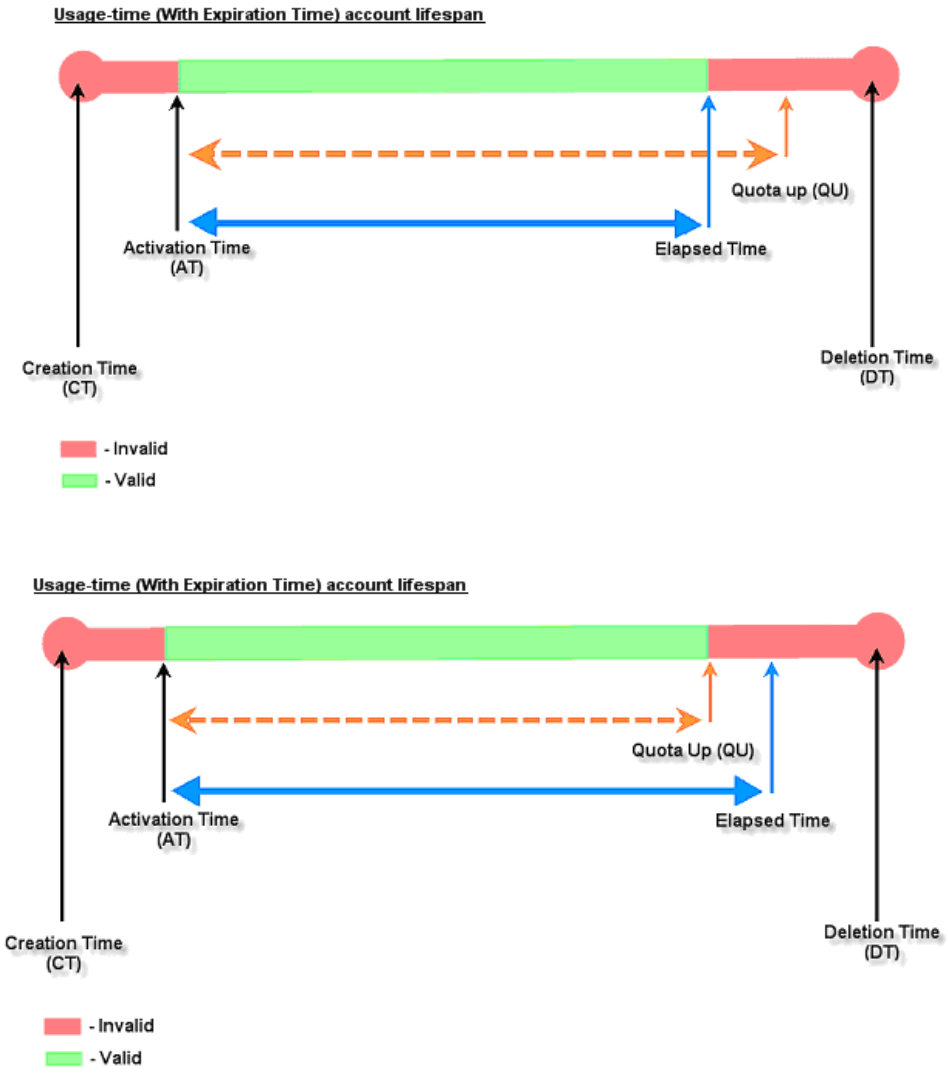


Appendix E. On-demand Account types & Billing Plan

This section explains the parameters as well as the different account types provided when editing billing plans in On-demand authentication.

- **Usage-time with Expiration Time:** Can access internet as long as account valid with remaining quota (usable time). Need to activate the purchased account within a given time period by logging in for the first time. Ideal for short term usage. For example in coffee shops, airport terminals etc. Only deducts quota while using, however the count down to Expiration Time is continuous regardless of logging in or out. Account expires when ***Valid Period*** has been used up or quota depleted.
  - **Quota** is the total period of time (xx *days* yy *hrs* zz *mins*), during which On-demand users are allowed to access the network. The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeeming.
  - **Account Activation** is the time period for which the user must execute a first login. Failure to do so in the time period set in Account Activation, the account will expire.
  - **Valid Period** is the valid time period for using. After this time period, even with remaining quota the account will still expire.
  - **Price** is the unit price of this plan.
  - **Group** will be the applied Group to users created from this plan.
  - **Reference** field allows administrator to input additional information.





- **Usage-time with No Expiration Time:** Can access internet as long as account has remaining quota (usable time). Need to activate the purchased account within a given time period by logging in for the first time. Ideal for short term usage. For example in coffee shops, airport terminals etc. Only deducts quota while using. Account expires only when quota depleted.
  - **Quota** is the total period of time (xx *days* yy *hrs* zz *mins*), during which On-demand users are allowed to access the network. The total maximum quota is “364Days 23hrs 59mins 59secs” even after redeem.
  - **Account Activation** is the time period for which the user must execute a first login. Failure to do so in the time period set in Account Activation, the account will expire.
  - **Price** is the unit price of this plan.
  - **Group** will be the applied Group to users created from this plan.
  - **Reference** field allows administrator to input additional information.

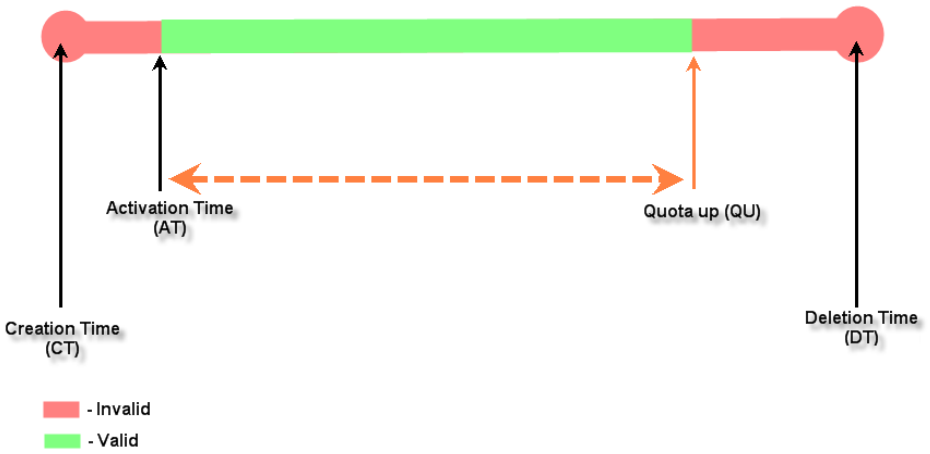
Editing Billing Plan

Plan	3
Account Type	Usage-time
Expiration Time	○ With Expiration Time ◉ No Expiration Time
Quota	2 day(s) 3 hr(s) 4 min(s) *(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)
Account Activation	First time login must be done within 5 day(s) 6 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Price	7 ($) *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1
Reference	

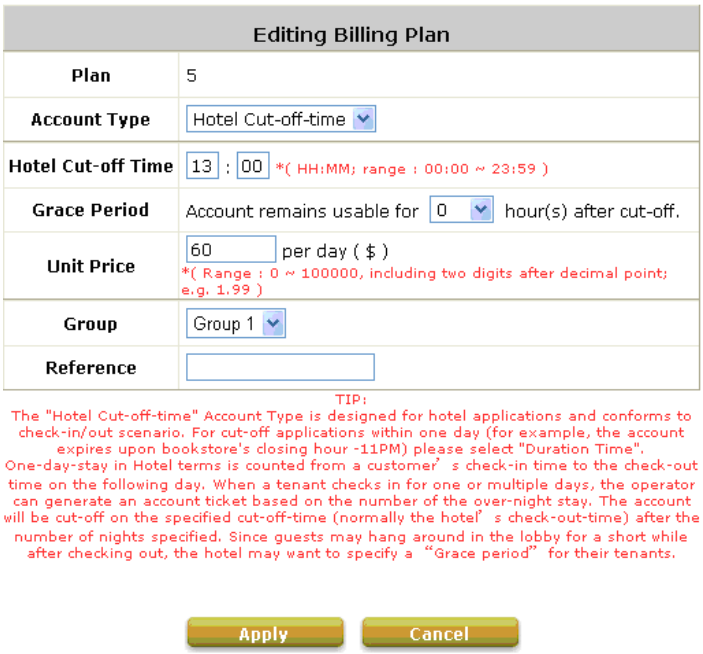
TIP:
If the Account Type is "Usage Time", Customer can access internet as long as the account is valid with remaining quota (connection time) and within the valid period.
Customer alse needs to activate the issued account within a given time period by logging in for the first time.

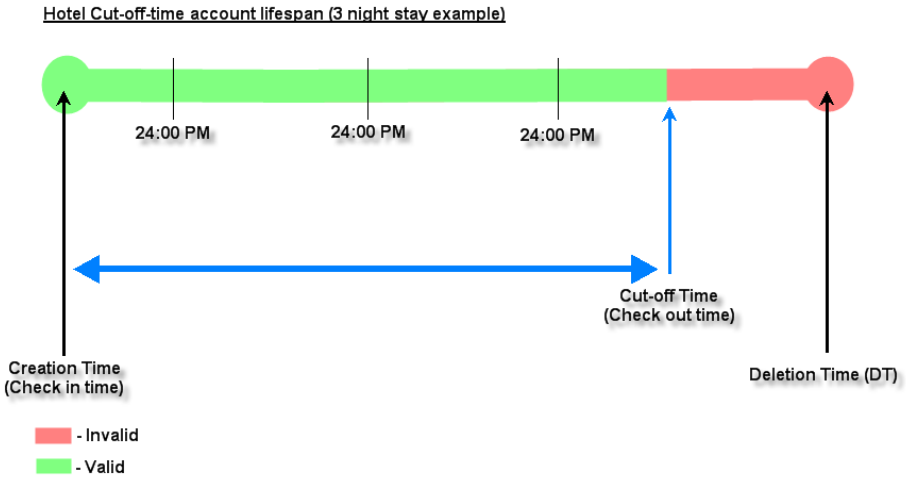
Apply Cancel

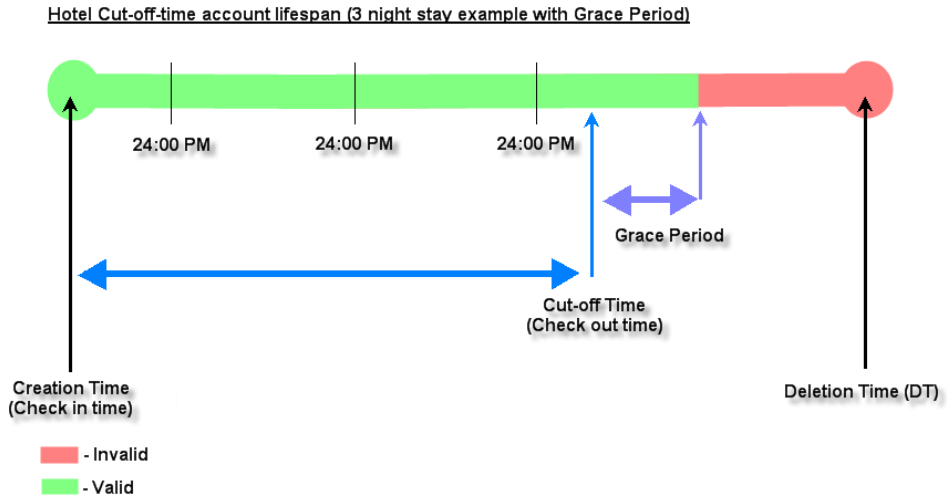
Usage-time (No Expiration) account lifespan



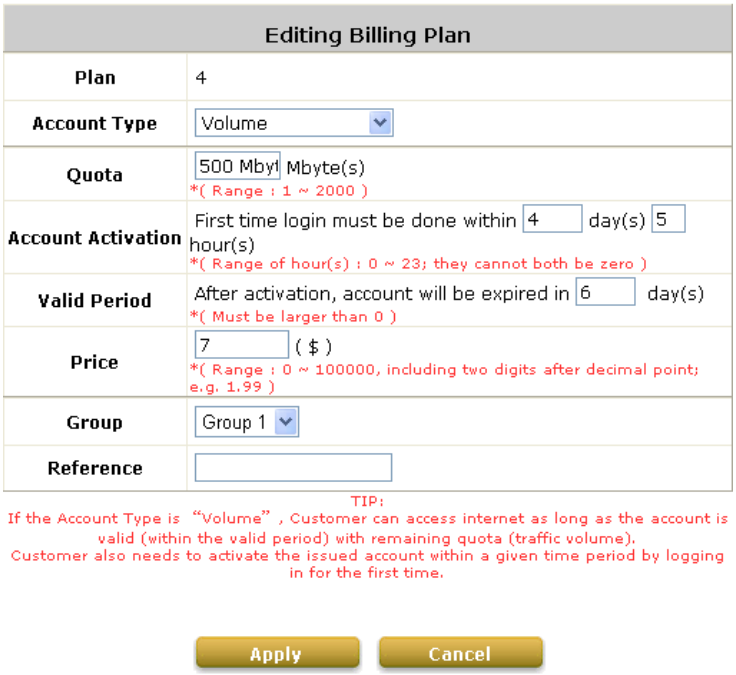
- **Hotel Cut-off-time: Hotel Cut-off-time** is the clock time (normally check-out time) at which the on-demand account is cut off (made expired) by the system on the following day or many days later. On the account creation UI of this plan, operator can enter a Unit value which is the number of days to Cut-off-time according to customer stay time. For example: Unit = 2 days, Cut-off Time = 13:00 then account will expire on 13:00 two days later. **Grace Period** is an additional, short period of time after the account is cut off that allows user to continue to use the on-demand account to access the Internet without paying additional fee. **Unit Price** is a daily price of this billing plan. Mainly used in hostel venues to provide internet service according to guests' stay time. **Group** will be the applied Group to users created from this plan. **Reference** field allows administrator to input additional information.



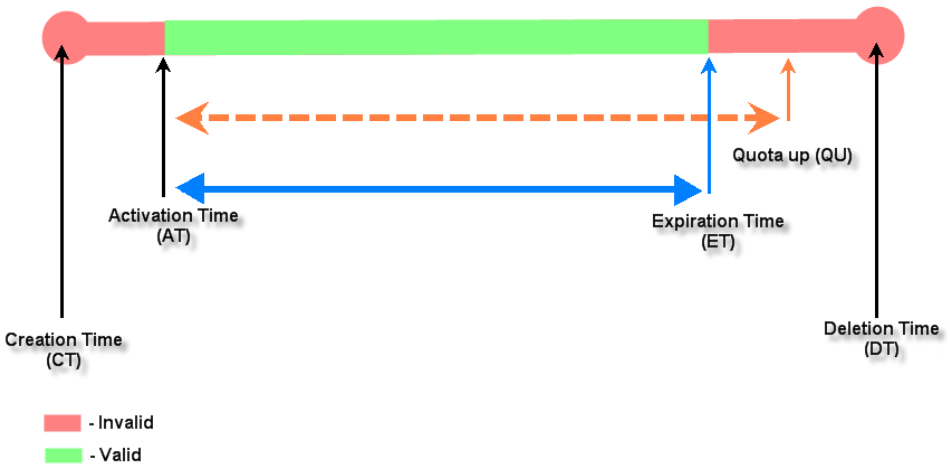




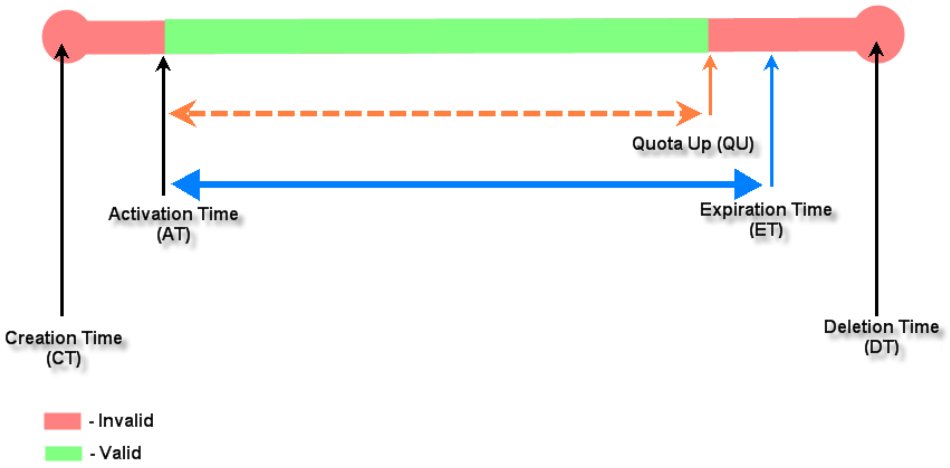
- **Volume:** Can access internet as long as account valid with remaining quota (traffic volume). Account expires when *Valid Period* has been used up or quota depleted. Ideal for small quantity applications such as sending/receiving mail, transferring a file etc. Count down of Valid Period is continuous regardless of logging in or out.
  - **Quota** is the total Mbytes (1~2000), during which On-demand users are allowed to access the network.
  - **Account Activation** is the time period for which the user must execute a first login. Failure to do so in the time period set in Account Activation, the account will expire.
  - **Valid Period** is the valid time period for using. After this time period, even with remaining quota the account will still expire.
  - **Price** is the unit price of this plan.
  - **Group** will be the applied Group to users created from this plan.
  - **Reference** field allows administrator to input additional information.



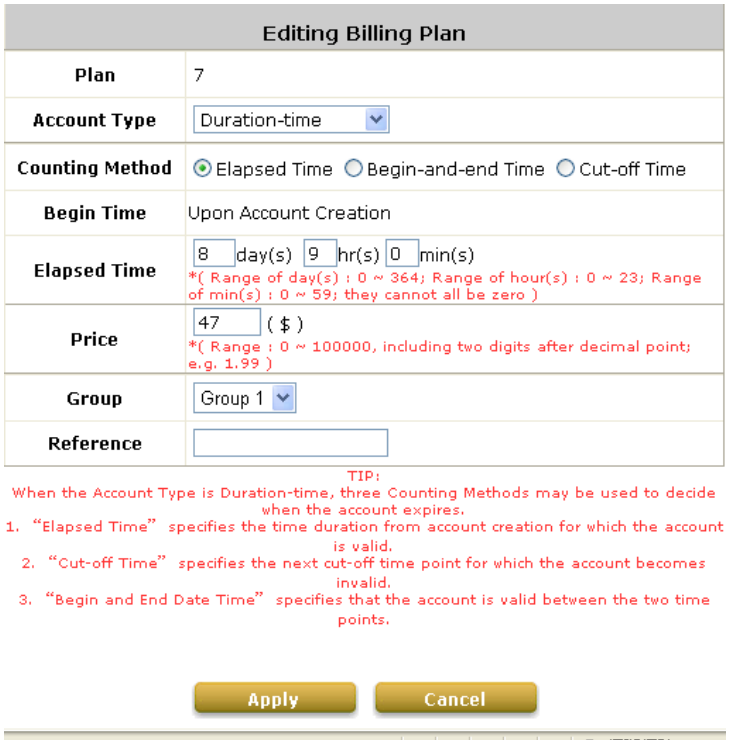
Volume account lifespan

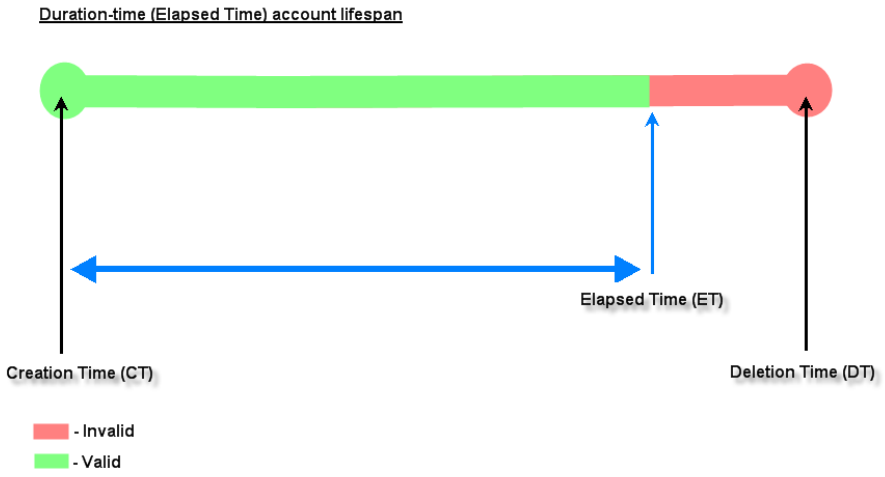


Volume account lifespan

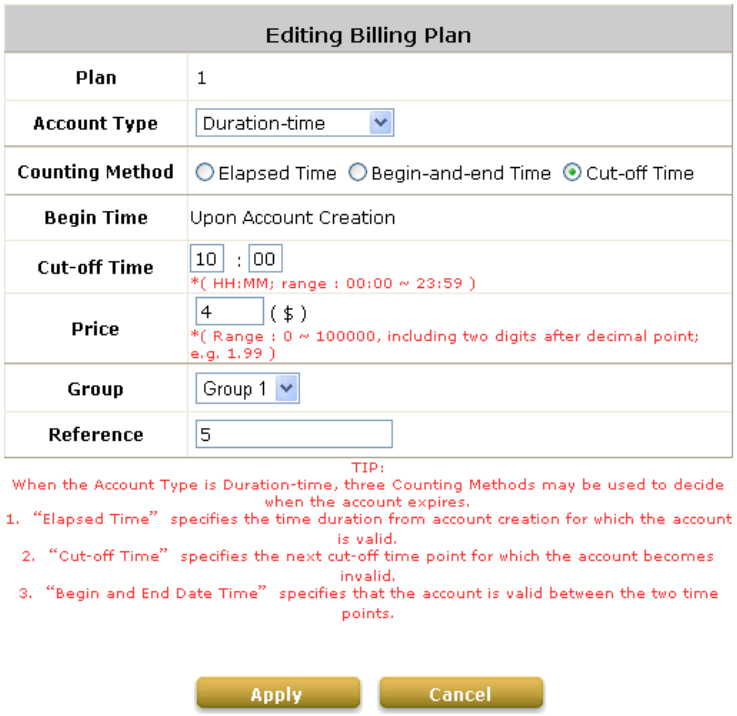


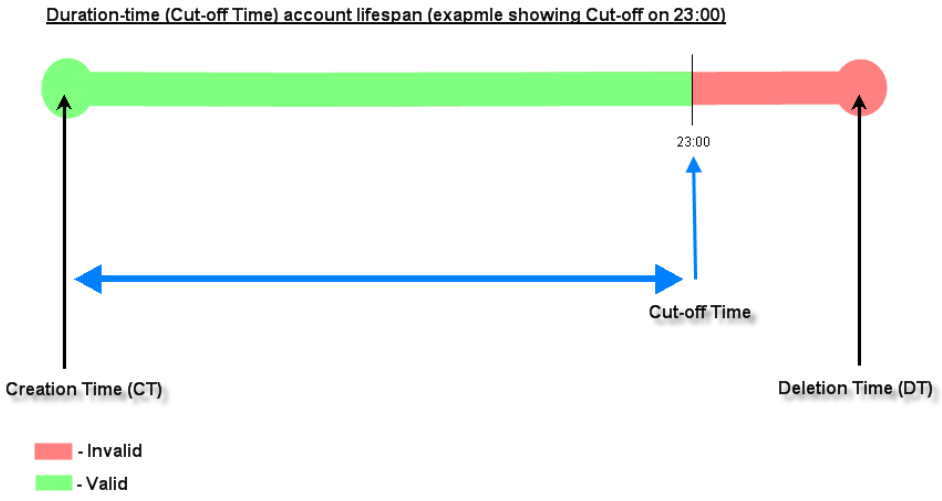
- **Duration-time with Elapsed Time:** Account activated upon the account creation time. Countdown begins immediately after account created and is continuous regardless of logging in or out. Account expires once the *Elapsed Time* has been reached. Ideal for providing internet service immediately after account creation throughout a specific period of time.
  - **Begin Time** is the time that the account will be activated for use. It is set to account creation time.
  - **Elapsed Time** is the time interval for which the account is valid for internet access (xx *hrs* yy *mins*).
  - **Price** is the unit price of this plan.
  - **Group** will be the applied Group to users created from this plan.
  - **Reference** field allows administrator to input additional information.



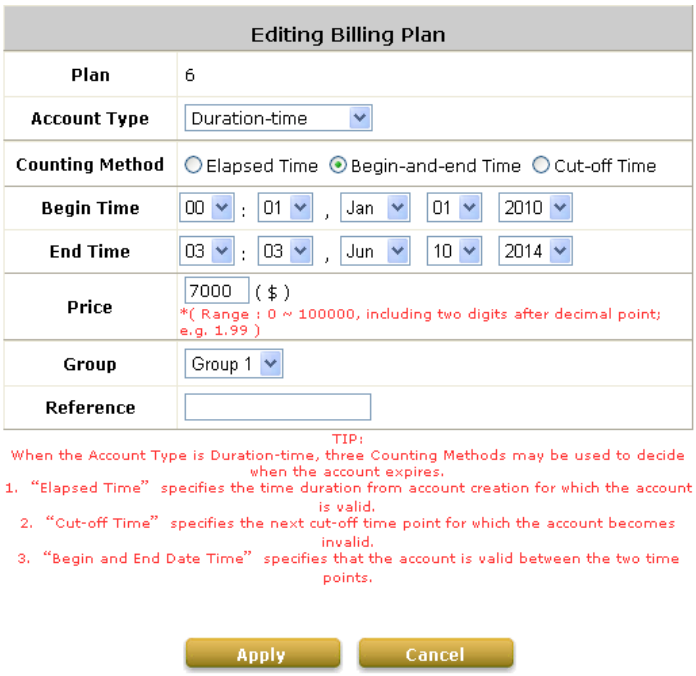


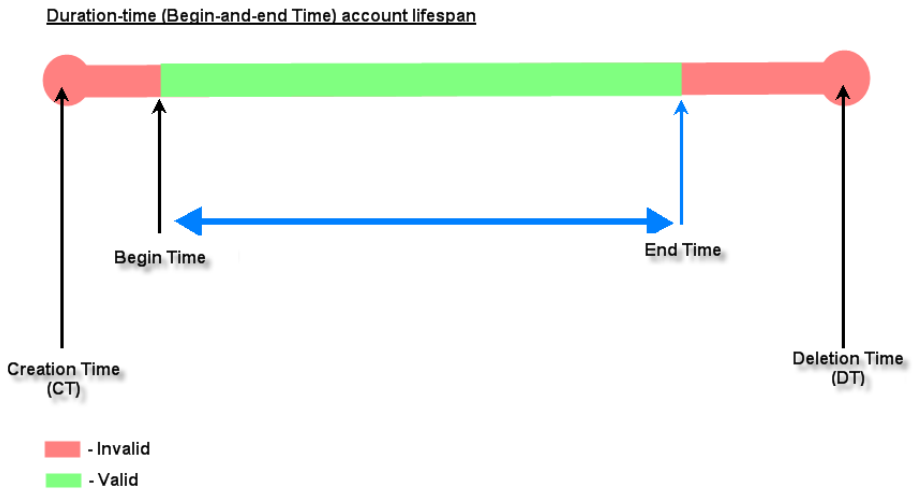
- **Duration-time with Cut-off Time: Cut-off Time** is the clock time at which the on-demand account is cut off (made expired) by the system on that day. For example a shopping mall closing hour is 23:00, operators selling on-demand tickets can create use this plan to create ticket set to be Cut-off on 23:00. If an account of this kind is created after the Cut-off Time, the account will automatically expire.
  - **Begin Time** is the time that the account will be activated for use. It is set to account creation time.
  - **Cut-off Time** is the clock time when the account will expire.
  - **Price** is the unit price of this plan.
  - **Group** will be the applied Group to users created from this plan.
  - **Reference** field allows administrator to input additional information.





- **Duration-time with Begin-and End Time:** Define explicitly the *Begin Time* and *End Time* of the account. Countdown begins immediately after account activation and expires when the *End Time* has been reached. Ideal for providing internet service throughout a specific period of time. For example during exhibition events or large conventions such as Computex where each registered participant will get an internet account valid from 8:00 AM Jun 1 to 5:00 PM Jun 5 created in batch like coupons.
  - **Begin Time** is the time that the account will be activated for use, defined explicitly by the operator.
  - **End Time** is the time that the account will become expired and not able to use any more, defined explicitly by the operator.
  - **Price** is the unit price of this plan.
  - **Group** will be the applied Group to users created from this plan.
  - **Reference** field allows administrator to input additional information.





Appendix F. External Payment Gateways

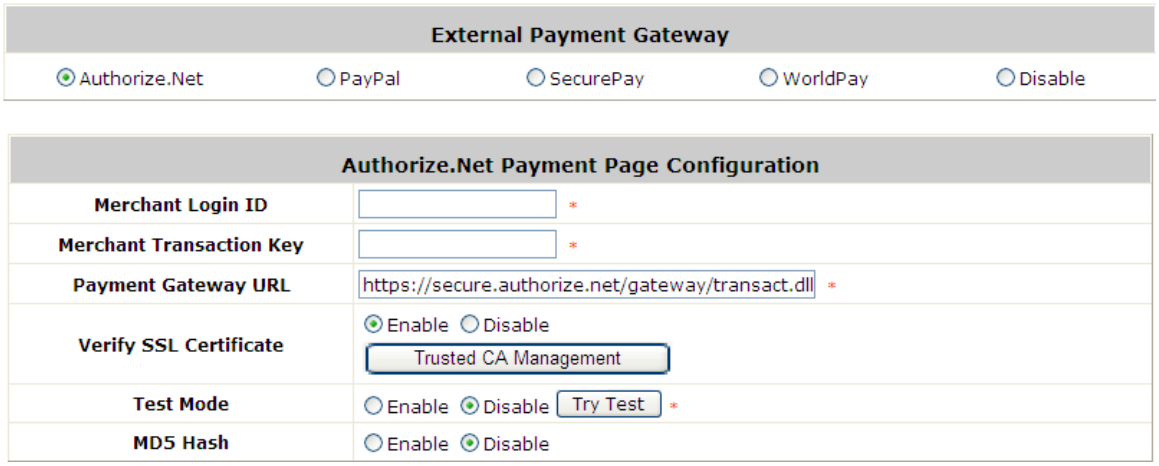
This section is to show independent Hotspot owners how to configure related settings in order to accept payments via Authorize.net, PayPal, SecurePay or WorldPay, making the Hotspot an e-commerce environment for end users to pay for and obtain Internet access with credit cards.

1. Payments via Authorize.Net

To configure Payments via Authorize.Net, go to:
Users >> Authentication >> On-demand User >> External Payment Gateway >> Authorize.Net.

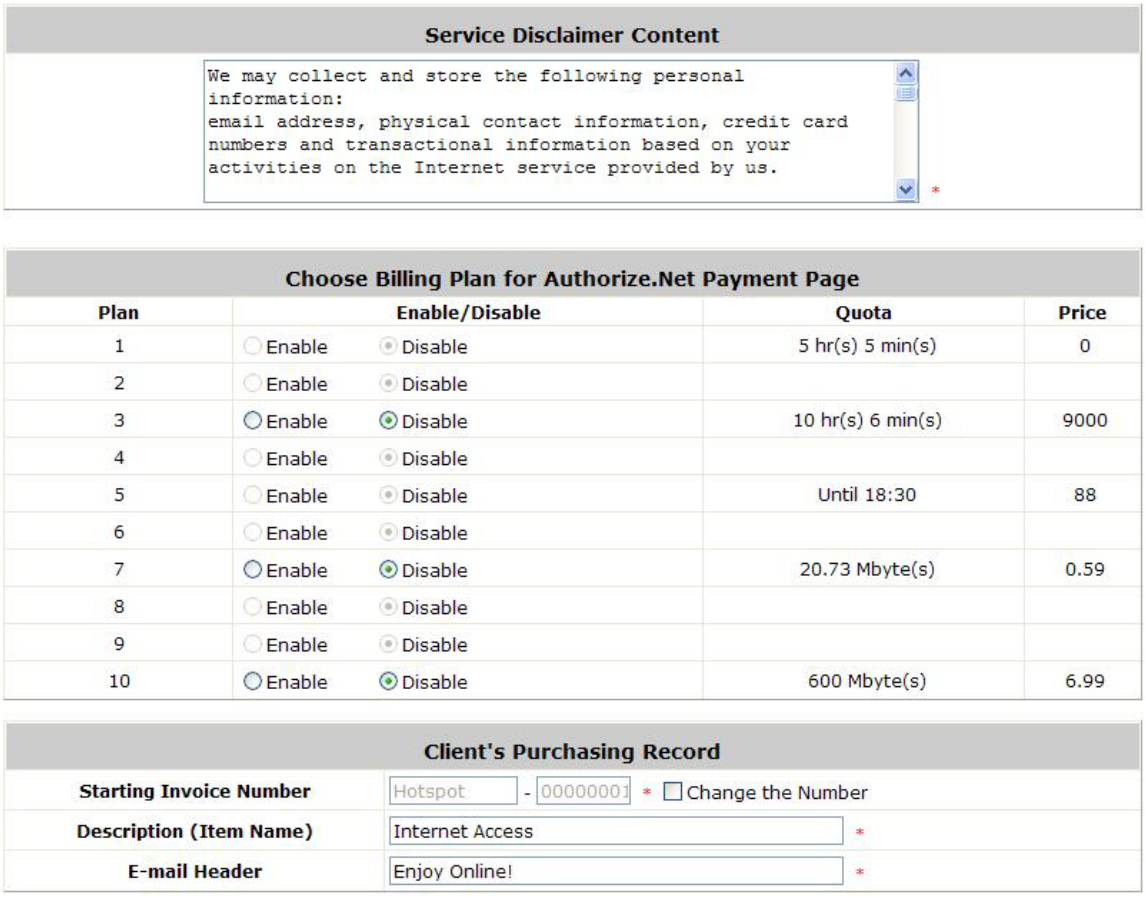
Before setting up "Authorize.Net", it is required that the merchant owners have a valid Authorize.Net account.

- **Authorize.Net Payment Page Configuration**



Merchant ID: This is 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: This is 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.
Test Mode: In this mode, merchants 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/ Choose Billing Plan for Authorize.Net Payment Page/Client's Purchasing Record**



Service Disclaimer Content

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. *

Choose Billing Plan for Authorize.Net Payment Page

Choose Billing Plan for Authorize.Net Payment Page

Plan	Enable/Disable	Quota	Price
1	Enable / Disable	5 hr(s) 5 min(s)	0
2	Enable / Disable		
3	Enable / Disable	10 hr(s) 6 min(s)	9000
4	Enable / Disable		
5	Enable / Disable	Until 18:30	88
6	Enable / Disable		
7	Enable / Disable	20.73 Mbyte(s)	0.59
8	Enable / Disable		
9	Enable / Disable		
10	Enable / Disable	600 Mbyte(s)	6.99

Client's Purchasing Record

Client's Purchasing Record

Starting Invoice Number	Hotspot - 00000001 * Change the Number
Description (Item Name)	Internet Access *
E-mail Header	Enjoy Online! *

Service Disclaimer Content

View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.

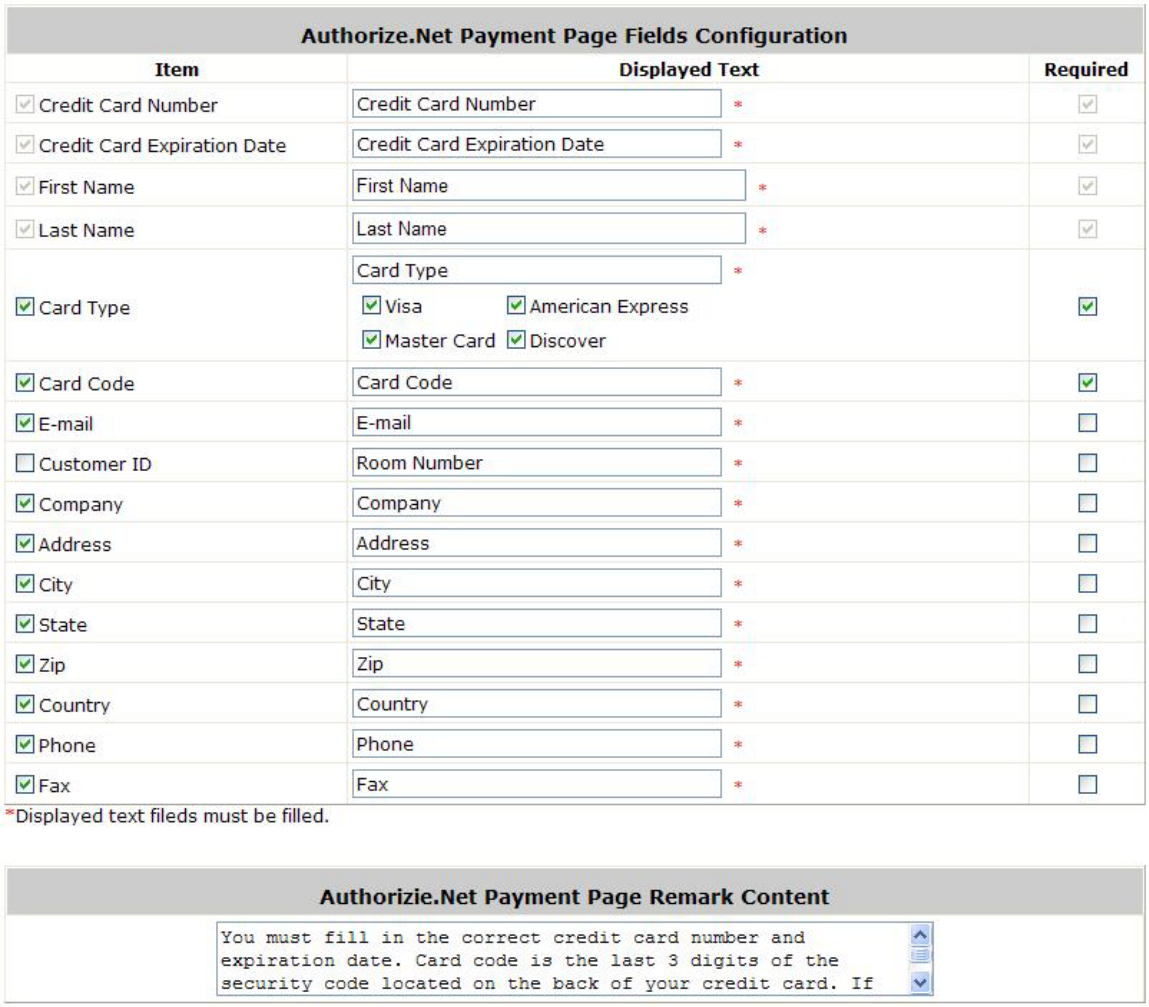
Choose Billing Plan for Authorize.Net Payment Page

These 10 plans are the plans configured in **Billing Plans** page, and all previously enabled plans can be further enabled or disabled here, as needed.

Client's Purchasing Record

- **Starting Invoice Number:** An invoice number may be provided as additional information with a transaction. The number will be incremented automatically for each following transaction. Click the "Change the Number" checkbox to change it.
- **Description (Item Name):** This is the item information to describe the product (for example, Internet Access).
- **Email Header:** Enter the information that should appear in the header of the invoice.

- **Authorize.Net Payment Page Fields Configuration/ Authorize.Net Payment Page Remark Content**



Authorize.Net 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 * Visa American Express 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 fileds must be filled.

Authorizie.Net 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
```

Authorize.Net Payment Page Fields Configuration

- **Item:** Check the box to show this item on the customer's payment interface.
- **Displayed Text:** Enter what needs to be shown for this field.
- **Required:** Check the box to indicate this item as a required field.
- **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:** Expiration date of the credit card. This should be entered in the format of MMYY. For example, an expiration date of July September 2009 should be entered as 0709.
- **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 (at the end of the credit card number found either on the front of the card 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 format of information.
  - **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 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 name.
  - **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 and 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 name.
  - **Phone:** A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number 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 number or contain parentheses and dashes to separate the area code and number.

Authorizie.Net 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.

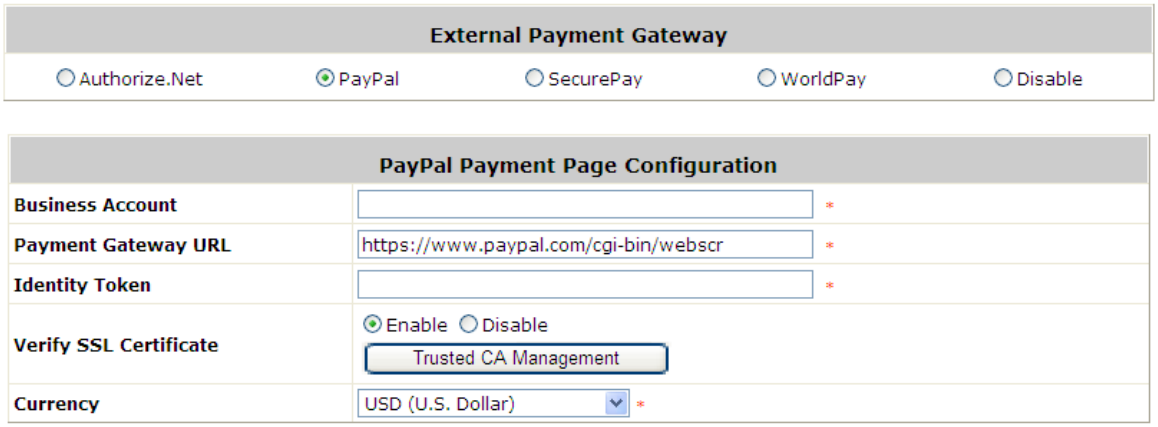
2. Payments via PayPal

To configure Payments via PayPal, go to:

User >> Authentication >> On-demand User >> External Payment Gateway >> PayPal.

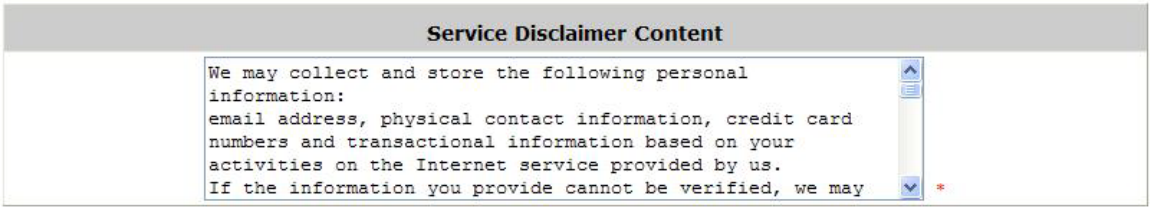
Before setting up “PayPal”, it is required that the hotspot owners have a valid PayPal “Business Account”. After opening a PayPal Business Account, the hotspot owners should find the **“Identity Token”** of this PayPal account to continue “PayPal Payment Page Configuration”.

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



- **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 / Choose Billing Plan for PayPal Payment Page**



- **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.
- **Choose Billing Plan for PayPal 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:

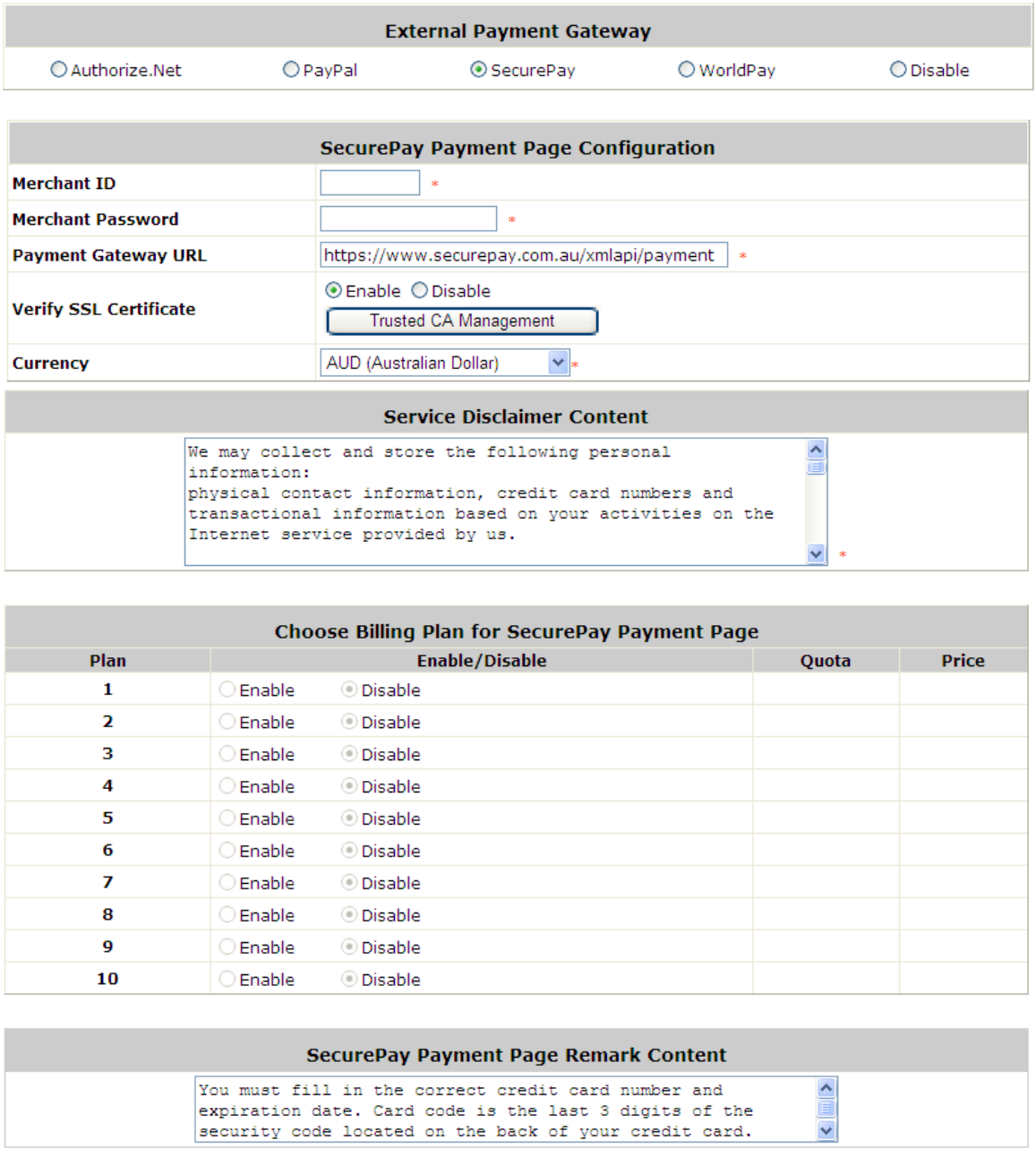
- **Starting Invoice Number:** An invoice number may be provided as additional information against a transaction. This is a reference field that may contain any kind of information.
- **Description:** Enter the product/service description (e.g. wireless access service).
- **Title for Message to Seller:** 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.

4. Payments via SecurePay

To configure Payments via SecurePay, go to: ***Users >> Authentication >> On-demand User>> External Payment Gateway >> SecurePay***.

Before setting up “SecurePay”, it is required that the hotspot owners have a valid SecurePay “Merchant Account” from its official website.



- **SecurePay Page Configuration**

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

  Merchant 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.

- **Choose Billing Plan for SecurePay Payment Page**

  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.

5. Payments via World Pay

To configure Payments via WorldPay, go to:

Users >> Authentication >> On-demand User >> External Payment Gateway >> WorldPay.

WorldPayPaymentConfiguration	
WorldPayInstallationID	*
Payment Gateway URL	https://select.wp3.rbsworldpay.com/wcc/purchase *
Currency	GBP (Pound Sterling) *

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. *

WorldPayBillingConfiguration			
Plan	**Enable/Disable**	**Quota**	**Price**
1	Enable Disable	15 min(s) connection time quota with expiration	10.91
2	Enable Disable	11 min(s) connection time quota	1
3	Enable Disable	Valid until 12:00 the following day	5
4	Enable Disable	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1
5	Enable Disable		
6	Enable Disable		
7	Enable Disable		
8	Enable Disable		
9	Enable Disable		
10	Enable Disable		

WorldPayNoteContent
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.

- **WorldPay Payment Configuration**

  WorldPayInstallation ID: The ID of the associated Merchant Account.

  Payment Gateway URL: The default website of posting all transaction data.

  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.

- **WorldPay Billing Configuration**

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

- **WorldPay Note Content**

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

Before setting up “WorldPay”, it is required that the hotspot owners have a valid WorldPay “Merchant Account”

from its official website: RBS WorldPay: Merchant Services & Payment Processing, going to ***rbsworldpay.com >> support centre >> account login***.

STEP①. Log in to the Merchant Interface.

- Login url: www.rbsworldpay.com/support/index.php?page=login&c=WW
- Select Business Gateway - Formerly WorldPay
- Click Merchant Interface
- Username: user2009
- Password: user2009

STEP②. Select Installations from the left hand navigation

STEP③. Choose an installation and select the Integration Setup button for the specific environment.

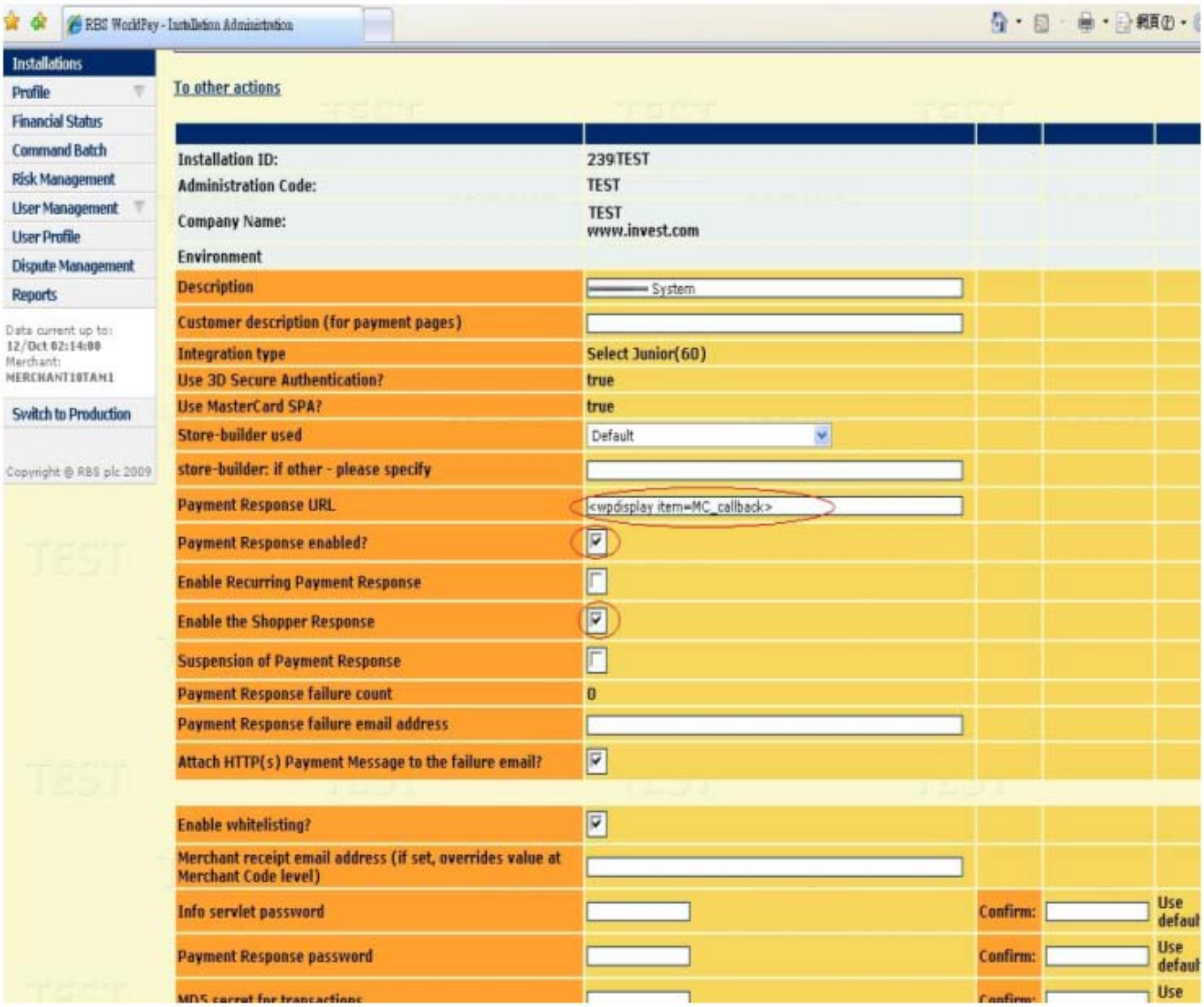
- Installation ID: 239xxx

STEP④. Check the Enable Payment Response checkbox.

STEP⑤. Enter the Payment Response URL.

- URL : <wpdisplay item=MC_callback>

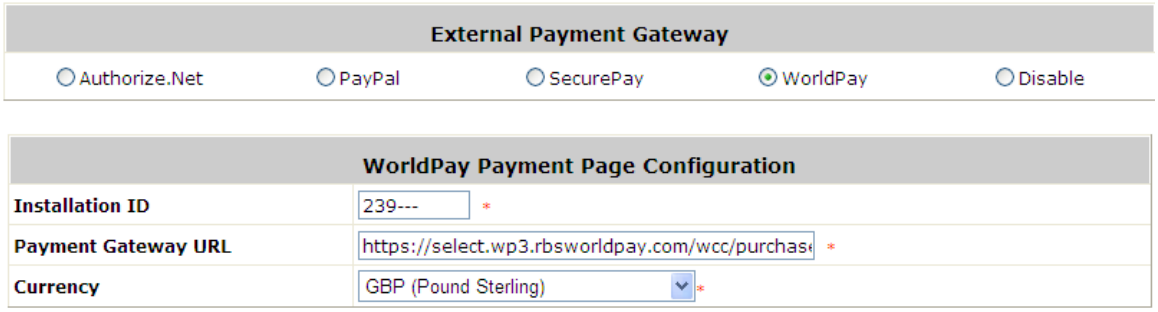
STEP⑥. Check the Enable the Shopper Response.



STEP⑦. Select the Save Changes button

STEP⑧. Input Installation ID and Payment Gateway URL in gateway UI.

- Installation ID: 2009test
- URL : https://select.wp3.rbsworldpay.com/wcc/purchase



Note: *The WAN IP of gateway must be real IP.*

Legal & Regulatory Information

Limitation of Liability

NetComm Limited reserves the right to change the specifications and operating details of this product without notice. The information in this document does not represent a commitment on the part of NetComm Limited.

To the fullest extent permitted by law NetComm Limited and its affiliates disclaim liability for any and all direct, indirect, special, general, incidental, consequential, punitive or exemplary damages including, but not limited to , loss of profits or revenue or anticipated profits or revenue arising out of the use or inability to use any NetComm product, even if NetComm Limited and/or its affiliates has been advised of the possibility of such damages or they are foreseeable or for claims by any third party.

Notwithstanding the foregoing, in no event shall NetComm Limited and/or its affiliates aggregate liability arising under or in connection with the NetComm product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the NetComm product.

Where the NetComm product supplied is not of a kind ordinarily acquired for personal, domestic or household use or consumption, NetComm Limited and its affiliates limit their liability to, at their option, the replacement or repair of the NetComm product or the payment of the cost of replacement or repair of the NetComm product.

Nothing in this clause excludes, restricts or modifies any condition, warranty, guarantee, right or remedy under a mandatory law.

Copyright

Trademarks

NetComm, the NetComm logo and NetComm CallDirect™ are trademarks of NetComm Limited. Sierra Wireless is trademark of Sierra Wireless. Windows® is a registered trademark of Microsoft Corporation.

All other trademarks are acknowledged the property of their respective owners.

Regulatory Information (Australia)

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.

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

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-commercial.com.au**

NETCOMM LIMITED Head Office
PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: int.sales@netcomm.com.au
W: www.netcommlimited.com.