Air Live®
Powered by OvisLink Corp.

MW-2000Sv2

Hotspot Management Gateway

User's Manual

www.airlive.com

Declaration of Conformity

We, Manufacturer/Importer

OvisLink Corp.
5F., NO.6, Lane 130, Min-Chuan RD.,
Hsin-Tien City, Taipei County, Taiwan

Declare that the product

Firewall

MW-2000S

is in conformity with

In accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

Clause	Description
■ **EN 55022:1994/A1 :1995/A2:1997**	Limits and methods of measurement of radio disturbance characteristics of information technology equipment
■ **EN 61000-3-2:2000**	Disturbances in supply systems caused by household appliances and similar electrical equipment "Harmonics"
■ **EN 61000-3-3:1995/ A1:2001**	Disturbances in supply systems caused by household appliances and similar electrical equipment "Voltage fluctuations"
■ **EN 55024:1998/A1 :2001**	Information Technology equipment-Immunity characteristics-Limits And methods of measurement
■ **CE marking**	CE

Manufacturer/Importer

Signature： albert Ye

Name : **Albert Yeh**

Position/ Title : **Vice President**

Date： **2006/10/5**

(Stamp)

AirLive MW-2000S CE Declaration Statement

Country	Declaration	Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento AirLive MW-2000S je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	**lt** Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šis AirLive MW-2000S atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr AirLive MW-2000S overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	**nl** Nederlands [Dutch	Hierbij verklaart OvisLink Corp. dat het toestel AirLive MW-2000S in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
de Deutsch [German]	Hiermit erklärt OvisLink Corp., dass sich das Gerät AirLive MW-2000S in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.	**mt** Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan AirLive MW-2000S jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme AirLive MW-2000S vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	**hu** Magyar [Hungarian]	Az OvisLink Corporation kijelenti, hogy az AirLive MW-2000S megfelel az 1999/05/CE irányelv alapvető követelményeinek és egyéb vonatkozó rendelkezéseinek.
en English	Hereby, OvisLink Corp., declares that this AirLive MW-2000S is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**pl** Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że AirLive MW-2000S jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
es Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el AirLive MW-2000S cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.	**pt** Português [Portuguese]	OvisLink Corp declara que este AirLive MW-2000S está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙ AirLive MW-2000S ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.	**sl** Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta AirLive MW-2000S v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
fr Français [French]	Par la présente OvisLink Corp. déclare que l'appareil AirLive MW-2000S est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	**sk** Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že AirLive MW-2000S spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo AirLive MW-2000S è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	**fi** Suomi [Finnish]	OvisLink Corp vakuuttaa täten että AirLive MW-2000S tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka AirLive MW-2000S atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að AirLive MW-2000S er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
sv Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna AirLive MW-2000S står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.	**no** Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret AirLive MW-2000S er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

A copy of the full CE report can be obtained from the following address:

OvisLink Corp.
5F, No.6 Lane 130,
Min-Chuan Rd, Hsin-Tien City,
Taipei, Taiwan, R.O.C.

This equipment may be used in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, SK, SI, ES, SE, GB, IS, LI, NO, CH, BG, RO, TR

Table of Contents

Chapter 1. Before You Start

1.1 Audience

This manual is intended for the system or network administrators with the networking knowledge to complete the step by step instructions of this manual in order to use the MW-2000S for a better management of network system and user data.

1.2 Document Convention

- For any caution or warning that requires special attention of readers, a highlight box with the eye-catching italic font is used as below:

Warning: *For security purposes, you should immediately change the Administrator's password.*

⌂ indicates that clicking this button will return to the homepage of this section.

↑ indicates that clicking this button will return to the previous page.

✓ Apply indicates that clicking this button will apply all of your settings.

✕ Clear indicates that clicking this button will clear what you set before these settings are applied.

Chapter 2. System Overview

2.1 Introduction of MW-2000S

Thank you for purchasing AirLive Hotspot Management Gateway MW-2000S.

MW-2000S is a Hotspot Management Gateway, dedicatedly designed for small to medium-sized wireless network deployment and management, making it an ideal solution for easily managing the Hotspot service. With its user management features, administrators will be able to manage the whole process of wireless network access. In addition, Access Point (AP) management functions allow administrators to discover, configure, update, and monitor all managed APs from a single secured interface, and from there, gain full control of the entire wireless network.

2.2 System Concept

MW-2000S is capable of managing user authentication, authorization and accounting. The user account information is stored in the local database or a specified external databases server. Featured with user authentication and integrated with external payment gateway, MW-2000S allows users to easily pay the fee and enjoy the Internet service. With centralized AP management system, the administrator does not need to worry about how to maintain several wireless access point devices in a short time. The following diagram is an example of MW-2000S set to manage the Internet access service at a hotel.

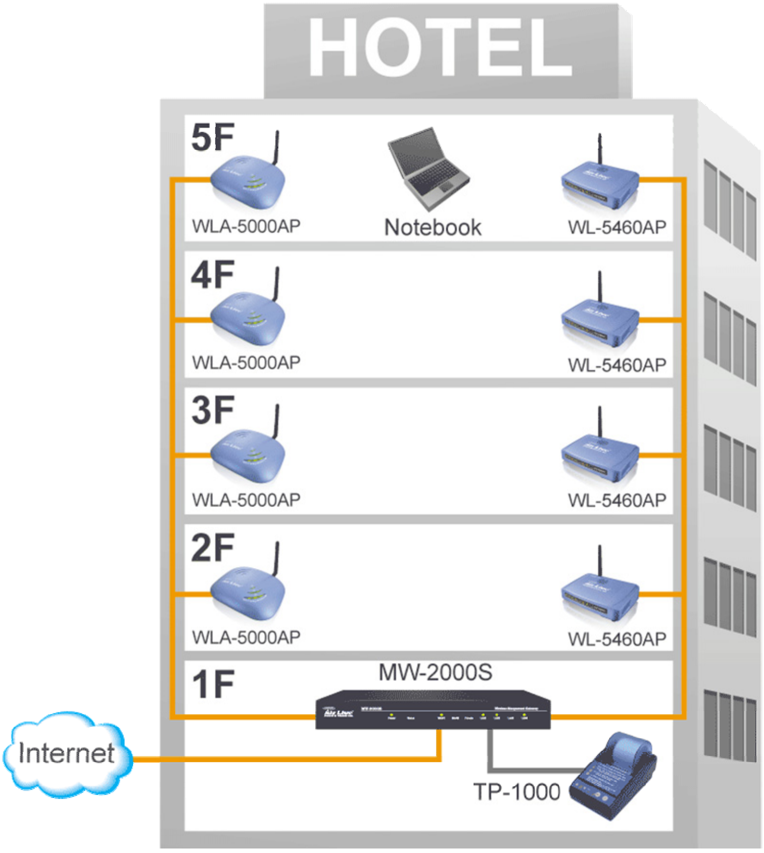


Figure-1: An example of managed network

2.3 Specification

2.3.1 Hardware Specification

- **General**
  Form Factor: Mini-desktop
  Dimensions (W x D x H): 235 mm x 161.9 mm x 37.6 mm
  Weight: 1Kg
  Operating Temperature: 0 ~ 40°C
  Storage Temperature: 20 ~ 70°C
  Power: 100~240 VAC, 50/60 Hz
  Ethernet Interfaces: 7 x Fast Ethernet (10/100 Mbps)
- **Connectors & Display**
  WAN Ports: 2 x 10BASE-T/100BASE-TX RJ-45
  Private Port: 1 x 10BASE-T/100BASE-TX RJ-45
  LAN Ports: 4 x 10BASE-T/100BASE-TX RJ-45
  Console Port: 1 x RS-232 DB9
  LED Indicators: 1 x Power, 1 x Status, 2 x WAN, 1 x Private, 4 x LAN

2.3.2 Software Specification

Hotspot Authentication

- **Instant Account**
  Administrator can define account type base upon price, usage time limit, or traffic limit. It supports up to 10 different accounts type, and user can select the type he wants to pay for Internet access, and then the information can be printed out on a conventional printer, or to the ticket printer TP-1000S. Up to 2000 on-demand accounts can be generated and the concurrent users can be up to 120.

- **Web Trigger Authentication**
  When user opens the web browser, the MW-2000S will switch a window asking you to enter user name and password. The login window can be customized to put company's logo or art design.

- **Payment System**
  MW-2000S is featured with Authorize.Net and PayPal billing system, so that users can easily pay the fee with credit cards or PayPal accounts for the Internet access.

- **Personal Bandwidth Control**
  When you construct the environment for public Internet access, it is necessary to restrict user's access bandwidth in order to keep up the access speed of else users. MW-2000S features Individual Maximum Bandwidth and Individual Request Bandwidth to remain each user's access speed. It also features Maximum Concurrent Sessions to limit the access sessions, in order to avoid the bandwidth occupied by virus or P2P software to spread out lots of sessions.

- **WAN Load Balance and Fail-over**
  Built-in with 2 WAN interfaces, MW-2000S features WAN Load Balance and Fail-over function to enlarge useful bandwidth and keep up the Internet connection.

- **Customized Template Page**
  The Login and Logout page can be customized to change text / background color, the text contents, insert your own logo, and switch background image. The preview function can help user easily to adjust the page.

- **Traffic History and Session Log**
  MW-2000S features daily and monthly report to calculate the network access statistics of users; Session Log function records Source IP/MAC address, Destination IP/MAC address, port number, account name, and the time.

> ***Note:*** *Please refer to the following chapter and learn more configurations to accomplish the Hotspot environment:*
> ***Chapter 3.2*** *– Quick Software Configuration*
> ***Chapter 7.1*** *– System Configuration*
> ***Chapter 7.2*** *– User Authentication*
> ***Appendix B*** *– An Example of User Login*
> ***Appendix D*** *– Accepting Payment via Authorize.net*
> ***Appendix E*** *– Accepting Payment via PayPal*
> ***Appendix F*** *– Examples of Making Payment for End Users*
> ***Appendix H*** *– Customizable Pages*

AP Management

- **Auto AP Discovery**
  Keep your AP in the factory default configuration, and connect it to the MW-2000S. Then press “Auto Discover” and the MW-2000S will find all the APs for you.

- **Auto IP Address Assignment**
  After APs are discovered, MW-2000S will assign different IP address to each AP automatically.

- **Template Configuration**
  Default configurations for the AP can be defined in a template profile. So after an AP is discovered by the security gateway, you can apply the configuration template to each AP. You no longer have to configure each AP independently. Up to 3 configurations template can be defined.

- **View AP Status**
  View the wireless and LAN status and Disable or Enable each AP.

- **Detailed Configuration**
  Configure all the AP’s function from the MW-2000S web management interface.

- **Keep Alive Status**
  Up to 40 IP addresses can be set in the Keep Alive status function, so when one network device is down, the administrator would receive email about this event.

> ***Note:*** *MW-2000S* ***v2.00 build 900*** *version firmware currently works with* ***WL-5460AP e10.1*** *firmware, and* ***WLA-5000AP v2.00e12*** *firmware. Please download the firmware from our website (http://www.airlive.com) if you do not have the correct firmware installed on WL-5460AP or WLA-5000AP. We will also announce the updated information in AirLive website if the available firmware is changing.*

> ***Note:*** *Please refer to the following chapter and learn more configurations to accomplish the AP Management setting.*
> ***Chapter 7.3*** *– AP Management*

Service Zones

- **Co-work with WLA-5000AP**
  With WLA-5000AP Multiple SSID function, MW-2000S can create and configure Multi-Service Zones.

- **Isolate Service Zones**
  With VLAN, Multiple SSID and Policy setting, MW-2000S can separate the Service Zones from being accessed with each other.

- **Standalone Authentication system and customized template page**
  Each service zone can have its own settings:
  - NAT or router mode
  - Enable or disable DHCP service, and define DHCP address range
  - Enable or disable authentication
  - Type of authentication options (Local, LDAP, RADIUS, …)
  - Customized the Login, Logout, Redirected web page
  - Default Policy (Firewall rule, Specific route, Schedule, and Bandwidth)
  - Wireless Setting, SSID, and wireless security

Note: *Please refer to the following chapter and learn more configurations to accomplish the Service Zones setting.*
Chapter 5 *– Multi-Service Providers*
Chapter 6 *– Multi-Service Zones*
Chapter 7.1.7 *– Service Zones*
Appendix C *– A Deployment Example of Service Zones*

Local VPN

Data encryption means to encode the data so that confidential information can not be stolen by intruder. Since wireless data can be received by anyone with a wireless device, the data encryption is even more important. The current solution require administrator to set wireless encryption key on the wireless device. The problem with this implementation is that when the key is known to one user, the entire network security is in jeopardy. The Local VPN is the perfect solution to this problem. It is achieved in 5 easy steps.

- Each user will be given a different account with username and password.
- When user tries to access the network, a window will pop up to ask for the account information.
- After user enters the correct password, the MW-2000S will download an ActiveX VPN client into the user's PC.
- The VPN key is automatically assigned, the end user does not need to do anything.
- After the account expired, the user will not be able to access the network anymore.

Note: *Please refer to the following chapter and learn more configurations to accomplish the Local VPN setting.*
Chapter 7.4.8 *– VPN Configuration*
Chapter 7.2.1.1 ~ 7.2.1.5 *– Authentication Method (Local, POP3, RADIUS, LDAP, NT Domain)*
Appendix G *– Local VPN*

Note: *On-demand and SIP Authentication Method are not supported Local VPN function.*

Chapter 3. Base Installation

3.1 Hardware Installation

3.1.1 System Requirements

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

3.1.2 Package Contents

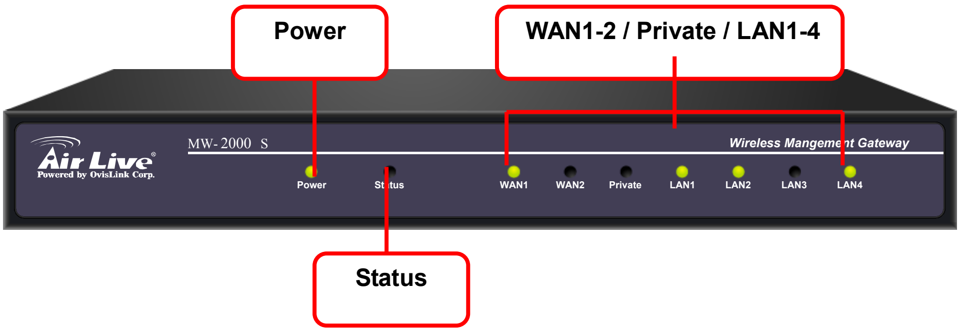
The standard package of MW-2000S includes:

- MW-2000S x 1
- CD-ROM x 1
- Quick Installation Guide x 1
- Power Adaptor (DC 5V) x 1
- Cross-over Ethernet Cable x 1
- Straight-through Ethernet Cable x 1
- Console Cable x 1

Warning: *Using a power supply with different voltage rating will damage this product.*

3.1.3 Panel Function Descriptions

Front Panel


Power
WAN1-2 / Private / LAN1-4
Air Live
Powered by OvisLink Corp.
MW-2000 S
Wireless Mangement Gateway
Power
Status
WAN1
WAN2
Private
LAN1
LAN2
LAN3
LAN4
Status

LED: There are four kinds of LED, Power, Status, WAN and LAN, to indicate different status of the system.

- **Status:**
  - **For Normal Startup:**
    - **Flashing:** during system startup.
    - **Steady ON:** to indicate the system is in "Normal Operation" modes.
  - **In Reset Operation:**
    - **Flashing:** Status LED is flashing if the Reset button is pressed for more than 3 sec and released in less than 10 sec. When the Status LED starts flashing is the indication that the system has been successfully reset.
    - **Steady ON:** status LED will switch from flashing to steadily ON if the Reset button is pressed over 10 sec, it indicates that the system has been reset to factory default setting.

- **WAN1~2/Private/LAN1~4**
  - **Light blinking:** data packets are being transmitted or received.
  - **Light on:** linked/established Ethernet connection present.
  - **Light off:** no existing Ethernet port connections to MW-2000S.

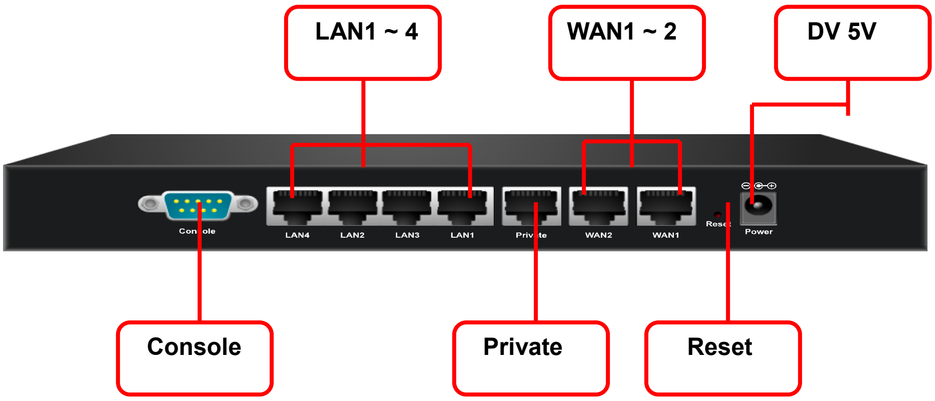
- **Power:**
  - **Light on:** The power is switched on.
  - **Light off:** no power connected.

WAN1/WAN2: The two WAN ports are connected to a network which is not managed by the AirLive MW-2000S system, and this port can be used to connect the ATU-Router of the ADSL, the port of a cable modem, or a switch or a hub on the LAN of a company.

LAN1~LAN4: Clients' machines connect to AirLive MW-2000S via LAN ports. Each LAN port can be configured to one of the two roles, controlled or uncontrolled. The differences of these two roles for a client connected to are:

- Clients connected to the controlled port need to be authenticated to access network.
- Clients connected to uncontrolled port don't need to be authenticated to access network and can access the web management interface.

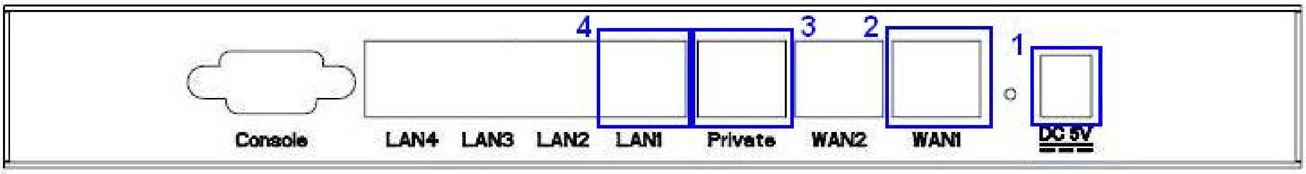
Rear Panel



- **Reset:** Press this button to restart the system.
- **Console:** The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft's HyperTerminal to login to the configuration console interface to change admin password or monitor system status, etc.
- **DC 5V:** The power adapter attaches here.
- **LAN1~4:** Connects to LAN1~4 port to access the network with authentication.
- **Private:** Connects to the private port to access the web management interface without authentication.
- **WAN1~2:** Connects to the Intranet or Internet by Switch.

3.1.4 Installation Steps

Please follow the following steps to install MW-2000S:



1. Connect the DC power adapter to the power connector socket on the rear panel. The Power LED should be on to indicate a proper connection.

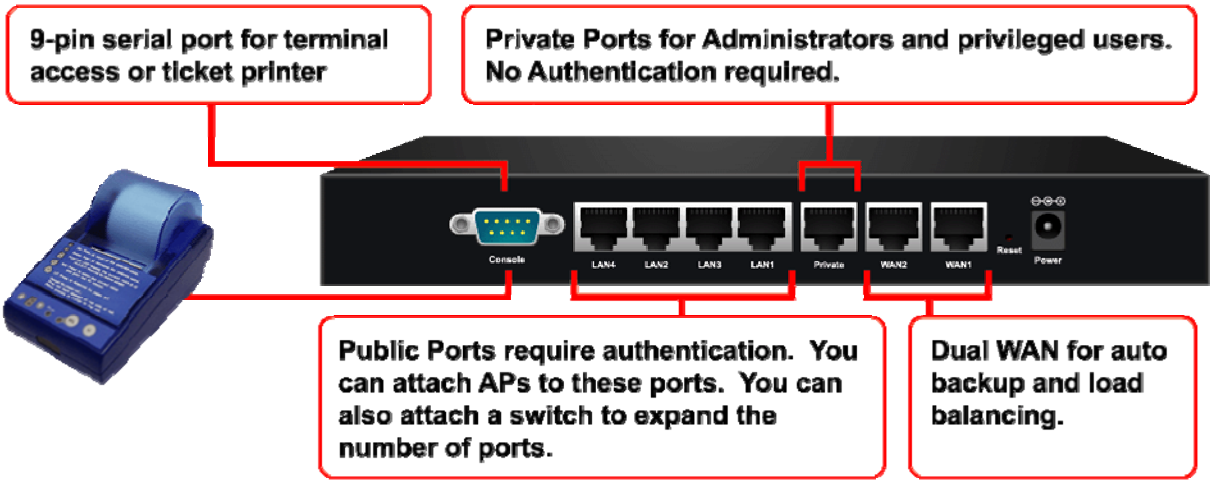
2. Connect an Ethernet cable to the WAN Port on the rear panel. Connect the other end of the Ethernet cable to ADSL modem, cable modem or a switch/hub of the internal network. The LED of this WAN port should be on to indicate a proper connection.

3. Connect an Ethernet cable to Private Port on the rear panel. Connect the other end of the Ethernet cable to a client's PC. The LED of Private Port should be on to indicate a proper connection. (**Note:** No authentication is required for the users to access the network via Private Port and the administrator can enter the administrative user interface to perform configurations via Private Port.)

4. Connect an Ethernet cable to the LAN1~LAN4 Port on the rear panel. Connect the other end of the Ethernet cable to an AP or switch. The LED of LAN1~LAN4 should be on to indicate a proper connection. (**Note:** Authentication is required for the users to access the network via these LAN Ports.)

> ***Attention:*** *Usually a straight-through cable could be applied when the MW-2000S connects to an Access Point which supports automatic crossover. If after the AP hardware resets, the MW-2000S could not be able to connect to the AP while connecting with a straight-through cable, the user have to pull out and plug-in the straight-through cable again. This scenario does NOT occur while using a crossover cable.*

After the hardware of MW-2000S is installed completely, the system is ready to be configured in the following sections.


9-pin serial port for terminal access or ticket printer

Private Ports for Administrators and privileged users. No Authentication required.

Public Ports require authentication. You can attach APs to these ports. You can also attach a switch to expand the number of ports.

Dual WAN for auto backup and load balancing.

3.2 Quick Software Configuration

There are two simple ways to configure the Hotspot system: **Instant Account** and **Configuration Wizard**.

3.2.1 Instant Account

MW-2000S provides three different level account; **admin**, **manager** and **operator**. The default username and password as follows:

Admin: The administrator can access all area of the AirLive MW-2000S.

User Name: **admin**
Password: **airlive**

Manager: The manager only can access the area under ***User Authentication*** to manager the user account, but no permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**
Password: **airlive**

Operator: The operator only can access the area of ***On-demand Account Creation*** to create and print out the new on-demand user accounts.

User Name: **operator**
Password: **airlive**

Each account owns the specific access right:
The network constructor can deploy the default system by **admin** account;
The system manager can change or create further authentication rule by **manager** account;
The operator just needs to create new account and print out the ticket for customer by **operator** account.

Following is the example to configure the system per different user account:
For admin account:

1. Select the Connection Type for WAN Port
2. Choose System's Time Zone
3. Configure Policy setting based on customer's request

For manager account:

1. Set up Authentication Configuration for on-demand User Server Configuration
2. Change Billing Configuration
3. Select the Policy to configure Traffic Class, Individual bandwidth for uplink and downlink, and also create Black list and Additional Configuration.

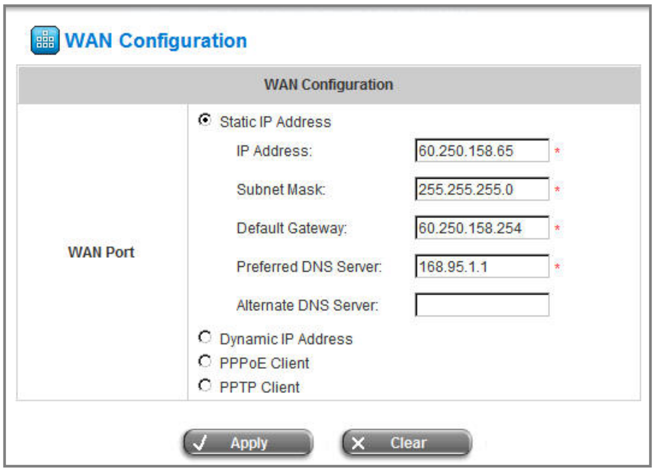
For operator account:

1. Create new account
2. Print out the ticket

Please check the following steps to complete the quick configuration

Login with admin account:

1. Select **System Configuration → WAN Configuration**, and set up the WAN type and enter the necessary data. For more detail information please check chapter 7.1.3 WAN configuration.



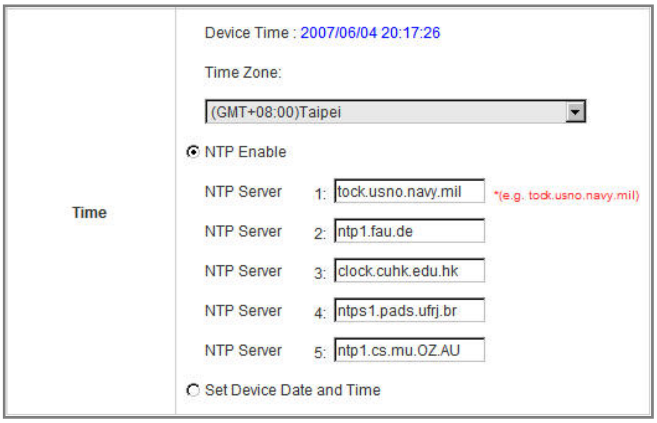
WAN Configuration

WAN Configuration

WAN Port

● Static IP Address
IP Address: 60.250.158.65 *
Subnet Mask: 255.255.255.0 *
Default Gateway: 60.250.158.254 *
Preferred DNS Server: 168.95.1.1 *
Alternate DNS Server:
○ Dynamic IP Address
○ PPPoE Client
○ PPTP Client

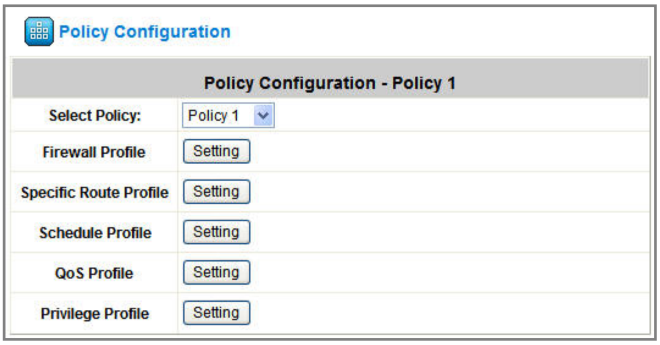
2. Select **System Configuration → System Information**, configure the correct Time Zone and select to enable NTP server or set up time by manually.



Time

Device Time : 2007/06/04 20:17:26
Time Zone:
(GMT+08:00)Taipei
● NTP Enable
NTP Server 1: tock.usno.navy.mil *(e.g. tock.usno.navy.mil)
NTP Server 2: ntp1.fau.de
NTP Server 3: clock.cuhk.edu.hk
NTP Server 4: ntps1.pads.ufrj.br
NTP Server 5: ntp1.cs.mu.OZ.AU
○ Set Device Date and Time

3. Select **User Authentication → Policy Configuration**, to define Policy 1 with configuring specific Firewall Profile, Route Profile, and Schedule Profile.

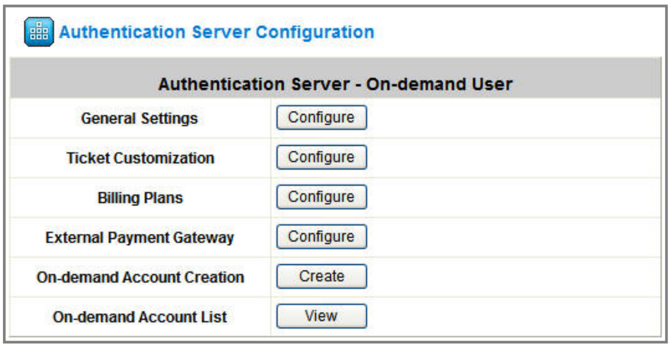


Policy Configuration

Policy Configuration - Policy 1	
Select Policy:	Policy 1
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

Login with manager account:

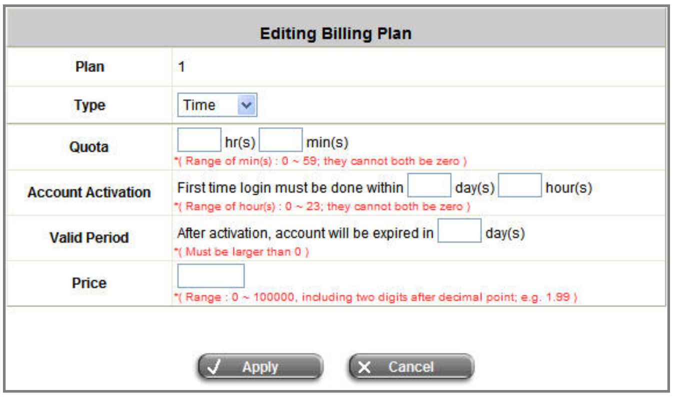
1. Select **User Authentication → Authentication Configuration → On-demand User**; in this item you can define General Settings, Ticket Customization, Billing Plans, External Payment Gateway, On-demand Account Creation, and On-demand Account List.



Authentication Server Configuration

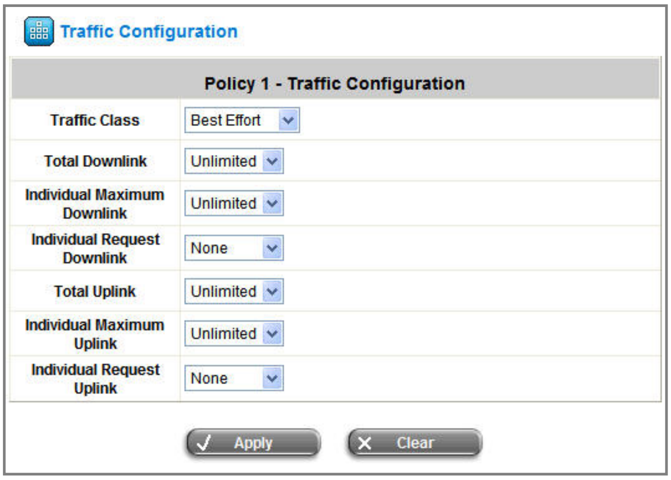
Authentication Server - On-demand User	
General Settings	Configure
Ticket Customization	Configure
Billing Plans	Configure
External Payment Gateway	Configure
On-demand Account Creation	Create
On-demand Account List	View

2. Select **User Authentication → Authentication Configuration → On-demand User → Billing Plans**, click **Edit** button to define the related information based on your policy. The contents include Pay for data or Pay for time, Account Activation, Account Valid Period, and price.



Editing Billing Plan	
Plan	1
Type	Time
Quota	hr(s) min(s) *(Range of min(s) : 0 ~ 59; they cannot both be zero)
Account Activation	First time login must be done within day(s) hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in day(s) *(Must be larger than 0)
Price	*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)

3. Select **User Authentication → Policy Configuration → QoS Profile**, and click **Setting** button to define **Traffic Class**, **Total Downlink**, **Individual Maximum Downlink**, **Individual Request Downlink**, **Total Uplink**, **Individual Maximum Uplink**, and **Individual Request Uplink**.

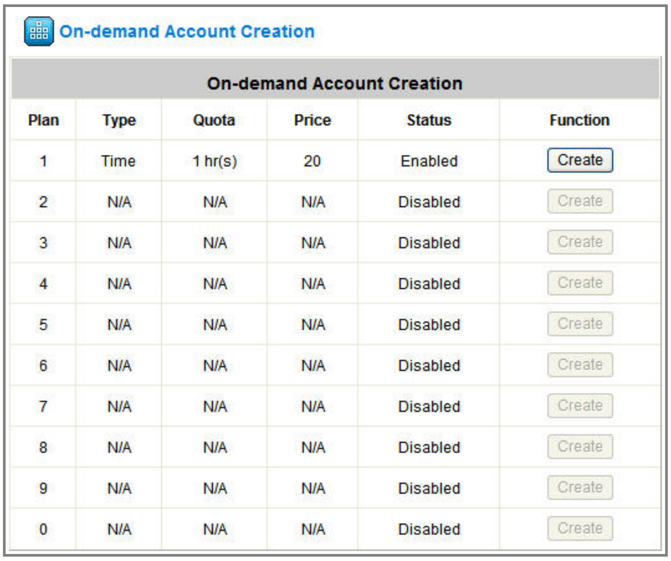


Traffic Configuration

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

Login with operator account:

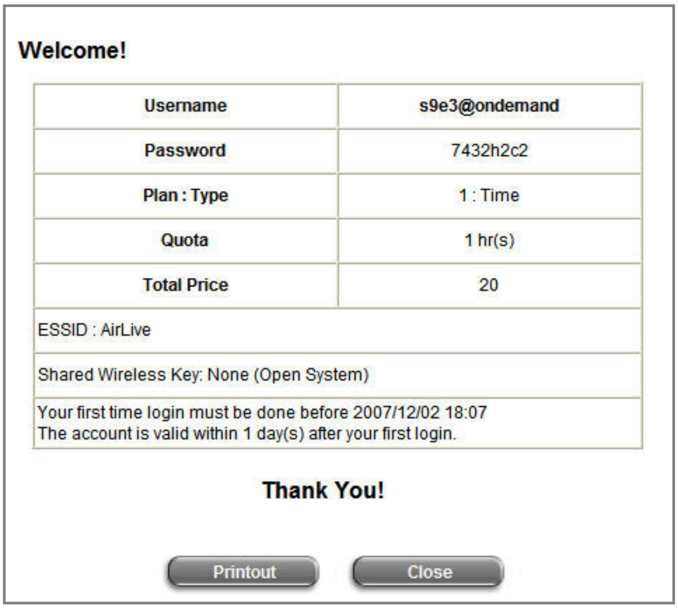
1. Click **Create** to create a new account.



On-demand Account Creation

Plan	Type	Quota	Price	Status	Function
1	Time	1 hr(s)	20	Enabled	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

2. Click **Printout** to print ticket.



Welcome!

Username	s9e3@ondemand
Password	7432h2c2
Plan : Type	1 : Time
Quota	1 hr(s)
Total Price	20

ESSID : AirLive

Shared Wireless Key: None (Open System)

Your first time login must be done before 2007/12/02 18:07
The account is valid within 1 day(s) after your first login.

Thank You!

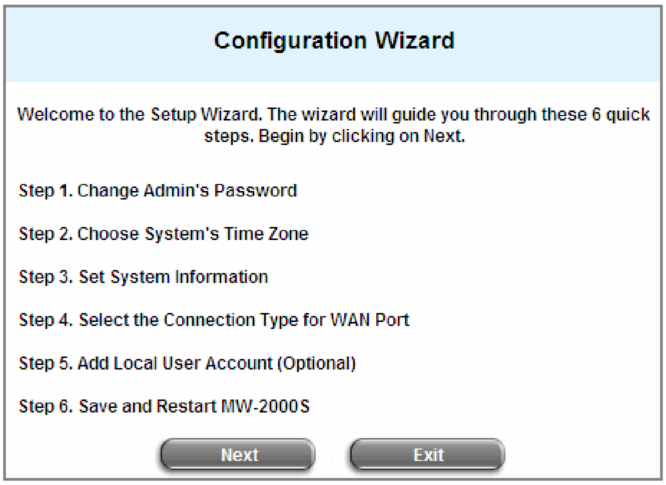
Following is the list to display the access right of MW-2000S feature per each account:

		admin	manager	operator
System Configuration		Y	--	--
User Authentication	Authentication Configuration	Y	Y	--
	Black List Configuration	Y	Y	--
	Policy Configuration	Y	Y	--
	Additional Configuration	Y	Y	--
Network Configuration		Y	--	--
Utility		Y	--	--
Status		Y	--	--

3.2.2 Configuration Wizard

MW-2000S provides **Configuration Wizard** for network administrators to quickly set up a basic system as a starting point to easily test the authentication and network connection. The **6** steps are listed below:

1. Change Admin's Password
2. Choose System's Time Zone
3. Set System Information
4. Select the Connection Type for WAN Port
5. Set Authentication Method
6. Save and Restart MW-2000S



Configuration Wizard

Welcome to the Setup Wizard. The wizard will guide you through these 6 quick steps. Begin by clicking on Next.

Step 1. Change Admin's Password

Step 2. Choose System's Time Zone

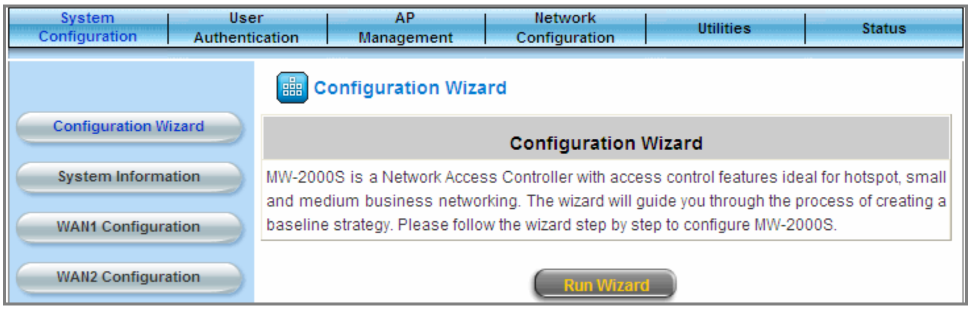
Step 3. Set System Information

Step 4. Select the Connection Type for WAN Port

Step 5. Add Local User Account (Optional)

Step 6. Save and Restart MW-2000S

Click the ***System Configuration*** from the top menu and the **System Configuration** page will appear. Then, click on ***Configuration Wizard*** and click the ***Run Wizard*** button to start the wizard.

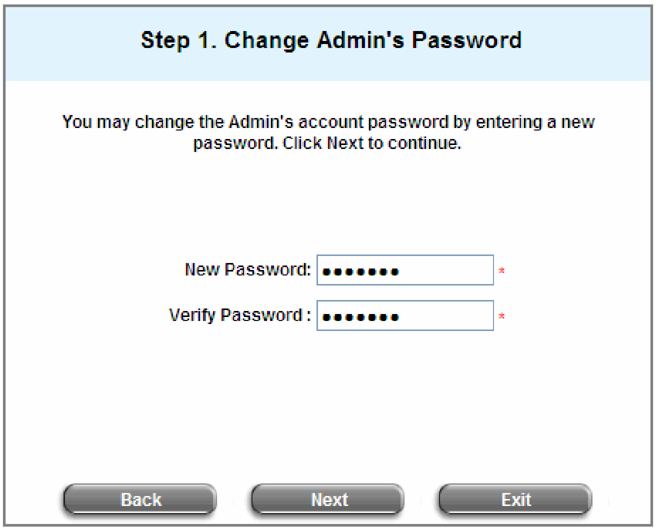


Configuration Wizard

MW-2000S is a Network Access Controller with access control features ideal for hotspot, small and medium business networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure MW-2000S.

- **Running the Wizard**
  First, a welcome screen that briefly introduces the 6 steps will appear. Click ***Next*** to begin after reviewing these steps.

- **Step 1: Change Admin's Password**
  Enter a new password for the admin account and retype it in the verifying password field (twenty-character maximum and no spaces). Click ***Next*** to continue.

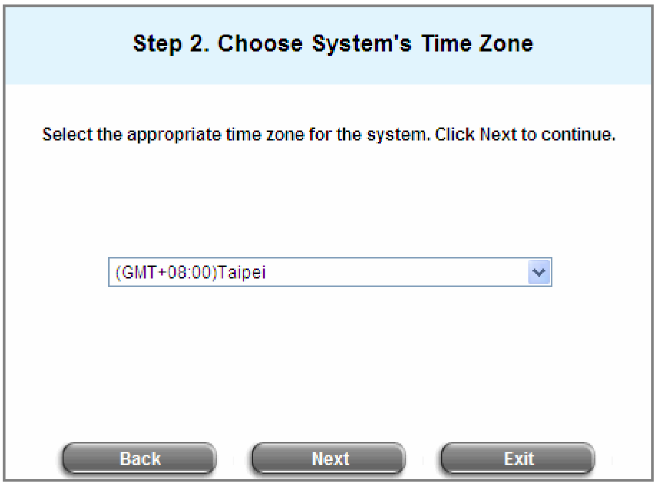


Step 1. Change Admin's Password

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

New Password: ••••••• *

Verify Password : ••••••• *



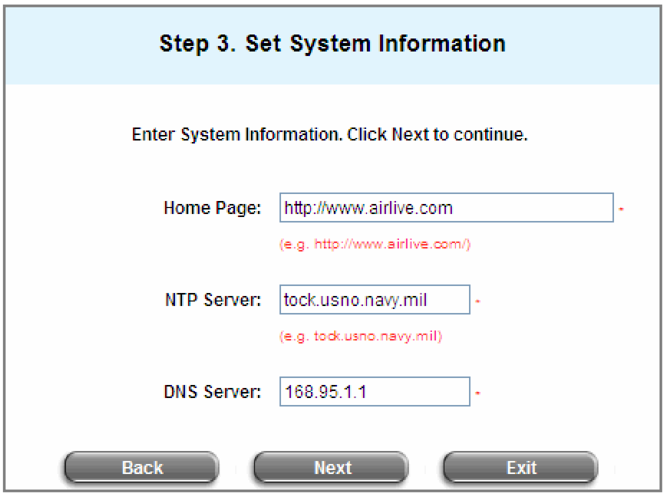
Step 2. Choose System's Time Zone

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

(GMT+08:00)Taipei

- **Step 2: Choose System's Time Zone**
  Select a proper time zone via the pull-down menu. Click ***Next*** to continue.

- **Step 3: Set System Information**
  Home Page: Enter the URL to where users should be directed when the user is successfully authenticated. A default address is supplied too.
  NTP Server: Enter the URL of external time server for MW-2000S time synchronization or use the default server address.
  DNS Server: Enter a DNS Server provided by the ISP (Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.
  Click ***Next*** to continue.



Step 3. Set System Information

Enter System Information. Click Next to continue.

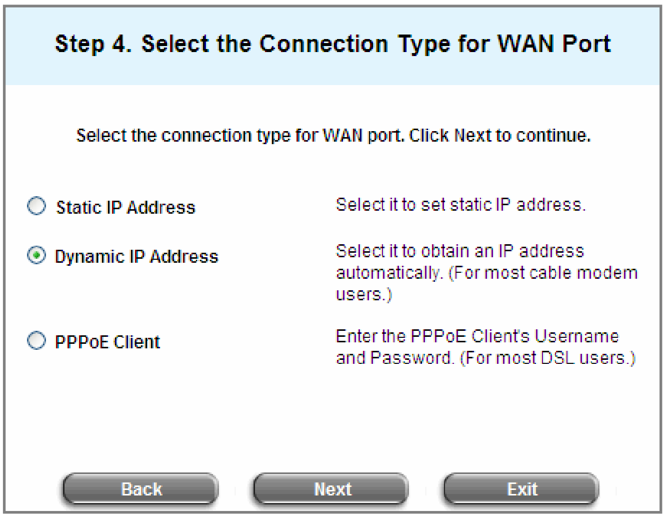
Home Page: http://www.airlive.com *
(e.g. http://www.airlive.com/)

NTP Server: tock.usno.navy.mil *
(e.g. tock.usno.navy.mil)

DNS Server: 168.95.1.1 *

- **Step 4: Select the Connection Type for WAN1 Port**
  There are three types of WAN ports that can be selected: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**. Select a proper Internet connection type and click ***Next*** to continue.

  ➢ **Dynamic IP Address**
  If this option is selected, an appropriate IP address and related information will automatically be assigned.
  Click ***Next*** to continue.



Step 4. Select the Connection Type for WAN Port

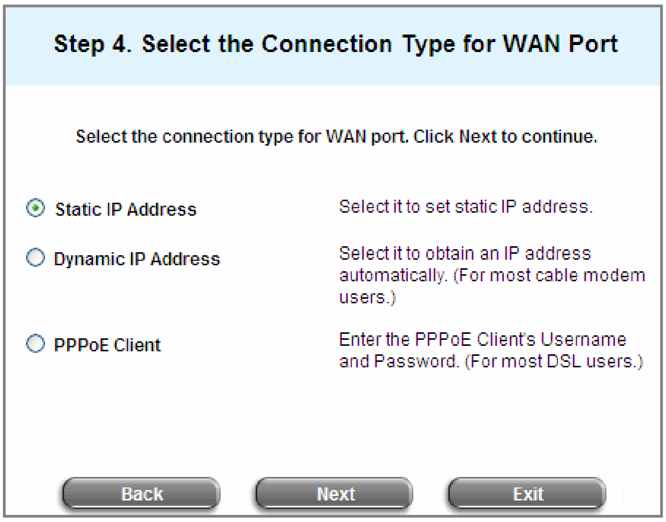
Select the connection type for WAN port. Click Next to continue.

○ Static IP Address — Select it to set static IP address.

● Dynamic IP Address — Select it to obtain an IP address automatically. (For most cable modem users.)

○ PPPoE Client — Enter the PPPoE Client's Username and Password. (For most DSL users.)

  ➢ **Static IP Address: Set WAN1 Port's Static IP Address**
  Enter the **"IP Address"**, **"Subnet Mask"** and **"Default Gateway"** provided by the ISP.
  Click ***Next*** to continue.



Step 4. Select the Connection Type for WAN Port

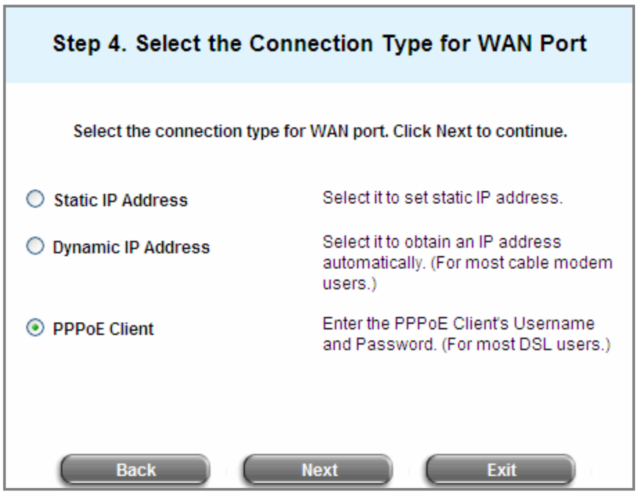
Select the connection type for WAN port. Click Next to continue.

● Static IP Address — Select it to set static IP address.

○ Dynamic IP Address — Select it to obtain an IP address automatically. (For most cable modem users.)

○ PPPoE Client — Enter the PPPoE Client's Username and Password. (For most DSL users.)

- **PPPoE Client: Set PPPoE Client's Information**
  Enter the **"Username"** and **"Password"** provided by the ISP.
  Click ***Next*** to continue.



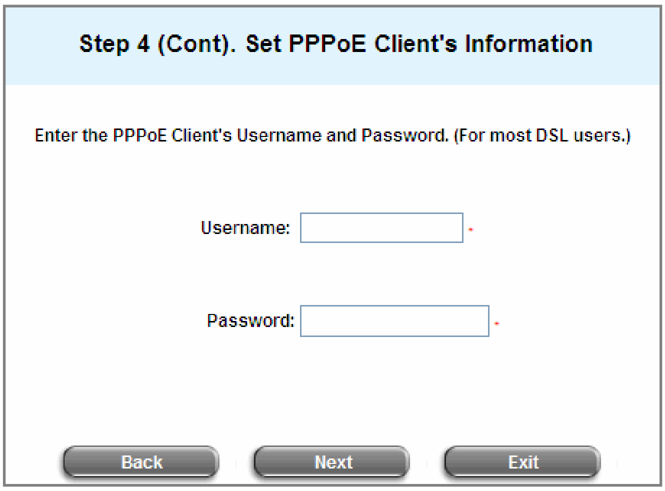
Step 4. Select the Connection Type for WAN Port

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

○ Static IP Address — Select it to set static IP address.

○ Dynamic IP Address — Select it to obtain an IP address automatically. (For most cable modem users.)

● PPPoE Client — Enter the PPPoE Client's Username and Password. (For most DSL users.)



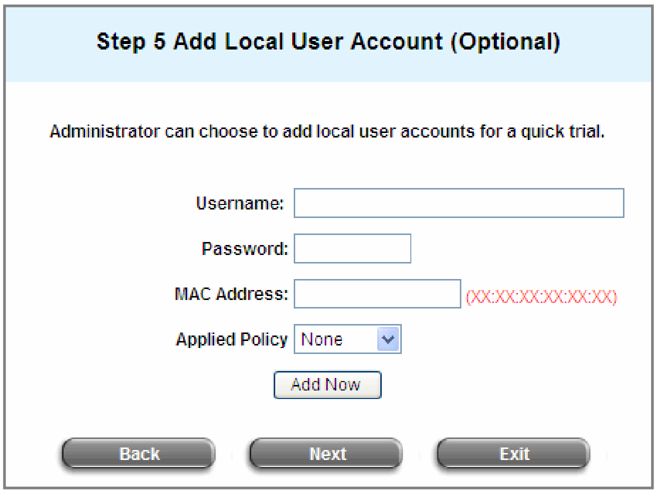
Step 4 (Cont). Set PPPoE Client's Information

Enter the PPPoE Client's Username and Password. (For most DSL users.)

Username: *

Password: *

- **Step 5: Step 5. Add Local User Account**
  A new user can be added to the local user data base. To add a user here, enter the ***Username*** (e.g. test), ***Password*** (e.g. test), ***MAC*** (optional, to specify the valid MAC address of this user) and assign it a policy (or use the default). Click the ***Add Now*** button to add the user. Multiple users can be added in this page. Click ***Next*** to continue.



Step 5 Add Local User Account (Optional)

Administrator can choose to add local user accounts for a quick trial.

Username:

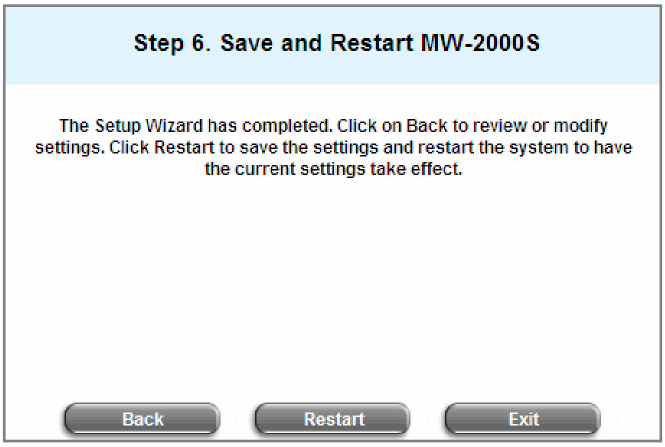
Password:

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

Applied Policy None

Note: *The policy selected in this step is applied to this user only. Per-user policy setting takes over the group policy setting at previous step unless you select None here.* Click ***Next*** to continue.

- **Step 6. Save and Restart MW-2000S**
  Click ***Restart*** to save the current settings and restart MW-2000S. The Setup Wizard is now completed. Click ***Restart*** to continue.



Step 6. Save and Restart MW-2000S

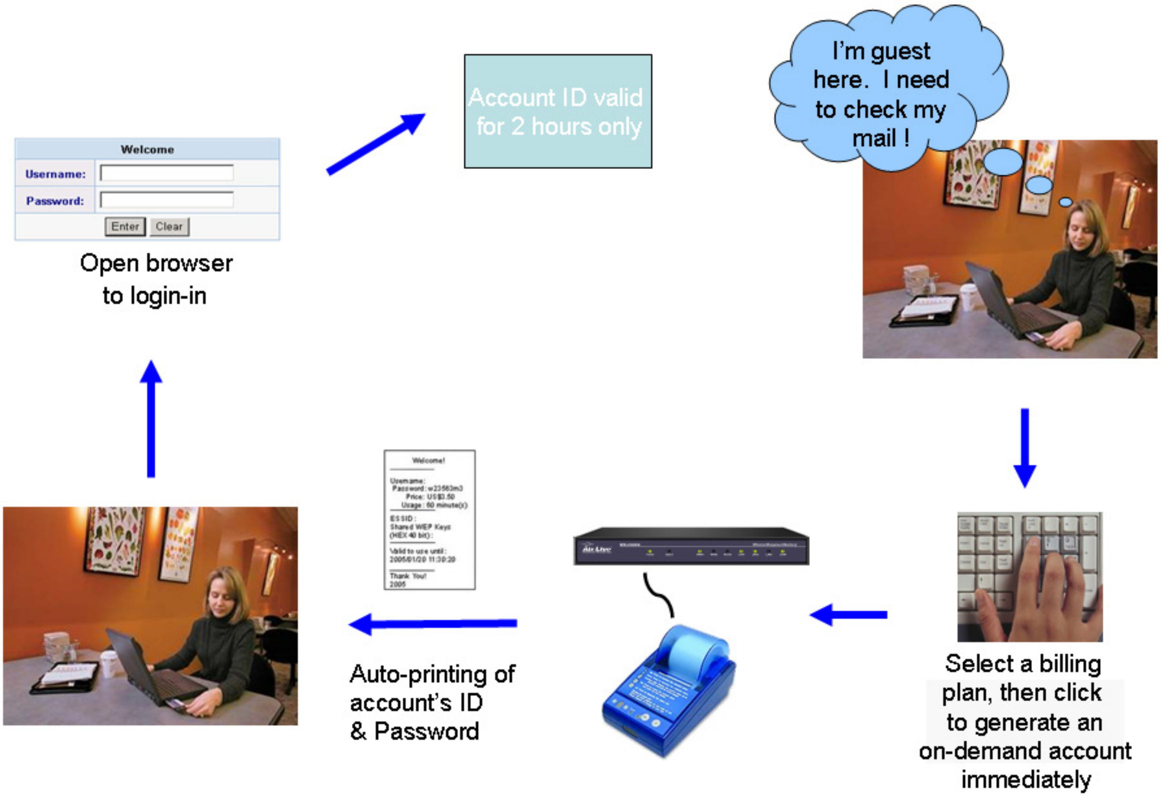
The Setup Wizard has completed. Click on Back to review or modify settings. Click Restart to save the settings and restart the system to have the current settings take effect.

- **Restart:** When MW-2000S is restarting, a **"Restarting now. Please wait for a moment."** message will appear on the screen. Please do not interrupt MW-2000S until the message has disappeared. This indicates that a complete and successful restart process has finished.

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

Chapter 4. Basic Hotspot Configuration

This chapter will guide user to install basic Hotspot function step by step, so user can realize how to install and configure MW-2000S. If user needs to configure more MW-2000S feature, please check ***Chapter 7 Web Interface Configuration*** to know more detail information.


Welcome
Username:
Password:
Enter
Clear
Open browser to login-in
Account ID valid for 2 hours only
I'm guest here. I need to check my mail !
Welcome!
Username:
Password: w23563m3
Price: US$0.50
Usage : 60 minute(s)
ESSID :
Shared WEP Keys (HEX 40 bit) :
Valid to use until : 2005/01/20 11:30:20
Thank You! 2005
Auto-printing of account's ID & Password
Select a billing plan, then click to generate an on-demand account immediately

User can follow the steps to configure basic Hotspot setting:

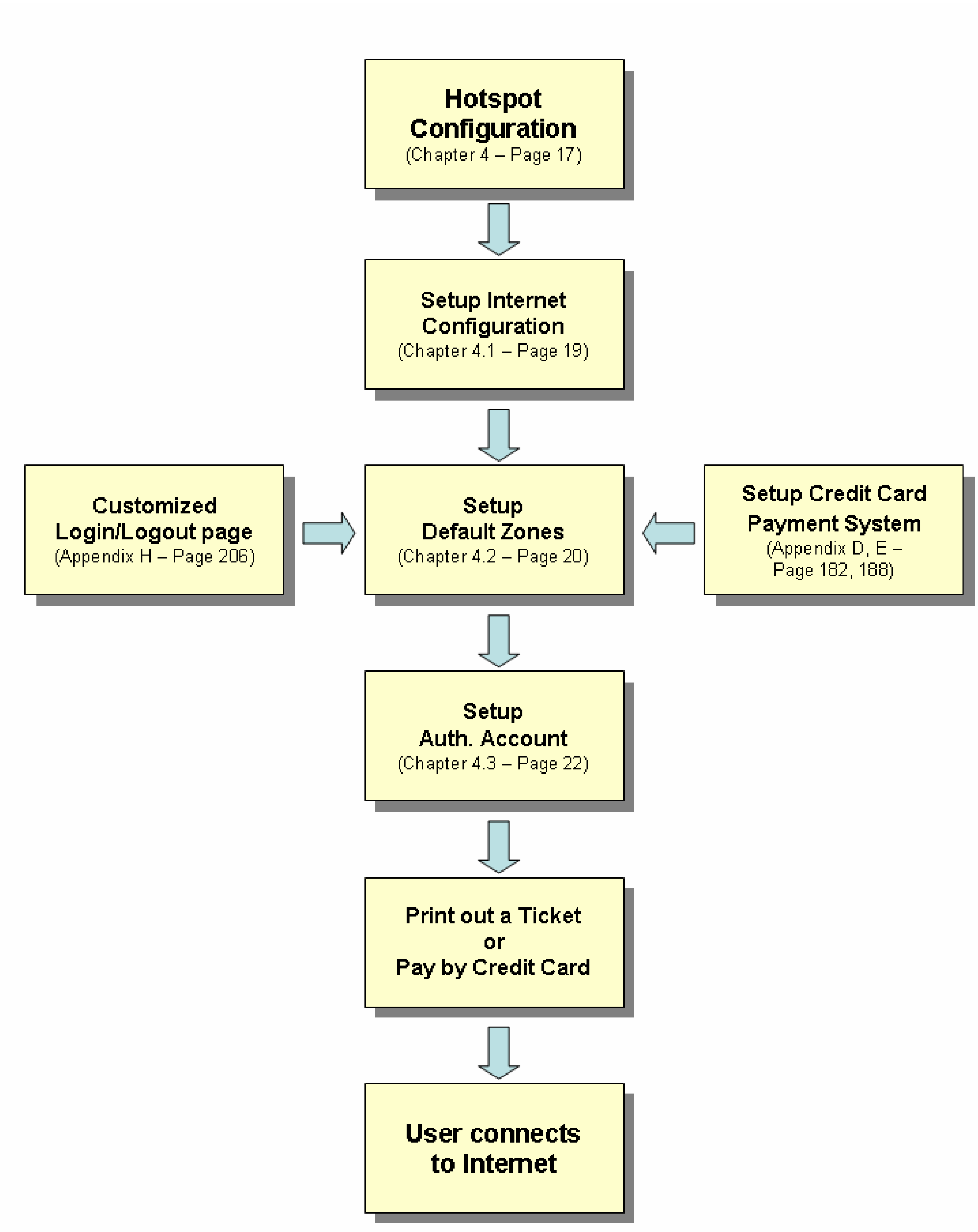
Chapter 4.1 – Setup Internet Connection

Chapter 4.2 – Setup Default Service Zone

Chapter 4.3 – Setup User Configuration

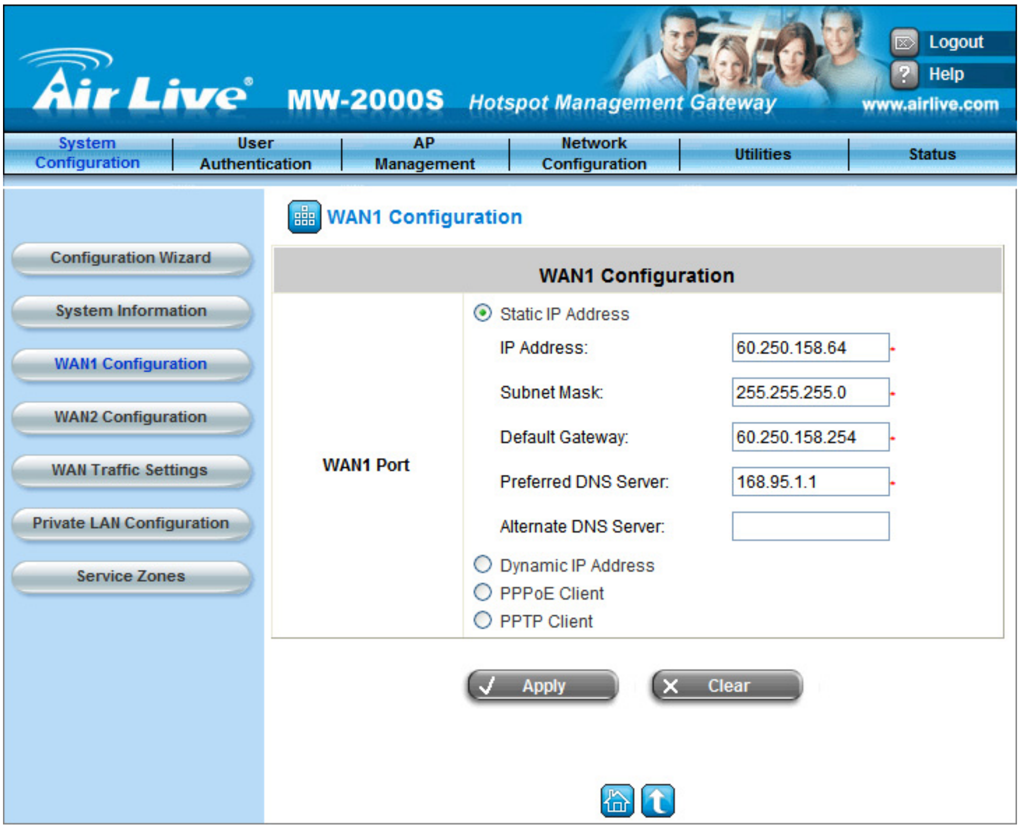
Chapter 4.4 – How to create On-demand account

Setup Flow:


Hotspot Configuration
(Chapter 4 – Page 17)
Setup Internet Configuration
(Chapter 4.1 – Page 19)
Customized Login/Logout page
(Appendix H – Page 206)
Setup Default Zones
(Chapter 4.2 – Page 20)
Setup Credit Card Payment System
(Appendix D, E – Page 182, 188)
Setup Auth. Account
(Chapter 4.3 – Page 22)
Print out a Ticket or Pay by Credit Card
User connects to Internet

4.1 Setup Internet Connection

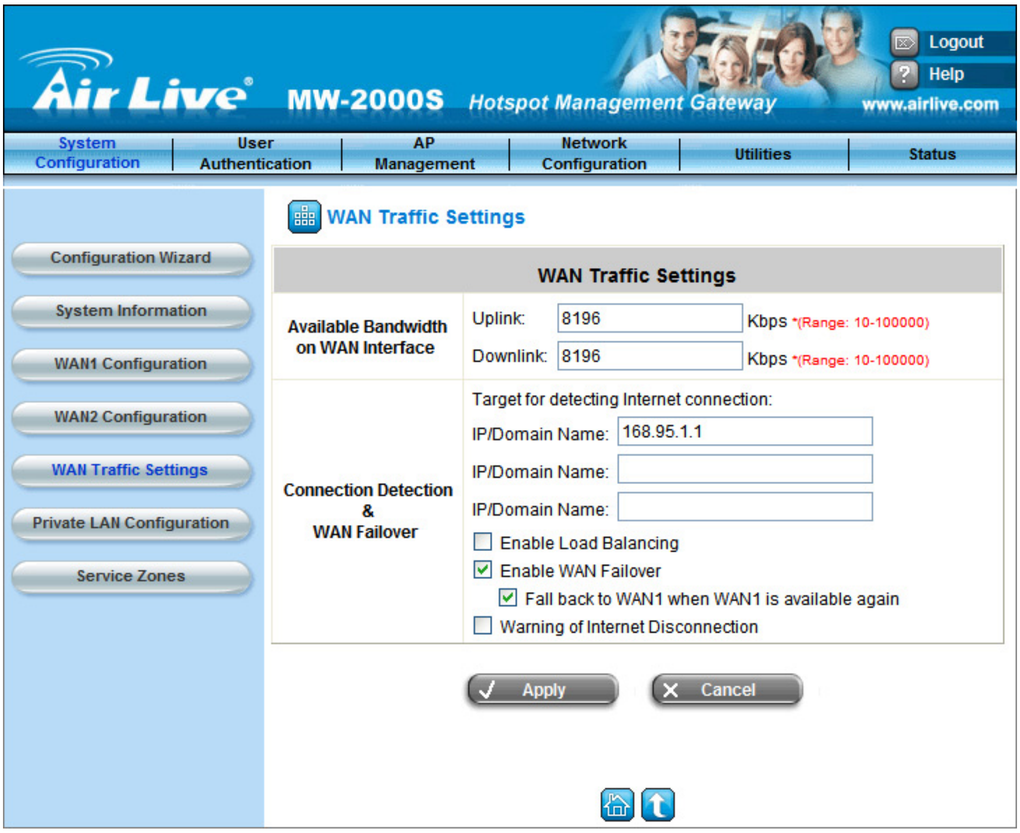
STEP 1 . Enter **System Configuration → WAN1 Configuration** to define the WAN connection. User can configure WAN connecting type with Static IP, Dynamic IP, PPPoE, or PPTP client based on the request.



WAN1 Configuration

WAN1 Configuration	
WAN1 Port	● Static IP Address IP Address: 60.250.158.64 Subnet Mask: 255.255.255.0 Default Gateway: 60.250.158.254 Preferred DNS Server: 168.95.1.1 Alternate DNS Server: ○ Dynamic IP Address ○ PPPoE Client ○ PPTP Client

STEP 2 . If user applies two Internet connections, the second line can be setup at WAN2, and enable Load balancing or Failover function at **WAN Traffic Setting**. For more information to configure WAN port setting, please check ***Chapter 7.1.3***, ***Chapter 7.1.4***, and ***Chapter 7.1.5***.

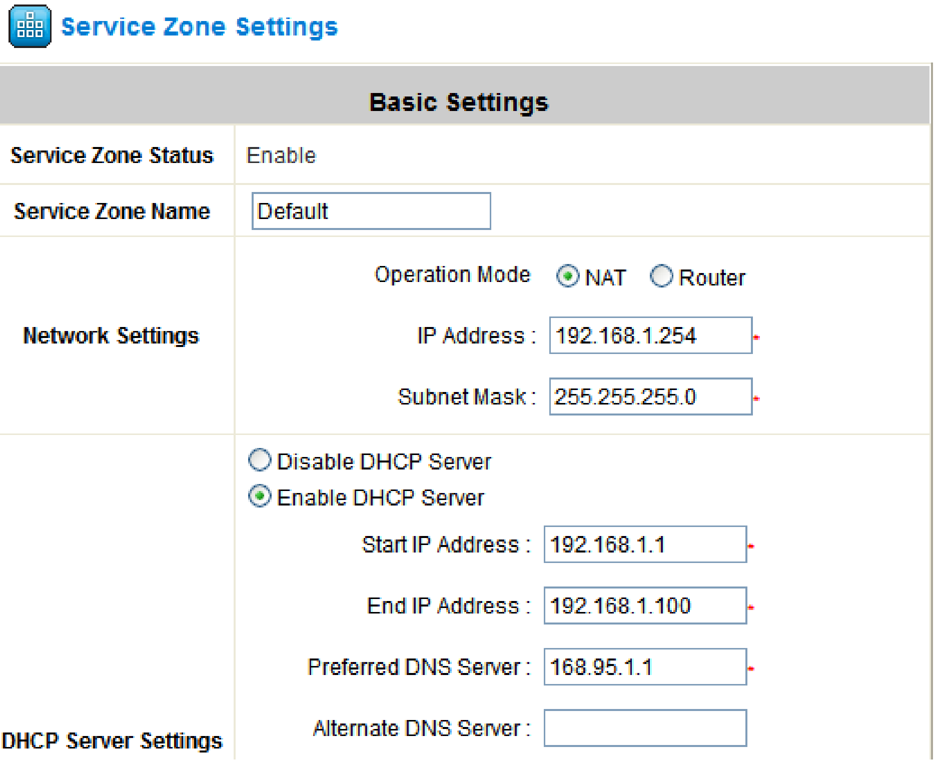


WAN Traffic Settings

WAN Traffic Settings	
Available Bandwidth on WAN Interface	Uplink: 8196 Kbps *(Range: 10-100000) Downlink: 8196 Kbps *(Range: 10-100000)
Connection Detection & WAN Failover	Target for detecting Internet connection: IP/Domain Name: 168.95.1.1 IP/Domain Name: IP/Domain Name: □ Enable Load Balancing ☑ Enable WAN Failover ☑ Fall back to WAN1 when WAN1 is available again □ Warning of Internet Disconnection

4.2 Setup Default Service Zones

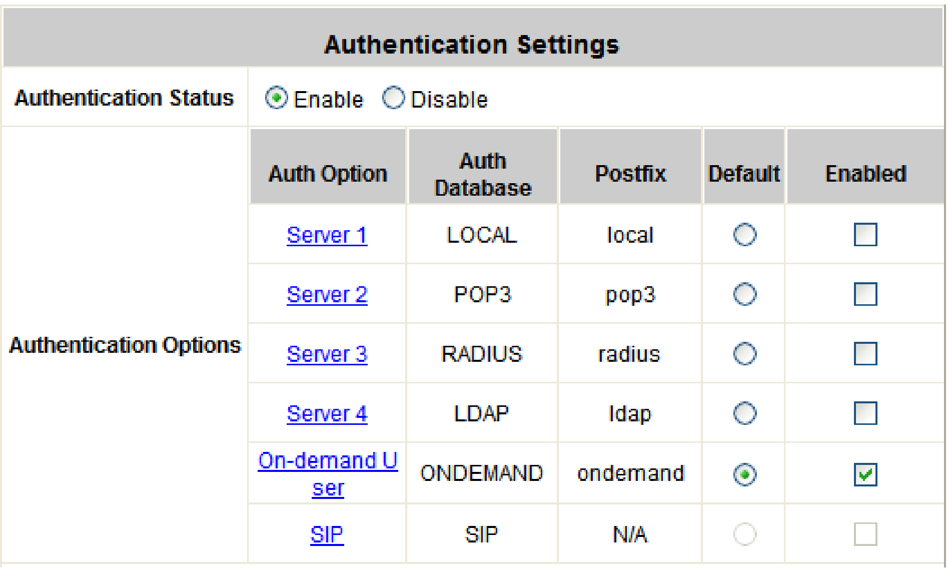
STEP 1 . **System Configuration → Service Zones:** If user does not configure specific Service Zones, each user will follow default zone. For more detail configuration please check **Chapter 7.1.7 Service Zones.**



Service Zone Settings

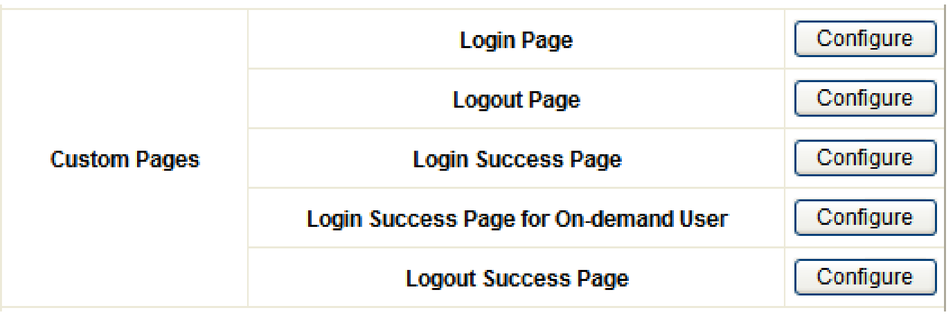
Basic Settings	
Service Zone Status	Enable
Service Zone Name	Default
Network Settings	Operation Mode ● NAT ○ Router IP Address : 192.168.1.254 Subnet Mask : 255.255.255.0
DHCP Server Settings	○ Disable DHCP Server ● Enable DHCP Server Start IP Address : 192.168.1.1 End IP Address : 192.168.1.100 Preferred DNS Server : 168.95.1.1 Alternate DNS Server :

STEP 2 . Select Authentication type as **On-demand User**.



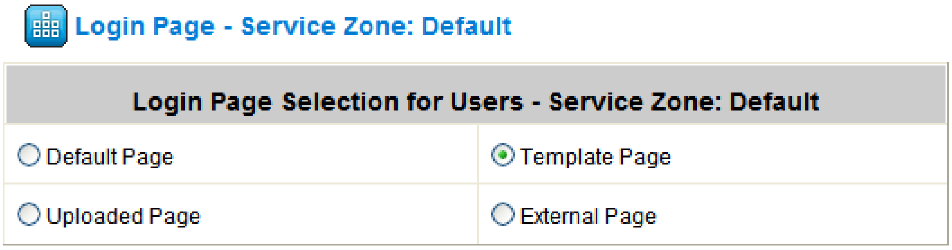
Authentication Settings					
Authentication Status	● Enable ○ Disable				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	○	□
	Server 2	POP3	pop3	○	□
	Server 3	RADIUS	radius	○	□
	Server 4	LDAP	ldap	○	□
	On-demand User	ONDEMAND	ondemand	●	☑
	SIP	SIP	N/A	○	□

STEP 3 . Customize the Login / Logout page. User can choose to use the default page, or use Template Page, Uploaded Page, or External Page to customize the page. For more detail information of customized page please check **Appendix H Customizable Pages**.



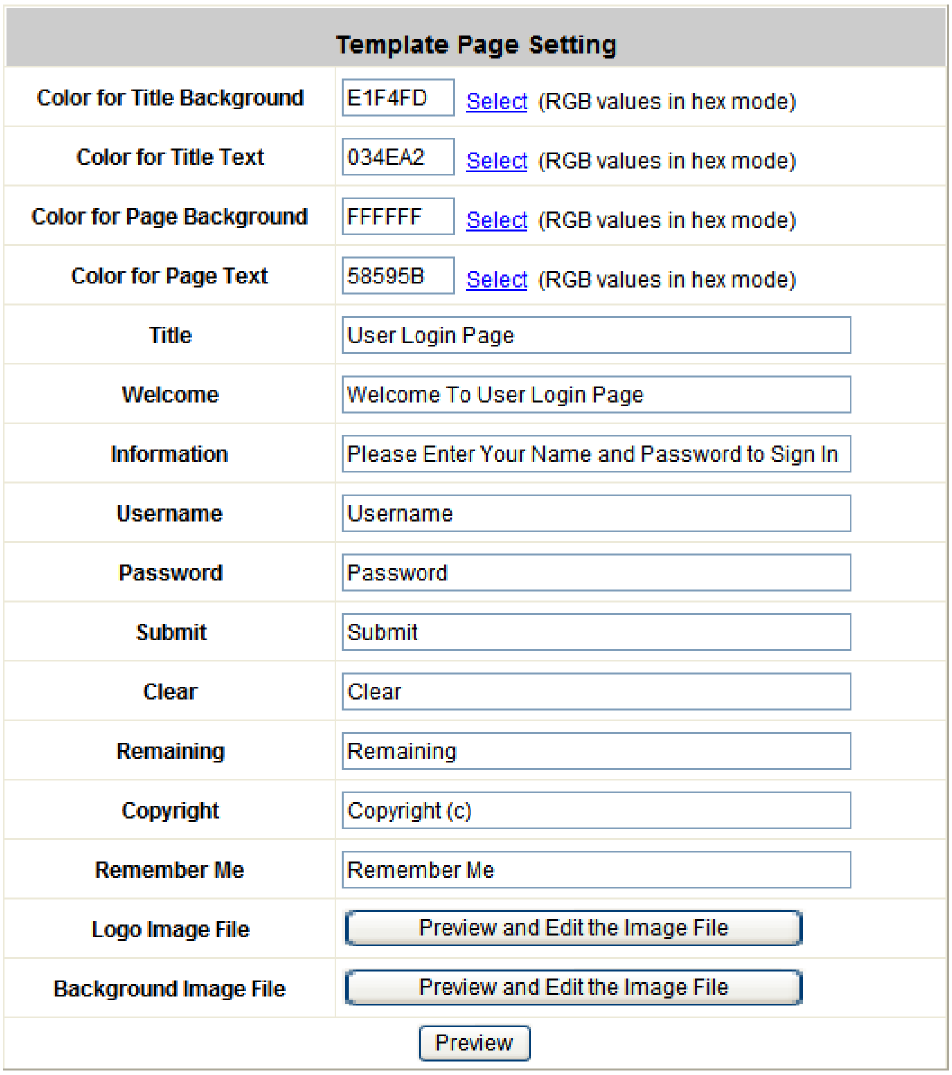
Custom Pages	Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Success Page for On-demand User	Configure
	Logout Success Page	Configure

STEP 4 . Take Template Page as example, user can select to design color of text and background, change the word of text and button, change logo, and replace the image file of background.



Login Page - Service Zone: Default

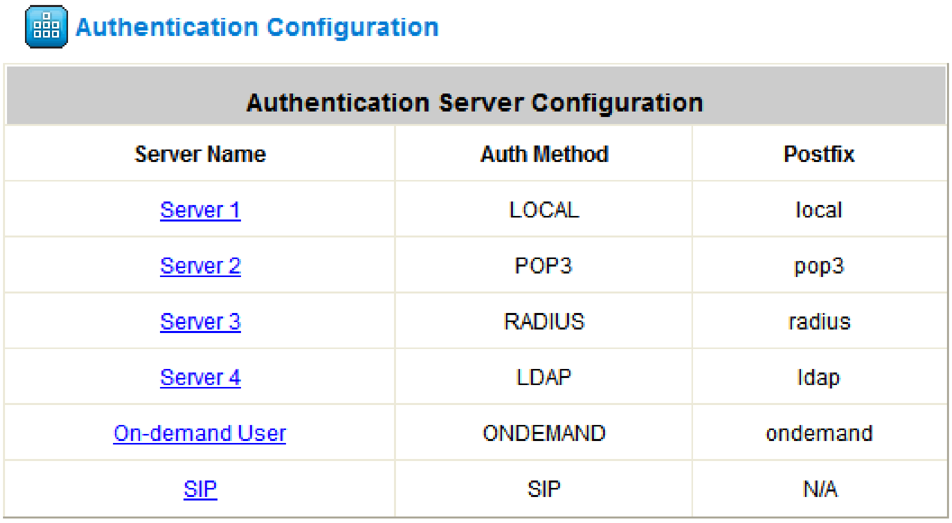
Login Page Selection for Users - Service Zone: Default	
○ Default Page	● Template Page
○ Uploaded Page	○ External Page



Template Page Setting	
Color for Title Background	E1F4FD Select (RGB values in hex mode)
Color for Title Text	034EA2 Select (RGB values in hex mode)
Color for Page Background	FFFFFF Select (RGB values in hex mode)
Color for Page Text	58595B Select (RGB values in hex mode)
Title	User Login Page
Welcome	Welcome To User Login Page
Information	Please Enter Your Name and Password to Sign In
Username	Username
Password	Password
Submit	Submit
Clear	Clear
Remaining	Remaining
Copyright	Copyright (c)
Remember Me	Remember Me
Logo Image File	Preview and Edit the Image File
Background Image File	Preview and Edit the Image File
Preview	

4.3 Setup Authentication Account

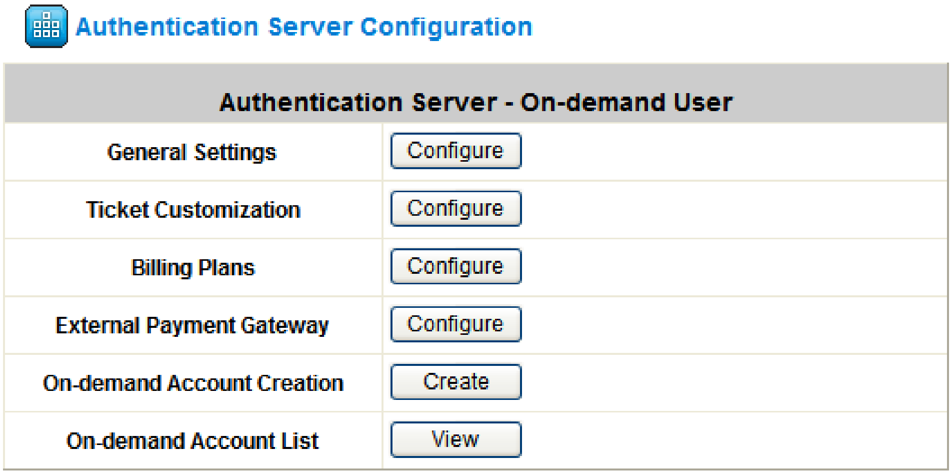
STEP 1 . Enter **User Authentication → Authentication Configuration**, select **On-demand User**.



Authentication Configuration

Authentication Server Configuration		
Server Name	**Auth Method**	**Postfix**
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

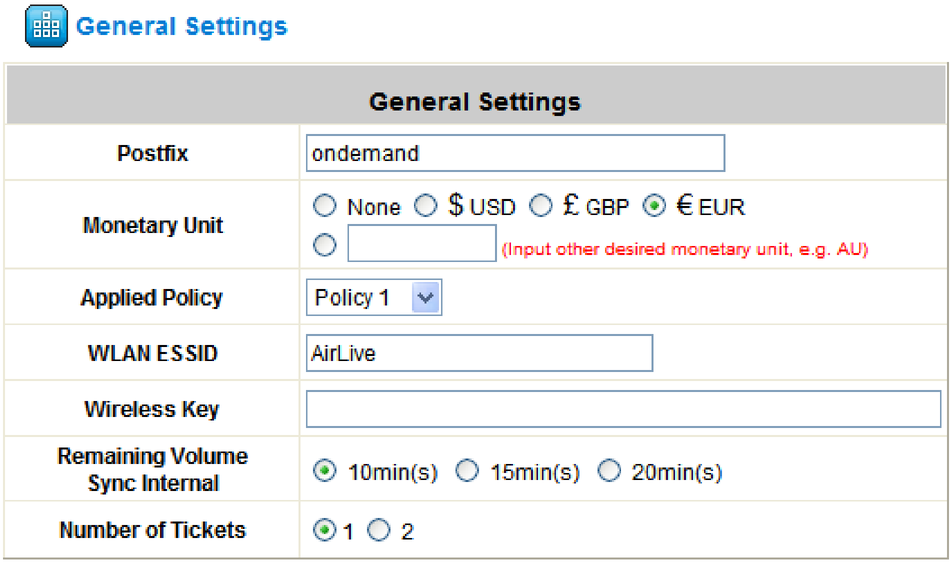
STEP 2 . User can configure the advanced feature at main page of Authentication Server.



Authentication Server Configuration

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 List	View

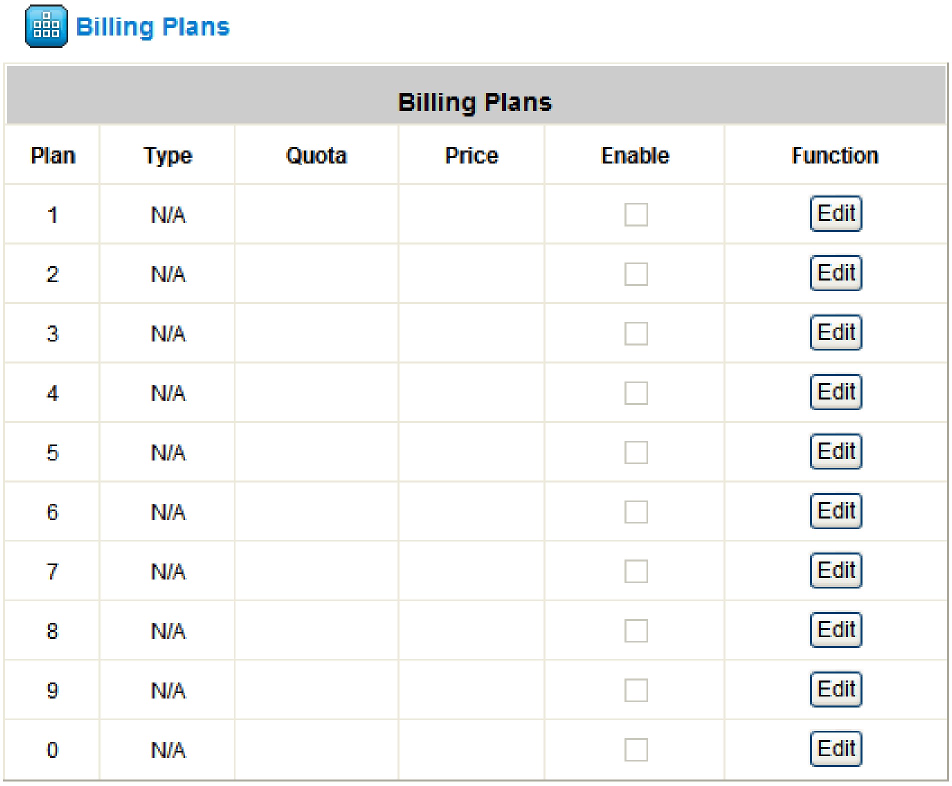
STEP 3 . Click **Configure** button of **General Settings** and change **Monetary Unit** to EUR.



General Settings

General Settings	
Postfix	ondemand
Monetary Unit	○ None ○ $ USD ○ £ GBP ● € EUR ○ (Input other desired monetary unit, e.g. AU)
Applied Policy	Policy 1
WLAN ESSID	AirLive
Wireless Key	
Remaining Volume Sync Internal	● 10min(s) ○ 15min(s) ○ 20min(s)
Number of Tickets	● 1 ○ 2

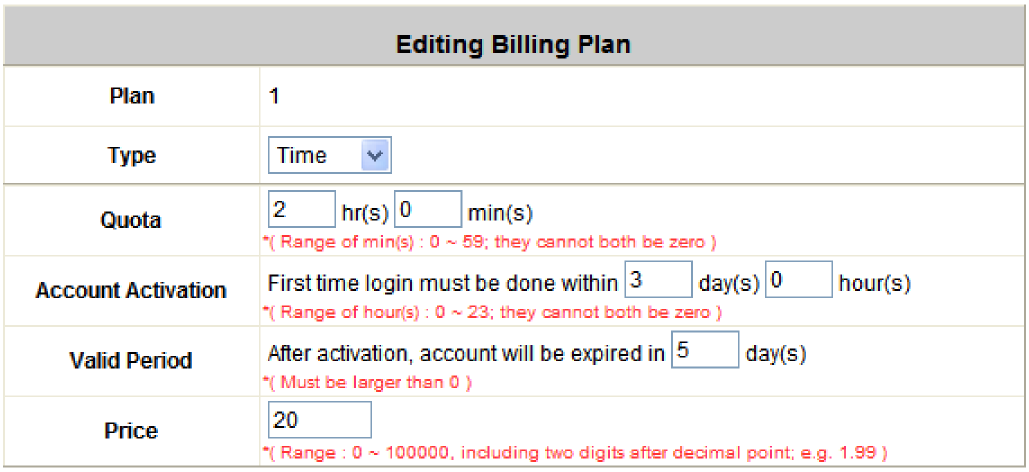
STEP 4 . Back to **Authentication Server Configuration** page, click **Configure** button of **Billing Plans** to create the billing plans.



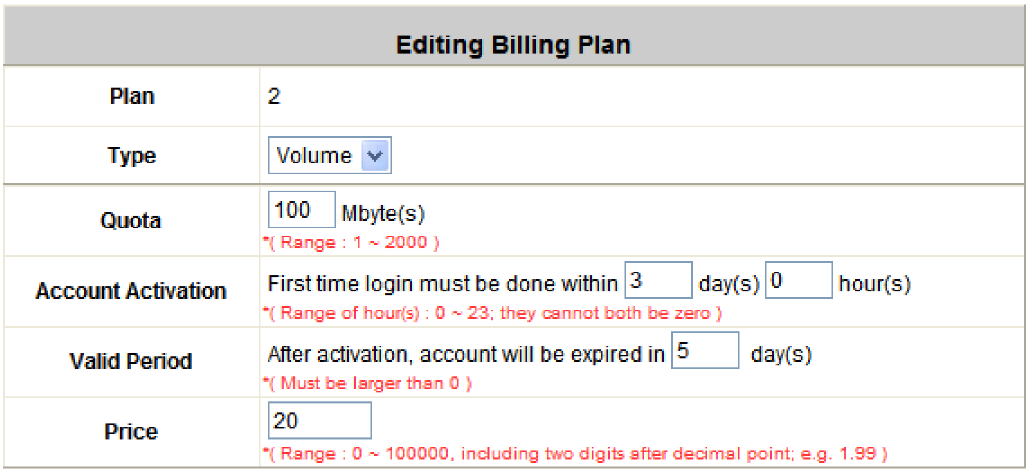
Billing Plans

Billing Plans					
Plan	Type	Quota	Price	Enable	Function
1	N/A			□	Edit
2	N/A			□	Edit
3	N/A			□	Edit
4	N/A			□	Edit
5	N/A			□	Edit
6	N/A			□	Edit
7	N/A			□	Edit
8	N/A			□	Edit
9	N/A			□	Edit
0	N/A			□	Edit

STEP 5 . Create two plans with **Time** and **Volume** type, specify the Quota and expired time, and then click **Apply** to save the configuration.

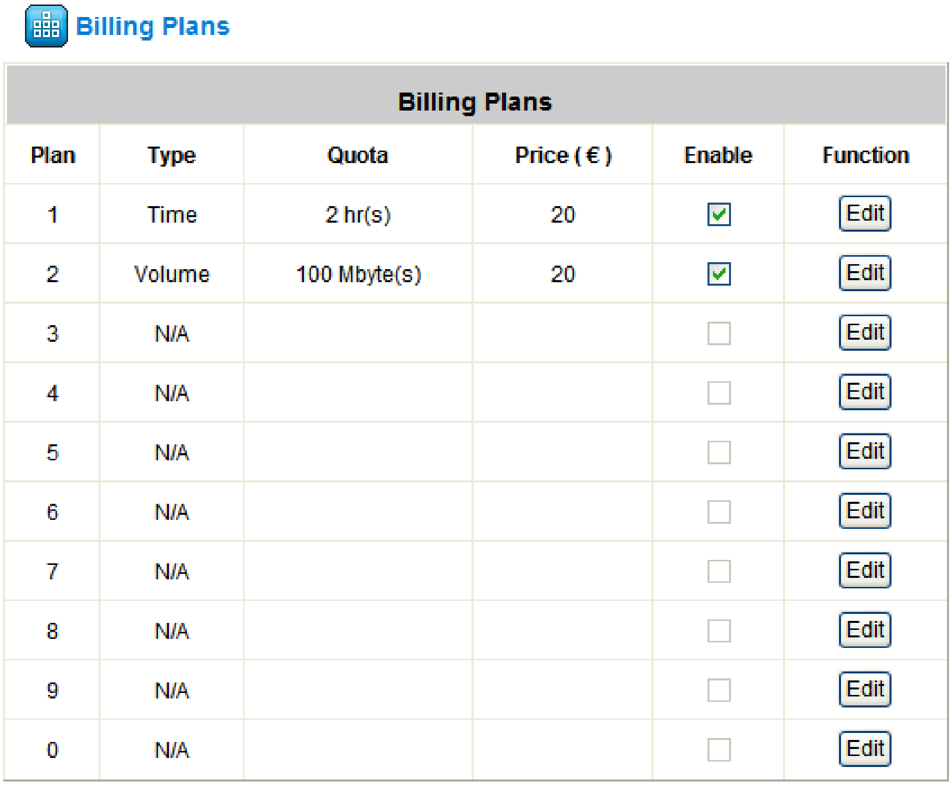


Editing Billing Plan	
Plan	1
Type	Time
Quota	2 hr(s) 0 min(s) *(Range of min(s) : 0 ~ 59; they cannot both be zero)
Account Activation	First time login must be done within 3 day(s) 0 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 5 day(s) *(Must be larger than 0)
Price	20 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)



Editing Billing Plan

Plan	2
Type	Volume
Quota	100 Mbyte(s) *(Range : 1 ~ 2000)
Account Activation	First time login must be done within 3 day(s) 0 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 5 day(s) *(Must be larger than 0)
Price	20 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)

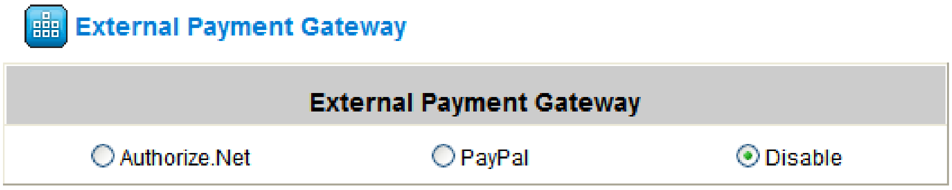


Billing Plans

Billing Plans

Plan	Type	Quota	Price (€)	Enable	Function
1	Time	2 hr(s)	20	☑	Edit
2	Volume	100 Mbyte(s)	20	☑	Edit
3	N/A			□	Edit
4	N/A			□	Edit
5	N/A			□	Edit
6	N/A			□	Edit
7	N/A			□	Edit
8	N/A			□	Edit
9	N/A			□	Edit
0	N/A			□	Edit

STEP 6 . Back to **Authentication Server Configuration** page, if user would like to enable Credit Card payment system, user can click **Create** button of **External Payment Gateway**. Select **Authorize.net** or **PayPal** system based on user's request. For more detail information of **Authorize.net** and **PayPal** please check **Appendix D** and **Appendix E**.



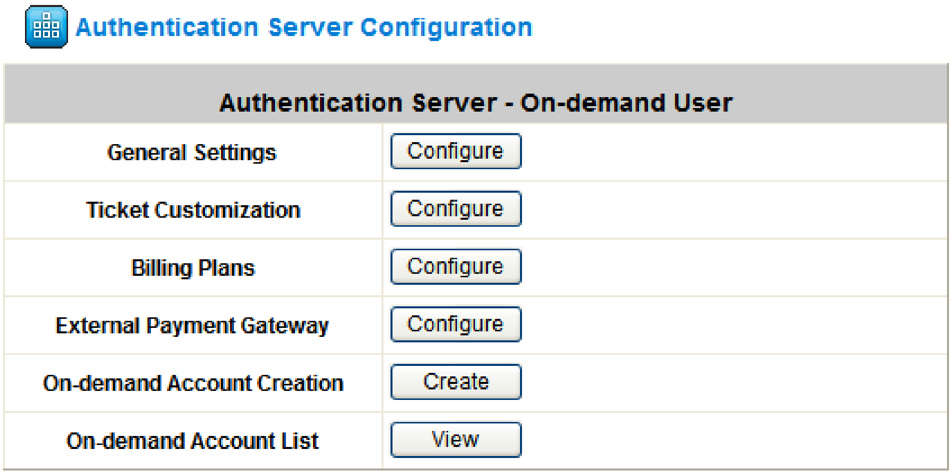
External Payment Gateway

External Payment Gateway

○ Authorize.Net ○ PayPal ● Disable

4.4 How to create On-demand account

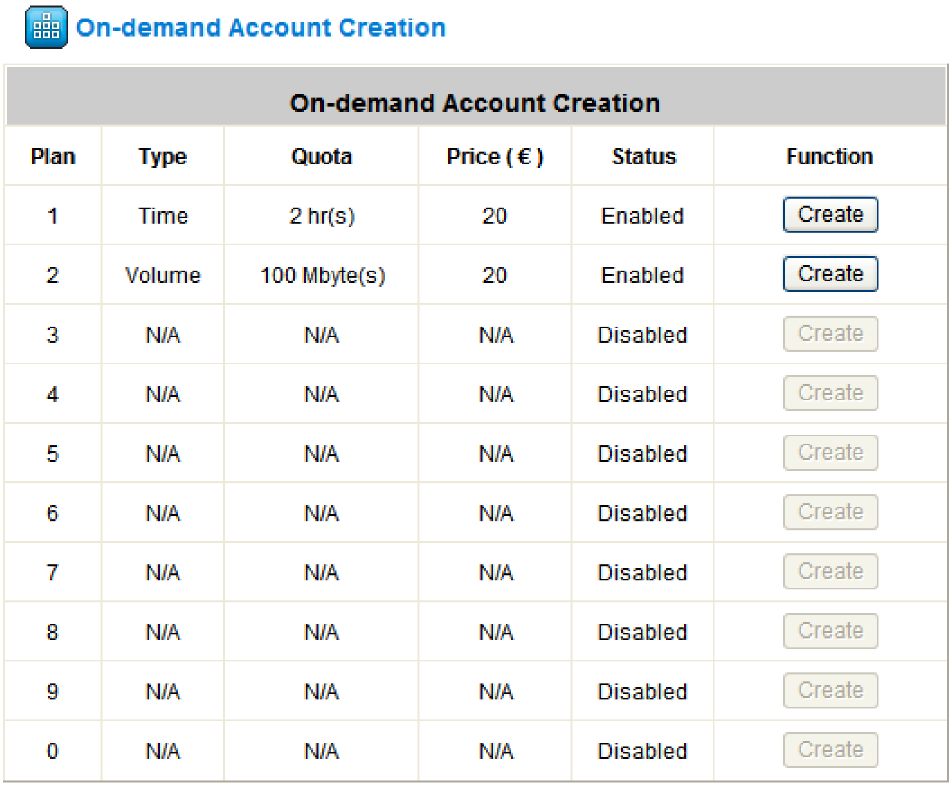
STEP 1 . Back to **Authentication Server Configuration** page, and click **Create** button.



Authentication Server Configuration

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 List	View

STEP 2 . Enter **On-demand Account Creation** page, press **Create** button to generate a random account.

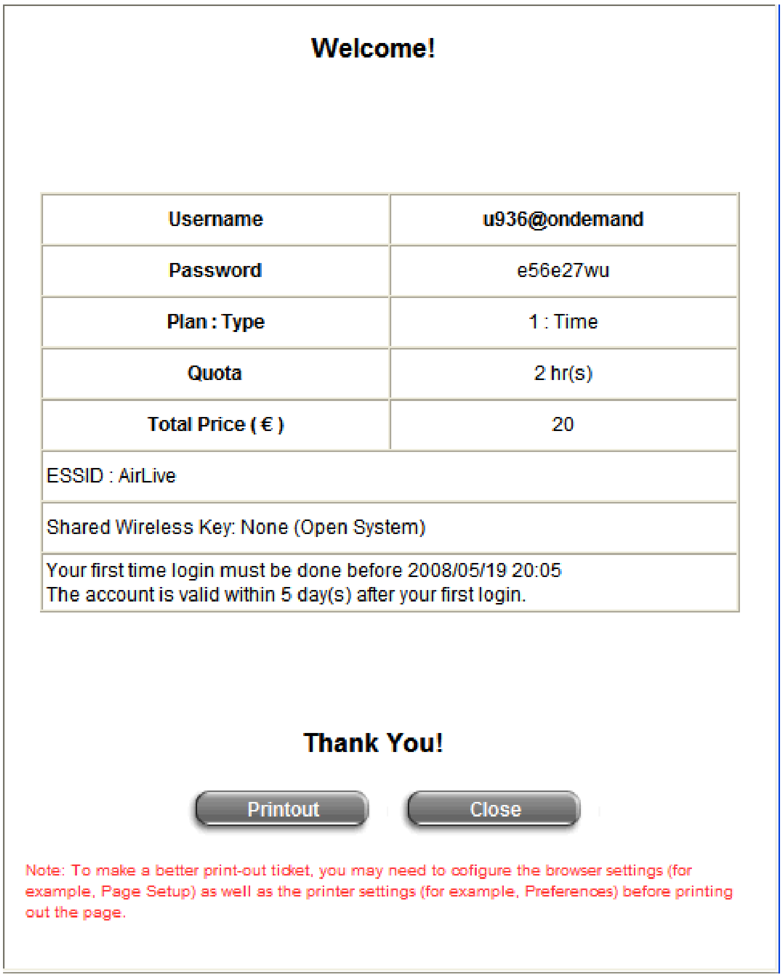


On-demand Account Creation

On-demand Account Creation

Plan	Type	Quota	Price (€)	Status	Function
1	Time	2 hr(s)	20	Enabled	Create
2	Volume	100 Mbyte(s)	20	Enabled	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

STEP 3 . Press **Printout** button, the ticket can be printed out via ticket printer..



Welcome!

Username	**u936@ondemand**
Password	e56e27wu
Plan : Type	1 : Time
Quota	2 hr(s)
Total Price (€)	20

ESSID : AirLive

Shared Wireless Key: None (Open System)

Your first time login must be done before 2008/05/19 20:05
The account is valid within 5 day(s) after your first login.

Thank You!

Note: To make a better print-out ticket, you may need to cofigure the browser settings (for example, Page Setup) as well as the printer settings (for example, Preferences) before printing out the page.

STEP 4 . If Billing Plans is created several plans, user can choose to generate the random account from ticket printer. Click the Function key Selection button to choose the billing rule.

Click on Function Selection button to choose the billing rule.

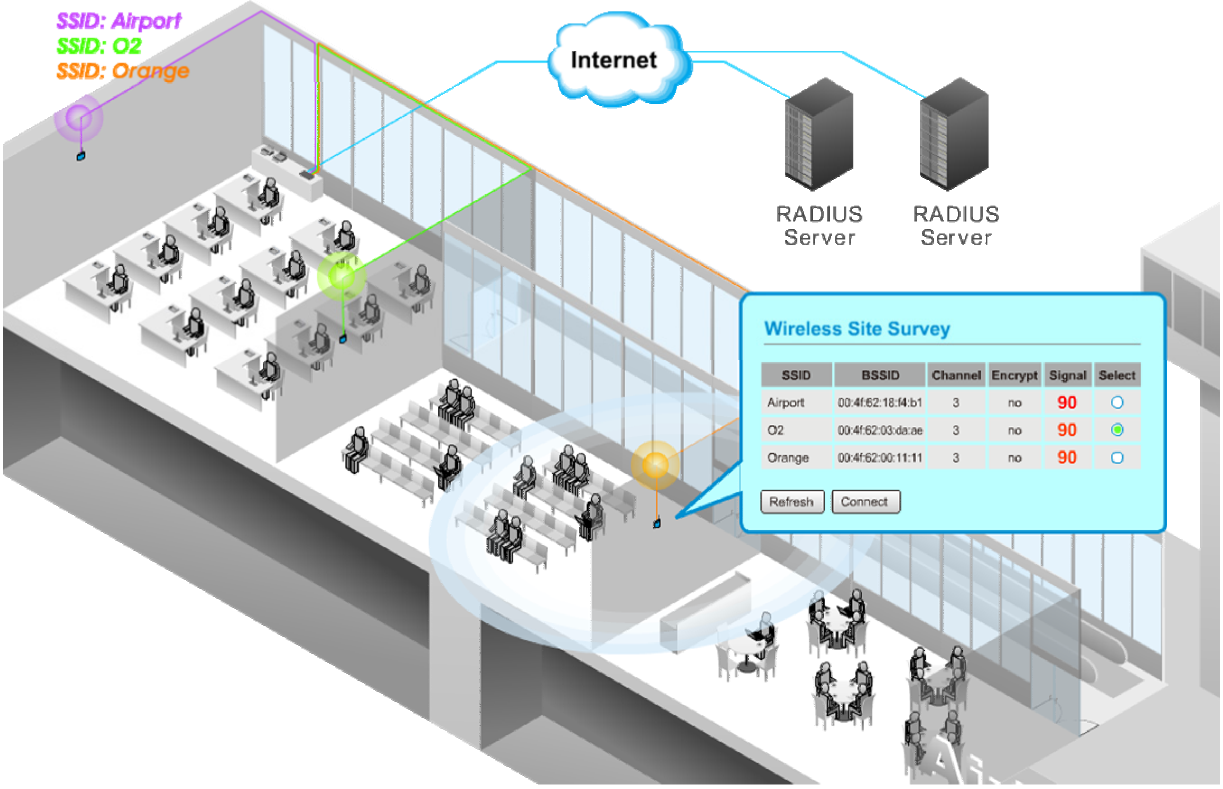
STEP 5 . Basic Hotspot configuration is done.

Chapter 5. Multi-Service Providers

5.1 Introduction

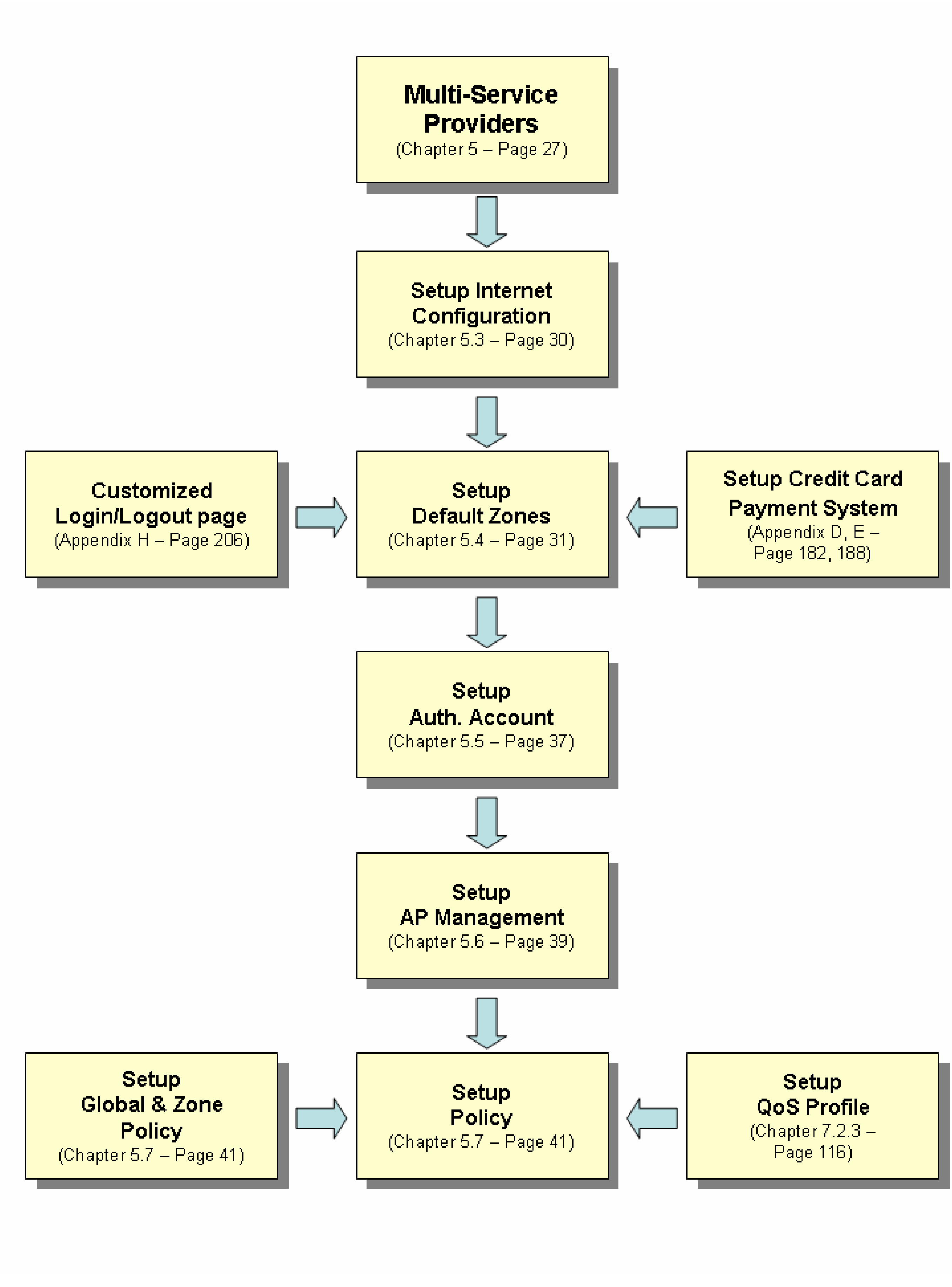
User can install one single MW-2000S to offer the Internet connecting service with several service providers; each service provider can design its own login page and connect to its own RADIUS server as the database of User Authentication.

Following steps offer the example of step-by-step configuration, and in the example, we will create a **Multi-Service Providers** environment for **Airport office worker**, **O2 service provider**, and **Orange service provider**.



SSID	BSSID	Channel	Encrypt	Signal	Select
Airport	00:4f:62:18:f4:b1	3	no	90	○
O2	00:4f:62:03:da:ae	3	no	90	●
Orange	00:4f:62:00:11:11	3	no	90	○

Setup Flow:


Multi-Service Providers
(Chapter 5 – Page 27)
Setup Internet Configuration
(Chapter 5.3 – Page 30)
Customized Login/Logout page
(Appendix H – Page 206)
Setup Default Zones
(Chapter 5.4 – Page 31)
Setup Credit Card Payment System
(Appendix D, E – Page 182, 188)
Setup Auth. Account
(Chapter 5.5 – Page 37)
Setup AP Management
(Chapter 5.6 – Page 39)
Setup Global & Zone Policy
(Chapter 5.7 – Page 41)
Setup Policy
(Chapter 5.7 – Page 41)
Setup QoS Profile
(Chapter 7.2.3 – Page 116)

5.2 Before to start

There are several things user must pay attention, before you start to configure it:

1. The firmware version must be correct

The current firmware version of MW-2000S is 2.00.00_00900, and WLA-5000AP firmware version must be v2.00e12, or MW-2000S will not succeed to detect WLA-5000AP.

2. WLA-5000AP must be reset with default setting

If user would like to allow MW-2000S auto-detecting WLA-5000AP, the WLA-5000AP device must be reset with default setting, or MW-2000S will not succeed to detect WLA-5000AP.

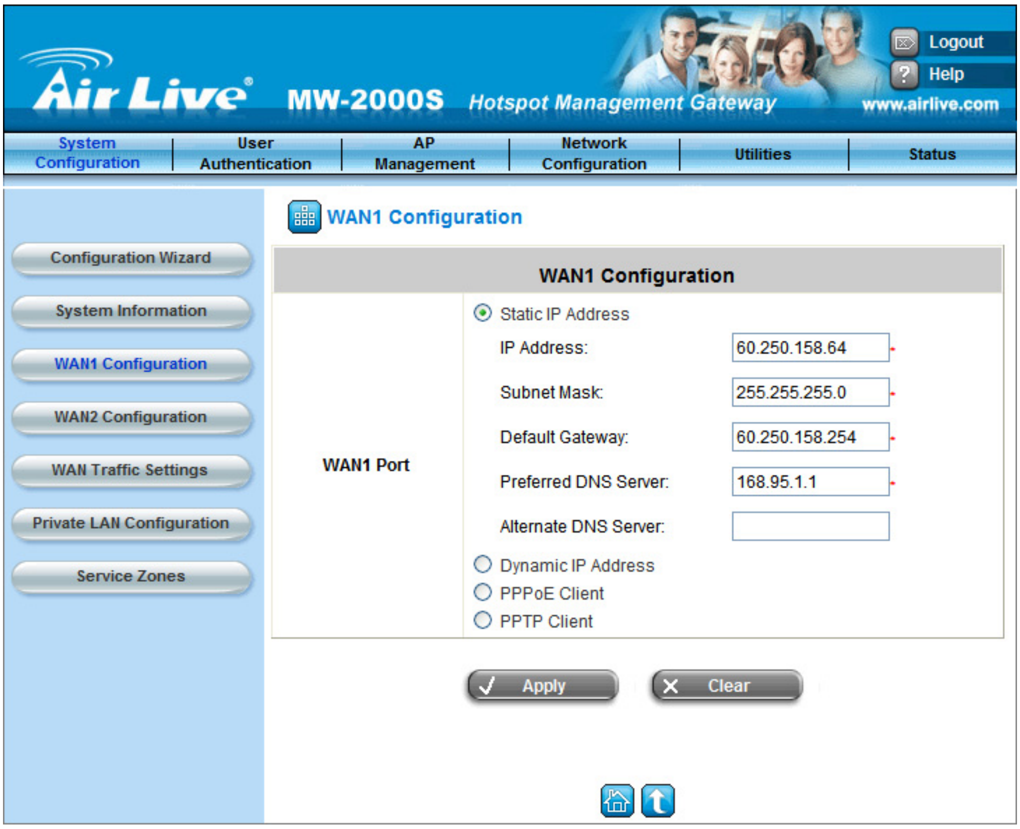
3. Do not power off MW-2000S and WLA-5000AP during auto-configuring WLA-5000AP

When MW-2000S starts to configure WLA-5000AP, user may not power off MW-2000S or WLA-5000AP, or it could damage WLA-5000AP, and possibly can not rescue it back even restore the boot loader.

User can follow the steps to create your own Multi-Service Providers setting:
Chapter 5.3 – Setup Internet Connection
Chapter 5.4 – Setup Service Zones
Chapter 5.5 – Setup Authentication Account
Chapter 5.6 – Setup AP Management
Chapter 5.7 – Setup Policy Configuration

5.3 Setup Internet Connection

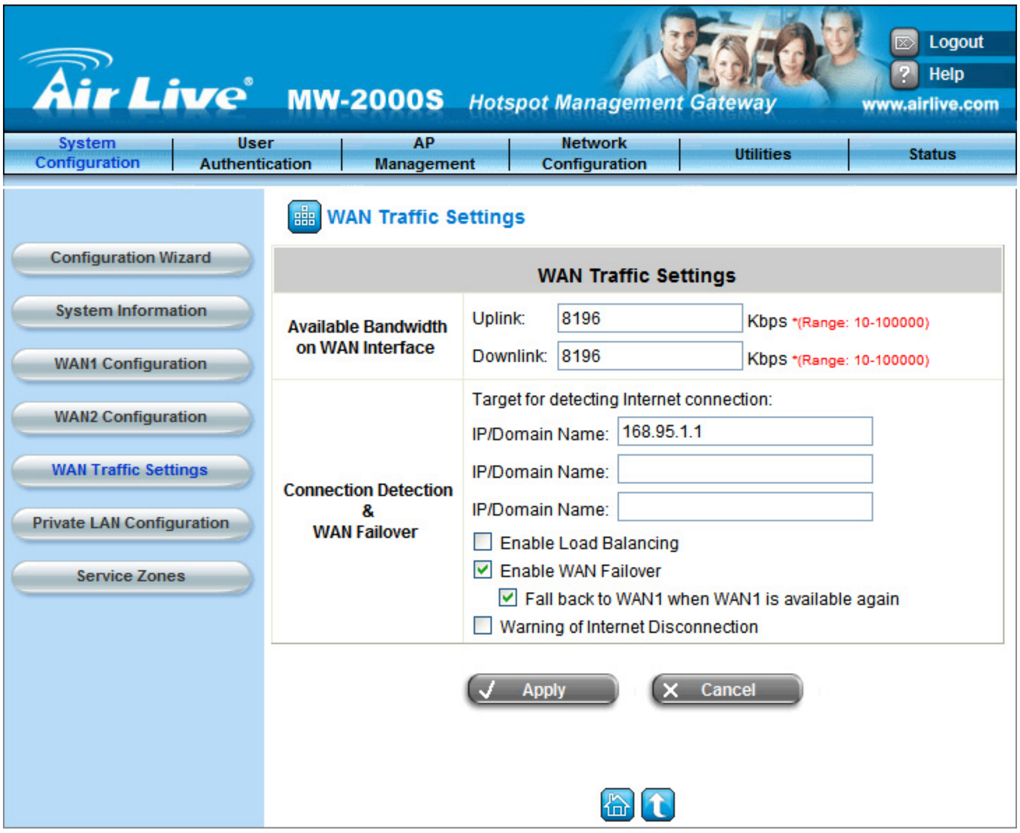
STEP 1 . Enter **System Configuration → WAN1 Configuration** to define the WAN connection. User can configure WAN connecting type with Static IP, Dynamic IP, PPPoE, or PPTP client based on the request.



WAN1 Configuration

WAN1 Configuration	
WAN1 Port	● Static IP Address IP Address: 60.250.158.64 * Subnet Mask: 255.255.255.0 * Default Gateway: 60.250.158.254 * Preferred DNS Server: 168.95.1.1 * Alternate DNS Server: ○ Dynamic IP Address ○ PPPoE Client ○ PPTP Client

STEP 2 . If user applies two Internet connections, the second line can be setup at WAN2, and enable Load balancing or Failover function at **WAN Traffic Setting**. For more information to configure WAN port setting, please check ***Chapter 7.1.3***, ***Chapter 7.1.4***, and ***Chapter 7.1.5***.



WAN Traffic Settings

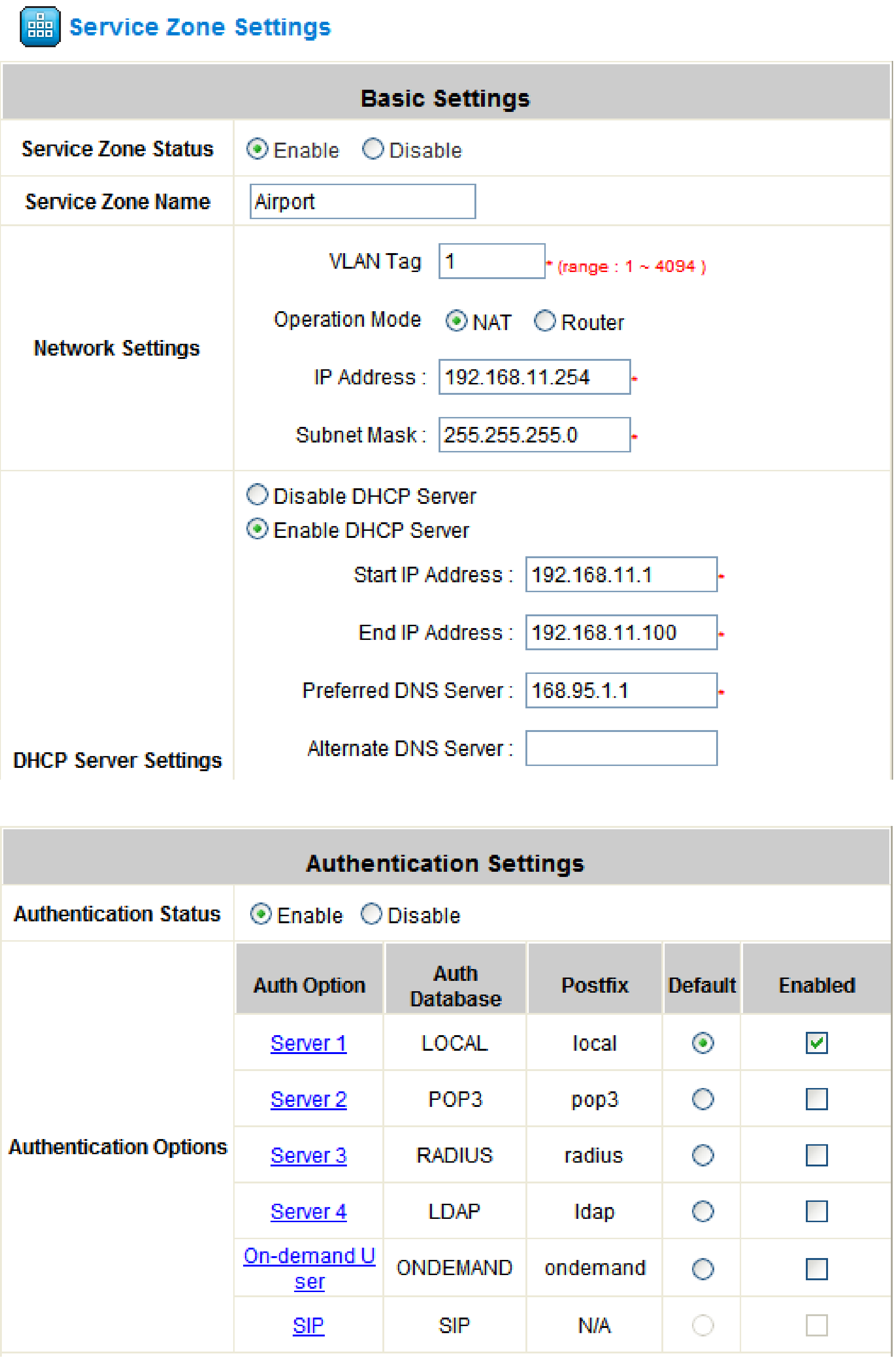
WAN Traffic Settings	
Available Bandwidth on WAN Interface	Uplink: 8196 Kbps *(Range: 10-100000) Downlink: 8196 Kbps *(Range: 10-100000)
Connection Detection & WAN Failover	Target for detecting Internet connection: IP/Domain Name: 168.95.1.1 IP/Domain Name: IP/Domain Name: □ Enable Load Balancing ☑ Enable WAN Failover ☑ Fall back to WAN1 when WAN1 is available again □ Warning of Internet Disconnection

5.4 Setup Service Zones

Environment:

Service Zone	SSID	IP Subnet	Authentication	Policy	Priority
Airport	Airport	192.168.11.x	Local database	Policy 1	Best Effort
O2	O2	192.168.12.x	RADIUS	Policy 2	Background
Orange	Orange	192.168.13.x	RADIUS	Policy 3	Background

STEP 1 . **System Configuration → Service Zones:** Create the first Service Zone for Airport office worker. You can check ***Chapter 7.1.7*** for more information about **Service Zones**.



Service Zone Settings

Basic Settings

Service Zone Status: ● Enable ○ Disable

Service Zone Name: Airport

Network Settings:
VLAN Tag: 1 * (range : 1 ~ 4094)
Operation Mode: ● NAT ○ Router
IP Address : 192.168.11.254 *
Subnet Mask : 255.255.255.0 *

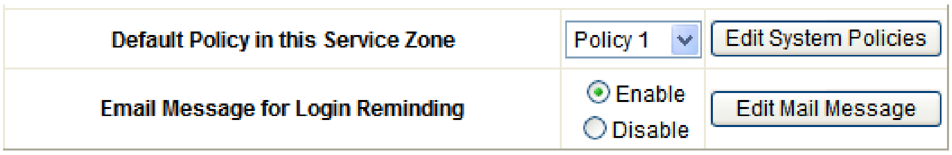
DHCP Server Settings:
○ Disable DHCP Server
● Enable DHCP Server
Start IP Address : 192.168.11.1 *
End IP Address : 192.168.11.100 *
Preferred DNS Server : 168.95.1.1 *
Alternate DNS Server :

Authentication Settings

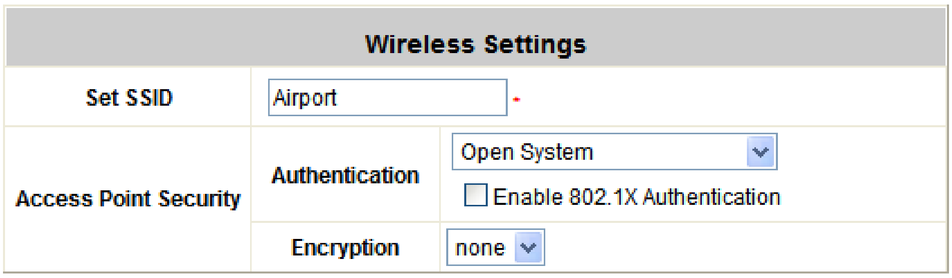
Authentication Status: ● Enable ○ Disable

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	○	□



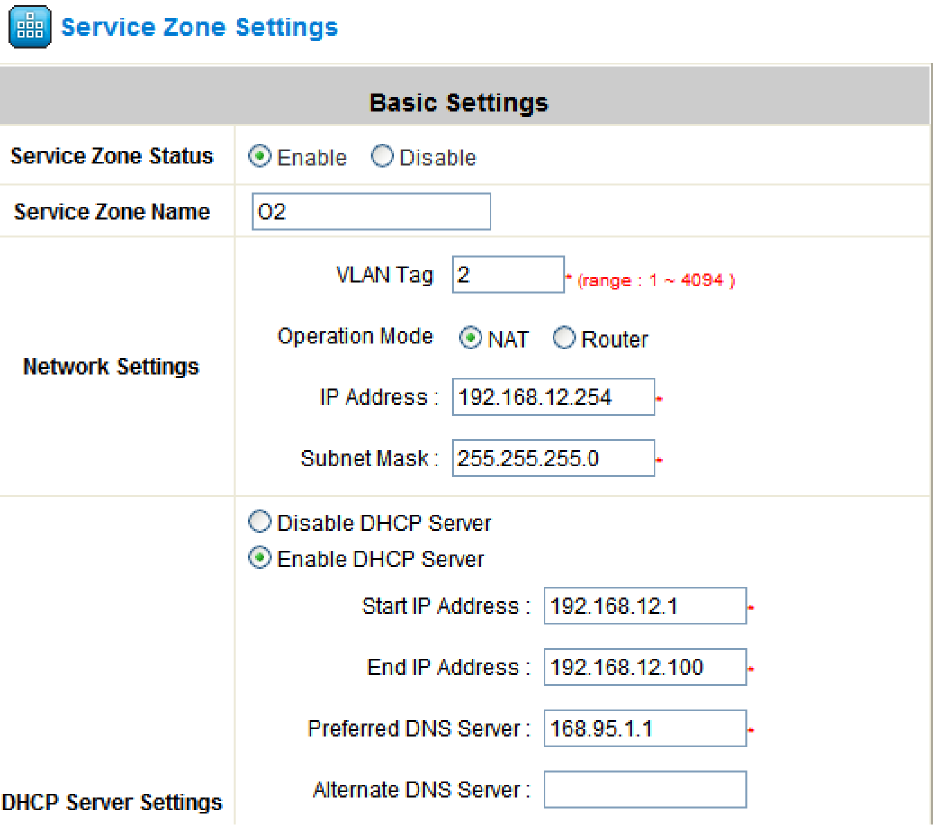
Default Policy in this Service Zone	Policy 1	Edit System Policies
Email Message for Login Reminding	● Enable ○ Disable	Edit Mail Message



Wireless Settings

Set SSID	Airport *	
Access Point Security	Authentication	Open System □ Enable 802.1X Authentication
	Encryption	none

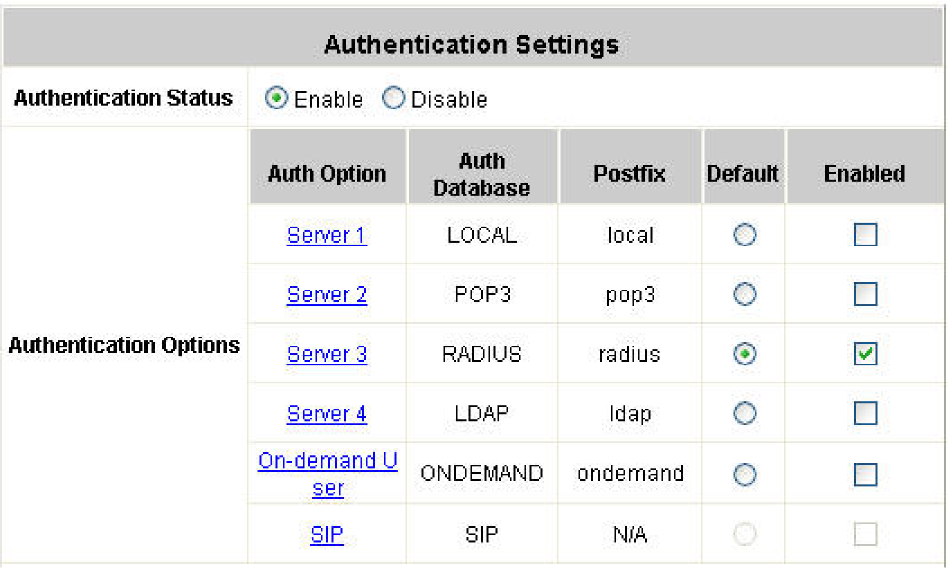
STEP 2 **. System Configuration → Service Zones:** Create the second Service Zone for O2 Service Provider.



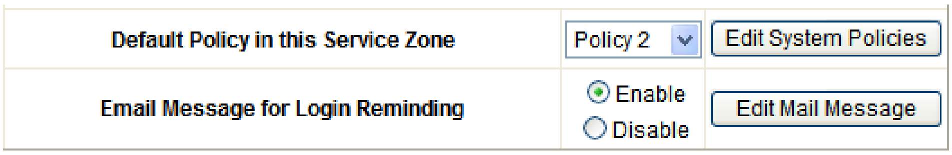
Service Zone Settings

Basic Settings

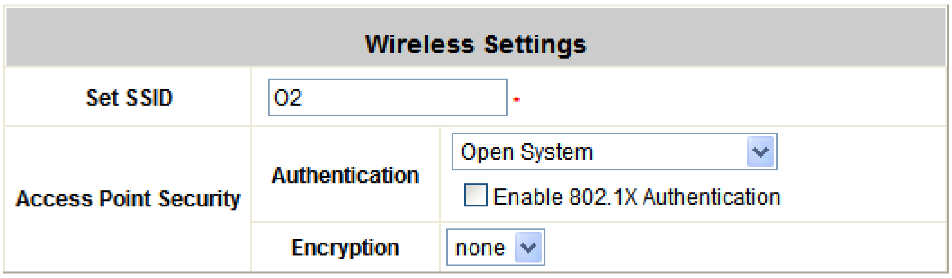
Service Zone Status	● Enable ○ Disable
Service Zone Name	O2
Network Settings	VLAN Tag: 2 * (range : 1 ~ 4094) Operation Mode: ● NAT ○ Router IP Address : 192.168.12.254 * Subnet Mask : 255.255.255.0 *
DHCP Server Settings	○ Disable DHCP Server ● Enable DHCP Server Start IP Address : 192.168.12.1 * End IP Address : 192.168.12.100 * Preferred DNS Server : 168.95.1.1 * Alternate DNS Server :



Authentication Settings					
Authentication Status	● Enable ○ Disable				
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	○	□

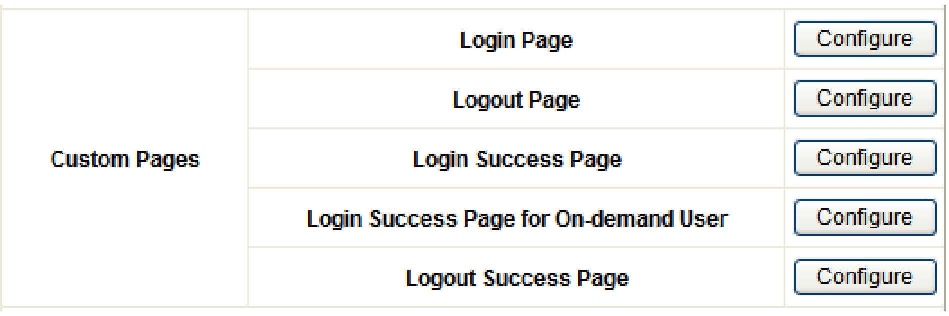


Default Policy in this Service Zone	Policy 2	Edit System Policies
Email Message for Login Reminding	● Enable ○ Disable	Edit Mail Message



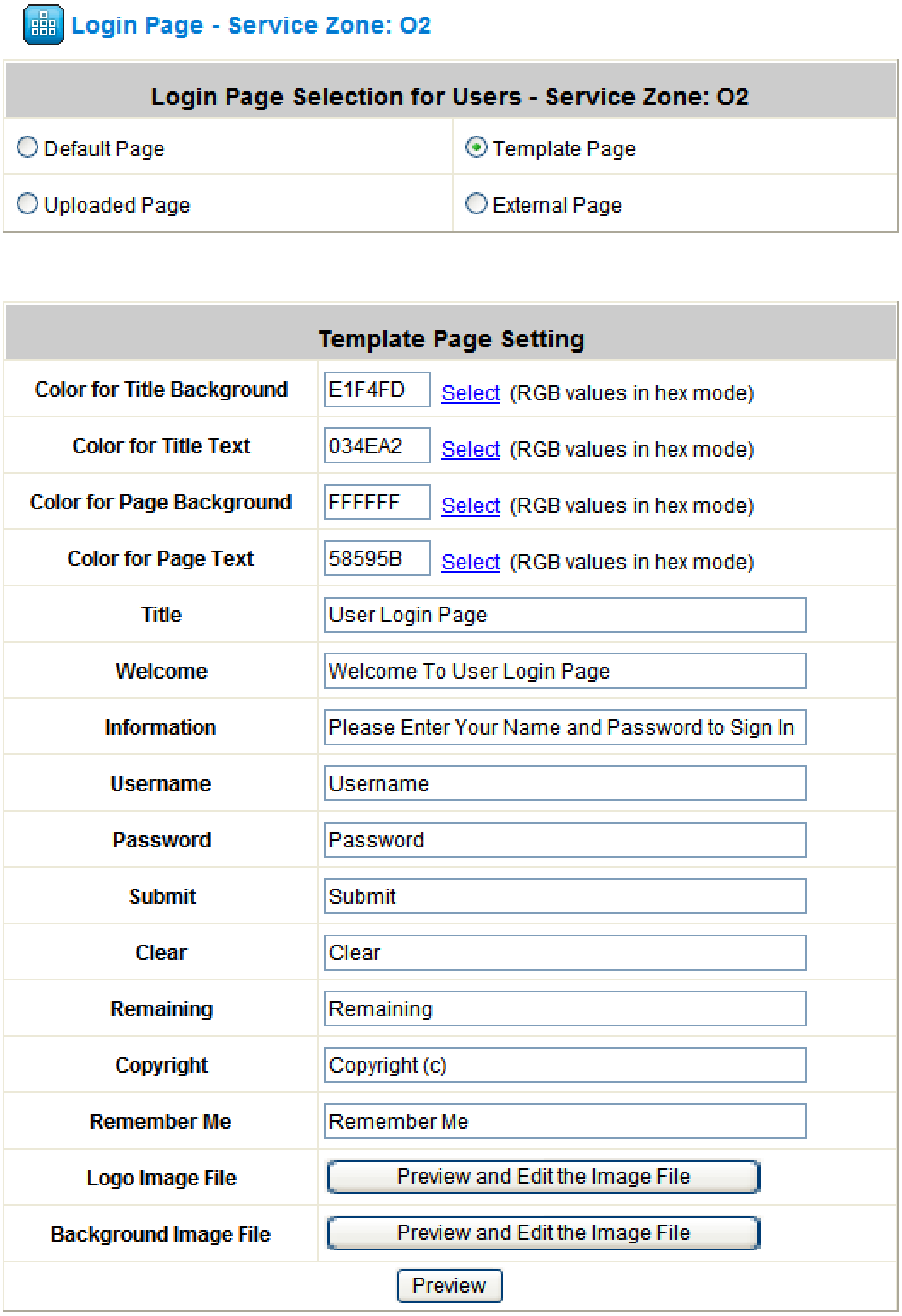
Wireless Settings		
Set SSID	O2 *	
Access Point Security	Authentication	Open System □ Enable 802.1X Authentication
	Encryption	none

STEP 3 . Customize the Login / Logout page. User can choose to use the default page, or use Template Page, Uploaded Page, or External Page to customize the page. For more detail information of customized page please check **Appendix H Customizable Pages**.



Custom Pages	Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Success Page for On-demand User	Configure
	Logout Success Page	Configure

STEP 4 . Take Template Page as example, user can select to design color of text and background, change the word of text and button, change logo, and replace the image file of background.

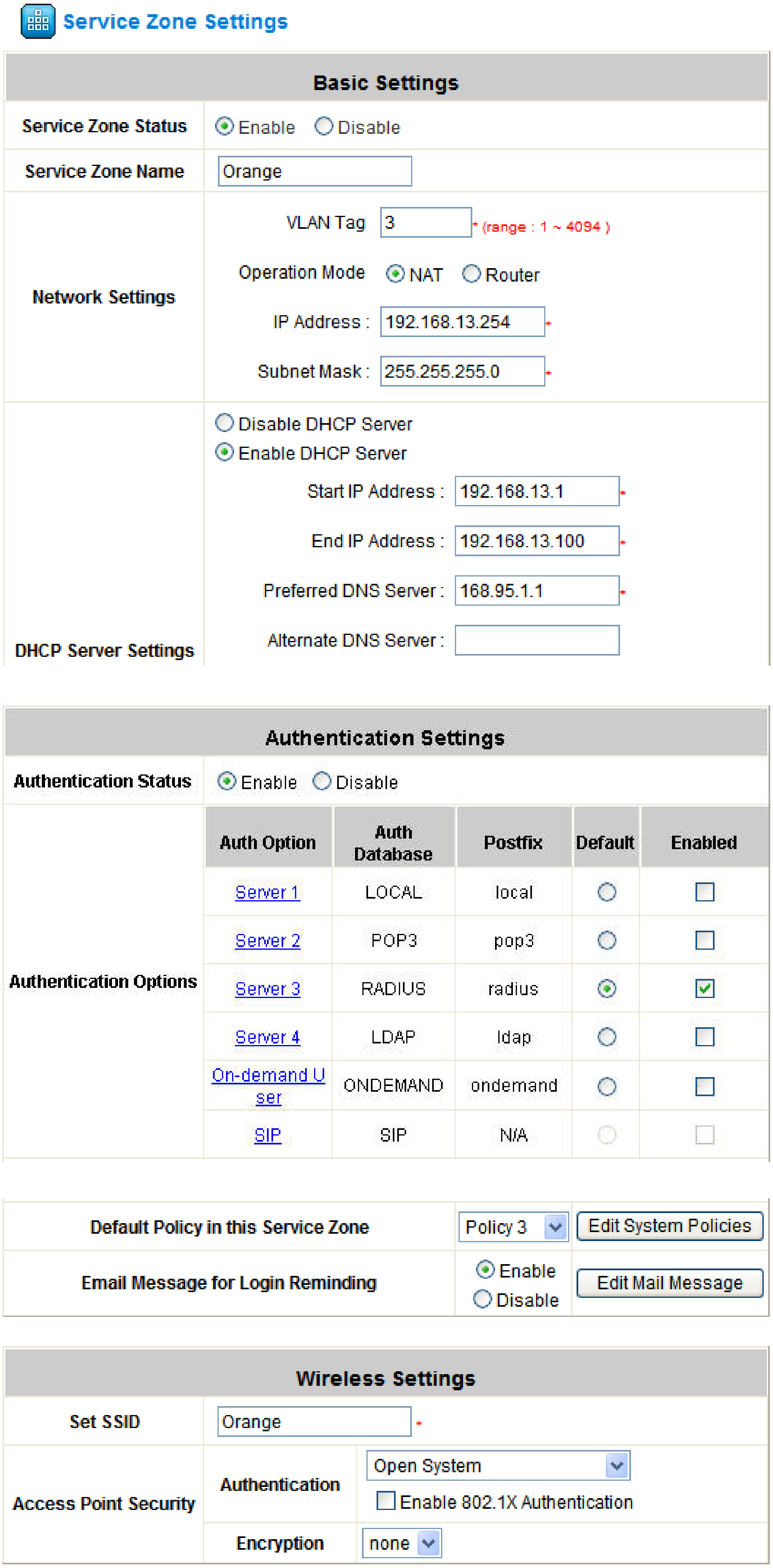


Login Page - Service Zone: O2

Login Page Selection for Users - Service Zone: O2	
○ Default Page	● Template Page
○ Uploaded Page	○ External Page

Template Page Setting	
Color for Title Background	E1F4FD Select (RGB values in hex mode)
Color for Title Text	034EA2 Select (RGB values in hex mode)
Color for Page Background	FFFFFF Select (RGB values in hex mode)
Color for Page Text	58595B Select (RGB values in hex mode)
Title	User Login Page
Welcome	Welcome To User Login Page
Information	Please Enter Your Name and Password to Sign In
Username	Username
Password	Password
Submit	Submit
Clear	Clear
Remaining	Remaining
Copyright	Copyright (c)
Remember Me	Remember Me
Logo Image File	Preview and Edit the Image File
Background Image File	Preview and Edit the Image File
Preview	

STEP 5 **. System Configuration → Service Zones:** Create the third Service Zone for Orange Service Provider.



Service Zone Settings

Basic Settings

Service Zone Status	● Enable ○ Disable
Service Zone Name	Orange
Network Settings	VLAN Tag: 3 * (range : 1 ~ 4094) Operation Mode: ● NAT ○ Router IP Address : 192.168.13.254 * Subnet Mask : 255.255.255.0 *
DHCP Server Settings	○ Disable DHCP Server ● Enable DHCP Server Start IP Address : 192.168.13.1 * End IP Address : 192.168.13.100 * Preferred DNS Server : 168.95.1.1 * Alternate DNS Server :

Authentication Settings

Authentication Status: ● Enable ○ Disable

Authentication Options

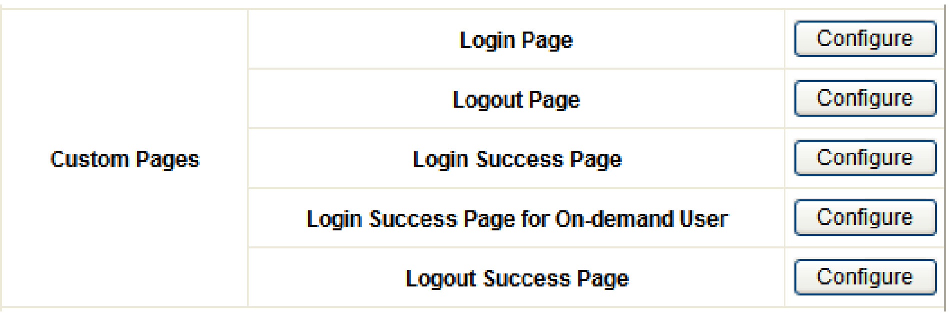
Auth Option	Auth Database	Postfix	Default	Enabled
Server 1	LOCAL	local	○	□
Server 2	POP3	pop3	○	□
Server 3	RADIUS	radius	●	☑
Server 4	LDAP	ldap	○	□
On-demand User	ONDEMAND	ondemand	○	□
SIP	SIP	N/A	○	□

Default Policy in this Service Zone	Policy 3	Edit System Policies
Email Message for Login Reminding	● Enable ○ Disable	Edit Mail Message

Wireless Settings

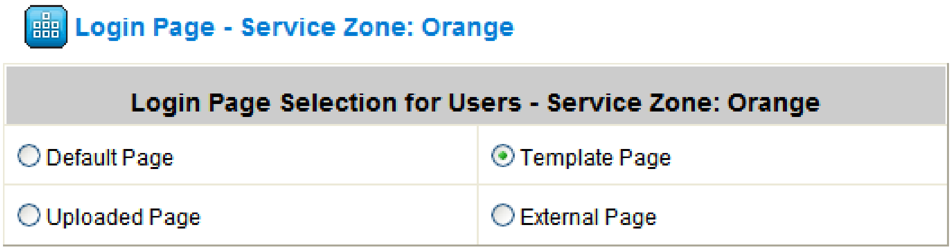
Set SSID	Orange *	
Access Point Security	Authentication	Open System □ Enable 802.1X Authentication
	Encryption	none

STEP 6 . Customize the Login / Logout page. User can choose to use the default page, or use Template Page, Uploaded Page, or External Page to customize the page. For more detail information of customized page please check **Appendix H Customizable Pages**.



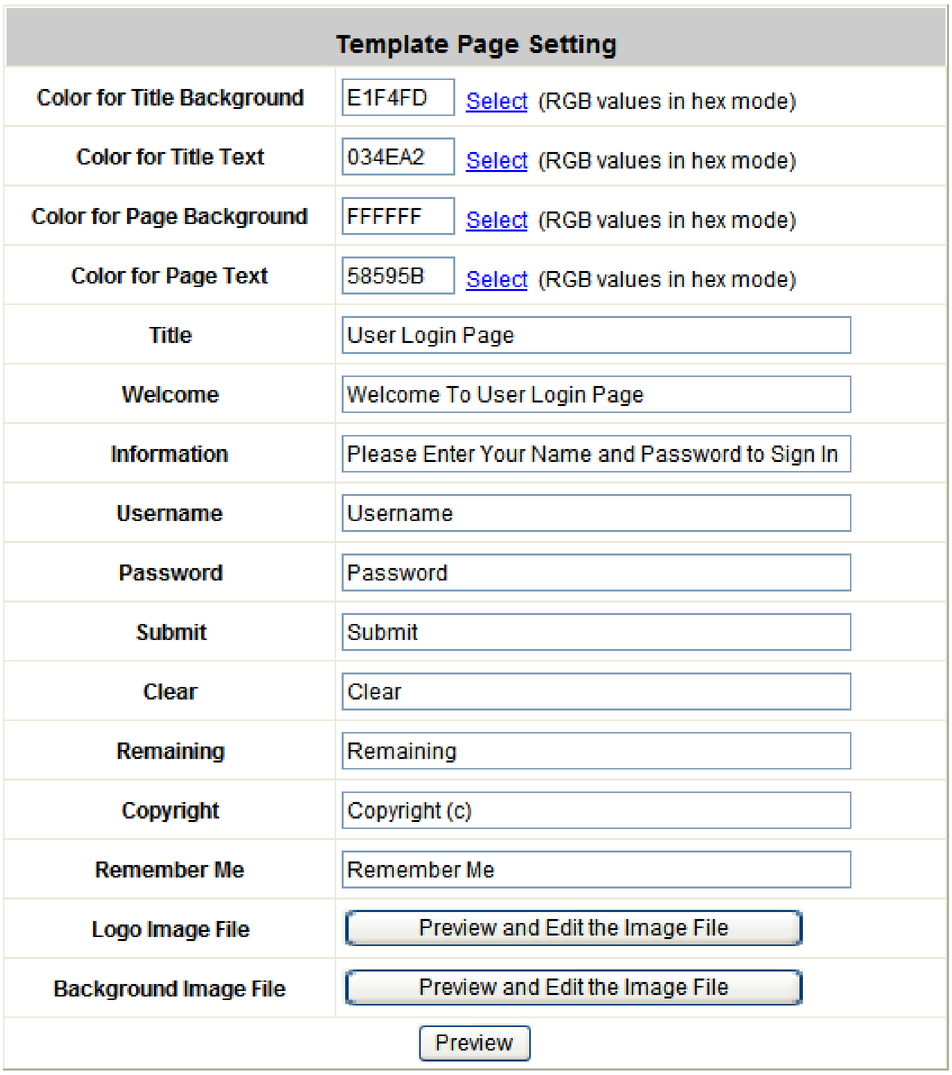
Custom Pages	Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Success Page for On-demand User	Configure
	Logout Success Page	Configure

STEP 7 . Take Template Page as example, user can select to design color of text and background, change the word of text and button, change logo, and replace the image file of background.



Login Page - Service Zone: Orange

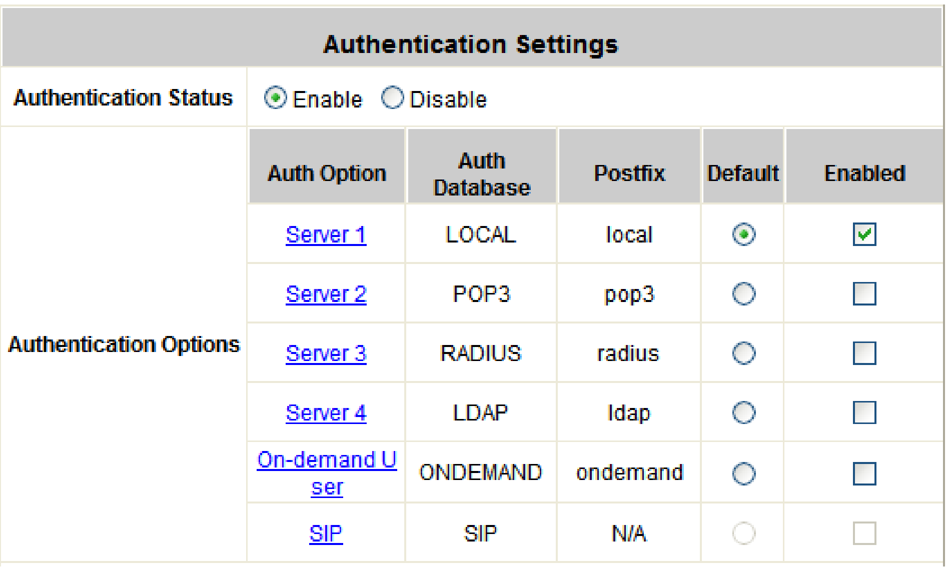
Login Page Selection for Users - Service Zone: Orange	
○ Default Page	● Template Page
○ Uploaded Page	○ External Page



Template Page Setting	
Color for Title Background	E1F4FD Select (RGB values in hex mode)
Color for Title Text	034EA2 Select (RGB values in hex mode)
Color for Page Background	FFFFFF Select (RGB values in hex mode)
Color for Page Text	58595B Select (RGB values in hex mode)
Title	User Login Page
Welcome	Welcome To User Login Page
Information	Please Enter Your Name and Password to Sign In
Username	Username
Password	Password
Submit	Submit
Clear	Clear
Remaining	Remaining
Copyright	Copyright (c)
Remember Me	Remember Me
Logo Image File	Preview and Edit the Image File
Background Image File	Preview and Edit the Image File
Preview	

5.5 Setup Authentication Account

STEP 1 . Create Local database account for **Airport** office worker. Select Server1 as default server of authentication, and enable the setting. Then click **Server1** to enter the next step.

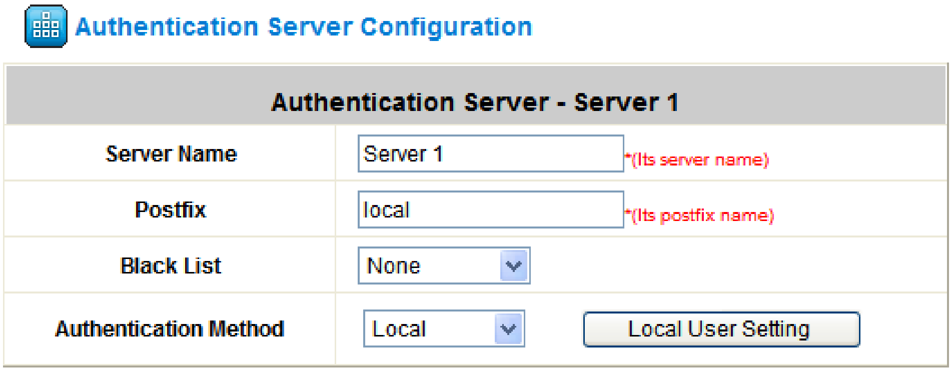


Authentication Settings

Authentication Status	● Enable ○ Disable

	Auth Option	Auth Database	Postfix	Default	Enabled
Authentication Options	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	○	□

STEP 2 . User can change **Server Name**, **Postfix Name**, or enable **Black List**; select **Local** as **Authentication Method**, and click **Local User Setting** button to enter **Local User Setting** page.

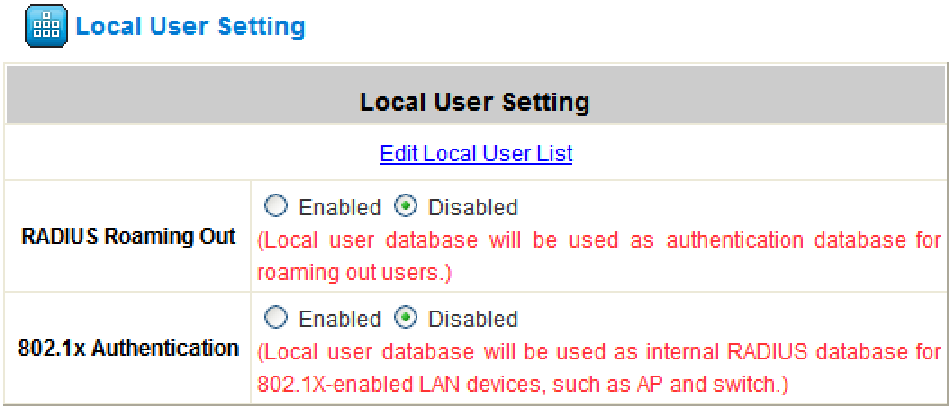


Authentication Server Configuration

Authentication Server - Server 1

Server Name	Server 1 *(Its server name)
Postfix	local *(Its postfix name)
Black List	None
Authentication Method	Local [Local User Setting]

STEP 3 . If user does not need to enable **RADIUS Roaming Out** or **802.1x Authentication**, just click **Edit Local User List** to check current user list or create new local user.



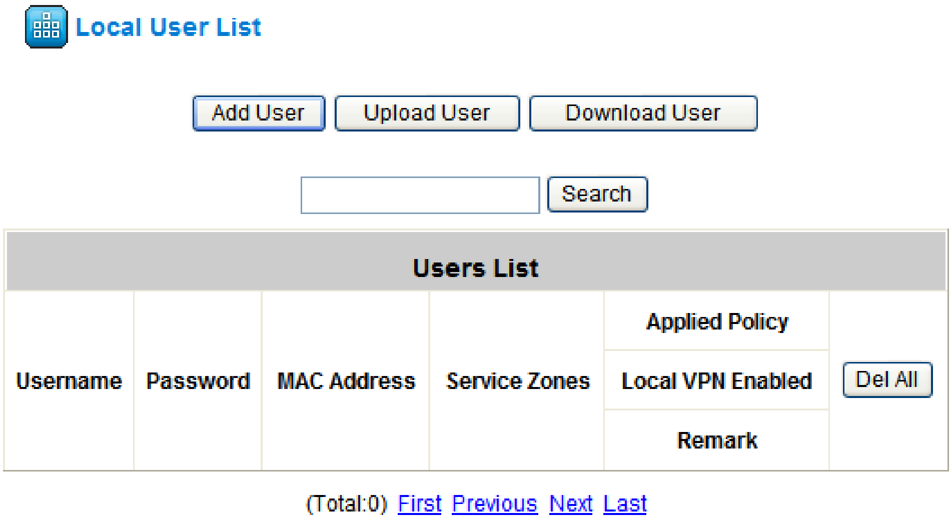
Local User Setting

Local User Setting

Edit Local User List

RADIUS Roaming Out	○ Enabled ● Disabled (Local user database will be used as authentication database for roaming out users.)
802.1x Authentication	○ Enabled ● Disabled (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)

STEP 4 . Click **Add User** to create new user.



Local User List

Add User | Upload User | Download User

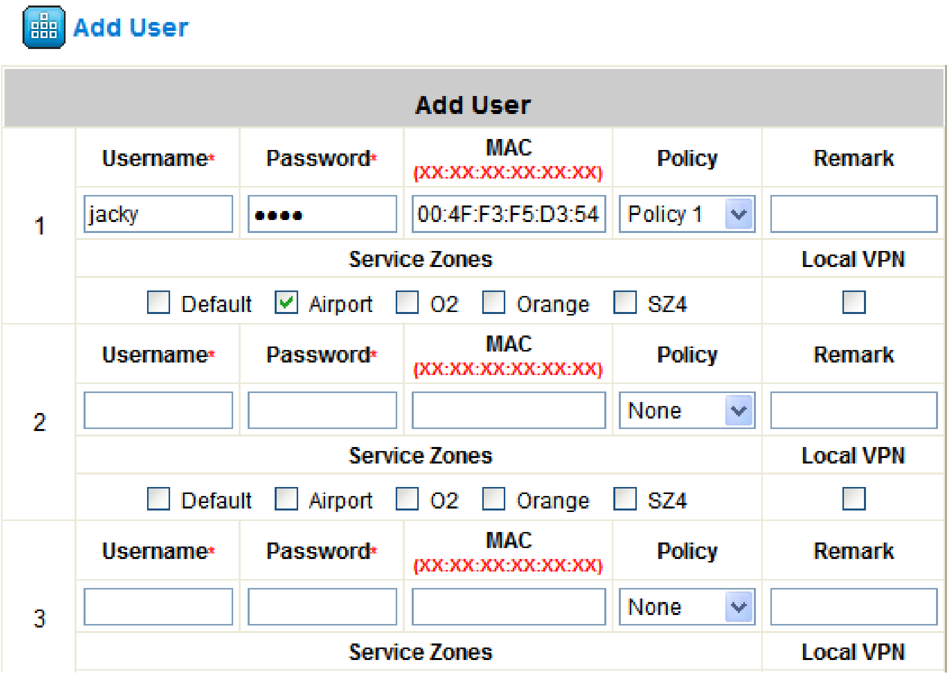
Search

Users List

Username	Password	MAC Address	Service Zones	Applied Policy Local VPN Enabled Remark	Del All

(Total:0) First Previous Next Last

STEP 5 . Fill in **Username**, **Password**, and else information; select a specific **Service Zones**, then click **Apply** to save the setting. For more detail information to setup local user please check ***Chapter 7.2.1.1 Authentication Method – Local***.

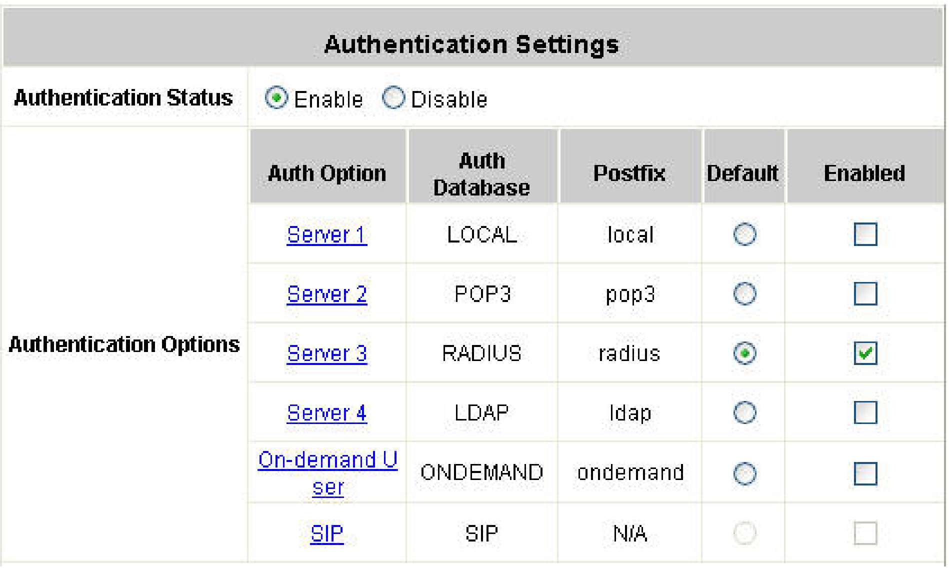


Add User

Add User

1	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
	jacky	●●●●	00:4F:F3:F5:D3:54	Policy 1	
	Service Zones				Local VPN
	□ Default ☑ Airport □ O2 □ Orange □ SZ4				□
2	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
				None	
	Service Zones				Local VPN
	□ Default □ Airport □ O2 □ Orange □ SZ4				□
3	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
				None	
	Service Zones				Local VPN

STEP 6 . Setup RADIUS connection with RADIUS Server for **O2** and **Orange** Service providers. Authorized the account with different RADIUS server, therefore the Service Provider can provide the Internet service with own billing system and user authentication database. For more detail information to setup local user please check ***Chapter 7.2.1.3 Authentication Method – RADIUS***.



Authentication Settings

Authentication Status: ● Enable ○ Disable

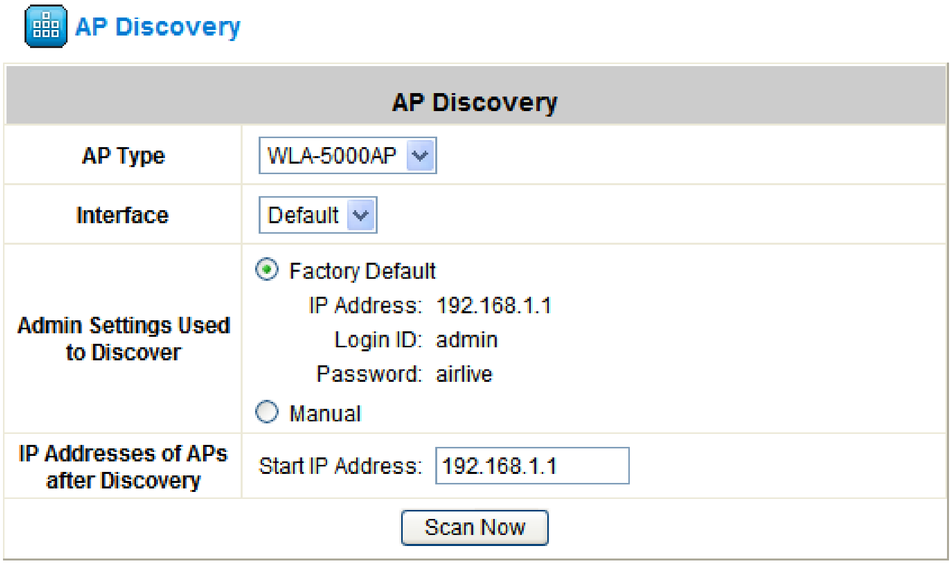
Authentication Options:

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	○	□

5.6 Setup AP Management

STEP 1 . **AP Management → AP Discovery:** Connect WLA-5000AP to MW-2000S Public Port, and use **AP Management** function to auto-detect and auto-configure WLA-5000AP. For more information please check ***Chapter 7.3.2 AP Discovery***.

STEP 2 . Select "WLA-5000AP" and press **Scan Now** to detect AP.

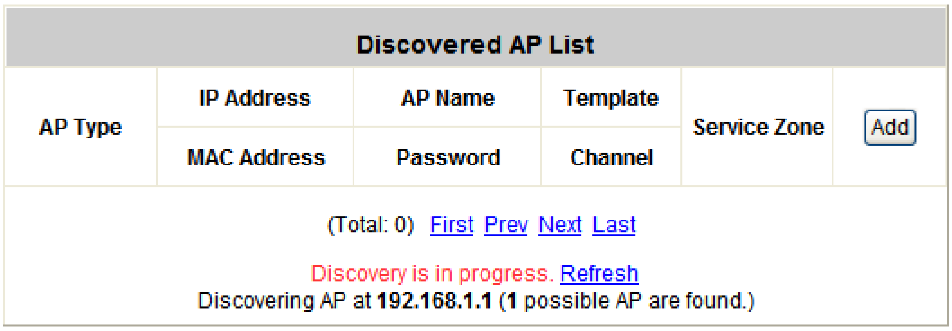


AP Discovery

AP Discovery

AP Type	WLA-5000AP
Interface	Default
Admin Settings Used to Discover	● Factory Default IP Address: 192.168.1.1 Login ID: admin Password: airlive ○ Manual
IP Addresses of APs after Discovery	Start IP Address: 192.168.1.1

STEP 3 . When MW-2000S detects the AP, system will create the connection automatically, so user can define AP's setting via MW-2000S.



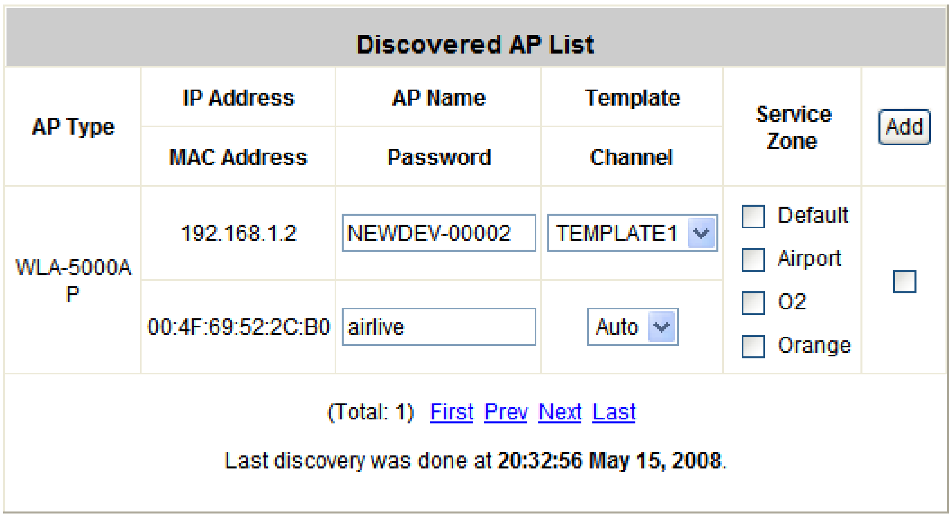
Discovered AP List

AP Type	IP Address	AP Name	Template	Service Zone	Add
	MAC Address	Password	Channel		

(Total: 0) First Prev Next Last

Discovery is in progress. Refresh

Discovering AP at **192.168.1.1** (**1** possible AP are found.)



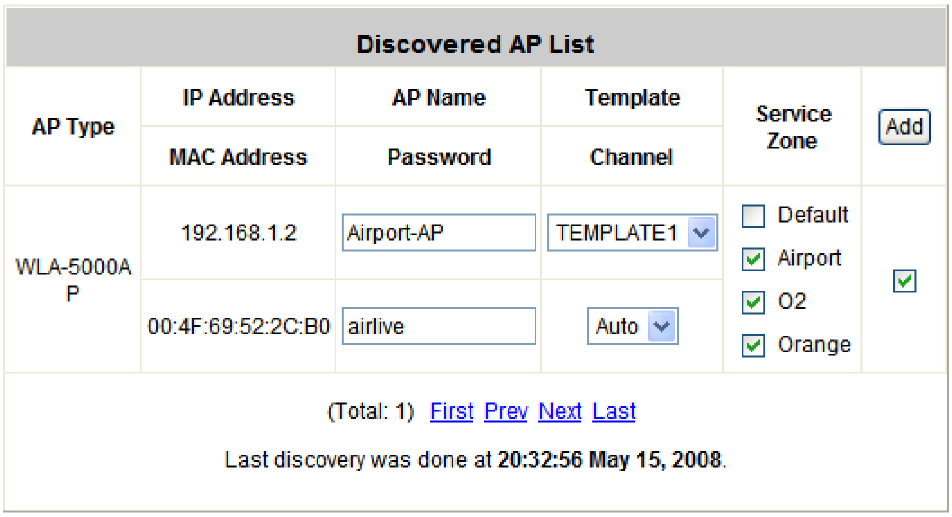
Discovered AP List

AP Type	IP Address	AP Name	Template	Service Zone	Add
	MAC Address	Password	Channel		
WLA-5000AP	192.168.1.2	NEWDEV-00002	TEMPLATE1	□ Default □ Airport □ O2 □ Orange	□
	00:4F:69:52:2C:B0	airlive	Auto		

(Total: 1) First Prev Next Last

Last discovery was done at **20:32:56 May 15, 2008**.

STEP 4 . Change **AP Name**, select **AirPort**, **O2**, and **Orange** Service Zone, and click **Add** to modify WLA-5000AP.



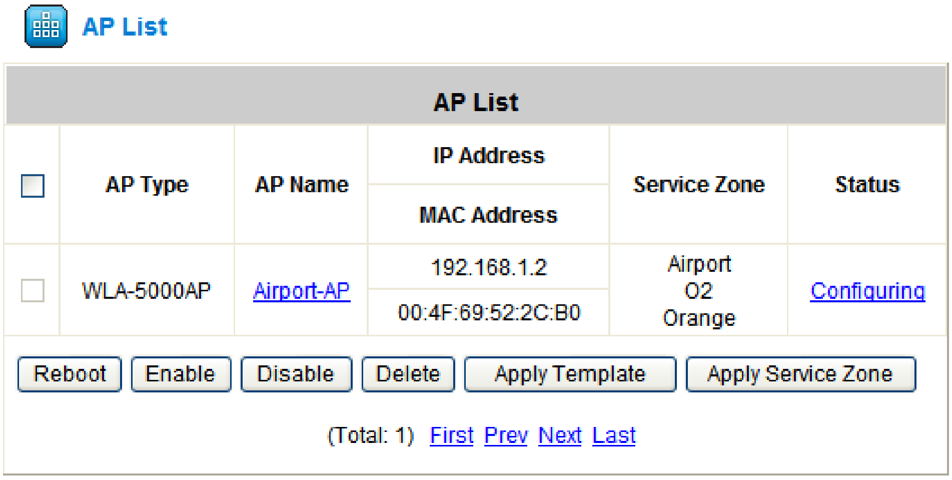
Discovered AP List

AP Type	IP Address	AP Name	Template	Service Zone	Add
	MAC Address	Password	Channel		
WLA-5000AP	192.168.1.2	Airport-AP	TEMPLATE1	□ Default ☑ Airport ☑ O2 ☑ Orange	☑
	00:4F:69:52:2C:B0	airlive	Auto		

(Total: 1) First Prev Next Last

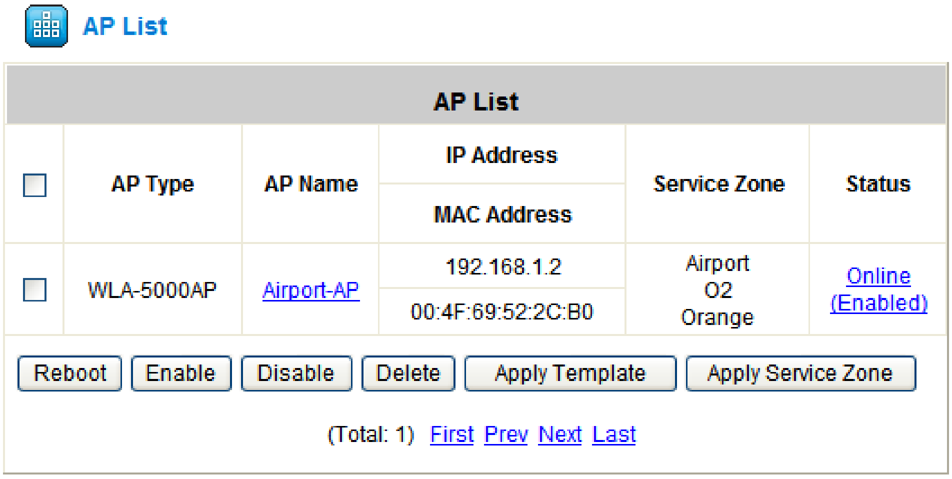
Last discovery was done at **20:32:56 May 15, 2008**.

STEP 5 . Page will turn to **AP List** and WLA-5000AP will be configuring with the data we set; when the configuration is done, the table will be listed a new AP device in **AP List**.



AP List

AP List					
□	AP Type	AP Name	IP Address MAC Address	Service Zone	Status
□	WLA-5000AP	Airport-AP	192.168.1.2 00:4F:69:52:2C:B0	Airport O2 Orange	Configuring



AP List

AP List					
□	AP Type	AP Name	IP Address MAC Address	Service Zone	Status
□	WLA-5000AP	Airport-AP	192.168.1.2 00:4F:69:52:2C:B0	Airport O2 Orange	Online (Enabled)

5.7 Setup Policy

Currently, the default setting of MW-2000S allows passing through every Service Zones. So, if system does not block all connection at first, it might need to create more complicate Policy setting in order to reach the request.

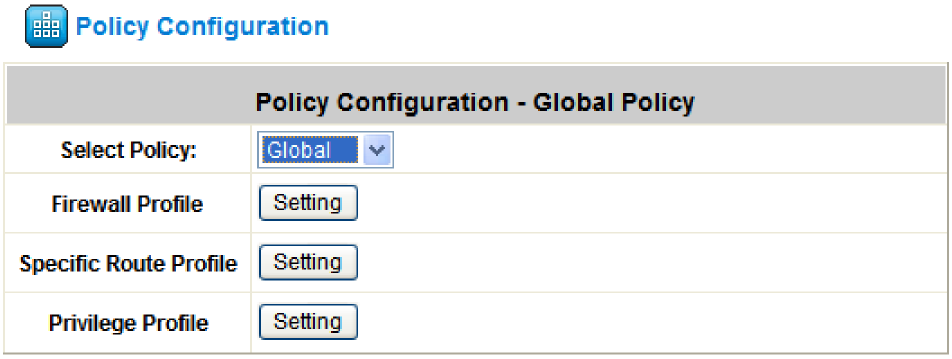
Once the default setting is changing to block all connection, the policy can be more easily that you just need to open the necessary connection.

User can follow the steps to configure the Policy rules for Multi-Service Providers:

1. Configure **Global Policy** to block all connection
2. Configure **Policy 1** for **Airport** Service Zone to allow user accessing Internet.
3. Configure **Policy 2** for **O2** Service Zone to allow user accessing Internet.
4. Configure **Policy 3** for **Orange** Service Zone to allow user accessing Internet.

Attention: *Next version firmware will be modified to block all connection by default, so the first step can be ignored in future.*

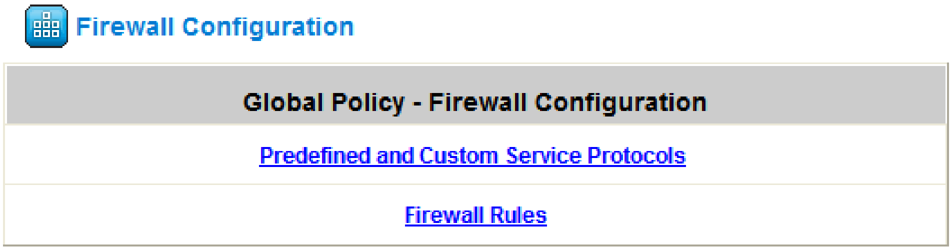
STEP 1 . Click **User Authentication** → **Policy Configuration** and select **Global**"; click **Setting** button of **Firewall Profile** to enter the setting.



Policy Configuration

Policy Configuration - Global Policy	
Select Policy:	Global
Firewall Profile	Setting
Specific Route Profile	Setting
Privilege Profile	Setting

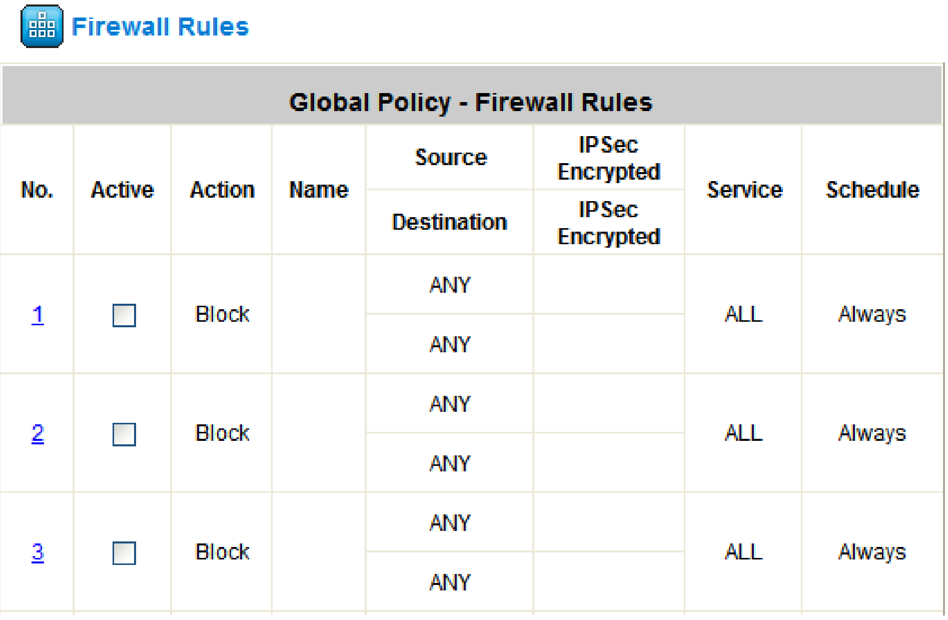
STEP 2 . Click **Firewall Rules** to configure the firewall setting.



Firewall Configuration

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

STEP 3 . Click **No. 1** firewall rule to edit more firewall setting.

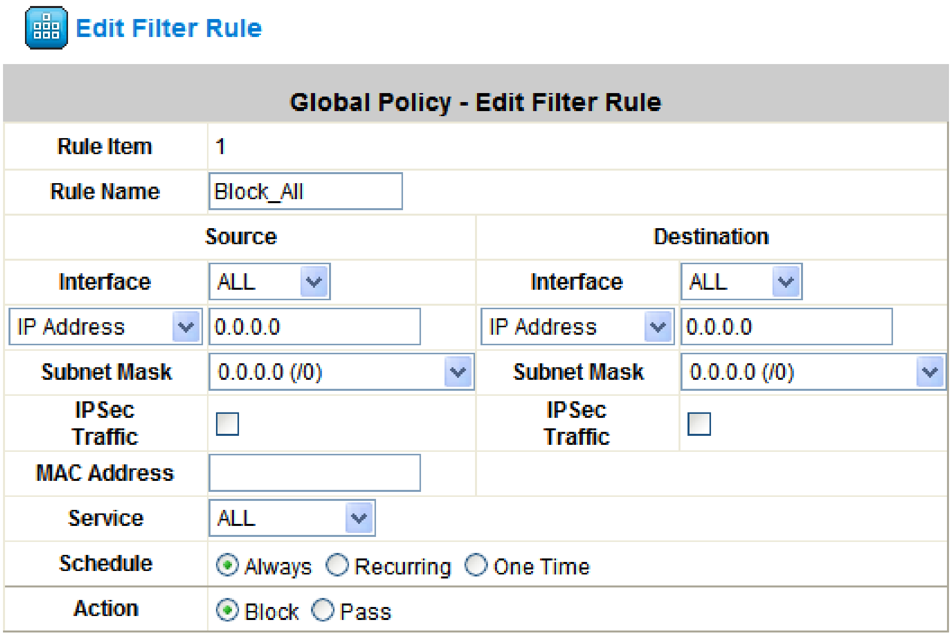


Firewall Rules

Global Policy - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	□	Block		ANY		ALL	Always
				ANY			
2	□	Block		ANY		ALL	Always
				ANY			
3	□	Block		ANY		ALL	Always
				ANY			

STEP 4 . Input the **Rule name**, select **Source** and **Destination** Interface as **ALL**, and enable the **Action** as **Block**.

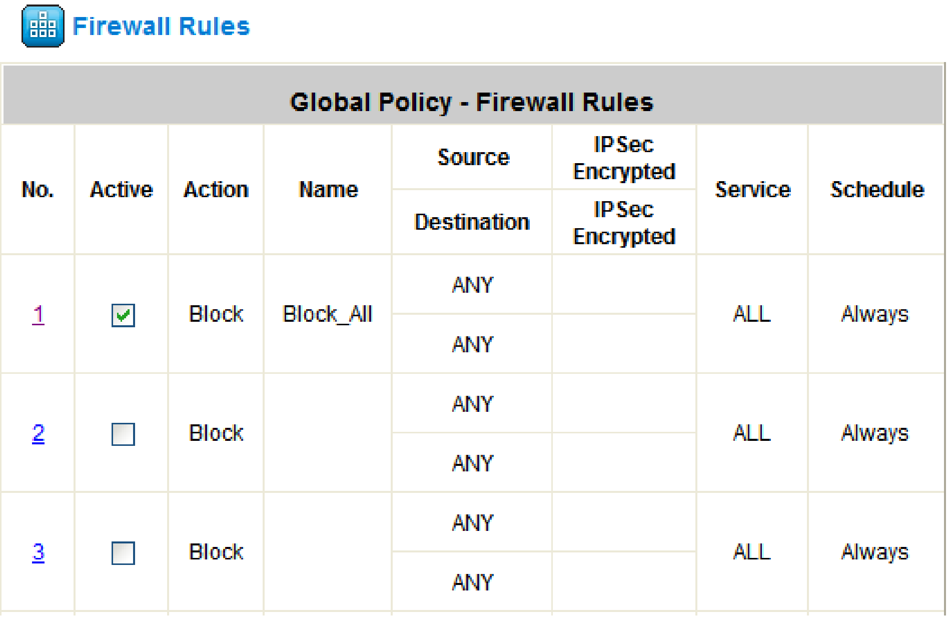


Edit Filter Rule

Global Policy - Edit Filter Rule

Rule Item	1		
Rule Name	Block_All		
	Source		Destination
Interface	ALL	Interface	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)
IPSec Traffic	☐	IPSec Traffic	☐
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	● Block ○ Pass		

STEP 5 . Enable the Active of first rule, and click **Apply** to save the setting.



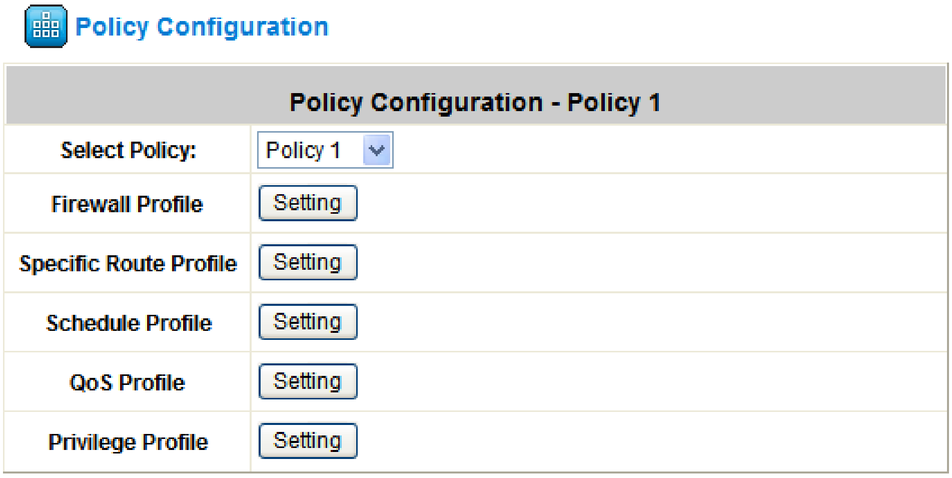
Firewall Rules

Global Policy - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	☑	Block	Block_All	ANY		ALL	Always
				ANY			
2	☐	Block		ANY		ALL	Always
				ANY			
3	☐	Block		ANY		ALL	Always
				ANY			

STEP 6 . When **Global Policy** setting is done, then to configure **Policy 1, 2** and **3**.

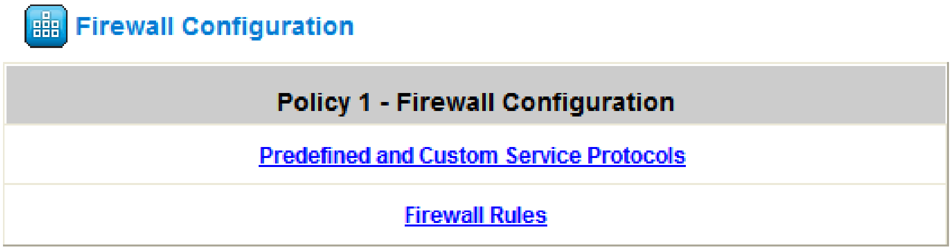
STEP 7 . Configure **Policy 1** to enable the connection from **Airport** Service Zone to Internet, and define the **Traffic Class** as **Best Effort**. Click **Setting** button of **Firewall Profile** to enter the setting.



Policy Configuration

Policy Configuration - Policy 1	
Select Policy:	Policy 1
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

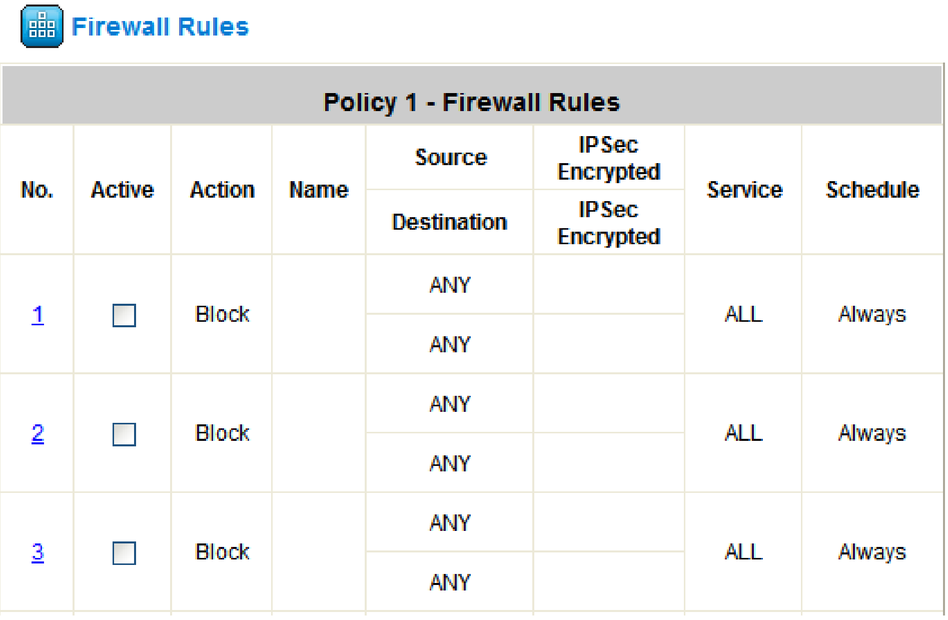
STEP 8 . Click **Firewall Rules** to configure the firewall setting.



Firewall Configuration

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

STEP 9 . Click **No. 1** firewall rule to edit more firewall setting.

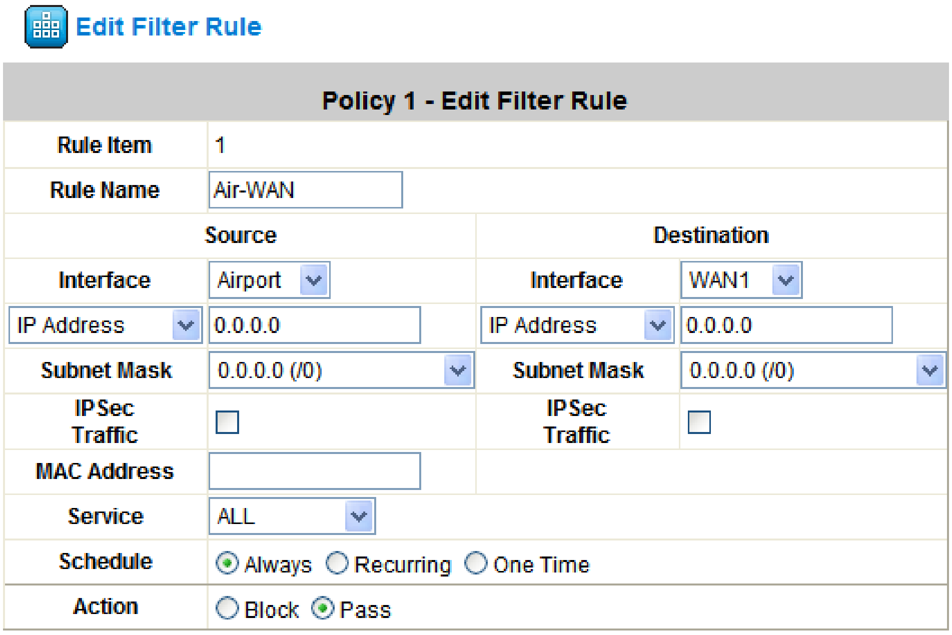


Firewall Rules

Policy 1 - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	☐	Block		ANY		ALL	Always
				ANY			
2	☐	Block		ANY		ALL	Always
				ANY			
3	☐	Block		ANY		ALL	Always
				ANY			

STEP 10 . Input the **Rule name**, select **Source** Interface as **Airport** and **Destination** Interface as **WAN1**, then enable the **Action** to **Pass**.

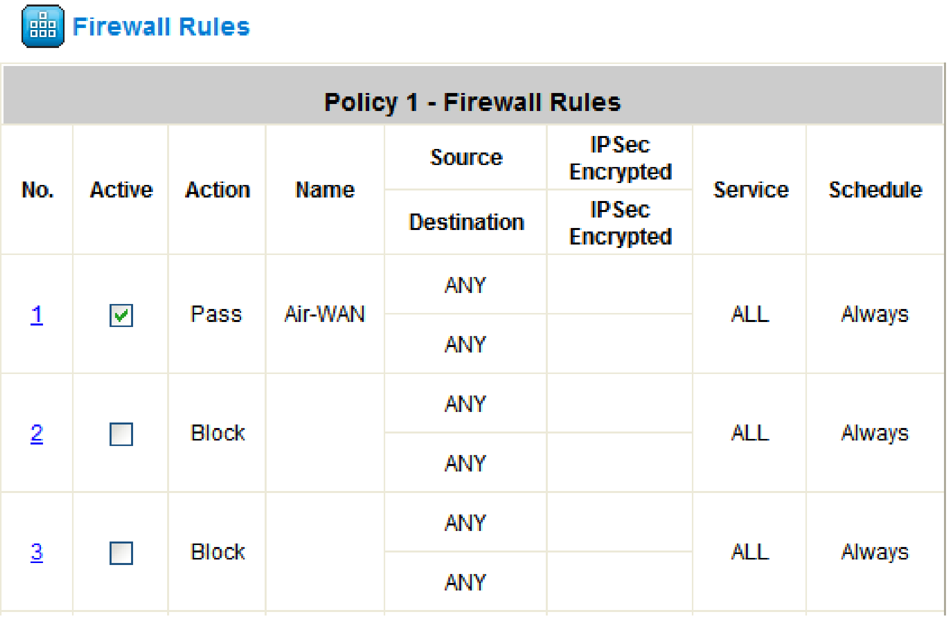


Edit Filter Rule

Policy 1 - Edit Filter Rule

Rule Item	1		
Rule Name	Air-WAN		
	Source		Destination
Interface	Airport	Interface	WAN1
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)
IPSec Traffic	□	IPSec Traffic	□
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	○ Block ● Pass		

STEP 11 . Enable the Active of first rule, and click **Apply** to save the setting.

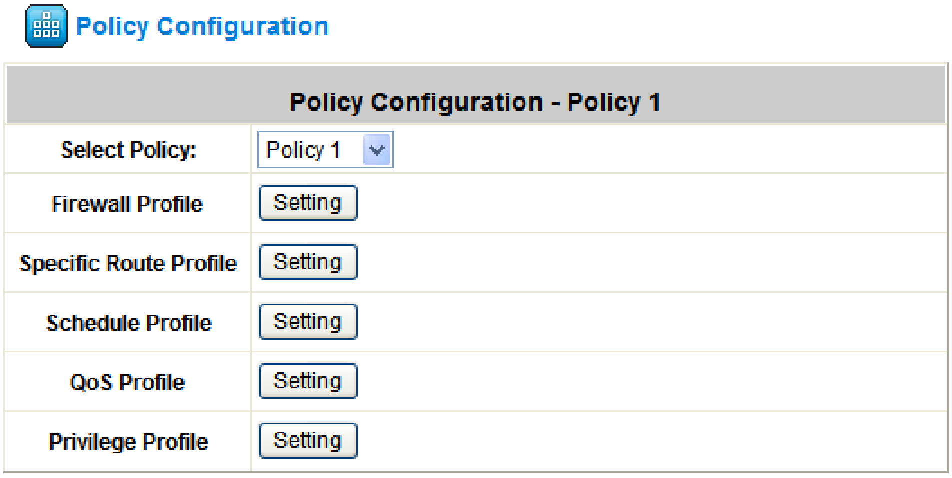


Firewall Rules

Policy 1 - Firewall Rules

No.	Active	Action	Name	Source Destination	IPSec Encrypted IPSec Encrypted	Service	Schedule
1	☑	Pass	Air-WAN	ANY ANY		ALL	Always
2	□	Block		ANY ANY		ALL	Always
3	□	Block		ANY ANY		ALL	Always

STEP 12 . Enter **User Authentication → Policy Configuration**, and press **QoS Profile** button.

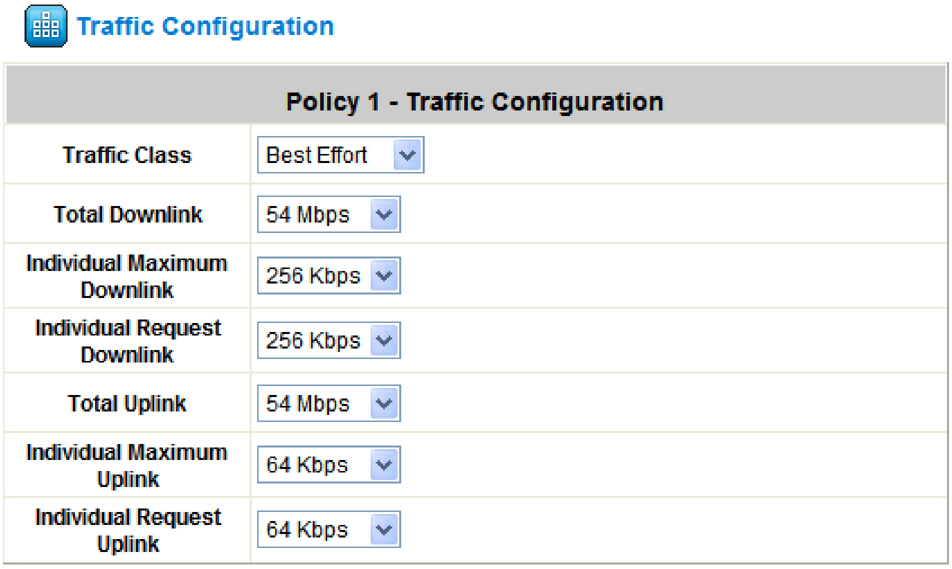


Policy Configuration

Policy Configuration - Policy 1

Select Policy:	Policy 1
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

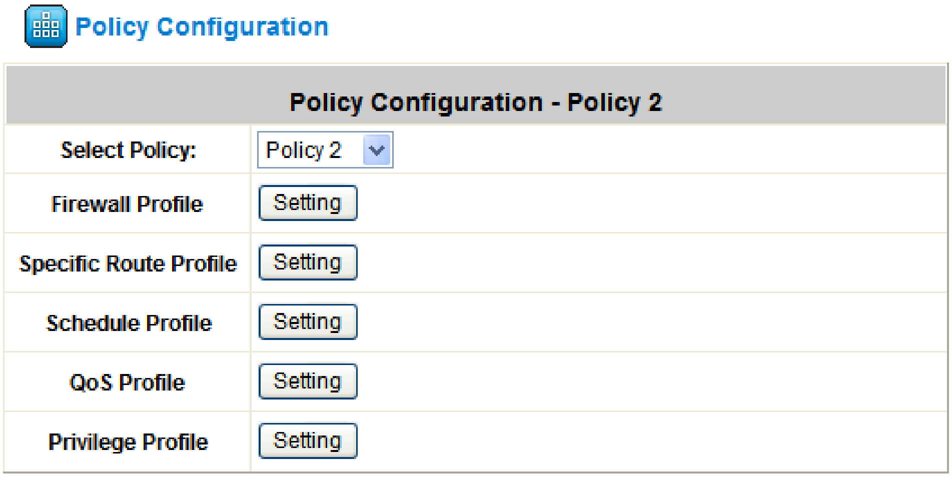
STEP 13 . Select **Best Effort** for **Traffic Class**, and specify the total speed and the limitation for Downlink and Uplink. Click **Apply** to save the setting and finish the configuration of **Policy 1**.



Traffic Configuration

Policy 1 - Traffic Configuration	
Traffic Class	Best Effort
Total Downlink	54 Mbps
Individual Maximum Downlink	256 Kbps
Individual Request Downlink	256 Kbps
Total Uplink	54 Mbps
Individual Maximum Uplink	64 Kbps
Individual Request Uplink	64 Kbps

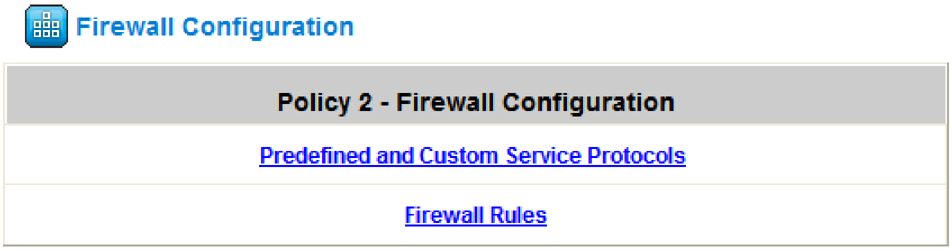
STEP 14 . Configure **Policy 2** to enable the connection from **O2** Service Zone to Internet, and define the **Traffic Class** as **Background**. Click **Setting** button of **Firewall Profile** to enter the setting.



Policy Configuration

Policy Configuration - Policy 2	
Select Policy:	Policy 2
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

STEP 15 . Click **Firewall Rules** to configure the firewall setting.



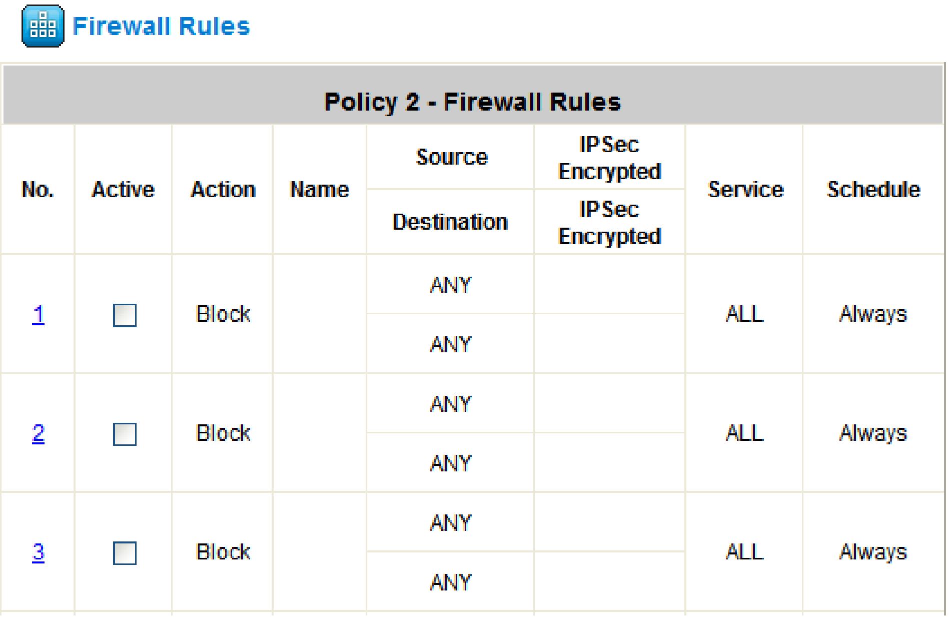
Firewall Configuration

Policy 2 - Firewall Configuration

Predefined and Custom Service Protocols

Firewall Rules

STEP 16 . Click **No. 1** firewall rule to edit more firewall setting.

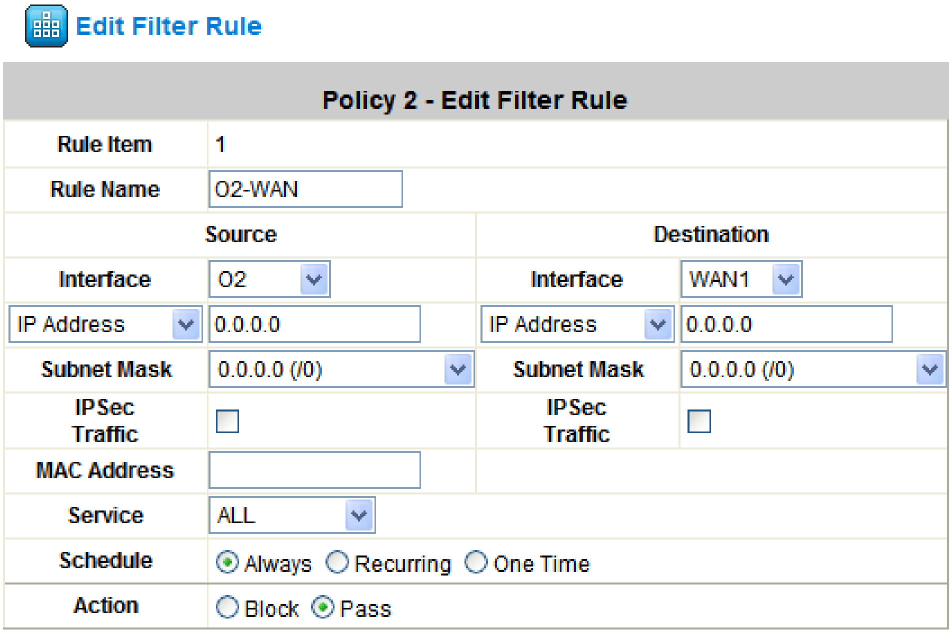


Firewall Rules

Policy 2 - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	□	Block		ANY		ALL	Always
				ANY			
2	□	Block		ANY		ALL	Always
				ANY			
3	□	Block		ANY		ALL	Always
				ANY			

STEP 17 . Input the **Rule name**, select **Source** Interface as **O2** and **Destination** Interface as **WAN1**, then enable the **Action** to **Pass**.

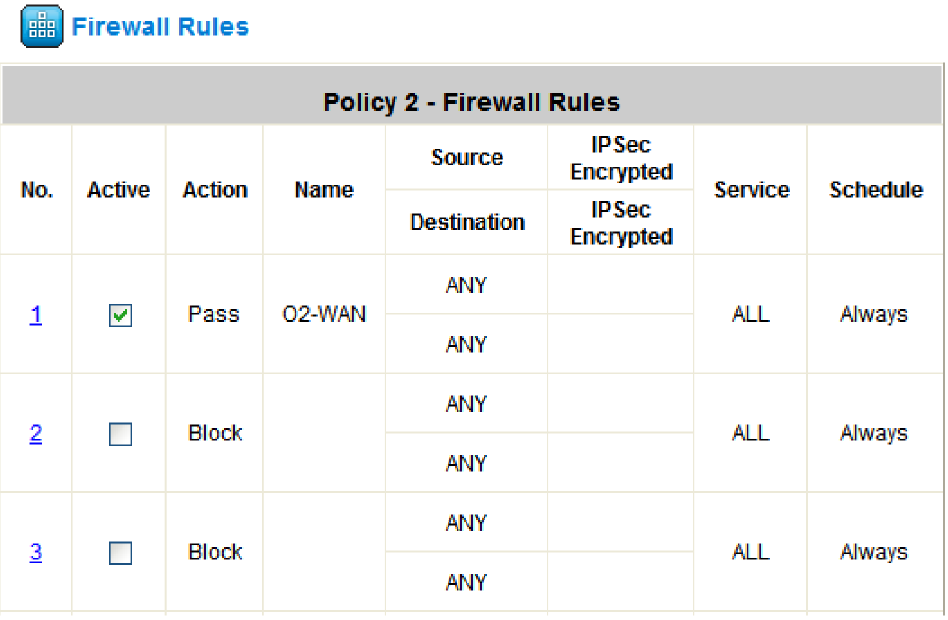


Edit Filter Rule

Policy 2 - Edit Filter Rule

Rule Item	1		
Rule Name	O2-WAN		
Source		Destination	
Interface	O2	Interface	WAN1
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)
IPSec Traffic	□	IPSec Traffic	□
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	○ Block ● Pass		

STEP 18 . Enable the Active of first rule, and click **Apply** to save the setting.

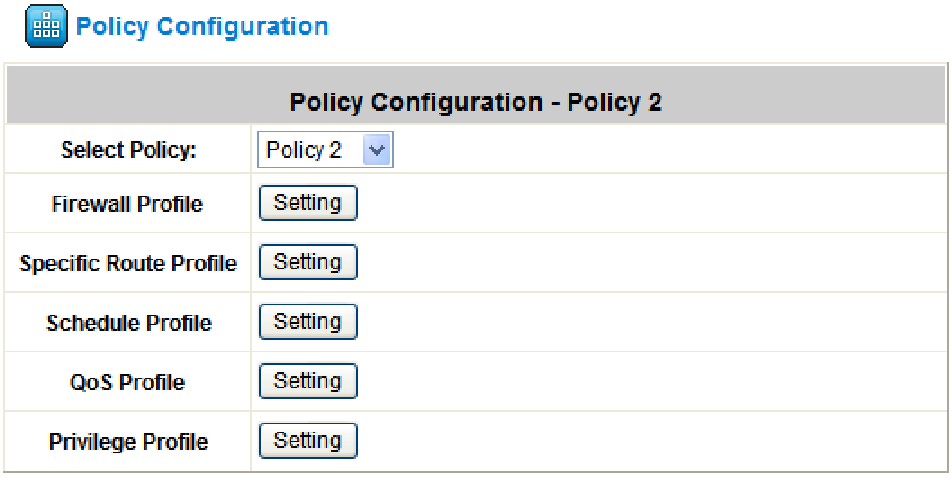


Firewall Rules

Policy 2 - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	☑	Pass	02-WAN	ANY		ALL	Always
				ANY			
2	□	Block		ANY		ALL	Always
				ANY			
3	□	Block		ANY		ALL	Always
				ANY			

STEP 19 . Enter **User Authentication** → **Policy Configuration**, and press **QoS Profile** button.

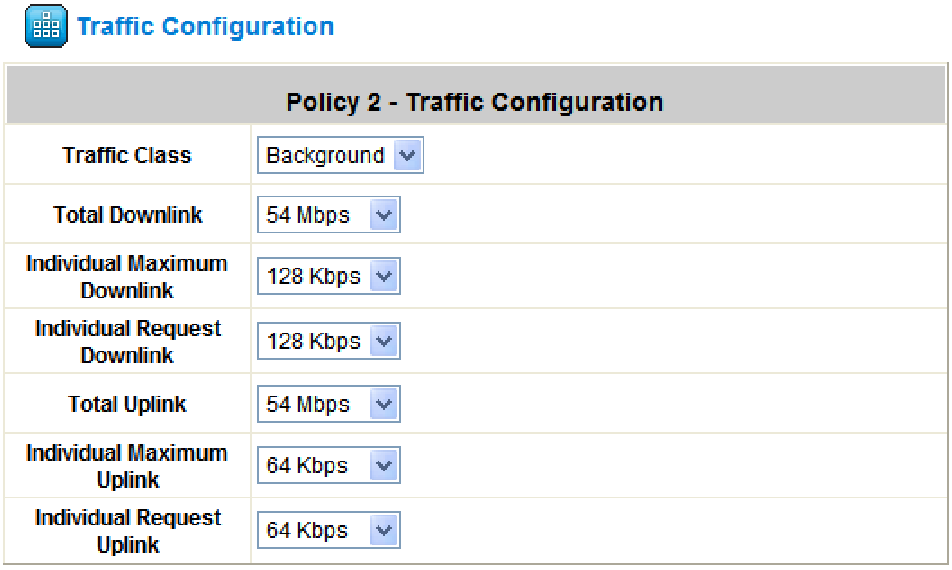


Policy Configuration

Policy Configuration - Policy 2

Select Policy:	Policy 2
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

STEP 20 . Select **Background** for **Traffic Class**, and specify the total speed and the limitation for Downlink and Uplink. Click **Apply** to save the setting and finish the configuration of **Policy 2**.

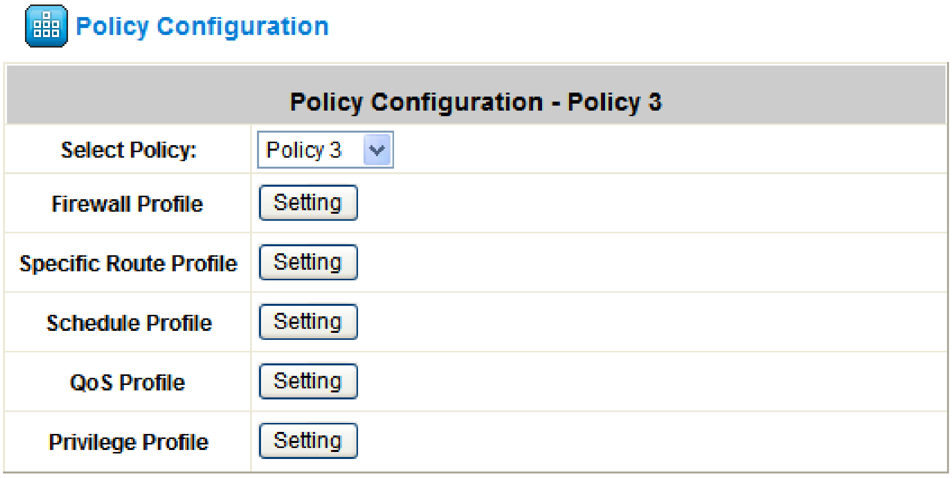


Traffic Configuration

Policy 2 - Traffic Configuration

Traffic Class	Background
Total Downlink	54 Mbps
Individual Maximum Downlink	128 Kbps
Individual Request Downlink	128 Kbps
Total Uplink	54 Mbps
Individual Maximum Uplink	64 Kbps
Individual Request Uplink	64 Kbps

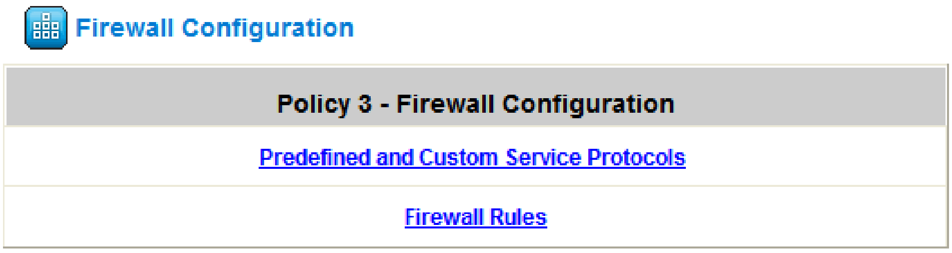
STEP 21 . Configure **Policy 3** to enable the connection from **Orange** Service Zone to Internet, and define the **Traffic Class** as **Background**. Click **Setting** button of **Firewall Profile** to enter the setting.



Policy Configuration

Policy Configuration - Policy 3	
Select Policy:	Policy 3
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

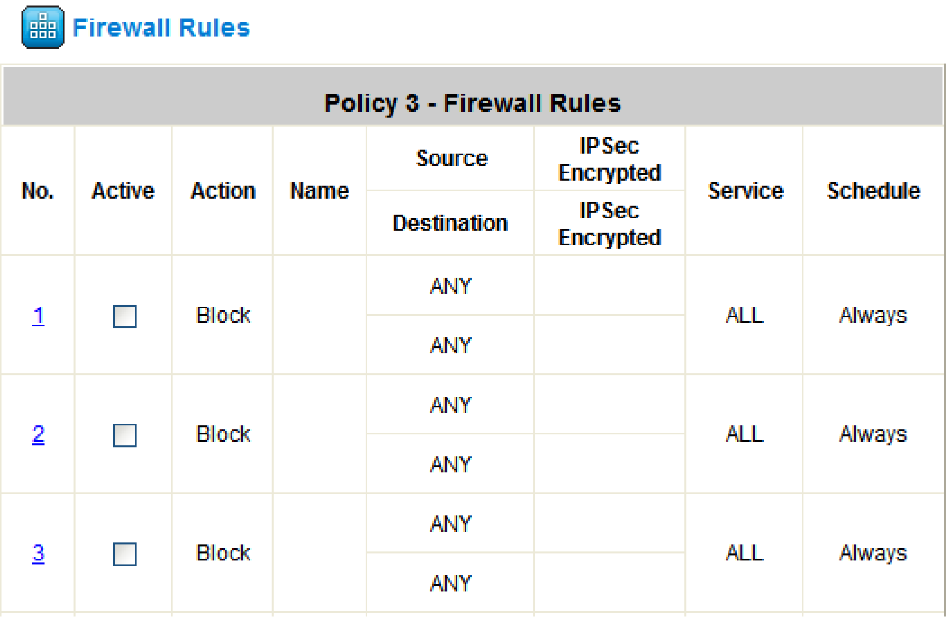
STEP 22 . Click **Firewall Rules** to configure the firewall setting.



Firewall Configuration

Policy 3 - Firewall Configuration
Predefined and Custom Service Protocols
Firewall Rules

STEP 23 . Click **No. 1** firewall rule to edit more firewall setting.

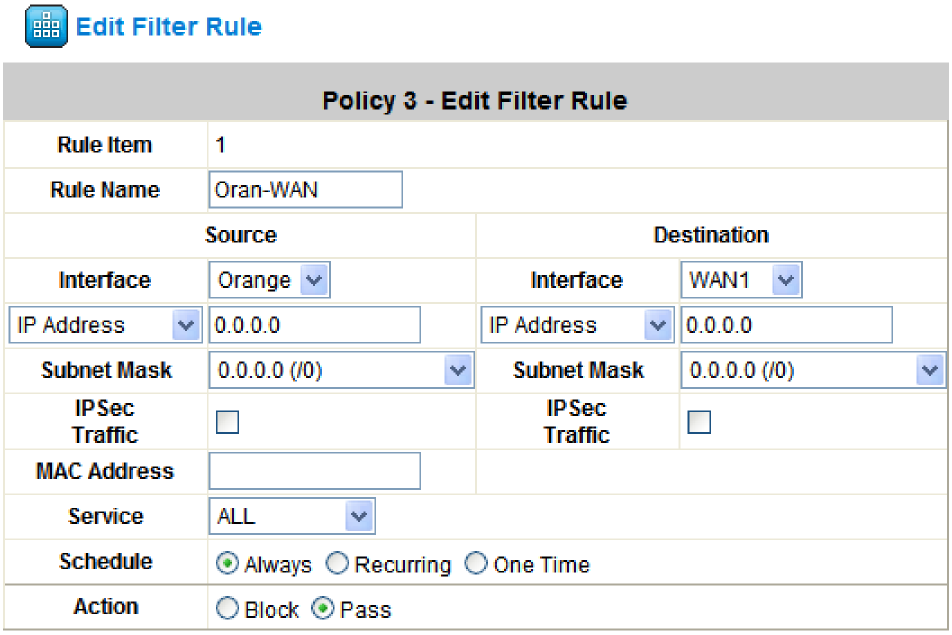


Firewall Rules

Policy 3 - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	□	Block		ANY		ALL	Always
				ANY			
2	□	Block		ANY		ALL	Always
				ANY			
3	□	Block		ANY		ALL	Always
				ANY			

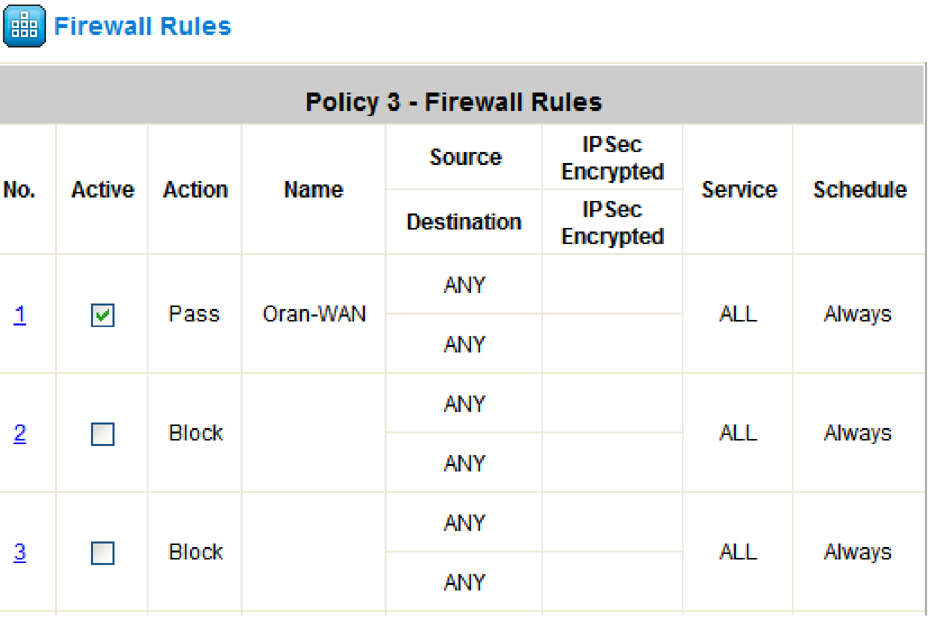
STEP 24 . Input the **Rule name**, select **Source** Interface as **Orange** and **Destination** Interface as **WAN1**, then enable the **Action** to **Pass**.



Edit Filter Rule

Policy 3 - Edit Filter Rule			
Rule Item	1		
Rule Name	Oran-WAN		
Source		Destination	
Interface	Orange	Interface	WAN1
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)
IPSec Traffic	□	IPSec Traffic	□
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	○ Block ● Pass		

STEP 25 . Enable the Active of first rule, and click **Apply** to save the setting.

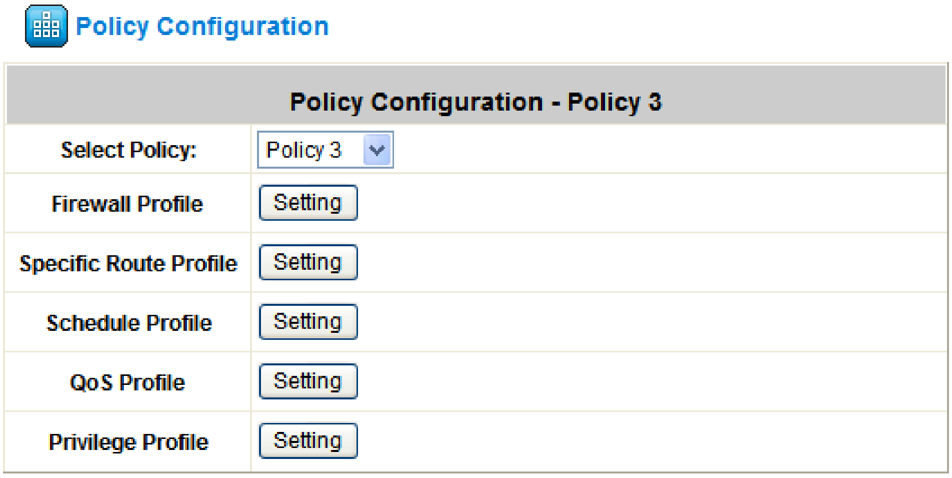


Firewall Rules

Policy 3 - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	☑	Pass	Oran-WAN	ANY		ALL	Always
				ANY			
2	□	Block		ANY		ALL	Always
				ANY			
3	□	Block		ANY		ALL	Always
				ANY			

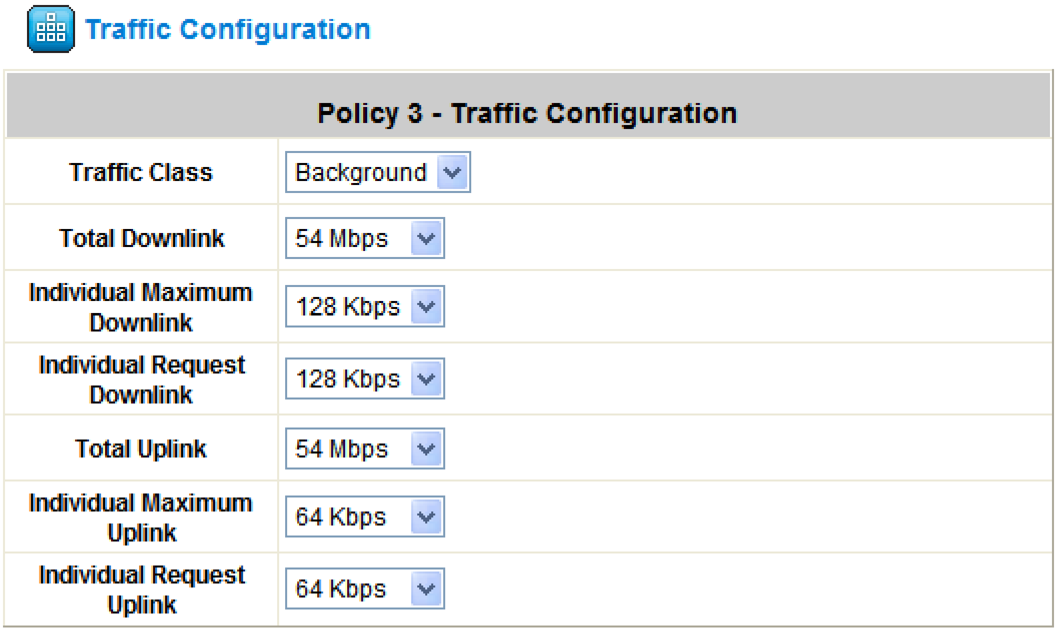
STEP 26 . Enter **User Authentication → Policy Configuration**, and press **QoS Profile** button.



Policy Configuration

Policy Configuration - Policy 3	
Select Policy:	Policy 3
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

STEP 27 . Select **Background** for **Traffic Class**, and specify the total speed and the limitation for Downlink and Uplink. Click **Apply** to save the setting and finish the configuration of **Policy 3**.



Traffic Configuration

Policy 3 - Traffic Configuration	
Traffic Class	Background
Total Downlink	54 Mbps
Individual Maximum Downlink	128 Kbps
Individual Request Downlink	128 Kbps
Total Uplink	54 Mbps
Individual Maximum Uplink	64 Kbps
Individual Request Uplink	64 Kbps

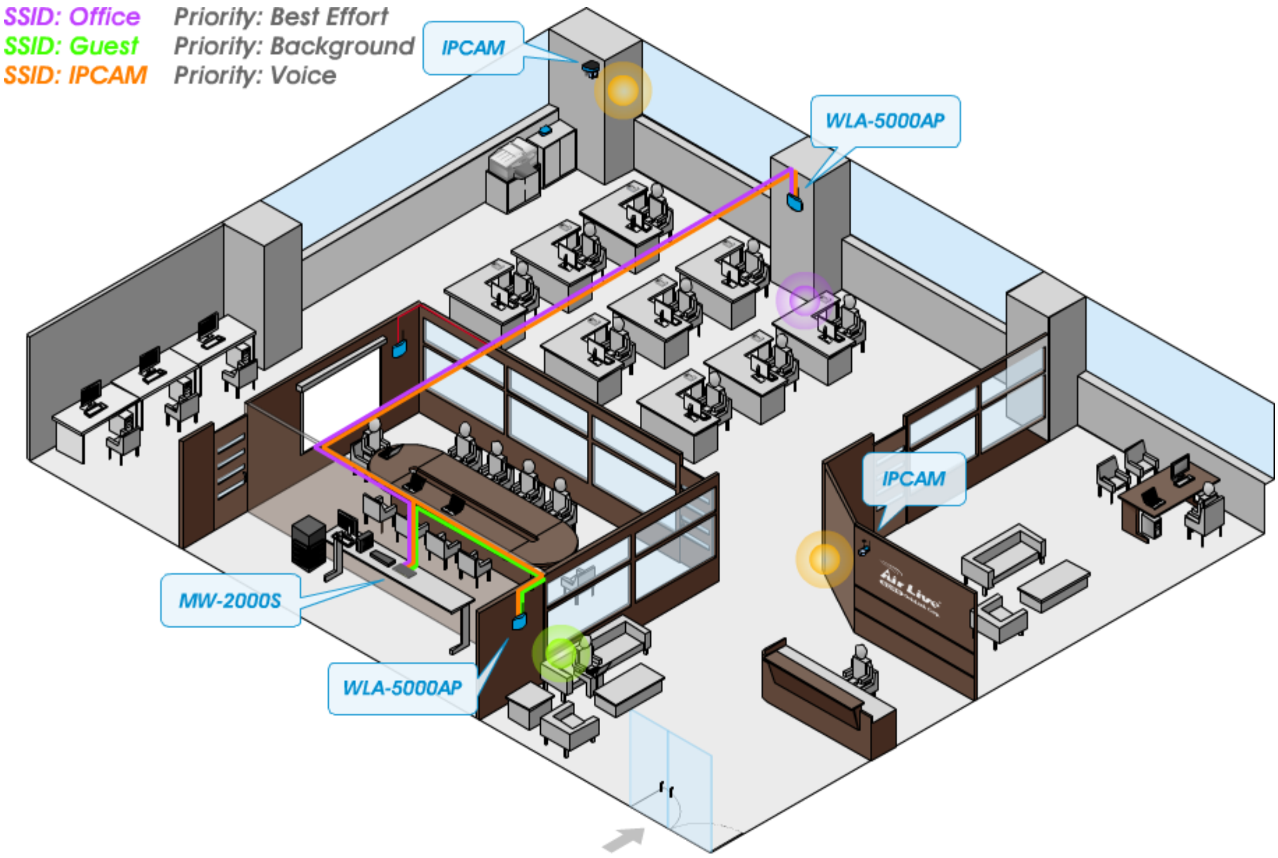
STEP 28 . Multi-Service Providers setting is complete.

Chapter 6. Multi-Service Zones

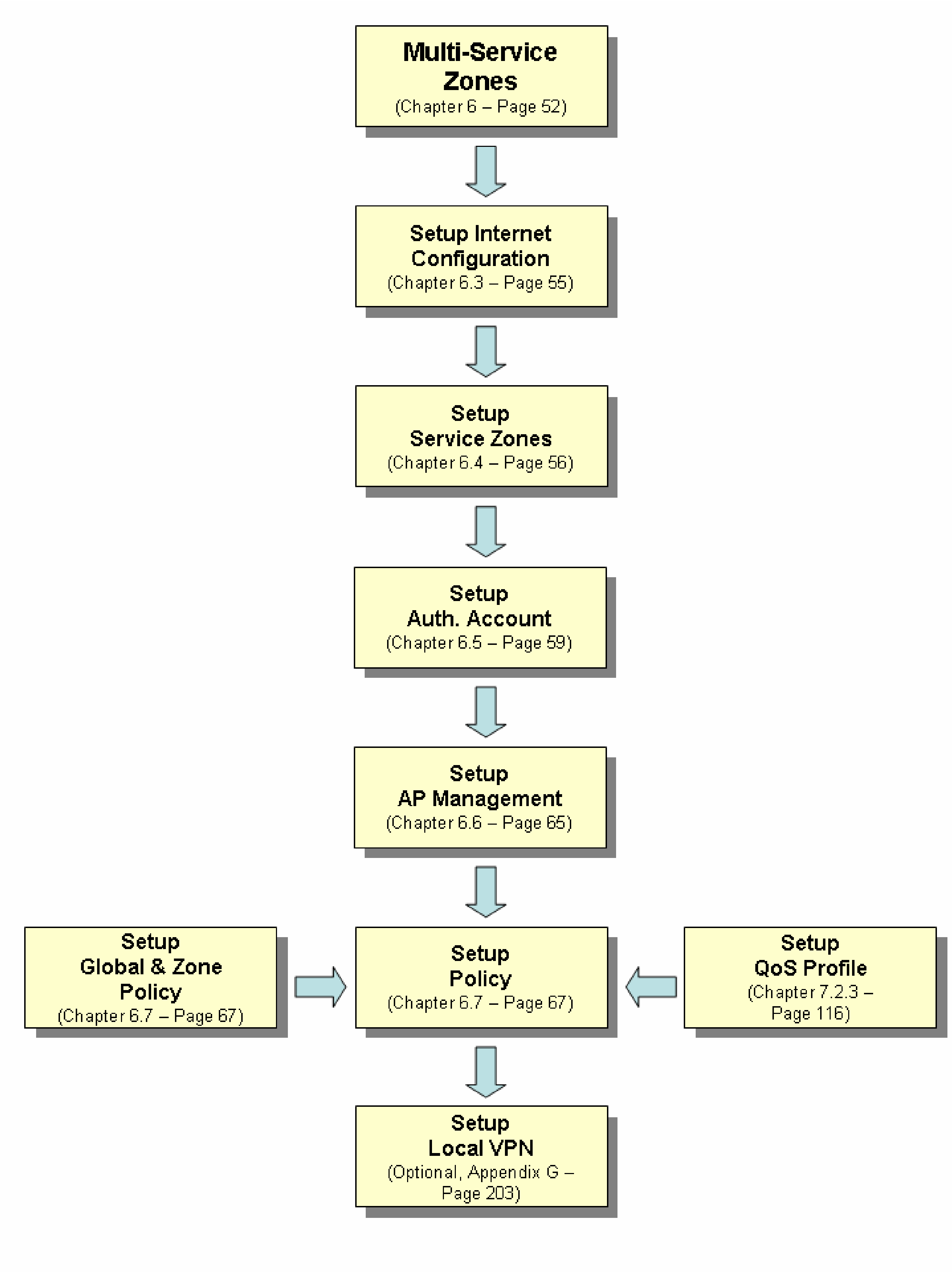
6.1 Introduction

MW-2000S supports WMM QoS to classify packets' priority, **Voice**, **Video**, **Best Effort**, and **Background**. So user can deploy MW-2000S and create several Service Zones with different priority, in order to make internal network more efficiency.

Following steps offer the example of step-by-step configuration. In the example, we will create a **Multi-Service Zones** environment for **Office Users**, **Guest**, and **IPCAM**.



Setup Flow:


Multi-Service Zones
(Chapter 6 – Page 52)
Setup Internet Configuration
(Chapter 6.3 – Page 55)
Setup Service Zones
(Chapter 6.4 – Page 56)
Setup Auth. Account
(Chapter 6.5 – Page 59)
Setup AP Management
(Chapter 6.6 – Page 65)
Setup Global & Zone Policy
(Chapter 6.7 – Page 67)
Setup Policy
(Chapter 6.7 – Page 67)
Setup QoS Profile
(Chapter 7.2.3 – Page 116)
Setup Local VPN
(Optional, Appendix G – Page 203)

6.2 Before to start

There are several things user must pay attention, before you start to configure it:

1. The firmware version must be correct

The current firmware version of MW-2000S is 2.00.00_00900, and WLA-5000AP firmware version must be v2.00e12, or MW-2000S will not succeed to detect WLA-5000AP.

2. WLA-5000AP must be reset with default setting

If user would like to allow MW-2000S auto-detecting WLA-5000AP, the WLA-5000AP device must be reset with default setting, or MW-2000S will not succeed to detect WLA-5000AP.

3. Do not power off MW-2000S and WLA-5000AP during auto-configuring WLA-5000AP

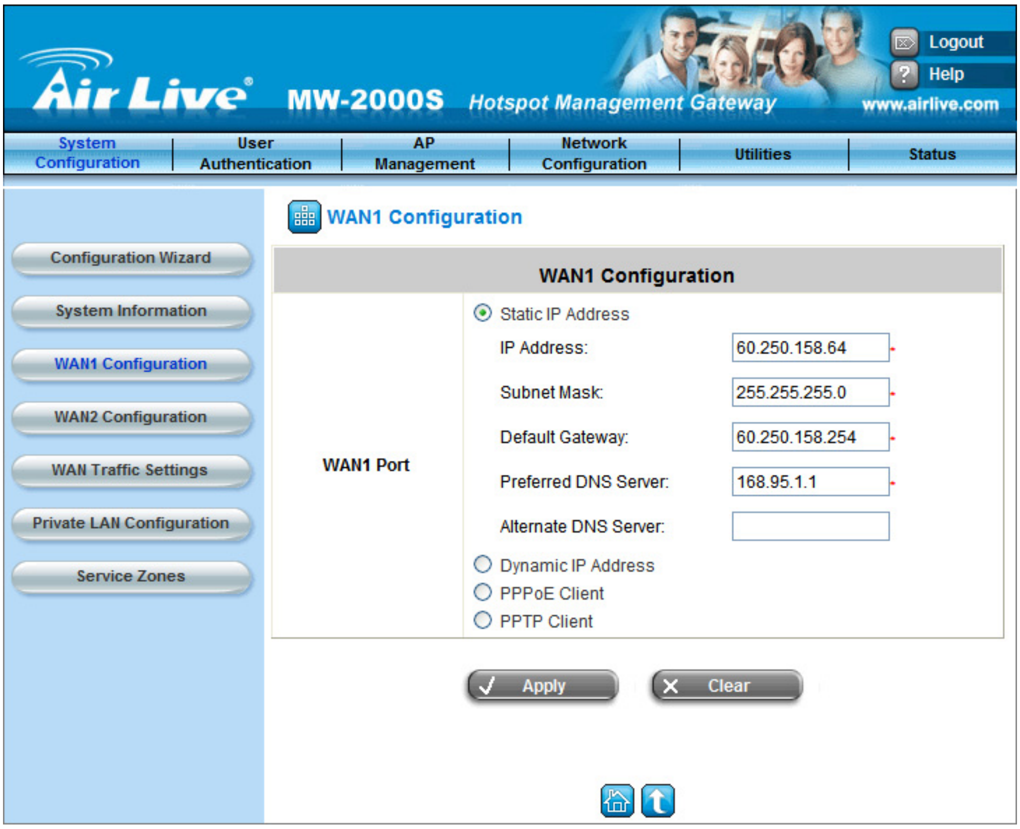
When MW-2000S starts to configure WLA-5000AP, user may not power off MW-2000S or WLA-5000AP, or it could damage WLA-5000AP, and possibly can not rescue it back even restore the boot loader.

User can follow the steps to create your own Multi-Service Zones setting:

Chapter 6.3 – Setup Internet Connection
Chapter 6.4 – Setup Service Zones
Chapter 6.5 – Setup Authentication Account
Chapter 6.6 – Setup AP Management
Chapter 6.7 – Setup Policy Configuration

6.3 Setup Internet Connection

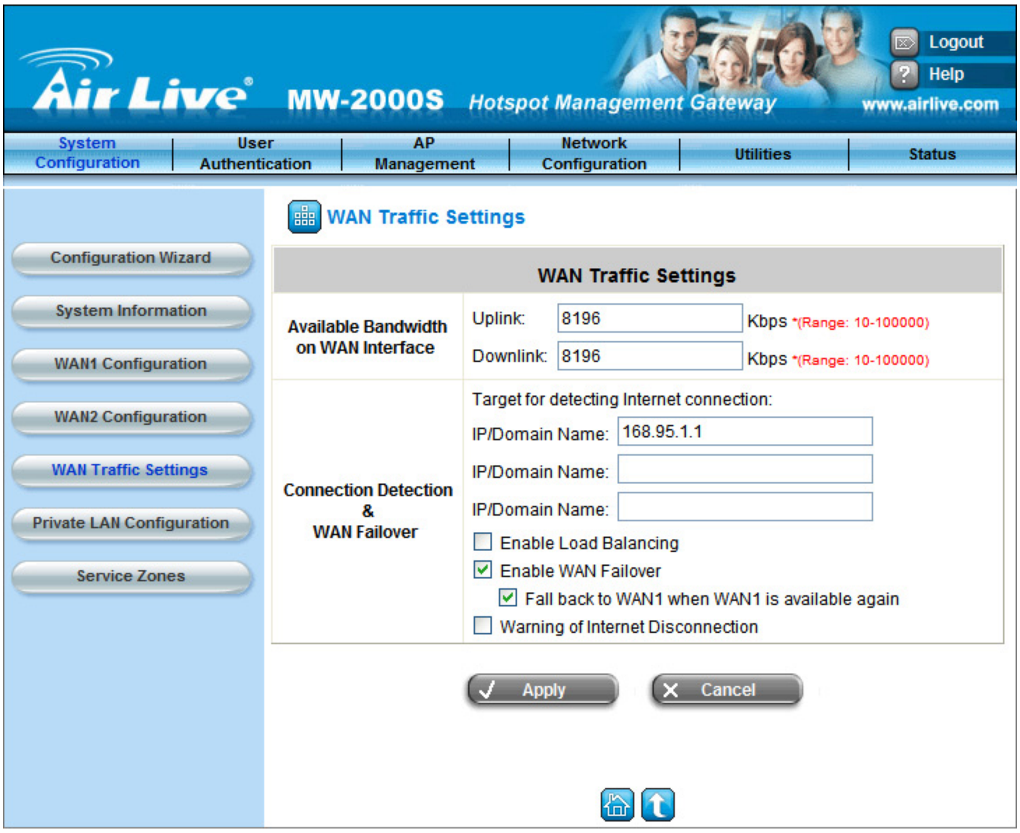
STEP 1 . Enter **System Configuration → WAN1 Configuration** to define the WAN connection. User can configure WAN connecting type with Static IP, Dynamic IP, PPPoE, or PPTP client based on the request.



WAN1 Configuration

WAN1 Configuration	
WAN1 Port	● Static IP Address IP Address: 60.250.158.64 * Subnet Mask: 255.255.255.0 * Default Gateway: 60.250.158.254 * Preferred DNS Server: 168.95.1.1 * Alternate DNS Server: ○ Dynamic IP Address ○ PPPoE Client ○ PPTP Client

STEP 2 . If user applies two Internet connections, the second line can be setup at WAN2, and enable Load balancing or Failover function at **WAN Traffic Setting**. For more information to configure WAN port setting, please check ***Chapter 7.1.3***, ***Chapter 7.1.4***, and ***Chapter 7.1.5***.



WAN Traffic Settings

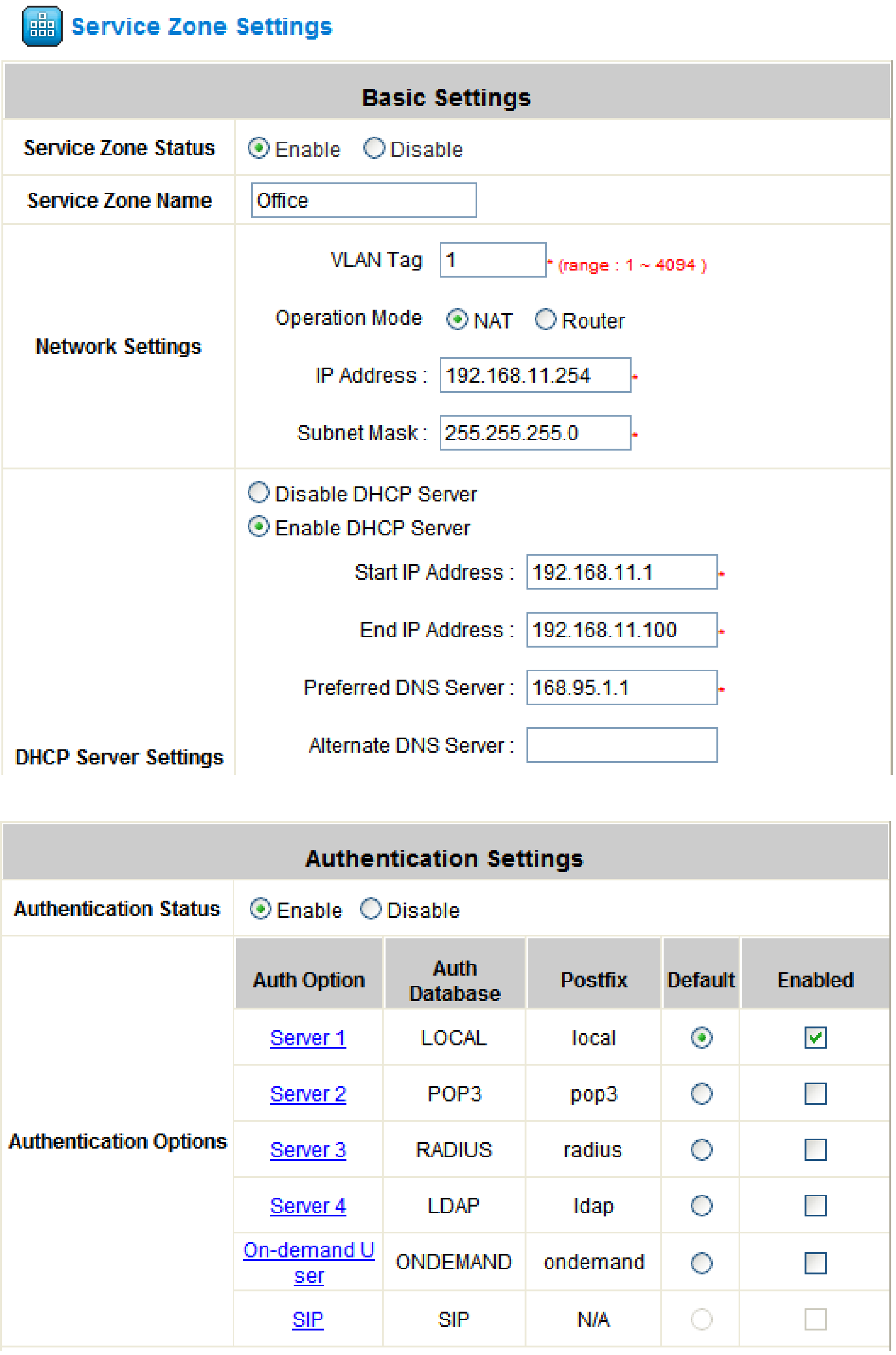
WAN Traffic Settings	
Available Bandwidth on WAN Interface	Uplink: 8196 Kbps *(Range: 10-100000) Downlink: 8196 Kbps *(Range: 10-100000)
Connection Detection & WAN Failover	Target for detecting Internet connection: IP/Domain Name: 168.95.1.1 IP/Domain Name: IP/Domain Name: □ Enable Load Balancing ☑ Enable WAN Failover ☑ Fall back to WAN1 when WAN1 is available again □ Warning of Internet Disconnection

6.4 Setup Service Zones

Environment:

Service Zone	SSID	IP Subnet	Authentication	Policy	Priority
Office	Office	192.168.11.x	Local database	Policy 1	Best Effort
IPCAM	IPCAM	192.168.12.x	Disable	Policy 2	Video
Guest	Guest	192.168.13.x	On-demand	Policy 3	Background

STEP 1 . **System Configuration → Service Zones:** Create the first Service Zone for office worker. You can check ***Chapter 7.1.7*** for more information about **Service Zones**.



Service Zone Settings

Basic Settings

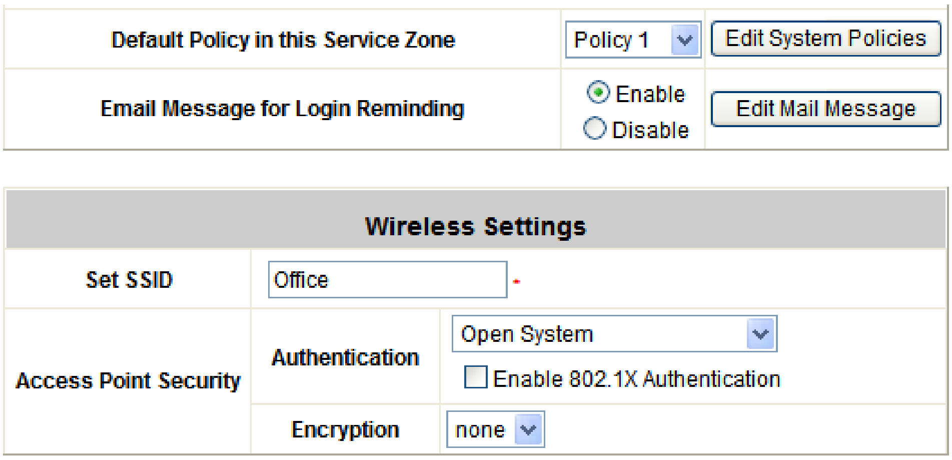
Service Zone Status	● Enable ○ Disable
Service Zone Name	Office
Network Settings	VLAN Tag 1 * (range : 1 ~ 4094) Operation Mode ● NAT ○ Router IP Address : 192.168.11.254 * Subnet Mask : 255.255.255.0 *
DHCP Server Settings	○ Disable DHCP Server ● Enable DHCP Server Start IP Address : 192.168.11.1 * End IP Address : 192.168.11.100 * Preferred DNS Server : 168.95.1.1 * Alternate DNS Server :

Authentication Settings

Authentication Status ● Enable ○ Disable

Authentication Options

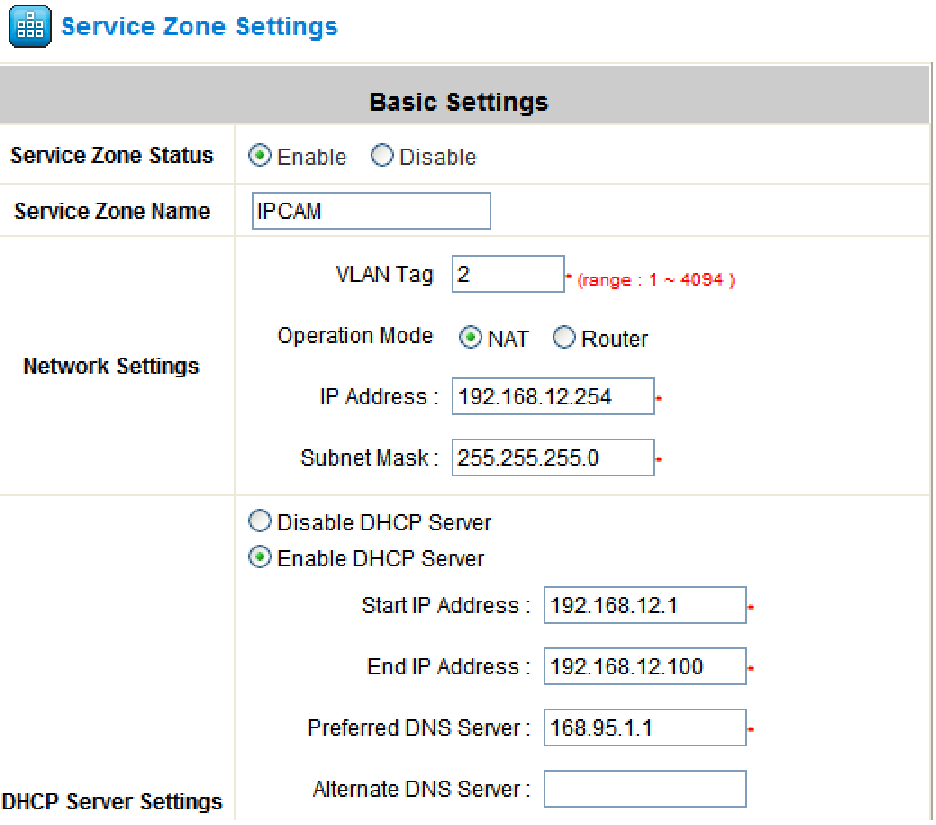
Auth Option	Auth Database	Postfix	Default	Enabled
Server 1	LOCAL	local	●	☑
Server 2	POP3	pop3	○	□
Server 3	RADIUS	radius	○	□
Server 4	LDAP	ldap	○	□
On-demand User	ONDEMAND	ondemand	○	□
SIP	SIP	N/A	○	□



Default Policy in this Service Zone	Policy 1	Edit System Policies
Email Message for Login Reminding	● Enable ○ Disable	Edit Mail Message

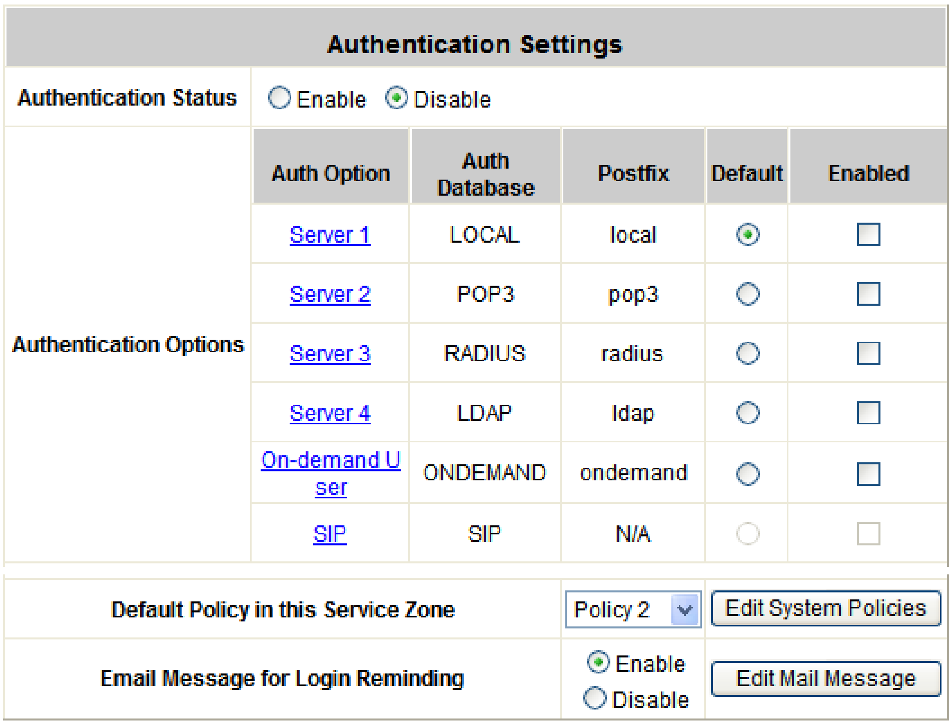
Wireless Settings		
Set SSID	Office *	
Access Point Security	Authentication	Open System □ Enable 802.1X Authentication
	Encryption	none

STEP 2 . **System Configuration → Service Zones:** Create the second Service Zone for IP Camera.



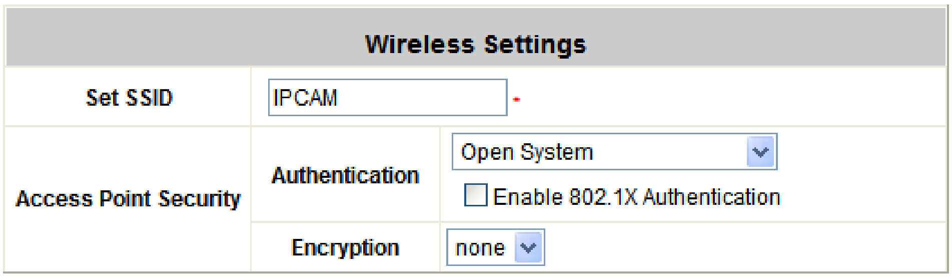
Service Zone Settings

Basic Settings		
Service Zone Status	● Enable ○ Disable	
Service Zone Name	IPCAM	
Network Settings	VLAN Tag	2 * (range : 1 ~ 4094)
	Operation Mode	● NAT ○ Router
	IP Address :	192.168.12.254 *
	Subnet Mask :	255.255.255.0 *
DHCP Server Settings	○ Disable DHCP Server ● Enable DHCP Server	
	Start IP Address :	192.168.12.1 *
	End IP Address :	192.168.12.100 *
	Preferred DNS Server :	168.95.1.1 *
	Alternate DNS Server :	



Authentication Settings					
Authentication Status	○ Enable ● Disable				
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	○	□

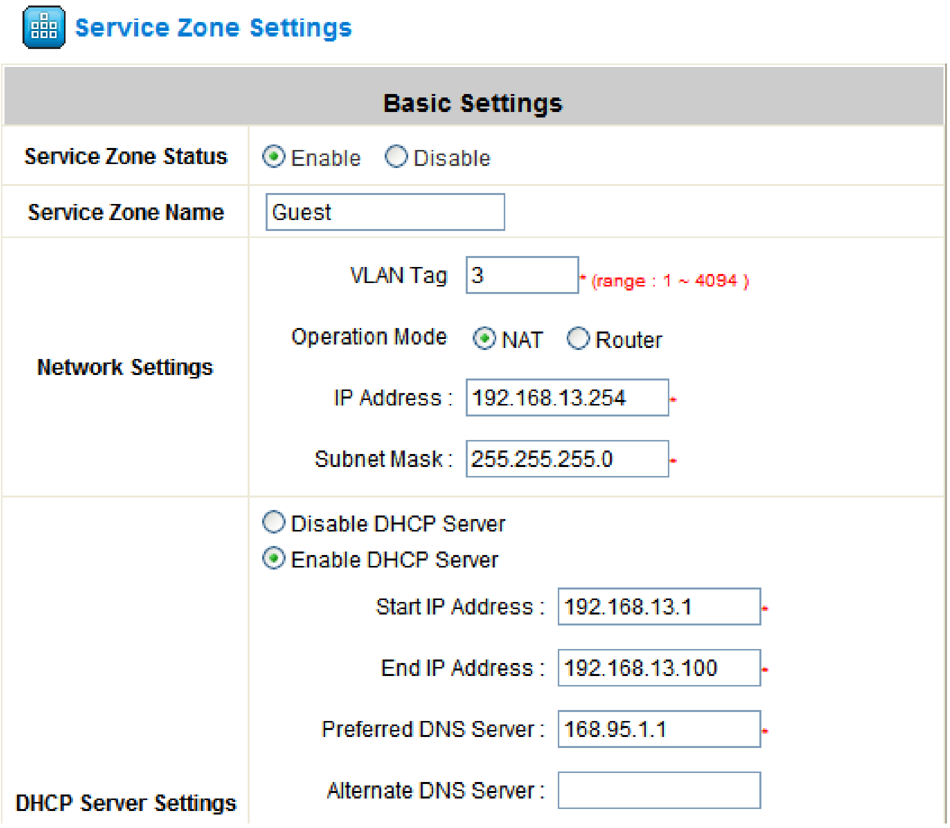
Default Policy in this Service Zone	Policy 2	Edit System Policies
Email Message for Login Reminding	● Enable ○ Disable	Edit Mail Message



Wireless Settings		
Set SSID	IPCAM *	
Access Point Security	Authentication	Open System □ Enable 802.1X Authentication
	Encryption	none

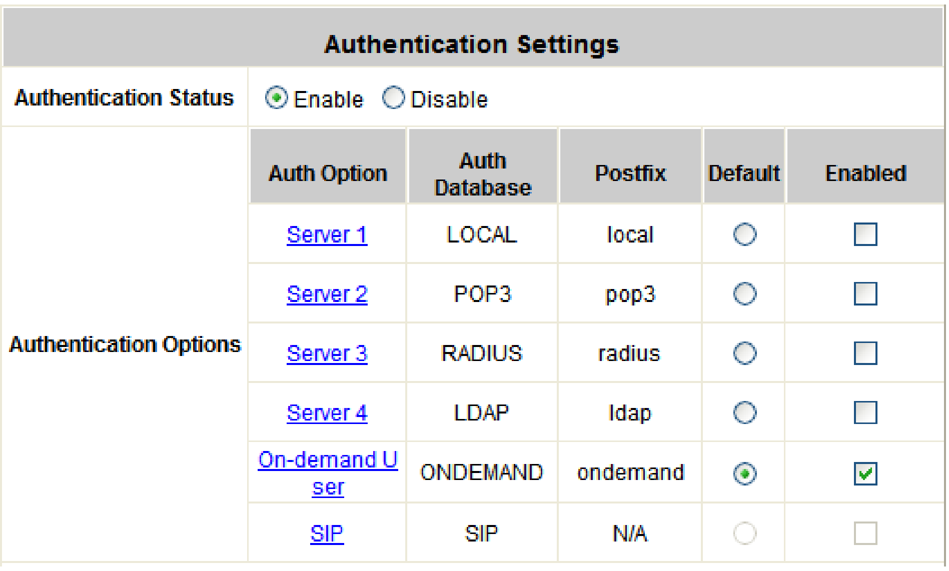
STEP 3 . **System Configuration → Service Zones:** Create the third Service Zone for Guest uses

.



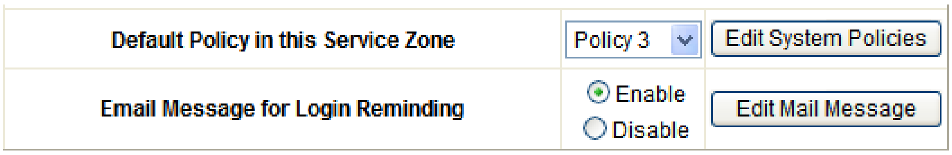
Service Zone Settings

Basic Settings	
Service Zone Status	● Enable ○ Disable
Service Zone Name	Guest
Network Settings	VLAN Tag 3 * (range : 1 ~ 4094) Operation Mode ● NAT ○ Router IP Address : 192.168.13.254 * Subnet Mask : 255.255.255.0 *
DHCP Server Settings	○ Disable DHCP Server ● Enable DHCP Server Start IP Address : 192.168.13.1 * End IP Address : 192.168.13.100 * Preferred DNS Server : 168.95.1.1 * Alternate DNS Server :

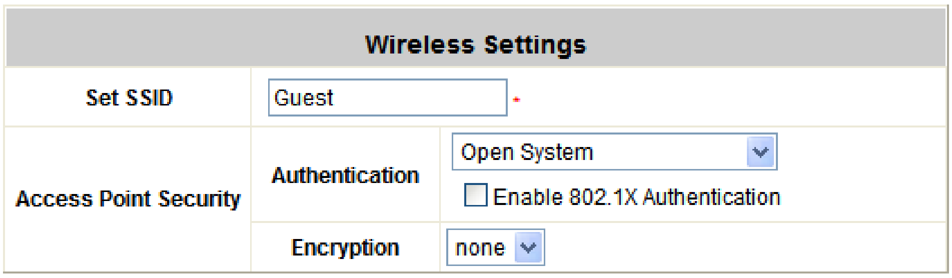


Authentication Settings

Authentication Status	● Enable ○ Disable				
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	○	□



Default Policy in this Service Zone	Policy 3	Edit System Policies
Email Message for Login Reminding	● Enable ○ Disable	Edit Mail Message

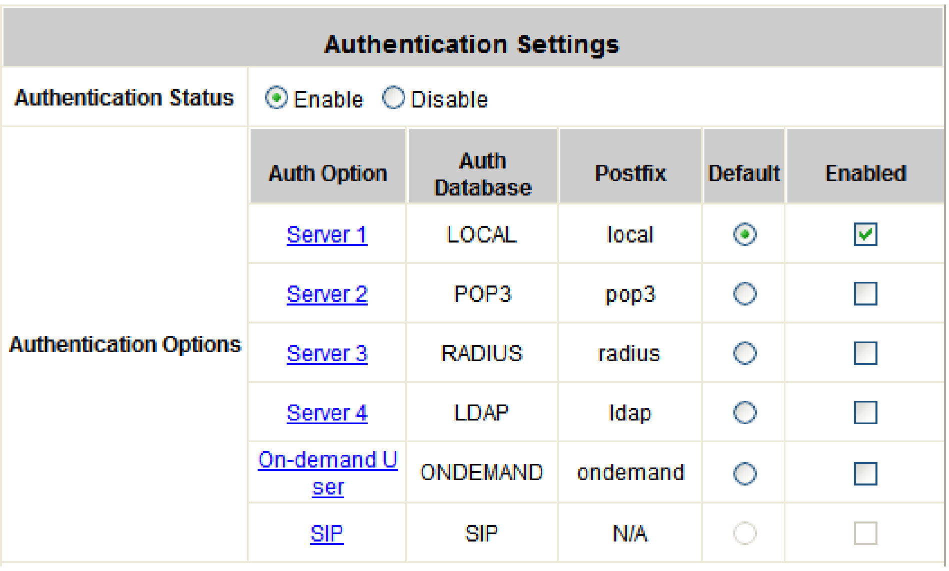


Wireless Settings

Set SSID	Guest *	
Access Point Security	Authentication	Open System □ Enable 802.1X Authentication
	Encryption	none

6.5 Setup Authentication Account

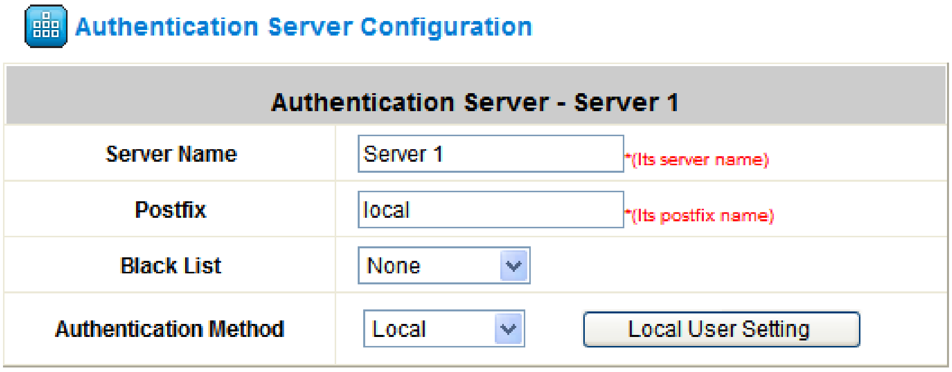
STEP 1 . Create Local database account for office worker. Select Server1 as default server of authentication, and enable the setting. Then click **Server1** to enter the next step.



Authentication Settings

Authentication Status	● Enable ○ Disable				
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	○	□

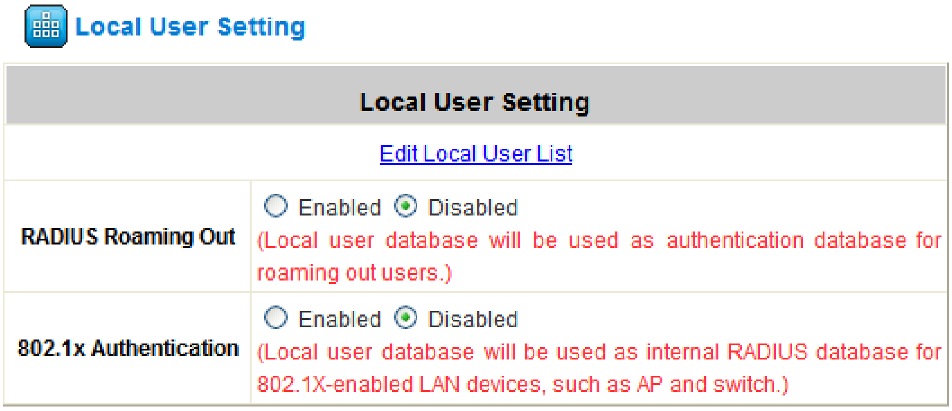
STEP 2 . User can change **Server Name**, **Postfix Name**, or enable **Black List**; select **Local** as **Authentication Method**, and click **Local User Setting** button to enter **Local User Setting** page.



Authentication Server Configuration

Authentication Server - Server 1	
Server Name	Server 1 *(Its server name)
Postfix	local *(Its postfix name)
Black List	None
Authentication Method	Local · Local User Setting

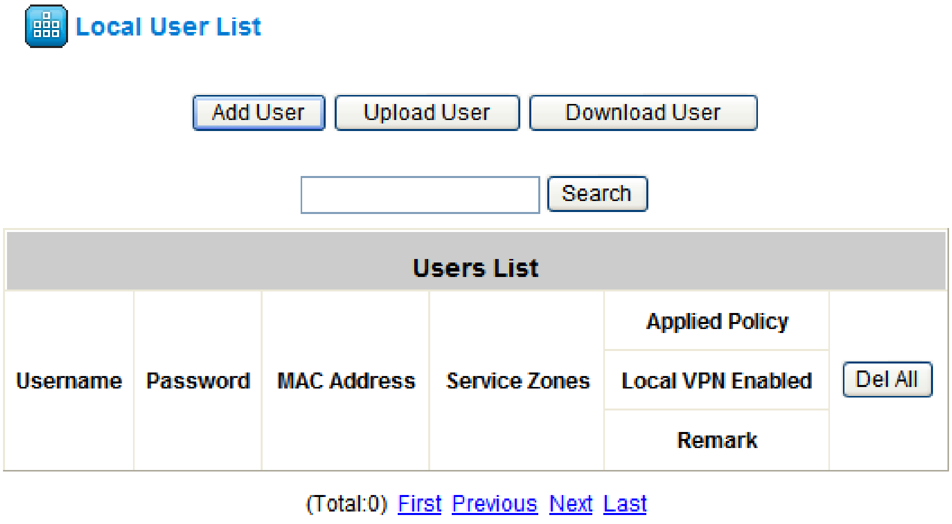
STEP 3 . If user does not need to enable **RADIUS Roaming Out** or **802.1x Authentication**, just click **Edit Local User List** to check current user list or create new local user.



Local User Setting

Local User Setting	
Edit Local User List	
RADIUS Roaming Out	○ Enabled ● Disabled (Local user database will be used as authentication database for roaming out users.)
802.1x Authentication	○ Enabled ● Disabled (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)

STEP 4 . Click **Add User** to create new user.



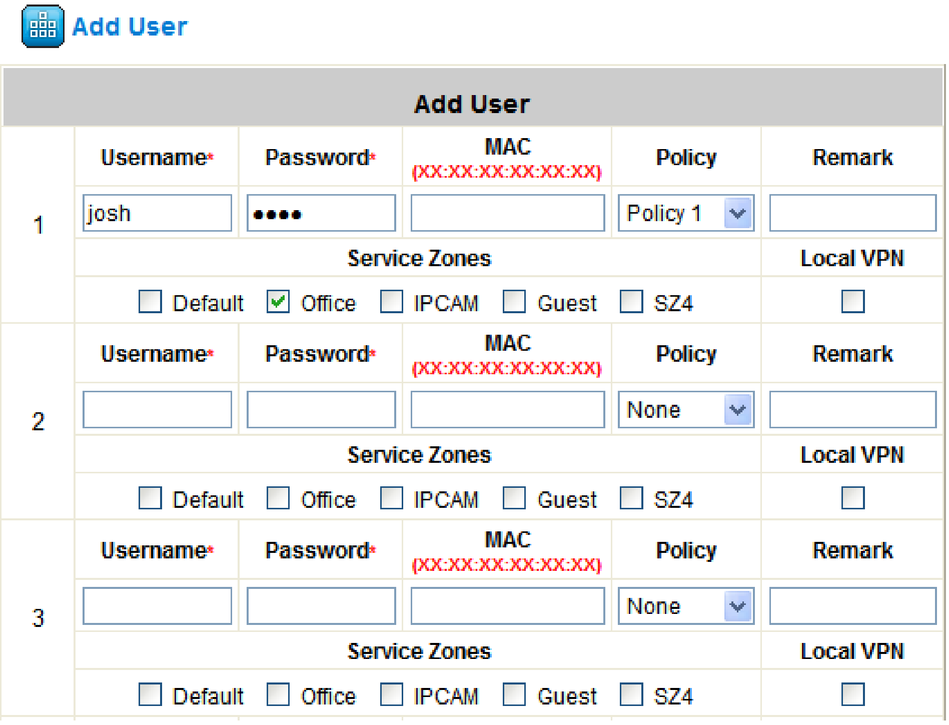
Local User List

Users List

Username	Password	MAC Address	Service Zones	Applied Policy Local VPN Enabled Remark	Del All

(Total:0) First Previous Next Last

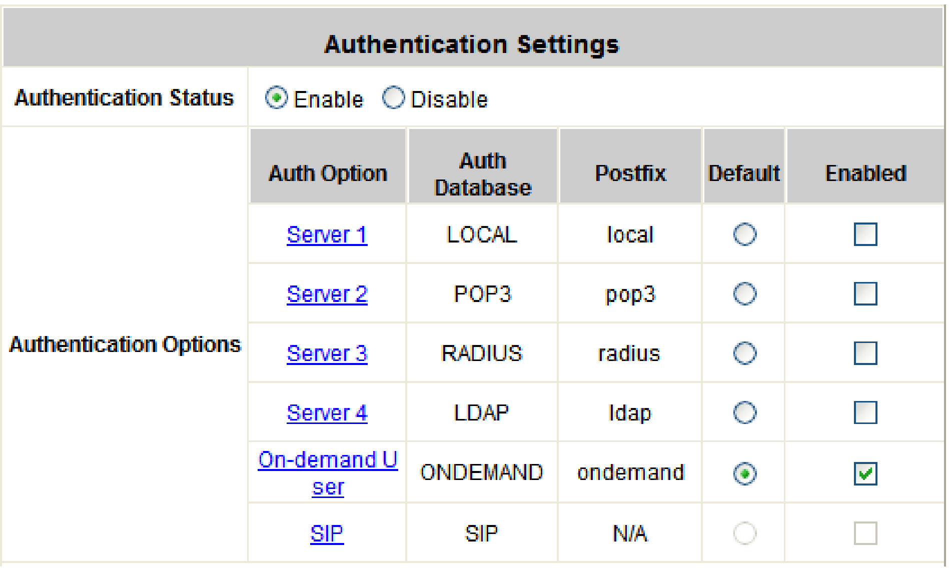
STEP 5 . Fill in **Username**, **Password**, and else information; select a specific **Service Zones**, then click **Apply** to save the setting. For more detail information to setup local user please check ***Chapter 7.2.1.1 Authentication Method – Local***.



Add User

Add User					
1	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
	josh	••••		Policy 1	
	Service Zones				Local VPN
	☐ Default ☑ Office ☐ IPCAM ☐ Guest ☐ SZ4				☐
2	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
				None	
	Service Zones				Local VPN
	☐ Default ☐ Office ☐ IPCAM ☐ Guest ☐ SZ4				☐
3	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
				None	
	Service Zones				Local VPN
	☐ Default ☐ Office ☐ IPCAM ☐ Guest ☐ SZ4				☐

STEP 6 . Setup **On-demand** account for **Guest** user. The account can be generated by randomly, and specify part of limitation. Click **On-demand User** to enter the next step.



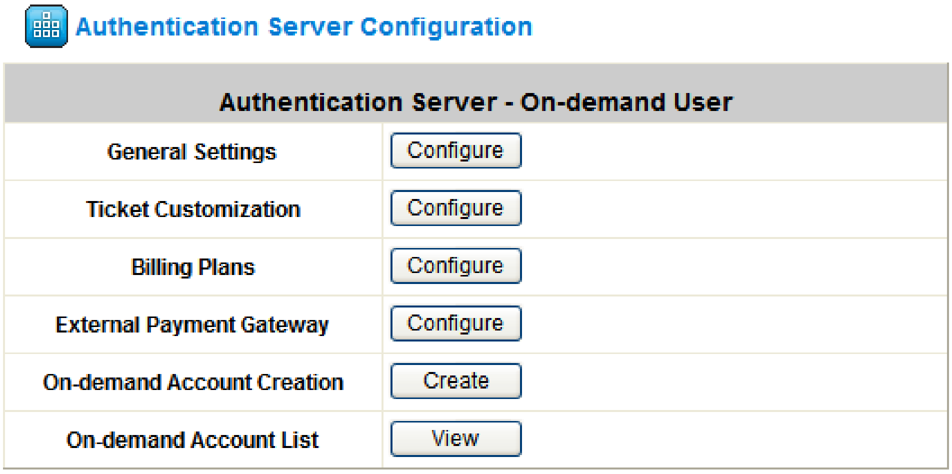
Authentication Settings

Authentication Status: ● Enable ○ Disable

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	○	☐

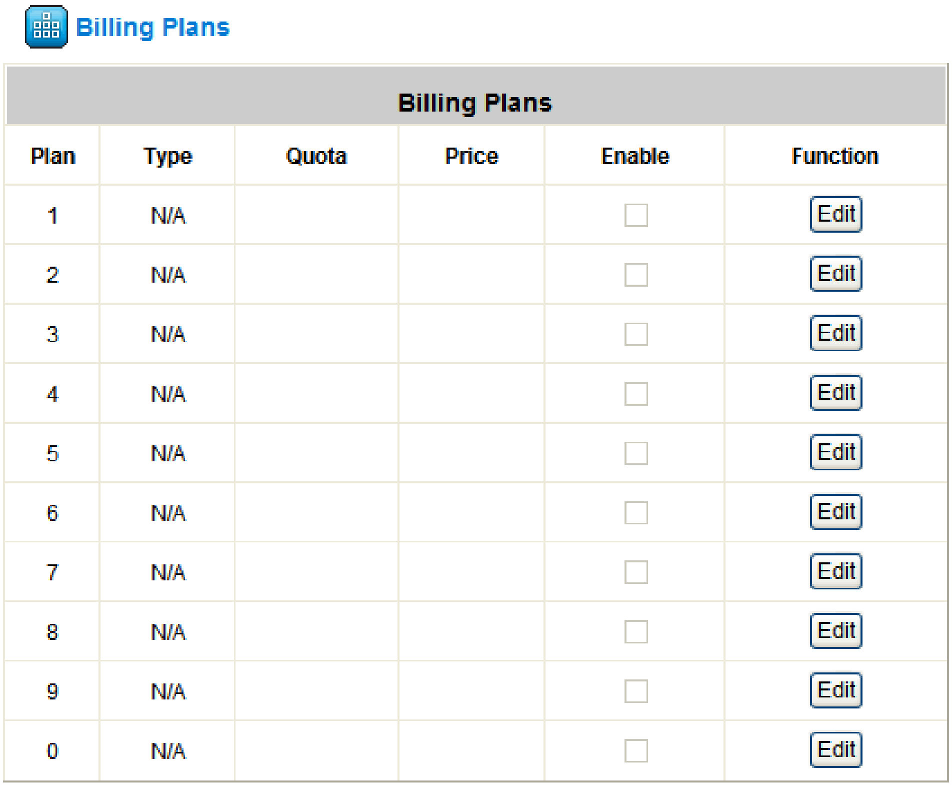
STEP 7 . Click **Configure** button of **Billing Plans** to define the limitation for **Guest** account.



Authentication Server Configuration

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 List	View

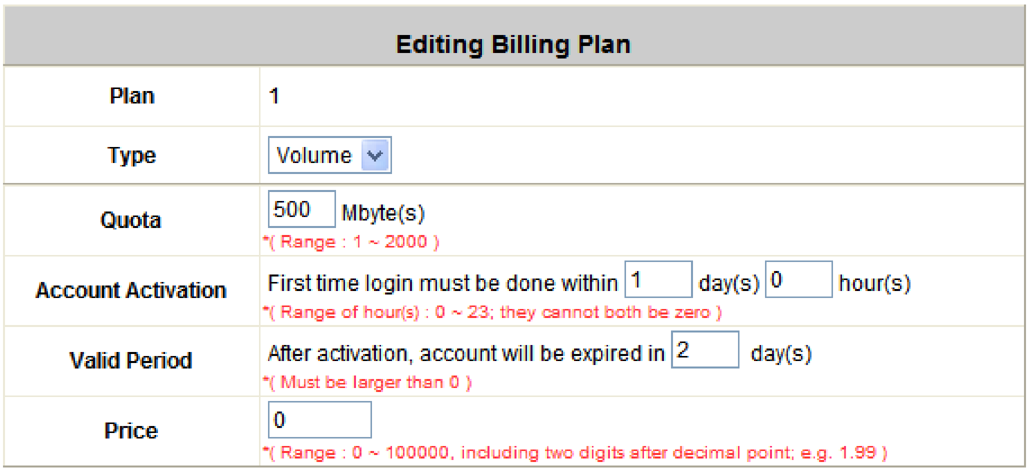
STEP 8 . Click Edit button to configure the setting.



Billing Plans

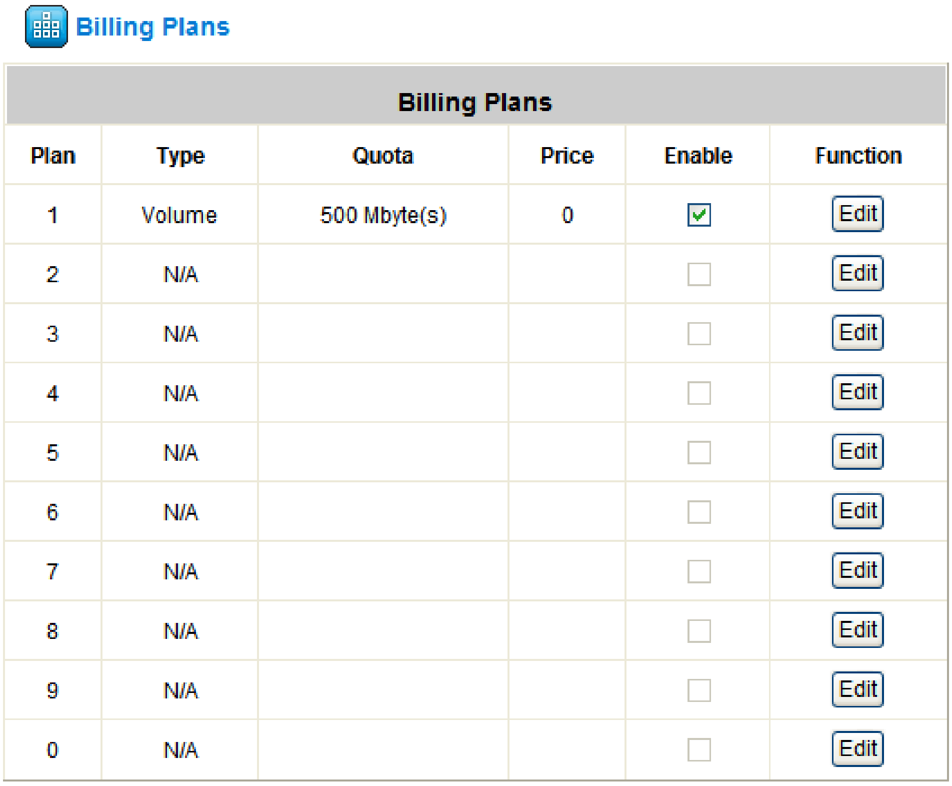
Billing Plans					
Plan	Type	Quota	Price	Enable	Function
1	N/A			□	Edit
2	N/A			□	Edit
3	N/A			□	Edit
4	N/A			□	Edit
5	N/A			□	Edit
6	N/A			□	Edit
7	N/A			□	Edit
8	N/A			□	Edit
9	N/A			□	Edit
0	N/A			□	Edit

STEP 9 . Select **Volume** at **Type**; the available **Quota** is 500Mbyes; guest has to use the account in one day; the account will be expired in 2 days; and the price is free of charge. Click **Apply** to save the configuration.



Editing Billing Plan	
Plan	1
Type	Volume
Quota	500 Mbyte(s) *(Range : 1 ~ 2000)
Account Activation	First time login must be done within 1 day(s) 0 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 2 day(s) *(Must be larger than 0)
Price	0 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)

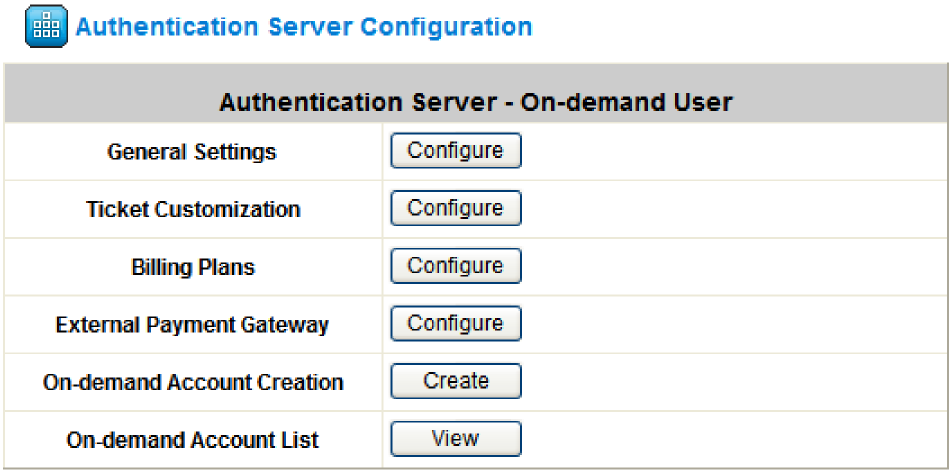
STEP 10 . Click Enable and then click Apply to save the setting.



Billing Plans

Billing Plans					
Plan	Type	Quota	Price	Enable	Function
1	Volume	500 Mbyte(s)	0	☑	Edit
2	N/A			□	Edit
3	N/A			□	Edit
4	N/A			□	Edit
5	N/A			□	Edit
6	N/A			□	Edit
7	N/A			□	Edit
8	N/A			□	Edit
9	N/A			□	Edit
0	N/A			□	Edit

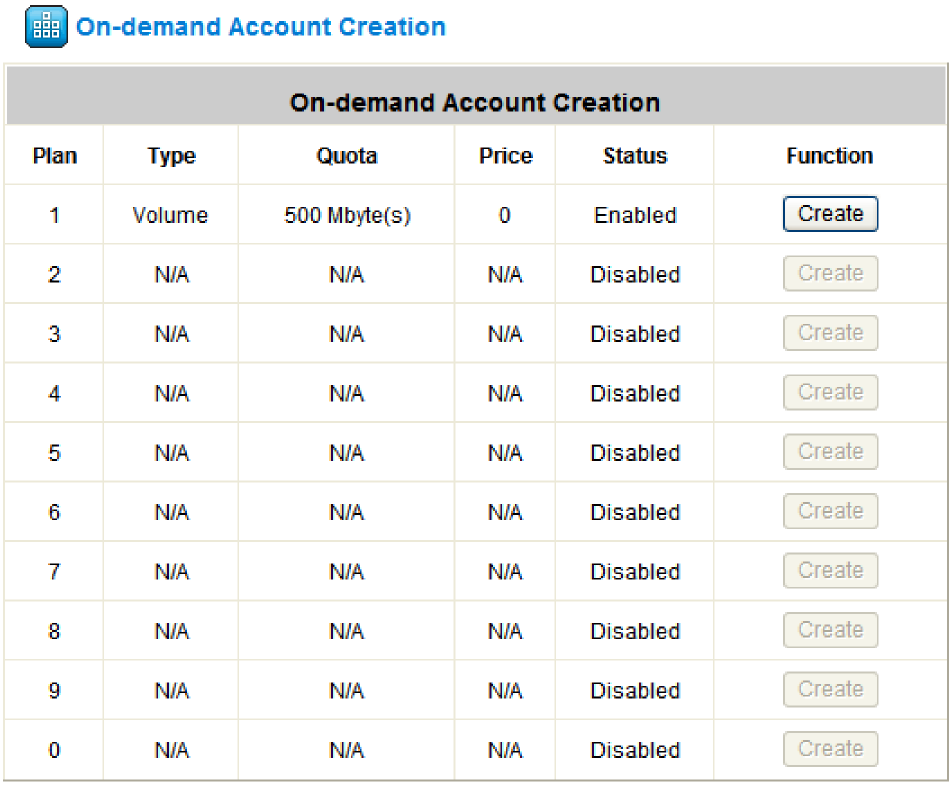
STEP 11 . Back to **Authentication Server Configuration** page, click **Create** button of **On-demand Account Creation** to create a random account for guest user.



Authentication Server Configuration

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 List	View

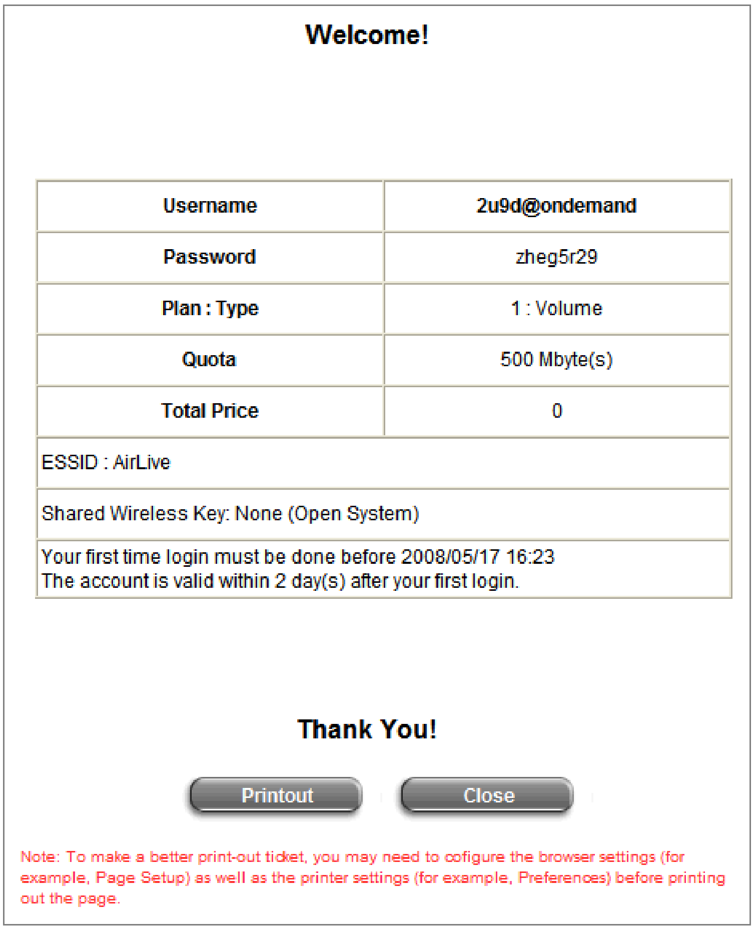
STEP 12 . Select the Plan Type and press Create button to create a new account.



On-demand Account Creation

On-demand Account Creation					
Plan	Type	Quota	Price	Status	Function
1	Volume	500 Mbyte(s)	0	Enabled	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

STEP 13 . When guest user receives the ticket, he can input the username and password to pass the authentication and access Internet, till he spends out the quota. For more detail information to setup local user please check ***Chapter 7.2.1.6 Authentication Method – ONDEMAND***.



Welcome!

Username	2u9d@ondemand
Password	zheg5r29
Plan : Type	1 : Volume
Quota	500 Mbyte(s)
Total Price	0

ESSID : AirLive

Shared Wireless Key: None (Open System)

Your first time login must be done before 2008/05/17 16:23
The account is valid within 2 day(s) after your first login.

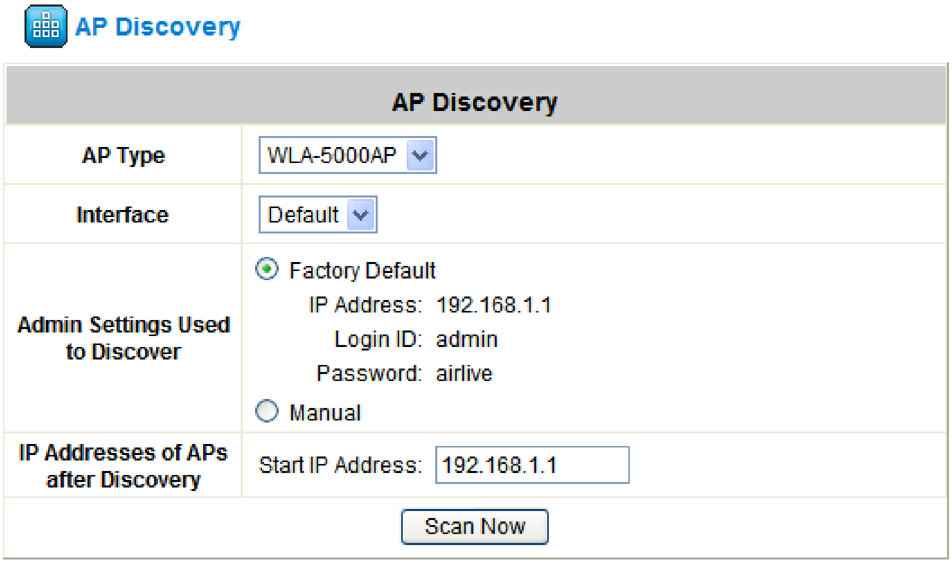
Thank You!

Note: To make a better print-out ticket, you may need to cofigure the browser settings (for example, Page Setup) as well as the printer settings (for example, Preferences) before printing out the page.

6.6 Setup AP Management

STEP 6 . **AP Management → AP Discovery:** Connect WLA-5000AP to MW-2000S Public Port, and use **AP Management** function to auto-detect and auto-configure WLA-5000AP. For more information please check ***Chapter 7.3.2 AP Discovery***.

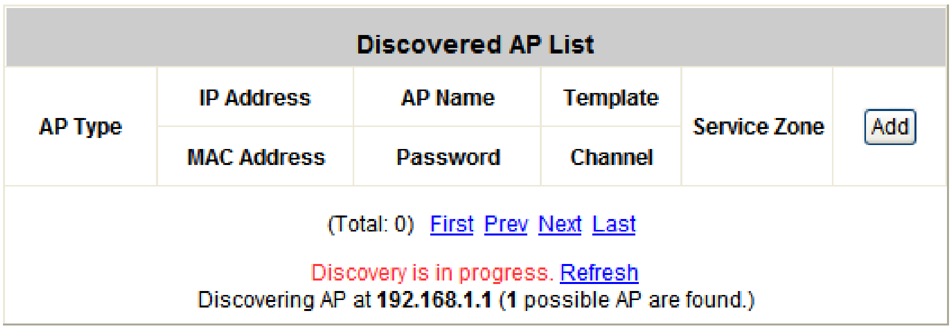
STEP 7 . Select "WLA-5000AP" and press **Scan Now** to detect AP.



AP Discovery

AP Discovery	
AP Type	WLA-5000AP
Interface	Default
Admin Settings Used to Discover	● Factory Default IP Address: 192.168.1.1 Login ID: admin Password: airlive ○ Manual
IP Addresses of APs after Discovery	Start IP Address: 192.168.1.1
	Scan Now

STEP 8 . When MW-2000S detects the AP, system will create the connection automatically, so user can define AP's setting via MW-2000S.

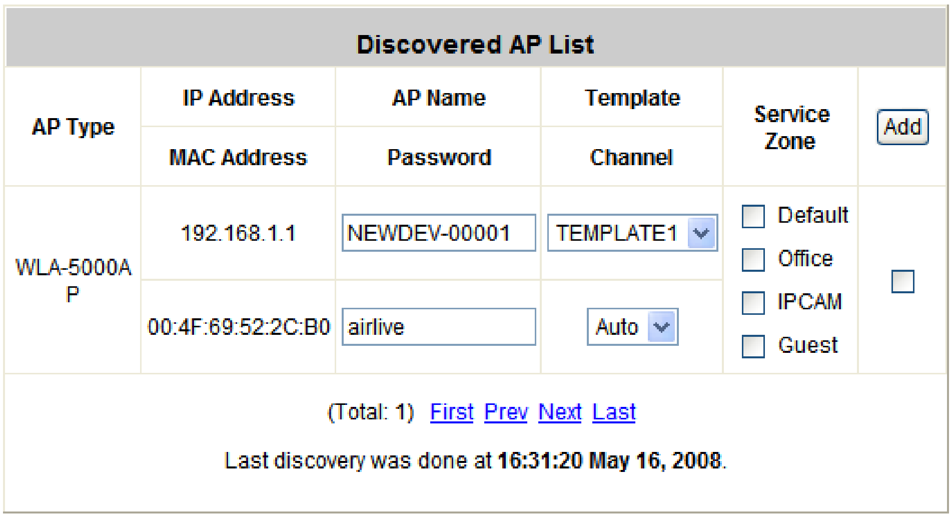


Discovered AP List

AP Type	IP Address MAC Address	AP Name Password	Template Channel	Service Zone	Add

(Total: 0) First Prev Next Last

Discovery is in progress. Refresh
Discovering AP at **192.168.1.1** (**1** possible AP are found.)



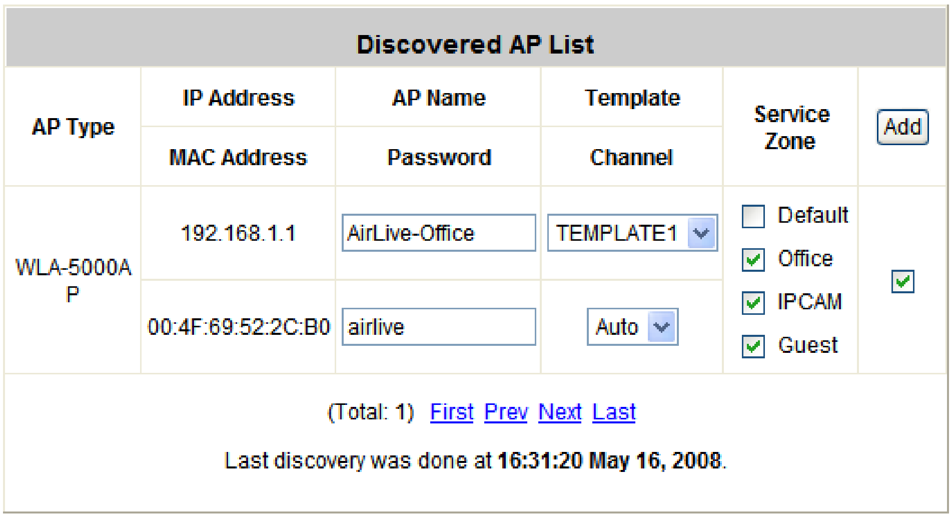
Discovered AP List

AP Type	IP Address MAC Address	AP Name Password	Template Channel	Service Zone	Add
WLA-5000AP	192.168.1.1 00:4F:69:52:2C:B0	NEWDEV-00001 airlive	TEMPLATE1 Auto	□ Default □ Office □ IPCAM □ Guest	□

(Total: 1) First Prev Next Last

Last discovery was done at **16:31:20 May 16, 2008**.

STEP 9 . Change **AP Name**, select **Office**, **IPCAM**, and **Guest** Service Zone, and click **Add** to modify WLA-5000AP.



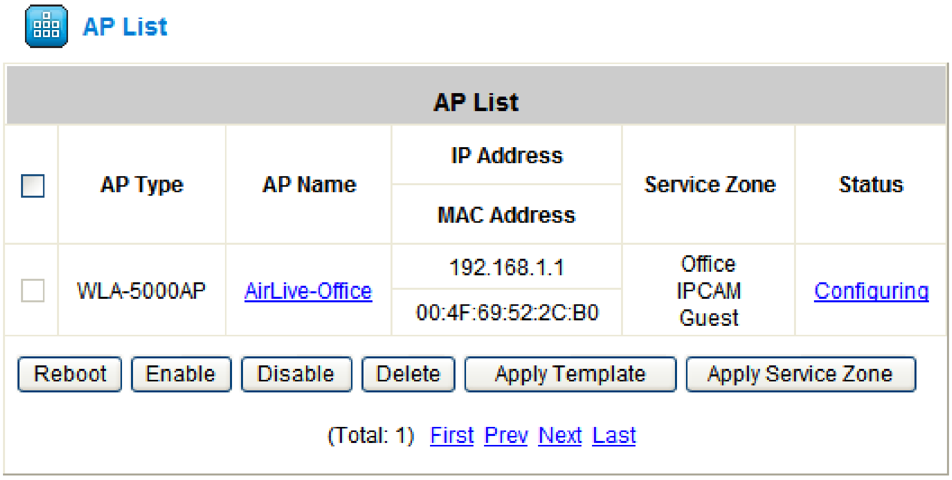
Discovered AP List

AP Type	IP Address MAC Address	AP Name Password	Template Channel	Service Zone	Add
WLA-5000AP	192.168.1.1 00:4F:69:52:2C:B0	AirLive-Office airlive	TEMPLATE1 Auto	□ Default ☑ Office ☑ IPCAM ☑ Guest	☑

(Total: 1) First Prev Next Last

Last discovery was done at **16:31:20 May 16, 2008**.

STEP 10 . Page will turn to **AP List** and WLA-5000AP will be configuring with the data we set; when the configuration is done, the table will be listed a new AP device in **AP List**.

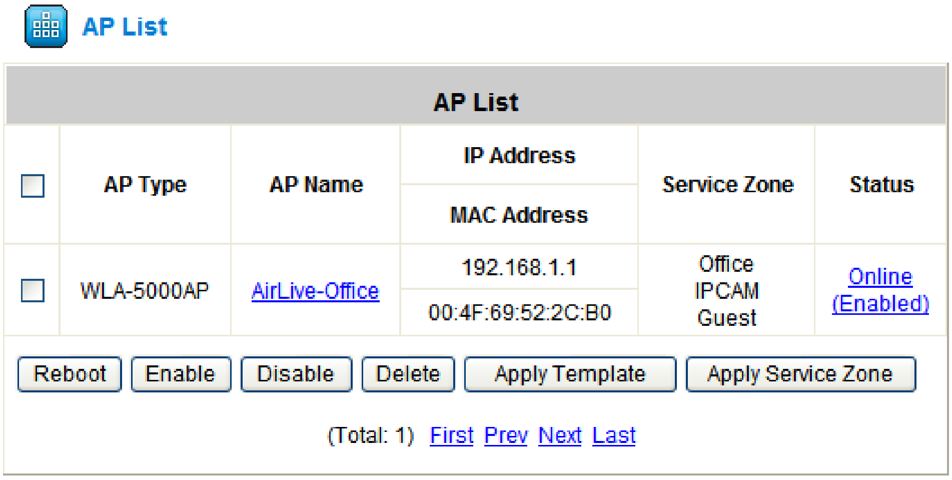


AP List

AP List

□	AP Type	AP Name	IP Address MAC Address	Service Zone	Status
□	WLA-5000AP	AirLive-Office	192.168.1.1 00:4F:69:52:2C:B0	Office IPCAM Guest	Configuring

(Total: 1) First Prev Next Last



AP List

AP List

□	AP Type	AP Name	IP Address MAC Address	Service Zone	Status
□	WLA-5000AP	AirLive-Office	192.168.1.1 00:4F:69:52:2C:B0	Office IPCAM Guest	Online (Enabled)

(Total: 1) First Prev Next Last

6.7 Setup Policy

Currently, the default setting of MW-2000S allows passing through every Service Zones. So, if system does not block all connection at first, it might need to create more complicate Policy setting in order to reach the request.

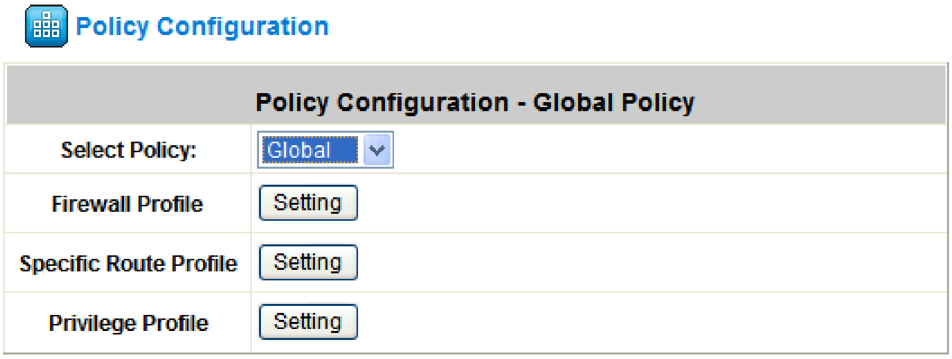
Once the default setting is changing to block all connection, the policy can be more easily that you just need to open the necessary connection.

User can follow the steps to configure the Policy rules for Multi-Service Providers:

1. Configure **Global Policy** to block all connection
2. Configure **Policy 1** for **Office** Service Zone to allow office user accessing Internet, and the connection between MIS (192.168.11.11) and IPCAM (192.168.12.12).
3. Configure **Policy 2** for **IPCAM** Service Zone to allow the connection between IPCAM (192.168.12.12) and MIS (192.168.11.11).
4. Configure **Policy 3** for **Guest** Service Zone to allow user accessing Internet.

Attention: *Next version firmware will be modified to block all connection by default, so the first step can be ignored in future.*

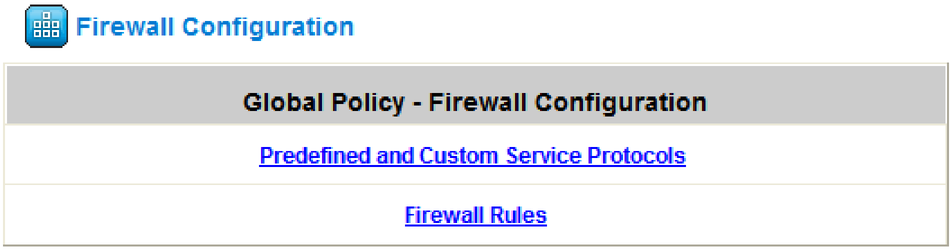
STEP 1 . Click **User Authentication → Policy Configuration** and select **Global**"; click **Setting** button of **Firewall Profile** to enter the setting.



Policy Configuration

Policy Configuration - Global Policy	
Select Policy:	Global
Firewall Profile	Setting
Specific Route Profile	Setting
Privilege Profile	Setting

STEP 2 . Click **Firewall Rules** to configure the firewall setting.



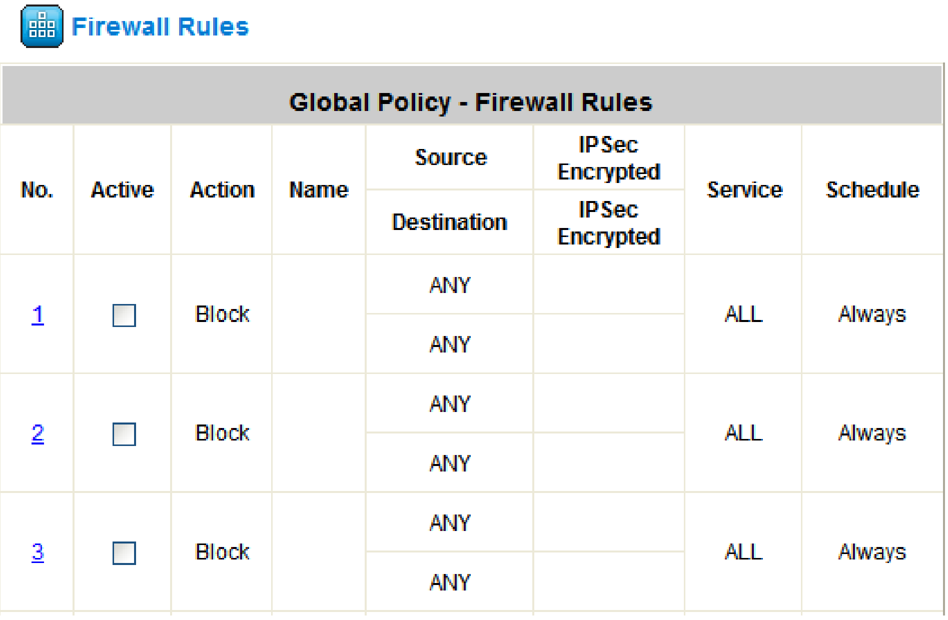
Firewall Configuration

Global Policy - Firewall Configuration

Predefined and Custom Service Protocols

Firewall Rules

STEP 3 . Click **No. 1** firewall rule to edit more firewall setting.

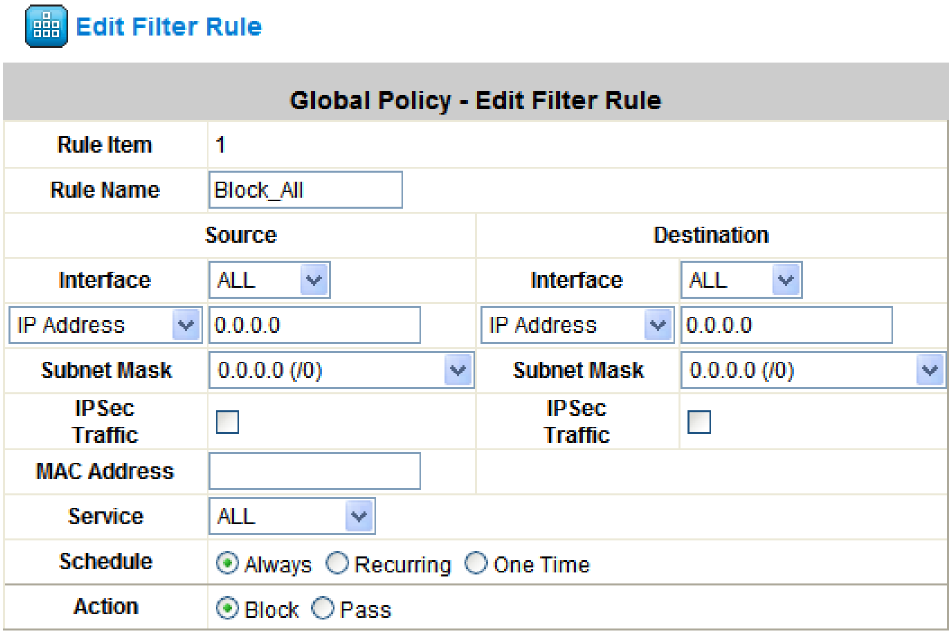


Firewall Rules

Global Policy - Firewall Rules

No.	Active	Action	Name	Source Destination	IPSec Encrypted IPSec Encrypted	Service	Schedule
1	□	Block		ANY ANY		ALL	Always
2	□	Block		ANY ANY		ALL	Always
3	□	Block		ANY ANY		ALL	Always

STEP 4 . Input the **Rule name**, select **Source** and **Destination** Interface as **ALL**, and enable the **Action** as **Block**.

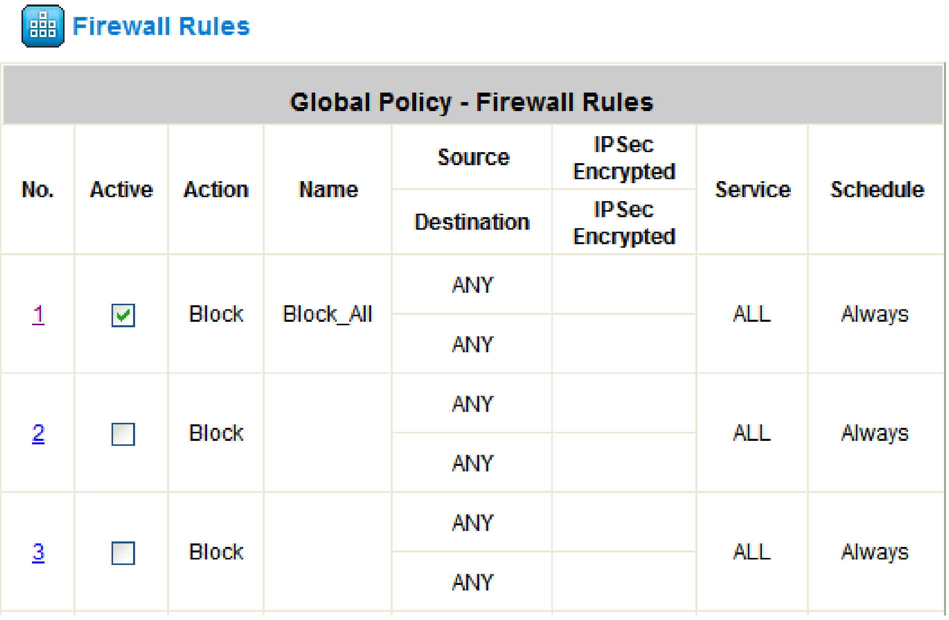


Edit Filter Rule

Global Policy - Edit Filter Rule

Rule Item	1		
Rule Name	Block_All		
	Source		Destination
Interface	ALL	Interface	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)
IPSec Traffic	□	IPSec Traffic	□
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	● Block ○ Pass		

STEP 5 . Enable the Active of first rule, and click **Apply** to save the setting.



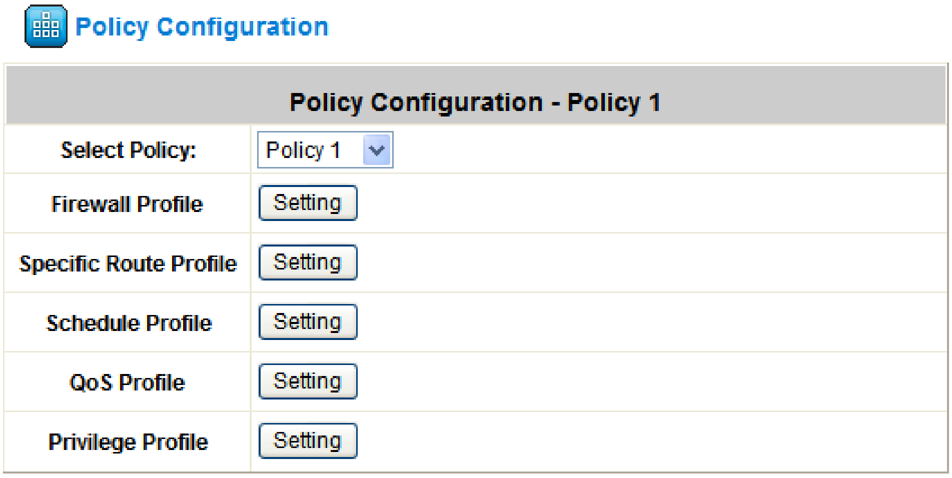
Firewall Rules

Global Policy - Firewall Rules

No.	Active	Action	Name	Source Destination	IPSec Encrypted IPSec Encrypted	Service	Schedule
1	☑	Block	Block_All	ANY ANY		ALL	Always
2	□	Block		ANY ANY		ALL	Always
3	□	Block		ANY ANY		ALL	Always

STEP 6 . When **Global Policy** setting is done, then to configure **Policy 1, 2** and **3**.

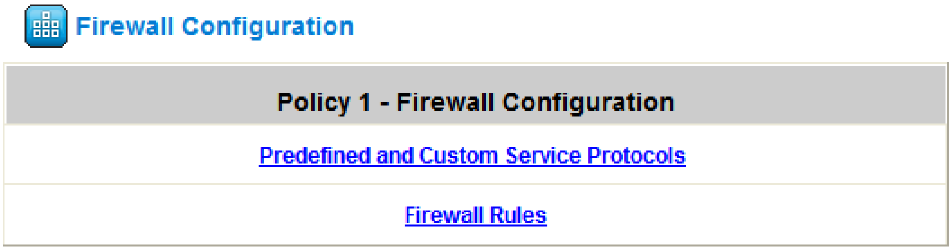
STEP 7 . Configure **Policy 1** to enable the connection from **Office** Service Zone to Internet, the connection between **MIS** (192.168.11.11) and **IPCAM** (192.168.12.12), and define the **Traffic Class** as **Best Effort**. Click **Setting** button of **Firewall Profile** to enter the setting.



Policy Configuration

Policy Configuration - Policy 1	
Select Policy:	Policy 1
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

STEP 8 . Click **Firewall Rules** to configure the firewall setting.



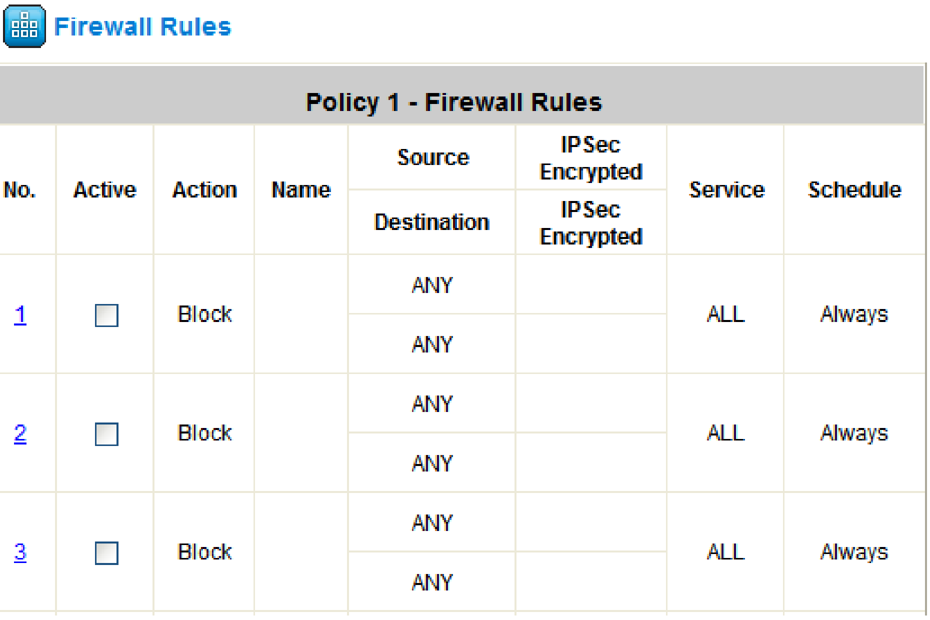
Firewall Configuration

Policy 1 - Firewall Configuration

Predefined and Custom Service Protocols

Firewall Rules

STEP 9 . Click **No. 1** firewall rule to edit more firewall setting.

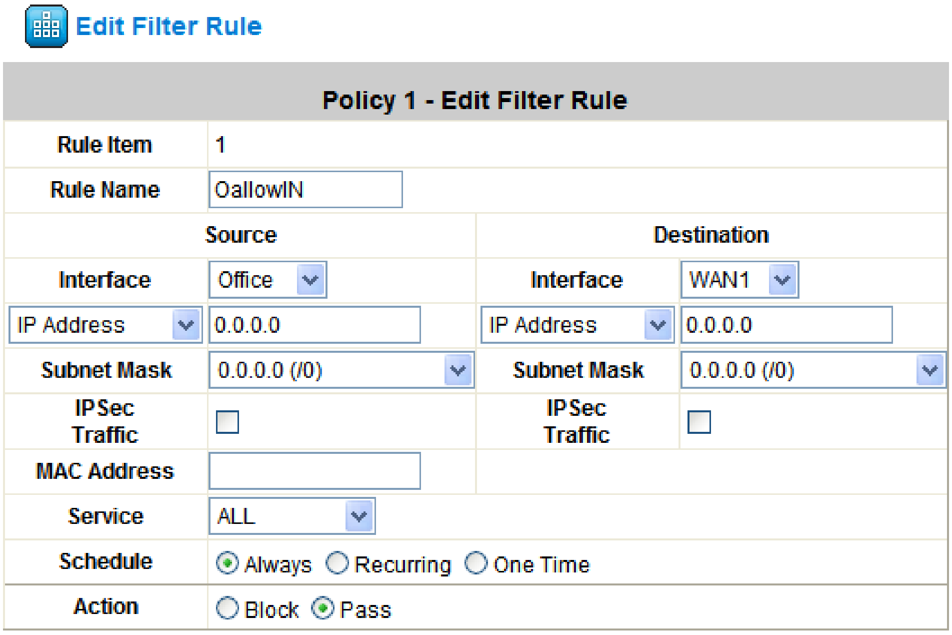


Firewall Rules

Policy 1 - Firewall Rules

No.	Active	Action	Name	Source / Destination	IPSec Encrypted	Service	Schedule
1	□	Block		ANY		ALL	Always
				ANY			
2	□	Block		ANY		ALL	Always
				ANY			
3	□	Block		ANY		ALL	Always
				ANY			

STEP 10 . Enter the first rule and input the **Rule name**, select **Source** Interface as **Office** and **Destination** Interface as **WAN1**; then enable the **Action** to **Pass**.

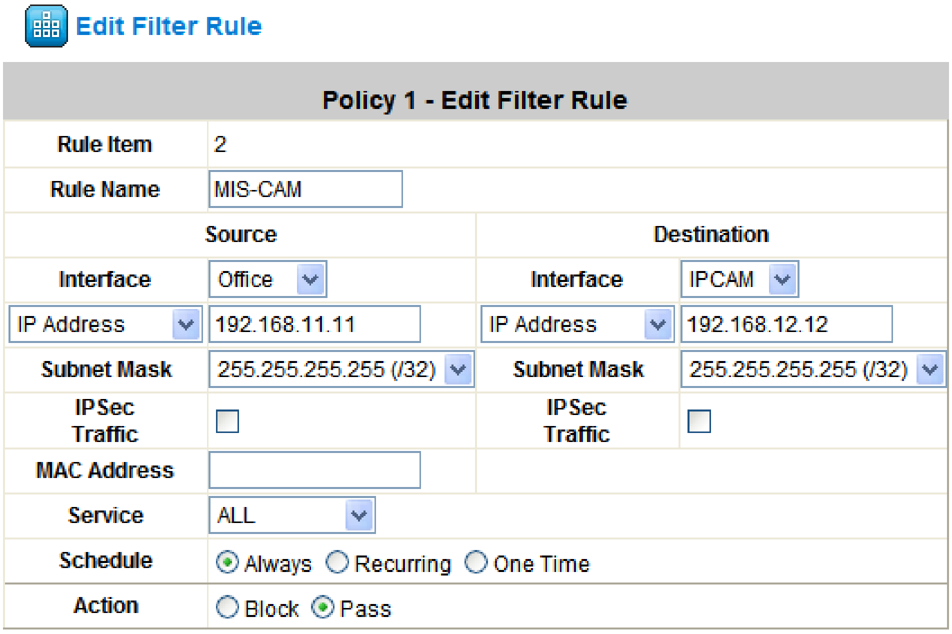


Edit Filter Rule

Policy 1 - Edit Filter Rule

Rule Item	1		
Rule Name	OallowIN		
	Source		Destination
Interface	Office	Interface	WAN1
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)
IPSec Traffic	□	IPSec Traffic	□
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	○ Block ● Pass		

STEP 11 . Enter the second rule and input the **Rule name**, select **Source** Interface as **Office** and specify the IP address with 192.168.11.11; select **Destination** Interface as **IPCAM** and specify the IP address with 192.168.12.12; then enable the **Action** to **Pass**.

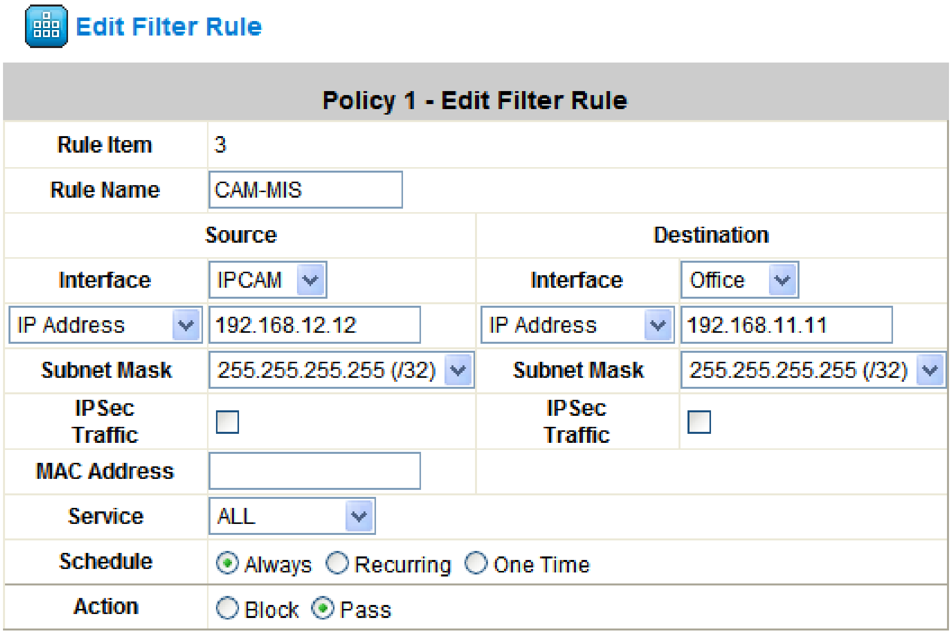


Edit Filter Rule

Policy 1 - Edit Filter Rule

Rule Item	2		
Rule Name	MIS-CAM		
	Source		Destination
Interface	Office	Interface	IPCAM
IP Address	192.168.11.11	IP Address	192.168.12.12
Subnet Mask	255.255.255.255 (/32)	Subnet Mask	255.255.255.255 (/32)
IPSec Traffic	□	IPSec Traffic	□
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	○ Block ● Pass		

STEP 12 . Enter the third rule and input the **Rule name**, select **Source** Interface as **IPCAM** and specify the IP address with 192.168.12.12; select **Destination** Interface as **Office** and specify the IP address with 192.168.11.11; then enable the **Action** to **Pass**.

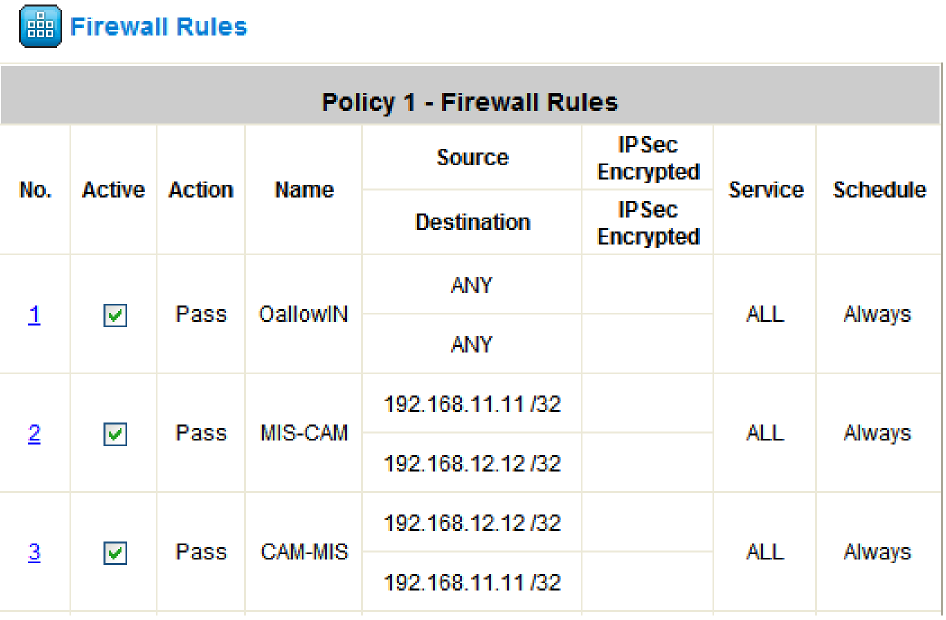


Edit Filter Rule

Policy 1 - Edit Filter Rule

Rule Item	3		
Rule Name	CAM-MIS		
Source		Destination	
Interface	IPCAM	Interface	Office
IP Address	192.168.12.12	IP Address	192.168.11.11
Subnet Mask	255.255.255.255 (/32)	Subnet Mask	255.255.255.255 (/32)
IPSec Traffic	□	IPSec Traffic	□
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	○ Block ● Pass		

STEP 13 . Enable the Active of rules, and click **Apply** to save the setting.

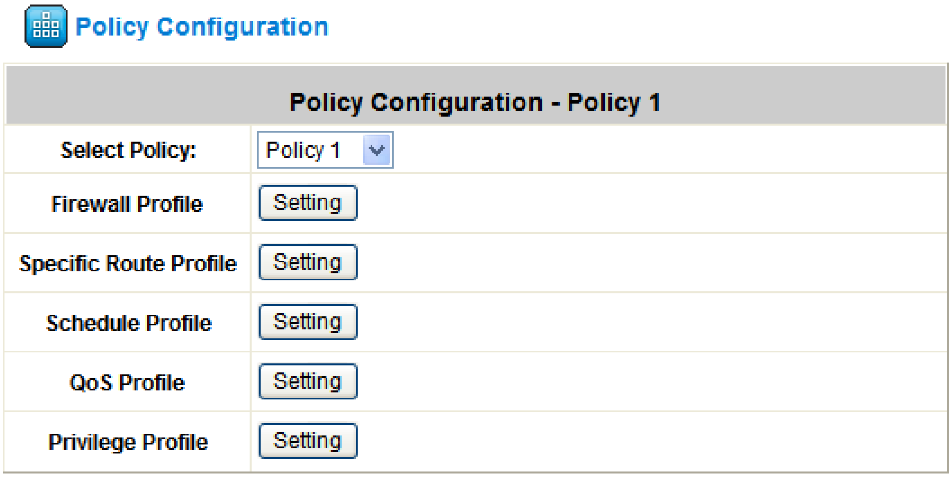


Firewall Rules

Policy 1 - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	☑	Pass	OallowIN	ANY		ALL	Always
				ANY			
2	☑	Pass	MIS-CAM	192.168.11.11 /32		ALL	Always
				192.168.12.12 /32			
3	☑	Pass	CAM-MIS	192.168.12.12 /32		ALL	Always
				192.168.11.11 /32			

STEP 14 . Enter **User Authentication → Policy Configuration**, and press **QoS Profile** button.

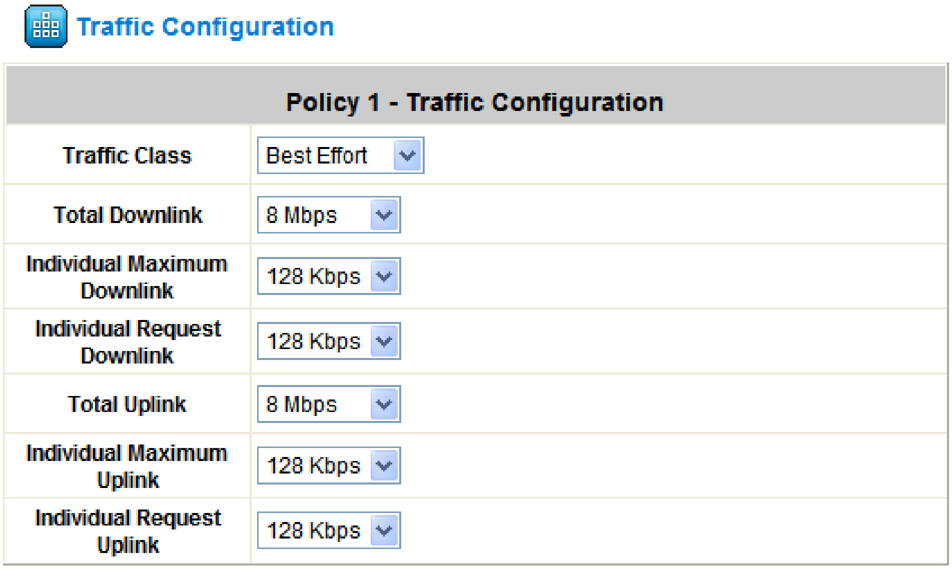


Policy Configuration

Policy Configuration - Policy 1

Select Policy:	Policy 1
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

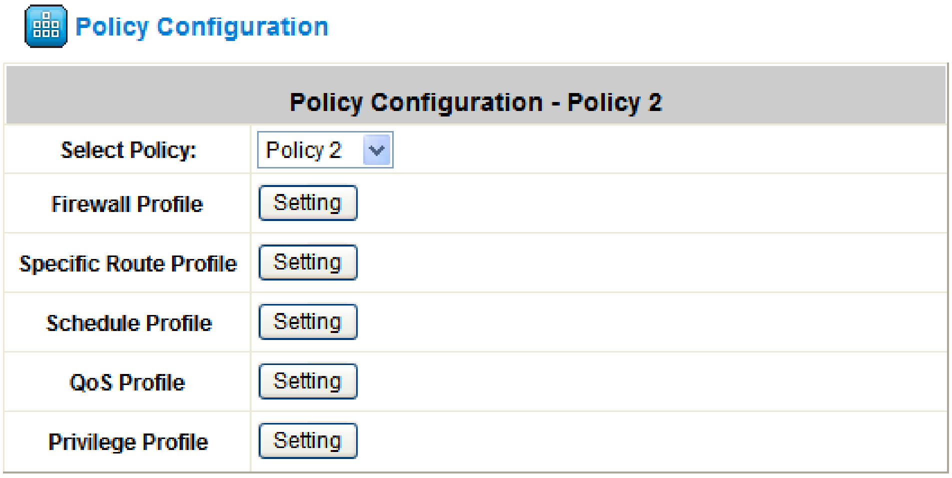
STEP 15 . Select **Best Effort** for **Traffic Class**, and specify the total speed and the limitation for Downlink and Uplink. Click **Apply** to save the setting and finish the configuration of **Policy 1**.



Traffic Configuration

Policy 1 - Traffic Configuration	
Traffic Class	Best Effort
Total Downlink	8 Mbps
Individual Maximum Downlink	128 Kbps
Individual Request Downlink	128 Kbps
Total Uplink	8 Mbps
Individual Maximum Uplink	128 Kbps
Individual Request Uplink	128 Kbps

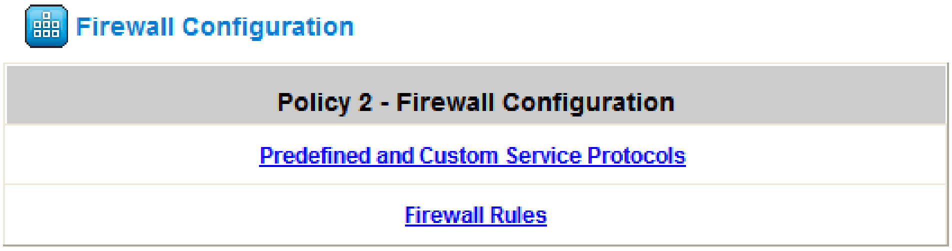
STEP 16 . Configure **Policy 2** to enable the connection between **IPCAM** (192.168.12.12) and **MIS** (192.168.11.11), and define the **Traffic Class** as **Video**. Click **Setting** button of **Firewall Profile** to enter the setting.



Policy Configuration

Policy Configuration - Policy 2	
Select Policy:	Policy 2
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

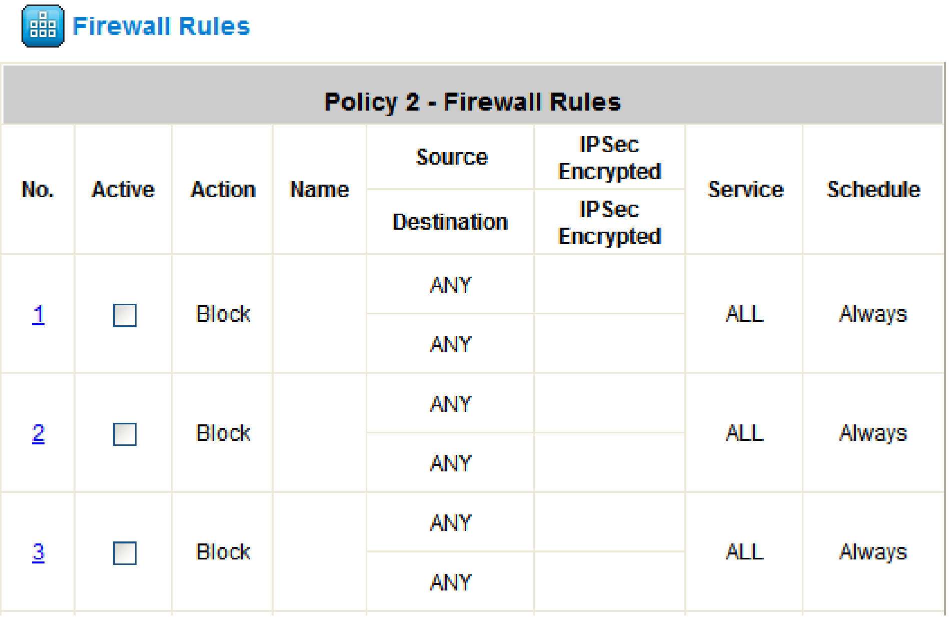
STEP 17 . Click **Firewall Rules** to configure the firewall setting.



Firewall Configuration

Policy 2 - Firewall Configuration
Predefined and Custom Service Protocols
Firewall Rules

STEP 18 . Click **No. 1** firewall rule to edit more firewall setting.

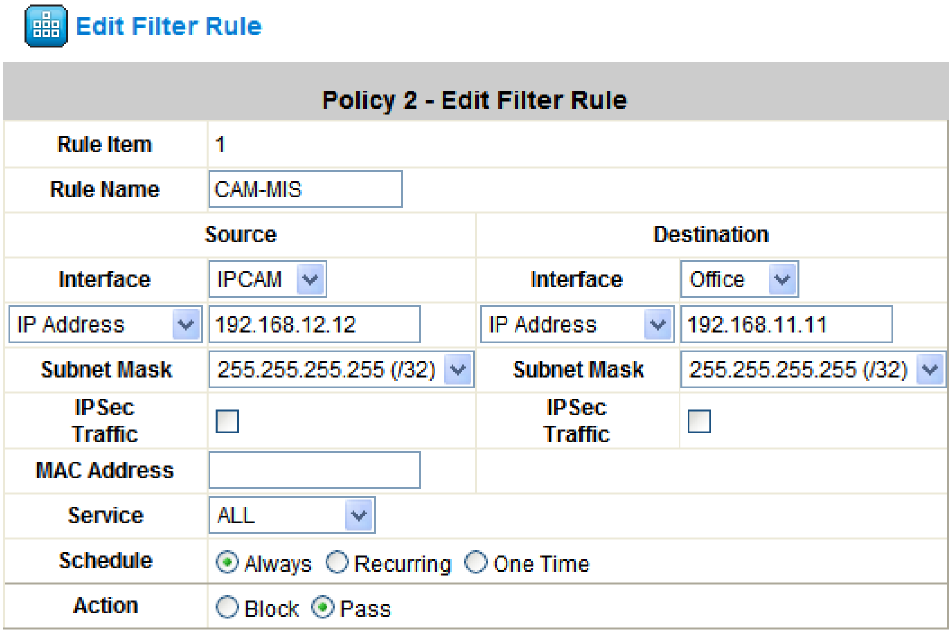


Firewall Rules

Policy 2 - Firewall Rules

No.	Active	Action	Name	Source Destination	IPSec Encrypted IPSec Encrypted	Service	Schedule
1	□	Block		ANY ANY		ALL	Always
2	□	Block		ANY ANY		ALL	Always
3	□	Block		ANY ANY		ALL	Always

STEP 19 . Enter the first rule and input the **Rule name**, select **Source** Interface as **IPCAM** and specify the IP address with 192.168.12.12; select **Destination** Interface as **Office** and specify the IP address with 192.168.11.11; then enable the **Action** to **Pass**.

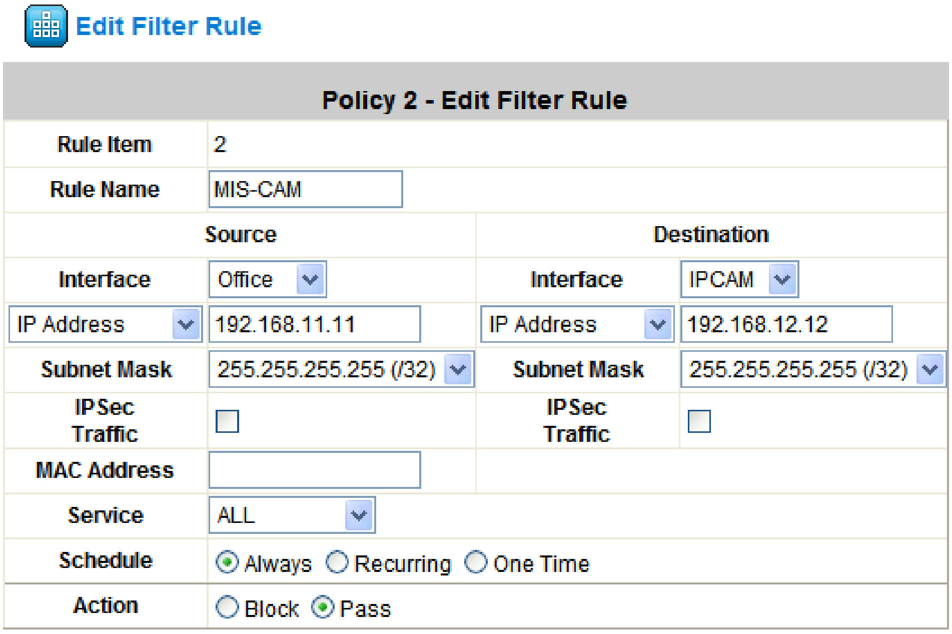


Edit Filter Rule

Policy 2 - Edit Filter Rule

Rule Item	1		
Rule Name	CAM-MIS		
Source		Destination	
Interface	IPCAM	Interface	Office
IP Address	192.168.12.12	IP Address	192.168.11.11
Subnet Mask	255.255.255.255 (/32)	Subnet Mask	255.255.255.255 (/32)
IPSec Traffic	□	IPSec Traffic	□
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	○ Block ● Pass		

STEP 20 . Enter the second rule and input the **Rule name**, select **Source** Interface as **Office** and specify the IP address with 192.168.11.11; select **Destination** Interface as **IPCAM** and specify the IP address with 192.168.12.12; then enable the **Action** to **Pass**.

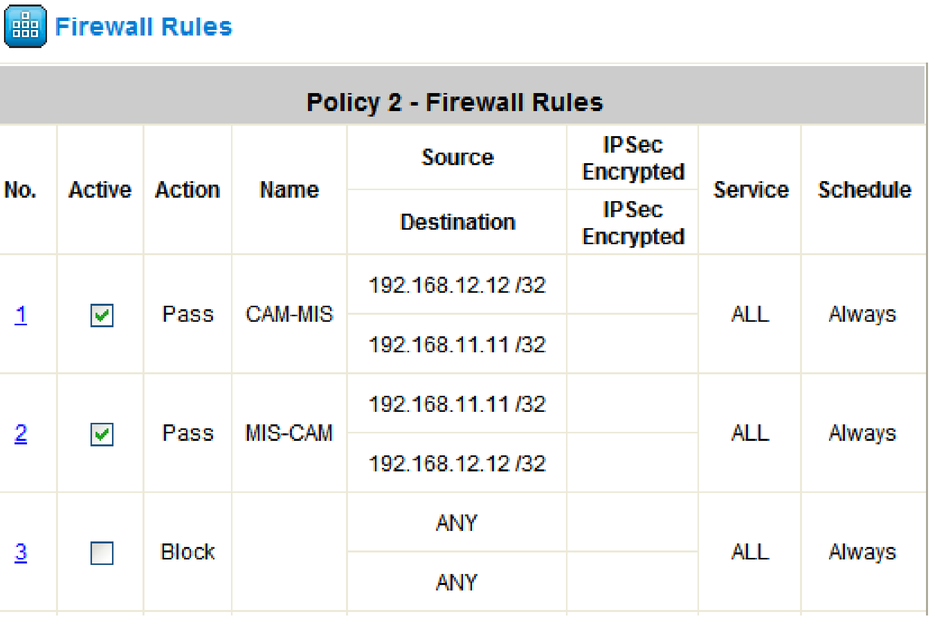


Edit Filter Rule

Policy 2 - Edit Filter Rule

Rule Item	2		
Rule Name	MIS-CAM		
Source		Destination	
Interface	Office	Interface	IPCAM
IP Address	192.168.11.11	IP Address	192.168.12.12
Subnet Mask	255.255.255.255 (/32)	Subnet Mask	255.255.255.255 (/32)
IPSec Traffic	□	IPSec Traffic	□
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	○ Block ● Pass		

STEP 21 . Enable the Active of first rule, and click **Apply** to save the setting.

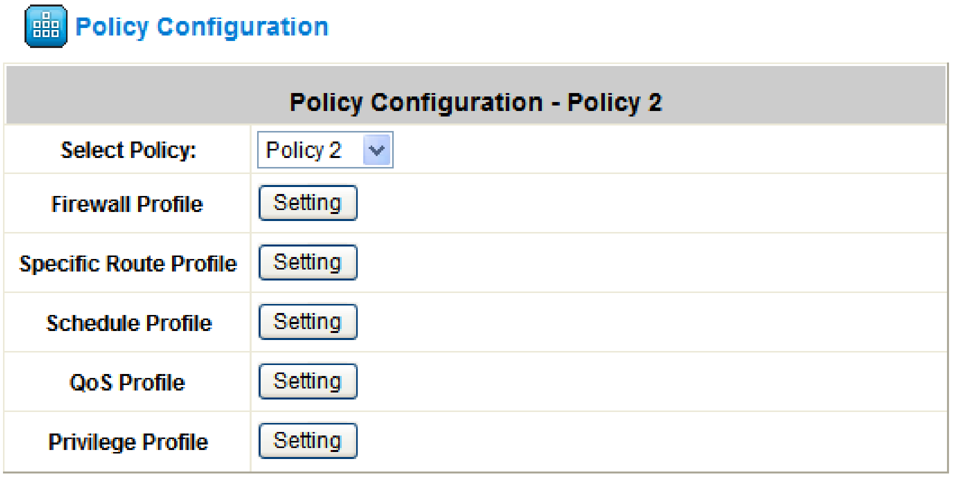


Firewall Rules

Policy 2 - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	☑	Pass	CAM-MIS	192.168.12.12 /32		ALL	Always
				192.168.11.11 /32			
2	☑	Pass	MIS-CAM	192.168.11.11 /32		ALL	Always
				192.168.12.12 /32			
3	□	Block		ANY		ALL	Always
				ANY			

STEP 22 . Enter **User Authentication → Policy Configuration**, and press **QoS Profile** button.

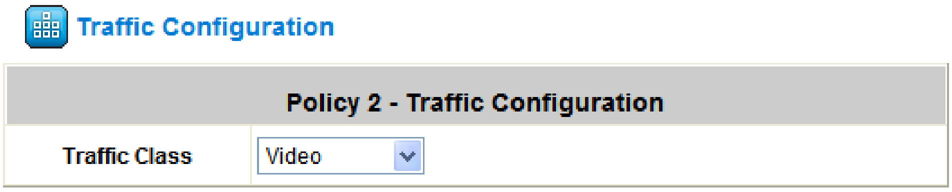


Policy Configuration

Policy Configuration - Policy 2

Select Policy:	Policy 2
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

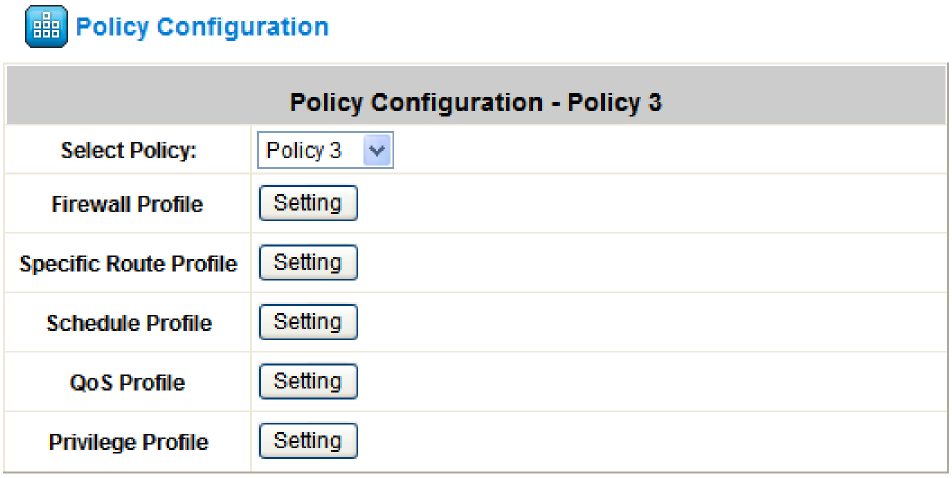
STEP 23 . Select **Video** for **Traffic Class**, and click **Apply** to save the setting and finish the configuration of **Policy 2**.



Traffic Configuration

Policy 2 - Traffic Configuration	
Traffic Class	Video

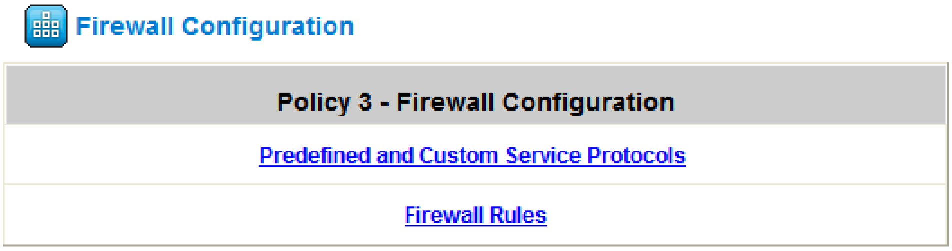
STEP 24 . Configure **Policy 3** to enable the connection from **Guest** Service Zone to Internet, and define the **Traffic Class** as **Background**. Click **Setting** button of **Firewall Profile** to enter the setting.



Policy Configuration

Policy Configuration - Policy 3	
Select Policy:	Policy 3
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

STEP 25 . Click **Firewall Rules** to configure the firewall setting.



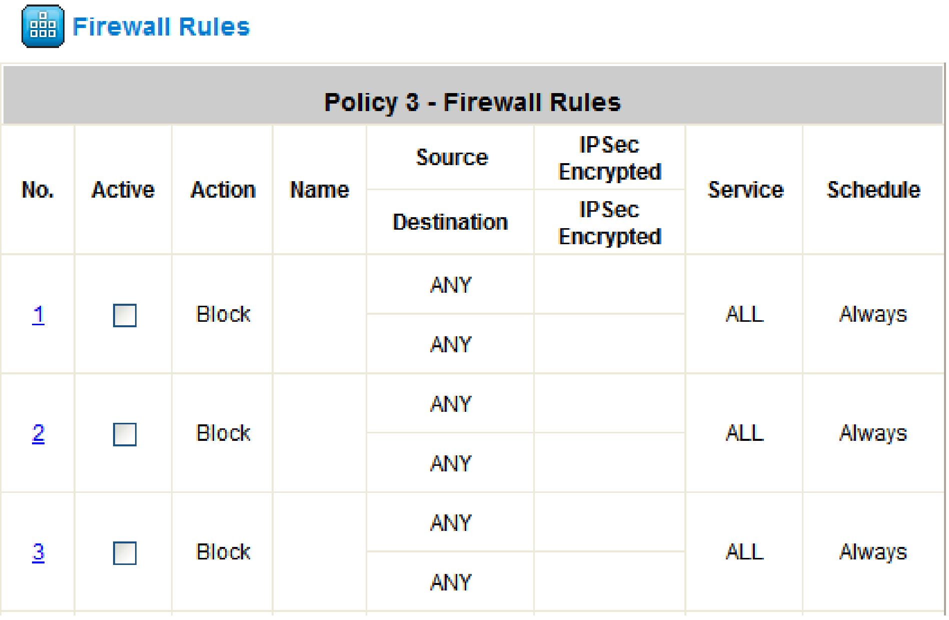
Firewall Configuration

Policy 3 - Firewall Configuration

Predefined and Custom Service Protocols

Firewall Rules

STEP 26 . Click **No. 1** firewall rule to edit more firewall setting.

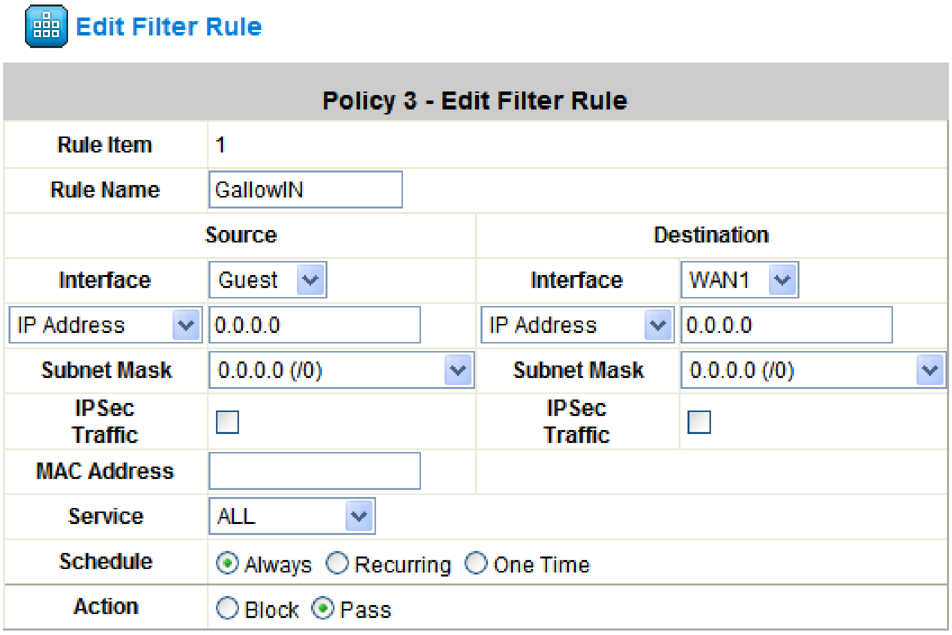


Firewall Rules

Policy 3 - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	□	Block		ANY		ALL	Always
				ANY			
2	□	Block		ANY		ALL	Always
				ANY			
3	□	Block		ANY		ALL	Always
				ANY			

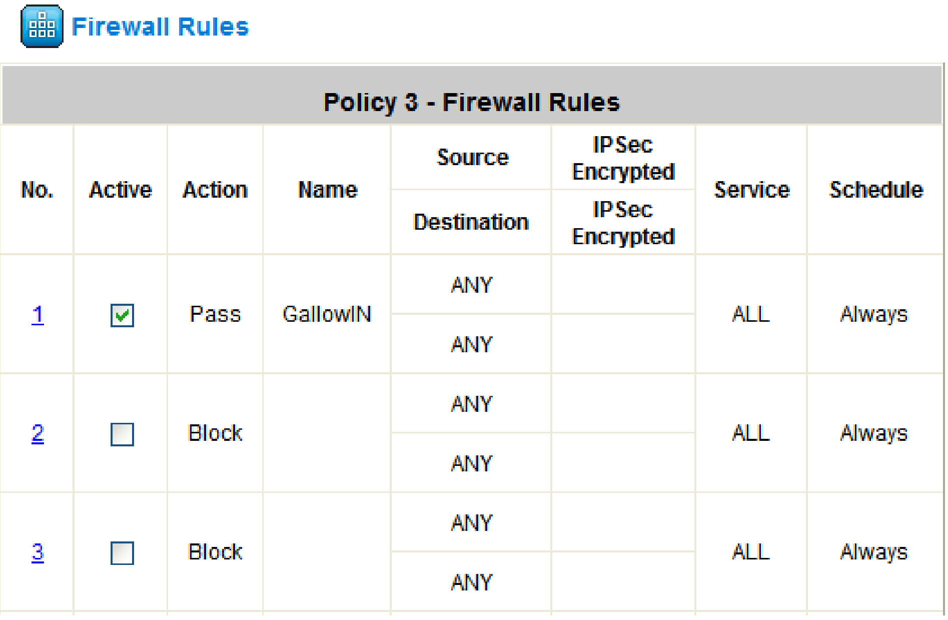
STEP 27 . Input the **Rule name**, select **Source** Interface as **Guest** and **Destination** Interface as **WAN1**, and then enable the **Action** to **Pass**.



Edit Filter Rule

Policy 3 - Edit Filter Rule			
Rule Item	1		
Rule Name	GallowIN		
	Source		Destination
Interface	Guest	Interface	WAN1
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)
IPSec Traffic	☐	IPSec Traffic	☐
MAC Address			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	○ Block ● Pass		

STEP 28 . Enable the Active of first rule, and click **Apply** to save the setting.

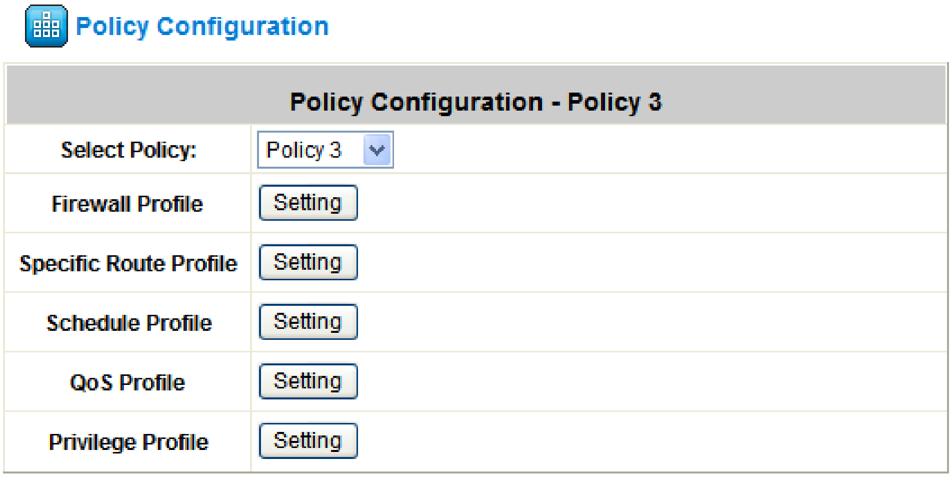


Firewall Rules

Policy 3 - Firewall Rules

No.	Active	Action	Name	Source Destination	IPSec Encrypted IPSec Encrypted	Service	Schedule
1	☑	Pass	GallowIN	ANY ANY		ALL	Always
2	☐	Block		ANY ANY		ALL	Always
3	☐	Block		ANY ANY		ALL	Always

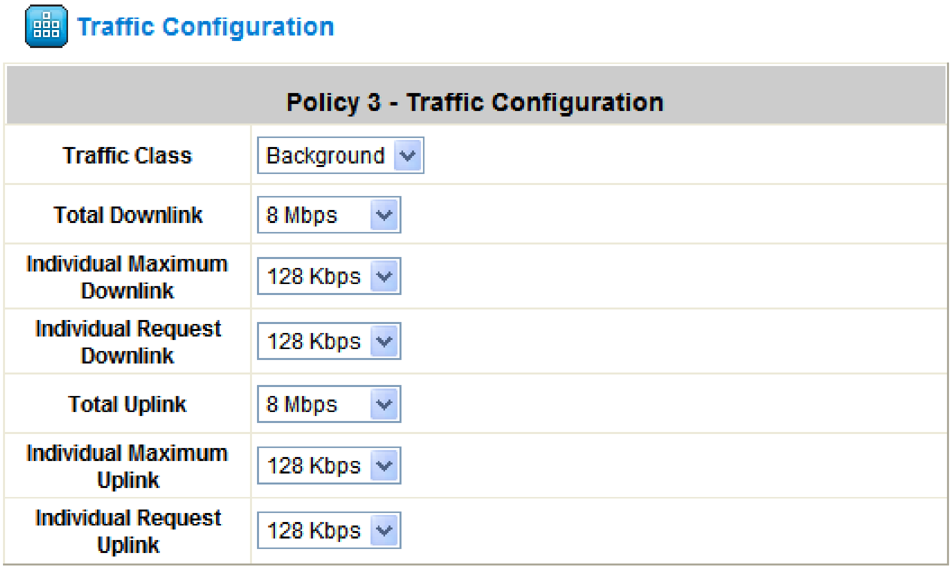
STEP 29 . Enter **User Authentication → Policy Configuration**, and press **QoS Profile** button.



Policy Configuration

Policy Configuration - Policy 3	
Select Policy:	Policy 3
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

STEP 30 . Select **Background** for **Traffic Class**, and specify the total speed and the limitation for Downlink and Uplink. Click **Apply** to save the setting and finish the configuration of **Policy 3**.



Traffic Configuration

Policy 3 - Traffic Configuration

Traffic Class	Background
Total Downlink	8 Mbps
Individual Maximum Downlink	128 Kbps
Individual Request Downlink	128 Kbps
Total Uplink	8 Mbps
Individual Maximum Uplink	128 Kbps
Individual Request Uplink	128 Kbps

STEP 31 . Multi-Service Providers setting is complete.

Chapter 7. Web Interface Configuration

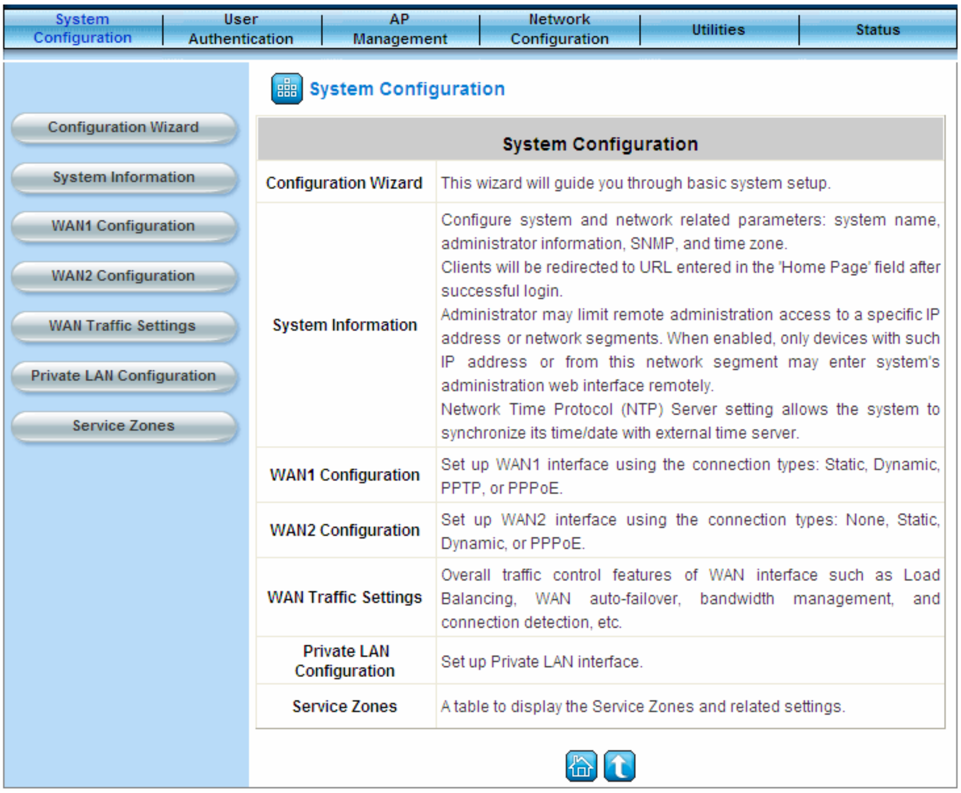
This chapter will guide you through further detailed settings. The following table is the UI and functions of the MW-2000S.

OPTION	System Configuration	User Authentication	AP Management	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	AP List	Network Address Translation	Change Password	System Status
	System Information	Black List Configuration	AP Discovery	Privilege List	Backup/Restore Settings	Interface Status
	WAN1 Configuration	Policy Configuration	Manual Configuration	Monitor IP List	Firmware Upgrade	Routing Table
	WAN2 Configuration	Additional Configuration	Template Settings	Walled Garden List	Restart	Current Users
	WAN Traffic Settings		Firmware Management	Proxy Server Properties	Network Utilities	Traffic History
	Private LAN Configuration		AP Upgrade	Dynamic DNS		Notification Configuration
	Service Zones			IP Mobility		
				VPN Configuration		

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

7.1 System Configuration

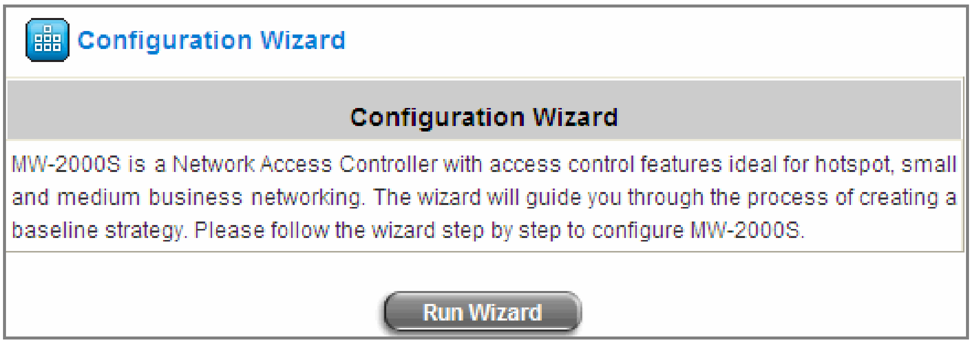
This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN1 Configuration**, **WAN2 Configuration**, **WAN Traffic Settings**, **Private LAN Configuration** and **Service Zone**.



System Configuration	
Configuration Wizard	This wizard will guide you through basic system setup.
System Information	Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be redirected to URL entered in the 'Home Page' field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely. Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
WAN1 Configuration	Set up WAN1 interface using the connection types: Static, Dynamic, PPTP, or PPPoE.
WAN2 Configuration	Set up WAN2 interface using the connection types: None, Static, Dynamic, or PPPoE.
WAN Traffic Settings	Overall traffic control features of WAN interface such as Load Balancing, WAN auto-failover, bandwidth management, and connection detection, etc.
Private LAN Configuration	Set up Private LAN interface.
Service Zones	A table to display the Service Zones and related settings.

7.1.1 Configuration Wizard

Please refer to **3.2 Quick Software Configuration** for the detailed description of **Configuration Wizard**.

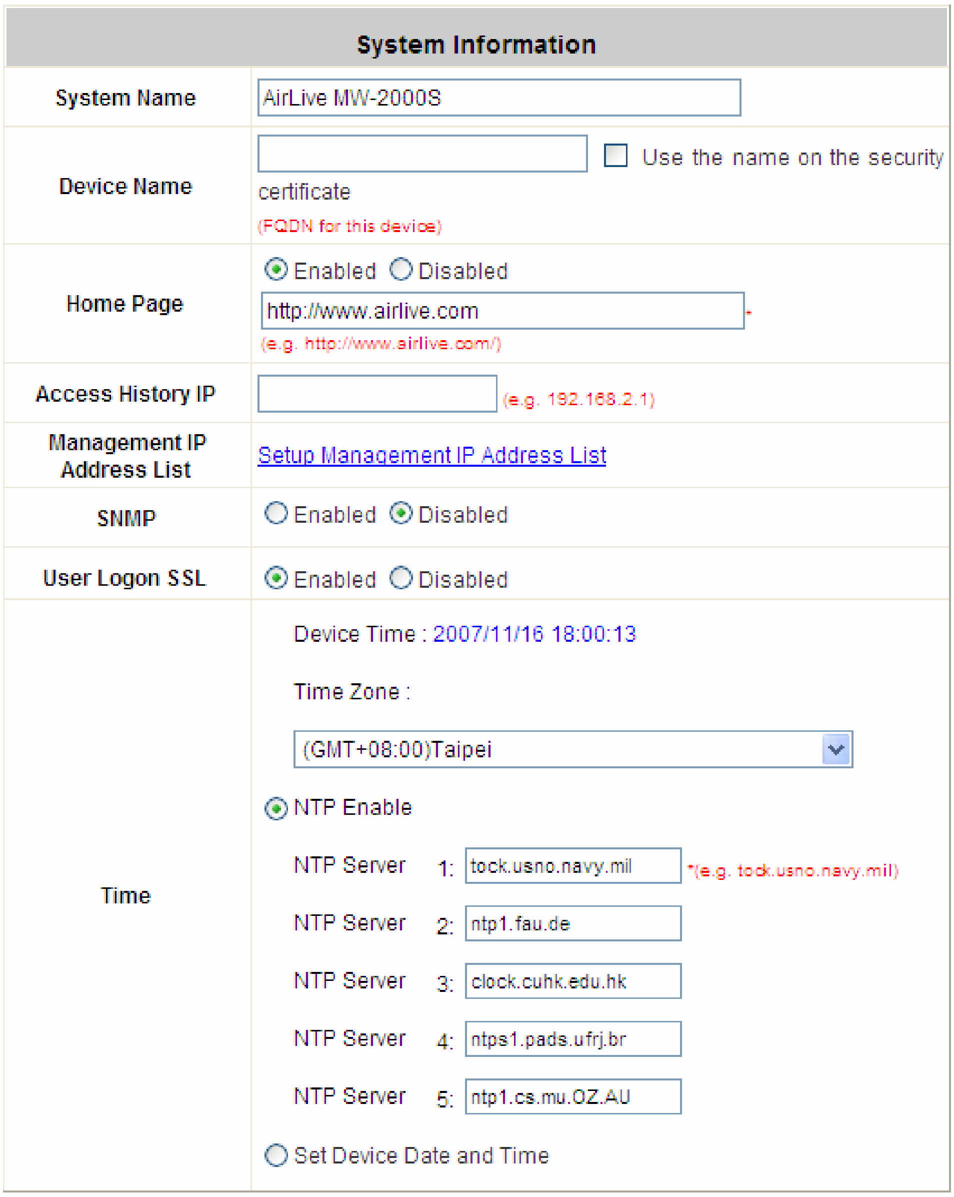


Configuration Wizard

MW-2000S is a Network Access Controller with access control features ideal for hotspot, small and medium business networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure MW-2000S.

7.1.2 System Information

Most of the major system information about MW-2000S can be set here. Please refer to the following description for each field:



System Information

System Name	AirLive MW-2000S
Device Name	□ Use the name on the security certificate (FQDN for this device)
Home Page	● Enabled ○ Disabled http://www.airlive.com * (e.g. http://www.airlive.com/)
Access History IP	(e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List
SNMP	○ Enabled ● Disabled
User Logon SSL	● Enabled ○ Disabled
Time	Device Time : 2007/11/16 18:00:13 Time Zone : (GMT+08:00)Taipei ● NTP Enable NTP Server 1: tock.usno.navy.mil *(e.g. tock.usno.navy.mil) NTP Server 2: ntp1.fau.de NTP Server 3: clock.cuhk.edu.hk NTP Server 4: ntps1.pads.ufrj.br NTP Server 5: ntp1.cs.mu.OZ.AU ○ Set Device Date and Time

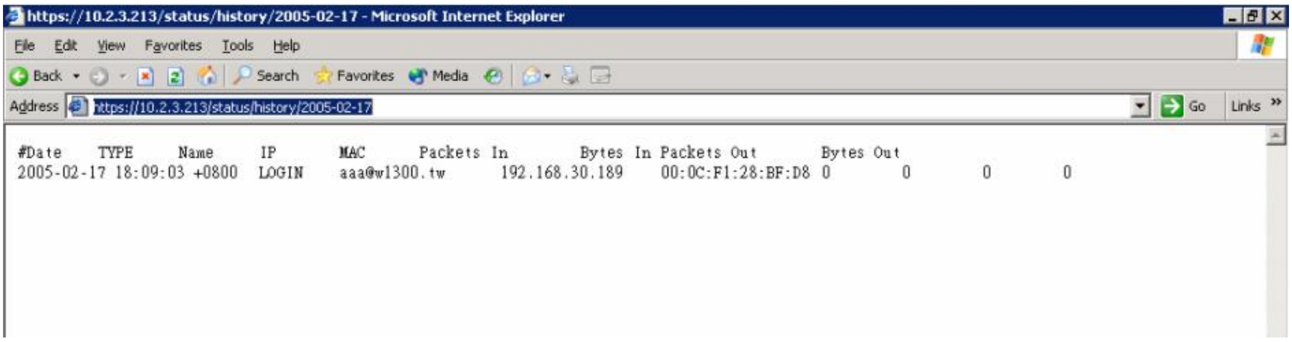
- **System Name:** Set the system's name or use the default name.

- **Device Name:** FQDN (Fully-Qualified Domain Name). This is the domain name of the MW-2000S as seen on client machines connected on LAN ports. A user on client machine can use this domain name to access MW-2000S 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.

- **Home Page:** Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set. Usually, the homepage is set to the company's website, such as http://www.airlive.com. If the home page function is disabled, the user will be directed to the URL she/he tries to visit originally.

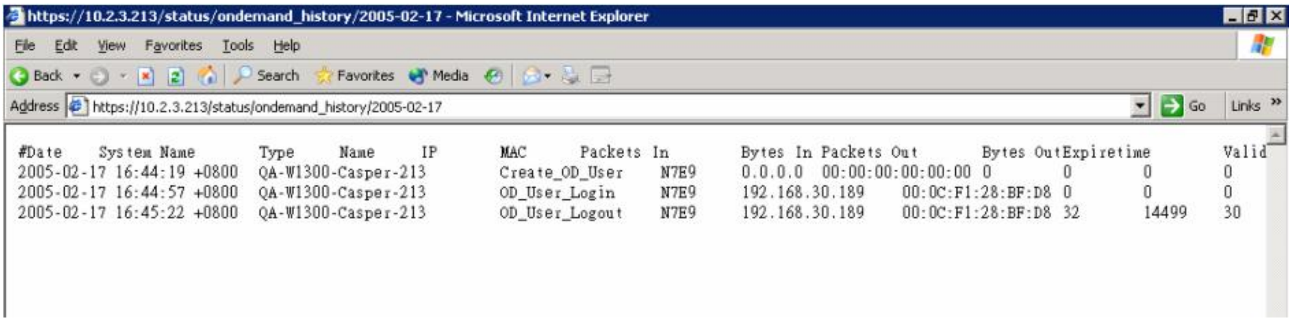
- **Access History IP:** Specify an IP address of the administrator's computer or a billing system to get billing history information of MW-2000S with the predefined URLs as the following:

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


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

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

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


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

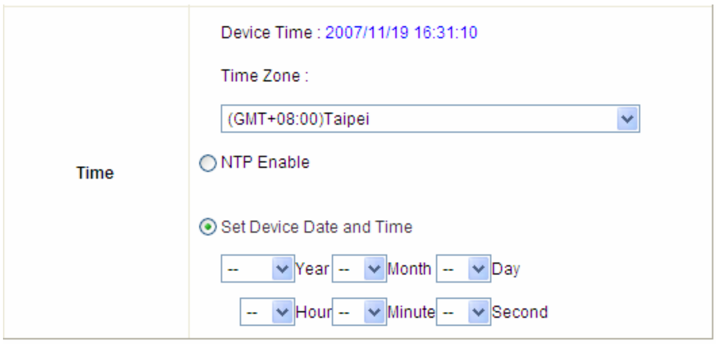
```
#Date      System Name          Type      Name      IP         MAC       Packets  In        Bytes  In Packets  Out        Bytes  OutExpiretime         Valid
2005-02-17 16:44:19 +0800  QA-W1300-Casper-213        Create_OD_User     N7E9      0.0.0.0   00:00:00:00:00:00 0         0         0       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

- **Management IP Address List:** The IP address or subnet of remote management PCs. 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.

- **SNMP:** If the function is enabled, the Manager IP and the community can be assigned to access the management information base (MIB) of the system.

- **User Logon SSL:** Enable to activate https (encryption) or disable to activate http (non encryption) login page.

- **Time:** NTP 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). The system time can also be manually configured by selecting **"Set Device Date and Time"** and enter the date and time for the corresponding fields.



Time

Device Time : 2007/11/19 16:31:10

Time Zone :

(GMT+08:00)Taipei

○ NTP Enable

● Set Device Date and Time

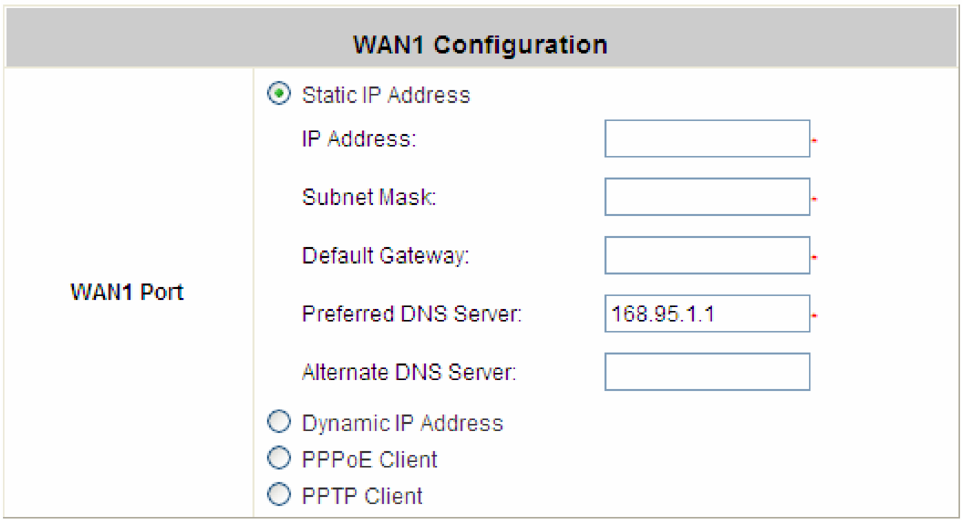
-- Year -- Month -- Day

-- Hour -- Minute -- Second

7.1.3 WAN1 Configuration

There are 4 connection types for the WAN1 Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE** and **PPTP Client**.

- **Static IP Address:** 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 WAN1 port.
  Subnet mask: the subnet mask of the network WAN1 port connects to.
  Default gateway: a gateway of the network WAN1 port connects to.
  Preferred DNS Server: The primary DNS server is used by the system.
  Alternate DNS Server: The substitute DNS server is used by the system. This is an optional field.

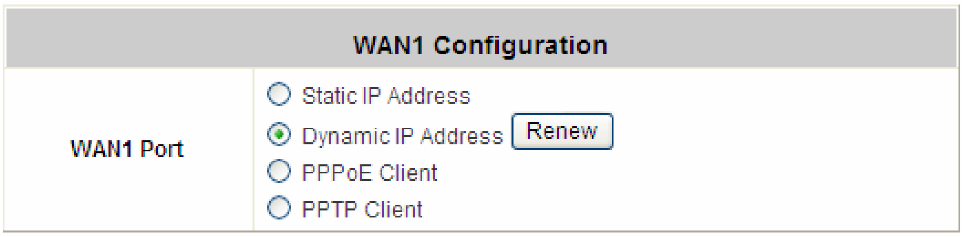


WAN1 Configuration

WAN1 Port

● Static IP Address
IP Address: *
Subnet Mask: *
Default Gateway: *
Preferred DNS Server: 168.95.1.1 *
Alternate DNS Server:
○ Dynamic IP Address
○ PPPoE Client
○ PPTP Client

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

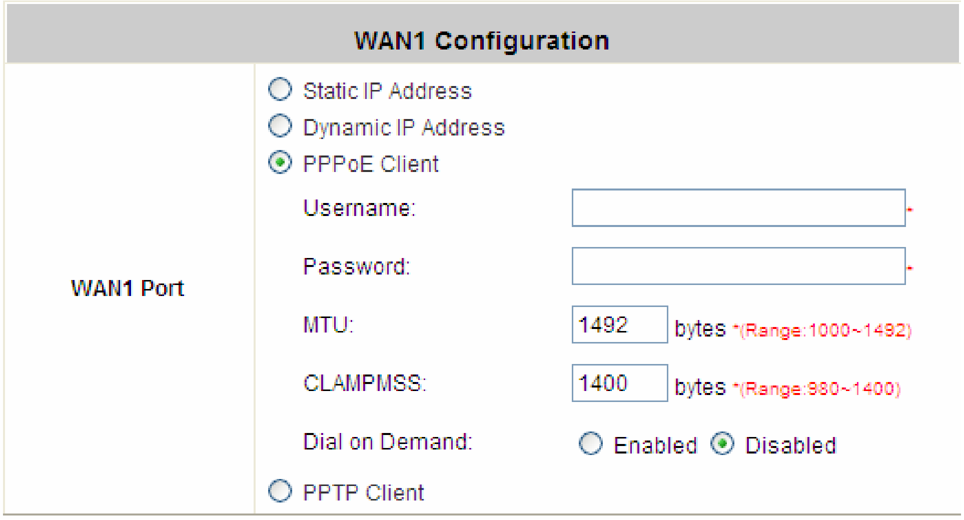


WAN1 Configuration

WAN1 Port

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

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



WAN1 Configuration

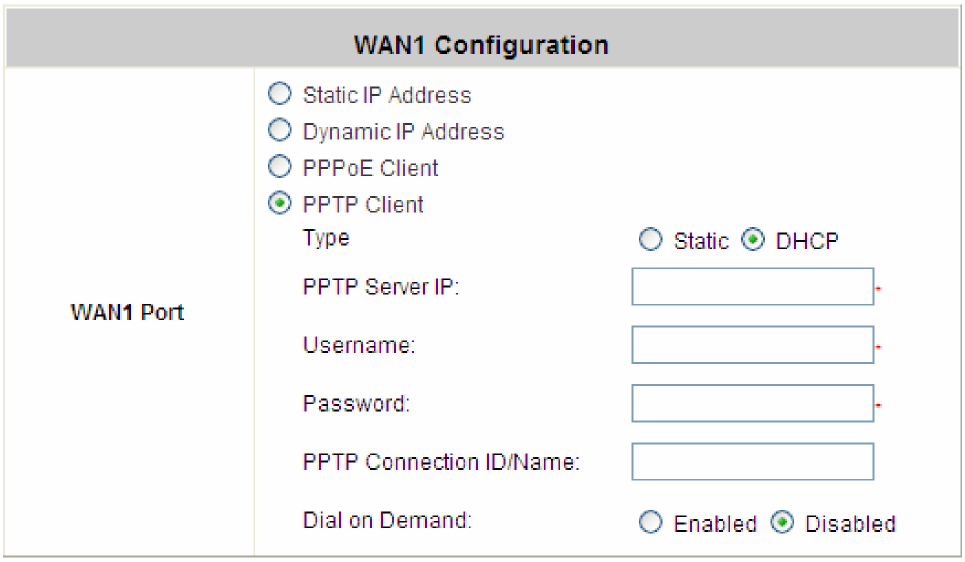
WAN1 Port

○ Static IP Address
○ Dynamic IP Address
● PPPoE Client

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

○ PPTP Client

- **PPTP Client:** Set WAN1 port to connect to external PPTP server to establish PPTP VPN tunnel. Select **STATIC** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red mark are required. Please fill in these fields. There is a **Dial on demand** function under PPTP. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.



WAN1 Configuration

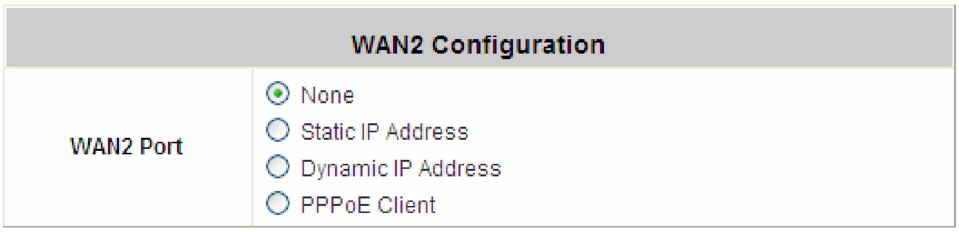
WAN1 Port

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

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

7.1.4 WAN2 Configuration

Select **None** to disable this WAN2 interface, or there are 3 connection types for the WAN2 port: **Static IP Address, Dynamic IP Address** and **PPPoE Client**.

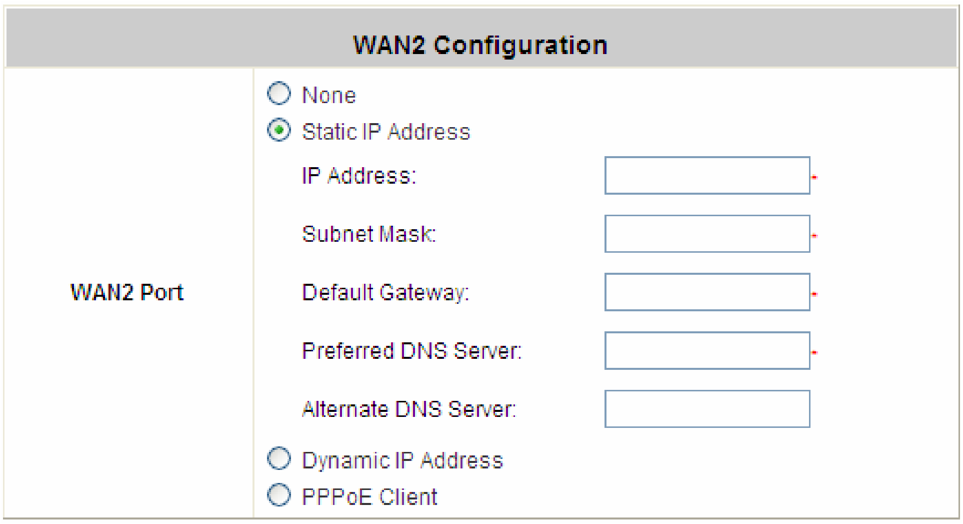


WAN2 Configuration

WAN2 Port
● None
○ Static IP Address
○ Dynamic IP Address
○ PPPoE Client

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

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

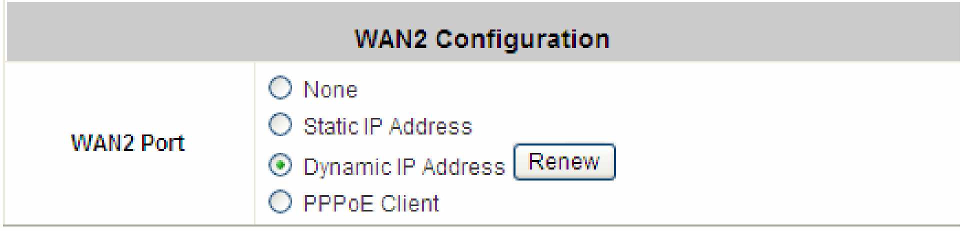


WAN2 Configuration

WAN2 Port
○ None
● Static IP Address
IP Address: ____ *
Subnet Mask: ____ *
Default Gateway: ____ *
Preferred DNS Server: ____ *
Alternate DNS Server: ____
○ Dynamic IP Address
○ PPPoE Client

IP address: the IP address of the WAN2 port.
Subnet mask: the subnet mask of the network WAN2port connects to.
Default gateway: a gateway of the network WAN2 port connects to.
Preferred DNS Server: The primary DNS server is used by the system.
Alternate DNS Server: The substitute DNS server is used by the system. This is an optional field.

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

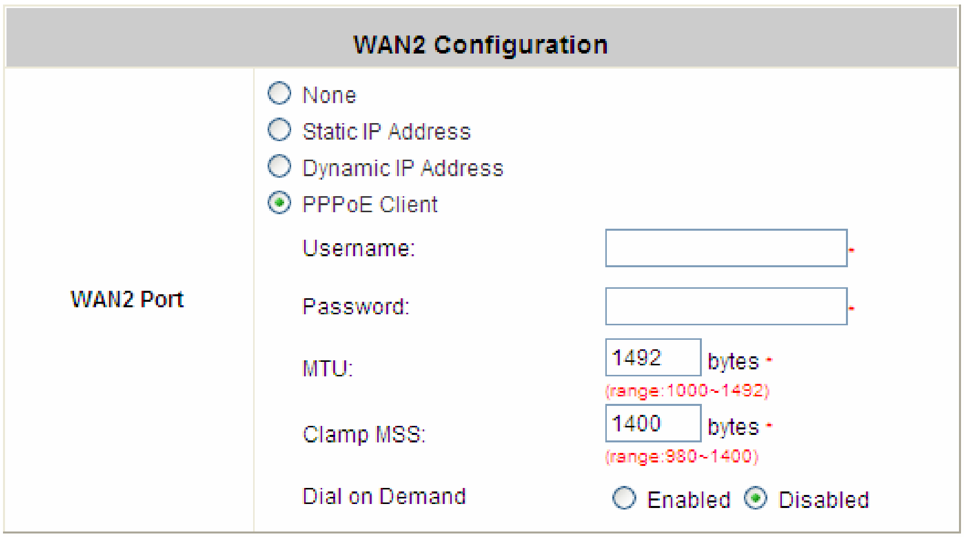


WAN2 Configuration

WAN2 Port
○ None
○ Static IP Address
● Dynamic IP Address

○ PPPoE Client

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



WAN2 Configuration

WAN2 Port

○ None
○ Static IP Address
○ Dynamic IP Address
● PPPoE Client

Username: ____ *

Password: ____ *

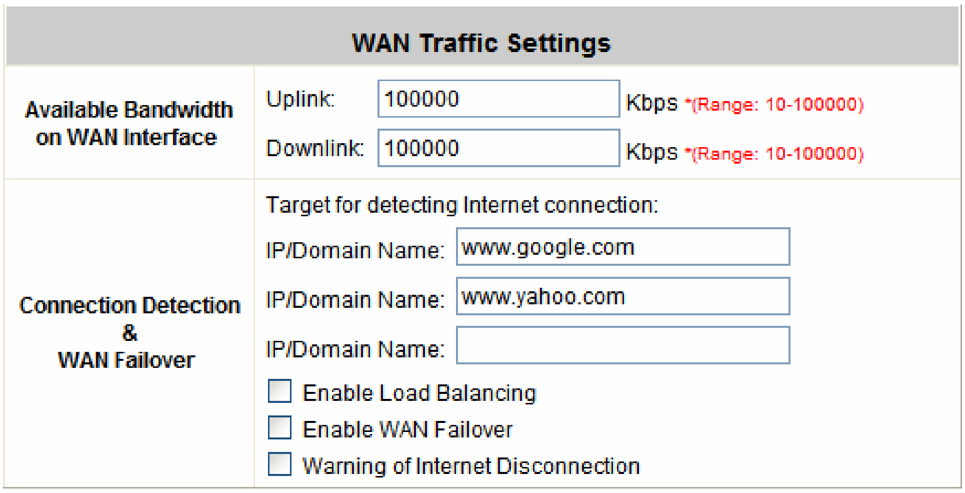
MTU: 1492 bytes *
(range:1000~1492)

Clamp MSS: 1400 bytes *
(range:980~1400)

Dial on Demand ○ Enabled ● Disabled

7.1.5 WAN Traffic Settings

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



WAN Traffic Settings

Available Bandwidth on WAN Interface	Uplink: 100000 Kbps *(Range: 10-100000) Downlink: 100000 Kbps *(Range: 10-100000)
Connection Detection & WAN Failover	Target for detecting Internet connection: IP/Domain Name: www.google.com IP/Domain Name: www.yahoo.com IP/Domain Name: □ Enable Load Balancing □ Enable WAN Failover □ Warning of Internet Disconnection

Available Bandwidth on WAN Interface:

- **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.

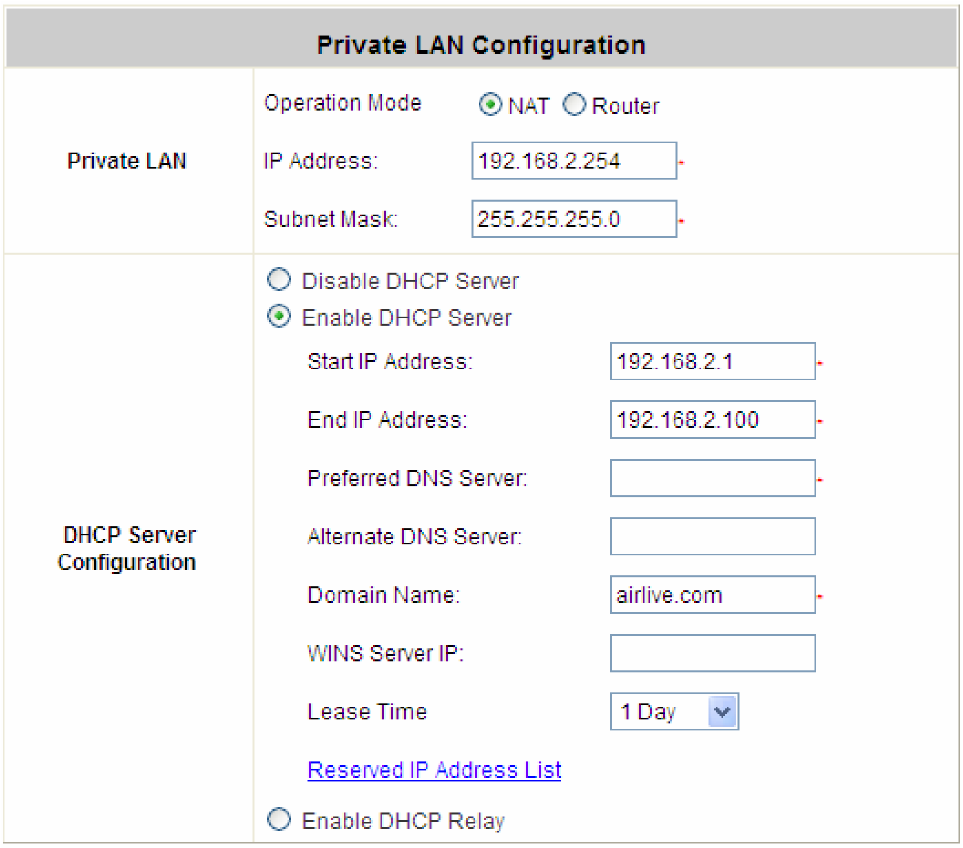
Connection Detection & WAN Failover:

- **Target for detecting Internet connection:** These URLs are used by the system as the targets to detect Internet connection, for the purpose of alert of Internet disconnection and WAN Failover. At least one URL is required to enable WAN Failover.
- **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 Percentage:** 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.
- **Enable WAN Failover:** Normally a Service Zone uses WAN1 as it primary WAN interface. When 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 enabled, the routed traffic will be back to WAN1 when WAN1 connection is recovered.
- **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.

Note: *SIP authentication is exempt from* ***Load Balancing*** *and* ***WAN Failover****. A fixed WAN port is used for SIP traffic.*

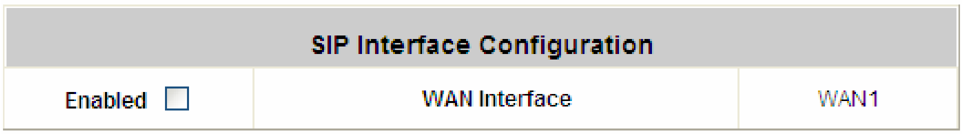
7.1.6 Private LAN Configuration

When accessing the network through the Private LAN port, users are not required to be authenticated. In this section, you can set the related configuration for the private LAN port and DHCP server.



Private LAN Configuration

Private LAN	Operation Mode	● NAT ○ Router
	IP Address:	192.168.2.254 *
	Subnet Mask:	255.255.255.0 *
DHCP Server Configuration	○ Disable DHCP Server	
	● Enable DHCP Server	
	Start IP Address:	192.168.2.1 *
	End IP Address:	192.168.2.100 *
	Preferred DNS Server:	*
	Alternate DNS Server:	
	Domain Name:	airlive.com *
	WINS Server IP:	
	Lease Time	1 Day
	Reserved IP Address List	
	○ Enable DHCP Relay	

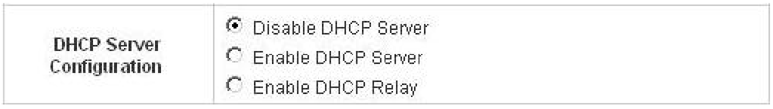


SIP Interface Configuration

Enabled □	WAN Interface	WAN1

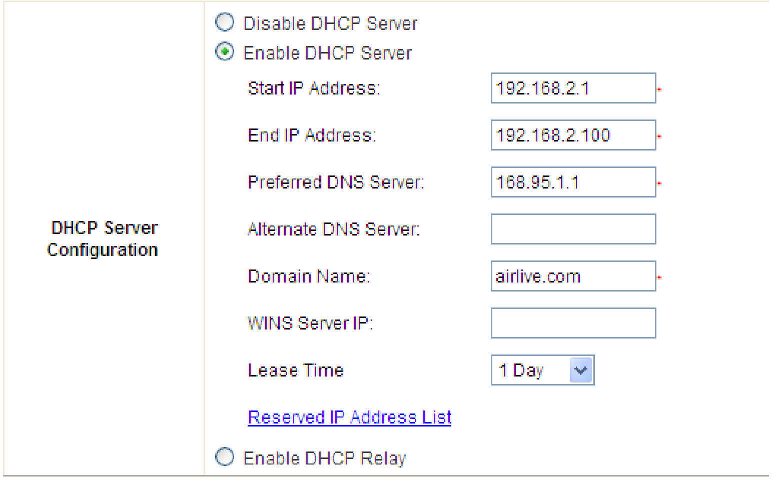
- **Private LAN**
  Operation Mode: Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.
  IP Address: Enter the desired IP address for the uncontrolled port.
  Subnet Mask: Enter the desired subnet mask for the uncontrolled port.

- **DHCP Server Configuration**
  There are three methods to set the DHCP server:
  1. **Disable DHCP Server:** Disable DHCP Server function.



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

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



DHCP Server Configuration

○ Disable DHCP Server

● Enable DHCP Server

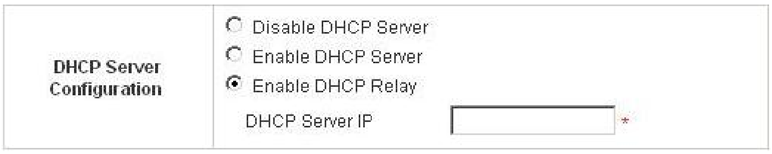
Start IP Address:	192.168.2.1 *
End IP Address:	192.168.2.100 *
Preferred DNS Server:	168.95.1.1 *
Alternate DNS Server:	
Domain Name:	airlive.com *
WINS Server IP:	
Lease Time	1 Day

Reserved IP Address List

○ Enable DHCP Relay

Start/End IP Address: These fields define the IP address range that will be assigned to the Private LAN clients.
Preferred DNS Server: The primary DNS server for the DHCP.
Alternate DNS Server: The substitute DNS server for the DHCP.
Domain Name: Enter the domain name.
WINS IP Address: Enter the IP address of WINS.
Lease Time: Choose the time to change the DHCP.
Reserved IP Address List: Enter the related Reserved IP Address, MAC, and some description (not compulsory), and click ***Apply*** to complete the setup.

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



DHCP Server Configuration

○ Disable DHCP Server

○ Enable DHCP Server

● Enable DHCP Relay

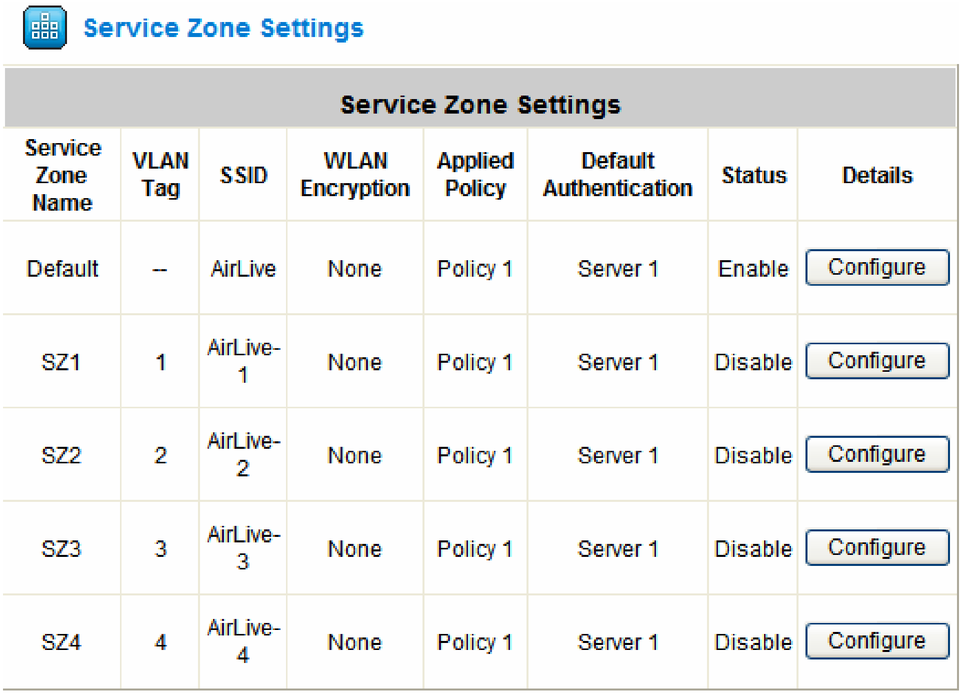
DHCP Server IP *

- **SIP Interface Configuration**
  The system provides SIP proxy functionality, which allows SIP clients to pass through NAT. When enabled, all SIP traffic of Private LAN can pass through NAT via the fixed WAN interface.

7.1.7 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, etc.

There are up to five Service Zones to be utilized; by default, they are named as: **Default**, **SZ1**, **SZ2**, **SZ3 and SZ4**, as shown in the table below.



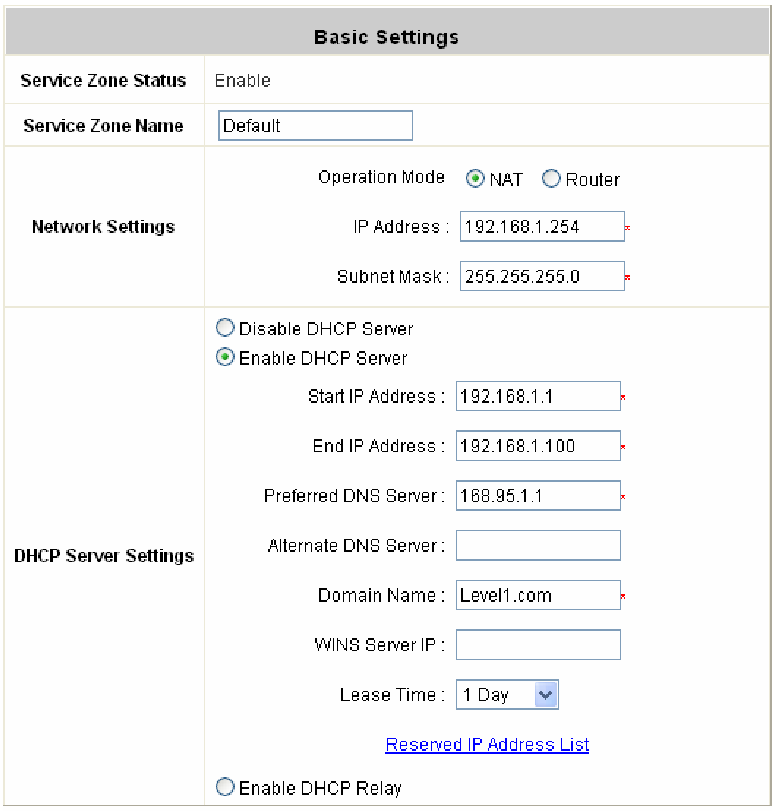
Service Zone Settings

Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default	--	AirLive	None	Policy 1	Server 1	Enable	Configure
SZ1	1	AirLive-1	None	Policy 1	Server 1	Disable	Configure
SZ2	2	AirLive-2	None	Policy 1	Server 1	Disable	Configure
SZ3	3	AirLive-3	None	Policy 1	Server 1	Disable	Configure
SZ4	4	AirLive-4	None	Policy 1	Server 1	Disable	Configure

- **Service Zone Name:** Mnemonic name of the Service Zone.
- **VLAN Tag:** 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 Authentication:** 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**, **Authentication Settings** and **Wireless Settings**.

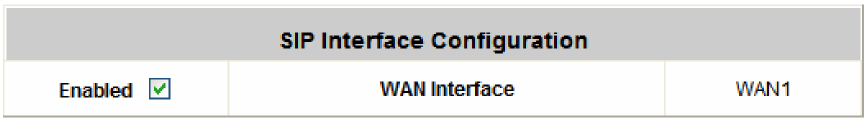
1) Service Zone Settings – Basic Settings



Basic Settings	
Service Zone Status	Enable
Service Zone Name	Default
Network Settings	Operation Mode ● NAT ○ Router IP Address : 192.168.1.254 * Subnet Mask : 255.255.255.0 *
DHCP Server Settings	○ Disable DHCP Server ● Enable DHCP Server Start IP Address : 192.168.1.1 * End IP Address : 192.168.1.100 * Preferred DNS Server : 168.95.1.1 * Alternate DNS Server : Domain Name : Level1.com * WINS Server IP : Lease Time : 1 Day Reserved IP Address List ○ Enable DHCP Relay

- **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 Settings:**
  - **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 Settings:** Related information needed on setting up the DHCP Server is described as follows. 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 MW-2000S 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 IP:** 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.

2) Service Zone Settings – SIP Interface Configuration



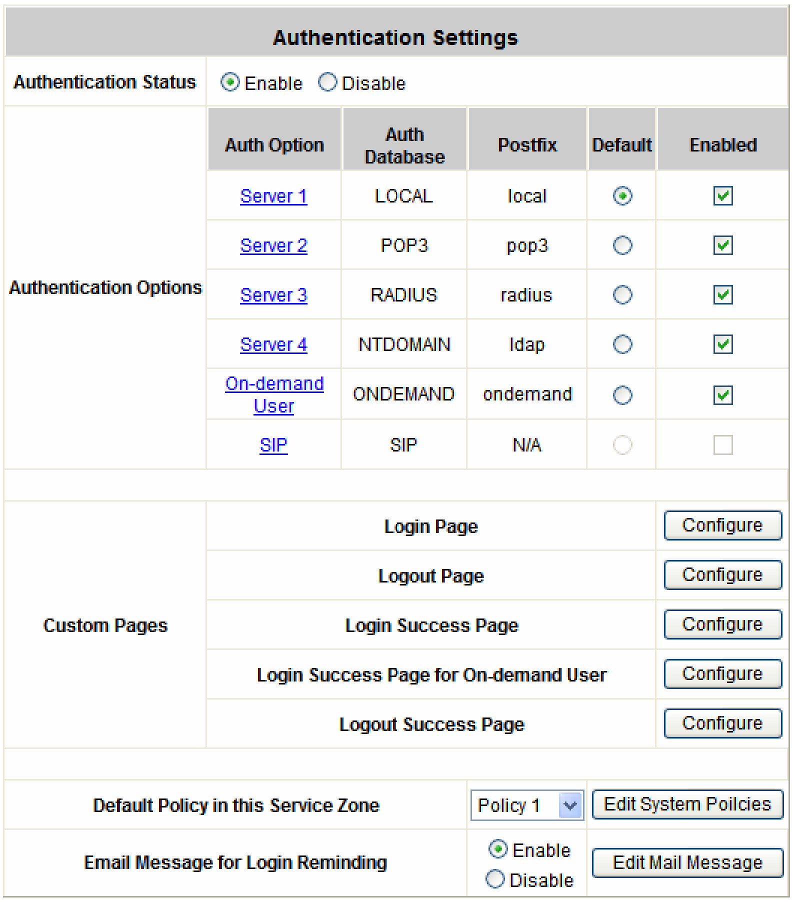
SIP Interface Configuration

Enabled ☑	WAN Interface	WAN1

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 policy 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 policy will be applied to SIP traffic.

3) Service Zone Settings – Authentication Settings



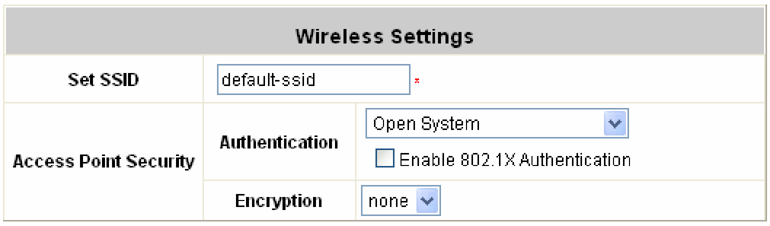
Authentication Settings

Authentication Status	● Enable ○ Disable				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	●	☑
	Server 2	POP3	pop3	○	☑
	Server 3	RADIUS	radius	○	☑
	Server 4	NTDOMAIN	ldap	○	☑
	On-demand User	ONDEMAND	ondemand	○	☑
	SIP	SIP	N/A	○	□
Custom Pages	Login Page				Configure
	Logout Page				Configure
	Login Success Page				Configure
	Login Success Page for On-demand User				Configure
	Logout Success Page				Configure
Default Policy in this Service Zone			Policy 1	Edit System Poilcies	
Email Message for Login Reminding			● Enable ○ Disable	Edit Mail Message	

- **Authentication Status:** When enabled, users must be authenticated before they get access to the network within this Service Zone.
- **Authentication Options:** There are total seven types of authentication database (LOCAL, POP3, RADIUS, LDAP, NTDOMAIN, ONDEMAND, and SIP) that are supported by the entire system. For each Service Zone, up to six authentication options can be enabled, and one of them can be set as the default option – so that users do not have to type in the postfix string while entering username during login.
- **Custom Pages:** Related login and logout pages can be customized by administrators for each service zone. Please refer to ***Appendix H – Customizable Pages*** for more details.
- **Default Policy in this Service Zone:** For each Service Zone, one policy can be applied to enforce the access control over the users. Please refer to ***5.2.3 Policy Configuration*** for complete description.

- **Email Message for Login Reminding:** 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:

4) *Service Zone Settings – Wireless Settings*

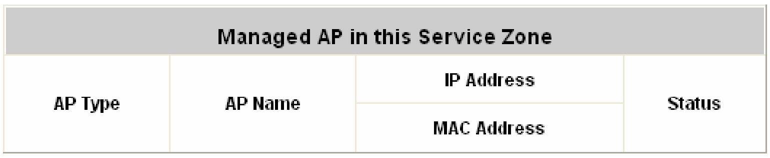


Wireless Settings		
Set SSID	default-ssid *	
Access Point Security	Authentication	Open System ▼ □ Enable 802.1X Authentication
	Encryption	none ▼

- **Set SSID:** Each service zone can be mapped with its own SSID.
- **Access Point Security:** For each service zone, administrators can set up the wireless security profile, including **Authentication** and **Encryption**.

5) *Service Zone Settings – Managed AP in this Service Zone*

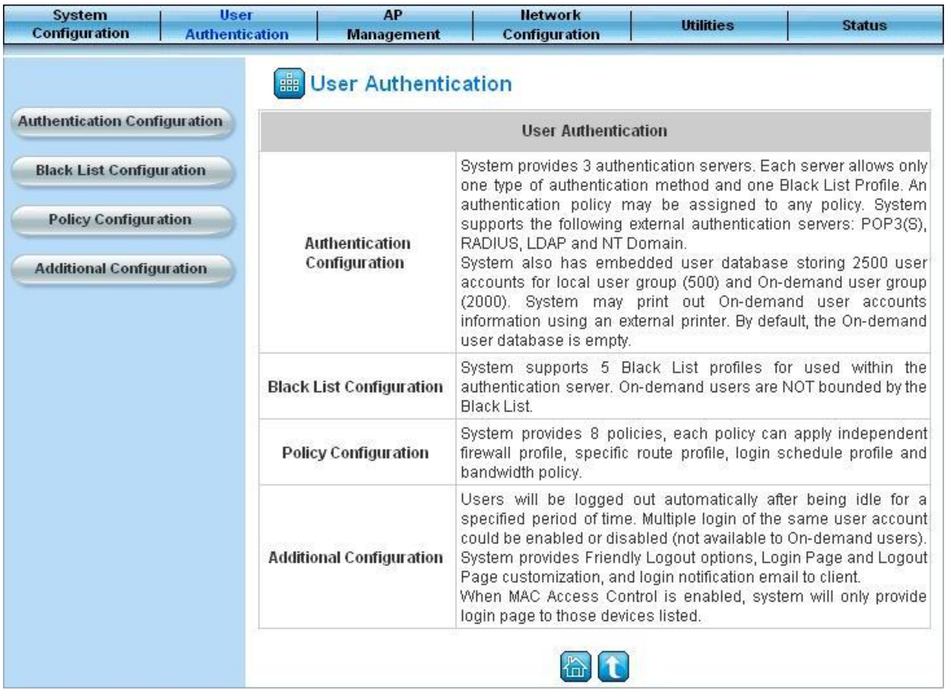
All managed APs that belong to this service zone are listed here.



Managed AP in this Service Zone			
AP Type	AP Name	IP Address	Status
		MAC Address	

7.2 User Authentication

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

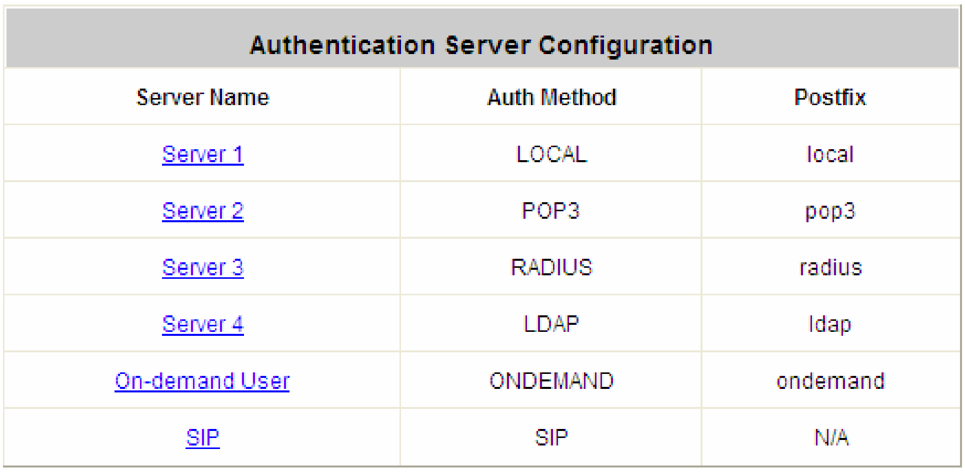


User Authentication

User Authentication	
Authentication Configuration	System provides 3 authentication servers. Each server allows only one type of authentication method and one Black List Profile. An authentication policy may be assigned to any policy. System supports the following external authentication servers: POP3(S), RADIUS, LDAP and NT Domain. System also has embedded user database storing 2500 user accounts for local user group (500) and On-demand user group (2000). System may print out On-demand user accounts information using an external printer. By default, the On-demand user database is empty.
Black List Configuration	System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.
Policy Configuration	System provides 8 policies, each policy can apply independent firewall profile, specific route profile, login schedule profile and bandwidth policy.
Additional Configuration	Users will be logged out automatically after being idle for a specified period of time. Multiple login of the same user account could be enabled or disabled (not available to On-demand users). System provides Friendly Logout options, Login Page and Logout Page customization, and login notification email to client. When MAC Access Control is enabled, system will only provide login page to those devices listed.

7.2.1 Authentication Configuration

This section is for administrators to pre-configure authentication servers for the entire system's Service Zones. For a particular Service Zone, administrators can enable all the authentication servers which will be used and also specify a default authentication server in the page of *Service Zone Settings*. Concurrently up to four servers can be selected and pre-configured here by administrators from the five types of authentication databases (LOCAL, POP3, RADIUS, LDAP, and NTDOMAIN). In addition, there are two servers (On-demand User and SIP) are selected by the system. For the Authentication Settings of each Service Zone, please see ***5.1.7 Service Zones***.



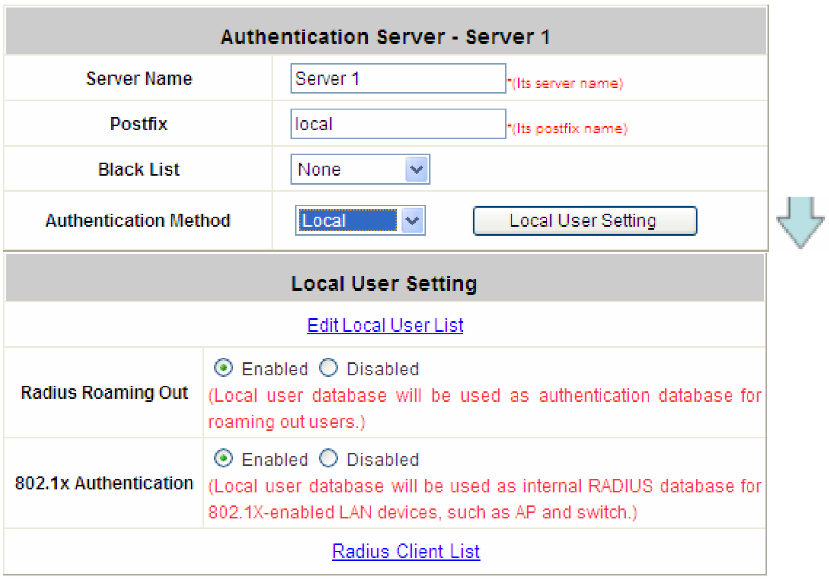
Authentication Server Configuration

Server Name	Auth Method	Postfix
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

- **Server Name:** There are several authentication options supported by MW-2000S: Server 1 to Server 4, On-demand User and SIP. Click the hyperlink of the respective Server Name to configure the authentication server.
- **Auth Method:** There are different authentication methods in MW-2000S: **LOCAL**, **POP3**, **RADIUS**, **LDAP, NTDOMAIN**, **ONDEMAND** and **SIP**.
- **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.

Note: *Concurrently only one server is allowed to be set as LOCAL or NTDOMAIN authentication method.*

7.2.1.1 Authentication Method - Local



Authentication Server - Server 1	
Server Name	Server 1 *(Its server name)
Postfix	local *(Its postfix name)
Black List	None
Authentication Method	Local · Local User Setting

Local User Setting	
Edit Local User List	
Radius Roaming Out	● Enabled ○ Disabled (Local user database will be used as authentication database for roaming out users.)
802.1x Authentication	● Enabled ○ Disabled (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
Radius Client List	

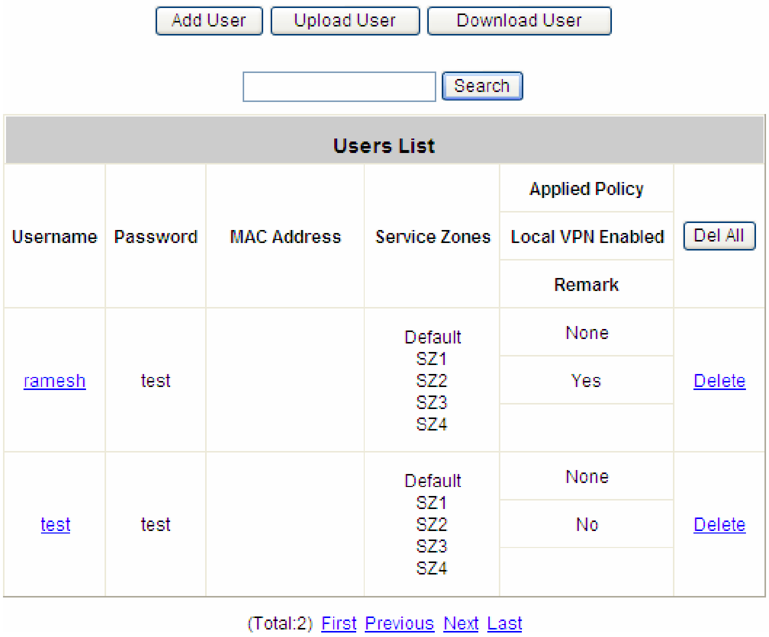
- **Name:** Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_), space and dot (.) only. The length of this field is up to 40 characters. This name is used for the administrator to identify the authentication options easily such as HQ-RADIUS.

- **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 5 sets of black lists provided by the system. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one black list from the drop-down menu and this black list will be applied to this specific authentication option.

- **Authentication Database:** The system supports five types of authentication database that are **Local, POP3**, **RADIUS**, **LDAP**, **NT Domain** and **SIP authentication**. For a specific authentication option, the Administrator can select the desired database type from the dropdown menu. Click the hyperlink ***Configure*** to enter the Local User Database Settings and then click the hyperlink ***Local User List***:

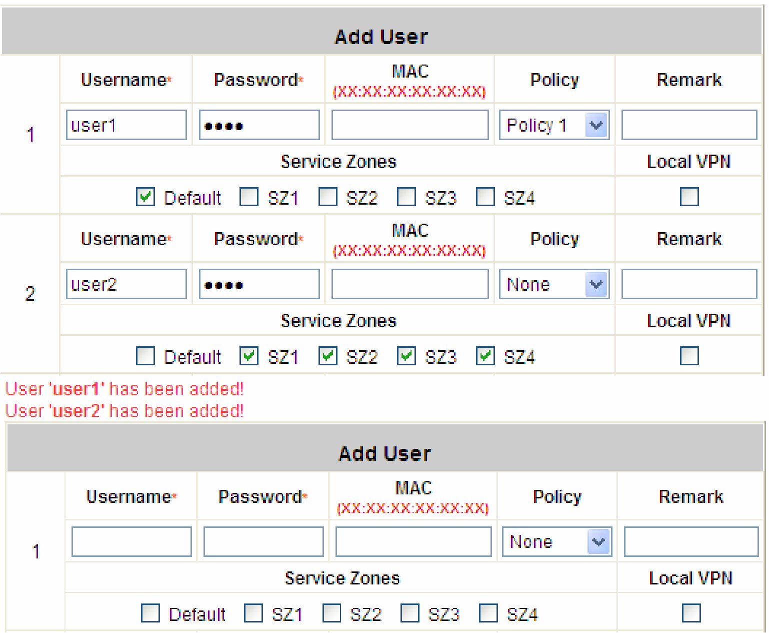
- **Local User List:** It let the administrator to view, add, and delete local user account. The *Upload User* button is for importing a list of user account from a text file. The *Download User* button is for exporting all local user accounts into a text file. Clicking on each user account leads to a page for configuring the individual local account. Local user account can be assigned a policy and applied Local VPN individually. Check the check box of individual local user account in the Enable Local VPN column to enable individually. MAC address of a networking device can be bound with a local user as well.



Users List					
Username	Password	MAC Address	Service Zones	Applied Policy Local VPN Enabled Remark	Del All
ramesh	test		Default SZ1 SZ2 SZ3 SZ4	None Yes	Delete
test	test		Default SZ1 SZ2 SZ3 SZ4	None No	Delete

(Total:2) First Previous Next Last

- ***Add User***: Click this button to enter into the **Adding User(s) to the List** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC"** and **"Remark"**. Select a desired **Policy and choose whether to enable Local VPN.** Only **"Username"** and **"Password"** are required information. Check the desired service zone(s) in **Service Zones** area; it means that the client is able to log in the system via the checked service zone(s). The rest are optional.
  For the Policy configuration, please check section on Policy Configuration.
  Click ***Apply*** to complete adding the user or users.

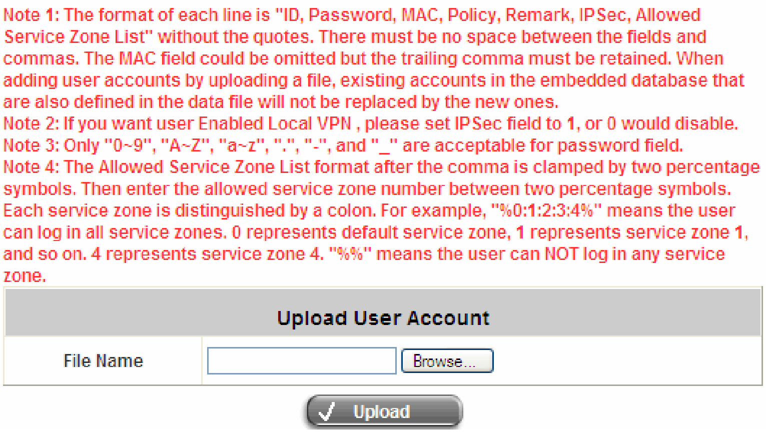


Add User					
	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
1	user1	••••		Policy 1	
	Service Zones				Local VPN
	☑ Default ☐ SZ1 ☐ SZ2 ☐ SZ3 ☐ SZ4				☐
	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
2	user2	••••		None	
	Service Zones				Local VPN
	☐ Default ☑ SZ1 ☑ SZ2 ☑ SZ3 ☑ SZ4				☐

User 'user1' has been added!
User 'user2' has been added!

Add User					
	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
1				None	
	Service Zones				Local VPN
	☐ Default ☐ SZ1 ☐ SZ2 ☐ SZ3 ☐ SZ4				☐

- ***Upload User***: Click this to enter the **Upload User from File** interface. Click the ***Browse*** button to select the text file for uploading user account, then click ***Upload*** to execute the upload process.
  The file for uploading should be a text file containing in each line the following information: ***Username, Password, MAC Address, Applied Policy, Remark, Local VPN enabled*.** There must be no spaces between the fields and commas. The MAC field can be omitted, but the trailing comma must be retained. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by the new.

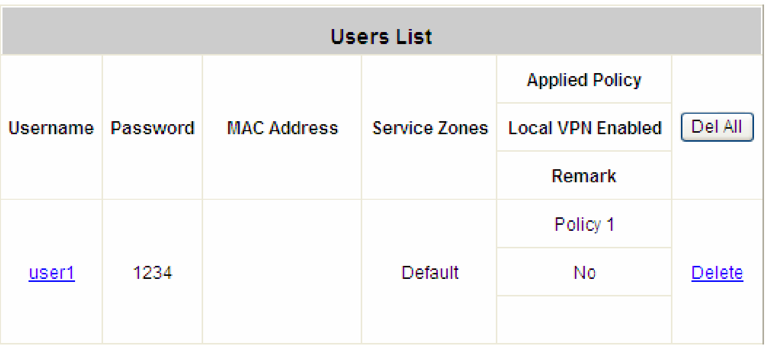


Note 1: The format of each line is "ID, Password, MAC, Policy, Remark, IPSec, Allowed Service Zone List" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.
Note 2: If you want user Enabled Local VPN , please set IPSec field to 1, or 0 would disable.
Note 3: Only "0~9", "A~Z", "a~z", ".", "-", and "_" are acceptable for password field.
Note 4: The Allowed Service Zone List format after the comma is clamped by two percentage symbols. Then enter the allowed service zone number between two percentage symbols. Each service zone is distinguished by a colon. For example, "%0:1:2:3:4%" means the user can log in all service zones. 0 represents default service zone, 1 represents service zone 1, and so on. 4 represents service zone 4. "%%" means the user can NOT log in any service zone.

Upload User Account

File Name	Browse...

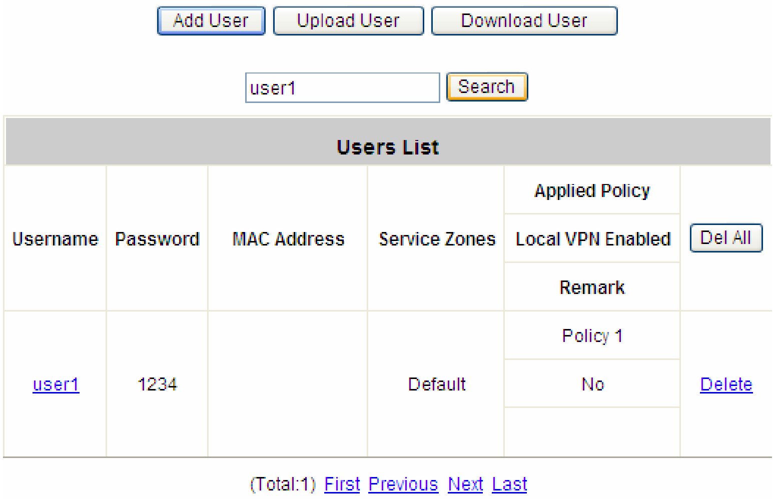
- ***Download User***: Use this function to create a .txt file with all built-in user account information and then save it on disk.



Users List

Username	Password	MAC Address	Service Zones	Applied Policy Local VPN Enabled Remark	Del All
user1	1234		Default	Policy 1 No	Delete

- ***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.



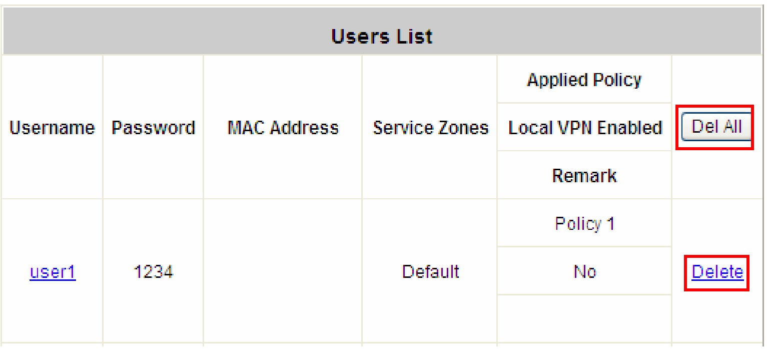
user1 Search

Users List

Username	Password	MAC Address	Service Zones	Applied Policy Local VPN Enabled Remark	Del All
user1	1234		Default	Policy 1 No	Delete

(Total:1) First Previous Next Last

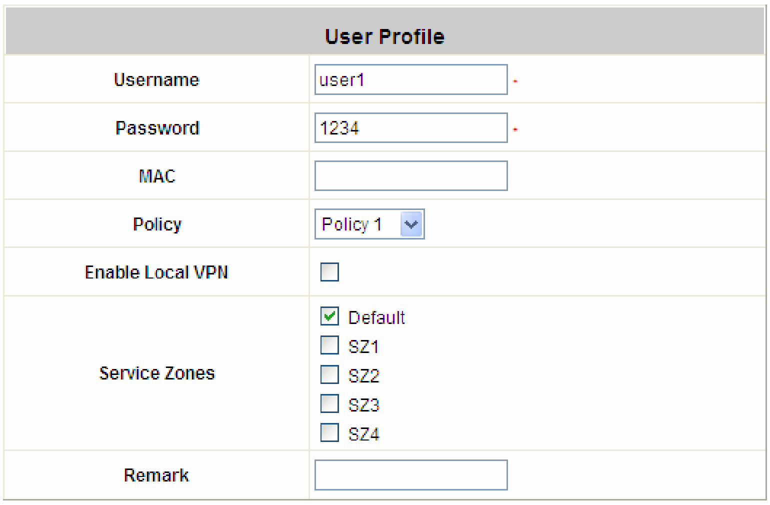
- ***Del All***: Click on this button to delete all the users at once and click on ***Delete*** to delete the user individually.



Users List

Username	Password	MAC Address	Service Zones	Applied Policy Local VPN Enabled Remark	Del All
user1	1234		Default	Policy 1 No	Delete

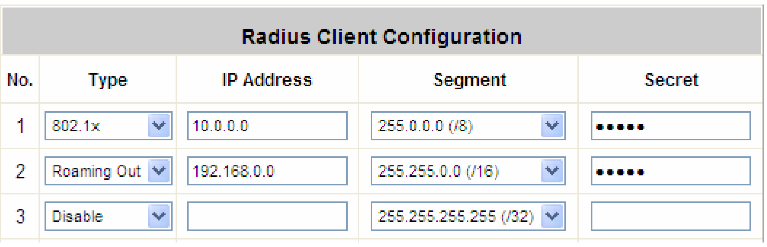
- **Edit User:** If editing the content of individual user account is needed, click the username of the desired user account to enter the **Editing Existing User Data** Interface for that particular user, and then modify or add any desired information such as **"Username"**, **"Password"**, **"MAC"**,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



User Profile

Username	user1
Password	1234
MAC	
Policy	Policy 1
Enable Local VPN	☐
Service Zones	☑ Default ☐ SZ1 ☐ SZ2 ☐ SZ3 ☐ SZ4
Remark	

- **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. Please see more explanation above in the section for **Roaming Out** and the section for **802.1X Authentication**.



Radius Client Configuration

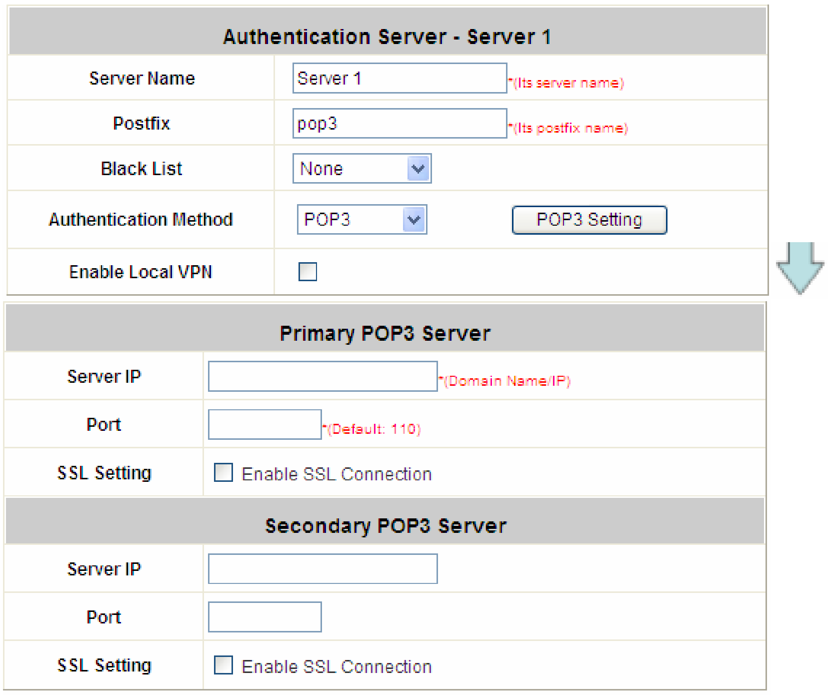
No.	Type	IP Address	Segment	Secret
1	802.1x	10.0.0.0	255.0.0.0 (/8)	●●●●●
2	Roaming Out	192.168.0.0	255.255.0.0 (/16)	●●●●●
3	Disable		255.255.255.255 (/32)	

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

- **802.1x Authentication:** When **802.1X Authentication** is enabled, the Local authentication database will be used as a RADIUS database for connection with 802.1x enabled devices such as APs or switches.
- **Account Roaming Out:** The system's local user database can also be an external RADIUS database to another system. When *Account Roaming Out* is enabled, local users can login from other domains with their original local user accounts. The authentication database with their original local user accounts acts as a RADIUS Server and roaming out local users act as RADIUS clients.

7.2.1.2 Authentication Method - POP3

Clients may login the system by their POP3 accounts. There are two sets of POP3 server provided by the system, primary and secondary which are for fault tolerance. When POP3 Server is enabled, at least one POP3 server will be required. Local VPN function can be enabled for clients authenticated by POP3 authentication method.



Authentication Server - Server 1	
Server Name	Server 1 *(Its server name)
Postfix	pop3 *(Its postfix name)
Black List	None
Authentication Method	POP3 POP3 Setting
Enable Local VPN	□

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

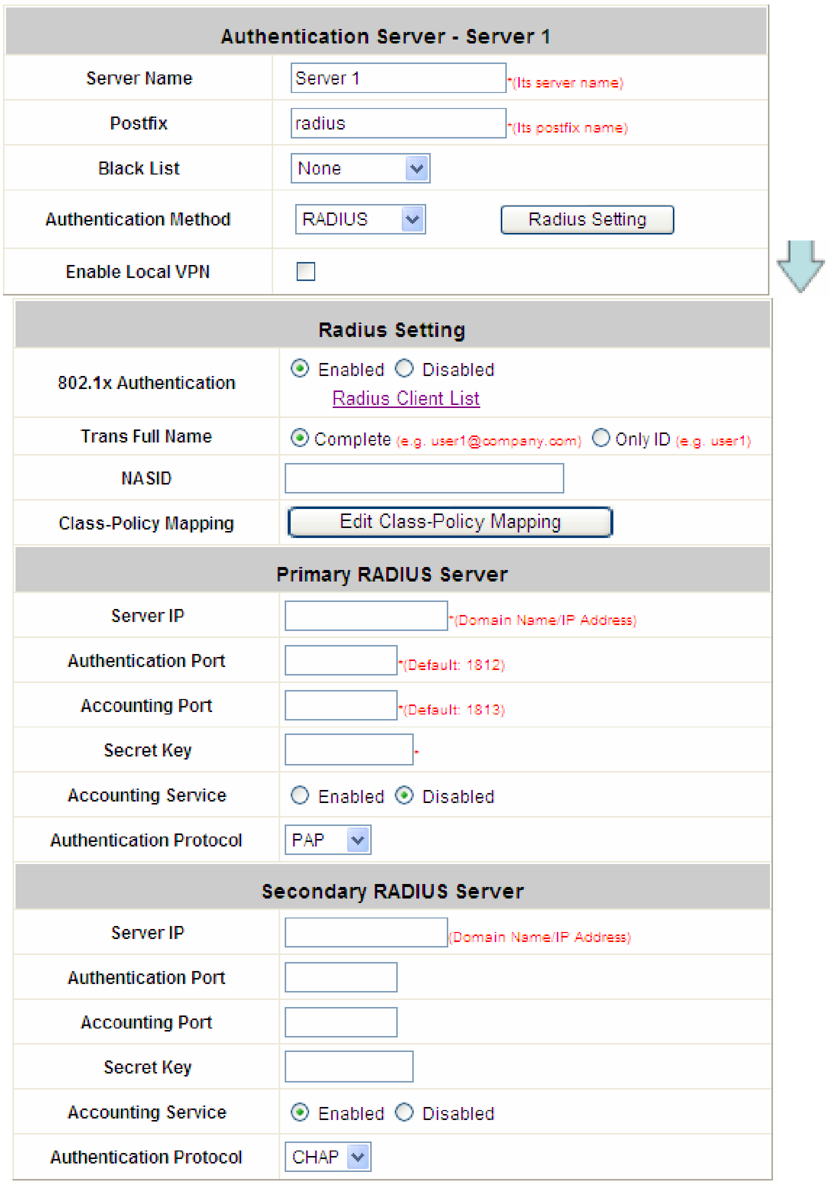
Secondary POP3 Server	
Server IP	
Port	
SSL Setting	□ Enable SSL Connection

- **Name:** Set a name for the server using 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.
- **Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using 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 five sets of the black lists. Select one of them or choose **"None"**. For details, please refer to **5.2.2 Black List.**
- **Authentication Database:** There are five authentication methods, **Local, POP3**, **RADIUS**, **LDAP** and **NT Domain**, to configure from. Select the desired method and then click the link besides the pull-down menu for more advanced configuration. Local authentication method can be chosen for one Auth Option.
- **Enable Local VPN:** When Local VPN function is enabled for the authentication option, upon the successful login of a client, a VPN tunnel will be established between a client's device and the system. The data passing through the VPN tunnel are encrypted. The system's Local VPN supports end-users' devices under Windows 2000 and Windows XP SP1, SP2.
- **Server:** The IP address of the external POP3 Server.
- **Port:** The authentication port of the external POP3 Server.
- **SSL Setting**: The system supports POP3S. Check the check box of the SSL Connection to enable POP3S.

7.2.1.3 Authentication Method - RADIUS

The system supports authentication by an external RADIUS authentication database. The system allows each RADIUS domain to have a pair of RADIUS servers, primary and secondary, for backing up each other. The system functions as a RADIUS authenticator for external RADIUS servers.

Click the hyperlink Configure for further configuration. The RADIUS server sets the external authentication for clients. Enter the related information for the primary RADIUS server and/or the secondary RADIUS server (the secondary server is not required). Information must be entered for fields with red asterisks. These settings will be effective immediately after clicking the *Apply* button.



Authentication Server - Server 1

Server Name	Server 1 *(Its server name)
Postfix	radius *(Its postfix name)
Black List	None
Authentication Method	RADIUS Radius Setting
Enable Local VPN	□

Radius Setting

802.1x Authentication	● Enabled ○ Disabled Radius Client List
Trans Full Name	● Complete (e.g. user1@company.com) ○ Only ID (e.g. user1)
NASID	
Class-Policy Mapping	Edit Class-Policy Mapping

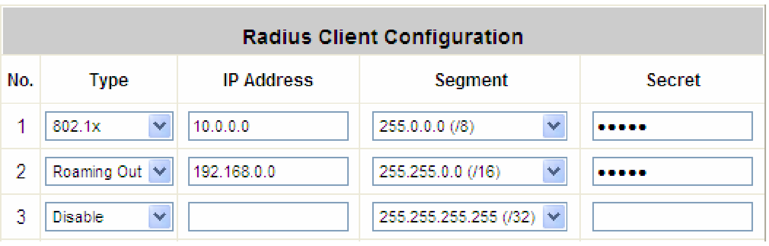
Primary RADIUS Server

Server IP	*(Domain Name/IP Address)
Authentication Port	*(Default: 1812)
Accounting Port	*(Default: 1813)
Secret Key	*
Accounting Service	○ Enabled ● Disabled
Authentication Protocol	PAP

Secondary RADIUS Server

Server IP	(Domain Name/IP Address)
Authentication Port	
Accounting Port	
Secret Key	
Accounting Service	● Enabled ○ Disabled
Authentication Protocol	CHAP

- **802.1X Authentication:** The system supports 802.1X. When the option is enabled, an extra link will become available for going to the **Roaming Out and 802.1X Client Device Settings** page, the administrator could further set up for the 802.1x capable device that are allowed to authenticate against the local user database. Select **802.1X Authentication** from the hyperlink. Enter IP address, Subnet Mask, and shared Secret Key of the authorized devices. An example would be those downstream Access Points with 802.1x option turned on and shared Secret Key set accordingly.



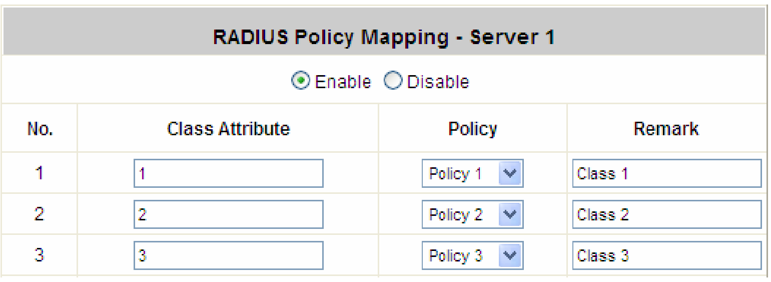
Radius Client Configuration

No.	Type	IP Address	Segment	Secret
1	802.1x	10.0.0.0	255.0.0.0 (/8)	●●●●●
2	Roaming Out	192.168.0.0	255.255.0.0 (/16)	●●●●●
3	Disable		255.255.255.255 (/32)	

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

- **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:** The Network Access Server (NAS) Identifier of the system for the external RADIUS server.
- **Class-Policy Mapping**

  This function applies the selected policy to specific clients grouped by the RADIUS class attribute. The clients will be applied with the assigned policy while logging on to the system.



RADIUS Policy Mapping - Server 1

● Enable ○ Disable

No.	Class Attribute	Policy	Remark
1	1	Policy 1	Class 1
2	2	Policy 2	Class 2
3	3	Policy 3	Class 3

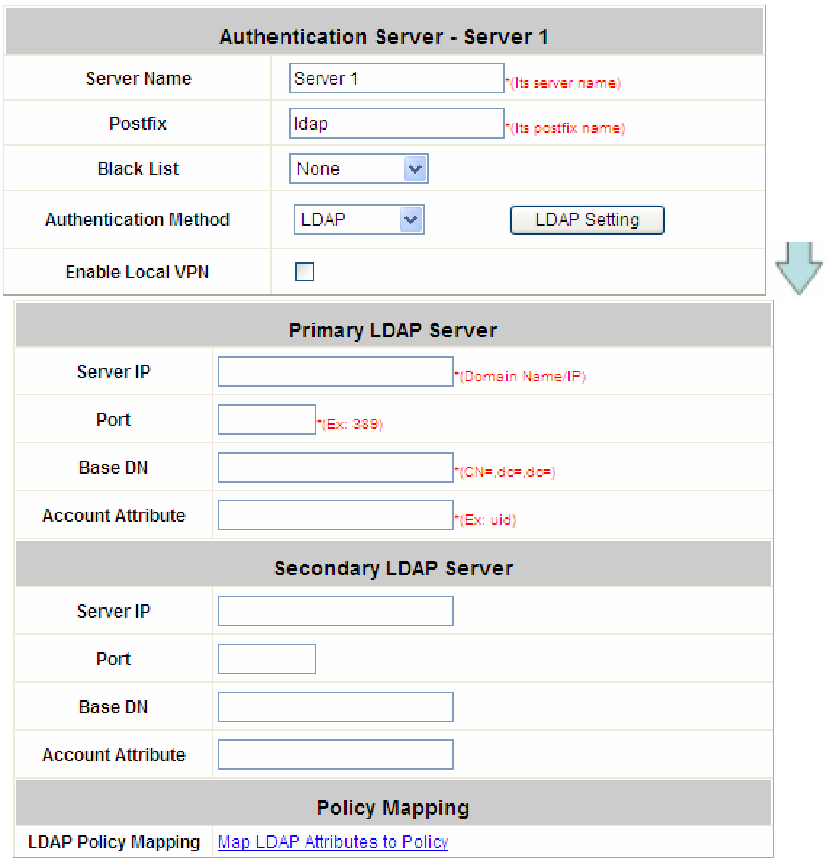
- **Server:** The IP address of the external RADIUS server.
- **Authentication Port:** Enter the authentication port of the RADIUS server.
- **Accounting Port:** The accounting port of the external RADIUS server.
- **Secret Key:** The Secret Key for RADIUS authentication.
- **Accounting Service:** The system supports RADIUS accounting that can be enabled or disabled.
- **Authentication Protocol:** The configurations of the system must match the configurations of the remote RADIUS server. **RAP** (Password Authentication Protocol) transmits password in plain text without encryption. **CHAP** (Challenge Handshake Authentication Protocol) is a more secured authentication protocol with hash encryption.

Notice: *If the RADIUS Server does not assign idle-timeout value, the MW-2000S will use the local idle-timeout.*

7.2.1.4 Authentication Method - LDAP

The system supports authentication by an external LDAP authentication database. There are two sets of LDAP server provided by the system, primary and secondary, which are for fault tolerance.

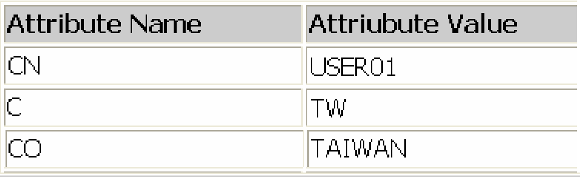
Click the hyperlink ***Configure*** for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). Information is required for fields with red asterisks. These settings will be effective immediately after clicking the ***Apply*** button.



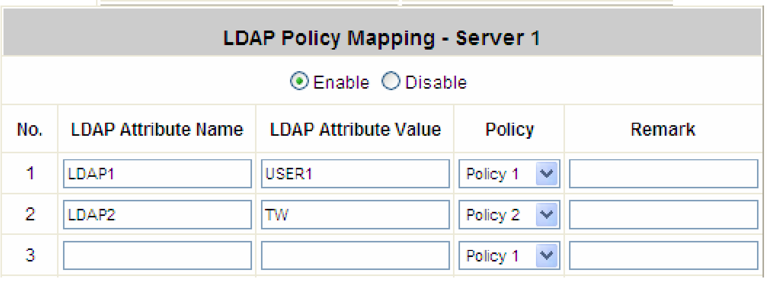
Authentication Server - Server 1		
Server Name	Server 1 *(Its server name)	
Postfix	ldap *(Its postfix name)	
Black List	None	
Authentication Method	LDAP	LDAP Setting
Enable Local VPN	□	

Primary LDAP Server	
Server IP	*(Domain Name/IP)
Port	*(Ex: 389)
Base DN	*(CN=,dc=,dc=)
Account Attribute	*(Ex: uid)
Secondary LDAP Server	
Server IP	
Port	
Base DN	
Account Attribute	
Policy Mapping	
LDAP Policy Mapping	Map LDAP Attributes to Policy

- **Server:** The IP address of the external LDAP Server.
- **Port:** The authentication port of the external LDAP Server.
- **Base DN:** The Distinguished Name for the navigation path of LDAP account.
- **Account Attribute**: The attribute of LDAP accounts.
- **LDAP Policy Mapping**: This function is to apply selected policy to certain clients grouped by LDAP attribute. The clients will be applied with the assigned policy while logging on the system. To show the attribute name and value, enter Username and Password; press ***Show Attribute***. The table of Attribute will be displayed. Enter the selected **Attribute Name** and **Attribute Value** from attribute table and **Policy** to **LDAP Attributes Mapping** page.



Attribute Name	Attriubute Value
CN	USER01
C	TW
CO	TAIWAN



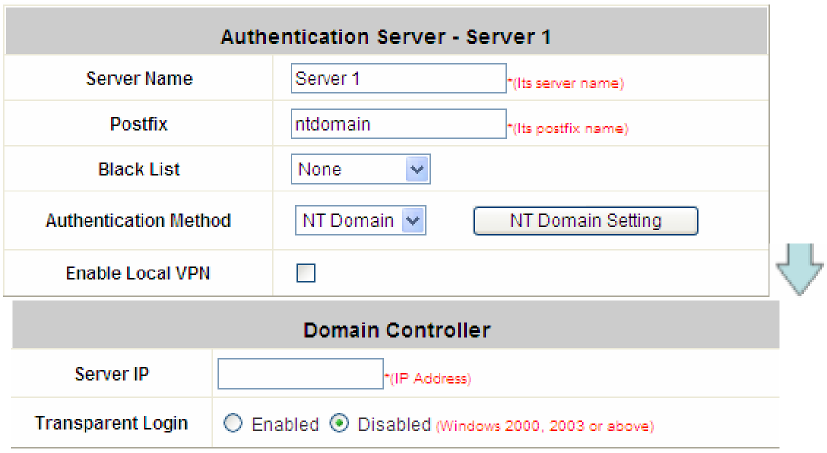
LDAP Policy Mapping - Server 1

● Enable ○ Disable

No.	LDAP Attribute Name	LDAP Attribute Value	Policy	Remark
1	LDAP1	USER1	Policy 1	
2	LDAP2	TW	Policy 2	
3			Policy 1	

7.2.1.5 Authentication Method - NT Domain

The system supports authentication by an external NT Domain authentication database.



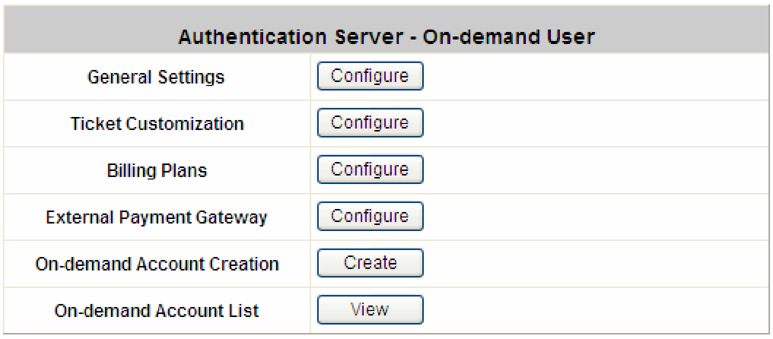
Authentication Server - Server 1	
Server Name	Server 1 *(Its server name)
Postfix	ntdomain *(Its postfix name)
Black List	None
Authentication Method	NT Domain NT Domain Setting
Enable Local VPN	□

Domain Controller	
Server IP	*(IP Address)
Transparent Login	○ Enabled ● Disabled (Windows 2000, 2003 or above)

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

7.2.1.6 Authentication Method - ONDEMAND

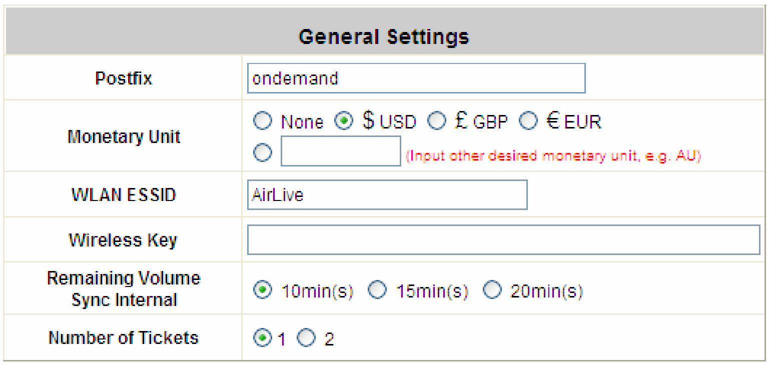
There are some deployment scenarios (for example, at venues such as coffee shops, hotels, restaurants, etc.) where retail customers or casual visitors want to get wireless Internet access. To offer the Wi-Fi access (either for commercial use or for free), user accounts should be able to be created upon request and account tickets/receipts should also be provided. Therefore, **On-demand User** is designed as the authentication option for this type of deployment scenarios.



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 List	View

1) General Settings

The common setting is for the On-demand User authentication option. The generated on-demand users and all accounts related information such postfix and unit will be shown in this list.

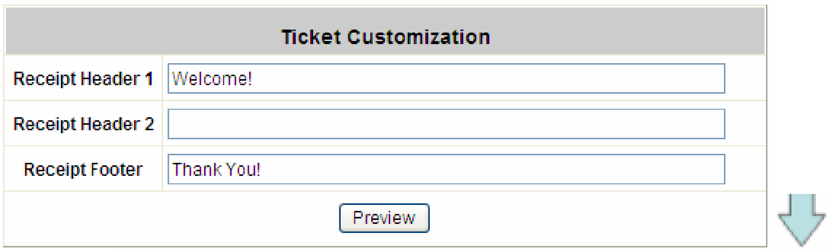


General Settings	
Postfix	ondemand
Monetary Unit	○ None ● $ USD ○ £ GBP ○ € EUR ○ (Input other desired monetary unit, e.g. AU)
WLAN ESSID	AirLive
Wireless Key	
Remaining Volume Sync Internal	● 10min(s) ○ 15min(s) ○ 20min(s)
Number of Tickets	● 1 ○ 2

- **Postfix:** Postfix is used to inform the system which type of authentication database to be used for authentication when multiple databases are concurrently in use. Enter the postfix used for on-demand users.
- **Monetary Unit:** Select the desired monetary unit or specified the unit by users.
- **WLAN ESSID:** The administrator can enter the defined wireless ESSID in this field and it will be printed on the receipt for on-demand users' reference when accessing the Internet via wireless LAN service. The ESSIDs given here should be those of the Service Zones enabled for On-demand Users.
- **Wireless Key:** The administrator can enter the defined wireless key such as WEP or WPA in the field. The Wireless Key will be printed on the receipt for the on-demand users' reference when accessing the Internet via wireless LAN service.
- **Remaining Volume Sync Internal:** While the on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval defined here.
- **Number of Tickets:** Print one or duplicate receipts, when pressing the print button of the ticket printer which connected to serial port.

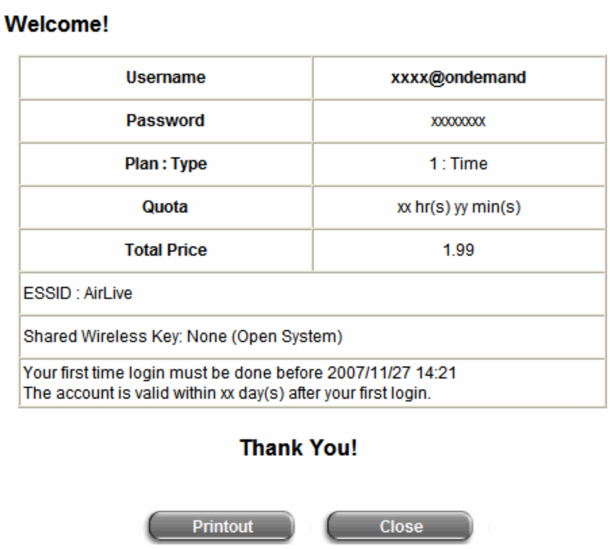
2) Ticket Customization

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



Ticket Customization

Receipt Header 1	Welcome!
Receipt Header 2	
Receipt Footer	Thank You!



Welcome!

Username	xxxx@ondemand
Password	xxxxxxxx
Plan : Type	1 : Time
Quota	xx hr(s) yy min(s)
Total Price	1.99

ESSID : AirLive

Shared Wireless Key: None (Open System)

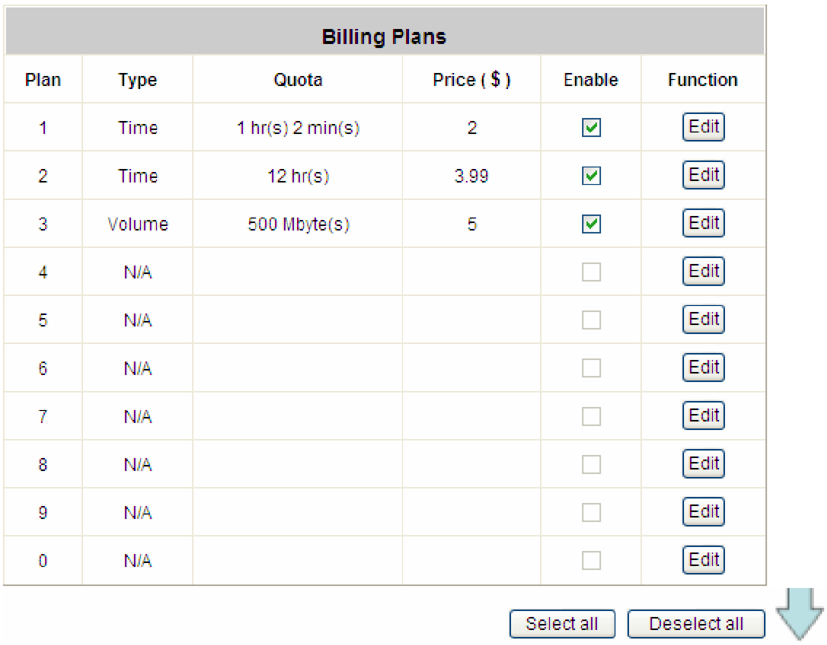
Your first time login must be done before 2007/11/27 14:21
The account is valid within xx day(s) after your first login.

Thank You!

- **Receipt Header:** There are two 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. This footer is optional.
- **Preview:** Click ***Preview*** button, the ticket will be shown including the information of username and password with the selected background. Print the ticket here.

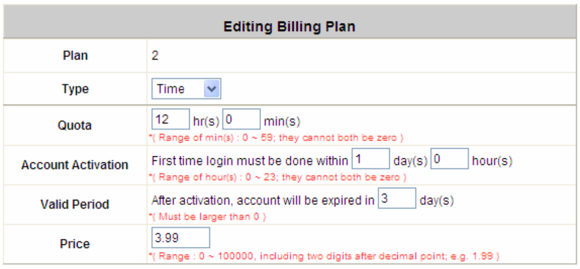
3) Billing Plans

Administrators can configure several billing plans. Click ***Edit*** button to enter the page of Editing Billing Plan. While choose the different type of the plan, the details will be shown different. Click ***Apply*** to save the plan that manually set up by the administrators. Go back to the screen of Billing Plans, click ***Enable*** button, and then the plan is activated.



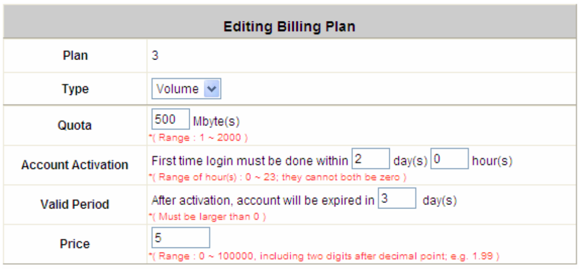
Billing Plans					
Plan	Type	Quota	Price ($)	Enable	Function
1	Time	1 hr(s) 2 min(s)	2	☑	Edit
2	Time	12 hr(s)	3.99	☑	Edit
3	Volume	500 Mbyte(s)	5	☑	Edit
4	N/A			□	Edit
5	N/A			□	Edit
6	N/A			□	Edit
7	N/A			□	Edit
8	N/A			□	Edit
9	N/A			□	Edit
0	N/A			□	Edit

- **Plan:** The number of the specific plan.
- **Type:** This is the type of the plan, based on which it defines how the account can be used.
- **Quota:** The limit on how On-demand users are allowed to access the network.
  - **Time:** Total period of time (xx hrs yy mins), during which On-demand users are allowed to access the network.



Editing Billing Plan	
Plan	2
Type	Time
Quota	12 hr(s) 0 min(s) *(Range of min(s) : 0 ~ 59; they cannot both be zero)
Account Activation	First time login must be done within 1 day(s) 0 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 3 day(s) *(Must be larger than 0)
Price	3.99 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)

  - **Volume:** Total traffic volume (xx Mbytes), up to which On-demand users are allowed to transfer data.



Editing Billing Plan	
Plan	3
Type	Volume
Quota	500 Mbyte(s) *(Range : 1 ~ 2000)
Account Activation	First time login must be done within 2 day(s) 0 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 3 day(s) *(Must be larger than 0)
Price	5 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)

- **Price:** The unit price of the plan.
- **Enable:** Click the radio button to activate the plan.
- **Function:** Click the button ***Edit*** to add one billing plan and.

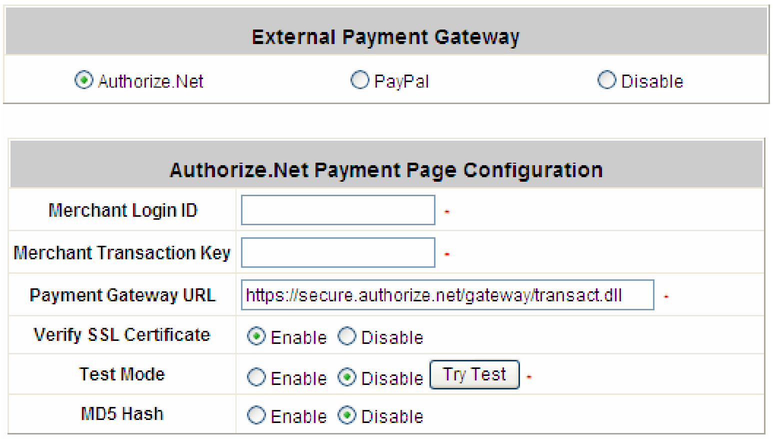
4) External Payment Gateway

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 three payment selections include: **Authorize.Net**, **PayPal** and **Disable**.

- **Authorize.Net**

  Before setting up “Authorize.Net”, it is required that the merchant owners have a valid Authorize.Net account. Please see ***Appendix D. Accepting Payments via Authorize.Net*** & ***Appendix F. Examples of Making Payments for End Users*** for more information about opening an Authorize.Net account, relevant maintenance functions, and an example for end users.



External Payment Gateway		
● Authorize.Net	○ PayPal	○ Disable

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

➢ **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.

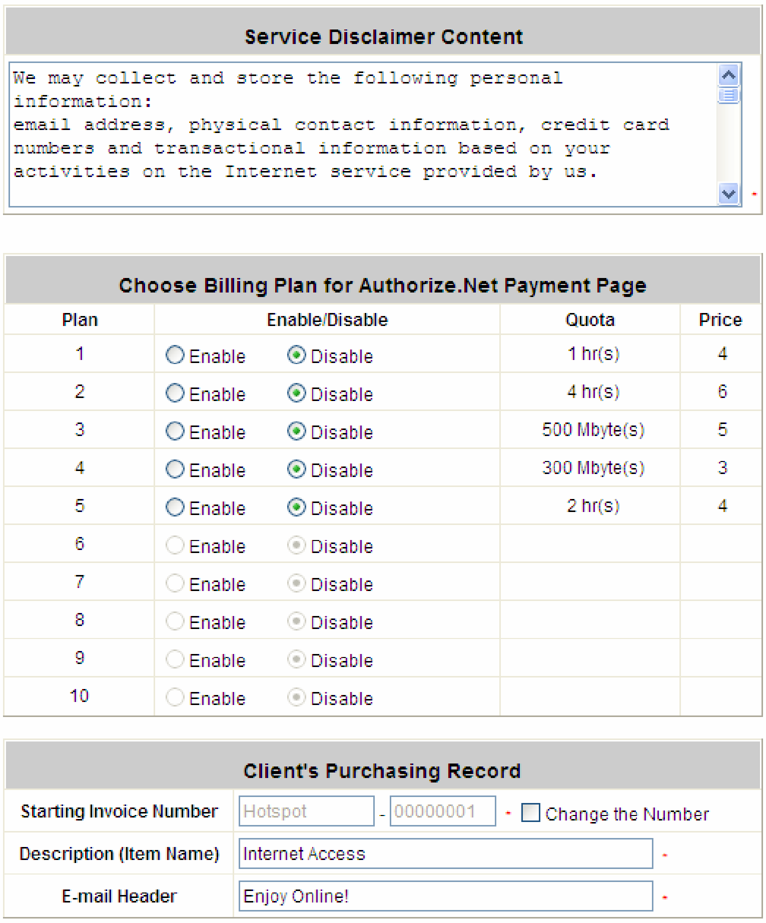
Payment Gateway URL: This is the default website address to post all transaction data.

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

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.

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

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

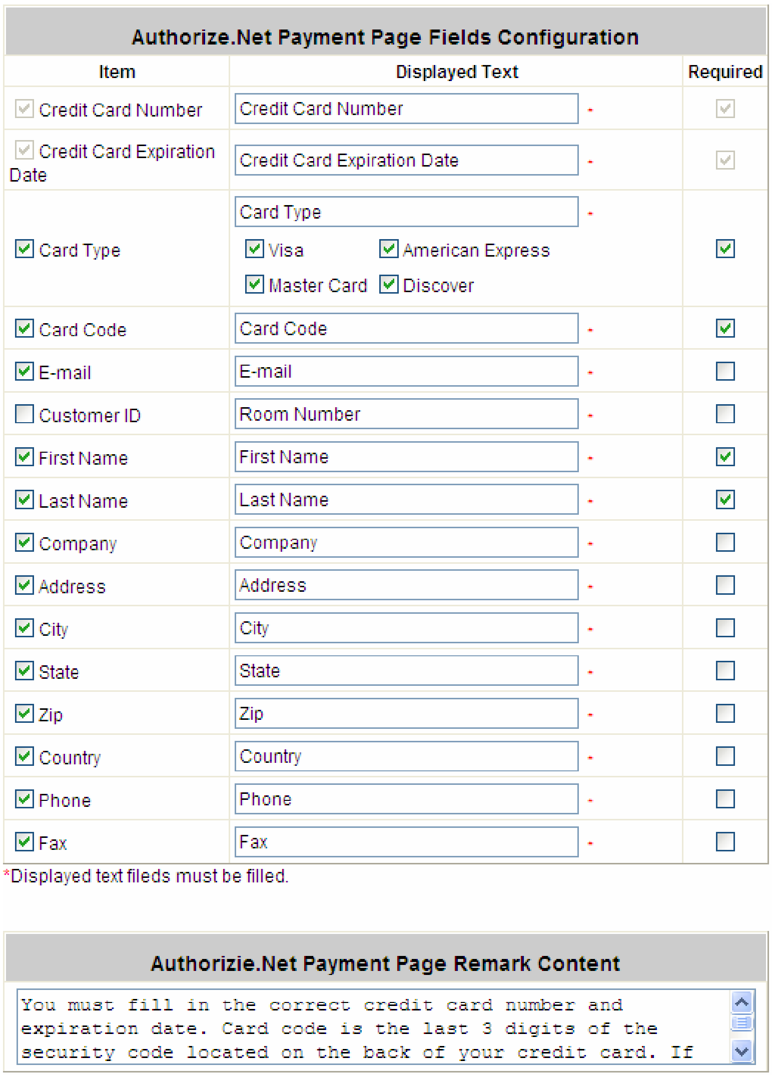
Plan	Enable/Disable		Quota	Price
1	○ Enable	● Disable	1 hr(s)	4
2	○ Enable	● Disable	4 hr(s)	6
3	○ Enable	● Disable	500 Mbyte(s)	5
4	○ Enable	● Disable	300 Mbyte(s)	3
5	○ Enable	● Disable	2 hr(s)	4
6	○ Enable	● Disable		
7	○ Enable	● Disable		
8	○ Enable	● Disable		
9	○ Enable	● Disable		
10	○ Enable	● Disable		

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 *	☑
☑ Card Type	Card Type * ☑ Visa ☑ American Express ☑ Master Card ☑ Discover	☑
☑ Card Code	Card Code *	☑
☑ E-mail	E-mail *	☐
☐ Customer ID	Room Number *	☐
☑ First Name	First Name *	☑
☑ Last Name	Last Name *	☑
☑ 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.

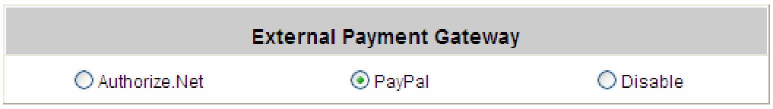
➢ **Authorizie.Net Payment Page Remark Content**

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

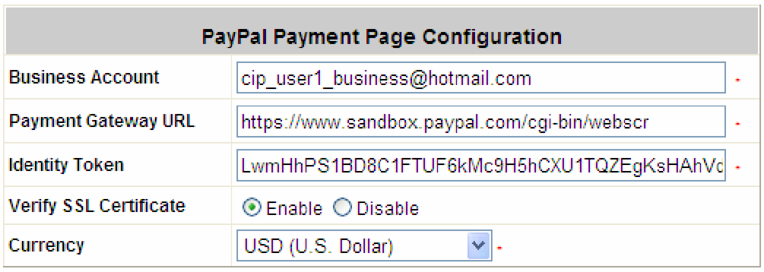
- **PayPal**

Before setting up "PayPal", it is required that the merchant owners have a valid PayPal "Business Account". Please see ***Appendix D. Accepting Payments via PayPal & Appendix E. Examples of Making Payments for End Users*** for more information about setting up a PayPal Business Account, relevant maintenance functions, and an example for end users.

After opening a PayPal Business Account, the merchant should find the **"Identity Token"** of this PayPal account to continue **"PayPal Payment Page Configuration"**.



External Payment Gateway		
○ Authorize.Net	● PayPal	○ Disable



PayPal Payment Page Configuration	
Business Account	cip_user1_business@hotmail.com -
Payment Gateway URL	https://www.sandbox.paypal.com/cgi-bin/webscr -
Identity Token	LwmHhPS1BD8C1FTUF6kMc9H5hCXU1TQZEgKsHAhVc -
Verify SSL Certificate	● Enable ○ Disable
Currency	USD (U.S. Dollar) -

➢ **PayPal Payment Page Configuration**

Business Account: This is the "Login ID" (email address) that is associated with the PayPal Business Account.

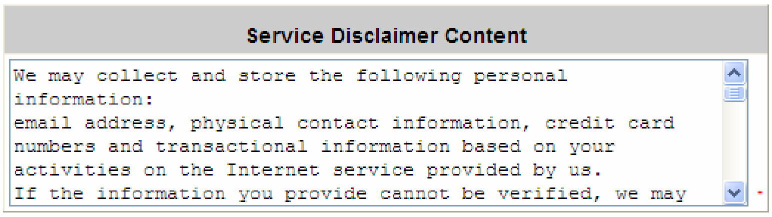
Payment Gateway URL: This is the default website address to post all transaction data.

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

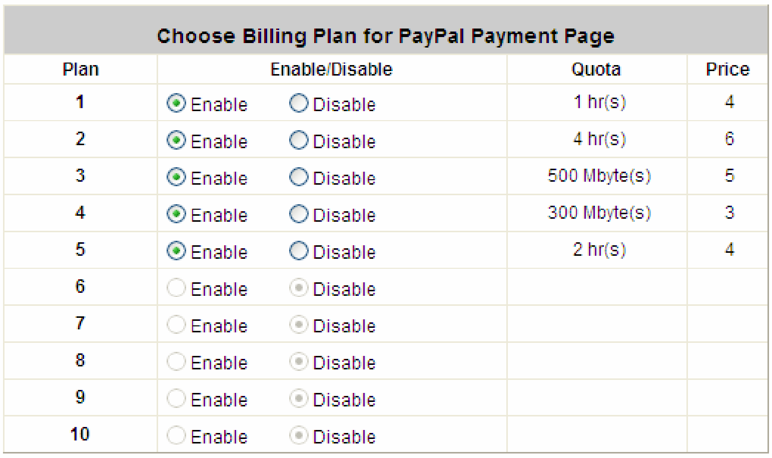
Currency: It is the currency to be used for the payment transactions.

Service Disclaimer Content /Choose Billing 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	1 hr(s)	4
2	● Enable	○ Disable	4 hr(s)	6
3	● Enable	○ Disable	500 Mbyte(s)	5
4	● Enable	○ Disable	300 Mbyte(s)	3
5	● Enable	○ Disable	2 hr(s)	4
6	○ Enable	● Disable		
7	○ Enable	● Disable		
8	○ Enable	● Disable		
9	○ Enable	● Disable		
10	○ Enable	● Disable		

- **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 PayPal Payment Page**

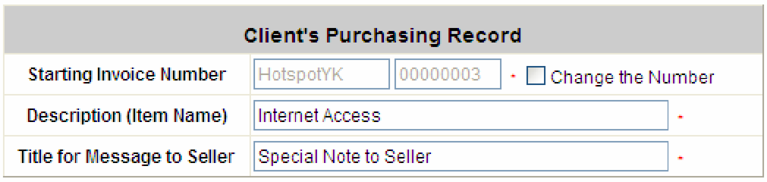
  These 10 plans are the plans configured in **Billing Plans** page, and all previously enabled plans can be further enabled or disabled here, as needed.

  Enable/Disable: Choose to enable or cancel the plan.

  Quota: The usage time or condition of each plan.

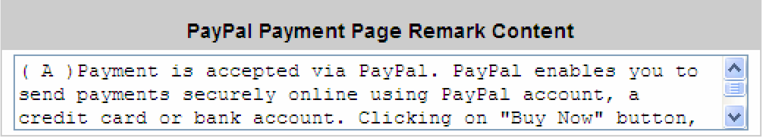
  Price: The price charged for this plan.

Client's Purchasing Record/ PayPal Payment Page Remark Content



Client's Purchasing Record

Starting Invoice Number	HotspotYK 00000003 * □ 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**

  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).

  Title for Message to Seller: Administrators can edit the header "**title**" of the message note, used in the PayPal payment page.

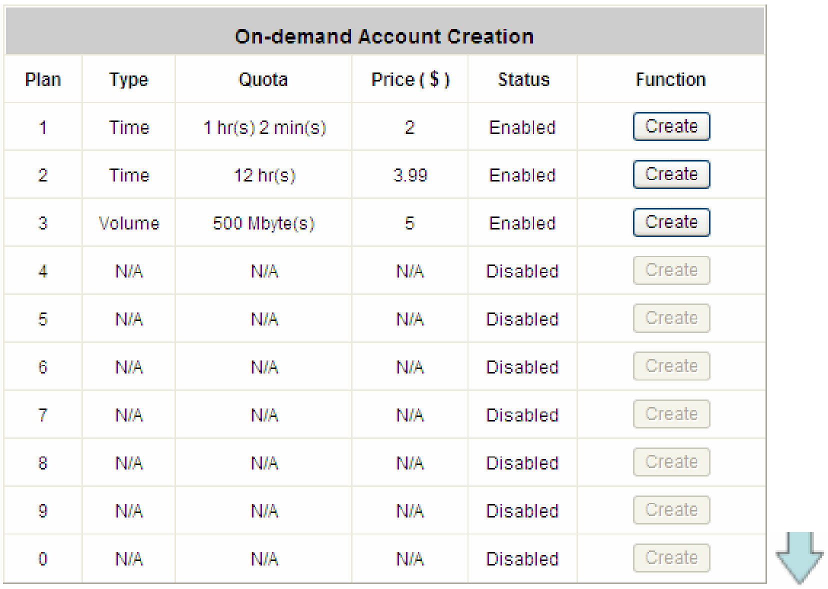
- **PayPal Payment Page Remark Content**
  The message content will be displayed as a special notice to end customers in the page of "Rate Plan". For example, it can describe the cautions for making a payment via PayPal.

5) On-demand Account Creation

On-demand accounts are listed and related. When at least one plan is enabled, the administrator can generate on-demand user accounts here. Click this to enter the On-demand Account Creation screen. Click on the ***Create*** button of the desired plan and an on-demand user account will be created. Click ***Print*** to print a receipt which will contain the on-demand user's information, including the username and password.

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.*

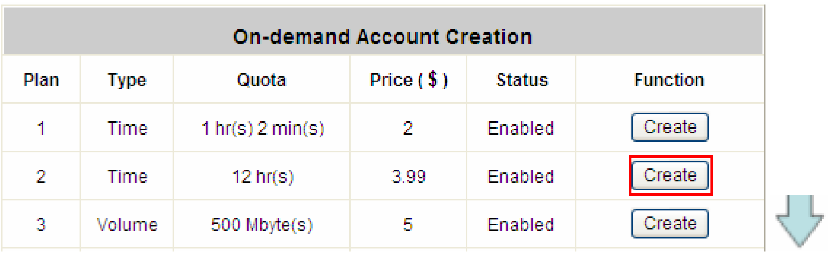
The printer used by ***Print*** *is a pre-configured printer connected to the administrator's computer.*



On-demand Account Creation

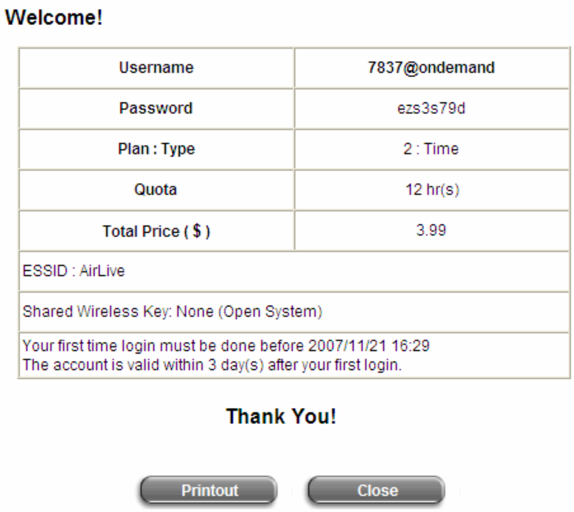
Plan	Type	Quota	Price ($)	Status	Function
1	Time	1 hr(s) 2 min(s)	2	Enabled	Create
2	Time	12 hr(s)	3.99	Enabled	Create
3	Volume	500 Mbyte(s)	5	Enabled	Create
4	N/A	N/A	N/A	Disabled	Create
5	N/A	N/A	N/A	Disabled	Create
6	N/A	N/A	N/A	Disabled	Create
7	N/A	N/A	N/A	Disabled	Create
8	N/A	N/A	N/A	Disabled	Create
9	N/A	N/A	N/A	Disabled	Create
0	N/A	N/A	N/A	Disabled	Create

- **Plan:** The number of a specific plan.
- **Type:** Show one type of the plan in Time, Volume or Cut-off.
- **Quota:** The Time Volume is how long the on-demand user is allowed to access the Internet.
- **Price:** The unit price of each plan.
- **Status:** Show the status in enabled or disabled.
- **Function:** Press ***Create*** button for the desired plan; an On-demand user account will be created, then to click ***Printout*** to print a receipt which will contain this on-demand user's information.



On-demand Account Creation

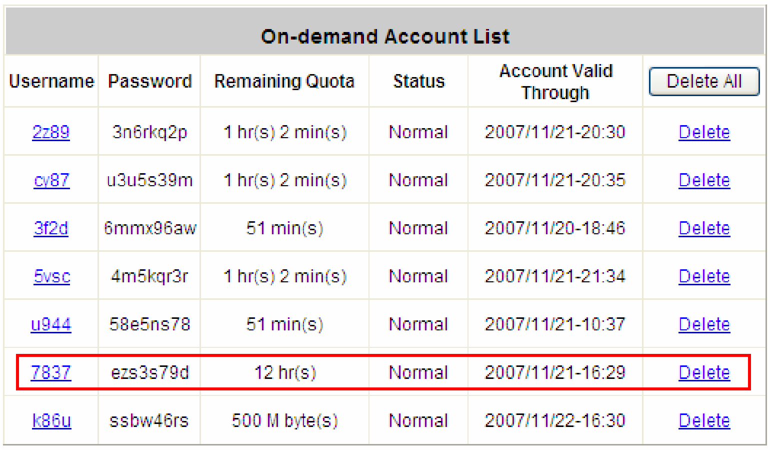
Plan	Type	Quota	Price ($)	Status	Function
1	Time	1 hr(s) 2 min(s)	2	Enabled	Create
2	Time	12 hr(s)	3.99	Enabled	Create
3	Volume	500 Mbyte(s)	5	Enabled	Create



Welcome!

Username	7837@ondemand
Password	ezs3s79d
Plan : Type	2 : Time
Quota	12 hr(s)
Total Price ($)	3.99
ESSID : AirLive	
Shared Wireless Key: None (Open System)	
Your first time login must be done before 2007/11/21 16:29 The account is valid within 3 day(s) after your first login.	

Thank You!

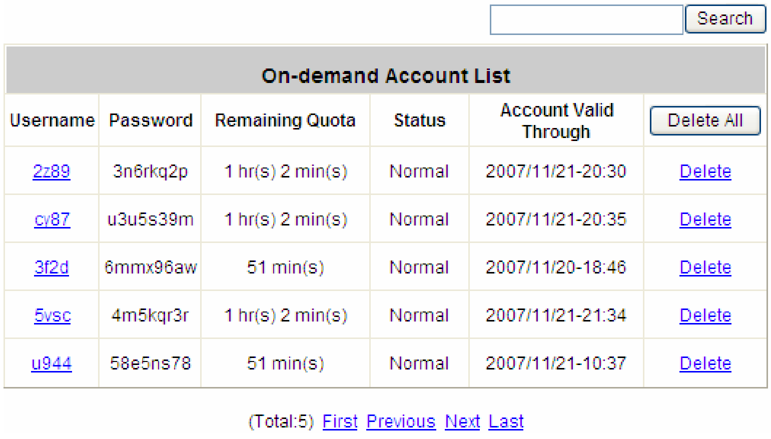


On-demand Account List

Username	Password	Remaining Quota	Status	Account Valid Through	Delete All
2z89	3n6rkq2p	1 hr(s) 2 min(s)	Normal	2007/11/21-20:30	Delete
cy87	u3u5s39m	1 hr(s) 2 min(s)	Normal	2007/11/21-20:35	Delete
3f2d	6mmx96aw	51 min(s)	Normal	2007/11/20-18:46	Delete
5vsc	4m5kqr3r	1 hr(s) 2 min(s)	Normal	2007/11/21-21:34	Delete
u944	58e5ns78	51 min(s)	Normal	2007/11/21-10:37	Delete
7837	ezs3s79d	12 hr(s)	Normal	2007/11/21-16:29	Delete
k86u	ssbw46rs	500 M byte(s)	Normal	2007/11/22-16:30	Delete

6) On-demand Account List

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



On-demand Account List

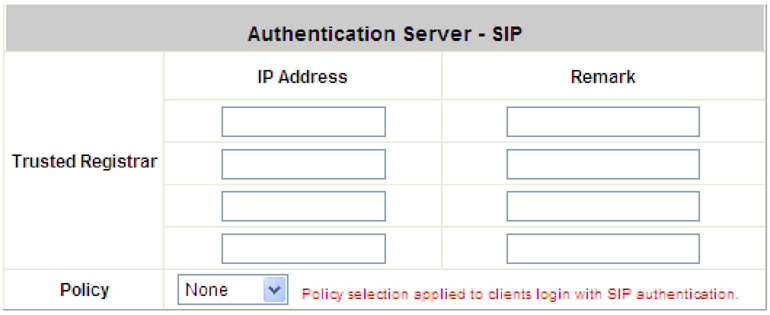
Username	Password	Remaining Quota	Status	Account Valid Through	Delete All
2z89	3n6rkq2p	1 hr(s) 2 min(s)	Normal	2007/11/21-20:30	Delete
cy87	u3u5s39m	1 hr(s) 2 min(s)	Normal	2007/11/21-20:35	Delete
3f2d	6mmx96aw	51 min(s)	Normal	2007/11/20-18:46	Delete
5vsc	4m5kqr3r	1 hr(s) 2 min(s)	Normal	2007/11/21-21:34	Delete
u944	58e5ns78	51 min(s)	Normal	2007/11/21-10:37	Delete

(Total:5) First Previous Next Last

- **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.
- **Username:** The login name of the user.
- **Password:** The login password of the user.
- **Remaining Quota:** The remaining time or volume that the user 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
- **Delete All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

7.2.1.7 Authentication Method - SIP

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. Administrator will be able to add trusted SIP Registrars up to four of them. A policy can be chosen to govern SIP traffic.

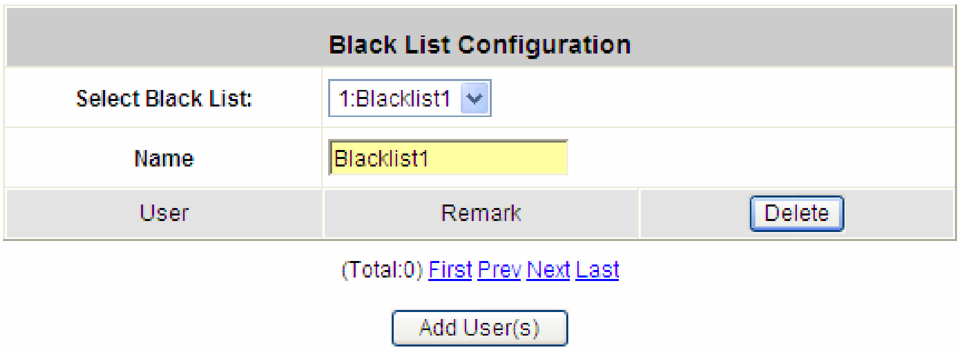


Authentication Server - SIP		
	IP Address	Remark
Trusted Registrar		
Policy	None	Policy selection applied to clients login with SIP authentication.

- **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.
- **Policy:** The Policy applied to the clients that login with SIP Authentication.

7.2.2 Black List Configuration

The administrator can add, delete, or edit the black list for user access control. Each black list can include up to 40 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.

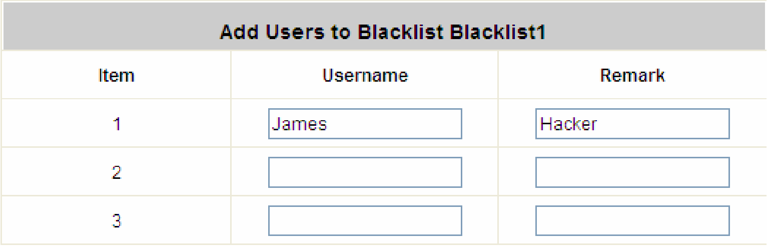


Black List Configuration		
Select Black List:	1:Blacklist1	
Name	Blacklist1	
User	Remark	Delete

(Total:0) First Prev Next Last

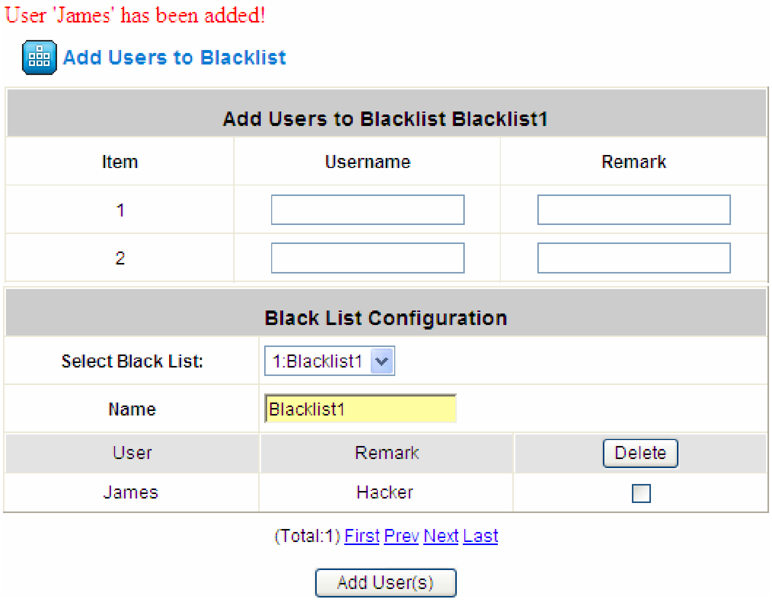
Add User(s)

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



Add Users to Blacklist Blacklist1		
Item	Username	Remark
1	James	Hacker
2		
3		

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



User 'James' has been added!

Add Users to Blacklist

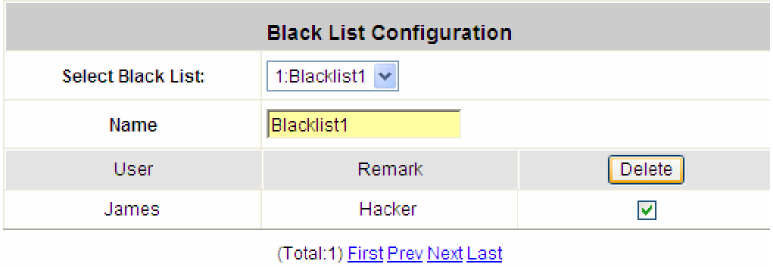
Add Users to Blacklist Blacklist1		
Item	Username	Remark
1		
2		

Black List Configuration		
Select Black List:	1:Blacklist1	
Name	Blacklist1	
User	Remark	Delete
James	Hacker	□

(Total:1) First Prev Next Last

Add User(s)

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



Black List Configuration		
Select Black List:	1:Blacklist1	
Name	Blacklist1	
User	Remark	Delete
James	Hacker	☑

(Total:1) First Prev Next Last

7.2.3 Policy Configuration

Global policy is the system's universal policy including Firewall, Specific Route and Privilege, which will be applied to all users unless the user has been regulated and applied to another policy. Each policy consists of Firewall Profile, Specific Route Profile, Schedule Profile, QoS Profile and Privilege Profile. Policies can be defined in the Policy tab. The administrator can select one of the defined policies to apply it to the specific authentication option. All clients belong to this authentication option will be bound by this policy.

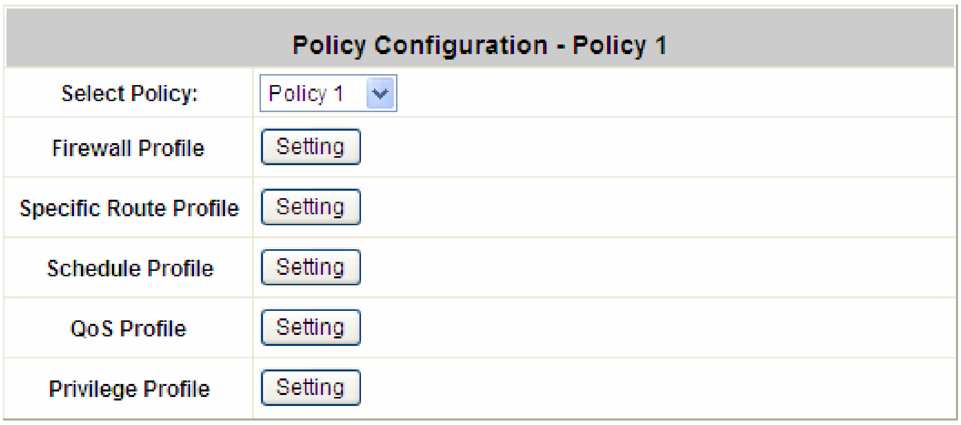
When the type of authentication method is "Local", a policy can be applied on a per-user basis. When the type of method is NT Domain or ONDEMAND, a policy is applied to the whole user database.

When the type of method is RADIUS, a policy is mapped to a user group of a RADIUS class. The Class-Policy Mapping function will be available to let the administrator assign a policy for a RADIUS Class attribute.

When the type of method is LDAP, a policy is applied to user group defined an attribute-value pair. The Attribute-Policy Mapping function will be available to let the administrator assign a policy for a LDAP Attribute.

When the type of method is SIP, the Policy selection function will be available to let the administrator assign a policy for all SIP users.

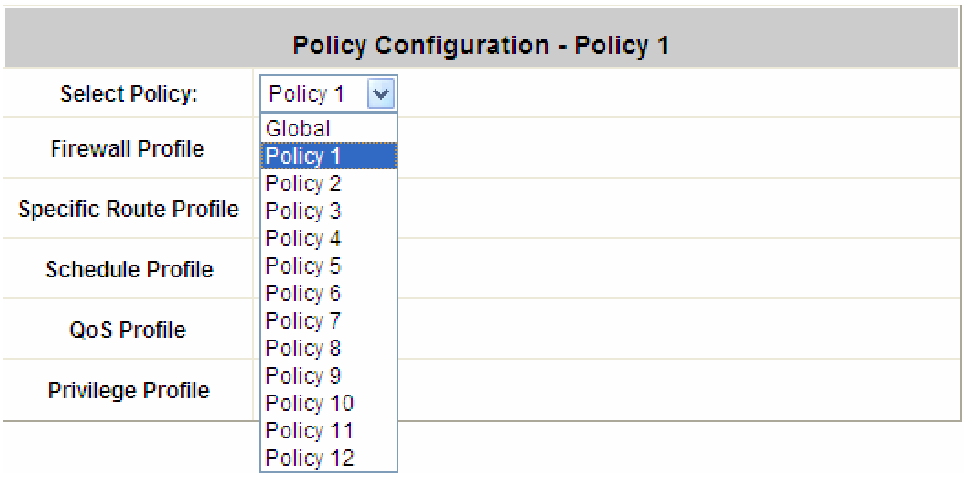
- **Policy 1~12**



Policy Configuration - Policy 1

Select Policy:	Policy 1
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
QoS Profile	Setting
Privilege Profile	Setting

➢ **Select Policy:** Select one Policy from **Policy 1 ~ Policy 12**.

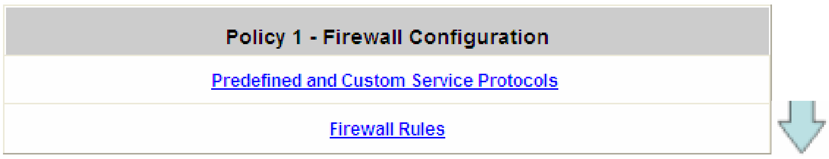


Policy Configuration - Policy 1

Select Policy: Policy 1

➢ **Firewall Profile**

Click the hyperlink of ***Setting*** for **Firewall Profile**, the Firewall Profiles list will appear.

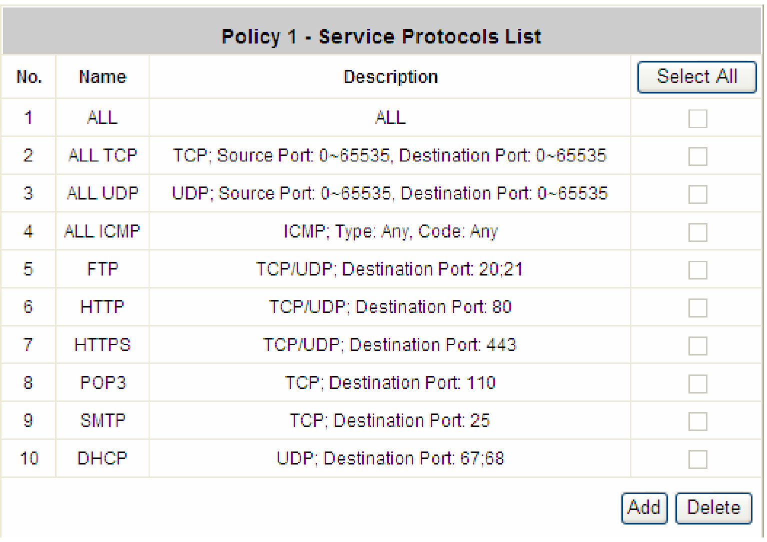


Policy 1 - Firewall Configuration

Predefined and Custom Service Protocols

Firewall Rules

Predefined and Custom Service Protocols: This link leads to a policy's Service List page where the administrator can define a list of services by protocols. The service names defined here forms a choice list for configuring firewall rules.

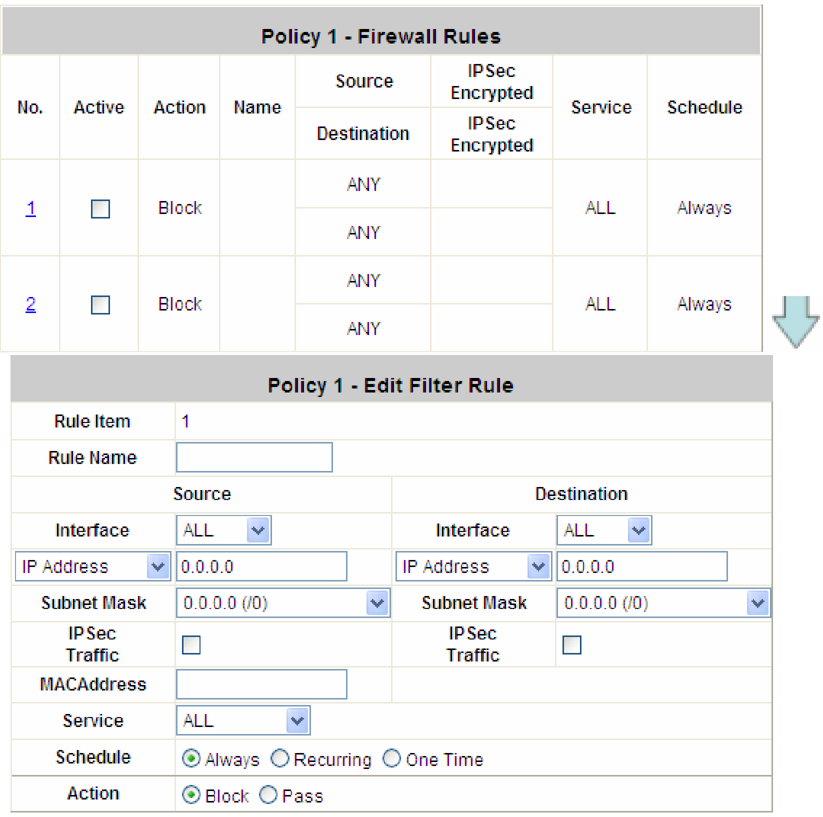


Policy 1 - Service Protocols List

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

Firewall Rules: This link leads to the policy's 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, a Service out of the policy's Service List and a 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.

Attention: *Filter Rule Item 1 is the highest priority, Filter Rule Item 2 is the second priority, and so on.*



Policy 1 - Firewall Rules

No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	□	Block		ANY		ALL	Always
				ANY			
2	□	Block		ANY		ALL	Always
				ANY			

Policy 1 - Edit Filter Rule

Rule Item	1		
Rule Name			
Source		Destination	
Interface	ALL	Interface	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)
IPSec Traffic	□	IPSec Traffic	□
MACAddress			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	● Block ○ Pass		

Rule Item: This is the rule selected.

Rule Name: The rule name can be changed here. The rule name can be set to easily identify, for example: ***"from file server"***, ***"HTTP request"*** or ***"to web"***, etc.

Source/Destination Interface: There are five interfaces to choose: **ALL**, **WAN1**, **WAN2**, **LAN1~LAN4** and **Private LAN**.

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

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

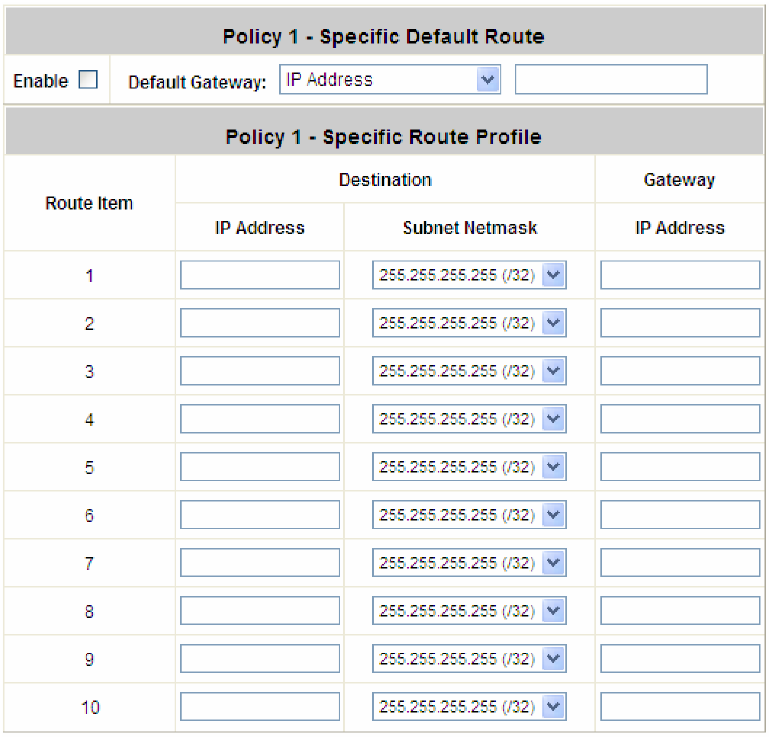
Source/Destination Start/End Port: Enter the range of source and destination ports.

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

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

- **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 default gateway.



Policy 1 - Specific Default Route

Enable □ Default Gateway: IP Address

Policy 1 - Specific Route Profile

Route Item	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)	

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

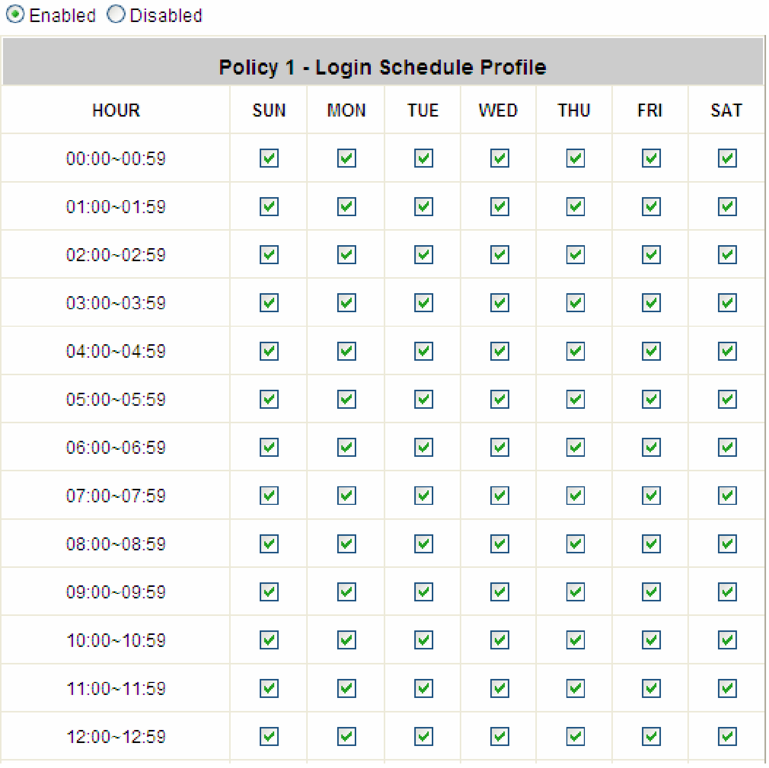
Subnet Netmask: Select a destination subnet netmask of the host or the network.

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

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

- **Schedule Profile**

  The Schedule table in a 7x24 format is used to control the clients' login time. When Schedule is enabled, clients applied polices are only allowed to login the system at the time which is checked in the applied policy.



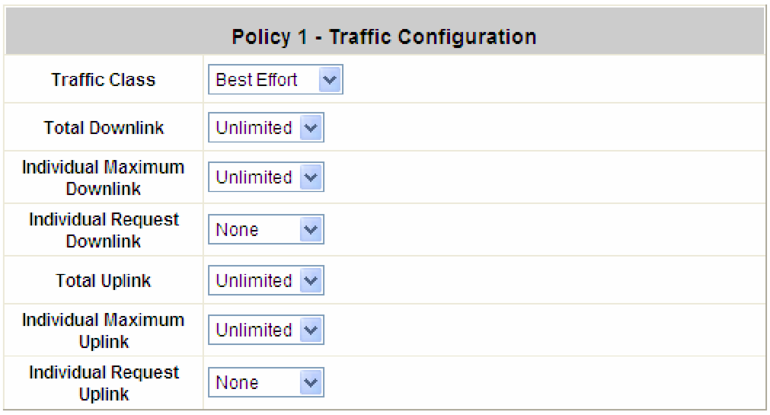
● Enabled ○ Disabled

Policy 1 - Login Schedule Profile

HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
00:00~00:59	☑	☑	☑	☑	☑	☑	☑
01:00~01:59	☑	☑	☑	☑	☑	☑	☑
02:00~02:59	☑	☑	☑	☑	☑	☑	☑
03:00~03:59	☑	☑	☑	☑	☑	☑	☑
04:00~04:59	☑	☑	☑	☑	☑	☑	☑
05:00~05:59	☑	☑	☑	☑	☑	☑	☑
06:00~06:59	☑	☑	☑	☑	☑	☑	☑
07:00~07:59	☑	☑	☑	☑	☑	☑	☑
08:00~08:59	☑	☑	☑	☑	☑	☑	☑
09:00~09:59	☑	☑	☑	☑	☑	☑	☑
10:00~10:59	☑	☑	☑	☑	☑	☑	☑
11:00~11:59	☑	☑	☑	☑	☑	☑	☑
12:00~12:59	☑	☑	☑	☑	☑	☑	☑

- **QoS Profile**

  Click the button of ***Setting*** for **Schedule Profile** to enter the Traffic Configuration list.



Policy 1 - Traffic Configuration

Traffic Class	Best Effort
Total Downlink	Unlimited
Individual Maximum Downlink	Unlimited
Individual Request Downlink	None
Total Uplink	Unlimited
Individual Maximum Uplink	Unlimited
Individual Request Uplink	None

Traffic Class: Each policy can choose its own traffic class. There are four traffic classes: Voice, Video, Best-Effort and Background. Voice and Video will be put into high priority queue. When select Best-Effort or Background, it also can configure the Downlink and Uplink Bandwidth.

Total Downlink: It defines the maximum bandwidth allowed to share by clients within the same policy.

Individual Maximum Downlink: It defines the maximum bandwidth allowed for an individual client; the Individual Maximum Downlink can not exceed the value of Total Downlink.

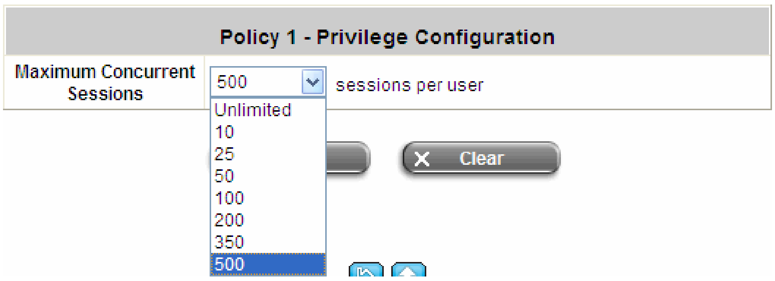
Individual Request Downlink: It defines the guaranteed minimum bandwidth allowed for an individual client; the Individual Request Downlink can not exceed the value of Total Downlink and Individual Maximum Downlink.

Total Uplink: It defines the maximum bandwidth allowed to share by clients within the same policy.

Individual Maximum Uplink: It defines the maximum bandwidth allowed for an individual client; the Individual Maximum Uplink can not exceed the value of Total Uplink.

Individual Request Uplink: It defines the guaranteed minimum bandwidth allowed for an individual client; the Individual Request Uplink can not exceed the value of Total Uplink and Individual Maximum Uplink.

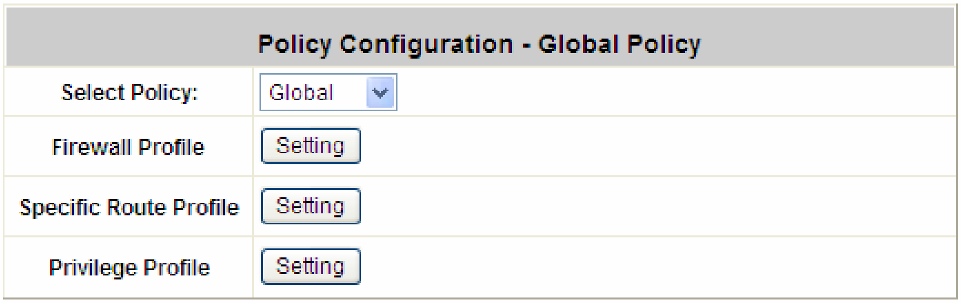
- **Privilege Profile**
  Click the button of ***Setting*** for **Privilege Profile** to enter the Policy Privilege Configuration list.



Policy 1 - Privilege Configuration	
Maximum Concurrent Sessions	500 sessions per user

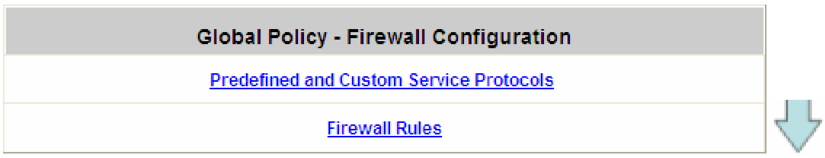
Maximum Concurrent Sessions: The concurrent sessions for each user; it can be restricted by administrator. When a user reaches the session limit, this user will be implicitly suspended from any new connection for a fixed time period.

- **Global Policy**



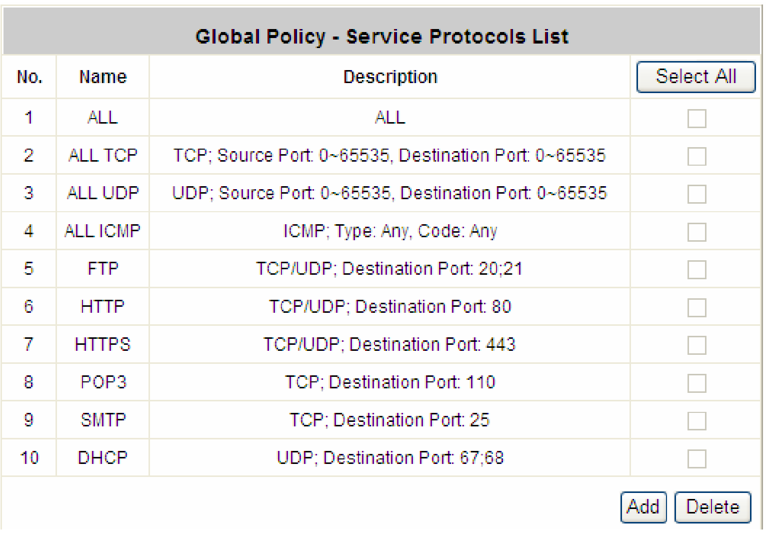
Policy Configuration - Global Policy	
Select Policy:	Global
Firewall Profile	Setting
Specific Route Profile	Setting
Privilege Profile	Setting

- **Select Policy:** Select **Global** to set the **Firewall Profile, Specific Route Profile** and **Privilege Profile**.
- **Firewall Profile:** Click the hyperlink of ***Setting*** for **Firewall Profile**, the Firewall Profiles list will appear. Click the numbers of ***Filter Rule Item*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list. Check **"Active"** to enable that rule.



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

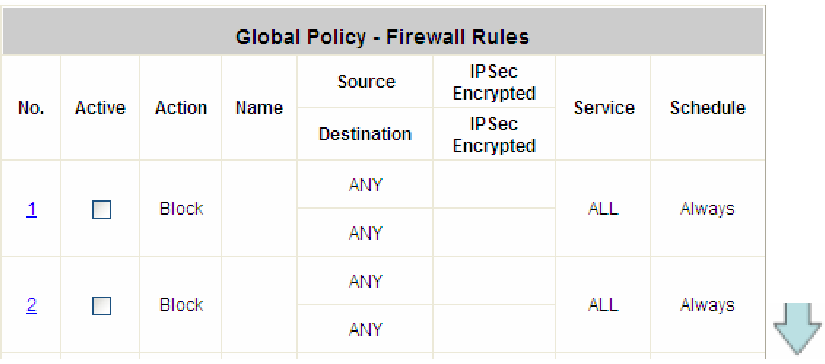
Predefined and Custom Service Protocols: This link leads to a policy's Service List page where the administrator can define a list of services by protocols (TCP/UDP/ICMP/IP). The service names defined here forms a choice list for configuring firewall rules.



Global Policy - Service Protocols List

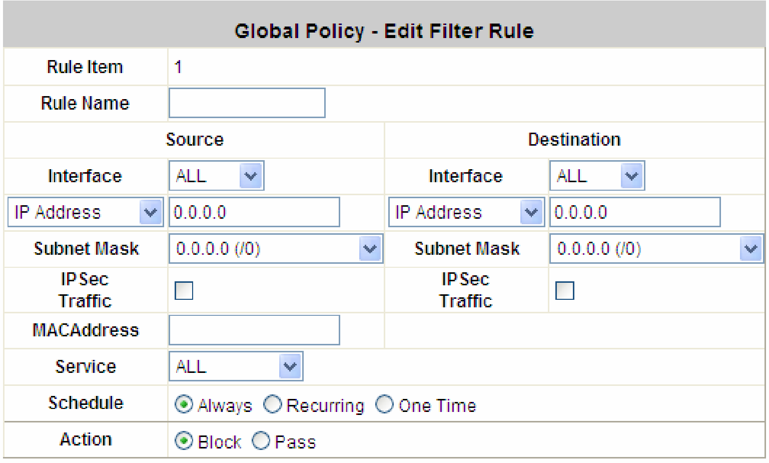
No.	Name	Description	Select All
1	ALL	ALL	☐
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	☐
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	☐
4	ALL ICMP	ICMP; Type: Any, Code: Any	☐
5	FTP	TCP/UDP; Destination Port: 20;21	☐
6	HTTP	TCP/UDP; Destination Port: 80	☐
7	HTTPS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

Firewall Rules: This link leads to the policy's 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, a Service out of the policy's Service List and a 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

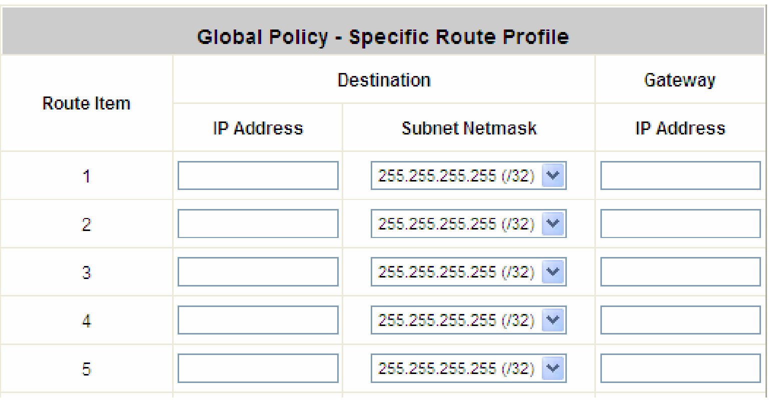
No.	Active	Action	Name	Source Destination	IPSec Encrypted IPSec Encrypted	Service	Schedule
1	□	Block		ANY ANY		ALL	Always
2	□	Block		ANY ANY		ALL	Always



Global Policy - Edit Filter Rule

Rule Item	1		
Rule Name			
Source		Destination	
Interface	ALL	Interface	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)
IPSec Traffic	□	IPSec Traffic	□
MACAddress			
Service	ALL		
Schedule	● Always ○ Recurring ○ One Time		
Action	● Block ○ Pass		

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

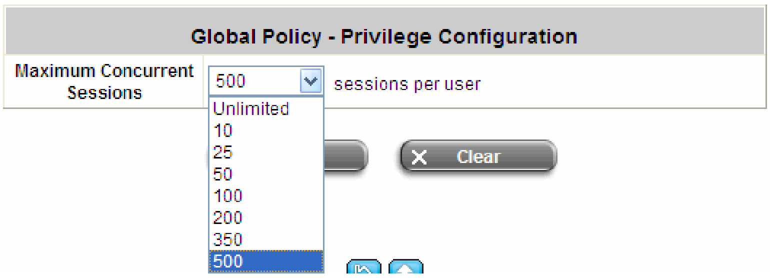


Global Policy - Specific Route Profile

Route Item	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)	

IP Address (Destination): The destination IP address of the host or the network.
Subnet Netmask: Select a destination subnet netmask of the host or the network.
IP Address (Gateway): The IP address of the next router to the destination.

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

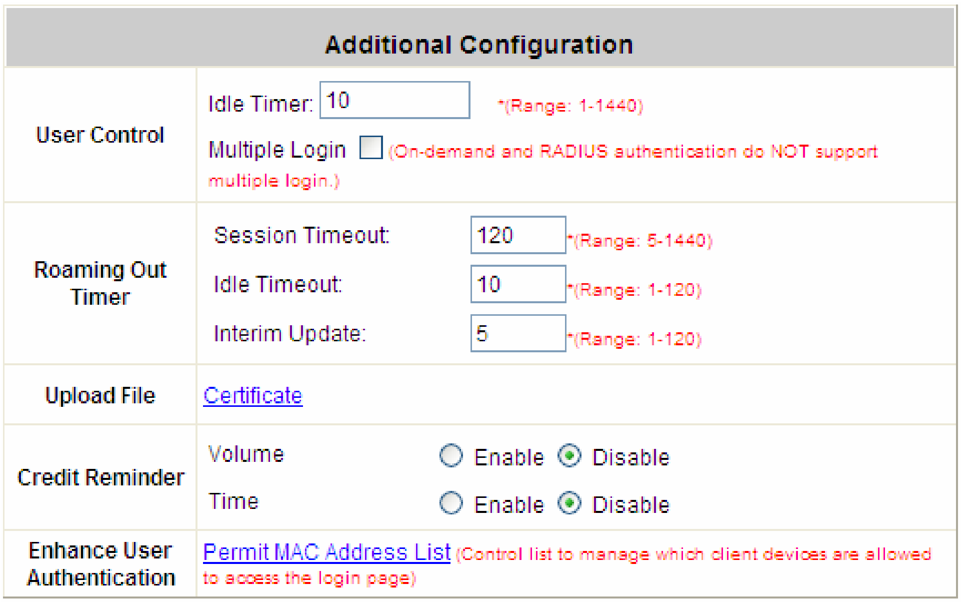


Global Policy - Privilege Configuration

Maximum Concurrent Sessions: 500 sessions per user

Maximum Concurrent Sessions: The concurrent sessions for each user; it can be restricted by administrator. When a user reaches the session limit, this user will be implicitly suspended from any new connection for a fixed time period.

7.2.4 Additional Configuration

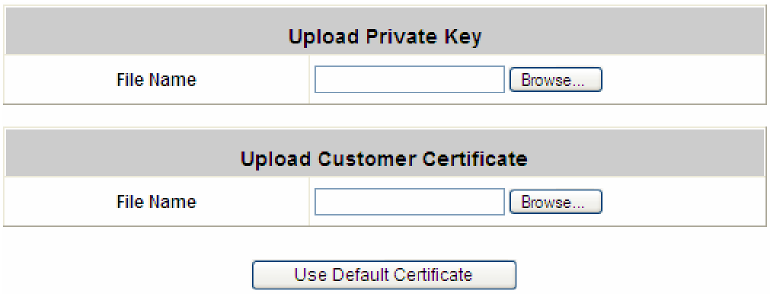


Additional Configuration	
User Control	Idle Timer: 10 *(Range: 1-1440) Multiple Login □ (On-demand and RADIUS authentication do NOT support multiple login.)
Roaming Out Timer	Session Timeout: 120 *(Range: 5-1440) Idle Timeout: 10 *(Range: 1-120) Interim Update: 5 *(Range: 1-120)
Upload File	Certificate
Credit Reminder	Volume ○ Enable ● Disable Time ○ Enable ● Disable
Enhance User Authentication	Permit MAC Address List (Control list to manage which client devices are allowed to access the login page)

- **User Control:** Functions under this section apply to all general users.
  Idle Timer: 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 logout time is 10 minutes.
  Multiple Login: When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS authentication.)

- **Roaming Out Timer:**
  Session Timeout: The time that the user can access the network while roaming. When the time is up, the user will be kicked out automatically.
  Idle Timeout: If a user has idled with no network activities, the system will automatically kick out the user.
  Interim Update: The system will update the users' current status and usage according to this time period.

- **Upload File**
  Certificate: The administrator can upload new private key and customer certification. Click the ***Browse*** button to select the file of a certificate to upload. Click ***Apply*** to complete the upload process.

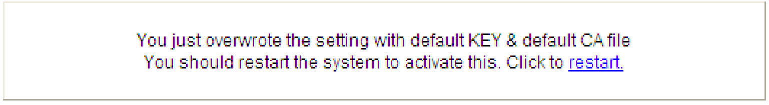


Upload Private Key	
File Name	Browse...

Upload Customer Certificate	
File Name	Browse...

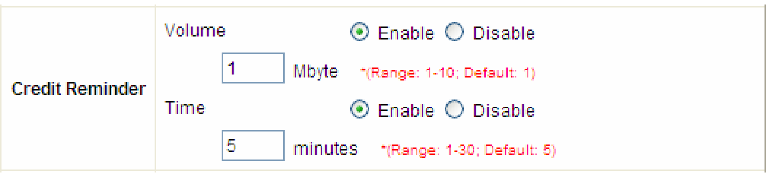
Use Default Certificate

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



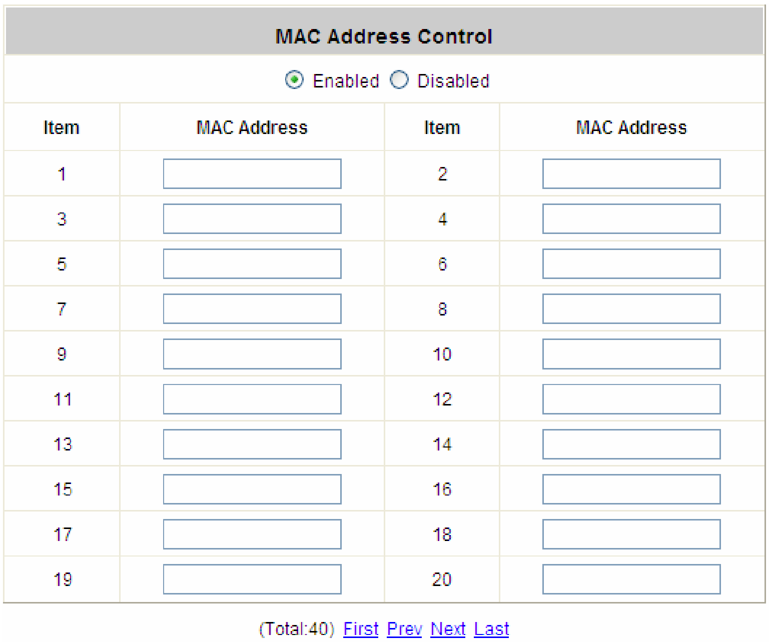
You just overwrote the setting with default KEY & default CA file
You should restart the system to activate this. Click to restart.

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



Credit Reminder	Volume	● Enable ○ Disable
	1 Mbyte	*(Range: 1-10; Default: 1)
	Time	● Enable ○ Disable
	5 minutes	*(Range: 1-30; Default: 5)

- **Enhance User Authentication:** With this function, only the users with their MAC addresses in this list can log into MW-2000S. There are 40 users maximum allowed in this MAC address list. User authentication is still required for these users. Please enter the **Permit MAC Address List** to fill in these MAC addresses, select **Enable**, and then click ***Apply***.



MAC Address Control

● Enabled ○ Disabled

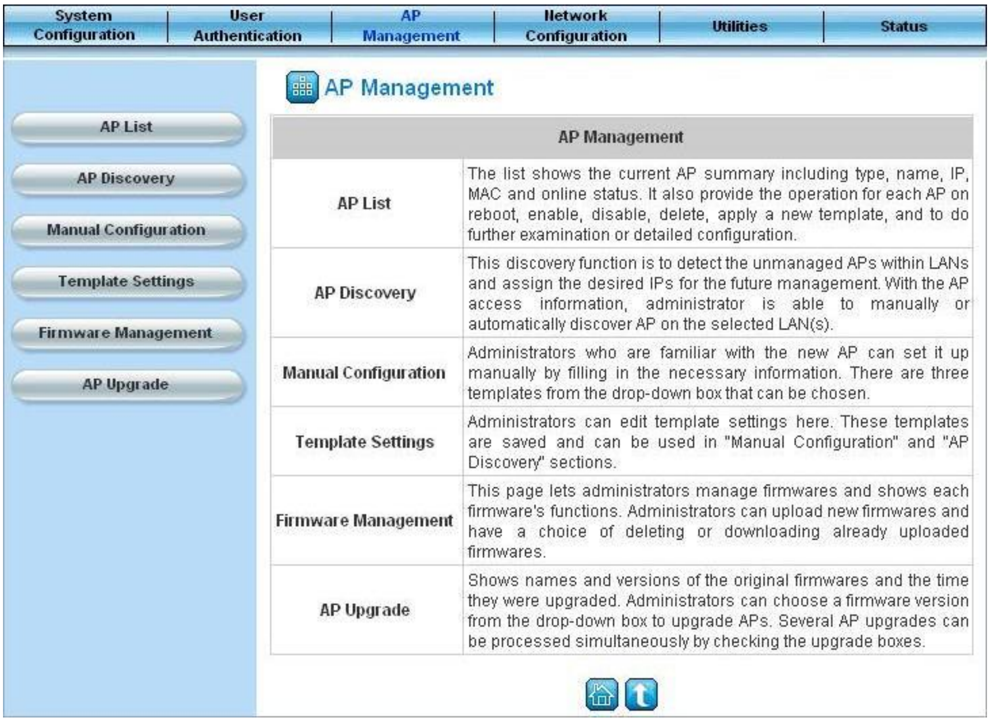
Item	MAC Address	Item	MAC Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

(Total:40) First Prev Next Last

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

7.3 AP Management

MW-2000S supports to manage up to 12 access points (AP), and they can be configured in this section. This section includes the following functions: **AP List**, **AP Discovery**, **Manual Configuration**, **Template Settings**, **Firmware Management** and **AP Upgrade**.

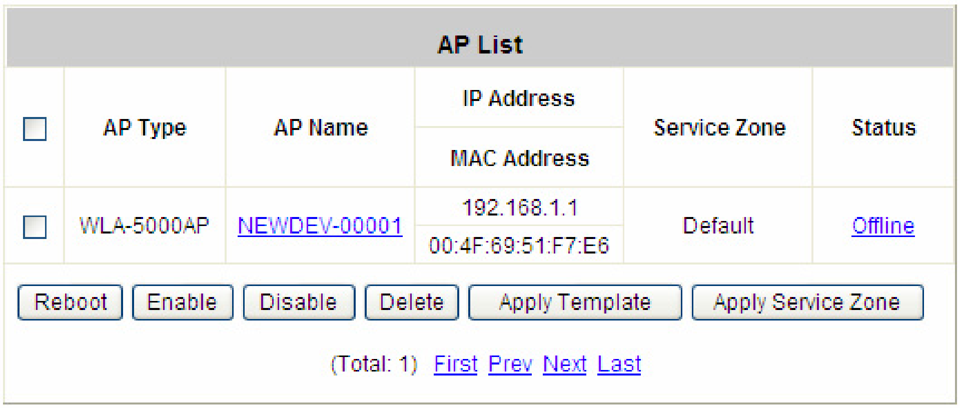


AP Management

AP Management	
AP List	The list shows the current AP summary including type, name, IP, MAC and online status. It also provide the operation for each AP on reboot, enable, disable, delete, apply a new template, and to do further examination or detailed configuration.
AP Discovery	This discovery function is to detect the unmanaged APs within LANs and assign the desired IPs for the future management. With the AP access information, administrator is able to manually or automatically discover AP on the selected LAN(s).
Manual Configuration	Administrators who are familiar with the new AP can set it up manually by filling in the necessary information. There are three templates from the drop-down box that can be chosen.
Template Settings	Administrators can edit template settings here. These templates are saved and can be used in "Manual Configuration" and "AP Discovery" sections.
Firmware Management	This page lets administrators manage firmwares and shows each firmware's functions. Administrators can upload new firmwares and have a choice of deleting or downloading already uploaded firmwares.
AP Upgrade	Shows names and versions of the original firmwares and the time they were upgraded. Administrators can choose a firmware version from the drop-down box to upgrade APs. Several AP upgrades can be processed simultaneously by checking the upgrade boxes.

7.3.1 AP List

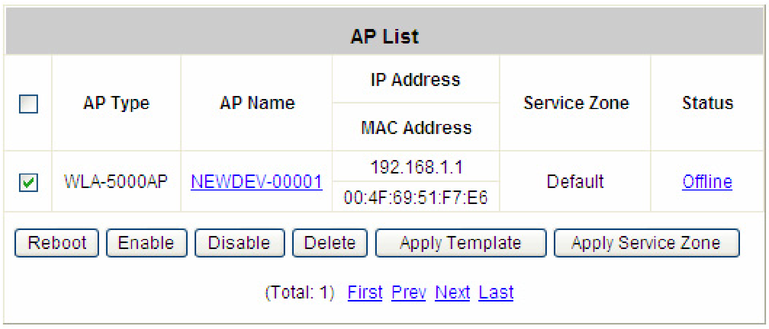
All of the APs under the management of MW-2000S will be shown in the list. The AP can be edited by clicking the hyperlink of ***AP Name*** and the AP status can be got by clicking the hyperlink of ***Status***.



AP List

☐	AP Type	AP Name	IP Address MAC Address	Service Zone	Status
☐	WLA-5000AP	NEWDEV-00001	192.168.1.1 00:4F:69:51:F7:E6	Default	Offline

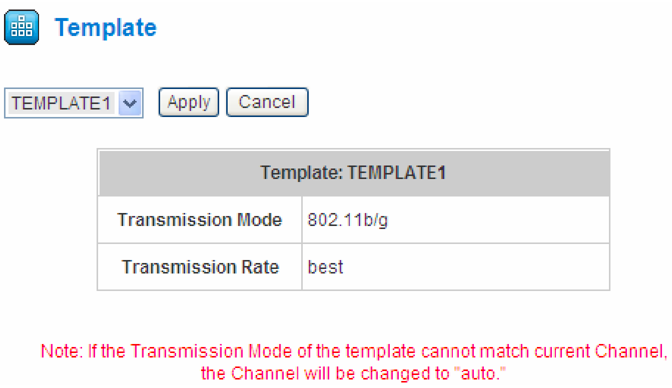
Check any AP and then click the button below to ***Reboot***, ***Enable***, ***Disable*** and ***Delete*** the checked AP if desired.



AP List

☐	AP Type	AP Name	IP Address MAC Address	Service Zone	Status
☑	WLA-5000AP	NEWDEV-00001	192.168.1.1 00:4F:69:51:F7:E6	Default	Offline

Click ***Apply Template*** to select one template to apply to the AP.



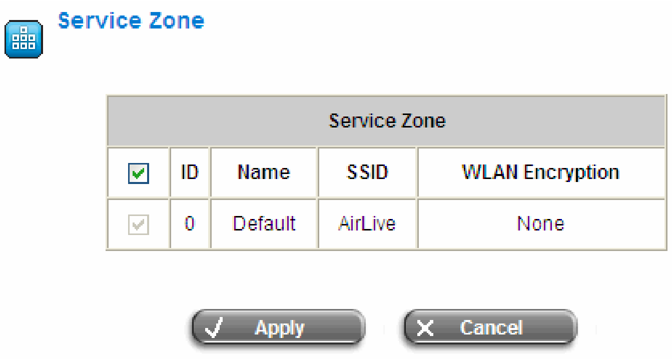
Template

TEMPLATE1

Template: TEMPLATE1	
Transmission Mode	802.11b/g
Transmission Rate	best

Note: If the Transmission Mode of the template cannot match current Channel, the Channel will be changed to "auto."

Click ***Apply Service Zone*** to setup one Service Zone to the AP.

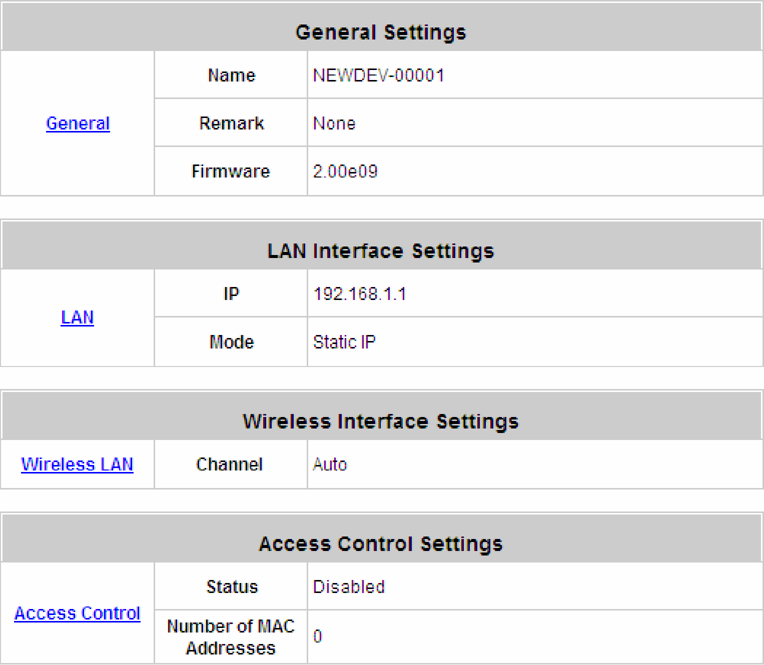


Service Zone

☑	ID	Name	SSID	WLAN Encryption
☑	0	Default	AirLive	None

- **AP Name**

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



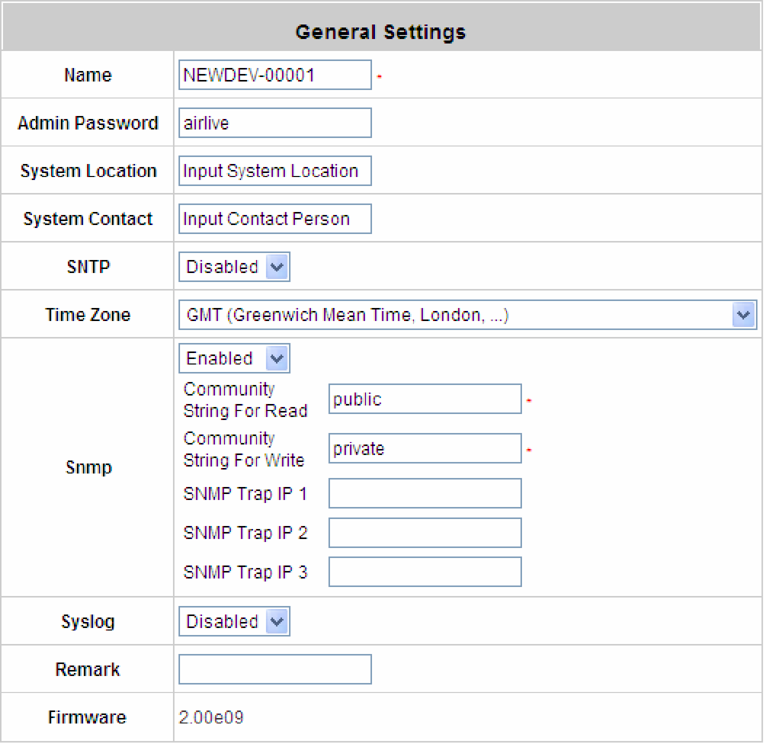
General Settings		
General	Name	NEWDEV-00001
	Remark	None
	Firmware	2.00e09

LAN Interface Settings		
LAN	IP	192.168.1.1
	Mode	Static IP

Wireless Interface Settings		
Wireless LAN	Channel	Auto

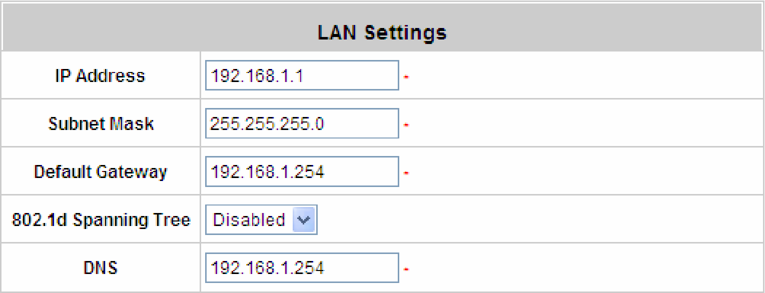
Access Control Settings		
Access Control	Status	Disabled
	Number of MAC Addresses	0

➢ **General Setting:** Click ***Setting*** to enter the **General Setting** interface. Revise the AP **Name**, **Admin Password** and **Remark** if desired. Firmware information can also be observed here.



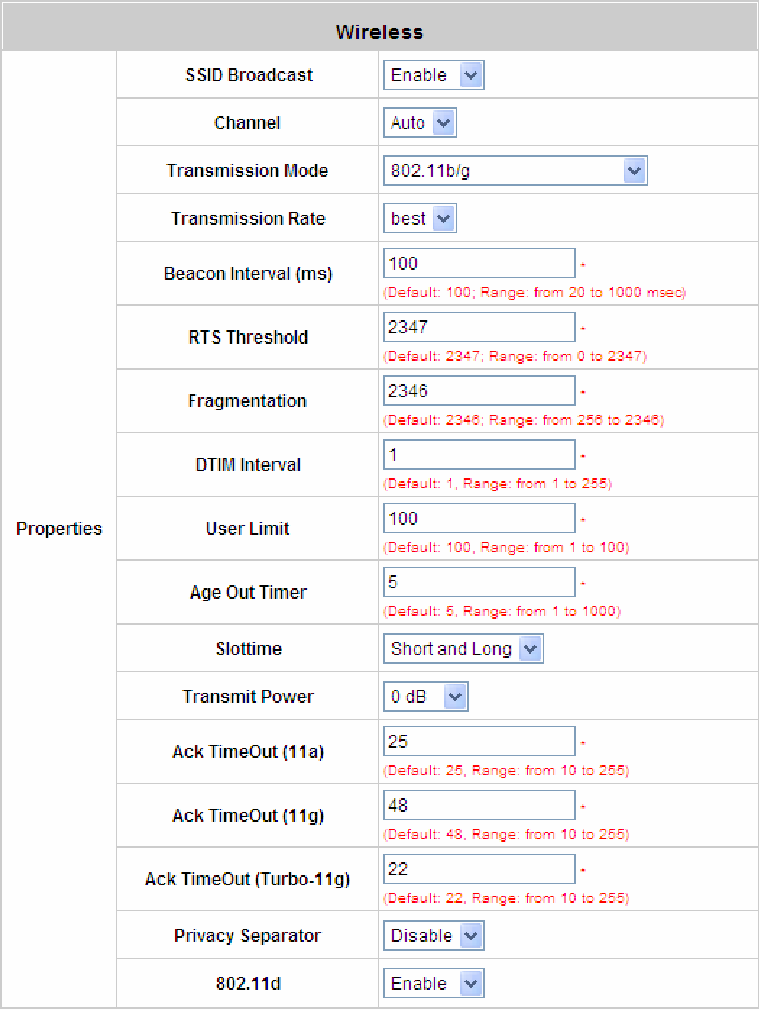
General Settings	
Name	NEWDEV-00001 -
Admin Password	airlive
System Location	Input System Location
System Contact	Input Contact Person
SNTP	Disabled
Time Zone	GMT (Greenwich Mean Time, London, ...)
Snmp	Enabled Community String For Read: public - Community String For Write: private - SNMP Trap IP 1: SNMP Trap IP 2: SNMP Trap IP 3:
Syslog	Disabled
Remark	
Firmware	2.00e09

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



LAN Settings	
IP Address	192.168.1.1 *
Subnet Mask	255.255.255.0 *
Default Gateway	192.168.1.254 *
802.1d Spanning Tree	Disabled
DNS	192.168.1.254 *

- **Wireless LAN:** Click ***Wireless LAN*** to enter the **Wireless** interface. The data of Properties and Security need to be filled.



Wireless		
Properties	SSID Broadcast	Enable
	Channel	Auto
	Transmission Mode	802.11b/g
	Transmission Rate	best
	Beacon Interval (ms)	100 * (Default: 100; Range: from 20 to 1000 msec)
	RTS Threshold	2347 * (Default: 2347; Range: from 0 to 2347)
	Fragmentation	2346 * (Default: 2346; Range: from 256 to 2346)
	DTIM Interval	1 * (Default: 1, Range: from 1 to 255)
	User Limit	100 * (Default: 100, Range: from 1 to 100)
	Age Out Timer	5 * (Default: 5, Range: from 1 to 1000)
	Slottime	Short and Long
	Transmit Power	0 dB
	Ack TimeOut (11a)	25 * (Default: 25, Range: from 10 to 255)
	Ack TimeOut (11g)	48 * (Default: 48, Range: from 10 to 255)
	Ack TimeOut (Turbo-11g)	22 * (Default: 22, Range: from 10 to 255)
	Privacy Separator	Disable
	802.11d	Enable

Properties

- **SSID:** The SSID is the unique name shared among all APs in a wireless network. The SSID must be the same for all APs in the wireless network. It is case sensitive and has a maximum length of 32 bytes.

- **SSID Broadcast:** Select this option to enable the SSID to broadcast in the network. When configuring the network, it's suggested to enable this function but also make sure to disable it when finished. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to an individual's network. With this disabled to increase network security and prevent the SSID from being seen on networked.

- **Channel:** Select the appropriate channel from the list to correspond with the network settings; for example, 1 to 11 channels are suitable for the North America area.

- **Transmission Mode:** There are 3 modes to select from, **802.11b** (2.4G, 1~11Mbps)**, 802.11g** (2.4G, 54Mbps) and **Mix mode** (b and g).

- **Transmission 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 is desired or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.

- **802.11 Protection:** Choose to enable or disable this function from the drop-down box.

- **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:** Enter the desired RTS Threshold value, the range is from 0 to 2347, and the default is 2347.

- **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 transmits between the access point and the wireless network.

- **Inactivity Time:** Enter the desired inactivity time. The range is from 100 to 60480000 msec, and the default is 50000.

- **Preamble Type:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select from 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.

- **Tx Power Level:** Choose the suitable value from the drop-down box.

- **Ack Timeout:** Enter a desired value, the range is from 0 to 255.

- **Watch Dog:** Check to enable or disable this function.

Security: There are four kinds of security type, **WEP**, **WPA**, **WPA2** and **WPA2 MIXED** for selection.

- **Disable:** Choose this type, there is no any encryption used but **802.1x Authentication** and **Authentication Type**. For Authentication Type, choose **Open System**, **Shared Key,** or **Both** according to the settings of the AP and Client. Check **802.1x Authentication** to enable this function and enter the related data, if necessary.

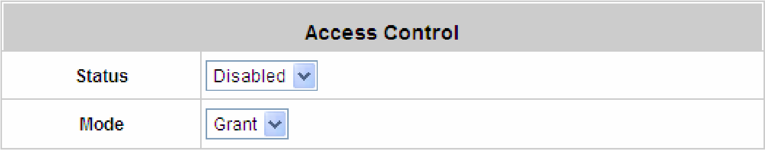
- **WEP:** WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read. Select **Authentication Type** (Open System, Shared Key or Both), **Key Length** (64 bits or 128 bits), **Key Index** (Key1~Key4) and then input the **Key**. Check **802.1x Authentication** to enable this function and enter the related data, if necessary.

- **WPA:** WPA is Wi-Fi's encryption method that protects unauthorized network access by verifying network users through a server. Select 802.1x or WPA-PSK security type and enter the related information below.

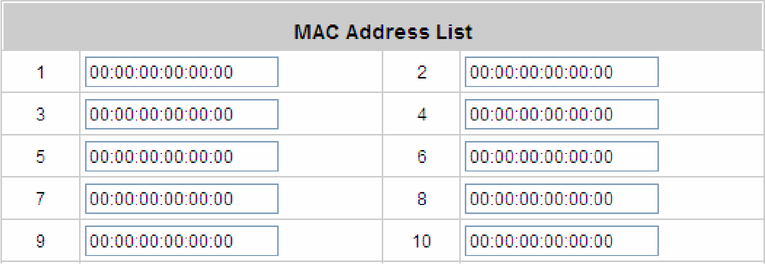
- **WPA2**: Wi-Fi Protected Access version 2. It is similar to security method of WPA to protect Wi-Fi networks but provides stronger data protection and network access control than WPA. Select 802.1x or WPA-PSK security type and enter the related information below. WPA2 only can use AES encryption type.

- **WPA Mixed:** If using TKIP and AES encryption type at the same time is desired, choose this security type. Select 802.1x or WPA-PSK security type and enter the related information below.

- **Access Control:** In this function, when the status is **"Enabled"**, only these clients whose MAC addresses are listed in this list can be allowed to connect to the AP. When **"Disabled"** is selected, all clients can connect to the AP. The default is **Disabled**.



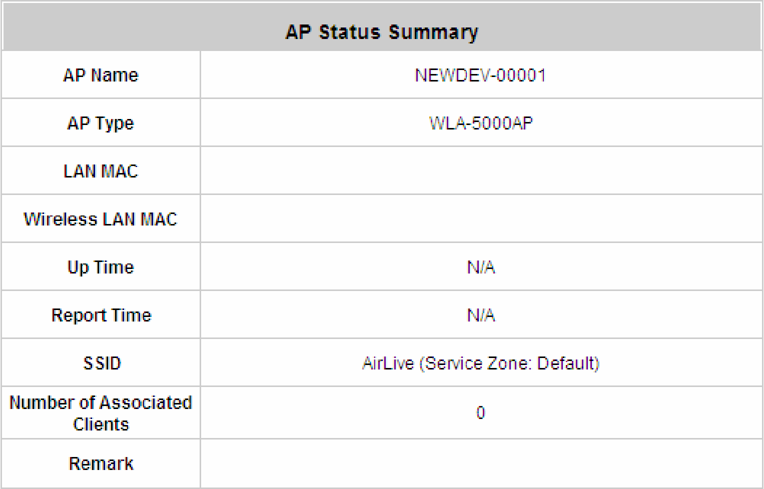
Access Control	
Status	Disabled
Mode	Grant



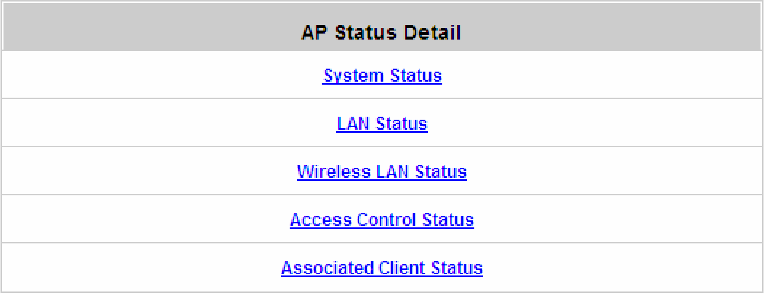
MAC Address List			
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:00
9	00:00:00:00:00:00	10	00:00:00:00:00:00

- **Status**

  After clicking the hyperlink of Status, the basic information of the AP including **AP Name**, **AP Type**, **LAN MAC**, **LAN MAC**, **Wireless LAN MAC**, **Up Time**, **Report Time**, **SSID**, **Number of Associated Clients** and **Remark** can be observed. In the below of the **AP Status Detail**, there are related detailed information, **System Status**, **LAN Status**, **Wireless LAN Status**, **Access Control Status** and **Associated Client Status**.

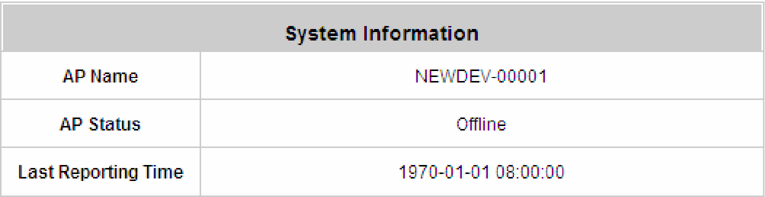


AP Status Summary	
AP Name	NEWDEV-00001
AP Type	WLA-5000AP
LAN MAC	
Wireless LAN MAC	
Up Time	N/A
Report Time	N/A
SSID	AirLive (Service Zone: Default)
Number of Associated Clients	0
Remark	



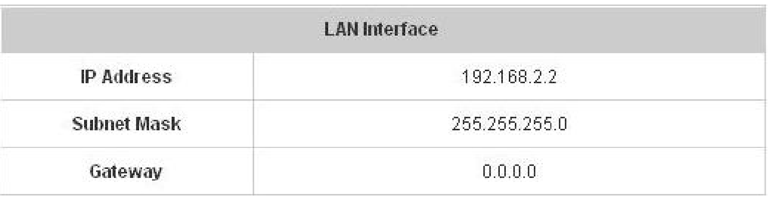
AP Status Detail
System Status
LAN Status
Wireless LAN Status
Access Control Status
Associated Client Status

- **System Status:** The table shows information about **AP Name**, **AP Status** and **Last Reporting Time**.



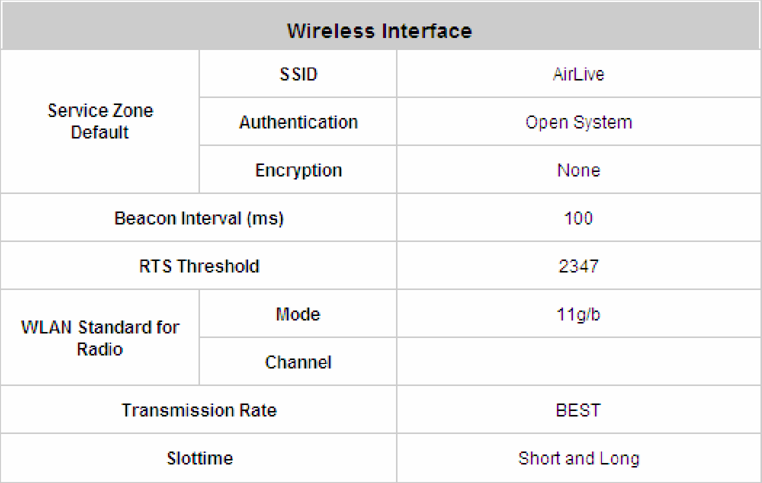
System Information	
AP Name	NEWDEV-00001
AP Status	Offline
Last Reporting Time	1970-01-01 08:00:00

- **LAN Status:** The table shows information about **IP Address**, **Subnet Mask** and **Gateway**.



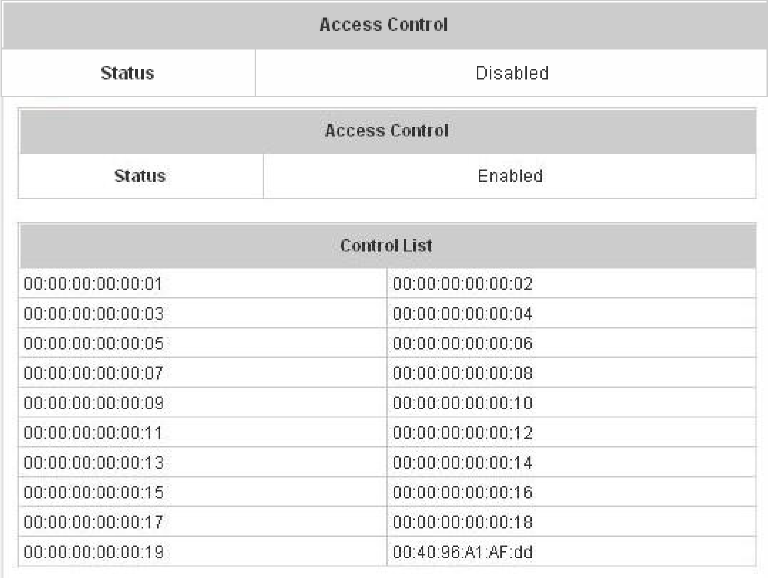
LAN Interface	
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Gateway	0.0.0.0

- **Wireless LAN Status:** The table shows all of the related wireless information.



Wireless Interface		
Service Zone Default	SSID	AirLive
	Authentication	Open System
	Encryption	None
Beacon Interval (ms)		100
RTS Threshold		2347
WLAN Standard for Radio	Mode	11g/b
	Channel	
Transmission Rate		BEST
Slottime		Short and Long

- **Access Control Status:** The table shows the status of MAC of clients under the control of the AP.

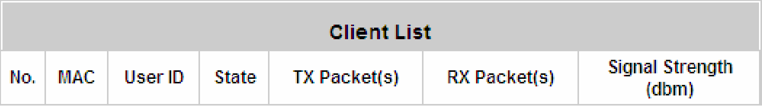


Access Control	
Status	Disabled

Access Control	
Status	Enabled

Control List	
00:00:00:00:00:01	00:00:00:00:00:02
00:00:00:00:00:03	00:00:00:00:00:04
00:00:00:00:00:05	00:00:00:00:00:06
00:00:00:00:00:07	00:00:00:00:00:08
00:00:00:00:00:09	00:00:00:00:00:10
00:00:00:00:00:11	00:00:00:00:00:12
00:00:00:00:00:13	00:00:00:00:00:14
00:00:00:00:00:15	00:00:00:00:00:16
00:00:00:00:00:17	00:00:00:00:00:18
00:00:00:00:00:19	00:40:96:A1:AF:dd

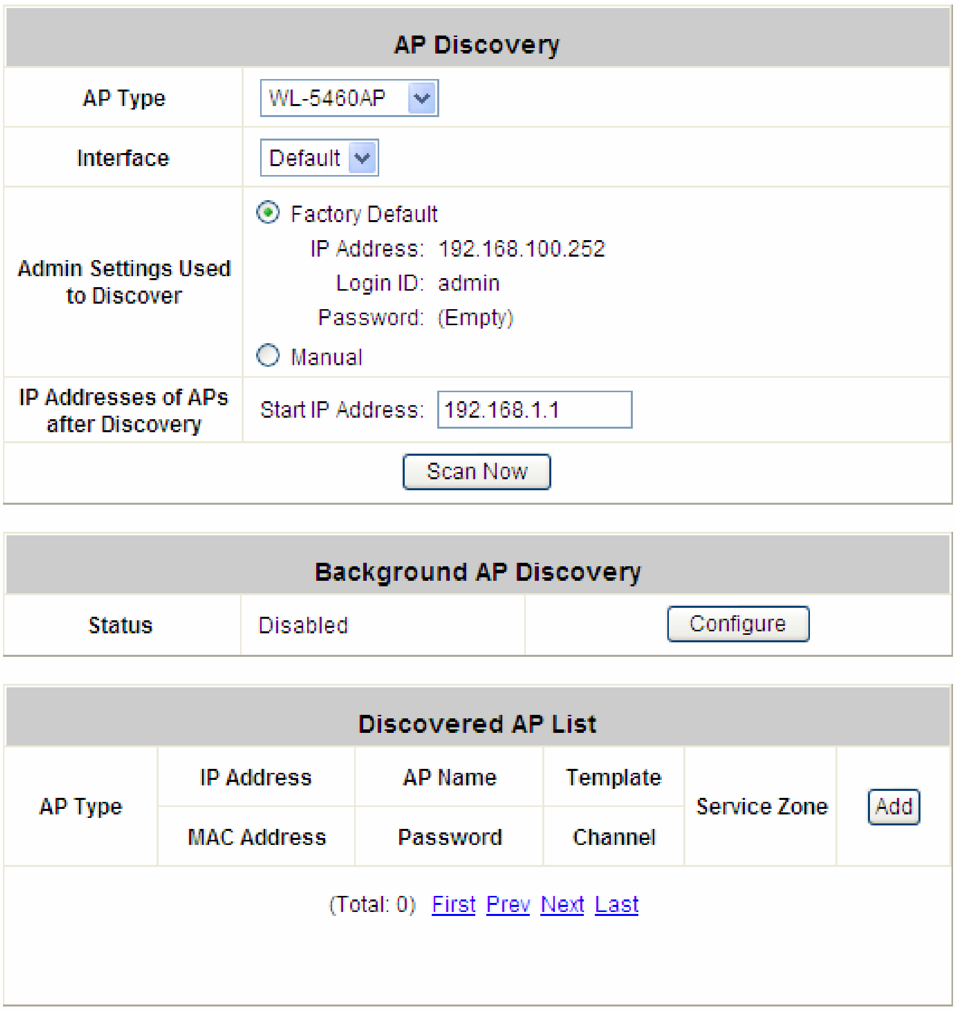
- **Associated Client Status:** The table shows the clients connecting to the AP and the related information of the client.



Client List						
No.	MAC	User ID	State	TX Packet(s)	RX Packet(s)	Signal Strength (dbm)

7.3.2 AP Discovery

Use this function to detect and manage all of the APs in the network segments.



AP Discovery

AP Type	WL-5460AP
Interface	Default
Admin Settings Used to Discover	● Factory Default IP Address: 192.168.100.252 Login ID: admin Password: (Empty) ○ Manual
IP Addresses of APs after Discovery	Start IP Address: 192.168.1.1

Background AP Discovery

Status	Disabled	Configure

Discovered AP List

AP Type	IP Address MAC Address	AP Name Password	Template Channel	Service Zone	Add

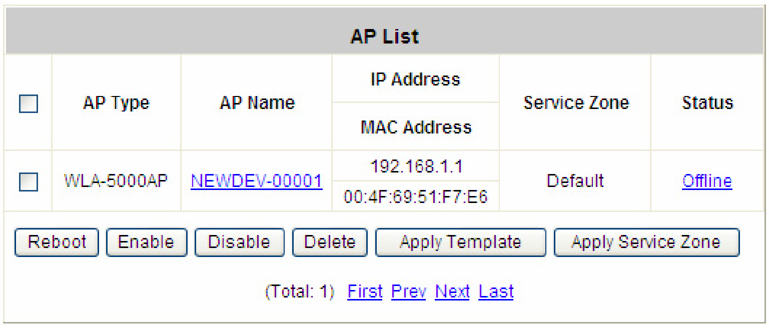
(Total: 0) First Prev Next Last

- To discover AP manually, please fill in the required data.
  - **Interface:** Check **Private LAN** or/and **LAN1~4** and enter the **Base IP** and **Pool Size** (the discovered APs will be configured to use IP address among the pool).
  - **AP Access:** Input the **IP Address Range** (the default is 192.168.2.1/192.168.2.1), **ID** (the default is admin) and **Password** (the default is 1234) of the AP.

  Then click the ***Discover*** 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 on Base IP or Pool Size and then click ***Discover*** again. Input the desired name and password for the AP. Select one template, and then click ***Add*** to add it under the managed list. (About the template, please see 5.3.4 Template).

  When the matched AP is discovered, it will show up in the list below and be given a new IP address set here (ex: 192.168.2.2). Check the **Add** box to add the AP and it will be listed to the AP list. When an AP is added, its MAC address will be automatically recorded into MAC Privilege List (please see 5.4.2 Privilege List) so its management page can be accessed.

  Click Configuring to go on the related configuration. For the details, please refer to **5.3.1 AP List**.

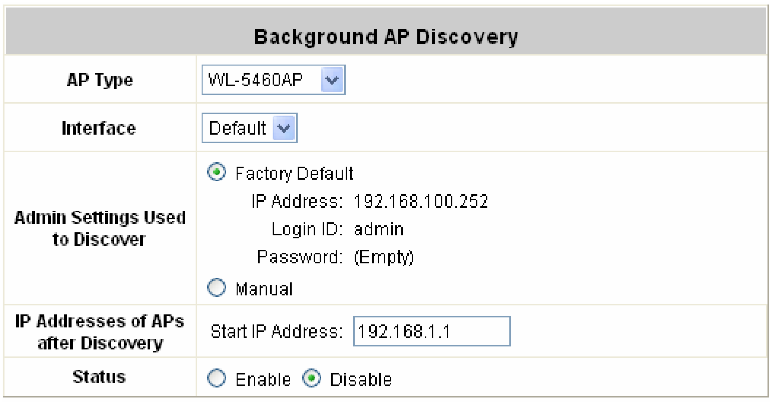


AP List

□	AP Type	AP Name	IP Address MAC Address	Service Zone	Status
□	WLA-5000AP	NEWDEV-00001	192.168.1.1 00:4F:69:51:F7:E6	Default	Offline

(Total: 1) First Prev Next Last

- **Auto-Discover:** Click ***Configure*** to enter Auto-Discovery interface to go on related configuration.



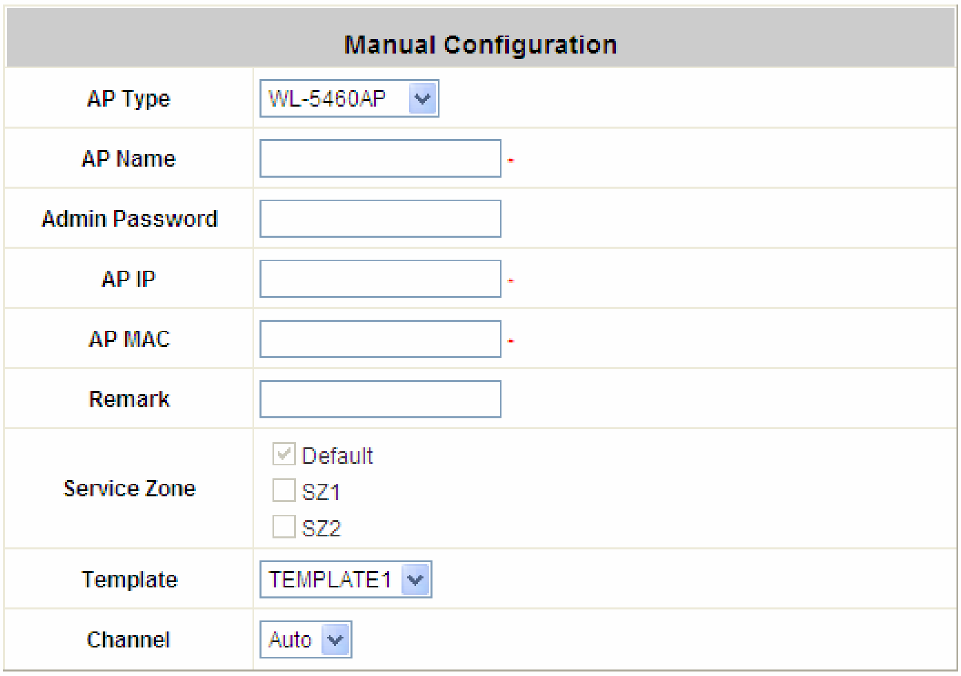
Background AP Discovery

AP Type	WL-5460AP
Interface	Default
Admin Settings Used to Discover	● Factory Default IP Address: 192.168.100.252 Login ID: admin Password: (Empty) ○ Manual
IP Addresses of APs after Discovery	Start IP Address: 192.168.1.1
Status	○ Enable ● Disable

The **Interface** and **AP Access** configuration is the same as the settings mentioned above. When **Auto-Discovery Status** 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 IP pool set within the interfaces and applied with the selected template.

7.3.3 Manual Configuration

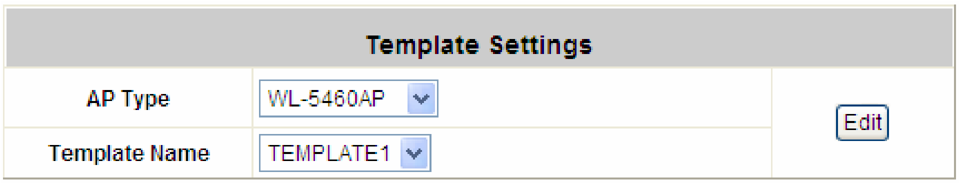
The AP also can be added manually even though when it is offline. Input the related data of the AP and select a Template. After clicking ***Add***, the AP will be added to the managed list.



Manual Configuration	
AP Type	WL-5460AP
AP Name	*
Admin Password	
AP IP	*
AP MAC	*
Remark	
Service Zone	☑ Default ☐ SZ1 ☐ SZ2
Template	TEMPLATE1
Channel	Auto

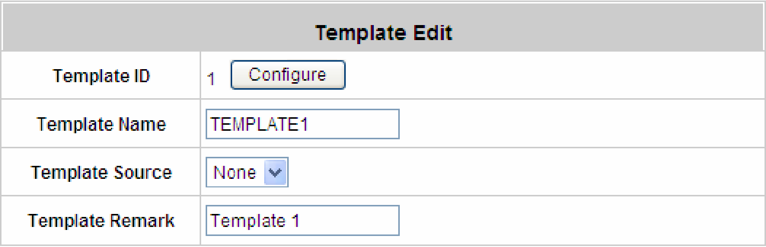
7.3.4 Template Settings

Template is a model that can be copied to every AP and not necessary to configure the AP individually. There are three templates provided. Click ***Edit*** to go on configuration.



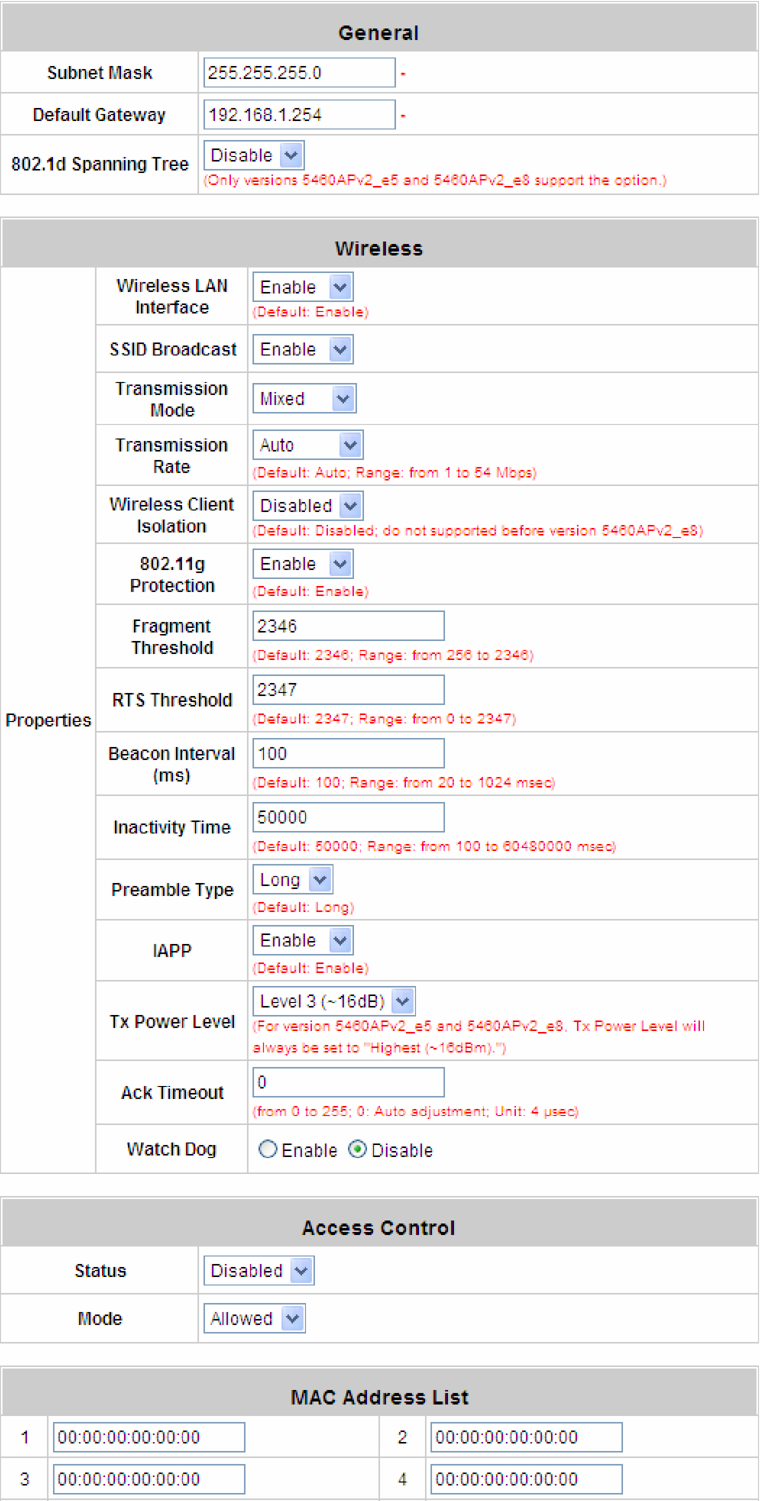
Template Settings		
AP Type	WL-5460AP	Edit
Template Name	TEMPLATE1	

Before configure the template, copy the configuration mode of an AP to the template by selecting 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 **Template Name** and **Template Remark** and click the button of ***Configure*** to go on configuration.



Template Edit	
Template ID	1 Configure
Template Name	TEMPLATE1
Template Source	None
Template Remark	Template 1

After entering the interface, revise the configuration for demand and change administrator's password if desired. About other function settings, please refer to **5.3.1 AP List**.



General	
Subnet Mask	255.255.255.0 *
Default Gateway	192.168.1.254 *
802.1d Spanning Tree	Disable (Only versions 5460APv2_e5 and 5460APv2_e8 support the option.)

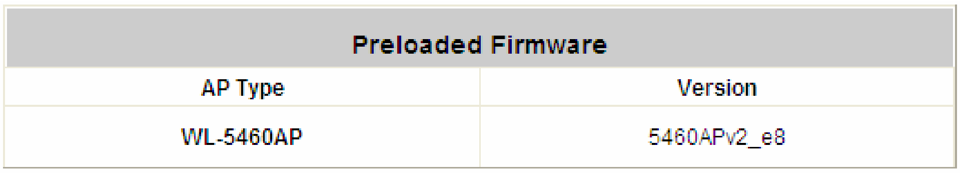
Wireless		
Properties	Wireless LAN Interface	Enable (Default: Enable)
	SSID Broadcast	Enable
	Transmission Mode	Mixed
	Transmission Rate	Auto (Default: Auto; Range: from 1 to 54 Mbps)
	Wireless Client Isolation	Disabled (Default: Disabled; do not supported before version 5460APv2_e8)
	802.11g Protection	Enable (Default: Enable)
	Fragment Threshold	2346 (Default: 2346; Range: from 256 to 2346)
	RTS Threshold	2347 (Default: 2347; Range: from 0 to 2347)
	Beacon Interval (ms)	100 (Default: 100; Range: from 20 to 1024 msec)
	Inactivity Time	50000 (Default: 50000; Range: from 100 to 60480000 msec)
	Preamble Type	Long (Default: Long)
	IAPP	Enable (Default: Enable)
	Tx Power Level	Level 3 (~16dB) (For version 5460APv2_e5 and 5460APv2_e8, Tx Power Level will always be set to "Highest (~16dBm).")
	Ack Timeout	0 (from 0 to 255; 0: Auto adjustment; Unit: 4 µsec)
	Watch Dog	○ Enable ● Disable

Access Control	
Status	Disabled
Mode	Allowed

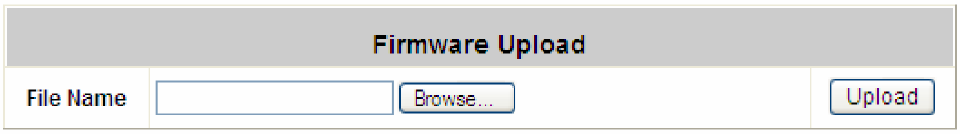
MAC Address List			
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00

7.3.5 Firmware Management

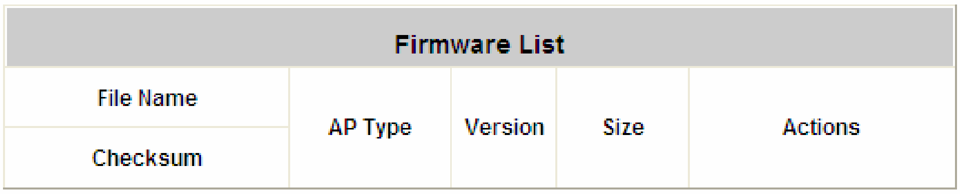
Here AP's firmware can be uploaded and the present firmware can be downloaded deleted.



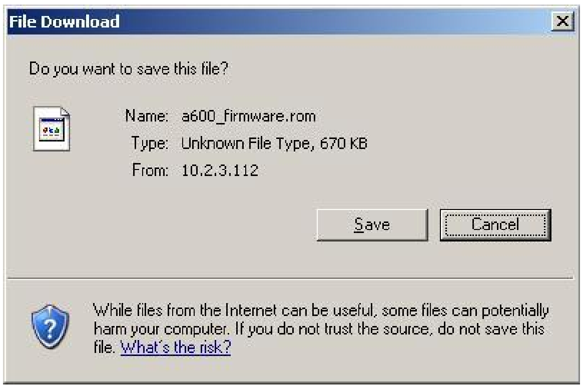
Preloaded Firmware	
AP Type	Version
WL-5460AP	5460APv2_e8



Firmware Upload		
File Name	Browse...	Upload



Firmware List				
File Name Checksum	AP Type	Version	Size	Actions



File Download

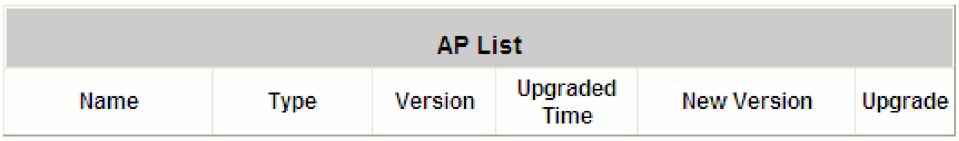
Do you want to save this file?

Name: a600_firmware.rom
Type: Unknown File Type, 670 KB
From: 10.2.3.112

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

7.3.6 AP Upgrade

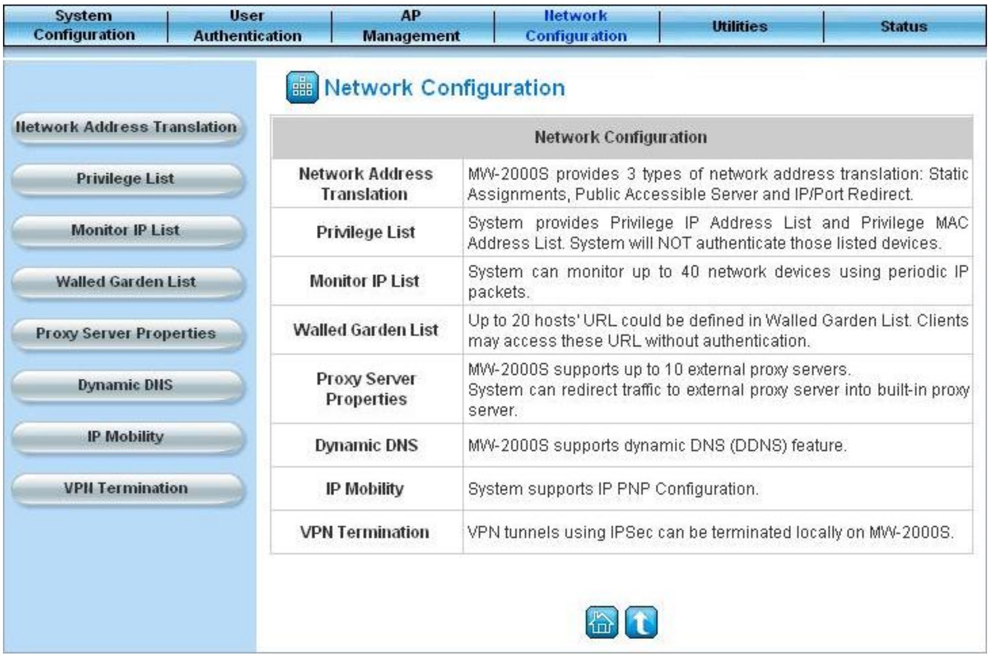
Check the APs which need to be upgraded and select the upgrade version of firmware, and click ***Apply*** to upgrade firmware.



AP List					
Name	Type	Version	Upgraded Time	New Version	Upgrade

7.4 Network Configuration

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

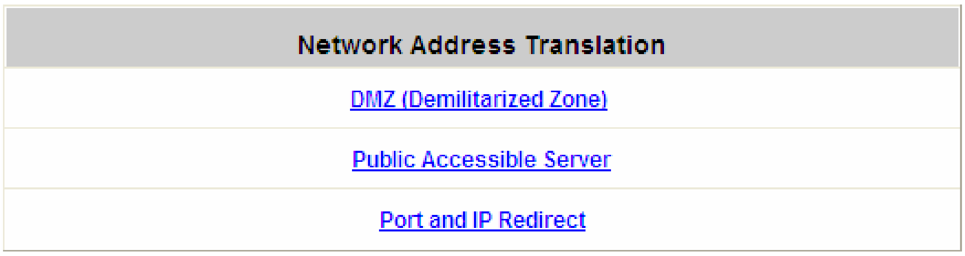


Network Configuration

Network Configuration	
Network Address Translation	MW-2000S provides 3 types of network address translation: Static Assignments, Public Accessible Server and IP/Port Redirect.
Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices.
Monitor IP List	System can monitor up to 40 network devices using periodic IP packets.
Walled Garden List	Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
Proxy Server Properties	MW-2000S supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS	MW-2000S supports dynamic DNS (DDNS) feature.
IP Mobility	System supports IP PNP Configuration.
VPN Termination	VPN tunnels using IPSec can be terminated locally on MW-2000S.

7.4.1 Network Address Translation

There are three parts, **Demilitarized Zone, Public Accessible Server** and **Port and Redirect**, that can be set.



Network Address Translation

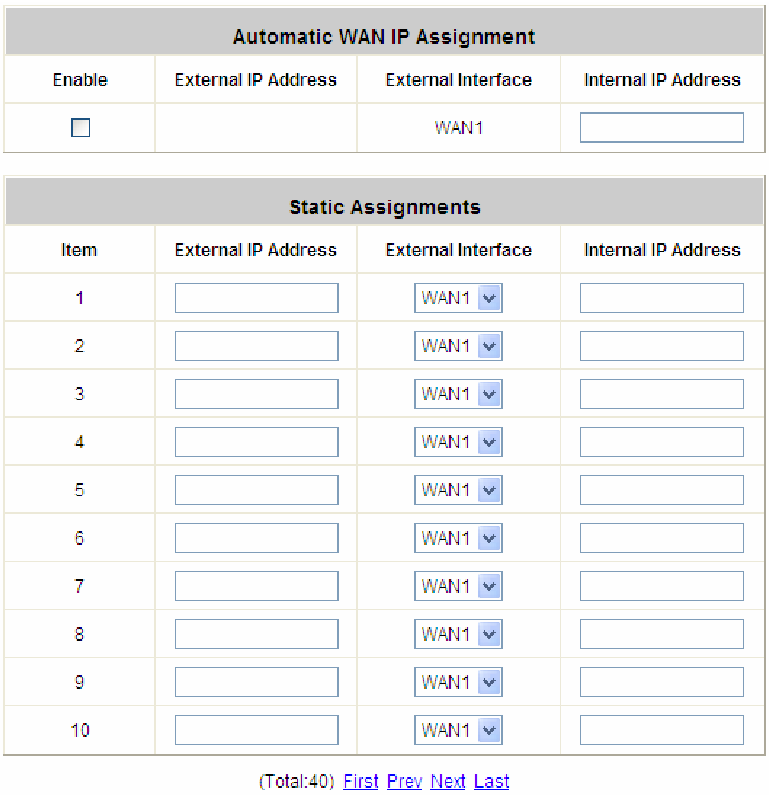
DMZ (Demilitarized Zone)

Public Accessible Server

Port and IP Redirect

- **DMZ**

  DMZ allows administrators to define mandatory external to internal IP mapping, hence a user on WAN side network can access the private machine via the external IP (similar to DMZ usage in firewall product). There are 40 sets of static **Internal IP Address** and **External IP Address** available. If a host needs a static IP address to access the network through WAN port, set a static IP for the host. These settings will become effective immediately after clicking the ***Apply*** button.



Automatic WAN IP Assignment

Enable	External IP Address	External Interface	Internal IP Address
□		WAN1	

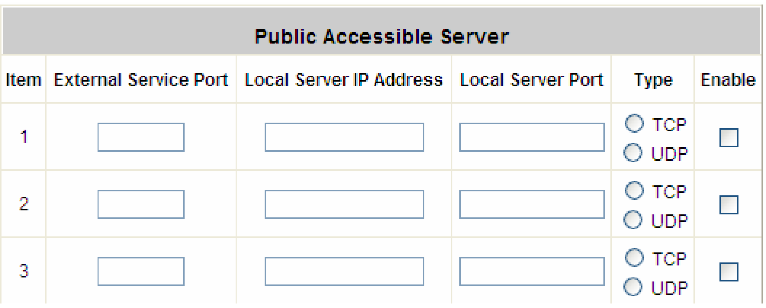
Static Assignments

Item	External IP Address	External Interface	Internal IP Address
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

- **Public Accessible Server**

  This function allows the administrator to set 40 virtual servers at most, so that the computers not belonging to the managed network can access the servers in the managed network via WAN port IP of MW-2000S. Please enter the **"External Service Port"**, **"Local Server IP Address"** and **"Local Server Port"**. According to the different services provided, the network service can use the **TCP** protocol or the **UDP** protocol. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the ***Apply*** button.

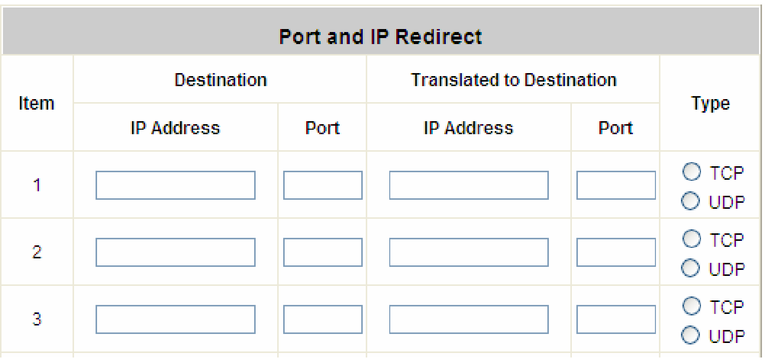


Public Accessible Server

Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				○ TCP ○ UDP	□
2				○ TCP ○ UDP	□
3				○ TCP ○ UDP	□

- **Port and IP Redirect**

  This function allows the administrator to set 40 sets of the IP addresses maximum 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**. According to the different services provided, choose the **"TCP"** protocol or the **"UDP"** protocol. These settings will become effective immediately after clicking ***Apply***.

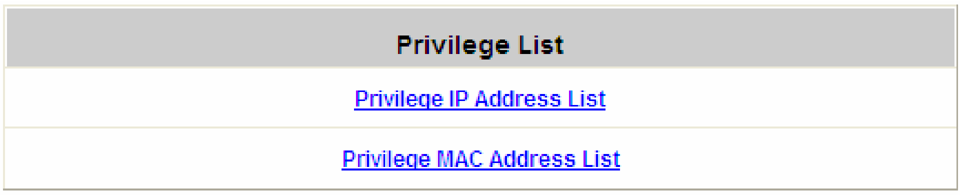


Port and IP Redirect

Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1					○ TCP ○ UDP
2					○ TCP ○ UDP
3					○ TCP ○ UDP

7.4.2 Privilege List

There are two parts, **Privilege IP Address List** and **Privilege MAC Address List** that can be set.



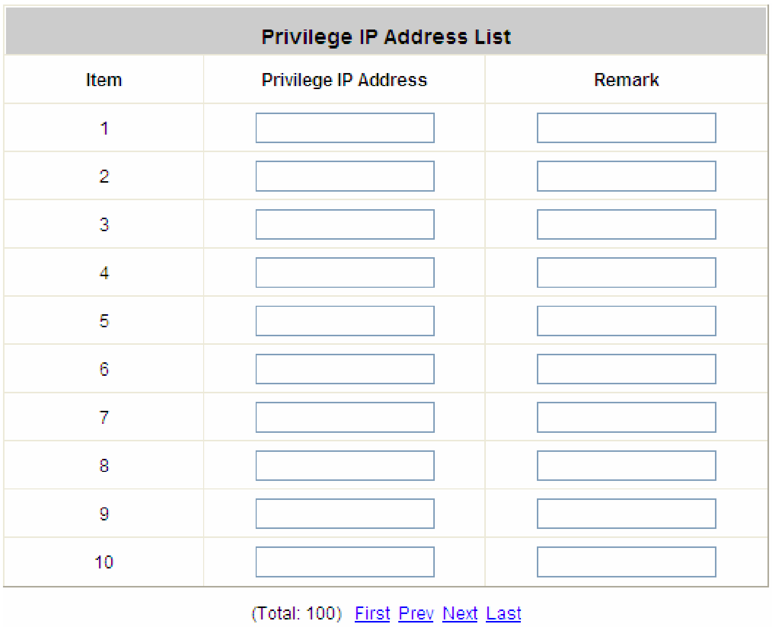
Privilege List

Privilege IP Address List

Privilege MAC Address List

- **Privilege IP Address List**

  If there are some workstations belonging to the managed server that need to access the network without getting authenticated, enter the IP addresses of these workstations in this list. The **"Remark"** blank is not necessary to be filled in but is useful in record-keeping. MW-2000S allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking ***Apply***.



Privilege IP Address List

Item	Privilege IP Address	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

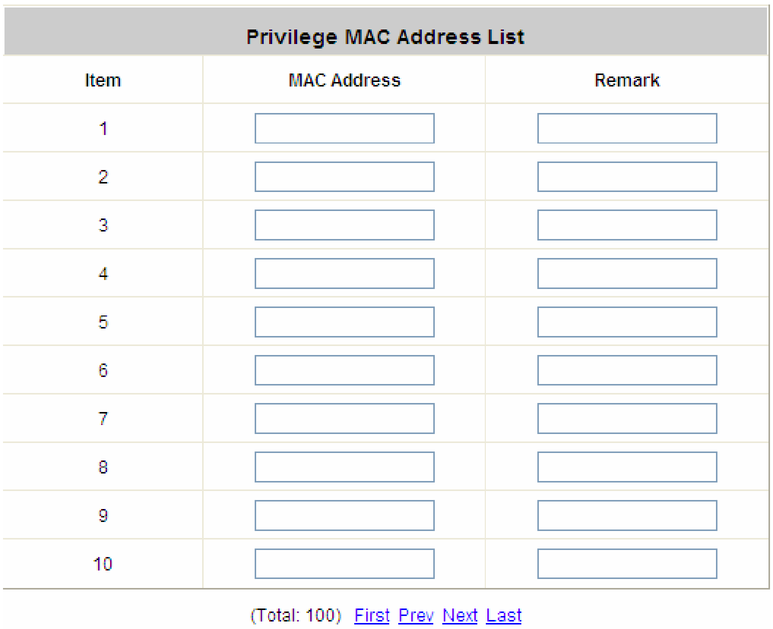
(Total: 100) First Prev Next Last

Warning: *Permitting specific IP addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.*

- **Privilege MAC Address List**

  In addition to the IP address, the MAC address of the workstations that need to access the network without getting authenticated can also be set in this list. MW-2000S allows 100 privilege MAC addresses at most.

  It is possible to manually create the list by entering the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as entering the remark (not required). These settings will become effective immediately after clicking ***Apply***.



Privilege MAC Address List

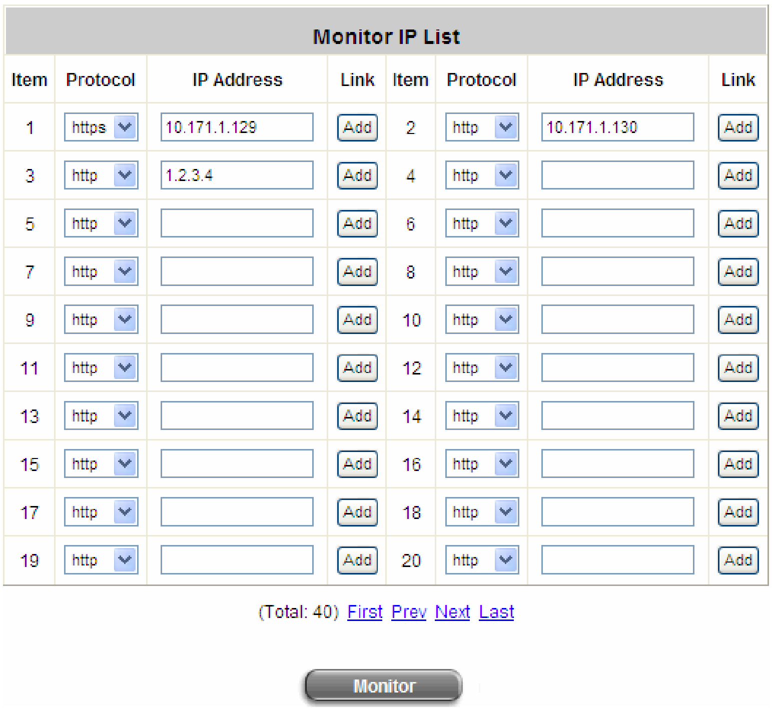
Item	MAC Address	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(Total: 100) First Prev Next Last

Warning: *Permitting specific MAC addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.*

7.4.3 Monitor IP List

MW-2000S 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 related information, click ***Apply*** and these settings will become effective immediately. Click ***Monitor*** to check the current status of all the monitored IPs. Green light means online and red light means offline. The system provides 40 monitor IP address fields on the **"Monitor IP List"**.



Monitor IP List

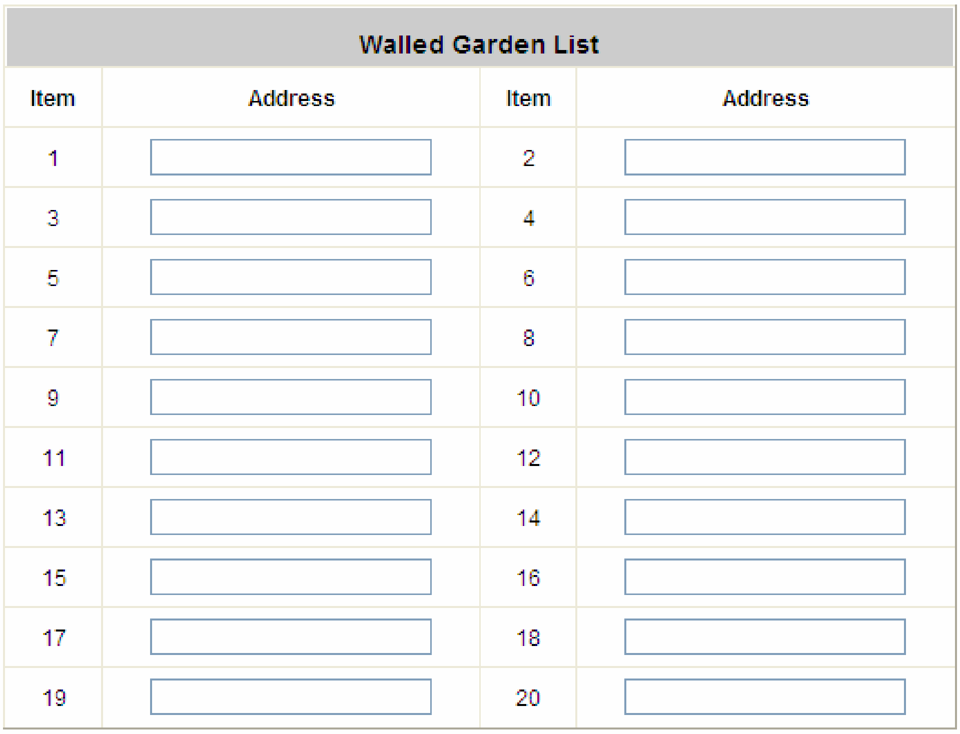
Item	Protocol	IP Address	Link	Item	Protocol	IP Address	Link
1	https	10.171.1.129	Add	2	http	10.171.1.130	Add
3	http	1.2.3.4	Add	4	http		Add
5	http		Add	6	http		Add
7	http		Add	8	http		Add
9	http		Add	10	http		Add
11	http		Add	12	http		Add
13	http		Add	14	http		Add
15	http		Add	16	http		Add
17	http		Add	18	http		Add
19	http		Add	20	http		Add

(Total: 40) First Prev Next Last

On each monitored item with a WEB server running, administrators may add a link for the easy access by selecting a protocol, http or https, and click the ***Add*** button. After clicking ***Add*** button, the IP address will become a hyperlink, and administrators can easily access the host by clicking the hyperlink remotely. Click the ***Del*** button to remove the setting.

7.4.4 Walled Garden List

This function provides some free services to the users to access websites listed here before login to the network and without being authenticated. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Enter the website **IP Address** or **Domain Name** in the list and these settings will become effective immediately after clicking ***Apply***.



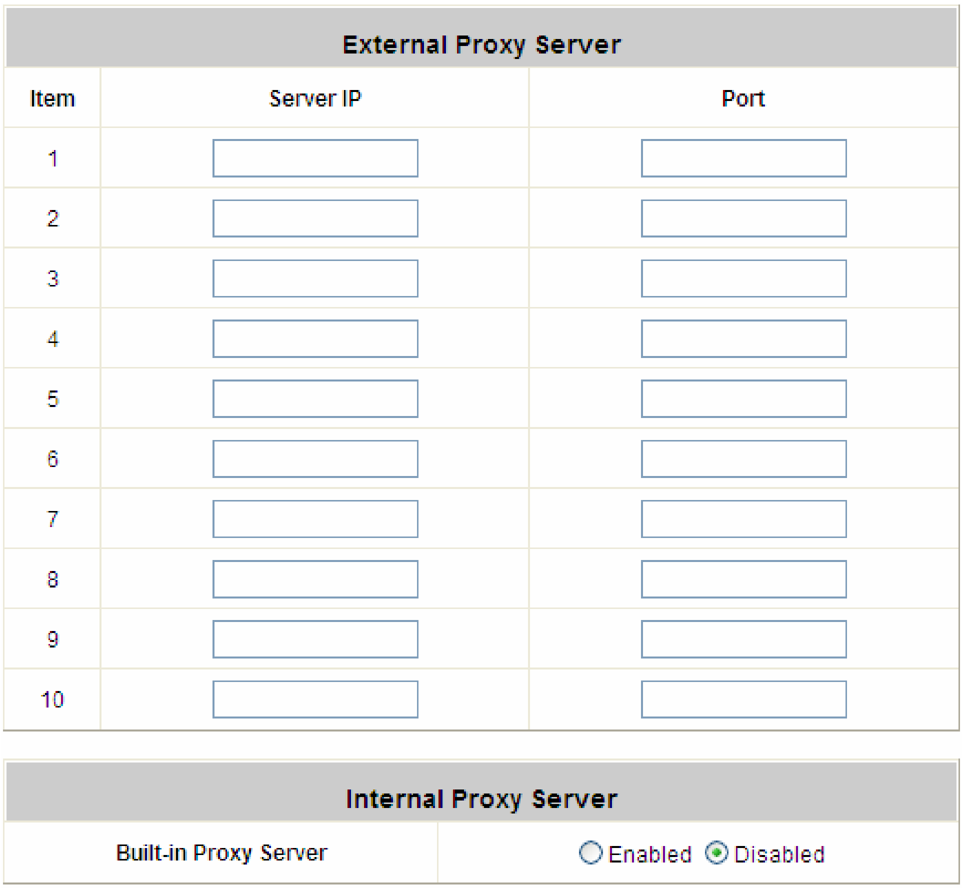
Walled Garden List

Item	Address	Item	Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

Caution: To use the domain name, the MW-2000S has to connect to DNS server first or this function will not work.

7.4.5 Proxy Server Properties

MW-2000S supports Internal Proxy Server and External Proxy Server functions.



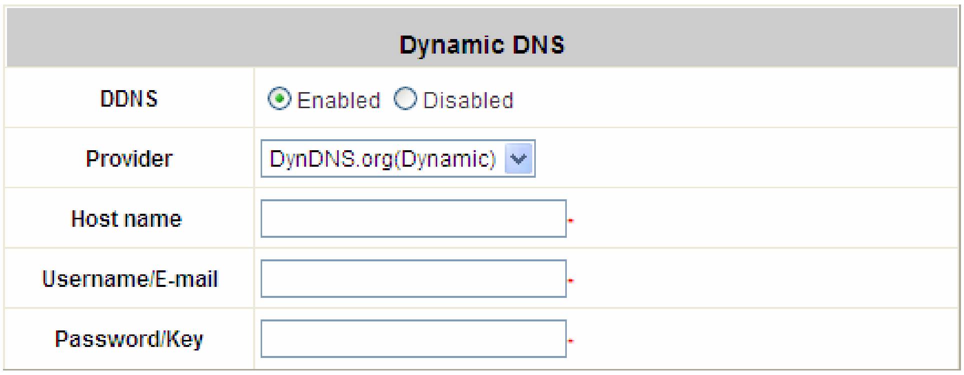
External Proxy Server		
Item	Server IP	Port
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	○ Enabled ● Disabled

- **External Proxy Server:** Under the MW-2000S security management, the system will match the External Proxy Server list to the end-users' proxy setting. If there isn't a matching, then the end-users will no be able to reach the login page and thus unable to access the network. If there is a matching, then the end-users will be directed to the system first for authentication. After a successful authentication, the end-users will be redirected back to the desired proxy servers depending on various situations.
- **Internal Proxy Server:** MW-2000S has a built-in proxy server. If this function is enabled, the end users will be forced to treat MW-2000S as the proxy server regardless of the end-users' original proxy settings.

7.4.6 Dynamic DNS

MW-2000S provides a convenient DNS function to translate a domain name to the IP address of WAN port that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server. These settings will become effective immediately after clicking ***Apply***.

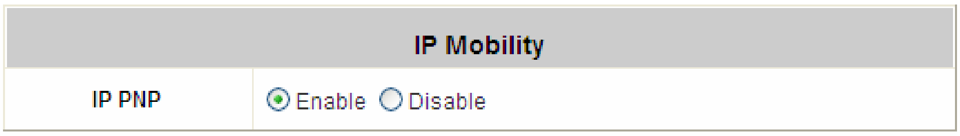


Dynamic DNS	
DDNS	● Enabled ○ Disabled
Provider	DynDNS.org(Dynamic)
Host name	*
Username/E-mail	*
Password/Key	*

- **DDNS:** Enabling or disabling of this function.
- **Provider:** Select a 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.

7.4.7 IP Mobility

MW-2000S supports IP PNP function.

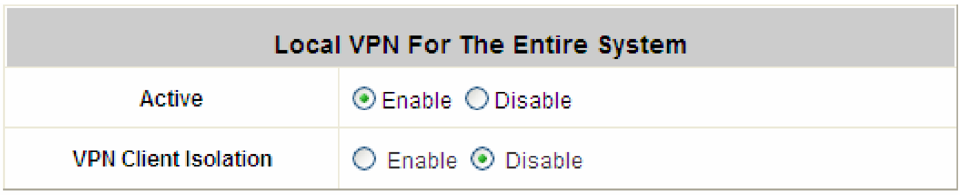


IP Mobility	
IP PNP	● Enable ○ Disable

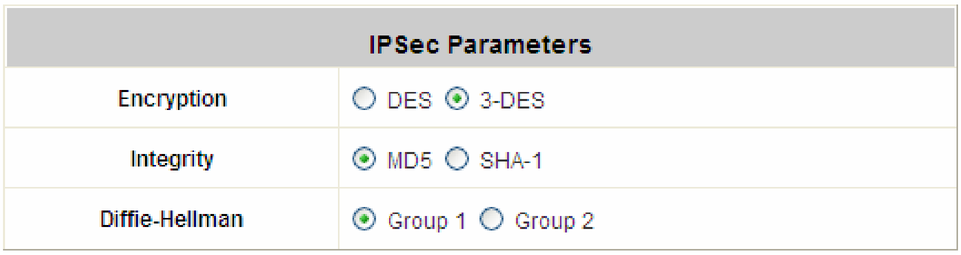
At the user end, a static IP address can be used to connect to the system. Regardless of what the IP address at the user end is, authentication can still be performed through MW-2000S

7.4.8 VPN Configuration

V*irtual* ***P****rivate* ***N****etwork*, or **VPN**, a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.



Local VPN For The Entire System	
Active	● Enable ○ Disable
VPN Client Isolation	○ Enable ● Disable

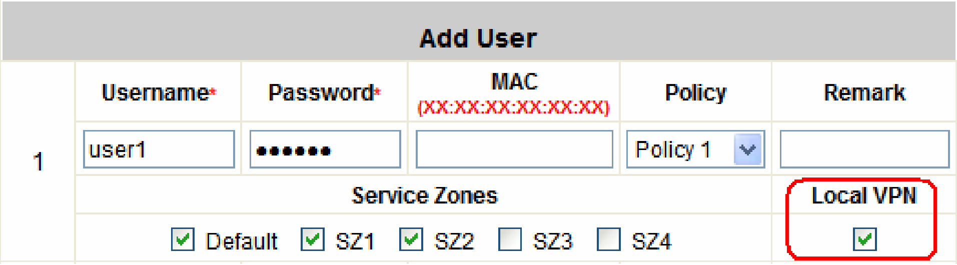


IPSec Parameters	
Encryption	○ DES ● 3-DES
Integrity	● MD5 ○ SHA-1
Diffie-Hellman	● Group 1 ○ Group 2

Local VPN The Entire System: Local VPN allows to create the VPN tunnel between a user's device and MW-2000S, to encrypt the data transmission. In addition, only when this function is enabled (***Active***) here do users of the entire system are able to use Local VPN. Local VPN users can also be isolated from each other when ***VPN Client Isolation*** is enabled.

For more information about Local VPN, please see ***Appendix E. Local VPN***.

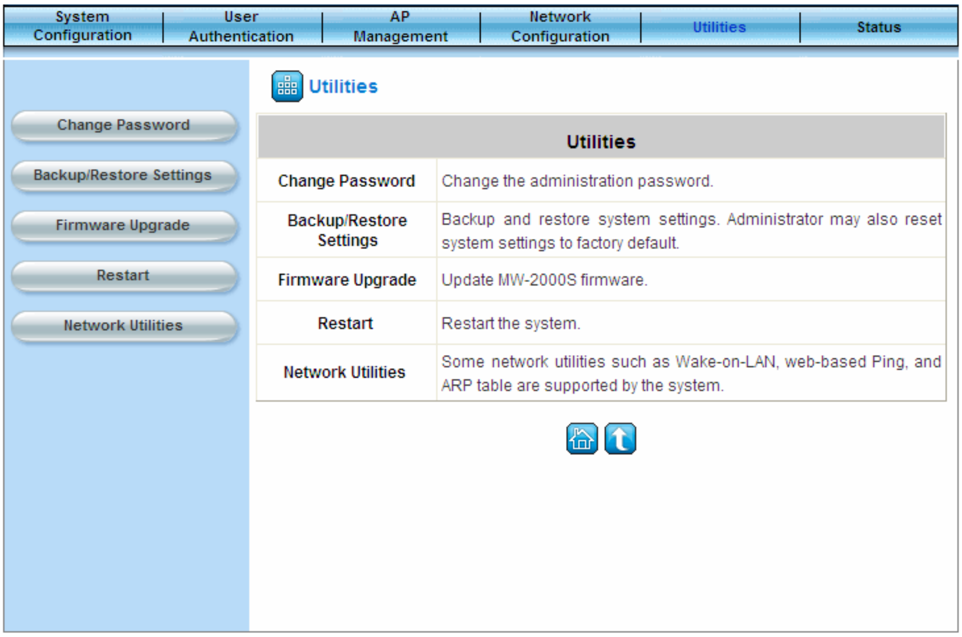
Note: *When users are required to use Local VPN for data security, their user accounts have to be configured properly to do so. For example, when adding a user account (user1) into the* ***Local*** *user database, administrator should check the "****Local VPN****" box:*



Add User					
	Username*	Password*	MAC (XX:XX:XX:XX:XX:XX)	Policy	Remark
1	user1	••••••		Policy 1	
	Service Zones				Local VPN
	☑ Default ☑ SZ1 ☑ SZ2 □ SZ3 □ SZ4				☑

7.5 Utilities

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



Utilities	
Change Password	Change the administration password.
Backup/Restore Settings	Backup and restore system settings. Administrator may also reset system settings to factory default.
Firmware Upgrade	Update MW-2000S firmware.
Restart	Restart the system.
Network Utilities	Some network utilities such as Wake-on-LAN, web-based Ping, and ARP table are supported by the system.

7.5.1 Change Password

MW-2000S supports three accounts with different access privileges. Choose to log in as **admin**, **manager** or **operator**. The default password and access privilege for each account are as follow:

Admin: The administrator can access all configuration pages of the MW-2000S.

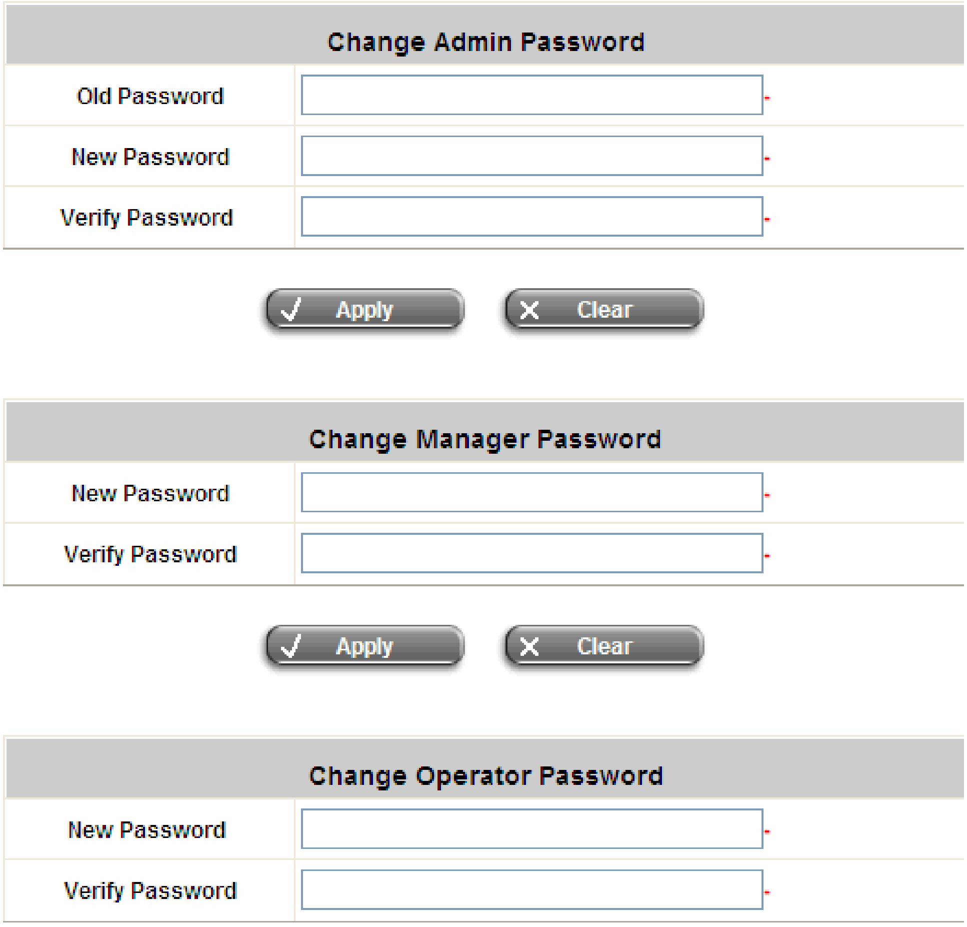
User Name: **admin**
Password: **airlive**

Manager: The manager can only access the configuration pages under ***User Authentication*** to manage the user accounts, but has no permission to change the settings of the profiles for Firewall, Specific Route and Schedule.

User Name: **manager**
Password: **airlive**

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

User Name: **operator**
Password: **airlive**



Change Admin Password

Old Password	
New Password	
Verify Password	

Change Manager Password

New Password	
Verify Password	

Change Operator Password

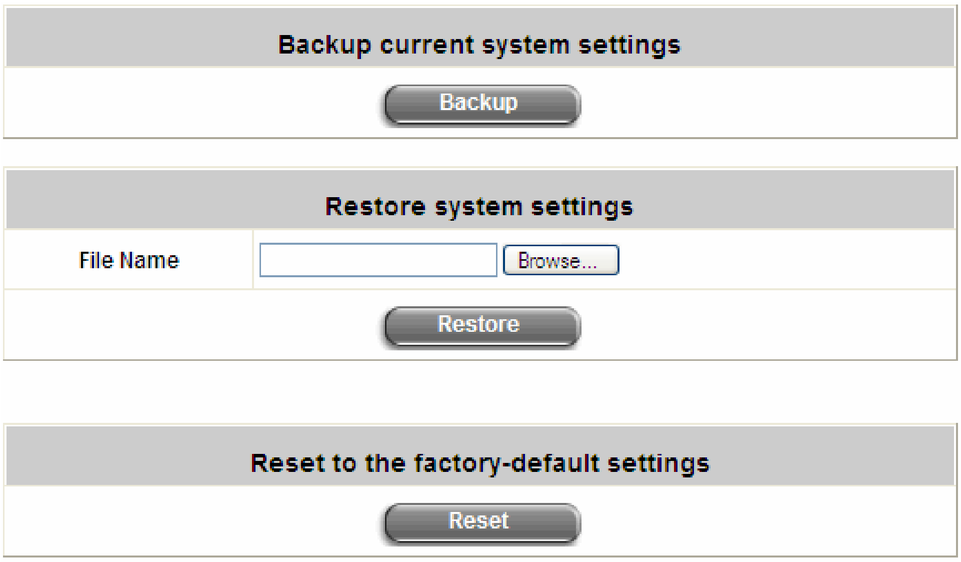
New Password	
Verify Password	

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.

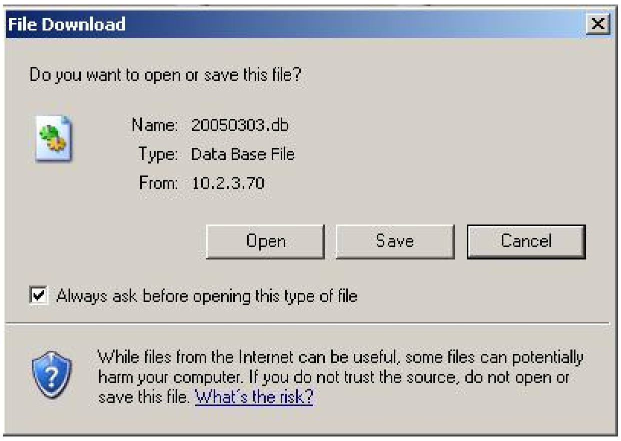
Caution: *If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port, console/printer port.*

7.5.2 Backup/Restore Setting

This function is used to backup/restore the MW-2000S settings. Also, MW-2000S can be restored to the factory default settings here.


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

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



Do you want to open or save this file?

Name: 20050303.db
Type: Data Base File
From: 10.2.3.70

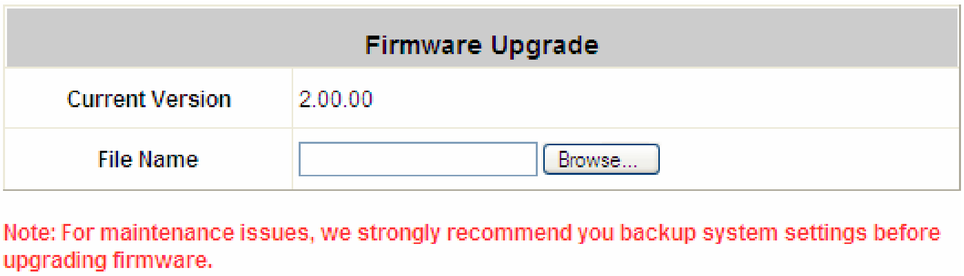
☑ Always ask before opening this type of file

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

- **Restore system setting:** Click ***Browse*** to search for a .db database backup file created by MW-2000S and click ***Restore*** to restore to the same settings at the time the backup file was created.
- **Resetting to the factory-default settings:** Click ***Reset*** to load the factory default settings of MW-2000S.

7.5.3 Firmware Upgrade

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



Firmware Upgrade	
Current Version	2.00.00
File Name	

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

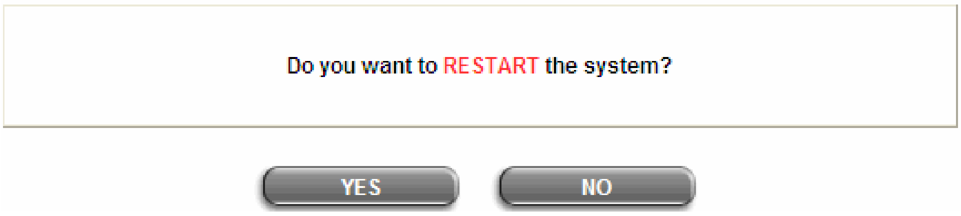
Warning:

1. Firmware upgrade may cause the loss of some of the data. Please refer to the release notes for the limitation before upgrading the firmware.

2. Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or the restart process. It may damage the system and cause it to malfunction.

7.5.4 Restart

This function allows the administrator to safely restart MW-2000S and the process should take about 100 seconds. Click ***YES*** to restart MW-2000S; click ***NO*** to go back to the previous screen. If turning off the power is necessary, it is recommended to restartMW-2000S first and then turn off the power after completing the restart process.

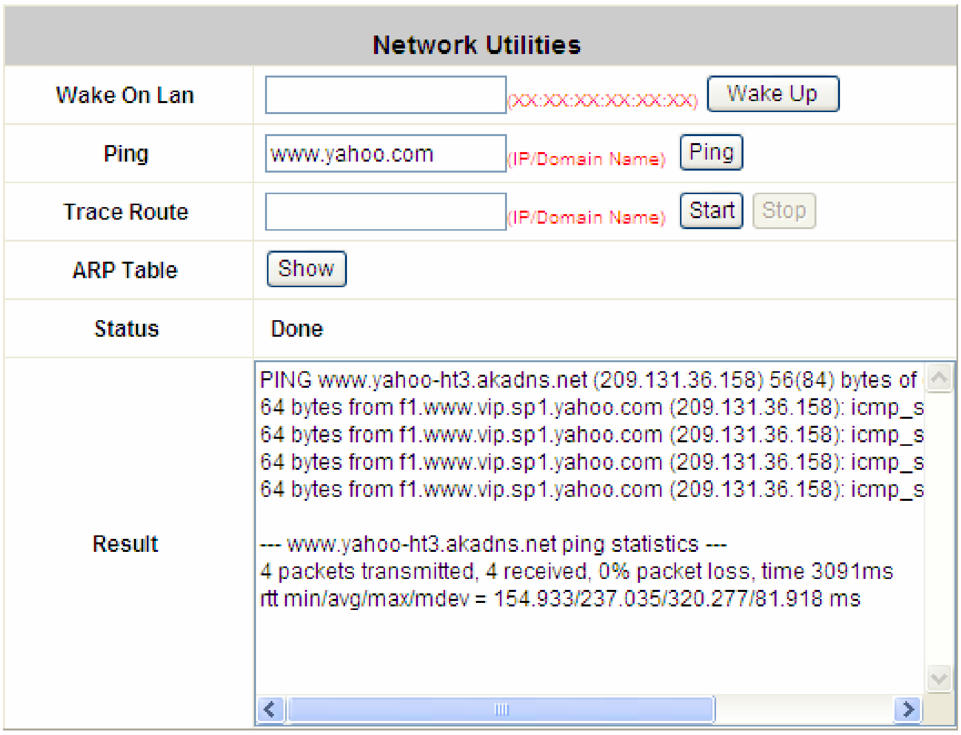


Do you want to RESTART the system?

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

7.5.5 Network Utilities

This function allows the administrators to manage functions including **Wake-on-LAN**, **Ping**, **Trace Route**, and showing **ARP Table** by entering IP or Domain Name.



Network Utilities

Wake On Lan	(XX:XX:XX:XX:XX:XX)
Ping	www.yahoo.com (IP/Domain Name)
Trace Route	(IP/Domain Name)
ARP Table	
Status	Done

Result

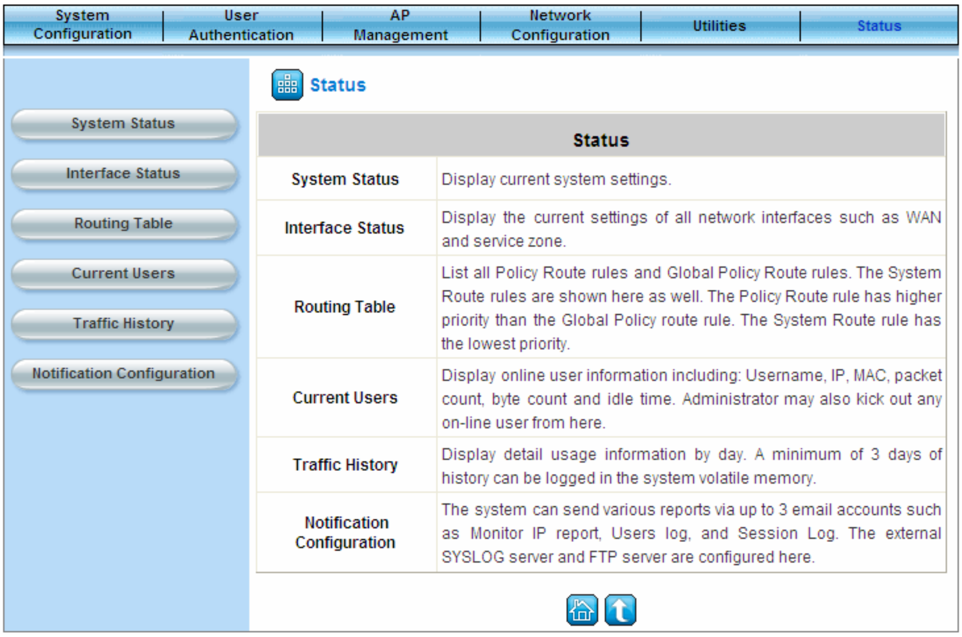
```
PING www.yahoo-ht3.akadns.net (209.131.36.158) 56(84) bytes of
64 bytes from f1.www.vip.sp1.yahoo.com (209.131.36.158): icmp_s
64 bytes from f1.www.vip.sp1.yahoo.com (209.131.36.158): icmp_s
64 bytes from f1.www.vip.sp1.yahoo.com (209.131.36.158): icmp_s
64 bytes from f1.www.vip.sp1.yahoo.com (209.131.36.158): icmp_s

--- www.yahoo-ht3.akadns.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3091ms
rtt min/avg/max/mdev = 154.933/237.035/320.277/81.918 ms
```

- **Wake on LAN:** It allows the system to remotely boot up a power-down computer with Wake-On-LAN feature enabled and is on the LAN side. Enter the MAC Address of the desired device and click Wake Up button to execute this function.
- **Ping:** It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.
- **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.
- **ARP Table:** It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).

7.6 Status

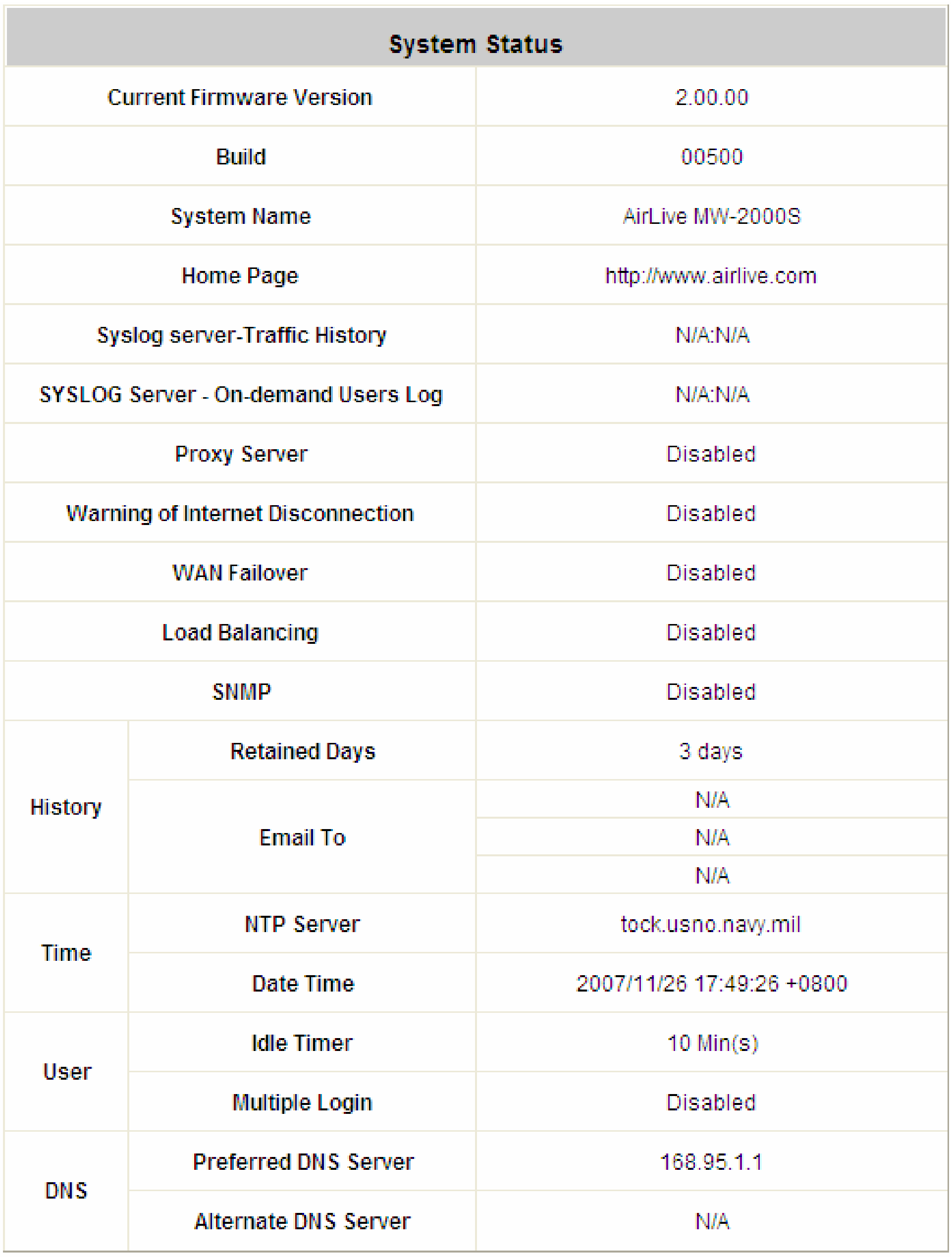
This section includes **System Status**, **Interface Status**, **Routing Table**, **Current Users**, **Traffic History**, and **Notification Configuration** to provide system status information and online user status.



Status	
System Status	Display current system settings.
Interface Status	Display the current settings of all network interfaces such as WAN and service zone.
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.
Current Users	Display online user information including: Username, IP, MAC, packet count, byte count and idle time. Administrator may also kick out any on-line user from here.
Traffic History	Display detail usage information by day. A minimum of 3 days of history can be logged in the system volatile memory.
Notification Configuration	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.

7.6.1 System Status

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



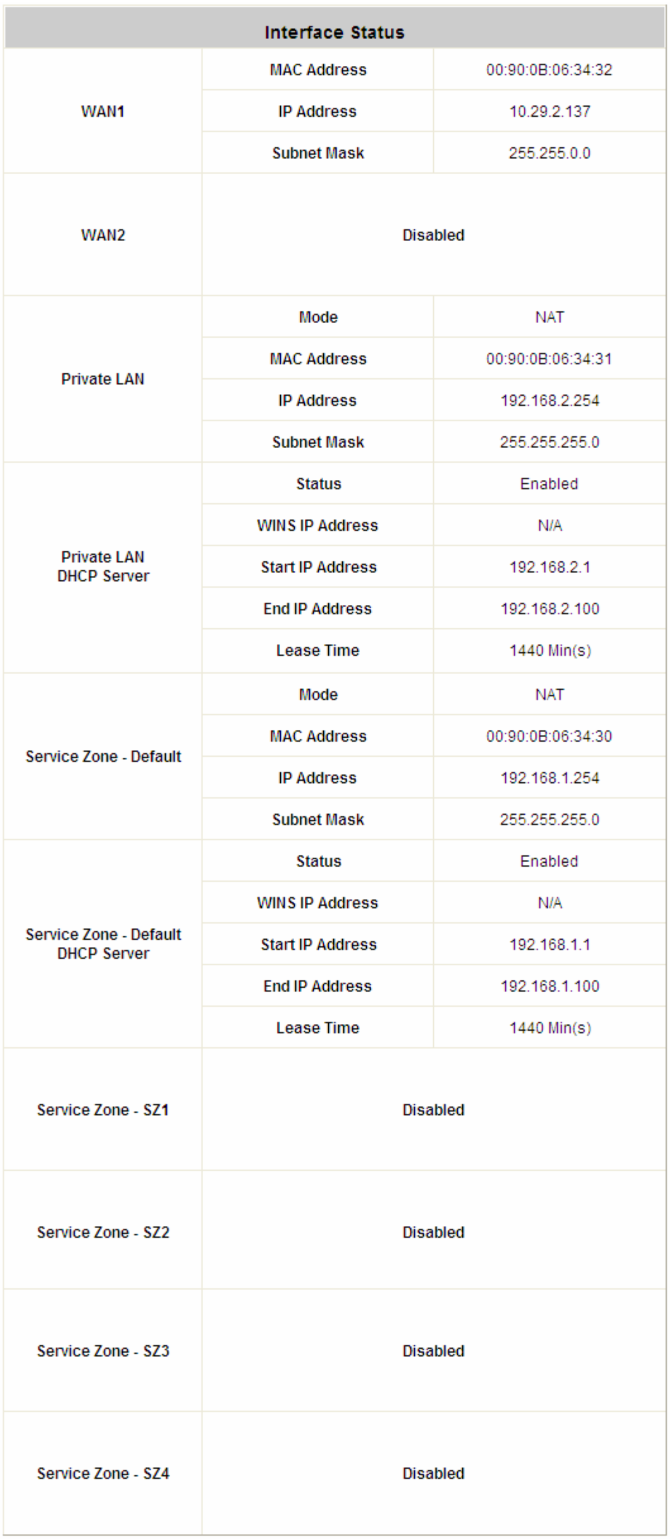
System Status		
Current Firmware Version		2.00.00
Build		00500
System Name		AirLive MW-2000S
Home Page		http://www.airlive.com
Syslog server-Traffic History		N/A:N/A
SYSLOG Server - On-demand Users Log		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Load Balancing		Disabled
SNMP		Disabled
History	Retained Days	3 days
	Email To	N/A
		N/A
		N/A
Time	NTP Server	tock.usno.navy.mil
	Date Time	2007/11/26 17:49:26 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A

The description of the table is as follows:

Item		***Description***
Current Firmware Version		The present firmware version of MW-2000S
System Name		The system name. The default is MW-2000S
Home Page		The page the users are directed to after initial login success.
Syslog server-Traffic History		The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Syslog server-On demand User log		The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Proxy Server		Enabled/disabled stands for that the system is currently using the proxy server or not.
Warning of Internet Connection 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 is currently being used or not.
SNMP		Enabled/disabled stands for the current status of the SNMP management function.
History	**Retained Days**	The maximum number of days for the system to retain the users' information.
	Email To	The email address to which the traffic history or user's traffic history information will be sent.
Time	**NTP Server**	The network time server that the system is set to align.
	Date Time	The system time is shown as the local time.
User	**Idle Timer**	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.
	Guest Account	Enabled/disabled stands for the current status of allowing Guest Accounts to log in.
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

7.6.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **LAN1~4, LAN1~4 DHCP Server, Private LAN,** and **Private LAN DHCP Server**.



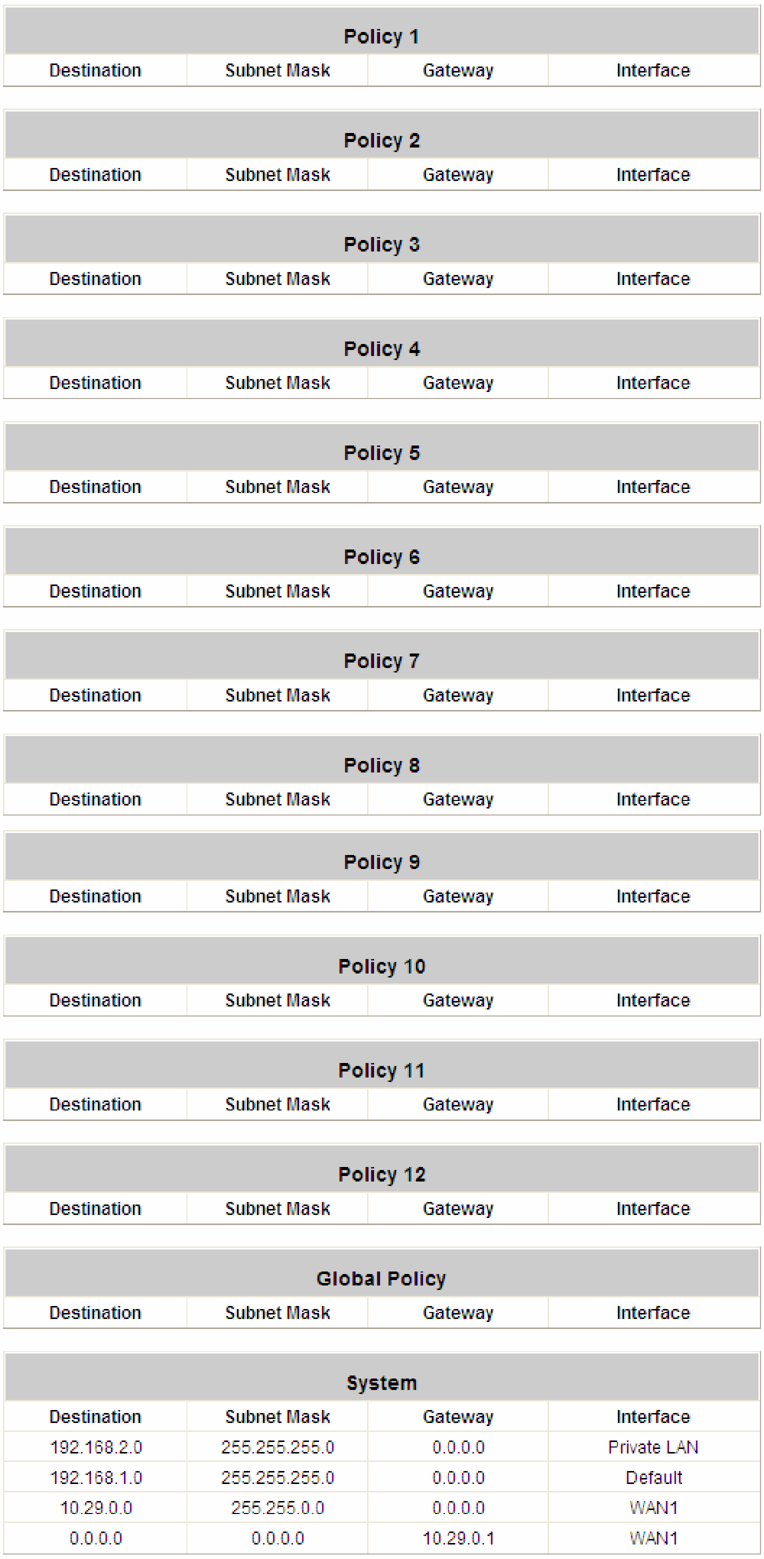
Interface Status		
WAN1	MAC Address	00:90:0B:06:34:32
	IP Address	10.29.2.137
	Subnet Mask	255.255.0.0
WAN2	Disabled	
Private LAN	Mode	NAT
	MAC Address	00:90:0B:06:34:31
	IP Address	192.168.2.254
	Subnet Mask	255.255.255.0
Private LAN DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.2.1
	End IP Address	192.168.2.100
	Lease Time	1440 Min(s)
Service Zone - Default	Mode	NAT
	MAC Address	00:90:0B:06:34:30
	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 - SZ2	Disabled	
Service Zone - SZ3	Disabled	
Service Zone - SZ4	Disabled	

The description of the 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.
LAN1~4 DHCP Server	**Status**	Enable/disable stands for status of the DHCP server on the LAN1~4 port.
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.
Private LAN	**Mode**	The mode of the private port.
	MAC Address	The MAC address of the private port.
	IP Address	The IP address of the private port.
	Subnet Mask	The Subnet Mask of the private port.
Private LAN DHCP Server	**Status**	Enable/disable stands for status of the DHCP server on the private port
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP Address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.

7.6.3 Routing Table

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



Policy 1			
Destination	Subnet Mask	Gateway	Interface

Policy 2			
Destination	Subnet Mask	Gateway	Interface

Policy 3			
Destination	Subnet Mask	Gateway	Interface

Policy 4			
Destination	Subnet Mask	Gateway	Interface

Policy 5			
Destination	Subnet Mask	Gateway	Interface

Policy 6			
Destination	Subnet Mask	Gateway	Interface

Policy 7			
Destination	Subnet Mask	Gateway	Interface

Policy 8			
Destination	Subnet Mask	Gateway	Interface

Policy 9			
Destination	Subnet Mask	Gateway	Interface

Policy 10			
Destination	Subnet Mask	Gateway	Interface

Policy 11			
Destination	Subnet Mask	Gateway	Interface

Policy 12			
Destination	Subnet Mask	Gateway	Interface

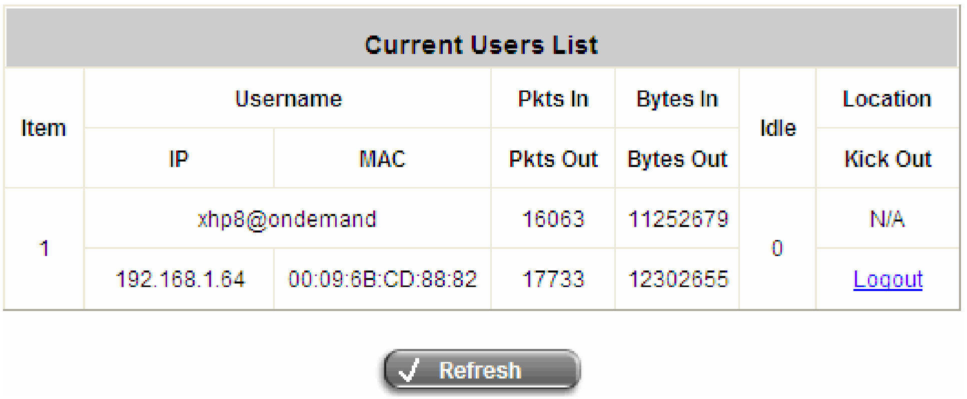
Global Policy			
Destination	Subnet Mask	Gateway	Interface

System			
Destination	Subnet Mask	Gateway	Interface
192.168.2.0	255.255.255.0	0.0.0.0	Private LAN
192.168.1.0	255.255.255.0	0.0.0.0	Default
10.29.0.0	255.255.0.0	0.0.0.0	WAN1
0.0.0.0	0.0.0.0	10.29.0.1	WAN1

- **Policy 1~12:** Shows the information of the individual Policy from 1 to 12.
- **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.

7.6.4 Current Users

In this function, each online user's information including **Username**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Idle**, **Location** and **Kick Out** will be shown. Administrators can force out a specific online user by clicking the hyperlink of ***"Logout"*** and check the user access AP status by clicking the hyperlink of the AP name for "**Location**." Click ***Refresh*** is to update the current users list.

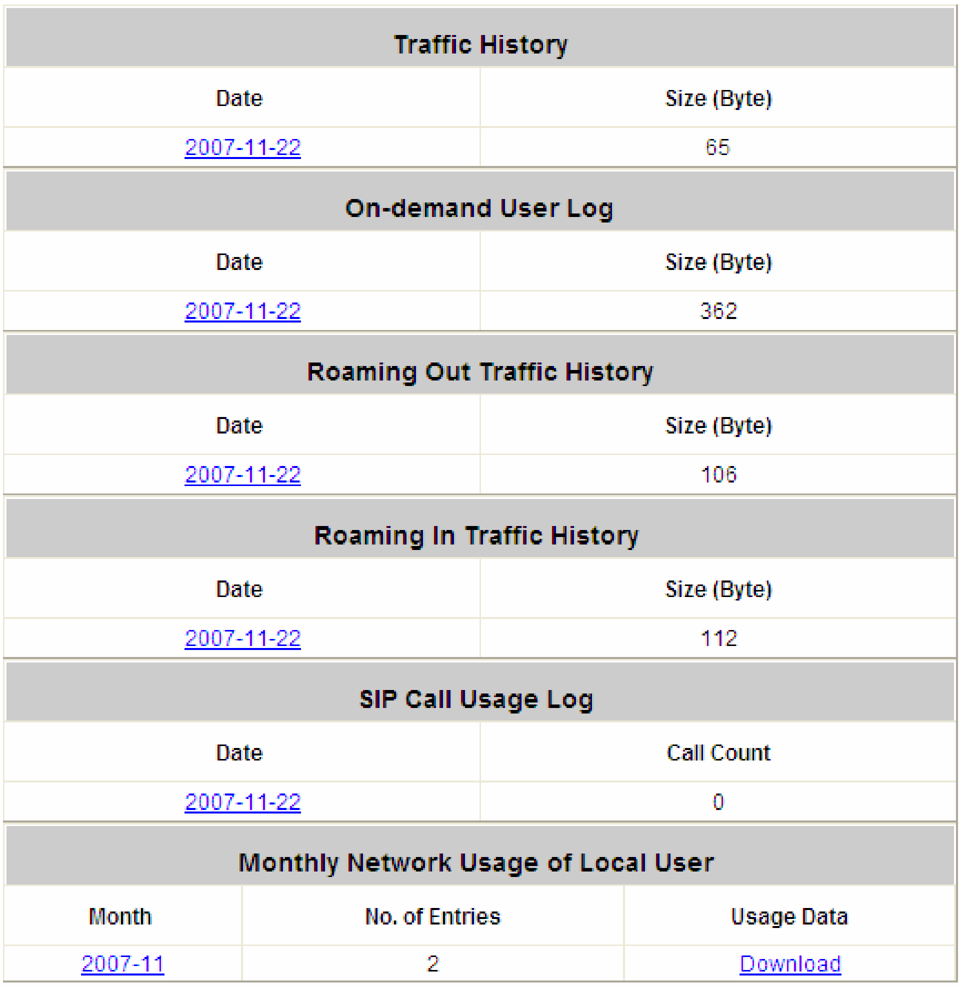


Current Users List

Item	Username		Pkts In	Bytes In	Idle	Location
	IP	MAC	Pkts Out	Bytes Out		Kick Out
1	xhp8@ondemand		16063	11252679	0	N/A
	192.168.1.64	00:09:6B:CD:88:82	17733	12302655		Logout

7.6.5 Traffic History

Administrator may view traffic history and On-demand User Log of up to 3 days. All records are sorted by date and listed accordingly. This function is used to check the traffic history of MW-2000S. The traffic history of each day will be saved separately in the DRAM for at least 3 days.



Traffic History

Date	Size (Byte)
2007-11-22	65

On-demand User Log

Date	Size (Byte)
2007-11-22	362

Roaming Out Traffic History

Date	Size (Byte)
2007-11-22	106

Roaming In Traffic History

Date	Size (Byte)
2007-11-22	112

SIP Call Usage Log

Date	Call Count
2007-11-22	0

Monthly Network Usage of Local User

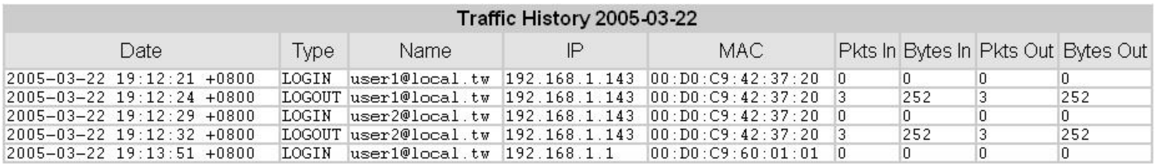
Month	No. of Entries	Usage Data
2007-11	2	Download

***Caution:** Since the history is saved in the DRAM, if you need to restart the system and also keep the history, please manually copy and save the information before restarting.*

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

- **Traffic History**

  As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type, Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out,** and **Bytes Out**, of user activities.

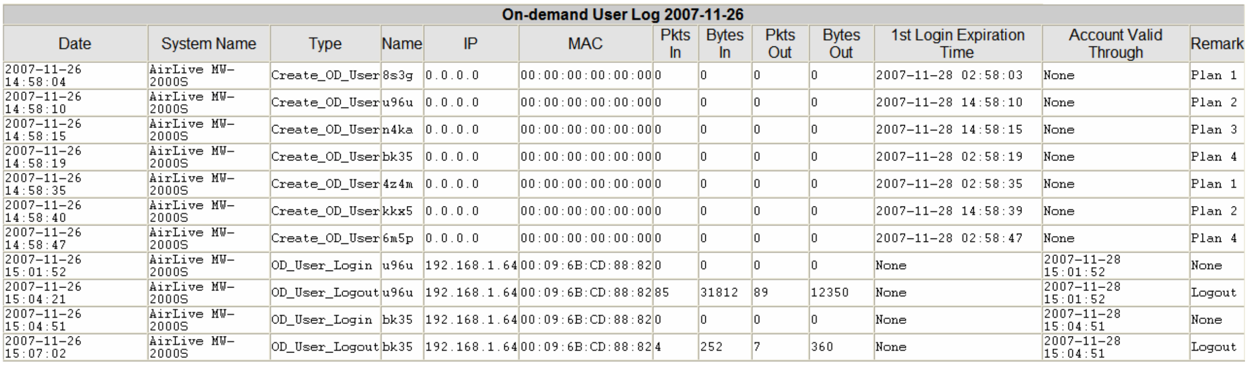


Traffic History 2005-03-22

Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out
2005-03-22 19:12:21 +0800	LOGIN	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0
2005-03-22 19:12:24 +0800	LOGOUT	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252
2005-03-22 19:12:29 +0800	LOGIN	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0
2005-03-22 19:12:32 +0800	LOGOUT	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252
2005-03-22 19:13:51 +0800	LOGIN	user1@local.tw	192.168.1.1	00:D0:C9:60:01:01	0	0	0	0

- **On-demand User Log**

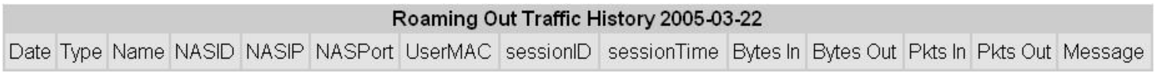
  As shown in the following figure, each line is a on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, 1st Login Expiration Time**, **Account Valid Through** and **Remark**, of user activities.



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 MW-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 MW-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 MW-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 MW-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 MW-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 MW-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 MW-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 MW-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 MW-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 MW-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 MW-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

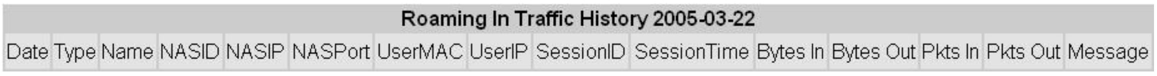
- **Roaming Out Traffic History**
  As shown in the following figure, each line is a roaming out traffic history record consisting of 14 fields, **Date**, **Type**, **Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of 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

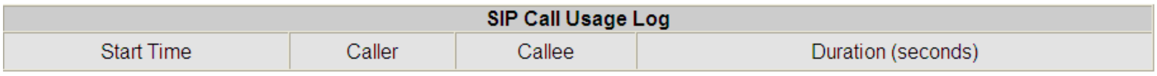
- **Roaming In Traffic History**
  As shown in the following figure, each line is a roaming in traffic history record consisting of 15 fields, **Date**, **Type**, **Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of 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

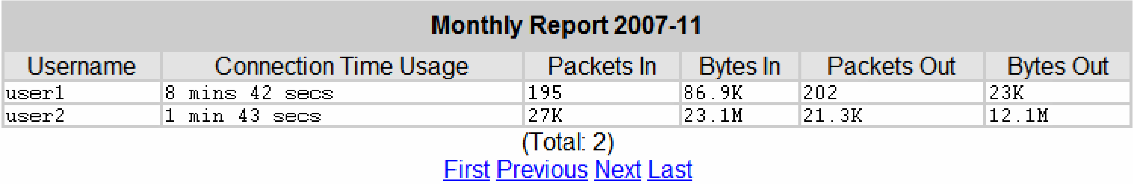
- **SIP Call Usage Log**
  The log provides the login and logout activities of SIP clients (device and soft clients) such as Start Time, Caller, Callee and Duration (seconds)



SIP Call Usage Log

Start Time	Caller	Callee	Duration (seconds)

- **Monthly Network Usage of Local User**
  The system will record the network usage of local users every month. In addition, the data will be stored locally for up to two months and can be exported as a text file in CSV format. As follows are the descriptions of fields in the usage record.



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

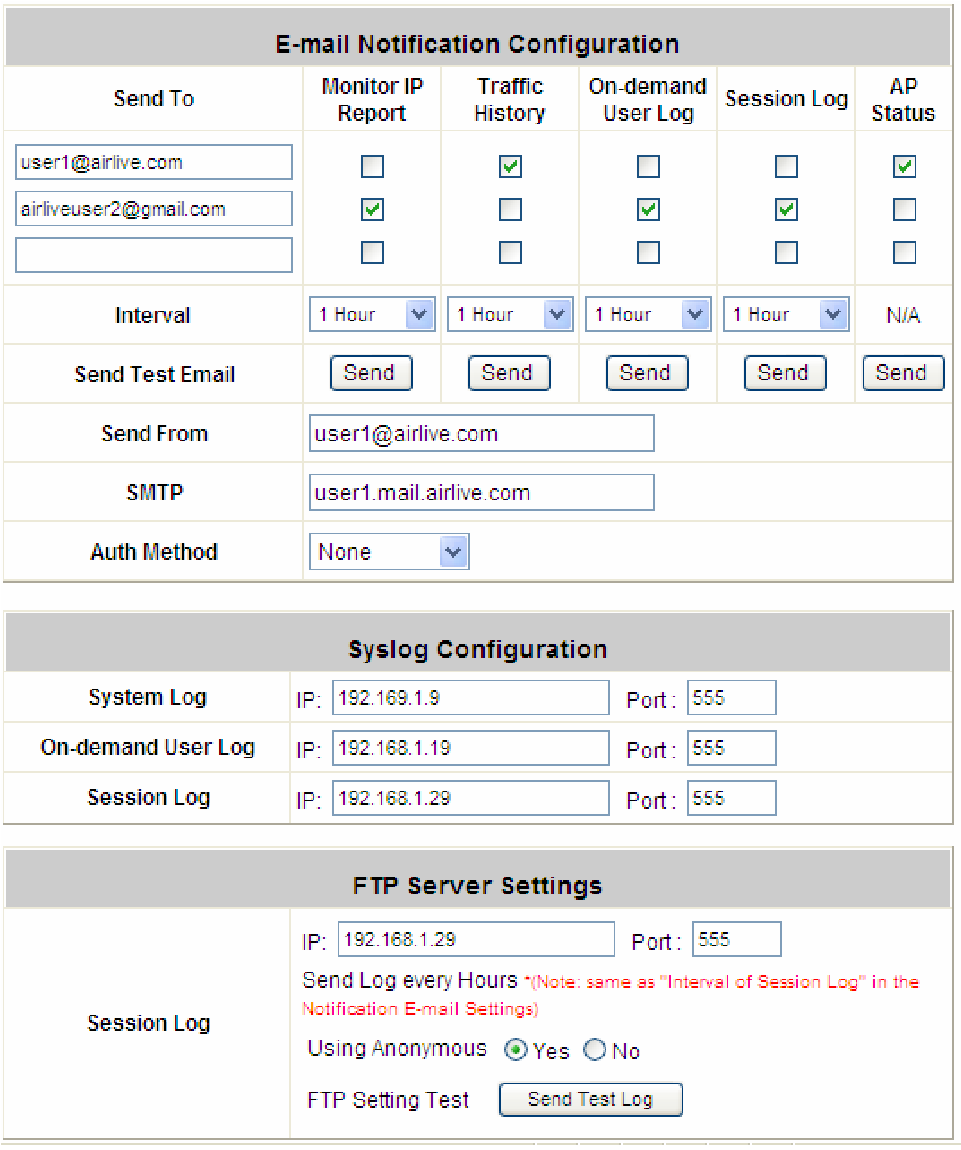
(Total: 2)

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.

7.6.6 Notification Configuration

MW-2000S can automatically send the notification of **Monitor IP Report**, **Traffic History**, **On-demand User Log**, **Session Log** and **AP status** to up to 3 particular e-mail address. 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 Syslog of Traffic History, On-demand User Log and Session 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.



E-mail Notification Configuration

Send To	Monitor IP Report	Traffic History	On-demand User Log	Session Log	AP Status
user1@airlive.com	□	☑	□	□	☑
airliveuser2@gmail.com	☑	□	☑	☑	□
	□	□	□	□	□
Interval	1 Hour	1 Hour	1 Hour	1 Hour	N/A
Send Test Email	Send	Send	Send	Send	Send
Send From	user1@airlive.com				
SMTP	user1.mail.airlive.com				
Auth Method	None				

Syslog Configuration

System Log	IP: 192.169.1.9	Port : 555
On-demand User Log	IP: 192.168.1.19	Port : 555
Session Log	IP: 192.168.1.29	Port : 555

FTP Server Settings

Session Log

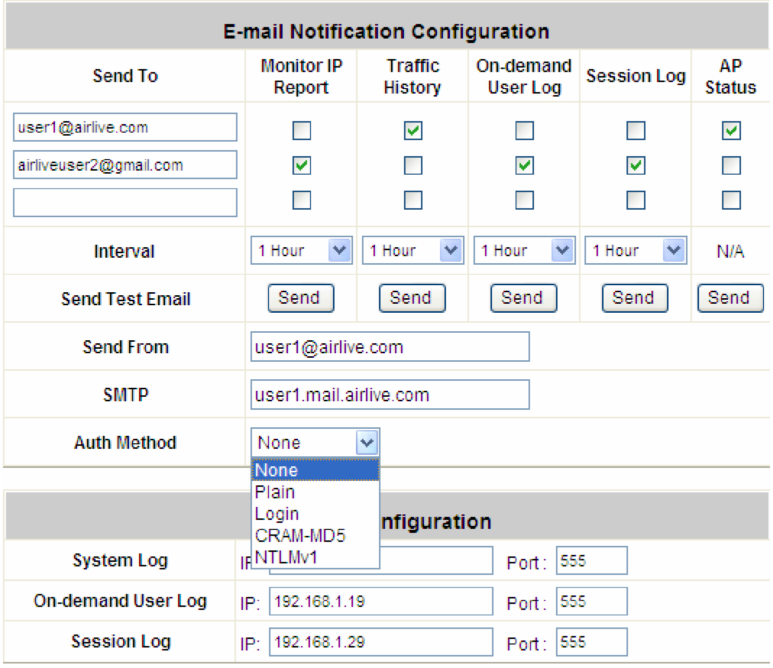
IP: 192.168.1.29 Port : 555

Send Log every Hours *(Note: same as "Interval of Session Log" in the Notification E-mail Settings)

Using Anonymous ● Yes ○ No

FTP Setting Test Send Test Log

- **E-mail Notification Configuration:**
  - **Send To:** Up to 3 e-mail address can be set up to receive the notification. These are the receiver's e-mail addresses. There are four kinds of notification to selection -- Monitor IP Report, Traffic History, On-demand User Log and AP Status, and check which type of notification to be sent.
  - **Interval:** The time interval to send the e-mail report.
  - **Send Test Email:** To test the settings immediately.
  - **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
  - **SMTP:** The IP address of the sender's SMTP server.
  - **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.



E-mail Notification Configuration

Send To	Monitor IP Report	Traffic History	On-demand User Log	Session Log	AP Status
user1@airlive.com	□	☑	□	□	☑
airliveuser2@gmail.com	☑	□	☑	☑	□
	□	□	□	□	□
Interval	1 Hour	1 Hour	1 Hour	1 Hour	N/A
Send Test Email	Send	Send	Send	Send	Send
Send From	user1@airlive.com				
SMTP	user1.mail.airlive.com				
Auth Method	None				

nfiguration

System Log	IP:	Port: 555
On-demand User Log	IP: 192.168.1.19	Port: 555
Session Log	IP: 192.168.1.29	Port: 555

- **Syslog Configuration:** There are 2 types of Syslog supported: System Log and On-demand User Log. Enter the IP address and Port number to specify which and from where the report should be sent to.

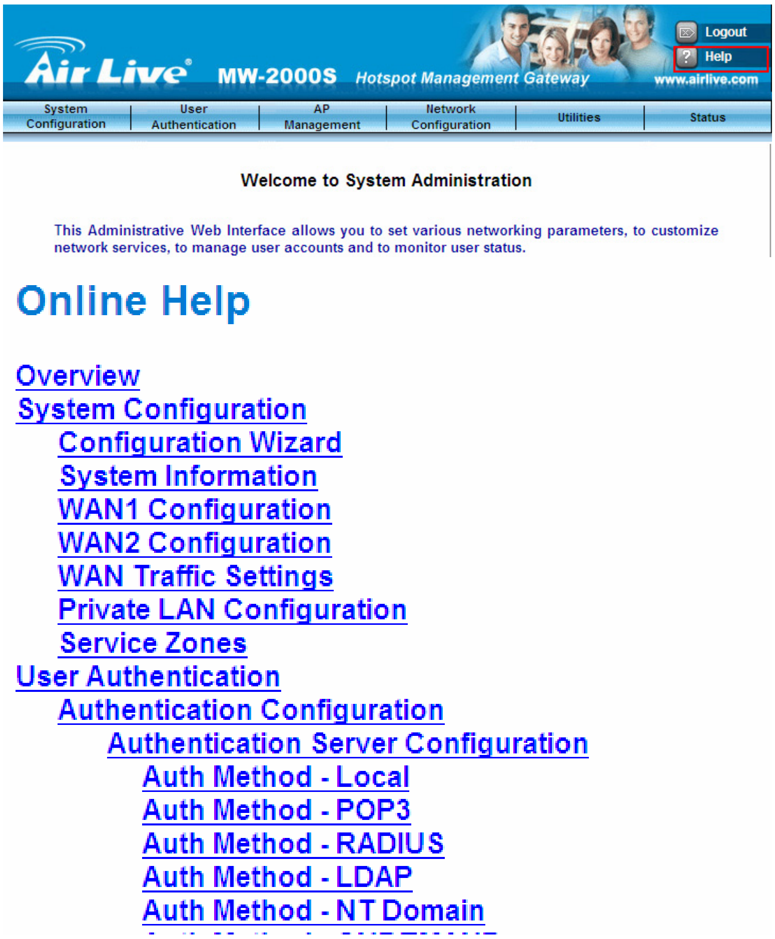
> ***Note:*** *When the number of a user's session (TCP and UDP) reaches the session limit specified in the policy, a record will be logged to this Syslog server.*

- **FTP Server Settings**
  - **Session Log:** Log each connection created by users and tracking the source IP and destination IP. If Syslog is enabled, Session Log will be sent to the Syslog 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 will be sent to the FTP server once the file size reaches its maximum size or periodical time interval.

7.7 Help

On the screen, the **Help** button is on the upper right corner.

Click ***Help*** to the **Online Help** window and then click the hyperlink of the items to get the information.



Welcome to System Administration

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

Online Help

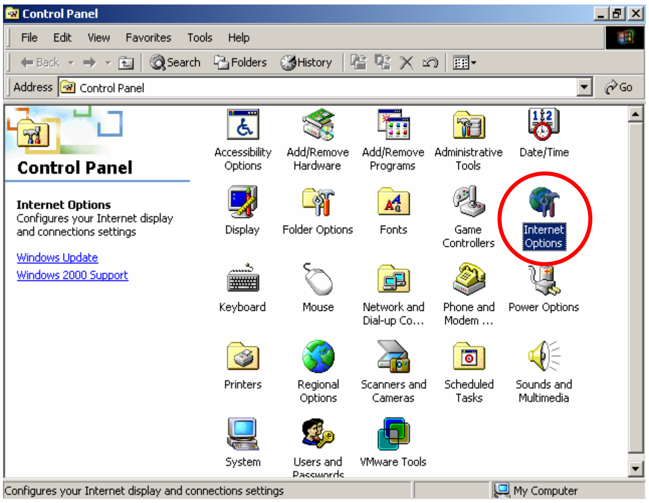
Overview
System Configuration
Configuration Wizard
System Information
WAN1 Configuration
WAN2 Configuration
WAN Traffic Settings
Private LAN Configuration
Service Zones
User Authentication
Authentication Configuration
Authentication Server Configuration
Auth Method - Local
Auth Method - POP3
Auth Method - RADIUS
Auth Method - LDAP
Auth Method - NT Domain

Appendix A: Network Configuration on PC

After MW-2000S is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

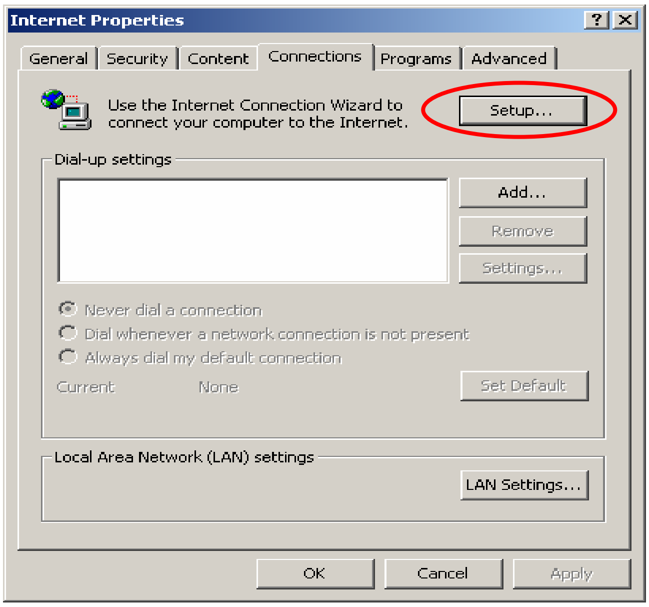
- **Internet Connection Setup**
  - ◆ **Windows 9x/2000**

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



Configures your Internet display and connections settings

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

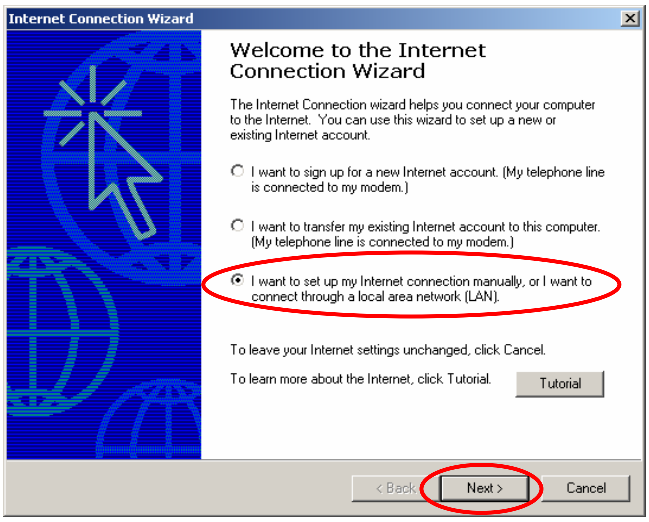


Use the Internet Connection Wizard to connect your computer to the Internet.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

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***.



Welcome to the Internet Connection Wizard

The Internet Connection wizard helps you connect your computer to the Internet. You can use this wizard to set up a new or existing Internet account.

○ I want to sign up for a new Internet account. (My telephone line is connected to my modem.)

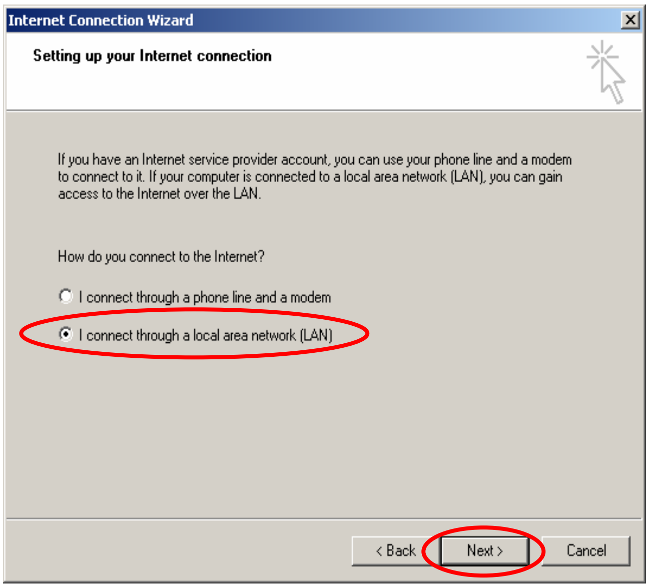
○ I want to transfer my existing Internet account to this computer. (My telephone line is connected to my modem.)

● I want to set up my Internet connection manually, or I want to connect through a local area network (LAN).

To leave your Internet settings unchanged, click Cancel.

To learn more about the Internet, click Tutorial.

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



Internet Connection Wizard

Setting up your Internet connection

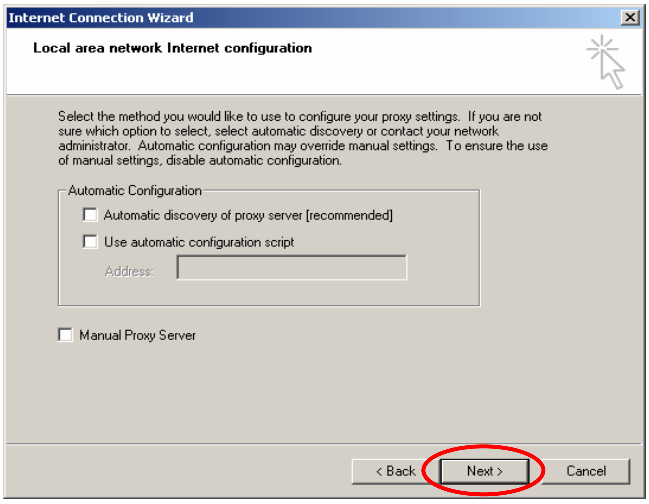
If you have an Internet service provider account, you can use your phone line and a modem to connect to it. If your computer is connected to a local area network (LAN), you can gain access to the Internet over the LAN.

How do you connect to the Internet?

○ I connect through a phone line and a modem

● I connect through a local area network (LAN)

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



Internet Connection Wizard

Local area network Internet configuration

Select the method you would like to use to configure your proxy settings. If you are not sure which option to select, select automatic discovery or contact your network administrator. Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

Automatic Configuration

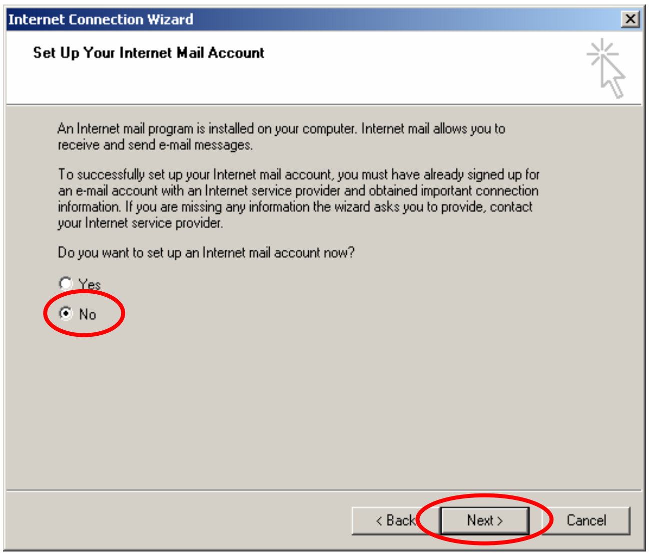
□ Automatic discovery of proxy server [recommended]

□ Use automatic configuration script

Address:

□ Manual Proxy Server

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



Internet Connection Wizard

Set Up Your Internet Mail Account

An Internet mail program is installed on your computer. Internet mail allows you to receive and send e-mail messages.

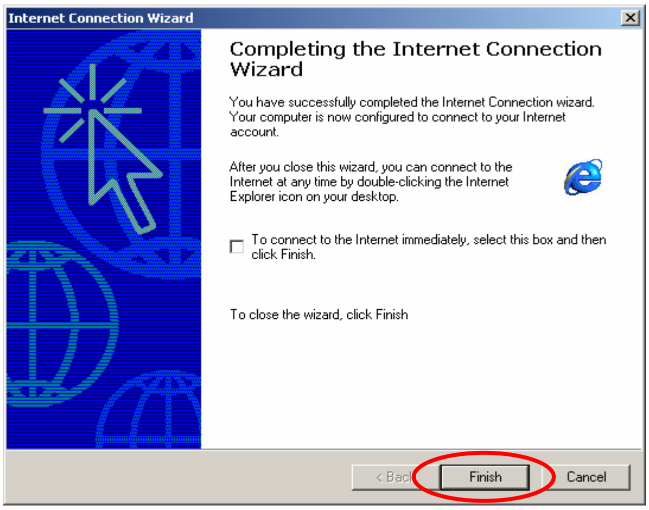
To successfully set up your Internet mail account, you must have already signed up for an e-mail account with an Internet service provider and obtained important connection information. If you are missing any information the wizard asks you to provide, contact your Internet service provider.

Do you want to set up an Internet mail account now?

○ Yes

● No

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



Completing the Internet Connection Wizard

You have successfully completed the Internet Connection wizard. Your computer is now configured to connect to your Internet account.

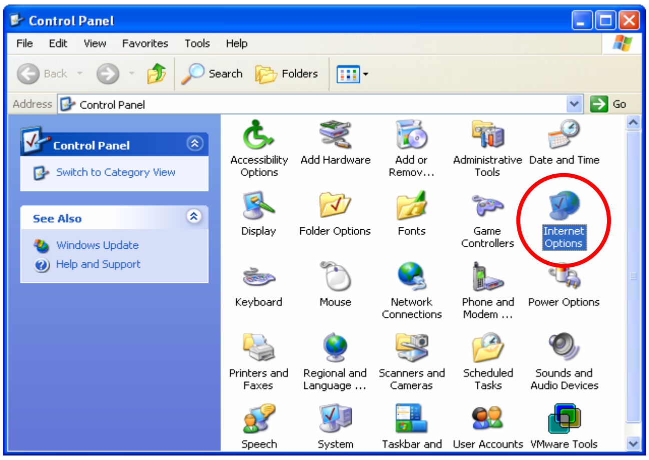
After you close this wizard, you can connect to the Internet at any time by double-clicking the Internet Explorer icon on your desktop.

□ To connect to the Internet immediately, select this box and then click Finish.

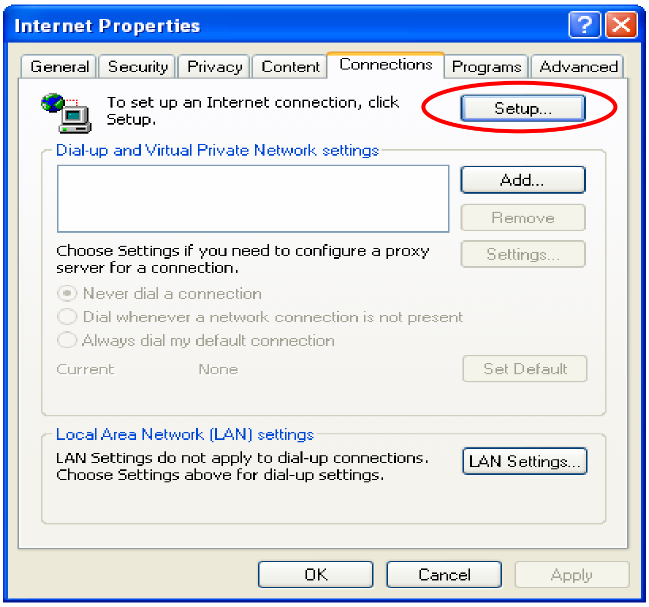
To close the wizard, click Finish

◆ **Windows XP**

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



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



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

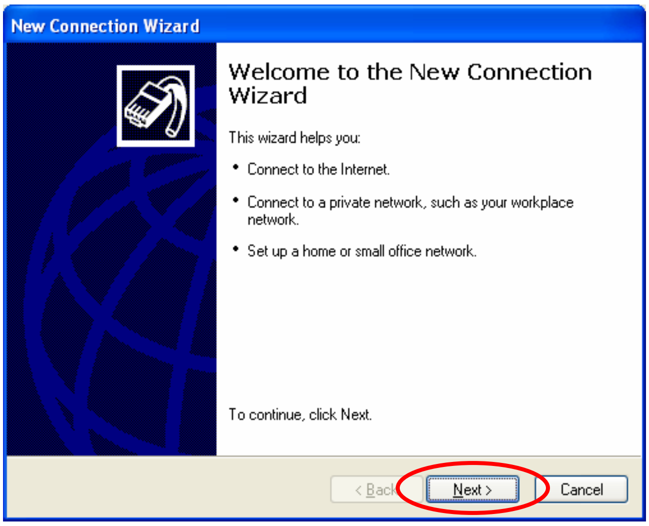
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

3) Click ***Next*** when **Welcome to the New Connection Wizard** screen appears.



New Connection Wizard

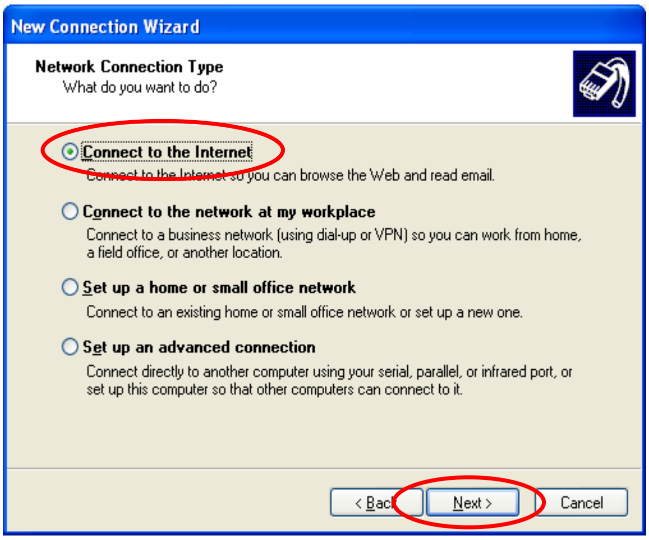
Welcome to the New Connection Wizard

This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To continue, click Next.

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



New Connection Wizard

Network Connection Type
What do you want to do?

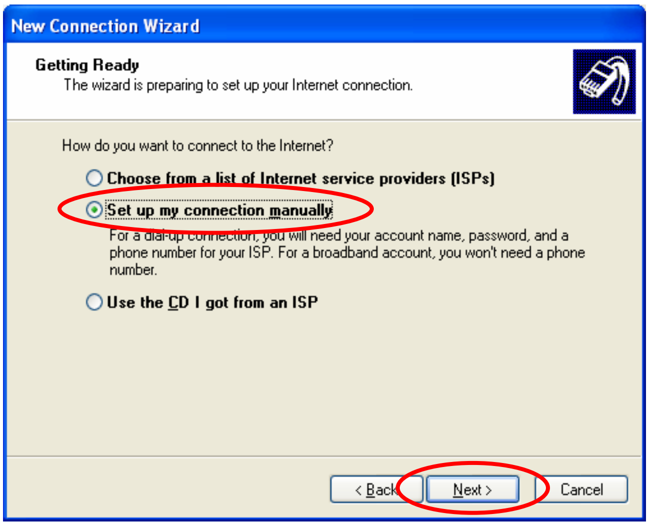
● **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

○ **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

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



New Connection Wizard

Getting Ready
The wizard is preparing to set up your Internet connection.

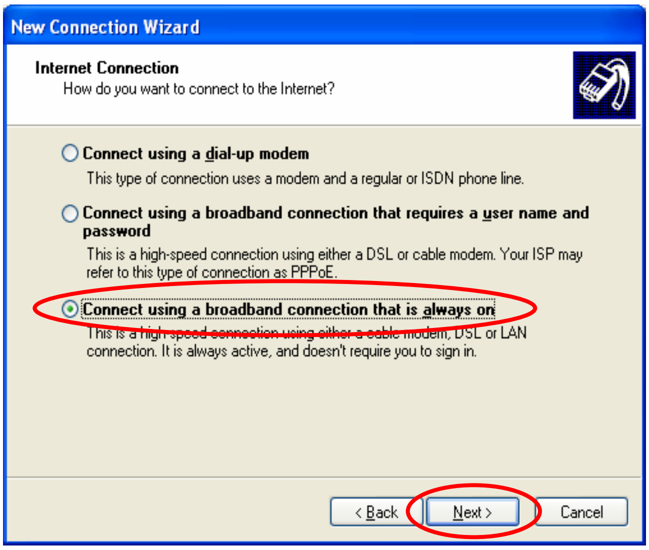
How do you want to connect to the Internet?

○ **Choose from a list of Internet service providers (ISPs)**

● **Set up my connection manually**
For a dial-up connection, you will need your account name, password, and a phone number for your ISP. For a broadband account, you won't need a phone number.

○ **Use the CD I got from an ISP**

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



New Connection Wizard

Internet Connection

How do you want to connect to the Internet?

○ **Connect using a dial-up modem**

This type of connection uses a modem and a regular or ISDN phone line.

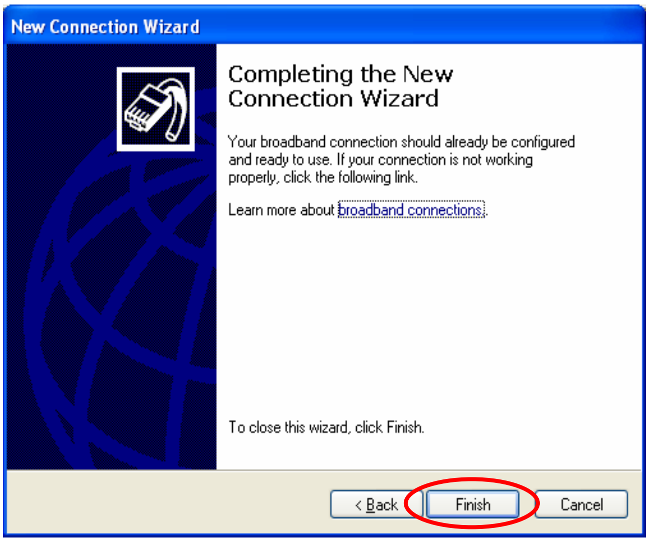
○ **Connect using a broadband connection that requires a user name and password**

This is a high-speed connection using either a DSL or cable modem. Your ISP may refer to this type of connection as PPPoE.

● **Connect using a broadband connection that is always on**

This is a high-speed connection using either a cable modem, DSL or LAN connection. It is always active, and doesn't require you to sign in.

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



New Connection Wizard

Completing the New Connection Wizard

Your broadband connection should already be configured and ready to use. If your connection is not working properly, click the following link.

Learn more about broadband connections.

To close this wizard, click Finish.

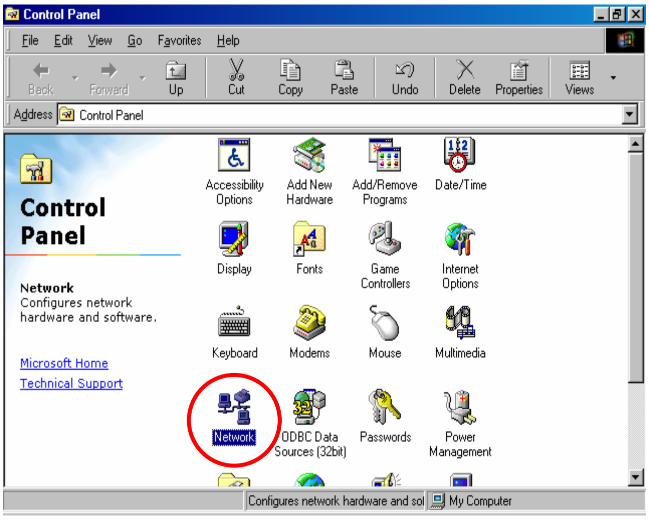
- **TCP/IP Network Setup**

  If the operating system of your PC is Windows 95/98/ME/2000/XP, keep the default settings without any change to directly start/restart the system. With the factory default settings, during the process of starting the system, MW-2000S 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"**.

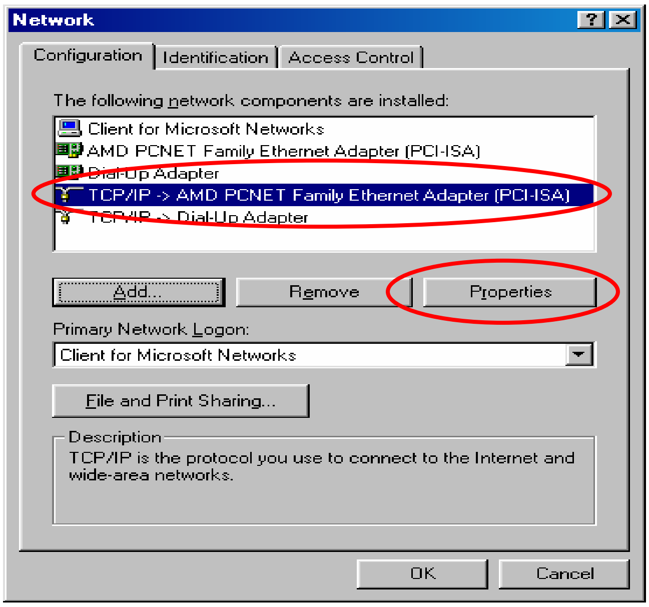
  If you want to check the TCP/IP setup or use the static IP in the LAN1/LAN2 or LAN3/LAN4 section, please follow the following steps:

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

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



2) Choose **"Configuration"** label and select **"TCP/IP → AMD PCNET Family Ethernet Adapter (PCI-ISA)"**, and then click ***Properties***. Now, you can choose to use **DHCP** or **specific IP address**.



The following network components are installed:

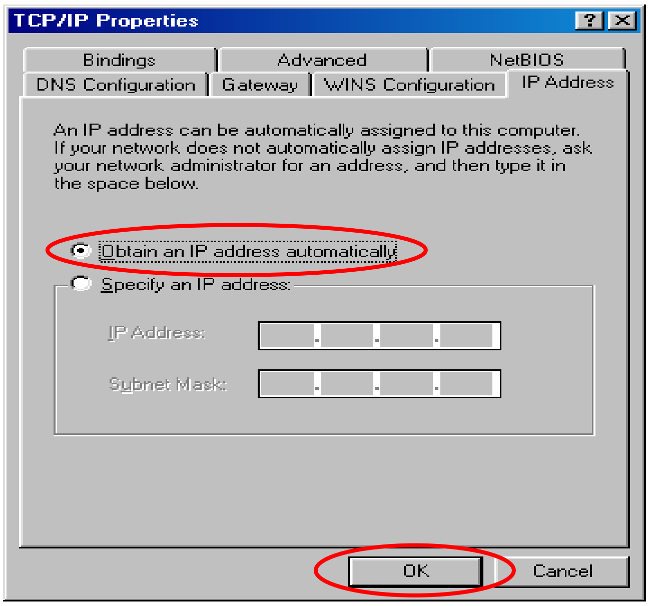
Client for Microsoft Networks
AMD PCNET Family Ethernet Adapter (PCI-ISA)
Dial-Up Adapter
TCP/IP -> AMD PCNET Family Ethernet Adapter (PCI-ISA)
TCP/IP -> Dial-Up Adapter

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

3) **Using DHCP:** If you want to use DHCP, please choose **"Obtain an IP address automatically"** on the **"IP Address"** label and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from MW-2000S.

4) **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of MW-2000S: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.



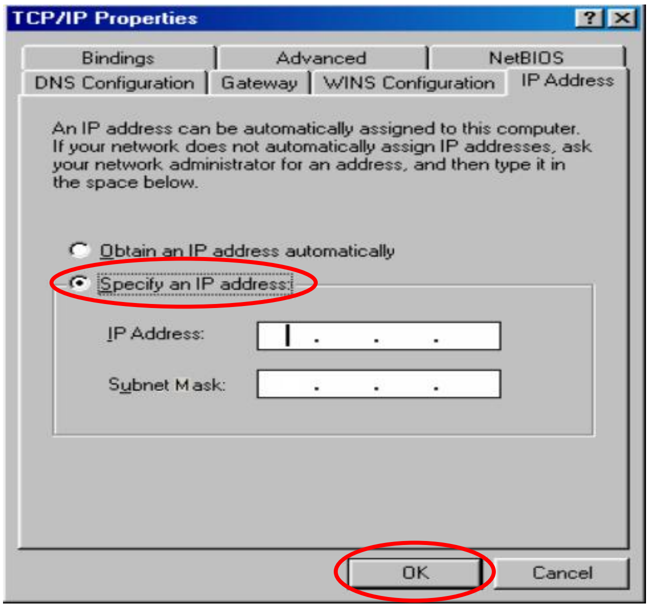
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

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

- Please choose **"Specify an IP address"** and enter the information given by the network administrator in **"IP Address"** and **"Subnet Mask"** on the **"IP Address"** label and then click ***OK***.

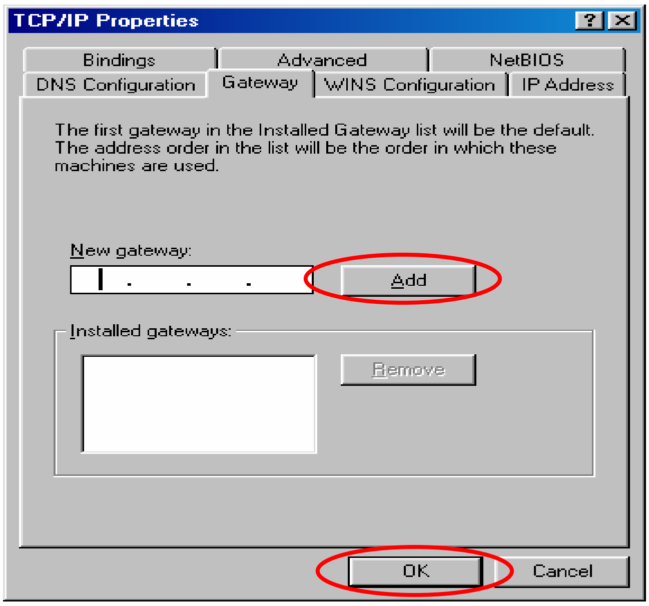


An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

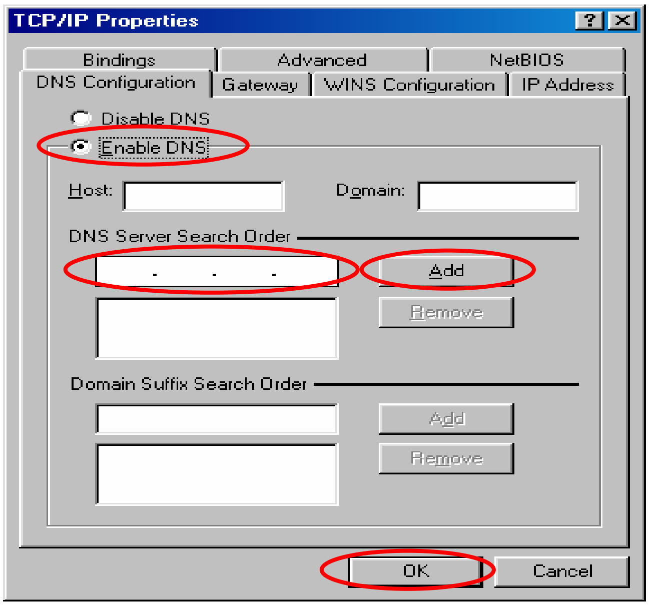
● Specify an IP address:

- Choose **“Gateway”** label and enter the gateway address of MW-2000S in the **“New gateway:”** and then click ***Add*** and ***OK***.



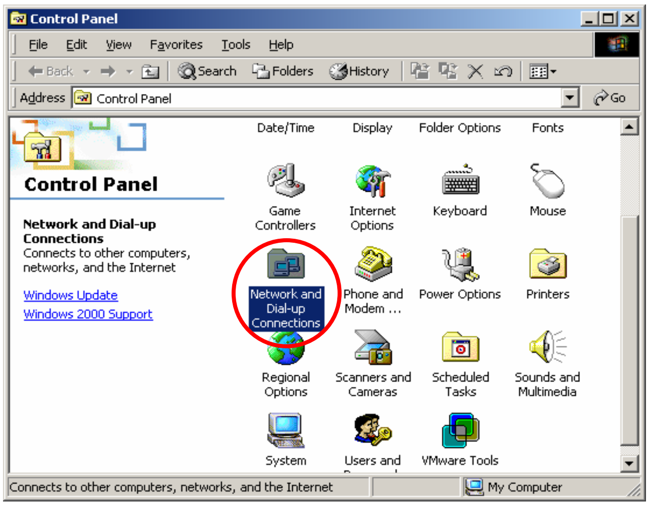
The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

- Choose **“DNS Configuration”** label. If the DNS Server column is blank, please click ***Enable DNS*** and then enter the DNS address or the DNS address provided by ISP. Then, click ***Add*** and click ***OK***.



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

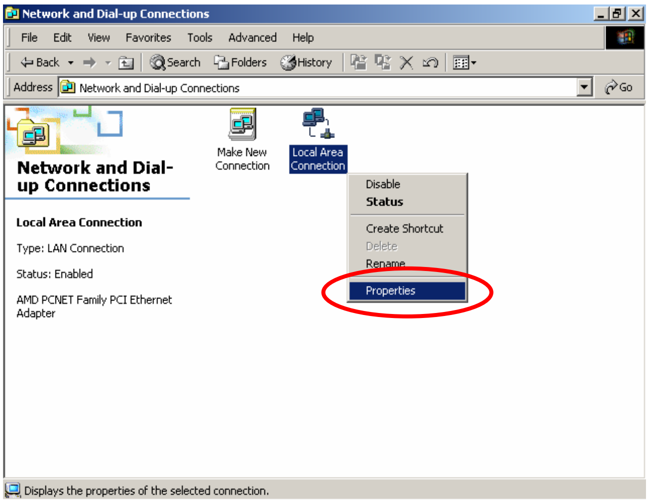
1) Select **Start → Control Panel → Network and Dial-up Connections**.



Network and Dial-up Connections
Connects to other computers, networks, and the Internet

Connects to other computers, networks, and the Internet

2) Click the right button of the mouse on **"Local Area Connection"** icon and then select **"Properties"**.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
Local Area Connection
Disable
Status
Create Shortcut
Delete
Rename
Properties

Network and Dial-up Connections

Local Area Connection

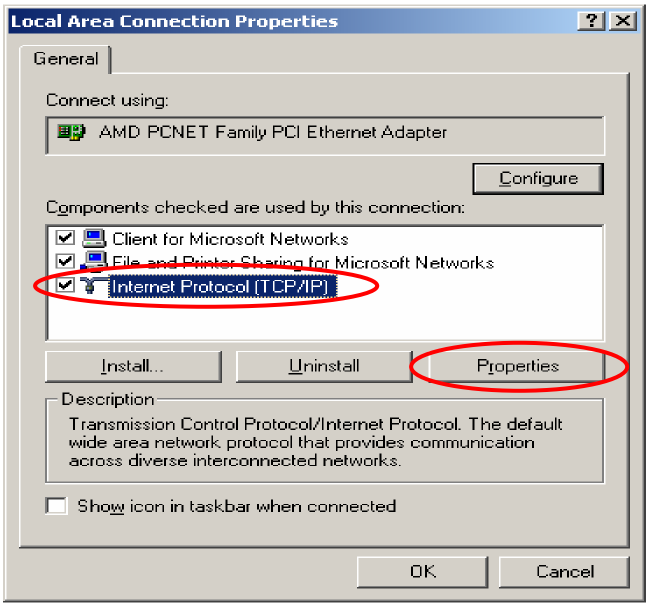
Type: LAN Connection

Status: Enabled

AMD PCNET Family PCI Ethernet Adapter

Displays the properties of the selected connection.

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



Connect using:

AMD PCNET Family PCI Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

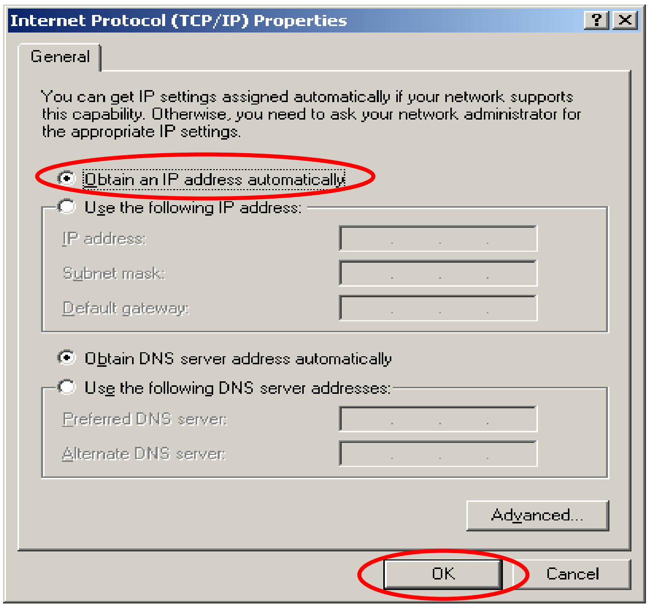
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

4) **Using DHCP:** If want to use DHCP, please 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 MW-2000S.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

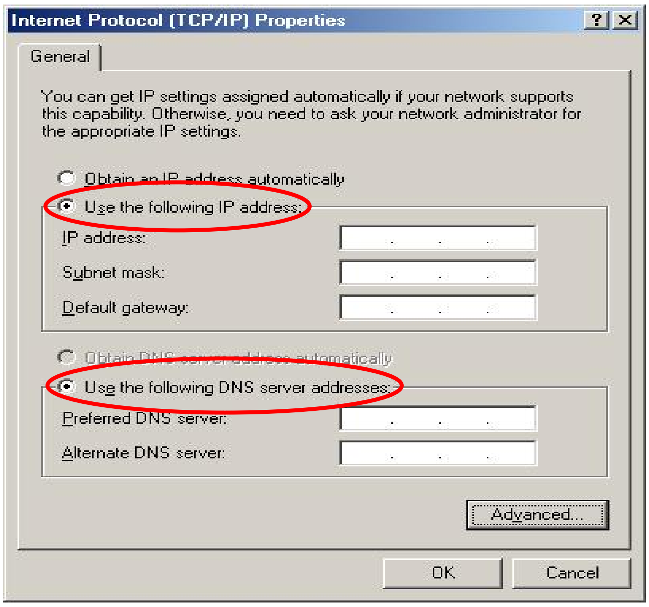
Preferred DNS server: . . .

Alternate DNS server: . . .

5) **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of the MW-2000S: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

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

- Please choose **"Use the following IP address"** and enter the information given from the network administrator in **"IP address"** and **"Subnet mask"** If the DNS Server column is blank, please choose **"Using the following DNS server addresses"** and then enter the DNS address or the DNS address provided by ISP and then click ***OK***.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

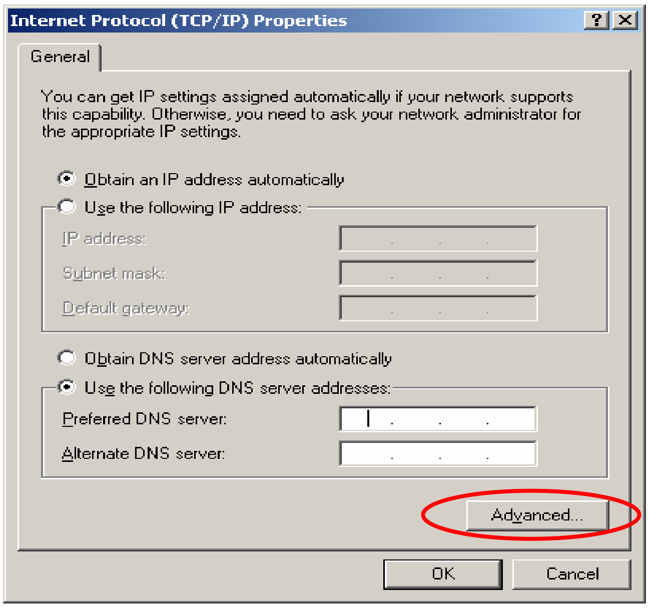
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

- Then, click ***Advanced*** in the window of **"Internet Protocol (TCP/IP)"**.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

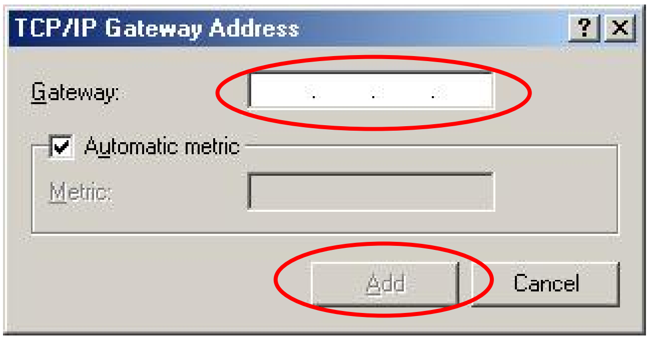
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

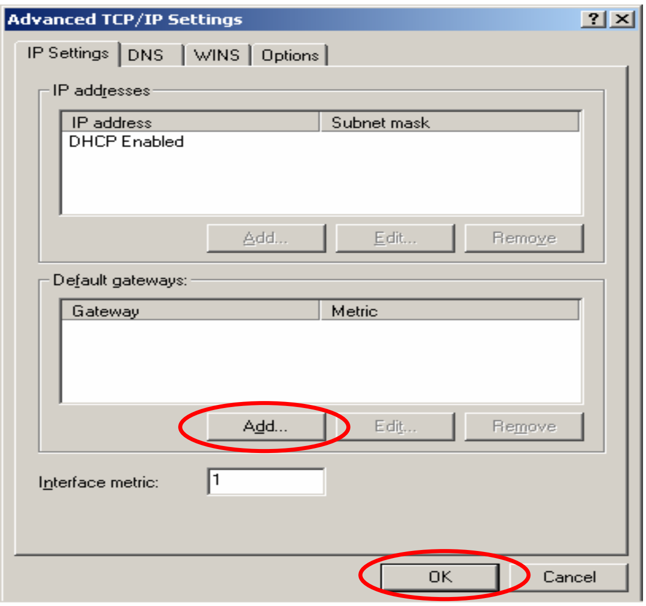
- Choose the **“IP Settings”** label and click ***Add*** below the **“Default Gateways”** column and the **“TCP/IP Gateway Address”** window will appear. Enter the gateway address of MW-2000S in the **“Gateway”** of **“TCP/IP Gateway Address”** window, and then click ***Add***. After back to the **“IP Settings”** label, click ***OK*** to finish.


TCP/IP Gateway Address

Gateway: . . .

☑ Automatic metric

Metric:


Advanced TCP/IP Settings

IP addresses

IP address	Subnet mask
DHCP Enabled	

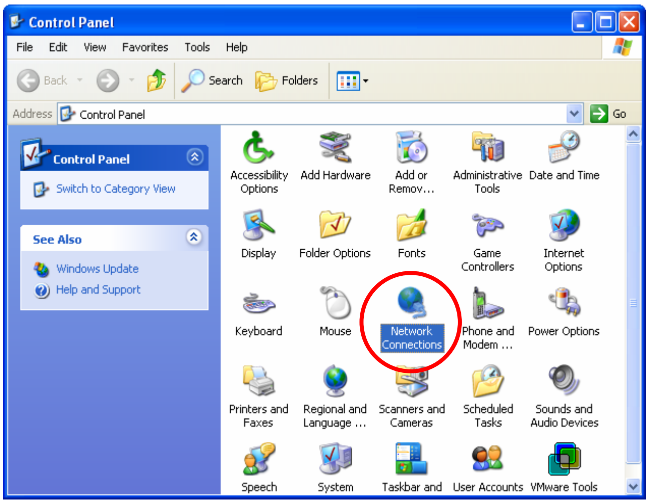
Default gateways:

Gateway	Metric

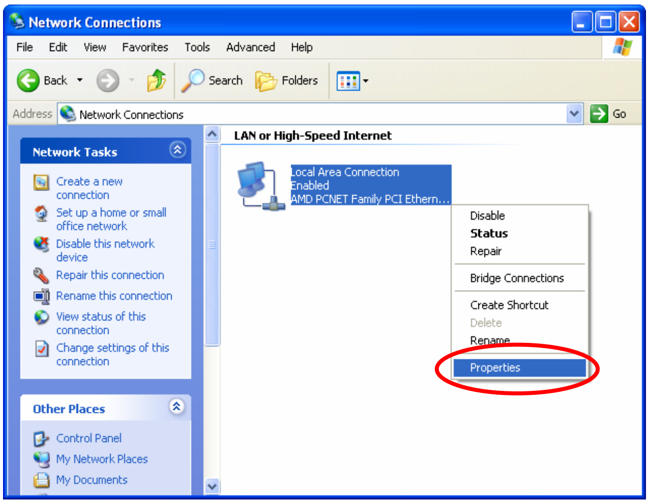
Interface metric: 1

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

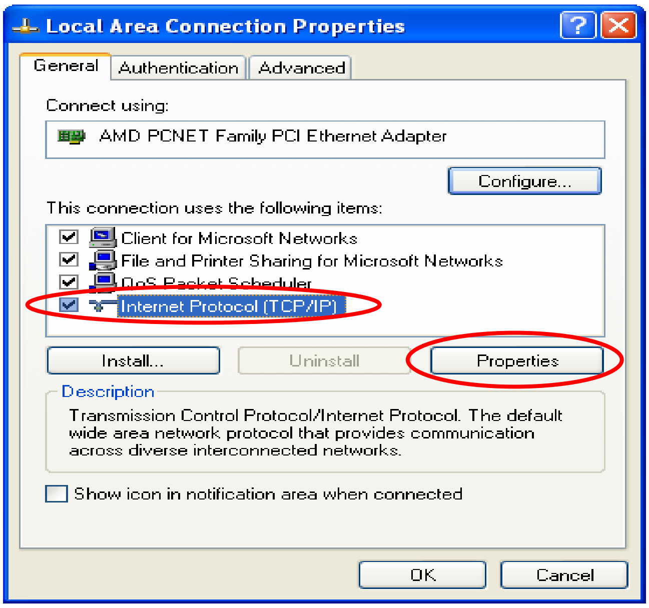
1) Select **Start → Control Panel → Network Connection**.



2) Click the right button of the mouse on the **“Local Area Connection”** icon and select **“Properties”**



3) Select **“General”** label and choose **“Internet Protocol (TCP/IP)”** and then click ***Properties***. Now, you can choose to use **DHCP** or **specific IP address**, please proceed to the following steps.



Connect using:

AMD PCNET Family PCI Ethernet Adapter

This connection uses the following items:

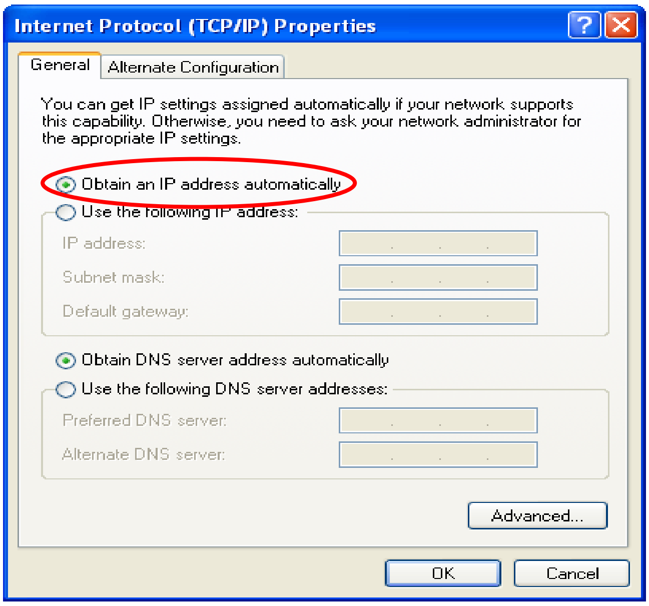
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

4) **Using DHCP:** If want to use DHCP, please 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 MW-2000S.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

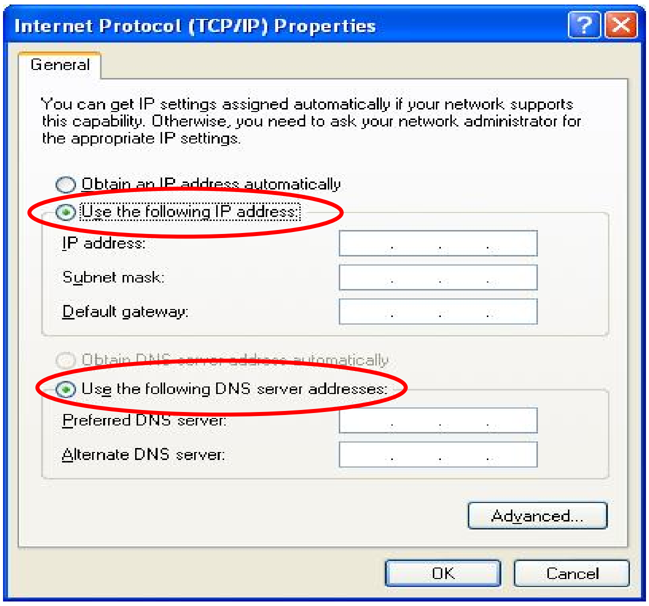
Preferred DNS server: . . .

Alternate DNS server: . . .

5) **Using Specific IP Address:** If want to use specific IP address, you have to ask the network administrator for the information of the MW-2000S: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

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

- Please choose **"Use the following IP address"** and enter the information given from the network administrator in **"IP address"** and **"Subnet mask"** If the DNS Server column is blank, please choose **"Using the following DNS server addresses"** and then enter the DNS address or the DNS address provided by ISP and then click ***OK***.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

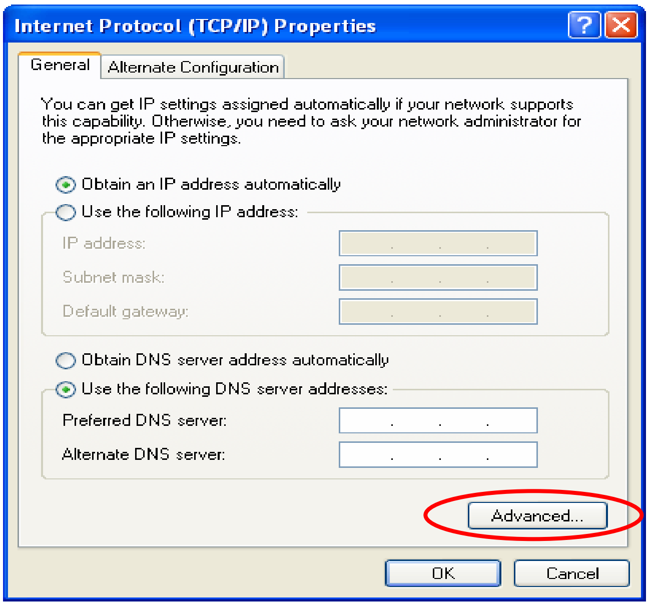
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

- Then, click ***Advanced*** in the window of **"Internet Protocol (TCP/IP)"**.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

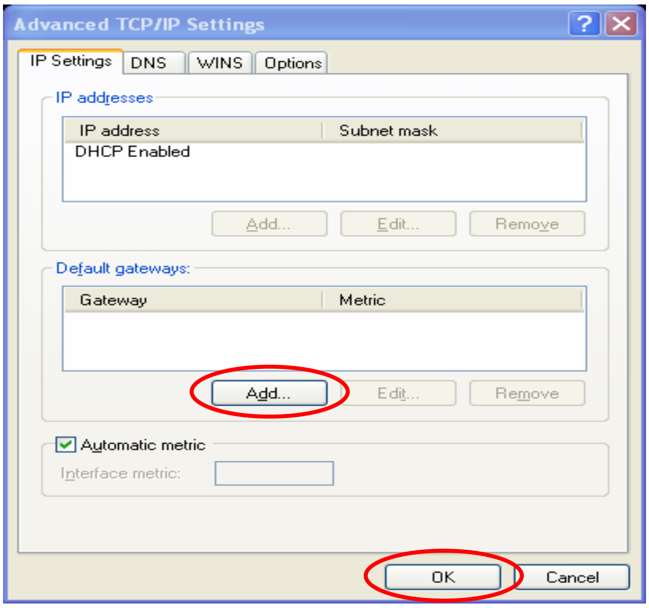
○ Obtain DNS server address automatically

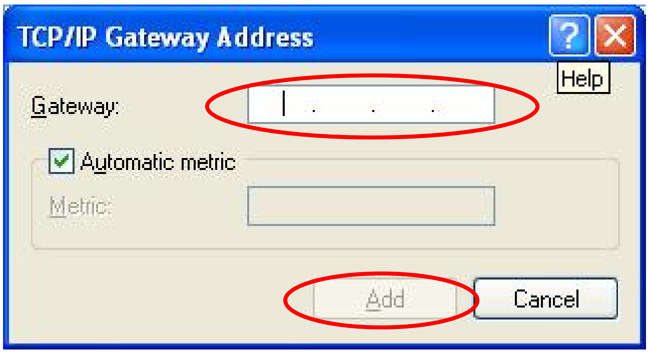
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

- Choose the **"IP Settings"** label and click **"Add"** below the **"Default Gateways"** column and the **"TCP/IP Gateway Address"** window will appear. Enter the gateway address of MW-2000S in the **"Gateway"** of **"TCP/IP Gateway Address"** window, and then click ***Add***. After back to the **"IP Settings"** label, click ***OK*** to finish.

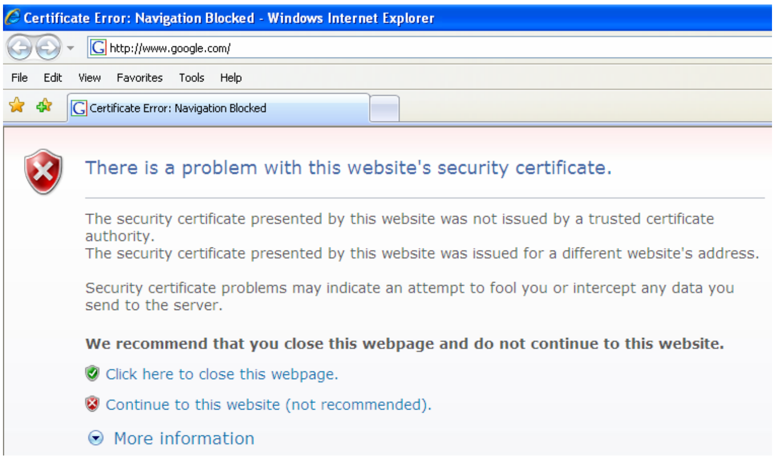




Appendix B: An Example of User Login

Normally, users will be authenticated before they get network access through MW-2000S. This section presents the basic authentication flow for end users. Please make sure that the MW-2000S 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 MW-2000S is not using a trusted SSL certificate (for more information, please see *4.2.4 Additional Configuration*), there will be a "Certificate Error", because the browser treats MW-2000S as an illegal website.



Certificate Error: Navigation Blocked - Windows Internet Explorer

http://www.google.com/

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

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

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

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

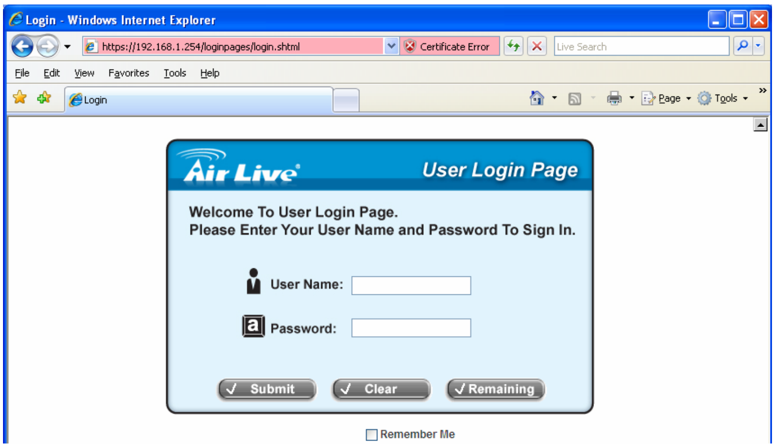
Click here to close this webpage.

Continue to this website (not recommended).

More information

File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked

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



Login - Windows Internet Explorer

https://192.168.1.254/loginpages/login.shtml

User Login Page

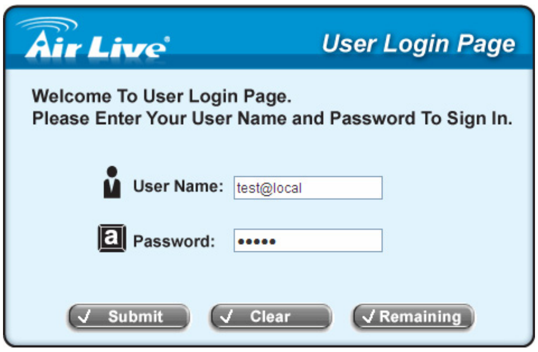
Welcome To User Login Page.
Please Enter Your User Name and Password To Sign In.

User Name:

Password:

□ Remember Me

2) Enter the username and password (for example, we use a local user account: test@local here) and then click ***Submit*** button.



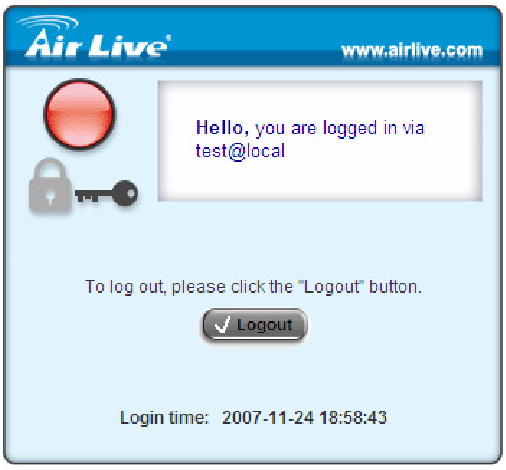
User Login Page

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

User Name: test@local

Password: •••••

3) Successful! Now you can start using the network. The “Starting Browsing” button will take you to the website where you originally want to visit or the home page that is configured in the system.



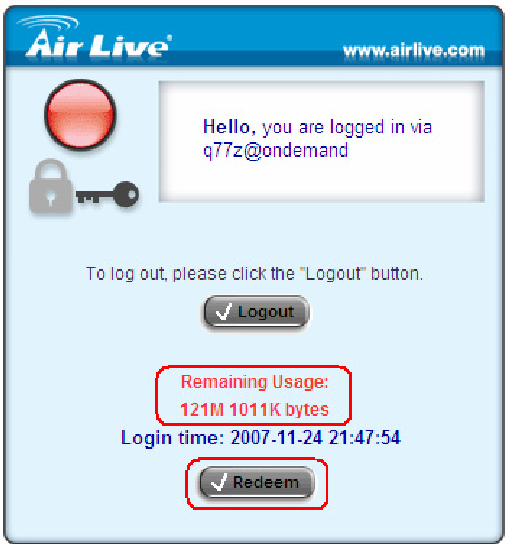
Hello, you are logged in via test@local

To log out, please click the "Logout" button.

Login time: 2007-11-24 18:58:43

Note: When On-demand accounts are used (for example, we use q77z@ondemand here), the system will display more information, as shown below.

- **Remaining usage:** The remaining quota of this On-demand account that the user can surf the Internet.



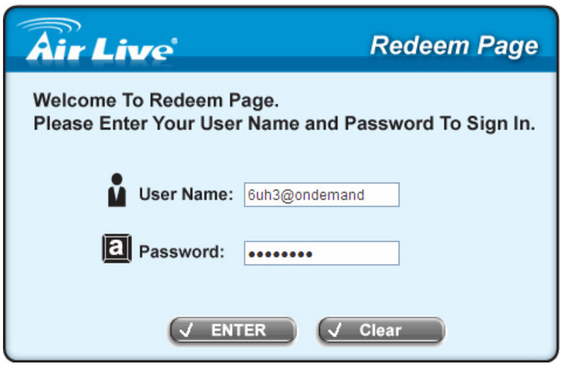
Hello, you are logged in via q77z@ondemand

To log out, please click the "Logout" button.

Remaining Usage:
121M 1011K bytes

Login time: 2007-11-24 21:47:54

- **Redeem**: When the remaining quota is insufficient, the user can add up the quota by purchasing an additional account. Please enter the new username (for example, we use 6uh3@ondemand here) and password in the Redeem Page and click ENTER button to merge the two accounts so that there will be more quota for the original account (in this case, we add up additional quota of 200M bytes).

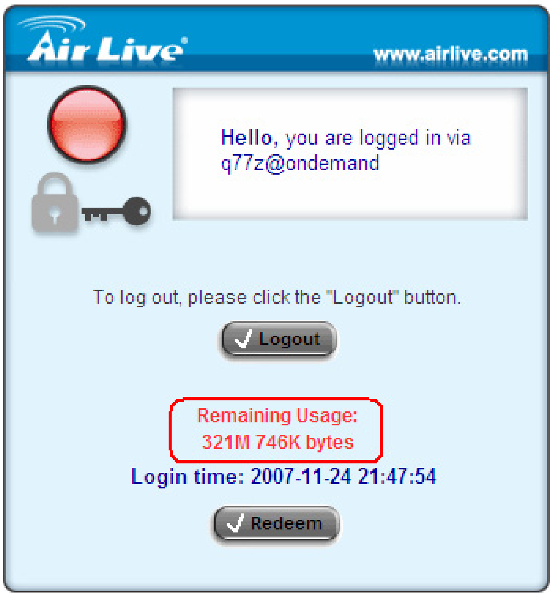


Redeem Page

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

User Name: 6uh3@ondemand

Password: ••••••••



Hello, you are logged in via q77z@ondemand

To log out, please click the "Logout" button.

Remaining Usage: 321M 746K bytes

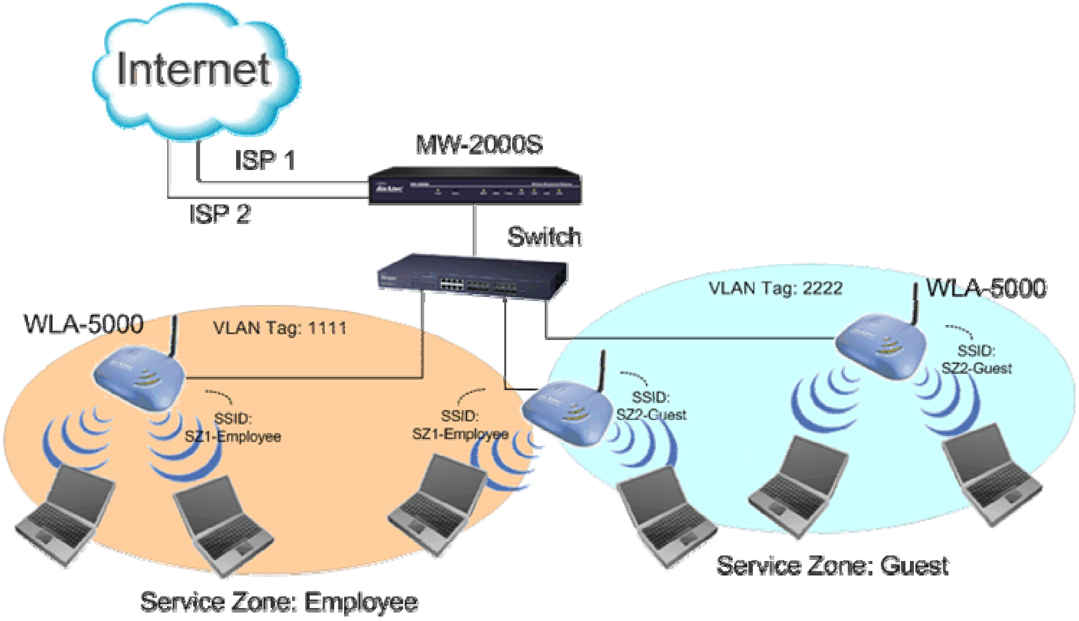
Login time: 2007-11-24 21:47:54

Note: *The maximum session time/data transfer is 24305 days/9,999,999 Mbyte. If the redeem amount exceeds this number, the system will automatically reject the redeem process.*

Appendix C: A Deployment Example of Service Zones

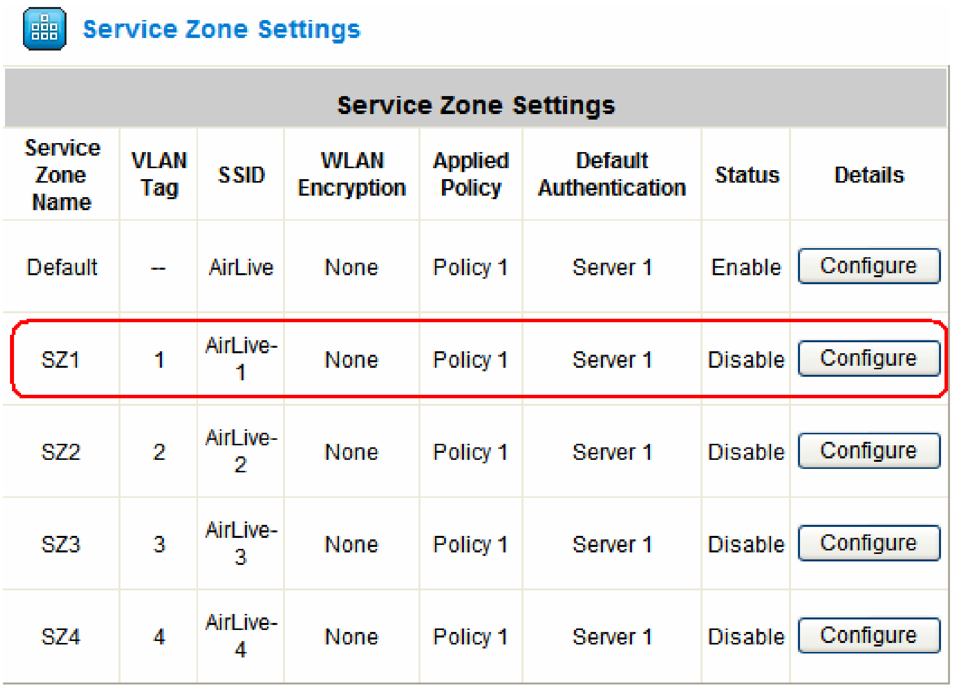
- **Typical Application Scenario: Employee vs. Guest**
  In this scenario, users are separated into **Employee** and **Guest** for the purpose of different levels of access control.

- **Application Network Diagram:**
  One Service Zone (associated with VLAN tag: 1111 and SSID: SZ1-Employee) is set up for employees while the other Service Zone (associated with VLAN tag: 2222 and SSID: SZ1-Guest) is set up for guests.



- **Requirements for the Application Scenario :**
  1. No matter where they stay in the office, all users should be divided into two groups (**Employee** and **Guest**) for the purpose of authentication differences.
  2. Each service zone must setup its own **SSID** to let users to access the wireless network using the specific SSID. The system will give a unique Session ID to authenticated users when they start new sessions.
  3. Both groups of **Employees** and **Guests** will be redirected to different login portal pages and will be authenticated against different authentication database.
  4. Apply different access control policies to seperated groups **Employee** and **Guests**.

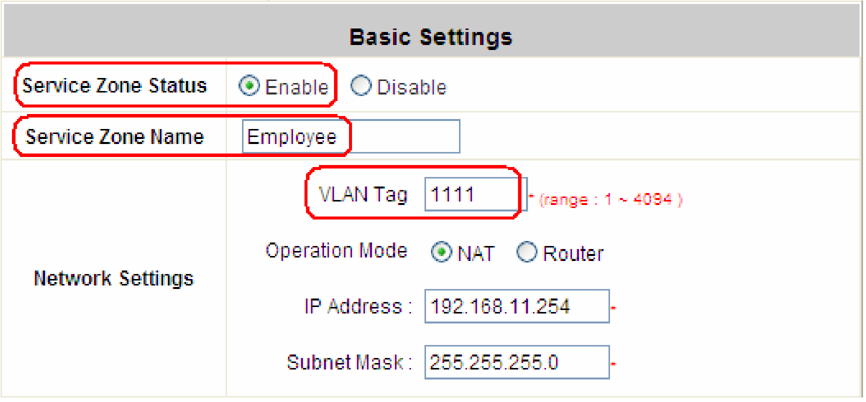
- **Solution and Configuration in MW-2000S**
  1. Choose the SZ1 for the **Employee** group (Take **Employee** for an example of Service Zone configuration)



Service Zone Settings

Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default	--	AirLive	None	Policy 1	Server 1	Enable	Configure
SZ1	1	AirLive-1	None	Policy 1	Server 1	Disable	Configure
SZ2	2	AirLive-2	None	Policy 1	Server 1	Disable	Configure
SZ3	3	AirLive-3	None	Policy 1	Server 1	Disable	Configure
SZ4	4	AirLive-4	None	Policy 1	Server 1	Disable	Configure

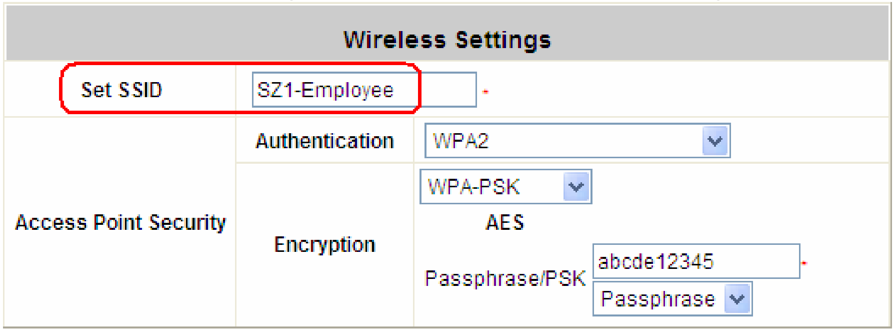
2. Enable the **Service Zone** and set up other basic information



Basic Settings

Service Zone Status	● Enable ○ Disable
Service Zone Name	Employee
Network Settings	VLAN Tag 1111 * (range : 1 ~ 4094) Operation Mode ● NAT ○ Router IP Address : 192.168.11.254 * Subnet Mask : 255.255.255.0 *

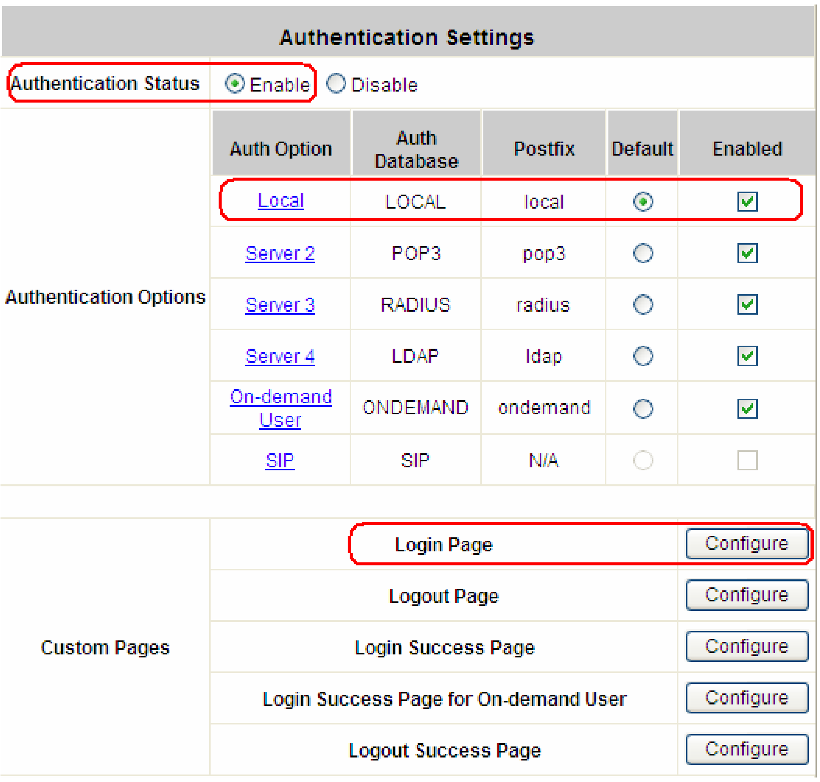
3. Configure the **SSID** and other settings which will be applied to the managed APs in this Service Zone



Wireless Settings

Set SSID	SZ1-Employee *	
Access Point Security	Authentication	WPA2
	Encryption	WPA-PSK AES Passphrase/PSK abcde12345 * Passphrase

4. Enable the Authentication Status, select the default Authentication Option and customize the Login Page and other pages



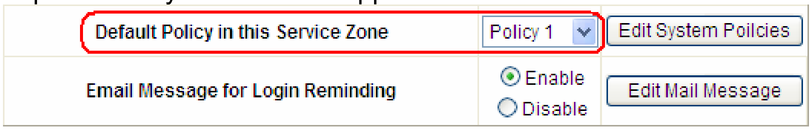
Authentication Settings

Authentication Status ● Enable ○ Disable

	Auth Option	Auth Database	Postfix	Default	Enabled
Authentication Options	Local	LOCAL	local	●	☑
	Server 2	POP3	pop3	○	☑
	Server 3	RADIUS	radius	○	☑
	Server 4	LDAP	ldap	○	☑
	On-demand User	ONDEMAND	ondemand	○	☑
	SIP	SIP	N/A	○	□

Custom Pages	Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Success Page for On-demand User	Configure
	Logout Success Page	Configure

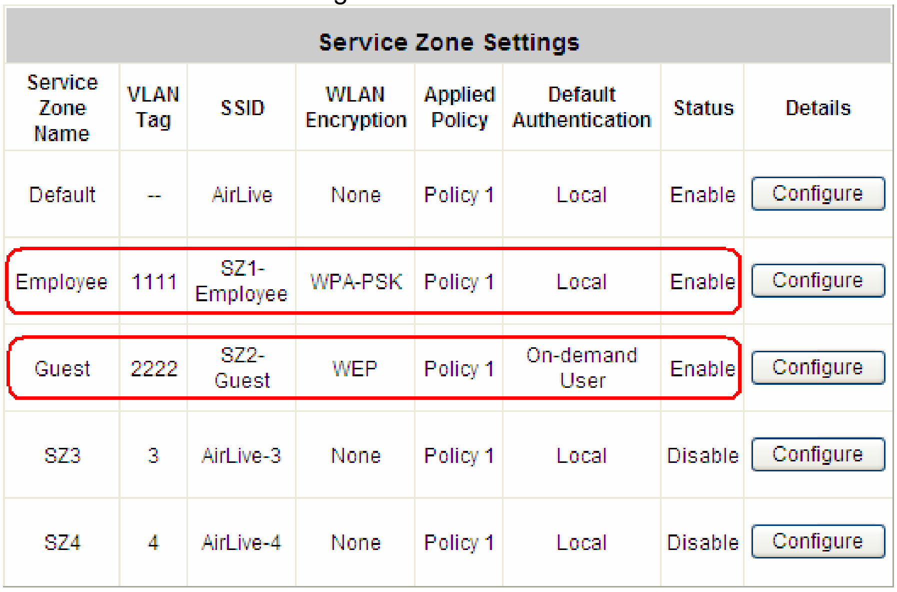
5. Choose the appropriate Policy which will be applied to this **Service Zone**



Default Policy in this Service Zone	Policy 1	Edit System Poilcies
Email Message for Login Reminding	● Enable ○ Disable	Edit Mail Message

- **Finished Configuration – Service Zone Settings**

The table will summarize the current configuration and status for each Service Zone:

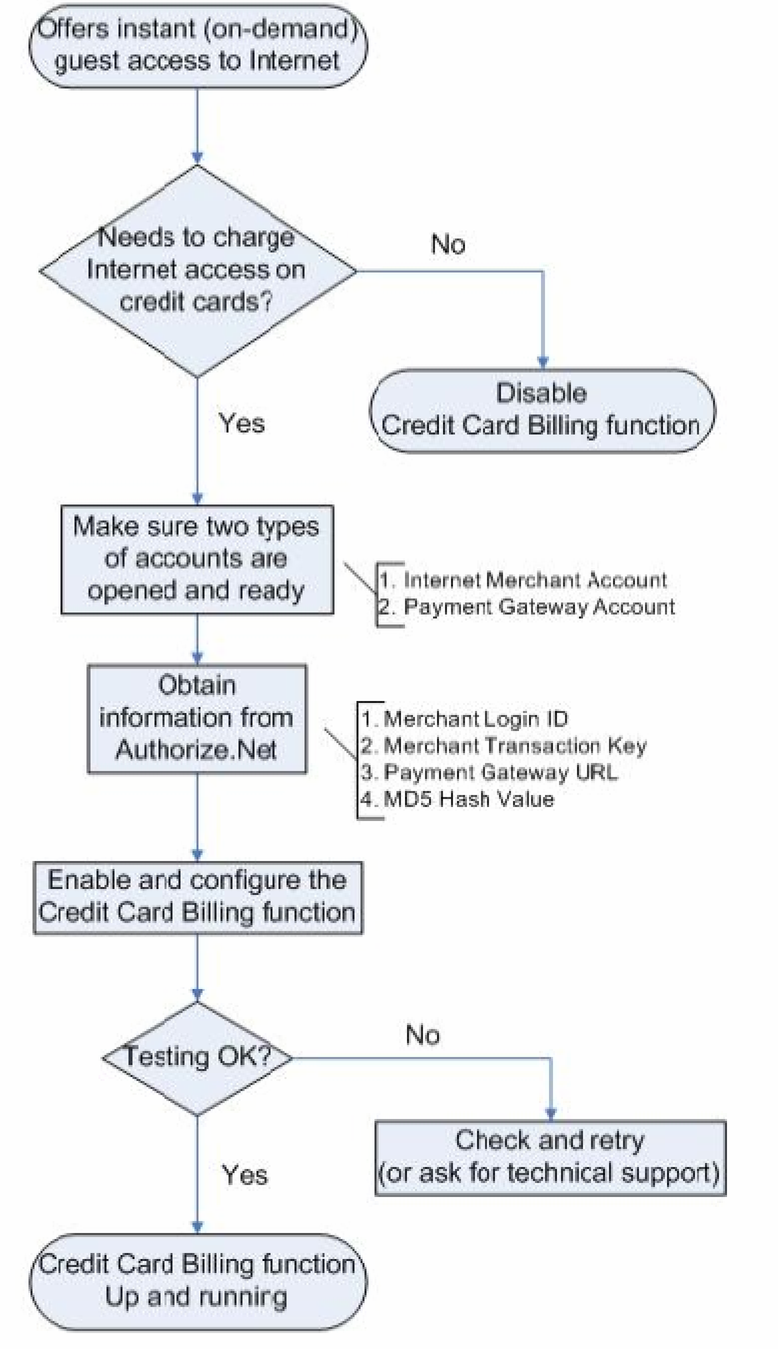


Service Zone Settings

Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default	--	AirLive	None	Policy 1	Local	Enable	Configure
Employee	1111	SZ1-Employee	WPA-PSK	Policy 1	Local	Enable	Configure
Guest	2222	SZ2-Guest	WEP	Policy 1	On-demand User	Enable	Configure
SZ3	3	AirLive-3	None	Policy 1	Local	Disable	Configure
SZ4	4	AirLive-4	None	Policy 1	Local	Disable	Configure

Appendix D: Accepting Payments via Authorize.Net

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

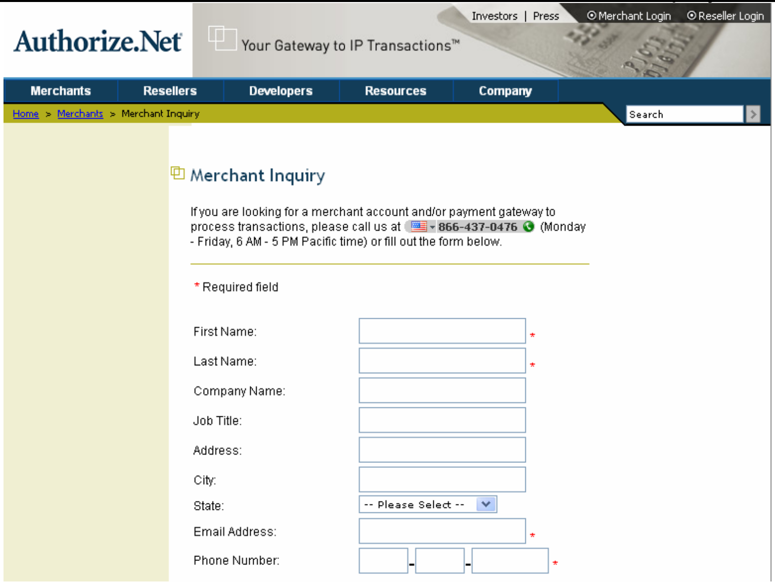

Offers instant (on-demand) guest access to Internet
Needs to charge Internet access on credit cards?
No
Disable Credit Card Billing function
Yes
Make sure two types of accounts are opened and ready
1. Internet Merchant Account
2. Payment Gateway Account
Obtain information from Authorize.Net
1. Merchant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

1. Setting Up

1.1 Open Accounts

To set up MW-2000S to process credit card billing, the merchant owner will need two accounts (Internet Merchant account and Authorize.Net account).

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



Merchant Inquiry

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

* Required field

First Name: *

Last Name: *

Company Name:

Job Title:

Address:

City:

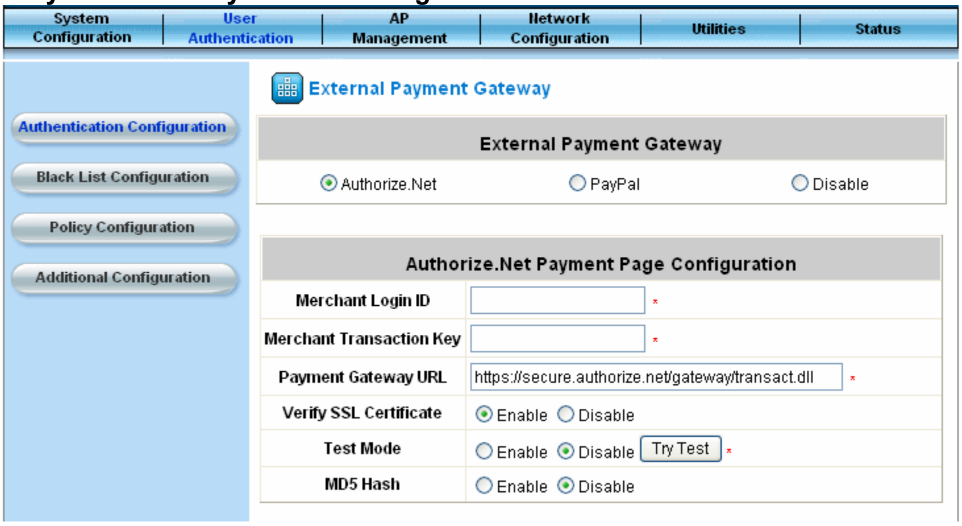
State: -- Please Select --

Email Address: *

Phone Number: - - *

1.2 Configure MW-2000S using an Authorize.Net account

Please log in MW-2000S. **User Authentication → Authentication Configuration →** Click the server ***On-demand User* → External Payment Gateway →** Click ***Configure*** **→** Select ***Authorize.Net***



External Payment Gateway

External Payment Gateway

● Authorize.Net ○ PayPal ○ Disable

Authorize.Net Payment Page Configuration

Merchant Login ID	*
Merchant Transaction Key	*
Payment Gateway URL	https://secure.authorize.net/gateway/transact.dll *
Verify SSL Certificate	● Enable ○ Disable
Test Mode	○ Enable ● Disable Try Test *
MD5 Hash	○ Enable ● Disable

Some major fields are required:

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

Note: For detailed description, please see 4.2.1.6 ONDEMAND Authentication

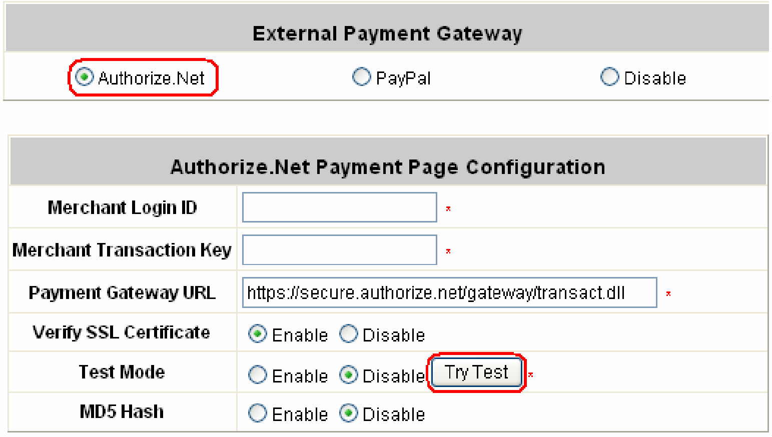
1.3 Configure the Authorize.Net Merchant Account to Match the Configuration of MW-2000S

Settings of the merchant account on Authorize.Net should be matched with the configuration of MW-2000S:

Setting	Description
MD5 Hash	To configure **"MD5 Hash Value"**, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → click ***MD5 Hash*** → Enter **"New Hash Value"** & **"Confirm Hash Value"** → Click ***Submit***.
Required Card Code	If the **"Card Code"** is set up as a required field, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → click ***Card Code Verification*** → Check the ***Does NOT Match (N)*** box → Click ***Submit***.
Required Address Fields	After setting up the required address fields on the **"Credit Card Payment Page Billing Configuration"** section of MW-2000S, the same requirements must be set on Authorize.Net. To do so, please log in Authorize.Net → Click ***Settings and Profile*** → Go to the **"Security"** section → click ***Address Verification System (AVS)*** → Check the boxes accordingly → Click ***Submit***.

1.4 Test The Credit Card Payment via Authorize.Net

To test the connection between MW-2000S and Authorize.Net, please log in MW-2000S. **User Authentication → Authentication Configuration** → Click the server ***On-demand User*** → **External Payment Gateway** → Click ***Configure*** → Select ***Authorize.Net*** →Go to "***Authorize.Net Payment Page Configuration***" section → Enable the **"Test Mode"** → Click ***Try Test*** and follow the instructions



External Payment Gateway

● Authorize.Net ○ PayPal ○ Disable

Authorize.Net Payment Page Configuration

Merchant Login ID	*
Merchant Transaction Key	*
Payment Gateway URL	https://secure.authorize.net/gateway/transact.dll *
Verify SSL Certificate	● Enable ○ Disable
Test Mode	○ Enable ● Disable Try Test *
MD5 Hash	○ Enable ● Disable

2. Basic Maintenance

In order to maintain the operation, merchant owners will have to manage the accounts and transactions via Authorize.Net as well as MW-2000S.

2.1 Void A Transaction and Remove the On-demand Account Created on MW-2000S

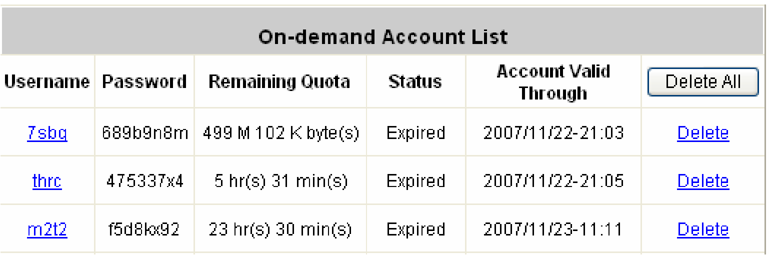
Sometimes, a transaction (as well as the related user account on MW-2000S) may have to be canceled before it has been settled with the bank.

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

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

b. To remove the specific account from MW-2000S, please log in MW-2000S. **User Authentication → Authentication Configuration** → Click the server ***On-demand User*** → ***On-demand Account List*** → Click ***View*** → Click ***Delete*** on the record with the account name.

c. Click ***Delete All*** to delete all users at once.



On-demand Account List

Username	Password	Remaining Quota	Status	Account Valid Through	Delete All
7sbq	689b9n8m	499 M 102 K byte(s)	Expired	2007/11/22-21:03	Delete
thrc	475337x4	5 hr(s) 31 min(s)	Expired	2007/11/22-21:05	Delete
m2t2	f5d8kx92	23 hr(s) 30 min(s)	Expired	2007/11/23-11:11	Delete

2.2 Refund A Settled Transaction and Remove the On-demand Account Generated on MW-2000S

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

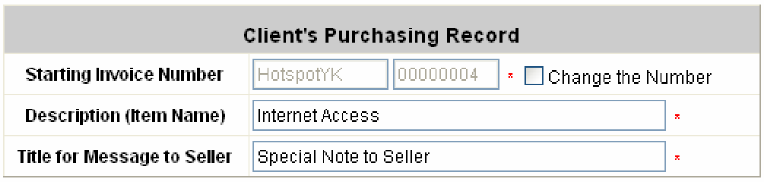
b. To remove the specific account from MW-2000S, please log in MW-2000S. ***User Authentication*** → ***Authentication Configuration*** → Click the server ***On-demand User*** → ***On-demand User Server Configuration*** → ***Users List*** → Click ***Delete*** on the record with the account name

2.3 Find the Username and Password for A Specific Customer

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

2.4 Send An Email Receipt to A Customer

If a valid email address is provided, MW-2000S will automatically send the customer an email receipt for each successful transaction via Authorize.Net. To change the information on the receipt for customer, please log in MW-2000S. **User Authentication** → **Authentication Configuration** → Click the server ***On-demand User*** → **External Payment Gateway** → Click ***Configure*** → Select ***Authorize.Net*** → Scroll down to ***Client's Purchasing Record*** section of the page → Type in information in the text boxes: **"Description (Item Name)"** → Confirm and click ***Apply***.



Client's Purchasing Record

Starting Invoice Number	HotspotYK 00000004 * □ Change the Number
Description (Item Name)	Internet Access *
Title for Message to Seller	Special Note to Seller *

2.5 Send An Email Receipt for Each Transaction to the Merchant Owner

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

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

3. Reporting

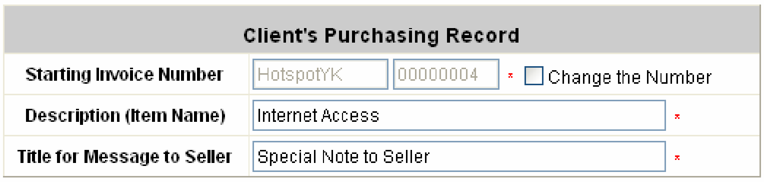
During normal operation, the following steps will be necessary to generate transaction reports.

3.1 Transaction Statistics by Credit Card Type during the Period

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

3.2 Transaction Statistics by Different Location

a. To deploy more than one MW-2000S, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in MW-2000S. **User Authentication → Authentication Configuration** → Click the server ***On-demand User*** → **External Payment Gateway** → Click ***Configure*** → Select ***Authorize.Net*** → Scroll down to **"Client's Purchasing Record"** section of the page → Check the **"Change the Number"** box → A location-specific ID (for example, Hotspot-A) can be used as the first part of **"Starting Invoice Number"** → Confirm and click ***Apply***.



Client's Purchasing Record

Starting Invoice Number	HotspotYK 00000004 * □ Change the Number
Description (Item Name)	Internet Access *
Title for Message to Seller	Special Note to Seller *

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

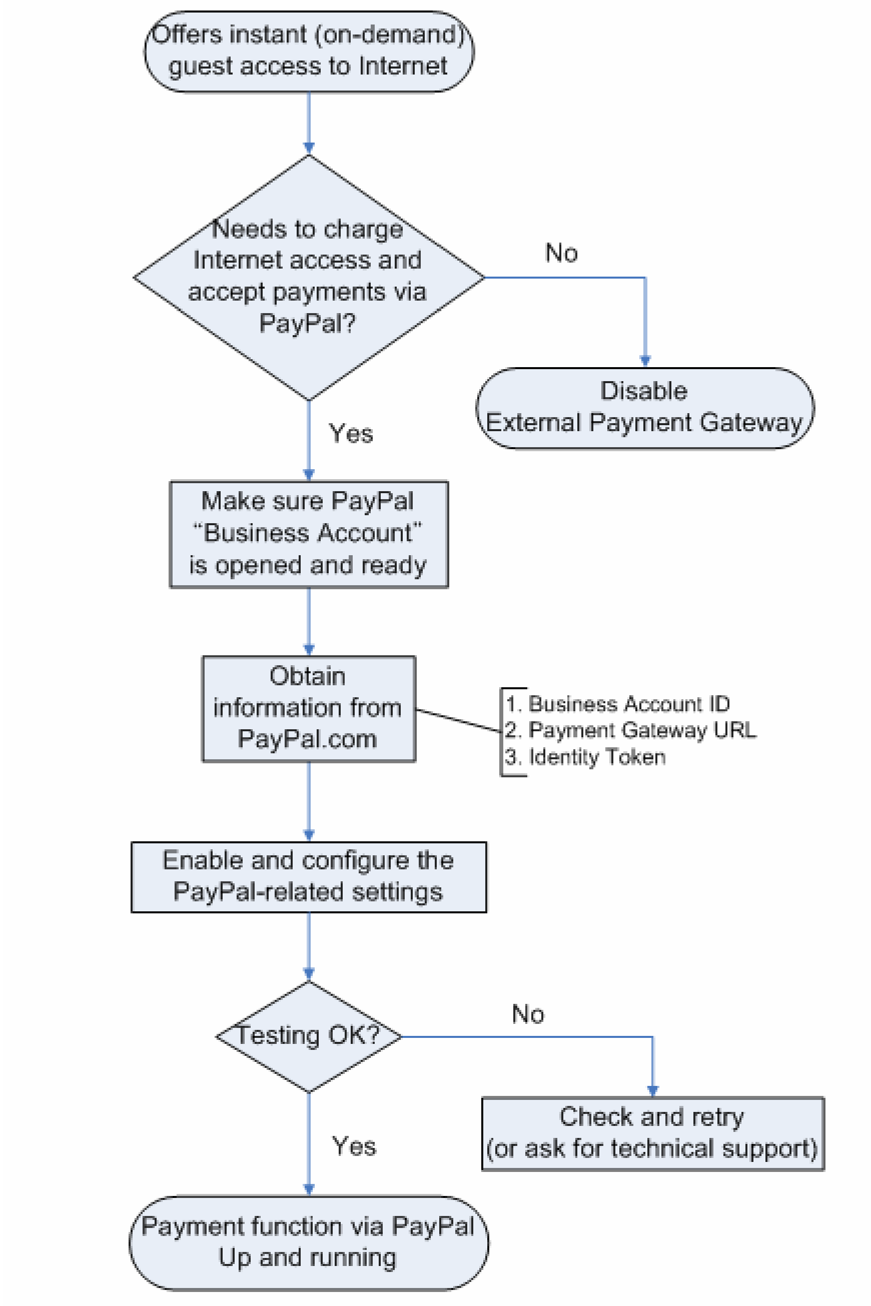
3.3 Search for The Transaction Details for A Specific Customer

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

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

Appendix E: Accepting Payments via PayPal

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

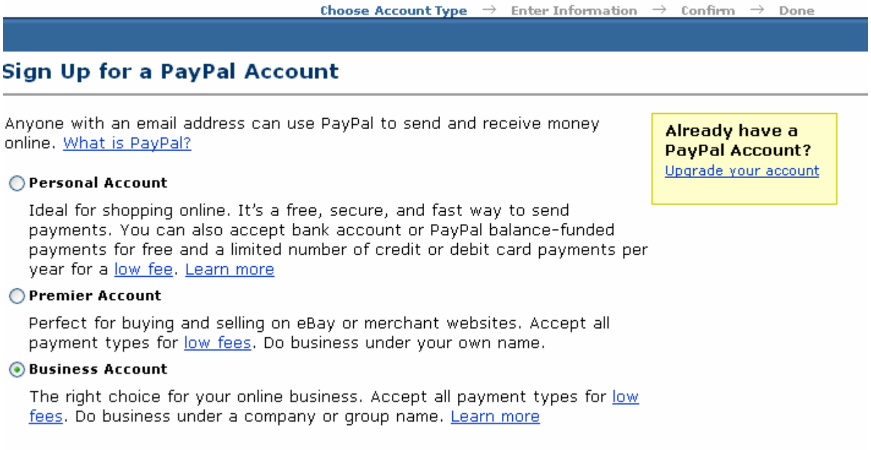

Offers instant (on-demand) guest access to Internet
Needs to charge Internet access and accept payments via PayPal?
No
Disable External Payment Gateway
Yes
Make sure PayPal "Business Account" is opened and ready
Obtain information from PayPal.com
1. Business Account ID
2. Payment Gateway URL
3. Identity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

1. Setting Up

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

1.1 Open An Account

Step 1: Sign up for a PayPal Business Account and login.
Here is a link: https://www.paypal.com/cgi-bin/webscr?cmd=_registration-run



Choose Account Type → Enter Information → Confirm → Done

Sign Up for a PayPal Account

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

Already have a PayPal Account?
Upgrade your account

○ **Personal Account**

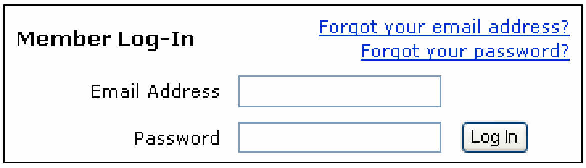
Ideal for shopping online. It's a free, secure, and fast way to send payments. You can also accept bank account or PayPal balance-funded payments for free and a limited number of credit or debit card payments per year for a low fee. Learn more

○ **Premier Account**

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

● **Business Account**

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



Member Log-In

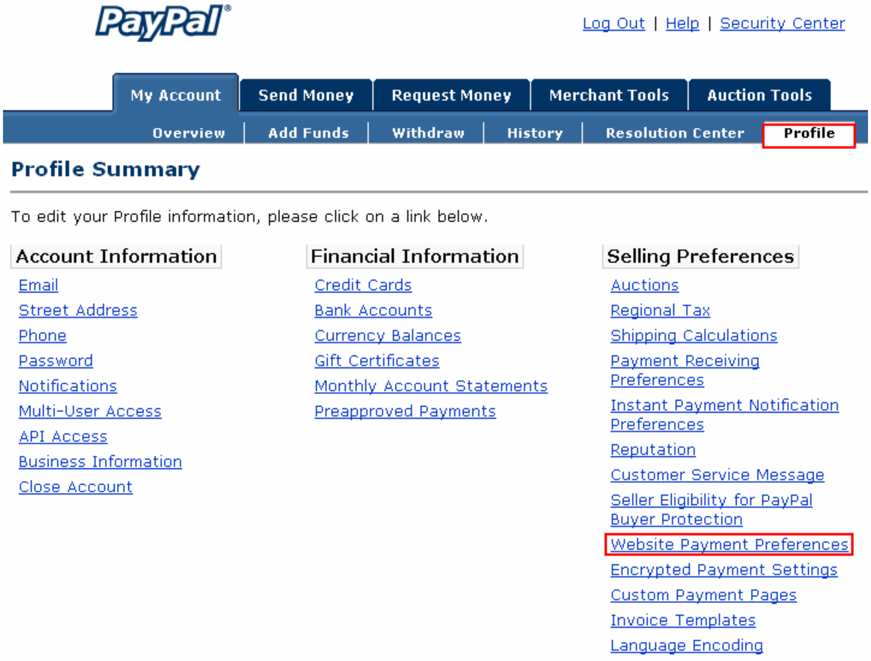
Forgot your email address?
Forgot your password?

Email Address

Password

Log In

Step 2: Edit necessary settings in "Website Payment Preferences"
Click **Profile** → Click **Website Payment Preferences** in the **Selling Preferences** section



Log Out | Help | Security Center

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

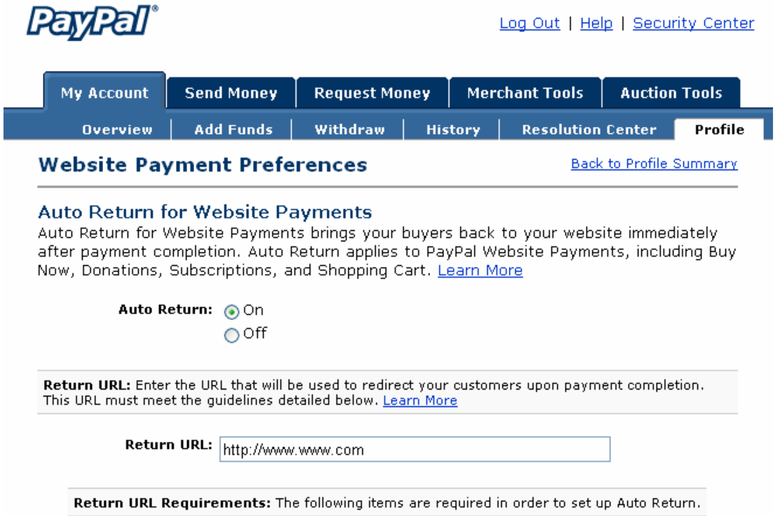
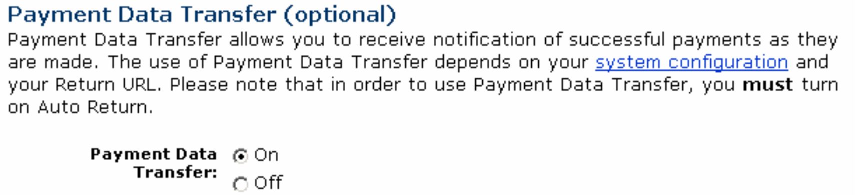
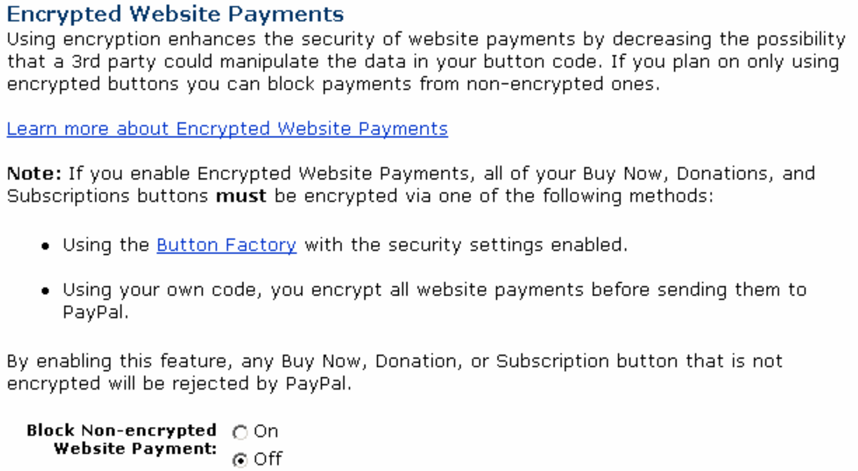
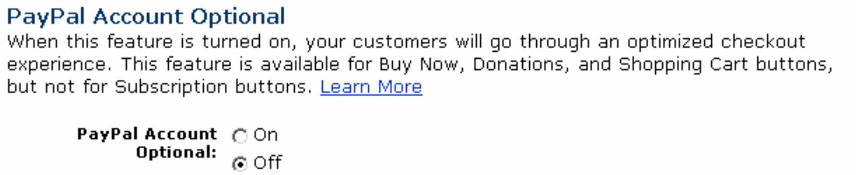
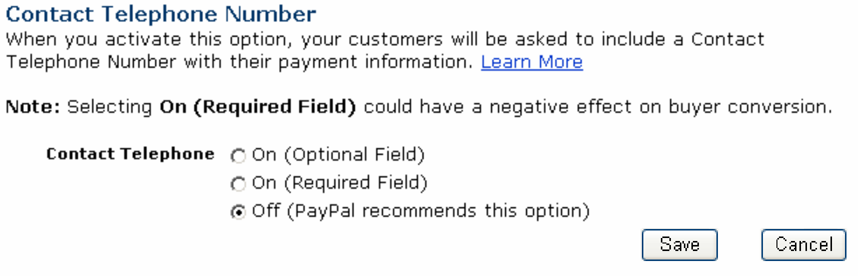
Overview | Add Funds | Withdraw | History | Resolution Center | Profile

Profile Summary

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

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

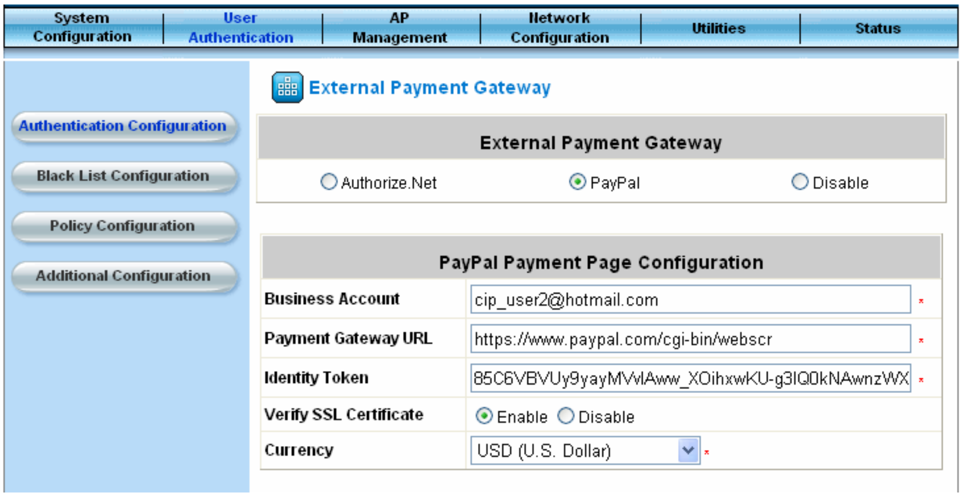
Administrators should scroll down to edit each setting as shown in the table below. To activate all the changes, please click ***Save*** at the end of the page.

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

1.2 Configure MW-2000S with a PayPal Business Account

Please log in MW-2000S:

User Authentication → Authentication Configuration → Click the server ***On-demand User*** **→ External Payment Gateway →** Click ***Configure*** → Select ***PayPal***



External Payment Gateway

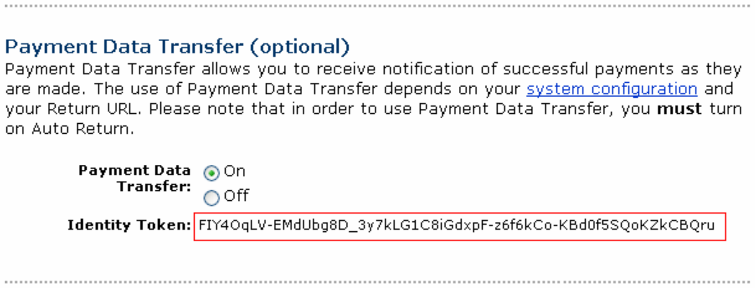
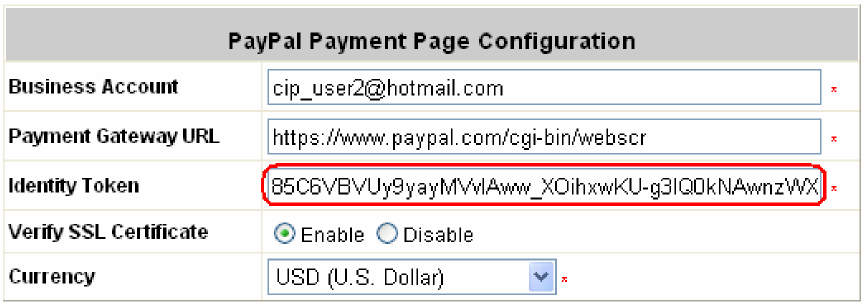
External Payment Gateway

○ Authorize.Net ● PayPal ○ Disable

PayPal Payment Page Configuration

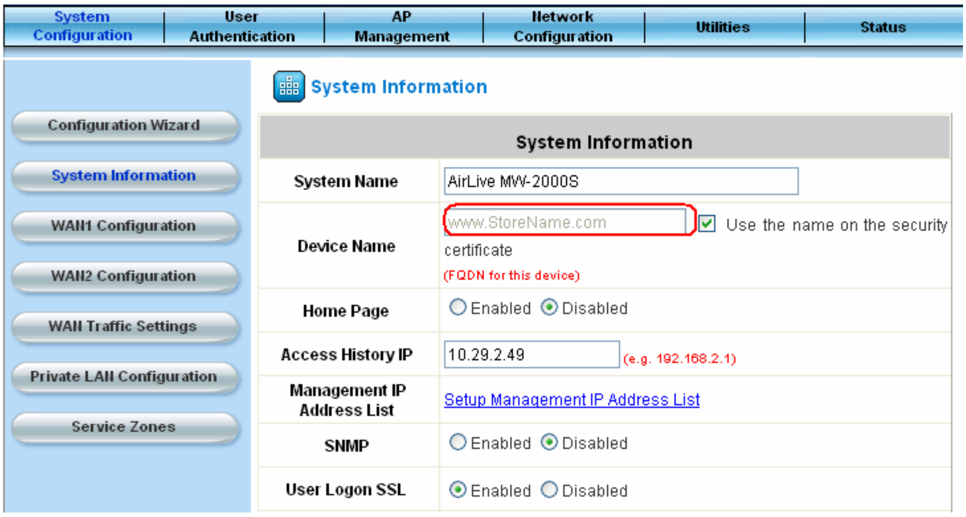
Business Account	cip_user2@hotmail.com *
Payment Gateway URL	https://www.paypal.com/cgi-bin/webscr *
Identity Token	85C6VBVUy9yayMVvlAww_XOihxwKU-g3lQ0kNAwnzWX *
Verify SSL Certificate	● Enable ○ Disable
Currency	USD (U.S. Dollar) *

Three fields are required:

Setting	Description
Business Account ID	This is the “Login ID” (email address) that is associated with the PayPal Business Account.
Payment Gateway URL	https://www.paypal.com/cgi-bin/webscr (default URL for PayPal)
Identity Token	Please log in PayPal after saving the above settings → Click **Profile** → Click **Website Payment Preferences** in the **Selling Preferences** section → Scroll down to the section, **Payment Data Transfer (optional)**.  Payment Data Transfer (optional) Payment Data Transfer allows you to receive notification of successful payments as they are made. The use of Payment Data Transfer depends on your system configuration and your Return URL. Please note that in order to use Payment Data Transfer, you **must** turn on Auto Return. **Payment Data Transfer:** ● On ○ Off **Identity Token:** FIY4OqLV-EMdUbg8D_3y7kLG1C8iGdxpF-z6f6kCo-KBd0f5SQoKZkCBQru Copy the **Identity Token** in the above page to the section “**PayPal Payment Page Configuration**” of MW-2000S.  PayPal Payment Page Configuration Business Account: cip_user2@hotmail.com * Payment Gateway URL: https://www.paypal.com/cgi-bin/webscr * Identity Token: 85C6VBVUy9yayMVvlAww_XOihxwKU-g3lQ0kNAwnzWX * Verify SSL Certificate: ● Enable ○ Disable Currency: USD (U.S. Dollar) *

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

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



System Information

System Information	
System Name	AirLive MW-2000S
Device Name	www.StoreName.com ☑ Use the name on the security certificate (FQDN for this device)
Home Page	○ Enabled ● Disabled
Access History IP	10.29.2.49 (e.g. 192.168.2.1)
Management IP Address List	Setup Management IP Address List
SNMP	○ Enabled ● Disabled
User Logon SSL	● Enabled ○ Disabled

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

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

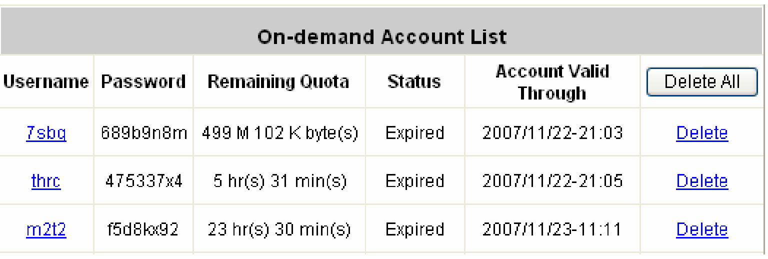
2. Basic Maintenance

In order to maintain the operation, the merchant owner will have to manage the accounts and payment transactions on PayPal website as well as MW-2000S.

2.1 Refund a completed payment and remove the on-demand account generated on MW-2000S

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

b. To remove the specific account from MW-2000S, please log in MW-2000S: **User Authentication** → **Authentication Configuration** → Click the server ***On-demand User*** → ***On-demand Account List*** → Click ***View*** → Click ***Delete*** on the record with the account ID. Click ***Delete All*** to delete all users at once



On-demand Account List

Username	Password	Remaining Quota	Status	Account Valid Through	Delete All
7sbq	689b9n8m	499 M 102 K byte(s)	Expired	2007/11/22-21:03	Delete
thrc	475337x4	5 hr(s) 31 min(s)	Expired	2007/11/22-21:05	Delete
m2t2	f5d8kx92	23 hr(s) 30 min(s)	Expired	2007/11/23-11:11	Delete

2.2 Find the username and password for a specific customer

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

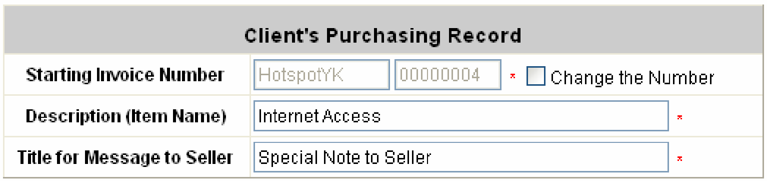
b. To find the password associated with a specific username, please log in MW-2000S: **User Authentication** → **Authentication Configuration** → Click the server ***On-demand User*** → ***On-demand Account List*** → Click ***View***. Search for the specific username. Password can be found in the same record

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

2.3 Send an email receipt to a customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via PayPal. To change the information on the receipt for customer, please log in MW-2000S:
User Authentication → **Authentication Configuration** → Click the server ***On-demand User*** → **External**

Payment Gateway → Click ***Configure*** → Select ***PayPal*** → Go to "**Client's Purchasing Record**" section → Type in information in the text boxes: **Invoice Number** and **Description (Item Name)** → Confirm and click ***Apply***



Client's Purchasing Record	
Starting Invoice Number	HotspotYK 00000004 * □ Change the Number
Description (Item Name)	Internet Access *
Title for Message to Seller	Special Note to Seller *

2.4 Send an email receipt for each transaction to the merchant

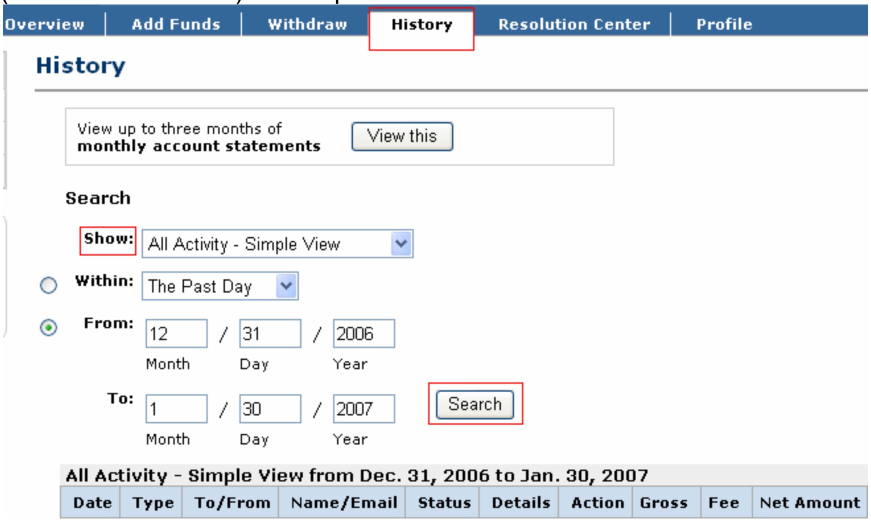
A copy of email receipt with payment details (including available message note from buyer) for each successful transaction will also be automatically sent to the merchant owner/administrator via PayPal.

3. Reporting

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

3.1 Transaction activity during a period

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



History

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

Search

Show: All Activity - Simple View

○ Within: The Past Day

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

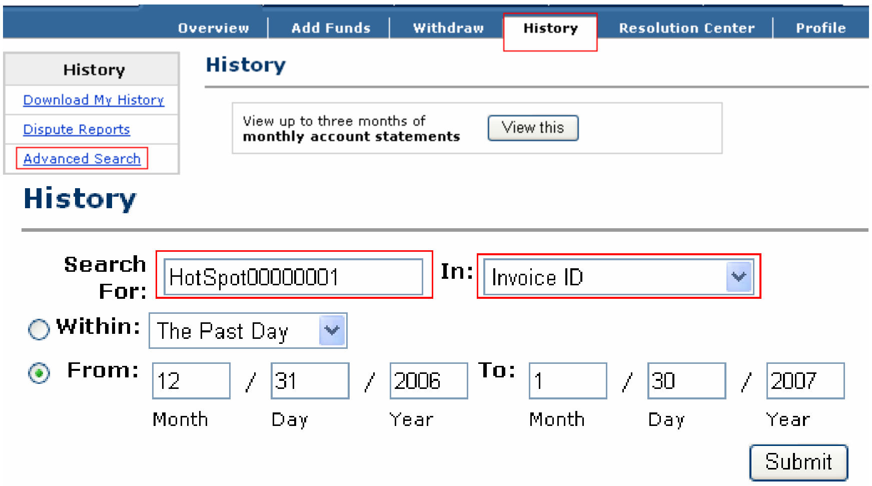
To: 1 / 30 / 2007 (Month / Day / Year)

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

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

3.2 Search for the transaction details for a specific customer

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



History

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

History

Search For: HotSpot00000001 In: Invoice ID

○ Within: The Past Day

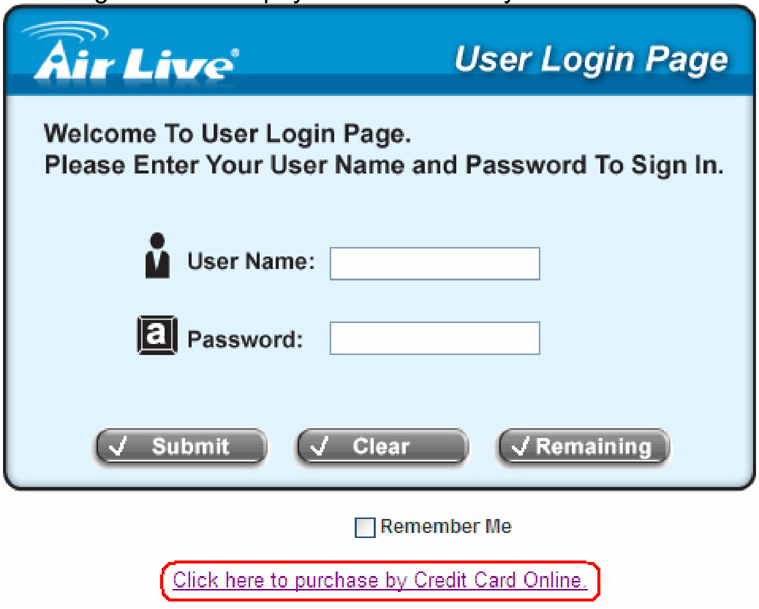
● From: 12 / 31 / 2006 (Month / Day / Year) To: 1 / 30 / 2007 (Month / Day / Year)

Note: *For more information about PayPal, please see http://www.paypal.com*

Appendix F: Examples of Making Payments for End Users

1. Making Payments via Authorize.Net

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



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

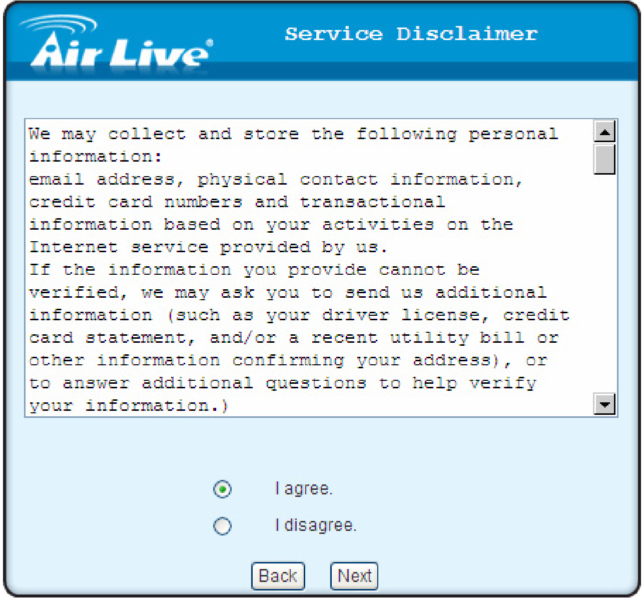
User Name:

Password:

□ Remember Me

Click here to purchase by Credit Card Online.

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

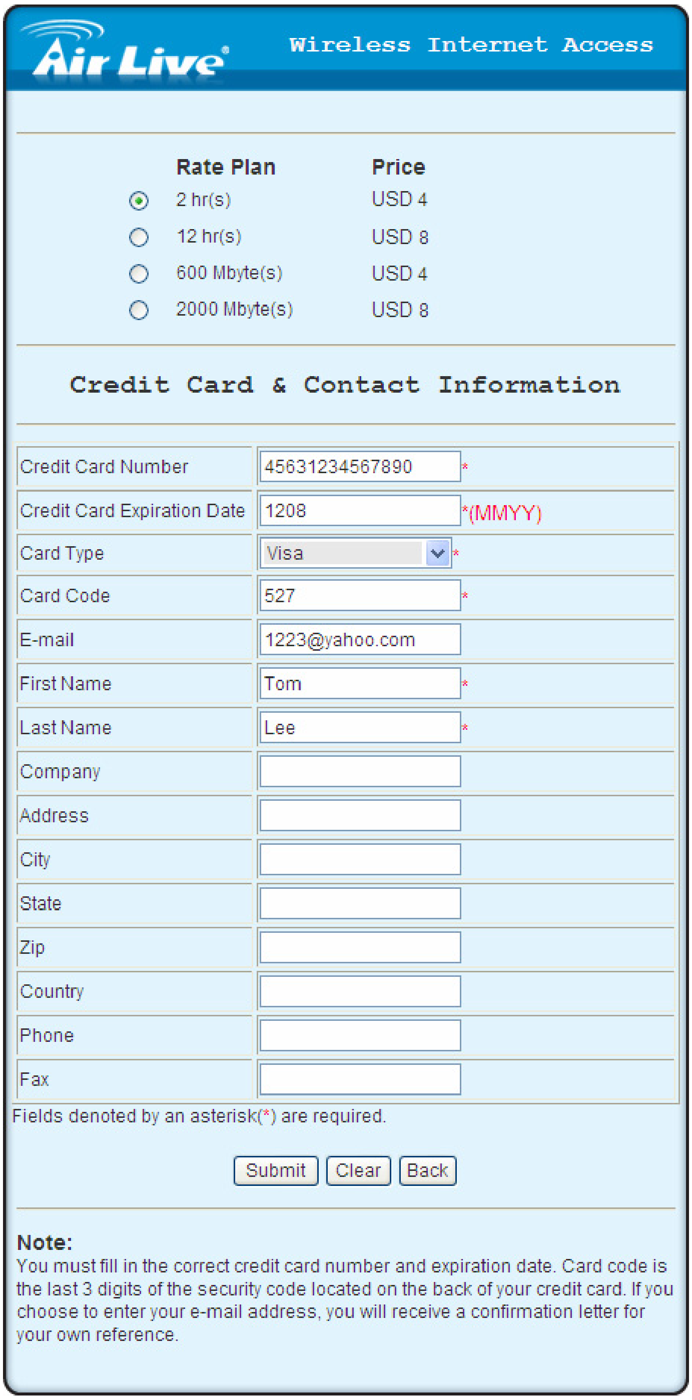


We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)

● I agree.

○ I disagree.

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



	Rate Plan	Price
●	2 hr(s)	USD 4
○	12 hr(s)	USD 8
○	600 Mbyte(s)	USD 4
○	2000 Mbyte(s)	USD 8

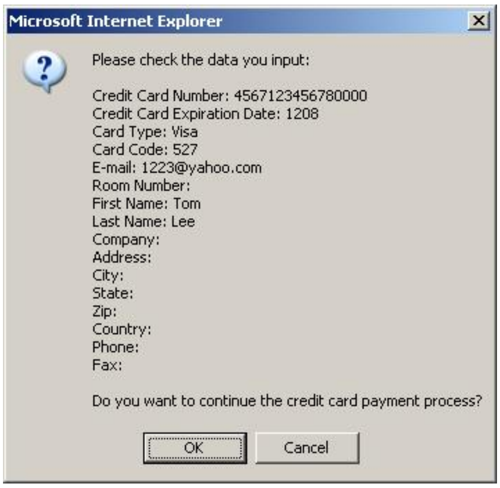
Credit Card & Contact Information

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

Fields denoted by an asterisk(*) are required.

Note:
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If you choose to enter your e-mail address, you will receive a confirmation letter for your own reference.

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

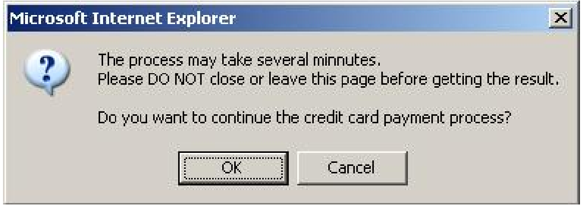


Please check the data you input:

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

Do you want to continue the credit card payment process?

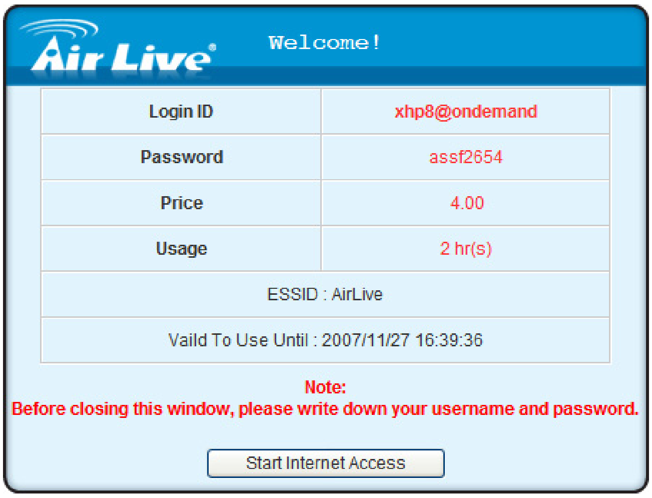
Step 5: Click ***OK*** to complete the process or click ***Cancel*** to revise the data or cancel this transaction.



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

Do you want to continue the credit card payment process?

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



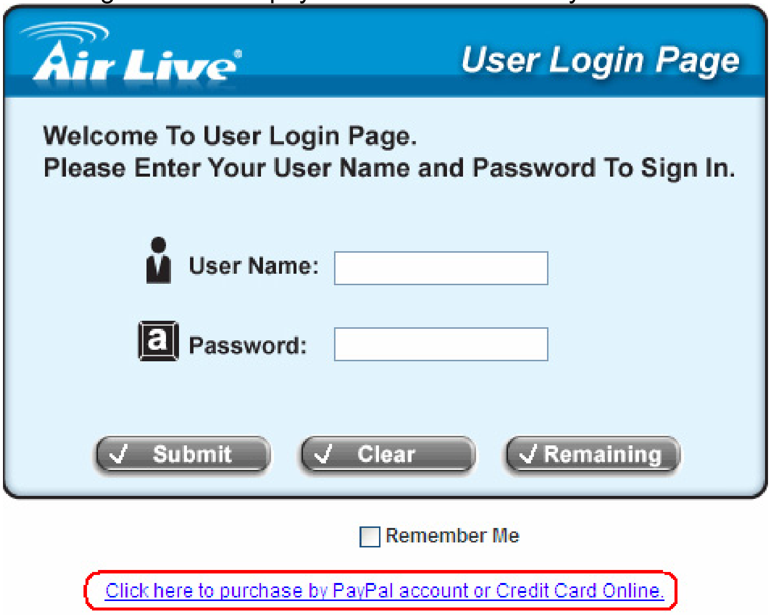
Login ID	xhp8@ondemand
Password	assf2654
Price	4.00
Usage	2 hr(s)
ESSID : AirLive	
Vaild To Use Until : 2007/11/27 16:39:36	

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

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

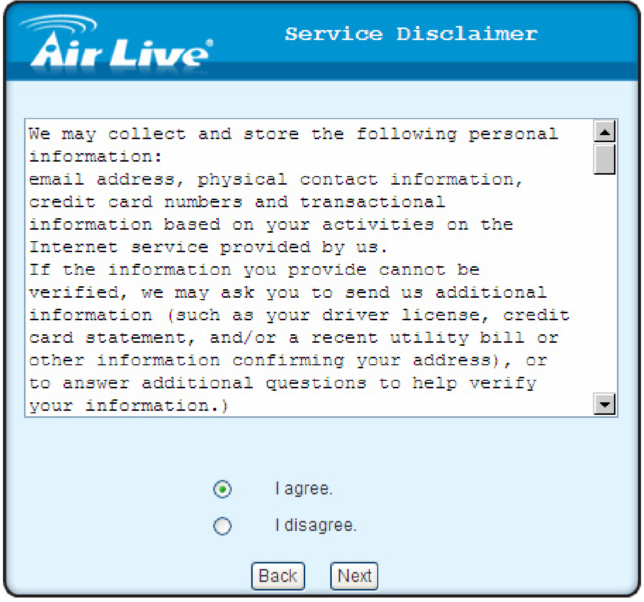
2. Making Payments via PayPal

Step 1: Click the link below the login window to pay for the service via PayPal.



Air Live
User Login Page
Welcome To User Login Page.
Please Enter Your User Name and Password To Sign In.
User Name:
Password:
Submit
Clear
Remaining
□ Remember Me
Click here to purchase by PayPal account or Credit Card Online.

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

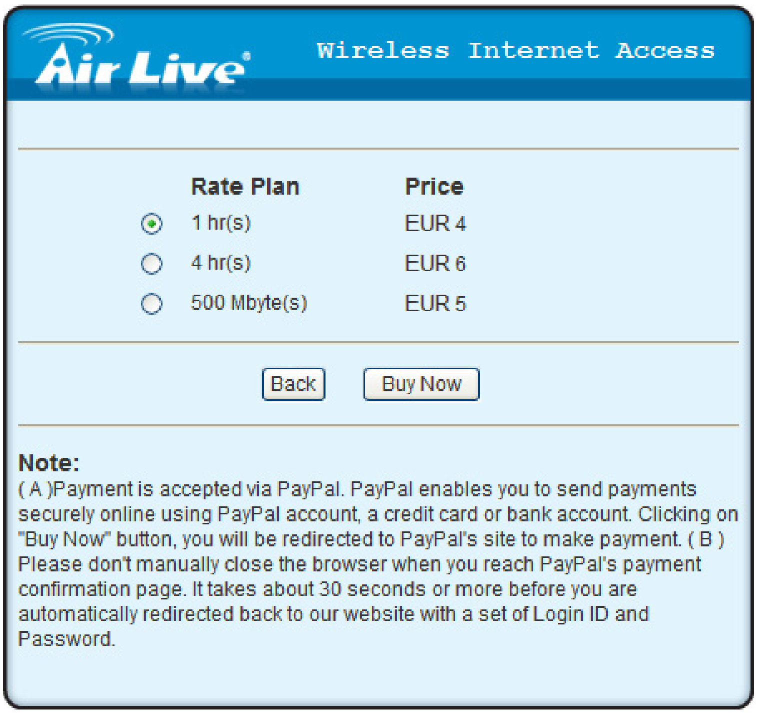


We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)

● I agree.

○ I disagree.

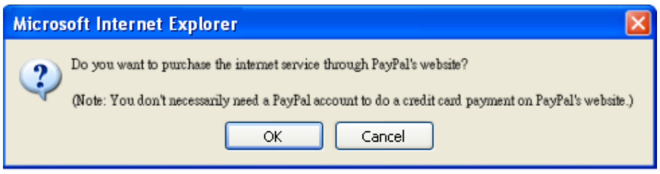
Step 3: Please fill out the form and Click ***Submit*** to send out this transaction. There will be a confirm dialog box.



Wireless Internet Access

	Rate Plan	Price
●	1 hr(s)	EUR 4
○	4 hr(s)	EUR 6
○	500 Mbyte(s)	EUR 5

Note:
(A)Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button, you will be redirected to PayPal's site to make payment. (B) Please don't manually close the browser when you reach PayPal's payment confirmation page. It takes about 30 seconds or more before you are automatically redirected back to our website with a set of Login ID and Password.

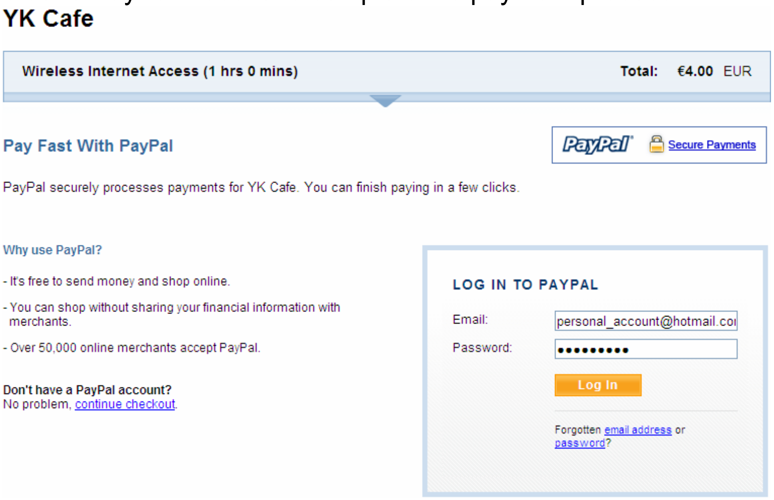


Microsoft Internet Explorer

Do you want to purchase the internet service through PayPal's website?

(Note: You don't necessarily need a PayPal account to do a credit card payment on PayPal's website.)

Step 4: You will be redirected to PayPal website to complete the payment process.



YK Cafe

Wireless Internet Access (1 hrs 0 mins) Total: €4.00 EUR

Pay Fast With PayPal

PayPal securely processes payments for YK Cafe. You can finish paying in a few clicks.

Why use PayPal?

- It's free to send money and shop online.
- You can shop without sharing your financial information with merchants.
- Over 50,000 online merchants accept PayPal.

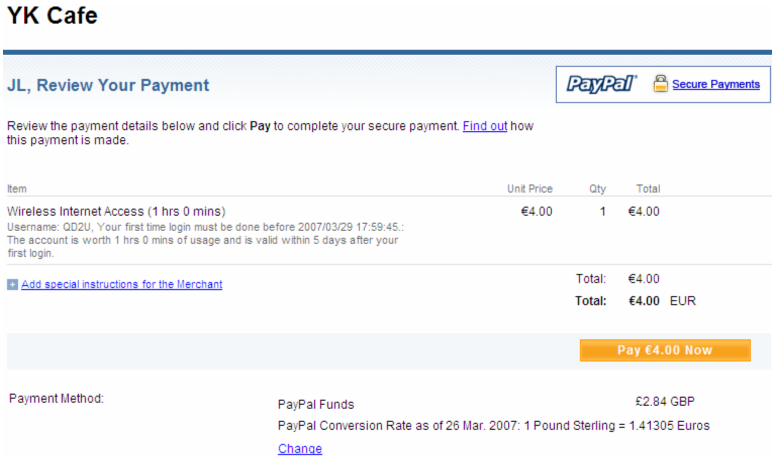
Don't have a PayPal account?
No problem, continue checkout.

LOG IN TO PAYPAL

Email: personal_account@hotmail.coı

Password: ●●●●●●●●●

Forgotten email address or password?



YK Cafe

JL, Review Your Payment

Review the payment details below and click **Pay** to complete your secure payment. Find out how this payment is made.

Item	Unit Price	Qty	Total
Wireless Internet Access (1 hrs 0 mins) Username: QD2U, Your first time login must be done before 2007/03/29 17:59:45.: The account is worth 1 hrs 0 mins of usage and is valid within 5 days after your first login.	€4.00	1	€4.00

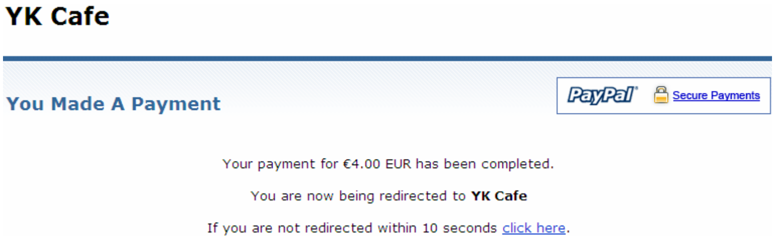
Add special instructions for the Merchant

Total: €4.00
Total: €4.00 EUR

Payment Method: PayPal Funds £2.84 GBP

PayPal Conversion Rate as of 26 Mar. 2007: 1 Pound Sterling = 1.41305 Euros

Change



YK Cafe

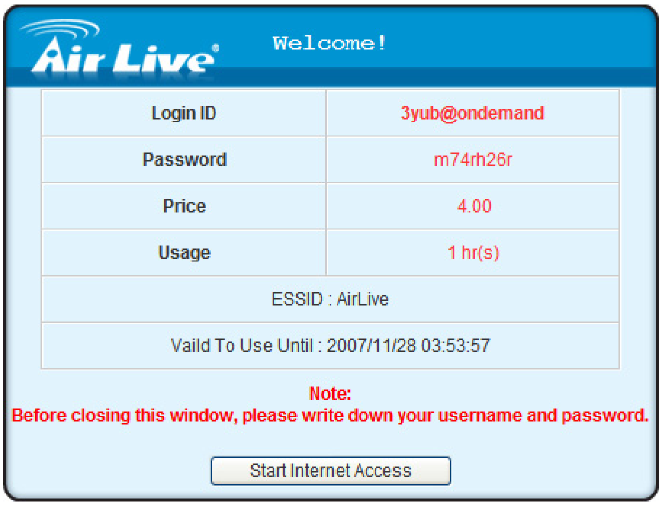
You Made A Payment

Your payment for €4.00 EUR has been completed.

You are now being redirected to **YK Cafe**

If you are not redirected within 10 seconds click here.

Step 5: Click ***Start Internet Access*** to use the Internet access service.



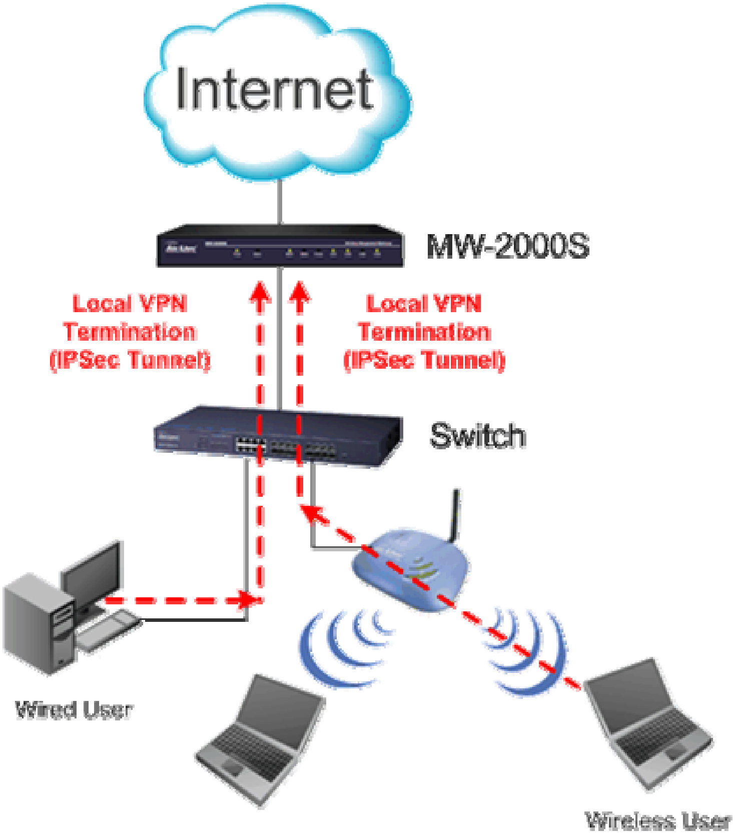
Login ID	3yub@ondemand
Password	m74rh26r
Price	4.00
Usage	1 hr(s)
ESSID : AirLive	
Vaild To Use Until : 2007/11/28 03:53:57	

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

Note:
Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on ***Buy Now*** *button, you will be redirected to PayPal's site to make payment. Please* ***do not manually close the browser*** *when you reach PayPal's payment confirmation page. It takes about 30 seconds or more before you are* ***automatically redirected back to our website with a set of Login ID and Password****.*

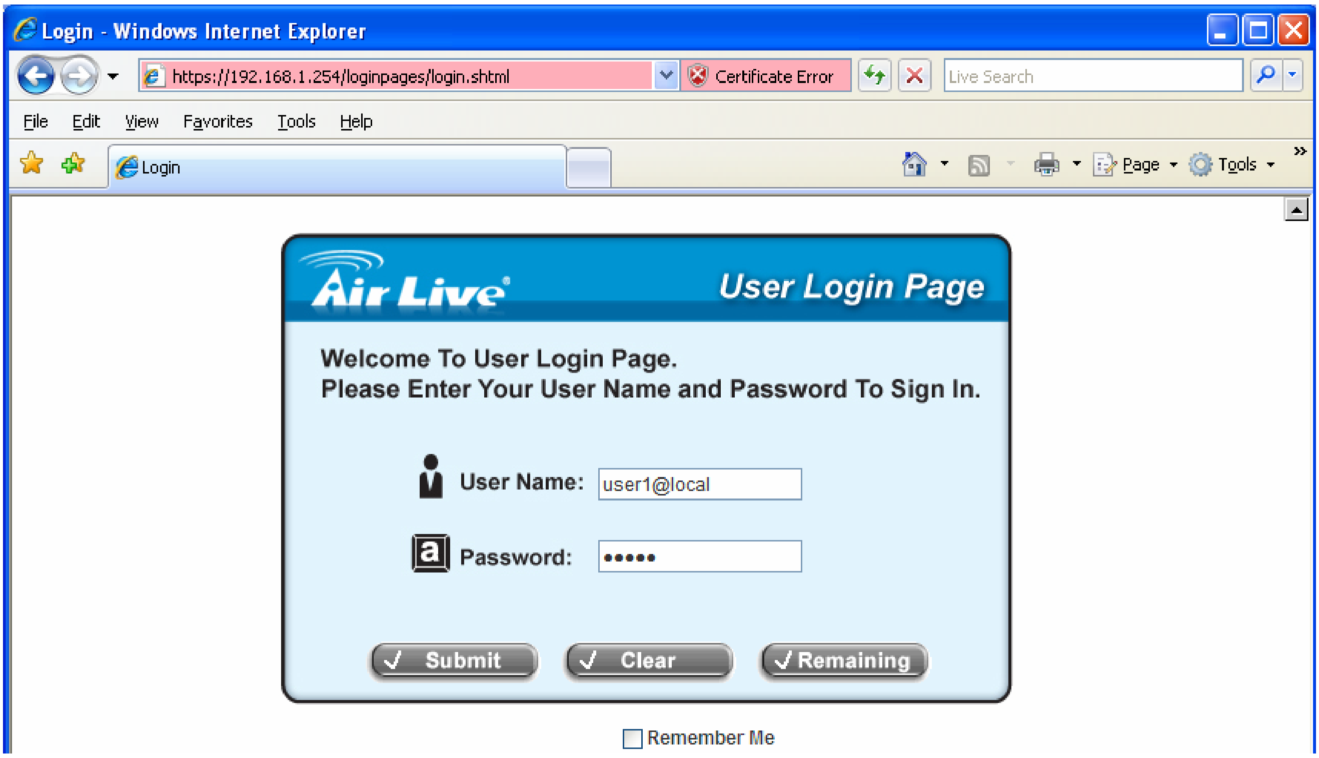
Appendix G: Local VPN

MW-2000S has the ability to establish IPSec VPN tunnels between local user's Windows devices (on local wired or wireless network) and MW-2000S itself, for the purpose of traffic protection on local networks. By pushing down ActiveX Control to the user's browser from MW-2000S, the system will be able to install a so-called "clientless" IPSec VPN.


Internet
MW-2000S
Local VPN Termination (IPSec Tunnel)
Local VPN Termination (IPSec Tunnel)
Switch
Wired User
Wireless User

1. User Operation Flow

a. As usual, enter username and password in the User Login Page


Login - Windows Internet Explorer

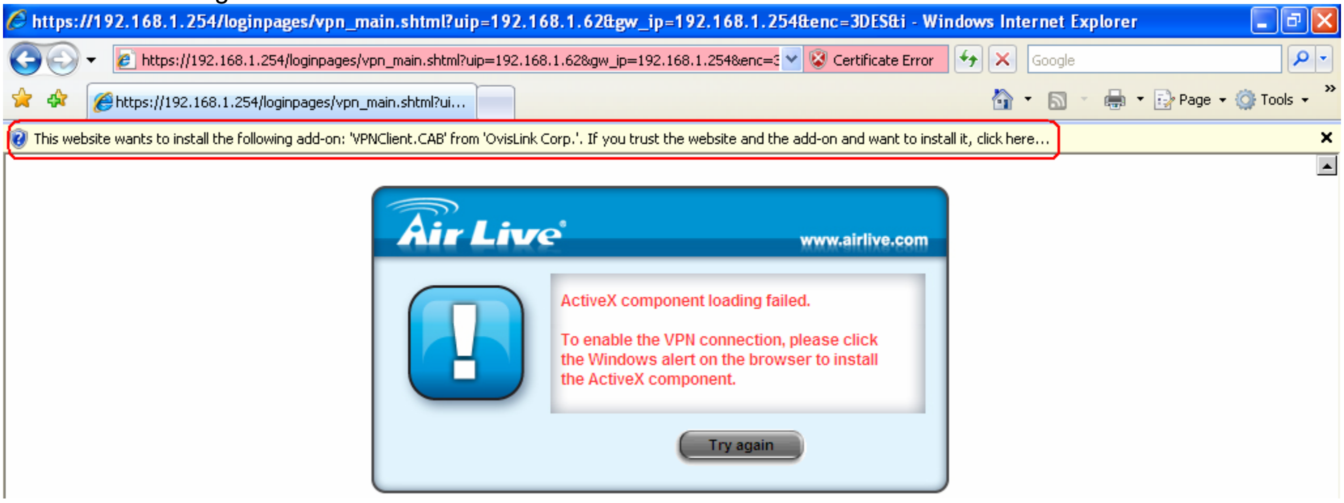
https://192.168.1.254/loginpages/login.shtml

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

User Name: user1@local

Password: •••••

b. For the first time, if the user has never used Local VPN feature, Windows IE browser (6.0 or above) will display an alert message to ask the user whether she or he wants to install the "add-on" software.


https://192.168.1.254/loginpages/vpn_main.shtml?uip=192.168.1.62&gw_ip=192.168.1.254&enc=3DES&i - Windows Internet Explorer

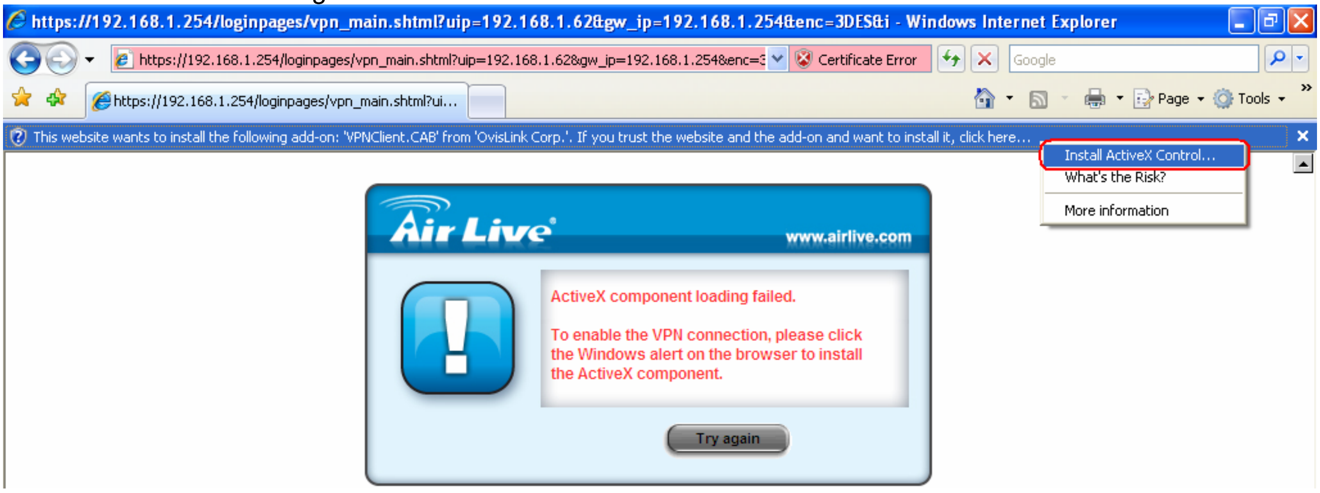
This website wants to install the following add-on: 'VPNClient.CAB' from 'OvisLink Corp.'. If you trust the website and the add-on and want to install it, click here...

ActiveX component loading failed.

To enable the VPN connection, please click the Windows alert on the browser to install the ActiveX component.

https://192.168.1.254/loginpages/vpn_main.shtml?uip=192.168.1.62&gw_ip=192.168.1.254&enc=3
Certificate Error
Google
https://192.168.1.254/loginpages/vpn_main.shtml?ui...
Page Tools
Air Live
www.airlive.com
Try again

c. Click on the alert message and then choose the “Install ActiveX Control” to install the software.



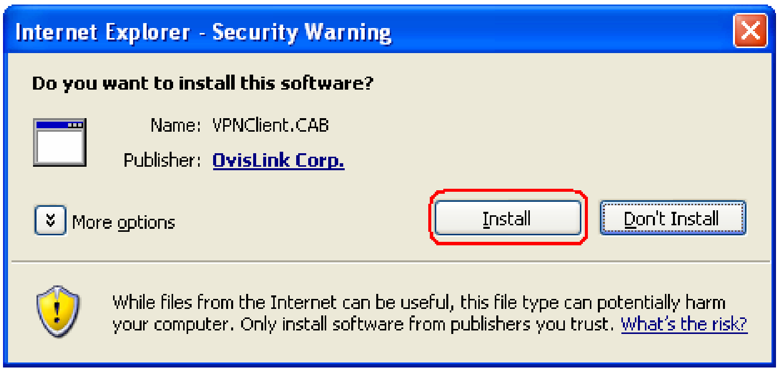
https://192.168.1.254/loginpages/vpn_main.shtml?uip=192.168.1.62&gw_ip=192.168.1.254&enc=3DES&i - Windows Internet Explorer

This website wants to install the following add-on: 'VPNClient.CAB' from 'OvisLink Corp.'. If you trust the website and the add-on and want to install it, click here...

ActiveX component loading failed.

To enable the VPN connection, please click the Windows alert on the browser to install the ActiveX component.

https://192.168.1.254/loginpages/vpn_main.shtml?uip=192.168.1.62&gw_ip=192.168.1.254&enc=3
Certificate Error
Google
https://192.168.1.254/loginpages/vpn_main.shtml?ui...
Page
Tools
Install ActiveX Control...
What's the Risk?
More information
Air Live
www.airlive.com
Try again



Internet Explorer - Security Warning

Do you want to install this software?

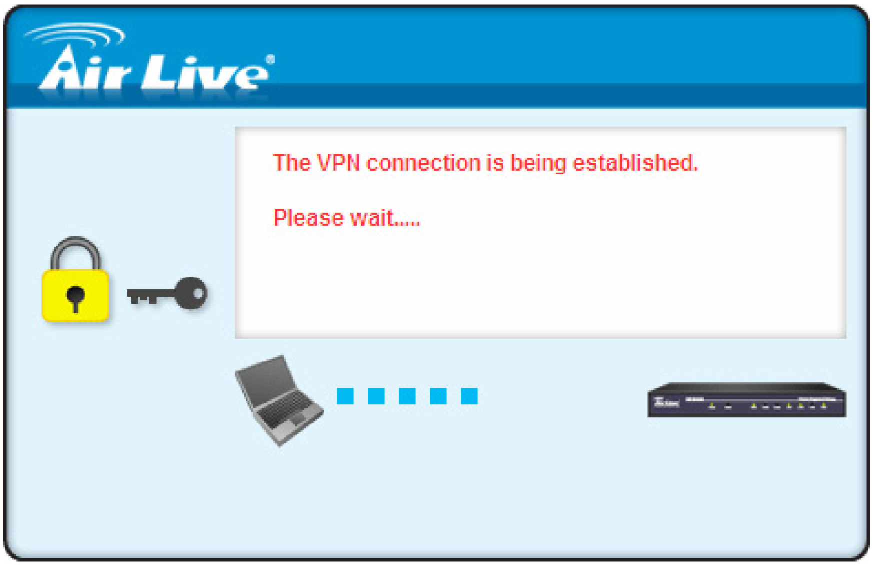
Name: VPNClient.CAB

Publisher: OvisLink Corp.

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

More options
Install
Don't Install

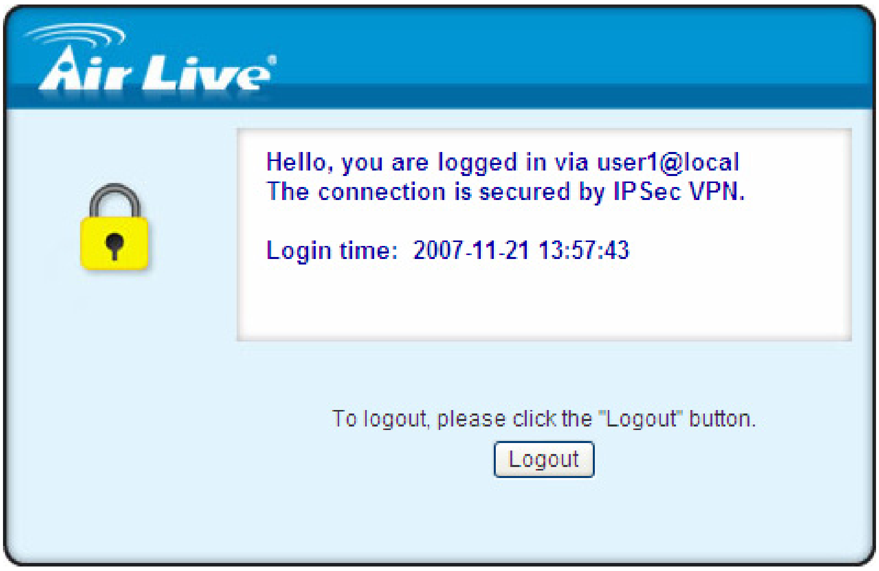
d. After the software is installed well, the system will try to establish the IPSec VPN tunnel for the user automatically.



The VPN connection is being established.

Please wait.....

e. Once the IPSec VPN tunnel is established, the user has successfully logged in and the connection is secured by IPSec VPN.



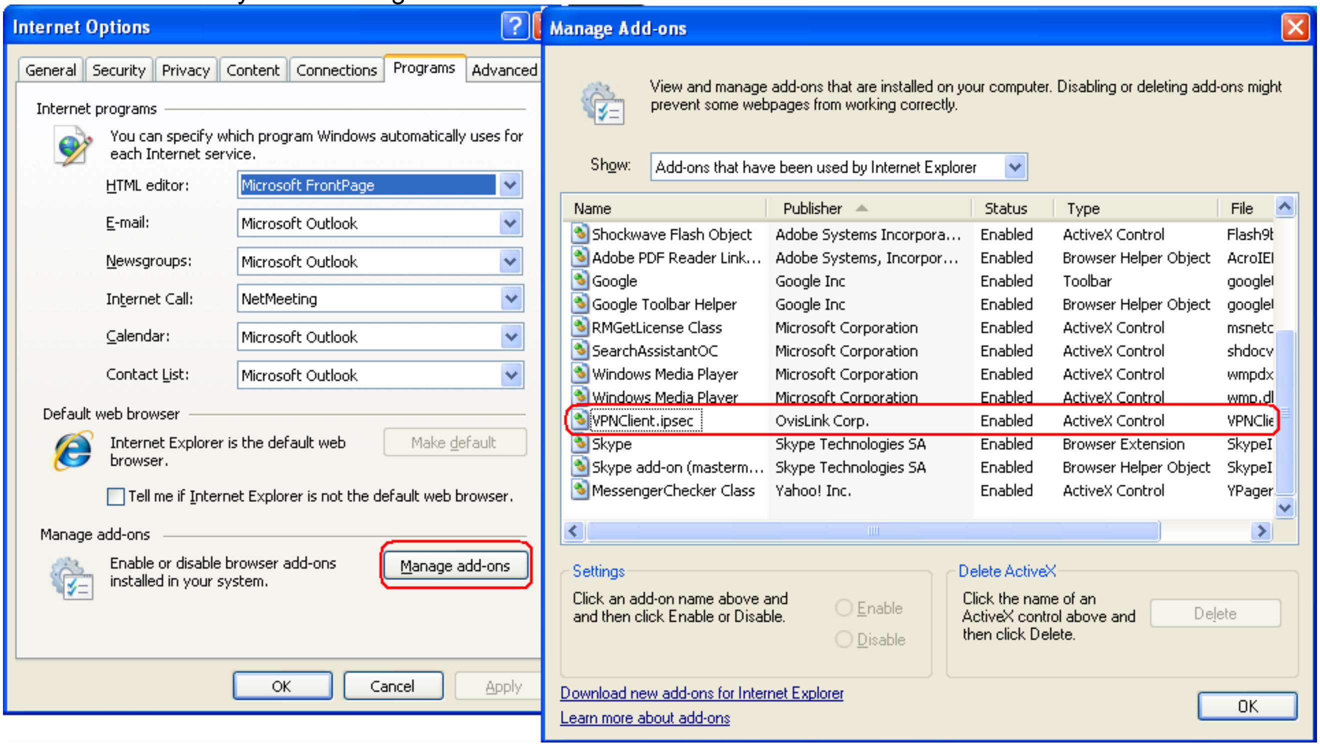
Hello, you are logged in via user1@local
The connection is secured by IPSec VPN.

Login time: 2007-11-21 13:57:43

To logout, please click the "Logout" button.

2. ActiveX Control component

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



Internet programs

You can specify which program Windows automatically uses for each Internet service.

HTML editor: Microsoft FrontPage
E-mail: Microsoft Outlook
Newsgroups: Microsoft Outlook
Internet Call: NetMeeting
Calendar: Microsoft Outlook
Contact List: Microsoft Outlook

Default web browser

Internet Explorer is the default web browser.

□ Tell me if Internet Explorer is not the default web browser.

Manage add-ons

Enable or disable browser add-ons installed in your system.

View and manage add-ons that are installed on your computer. Disabling or deleting add-ons might prevent some webpages from working correctly.

Show: Add-ons that have been used by Internet Explorer

Name	Publisher	Status	Type	File
Shockwave Flash Object	Adobe Systems Incorpora...	Enabled	ActiveX Control	Flash9t
Adobe PDF Reader Link...	Adobe Systems, Incorpor...	Enabled	Browser Helper Object	AcroIEI
Google	Google Inc	Enabled	Toolbar	google
Google Toolbar Helper	Google Inc	Enabled	Browser Helper Object	google
RMGetLicense Class	Microsoft Corporation	Enabled	ActiveX Control	msnetc
SearchAssistantOC	Microsoft Corporation	Enabled	ActiveX Control	shdocv
Windows Media Player	Microsoft Corporation	Enabled	ActiveX Control	wmpdx
Windows Media Player	Microsoft Corporation	Enabled	ActiveX Control	wmp.dl
VPNClient.ipsec	OvisLink Corp.	Enabled	ActiveX Control	VPNClie
Skype	Skype Technologies SA	Enabled	Browser Extension	SkypeI
Skype add-on (masterm...	Skype Technologies SA	Enabled	Browser Helper Object	SkypeI
MessengerChecker Class	Yahoo! Inc.	Enabled	ActiveX Control	YPager

Settings

Click an add-on name above and and then click Enable or Disable.

Delete ActiveX

Click the name of an ActiveX control above and then click Delete.

From Windows Internet Explorer, click “Manage add-ons” button inside “Programs” page under “Tools” to show the add-ons programs list. You can see VPNClient.ipsec was enabled.

3. Limitations

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

a. 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.

b. Without Windows patch KB889527, ICMP (Ping) and PORT command of FTP cannot work in Windows XP SP2.

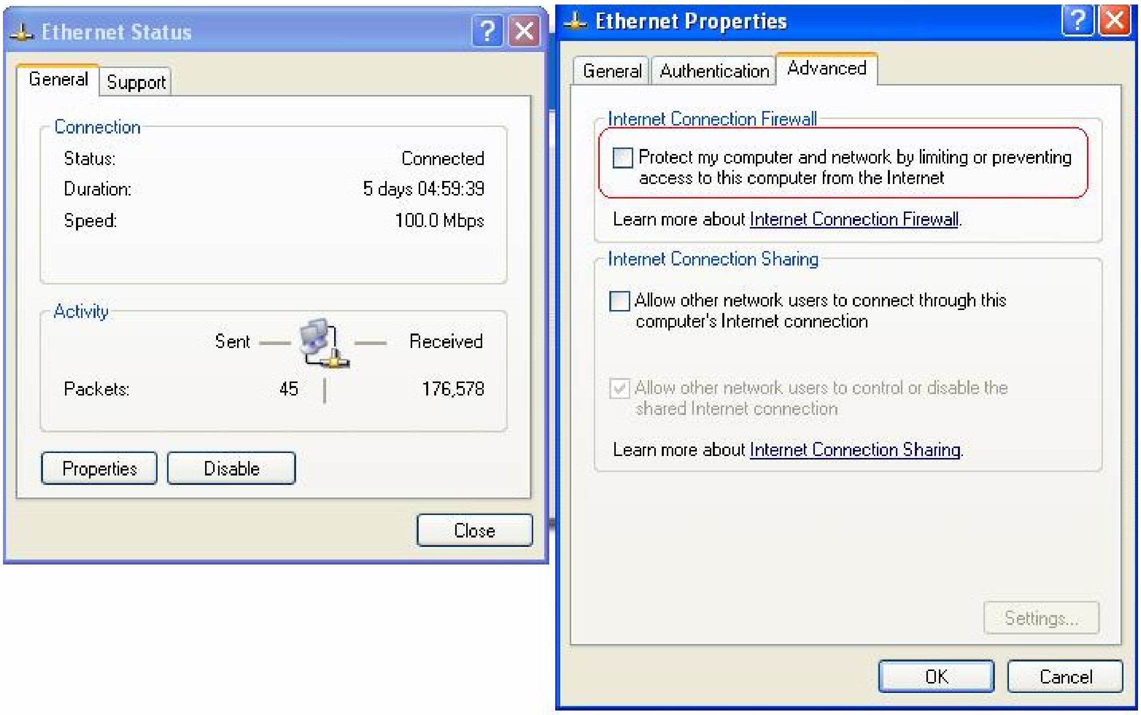
c. The forced termination (through CTRL+ALT+DEL or Task Manager) of the Internet Explorer will stop the running of ActiveX. It causes IPSec tunnel can't be cleared properly at client's device. In this case, a reboot of client's device is needed to clear the IPSec tunnel.

d. The crash of Windows Internet Explorer may cause the same result.

e. There are some OS and browser which may not support Local VPN.

(1) 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.



Connection
Status: Connected
Duration: 5 days 04:59:39
Speed: 100.0 Mbps

Activity
Sent — Received
Packets: 45 176,578

Internet Connection Firewall
□ Protect my computer and network by limiting or preventing access to this computer from the Internet
Learn more about Internet Connection Firewall.

Internet Connection Sharing
□ Allow other network users to connect through this computer's Internet connection
☑ Allow other network users to control or disable the shared Internet connection
Learn more about Internet Connection Sharing.

***Suggestion:** Please **TURN OFF** Internet Connection Firewall feature or upgrade the Windows OS into Windows XP SP2.*

(2) ICMP and Active Mode FTP

On 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 device, 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.

***Suggestion:** Please UPDATE client's Windows XP SP2 with this patch.*

(3) The Termination of ActiveX

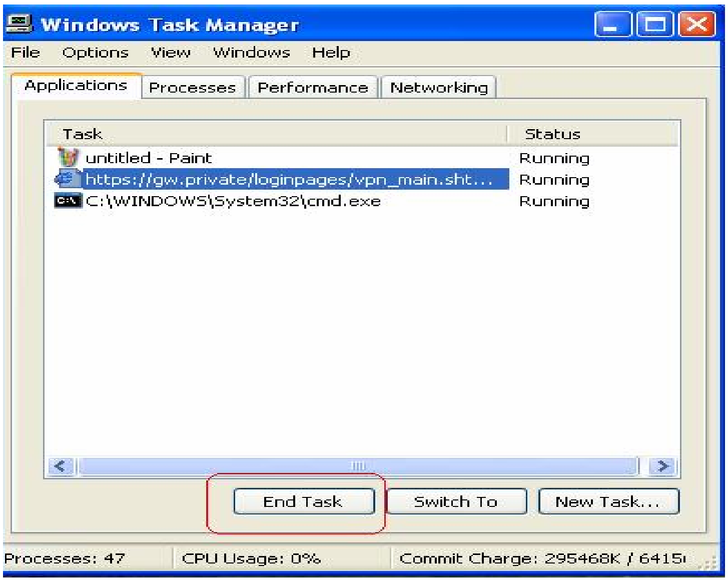
The ActiveX component for IPSec VPN is running paralleled with the web page of "Login Success". Unless user decides to close the session and to disconnect with MW-2000S, the following conditions or behaviors of using browser shall be avoided in order to maintain the built IPSec VPN tunnel always alive.

Reasons may cause the Internet Explorer to stop the ActiveX unexpectedly as follows:

The crash of Internet Explorer on running ActiveX

***Suggestion:** Please reboot client's computer, once Windows service is resumed, go through the login process again.*

Terminate the Internet Explorer Task from Windows Task Manager



Windows Task Manager
File Options View Windows Help
Applications Processes Performance Networking

Task	Status
untitled - Paint	Running
https://gw.private/loginpages/vpn_main.sht...	Running
C:\WINDOWS\System32\cmd.exe	Running

End Task
Switch To
New Task...

Processes: 47 CPU Usage: 0% Commit Charge: 295468K / 64151

Suggestion: *Don't terminate this VPN task of Internet Explorer.*

There are some cases of Windows messages by which MW-2000S will warn current user to:

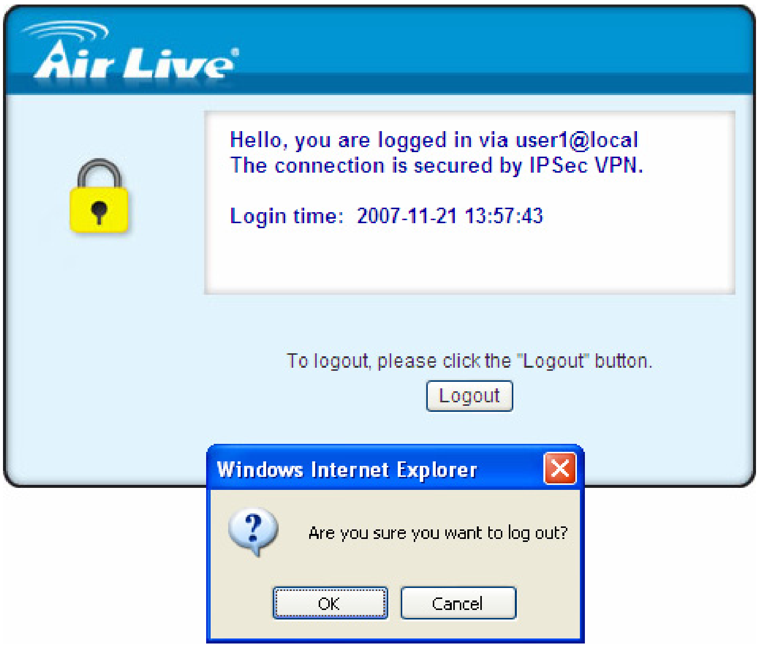
① Close the Windows Internet Explorer,

② Click "logout" button on "login success" page,

③ Click "back" or "refresh" of the same Internet Explorer,

④ Enter new URL in the same Internet Explorer,

⑤ Open a URL from the other application (e.g. email of Outlook) that occupies this existing Internet Explorer.



Hello, you are logged in via user1@local
The connection is secured by IPSec VPN.

Login time: 2007-11-21 13:57:43

To logout, please click the "Logout" button.

Are you sure you want to log out?

That shall all cause the termination of IPSec VPN tunneling if user chooses to click "Yes". The user has to log in again to regain the network access.

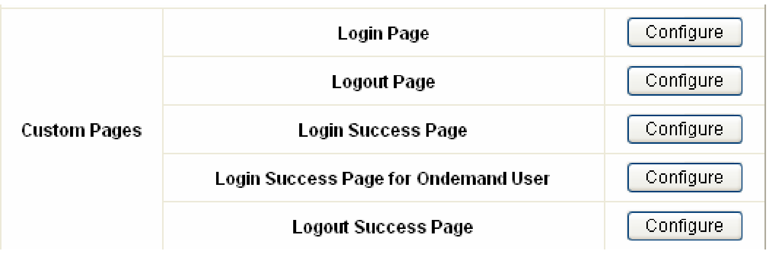
Suggestion: *Click "Cancel" if you do not intend to stop the IPSec VPN connection yet.*

(4) Non-supported OS and Browser

In current version, Windows Internet Explorer (6.0 or above) is the only browser supported by MW-2000S. Windows XP and Windows 2000 are the only two supported OS along with this release.

Appendix H: Customizable Pages

There are five users' login and logout pages for each service zone that can be customized by administrators. Click the button of ***Configure***, the **Login (Logout)** page will appear, including **Login page**, **Logout Page**, **Login Success Page**, **Login Success Page for Instant Account** and **Logout Success Page.**
Click the radio button of page selections to have further configuration.

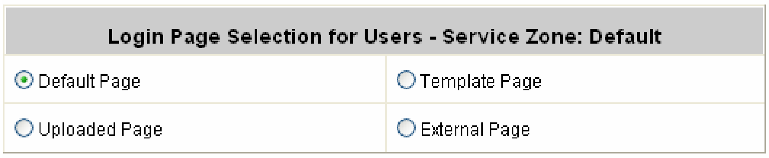


Custom Pages	Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Success Page for Ondemand User	Configure
	Logout Success Page	Configure

1 Custom Pages→ ***Login Page***

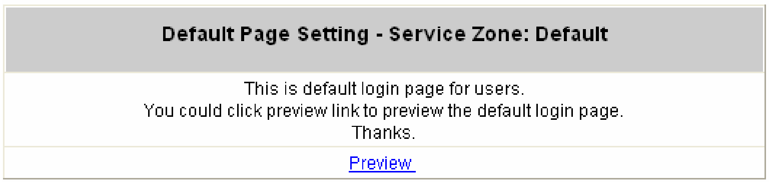
The administrator can use the default login page or get the customized login page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click ***Preview*** to see the login page.

- *Custom Pages→ Login Page→* ***Default Page***
  Choose Default Page to use the default login page
  .



Login Page Selection for Users - Service Zone: Default

● Default Page	○ Template Page
○ Uploaded Page	○ External Page

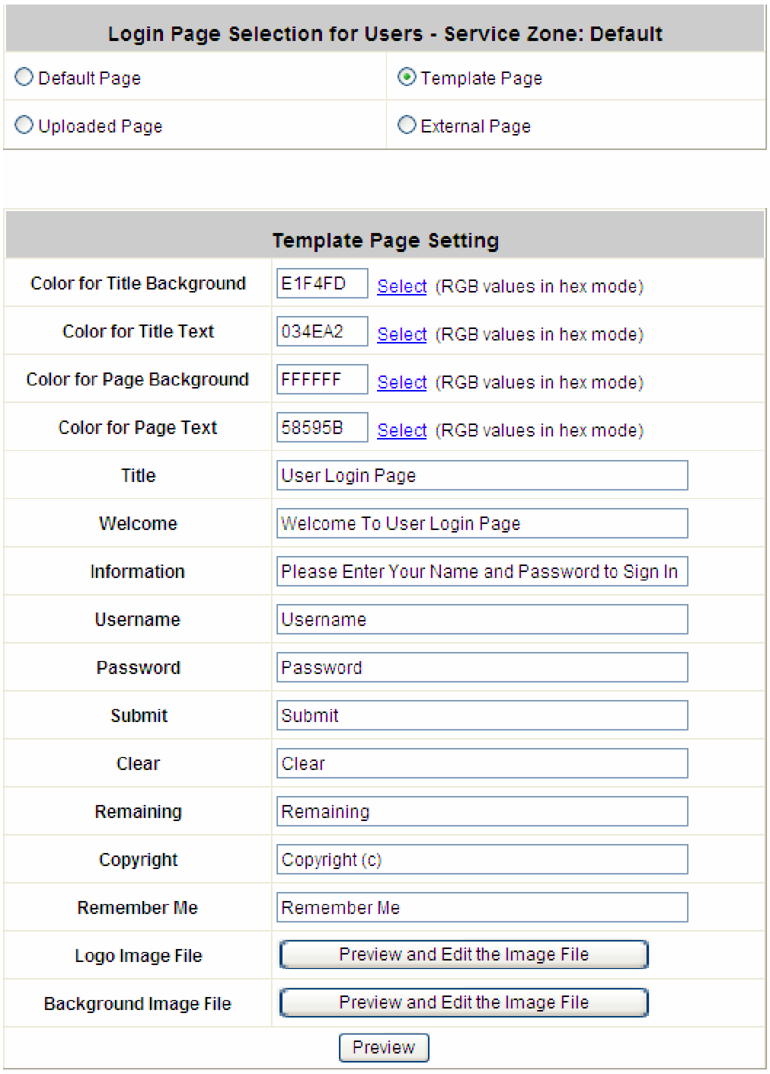


Default Page Setting - Service Zone: Default

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

Preview

- *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. Click Preview to see the result first.



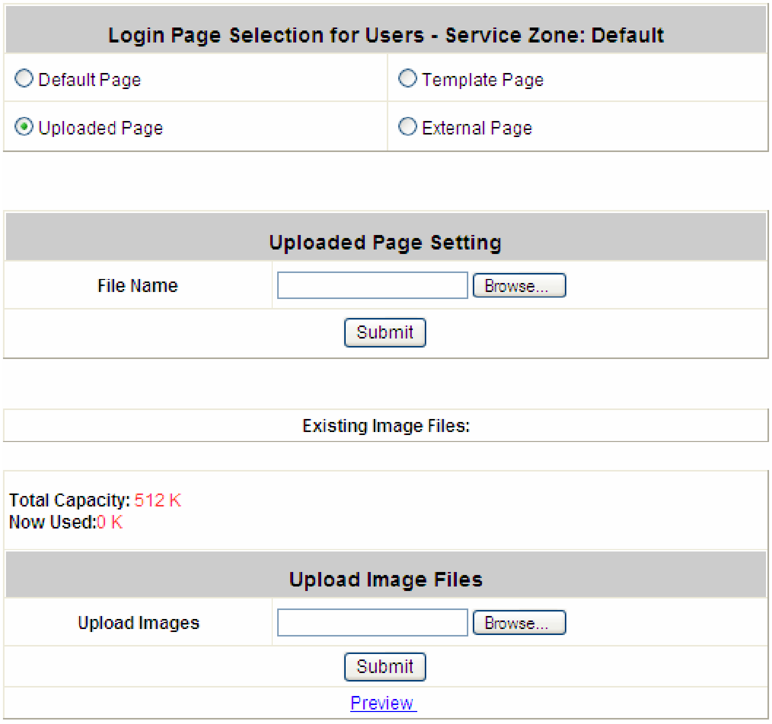
Login Page Selection for Users - Service Zone: Default

○ Default Page	● Template Page
○ Uploaded Page	○ External Page

Template Page Setting

Color for Title Background	E1F4FD Select (RGB values in hex mode)
Color for Title Text	034EA2 Select (RGB values in hex mode)
Color for Page Background	FFFFFF Select (RGB values in hex mode)
Color for Page Text	58595B Select (RGB values in hex mode)
Title	User Login Page
Welcome	Welcome To User Login Page
Information	Please Enter Your Name and Password to Sign In
Username	Username
Password	Password
Submit	Submit
Clear	Clear
Remaining	Remaining
Copyright	Copyright (c)
Remember Me	Remember Me
Logo Image File	Preview and Edit the Image File
Background Image File	Preview and Edit the Image File

- *Custom Pages→ Login Page →**Uploaded Page***
  Choose Uploaded Page and upload a login page.



Login Page Selection for Users - Service Zone: Default

○ Default Page	○ Template Page
● Uploaded Page	○ External Page

Uploaded Page Setting

File Name	Browse...

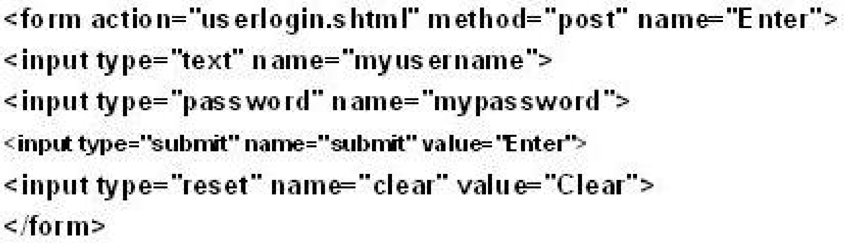
Existing Image Files:

Total Capacity: 512 K
Now Used:0 K

Upload Image Files

Upload Images	Browse...

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



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

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”>**

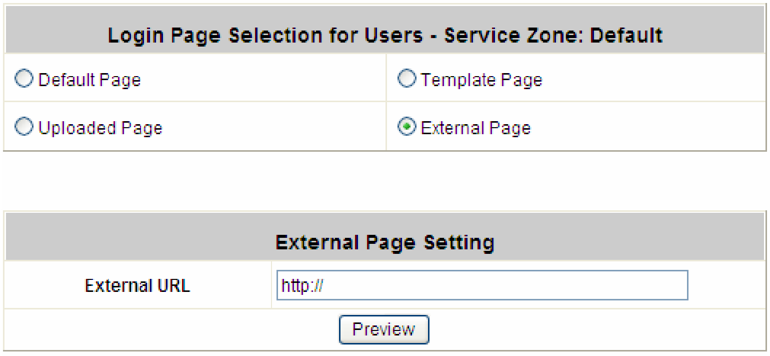
Click the ***Browse*** button to select the file to upload. Then click ***Submit*** to complete the upload process.

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***



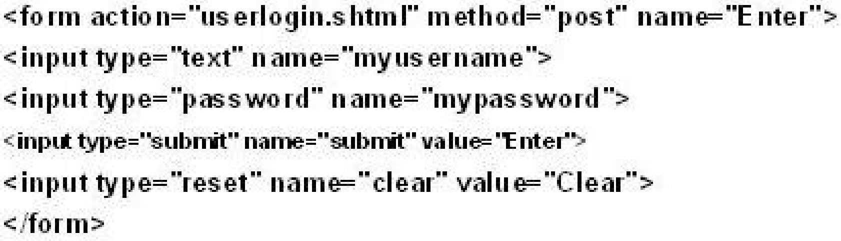
Login Page Selection for Users - Service Zone: Default	
○ Default Page	○ Template Page
○ Uploaded Page	● External Page

External Page Setting	
External URL	http://
	Preview

Choose the ***External Page*** selection and get the login page from the specific 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.

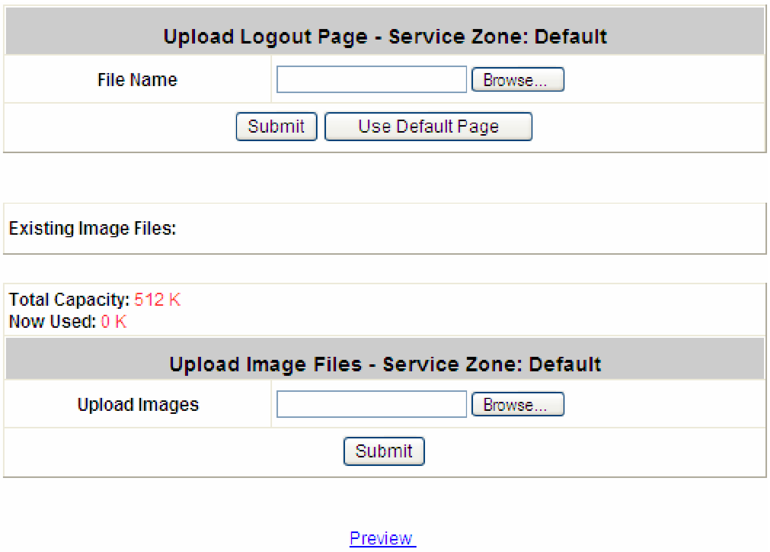
The user-defined logout page must include the following HTML codes to provide the necessary fields for username and password.



```
<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>
```

2 *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.



Upload Logout Page - Service Zone: Default

File Name	[ ] Browse...
Submit Use Default Page	

Existing Image Files:

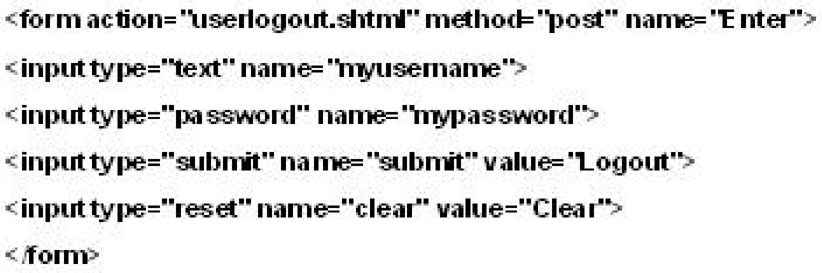
Total Capacity: 512 K
Now Used: 0 K

Upload Image Files - Service Zone: Default

Upload Images	[ ] Browse...
Submit	

Preview

***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.*

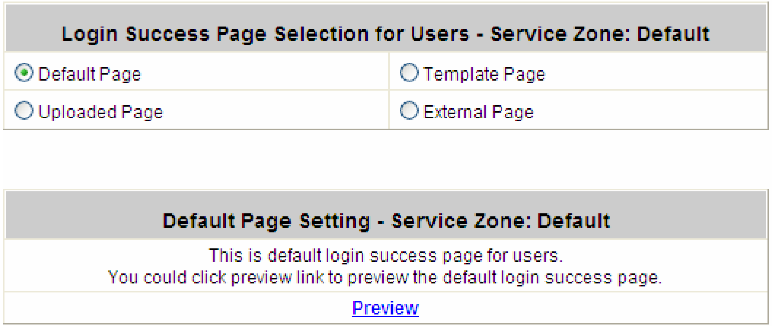


```
<form action="userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Logout">
<input type="reset" name="clear" value="Clear">
</form>
```

3 *Custom Pages→ **Login Success Page***

The users can apply their own Login Success page in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

- *Custom Pages→ Login Success Page→ Default Page*



Login Success Page Selection for Users - Service Zone: Default

● Default Page	○ Template Page
○ Uploaded Page	○ External Page

Default Page Setting - Service Zone: Default

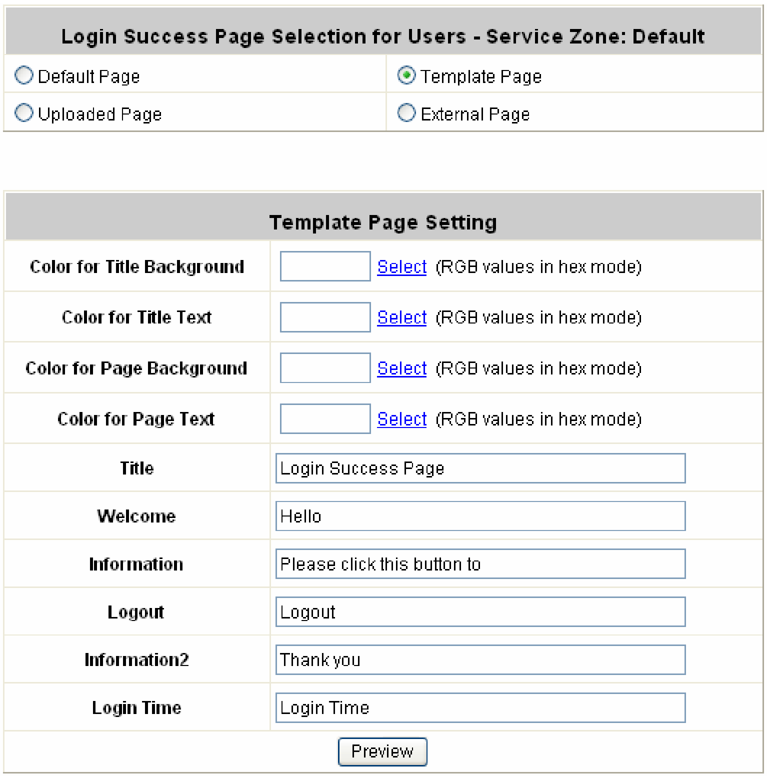
This is default login success page for users.
You could click preview link to preview the default login success page.

Preview

Choose Default Page to use the default login success page.

- *Custom Pages→ Login Success Page→ Template Page*

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



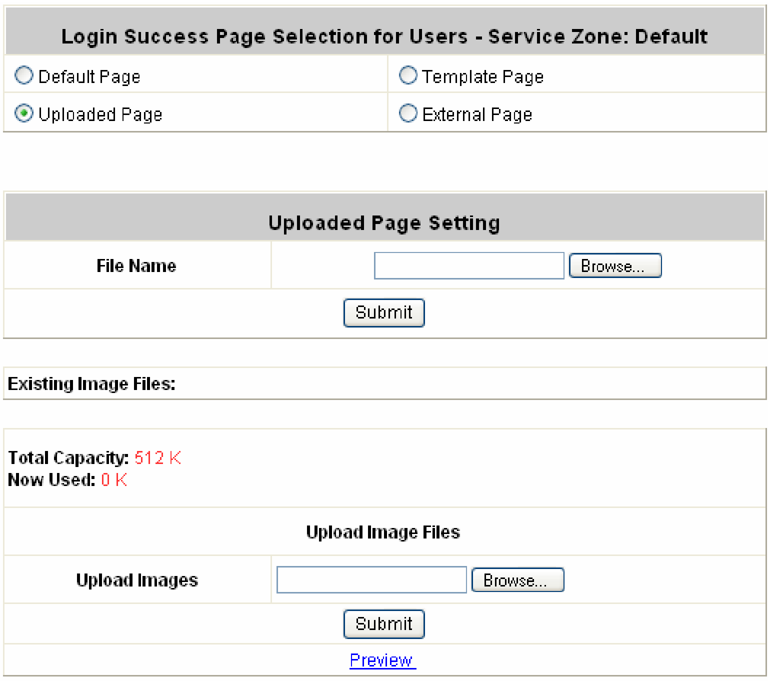
Login Success Page Selection for Users - Service Zone: Default	
○ Default Page	● Template Page
○ Uploaded Page	○ External Page

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

- *Custom Pages→ Login Success Page→* ***Uploaded Page***

Choose Uploaded Page and get the login success page to upload. Click the Browse button to select the file for the login success page upload. Then click Submit to complete the upload process.

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



Login Success Page Selection for Users - Service Zone: Default	
○ Default Page	○ Template Page
● Uploaded Page	○ External Page

Uploaded Page Setting	
File Name	

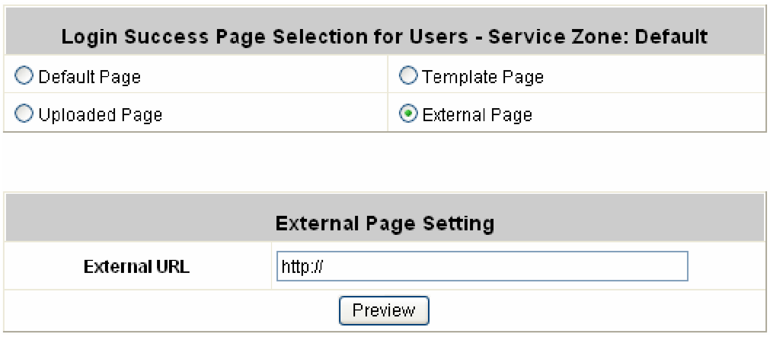
Existing Image Files:

Total Capacity: 512 K
Now Used: 0 K

Upload Image Files	
Upload Images	

- *Custom Pages→ Login Success Page→* ***External Page***

Choose the External Page selection and get the login success page from the specific website. In the External Page Setting, enter URL of the external login page and then click Apply. After applying the setting, the new login success page can be previewed by clicking Preview button at the bottom of this page



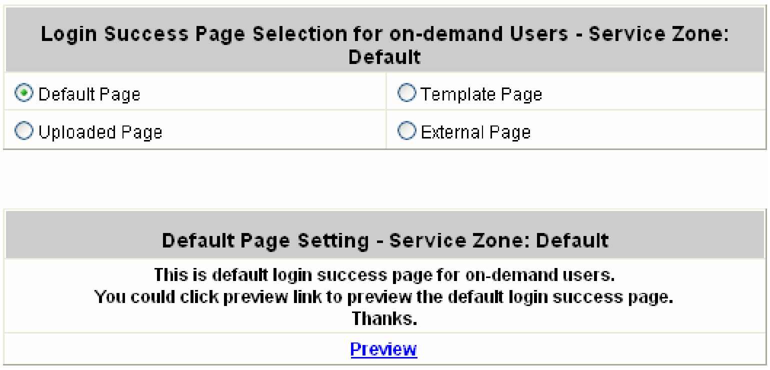
Login Success Page Selection for Users - Service Zone: Default	
○ Default Page	○ Template Page
○ Uploaded Page	● External Page

External Page Setting	
External URL	http://
Preview	

4 *Custom Pages→* ***Login Success Page for On-demand User***

The users can apply their own Login Success page for Instant Users in the menu. As the process is similar to that of the Login Page, please refer to the “Login Page” instructions for more details.

- *Custom Pages→ Login Success Page for On-demand Users→* ***Default Page***
  Choose Default Page to use the default login success page for Instant account



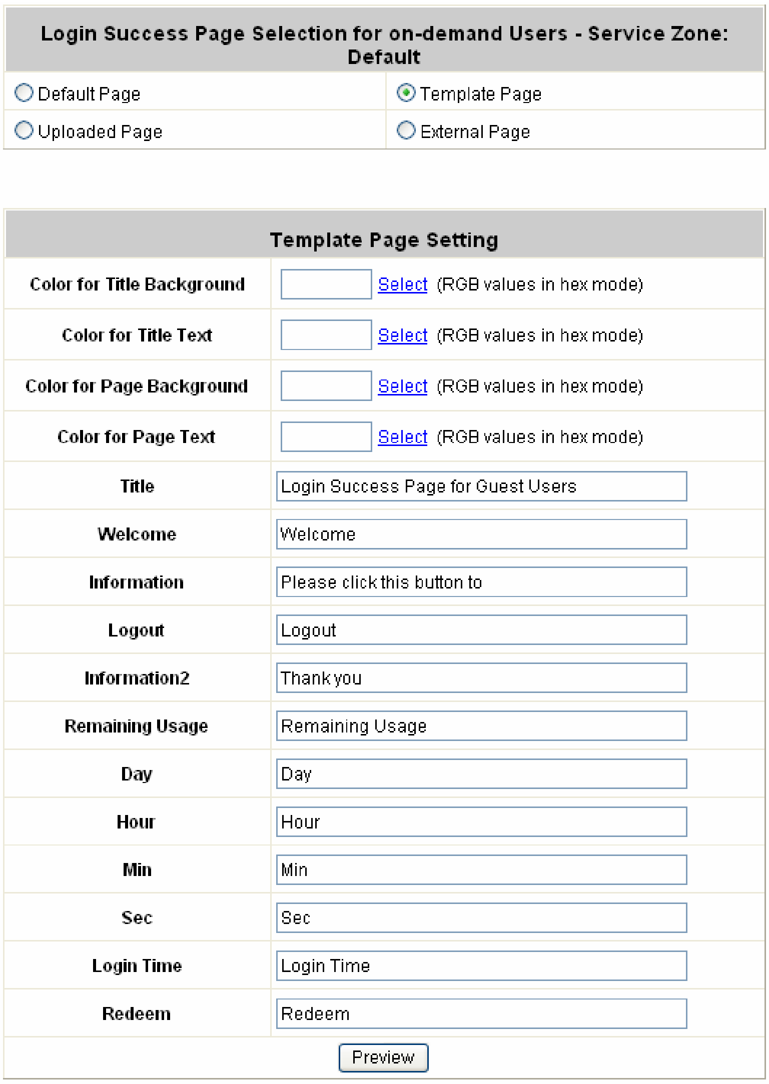
Login Success Page Selection for on-demand Users - Service Zone: Default	
● Default Page	○ Template Page
○ Uploaded Page	○ External Page

Default Page Setting - Service Zone: Default

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

Preview

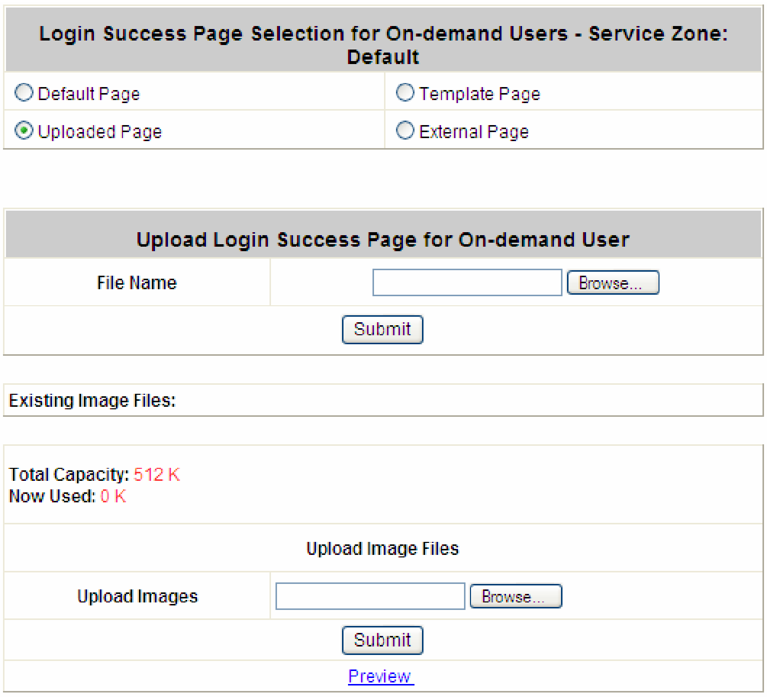
- *Custom Pages→ Login Success Page for On-demand Users→* ***Template Page***
  Choose Template to make a customized login success for Instant account. Click *Select* to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result.



Login Success Page Selection for on-demand Users - Service Zone: Default	
○ Default Page	● Template Page
○ Uploaded Page	○ External Page

Template Page Setting	
Color for Title Background	Select (RGB values in hex mode)
Color for Title Text	Select (RGB values in hex mode)
Color for Page Background	Select (RGB values in hex mode)
Color for Page Text	Select (RGB values in hex mode)
Title	Login Success Page for Guest Users
Welcome	Welcome
Information	Please click this button to
Logout	Logout
Information2	Thank you
Remaining Usage	Remaining Usage
Day	Day
Hour	Hour
Min	Min
Sec	Sec
Login Time	Login Time
Redeem	Redeem

- *Custom Pages→ Login Success Pages for On-demand Users→* ***Uploaded Page***
  Choose Uploaded Page and get the login success page for Instant by uploading. Click the ***Browse*** button to select the file for the login success page for Instant upload. Then click ***Submit*** to complete the upload process.



Login Success Page Selection for On-demand Users - Service Zone: Default	
○ Default Page	○ Template Page
● Uploaded Page	○ External Page

Upload Login Success Page for On-demand User	
File Name	Browse...

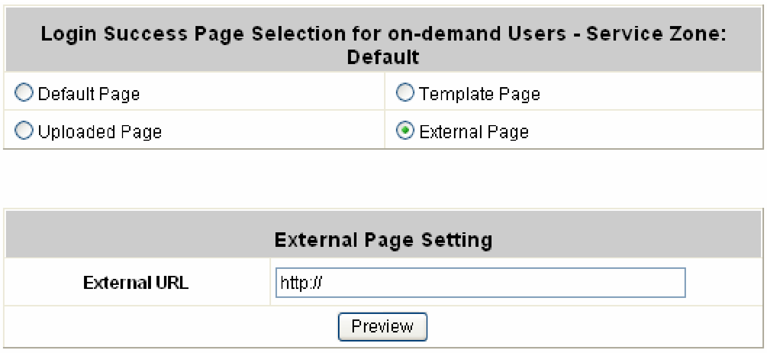
Existing Image Files:

Total Capacity: 512 K
Now Used: 0 K

Upload Image Files	
Upload Images	Browse...

- *Custom Pages→ Login Success Pages for On-demand Users→* ***External Page***
  Choose the External Page selection and get the login success page from the specific website. In the External Page Setting, enter URL of the external login page and then click Apply. After applying the setting,

the new login success page can be previewed by clicking Preview button at the bottom of this page.



Login Success Page Selection for on-demand Users - Service Zone: Default

○ Default Page	○ Template Page
○ Uploaded Page	● External Page

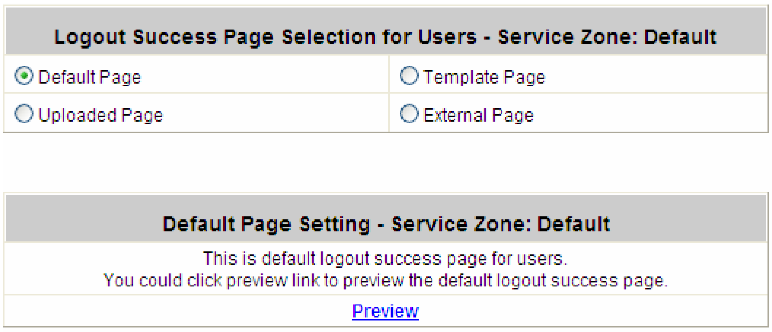
External Page Setting

External URL	http://

5 *Custom Pages→* ***Logout Success Page***

The administrator can apply their own Logout Success page for Users in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

- *Custom Pages →Logout Success Page →**Default Page***
  Choose ***Default Page*** to use the default logout success page.



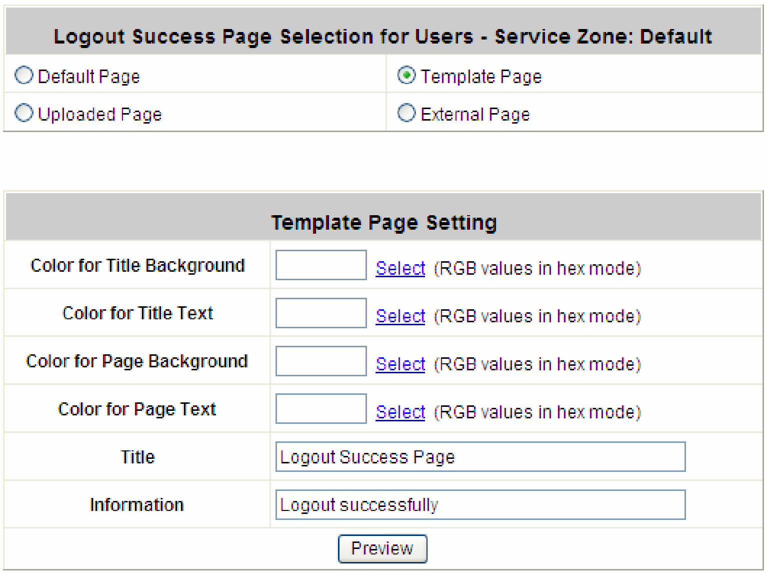
Logout Success Page Selection for Users - Service Zone: Default

● Default Page	○ Template Page
○ Uploaded Page	○ External Page

Default Page Setting - Service Zone: Default

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

- *Custom Pages→ Logout Success Page→**Template Page***
  Choose Template Page to make a customized logout success page. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



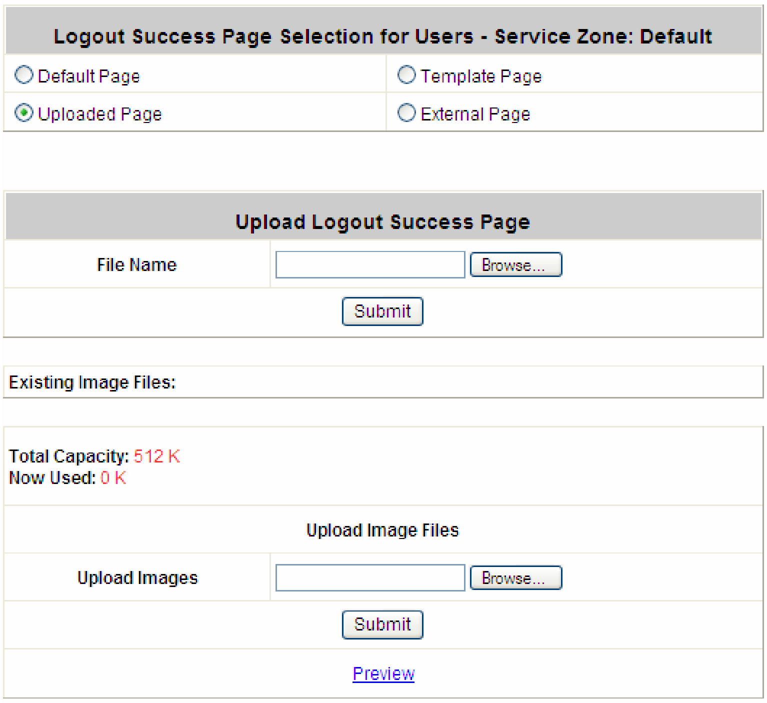
Logout Success Page Selection for Users - Service Zone: Default

○ Default Page	● Template Page
○ Uploaded Page	○ External Page

Template Page Setting

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

- *Custom Pages→ Logout Success Page→* ***Uploaded Page***
  Choose Uploaded Page and get the logout success page to upload. Click the ***Browse*** button to select the file for the logout success page upload. Then click ***Submit*** to complete the upload process.
  After the upload process is completed and applied, the new logout success page can be previewed by clicking ***Preview*** button at the bottom.



Logout Success Page Selection for Users - Service Zone: Default

○ Default Page	○ Template Page
● Uploaded Page	○ External Page

Upload Logout Success Page

File Name

Existing Image Files:

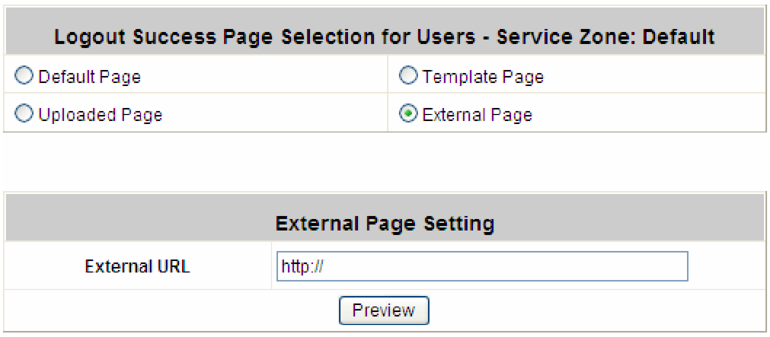
Total Capacity: 512 K
Now Used: 0 K

Upload Image Files

Upload Images

- *Custom Pages →Logout Success Page →**External Page***

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



Logout Success Page Selection for Users - Service Zone: Default

○ Default Page	○ Template Page
○ Uploaded Page	● External Page

External Page Setting

External URL: http://

Appendix I: Session Limit and Session Log

Session Limit

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

- The maximum number of concurrent sessions (TCP and UDP) for each user can be specified in the Global policy, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones.
- When the number of a user's sessions reaches the session limit (a choice of Unlimited, 10, 25, 50, 100, 200, 350, and 500), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to the Syslog server specified in ***Notification Configuration*** (please see section **4.6.6**).
- 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 the network deployment to protect the network in daily operation.

Session Log

The system can record connection details of each user accessing the Internet. In addition, the log data can be sent out to a specified Syslog Server, Email Box or FTP Server based on pre-defined interval time.

- The following table shows the fields of a session log record.

Field	**Description**
Date and Time	The date and time that the session is established
Session Type	[New]: This is the newly established session. [Blocked]: This session is blocked by a Firewall rule.
Username	The account name (with postfix) of the user; It shows "N.A." if the user or device does not need to log in with a username. For example, the user or device is on a non-authenticated port or on the privileged MAC/IP list. Note: Only 31 characters are available for the combination of Session Type plus Username. Please change the account name accordingly, if the name is not identifiable in the record.
Protocol	The communication protocol of session: TCP or UDP
MAC	The MAC address of the user's computer or device
SIP	The source IP address of the user's computer or device
SPort	The source port number of the user's computer or device
DIP	The destination IP address of the user's computer or device
DPort	The destination port number of the user's computer or device

- The following table shows an example of the session log data.

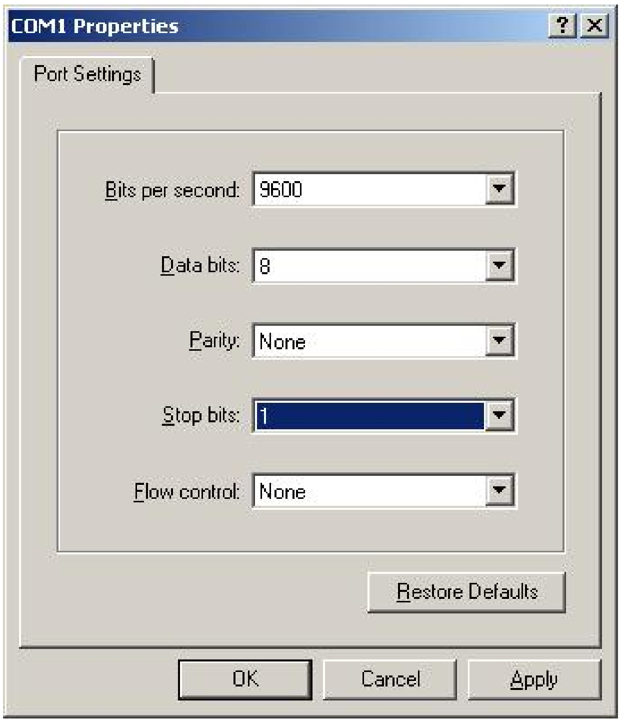
```
Jul 20 12:35:05 2007   [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1626 DIP=203.125.164.132 DPort=80
Jul 20 12:35:05 2007   [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1627 DIP=203.125.164.132 DPort=80
Jul 20 12:35:06 2007   [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1628 DIP=203.125.164.142 DPort=80
Jul 20 12:35:06 2007   [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1629 DIP=203.125.164.142 DPort=80
Jul 20 12:35:07 2007   [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1630 DIP=67.18.163.154 DPort=80
Jul 20 12:35:09 2007   [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1631 DIP=202.43.195.52 DPort=80
Jul 20 12:35:10 2007   [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1632 DIP=203.84.196.242 DPort=80
```

Appendix J: Console Interface

Via this port, administrators can enter the console interface to handle the problems and situations occurred during operation.

1. To connect the console port of MW-2000S, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.

2. Please set the parameters as **9600,8,n,1,n** if a Hyper Terminal is used.

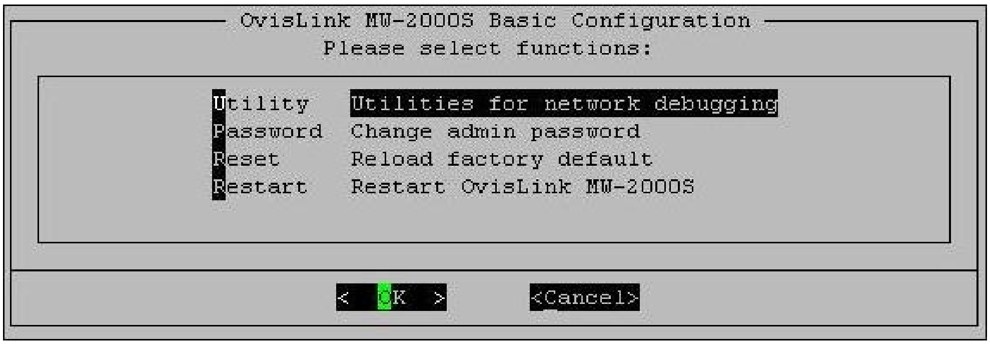


COM1 Properties

Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: 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 MW-2000S 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, and the welcome screen or the main menu will appear. If the welcome screen or the main menu of the console does not appear, please check the connection of the cables and the settings of the terminal simulation program.

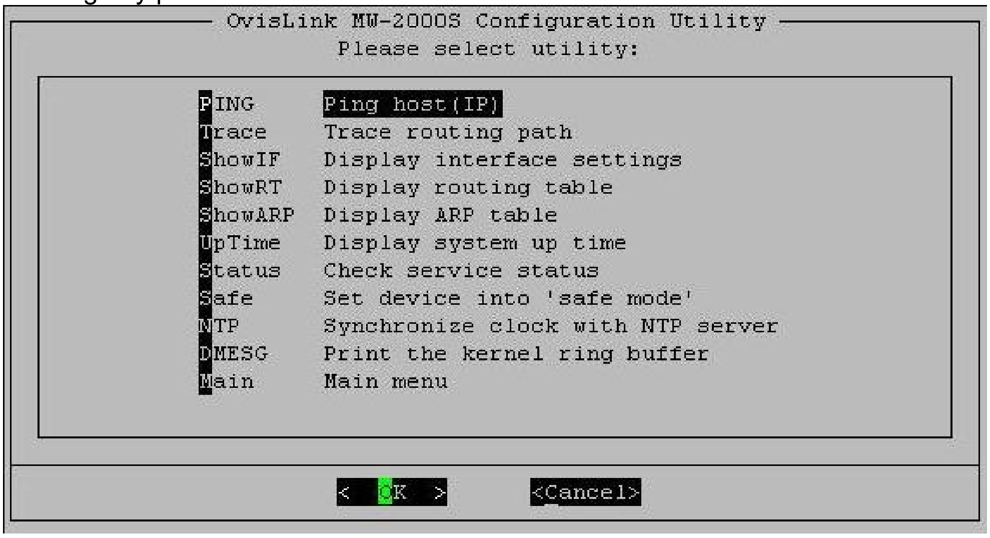


```
              OvisLink MW-2000S Basic Configuration
                    Please select functions:

              Utility    Utilities for network debugging
              Password   Change admin password
              Reset      Reload factory default
              Restart    Restart OvisLink MW-2000S


                     <  OK  >      <Cancel>
```

- **Utilities for network debugging**
  The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follow:



```
OvisLink MW-2000S Configuration Utility
          Please select utility:

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

        <  OK  >        <Cancel>
```

  - ➢ Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
  - ➢ Trace routing path: Trace and inquire the routing path to a specific target.
  - ➢ Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
  - ➢ Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
  - ➢ Display ARP table: The internal ARP table of the system is displayed.
  - ➢ Display system up time: The system live time (time for system being turn on) is displayed.
  - ➢ Check service status: Check and display the status of the system.
  - ➢ Set device into "safe mode": If administrator is unable to use Web Management Interface via the browser for the system failed inexplicitly. Administrator can choose this utility and set MW-2000S into safe mode, then administrator can management 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 bootup 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, the administrator's password is not required to be entered to access the console management interface. If connecting the system by SSH, username and password are required.
  The username is "admin" and the default password is also "admin", which is the same as for the web management interface. By using the null modem to connect the console management interface, administrator's password can be reset if for any reason the password is forgotten.

***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 MW-2000S 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 AirLive MW-2000S**
  Choosing this option will restart MW-2000S