DSA-3600
User Guide

Version DSA-3600-3.00 December, 2007

Copyright © 2007 D-Link Corporation

All rights reserved. Printed in Taiwan. D-Link Corporation reserves the right to change, modify, and revise this publication without notice.

Trademarks

Copyright 2007 D-Link Corporation. All rights reserved. D-Link, the D-Link logo, and DSA-3600 are trademarks of D-Link Corporation. All other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, D-Link Corporation reserves the right to make any changes to products described in this document without notice. D-Link Corporation shall be indemnified against any liability that may occur due to the use or application of the product(s) described herein.

Table of Contents

Chapter 1. Before You Start

1.1 Audience

This manual is intended for use by system integrators, field engineers and network administrators to help them set up DSA-3600 Multi-Service Business Gateway in their network environments. It contains step by step procedures and pictures to guide users with basic network system knowledge to complete the installation.

1.2 Document Conventions

The following information provides the details of conventions used in this manual.

For cautionary statements or warning requiring special attention by readers, a text box with italic font will be used:

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

When any of the button symbol shown below is selected, the following action will be executed accordingly:

Log out the system.

Access **Online Help** interface.

Apply all settings configured.

Clear all settings configured prior to applying.

* The red asterisk indicates information in this field is compulsory.

Please Note: *Screen captures and pictures used in this manual may be displayed in part or in whole, and may vary or differ slightly from the actual product, depending on versioning and menu accessed.*

Chapter 2. Overview

2.1 Introduction of DSA-3600

DSA-3600 is a Multi-Service Business Gateway specially designed for small and medium business, and branch office operational environments. The major functional areas include user management, access control, AP management, security management, and VLAN. The major features of DSA-3600 can be grouped into four functional blocks:

A. User Access Control

B. Network Security (examples: Firewall, VLAN and VPN)

C. Web-based administration and centralized AP management

D. General networking features

2.2 System Concept

Small and Midsize Business (SMB) Network Environment

Networking devices such as switches, hubs, and access points are usually included in SMB environments. The Internet connection of a SMB is usually via ADSL or cable modem. Figure-2.2a shows a typical network deployment example which includes switches, access points, and connections to the Internet via ADSL/cable modem.

The DSA-3600 provides user authentication, authorization and management. The user account information is stored in the local database or specified external database servers. User authentication is processed via the SSL encrypted web interface. This interface is compatible to most desktop devices and palm computers. The appended figures are typical examples of DSA-3600 deployed in a SMB environment. Figure-2.2b shows DSA-3600 authenticating the users of its built-in database, as well as the users of external authentication database. Both LAN and WLAN can be secured by IPSec VPN. PPTP VPN is supported for remote users to increase security at remote sites. The DSA-3600 also supports Site-to-site VPN, WAN Failover, and DMZ.

The DSA-3600 can be used to control access to the company's intranet. In a managed network that includes cable and wireless network users, users located at the managed network can be set to be unable to access the network resource without permission. In the event access right to the network beyond the managed area is required, an Internet browser, such as the Internet Explorer, may be opened to connect to any website. When the browser attempts to connect to a website, the DSA-3600 will force the browser to redirect to the user login webpage. The user must then enter the username and password, where upon successful identification and authentication, the user will then be granted proper access right as defined in the DSA-3600.

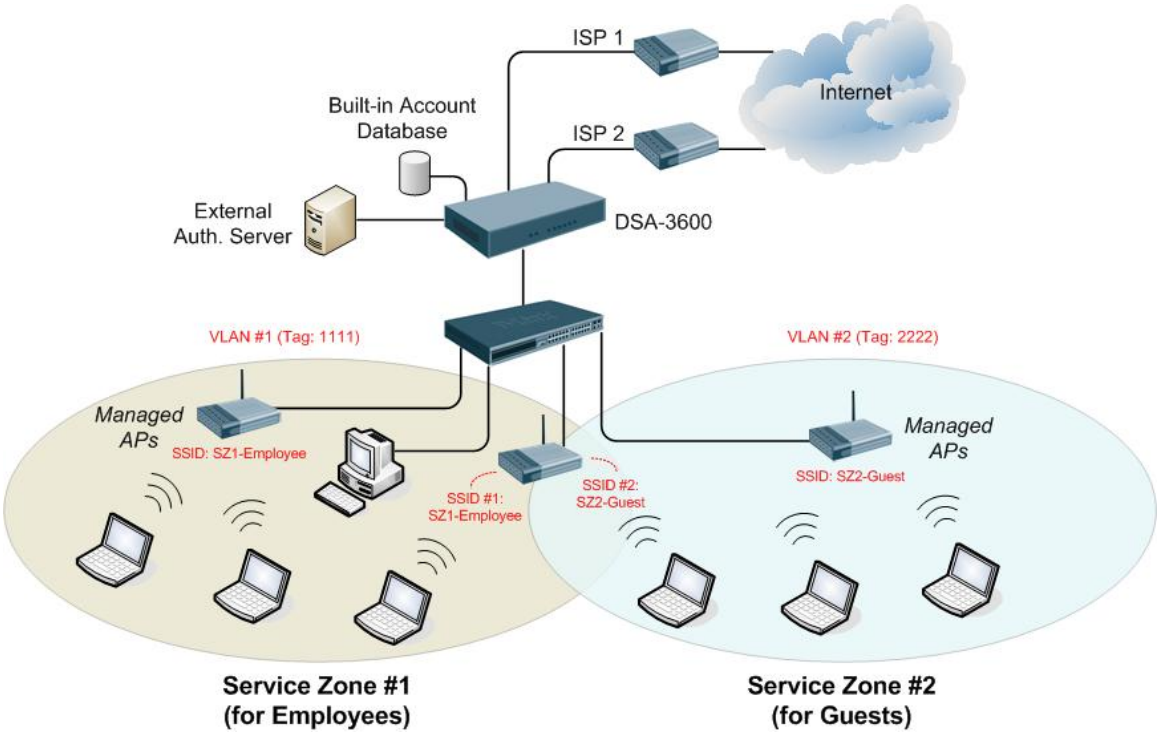


Figure-2.2a: An example deployment using DSA-3600

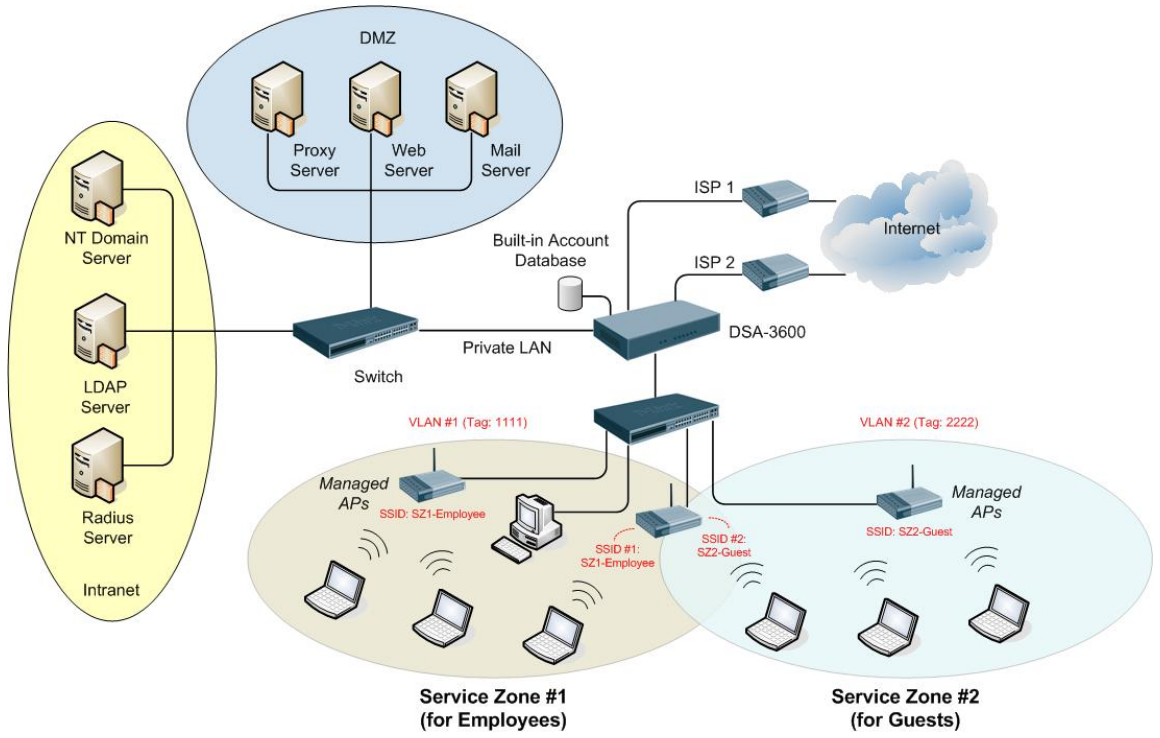


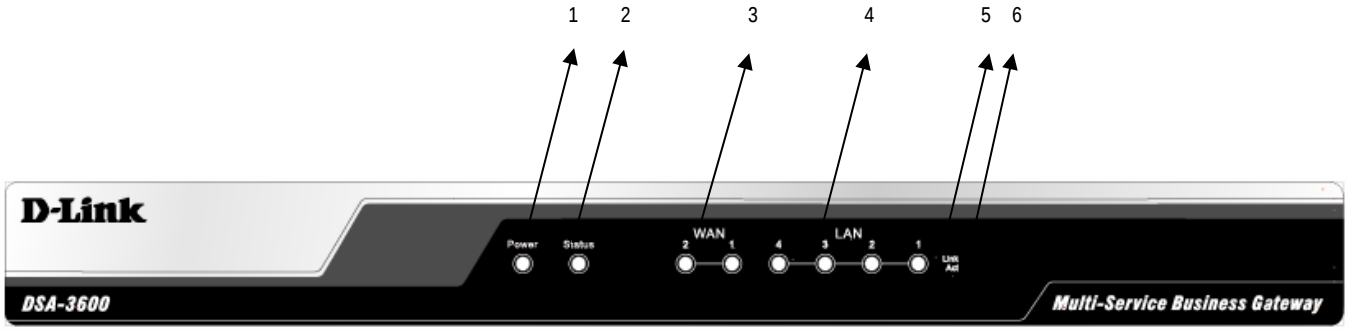
Figure-2.2b: An example of SMB environment using DSA-3600

Chapter 3. Hardware Installation

3.1 Panel Function Descriptions

The DSA-3600 is implemented on an embedded platform with mini-desktop form factor. On the front panel of the product, there are eight LEDs that are used to indicate the system power, system status, and the link status of the six fast Ethernet ports. The interface ports are installed on the rear panel. Six fast Ethernet (100Mbps) ports are provided by DSA-3600. Two are configured as WAN Ports, and the other four are configured as LAN Ports. Located on the rear panel are a serial console port, a reset button, and the power socket.

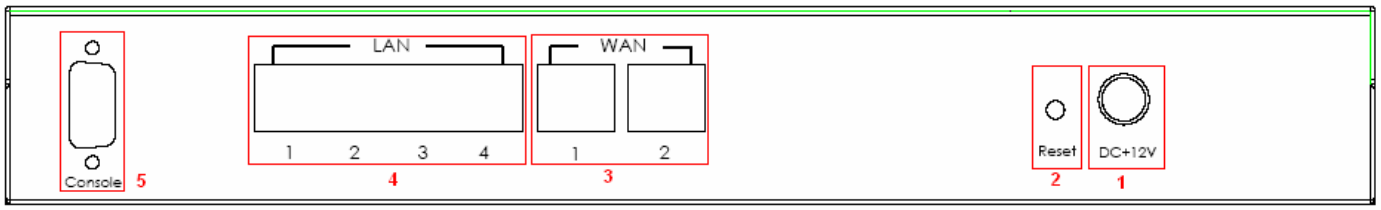
Front Panel



1. Power	**3. LEDs: WAN1~WAN2**	**5. Sign: Link**
2. Status	**4. LEDs: LAN1~LAN4**	**6. Sign: Act**

1. **Power**
   - ON indicates that power is on and OFF indicates that power is off.
2. **Status**
   - While system power is on, status OFF indicates BIOS is running; BLINKING indicates the OS is running, and ON indicates system is ready.
3. **WAN1~WAN2 LEDs**
   - OFF indicates no connection; ON indicates connection and BLINKING indicates transmitting data.
4. **LAN1~LAN4 LEDs**
   - OFF indicates no connection; ON indicates connection and BLINKING indicates transmitting data.
5. **Link Sign**
   - Sign to indicate the LED of WAN1~WAN2 and LAN1~LAN4 in the status of connection.
6. **Act Sign**
   - Sign to indicate the LED of WAN1~WAN2 and LAN1~LAN4 in the status of transmitting data.

Rear Panel



1 **Power Socket:**

- The power adapter is attached here.

2 **Reset Button:**

- Press and hold the Reset button about five seconds, status LED on front panel starts to blink before restarting the DSA-3600.
- Press and hold the Reset button for more than ten seconds; status LED on the front panel starts to speed up blinking before resetting the DSA-3600 to default configuration.

3 **WAN1~WAN2:**

- The two WAN ports connected to an external network not managed by the DSA-3600. These ports may be used to connect to the ATU-Router of an ADSL, or the port of a Cable Modem, or a Switch or Hub on the LAN of an organization.

4 **LAN1~LAN4:**

- The four LAN ports connect to networks managed by DSA-3600, such as to clients' networking devices or APs. There are two modes for service zone supported by DSA-3600, Port-Based and Tag-Based. By default, all LAN ports are in Tag-based service zone. Under Tag-Based mode, service zones will be distinguished by VLAN tagging instead of physical LAN ports.

5 **Console:**

- The serial RS-232 DB9 cable attaches here.

3.2 Package Contents

The standard package of the DSA-3600 includes:

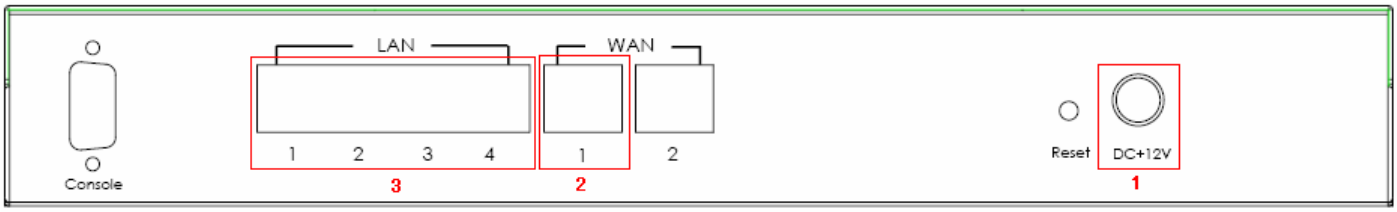
- DSA-3600 x 1
- Quick Install Guide x 1
- CD-ROM x 1
- Console Cable x 1
- Straight-through Ethernet Cable x 1
- Power Cord x 1
- Power Adapter x 1

3.3 System Requirement

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

3.4 Installation Steps

Please follow the steps mentioned below to install the hardware of DSA-3600:



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

   ***Warning**: Using a non-certified power adapter may damage this product.*

2. Connect an Ethernet cable to the WAN1 Port on the rear panel. Connect the other end of the Ethernet cable to a networking device such as an ADSL modem, a cable modem, a switch, or a hub. The LED of WAN1 port should light up to indicate a proper connection.
3. Connect an Ethernet cable to any LAN Port on the rear panel. Connect the other end of the cable to a networking device such as the administrator's PC. The LED of the LAN should be ON to indicate a proper connection.

After the hardware of the DSA-3600 is installed completely, the system is ready to be configured in the following sections. This manual will guide you step by step to set up the system using a single DSA-3600 to manage the network.

Chapter 4. Web Interface Configuration

This chapter provides further detailed information on setting up the DSA-3600. The following table shows all the functions of DSA-3600.

In the web management interface, there are three main interface areas: **Tools Menu**, **Main Menu Tree** and **Working Area**. The **Working Area** occupies the largest area of the web interface on the center right. It is also referred as the current management page. The current management page is where status is displayed; controlled are issued or parameters are configured. **Tools Menu**, near the upper left corner, provides the access to system utilities, including: Setup Wizard, Password Change, Backup & Restore, System Upgrade, Restart, Wake-on-LAN and Quick Links. **Menu Tree**, on the left side of the web interface, allows administrators to traverse to various management functions of this system. The management functions are grouped into five branches: **System** (System Settings), **Users** (User Management), **Access Points** (AP Management), **Network** (Network Settings) and **Status** (Status and Report).

OPTION	FUNCTION
System	General
	WAN 1
	WAN 2
	WAN Traffic
	LAN Port Mapping
	Service Zones
Users	Authentication
	Black List
	Policy
	Additional Control
Access Points	List
	Discovery
	Adding
	Templates
	Firmware
	Upgrade

OPTION	FUNCTION
Network	NAT
	Privilege
	Monitor IP
	Walled Garden
	Proxy Server
	DDNS
	Client Mobility
	VPN
Status	System
	Interface
	Routing Table
	Online Users
	User Logs
	E-mail & SYSLOG
Tools	Setup Wizard
	Password Change
	Backup & Restore
	System Upgrade
	Restart
	Utilities
	Quick Links

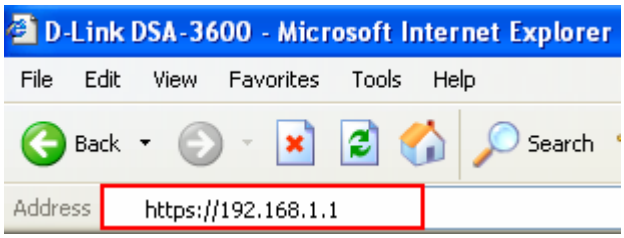
Caution: *After finishing the configuration, please click* ***Apply*** *and pay attention to see if a restart message appears at the bottom of the screen. If the message appears, the system must be restarted to allow the configurations to take effect. All on-line users will be disconnected during restart.*

- **Web Management Interface**

The DSA-3600 provides a web management interface for configuration. After completing the hardware installation, the administrator can configure the DSA-3600 via web browsers with JavaScript enabled such as Internet Explorer version 6.0 or above.

After the basic installation has been completed according to the instructions of the previous chapter, the DSA-3600 can further be configured with the following steps:

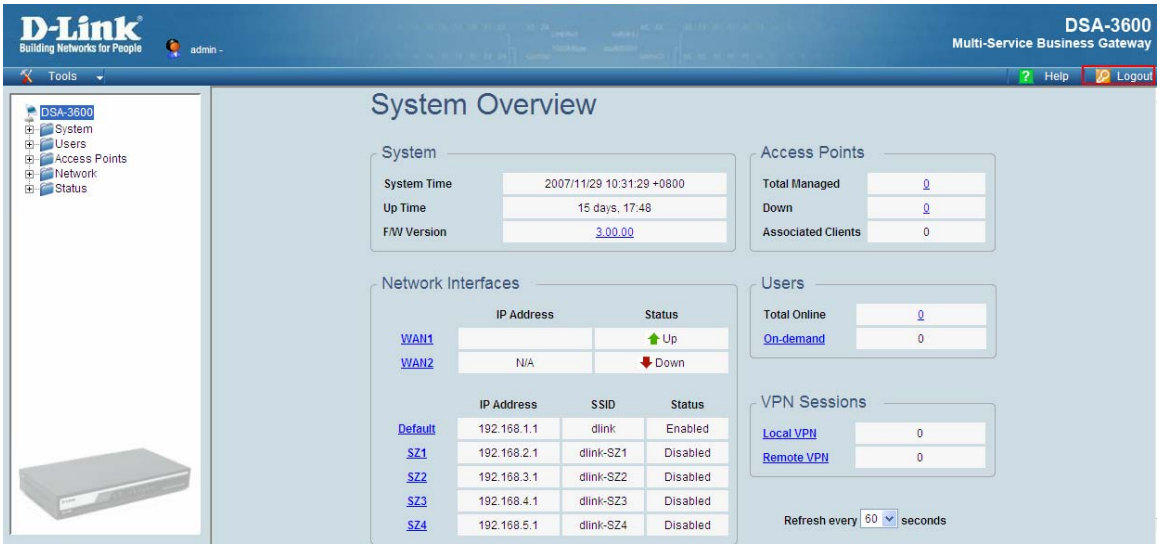
1. First, set a PC as DHCP in the network with TCP/IP setting to get an IP address from the DHCP server automatically. Next, connect the PC to the DSA-3600 via any LAN port. An IP address will be assigned to the PC automatically via the DSA-3600 built-in DHCP server. Launch a web browser to access the web management interface of DSA-3600 by entering ***"https://192.168.1.1"*** in the URL. (Note: ***https*** is used for a secured connection.)



Once the DSA-3600 has been connected, the Administrator Login Page will appear. Enter "**admin**" for both the default username and password in the Username and Password fields. Select the ***Enter*** button to log in.

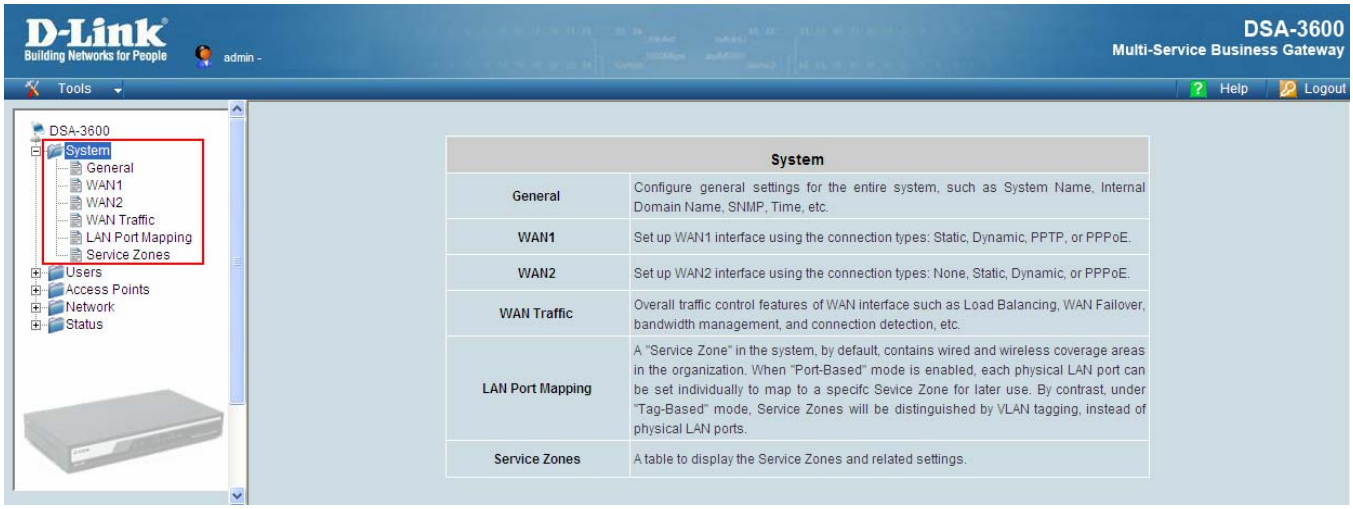
Caution: *If you are unable to get to the login screen, please check the IP address used. The IP address should be in the same subnet of the default gateway. For using static IP in TCP/IP setting, set a static IP address such as 192.168.1.x for your network interface and then open a new browser again.*

2. After successfully logging into the DSA-3600, the System Overview page of the web management interface will appear. To logout, simply click the ***Logout*** icon on the upper right corner of the interface to return to the Administrator Login Page.



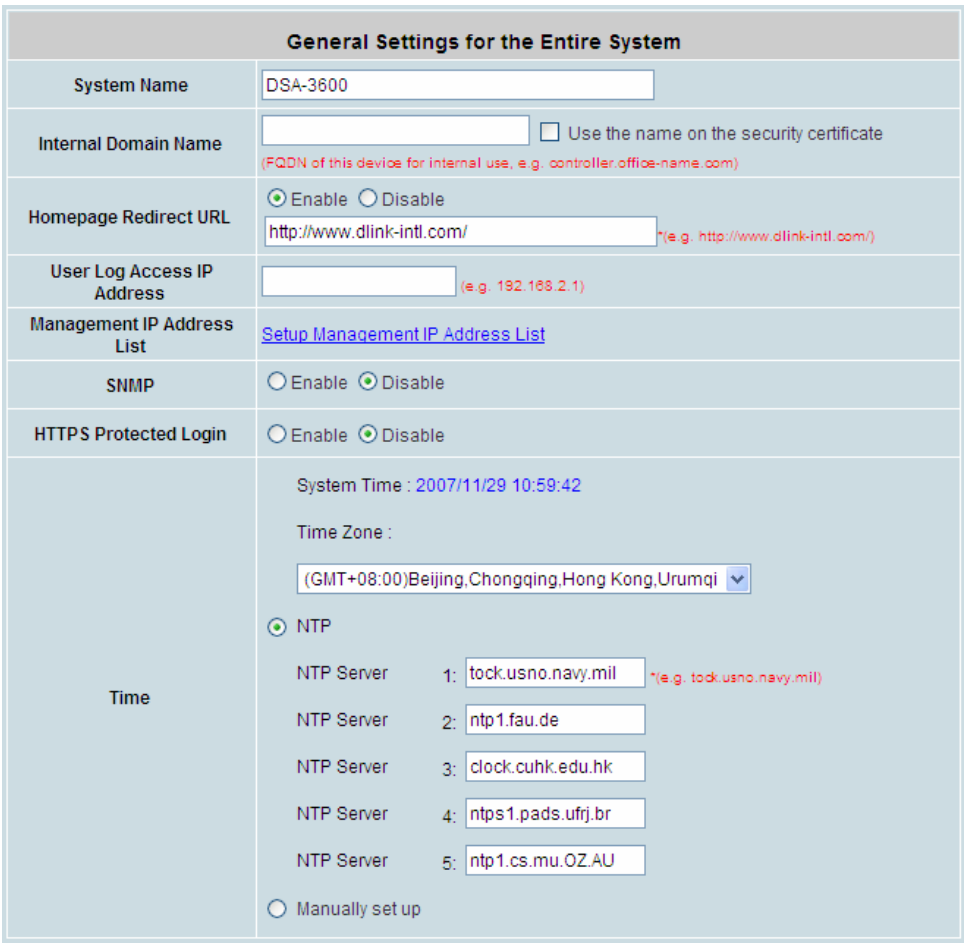
4.1 System

This section provides information on the following functions: **General**, **WAN1**, **WAN2, WAN Traffic, LAN Port Mapping** and **Service Zones**. It displays the information such as System Time, Up Time and Firmware version.



4.1.1 General

The system and network related parameters such as System Name, Homepage Redirect URL, Management IP Address List, and HTTPS Protected Login can be configured from the menu shown as below.

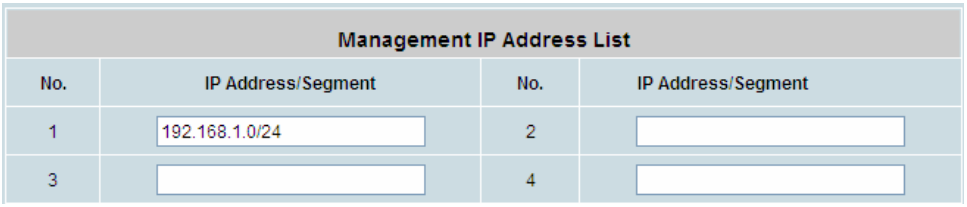


- **System Name:** Set the name of the system or use the default.
- **Internet Domain Name:** A fully qualified domain name (FQDN) of the system. When the administrator enters a desired domain name in the Internal Domain Name field, the entered Internal Domain Name will be shown in the top left of the Login Success page instead of an LAN IP address. In addition, when HTTPS is enabled, entering the domain name of the uploaded certificate will increase login speed and the URL in the User Login page will be changed. For example, if the Internal Domain Name is configured as ashop.com, the URL in the User Login page will be https://ashop.com/loginpages/login.shtml.
- **Homepage Redirect URL:** Enter a URL in this field. When the clients are logged-in to the DSA-3600 successfully, their browsers will be directed to this URL regardless of the original homepage setting in their browsers when Local VPN is disabled.
- **User Log Access IP Address:** An external billing system may access the system's user logs by specifying a desired IP address of the external billing system in this field. Only the billing system with this IP address may directly access the system's user logs in text format via browsers. For example, if the access interface of DSA-3600 is “10.30.1.23”, the user log can be found in following URLs.

  User Log is located in the URL：https://10.30.1.23/status/history/2006-11-01

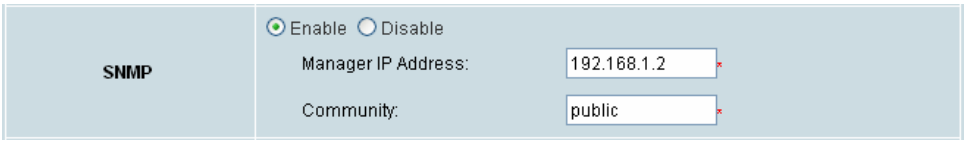
  On-demand User Log is located in the URL：https://10.30.1.23/status/odhistory/2006-11-01

- **Management IP Address List:** Set the IP addresses within a range which the administrator can use to connect to the web management interface of DSA-3600 via its WAN and/or LAN ports. The administrator can grant the access of the web management interface by specifying a list specific IP address or ranges of IP addresses, no matter the access is from WAN or LAN port. For example, entering "192.168.3.1" and "192.168.1.0/24" means the computer at 192.168.3.1 and the computers the range of 192.168.1.0 to 192.168.1.255 are able to reach the web management interface.

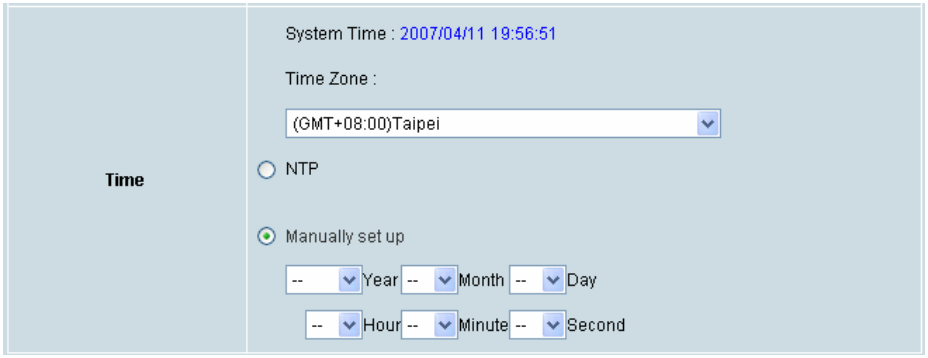


***Please Note**: While the default IP address of Network Interface is changed at System→Service Zones→Basic Settings→DHCP Server→Enable DHCP Server, the management IP address has to be setup again from default IP address to the new IP as the format, x.x.x.x/x.*

- **SNMP:** The DSA-3600 supports SNMPv2. When the function is enabled, an implemented SNMP server is able to access the system's management information base.

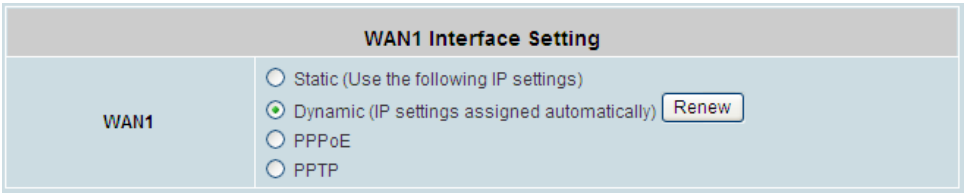


- **HTTPS Protected Login:** The system supports HTTPS (encrypted) and HTTP (non-encrypted) when clients log into the system. When this function is enabled, the Secured Socket Layer (SSL) will be activated and implemented to the web-based user login page.
- **Time:** The system time can be set up manually or synchronized with remote NTP (Network Time Protocol) servers. It supports up to five NTP servers. When ***NTP*** is enabled, at least one NTP server has to be configured and the system time will be adjusted automatically according to the remote NTP servers. When manually set up is enabled, the administrator needs to set configurations manually. The system time can also be manually configured when selecting ***Manually set up***. Please enter the date and time into the respective fields.

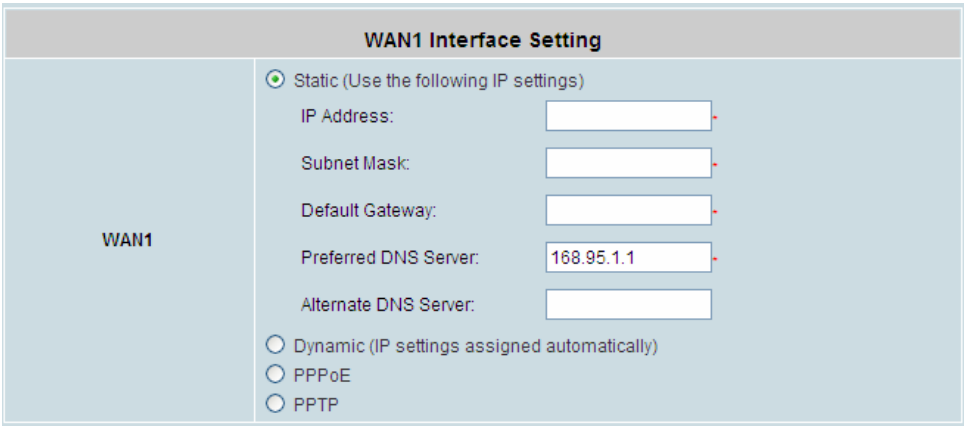


4.1.2 WAN1

There are four connection types supported on the WAN1 Port: **Static**, **Dynamic**, **PPPoE**, and **PPTP**.



- **Static (Use the following IP Settings):** Select **Static** to specify a static IP address for WAN1 port manually when a static IP address is available for DSA-3600. Fields with red asterisks are required to be filled in.



IP Address: The IP address of the WAN1 port.

Subnet Mask: The subnet mask of the WAN1 port.

Default Gateway: The gateway of the WAN1 port.

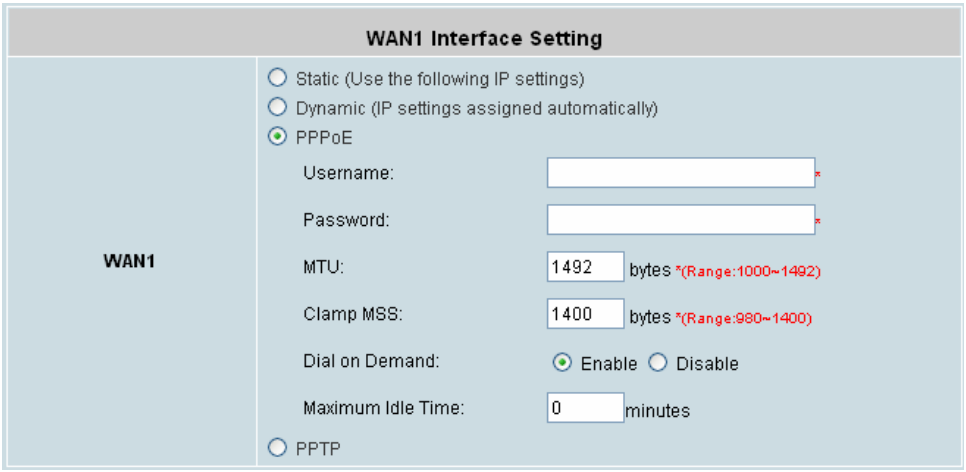
Preferred DNS Server: The primary DNS Server of the WAN1 port.

Alternate DNS Server: The substitute DNS Server of the WAN1 port. This is optional.

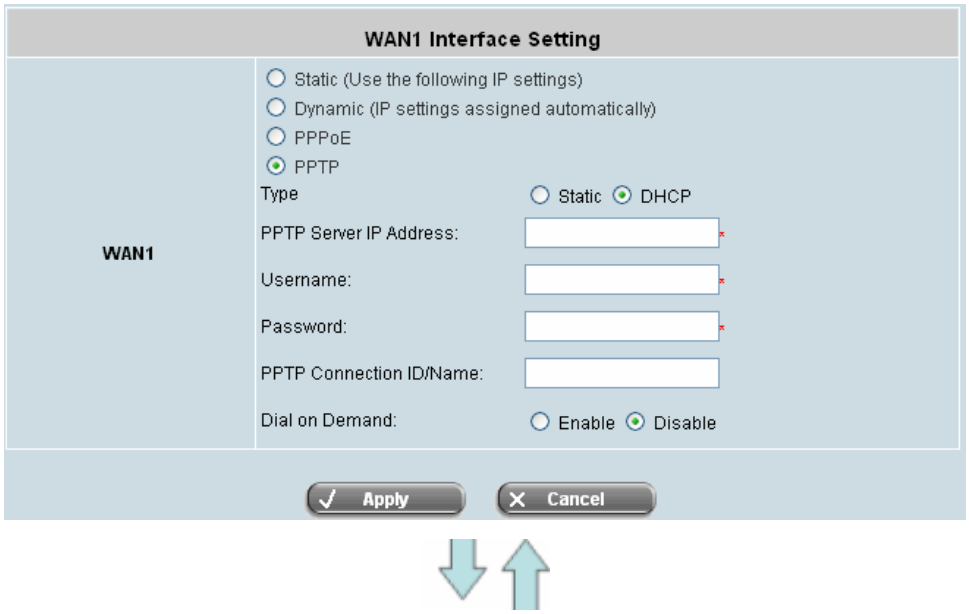
- **Dynamic (IP settings assigned automatically):** Select the option when a DHCP server is available in the network implementation above the WAN1 port of the system. When Dynamic is selected, the system works as a DHCP client and get an IP address for its WAN1 port automatically from the DHCP server.

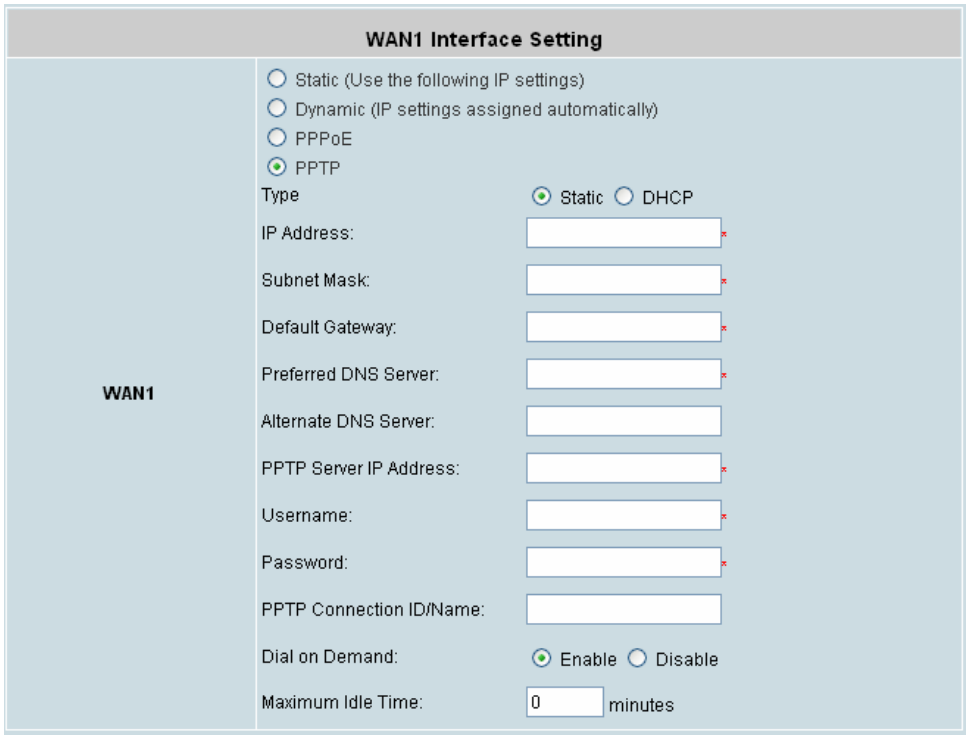
- **PPPoE:** Select the option when PPPoE is the connection protocol provided by the network service providers. When **Dial on Demand** is enabled, there is a Maximum Idle Time available. The system will disconnect itself from the Internet automatically when the Maximum Idle Time is reached.

  To properly configure PPPoE connection type, the **Username**, **Password**, **MTU** and **Clamp MSS** fields are required. The **Dial on Demand** function is used to guard the idle time out of the connection. The **Maximum Idle Time** field is required to enable this function. When the idle time is reached, the connection will be automatically disconnected.



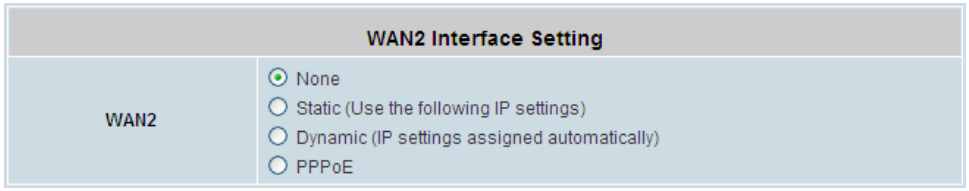
- **PPTP:** Select the option when PPTP (Point to Point Tunneling Protocol) is the connection protocol provided by the network service providers. When **Dial on Demand** is enabled, there is a Maximum Idle Time available. The system will disconnect itself from the Internet automatically when the Maximum Idle Time is reached.



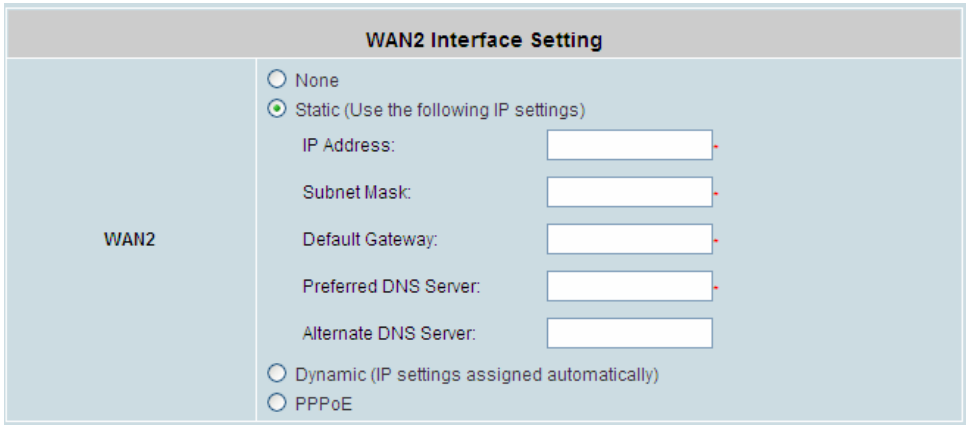

WAN1 Interface Setting
WAN1
Static (Use the following IP settings)
Dynamic (IP settings assigned automatically)
PPPoE
PPTP
Type
Static
DHCP
IP Address:
Subnet Mask:
Default Gateway:
Preferred DNS Server:
Alternate DNS Server:
PPTP Server IP Address:
Username:
Password:
PPTP Connection ID/Name:
Dial on Demand:
Enable
Disable
Maximum Idle Time:
0
minutes

4.1.3 WAN2

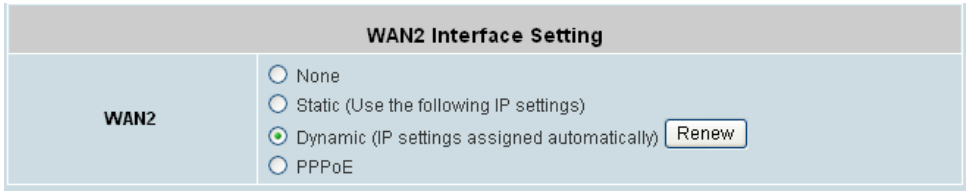
WAN2 can be disabled when selecting **None**. When WAN2 Port is enabled, it supports 3 connection types: **Static**, **Dynamic** and **PPPoE**.



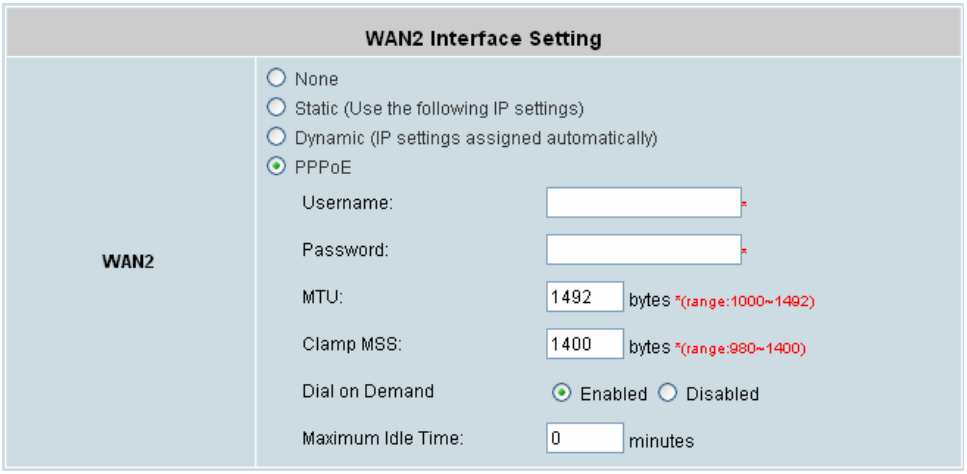
- **None**: The WAN2 Port is disabled.
- **Static:** Select the option to specify a static IP address for WAN2 interface manually when a static IP address is available for the system. Specify the **IP Address**, **Subnet Mask**, **Default Gateway, Preferred DSN Server and Alternate DSN Server** of WAN2 Port, which should be applicable for the network environment.



- **Dynamic (IP settings assigned automatically):** Select the option when a DHCP server is available in the network implementation above the WAN2 port of the system. When Dynamic is selected, the system works as a DHCP client and get an IP address for its WAN2 port automatically from the DHCP server.

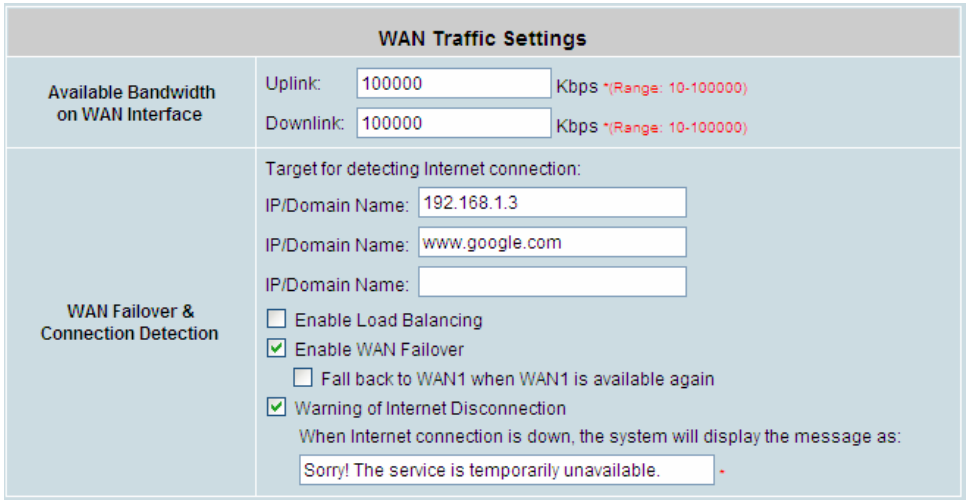


- **PPPoE:** Select the option when PPPoE is the connection protocol provided by the network service providers. When Dial on Demand is enabled, there is a Maximum Idle Time available. The system will disconnect itself from the Internet automatically when the Maximum Idle Time is reached. This is the common connection type for ADSL. To properly configure PPPoE connection type, the **Username**, **Password**, **MTU** and **Clamp MSS** fields are required. The **Dial on Demand** function is used to guard the idle time out of the connection. The **Maximum Idle Time** field is required to enable this function. When the idle time is reached, the connection will be automatically disconnected.


WAN2 Interface Setting
WAN2
None
Static (Use the following IP settings)
Dynamic (IP settings assigned automatically)
PPPoE
Username:
Password:
MTU:
1492
bytes *(range:1000~1492)
Clamp MSS:
1400
bytes *(range:980~1400)
Dial on Demand
Enabled
Disabled
Maximum Idle Time:
0
minutes

4.1.4 WAN Traffic

DSA-3600 supports uplink/downlink bandwidth management and WAN Failover features, including WAN Failover, Load Balancing and Connection Detection features.

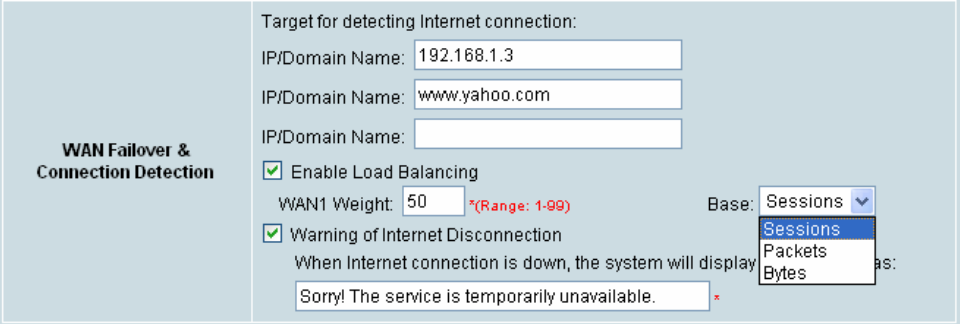


Available Bandwidth on WAN Interface:

- **Uplink:** It defines the maximum uplink bandwidth allowed to share by clients within WAN interface.
- **Downlink:** It defines the maximum downlink bandwidth allowed to share by clients within WAN interface.

WAN Failover & Connection Detection: The DSA-3600 supports WAN Failover, Load Balancing feature and the ability to detect WAN connection.

- **Target for detecting Internet connection:** To verify the connection to the Internet, the system keeps up to three Target IP or Domain Name. These targets are used for the system as the detected targets of **Enable Load Balancing** and **Warning of Internet Disconnection**. To enable WAN Failover, at least one target must be configured.
- **Enable Load Balancing:** Check this option to active the system's load balance function. System will allot all traffic to WAN1 and WAN2 by the weight radio. The weight radio between WAN1 and WAN2 can be based on Sessions, Packets or Bytes.
  - **WAN1 Weight:** Enter value range between 1~99. The default is 50.
  - **Base:** Three bases of the Load Balancing ratio are supported, **session**, **packet**, and **byte**. Packet and Byte are based on historic downlink data. New connection sessions will be distributed between WAN1 and WAN2 by a weight ratio using random number.
    - Limitation:
      - DMZ hosts will be excluded from WAN Load Balancing.
      - SIP authentication is excluded from WAN Load Balancing.



- **Enable WAN Failover:** The purpose of WAN Failover is to have a backup link for WAN1 when WAN2 is available. Check the check box of Enable WAN Failover to active the WAN failover function of the DSA-3600. Normally a service zone uses WAN1 as it primary gateway. When WAN Failover is enabled, WAN1's traffic will be routed to WAN2 when WAN1 connection is down. On the other hand, a service zone's policy can also use WAN2 as its gateway; in that case, if WAN2 is down, the WAN2's traffic under its policy also will 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. A **Fall back to WAN1 when WAN1 is available again** function will appear when Enable WAN Failover check box is checked. If **Fall back to WAN1 when WAN1 is available again** function is enabled, the routed traffic will be back to WAN1 when WAN1 connection is recovered.
- **Warning of Internet Disconnection:** An Internet disconnection detection feature is supported by the system. Check the check box of **Warning of Internet Disconnection** will enable this function. 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.

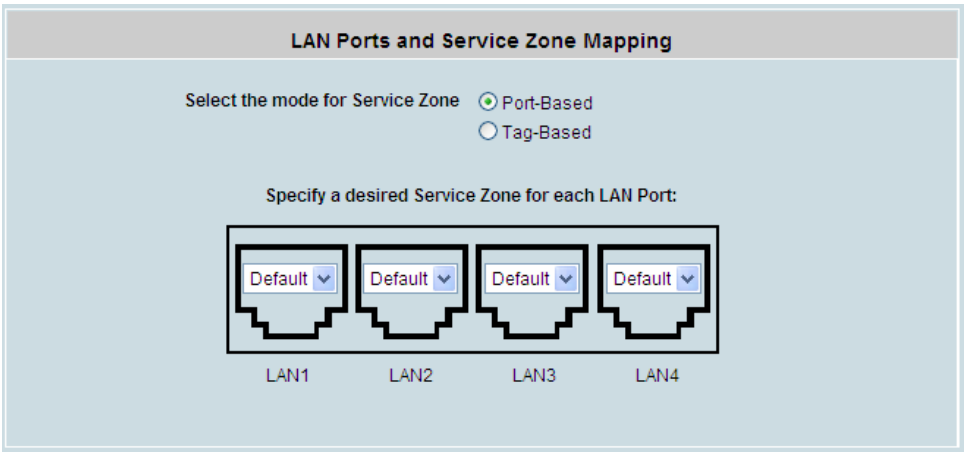
Note: *SIP authentication is exempt from* ***Load Balancing*** *and* ***WAN Failover****. A fixed WAN port is chosen for SIP traffic.*

4.1.5 LAN Port Mapping

DSA-3600 supports multiple service zones in either of the two VLAN modes, **Port-Based** or **Tag-Based**, but not concurrently. In the wireless environment, a service zone of the DSA-3600 is mapped to the VLAN with an associated SSID. When the DSA-3600 is set for tag-based VLAN, a managed Access Point with multiple SSIDs turned on can service multiple service zones. It is recommended that the administrator decides a mode before the system configuration when considering which mode is better for a multiple-service-zone deployment.

In LAN Port Mapping, the service zones can be configured by modes, **Port-Based,** which will be distinguished by physical LAN ports, or **Tag-Based**, which will be distinguished by VLAN tagging. Each LAN port of Port-Based mode can be selected among **Default** to **SZ1~SZ4**.

Supporting multiple service zones, one D-Link DSA-3600 system can behave virtually like multiple systems. Each service zone is one-to-one mapped to a VLAN. Messages to or from each service zone are sorted by the VLAN tag in the message frame.

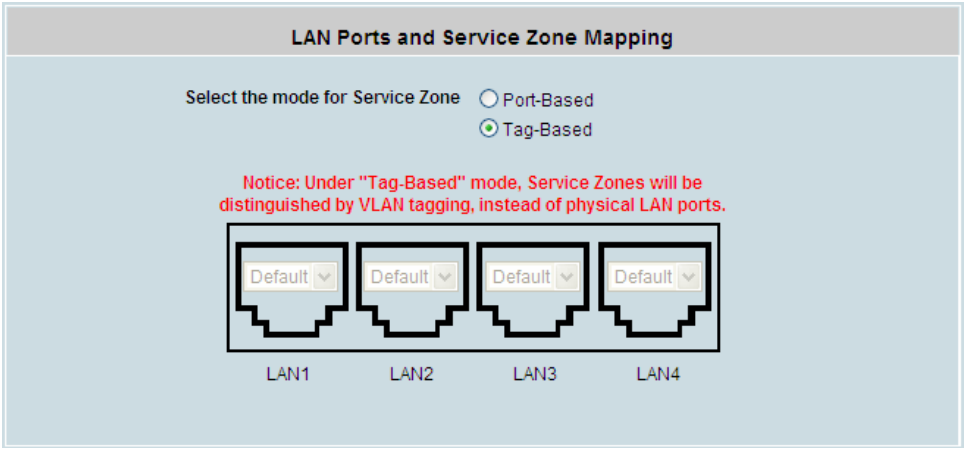


- **Tag-Based:**
  For Tag-Based service zone, each LAN port is Hybrid port, which supports both tagged and untagged frames. Each port can join any VLAN (up to 4) group.

  The system supports five service zones, one default and other 4 service zones; each can be enabled or disabled except the default one. The five service zones are mapped to 4 VLANs and 1 untagged subnet. Each service zone functions like a virtual system; each has an independent set of settings such as SSID, Wireless Security, Network setting, DHCP setting, Customized Pages, Default Policy, Authentication Servers setting and Default Authentication Server.

➢ **Tag-based Service Zones Configuration Example – Enabling Two Service Zones**

Log in to the web management interface and enter **"admin"** for both the default username and password in the Username and Password fields of the Administrator Login Page. After logging-in the web management interface, from the Menu Tree, click ***System*** and then click ***LAN Port Mapping*** to verify that **Tag-Based** service zone mode is selected.

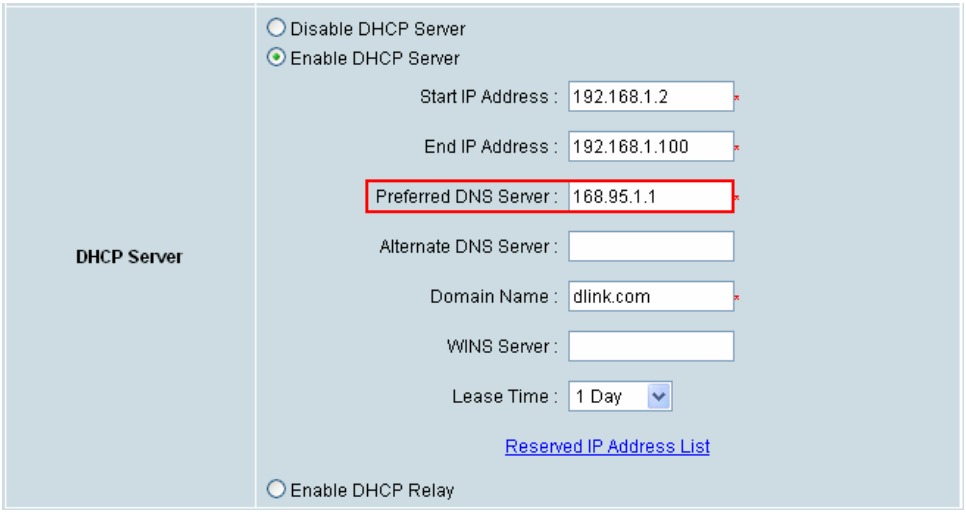


Click ***System*** and then click ***Service Zones*** to enter the **Service Zone Settings** page as shown below.

Service Zone Settings

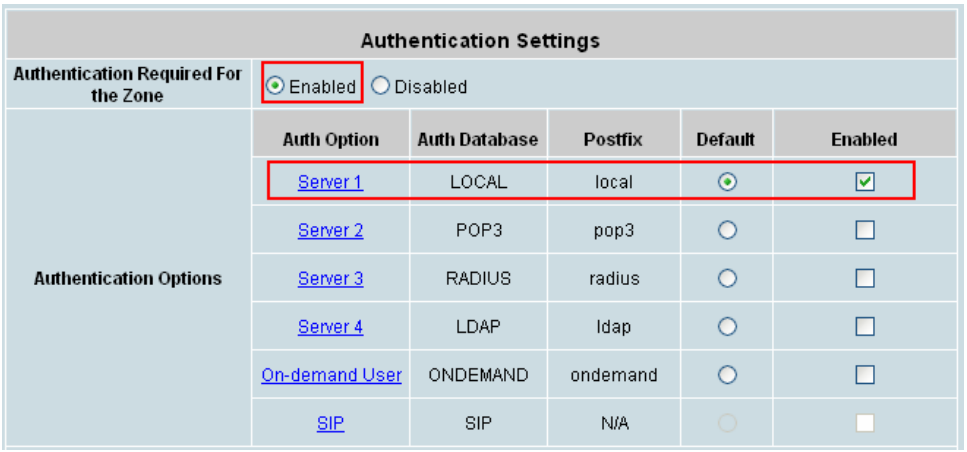
Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default	N/A	dlink	None	None	Server 1	Enabled	Configure
SZ1	1	dlink-SZ1	None	None	Server 1	Disabled	Configure
SZ2	2	dlink-SZ2	None	None	Server 1	Disabled	Configure
SZ3	3	dlink-SZ3	None	None	Server 1	Disabled	Configure
SZ4	4	dlink-SZ4	None	None	Server 1	Disabled	Configure

Click the ***Configure*** button of Default Service zone to enter its Basic Settings page. While in this Basic Settings page, enter an IP address for **Preferred DNS Server** in the area of DHCP Server. (Empty **Preferred DNS Server** will result in problems when using the Internet.)



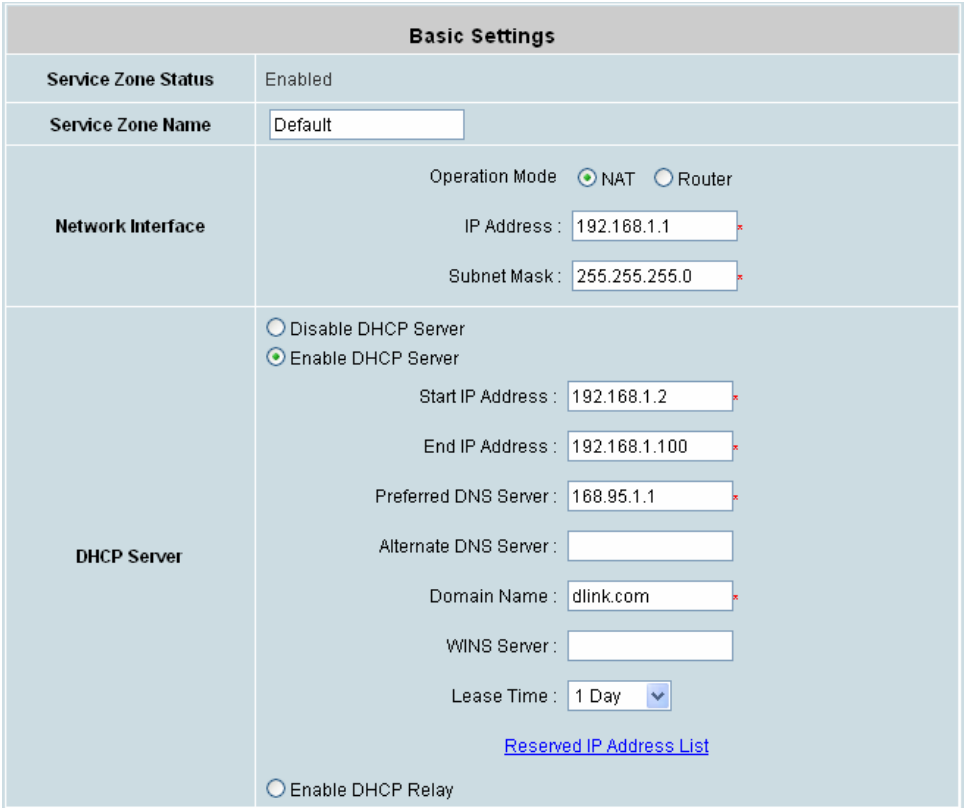
Scroll down to near bottom of page and in the Wireless Settings area enter the **SSID** (e.g. ssid-staff) for connecting to this service zone.

Scroll up to the middle of the page where the **Authentication Settings** is, and check the ***Enabled*** box for the **Authentication Required for the Zone** option. The users will now need to be authenticated to connect to the service zone. Make sure only Server1 is checked ***Enabled*** for this service zone.

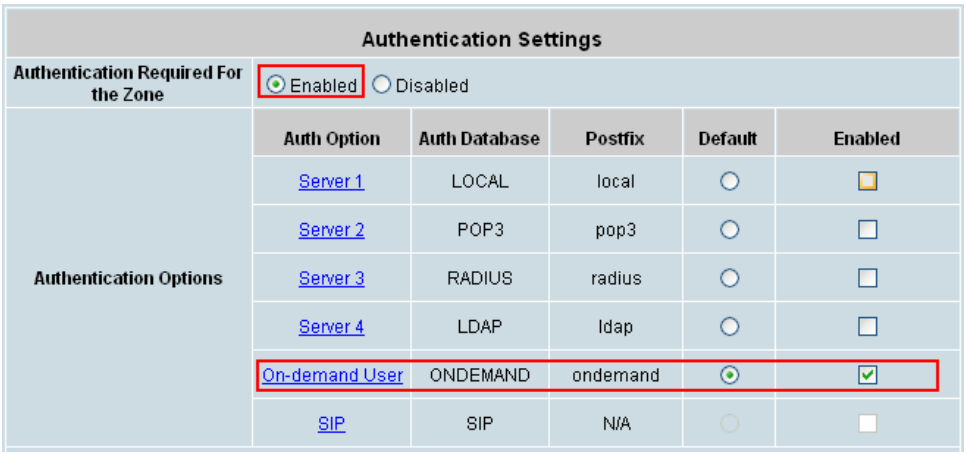


Click the ***Apply*** button to activate the changes for the default service zone. (We can restart the system later, since we want to continue to configure a second service zone for the on-demand users.)

Following similar procedures, click on **Service Zones** menu item on the Menu Tree again, this time is to configure another service zone such as SZ1. Enter its Basic Settings page. Enable the service zone, enter the IP address of the **Preferred DNS server**, and set its **SSID** for On-demand users such as '**ssid-guest**'.



Remember to enable Authentication requirement for this service zone and enable the **On-demand Users** authentication options only.



Click ***Apply*** to activate the changes for the second service zone. Now is the time to restart the system. After the restart, the system will be configured according to Figure-4.1.5a.

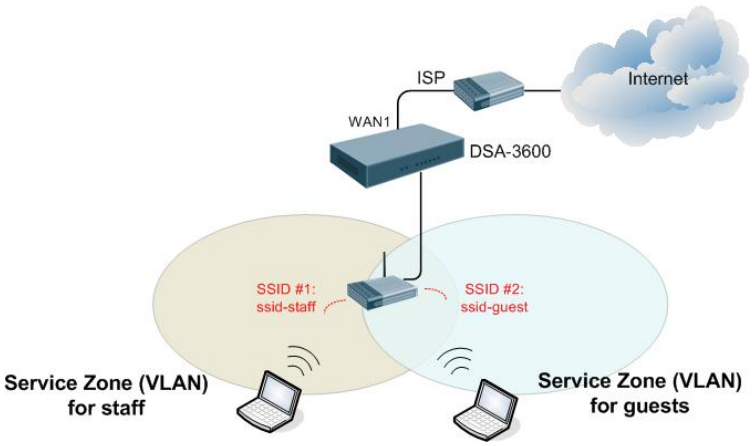


Figure-4.1.5a: An example using Tag-Based service zones

- **Port-Based:**

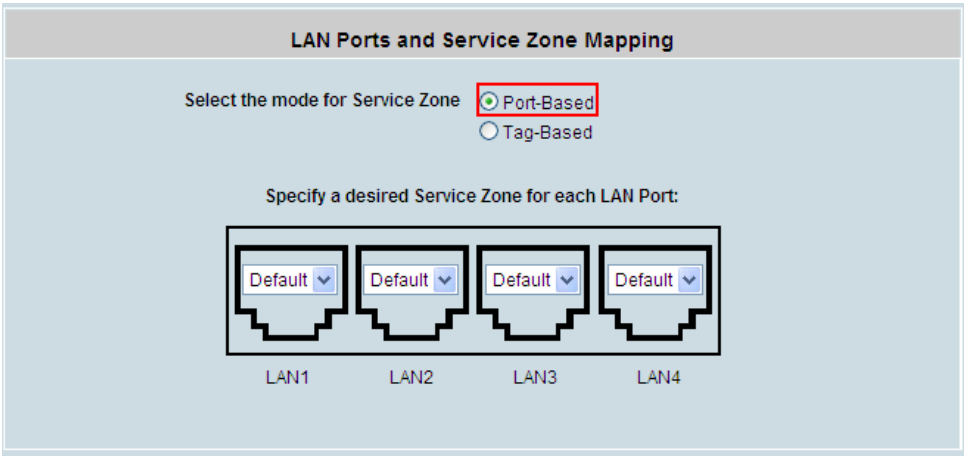
  For port-based service zone, each LAN port can be assigned to a service zone since a LAN port can be mapped to a VLAN tag. The mapping between the ports and the service zones are many-to-one. With factory default setting, all ports belong to the Default service zone and other 4 service zones are gray-out. The other 4 service zones will appear after the specific service zone is configured as enabled in System--Service Zones.

  ➢ **Port-Based Service Zones Configuration Example**

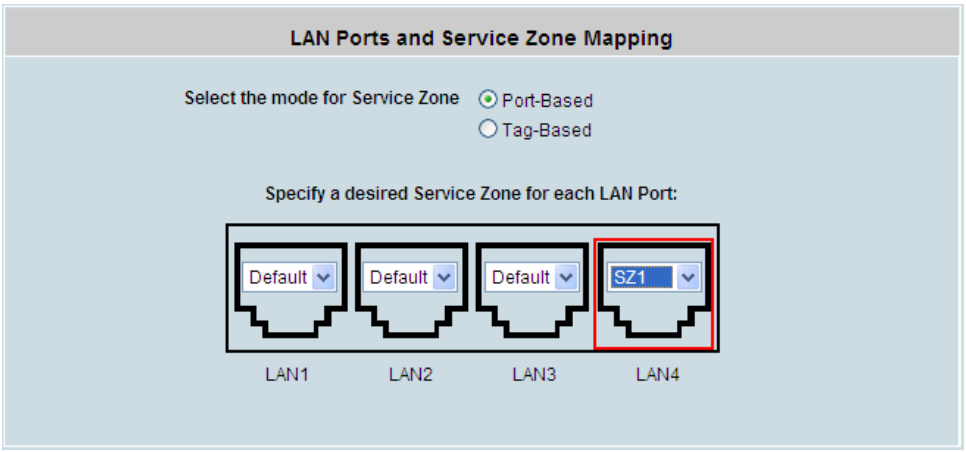
  After running through **Setup Wizard** on a factory default system, the DSA-3600 is ready to use the default tag-based VLAN for separating networks.

  Log in to the web management interface and enter **"admin"** for both the default username and password in the Username and Password fields of the Administrator Login Page. After logging-in the web management interface, from the Menu Tree, click **System** then **Service Zones** to enter the Service Zone Settings page. Click ***Configure*** of the desired service zone to enter its Basic Settings page, and then enable the service zone used for port-based service zone deployment.

Click ***System*** from the Menu Tree and then click ***LAN Port Mapping***. Select **Port-Based** mode for service zone.



Assume LAN1, LAN2, LAN3 will be used by Default service zone for internal staff while LAN4 is to be assigned to another service zone for external users only. In the above mentioned page, click **LAN4**'s drop-down menu to select the desired second zone such as 'SZ1' for LAN4 (select only enabled service zones). Click ***Apply*** and reboot the system.



In tag-based mode, each LAN port can serve traffic from any service zone because VLAN tags carried in message frame will not be modified. In port-based mode, each LAN port can only service traffic of one service zone, where all messages through the LAN port will be re-tagged with the tag assigned to the port. Compare Figure-4.1.5a and Figure-4.1.5b to see the differences.

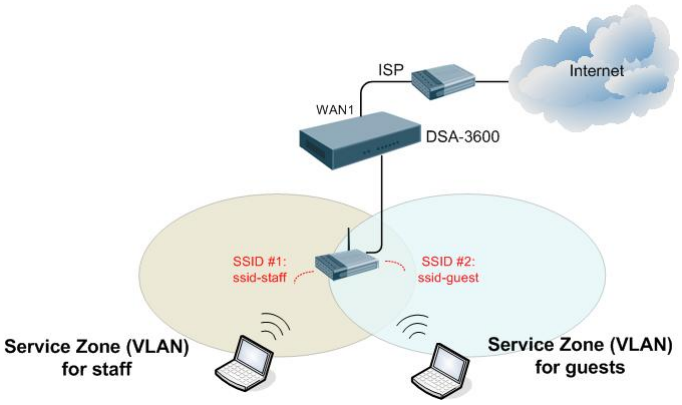


Figure-4.1.5a: An example using Tag-Based service zones

For single zone deployment, use the Default service zone with port-based mode.

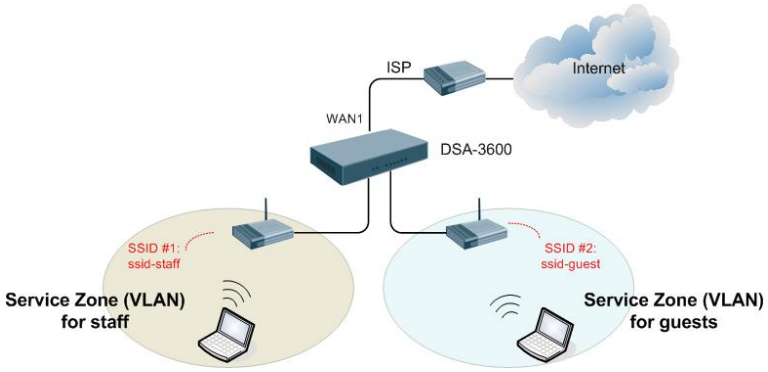


Figure-4.1.5b: An example using Port-Based service zones

4.1.6 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.

For more details about Service Zones, please refer to Appendix E and F.

Service Zone Settings

Service Zone Name	LAN Port Mapping	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default		dlink	None	None	Server 1	Enabled	Configure
SZ1		dlink-SZ1	None	None	Server 1	Disabled	Configure
SZ2		dlink-SZ2	None	None	Server 1	Disabled	Configure
SZ3		dlink-SZ3	None	None	Server 1	Disabled	Configure
SZ4		dlink-SZ4	None	None	Server 1	Disabled	Configure

Service Zone Settings

Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default	N/A	dlink	None	None	Server 1	Enabled	Configure
SZ1	1	dlink-SZ1	None	None	Server 1	Disabled	Configure
SZ2	2	dlink-SZ2	None	None	Server 1	Disabled	Configure
SZ3	3	dlink-SZ3	None	None	Server 1	Disabled	Configure
SZ4	4	dlink-SZ4	None	None	Server 1	Disabled	Configure

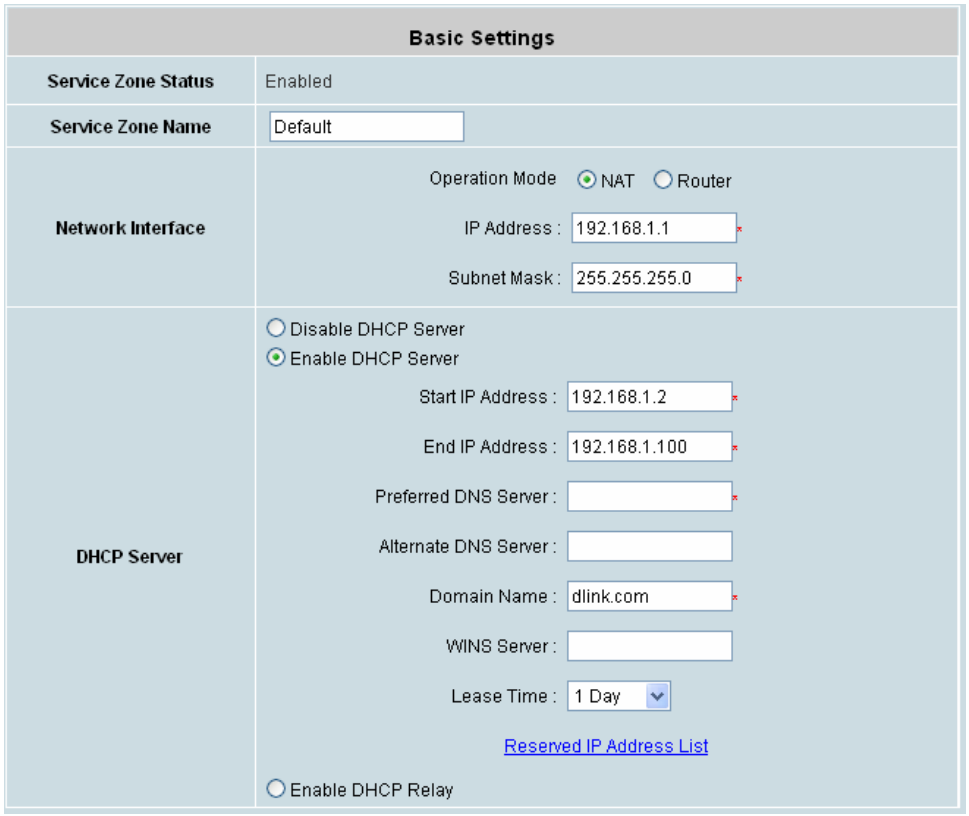
- **Service Zone Name:** Mnemonic name of the Service Zone.
- **LAN Port Mapping:** When the system is set to Port-based mode for Service Zones, it shows the physical LAN ports that belong to the specific Service Zone.
- **VLAN Tag:** When the system is set to Tag-based mode for Service Zones, it shows the VLAN tag number that is mapped to the specific 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 Option:** Default authentication database/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 the button of ***Configure*** to configure each Service Zone: **Basic Settings**, **SIP Interface Configuration**, **Authentication Settings** and **Wireless Settings**. The managed AP(s) in the specific service zone will be shown in this page as well if there are APs set in this service zone.

Basic Settings

The system supports three types of DHCP modes, **Disable DHCP Server**, **Enable DHCP server**, and **Enable DHCP relay**. Each service zone can have its own DHCP setting. Select the radio button of Disable DHCP Server to disable the built-in DHCP server when clients are assigned static IP addresses. Select the radio button of Enable DHCP Server to enable the built-in DHCP server. When the Enable DHCP server is chosen, the system will act as a DHCP server and assign IP addresses to its clients. Select the radio button of Enable DHCP Relay when a service zone is connected to an external DHCP server. When Enable DHCP Relay is chosen, the IP addresses of clients will be assigned by the external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this service zone.



- **Service Zone Status:** Each service zone can be enabled or disabled except the default service zone.
- **Service Zone Name:** The name of service zone can be input here. Service name can accept 'space', <, > and double-quote and etc.
- **Network Interface:**
  - **Operation Mode:** The system supports **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:** The system supports three types of DHCP modes, Disable DHCP server, Enable DHCP server or Enable DHCP Relay.

- **Enable DHCP server:** This allows the enabling the DHCP server.
- **Start IP / End IP:** Set a range of IP addresses that built-in DHCP server will assign to clients. Please change it accordingly at *System→General→Management IP Address List* to let the administrator to login to the DSA-3600 admin page after the default IP address of Network Interface is changed.
- **Domain Name:** Enter the Windows domain name for this service zone.
- **WIN 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 some IP addresses from predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. The administrator can reserve some specific IP addresses for special devices with MAC address.
- **Enable DHCP Relay:** Selecting the radio when a service zone is connected to an external DHCP server. When Enable DHCP Relay is chosen, 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.

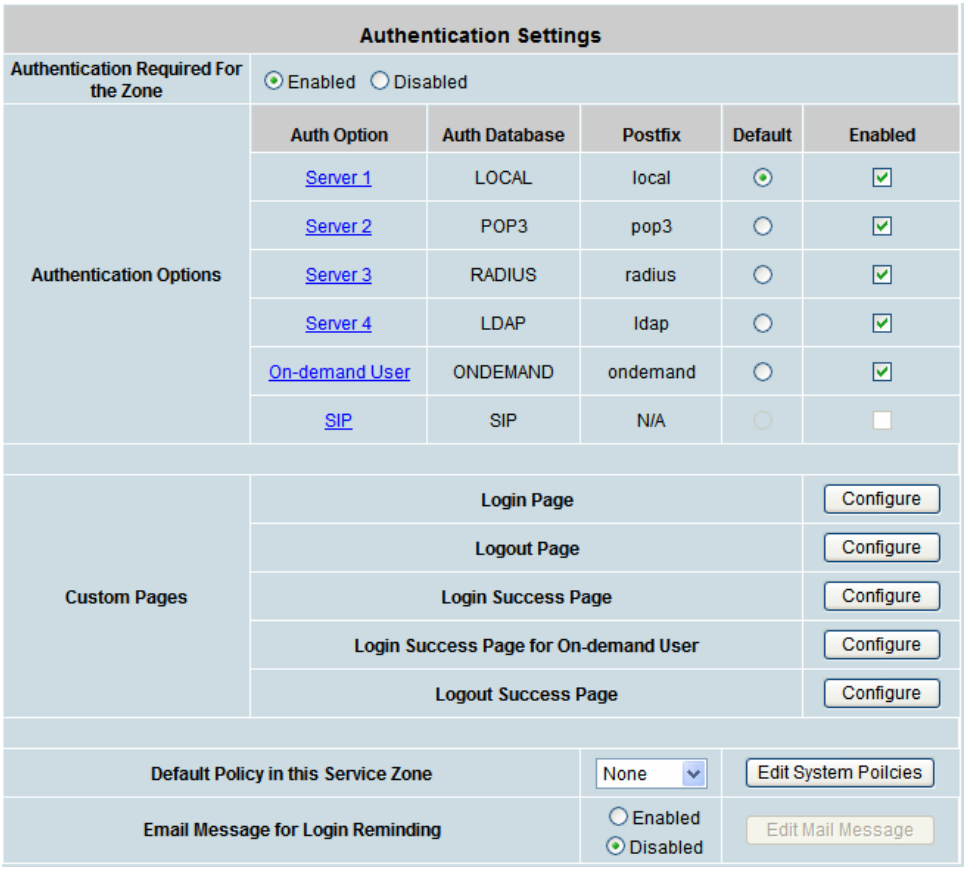
▪ *SIP Interface Configuration*

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 traffics.

- ***Authentication Settings***

The system supports several authentication databases that are **Local**, **POP3**, **RADIUS**, **LDAP**, and **NT Domain** and provides up to four authentication options **Server1~4**, one **On-demand Users** authentication option and one **SIP** authentication. The administrator needs to activate and configure at least one of these authentication databases for an enabled service zone. Postfix is used to inform the system which type of authentication database to be used for authentication when multiple databases are concurrently in use. Each authentication option is distinguished by the postfix in clients' username such as "user1@Local". One of authentication database (except SIP Authentication) can be assigned as Default for a service zone. For authentication option assigned as default, the postfix can be omitted while entering username.



- **Authentication Required for the Zone**

  Enable or disable this feature.

- **Authentication Options**

  Click the hyperlink of **Auth Option**, the **Authentication option** page will appear, options including **Server1** to **Server4**, **On-demand Users** and **SIP.**

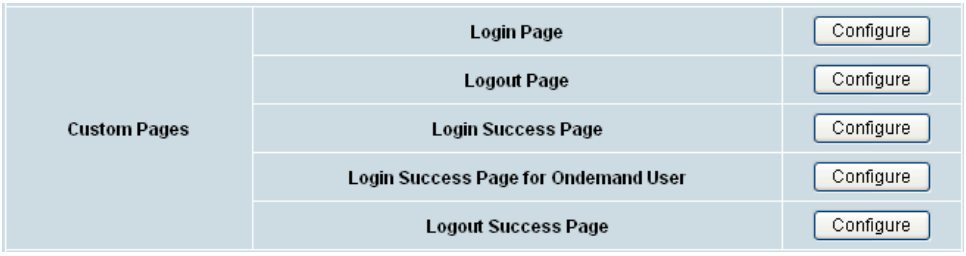
  - **Authentication Database:**

    The system supports several types of authentication database that are **Local, POP3**, **RADIUS**, **LDAP**, and **NT Domain**, and provides up to four authentication options and one **On-demand Users** authentication option and **SIP** authentication. Select the desired method and then click the link besides the pull-down menu for more advanced configuration.

    For more information on **Authentication Methods,** please refer to next section **4.2.1 Authentication.**

- **Default Policy in this Service Zone:** Multiple sets of policy are provided by the system. 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 service zone. All clients belong to this service zone will be bound by this policy. But when RADIUS is the selected Authentication Database, the **Class-Policy Mapping** function will be available to let the administrator assign a policy for a RADIUS Class. Also when LDAP is the selected Authentication Database, the **Attribute-Policy Mapping** function will be available to let the administrator assign a policy for a LDAP Attribute. Please refer to **4.2.3 Policy→Policy1~12**.
- **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 ***Enabled*** and ***Edit Mail Message*** to edit the message in HTML format. Each service zone can has its own message.
- **Custom Pages:** There are five users' login and logout pages that can be customized by administrators for each service zone.

  Click the button ***Configure***, and the **Login (Logout)** page will appear, with configuration options for **Login Page**, **Logout Page**, **Login Success Page**, **Login Success Page for On-demand User** and **Logout Success Page.** Click the button of the respective page selections to make further configuration.

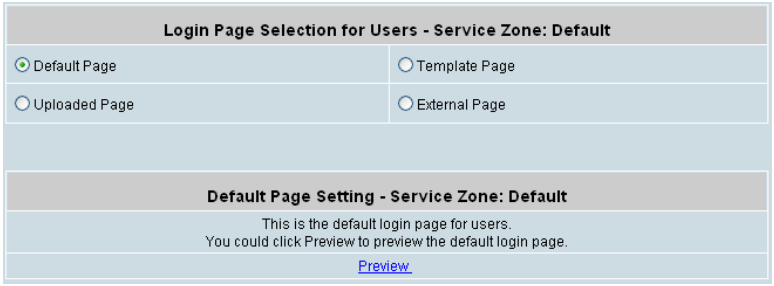


1) Login Page

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.

- *Login Page→**Default Page***

  Choose Default Page to use the default login page.

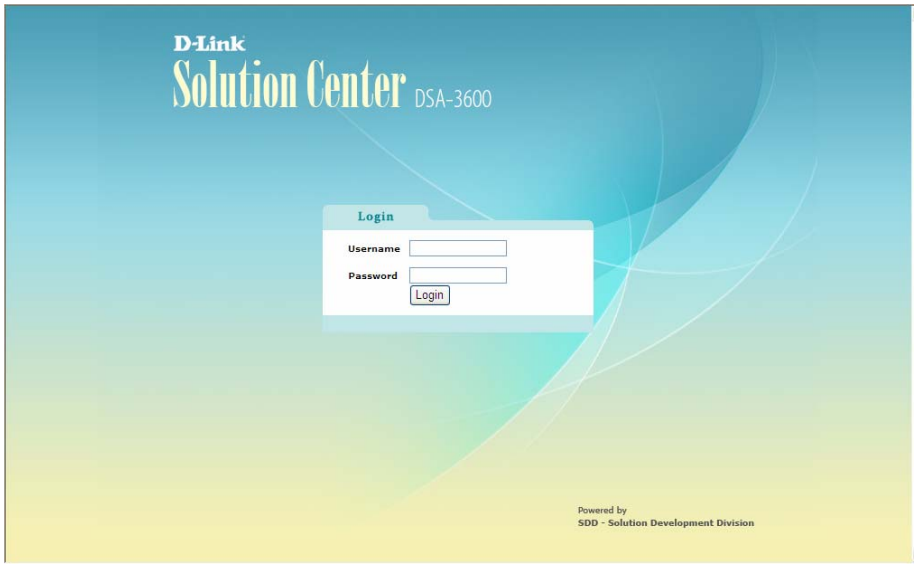


- *Login Page →**Template Page***

  Choose Template Page to make a customized login page. All customizable items are shown here. Click Select to pick up a color for the title, text, and the background in the center area and change the wording of each item as needed. In addition, a logo and a background image can be used to create a customized page for branding or other purpose. Click Preview to see the result first.

Template Page Setting	
Color for Title Background	80C0FF Select (RGB values in hex mode)
Color for Title Text	000080 Select (RGB values in hex mode)
Color for Page Background	FFFFFF Select (RGB values in hex mode)
Color for Page Text	000080 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
Cancel	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	

An example of Template Login Page:



- *Login Page* → ***Uploaded Page***

  Choose Uploaded Page and upload a login page.

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

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

  If the user-defined login page includes an image file, the image file path in the HTML code must be as follows.

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”>**

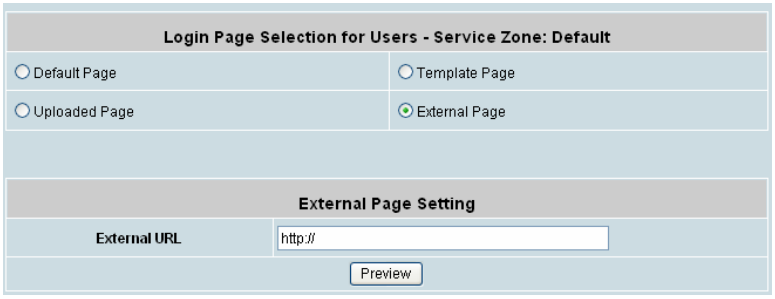
  Click the ***Browse*** button to select the file to upload. Then click ***Submit*** to complete the upload process.

  Next, enter or browse the filename of the images to be uploaded 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 bottom.

- *Login Pages* → ***External Page***



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.

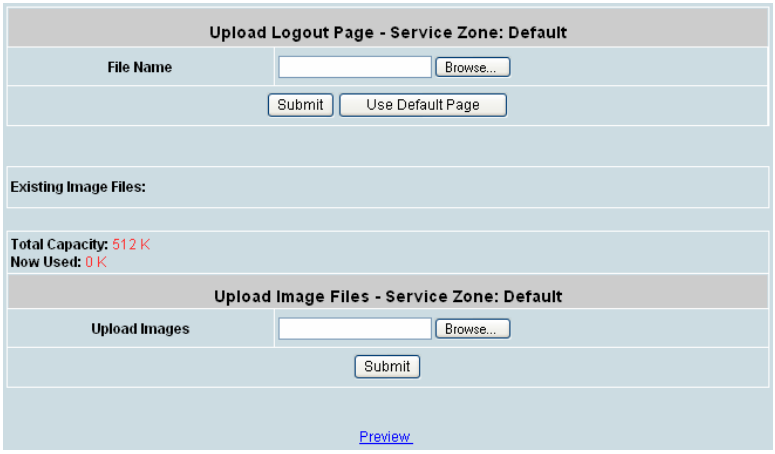
The user-defined login page must include the following HTML codes to provide the necessary fields for username and password.

```
<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>
```

For example, the device name of one DSA-3600 is ”abc.3322.org” then the first line of the html code would be “https://abc.3322.org/loginpages/userlogin.shtml”

2) 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 instructions on *Login Page → Uploaded Page* for details.



***Please Note**: While this process is similar to that of the Login Page, the HTML code for the user-defined logout interface however is different. The following HTML code must be added in order for the user to enter the username and password.*

```
<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>
```

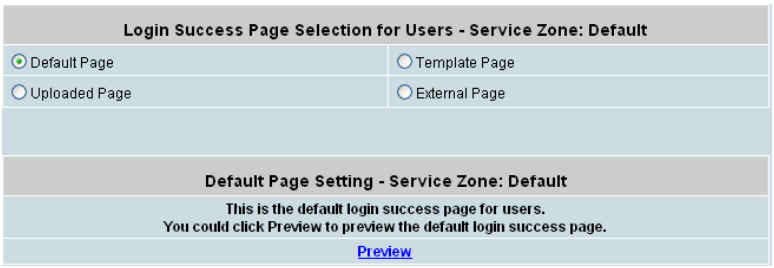
After the upload is completed, the customized logout page can be previewed by clicking ***Preview*** at the bottom of this page. If restore to factory default setting is needed for the logout interface, click the "**Use Default Page"** button.

3) Login Success Page

The administrators can apply their own Login Success page. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

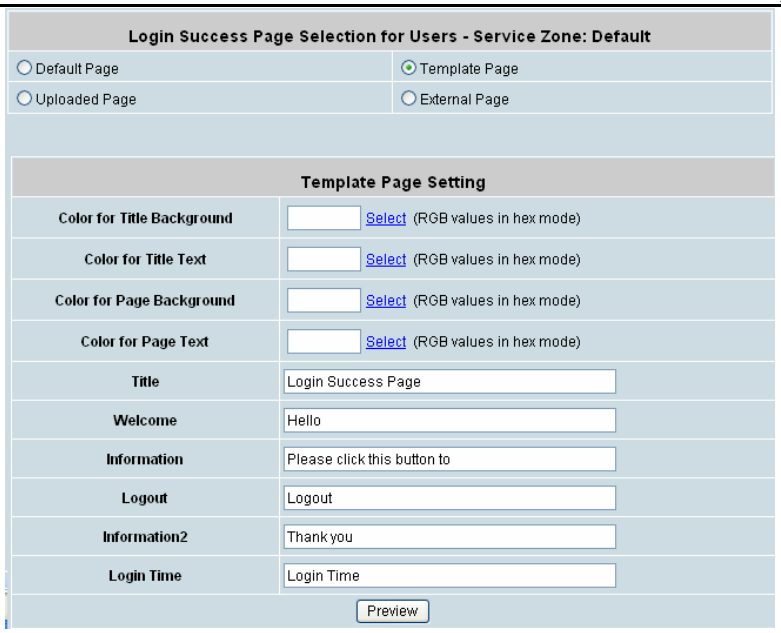
- *Login Success Page* → ***Default Page***

  Choose Default Page to use the default login success page.



- *Login Success Page* → ***Template Page***

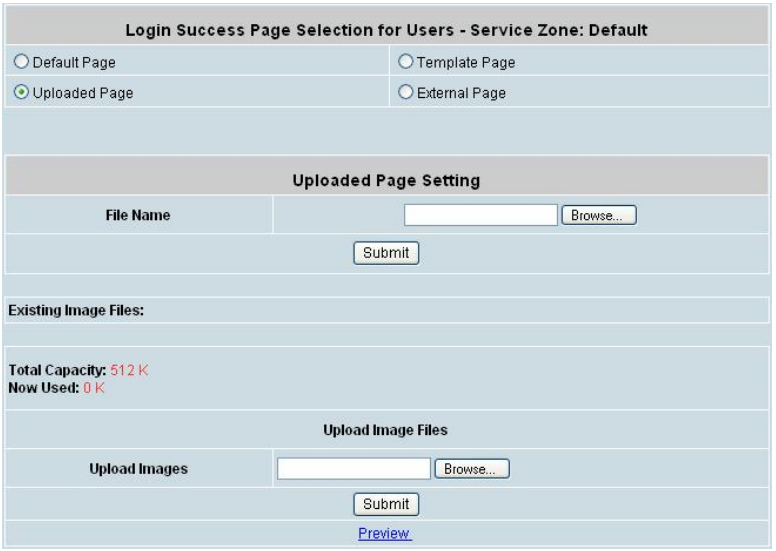
  Choose Template Page to make a customized login success page. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



- *Login Success Page→* ***Uploaded Page***

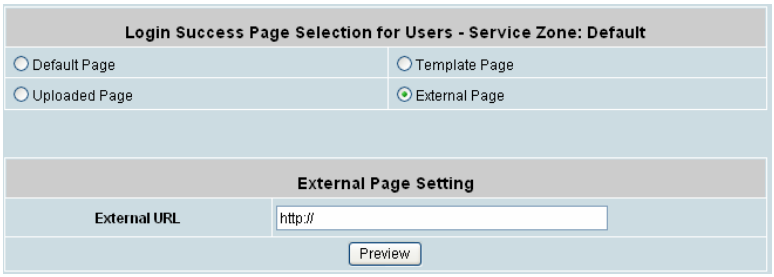
  Choose Uploaded Page to upload the login success page. Click the ***Browse*** button to select the file for the login success page upload. Next, click ***Submit*** to complete the upload process.

  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→* ***External Page***

  Choose the External Page selection to get the Login Success 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 Success Page can be previewed by clicking ***Preview*** button at the bottom of this page.

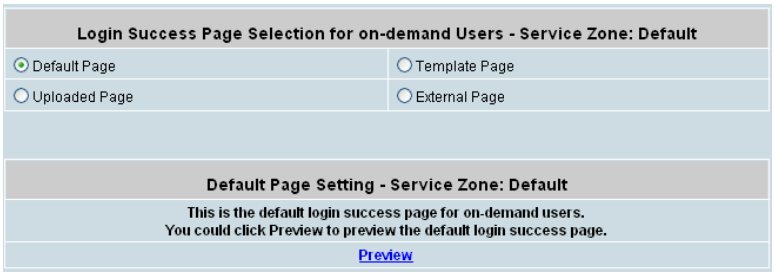


4) *Login Success Page for On-demand User*

The users can apply their own Login Success page for On-demand Users in the menu. As the process is similar to that of the Login Page, please refer to the instructions on Login Page for more details.

- *Login Success Page for On-demand User* → ***Default Page***

  Choose Default Page to use the default login success page for On-demand User.

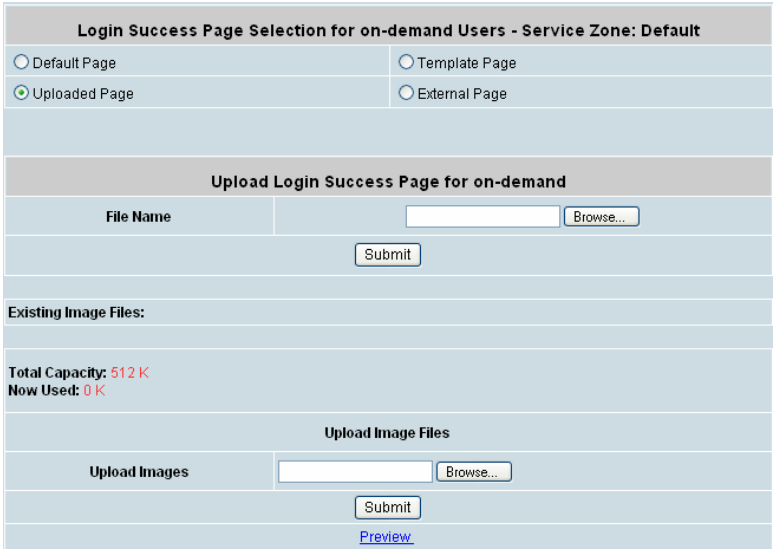


- *Login Success Page for On-demand User* → ***Template Page***

  Choose Template to make a customized login success for On-demand User. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result.

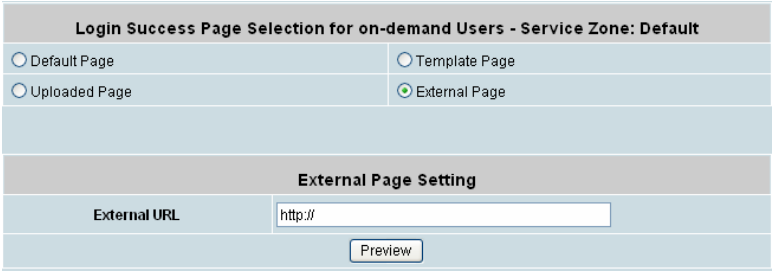
- *Login Success Page for On-demand User* → ***Uploaded Page***

Choose Uploaded Page and get the login success page for On-demand User by uploading. Click the ***Browse*** button to select the Login Success Page file for instant upload. Then click ***Submit*** to complete the upload process.



- *Login Success Page for On-demand User→* ***External Page***

  Choose the External Page selection to get the Login Success Page for On-demand User from the specific website. In the External Page Setting, enter the URL of the external Login Success Page and then click ***Apply***. After applying the setting, the new Login Success Page for On-demand User can be previewed by clicking ***Preview*** button at the bottom of this page.

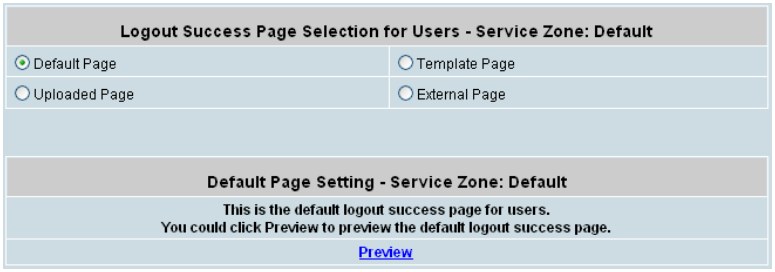


5) Logout Success Page

The administrator can apply their own Logout Success Page. As the process is similar to that of the Login Page, please refer to the instructions on Login Page for more details.

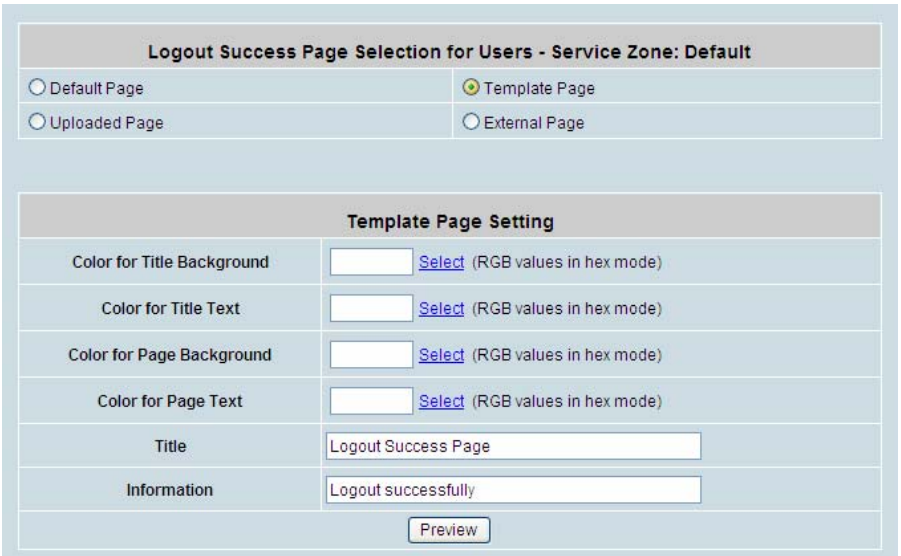
- *Logout Success Page →* ***Default Page***

  Choose Default Page to use the default logout success page.



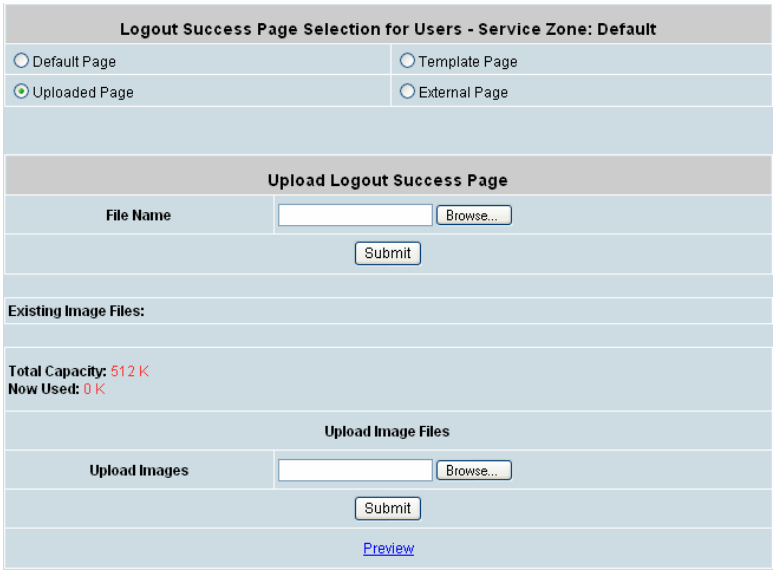
- *Logout Success Page →* ***Template Page***

  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.



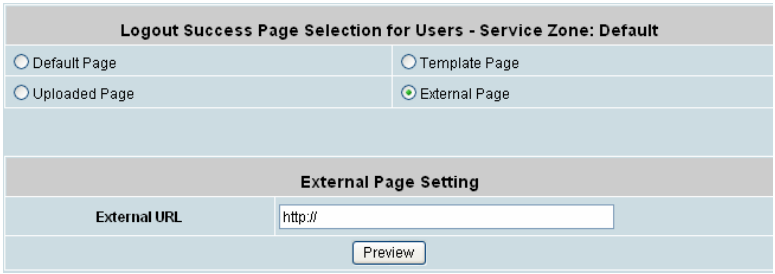
- *Logout Success Page* → ***Uploaded Page***

  Choose Uploaded Page to get the logout success page for upload. Click the ***Browse*** button to select the file for the logout success page upload. Next, 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.

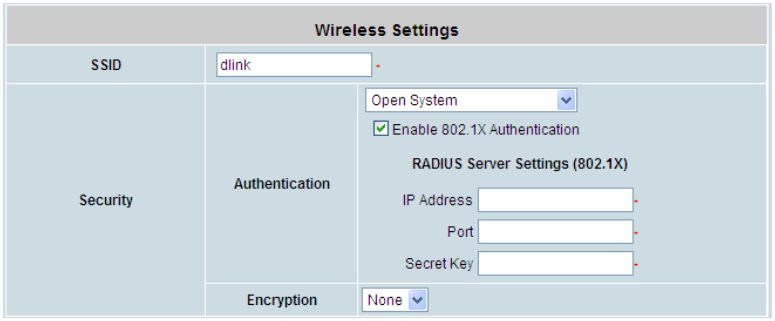


- *Logout Success Page* → ***External Page***

  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.



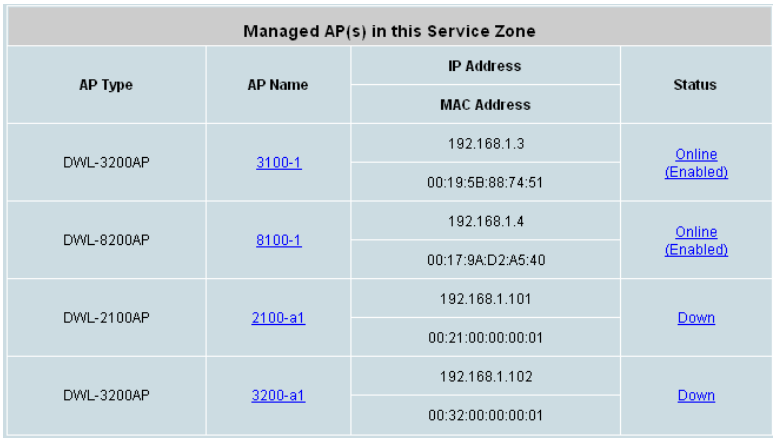
- ***Wireless Settings***



- **SSID:** Each service zone must setup its own SSID. Each SSID as unique name could not be repeated.
- **Security:** Each service zone can setup its own **Authentication** and **Encryption** support for AP security setting. Authentication support: **WPA**, **WAP2**, **WAP/WAP2 Mixed**, **Open System**, **Shared Key** and **Open System/Shared Key**; and encryption support: **WEP**.

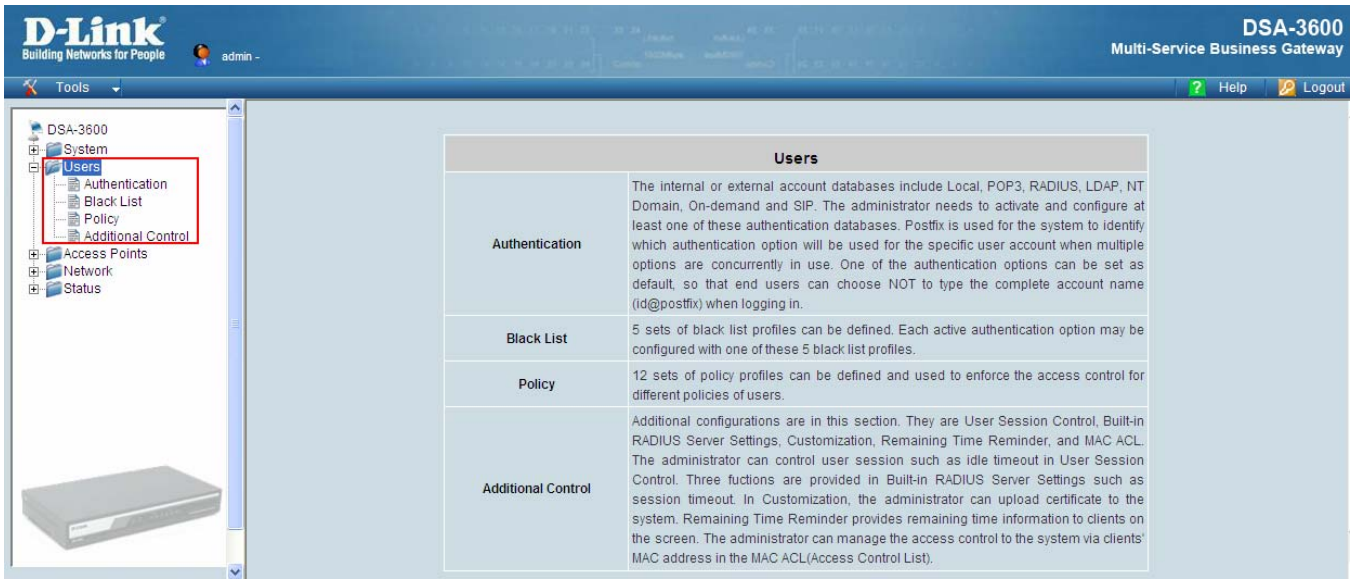
- ***Managed AP(s) in this Service Zone***

- **Managed AP in this Service Zone:** List all APs belonging to this service zone.



4.2 Users

This section provides information on the following functions: **Authentication, Black List, Policy** and **Additional Control**. It displays the information of the User, such as the number of Total Online users and the number of On-demand Users.



4.2.1 Authentication

This section is for administrators to pre-configure authentication options for the entire system's Service Zones. For a particular Service Zone, administrators can enable all the authentication options which will be used and also specify a default authentication option in the page of Service Zone Settings. Concurrently up to four options 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 options (On-demand User and SIP) that are selected by the system. For the Authentication Settings of each Service Zone, please see ***4.1.6 Service Zones***.

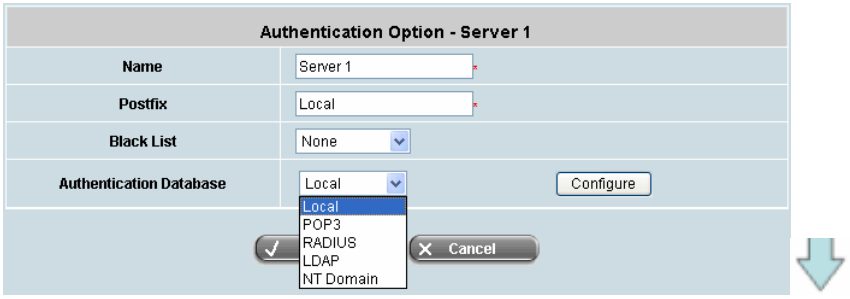
Authentication Settings		
Auth Option	Auth Database	Postfix
Server 1	LOCAL	local
Server 2	POP3	pop3
Server 3	RADIUS	radius
Server 4	LDAP	ldap
On-demand User	ONDEMAND	ondemand
SIP	SIP	N/A

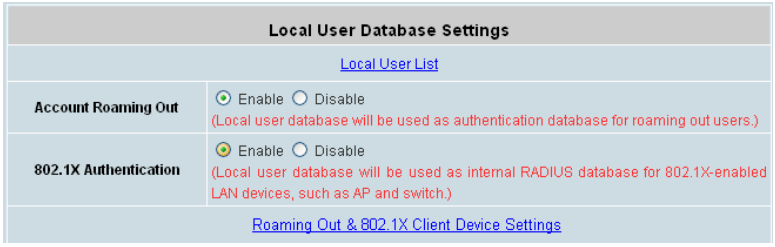
- **Authentication Option:** There are several authentication options supported by DSA-3600: Server 1 to Server 4, On-demand Users and SIP. Click the hyperlink of the respective Authentication Option to configure the authentication option.

  Authentication Database: There are different authentication databases supported in DSA-3600: **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.

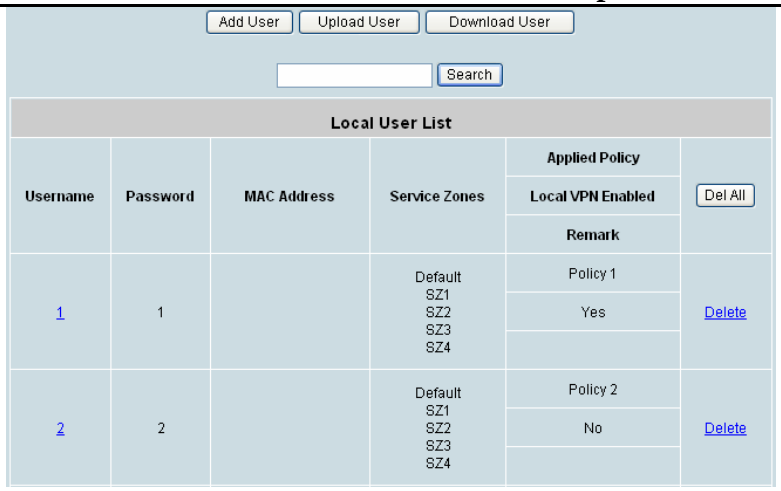
Note: *Concurrently only one server is allowed to be set as LOCAL or NTDOMAIN authentication database.*

4.2.1.1 Authentication Database – Local





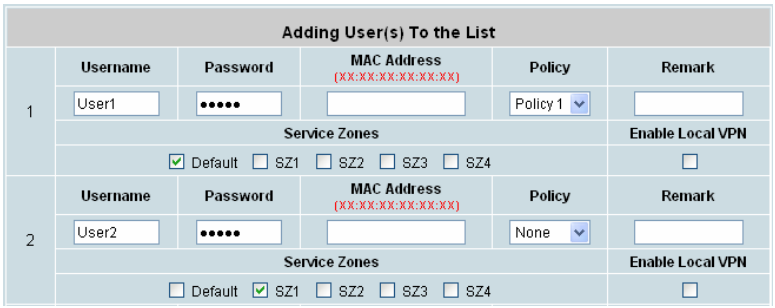
- **Name:** Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_), space and dot (.) only. The length of this field is up to 40 characters. This name is used for the administrator to identify the authentication options easily such as HQ-RADIUS.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



- ***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.

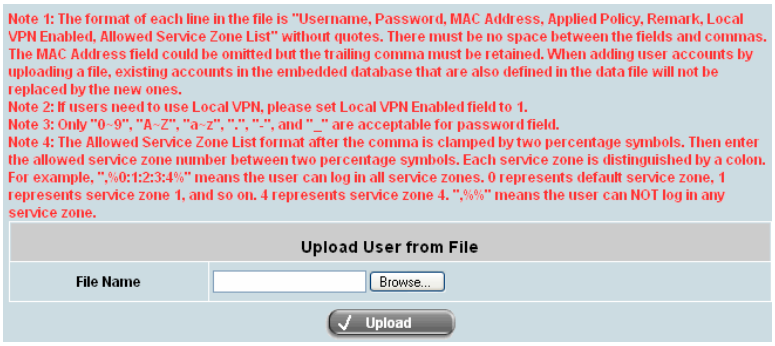
  For the Policy configuration, please check section on Policy Configuration.

  Click ***Apply*** to complete adding the user or users.

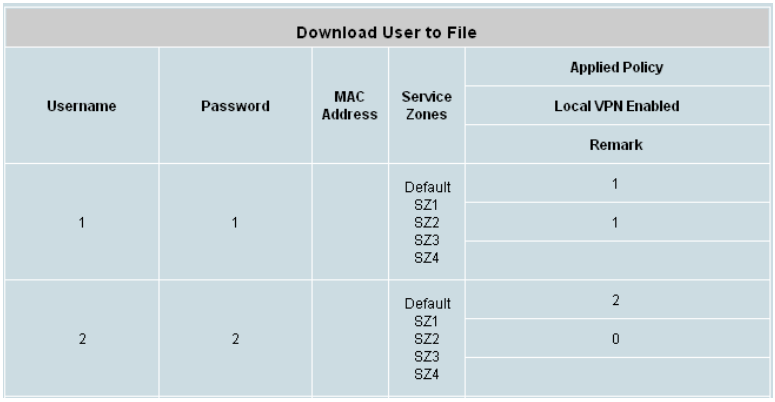


- ***Upload User*:** Click this to enter the **Upload User from File** interface. Click the ***Browse*** button to select the text file for uploading user account, then click ***Upload*** to execute the upload process.

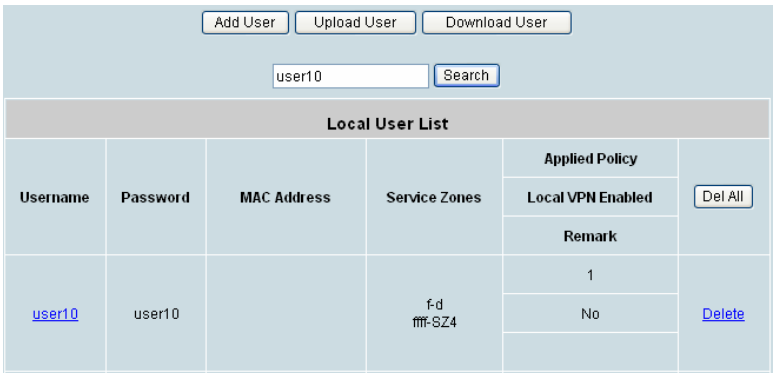
  The file for uploading should be a text file containing in each line the following information: ***Username, Password, MAC Address, Applied Policy, Remark, Local VPN enabled***. There must be no spaces between the fields and commas. The MAC field can be omitted, but the trailing comma must be retained. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by the new.



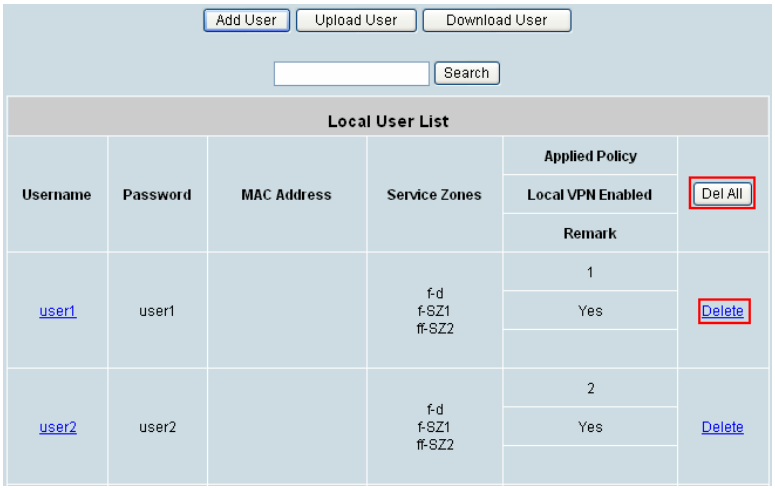
- ***Download User***: Use this function to create a .txt file with all built-in user account information and then save it on disk.



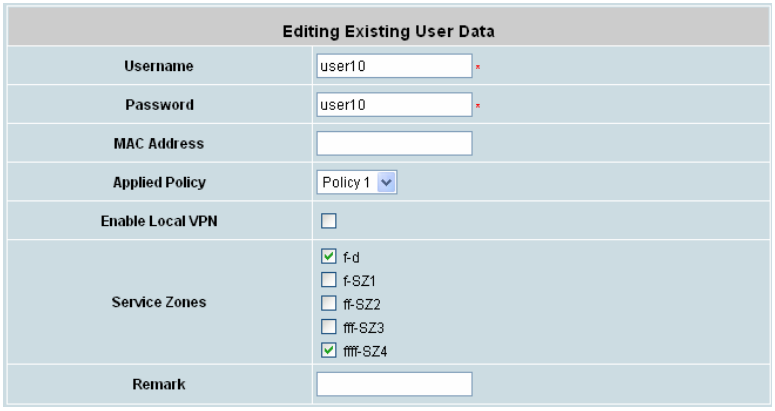
- ***Search***: Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.



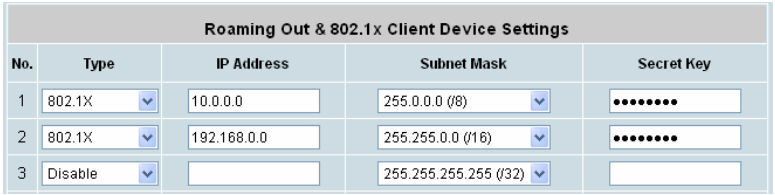
- ***Del All***: Click on this button to delete all the users at once and click on ***Delete*** to delete the user individually.



- **Edit User:** If editing the content of individual user account is needed, click the username of the desired user account to enter the **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.



- **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**.



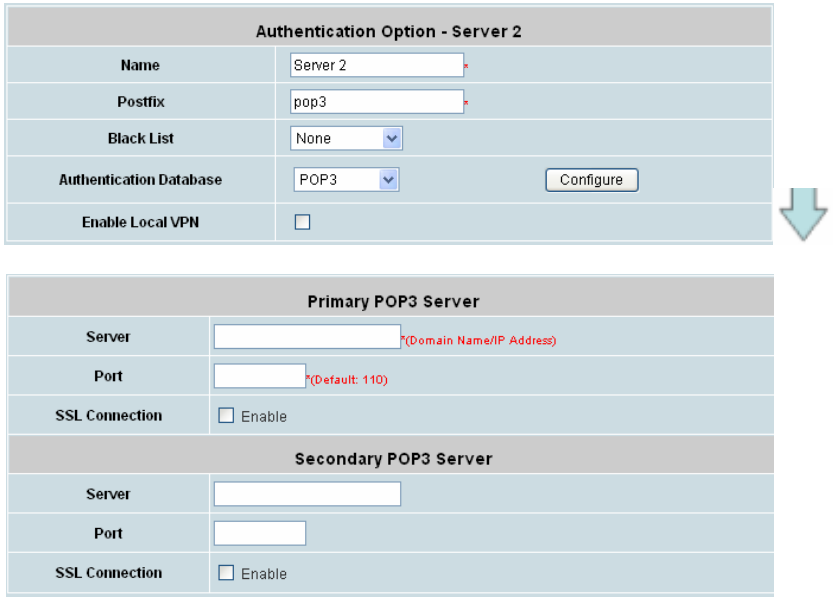
Click the hyperlink ***Roaming out & 802.1X Client Device Settings*** to enter the **Roaming out & 802.1X Client Device Settings** interface. Choose the desired type, **Disable**, **Roaming Out** or **802.1X**, and key in the 802.1x client's IP address and network mask and then click ***Apply*** to complete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

4.2.1.2 Authentication Database – 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.



- **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 **4.2.2 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

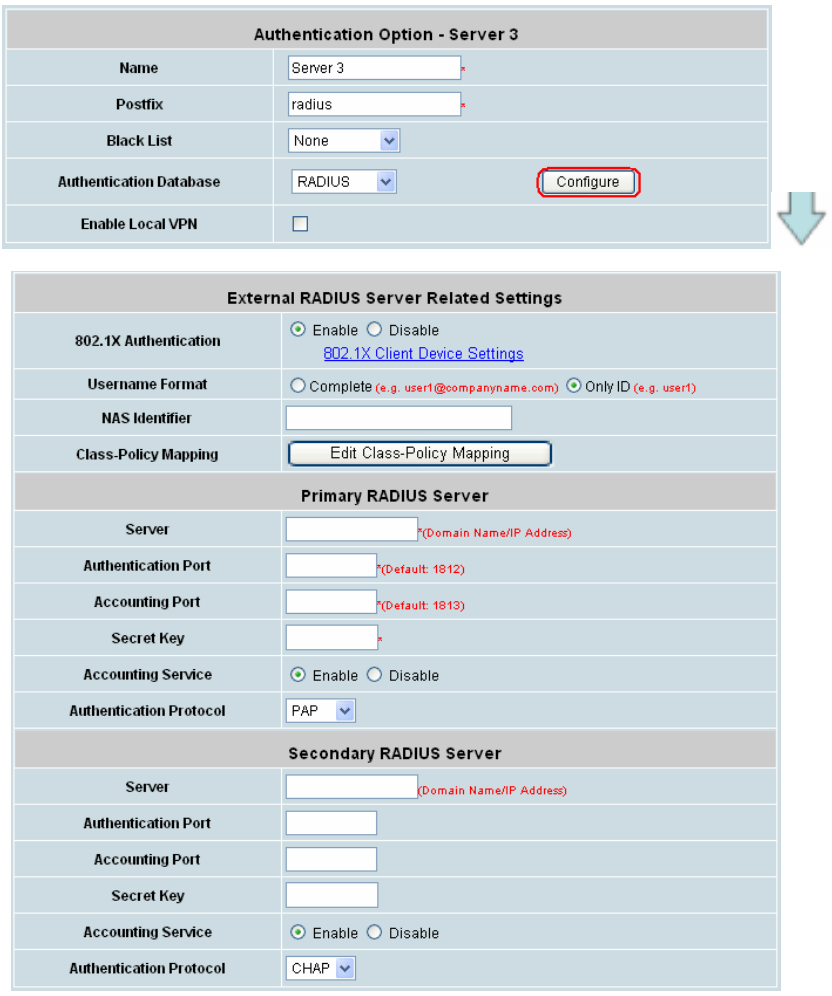
supports end-users' devices under Windows 2000 and Windows XP SP1, SP2.

- **Server:** The IP address of the external POP3 Server.
- **Port:** The authentication port of the external POP3 Server.
- **SSL Setting**: The system supports POP3. Check the check box of the SSL Connection to enable POP3.

4.2.1.3 Authentication Database – RADIUS

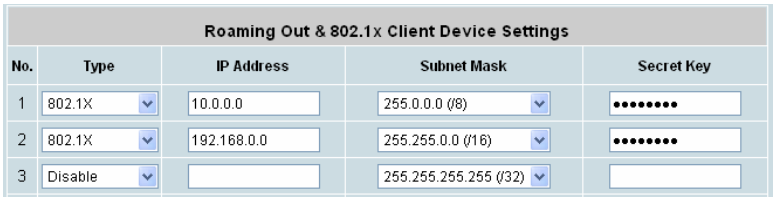
The system supports authentication by an external RADIUS authentication database. The system allows each RADIUS domain to have a pair of RADIUS servers, primary and secondary, for backing up each other. The system functions as a RADIUS authenticator for external RADIUS servers.

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.



- **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,

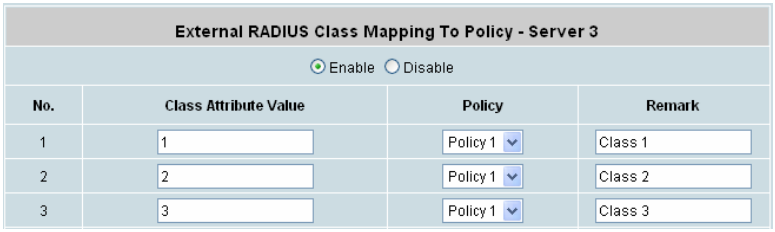
Subnet Mask, and shared Secret Key of the authorized devices. An example would be those downstream Access Points with 802.1x option turned on and shared Secret Key set accordingly.



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.



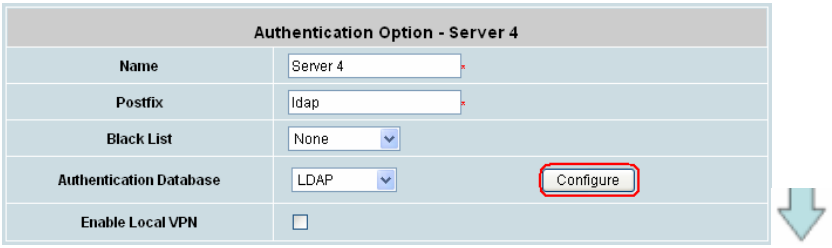
- **Server:** The IP address of the external RADIUS server.
- **Authentication Port:** Enter the authentication port of the RADIUS server.
- **Accounting Port:** The accounting port of the external RADIUS server.
- **Secret Key:** The Secret Key for RADIUS authentication.
- **Accounting Service:** The 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.

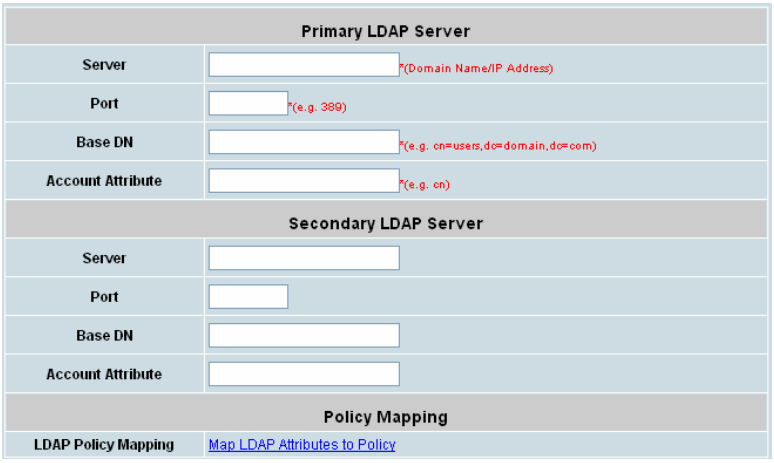
Notice: *If the RADIUS Server does not assign idle-timeout value, the DSA-3600 will use the local idle-timeout.*

4.2.1.4 Authentication Database – 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.

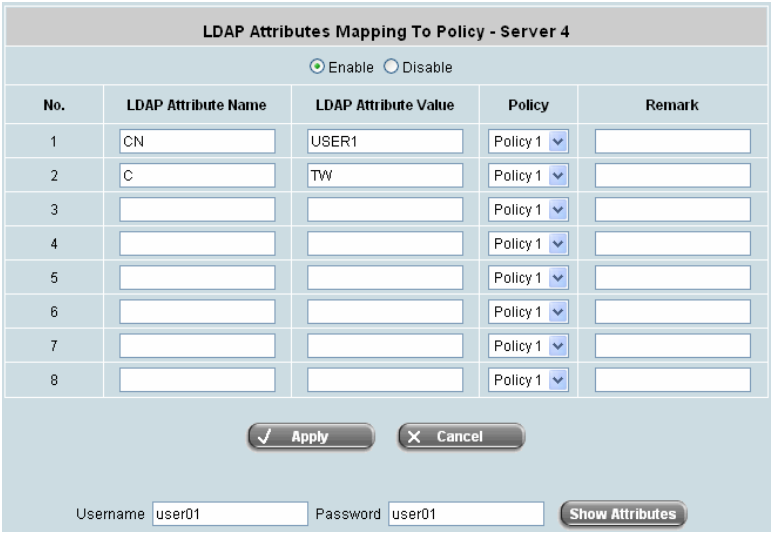
Click the hyperlink ***Configure*** for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). Information is required for fields with red asterisks. These settings will be effective immediately after clicking the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





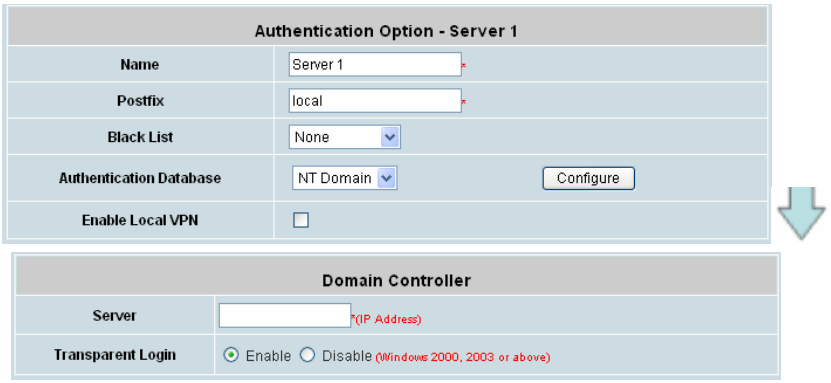
- **Server:** The IP address of the external LDAP Server.
- **Port:** The authentication port of the external LDAP Server.
- **Base DN:** The Distinguished Name for the navigation path of LDAP account.
- **Account Attribute**: The attribute of LDAP accounts.
- **LDAP Policy Mapping**: This function is 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



4.2.1.5 Authentication Database – NT Domain

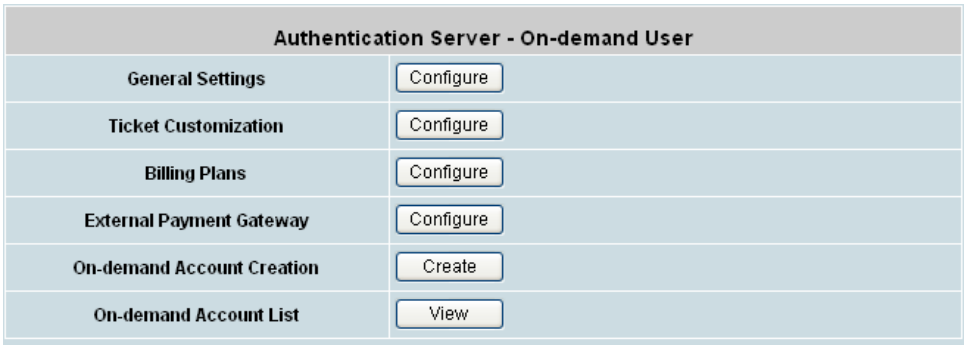
The system supports authentication by an external NT Domain authentication database.



- **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.

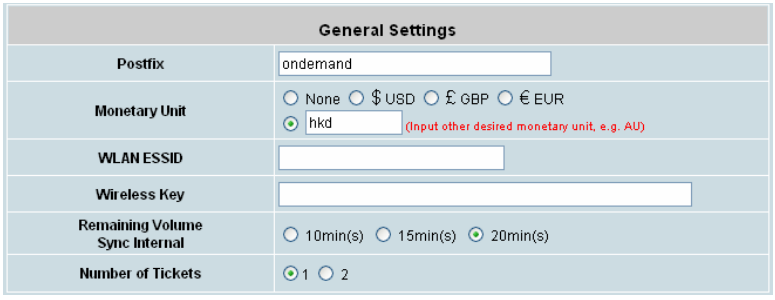
4.2.1.6 Authentication Database – ONDEMAND

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.



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.

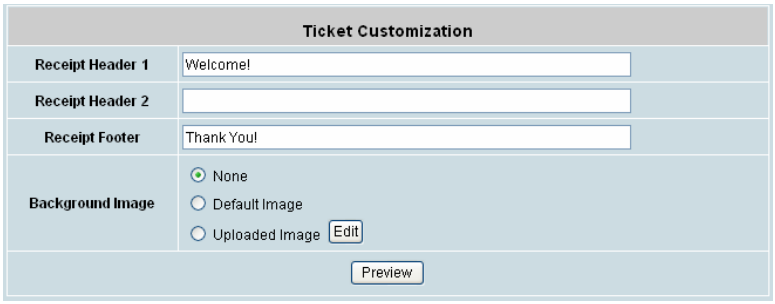


- **Postfix:** Postfix is used to inform the system which type of authentication database to be used for authentication when multiple databases are concurrently in use. Enter the postfix used for on-demand users.
- **Monetary Unit:** Select the desired monetary unit or specified the unit by yourself.
- **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 is connected to the serial port.

2) Ticket Customization

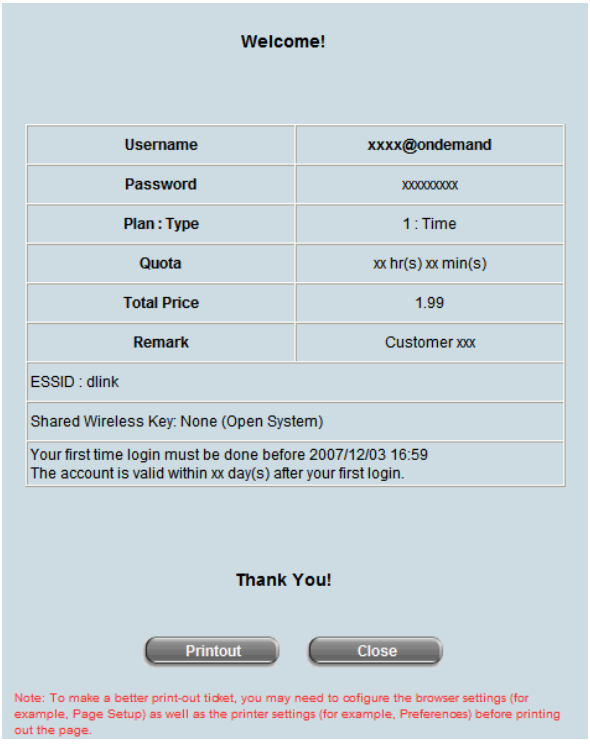
On-demand account ticket can be customized here and previewed on the screen.



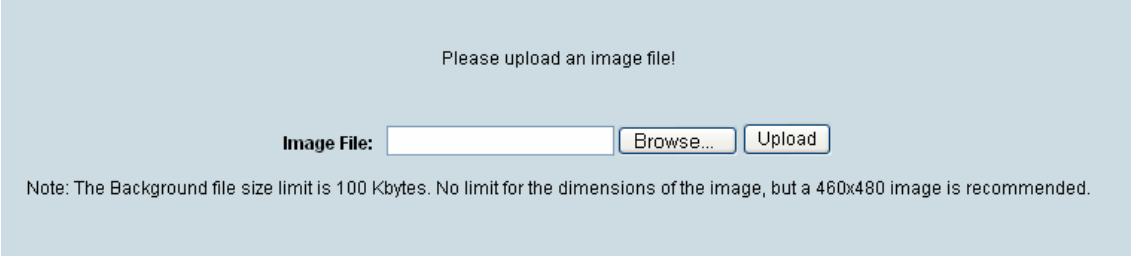
- **Receipt Header 1/2:** The entered content will be printed on the header area. These headers are optional.
- **Receipt Footer:** The entered content will be printed on the footer area. This footer is optional.
- **Background Image:** Set the background image of the ticket here.

  None: No picture.

  Default Image: below show the default picture.



Uploaded Image: click on ***edit*** button to upload the picture in the popup

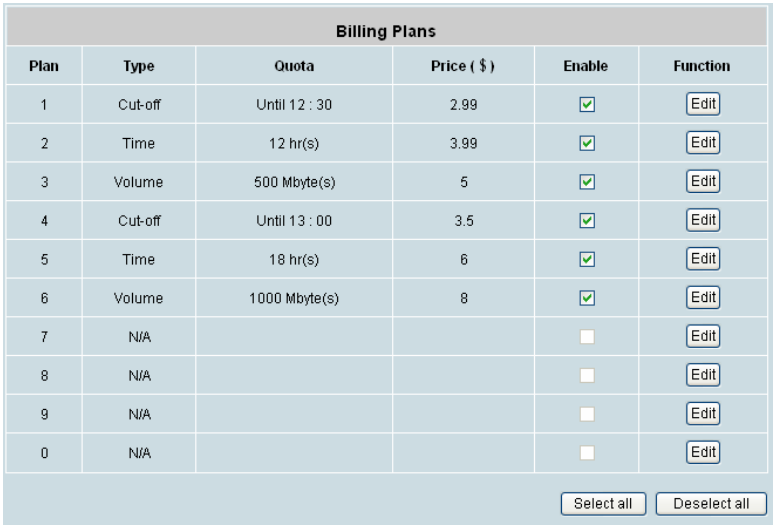


- **Preview:** Click ***Preview*** button to see the ticket with the items that are customized above.

***Please Note**: A dimension of 460x480 image is recommended.*

3) Billing Plans

With the billing plans configured and enabled, administrators are able to control and charge the network usage of On-demand users.

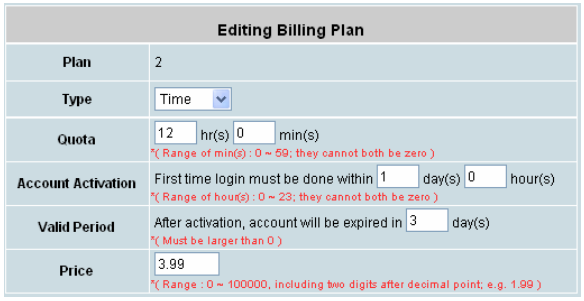


Billing Plans

Plan	Type	Quota	Price ($)	Enable	Function
1	Cut-off	Until 12 : 30	2.99	☑	Edit
2	Time	12 hr(s)	3.99	☑	Edit
3	Volume	500 Mbyte(s)	5	☑	Edit
4	Cut-off	Until 13 : 00	3.5	☑	Edit
5	Time	18 hr(s)	6	☑	Edit
6	Volume	1000 Mbyte(s)	8	☑	Edit
7	N/A			☐	Edit
8	N/A			☐	Edit
9	N/A			☐	Edit
0	N/A			☐	Edit

Select all | Deselect all

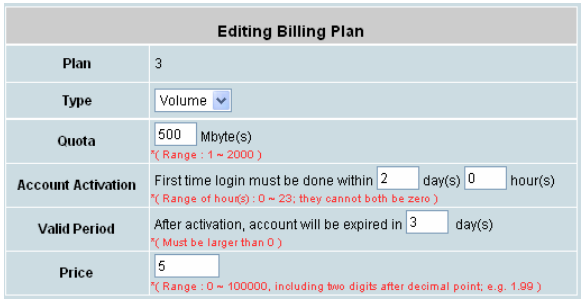
- **Plan:** The number of the specific plan.
- **Type:** This is the type (Time, Volume, or Cut-off) of the plan, based on which it defines how the account can be used.
- **Quota:** The limit on how On-demand users are allowed to access the network.
  - **Time:** Total period of time (xx hrs yy mins),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

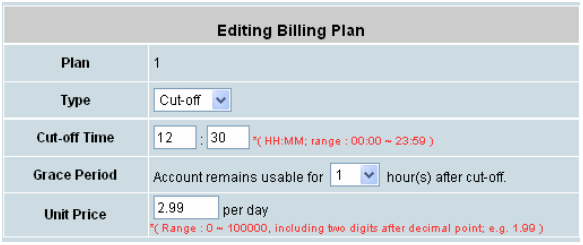


Editing Billing Plan

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)

  - **Cut-off:** The time of day at which the on-demand account is cut off (made expired) by the system on that day. Please note that the “Grace Period” is an additional, short period of time after the account is cut off, during which a user is allowed to continue to use the on-demand account to access the Internet

without paying additional fee.



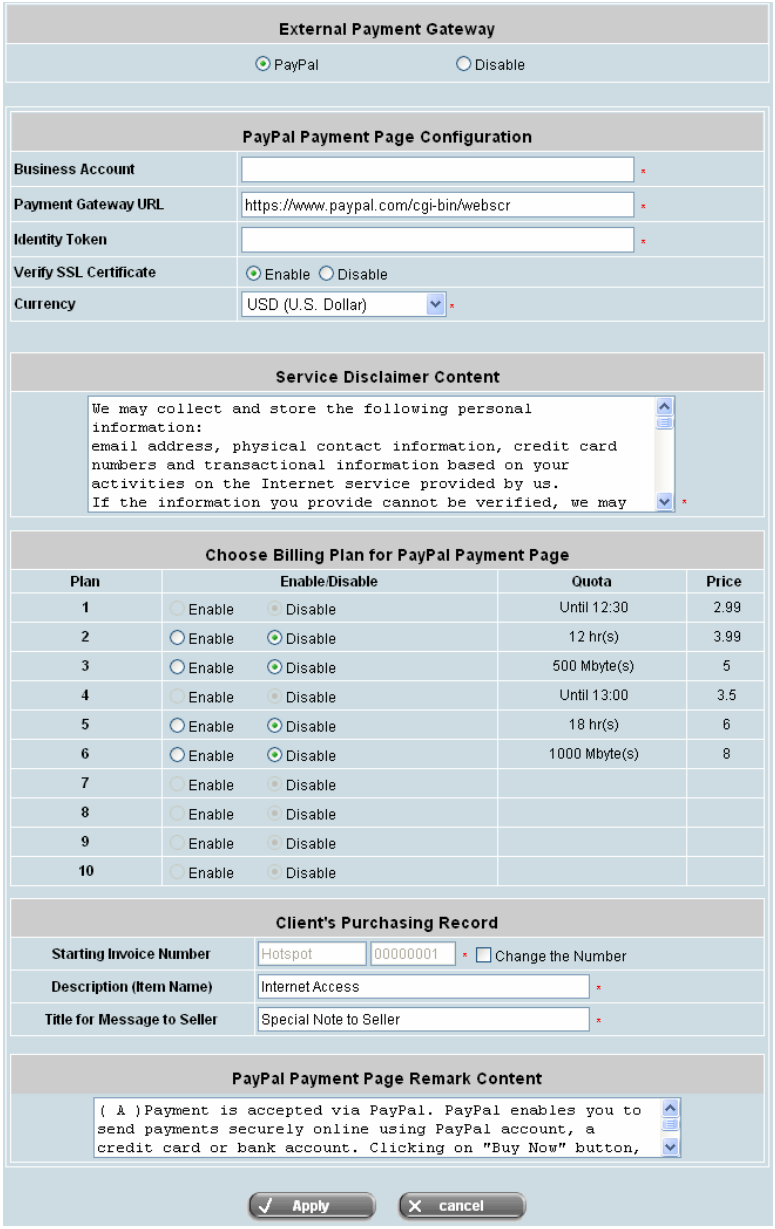
- **Price:** The unit price of each plan.
- **Enable:** Click the check box to activate the plan.
- **Function:** Click the **Edit** button to add or edit the specific billing plan.

4) External Payment Gateway

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

Before setting up “PayPal”, it is required that the merchant owners have a valid PayPal “Business Account”. Please see ***Appendix K. Accepting Payments via PayPal,***

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



- **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**

  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**

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).

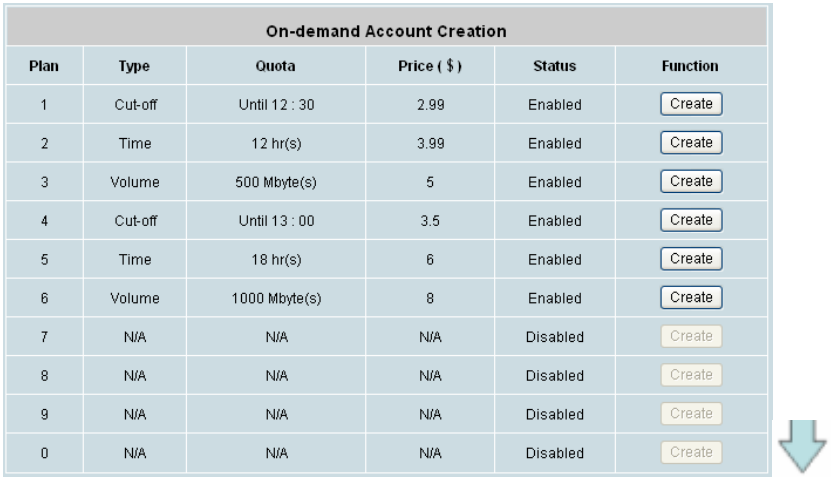
Title for Message to Seller: Administrators can edit the header "**title**" of the message note, used in the PayPal payment page.

➢ **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

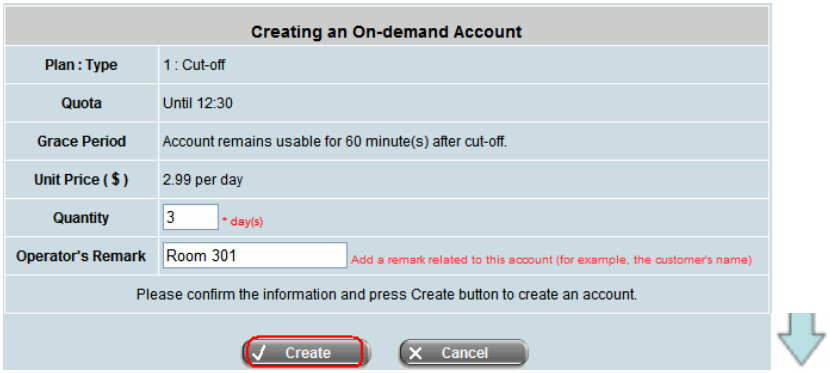
After one or more billing plans are configured and enabled in the *Billing Plans* page, administrators (including manager and operator accounts) are able to create On-demand user accounts in this page.

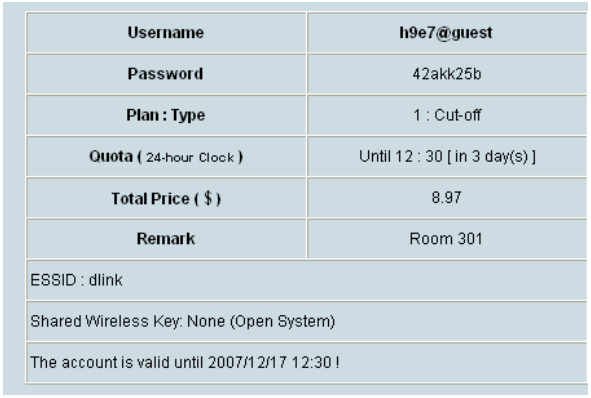


On-demand Account Creation

Plan	Type	Quota	Price ($)	Status	Function
1	Cut-off	Until 12 : 30	2.99	Enabled	Create
2	Time	12 hr(s)	3.99	Enabled	Create
3	Volume	500 Mbyte(s)	5	Enabled	Create
4	Cut-off	Until 13 : 00	3.5	Enabled	Create
5	Time	18 hr(s)	6	Enabled	Create
6	Volume	1000 Mbyte(s)	8	Enabled	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 the specific plan.
- **Type:** This is the type (Time, Volume, or Cut-off) 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.
- **Price:** The unit price of each plan.
- **Status:** Show the status in enabled or disabled.
- **Function:** To create an On-demand user account, press the ***Create*** button for the desired plan and a pop-up window will appear for operator's confirmation and additional input. Also, operators can click ***Printout*** button to print out the ticket as a copy of receipt to customers.

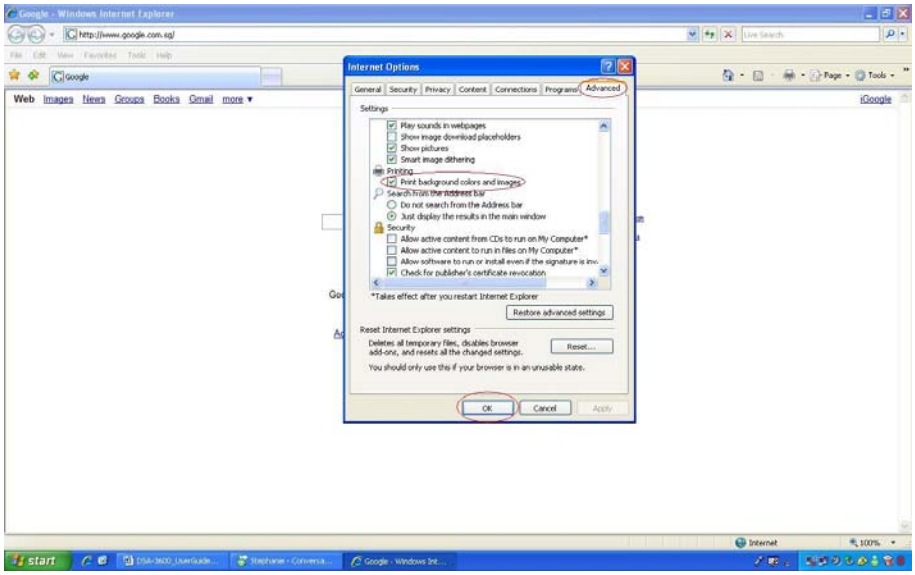




Note: In order to printout the ticket with the background picture, the web browser should configure as show below:

- **First**: Open the internet Explorer and select "**Tools**" for the drop down menu then click on "**Internet Options**"

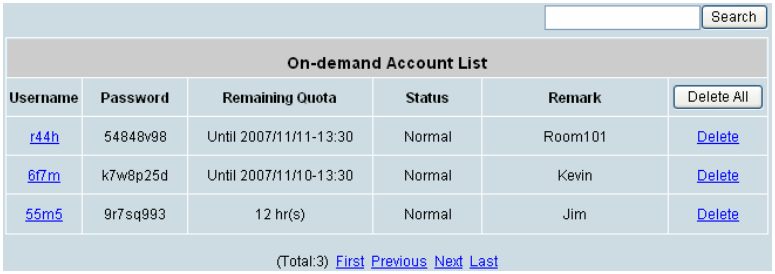
- **Second:** Inside the "**internet option**" menu click on the "**Advanced**" tap, scroll down and look out for the "**printing**" option and tick the box for the "**print background colors and images**" then click "**OK**".



- **Last:** Printout the ticket and it will show the ticket together with the background.

6) On-demand Account List

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



Search

On-demand Account List

Username	Password	Remaining Quota	Status	Remark	Delete All
r44h	54848v98	Until 2007/11/11-13:30	Normal	Room101	Delete
6f7m	k7w8p25d	Until 2007/11/10-13:30	Normal	Kevin	Delete
55m5	9r7sq993	12 hr(s)	Normal	Jim	Delete

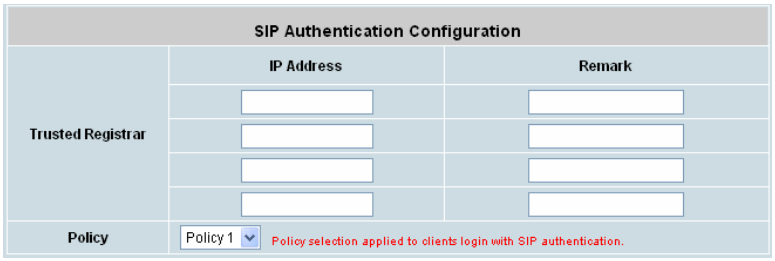
(Total:3) First Previous Next Last

- **Search:** A keyword can be used to search for the matching accounts that have been created (the contents of "Username" and "Remark" fields will be searched).
- **Username:** The login name of the account.
- **Password:** The login password of the account.
- **Remaining Quota:** The remaining time or volume for which the user can continue to access the network, or the cut-off time until which the user are allowed 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 when there is remaining quota to be used.
  - **Out of Quota:** the account has exceeded the quota limit
  - **Redeemed:** the quota of the account has been fully added to another account
- **Remark:** Additional information for operator's reference.
- **Delete All:** This will delete all the accounts at once.

- **Delete:** This will delete the account individually.

4.2.1.7 Authentication Database – SIP

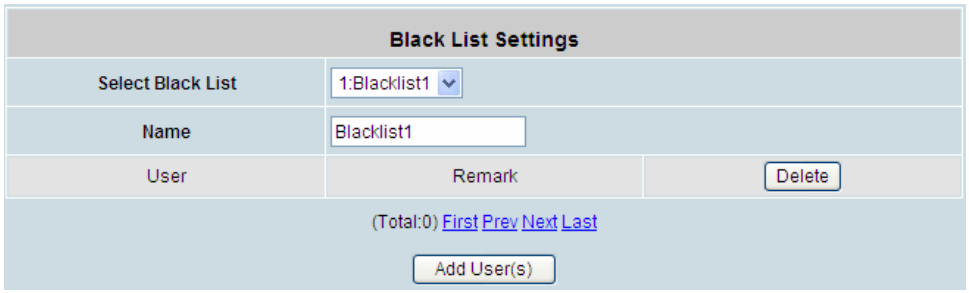
The system provides SIP proxy functionality, which allows SIP clients to pass through NAT. When enabled, all SIP traffic can pass through NAT via a fixed WAN interface.
Administrators are able to add up to four trusted SIP Registrars in order to authenticate SIP clients. Also, a policy can be chosen to govern the SIP traffic.



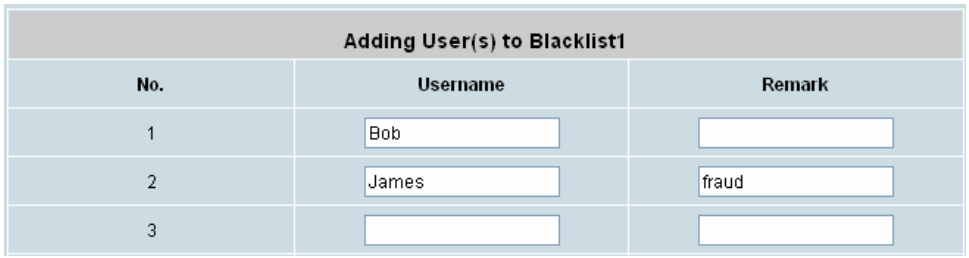
- **SIP:** SIP authentication supports 4 Trusted SIP Registrar.
- **IP Address:** The IP address of the Trusted SIP Registrar.
- **Remark:** The administrator can enter extra information in this field for remark.
- **Policy:** The Policy applied to the clients that login with SIP Authentication.

4.2.2 Black List

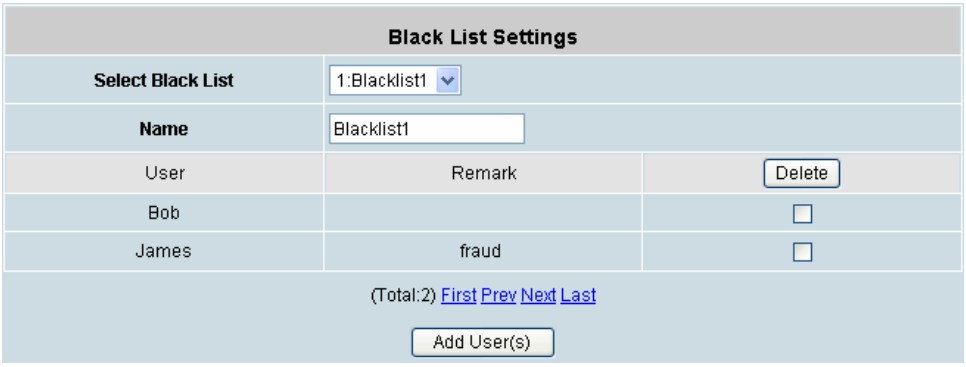
The administrator can add or delete users in the black list for user access control. There are 5 sets of black lists provided by the system. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one black list from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



- **Select Black List:** There are 5 lists supported by DSA-3600 for selections.
- **Name:** Set the name of the black list and it will show in the pull-down menu above.
- **Adding User(s):** After clicking ***Adding User(s),*** the **Adding Users to Blacklist** page will appear for adding users to the selected black list.



After entering the usernames in the **Username** field and the related information in the **Remark** field, click ***Apply*** to save the settings and the following page will appear.

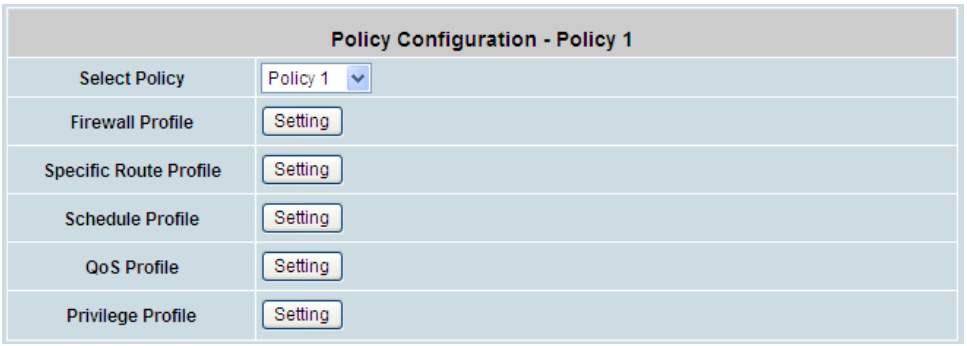


If the administrator wants to remove a user from the black list, just select the user's **"Delete"** check box and then click the ***Delete*** button to remove that user from the black list.

4.2.3 Policy

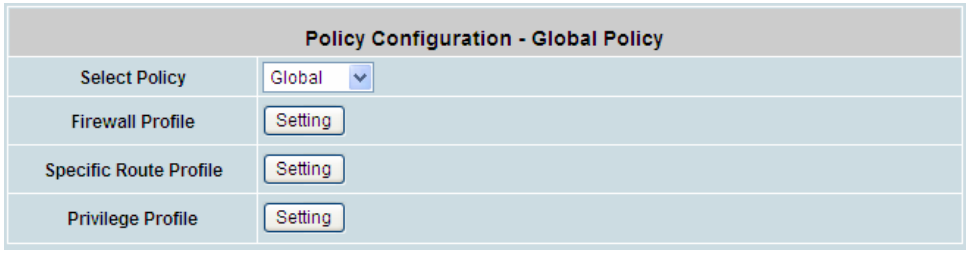
There are twelve sets of **Policy** provided by the system and one **Global policy**. Global is the system's universal policy including **Firewall Profile**, **Specific Routes Profile** and **Privilege Profile**. Each Policy consists of **Firewall Profile, Specific Route Profile, Schedule Profile, QoS Profile,** and **Privilege Profile.**

Policy1 to **Policy12** will be used and shared with the **Service Zone** default policy settings and Authentication Databases settings. Once a policy is configured, you may assign it to the default policy of a service zone. Two service zones may share the same policy. Policies can be selected in the Policy tab. The administrator can select one of the defined policies to have policy-based user management supported by the DSA-3600. All user clients' access to this service zone will be bound to this policy.



4.2.3.1 Global Policy

Global is the system's universal policy including **Firewall Rules**, **Specific Routes** and **Privilege** which will be applied to all users unless the user has been regulated and applied to another 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:** Global policy and each policy have a firewall service list and a set of firewall profile which is composed of firewall rules.
- **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.
- **Privilege Profile:** Include Maximum Concurrent Session for User, from 10 to Unlimited.

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

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

a. **Predefined and Custom Service Protocols:** There are predefined service protocols available for firewall rules editing. The administrator is able to add new custom service protocols by clicking ***Add***, and delete the added protocols with ***Select All*** and ***Delete*** operations.
This link leads to a Service Protocols List where the administrator can defined a list of service by protocols (TCP/UDP/ICMP/IP).

Global Policy - Service Protocols List

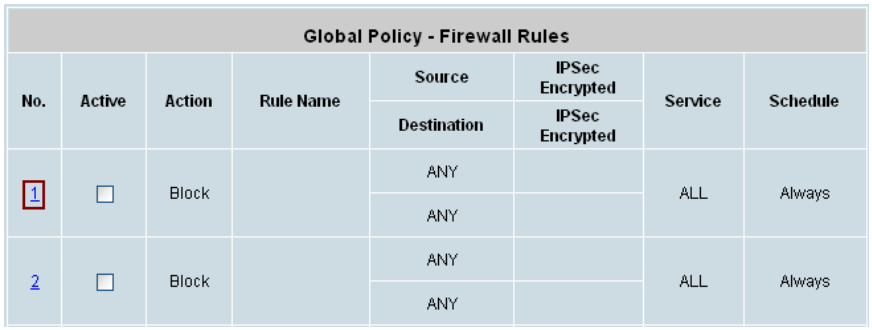
No.	Name	Description	Select All
1	ALL	ALL	☐
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	☐
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	☐
4	ALL ICMP	ICMP; Type: Any, Code: Any	☐
5	FTP	TCP/UDP; Destination Port: 20;21	☐
6	HTTP	TCP/UDP; Destination Port: 80	☐
7	HTTPS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

Add Delete

(Total: 27) First Prev Next Last

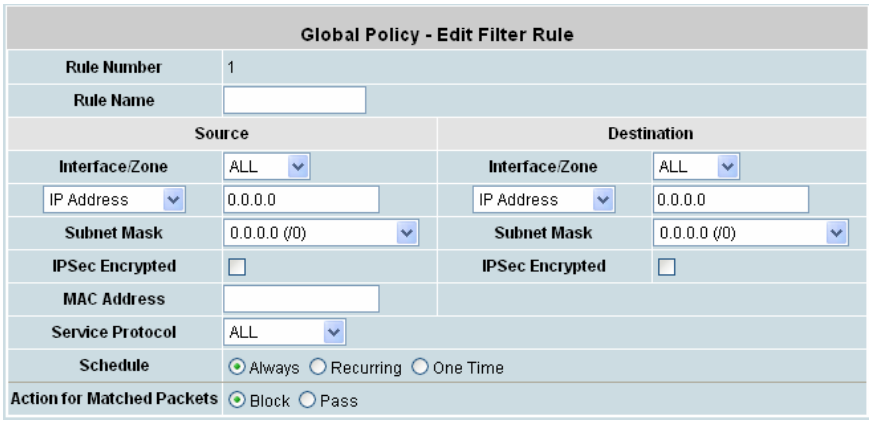
b. **Firewall Rules:** Click the number of ***Filter Rule No.*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list. Check **"Active"** box and click ***Apply*** to enable that rule.

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



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

Selecting the Filter Rule Number 1 as the example:

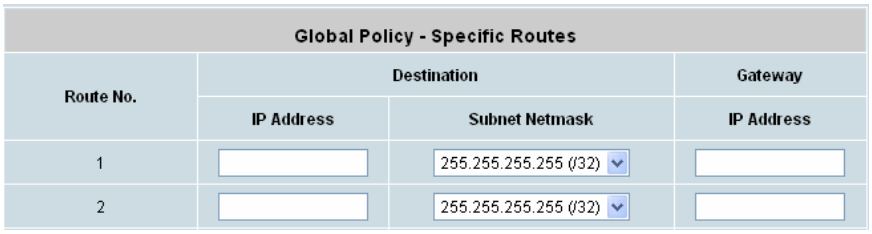


Global Policy - Edit Filter Rule			
Rule Number	1		
Rule Name			
Source		Destination	
Interface/Zone	ALL	Interface/Zone	ALL
IP Address	0.0.0.0	IP Address	0.0.0.0
Subnet Mask	0.0.0.0 (/0)	Subnet Mask	0.0.0.0 (/0)
IPSec Encrypted	☐	IPSec Encrypted	☐
MAC Address			
Service Protocol	ALL		
Schedule	◉ Always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

- **Rule Number:** This is the rule selected "1". Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on.
- **Rule Name:** The rule name can be changed here.
- **Source/Destination – Interface/Zone:** There are choices of **ALL, WAN1**, **WAN2**, **Default**, and the named **Service Zones** to be applied for the traffic interface.
- **Source/Destination – IP Address/Domain Name:** Enter the source and destination IP addresses. Domain Host filtering is supported but Domain name filtering is not.
- **Source/Destination – Subnet Mask:** Select the source and destination subnet masks.
- **Source- MAC Address:** The MAC Address of the source IP address. This is for specific MAC address filter.
- **Source/Destination – IPSec Encrypted:** Check the box for only filtering on the encrypted traffic.
- **Service Protocol:** There are defined protocols in the **service protocols list** to be selected.
- **Schedule:** When schedule is selected, clients assigned with this policy are applied the firewall rule only within the time checked. There are three options, **Always**, **Recurring** and **One Time. Recurring** is set with the hours within a week.

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

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



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

- **Route No.:** The number of route.
- **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.

C. **Privilege Profile:** Click the button of ***Setting*** for **Privilege Profile** to enter the **Privilege Configuration** for configuring the item of **Maximum Concurrent Session for User** from *Unlimited* to *10*.

Global Policy - Privilege Configuration	
Maxinum Concurrent Session for User	500

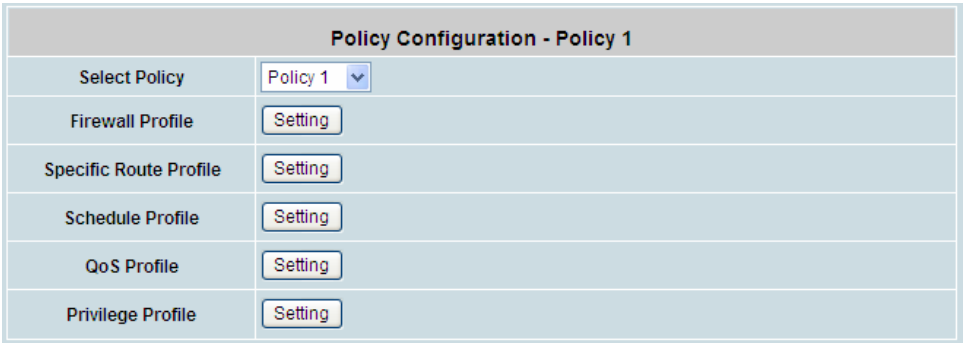
- **Maximum Concurrent Session for User:** Include Maximum Concurrent Session for User, from 10 to Unlimited. The concurrent sessions for each user, it can be restricted by administrator.

> ***Note:*** *For more information, please refer to* ***Appendix J. Session Limit and Session Log****.*

4.2.3.2 Policy 1 ~ Policy 12

Polices 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. A policy could be applied at zone level, at group level or at user level. User level policy overrides group level policy. Group level policy overrides zone level policy. Zone level policy overrides the global policy.

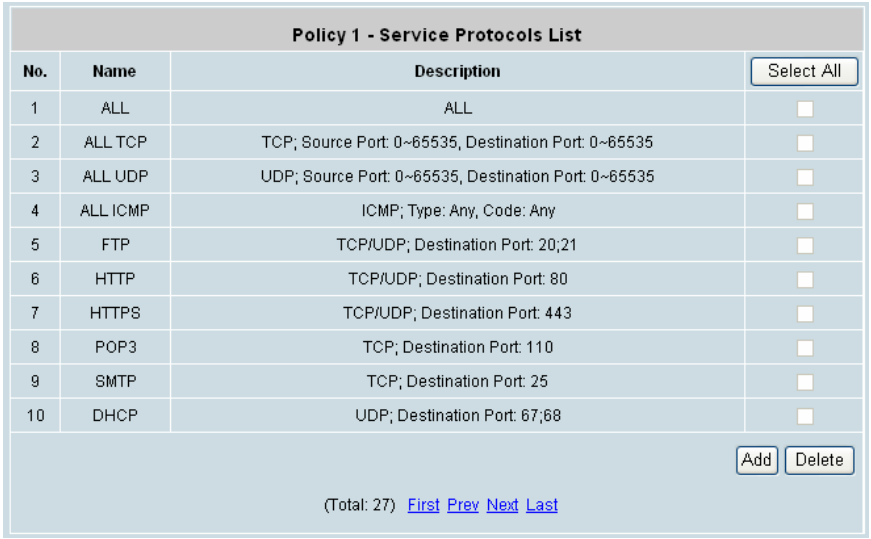
When the type of authentication database is “Local”, a policy is applied at per user basis. When the type of database is NTDOMAIN or ONDEMAND, a policy is applied to the whole user database. When type of database is RADIUS, a policy is mapped to a user group of a RADIUS class. The Class-Policy Mapping function will be available to let the administrator assign a policy for a RADIUS Class attribute. When the type of database is LDAP, a policy is applied to user group defined an attribute-value pair. The Attribute-Policy Mapping function will be available to let administrator assign a policy for a LDAP Attribute. When the type of database is SIP, the Policy selection function will be available to let the administrator assign a policy for all SIP users.



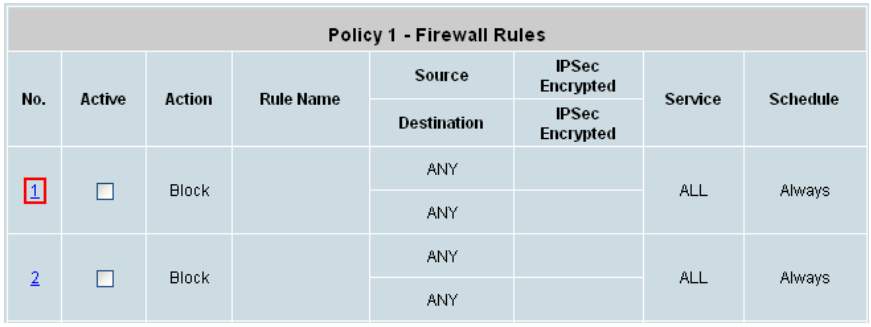
- **Select Policy:** Select a desired individual policy for configuration.
- **Firewall Profile:** Global policy and each policy have a firewall service list and a set of firewall profile which is composed of firewall rules.
- **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.
- **Schedule Profile:** The Schedule table in a 7X24 format is used to control the clients' login time. When Schedule is enabled, clients applied policies are only allowed to login the system at the time which is checked in the applied policy.
- **QoS Profile:** Set up the information of Traffic Configuration, including Traffic Class, Total Downlink, Individual Maximum Downlink, Individual Request Downlink, Total Uplink, Individual Maximum Uplink, and Individual Request Uplink.
- **Privilege Profile:** Include Maximum Concurrent Session for User, and Change Password Privilege.

A. **Firewall Profile:** Click the button of ***Setting*** for **Firewall Profile**, the Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules. Please refer to **Global Policy** section **A** for the same operations.

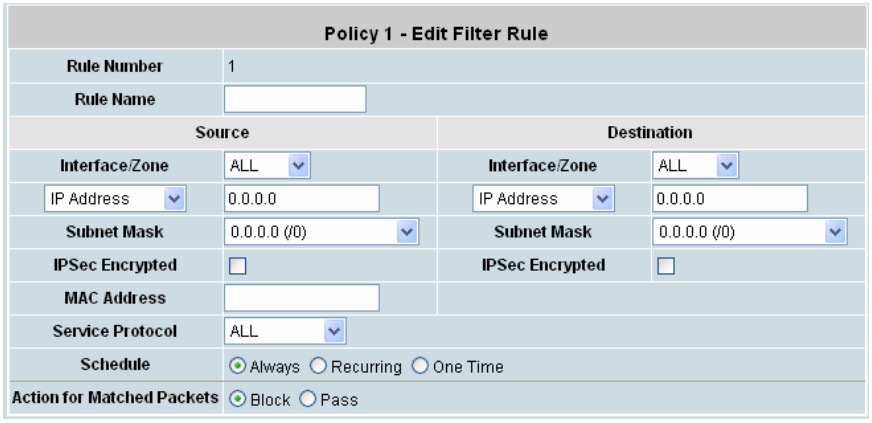
a. **Predefined and Custom Service Protocols:** There are predefined service protocols available for firewall rules editing. The administrator is able to add new custom service protocols by clicking ***Add***, and delete the added protocols with ***Select All*** and ***Delete*** operations.



b. **Firewall Routes:** Click the number of ***Filter Rule No.*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list. Check **"Active"** box and click ***Apply*** to enable that rule.



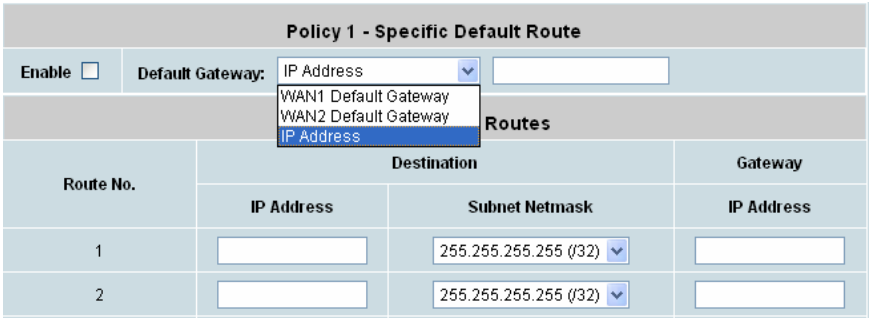
Selecting the Filter Rule Number 1 as the example:



- **Rule Number:** This is the rule selected "1". Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on.
- **Rule Name:** The rule name can be changed here.
- **Source/Destination – Interface/Zone:** There are choices of **ALL, WAN1**, **WAN2**, **Default**, and the named **Service Zones** to be applied for the traffic interface.
- **Source/Destination – IP Address/Domain Name:** Select the source and destination IP addresses.
- **Source/Destination – Subnet Mask:** Enter the source and destination subnet masks.
- **Source- MAC Address:** The MAC address of the source IP address. This is for specific MAC address filter.
- **Source/Destination – IPSec Encrypted:** Check the box for only filtering on the encrypted traffic.
- **Service Protocol:** There are defined protocols in the **service protocols list** to be selected.
- **Schedule:** When schedule is selected, clients assigned with this policy are applied the firewall rule only within the time checked. There are three options, **Always**, **Recurring** and **One Time. Recurring** is set with the hours within a week.
- **Action for Matched Packets:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.

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

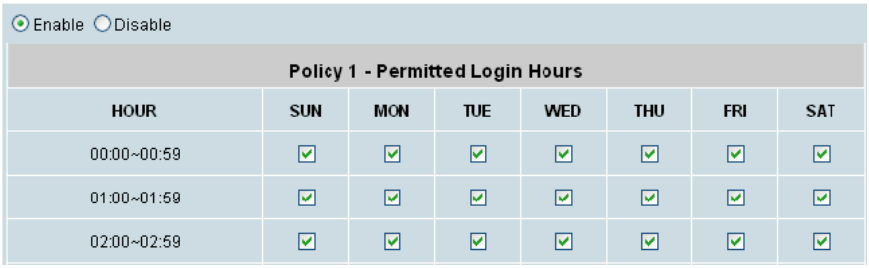
The **Default Gateway** of WAN1, WAN2, or a desired IP address can be defined in a policy. When **Default Gateway** is enabled, all clients applied this policy will access the Internet through this default gateway.



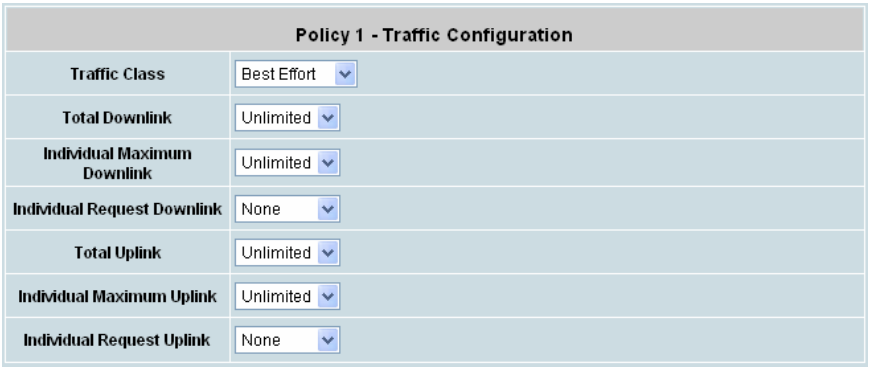
- **Enable:** Check this option to apply the **Default Gateway**.

- **Default Gateway:** Select the default gateway as WAN1, WAN2 or an assigned IP Address.
  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.

C. **Schedule Profile:** Click the button of ***Setting*** for **Schedule Profile** to enter the Schedule Profile list. Select "Enable" to show the list. This function is used to restrict the hours the users can log in. Please check the desired time slot and click ***Apply*** to save and enable the settings (on the screen below is shown only for 0 to 02:59, but the system can be configured based on 24 hours, 00:00 to 23:59). These settings will become effective immediately after clicking the Apply button. The Login Hours 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 policies.



D. **QoS Profile:** Click the button of ***Setting*** for **QoS Profile** to enter the Traffic Configuration.

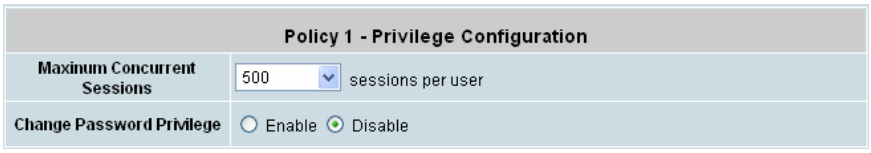


- **Traffic Class:** Each login user will be categorized into a policy. Each policy can choose its own traffic class. There are four traffic classes: Voice, Video, Best-Effort and Background. Voice and Video will be put into high priority queue. When select Best-Effort or Background, it also can configure the Downlink and Uplink Bandwidth.
- **Total Downlink:** The Total Downlink defines the maximum bandwidth allowed to share by clients within the same policy.
- **Individual Maximum Downlink:** The Individual Maximum Downlink defines the maximum bandwidth allowed for an individual client; the Individual Maximum Bandwidth can not exceed the value of Total Bandwidth.
- **Individual Request Downlink:** The Individual Request Downlink defines the guaranteed minimum bandwidth allowed for an individual client; the Individual Request Bandwidth can not exceed the value of Total Downlink and Individual Maximum Downlink.
- **Total Uplink:** The Total Uplink defines the maximum bandwidth allowed to share by clients

within the same policy.

- **Individual Maximum Uplink:** The Individual Maximum Uplink defines the maximum bandwidth allowed for an individual client; the Individual Maximum Uplink can not exceed the value of Total Uplink.
- **Individual Request Uplink:** The Individual Request Uplink Bandwidth 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.

E. **Privilege Profile:** Click the button of ***Setting*** for **Privilege Profile** to enter the Privilege Configuration including Maximum Concurrent Session, and Change Password Privilege.



- **Maximum Concurrent Sessions:** The maximum number of concurrent sessions which is allowed to be established by each user. Use the drop-down list to select the maximum number of concurrent sessions which is allowed to be established by each user.
  A session limit can be specified in each policy for service zones for authenticated users.

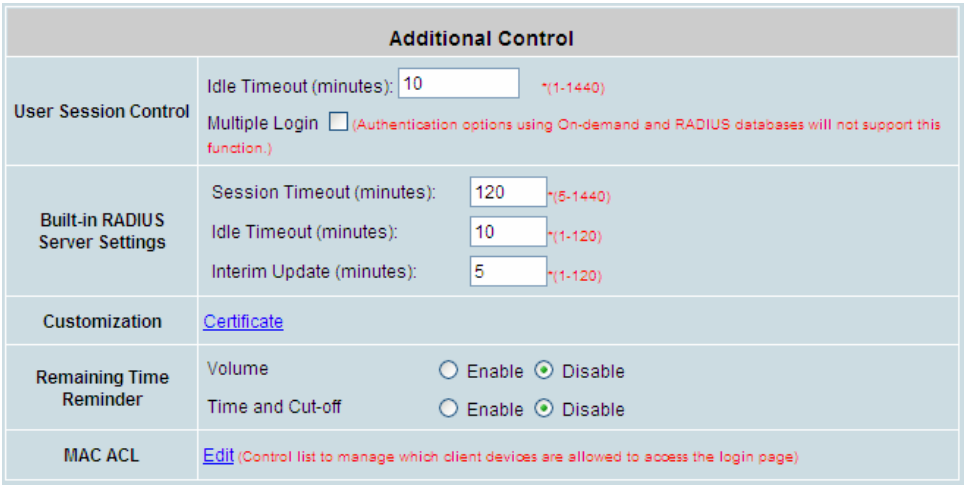
Note: *For more information, please refer to* ***Appendix J. Session Limit and Session Log****.*

- **Change Password Privilege:** When Change Password Privilege is enabled, the authenticated Local users are allowed to change password via the Login Success Page.

.

4.2.4 Additional Control

In this section, additional settings are provided for the administrator to the following for user management.



- **User Session Control:** Functions under this section applies for all general users.

  Idle Timeout: Define the time that the system will log out users when users have been inactive for the time period set in this field. This setting will be applied to all users.

  Multiple Login: When Multiple Login is enabled, the same account can be logged in by different clients at the same time. This function is not valid for On-demand Users Account and RADIUS Account.

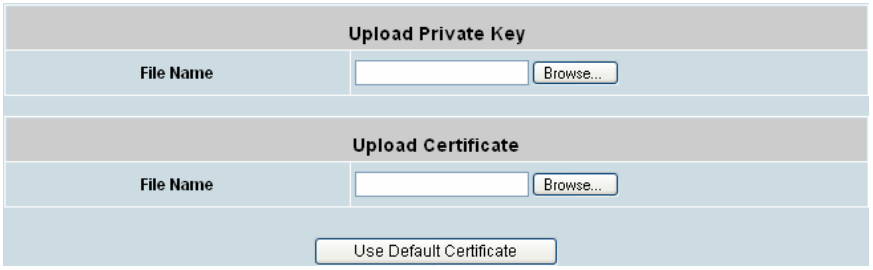
- **Built-in RADIUS Server Settings**

  Session Timeout: Define the time that how long users who are authenticated by the built-in RADIUS server can access the Internet since they logged in. The system will log out users after Session Timeout is reached.

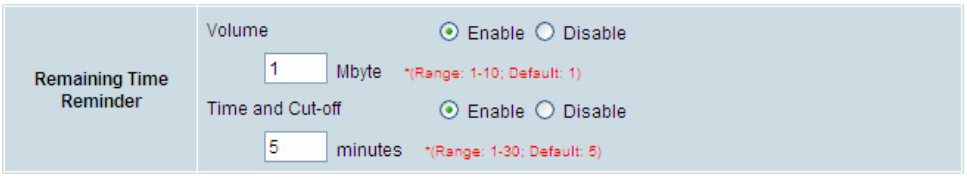
  Idle Timeout: Define the time that the system will log out users when users have been inactive for the time period set in this field. This setting will be applied to users who are authenticated by the built-in RADIUS server.

  Interim Update: The system supports to update records of users who are authenticated by the built-in RADIUS server constantly based on the time interval set in this field.

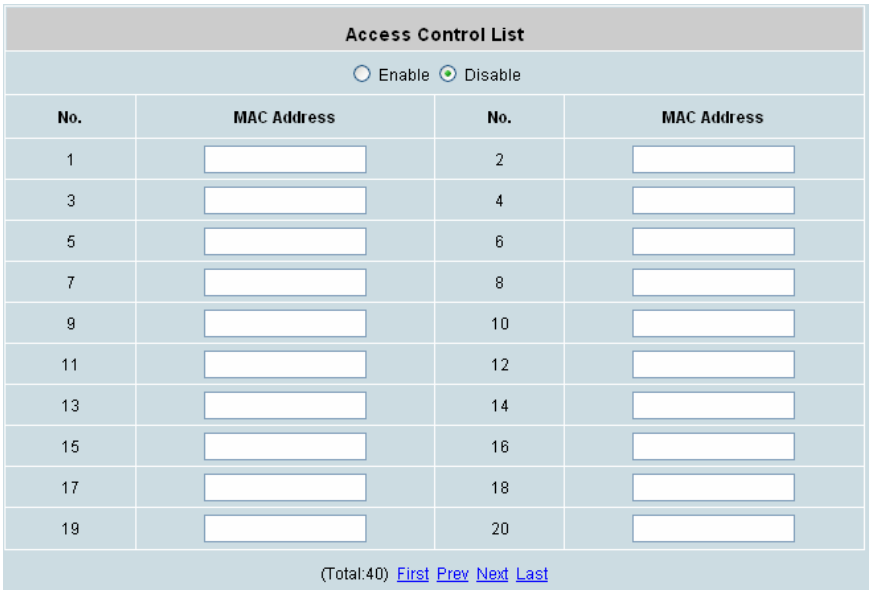
- **Customization:** The system supports upload customized certificate to system.



- **Remaining Time Reminder:** There is a Remaining Time Reminder supported by the system to remind users that their accounts are about to cut-off within the set time. When Remaining Time Reminder is enabled, there will be a message appearing on user's screen to remind them.



- **MAC ACL:** Enter the MAC address of the network device. When MAC ACL is enabled, only the clients with their MAC addresses listed in this list can log into the system.



4.3 Access Points

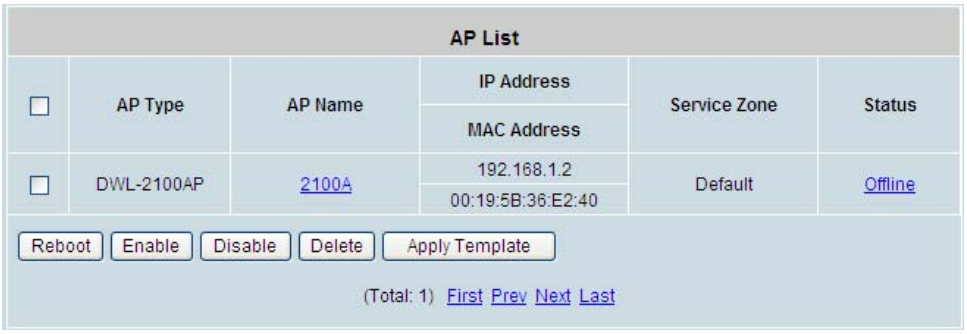
This section provides information on the following functions: **List, Discovery, Adding, Templates, Firmware** and **Upgrade**. It displays the information of the Access Points, such as the number of Total Managed AP, the number of Down AP and the number of Associated Clients.

Access Points	
List	A list to show the information of each managed AP, including Type, Name, IP Address, MAC Address, and online Status. Functions in this section also include the operations such as reboot, enable, disable, delete, apply a new template, and other configuration.
Discovery	This Discovery function is to manually or automatically detect the supported types of APs when connected to the LAN ports and automatically assign a unique IP address to each AP discovered.
Adding	The Adding function is used to manually set up an AP via filling in the required information for that AP. The system provides 3 templates that can be used to simplify the AP configuration.
Templates	3 AP setting templates can be defined. These templates can be edited, saved, and used in "Adding" and "Discovery" sections.
Firmware	The Firmware function provides the tools to see the AP firmware version and upload new AP firmware into the system. The system stores up to three versions of AP firmware.
Upgrade	The Upgrade function allows administrators to upgrade the AP firmware using the firmware files stored in the system. Multiple AP firmware upgrade can be done at the same time.

4.3.1 List

All of the supported managed APs (such as DWL-2100AP F/W version v2.2, v2.3) under management of the system will be shown in the list. The list is empty during first setup. The administrator can add supported APs from **Discovery** or the **Adding** tabs. After the APs are added, this list will show the current managed APs including AP type, AP name, IP Address, MAC Address, Service Zone and Status. The administrator can reboot, enable, disable, delete the managed APs, or apply template or apply service zone to them by checking the check box in front of each individual AP or selecting all the APs together by checking the top check box.

Please Note: *The supported managed AP may be varied for different DSA-3600 firmware version.*



After adding an AP:

Check any AP and click the button below to **Reboot, Enable, Disable, Delete**, and **Apply Template** to the checked AP.

- **AP Name**

  The AP name will be shown as hyperlink. Click the hyperlink of each managed AP can have for configurations about the specific AP. Click the hyperlink of the **AP Name** to have more configurations. There are four kinds of settings available: **General**, **LAN**, **Wireless LAN** and **Access Control**. Click the hyperlink of each individual setting to have further configurations.

- **Service Zone**

  After the AP is added into AP List, the managed AP can be assigned to one or multiple service zone.

- **Status:**

  Each AP's status will be shown in this column. Click the hyperlink of the shown status of each managed AP to see detailed status information about the specific AP, such as System Status, Service Zone Status, Wireless Status, Access Control Status and Associated Client Status. The status includes:

  (1) **Online:** The hyperlink of Online (Enabled) indicates that the AP is currently online and in service; Online (Disabled) indicates that the AP is currently online but not ready in service.

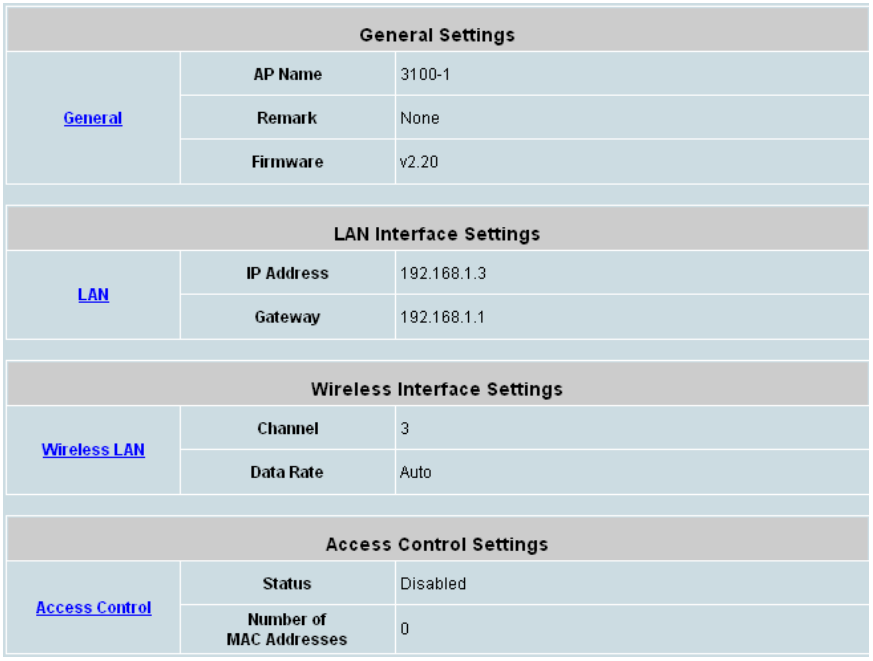
  (2) **Offline:** The AP is currently offline; for example: it is displayed as Offline when the power of the AP is off or the network connection between the AP and the DSA-3600 is down.

  (3) **Configuring:** It is displayed as Configuring when the newly discovered AP is being added to the list (and being configured) or new setting is being applied to the AP.

  (4) **Upgrading:** The AP is undergoing firmware upgrade.

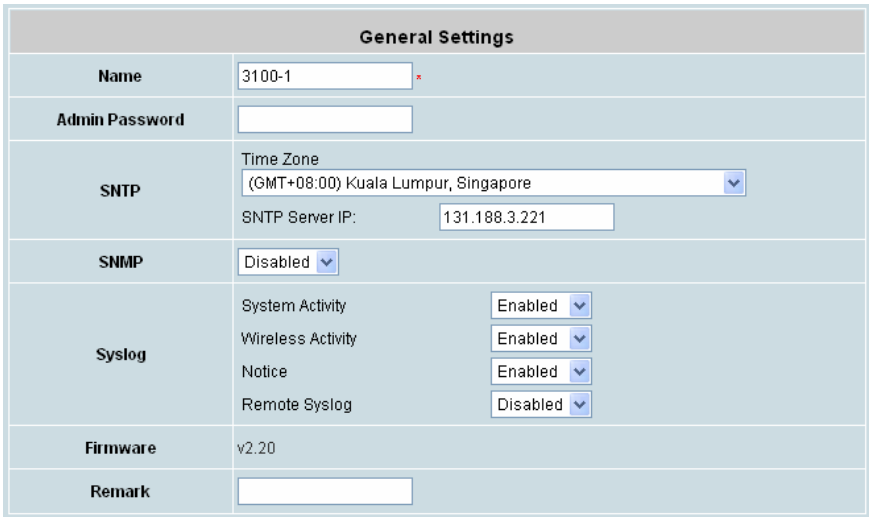
(5) **Lost/Unknown:** After DSA-3600's rebooting and before it tries to probe the AP and determine the exact status, the status will be displayed as Lost or Unknown temporarily.

- Enter the hyperlink of ***AP Name:***



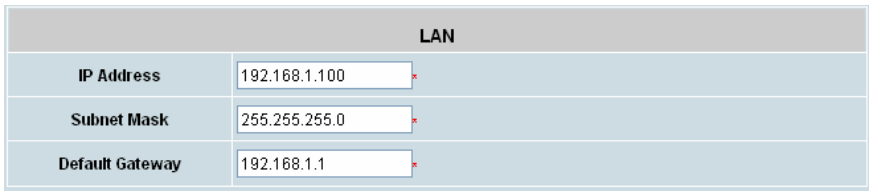
General Settings		
General	AP Name	3100-1
	Remark	None
	Firmware	v2.20
LAN Interface Settings		
LAN	IP Address	192.168.1.3
	Gateway	192.168.1.1
Wireless Interface Settings		
Wireless LAN	Channel	3
	Data Rate	Auto
Access Control Settings		
Access Control	Status	Disabled
	Number of MAC Addresses	0

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



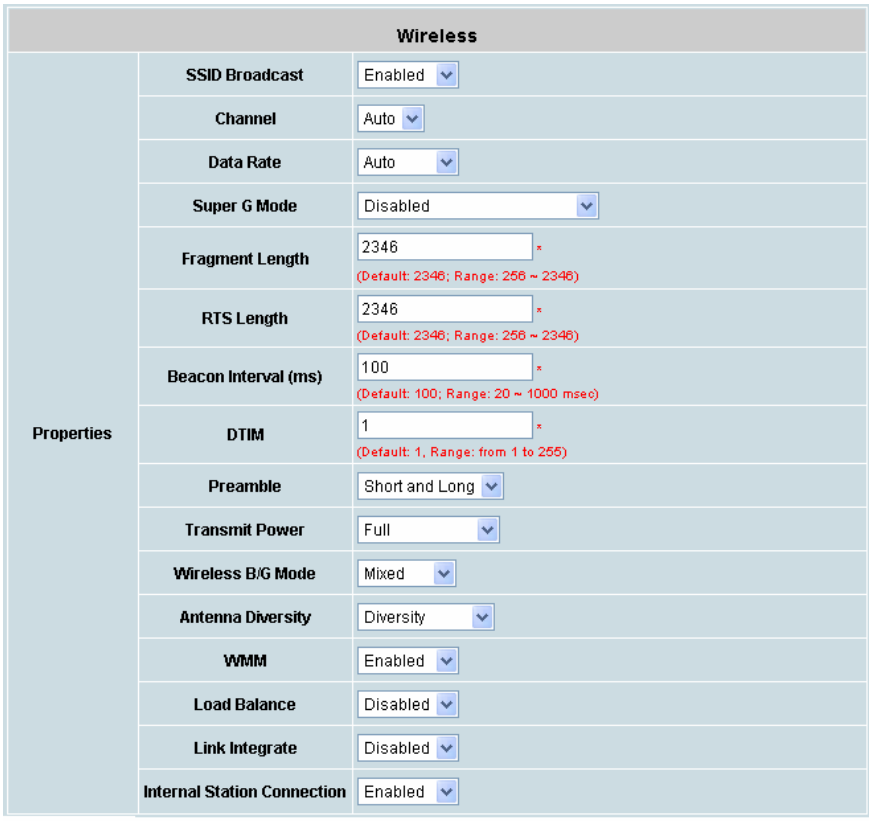
General Settings	
Name	3100-1 *
Admin Password	
SNTP	Time Zone: (GMT+08:00) Kuala Lumpur, Singapore SNTP Server IP: 131.188.3.221
SNMP	Disabled
Syslog	System Activity: Enabled Wireless Activity: Enabled Notice: Enabled Remote Syslog: Disabled
Firmware	v2.20
Remark	

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



LAN	
IP Address	192.168.1.100 *
Subnet Mask	255.255.255.0 *
Default Gateway	192.168.1.1 *

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



Properties:

- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from being seen on networked.
  - **SSID:** The SSID is the unique name shared among all devices in a wireless network. The SSID must be the same for all devices in the wireless network. It is case sensitive and has a maximum length of 32 bytes.
- **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.
- **Data Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **Fragment Length:** The fragmentation threshold determines whether packets will be fragmented. Enter a value between 256 and 2346.
- **RTS Length:** Enter a value between 256 and 2346. When wireless clients would like to send a packet which is larger than this value, it transmits an RTS and waits for reply.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network.

- **DTIM Interval:** Delivery Traffic Indication Message. Enter a value between 1 and 255.
- **Preamble:** Select Long Only or Short and Long. A short preamble is recommended for high-traffic networks.
- **Transmit Power:** Select either Full, Half(-3dB), Quarter(-6dB), Eighth (-9dB) or Minimum (minimum power).
- **Internal Station Connection:** Select either Enabled or Disabled. The connection allows clients to communicate with each other when enabled.

- **Status**

After clicking the hyperlink in the Status column, there are two areas of information shown: **AP Status Summary** and **AP Status Details.** AP Status Summary includes **AP Name, AP Type**, **LAN interface MAC address**, **Wireless Interface MAC address**, **Report Time**, **SSID**, **Number of Associated Clients** and **Remark**. AP Status Details include **System Status**, **LAN Status**, **Wireless LAN Status**, **Access Control Status** and **Associated Client Status**.

AP Status Summary	
AP Name	3100-1
AP Type	DWL-3200AP
LAN Interface MAC Address	00:19:5b:88:74:51
Wireless Interface MAC Address	00:19:5b:88:74:51
Report Time	2007-08-09 18:32:46
SSID	Felix-3600-0 (Service Zone: f-d) Felix-3600-1 (Service Zone: f-SZ1) Felix-3600-2 (Service Zone: ff-SZ2) Felix-3600-3 (Service Zone: fff-SZ3) Felix-3600-4 (Service Zone: ffff-SZ4)
Number of Associated Clients	0
Remark	

AP Status Details
System
LAN Interface
Wireless Interface
Access Control
Associated Clients

- **AP Name:** Mnemonic name of the specified AP.
- **AP Type:** This is the supported type of APs for centralized management.
- **LAN Interface MAC Address:** The LAN's Media Access Control address.
- **Wireless Interface MAC Address:** The wireless LAN's Media Access Control Address.
- **SSID:** The SSID is the unique name shared among all devices in a wireless network.
- **System Status:** The table shows the information about **AP Name, AP Status** and **Last Reporting Time.**

System	
AP Name	3100-1
AP Status	Online
Last Report Time	2007-08-09 18:34:47

- **Last Reporting Time:** The time when this summary is last updated.

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

LAN Interface	
IP Address	192.168.1.3
Subnet Mask	255.255.255.0
Gateway	192.168.1.1

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

Wireless Interface		
Service Zone Default	SSID	dlinkxxxxx
	Authentication	WPA/WPA2 Mixed
	Encryption	WPA-PSK
Service Zone SZ1	SSID	dlink-SZ1
	Authentication	Open System
	Encryption	None
Service Zone SZ2	SSID	dlink-SZ2
	Authentication	Shared Key
	Encryption	WEP
Beacon Interval (ms)		100
RTS Length		2346
Channel		Auto
Data Rate		Auto
Preamble		Short and Long

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

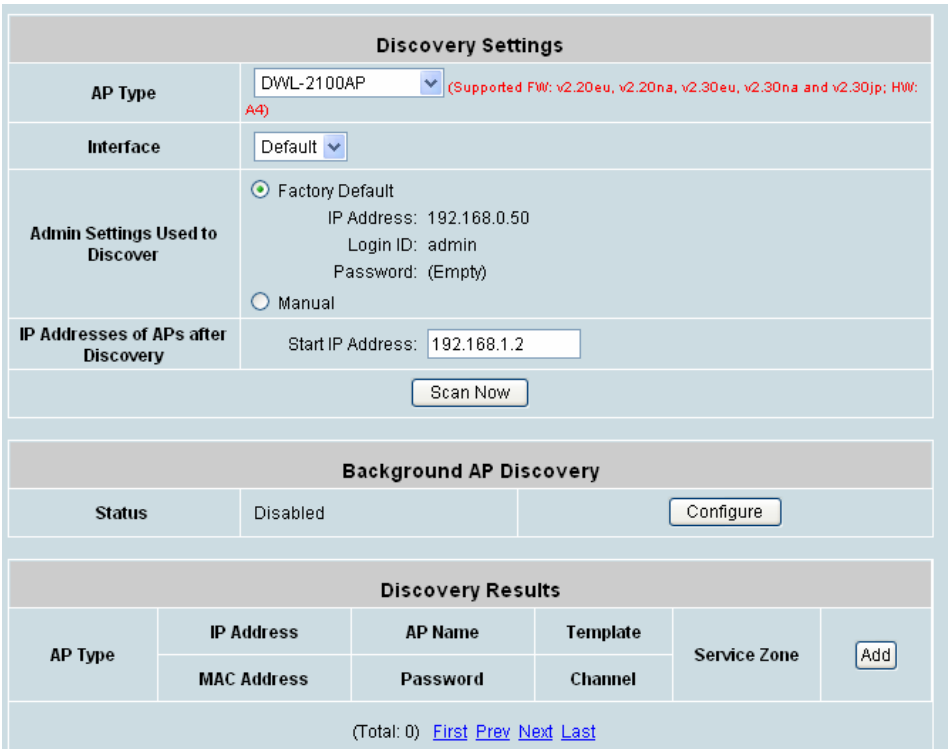
Access Control			
Status	Accept		
Control List			
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:08

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

Associated Clients List							
No.	SSID	MAC Address	Username	Band	Authentication	Signal	Power Save Mode

4.3.2 Discovery

Use this function to detect and manage all the supported APs in the network segment.



- **Discovery Settings**

  When the administrator tries to discover a new AP, select the AP Type and select the Interface (Service Zone) first. If the system is set to Tag-Base mode, only Default Service Zone is available for AP Discovery. Second, select *Manual* in **Admin Settings Used to Discover** field. If the AP is reset to default setting, please select Factory Default, enter the current IP range of the APs, Login ID and Password. The IP of AP with factory default setting is “192.168.0.50”. Then click ***Scan Now*** button. If the new AP has been discovered, it will appear in the following Discovery Results list. If there is a warning message showing below the Discovery Settings, follow the instructions to change configurations.

Note: *Please refer to the datasheet for the supported APs (and the firmware version as well as the hardware version).*

Please fill in the required data.

- **Interface**: Select the default service zone of the interface where APs are connected and to be scanned.
- **Admin Settings Used to Discover:** Select Manual, enter the current IP range of the APs in IP Address field if they are not in default value. The IP of AP with factory default setting is "192.168.0.50". If the AP was discovered before, the IP address of the AP should have been changed. Please enter the right IP address of the AP or reset the AP to default values. Login ID is the admin ID of the AP. Password is the admin password of the AP. If the AP is in default value, just select Factory Default, system can discovery

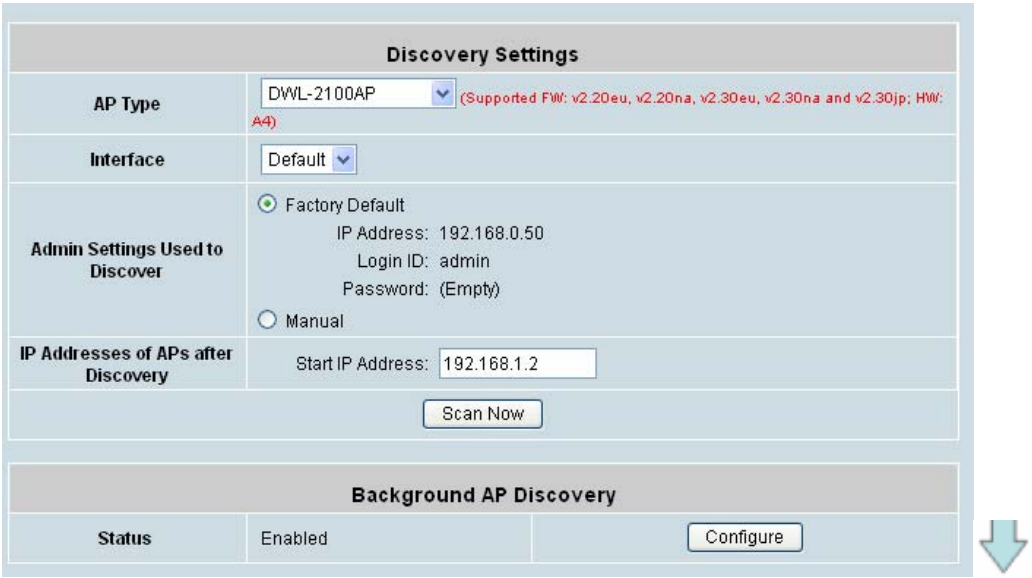
the APs.

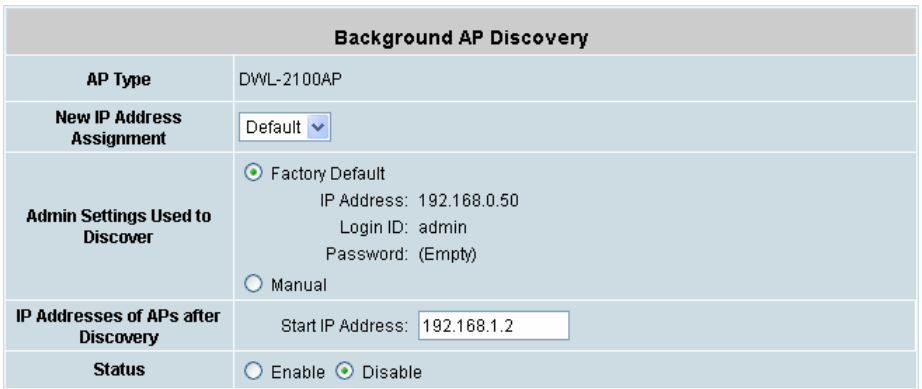
- **IP Addresses of APs after Discovery**: It is the start IP address that will be assigned to the discovered APs and it must be in the same segment of the selected ALN interface (Service Zone).
- **Scan Now:** Click the ***Scan Now*** button and the APs that match the given settings will be shown in the Discovered Results below. If any IP address among the IP range assigned for a specific AP is used, there will be a warning message showing up. Please change the **IP Addresses of APs after Discovery** and then click Scan Now again. For the desired AP, input the desired AP name and admin password, select one template to apply, select the check box, and click ***Add*** to add the discovered AP to the List. For more information about the template, please refer to **4.3.4 Templates**.

- **Background AP Discovery**

The system supports discovering APs periodically in background. The New IP Address Assignment and Access to the AP Admin Interface configuration in Background Auto Discovery page are the same as in the Discovery Settings. Click ***Configure*** and then select ***Enable*** to set the configuration. When **Auto Adding AP to the list** is enabled, the system will add the discovered APs into the List table automatically and apply the selected template in the Template Applied option to the AP. When the configurations are set as requirement, the system will discover new APs periodically and automatically in background.

Click ***Configure*** to enter the **Background AP Discovery** page to have further configuration.





- **New IP Address Assignment**: Service Zone is the service zone where APs are connected to. Start IP Address is the start IP address that will be assigned to the discovered APs and it must be in the same segment of the selected LAN interface.
- **Admin Settings Used to Discover**: Select *Manual*, enter the current IP range of the APs in **IP Address** field if they are in default value. The IP of AP with factory default setting is "192.168.0.50.". If the AP was discovered before, the IP address of AP should have been changed. Please enter the right IP address of the AP or reset the AP to default values. **Login ID** is the admin ID of the AP. **Password** is the password of the AP. If the AP is in default value, just select **Factory Default**, system can discovery the APs.

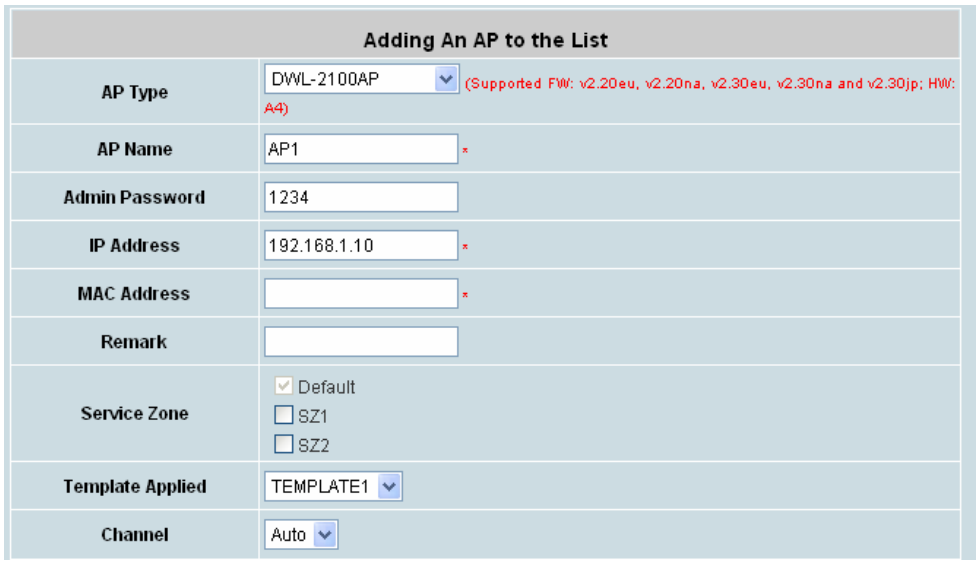
The **Interface, Admin Settings Used to Discover** and **IP Addresses of APs after Discovery** configurations are the same as the settings mentioned above. Check **Enable** to have more configuration. Select **Interval** setting from the drop-down menu to set the system to scan periodically according to this setting (the default value is 10 minutes). If **Auto Adding AP to the list** is enabled, a new detected AP will be assigned an available IP address from the IP address range set in **IP Addresses of APs after Discovery** and applied with the selected template automatically.

- **Discovery Results**

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

4.3.3 Adding

The administrator can add supported APs into the **List** table manually here. Enter the related information of the AP and select a **Template Applied**. Click ***ADD*** and then the AP will be added to the **List**. Similar to the AP added after discovery, a manually added AP will show up with a status of "configuring" in the AP List initially. The system will attempt to configure the AP with the value specified. A couple of minutes later, the AP's status will become "online" or "offline" on the AP List.



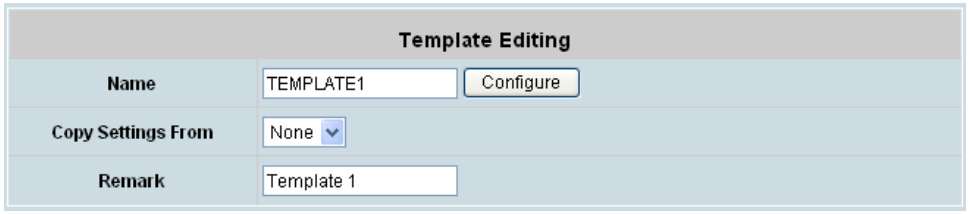
- **AP Type:** The type of supported AP.
- **AP Name:** The mnemonic name of the specific AP.
- **Admin Password:** The password of the AP for the system to access it.
- **IP Address:** The IP address of the AP.
- **MAC Address:** The Media Access Control (MAC) address of the AP.
- **Remark:** The administrator can add some extra information for the AP in this field if desired.
- **Service Zone:** When the system's Service Zone is set to Tag-based mode, additional Service Zone field will be here for assigning services zones to the AP.
- **Template Applied:** The template which will be applied to the AP.
- **Channel:** The Channel of the AP.

4.3.4 Templates

A template is a model that can be copied to every AP without having to configure the each AP individually. The administrator can configure the setting together in the template instead of logging the AP management interface to set the configurations one by one. Click ***Edit*** to go to configuration. Select the **AP type** (if available) and one of the three available templates, and then click ***Edit*** to have the **Template Editing** page.

Except configuring all the template setting manually, copy the configuration of an AP to the template by selecting a **Copy Settings From** and revise some settings is also acceptable. Please select **None** if configuring the whole template from the draft is desired. Enter the **Name** and **Remark** (optional) and click ***Configure*** to have further configuration.

After clicking ***Edit*** to enter the **Details** page, revise the configuration on demands such as **SSID** or **Channel**. About other functions of **Wireless** part please refer to **4.3.1 List**.

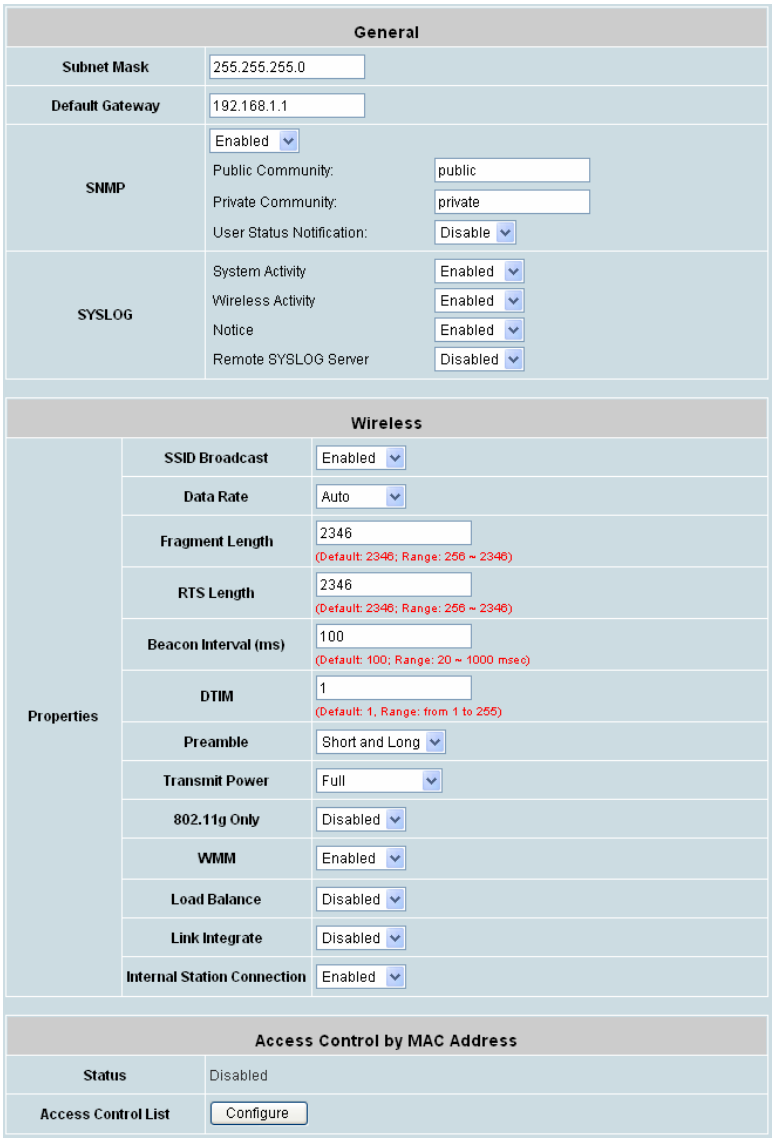


- **Template Editing**

  The administrator can set the template configuration manually or copy the configurations from a specific existing managed AP by **Copy Settings From** option. Click ***Configure*** button to have detailed configurations.

I. DWL-2100AP

DWL-2100AP includes all standards 802.11b/g only. The connection could be select to enable 802.11b/g or disable. The DWL-2100AP is fully compatible with the IEEE 802.11b and 802.11g standards.



Subnet Mask: The default is 255.255.255.0. All devices in the network must share the same subnet mask.

Default Gateway: The default is 192.168.1.1. Enter the gateway IP address for the network, typically a router.

SNMP

- **Public Community:** When SNMP is enabled, modify the public community string.
- **Private Community:** When SNMP is enabled, modify the private community string.
- **User Status Notification:** Select Enable or Disable the notification.

SYSLOG

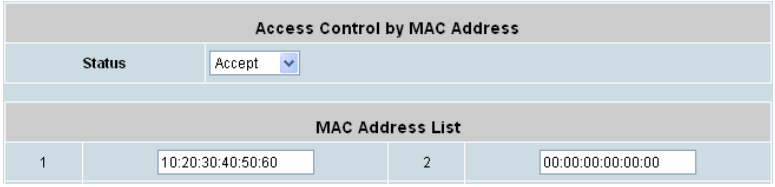
- **System Activity:** Select “Enable” to allow the logging of system actions, such as logging a firmware upgrade.
- **Wireless Activity:** Select “Enable” to allow the logging of any wireless clients that connect to the AP.
- **Notice:** Select “Enable” to allow all other information to be logged.
- **Remote SYSLOG Server:** If you require more space to hold your logs, please provide the IP address of

the Server. The embedded memory can only have up to 300 logs.

Properties

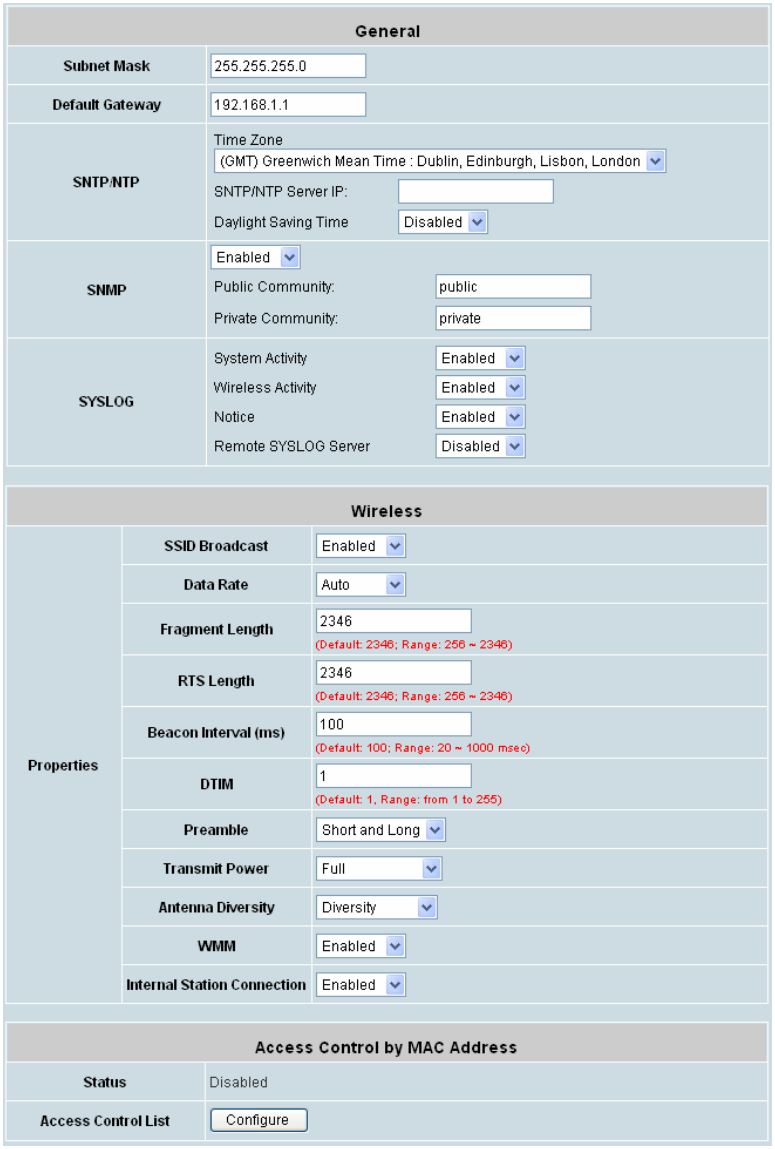
- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from being seen on networked.
- **Data Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **Fragment Length:** The fragmentation threshold determines whether packets will be fragmented. Enter a value between 256 and 2346.
- **RTS Length:** Enter a value between 256 and 2346. When wireless clients would like to send a packet which is larger than this value, it transmits an RTS and waits for reply.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network. Beacons are packets sent by an access point to synchronize a network. Specify a beacon interval value.
- **DTIM:** Delivery Traffic Indication Message. Enter a value between 1 and 255. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Preamble:** Select Long Only or Short and Long. A short preamble is recommended for high-traffic networks.
- **Transmit Power:** Choose full, half (-3dB), 1quarter (-6dB), eighth (-9dB), minimum power.
- **WMM:** WMM stands for Wi-Fi Multimedia, by enabling this feature. It will improve the user experience for audio and video applications over a Wi-Fi network.
- **Load Balance:** When enabled, you allow several APs to balance wireless network traffic and wireless clients among APs in the networks. Assign each access point a different non-overlapping channel.
  - **User Limit:** Enter the number of the limit of load balancing users from 0~64.
- **Link Integrate:** Enable or disable the feature.
- **Internal Station Connection:** Select either Enabled or Disabled. The connection allows clients to communicate with each other when enabled. If this is disabled, wireless stations of the selected band are not allowed to exchange data through the access point.

Access Control by MAC Address: This function provides to control the clients' devices that are allowed to associate with the APs applied with the desired template setting. Choose **Disabled** or **Enabled** in the **Status** column and enter the desired clients' MAC addresses in the MAC Address List. When this function is enabled, please make sure the MAC Address List is not empty.



II. DWL-3200AP v2.2

DWL-3200AP version 2.2 Templates settings allow users to configure General, Wireless Properties, Access Control and wireless 802.11b/g mode settings. Compatible with the 802.11b standard to provide a wireless data rate up to 11 Mbps, users can migrate the system to the 802.11g standard on their own schedule without sacrificing connectivity.



Subnet Mask: The default is 255.255.255.0. All devices in the network must share the same subnet mask.

Default Gateway: The default is 192.168.1.1. Enter the gateway IP address for the network, typically a router.

SNTP/NTP: The time server IP address, time zone, and the local time will be displayed.

- **Time Zone:** Select your time zone from the drop-down menu.

- **SNTP/NTP Server IP:** Enter the IP address of a SNTP/NTP server.
- **Daylight Saving Time:** Check the box to enable daylight saving time.

SNMP

- **Public Community:** When enabled, change the Public Community Name here.
- **Private Community:** When enabled, change the Private Community Name here.

SYSLOG

- **System Activity:** Select "Enable" to allow the logging of system actions, such as logging a firmware upgrade.
- **Wireless Activity:** Select "Enable" to allow the logging of any wireless clients that connect to the AP.
- **Notice:** Select "Enable" to allow all other information to be logged.
- **Remote SYSLOG Server:** If you require more space to hold your logs, please provide the IP address of the Server. The embedded memory can only have up to 300 logs.

Properties

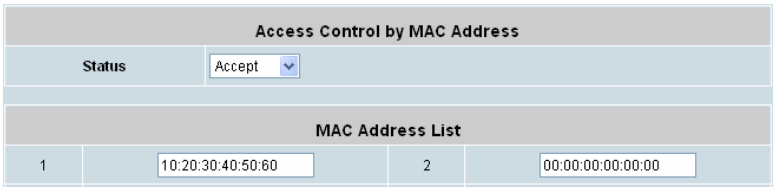
- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from being seen on networked.
- **Data Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **Fragment Length:** The fragmentation threshold determines whether packets will be fragmented. Enter a value between 256 and 2346.
- **RTS Length:** Enter a value between 256 and 2346. When wireless clients would like to send a packet which is larger than this value, it transmits an RTS and waits for reply.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network. Beacons are packets sent by an access point to synchronize a network. Specify a beacon interval value.
- **DTIM:** Delivery Traffic Indication Message. Enter a value between 1 and 255. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Preamble:** Select Long Only or Short and Long. A short preamble is recommended for high-traffic networks.
- **Transmit Power:** Select either Full, Half(-3dB), Quarter(-6dB), Eighth (-9dB) or Minimum (minimum power). This tool can be helpful for security purpose if you wish to limit the transmission range.
- **Antenna Diversity:** Radio is connected to each antenna and supports auto diversity mode by default. The access point will auto switch to the antenna with better RSSI value.
  - **Diversity:** The AP will auto switch to the antenna with better RSSI value.
  - **Left Antenna:** The AP will not switch antenna and the radio will use the left antenna to transmit and

receive packets.

- **Right Antenna:** AP won't switch antenna and the radio will use the right antenna to transmit and receive packets.

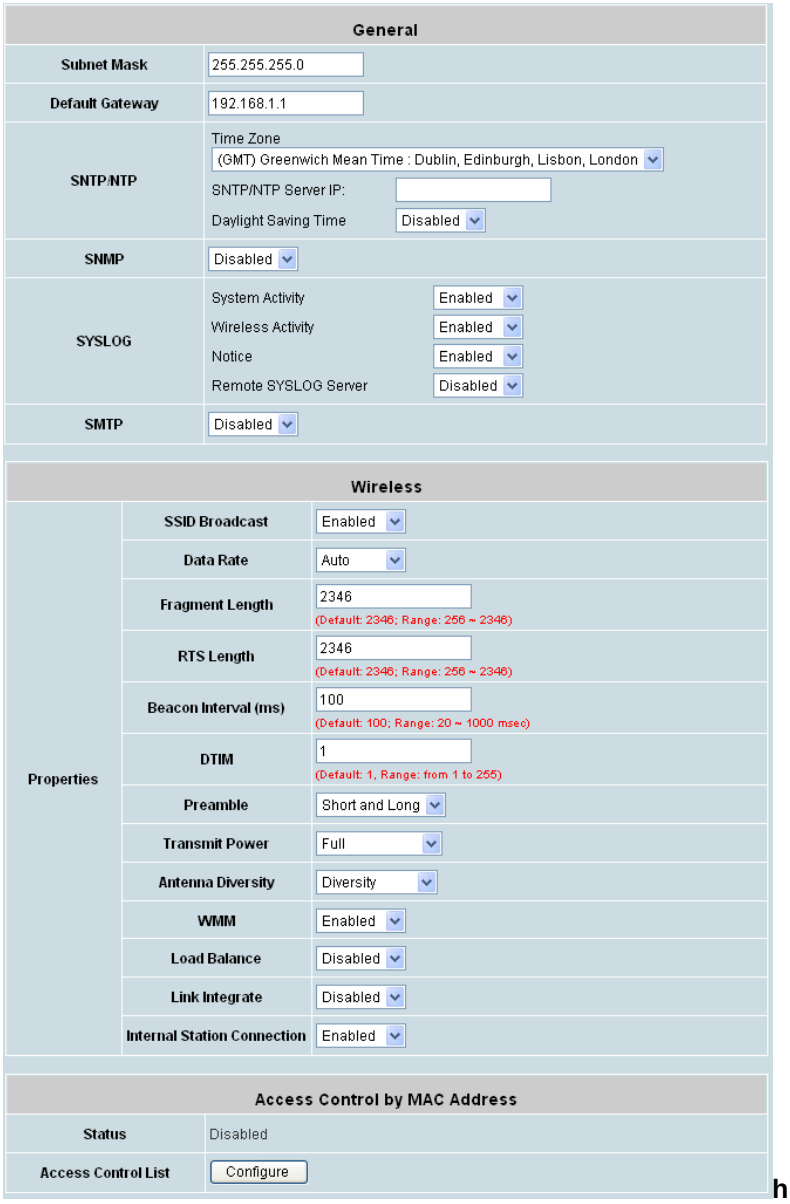
- **WMM:** WMM stands for Wi-Fi Multimedia, by enabling this feature. It will improve the user experience for audio and video applications over a Wi-Fi network.
- **Internal Station Connection:** Select either Enabled or Disabled. The connection allows clients to communicate with each other when enabled.

Access Control by MAC Address: This function provides to control the clients' devices that are allowed to associate with the APs applied with the desired template setting. Choose **Disabled** or **Enabled** in the **Status** column and enter the desired clients' MAC addresses in the MAC Address List. When this function is enabled, please make sure the MAC Address List is not empty.



III. DWL-3200AP v2.3+

DWL-3200AP version 2.3 Templates settings allow users to configure wireless 802.11b/g mode settings. Compared with DWL-3200 v2.2, DWL-3200AP 2.3+ enables users to configure SNMP of General settings and adding the properties of Load Balance and Link Integrate. Due to firmware upgrade issues between DWL-3200AP v2.20 and v2.30 itself, the system treats DWL-3200AP v2.20 and v2.30 as two different AP types and names DWL-3200AP v2.20 as DWL-3200AP-v2.2 and DWL-3200AP v2.30 as DWL-3200AP-v2.3+. Moreover, firmware upgrade from DWL-3200AP v2.20 to v2.3 is NOT supported by the system.



Subnet Mask: The default is 255.255.255.0. All devices in the network must share the same subnet mask.

Default Gateway: The default is 192.168.1.1. Enter the gateway IP address for the network, typically a router.

SNTP/NTP: The time server IP address, time zone, and the local time will be displayed.

- **Time Zone:** Select your time zone from the drop-down menu.
- **SNTP/NTP Server IP:** Enter the IP address of a SNTP/NTP server.
- **Daylight Saving Time:** Check the box to enable daylight saving time.

SNMP

- **Public Community:** When enabled, change the Public Community Name here.
- **Private Community:** When enabled, change the Private Community Name here.

SYSLOG

- **System Activity:** Select "Enable" to allow the logging of system actions, such as logging a firmware upgrade.
- **Wireless Activity:** Select "Enable" to allow the logging of any wireless clients that connect to the AP.
- **Notice:** Select "Enable" to allow all other information to be logged.
- **Remote SYSLOG Server:** If you require more space to hold your logs, please provide the IP address of the Server. The embedded memory can only have up to 300 logs.

SMTP

- **SMTP Server IP:** IP address of SMTP Server
- **SMTP Sender:** The sender's Email address
- **SMTP Recipient:** The receiver's Email address

Properties

- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from being seen on networked.
- **Data Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **Fragment Length:** The fragmentation threshold determines whether packets will be fragmented. Enter a value between 256 and 2346.
- **RTS Length:** Enter a value between 256 and 2346. When wireless clients would like to send a packet which is larger than this value, it transmits an RTS and waits for reply.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network.
- **DTIM:** Delivery Traffic Indication Message. Enter a value between 1 and 255.
- **Preamble:** Select Long Only or Short and Long. A short preamble is recommended for high-traffic networks.
- **Transmit Power:** Select either Full, Half(-3dB), Quarter(-6dB), Eighth (-9dB) or Minimum (minimum power). This tool can be helpful for security purpose if you wish to limit the transmission range.
- **Antenna Diversity:** Radio is connected to each antenna and supports auto diversity mode by default. The access point will auto switch to the antenna with better RSSI value.
  - **Diversity:** The AP will auto switch to the antenna with better RSSI value.
  - **Left Antenna:** The AP will not switch antenna and the radio will use the left antenna to transmit and

receive packets.

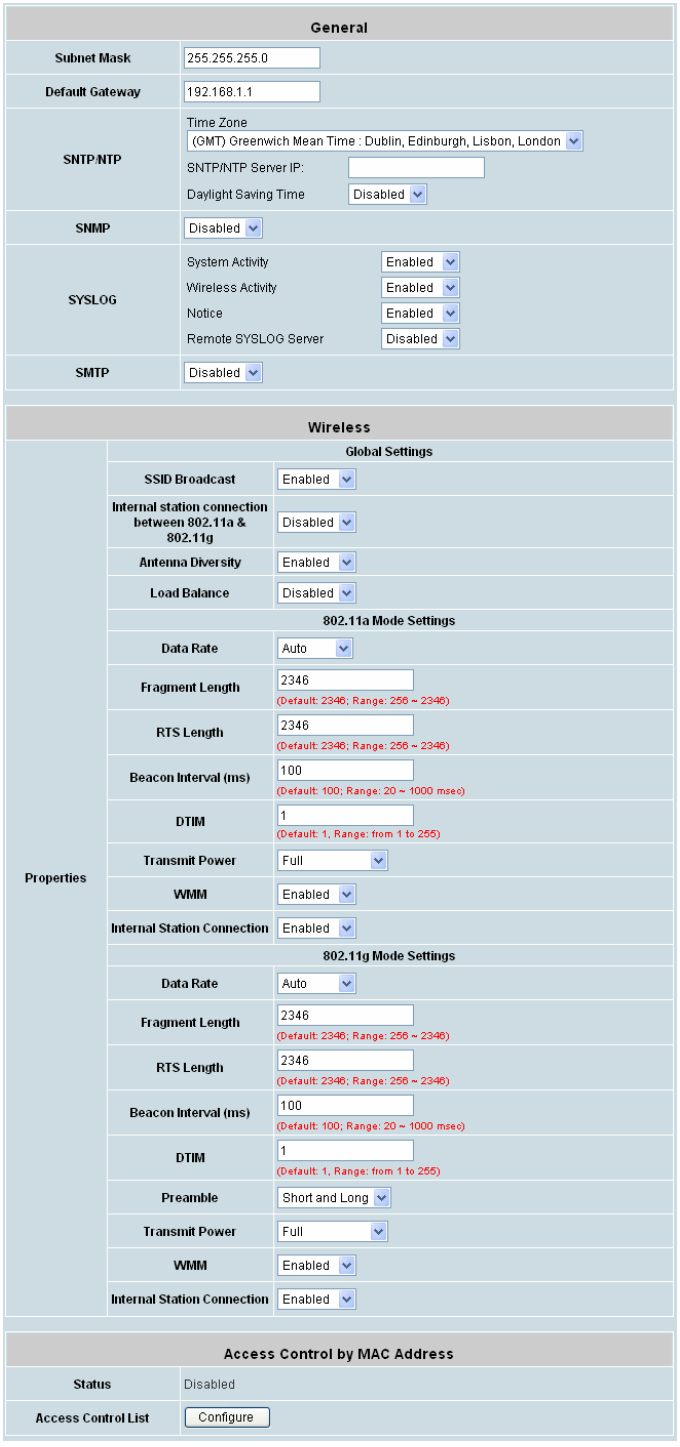
- **Right Antenna:** AP won't switch antenna and the radio will use the right antenna to transmit and receive packets.

- **WMM:** WMM stands for Wi-Fi Multimedia, by enabling this feature. It will improve the user experience for audio and video applications over a Wi-Fi network.
- **Load Balance:** When enabled, you allow several APs to balance wireless network traffic and wireless clients among APs in the networks. Assign each access point a different non-overlapping channel.
  - **User Limit:** Enter the number of the limit of load balancing users from 0~64.
- **Link Integrate:** Enable or disable the feature.
- **Internal Station Connection:** Select either Enabled or Disabled. The connection allows clients to communicate with each other when enabled. If this is disabled, wireless stations of the selected band are not allowed to exchange data through the access point.

Access Control by MAC Address: This function provides to control the clients' devices that are allowed to associate with the APs applied with the desired template setting. Choose **Disabled** or **Enabled** in the **Status** column and enter the desired clients' MAC addresses in the MAC Address List. When this function is enabled, please make sure the MAC Address List is not empty.

IV DWL-8200AP

DWL-8200AP Templates settings allows users to configure 802.11a and 802.11b and g mode settings. The connection could be select to enable 802.11a, 802.11b/g, or disable. Compatible with 802.11a, 802.11b and 802.11g Devices that is fully compatible with the IEEE 802.11a, 802.11b and 802.11g standards, the DWL-8200AP can connect with existing 802.11b-, 802.11g- or 802.11a-compliant wireless network adapter cards. It is compatible with the 802.11b standard to provide a wireless data rate of up to 11Mbps.



Subnet Mask: The default is 255.255.255.0. All devices in the network must share the same subnet mask.

Default Gateway: The default is 192.168.1.1. Enter the gateway IP address for the network, typically a router.

SNTP/NTP: The time server IP address, time zone, and the local time will be displayed.

- **Time Zone:** Select your time zone from the drop-down menu.
- **SNTP/NTP Server IP:** Enter the IP address of a SNTP/NTP server.
- **Daylight Saving Time:** Check the box to enable daylight saving time.

SNMP

- **Public Community:** When enabled, change the Public Community Name here.
- **Private Community:** When enabled, change the Private Community Name here.

SYSLOG

- **System Activity:** Select "Enable" to allow the logging of system actions, such as logging a firmware upgrade.
- **Wireless Activity:** Select "Enable" to allow the logging of any wireless clients that connect to the AP.
- **Notice:** Select "Enable" to allow all other information to be logged.
- **Remote SYSLOG Server:** If you require more space to hold your logs, please provide the IP address of the Server. The embedded memory can only have up to 300 logs.

SMTP

- **SMTP Server IP:** IP address of SMTP Server
- **SMTP Sender:** The sender's Email address
- **SMTP Recipient:** The receiver's Email address

Properties

Global Settings

- **SSID Broadcast:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from being seen on networked.
- **Internal Station Connection between 802.11a & 802.11g:** Enabling this feature allows devices on the 802.11a network, to exchange data with devices on the 802.11g network through Access Point. If disabled, a partition is created between the networks within the Access point. This feature is only available when both 11a and 11g are both in Access Point mode.
- **Antenna Diversity:** When enabled, each radio will automatically switch to the antenna with the greatest RSSI value. When disabled, each radio will use its main antenna.
- **Load Balance:** When enabled, you allow several APs to balance wireless network traffic and wireless clients among APs in the networks. Assign each access point a different non-overlapping channel.
  - **User Limit:** Enter the number of the limit of load balancing users from 0~64.

802.11a Mode Settings:

- **Data Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **Fragment Length:** The fragmentation threshold determines whether packets will be fragmented. Enter a value between 256 and 2346.

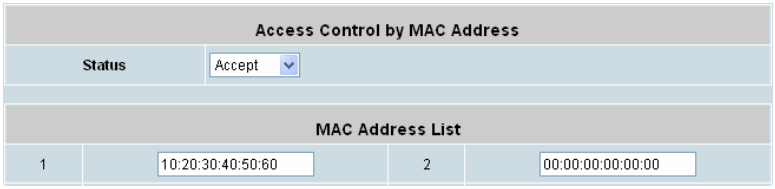
- **RTS Length:** Enter a value between 256 and 2346. When wireless clients would like to send a packet which is larger than this value, it transmits an RTS and waits for reply.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network.
- **DTIM:** Delivery Traffic Indication Message. Enter a value between 1 and 255. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Transmit Power:** Select either Full, Half(-3dB), Quarter(-6dB), Eighth (-9dB) or Minimum (minimum power). This tool can be helpful for security purpose if you wish to limit the transmission range.
- **WMM:** WMM stands for Wi-Fi Multimedia, by enabling this feature. It will improve the user experience for audio and video applications over a Wi-Fi network.
- **Internal Station Connection:** Select either Enabled or Disabled. The connection allows clients to communicate with each other when enabled.

802.11g Mode Settings

- **Data Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **Fragment Length:** The fragmentation threshold determines whether packets will be fragmented. Enter a value between 256 and 2346.
- **RTS Length:** Enter a value between 256 and 2346. When wireless clients would like to send a packet which is larger than this value, it transmits an RTS and waits for reply.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmission between the access point and the wireless network. Beacons are packets sent by an access point to synchronize a network. Specify a beacon interval value.
- **DTIM:** Delivery Traffic Indication Message. Enter a value between 1 and 255. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Preamble:** Select Long Only or Short and Long. A short preamble is recommended for high-traffic networks.
- **Transmit Power:** Select either Full, Half(-3dB), Quarter(-6dB), Eighth (-9dB) or Minimum (minimum power). This tool can be helpful for security purpose if you wish to limit the transmission range.
- **WMM:** (Wi-Fi Multimedia) Improve the user experience for audio, video and voice applications over a Wi-Fi network. WMM is based on a subnet of the IEEE 802.11e WLAN QoS draft standard.
- **Internal Station Connection:** Select either Enabled or Disabled. The connection allows clients to communicate with each other when enabled. If this is disabled, wireless stations of the selected band are not allowed to exchange data through the access point.

Access Control by MAC Address: This function provides to control the clients' devices that are allowed to associate with the APs applied with the desired template setting. Choose **Disabled** or **Enabled** in the

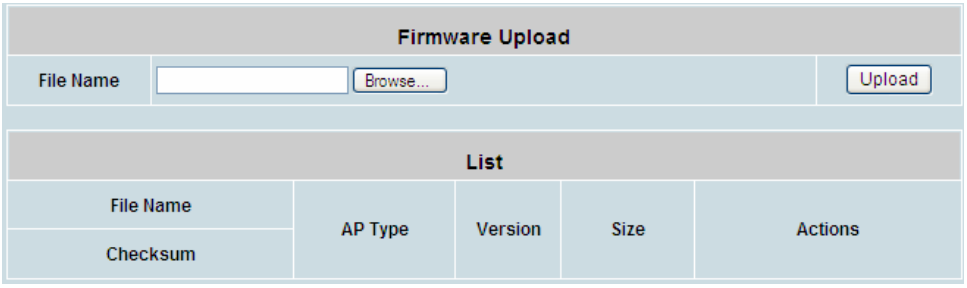
Status column and enter the desired clients' MAC addresses in the MAC Address List. When this function is enabled, please make sure the MAC Address List is not empty.



4.3.5 Firmware

This is where AP's firmware can be uploaded. The current firmware can also be downloaded to the local storage if required.

The system supports the firmware management of APs to upload new firmware, delete the existing firmware, and download the firmware to managed APs. Note that the AP's firmware version must be one that has been integrated.



- **Firmware Upload**
  - **File Name:** The name of the AP firmware to be uploaded. Click ***Browse*** to select an AP firmware file to upload.
  - **Upload:** Click ***Upload*** button to upload the file from a local disk to the system.
- **List:** All uploaded firmware will be listed here.
  - **File Name:** The name of the AP firmware has been uploaded.
  - **Checksum:** The automatically detected security identification of the firmware.
  - **AP Type:** The AP type of the firmware.
  - **Version:** The version of the firmware.
  - **Size:** The file size of the firmware.
  - **Download:** Click ***Download*** to save the selected firmware to local disk.

  - **Delete:** Click ***Delete*** to delete the selected firmware from the system.

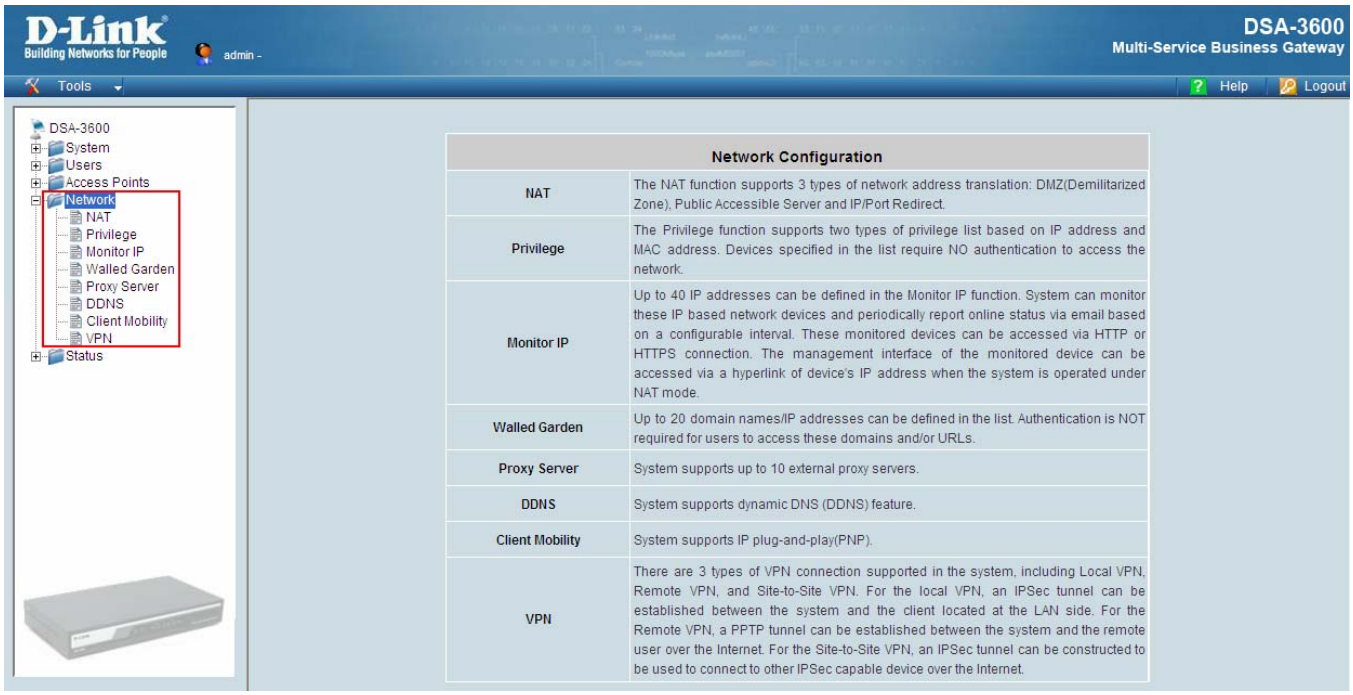
4.3.6 Upgrade

The administrator can upgrade the firmware of selected APs individually or at the same time by checking the check box of the APs in Selection column. Note that both the version before upgrade and the next version must be ones that have been integrated with the system. Check the APs which need to be upgraded and select the upgrade version of firmware, and click ***Apply*** to upgrade firmware.

- **Last Upgraded Time:** The time when the AP was last upgraded.
- **Next Version:** The firmware version to be upgrade to the AP.

4.4 Network

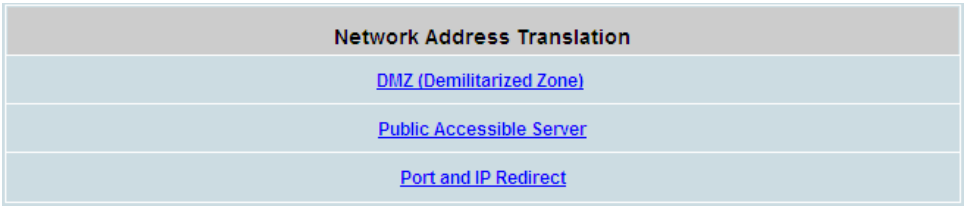
This section provides information on **NAT, Privilege, Monitor IP, Walled Garden, Proxy Server, DDNS, Client Mobility** and **VPN.** It displays the information of the interfaces. For WAN1 and WAN2, it will show the IP Address and the connection Status. For LAN Ports, it will show the IP Address, SSID and Status of each Service Zone.



Network Configuration	
NAT	The NAT function supports 3 types of network address translation: DMZ(Demilitarized Zone), Public Accessible Server and IP/Port Redirect.
Privilege	The Privilege function supports two types of privilege list based on IP address and MAC address. Devices specified in the list require NO authentication to access the network.
Monitor IP	Up to 40 IP addresses can be defined in the Monitor IP function. System can monitor these IP based network devices and periodically report online status via email based on a configurable interval. These monitored devices can be accessed via HTTP or HTTPS connection. The management interface of the monitored device can be accessed via a hyperlink of device's IP address when the system is operated under NAT mode.
Walled Garden	Up to 20 domain names/IP addresses can be defined in the list. Authentication is NOT required for users to access these domains and/or URLs.
Proxy Server	System supports up to 10 external proxy servers.
DDNS	System supports dynamic DNS (DDNS) feature.
Client Mobility	System supports IP plug-and-play(PNP).
VPN	There are 3 types of VPN connection supported in the system, including Local VPN, Remote VPN, and Site-to-Site VPN. For the local VPN, an IPSec tunnel can be established between the system and the client located at the LAN side. For the Remote VPN, a PPTP tunnel can be established between the system and the remote user over the Internet. For the Site-to-Site VPN, an IPSec tunnel can be constructed to be used to connect to other IPSec capable device over the Internet.

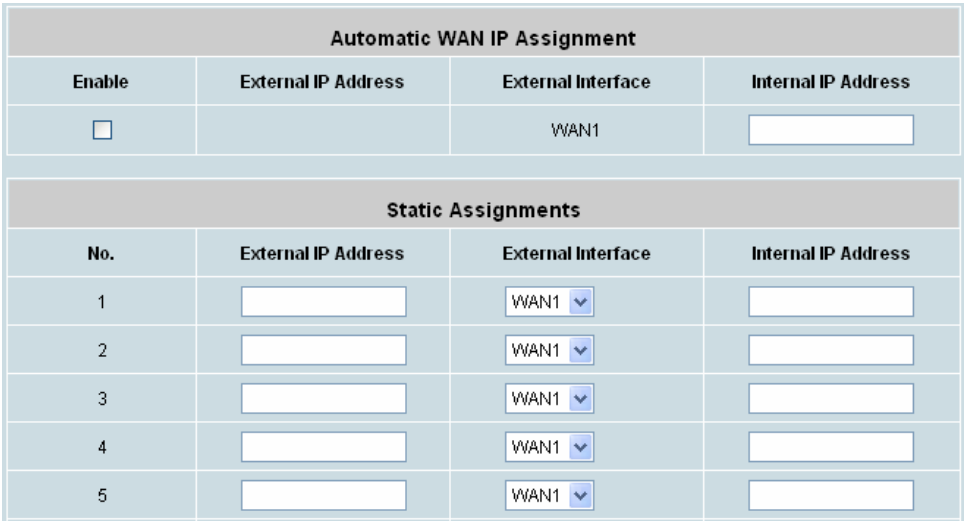
4.4.1 NAT

There are three functions that need to be set here: **DMZ (Demilitarized Zone), Public Accessible Server** and **Port and Redirect**.



- **DMZ (Demilitarized Zone)**

The administrator can define mandatory external to internal IP mapping using this function, so that a client on the WAN side network can access the private machine by accessing the external IP. Choose to enable Automatic WAN IP Assignment by checking the **Enable** check box and enter the **Internal IP address**. When **Automatic WAN IP Assignment** function is enabled, accessing WAN1 will be mapped to access the **Internal IP Address**. For **Static Assignments**, enter **Internal** and **External** IP Addresses as a set and choose to use WAN1 or WAN2 for the **External Interface** from the drop-down menu. These settings will become effective immediately after clicking the ***Apply*** button.



- **Public Accessible Server**

The administrator can set up virtual servers using this function, so that the computers not belonging to the managed network can access the servers in the managed network via WAN port IP of DSA-3600. Enter the **External Service Port**, **Local Server IP Address** and **Local Server Port** accordingly. Depending on the different services selected, the network service will be able to use the **TCP** protocol or the **UDP** protocol. In the **Enable** column, check the desired server to be enabled. These settings will be effective immediately after clicking the ***Apply*** button.

Public Accessible Server					
No.	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				TCP UDP	
2				TCP UDP	
3				TCP UDP	
4				TCP UDP	
5				TCP UDP	

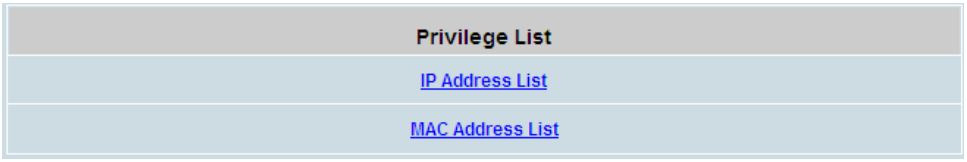
- **Port and IP Redirect**

When users attempt to connect to the port of a **Destination IP Address** listed here, the connection packet will be converted and redirected to the port of the **Translated to Destination IP Address**. Enter the **IP Address** and **Port of Destination**, and the **IP Address** and **Port of Translated to Destination** accordingly. Depending on the different services selected, choose the **TCP** protocol or **UDP** protocol. These settings will become effective immediately after clicking ***Apply***.

Port and IP Redirect					
No.	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1					TCP UDP
2					TCP UDP
3					TCP UDP
4					TCP UDP
5					TCP UDP

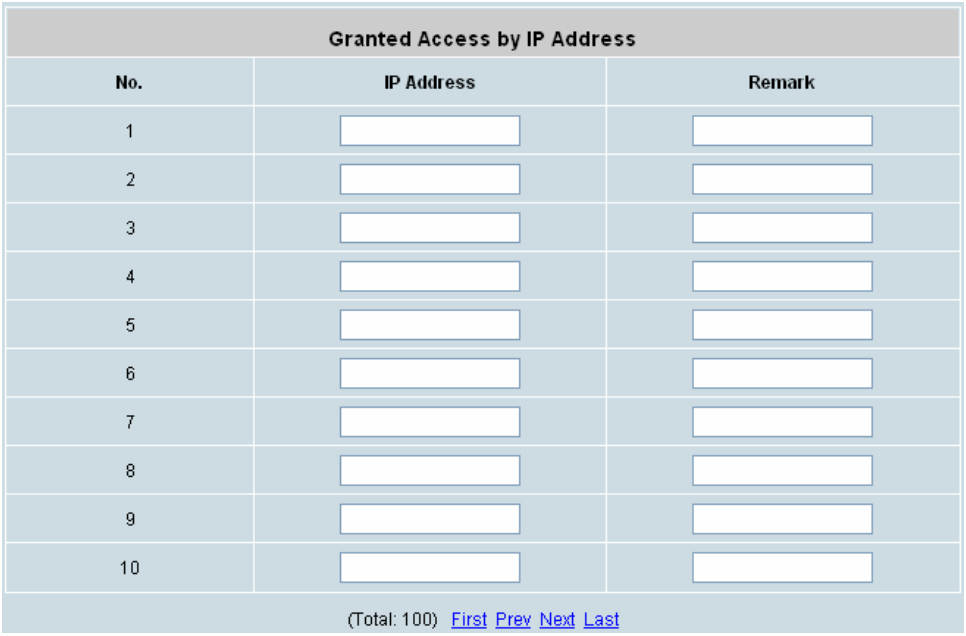
4.4.2 Privilege

The DSA-3600 provides two **Privilege Lists**, **IP Address List** and **MAC Address List**. The administrator can add desired IP addresses and MAC addresses in these lists using the Privilege List function. The IP addresses and MAC addresses in these lists are allowed to access the network without authentication.



- **IP Address List**

Clients in the IP Address List are allowed to access the Internet directly without authentication. **Remark** is optional but useful for tracking purpose. These settings will be effective immediately after clicking ***Apply***.



Warning: *Permitting specific IP addresses to have network access rights without going through standard authentication process may result in security problems.*

- **MAC Address List**

Clients in the MAC Address List are allowed to access the Internet directly without authentication. Enter the MAC address (in format: xx:xx:xx:xx:xx:xx) and the remark (optional) accordingly. These settings will be effective immediately after clicking ***Apply***.

Granted Access by MAC Address		
No.	**MAC Address**	**Remark**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
(Total: 100) First Prev Next Last		

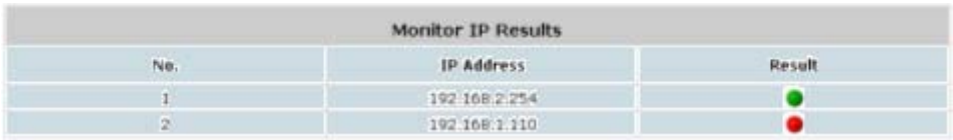
Warning: *Permitting specific MAC addresses to have network access rights without going through standard authentication process may result in security problems.*

4.4.3 Monitor IP

The DSA-3600 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.

The Monitor IP supported by the system can monitor the devices in this list by pinging them periodically. The administrator can use this function to monitor third-party APs or any other IP devices. Enter the IP addresses of the devices that the administrator wants to monitor and click the ***Apply*** button. When the administrator logs in the system, click the ***Monitor Now*** button to execute the monitor action manually and a new page with status of monitored devices will appear. The red dots mean the devices are unreachable and the green dots mean the devices are reachable and alive. A notification e-mail of the monitored status can be set to notify the administrator in a set interval. For more information, please refer to E-mail & SYSLOG in Status category. For monitored devices on LAN, such as third-party APs or web cameras with built-in web-based administrative interface, hyperlinks can be created for the administrator to access the administrative interface of the devices by clicking the ***Create*** button in the Hyperlink column. This hyperlink function enables the administrator to manage the devices from WAN easily.

When the ***Monitor Now*** button is clicked, **Monitor IP Results** page will appear. If the entered IP address is unreachable, a red dot under Result field will appear. A green dot indicates that the IP address is reachable and alive.



Monitor IP Results

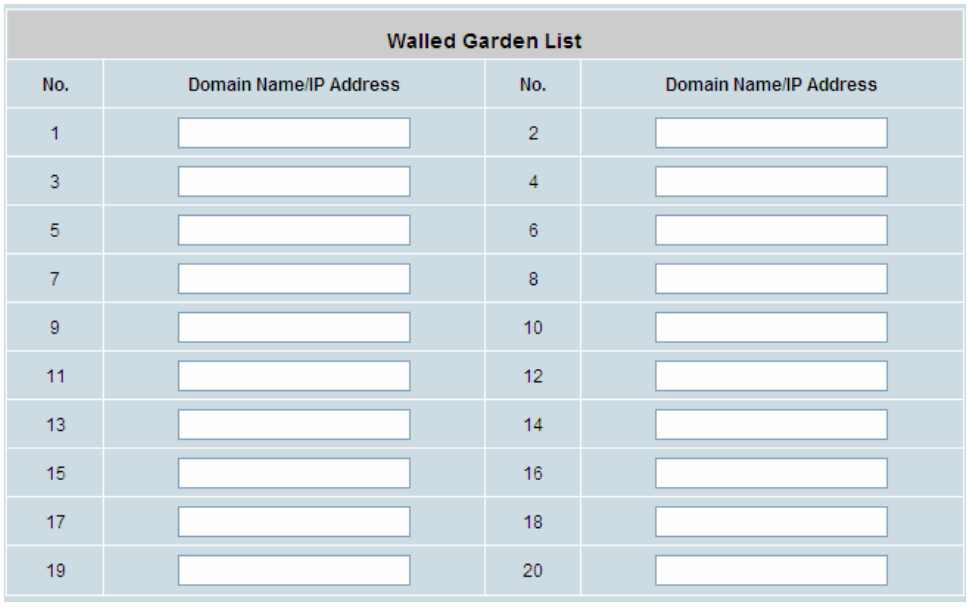
No.	IP Address	Result
1	192.168.2.254	
2	192.168.1.110	

4.4.4 Walled Garden

This function allows clients of specified addresses or domain names to access the Internet before login and authentication. Users without network access right in this list can make use of the actual network service free of charge.

Enter the **IP Address** or **Domain Name** of the websites in the list. The settings will be effective immediately after clicking ***Apply***.

The **Walled Garden** supported by the system provides free surfing areas for clients to access before they are authenticated by the system. For example, on-demand users without the network access right in hotels can still have a chance to experience the actual network service free of charge.

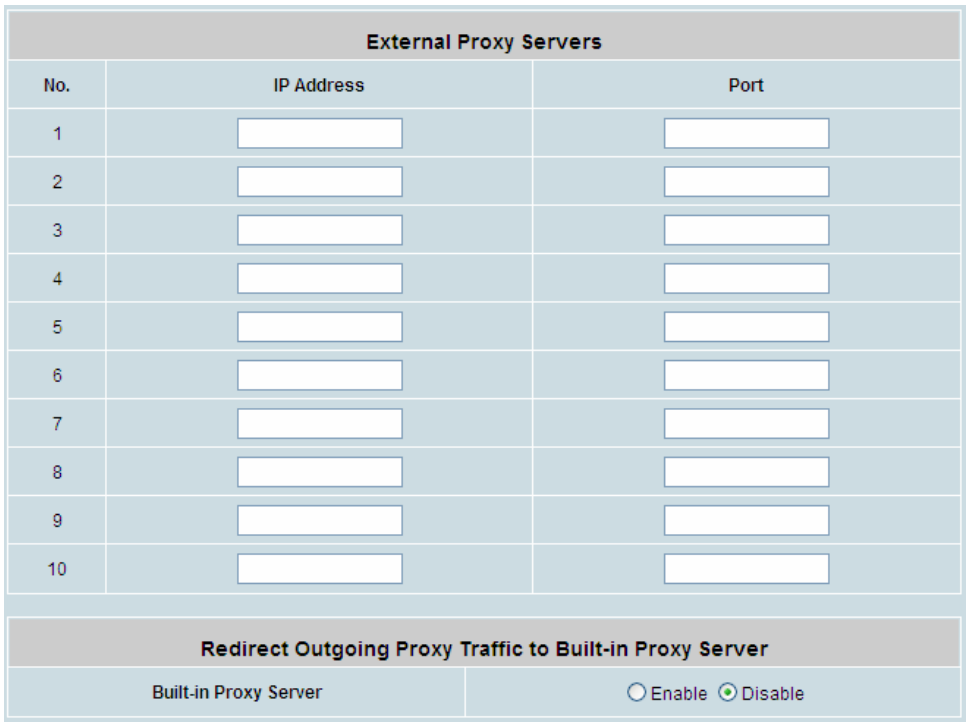


Walled Garden List			
No.	Domain Name/IP Address	No.	Domain Name/IP Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

Caution: *To use domain names in list, a DNS server must first be configured in the network in order for this function to work.*

4.4.5 Proxy Server

The system provides a Build-in Proxy Server and External Proxy Server function. Under its security management, the system will match the proxy setting of **External Proxy Servers** list to the clients' proxy setting in their browsers. If no matching, the clients will not be able to get the login page and thus unable to access the network. If there is matching, then the clients will be directed to the system first for authentication. After successful authentication, the clients' will be redirected back to the desired proxy servers.

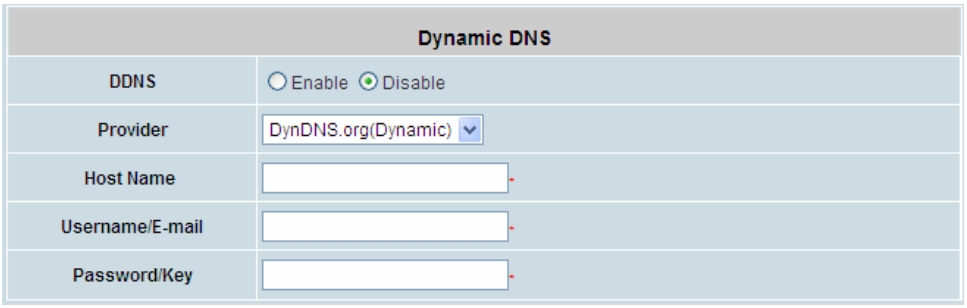


- **External Proxy Servers:** The system will match the proxy setting of the **External Proxy Servers** list to the clients' proxy setting if the setting is found in their browsers. If no matching is found, the clients will not be able to get the login page nor access the network. If a matching is found, the clients will first be directed to the system for authentication, and upon successful authentication, redirect the clients back to the desired proxy servers.
- **Redirect Outgoing Proxy Traffic To Built-in Proxy Server:** The DSA-3600 has a built-in proxy server. If this function is enabled, the clients will be forced to treat the DSA-3600 as the proxy server regardless of the clients' original proxy settings, and all traffic will be redirected through the built-in proxy server.

Note: *For more information about setting up the proxy servers, please refer to Appendix C. Proxy Configuration.*

4.4.6 DDNS

The system provides a convenient dynamic DNS function to translate the IP address of WAN port to a domain name that helps the administrator memorize and connect to WAN1 port. When the DDNS is enabled, the system will update the newest IP address regularly to the DNS server if the WAN1 interface is set to Dynamic. These settings will become effective immediately after clicking ***Apply***.

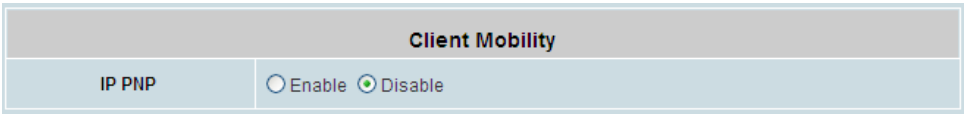


- **DDNS:** Dynamic DNS, choose to enable or disable this function.
- **Provider:** Select the DNS provider.
- **Host name:** The IP address/domain name of the WAN port.
- **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- **Password/Key:** The register password for the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

Note: *The fields with red asterisks are required to be filled in.*

4.4.7 Client Mobility

The DSA-3600 supports **IP PNP** function. When enabled, this function allows clients with fixed or assigned IP address to authenticate through the DSA-3600 to access the network. By enabling IP PNP, a PC with a static IP address will be able to access the network even if the system enables the built-in DHCP server. No TCP/IP reconfiguration is needed.

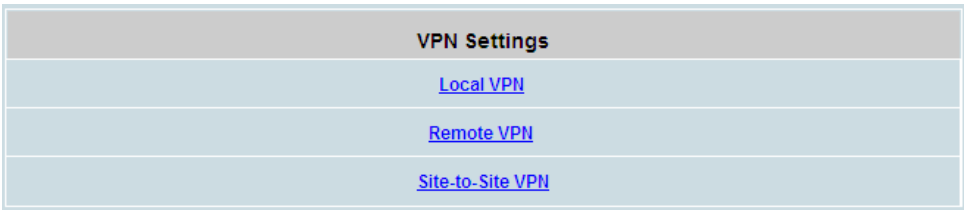


- **IP PNP:** When IP PNP is enabled, a PC with a static IP address can still access the network even the system enables built-in DHCP server. No TCP/IP reconfiguration is needed.

4.4.8 VPN

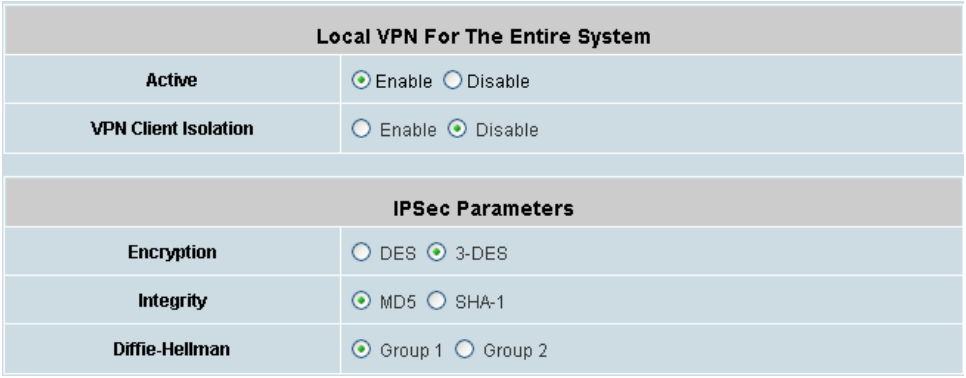
Virtual **P**rivate **N**etwork (VPN) is designed to increase the security of information transferred over the Internet. VPN can work with wired or wireless networks and dial-up connections over POPS. It can create a private encrypted tunnel from the end user's computer, through the local wireless network and the Internet, to corporate servers and databases. There are 3 types of VPN connection supported by this system: **Local**, **Remote**, and **Site-to-Site**.

Windows Vista clients are able to use VPN from local and remote. Windows Vista's local VPN is implemented via PPTP in this release and named as "Local PPTP VPN" because Windows Vista's IPSec tunnel mode behaves differently from Windows XP and 2000. Local PPTP VPN uses the configuration of Remote VPN. When Remote VPN is disabled, Windows Vista's clients can only use non-IPSec login even though this user is configured as Local VPN required.



- **Local VPN**

Local VPN allows a user to create the VPN tunnel between the user's device and DSA-3600, 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 on Local VPN, please refer to ***Appendix H. Local VPN***.

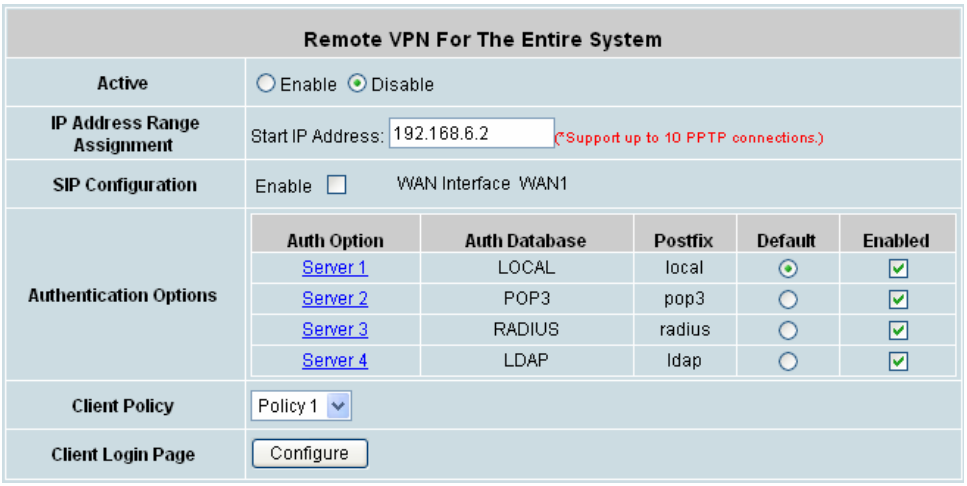


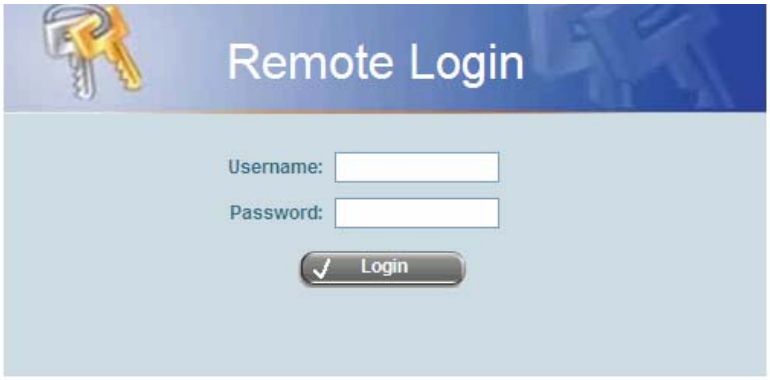
- **Remote VPN**

When the setting is enabled, the system allows the VPN tunnel between a remote client and the system to encrypt the data transmission via PPTP. The system's VPN supports end-users' devices under Windows 2000, Windows XP SP1, SP2 and Windows Vista. Start IP field must be entered when enabled. The Client Policy, Supported Authentication Servers and the Remote VPN login page also can be customizing here. Check the **Enable** or **Disable** radio button in the Active column to activate or deactivate this function. If the Remote VPN function is enabled, enter the **Start IP** in the Client IP Address Range column.

Note: *Vista users have to check enable in the Active column.*

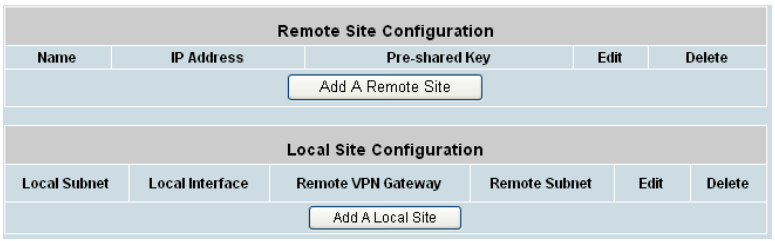
SIP transparent proxy will help the SIP traffic of authenticated Remote VPN users when the SIP service is enabled in the last service zone. Remote users can use SIP when SIP Configuration here is enabled.





- **Site-to-Site VPN**

When the setting is enabled, the system will enable the IPSec VPN tunnel between two remote networks/sites to encrypt the data transmission. Click ***Add a Remote Site*** button to set the configuration about remote VPN capable devices, such as a VPN gateway. Click ***Add a Local Site*** button to set the configuration of the local site. An IPSec tunnel can be constructed and used to connect to other IPSec capable devices on the Internet.



Click ***Add a Remote Site*** to enter the **Remote VPN Gateway** page for further configuration.

Remote VPN Gateway	
Name	
IP Address	
Authentication Method	Pre-shared Key
Pre-shared Key	
Phase1 Proposal	Encryption AES256 Authentication SHA-1
Diffie-Hellman Group	Group 1 Group 2 Group 5
IKE Life Time	IKE Life Time 8h (s: second, m: minute, h: hour, d: day)
Dead Peer Detection	DPD Delay 10 (second) DPD Timeout 15 (second)

Remote Subnet		
No.	Network	Mask
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)

Click ***Add a Local Site*** to enter the **Local Site Information** page for further configuration.

Local Site Information	
Local Interface	WAN1
Remote VPN Gateway	Edit Host Add a New Host
Local Subnet	(in prefix notation: x.x.x.x/yy)
Remote Subnet	
Phase2 Proposal	Encryption AES256 Authentication SHA-1
Key's Life Time	Key's Life Time 24h (s: second, m: minute, h: hour, d: day)
Rekey	Enable Rekey Rekey Margin 9m (s: second, m: minute, h: hour, d: day)
Perfect Forward Secrecy	Enable PFS PFS GroupMODP1024 Group 2

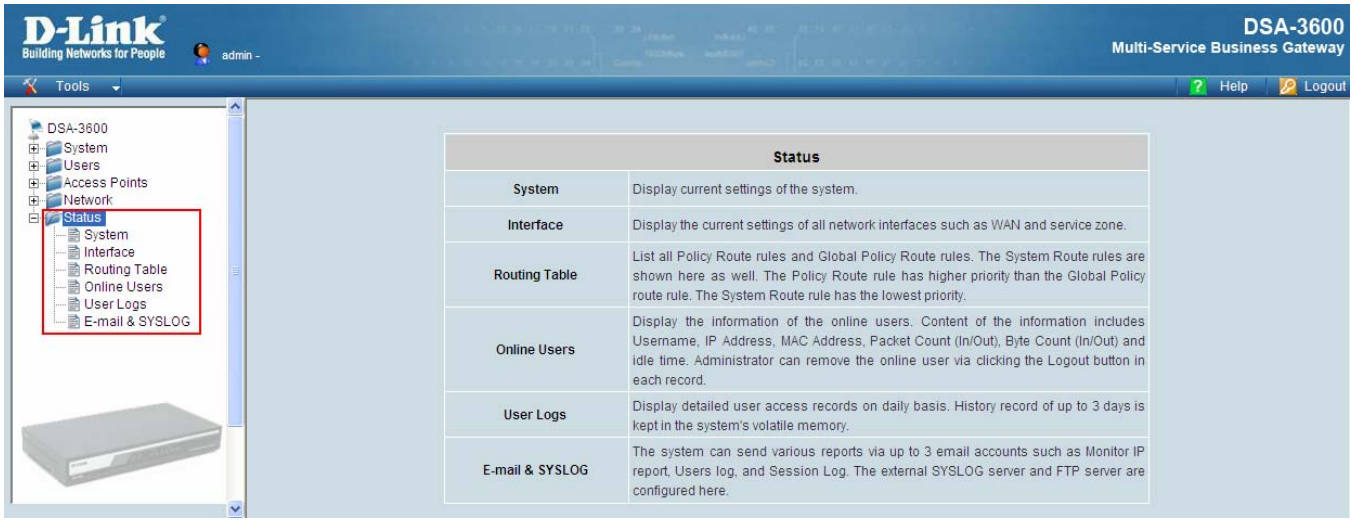
Click ***Add a New Host*** to enter the screen of **Remote VPN Gateway**.

Remote VPN Gateway	
Name	
IP Address	
Authentication Method	Pre-shared Key
Pre-shared Key	
Phase1 Proposal	Encryption AES256 Authentication SHA-1
Diffie-Hellman Group	Group 1 Group 2 Group 5
IKE Life Time	IKE Life Time 8h (s: second, m: minute, h: hour, d: day)
Dead Peer Detection	DPD Delay 10 (second) DPD Timeout 15 (second)

Remote Subnet		
No.	Network	Mask
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)

4.5 Status

This section covers the description of system status information and online user status, which include **System**, **Interface**, **Online Users**, **User Logs**, and **E-mail & SYSLOG**. An overview of the system is also provided here for the administrator's reference.



Status	
System	Display current settings of the system.
Interface	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.
Online Users	Display the information of the online users. Content of the information includes Username, IP Address, MAC Address, Packet Count (In/Out), Byte Count (In/Out) and idle time. Administrator can remove the online user via clicking the Logout button in each record.
User Logs	Display detailed user access records on daily basis. History record of up to 3 days is kept in the system's volatile memory.
E-mail & SYSLOG	The system can send various reports via up to 3 email accounts such as Monitor IP report, Users log, and Session Log. The external SYSLOG server and FTP server are configured here.

4.5.1 System

This section provides an overview of the system administration.

System Setting Overview		
Firmware Version		3.00.00
Build		03000
System Name		DSA-3600
Homepage Redirect URL		http://www.dlink-intl.com/
SYSLOG Server - System Log		N/A:N/A
SYSLOG Server - On-demand Users Log		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Load Balancing		Disabled
SNMP		Disabled
User Logs	Retained Days	3 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
System Time	NTP Server	tock.usno.navy.mil
	Time	2007/11/29 14:19:43 +0800
User Session Control	Idle Time Out	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A

The following information in the table describes all the items found in the System Setting Overview menu:

Item		***Description***
Firmware Version		The present firmware version of DSA-3600
Build		The build version of firmware
System Name		The system name. The default is DSA-3600
Homepage Redirect URL		The page to which the users are directed after initial login success.
SYSLOG server - System Log		The IP address and port number of the external SYSLOG Server. N/A means that it is not configured.
SYSLOG server – On-demand 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 Disconnection		Enabled/Disabled stands for the connection at WAN is normal or abnormal and all online users are allowed/disallowed to log in the network.
WAN Failover		Shows the connection status of WAN1 and WAN2.
SNMP		Enabled/Disabled stands for the current status of the SNMP management function.
User Logs	**Retained Days**	The maximum number of days for the system to retain the users' information.
	Receiver E-mail Address(es)	The e-mail address that the traffic history information will be sent to.
System Time	**NTP Server**	The network time server that the system is set to align.
	Time	The system time is shown as the local time.
User Session Control	**Idle Time Out**	The number of minutes allowed for the users to be inactive.
	Multiple Login	Enabled/Disabled stands for the current setting to allow/ not allow multiple logins form the same account.
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

4.5.2 Interface

This section provides an overview of the all interfaces for the administrator such as **WAN1, WAN2, Service Zone - Default, Service Zone** - **Default DHCP Server**. Each service zone represents a virtual system. Therefore, the information of the system's network interface is grouped by service zone.

Network Interface		
WAN1	MAC Address	00:0B:01:02:00:01
	IP Address	10.29.2.197
	Subnet Mask	255.255.0.0
WAN2	Disabled	
	WAN1	WAN2
Packets In	4030783 (Δ 3421586)	0 (Δ 0)
Packets Out	188268 (Δ 61010)	0 (Δ 0)
Bytes In	344139146 (Δ 286440251)	0 (Δ 0)
Bytes Out	41052361 (Δ 14056151)	0 (Δ 0)
Service Zone - Default	Mode	NAT
	MAC Address	00:0B:01:02:00:02
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
Service Zone - Default DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.2
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
Service Zone - SZ1	Disabled	

The description of the table is as follows:

Item		Description
WAN1	**MAC Address**	The MAC address of 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 WAN2 port.
	IP Address	The IP address of the WAN2 port.
	Subnet Mask	The Subnet Mask of the WAN2 port.
Packets In/Out		Accumulated traffic counts (in packets) of WAN1 and WAN2 since system boot up are displayed; the delta counts (current - last) are also displayed and it count and display the time during the period when page is being refresh only.
Bytes In/Out		Accumulated traffic counts (in bytes) of WAN1 and WAN2 are displayed; the delta counts (current - last) are also displayed and it count and display the time during the period when page is being refresh only.
Service Zone - Default	**Mode**	The mode address of the default service zone.
	MAC Address	The MAC Address of the default service zone.
	IP Address	The IP address of the default service zone.
	Subnet Mask	The Subnet Mask of the default service zone.
Service Zone – Default DHCP Server	**Status**	Enable/Disable stands for status of the build-in DHCP server on the service zone.
	WINS IP Address	The WINS server IP.
	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 service zone.
Service Zone – SZ1~SZ4	**Disabled**	Enable/Disable stands for status of the SZ1~SZ4 server on the service zone.

4.5.3 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
192.168.1.0	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 1~8:** Shows the information of the individual Policy from 1 to 8.
- **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.

4.5.4 Online Users

Each online user's information can be obtained using this function. These include **Username**, **IP Address**, **MAC Address**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out, Idle, Access From** and **Kick Out**. All online users will be listed here. The administrator can use this function to force a specific online user to log out, or terminate any user session by clicking the hyperlink of ***Logout*** button.

Online Users List

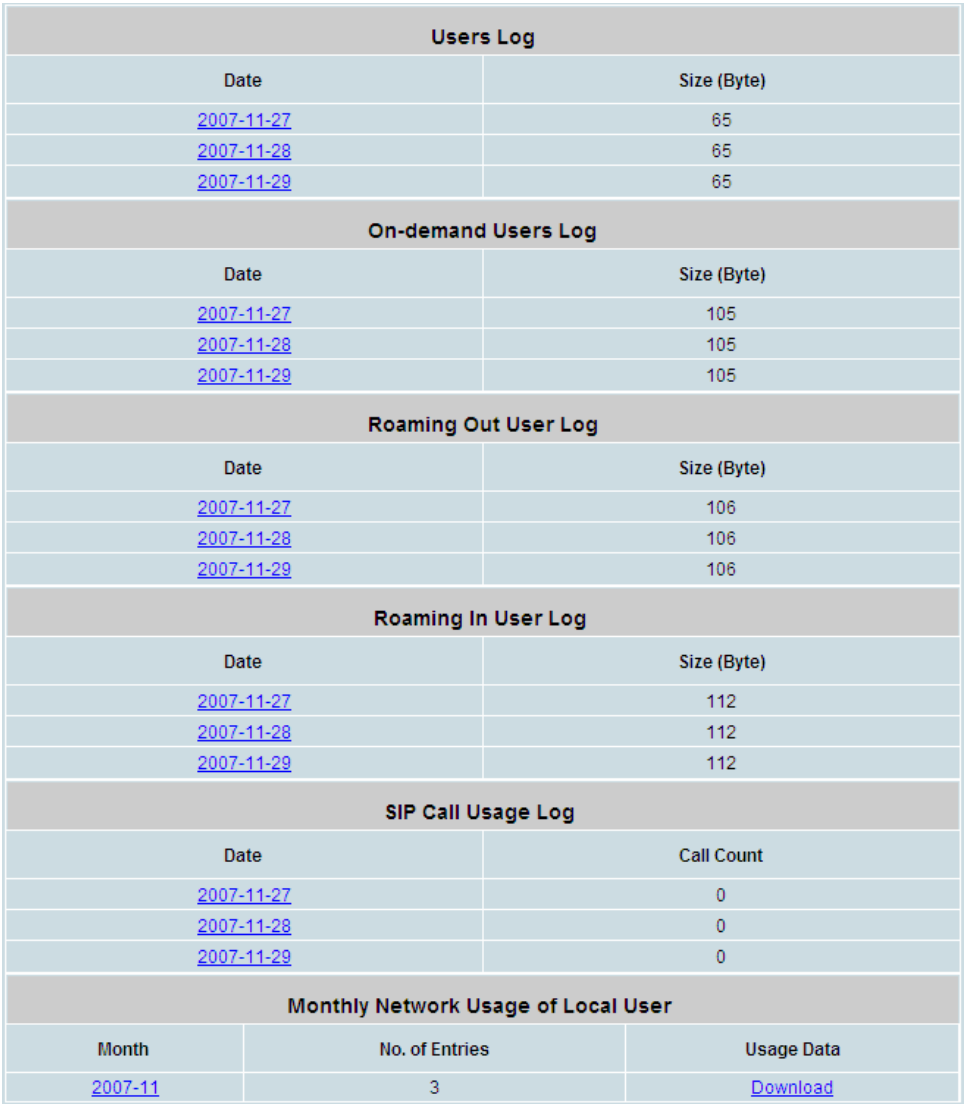
No.	Username		Pkts In	Bytes In	Idle (Sec.)	Access From
	IP Address	MAC Address	Pkts Out	Bytes Out		Kick Out
1	1@local		591	42040	0	N/A
	192.168.2.55	00:06:1B:DD:90:3C	624	82791		Logout

Click ***Refresh*** to renew the current users list.

A user may register with SIP Register after authentication. In Online User List, this user is shown as a UAM user (User Authentication Management). While monitoring online SIP users, the page should show registered SIP clients through SIP authentication.

4.5.5 User Logs

This function is used to check the history of DSA-3600. There are several types of log provided by the system. The log will be saved separately by day in the DRAM and the system supports up to 3 days. These logs are stored in volatile memory and will lose when the system is turn off.



Users Log	
Date	Size (Byte)
2007-11-27	65
2007-11-28	65
2007-11-29	65
On-demand Users Log	
Date	Size (Byte)
2007-11-27	105
2007-11-28	105
2007-11-29	105
Roaming Out User Log	
Date	Size (Byte)
2007-11-27	106
2007-11-28	106
2007-11-29	106
Roaming In User Log	
Date	Size (Byte)
2007-11-27	112
2007-11-28	112
2007-11-29	112
SIP Call Usage Log	
Date	Call Count
2007-11-27	0
2007-11-28	0
2007-11-29	0

Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
2007-11	3	Download

Caution: *Since the history is saved in the DRAM, if you need to restart the system and also keep the history, then please manually copy and save the information before restarting.*

If the **Receiver E-mail Address for System Log** has been entered under the **E-mail & SYSLOG** page, then the system will automatically send out the history information to that e-mail address.

- **Users Log**

  The **Users Log** provides users' login and logout activities except on-demand users and RADIUS roaming in/out users such as Date, Type, Name, IP address, MAC address, Packets In, Packets Out, Bytes In and Bytes Out.

Users Log 2007-08-13								
Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out
2007-08-13 14:46:51	LOGIN	user7@local	192.168.6.2	Remote	0	0	0	0
2007-08-13 14:52:56	LOGOUT	user7@local	192.168.6.2	Remote	499	350468	532	46643
2007-08-13 14:57:35	LOGIN	user7@local	192.168.6.2	Remote	0	0	0	0
2007-08-13 15:01:50	LOGOUT	user7@local	192.168.6.2	Remote	2934	1103641	2383	394180
2007-08-13 15:06:29	LOGIN	1@local	192.168.2.55	00:06:1B:DD:90:3C	0	0	0	0
2007-08-13 15:12:36	Force logout	1@local	192.168.2.55	00:06:1B:DD:90:3C	740	48180	780	103791

- **On-demand User Log**

  The On-demand User Log provides the login and logout activities of on-demand users such as Date, System Name, IP address, MAC address, Packets In, Packets Out, Bytes In, Bytes Out, 1st Login Expiration Time, and Account Valid Through.

On-demand Users Log 2007-11-03												
Date	System Name	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	1st Login Expiration Time	Account Valid Through	Remark

  - **System Name:** The system name defined in General tab of System category.
  - **Type:** The authentication status of the user.
  - **1st Login Expiration Time:** This is a constant value of one day.
  - **Account Valid Through:** This is the Expired information setting in Plan Configuration of On-demand User.
  - **Remark:** The administrator can add extra information here about each On-demand User.

- **Roaming Out User Log**

  The Roaming Out User Log provides the login and logout activities of roaming out users such as Date, Type, Name, NAS ID, NASIP, NASPORT, UserMAC, Session ID, Session Time, Packets In, and Packets Out, Bytes In, Bytes Out, Message.

Roaming Out User Log 2007-08-13												
Date	Type	Name	NASID	NASIP	NASPort	UserMAC	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

  - **Type:** The authentication and accounting type of the external RADIUS server. There is a type called Accept for authentication. There are three types of accounting, Start, Interim-update, and Stop.
  - **Name:** The user name of roaming out user.
  - **NASID:** The System ID of the system. Usually, NASID is the MAC address of the WAN port of the system.
  - **NASIP:** The IP address of the WAN port of the system.
  - **NASPort:** The port of the WAN port of the system.
  - **UserMAC:** The MAC address of the user.
  - **SessionID:** The system will give a unique Session ID to an authenticated user when he/she starts a new session.
  - **SessionTime:** The time in seconds of this session.
  - **Bytes In/Out:** The traffic amount of inbound/outbound traffic based on byte.
  - **Pkts In/Out:** The traffic amount of inbound/outbound traffic based on packet.
  - **Message:** The system response of why the client stops this session.

- **Roaming In User Log**

  The Roaming In User Log provides the login and logout activities of roaming in users.

Roaming In User Log 2007-08-13													
Date	Type	Name	NASID	NASIP	NASPort	UserMAC	UserIP	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

  - **Type:** The authentication and accounting type of the external RADIUS server. There is a type called Accept for authentication. There are three types of accounting, Start, Interim-update, and Stop.
  - **Name:** The user name of roaming in user.
  - **NASID:** The System ID of the system. Usually, NASID is the MAC address of the WAN port of the system.
  - **NASIP:** The IP address of the WAN port of the system.
  - **NASPort:** The port of the WAN port of the system.
  - **UserMAC:** The MAC address of the user.
  - **UserIP:** The IP address of the user.
  - **SessionID:** The system will give a unique Session ID to an authenticated user when he/she starts a new session.
  - **SessionTime:** The time in seconds of this session.
  - **Bytes In/Out:** The traffic amount of inbound/outbound traffic based on byte.
  - **Pkts In/Out:** The traffic amount of inbound/outbound traffic based on packet.
  - **Message:** The system response of why the client stops this session.

- **SIP Call Usage Log**

  The **SIP Call Usage Log** provides the login and logout activities SIP users such as Start Time, Caller, Callee(Receiver) and Duration(seconds). A user may register with a SIP Registrar after authentication. Their calls will be logged in SIP call history.

SIP Call Usage Log			
Start Time	Caller	Callee	Duration (seconds)
2007-08-13 14:59:07	1003@10.2.3.175	1001@10.2.3.175	29
2007-08-13 14:59:42	1001@10.2.3.175	1003@10.2.3.175	13
2007-08-13 15:00:03	1001@10.2.3.175	1003@10.2.3.175	6

  - **Start Time:** The starting time, date, year of the call.
  - **Caller:** The caller's address.
  - **Callee:** The receiver's address.
  - **Duration(seconds):** The time in seconds of the duration.

- **Monthly Network Usage of Local User**

  The **Monthly Network Usage** provides the monthly activities of local users such as Username, Connection Time Usage, Packets In, Bytes In, Packets Out and Bytes Out. 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.s

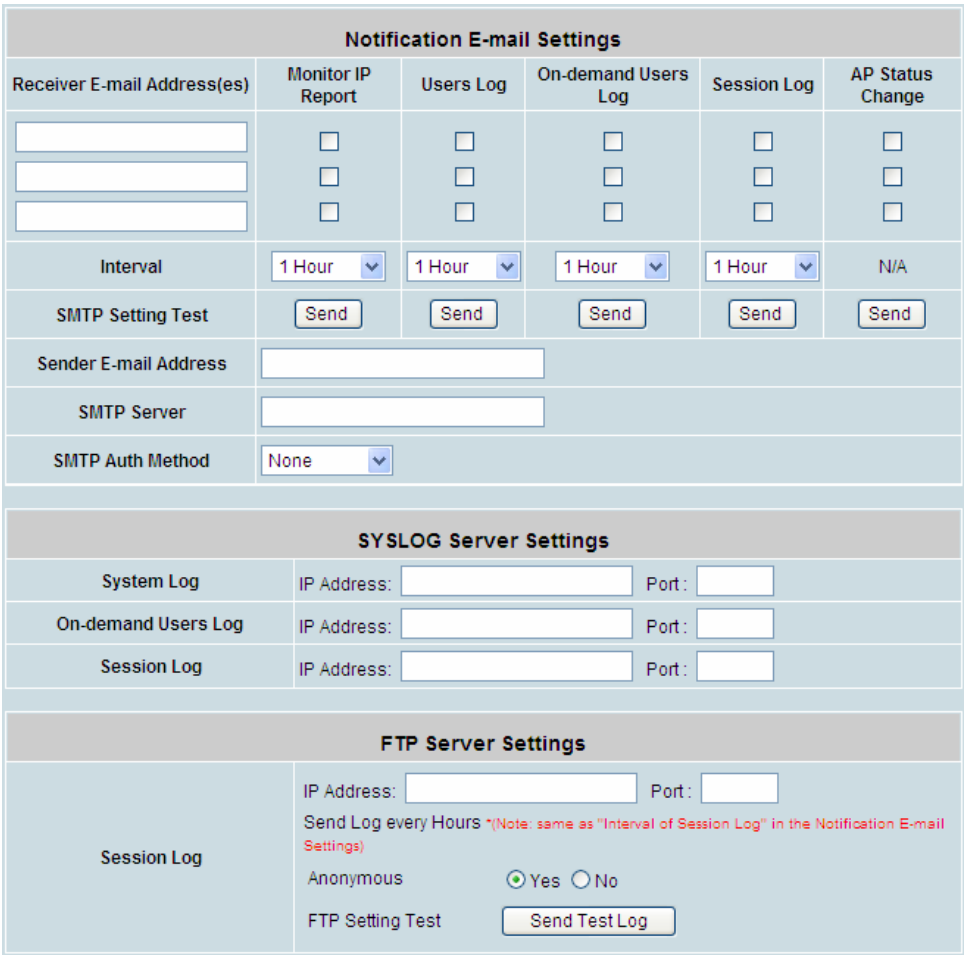
Monthly Report 2007-11

Username	Connection Time Usage	Packets In	Bytes In	Packets Out	Bytes Out
user11	7 mins 4 secs	3875	4949K	2592	162.5K
user22	6 mins 58 secs	3414	2496K	2830	374.3K
user33	2 mins 45 secs	1000	918.4K	587	80.5K

- **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.

4.5.6 E-mail & SYSLOG

The system supports sending notification e-mails of Monitor IP Report, Users Log, On-demand Users Log, Session Log and AP Status Change up to 3 email accounts automatically. The notification of AP Status Change is triggered by event when a managed AP becomes unreachable, while the other three types of e-mails are sent periodically in given intervals such as one hour. A trial e-mail is provided by the system for validation. In addition, the system supports recording SYSLOG of User Log, On-demand User Log and Session Log via external SYSLOG servers. Furthermore, the Session Log can send to a specify FTP server.



- **Notification E-mail Settings**
  - **Receiver E-mail Address(es):** The e-mail address of the person whom the history e-mail is for. This will be the receiver's e-mail. Check which type of report to be sent—Monitor IP Report, System Log, On-demand Users Log, and AP Status Change.
  - **Interval:** The time interval to send the e-mail report. Choose a proper number from the drop-down box.
  - **SMTP Setting Test:** Test if the settings is correct or not.
  - **Sender E-mail Address:** The e-mail address of the sender in charge of the monitoring.
  - **SMTP Server:** The IP address of the SMTP server.
  - **SMTP Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method you select, you have to 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 uses **Login** as default, although they can be set to use **NTLMv1**.
- Pegasus uses **CRAM-MD5** or **Login** but can not be configured which method to use.

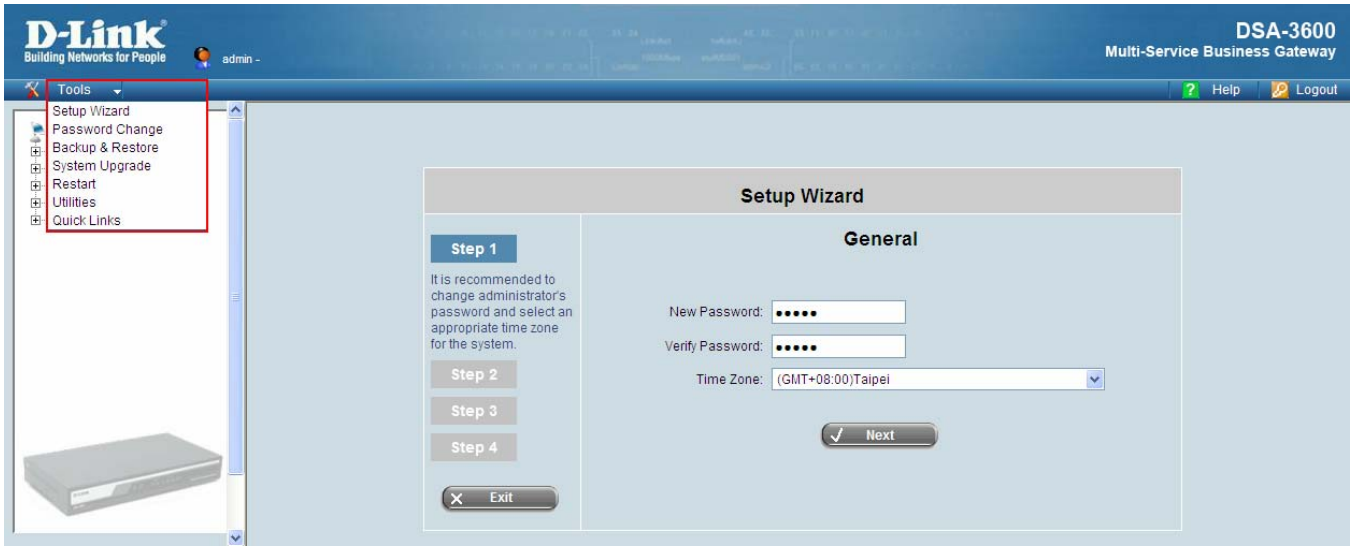
- **SYSLOG Server Settings:** There are 2 types of SYSLOG supported: System Log and On-demand Users Log. Enter the IP address and Port number to specify which and from where the report should be sent to.

Note: *When the number of a user's sessions (TCP and UDP) reaches the session limit specified in the policy, a record will be logged to this SYSLOG server. For more information about Session Limit, please refer to Appendix K.*

- **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 max size or periodical time interval.

4.6 Tools

This section provides information on utilities used for customizing and maintaining the system, including **Setup Wizard**, **Password Change**, **Backup & Restore**, **System Upgrade, Restart, Utilities,** and **Quick Links**.



4.6.1 Setup Wizard

The administrator can configure the DSA-3600 via its web management interface as specified. In order to connect to the Internet, the TCP/IP related information such as IP address, subnet mask, and gateway address, must first be obtained from the ISP. The Configuration Wizard uses four simple steps to provide easy setup of the DSA-3600.

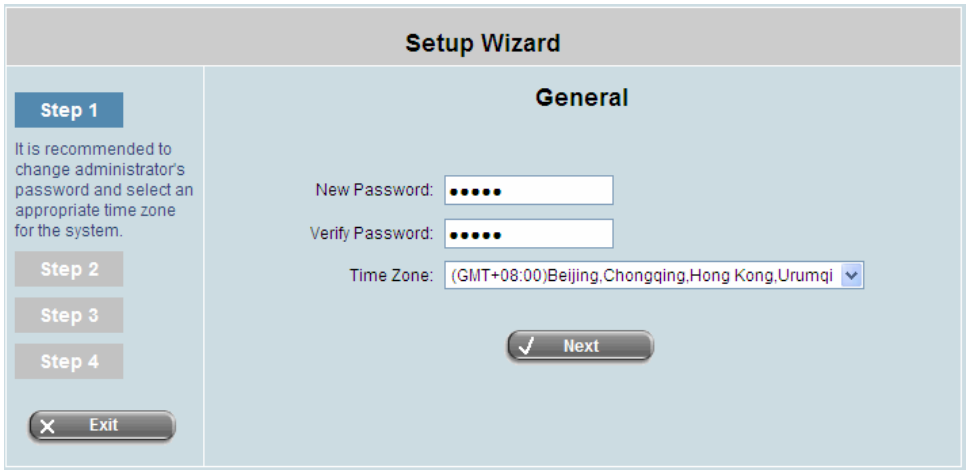
- General
- WAN1 Interface
- Local User Account (Optional)
- Confirm and Restart

The **Setup Wizard** is to provide express setup procedures for DSA-3600. Follow the instructions given at each step to change the system admin password, select time zone, configure WAN1 interface, and create local user account. Upon completing the Setup Wizard procedures, the system has to be restarted to have the setting take effort. The system is ready for operation after restart. Please refer to the Quick Install Guide of DSA-3600 if step-by-step screen images could help the process.

- **Running the Wizard**

  Click ***Tools*** and **Setup Wizard** the left-top menu, and the **Setup Wizard** page will appear.

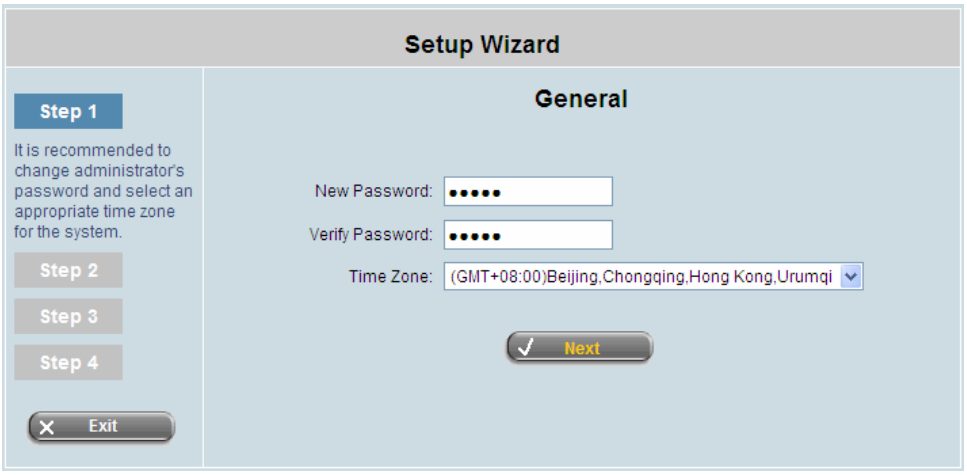
  Please read the recommendation of each step.



- **Step 1: General**

  Change Password

  Enter the administrator's **New Password** in the New Password field and retype it again in the **Verify Password** field. (Note: The maximum length of the password is twenty-character and no space is allowed.) To secure the system, changing the administration account password is recommended. Next, select a proper time zone from the **Time Zone** drop-down menu to set the system time. Click ***Next*** to continue.



- **Step 2: WAN1 Interface**

  Select the Connection Type for WAN1 Port

  Select an Internet connection type for WAN1 interface. Contact your ISP or the network administrator to make sure the connection type for WAN1. There are three connection types provided by DSA-3600: **Static**, **Dynamic** and **PPPoE**. Enter the **Username** and **Password** provided by the ISP. Click ***Next*** to continue, or click ***Back*** to change configurations in previous step.

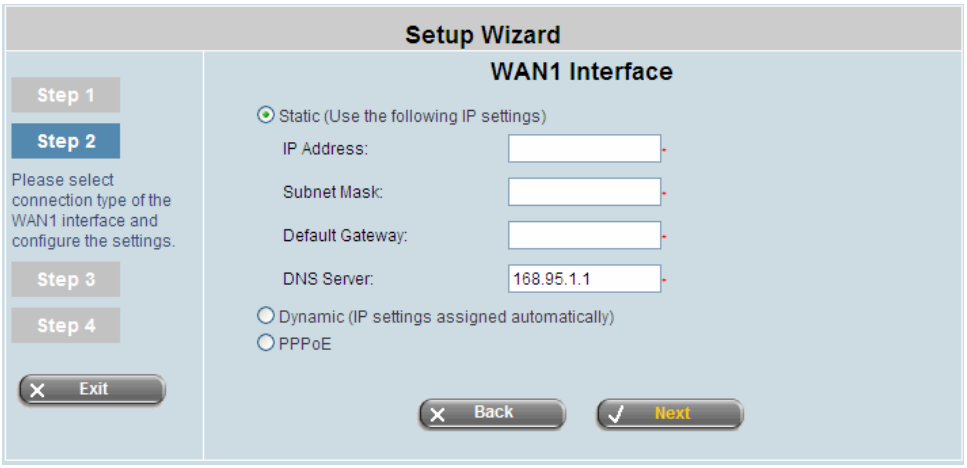
  - **Dynamic IP Address**

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

- **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.



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

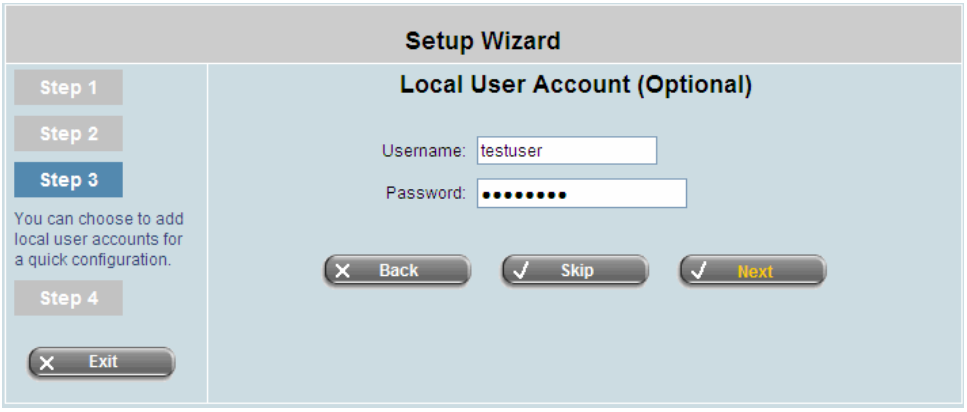
  Enter the **Username** and **Password** provided by the ISP.

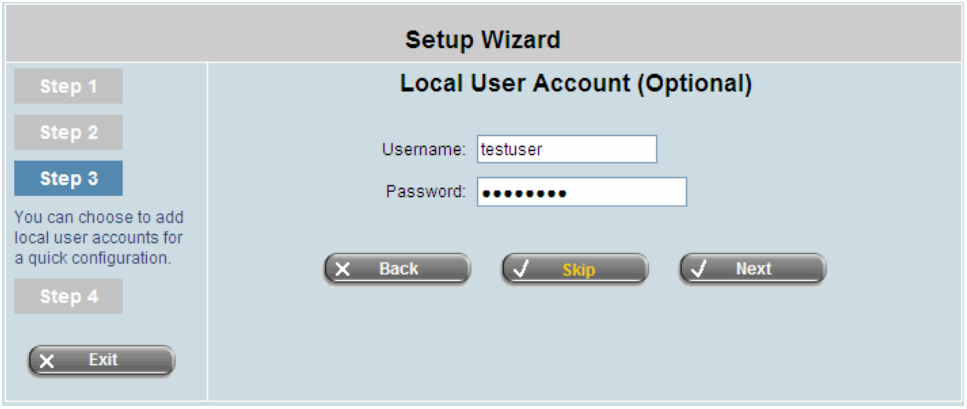
  Click ***Next*** to continue.

- **Step 3: Local User Account (Optional)**

  Local User - Add User

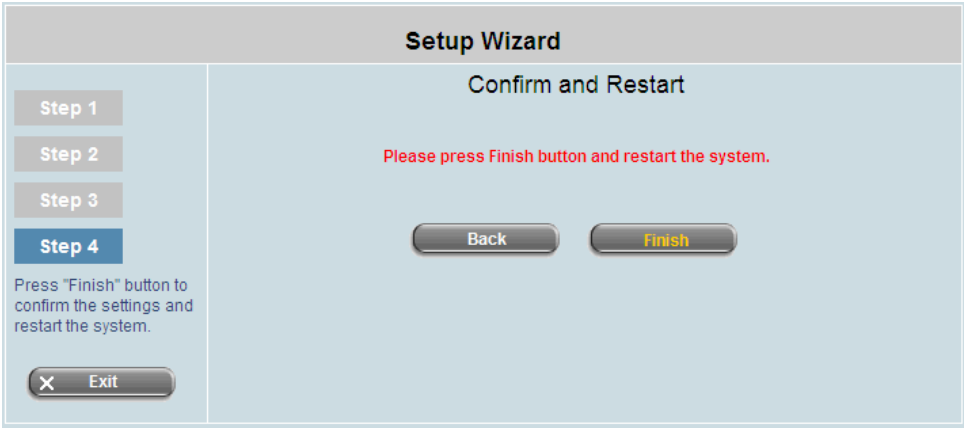
  New local accounts can be added into the local user database. Enter the **Username** (e.g. testuser) and **Password** (e.g. testuser) of the desired new account to add a new local account into the system. Click ***Skip*** to exit step 3 or click ***Next*** to validate added local accounts and continue.

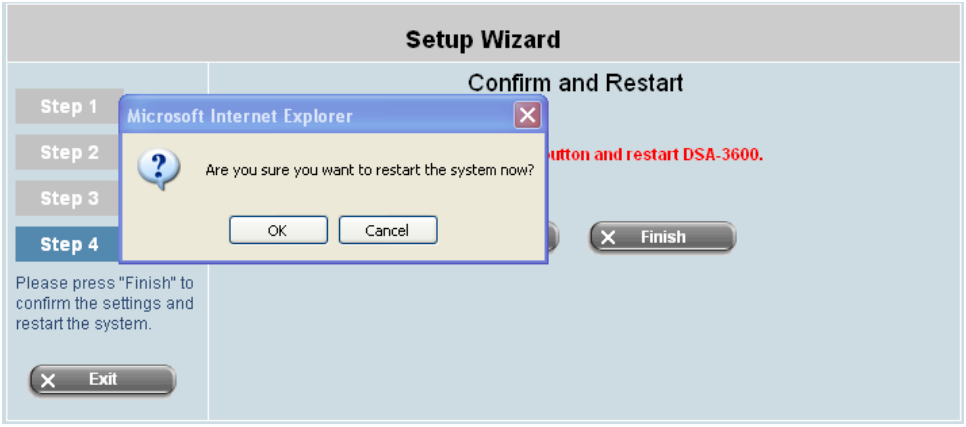




- **Step 4: Confirm and Restart**

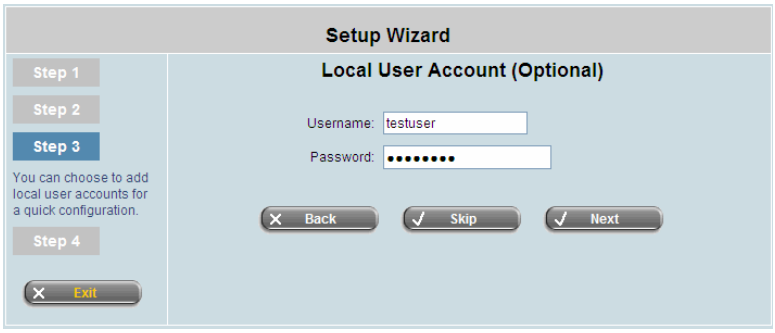
  Click ***Finish*** button to save the current settings and restart the DSA-3600. A confirming message will appear after clicking ***Finish***. Click ***OK*** to continue. The **Setup Wizard** is now completed.





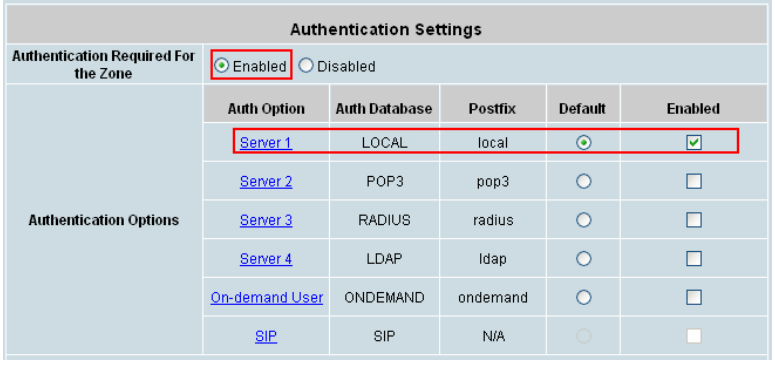
During the DSA-3600 restarting, a **Confirm and Restart** page will appear on the screen. Please do not interrupt the DSA-3600 until the DSA-3600 Administrator Login Page reappears. This indicates that the restart process has been completed.

Back and Exit: *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. Click* ***Exit*** *to leave the Wizard.*



Please Note: *Login to the web management interface again by using username "admin" and the selected password. After logged in the web management interface, click* ***System*** *and then click* ***Service Zones*** *to enter the* ***Basic Settings*** *page. Next, click the Server 1 hyperlink.*

The DSA-3600 uses Virtual LAN (VLAN) along with a SSID to separate service zones. At this stage, the system is ready for use in minimum configuration. The factory default configuration uses tag-based VLAN. The 'Default' service zone (with SSID='dlink') is enabled and requires no user authentication at this initial stage.



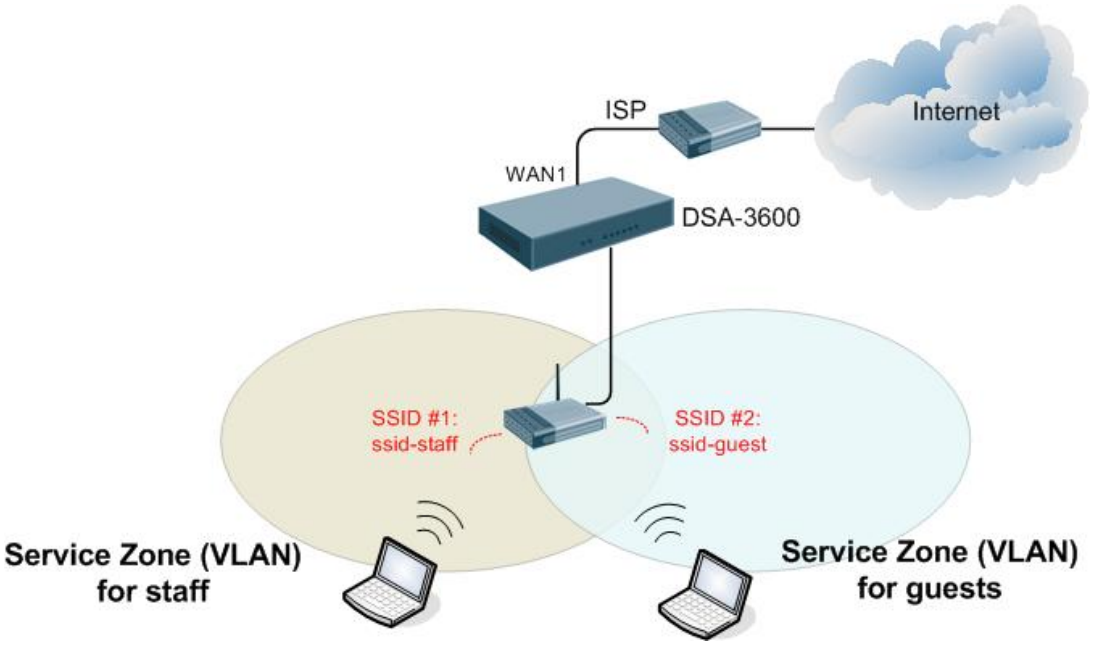


Figure-4.6.1a: An example using Tag-Based service zones

4.6.2 Password Change

DSA-3600 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 DSA-3600.

User Name: **admin**

Password: **admin**

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.

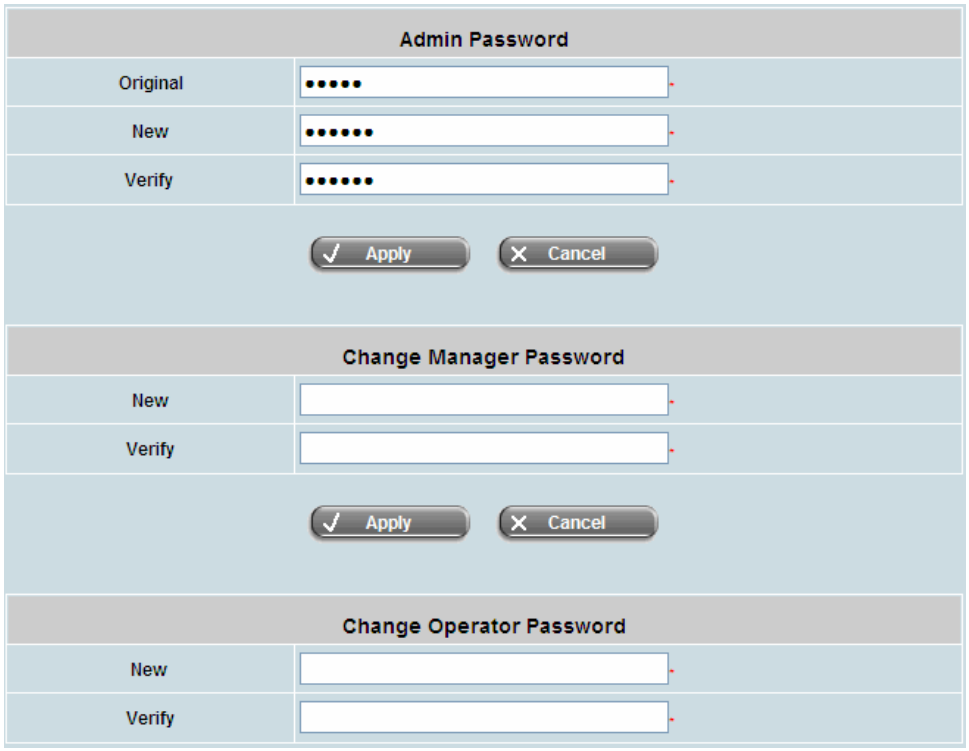
User Name: **manager**

Password: **manager**

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: **operator**

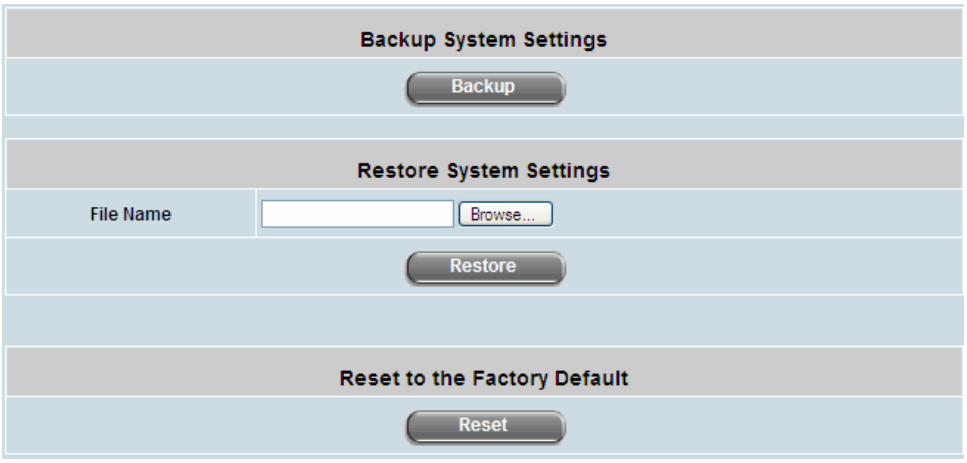


The administrator can change the passwords here. Please enter the current password and then enter the new password twice to verify. Click ***Apply*** to activate this new password.

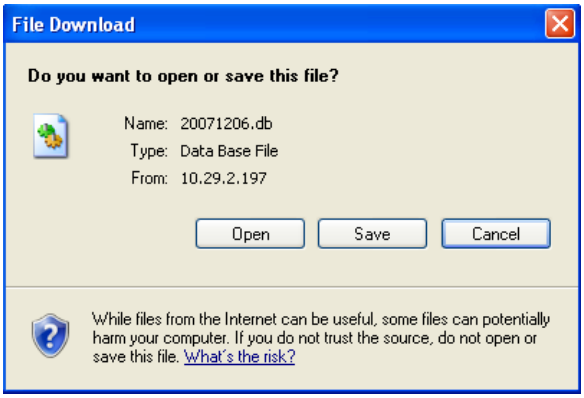
Caution: *If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port, console/printer port.*

4.6.3 Backup & Restore

This function is used to backup/restore the DSA-3600 settings. The DSA-3600 can also be restored to the factory default settings using this function.

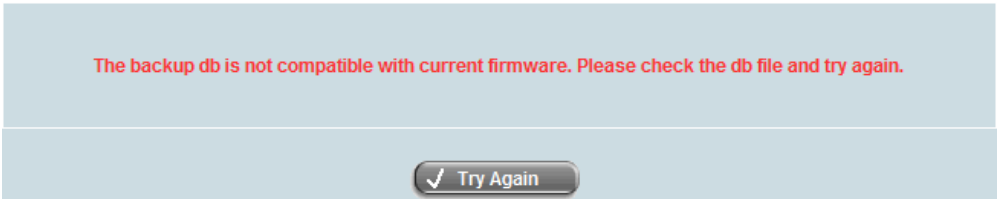


- **Backup System Setting:** Click ***Backup*** button to save the current system configurations to a backup file on a local disk of the management console. The backup file keeps the current system settings as well as the local user accounts information.

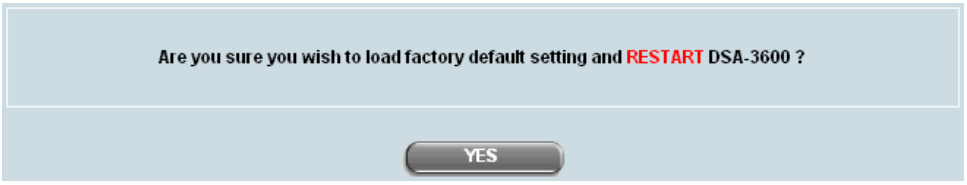


- **Restore System Settings:** Click ***Browse*** to search for a .db database backup file created by the DSA-3600 and click ***Restore*** to restore to the same settings at the time the backup file is created.

Caution: *Due to the limitation on database compatibility, the backup database file from a major release of previous firmware version cannot be restored to a later major release of current firmware - for example, a backup of v2.00 cannot be restored to v3.00. An alert will appear when the backup database file is not compatible with current firmware, as shown below.*



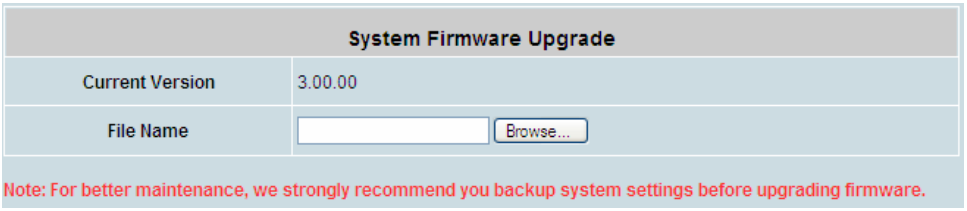
- **Reset to the Factory Default:** Click ***Reset*** to load the factory default settings of the DSA-3600.
  Note that a Reset action will wipe out the existing local user accounts. To back up the local user accounts, please export the local user accounts to a text first. Please refer to the section on **Local User List** for more details.



Caution: *Resetting to factory default settings will clear all settings, such as policies, billing plans, all user databases, and any configuration, to its initial state.*

4.6.4 System Upgrade

To upgrade the system firmware, click the ***Browse*** button to choose the new firmware file and then click ***Apply*** to execute the process. There will be a prompt confirmation message appearing to notify the administrator to restart the system upon successful firmware upgrade.



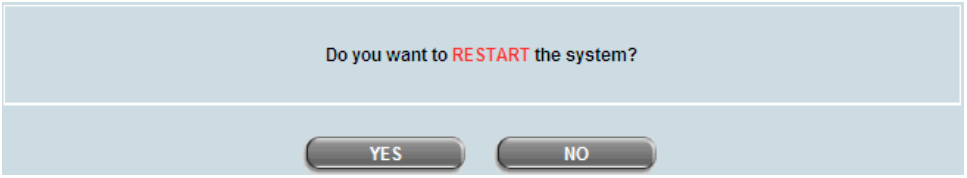
Warning: *1. Firmware upgrade may sometime result in loss of some data. Please ensure you read the release notes to understand the limitations before upgrading the firmware.*

2. Please restart the system after upgrading the firmware. Do not interrupt upgrade process such as power on/off the system during the upgrade or the restart process, as it may damage the system and cause it to malfunction.

4.6.5 Restart

This function allows the administrator to safely restart the DSA-3600. The process should take about three minutes. Click ***YES*** to restart the DSA-3600; click ***NO*** to go back to the previous screen. If turning off the power is necessary, restart the DSA-3600 and wait for it to complete the restart process before turning off.

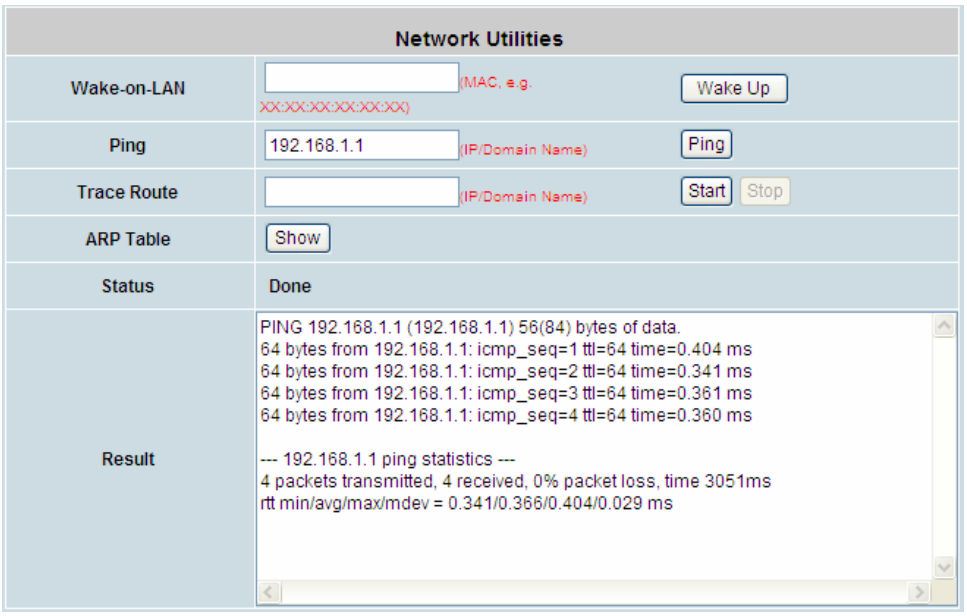
Click ***Restart*** to restart the system. Please wait for the blinking timer to finish before accessing the system web management interface again.



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

4.6.6 Utilities

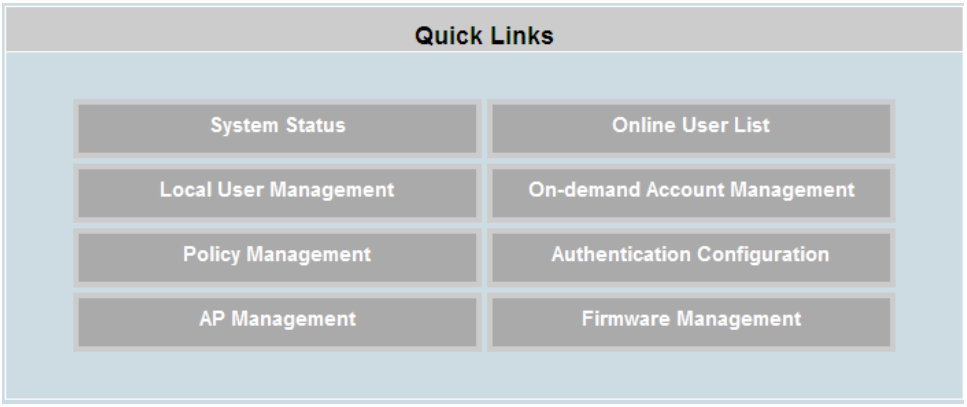
The Utilities allows the administrators to manage functions including **Wake-on-LAN**, **Ping**, **Trace Route**, and showing **ARP Table** by entering IP or Domain Name.



- **Wake-on-LAN:** It supports to boot up a power-down computer with Wake-on-LAN feature connected on the LAN side remotely from the system. Enter the MAC Address of the desired device and click Wake Up button to execute this function.
- **Ping:** The Ping function let administrator to detect a device with IP or Host domain name that it is alive or not.
- **Trace Route:** It lets administrator to find out the real path of packets from our gateway to a destination with IP or Host domain name that it will show all the nodes between gateway and destination.
- **ARP Table:** It lets administrator to view all the IP address and MAC address the device has already matched together from each interface that stored in gateway.

4.6.7 Quick Links

The **Quick Links** provide the shortcut to eight links for administrators to directly access frequently used functions of the web management interface. The eight functional links are: **System Status**, **Local User Management**, **Policy Management**, **AP Management**, **Online User List**, **On-demand Account Management**, **Authentication Configuration** and **Firmware Management**.



Link 1. System Status

The System Status quick link provides at a glance, the **System Setting Overview**, a shortcut to **4.5.1 System** in **Status** section. It provides a summary of system information to the administrator in a single page. Please refer to the section on System for details.

System Setting Overview		
Firmware Version		3.00.00
Build		03000
System Name		DSA-3600
Homepage Redirect URL		http://www.dlink-intl.com/
SYSLOG Server - System Log		N/A:N/A
SYSLOG Server - On-demand Users Log		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Load Balancing		Disabled
SNMP		Disabled
User Logs	Retained Days	3 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
System Time	NTP Server	tock.usno.navy.mil
	Time	2007/11/29 15:13:23 +0800
User Session Control	Idle Time Out	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A

Link 2. Online User List

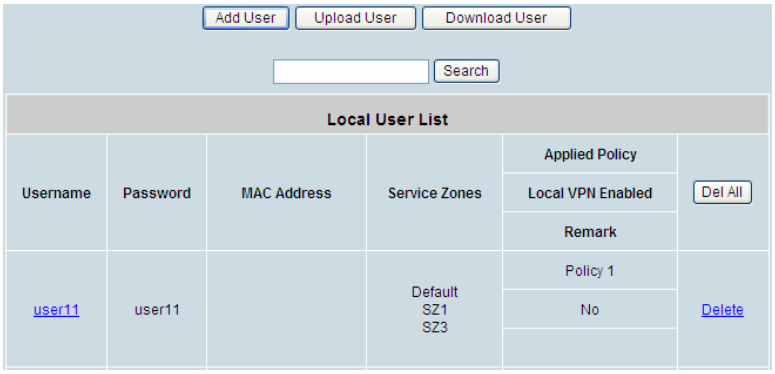
Online Users List provides information from the **Users List**, a shortcut to **4.5.3 Online Users** in **Status** section. This list provides to the administrator at a glance all the users online for easy termination of any user session. Please refer to the section on Online Users for details.

Online Users List						
No.	Username		Pkts In	Bytes In	Idle (Sec.)	Access From
	IP Address	MAC Address	Pkts Out	Bytes Out		Kick Out

Refresh

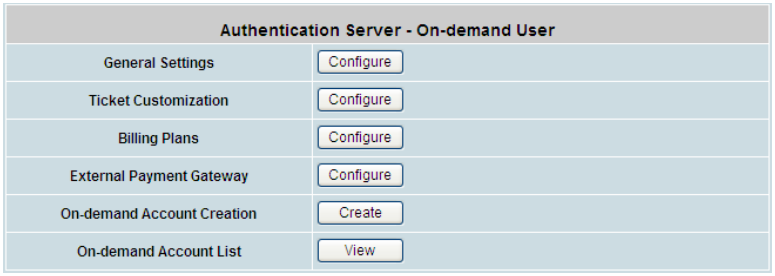
Link 3. Local User Management

Local User Management provides information from the **Local User List**, a shortcut to **4.3.1 List** in **Access Points** sections and **4.1.6 Service Zone→Authentication Settings** as well as **Authentication database→Local** in **System**. It lets the administrator add supported APs from Discovery or from the Adding menu tab, reboot, disable, and delete managed APs, and apply template. Please refer to the section on Local User List for details.



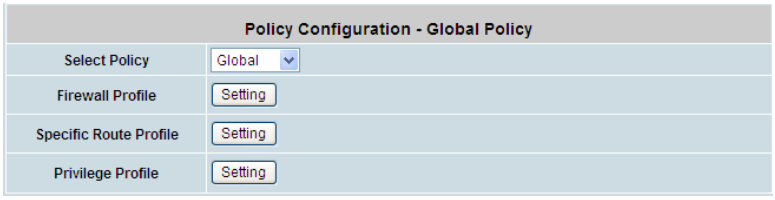
Link 4. On-demand Account Management

On-demand Account Management provides information from the **On-demand Account Configuration**, a shortcut to **4.2.1 Authentication** in **Users** sections and **4.1.6 Service Zone → On-demand User**. It lets the customers use wireless Internet with username and password from retail environment for access. Please refer to the section on On-demand Account Configuration for details.



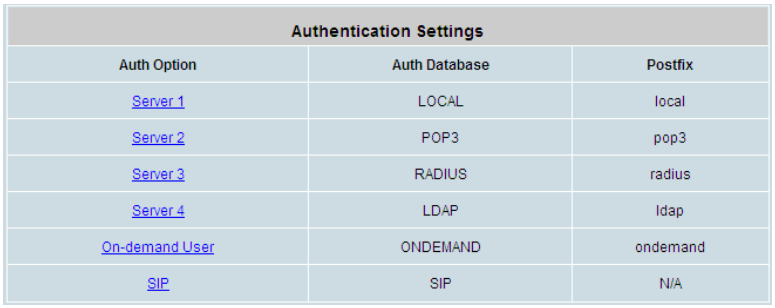
Link 5. Policy Management

Policy provides information from the **Policy Configuration**, a shortcut to **4.2.3 Policy** in **Users** sections. It lets the administrator select one of the defined policies to apply to specific authentication option. Please refer to the section on Policy Configuration for details.



Link 6. Authentication Configuration

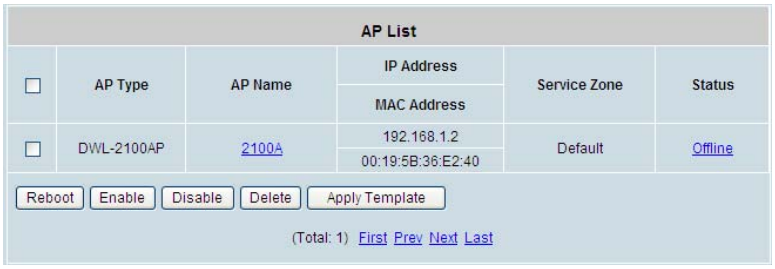
Authentication Configuration provides information from the **Authentication Settings**, a shortcut to **4.2.1 Authentication** in **Users** sections and **4.1.6 Service Zone: Authentication Settings** . It lets the administrator configure a list of authentication options which can be enabled or disabled within each service zone's management. Please refer to the section on Authentication for details.



Authentication Settings		
Auth Option	Auth Database	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

Link 7. AP Management

AP Management provides information from the **AP List**, a shortcut to **4.3.1 List** in **Access Points**. It lets the administrator add supported APs from Discovery or from the Adding menu tab, reboot, enable, disable, delete the managed APs, apply template or apply service zone. Please refer to the section on AP List for details.



AP List

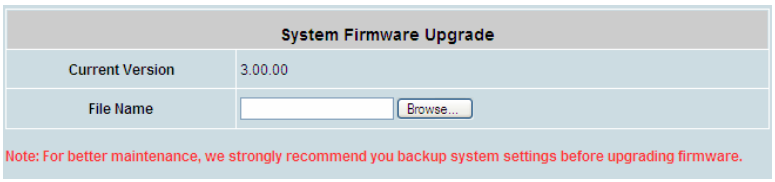
☐	AP Type	AP Name	IP Address / MAC Address	Service Zone	Status
☐	DWL-2100AP	2100A	192.168.1.2 / 00:19:5B:36:E2:40	Default	Offline

Reboot | Enable | Disable | Delete | Apply Template

(Total: 1) First Prev Next Last

Link 8. Firmware Management

Firmware Management provides information from the **System Firmware Upgrade**, a shortcut to **4.6.5 System Upgrade** in **Tools**. It lets the administrator download the latest firmware from the website and upgrade the system. Please refer to the section on System Upgrade for details.



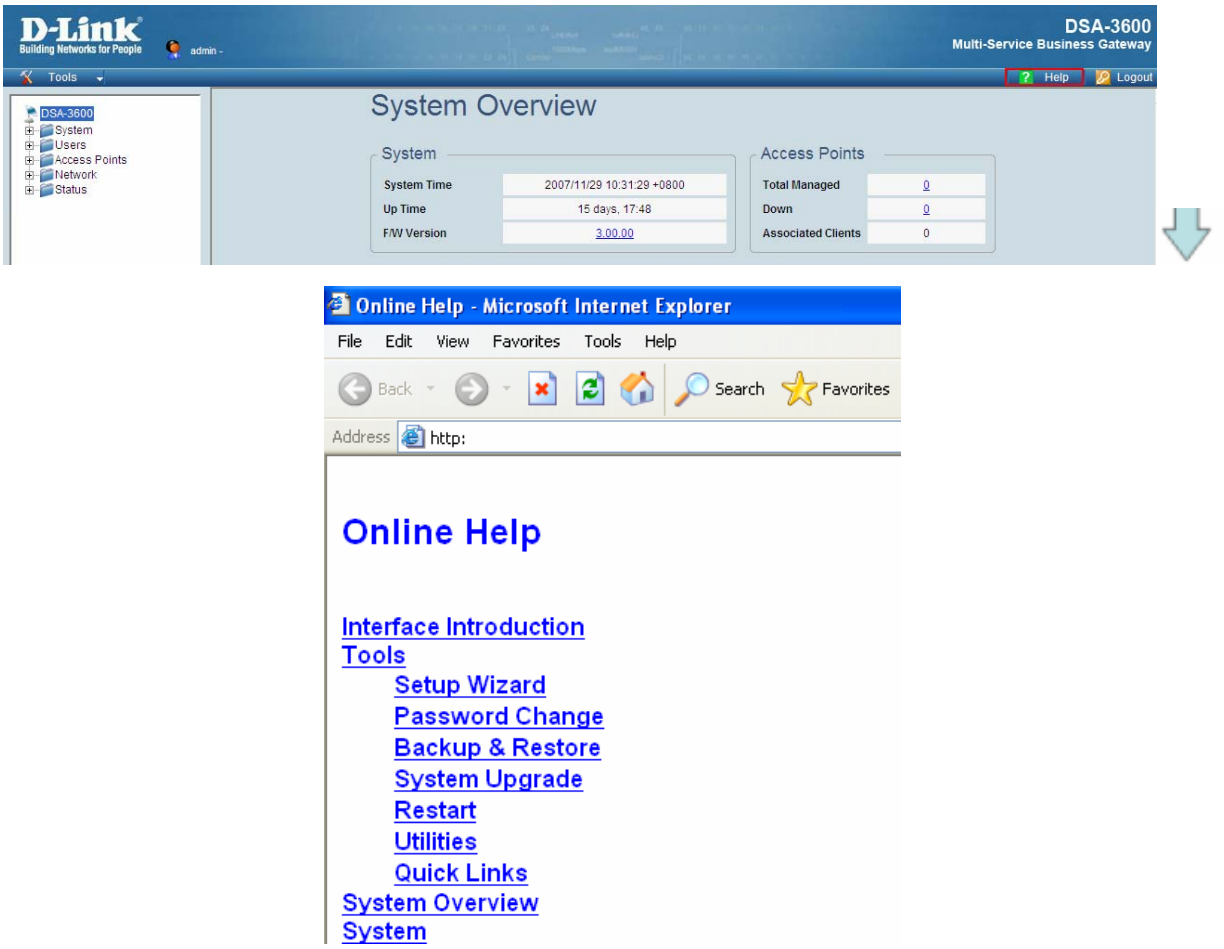
System Firmware Upgrade	
Current Version	3.00.00
File Name	Browse...

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

4.7 Help

The **Help** button is at the upper right corner of the DSA-3600 display screen.

Click ***Help*** for the **Online Help** window, then click the hyperlink of the relevant information required.



Appendix A. An Example of User Login

Normally, users will be authenticated before they get network access through DSA-3600. This section presents the basic authentication flow for end users. Please make sure that the DSA-3600 is configured properly and network related settings are finished.

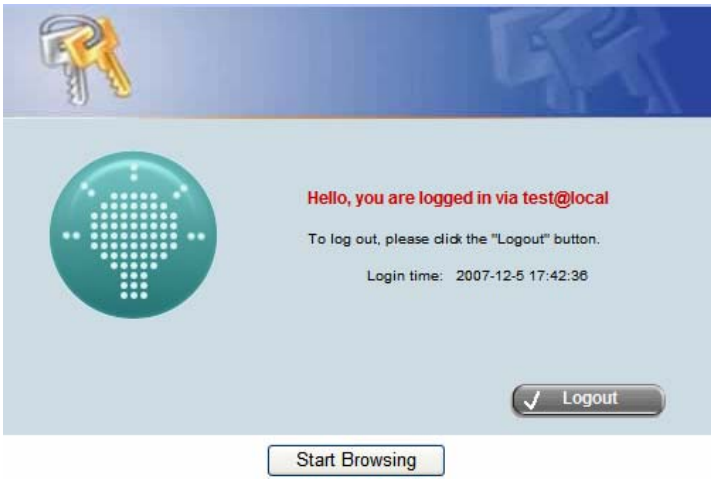
1. Open an Internet browser and try to connect to any website. The default user login page will appear in the browser.

   Enter the username and password (for example, we use a local user account: test@local here) and then click ***Login*** button.

   If wanted the computer to remember your "**Username"** and **"Password"** the next time u login in, Tick the "**Remember me"** before clicking "**Login**"

Note: *If you see the "Certificate Error", please press "Continue to this website" to continue or reference* ***Appendix D. Certificate Settings for IE6 and IE7*** *for more information.*

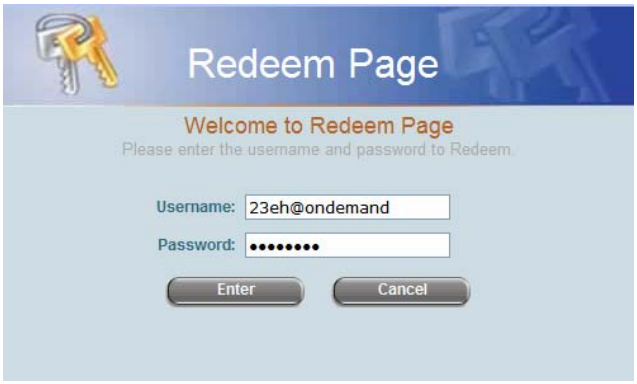
2. Successful! Now you can start using the network. The ***Start Browsing*** button will take you to the website where you originally want to visit or the home page that is configured in the system.



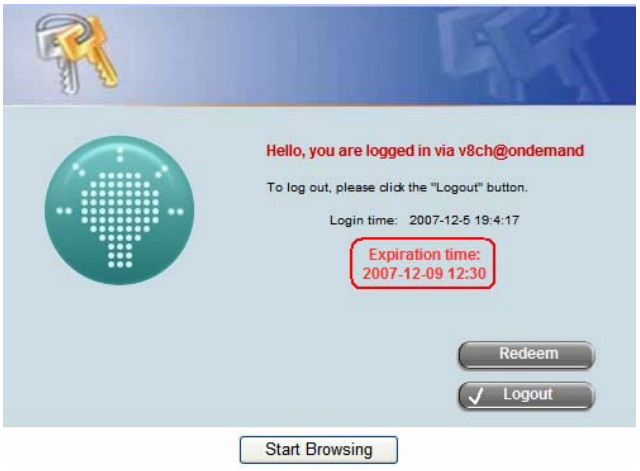
Note: *When On-demand accounts are used (for example, we use v8ch@ondemand here), the system will display additional information and function.*

(1) **Remaining usage/Expiration time:** The remaining quota of this On-demand account that the user can surf the Internet. In this example, it is an account of Cut-off type that will be expired by 2007-12-07 12:30.

(2) **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 23eh@ondemand here) and password in the Redeem Page and click ***Enter*** button to merge the two accounts.



As a result, there will be more quotas for the original account (in this case, we add up additional quota of 2 days).

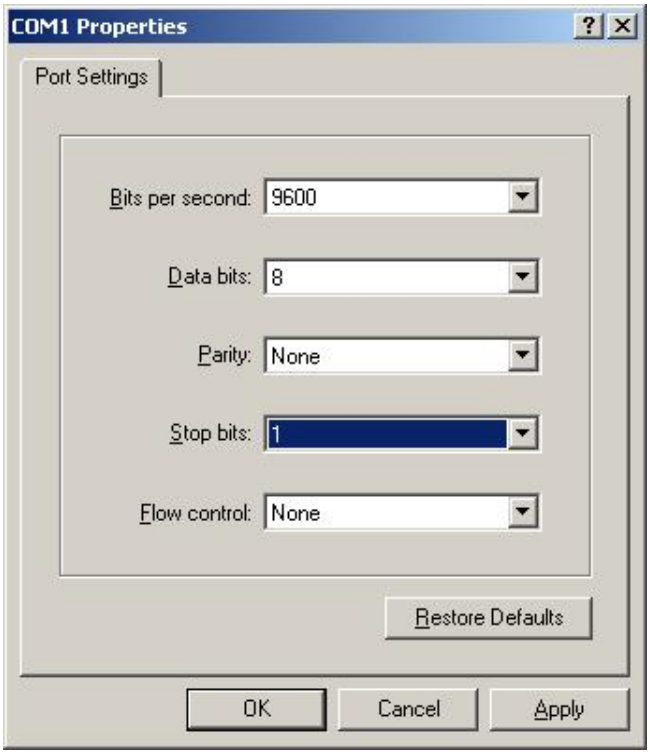


Appendix B. Console Interface Configuration

Upon completing this process, the console interface configuration will be accessible via the console port to handle problems and situations occurring during operation.

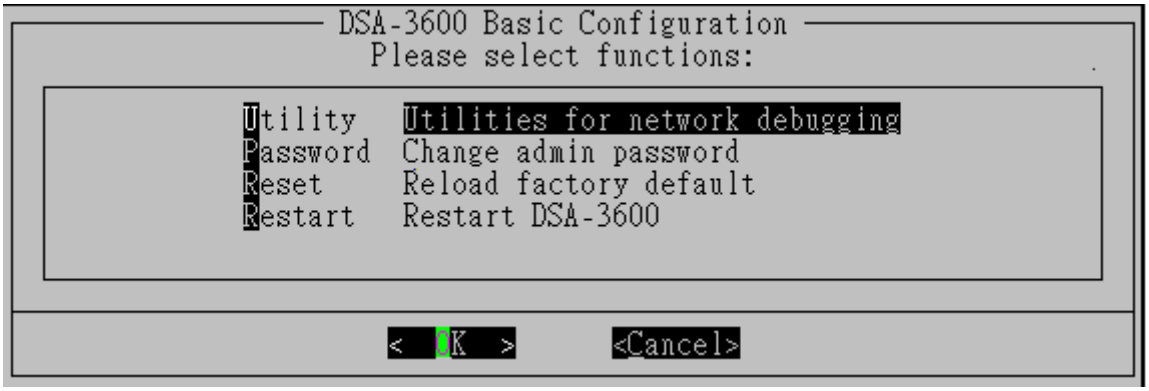
1. To connect to the console port of the DSA-3600, a console, modem cable, and a terminal simulation program such as the Hyper Terminal will be required.

2. Set the parameters as **9600, 8, n, 1** for Hyper Terminal.



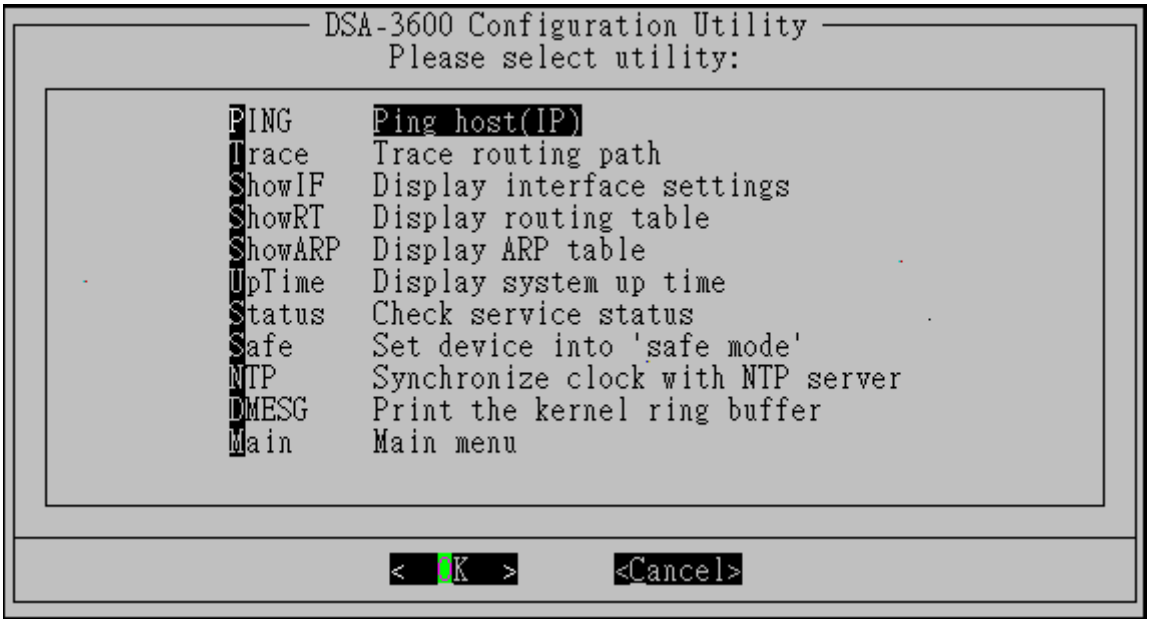
Caution: *The main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the* ***Enter*** *key to make selection or confirm what you enter.*

3. Once the console port of the DSA-3600 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, press the arrow keys of the keyboard to enable the terminal simulation program to send out some messages. The welcome screen or the main menu should then appear. If the welcome screen or the main menu of the console still does not appear, please check the connection of the cables and the settings of the terminal simulation program.



(1) Utilities for network debugging

The console interface provides several utilities to assist the administrator to check the system conditions and perform debugging. The utilities are described as following:



- 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: 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 turned on) is displayed.
- Check service status: Check and display the status of the system.
- Set device into “safe mode”: Used when the administrator is unable to access the Web Management Interface via the browser or when it fails inexplicitly. The administrator can choose this utility and set the DSA-3600 into safe mode to manage the device using a browser.
- 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, reset of internal clock can only be performed through the NTP.
- DMESG: Display the kernel ring buffer to the screen. The dmesg program helps users to print out their boot-up messages.

(2) **Change admin password**

The username and the default password is “admin” by default, which is similar to the web management interface. The administrator’s password can be changed. If the password cannot be remembered and the management interface cannot be accessed from the web or the remote end of the SSH, the console cable can still be used to connect the console management interface, where the administrator can then reset the password.

(3) **Reload factory default**

Choose this option to reset the system configuration to the factory default settings.

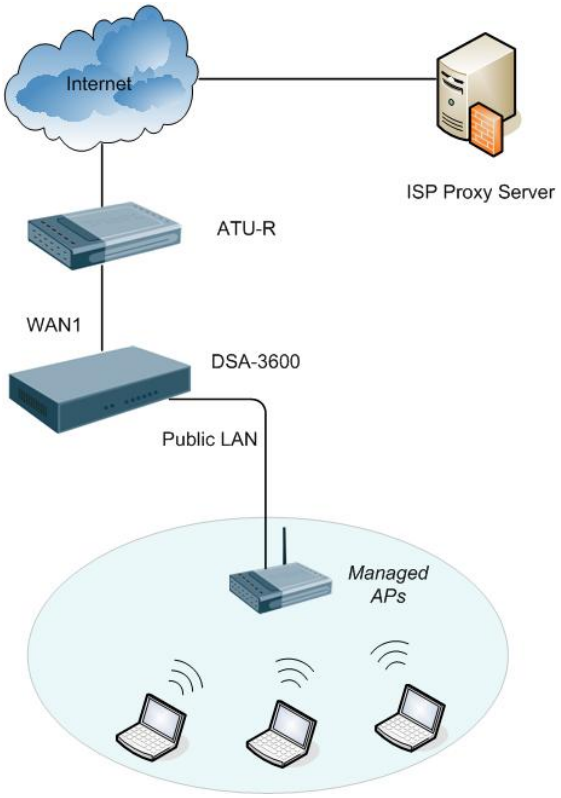
(4) **Restart the DSA-3600**

Appendix C. Proxy Configuration

Basically, a proxy server can help clients access the network resources more quickly. This section presents basic examples for configuring the proxy server settings of the DSA-3600.

▪ Using Internet Proxy Server

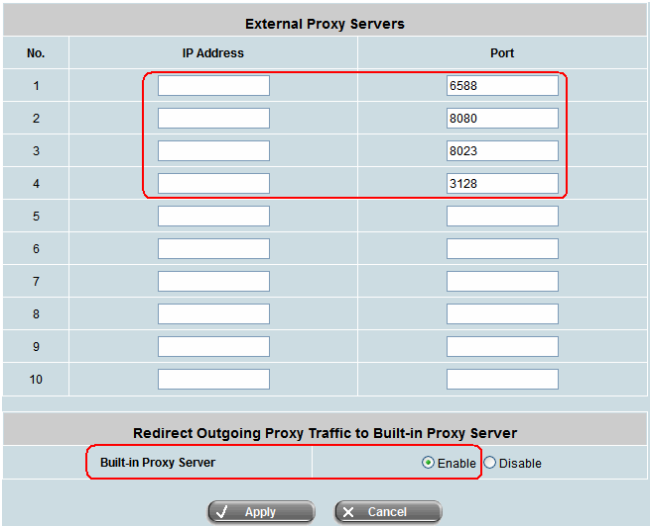
The first scenario is that a proxy server is placed outside the LAN environment or in the Internet. For example, the following diagram shows that a proxy server of an ISP will be used.



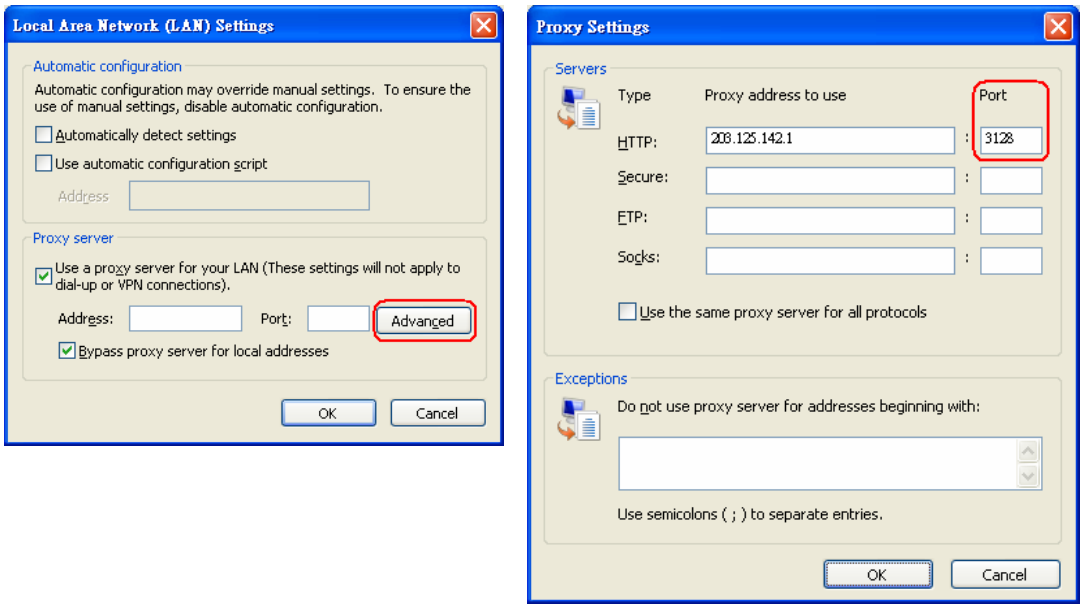
Follow the following steps to complete the proxy configuration:

Step 1. Log into the DSA-3600 by using the ***admin*** account.

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



Step 3. Make sure that the proxy server settings match with at least one of the proxy server setting of the DSA-3600 – for example, in this case, 203.125.142.1:**3128** matches with blank:**3128**.



Note:

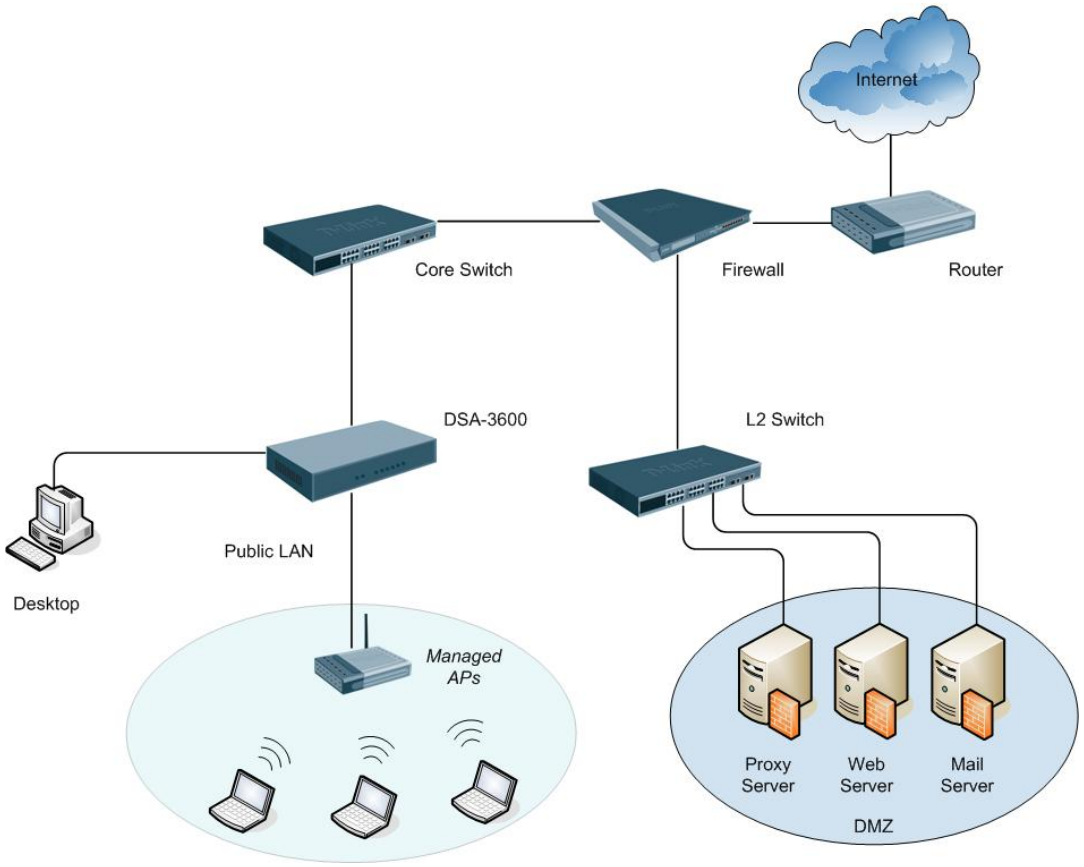
1. *It is required that the proxy server setting of the clients match with at least one of the proxy server setting of the DSA-3600. Otherwise, users will not be able to get the Login page for authentication via browsers and it will show an error page in the browser.*

2. *When the* ***Built-in Proxy Server*** *is enabled, all the outgoing proxy requests will be processed by the built-in proxy server. This will be useful when the specific proxy servers of clients are not listed in the* ***External Proxy Servers***

setting.

▪ Using Extranet Proxy Server

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

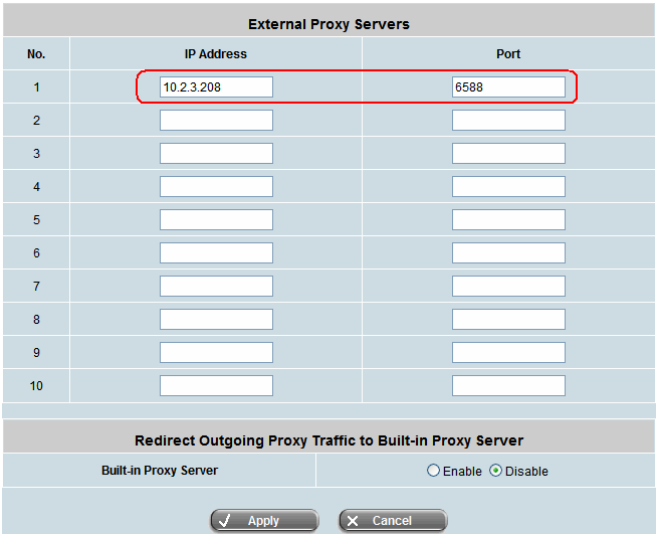


Note: *A special scenario is that a proxy server is placed in a zone like Intranet – where users can reach each other without going through the DSA-3600. In this case, whenever any one of users in the Intranet has been authenticated and connects to the network via the proxy server, other users using the same proxy setting in their browsers will be able to access the network without any authentication. Therefore, to stop the risk, it is strongly recommended to put all proxy servers outside the Intranet.*

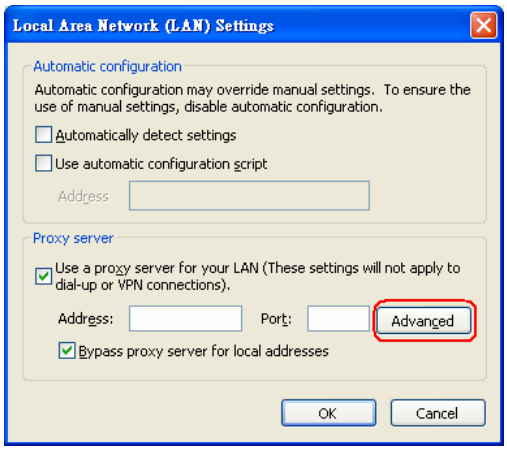
Follow the following steps to complete the proxy configuration:

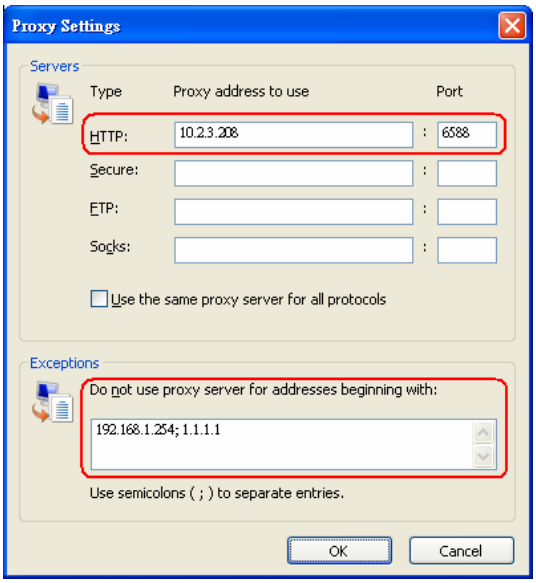
Step 1. Log in the DSA-3600 by using the ***admin*** account.

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



Step 3. Make sure that clients use the same proxy server settings. Please also configure appropriate exceptions if there is any traffic which is not needed to go through proxy server – for example, there is no need to use proxy server for the Default Gateway (192.168.1.254).





Note: *It is required that the proxy server setting of the clients match with the proxy server setting of the DSA-3600. Otherwise, users will not be able to get the Login page for authentication via browsers and it will show an error page in the browser.*

Appendix D. Certificate Settings for IE6 and IE7

▪ Certificate setting for the company with Certificate Authority

➢ Background information

Any website or high-value Web Applications will require a client to access their websites via Secure Sockets Layer (SSL). The browser will automatically ask for a public SSL certificate from the website and check if it is valid. The public SSL Certificate consists of the public key and identity information which can be signed by any established certificate authority (e.g. VeriSign). The certificate authority guarantees that the public key belongs to the named entity. Usually, website's security certificate may encounter problem only if the security certificate presented to the browser has not been signed by any certificate authority which can be trusted.

As long as the SSL function is enabled in the DSA-3600, there must be a public SSL certificate signed by an established certificate authority. To avoid the error message in the browser, a company should have its own Certificate Authority (CA). The IT department must therefore install the SSL certificate for each normal user when deploying the DSA-3600.

➢ Secure Certificate setting for both IE6 and IE7

For the company with its own Certificate Authority (CA), the certificate of the company should be trusted by all his employees' computers, and the certificate should be delivered through a trusted media. For example, the MIS staff should install the CA certificate in each computer. The company CA will issue a certificate for the DSA-3600 and export it to the DSA-3600.

Note: *If the DSA-3600 is installed in a company, the administrator can create a certificate using software instead of purchasing a public trusted certificate.*

▪ Certificate setting for the company without Certificate Authority

For a company that does not have it own Certificate Authority (CA), the administrators should first apply for a trusted certificate, or create one by using certificate software. Second, the administrators should use some trusted media to install this certificate (as trusted CA) in each employee's computer, and in the meantime export this certificate to the DSA-3600.

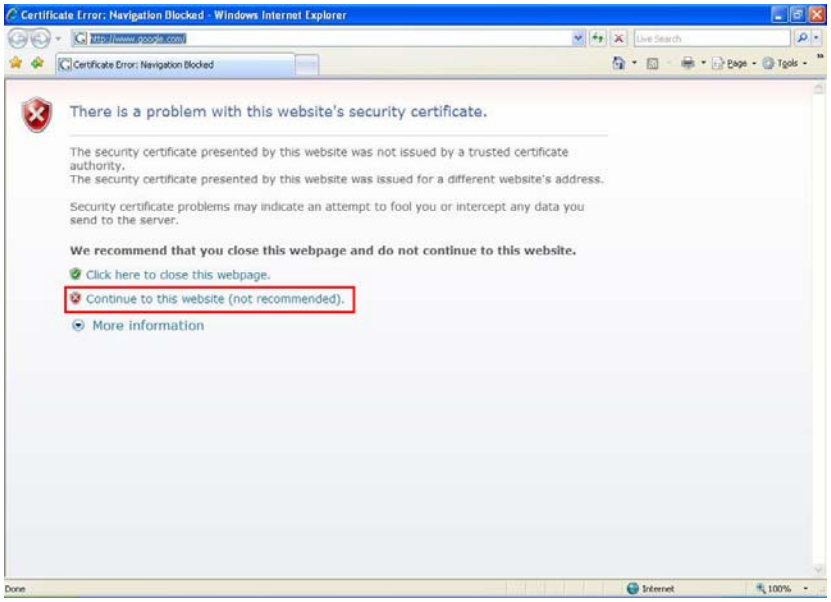
In some circumstance, the company without Certificate Authority may follow the steps stated below to avoid error message. When in the LAN environment of the office instead of a wireless environment, administrators may already have recognized certificates in the system which the CA must be verified as secured.

▪ Certificate setting for Internet Explorer 7

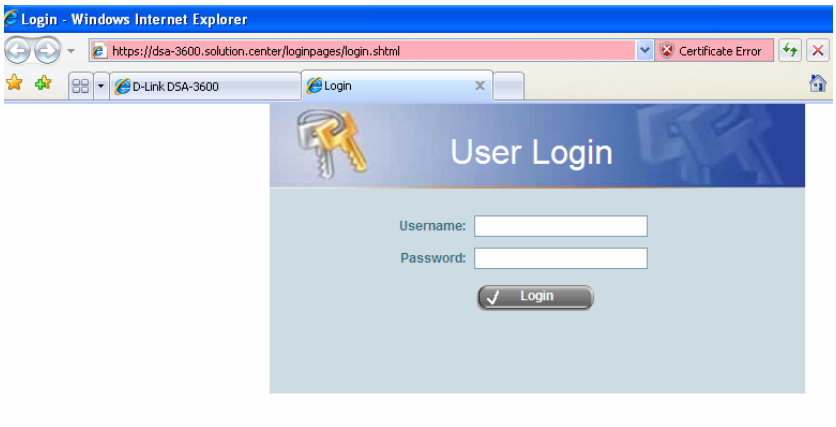
For IE7, certificate issues caused by certificate publisher not being trusted by IE7, the following steps may be taken to provide a workaround or to bypass the issue.

(1) Open the IE7 browser, and you will be redirected to the default login page. If the certificate is not trusted, the following page will appear.

Click ***"Continue to this website"***.

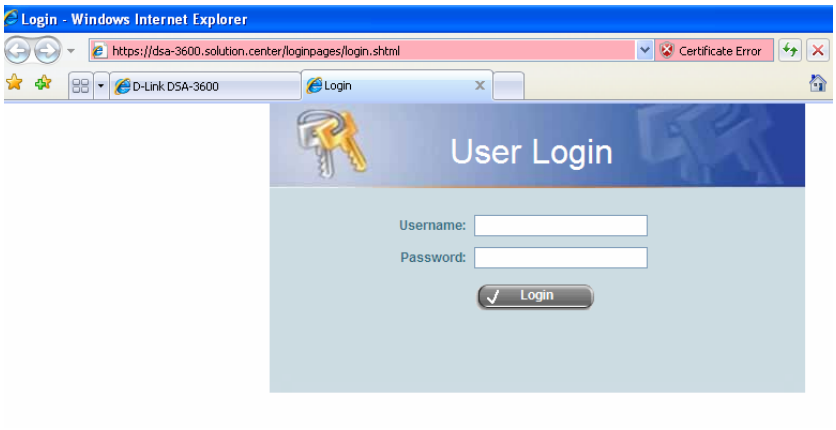


(2) The default User Login Page will appear and the users can then login normally.

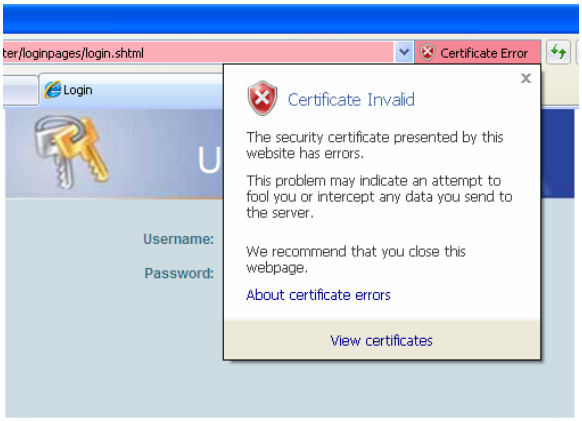


For installing a trusted certificate to solve the IE7 certificate issue, please follow the instructions stated below.

(1) When the User Login page appears, click ***"Certificate Error"*** at the top.



(2) Click ***"View Certificate"***.

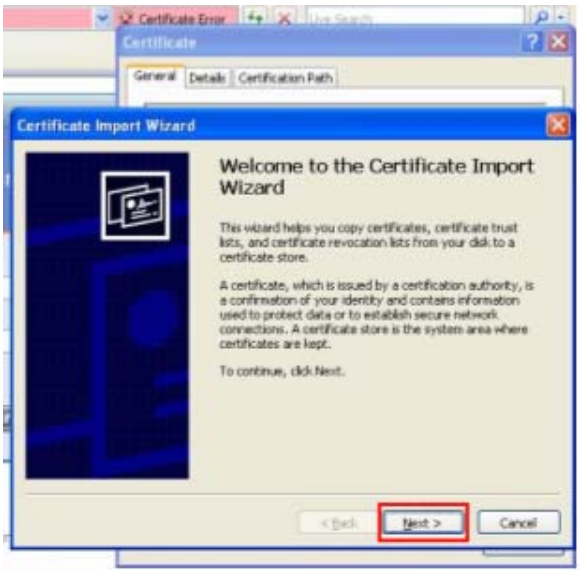


(3) Click ***"Certification path"***.

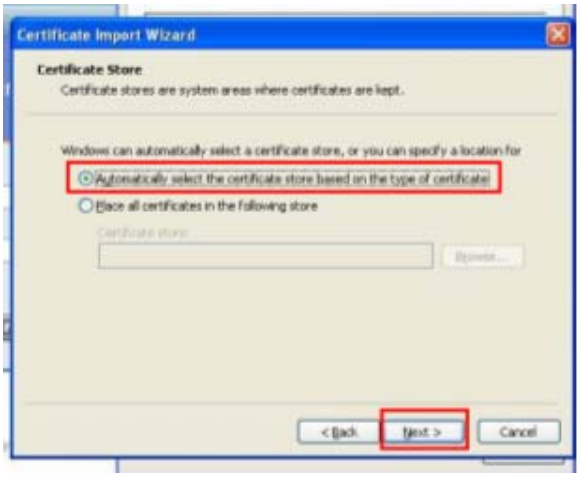
(4) Select root certification, then click ***"View Certificate"***.

(5) Click ***"Install Certificate"***.

(6) Click ***"Next"***.

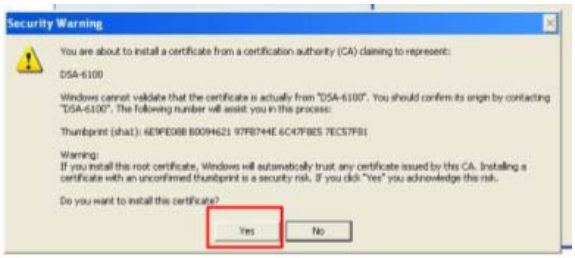


(7) Select ***"Automatically select the certificate store based on the type of certificate"***, then click ***"Next"***.



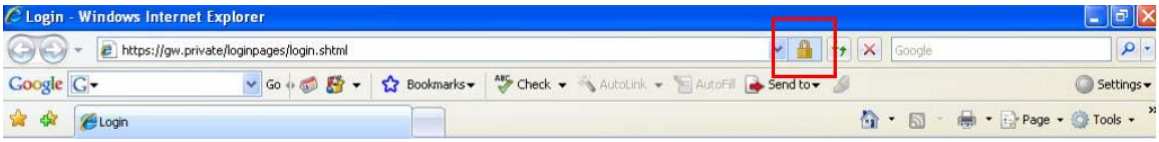
(8) Click ***"Finish"***.

(9) Click ***"Yes"***.



*(10)*Click ***"OK"***.

*(11)*Launch a new IE7 browser. The certificate is now trusted via IE7 according to the key symbol shown at top next to the address field.



▪ Certificate setting for Internet Explorer 6

For issues relating to IE6 certificate error, the following information provides the step to take when the certificate publisher is not trusted by IE6.

(1) Open an IE6 browser, the Security Alert message will be appeared if the certificate is not trusted. Click ***"Yes"*** to proceed.

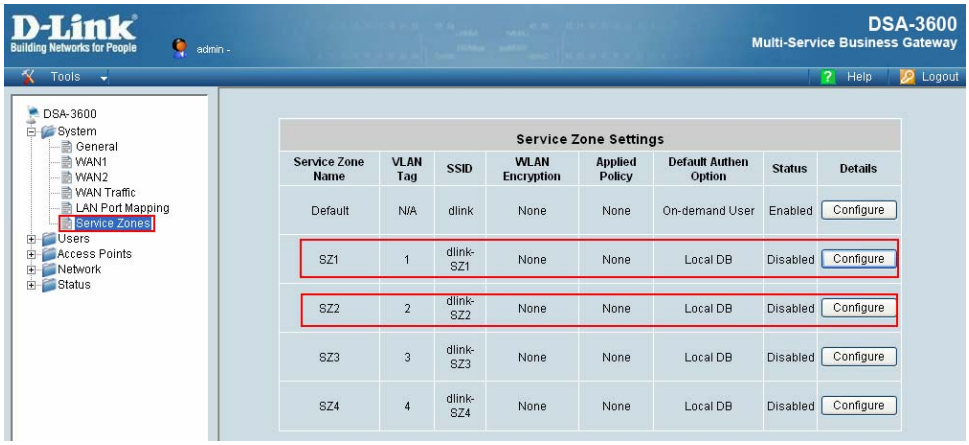
(2) The User Login Page will appear.

(3) The user can now login normally.

Appendix E. Service Zones – Deployment Examples

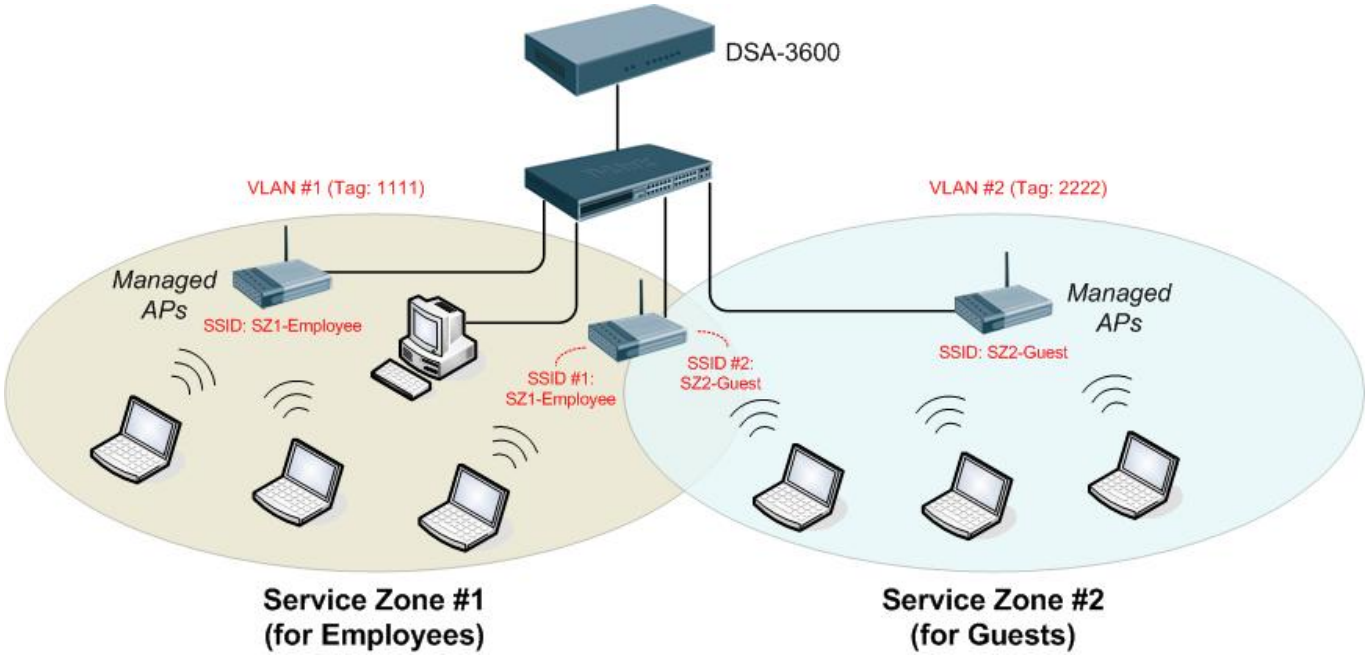
▪ Typical Application Scenario: Employees vs. Guests

Typical service zone settings will separate users groups into **Employee** and **Guests** for the purpose of different authentication level.



➢ Application Network Diagram:

As shown in the diagram, assign service zone 1 to Employees and service zone 2 to Guest.



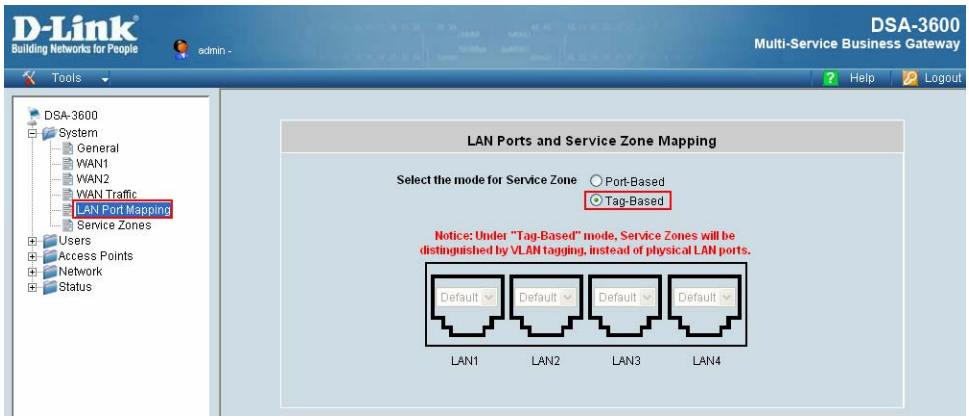
➢ Requirements for the Application Scenario :

1. Regardless of the location 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 ID. The system will give a unique Session ID to authenticated users when they start new sessions.
3. Both groups, **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 separated groups **Employee** and **Guests**.

▪ Solution and Configuration in DSA-3600

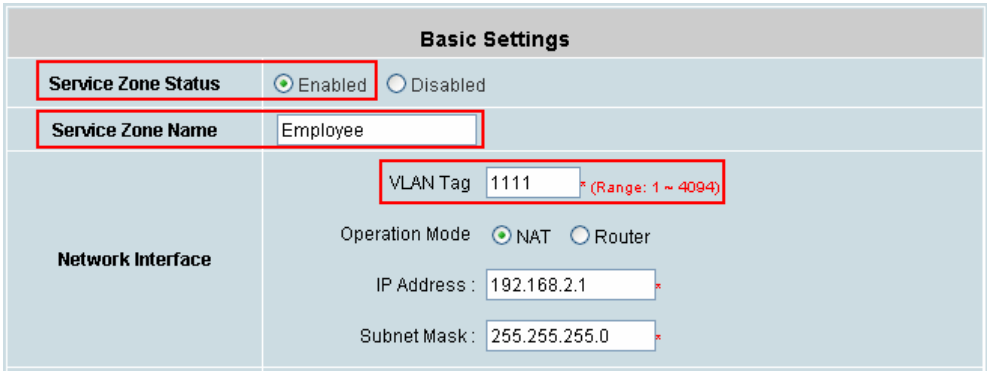
➢ Configure two **service zones** to map to the two groups

Step 1: Select "**Tag-Based mode**" for all "**service zones**"

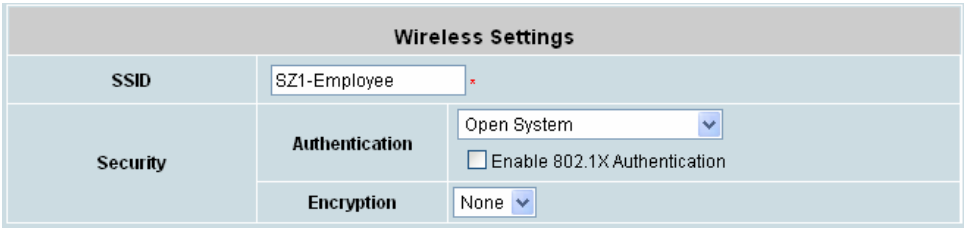


Step 2: Choose and configure the desired "**service zone**" for the specific group (e.g. Choose and configure " **SZ1**" for **Employees**)

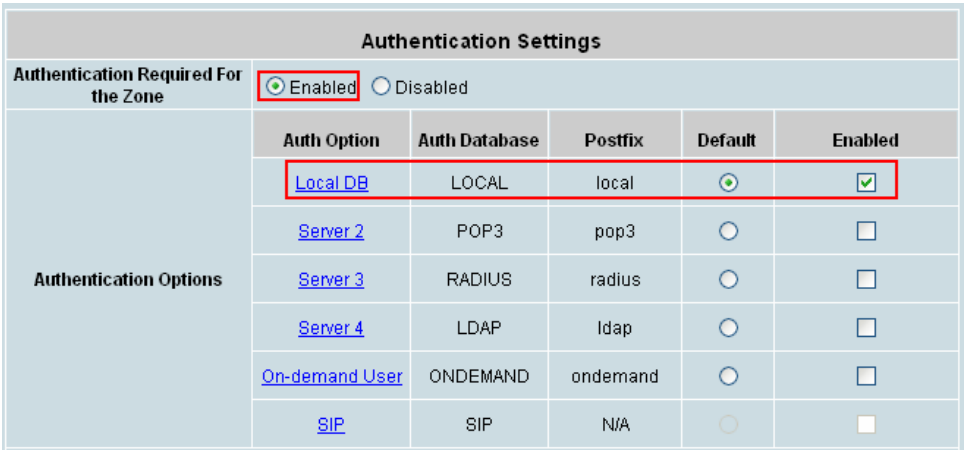
Step 3: Configure the "**service zone**" accordingly



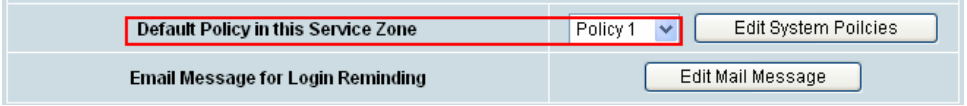
➢ Configure the **SSID**



➢ Choose the authentication option and configure the login page

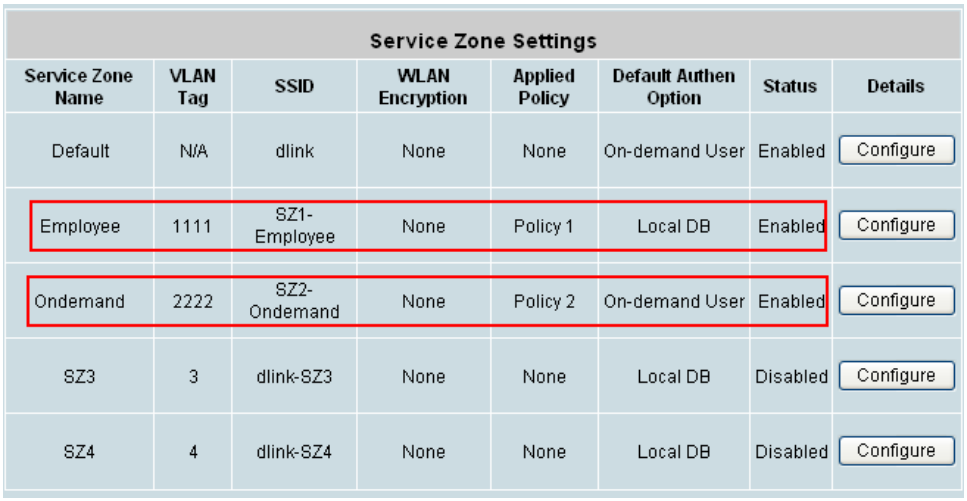


➢ Choose the appropriate policy for this "**service zone**"



- **Finished Configuration – Service Zone Settings:**

  Once the settings of two service zones are completed, the configured result will be displayed on screen in the **Service Zone Settings**. The name of the service zone and the enabled status should appear in the display.



Service Zone Settings

Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default	N/A	dlink	None	None	On-demand User	Enabled	Configure
Employee	1111	SZ1-Employee	None	Policy 1	Local DB	Enabled	Configure
Ondemand	2222	SZ2-Ondemand	None	Policy 2	On-demand User	Enabled	Configure
SZ3	3	dlink-SZ3	None	None	Local DB	Disabled	Configure
SZ4	4	dlink-SZ4	None	None	Local DB	Disabled	Configure

Appendix F. Deploying DSA-3600 Using DWL-2100AP

▪ Wireless Features of DWL-2100AP

Wireless security can be addressed using the *DWL-2100AP* access point with **WPA** (Wi-Fi Protected Access) and **802.1X authentication** to provide a higher level of security for data communication among wireless clients. The *DWL-2100AP* is fully compatible with industry standards such as **WEP**, and can support **Multiple SSIDs**, each of which can be mapped to a specific **Service Zone** (see Section 4.1.6 Service Zone) defined in the *DSA-3600*. Using the **Service Zone** based architecture, administrators can assign wireless security settings to different **SSIDs** according to the **Service Zone** profiles.

The *DWL-2100AP* can be deployed in the **Service Zones** and centrally managed via the *DSA-3600*. The **Service Zone** and **Centralized AP Management** provide an ideal solution using the *DSA-3600* together with *DWL-2100AP* for quick creation and extension of wireless local area network (WLAN) in offices and other workplaces, including hotspots.

▪ Best Practice for Wireless Settings of DWL-2100AP

To use multiple **SSIDs** in *DWL-2100AP*, creation and configuration of different **Service Zones** will be needed.

➢ Two Types of SSIDs:

The *DWL-2100AP* has two types of **SSIDs**:

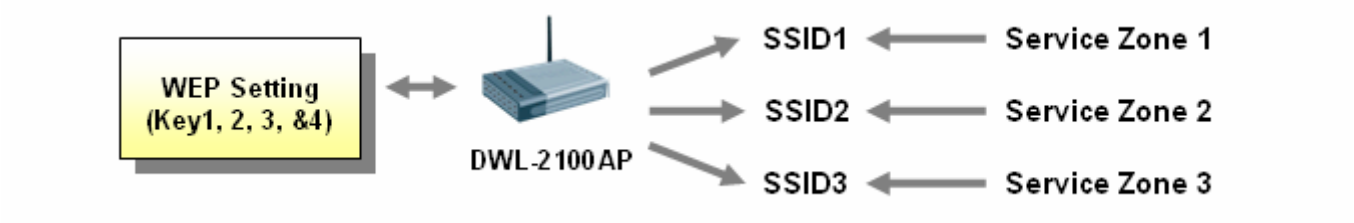
I. **Primary** (Only one for each *DWL-2100AP*) – Support every mode (**Open System**, **Shared Key**, **Open System/Shared Key**, **WPA-EAP**, **WPA2-EAP**, **WPA-Auto-EAP**, **WPA-PSK**, **WPA2-PSK**, and **WPA-Auto-PSK**) for security.

II. **Guest** (Up to 7 for each *DWL-2100AP*) – Does not support "**Open System/Shared Key**" mode for security

Caution: *If an existing* ***SSID*** *is already using* ***Guest*** *type, the wireless security of a* ***Service Zone*** *which is associated with this* ***SSID*** *cannot be set in the* ***Open System or Shared Key*** *mode in DSA-3600.*

➢ Single Set of WEP Keys:

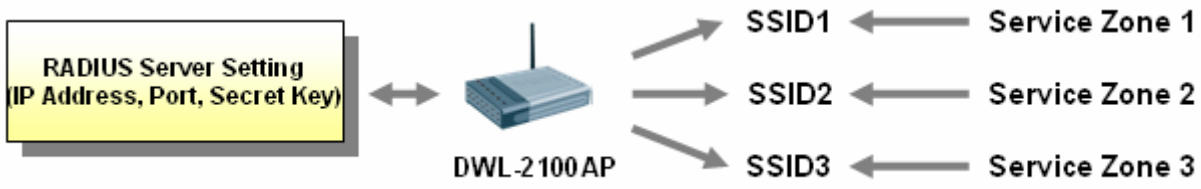
All **SSIDs** which belong to the same *DWL-2100AP* share the same set of **WEP** Keys (Key1 ~ Key4):



Caution: *If two or more* ***SSIDs*** *belong to the same DWL-2100AP and the wireless security of the associated* ***Service Zones*** *is set in the "****Shared Key"*** *mode in the DSA-3600, those* ***SSIDs*** *cannot be mapped to the* ***Service Zones*** *that have different sets of* ***WEP*** *Keys in the DSA-3600.*

➢ Single Set of RADIUS Server Setting:

Only one set of **RADIUS Server** setting is provided in *DWL-2100AP*.



Caution: *If two or more* ***SSIDs*** *belong to the same DWL-2100AP, and the wireless security of the associated* ***Service Zones*** *is set in the modes which use* ***RADIUS****, those* ***SSIDs*** *cannot be mapped to the* ***Service Zones*** *that have different sets of* ***RADIUS*** *Server settings in the DSA-3600.*

➢ Availability of WEP Keys:

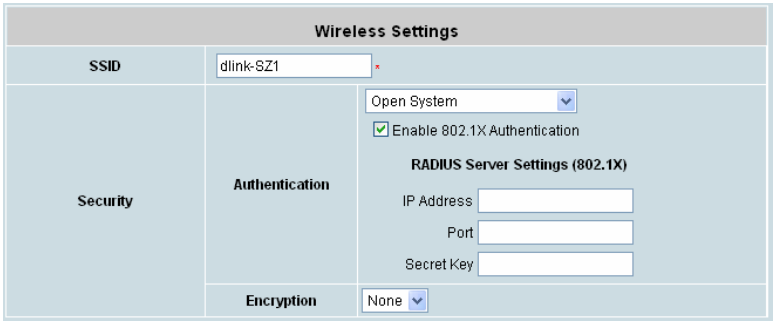
When an **SSID** of the *DWL-2100AP* is set in "**WPA**" related modes (such as **WPA-EAP**, **WPA2-EAP**, **WPA-Auto-EAP**, **WPA-PSK**, **WPA2-PSK**, and **WPA-Auto-PSK**), it will disable the availability of **WEP** Key2 and Key3 for another **SSID**, which is set in "**Shared Key**" modes (**Shared Key or Open System/Shared Key**), in the same *DWL-2100AP*.

Caution*: If two or more* ***SSIDs*** *belong to the same DWL-2100AP and the wireless security of one associated* ***Service Zone*** *is set in the modes of "****WPA****", "****WPA2****" or "****WPA Mixed****", those* ***SSIDs*** *that are in the modes of "****Shared Key****" and "****Open System or Shared Key****" cannot use* ***WEP*** *Key2 and Key3 in the DSA-3600.*

➢ Availability of 802.1x Authentication :

When an **SSID** (**Primary type**) of the *DWL-2100AP* is set in the mode of "**Open System**", "**Shared Key**", or "**Open System or Shared Key**", it will not support **802.1x authentication**.

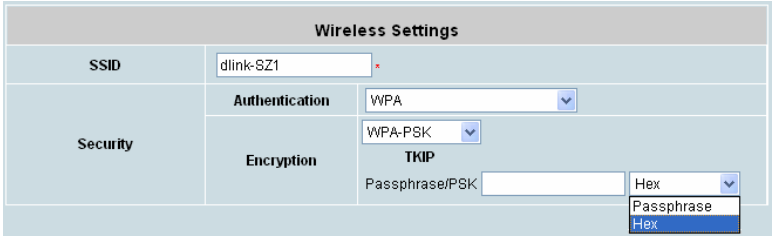
> ***Caution: 802.1x Authentication*** *should NOT be enabled in DSA-3600 if any DWL-2100AP exists in the* ***Service Zone*** *and the associated* ***SSID*** *is in the mode of "****Open System****" "****Shared Key****" or "****Open System or Shared Key****".*



➢ Availability of WPA Pre-Shared Keys (WPA) :

When an **SSID** of the *DWL-2100AP* is set in the mode of **WPA**, **WPA2**, and **WPA/WPA2 Mixed** in *DWL-2100AP*, "**Passphrase**" is the only available Key type for Pre-Shared keys (**PSK**). In addition, the length of "**Passphrase**" for the **SSID** of Guest type is 8 to 34 characters.

> ***Caution:*** *The "****HEX****" (the other Key type) should NOT be enabled in DSA-3600 if any DWL-2100AP exists in the* ***Service Zone*** *and the associated* ***SSID*** *is in the mode of* ***WPA****,* ***WPA2*** *or* ***WPA/WPA2 Mixed****. Also, administrators will have to ensure the length of "****Passphrase****" does not exceed 34 characters and not shorter than 8 characters in DSA-3600.*



Appendix G. Network Configuration on PC

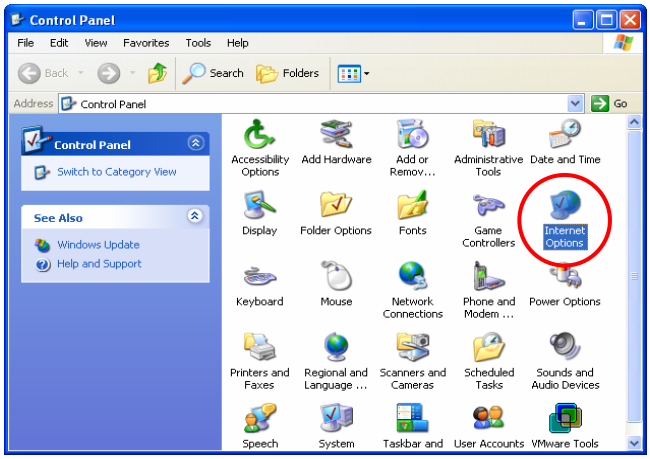
After the DSA-3600 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

▪ Internet Connection Setup

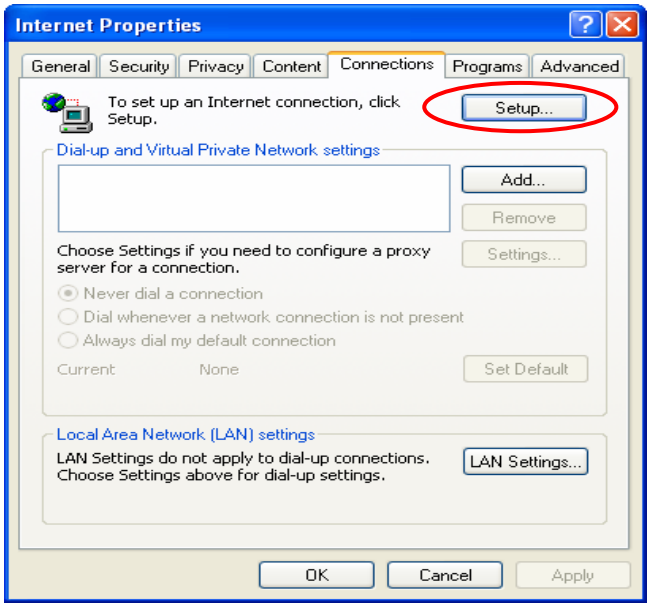
If the Internet Connection of this client PC has been configured as use local area network already, you can skip this setup.

➢ **Windows XP**

1. Choose **Start → Control Panel → Internet Option**.

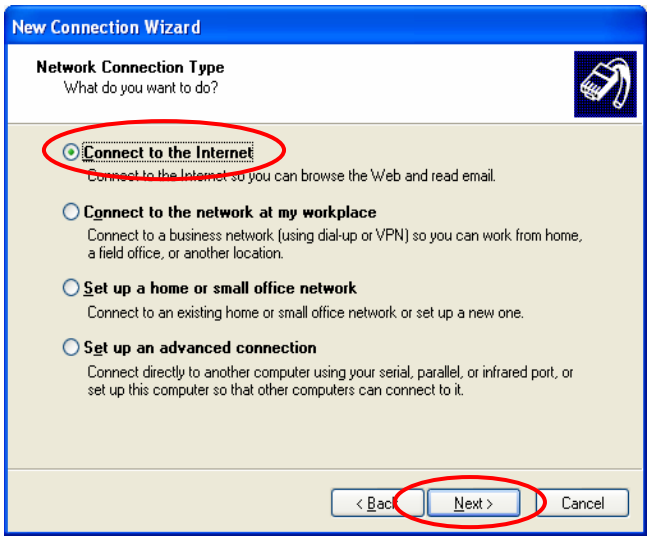


2. Choose the **"Connections"** label, and then click ***Setup***.

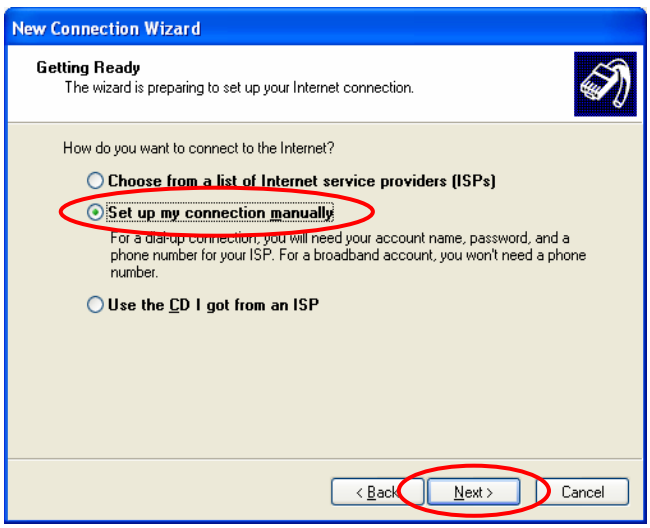


3. Click ***Next*** when **Welcome to the New Connection Wizard** screen appears.

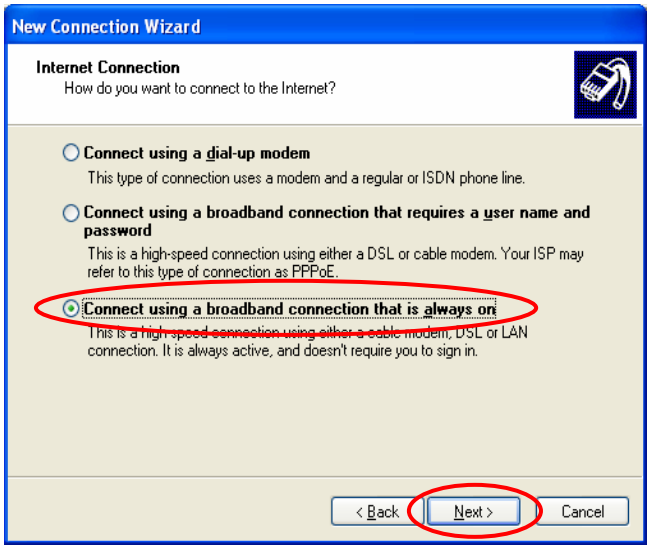
4. Choose **"Connect to the Internet"** and then click ***Next***.



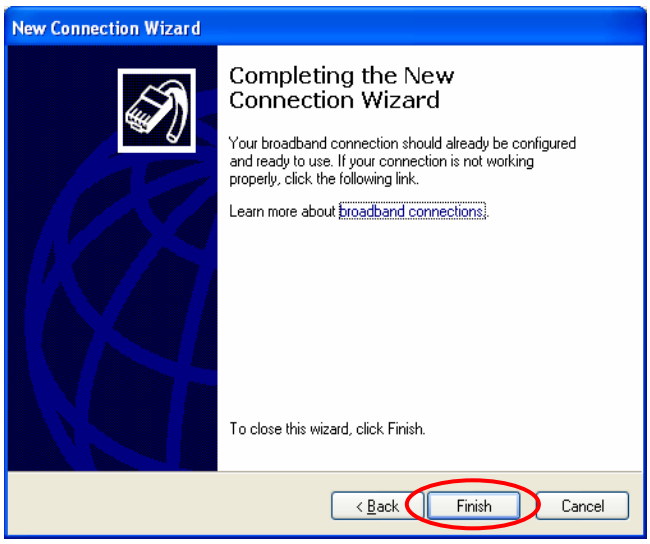
5. Choose **"Set up my connection manually"** and then click ***Next***.



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



7. Finally, click ***Finish*** to exit the **Connection Wizard**. Now, you have completed the setup.



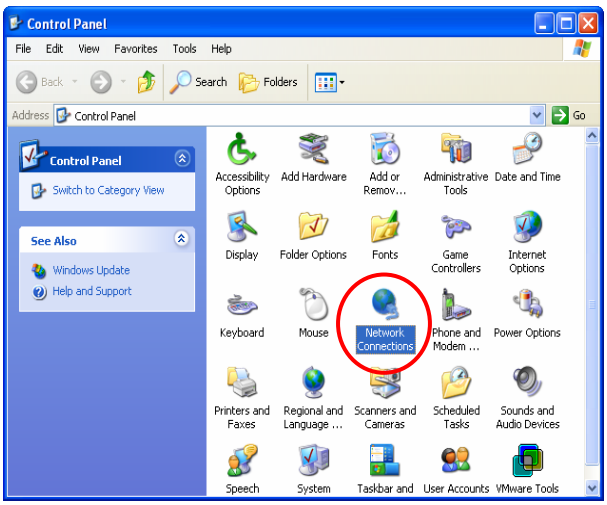
▪ TCP/IP Network Setup

In the default configuration, the DSA-3600 will assign an appropriate IP address to a client PC which uses DHCP to obtain IP address automatically. Windows 95/98/2000/XP configures IP setup to **"Obtain an IP address automatically"** in default settings.

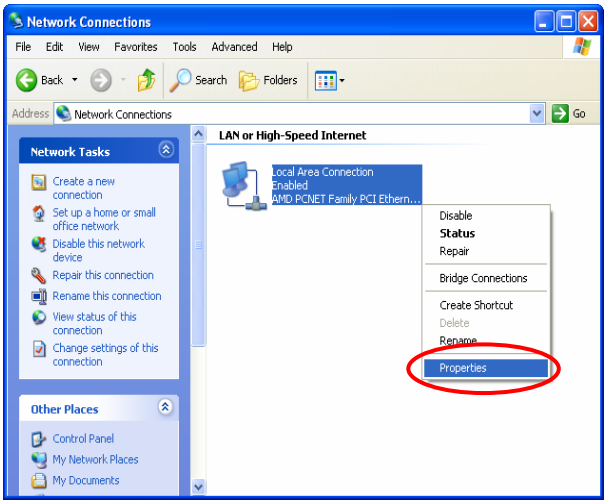
To check the TCP/IP setup or use a static IP to connect to the DSA-3600 LAN port, please follow the following steps:

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

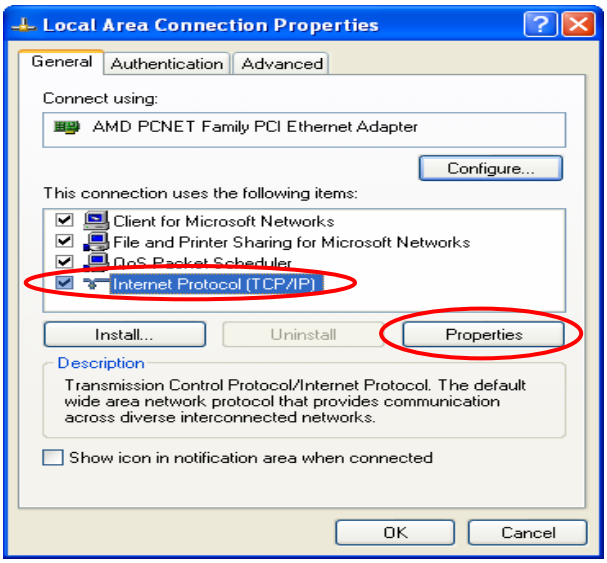
1. Select **Start → Control Panel → Network Connection**.



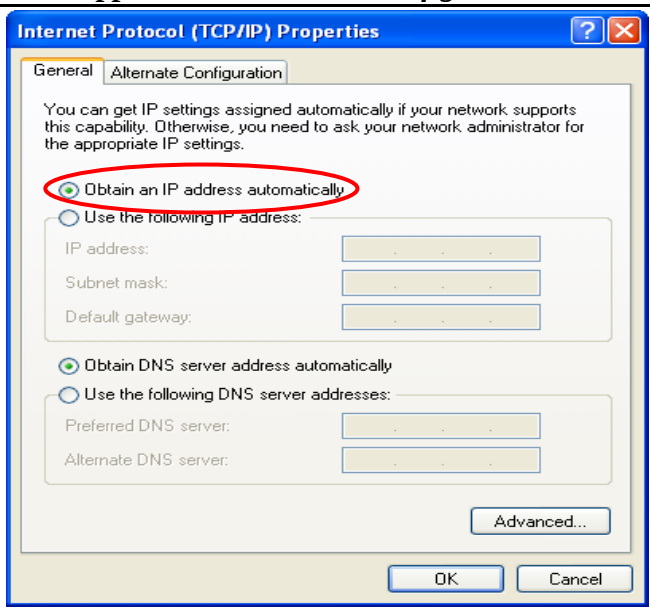
2. Click the right button of the mouse on the **"Local Area Connection"** icon and select **"Properties"**



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.

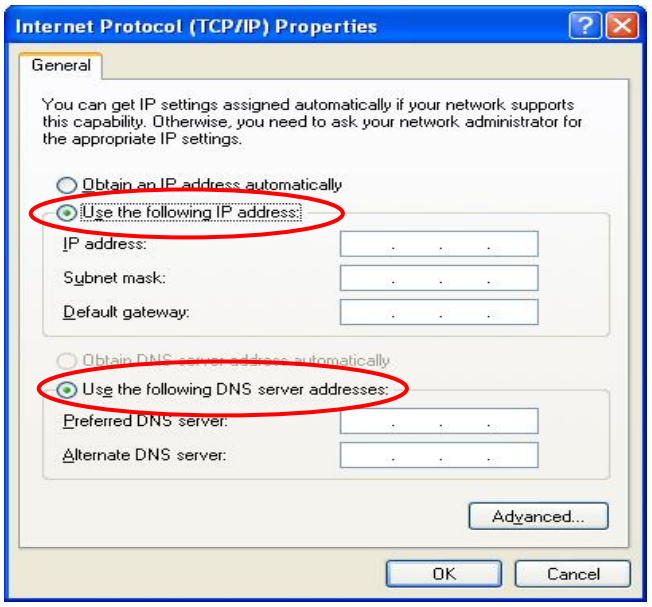


4. **Using DHCP:** To use DHCP, choose **"Obtain an IP address automatically"** and click ***OK***. This is the default setting of Windows. Reboot the PC to make sure an IP address is obtained from the DSA-3600.



5. **Using Specific IP Address:** To use specific IP address, please request from your network administrator the following information of the DSA-3600: ***IP address***, ***Subnet Mask***, ***New gateway*** and ***DNS server address***.

   Choose **"Use the following IP address"** and enter the information given from the network administrator in **"IP address"**, **"Subnet mask"** and the **"DNS address(es)"** and then click ***OK***.



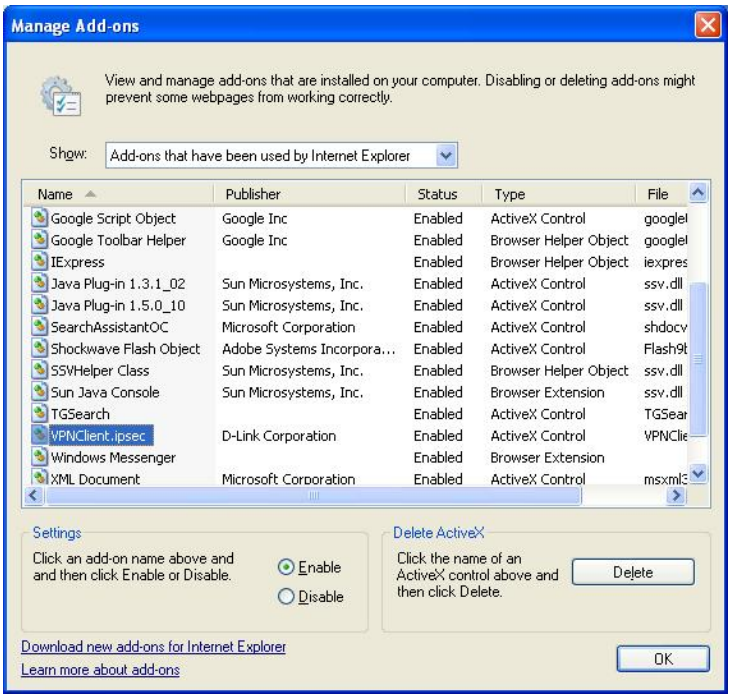
Appendix H. Local VPN

The DSA-3600 is equipped with IPSec VPN feature starting from release v1.00. To utilize IPSec VPN supported by Microsoft Windows XP SP2 (with patch) and Windows 2000 operating systems, the DSA-3600 implements IPSec VPN tunneling technology between client's windows devices and the DSA-3600 itself regardless of wired or wireless network.

By pushing down ActiveX to the client's Windows device from the DSA-3600, no extra client software is required to be installed except ActiveX, in which a so-called "clientless" IPSec VPN setting is then configured automatically. At the end of this setup, a build-in IPSec VPN feature will be enabled and ready to serve once it is launched for setup. The goal of this design is to eliminate the configuration difficulty from IPSec VPN users. At the client side, the IPSec VPN implementation of the DSA-3600 is based on ActiveX and the built-in IPSec VPN client of Windows OS.

1. ActiveX component

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



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 is enabled.

During the first login to the DSA-3600, Internet Explorer will ask user to download the ActiveX component of IPSec VPN. This ActiveX component once downloaded will be running parallel with the “Login Success” page. The ActiveX component helps to setup the IPSec VPN tunnel between client’s device and the DSA-3600. It also helps to check the validity of the IPSec VPN tunnel between them. If the connection is down, the ActiveX component will detect the broken link and recompose the IPSec tunnel. Once the IPSec VPN tunnel is built, any packet sent will be encrypted. Without connecting to the original IPSec VPN tunnel, user or client device has no alternative to gain network connection beyond this. The DSA-3600’s IPSec VPN feature is designed to solve possible data security leak between client and the controller via either wireless or wired connection without extra hardware or client software installed.

2. Limitations

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

a. Internet Connection Firewall of Windows XP or Windows XP SP1 not being compatible with IPSec protocol, hence it shall be turned off to allow IPSec packets to pass through.

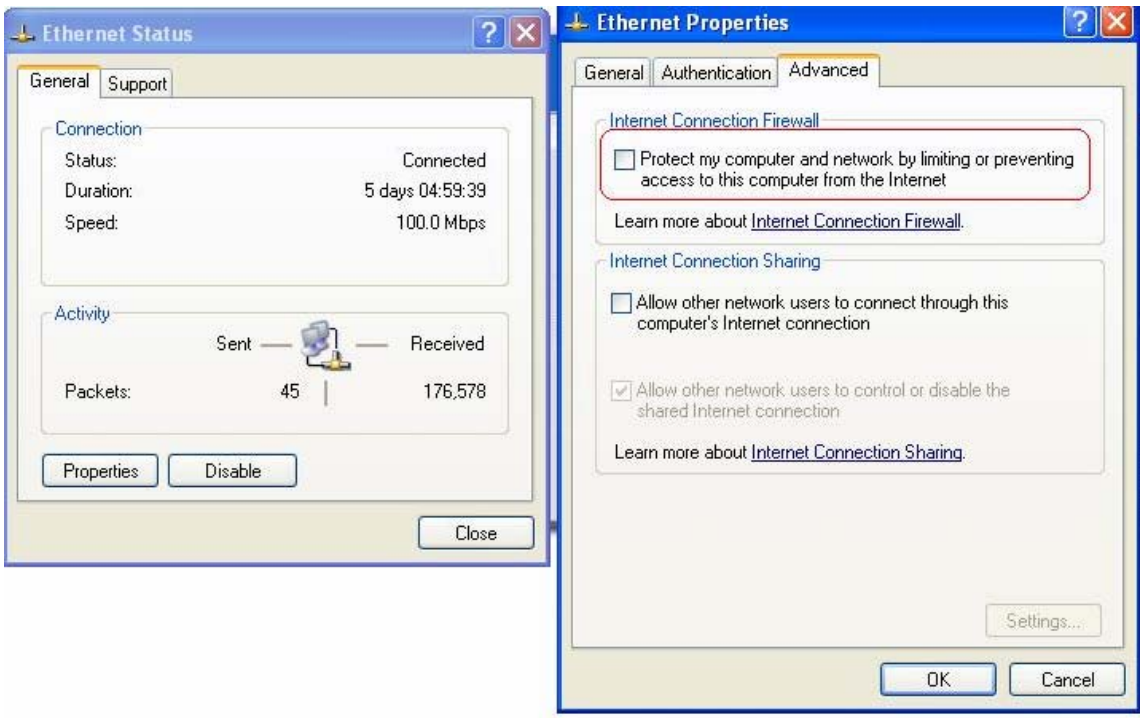
b. Without patch, ICMP (Ping) and PORT command of FTP cannot work in Windows XP SP2.

c. The Forced termination (through CTRL+ALT+DEL, Task Manager) of the Internet Explorer will stop the running of ActiveX, which may result in IPSec tunnel not being able to work properly at client’s device. 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.

3. 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.



Suggestion: *Please* ***TURN OFF*** *Internet Connection Firewall feature or upgrade the Windows OS into Windows XP SP2.*

4. ICMP and Active Mode FTP

On Windows XP SP2 that is without patch KB889527, ICMP packets will be dropped from IPSec tunnel. This issue 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 issues of supporting active mode FTP inside IPSec VPN tunnel of Windows XP SP2.

Suggestion: *Please UPDATE client's Windows XP SP2 with patch KB889527.*

5. The Termination of ActiveX

The ActiveX component for IPSec VPN is running parallel with the “Login Success” web page. Unless user decides to close the session and to disconnect with DSA-3600, the following conditions or behaviors of user’s browser can be avoided in order to maintain the built IPSec VPN tunnel always alive.

Reasons why Internet Explorer may cause ActiveX to stop unexpectedly are as follows:

a. **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.*

b. **Terminate the Internet Explorer Task from Windows Task Manager**

Suggestion: *Do not terminate this VPN task of Internet Explorer.*

c. **There are some cases of Windows messages by which DSA-3600 will hint 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. e-mail of Outlook) that occupies this existing Internet Explorer.

All these will cause the termination of IPSec VPN tunneling if the 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.*

6. Non-supported OS and Browser

Currently, Windows Internet Explorer is the only browser supported by DSA-3600.Windows XP and Windows 2000 are the only two supported OS along with this release.

7. FAQ

a. How to clean IPSec client?

ANS:

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

C:\> **cd %windir%\system32**

C:\> **Clean_IPSEC.bat**

Or

C:\> **cd %windir%\system32**

C:\> **ipsec2k.exe stop**

b. How to remove ActiveX component in client's computer?

ANS:

(1) Uninstall and delete ActiveX component

(2) Close all Internet Explorer windows

(3) Open a command prompt window and type the commands as follows

C:\> **cd %windir%\system32**

C:\> **regsvr32 /u VPNClient_1_5.ocx**

C:\> **del VPNClient_1_5.ocx**

c. What can I do if unable establish IPSec connection for Windows XP SP1?

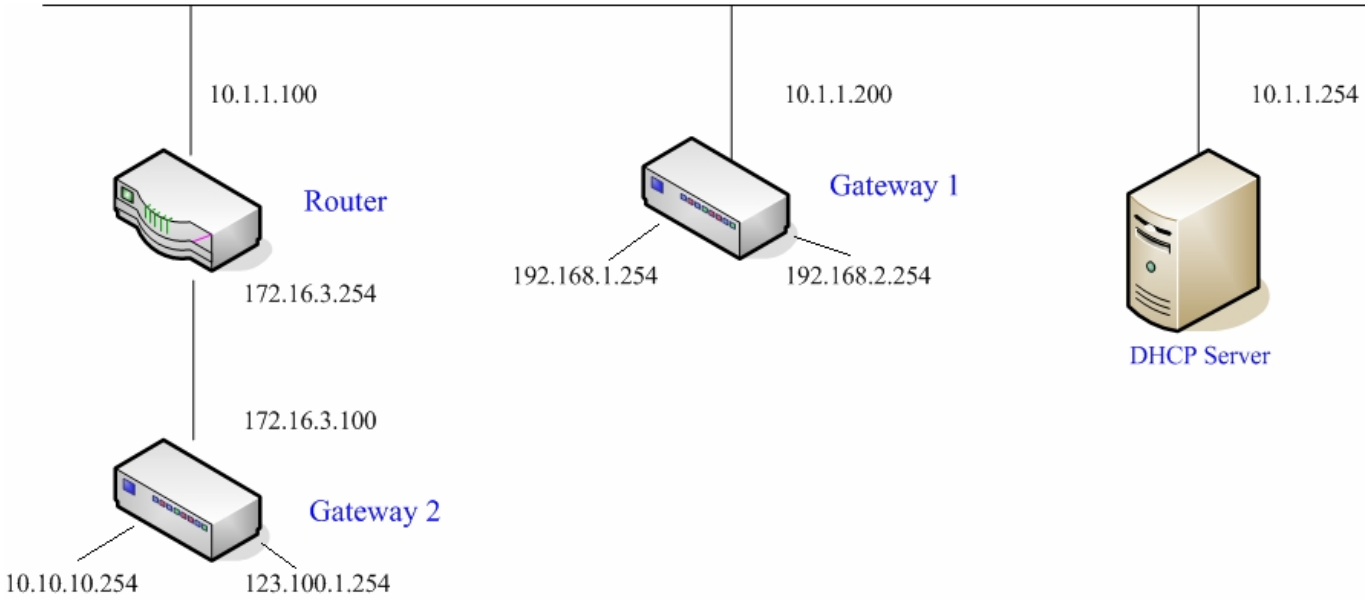
ANS:

Disable Windows XP firewall

Appendix I. DHCP Relay

The DSA-3600 supports DHCP Relay defined according to RFC 3046. For scaling reasons, it is advantageous to set up an external DHCP server apart from using the internal DHCP server implemented in the DSA-3600 for assigning IP. When client-originated DHCP packets are forwarded to a DHCP server, a new option called the "Relay Agent Information option" is inserted by the DHCP relay agent. External DHCP servers that recognize the Relay Agent Information option may use this information to implement IP address or other parameter assignment policies. The external DHCP server will echo the option back to the relay agent in server-to-client replies, and strip-off the option before forwarding the reply to the client.

A graphic example of connecting 2 gateways with an external DHCP server:



Please note that the Router and Gateway 1 connected to the DHCP Server have to be under the same network segment as the DHCP Server.

When a client requests IP address from Gateway 1 Public LAN through the build-in DHCP relay agent of the DSA-3600, the DHCP server will receive a DHCP REQUEST packet with Option 82 (a code defined in RFC 3046). A Circuit ID will be sent by the DSA-3600 when the DHCP relay is enabled to define where the packet is sent from, and this Circuit ID will have a format of MAC_IP, such as 00:E0:22:DF:AC:DF_192.168.1.254. When the external DHCP server gets the request packet, it will therefore know where to reply to and which IP to assign.

Here is an example of configuration file of the DHCP server:

```
class "g1_public_lan" {
        match if option agent.circuit-id = "00:90:0B:07:60:91_192.168.1.254";
}

class "g1_private_lan" {
        match if option agent.circuit-id = "00:90:0B:07:60:92_192.168.2.254";
}

class "g2_public_lan" {
        match if option agent.circuit-id = "00:12:43:AD:32:F2_10.10.10.254";
}

class "g2_private_lan" {
        match if option agent.circuit-id = "00:12:43:AD:32:F2_123.100.1.254";
}

subnet 0.0.0.0 netmask 0.0.0.0 {

        option domain-name-servers      168.95.1.1;

        pool {
                allow members of "g1_public_lan";
                range 192.168.1.30 192.168.1.50;
                option routers 192.168.1.254;
                option subnet-mask 255.255.255.0;
        }

        pool {
                allow members of "g1_private_lan";
                range 192.168.2.30 192.168.2.50;
                option routers 192.168.2.254;
                option subnet-mask 255.255.255.0;
        }
```

Based on the above example, the client that connects to the DSA-3600 sends out a DHCP request. The DHCP relay function being enabled in the DSA-3600 sends a Circuit ID 00:90:0B:07:60:91_192.168.1.254 to the external DHCP server. When the DHCP server gets the Circuit ID, it recognizes that the request is sent from g1_public_lan and thus assigns the client a DNS server of 169.95.1.1, an IP that is in the range of 192.168.1.30 and 192.168.1.50, a default gateway of 192.168.1.254, and a subnet-mask of 255.255.255.0

Appendix J. 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 the *Email & SYSLOG*.
- 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.

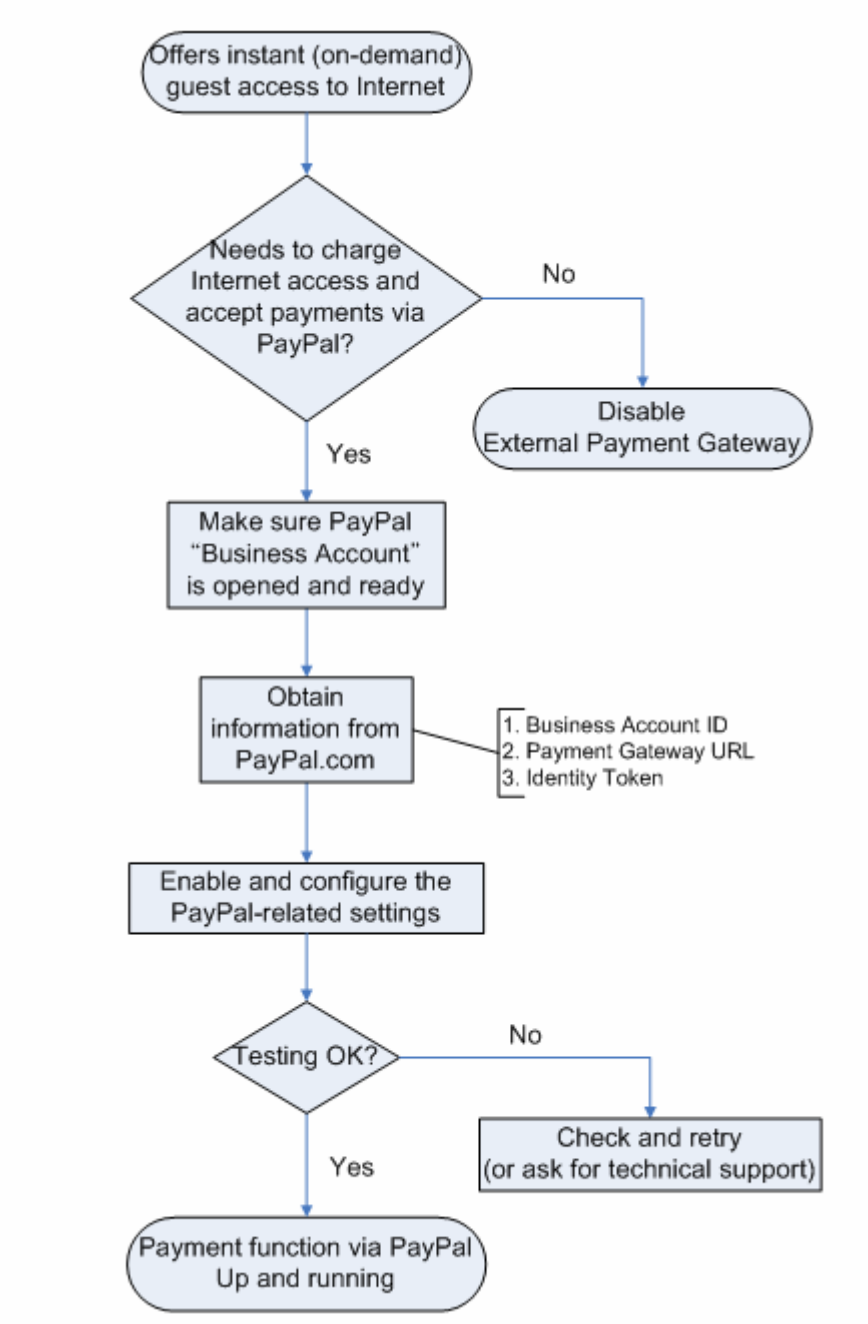
Field	**Description**
Date and Time	The date and time that the session is established
Session Type	[New]: This is the newly established session. [Blocked]: This session is blocked by a Firewall rule.
Username	The account name (with postfix) of the user; It shows "N.A." if the user or device does not 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 K. 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.



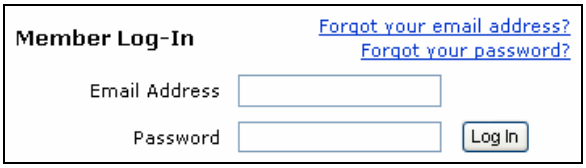
1. Setting Up

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

1.1 Open An Account

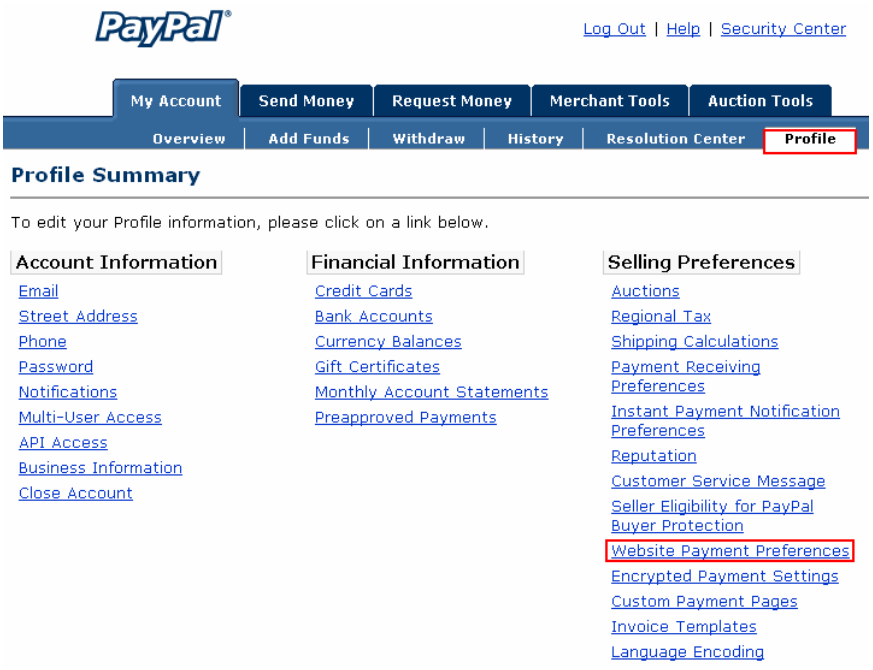
Step 1: Sign up for a PayPal Business Account and login.

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

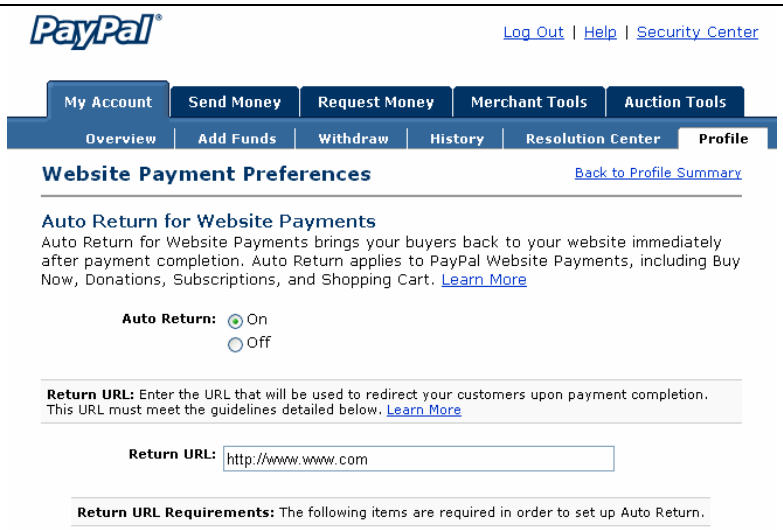
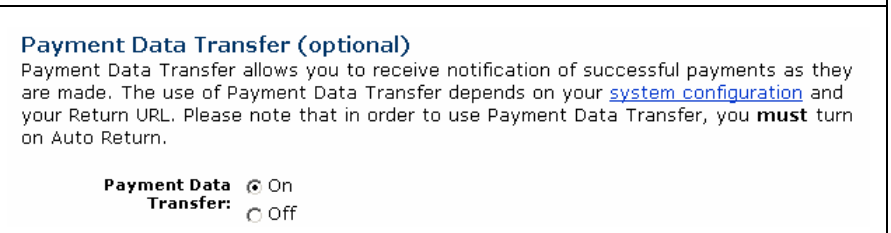
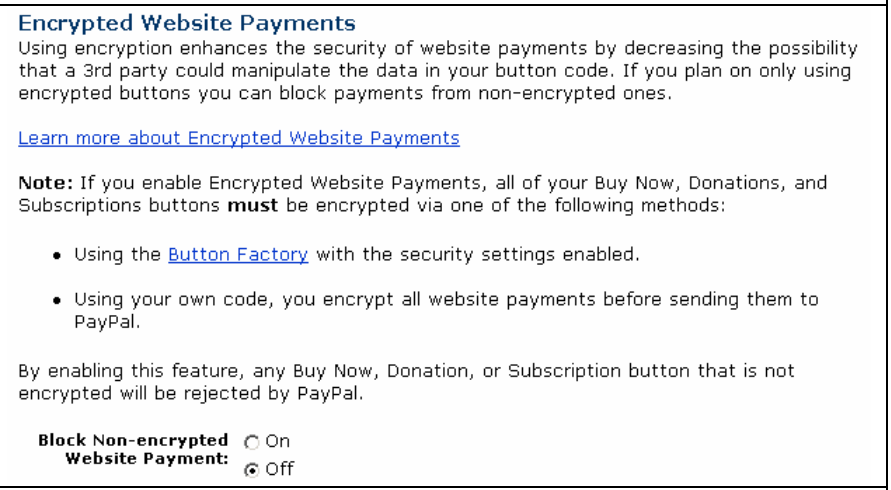
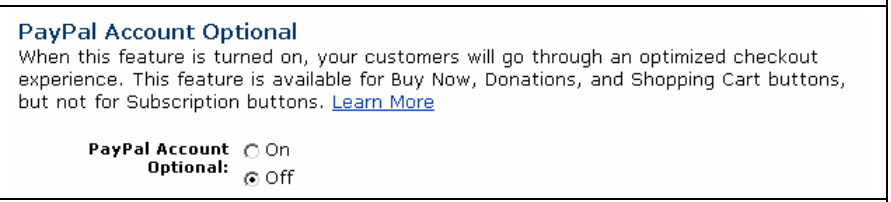
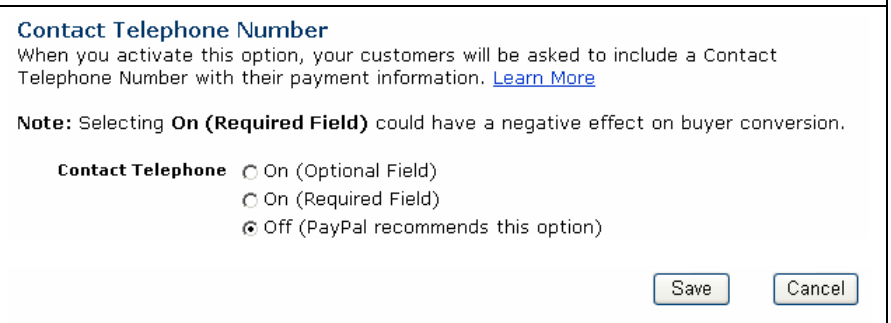


Step 2: Edit necessary settings in "Website Payment Preferences"

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



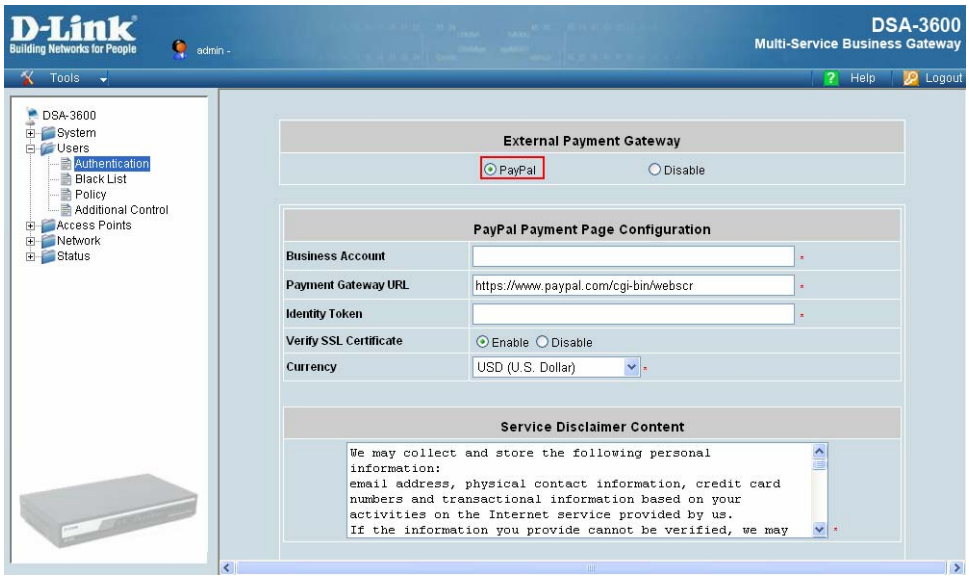
Administrators should scroll down to edit each setting as shown in the table below. To activate all the changes, please click ***Save*** at the end of the page.

Settings	Screenshots
Auto Return (On) **Return URL (Redirect Webpage)** Type http://www.www.com or other URL.	
Payment Data Transfer (On)	
Block Non-encrypted Website Payment (Off)	
PayPal Account Optional (Off)	
Contact Telephone Number (Off) **Click *Save*.**	

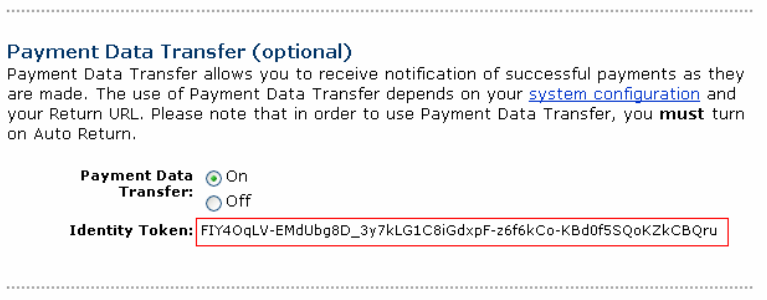
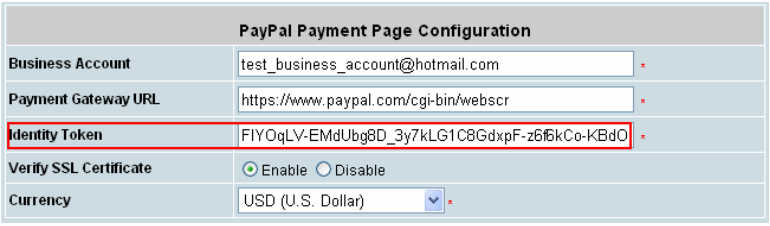
1.2 Configure DSA-3600 with a PayPal Business Account

Please log in DSA-3600:

Users → Authentication → Click the Option **On-demand User → External Payment Gateway →** Click ***Configure*** **→ External Payment Gateway →** Select ***PayPal***

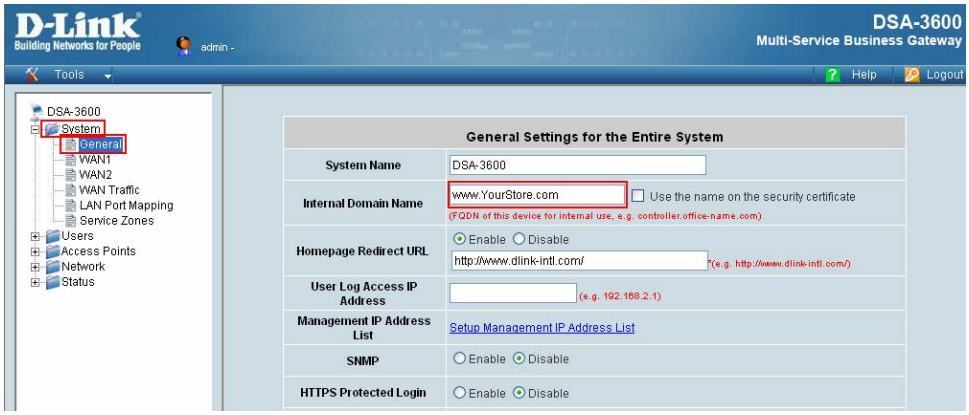


Three fields are required:

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)**.  Copy the **Identity Token** in the above page to the section "**PayPal Payment Page Configuration**" of DSA-3600. 

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.



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.

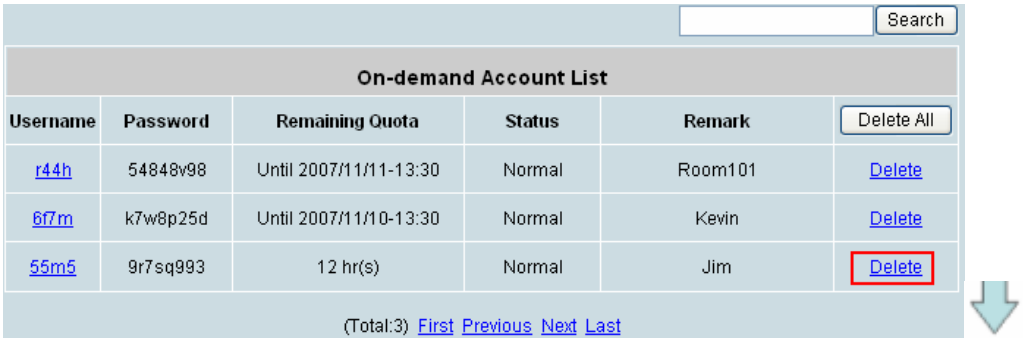
2. Basic Maintenance

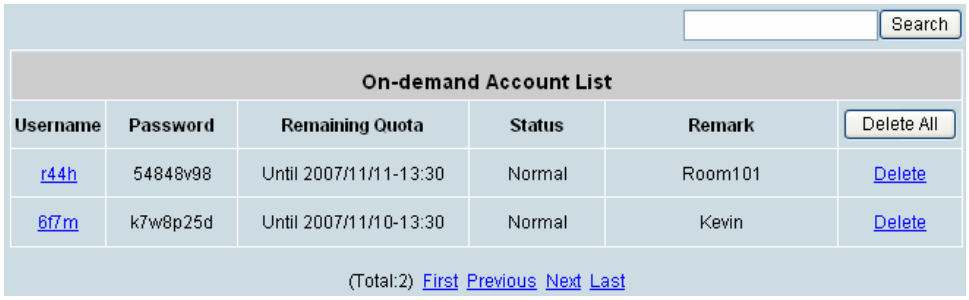
In order to maintain the operation, the merchant owner will have to manage the accounts and payment transactions on PayPal website as well as DSA-3600.

2.1 Refund a completed payment and remove the on-demand account generated on DSA-3600

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 DSA-3600, please log in DSA-3600:
Users → Authentication → Click the Option **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.

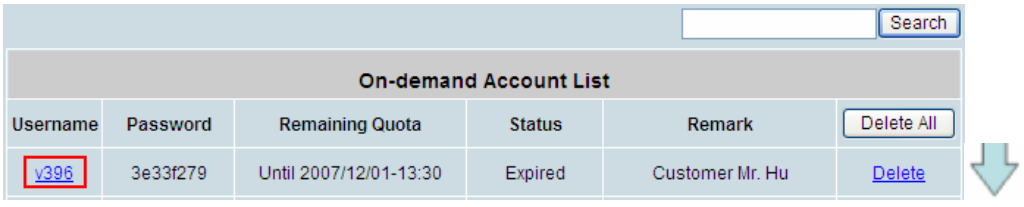




2.2 Find the username and password for a specific customer

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 DSA-3600:
Users → Authentication → Click the Option **On-demand User → On-demand Account List →** Click ***View*** → **On-demand Account List**. Search for the specific username. Password can be found in the same record



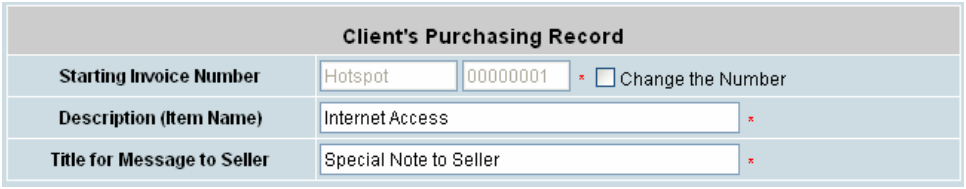
Note:

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

2.3 Send an email receipt to a customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via PayPal. To change the information on the receipt for customer, please log in DSA-3600:

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



2.4 Send an email receipt for each transaction to the merchant

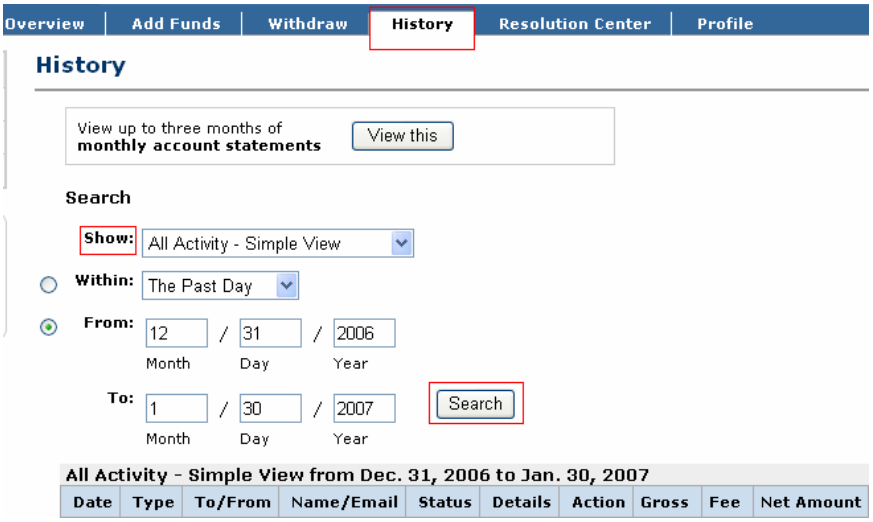
A copy of email receipt with payment details (including available message note from buyer) for each successful transaction will also be automatically sent to the merchant owner/administrator via PayPal.

3. Reporting

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

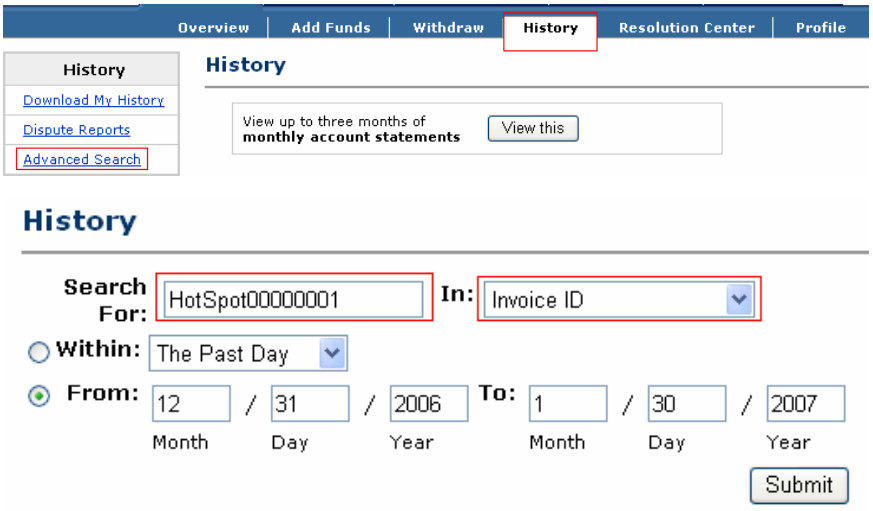
3.1 Transaction activity during a period

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***



3.2 Search for the transaction details for a specific customer

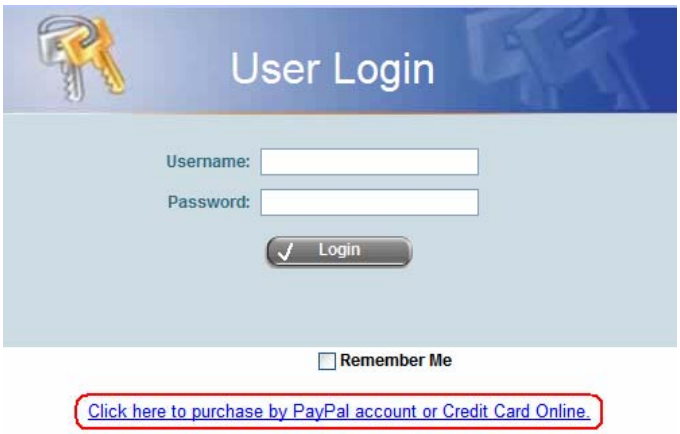
Please log in PayPal → Click **History** → Click **Advanced Search** → Enter the name for a specific customer as criteria in the **Search For** field and Choose Last Name or Last Name, First Name in the **In** field → Specify the time period → Click ***Submit*** → Click **Details** to view the transaction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



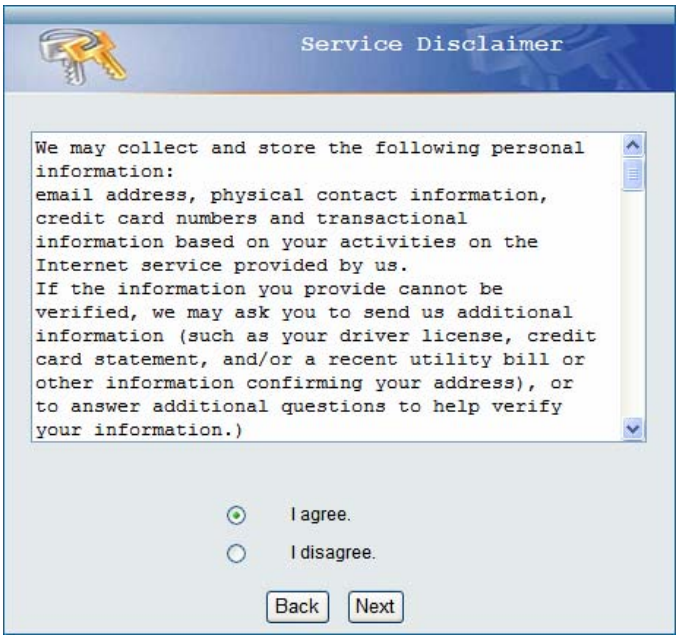
Note: *For more information about PayPal, please see http://www.paypal.com*

4. An Example of Making Payments via PayPal

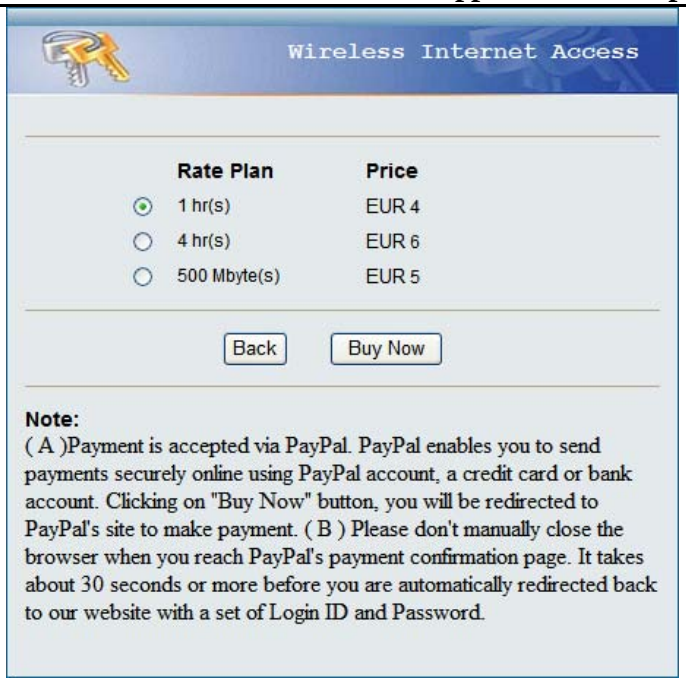
Step 1: Click the link below the login window to pay for the service via PayPal.

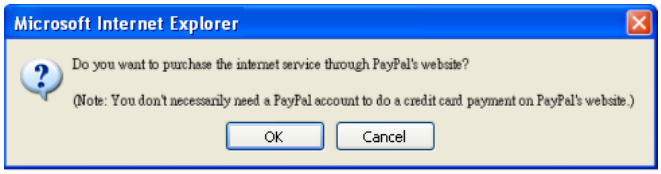


Step 2: Choose ***I agree*** to accept the terms of use and click ***Next***.

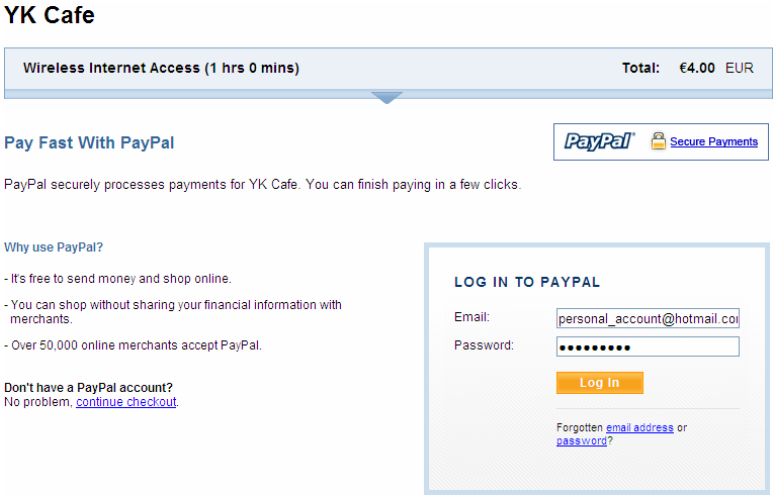


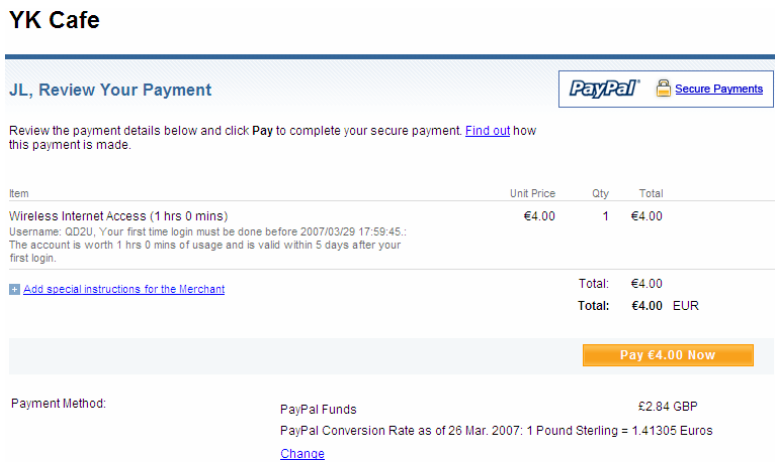
Step 3: Please fill out the form and click ***Buy Now*** to send out this transaction. There will be a confirm dialog box.

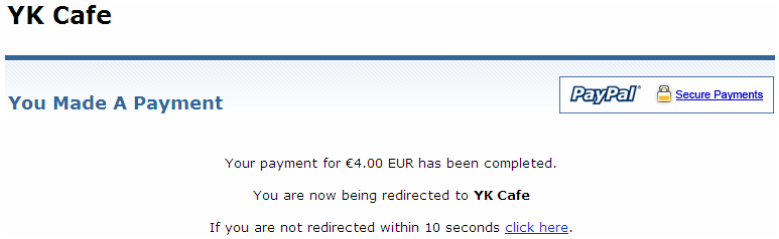




Step 4: You will be redirected to PayPal website to complete the payment process.







Step 5: Click ***Start Internet Access*** to use the Internet access service.

Note:

1. *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.*
2. *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.*