D-Link®
Building Networks for People

DSA-6100
User Guide

Version DSA-6100-2.10 July, 2009

Copyright © 2009 D-Link Corporation

Trademarks

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-6100 Wireless Access Controller 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:

⌂ Return to the homepage of this section.

↑ Return to the previous page.

✓ Apply Apply all settings configured.

✕ Clear Clear all settings configured prior to applying.

> ***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

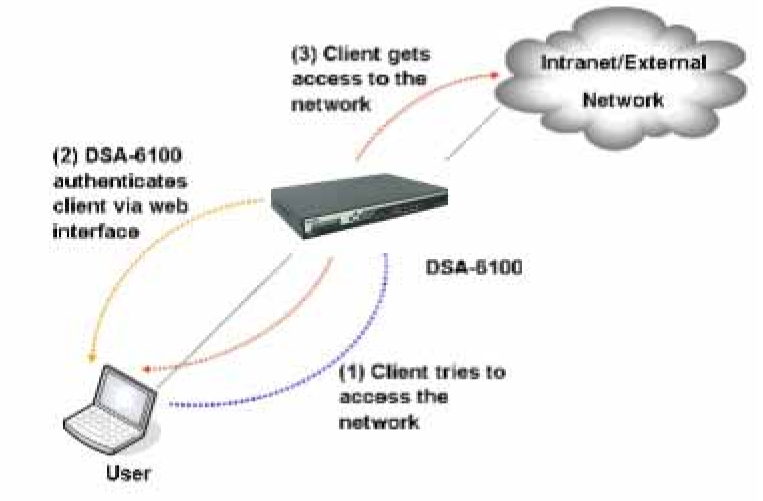
2.1 Introduction of DSA-6100

The DSA-6100 is a Network Access Controller designed for medium to large network environments to provide network **"manageability"**, **"efficiency"** and a **"friendly interface"** suitable for campuses, libraries, gymnasiums, small and middle enterprises, factories, hotspots and community hospitals.

2.2 System Concept

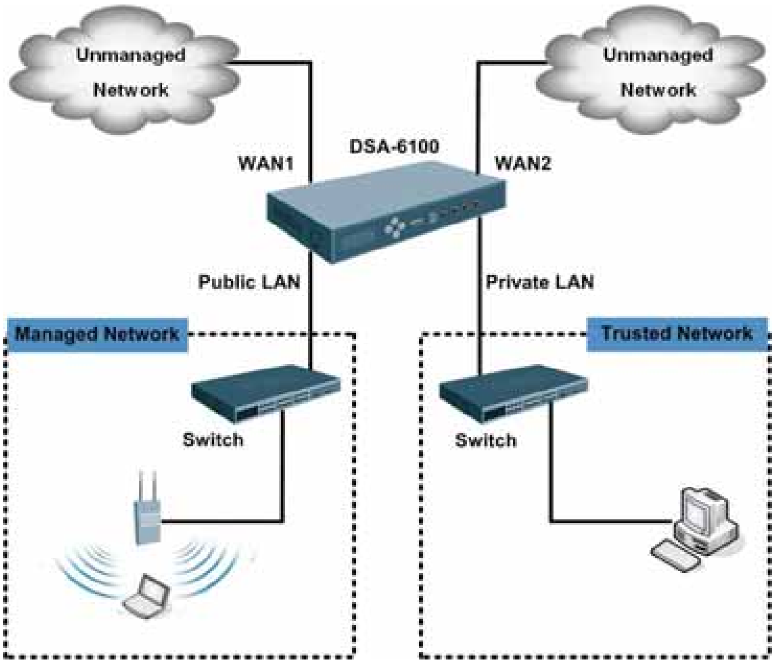
The DSA-6100 is built for the purpose of controlling all network data passing through its system. Users, under the managed network, must be authenticated in order to access the network beyond the managed area. The authentication mechanism at the user's end is provided by the DSA-6100 server using SSL encryption to protect the webpage. The DSA-6100 is responsible for the authentication, authorization, and management functions in the system. User account information may be stored in the DSA-6100 database or in other specified external authentication databases.

The process of authenticating the user's identity is executed via the SSL encrypted webpage. The use of web interface ensures the system is compatible to most desktop systems and palm computers. When a user authentication is requested, the DSA-6100 server software checks the authentication database at the rear end to confirm the user's access right. The authentication database may be the local database of the DSA-6100 or any external database that the DSA-6100 supports. If the user is not an authorized user, the DSA-6100 will refuse the user's request for access and block the user from accessing the network. If the user is an authorized user, the DSA-6100 will grant the user appropriate access right so that the user can use the network. If the online user remains idle without using the network for a time exceeding a predetermined idle time on the DSA-6100, or if the online user logs out of the system, the DSA-6100 will exit the working stage of the user and terminate the user's access right of the network.

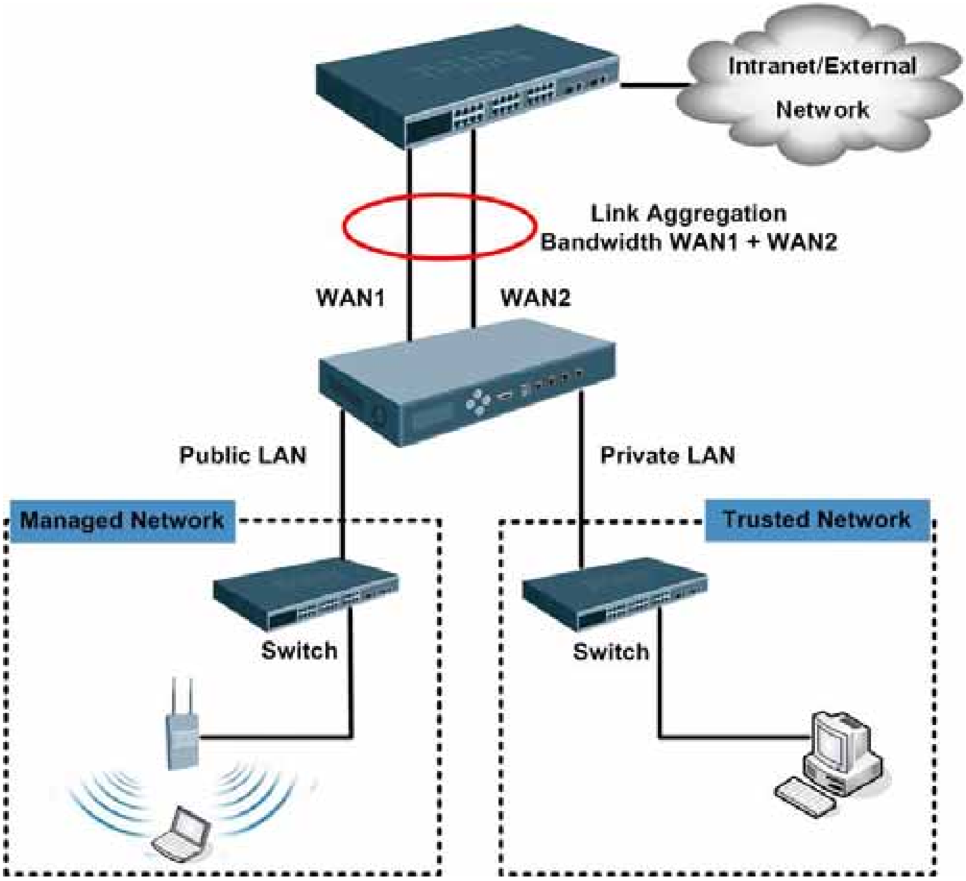

(3) Client gets access to the network
Intranet/External Network
(2) DSA-6100 authenticates client via web interface
DSA-6100
(1) Client tries to access the network
User

The following picture provides a simple example of setting up middle to large enterprise network. The DSA-6100 is set to control a part of the company's intranet. The whole managed network includes cable network users, and wireless network users. In the beginning, any user located at the managed network is unable to access the network resource without permission. If the access right to the network beyond the managed area is required, an Internet browser such as the Internet Explorer must be opened and a connection to any website must be performed. When the browser attempts to connect to a website, the DSA-6100 will force the browser to redirect to the user login webpage. The user must enter the username and password for authentication. After the identity is authenticated successfully, the user will be granted proper access right as defined in the DSA-6100.

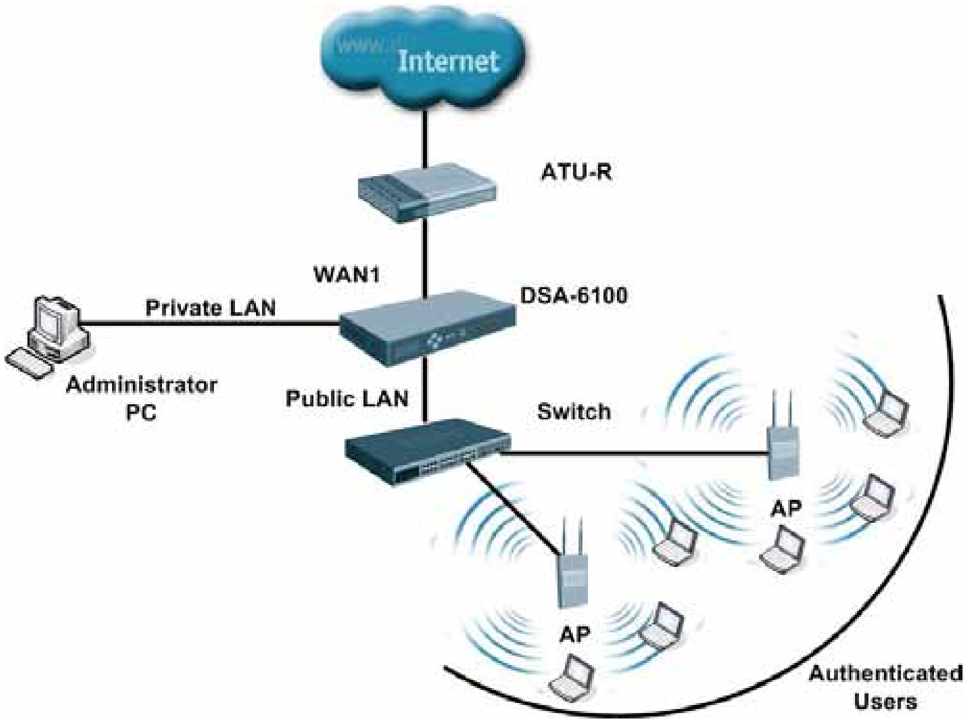
***Attention: Public LAN** is referred to as the LAN port with the authentication function enabled from where the Authentication is required for the users to get access of the network. **Private LAN** is referred to as the LAN port with the authentication function disabled.*



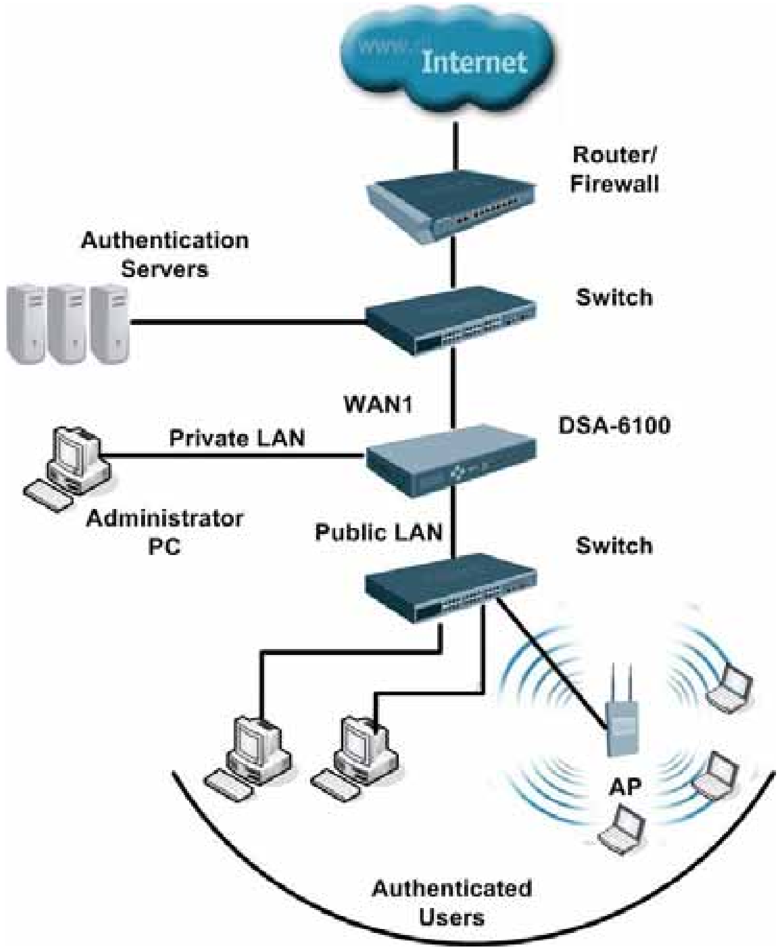
Another setup example is shown in the following diagram, where the administrator is able to increase the uplink bandwidth capacity beyond the capacity of any single WAN port. This is done by the DSA-6100's *Bonding* feature.



The DSA-6100 can be used as the gateway for Internet access, where an external connection can be established for sharing, accounting, authentication and users management. This solution can be applied for environments such as hotels, campus, hot spots and others. An example of the network topology is as follows:



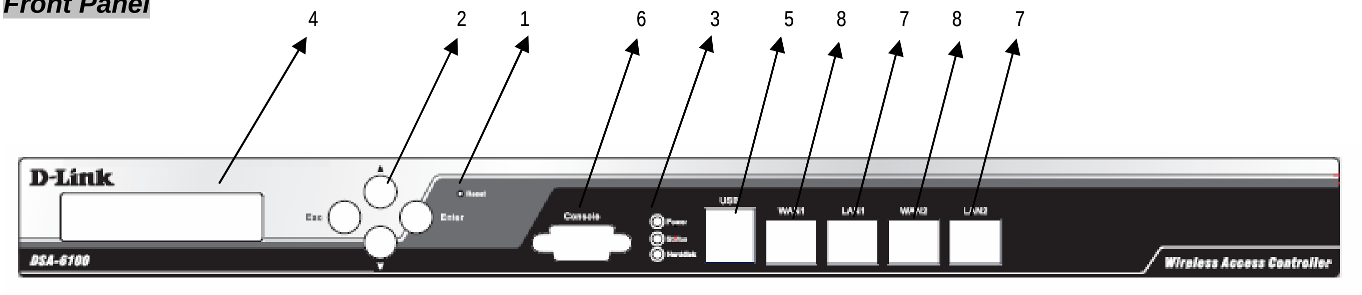
The DSA-6100 is able to use a Local Database or authentication servers (NT-Domain, POP3, LDAP and Radius) to authenticate users. This type of solution is suitable for environments such as hotels, campus, hot spots, enterprises and others.



Chapter 3. Hardware Installation

3.1 Panel Function Descriptions

Front Panel



1. Reset	**3.** LED	**5.** Port: USB	**7.** Port: LAN1 / LAN2
2. Select / Execute	**4.** LCD	**6.** Port: Console	**8.** Port: WAN1 / WAN2

1. **Reset**
   - Press and hold the Reset Button for 5 seconds to restart the DSA-6100.
   - Press and hold the Reset Button for more than 10 seconds to restart the DSA-6100 in default configuration.

2. **Select / Execute**
   - **Esc:** Cancel selected function
   - **Enter:** Execute selected function in menu
   - **Arrow Up:** Navigate upward to select required function in menu
   - **Arrow Down:** Navigate downward to select required function in menu

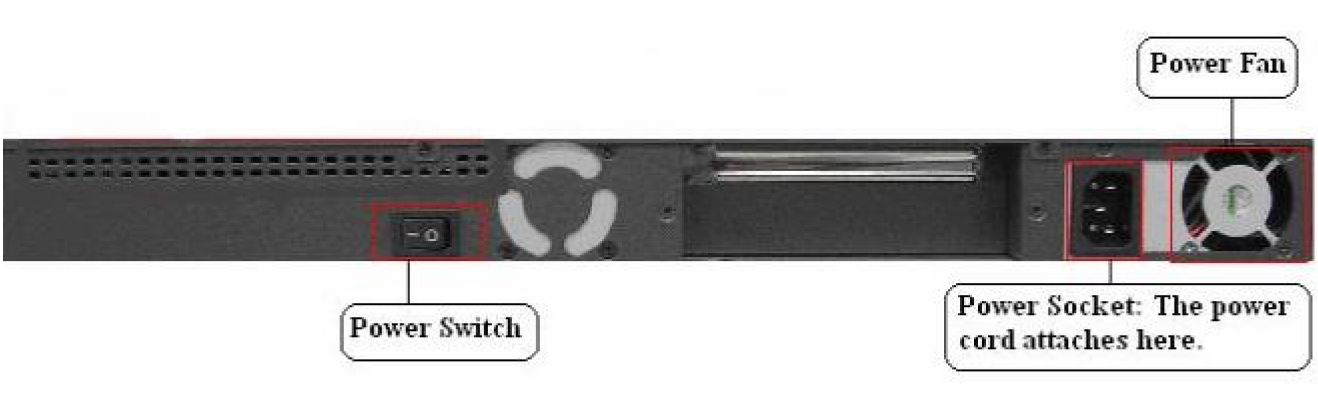
3. **LED**
   - **Power**: ON indicates that power is on and OFF indicates that power is off.
   - **Status**: OFF indicates BIOS is running, BLINKING indicates the OS is running, and ON indicates system is ready.
   - **Hard Disk**: Reserved for future usage.
   - **Port Speed**:
   - ➢ Upper left indicator: OFF indicates no connection, ON (orange color) indicates connection and BLINKING indicates transmitting data.
   - ➢ Upper right indicator: OFF indicates 10Mbps connection, ON (green color) indicates 100Mbps connection and ON (orange color) indicates 1000Mbps connection.

4. **LCD:** Shows the information about the System and Network listed below:
   - System Info:
     - H.W. Status (CPU Temperature)
     - Utilization (CPU (%) and Memory (%))
     - System Time
     - Boot-up Time
     - Firmware

   - Network Info: WAN 1 / WAN 2 / LAN 1 / LAN 2
     - Setting (IP Address and Netmask)
     - Loading (In/Out Pkts/s and In/Out Bytes/s)
     - Status (Connected or Disconnected)

5. **USB Port:** Reserved for future use.
6. **Console Port:** The system can be configured via HyperTerminal. For example, if you need to set the Administrator's Password, you can connect a PC to this port as a Console Serial Port via a terminal connection program (the terminal's configuration must be 9600bps, 8, N, 1, flow control - none) to change the Administrator's Password.
7. **LAN1 / LAN2 Ports:** The two LAN ports can be independently configured and set to disallow users to access Internet before authentication. Administrators can therefore choose to force authentication on users connected to these ports.
8. **WAN1 / WAN2 Ports:** The two WAN ports are connected to a network which is not managed by the DSA-6100, and this port can be used to connect to the ATU-Router of an ADSL, or the port of a Cable Modem, or the Switch or Hub on the LAN of an organization.

Rear Panel



Power Fan: Keeps the power cool.

Power Socket: The power cord is attached here.

Power Switch: Turns on and off the machine.

3.2 Package Contents

The standard package of the DSA-6100 includes:

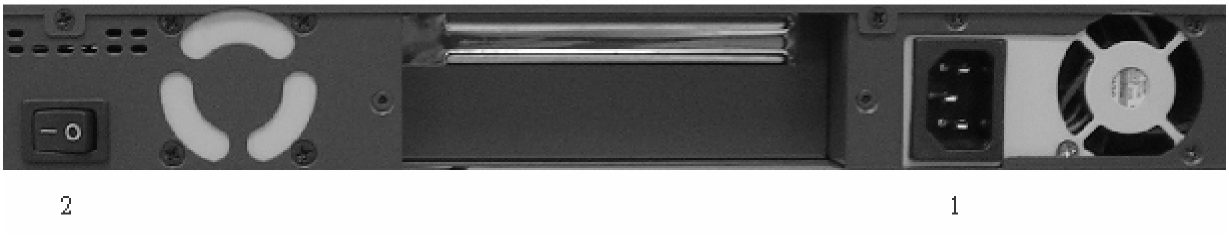
- DSA-6100 x 1
- Console Cable x 1
- Crossover Ethernet Cable x 1
- Straight-through Ethernet Cable x 1
- Power Cord x 1
- CD-ROM x 1
- Quick Installation Guide x 1
- Screw Set x 1
- Rack Mount Bracket x 1

3.3 System Requirement

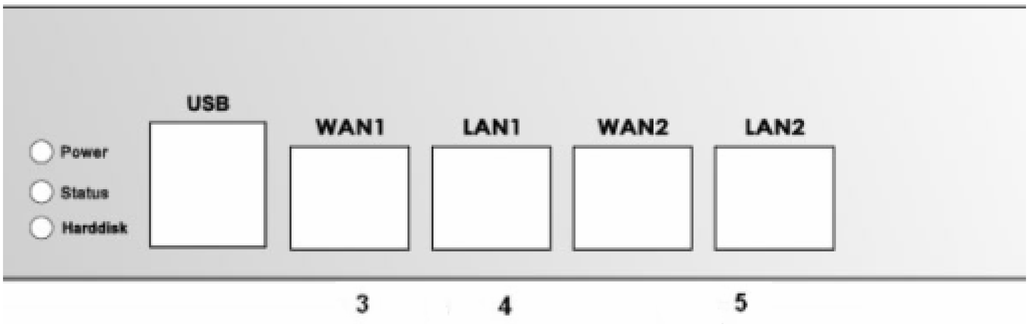
- Standard 10/100BaseT including network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

3.4 Installation Steps

Please follow the steps mentioned below to install the DSA-6100:



1. Connect the power cord to the power socket on the rear panel.
2. Turn on the power switch at the rear panel. The Power LED will light up.



3. Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the Ethernet cable to an ADSL modem, a cable modem or a switch/hub of the internal network. The LED of this WAN1 should light up to indicate a proper connection.
4. Connect an Ethernet cable to LAN1 port with the user authentication function enabled on the front panel. The default port is LAN1 port. The ***LAN1*** port with authentication function is referred to as ***Public LAN***. Connect the other end of the Ethernet cable to an AP or switch. The LED of this LAN1 should light up to indicate a proper connection.
5. Connect an Ethernet cable to LAN2 Port with the user authentication function disabled on the front panel. The ***LAN2*** port without authentication function is referred to as ***Private LAN*** and the administrator can enter the administrative user interface to perform configurations via Private LAN. Connect the other end of the Ethernet cable to a client’s PC. The LED of this LAN2 should light up to indicate a proper connection.

Attention: *Usually a straight RJ-45 can be applied if the DSA-6100 is connected to a hub/computer which supports automatic crossover, such as the Access Point. However, after the Access Point hardware resets, the DSA-6100 may not be able to connect to the Access Point while connecting with a straight cable, unless the cable is pulled out and plug-in again. This scenario does NOT occur while using a crossover cable.*

After the hardware of the DSA-6100 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-6100 to manage the network.

Chapter 4. Web Interface Configuration

This chapter provides further detailed information on setting up the DSA-6100. The administration system allows you to set various networking parameters, such as to enable and to customize network services, to manage user accounts and to monitor user status. The following table shows all the functions of DSA-6100. The administration functions are separated into several categories: System Configuration, Network Configuration, AP Management, User Authentication, Status and Tool.

OPTION	FUNCTION
System Configuration	Configuration Wizard
	System Information
	WAN1 Configuration
	WAN2 & Failover
	LAN1 Configuration
	LAN 2 Configuration
Network Configuration	Network Address Translation
	Privilege List
	Monitor IP List
	Walled Garden List
	Proxy Server Properties
	Dynamic DNS
	IP Mobility
AP Management	AP List
	AP Discovery
	Manual Configuration
	Template Settings
	Firmware Management
	AP Upgrade
User Authentication	Authentication Configuration
	Policy Configuration
	Black List Configuration
	Guest User Configuration
	Additional Configuration

OPTION	FUNCTION
Status	System Status
	Interface Status
	Current Users
	Traffic History
	Notification Configuration
	Online report
Tool	Change Password
	Backup /Restore Setting
	Firmware Upgrade
	Ping Utility
	Restart

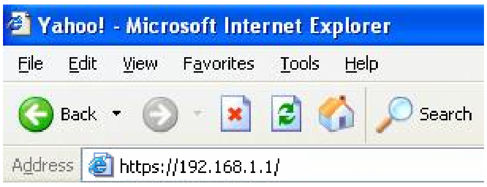
> ***Note:*** *After finishing the configuration, please click* ***Apply*** *and pay attention to see if a restart message appears at the bottom of the screen. If the message appears, the system must be restarted to allow the configurations to take effect. All on-line users will be disconnected during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

- **Web Management Interface**

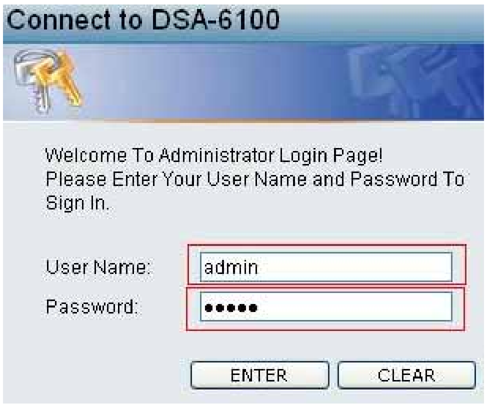
The DSA-6100 provides a web management interface for configuration. After completing the hardware installation, the administrator can configure the DSA-6100 via web browsers with JavaScript enabled such as Internet Explorer version 6.0.

After the basic installation has been completed according to the instructions of the previous chapter, the DSA-6100 can further be configured with the following steps:

1. Use the network cable of the 10/100BaseT to connect a PC to the Private LAN (LAN2), and then start a browser (such as Microsoft IE). Next, enter the gateway address for that port in the opened webpage, the default which is https://192.168.1.1. A login screen will then appear. Enter ***"admin"*** for the default username and password and click ***Enter*** to log in.


Yahoo! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Address
https://192.168.1.1/

Once the DSA-6100 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.

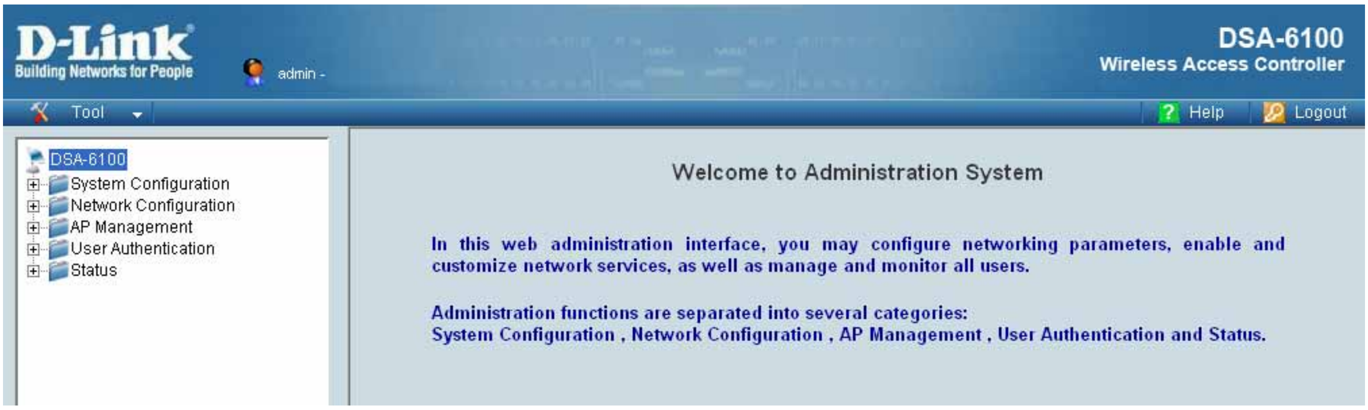


Connect to DSA-6100

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

User Name: admin

Password: •••••



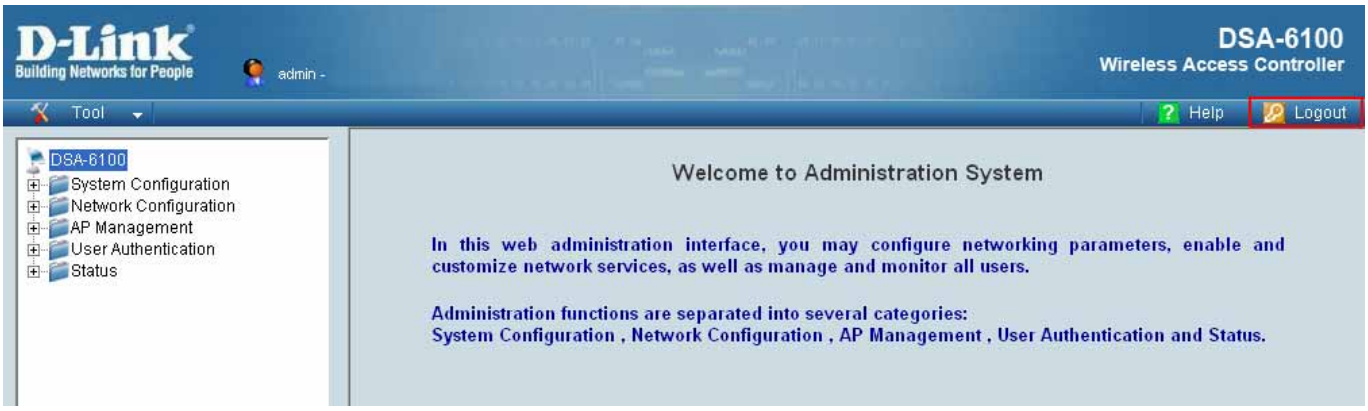
Welcome to Administration System

In this web administration interface, you may configure networking parameters, enable and customize network services, as well as manage and monitor all users.

Administration functions are separated into several categories:
System Configuration , Network Configuration , AP Management , User Authentication and Status.

Note: *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-6100, the **Administration System** page of the web management interface will appear. To log out of the system when completed, select the ***Logout*** icon on the upper right corner of the interface to return to the Administrator Login Page.



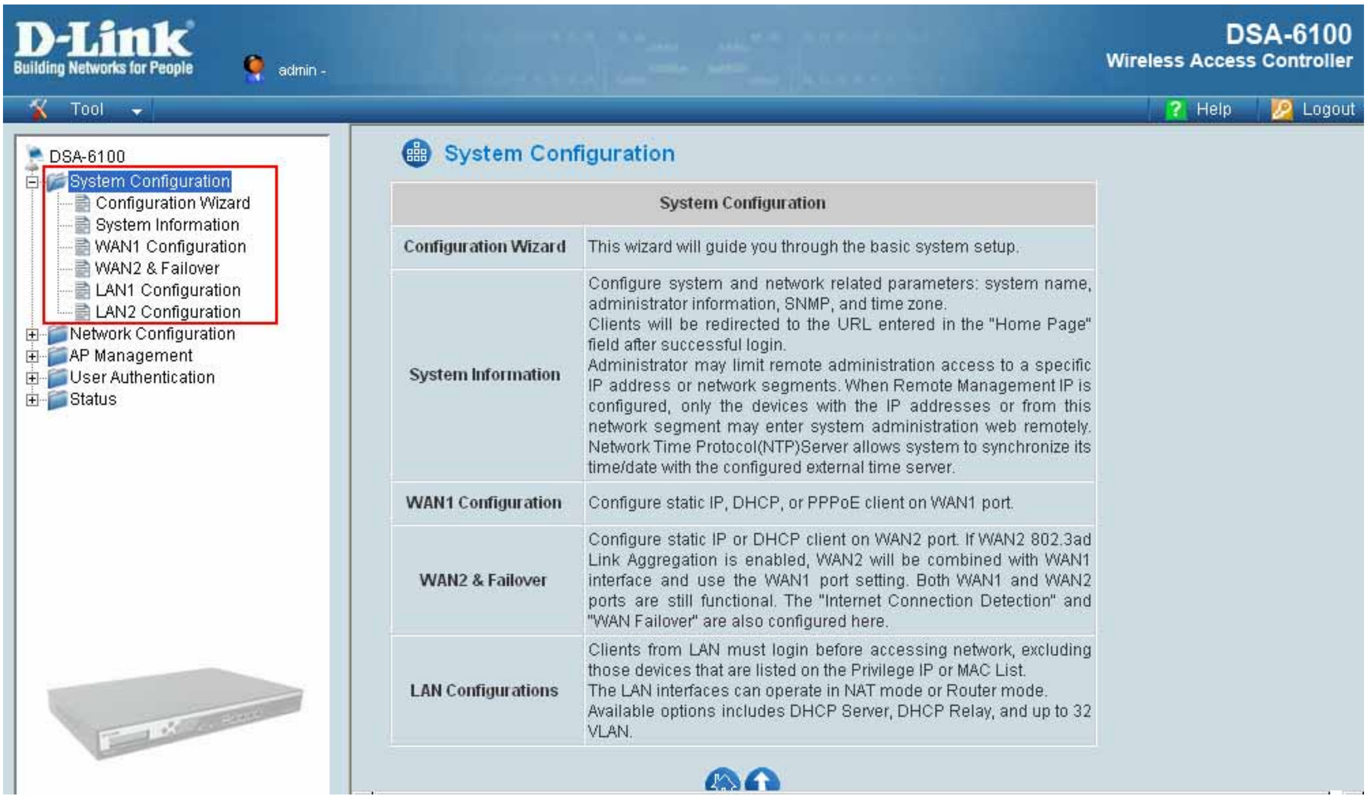
Welcome to Administration System

In this web administration interface, you may configure networking parameters, enable and customize network services, as well as manage and monitor all users.

Administration functions are separated into several categories:
System Configuration , Network Configuration , AP Management , User Authentication and Status.

4.1 System Configuration

This section relates to system configuration and provides the information on the following functions: **Configuration Wizard**, **System Information**, **WAN Configuration** and **LAN Configuration**.



System Configuration

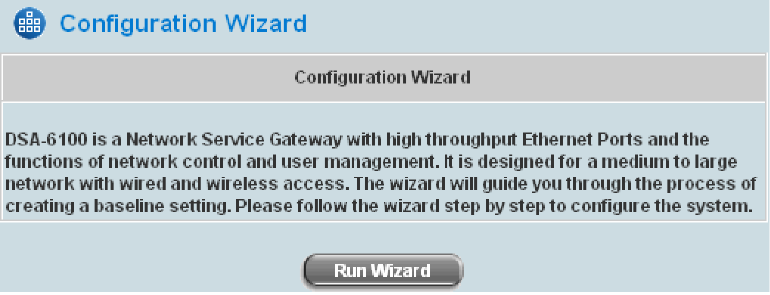
System Configuration	
Configuration Wizard	This wizard will guide you through the basic system setup.
System Information	Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be redirected to the URL entered in the "Home Page" field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When Remote Management IP is configured, only the devices with the IP addresses or from this network segment may enter system administration web remotely. Network Time Protocol(NTP)Server allows system to synchronize its time/date with the configured external time server.
WAN1 Configuration	Configure static IP, DHCP, or PPPoE client on WAN1 port.
WAN2 & Failover	Configure static IP or DHCP client on WAN2 port. If WAN2 802.3ad Link Aggregation is enabled, WAN2 will be combined with WAN1 interface and use the WAN1 port setting. Both WAN1 and WAN2 ports are still functional. The "Internet Connection Detection" and "WAN Failover" are also configured here.
LAN Configurations	Clients from LAN must login before accessing network, excluding those devices that are listed on the Privilege IP or MAC List. The LAN interfaces can operate in NAT mode or Router mode. Available options includes DHCP Server, DHCP Relay, and up to 32 VLAN.

4.1.1 Configuration Wizard (Also served as Quick Installation Guide)

There are two ways to configure the system. One is by using the **Configuration Wizard**, and the other is by changing the setting manually. The Configuration Wizard uses seven simple steps to provide the easy set up of the DSA-6100. These steps may also be used as the Quick Installation Guide. The 7 steps are listed below:

1. Change the Admin Password
2. Choose the System's Time Zone
3. Set the System Information
4. Select the Connection Type for WAN1 Port
5. Configure LAN1
6. Select Authentication Method
7. Restart

Click ***System Configuration*** to go to the **System Configuration** page.
Click the ***System Configuration*** from the left menu, and the **System Configuration** page will appear. Next, click on the buttons, ***Configuration Wizard*** then ***Run Wizard*** to start the wizard.



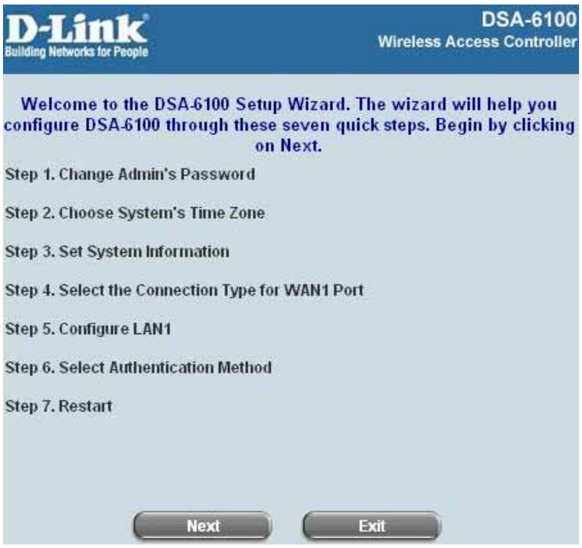
Configuration Wizard

Configuration Wizard

DSA-6100 is a Network Service Gateway with high throughput Ethernet Ports and the functions of network control and user management. It is designed for a medium to large network with wired and wireless access. The wizard will guide you through the process of creating a baseline setting. Please follow the wizard step by step to configure the system.

- **Running the Wizard**

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



Welcome to the DSA-6100 Setup Wizard. The wizard will help you configure DSA-6100 through these seven quick steps. Begin by clicking on Next.

Step 1. Change Admin's Password

Step 2. Choose System's Time Zone

Step 3. Set System Information

Step 4. Select the Connection Type for WAN1 Port

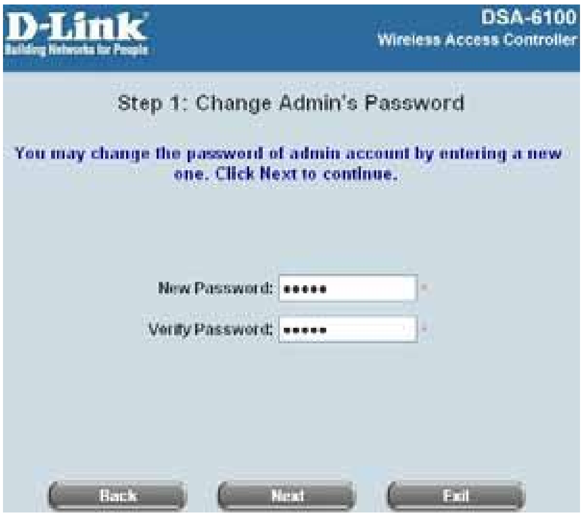
Step 5. Configure LAN1

Step 6. Select Authentication Method

Step 7. Restart

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

  Enter a new password for the admin account and retype it in the *Verify Password* field (twenty-character maximum and no spaces). Click ***Next*** to continue.



Step 1: Change Admin's Password

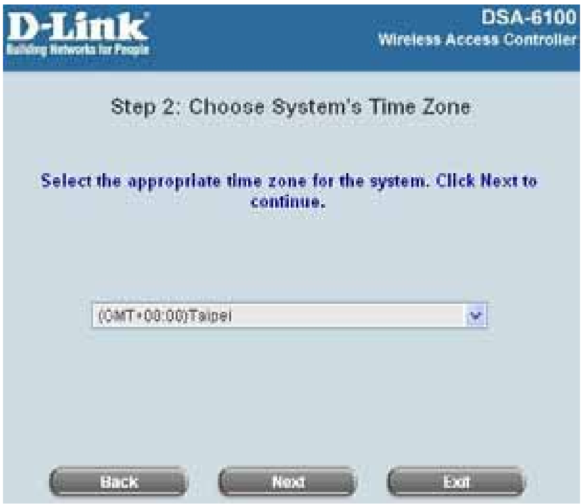
You may change the password of admin account by entering a new one. Click Next to continue.

New Password: ●●●●● *

Verify Password: ●●●●● *

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

  Select a proper time zone via the pull-down menu. Click ***Next*** to continue.



Step 2: Choose System's Time Zone

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

(GMT+08:00)Taipei

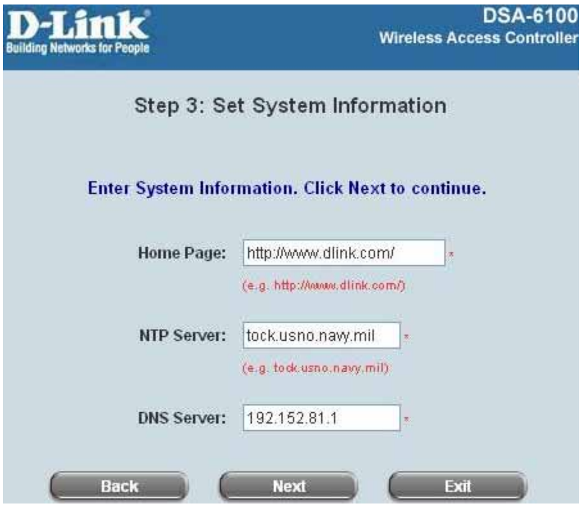
- **Step 3: Set System Information**

  Home Page: Enter the URL to where the clients should be directed when they are properly authenticated.

  NTP Server: Enter the URL of the external time server for the DSA-6100 time synchronization or use the default.

  DNS Server: Enter a DNS Server provided by the ISP (Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.

  Click ***Next*** to continue.



Step 3: Set System Information

Enter System Information. Click Next to continue.

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

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

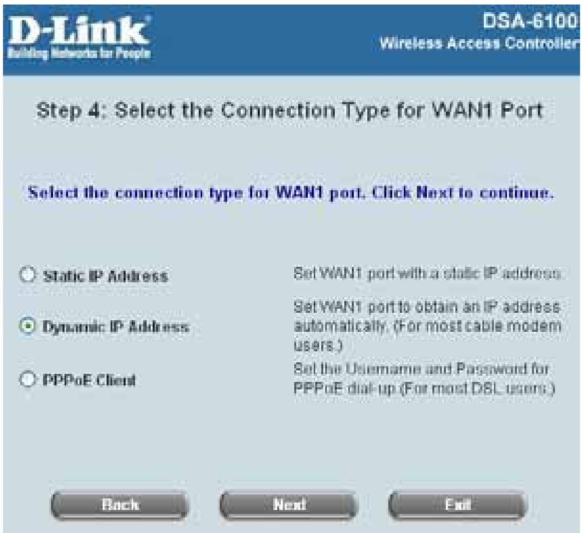
DNS Server: 192.152.81.1 *

- **Step 4: Select the Connection Type for WAN1 Port**

  There are three types of WAN port to select: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**. Select a proper Internet connection type and click ***Next*** to continue.

  - **Dynamic IP Address**

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



Step 4: Select the Connection Type for WAN1 Port

Select the connection type for WAN1 port. Click Next to continue.

○ Static IP Address — Set WAN1 port with a static IP address.

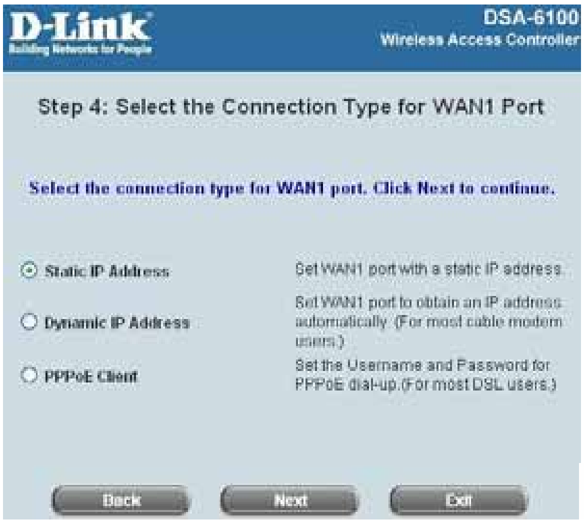
● Dynamic IP Address — Set WAN1 port to obtain an IP address automatically. (For most cable modem users.)

○ PPPoE Client — Set the Username and Password for PPPoE dial-up (For most DSL users.)

  - **Static IP Address: Set WAN1 Port’s Static IP Address**

    Enter the **“IP Address”**, **“Subnet Mask”** and **“Default Gateway”** provided by the ISP.

    Click ***Next*** to continue.



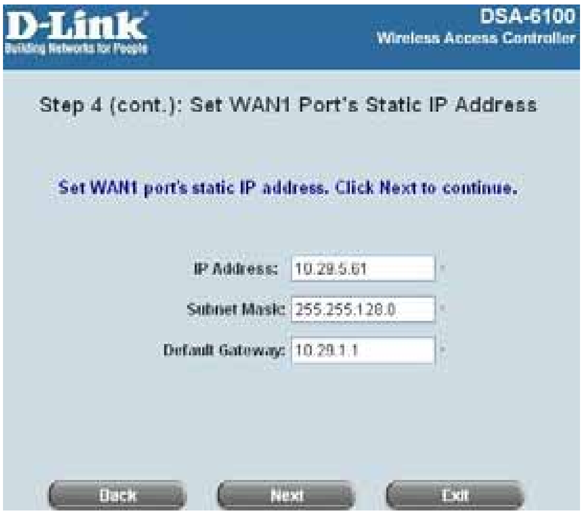
Step 4: Select the Connection Type for WAN1 Port

Select the connection type for WAN1 port. Click Next to continue.

● Static IP Address — Set WAN1 port with a static IP address.

○ Dynamic IP Address — Set WAN1 port to obtain an IP address automatically. (For most cable modem users.)

○ PPPoE Client — Set the Username and Password for PPPoE dial-up.(For most DSL users.)



Step 4 (cont.): Set WAN1 Port's Static IP Address

Set WAN1 port's static IP address. Click Next to continue.

IP Address: 10.29.5.61 *

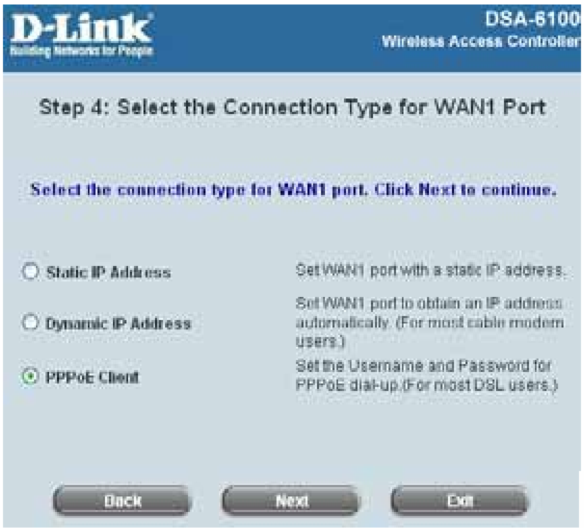
Subnet Mask: 255.255.128.0 *

Default Gateway: 10.29.1.1 *

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

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

  Click ***Next*** to continue.



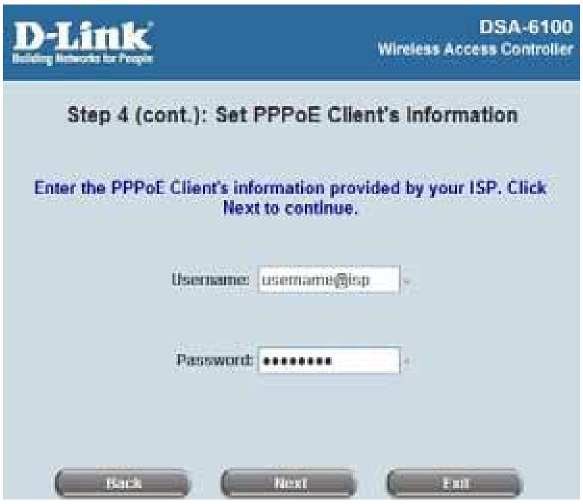
Step 4: Select the Connection Type for WAN1 Port

Select the connection type for WAN1 port. Click Next to continue.

○ Static IP Address — Set WAN1 port with a static IP address.

○ Dynamic IP Address — Set WAN1 port to obtain an IP address automatically. (For most cable modem users.)

● PPPoE Client — Set the Username and Password for PPPoE dial-up.(For most DSL users.)



Step 4 (cont.): Set PPPoE Client's Information

Enter the PPPoE Client's information provided by your ISP. Click Next to continue.

Username: username@isp

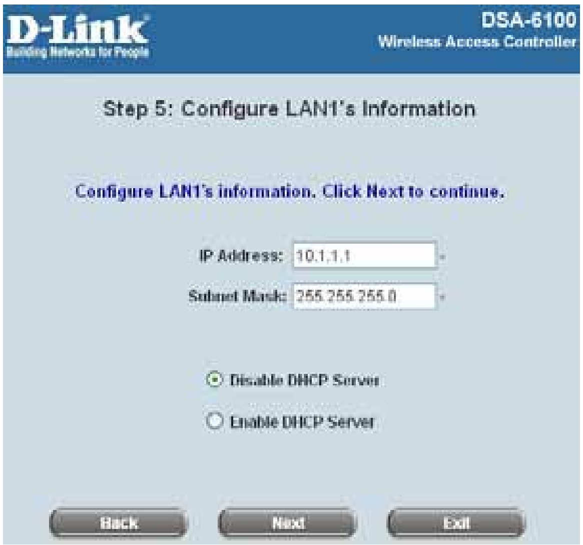
Password: ••••••••

- **Step 5: Configure LAN1's Information**

  IP Address: Enter the Public LAN port IP Address or use the default.

  Subnet Mask: Enter the Public port Subnet Mask or use the default.

  Disable DHCP Server: If the DHCP server is disabled, the Public LAN clients must be configured with an IP address manually.



Step 5: Configure LAN1's Information

Configure LAN1's information. Click Next to continue.

IP Address: 10.1.1.1

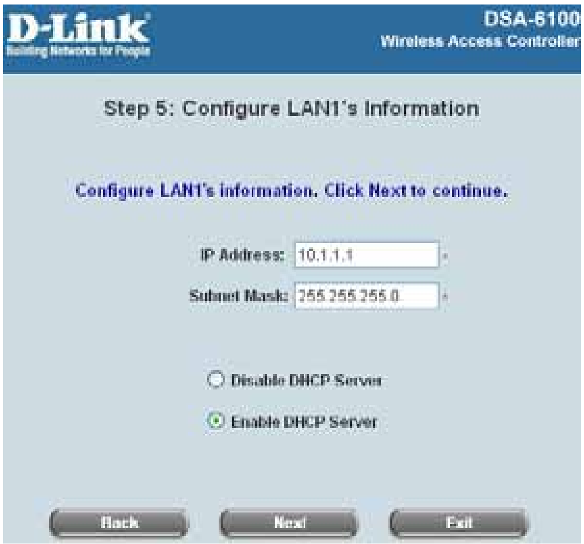
Subnet Mask: 255.255.255.0

● Disable DHCP Server

○ Enable DHCP Server

Enable DHCP Server: When the option is selected, the DSA-6100 will automatically provide the necessary IP address to all Public LAN clients.

Click ***Next*** to continue.



Step 5: Configure LAN1's Information

Configure LAN1's information. Click Next to continue.

IP Address: 10.1.1.1 *

Subnet Mask: 255.255.255.0 *

○ Disable DHCP Server

● Enable DHCP Server

- **Step 5 (cont.): Set LAN1 DHCP Server**

If the *Enable DHCP Server* option is selected, more information about the LAN1 DHCP server will be needed. Fields marked with red asterisks must be filled in.

Start IP Address: The start IP address of the DHCP scope of LAN1.

End IP Address: The end IP address of the DHCP scope of LAN1.

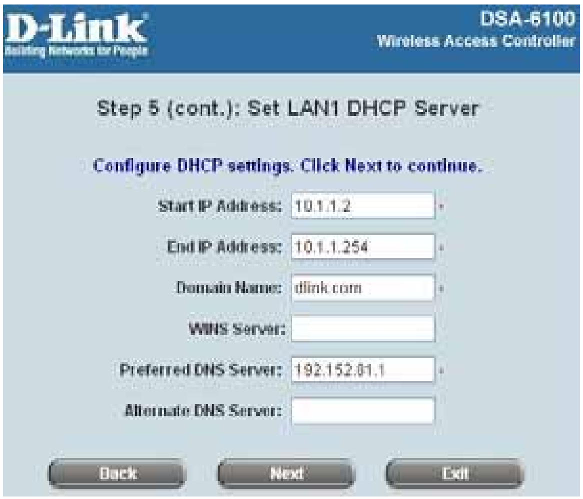
These IP address will be assigned to the LAN1 clients. ***(Note: Be sure that IP address assigned in this range is NOT used in other setting of DSA-6100.)***

Domain Name: Enter a domain name provided by your ISP (e.g. dlink.com).

WINS Server: Enter the IP address of the WINS server.(Windows Internet Naming Service Server) This field is optional.

Preferred DNS Server: The DNS Server settings are provided by your ISP. Only the Preferred DNS Server field is mandatory. Contact your ISP if you are unsure of the DNS Server settings.

Alternate DNS Server: The DNS Server settings are provided by your ISP. The field is optional. Click ***Next*** to continue.



Step 5 (cont.): Set LAN1 DHCP Server

Configure DHCP settings. Click Next to continue.

Start IP Address: 10.1.1.2 *

End IP Address: 10.1.1.254 *

Domain Name: dlink.com *

WINS Server:

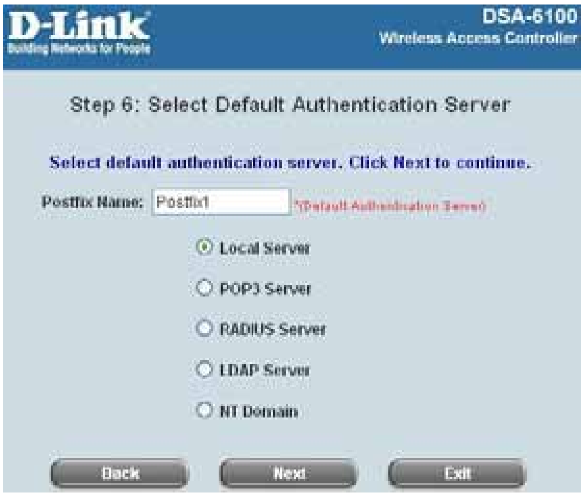
Preferred DNS Server: 192.152.81.1 *

Alternate DNS Server:

- **Step 6: Select Default Authentication Server**

  Please specify the postfix name for this authentication method. The ***Postfix Name*** field (e.g. Local) will be used as the postfix name (e.g. username@Local). An authentication method has to be selected from one of the five options appeared in this window (Local User is selected for this setup example).

  Click ***Next*** to continue.



Step 6: Select Default Authentication Server

Select default authentication server. Click Next to continue.

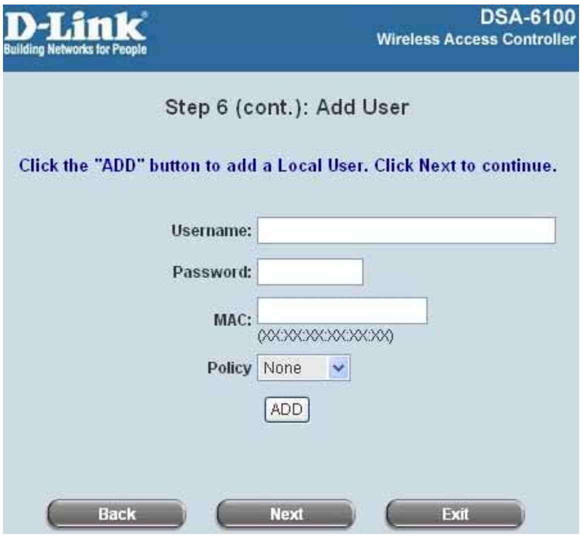
Postfix Name: Postfix1 *(Default Authentication Server)

● Local Server
○ POP3 Server
○ RADIUS Server
○ LDAP Server
○ NT Domain

▪ **Local User - Add User**

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

  Click ***Next*** to continue.



Step 6 (cont.): Add User

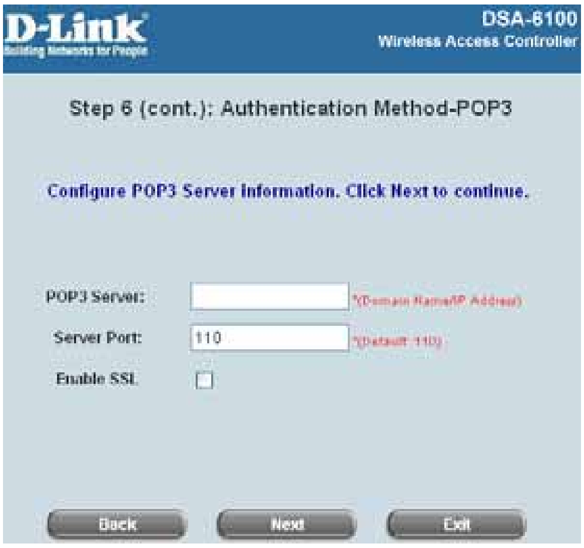
Click the "ADD" button to add a Local User. Click Next to continue.

Username:
Password:
MAC: (XX:XX:XX:XX:XX:XX)
Policy None

- **User Authentication Method-POP3**

  Enter IP/Domain Name and server port of the POP3 server provided by the ISP, and then choose enable SSL or not.

  Click ***Next*** to continue.



Step 6 (cont.): Authentication Method-POP3

Configure POP3 Server Information. Click Next to continue.

POP3 Server: *(Domain Name/IP Address)

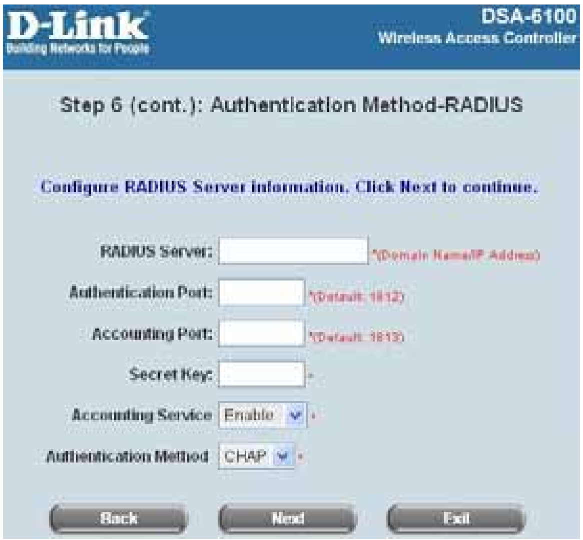
Server Port: 110 *(Default: 110)

Enable SSL □

- **User Authentication Method-RADIUS**

  Enter RADIUS server IP/Domain Name, authentication port, accounting port and secret key, then choose whether to enable accounting service. Next, choose the desired authentication method.

  Click ***Next*** to continue.



Step 6 (cont.): Authentication Method-RADIUS

Configure RADIUS Server information. Click Next to continue.

RADIUS Server: *(Domain Name/IP Address)

Authentication Port: *(Default: 1812)

Accounting Port: *(Default: 1813)

Secret Key: *

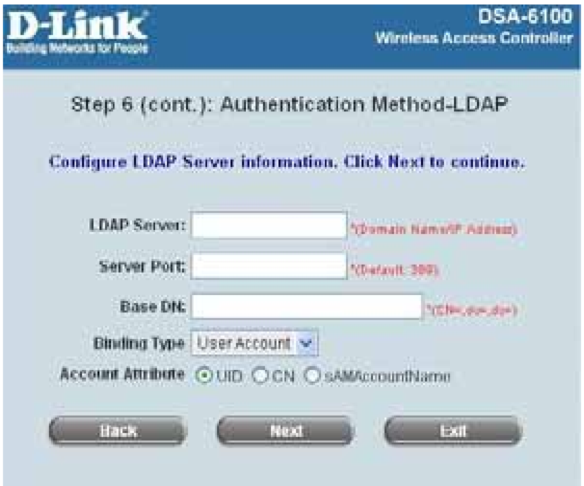
Accounting Service: Enable *

Authentication Method: CHAP *

- **User Authentication Method-LDAP**

  Add a new user to the LDAP user database. Enter the **"LDAP Server"**, **"Server Port"** and **"Base DN"** and select one kind of **Binding Type** and **Account Attribute** to access the LDAP server.

  If the **User Account** binding type is selected, the system will use the **Base DN** to be the user account to access the LDAP server.



Step 6 (cont.): Authentication Method-LDAP

Configure LDAP Server information. Click Next to continue.

LDAP Server: *(Domain Name/IP Address)

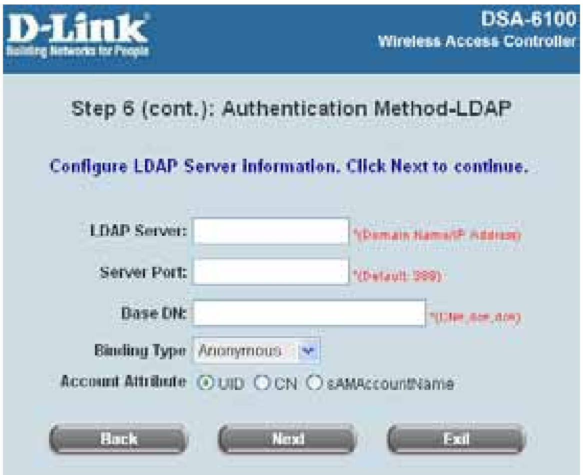
Server Port: *(Default: 389)

Base DN: *(CN=,dc=,dc=)

Binding Type: User Account

Account Attribute: ● UID ○ CN ○ sAMAccountName

- If **Anonymous** binding type is selected, the system will access the LDAP servers without requiring authentication.



Step 6 (cont.): Authentication Method-LDAP

Configure LDAP Server information. Click Next to continue.

LDAP Server: *(Domain Name/IP Address)

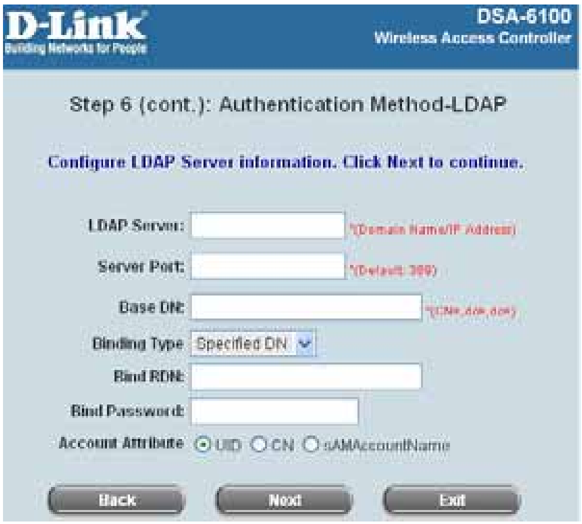
Server Port: *(Default: 389)

Base DN: *(CN=,dc=,dc=)

Binding Type: Anonymous

Account Attribute: ● UID ○ CN ○ sAMAccountName

- If **Specific DN** binding type is selected, ***username*** and ***password*** in the **"Bind RDN"** and **"Bind Password"** fields must be entered to access the LDAP server.



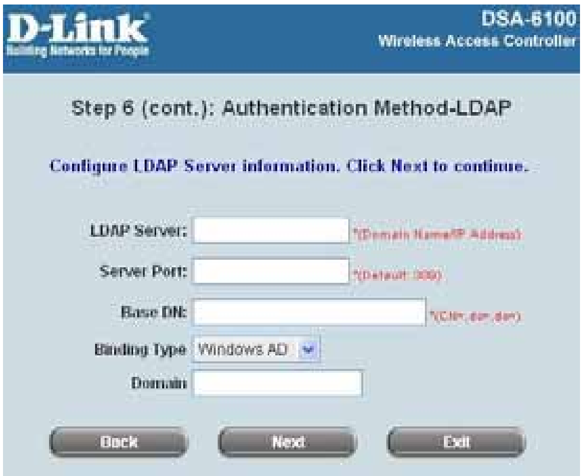
Step 6 (cont.): Authentication Method-LDAP

Configure LDAP Server information. Click Next to continue.

LDAP Server: *(Domain Name/IP Address)
Server Port: *(Default: 389)
Base DN: *(CN=,dc=,dc=)
Binding Type: Specified DN
Bind RDN:
Bind Password:
Account Attribute ● UID ○ CN ○ sAMAccountName

- If **Windows AD** binding type is selected, please enter the domain name of Windows AD to access the LDAP server.

Click ***Next*** to continue.



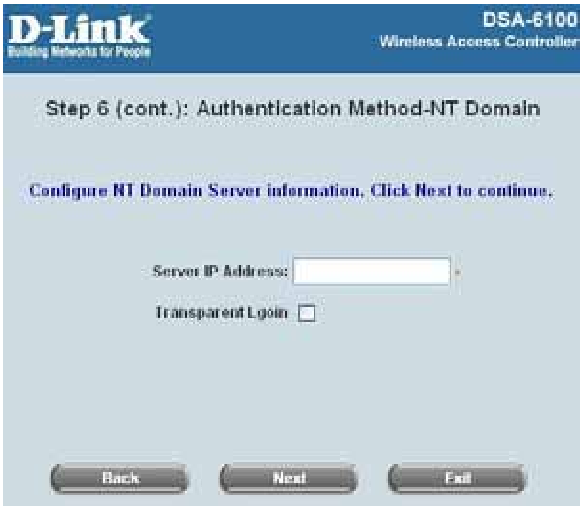
Step 6 (cont.): Authentication Method-LDAP

Configure LDAP Server information. Click Next to continue.

LDAP Server: *(Domain Name/IP Address)
Server Port: *(Default: 389)
Base DN: *(CN=,dc=,dc=)
Binding Type: Windows AD
Domain:

- **User Authentication Method-NT Domain**

  When NT Domain User is selected, enter the information for **"Server IP Address"**, and enable/disable **"Transparent Login"**. After this setup is completed, click ***Next*** to continue.



Step 6 (cont.): Authentication Method-NT Domain

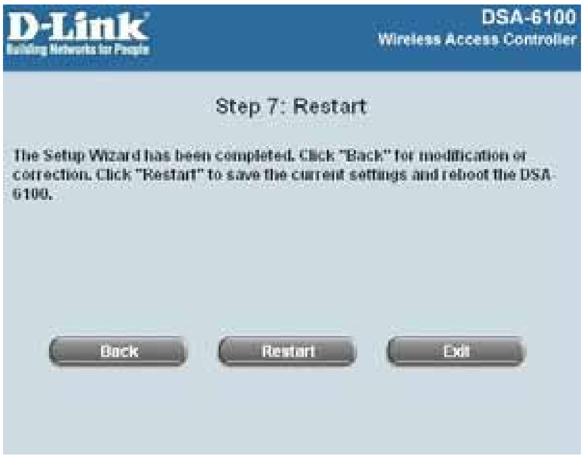
Configure NT Domain Server information. Click Next to continue.

Server IP Address: *

Transparent Lgoin □

- **Step 7: Restart**

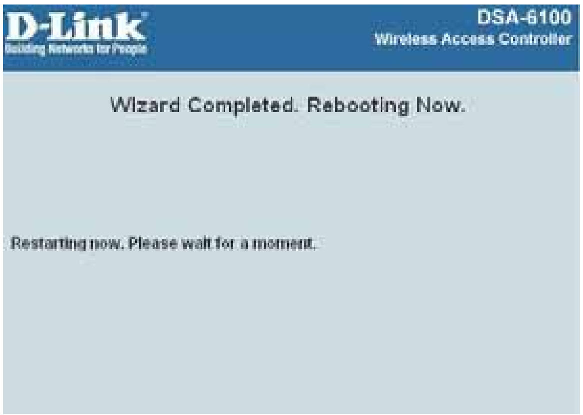
  Click ***Restart*** to save the current settings and restart DSA-6100. The Setup Wizard is now completed.



Step 7: Restart

The Setup Wizard has been completed. Click "Back" for modification or correction. Click "Restart" to save the current settings and reboot the DSA-6100.

- During the DSA-6100 restarting, a ***"Restarting now. Please wait for a moment."*** message will appear on the screen. Please do not interrupt the DSA-6100 until the ***Configuration Wizard*** has disappeared. This indicates that the restart process has been completed.



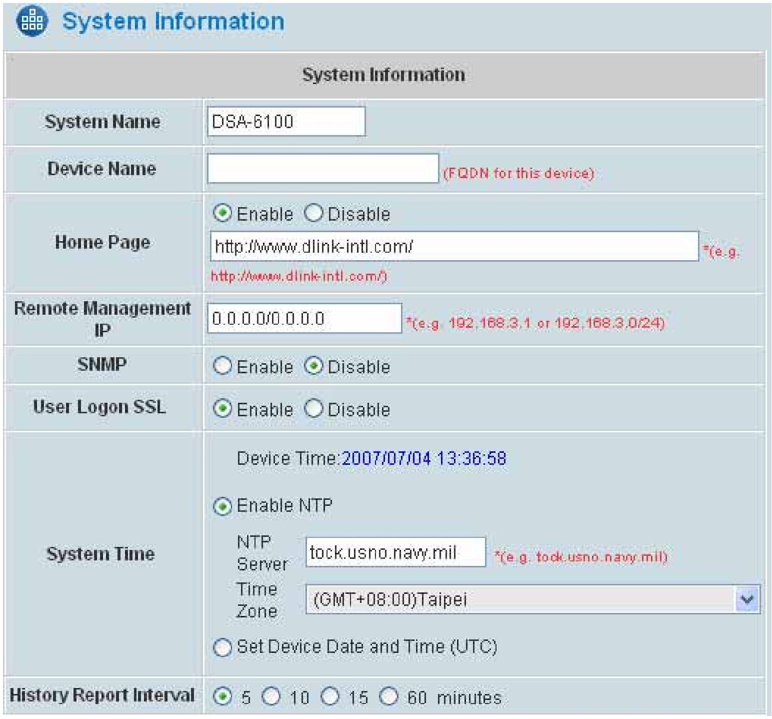
Wizard Completed. Rebooting Now.

Restarting now. Please wait for a moment.

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.*

4.1.2 System Information

The system and network related parameters such as System Name, Device Name, Homepage Redirect URL, Management IP Address List, and User Logon SSL can be configured from the menu as shown below.



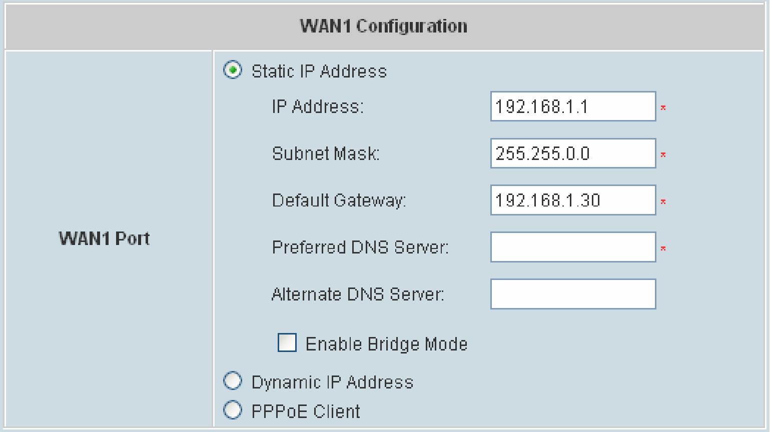
System Information

System Information	
System Name	DSA-6100
Device Name	(FQDN for this device)
Home Page	● Enable ○ Disable http://www.dlink-intl.com/ *(e.g. http://www.dlink-intl.com/)
Remote Management IP	0.0.0.0/0.0.0.0 *(e.g. 192.168.3.1 or 192.168.3.0/24)
SNMP	○ Enable ● Disable
User Logon SSL	● Enable ○ Disable
System Time	Device Time:2007/07/04 13:36:58 ● Enable NTP NTP Server: tock.usno.navy.mil *(e.g. tock.usno.navy.mil) Time Zone: (GMT+08:00)Taipei ○ Set Device Date and Time (UTC)
History Report Interval	● 5 ○ 10 ○ 15 ○ 60 minutes

- **System Name:** The name of this system. Set the system's name or use the default.
- **Device Name:** FQDN (Fully-Qualified Domain Name). This is the domain name used in login page. For example, if Device Name is dlink.com, the URL of login page will be https://dlink.com/loginpages/login.shtml.
- **Home Page:** Enter the website of a Web Server to be the homepage. User will be directed to this webpage after successful login. Usually, the homepage is the company's website, such as http://www.dlink.com. Regardless of the original webpage set in the users' computer, they will be redirected to this page after login.
- **Remote Management IP:** Set the IP Address or the IP Subnet with a system which is able to connect to the web management interface via the authenticated port. For example: 10.2.3.0/24 means that as long as an administrator is within the IP address range of 10.2.3.0/24, he or she can reach the administration page of the DSA-6100. If the administrator configures a single IP, such as 10.2.3.5, only this IP address can reach the administration page.
- **SNMP:** Configure IP address and Community ID of external SNMP management device. This system supports SNMP v.3.
- **User Logon SSL:** Enable SSL, HTTPS or disable HTTP when user login with encryption to have a safer login process.
- **System Time:** DSA-6100 supports NTP communication protocol to synchronize the network time. Please specify the IP address of a server and select the desired time zone in the system configuration interface for adjusting the time automatically. (Universal Time is Greenwich Mean Time, GMT). Time can also be set manually when by selecting **"Set Device Date and Time"**. Please enter the date and time for these fields.
- **History Report Interval:** Time interval to update length of minutes that traffic log in the Traffic History page will be updated by the unit.

4.1.3 WAN1 Configuration

System supports three different WAN connection types for the WAN1 Port configuration including: **Static IP Address**, **Dynamic IP Address**, and **PPPoE Client**.



WAN1 Configuration

WAN1 Port

● Static IP Address

IP Address: 192.168.1.1 *

Subnet Mask: 255.255.0.0 *

Default Gateway: 192.168.1.30 *

Preferred DNS Server: *

Alternate DNS Server:

□ Enable Bridge Mode

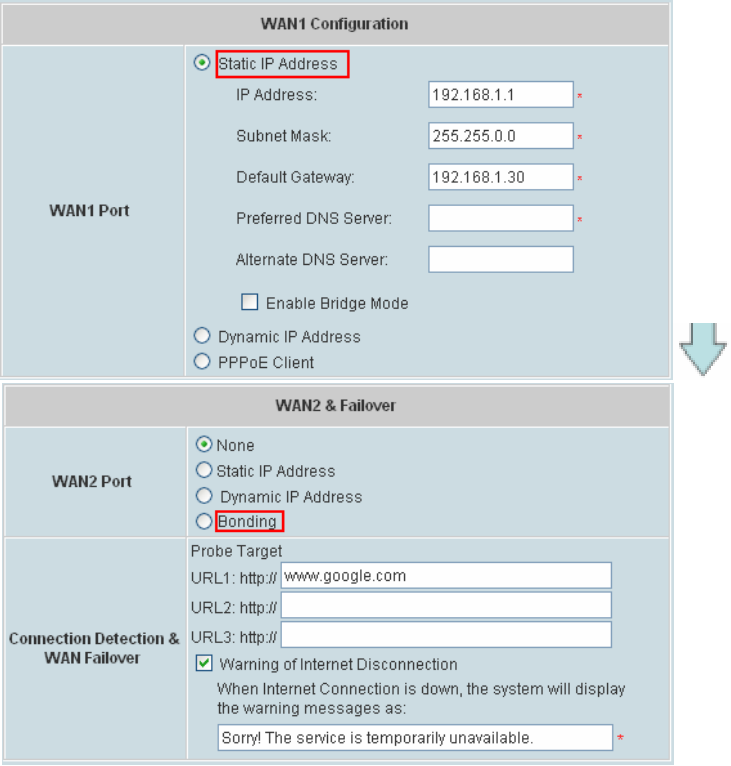
○ Dynamic IP Address

○ PPPoE Client

- **Static IP Address:** Manually specifying the IP address of the WAN1 Port regarding your ISP network information, which is applicable for the network environment where IP address cannot be obtained automatically.

Note: *The option of Bonding for WAN2 is only available when WAN1 is set to static IP address.*

The fields with red asterisks are required. Please fill in these fields.



WAN1 Configuration

WAN1 Port

● Static IP Address

IP Address: 192.168.1.1 *

Subnet Mask: 255.255.0.0 *

Default Gateway: 192.168.1.30 *

Preferred DNS Server: *

Alternate DNS Server:

□ Enable Bridge Mode

○ Dynamic IP Address

○ PPPoE Client

WAN2 & Failover

WAN2 Port

● None

○ Static IP Address

○ Dynamic IP Address

○ Bonding

Connection Detection & WAN Failover

Probe Target

URL1: http:// www.google.com

URL2: http://

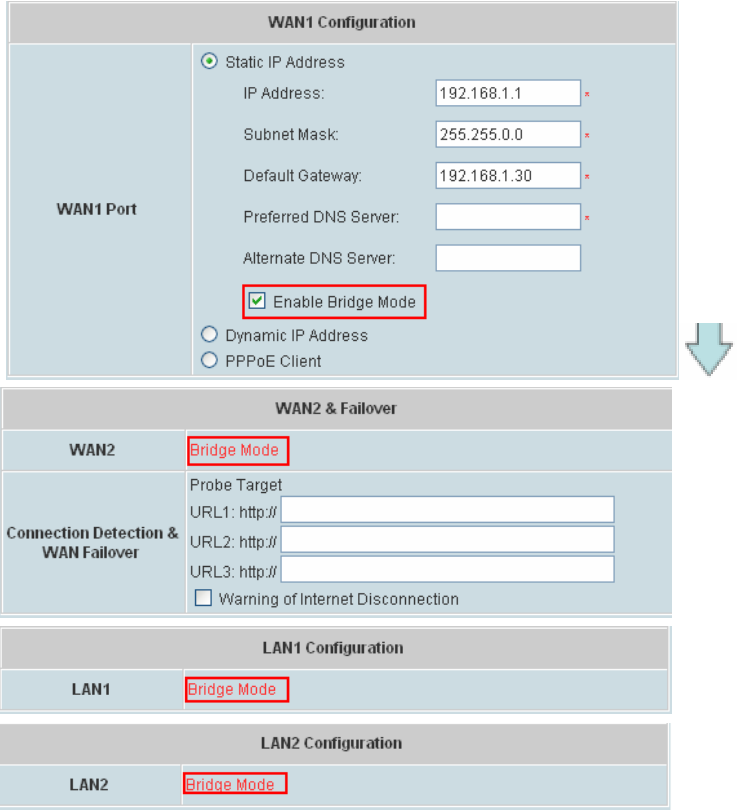
URL3: http://

☑ Warning of Internet Disconnection

When Internet Connection is down, the system will display the warning messages as:

Sorry! The service is temporarily unavailable. *

- **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 not required.
- **Enable Bridge Mode:** Bridge all WAN and LAN interfaces. These interfaces will be in the same network segment. When the WAN1 is set to use a static IP address and **"Enable Bridge Mode"** is checked, the DSA-6100 will act as a switch and WAN2, LAN1 and LAN2 ports will share the same static IP address from WAN1. The pictures below are the results on the WAN2 and LAN2 when Bridge Mode is enabled on the WAN1 interface.



WAN1 Configuration

WAN1 Port

● Static IP Address

IP Address:	192.168.1.1 *
Subnet Mask:	255.255.0.0 *
Default Gateway:	192.168.1.30 *
Preferred DNS Server:	*
Alternate DNS Server:	

☑ Enable Bridge Mode

○ Dynamic IP Address

○ PPPoE Client

WAN2 & Failover

WAN2	Bridge Mode
Connection Detection & WAN Failover	Probe Target URL1: http:// URL2: http:// URL3: http:// □ Warning of Internet Disconnection

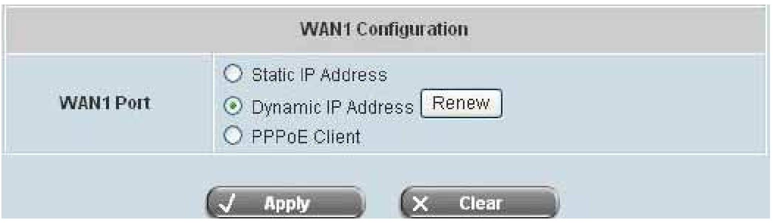
LAN1 Configuration

LAN1	Bridge Mode

LAN2 Configuration

LAN2	Bridge Mode

- **Dynamic IP address:** Configure WAN port settings automatically using external DHCP Server. It is only applicable for the network environment where the DHCP Server is available in the network. Click the ***Renew*** button to get an IP address.



WAN1 Configuration

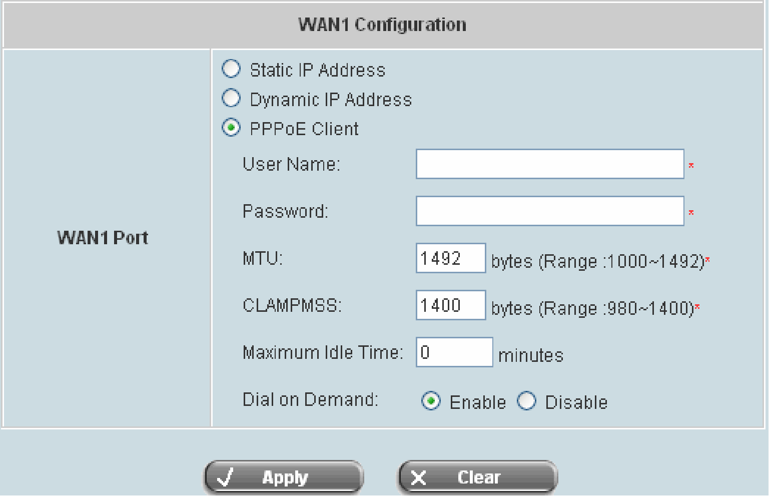
WAN1 Port

○ Static IP Address

● Dynamic IP Address Renew

○ PPPoE Client

- **PPPoE Client:** Common ADSL connection type. Enter User Name and Password of your PPPoE account. When dial on Demand is enabled, you can set the idle timer before the system is disconnected from the Internet. When selecting PPPoE to connect to the network, please set the **"User Name"** and **"Password"** from your ISP to access the network. There is a **Dial on demand** function under PPPoE and if this function is enabled, you can set a **Maximum Idle Time**. When the idle time is reached, the system will automatically disconnect itself.



WAN1 Configuration

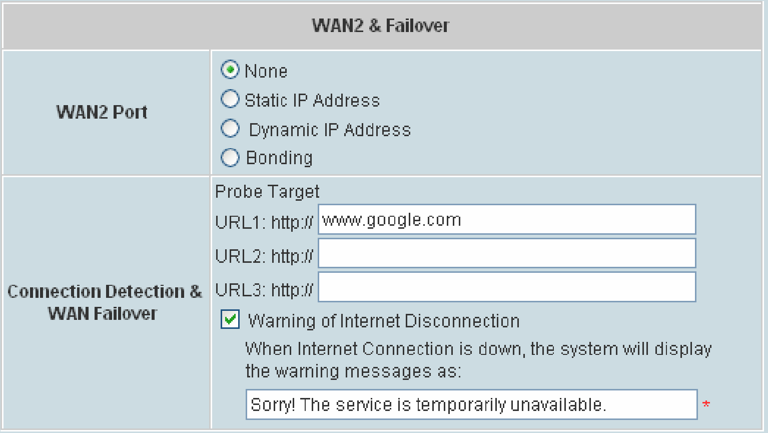
WAN1 Port

○ Static IP Address
○ Dynamic IP Address
● PPPoE Client

User Name: *
Password: *
MTU: 1492 bytes (Range :1000~1492)*
CLAMPMSS: 1400 bytes (Range :980~1400)*
Maximum Idle Time: 0 minutes
Dial on Demand: ● Enable ○ Disable

4.1.4 WAN2 & Failover

WAN2 can be configured to one of the following types: **None**, **Static IP Address**, **Dynamic IP Address** and **Bonding**. **None** means that WAN2 Port is disabled. **Bonding** is shown as one of the option when WAN1 is set to Static IP Address.



WAN2 & Failover

WAN2 Port	● None ○ Static IP Address ○ Dynamic IP Address ○ Bonding
Connection Detection & WAN Failover	Probe Target URL1: http:// www.google.com URL2: http:// URL3: http:// ☑ Warning of Internet Disconnection When Internet Connection is down, the system will display the warning messages as: Sorry! The service is temporarily unavailable. *

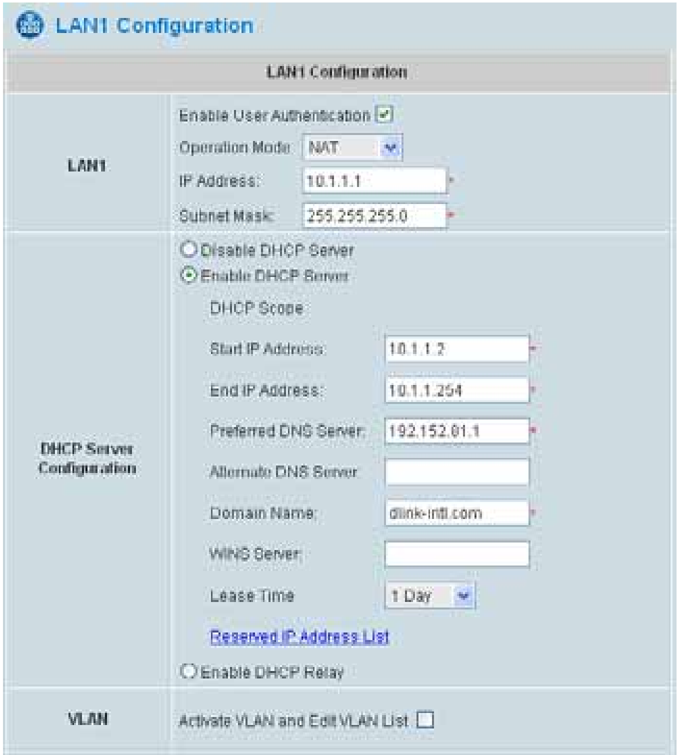
- **WAN2 Port:**
  - **None:** No WAN2 connection or WAN2 connection is disabled
  - **Static IP Address, Dynamic IP Address:** Please refer to WAN1 Port settings
  - **Bonding:** When enabled, it allows administrators to increase the uplink bandwidth capacity beyond the capacity of one single WAN port (WAN1 and WAN2 links are combined and outgoing packets are transmitted in a specific round-robin order)

***Note:** The option of **Bonding** is only available when WAN1 is set to **Static IP Address**.*

- **Connection Detection & WAN Failover:**
  - **Probe Target:** To verify the connection to the Internet, the system keeps up to three target URLs. These URLs are used for the system as the detect targets of WAN Failover and Warning of Internet Disconnection. At least one URL is required for the system to verify the Internet connection.
  - **WAN Failover:** When enabled and WAN1 connection fails, the traffic will be routed to WAN2 automatically. If the **Fallback to WAN1 when possible** function is enabled, and WAN1 connection is recovered, the routed traffic will return to WAN1.
  - **Warning of Internet Disconnection:** When enabled, the reminding message will appear on clients' screens when Internet connection is down.

4.1.5 LAN1 Configuration

LAN1 is required to obtain authentication (this configuration can be disabled). In this section, you will be advised on how to set the related configurations of LAN1 port and DHCP server.



LAN1 Configuration

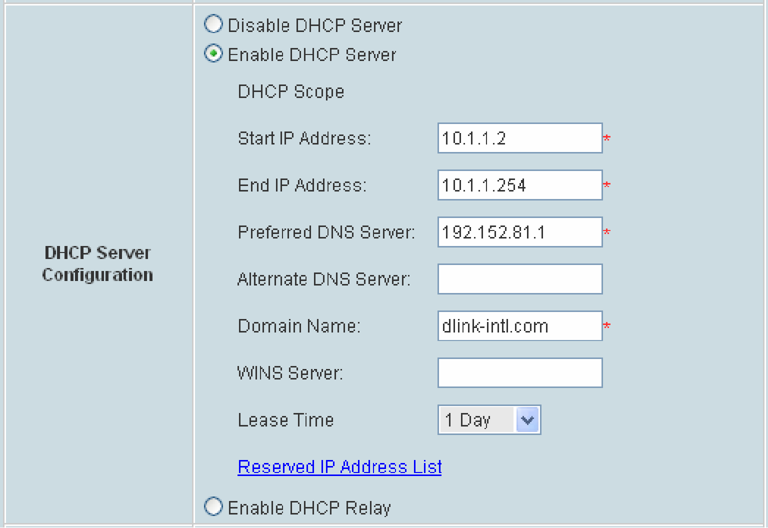
LAN1 Configuration	
LAN1	Enable User Authentication ☑ Operation Mode: NAT IP Address: 10.1.1.1 * Subnet Mask: 255.255.255.0 *
DHCP Server Configuration	○ Disable DHCP Server ● Enable DHCP Server DHCP Scope Start IP Address: 10.1.1.2 * End IP Address: 10.1.1.254 * Preferred DNS Server: 192.152.81.1 * Alternate DNS Server: Domain Name: dlink-intl.com * WINS Server: Lease Time: 1 Day Reserved IP Address List ○ Enable DHCP Relay
VLAN	Activate VLAN and Edit VLAN List □

LAN1: These are the basic, global configuration options for LAN1 port.

- **Enable User Authentication:** When enabled, users on the LAN1 interface are required to log in before accessing the network. By default, user authentication under LAN1 port is required.
- **Operation Mode:** The system supports NAT mode and Route Mode.
  NAT: All IP addresses of internal hosts connected to the LAN1 port, where the internal hosts belong to the same network as the LAN1 interface, will be converted into the IP address of the WAN1 interface by the DSA-6100 and onward to outside the network.
  ROUTER: All IP addresses of internal hosts connected to the LAN1 interface will remain the same while the IP packets travel through WAN1 interface, thus making the DSA-6100 act like a router.
- **IP Address:** IP address of each network interface.
- **Subnet Mask:** Subnet Mask of the LAN/VLAN interface.

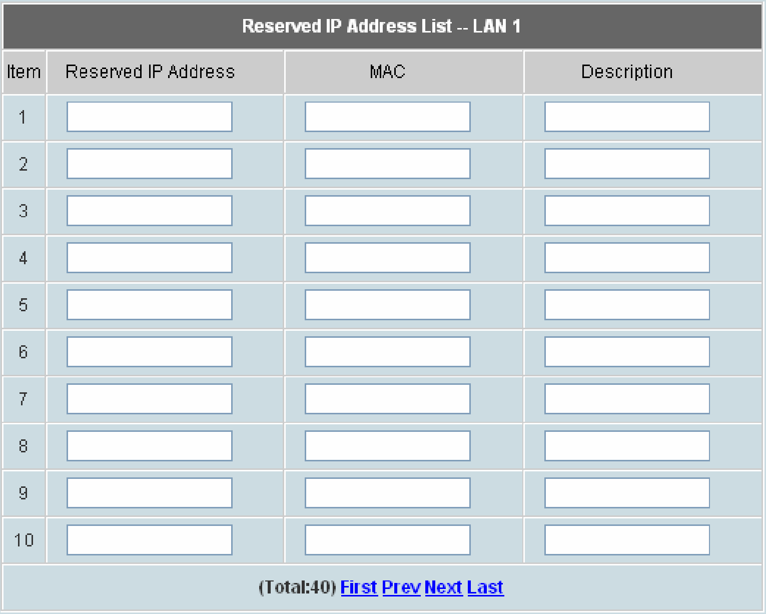
DHCP Server Configuration: DHCP options for LAN1 port include Disable, Enable, and Relay.

- **Disable DHCP Server:** Disable the function of the DHCP Server.
- **Enable DHCP Server:** When enabled, related information has to be filled in properly: DHCP Pool Start IP Address, DHCP Pools End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Server, Lease Time, and Reserved IP Address List.



DHCP Server Configuration	○ Disable DHCP Server ● Enable DHCP Server DHCP Scope Start IP Address: 10.1.1.2 * End IP Address: 10.1.1.254 * Preferred DNS Server: 192.152.81.1 * Alternate DNS Server: Domain Name: dlink-intl.com * WINS Server: Lease Time: 1 Day Reserved IP Address List ○ Enable DHCP Relay

If you want to use the reserved IP address function, click on the **Reserved IP Address List**. The setup menu of the Reserved IP Address List will appear, as shown in the following picture. Enter the related Reserved IP Address, the MAC Address of the client, and some Description (optional). When finished, click ***Apply*** to complete the setup. The list reserves IP addresses from predefined DHCP Scope and prevents systems from issuing these IP address to downstream users.

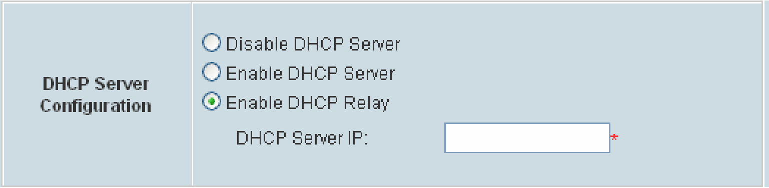


Reserved IP Address List -- LAN 1

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

(Total:40) First Prev Next Last

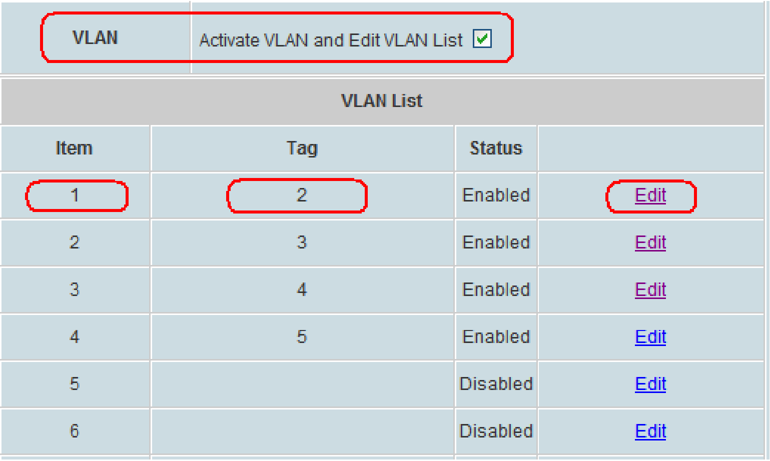
- **Enable DHCP Relay**: Specify the IP address of the DHCP Relay Server.



DHCP Server Configuration	○ Disable DHCP Server ○ Enable DHCP Server ● Enable DHCP Relay DHCP Server IP: ____ *

VLAN: In the VLAN mode, the LAN interface can be separated into several virtual LAN interfaces. It allows switches to assign end stations to different virtual LANs.

- **Activate VLAN and Edit VLAN List:** Select the check box to activate the VLAN. Thereafter, on the VLAN List, 32 VLANs can be configured accordingly. Select the desired Item and click ***Edit*** to configure the VLAN.

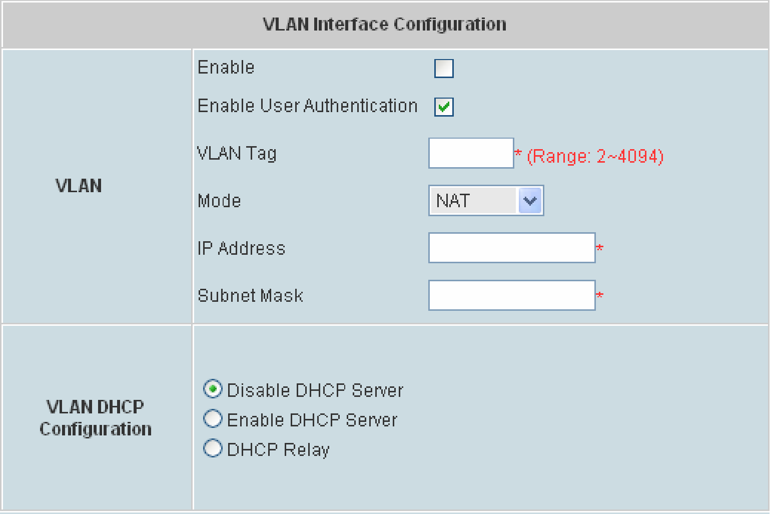


VLAN — Activate VLAN and Edit VLAN List ☑

VLAN List

Item	Tag	Status	
1	2	Enabled	Edit
2	3	Enabled	Edit
3	4	Enabled	Edit
4	5	Enabled	Edit
5		Disabled	Edit
6		Disabled	Edit

VLAN Interface Configuration for LAN1:



VLAN Interface Configuration

VLAN	Enable	□
	Enable User Authentication	☑
	VLAN Tag	____ * (Range: 2~4094)
	Mode	NAT
	IP Address	____ *
	Subnet Mask	____ *
VLAN DHCP Configuration	● Disable DHCP Server ○ Enable DHCP Server ○ DHCP Relay	

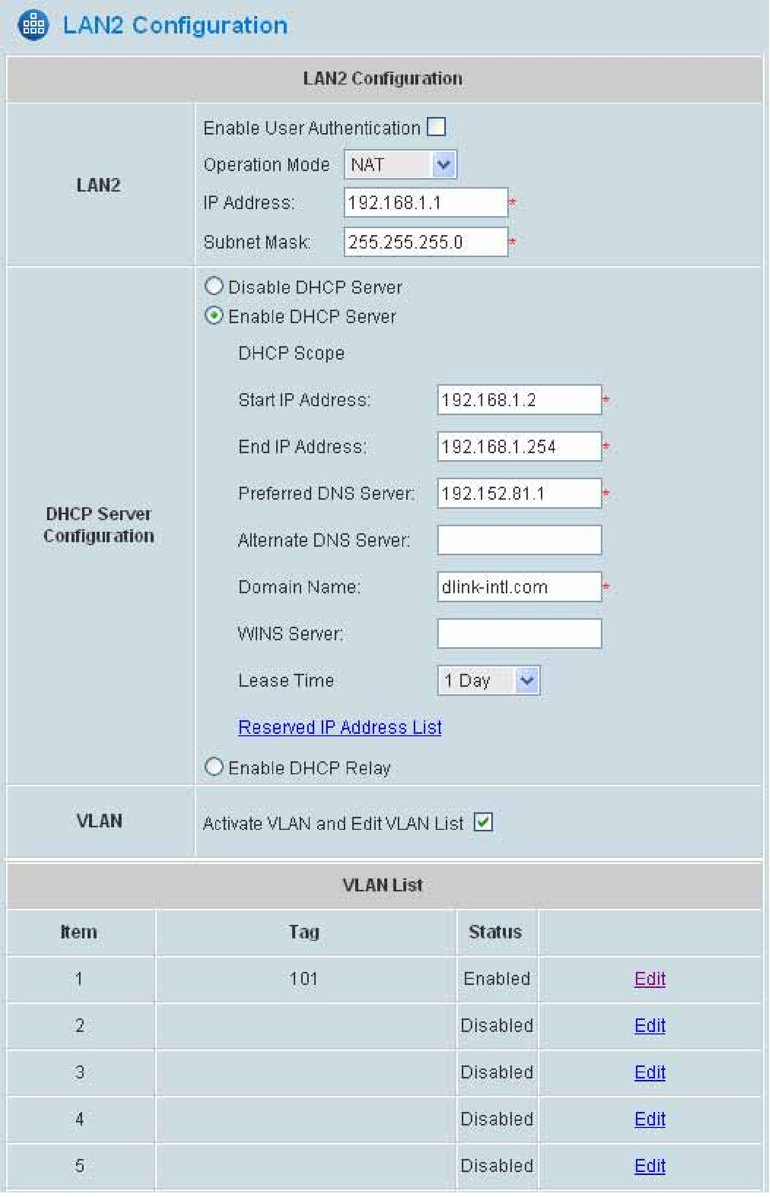
VLAN:

- **Enable:** When enabled, this VLAN segment will be active.
- **Enable User Authentication:** When enabled, users on this VLAN interface are required to log in before accessing the network.
- **VLAN Tag:** Enter any integer number within the range of 2 ~ 4094 (1 is reserved for system) as the Tag ID for this VLAN segment.
- **Mode:**
  - *NAT:* All IP addresses of hosts on the VLAN interface will be converted into the IP address of the WAN1 interface and onward to outside the network.
  - *ROUTER:* All IP addresses of hosts on the VLAN interface will remain the same while the IP packets travel through WAN1 interface, thus making the DSA-6100 act like a router.
- **IP address:** IP address of each network interface.
- **Subnet Mask:** Subnet Mask of the LAN/VLAN interface.

VLAN DHCP Configuration: DHCP options for this VLAN interface include Disable, Enable, and Relay.

4.1.6 LAN2 Configuration

By default, users on the LAN2 interface are not required to log in before accessing the network, but administrator can enable the user authentication based upon actual network deployment requirements. Please refer to the previous section "LAN1 Configuration" for details about the similar configuration of LAN2 port.



LAN2 Configuration

LAN2 Configuration	
LAN2	Enable User Authentication □ Operation Mode: NAT IP Address: 192.168.1.1 * Subnet Mask: 255.255.255.0 *
DHCP Server Configuration	○ Disable DHCP Server ● Enable DHCP Server DHCP Scope Start IP Address: 192.168.1.2 * End IP Address: 192.168.1.254 * Preferred DNS Server: 192.152.81.1 * Alternate DNS Server: Domain Name: dlink-intl.com * WINS Server: Lease Time: 1 Day Reserved IP Address List ○ Enable DHCP Relay
VLAN	Activate VLAN and Edit VLAN List ☑

VLAN List

Item	Tag	Status	
1	101	Enabled	Edit
2		Disabled	Edit
3		Disabled	Edit
4		Disabled	Edit
5		Disabled	Edit

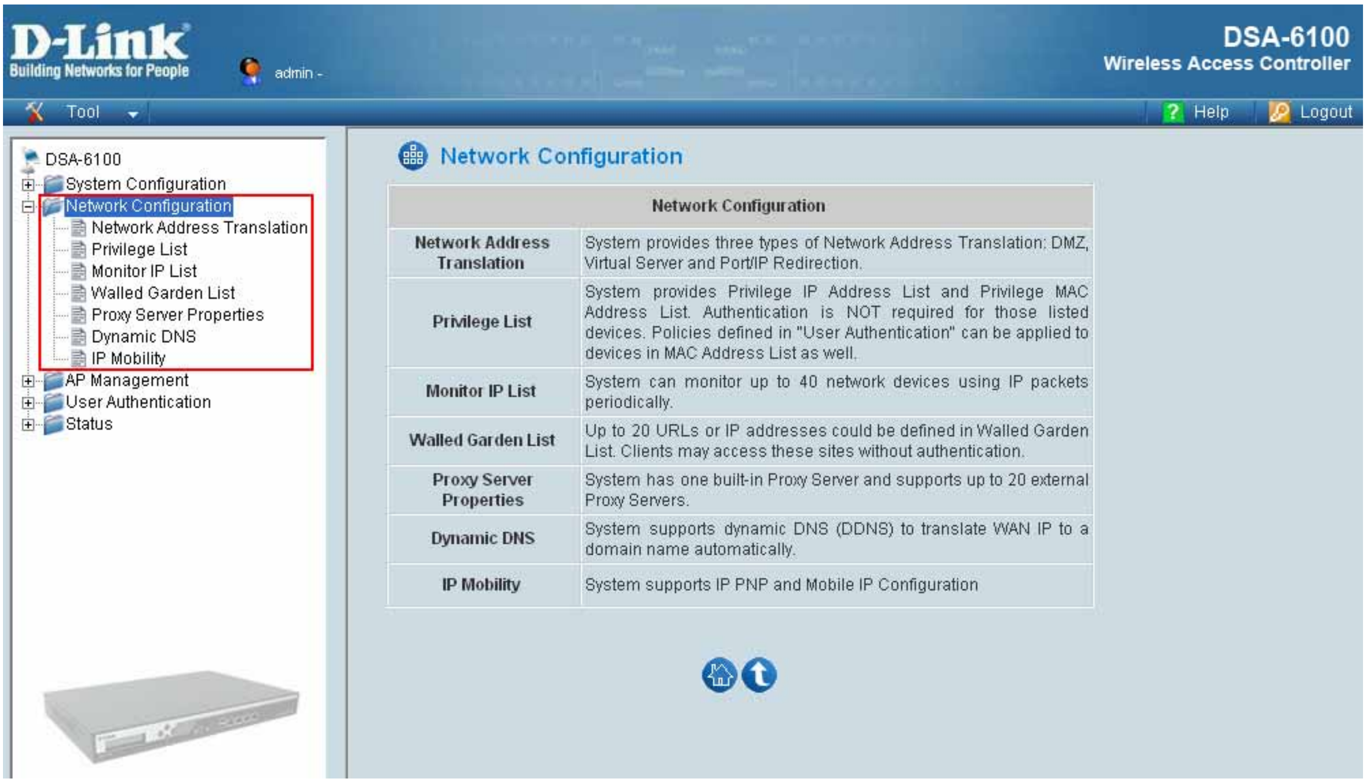
LAN2: These are the basic, global configuration options for LAN2 port.

DHCP Server Configuration: DHCP options for LAN2 port include Disable, DHCP, and Relay.

VLAN: To activate the VLAN interfaces for LAN2 port, please check "**Activate VLAN and Edit VLAN List**". Thereafter, on the VLAN List, 32 VLANs can be edited accordingly.

4.2 Network Configuration

This section is used to set all the internet settings. The section provides information on the following functions: **Network Address Translation**, **Privilege List**, **Monitor IP List**, **Walled Garden List**, **Proxy Server Properties**, **Dynamic DNS** and **IP Mobility**.

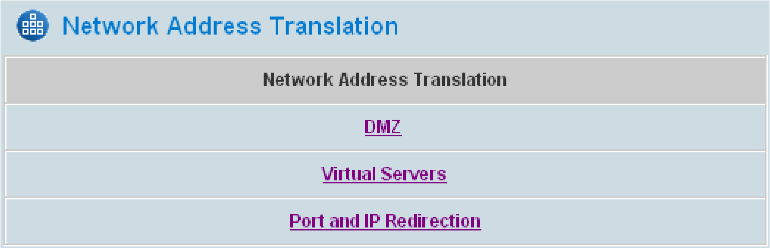


Network Configuration

Network Configuration	
Network Address Translation	System provides three types of Network Address Translation: DMZ, Virtual Server and Port/IP Redirection.
Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. Authentication is NOT required for those listed devices. Policies defined in "User Authentication" can be applied to devices in MAC Address List as well.
Monitor IP List	System can monitor up to 40 network devices using IP packets periodically.
Walled Garden List	Up to 20 URLs or IP addresses could be defined in Walled Garden List. Clients may access these sites without authentication.
Proxy Server Properties	System has one built-in Proxy Server and supports up to 20 external Proxy Servers.
Dynamic DNS	System supports dynamic DNS (DDNS) to translate WAN IP to a domain name automatically.
IP Mobility	System supports IP PNP and Mobile IP Configuration

4.2.1 Network Address Translation

There are three options of Network Address Translation that can be set: **DMZ, Virtual Servers** and **Port and IP Redirect**.



Network Address Translation

Network Address Translation

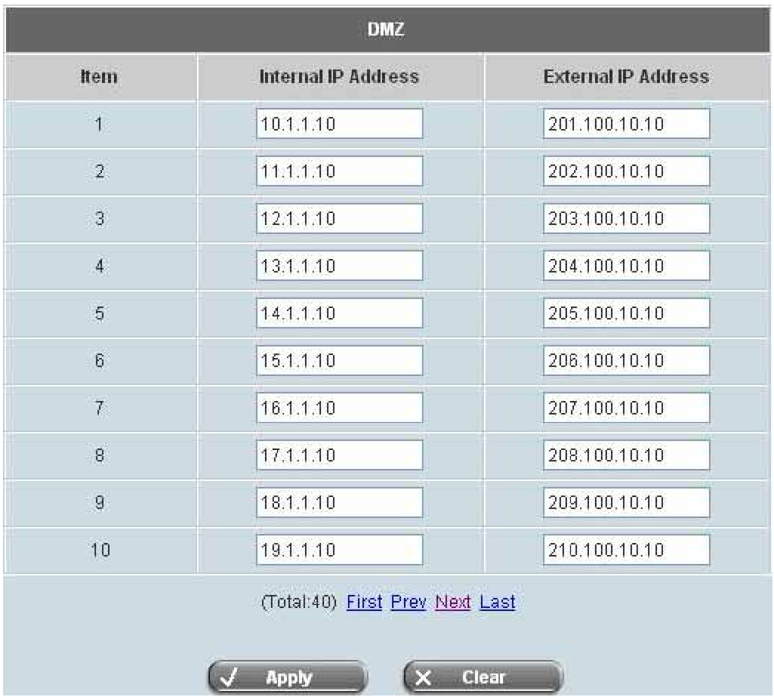
DMZ

Virtual Servers

Port and IP Redirection

- **DMZ**

  De-**M**ilitarized **Z**one. It maps external WAN IP address to the internal LAN IP addresses. A computer within a DMZ is unprotected by firewall and typically all port accesses are routed through that computer. A router will forward all traffic to the computer specified in the DMZ if it does not otherwise have a rule for how to forward traffic on a given port. There are 40 sets of static **Internal IP Address** and **External IP Address** available. These settings will become effective immediately after clicking the ***Apply*** button. Click ***Next*** to set up more than 10 IP addresses.



DMZ

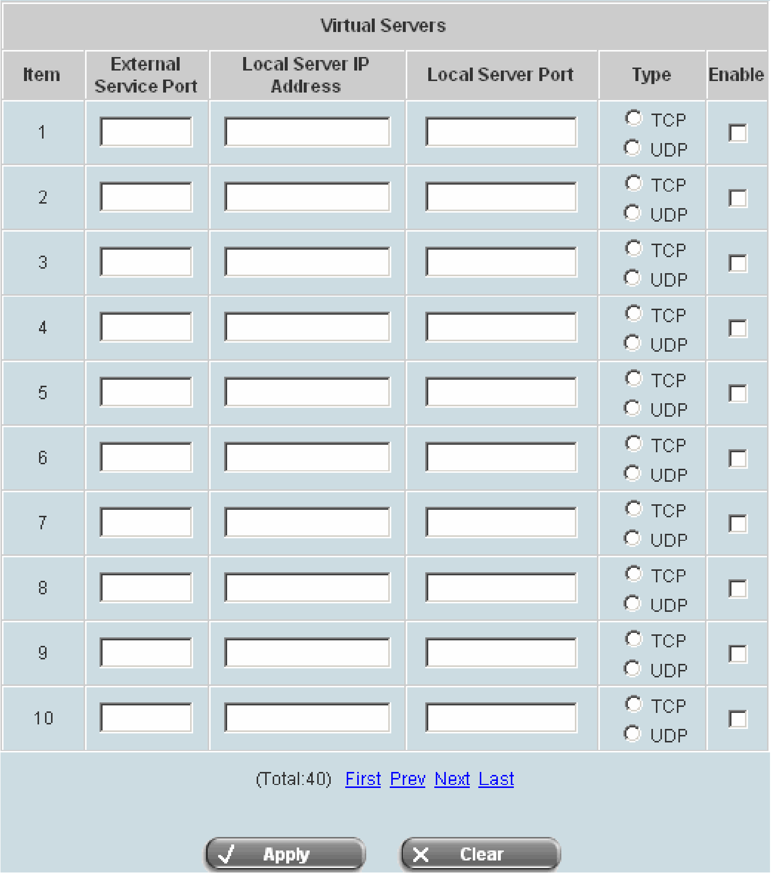
Item	Internal IP Address	External IP Address
1	10.1.1.10	201.100.10.10
2	11.1.1.10	202.100.10.10
3	12.1.1.10	203.100.10.10
4	13.1.1.10	204.100.10.10
5	14.1.1.10	205.100.10.10
6	15.1.1.10	206.100.10.10
7	16.1.1.10	207.100.10.10
8	17.1.1.10	208.100.10.10
9	18.1.1.10	209.100.10.10
10	19.1.1.10	210.100.10.10

(Total:40) First Prev Next Last

- **Virtual Servers**

  This function allows servers within LAN to become accessible from WAN. This function allows the administrator to set up to 40 virtual servers, to allow computers not belonging to the managed network (WAN network), to access the servers in the managed network (LAN network). Enter the **"External Service Port"**, **"Local Server IP Address"** and **"Local Server Port"** accordingly. Depending on the different services provided, the network service will be able to use the **TCP** protocol or the **UDP** protocol. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the ***Apply*** button.

  Virtual Servers will transfer External port to Local port. This function allows servers with specific communication port within LAN to become accessible from WAN.



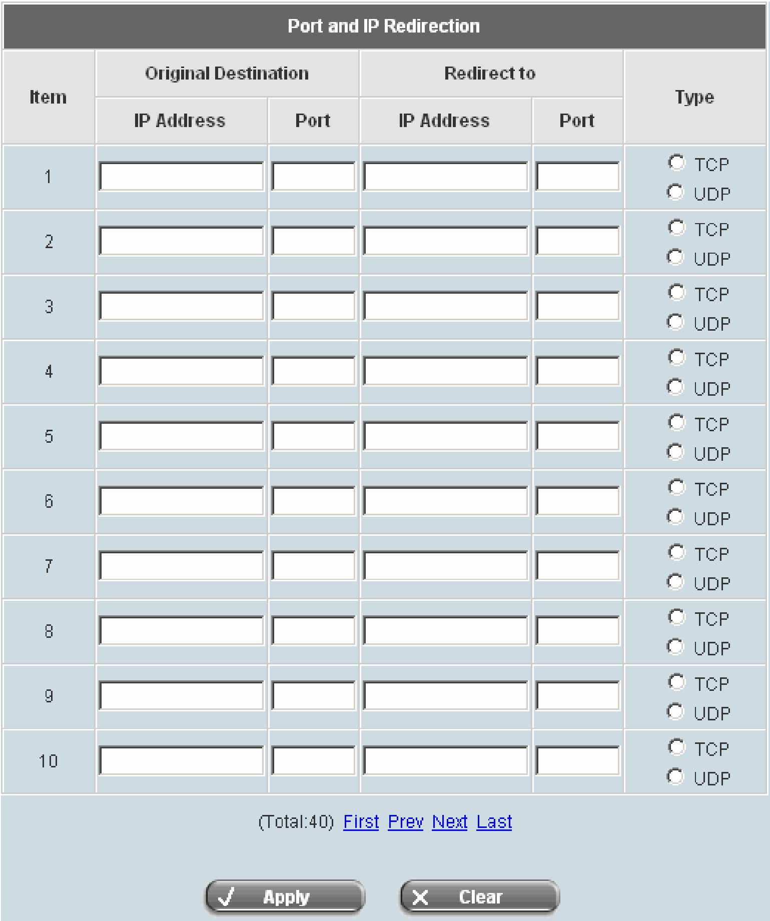
Virtual Servers

Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				○ TCP ○ UDP	□
2				○ TCP ○ UDP	□
3				○ TCP ○ UDP	□
4				○ TCP ○ UDP	□
5				○ TCP ○ UDP	□
6				○ TCP ○ UDP	□
7				○ TCP ○ UDP	□
8				○ TCP ○ UDP	□
9				○ TCP ○ UDP	□
10				○ TCP ○ UDP	□

(Total:40) First Prev Next Last

- **Port and IP Redirect**

  When the user attempts to connect to a destination IP address/Port listed here, the connection packet will be converted and redirected to the corresponding destination. Port and IP Redirection enables the redirection of the original IP address. When the user attempts to connect to a destination IP address/Port, the connection packet will be converted and redirected to the corresponding destination. This function allows the administrator to set up to 40 IP addresses for redirection purpose. Enter the **"IP Address"** and **"Port"** of **Original Destination**, and the **"IP Address"** and **"Port"** of **Redirect to**. According to the different services provided, choose the **"TCP"** protocol or the **"UDP"** protocol. These settings will become effective immediately after clicking ***Apply***.

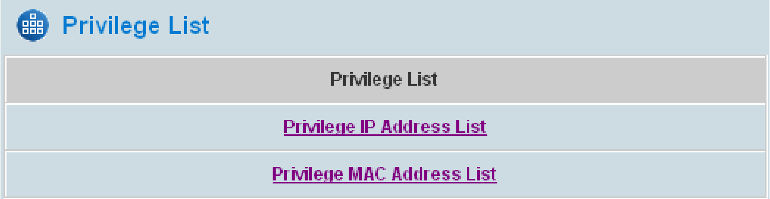


Port and IP Redirection

Item	Original Destination		Redirect to		Type
	IP Address	Port	IP Address	Port	
1					○ TCP ○ UDP
2					○ TCP ○ UDP
3					○ TCP ○ UDP
4					○ TCP ○ UDP
5					○ TCP ○ UDP
6					○ TCP ○ UDP
7					○ TCP ○ UDP
8					○ TCP ○ UDP
9					○ TCP ○ UDP
10					○ TCP ○ UDP

4.2.2 Privilege List

There are two lists that will need to be set: **Privilege IP Address List** and **Privilege MAC Address List**.

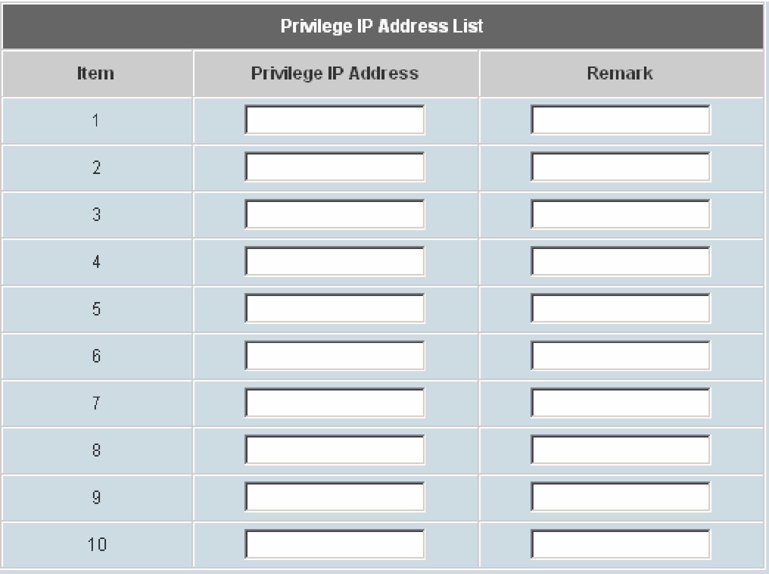


Privilege List

Privilege List
Privilege IP Address List
Privilege MAC Address List

- **Privilege IP Address List**

  Clients with the IP Address on the List are allowed to access the Internet directly; authentication is not required. If there are some workstations belonging to the managed server that need to access the network without authentication, enter the IP addresses to this list. The **"Remark"** field is not necessary but is useful to keep track. The DSA-6100 allows up to 100 privilege IP addresses. These settings will become effective immediately after clicking ***Apply***.



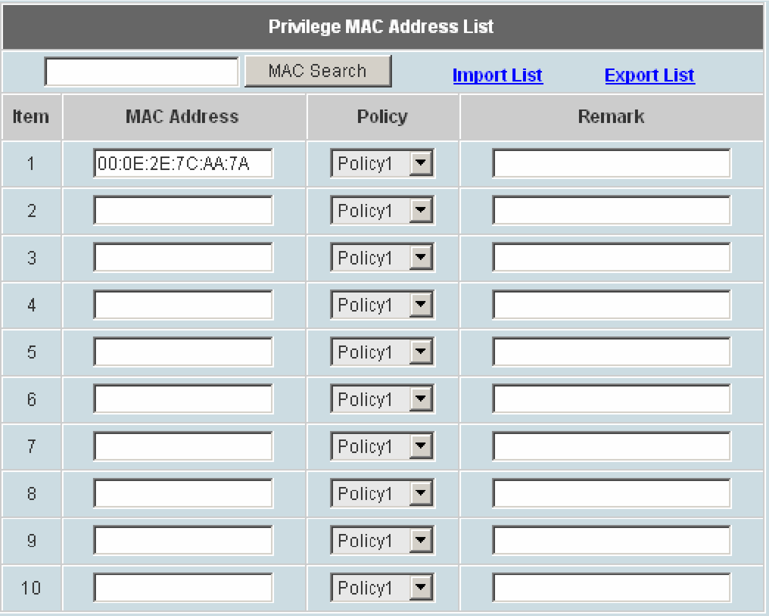
Privilege IP Address List

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

> ***Warning:*** *Permitting specific IP addresses to have network access rights without going through standard authentication process at the authenticated LAN can result in security risks.*

- **Privilege MAC Address List**

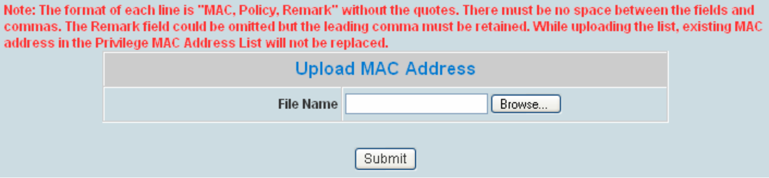
  Clients with the MAC Address on the List are allowed to access the Internet directly; authentication is not required. In addition to the IP address, the MAC address of the device that needs to access the network without authentication can also be set in this list. The DSA-6100 allows up to 100 privilege MAC addresses. The list can be created by entering data in the table or by import from a file. The list can be exported as well. Be sure to enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (optional) if manually creating the list is desired, and select a policy for the individual entry. These settings will become effective immediately after clicking ***Apply***.



Privilege MAC Address List

Item	MAC Address	Policy	Remark
1	00:0E:2E:7C:AA:7A	Policy1	
2		Policy1	
3		Policy1	
4		Policy1	
5		Policy1	
6		Policy1	
7		Policy1	
8		Policy1	
9		Policy1	
10		Policy1	

Import List: click ***Import List*** to enter the **Upload MAC Address List** interface. Click the ***Browse*** button to select the text file for the user account upload. Then click ***Submit*** to complete the upload.



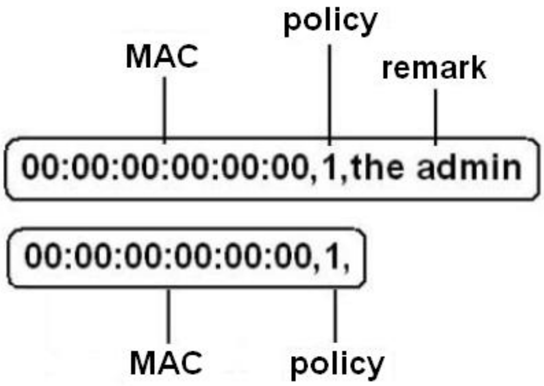
Note: The format of each line is "MAC, Policy, Remark" without the quotes. There must be no space between the fields and commas. The Remark field could be omitted but the leading comma must be retained. While uploading the list, existing MAC address in the Privilege MAC Address List will not be replaced.

Upload MAC Address

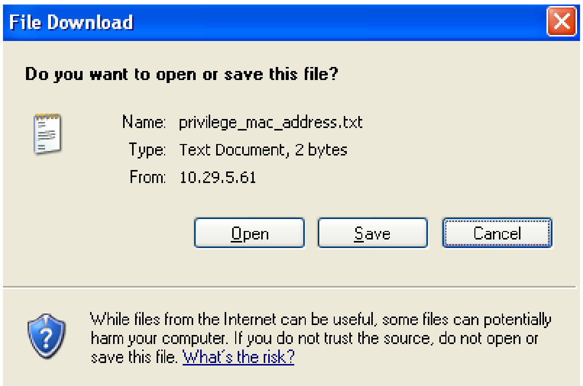
File Name [ ] Browse...

Submit

The uploading file should be a text file and the format of each line is ***" MAC, Policy, Remark"*** without the quotes. There must be no spaces between the fields and commas. The remark 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 new ones.



Export List: Click ***Export List*** to export or create the Mac List into a .txt files and then save it on disk.



File Download

Do you want to open or save this file?

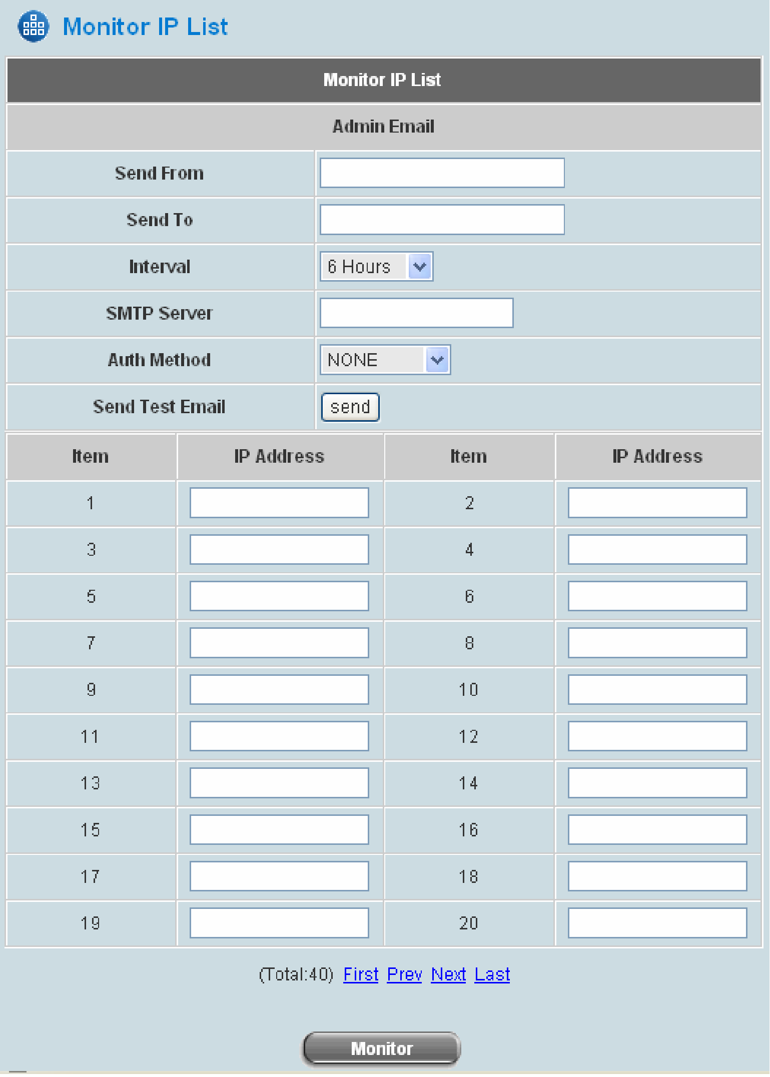
Name: privilege_mac_address.txt
Type: Text Document, 2 bytes
From: 10.29.5.61

Open Save Cancel

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

4.2.3 Monitor IP List

The system will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the related information, click ***Apply*** and these settings will become effective immediately. Click ***Monitor*** to check the current status of all the monitored IP. The system provides up to 40 IP addresses for the **"Monitor IP List"**.



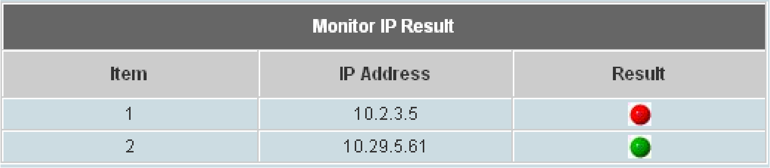
Monitor IP List

Monitor IP List	
Admin Email	
Send From	
Send To	
Interval	6 Hours
SMTP Server	
Auth Method	NONE
Send Test Email	send

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

(Total:40) First Prev Next Last

- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person whom the monitoring result is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Server:** The IP address of the SMTP server.
- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method selected, enter the **Account Name**, **Password** and **Domain**.
- **Send Test Email:** Click ***Send*** to send out a test e-mail of the IP monitoring report.
- **IP Address:** The IP addresses under monitoring.



Monitor IP Result

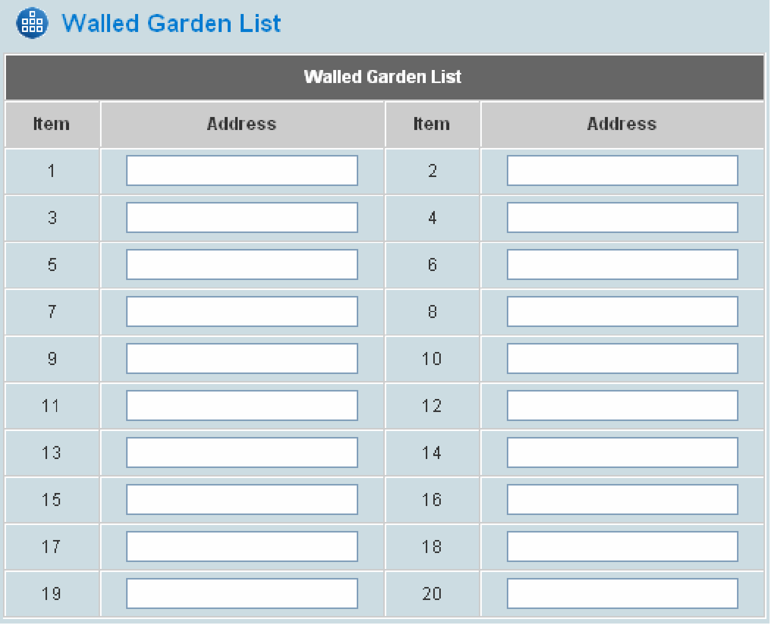
Item	IP Address	Result
1	10.2.3.5	🔴
2	10.29.5.61	🟢

4.2.4 Walled Garden List

This system provides the free services to the users to access websites listed here before authentication. IP addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. This function allows clients of specified addresses or domain names to access the Internet before login and authentication. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right in the list can make use of the actual network service free of charge.

Please enter **IP Address** or **Domain Name** of the website 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. An example may be seen in hotels, where guests without network access right are allowed to utilize the network service free of charge such as accessing the Hotel’s homepage.

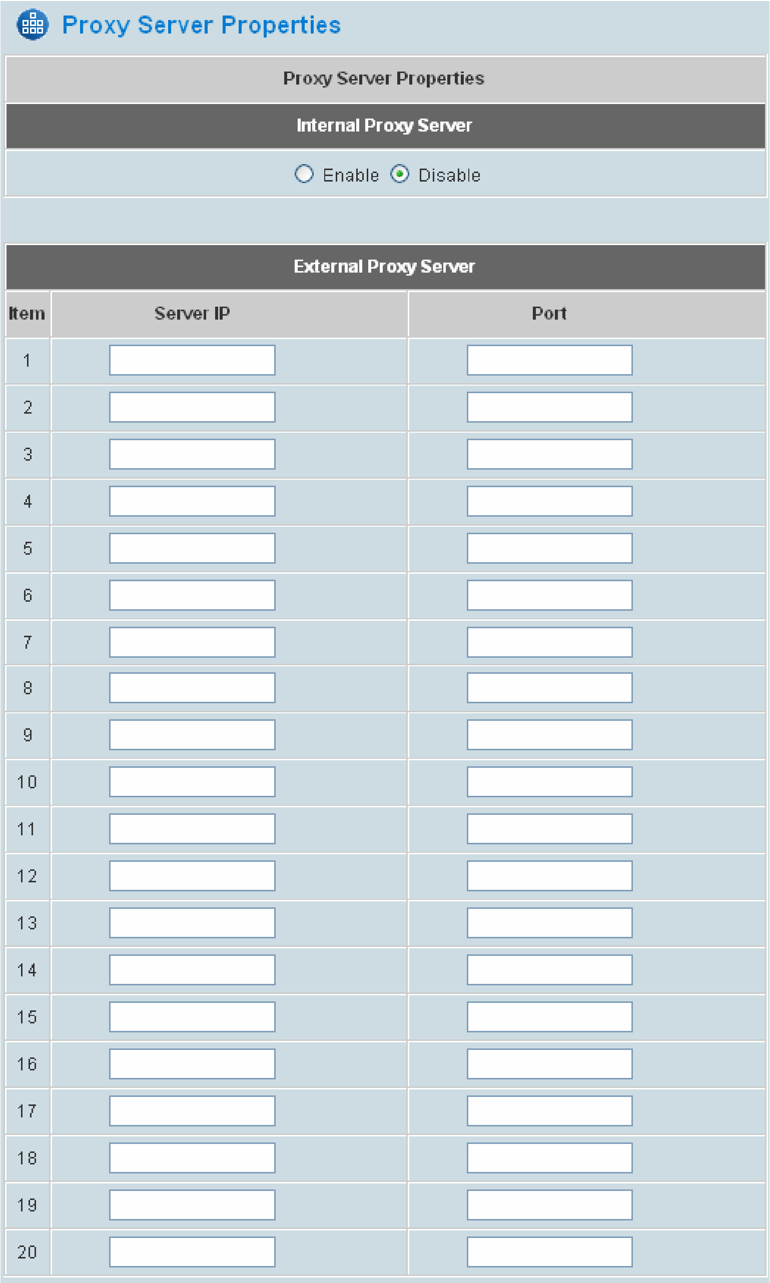


Walled Garden List

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

4.2.5 Proxy Server Properties

The DSA-6100 supports Internal Proxy Server and External Proxy Server functions. Please perform the necessary configurations. Please click ***Apply*** and these settings will become effective immediately. *For an example of Proxy Configuration, please go to* ***Appendix C. Proxy Configuration****.*



Proxy Server Properties

Proxy Server Properties

Internal Proxy Server

○ Enable ● Disable

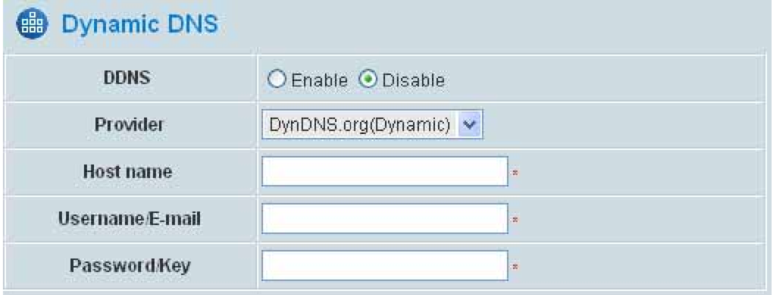
External Proxy Server

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

- **Internal Proxy Server:** The DSA-6100 has a built-in proxy server. If this function is enabled, the end users will be forced to treat the DSA-6100 as the proxy server regardless of the end-users' original proxy settings.
- **External Proxy Server:** Under the DSA-6100 security management, the system will match the External Proxy Server list to the end-users' proxy setting. If a match is not available, the end-users will not be able to reach the login page and thus unable to access the network. If a match is available, the end-users will be directed to the system first for authentication. After a successful authentication, the end-users will be redirected back to the desired proxy servers depending on various situations.

4.2.6 Dynamic DNS

The DSA-6100 provides a convenient dynamic DNS (DDNS) function to translate the IP address of the WAN port to a domain name that helps administrators easily memorize and connect to the WAN port. When the DHCP is activated at WAN port, this function will also 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***.



Dynamic DNS

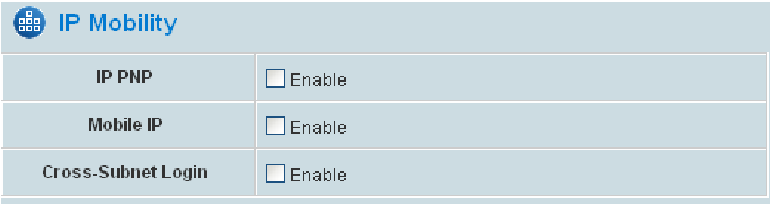
DDNS	○ Enable ● Disable
Provider	DynDNS.org(Dynamic)
Host name	*
Username/E-mail	*
Password/Key	*

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

Please click ***Apply*** and these settings will become effective immediately.

4.2.7 IP Mobility

The DSA-6100 supports functions of IP PNP, Mobile IP and Cross-Subnet Login.



IP Mobility

IP PNP	□ Enable
Mobile IP	□ Enable
Cross-Subnet Login	□ Enable

- **Enable IP PNP**

  Allow or disallow users with wrong IP configuration. Clients can use any IP address to connect to the system. Regardless of what the IP address at the client end is, he or she can still authenticate through the DSA-6100 and access the network.

- **Enable Mobile IP**

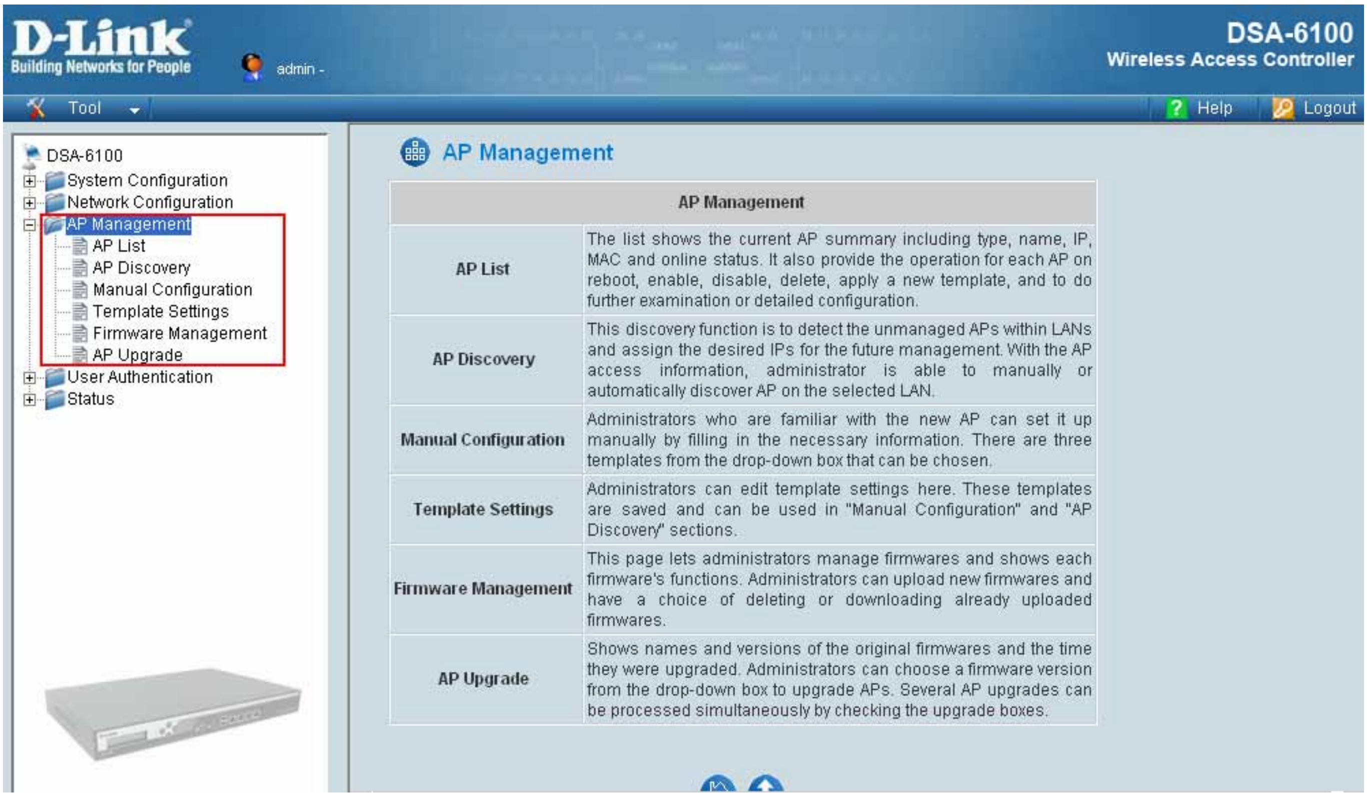
  Allow or disallow users to move from one LAN segment to another without login again. When Mobil IP is enabled, wireless clients roaming from two subnets behind the DSA-6100 with the same SSID will be able to stay connected with the system, and disconnection will not occur. For example, when downloading data, transmission will not be interrupted even while clients are roaming.

- **Enable Cross-Subnet Login**

  If connecting a router between the LAN ports and the end computer (users, access points, etc), this function must be enabled. Unlike bridge, switch, and hub, a router only use IP address to recognize source and destination, thus by enabling this function, the DSA-6100 is able to use IP address as the only information to process the request from the end computer.

4.3 AP Management

This section includes the following functions: **AP List**, **AP Discovery**, **Manual Configuration**, **Template Settings**, **Firmware Management** and **AP Upgrade**.

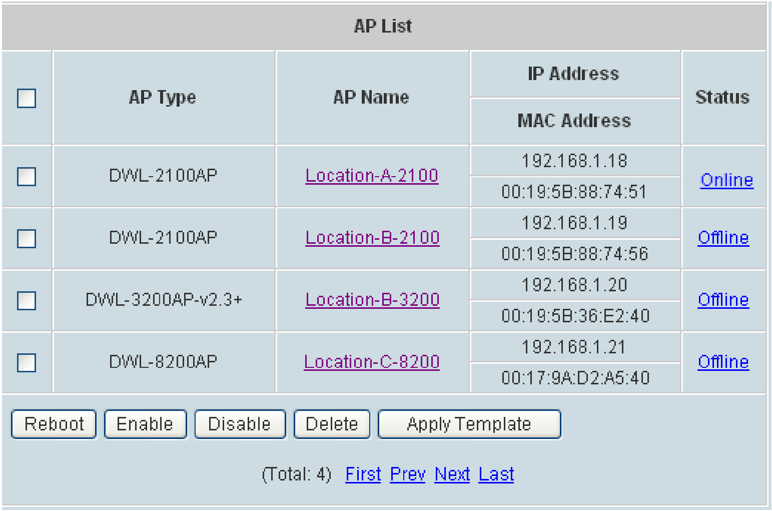


AP Management

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

4.3.1 AP List

All of the managed APs will be shown in the list. The list is empty during first setup. To add APs to the list, the administrator should first discover the manageable APs from *AP Discovery* or the *Manual Configuration* menu. After the APs are added, this list will show the current status of all managed APs, including AP type, AP name, IP Address, MAC Address, and Status. To perform functions for the specific APs on the list, select the check boxes of the APs and click on ***Reboot, Enable, Disable, Delete*** or ***Apply Template***.

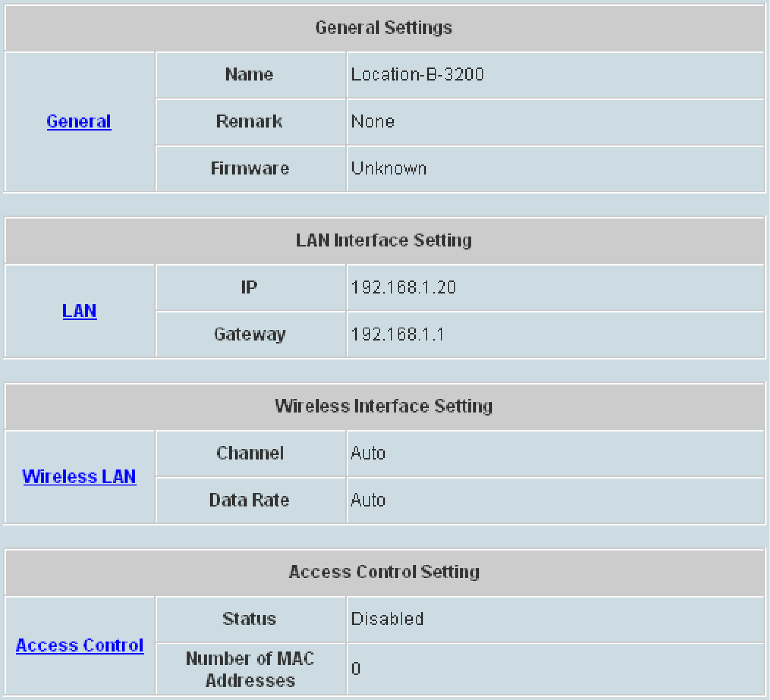


AP List

□	AP Type	AP Name	IP Address MAC Address	Status
□	DWL-2100AP	Location-A-2100	192.168.1.18 00:19:5B:88:74:51	Online
□	DWL-2100AP	Location-B-2100	192.168.1.19 00:19:5B:88:74:56	Offline
□	DWL-3200AP-v2.3+	Location-B-3200	192.168.1.20 00:19:5B:36:E2:40	Offline
□	DWL-8200AP	Location-C-8200	192.168.1.21 00:17:9A:D2:A5:40	Offline

- **AP Type:** This is the supported type of the AP for centralized management, including DWL-2100AP (v2.20eu, v2.20na, v2.30eu, and v2.30na), DWL-3200AP (v2.30), DWL-8200AP (v1.20)
- **AP Name:** This is the mnemonic name of the AP. By clicking the hyperlink of **AP Name**, you can do further configurations, including **General Settings**, **LAN Interface Setting**, **Wireless Interface Setting** and **Access Control Setting**.
- **Status:** Current status of the AP, including **Configuring**, **Online**, **Offline**, **Upgrading**, and **Lost/Unknown**.
  - *(1)* **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.
  - *(2)* **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.
  - *(3)* **Offline:** The AP is currently offline; for example: it is displayed as Offline when the power of the AP is off for any reason.
  - *(4)* **Upgrading:** The AP is undergoing firmware upgrade.
  - *(5)* **Lost/Unknown:** After DSA-6100'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.

Note: *The supported types and firmware of APs are subject to change for different DSA-6100 firmware releases.*



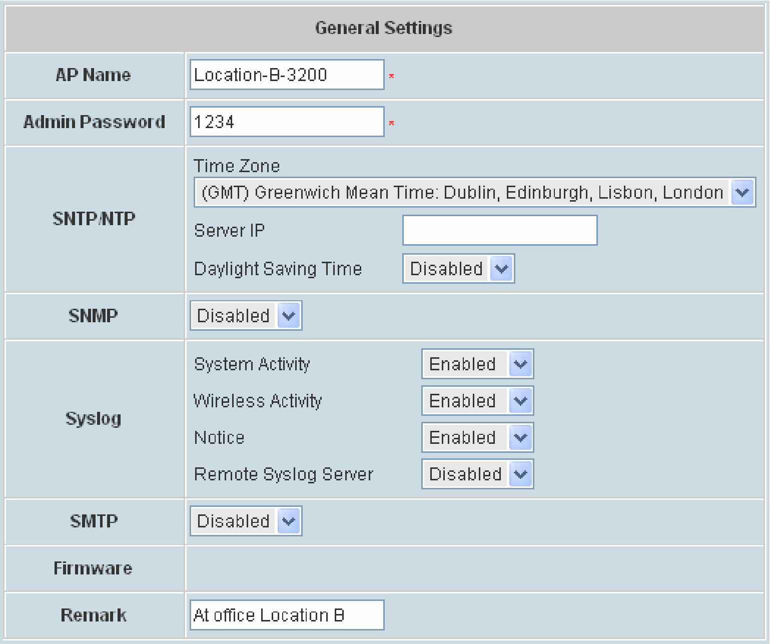
General Settings		
General	Name	Location-B-3200
	Remark	None
	Firmware	Unknown

LAN Interface Setting		
LAN	IP	192.168.1.20
	Gateway	192.168.1.1

Wireless Interface Setting		
Wireless LAN	Channel	Auto
	Data Rate	Auto

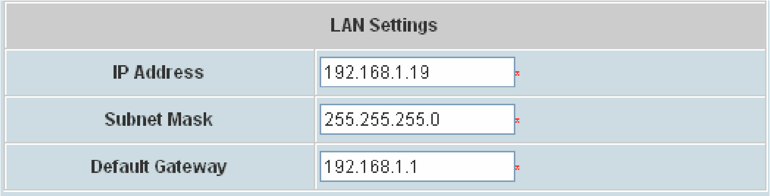
Access Control Setting		
Access Control	Status	Disabled
	Number of MAC Addresses	0

- **General Settings:** Click ***General*** to enter the **General Settings** interface. Revise the **AP Name**, **Admin Password, SNTP/NTP**, **SMTP**, **Syslog** and **Remark** here if desired. **Firmware** information can also be viewed here.



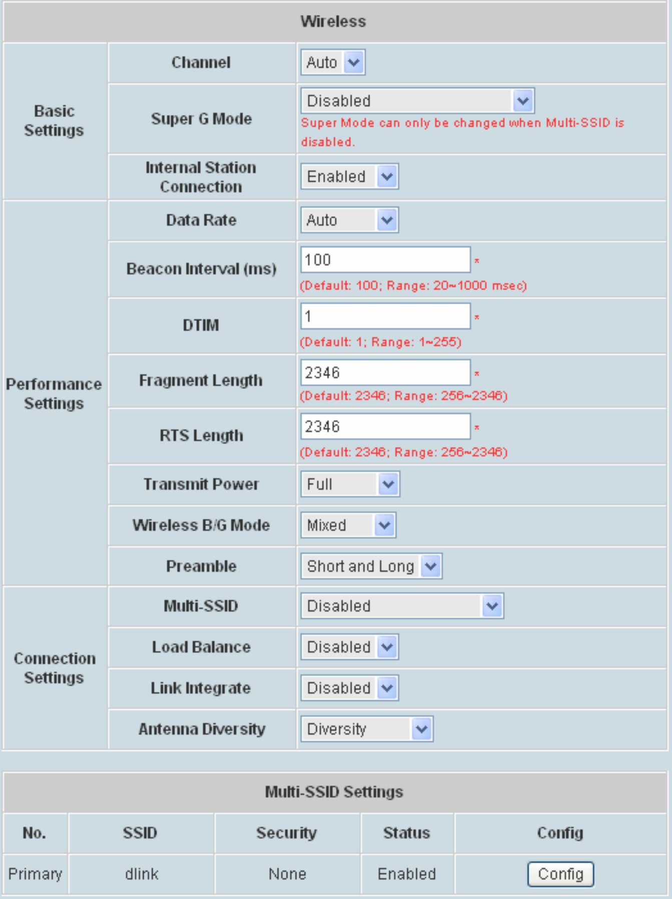
General Settings	
AP Name	Location-B-3200 *
Admin Password	1234 *
SNTP/NTP	Time Zone (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London Server IP Daylight Saving Time: Disabled
SNMP	Disabled
Syslog	System Activity: Enabled Wireless Activity: Enabled Notice: Enabled Remote Syslog Server: Disabled
SMTP	Disabled
Firmware	
Remark	At office Location B

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



LAN Settings	
IP Address	192.168.1.19 *
Subnet Mask	255.255.255.0 *
Default Gateway	192.168.1.1 *

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



Wireless

Basic Settings	Channel	Auto
	Super G Mode	Disabled Super Mode can only be changed when Multi-SSID is disabled.
	Internal Station Connection	Enabled
Performance Settings	Data Rate	Auto
	Beacon Interval (ms)	100 * (Default: 100; Range: 20~1000 msec)
	DTIM	1 * (Default: 1; Range: 1~255)
	Fragment Length	2346 * (Default: 2346; Range: 256~2346)
	RTS Length	2346 * (Default: 2346; Range: 256~2346)
	Transmit Power	Full
	Wireless B/G Mode	Mixed
	Preamble	Short and Long
Connection Settings	Multi-SSID	Disabled
	Load Balance	Disabled
	Link Integrate	Disabled
	Antenna Diversity	Diversity

Multi-SSID Settings

No.	SSID	Security	Status	Config
Primary	dlink	None	Enabled	Config

Basic Settings:

- **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.
- **Super Mode:** Select either **Disabled**, **Super Mode with Turbo** or **Super Mode without Turbo**. When Multi-SSID is selected as enabled, the item Super Mode cannot be active. Super G Mode can only be changed when Multi-SSID is disabled.
- **Internal Station Connection:** Select either Enabled or Disabled. The connection allows clients to communicate with each other when enabled.

Performance 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.
- **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.

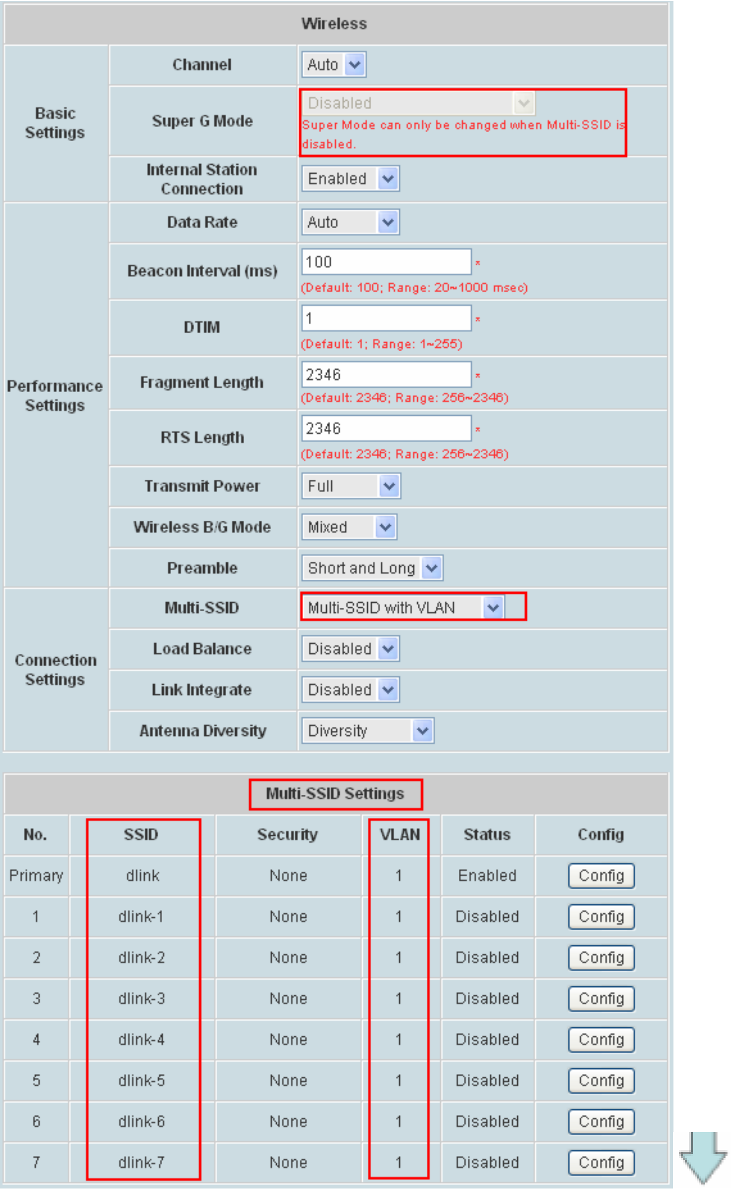
- **Fragment Length:** The fragmentation threshold determines whether packets will be fragmented. Enter a value between 256 and 2346.
- **RTS Length:** Enter a value between 256 and 2346.
- **Transmit Power:** Select either Full, Half(-3dB), Quarter(-6dB), Eighth (-9dB) or Minimum (minimum power).
- **Wireless B/G mode:** Enable supporting 802.11mixed mode 802.11b or 802.11g only.
- **Preamble:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select either Short Preamble or Long Preamble.

Connection Settings:

- **Multi-SSID:** Select **Disabled**, **Multi-SSID with VLAN** or **Multi-SSID without VLAN**. While *Multi-SSI*D enabled, **Super G Mode** will be disabled automatically. While selecting *Multi-SSID with VLAN*, Multi-SSID settings could configure up to multiple SSID. Click ***Configure*** button to setup SSID Configuration, the information of **SSID**, **Broadcast SSID**, **WMM**, and **Security**.

  SSID Configuration Page:

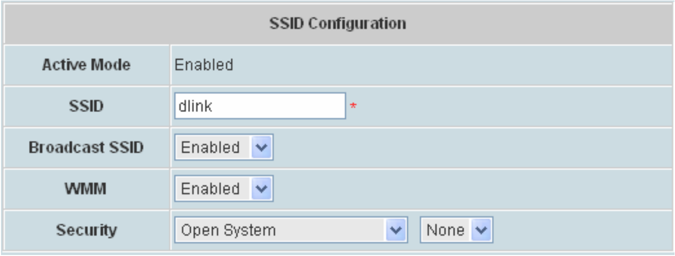
  - **SSID:** Service Set Identifier.
  - **Broadcast SSID:** Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID 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.
  - **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.
  - **Security:** Choose one of security types from SSID Configuration, also selecting whether WEP included or not.



Wireless		
Basic Settings	Channel	Auto
	Super G Mode	Disabled Super Mode can only be changed when Multi-SSID is disabled.
	Internal Station Connection	Enabled
Performance Settings	Data Rate	Auto
	Beacon Interval (ms)	100 * (Default: 100; Range: 20~1000 msec)
	DTIM	1 * (Default: 1; Range: 1~255)
	Fragment Length	2346 * (Default: 2346; Range: 256~2346)
	RTS Length	2346 * (Default: 2346; Range: 256~2346)
	Transmit Power	Full
	Wireless B/G Mode	Mixed
	Preamble	Short and Long
Connection Settings	Multi-SSID	Multi-SSID with VLAN
	Load Balance	Disabled
	Link Integrate	Disabled
	Antenna Diversity	Diversity

Multi-SSID Settings

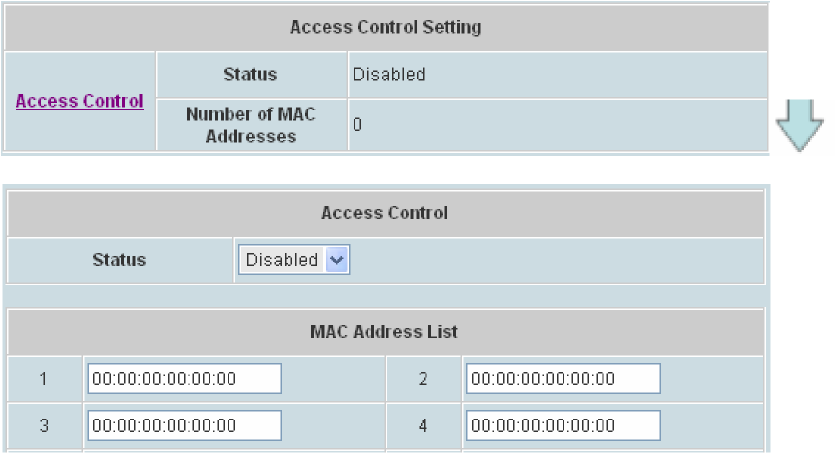
No.	SSID	Security	VLAN	Status	Config
Primary	dlink	None	1	Enabled	Config
1	dlink-1	None	1	Disabled	Config
2	dlink-2	None	1	Disabled	Config
3	dlink-3	None	1	Disabled	Config
4	dlink-4	None	1	Disabled	Config
5	dlink-5	None	1	Disabled	Config
6	dlink-6	None	1	Disabled	Config
7	dlink-7	None	1	Disabled	Config



SSID Configuration	
Active Mode	Enabled
SSID	dlink *
Broadcast SSID	Enabled
WMM	Enabled
Security	Open System None

- **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.
- **Antenna Diversity:** Choose from Diversity, Left Antenna or Right Antenna. 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.

- **Access Control Setting:** In this function, when the status is **Enabled**, only these clients which MAC addresses are listed in the list can be allowed to connect DSA-6100. When **Disabled** is selected, all clients can connect DSA-6100. The default is **Disabled**.



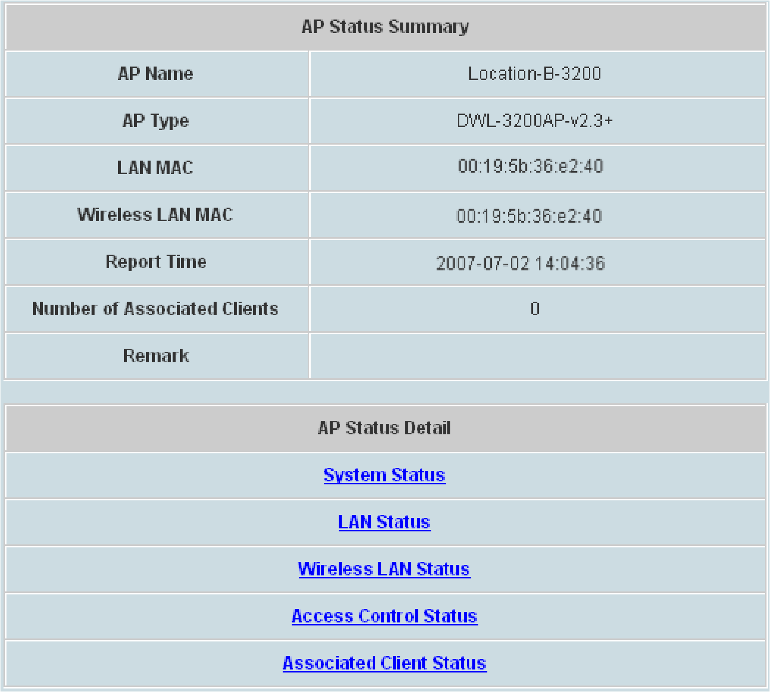
Access Control Setting		
Access Control	Status	Disabled
	Number of MAC Addresses	0

Access Control	
Status	Disabled

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

- **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**, **Number of Associated Clients** and **Remark**. AP Status Details include **System Status**, **LAN Status**, **Wireless LAN Status**, **Access Control Status** and **Associated Client Status**.

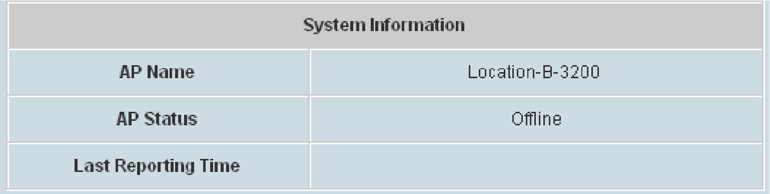


AP Status Summary	
AP Name	Location-B-3200
AP Type	DWL-3200AP-v2.3+
LAN MAC	00:19:5b:36:e2:40
Wireless LAN MAC	00:19:5b:36:e2:40
Report Time	2007-07-02 14:04:36
Number of Associated Clients	0
Remark	

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

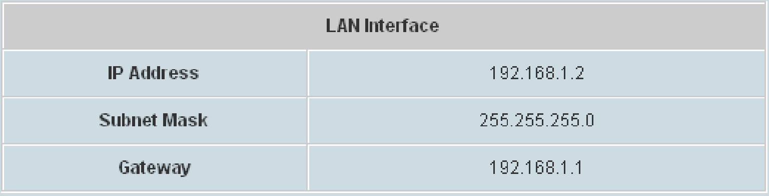
- **AP Name:** Mnemonic name of the specified AP.
- **AP Type:** This is the supported type of APs for centralized management.
- **LAN MAC:** The LAN’s Media Access Control address.
- **Wireless LAN MAC:** The wireless LAN’s Media Access Control Address.

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



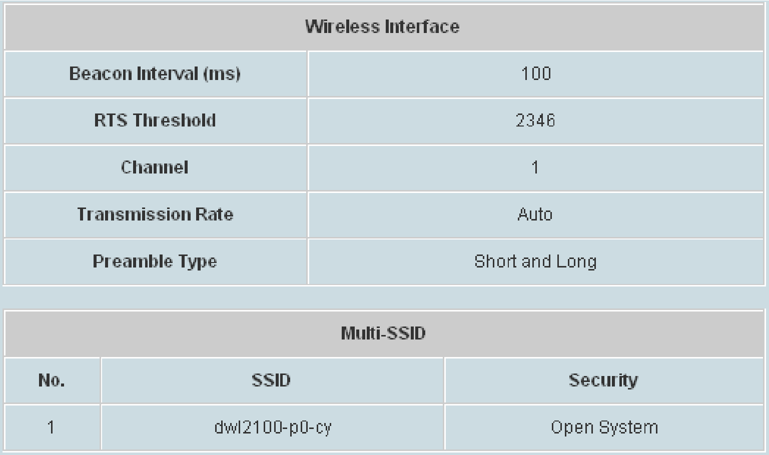
System Information	
AP Name	Location-B-3200
AP Status	Offline
Last Reporting Time	

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



LAN Interface	
IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Gateway	192.168.1.1

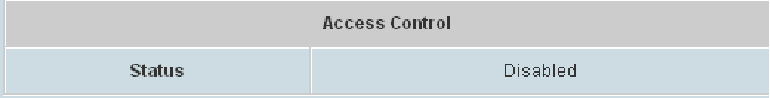
- **Wireless LAN Status:** The table shows all of the related wireless information.



Wireless Interface	
Beacon Interval (ms)	100
RTS Threshold	2346
Channel	1
Transmission Rate	Auto
Preamble Type	Short and Long

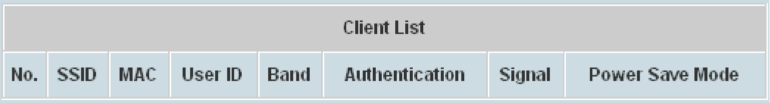
Multi-SSID		
No.	SSID	Security
1	dwl2100-p0-cy	Open System

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



Access Control	
Status	Disabled

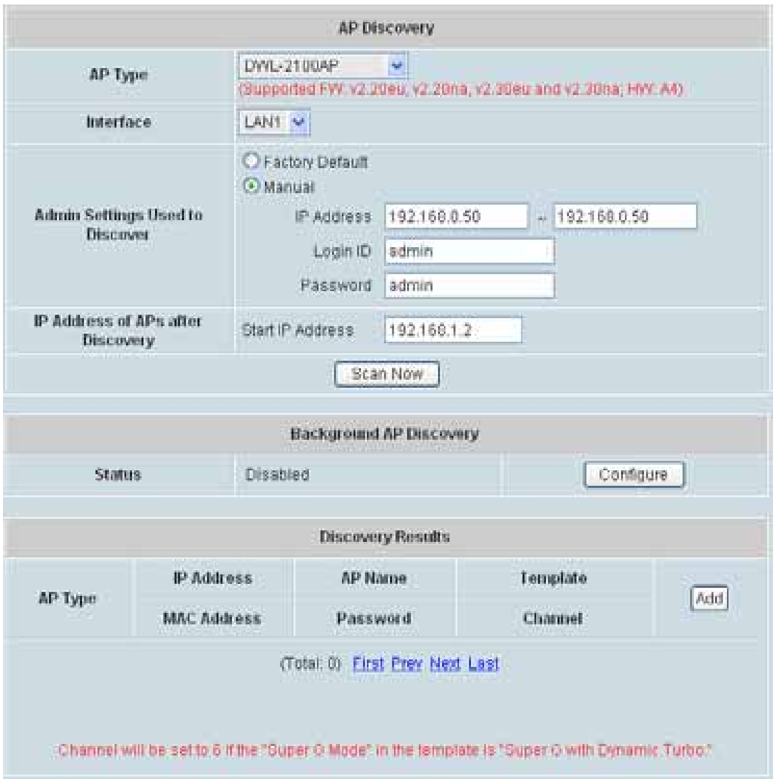
- **Associated Client Status:** The table shows the clients connecting to the AP and the related information of the client.



Client List							
No.	SSID	MAC	User ID	Band	Authentication	Signal	Power Save Mode

4.3.2 AP Discovery

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



AP Discovery	
AP Type	DWL-2100AP (Supported FW: v2.20eu, v2.20na, v2.30eu and v2.30na; HW: A4)
Interface	LAN1
Admin Settings Used to Discover	○ Factory Default ● Manual IP Address 192.168.0.50 ~ 192.168.0.50 Login ID admin Password admin
IP Address of APs after Discovery	Start IP Address 192.168.1.2

Background AP Discovery		
Status	Disabled	Configure

Discovery Results				
AP Type	IP Address	AP Name	Template	Add
	MAC Address	Password	Channel	

(Total: 0) First Prev Next Last

Channel will be set to 6 if the "Super G Mode" in the template is "Super G with Dynamic Turbo."

- **AP Discovery Settings**

  When the administrator tries to discover a new AP, select **Factory Default** or **Manual** in **Admin Settings Used to Discover** field; enter the current IP range of the APs if they are not in default value. 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. Please fill in the required data.

Note: *The APs (and the firmware version as well as the hardware number) that are supported include:*

1. DWL-2100 (FW v2.20/2.30eu and v2.20/2.30na;HW A4),

2. DWL-3200-v2.3+ (FW v2.30; HW B1)

3. DWL-8200 (FW v1.20; HW A2)

- To discover AP manually, please select/fill in the required data.
  - **AP Type:** List the current AP types to choose from.
  - **Interface:** Select between LAN ports where the APs are connected.
  - **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

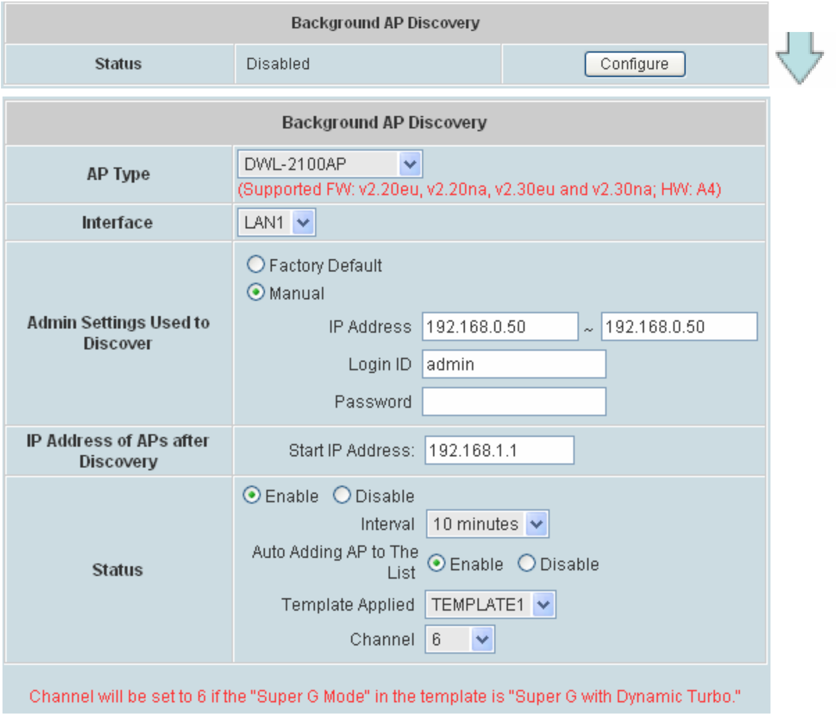
is the admin password of the AP. If the AP is in default value, just select Factory Default, system can discovery the APs.

- **IP Addresses of APs after Discovery**: The start IP to be assigned will be entered here.
- **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.



Background AP Discovery		
Status	Disabled	Configure

Background AP Discovery	
AP Type	DWL-2100AP (Supported FW: v2.20eu, v2.20na, v2.30eu and v2.30na; HW: A4)
Interface	LAN1
Admin Settings Used to Discover	○ Factory Default ● Manual IP Address 192.168.0.50 ~ 192.168.0.50 Login ID admin Password
IP Address of APs after Discovery	Start IP Address: 192.168.1.1
Status	● Enable ○ Disable Interval 10 minutes Auto Adding AP to The List ● Enable ○ Disable Template Applied TEMPLATE1 Channel 6

Channel will be set to 6 if the "Super G Mode" in the template is "Super G with Dynamic Turbo."

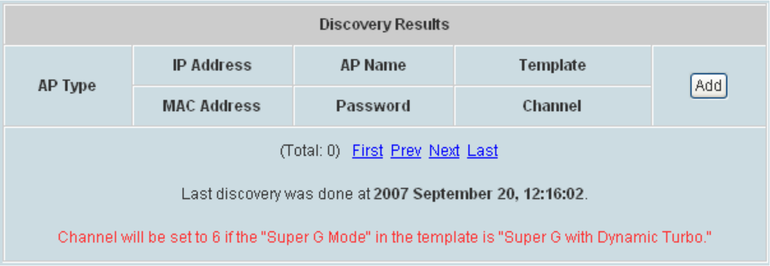
The **Interface, Admin Settings Used to Discover** and **IP Addresses of APs after Discovery** configurations are the same as the settings mentioned above. Check **Enable** in the **Status** field to have more configuration. Select **Interval** setting from the drop-down menu to set the system to scan 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**

  Then click the ***Scan Now*** button and the APs that match the given settings will show in the **Discovery 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. For the desired AP, input the desired name and password, select one template to apply, select the check box, and click ***Add*** to add the AP to the AP List. (About the template, please see **4.3.4 Template Settings**).

  When the matched AP is discovered, it will be shown in the **AP List** below and be given a new IP address as set previously (ex: 192.168.2.2). Check the Add box to add the AP, and it will be listed in the **AP List**.

  Click Configuring to go to the related configuration. For the details, please refer to **4.3.1 AP List**.



Discovery Results

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

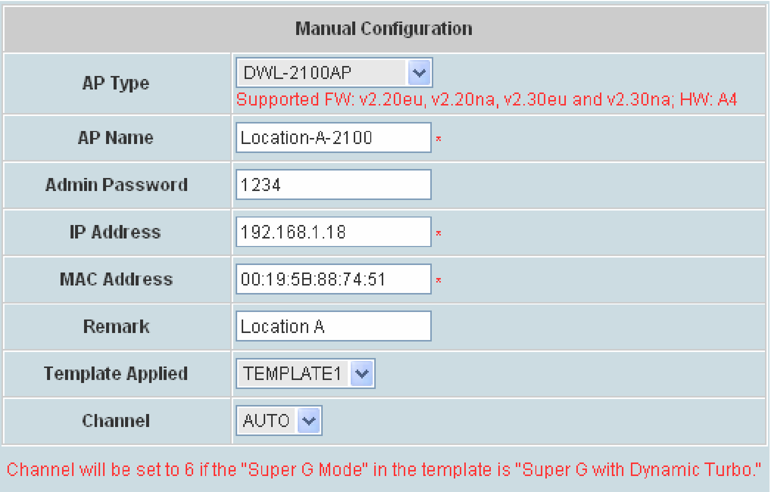
(Total: 0) First Prev Next Last

Last discovery was done at **2007 September 20, 12:16:02**.

Channel will be set to 6 if the "Super G Mode" in the template is "Super G with Dynamic Turbo."

4.3.3 Manual Configuration

The administrators who choose to configure an AP manually can utilize this page, in which provides several fields to be filled in. The supported APs (such as DWL-2100AP) can also be added manually. Enter the related information of the AP and select a **Template**. 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.



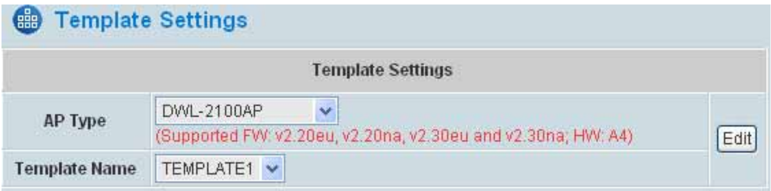
Manual Configuration	
AP Type	DWL-2100AP Supported FW: v2.20eu, v2.20na, v2.30eu and v2.30na; HW: A4
AP Name	Location-A-2100 *
Admin Password	1234
IP Address	192.168.1.18 *
MAC Address	00:19:5B:88:74:51 *
Remark	Location A
Template Applied	TEMPLATE1
Channel	AUTO

Channel will be set to 6 if the "Super G Mode" in the template is "Super G with Dynamic Turbo."

- **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.
- **Template Applied:** The template which will be applied to the AP.
- **Channel:** The RF channel to be used in the added AP.

4.3.4 Template Settings

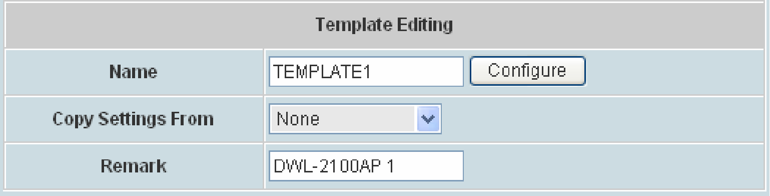
A template is a model that can be copied to every AP without having to configure the each AP individually. The system supports up to three templates which include configurations of APs. The administrator can configure the setting together in the template instead of logging the AP management interface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



Template Settings

Template Settings		
AP Type	DWL-2100AP (Supported FW: v2.20eu, v2.20na, v2.30eu and v2.30na; HW: A4)	Edit
Template Name	TEMPLATE1	

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.



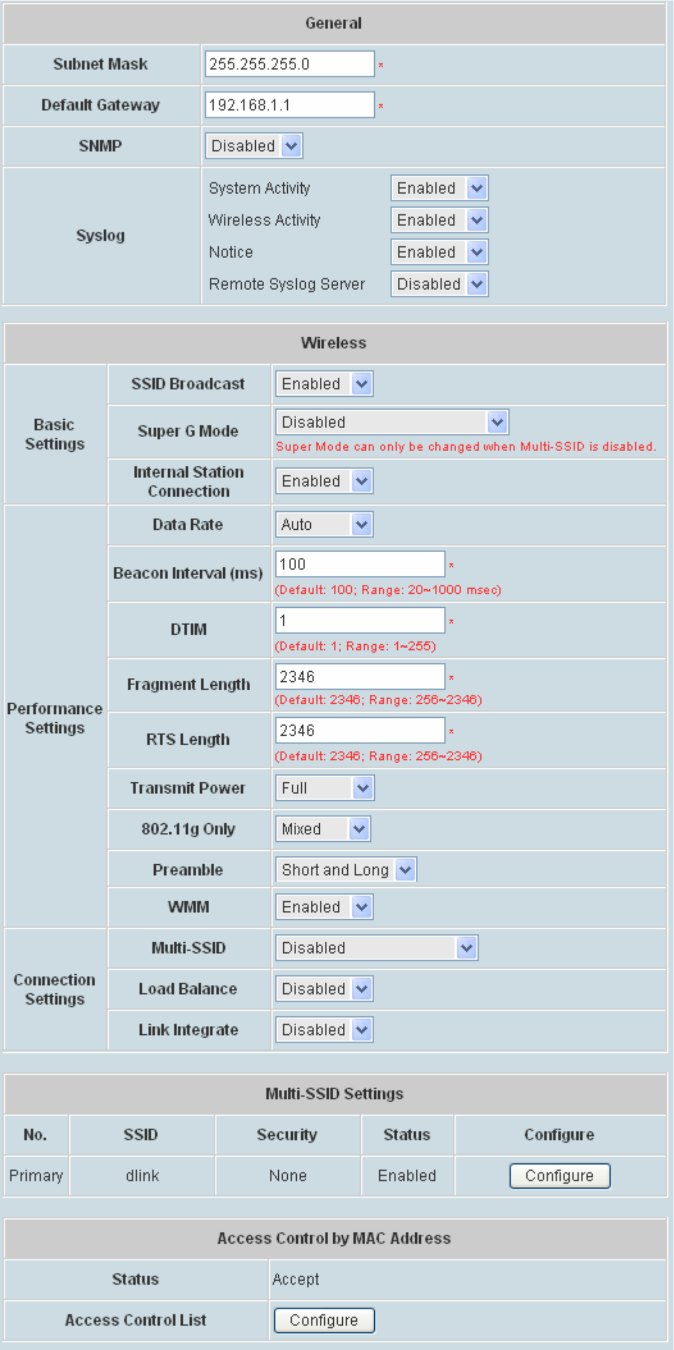
Template Editing	
Name	TEMPLATE1 Configure
Copy Settings From	None
Remark	DWL-2100AP 1

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



General		
Subnet Mask	255.255.255.0 *	
Default Gateway	192.168.1.1 *	
SNMP	Disabled	
Syslog	System Activity	Enabled
	Wireless Activity	Enabled
	Notice	Enabled
	Remote Syslog Server	Disabled

Wireless		
Basic Settings	SSID Broadcast	Enabled
	Super G Mode	Disabled Super Mode can only be changed when Multi-SSID is disabled.
	Internal Station Connection	Enabled
Performance Settings	Data Rate	Auto
	Beacon Interval (ms)	100 * (Default: 100; Range: 20~1000 msec)
	DTIM	1 * (Default: 1; Range: 1~255)
	Fragment Length	2346 * (Default: 2346; Range: 256~2346)
	RTS Length	2346 * (Default: 2346; Range: 256~2346)
	Transmit Power	Full
	802.11g Only	Mixed
	Preamble	Short and Long
	WMM	Enabled
Connection Settings	Multi-SSID	Disabled
	Load Balance	Disabled
	Link Integrate	Disabled

Multi-SSID Settings

No.	SSID	Security	Status	Configure
Primary	dlink	None	Enabled	Configure

Access Control by MAC Address	
Status	Accept
Access Control List	Configure

- ***General***

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 enabled, change the Public Community Name here.
- **Private Community:** When enabled, change the Private Community Name here.
- **User Status Notification:** Enable or Disable the feature.

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.

- ***Wireless***

Basic 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.
- **Super G Mode:** Select either **Disabled**, **Super G Mode with Turbo** or **Super G Mode without Turbo**. When Multi-SSID is selected as enabled, the item Super Mode cannot be active. Super G Mode can only be changed when Multi-SSID is disabled.
- **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.

Performance 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.
- **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.
- **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.
- **Transmit Power:** Select either Full, Half(-3dB), Quarter(-6dB), Eighth (-9dB) or Minimum (minimum power).
- **802.11g Only:** The function allows you to configure the wireless network with IEEE 802.11g only, Mixed.
- **Preamble:** Select Long Only or Short and Long. A short preamble is recommended for high-traffic

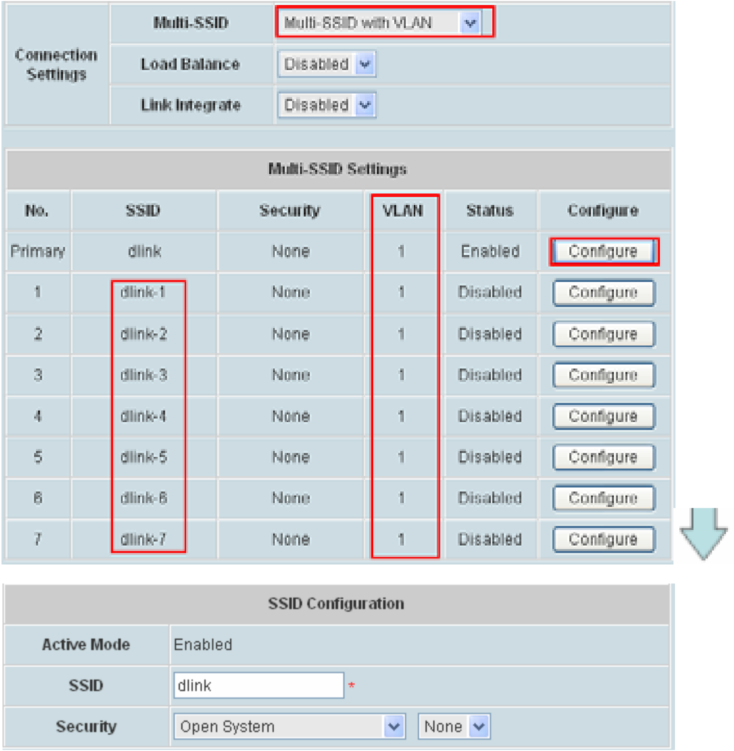
networks.

- ➢ **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.

Connection Settings:

- ➢ **Multi-SSID:** Multiple Service Set Identifier. Select either **Disabled**, **Multi-SSID with VLAN** or **Multi-SSID without VLAN**.
- ➢ **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.
  - o **User Limit:** Enter the number of the limit of load balancing users from 0~64.
- ➢ **Link Integrate:** Enable or disable the feature.

- ▪ ***Multi-SSID Settings***: Select **Disabled**, **Multi-SSID with VLAN** or **Multi-SSID without VLAN**. While *Multi-SSI*D enabled, **Super G Mode** will be disabled automatically. While selecting *Multi-SSID with VLAN*, Multi-SSID settings could configure up to multiple SSID. Click ***Configure*** button to setup SSID Configuration, the information of **SSID** and **Security**.



Connection Settings	Multi-SSID	Multi-SSID with VLAN
	Load Balance	Disabled
	Link Integrate	Disabled

Multi-SSID Settings

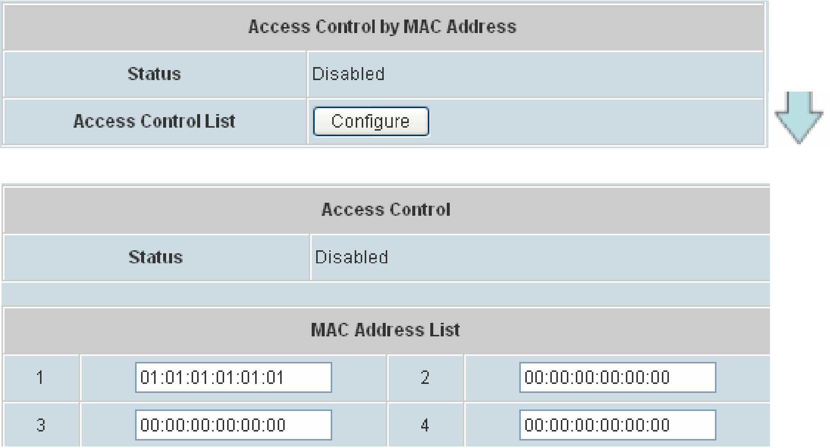
No.	SSID	Security	VLAN	Status	Configure
Primary	dlink	None	1	Enabled	Configure
1	dlink-1	None	1	Disabled	Configure
2	dlink-2	None	1	Disabled	Configure
3	dlink-3	None	1	Disabled	Configure
4	dlink-4	None	1	Disabled	Configure
5	dlink-5	None	1	Disabled	Configure
6	dlink-6	None	1	Disabled	Configure
7	dlink-7	None	1	Disabled	Configure

SSID Configuration

Active Mode	Enabled
SSID	dlink *
Security	Open System None

- ○ **SSID Configuration Page:**
  - ➢ **SSID:** Service Set Identifier.
  - ➢ **Security:** Choose one of security types from SSID Configuration, also selecting whether WEP included or not.

- ***Access Control by MAC Address:*** MAC address based control for access the network (AP). 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.

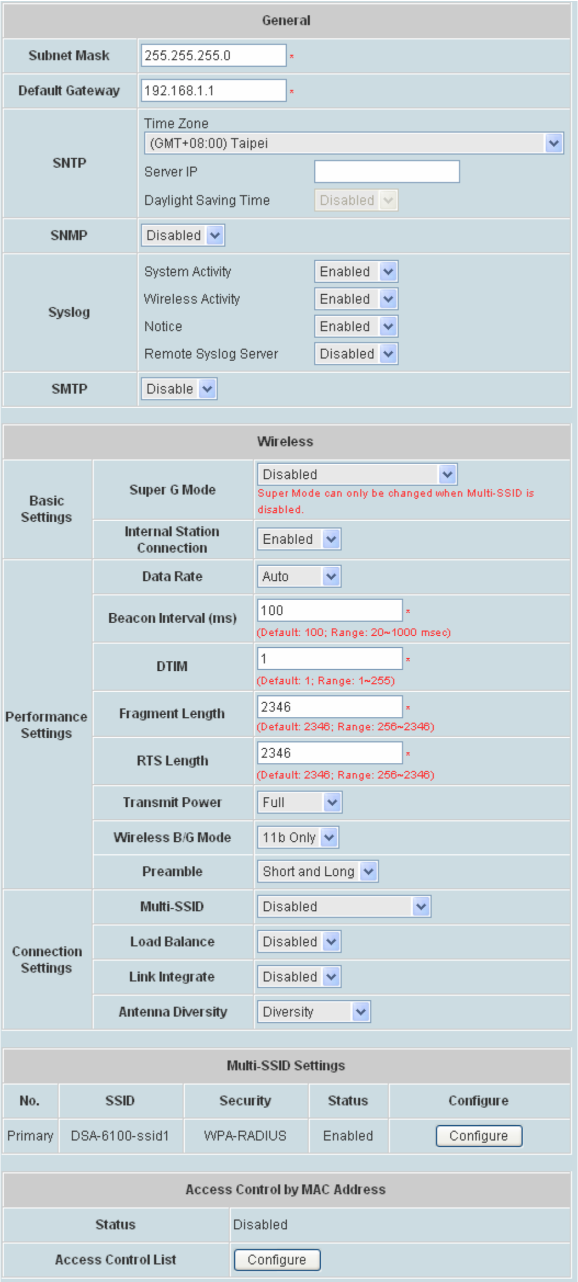


Access Control by MAC Address	
Status	Disabled
Access Control List	Configure

Access Control			
Status	Disabled		
MAC Address List			
1	01:01:01:01:01:01	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00

II. DWL-3200AP-v2.3+

DWL-3200AP version 2.3 Templates settings allow users to configure wireless 802.11b/g mode settings. DWL-3200AP includes all three standards 802.11b/g mixed, 802.11b only and 802.11g only. *Firmware upgrade from DWL-3200AP v2.20 to v2.3 is NOT supported by the system.*



General	
Subnet Mask	255.255.255.0 *
Default Gateway	192.168.1.1 *
SNTP	Time Zone (GMT+08:00) Taipei Server IP Daylight Saving Time: Disabled
SNMP	Disabled
Syslog	System Activity: Enabled Wireless Activity: Enabled Notice: Enabled Remote Syslog Server: Disabled
SMTP	Disable

Wireless		
Basic Settings	Super G Mode	Disabled Super Mode can only be changed when Multi-SSID is disabled.
	Internal Station Connection	Enabled
Performance Settings	Data Rate	Auto
	Beacon Interval (ms)	100 * (Default: 100; Range: 20~1000 msec)
	DTIM	1 * (Default: 1; Range: 1~255)
	Fragment Length	2346 * (Default: 2346; Range: 256~2346)
	RTS Length	2346 * (Default: 2346; Range: 256~2346)
	Transmit Power	Full
	Wireless B/G Mode	11b Only
	Preamble	Short and Long
Connection Settings	Multi-SSID	Disabled
	Load Balance	Disabled
	Link Integrate	Disabled
	Antenna Diversity	Diversity

Multi-SSID Settings				
No.	SSID	Security	Status	Configure
Primary	DSA-6100-ssid1	WPA-RADIUS	Enabled	Configure

Access Control by MAC Address	
Status	Disabled
Access Control List	Configure

- ***General***

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.
- **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

- ***Wireless***

Basic Settings:

- **Super G Mode:** Select either **Disabled**, **Super G Mode with Turbo** or **Super G Mode without Turbo**. When Multi-SSID is selected as enabled, the item Super Mode cannot be active. Super G Mode can only be changed when Multi-SSID is disabled
- **Internal Station Connection:** Select either Enabled or Disabled. The connection allows clients to communicate with each other when enabled.

Performance 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.
- **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.
- **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.
- **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.
- **Wireless B/G mode:** Choose between Mixed, 11b only or 11g only. The function allows you to configure the wireless network with IEEE 802.11g only, IEEE 802.11b only, or IEEE 802.11g with backward

interoperability with IEEE 802.11b.

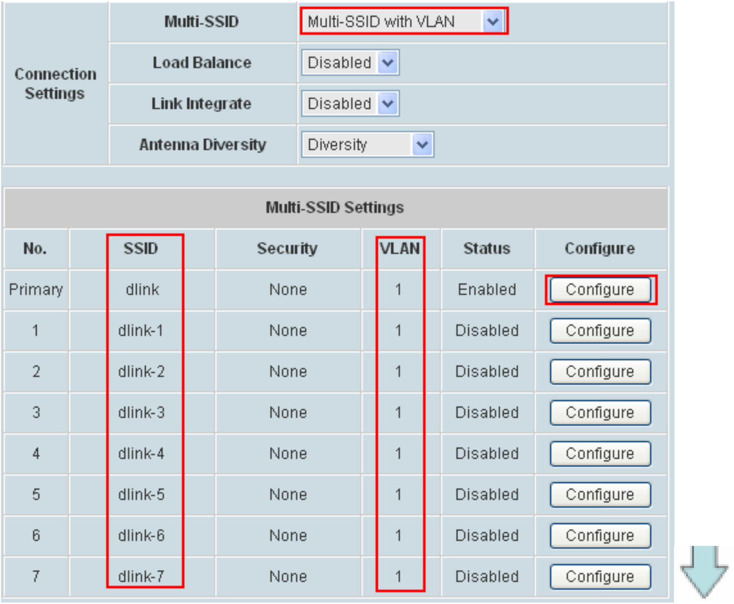
- **Mixed:** Select when using 802.11b and 802.11g wireless device.
- **802.11g Only:** Select when using all 802.11g wireless device.
- **802.11b Only:** Select when using all 802.11b wireless device.

- **Preamble:** Select Long Only or Short and Long. A short preamble is recommended for high-traffic networks.

Connection Settings:

- **Multi-SSID:** Multiple Service Set Identifier. Select either **Disabled**, **Multi-SSID with VLAN** or **Multi-SSID without VLAN**.
- **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:** Disable or Enable this feature.
- **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.

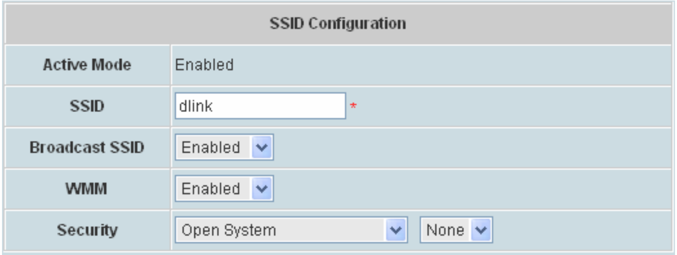
- ***Multi-SSID Settings*****:** Select **Disabled**, **Multi-SSID with VLAN** or **Multi-SSID without VLAN**. While *Multi-SSI*D enabled, **Super G Mode** will be disabled automatically. While selecting *Multi-SSID with VLAN*, Multi-SSID settings could configure up to multiple SSID. Click ***Configure*** button to setup SSID Configuration, the information of **SSID, Broadcast SSID, WMM** and **Security**.



Connection Settings	Multi-SSID	Multi-SSID with VLAN
	Load Balance	Disabled
	Link Integrate	Disabled
	Antenna Diversity	Diversity

Multi-SSID Settings

No.	SSID	Security	VLAN	Status	Configure
Primary	dlink	None	1	Enabled	Configure
1	dlink-1	None	1	Disabled	Configure
2	dlink-2	None	1	Disabled	Configure
3	dlink-3	None	1	Disabled	Configure
4	dlink-4	None	1	Disabled	Configure
5	dlink-5	None	1	Disabled	Configure
6	dlink-6	None	1	Disabled	Configure
7	dlink-7	None	1	Disabled	Configure



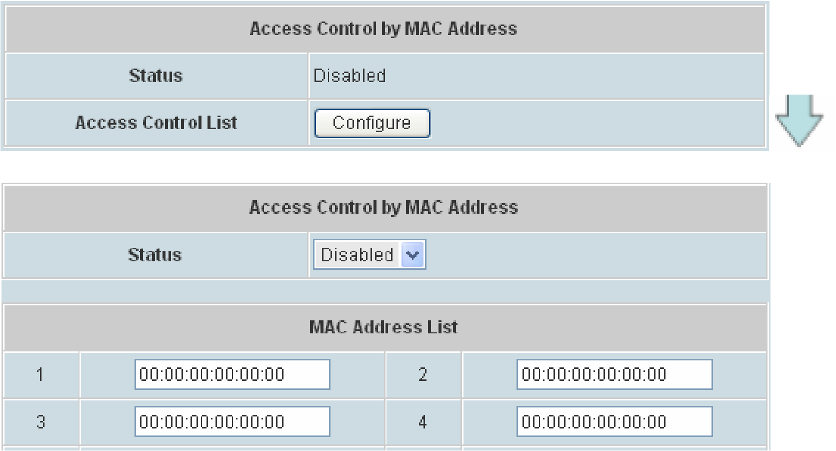
SSID Configuration

Active Mode	Enabled
SSID	dlink *
Broadcast SSID	Enabled
WMM	Enabled
Security	Open System · None

○ **SSID Configuration Page:**

- **SSID:** Service Set Identifier.
- **Broadcast SSID:** 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.
- **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.
- **Security:** Choose one of security types from SSID Configuration, also selecting whether WEP included or not.

- ***Access Control by MAC Address:*** MAC address based control for access the network (AP). 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.



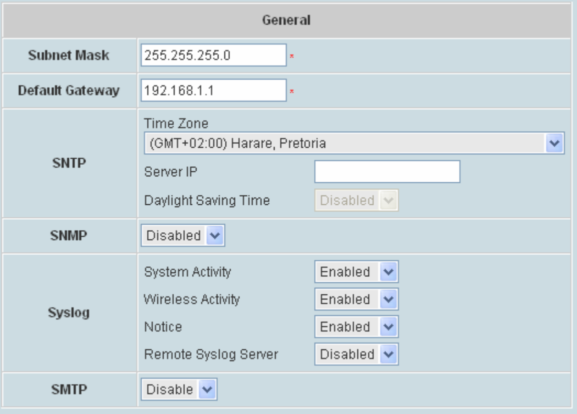
Access Control by MAC Address	
Status	Disabled
Access Control List	Configure

Access Control by MAC Address	
Status	Disabled

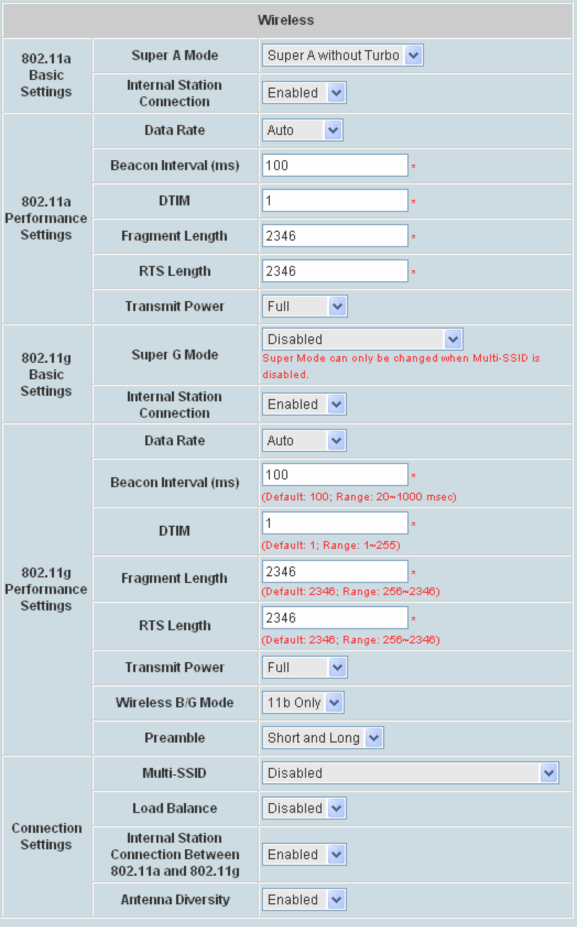
MAC Address List			
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00

III. DWL-8200AP

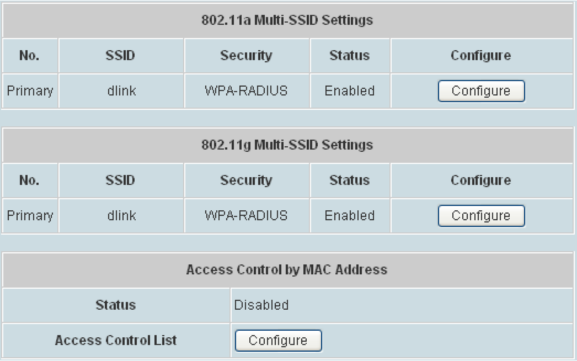
DWL-8200AP includes all three standards 802.11a, 802.11b and 802.11g. DWL-8200AP Templates settings allows users to configure 802.11a and 802.11b and g mode settings. The connection could be select to enable 802.11a, 802.11b/g, or disable. Compatible with 802.11a, 802.11b and 802.11g Devices that is 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.



General		
Subnet Mask	255.255.255.0 *	
Default Gateway	192.168.1.1 *	
SNTP	Time Zone	(GMT+02:00) Harare, Pretoria
	Server IP	
	Daylight Saving Time	Disabled
SNMP	Disabled	
Syslog	System Activity	Enabled
	Wireless Activity	Enabled
	Notice	Enabled
	Remote Syslog Server	Disabled
SMTP	Disable	



Wireless		
802.11a Basic Settings	Super A Mode	Super A without Turbo
	Internal Station Connection	Enabled
802.11a Performance Settings	Data Rate	Auto
	Beacon Interval (ms)	100 *
	DTIM	1 *
	Fragment Length	2346 *
	RTS Length	2346 *
	Transmit Power	Full
802.11g Basic Settings	Super G Mode	Disabled Super Mode can only be changed when Multi-SSID is disabled.
	Internal Station Connection	Enabled
802.11g Performance Settings	Data Rate	Auto
	Beacon Interval (ms)	100 * (Default: 100; Range: 20~1000 msec)
	DTIM	1 * (Default: 1; Range: 1~255)
	Fragment Length	2346 * (Default: 2346; Range: 256~2346)
	RTS Length	2346 * (Default: 2346; Range: 256~2346)
	Transmit Power	Full
	Wireless B/G Mode	11b Only
	Preamble	Short and Long
Connection Settings	Multi-SSID	Disabled
	Load Balance	Disabled
	Internal Station Connection Between 802.11a and 802.11g	Enabled
	Antenna Diversity	Enabled



802.11a Multi-SSID Settings				
No.	SSID	Security	Status	Configure
Primary	dlink	WPA-RADIUS	Enabled	Configure

802.11g Multi-SSID Settings				
No.	SSID	Security	Status	Configure
Primary	dlink	WPA-RADIUS	Enabled	Configure

Access Control by MAC Address	
Status	Disabled
Access Control List	Configure

- ***General***

  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.
  - **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

- ***Wireless***

  802.11a Basic Settings / 802.11g Basic Settings:

  - **Super Mode A/G Mode:** Select either **Disabled**, **Super A without Turbo**, **Super G without Turbo** or **Super G with Dynamic Turbo**. When Multi-SSID is selected as enabled, the item Super Mode cannot be active. Super G Mode can only be changed when Multi-SSID is disabled.
    - **Disabled:** Standard 802.11a/g support, no enhanced capability.
    - **Super A/G without Turbo:** Capable of Packet Bursting, FastFrames, Compression, and no Turbo mode.
    - **Super G with Dynamic Turbo:** Dynamic Turbo Mode is only enabled when all devices on the wireless

network are configured with Super Mode with Dynamic Turbo enabled.

- **Internal Station Connection:** Select either Enabled or Disabled. The connection allows clients to communicate with each other when enabled.

802.11a Performance Settings/ 802.11g Performance Settings:

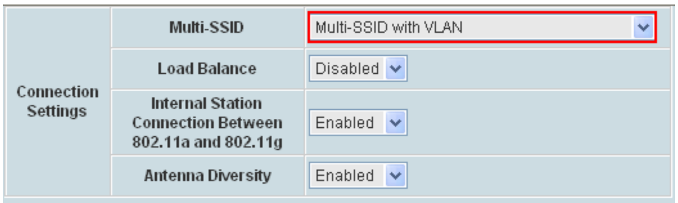
- **Data Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **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.
- **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.
- **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.
- **Wireless B/G mode:** Choose between Mixed, 11b only or 11g only. The function allows you to configure the wireless network with IEEE 802.11g only, IEEE 802.11b only, or IEEE 802.11g with backward interoperability with IEEE 802.11b.
    - **Mixed:** Select when using 802.11b and 802.11g wireless device.
    - **802.11g Only:** Select when using all 802.11g wireless device.
    - **802.11b Only:** Select when using all 802.11b wireless device.
- **Preamble:** Select Long Only or Short and Long. A short preamble is recommended for high-traffic networks.

Connection Settings:

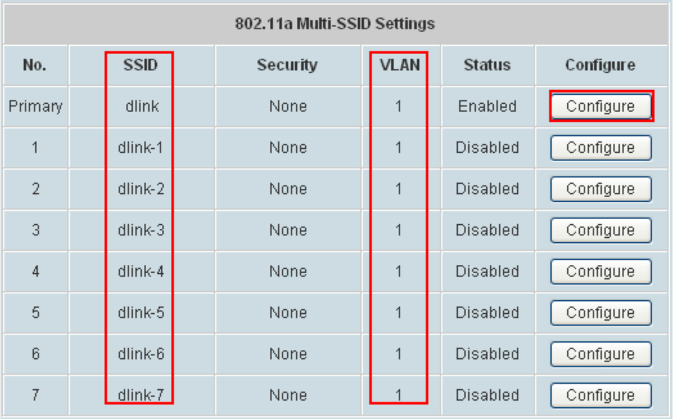
- **Multi-SSID:** Multiple Service Set Identifier. Select either **Disabled**, **Multi-SSID without VLAN 802.11g mode only**, **Multi-SSID without VLAN 802.11b mode only**, **Multi-SSID without VLAN for both modes** or **Multi-SSID with VLAN**.
- **Load Balance:** Select either **Enabled** or **Disabled**. 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.
- **Internal Station Connection Between 802.11a and 802.11g:** Select **Enabled** or **Disabled** the connection feature.
- **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.

- ***802.11g Multi-SSID Settings /802.11a Multi-SSID Settings:*** Select **Disabled**, **Multi-SSID without VLAN 802.11g mode only**, **Multi-SSID without VLAN 802.11b mode only**, **Multi-SSID without VLAN for both modes** or **Multi-SSID with VLAN**. While *Multi-SSI*D enabled, **Super G / A Mode** will be disabled automatically. While selecting *Multi-SSID with VLAN*, Multi-SSID settings could configure up to multiple SSID. Click ***Configure*** button to setup SSID Configuration, the information of **SSID, Broadcast SSID, WMM** and **Security**.

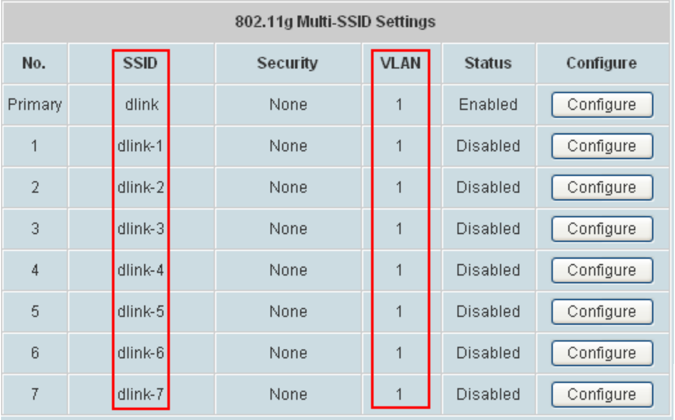


Connection Settings	Multi-SSID	Multi-SSID with VLAN
	Load Balance	Disabled
	Internal Station Connection Between 802.11a and 802.11g	Enabled
	Antenna Diversity	Enabled



802.11a Multi-SSID Settings

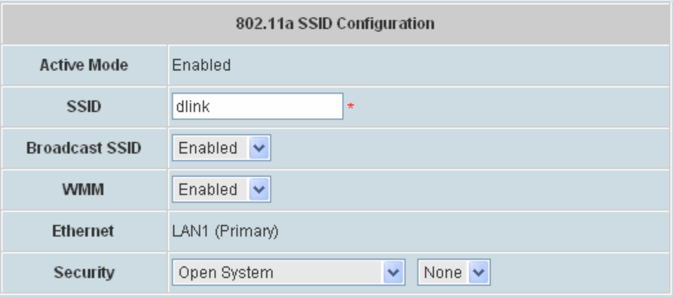
No.	SSID	Security	VLAN	Status	Configure
Primary	dlink	None	1	Enabled	Configure
1	dlink-1	None	1	Disabled	Configure
2	dlink-2	None	1	Disabled	Configure
3	dlink-3	None	1	Disabled	Configure
4	dlink-4	None	1	Disabled	Configure
5	dlink-5	None	1	Disabled	Configure
6	dlink-6	None	1	Disabled	Configure
7	dlink-7	None	1	Disabled	Configure



802.11g Multi-SSID Settings

No.	SSID	Security	VLAN	Status	Configure
Primary	dlink	None	1	Enabled	Configure
1	dlink-1	None	1	Disabled	Configure
2	dlink-2	None	1	Disabled	Configure
3	dlink-3	None	1	Disabled	Configure
4	dlink-4	None	1	Disabled	Configure
5	dlink-5	None	1	Disabled	Configure
6	dlink-6	None	1	Disabled	Configure
7	dlink-7	None	1	Disabled	Configure

Click button of ***Configure*** to further setup Multi-SSID Settings.

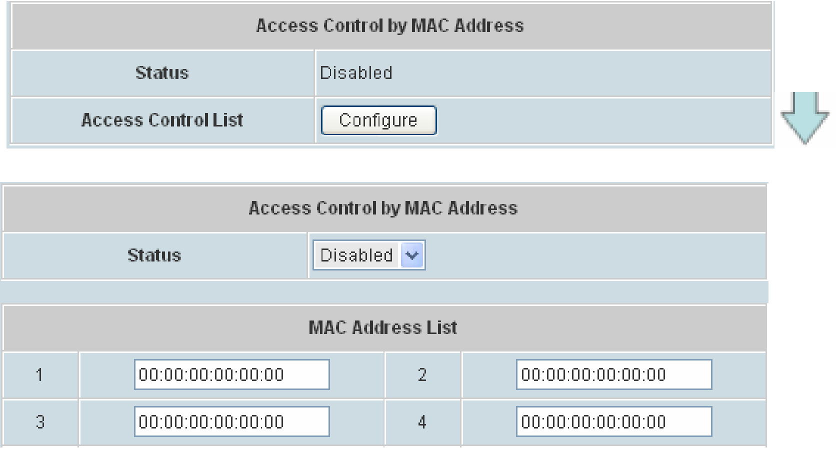


802.11a SSID Configuration

Active Mode	Enabled
SSID	dlink *
Broadcast SSID	Enabled
WMM	Enabled
Ethernet	LAN1 (Primary)
Security	Open System None

- **SSID Configuration Page:**
  - **SSID:** Service Set Identifier.
  - **Broadcast SSID:** 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.
  - **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.
  - **Security:** Choose one of security types from SSID Configuration, also selecting whether WEP included or not.

- ***Access Control by MAC Address:*** MAC address based control for access the network (AP). 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.



Access Control by MAC Address	
Status	Disabled
Access Control List	Configure

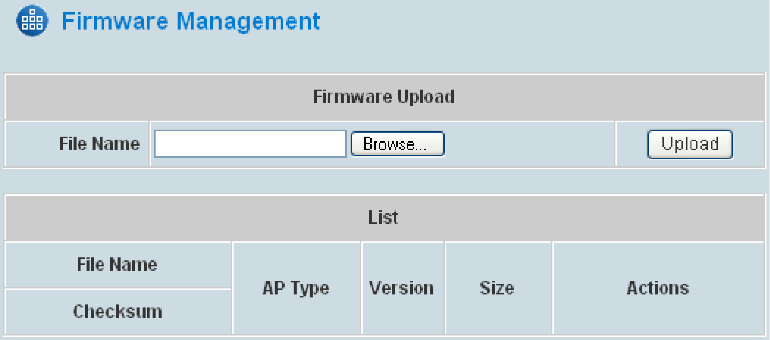
Access Control by MAC Address	
Status	Disabled

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

4.3.5 Firmware Management

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.

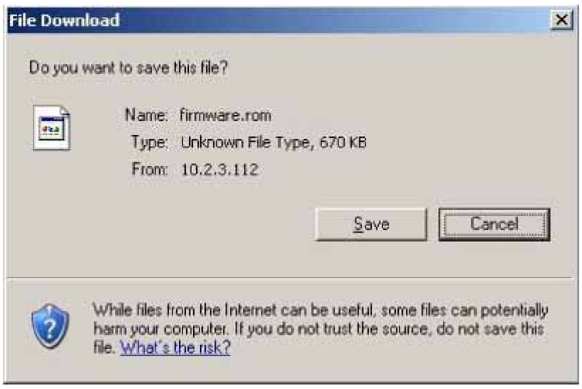


Firmware Management

Firmware Upload		
File Name		Upload

List				
File Name Checksum	AP Type	Version	Size	Actions

- **File Name:** The name of the AP firmware to be uploaded.
- **Upload:** Click ***Upload*** button to upload the file from a local disk to the system.
- **List:** All uploaded firmware will be listed here.
- **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.



File Download

Do you want to save this file?

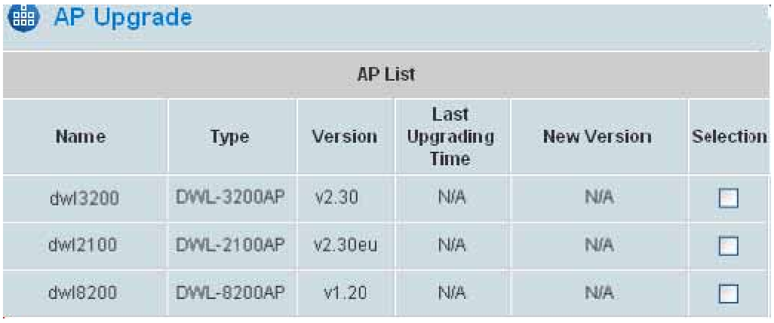
Name: firmware.rom
Type: Unknown File Type, 670 KB
From: 10.2.3.112

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

- **Delete:** Can be clicked to delete the current firmware.

4.3.6 AP 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.



AP Upgrade

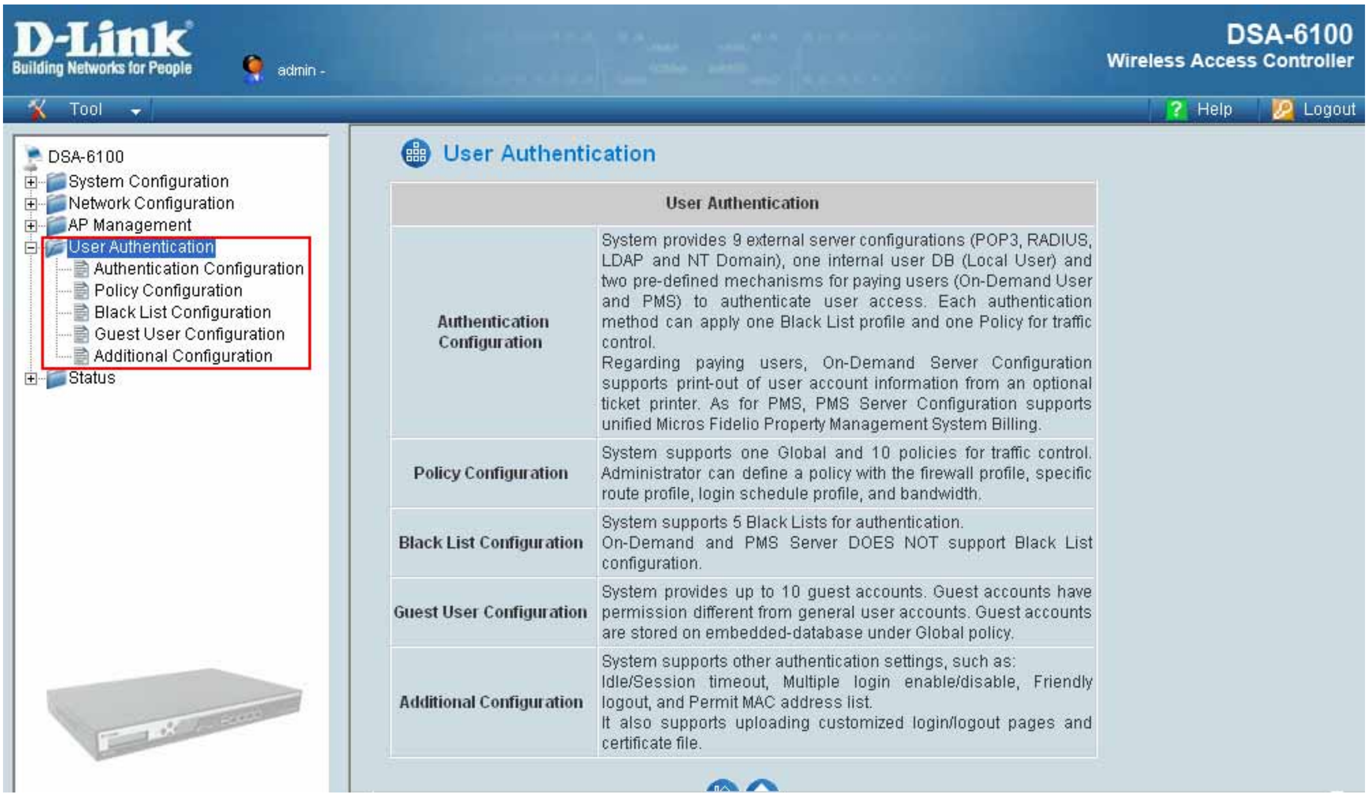
AP List

Name	Type	Version	Last Upgrading Time	New Version	Selection
dwl3200	DWL-3200AP	v2.30	N/A	N/A	□
dwl2100	DWL-2100AP	v2.30eu	N/A	N/A	□
dwl8200	DWL-8200AP	v1.20	N/A	N/A	□

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

4.4 User Authentication

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

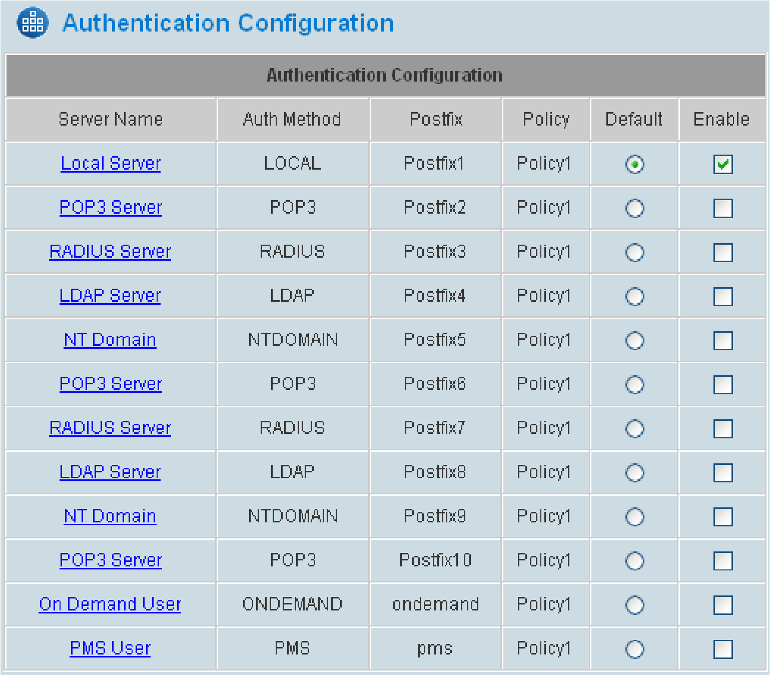


User Authentication

User Authentication	
Authentication Configuration	System provides 9 external server configurations (POP3, RADIUS, LDAP and NT Domain), one internal user DB (Local User) and two pre-defined mechanisms for paying users (On-Demand User and PMS) to authenticate user access. Each authentication method can apply one Black List profile and one Policy for traffic control. Regarding paying users, On-Demand Server Configuration supports print-out of user account information from an optional ticket printer. As for PMS, PMS Server Configuration supports unified Micros Fidelio Property Management System Billing.
Policy Configuration	System supports one Global and 10 policies for traffic control. Administrator can define a policy with the firewall profile, specific route profile, login schedule profile, and bandwidth.
Black List Configuration	System supports 5 Black Lists for authentication. On-Demand and PMS Server DOES NOT support Black List configuration.
Guest User Configuration	System provides up to 10 guest accounts. Guest accounts have permission different from general user accounts. Guest accounts are stored on embedded-database under Global policy.
Additional Configuration	System supports other authentication settings, such as: Idle/Session timeout, Multiple login enable/disable, Friendly logout, and Permit MAC address list. It also supports uploading customized login/logout pages and certificate file.

4.4.1 Authentication Configuration

The system supports up to 9 external user authentication servers of using one of the RADIUS, LDAP, POP3, and NT Domain, plus three internal user authentication servers of Local User, On-demand User and PMS User. The system may authenticate users based on external authentication servers and/or local user database. Each user is distinguished by the postfix with the username. This function is to configure the settings for different authentication servers. Using the DSA-6100, on-demand user and PMS user can be administered with different policy. Click on the server name to set the related configurations for that particular server. After completing and clicking ***Apply*** to save the settings, go back to the previous screen to choose a server to be the default server and enable or disable any server on the list.



Authentication Configuration

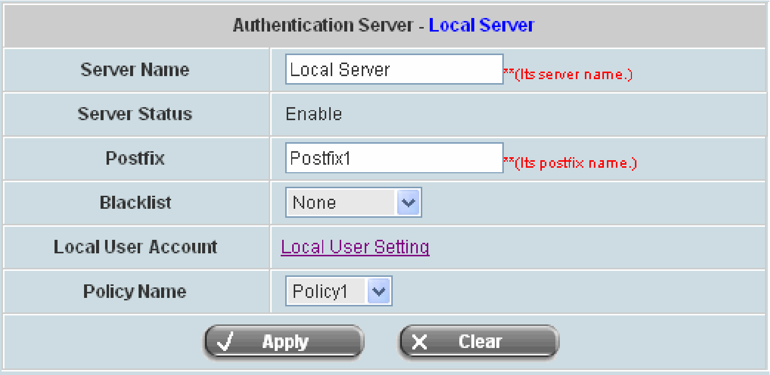
Authentication Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enable
Local Server	LOCAL	Postfix1	Policy1	●	☑
POP3 Server	POP3	Postfix2	Policy1	○	□
RADIUS Server	RADIUS	Postfix3	Policy1	○	□
LDAP Server	LDAP	Postfix4	Policy1	○	□
NT Domain	NTDOMAIN	Postfix5	Policy1	○	□
POP3 Server	POP3	Postfix6	Policy1	○	□
RADIUS Server	RADIUS	Postfix7	Policy1	○	□
LDAP Server	LDAP	Postfix8	Policy1	○	□
NT Domain	NTDOMAIN	Postfix9	Policy1	○	□
POP3 Server	POP3	Postfix10	Policy1	○	□
On Demand User	ONDEMAND	ondemand	Policy1	○	□
PMS User	PMS	pms	Policy1	○	□

- **Server Name:** There are several kinds of authentication options supported by DSA-6100: Local Server, POP3 Server, RADIUS Server, LDAP Server, NT Domain, On-demand User and PMS User. Click the hyperlink of the respective Authentication Option to enter the Authentication Option page.
- **Authentication Method:** The field selects the authentication method used in the server. There are different authentication methods supported in DSA-6100 Authentication Database: Local, POP3, RADIUS, LDAP, NT Domain, On Demand and PMS.
- **Postfix:** Set a postfix that is easy to identify (e.g. local) for the authentication option by 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.

4.4.1.1 Local Server

This server is only for **“Local User”** and the authentication method can not be changed for this server which manages user accounts on lists of the local user setting.

Choose **“Local Server”** in the **Server Name** field, the hyperlink beside the pull-down menu will become setting of **“Local Server”**.



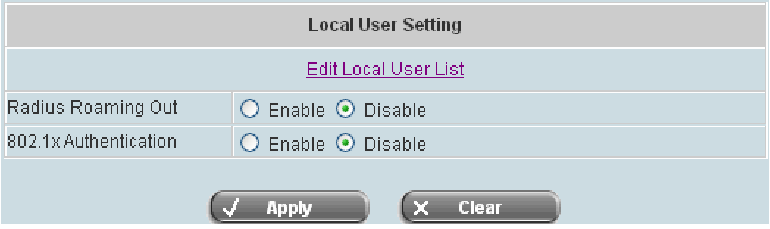
Authentication Server - Local Server	
Server Name	Local Server **(Its server name.)
Server Status	Enable
Postfix	Postfix1 **(Its postfix name.)
Blacklist	None
Local User Account	Local User Setting
Policy Name	Policy1

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

***Warning:** The Postfix Name cannot contain these words: MAC and IP.*

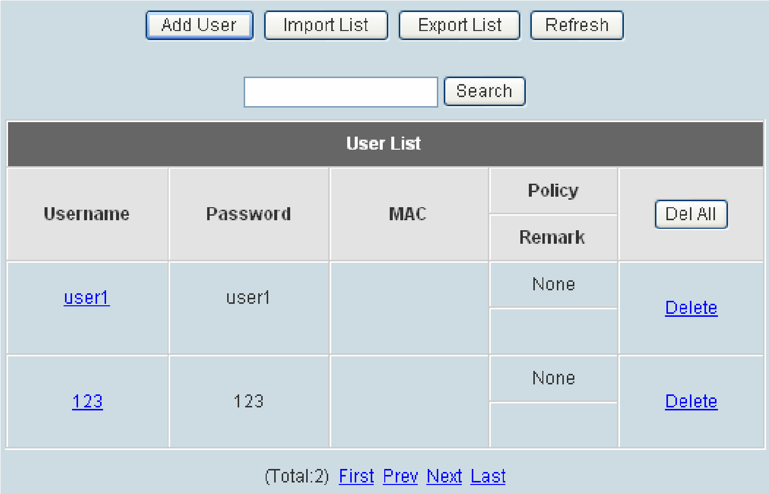
- **Blacklist:** There are five sets of the black lists. Select one of them or choose **“None”**. Please refer to **4.4.3 Black List Configuration.**
- **Local User Account:** Click the Local User Setting hyperlink to set the further configuration.
- **Policy Name:** There are ten policies to choose from to apply to this particular server.

Clicking in the ***Local User Setting***:



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

- **Edit Local User List:** Click this to enter the **“User List”** screen. View, add, delete and backup user accounts.
- **Radius Roaming Out:** Enable or disable roaming out. When enabled, this system becomes a RADIUS server for other external RADIUS clients.
- **802.1x Authentication:** Enable or disable 802.1x Authentication. When enabled, this system becomes a RADIUS server for other external RADIUS clients as long as the RADIUS clients are configured accordingly.

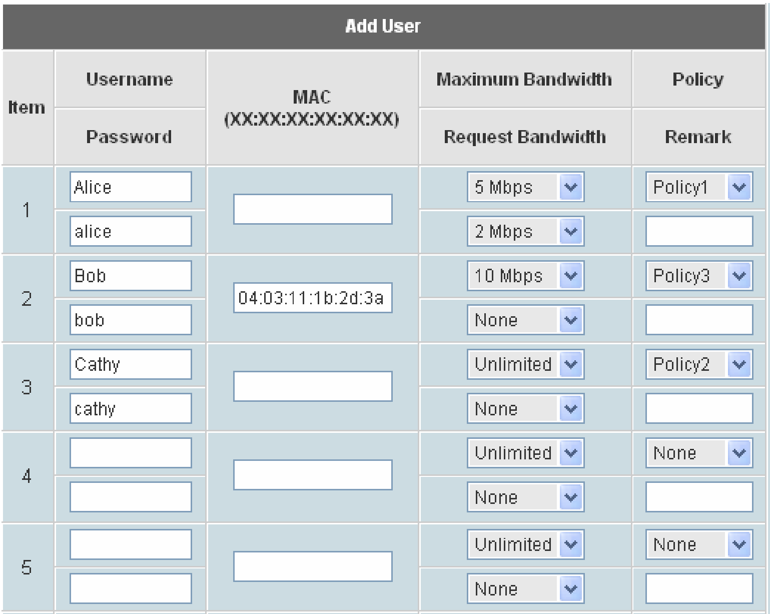


User List

Username	Password	MAC	Policy Remark	Del All
user1	user1		None	Delete
123	123		None	Delete

(Total:2) First Prev Next Last

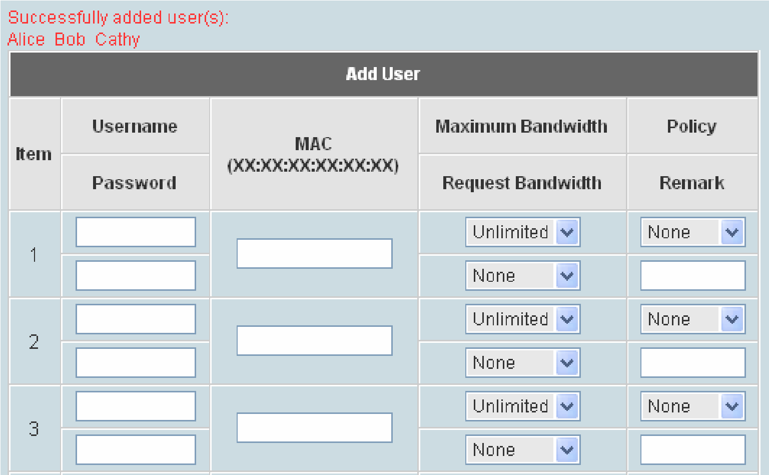
Add User: Click this button to enter into the **Add User** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC"** and **"Remark"**. Select a desired **Maximum Bandwidth**, **Request Bandwidth** and **Policy**. **"Username"** and **"Password"** are required information, the rest are optional, For the Policy configuration, please check section of Policy Configuration.



Add User

Item	Username Password	MAC (XX:XX:XX:XX:XX:XX)	Maximum Bandwidth Request Bandwidth	Policy Remark
1	Alice alice		5 Mbps 2 Mbps	Policy1
2	Bob bob	04:03:11:1b:2d:3a	10 Mbps None	Policy3
3	Cathy cathy		Unlimited None	Policy2
4			Unlimited None	None
5			Unlimited None	None

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

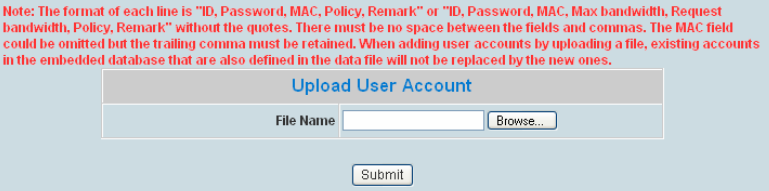


Successfully added user(s):
Alice Bob Cathy

Add User

Item	Username Password	MAC (XX:XX:XX:XX:XX:XX)	Maximum Bandwidth Request Bandwidth	Policy Remark
1			Unlimited None	None
2			Unlimited None	None
3			Unlimited None	None

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

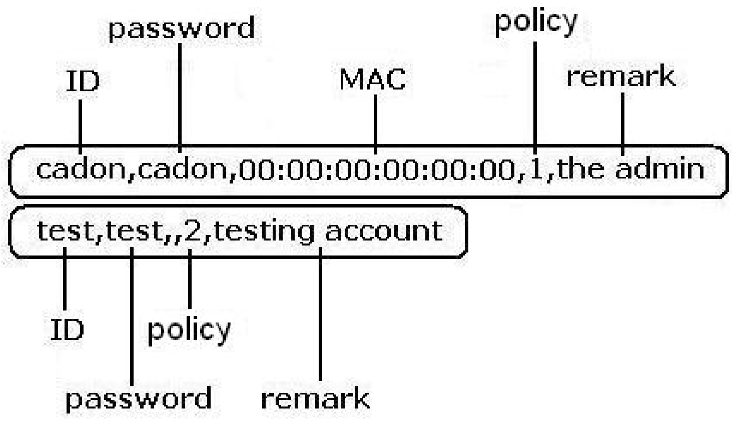


Note: The format of each line is "ID, Password, MAC, Policy, Remark" or "ID, Password, MAC, Max bandwidth, Request bandwidth, Policy, Remark" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.

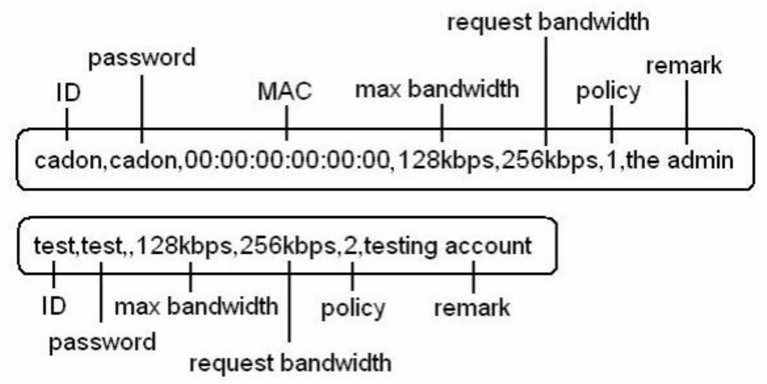
Upload User Account

File Name

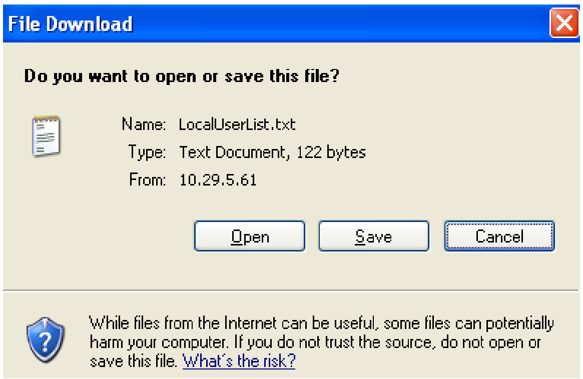
The uploading file should be a text file and the format of each line is ***"ID, Password, MAC, Policy, Remark"*** or ***"ID, Password, MAC, Max bandwidth, Request bandwidth, Policy, Remark"*** without the quotes. There must be no spaces between the fields and commas. The MAC field can be omitted, but 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 new ones.



password
policy
ID
MAC
remark
cadon,cadon,00:00:00:00:00:00,1,the admin
test,test,,2,testing account
ID
policy
password
remark



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



Do you want to open or save this file?

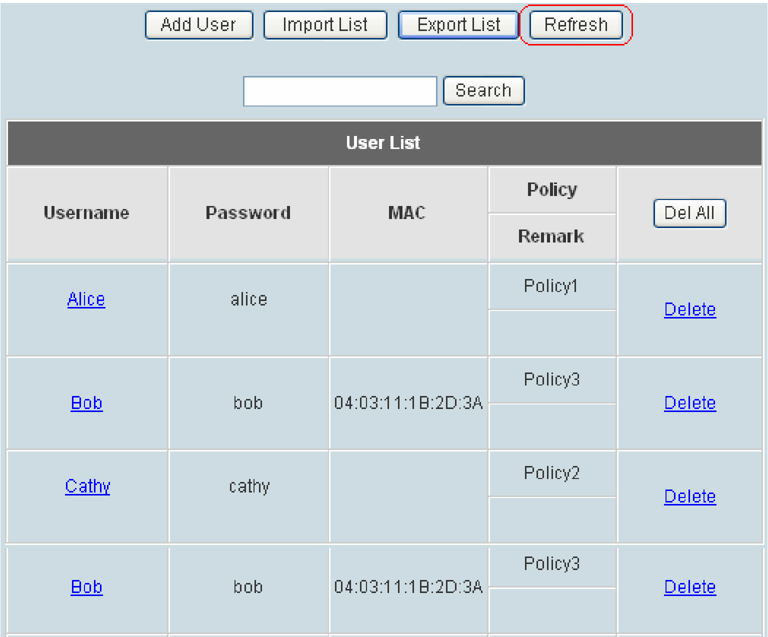
Name: LocalUserList.txt

Type: Text Document, 122 bytes

From: 10.29.5.61

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

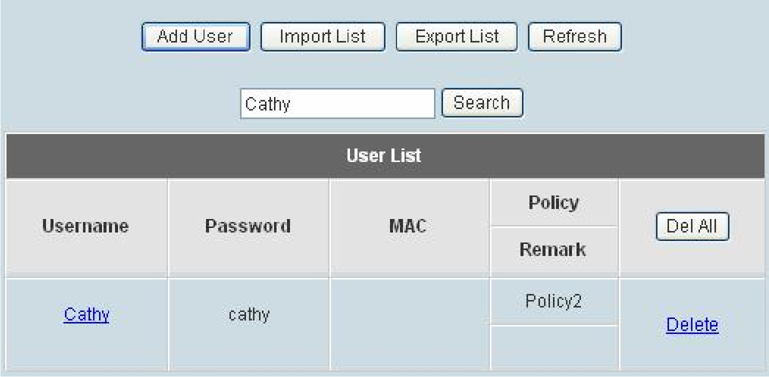
- **Refresh:** Click this to renew the list. Refresh button.



User List

Username	Password	MAC	Policy Remark	Del All
Alice	alice		Policy1	Delete
Bob	bob	04:03:11:1B:2D:3A	Policy3	Delete
Cathy	cathy		Policy2	Delete
Bob	bob	04:03:11:1B:2D:3A	Policy3	Delete

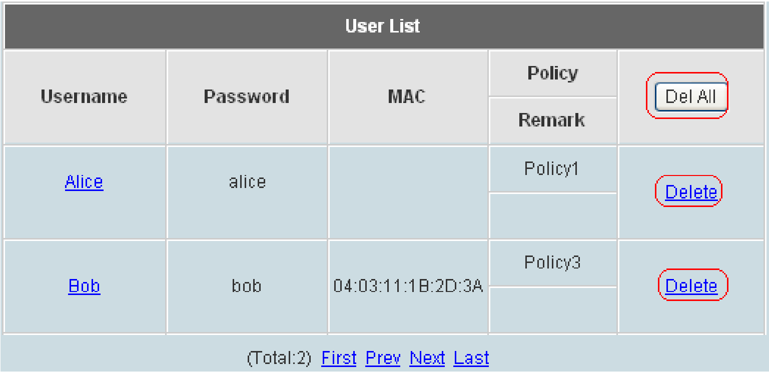
- **Search:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.



User List

Username	Password	MAC	Policy Remark	Del All
Cathy	cathy		Policy2	Delete

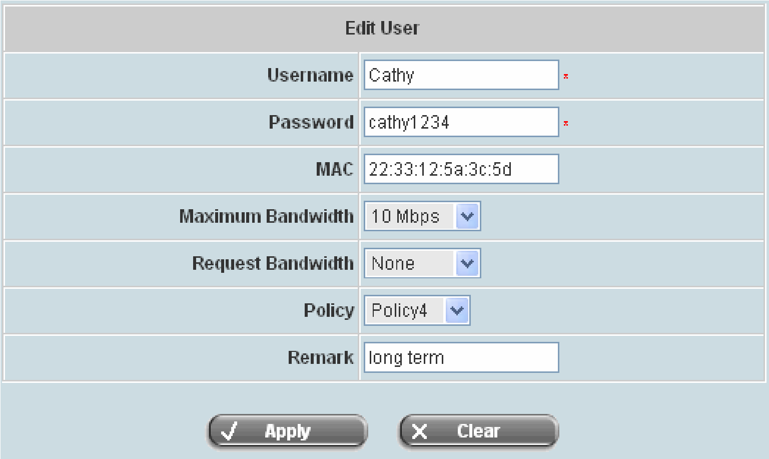
- **Del All:** click on this button to delete all the users at once and click on **Delete** to delete the user individually.



User List

Username	Password	MAC	Policy Remark	Del All
Alice	alice		Policy1	Delete
Bob	bob	04:03:11:1B:2D:3A	Policy3	Delete

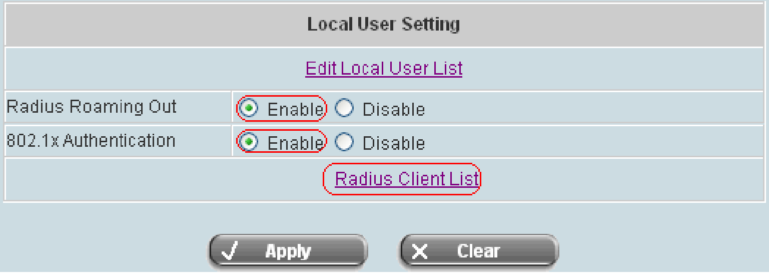
- **Edit User**: If editing the content of individual user account is needed, click the username of the desired user account to enter the **Edit User** Interface for that particular user, and then modify or add any desired information such as **"Username"**, **"Password"**, **"MAC"**, **"Maximum Bandwidth"**,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



Edit User

Username	Cathy *
Password	cathy1234 *
MAC	22:33:12:5a:3c:5d
Maximum Bandwidth	10 Mbps
Request Bandwidth	None
Policy	Policy4
Remark	long term

- **RADIUS Roaming Out / 802.1x Authentication:** When RADIUS Roaming Out is enabled, this system becomes a RADIUS server for other external RADIUS clients. The Local user with RADIUS roaming out permission need to be configured in the Radius Client List first. The Local user in the list may then log on the system via the other domain, such as a branch office, as long as the RADIUS clients are configured accordingly. Selecting either of the options will bring up the hyperlink called ***RADIUS Client List***.



Local User Setting

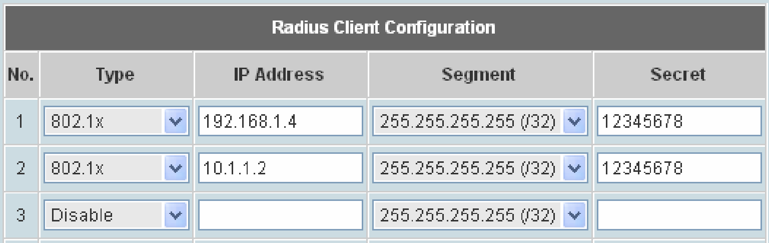
Edit Local User List

Radius Roaming Out	● Enable ○ Disable
802.1x Authentication	● Enable ○ Disable

Radius Client List

- **RADIUS Client List:** Configure RADIUS clients and secret key. Local user may log on any of the listed RADIUS clients as long as the RADIUS clients are configured accordingly.

Click the hyperlink ***RADIUS Client List*** to enter the **RADIUS Client Configuration interface**. Choose the desired type, **Disable**, **Roaming Out** or **802.1x** and key in the related data and then click ***Apply*** to complete the settings.



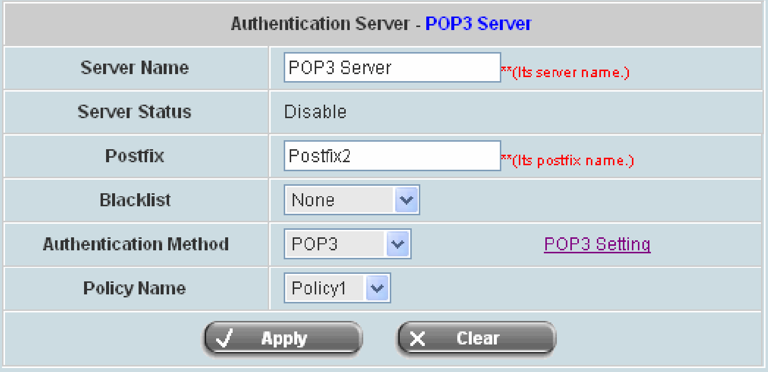
Radius Client Configuration

No.	Type	IP Address	Segment	Secret
1	802.1x	192.168.1.4	255.255.255.255 (/32)	12345678
2	802.1x	10.1.1.2	255.255.255.255 (/32)	12345678
3	Disable		255.255.255.255 (/32)	

- **802.1x Authentication:** 802.1x is a security standard for wired and wireless LANs. It encapsulates EAP (Extensible Authentication Protocol) processes into Ethernet packets instead of using the protocol's native PPP (Point-to-Point Protocol) environment, thus reducing some network overhead. It also puts the bulk of the processing burden upon the client (called a supplicant in 802.1x parlance) and the authentication server (such as a RADIUS), letting the "authenticator" middleman simply pass the packets back and forth.

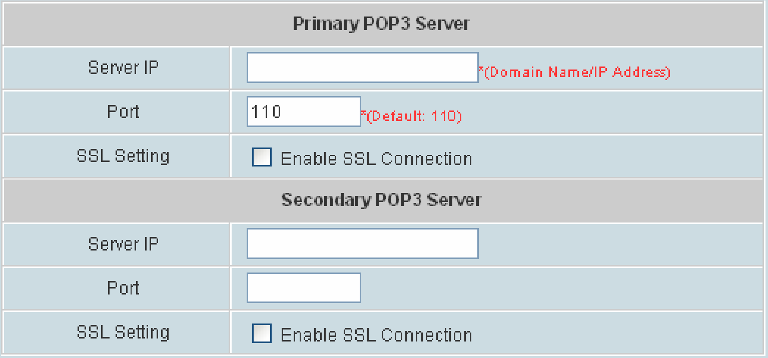
4.4.1.2 POP3 Server

The system may authenticate users using their POP3 email account. You may configure both primary and secondary POP3 server for fault tolerance. POP3 refers to Post Office Protocol 3, a standard protocol used to retrieve email stored in a mail server. The system may authenticate users by using POP mail accounts. Two POP3 servers are supported by the system, primary and secondary. When POP3 Server is enabled, at least one POP3 server is needed. Choose **"POP3"** in the **Server Name** field, the hyperlink beside the pull-down menu will become **"POP3 Setting"**.



Authentication Server - POP3 Server	
Server Name	POP3 Server **(Its server name.)
Server Status	Disable
Postfix	Postfix2 **(Its postfix name.)
Blacklist	None
Authentication Method	POP3 POP3 Setting
Policy Name	Policy1

Click the hyperlink ***POP3 Setting*** for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the ***Apply*** button.

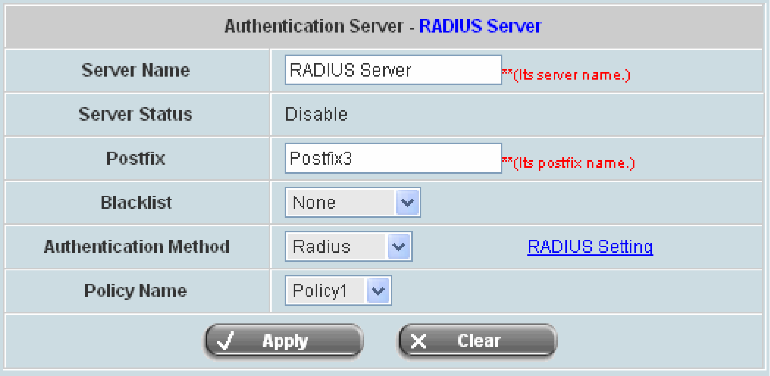


Primary POP3 Server	
Server IP	*(Domain Name/IP Address)
Port	110 *(Default: 110)
SSL Setting	☐ Enable SSL Connection
Secondary POP3 Server	
Server IP	
Port	
SSL Setting	☐ Enable SSL Connection

- **Server IP:** Enter the IP address/domain name given by the ISP.
- **Port:** Enter the Port given by the ISP. The default value is 110.
- **SSL Setting:** If this option is enabled, the POP3 protocol will perform the authentication.

4.4.1.3 RADIUS Server

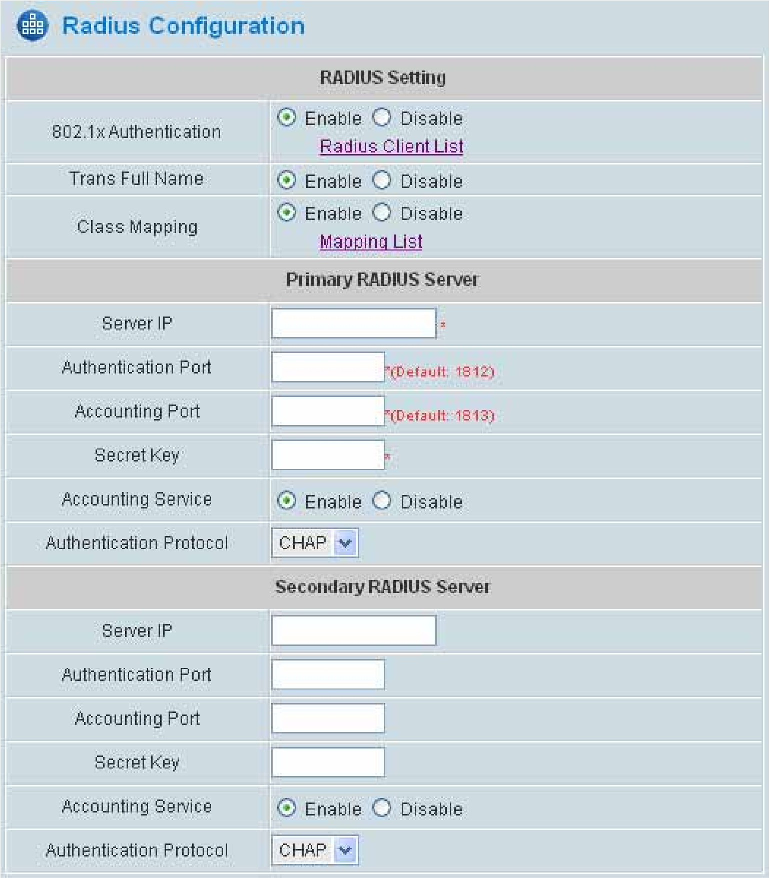
The system supports 802.1x Authentication using external RADIUS server. You may configure both primary and secondary RADIUS server for fault tolerance. RADIUS refers to Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). The system may authenticate users using external RADIUS server including both primary and secondary RADIUS server. Choose **“RADIUS Server”** in the **Server Name** field, the hyperlink beside the pull-down menu will become **“RADIUS Setting”**.



Authentication Server - RADIUS Server

Server Name	RADIUS Server **(Its server name.)
Server Status	Disable
Postfix	Postfix3 **(Its postfix name.)
Blacklist	None
Authentication Method	Radius RADIUS Setting
Policy Name	Policy1

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



Radius Configuration

RADIUS Setting	
802.1x Authentication	● Enable ○ Disable Radius Client List
Trans Full Name	● Enable ○ Disable
Class Mapping	● Enable ○ Disable Mapping List
Primary RADIUS Server	
Server IP	*
Authentication Port	*(Default: 1812)
Accounting Port	*(Default: 1813)
Secret Key	*
Accounting Service	● Enable ○ Disable
Authentication Protocol	CHAP
Secondary RADIUS Server	
Server IP	
Authentication Port	
Accounting Port	
Secret Key	
Accounting Service	● Enable ○ Disable
Authentication Protocol	CHAP

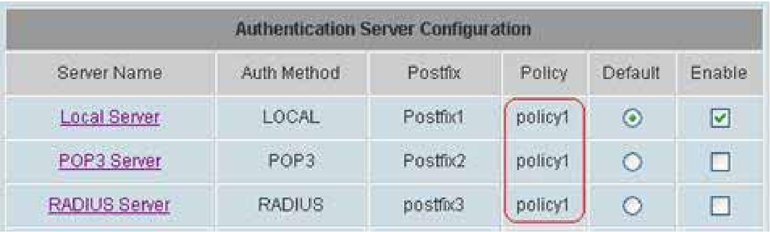
- **802.1X Authentication:** When enabled, this system can authenticate RADIUS clients against the external RADIUS server. Enable this function and the hyperlink of ***RADIUS Client List*** will appear. Click the hyperlink to get into the RADIUS Client Configuration list for further configuration. Please refer to **RADIUS Roaming Out/802.1x Authentication** in **4.4.1.1 Local Server**.
- **RADIUS Client List:** The administrator could further set up for the 802.1x capable device that are allowed to be authenticated against the external RADIUS server via this system. Select type "802.1x Authentication" from the drop down list, and then enter IP address, Subnet Mask, and shared Secret Key of the authorized devices.
- **Trans Full Name:** When enabled, both the username and postfix will be transferred to the RADIUS server for authentication. When disabled, only the username will be transferred to RADIUS server for authentication.
- **Class Mapping:** Class Attribute can be specified to map to internal Policy.
- **Server IP:** Enter the IP address/domain name of the RADIUS server.
- **Authentication Port:** Enter the authentication port of the RADIUS server and the default value is 1812.
- **Accounting Port:** Enter the accounting port of the RADIUS server and the default value is 1813.
- **Secret Key:** Enter the key for encryption and decryption.
- **Accounting Service:** Select this to enable or disable the **"Accounting Service"** for accounting capabilities.
- **Authentication Protocol:** Define authentication transmission protocol. Configurations must match remote RADIUS configurations. PAP (Password Authentication Protocol) transmit password in plain text without encryption. CHAP (Challenge Handshake Authentication Protocol) is a more secured authentication protocol using hash encryption.

Notice: *If RADIUS Server does not assign idle-timeout value, DSA-6100 will use the local idle-timeout instead.*

- **Class Mapping**

  In DSA6100, each authentication server can be associated with a policy.

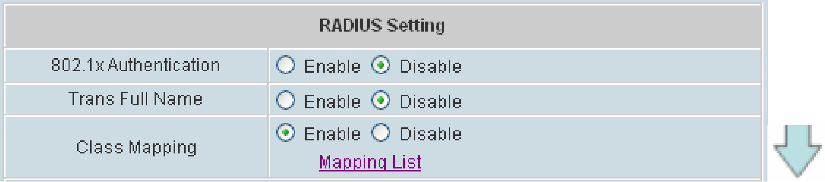
  The policy at this level is to provide a default policy value. Under a server, a different policy may be further specified for a specific sub-group or a specific user to override the default policy.



Authentication Server Configuration

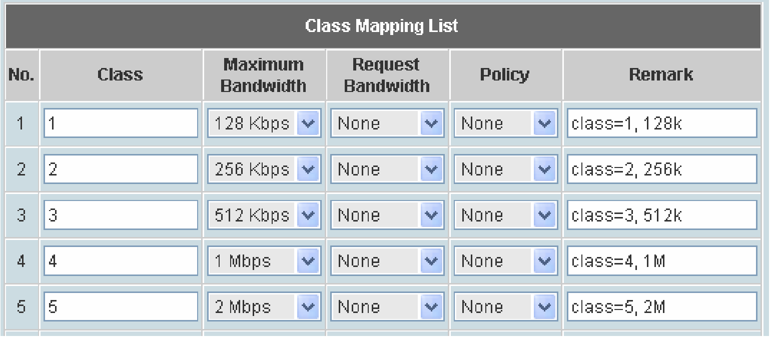
Server Name	Auth Method	Postfix	Policy	Default	Enable
Local Server	LOCAL	Postfix1	policy1	●	☑
POP3 Server	POP3	Postfix2	policy1	○	□
RADIUS Server	RADIUS	postfix3	policy1	○	□

For a **RADIUS server**, if a **class mapping** is enabled, a configuration page allows the mapping of RADIUS class attributes to a policy on DSA-6100. If there is no policy chosen for a RADIUS Class attribute, the total bandwidth for that RADIUS Class is bounded by the total bandwidth of the default policy of the authentication server. If there is a specific policy selected for that RADIUS Class attribute, the total bandwidth of that class is bounded by the total bandwidth of the chosen policy. The **maximum bandwidth** allowed for the users of a class is also set in this page of **RADIUS Class configuration**.



RADIUS Setting

802.1x Authentication	○ Enable ● Disable
Trans Full Name	○ Enable ● Disable
Class Mapping	● Enable ○ Disable Mapping List

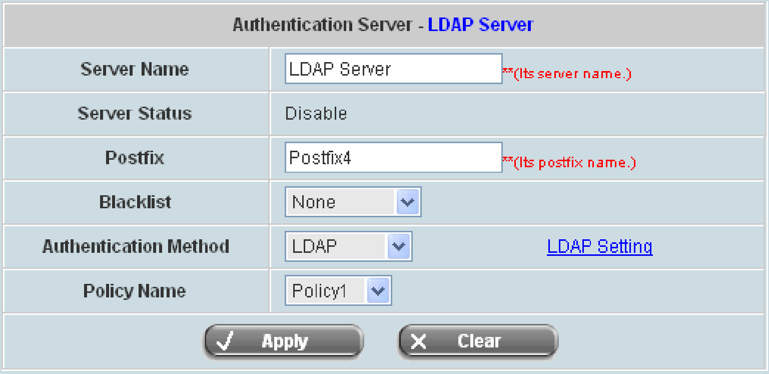


Class Mapping List

No.	Class	Maximum Bandwidth	Request Bandwidth	Policy	Remark
1	1	128 Kbps	None	None	class=1, 128k
2	2	256 Kbps	None	None	class=2, 256k
3	3	512 Kbps	None	None	class=3, 512k
4	4	1 Mbps	None	None	class=4, 1M
5	5	2 Mbps	None	None	class=5, 2M

4.4.1.4 LDAP Server

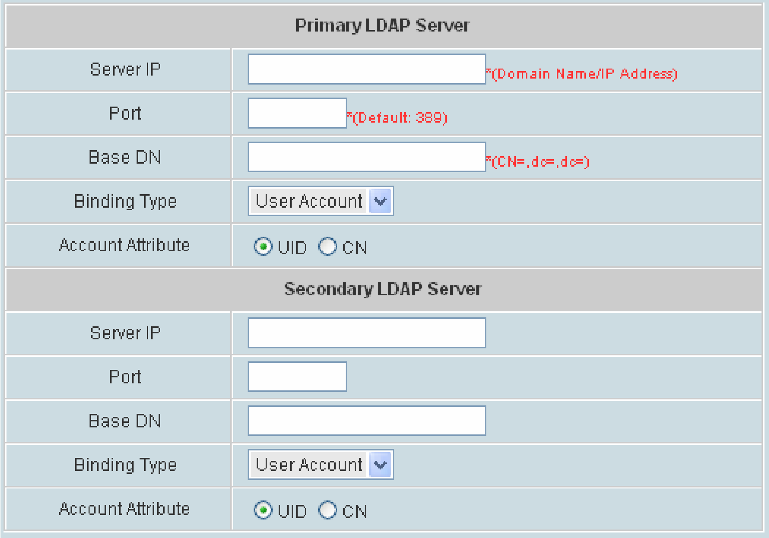
The system may authenticate users using external LDAP server. You may configure both primary and secondary LDAP server for fault tolerance. LDAP refers to Lightweight Directory Access Protocol, a set of protocols for accessing information directories. The system may authenticate users using external LDAP server including both primary and secondary. Choose **"LDAP"** in the **Server Name** field, the hyperlink beside the pull-down menu will become **"LDAP Setting"**.



Authentication Server - LDAP Server

Server Name	LDAP Server **(Its server name.)
Server Status	Disable
Postfix	Postfix4 **(Its postfix name.)
Blacklist	None
Authentication Method	LDAP — LDAP Setting
Policy Name	Policy1

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



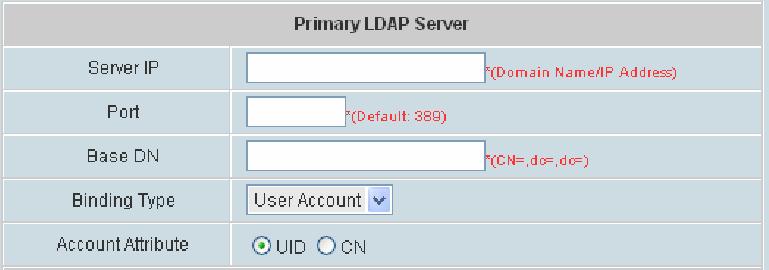
Primary LDAP Server

Server IP	*(Domain Name/IP Address)
Port	*(Default: 389)
Base DN	*(CN=,dc=,dc=)
Binding Type	User Account
Account Attribute	● UID ○ CN

Secondary LDAP Server

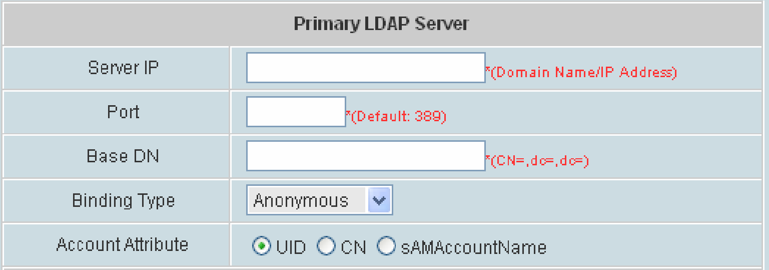
Server IP	
Port	
Base DN	
Binding Type	User Account
Account Attribute	● UID ○ CN

- **Server IP:** Enter the IP address/domain name of the LDAP server.
- **Port:** Enter the Port of the LDAP server, and the default value is 389.
- **Base DN:** Enter the distinguished name of the LDAP server.
- **Binding Type:** There are four binding types, User Account, Anonymous, Specific DN and Windows AD to select.
  - **User Account**: Use the user account's login username and password of the system, and then select one **Account Attribute** (UID, CN) to access the LDAP server.
- **Account Attribute:** Attribute of LDAP accounts.



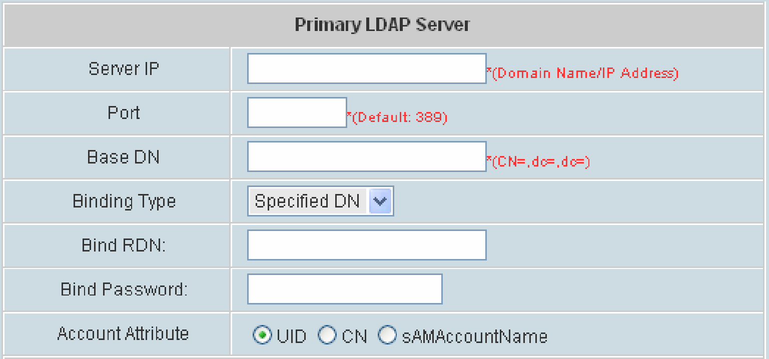
Primary LDAP Server	
Server IP	*(Domain Name/IP Address)
Port	*(Default: 389)
Base DN	*(CN=,dc=,dc=)
Binding Type	User Account
Account Attribute	● UID ○ CN

- **Anonymous:** Access the LDAP servers without requiring authentication but only select one **Account Attribute** (UID, CN or Account Name).



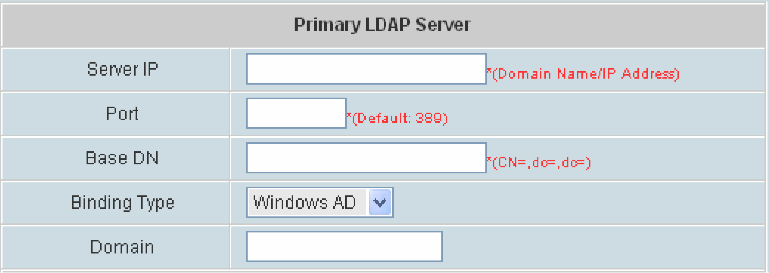
Primary LDAP Server	
Server IP	*(Domain Name/IP Address)
Port	*(Default: 389)
Base DN	*(CN=,dc=,dc=)
Binding Type	Anonymous
Account Attribute	● UID ○ CN ○ sAMAccountName

- **Specified DN:** Entering the specific DN username and password in the **"Bind RDN"** and **"Bind Password"** fields, and then select one **Account Attribute** (UID, CN or Account Name) to access the LDAP server.



Primary LDAP Server	
Server IP	*(Domain Name/IP Address)
Port	*(Default: 389)
Base DN	*(CN=,dc=,dc=)
Binding Type	Specified DN
Bind RDN:	
Bind Password:	
Account Attribute	● UID ○ CN ○ sAMAccountName

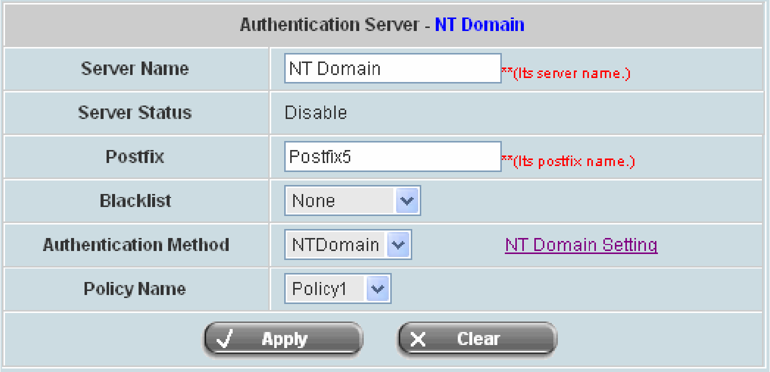
- **Window AD:** Enter the domain name of Windows AD to access the LDAP server.



Primary LDAP Server	
Server IP	*(Domain Name/IP Address)
Port	*(Default: 389)
Base DN	*(CN=,dc=,dc=)
Binding Type	Windows AD
Domain	

4.4.1.5 NT Domain Server

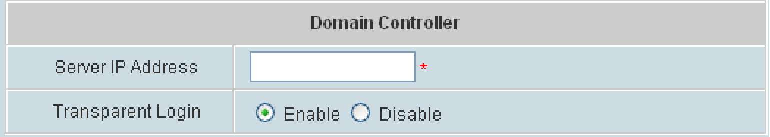
This system may authenticate users using external MS Domain Server. NT Domain Server refers to external MS Domain Server. Choose **"NTDomain"** in the **Server Name** field, the hyperlink beside the pull-down menu will become **"NT Domain Setting"**.



Authentication Server - NT Domain

Server Name	NT Domain **(Its server name.)
Server Status	Disable
Postfix	Postfix5 **(Its postfix name.)
Blacklist	None
Authentication Method	NTDomain NT Domain Setting
Policy Name	Policy1

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



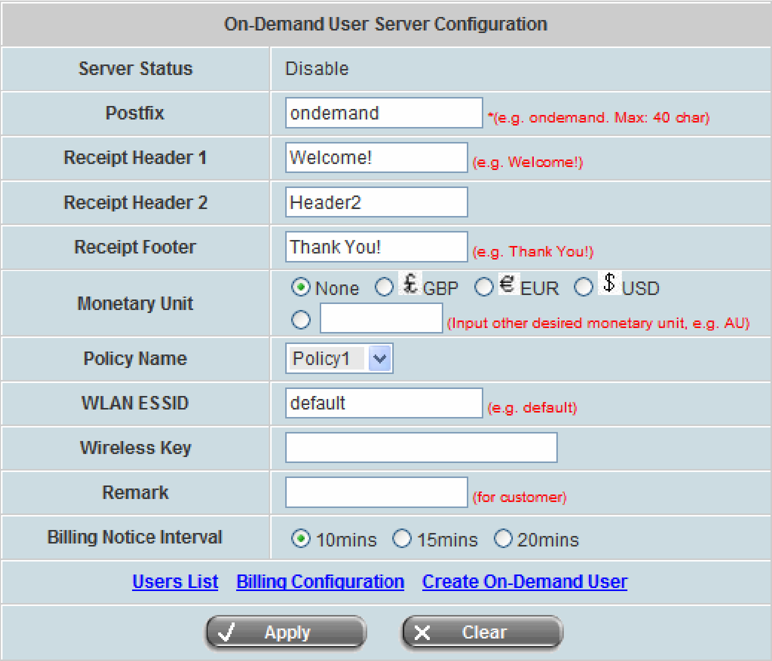
Domain Controller

Server IP Address	*
Transparent Login	● Enable ○ Disable

- **Server IP Address:** Domain Server IP address. Enter the server IP address of the domain controller.
- **Transparent Login:** Enable this option for transparent user login to MS Domain.

4.4.1.6 On Demand User

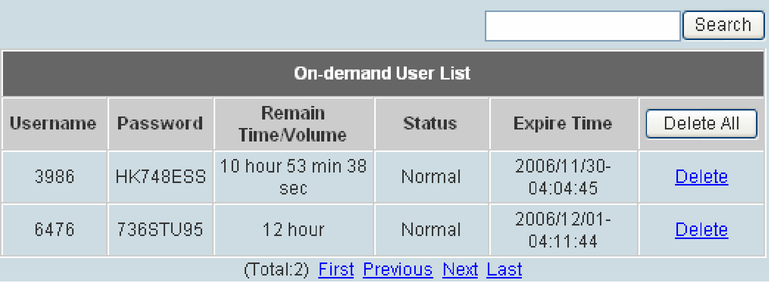
This is needed in a retail environment. When customers need to use wireless Internet in a store, they have to get a printed receipt with username and password from the store to log in the system for wireless access. Choose **"On Demand User"** in the **Server Name** field, the hyperlink beside the pull-down menu will become **"On-Demand User Server Configuration"**.



On-Demand User Server Configuration	
Server Status	Disable
Postfix	ondemand *(e.g. ondemand. Max: 40 char)
Receipt Header 1	Welcome! (e.g. Welcome!)
Receipt Header 2	Header2
Receipt Footer	Thank You! (e.g. Thank You!)
Monetary Unit	● None ○ £ GBP ○ € EUR ○ $ USD ○ (Input other desired monetary unit, e.g. AU)
Policy Name	Policy1
WLAN ESSID	default (e.g. default)
Wireless Key	
Remark	(for customer)
Billing Notice Interval	● 10mins ○ 15mins ○ 20mins
Users List Billing Configuration Create On-Demand User	
Apply Clear	

- **Server Status:** The status shows that the server is enabled or disabled.
- **Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0 ~ 9), alphabets (a ~ z or A ~ Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters. All other letters are not allowed.
- **Receipt Header 1/2:** There are two fields, **Receipt Header 1** and **Receipt Header 2**, for the receipt's header. Enter receipt header message or use the default.
- **Receipt Footer:** Enter receipt footer message here or use the default.
- **Monetary Unit:** Select the desired monetary unit for a region or input the needed monetary unit if not listed.
- **Policy Name:** Select a policy for the on-demand user.
- **WLAN ESSID:** Enter the ESSID of the AP.
- **Wireless Key:** Enter the Wireless key of the AP.
- **Remark:** Enter any additional information that will appear at the bottom of the receipt.
- **Billing Notice Interval:** While the on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval defined here.

A. **User List:** The page shows all valid on-demand accounts and their status. Click to enter the **On-demand User List** screen. In the **On-demand User List**, detailed information will be documented here. By default, the On-demand user database is empty.



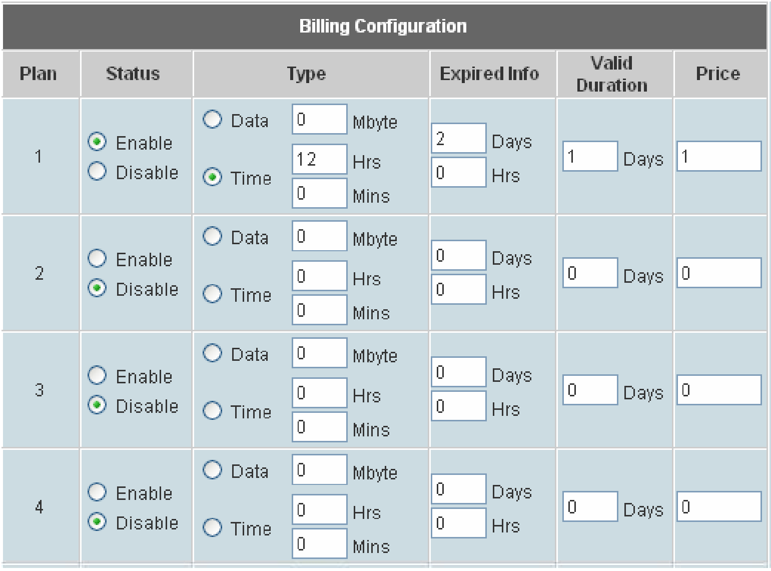
On-demand User List

Username	Password	Remain Time/Volume	Status	Expire Time	Delete All
3986	HK748ESS	10 hour 53 min 38 sec	Normal	2006/11/30-04:04:45	Delete
6476	736STU95	12 hour	Normal	2006/12/01-04:11:44	Delete

(Total:2) First Previous Next Last

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

B. **Billing Configuration:** This page allows administrators to change the billing configuration for on-demand accounts. Click this to enter the **Billing Configuration** screen. In the **Billing Configuration** screen, the Administrator may configure up to 10 billing plans.

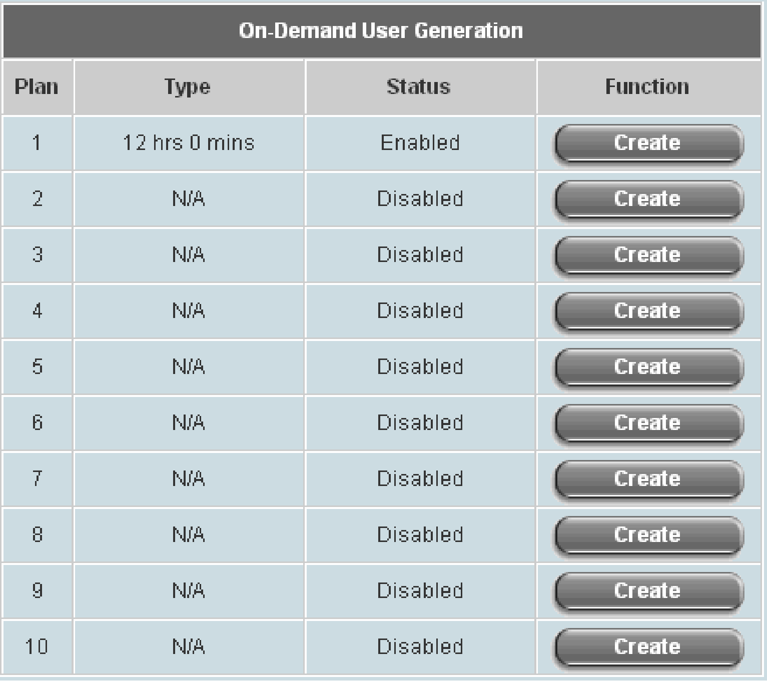


Billing Configuration

Plan	Status	Type	Expired Info	Valid Duration	Price
1	● Enable ○ Disable	○ Data 0 Mbyte ● Time 12 Hrs 0 Mins	2 Days 0 Hrs	1 Days	1
2	○ Enable ● Disable	○ Data 0 Mbyte ○ Time 0 Hrs 0 Mins	0 Days 0 Hrs	0 Days	0
3	○ Enable ● Disable	○ Data 0 Mbyte ○ Time 0 Hrs 0 Mins	0 Days 0 Hrs	0 Days	0
4	○ Enable ● Disable	○ Data 0 Mbyte ○ Time 0 Hrs 0 Mins	0 Days 0 Hrs	0 Days	0

- **Status:** Select to enable or disable this billing plan.
- **Type:** Set the billing plan by **"Data"** (the maximum volume allowed is 9,999,999 MByte) or **"Time"** (the maximum days allowed are 999 days).
- **Expired Info:** This is the time that the system will store this account information after the account generation, if the account is not activated during this time, the account will self-expire (the maximum time allowed is 999 days). **Valid Duration:** This is the time that the end-user can use the account after the account is activated. After this time, the account will self-expire (the maximum time allowed is 999 days) and end-user will be logged out from the system (the maximum time allowed is 999 days).
- **Price:** The price charged for this billing plan.

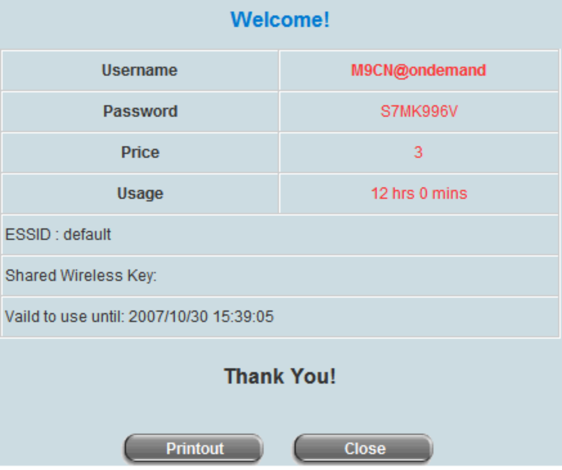
C. **Create On-Demand User:** This page allows administrators to create on-demand accounts. Click this to enter the **On-Demand User Generate** screen.



On-Demand User Generation

Plan	Type	Status	Function
1	12 hrs 0 mins	Enabled	Create
2	N/A	Disabled	Create
3	N/A	Disabled	Create
4	N/A	Disabled	Create
5	N/A	Disabled	Create
6	N/A	Disabled	Create
7	N/A	Disabled	Create
8	N/A	Disabled	Create
9	N/A	Disabled	Create
10	N/A	Disabled	Create

Pressing the ***Create*** button for the desired plan, an On-demand user will be created, then click ***Printout*** to print a receipt which will contain this on-demand user's information.



Welcome!

Username	M9CN@ondemand
Password	S7MK996V
Price	3
Usage	12 hrs 0 mins

ESSID : default

Shared Wireless Key:

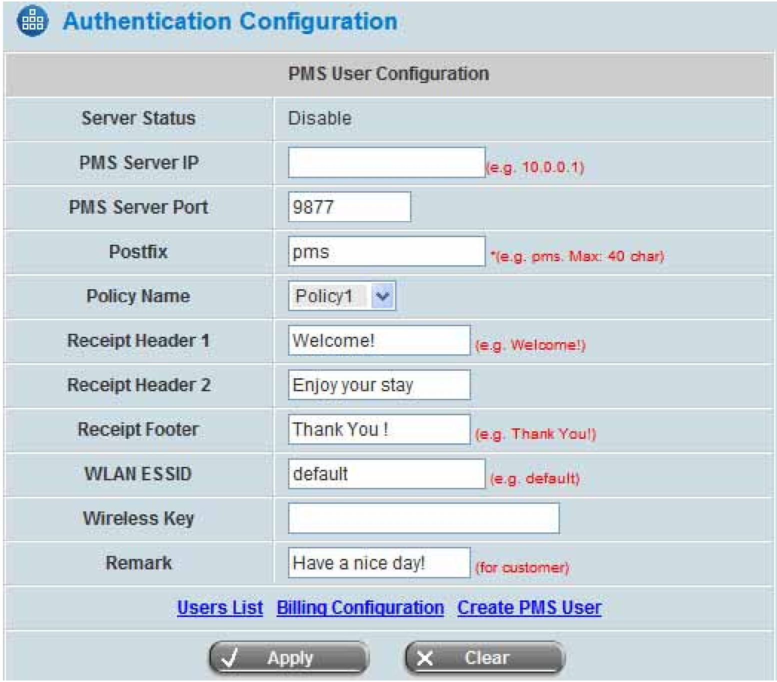
Vaild to use until: 2007/10/30 15:39:05

Thank You!

Notice: *Printout is related to a local printer connected or configured at the Administrator's computer.*

4.4.1.7 PMS User

The system integrates a hotel indoor billing system, PMS (Property Management System), developed by Micros Fidelio, and it usually used in a hotel environment. When the customers need to use wireless Internet in the hotel, they have to get a printed receipt with username and password form the hotel to log in the system for wireless access. Choose **"PMS User"** in the **Server Name** field, the hyperlink beside the pull-down menu will become **"PMS User Configuration"**.

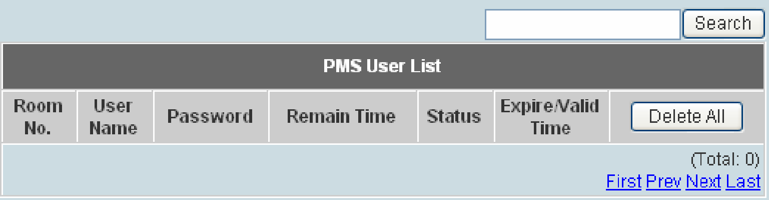


Authentication Configuration

PMS User Configuration	
Server Status	Disable
PMS Server IP	(e.g. 10.0.0.1)
PMS Server Port	9877
Postfix	pms *(e.g. pms. Max: 40 char)
Policy Name	Policy1
Receipt Header 1	Welcome! (e.g. Welcome!)
Receipt Header 2	Enjoy your stay
Receipt Footer	Thank You ! (e.g. Thank You!)
WLAN ESSID	default (e.g. default)
Wireless Key	
Remark	Have a nice day! (for customer)

- **Server Status:** The status shows that the server is enabled or disabled.
- **PMS Server IP:** Enter the IP address of the PMS server.
- **PMS Server Port:** Enter the Port of the PMS server.
- **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 (.) with a maximum of 40 characters. All other letters are not allowed.
- **Policy Name:** There are five policies to select from.
- **Receipt Header 1/2:** There are two fields, **Receipt Header 1** and **Receipt Header 2**, for the receipt's header. Enter receipt header message or use the default.
- **Receipt Footer:** Enter receipt footer message here or use the default.
- **WLAN ESSID:** Enter the ESSID of the AP.
- **Wireless Key:** Enter the Wireless key of the AP.
- **Remark:** Enter any additional information that will appear at the bottom of the receipt.

A. **Users List:** This page shows all valid PMS accounts and their status. Click to enter the **PMS User List** screen. In the **PMS User List**, detailed information will be documented here. By default, the PMS user database is empty.



Room No.	User Name	Password	Remain Time	Status	Expire/Valid Time	Delete All

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.

Room No.: The room number of the PMS user.

Username: The login name of the PMS user.

Password: The login password of the PMS user.

Remain Time: The total time/Volume that the user can use currently.

Status: The status of the account.

- **Normal** indicates that the account is not in-use and not overdue.
- **Online** indicates that the account is in-use and not overdue.
- **Expire** indicates that the account is overdue and cannot be used.

Expire/Valid Time:

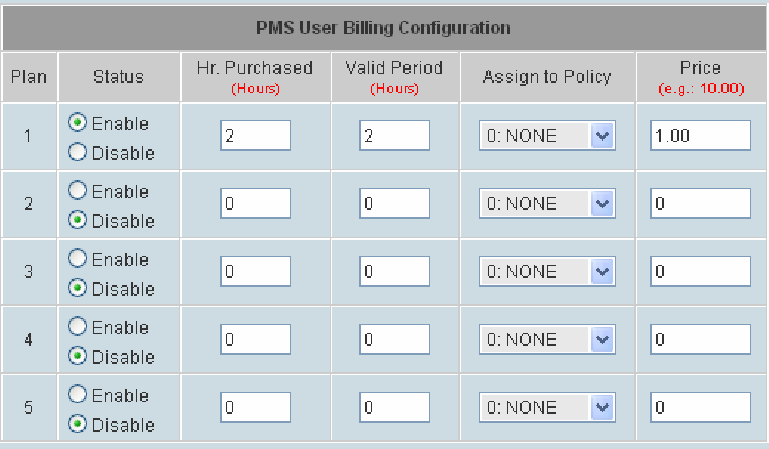
- The ***Valid Time*** indicates the duration of time that the end-user can use the account after the activation of the account. After the time, the account will self-expire (the maximum time allowed is 999 days).
- **Expire Time:** This is the time that system will store this account information after the account generation, if the account is not activated during this time, the account will self-expire (the maximum time allowed is 999 days).

Delete All: This will delete all the users at once.

Delete: This will delete the users individually.

Redeem: This is used to increase the remaining time of the account. When the remaining time or data quota is insufficient, the user has to pay for adding credit at the counter and the user will get a new username and password.

B. **Billing Configuration:** This page allows administrators to change the billing configuration for PMS accounts. Click this to enter the **Billing Configuration** screen. In the **Billing Configuration** screen, Administrator may configured up to 5 billing plans.



PMS User Billing Configuration

Plan	Status	Hr. Purchased (Hours)	Valid Period (Hours)	Assign to Policy	Price (e.g.: 10.00)
1	● Enable ○ Disable	2	2	0: NONE	1.00
2	○ Enable ● Disable	0	0	0: NONE	0
3	○ Enable ● Disable	0	0	0: NONE	0
4	○ Enable ● Disable	0	0	0: NONE	0
5	○ Enable ● Disable	0	0	0: NONE	0

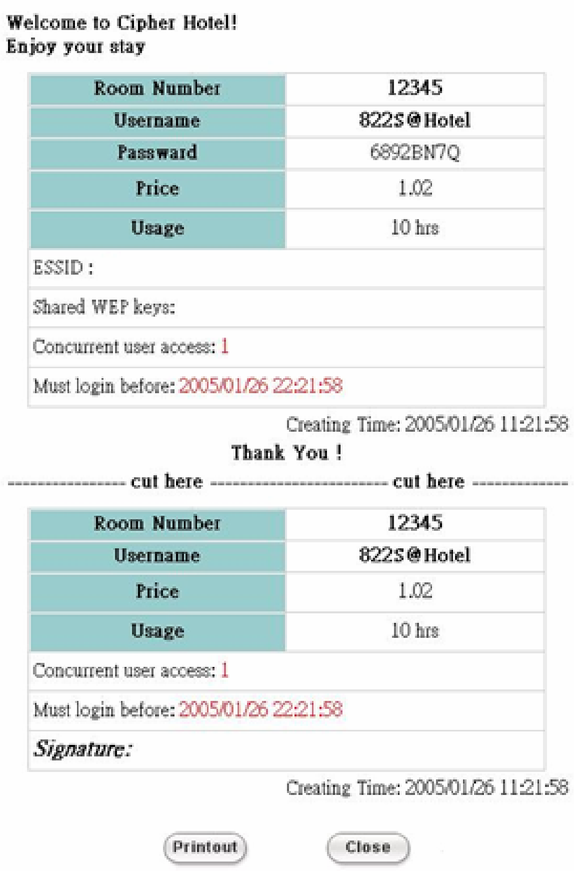
Status: Select to enable or disable this billing plan.

Hr. Purchased: This is the duration of time that the user can use the account after the activation of the account. After this duration, the account will self-expires. 1-999 hours can be entered.

Valid Period: This is the duration of time that the user needs to activate the account after the generation of the account. If the account is not activated during this duration, the account will self-expires. 1-999 hours can be entered.

Assign to Policy: Assign a policy for this billing plan.

Price: The price charged for this billing plan.



Welcome to Cipher Hotel!
Enjoy your stay

Room Number	12345
Username	822s@Hotel
Passward	6892BN7Q
Price	1.02
Usage	10 hrs

ESSID :

Shared WEP keys:

Concurrent user access: 1

Must login before: 2005/01/26 22:21:58

Creating Time: 2005/01/26 11:21:58

Thank You !

---------------- cut here ------------------------ cut here -------------

Room Number	12345
Username	822s@Hotel
Price	1.02
Usage	10 hrs

Concurrent user access: 1

Must login before: 2005/01/26 22:21:58

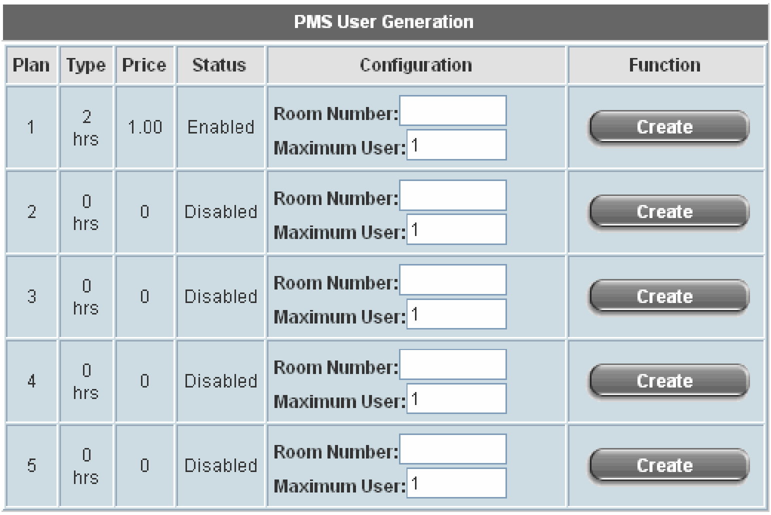
Signature:

Creating Time: 2005/01/26 11:21:58

*Note: There is an **Auto Expired** built-in mechanism that helps monitor accounts that are created but never logged-in. If this account exists, it will automatically expire, and become invalid after a period of time.*

The auto expired time = the exact created time of the account + Valid Period.

C. **Created PMS User:** This page allows administrators to create PMS accounts. Click this to enter the **PMS User Generate** screen. There are 5000 PMS user accounts available.



PMS User Generation

Plan	Type	Price	Status	Configuration	Function
1	2 hrs	1.00	Enabled	Room Number: Maximum User: 1	Create
2	0 hrs	0	Disabled	Room Number: Maximum User: 1	Create
3	0 hrs	0	Disabled	Room Number: Maximum User: 1	Create
4	0 hrs	0	Disabled	Room Number: Maximum User: 1	Create
5	0 hrs	0	Disabled	Room Number: Maximum User: 1	Create

By default, the PMS user database is empty. After entering the ***"Room Number"*** and ***"Maximum User"***, select the desired plan and press the ***Create*** button. A PMS user will be created. Click ***Printout*** to print a receipt which will contain this PMS user's information.

- ***Maximum User:*** The maximum number of accounts in one room.

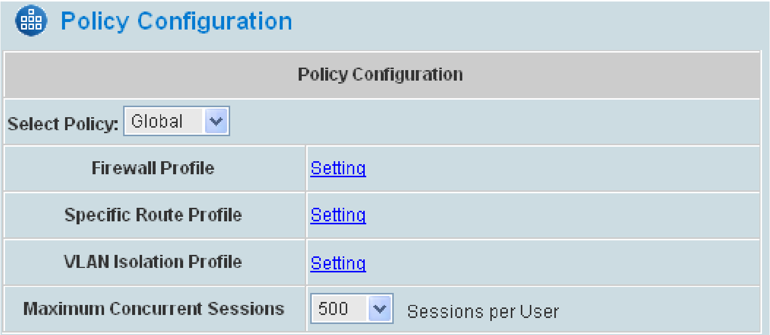
Notice: *Printout is related to a local printer or configured at the computer of the hotel counter.*

4.4.2 Policy Configuration

System supports up to **10 individual policies**, each of which consists of access control profiles that can be applied to a certain group of users. In the DSA-6100 system architecture, a group of users are associated with an authentication method which is defined by Authentication Server configuration. On the other hand, the **Global policy** also consists of access control profiles and can be globally applied to all users.

I. Global Policy:

Global Policy is the system's universal policy including Firewall, Specific Route and VLAN Isolation Profiles constrained all network users unless the network user is already regulated and followed the control rules of the other policies. The Global Policy applies to all users. Once a policy is configured, you may assign the policy to any authentication server. Two authentication servers may share the same policy.

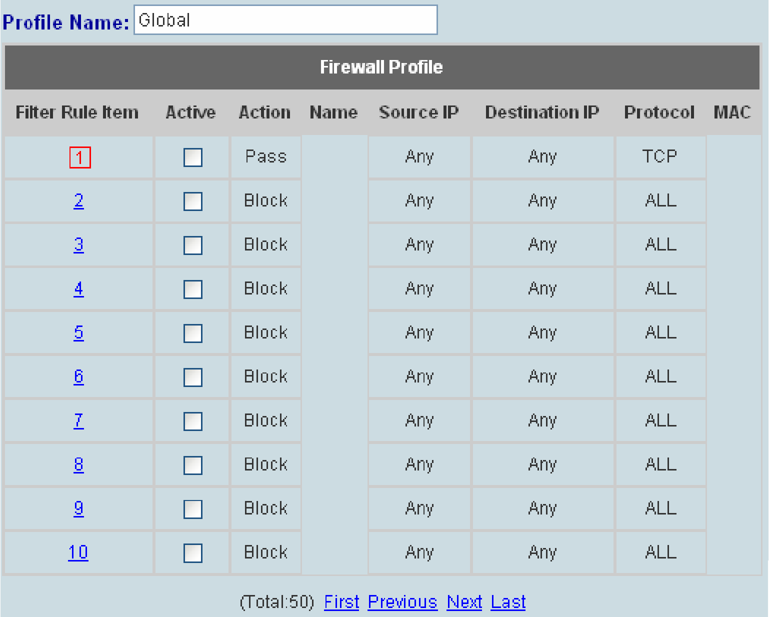


Policy Configuration

Policy Configuration	
Select Policy: Global	
Firewall Profile	Setting
Specific Route Profile	Setting
VLAN Isolation Profile	Setting
Maximum Concurrent Sessions	500 Sessions per User

- **Select Policy:** Select Global for setting up Global policy configuration.
- **Firewall Profile:** Global firewall rules can be defined and applied to all users.
- **Specific Route Profile:** Static routing rules can be specified to route IP traffic from the system to the destination in a controlled fashion.
- **VLAN Isolation Profile:** Default isolation rule can be selected to pass or to block all traffic between VLAN and LAN interfaces. In addition, exception rules can be set up to accompanied with the Default rule.
- **Maximum Concurrent Sessions:** The maximum number of concurrent sessions which is allowed to be established by each user.

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



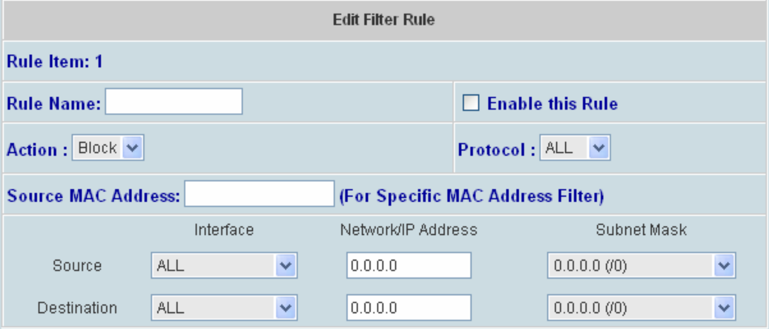
Profile Name: Global

Firewall Profile

Filter Rule Item	Active	Action	Name	Source IP	Destination IP	Protocol	MAC
1	□	Pass		Any	Any	TCP	
2	□	Block		Any	Any	ALL	
3	□	Block		Any	Any	ALL	
4	□	Block		Any	Any	ALL	
5	□	Block		Any	Any	ALL	
6	□	Block		Any	Any	ALL	
7	□	Block		Any	Any	ALL	
8	□	Block		Any	Any	ALL	
9	□	Block		Any	Any	ALL	
10	□	Block		Any	Any	ALL	

(Total:50) First Previous Next Last

Selecting the Filter Rule Item 1:



Edit Filter Rule

Rule Item: 1

Rule Name: □ **Enable this Rule**

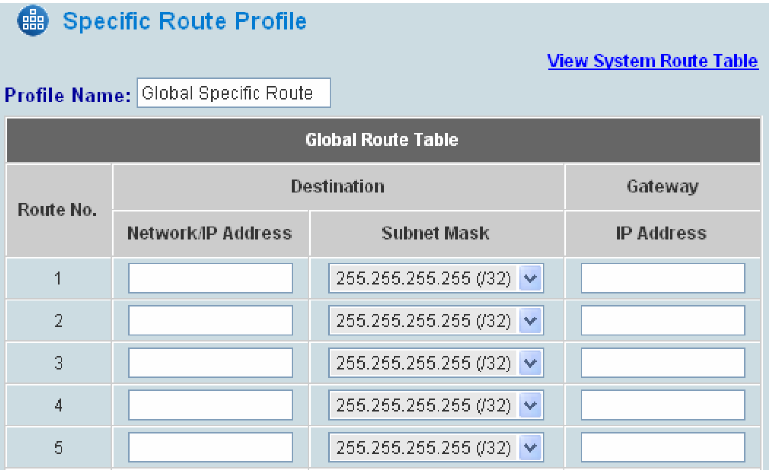
Action : Block **Protocol :** ALL

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

	Interface	Network/IP Address	Subnet Mask
Source	ALL	0.0.0.0	0.0.0.0 (/0)
Destination	ALL	0.0.0.0	0.0.0.0 (/0)

- **Rule Item:** This is the rule selected.
- **Rule Name:** The rule name can be changed here.
- **Enable this Rule:** After checking this function, the rule will be enabled.
- **Action:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.
- **Protocol:** There are three protocols to select, **TCP**, **UDP** and **ICMP**, or choose **ALL** to use all three protocols.
- **Source MAC Address:** The MAC address of the source IP address. This is for specific MAC address filter.
- **Source/Destination Interface:** There are four interfaces to choose, **WAN1**, **WAN2**, **LAN1** and **LAN2**.
- **Source/Destination IP:** Enter the source and destination IP addresses.
- **Source/Destination Subnet Mask:** Enter the source and destination subnet masks.

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



Specific Route Profile

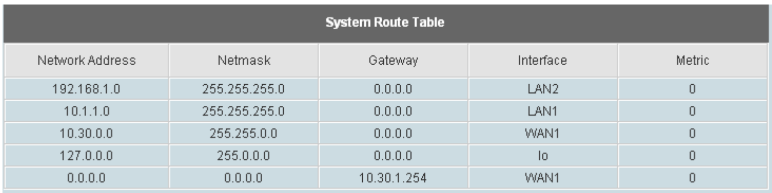
View System Route Table

Profile Name: Global Specific Route

Global Route Table			
Route No.	Destination		Gateway
	Network/IP Address	Subnet Mask	IP Address
1		255.255.255.255 (/32)	
2		255.255.255.255 (/32)	
3		255.255.255.255 (/32)	
4		255.255.255.255 (/32)	
5		255.255.255.255 (/32)	

- **Profile Name:** The profile name can be changed here.
- **Network/IP Address (Destination):** The destination network address or IP address of the destination host. Please note that, if applicable, the system will calculate and display the appropriate value of address based on the combination of Network/IP Address and Subnet Mask that are just entered and applied.
- **Subnet Mask:** The Subnet Mask of the destination network or just 255.255.255.255(/32) if the destination is a single host.
- **IP Address (Destination):** The destination IP address of the host or the network.

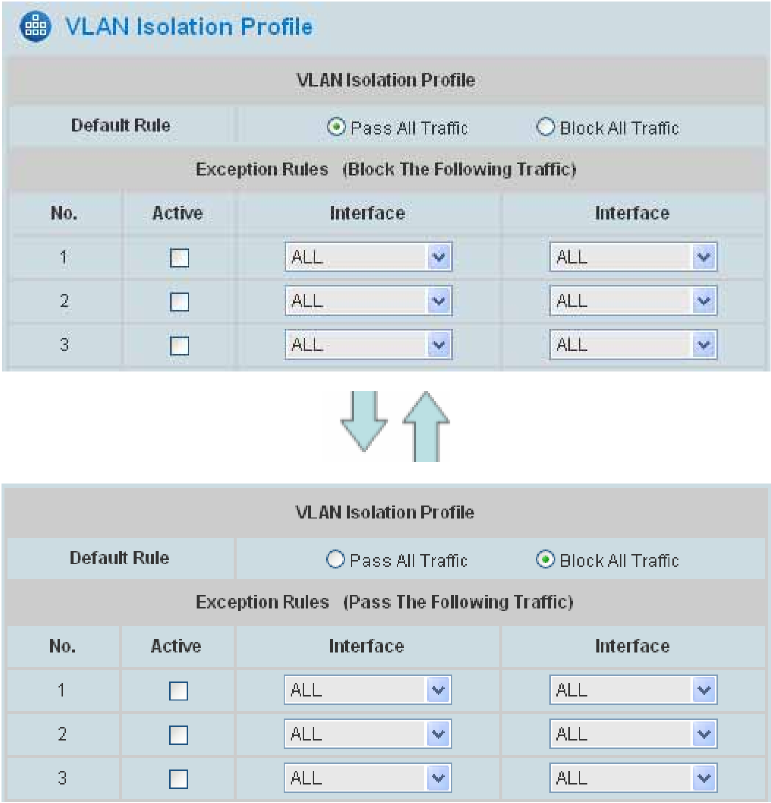
- **View System Route Table:** Click the hyperlink ***View System Route Table*** to see the routing information for the entire system.



System Route Table				
Network Address	Netmask	Gateway	Interface	Metric
192.168.1.0	255.255.255.0	0.0.0.0	LAN2	0
10.1.1.0	255.255.255.0	0.0.0.0	LAN1	0
10.30.0.0	255.255.0.0	0.0.0.0	WAN1	0
127.0.0.0	255.0.0.0	0.0.0.0	lo	0
0.0.0.0	0.0.0.0	10.30.1.254	WAN1	0

- **VLAN Isolation Profile:** Click the hyperlink of ***Setting*** for **VLAN Isolation Profile**, the VLAN Isolation Profile list will appear. The isolation rules apply to all users including authenticated users, non-authenticated users, privileged users, VPN users, users on a non-authenticated port, DMZ clients, and virtual servers. While the system is not set in Bridge mode, the isolation rules will be displayed in two tiers, a default rule accompanied by some exceptional rules.

Note: For more information, please refer to ***Appendix E. VLAN Isolation.***



VLAN Isolation Profile

VLAN Isolation Profile			
Default Rule		● Pass All Traffic	○ Block All Traffic
Exception Rules (Block The Following Traffic)			
No.	Active	Interface	Interface
1	□	ALL	ALL
2	□	ALL	ALL
3	□	ALL	ALL

VLAN Isolation Profile			
Default Rule		○ Pass All Traffic	● Block All Traffic
Exception Rules (Pass The Following Traffic)			
No.	Active	Interface	Interface
1	□	ALL	ALL
2	□	ALL	ALL
3	□	ALL	ALL

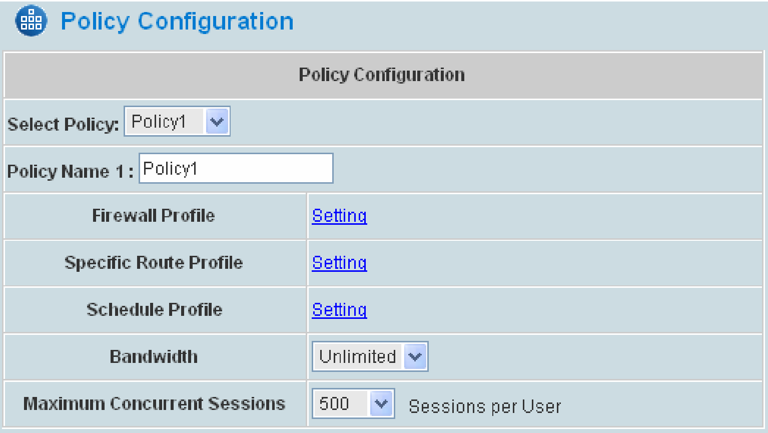
- **Default Rule:** It is to specify the default action that the system should perform for the traffic between all VLAN interfaces as well as the LAN interfaces.
  - **Pass All Traffic:** When selected, the system allows all traffic to travel between all VLAN interfaces as well as the LAN interfaces.
  - **Block All Traffic:** When selected, the system does not allow any traffic to travel between all VLAN interfaces as well as the LAN interfaces.
- **Exception Rule:** The default action for the traffic between all interfaces could be either **Pass All** or **Block All**. If traffic between any particular interfaces has to be blocked or passed, administrators will need to create the custom, exceptional rules to block or to pass the traffic that are traveling between the selected interfaces.
  - **Active:** Select the check box to activate the exception rule.
  - **Interface:** Use the drop-down list to select the interfaces where the traffic will be blocked or passed, according to the Default Rule.

- **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.

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

II. Policy 1~Policy 10:

10 individual policies, each policy consists of three different network related access profiles and bandwidth controls.

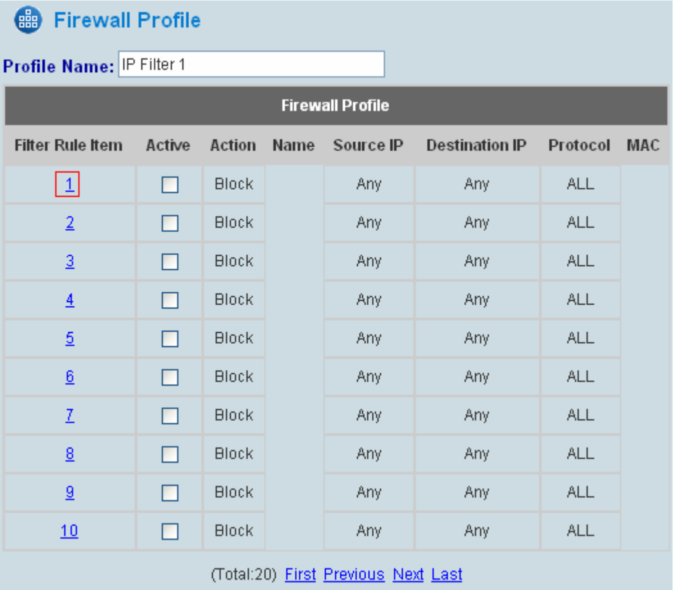


Policy Configuration

Policy Configuration	
Select Policy: Policy1	
Policy Name 1 : Policy1	
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
Bandwidth	Unlimited
Maximum Concurrent Sessions	500 Sessions per User

- ➢ **Select Policy:** Select Policy1~10 for setting up policy configuration.
- ➢ **Firewall Profile:** Policy firewall rules can be defined.
- ➢ **Specific Route Profile:** Define up to 10 static routes.
- ➢ **Schedule Profile:** Define allowed access hours.
- ➢ **Bandwidth:** Define maximum bandwidth allowed.
- ➢ **Maximum Concurrent Sessions:** The maximum number of concurrent sessions which is allowed to be established by each user.

- ▪ **Select Policy / Policy Name:** Select a desired policy and rename it in the Policy Name field if desired. Select ***Policy1~Policy10*** for setting up 10 policies configuration.
- ▪ **Firewall Profile:** Click the hyperlink of ***Setting*** for **Firewall Profile**, the Firewall Profiles list will appear. Click the numbers of Filter Rule Item to edit individual rules and click Apply to save the settings. The rule status will show on the list. Check “Active” to enable that rule.



Firewall Profile

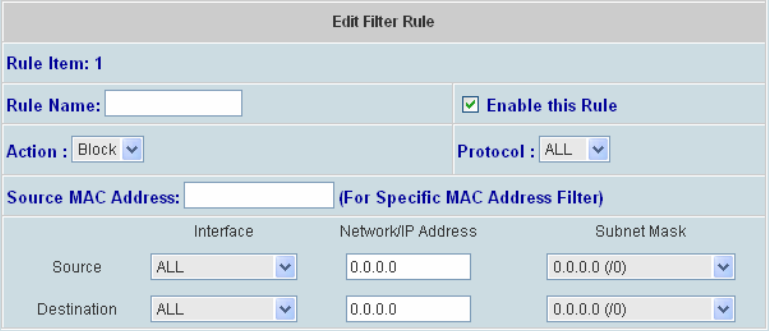
Profile Name: IP Filter 1

Firewall Profile

Filter Rule Item	Active	Action	Name	Source IP	Destination IP	Protocol	MAC
1	□	Block		Any	Any	ALL	
2	□	Block		Any	Any	ALL	
3	□	Block		Any	Any	ALL	
4	□	Block		Any	Any	ALL	
5	□	Block		Any	Any	ALL	
6	□	Block		Any	Any	ALL	
7	□	Block		Any	Any	ALL	
8	□	Block		Any	Any	ALL	
9	□	Block		Any	Any	ALL	
10	□	Block		Any	Any	ALL	

(Total:20) First Previous Next Last

Selecting the Filter Rule Item 1:



Edit Filter Rule

Rule Item: 1

Rule Name: 　　☑ Enable this Rule

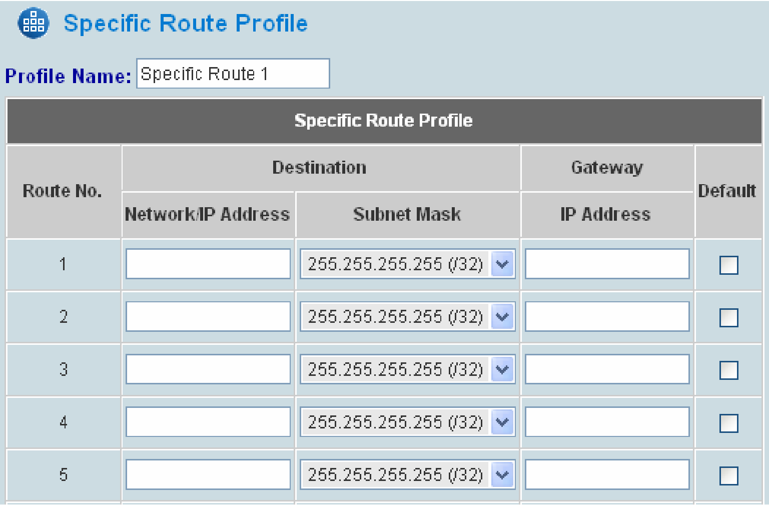
Action : Block 　　Protocol : ALL

Source MAC Address: 　　(For Specific MAC Address Filter)

	Interface	Network/IP Address	Subnet Mask
Source	ALL	0.0.0.0	0.0.0.0 (/0)
Destination	ALL	0.0.0.0	0.0.0.0 (/0)

- ➢ **Rule Item:** This is the rule selected.
- ➢ **Rule Name:** The rule name can be changed here.
- ➢ **Enable this Rule:** After checking this function, the rule will be enabled.
- ➢ **Action:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.
- ➢ **Protocol:** There are three protocols to select, **TCP**, **UDP** and **ICMP**, or choose **ALL** to use all three protocols.
- ➢ **Source MAC Address:** The MAC address of the source IP address. This is for specific MAC address filter.
- ➢ **Source/Destination Interface:** There are five interfaces to choose, **ALL**, **WAN1**, **WAN2**, **LAN1** and **LAN2**.
- ➢ **Source/Destination IP:** Enter the source and destination IP addresses. Domain Host filtering is supported but Domain name filtering is not.
- ➢ **Source/Destination Subnet Mask:** Enter the source and destination subnet masks which

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



Specific Route Profile

Profile Name: Specific Route 1

Specific Route Profile

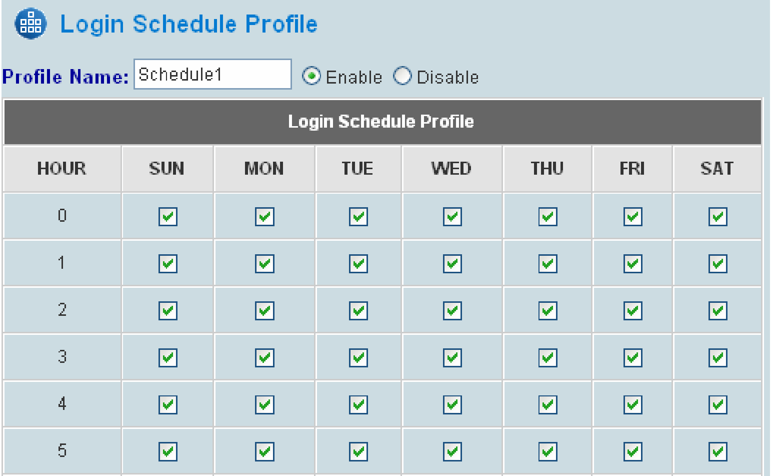
Route No.	Destination		Gateway	Default
	Network/IP Address	Subnet Mask	IP Address	
1		255.255.255.255 (/32)		□
2		255.255.255.255 (/32)		□
3		255.255.255.255 (/32)		□
4		255.255.255.255 (/32)		□
5		255.255.255.255 (/32)		□

- ➢ **Profile Name:** The profile name can be changed here.
- ➢ **Network/IP Address (Destination):** The destination network address or IP address of the destination host. Please note that, if applicable, the system will calculate and display the

appropriate value of address based on the combination of Network/IP Address and Subnet Mask that are just entered and applied.

- **Subnet Mask:** The Subnet Mask of the destination network or just 255.255.255.255(/32) if the destination is a single host.
- **IP Address (Gateway):** The IP address of the next router to the destination.
- **Default:** Select the check box to activate the routing rule as the default route.

- **Schedule Profile:** Click the hyperlink of ***Setting*** for **Schedule Profile** to enter the Schedule Profile list. Select "Enable" to show the list. This function is used to restrict the time the users can log in. Please enable/disable the desired time slot and click Apply to save the settings (on the screen below is shown only for 0 to 10, but the system can be configured based on 24 hours). These settings will become effective immediately after clicking the Apply button.



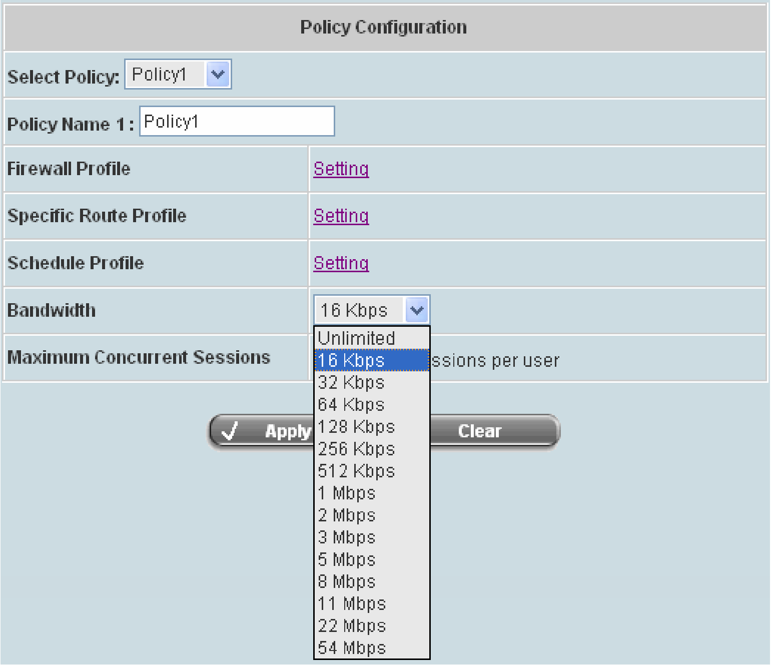
Login Schedule Profile

Profile Name: Schedule1 ● Enable ○ Disable

Login Schedule Profile

HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
0	☑	☑	☑	☑	☑	☑	☑
1	☑	☑	☑	☑	☑	☑	☑
2	☑	☑	☑	☑	☑	☑	☑
3	☑	☑	☑	☑	☑	☑	☑
4	☑	☑	☑	☑	☑	☑	☑
5	☑	☑	☑	☑	☑	☑	☑

- **Bandwidth:** Use the drop-down list to select the maximum bandwidth for the users who are assigned to this policy.

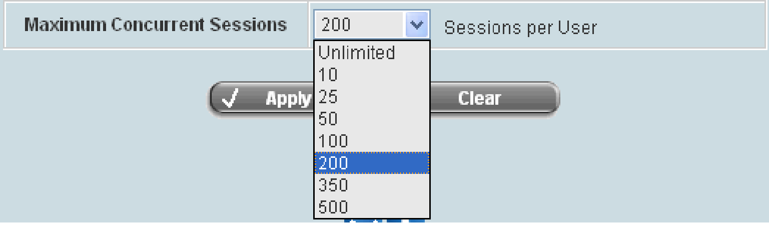


Policy Configuration

Select Policy:	Policy1
Policy Name 1 :	Policy1
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
Bandwidth	16 Kbps
Maximum Concurrent Sessions	ssions per user

- **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.

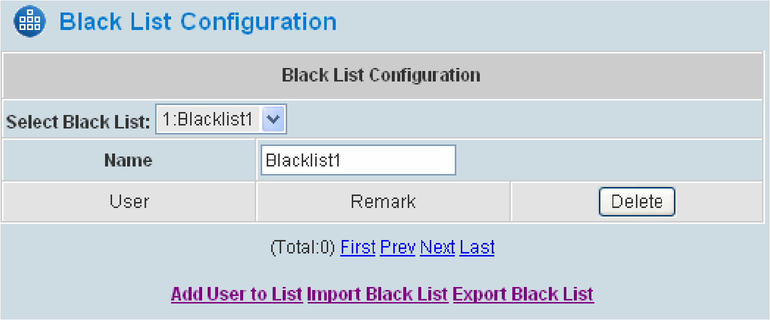
Note: For more information, please refer to ***Appendix F. Session Limit and Session Log***.



Maximum Concurrent Sessions 200 Sessions per User

4.4.3 Black List Configuration

These user accounts in the black list cannot access network even with correct user name and password. The administrator can add, delete, or edit the black list for user access control. There are 5 sets of black lists provided by the system. Each black list can include up to 40 users. 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 the black list can be applied to this specific authentication option.



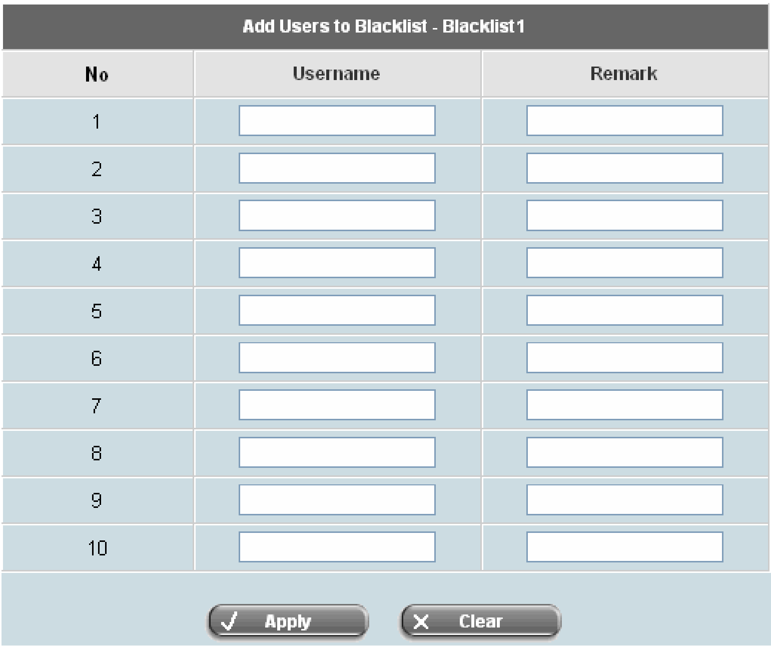
Black List Configuration

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

(Total:0) First Prev Next Last

Add User to List Import Black List Export Black List

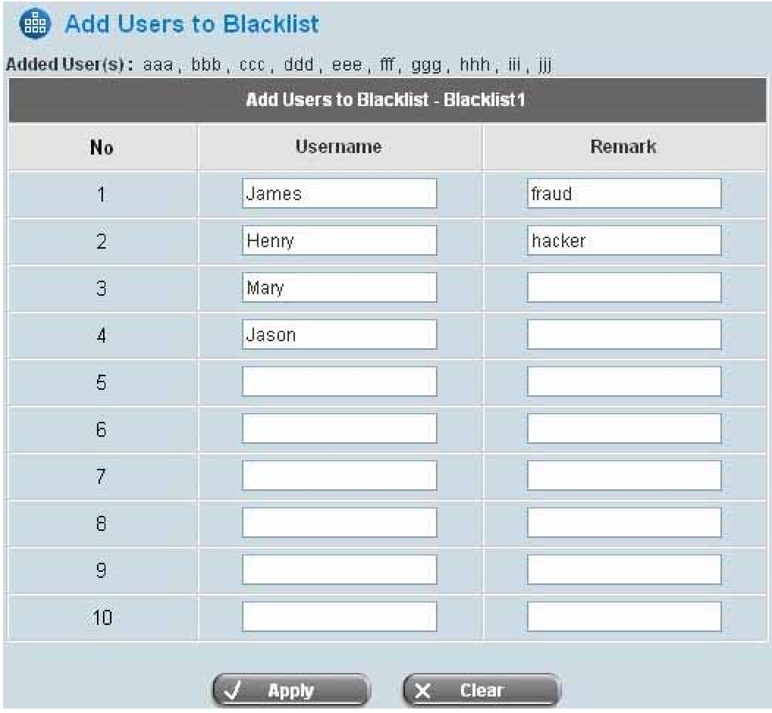
- **Select Black List:** There are 5 lists supported by DSA-6100 for selections.
- **Name:** Set the name of the black list and it will show in the pull-down menu above.
- **Add User to List:** After clicking this, the **Add Users to Blacklist** page will appear for adding users to the selected black list.



Add Users to Blacklist - Blacklist1

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

After entering the usernames in the **"Username"** blanks and the related information in the **"Remark"** blank (not required).



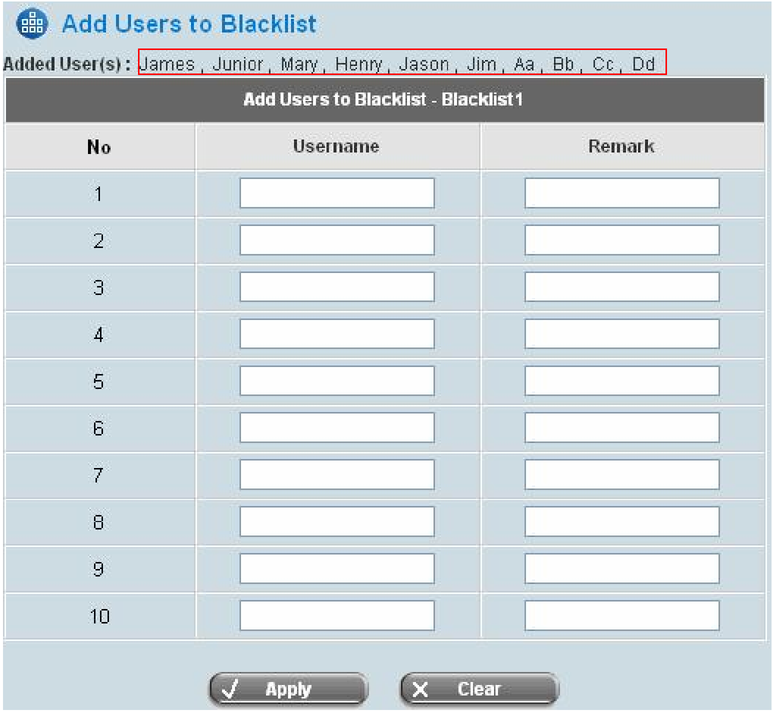
Add Users to Blacklist

Added User(s) : aaa , bbb , ccc , ddd , eee , fff , ggg , hhh , iii , jjj

Add Users to Blacklist - Blacklist1

No	Username	Remark
1	James	fraud
2	Henry	hacker
3	Mary	
4	Jason	
5		
6		
7		
8		
9		
10		

Click ***Apply*** to add the users.



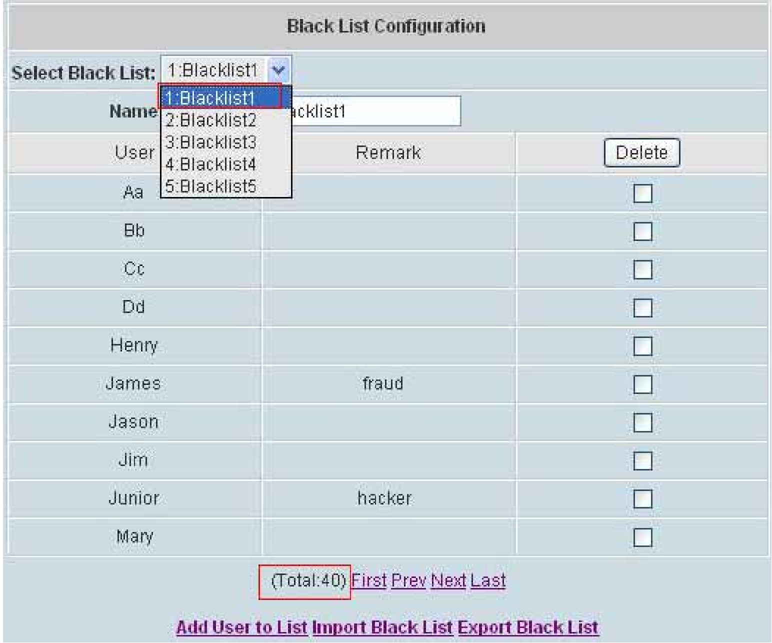
Add Users to Blacklist

Added User(s) : James , Junior , Mary , Henry , Jason , Jim , Aa , Bb , Cc , Dd

Add Users to Blacklist - Blacklist1

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

Check **Black List Configuration** screen; the added black list usernames will be shown on the list.



Black List Configuration

Select Black List: 1:Blacklist1

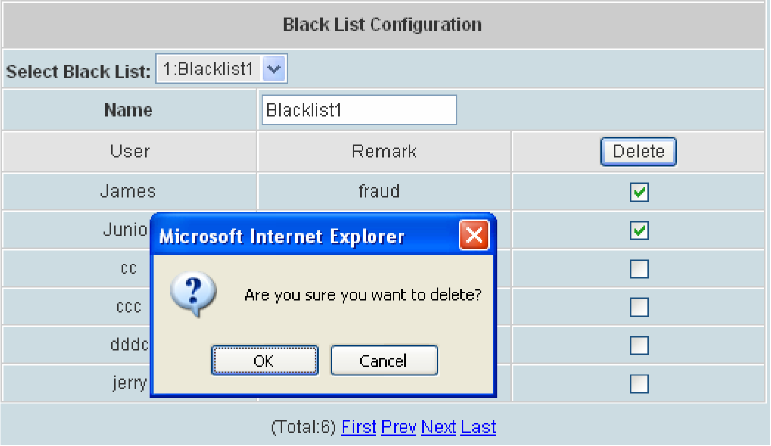
Name: acklist1

User	Remark	Delete
Aa		□
Bb		□
Cc		□
Dd		□
Henry		□
James	fraud	□
Jason		□
Jim		□
Junior	hacker	□
Mary		□

(Total:40) First Prev Next Last

Add User to List Import Black List Export Black List

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.



Black List Configuration

Select Black List: 1:Blacklist1

Name: Blacklist1

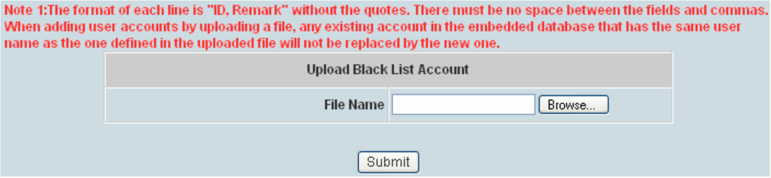
User	Remark	Delete
James	fraud	☑
Junio		☑
cc		□
ccc		□
dddd		□
jerry		□

Microsoft Internet Explorer

Are you sure you want to delete?

(Total:6) First Prev Next Last

- **Import Black List:** Click this to enter the **Upload Black List Account – (Blacklist1)** interface. Click the ***Browse*** button to select the text file for the user account upload to the black list. Then click ***Submit*** to complete the upload process.

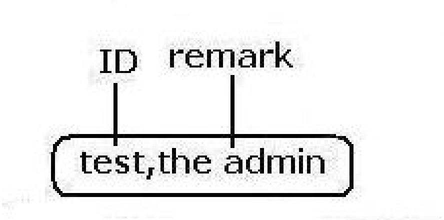


Note 1:The format of each line is "ID, Remark" without the quotes. There must be no space between the fields and commas. When adding user accounts by uploading a file, any existing account in the embedded database that has the same user name as the one defined in the uploaded file will not be replaced by the new one.

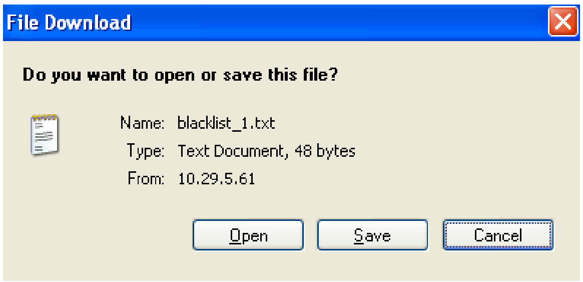
Upload Black List Account

File Name

The uploading file should be a text file and the format of each line should be ***"ID, Remark"*** without the quotes. There must be no spaces between the fields and commas. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by new ones.



- **Export Black List:** Click ***Export List*** to create a .txt file and then save it on disk.



File Download

Do you want to open or save this file?

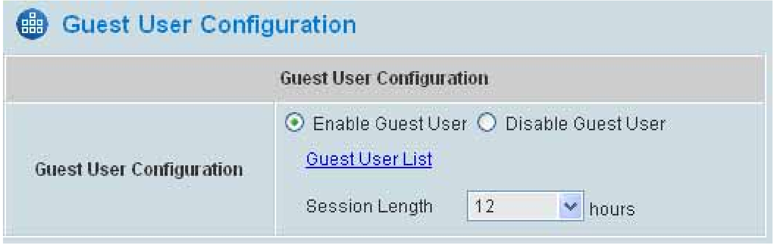
Name: blacklist_1.txt

Type: Text Document, 48 bytes

From: 10.29.5.61

4.4.4 Guest User Configuration

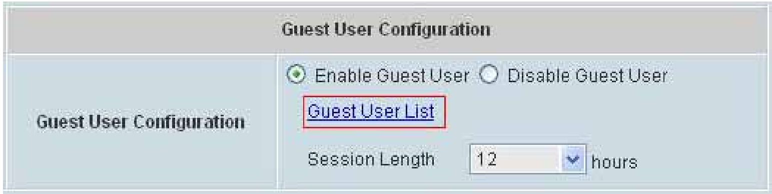
System provides 10 guest accounts with customized session length. This function can permit guests to log into the system. Select **“Enable Guest User”** and click ***Apply*** to save the settings.



Guest User Configuration

Guest User Configuration	
Guest User Configuration	● Enable Guest User ○ Disable Guest User Guest User List Session Length 12 hours

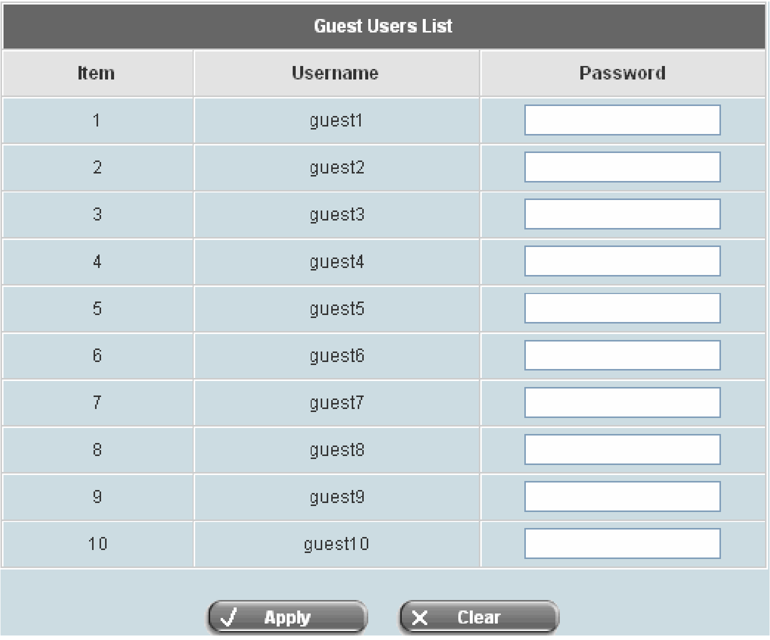
Guest User List: The DSA-6100 offers ten guest users for log in. To activate a guest user, just enter the password in the corresponding **“Password”** text field for that guest account. Guest accounts with blank password will not be activated.



Guest User Configuration	
Guest User Configuration	● Enable Guest User ○ Disable Guest User Guest User List Session Length 12 hours

Session Length: This restricts the connection time of the guest users. The default session length is 6 hours and the available session time ranges from 1 to 12 hours or unlimited

Click on “**Guest User List**” and add the password for the Guest accounts:

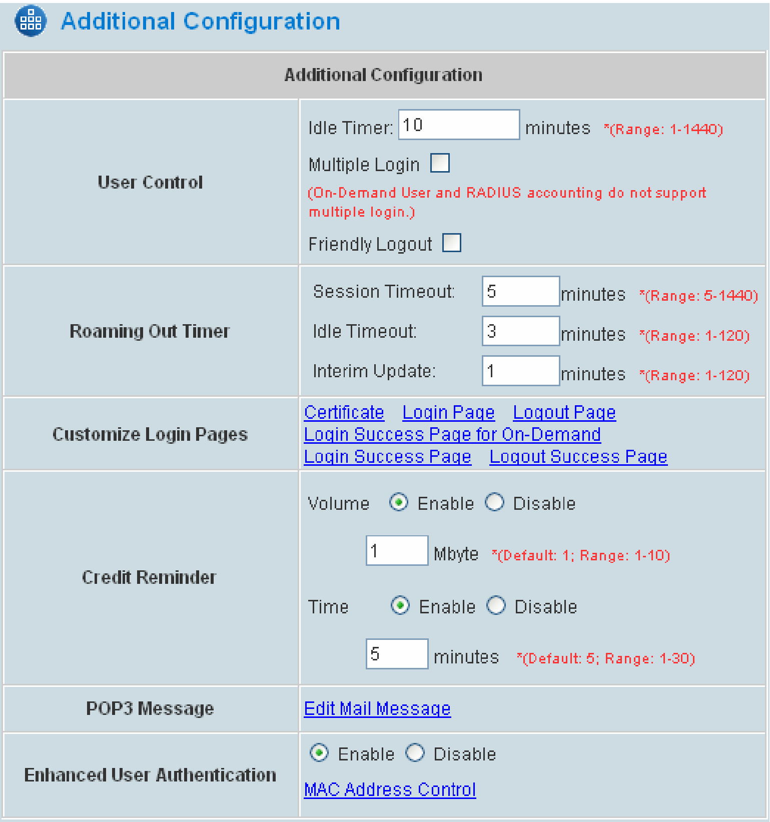


Guest Users List

Item	Username	Password
1	guest1	
2	guest2	
3	guest3	
4	guest4	
5	guest5	
6	guest6	
7	guest7	
8	guest8	
9	guest9	
10	guest10	

4.4.5 Additional Configuration

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



Additional Configuration

Additional Configuration	
User Control	Idle Timer: 10 minutes *(Range: 1-1440) Multiple Login □ (On-Demand User and RADIUS accounting do not support multiple login.) Friendly Logout □
Roaming Out Timer	Session Timeout: 5 minutes *(Range: 5-1440) Idle Timeout: 3 minutes *(Range: 1-120) Interim Update: 1 minutes *(Range: 1-120)
Customize Login Pages	Certificate Login Page Logout Page Login Success Page for On-Demand Login Success Page Logout Success Page
Credit Reminder	Volume ● Enable ○ Disable 1 Mbyte *(Default: 1; Range: 1-10) Time ● Enable ○ Disable 5 minutes *(Default: 5; Range: 1-30)
POP3 Message	Edit Mail Message
Enhanced User Authentication	● Enable ○ Disable MAC Address Control

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

Idle Timer: If a user has been idled with no network activities, the system will automatically log out the user. The logout timer can be set in the range of 1~1440 minutes, and the default logout time is 10 minutes.

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

Friendly Logout: When a user logs into the network with wireless connection, a small window will appear to show the user's information and there is a logout button for the logout. If enabled. When the users try to close the small window, there will be a new popup window to confirm the logout in case the users click the logout button by accident.

B. **Roaming Out Timer:** This function refers to RADIUS Roaming Out, which includes the following:

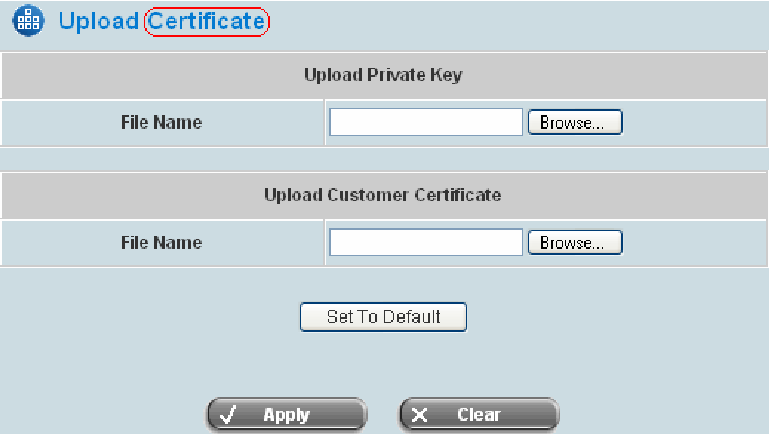
Session Timeout: The time that the user can access the network while roaming. When the time is up, the user will be kicked out automatically.

Idle Timeout: If a user has been idled with no network activities, the system will automatically log out the user.

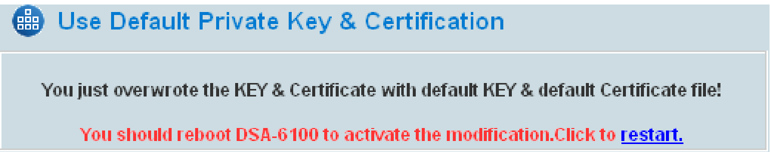
Interim Update: The system will update the users' current status and usage according to this periodically.

C. **Customize Login Pages:** The system allows the great customization on end-user interface. Administrators may upload device certificate, customized login, and logout webpage.

1). **Certificate:** The administrator can upload new private key and customer certification, external certificate issued by public or private authority. Click the first ***Browse*** button to select the Private Key. Click the second ***Browse*** button to select the file for the certificate upload. Next, click ***Apply*** to complete the upload process.



Click ***Set To Default*** and then click ***restart*** to use the default certificate and key.

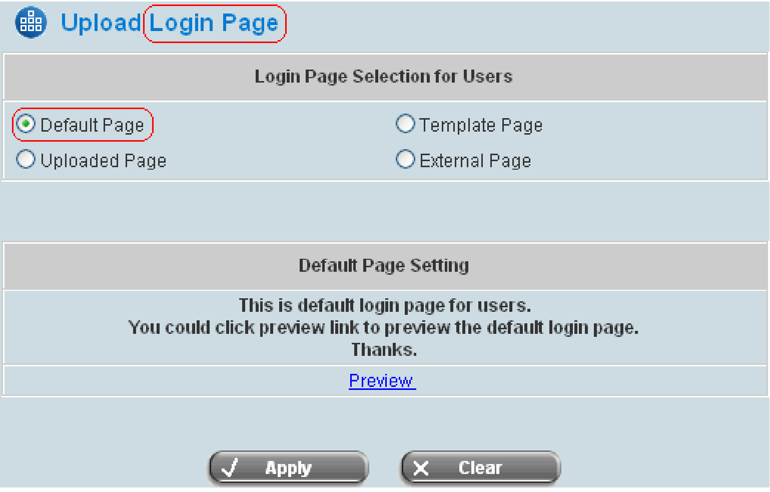


You just overwrote the KEY & Certificate with default KEY & default Certificate file!

You should reboot DSA-6100 to activate the modification.Click to restart.

2). **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.

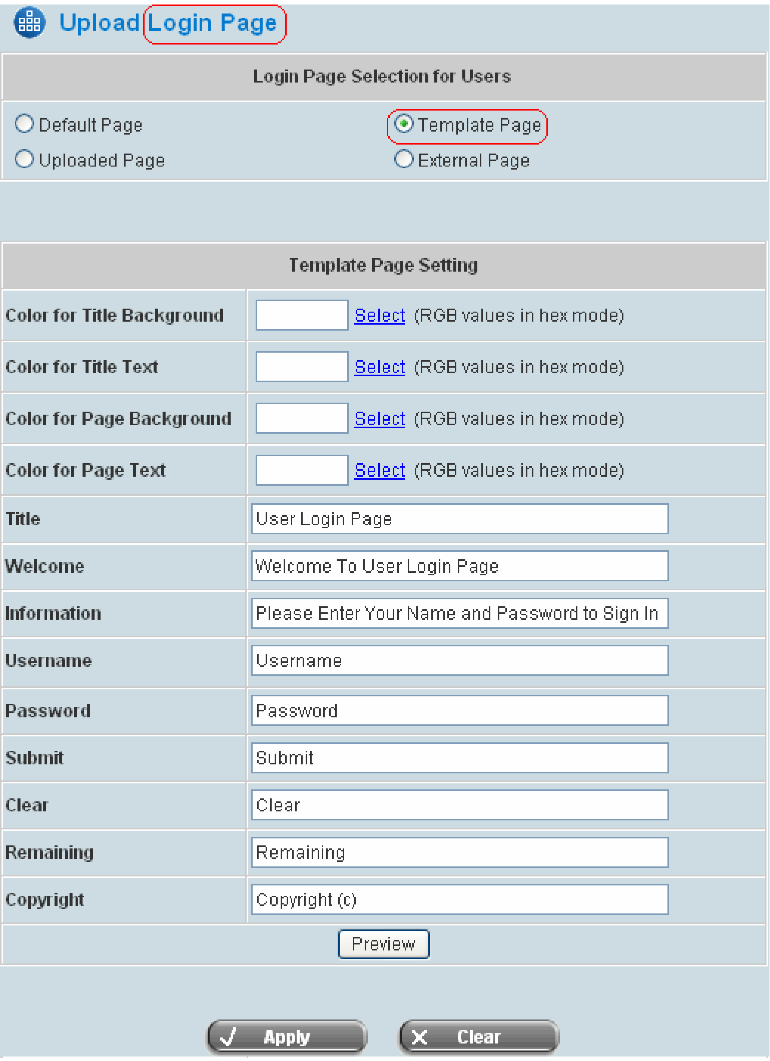
a. Choose Default Page to use the default login page.



● Default Page ○ Template Page
○ Uploaded Page ○ External Page

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

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



Upload Login Page

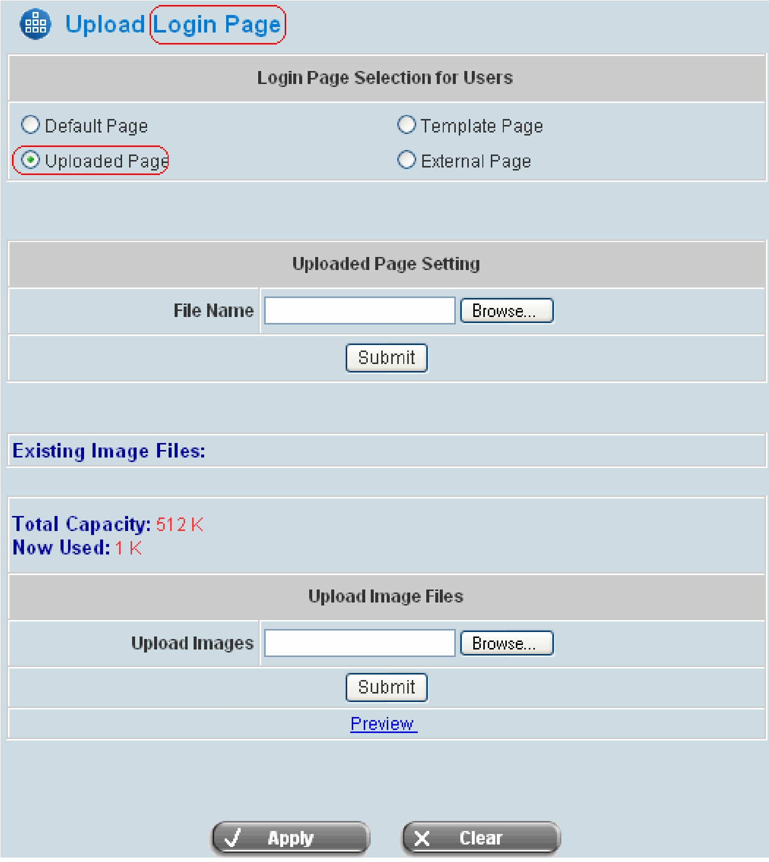
Login Page Selection for Users

○ Default Page ● Template Page
○ Uploaded Page ○ External Page

Template Page Setting

Color for Title Background	Select (RGB values in hex mode)
Color for Title Text	Select (RGB values in hex mode)
Color for Page Background	Select (RGB values in hex mode)
Color for Page Text	Select (RGB values in hex mode)
Title	User Login Page
Welcome	Welcome To User Login Page
Information	Please Enter Your Name and Password to Sign In
Username	Username
Password	Password
Submit	Submit
Clear	Clear
Remaining	Remaining
Copyright	Copyright (c)

c. Choose ***Uploaded Page*** and upload a login page.



Upload Login Page

Login Page Selection for Users

○ Default Page ○ Template Page

● Uploaded Page ○ External Page

Uploaded Page Setting

File Name [ ] Browse...

Submit

Existing Image Files:

Total Capacity: 512 K
Now Used: 1 K

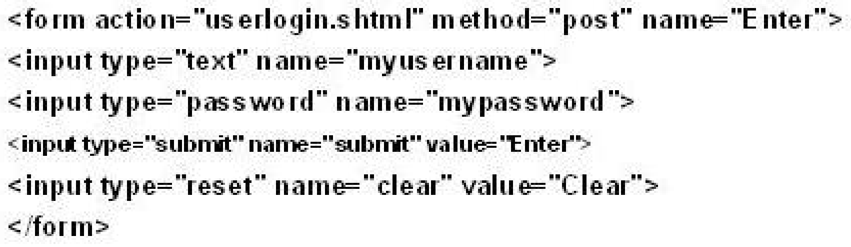
Upload Image Files

Upload Images [ ] Browse...

Submit

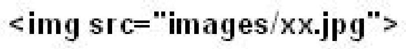
Preview

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



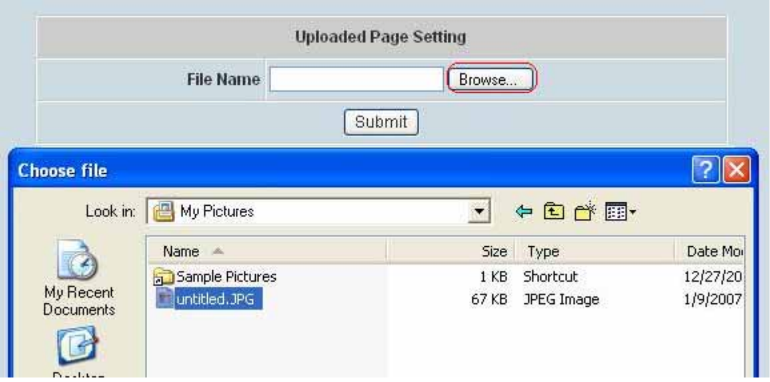
```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

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



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

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



Uploaded Page Setting

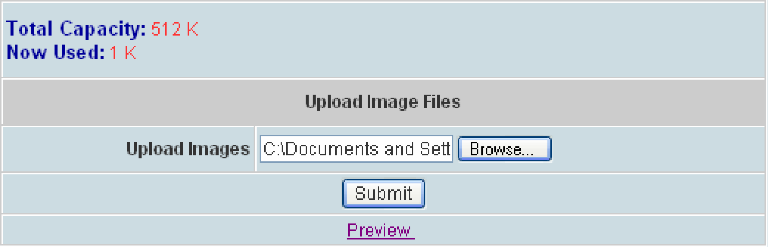
File Name

Choose file

Look in: My Pictures

Name	Size	Type	Date Mo
Sample Pictures	1 KB	Shortcut	12/27/20
untitled.JPG	67 KB	JPEG Image	1/9/2007

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

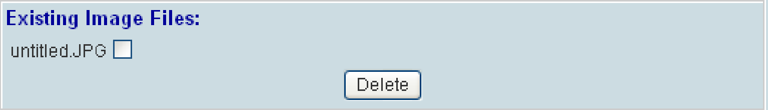


Total Capacity: 512 K
Now Used: 1 K

Upload Image Files

Upload Images: C:\Documents and Sett

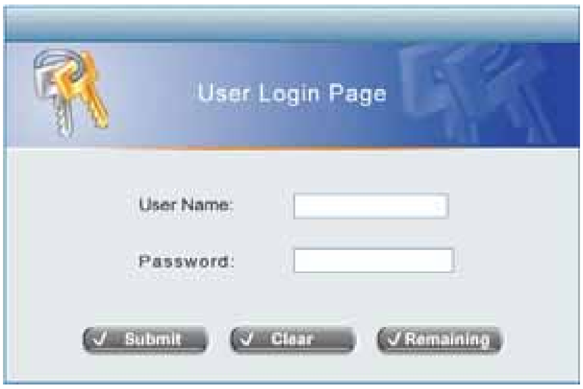
After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.



Existing Image Files:

untitled.JPG □

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



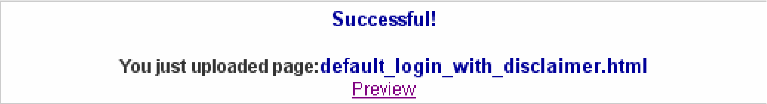
User Login Page

User Name:

Password:

In DSA-6100, the end user first gets a login page when she/he opens its web browser right after associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display "terms of use" or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking I agree, users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

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

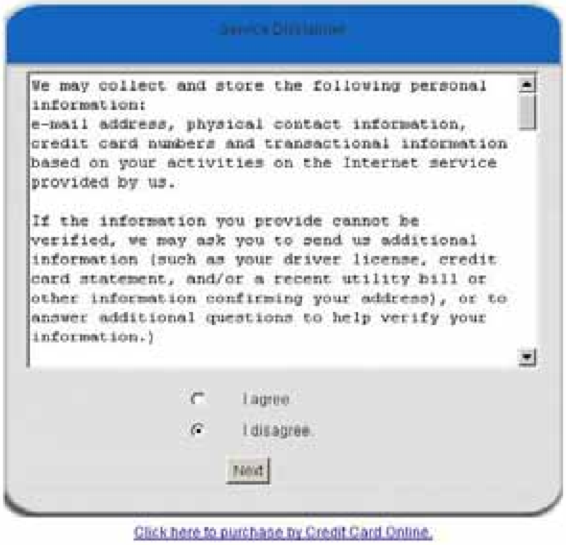


Successful!

You just uploaded page:default_login_with_disclaimer.html

Preview

"Preview" can be clicked to see the uploaded page.



Service Disclaimer

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

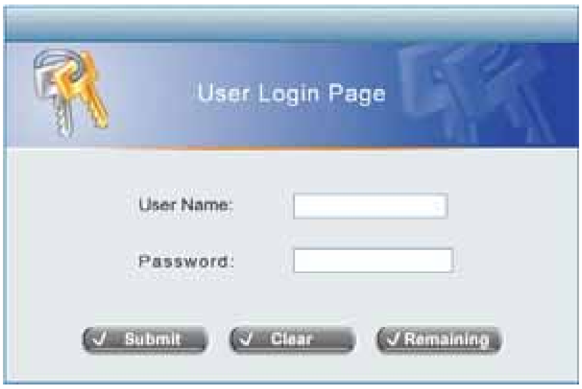
If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)

○ I agree

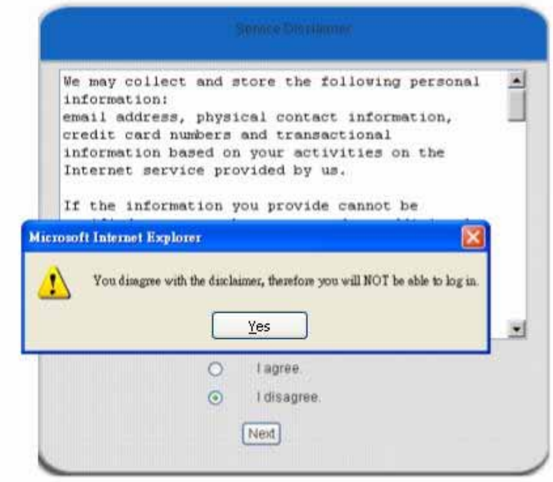
● I disagree

Click here to purchase by Credit Card Online.

If user checks **"I agree"** and clicks ***Next***, then he/she is prompted to fill in the login name and password.



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



Service Disclaimer

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

If the information you provide cannot be
```

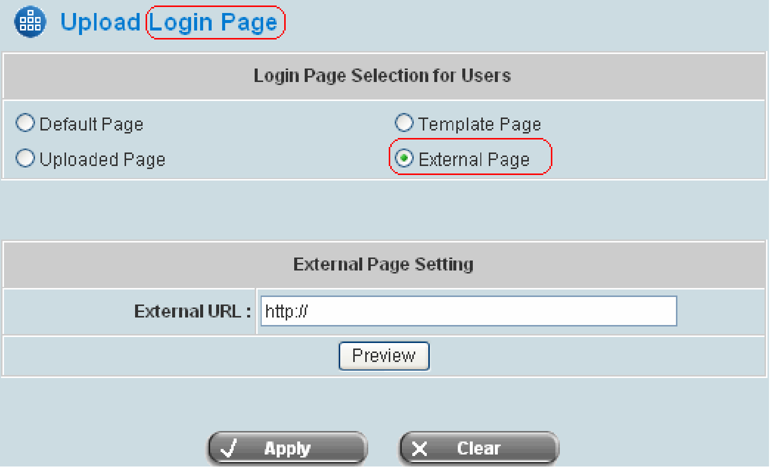
Microsoft Internet Explorer

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

○ I agree.

● I disagree.

d. Choose the ***External Page*** selection and get the login page from the specific website. In the "External Page Setting", enter URL of the external login page on the external web server and then click ***Apply***.

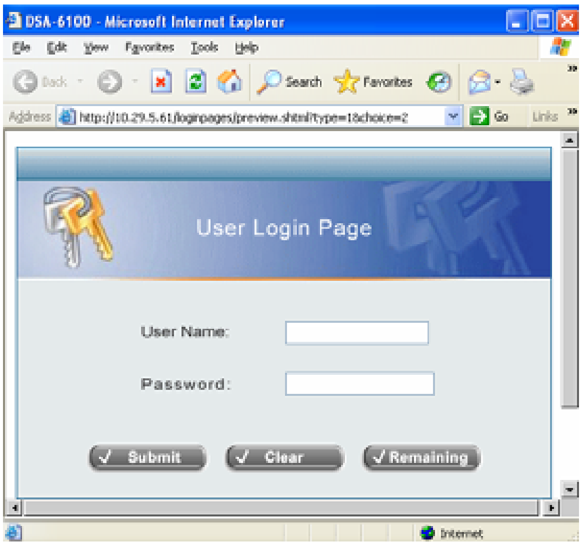


Upload Login Page

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

External Page Setting	
External URL :	http://

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


DSA-6100 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.29.5.61/loginpages/preview.shtml?type=1&choice=2
Go Links
Internet

User Login Page

User Name:

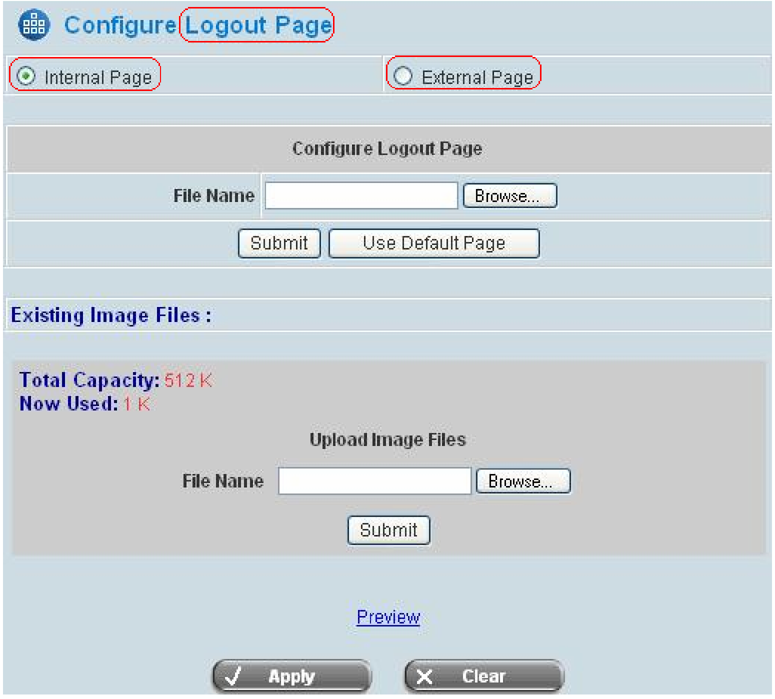
Password:

✓ Submit
✓ Clear
✓ Remaining

The user-defined logout page must include the following HTML codes to provide the necessary fields for 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>
```

3). **Logout Page:** The users can apply their own logout page in the menu. As the process is similar to that of the Login Page, please refer to the “Login Page” instructions for more details.



Configure Logout Page

● Internal Page ○ External Page

Configure Logout Page

File Name [Browse...]

[Submit] [Use Default Page]

Existing Image Files :

Total Capacity: 512 K
Now Used: 1 K

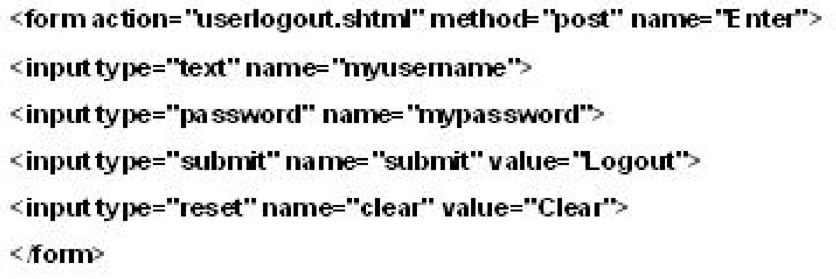
Upload Image Files

File Name [Browse...]

[Submit]

Preview

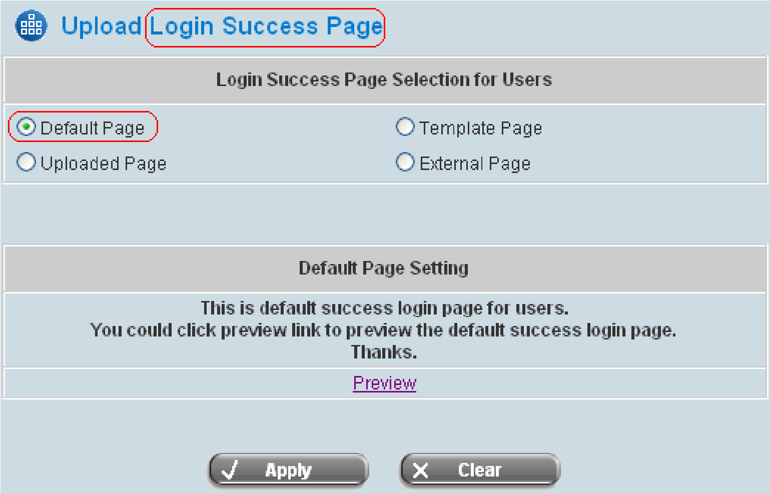
Note: The different part is the HTML code of the user-defined logout interface must include the following HTML code that the user can enter the username and password. After the upload is completed, the user-defined login user interface can be previewed by clicking ***Preview*** at the bottom of this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



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

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

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



Upload Login Success Page

Login Success Page Selection for Users

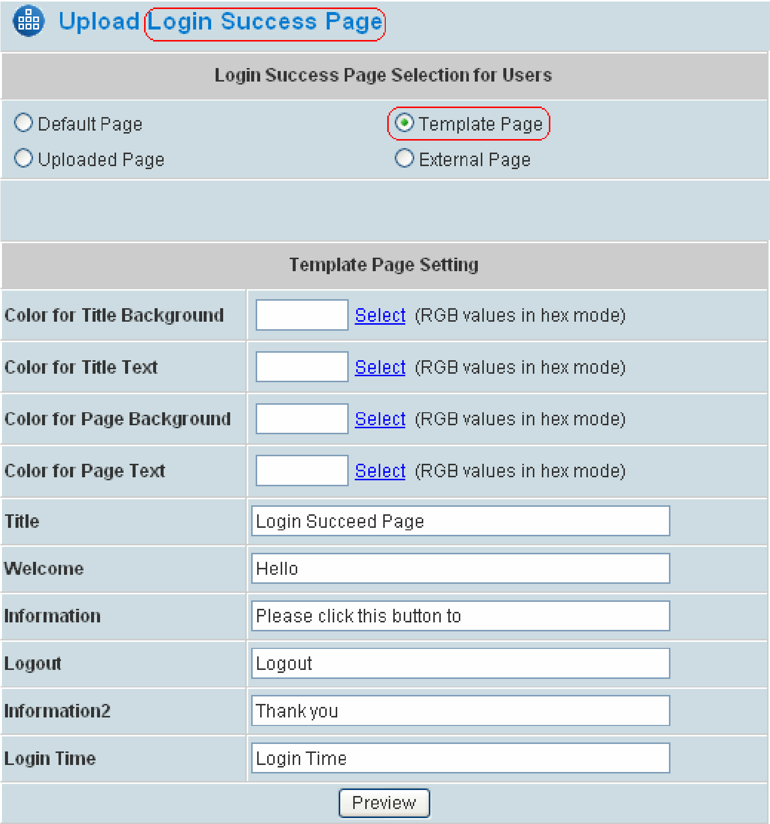
● Default Page ○ Template Page

○ Uploaded Page ○ External Page

Default Page Setting

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

b. 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.



Upload Login Success Page

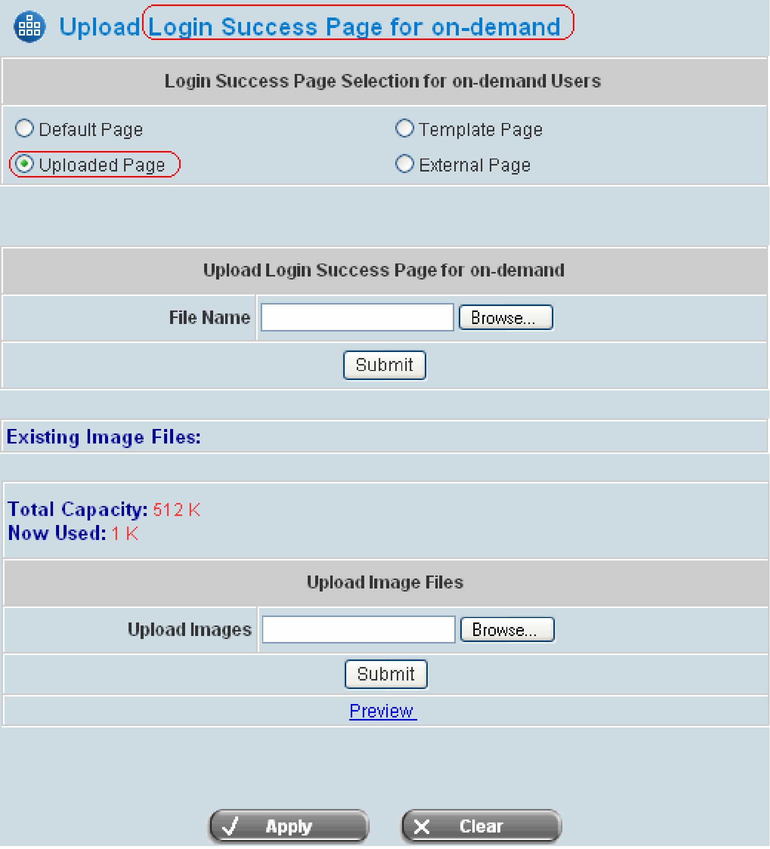
Login Success Page Selection for Users

○ Default Page　● Template Page
○ Uploaded Page　○ External Page

Template Page Setting

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

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



Upload Login Success Page for on-demand

Login Success Page Selection for on-demand Users

○ Default Page ○ Template Page
● Uploaded Page ○ External Page

Upload Login Success Page for on-demand

File Name

Existing Image Files:

Total Capacity: 512 K
Now Used: 1 K

Upload Image Files

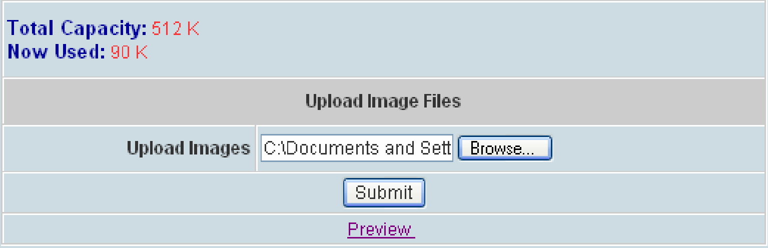
Upload Images

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

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

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

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

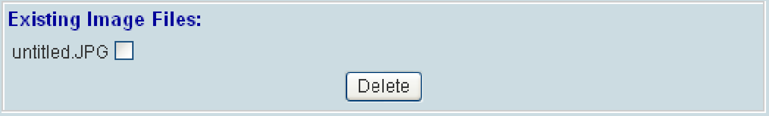


Total Capacity: 512 K
Now Used: 90 K

Upload Image Files

Upload Images: C:\Documents and Sett

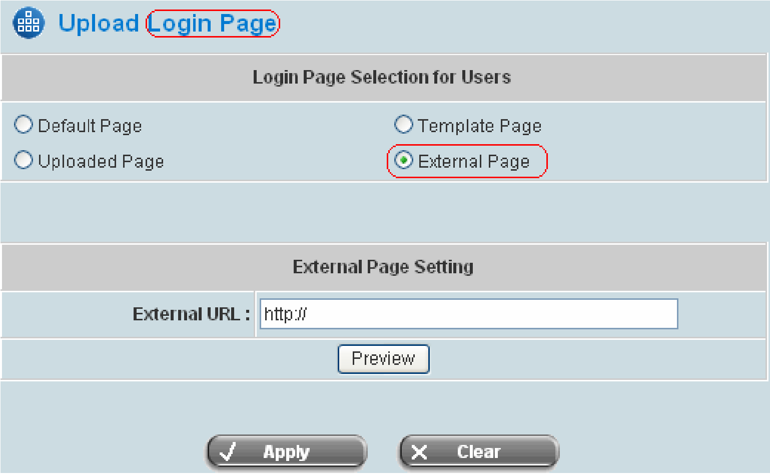
After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.



Existing Image Files:

untitled.JPG □

d. Choose the ***External Page*** selection and get the login success page from the specific website. In the "External Page Setting", enter URL of the external login page on the external web server and then click ***Apply***. After applying the setting, the new login success page for On-Demand can be previewed by clicking ***Preview*** button at the bottom of this page



Upload Login Page

Login Page Selection for Users

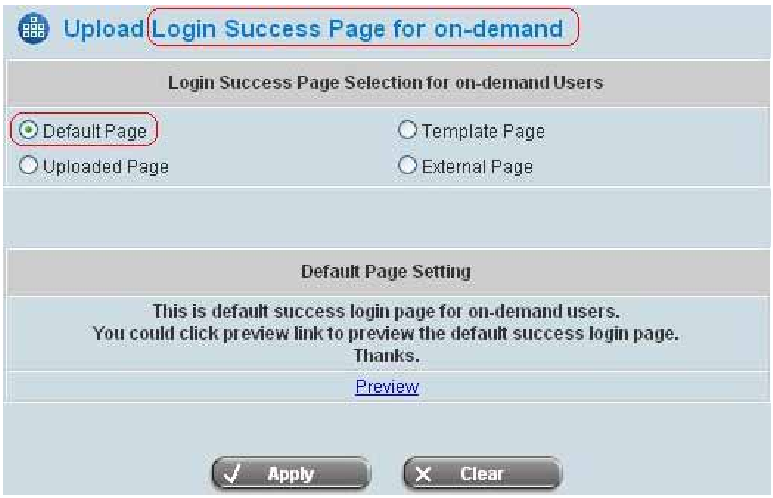
○ Default Page	○ Template Page
○ Uploaded Page	● External Page

External Page Setting

External URL : http://

5). **Login Success Page for On-Demand:** The administrator can use the default login succeed page for On-Demand or get the customized login success page for On-Demand by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click ***Preview*** to see the login success page for On-Demand.

a. Choose ***Default Page*** to use the default login success page for On-Demand.



Upload Login Success Page for on-demand

Login Success Page Selection for on-demand Users

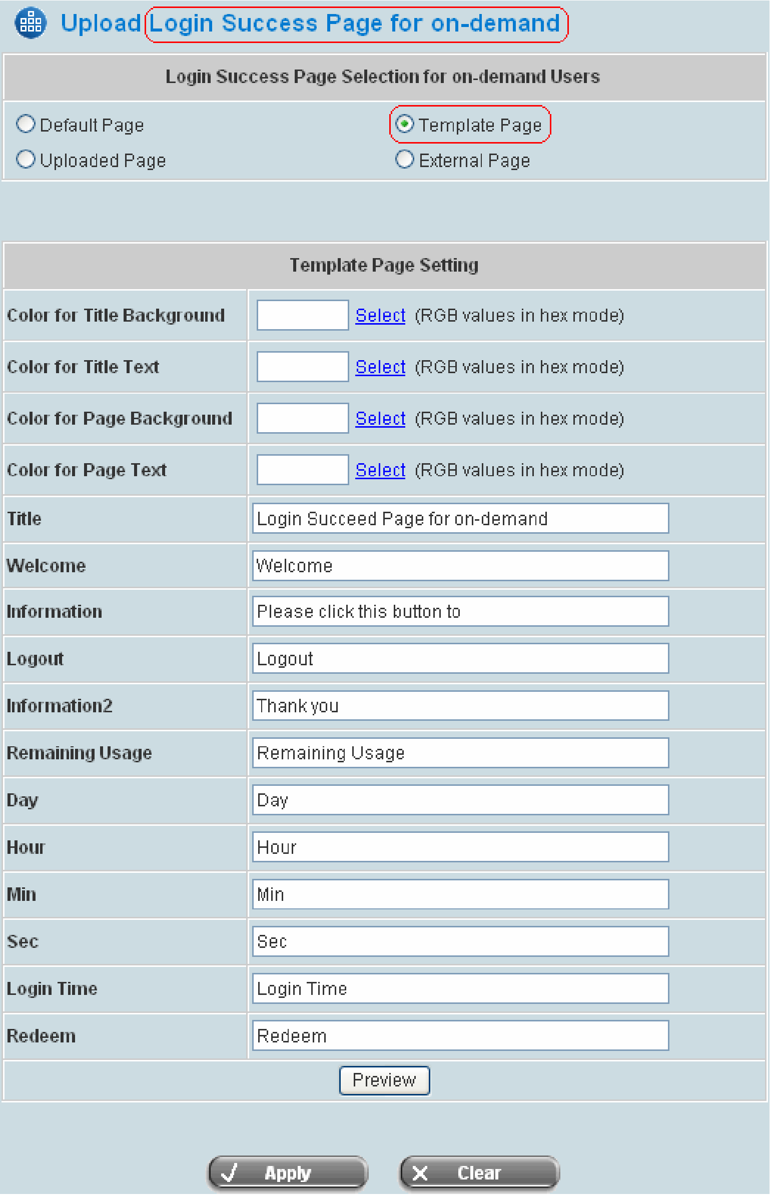
● Default Page ○ Template Page

○ Uploaded Page ○ External Page

Default Page Setting

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

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



Upload Login Success Page for on-demand

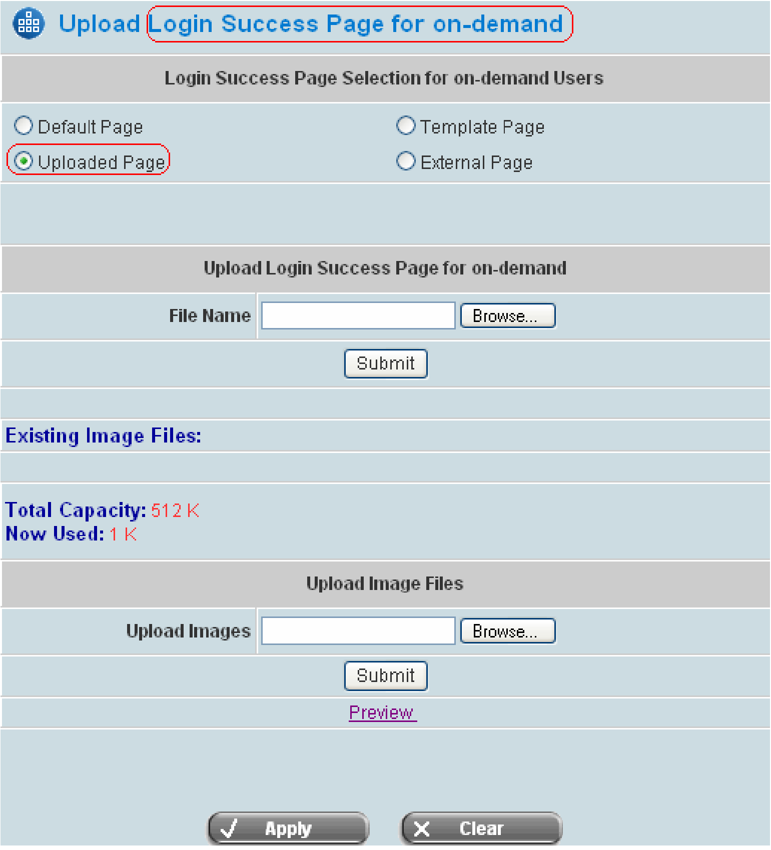
Login Success Page Selection for on-demand Users

○ Default Page ● Template Page
○ Uploaded Page ○ External Page

Template Page Setting

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

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



Upload Login Success Page for on-demand

Login Success Page Selection for on-demand Users

○ Default Page	○ Template Page
● Uploaded Page	○ External Page

Upload Login Success Page for on-demand

File Name

Existing Image Files:

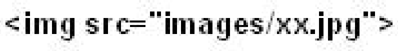
Total Capacity: 512 K
Now Used: 1 K

Upload Image Files

Upload Images

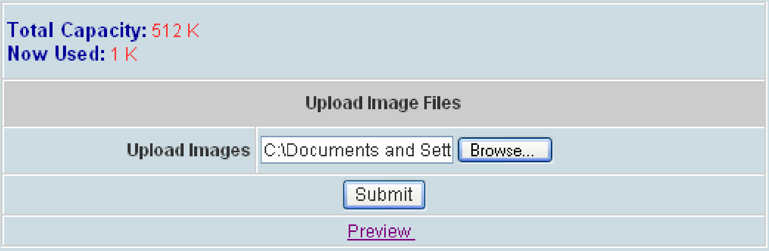
After the upload process is completed and applied, the new l login success page for On-Demand can be previewed by clicking ***Preview*** button at the bottom.

If the user-defined login success page for On-Demand includes an image file, the image file path in the HTML code must be the image file to be uploaded.



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

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

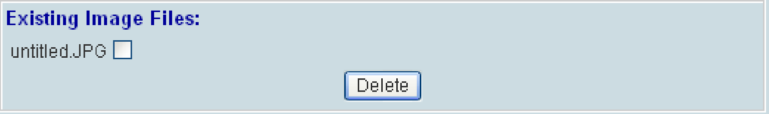


Total Capacity: 512 K
Now Used: 1 K

Upload Image Files

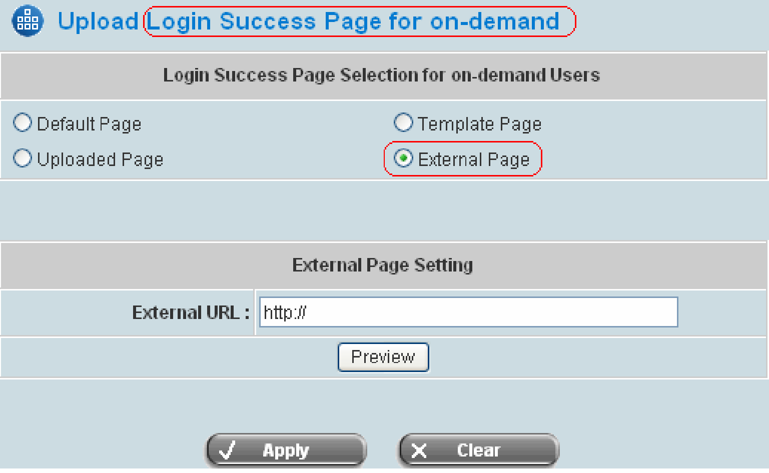
Upload Images: C:\Documents and Sett

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



Existing Image Files:
untitled.JPG □

d. Choose the ***External Page*** selection and get the login 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 login success page for On-Demand can be previewed by clicking ***Preview*** button at the bottom of this page.



Upload Login Success Page for on-demand

Login Success Page Selection for on-demand Users

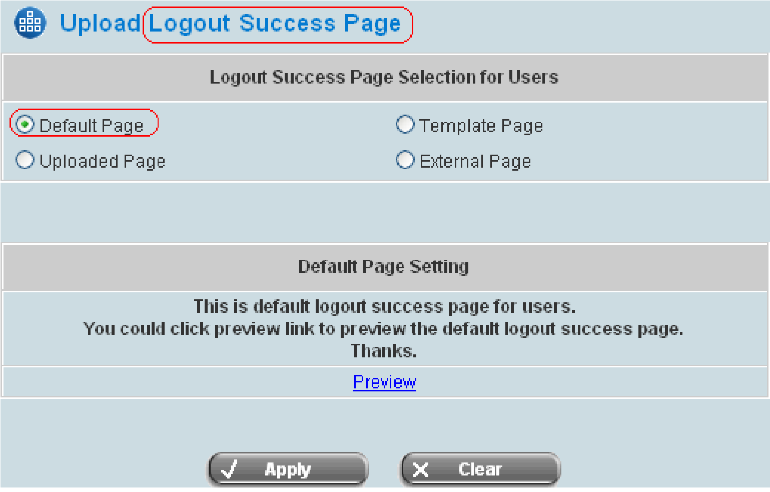
○ Default Page ○ Template Page
○ Uploaded Page ● External Page

External Page Setting

External URL : http://

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

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



Upload Logout Success Page

Logout Success Page Selection for Users

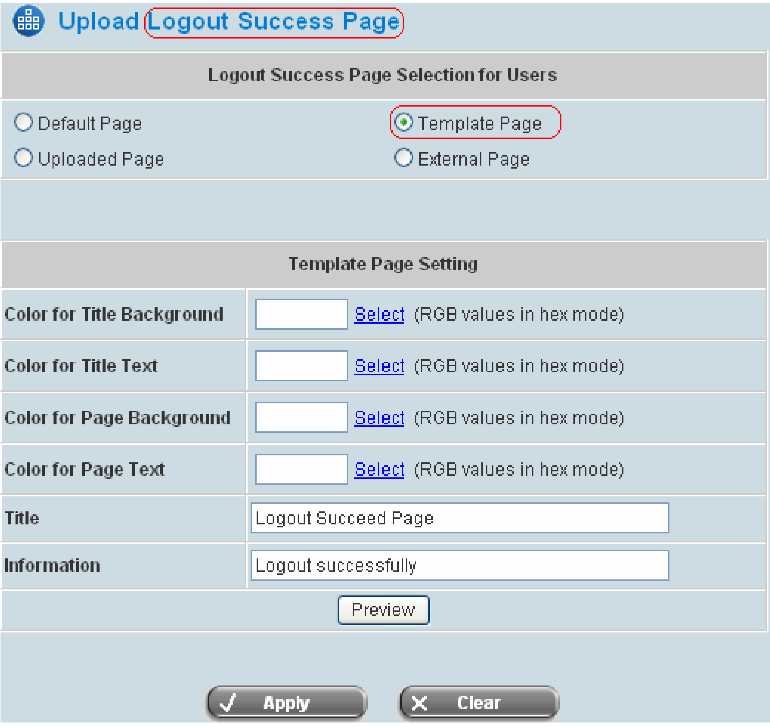
● Default Page	○ Template Page
○ Uploaded Page	○ External Page

Default Page Setting

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

Preview

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



Upload Logout Success Page

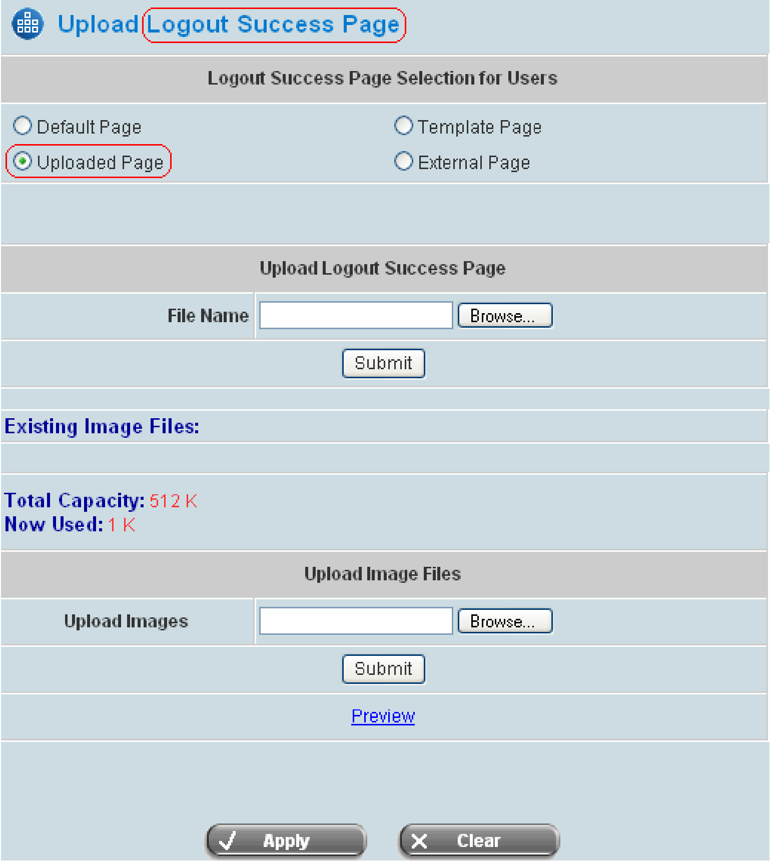
Logout Success Page Selection for Users

○ Default Page	● Template Page
○ Uploaded Page	○ External Page

Template Page Setting

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

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



Upload Logout Success Page

Logout Success Page Selection for Users

○ Default Page ○ Template Page

● Uploaded Page ○ External Page

Upload Logout Success Page

File Name

Existing Image Files:

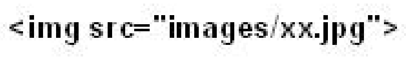
Total Capacity: 512 K
Now Used: 1 K

Upload Image Files

Upload Images

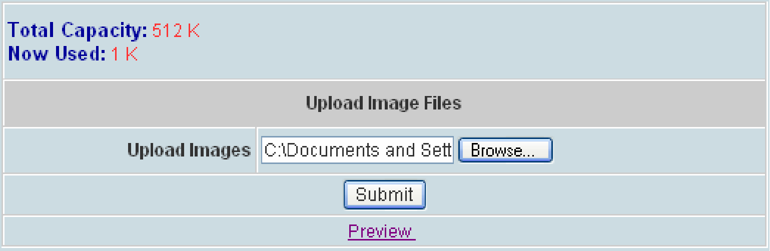
After the upload process is completed and applied, the new logout success page can be previewed by clicking ***Preview*** button at the bottom.

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



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

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

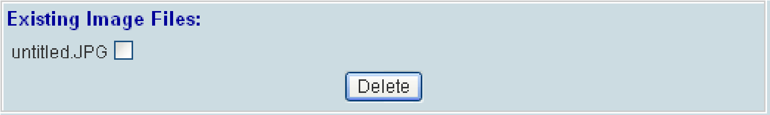


Total Capacity: 512 K
Now Used: 1 K

Upload Image Files

Upload Images: C:\Documents and Sett

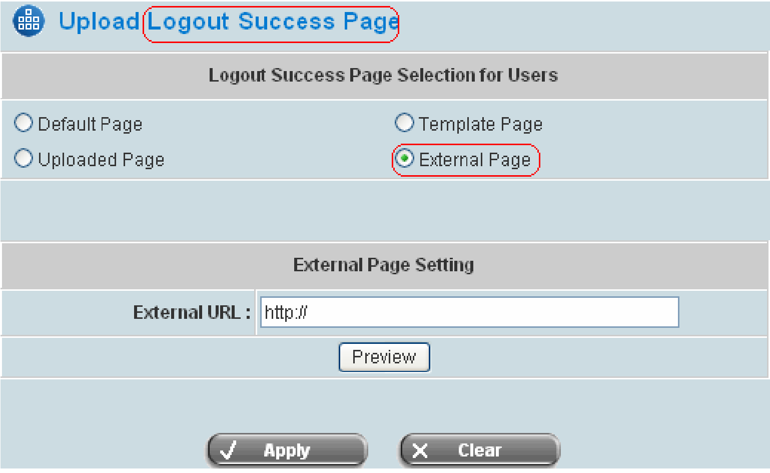
After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click ***Delete*** to delete the file.



Existing Image Files:

untitled.JPG □

d. 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.



Upload Logout Success Page

Logout Success Page Selection for Users

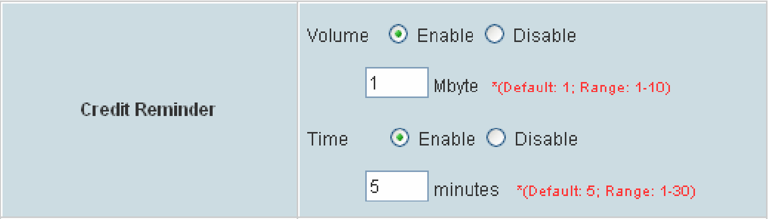
○ Default Page ○ Template Page

○ Uploaded Page ● External Page

External Page Setting

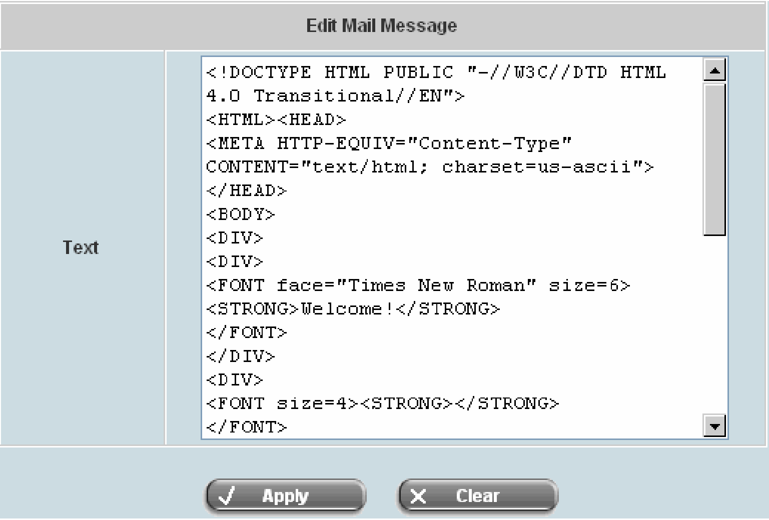
External URL : http://

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



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

E. **POP3 Message:** If a user tries to retrieve mail from POP3 mail server before login, the users will receive a welcome mail from DSA-6100. The administrator can edit the content of this welcome mail.

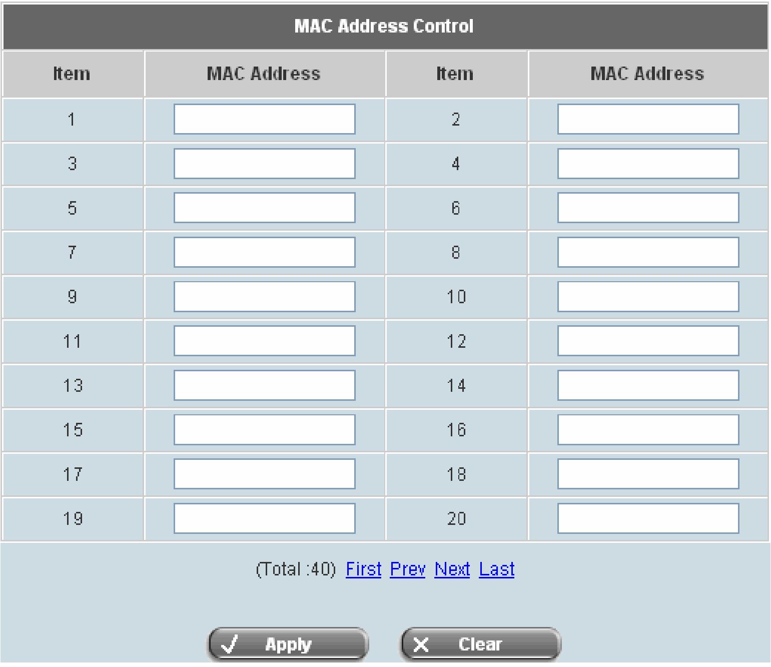


Edit Mail Message

Text

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

F. **Enhance User Authentication:** With this function, only the users with their MAC addresses in this list can log into the DSA-6100. There will only be 40 users allowed in this MAC address list. User authentication is still required for these users. Please enter the **MAC Address Control** to fill in these MAC addresses, select **Enable**, and then click ***Apply***.



MAC Address Control

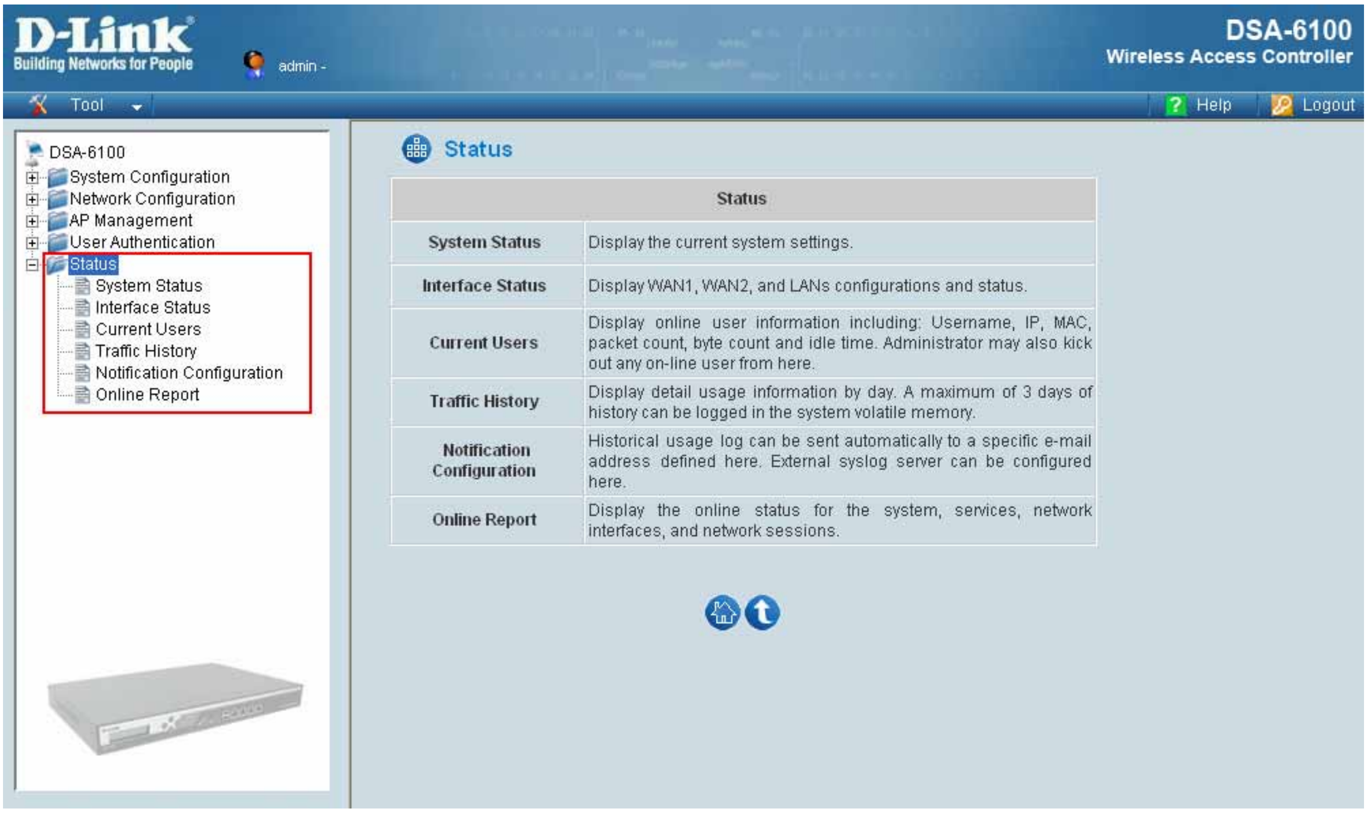
Item	MAC Address	Item	MAC Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

(Total :40) First Prev Next Last

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

4.5 Status

This section is to display information on **System Status**, **Interface Status**, **Current Users**, **Traffic History**, **Notification Configuration** and **Online Report**.

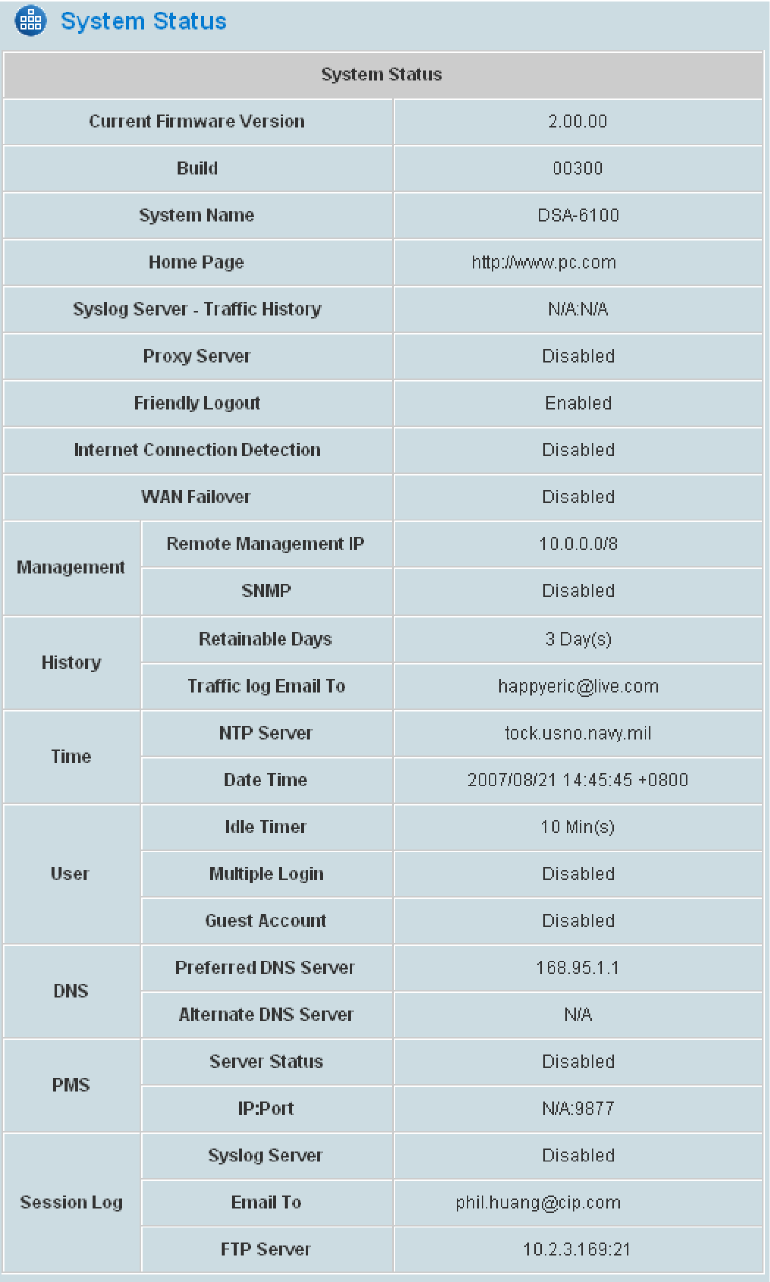


Status

Status	
System Status	Display the current system settings.
Interface Status	Display WAN1, WAN2, and LANs configurations and status.
Current Users	Display online user information including: Username, IP, MAC, packet count, byte count and idle time. Administrator may also kick out any on-line user from here.
Traffic History	Display detail usage information by day. A maximum of 3 days of history can be logged in the system volatile memory.
Notification Configuration	Historical usage log can be sent automatically to a specific e-mail address defined here. External syslog server can be configured here.
Online Report	Display the online status for the system, services, network interfaces, and network sessions.

4.5.1 System Status

The **System Status** function provides an overview of the system, the important system, network, user configurations and the system time.



System Status

System Status		
Current Firmware Version		2.00.00
Build		00300
System Name		DSA-6100
Home Page		http://www.pc.com
Syslog Server - Traffic History		N/A:N/A
Proxy Server		Disabled
Friendly Logout		Enabled
Internet Connection Detection		Disabled
WAN Failover		Disabled
Management	Remote Management IP	10.0.0.0/8
	SNMP	Disabled
History	Retainable Days	3 Day(s)
	Traffic log Email To	happyeric@live.com
Time	NTP Server	tock.usno.navy.mil
	Date Time	2007/08/21 14:45:45 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
	Guest Account	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A
PMS	Server Status	Disabled
	IP:Port	N/A:9877
Session Log	Syslog Server	Disabled
	Email To	phil.huang@cip.com
	FTP Server	10.2.3.169:21

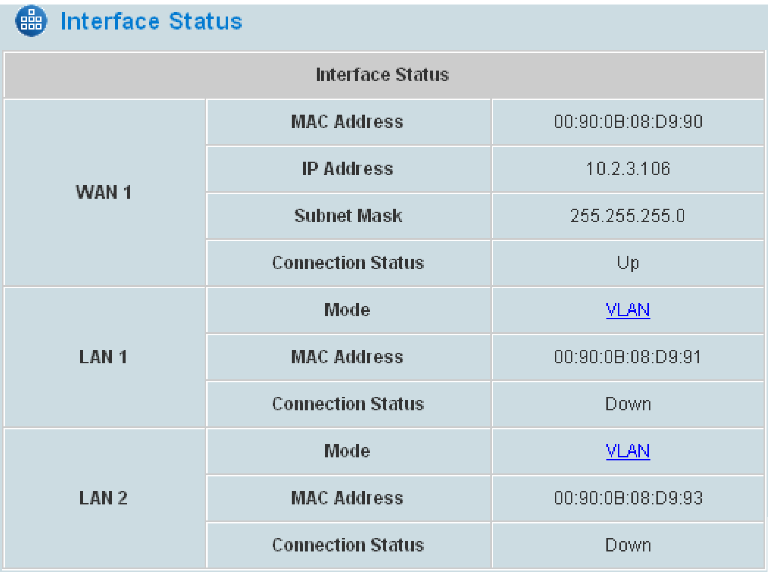
The following is a description of the information available in **System Status**:

Item	***Description***
Current Firmware Version	The present firmware version of the DSA-6100.
System Name	The system name. The default is the DSA-6100.
Home Page	The page the users are directed to after initial login success.

Syslog Server- Traffic History		The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Proxy Server		Enabled/disabled indicates whether the system is currently using a proxy server.
Friendly Logout		Enabled/disabled indicates whether a logout confirmation message has been set for display when users click the logout button.
Internet Connection Detection		Show a warning message when Internet connection is down.
WAN Failover		Show WAN1 and WAN2 status when WAN Failover is enabled.
Management	**Remote Management IP**	The IP addresses of remote computers that are allowed to access the management interface.
	SNMP	Enabled/disabled indicates the current status of the SNMP management function.
History	**Retainable Days**	The maximum number of days for the system to retain the users' traffic information.
	Traffic log Email To	The email address that the traffic history information will be sent to.
Time	**NTP Server**	The network time server that the system is set to align.
	Date Time	The system time is shown as the local time.
User	**Idle Timer**	The number of minutes allowed for the users to be inactive.
	Multiple Login	Enabled/Disabled indicates whether the current setting allow/disallow multiple logins from the same account.
	Guest Account	Enabled/Disabled indicates whether the current status allows Guest Accounts log in.
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.
PMS	**Server Status**	The current status of the PMS server.
	IP:Port	The IP and Port information of the PMS server.
Session Log	**Syslog Server**	Shows Disabled or Enable the IP address and port number of the Syslog Server in Session Log.
	Email To	The email address of the receiver.
	FTP Server	Shows Disabled or Enabled the IP address and port number of the FTP Server in Session Log.

4.5.2 Interface Status

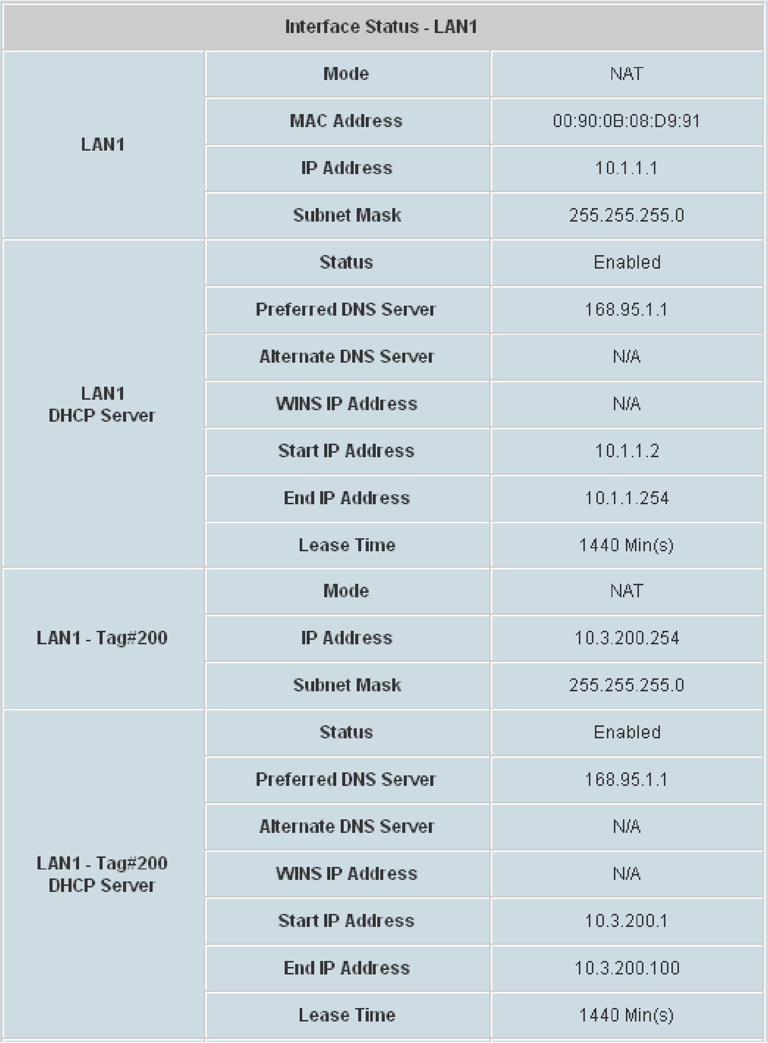
The **Interface Status** function provides an overview of the interfaces on the network, including **WAN1**, **LAN1** and **LAN2** interfaces.



Interface Status

Interface Status		
WAN 1	MAC Address	00:90:0B:08:D9:90
	IP Address	10.2.3.106
	Subnet Mask	255.255.255.0
	Connection Status	Up
LAN 1	Mode	VLAN
	MAC Address	00:90:0B:08:D9:91
	Connection Status	Down
LAN 2	Mode	VLAN
	MAC Address	00:90:0B:08:D9:93
	Connection Status	Down

Click on **VLAN** hyperlink to enter VLAN Interface Status, including status of **LAN DHCP Server**, **LAN Tag#** and **LAN Tag# DHCP Server**.



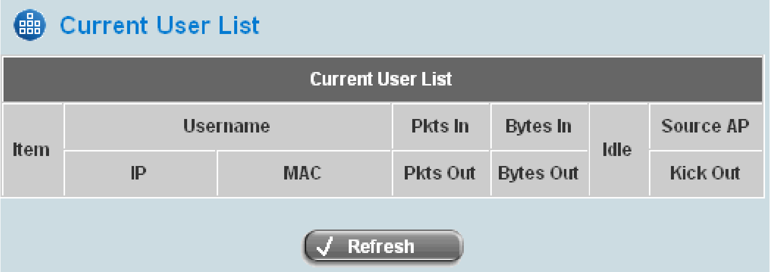
Interface Status - LAN1		
LAN1	Mode	NAT
	MAC Address	00:90:0B:08:D9:91
	IP Address	10.1.1.1
	Subnet Mask	255.255.255.0
LAN1 DHCP Server	Status	Enabled
	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A
	WINS IP Address	N/A
	Start IP Address	10.1.1.2
	End IP Address	10.1.1.254
	Lease Time	1440 Min(s)
LAN1 - Tag#200	Mode	NAT
	IP Address	10.3.200.254
	Subnet Mask	255.255.255.0
LAN1 - Tag#200 DHCP Server	Status	Enabled
	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A
	WINS IP Address	N/A
	Start IP Address	10.3.200.1
	End IP Address	10.3.200.100
	Lease Time	1440 Min(s)

The following is a description of the information available for **Interface Status**:

Item		***Description***
WAN1	**MAC Address**	The MAC address of the WAN1 port.
	IP Address	The IP address of the WAN1 port.
	Subnet Mask	The Subnet Mask of the WAN1 port.
	Connection Status	The status of connection in active or inactive.
LAN1/LAN2	**Mode**	The mode of the LAN port.
	MAC Address	The MAC address of the LAN.
	IP Address	The IP address of the LAN.
	Subnet Mask	The Subnet Mask of the LAN.
	Connection Status	The status of connection in active or inactive.
LAN1/LAN2 DHCP Server	**Status**	Enabled/Disabled indicates the status of the DHCP server on the LAN.
	Preferred DNS Server	The primary DNS server of the LAN.
	Alternate DNS Server	The secondary DNS server of the LAN.
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP Address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address distributed by the DHCP server.
LAN1/2- Tag#		Tag numbers of VLANs under LAN1/LAN2 interface.
LAN1/2- Tag# DHCP Server		DHCP settings for the VLANs under LAN1/LAN2 interface.

4.5.3 Current Users

In this function, each online user's information including **Username**, **IP Address**, **MAC Address**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out, Idle** and **Kick Out** can be obtained. Administrator can use this function to force a specific online user to log out. Just click the hyperlink of ***Logout*** next to the online user's name to logout that particular user. Click ***Refresh*** to renew the current users list.



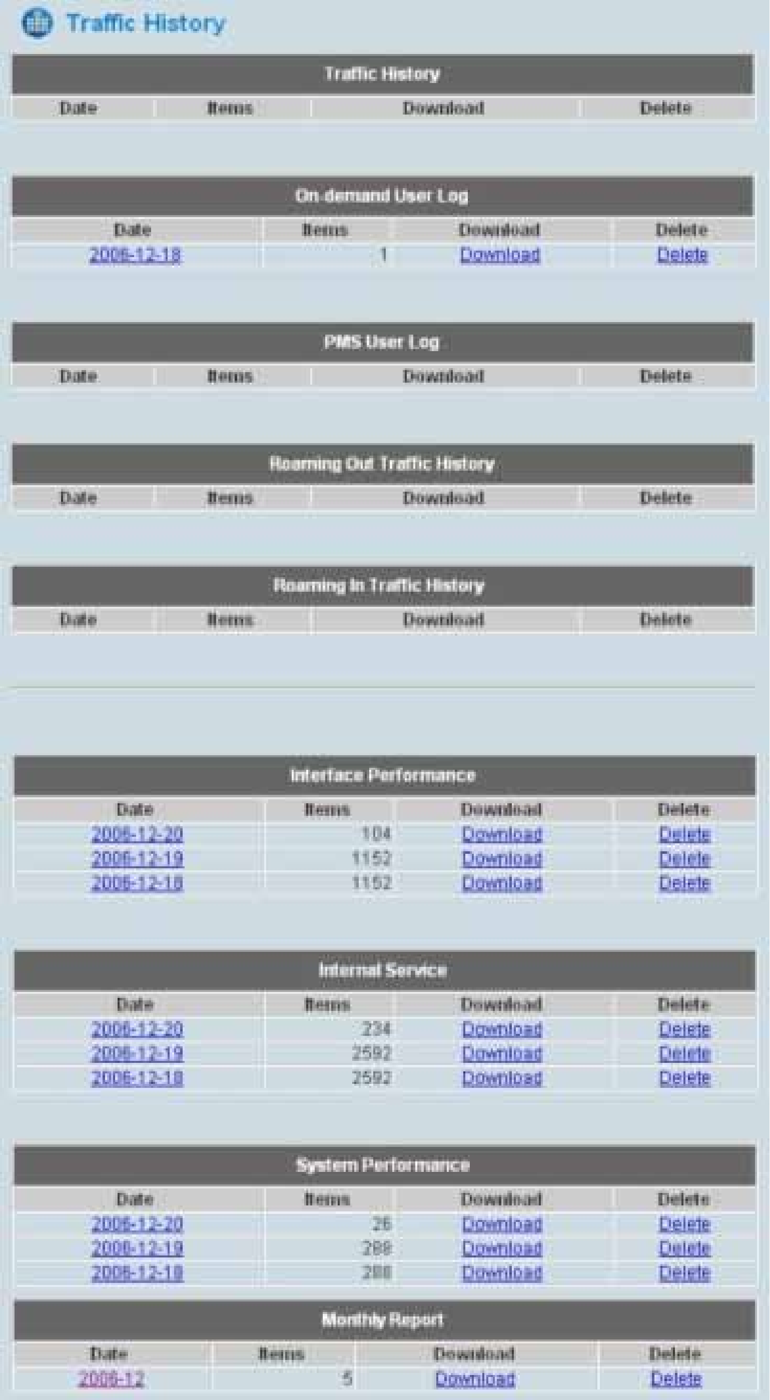
Current User List

Current User List

Item	Username		Pkts In	Bytes In	Idle	Source AP
	IP	MAC	Pkts Out	Bytes Out		Kick Out

4.5.4 Traffic History

This function is used to check the history of the DSA-6100. Administrator may keep the following records for up to 3 days. All records are sorted by date and listed accordingly. Please note that these records are stored on the volatile memory and will be lost if the system is turnoff.



Traffic History

Traffic History			
Date	Items	Download	Delete

On-demand User Log			
Date	Items	Download	Delete
2006-12-18	1	Download	Delete

PMS User Log			
Date	Items	Download	Delete

Roaming Out Traffic History			
Date	Items	Download	Delete

Roaming In Traffic History			
Date	Items	Download	Delete

Interface Performance			
Date	Items	Download	Delete
2006-12-20	104	Download	Delete
2006-12-19	1152	Download	Delete
2006-12-18	1152	Download	Delete

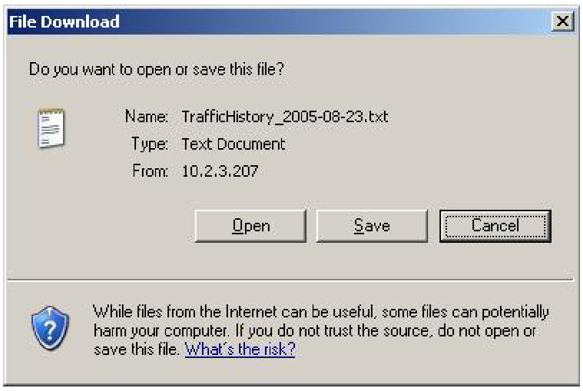
Internal Service			
Date	Items	Download	Delete
2006-12-20	234	Download	Delete
2006-12-19	2592	Download	Delete
2006-12-18	2592	Download	Delete

System Performance			
Date	Items	Download	Delete
2006-12-20	26	Download	Delete
2006-12-19	288	Download	Delete
2006-12-18	288	Download	Delete

Monthly Report			
Date	Items	Download	Delete
2006-12	5	Download	Delete

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

Click ***Download*** to save every history log in a text file.



File Download

Do you want to open or save this file?

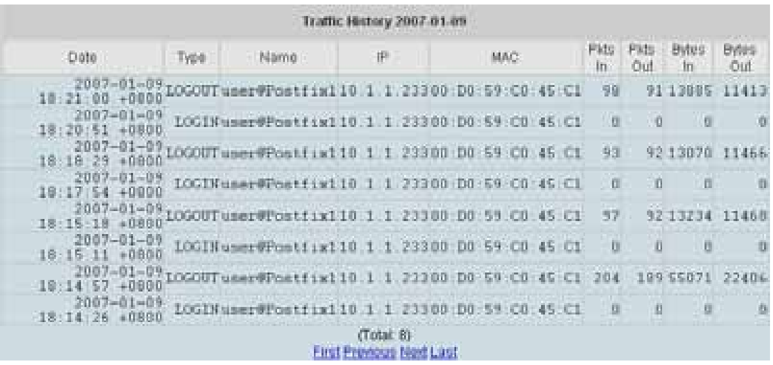
Name: TrafficHistory_2005-08-23.txt
Type: Text Document
From: 10.2.3.207

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

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

- **Traffic History**

  Sorted by time, the traffic history provided all login and logout activities of the specific date. It includes User Name, IP address, MAC address, In-bound Packet Count, Out-bound Packet Count, In-bound Byte Count, and Out-bound Byte Count. As shown in the following picture, each line is a traffic history record consisting of 9 fields, **Date**, **Type, Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out,** and **Bytes Out**, of user activities.



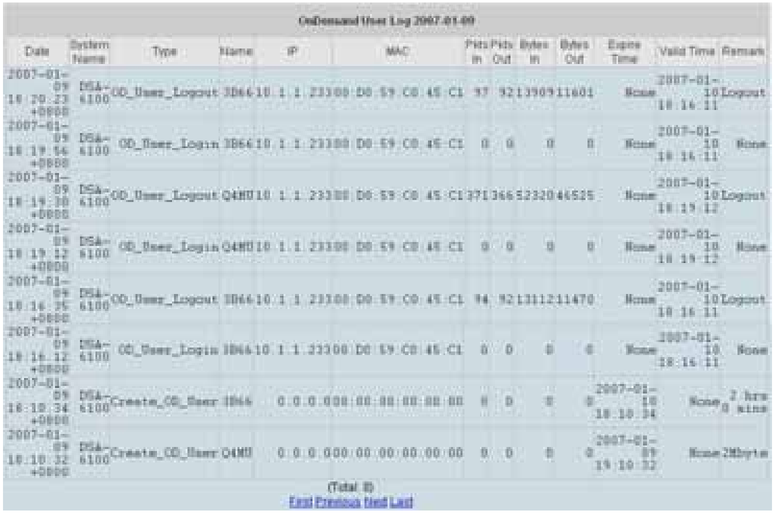
Traffic History 2007-01-09

Date	Type	Name	IP	MAC	Pkts In	Pkts Out	Bytes In	Bytes Out
2007-01-09 18:21:00 +0800	LOGOUT	user@Postfix1	10.1.1.233	00:D0:59:C0:45:C1	99	91	13885	11413
2007-01-09 18:20:51 +0800	LOGIN	user@Postfix1	10.1.1.233	00:D0:59:C0:45:C1	0	0	0	0
2007-01-09 18:18:29 +0800	LOGOUT	user@Postfix1	10.1.1.233	00:D0:59:C0:45:C1	93	92	13070	11466
2007-01-09 18:17:54 +0800	LOGIN	user@Postfix1	10.1.1.233	00:D0:59:C0:45:C1	0	0	0	0
2007-01-09 18:15:18 +0800	LOGOUT	user@Postfix1	10.1.1.233	00:D0:59:C0:45:C1	97	92	13234	11468
2007-01-09 18:15:11 +0800	LOGIN	user@Postfix1	10.1.1.233	00:D0:59:C0:45:C1	0	0	0	0
2007-01-09 18:14:57 +0800	LOGOUT	user@Postfix1	10.1.1.233	00:D0:59:C0:45:C1	204	189	55071	22406
2007-01-09 18:14:26 +0800	LOGIN	user@Postfix1	10.1.1.233	00:D0:59:C0:45:C1	0	0	0	0

(Total: 8)

- **On-demand User Log**

  This page includes the on-demand user account status changes and the traffic history. As shown in the following picture, each line shows a on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, Expiretime**, **Validtime** and **Remark**, of user activities.



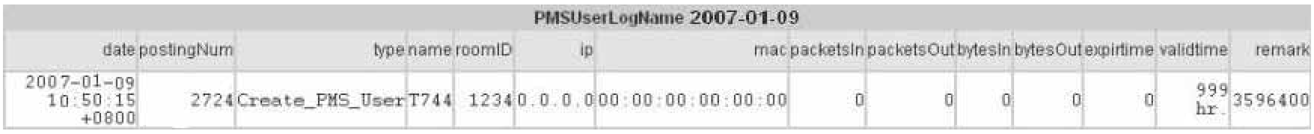
OnDemand User Log 2007-01-09

Date	System Name	Type	Name	IP	MAC	Pkts In	Pkts Out	Bytes In	Bytes Out	Expire Time	Valid Time	Remark
2007-01-09 18:20:23 +0800	DSA-6100	OD_User_Logout	3B66	10.1.1.233	00:D0:59:C0:45:C1	97	92	13909	11601	None	2007-01-10 18:16:11	Logout
2007-01-09 18:19:56 +0800	DSA-6100	OD_User_Login	3B66	10.1.1.233	00:D0:59:C0:45:C1	0	0	0	0	None	2007-01-10 18:16:11	None
2007-01-09 18:19:30 +0800	DSA-6100	OD_User_Logout	Q4MU	10.1.1.233	00:D0:59:C0:45:C1	371	366	52320	46525	None	2007-01-10 18:19:12	Logout
2007-01-09 18:19:12 +0800	DSA-6100	OD_User_Login	Q4MU	10.1.1.233	00:D0:59:C0:45:C1	0	0	0	0	None	2007-01-10 18:19:12	None
2007-01-09 18:16:35 +0800	DSA-6100	OD_User_Logout	3B66	10.1.1.233	00:D0:59:C0:45:C1	94	92	13112	11470	None	2007-01-10 18:16:11	Logout
2007-01-09 18:16:12 +0800	DSA-6100	OD_User_Login	3B66	10.1.1.233	00:D0:59:C0:45:C1	0	0	0	0	None	2007-01-10 18:16:11	None
2007-01-09 18:10:34 +0800	DSA-6100	Create_OD_User	3B66	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-01-10 18:10:34	None	2 hrs 0 mins
2007-01-09 18:10:32 +0800	DSA-6100	Create_OD_User	Q4MU	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-01-09 19:10:32	None	2Mbyte

(Total: 8)

- **PMS User Log**

  This page includes the PMS user account status changes and the traffic history. The following picture shows each line of the on-demand user log record consisting of 14 fields: **Date**, **Posting Number**, **Type**, **Name**, **Room ID**, **IP**, **MAC**, **Packets In**, **Packets Out**, **Bytes In**, **Bytes Out**, **ExpireTime**, **ValidTime** and **Remark**.

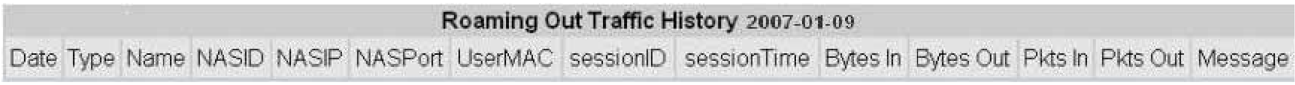


PMSUserLogName 2007-01-09

date	postingNum	type	name	roomID	ip	mac	packetsIn	packetsOut	bytesIn	bytesOut	expirtime	validtime	remark
2007-01-09 10:50:15 +0800	2724	Create_PMS_User	T744	1234	0.0.0.0	00:00:00:00:00:00	0	0	0	0	0	999 hr.	3596400

- **Roaming Out Traffic History**

  This page includes all traffic history of the users who have roamed out to the other hotspots. The following picture shows each of the roaming out traffic history record of user activities, consisting 14 fields: **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**.

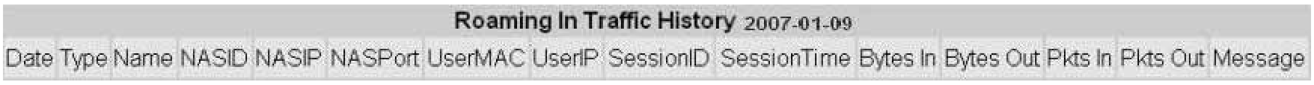


Roaming Out Traffic History 2007-01-09

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

- **Roaming In Traffic History**

  This page includes all traffic history of the users who have roamed into this system. The following picture shows each line of the roaming in traffic history record of user activities, consisting of 15 fields: **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**.

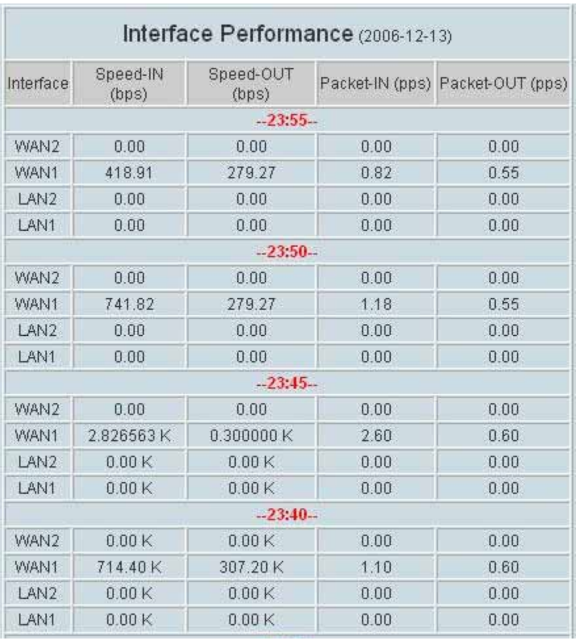


Roaming In Traffic History 2007-01-09

Date	Type	Name	NASID	NASIP	NASPort	UserMAC	UserIP	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **Interface Performance**

  As shown in the following picture, the history record consists of 5 fields for WAN and LAN status: **Interface**, **Speed-IN (bps)**, **Speed-OUT (bps)**, **Packet-IN (pps)** and **Packet-OUT (pps)**.

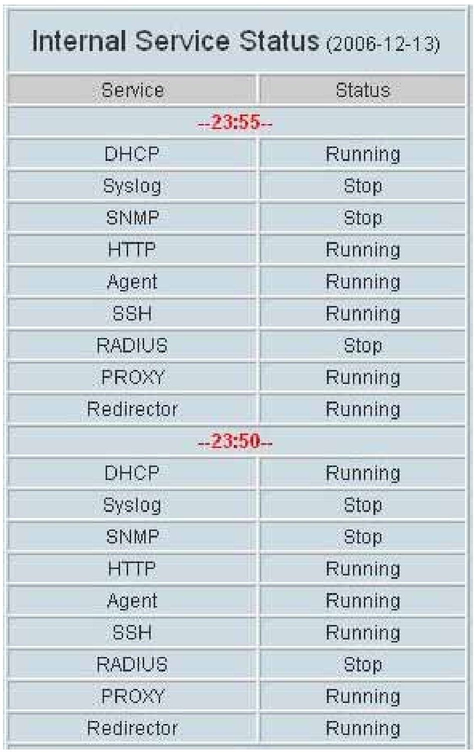


Interface Performance (2006-12-13)

Interface	Speed-IN (bps)	Speed-OUT (bps)	Packet-IN (pps)	Packet-OUT (pps)
--23:55--				
WAN2	0.00	0.00	0.00	0.00
WAN1	418.91	279.27	0.82	0.55
LAN2	0.00	0.00	0.00	0.00
LAN1	0.00	0.00	0.00	0.00
--23:50--				
WAN2	0.00	0.00	0.00	0.00
WAN1	741.82	279.27	1.18	0.55
LAN2	0.00	0.00	0.00	0.00
LAN1	0.00	0.00	0.00	0.00
--23:45--				
WAN2	0.00	0.00	0.00	0.00
WAN1	2.826563 K	0.300000 K	2.60	0.60
LAN2	0.00 K	0.00 K	0.00	0.00
LAN1	0.00 K	0.00 K	0.00	0.00
--23:40--				
WAN2	0.00 K	0.00 K	0.00	0.00
WAN1	714.40 K	307.20 K	1.10	0.60
LAN2	0.00 K	0.00 K	0.00	0.00
LAN1	0.00 K	0.00 K	0.00	0.00

- **Internal Service**

  This page shows the history records of the internal daemon services. As shown in the following picture, the history record consists of 6 fields for network service status: **DHCP Server**, **Syslog Server**, **SNMP Server**, **HTTP Server**, **Agent**, **SSH Server**, **RADIUS Server**, **Proxy Server** and **Redirector Server**.

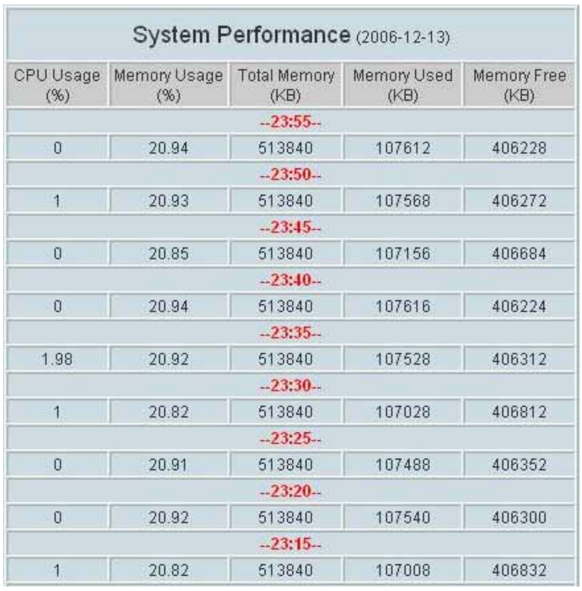


Internal Service Status (2006-12-13)

Service	Status
--23:55--	
DHCP	Running
Syslog	Stop
SNMP	Stop
HTTP	Running
Agent	Running
SSH	Running
RADIUS	Stop
PROXY	Running
Redirector	Running
--23:50--	
DHCP	Running
Syslog	Stop
SNMP	Stop
HTTP	Running
Agent	Running
SSH	Running
RADIUS	Stop
PROXY	Running
Redirector	Running

- **System Performance**

  This page shows the history records of the CPU and memory usage. As shown in the following picture, the history record consists of 5 fields of the DSA-6100 status: **CPU Usage %**, **Memory Usage %**, **Total Memory (KB)**, **Memory Used (KB)** and **Memory Free (KB)**.

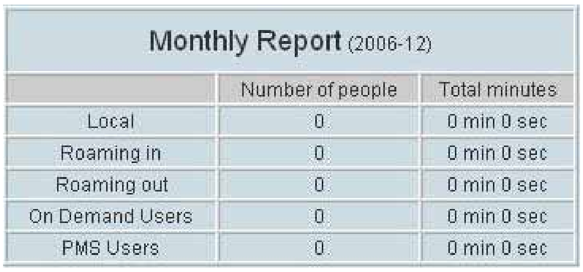


System Performance (2006-12-13)

CPU Usage (%)	Memory Usage (%)	Total Memory (KB)	Memory Used (KB)	Memory Free (KB)
--23:55--				
0	20.94	513840	107612	406228
--23:50--				
1	20.93	513840	107568	406272
--23:45--				
0	20.85	513840	107156	406684
--23:40--				
0	20.94	513840	107616	406224
--23:35--				
1.98	20.92	513840	107528	406312
--23:30--				
1	20.82	513840	107028	406812
--23:25--				
0	20.91	513840	107488	406352
--23:20--				
0	20.92	513840	107540	406300
--23:15--				
1	20.82	513840	107008	406832

- **Monthly Report**

  Monthly traffic statistics. As shown in the following picture, the monthly report consists of 5 fields: **Local**, **Roaming in**, **Roaming out**, **On Demand Users**, **PMS Users**.

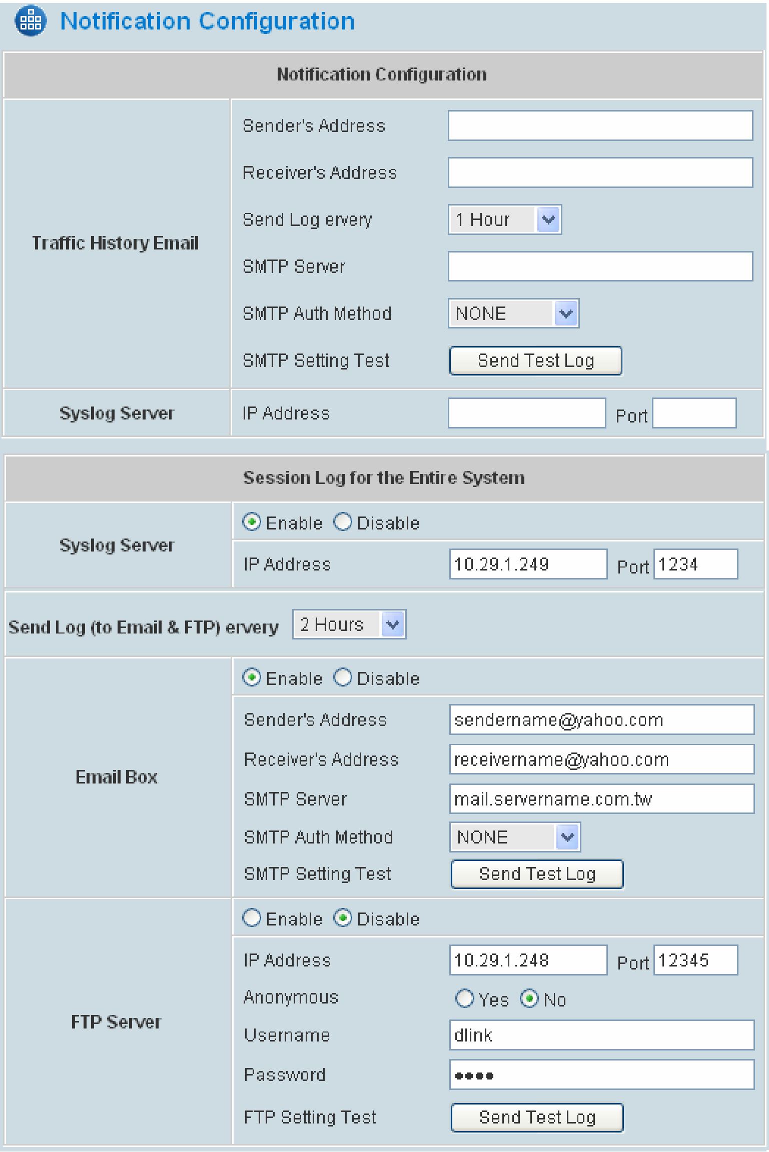


Monthly Report (2006-12)

	Number of people	Total minutes
Local	0	0 min 0 sec
Roaming in	0	0 min 0 sec
Roaming out	0	0 min 0 sec
On Demand Users	0	0 min 0 sec
PMS Users	0	0 min 0 sec

4.5.5 Notification Configuration

As earlier mentioned, the DSA-6100 will save the traffic history into the internal DRAM. If the administrator wants the system to automatically send out the history to a particular email address, a notification configuration may be set as shown in the picture below. Please enter the related information in these fields.



Notification Configuration

Notification Configuration			
Traffic History Email	Sender's Address		
	Receiver's Address		
	Send Log ervery	1 Hour	
	SMTP Server		
	SMTP Auth Method	NONE	
	SMTP Setting Test	Send Test Log	
Syslog Server	IP Address		Port

Session Log for the Entire System			
Syslog Server	● Enable ○ Disable		
	IP Address	10.29.1.249	Port 1234
Send Log (to Email & FTP) ervery 2 Hours			
Email Box	● Enable ○ Disable		
	Sender's Address	sendername@yahoo.com	
	Receiver's Address	receivername@yahoo.com	
	SMTP Server	mail.servername.com.tw	
	SMTP Auth Method	NONE	
	SMTP Setting Test	Send Test Log	
FTP Server	○ Enable ● Disable		
	IP Address	10.29.1.248	Port 12345
	Anonymous	○ Yes ● No	
	Username	dlink	
	Password	●●●●	
	FTP Setting Test	Send Test Log	

Notification Configuration

- **Traffic History Email:** The system will send Traffic History and On-demand User Log automatically to any valid email account and external Syslog Server. Administrator can configure the sending interval of each notification email. SMTP Server and a valid email account are required to send notification email.
  - **Sender's Address:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
  - **Receiver's Address:** The e-mail address of the person whom the history email is for. This will be the receiver's e-mail.
  - **Send Log every:** The time interval to send the e-mail report.

- **SMTP Server:** The IP address or domain name 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 selected, enter the **Account Name**, **Password** and **Domain**.

  NTLMv1 is not currently available for general use.

  Plain and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**. Outlook and Outlook express uses **Login** as default, although they can be set to use **NTLMv1**. Pegasus uses **CRAM-MD5** or **Login** but which method to be used can not be decided manually.
- **SMTP Setting Test**: Click ***Send Test Log*** button to send a test email of the report.

- **Syslog Server:** Enter the IP address and Port number of the Syslog server.

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 F.*

Session Log for the Entire System

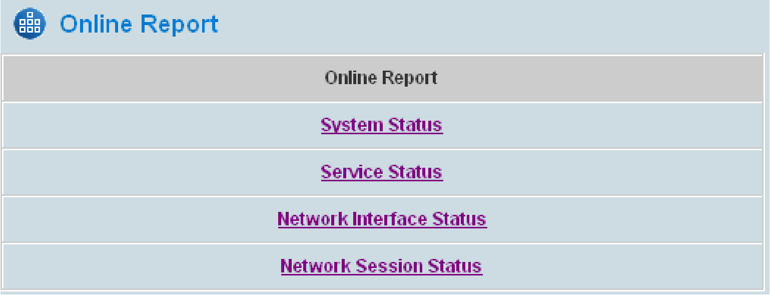
When enabled, the system can record connection details of each user accessing the Internet. In addition, the log data can be sent out to specified Syslog Server, Email Box or FTP Server.

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

- **Syslog Server**
  - **IP Address:** The IP address of the external Syslog server.
  - **Port:** The port number of the Syslog server setting.
- **Send Log (to Email & FTP) every:** The time interval to send the log data to Email Box and FTP server.
- **Email Box:** Send Log to Email Box.
  - **Sender’s Address:** The sender’s Email address.
  - **Receiver’s Address:** The receiver’s Email address.
  - **SMTP Server:** The IP address of the SMTP server.
  - **SMTP Auth Method:** Specify the authentication method used for the SMTP server.
  - **SMTP Setting Test:** For the first time, it is useful the SMTP setting by sending a test log.
- **FTP Server:** Send Log to FTP Server.
  - **IP Address:** The IP address of the external FTP server.
  - **Port:** The port number of the FTP server setting.
  - **Anonymous:** "Yes": send the log data to FTP server without entering username and password; "No": administrators must provide the username and password.
  - **Username:** The username of the FTP account.
  - **Password:** The password of the FTP account.
  - **FTP Setting Test:** For the first time, it is useful to test the FTP setting by sending a test log.

4.5.6 Online Report

This function provides real time on-line report of the DSA-6100 system including **System Status**, **Service Status**, **Network Interface Status** and **Network Session Status**.

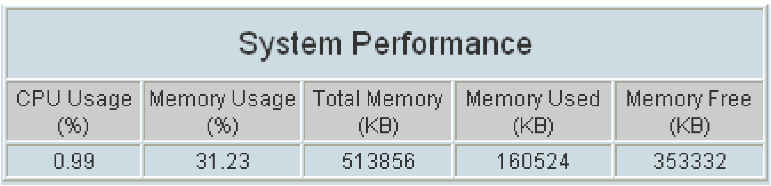


Online Report

Online Report
System Status
Service Status
Network Interface Status
Network Session Status

- **System Status**

  The page shows the current CPU and memory usage. This online report of DSA-6100 status consists of 5 fields: **CPU Usage**, **Memory Usage**, **Total Memory**, **Memory Used** and **Memory Free**.

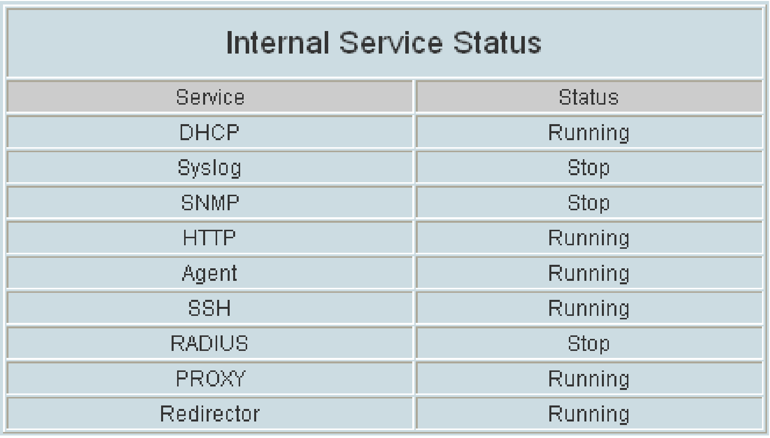


System Performance

CPU Usage (%)	Memory Usage (%)	Total Memory (KB)	Memory Used (KB)	Memory Free (KB)
0.99	31.23	513856	160524	353332

- **Service Status**

  This page shows the current status of the internal daemon service. The online report for network service status consists of 6 fields: **DHCP Server**, **Syslog Server**, **SNMP Server**, **HTTP Server**, **Agent**, **SSH Server**, **RADIUS Server**, **Proxy Server** and **Redirector Server**.

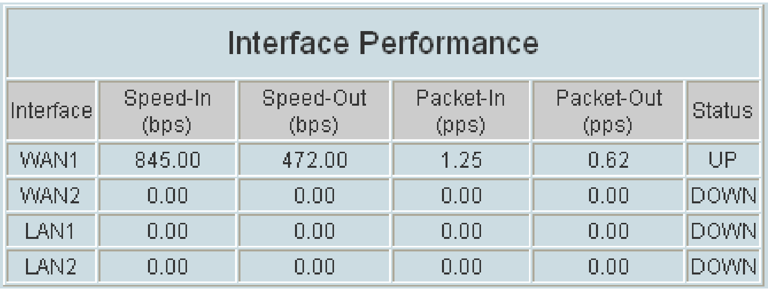


Internal Service Status

Service	Status
DHCP	Running
Syslog	Stop
SNMP	Stop
HTTP	Running
Agent	Running
SSH	Running
RADIUS	Stop
PROXY	Running
Redirector	Running

- **Network Interface Status**

  This page shows current throughput of every WAN and LAN interface. The online report for WAN and LAN status consists of 5 fields: **Interface**, **Speed-IN (bps)**, **Speed-OUT (bps)**, **Packet-IN (pps)** and **Packet-OUT (pps)**.

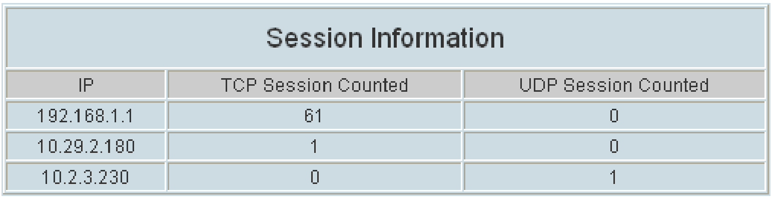


Interface Performance

Interface	Speed-In (bps)	Speed-Out (bps)	Packet-In (pps)	Packet-Out (pps)	Status
WAN1	845.00	472.00	1.25	0.62	UP
WAN2	0.00	0.00	0.00	0.00	DOWN
LAN1	0.00	0.00	0.00	0.00	DOWN
LAN2	0.00	0.00	0.00	0.00	DOWN

- **Network Session Status**

  This report tells how many connections (TCP and UDP) each IP address is using now. The online session information report consists of 3 fields: **IP**, **TCP session count** and **UDP session count**. This report tells how many connections each IP address uses currently.

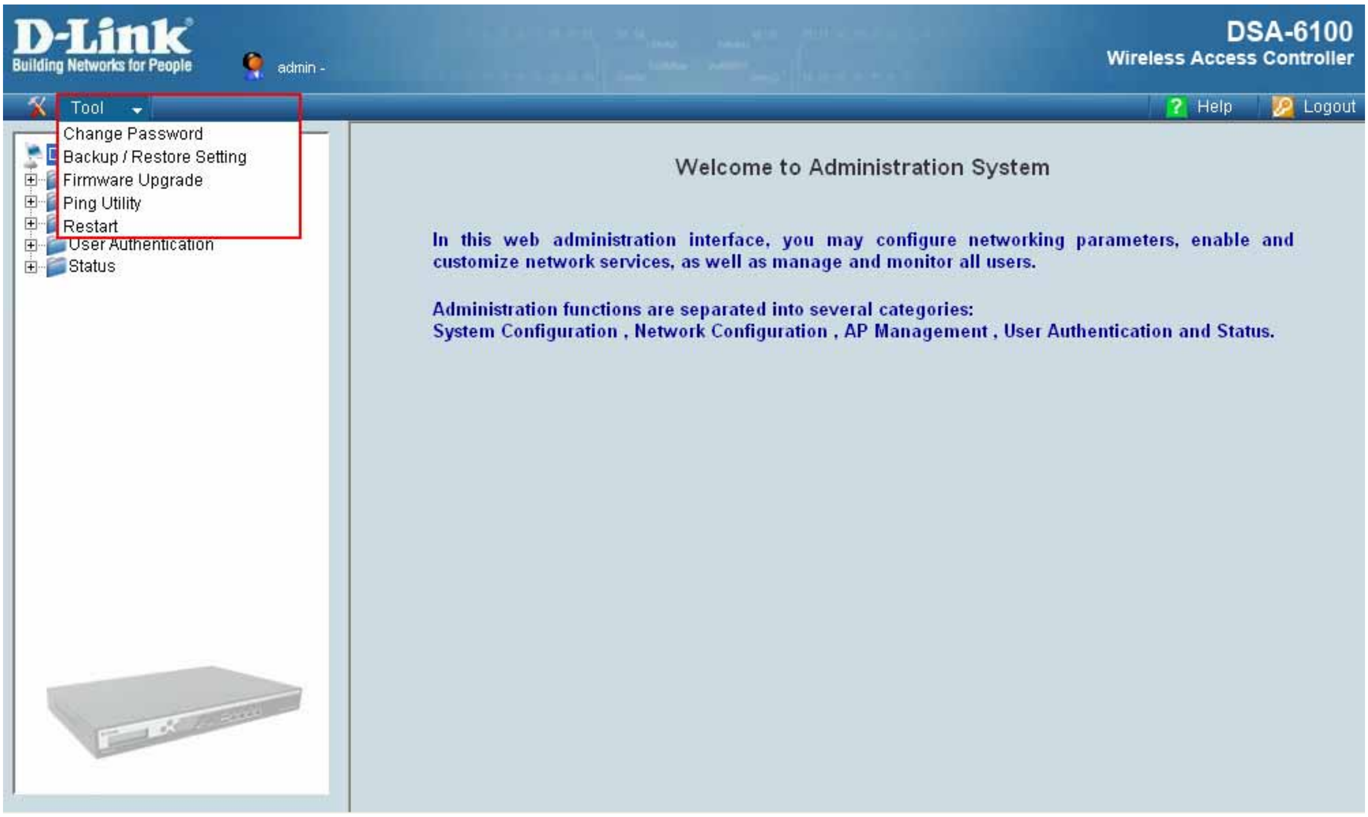


Session Information

IP	TCP Session Counted	UDP Session Counted
192.168.1.1	61	0
10.29.2.180	1	0
10.2.3.230	0	1

4.6 Tool

This section provides information on four utilities used for customizing and maintaining the system, including **Change Password**, **Backup/Restore Setting**, **Firmware Upgrade**, **Ping Utility** and **Restart**.



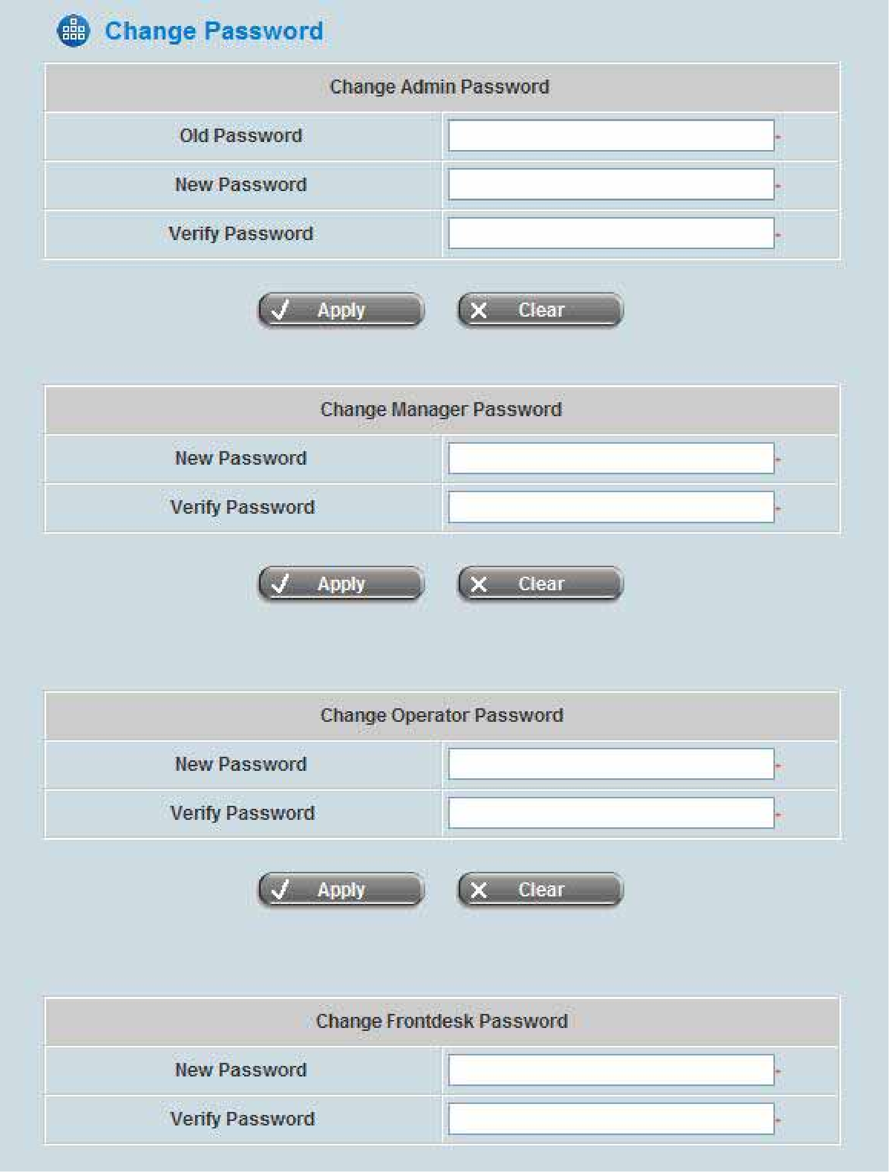
Welcome to Administration System

In this web administration interface, you may configure networking parameters, enable and customize network services, as well as manage and monitor all users.

Administration functions are separated into several categories:
System Configuration , Network Configuration , AP Management , User Authentication and Status.

4.6.1 Change Password

The administrator can change the passwords of the system. Enter the required fields marked with red asterisks as show in the picture below. Please enter the current password and then enter the new password twice to verify. Click ***Apply*** to activate the new passwords.



Change Password

Change Admin Password	
Old Password	*
New Password	*
Verify Password	*

Change Manager Password	
New Password	*
Verify Password	*

Change Operator Password	
New Password	*
Verify Password	*

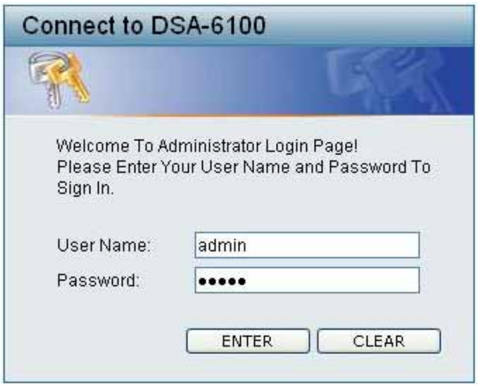
Change Frontdesk Password	
New Password	*
Verify Password	*

The DSA-6100 supports three types of account interface: **admin**, **manager**, **operator** or **frontdesk**. These account interfaces **are authenticated to access only certain configuration pages.** The default usernames and passwords are as follow:

Admin: The administrator can access all configuration pages of the DSA-6100.

User Name: **admin**

Password: **admin**

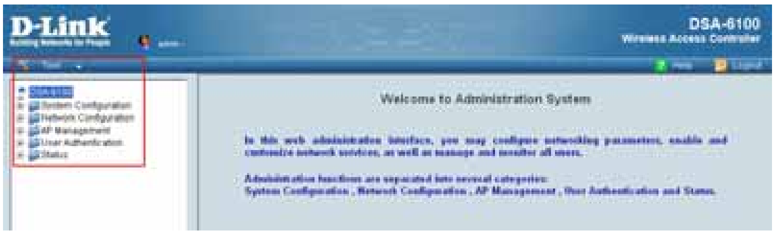


Connect to DSA-6100

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

User Name: admin

Password: •••••



Welcome to Administration System

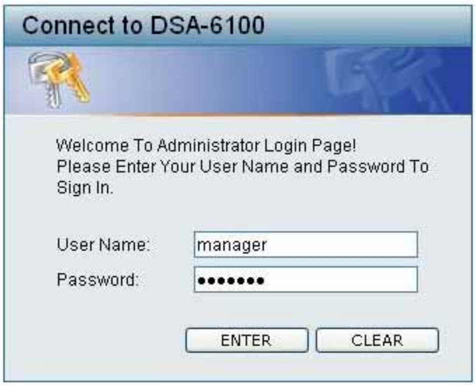
In this web administration interface, you may configure networking parameters, enable and customize network services, as well as manage and monitor all users.

Administration functions are separated into several categories:
System Configuration , Network Configuration , AP Management , User Authentication and Status.

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**

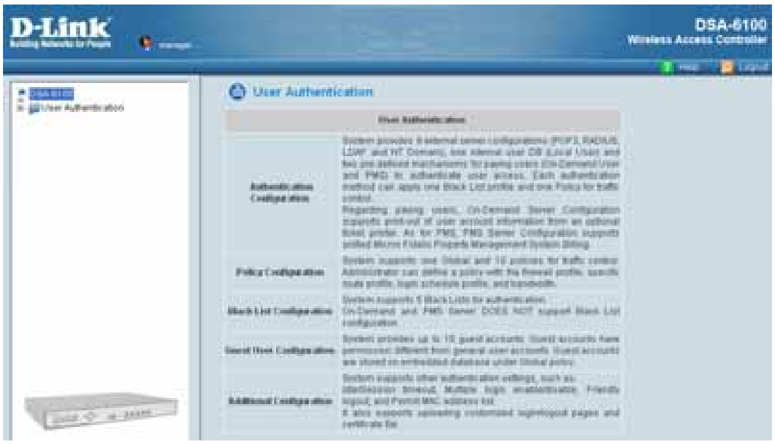


Connect to DSA-6100

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

User Name: manager

Password: •••••••



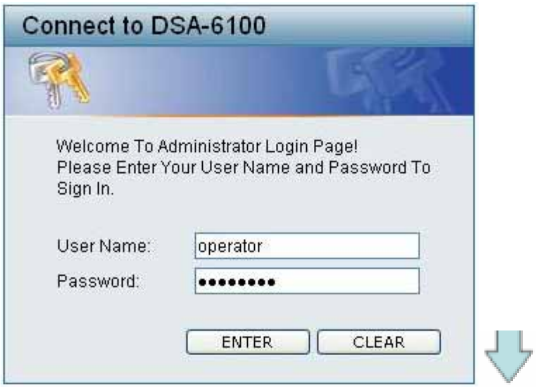
User Authentication

User Authentication	
Authentication Configuration	System provides 4 external server configurations (POP3, RADIUS, LDAP and NT Domain), one internal user DB (Local User) and two pre-defined mechanisms for paying users (On-Demand User and PMS) to authenticate user access. Each authentication method can apply one Black List profile and one Policy for traffic control. Regarding paying users, On-Demand Server Configuration supports print-out of user account information from an optional ticket printer. As for PMS, PMS Server Configuration supports unified Micro Fidelio Property Management System Billing.
Policy Configuration	System supports one Global and 10 policies for traffic control. Administrator can define a policy with the firewall profile, specific route profile, login schedule profile, and bandwidth.
Black List Configuration	System supports 5 Black Lists for authentication. On-Demand and PMS Server DOES NOT support Black List configuration.
Guest User Configuration	System provides up to 10 guest accounts. Guest accounts have permission different from general user accounts. Guest accounts are stored on embedded database under Global policy.
Additional Configuration	System supports other authentication settings, such as: Idle/Session timeout, Multiple login enable/disable, Friendly logout, and Permit MAC address list. It also supports uploading customized login/logout pages and certificate file.

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**

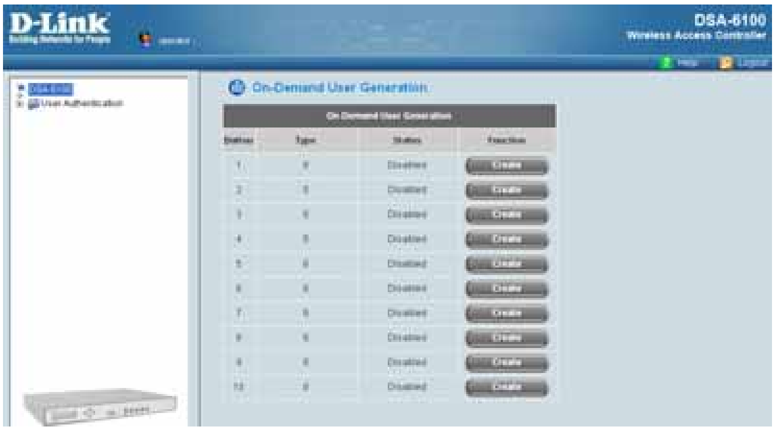


Connect to DSA-6100

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

User Name: operator

Password: ●●●●●●●●●



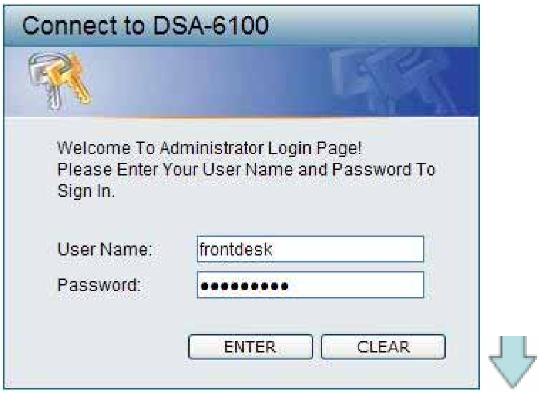
On-Demand User Generation

On Demand User Generation			
[illegible]	Type	Status	Function
1	[illegible]	Disabled	Create
2	[illegible]	Disabled	Create
3	[illegible]	Disabled	Create
4	[illegible]	Disabled	Create
5	[illegible]	Disabled	Create
6	[illegible]	Disabled	Create
7	[illegible]	Disabled	Create
8	[illegible]	Disabled	Create
9	[illegible]	Disabled	Create
10	[illegible]	Disabled	Create

Frontdesk: The frontdesk can only access the configuration page of ***PMS Frontdesk Tools*** to view the PMS users list or create and print out the new PMS users.

User Name: **frontdesk**

Password: **frontdesk**

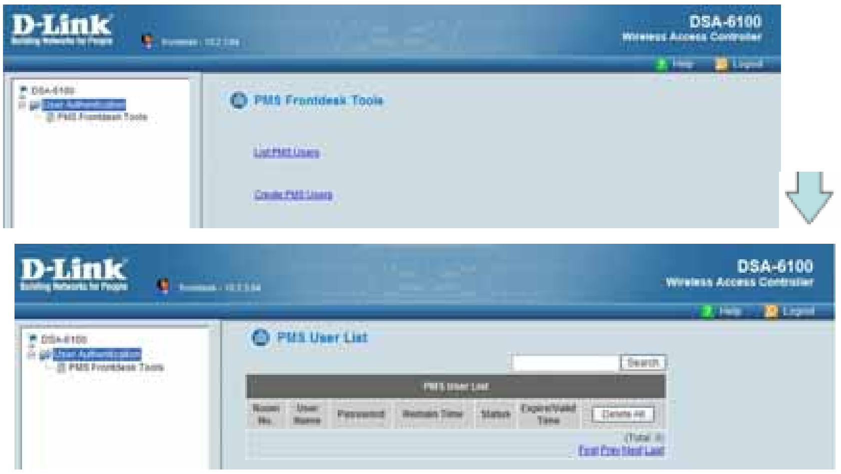


Connect to DSA-6100

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

User Name: frontdesk

Password: ●●●●●●●●●●



PMS Frontdesk Tools

List PMS Users

Create PMS Users

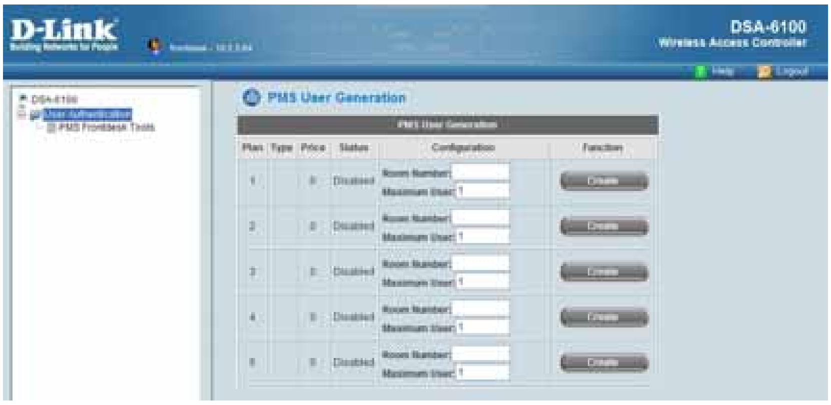
PMS User List

Search

PMS User List						
Room No.	User Name	Password	Remain Time	Status	Expire/Valid Time	Delete All

(Total: 0)
First Prev Next Last

PMS User List



PMS User Generation

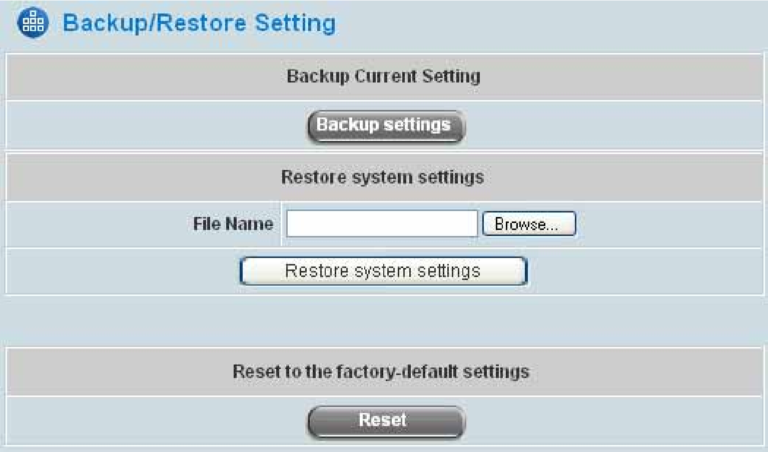
Plan	Type	Price	Status	Configuration	Function
1		0	Disabled	Room Number: Maximum User: 1	Create
2		0	Disabled	Room Number: Maximum User: 1	Create
3		0	Disabled	Room Number: Maximum User: 1	Create
4		0	Disabled	Room Number: Maximum User: 1	Create
5		0	Disabled	Room Number: Maximum User: 1	Create

PMS User Creation

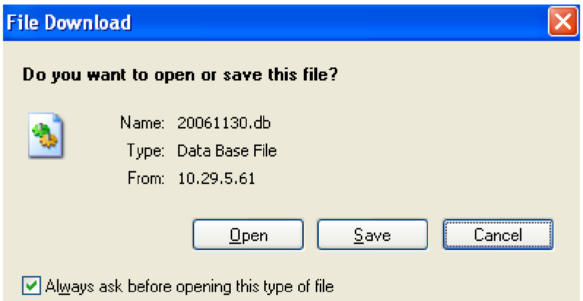
Caution: *If the administrator’s password is lost, the administrator’s password can still be changed through the text mode management interface on the console port.*

4.6.2 Backup/Restore Setting

This function is used to backup/restore the DSA-6100 settings. The DSA-6100 can also be restored to the factory default settings using this function.



- **Backup Current Setting:** Click ***Backup Settings*** to save the current system configuration 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.

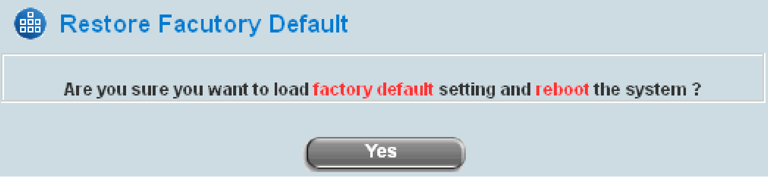


Do you want to open or save this file?

Name: 20061130.db
Type: Data Base File
From: 10.29.5.61

- **Restore System Setting:** Click ***Browse*** to search for a .db database backup file created by the DSA-6100 and click ***Restore System Setting*** to restore to the same settings at the time the backup file is created.

- **Reset to the Factory-Default Setting:** Click ***Yes*** to load the factory default settings of the DSA-6100.

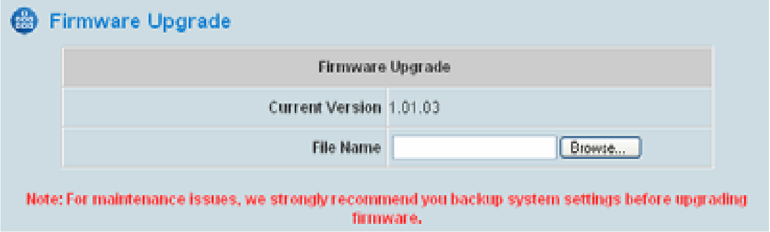


Are you sure you want to load factory default setting and reboot the system ?

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

4.6.3 Firmware Upgrade

The administrator can download the latest firmware from the website and upgrade the system. Click ***Browse*** to search for the firmware file and click ***Apply*** to go on with the firmware upgrade process. It may take a few minutes before the upgrade process completes. Upon completion, the system will need to be restarted for the firmware to take effect.



Firmware Upgrade

Firmware Upgrade	
Current Version	1.01.03
File Name	Browse...

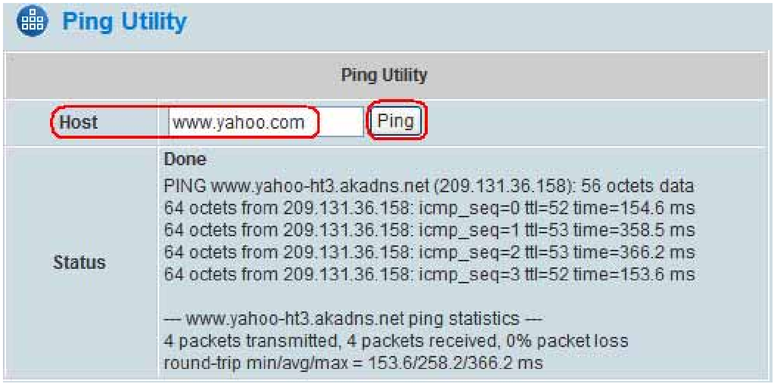
Note: For maintenance issues, we strongly recommend you backup system settings before upgrading firmware.

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.

4.6.4 Ping Utility

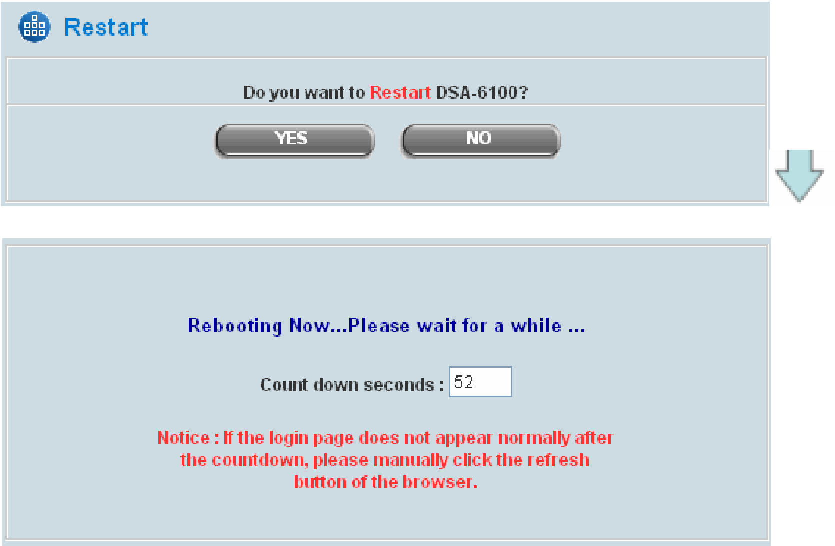
This utility is for administrator's convenience to easily test the network connection on the DSA-6100 administration interface. Enter IP address or domain name in **Host** field and press ***Ping*** button. The results will show whether the connection is successful.



```
Done
PING www.yahoo-ht3.akadns.net (209.131.36.158): 56 octets data
64 octets from 209.131.36.158: icmp_seq=0 ttl=52 time=154.6 ms
64 octets from 209.131.36.158: icmp_seq=1 ttl=53 time=358.5 ms
64 octets from 209.131.36.158: icmp_seq=2 ttl=53 time=366.2 ms
64 octets from 209.131.36.158: icmp_seq=3 ttl=52 time=153.6 ms

--- www.yahoo-ht3.akadns.net ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 153.6/258.2/366.2 ms
```

4.6.5 Restart

This function allows the administrator to safely restart the DSA-6100. The process should take about three minutes. Click ***YES*** to restart the system; click ***NO*** to go back to the previous screen. Please wait for countdown timer to finish before accessing the system management webpage again. If turning off the power is necessary, restart the DSA-6100 and wait for it to complete the restart process before turning off.



Do you want to Restart DSA-6100?

Rebooting Now...Please wait for a while ...

Count down seconds : 52

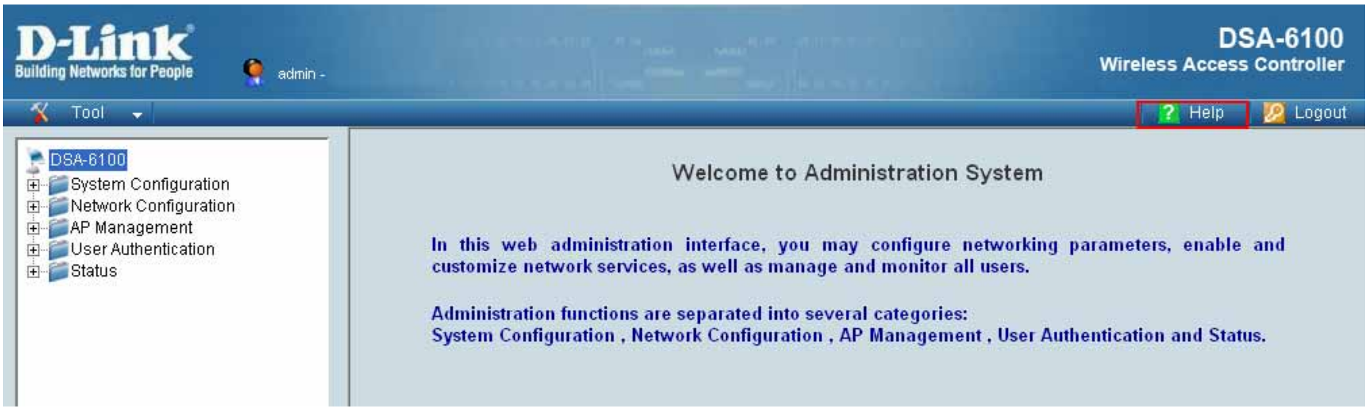
Notice : If the login page does not appear normally after the countdown, please manually click the refresh button of the browser.

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

4.7 Help

The **Help** button is at the upper right corner of the DSA-6100 display screen.

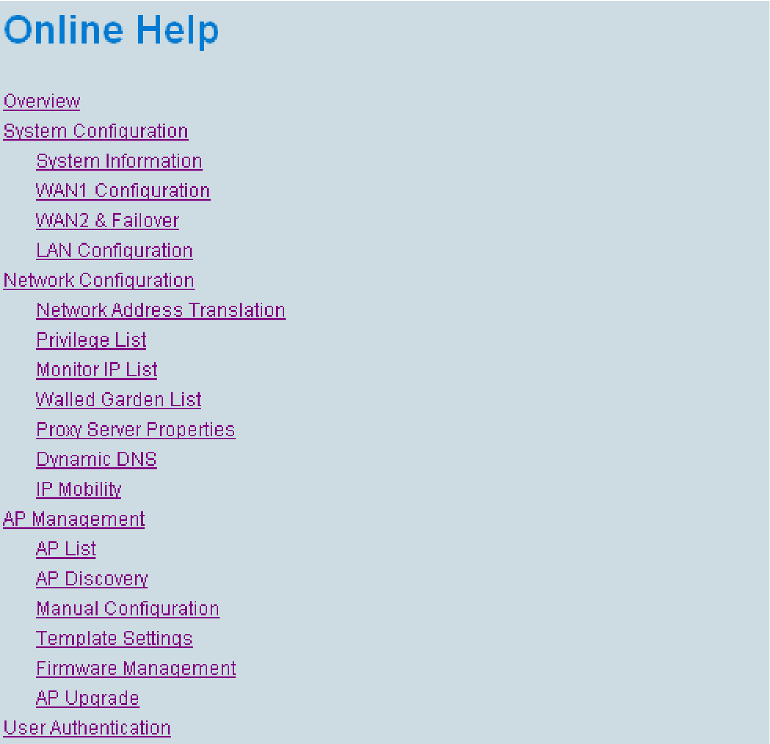
Click ***Help*** for the **Online Help** window, and then click the hyperlink of the relevant information required.



Welcome to Administration System

In this web administration interface, you may configure networking parameters, enable and customize network services, as well as manage and monitor all users.

Administration functions are separated into several categories:
System Configuration , Network Configuration , AP Management , User Authentication and Status.



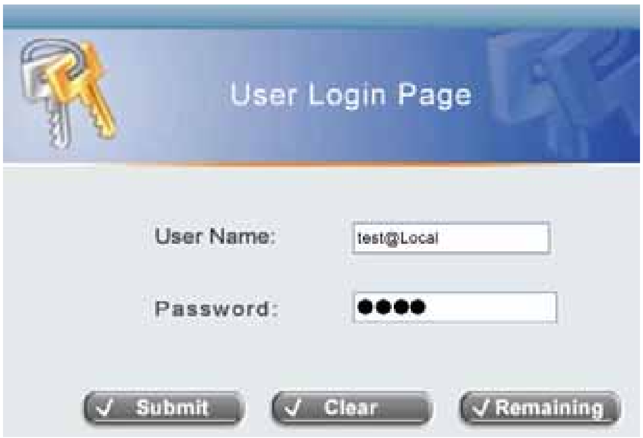
Online Help

Overview
System Configuration
System Information
WAN1 Configuration
WAN2 & Failover
LAN Configuration
Network Configuration
Network Address Translation
Privilege List
Monitor IP List
Walled Garden List
Proxy Server Properties
Dynamic DNS
IP Mobility
AP Management
AP List
AP Discovery
Manual Configuration
Template Settings
Firmware Management
AP Upgrade
User Authentication

Appendix A. External Network Access

Upon completing this process, the DSA-6100 will be connected to a managed network in a controlled network access environment.

1. Connect a client's device such as a PC to the Public LAN port of the DSA-6100. The device will get an IP address automatically via DHCP. Next, open a web browser and access any URL. The default **User Login Page** will appear. Enter the ***User Name*** and ***Password*** created in the local user account database by the Configuration Wizard, then click ***Submit*** (e.g. ***test@Local*** for the username and ***test*** for the password).

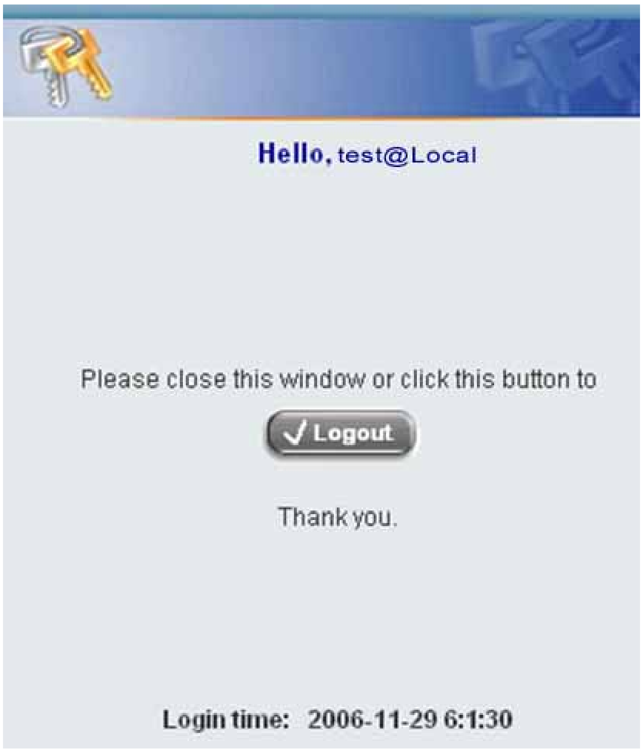


User Login Page

User Name: test@Local

Password: ●●●●

2. If the Login page appears, it means the DSA-6100 has been installed and configured successfully. The client user can now browse the network or surf the Internet!



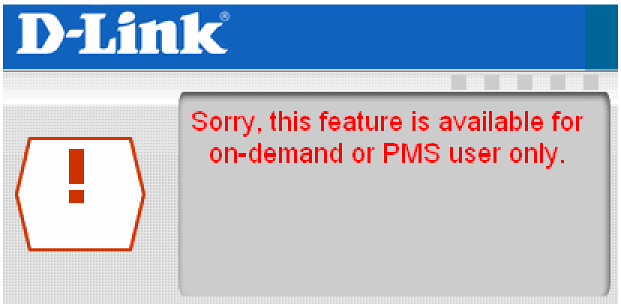
Hello, test@Local

Please close this window or click this button to

Thank you.

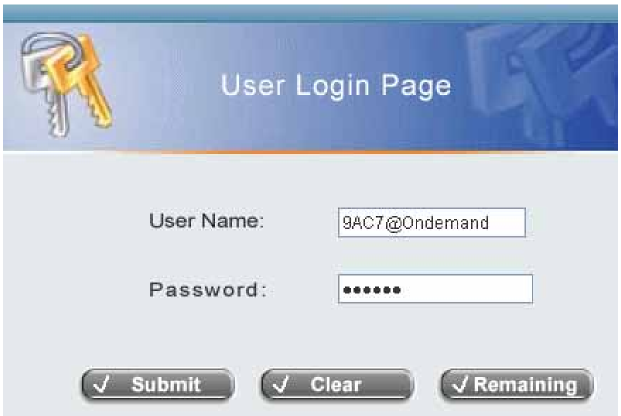
Login time: 2006-11-29 6:1:30

3. If a message **"Sorry, this feature is available for on-demand user only"** appears instead, it means a wrong button has been clicked. **"*Remaining*"** is only for on-demand users. Please click the ***Submit*** button instead.



Sorry, this feature is available for on-demand or PMS user only.

4. An on-demand user can enter the username and password in the **"User Login Page"** and click ***Remaining*** button to know the remaining time or data quota of the account.

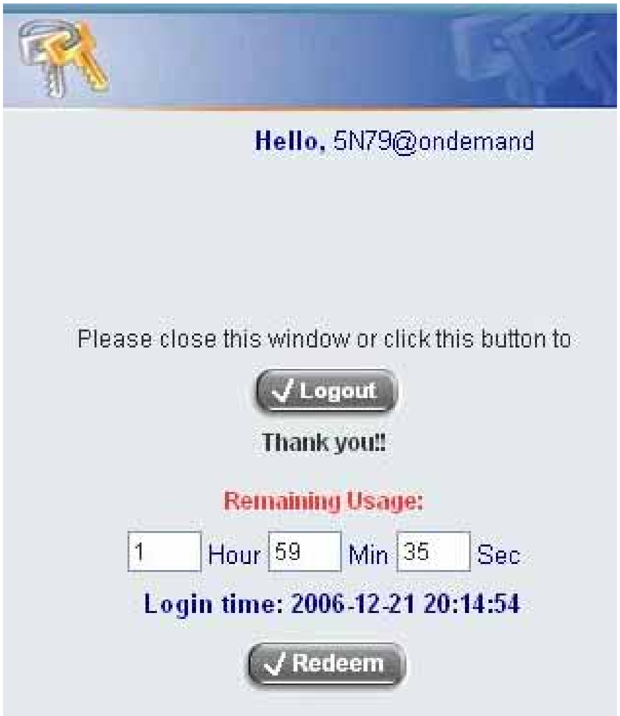


User Login Page

User Name: 9AC7@Ondemand

Password: ••••••

5. When an on-demand user logs in successfully, the successful **Login** screen will appear, which differs from the usual user's login successfully screen, as it contains an extra line showing **"Remaining usage"** and a **"Redeem"** button.
   - **Remaining usage:** Shows the remainder usage time that the on-demand user can surf the Internet.
   - **Redeem:** When the remaining time or data size is insufficient, the user will have to pay to add credit at the counter, where the user will then get a new username and password. After clicking the ***Redeem*** button, the following screen will show up.



Hello, 5N79@ondemand

Please close this window or click this button to

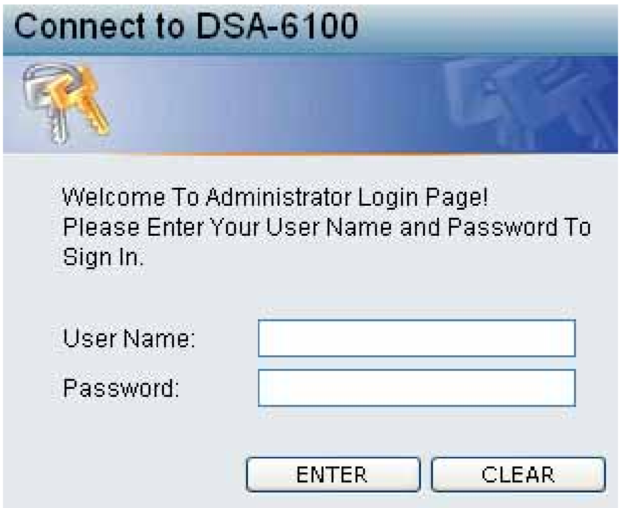
Thank you!!

Remaining Usage:

1 Hour 59 Min 35 Sec

Login time: 2006-12-21 20:14:54

Enter the new username and password obtained, and click the ***Redeem*** button to merge the two accounts to add up the available usage time and data size by the system. The total available usage time and data size after adding credit will then be shown.



Connect to DSA-6100

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

User Name:

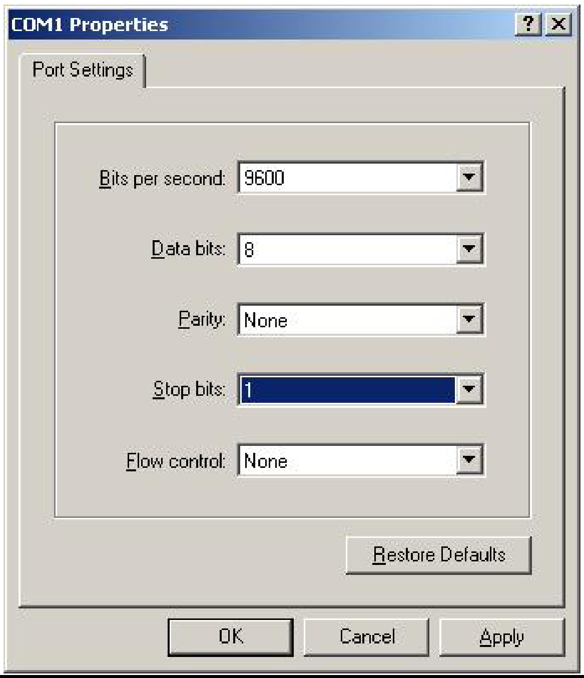
Password:

Caution: *The maximum session time/data transfer is 24305 days/2003 Mbyte. If the redeem amount exceeds this number, the system will automatically reject the redeem process.*

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-6100, 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.



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

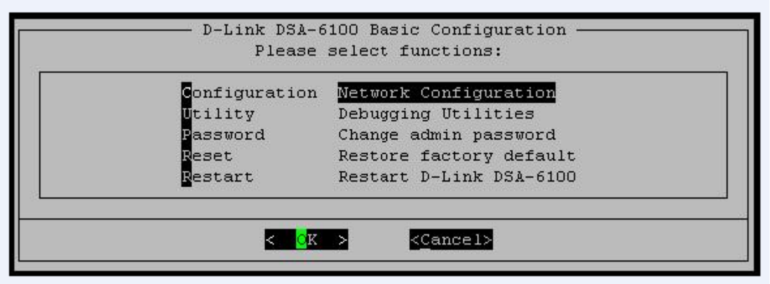
Parity: None

Stop bits: 1

Flow control: None

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

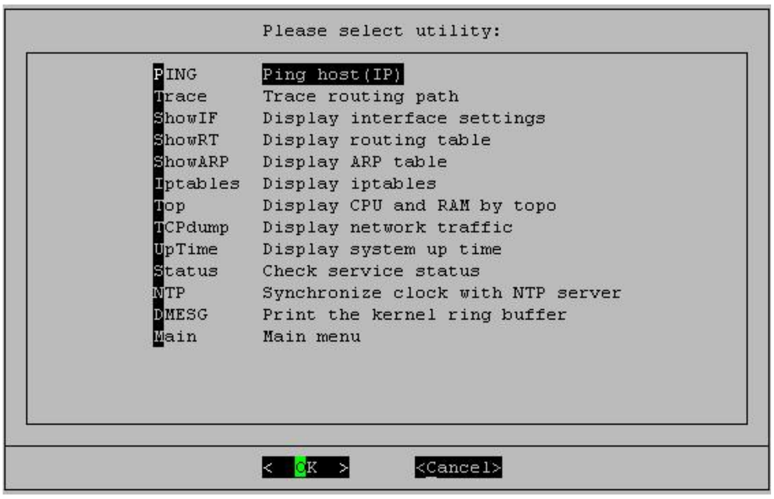
3. Once the console port of the DSA-6100 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys so that the terminal simulation program will send out some messages, and the welcome screen or the main menu will 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.



```
D-Link DSA-6100 Basic Configuration
      Please select functions:

Configuration   Network Configuration
Utility         Debugging Utilities
Password        Change admin password
Reset           Restore factory default
Restart         Restart D-Link DSA-6100

        <  OK  >        <Cancel>
```

- **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:



```
                    Please select utility:

            PING      Ping host(IP)
            Trace     Trace routing path
            ShowIF    Display interface settings
            ShowRT    Display routing table
            ShowARP   Display ARP table
            Iptables  Display iptables
            Top       Display CPU and RAM by topo
            TCPdump   Display network traffic
            UpTime    Display system up time
            Status    Check service status
            NTP       Synchronize clock with NTP server
            DMESG     Print the kernel ring buffer
            Main      Main menu

                    <  OK  >      <Cancel>
```

- Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
- Trace routing path: Trace and inquire the routing path to a specific target.
- Display interface settings: 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 live time: The system live time (time for system being turn on) is displayed.
- Check service status: Check and display the status of the system.
- Set device into “safe mode”: 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-6100 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.

- **Change admin password**

  Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, there is no need to enter that administrator's password to access the console management interface. When connecting the system via SSH, however, the username and password will be needed.

  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. Even if the password is forgotten and the management interface cannot be accessed from the web or the remote end of the SSH, the null modem can still be used to connect the console management interface where the administrator's password can then be reset.

Caution: *Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, it is recommended that you immediately change the DSA-6100 Admin username and password after logging into the system for the first time.*

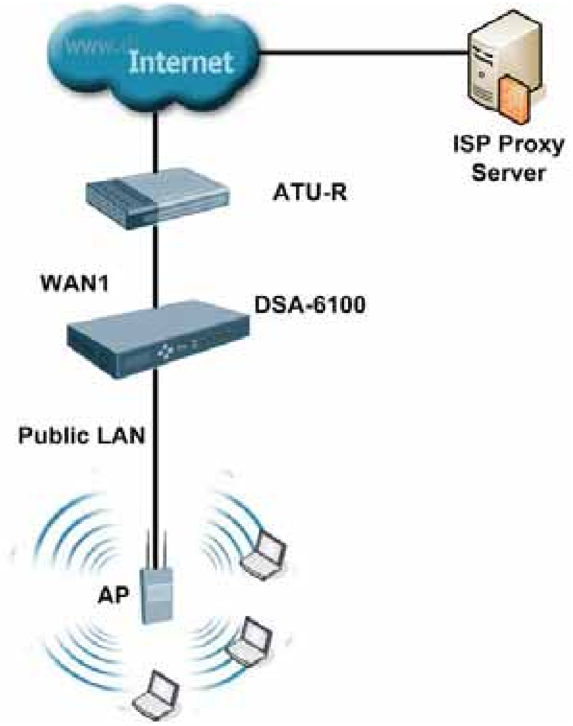
- **Reload factory default**

  Choose this option to reset the system configuration to the factory default settings.
- **Restart DSA-6100**

Appendix C. Proxy Configuration

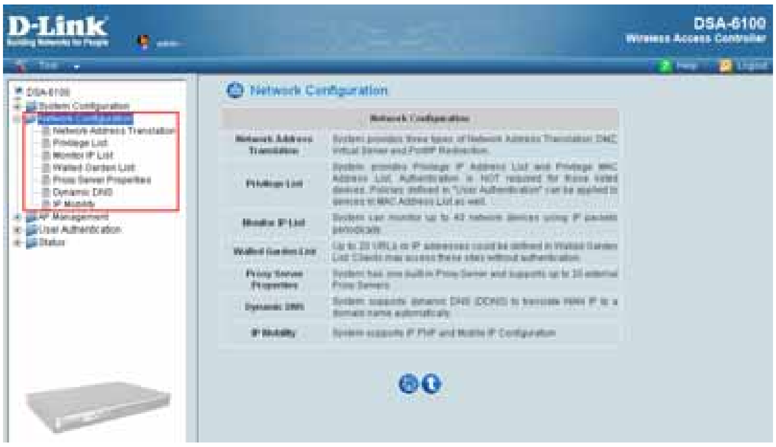
For Hotspot

A hot spot is a wireless LAN node provides Internet connection and virtual private network access from a given location, such as a coffee shop, hotel, or a public place where Wi-Fi service is made available for mobile and users. A hotspot is usually implemented without sophisticated network architecture via proxy servers from Internet Service Providers.



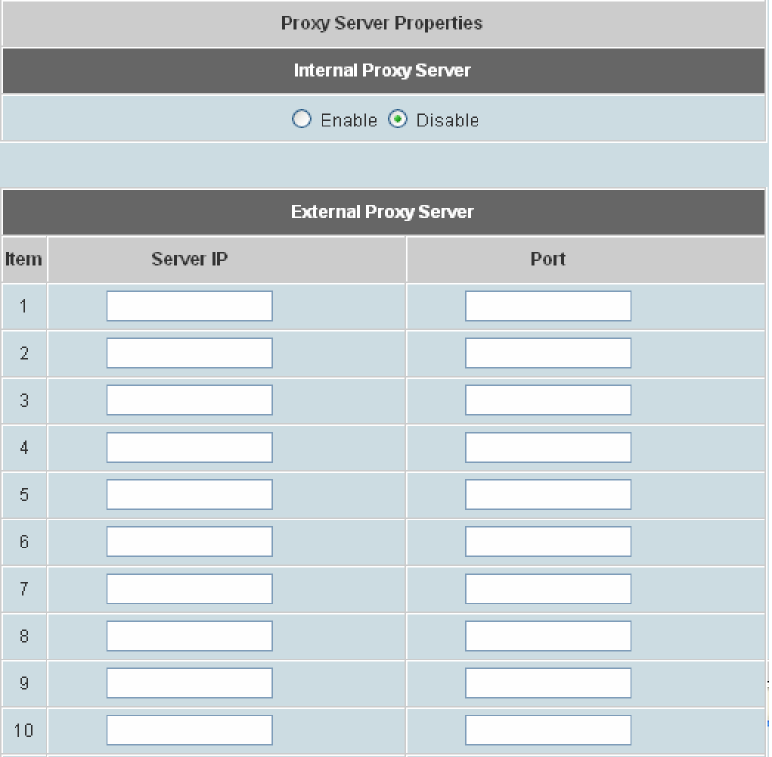
In a hotspot environment, users usually enable their proxy setting at their browsers, such as IE and Firefox. Likewise, the DSA-6100 also needs to set some proxy configuration in the Gateway. Follow these steps to complete the proxy configuration：

1. Login Gateway by using “***admin***”.
2. Click the ***Network Configuration from top menu*** and the homepage of the ***Network Configuration*** will appear.



Network Configuration	
Network Address Translation	System provides three types of Network Address Translation: DMZ, Virtual Server and Port/IP Redirection.
Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. Authentication is NOT required for those listed devices. Policies defined in "User Authentication" can be applied to devices in MAC Address List as well.
Monitor IP List	System can monitor up to 40 network devices using IP packets periodically.
Walled Garden List	Up to 20 URLs or IP addresses could be defined in Walled Garden List. Clients may access these sites without authentication.
Proxy Server Properties	System has one built-in Proxy Server and supports up to 10 external Proxy Servers.
Dynamic DNS	System supports dynamic DNS (DDNS) to translate WAN IP to a domain name automatically.
IP Mobility	System supports IP PNP and Mobile IP Configuration.

3. Click the ***Proxy Server Properties*** from left menu and the homepage of the **Proxy Server Properties** will appear.



Proxy Server Properties

Internal Proxy Server

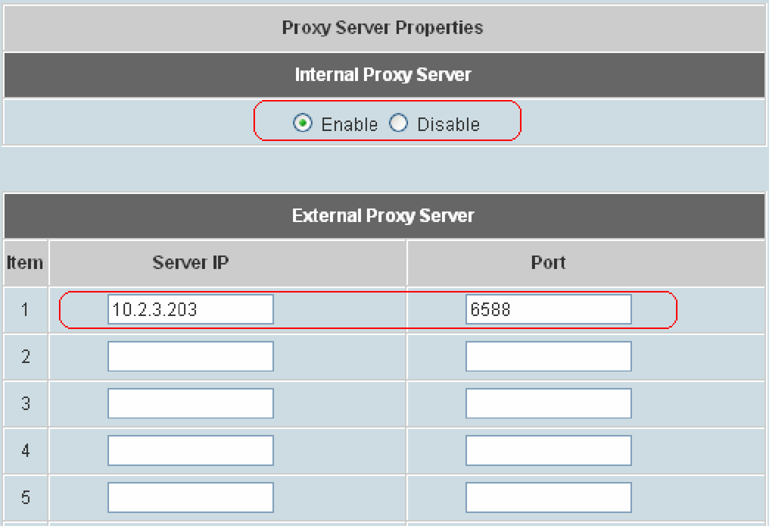
○ Enable ● Disable

External Proxy Server

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

4. Add the ISP's proxy Server IP and Port into ***External Proxy Server*** Setting.

5. ***Enable Built-in Proxy Server*** in ***Internal Proxy Server*** Setting.



Proxy Server Properties

Internal Proxy Server

● Enable ○ Disable

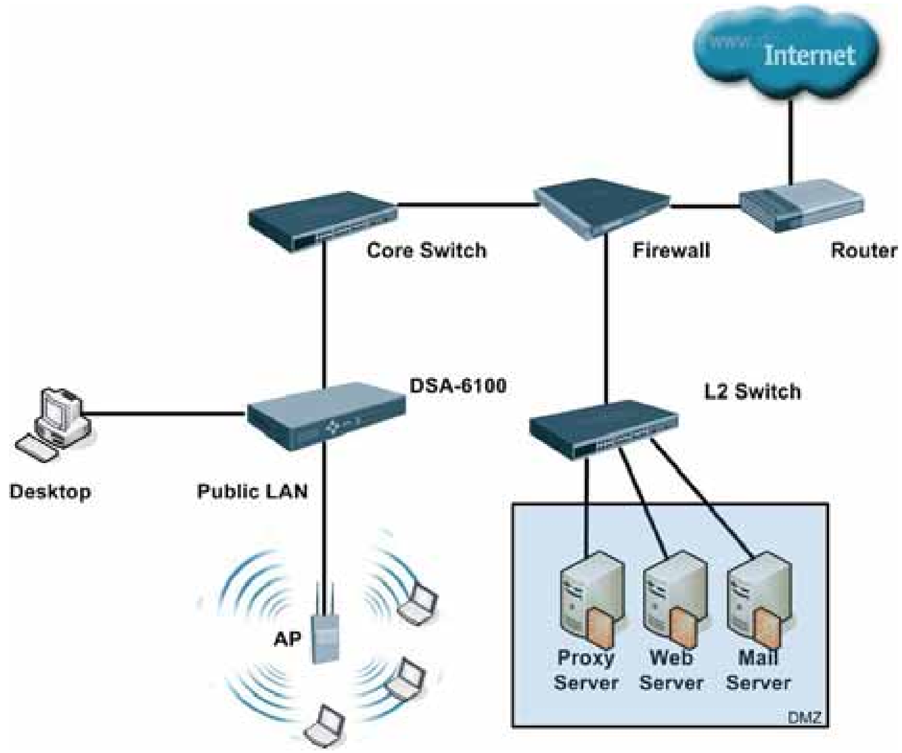
External Proxy Server

Item	Server IP	Port
1	10.2.3.203	6588
2		
3		
4		
5		

6. Click ***Apply*** to save the settings***.***

For Enterprise

Enterprises usually isolate their intranet and internet by using more elaborated network architecture. Many enterprises have their own proxy server which is usually located at the intranet or DMZ under firewall protection.



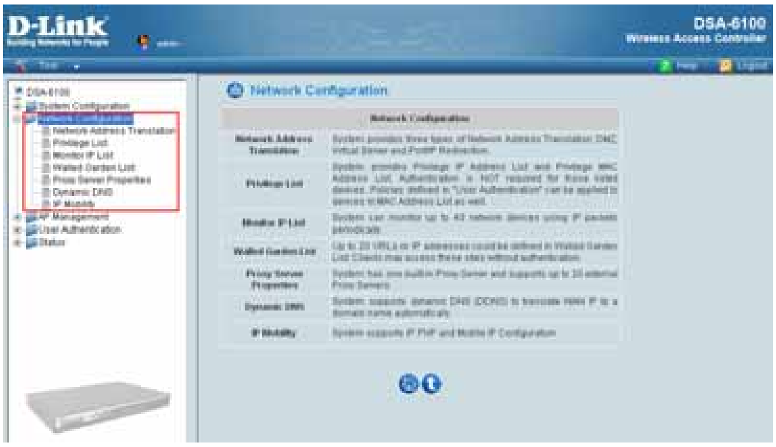
In enterprises, network managers or MIS staff may often ask their users to enable their proxy setting of the browsers such as IE and Firefox to reduce the internet access loading. Therefore some proxy configurations in the Gateway need to be set.

> ***Caution***：*Some enterprises will automatically redirect packets to proxy server by using core switch or Layer 7 devices. By the way, the clients don't need to enable their browsers' proxy settings, and administrators don't need to set any proxy configuration in the Gateway.*

Please follow the steps to complete the proxy configuration：

▪ Gateway setting

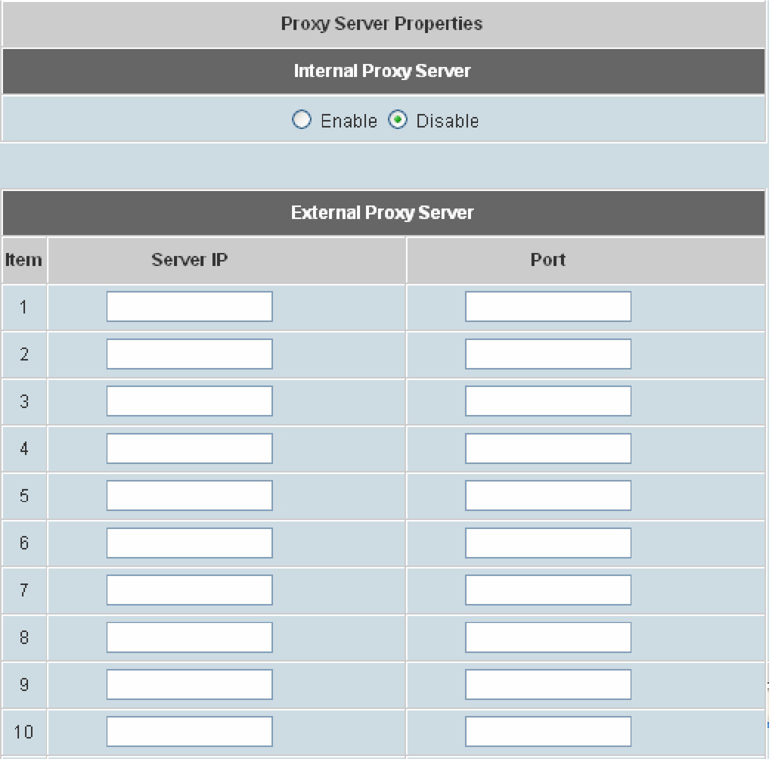
1. Login Gateway by using "***admin***".
2. Click the ***Network Configuration from top menu*** and the homepage of the ***Network Configuration*** will appear.



Network Configuration

Network Configuration	
Network Address Translation	System provides three types of Network Address Translation: DMZ, Virtual Server and Port/IP Redirection.
Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. Authentication is NOT required for those listed devices. Policies defined in "User Authentication" can be applied to devices in MAC Address List as well.
Monitor IP List	System can monitor up to 40 network devices using IP packets periodically.
Walled Garden List	Up to 20 URLs or IP addresses could be defined in Walled Garden List. Clients may access these sites without authentication.
Proxy Server Properties	System has one built-in Proxy Server and supports up to 10 external Proxy Servers.
Dynamic DNS	System supports dynamic DNS (DDNS) to translate WAN IP to a domain name automatically.
IP Mobility	System supports IP PNP and Mobile IP Configuration.

3. Click the ***Proxy Server Properties*** from left menu and the homepage of the ***Proxy Server Properties*** will appear.



Proxy Server Properties

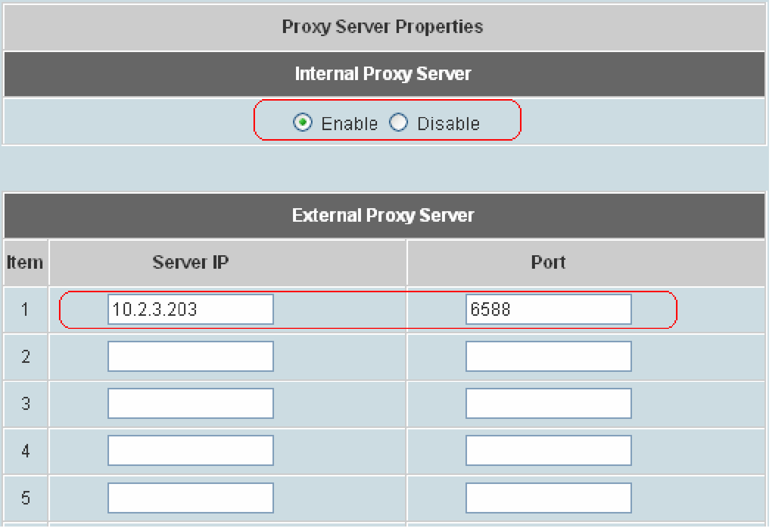
Internal Proxy Server

○ Enable ● Disable

External Proxy Server

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

4. Add your proxy Server IP and Port into ***External Proxy Server*** Setting.
5. ***Disable Built-in Proxy Server*** in ***Internal Proxy Server*** Setting.



Proxy Server Properties

Internal Proxy Server

● Enable ○ Disable

External Proxy Server

Item	Server IP	Port
1	10.2.3.203	6588
2		
3		
4		
5		

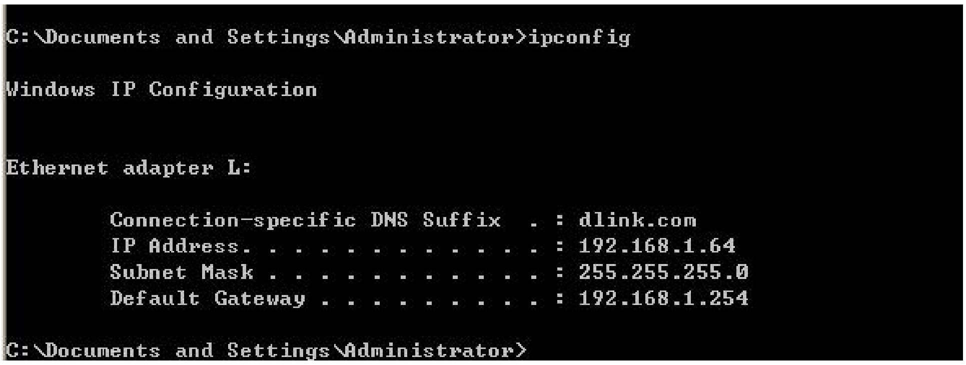
6. Click ***Apply*** to save the settings**.**

Warning：*If your proxy server is disabled, it will make the user authentication operation abnormal. When users open the browser, the login page will not appear because the proxy server is down. Please make sure your proxy server is always available.*

▪ Client setting

Adding a default gateway IP address into proxy exception information is a necessity for clients so that the user login successful page can show up normally.

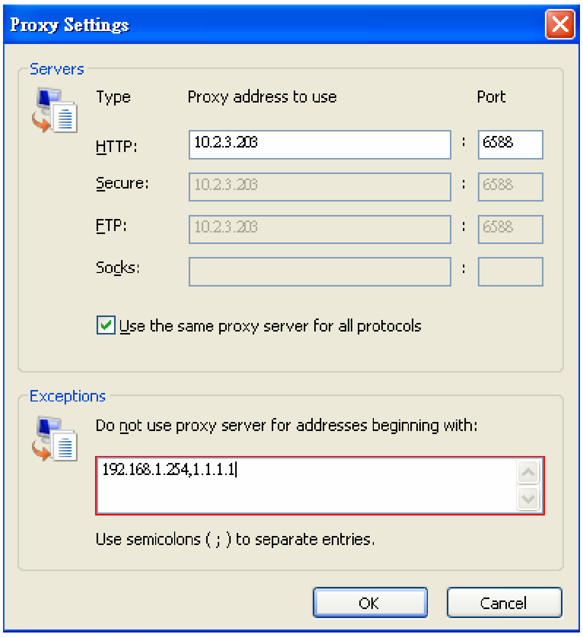
1. Use the command "***ipconfig***" to obtain the Default Gateway IP Address.



```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter L:

        Connection-specific DNS Suffix  . : dlink.com
        IP Address. . . . . . . . . . . . : 192.168.1.64
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254

C:\Documents and Settings\Administrator>
```

2. Open the browser to add the ***default gateway IP address (e.g. 192.168.1.254)*** and ***logout page IP address "1.1.1.1"*** into the proxy exception information.

- **For Internet Explorer**



Proxy Settings

Servers

Type	Proxy address to use		Port
HTTP:	10.2.3.203	:	6588
Secure:	10.2.3.203	:	6588
FTP:	10.2.3.203	:	6588
Socks:		:	

☑ Use the same proxy server for all protocols

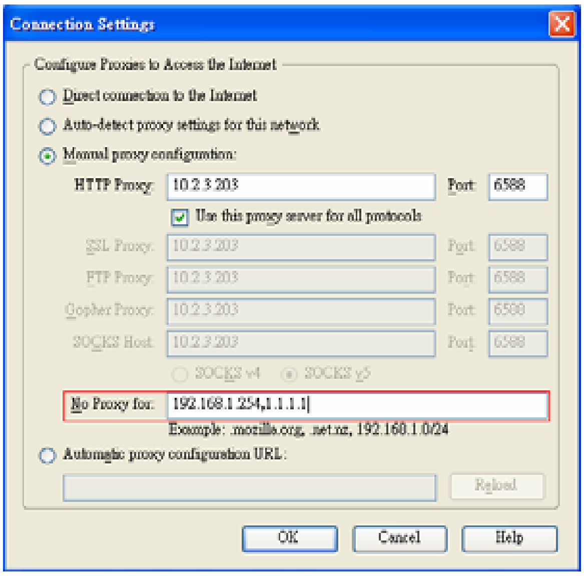
Exceptions

Do not use proxy server for addresses beginning with:

192.168.1.254,1.1.1.1

Use semicolons (;) to separate entries.

- **For Mozilla Firefox**



Connection Settings

Configure Proxies to Access the Internet

○ Direct connection to the Internet

○ Auto-detect proxy settings for this network

● Manual proxy configuration:

HTTP Proxy:	10.2.3.203	Port:	6588
	☑ Use this proxy server for all protocols		
SSL Proxy:	10.2.3.203	Port:	6588
FTP Proxy:	10.2.3.203	Port:	6588
Gopher Proxy:	10.2.3.203	Port:	6588
SOCKS Host:	10.2.3.203	Port:	6588

○ SOCKS v4 ● SOCKS v5

No Proxy for: 192.168.1.254,1.1.1.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

Appendix D. Certificate Setting 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 encounters problem occurs 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-6100, 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-6100.

▪ 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-6100 and export it to the DSA-6100.

Note: *If the DSA-6100 is installed in a company, the administrator can create a certificate using some software instead of purchasing a public trusted certificate.*

1) Certificate setting for the company without Certificate Authority

For a company that does not have it own Certificate Authority (CA), the administrators should first create a certificate either by applying for a trusted one or by some certificate software. Second, the administrators should use some trusted media to install this certificate (as trusted CA) in each employee's computer. In the meantime, export this certificate to the DSA-6100.

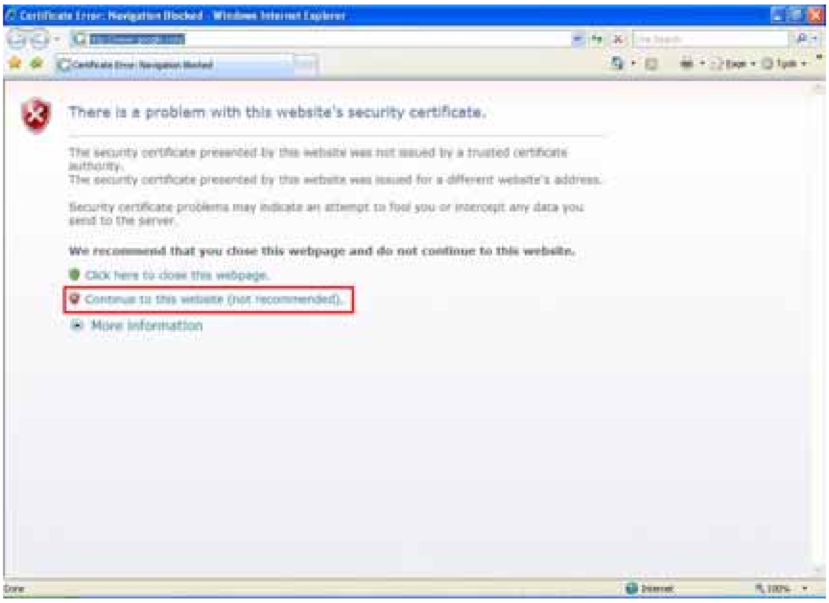
In certain condition, the company without Certificate Authority can follow the steps below to avoid error message. When in the LAN environment of the office rather than when in wireless environment, administrators may already have recognized certificates in the system, which CA must be verified as secured.

2) Certificate setting for Internet Explorer 7

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

a. 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"***.



Certificate Error: Navigation Blocked - Windows Internet Explorer

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

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

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

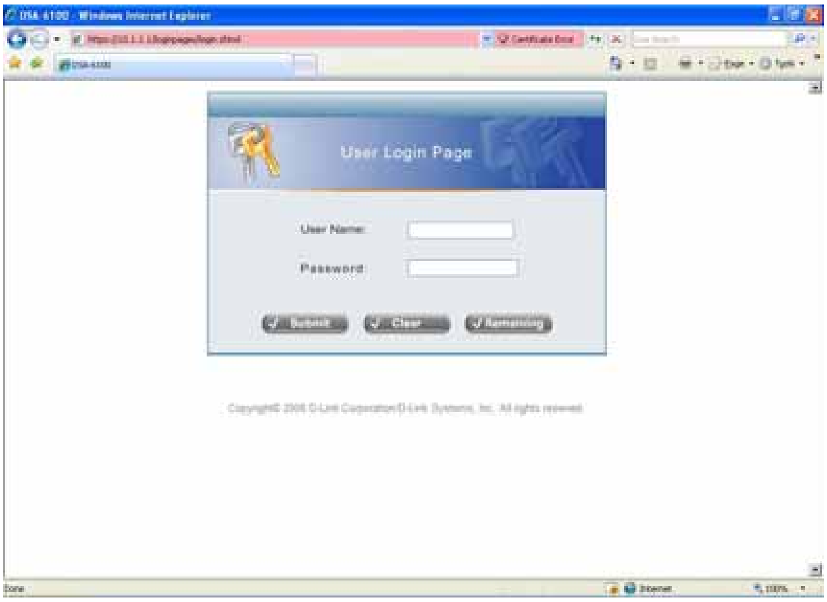
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

b. The default User Login Page will appear and the users can then login normally.



DSA-6100 - Windows Internet Explorer

User Login Page

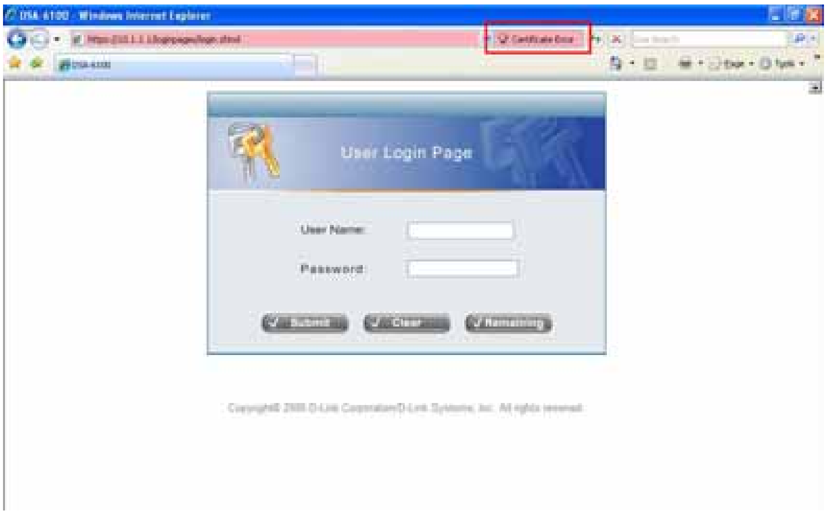
User Name:

Password:

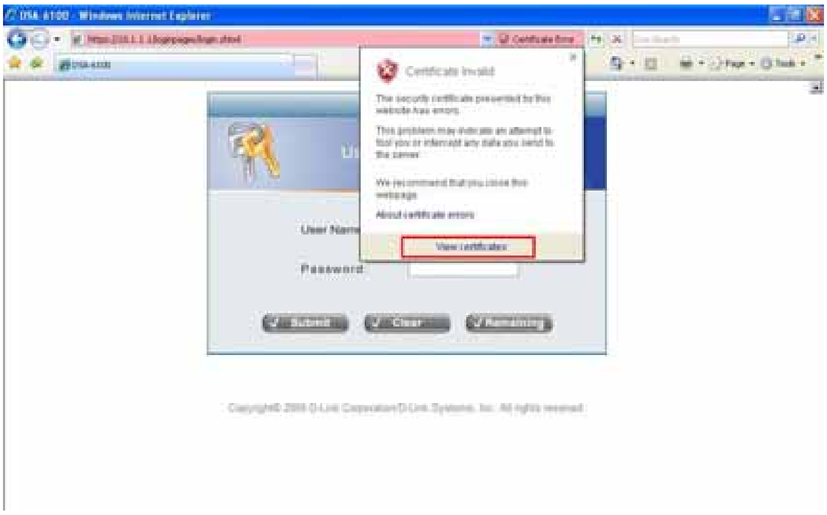
Copyright© 2008 D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

a. When the User Login page appears, click ***“Certificate Error”*** at the top.



b. Click ***“View Certificate”***.

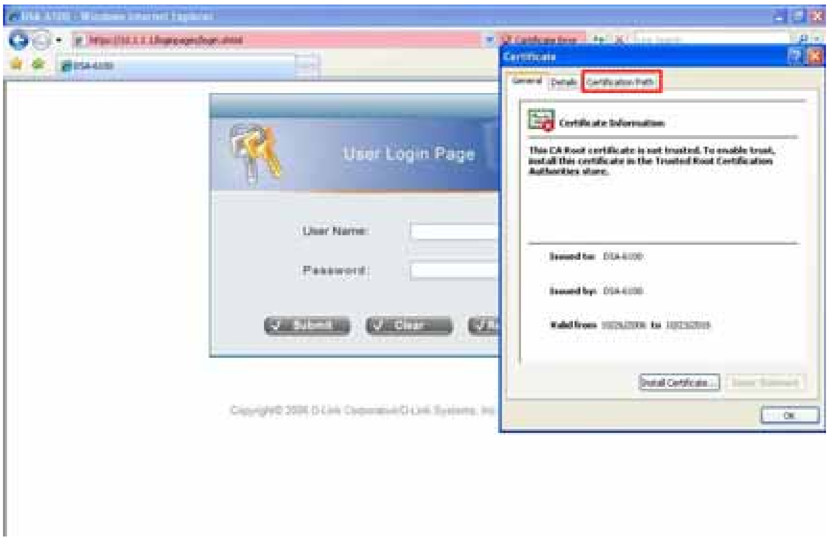


The security certificate presented by this website has errors.

This problem may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

c. Click ***“Certification path”***.



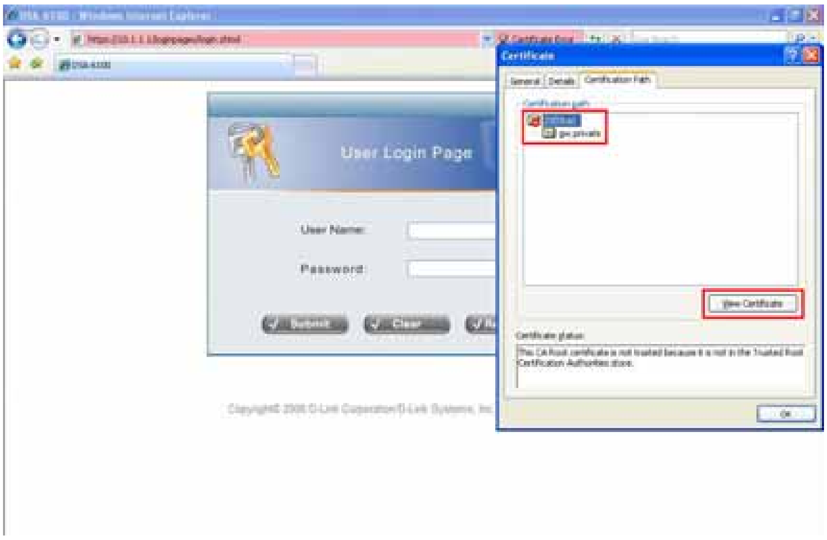
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: DSA-6100

Issued by: DSA-6100

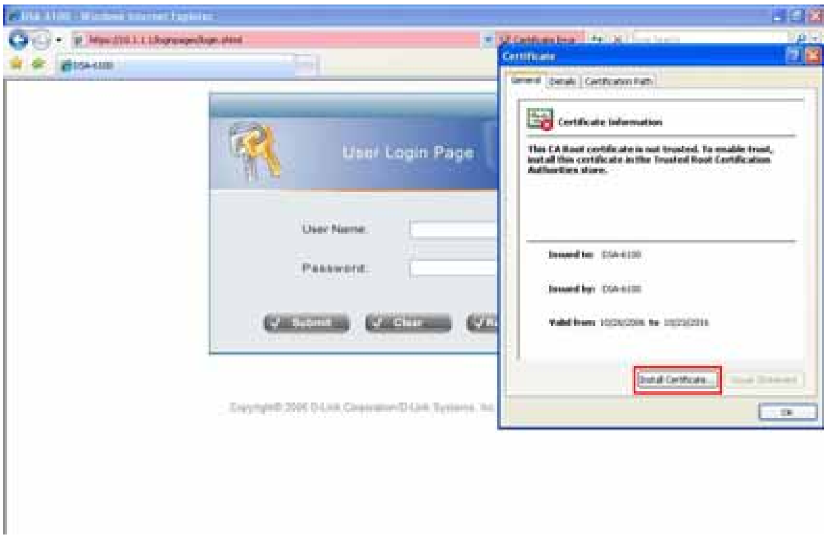
Valid from [illegible] to [illegible]

d. Select root certification, then click ***"View Certificate"***.



This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

e. Click ***"Install Certificate"***.



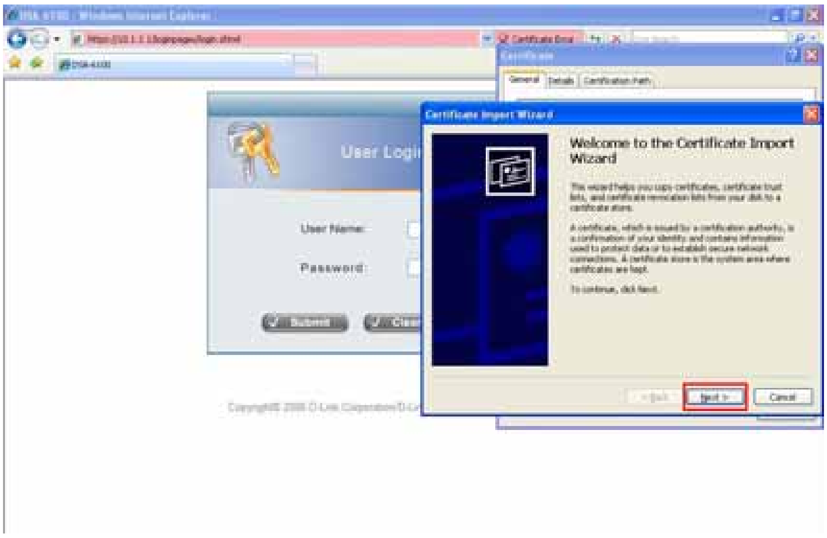
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: DSA-6100

Issued by: DSA-6100

Valid from 10/26/2006 to 10/23/2016

f. Click ***"Next"***.



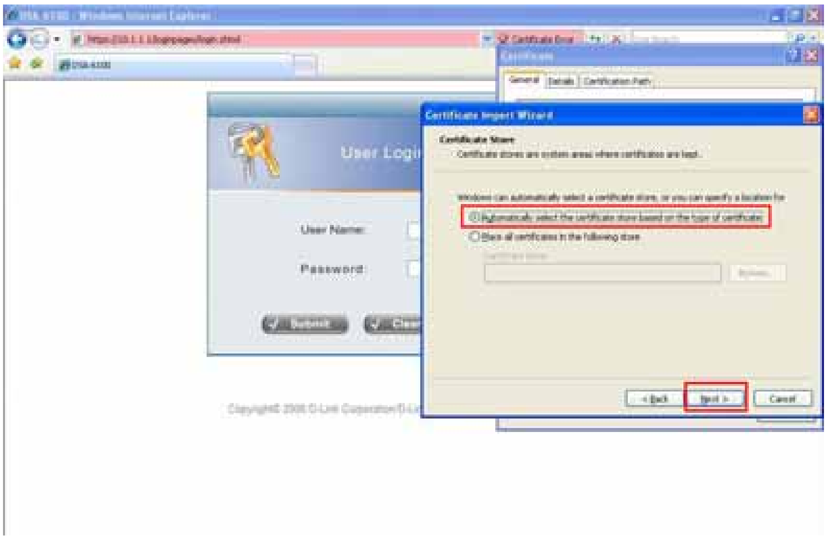
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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



Certificate Store

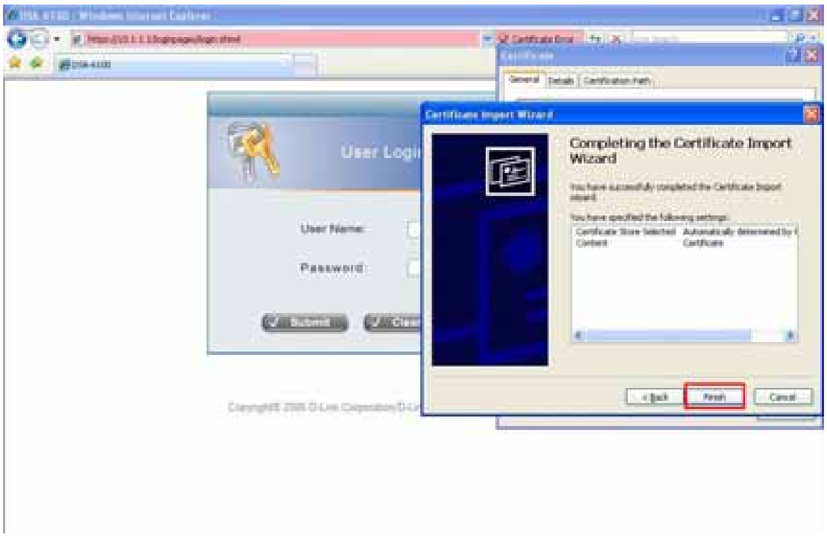
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

h. Click ***"Finish"***.



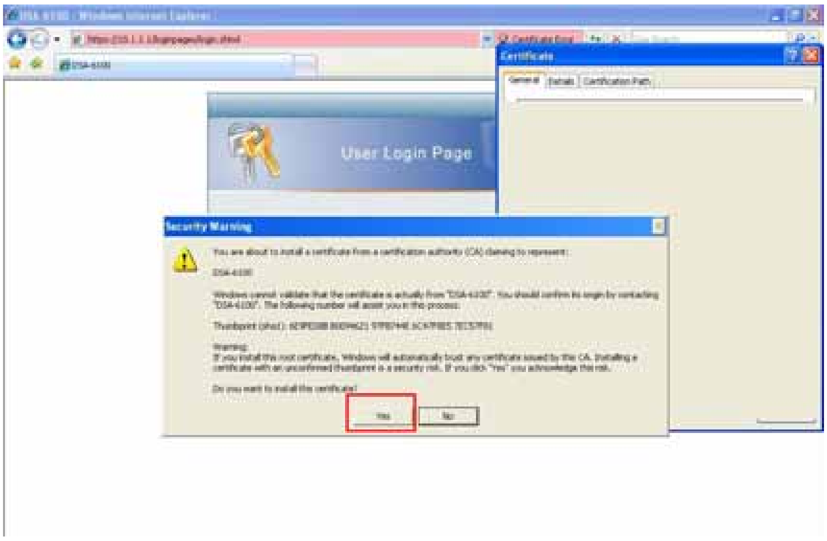
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

i. Click ***"Yes"***.



You are about to install a certificate from a certification authority (CA) claiming to represent:

DSA-6100

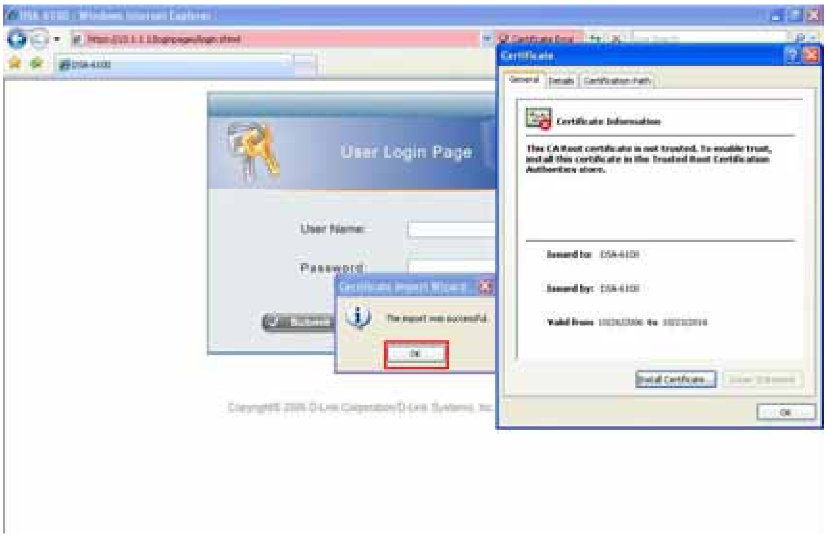
Windows cannot validate that the certificate is actually from "DSA-6100". You should confirm its origin by contacting "DSA-6100". The following number will assist you in this process:

Thumbprint (sha1): [illegible]

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

j. Click ***"OK"***.



Certificate Information

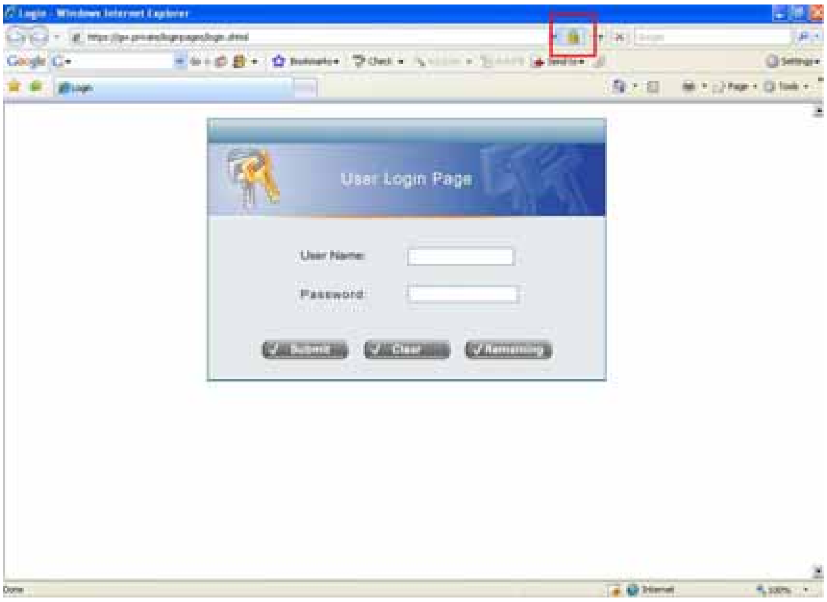
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: DSA-6100

Issued by: DSA-6100

The import was successful.

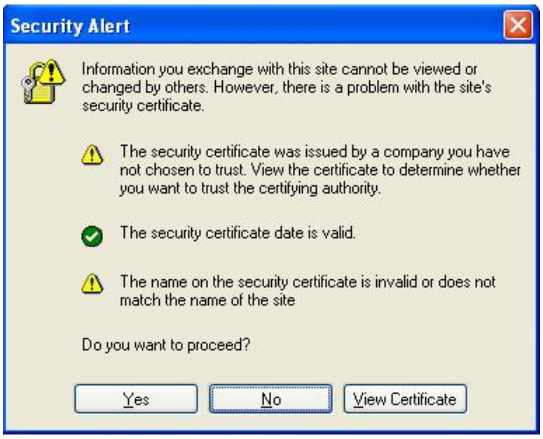
k. Launch a new IE7 browser. The certificate is now trusted via IE7 according to the key symbol shown at top next to the address field.



▪ Certificate setting for Internet Explorer 6

For issues relating to IE6 certificate error, the following information provides the step to proceed 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.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

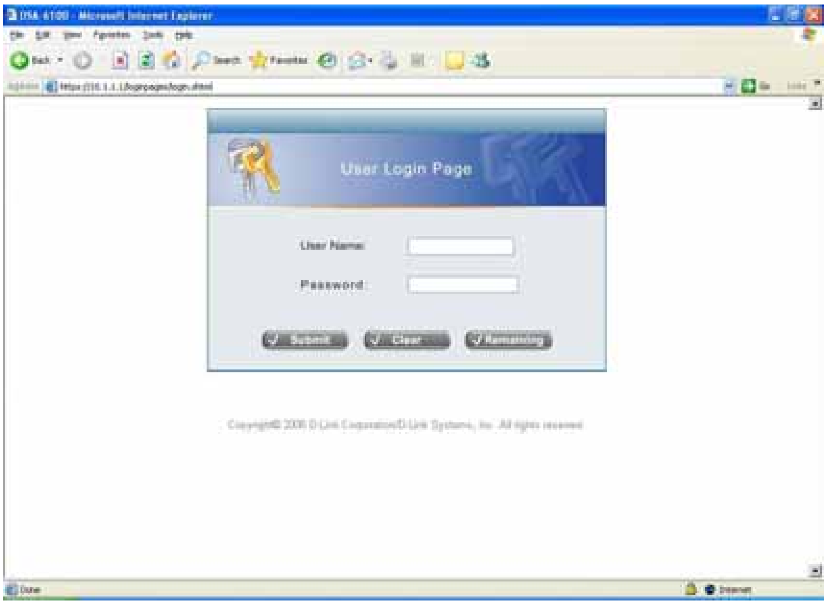
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

2. The User Login Page will appear.



DSA-6100 - Microsoft Internet Explorer
User Login Page
User Name:
Password:
Submit
Clear
Remaining
Copyright© 2006 D-Link Corporation/D-Link Systems, Inc. All rights reserved.
Done
Internet

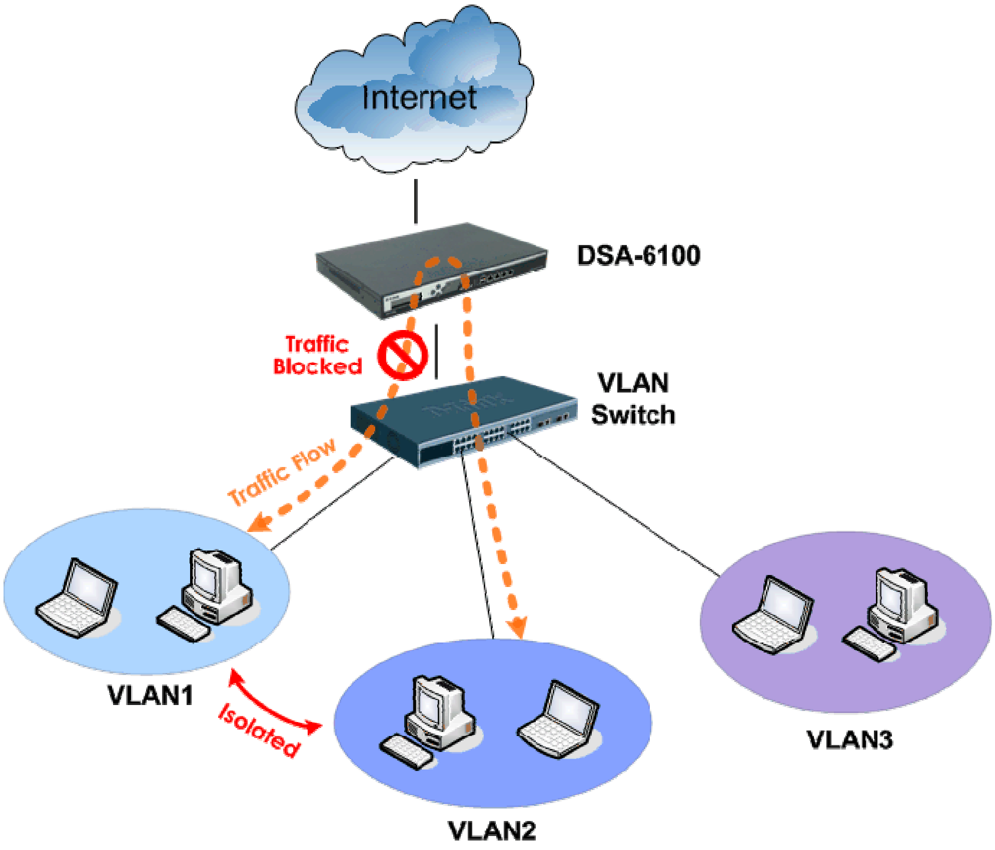
3. The user can now login normally.

Appendix E. VLAN Isolation

VLAN mode

In the VLAN mode, the system can serve both tagged and untagged packets at the same time and LAN interface will also be associated with an IP address. Currently, there are 32 VLANs available on each LAN interface. Therefore, there will be total thirty-three "subnets" connected to each LAN port.

User/VLAN Isolation



As shown in the above example diagram, the traffic between VLAN1and VLAN2 will travel through the DSA-6100. When the specific VLAN isolation rule (which is applicable to VALN1 and VLAN2) is activated in DSA-6100, the traffic will be blocked by DSA-6100 and therefore the users on two VLANs are "isolated" from each other. For more information about the VLAN isolation, here are the details:

1) The VLAN isolation rules are configured in "Global Policy" and therefore apply globally to the entire system. In other words, the rules apply to all users, including authenticated users, users on a non-authenticated port, privileged users, VPN users, DMZ clients, and virtual servers.

2) If the system is not in Bridge mode, the isolation rules are applied in two tiers, a big default rule and up to ten exceptional rules. The default action (the big default isolation rule) for the traffic between all interfaces is either Pass All or Block All. If traffic between any particular interfaces has to be blocked or passed, administrators will need to create the custom, exceptional rules to block or to pass the traffic that are traveling between the selected interfaces.

3) The following table shows the choices and conventions of the interfaces for exception rules.

Convention	**Description**
ALL	All the LAN interfaces and VLAN interfaces on LAN1 and LAN2 ports.
LAN1-Tag#nnnn	The VLAN with Tag ID "nnnn" on LAN1 port (for example, LAN1-Tag#1111 is the VLAN with Tag ID 1111 on LAN1)
LAN2-Tag#nnnn	The VLAN with Tag ID "nnnn" on LAN2 port (for example, LAN2-Tag#3333 is the VLAN with Tag ID 3333 on LAN2)
LAN1-Untagged	The LAN interface on LAN1 port
LAN2-Untagged	The LAN interface on LAN2 port

Please note that the exception rule is bi-directional. For example, the pair {LAN1-Tag#1111, LAN2-Tag#3333} is the same as the pair {LAN2-Tag#3333, LAN1-Tag#1111}.

4) *An Example*: The Default Isolation Rule specifies "Block All Traffic" and an exception rule says "Pass" the pair {LAN1-Untagged, ALL}. In this example, the system will block all traffic between all VLAN interfaces, except for the traffic between VLAN1 and other VLANs.

5) The priority of basic system security rules:

a. When the Default Isolation Rule is "Pass All Traffic", the priority of exception rules (Block) is higher than the firewall rules. In other words, in this case, the exception rules will block traffic between the specified interfaces, even when the Firewall rules are configured to pass all traffic.

b. When the Default Isolation Rule is "Block All Traffic", the priority of exception rule (Pass) is lower than the firewall rules. In other words, in this case, the exception rules will not pass traffic between the specified interfaces, if the Firewall rules are configured to block traffic between the specified interfaces.

c. Walled Garden will not be blocked by VLAN isolation rules. For example, there is a server in Walled Garden in VLAN1. The "Block All Traffic" rule will not prevent users on VLAN2 from seeing the server in Walled Garden.

d. DMZ and Virtual Servers are subject to VLAN isolation rules. For example, there is a virtual server in VLAN1. A "Block All Traffic" rule will prevent users on VLAN2 from seeing the virtual server.

Appendix F. 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 *Notification Configuration* - please refer to 4.5.5.
- ➢ 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
```