

DSA-5100

INSTALLATION GUIDE



Package Contents

- D-Link[®] DSA-5100 *Airspot*[™] Enterprise Gateway
- CAT5 UTP Straight-Through Ethernet Cables (Qty. 3)
- CAT5 UTP Crossover Cable (Qty. 1)
- CD-ROM with manual
- Null modem RS-232 console cable (Qty. 1)
- Power Cord

System Requirements

- Computer with an Ethernet adapter and a Windows, Mac, or Unix based operating system.
- Internet Explorer or Netscape Navigator, version 6.0 or above, with JavaScript enabled.

Hardware Overview

Front Panel



LED	Function
Link	Solid green indicates a good connection on the associated port.
Act	The Act LED flashes during data transmission on the associated port.
Power	A solid light indicates a proper connection to the power supply.
Status	The status LED has three states: <ul style="list-style-type: none"> • Unlit when the system's BIOS is loading or when powered off. • Flashing indicates the operating system is loading. • Solid when the system is fully loaded and ready to use.

Port	Function
Console	Direct connection to your computer's serial port using an RS-232 cable for gateway configuration. (The console settings are: Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1)
Public LAN	Connects to your open network environment. Requires authentication to use network resources and Internet.
Private LAN	Connects to your trusted internal network. Authentication is not required to access network resources.
WAN1	Connects to your Internet connection or Intranet.
WAN2	Connects to your Internet connection or Intranet.

Rear Panel



Item	Description
Power Connector	The power cord attaches here.
Power Switch	Powers the unit off and on.
Cooling Fans	Be sure to keep the unit in a well ventilated area and do not block the cooling fan vents.

Hardware Installation

1. Connect the power cord to the power connector on the rear panel of the DSA-5100. Plug the other end of the power cord to a wall outlet or power strip.
2. Turn on the power switch on the rear panel of the DSA-5100. The Power LED will illuminate.
3. Connect an Ethernet cable to the port labeled **Public LAN** on the DSA-5100. Connect the other end of the Ethernet cable to a switch or wireless access point that will provide public access to your broadband connection. The Public LAN LED should illuminate to indicate a proper connection.
4. Connect an Ethernet cable to the port labeled **Private LAN** on the DSA-5100. Connect the other end of the Ethernet cable to a switch. The Private LAN LED should illuminate to indicate a proper connection.
5. Connect an Ethernet cable to the port labeled **WAN1** on the DSA-5100. Connect the other end of the Ethernet cable to a broadband modem. If the connection is live, the WAN1 LED will illuminate.
6. (Optional) Connect an Ethernet cable to the port labeled **WAN2** on the DSA-5100. Connect the other end of the Ethernet cable to a router or directly to a high speed connection. If the connection is live, the WAN2 LED will illuminate.

The Setup Wizard

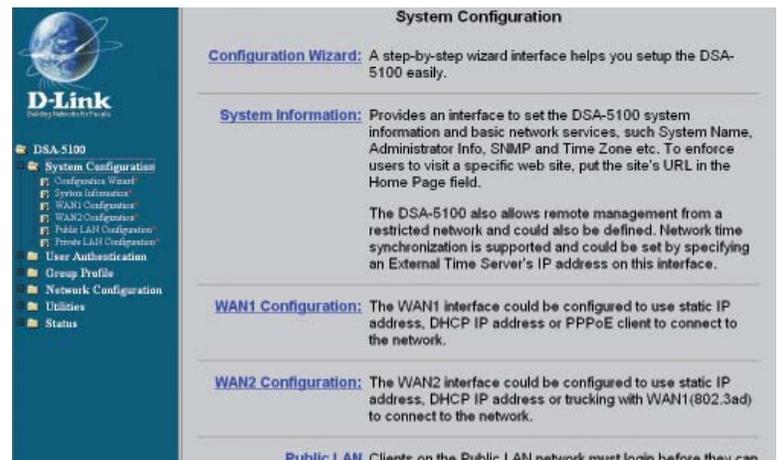
The DSA-5100 provides Web based configuration. You can configure your DSA-5100 using Internet Explorer or Netscape Navigator version 6.0 or above with JavaScript enabled. To access the configuration screen, launch your Web browser and enter the IP address of the DSA-5100 in the address field and press enter. If using the DSA-5100's default IP address, you would enter **https://192.168.0.40** (Note: Include the "s" at the end of **https** to ensure a secure connection).



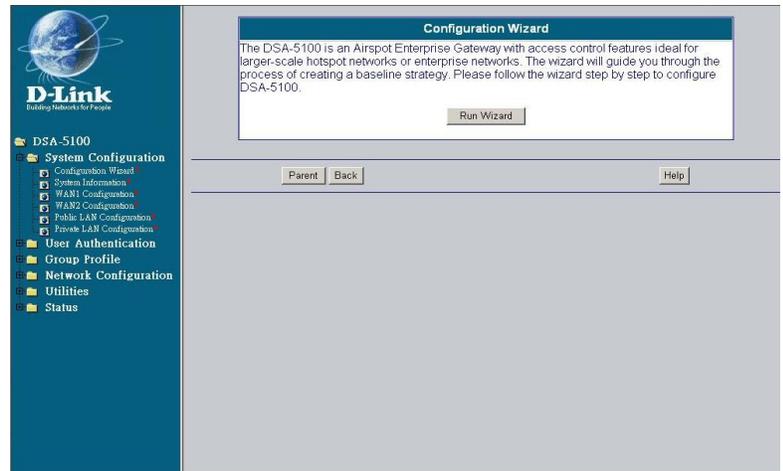
Once you've connected to the DSA-5100, the Login screen appears. By default, **admin** is the User Name and Password. Type **admin** in the User Name and Password fields and click **Enter**.



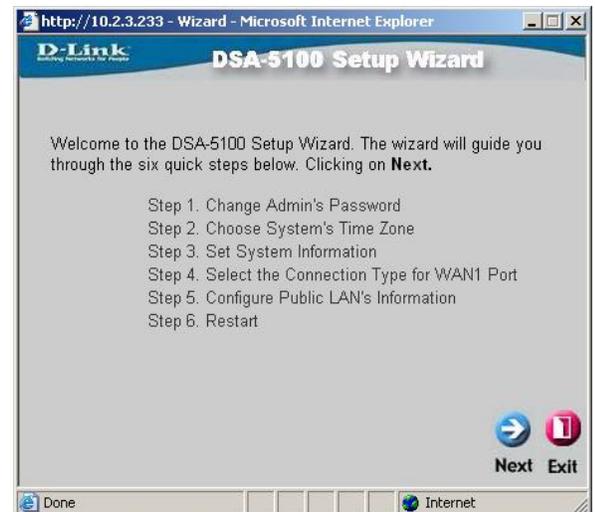
After successfully logging in, the Home screen will appear. Click on the System Configuration folder on the left panel to reveal the System Configuration options. The first option displayed is the Configuration Wizard. Click on this to display the Configuration Wizard screen.



Click on the **Run Wizard** button to begin the Setup Wizard.



The Setup Wizard appears, click **Next** to begin.



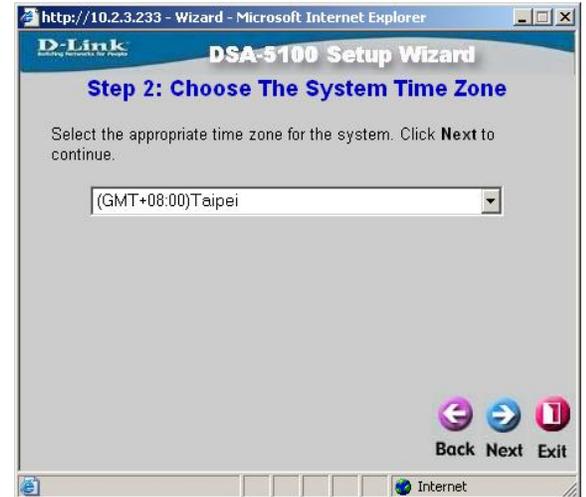
Step 1 - Change Admin's Password

Enter a new password for the admin account and retype it in the verify password field. Click **Next** to continue.



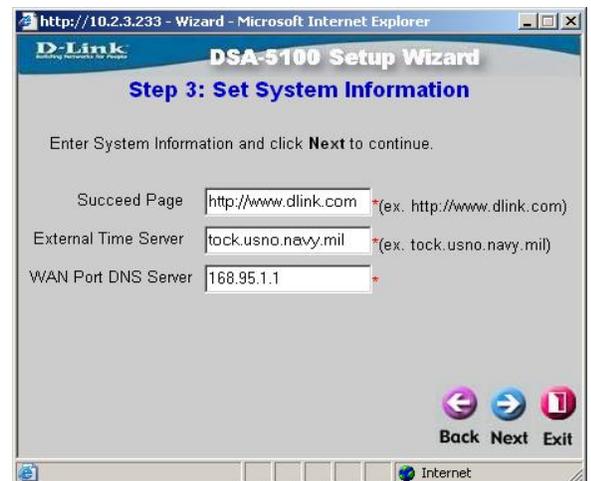
Step 2 - Choose System's Time Zone

Select your time zone and click **Next** to continue.



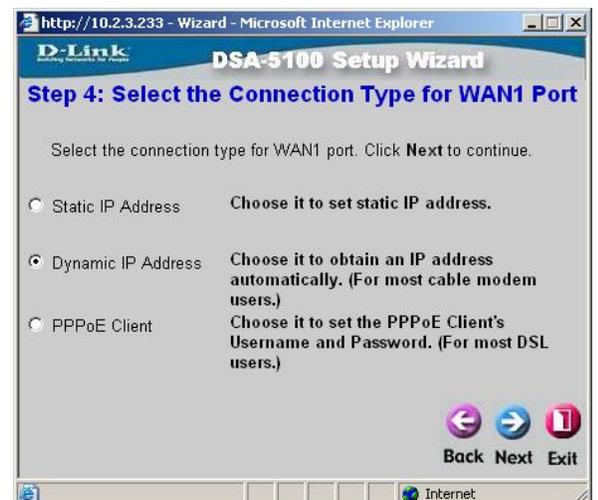
Step 3 - Set System Information

- **Succeed Page:** Enter the URL that users should be directed to when successfully authenticated.
- **External Time Server:** Enter the URL of external time server for the gateway to synchronize the time from.
- **WAN Port DNS Server:** Enter a DNS Server provided by your Internet Service Provider. Contact your ISP if you are unsure of the IP Address to enter here.



Step 4 - Select the Connection Type for WAN1 Port

Select the type of Internet connection that you have. If you are unsure of which to select, please contact you Internet Service Provider. Click **Next** to continue. If you selected DHCP, proceed to step 5 on page 8.



Step 4 - Set WAN1 Port's Static IP Address

If you selected Static IP, enter the IP address information provided by your Internet Service Provider. You must complete all of the fields. Click **Next** and continue to Step 5 on page 8.

The screenshot shows a web browser window titled "http://10.2.3.233 - Wizard - Microsoft Internet Explorer". The page header includes the D-Link logo and "DSA-5100 Setup Wizard". The main heading is "Step 4: Set WAN1 Port's Static IP Address". Below the heading, the instruction reads: "Configure WAN1 static IP address, and click **Next** to continue." There are three input fields: "IP address" with the value "10.2.3.233", "Subnet mask" with the value "255.255.255.0", and "Default gateway" with the value "10.2.3.254". At the bottom right, there are three buttons: "Back" (left arrow), "Next" (right arrow), and "Exit" (stop sign).

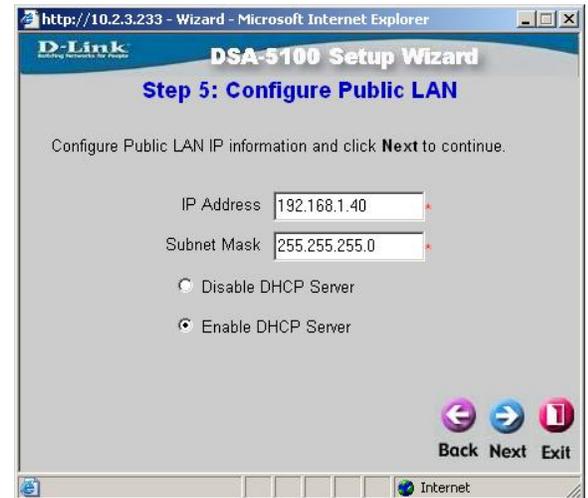
Step 4 - Set PPPoE Client's Information

If you selected PPPoE, enter the Username and Password provided by your Internet Service Provider. Click **Next** and continue to Step 5 on page 8.

The screenshot shows a web browser window titled "http://10.2.3.233 - Wizard - Microsoft Internet Explorer". The page header includes the D-Link logo and "DSA-5100 Setup Wizard". The main heading is "Step 4: Set PPPoE Client's Information". Below the heading, the instruction reads: "Enter the PPPoE Client's information provided by your ISP. Click **Next** to continue." There are two input fields: "Username" and "Password". At the bottom right, there are three buttons: "Back" (left arrow), "Next" (right arrow), and "Exit" (stop sign).

Step 5 - Configure Public LAN

- **IP Address and Subnet Mask:** Enter the IP Address and Subnet Mask of the DSA-5100 for the Public LAN port.
- **Disable DHCP Server:** If this option is selected, then LAN clients must be configured with an IP address manually.
- **Enable DHCP Server:** When selected, this allows the DSA-5100 to automatically provide the necessary IP information to all Public LAN clients configured for DHCP.

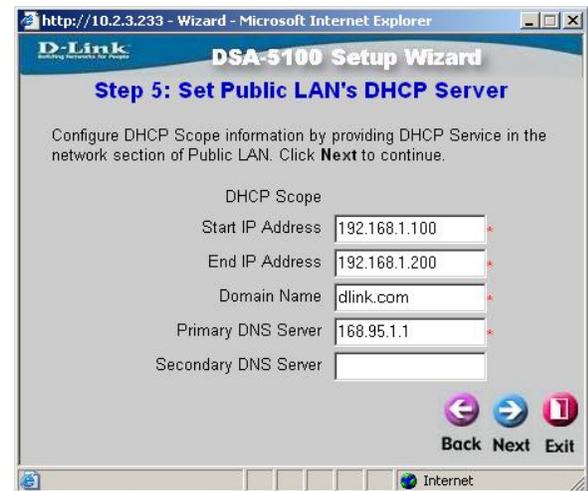


Step 5 - Set Public LAN's DHCP Server

- **Start IP Address, End IP Address:** These fields define the IP address range that will be assigned to the Public LAN clients configured for DHCP.

Be sure the IP range does not conflict with any manually configured network devices or the IP address of the DSA-5100.

- **Domain Name:** Enter a domain name provided by your ISP.
- **Primary DNS Server, Secondary DNS Server:** The DNS Server settings are provided by your Internet Service Provider. Only the Primary DNS Server field is mandatory. Contact your ISP if you are unsure of the DNS Server settings.



Step 6 - Restart

Click on **Restart** to save the current settings and restart the DSA-5100. The Setup Wizard is complete!



System Configuration

System Information

System Information	
System Name	<input type="text" value="DSA-5100"/>
Administrator Info	<input type="text"/> (It'll appear when Internet connection fails.)
Succeed Page	<input type="text" value="http://www.dlink.com"/> * (http://www.dlink.com)
Remote Management IP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="0.0.0.0/0.0.0.0"/> (ex: 192.168.3.1 or 192.168.3.0/24)
Access History IP	<input type="text"/> (ex: 192.168.2.1)
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
User Logon SSL	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time	Device Time : 2006/01/12 14:20:55 <input checked="" type="radio"/> Enable NTP NTP Server <input type="text" value="tock.usno.navy.mil"/> *(ex. tock.usno.navy.mil) Time Zone <input type="text" value="(GMT+08:00)Taipei"/> <input type="button" value="v"/> <input type="radio"/> Set Device Date and Time

- **System Name:** The system name of the DSA-5100. Used for SNMP purposes. The default is DSA-5100.
- **Administrator Info:** Information on how to contact the system administrator can be entered here. The administrator's name, phone number, and e-mail address can be entered here. If a user connects to the DSA-5100 and WAN1 has a connection problem, the user logon screen will show the system administrator information that was entered here.
- **Succeed Page:** Enter a URL to direct users to once they have been authenticated. Typically this would be a company web page such as www.dlink.com.
- **Remote Management IP:** When enabled, the IP address entered has the ability to manage the DSA-5100 via the WAN1 interface. This allows the system at the specified IP address to manage the DSA-5100 over the Internet.
- **Access History IP:** The IP address of your billing system should be entered here to allow the billing system to access the DSA-5100's billing history information.
- **SNMP:** The DSA-5100 supports SNMP v2 read only data access. The administrator can specify the IP address and the SNMP community name to determine the target of the management information base (MIB) exported from the DSA-5100.
- **User Logon SSL:** When enabled, the user logon is secure using https. If disabled, standard http is used.
- **Time:** The DSA-5100 supports NTP Time Server configuration for accurately synchronizing the network time. If NTP is enabled, you can enter an NTP server for time synchronization. The alternate option is Set Device Date and Time, which allows you to manually specify the time.

Global LAN Configuration

You can set the system to Enable or Disable the IP PNP or mobile IP options for the public LAN and private LAN simultaneously.

Global LAN Configuration	
Enable IP PNP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Enable Mobile IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

IP PNP: When enabled, you can use any IP address to connect to the Public LAN. You can authenticate to the DSA-5100 and access network resources regardless of your IP configuration. **Note: This function only works when NAT is used.**

Mobile IP: This option allows a user to use the same IP configuration across a network using several DSA-5100 units.

Interface Configuration

The Interface Configuration options only vary slightly between the Public LAN, Private LAN, and VLAN Configurations. The VLAN Configuration is the only configuration that provides the VLAN Tag option. The Private LAN Port doesn't have the option for User Authentication.

VLAN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Enable User Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Operation Mode	<input type="text" value="NAT"/>
IP Address	<input type="text" value="192.168.1.40"/> *
Subnet Mask	<input type="text" value="255.255.255.0"/> *

- **VLAN:** Enable or disable the VLAN option (only applicable in the Public LAN and VLAN Interface Configuration).
- **Enable User Authentication:** Controls user authentication per selected interface when enabled. The default is disabled.
- **Operation Mode:**

NAT Mode: In this mode, all IP addresses that are connected through the Public LAN Port are converted into the IP address of the WAN1 Port for external communication.

Router Mode: All IP addresses that are connected through the Public LAN Port use their individual IP addresses for external communication. In this mode, the DSA-5100 acts like a Router.

- **IP Address:** The IP address to be used for the selected interface.
- **Subnet Mask:** The subnet mask to be used for the selected interface.

DHCP Server Options

You will find the DHCP Configuration options are the same beneath the Public LAN, Private LAN, and VLAN Port configurations. The functionality is the same for all of the options, the only difference is the port to which they are applied.

Disable DHCP Server: When selected, the DSA-5100 will not provide IP addresses to the clients connected to the Public LAN Port.

Enable DHCP Server: When the DHCP Server is enabled, the fields with the red asterisks must be filled in.

The DHCP Scope defines the range of IP addresses available for assignment.

Start IP Address: Defines the first available IP address for the unit to assign to a client.

End IP Address: Defines the last available IP address for the unit to assign a client.

All addresses between the Start IP Address and End IP Address are available for assignment to clients.

Primary DNS Server: Enter the IP address of the primary DNS server.

Secondary DNS Server: A secondary DNS server's IP address can be entered here but is not required.

Domain Name: Enter the domain name.

WINS Server IP: Enter the IP address of the WINS server.

Lease Time: Select the amount of time for the DHCP assigned IP addresses to be in effect.

Reserved IP Address List: This function allows you to reserve specific IP addresses for specific systems/devices. The IP address will be reserved for the specified MAC address. To use this function, click on the [Reserved IP Address List](#) link and the Reserved IP Address List options will appear. Enter the IP address to be reserved and the MAC address of the device to assign it to. A description can be entered but is not mandatory. Click Apply to save the settings.

- Disable DHCP Server
- Enable DHCP Server

DHCP Scope

Start IP Address

End IP Address

Primary DNS Server

Secondary DNS Server

Domain Name

WINS Server

Lease Time

[Reserved IP Address List](#)

- Enable DHCP Relay

Reserved IP Address List -- Public LAN			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>

DHCP Server Relay: Select this mode to specify another DHCP server's IP address.

User Authentication

Authentication Policies

The DSA-5100 provides five different management setups. The Administrator can adopt different authentication methods according to each management setup. Each management setup can use up to twenty management rules in addition to the group configuration. This allows more diversified and flexible management options for general users.

Authentication Policies Configuration					
Item	Policy Name	Status	Default	Group	
1	postfix1	Enabled	Yes	1	Edit
2	postfix2	Enabled	No	1	Edit
3	postfix3	Enabled	No	1	Edit
4	postfix4	Enabled	No	1	Edit
5	postfix5	Enabled	No	1	Edit

- **Item:** The item number.
- **Policy Name:** The policy name is displayed here.
- **Status:** Displays whether the policy is enabled or disabled.
- **Default:** Lists the policy that is the default. Only one policy may be selected as the default.
- **Group:** Displays the group assignment.

Authentication Policies Configuration

Preferred Authentication Policies	
Authentication Policy	1:postfix1
Authentication Policies Configuration	
Policy ID	1:postfix1 <input type="checkbox"/> Set as Default: <input checked="" type="checkbox"/>
Policy Name	postfix1 <small>*(It's postfix name)</small>
Policy Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Black List Profile	None
Authentication Server	<input checked="" type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> NT Domain <u>Local Users List</u> Assign to Group: 1:Group1 Exception Configuration <input type="radio"/> Enable <input checked="" type="radio"/> Disable Edit

- **Policy ID:** The system provides five separate authentication policies. Select the desired control group from the pull-down menu.
- **Set as Default:** Selecting this option will set the selected control group as the preferred authentication method. Only one policy can be selected as the default.
- **Policy Name:** The friendly name for the authentication policy. The DSA-5100 controls priority according to the following postfix when the user logs on the system (example user1@postfix1).
- **Policy Status:** The policy is enabled or disabled here.
- **Black List Profile:** Select one of the five profiles from the Black List configuration or None if you don't wish to use one.
- **Authentication Server:** There are five authentication options listed here (Local, POP3, RADIUS, LDAP, and NT Domain) and an additional option on the External Authentication screen (http or https).
- **Assign to Group:** Select a group to assign to the Authentication Policy using the pull-down menu.
- **Exception Configuration:** Allows exceptions to the configuration rules to be defined. Exceptions are defined based on user's attributes.

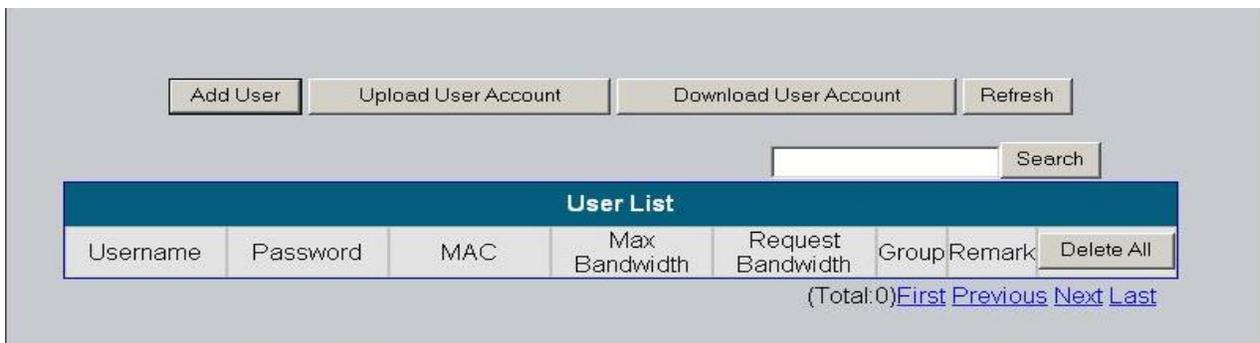
Exception Configuration				
If	Attribute	Logic	Value	Group
1	<input type="text"/>	equal to <input type="button" value="v"/>	<input type="text"/>	1:Group1 <input type="button" value="v"/>
2	<input type="text"/>	equal to <input type="button" value="v"/>	<input type="text"/>	1:Group1 <input type="button" value="v"/>
3	<input type="text"/>	equal to <input type="button" value="v"/>	<input type="text"/>	1:Group1 <input type="button" value="v"/>
4	<input type="text"/>	equal to <input type="button" value="v"/>	<input type="text"/>	1:Group1 <input type="button" value="v"/>
5	<input type="text"/>	equal to <input type="button" value="v"/>	<input type="text"/>	1:Group1 <input type="button" value="v"/>

- **Attribute:** After authentication, the DSA-5100 will obtain the user’s attributes from the authentication server. Attributes can be defined for management rules.
- **Logic:** The pull-down menu displays the logic conditions that filter the attribute.
- **Value:** This is the value that is matched to the attribute and logic.
- **Group:** Specifies the group the exception will be applied to.

Authentication Methods

Local

The Local user authentication method authenticates users from a list of users created on the DSA-5100. The DSA-5100 has a maximum of 2000 user accounts. To access the list of accounts, click on the [Local Users List](#) hyperlink from the Authentication Policies Configuration page when Local is selected as the Authentication Server.



To Add Users, click the **Add User** button and enter the following information:

- **Username:** Usernames can be up to 32 characters maximum. No spaces can be used.
- **Password:** Enter a password consisting of up to 20 characters. No spaces can be used.
- **MAC:** This field is optional. Enter the MAC address of the system the user will authenticate from. Be sure to include the colon (:) between each octet (xx:xx:xx:xx:xx:xx).
- **Max Bandwidth:** The amount of maximum transmission capacity that is available on a network at any point in time.
- **Request Bandwidth:** The amount of minimum transmission capacity that is available on a network at any point in time.
- **Group:** You can assign users to groups to simplify administration.

• **Remark:** This comment field is optional and for your reference only. You can enter up to 50 characters in this field. Click Apply to add the users. Note: Each page only displays ten users at a time. If you've entered ten users and need to add more, click Apply and a new screen will appear allowing you to enter up to ten more. Repeat the process until you've added all of your users.

To see newly added users, click the **Refresh** button. To edit a user, simply click on the Username. To delete a user, click the **Delete** button. To delete all user accounts, click the **Delete All** button. To search the user list, enter the name to search and click the **Search** button. The search function retrieves all usernames that contain the exact character(s) entered. The user list displays names in sets of ten. The bottom right displays a menu for navigating through the list of users.

Editing Accounts

The user account can be edited by clicking on the Username. The Edit Account window will appear. Modify the account as needed and click **Submit** to save changes. To retrieve the currently saved account settings, click the **Reset** button. To return without saving changes, click the [Back to Users List](#) hyperlink.

Upload User Account

You can copy user account information to the DSA-5100 from a text file. You can either upload a previously saved file or create a text file using the proper format. In the text file, each user must have their own line and there are no spaces. Use the colon (:) between the octets of the MAC address. Spaces can only be used in the remarks section. There must not be any spaces between the fields and the commas. The MAC field may be omitted but the trailing comma must remain. When uploading user accounts, existing accounts in the embedded database that are also listed in the data file will be replaced with the uploaded account information. The format is as follows:

username,password,MAC,remark

Note: The format of each line is "ID,Password,MAC,Max bandwidth,Request bandwidth,Group,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 be replaced by the new ones.

Download User Account

This option will save all of your user accounts to a text file that can be uploaded back to the DSA-5100. To Download the user accounts, click on the Download User Account button. The user accounts will be displayed on the screen. Scroll to the bottom of the page. Right click on the Download hyperlink and select Save Target As. Choose a file name and location. Click the Close button when finished.

POP3

When selecting POP3 as the authentication method, you must enter the IP address or domain name of the POP3 server. You must also enter the port number. The standard port number is 110. A secondary POP3 server can be entered but is not mandatory. The Enable SSL Connection option can be selected if your configuration supports this.

Preferred Authentication Policies	
Authentication Policy	1:postfix1
Authentication Policies Configuration	
Policy ID	1:postfix1 <input type="button" value="Set as Default"/> <input checked="" type="checkbox"/>
Policy Name	postfix1 <small>*(It's postfix name)</small>
Policy Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Black List Profile	None
Authentication Server	<input type="radio"/> Local <input checked="" type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> NT Domain
	Primary POP3 Server
	Server IP <input type="text"/> <small>*(Domain Name /IP address)</small>
	Port <input type="text"/> <small>*(Default:110)</small>
	<input type="checkbox"/> Enable SSL Connection
	Secondary POP3 Server
	Server IP <input type="text"/>
	Port <input type="text"/>
	<input type="checkbox"/> Enable SSL Connection
	Assign to Group: <input type="text" value="1:Group1"/>
Exception Configuration <input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Edit	

RADIUS

When selecting RADIUS as the authentication method, there are several parameters that need to be configured.

Preferred Authentication Policies	
Authentication Policy	1:postfix1
Authentication Policies Configuration	
Policy ID	1:postfix1 <input type="checkbox"/> Set as Default: <input checked="" type="checkbox"/>
Policy Name	postfix1 <small>*(It's postfix name)</small>
Policy Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Black List Profile	1:Blacklist1
Authentication Server	<input type="radio"/> Local <input type="radio"/> POP3 <input checked="" type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> NT Domain 802.1x Authentication <input type="radio"/> Enable <input checked="" type="radio"/> Disable Trans Full Name <input type="radio"/> Enable <input checked="" type="radio"/> Disable Class Configuration <input type="radio"/> Enable <input checked="" type="radio"/> Disable Primary RADIUS Server Server IP <input type="text"/> * Authentication Port <input type="text"/> <small>*(Default:1812)</small> Accounting Port <input type="text"/> <small>*(Default:1813)</small> Secret Key <input type="text"/> * Accounting Service <input type="text" value="Disabled"/> Authentication Method <input type="text" value="PAP"/> Secondary RADIUS Server Server IP <input type="text"/> Authentication Port <input type="text"/> Accounting Port <input type="text"/> Secret Key <input type="text"/> Accounting Service <input type="text" value="Disabled"/> Authentication Method <input type="text" value="CHAP"/> Assign to Group: <input type="text" value="1:Group1"/> Exception Configuration <input type="radio"/> Enable <input checked="" type="radio"/> Disable Edit

802.1X Authentication: When 802.1x Authentication is enabled, an Edit option will appear just below the enable button. Click the [Edit](#) hyperlink to configure the additional parameters. You must define the IP (segment) address and the secret that you have configured.

Trans Full Name: If enabled, ID and postfix data will be transferred to the RADIUS server for authentication. When disabled, only the ID will be transferred to the RADIUS server for authentication.

Class Configuration: Configuration reads parameters from a configuration file and returns their values on demand. Set the Max Bandwidth and Request Bandwidth, and assign a group for every class.

Server IP: Enter the IP address or domain name of the RADIUS server.

Authentication Port: The authentication port number is entered in this field. The standard port number is 1812.

Accounting Port: Enter the port configured for accounting.

Secret Key: The secret key used for encryption /decryption.

Accounting Service: Select enabled or disabled as needed.

Authentication Method: Select either CHAP or PAP type of authentication.

LDAP

When selecting LDAP as the authentication method, you must configure all of the fields under Primary LDAP Server. The Secondary LDAP Server fields are optional.

Preferred Authentication Policies	
Authentication Policy	1:postfix1
Authentication Policies Configuration	
Policy ID	1:postfix1 <input checked="" type="checkbox"/> Set as Default:
Policy Name	postfix1 <small>*(It's postfix name)</small>
Policy Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Black List Profile	1:Blacklist1
Authentication Server	<input type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input checked="" type="radio"/> LDAP <input type="radio"/> NT Domain
	Primary LDAP Server
	Server IP <input type="text"/> <small>*(Domain Name/IP address)</small>
	Port <input type="text"/> <small>*(Default:389)</small>
	Base DN <input type="text"/> <small>*(CN=,dc=,dc=)</small>
	Account Attribute Type <input type="radio"/> UID <input type="radio"/> CN <input type="radio"/> sAMAccountName
	<input type="checkbox"/> Anonymous Bind
	Bind RDN <input type="text"/>
	Bind Password <input type="text"/>
	Secondary LDAP Server
	Server IP <input type="text"/>
	Port <input type="text"/>
	Base DN <input type="text"/>
	Account Attribute Type <input type="radio"/> UID <input type="radio"/> CN <input type="radio"/> sAMAccountName
	<input type="checkbox"/> Anonymous Bind
Bind RDN <input type="text"/>	
Bind Password <input type="text"/>	
Assign to Group: <input type="text" value="1:Group1"/>	
Exception Configuration <input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Edit	

Server IP: The IP address or domain name of the LDAP server.

Port: Enter the port number in this field. The standard port number is 389.

Base DN: Base DN data of LDAP Server.

Account Attribute Type: Select the account attribute type. There are types, UID, CN and sAMAccountName.

Anonymous Bind: If you want to access the data from some LDAP servers which need to be authenticated, you have to enter the **username** and **password** in the "**Bind RDN**" and "**Bind Password**" fields, or check "**Anonymous Bind**" to just access the LDAP servers which don't need to be authenticated.

NT Domain:

When selecting the NT Domain authentication method, be sure the WAN1 Port Preferred DNS Server IP address is the Domain Controller Server IP address. Policy Name is your complete domain name.

Server IP: Enter the IP address of the domain controller.

Transparent Login: When enabled, the user logs into the DSA-5100 after logging into the Windows Domain.

Note: *Currently only Windows 2000 domain controllers can be used.*

Preferred Authentication Policies	
Authentication Policy	1:postfix1
Authentication Policies Configuration	
Policy ID	1:postfix1 <input type="checkbox"/> Set as Default: <input checked="" type="checkbox"/>
Policy Name	postfix1 <small>*(It's postfix name)</small>
Policy Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Black List Profile	None
Authentication Server	<input type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP <input checked="" type="radio"/> NT Domain <p style="text-align: center;">Domain Controller</p> Server IP Address <input type="text"/> * Transparent Login <input type="radio"/> Enable <input checked="" type="radio"/> Disable Assign to Group: 1:Group1 Exception Configuration <input type="radio"/> Enable <input checked="" type="radio"/> Disable Edit

External Authentication

The DSA-5100 also allows external authentication, allowing you to put the login page on an external web server. The login page can be changed at any time.

External Authentication Configuration	
Protocol	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS
Server IP	<input type="text"/>
Server Port	80
Login Page	<input type="text"/>

Protocol: Select HTTP or HTTPS.

Server IP: The External Web server's IP address.

Server Port: The External Web server's port number.

Login Page: The URL of the login page.

Group Profile

The DSA-5100 has three types of profile configurations: Firewall Profile, Specific Route Profile, and Login Schedule Profile.

Firewall Profile

The system has a default global firewall profile and five additional firewall profiles. You can use the global firewall profile to define the firewall rules for all users and create independent profiles using the other five settings.

Firewall Profile							
Profile ID:		1:IP Filter 1 <input type="button" value="v"/>					
Profile Name:		IP Filter 1					
Filter Rule Item	Name	Active	Action	Source	Destination	Protocol	MAC
1		<input type="checkbox"/>	Block	ANY	ANY	ALL	
2		<input type="checkbox"/>	Block	ANY	ANY	ALL	
3		<input type="checkbox"/>	Block	ANY	ANY	ALL	
4		<input type="checkbox"/>	Block	ANY	ANY	ALL	
5		<input type="checkbox"/>	Block	ANY	ANY	ALL	
6		<input type="checkbox"/>	Block	ANY	ANY	ALL	
7		<input type="checkbox"/>	Block	ANY	ANY	ALL	
8		<input type="checkbox"/>	Block	ANY	ANY	ALL	
9		<input type="checkbox"/>	Block	ANY	ANY	ALL	
10		<input type="checkbox"/>	Block	ANY	ANY	ALL	

Profile Name: Enter a name for the profile here.

Filter Rule Item: The filter rules use a serial filter to determine permissions for transmitting from the source address to the target address or examine whether there is a data loss. Click on the item number to display the details.

Edit Filter Rule				
Profile Name: IP Filter 1				
Rule Item: 1				
Rule Name: <input type="text"/>			<input type="checkbox"/> Enable this Rule	
Action: <input type="text" value="Block"/>		Protocol: <input type="text" value="ALL"/>		
Source MAC Address: <input type="text"/> (For Specific MAC Address Filter, ex:00:00:00:00:00:00)				
	Interface	IP	Subnet Mask	Operator
Source	<input type="text" value="ALL"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>
Destination	<input type="text" value="ALL"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>

Rule Name: Name the IP Filter rule.

Enable this Rule: The rule is active when selected.

Action: Specifies the action to be taken when packets match the rule. Pass will allow matching packets to be passed immediately. Block will drop matching packets immediately.

Protocol: Select from TCP, UDP, and ICMP protocols or select ALL for all three.

Source MAC: Source MAC address. Be sure to include the colon (:) between each octet (xx:xx:xx:xx:xx:xx).

Source Interface: Select a specific interface or ALL.

Source IP Address: Enter the IP address of the source.

Source Subnet Mask: Enter the Subnet Mask of the source.

Source Operator: Select the comparison rules: =(Equal), !=(Not Equal), >(Greater Than), and <(Less Than).

Destination Interface: Select a specific interface or ALL.

Destination IP Address: Enter the destination IP address.

Destination Subnet Mask: Enter the destination Subnet Mask.

Destination Operator: Select the comparison rules: =(Equal), !=(Not Equal), >(Greater Than), and <(Less Than).

Specific Route Profiles

Specific Route Profile				
Route ID: 1:Policy Route 1 ▼				
Profile Name: Policy Route 1				
Route Item	Destination		Gateway	Default
	IP Address	Subnet Netmask	IP Address	
1	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>

Profile Name: The name for the Specific Route Profile.

Destination IP Address: Specifies the target network or host IP.

Subnet Mask: Specifies the target subnet mask.

Gateway IP Address: Specifies the IP address of the next hop router.

Login Schedule Profiles

This allows you to set the hours that users are allowed to login.

Login Schedule Profile							
Schedule ID: 1:Schedule1							
Profile Name: Schedule1 <input checked="" type="radio"/> Enable <input type="radio"/> Disable							
hour	SUN	MON	TUE	WED	THU	FRI	SAT
0	<input checked="" type="checkbox"/>						
1	<input checked="" type="checkbox"/>						
2	<input checked="" type="checkbox"/>						
3	<input checked="" type="checkbox"/>						
4	<input checked="" type="checkbox"/>						
5	<input checked="" type="checkbox"/>						
6	<input checked="" type="checkbox"/>						
7	<input checked="" type="checkbox"/>						
8	<input checked="" type="checkbox"/>						
9	<input checked="" type="checkbox"/>						
10	<input checked="" type="checkbox"/>						
11	<input checked="" type="checkbox"/>						
12	<input checked="" type="checkbox"/>						
13	<input checked="" type="checkbox"/>						
14	<input checked="" type="checkbox"/>						
15	<input checked="" type="checkbox"/>						
16	<input checked="" type="checkbox"/>						
17	<input checked="" type="checkbox"/>						
18	<input checked="" type="checkbox"/>						
19	<input checked="" type="checkbox"/>						
20	<input checked="" type="checkbox"/>						
21	<input checked="" type="checkbox"/>						
22	<input checked="" type="checkbox"/>						
23	<input checked="" type="checkbox"/>						

Network Configuration

Five functions are provided to control individual jobs of the network transmission: Network Address Translate, Privilege List, Monitor IP List, Free Surfing Area, and Proxy Server properties.

Network Address Translate

DMZ

If you have several Public IP addresses, you can assign External IP Addresses (Public IP Addresses) to Internal IP Addresses (Virtual IP Addresses). The WAN port of the system will automatically set the public address defined here. Up to forty virtual IP addresses can be defined. These settings are effective as soon as you click the Apply button.

DMZ		
Item	Internal IP Address	External IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Virtual Server

The Virtual Server permits you to define up to forty virtual servers. This allows the computers that are not on the managed network to access the server on the managed network. Network services can be provided on the TCP, UDP, or both ports. These settings are effective as soon as you click the Apply button.

Virtual Server					
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

Port and IP Redirect

When any user attempts to connect to the defined destination, the connection packet will be converted to the corresponding destination. You can define up to forty groups for redirection. These settings are effective as soon as you click the Apply button.

Port and IP Redirect					
Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP

Privilege List

IP Pass Through Configuration

This feature allows designated IP addresses to bypass authentication. Up to one hundred IP addresses can be added to be given network access rights without authentication. These settings are effective as soon as you click the Apply button.

Note: *Permitting specific IP addresses network rights without authentication can present a security risk on the network.*

IP Pass Through Configuration		
Item	Privilege IP Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

MAC Pass Through Configuration

This feature allows designated MAC addresses to bypass authentication. Up to one hundred MAC addresses can be added to be given network access rights without authentication. Be sure to include the colon (:) between each octet (xx:xx:xx:xx:xx:xx). These settings are effective as soon as you click the Apply button.

Note: *Permitting specific MAC addresses network rights without authentication can present a security risk on the network.*

MAC Pass Through Configuration		
Item	MAC Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

This page left blank intentionally.

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product.

U.S. and Canadian customers can contact D-Link technical support through our website or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

(877) 453-5465

Twenty four hours a day, seven days a week.

D-Link Technical Support over the Internet:

<http://support.dlink.com>

email: support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

(800) 361-5265

Monday through Friday, 7:30am to 12:00am EST.

D-Link Technical Support over the Internet:

<http://support.dlink.ca>

email: support@dlink.ca