AMG-2102
Gigabit Access and AP Management Gateway Pro
User's Manual **v1.0**

Table of Contents

General Public License

This product incorporates open source code into the software and therefore falls under the guidelines governed by the General Public License (GPL) agreement.

Adhering to the GPL requirements, the open source code and open source license for the source code are available for free download at http://global.level1.com.

If you would like a copy of the GPL or other open source code in this software on a physical CD medium, LevelOne (Digital Data Communications) offers to mail this CD to you upon request, for a price of US$9.99 plus the cost of shipping.

1.Before You Start

1.1 Preface

This User Manual is for WLAN service providers or network administrators to set up a network environment using the AMG-2102 system. It contains step-by-step procedures and graphic examples to guide MIS staff or individuals with basic network system knowledge to complete the installation.

Besides this document, there is a "Quick Installation Guide" (QIG), which serves well to start AMG-2102 quickly. It is recommended to start with the QIG first, and then refer to this manual for further details. Some special topics are addressed separately in the Appendixes.

1.2 Document Conventions

Caution:	Represents essential steps, actions, or messages that should not be ignored.
Note:	Contains related information that corresponds to a topic.
	Indicates that clicking this button will apply all of your settings.
	Indicates that clicking this button will clear what you have set before the settings are applied.
*	The red asterisk indicates that information in this field is compulsory.

1.3 Package Checklist

The standard package of AMG-2102 includes:

- AMG-2102 x 1
- CD-ROM (with User's Manual and QIG) x 1
- Quick Installation Guide (QIG) x 1
- Console Cable x 1
- Crossover Ethernet Cable x 1
- Straight-through Ethernet Cable x 1
- Power Cord x 1
- Rack Mounting Bracket (with Screws) x 1

Caution:

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

2.System Overview and Getting Start

2.1 Introduction of AMG-2102

AMG-2102 is an all-in-one product specially designed for wired and wireless data network environments in large scaled WLAN deployments. AMG-2102 is a high-performance industrial grade network appliance, able to support the network access management for a larger user base.

Access and AP Management Gateway Products (AMG Series) feature integrated management, secured data transmission, and enhanced accounting and billing. System administrators can effectively monitor wired and/or wireless users, including employees and guest users via its user management interface. Moreover, administrators can discover, configure, monitor, and upgrade all managed Access Points (APs) from a single, centralized AP management interface.

2.1.1 Key Features

Like other AMG Series products, AMG-2102 is designed to be a multi-service network access controller for enterprise or campus environment; it is also deployed as a hotspot subscriber gateway often. It is a pre-integrated multi-function network appliance, providing the following key features:

- **Standard based user authentications, including Web-based login and 802.1x (RADIUS)**
- **Customizable login portal pages and walled gardens to simplify branding**
- **User groups (roles) and user management**
- **Supports for multiple authentication databases (Local, On-demand, RADIUS, POP3, LDAP, NTDS)**
- **Virtual service zones and policy management**
- **Simple visitor account provisioning and billing plans by time or traffic volume**
- **Payment gateway supports, including PayPal, Authorize.net, and SecurePay**
- **Account roaming across multiple sites (branches)**
- **AP management and wireless roaming across APs**
- **Virtual Private Network (VPN) tunnels.**
- **Converged network for Data, Voice and Video traffics**
- **Dual uplinks (WAN) for better reliability and load balancing**
- **Firewall and Denial of Service (DoS) attack prevention**
- **Monitoring, notification and reporting**
- **Network gateway features, including NAT, DHCP, DMZ, firewall and port forwarding**

2.1.2 Who Uses AMG-2102

Because of its well-integrated and rich access management features and high performance, **hotels, academic campuses**, **government agencies** and **enterprises' IT departments** will find AMG-2102 is a money and time saver, sparing them from forced to integrate multiple applications and multiple equipments on their own in order to manage and secure the internet/network access for both wired and wireless clients.

With its billing plan and payment features, **WISPs** and **hospitalities** (such as hotels and convention halls) will find AMG-2102 an instant revenue generator without requiring hefty equipment investment or long term outsourcing service supports.

AMG Series products are most affordable, best price-performance appliances, comparing to the similar equipments in the fields of **Network Access Controllers**, **Wireless Controllers, Clientless VPN Gateway** or **Hotspot Subscriber Gateway**.

2.2 System Concept

If you have experienced other AMG Series products before and are familiar with its system concept, you may skip the concept description below. **Please proceed to the next section on (Hardware Description).**

AMG-2102 is capable of managing user authentication, authorization and accounting (AAA). The user account information is stored in the local database or a specified external database server. Featured with user authentication and integrated with external payment gateway, AMG-2102 allows users to easily pay the fee and enjoy the Internet service using credit cards through **Authorize.net**, **PayPal**, **SecurePay**, **PayPal** or **WorldPay**.

With centralized AP management feature, the administrator does not need to worry about how to manage multiple wireless access point devices.

Furthermore, AMG-2102 introduces the concept of Service Zones - multiple virtual networks, each with its own adjustable access control profiles. This is very useful for hotspot owners seeking to provide different customers or staff with different levels of network services.

The following portion of this section explains the basic concepts of AMG-2102; the same concepts also apply to the other AMG Series products. With the understanding of these concepts, the administrator will be able to do more advanced network planning and to manipulate the configurations of AMG-2102 to suit his own specific application. It is sufficient for most of administrators to use the default configuration with minor WAN/DNS address changes for simple deployments.

Gateway is a network node where a small network attaches to a bigger network. AMG-2102 is a kind of gateway in a network environment; hence it has those features a typical gateway has, such as NAT, DHCP, DMZ, Firewall and etc. Conventionally, the bigger network is referred as the gateway's ***WAN side*** or upstream network, while the small network is referred as the gateway's *LAN side*. The Ethernet ports leading to the WAN side network is called ***WAN ports***. The Ethernet ports leading to the LAN side network is called ***LAN ports***.

Local User is a type of user with its account credential stored in a database named "Local" within AMG-2102. The "Local" database of AMG-2102 allows local user accounts. A local user account does not have an expiration date once they are created. If administrator wishes to terminate the account, he

must remove it. A local database can be used as an external RADIUS database to another WLAN Controller product for account roaming.

On-demand User is a type of user with its account credential stored in a database named "On-demand" within AMG-2102. The "On-demand" database of AMG-2102 allows on-demand account records. On-demand User is used for short term usage purpose; it has an expiration period. An on-demand account record will be recycled for creating new on-demand account if it has expired for over certain days or has been modified by the Administrator/Manager manually.

External Authentication Database is a user account database that is not built inside AMG-2102. Besides Local database and On-demand database, AMG-2102 allows up to three additional External Authentication databases simultaneously. The types of external Authentication databases supported are RADIUS, POP3, LDAP (including ActiveDirectory), and NTDomain (Win2K's NTDS). The database of another WLAN Controller device can be used as an external RADIUS database. External Authentication Database is useful for implementing account roaming; for example, multiple AMG-2102 devices in multiple campuses can share one common external database. A user needs only one account in the common database to access the network from different campuses.

Service Zone *is a logic partition of AMG-2102's LAN network*. The concept of Service Zone is similar to the concept of virtual LAN (VLAN), which can be used to group the network traffic or network services for clients on the same VLAN segment, regardless of the clients' physical locations. That is, several VLAN segments may be in service at one physical network location while devices belonging to one VLAN segment may appear in multiple physical locations.

Each Service Zone *can also be viewed a virtual machine of AMG-2102* because each Service Zone can define its own customized login portal page, and its own gateway properties (such as LAN IP address, DHCP on/off and address range). The feature of Multiple Service Zone is also useful to service multiple hotspot franchises in shopping malls or airport terminals by a single AMG-2102.

A Service Zone *is uniquely defined by a VLAN tag id and an associated SSID attribute*. When a managed access point (MAP) is added to a Service Zone through AMG-2102 by the administrator, the associated SSID will be activated in the MAP along with the VLAN tag of the Service Zone.

For example, in the following Figure 2, the administrator plans three logical Service Zones for an academic campus:

- The first Service Zone (with SSID='Student", and VLAN tag=1) is for students.
- The second (with SSID="Faculty" and VLAN tag=2) for faculties.
- The third (SSID="Guest" and VLAN tag=3) for guests.

- A Service Zone *may or may not require client authentication*, depending on how the administrator sets it up. If a Service Zone requires user authentication, the client will be prompted for the login in first before using the network services, no matter the client is connecting to its SSID wirelessly or a switch port via wired line.

Group is a group of user accounts sharing the same access privileges, QoS properties and network policies. Each client account belongs to a Group. Each Group may or may not have the access privilege of a Service Zone, depending on the how the administrator define its policy. If the administrator does not assign a new account to any specific Group, the account belongs to a catch-all group named **"None"** by default.

Policy is for defining rules, privileges or properties for managing users. Each user group is bound by a Policy within a given Service Zone. The same group may or may not be bound to the same policy in different Service zones. There are two tiers of Policies. The first tier is a policy named 'Global-Policy'. The Global-Policy is a base policy which will be applied all users. The second tier is called 'Group-Policy' or simply 'Policy', which can be chosen to bound the network behaviors of a Group. The administrator can define the Firewall Profile, Route Profile, Schedule Profile and Max Sessions in a Policy.

The following Figure 1 depicts an example relationship of Service Zone, Group and Policy. In this example, Students and faculties logging into Service Zone 1 will be governed by Policy-A. Guests only have the access of Service Zone 3, and will be bounded by Policy-C. Faculties have the access to both Service Zone 1 and Service Zone 2 under two different policies.

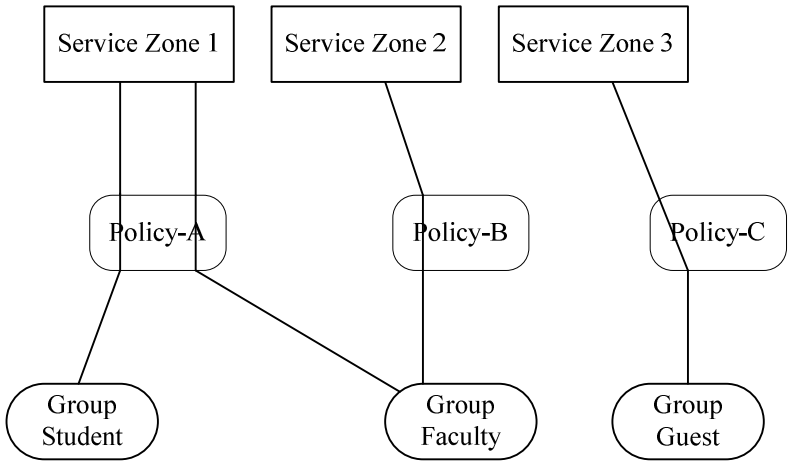


Figure1: An example relationship of Service Zone, Group and Policy

The following Figure 2 depicts an example using AMG-2102 in managing network/internet access in an academic campus environment. Imagine the network administrator may wish to set different privileges and bandwidth limits for staff, students, and guests; he could use several Service Zones of AMG-2102 – one for staff, one for students, and one for the guests. He also uses one zone for some shared servers in the diagram.

The access points at a physically location like the administration building may only allow the access of faculties; hence the access points there are added only to the second Service Zone, enabling only the "Faculty" SSID. On the other hand, the access points in the Cafeteria may allow the access of all groups; hence the APs at Cafeteria are added to all Service Zones, enabling SSID="Student", SSID="Faculty", and SSID="Guest".

There traffic of students, faculties, and guests will be segregated by the three VLAN segments.

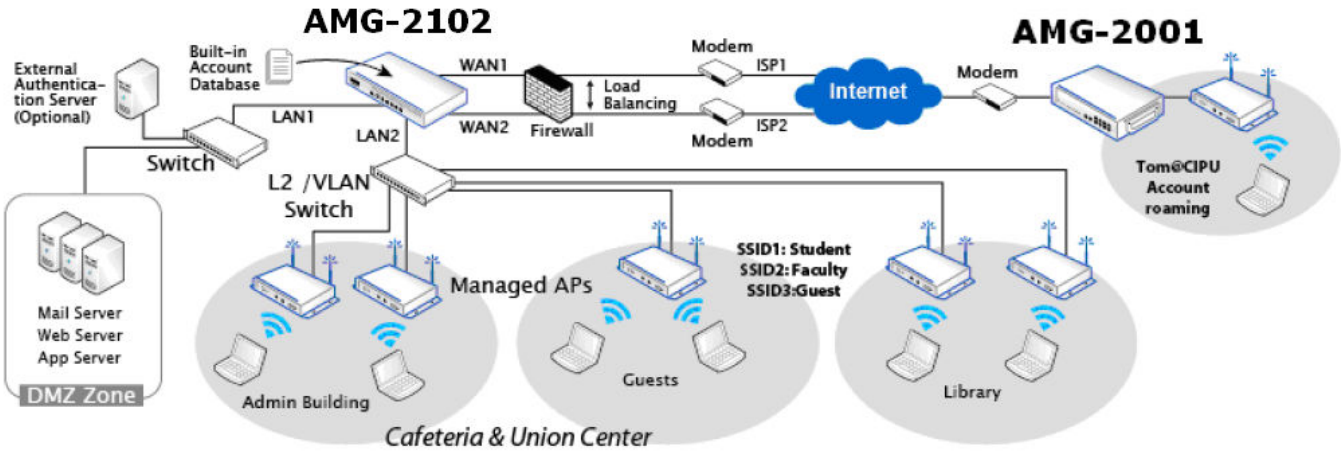
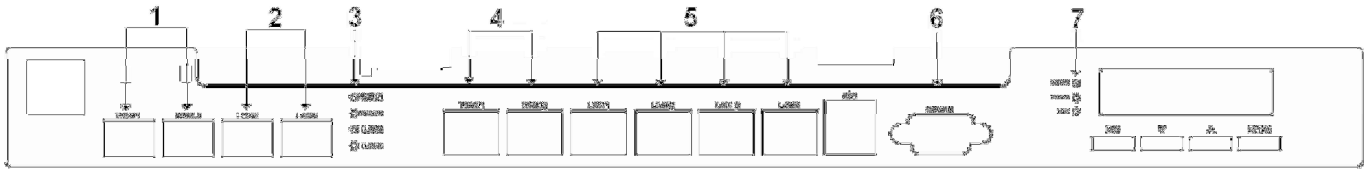


Figure2: An example of managed network

2.3 Hardware Description

2.3.1 Front Panel



1. **WAN1/ WAN2 (SFP)**: Two combo WAN ports (SFP) are connected to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
2. **LAN5/ LAN6 (SFP)**: Client machines connect to AMG-2102 via these LAN ports (SFP).
3. **LED Indicators**: There are four kinds of LED, WAN1, WAN2, LAN5, and LAN6, to indicate the traffic status of the SFP ports.
4. **WAN1/ WAN2**: Two WAN ports (10/100/1000 Base-T RJ-45) are connected to the external network, such as the ADSL Router from your ISP (Internet Service Provider).
5. **LAN1 ~ LAN4**: Client machines connect to AMG-2102 via these LAN ports (10/100/1000 Base-T RJ-45).
6. **Console**: The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft's Hyper Terminal to login to the configuration console interface to change admin password or monitor system status, etc.
7. **LED Indicators**: There are three kinds of LED, Power, Status and Hard-disk, to indicate different status of the system.

Note:

By default, all LAN ports are set with Port-based Default Service Zone; for Service Zone configuration, please refer to **3.3 What is Service Zone**.

2.3.2 Real Panel

1. **Power Supply Socket:** Connecting the power cord to the built-in open-frame power supply (Input: 100~240 VAC, 50/60 Hz).
2. **Power Switch**: Press once to Power-On or Power-Off.
3. **Device Cooling Fan**: Don't block the cooling fans. Leave enough open space for ventilation.

2.4 Preparation before the Installation

Before you start the installation by either following this User Manual or the Quick Installation Guide, below is a short preparation list to do.

1) Unpack the AMG-2102 and go thorough the package checklist.

2) Review the front panel and the back panel and identify each control and network interface that is described in the previous Hardware Description section.

3) Prepare a couple of CAT5 Ethernet cables with using RJ-45 connectors. The cables are for connecting IP devices, including this AMG-2102, IP switches, and your PC.

4) Prepare a PC with Web browser for accessing the Web Management Interface.

5) Identify an upstream device to plug in AMG-2102 in your network, such as ADSL, CABLE modem or other edge devices. Collect the DNS server address provided by your ISP.

If you use WLAN Controller product for the first time, it is recommended that you follow the Quick Installation Guide to start up the AMG-2102 in a near default state with minimum configuration changes (such as WAN settings and admin password), then refer to this manual later when you want to configure the system for specific application needs.

The recommended general steps for the configuration are:

- Set up system's Time Zone, NTP server, DNS server and WAN1address
- Configure LAN address range for at least one Service Zone, and enable its authentication. The Default Service Zone is enabled by the factory default.
- Create user accounts to test the login page via wire line in the enabled Service Zone.
- Try to generate on-demand user and test the account.
- Configure Wireless environment of Service Zone, then add in AP
- Configure more Service Zones base on your application.
- Set up Group and Policy (including Firewall rules and Session Limit).
- Customize the portal login page and add walled garden Advertisement links if needed.
- Set up Payment gateway if you want to use credit card for the on-demand accounts.
- Load SSL certificate for the Web Server before operation.
- Monitor the status pages and reports generated.
- Perform other advanced setting for your specific application.

2.5 Hardware Installation

Please follow the steps below to install the hardware of AMG-2102:

1) Connect the power cord to the power socket on the rear panel.

2) Turn on the power switch on the rear panel. The Power LED should be on to indicate a proper connection.

3) Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an xDSL/cable modem, or a switch/hub of an internal network. The LED of this port should be on to indicate a proper connection.

4) Connect an Ethernet cable to the Mgmt Port on the front panel. Connect the other end of the Ethernet cable to an administrator PC for configuring the AMG-2102 system. Connect an Ethernet cable to any one of the LAN Ports on the front panel. Connect the other end of the Ethernet cable to an AP for extending wireless coverage; a switch for connecting more wired clients; or directly to a client PC. The LED of port should be on to indicate a proper connection.

Caution: *The two SFP WAN ports are the combo ports with the other Ethernet WAN ports. You can either use the SFP or the Ethernet WAN for the WAN traffic. For example, you can use SFP WAN1 and Ethernet WAN2, or Ethernet WAN1 and SFP WAN2, or both two SFP for WAN1/WAN2 or both WAN1/WAN2 are use Ethernet ports. If you connect the SFP and Ethernet for same WAN port simultaneously, the traffic will go through the SFP port only.*

Figure 3 below is a simple network diagram for the initial installation and configuration. Start with this simple network topology to set up AMG-2102 for the first time; it helps to plan a more sophisticated network topology to suits your specific application needs later.

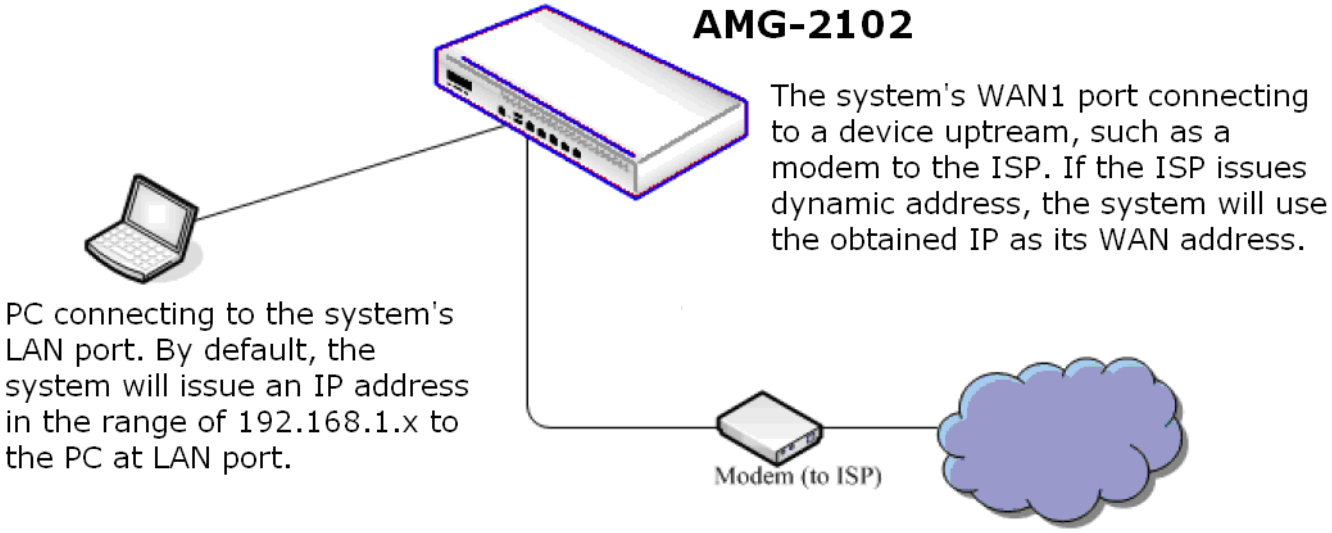


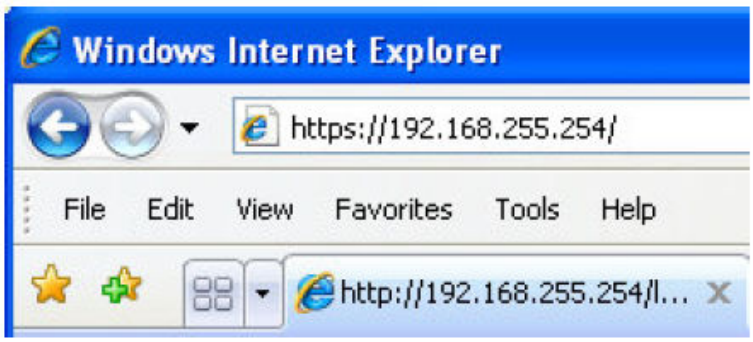
Figure3: A simple network diagram for the initial setup

2.6 Accessing Web Management Interface

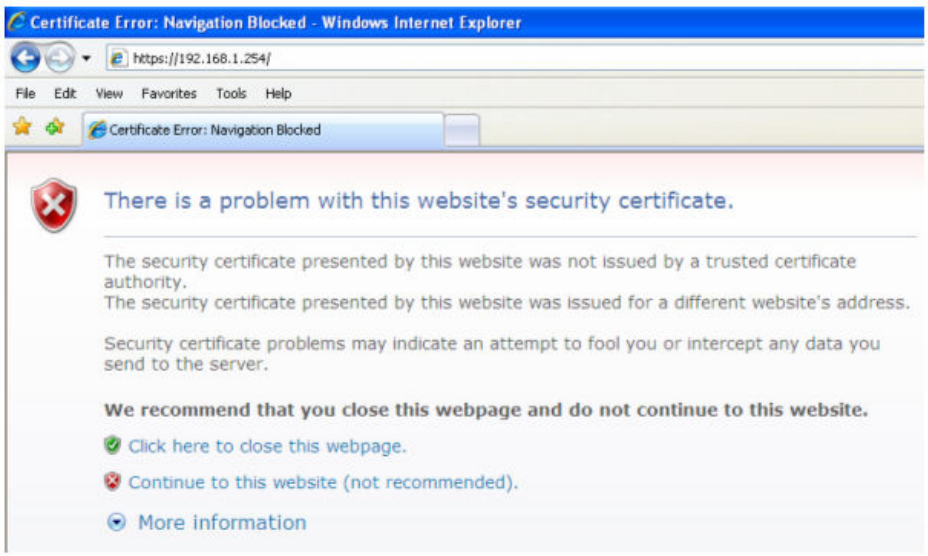
AMG-2102 supports web-based configuration. Upon the completion of hardware installation, AMG-2102 can be configured via web browsers with JavaScript enabled such as Internet Explorer version 6.0 and above or Firefox.

To access the web management interface, connect a PC to any **LAN port**, and then launch a browse. **Make sure you have set DHCP in TCP/IP of your PC to get an IP address dynamically.**

Next, enter the gateway IP address of AMG-2102 at the address field. The default gateway IP address from **LAN Port** is**"*https://192.168.1.254*"** (**"https"** is used for a secured connection).



For the first time, if AMG-2102 is not using a **trusted SSL certificate**, there will be a **"Certificate Error"**, because the browser treats AMG-2102 as an illegal website. Please press **"Continue to this website"** to continue. The default user login page will then appear in the browser.



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

Caution:

If your PC is connecting to the Mgmt port, and you can't get the Administrator's login screen, the reasons may be:

(1) The PC is set incorrectly so that the PC can't obtain the IP address automatically from the Mgmt port;

(2) The IP address and the default gateway are not under the same network segment.

Please use default IP address such as 192.168.1.xx in your network and then try it again. For the configuration on PC, please refer to ***Appendix A. Network Configuration on PC.***

After a successful login, a "Home" page will appear on the screen.

3. Placing AMG-2102 in a Network Environment

3.1 Network Requirement

Typically, in a network environment, AMG-2102 plays the role of a gateway. On a gateway device, a network port leading upstream to the Internet or the backbone network is called a 'WAN port' or an uplink port, while a network port used for branching out to the service the clients downstream is referred as 'LAN port'.

AMG-2102 consists of two WAN ports, which are normally linking up to another routers or modems leading to ISP. A gateway needs one WAN port only, but if you want dual-homing or dual-uplink to add reliability and throughput, the second WAN port let you achieve the goal.

AMG-2102 has two LAN ports. There could be other network bridge devices, such as Layer-2 switches or VLAN switches, between AMG-2102's LAN ports and the client devices.

3.2 Setting up WAN1 Port

AMG-2102's two WAN ports are marked as WAN1 and WAN2 on the front panel. WAN1 port supports four connection types: **Static**, **Dynamic**, **PPPoE** and **PPTP**. WAN2 port supports 3 connection types: **Static**, **Dynamic** and **PPPoE**. These connection types are enough to support most ISP.

Depending on ISP or the upstream device the WAN port connects, you only need to select one connection type for the port. For example, if your ISP is Cable modem issuing Dynamic address, then you would select Dynamic connection when setting up the WAN ports.

Now, let us begin to configure WAN1 port:

Go to: ***System >> WAN1***.

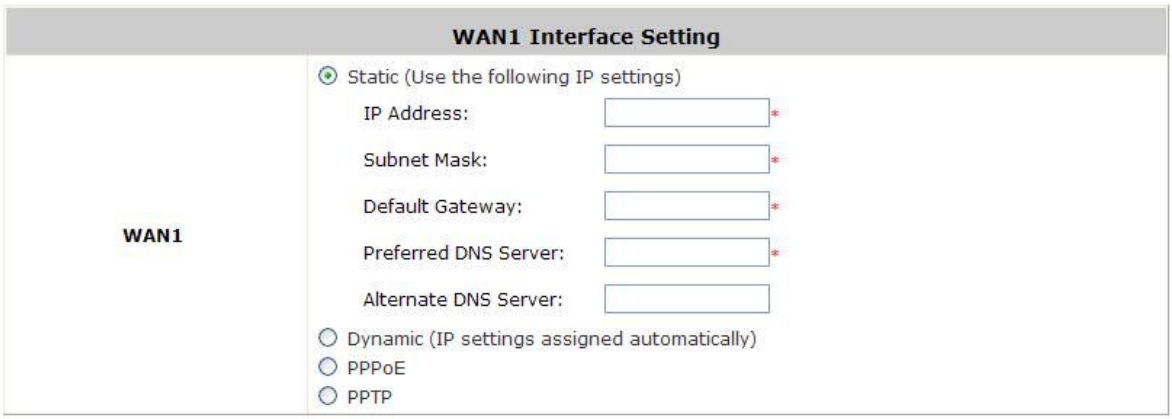
On the WAN1 Configuration Web page, you can decide which of the four connection options (Static, Dynamic, PPPoE and PPTP) to choose from.

3.2.1 Static IP

When the ISP assigns you static IP address, or for other reason, your network requires you to use a fixed IP address, then you (as the administrator of AMG-2102) will manually enter the fixed IP address as AMG-2102's WAN address.

Static: Manually specifying the IP address of the WAN Port. The fields with red asterisks are required to be filled in.

- **IP Address:** The IP address of the WAN1 port.
- **Subnet Mask:** The subnet mask of the WAN1 port.
- **Default Gateway:** The gateway of the WAN1 port.
- **Preferred DNS Server:** The primary DNS server used by the system.
- **Alternate DNS Server:** The substitute DNS server used by the system. This is an optional field.



3.2.2 DHCP (Dynamic IP)

When the ISP issues dynamic IP addresses or there is a DHCP server upstream for issuing dynamic IP addresses, then you (as the administrator of AMG-2102) can configure AMG-2102 to receive an IP address dynamically as AMG-2102's WAN1 address.

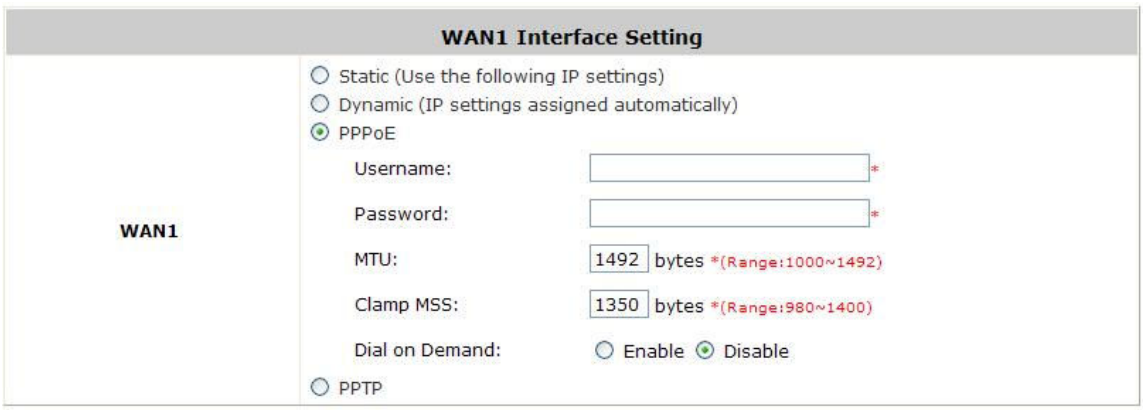
Dynamic: It is only applicable for the network environment where the DHCP server is available on the upstream network. Click the ***Renew*** button to get an IP address automatically.

3.2.3 PPPoE

If the ISP requires you use PPPoE Dialup connection, then the ISP will issue you an account with a password. You would need to enter the account credential in the WAN configuration page for dialing up to the ISP. If you are using ADSL/DSL Internet service, most likely, your ISP will require PPPoE connection.

PPPoE: When selecting PPPoE to connect to the network, please set the **"UserName"**, **"Password"**

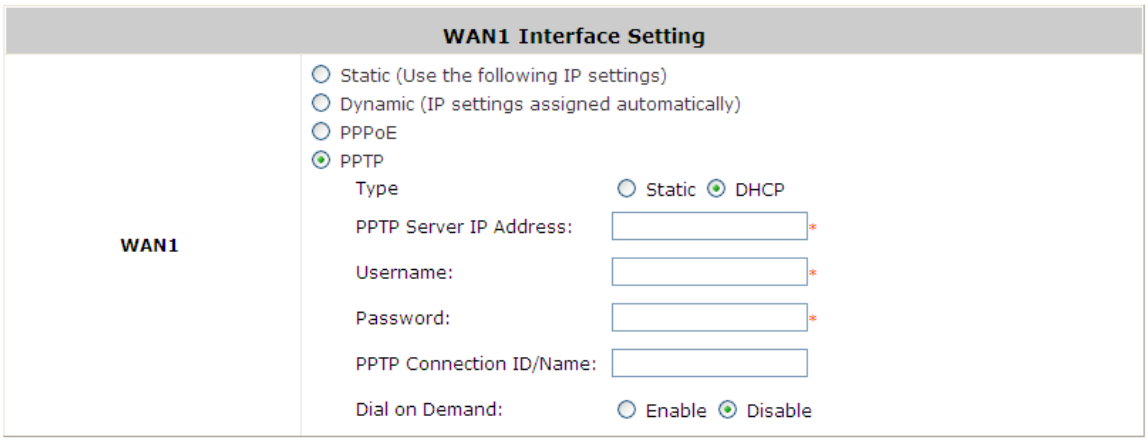
- **MTU:** Short for Maximum Transmission Unit of a PPPoE frame. The PPPoE protocol allows an Ethernet frame's size to be up to 1492 bytes, but some ISP's network equipments may support a smaller frame size of than 1492 bytes. In that case, you have to enter a smaller number MTU number to meet the ISP's networking requirement.
- **MSS:** Short for Maximum Segment Size for a TCP connection. An end-to-end TCP connection over PPPoE will consume additional overhead out of each packet. At least 40 bytes are used for the address. Hence, MSS must be smaller than MTU by at least 40.
- **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** will be available for input a value. When the idle time is reached, the system will automatically disconnect itself.

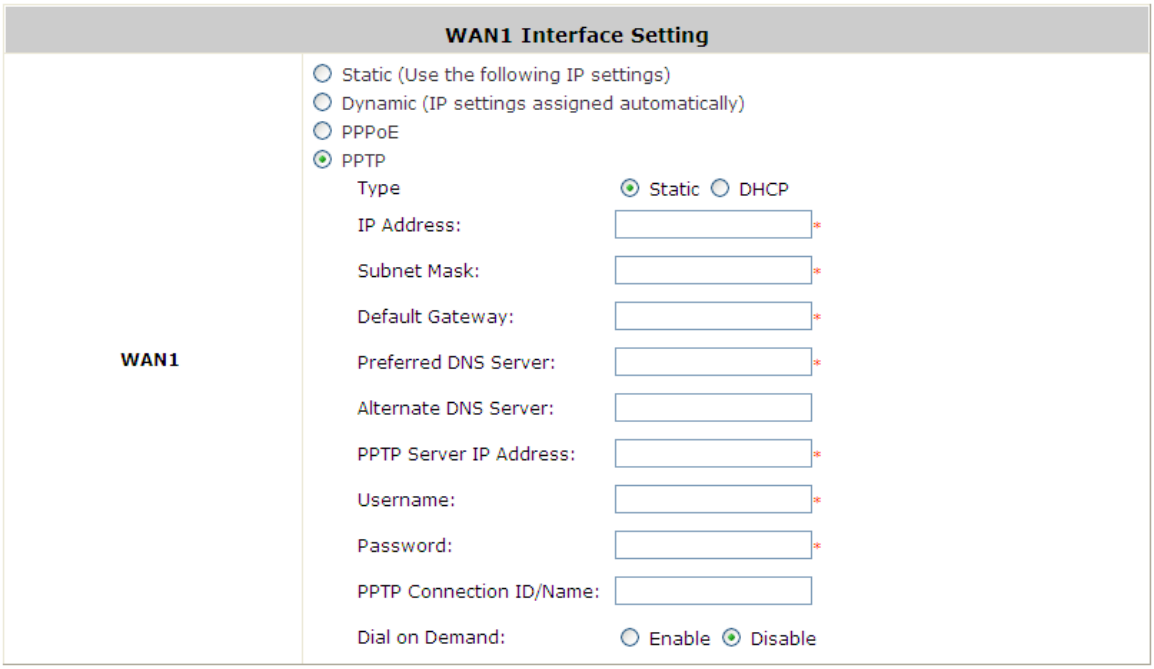


3.2.4 PPTP

Although not a popular method, PPTP protocol for dialup connections is adapted by some ISPs (in European Countries). AMG-2102 offers the PPTP dialup feature for the rare cases. Your PPTP ISP will issue you an account with a password as well as the PPTP server address.

- **PPTP:** When selecting PPTP to connect to the network, please specify the given **PPTP Server IP Address** and enter the **"User Name"**, **"Password"**.
  - **Static or DHCP:** Select **Static** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically.
  - **Dial on demand** function under PPTP: If this function is enabled, a **Maximum Idle Time** will be available for input a value. When the idle time is reached, the system will automatically disconnect itself.




WAN1 Interface Setting
WAN1
Static (Use the following IP settings)
Dynamic (IP settings assigned automatically)
PPPoE
PPTP
Type
Static
DHCP
IP Address:
Subnet Mask:
Default Gateway:
Preferred DNS Server:
Alternate DNS Server:
PPTP Server IP Address:
Username:
Password:
PPTP Connection ID/Name:
Dial on Demand:
Enable
Disable

3.3 Configuring WAN2 Port (optional)

AMG-2102 also supports a second WAN port, called WAN2. The second port is for connecting to a second feeding pipe upstream. When WAN1 is connected to an ISP and WAN2 is connected to another ISP, the network is referred as 'dual ISP homing', or 'having dual homed Internet feed'. That is when the first ISP via WAN1 is down, the second ISP via WAN2 still be able to service the client devices downstream of AMG-2102.

When WAN2 is enabled, the system can be set up to support more features, such as WAN Failover and Load Balance (but not a necessity). These two features will discuss in the next section (Other WAN traffic Settings).

Note:

By default, all Policies of AMG-2102 use WAN1 as the outgoing gateway; that is, all user groups' traffic will use WAN1 as the Internet feed. Administrator can change the Routing Profile of a Policy to use WAN2 as default gateway; that way, for the groups bounded by the Policy will use WAN2 as their Internet feed.

If dynamic "WAN Load Balancing" feature is not turned on, using the Policy's Routing Profile to route some users' traffics to WAN2 is considered a way of doing static "Load Balancing".

The configuration of WAN2 is similar to WAN1's, except that WAN2 connection can be disabled and WAN2's connection type does not have the PPTP choice.

If you only have one Internet feed from one ISP, please leave the WAN2 at its default option - **None,** so the WAN2 interface remains disable. If you want to use a second Internet feed (from an ISP or from your corporate headquarter), select one of the three connection types for your WAN2 port: **Static, Dynamic,** and **PPPoE**.

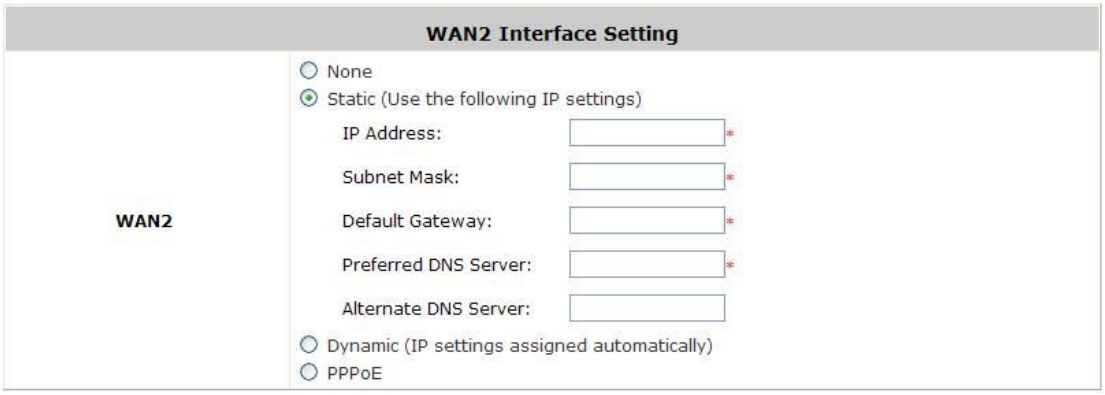
Now, let us enable and configure WAN2 port (optional):

Go to: ***System >> WAN2***.

- **None**: The WAN2 Port is disabled.

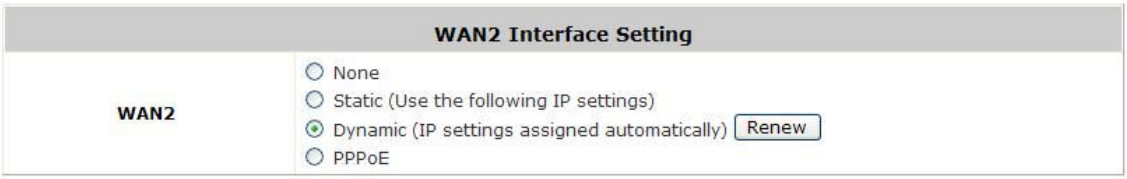
WAN2 Interface Setting	
WAN2	◉ None ○ Static (Use the following IP settings) ○ Dynamic (IP settings assigned automatically) ○ PPPoE

- **Static:** Manually specifying the IP address of the WAN port. The red asterisks indicate required fields to be filled in.

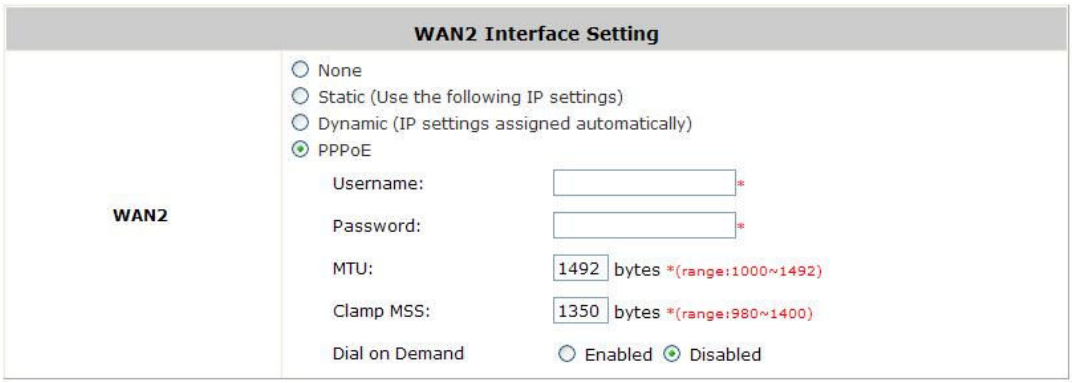


  - **IP Address:** the IP address of the WAN2 port.
  - **Subnet Mask:** the subnet mask of the network WAN2 port connects to.
  - **Default Gateway:** a gateway of the network WAN2 port connects to.
  - **Preferred DNS Server:** The primary DNS server used by the system.
  - **Alternate DNS Server:** The substitute DNS server used by the system. This is an optional field.

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



- **PPPoE:** When selecting PPPoE to connect to the network, please set the **"User Name"**, **"Password"**.
  - **MTU:** Short for Maximum Transmission Unit of a PPPoE frame. The PPPoE protocol allows an Ethernet frame's size to be up to 1492 bytes, but some ISP's network equipments may support a smaller frame size of than 1492 bytes. In that case, you have to enter a smaller number MTU number to meet the ISP's networking requirement.
  - **MSS:** Short for Maximum Segment Size for a TCP connection. An end-to-end TCP connection over PPPoE will consume additional overhead out of each packet. At least 40 bytes are used for the address. Hence, MSS must be smaller than MTU by at least 40.
  - **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** will be available for input a value. When the idle time is reached, the system will automatically disconnect itself.



3.4 Other WAN Traffic Settings

It is a good idea to have two Internet feeds to the system, especial from two different ISP; it adds the service reliability to your clients by turning on WAN-Failover feature. When one feed is out-of-service, the other feed automatically picks up the responsibly of serving the clients under the feed that goes outage.

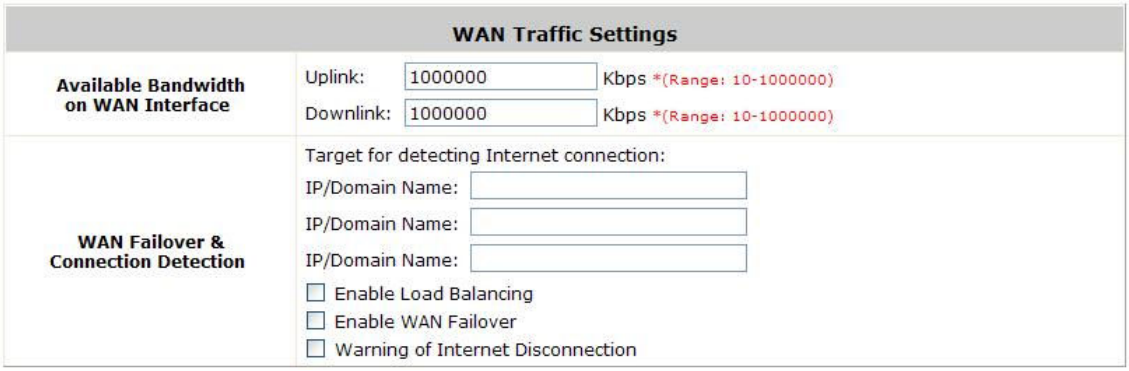
By default, the system assumes there is only one feed to WAN1. All the Policies by default route all clients' internet traffic via WAN1, using the Internet pipe at WAN1. When you have two pipes, you certainly want to set some Policies to utilize the bandwidth of the second pipe at WAN2, rather then just when the WAN1 pipe fails.

Beside the static load balancing by setting "Policy" route, alternatively, you can use the system's dynamic Load-Balancing feature. When the feature is turned on, the system can distribute the load of the up-going traffics to the two WAN pipes, according to the weight percentage assigned by the administrator.

3.4.1 WAN Failover

Configure WAN Failover:

Go to: ***System >> WAN Traffic***.

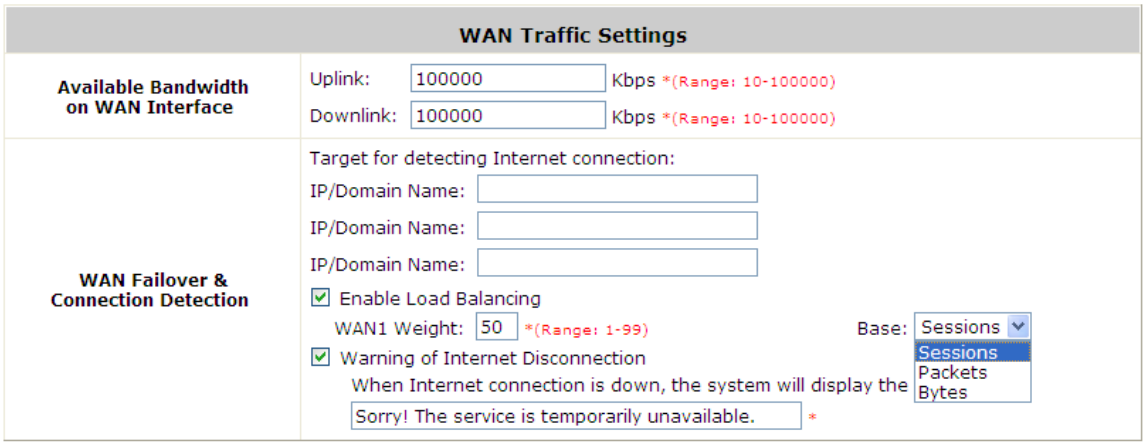


- **Enable WAN Failover:** Normally AMG-2102 uses WAN1 as it primary WAN interface. When **WAN Failover** is enabled and WAN2 is available, WAN1's traffic will be routed to WAN2 when WAN1 connection is down. On the other hand, a Service Zone's policy could also use WAN2 as its interface; in that case, if WAN2 is down, the WAN2's traffic under its policy will also be routed to WAN1.
  - **Fall back to WAN1 when WAN1 is available again:** If WAN Failover is enabled, the traffic will be routed to WAN2 automatically when WAN1 connection fails. When **fall back to WAN1** is enabled, the routed traffic will be connected back to WAN1 when WAN1 connection is recovered.

3.4.2 Load Balance

Configure Load Balance:

Go to: ***System >> WAN Traffic***.



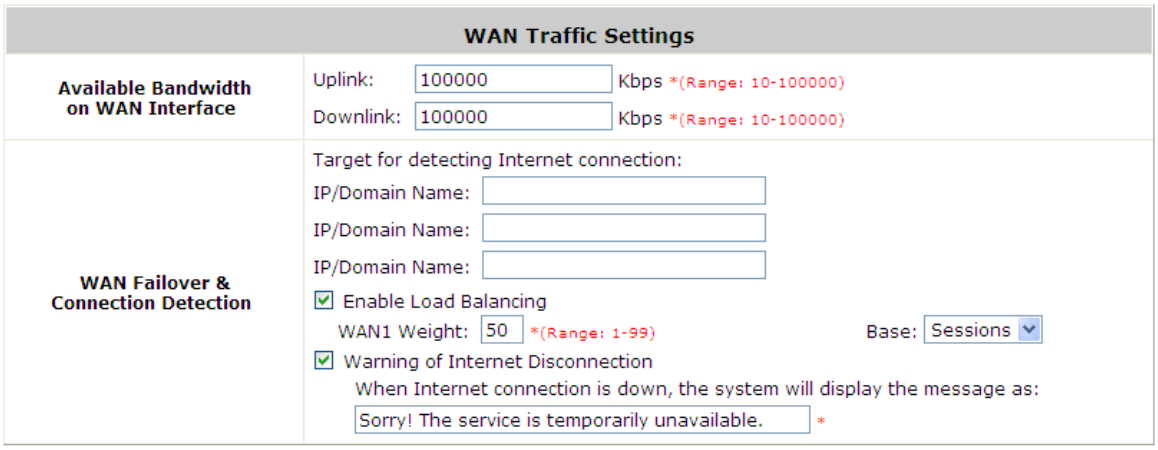
- **Enable Load Balancing:** Outbound load balancing is supported by the system. When enabled, the system will allocate traffic between WAN1 and WAN2 dynamically according to designed algorithms based on the weight ratio.
  - **WAN1 Weight:** The percentage of traffic through WAN1. (Range: 1~99; by default, it is 50)
  - **Base:** The weight ratio between WAN1 and WAN2 can be based on Sessions, Packets or Bytes. Packets and Bytes are based on historic data. New connection sessions will be distributed between WAN1 and WAN2 by a weight ratio using random number.

3.4.3 Internet Connection Detection

The system will periodically check to see if the Internet (uplink) connection is down by seeing if it can get responses from three target sites.

The administrator can specify the three target sites:

Go to: ***System >> WAN Traffic***.



Administrator can further specification a warning text, which will be displayed to the client "Login Success Page".

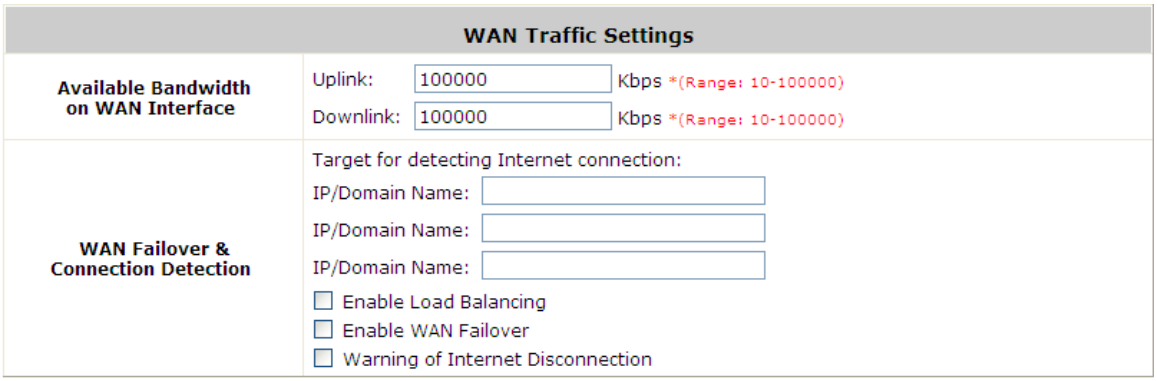
- **Warning of Internet Disconnection:** When enabled, there is a text box available for the administrator to enter a reminding message. This reminding message will appear on clients' screens when Internet connection is down.

3.4.4 WAN Bandwidth Control

The section is for administrators to configure the control over the entire system's traffic though the WAN interface (WAN1 and WAN2 ports).

To configure WAN Bandwidth Limit:

Go to: ***System >> WAN Traffic***.



These parameters in the raw of **Available Bandwidth on WAN Interface** are used for matching to the real bandwidth come from your ISP.

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

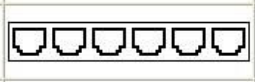
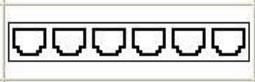
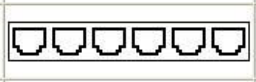
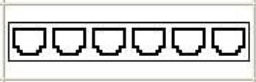
3.5 LAN Partition -- Service Zone

Configure Service Zone, go to: ***System >> Service Zones***.

A *Service Zone* is a logical network area to cover certain wired and wireless networks in an organization such as SMB or branch offices. By associating a unique VLAN Tag and SSID with a Service Zone, administrators can separate wired network and wireless network into different logical zones. Users attempting to access the resources within the Service Zone will be controlled based on the access control profile of the Service Zone, such as authentication, security feature, wireless encryption method, traffic control, and etc.

There are up to nine Service Zones to be utilized; by default, they are named as: **Default**, **SZ1~SZ8**, as shown in the table below.

Service Zone Settings

Service Zone Name	LAN Port Mapping	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default		SSID0	None	Policy 1	Server 1	Enabled	Configure
SZ1		SSID1	None	Policy 1	Server 1	Disabled	Configure
SZ2		SSID2	None	Policy 1	Server 1	Disabled	Configure
SZ3		SSID3	None	Policy 1	Server 1	Disabled	Configure
SZ4		SSID4	None	Policy 1	Server 1	Disabled	Configure
SZ5		SSID5	None	Policy 1	Server 1	Disabled	Configure
SZ6		SSID6	None	Policy 1	Server 1	Disabled	Configure
SZ7		SSID7	None	Policy 1	Server 1	Disabled	Configure
SZ8		SSID8	None	Policy 1	Server 1	Disabled	Configure

Port-Base

Service Zone Settings							
Service Zone Name	**VLAN Tag**	**SSID**	**WLAN Encryption**	**Applied Policy**	**Default Authen Option**	**Status**	**Details**
Default	N/A	SSID0	None	Policy 1	Server 1	Enabled	Configure
SZ1	1	SSID1	None	Policy 1	Server 1	Disabled	Configure
SZ2	2	SSID2	None	Policy 1	Server 1	Disabled	Configure
SZ3	3	SSID3	None	Policy 1	Server 1	Disabled	Configure
SZ4	4	SSID4	None	Policy 1	Server 1	Disabled	Configure
SZ5	5	SSID5	None	Policy 1	Server 1	Disabled	Configure
SZ6	6	SSID6	None	Policy 1	Server 1	Disabled	Configure
SZ7	7	SSID7	None	Policy 1	Server 1	Disabled	Configure
SZ8	8	SSID8	None	Policy 1	Server 1	Disabled	Configure

Tag-Base

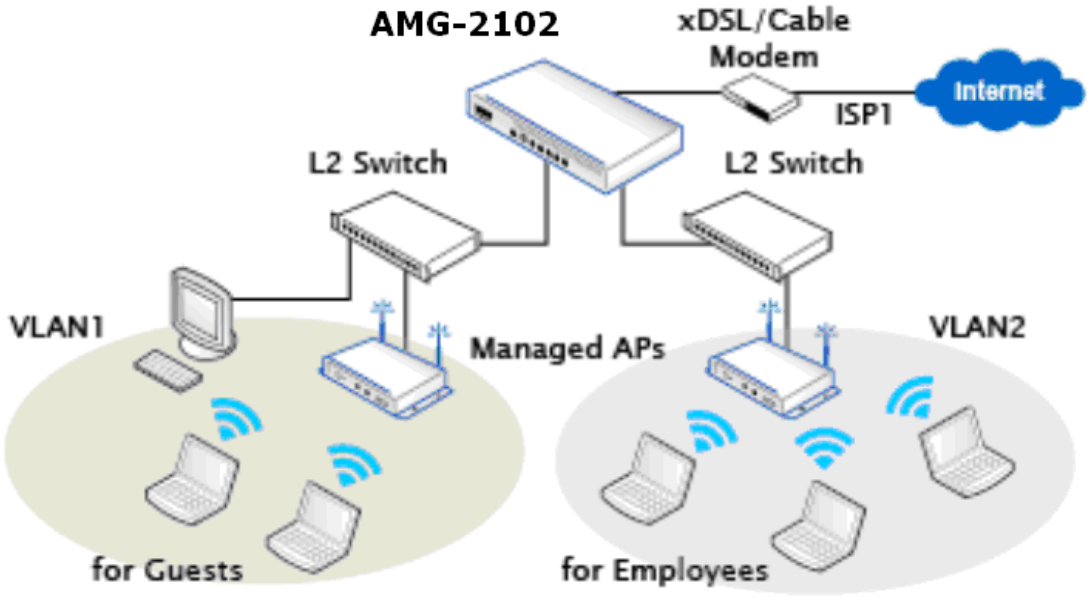
- **Service Zone Name:** Mnemonic name of the Service Zone.
- **LAN Port Mapping (Port Base only):** Choose which port is mapped to which Service Zone.
- **VLAN Tag (Tag Base only):** The VLAN tag number that is mapped to the Service Zone.
- **SSID:** The SSID that is associated with the Service Zone.
- **WLAN Encryption:** Data encryption method for wireless networks within the Service Zone.
- **Applied Policy:** The policy that is applied to the Service Zone.
- **Default Authen Option:** Default authentication method/server that is used within the Service Zone.
- **Status:** Each Service Zone can be enabled or disabled.
- **Details:** Configurable, detailed settings for each Service Zone.

Click ***Configure*** button to configure each Service Zone: **Basic Settings**, **SIP Interface Configuration**, **Authentication Settings**, **Wireless Settings**, and **Managed AP(s) in this Service Zone**.

3.5.1 Planning your internal network

1. Simple network environment

For most simple internal network, such as there are just only two subnets. Using Port-Based model is an easy and better way. In **Port-Based** mode, each LAN port can only serve traffic from one Service Zone. An example of network application diagram is shown as below: one Service Zone for **Employees** and one for **Guests**.

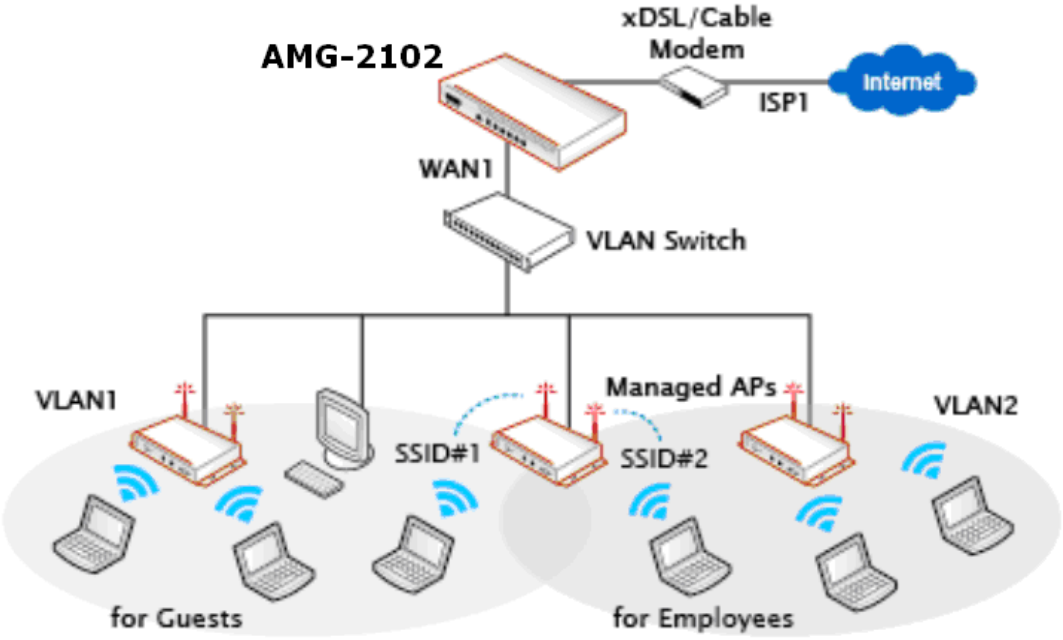


Caution:

The switches deployed under AMG-2102 in Port-Based mode must be Layer 2 switches only.

2. Multi subnet network environment

On the other hand, if the internal network is a multi subnets network environment. Tag-Based model will satisfy to your conditions. In **Tag-Based** mode, each LAN port will only serve traffic from Default Service Zone. So you need a VLAN switch or VLAN AP to take care the VLAN tags carried within the message frames. An example of network application diagram is shown as below: more than two Service Zones for different departments.

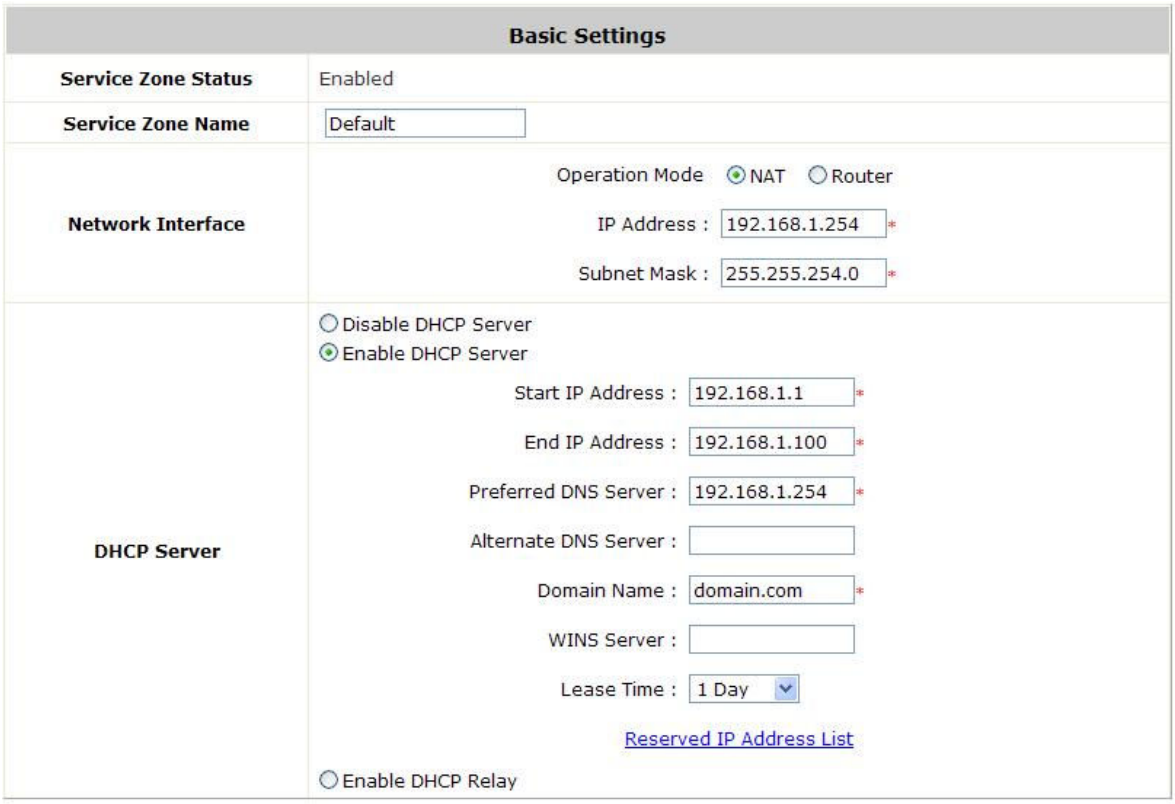


Caution:

*The switch deployed under AMG-2102 in **Tag-Based** mode must be a **VLAN switch** only.*

3.5.2 Configure Service Zone network

Configure Service Zone, go to: ***System >> Service Zones***.



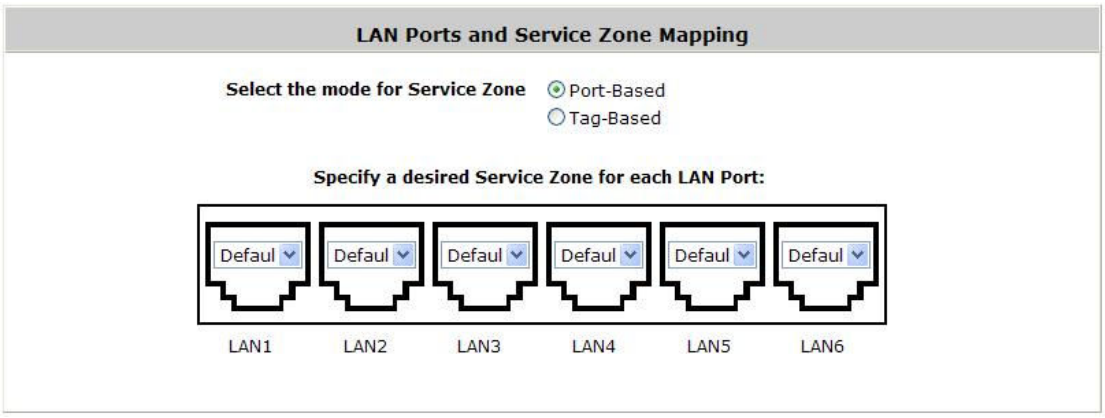
- **Service Zone Status:** Each service zone can be enabled or disabled except for the default service zone.
- **Service Zone Name:** The name of service zone could be input here.
- **Network Interface:**
  - **VLAN Tag (Tag-Base only):** The VLAN tag of this service zone.
  - **Operation Mode:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, the service zone runs in NAT mode. When Router mode is chosen this service zone runs in Router mode.
  - **IP Address:** The IP Address of this service zone.
  - **Subnet Mask:** The subnet Mask of this service zone.

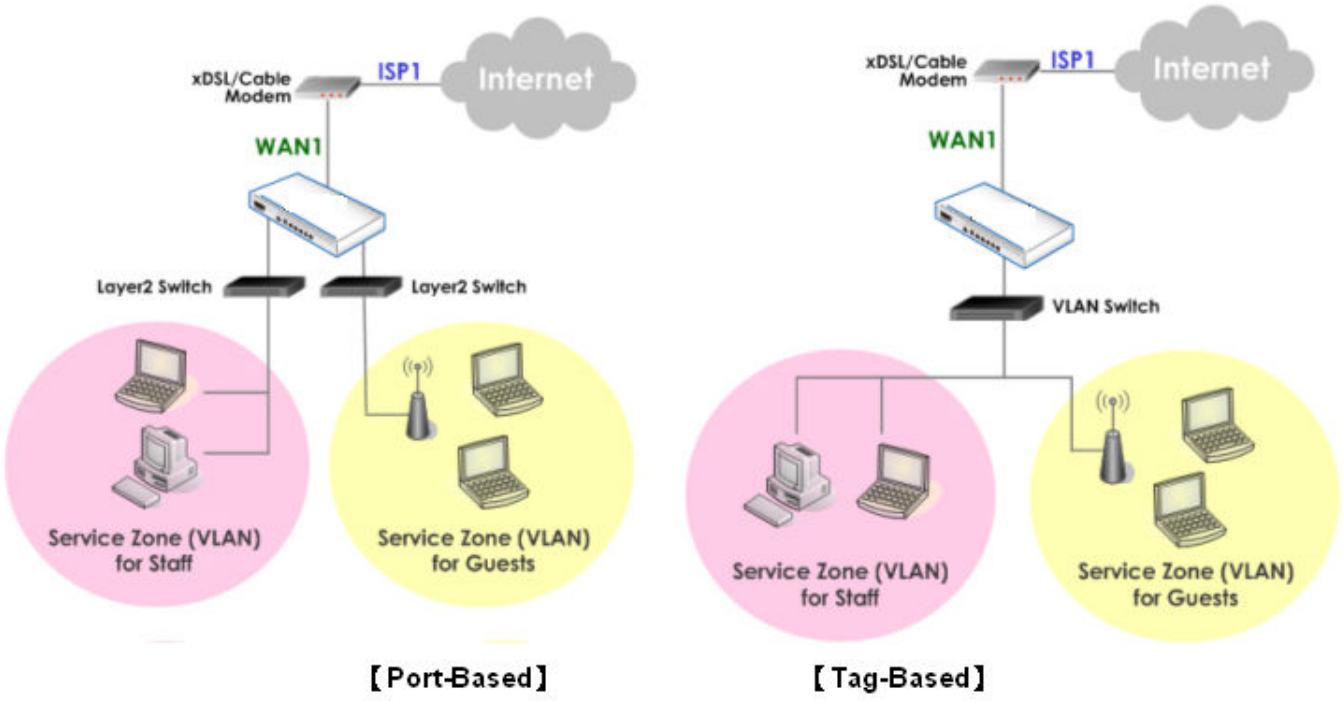
- **DHCP Server:** Related information needed on setting up the DHCP Server is listed here. Please note that when "*Enable DHCP Relay"* is enabled, the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this service zone.
  - **Start IP Address / End IP Address:** A range of IP addresses that built-in DHCP server will assign to clients. Note: please change the Management IP Address List accordingly (at *System Configuration>> System Information >> Management IP Address List*) to permit the administrator to access the AMG-2102 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 Service Zone.
  - **Alternate DNS Server:** The substitute DNS server that is used by this Service Zone.
  - **Domain Name:** Enter the domain name for this service zone.
  - **WINS Server:** The IP address of the WINS (Windows Internet Naming Service) server that if WINS server is applicable to this service zone.
  - **Lease Time:** This is the time period that the IP addresses issued from the DHCP server are valid and available.
  - **Reserved IP Address List:** Each service zone can reserve up to 40 IP addresses from 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 certain MAC address.

3.5.3 Tag Base and Port Base

Configure Tag Base or Port Base, go to: ***System >> LAN Port Mapping***.

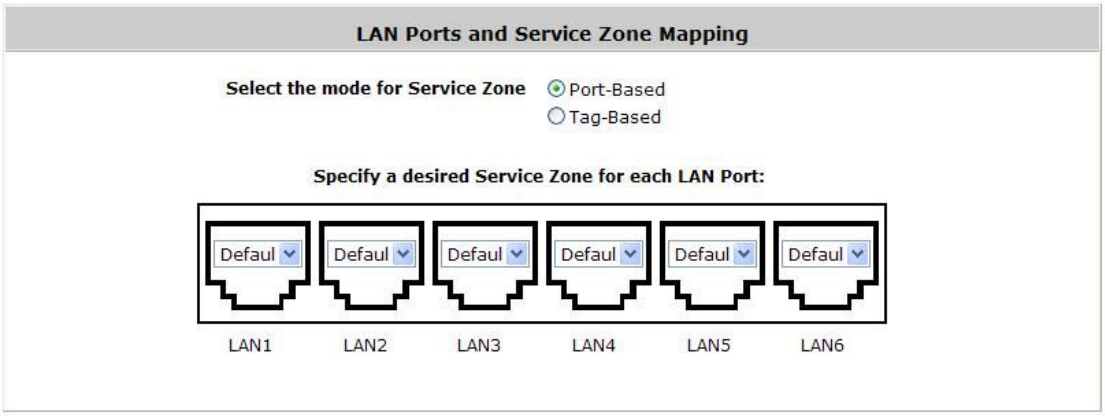
AMG-2102 supports multiple Service Zones in either of the two VLAN modes, **Port-Based** or **Tag-Based**, but not concurrently. In **Port-Base** mode, each LAN port can only serve traffic from one Service Zone as each Service Zone is identified by physical LAN ports. In **Tag-Based** mode, each LAN port can serve traffic from any Service Zone as each Service Zone is identified by VLAN tags carried within message frames. **By default, the system is in Port-Based mode with Default Service Zone enabled and all LAN ports are mapped to Default Service Zone.** Compare the two figures below to see the differences.





It is recommended that the administrator decides which mode is better for a multiple-service-zone deployment before proceeding further with the system configuration. Settings for the two VLAN modes are slightly different, for example, the VLAN Tag setting is required for Tag-Based mode.

- **Select Service Zone Mode**: Select a VLAN mode, either ***Port-Based*** or ***Tag-Based***.



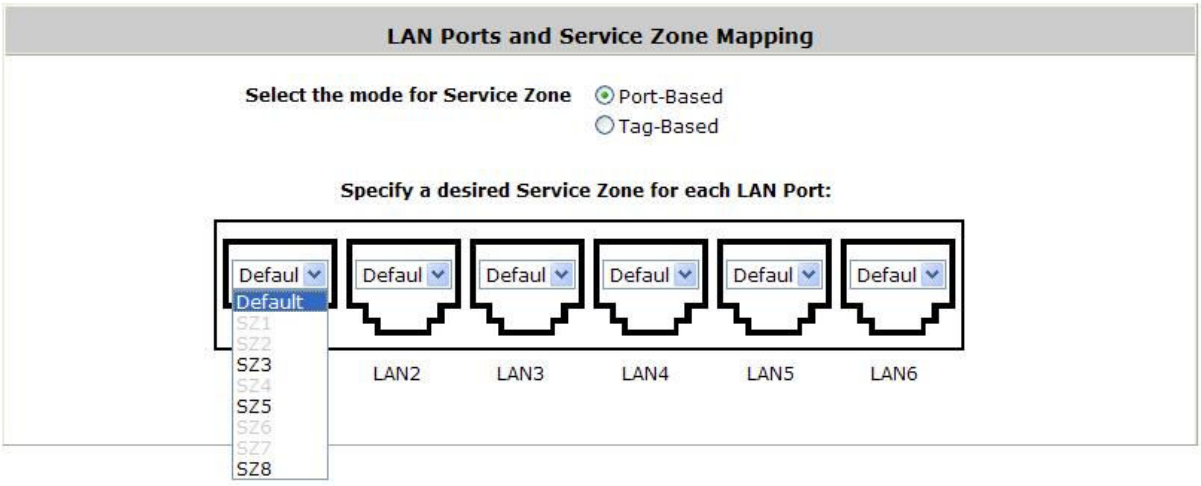
Caution:

The switches deployed under AMG-2102 in Port-Based mode must be Layer2 Switches only. The switch deployed under AMG-2102 in Tag-Based mode must be a VLAN switch only.

- **Port-Based:** When Port-Based mode is selected; traffic from different virtual Service Zones will be distinguished by physical LAN ports. Each LAN port can be mapped to one Service Zone in the form of a many-to-one mapping between ports and Service Zones.

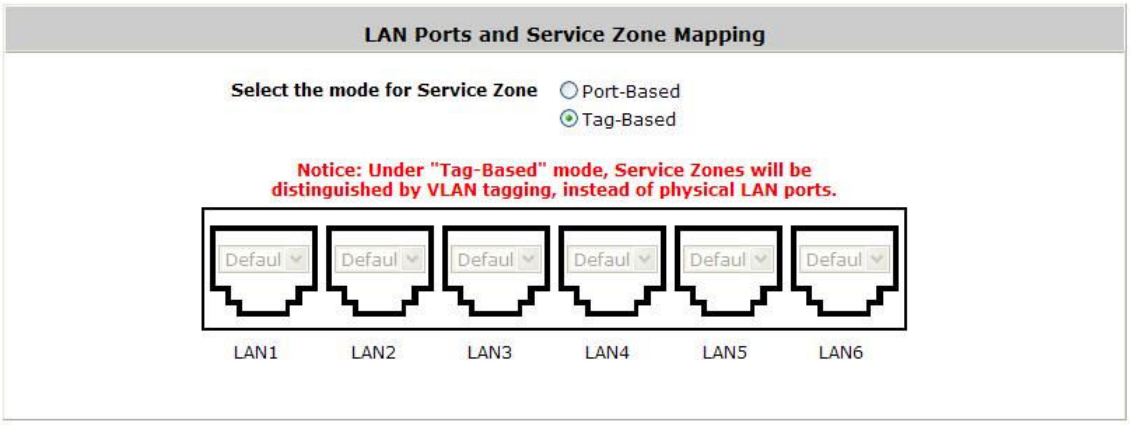
  - **Specify a desired Service Zone for each LAN Port:** For each LAN port, select a Service Zone to which the LAN port is to be mapped from the drop-down list box.

    By factory default, all LAN ports are mapped to Default Service Zone; therefore, the administrator can enter the web management interface via any LAN port upon the first power up of the system. From the drop-down list box, all disabled Service Zones are gray-out; to activate any desired Service Zone, please configure the desired Service Zone under the **Service Zone** tab and enable its *Service Zone Status*.



- **Tag-Based:** When the Tag-Based mode is selected, traffic from different virtual Service Zones will be distinguished by VLAN tagging, instead of by physical LAN ports.

  Select *Tag-Based* and then click ***Apply*** to activate the Tag-Based VLAN function. When a restart message screen appears, do NOT restart the system until you have completed the configuration under the **Service Zones** tab first.


LAN Ports and Service Zone Mapping
Select the mode for Service Zone
Port-Based
Tag-Based
Notice: Under "Tag-Based" mode, Service Zones will be distinguished by VLAN tagging, instead of physical LAN ports.
Defaul
Defaul
Defaul
Defaul
Defaul
Defaul
LAN1
LAN2
LAN3
LAN4
LAN5
LAN6

4. User Authentication and Grouping

4.1 Type of Users

Configure Authentication, go to: ***Users >>Authentication***.

This section is for administrators to pre-configure authentication servers for the entire system. Concurrently up to four servers can be selected in the meantime and pre-configured here by administrators from the five types of authentication databases (LOCAL, POP3, RADIUS, LDAP, and NTDOMAIN). In addition, there are two optional servers, On-demand User and SIP, which also can be selected by the system.

Authentication Settings			
Auth Option	**Auth Database**	**Postfix**	**Group**
Server 1	LOCAL	local	Group 1
Server 2	POP3	pop3	Group 1
Server 3	RADIUS	radius	Group 1
Server 4	LDAP	ldap	Group 1
On-demand User	ONDEMAND	ondemand	Group 1
SIP	SIP	N/A	Group 1

- **Auth Option:** There are several authentication options supported by AMG-2102: Server 1 to Server 4, On-demand User, and SIP. Click the hyperlink of the respective Server Name to configure the authentication server.
- **Auth Database:** There are different authentication databases in AMG-2102: **LOCAL**, **POP3**, **RADIUS**, **LDAP** and **NTDOMAIN**. **ONDEMAND** and **SIP** are not depend on Server 1 to Server4, so these two authentication options always can be enabled in each service zone.
- **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.
- **Group:** An authentication option, such as POP3 or NT Domain, can be set as a Group with the same QoS or Privilege Profile setting.

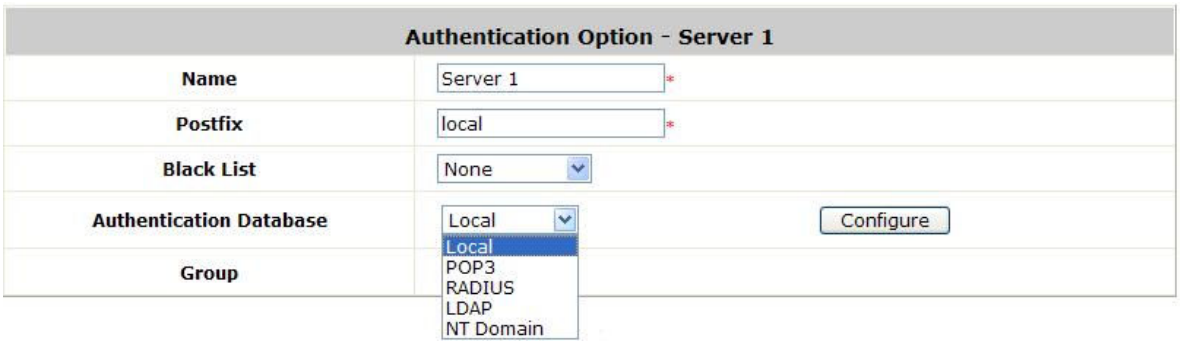
Note:

Concurrently only one server is allowed to be set as Local or NTDOMAIN authentication method simultaneously. For example, you can set two RADIUS authentication servers simultaneously.

- **Authentication Option Configuration**

  Click on the server name to set the configuration for that particular server. After completing and clicking ***Apply*** to save the settings, go back to the previous page to select a server to be the default server and enable or disable any server in each service zone. Users can log into the default server without the postfix to allow faster login process.

  Server 1~4: There are 5 authentication methods, **Local User, POP3, RADIUS, LDAP** and **NT Domain,** to select from.



  Name: Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_), space and dot (.) only. The length of this field is up to 40 characters. This name is used for the administrator to identify the authentication options easily such as HQ-RADIUS.

  Postfix: A postfix is used to inform the system which authentication option to be used for authenticating an account (e.g. bob@BostonLdap or tim@TaipeiRadius) when multiple options are concurrently in use. One of authentication option can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "BostonLdap" is the postfix of the default option, Bob can login as "bob" without having to type in "bob@BostonLdap". Set a postfix that is easy to distinguish (e.g. Local) and the server numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

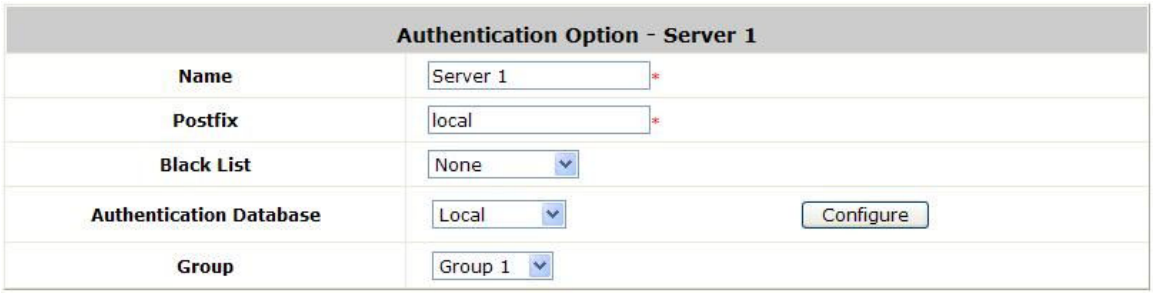
  Black List: There are multiple sets of black lists provided by the system. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one (or None) black list from the drop-down menu and this black list will be applied to this specific authentication option.

  Authentication Database: Click ***Configure*** button to enter the configuration page. For example, select *Local* from the drop-down list box and then click ***Configure*** button to enter the **Local User Database Settings**. Then, click the hyperlink of ***Local User List*.**

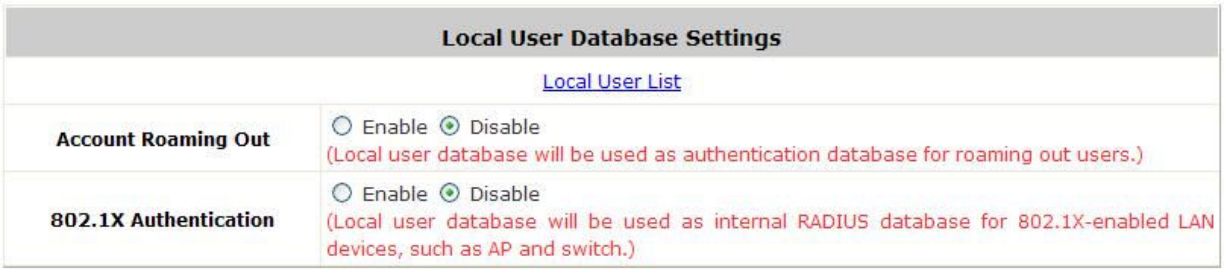
  Group: Select one Group from the drop-down list box for this specific authentication option.

4.1.1 Local

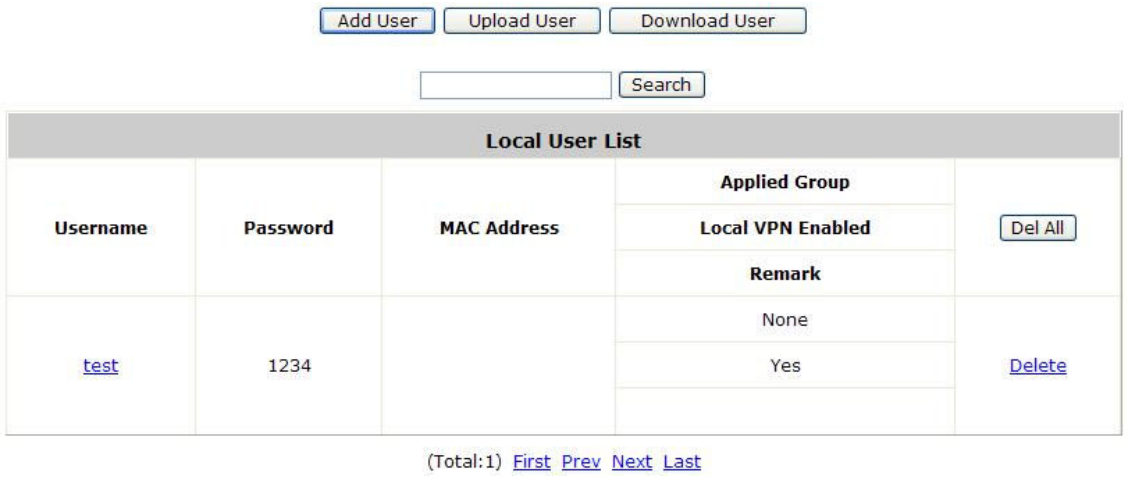
Choose **"Local"** from the **Authentication Database** field.



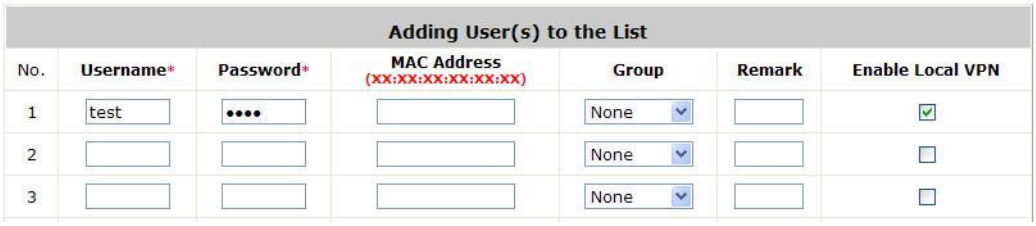
Click the button ***Configure*** for further configuration.



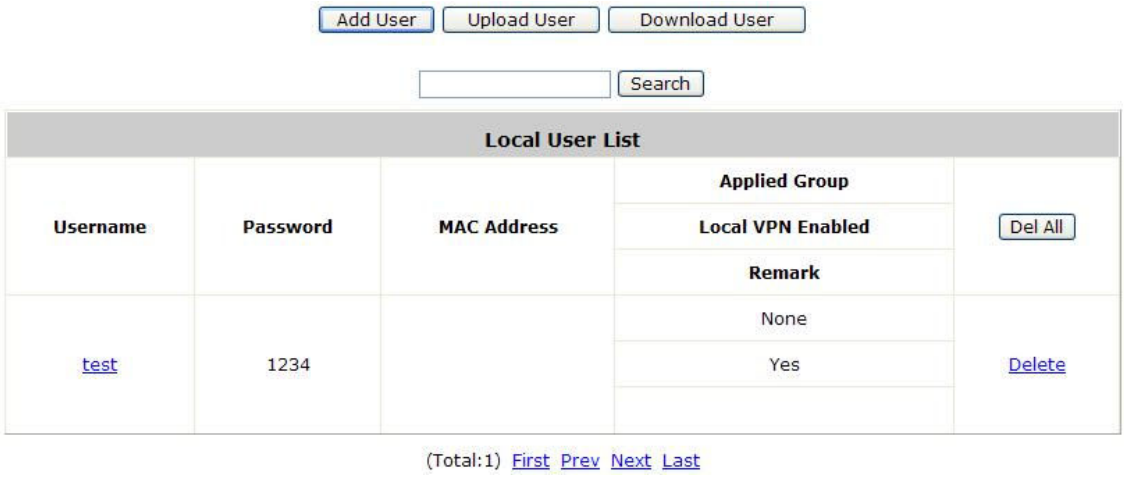
- **Local User List:** It let the administrator to view, add or delete local user account. The ***Upload User*** button is for importing a list of user account from a text file. The ***Download User*** button is for exporting all local user accounts into a text file. Clicking on each user account leads to a page for configuring the individual local account. Local user account can be assigned a Group and applied Local VPN individually.



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 **Group** to classify local users. Check to enable *Local VPN* in the **Enable Local VPN** column. Click ***Apply to complete adding the user(s). 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 this MAC address, so this user can not login with other networking device.

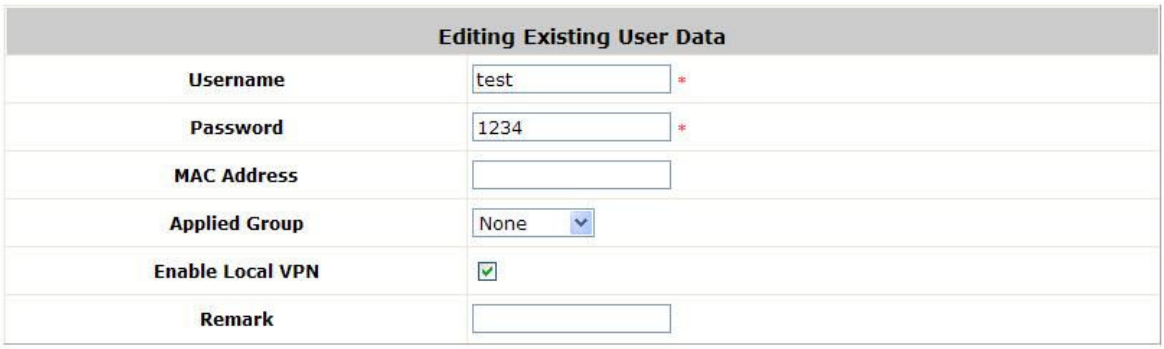


- ***Search*:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.



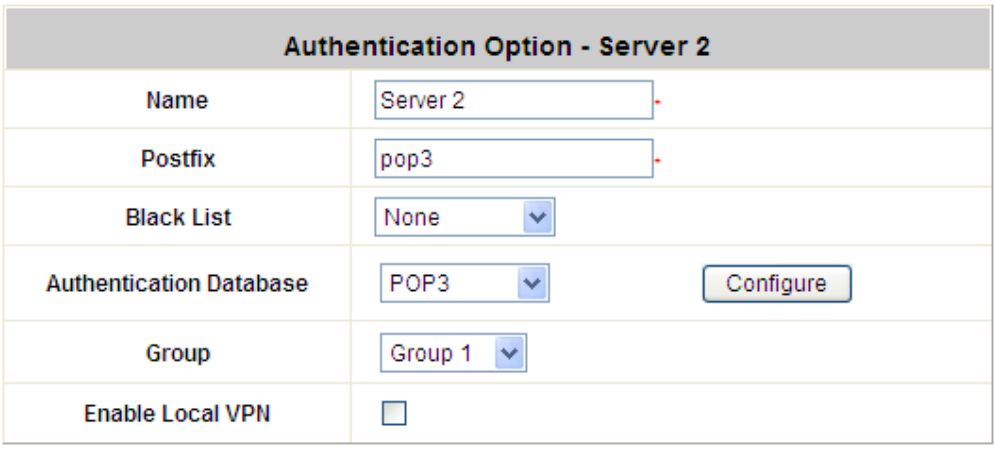
- ***Del All*:** Click on this button to delete all the users at once or click on ***Delete*** to delete the user individually.

- **Edit User:** If editing the content of individual user account is needed, click the username of the desired user account 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 Group* (optional), *Enable Local VPN* (optional) and *Remark* (optional). Click ***Apply*** to complete the modification.

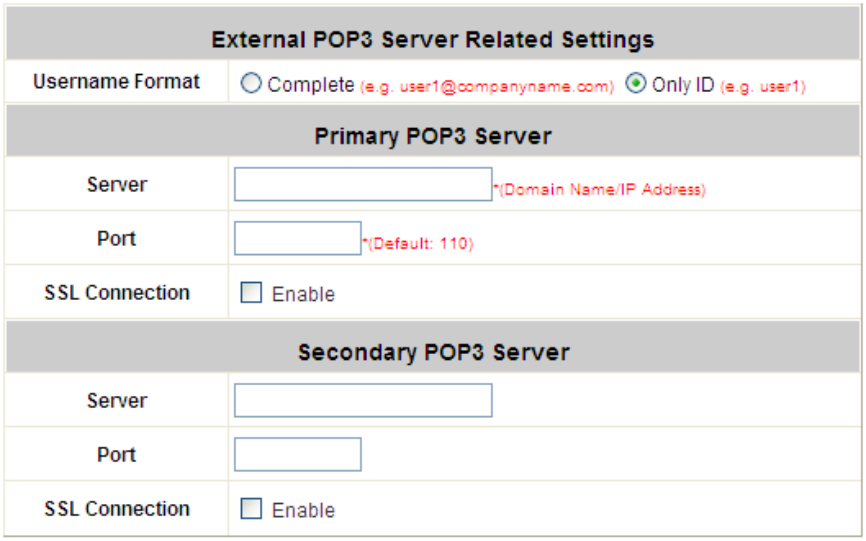


4.1.2 POP3

Choose **"POP3"** from the **Authentication Database** field. Except **Local** authentication, the **Local VPN** option in other authentication option only can be enabled or disabled for the entire **Authentication Database**.



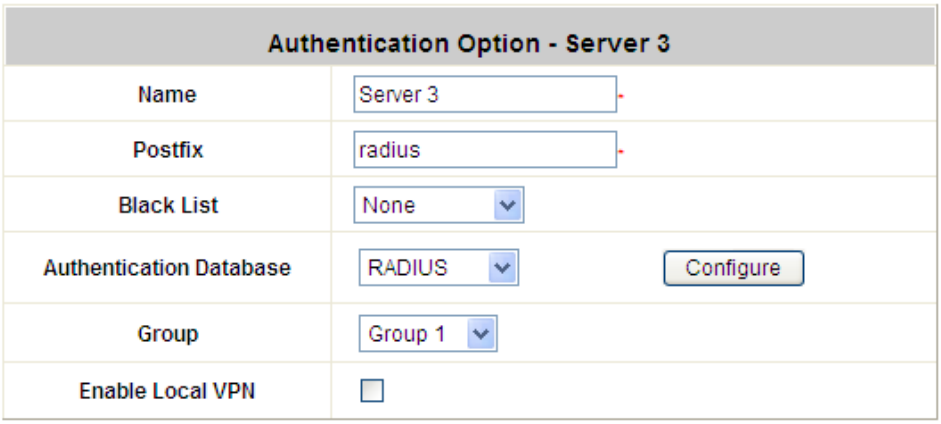
Click the button of ***Configure*** for further configuration. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The fields with red asterisk are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.



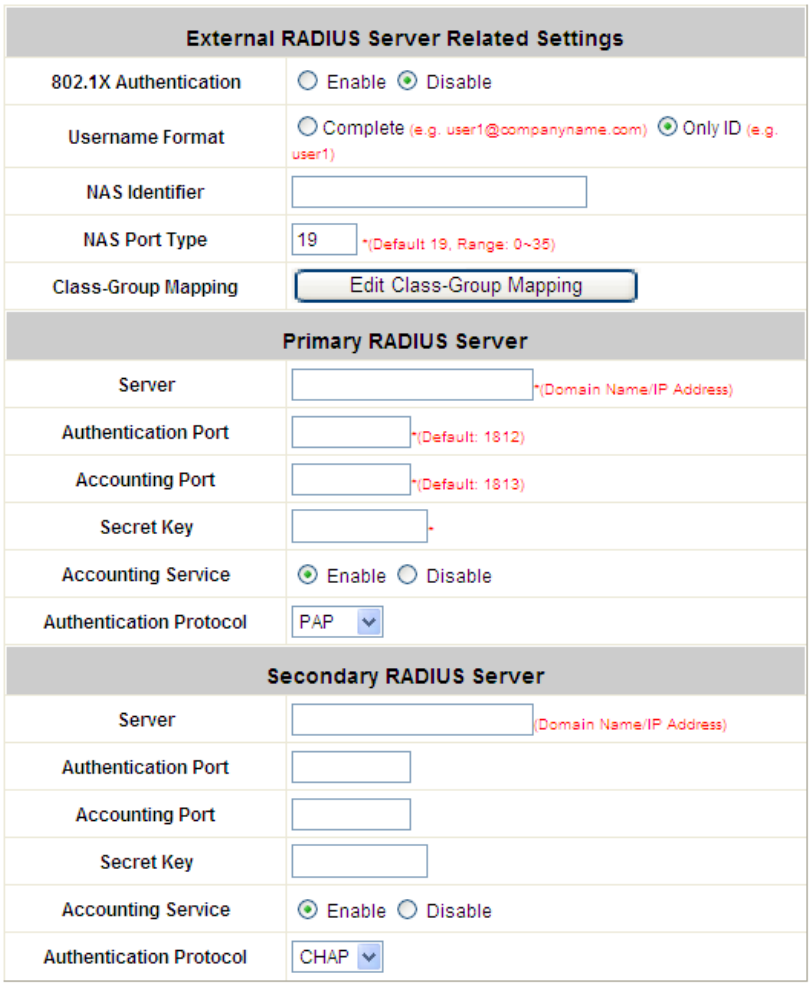
- **Username Format:** When ***Complete*** option is checked, both the username and postfix will be transferred to the server for authentication. When ***Only ID*** option is checked, only the username will be transferred to the external server for authentication.
- **Server:** The IP address of the external POP3 Server.
- **Port:** The authentication port of the external POP3 Server.
- **SSL Connection**: The system supports POP3S. Check the check box beside to **Enable SSL Connection** to POP3.

4.1.3 RADIUS

Choose **"RADIUS"** from the **Authentication Database** field. Except **Local** authentication, the **Local VPN** option in other authentication option only can be enabled or disabled for the entire **Authentication Database**.

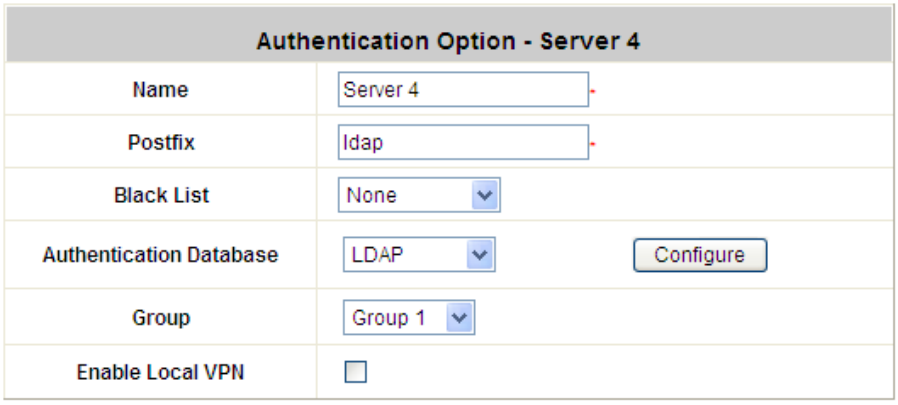


Click the button of ***Configure*** for further configuration. The RADIUS server sets the external authentication for user accounts. Enter the information for the primary server and/or the secondary server (the secondary server is not required). The fields with red asterisk are necessary information.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

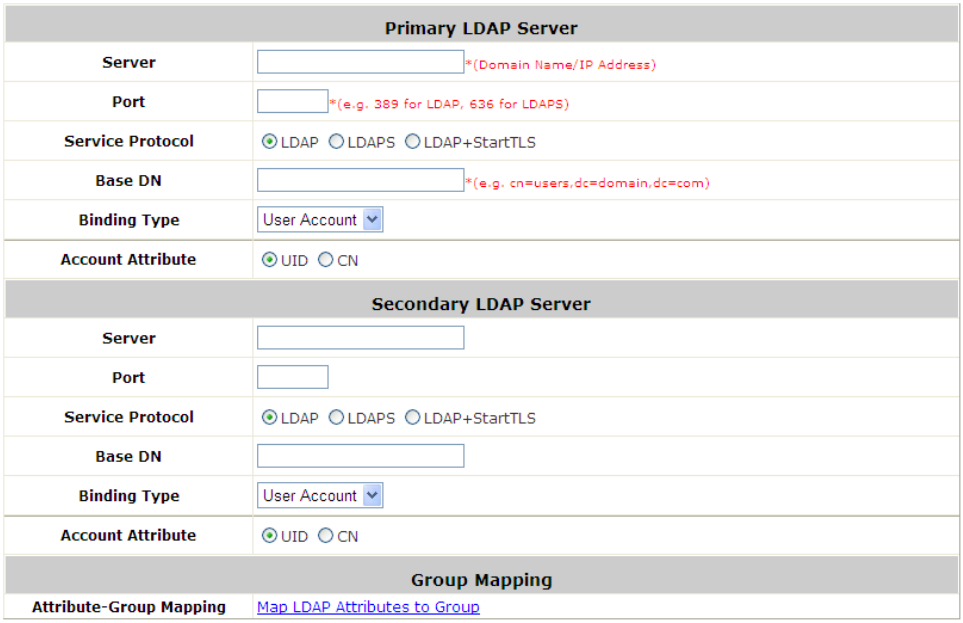


4.1.4 LDAP

Choose **"LDAP"** from the **Authentication Database** field. Except **Local** authentication, the **Local VPN** option in other authentication option only can be enabled or disabled for the entire **Authentication Database**.



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



- **Server:** The IP address of the external LDAP server.
- **Port:** The authentication port of the external LDAP server.
- **Service Protocol:** The transferring type of service protocol for LDAP authentication with 3 types available: LDAP, LDAPS, and LDAP+StartTLS.
- **Base DN:** The Base DN (Distinguished Name) is the LDAP search base, telling which part of the external directory tree to search from. Think of the Base DN as the "top" of the directory for your LDAP users although it may not always be the top of the directory itself. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.
- **Binding Type:** This specifies the binding type and search scope for LDAP authentication with 4 binding types available: User Account, Anonymous, Specified DN and Windows AD.

  User Account: Use the user account with base DN to authenticate user account/password.

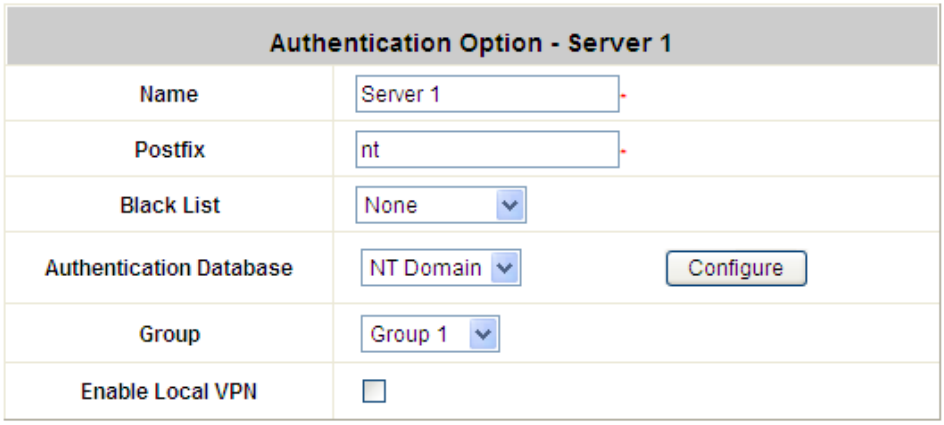
  Anonymous: Use anonymous to login LDAP server and use the user account with base DN to authenticate user account/password.

  Specified DN: Use the Admin DN/Bind password to login LDAP server and use the users' account with base DN to authenticate users' account/password.

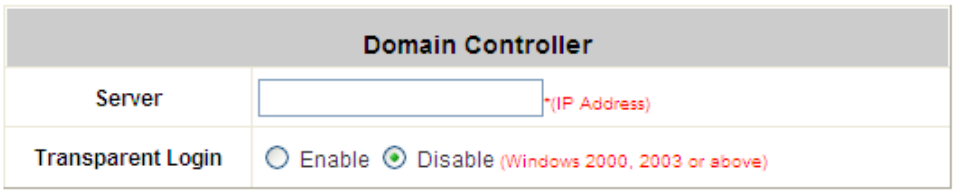
  Windows AD: Add a domain after user account with base DN to authenticate users' account/password.
- **Account Attribute**: The attribute of LDAP accounts.

4.1.5 NT Domain

Choose **"NT Domain"** from the **Authentication Database** field. Except **Local** authentication, the **Local VPN** option in other authentication option only can be enabled or disabled for the entire **Authentication Database**.



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



- **Server:** The IP address of the external NT Domain Server.
- **Transparent Login:** This function refers to Windows NT Domain single sign-on. When *Transparent Login* is enabled, clients will log into the system automatically after they have logged into the NT domain, which means that clients only need to log in once.

4.1.6 On-Demand Users

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

Authentication Server - On-demand User	
General Settings	Configure
Ticket Customization	Configure
Billing Plans	Configure
External Payment Gateway	Configure
On-demand Account Creation	Create
On-demand Account Batch Creation	Create
On-demand Account List	View

1) General Settings

This is the common setting for the On-demand User authentication option.

General Settings	
Postfix	ondemand
Currency	None $ USD £ GBP € EUR (Input other desired monetary unit, e.g. AU)
Group Name	Group 1
WLAN ESSID	SSID0
Wireless Key	
Remaining Volume Sync Interval	10min(s) 15min(s) 20min(s)
Terminal Server	Configuration
Expired Accounts Remain Days	15 *(1~30 days)
Delete All Expired Accounts	Delete

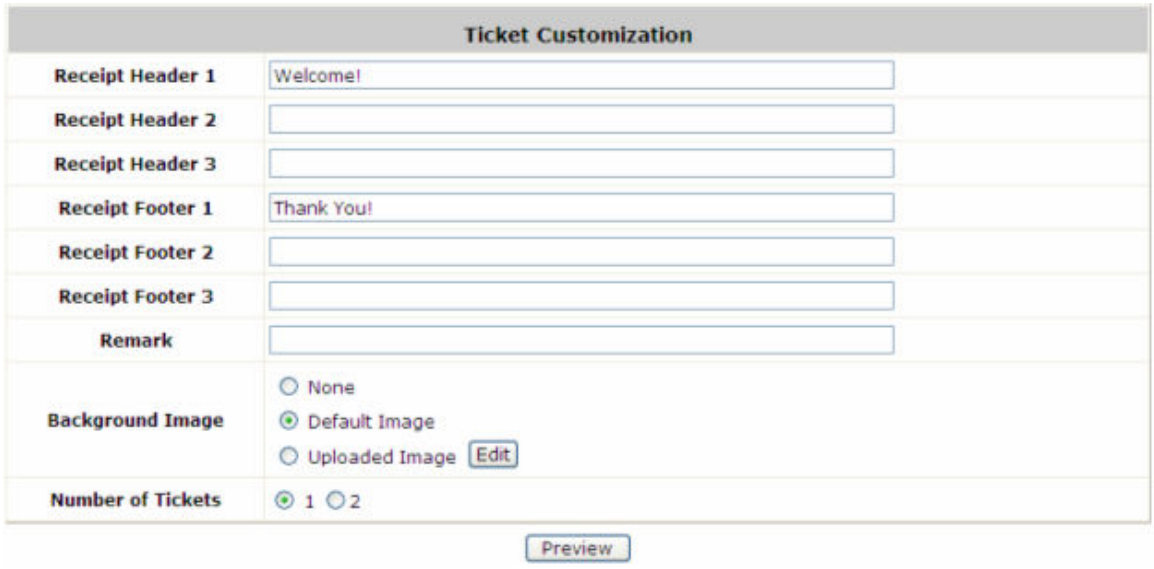
- **Currency:** Select the desired specified unit.
- **WLAN ESSID:** It will show the ESSID of Public Zone.
- **Wireless Key:** It will show the wireless key that configured in Public Zone.
- **Remaining Volume Sync Interval:** Enable it and input the count-down minute, system will remind users that their quota will run out soon when their quota reaches this time. The

reminding message will not show up if the Remaining Reminder time is configured longer than the quota of billing plans.

- **Expired Accounts Remain Days:** It will delete the expired accounts after the certain days.
- **Delete All Expired Accounts:** It will delete all expired accounts immediately.

2) Ticket Customization

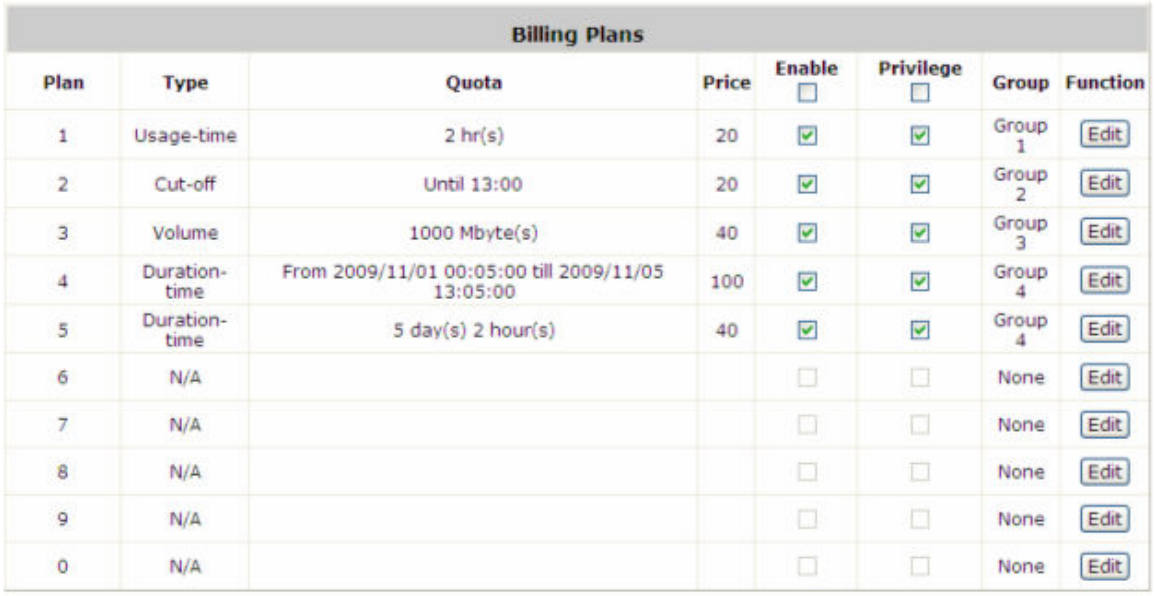
On-demand account ticket can be customized here and previewed on the screen.



- **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:** The entered content will be printed on the receipt. These footers are optional.
- **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.
- **Remark:** Enter any additional information that will appear at the bottom of the receipt.
- **Number of Tickets:** Enable this function to print duplicate receipts. Another Remark field will appear when 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 information of username and password with the selected background. Print the ticket here.

3) Billing Plans

Administrators can configure several billing plans. Click ***Edit*** button to enter the page of Editing Billing Plan. 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 be activated.

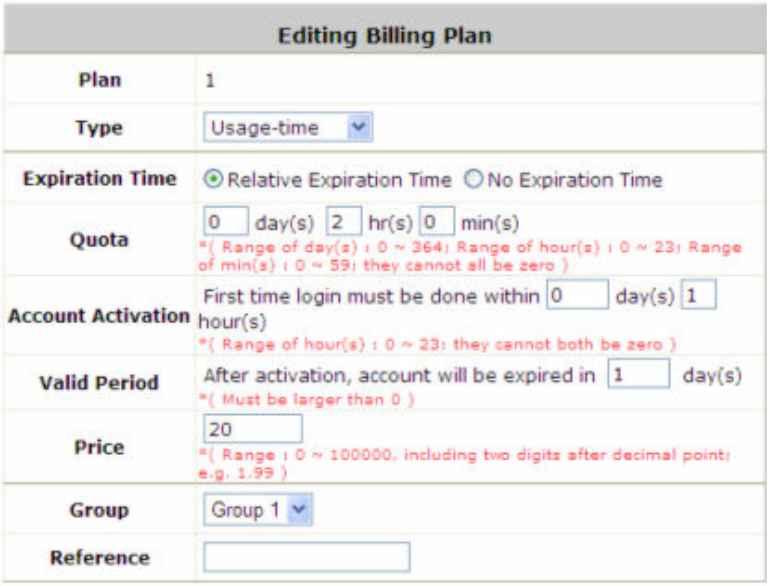


Billing Plans

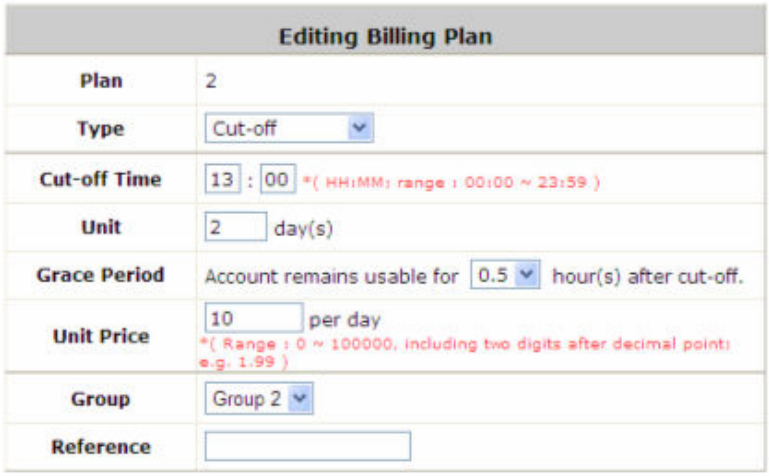
Plan	Type	Quota	Price	Enable	Privilege	Group	Function
1	Usage-time	2 hr(s)	20	☑	☑	Group 1	Edit
2	Cut-off	Until 13:00	20	☑	☑	Group 2	Edit
3	Volume	1000 Mbyte(s)	40	☑	☑	Group 3	Edit
4	Duration-time	From 2009/11/01 00:05:00 till 2009/11/05 13:05:00	100	☑	☑	Group 4	Edit
5	Duration-time	5 day(s) 2 hour(s)	40	☑	☑	Group 4	Edit
6	N/A			☐	☐	None	Edit
7	N/A			☐	☐	None	Edit
8	N/A			☐	☐	None	Edit
9	N/A			☐	☐	None	Edit
0	N/A			☐	☐	None	Edit

- **Plan:** The number of the specific plan.
- **Type:** This is the type of the plan, based on which it defines how the account can be used including Usage-time, Cut-off, and Duration-time.
- **Quota:** The limit on how On-demand users are allowed to access the network.
- **Enable:** Check the checkbox to activate the plan.
- **Function:** Click the button ***Edit*** to add one billing plan.
  - **Usage-time:** The scenario of this type is that a client goes to a cyber café and purchases an on-demand account. This account will be activated and ok to use once creation, quota will start to count down while creation and non-stop when logs out, and be expired after a configured time such as 4 hours or at 22:00 the day. For example, an on-demand account is created at 2009/6/30 18:00 and its quota is 4 hours. Thus it can become usable at 2009/6/30 18:00 and expired at 2009/6/30 22:00.
    - **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 for the first login time. If the first login time of this account is later that this settings. This account will be expired.
    - **Valid Period** is the valid time period for using. After this time period, although the quota is not exhausted, this account still is expired.

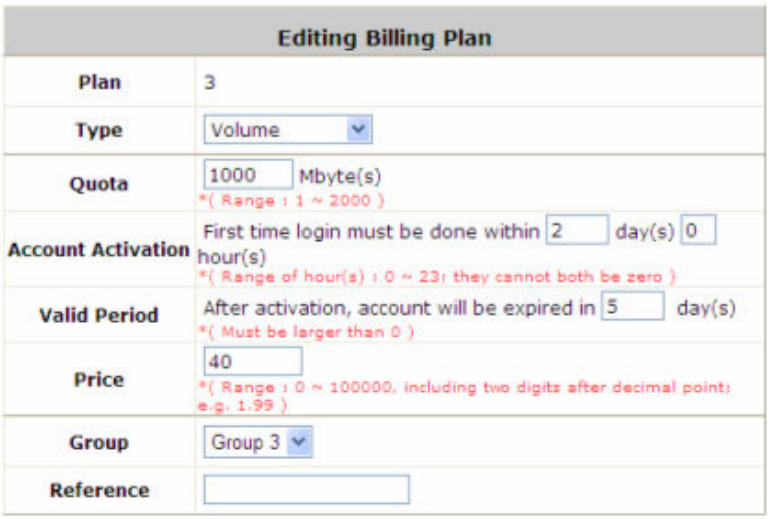
- **Price** is the unit price of this plan.



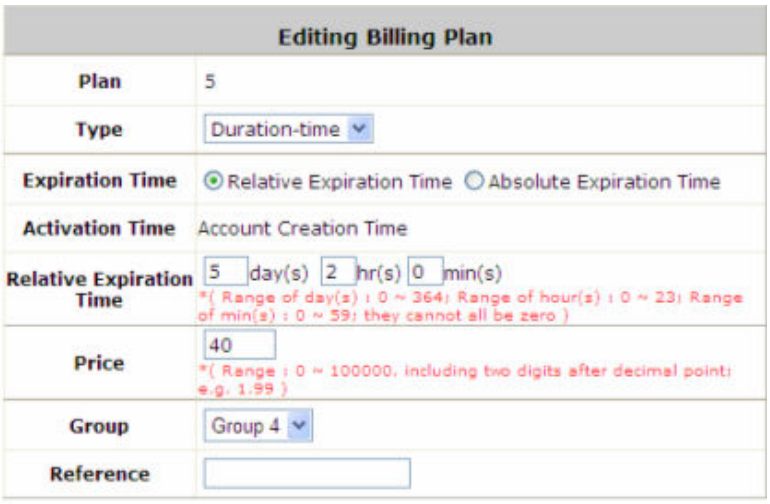
- **Cut-off: Cut-off Time** is the time of day at which the on-demand account is cut off (made expired) by the system on that day. **Unit** is the day periods of this Cut-off billing plan. Please note that the **Grace Period** is an additional, short period of time after the account is cut off, during which a user is allowed 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.



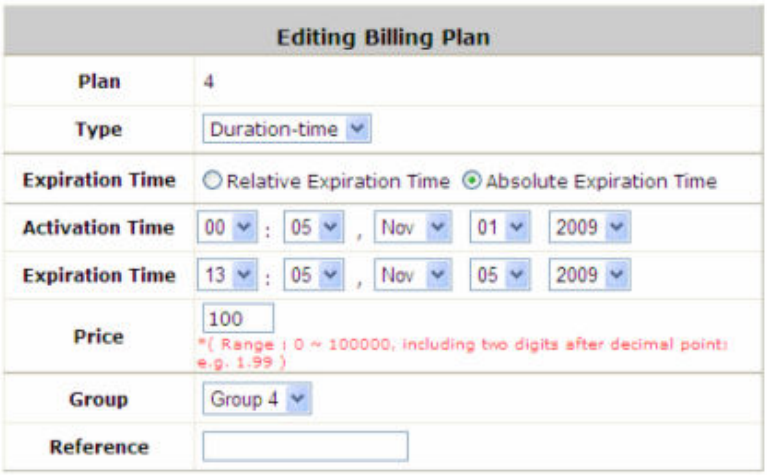
- **Volume: Volume** is the maximum Mbytes at which the on-demand account could be used by the system. **Quota** is the total Mbytes (1~2000), during which On-demand users are allowed to access the network.



- **Duration-time with Relative Expiration Time:** The scenario of this type is that a client purchases an on-demand account pre-paid card or a gift coupon with certain quota. This account must be activated before a configured activation time, will be activated and ok to use since the first login, its quota will be cut down while using only, and will not be expired unless its quota is used up. For example, an on-demand account is created at 2009/6/30 09:30 and must be activated before 2009/7/1 09:30, its quota is 24 hours, and there is no expiration time unless its quota is used up. Thus its first login must be done before 2009/7/1 09:30, the account becomes usable once activation when first login, for example, at 2009/7/01 08:00 and will not be expired unless its quota is used up.
  - **Account Activation** is the time that the account will be activated for use. It is set to account creation time of this type.
  - **Relative Expiration Time** is the total usage time (xx *hrs* yy *mins*), during which On-demand users are allowed to access the network. The usage time will be cut down while using only. The account will be expired while usage time is run out.
  - **Price** is the unit price of this plan.



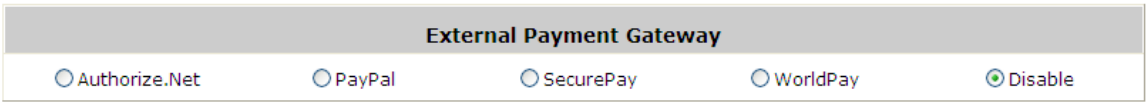
- **Duration-time with Absolute Expiration Time:** The scenario of this type is that a client goes to an exhibition and purchases an on-demand account. The exhibition is from 09:00 02/Jun/2009 ~ 18:00 07/Jun/2009. This account will be activated since 09:00 02/Jun/2009 and ok to use during the exhibition period, and will be expired after a configured time such as 18:00 07/Jun/2009.
  - **Account Activation** is the time that the account will be activated for use.
  - **Expiration Time** is the time that the account will become expired and not able to use any more.
  - **Price** is the unit price of this 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 service to end customers who wish to pay for the service on-line.

The options are **Authorize.Net**, **PayPal**, **SecurePay**, **WorldPay** or **Disable**.



5) On-demand Account Creation

After at least one 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 enabled plan to create an on-demand account. The username and password of to be created 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 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. Moreover, you can click ***Send to POS*** to print a receipt to a POS device.

Note:

If no Billing plan is enabled, accounts cannot be created by clicking ***Create*** button. Please goes back to Billing Plans to active 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.

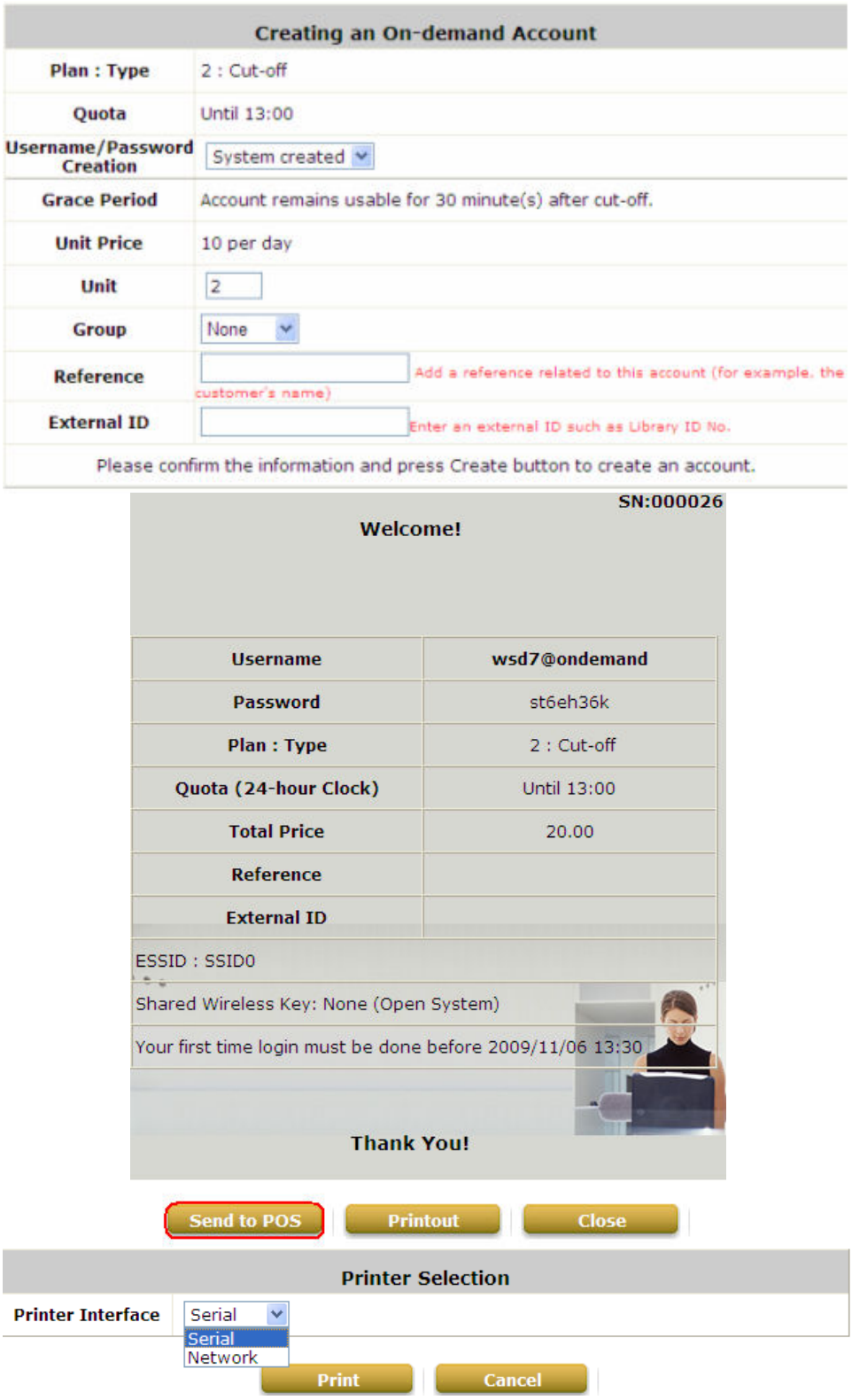
On-demand Account Creation

Plan	Type	Quota	Price	Status	Function
1	Usage-time	2 hr(s)	20	Enabled	Create
2	Cut-off	Until 13:00	20	Enabled	Create
3	Volume	1000 Mbyte(s)	40	Enabled	Create
4	Duration-time	From 2009/11/01 00:05:00 till 2009/11/05 13:05:00	100	Enabled	Create
5	Duration-time	5 day(s) 2 hour(s)	40	Enabled	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.
- **Type:** Show one type of the plan in Usage-time, Duration-time or Cut-off.
- **Quota:** The total time amount or period on how On-demand users are allowed to access the network.
- **Price:** The unit price of each plan.
- **Status:** Show the status in enabled or disabled.
- **Function:** Press ***Create*** button for the desired plan; the Creating an On-demand Account will appear for creation.

On-demand Account Creation

Plan	Type	Quota	Price	Status	Function
1	Usage-time	2 hr(s)	20	Enabled	Create
2	Cut-off	Until 13:00	20	Enabled	Create
3	Volume	1000 Mbyte(s)	40	Enabled	Create
4	Duration-time	From 2009/11/01 00:05:00 till 2009/11/05 13:05:00	100	Enabled	Create
5	Duration-time	5 day(s) 2 hour(s)	40	Enabled	Create


Creating an On-demand Account
Plan : Type
2 : Cut-off
Quota
Until 13:00
Username/Password Creation
System created
Grace Period
Account remains usable for 30 minute(s) after cut-off.
Unit Price
10 per day
Unit
2
Group
None
Reference
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.
SN:000026
Welcome!
Username
wsd7@ondemand
Password
st6eh36k
Plan : Type
2 : Cut-off
Quota (24-hour Clock)
Until 13:00
Total Price
20.00
Reference
External ID
ESSID : SSID0
Shared Wireless Key: None (Open System)
Your first time login must be done before 2009/11/06 13:30
Thank You!
Send to POS
Printout
Close
Printer Selection
Printer Interface
Serial
Serial
Network
Print
Cancel

6) On-demand Account Batch Creation

After at least one plan is enabled, the administrator can generate multiple on-demand user accounts once by batch creation. Click this 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 not to 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 notice that it takes time if you create lots of on-demand accounts by batch creation.

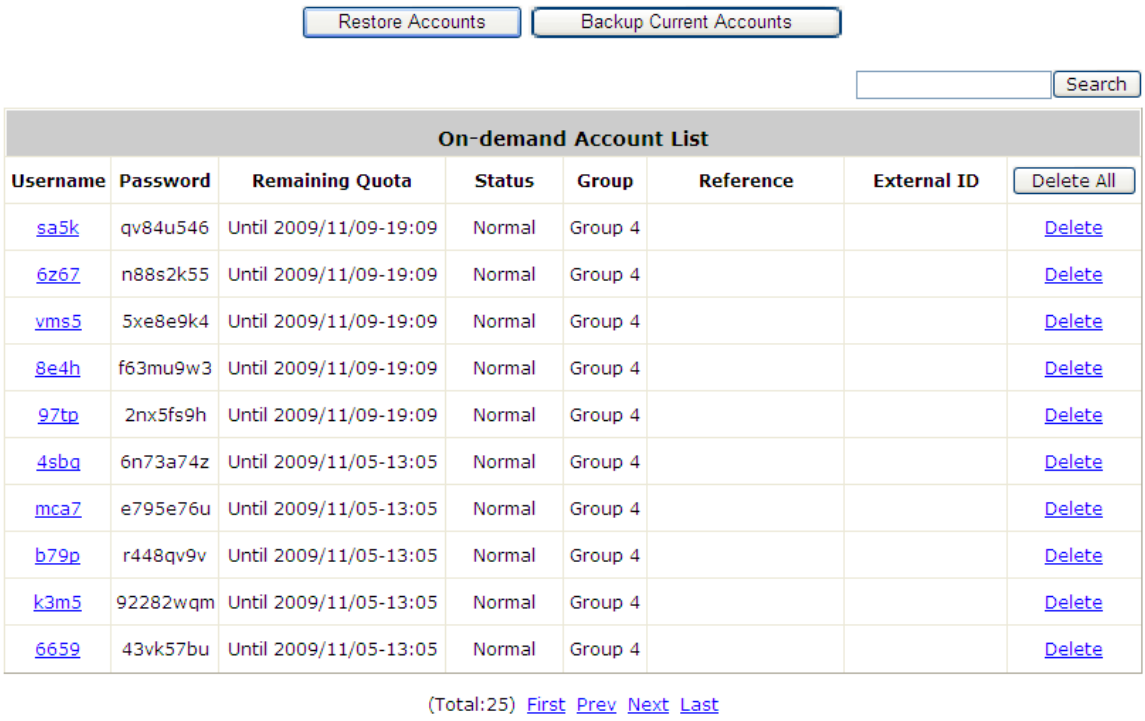
On-demand Account Batch Creation

Plan	Type	Quota	Price	Number of Accounts
1	Usage-time	2 hr(s)	20	5
2	Cut-off	Until 13:00	20	5
3	Volume	1000 Mbyte(s)	40	5
4	Duration-time	From 2009/11/01 00:05:00 till 2009/11/05 13:05:00	100	5
5	Duration-time	5 day(s) 2 hour(s)	40	5
6	N/A			
7	N/A			
8	N/A			
9	N/A			
0	N/A			

- **Plan:** The number of a specific plan.
- **Type:** Show one type of the plan in Usage-time, Duration-time or Cut-off.
- **Quota:** The total time amount or period on how On-demand users are allowed to access the network.
- **Price:** The unit price of each plan.
- **Number of Accounts:** The desired numbers to be created of the plan.

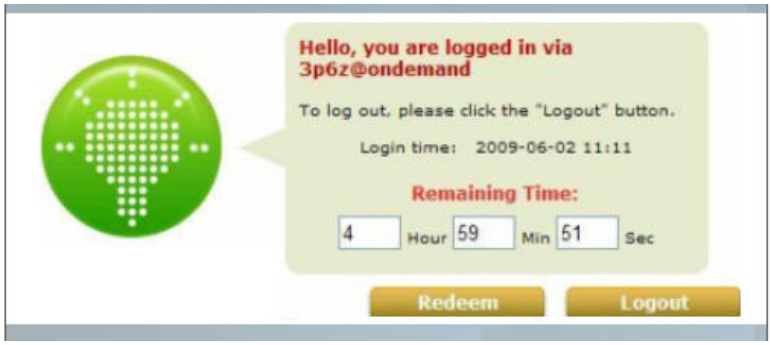
7) On-demand Account List

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



- **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 also does not exceed the quota limit.
    - **Online:** the account is currently in use.
    - **Expired:** the account is not valid any more, even there is remaining quota to be used.
    - **Out of Quota:** the account has exceeded the quota limit.
    - **Redeemed:** the account has been applied for account renewal.
- **External ID:** This is an additional information field for combined with a unique account only.
- **Delete All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

- **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, Redeem function must redeem to same billing type account only.

Note:

The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeem. If the redeem amount exceeds this number, the system will automatically reject the redeem process.

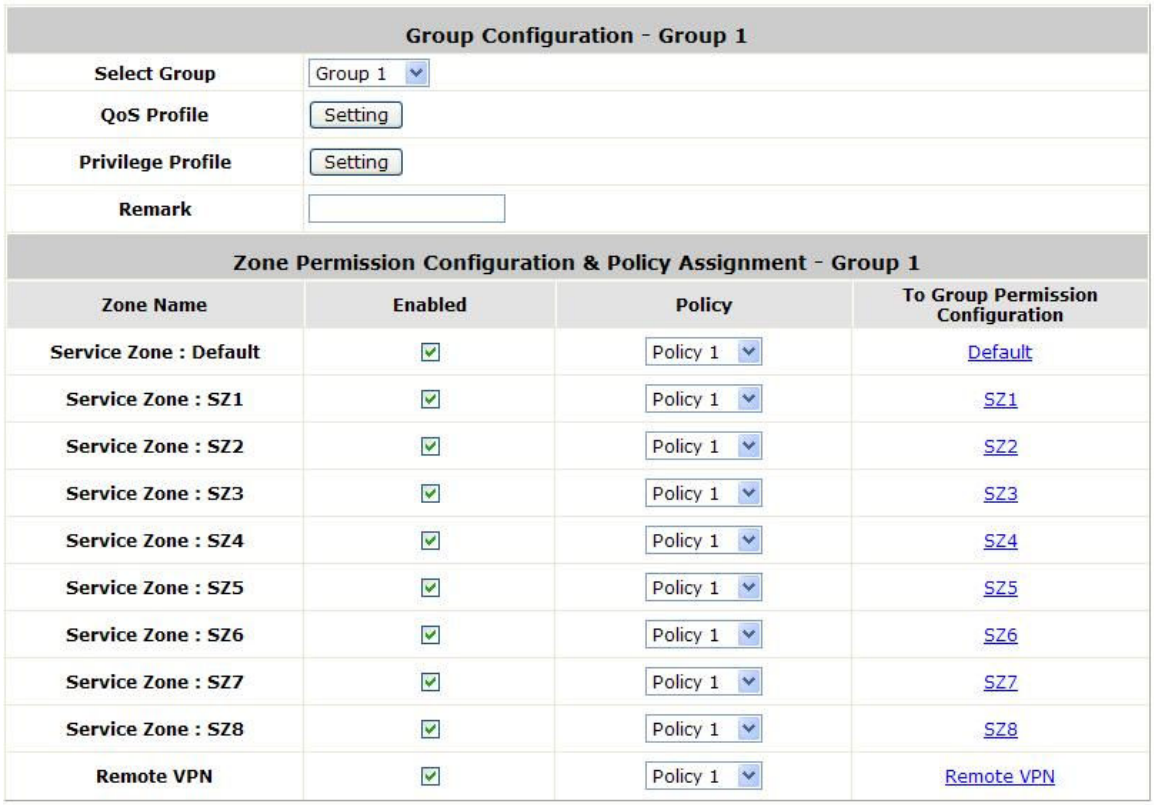
Note:

Duration-time and Cut-off type are support redeem function.

4.2 Users Group

Configure Users Group, go to: ***Users >> Group***.

There are multiple groups for divide users. A Group which can be allowed to access a Service Zone or not; and it also can be applied with a Policy within a Service Zone. The same Group within different Service Zones can be applied with different Policies as well as different Authentication Options.



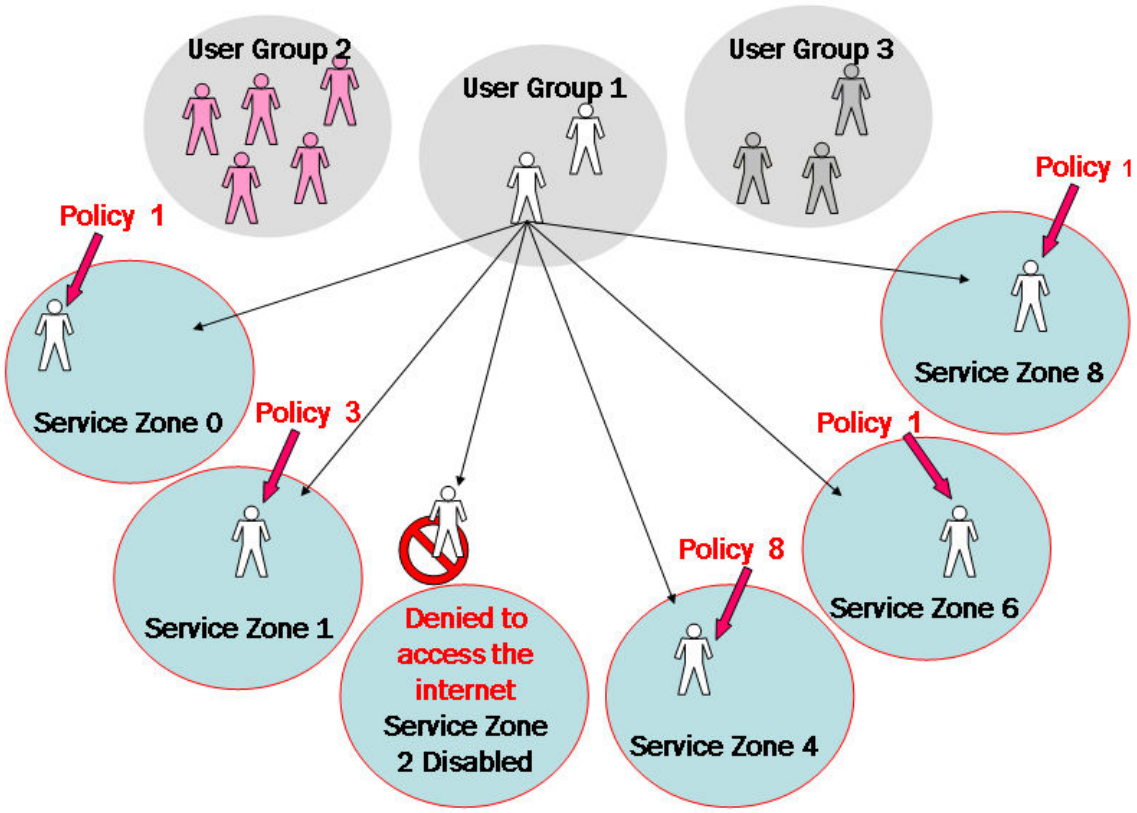
Group Configuration - Group 1			
Select Group	Group 1		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Zone Name	**Enabled**	**Policy**	**To Group Permission Configuration**
Service Zone : Default	☑	Policy 1	Default
Service Zone : SZ1	☑	Policy 1	SZ1
Service Zone : SZ2	☑	Policy 1	SZ2
Service Zone : SZ3	☑	Policy 1	SZ3
Service Zone : SZ4	☑	Policy 1	SZ4
Service Zone : SZ5	☑	Policy 1	SZ5
Service Zone : SZ6	☑	Policy 1	SZ6
Service Zone : SZ7	☑	Policy 1	SZ7
Service Zone : SZ8	☑	Policy 1	SZ8
Remote VPN	☑	Policy 1	Remote VPN

4.2.1 Assign users to a Group

Configure users to a Group, go to: ***Users >> Authentication***.

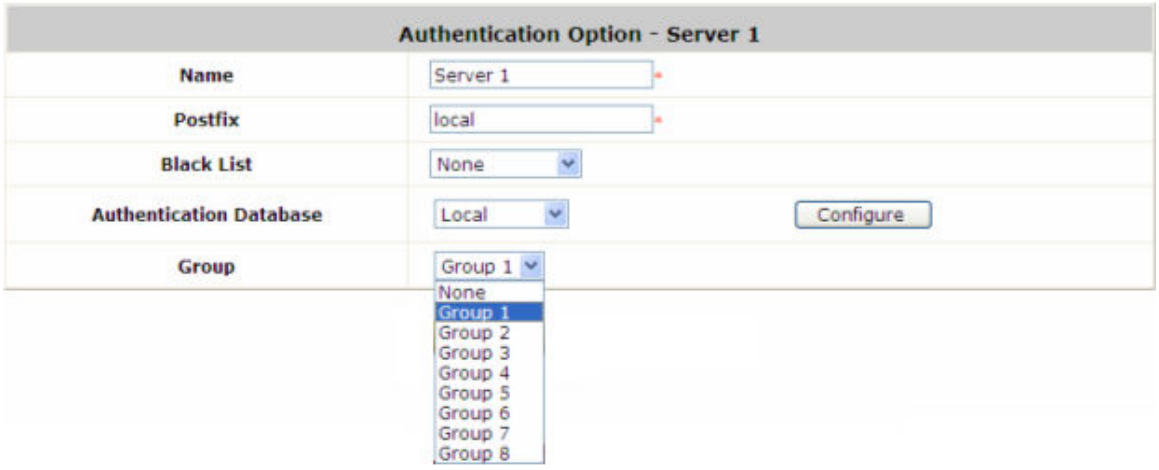
This section shows how to group users, how to rule each grouped user with different policy as he moves to different service zone. The following examples will help you better understand this section.

Group Configuration - Group 1			
Select Group	Group 1		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Zone Name	**Enabled**	**Policy**	**To Group Permission Configuration**
Service Zone : Default	☑	Policy 1	Default
Service Zone : SZ1	☑	Policy 3	SZ1
Service Zone : SZ2	☑	Policy 1	SZ2
Service Zone : SZ3	☑	Policy 1	SZ3
Service Zone : SZ4	☑	Policy 8	SZ4
Service Zone : SZ5	☑	Policy 1	SZ5
Service Zone : SZ6	☑	Policy 1	SZ6
Service Zone : SZ7	☑	Policy 1	SZ7
Service Zone : SZ8	☑	Policy 1	SZ8
Remote VPN	☑	Policy 1	Remote VPN



In this example, Group 1 users are allowed to access the internet in 5 places; Service Zone 0,1,4,6, and 8. They must follow policy 1 at Service Zone 1, 6 and 8. They are ruled by Policy 3 at Service Zone 1 and by Policy 8 at Service Zone 4.

In each authentication option, you can assign a Group with each authentication option. All users login with same authentication server will belong to same Group.



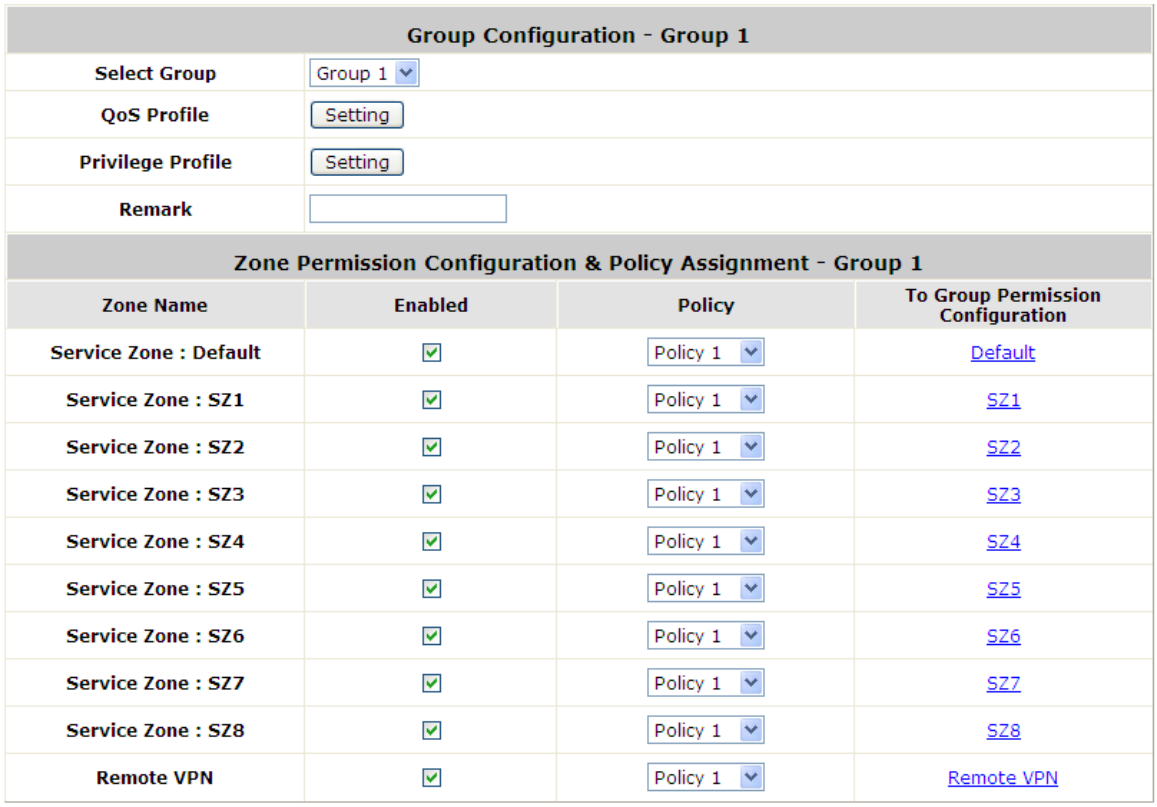
But there are some exceptions:

- In Local Authentication, each user can assign to different Group one by one.
- In RADIUS Authentication, the users can assign to different Group by Class-Group Mapping.
- In LDAP Authentication, the users can assign to different Group by Attribute-Group Mapping.

4.2.2 Permission in Service Zone

Configure Permission in Service Zone, go to: ***Users >> Group***.

A Group can be allowed to access one Service Zone or multiple Service Zones. Moreover, a Group can be applied different Policies within different Service Zones. Remote VPN is considered as a zone, where clients log into the system via remote VPN.



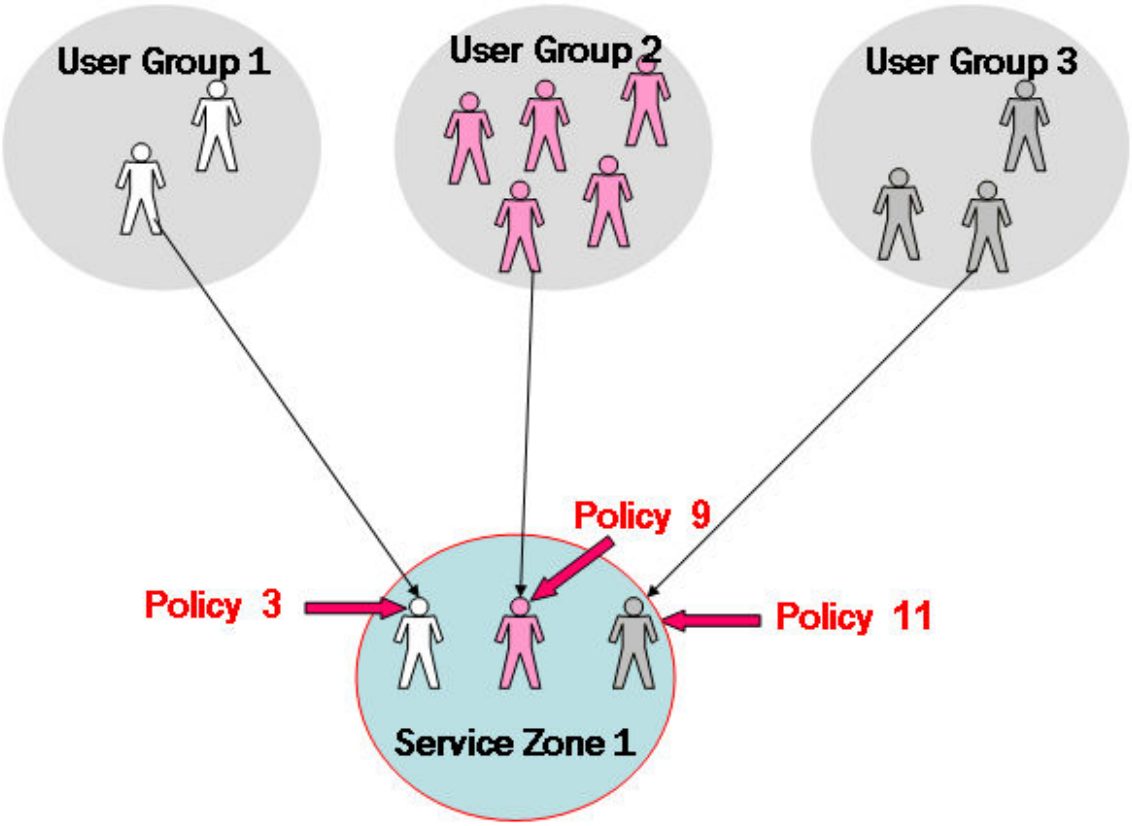
Group Configuration - Group 1			
Select Group	Group 1		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Zone Name	**Enabled**	**Policy**	**To Group Permission Configuration**
Service Zone : Default	☑	Policy 1	Default
Service Zone : SZ1	☑	Policy 1	SZ1
Service Zone : SZ2	☑	Policy 1	SZ2
Service Zone : SZ3	☑	Policy 1	SZ3
Service Zone : SZ4	☑	Policy 1	SZ4
Service Zone : SZ5	☑	Policy 1	SZ5
Service Zone : SZ6	☑	Policy 1	SZ6
Service Zone : SZ7	☑	Policy 1	SZ7
Service Zone : SZ8	☑	Policy 1	SZ8
Remote VPN	☑	Policy 1	Remote VPN

- **Zone Name:** The name of Service Zones and Remote VPN.
- **Enabled:** Select *Enabled* to allow clients of this Group to log into the selected Service Zones. For example, the above figure shows that users in Group 1 can access network services via every Service Zone as well as Remote VPN under constraints of Policy 1.
- **Policy:** Select a *Policy* that the Group will be applied with when accessing respective Service Zones.
- **To Group Permission Configuration:** The relation between Group and Service Zone is many to many; every Group can access network services via more than one Service Zone, and meanwhile, each Service Zone can serve more than one Group.

Click the hyperlink in the **To Group Permission Configuration** column to enter the **Group Configuration** interface, which is based on the role of Service Zone, to configure the relation between Group and Service Zone.

Group Permission Configuration & Policy Assignment - Service Zone : SZ1			
Group Option	**Enabled**	**Policy**	**To Zone Permission Configuration**
Group 1	☑	Policy 3	Group 1
Group 2	☑	Policy 9	Group 2
Group 3	☑	Policy 11	Group 3
Group 4	☑	Policy 4	Group 4
Group 5	☑	Policy 5	Group 5
Group 6	☑	Policy 6	Group 6
Group 7	☑	Policy 7	Group 7
Group 8	☑	Policy 8	Group 8

- **Group Option:** The name of Group options available for selection.
- **Enabled:** Select *Enabled* to allow clients of the enabled Groups to log in to this Service Zone under constraints of the selected Policies.
  Check *Enabled* of each individual Group to assign it to the Service Zone listed. For example, the above figure shows, clients in Group 1~8 can access Service Zone 1, where they are governed by the individual Policy respectively.
- **Policy:** Select a *Policy* that the Group will be applied with when accessing this Service Zone.
- **To Zone Permission Configuration:** Click the hyperlink in the **To Zone Permission Configuration** column to enter **Zone Permission Configuration & Policy Assignment** interface, which is based on the role of Group, to configure the relation between Group and Zone.



At Service Zone 1, Group 1 user is ruled by Policy 3. Group 2 is by Policy 9 and Group 3 is by Policy 11. Other Groups are not enabled to access Service Zone 1.

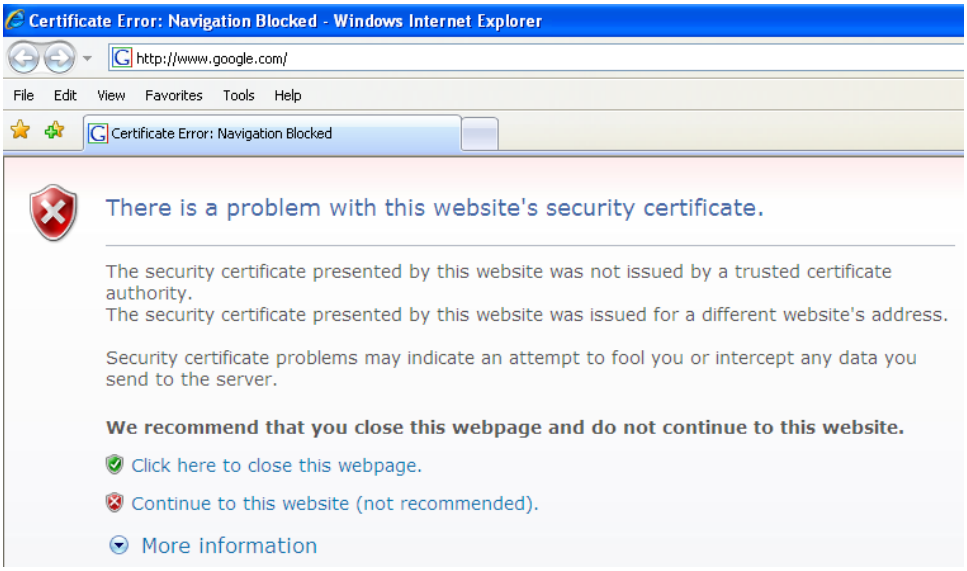
4.3 User Login

▪ An Example of User Login

Normally, users will be authenticated before they get network access through AMG-2102. This section presents the basic authentication flow for end users. Please make sure that the AMG-2102 is configured properly and network related settings are done.

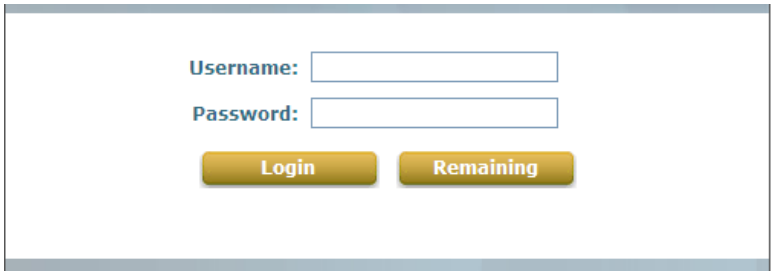
1. Open an Internet browser and try to connect to any website (in this example, we try to connect to www.google.com).

   a) For the first time, if the AMG-2102 is not using a trusted SSL certificate (for more information, please see *4.2.5 Additional Configuration*), there will be a "Certificate Error", because the browser treats AMG-2102 as an illegal website.



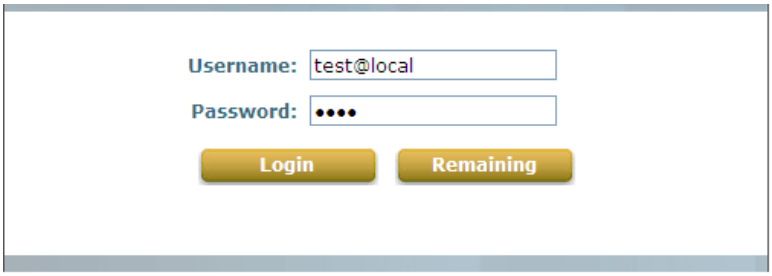
   b) Please press "Continue to this website" to continue.

   c) The default user login page will appear in the browser.

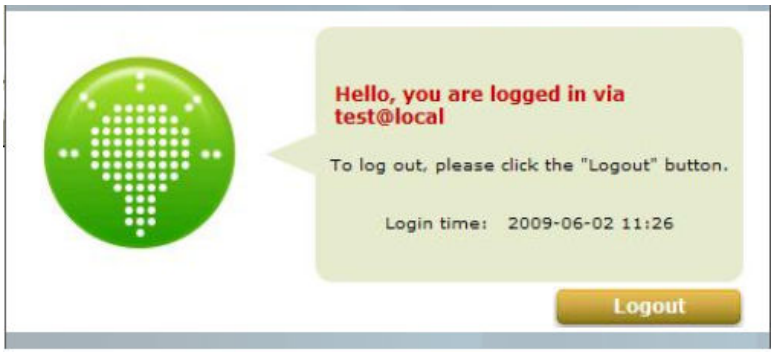


2. Enter the username and password (for example, we use a local user account: **test@local** here) and then click ***Submit*** button. If the ***Remember Me*** check box is checked, the browser will remember this user's name and password so that he/she can just click Submit next time he/she wants to login.

   Check the ***Remember Me*** box to store the username and password on the current computer in order to automatically login to the system at next login. Then, click the ***Submit*** button.
   The ***Remaining*** button on the **User Login Page** is for on-demand users only, where they can check their Remaining quota.

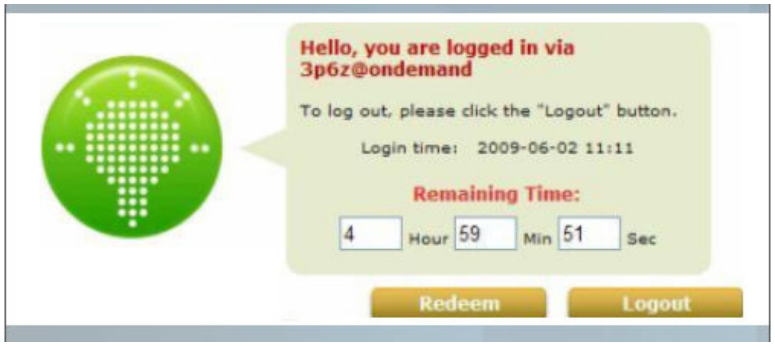


3. Successful! The **Login Successful** page appearing means you are connected to the network and Internet now!



Note:

When On-demand accounts are used, the system will display more information, as shown below.



4.3.1 Default Authentication

In each Service Zone, there are different types of authentication database (LOCAL, POP3, RADIUS, LDAP, NTDOMAIN, ONDEMAND, and SIP) that are supported by the entire system. There are up to six authentication options can be enabled, and one of them can be set as the **Default Authentication**– so that users do not have to type in the postfix string while entering username during login.

A postfix is used to inform the system which authentication option to be used for authenticating an account (e.g. bob@BostonLdap or tim@TaipeiRadius) when multiple options are concurrently in use. One of authentication option can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "BostonLdap" is the postfix of the default option, Bob can login as "bob" without having to type in "bob@BostonLdap".

4.3.2 Login with postfix

Set a postfix that is easy to distinguish (e.g. Local) user login with which authentication server. The acceptable characters are numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

Beside the Default Authentication, all other authentication server users login to system, the username must contain the postfix to identify the user is belong to which authentication server.

4.3.3 Disable Authentication in Service Zone

Configure Authentication in Service Zone, go to: ***System >> Service Zones***.

Authentication Settings					
Authentication Required For the Zone	◉ Enabled ○ Disabled				
Authentication Options	**Auth Option**	**Auth Database**	**Postfix**	**Default**	**Enabled**
	Server 1	LOCAL	local	◉	☑
	Server 2	POP3	pop3	○	☑
	Server 3	RADIUS	radius	○	☑
	Server 4	LDAP	ldap	○	☑
	On-demand User	ONDEMAND	ondemand	○	☑
	SIP	SIP	N/A	○	☐

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

5.Managing Wireless Network

5.1 AMG-2102 with Multiple Type of AP

Beside the LAN ports in AMG-2102, you can connect AP to AMG-2102 to extent the network access by wireless. AMG-2102 can manage multiple types of AP, such as WAB-3003 (108M 11g Outdoor PoE AP), WAP-3101 (108M 11g PoE Wireless Access Point), WAP-6022 (150M N Wireless Access Point), WAP-6011 (300M N_Max Wireless Access Point). Most settings of AP can be configuring from AMG-2102.

Beside the personal or home usage, most other environment always needs more than one AP to serve a lot of people; such as Hotspot or hotels. But in these areas, only Indoor AP can be satisfied. On the other hand, many complicated environments combine indoor and outdoor area. For industrial usage, it always combines office building and open-air factory; for campus usage, it must combines classrooms, lab, office and many open-air playgrounds. So it must need to use Indoor AP and Outdoor AP at the same time.

For this reason, the management of multiple type of AP is very important. Let us introduce the management of multiple type of AP.

View AP Overview, go to: ***Access Points >> Overview***.

In the Overview page, all of the supported AP type will list here.

AP Type List				
AP Type	No. of AP	OnLine	OffLine	No. of Client
WAB-3003	0	0	0	0
WAP-3101	0	0	0	0
WAP-6002	0	0	0	0
WAP-6011	0	0	0	0

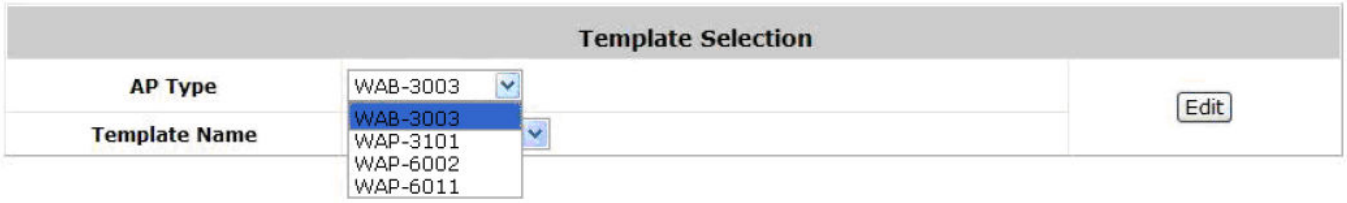
Because AMG-2102 can manage Single-RF access points and Wall-Jack access points, the best and easy way to configure a log of APs is by AP Template. You can configure one template, and then apply this

template to all or a log of APs by a simple way. Or when you are adding (discovery) APs to your network with same configurations, and then you also can apply this template to the discovered APs very easily.

5.2 Configure AP Template

Configure AP Template, go to: ***Access Points >> Templates***.

Template is a model that can be copied to every AP and not necessary to configure the AP individually. There are three templates provided for each type of AP. Select an AP Type, and click ***Edit*** to go on configuration.



Another easy way to configure the template, it is copy the configuration from an existing AP to the template. Select a **Source AP**, and without configuring the template from the beginning, administrators can also revise some settings for demand.

If copy is not desired, please select **NONE**. Input the **Name** and **Remark**, if you want to change these to memorize easily. If not, then click the button of ***Configure*** to go on configuration.

- **Template Editing**: Here is the section that administrators can configure template name, template source, and template remark.
  - **Name**: The name shown for this particular template will change according to what given by administrators.
  - **Copy Settings From**: Select an existing AP and click **Apply** to save its settings as the template settings.
  - **Remark:** The remark of this template profile.

- **Template Configuration**

  The administrator can set the template configuration manually. Click ***Configure*** button to have detailed configurations.

General - CPE100: TEMPLATE1	
Subnet Mask	255.255.254.0 *
Default Gateway	192.168.1.254 *
NTP	Time Zone (GMT+08:00)Taipei,Taiwan NTP Server 1: tick.stdtime.gov.tw * NTP Server 2: tock.stdtime.gov.tw
SNMP	Enabled Community String: Read: public * Write: private * Trap: Enabled Trap Server IP: 0.0.0.0 *
SYSLOG	Enabled SYSLOG Server IP Address: 0.0.0.0 * SYSLOG Server Port: 514 * Log Level: Emergency

  - **General Setting:** In this section, revise the **Subnet Mask** and **Default Gateway** here if desired. Configure the **NTP Servers** and **Time Zone**. Besides, it can enable **SYSLOG** server to receive the log from AP and enable **SNMP** read/write ability.

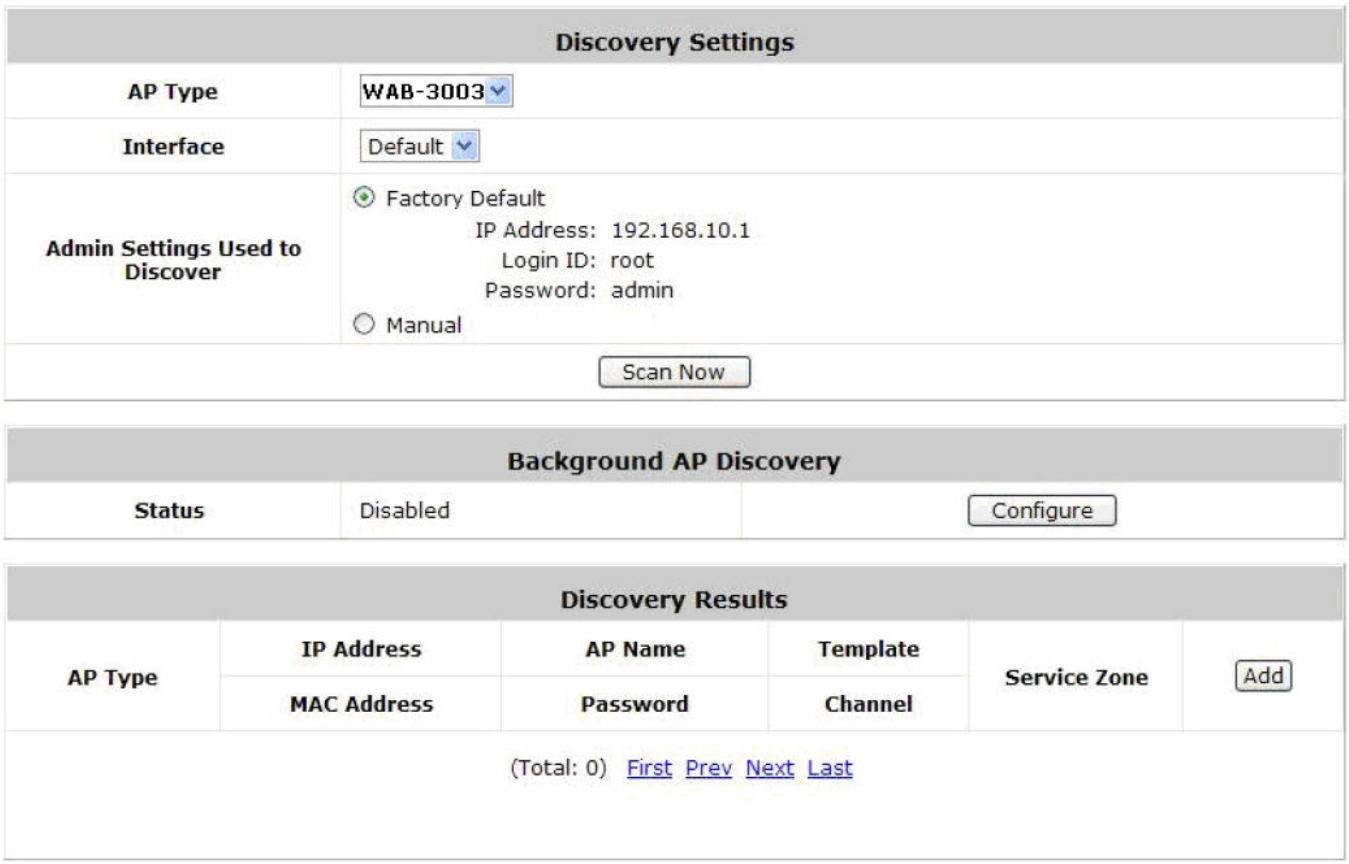
Wireless - CPE100: TEMPLATE1	
SSID Broadcast	Enabled
Band	802.11b+802.11g
Data Rate	Auto
Preamble	Long Only
IAPP	Disabled
Wireless Client Isolation	Disabled
Transmit Power	Highest
Wireless QoS WMM	Enabled
Fragment Threshold	2346 (Default: 2346; Range: 256 ~ 2346)
RTS Threshold	2346 (Default: 2346 ; Range: 1 ~ 2346)
Beacon Interval (ms)	100 (Default: 100; Range: 100 ~ 500)

- **Wireless:**
  - **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from being seen on networked.
  - **Band:** There are 3 modes to select, **802.11b** (2.4G, 1~11Mbps)**, 802.11g** (2.4G, 54Mbps) and **Mix mode** (b and g).
  - **Data 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.
  - **Preamble:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select either Short Preamble or Long Preamble.
  - **IAPP:** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period.
  - **Wireless Client Isolation:** The default value is **Disabled**. When select **"Enabled"**, all the wireless clients will be isolated each other.
  - **Transmit Power:** The default is **Auto**. Select from the range or keep the default setting, **Auto**, to make the Access Point use different transmit power as you wish.
  - **Wireless QoS WMM:** Select **Enabled**, the packets with QoS WMM will has higher priority.
  - **Fragment Threshold:** Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.
  - **RTS Threshold:** Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.
  - **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network.

5.3 Discovery AP

Configure Discovery AP, go to: ***Access Points >> Discovery***.

After AP template configuration is finish, use this function to detect and manage all of the APs in the network segments. Note that AMG-2102 can only manage APs that are connected to its LAN ports. Therefore, the AP discovery function is for adding locally connected APs to its management list. The administrator must know the local IP addresses of the APs he/she wishes to discover. Or the better way is reset the AP to default setting for discovery.

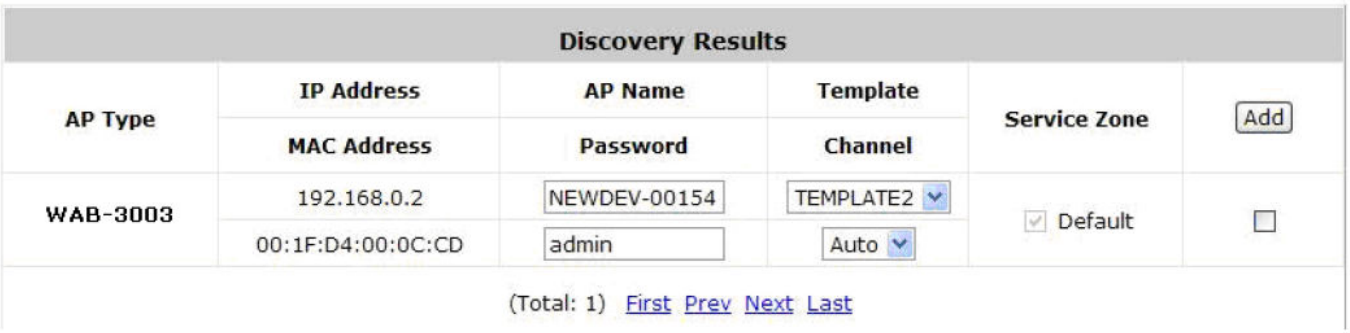


- To discover AP:
  - **AP Type:** Choose the type of AP you wish to discover.
  - **Interface:** Set to default.
  - **Admin Settings Used to Discover:** Choose from **Factory Default** or **Manual**, if the AP is not using the default IP.

Then click the ***Scan Now*** button and the APs match the given settings will show in the list below. If one

of the IP addresses intended is used, a warning message will show up. In this case, please change the IP range and then click ***Scan Now*** again.

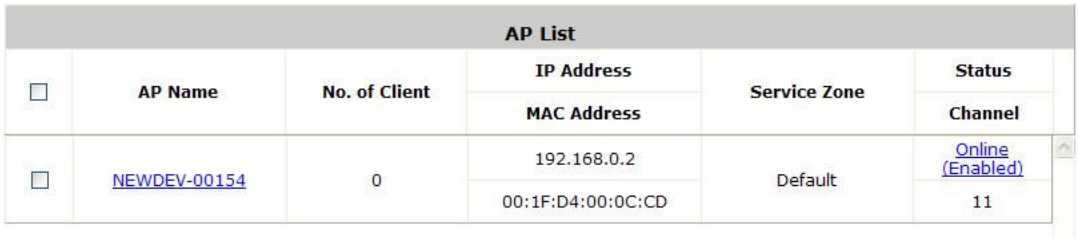
- **Discovery Results:** The discovered new APs will be listed here. When the system's Service Zone is set to Tag-based mode, service zones also can be assigned here. After clicking ***Add***, the current management page is directed to AP List, where the newly added APs will show up with a status of "configuring". It may take a couple of minutes to see the status of the newly added AP to change from "configuring" to "online" or "offline".



- **AP Type**: This is the supported type of APs for centralized management.
- **IP Address:** IP address of the specified AP.
- **MAC Address:** MAC address of the specific AP.
- **AP Name:** Mnemonic name of the specific AP.
- **Admin Password:** Password required for this AP.
- **Template:** The template which will be applied to the added AP.
- **Channel:** The selected channel will be applied to the added AP.
- **Service Zone:** The item is only shown when ***Tag-Based*** mode is selected. Select the name of Service Zone such as Service Zone 1, Guest or Employee.
- **Add:** The administrator can click ***Add*** button to register the APs to the ***List*** for management.

Input the desired name and password for the AP. Select one template, one channel, check the Add checkbox and then click ***Add*** to add it under the managed list.

When the AP is added, it will show up in the list below and be given a new IP address set here (ex: 192.168.0.1). Check the **Add** box to add the AP and it will be listed to the AP list.



AP List					
☐	AP Name	No. of Client	IP Address MAC Address	Service Zone	Status Channel
☐	NEWDEV-00154	0	192.168.0.2 00:1F:D4:00:0C:CD	Default	Online (Enabled) 11

5.4 AP with Service Zone

Configure AP with Service Zone, go to: ***System >> Service Zones***.

- **Service Zone Settings – Assigned IP Address for AP Management**

Assigned IP Address for AP Management	
IP Range	Start IP Address : 192.168.0.1 * End IP Address : 192.168.0.190 *

Under port-based service zone, each service zone can designate an IP segment for IP address assignment to the managed AP when the newly discovered AP is added into the service zone. Under tag-based service zone, only default service zone will designate an IP segment for IP address assignment to the managed AP when the newly discovered AP is added into the selected service zones.

- **Service Zone Settings – Managed AP in this Service Zone**

  All managed APs that belong to this service zone are listed here for reference.

Managed AP(s) in this Service Zone			
AP Type	AP Name	IP Address MAC Address	Status
WAB-3003	NEWDEV-00154	192.168.0.2 00:1F:D4:00:0C:CD	Online (Enabled)

- **Service Zone Settings – SSID for Service Zone**

  All managed APs that belong to this service zone have same SSID.

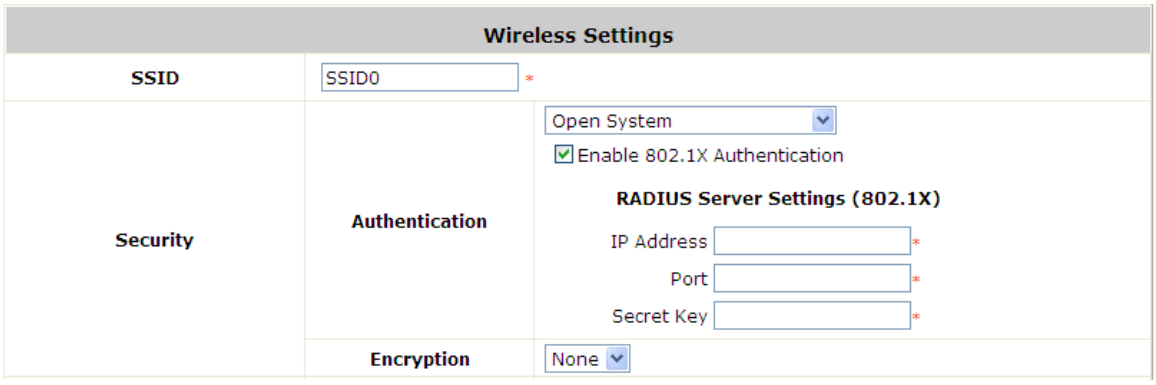
- **Service Zone Settings – Access Control for Service Zone**

  All managed APs (VAP) that belong to this service zone have same ACL table. When the status is **Allowed**, only these clients whose MAC addresses are listed in this list can be allowed to connect to the AP; on the other hand, when the status is **Denied**, the clients whose MAC addresses are listed in the list will be denied to connect to the AP. When **Disabled** is selected, any clients can connect to the AP. The default is **Disabled**.

  - **User Limit:** Limit the number of users connected to that AP. *Not all AP types support this option.*

5.5 AP Security

Configure AP Security, go to: ***System >> Service Zones***.

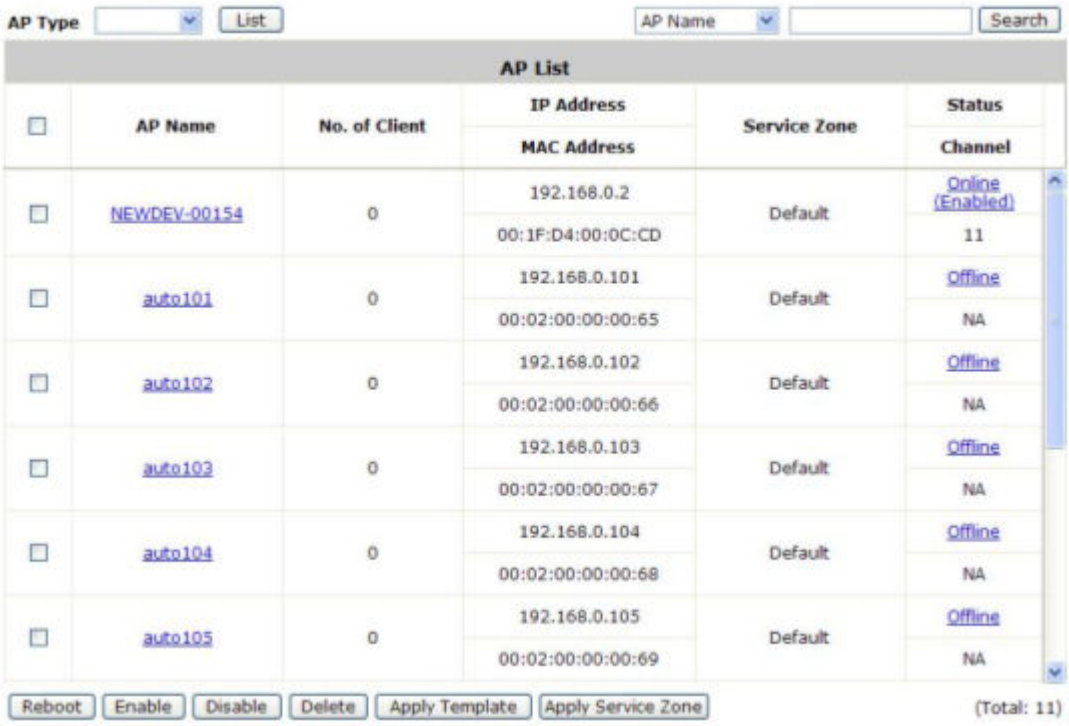


- **Security:** For each service zone, administrators can set up the wireless security profile, including **Authentication** and **Encryption**.
- **Authentication:** Including **Open System**, **Share Key**, **WPA**, **WPA2** or **WPA/WPA2 Mixed**.
- **Encryption:**
  - **WEP:** When **Authentication** is **Open System** or **Share Key**, **WEP** will be enabled.
  - **WPA:** When **Authentication** is **WPA**, **WPA-PSK** or **WPA-RADIUS** will be the options of **WPA**. For **WPA-PSK**, it also can select **Passphrase** or **HEX**.
  - **WPA2:** When **Authentication** is **WPA**, **WPA-PSK** or **WPA-RADIUS** will be the options of **WPA**. For **WPA-PSK**, it also can select **Passphrase** or **HEX**.
  - **WPA/WPA2 Mixed:** When **Authentication** is **WPA**, **WPA-PSK** or **WPA-RADIUS** will be the options of **WPA**. For **WPA-PSK**, it also can select **Passphrase** or **HEX**.

5.6 Change managed AP settings

Configure AP settings in AP List, go to: ***Access Points >> List***.

All of the APs under the management of AMG-2102 will be shown in the list. The AP can be edited by clicking the hyperlink of ***AP Name*** and the AP status can be got by clicking the hyperlink of ***Status***.



- **AP Name**

  Click ***AP Name*** and enter the interface about related settings. There are four kinds of settings, **General Settings**, **LAN Interface Setting** and **Wireless Interface Setting**. Click the hyperlink to go on the configuration.

General Settings		
General	AP Name	NEWDEV-00154
	Firmware	1.70.00

LAN Interface Settings		
LAN	IP Address	192.168.0.2
	Gateway	192.168.1.254

Wireless Interface Settings		
Wireless LAN	Channel	Auto
	Data Rate	Auto

- **General Setting:** Click the link to enter the **General Setting** interface. Firmware information also can be observed here.

General Settings	
Name	NEWDEV-00154 *
Admin Password	•••••
NTP	Time Zone: (GMT+08:00)Taipei,Taiwan NTP Server 1: tick.stdtime.gov.tw * NTP Server 2: tock.stdtime.gov.tw
SNMP	Disabled
SYSLOG	Disabled
Remark	
Firmware	1.70.00

- **LAN Setting:** Click the link to enter the **LAN Setting** interface. Input the data of LAN including **IP address**, **Subnet Mask** and **Default Gateway** of AP.

LAN	
IP Address	192.168.0.2 *
Subnet Mask	255.255.254.0 *
Default Gateway	192.168.1.254 *
Primary DNS	192.168.1.254 *
Secondary DNS	

- **Wireless LAN:** Click the link to enter the **Wireless** interface.

Wireless	
SSID Broadcast	Enabled
Channel	Auto
Band	802.11b+802.11g
Data Rate	Auto
Fragment Threshold	2346 (Default: 2346; Range: from 256 to 2346)
RTS Threshold	2346 (Default: 2346; Range: from 1 to 2346)
Beacon Interval (ms)	100 (Default:100 ; Range: from 100 to 500)
Preamble	Long Only
Transmit Power	Highest
Wireless QoS WMM	Enabled
Wireless Client Isolation	Disabled
IAPP	Disabled

- **Status**

After clicking the hyperlink in the **Status** column, there are two areas of information shown: **AP Status Summary** and **AP Status Details**.

AP Status Summary includes **AP Name**, **AP Type**, **LAN Interface MAC address**, **Wireless Interface MAC address**, **Report Time**, **SSID**, and **Number of Associated Clients**. AP Status Details include **System Status**, **LAN Status**, **Wireless LAN Status**, **Associated Client Status** and **Local Log Status.**

AP Status Summary	
AP Name	cpe110-00152
AP Type	
LAN Interface MAC Address	00:1F:7D:91:25:8B
Wireless Interface MAC Address	00:1F:7D:91:25:8C
Report Time	2009-08-06 14:25:01
SSID	SSID0 (Service Zone: Default)
Number of Associated Clients	0

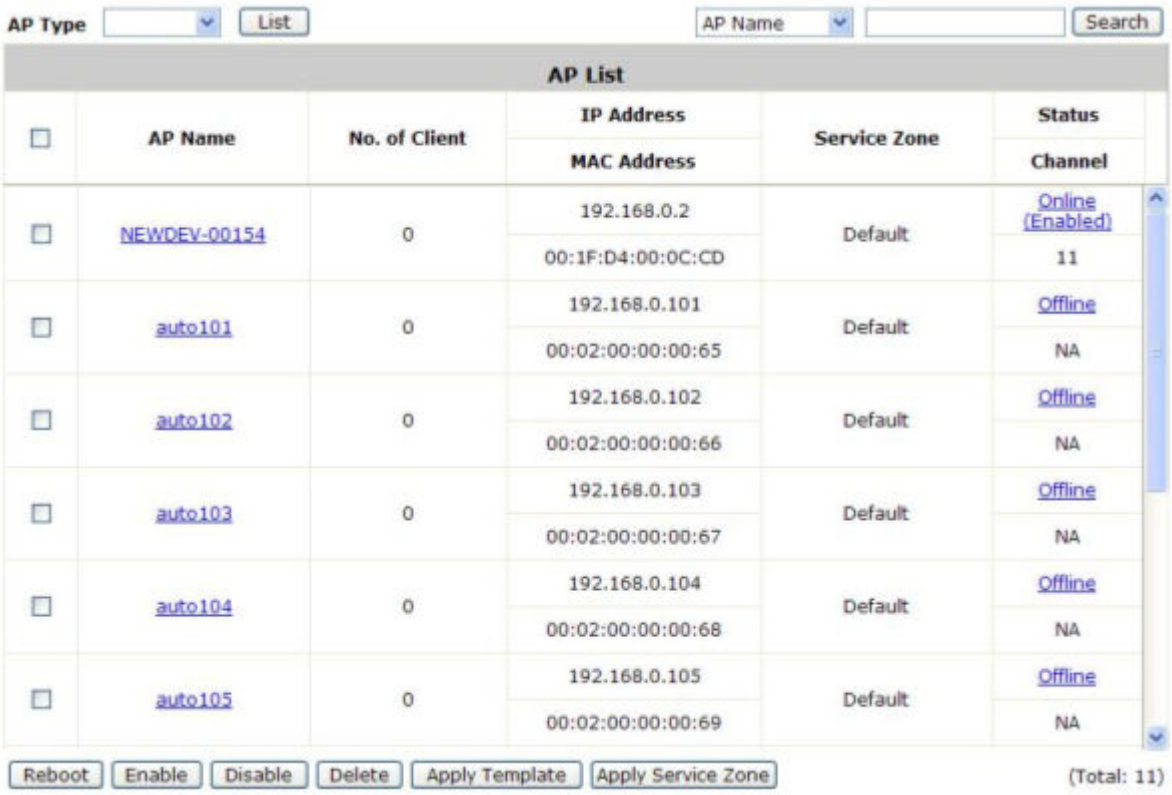
AP Status Details
System
LAN Interface
Wireless Interface
Associated Clients
Local Log Status

5.7 AP Operations from AP List

Configure AP List, go to: ***Access Points >> List***.

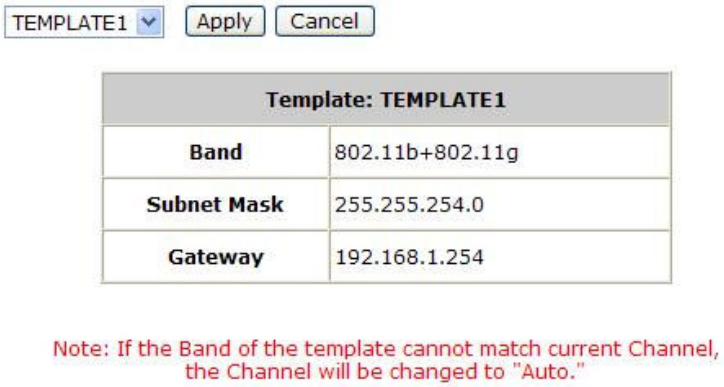
5.7.1 Reboot, Enable, Disable and Delete the AP

Select any AP by the check the checkbox and then click the button below to ***Reboot***, ***Enable***, ***Disable*** and ***Delete*** the selected AP if desired.



5.7.2 Apply Template

Select any AP by check the checkbox and then click ***Apply Template***; select one template to apply to the AP.



5.7.3 Change Service Zone

Select any AP by the check the checkbox and then click ***Apply Service Zone*** to select which Service Zones this AP associates to. For example, if **SZ3** and **SZ5** are selected for this AP, then these two Service Zones will be available under this AP. This AP will have two VAPs with two SSIDs according to two Service Zones for clients to associate. If a user connected to one SSID (for example, SSID3) of this AP and wishing to access the Internet, this user must log into these Service Zones (SZ3) first.

Service Zone				
☐	ID	Name	SSID	WLAN Encryption
☐	0	Default	SSID0	None
☐	3	SZ3	SSID3	None
☐	5	SZ5	SSID5	None

Check the checkbox to select the available Service Zones from the list. Click ***Apply*** to finish the settings.

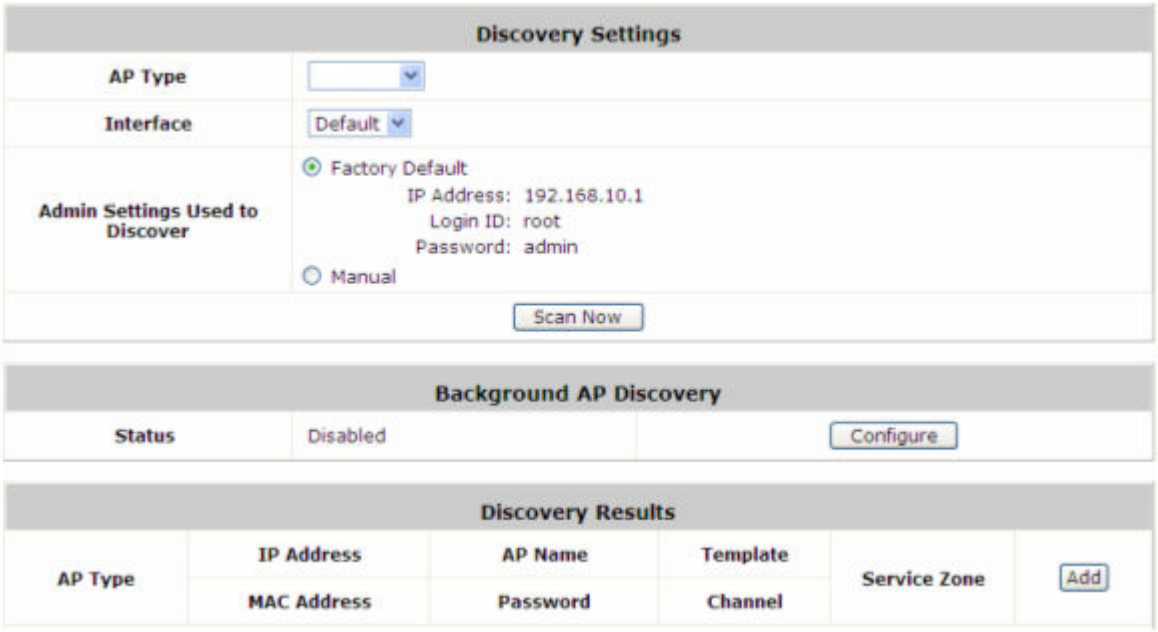
Caution:

1. *This function only support in **Tag-Base** mode.*
2. *Not all AP types support this feature, only Multi-VAP-AP can Apply Service Zone in **Tag-Based** mode.*

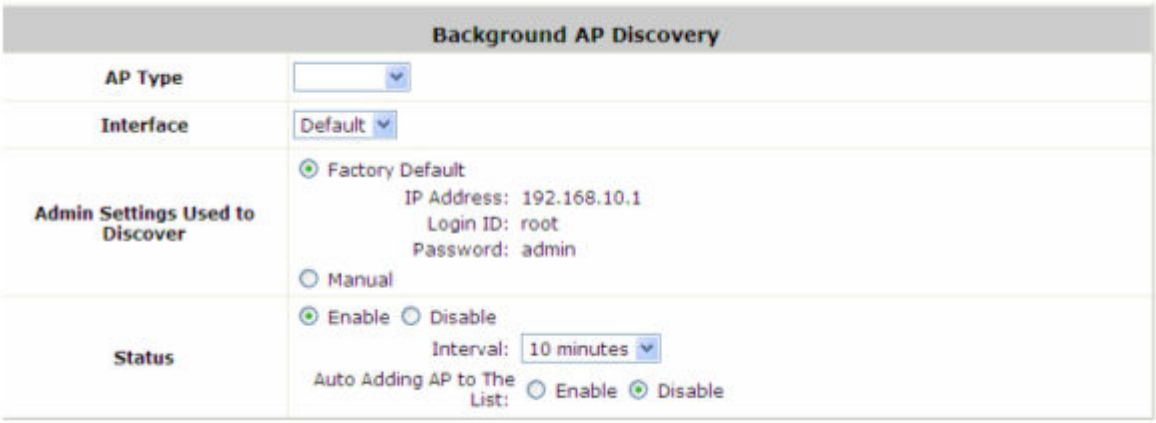
5.7.4 AP Background Discovery

Configure AP Background Discovery, go to: ***AP Management >> Discovery***.

Background AP Discovery: Click **Configure** to enter **Background AP Discovery** interface and go on related configuration.



The configuration is the same as **AP Discovery**. When **Background AP Discovery** function is enabled, the system will scan once every 10 minutes or according to the time set by the administrator. If any AP is discovered and **Auto-Add AP** is enabled, it will be assigned an available IP from the starting IP address and apply the selected template. You can also set the channel of the AP would use.



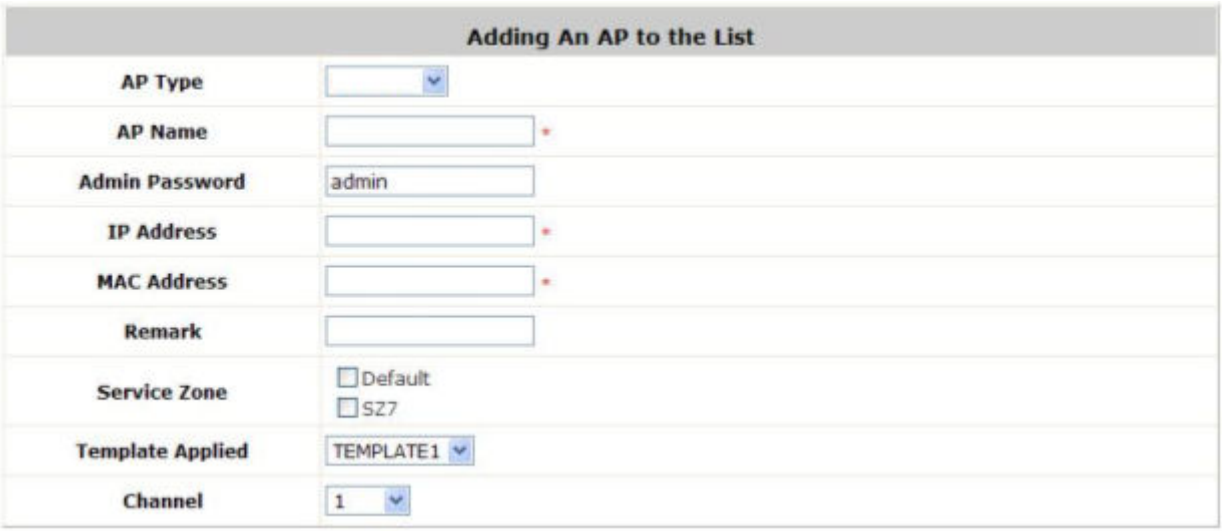
Caution:

The scanning process may take a long time if the IP range assigned to scan is too wide.

5.7.5 Manually add AP

Configure AP Adding manually, go to: ***Access Points >> Adding***.

The AP also can be added manually even though when it is offline. Input the related data of the AP and select a Template. After clicking ***Add***, the AP will be added to the managed list.

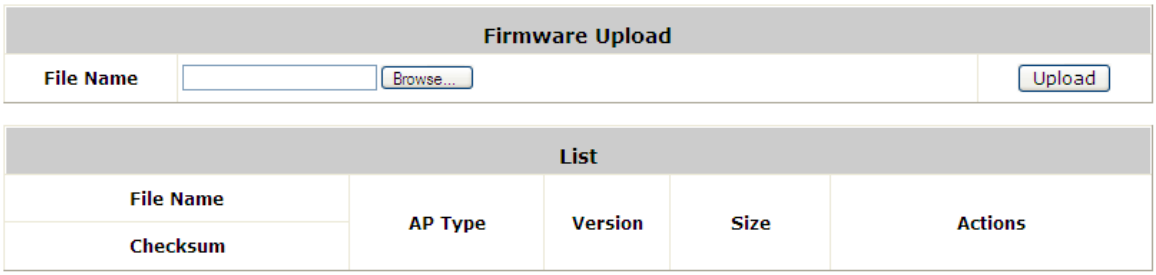


- **AP Type**: This is the supported type of APs for centralized management.
- **AP Name:** Mnemonic name of the specific AP.
- **Admin Password:** Password required for this AP.
- **IP Address:** IP address of the specified AP.
- **MAC Address:** MAC address of the specific AP.
- **Remark:** Some extra information to be filled in for this AP if desired.
- **Service Zone (Tag-Based** only**):** This item is only shown when Tag-Based mode is selected in *System Configuration >> LAN Port Mapping*. Select the name of Service Zone such as Service Zone 1, Guest or Employee. And it is only for Multi-VAP AP only.
- **Template Applied:** The template which will be applied to the added AP.
- **Channel:** The selected channel will be applied to the added AP.

5.7.6 Firmware management and upgrade

Configure Firmware management, go to: ***Access Points >> Firmware***.

Firmware Upload displays the current version of the AP's firmware. New firmware can be uploaded here to update the current firmware. To upload, click **Browse** to select the file and then click **Upload**.



Configure Firmware upgrade, go to: ***Access Points >> Upgrade***.

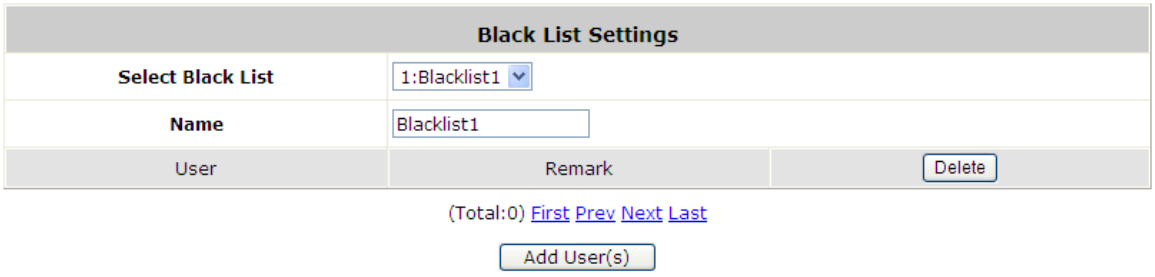
AP Upgrade Select the APs which need to be upgraded and select the upgrade version of firmware, and click **Apply** to upgrade firmware.

6. Policies and Access Control

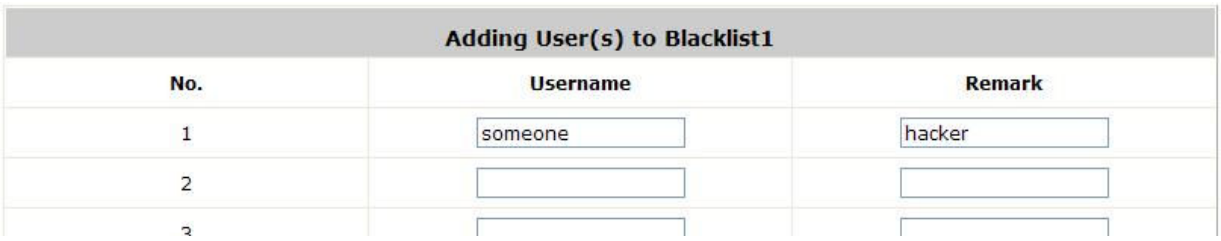
6.1 Black List

Configure Black List, go to: ***Users >> Black List***.

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

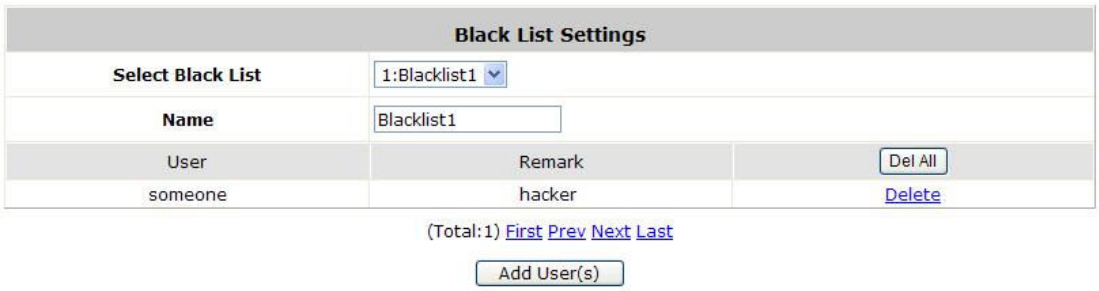


- **Select Black List:** There are multiple lists to select from for the desired black list.
- **Name:** Set the black list name and it will show on the pull-down menu above.
- **Add User(s):** Click the hyperlink to add users to the selected black list.

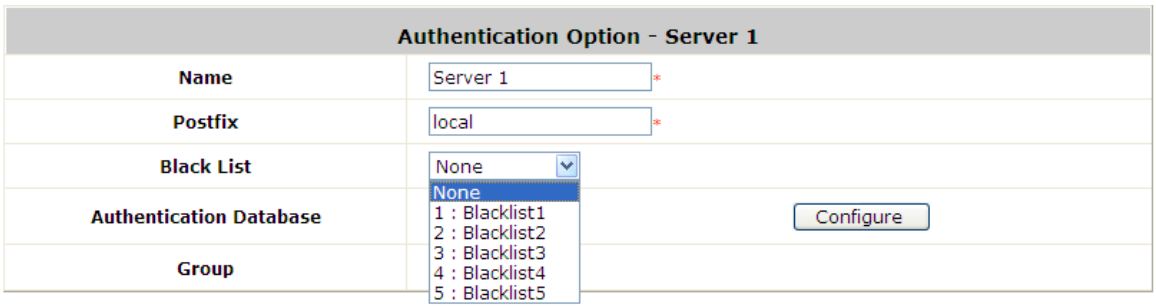


After entering the usernames in the **Username** blanks and the related information in the **Remark** blank (not required), click ***Apply*** to add the users.

If removing a user from the black list is desired, click the user's **Delete** link or click the ***Del All*** button to remove all users from the black list.



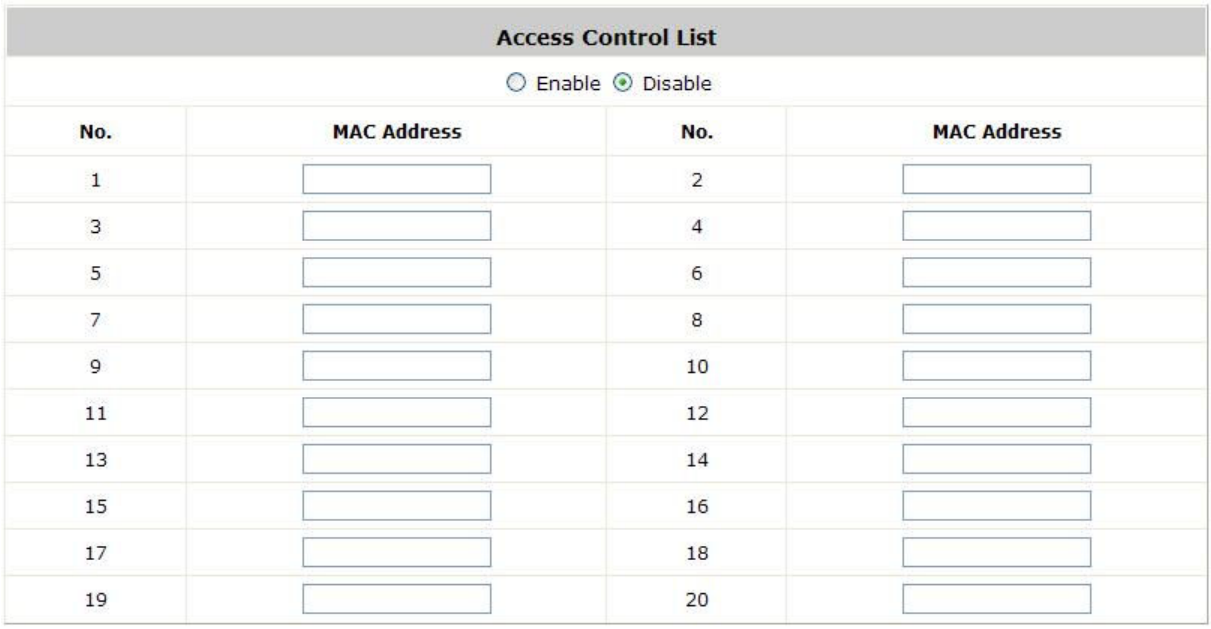
After the Black List is setup completed. You can select the Black List in each Authentication Server to let it to become effective.



6.2 MAC Address Control

Configure MAC Address Control, go to: ***Users >> Additional Control >> MAC ACL***.

MAC ACL: With this function, only the users with their MAC addresses in this list can login to AMG-2102. There are maximum users 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

Configure Policy, go to: ***Users >> Policy***.

AMG-2102 supports multiple Policies, including one **Global Policy** and other individual **Policy**. Each Policy consists of access control profiles that can be configured respectively and applied to a certain Group of users. **Global Policy** is the system's universal policy and applied to all clients, while other individual Policy can be selected and defined to be applied to any Service Zone.

The clients belonging to a Service Zone will be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. The same Group can be applied with different Policies within different Service Zones.

When the type of authentication database is **RADIUS**, the **Class-Group Mapping** function will be available to allow the administrator to assign a Group for a RADIUS class attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a RADIUS class attribute.

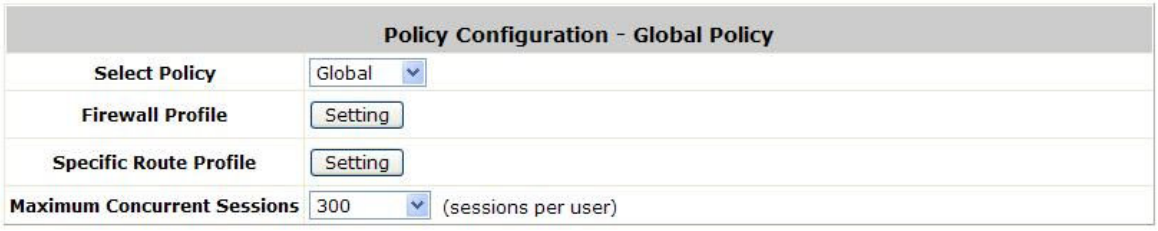
When the type of authentication database is **LDAP**, the **Attribute-Group Mapping** function will be available to allow the administrator to assign a Group for LDAP attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a LDAP attribute.

When the type of database is **Local**, the **Group** selection function will be available to allow the administrator to assign a Group to each user one by one.

When the type of database is **On-demand**, the **Group** selection function will be available in each Billing Plan to allow the administrator to assign a Group to each Billing Plan; also it can assign a Group to each user one by one when the On-demand user is creating.

- **Global Policy**

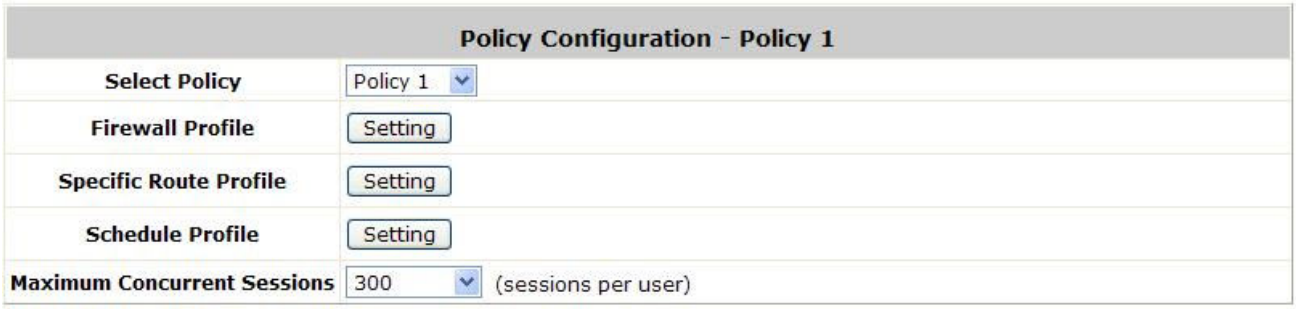
Global is the system's universal policy including **Firewall Rules**, **Specific Routes Profile** and **Maximum Concurrent Session** which will be applied to all users unless the user has been regulated and applied with another Policy.



- **Select Policy:** Select **Global** to set the **Firewall Profile**, **Specific Route Profile** and **Maximum Concurrent Session**.
- **Firewall Profile:** Global policy and each policy have a firewall service list and a set of firewall profile which is composed of firewall rules.
- **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this gateway settings, include default gateway.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

- **Policy**

Beside **Global Policy**, there have **Policy 1** to **Policy X**, each Policy consists of access control profiles that can be configured respectively and applied to a certain Group of users. The clients belonging to a Service Zone will also be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. The same Group can be applied with different Policies within different Service Zones.



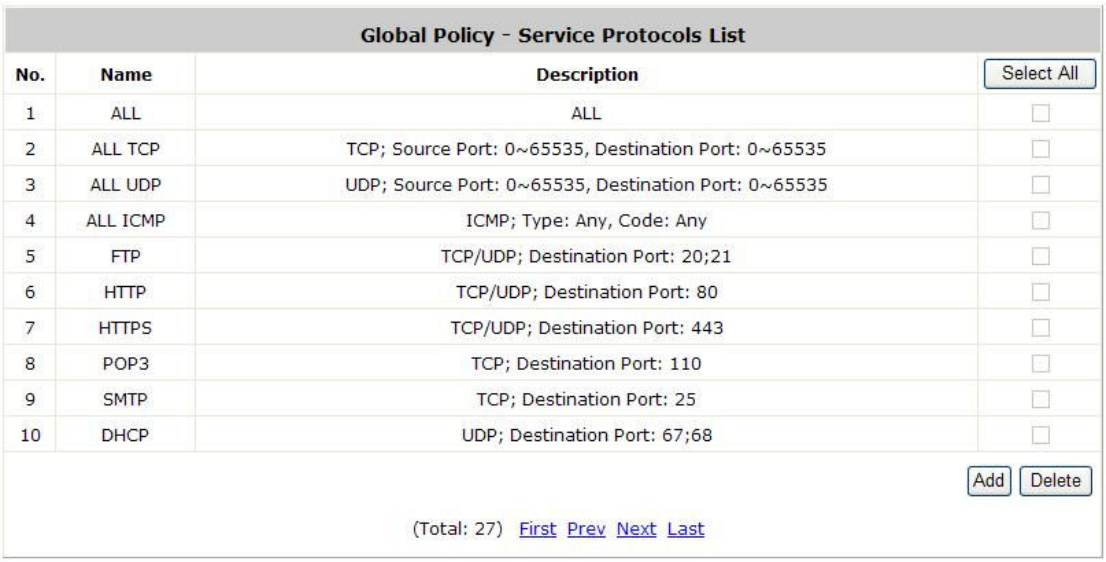
- **Select Policy:** Select **Policy 1~Policy X** to set the **Firewall Profile**, **Specific Route Profile, Schedule Profile** and **Maximum Concurrent Sessions**.
- **Firewall Profile:** Each Policy has a firewall service list and a set of firewall profile consisting of firewall rules.
- **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this gateway settings, include default gateway.
- **Schedule Profile:** The Schedule table in a 7X24 format is used to control the clients' login time. When Schedule is enabled, clients applied policies are only allowed to login the system at the time which is checked in the applied policy.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

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.

1. Predefined Protocols

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



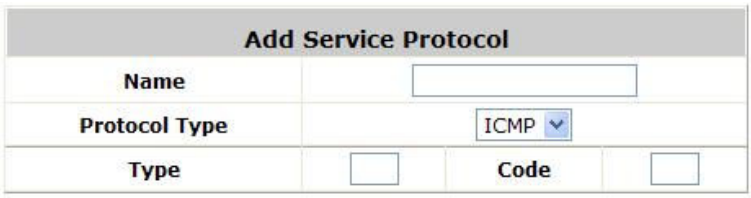
The administrator is able to add new custom service protocols by clicking ***Add***, and delete the added protocols with ***Select All*** and ***Delete*** operations.

> ***Caution:***
>
> *The Predefined Service Protocols can not be deleted.*

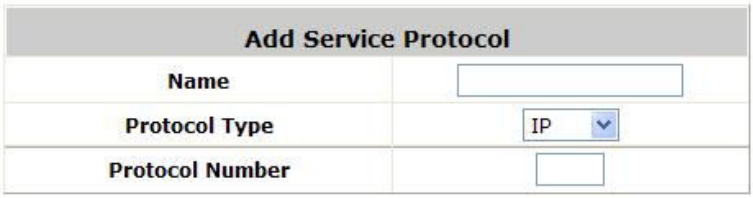
Click **Add** to add a custom service protocol. The **Protocol Type** can be defined from a list of service by

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**, it will need to define **Type** and **Code**.



If the **Protocol Type** is **IP**, it will need to define **Protocol Number**.



2. 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.

  This link leads to the Firewall Rules page. 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**.

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

Selecting the Filter Rule Number 1 as an example:

Global Policy - 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, WAN1**, **WAN2**, **Default**, and the named **Service Zones** to be applied for the traffic interface.
- **Source/Destination – IP Address/Domain Name:** Enter the source and destination IP addresses. Domain Host filtering is supported but Domain name 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:** There are 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 checked. 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 passing.

6.3.2 Routing

- **Specific Route Profile:** Click the button of ***Setting*** for **Specific Route Profile**, the Specific Route Profile list will appear.

1. Specific Route

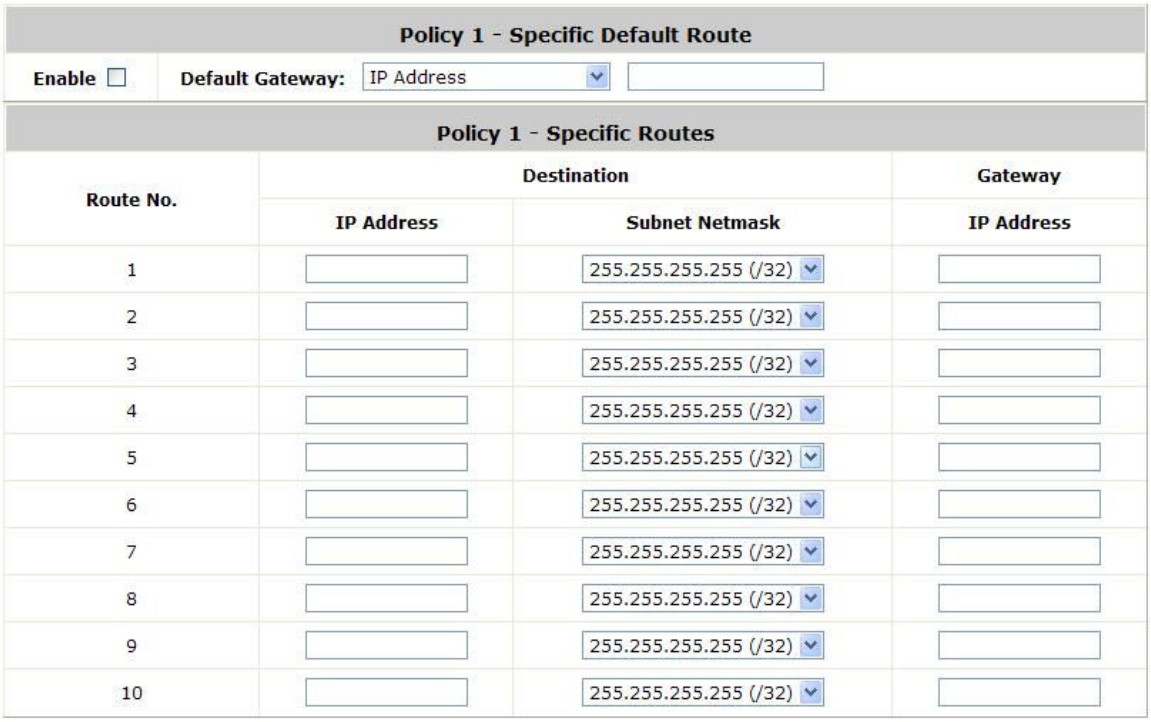
- **Specific Route Profile:** The Specific Route is use to control clients to access some specific IP segment by the specified gateway.

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)	
5		255.255.255.255 (/32)	
6		255.255.255.255 (/32)	
7		255.255.255.255 (/32)	
8		255.255.255.255 (/32)	
9		255.255.255.255 (/32)	
10		255.255.255.255 (/32)	

- **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 are just 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

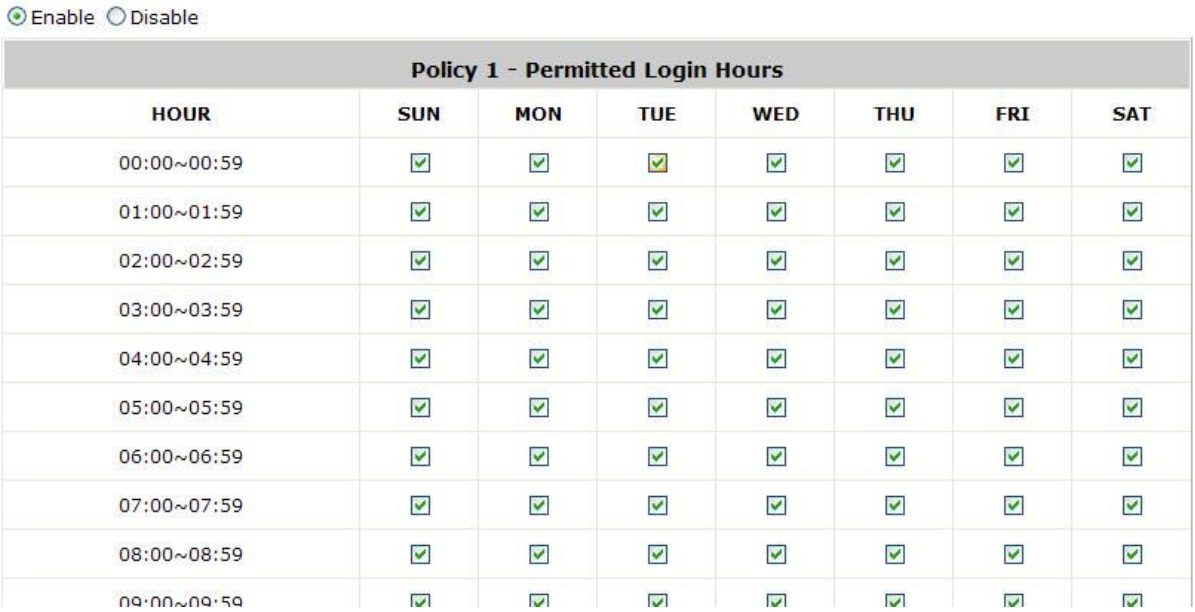
- **Default Gateway:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in each Policy except **Global Policy**. When Specific Default Route is enabled, all clients applied with this Policy will access the Internet through this default gateway.



- **Enable:** Check ***Enable*** box to activate this function or uncheck to inactivate it.
- **Default Gateway:** It may be **WAN1 Default Gateway**, **WAN2 Default Gateway** or to specific an **IP Address**, if you select **IP Address**, you may need to fill the IP address of the 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 Sessions Limit

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

- The maximum number of concurrent sessions (TCP and UDP) for each user can be specified in the Global policy, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones. Also this can 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 and 300), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to a Syslog server.
- Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in network deployment to maintain network operation.

6.4 QoS Traffic Class and Bandwidth Control

Configure QoS, go to: ***Users >> Group***.

- **QoS Profile:** Set parameters for traffic classification.

  - **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.
  - **Group Total Downlink:** Defines the maximum bandwidth allowed to be shared by clients within this Group.
  - **Individual Maximum Downlink:** Defines the maximum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Downlink cannot exceed the value of Group Total Downlink.
  - **Individual Request Downlink:** Defines the guaranteed minimum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Request Downlink cannot exceed the value of Group Total Downlink and Individual Maximum Downlink.
  - **Group Total Uplink:** Defines the maximum uplink bandwidth allowed to be shared by clients within this Group.
  - **Individual Maximum Uplink:** Defines the maximum uplink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Uplink cannot exceed the value of Group Total Uplink.
  - **Individual Request Uplink:** Defines the guaranteed minimum bandwidth allowed for an individual client belonging to this Group. The Individual Request Uplink cannot exceed the value of Group Total Uplink and Individual Maximum Uplink.

7.Users' Login and Logout

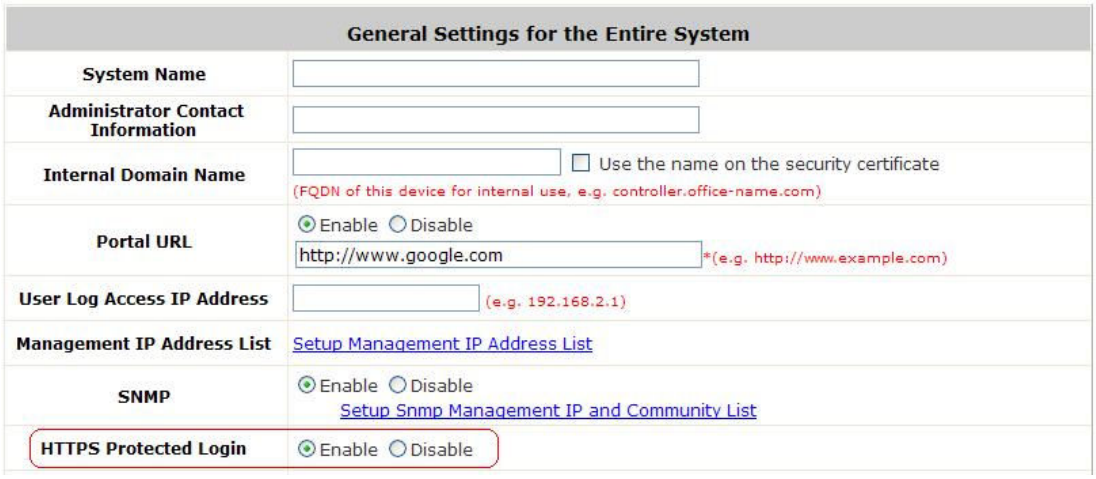
7.1 Before User Login

7.1.1 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 sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

This 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.

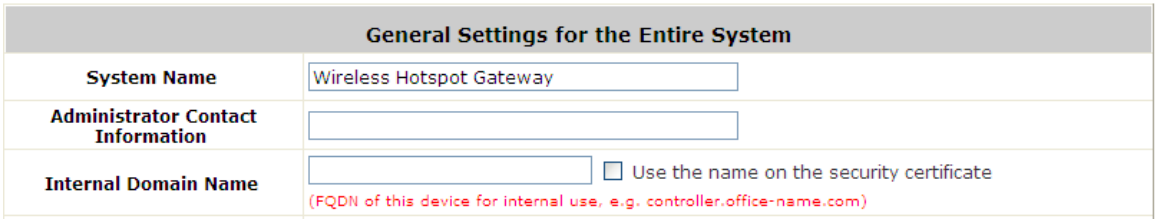


7.1.2 Internal Domain Name with Certificate

Configure Internal Domain Name, go to: ***System >> General***.

Internal Domain Name is the domain name of the AMG-2102 as seen on client machines connected under service zone. It must conform to FQDN (Fully-Qualified Domain Name) standard. A user on client machine can use this domain name to access AMG-2102 instead of its IP address.

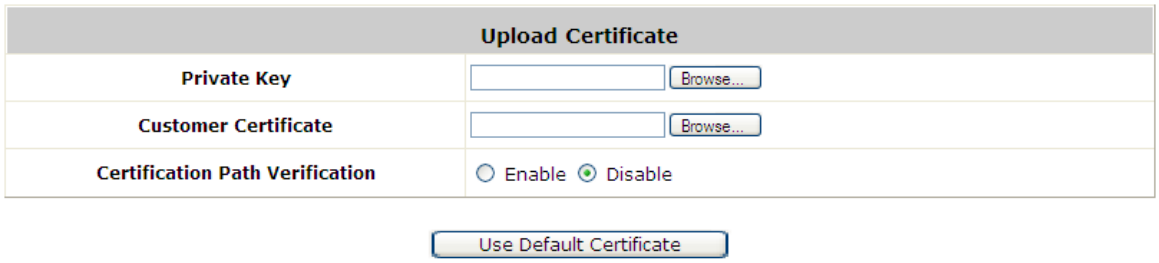
In addition, when "***Use the name on the security certificate***" option is checked, the system will use the CN (Common Name) value of the uploaded SSL certificate as the domain name.



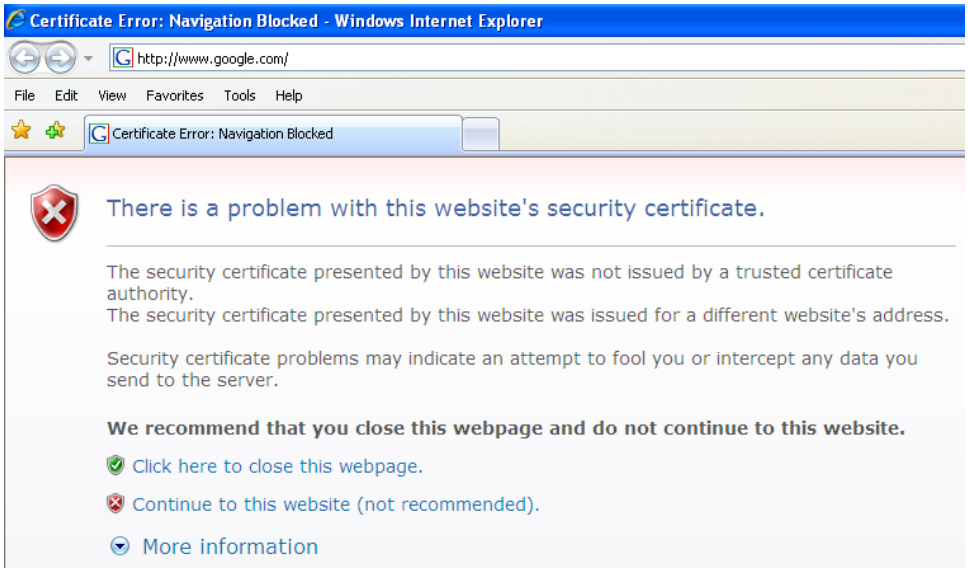
Configure Certificate, go to: ***Users >> Additional Configuration >> Certificate***.

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 an SSL Certificate, please Click Browse to select the file and upload it. Click ***Apply*** to complete the upload process.

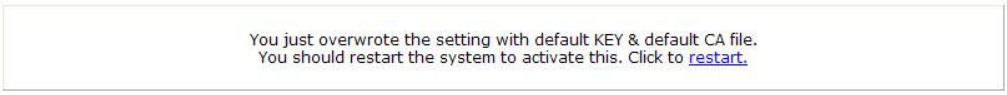


Without a valid certificate, users may encounter the following problem in IE7 when they try to open the login page.



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

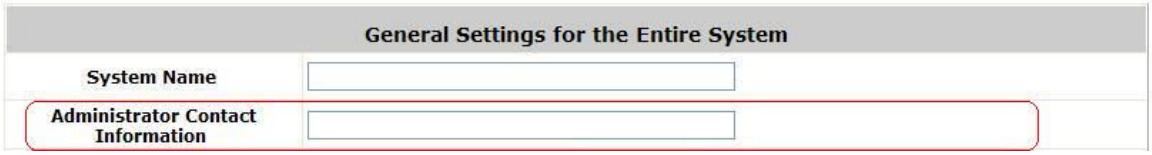
To Use Default Certificate: Click ***Use Default Certificate*** to use the default certificate and key. Click **restart** to validate the changes.



7.1.3 Administrator Contact Information

Configure Administrator Contact Information, go to: ***System >> General***.

Administrator Contact Information will appear in the user Login Fail window. When the user login fail with duplicate IP address or MAC address, system will show this contact information to the user by the Login Fail window.



7.1.4 Walled Garden

Configure 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. Multiple addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Enter the website **IP Address** or **Domain Name** in the list and click ***Apply*** to save the settings.

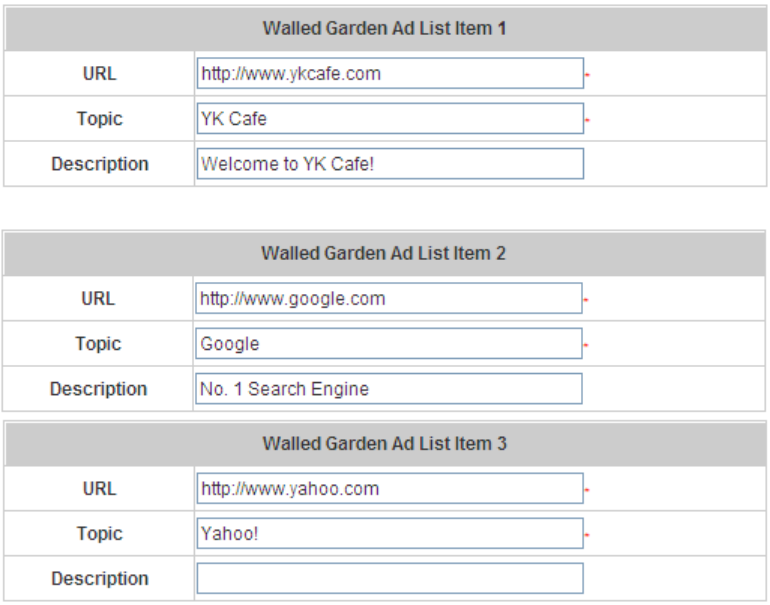
Walled Garden List			
No.	**Domain Name/IP Address**	**No.**	**Domain Name/IP Address**
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

7.1.5 Walled Garden AD List

Configure Walled Garden AD List, go to: ***Network >> Walled Garden AD List***.

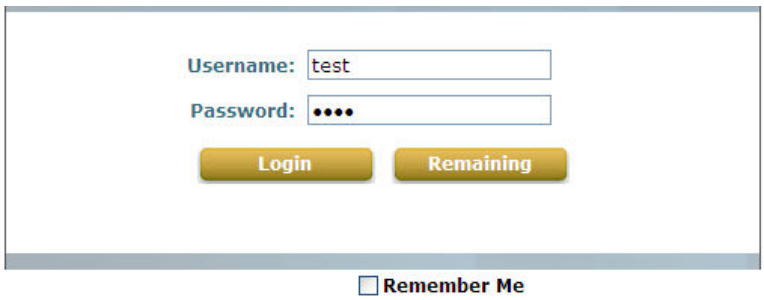
This function provides advertisement web pages for users to access free advertisement websites listed before login and authentication. Advertisement hyperlinks are displayed on the user's login page. Clients who click on it will be redirected to the listed advertisement websites.

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



Walled Garden Ad List

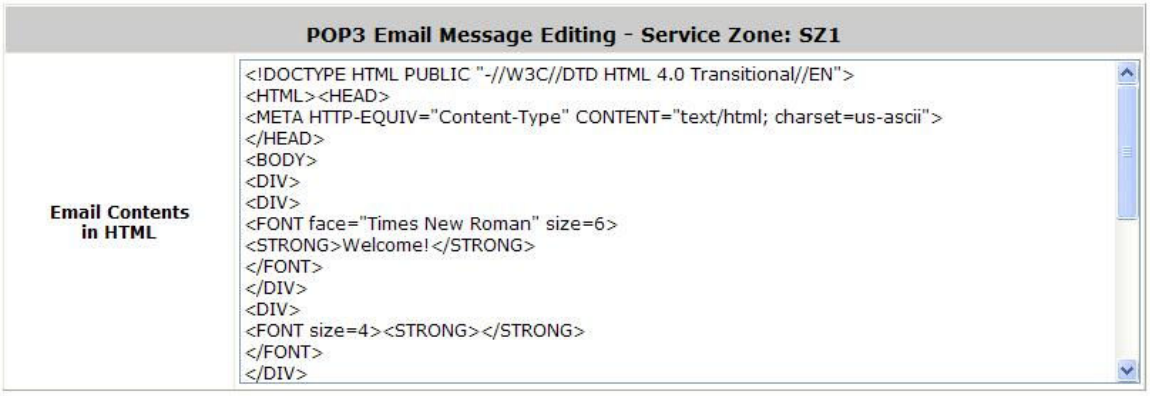
Item	URL / Description	Topic	Edit	Display
1	http://ykcafe.com Welcome to YK Cafe!	YK Cafe	Edit	☑
2	http://www.google.com No.1 Search Engine	Google	Edit	☑
3	http://www.yahoo.com	Yahoo!	Edit	☑



7.1.6 Mail Message

Configure Mail Message, go to: ***System >> Service Zones***.

When enabled, the system will automatically send an email to users if they attempt to send/receive their emails using POP3 email program (for example, Microsoft Outlook) before they are authenticated. Click ***Edit Mail Message*** to edit the message in HTML format.

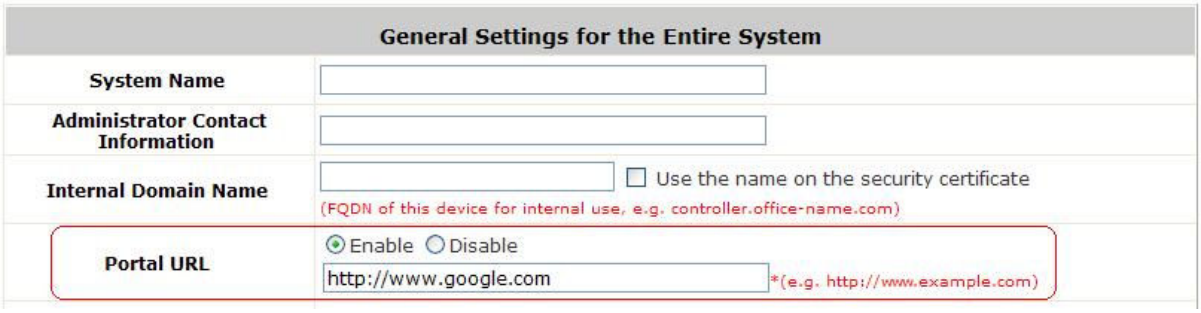


7.2 After User Login

7.2.1 Browse which Home Page after login success

Configure Portal URL, go to: ***System >> General***.

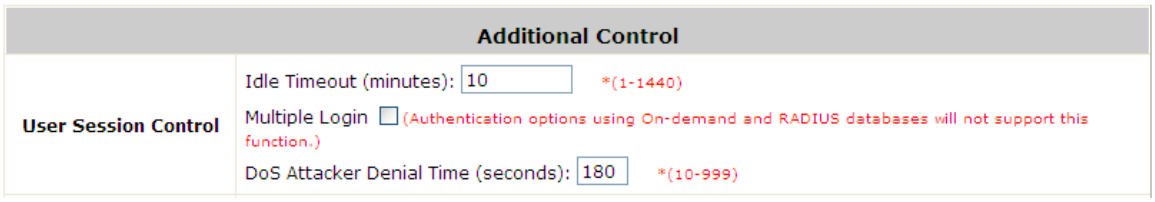
If enable this function, enter the URL of a Web server as the homepage. Once logged in successfully, users will be directed to this homepage, such as *http://www.google.com*, regardless of the original homepage set in their computers.



If disable this function, after users logged in successfully, users will be directed to the original homepage.

7.2.2 Idle Timer

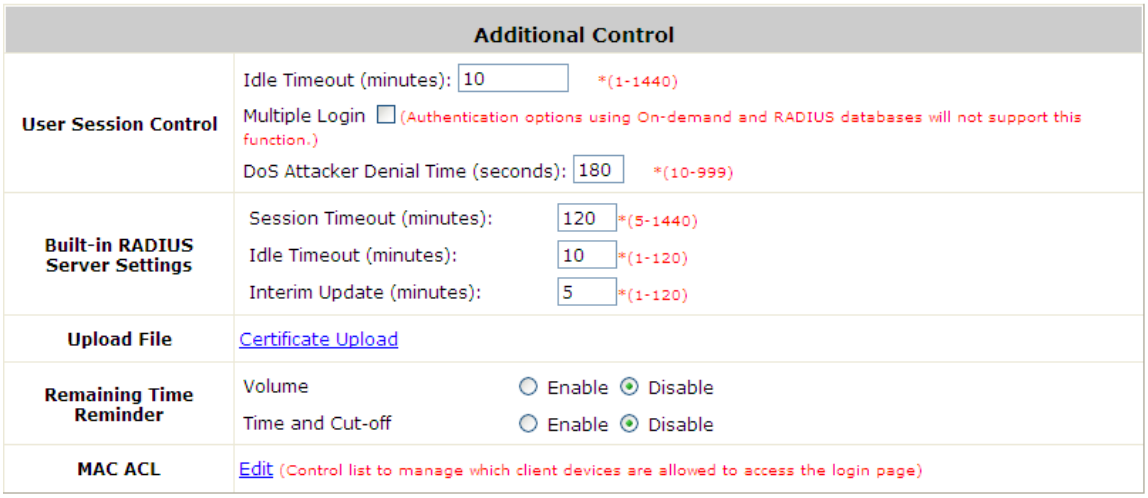
Configure Idle Timer, go to: ***Users >> Additional Configuration***.



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

7.2.3 Multiple Login

Configure Multiple Login, go to: ***Users >> Additional Configuration***.

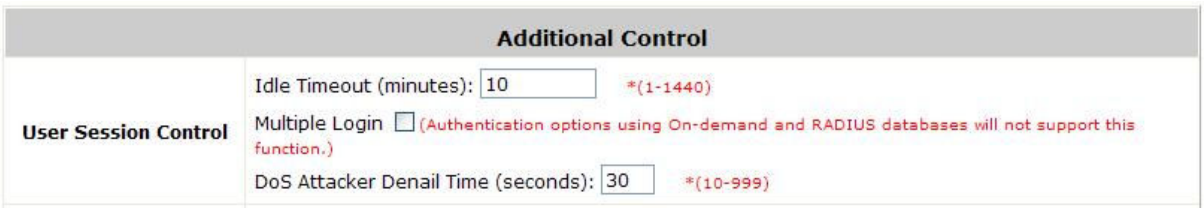


When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS authentication.)

7.2.4 DoS Attacker Denial Time

Configure DoS Attacker Denial Time, go to: ***Users >> Additional Configuration***.

It is the denial time to the DoS attacker. When system detect the user has DoS behaviors, system will prohibit the network access right of this user with this time period. After this time period, the user can access normally.



7.2.5 Local Users Change Password Privilege

Configure Local Users Change Password Privilege, go to: ***Users >> Group***.

- **Privilege Profile: Change Password**

Group 1 - Privilege Configuration	
Ondemand Account Privilege	◉ Enable ○ Disable
Change Password Privilege	◉ Enable ○ Disable

  - **Change Password Privilege:** When **Change Password Privilege** is enabled, the authenticated local users within this Group are allowed to change their password via the Login Success Page.

Caution:

This function is only for Local User.

7.2.6 On-demand Account Creation Privilege

Configure On-demand Account Creation Privilege, go to: ***Users >> Group***.

- **Privilege Profile: On-demand Account Creation**

Group 1 - Privilege Configuration	
Ondemand Account Privilege	◉ Enable ○ Disable
Change Password Privilege	◉ Enable ○ Disable

  - When **On-demand Account Creation Privilege** is enabled, the authenticated users within this **Group** are allowed to create On-demand account via the **Login Success Page**.

- **Privilege Profile: On-demand Billing Plans**

  Configure On-demand Billing Plans, go to:

  Users >> Authentication >> On-demand User >> Billing Plan.

Billing Plans							
Plan	**Type**	**Quota**	**Price**	**Enable** ☐	**Privilege** ☐	**Group**	**Function**
1	Usage-time	2 hr(s)	20	☑	☑	Group 1	Edit
2	Cut-off	Until 13:00	20	☑	☑	Group 2	Edit
3	Volume	1000 Mbyte(s)	40	☑	☑	Group 3	Edit
4	Duration-time	From 2009/11/01 00:05:00 till 2009/11/05 13:05:00	100	☑	☑	Group 4	Edit
5	Duration-time	5 day(s) 2 hour(s)	40	☑	☑	Group 4	Edit
6	N/A			☐	☐	None	Edit
7	N/A			☐	☐	None	Edit
8	N/A			☐	☐	None	Edit
9	N/A			☐	☐	None	Edit
0	N/A			☐	☐	None	Edit

  - Enable the **On-demand Account Creation Privilege** of the plans. After the user login success, in the Login Success Page, select a billing plan and click ***Create***. It will create

On-demand user account.

Caution:

This function is not for On-demand User. On-demand users can not create another On-demand user.

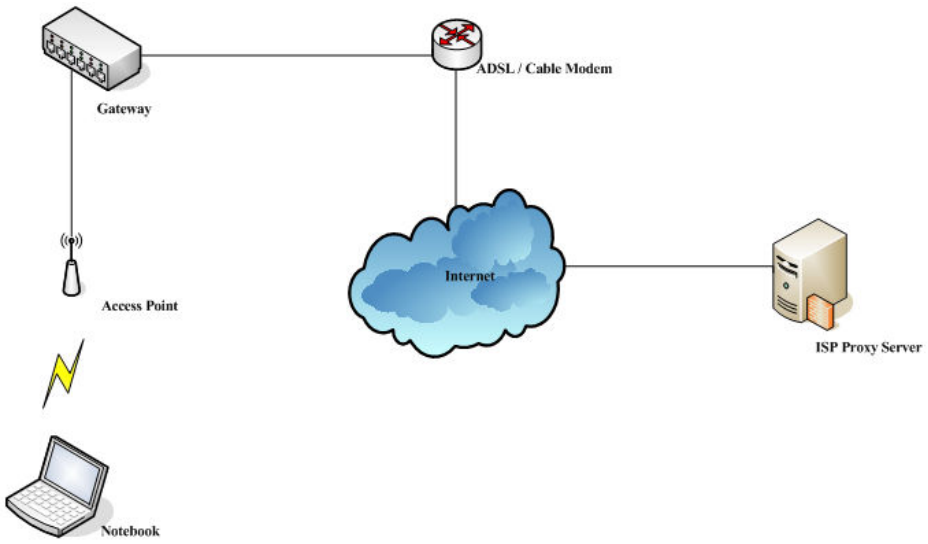
7.2.7 Proxy Server

Configure Proxy Server, go to: ***Network >> Proxy Server***.

Basically, a proxy server can help clients access the network resources more quickly. This section presents basic examples for configuring the proxy server settings of AMG-2102.

▪ Using Internet Proxy Server

The first scenario is that a proxy server is placed outside the LAN environment or in the Internet. For example, the following diagram shows that a proxy server of an ISP will be used.



Follow the following steps to complete the proxy configuration:

Step 1. Log into the system by using the ***admin*** account.

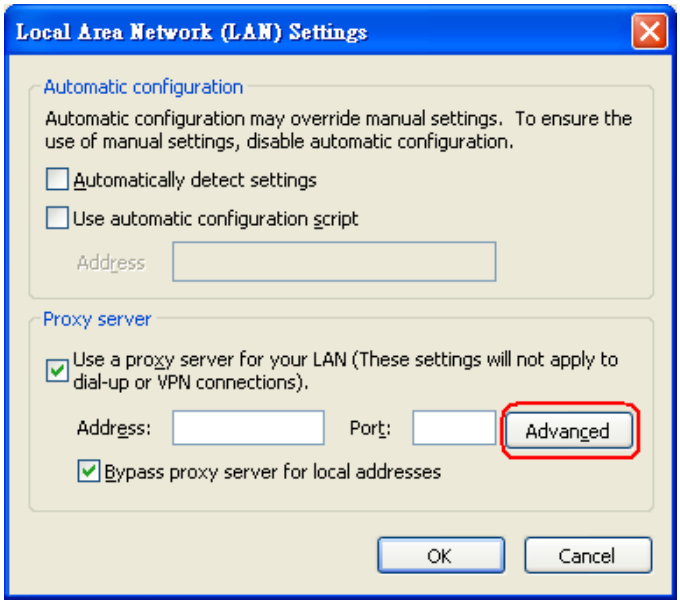
Step 2. ***Network >> Proxy Server >> External Proxy Servers*** page. Add the IP address (leaving it blank means any IP address) and port number of the proxy servers into ***External Proxy Servers*** setting. Enable the ***Built-in Proxy Server***. Click ***Apply*** to save the settings.

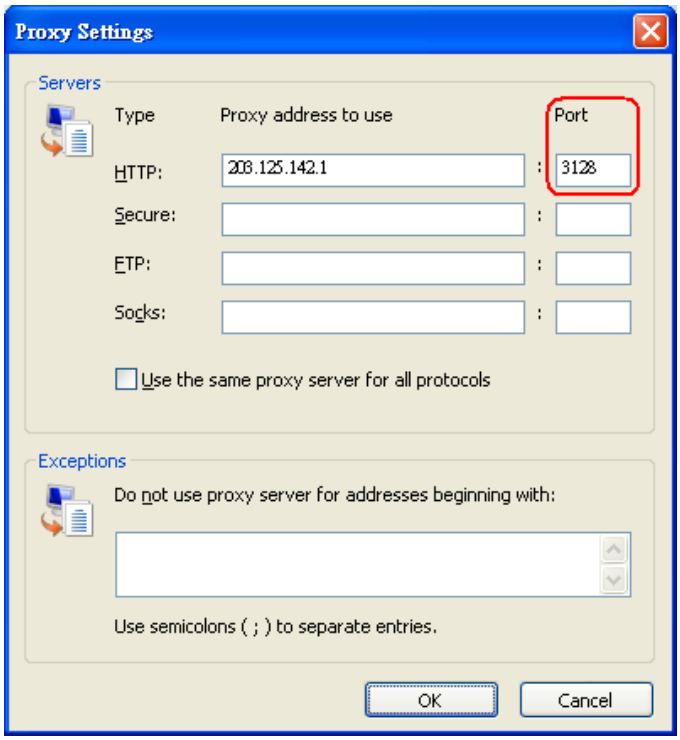
External Proxy Servers		
No.	**IP Address**	**Port**
1		6588
2		8080
3		8023
4		3128
5		
6		
7		
8		
9		
10		

(Total: 40) First Prev Next Last

Redirect Outgoing Proxy Traffic to Built-in Proxy Server	
Built-in Proxy Server	◉ Enable ○ Disable

Step 3. Make sure that the proxy server settings match with at least one of the proxy server setting of the system – for example, in this case, 203.125.142.1:**3128** matches with blank:**3128**.





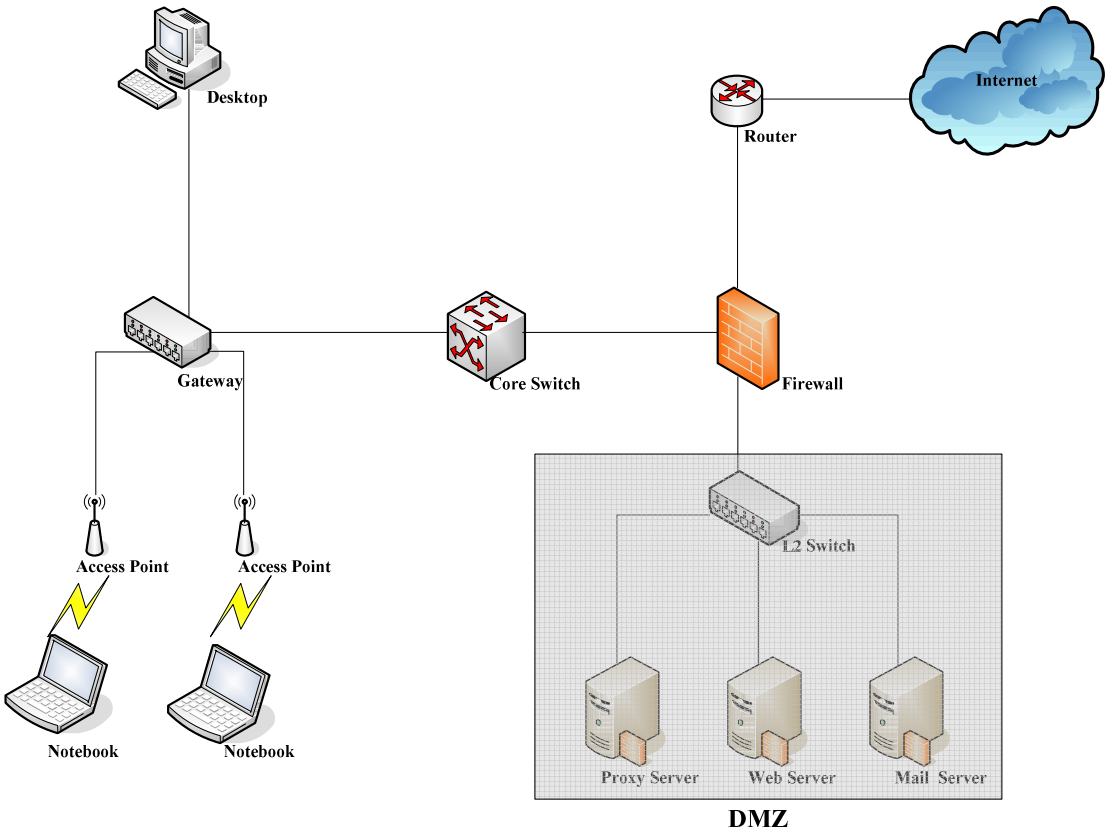
Caution:

1 *It is required that the proxy server setting of the clients match with the proxy server setting of the system. Otherwise, users will not be able to get the Login page for authentication via browsers and it will show an error page in the browser.*

2 *What the **Built-in Proxy Server** is enabled, all the outgoing proxy traffic will be automatically redirected to the built-in proxy server.*

▪ Using Extranet Proxy Server

The second scenario is that a proxy server is placed in the Extranet (such as DMZ), which all users from the Intranet or the Internet are able to access. For example, the following diagram shows that a proxy server of an organization in the DMZ will be used.



Caution: *A special scenario is that a proxy server is placed in a zone like Intranet – where users can reach each other without going through the system. In this case, whenever any one of users in the Intranet has been authenticated and connects to the network via the proxy server, other users using the same proxy setting in their browsers will be able to access the network without any authentication. Therefore, to stop the risk, it is strongly recommended to put all proxy servers outside the Intranet.*

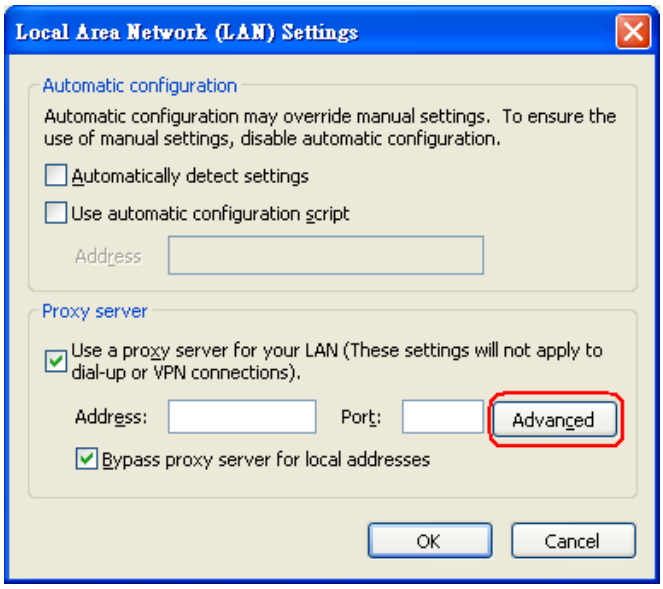
Follow the following steps to complete the proxy configuration:

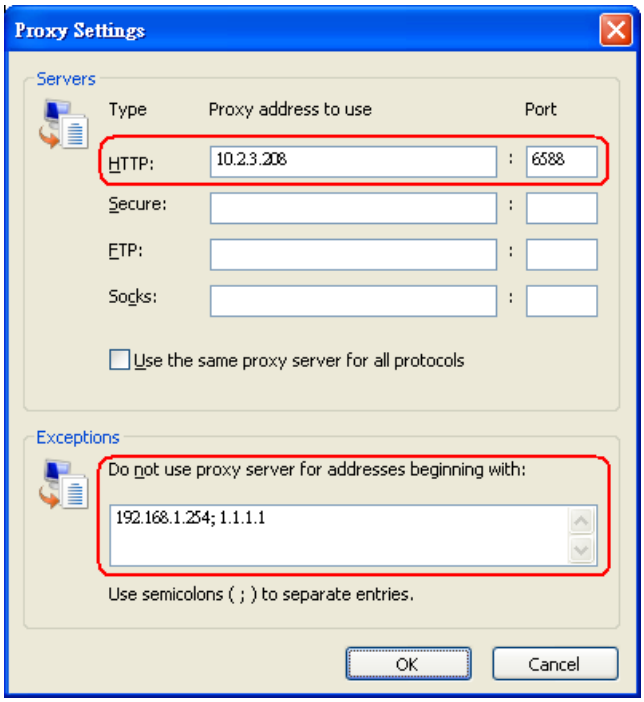
Step 1. Log in the system by using the ***admin*** account.

Step 2. **Network >> Proxy Server >> External Proxy Servers** page. Add the IP address and port number of the Proxy server into External Proxy Servers setting. Click ***Apply*** to save the settings.

Step 3. Make sure that clients use the same proxy server settings. Please also configure

appropriate exceptions if there is any traffic which is not needed to go through proxy server – for example, there is no need to use proxy server for the Default Gateway (192.168.1.254).





Caution: *It is required that the proxy server setting of the clients match with the proxy server setting of the system. Otherwise, users will not be able to get the Login page for authentication via browsers and it will show an error page in the browser.*

8. Networking Features of a Gateway

8.1 DMZ

Configure DMZ, go to: ***Network >> NAT >> DMZ (Demilitarized Zone)***.

The system supports Internal IP address (LAN) to External IP address (WAN) mapping in the Static Assignments. The External IP Address of the Automatic WAN IP Assignment is the IP address of External Interface (WAN1) that will change dynamically if WAN1 Interface is Dynamic. When **Automatic WAN IP Assignments** is enabled, the entered Internal IP Address of Automatic WAN IP Assignment will be bound with WAN1 interface. Each **Static Assignment** could be bound with the chosen External Interface, WAN1 or WAN2. There are static **Internal IP Address** and **External IP Address** available. Enter **Internal** and **External** IP Addresses as a set. After the setup, accessing the WAN will be mapped to access the Internal IP Address. These settings will become effective immediately after clicking the ***Apply*** button.

Automatic WAN IP Assignment

Enable	External IP Address	External Interface	Internal IP Address	Remark
☐		WAN1		

Static Assignments

No.	External IP Address	External Interface	Internal IP Address	Remark
1		WAN1		
2		WAN1		
3		WAN1		
4		WAN1		
5		WAN1		
6		WAN1		
7		WAN1		
8		WAN1		
9		WAN1		
10		WAN1		

(Total:40) First Prev Next Last

8.2 Virtual Server

Configure Virtual Server, go to: ***Network >> NAT >> Public Accessible Server***.

This function allows the administrator to set virtual servers, 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	Remark
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	☐	

8.3 Privilege List

Configure Privilege List, go to: ***Network >> Privilege***.

Setup the **Privilege IP Address List** and **Privilege MAC Address List**. The clients in the list can access the network without any login.

8.3.1 Privilege IP

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. AMG-2102 allows 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		
4		
5		
6		
7		
8		
9		
10		

Caution:

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

8.3.2 Privilege MAC

Privilege MAC Address List

In addition to the IP address, the MAC address of the workstations that need to access the network without authentication can also be set in the **"Granted Access by MAC Address"**. AMG-2102 allows privilege MAC addresses. 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		

Caution:

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

8.4 IP Plug and Play

Configure IP Plug and Play, go to: ***Network >> Client Mobility***

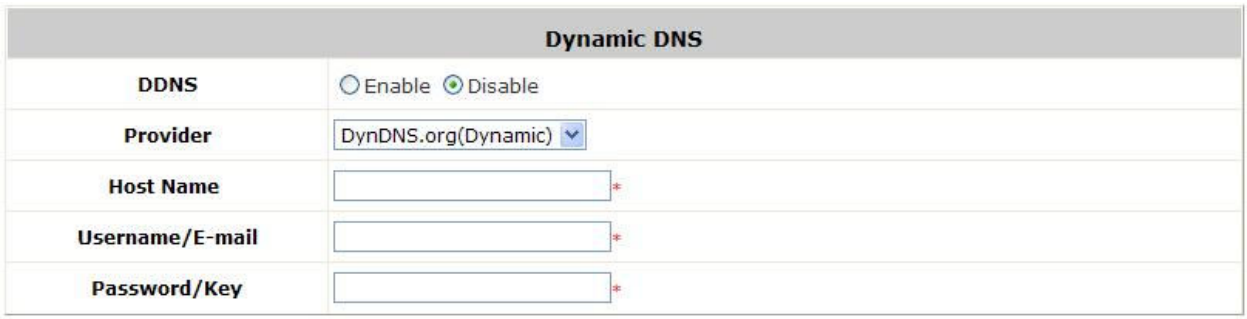
AMG-2102 supports IP PNP function. User can login and access network with any IP address setting.

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 AMG-2102.

8.5 Dynamic Domain Name Service

Configure 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. AMG-2102 supports DNS function to alias the dynamic IP address for the WAN port to a static domain name, allowing the administrator to easily access AMG-2102'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.

Note:

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

8.6 Port and IP Redirect

Configure Port and IP Redirect, go to: ***Network >> NAT >> Port and IP Forwarding***.

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

Port and IP Forwarding

No.	Destination		Translated to Destination		Type	Remark
	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	

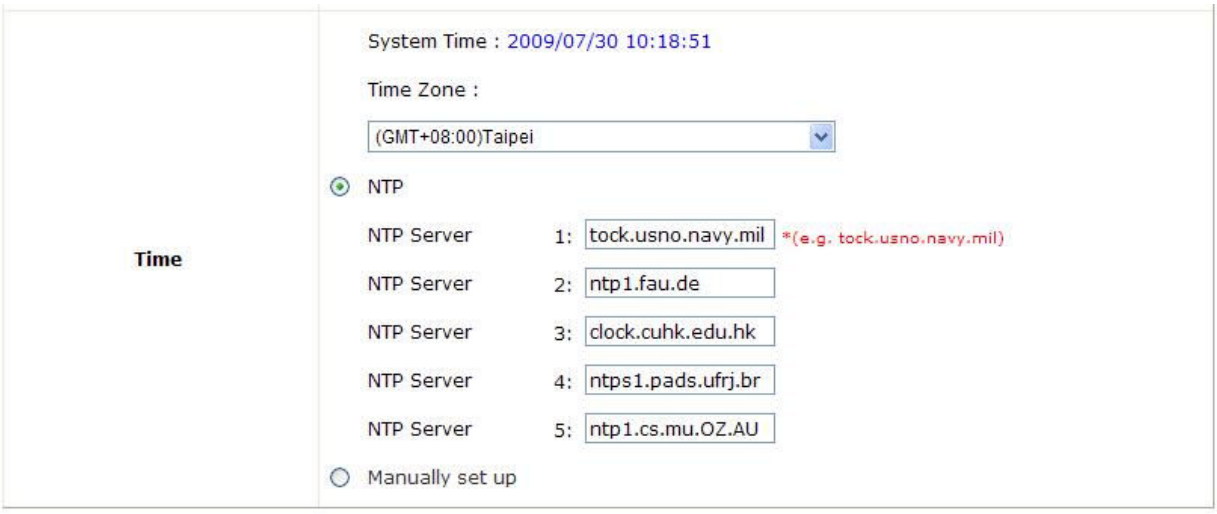
9.System Management and Utilities

9.1 System Time

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

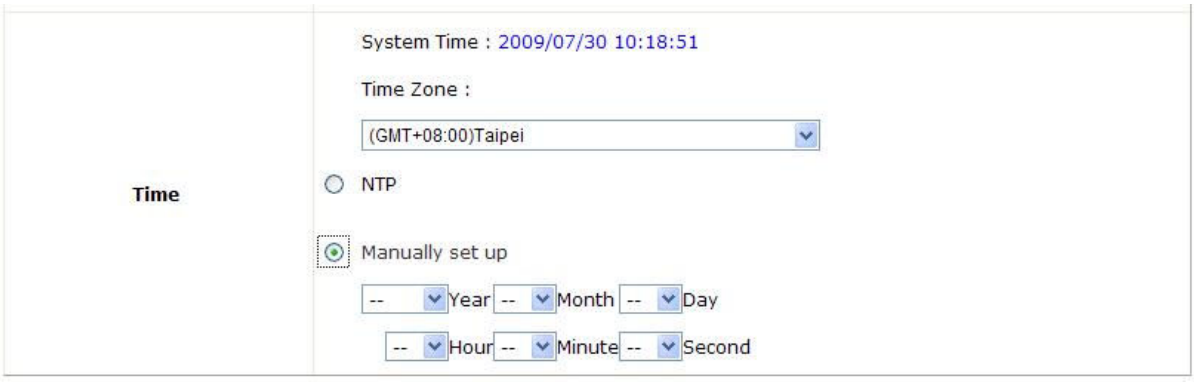
9.1.1 NTP

NTP (Network Time Protocol) communication protocol can be used to synchronize the system time with 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).



9.1.2 Manual Settings

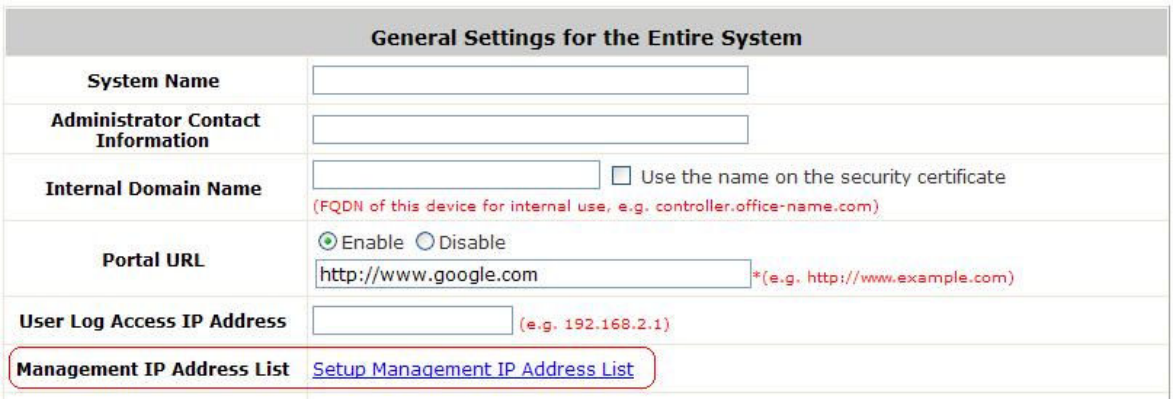
The time can also be manually configured by selecting **Manually set up** and then select the date and time in these fields.



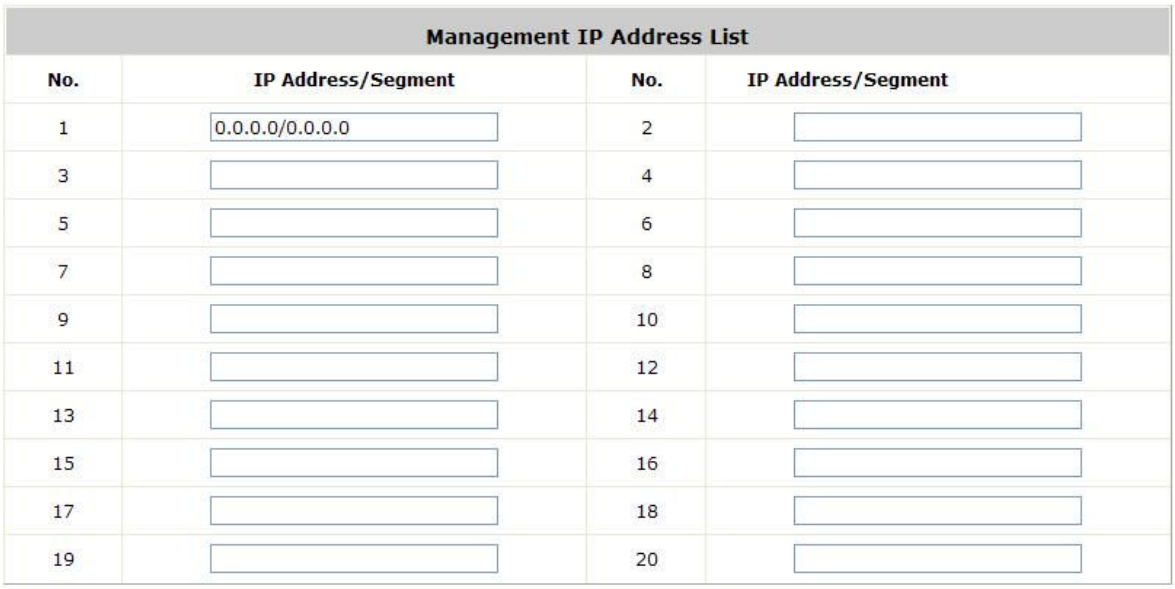
9.2 Management IP

Configure Management IP, go to: ***System >> General***.

Only PCs within this 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.

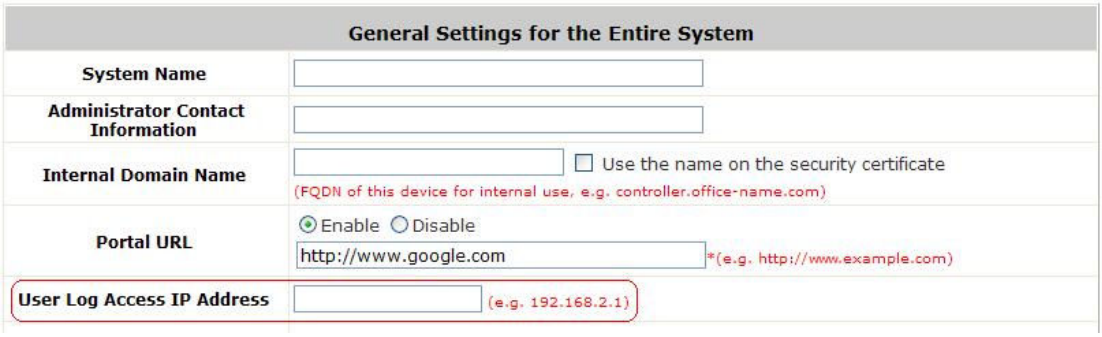


The default value is "0.0.0.0/0.0.0.0". It means that the WMI can be accessed by any IP address, for security consideration; please change this value before the system provides service.



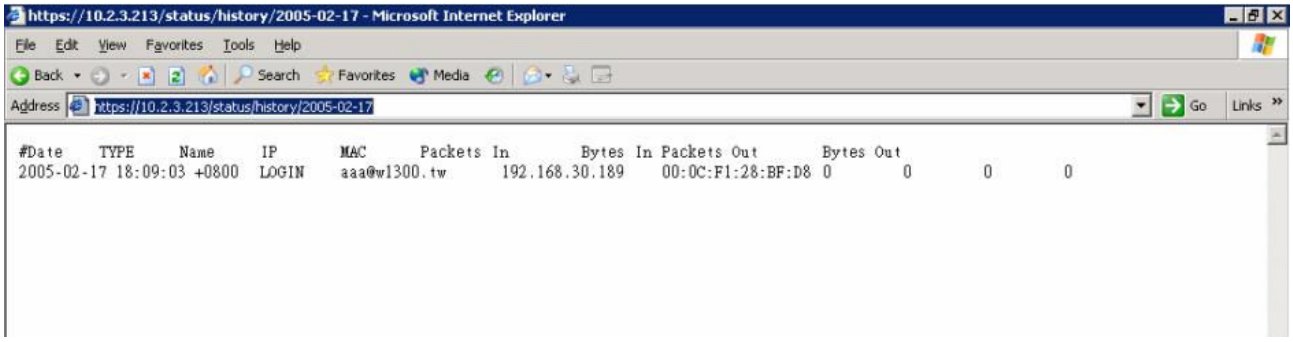
9.3 Access History IP

Configure Access History IP, go to: ***System >> General***.

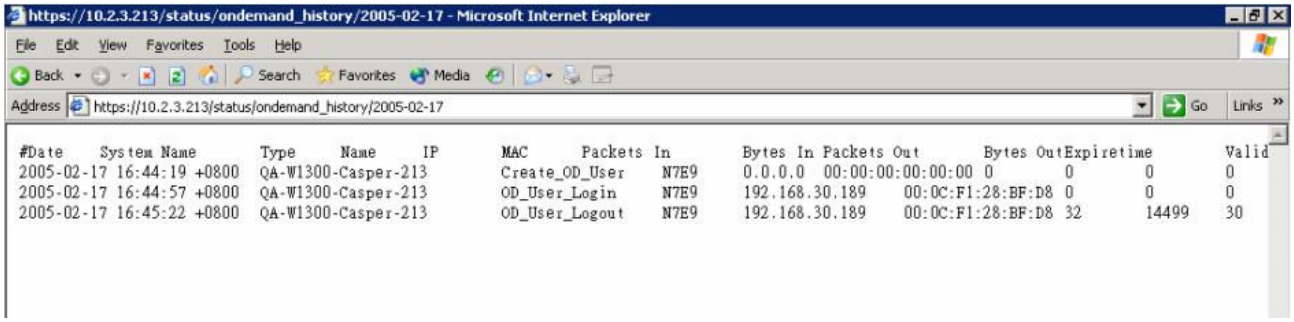


Specify an IP address of the administrator's computer or a billing system to get billing history information of AMG-2102 with the predefined URLs. The file name format is "yyyy-mm-dd". An example is provided as follows:

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



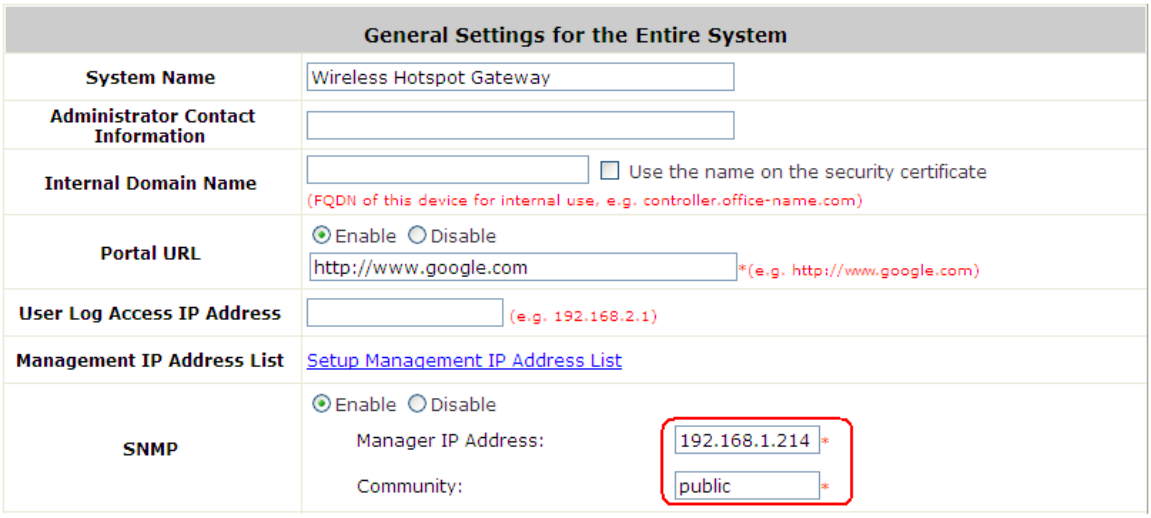
On-demand History : https://10.2.3.213**/status/ondemand_history/**2005-02-17



9.4 SNMP

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

If this function is enabled, the SNMP Management IP and the Community can be assigned to access the **SNMP Configuration List** of the system.



9.5 Three-Level Administration

AMG-2102 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 AMG-2102.

User Name: **admin**

Password: **admin**

After a successful login to AMG-2102, a web management interface will appear.

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

User Name: **manager**

Password: **manager**

Users	
Authentication	The internal or external account databases include Local, POP3, RADIUS, LDAP, NT Domain, On-demand and SIP. The administrator needs to activate and configure at least one of these authentication databases. Postfix is used for the system to identify which authentication option will be used for the specific user account when multiple options are concurrently in use. One of the authentication options can be set as default, so that end users can choose NOT to type the complete account name (id@postfix) when logging in.
Black List	5 sets of black list profiles can be defined. Each active authentication option may be configured with one of these 5 black list profiles.
Group	8 sets of group profiles including QoS Configurations, Instant Account Privilege, Change Password Privilege, and Zone Permission Configuration & Policy Assignment can be defined for each group option to enforce the access management for different groups of users.
Policy	A policy can be selected to apply to a group of users within a zone. 12 sets of policy profiles including Firewall Profile, Specific Route Profile, Schedule Profile, and Session Limit Management can be defined.
Additional Control	Additional configurations are in this section. They are User Session Control, Built-in RADIUS Server Settings, Customization, Remaining Time Reminder, and MAC ACL. The administrator can control user session such as idle timeout in User Session Control. Three fuctions are provided in Built-in RADIUS Server Settings such as session timeout. In Customization, the administrator can upload certificate to the system. Remaining Time Reminder provides remaining time information to clients on the screen. The administrator can manage the access control to the system via clients' MAC address in the MAC ACL(Access Control List).
Net Retriever	By setting up the connection to Net Retriever, the system can listen to certain messages from PMS behind Net Retriever. When hotel guest is buying an in-room billing plan for Internet access, the system will post a record to PMS through Net Retriever.

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	N/A	N/A	N/A	Disabled	Create
2	N/A	N/A	N/A	Disabled	Create
3	N/A	N/A	N/A	Disabled	Create
4	N/A	N/A	N/A	Disabled	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

Note:

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

9.6 Change Password

Configure Change 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 AMG-2102.

User Name: **admin**

Password: **admin**

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

User Name: **manager**

Password: **manager**

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

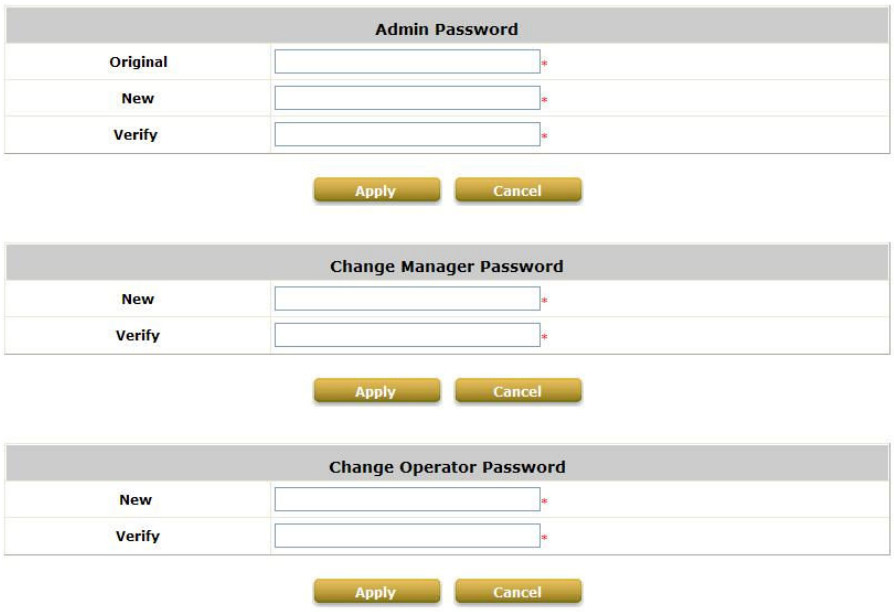
User Name: **operator**

Password: **operator**

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

Note:

Only login with **admin** can change password.



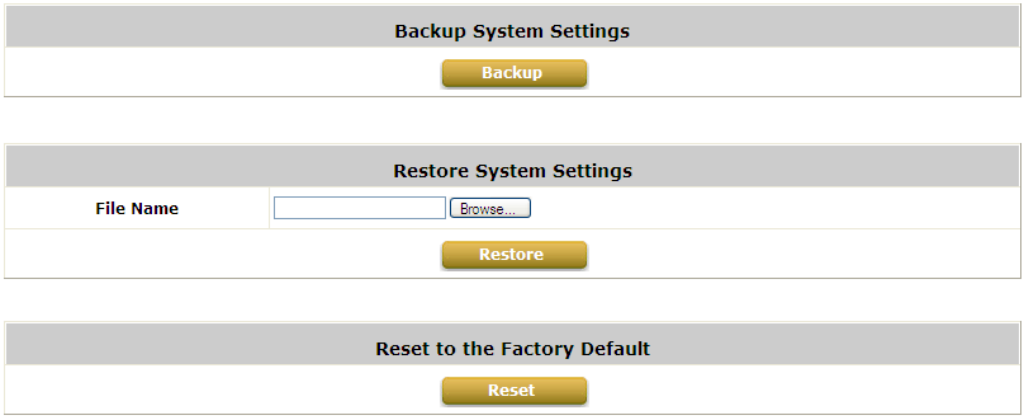
Caution:

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

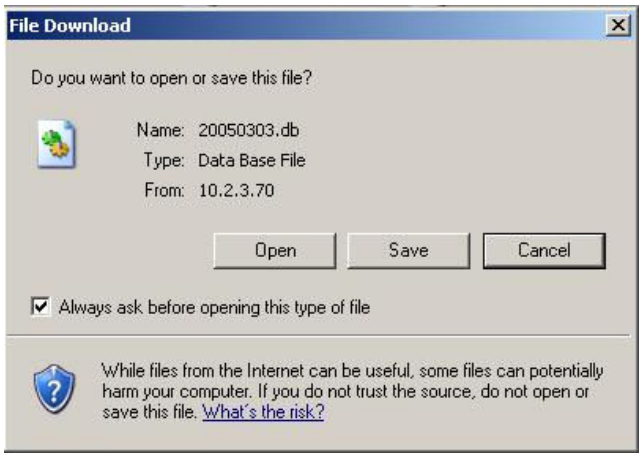
9.7 Backup / Restore and Reset to Factory Default

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

This function is used to backup/restore the AMG-2102 settings. Also, AMG-2102 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.

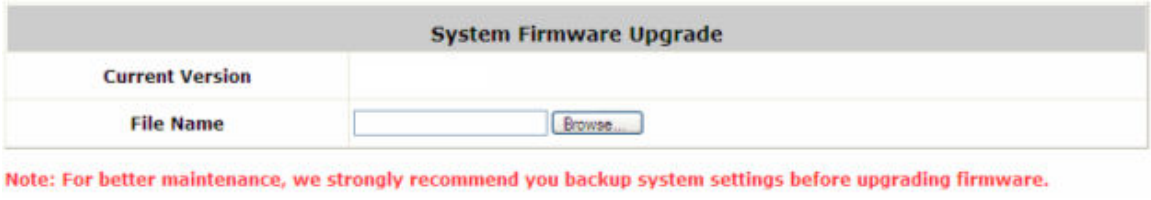


- **Restore System Settings:** Click ***Browse*** to search for a .db database backup file created by AMG-2102 and click ***Restore*** to restore to the same settings at the time when the backup file was saved.
- **Reset to Factory Default:** Click ***Reset*** to load the factory default settings of AMG-2102.

9.8 Firmware Upgrade

Configure Firmware Upgrade, go to: ***Utilities*** >> ***System Upgrade***.

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



Caution:

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

9.9 Restart

Configure Restart, go to: ***Utilities >> Restart***.

This function allows the administrator to safely restart AMG-2102, and the process might take approximately three minutes. Click ***YES*** to restart AMG-2102; click ***NO*** to go back to the previous screen. If the power needs to be turned off, it is highly recommended to restart AMG-2102 first and then turn off the power after completing the restart process.

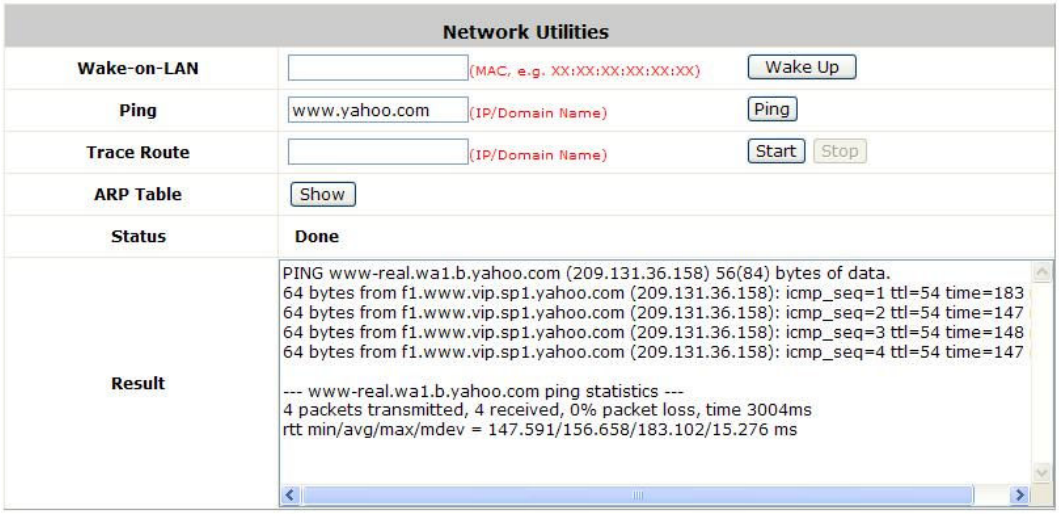
Caution:

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

9.10 Network Utility

Configure Network Utility, go to: ***Utilities >> Network Utilities***.

System provide some network utilities to allow administrators to use, the functions including **Wake-on-LAN**, **Ping**, **Trace Route** by entering IP or Domain Name and showing **ARP Table**.



9.10.1 Wake-on-LAN

It allows the system to remotely boot up a power-down computer with Wake-On-LAN feature enabled in its BIOS and it is connect to any service zone. Enter the MAC Address of the desired device and click Wake Up button.

9.10.2 Ping

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

9.10.3 Trace Route

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

9.10.4 Show ARP Table

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

9.11 Monitor IP Link

Configure Monitor IP Link, go to: ***Network >> Monitor IP***.

AMG-2102 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 setting.

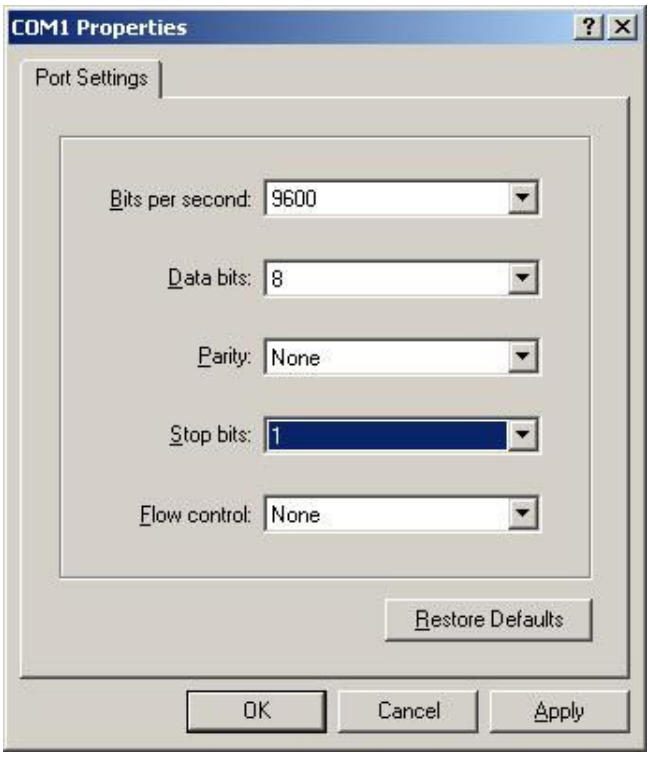
Monitor IP List

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	
11	http		Create	
12	http		Create	
13	http		Create	
14	http		Create	
15	http		Create	
16	http		Create	
17	http		Create	
18	http		Create	
19	http		Create	
20	http		Create	

9.12 Console Interface

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

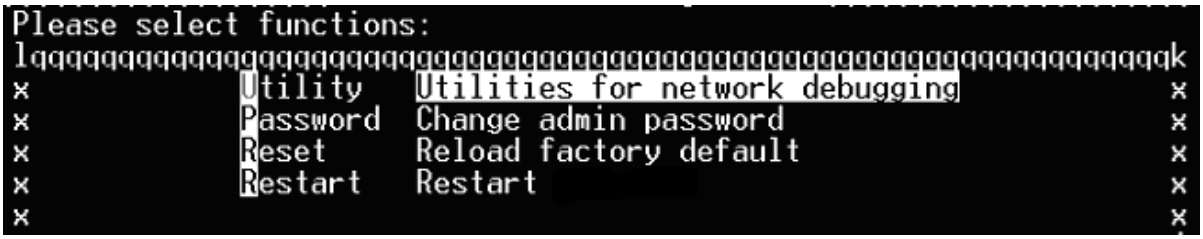
1. In order to connect to the console port of AMG-2102, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **9600, 8, None, 1, None.**



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 AMG-2102 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system, where the welcome screen or main menu should appear. If the welcome screen or main menu of the console still does not pop up, please check the connection of the cables and the settings of the terminal simulation program.


Please select functions:
Utility Utilities for network debugging
Password Change admin password
Reset Reload factory default
Restart Restart

- **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 request to a specified host and wait for the response to test the network status.
- Trace routing path: Trace and inquire the routing path to a specific target.
- Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and Netmask.
- Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
- Display ARP table: The internal ARP table of the system is displayed.
- Display system up time: The system live time (time for system being turn on) is displayed.
- Check service status: Check and display the status of the system.
- Set device into "safe mode": If the administrator is unable to use Web Management Interface via browser for the system failed inexplicitly. The administrator can choose this utility and set it into safe mode, which enables him to manage this device with browser again.
- Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.
- Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The

program helps users to print out their boot-up messages instead of copying the messages by hand.

- Main menu: Go back to the main menu.

- **Change admin password**

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

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

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 AMG-2102 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 AMG-2102**

  Choosing this option will restart AMG-2102.

10. System Status and Reports

10.1 View the status

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

Status	
System	Display current settings of the system.
Interface	Display the current settings of all network interfaces.
Hardware	Display current CPU amd memory usage.
Routing Table	List all Policy Route rules and Global Policy Route rules. The System Route rules are shown here as well. The Policy Route rule has higher priority than the Global Policy route rule. The System Route rule has the lowest priority.
Online Users	Display the information of the online users. Content of the information includes Username, IP Address, MAC Address, Packet Count (In/Out), Byte Count (In/Out) and idle time. Administrator can remove the online user via clicking the Logout button in each record.
User Logs	Display detailed user access records on daily basis. History record of up to 3 days is kept in the system.
E-mail & SYSLOG	The system can send various reports via up to 3 email accounts such as Monitor IP report, Users log, and Session Log. The external SYSLOG server and FTP server are configured here.

10.1.1 System Status

View System Status, go to: ***Status >> System***.

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

System Setting Overview		
Firmware Version		
Build		
System Name		Wireless Hotspot Gateway
Portal URL		http://www.google.com
SYSLOG Server - System Log		N/A:N/A
SYSLOG Server - On-demand Users Log		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Load Balancing		Disabled
SNMP		Disabled
User Logs	Retained Days	3 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
System Time	NTP Server	tock.usno.navy.mil
	Time	2009/11/04 18:52:53 +0800
User Session Control	Idle Time Out	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A

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

Item		***Description***
Firmware Version		The present firmware version of AMG-2102
Build		The current build number.
System Name		The system name. The default is AMG-2102
Homepage Redirect 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.
Proxy Server		Enabled/disabled stands for that the system is currently using the proxy server or not.
Warning of Internet Disconnection		Enabled/Disabled stands for the connection at WAN is normal or abnormal (**Internet Connection Detection**) and all online users are allowed/disallowed to log in the network.
WAN Failover		Enabled/Disabled stands for the function currently being used or not.
Load Balancing		Enabled/Disabled stands for the function currently being used or not.
SNMP		Enabled/disabled stands for the current status of the SNMP management function.
User Logs	**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 traffic history or user's traffic history information will be sent.
System Time	**NTP Server**	The network time server that the system is set to align.
	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 logins form the same account.

DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

10.1.2 Interface Status

View Interface Status, go to: ***Status >> Interface***.

This section provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **SZ Default** and **SZ1 ~ SZ8**.

Network Interface		
WAN1	**MAC Address**	00:03:01:7A:35:1E
	IP Address	
	Subnet Mask	255.255.0.0
WAN2	**Disabled**	
	WAN1	**WAN2**
Packets In	156956 (Δ 156956)	0 (Δ 0)
Packets Out	38073 (Δ 38073)	0 (Δ 0)
Bytes In	12914288 (Δ 12914288)	0 (Δ 0)
Bytes Out	16753482 (Δ 16753482)	0 (Δ 0)
Service Zone - Default	**Mode**	NAT
	MAC Address	00:03:01:7A:35:1C
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
Service Zone - Default DHCP Server	**Status**	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.1
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
Service Zone - SZ1	**Disabled**	

-
-

Service Zone - SZ8	**Disabled**

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

Item		***Description***
WAN1	**MAC Address**	The MAC address of the WAN1 port.
	IP Address	The IP address of the WAN1 port.
	Subnet Mask	The Subnet Mask of the WAN1 port.
WAN2	**MAC Address**	The MAC address of the WAN2 port.
	IP Address	The IP address of the WAN2 port.
	Subnet Mask	The Subnet Mask of the WAN2 port.
Packets In		The total accumulated packets in 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.
Packets Out		The total accumulated packets 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.
Bytes In		The total accumulated bytes in 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.
Bytes Out		The total accumulated packets 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.
Service Zone - DHCP Server **Default, SZ1~SZ8**	**Status**	Enable/disable stands for status of the DHCP server in Default Service Zone
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.
Service Zone – Default, SZ1~SZ8	**Mode**	The operation mode of the default SZ.
	MAC Address	The MAC address of the default SZ.
	IP Address	The IP address of the default SZ.
	Subnet Mask	The Subnet Mask of the default SZ.

10.1.3 Hardware Information

View Hardware Information, go to: ***Status >> Hardware***.

It will show the current **CPU** and **Memory** usage of the system.

Hardware Information	
CPU	0.00%
Memory	10.67%

10.1.4 Routing Table

View Routing Table, 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**

-
-
-

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

System			
Destination	**Subnet Mask**	**Gateway**	**Interface**
192.168.255.0	255.255.255.0	0.0.0.0	MGMT
192.168.0.0	255.255.254.0	0.0.0.0	Default
192.168.14.0	255.255.254.0	0.0.0.0	SZ4
192.168.12.0	255.255.254.0	0.0.0.0	SZ2
192.168.10.0	255.255.254.0	0.0.0.0	SZ1
192.168.18.0	255.255.254.0	0.0.0.0	SZ8
192.168.16.0	255.255.254.0	0.0.0.0	SZ6
10.2.0.0	255.255.0.0	0.0.0.0	WAN1
0.0.0.0	0.0.0.0	10.2.3.30	WAN1

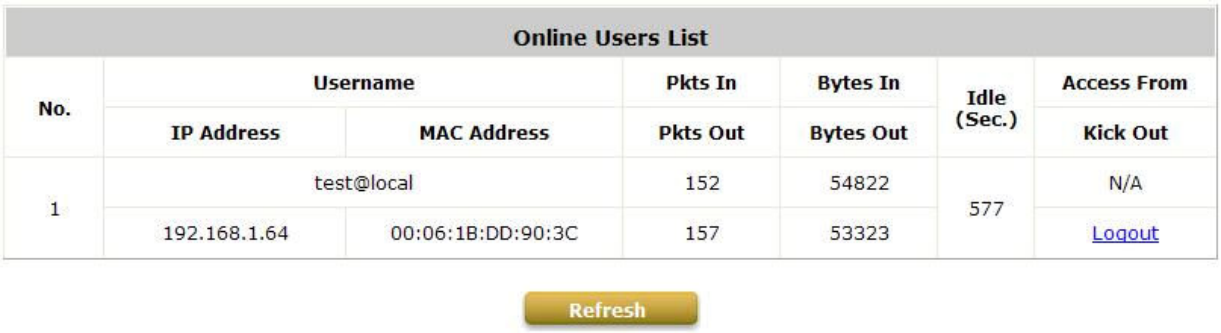
- **Policy 1~X:** Shows the information of each individual Policy.
- **Global Policy:** Shows the information of the Global Policy.
- **System:** Shows the information of the system administration.
  - **Destination:** The destination IP address of the device.
  - **Subnet Mask:** The Subnet Mask IP address of the port.
  - **Gateway**: The Gateway IP address of the port.

- **Interface:** The choice of interface network, including **WAN1**, **WAN2**, **Default**, or the named **Service Zones** to be applied for the traffic interface.

10.1.5 Online Users

View Online 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**, **Access From** and **Kick Out** will be shown. Administrators can force out a specific online user by clicking the hyperlink of **Kick Out** and check the user access AP status by clicking the hyperlink of the AP name for **Access From**. Click **Refresh** is to update the current users list.



Online Users List						
No.	Username		Pkts In	Bytes In	Idle (Sec.)	Access From
	IP Address	MAC Address	Pkts Out	Bytes Out		Kick Out
1	test@local		152	54822	577	N/A
	192.168.1.64	00:06:1B:DD:90:3C	157	53323		Logout

Refresh

10.1.6 User Logs

View User Logs, go to: ***Status >> User Logs***.

This page is used to check the traffic history of AMG-2102. The history of each day will be saved separately in the system 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 latest 2 calendar months.

Users Log	
Date	Size (Byte)
2009-07-30	65
2009-07-29	65
2009-07-28	65

On-demand Users Log	
Date	Size (Byte)
2009-07-30	105
2009-07-29	105
2009-07-28	105

Roaming Out User Log	
Date	Size (Byte)
2009-07-30	106
2009-07-29	106
2009-07-28	106

Roaming In User Log	
Date	Size (Byte)
2009-07-30	112
2009-07-29	112
2009-07-28	112

SIP Call Usage Log	
Date	Call Count
2009-07-30	0
2009-07-29	0
2009-07-28	0

Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
2009-07	5	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 **Notification Configuration** page, the system will automatically send out the history information to that specified email address.

- **Users Log**

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

Users Log 2008-04-14

Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out
2008-04-14 17:49:51	LOGIN	1@local	192.168.13.20	00:04:23:9A:6F:7B	0	0	0	0
2008-04-14 17:55:48	Force logout	1@local	192.168.13.20	00:04:23:9A:6F:7B	0	0	0	0

- **On-demand User Log**

  As shown in the following figure, each line is a on-demand user log record consisting of the following fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, 1st Login Expiration Time**, **Account Valid Through** and **Remark**, of user activities.

-

On-demand User Log 2007-11-26

Date	System Name	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	1st Login Expiration Time	Account Valid Through	Remark
2007-11-26 14:58:04	AirLive MV-2000S	Create_OD_User	8s3g	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 02:58:03	None	Plan 1
2007-11-26 14:58:10	AirLive MV-2000S	Create_OD_User	u96u	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 14:58:10	None	Plan 2
2007-11-26 14:58:15	AirLive MV-2000S	Create_OD_User	n4ka	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 14:58:15	None	Plan 3
2007-11-26 14:58:19	AirLive MV-2000S	Create_OD_User	bk35	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 02:58:19	None	Plan 4
2007-11-26 14:58:35	AirLive MV-2000S	Create_OD_User	4z4m	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 02:58:35	None	Plan 1
2007-11-26 14:58:40	AirLive MV-2000S	Create_OD_User	kkx5	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 14:58:39	None	Plan 2
2007-11-26 14:58:47	AirLive MV-2000S	Create_OD_User	6m5p	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 02:58:47	None	Plan 4
2007-11-26 15:01:52	AirLive MV-2000S	OD_User_Login	u96u	192.168.1.64	00:09:6B:CD:88:82	0	0	0	0	None	2007-11-28 15:01:52	None
2007-11-26 15:04:21	AirLive MV-2000S	OD_User_Logout	u96u	192.168.1.64	00:09:6B:CD:88:82	85	31812	89	12350	None	2007-11-28 15:01:52	Logout
2007-11-26 15:04:51	AirLive MV-2000S	OD_User_Login	bk35	192.168.1.64	00:09:6B:CD:88:82	0	0	0	0	None	2007-11-28 15:04:51	None
2007-11-26 15:07:02	AirLive MV-2000S	OD_User_Logout	bk35	192.168.1.64	00:09:6B:CD:88:82	4	252	7	360	None	2007-11-28 15:04:51	Logout

- **Roaming Out User Log**

  As shown in the following figure, each line is a roaming out traffic history record consisting of the following fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming Out Traffic History 2005-03-22

Date	Type	Name	NASID	NASIP	NASPort	UserMAC	sessionID	sessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **Roaming In User Log**

  As shown in the following figure, each line is a roaming in traffic history record consisting of the following fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming In Traffic History 2005-03-22													
Date	Type	Name	NASID	NASIP	NASPort	UserMAC	UserIP	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **SIP Call Usage Log**

  The log provides the login and logout activities of SIP clients (device and soft clients), such as Start Time, Caller, Callee and Duration (seconds).

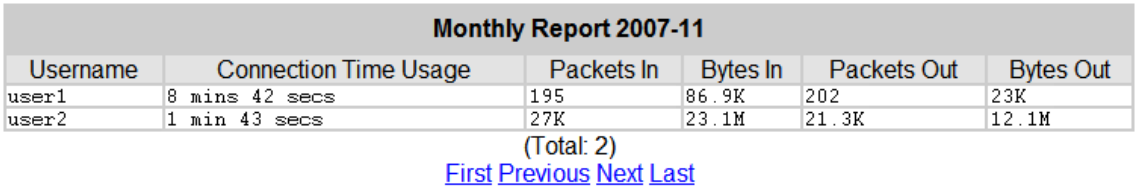
SIP Call Usage Log			
Start Time	Caller	Callee	Duration (seconds)

10.1.7 Local User Monthly Network Usage

View Local User Monthly Network Usage, go to: ***Status >> User Logs***.

- **Monthly Network Usage of Local User**

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

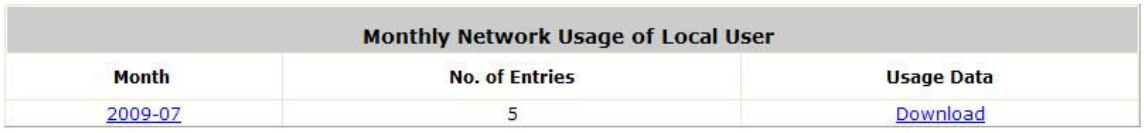


Monthly Report 2007-11					
Username	Connection Time Usage	Packets In	Bytes In	Packets Out	Bytes Out
user1	8 mins 42 secs	195	86.9K	202	23K
user2	1 min 43 secs	27K	23.1M	21.3K	12.1M

(Total: 2)
First Previous Next Last

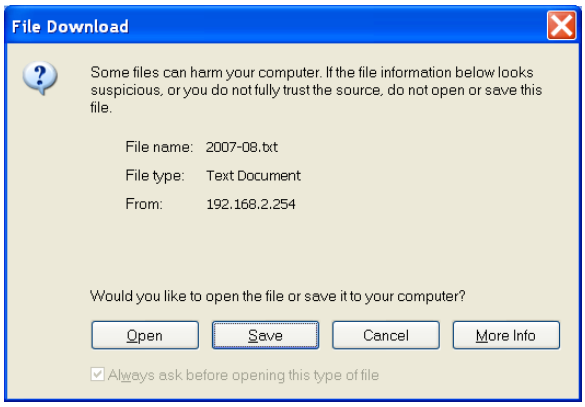
  - **Username:** Username of the local user account.
  - **Connection Time Usage:** The total time used by the user.
  - **Pkts In/ Pkts Out:** The total number of packets received and sent by the user.
  - **Bytes In/ Bytes Out:** The total number of bytes received and sent by the user.

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



Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
2009-07	5	Download

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


File Download
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.
File name: 2007-08.txt
File type: Text Document
From: 192.168.2.254
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

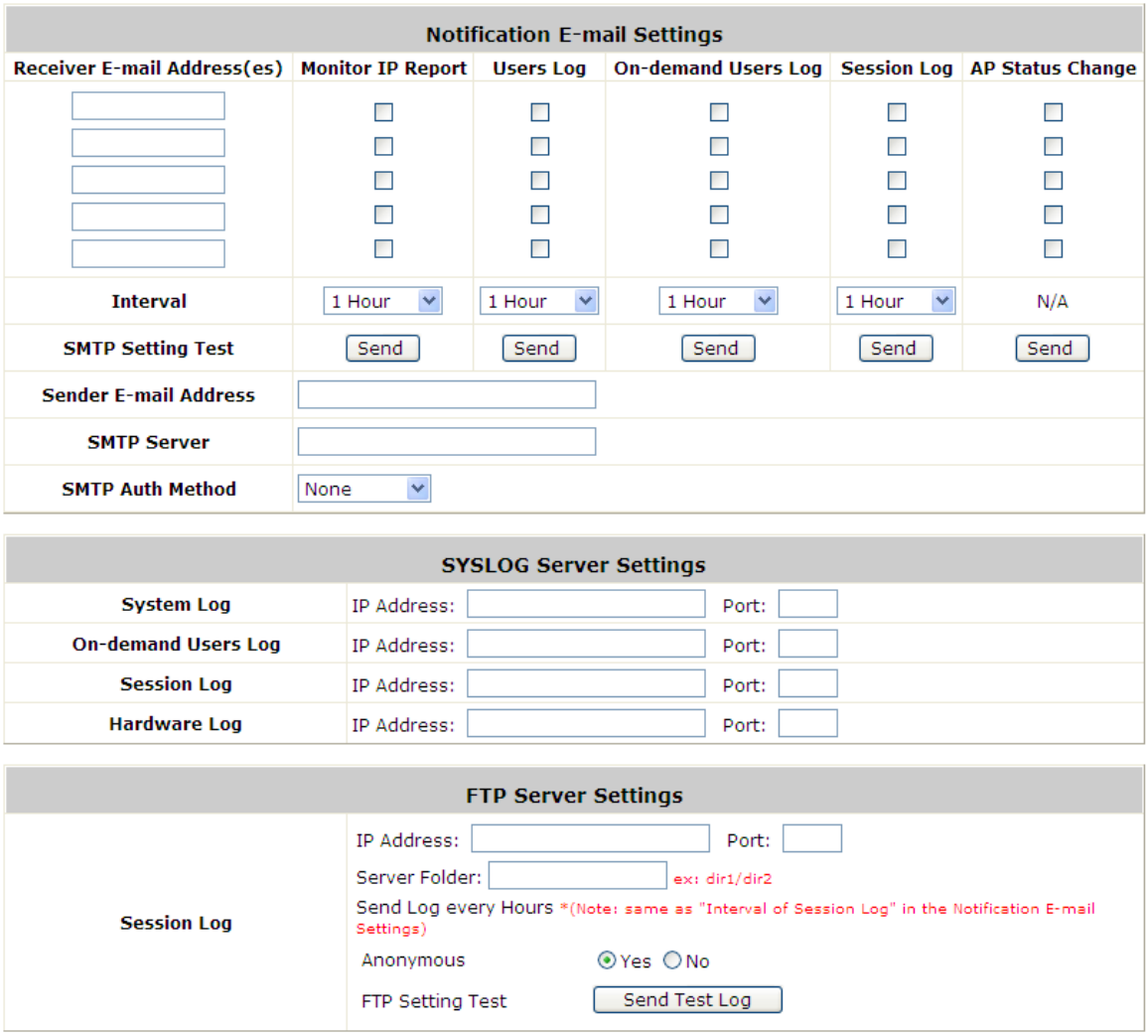
10.2 Notification

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

AMG-2102 can automatically send the notification of **Monitor IP Report**, **Users Log**, **On-demand Users Log**, **Session Log** and **AP Status Change** to more than one particular e-mail addresses. The notification of AP Status is triggered by the event when a managed AP becomes unreachable while the other types of emails are sent periodically in given intervals such as 1 hour. A trial email is provided by the system for validation.

In addition, the system supports recording of **System Log**, **On-demand Users Log**, **Session Log** and **Hardware Log** via external SYSLOG servers.

In addition, the Session Log can be sent to a specified FTP server. Enter the related information and select the desired items and then apply the settings.



10.2.1 E-Mail

- **Notification E-mail Settings:**
  - **Receiver Email Address(es):** The e-mail addresses can be set up to receive the notification. These are the receiver's e-mail addresses. There are different kinds of notification to be selected -- Monitor IP Report, Users Log, On-demand Users Log, Session Log and AP Status Change, and check which 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 can not be configured.

10.2.2 SYSLOG

- **SYSLOG Server Settings:** There are multiple types of Syslog supported: **System Log**, **On-demand User Log**, **Session Log** and **Hardware Log**. Enter the IP address and Port number to specify which and from where the report should be sent to.

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.

10.2.3 FTP

- **FTP Server Settings**

  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.

  - **IP Address/Port:** IP address and port number of FTP server.
  - **Server Folder:** The folder/directory on FTP server for upload.
  - **Send Log every hour:** The time interval for sending the log report.
  - **FTP Setting Test:** To test the FTP settings correct or not.

11. Virtual Private Network (VPN)

11.1 Local VPN

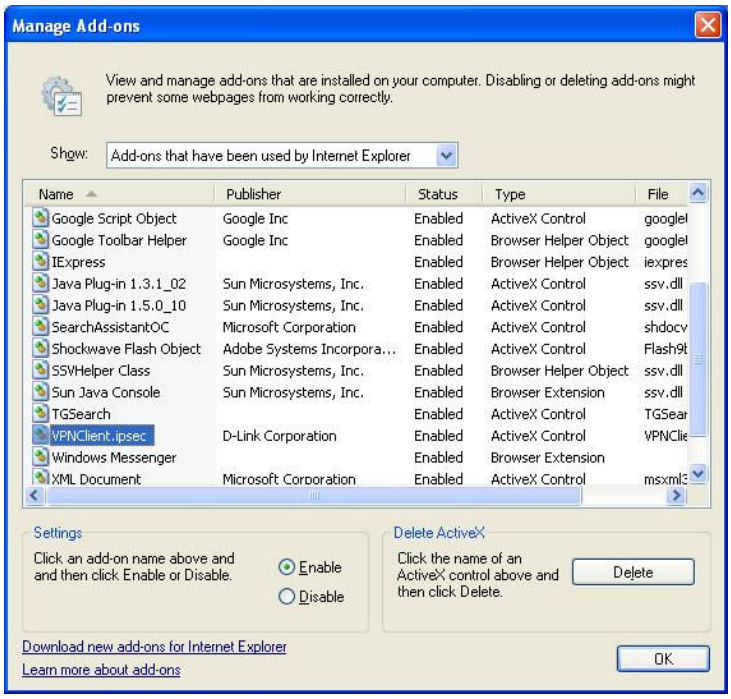
Configure Local VPN, go to: ***Users >> Authentication***.

The system is equipped with IPSec VPN feature. To utilize IPSec VPN supported by Microsoft Windows XP SP2 (with patch) and Windows 2000 operating systems, the system implements IPSec VPN tunneling technology between client's windows devices and the system itself regardless of wired or wireless network.

By pushing down ActiveX to the client's Windows device from the system, no extra client software is required to be installed except ActiveX, in which a so-called "clientless" IPSec VPN setting is then configured automatically. At the end of this setup, a build-in IPSec VPN feature will be enabled and ready to serve once it is launched for setup. The goal of this design is to eliminate the configuration difficulty from IPSec VPN users. At the client side, the IPSec VPN implementation of the system is based on ActiveX and the built-in IPSec VPN client of Windows OS.

- **ActiveX Component**

  The ActiveX is a software component running inside Internet Explorer. The ActiveX component can be checked by the following windows.



Windows Internet Explorer: From the **Tools** menu, click on **Internet Options**. Select the **Programs** tab and click ***Manage add-ons*** button to enter the **Manage add-ons** dialogue box, where you can see **VPNClient.ipsec** is enabled.

During the first-time login to AMG-2102 with Local VPN, Internet Explorer will ask clients to download an ActiveX component of IPSec VPN. Once this ActiveX component is downloaded, it will run in parallel with the "Login Success Page" after the page being brought up successfully. The ActiveX component helps set up individual IPSec VPN tunnels between clients and AMG-2102 and check the validity of IPSec VPN tunnels between them. If the connection is down, the ActiveX component will detect the broken link and decompose the IPSec tunnel. Once the IPSec VPN tunnel was built, all sent packets will be encrypted. Without connecting to the original IPSec VPN tunnel, a client has no alternative way to gain network connection beyond this. IPSec VPN feature supported by AMG-2102 directly solves possible data security leak problem between clients and the system via either wireless or wired connections without extra hardware or client software installed.

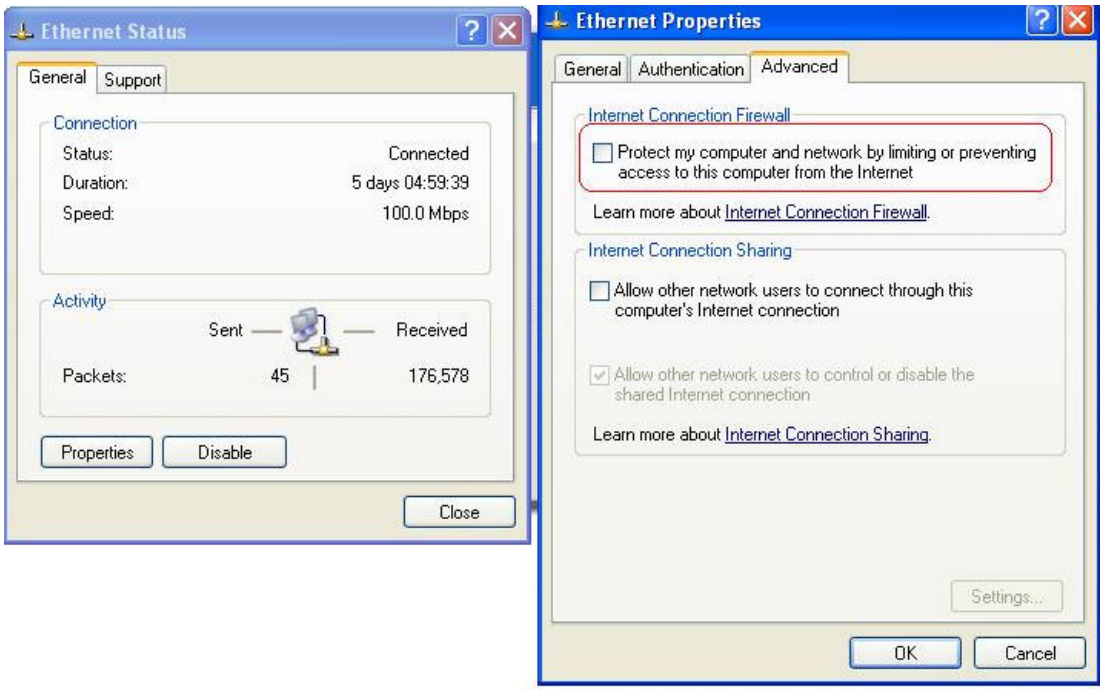
- ## Limitations

The limitation on the client side due to ActiveX and Windows OS includes:

- Internet Connection Firewall of Windows XP or Windows XP SP1 is not compatible with IPSec protocol. It shall be turned off to allow IPSec packets to pass through.
- Without patch, ICMP (Ping) and PORT command of FTP can not work in Windows XP SP2.
- The forced termination (through CTRL+ALT+DEL, Task Manager) of the Internet Explorer will stop the running of ActiveX. It causes that IPSec tunnel cannot be cleared properly at client device. A reboot of client device is needed to clear the IPSec tunnel.
- The crash of Windows Internet Explorer may cause the same result.

- ## Internet Connection Firewall

In Windows XP and Windows XP SP1, the Internet Connection Firewall is not compatible with IPSec. Internet Connection Firewall will drop packets from tunneling of IPSec VPN. Please **TURN OFF** Internet Connection Firewall feature or upgrade the Windows OS into Windows XP SP2.



- **ICMP and Active Mode FTP**

In Windows XP SP2 without patching by KB889527, it will drop ICMP packets from IPSec tunnel. This problem can be fixed by upgrading patch KB889527. Before enabling IPSec VPN function on client devices, please access the patch from Microsoft's web at http://support.microsoft.com/default.aspx?scid=kb;en-us;889527.

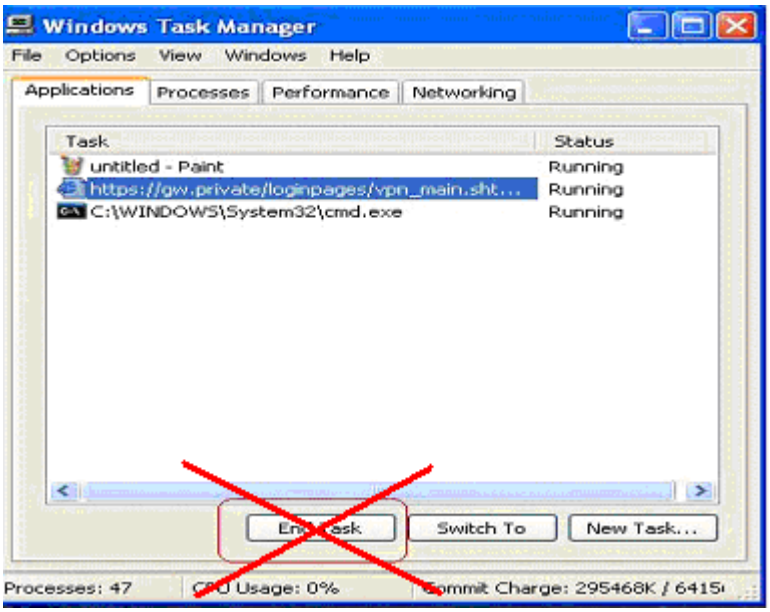
This patch also fixes the problem of supporting active mode FTP inside IPSec VPN tunnel of Windows XP SP2. Please **UPDATE** clients' Windows XP SP2 with this patch.

- **The Termination of ActiveX**

The ActiveX component for IPSec VPN is running in parallel with the web page of "Login Success". To ensure that the built-in IPSec VPN tunnel is always alive, unless clients decide to close the session and to disconnect from AMG-2102, **the following conditions or behaviors, which may cause the Internet Explorer to stop the ActiveX, should be avoided**.

(1) **The crash of Internet Explorer on running ActiveX.**
If it happens, please reboot the client computer. Once Windows service is resumed, go through the login process again.

(2) **Termination of the Internet Explorer Task from Windows Task Manager.**
Do NOT terminate this VPN task of Internet Explorer.



(3) **Execution of instructions given by the following Windows messages:**

- Close the Windows Internet Explorer.
- Click ***Logout*** on Login Success page.
- Click ***Back*** or ***Refresh*** of the same Internet Explorer browser page.
- Enter a new URL in the same Internet Explorer browser page.
- Open a URL from the other application (e.g. email of Outlook) that occupies this existing Internet Explorer.

*Click **Cancel** if you do not intend to stop the IPSec VPN connection.*

- **Non-supported OS and Browser**

Currently, Windows Internet Explorer is the only browser supported by the system. Windows XP and Windows 2000 are the only two supported OS along with this release.

- **FAQ**

(1) How to clean IPSec client?

ANS:

Open a command prompt window and type the commands as follows.

C:\> **cd %windir%\system32**
C:\> **Clean_IPSEC.bat**

Or

C:\> **cd %windir%\system32**
C:\> **ipsec2k.exe stop**

(2) How to remove ActiveX component in client's computer?

ANS:

① Uninstall and delete ActiveX component

② Close all Internet Explorer windows

③ Open a command prompt window and type the commands as follows
C:\> **cd %windir%\system32**
C:\> **regsvr32 /u VPNClient_1_5.ocx**
C:\> **del VPNClient_1_5.ocx**

(3) What can I do if unable establish IPSec connection for Windows XP SP1?

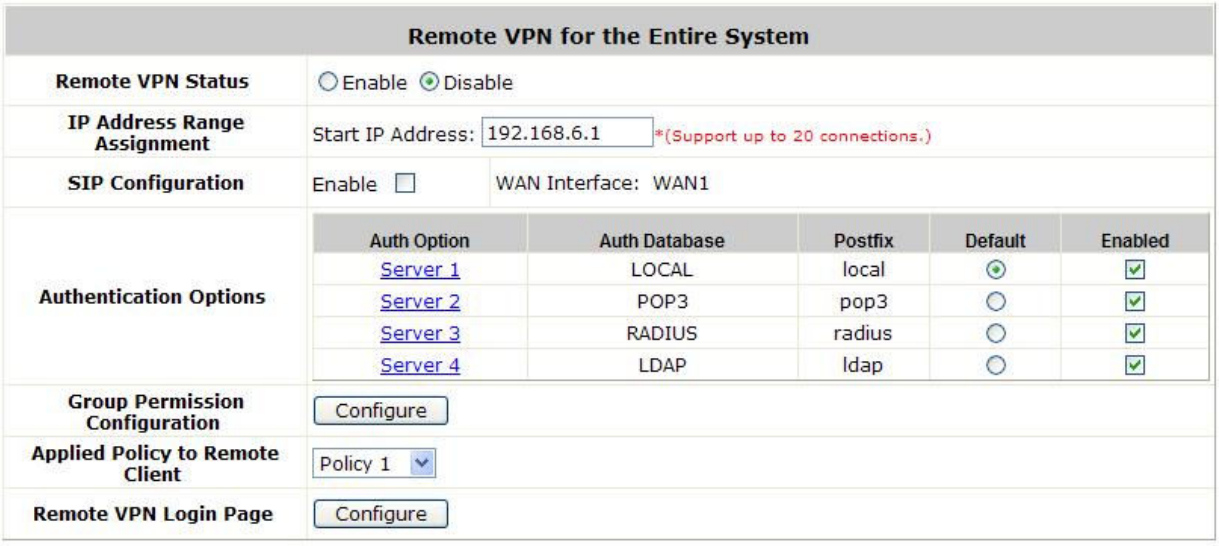
ANS:

Disable Windows XP firewall

11.2 Remote VPN

Configure Remote VPN, go to: ***Network >> VPN >>Remote VPN***.

AMG-2102 support **Remote VPN** for user login to system from remote area. After the user is login to system from the outside network of WAN, the user will feel that it is look like login to AMG-2102 under the service zone locally. They also can be applied Policy and are controlled by system to access the network.



All settings are look like the settings in Service Zone. It also can setup the **SIP WAN Interface**, **Authentication Options**, **Group Permission**, **Applied Policy** and customizable Login Page.

After Remote VPN is enabled, when you browse the home page with the WAN IP, you will get the Remote VPN login page, input the enabled authentication options username and password, then you will login success to system.

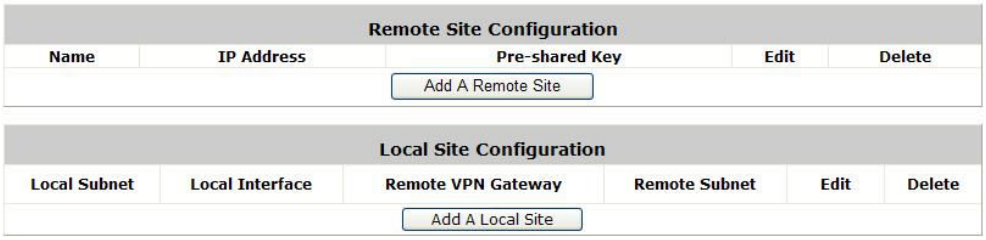
Caution:

After Remote VPN is enabled, the default home page will be the Remove VPN login page. If you want to access the WMI of AMG-2102, please input "login.shtml" after the WAN IP. For example, it may be: "http://10.2.3.4/login.shtnl"

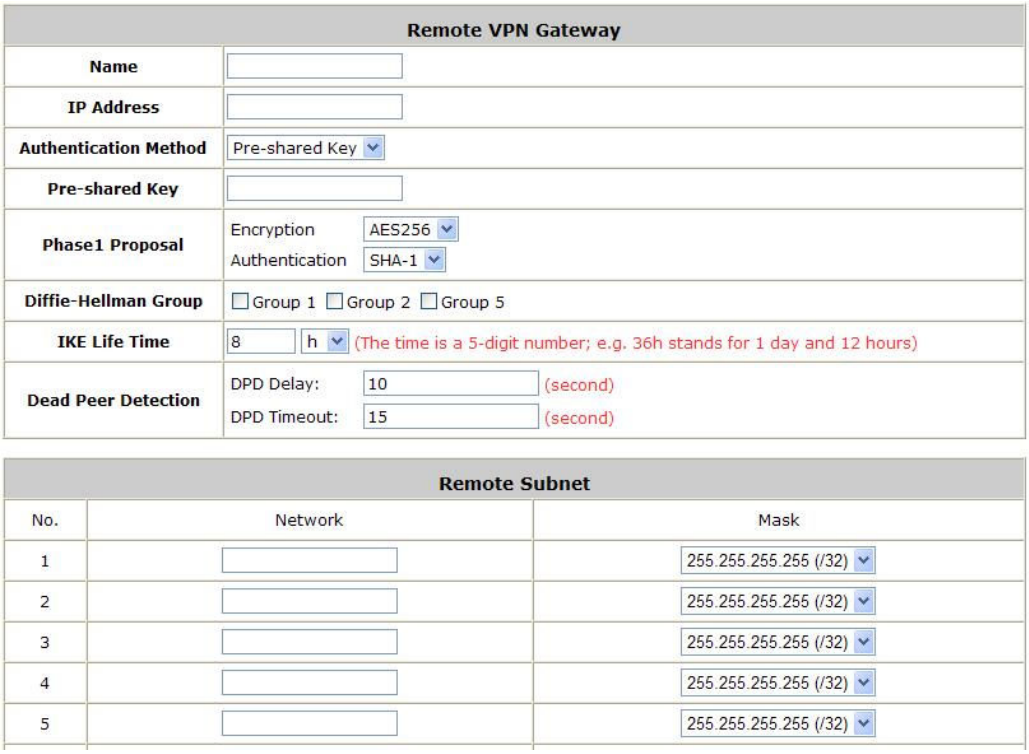
11.3 Site-to-Site VPN

Configure Site-to-Site VPN, go to: ***Network >> VPN >> Site-to-Site VPN***.

AMG-2102 support **Site-to-Site VPN** for more than 2 AMG-2102 create VPN tunnel to each other over the WAN network. For example, if there are 2 AMG-2102, you can create a VPN tunnel to let a subnet of one AMG-2102 to access the subnet of another AMG-2102.



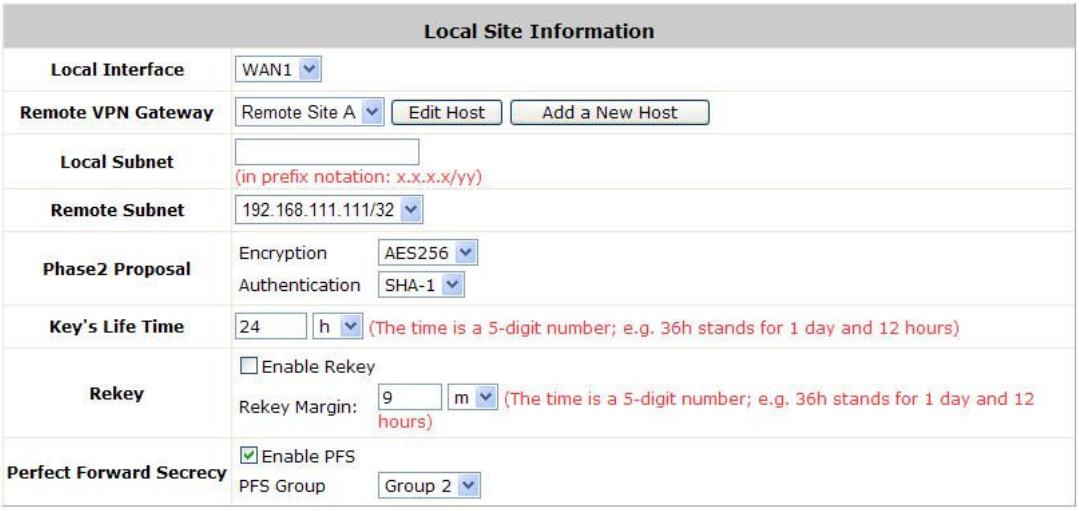
First, you need to add a Remote Site with remote subnet.



Caution:

The IPSec settings in both sites must be same.

And then create a Local Site with subnet for mapping to the remote site.



Such as "192.168.11.0/24" of AMG-2102_A **>>** "192.168.111.0/24" of AMG-2102_B, after the tunnel is created, the users within these two subnets can reach each other.

Caution:

You can create more than one VPN tunnel, but the IP segment mapping can not be overlap that same IP segment has more than one routing rule.

12. Customization of Portal Pages

12.1 Customizable Pages

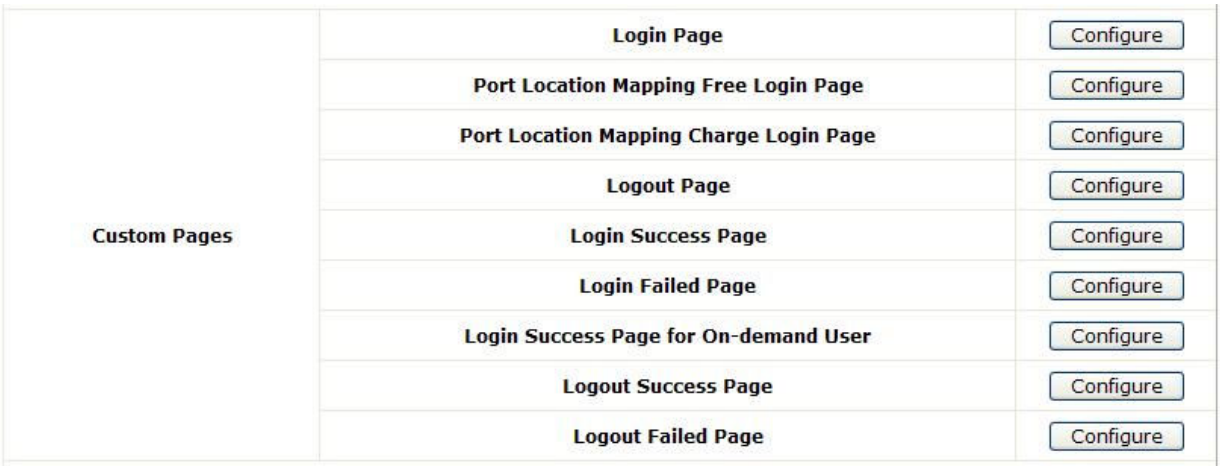
Configure Customizable Pages, go to: ***System >> Service Zones***.

There are several users' login and logout pages for each service zone that can be customized by administrators.

Go to System Configuration **>>** Service Zone **>>** Authentication Settings **>>** Custom Pages.

Click the button of ***Configure***, the setup page will appear.

Click the radio button of page selections to have further configuration.



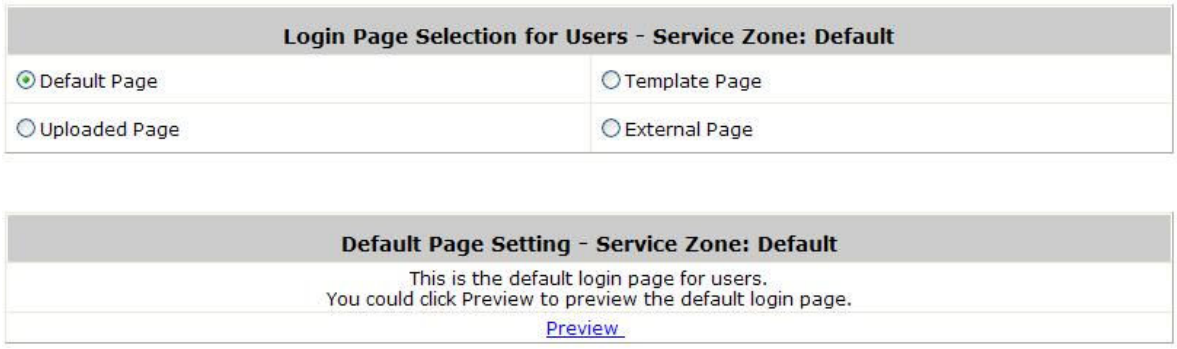
Now, let us discus two examples: ***Login Page*** and ***Logout Page***

12.2 Loading a Customized Login Page

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

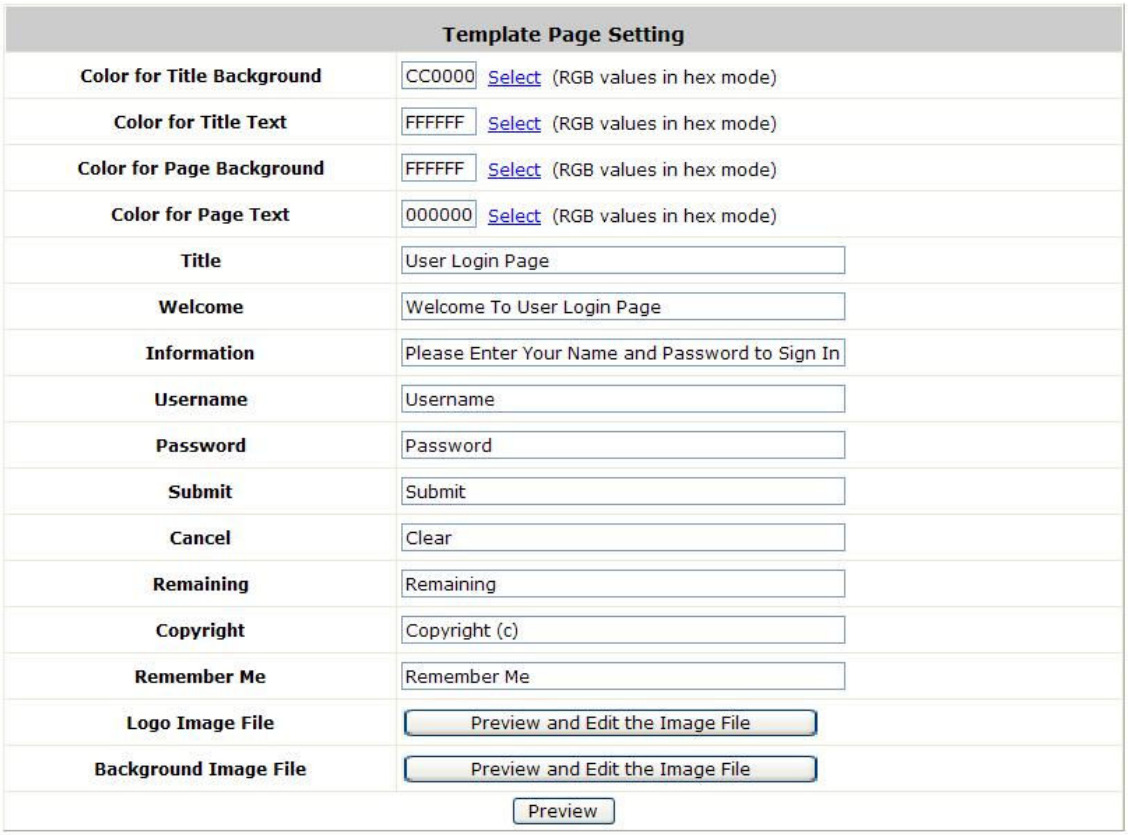
- *Custom Pages >> Login Page >>* ***Default Page***

  Choose Default Page to use the default login page.



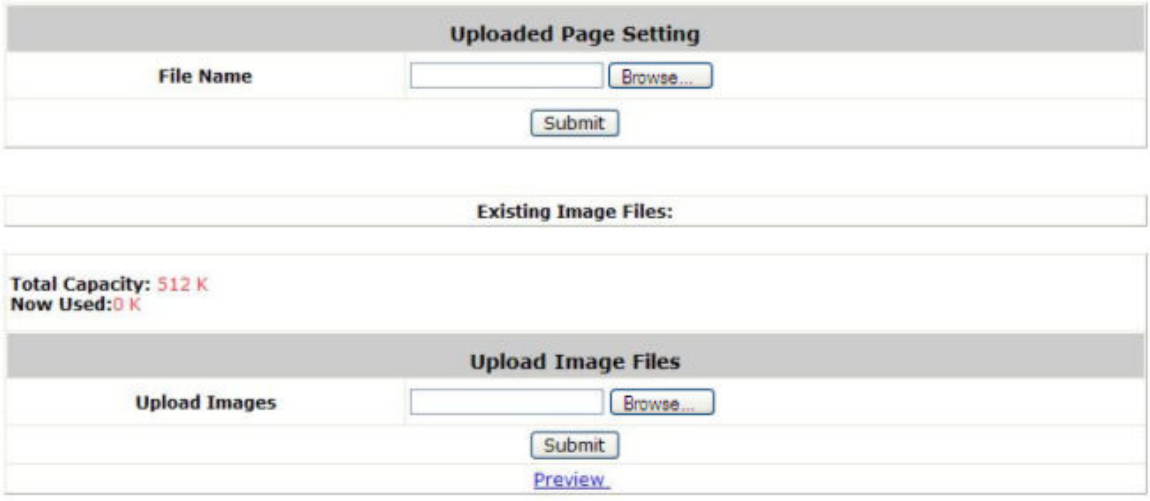
- *Custom Pages >> Login Page >>* ***Template Page***

  Choose Template Page to make a customized login page. Click Select to pick up a color and then fill in all of the blanks. You can also upload a background image file for your template. Click ***Preview*** to see the result first.



- *Custom Pages >> Login Page >>* ***Uploaded Page***

  Choose Uploaded Page and upload a login page.



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

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

And if the user-defined login page includes an image file, the image file path in the HTML code must be the image file to be uploaded.

Remote VPN : <img src=images/xx.jpg">

Default Service Zone: <img src=images0/xx.jpg">

Service Zone 1 : <img src=images1/xx.jpg">

Service Zone 2 : <img src=images2/xx.jpg">

Service Zone 3 : <img src=images3/xx.jpg">

Service Zone 4 : <img src=images4/xx.jpg">

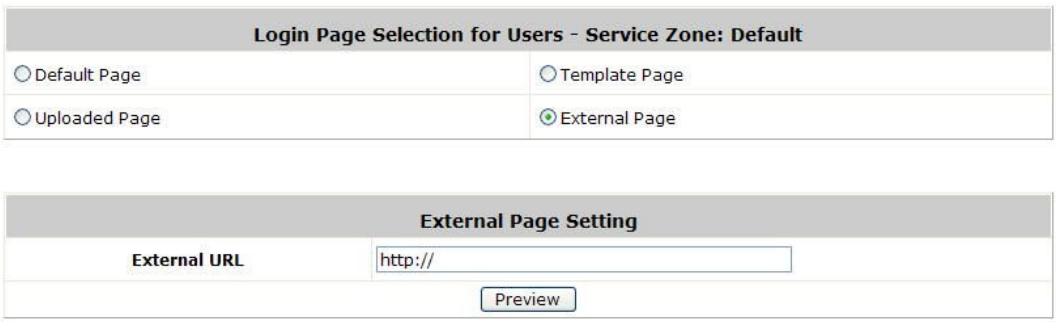
Click the ***Browse*** button to select the file to upload. Then click ***Submit*** to complete the upload process.

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

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

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

- *Custom Pages >> Login Pages >>* ***External Page***



Choose the ***External Page*** selection and get the login page from a designated website. In the External Page Setting, enter the URL of the external login page and then click ***Apply***.

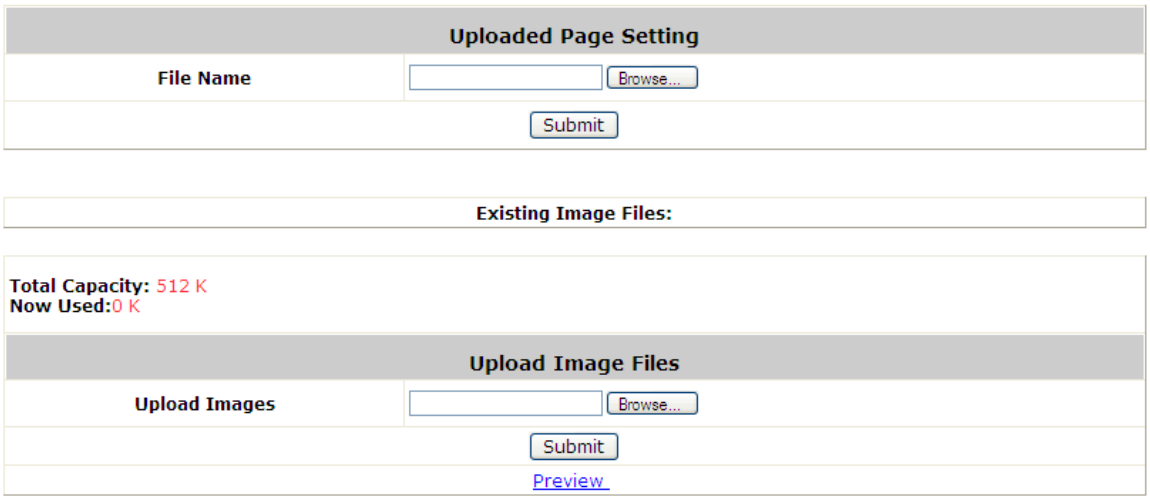
After applying the setting, the new login page can be previewed by clicking ***Preview*** button at the bottom of this page.

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

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

12.3 Load a Customized Logout Page

- *Custom Pages* >> ***Logout Page***
  The administrator can apply their own logout page in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page >> Uploaded Page" instructions for more details.



Note:

The different part is the HTML code of the user-defined logout interface must include the following HTML code that the user can enter the username and password. After the upload is completed, the customized logout page can be previewed by clicking **Preview** at the bottom of this page. If restore to factory default setting is needed for the logout interface, click the "**Use Default Page"** button.

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

13. Payment Gateways

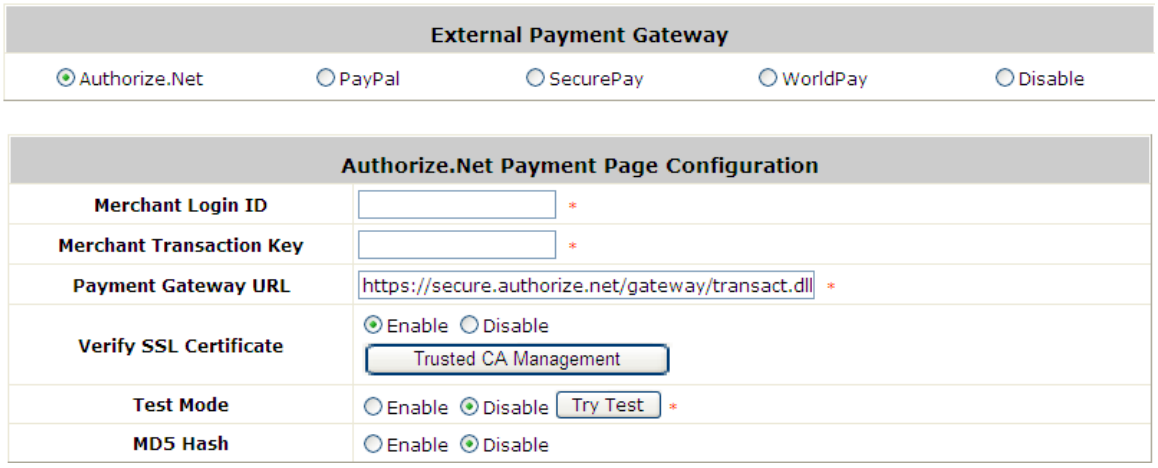
13.1 Payments via Authorize.Net

Configure Payments via Authorize.Net, go to:

Users >> Authentication >> On-demand>> 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.

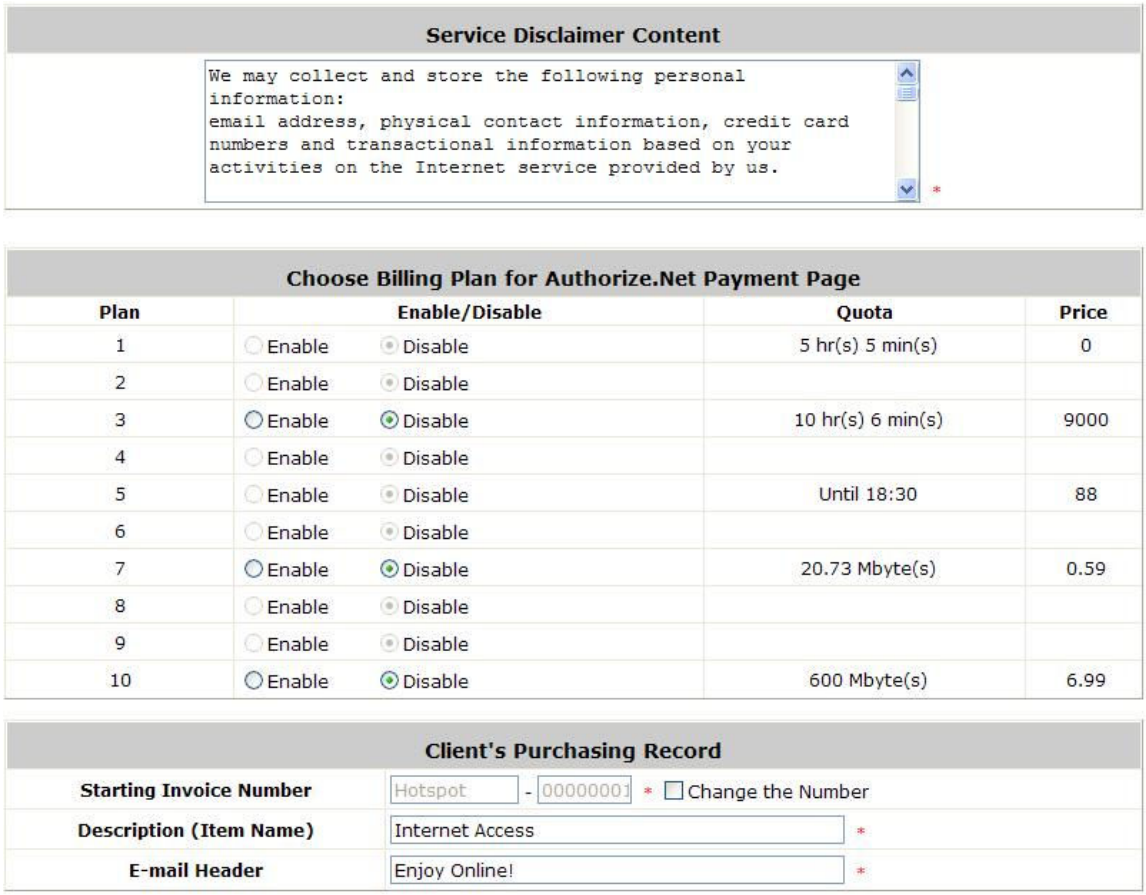
Verify SSL Certificate: This is to help protect the system from accessing a website other than Authorize.Net.

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

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

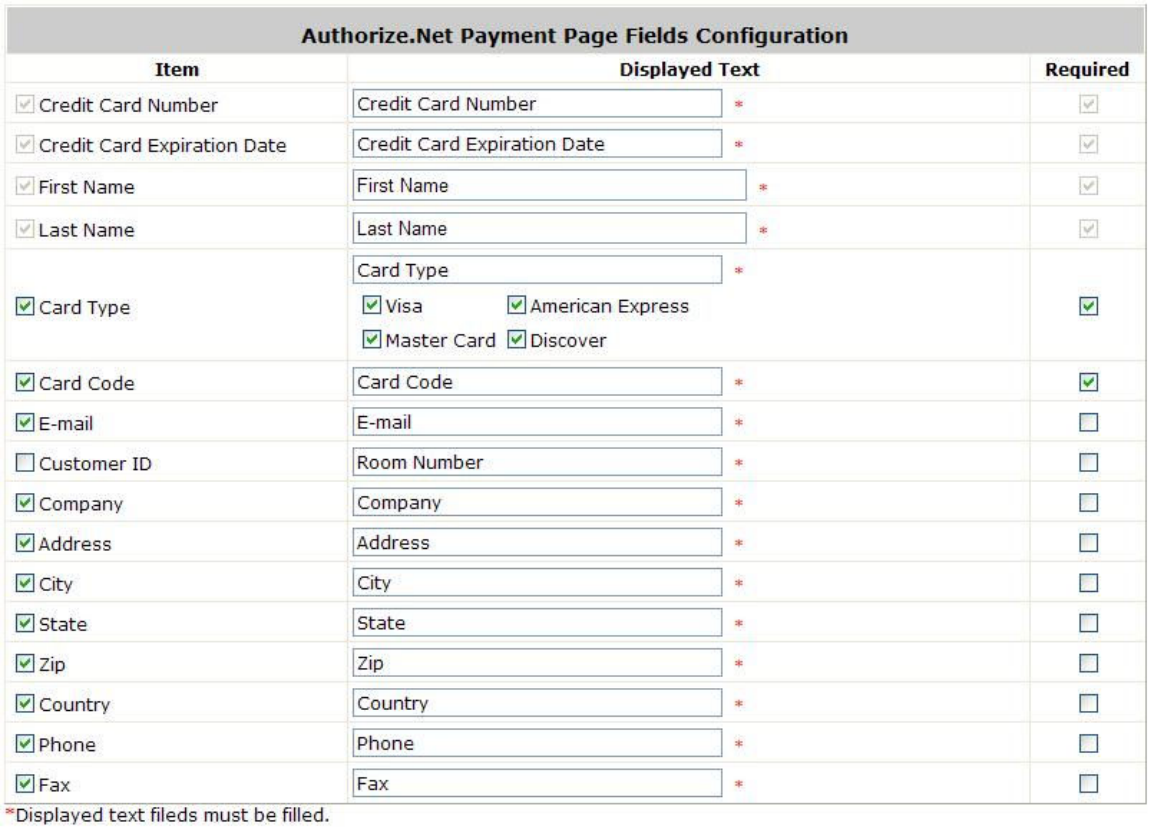
Plan	Enable/Disable		Quota	Price
1	Enable	Disable	5 hr(s) 5 min(s)	0
2	Enable	Disable		
3	Enable	Disable	10 hr(s) 6 min(s)	9000
4	Enable	Disable		
5	Enable	Disable	Until 18:30	88
6	Enable	Disable		
7	Enable	Disable	20.73 Mbyte(s)	0.59
8	Enable	Disable		
9	Enable	Disable		
10	Enable	Disable	600 Mbyte(s)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

Client's Purchasing Record

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:** Month and year 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 (found either on the front of the card at the end of the credit card number or on the back of the card).
- **E-mail:** An email address may be provided along with the billing information of a transaction. This is the customer's email address and should contain an @ symbol.
- **Customer ID:** This is an internal identifier for a customer that may be associated with the billing information of a transaction. This field may contain any 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 value.
- **Phone:** A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all 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.

13.2 Payments via PayPal

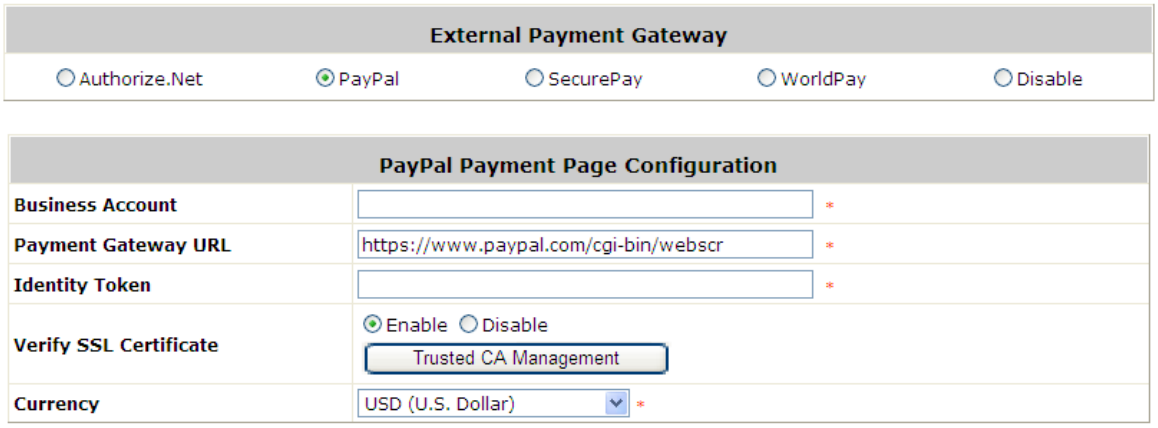
Configure Payments via PayPal, go to:

User >> Authentication >> On-demand>> 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.

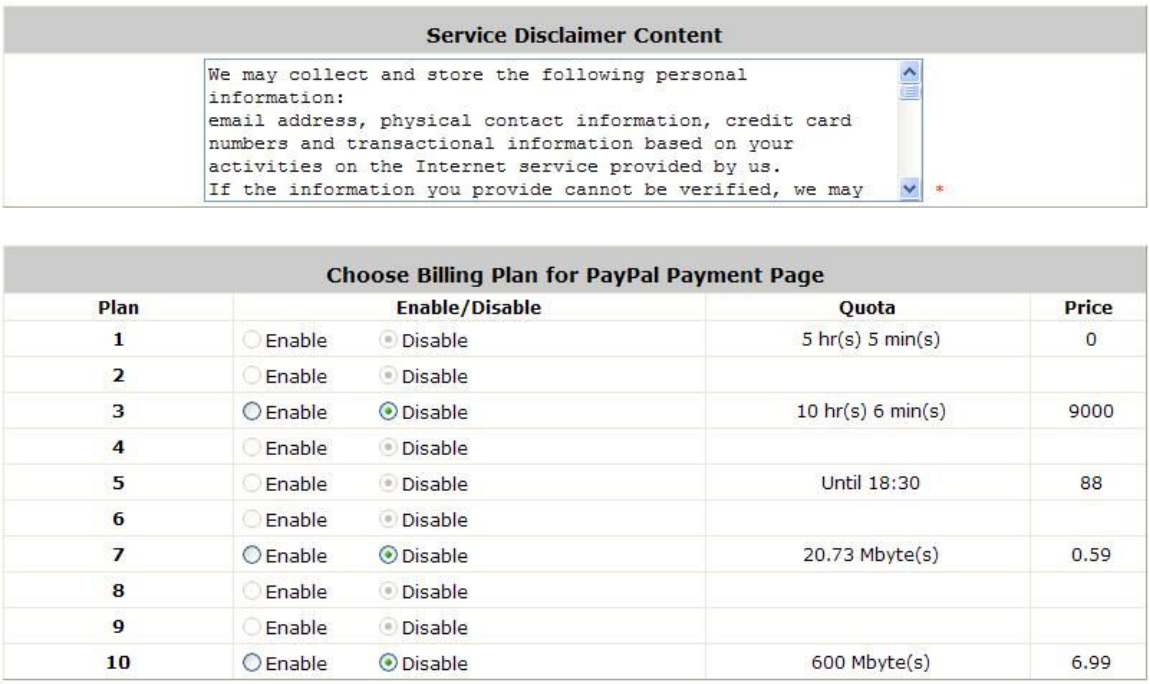
Payment Gateway URL: The default website address to post all transaction data.

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 / Billing Configuration for Payment Page**



Service Disclaimer Content

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

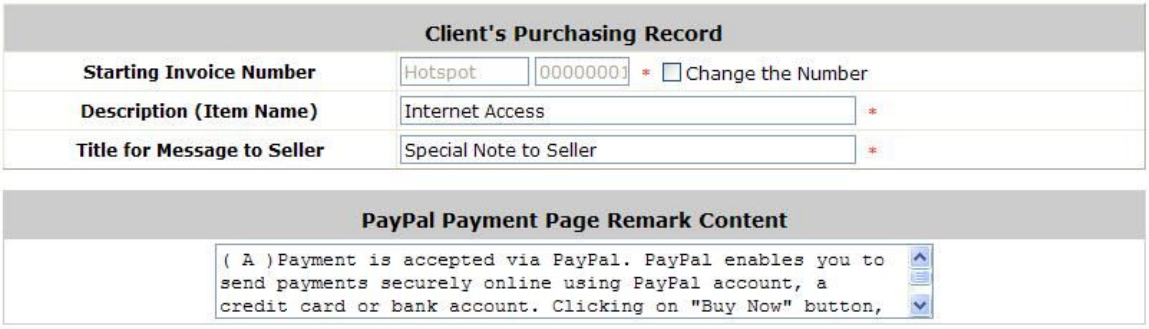
Choose Billing Plan for PayPal Payment Page

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

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	Hotspot 00000001 * ☐ Change the Number
Description (Item Name)	Internet Access *
Title for Message to Seller	Special Note to Seller *

PayPal Payment Page Remark Content

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

Client's Purchasing Record:

Invoice Number: An invoice number may be provided as additional information against a

transaction. This is a reference field that may contain any kind of information.

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

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

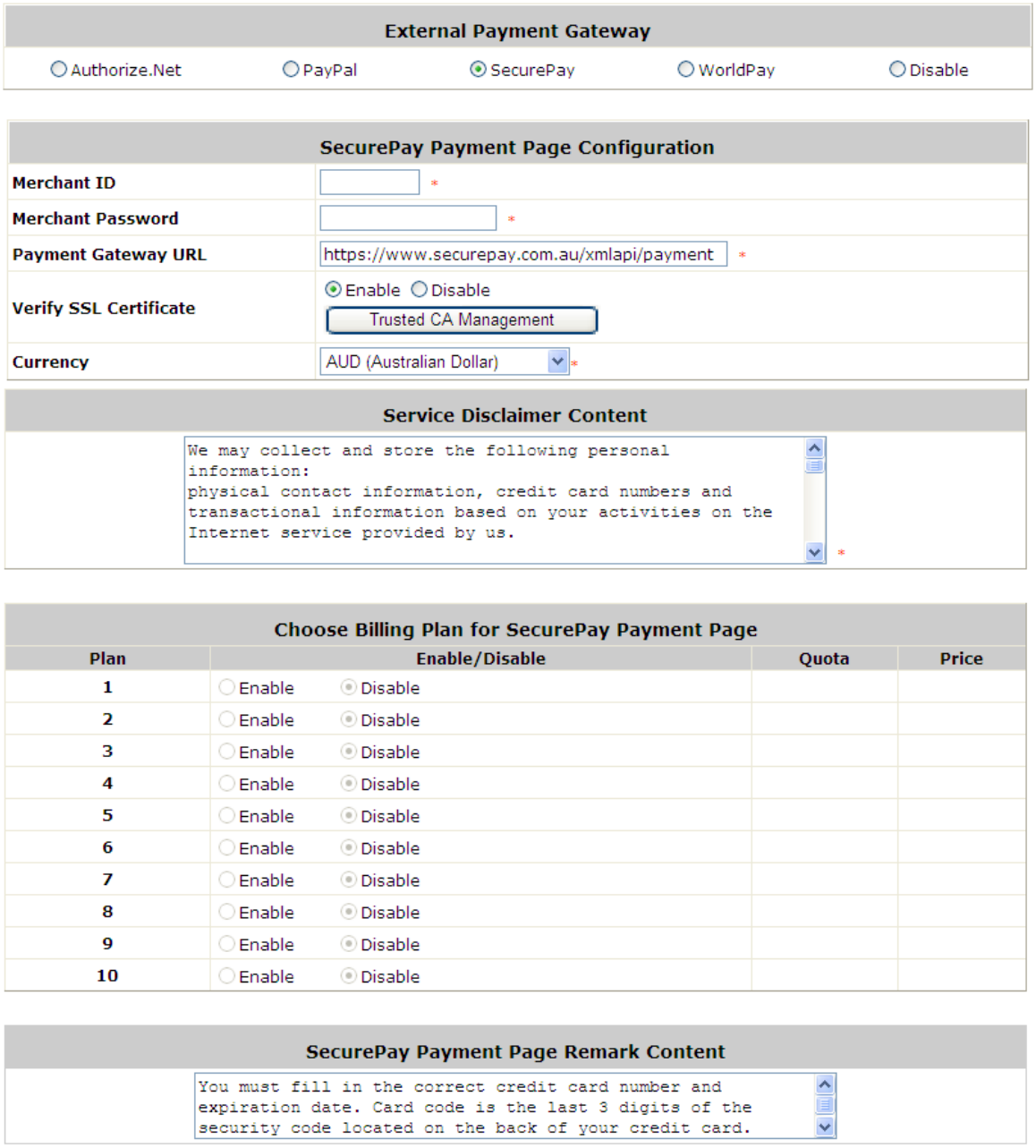
PayPal Payment Page Remark Content: The message content will be displayed as a special notice to end customers in the page of "Rate Plan". For example, it can describe the cautions for making a payment via PayPal.

13.3 Payments via SecurePay

Configure Payments via SecurePay, go to:

Users >> Authentication >> On-demand>> 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.



- **Payment Page Configuration**

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

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

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

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

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

- **Service Disclaimer Content**

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

- **SecurePay Payment Page Billing Configuration**

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

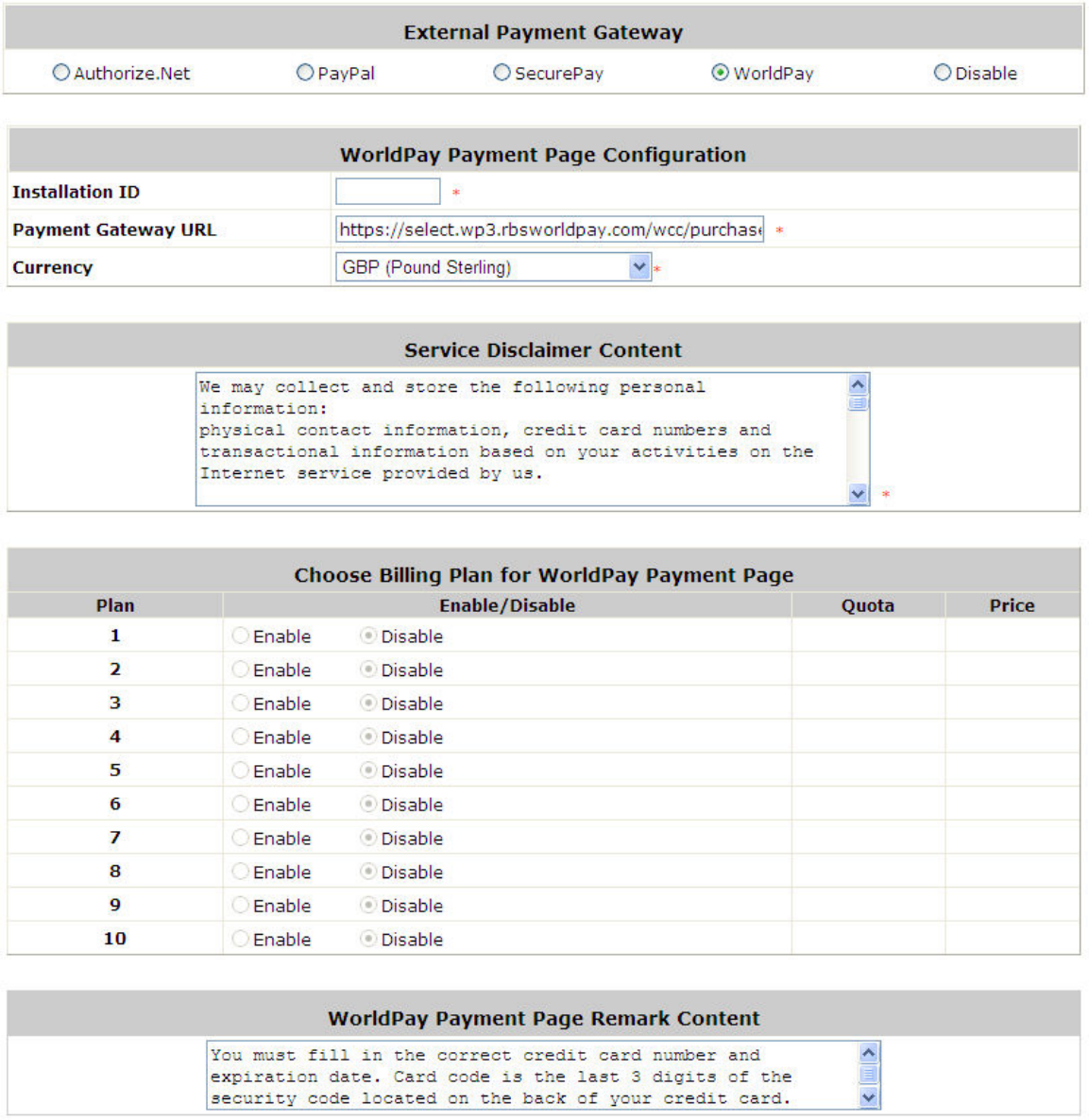
- **SecurePay Payment Page Remark Content**

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

13.4 Payments via World Pay

Configure Payments via WorldPay, go to:

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



- **WorldPay Payment Page Configuration**

  Installation ID: The ID of being associated with the Business 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.

- **SecurePay Payment Page Billing Configuration**

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

- **SecurePay Payment Page Remark Content**

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

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 center >> 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.

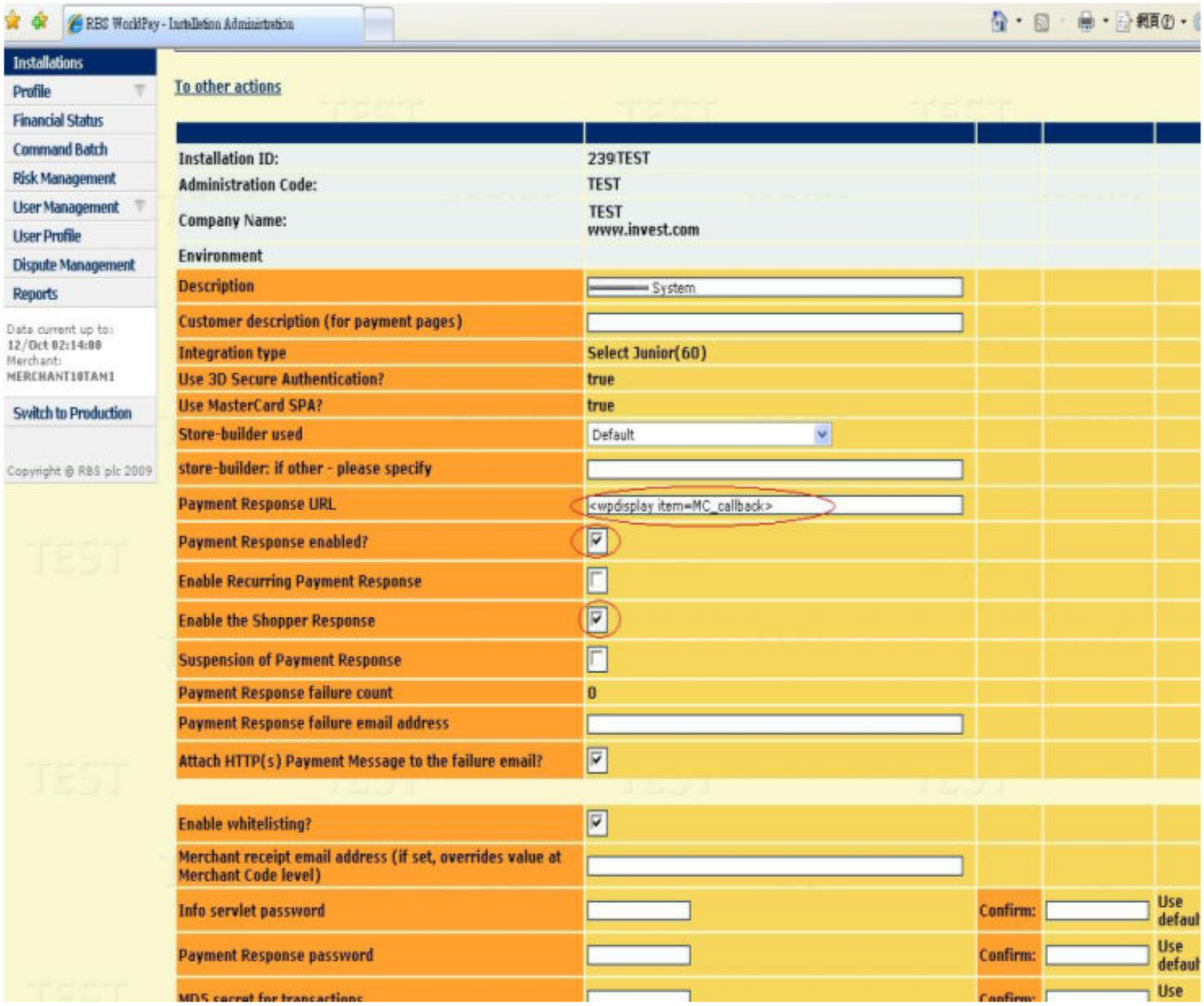
- Installation ID: 239xxx

STEP④. Check the Enable Payment Response checkbox.

STEP⑤. Enter the Payment Response URL.

- URL : <wpdisplay item=MC_callback>

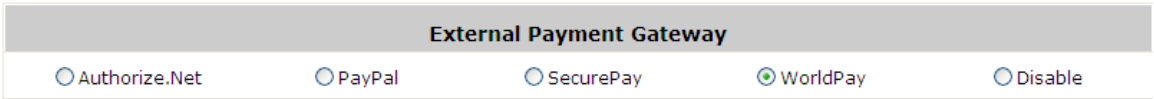
STEP⑥. Check the Enable the Shopper Response.

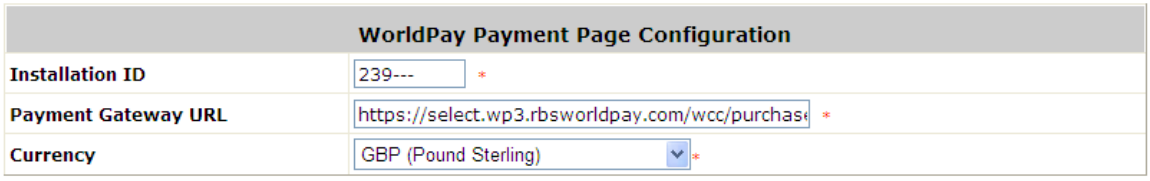


STEP⑦. Select the Save Changes button

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

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





Note:

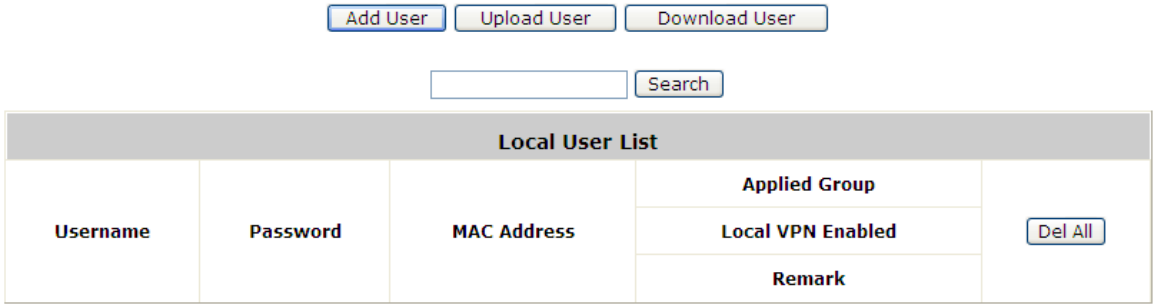
The WAN IP of gateway must be real IP.

14. Additional Applications

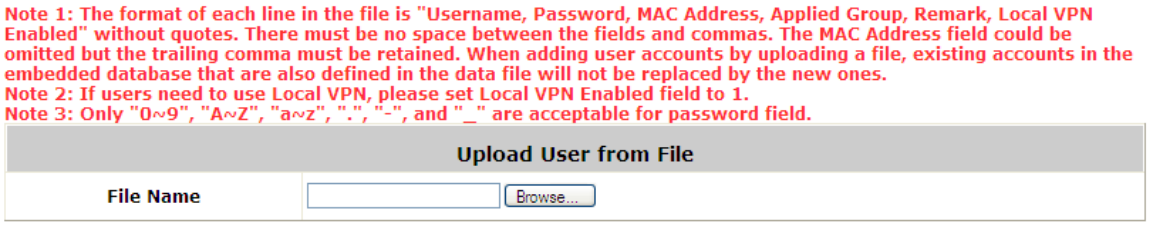
14.1 Upload / Download Local Users Accounts

Configure Upload / Download Local Users Accounts, go to:

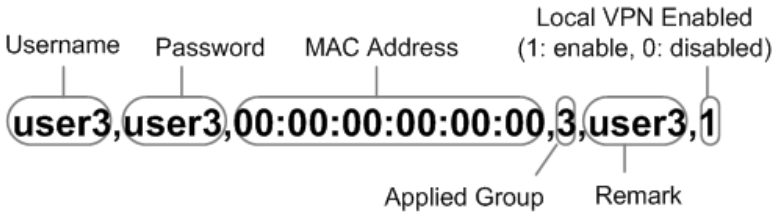
Users >> Authentication >> Local-Server1~4 >> Configure >> Local User List.



- **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 built-in user account information and then save it on disk.

Download User to File			
Username	Password	MAC Address	Applied Group
			Local VPN Enabled
			Remark
1	1		0
			0
2	2		0
			0

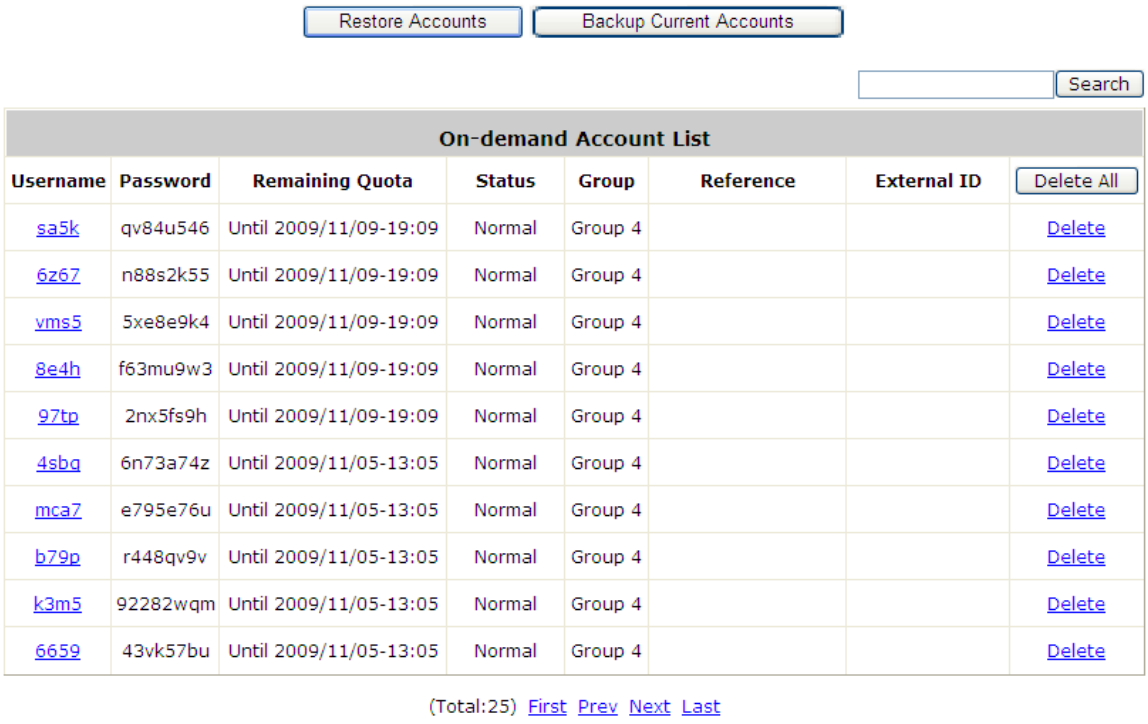
Download

14.2 Backup and Restore On-demand Users Accounts

Configure Backup / Restore On-demand Users Accounts, go to:

Users >> Authentication >> On-demand User >> On-demand Account List.

- **Backup Current Accounts:** Use this function to create a .txt file with all current user account information and then save it on disk.
- **Restore Accounts:** After the current user accounts have backup, you can restore all these accounts to another system. Click **Restore Accounts** to enter the **Restore On-demand User Account** interface. Click the ***Browse*** button to select the text file for restore the user accounts, and then click **Submit** to complete the restore process.



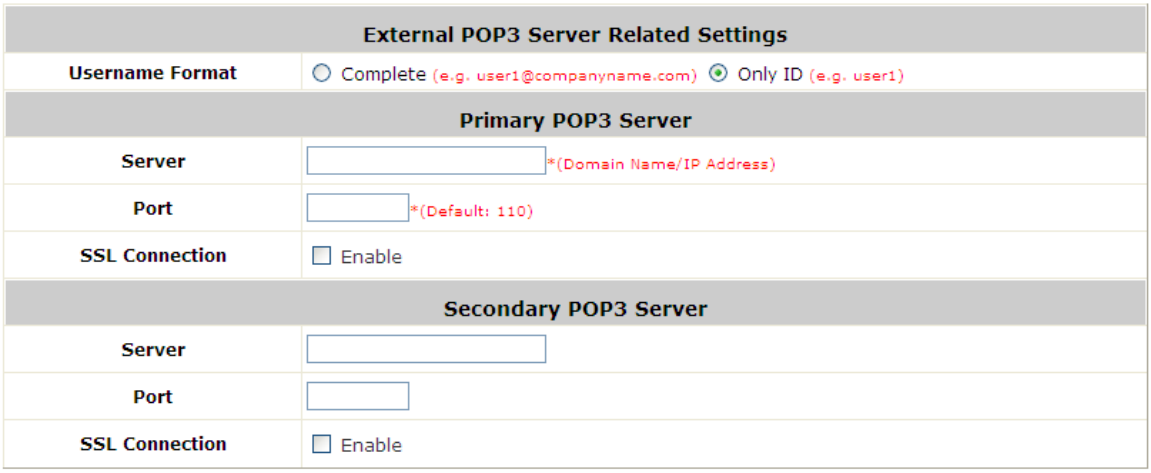
14.3 POP3 login with complete name format

Configure POP3 login with complete name format, go to:

Users >> Authentication >> POP3-Server1~4 >> Configure.

For POP3 authentication, there have 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 POP3 server for authentication. When **Only ID** option is checked, only the username will be transferred to the external server for authentication.



14.4 RADIUS Advance settings

Configure RADIUS Advance settings, go to:

Users >> Authentication >> RADIUS-Server1~4 >> Configure.

- Complete Name vs. Only ID

For RADIUS authentication, there have 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

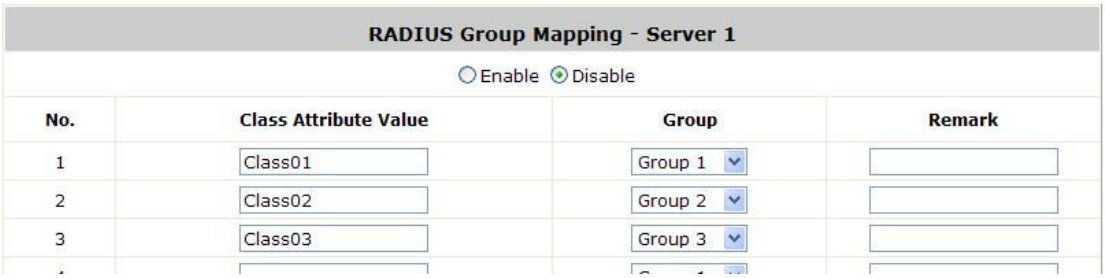
System will send this value to the external RADIUS server, if the external RADIUS server needs this.

- NAS Port Type

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

- Class-Group Mapping

This function is to assign a *Group* 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 Group.



14.5 LDAP Advance settings - Attribute-Group Mapping

Configure LDAP - Attribute-Group Mapping, go to:

Users >> Authentication>> LDAP-Server1~4 >> Configure.

This function is to assign a *Group* to a LDAP attribute sent from the LDAP server. When the clients classified by LDAP attributes log into the system via the LDAP server, each client will be mapped to its assigned Group. To get and show the attribute name and value from the configured LDAP server, enter *Username* and *Password* and click ***Show Attribute***. Then, the table of attribute will be displayed. Enter the *Attribute Name* and *Attribute Value* chosen from the attribute table, and select a *Group* from the drop-down list box.

Attribute Name	Attriubute Value
CN	USER01
C	TW

LDAP Group Mapping - Server 4

○ Enable ◉ Disable

No.	LDAP Attribute Name	LDAP Attribute Value	Group	Remark
1	CN	USER01	Group 1	
2	C	TW	Group 2	

14.6 NT Transparent Login

Configure NT Transparent Login, go to:

Users >> Authentication >> NT Domain-Server1~4 >> Configure.

This function refers to Windows NT Domain single sign-on. In Windows NT or AD environment, users must need to login to Domain first, and then they will be assigned the access right in this domain.

On the other hand, user also need to login to AMG-2102 to get the network access right. So user must login twice for network access right and domain resource access right.

So, this function is use to combine these by a single user login. Users only need to login once, and then they will be assigned the access right in this domain and network access right from AMG-2102.

When *Transparent Login* is enabled, clients will log into the system automatically after they have logged into the NT domain.

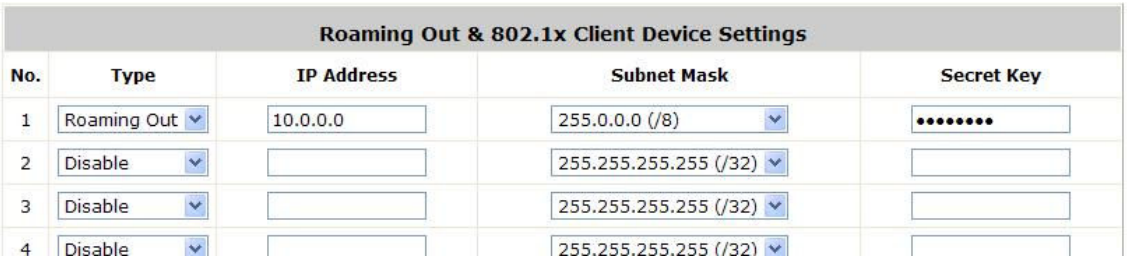
Enable Local VPN: Check the checkbox to enable local VPN under transparent login mode. When enabled, local VPN connection will be automatically created under transparent login mode. For the local VPN to work under transparent login mode, however, it requires support from Windows Server – need to install additional logon script on Windows Server.

14.7 Roaming Out

Configure Roaming Out, go to: ***Users >> Authentication >> Local-Server1~4 >> Configure >> Local User List >> Roaming Out & 802.1X Client Device Settings***.

In sometime, AMG-2102 can act as a RADIUS server for Roaming Out 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 this function will be available to define the authorized device with IP address, Subnet Mask, and Secret Key.



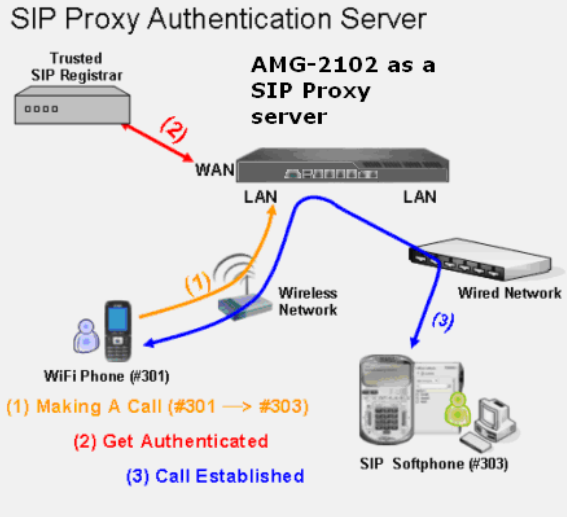
Click the hyperlink ***Roaming Out & 802.1x Client Device Settings*** to enter the ***Roaming Out & 802.1x Client Device Settings*** interface. Choose **Roaming Out** and key in the Roaming Out client's IP address and network mask and then click ***Apply*** to complete the settings.

In the other system, such as another AMG-2102, setup it's RADIUS server to this AMG-2102 with same postfix, then the local user in this AMG-2102 can login success from another AMG-2102 by RADIUS authentication.

14.8 SIP Proxy

SIP (Session Initiation Protocol) is a protocol for making real-time calls over IP network. Currently, most of the SIP extensions address audio communication. AMG-2102 can act like a SIP Proxy Server, it forwards end point' requests and responses. In other words, SIP Proxy server needs to log in the trusted registrar to verify identities of 2 clients. After enabling SIP proxy server, all SIP traffic pass through NAT with a selective but fixed WAN interface.

In this example, client extension #301 is trying to call #303. AMG-2102 asks an external trusted SIP registrar to verify both identities. After SIP registrar responds with a YES, call is established through AMG-2102.



The system provides SIP proxy for SIP clients (devices or soft clients) pass through NAT. After enable SIP proxy server, all SIP traffic can pass through NAT with a selective but fixed WAN interface. If the SIP Registrar settings in SIP client is same as the system setting, when the client try to access the SIP Registrar, system will let this client login automatically and all SIP traffic can pass through.

Configure SIP Trusted Registrar, go to: ***Users >> Authentication>> SIP***.

Authentication Server - SIP		
	IP Address	Remark
Trusted Registrar		
Group	Group 1 Group selection applied to clients login with SIP authentication.	

- **SIP:** SIP authentication supports 4 Trusted SIP Registrar.
- **IP Address:** The IP address of the Trusted SIP Registrar.
- **Remark:** The administrator can enter extra information in this field for remark.
- **Group:** A Group option can be applied to the clients who login with SIP Authentication. Be noted that the specific route of the applied Policy for the selected Group cannot conflict with the assigned WAN interface for SIP authentication.

SIP Interface Configuration

Configure SIP WAN Interface, go to: ***System Configuration >> Service Zones***.

The system provides SIP proxy functionality, which allows SIP clients to pass through NAT. When enabled, all SIP traffic can pass through NAT via a fixed WAN interface. The policy route setting of SIP Authentication must be configured carefully because it must cooperate with the fixed WAN interface for SIP authentication.

SIP Transparent Proxy can be activated in both NAT and Router mode. SIP Authentication must support in either mode. For users logging in through SIP authentication, a group can be chosen to govern SIP traffic. The policy's login schedule profile will be ignored for SIP authentication. Specific route and firewall rules of the chosen group will be applied to SIP traffic.

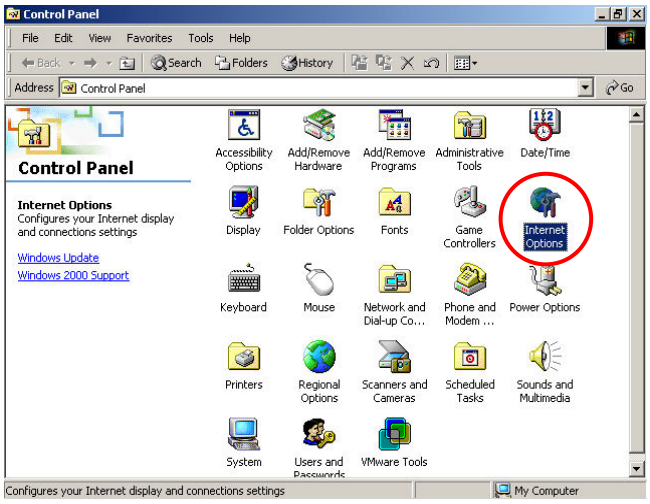
Appendix A. Network Configuration on PC & User Login

▪ Network Configuration on PC

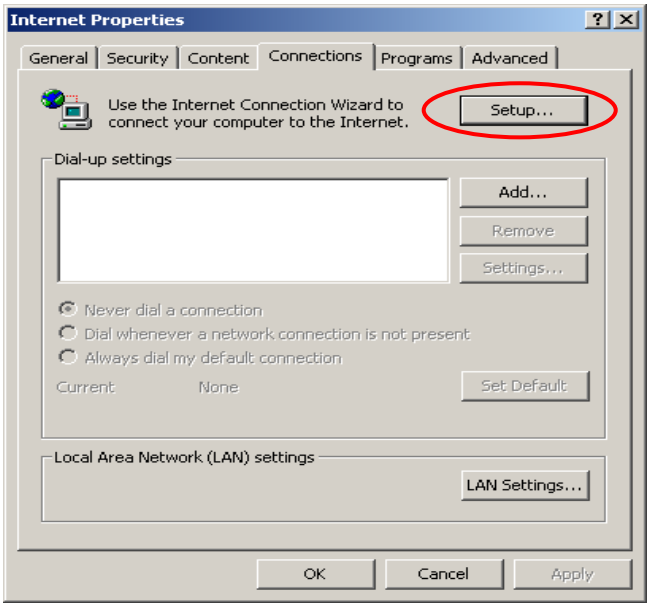
After AMG-2102 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**
  - **Windows 9x/2000**

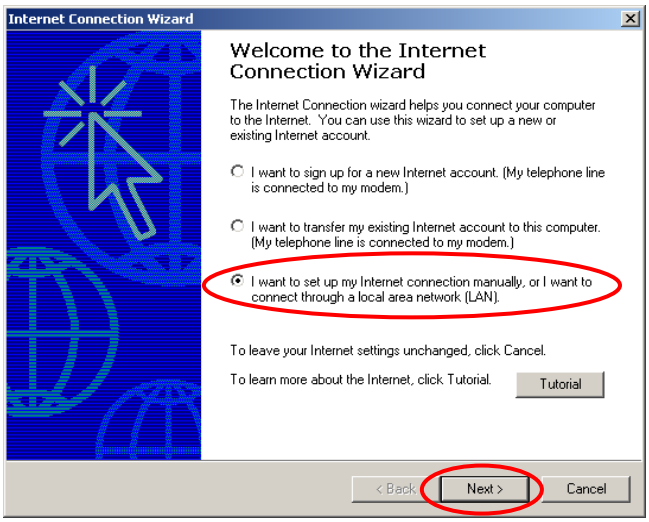
1) Choose **Start** >> **Control Panel** >> **Internet Options**.



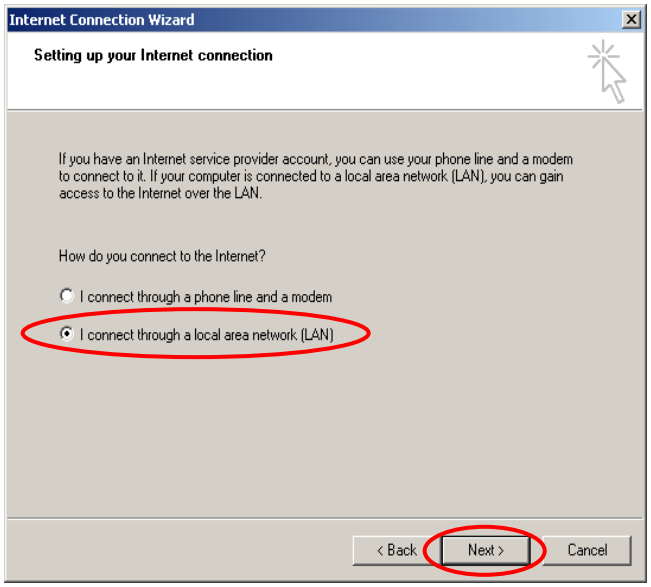
2) Choose the **Connections** tab, and then click ***Setup***.



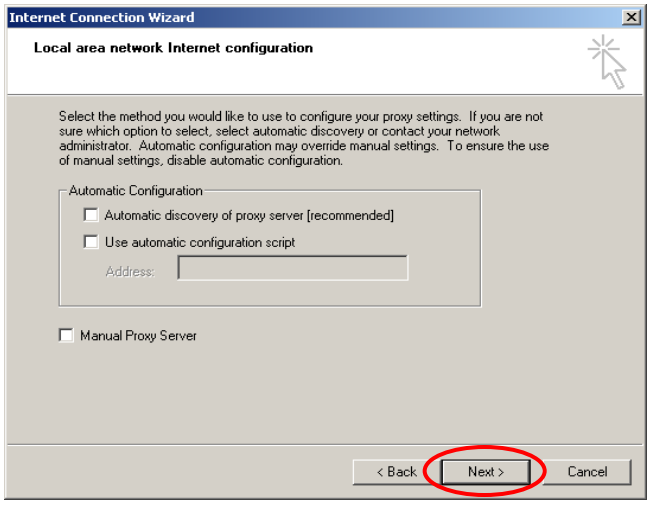
3) Choose **"I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)"**, and then click ***Next***.



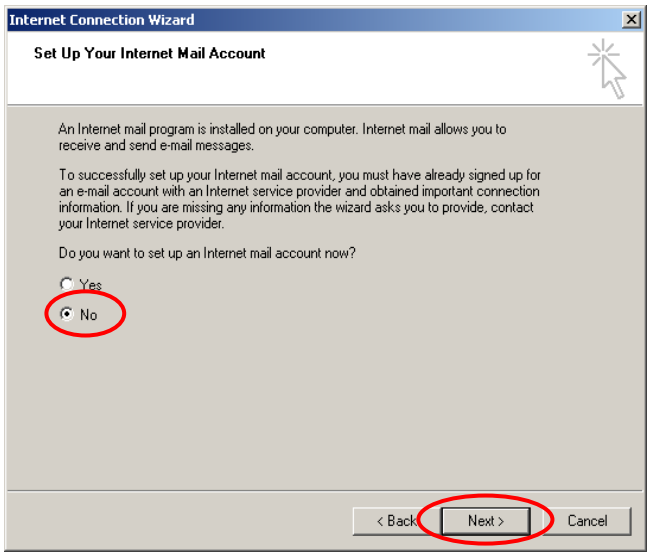
4) Choose **"I connect through a local area network (LAN)"** and then click ***Next***.



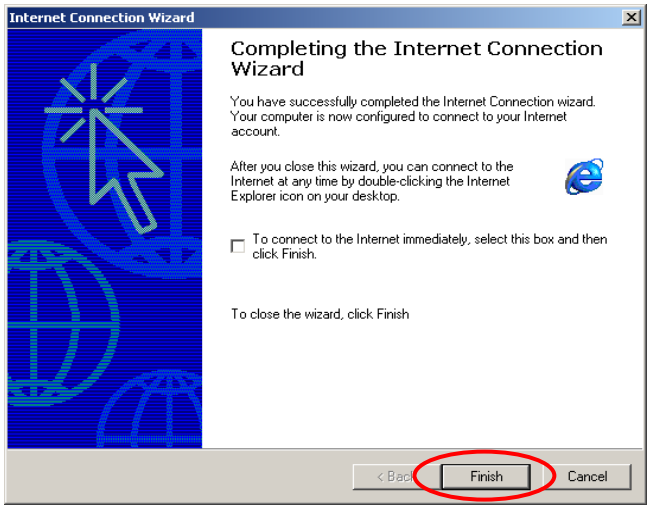
5) **DO NOT** choose any option in the following LAN window for Internet configuration, and just click ***Next***.



6) Choose **"No"** and then click ***Next***.

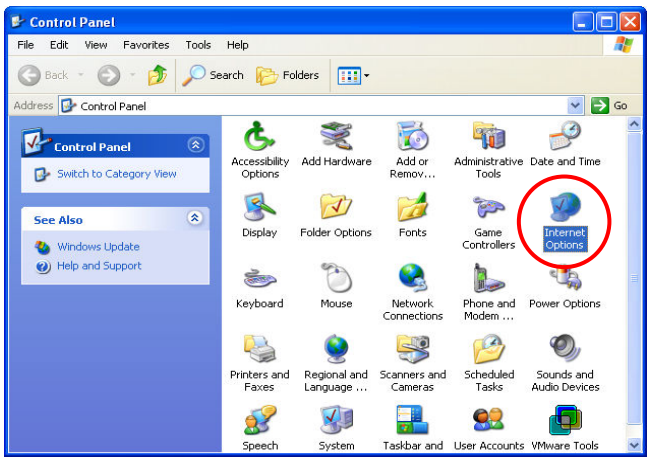


7) Finally, click ***Finish*** to exit the **Internet Connection Wizard**. Now, the set up is completed.

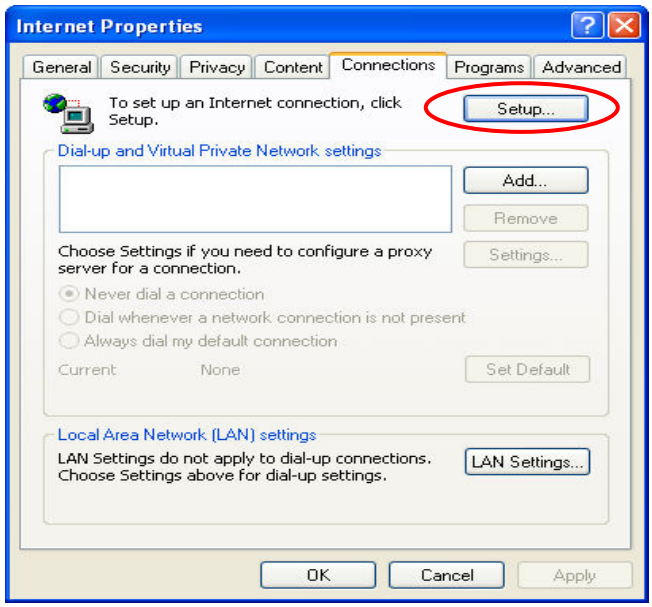


- **Windows XP**

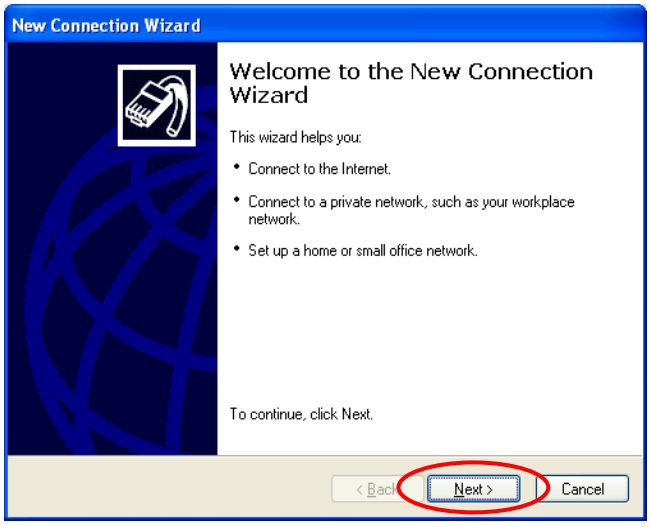
1) Choose **Start** >> **Control Panel** >> **Internet Option**.



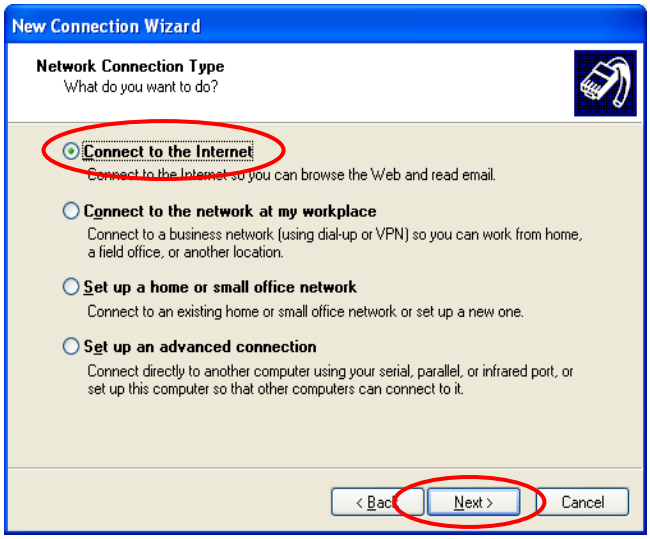
2) Choose the **Connections** tab, and then click ***Setup***.



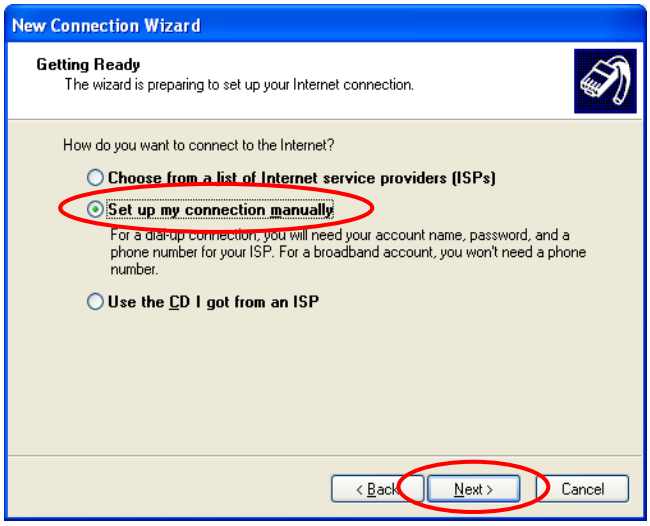
3) When the **Welcome to the New Connection Wizard** window appears, click ***Next***.



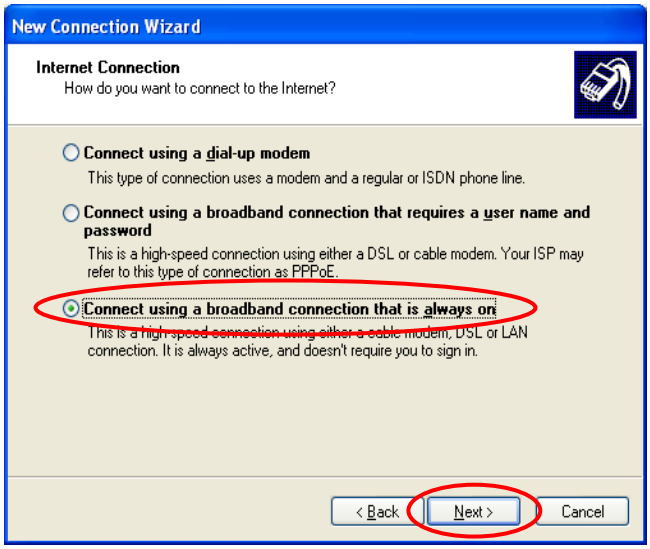
4) Choose **"Connect to the Internet"** and then click ***Next***.



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.

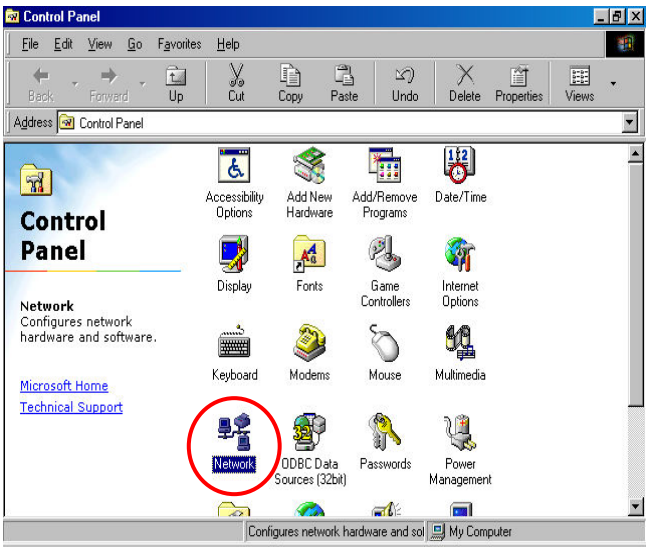
- **TCP/IP Network Setup**

If the operating system of the PC in use is Windows 95/98/ME/2000/XP, keep the default settings without any changes to directly start/restart the system. With the factory default settings, during the process of starting the system, AMG-2102 with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called **"Obtain an IP address automatically"**.

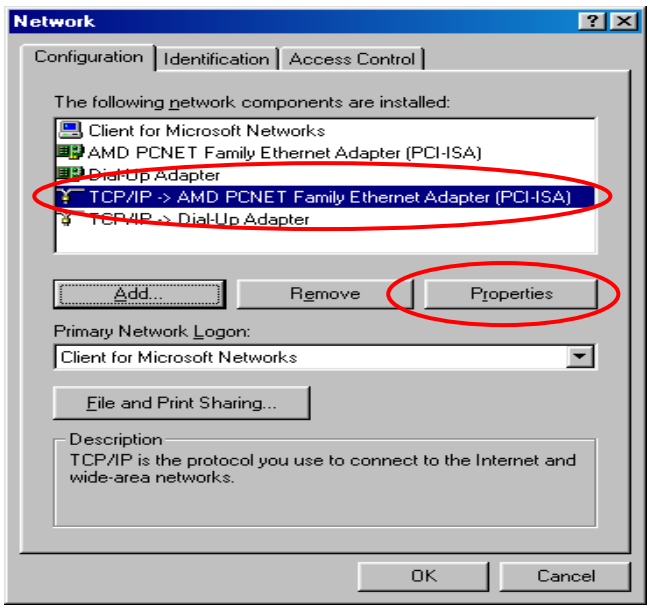
If checking the TCP/IP setup or using the static IP in the LAN1/LAN2 or LAN3/LAN4 section is desired, please follow these steps:

- **Check the TCP/IP Setup of Window 9x/ME**

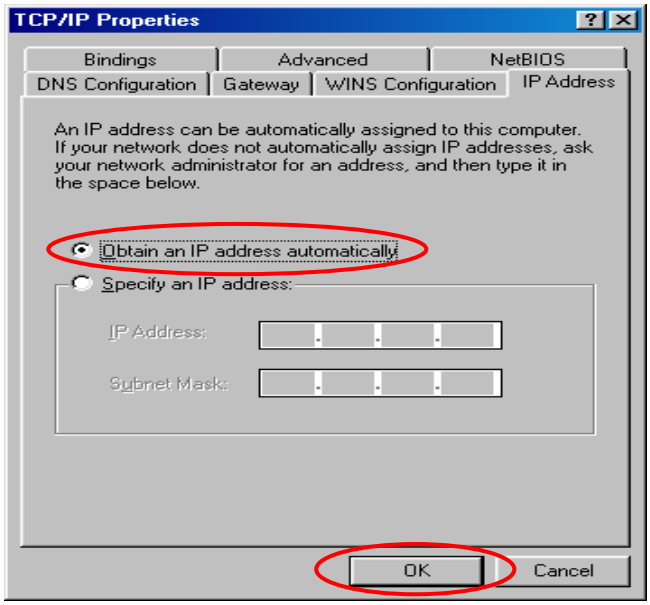
1) Choose **Start** >> **Control Panel** >> **Network**.



2) Click on the **Configuration** tab and select **"TCP/IP >> AMD PCNET Family Ethernet Adapter (PCI-ISA)"**, and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



3) **Using DHCP:** If you want to use DHCP, click on the **IP Address** tab and choose **"Obtain an IP address automatically"**, and then click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AMG-2102.

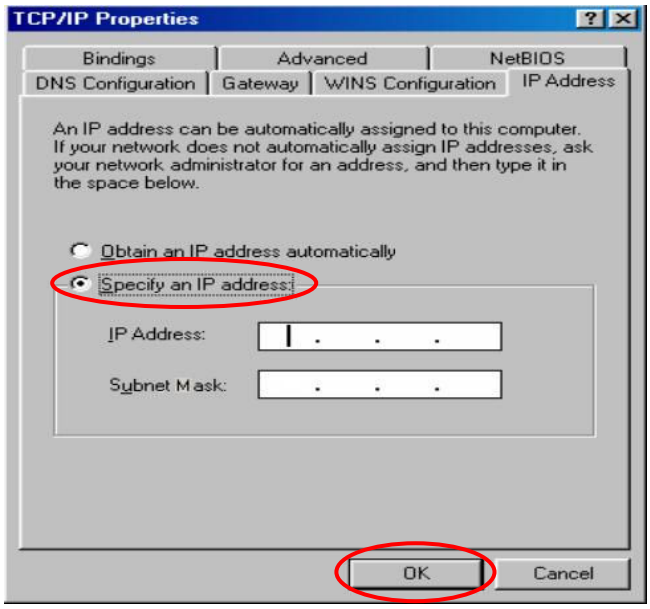


4) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of AMG-2102.

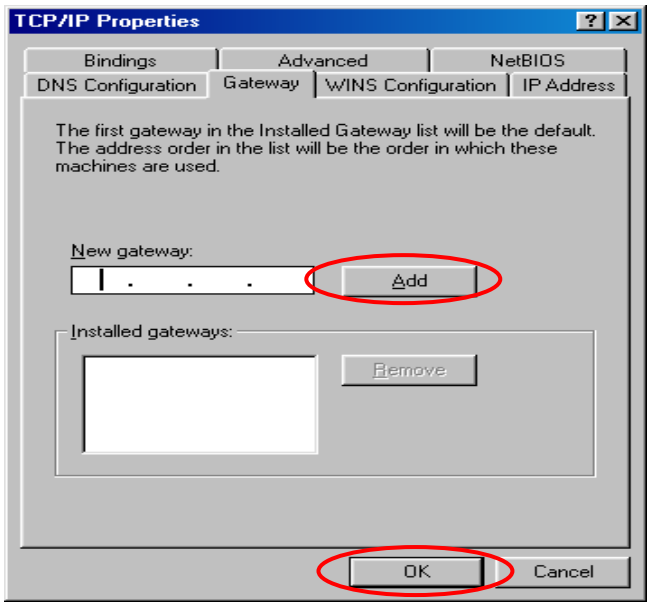
Caution:

If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

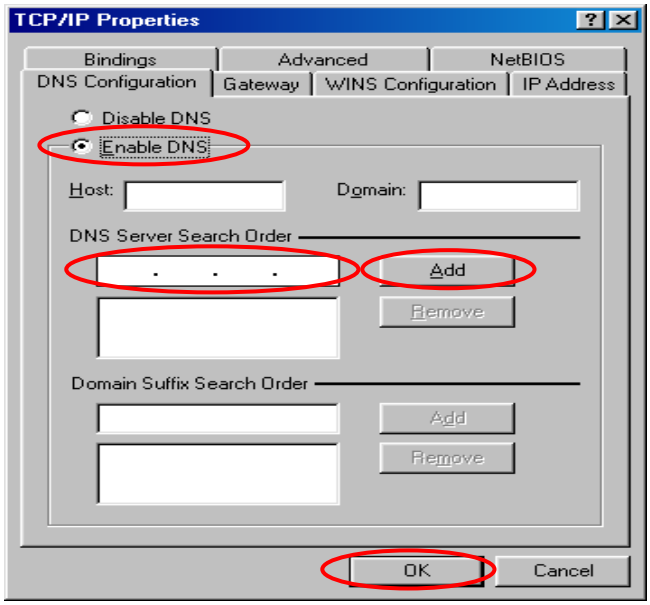
4.1) Click on the **IP Address** tab and choose **"Specify an IP address"**. Enter the *IP Address*, *Subnet Mask* and then click ***OK***.



4.2) Click on the **Gateway** tab. Enter the gateway address of AMG-2102 in the **"New gateway"** field and click ***Add***. Then, click ***OK***.

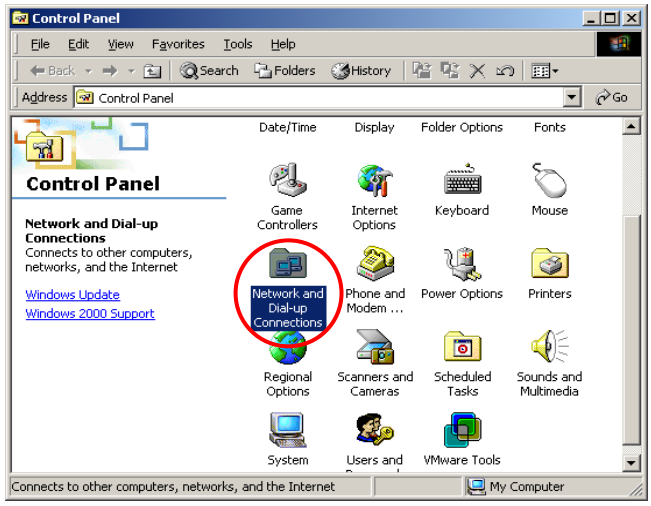


4.3) Click on **DNS Configuration** tab. If the DNS Server field is empty, select **"Enable DNS"** and enter *DNS Server address*. Click ***Add***, and then click ***OK*** to complete the configuration.

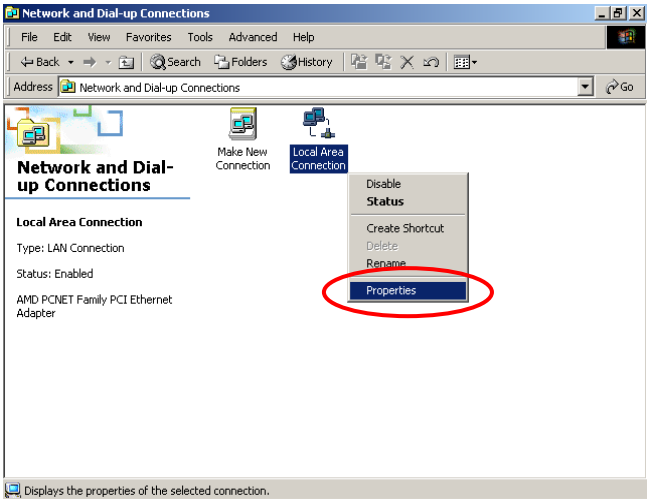


- **Check the TCP/IP Setup of Window 2000**

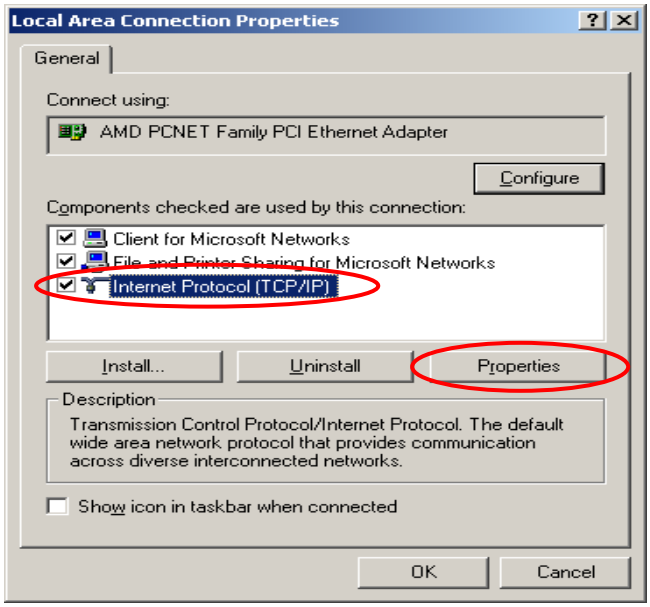
1) Select **Start** >> **Control Panel** >> **Network and Dial-up Connections**.



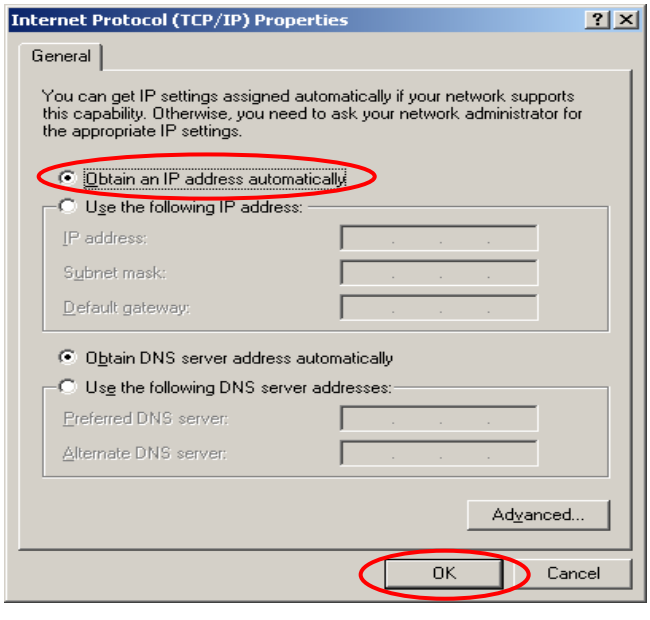
2) Right click on the **Local Area Connection** icon and select **"Properties"**.



3) Select **"Internet Protocol (TCP/IP)"** and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



4) **Using DHCP:** If you want to use DHCP, choose **"Obtain an IP address automatically"**, and then click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AMG-2102.

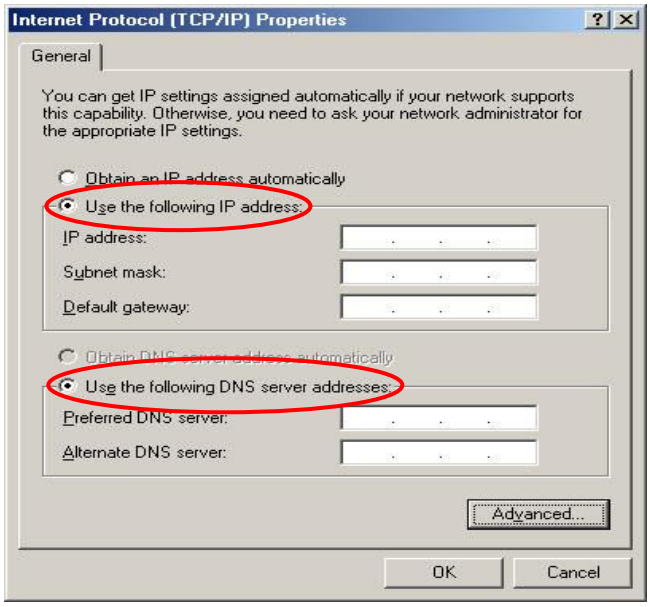


5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of AMG-2102.

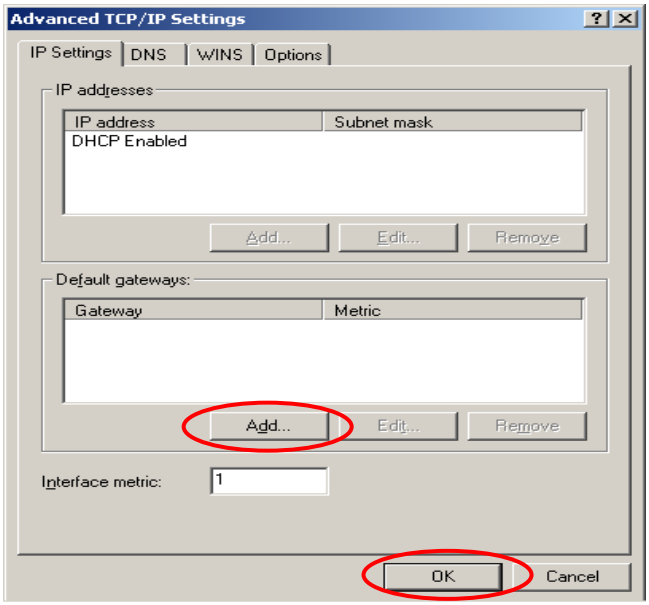
> *If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.*

5.1) Choose **"Use the following IP address"** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **"Using the following DNS server addresses"** and enter the *DNS Server address*. Then, click ***OK***.

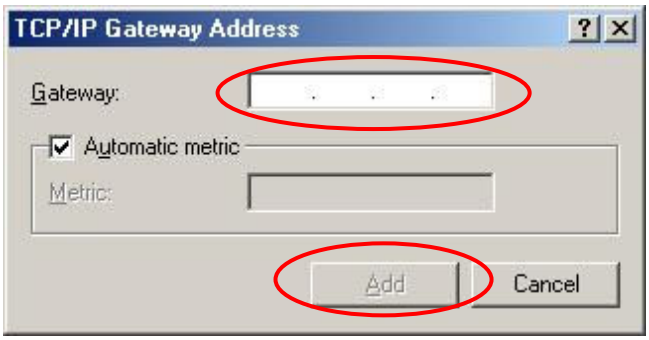
5.2) Click ***Advanced*** to enter the **Advanced TCP/IP Settings** window.



5.3) Click on the **IP Settings** tab and click ***Add*** below the **"Default gateways"** column and the **TCP/IP Gateway Address** window will appear.

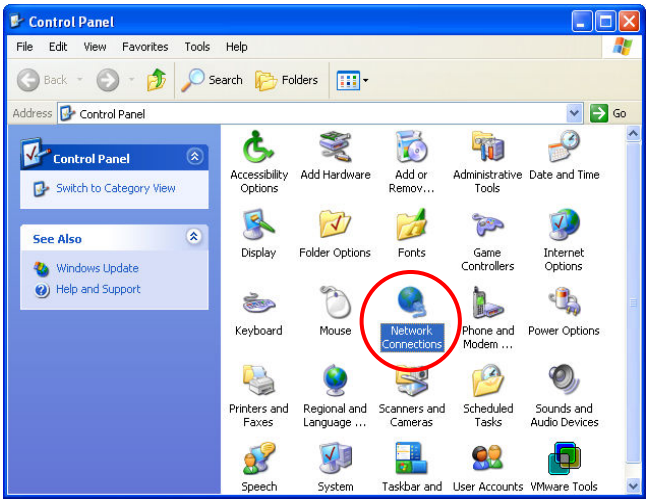


5.4) Enter the gateway address of AMG-2102 in the **"Gateway"** field, and then click ***Add***. After back to the **IP Settings** tab, click ***OK*** to complete the configuration.

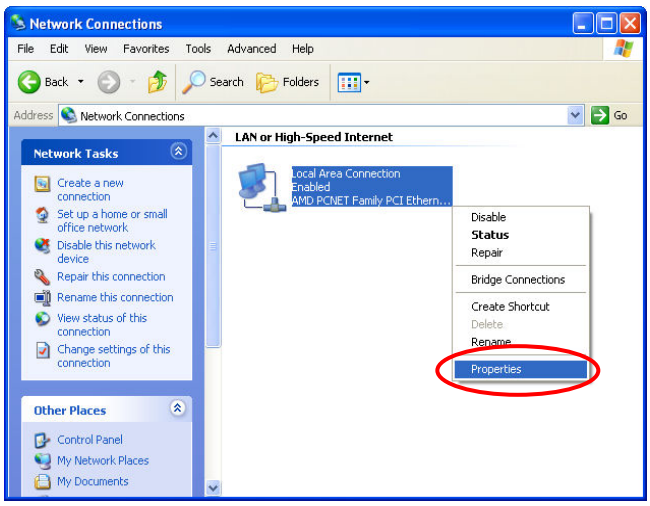


- **Check the TCP/IP Setup of Window XP**

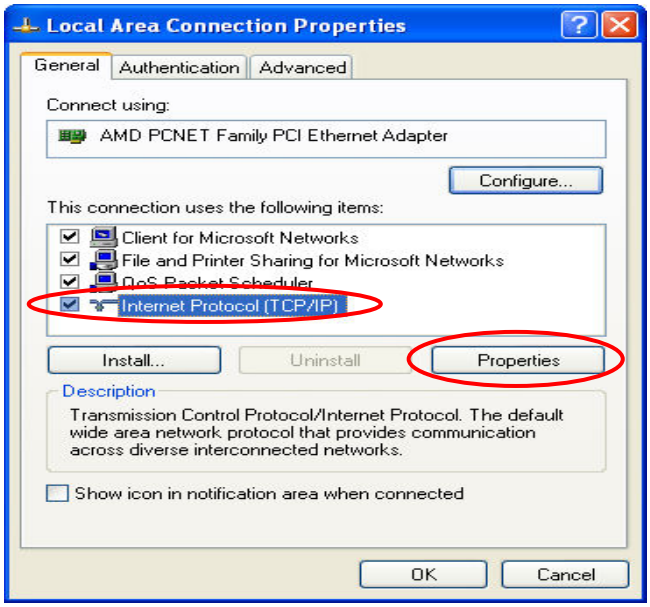
1) Select **Start** >> **Control Panel** >> **Network Connection**.



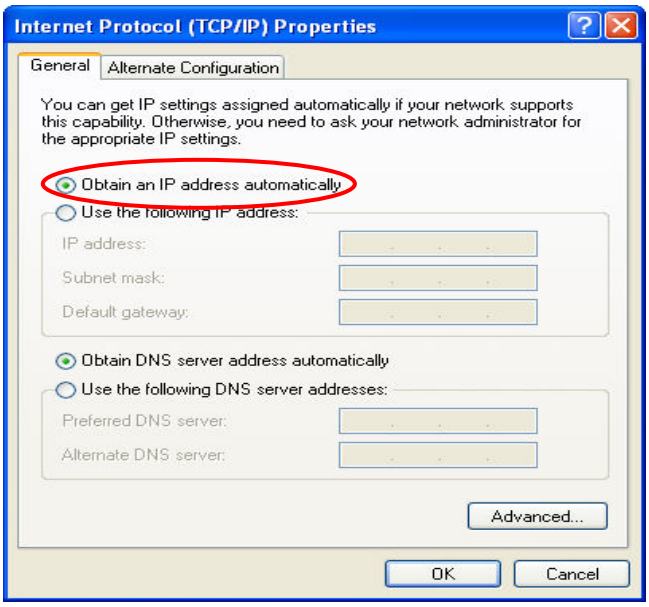
2) Right click on the **Local Area Connection** icon and select **"Properties"**.



3) Click on the **General** tab and choose **"Internet Protocol (TCP/IP)"**, and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



4) **Using DHCP:** If you want to use DHCP, choose **"Obtain an IP address automatically"** and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AMG-2102.



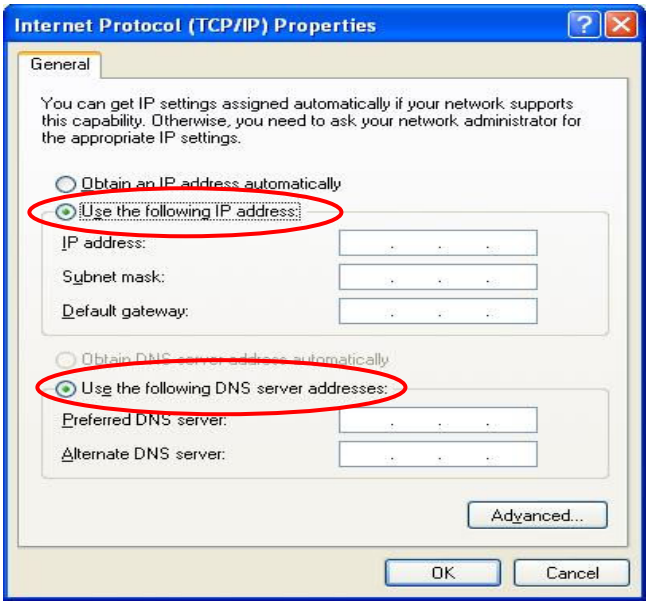
5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of AMG-2102.

Caution:

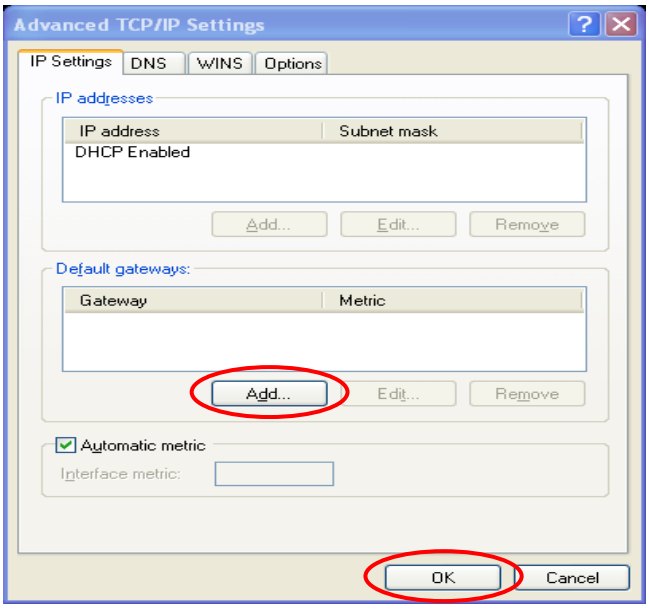
If your PC has been set up completely, please inform the network administrator before proceeding to the following steps.

5.1)Choose **"Use the following IP address"** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **"Using the following DNS server addresses"** and enter the *DNS Server address*. Then, click ***OK***.

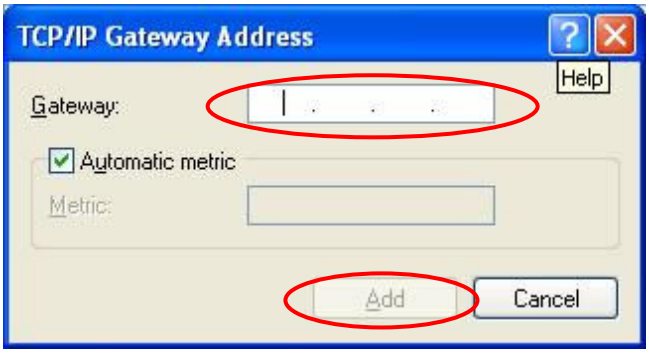
5.2)Click ***Advanced*** to enter the **Advanced TCP/IP Settings** window.



5.3)Click on the **IP Settings** tab and click ***Add*** below the **"Default gateways"** column and the **TCP/IP Gateway Address** window will appear.



5.4)Enter the gateway address of AMG-2102 in the **"Gateway"** field, and then click ***Add***. After back to the **IP Settings** tab, click ***OK*** to finish the configuration.



Appendix B. Policy Priority (Global Policy, Service Zone Policy, Authentication Policy and User Policy)

AMG-2102 supports multiple Policies, including one **Global Policy** and 24 individual **Policy** can be assign to different **Group**. **Global Policy** is the system's universal policy and applied to all clients, while other individual Policy can be selected and defined to be applied to any Service Zone. On the other hand, **Service Zone** also has a **Default Policy**. For some authentication, such as Local, RADIUS and LDP, user can assign to different Group individually. The clients belonging to a Service Zone will be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. So one user may be applied different policy at the same time. Which policy is actually applied to this user?

The Policy Priority must be:

User Policy >> Authentication Policy >> Service Zone Policy >> Global Policy

Now, let us discus different user policy type:

1. For Local, RADIUS and LDAP, if these users are assigned to different Group individually, these users can be assigned to their Group. For example, a Local user, user01, is assigned to Group1 and the Local Authentication is assigned to Group2. If Group1 in Service Zone1 can be applied Policy1. Then user01 login to Service Zone1 will get Policy1. This is a common case for users that can assign Group individually.

2. For Local, RADIUS and LDAP, if these users do not assigned any Group individually, so they are same as other authentication server users that they can not assign to Group individually. For example, a POP3 user, pop01, the POP3 Authentication is assigned to Group1. If Group1 in Service Zone1 can be applied Policy1. Then pop01 login to Service Zone1 will get Policy1. This is another common case for users that can assign Group by authentication server.

3. If Authentication server also do not assign to a Group, then the user will applied the Service Zone Default Policy. For example, a Local user, user01, is assigned to Group *None* and the Local Authentication is also assigned to Group *None*. If the Default Policy of Service Zone1 is applied Policy1. Then user01 login to Service Zone1 will get Policy1.

4. If the Default Service Zone Policy is *None*. Authentication server does not assign to a Group and user Group is *None* too. For example, a Local user, user01, is assigned to Group *None* and the Local Authentication is also assigned to Group *None*. If the Default Policy of Service Zone1 is *None*. Then

user01 login to Service Zone1 will apply the Global Policy.

So, the Global Policy has the lowest policy priority; on the other hand, the User Policy will be the highest one.

Appendix C. Monitoring 3rd Party AP

Configure Monitoring 3rd Party AP, go to: ***Network >> Monitor IP***.

If you are using 3rd party AP, you can use Monitor IP function to monitor the AP connection status. Because AMG-2102 can not manage these APs, Monitor IP is a better way to monitor the AP connection status.

AMG-2102 will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the necessary information, click ***Apply*** to save the settings.

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	
11	http		Create	
12	http		Create	
13	http		Create	
14	http		Create	
15	http		Create	
16	http		Create	
17	http		Create	
18	http		Create	
19	http		Create	
20	http		Create	

Click ***Monitor Now*** to check the current status of all the monitored IP. The system supports monitoring on IP addresses listed in the **"Monitor IP List"**.

Monitor IP result(s)			
No.	**IP Address**	**Result**	**Remark**
1	192.168.11.254		test

Appendix D. RADIUS Accounting

This section is trying to organize the basic configuration with RADIUS server to work with VSA. The aim is trying to control the maximum usage (upload; download or upload + download traffic) of clients in each session.

This **VSA** will send from RADIUS server to gateway along with an **Access-Accept** packet. In other words, when the external RADIUS server accepts the request, it will not only reply with an **Access-Accept** and it will also carry a maximum value in bytes that each user is allowed to transfer. This value may be the maximum upload traffic; download traffic or the summation of each user's download plus upload traffic in bytes. Gateway will check this value every minute, if the user is reached this value, gateway will stop the session of this user and send a "Stop" to RADIUS server.

1. Description

This Attribute is available to allow vendors to support their own extended Attributes not suitable for general usage. It MUST not affect the operation of the RADIUS protocol.

The standard **Attribute Type** of VSA is "26". Also we need to know the "**Vendor ID**", in this example; the **Vendor ID** of None is "21920". There must have other attribute to define the amount of traffic with "**Attribute Number**" and "**Attribute Value**":

Attribute Name	**Attribute Number**	**Attribute Value**
None-Byte-Amount	10	To be defined by administrator for different user group
None-MaxByteIn	11	To be defined by administrator for different user group
None-MaxByteOut	12	To be defined by administrator for different user group
None-Byte-Amount-4GB	20	To be defined by administrator for different user group

None-MaxByteIn-4GB	21	To be defined by administrator for different user group
None-MaxByteOut-4GB	22	To be defined by administrator for different user group

If the amount of traffic is larger than 4 GB, then the attribute of "XXXX-4GB" is for the carry. For example, if the amount is 5 GB, you must set "None-Byte-Amount = 1048576" and "None-Byte-Amount-4GB = 1".

On the other hand, if administrator fills in all attributes, it means that if any condition is reached, the user will be kicked out from system. For example, if administrator set "None-Byte-Amount = 1048576"; "None- MaxByteIn = 1048576" and "None- MaxByteOut = 1048576". It means that whatever the downlink or uplink or total traffic exceeded the limit, the user will be kicked out from system.

2. VSA configuration in RADIUS server (IAS Server)

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

2.1. Step 1

Assume there are already have **users** in RADIUS Server

Assume there are already have **Groups** and assigned **users** to belong these **Groups** in RADIUS Server

Assume there are already have **Policies** and assigned **Groups** to belong these **Policies** in RADIUS Server

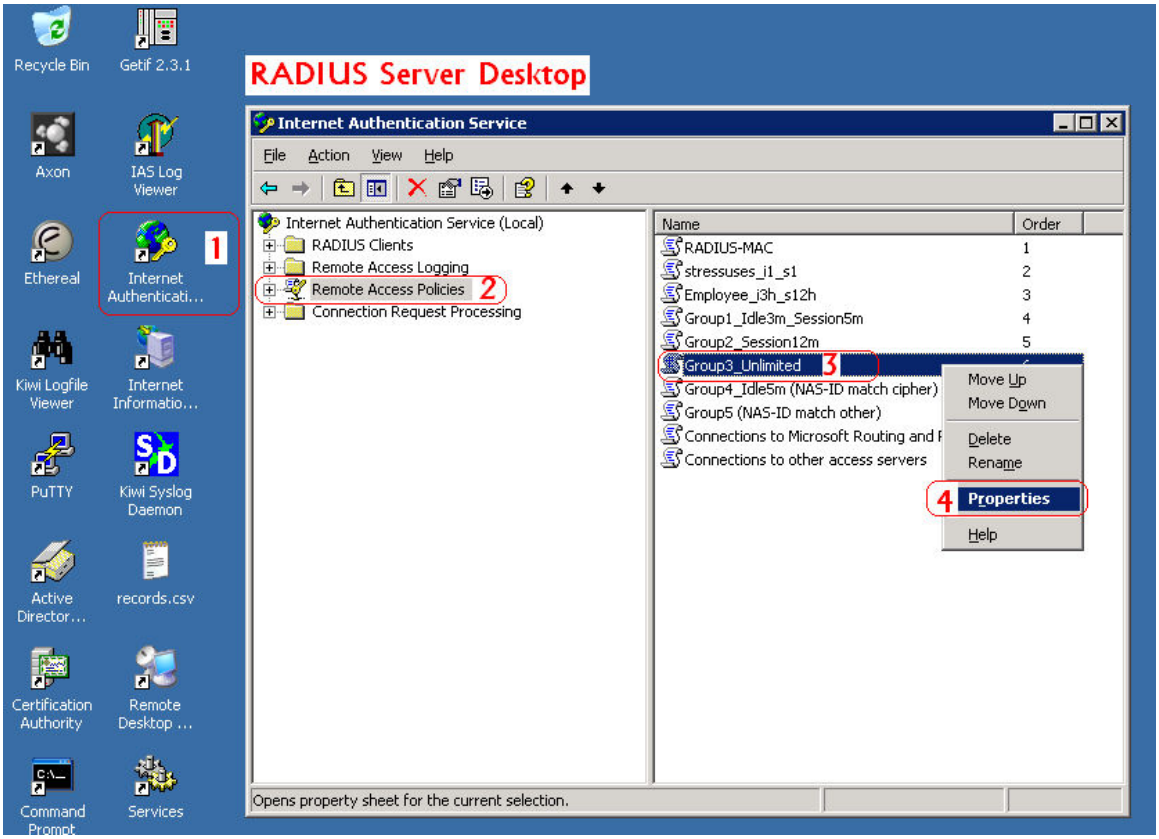
2.2. Step 2

Run "Internet Authentication Server"

Open "Remote Access Policies"

Select a **Policy**

Right click and scroll down to its properties page



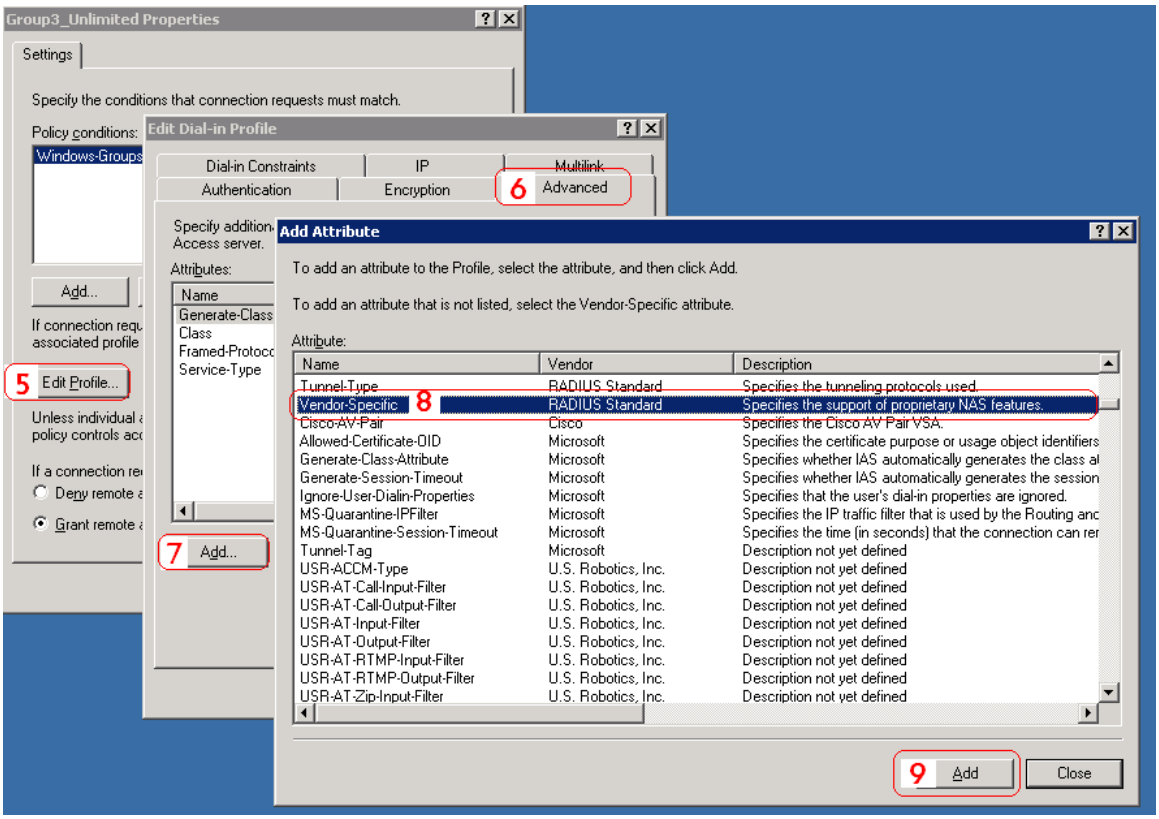
2.3. Step 3

Edit Profile

Select the **Advanced** Tag

Add a new attribute

Add a new **Vendor-specific** attribute



2.4. Step 4

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

Set "Vendor Code = 22426"

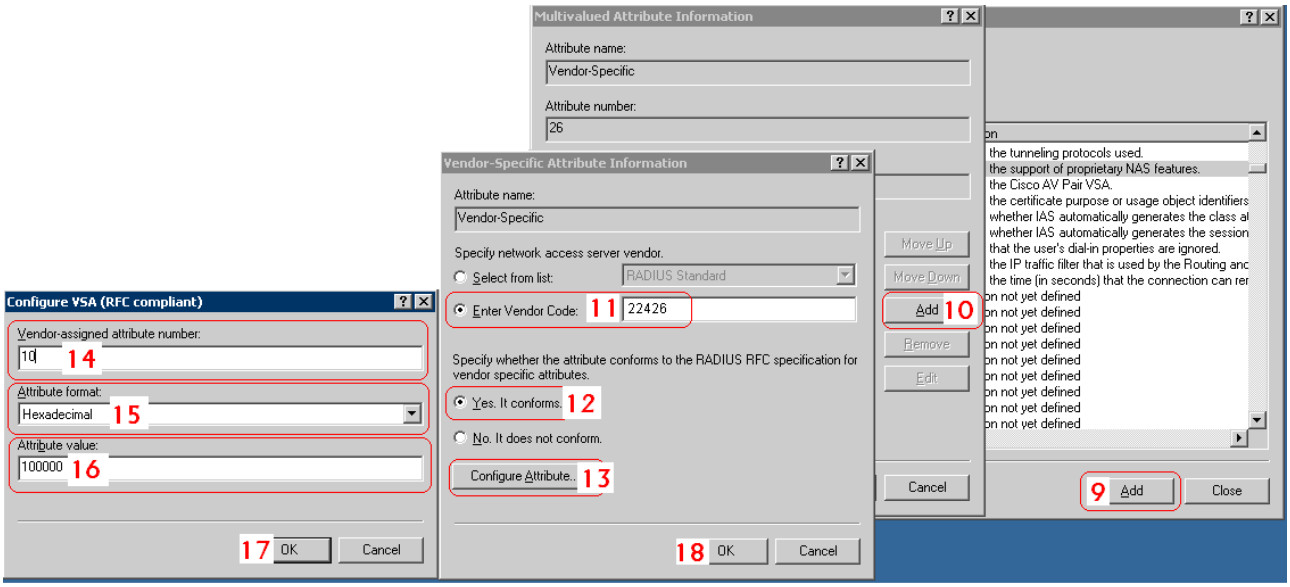
Set it conforms to the RADIUS RFC

Configure Attribute

Set "Vendor-assigned attribute number = 10"

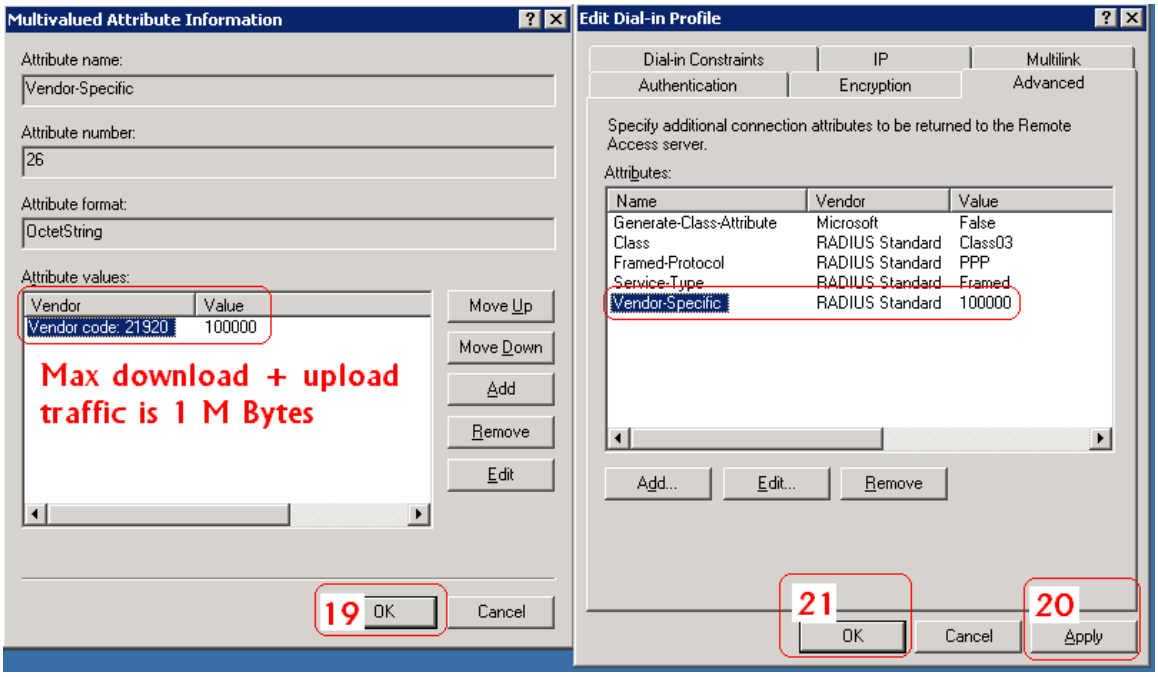
Set "Attribute format = Hexadecimal"

Set "Attribute Value = 1000000"



2.5. Step 5

Confirm the **Vendor-specific Attribute** has been added success

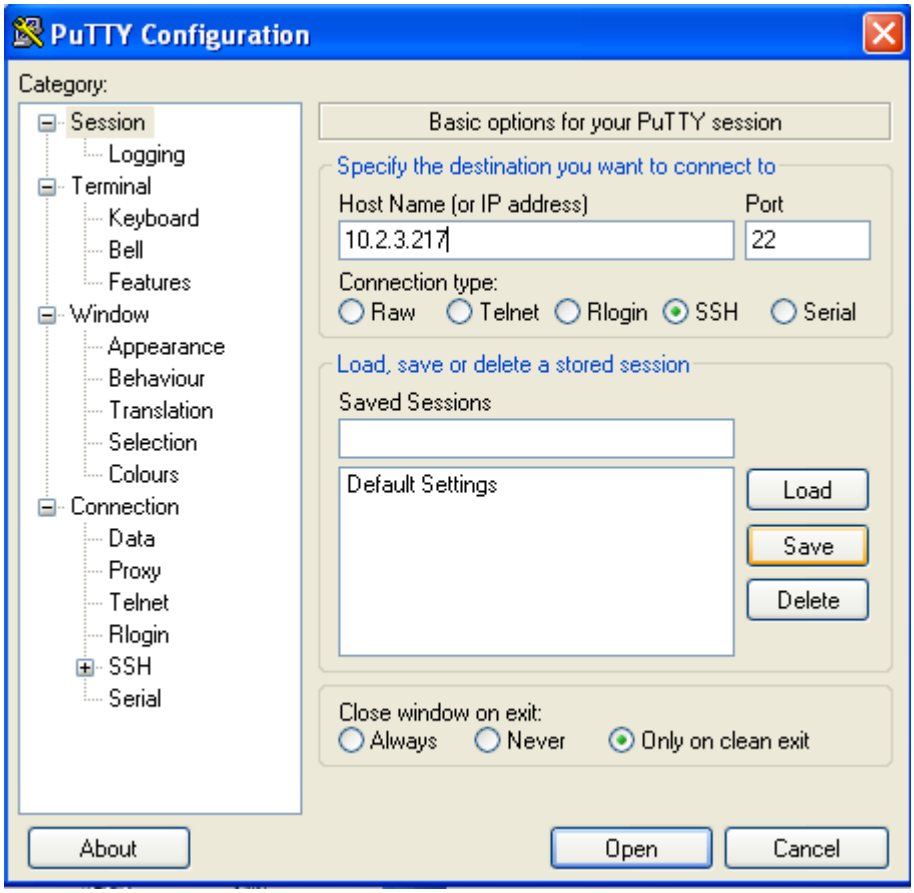


2.6. Step 6

Follow the same steps to create other **Vendor-specific Attribute** as you need.

3. VSA configuration in RADIUS server (FreeRADIUS)

This section will guide you through a **VSA** configuration using the operating system "Fedora" FreeRADIUS version 1.0.5. Before getting start, open the shell of RADIUS server, for example, use *Putty* to access the Linux Host:



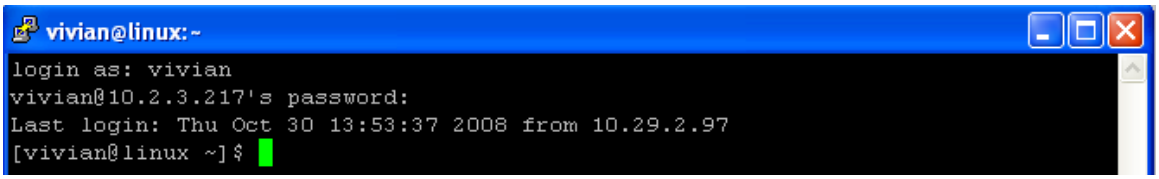
3.1. Step 1

Assume there are already have users in RADIUS Server

Assume there are already have **Groups** and assigned **users** to belong these **Groups** in RADIUS Server

3.2. Step 2

Login the Linux Host of the RADIUS server.



3.3. Step 3

Create a file "dictionary.none" under the "freeradius" folder.

```
[vivian@linux ~]$ vi /usr/share/freeradius/dictionary.none
```

3.4. Step 4

Edit and save the content of the file "dictionary.none" as the following:

```
VENDOR          none            21920

#
#     Standard attribute
#
ATTRIBUTE            none-Byte-Amount          10      integer  none
```

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

```
VENDOR          none            21920

#
#       Standard attribute
#
ATTRIBUTE            none-Byte-Amount          10      interger         none
ATTRIBUTE            none-MaxByteIn            11      interger         none
ATTRIBUTE            none-MaxByteOut           12      interger         none
ATTRIBUTE            none-Byte-Amount-4GB      20      interger         none
ATTRIBUTE            none-MaxByteIn-4GB        21      interger         none
ATTRIBUTE            none-MaxByteOut-4GB       22      interger         none
```

3.5. Step 5

Edit the file "dictionary" under the folder "freeradius".

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

3.6. Step 6

Include "dictionary.none" in the dictionary of RADIUS server. Insert it in an incremental position that easy to find it again.

```
vivian@linux:~
$INCLUDE dictionary.ascend
$INCLUDE dictionary.bay
$INCLUDE dictionary.bintec
$INCLUDE dictionary.cabletron
$INCLUDE dictionary.none
$INCLUDE dictionary.cisco
#
#   This is the same as the altiga dictionary.
#
#$INCLUDE dictionary.cisco.vpn3000
$INCLUDE dictionary.cisco.vpn5000
$INCLUDE dictionary.cisco.bbsm
$INCLUDE dictionary.colubris
```

3.7. 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>
```

3.8. Step 8

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

```
mysql> INSERT INTO radgroupreply (GroupName,Attribute,op,Value)
 VALUES ('group03','None-Byte-Amount',':=','1048576')
Query OK, 1 row affected (0.00 sec);
mysql> exit
Bye
```

3.9. Step 9

Restart RADIUS Demand to get your settings activated.

```
[vivian@linux ~] # /etc/init.d/radiusd restart
Stopping RADIUS server:                                    [  OK  ]
Starting RADIUS server: Thu Oct 30 14:26:41 2008 : Info: Starting - reading conf
iguration files ...
                                                           [  OK  ]
```

Appendix E. Net Retriever and Port Mapping

This section is trying to introduce the configuration of Net Retriever with VLAN Port Mapping. Net Retriever is a "middleware" that communicates with the popular High Speed Internet Access (HSIA) hardware and Front Office System (FOS) software to provide a seamless integration of the two. It can fill the void created by the hospitality industry's rapid adoption of High Speed Internet Access (HSIA) for their guest rooms and public areas.

Beside the communication between NONE and Net Retriever, it also needs the VLAN Port (Room) Mapping to identify the fee in each room. Each room will mapping to a unique VLAN Tag. In addition, it need to create at least one or more On-demand Billing Plan to let the user to choose a satisfactory one for the internet access right.

Note:

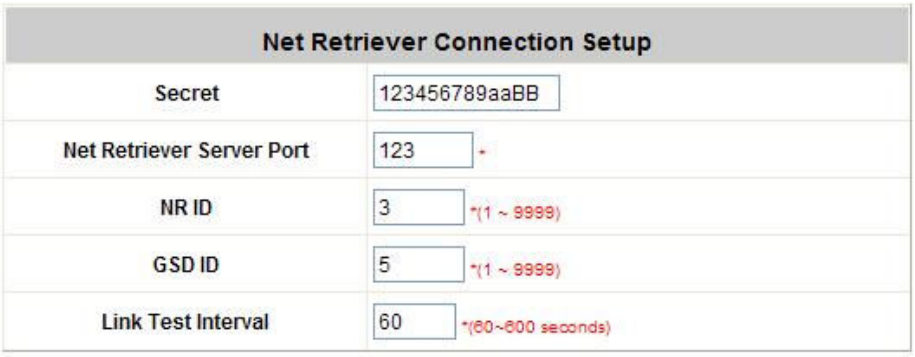
For more detail of On-demand Billing Plan configuration, please refer to the section of **On-demand Users**.

1. Net Retriever

Now, let us begin to configure Net Retriever connection:

Configure Net Retriever, go to: ***Users >>Net Retriever >>Connection Setup***.

- **Net Retriever Configuration**



Secret: The secret key between **Guest Service Device** and **Net Retriever** for challenge and response (MD5 Hash) to test the link. It should contain one or more lowercase letters, uppercase letters, numbers and symbols. It also should be between 8 ~ 16 characters.

Net Retriever Server Port: The port used by Net Retriever, the default is "8324".

NR IR: The ID of the **Net Retriever**.

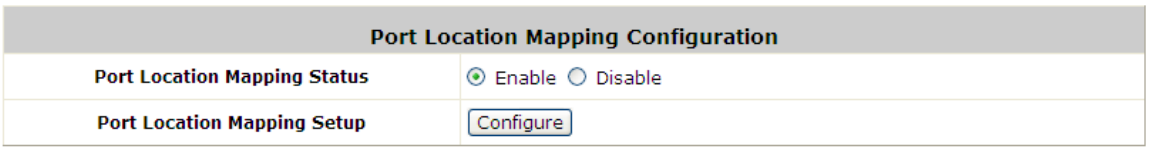
GSD IR: The ID of the **Guest Service Device**.

Link Test Interval: The time interval of the Link Test, the default is "300" seconds.

Now, the Net Retriever connection is finished in the **Guest Service Device** side. In the **Net Retriever** side, it has to know the *IP address* of **Guest Service Device**, and then they can communicate to each other.

2. VLAN Port (Room) Mapping

Configure VLAN Port Mapping, go to: ***System >>Port Location Mapping***.



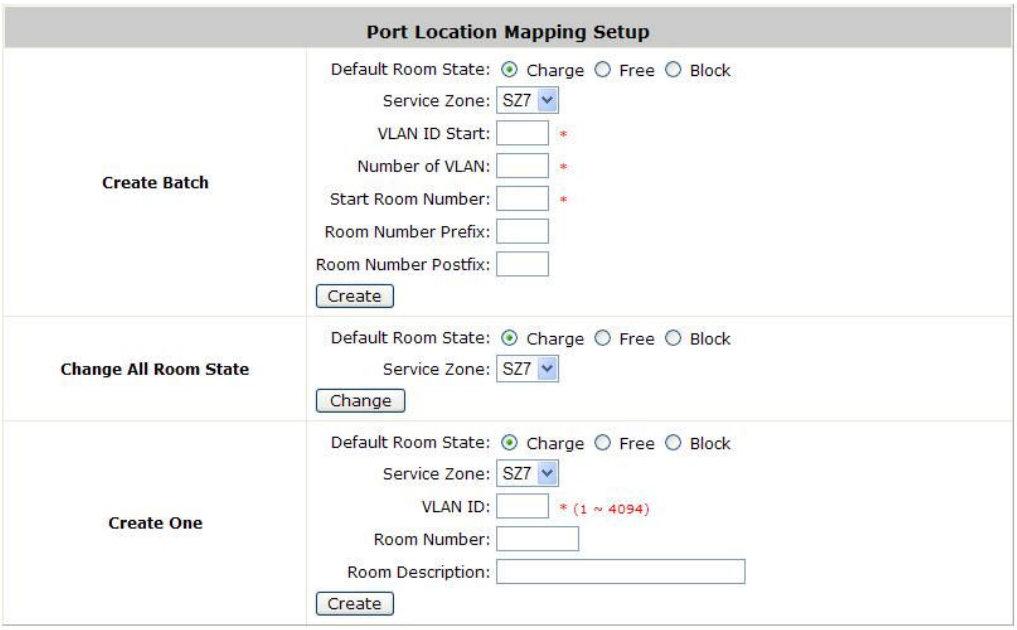
- **Port Location Mapping Status:** Enable or Disable the Port Location Mapping, clicking ***Configure*** to enter its setup.

After the Net Retriever connection is finished, you must setup the Room mapping. Each Room is mapping to one VLAN Tag. And each Room can be assign to different Service Zone to get different policy. Furthermore, you can configure the Room to different state: **Charge**, **Free** or **Block**.

- If the state is **Charge**, it is the most normally usage to charge the user. If the user opens a browser and tries to access internet, it will pop up a Login page with disclaimer, user can select a satisfactory billing plan and begin access internet until the quota has run out.

- If the state is **Free**, the user can access internet in this room without any charge.

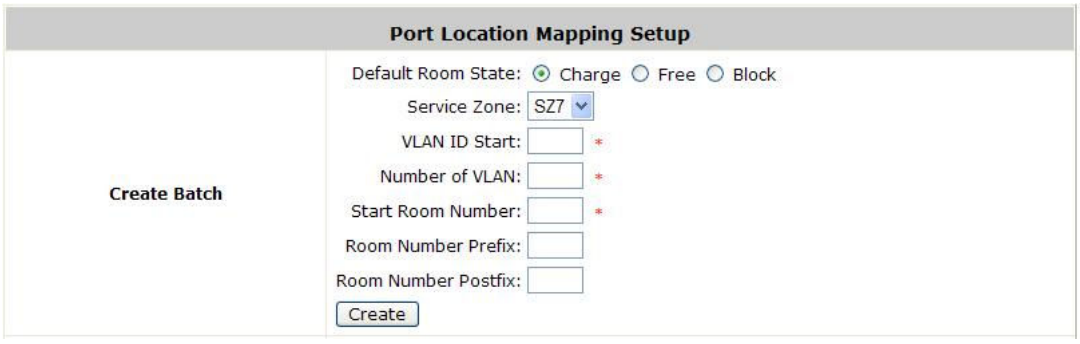
- If you do not want to provide any internet access right in the rooms, you may change the state of the rooms to **Block**. If the user opens a browser and tries to access internet, it will pop up a Blocking message to notice the user.



Now, let us begin to configure the Port Mapping. There are three main group of setting: **Create Batch**, **Change All Room State** and **Create One**.

You can create the Room Mapping by a batch processing that if you want to create a contiguously VLAN Tag and Room number.

- **Port Location Mapping Setup – Create Batch**



Default Room State: The default state of the rooms, it may be: Charge, Free or Block.

Service Zone: The service zone of these rooms

VLAN ID Start: The first VLAN ID.

Number of VLAN: The total number of VLAN.

Start Room Number: The start room number.

Room Prefix: The prefix of room number.

Room Postfix: The postfix of room number.

After you had created the VLAN Tag and Room number mapping, you can change all of the **Room State** in the same Service Zone.

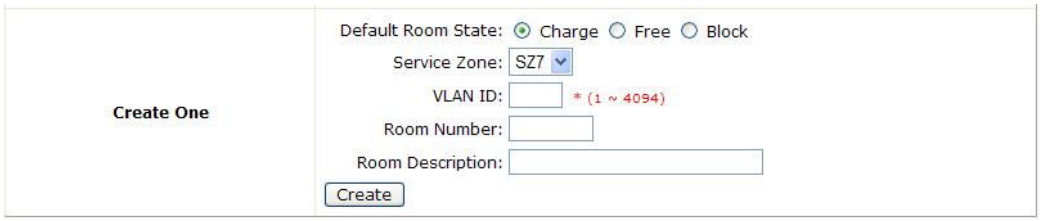
- **Port Location Mapping Setup – Change All Room State**

Default Room State: The default state of the rooms, it may be: Charge, Free or Block.

Service Zone: The service zone of these rooms

If you want to create the Room Mapping is not a contiguously VLAN Tag and Room number, then you can create it one by one.

- **Port Location Mapping Setup – Create One**



Room Default State: The default state of the rooms, it may be: Charge, Free or Block.

Service Zone: The service zone of these rooms

VLAN ID: The VLAN ID to be added.

Room Number: The room number mapping to this VLAN ID.

Room Description: The reference or remark information of this room.

Caution:

The VLAN Tag used in here, VLAN Port (Room) Mapping, must not be conflict with the VLAN Tag that has been assigned to each Service Zone.

3. Check or modify the VLAN Port (Room) Mapping

If you want to check the room mapping information or you want to change any setting of the room mapping.

Configure Port Location Mapping List, go to: ***System >>Port Location Mapping***.

Port Location Mapping List

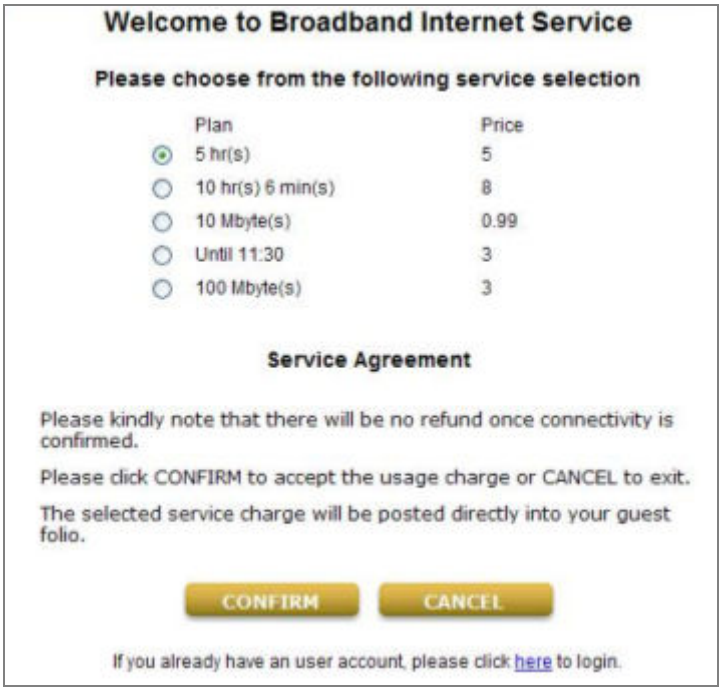
	VLAN ID	Room Num	State	Description	Service Zone	Delete All
🔴	101	101	Charge		SZ7	Delete
🟢	102	102	Charge		SZ7	Delete
🟢	103	103	Charge		SZ7	Delete
🟢	104	104	Charge		SZ7	Delete
🟢	105	105	Charge		SZ7	Delete
🟢	106	106	Free		SZ7	Delete
🟢	107	107	Free		SZ7	Delete
🟢	108	108	Free		SZ7	Delete
🟢	109	109	Block		SZ7	Delete
🟢	110	110	Block		SZ7	Delete

Click the **VLAN ID** link will go to the **Port Mapping Profile** page. You can change the **Room State** or **Service Zone** of this room. You also can check the presently user account information.

Port Mapping Profile	
VLAN ID	101
Room Number	101
Room State	○ Free ◉ Charge ○ Block
Room Description	
Service Zone	SZ7
Room Available	
User Name / Password	feh9 / 8sk7g282
Plan Type	TIME
Plan Quota	5 hr(s)
Remaining Quota	5 hr(s)
User Account Status	Online
Reference	roomN-101

4. View the Event Login

After all of the configuration has completed. User may try to login from the "**Charge**" room. Connect the user's notebook (laptop) to the Ethernet port of this room. Enable DHCP client in this notebook (laptop). Open a browser and try to access internet. The browser will show the Login page, user may chose a billing plan, click the Confirm button. Then user can access internet now.



If you already have the user account, you can click the **here** link to login with the user account that you have.

After the user select a billing plan and buy it to access Internet. You can check the Net Retriever Event Log.

View Net Retriever Event Log, go to: ***Users >>Net Retriever >>Event Log***.

Net Retriever Event Log	
Date	**Size (Byte)**
2009-08-20	267