RangeBooster G Wireless Router User's Guide

Version 1.00.70-09.12.2006

Contents

About This Manual

This manual describes the setup and usage steps you should perform to use the DIR-430 RangeBooster G Wireless Router.

Notational Conventions

This guide uses the following notational conventions:

Notation	Meaning
Menu options	Bold. Example, Select the **Settings** option on the screen.
Allowed URLs	Hyperlinks are underlined. Example, http://www.dlink.com/
Italics	Text in italics is used for emphasis.
	Warning. Follow the instructions provided to avoid this situation.
	Important note or instruction to read.

Chapter 1 Introduction

Introduction

The DIR-430 RangeBooster G Router provides access of your home network contents through a web-based portal on a secured SSL or HTTPS connection. The DIR-430 also features an ICSA certified, advanced Stateful Packet Inspection Firewall.

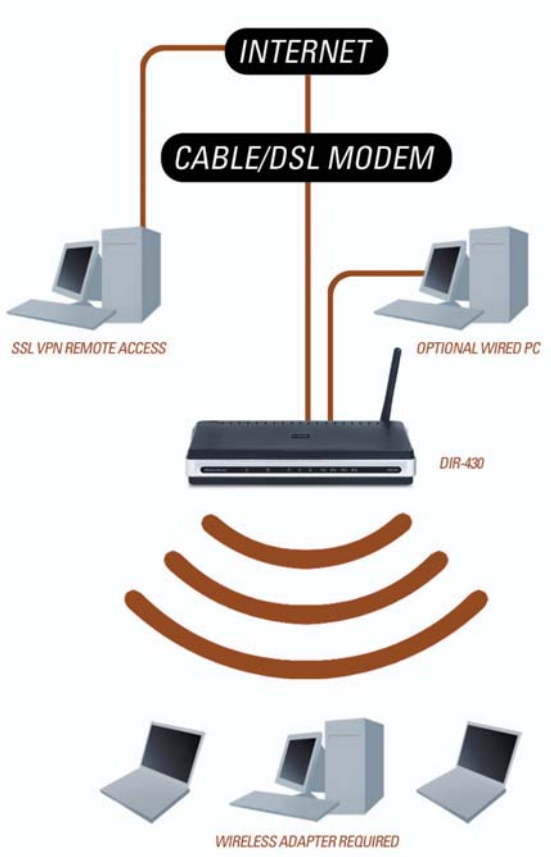
In addition the DIR-430 is a perfect solution for connecting a PC (or small group of PCs) through a switch, hub or Wi-Fi to a high-speed broadband Internet connection. With the performance and security features of the DIR-430, your network will take advantage of the Internet while keeping private data secure.

Features

- Ability to publish content on the Home Network to the Internet, content being photos, videos, music, files and blogs stored on network file shares. An external blog may also be referred.
- Ability to control who may view what content. Administrator can provide access facilities.
- Ability to provide secure remote access to PC desktops in the home network (RDP & VNC).
- Protects your PCs from 50 kinds of attacks known in the Internet world like Ping of Death, SYN Flood, Land Attacks, IP spoofing, and other Denial of Service Attacks.
- Supports URL keyword Filtering. Maximum of 10 keywords with each of size up to 32 characters.
- Facilitates web-hosting or any such service on your LAN PC for access from the Internet.
- Supports Universal Plug-n-Play.
- Easy configuration through a Web Browser from any PC connected.
- Administer and Upgrade your Gateway Firmware remotely over the Internet.
- Provide various Diagnostic tools such as ping – to find connectivity to particular computer on the Internet, Trace Route – utility to record route between Gateway and specified destination computer on the Internet and Name Resolution – Find the IP address of the given domain name.
- Configure your Gateway as DHCP server to serve your internal network.
- Supports synchronization of time with Internet real-time servers.
- Supports event Logging, statistics.
- Gateway User can block specific internal user's Internet access with filtering.
- Supports DHCP, PPPoE and PPTP Internet connections.
- Facilitates QoS support that guarantees quality for high priority traffic like voice.
- Supports multicasting.
- Supports soft-reboot.
- Factory-set firewall policies to allow commonly used applications.
- Provides comprehensive security wireless access point based on IEEE 802.11i standard. It provides robust wireless security by protecting wireless users against rogue access points.
- Acts as DNS server to the internal network.
- Allows hosting of Web and other server's and supports Dynamic Domain Name Service (DDNS) using dyndns protocol.
- Port Triggering, Port forwarding and default host configuration security feature.

LANs and WANs

Your DIR-430 is a network device that connects two networks; Local Area Network (LAN) (the group of PCs in your home or office) and the Wide Area Network (WAN), that is, the Internet. The Gateway processes and regulates the data that travels between these two networks.



Your DIR-430 is "equipped" with firewall software that protects your local area network of PCs so that users on the Internet cannot hack into your PCs, hence keeps your local PCs secure. The DIR-430 protects your network by inspecting the first packet coming in through the WAN connection before delivery to the final destination on Local PCs. The DIR-430 inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate PC on the LAN side.

DIR-430 ports connect to two sides: your 10/100 LAN ports and the Internet WAN port. The WAN and LAN ports can transmit data at 10 Mbps or 100 Mbps.

Static & Dynamic IP Addresses

IP stands for Internet Protocol. All IP based network devices like PCs, print servers, Gateways, and routers have IP addresses that are independent of the type of network interface. The IP address denotes the identity of the device on the IP networks, both LAN and WAN. IP addresses can be assigned manually to a device, or dynamically through a central server.

Static IP address is a fixed, and manually assigned to a PC or any other device on the network. They retain their address until you change it. This type of addressing is useful especially for the hosts/routers/Gateways that offer services (Web, FTP, printer), and you may want to access them using their known static IP address. If your ISP provides with static IP address, please use the static IP settings for the Internet Access Connection Mode.

Dynamic IP address is assigned for temporary usage, issued by a server (DHCP Server can be PC, Gateway or any other network service) in the network. The IP address obtained this way is not guaranteed to be constant. After a certain time period, they expire and may change. The DHCP server is notified of the expiry, and may assign the same or different IP address to a network device. This is used in the cases; where there is a constraint on the number of IP addresses, or to reduce the configuration on the network devices and keeping the IP addressing configuration centrally located.

For DSL connections, many ISPs may require you to log on with a user name and password to have access to the Internet. The technology used is Point-to-Point Protocol over Ethernet (PPPoE), which is similar to (PPP) dial-up connection, with no telephone number dialling involved, provides dynamic IP address.

Firewall – Its need

With a rapid growth in the Internet around the world, and because of its open nature of the Internet Protocol standard, network security has become a major concern to the companies around the world. Once you are connected to the Internet, you are physically connecting your network to few thousands of unknown networks and their users. This enables all the Internet users around the world to share the information. But the idea opens up the possibility of confidential information being leaked out to Internet users who are involved in unlawful activities.

There are various types of attacks on the Internet; few for example, Denial-of-service attacks, SMURF, SYN flooding, ping of death attacks, Application layer attacks. To protect a private network from all these type of attacks, firewall came into existence. Your RGS Pro Gateway has firewall that provides a single point of defence between two networks and can secure your Local Network.

Chapter 2 Getting to know the DIR-430

The DIR-430 Back Panel

WAN Port: The WAN (Wide Area Network) port is where you connect your cable or DSL modem through an Ethernet Cable.

Your DSL/Cable modem connection must be connected only to this port.

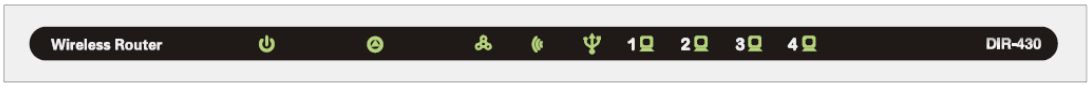
LAN Port: The Local Area Network port is where you will connect networked device such as PC, Laptop, switch, hub and anything other network element you want to put on your network.

USB Port: The USB port is reserved for future usage.

Power: The port to which you will connect the power adapter.

Reset: Explain the Reset button activity.

The DIR-430 Front Panel



Power: The Power LED will be solid when the DIR-430 is powered on.

Status: The Status LED will blink to indicate readiness.

Internet: The Internet LED will illuminate when connected to the Internet.

WLAN: The WLAN LED will blink to indicate WLAN function.

USB: The USB LED will illuminate to indicate a good USB connection.

LAN 1-4: The LAN1 LED will illuminate when connected and blink with activity

Chapter 3 Connecting the DIR-430

Overview

DIR-430 setup requires little more than Hub or Switch setup. PCs on your local network should be configured to obtain an IP address (or TCP/IP address) from the DIR-430 (the DIR-430 also needs to get an IP address). Please consult your Internet Service provider (ISP) for the method used in getting IP address for the DIR-430.

Connecting Hardware together and booting up

1. Make sure you power down all of your hardware including the DIR-430, PCs, hubs, switches and cable or DSL modem.

2. As in figure 3-1, Connect one end of an Ethernet cable to one of the LAN ports (labeled 1, 2, 3, 4) on the back of the Gateway, and the other end to a standard port on a network device, e.g., a PC, Laptop, hub or switch.

Figure 3-1

Repeat the above step to connect more PCs or Network devices to the Gateway.

3. Connect the Internet Cable from your cable or DSL modem to the DIR-430 WAN port on the back panel, as shown in the figure 3-2. This is the only port that will work for your cable/DSL modem connection.

Figure 3-2

4. Connect the power adapter to the Power port on the back panel of the DIR-430, and then plug the power adapter into a power outlet as shown in the figure 3-3.

The Power LED should illuminate indicating a proper connection to power. If the Power LED fails to illuminate check the connection.

Figure 3-3

5. Turn on the cable or DSL modem and PC or switch.

The DIR-430 hardware installation is now complete.

Chapter 4 Configuring your PCs

This chapter helps you configure commonly used Microsoft Windows computer to be able to communicate with the DIR-430. Users with computers running other operating systems can look through respective user manuals.

Before you try making your PC obtain an IP Address automatically, you need to know the operating system of your PC. This section covers configuration for PCs running Windows 95, 98, Millennium, 2000, XP, and 2003.

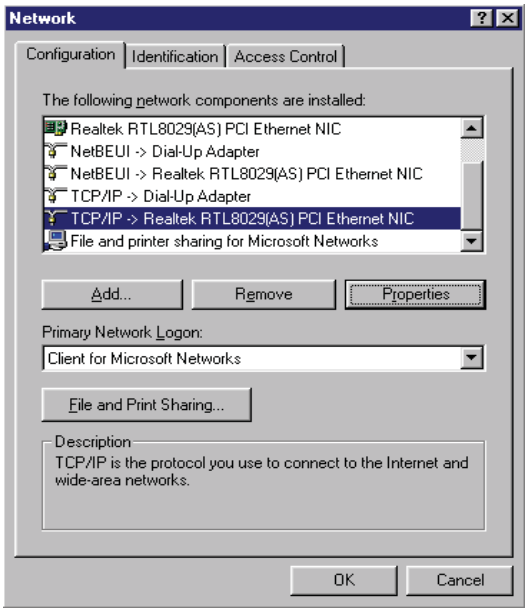
If you are running Windows 95, 98, Millennium, 2000, XP, or 2003 then you can Click on the **Start** button and then go to **Settings** option (does not exist for Windows XP, 2003). Then click on **Control Panel** button to open a window with all the tools.

You may need to do this for each computer you are connecting the DIR-430 through the switch or a hub. If a single PC is connected directly to the DIR-430, then doing it on the PC is sufficient.

The next few pages take you through step-by-step procedure to configure your network settings based on the type of operating system. Make sure that Ethernet card or adapter has been successfully installed in each PC you will configure.

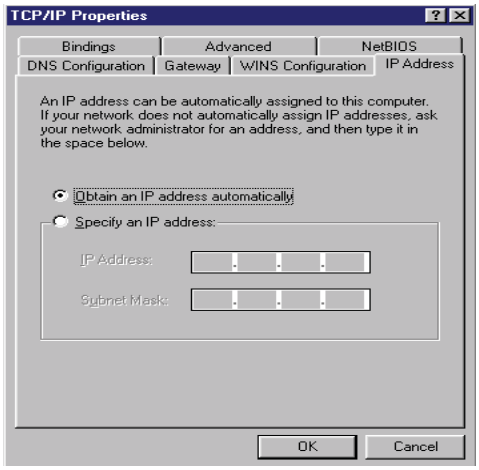
Configuring Windows 95, 98 and Millennium PCs

From the Control Panel window you just opened, double-click **Network** icon.



On the configuration Tab, as shown in **Error! Reference source not found.**, select the TCP/IP for the applicable Ethernet adapter. Do not choose the entries with names DUN, PPPoE, Dialup Adapter, VPN, or AOL. If the word TCP/IP alone appears on a line, select it. Click on **Properties** button. If no TCP/IP line is listed, click on Windows **Start** button, click on **Help** button to open help pages. In the Index tab, type TCP/IP in the edit box. Press Enter key to show you the list of options. Select a topic that is related to installation of TCP/IP and follow the guidelines.

Click on **IP Address** tab and select **Obtain an IP address automatically**, as shown in the figure below.



Click on **Gateway** tab to ensure that the installed gateway field is left blank. Click on **OK** button as shown in the figure on the following page. This closes the **TCP/IP Properties** window.

5. Click **OK** on Network window to be closed. Windows may ask you the original Windows installation disk or CD-ROM. Supply them. Supply them the correct file location, such as c:\windows\options\cabs, D:\win9x (where x is 5 or 8, and D may be your CD-ROM drive)

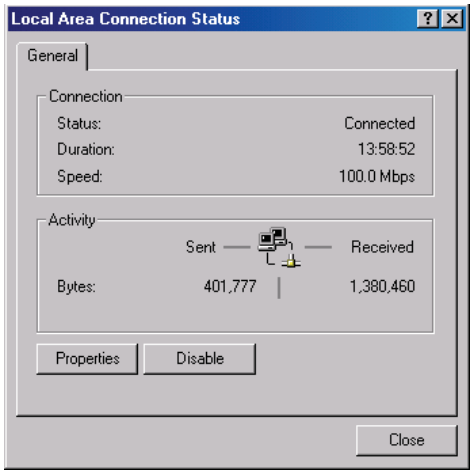
6. Windows may ask you restart your PC. Click the **Yes** button. Even if Windows does not ask you to restart, restart your computer anyway.

Move on to Next Chapter, "Configuring your Gateway".

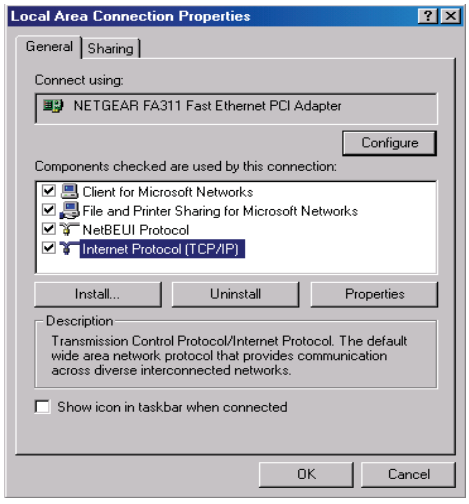
Configuring Windows 2000 PCs

From the Control Panel window you just opened, double-click the Network and Dial-up Connections icon.

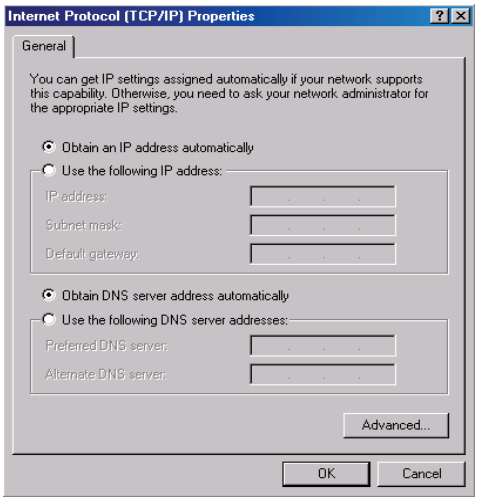
Double-click **Local Area Connection** icon to show Local Area Connection Status Window. Click on the **Properties** button as shown in the figure below.



Click on **Internet Protocol (TCP/IP)** tab and click on **Properties** button. This opens up Internet Protocol (TCP/IP) Properties window as shown in the figure below.



As shown in the figure below, select the radio button, **obtain an IP address automatically**. Then select the button, **Obtain DNS server address automatically**. Click **OK** button to close the window.



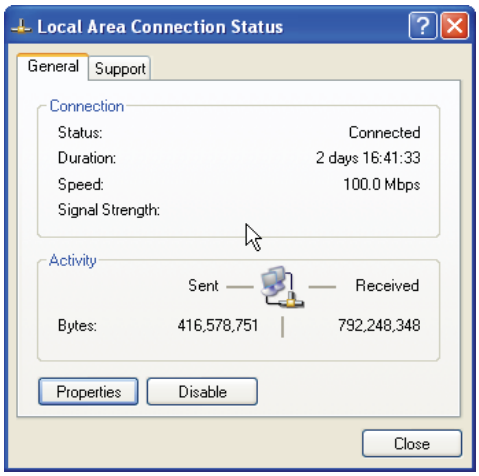
Windows may ask you restart your PC. Click the **Yes** button.

Move on to Next Chapter, "Configuring your Gateway".

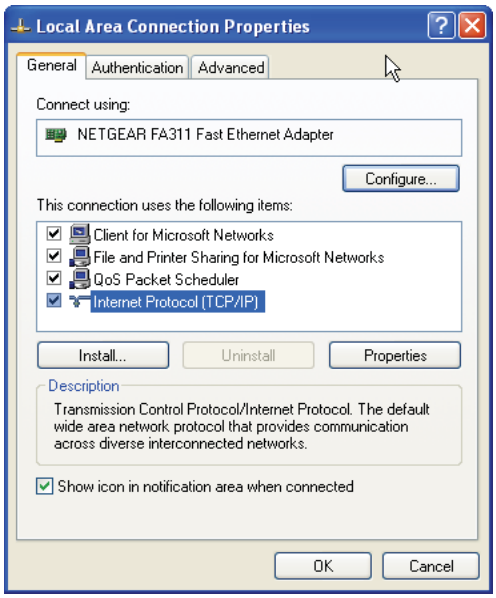
Configuring Windows XP PCs

If the Windows XP has a classic Interface (This has similar user interface as Windows 2000), then follow "Configuring Windows 2000 PCs". The following details in this section are exclusive to Windows XP with default Interface.

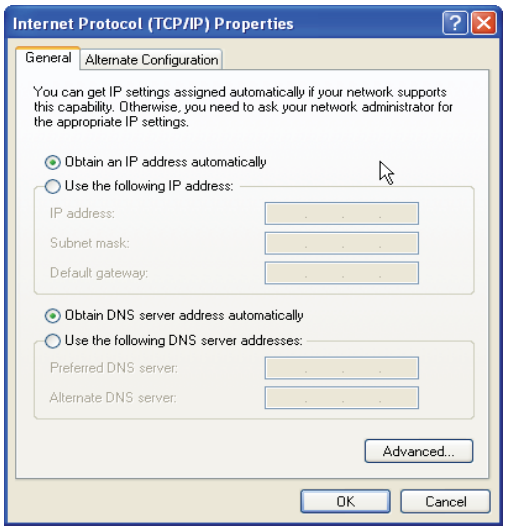
From the control panel window, double-click **Network connections** icon to open different window, where you have to double-click **Local Area Connection** icon. This opens up the Local Area Connection Status window as shown in the following figure.



Click on the **Internet Protocol (TCP/IP)** option, then on the **Properties** Button as shown in the following figure.



As shown in the figure below, select the radio button, **obtain an IP address automatically**. Then select the button, **Obtain DNS server address automatically**. Click **OK** button to close the window.

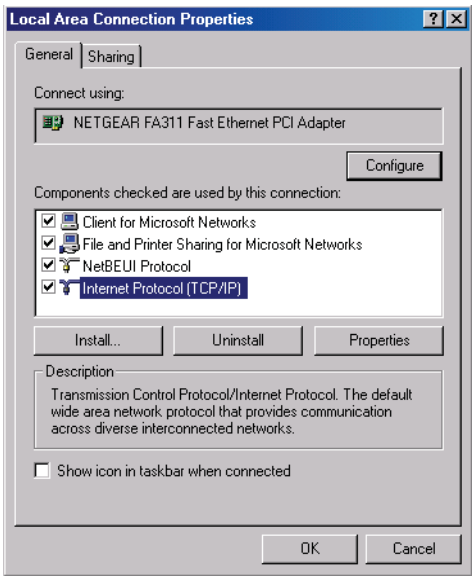


Windows may ask you restart your PC. Click the **Yes** button.

Move on to Next Chapter, "Configuring your Gateway".

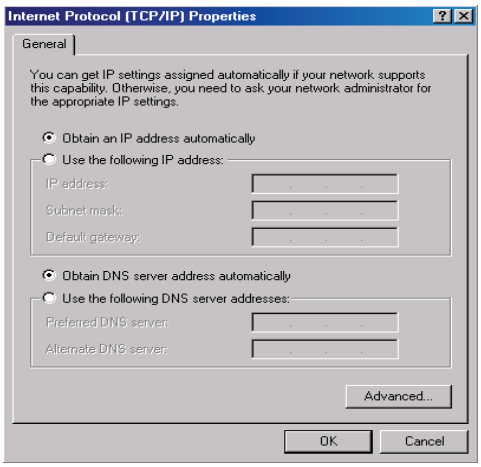
Configuring Windows 2003 PCs

Click on Windows **Start** button would open up a menu, click on **Control Panel** menu to open up another menu, where Network Connections is found. Click on **Local Area Connection** to open Local Area Connection properties window.



On the **configuration** Tab, as shown in the figure above, select the **TCP/IP** for the applicable Ethernet adapter. Do not choose the entries with names DUN, PPPoE, Dialup Adapter, VPN, or AOL. If the word TCP/IP alone appears on a line, select it. Click on **Properties** button. If no TCP/IP line is listed, click on Windows **Start** button, click on **Help** button to open help pages. In the Index tab, type TCP/IP in the edit box. Press Enter key to show you the list of options. Select a topic that is related to installation of TCP/IP and follow the guidelines.

Click on **IP Address** tab and select **Obtain an IP address automatically**, as shown in the following figure.



Click on **Gateway** tab to ensure that the installed gateway field is left blank. Click on **OK** button. This closes the TCP/IP Properties window.

Click OK on Network window to be closed. Windows may ask you the original Windows installation disk or CD-ROM. Supply them. Supply them the correct file location, such as c:\windows\options\cabs, D:\win9x (where x is 5 or 8, and D may be your CD-ROM drive)

Windows may ask you restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer anyway.

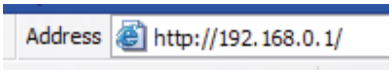
Move on to Next Chapter, "Configuring the DIR-430".

Chapter 5 Configuring the DIR-430

This chapter guides you through the configuration of your DIR-430 to make it function in your network and gain access to the Internet through your ISP.

Accessing the DIR-430 configuration

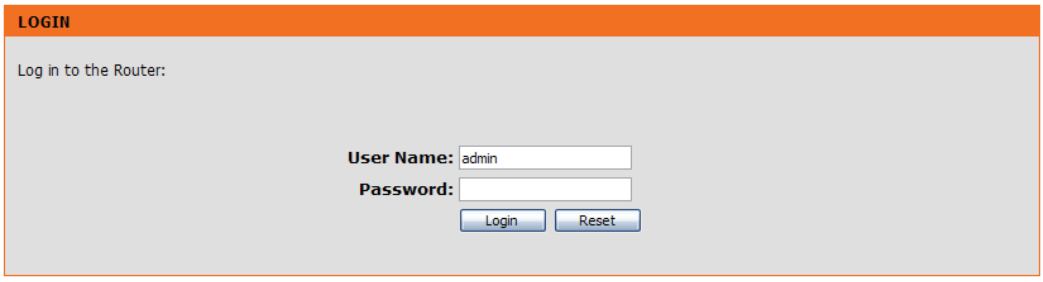
Once connections are made as shown in Section 3 "Connecting the DIR-430", the DIR-430 can be configured using an HTML browser, Internet Explorer 6.0 on your PC. At the address line, enter HTTP URL, http://192.168.0.1/ as shown in the figure below, where 192.168.0.1 is the DIR-430 Internal IP address (You may give different IP address if configured differently, refer to Local Area Network configuration). Subnet mask for all the machines on the local network is 255.255.255.0. All the PCs connected to the Local Network ports can reach the Gateway device at the address specified.



The user is prompted for the username and password for the DIR-430 as shown in the figure below. The default user name is **admin**. The factory setting for the password is **<blank>**. The user is expected to change password (optionally username) to protect the DIR-430 configuration from an unauthorized manipulation. Enter the changed password if it was already modified.

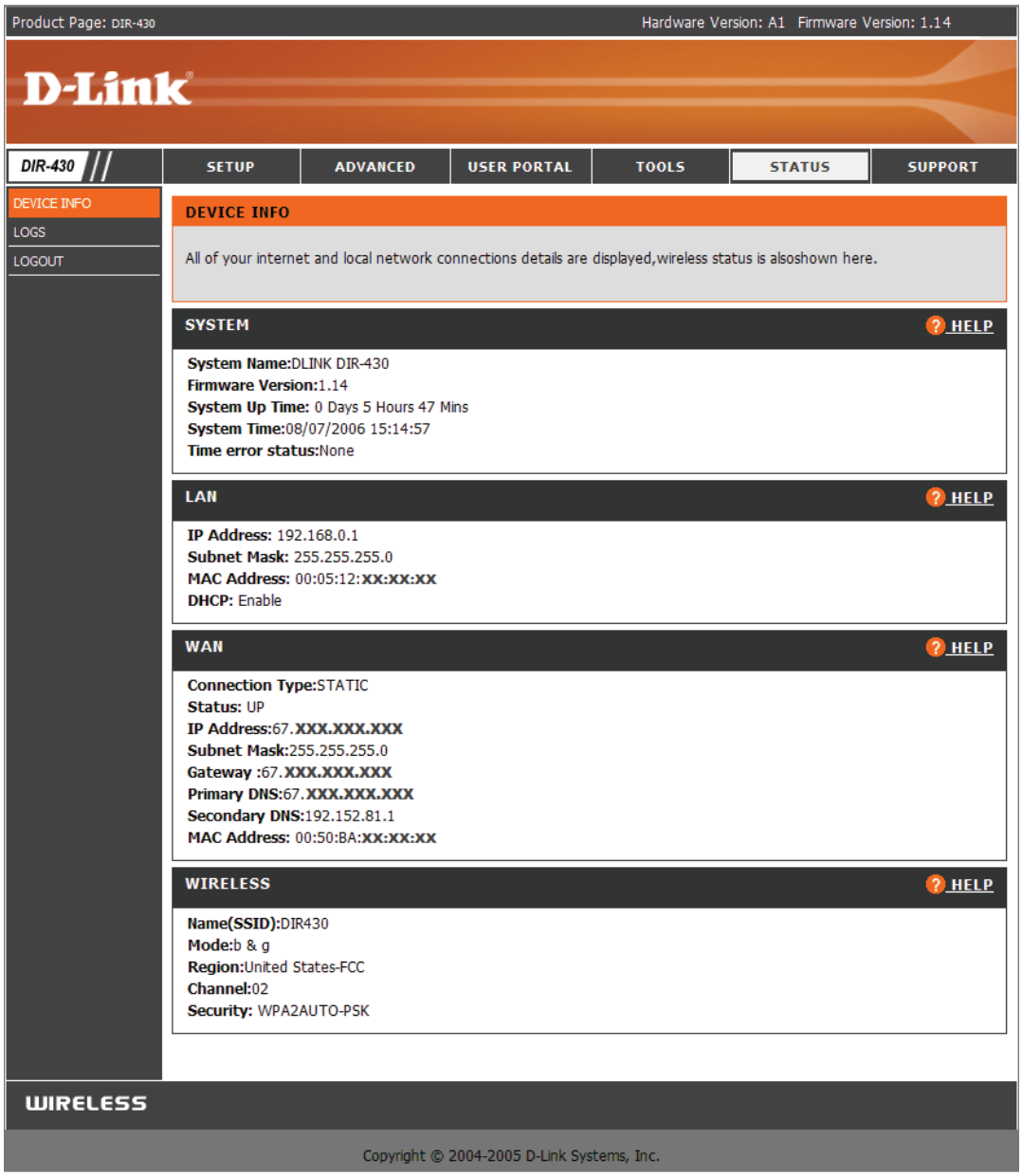
If the username, password combination is entered incorrectly three times, the login session will be locked for a minute. This is for security reasons.

In rest of the document, the term **user** is used for the person who configures the DIR-430.



The **Reset** button on this page clears off the password field for the user to re-enter it. Clicking on **Login** button leads to the DIR-430 configuration welcome page as shown in the following figure.

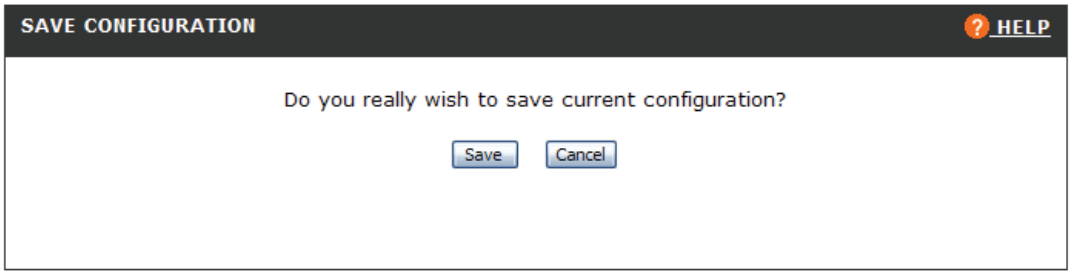
If you enter an incorrect password 3 times consecutively, the DIR-430 configuration pages will be locked for one minute. It is strongly advised to wait for one minute before re-attempting login.



As shown above, the welcome page represents the status of the various parameters of the DIR-430. The Top pane shown in the figure provides the sections of the DIR-430 configuration. The left pane shown in the figure provides the relevant sub-sections of DIR-430 configuration. Each section gets expanded when clicked to show few hyperlinks. Each hyperlink allows you to configure certain parameters of the Gateway.

Saving and Activating the Configuration

The user can save the current configuration to exist after the next reboot irrespective of any configuration changes done to the Gateway. This allows the user to configure the Gateway for customized behavior.



Changes made to the configuration of the DIR-430 will be effective immediately. Once a stable configuration exists on the DIR-430 it should be saved to the non-volatile memory. Click on **Tools** on the top panel and then click on **Save Configuration** on the left hand menu. In the resulting page as shown above, you will be prompted to press **Save** or **Cancel** buttons for saving the configuration.

By pressing **save** button, the configuration will be saved onto the DIR-430 for next reboot overriding the configuration saved earlier. Press **Cancel** button to cancel the operation.

If the DIR-430 is rebooted and the changes that were made prior to reboot were not saved, the DIR-430 will revert to the state of configuration that existed prior to the changes made.

Top Panel

The DIR-430 Management UI Top pane shown in the figure below provides the following categories to make configuration changes.

- Setup
- Advanced
- User Portal
- Tools
- Status
- Support

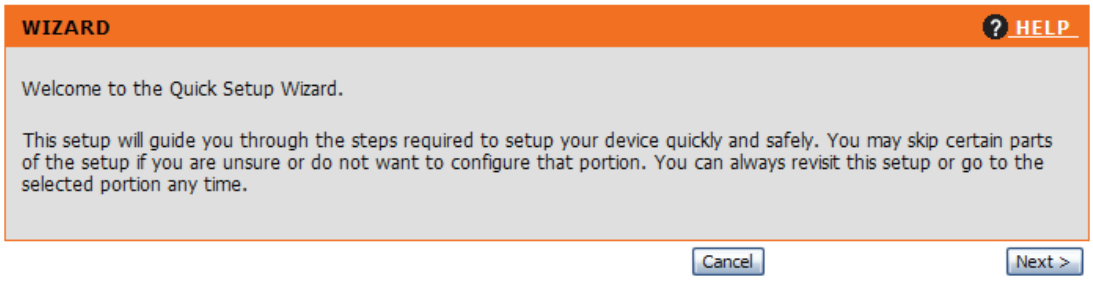
Setup

From the DIR-430 configuration home page, find the Setup hyperlink on the Top Panel of the DIR-430 Management UI. The Setup section contains configuration options pertaining to the Network Interfaces (WAN, LAN and Wi-Fi) as well as a link to the Quick Setup Wizard.

Quick Setup Wizard

If this is the first time logging in to the DIR-430 Management UI you will see the Wizard Page, which allows the Quick Setup Wizard to be run.

The Quick Setup Wizard will allow you to configure the administrator login and password, the Time and Date Settings, MAC Cloning, and Internet Connection Settings. You may skip certain parts of the configuration if you are unsure or do not wish to make changes to that portion. You can always revisit the setup or go to the selected portion any time.



WAN

The WAN section allows the configuration of Internet Connection Settings. Internet Connection types supported are: Static IP, Dynamic IP, PPPoE, and PPTP. Contact your ISP for specific information regarding the type and parameters needed for your broadband Internet Connection.

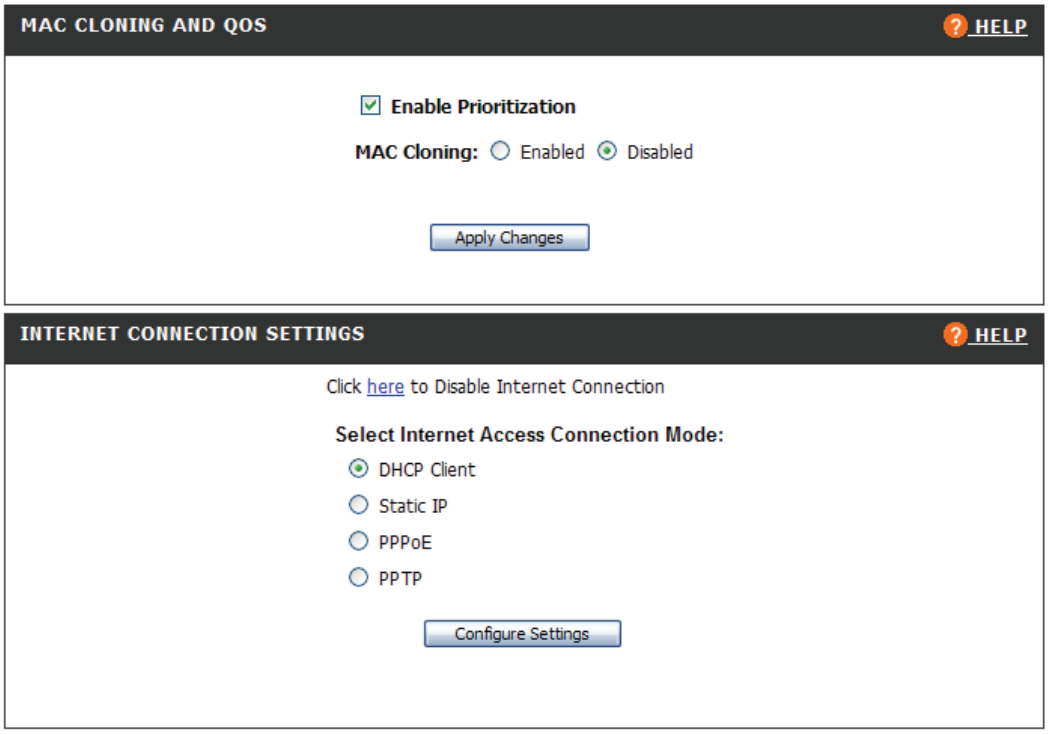
WAN Page configurations:

Prioritization – Enable or Disable

Mac Cloning – Enable or Disable

Internet Connection – Enable or Disable

Connection Type – Static, DHCP, PPPoE, or PPTP

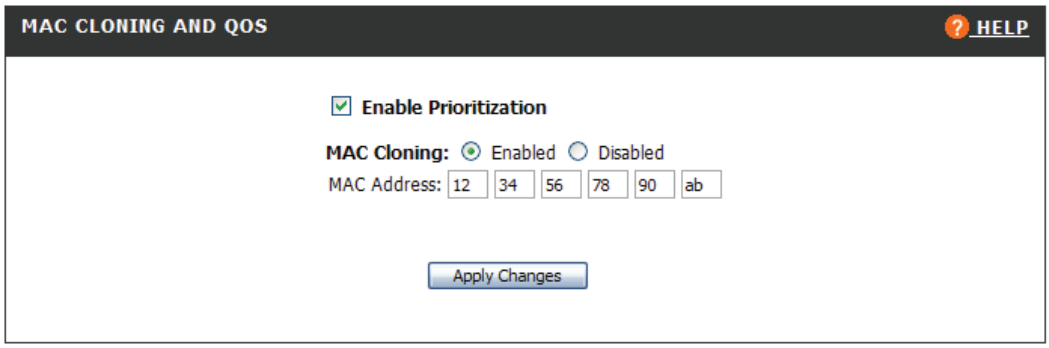


Prioritization

Prioritization will streamline traffic bound for the Internet based on configurations made in the Network Filter Section (within the Advanced Configuration Menu). In order for Prioritization to work properly you must know the Uplink Bandwidth of your ISP connection. Prioritization may be enabled or disabled on the WAN page.

MAC cloning settings

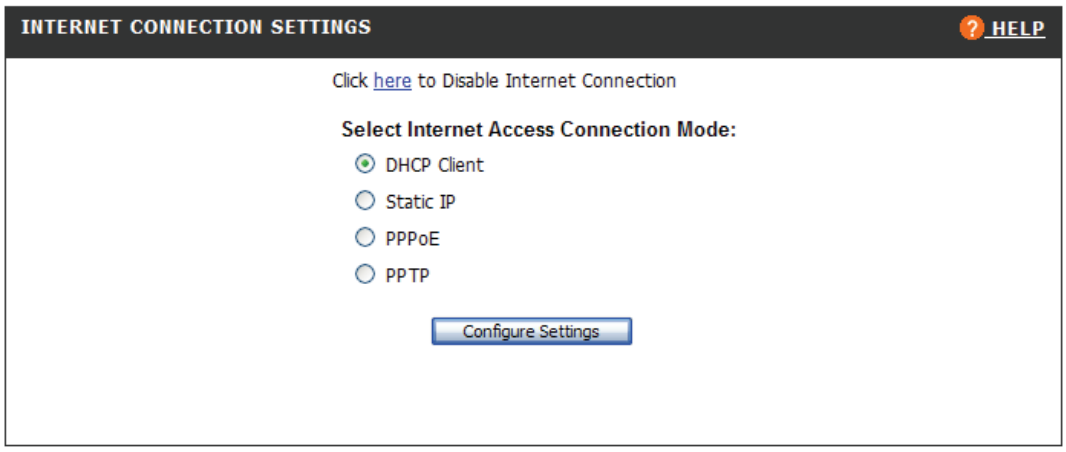
Some times, the Internet Service provider requires your PC and its hardware address to be registered with their network. Typically, they provide with an installation CD with software to be installed on your PC. ISP once registers the MAC address, allows the Internet access only to the computer with the hardware address (MAC) it registered. To make ISP transparent about your DIR-430, you have to clone your PC's MAC address on to your DIR-430. This allows the DIR-430 to use cloned MAC address to communicate to ISP.



Internet Connection Settings

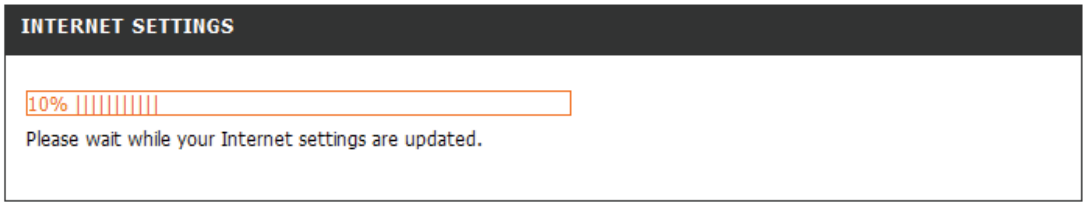
The DIR-430 allows you to access the Internet in four different ways: DHCP, Static IP, PPPoE, PPTP protocols as shown in below. DHCP is the default protocol for the DIR-430 to access the Internet.

Connectivity to the Internet may be disabled on the WAN page (if connected).



DHCP client

If the option selected is DHCP client, the DIR-430 tries to get the IP address automatically from the Internet. This requires a DHCP Server running on the network connected to your Internet Port. You should not disturb the configuration while the progress bar is displayed on your browser.

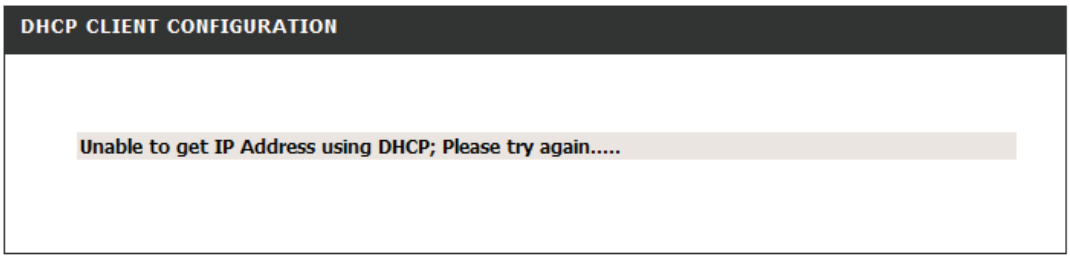


Once successful, your quick setup is complete. You are ready to use the Gateway. Proceed to **Advanced Configuration** section in this document for custom control over the Gateway.

Once DHCP client successfully receives the IP address from the ISP, the HTML configuration displays IP address information as shown in the following image.

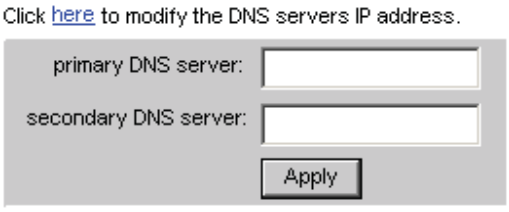
Insert pic here

In case the Gateway fails to get an IP address, it shows an error on the screen. You may press **<Previous** button and try again, or change the mode of the Internet access setting.



MAC cloning is disabled by default. Please see Section on MAC cloning if required.

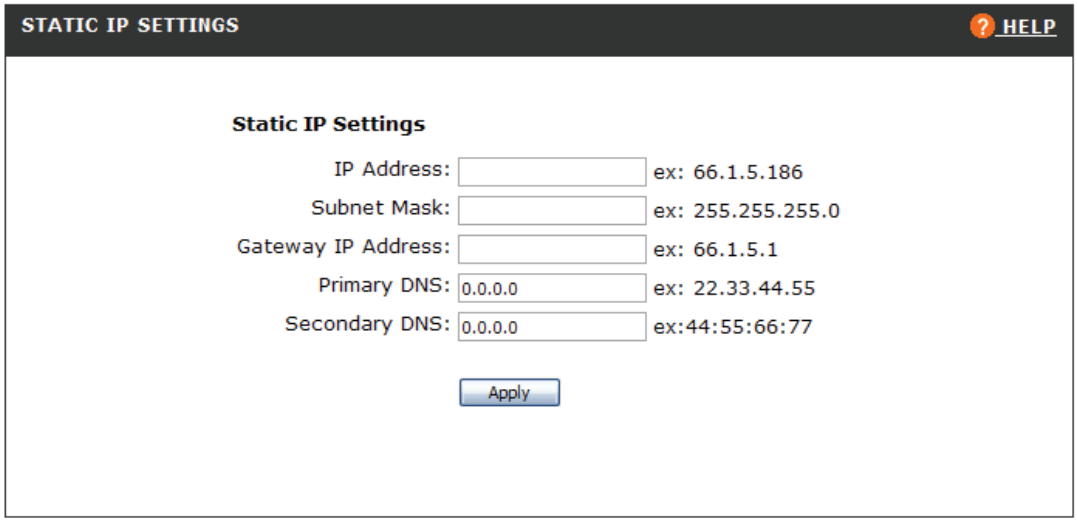
After the DIR-430 gets the new IP information, you are allowed to change ISP served DNS server IP addresses at any time by clicking here hyper-link. Once you click on the hyper-link, it is prompted to enter new DNS server IP address as shown below.



This facility helps you add custom DNS servers, or if ISP doesn't not provide DNS server information.

Static IP

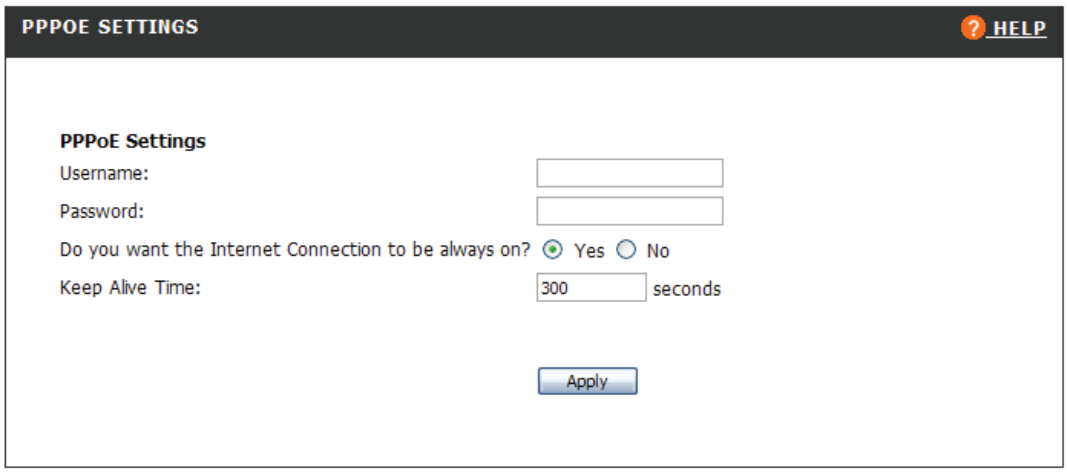
User can choose to set the External Network address to be static IP address, when the ISP offers you static/permanent IP address through a cable modem, DSL or a dial-up connection. The IP address does not have to change upon the rebooting of the device. As shown in the figure below, fill in the details, IP address, subnet mask and Gateway IP address as given by ISP.



PPPoE

Some DSL service providers use PPPoE (Point-to-Point Protocol over Ethernet) for Internet access for their end-users. Please check with your ISP whether PPPoE is used for your Internet access. Provide PPPoE user name, password given by your ISP in the configuration page as shown below.

Once configured, the DIR-430 is always connected to the Internet. If you would like to have Internet access to be available only on Demand, you can select the option "Connect on Demand" on this page. By default, the Maximum idle time allowed before the Gateway disconnects the Internet is 10 seconds. You may configure your own value.



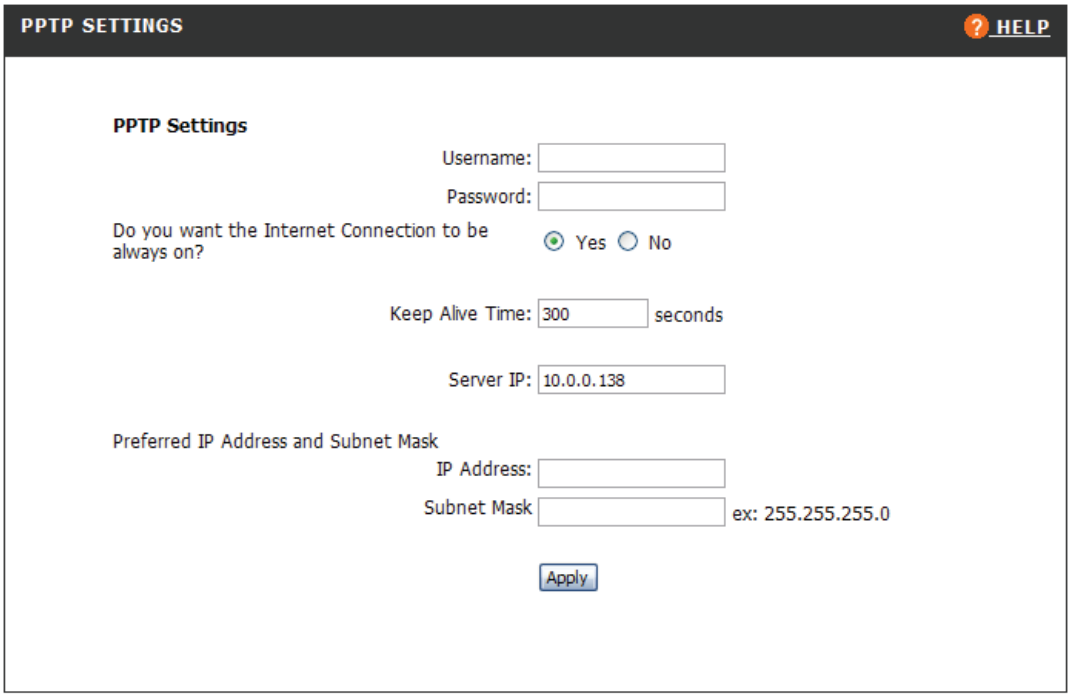
Your Gateway periodically checks for the Internet connection, for every **Keep Alive Time**. If your Gateway finds the Internet connection does not exist, it re-establishes the connection. The default period the Gateway verifies the Internet connection is 30 seconds. You may configure it to a different value.

PPTP

As the name indicates PPTP does tunnel the PPP (protocol used for dialup Internet connection) packets over IP network. Some ISPs use this protocol for a secured connection establishment. Please check with your ISP whether they are supporting PPTP connections.

As shown in the figure below, provide the PPTP user name and password provided by your ISP.

Once configured, the DIR-430 is always connected to the Internet. If you would like to have Internet access to be available only on Demand, you can select the option **No** for the question, **Do you want the Internet connection to be always on?** on this page. By default, the **Maximum idle timeout** allowed before the Gateway disconnects the Internet is 10 seconds. You may configure your own value.



The DIR-430 periodically checks for the Internet connection, for every **Keep Alive Time**. If the DIR-430 finds the Internet connection does not exist, it re-establishes the connection. The default period the DIR-430 verifies the Internet connection is 300 seconds. You may configure it to a different value.

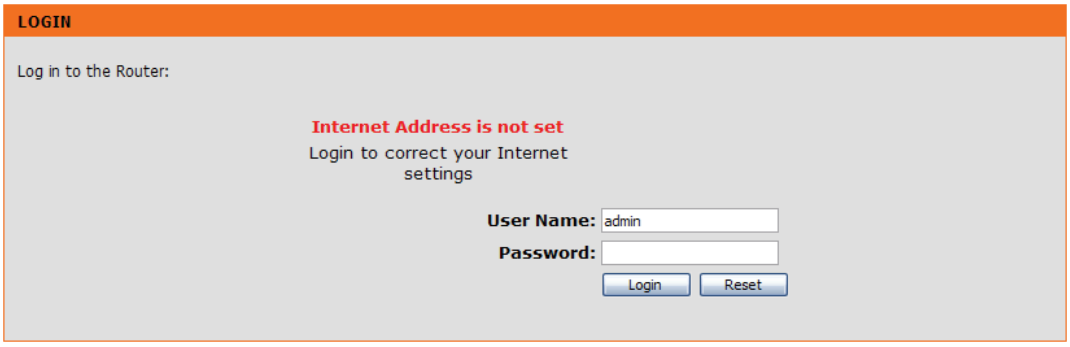
User account info is also required get PPTP server IP address information from ISP, and place it in the field. WAN IP and WAN subnet mask information can be obtained from Internet Service provider.

Internet Failure Detection

Your Gateway is intelligent enough to detect Internet connection failure automatically. While browsing the Internet using Internet Explorer, if the DIR-430 finds any problem with Internet connectivity, your browser will display the appropriate error page on the screen.

For example, if Internet cable is physically disconnected while you browse Internet, an error message is displayed on your HTML browser as shown below.

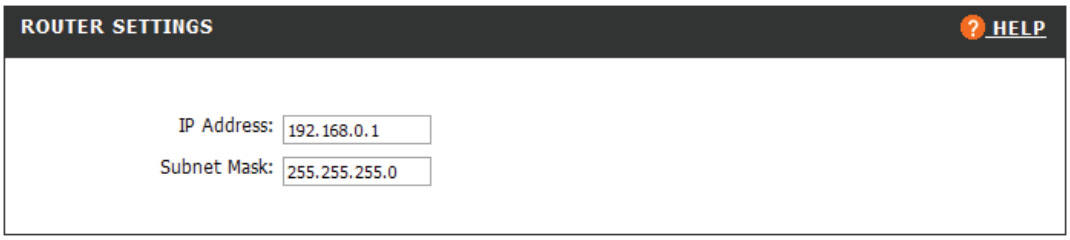
Also, if your Gateway is not configured for Internet address, it redirects your browser to Gateway configuration that allows you to set Internet address through **Quick setup wizard** after the logging into the Gateway configuration page as shown below.



Local Area Network

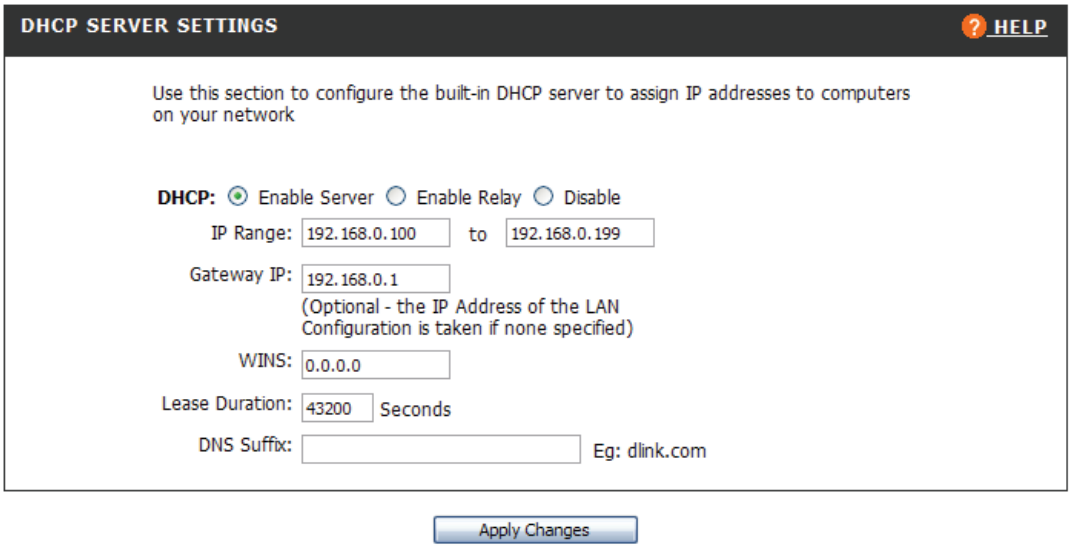
Router Settings

The DIR-430 by default has a LAN IP address of 192.168.0.1. This may be changed to any address within a Class C Network (except the Network or Broadcast Addresses).



DHCP Server

By default, the DIR-430 is already set to offer IP addresses for machines on the local network automatically. If you would like to change the configuration of Gateway for DHCP server, click on **Setup** on the top pane, and click on **LAN** to show the DHCP server related configuration as shown below.



The default configuration is shown above when you open this page for the first time. User may restrict the range of the IP addresses offered.

Gateway IP address should be specified same as the internal IP address of the DIR-430 (192.168.0.1 by default).

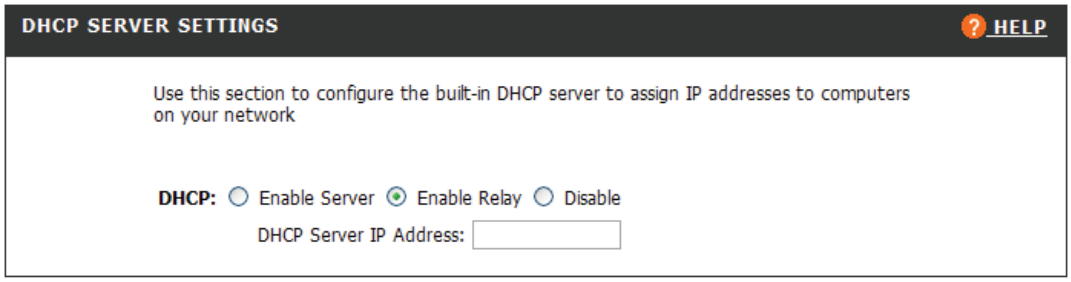
You may specify **WINS** server IP address, which handles DNS requests on the Local network for Microsoft PCs. **Lease duration**, is the time of the IP address to be offered for a PC.

You may view the local PCs that are issued dynamic IP addresses by the DIR-430.

User may disable DHCP server and manually configure IP addresses for machines on the local network.

DHCP Relay

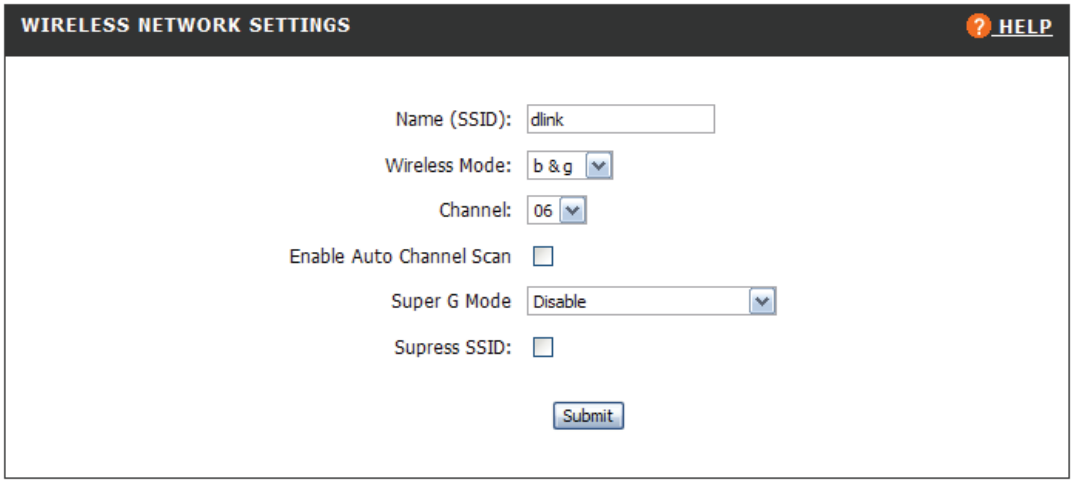
Sometimes, you may require getting IP addresses from a DHCP server on your WAN connection (may be Internet). To do so, you should enable DHCP relay feature so that the DIR-430 Provides bridging between your LAN and WAN for DHCP.



To configure the DHCP relay, click on Setup hyperlink on the DIR-430 configuration pane, and then click on Local Area Network hyperlink. This opens up the configuration for DHCP relay as shown in the above. Select the radio button, Enable Relay and enter the DHCP server IP address running on WAN.

Wireless

The DIR-430 can act as a wireless access point for wireless clients (PCs or laptops with wireless network cards). The image below shows the wireless network settings page. To access it, click on **Setup** hyperlink in the top panel, and then click the **Wireless** hyperlink.



Server Set Identifier (SSID): This is a string that will identify the service set started by this Gateway or other way called as wireless Access Point. All wireless client stations that wish to associate with this Access Point have to use the SSID that is configured here. The SSID will be a unique identifier for the wireless network.

It is advised to change the SSID name from the default to any other SSID to avoid security problems. Attackers can use this default SSID to attempt to penetrate. Use SSID something unique-not something easily guessed. Also advised to change SSID periodically.

Wireless mode: Describes the wireless mode of operation, and their capabilities that used at Access Point, which will be one of 802.11b or 802.11 g based on the card that is attached internally on your board.

Channel: Select channel to be used for the wireless network to communicate. The available channels supported by the wireless products in various countries are different. For example, Channels 1 to 11 are supported in the U.S. and Canada, and Channels 1 to 13 are supported in Europe and Australia. Based on the region in which the DIR-430 was purchased you will be displayed the channels allowed in that area in the drop-down menu.

Enable Auto Channel Scan: The DIR-430 can be configured to automatically select the best wireless channel on start-up. The DIR-430 will scan all available channels and choose the channel with the least amount of interference every time the router is rebooted.

Super G Mode: The DIR-430 supports D-Link's 108G Wireless mode for High-speed wireless client connections. To fully realize the performance potential of the included Super G modes it is necessary to have a D-Link 108G wireless client on the laptop or PC connecting to the DIR-430. Super G without Turbo will enable non-108G wireless clients to connect to the DIR-430 and see performance improvements. Super G with Dynamic Turbo will enable D-Link 108G wireless clients to maximize their Wi-Fi link when extra bandwidth is needed.

Suppress SSID: By default the DIR-430 broadcasts the SSID of the Wireless Network (wireless access point) at a regular interval; this is useful for mobile hotspots. Any wireless station wishing to connect to your Gateway can use this SSID for connection establishment. However it increases the likelihood of an unwelcome neighbour or hacker who can try to log in to your home network.

It is better advised to turn on the suppression of the SSID, by checking on Suppress SSID check box.

Wireless Security Mode

Wireless networks need to provide an extra level of security compared to wired networks. This is because wireless radio signals propagate through the air and are naturally easier to intercept.

You may wish to leave your wireless connectivity without any security settings, but this is not advised. Select "Disable Wireless Security" from the drop down menu if you do not wish to have security between clients and this access point.

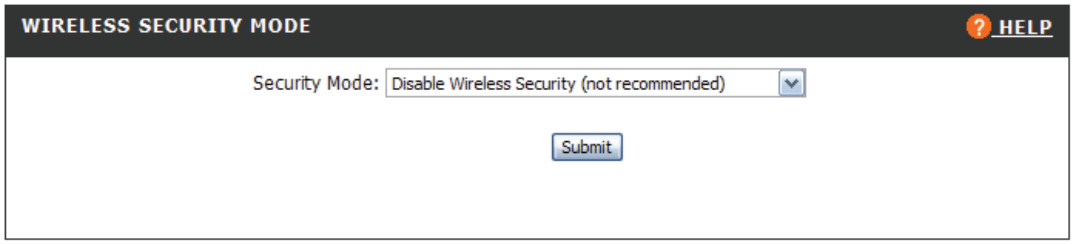
The DIR-430 supports the following types of wireless security to encrypt your data so that only the intended recipient will be able to read it.

WEP (Wired Equivalent Privacy)

WPA PSK (Wi-Fi Protected Access – Pre-Shared Key)

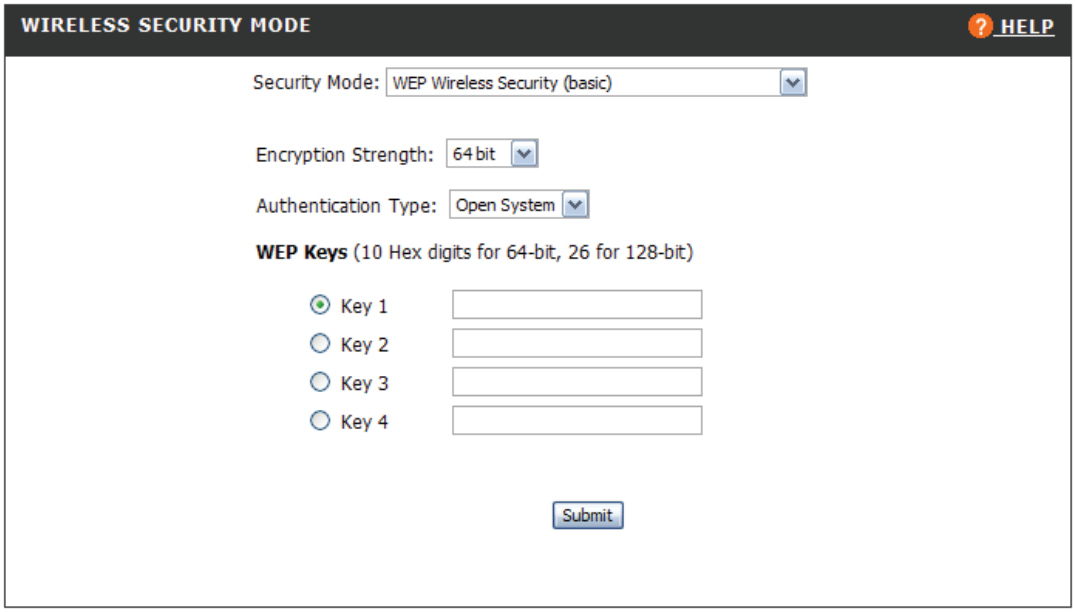
WPA2 PSK (Wi-Fi Protected Access version 2 – Pre-Shared Key)

WPA/WPA2 PSK (Accepts both WPA and WPA2 PSK connections)



WEP Wireless Security

WEP is the first generation wireless security. The figure below shows the WEP configuration information. You should choose the encryption bit length from the drop-down menu from one of the 64, 128 bit lengths. The more the bit length, the higher the security offered.



Authentication Type: Select "open system" or "shared key".

Open system authentication is a very basic form of authentication that consists of a simple authentication request containing the station ID and an authentication response containing success or failure. Upon success both stations are considered mutually authenticated.

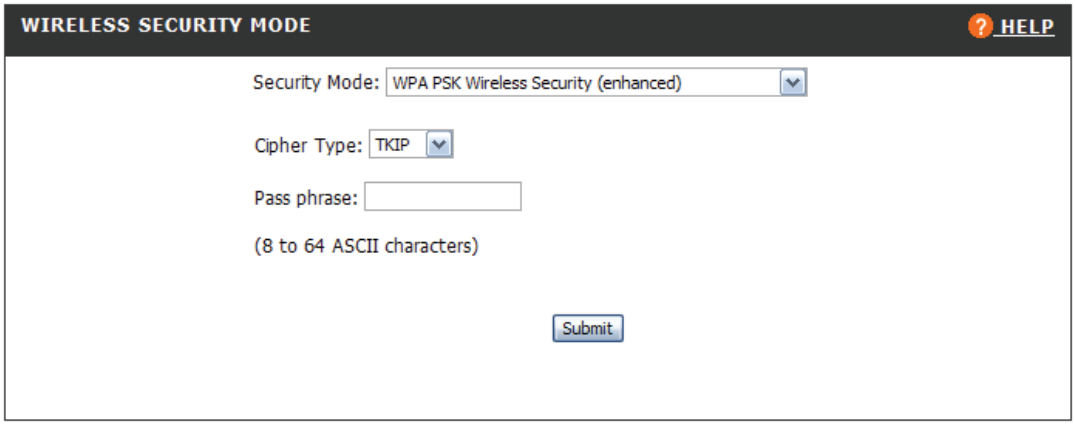
Shared key authentication is predicated on the fact that both stations taking part in the authentication process have the same "shared" key. It is assumed that the secret key has been distributed to both the transmitting and receiving stations by some secure means.

If you wish to allow access to the wireless PCs/laptops/PDAs based on their type, you may choose "automatic" entry from the drop-down list.

Keys specified on the configuration are useful in encrypting between your gateway and its wireless clients. You may specify 10 hex digits (0-9, A-F or a-f) if you selected 64-bit encryption key length, or 26 hex digits if selected 128-bit encryption key length. If the authentication type is shared, the keys are also used for the authentication. You can have four keys that can be configured between your access point and its wireless clients. Select a key to be used for encrypting/authenticating the wireless traffic.

WPA PSK (Wi-Fi Protected Access – Pre shared key)

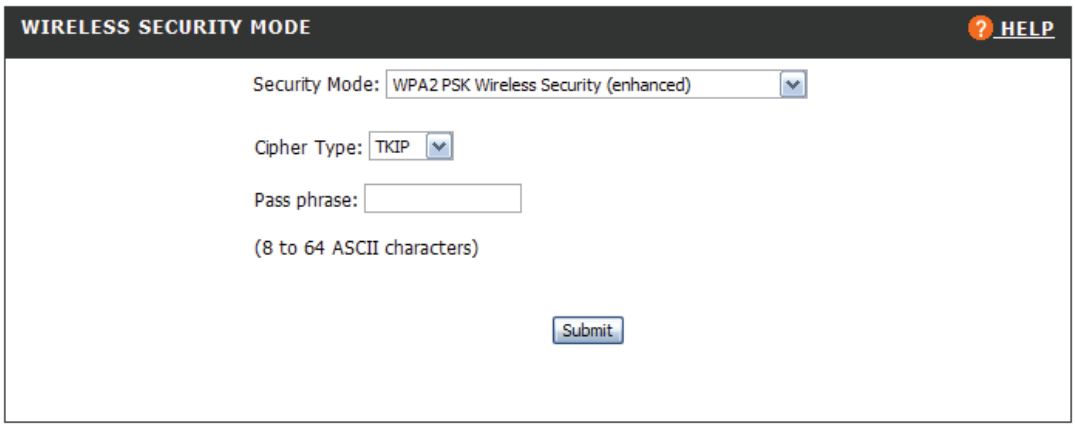
WPA is the second-generation wireless security. WPA's wireless security provides far greater protection than WEP. It avoids most of WEP's vulnerabilities.



The figure above shows the configuration for WPA under pre-shared key mode. Submit the pass phrase, which can have 8 to 64 characters. All the valid wireless clients must have the network key configured so as to associate to your access point.

WPA2 PSK (Wi-Fi Protected Access version 2 – Pre shared key)

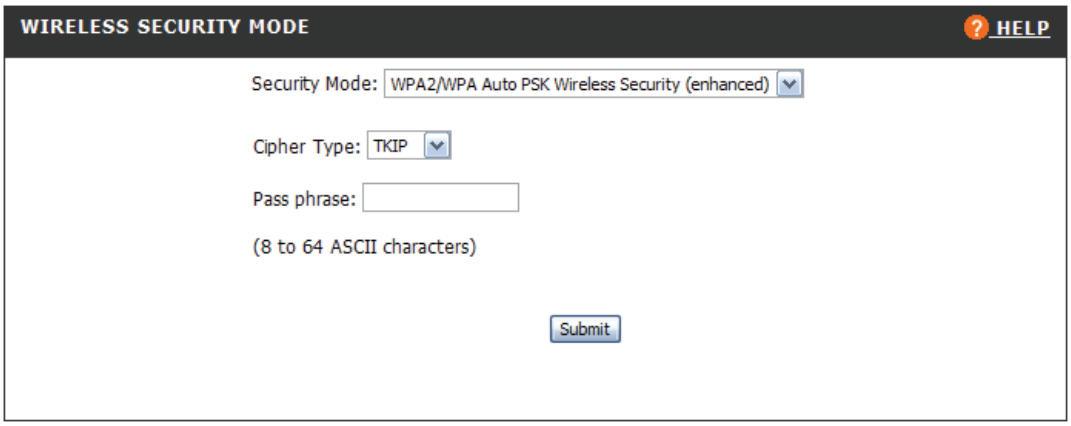
WPA2 is the third-generation wireless security also known as IEEE 802.11i. WPA2's wireless security provides far greater protection than WEP or WPA. It avoids most of WEP's vulnerabilities. It is also backward compatible with WPA clients.



The figure above shows the configuration for WPA under pre-shared key mode. Submit the pass phrase, which can have 8 to 64 characters. All the valid wireless clients must have the network key configured so as to associate to your access point.

WPA/WPA2 PSK (Accepts both WPA and WPA2 PSK connections)

The DIR-430 can accept both WPA and WPA2 PSK connections simultaneously allowing the use of the more advanced WPA2 without forcing client upgrades of legacy devices supporting only WPA PSK.



The figure above shows the configuration for WPA under pre-shared key mode. Submit the pass phrase, which can have 8 to 64 characters. All the valid wireless clients must have the network key configured so as to associate to your access point.

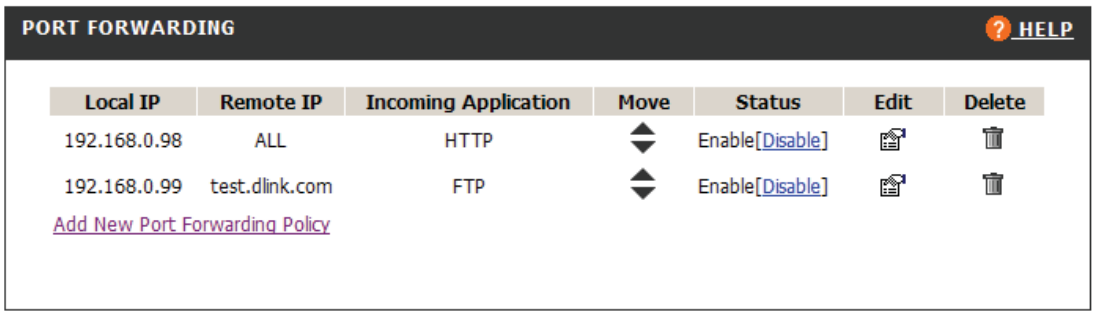
Advanced

The Advanced Section of the DIR-430 management UI allows administrators to configure various Networking parameters relating to LAN based Servers and Access Control. Refer to each section for more information.

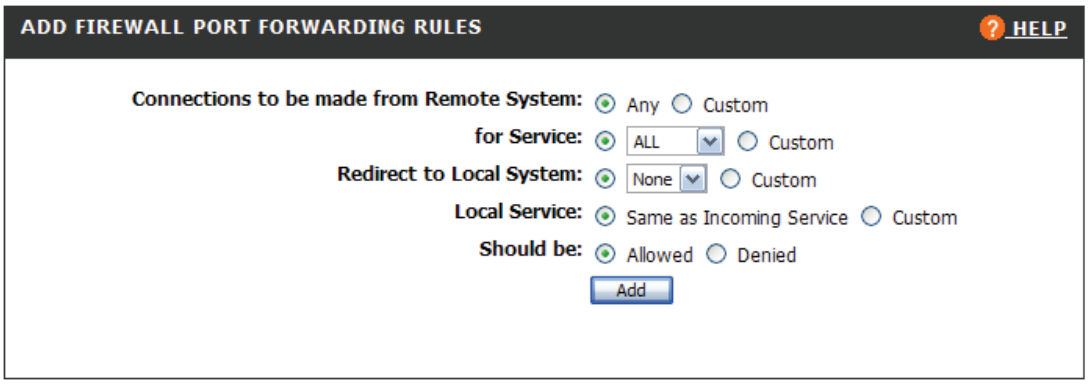
Port Forwarding

With this feature, you can setup services like web servers, file servers, e-mail servers, and any other customized applications to the Internet on internal PCs. To give access from the Internet, add a policy to allow the traffic initiated from Internet to internal network (inbound traffic). This uses Reverse Network Address Translation (RNAT) to forward specified ports from the WAN to the LAN.

To add a policy, click on **Advanced** on the top panel, and click on **Port Forwarding** to open up the page as shown below.



To create a new rule for inbound traffic, click on Add New Port Forwarding Policy button on the page shown above that will lead to the configuration page as shown in below.



The Port Forwarding configuration requires you to provide:

Connections from Remote Systems: Specify the remote host IP address, domain name, or IP range (select **Any** radio button if required for all machines) from which the Internet traffic is generated.

For Service: A pre-determined service from the drop-down list or specify port range (if only one port exists, provide duplicate entry) with transport protocol (TCP/UDP).

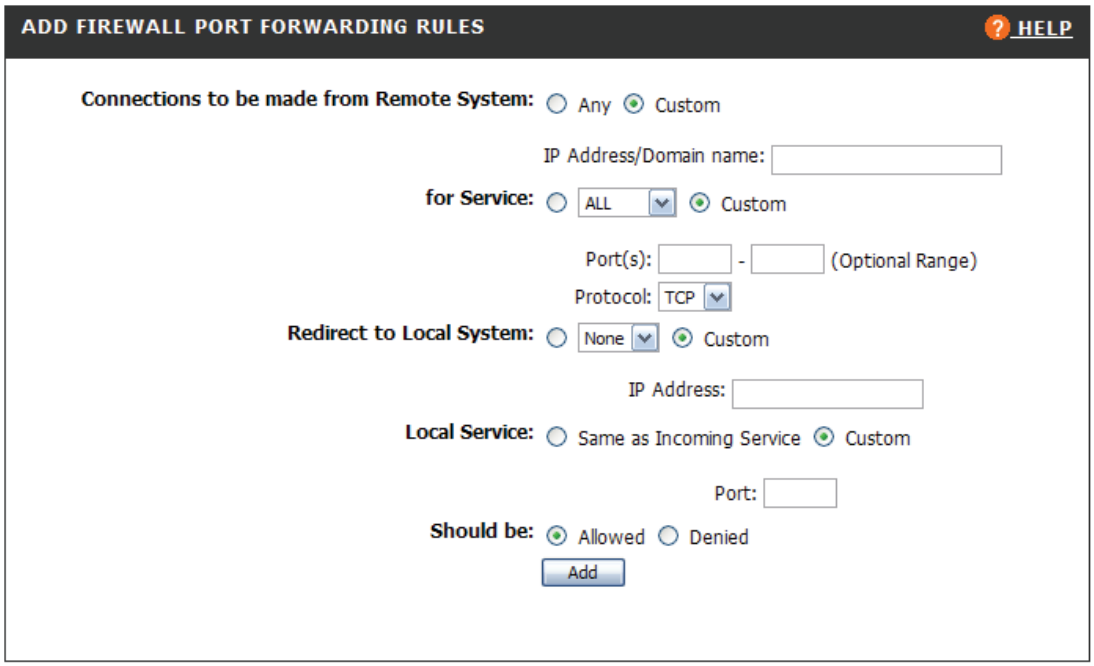
Redirect to Local System: The local host IP address to which traffic is destined from the Internet. Select the PC from the drop down box or choose the Custom radio button and specify its IP address.

Local Service: The local service allows for Port Translation for incoming services. If the local PC is running the desired service on a port that is different from the WAN port being forwarded choose Custom.

Should be: Select Allowed to allow traffic matching this policy or Denied to block traffic matching the policy.

Click **Add** button, to add the new Port Forwarding Policy.

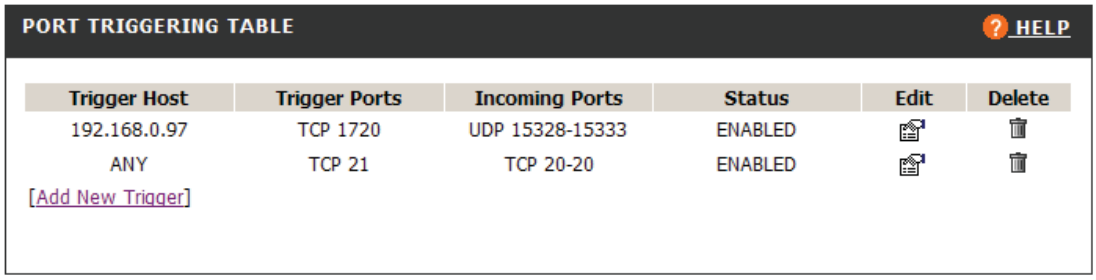
The Port Forwarding Policy is applied by the DIR-430 to the Internet traffic. If the rule matches, the traffic is directed to the specified internal pc, otherwise traffic is received by the DMZ host (if enabled).



A PC on a private network with an IP address such as 10.X.X.X, 172.16.X.X, 192, 168.X.X cannot be accessed directly by a user on the Internet. To access any PC on the private network, Internet user should use public IP address of the DIR-430 assigned by the ISP on the specified port.

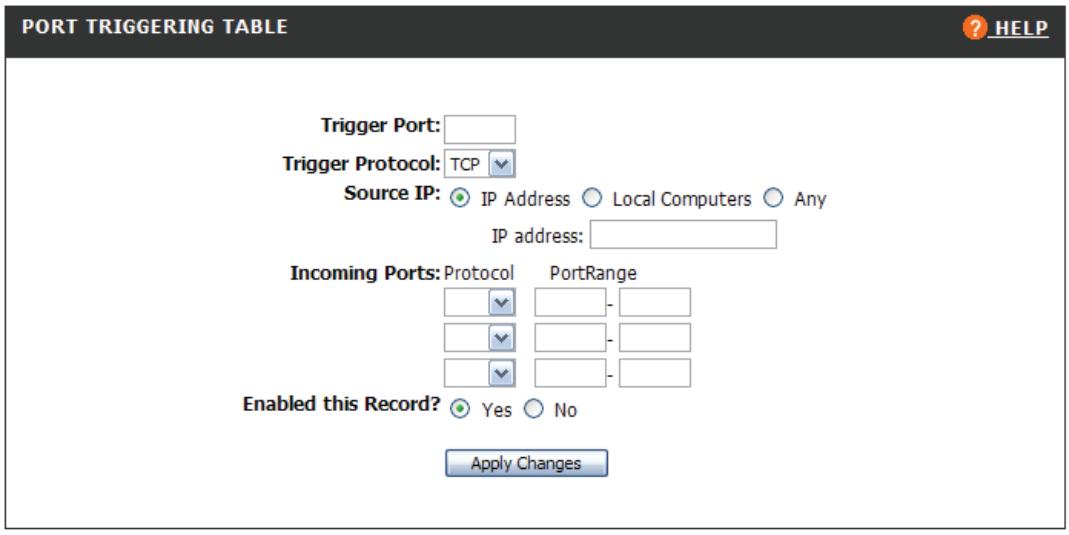
Application Rules

Some complex applications exchange the control information on well-known ports and the control messages may specify some port numbers to be used for the data exchange. For example, FTP uses TCP port 21 for its control information and uses different ports for the actual data transfer. There is increase in number of applications that use one control connection and multiple data connections, where the end user is asked to provide the TCP/UDP port information. To allow all such traffic, your Gateway must be configured to work with all the connections that will be used. More detailed explanation of the configuration follows.



To list port-triggering entries configured in the DIR-430, click on **Advanced** on the top panel, then click on **Application Rules** on the left hand menu to see the configuration page as shown above. Each entry can be either edited by clicking the icon or deleted by clicking the icon on the same line.

To add a new entry, click on Add New Trigger hyperlink, which opens a configuration page as shown in below.



Trigger Port is the standard port for the protocol/application at which the service is offered. You may select the radio button against drop-down list provided and select one from it. Or you may choose a custom port number for your custom application.

Trigger Protocol can be TCP, UDP, or both.

Source IP specifies for what host(s) on the local network, the port-trigger has to be applied. To choose IP address of a single host, select the radio button IP

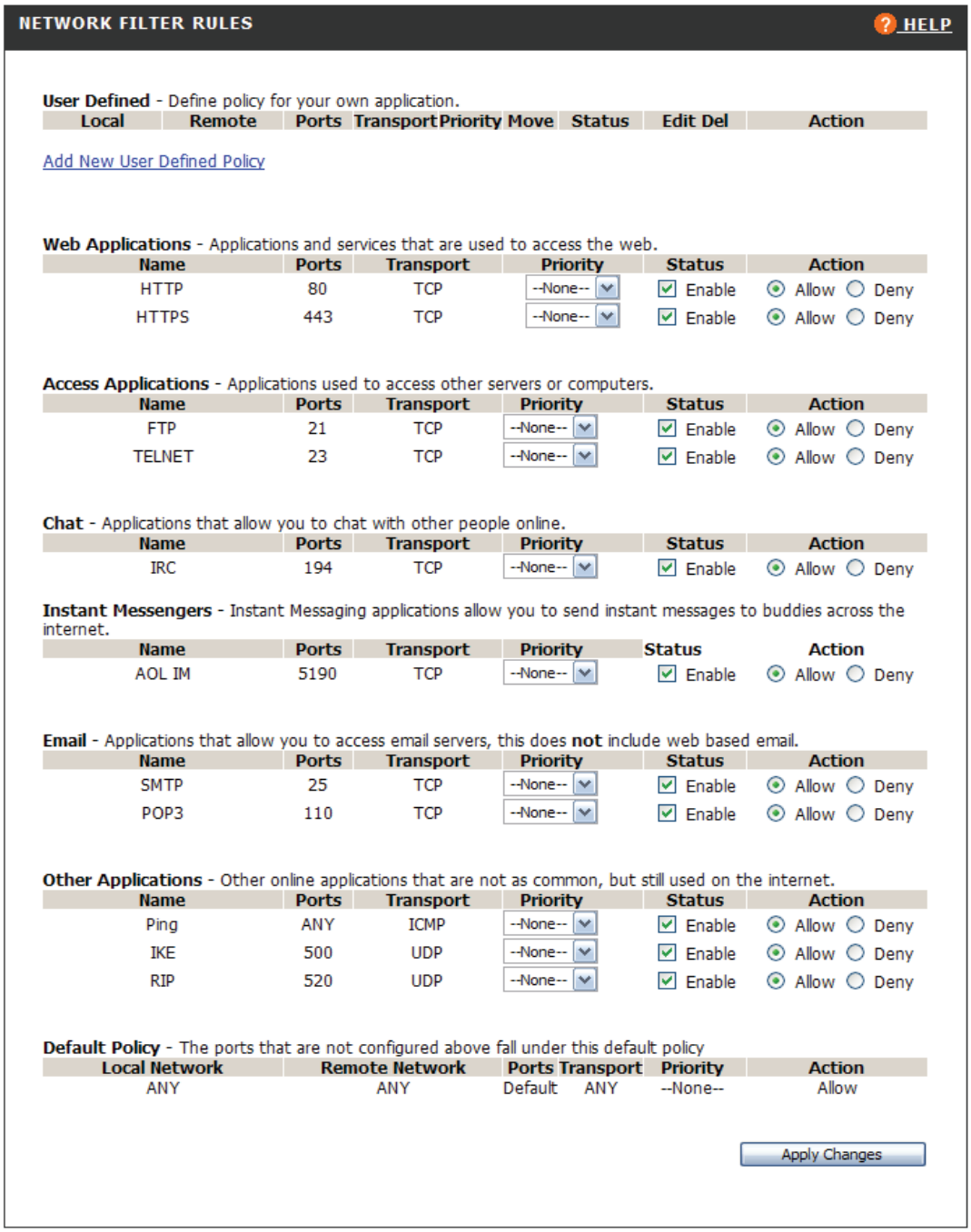
Address, and enter the IP address in the edit box. If you don't know the IP address of a host or if it changes dynamically, you may select Local Computers radio button to select a host name on the local network. If you want the port-trigger to be activated for any local computer, select the **Any** radio button.

Incoming ports are the data ports for the application that will be used during the data exchange. Incoming ports are the port numbers on which the data is received by your Gateway.

Instead of deleting a record when unnecessary, you may preserve the entry with **enable/disable** options. If you select the option **Yes** to enable the record for the question, **Enable this Record?** Choosing **No** would disable the record.

Once done, you may choose to click on **Apply Changes** to add a port-trigger entry.

Network Filter



As a factory setting, the DIR-430 Firewall allows Internet traffic related to certain commonly used PC applications that use the following protocols. They are ping, DNS, RIP, DHCP (client and server), SMTP (e-mail protocol), POP3, FTP (File Transfer Protocol), Telnet, HTTP, HTTPS (for web browsing), instant messengers like AOL, MSN and Yahoo, IKE (for VPN). You may choose to deny some protocol traffic by selecting "**Deny**" radio button for that service, or uncheck "**Enable**" to disable the policy.

Traffic not related to any of the above applications would be allowed to pass through the Gateway by default.

To add a firewall policy for your own application, click on Add New User Defined Policy hyperlink close to the top of the page shown on the previous page, to access the configuration page as shown below. The configuration makes the firewall allow/deny the traffic requested from the internal network to the Internet (outbound traffic). This uses concept of Network Address Translation (NAT), hence the DIR-430 allows all Local PCs to use same public IP address. All pre-defined policies shown in the figure on the previous page use the same concept.

Network Filter configuration requires you to provide:

Remote Network: The remote host domain name/IP address or subnet or IP address range (select "**Any**" radio button if required for all machines) to which connections will be made.

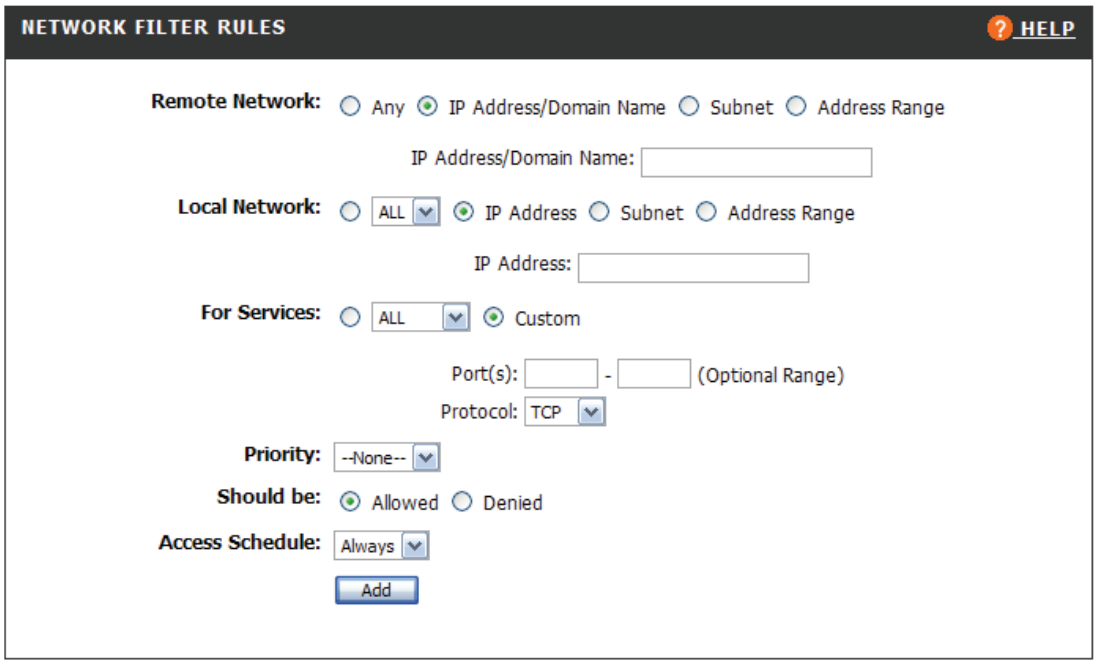
Local Network: Local host IP address or subnet or range of IP addresses (or select a radio button for "**ALL**" machines) from which the connections will be made.

For Services: A pre-determined service from the drop-down list or specify port range (if only one port exists, provide duplicate entry) with transport protocol (TCP/UDP).

Priority: Choose a priority level if Uplink Bandwidth and QoS are enabled.

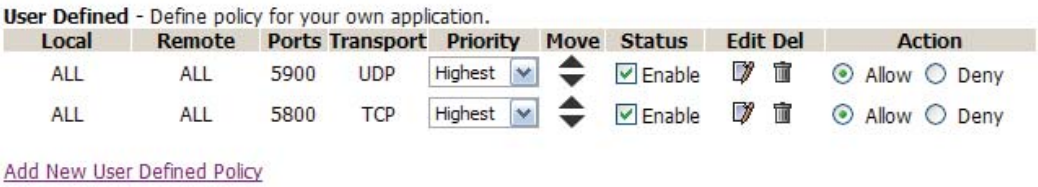
Should be: Select whether this policy should allow or deny traffic.

Access Schedule: Select the access schedule policy to be used (**always** by default). All the added time windows will appear in the drop-down list.



Once the configuration is complete, click the **Add** button to add the policy into the list.

The added entry is then displayed as in the figure below.



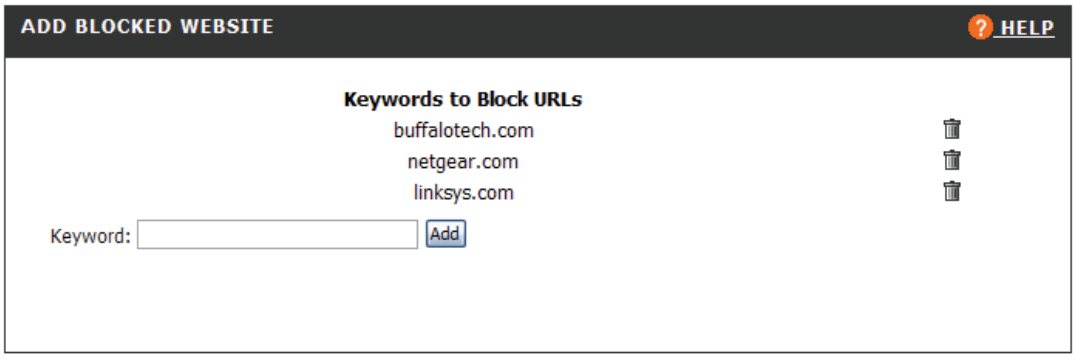
The firewall policy can then be changed to Allow/Deny, disabled/enabled, modified, or deleted.

Blocked URLs

You may wish to block your local network PCs access to some websites. If you are aware of such websites, you can add those to the URL keyword filter list so that when an http request is made to a particular website, the Gateway drops the http requests and the page is blocked.

This is specifically useful in parental control.

To access this feature, from the top panel click on **Advanced**, then click on **Blocked URLs** from the left hand menu.



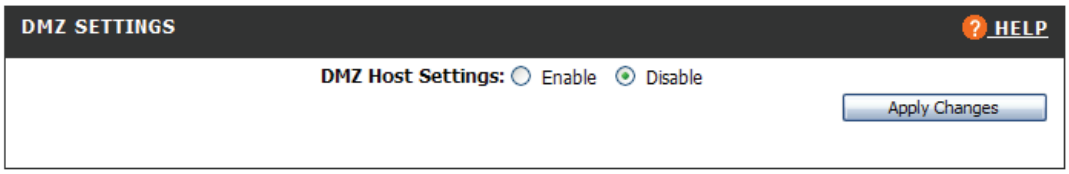
Enter the known URL keyword in URL that you may like to block in the edit box as shown. Click on **Add** button to add to the URL keyword filter list. The entry can be deleted by clicking on the delete icon.

Once http request is made by local network PCs, the DIR-430 tries to match the keywords in the URL. If a match is found, the http request will be dropped by the DIR-430.

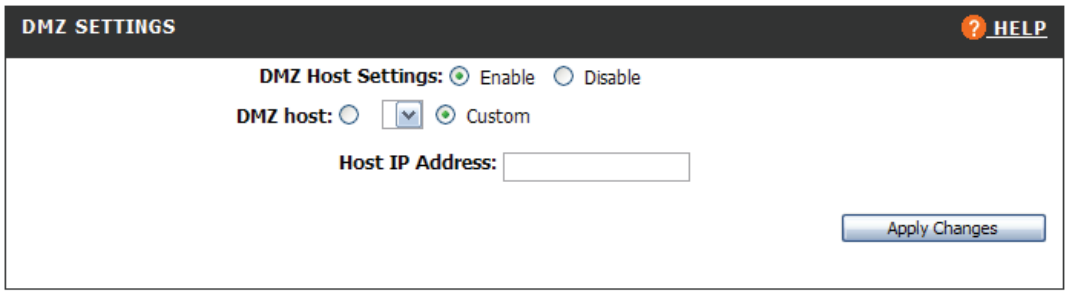
DMZ Settings

The DIR-430 provides the ability to specify a DMZ host for any traffic initiated on the Internet so that if none of the port forwarding policies match, the traffic reaches that DMZ host. This is useful for some applications like games where dynamic transport (TCP/UDP) port numbers are used by the applications.

To access this feature, click on the **Advanced** item on the top panel, then click on the **DMZ** item on the left hand menu.



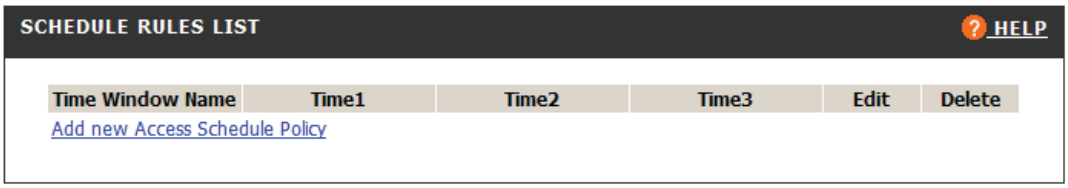
You may choose from drop-down list against **DMZ Host:** field that shows the list of all local networked PC names (that received dynamic IP addresses from Gateway). If any local PC is configured to a static IP address, select "Custom" radio button and enter the IP address in the edit box.



Click **Apply Changes** button.

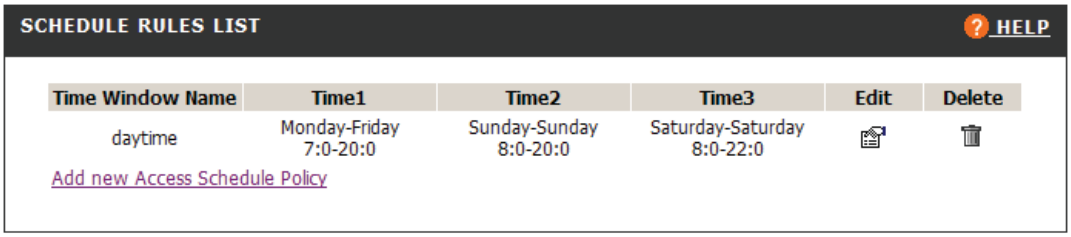
Scheduling

Scheduling allows the firewall to enable policies for specific time windows. For example, you might want the local network users to access the Internet only during certain hours of the day/week; Access can be restricted using **Scheduling**. Time windows are independent configuration from Firewall, though firewall makes use of time window configuration.

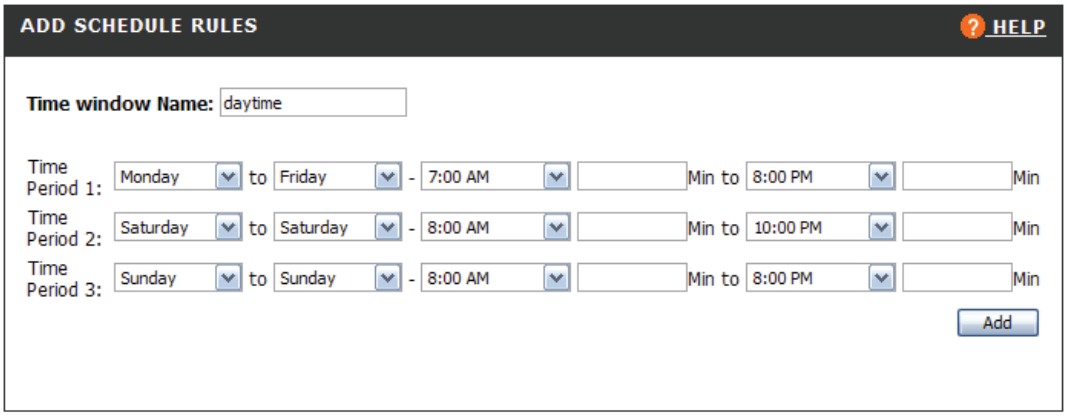


For **Scheduling**, click on the **Advanced** item on the top panel, then click on **Scheduling** in the left hand menu. This opens up a time window page, where you can view the existing entries and add a new time window. These time windows can be made use of in the firewall access policies.

Each entry can be either edited by clicking the icon or deleted by clicking the icon on the same line. As the following figure shows, every schedule profile can allot three different time slots on different days of the week. More explanation follows on adding the schedule profiles.



Click on **Add new Access Schedule Policy** to open the **Add Schedule Rules** configuration as shown below. You may like to give a meaningful name to the entry, since these names will be used while adding a firewall policy. The Time window name field accepts single words only.



The entries are explained with an example as follows: You may like to give Internet access to the PCs connected to Local network at the following times; 7:00 AM - 8:00 PM on all Mondays, Tuesdays, Wednesdays, Thursdays, Fridays; access is allowed on Saturdays and Sundays at different time periods; 8:00 AM - 10:00 PM on Saturday and 8:00 AM – 8:00 PM on Sunday. Hence there is a continuity loss (Saturday and Sunday have different time periods). You should split the time window entry into three different time periods. Add Monday to Friday - 7:00 AM - 8:00 PM in Time period 1, and the rest as shown in the figure above. The entries are not considered whose periods are conflicting in a time window.

Time period from "Monday to Friday - 7:00 AM - 8:00 PM" does not mean period from Monday 7:00 AM till Friday 8:00 PM. It means the time period between 7:00 AM - 8:00 PM on all Mondays through Fridays.

If you would like to have an overnight schedule like 10:30 PM to 6:00 AM everyday, the time schedule needs to be broken into two pieces. You may add Sunday-Saturday schedule from 10:30 PM- 11:59 PM as time period 1, and Sunday-Saturday schedule from 12:00 Midnight – 6:00 AM in the time period 2.

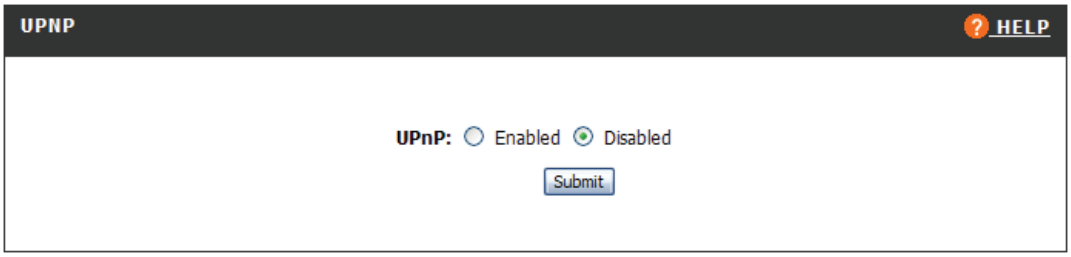
Universal Plug-n-Play (UPnP)

Universal Plug-n-Play (UPnP) architecture allows Windows XP computers to automatically configure the DIR-430 for some applications, such as the MSN messenger service. UPnP will also allow the DIR-430 management Interface to be saved as a link in the Network Neighborhood of a Windows XP PC.

MSN Instant Messenger: With Microsoft's MSN Messenger you can chat online via text, voice or even video conversation - in real time - with your friends, family or colleagues. It's faster than e-mail, a great choice for conversations and the perfect alternative when you can't be there in person

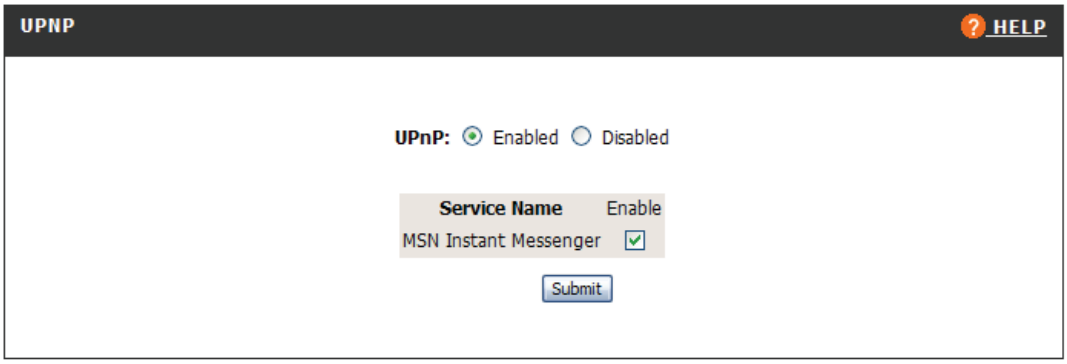
To configure the UPnP capabilities offered by the DIR-430, click on the **Advanced** item on the top panel. Click the **UPnP** item located on the left hand menu to access the configuration page.

The default setting for UPnP is **disabled**.



Click on **Enabled** or **Disabled** radio buttons to enable/disable the UPnP capabilities for the Gateway.

You can select the appropriate checkboxes that correspond to specific applications that you might want the Windows XP PC to configure in the Gateway, once the UPnP service is enabled.

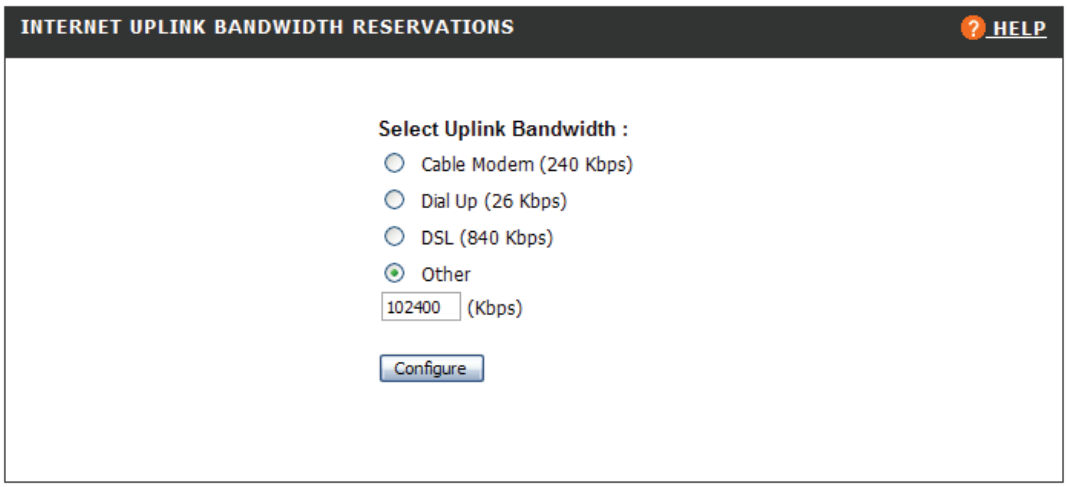


Click **Submit** button to save the changes.

Uplink Bandwidth

If the DIR-430 is connected to a typical Broadband Internet Connection (such as Cable or DSL), you may wish to limit the rate at which traffic is sent on the Internet. Without doing so there are chances of the Cable/DSL Modem dropping packets making an unpleasant Internet Experience. You can limit the Uplink Bandwidth by setting correct Uplink Bandwidth value (Check with your ISP for more information on your connection speed).

Click on the **Advanced** item on the top panel, then click on the **Uplink Bandwidth** item on the left hand menu.



Setting the uplink bandwidth value limits the speed of the traffic sent on the Internet to the value selected. Check with your ISP for the type of connection you purchased. Based on the type of connection selected, outgoing data bandwidth will be limited to the value shown in the bracket of each connection.

If you want to select different value from the standard uplink bandwidths shown, select other option that facilitate to enter any value you wish. You can enter any value between 26 Kbps and 102400 Kbps depending on the bandwidth you purchased from the ISP.

If you don't know to enter the exact uplink bandwidth value of your Internet connection, you may obtain the information using different standard bandwidth meters available on the Internet. You may test your connection bandwidth and speed from the website, http://reviews.cnet.com/7004-7254_7-0.html

Default uplink bandwidth is set to 256Kbps on the DIR-430.

User Portal

The User portal is a web-based secure access portal, which can be configured to give access to collections of blogs, photos, videos, music and desktop links located on local PCs or on Network Attached Storage devices. This portal can be access from within the LAN or from the Internet via an SSL capable web browser (Internet Explorer, Firefox, Opera, Netscape, etc.).

Admin Info

Configure the Administrator's details by clicking on **User Portal** and then on the **Admin Info** link to open up the page as shown below.

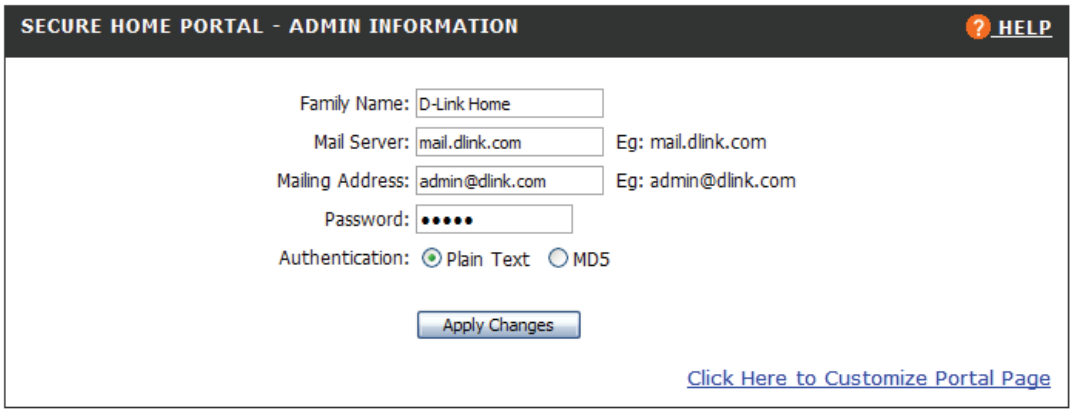
Family Name: The name to be displayed on the top left corner of the User Portal.

Mail Server: Enter the Domain name/IP Address of the SMTP server where e-mail will be sent.

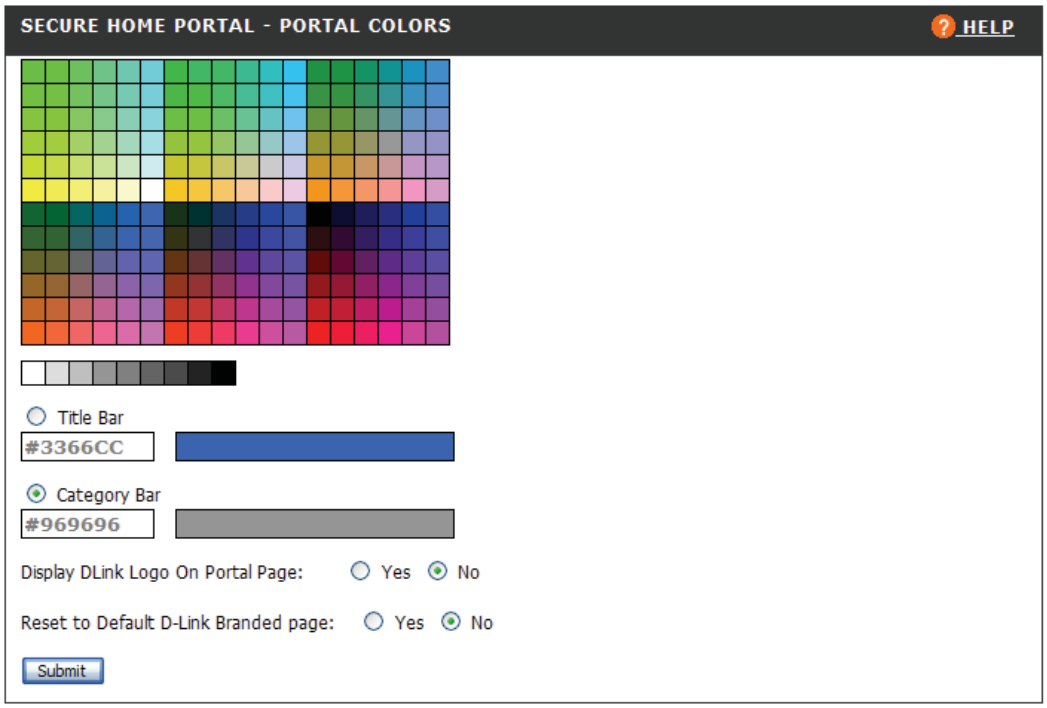
Mailing Address: Enter the E-mail address of the administrator. Any feedback sent from the user portal will be sent to this email address.

Password: Login password to the admin mail account.

Authentication: Authentication type to login to the SMTP server. Here you have two options to login, one with the **plain password** and the other by encrypting the password with **MD5** encryption.



To modify the appearance of the user portal, use the **Click Here to Customize Portal Page** link. This will allow you to change the top and bottom header color, the category bar color, remove the D-Link Logo, and reset the changes back to default.



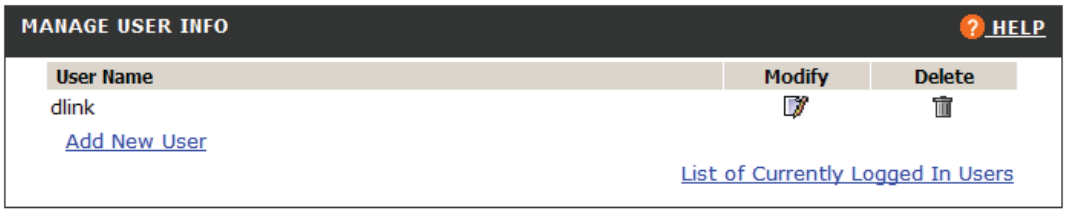
Choose the desired color from the color grid at the top of the configuration window. This color can be applied to the Title Bar and/or the Category Bar. You will see a preview of the selected color to the right of the respective selection.

To add the D-Link logo to the top-right corner of the Title Bar, choose the **Yes** radio button.

The default page layout may be re-instated by choosing the **Yes** radio button next to **Reset to Default D-Link Branded page**.

User Info

Click on **User Info** under **User Portal** tab on the top pane to access user details as shown below. Here you can manage users that may access the user portal. A list of all the users will be displayed here. You have options to add/modify/delete a user.

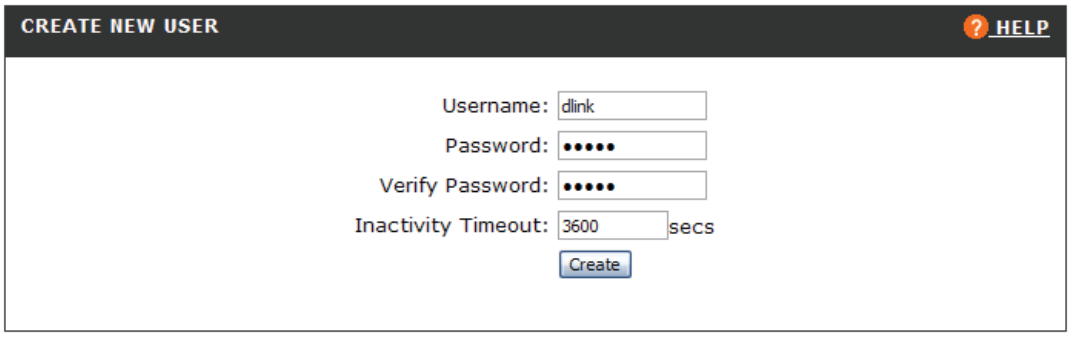


Click on Add New User hyperlink to add a new user. Each user has his own view of User Portal; this view has to be configured by the administrator.

While creating the user, one can enter the inactivity timeout, which is the idle time after which the user will be logged out. You need to login again to access the user specific content.

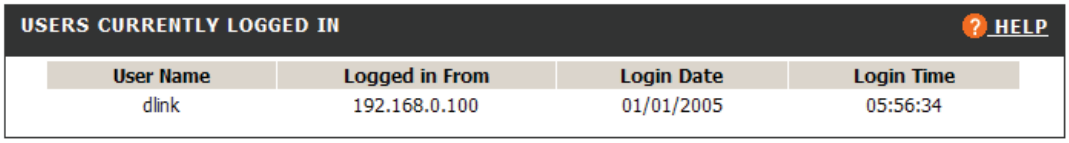
For a guest user there is no timeout.

You can modify user information by clicking on the **modify** button and to delete you can use the **delete** button. You cannot delete a user if the user has any references.



Before you delete a user, you have to delete all references which are currently associated to that user.

The list of currently logged in users can be viewed by clicking the **List of Currently Logged In Users** link on the main **User Info** page.

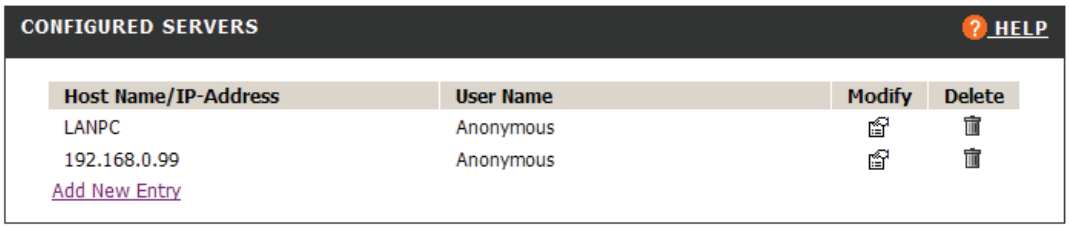


Manage Servers

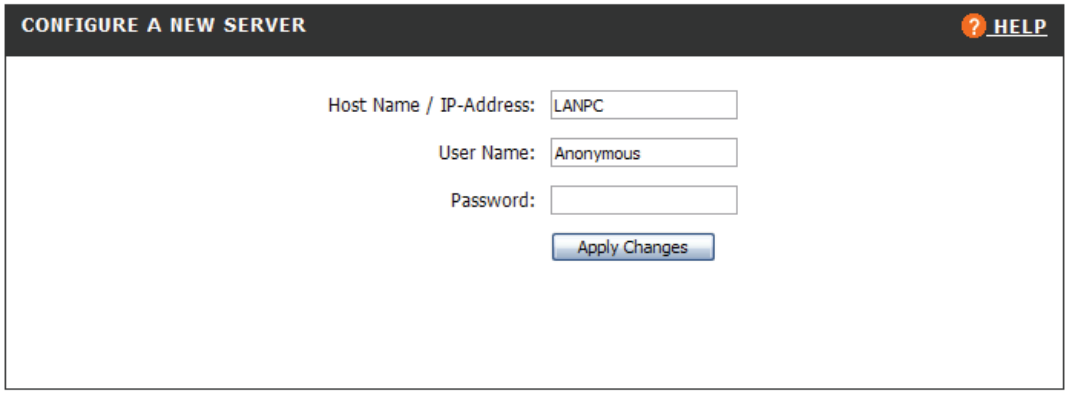
Click on **Manage Servers** under **User Portal** tab to view current servers configured. This list will be automatically populated when the administrator creates some references by browsing and selecting the server. As soon as the administrator logs into a server when creating the references, the server entry will be added to this table.

This server information will be useful to the administrator for two main reasons.

1. After creating some references to a server, if the administrator modifies the login details on the server (Windows/Linux PC's for which references were created), he/she can edit the entry in this table and enter the new login details. This way the references created earlier will work normally.
2. If the administrator cannot find the server listed in the "File Servers" list while navigating "Manage Views->User->Add New Reference->File Server", then he/she has to add the server entry first in this table and use the "Click here to add the reference manually" link provided in the "File Servers" page to add a new reference.



To create a manual reference, click on "Add New Entry" hyper link. Enter the Host name/IP Address for the server name and username/password to login to the server while creating a new entry. For servers, which do not require any username/password to login, those fields can be left empty, a default username/password as anonymous will be used in such cases.



You can modify the username/password information of a server at any point of time by clicking on modify button, and it will be effective immediately.

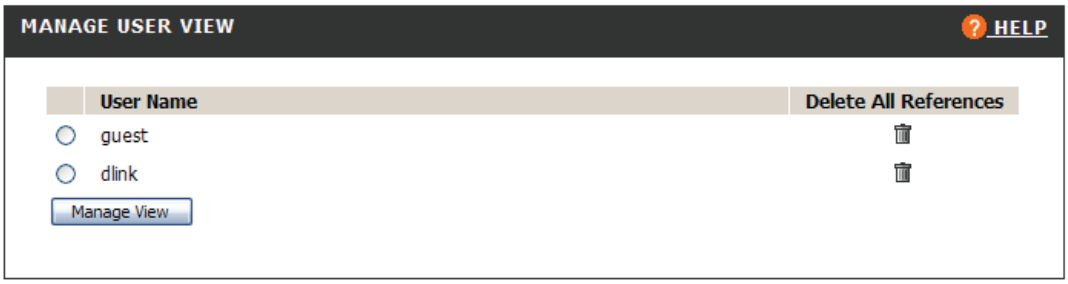
You can delete the server by clicking on the delete button.

Before deleting the server, you have to delete all references which are created based on this server. Selecting a server from the list of File servers under **Manage Views** adds the server to the server list.

Manage Views

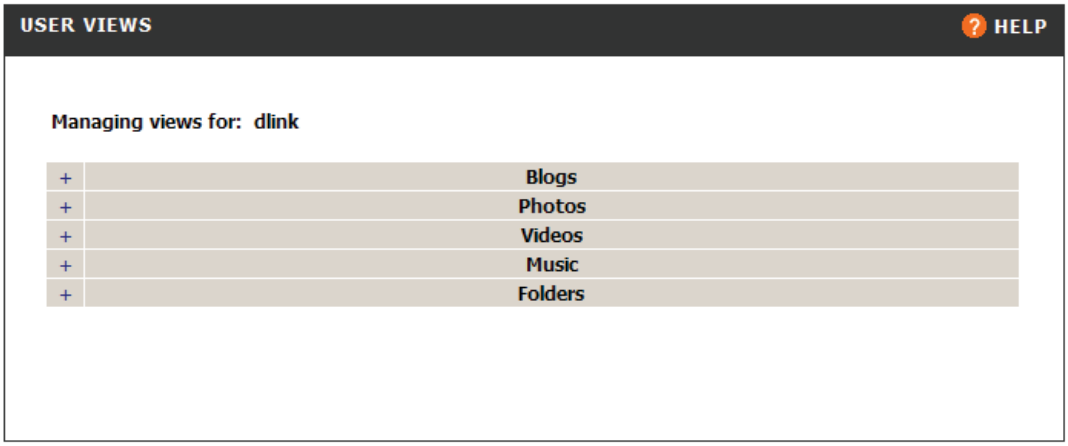
A User's View represents the collection of all resources presented or accessible to a single user of the portal. In the DIR-430, a default user exists with the name "guest". The Administrator is allowed to configure access for the guest user which can be accessed by anyone connecting to the DIR-430.

Administrator can configure the views for any user by clicking on the **Manage Views** under the **User Portal** tab. Here a list of all the users will be displayed as shown below, we have to select a user first and then click on the **Manage View** button to configure the views for that user. A view created for a user will be solely applicable for that particular user (although the administrator has the provision to copy the same view to another user).

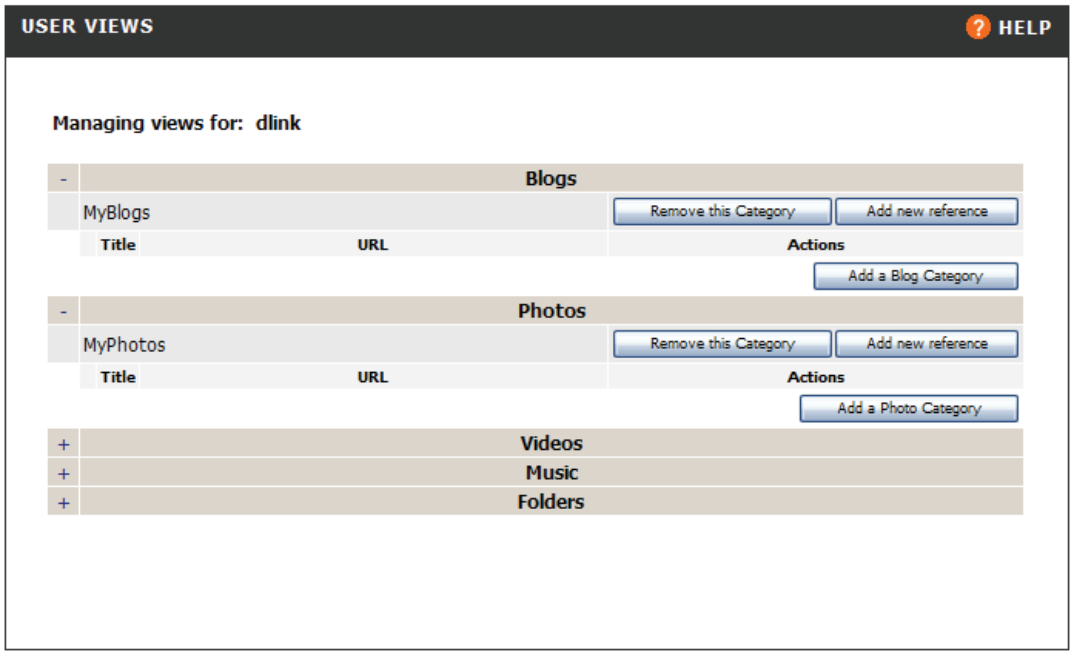


You can delete all references and albums of the user by clicking on the delete link, associated with the username. This operation will also delete the desktop references of that user.

There are five sections in **Manage Views** page - Blogs, Photos, Videos, Music and folders. In any section, one has to create a category first and then references under the category. These categories are like Albums and references within that category are like photos in an album. You can create any number of Categories and within each category you can have any number of references.



Click on + to see user views of corresponding section. Refer to the example on the following page relating to views of the blogs & Photos section.



Add a Category

You can add a category to the sections by clicking on the corresponding **Add a Category** button and providing a suitable name to the respective category as shown in above.

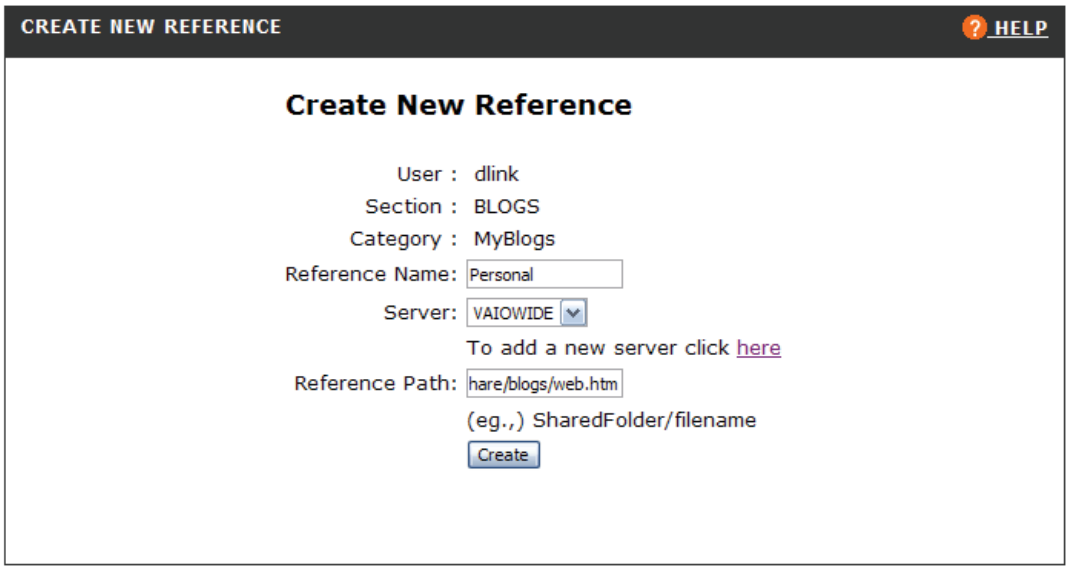
Remove a Category

You can remove the category by clicking on the **Remove this category** button. This action removes all the references in the selected category. You can also remove a reference by clicking on the delete button present in the same row of the reference.

Add new reference

Within each category, you can add new references by clicking on **Add new reference** as shown in above.

If the server you are looking for is listed in the list of File Servers you can simply select the server and navigate to the respective folder to create the reference. If the server is not listed in the File Servers then click on, "**Click here to add a reference manually"** hyperlink on the File servers page, shown previously.



Some of the possible reasons why the server, which is connected to the network, is not listed in the list of File Servers are

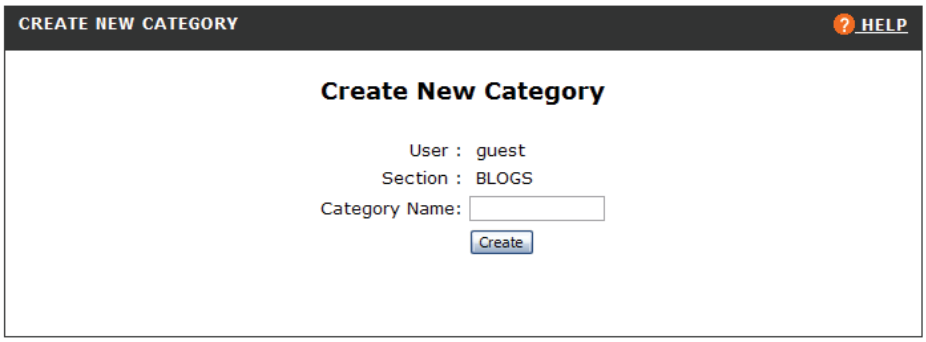
1. The DIR-430, enumerates/queries for the list of all the servers, which support File Sharing for every 1-minute. There could be a possibility that when the query happened the PC was not connected to the LAN or must have been shutdown. Correct the problem in such cases and please wait for sometime, so that the system will be displayed in the File Servers.
2. It could be a Linux PC running samba, which is a member of some workgroup, in which there is no other windows machine belonging to the same workgroup.
3. "Client for Microsoft Networks" should be installed for the Network interface in the Windows PC.
4. If any Firewall software is running on the Windows/Linux PC's you have to make sure that port numbers 137/138/139 are allowed. Otherwise the server will not be displayed in the File Servers page.

Manage Views - Blogs

A Blog can be static html page (saved locally), which has a description about a persons experience/ views / hobbies /useful information.

Add a Blog Category

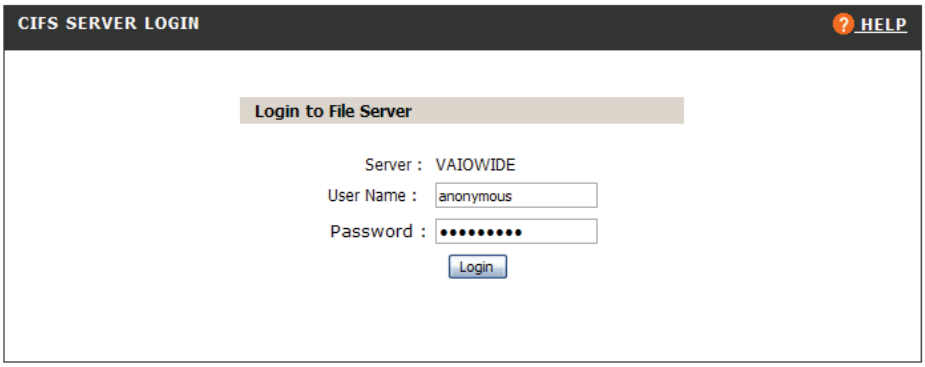
Click on "**Add a Blog Category**" to create an album. As shown in the following image, you need to enter album's **Category Name** and then press **Create** button to add the category to the Blogs section.



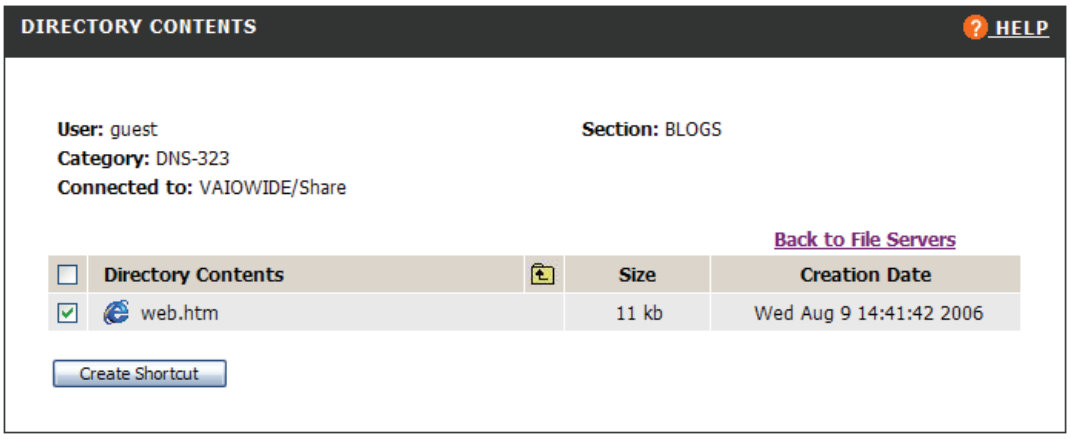
Add New Reference

Within each category, you can add new references by clicking on **Add new reference** as shown previously. You will then be shown a list of available file servers. If the server to which you want to create references is listed, click on the server name to select it.

You are then requested to provide the **Username** and **Password** of the selected server on the Network as shown below.

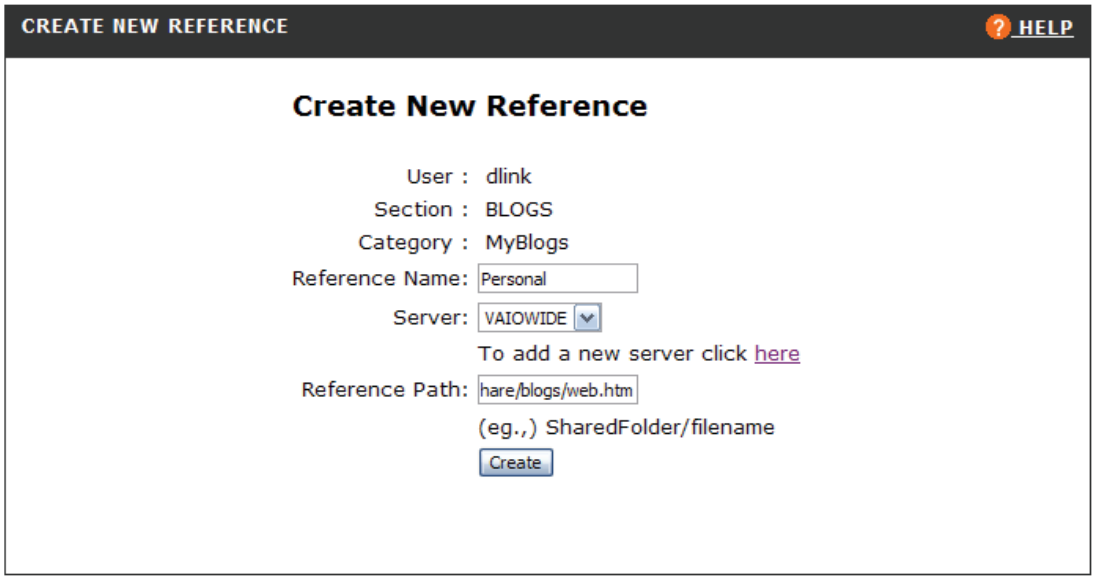


After a successful login, browse to the respective file and select the checkbox associated with the file to add it to the category. The figure on the following page provides an example for the listing of files and directories from a file server.



You cannot add more than 50 references in one instance. References already selected in the same category are shown as checked & disabled and therefore cannot be selected again. While using the File Browser feature, to add a reference to a category, selection of **Folders** is disabled. An administrator is expected to add only static HTML pages to the category created under Blogs.

If the server is not listed in the File Shares, use "Click here to add a reference manually". You are then directed to the **Create New reference** page as shown below.



Provide a valid **Reference Name**, select the Server and enter the complete Path to the reference on the server. Click **Create** button to add the reference to a category under Blogs. Reference path will be the path starting from the shared folder and you should also include the file extension when creating references manually.

Ex. If the server "VAIOWIDE" has a shared folder "MyBlogs" and inside the folder "Blogs" if you have a file "hobby.htm" then enter the reference path as follows.

MyBlogs/hobby.htm

A Blog is a static HTML page. You can create a HTML page using any editor (including MSWord) that provides **Save-As HTML** option.

Save the document in a shared folder and create references to this file.

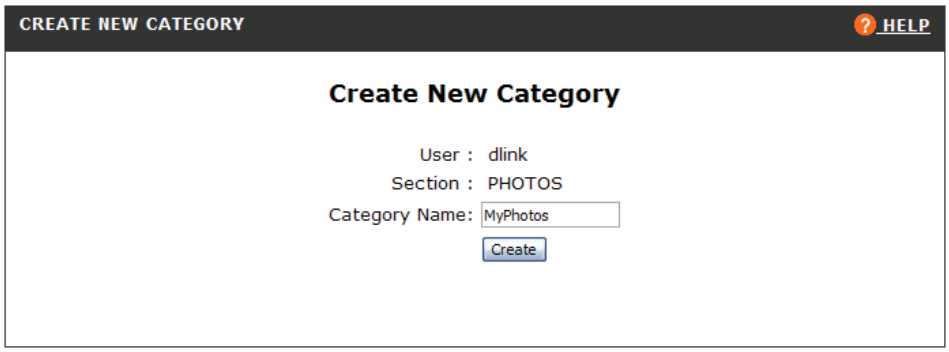
Manage Views – Photos

The references, which are created under photos, will also be displayed as thumbnails in the user portal. For this, the administrator has to create the thumbnails for all the photos, which are created as references. These thumbnails should be created in the same folder where the actual image exists but with a suffix of ".thumb.jpg".

Thumbnails are reduced-size versions of pictures - 64/64 pixels. You can create thumbnails by using the default windows paintbrush application. Open paintbrush, click "stretch/skew" option under "Image" menu to reduce the image size. Alternatively, you can create thumbnails using "Easy Thumbnails™ Copyright © 2001–2004 Fookes software". Download this software from www.fookes.com.

Add a Photo Category

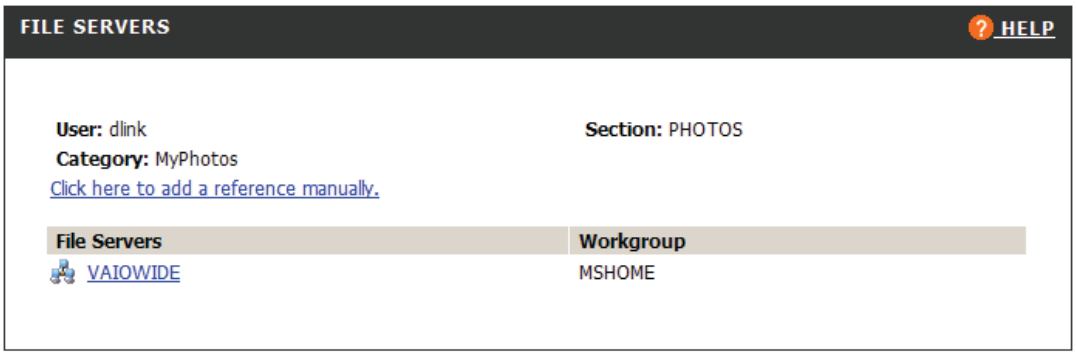
Click on "**Add a Photo Category**" to create an album. As shown below, you need to enter album's **Category Name** and then press **Create** button to add the category to the Photos section.



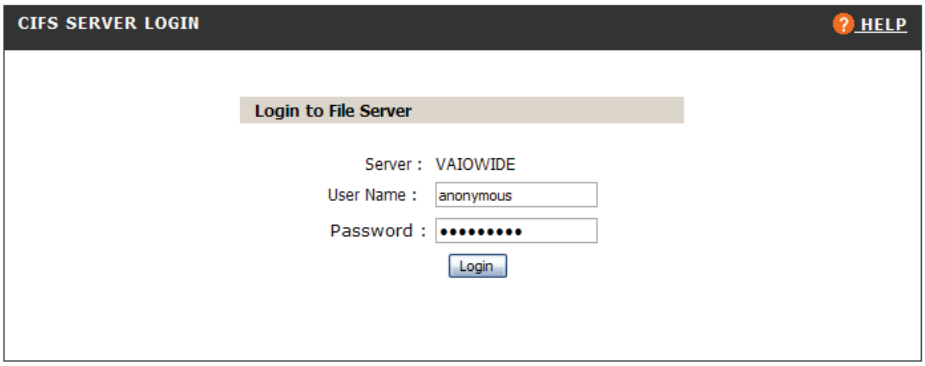
Add New Reference

Click on **Add new reference,** as shown above to add references to the newly created category.

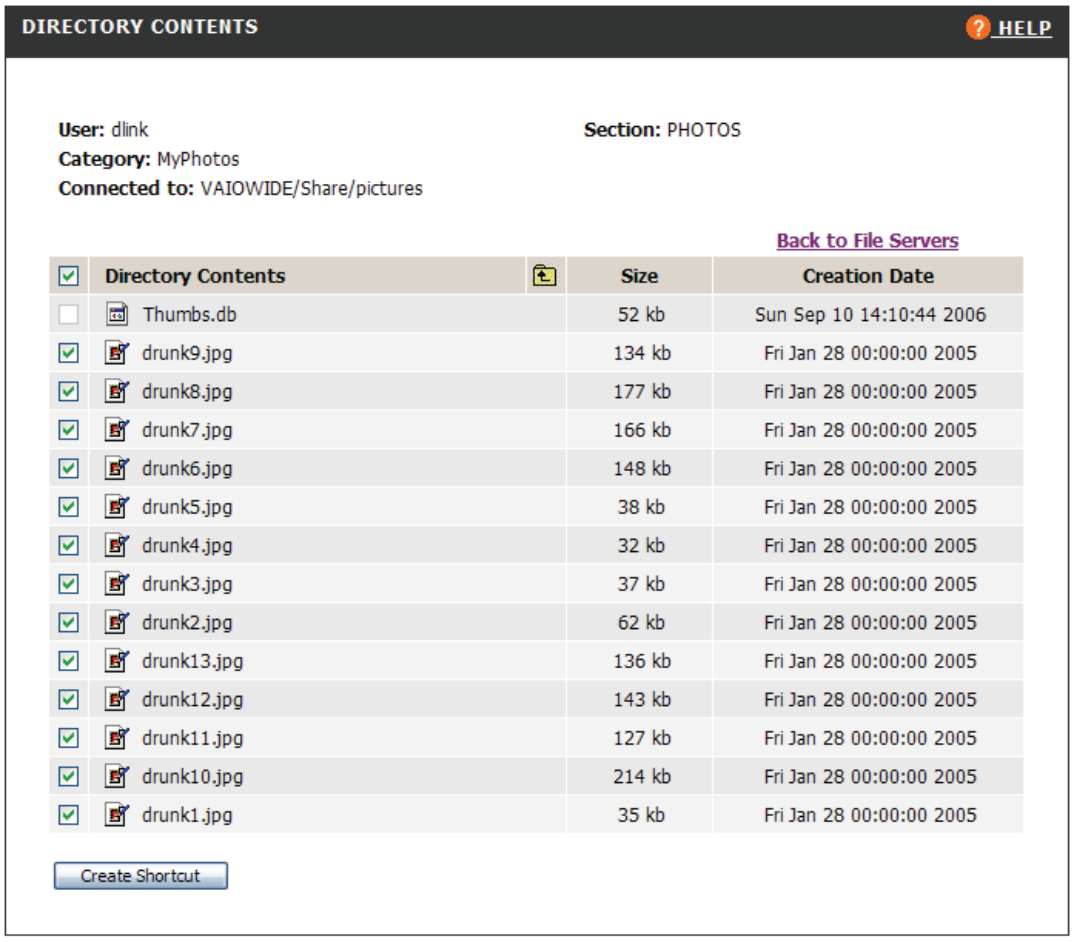
Select a **server** from a list of File Servers on the Network you are connected to, as shown below.



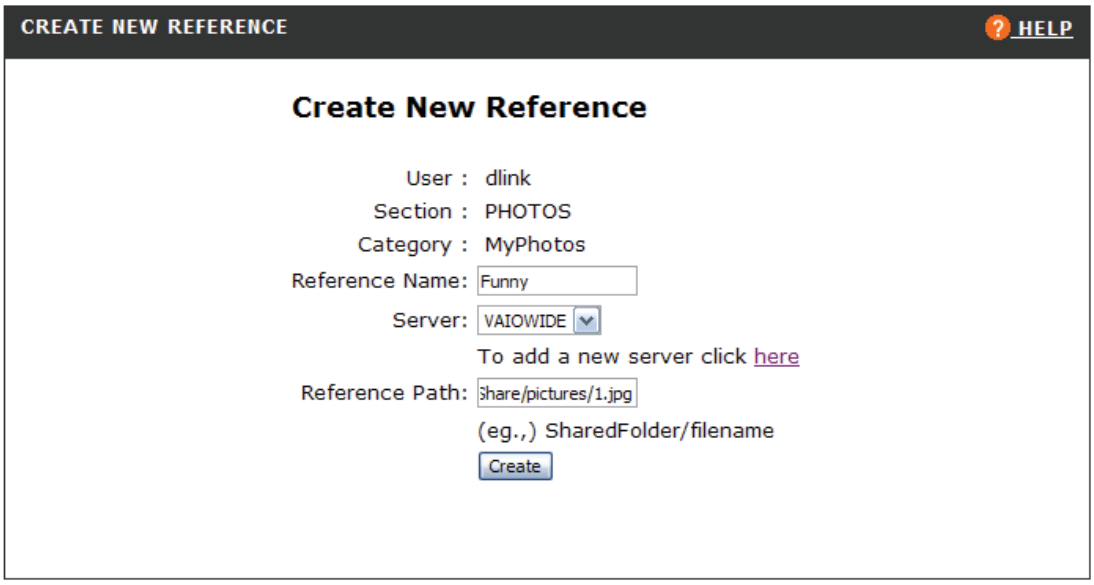
Provide the **Username** and **Password** of the selected server on the Network as shown below.



After a successful login, browse to the image file and select the checkbox associated with the file to add it to the category. The figure below provides an example for the listing of files and directories from a file server.



If the server is not listed in the file server list, use the **Click here to add a reference manually** hyperlink on the File servers page, as shown previously. You are then directed to the **Create New reference** page as shown below.



Provide a valid **Reference Name**, select the Server and enter the complete Path to the reference on the server. Click **Create** button to add the reference to a category under Photos.

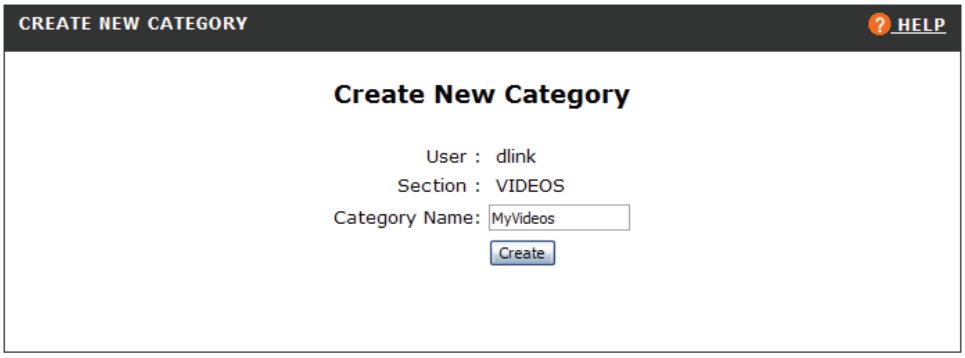
While using the File Browser feature, selection of **Thumbnails** is disabled. An administrator is expected to add reference to jpg/bmp/gif/png or any other graphic/image files to the category created under Photos.

Manage Views – Videos

This section provides you an interface to add references to your video files on Secure Home Portal. The references created in this section should point to video files like mpg, avi, et all.

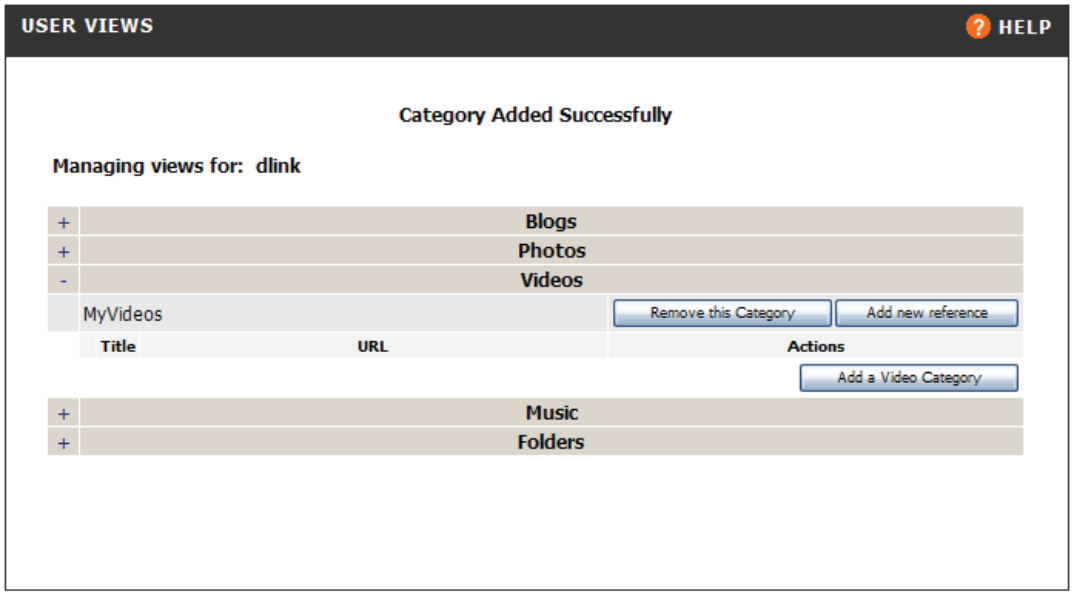
Add a Video Category

Click on "**Add a Video Category**" to create an album. As shown previously, you need to enter album's **Category Name** and then press **Create** button to add the category to the Videos section.

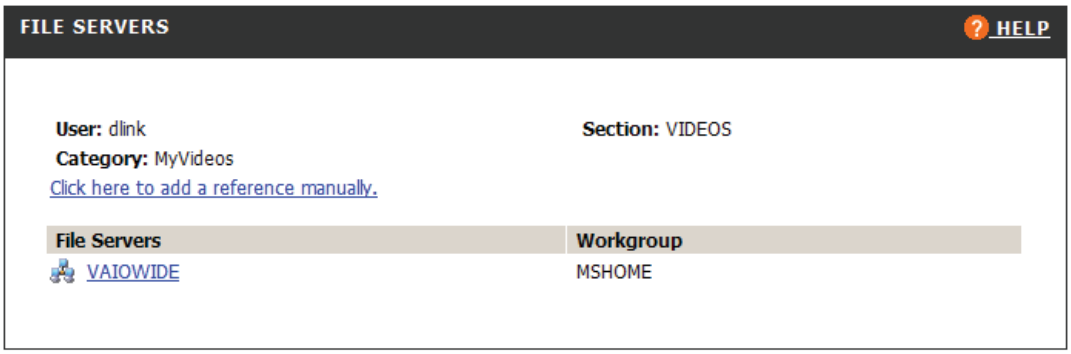


Add New Reference

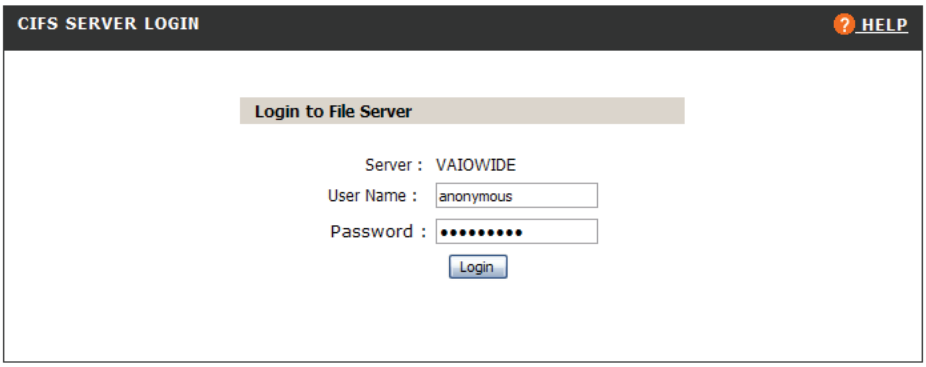
Click on **Add new reference,** as shown below, to add references to the newly created category.



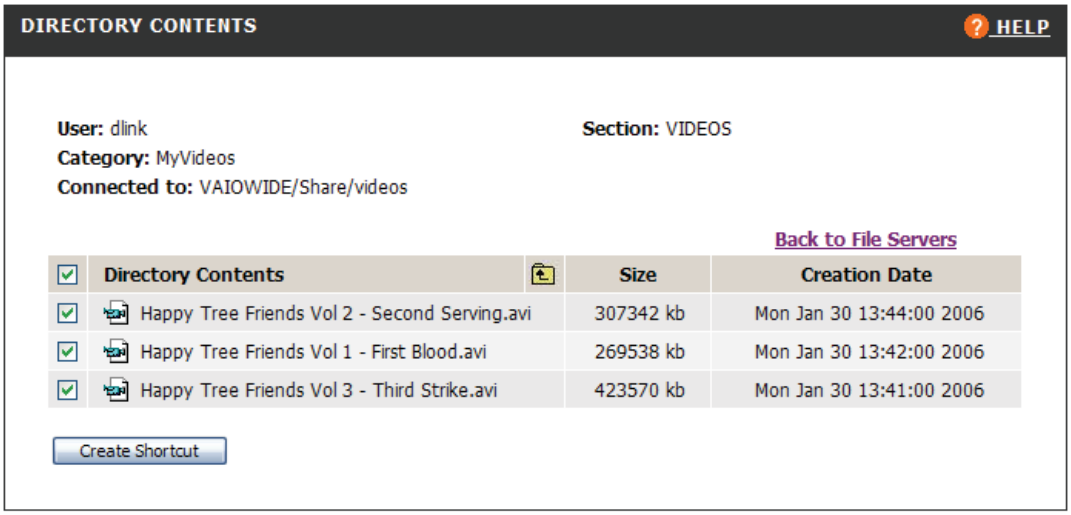
If the server is listed in the "File Servers", select a **server** from the list.



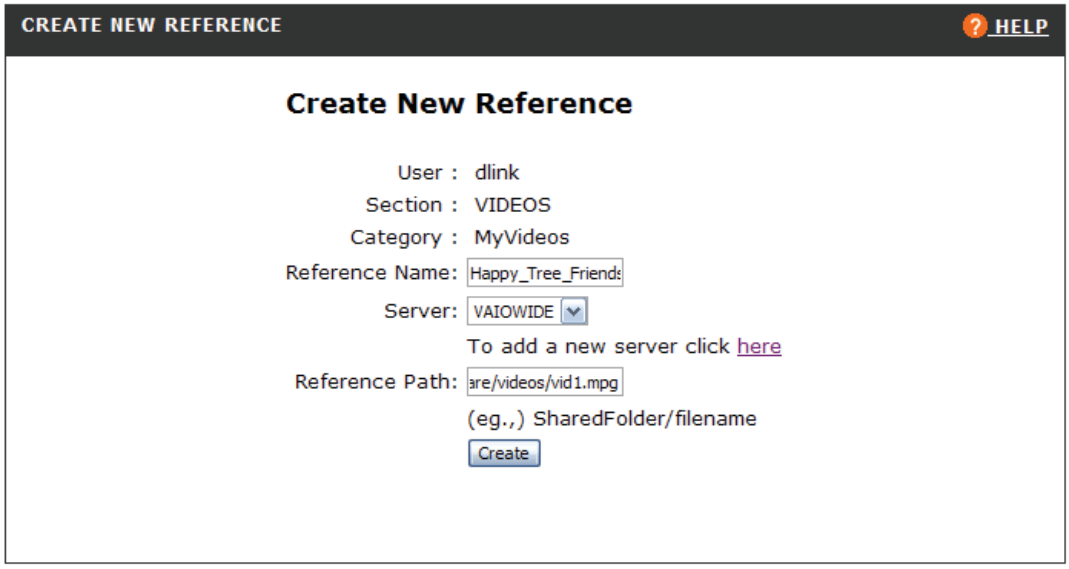
Provide the **Username** and **Password** of the selected server on the Network as shown below.



After a successful login, browse to the video file and select the checkbox associated with the file to add it to the category. The image below provides an example for the listing of files and directories from a file server.



If the server is not listed in the File Servers then click on," **Click here to add a reference manually"** hyperlink on the File servers page. You are then directed to the **Create New reference** page as shown below.



Provide a valid **Reference Name**, select the Server and enter the complete Path to the reference on the server. Click **Create** button to add the reference to a category under Photos. Reference path will be the path starting from the shared folder and you should also include the file extension when creating references manually.

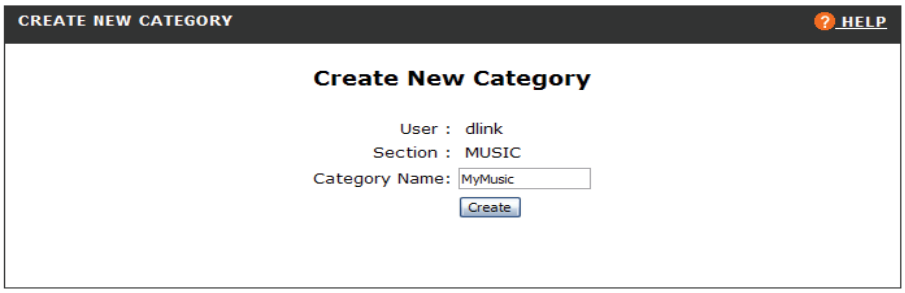
Any kind of video file can be added as a reference. Please make sure that suitable Video Player application is available on the Client PC to play the files.

Manage Views – Music

This section provides you an interface to add references to your Music files on Secure Home Portal. The references created in this section should point to audio files like mp3, mid, wav, et all.

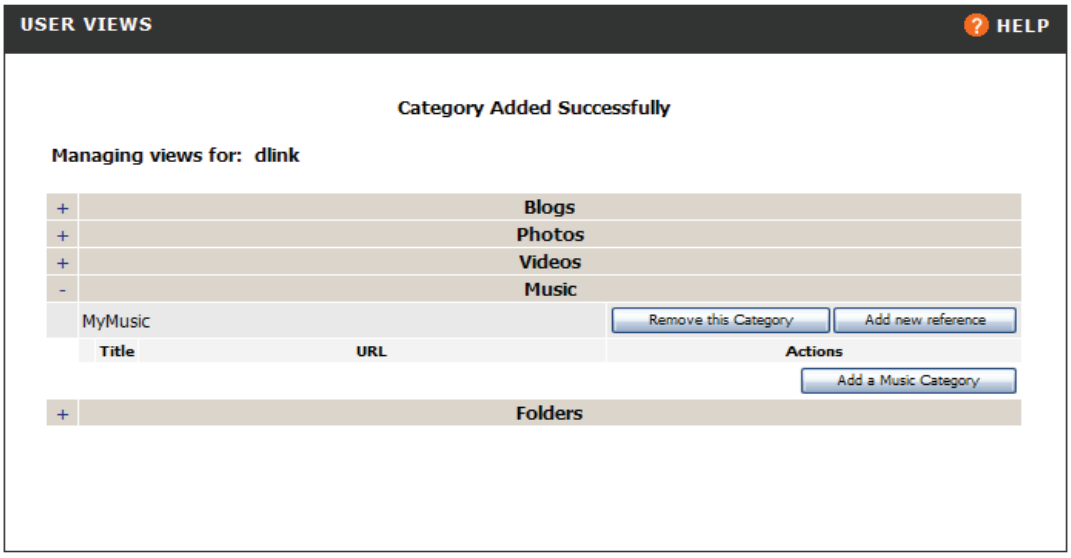
Add a Music Category

Click on "**Add a Music Category**" to create an album. As shown previously, you need to enter album's **Category Name** and then press **Create** button to add the category to the Music section.

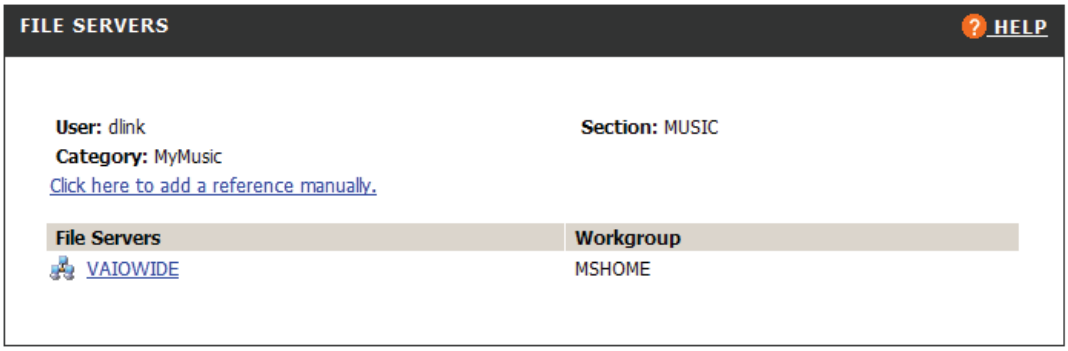


Add New Reference

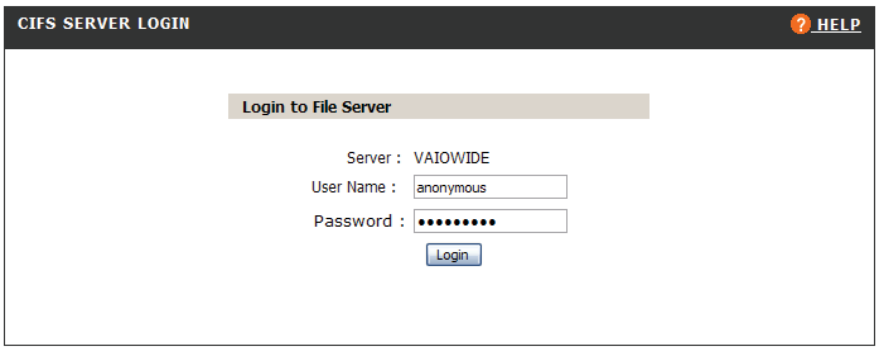
Click on **Add new reference,** as shown below to add references to the newly created category.



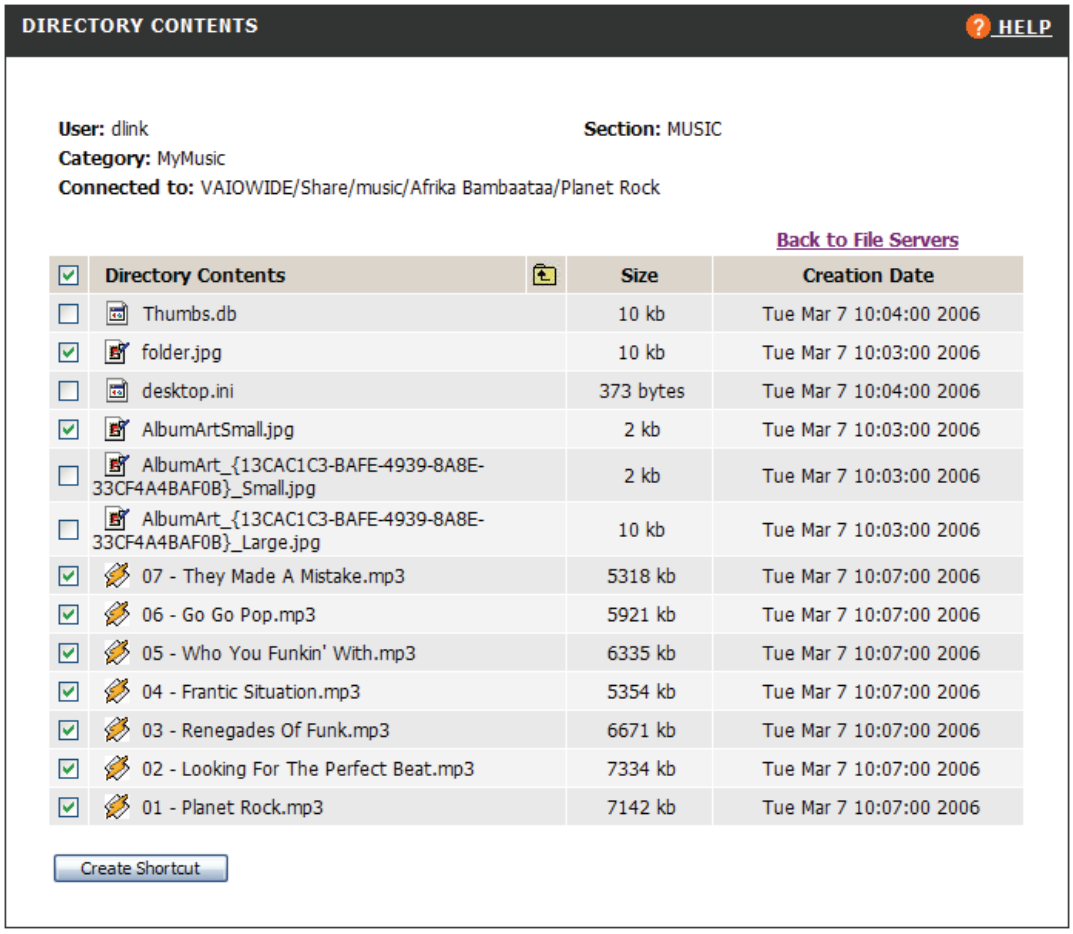
You will be directed to the File Servers list as shown below.



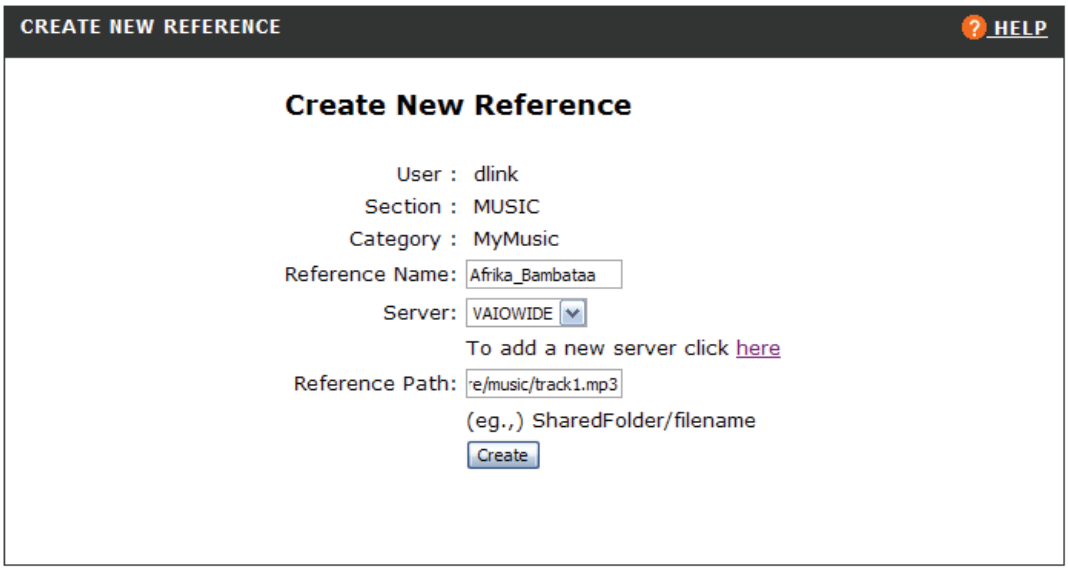
If the server is listed in the File Servers, then select it and provide the **Username** and **Password** of the selected server on the Network as shown in below.



After a successful login, browse to the video file and select the checkbox associated with the file to add it to the category. The figure below provides an example for the listing of files and directories from a file server.



If the server is not listed in the list of file servers, then use the **Click here to add a reference manually** hyperlink on the File servers page. You will be directed to the **Create New reference** page as shown below.



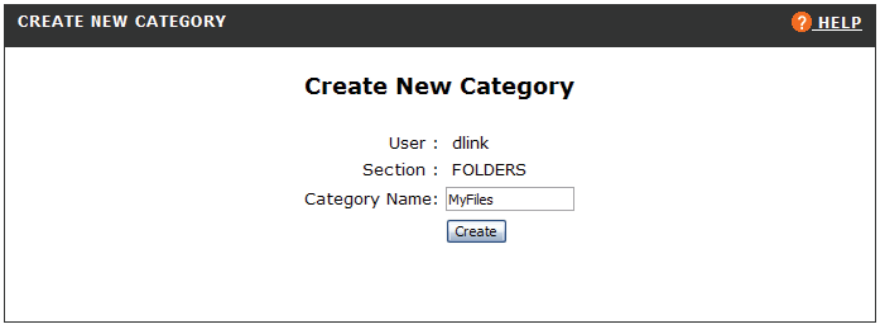
Provide a valid **Reference Name**, select the Server and enter the complete Path to the reference on the server. Click **Create** button to add the reference to a category under Photos.

Manage Views – Folders

This section helps you create references to shared folders. When you click on these references in User Portal, the shared folder along with its contents will be displayed. After the contents are displayed, you have an option to download/view the files in that folder.

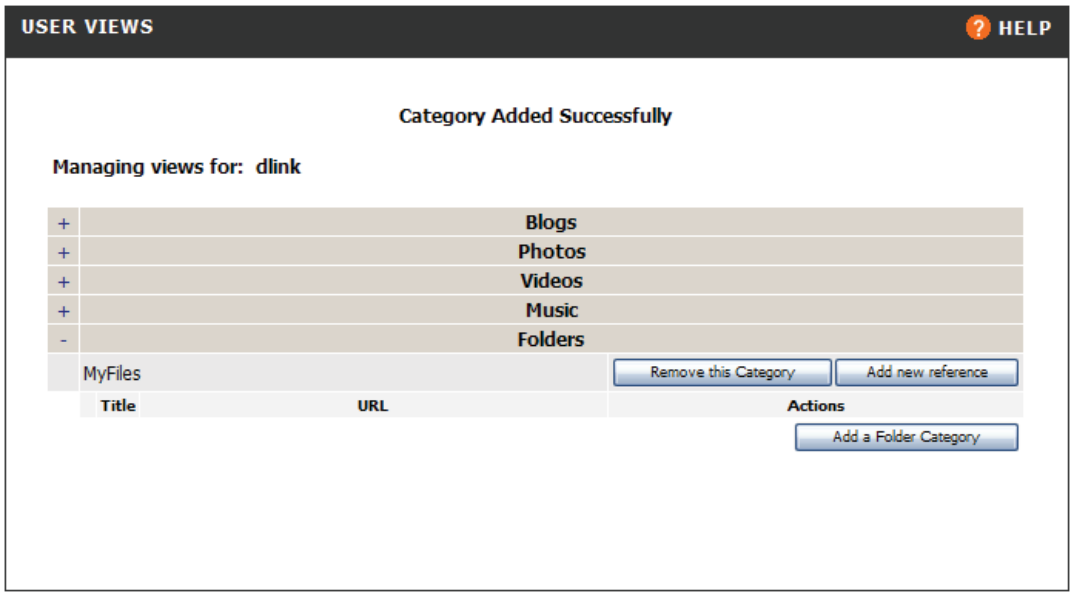
Add a Folder Category

Click on "**Add a Folder Category**" to create an album. As shown in the figure below, you need to enter album's **Category Name** and then press **Create** button to add the category to the Music section.



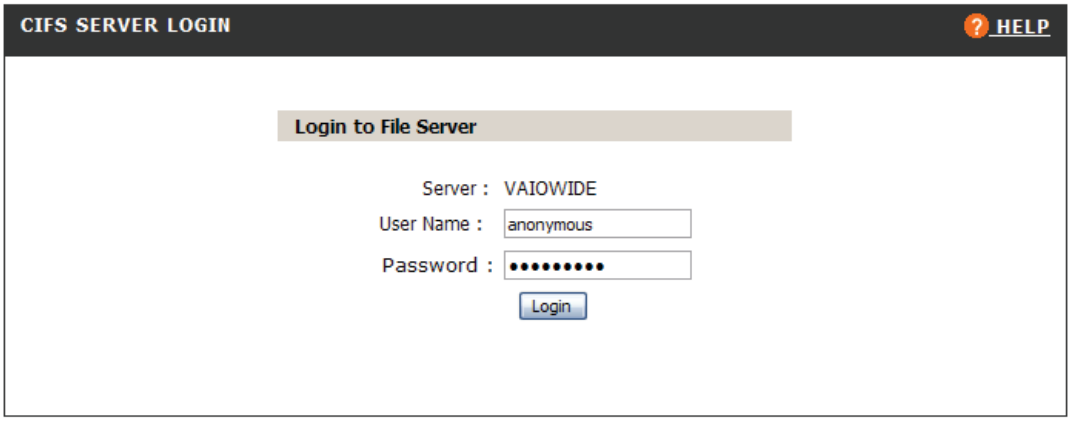
Add New Reference

Click on **Add new reference,** as shown in the following figure, to add references to the newly created category.

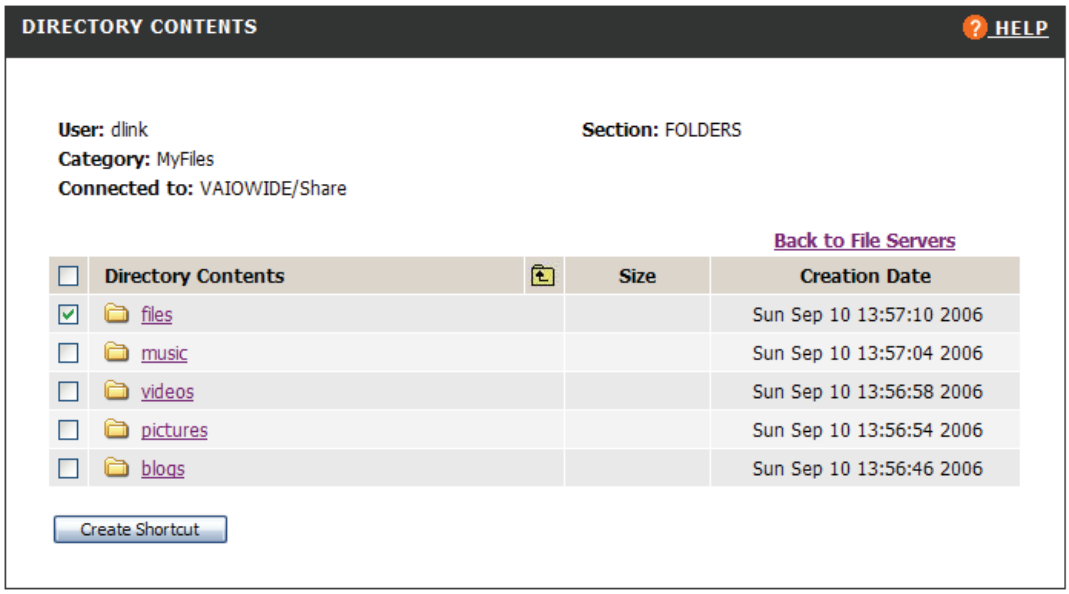


You will be directed to the File Servers List.

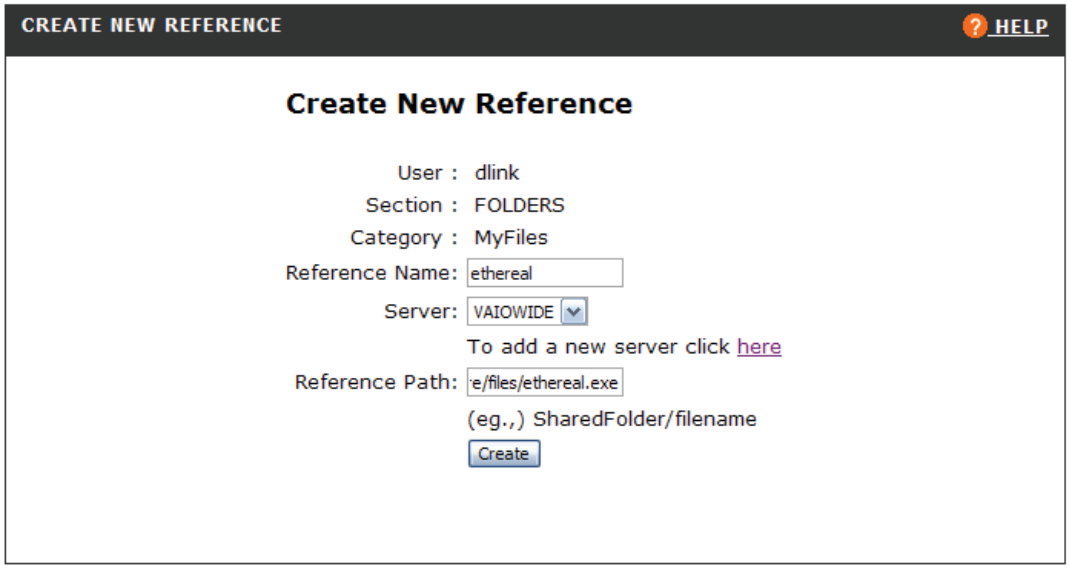
If the server is listed in the File Servers list, as shown in, then select it and provide the **Username** and **Password** of the selected server on the Network as shown below.



After a successful login, browse to the video file and select the checkbox associated with the file to add it to the category. The following figure provides an example for the listing of files and directories from a file server.



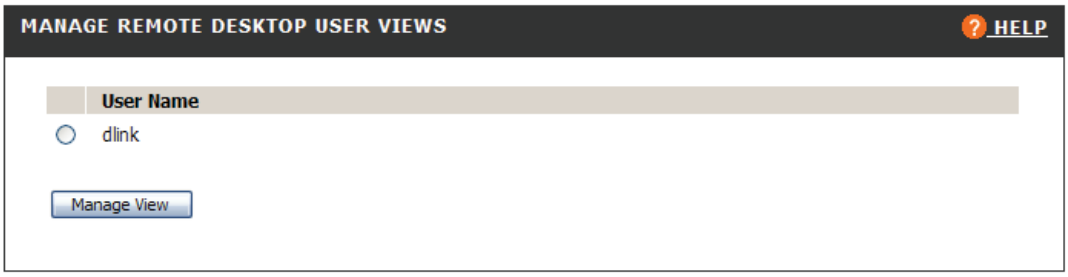
If the server is not listed in the list of file servers, then use the **Click here to add a reference manually** hyperlink on the File servers page, as shown previously. You are then directed to the **Create New reference** page as shown below.



While using the File Browser feature, to add a reference to a Folder category, selection of **Files** is disabled.

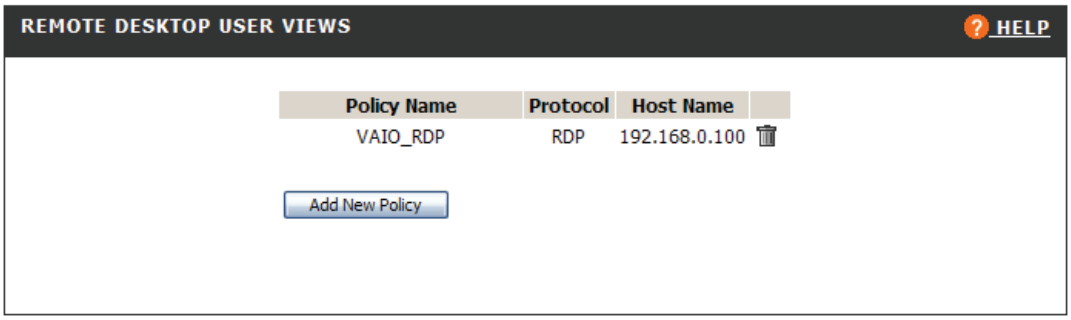
Desktop Links

The DIR-430 will support secured port-forwarded access to PC desktops in the home network. This is provided using VNC/RDP (Remote Desktop) running on those machines. Click on **Desktop Links** under **User Portal** tab on the top panel to manage Desktop links configured for the user as shown in the following figure.



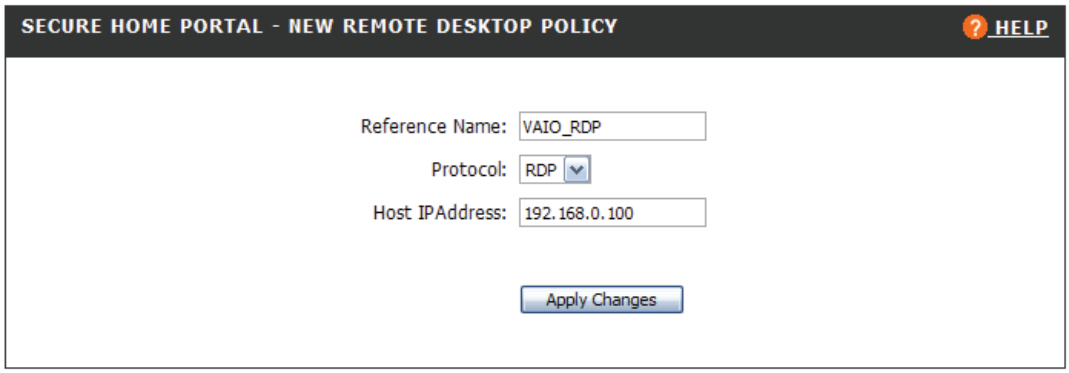
Select the user and click on **Manage View** button to configure desktop links for the user,

The following figure shows current desktop links configured for the selected user.



Here you can create references that allow a user to remotely access your machine. To use this feature you need to host a VNC/RDP server on the machine to which you are creating the reference, and you need to have a VNC/RDP Client installed on the machine from which the User Portal is accessed.

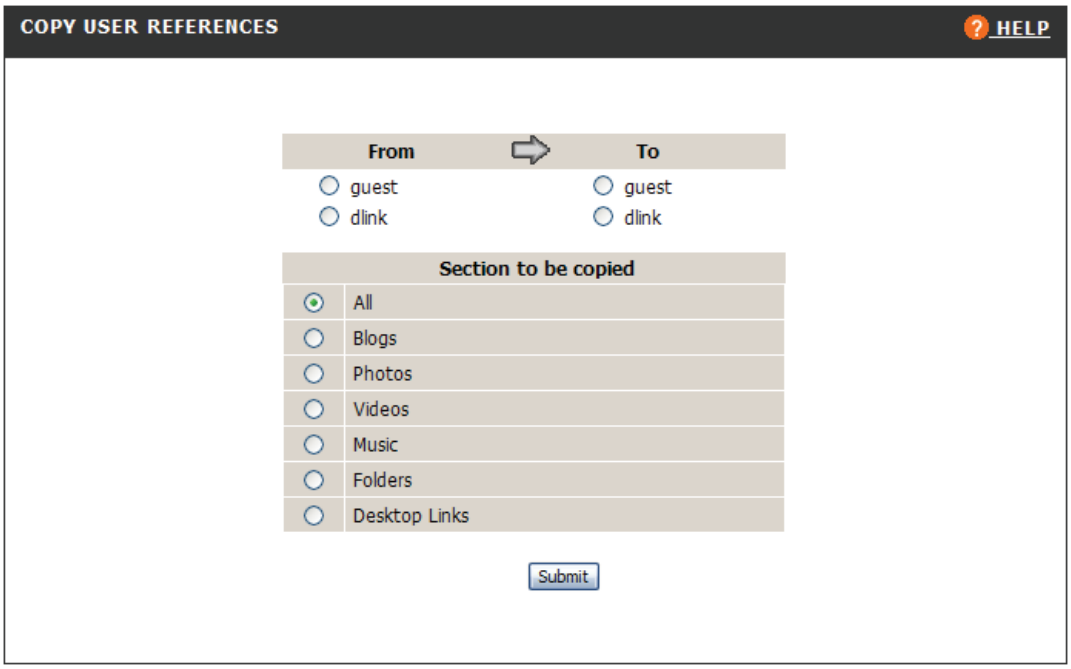
You can add the new policies for a user by selecting the user and clicking on the **manage view** button. As shown in the following figure, you need to enter **Reference Name**, Desktop **Protocol** type and **Host IP Address** of the LAN machine on which the VNC/RDP Server is running. The **Protocol** can be **VNC** if you are configuring a Desktop link for a system on which VNC server is running and **RDP** if RDP server is running on that system.



Desktop links cannot be created for the guest user (this is done for security reasons).

Copy User Views

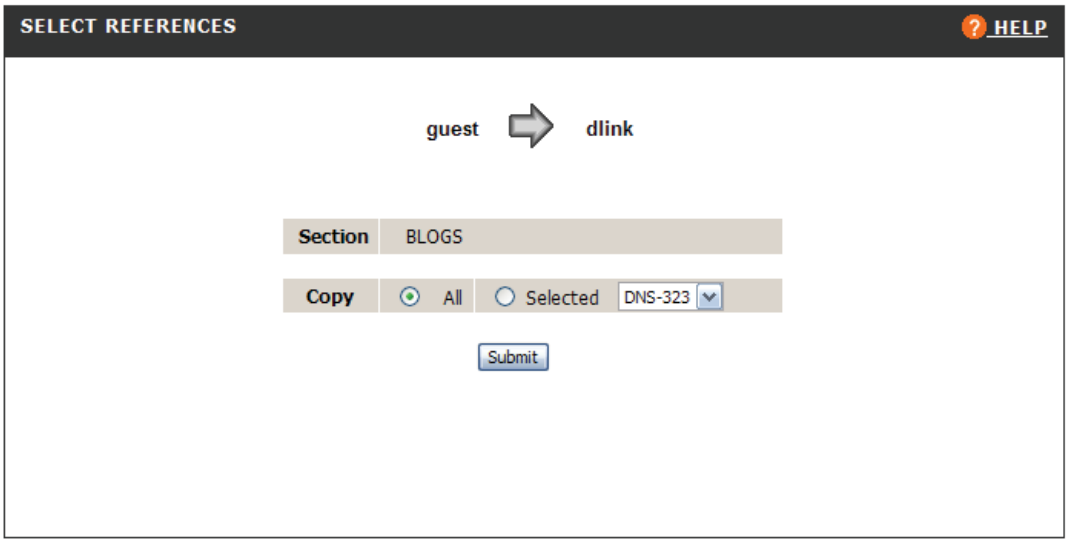
You can copy views of one user to another. Click on **Copy User Views** of **User Portal** tab to copy the views (albums & references in all the sections) of one user to another user.



Select the users in the **From** and the **To** sections and click on interested section to copy the views of one user to another.

If you select the "All" radio button while copying, complete information of the user will be copied.

Alternatively, you can select the section that you want to copy. If you are copying a specific section, then you will be presented with are the albums in that section. Here you can either copy the complete information in that section or copy a selected album.

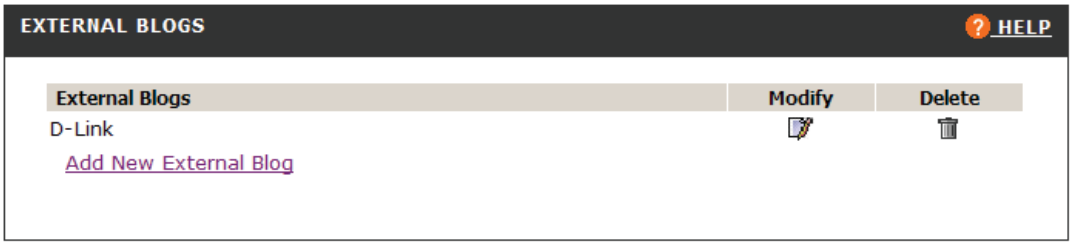


If the destination user has the same reference name/category, then that information will not be overwritten. Only references that does not exist for that user will be copied

When you are copying references of a user "john" (say) to "guest" user, all the sections except the "Desktop sections" will be copied. This is because, for a guest user, we do not allow desktop policies for security reasons.

External Blogs

You can create references to External blogs. Click on **External Blogs** of **User Portal** tab to view currently created external blogs references as shown in the following figure. These references will be displayed in the User Portal. These external blogs will be visible to all the portal users and are not user specific.



To add new external blog, click on the hyperlink **Add new external blog.** Here you need to provide the **External Blog Name** and URI of **External Blog Link** and finally press **Apply Changes** button. You can modify/delete the external blogs created using the modify/delete links.

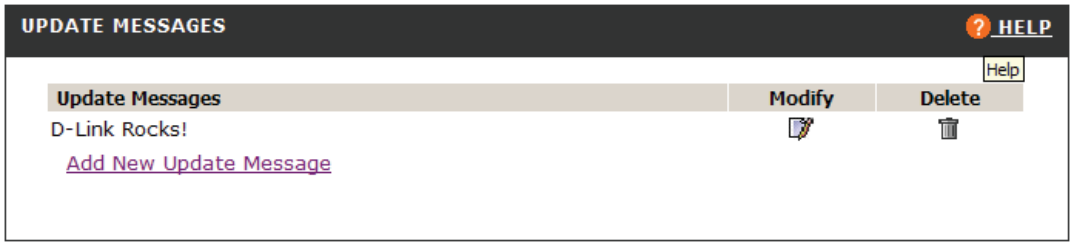
The difference between Blogs under "Manage Views" and "External Blogs" is that incase of the first one, the blog will be static html pages, which are stored locally on some local server, and in case of external blogs, they actually point to some external web server that is hosting the blogs.

You can create a maximum of 5 external blogs at a time.

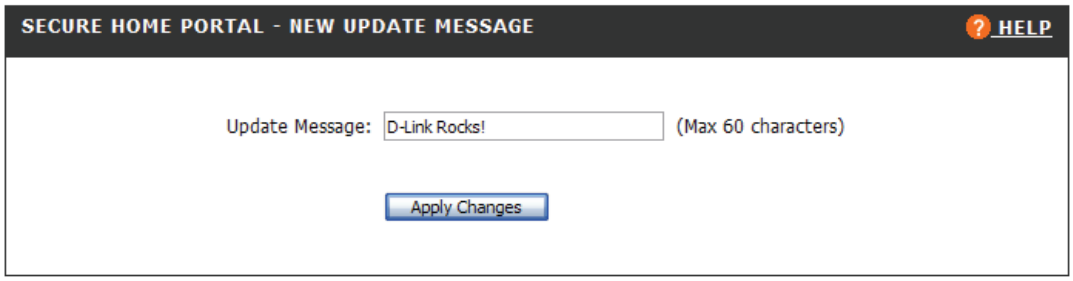
The length of the external blog name is restricted to sixty characters.

Updates

Update messages are small messages, which contain some information. These messages will be displayed on the user portal. Update messages will be visible to all the users and are not user specific. Click on **Updates** of **User Portal** tab to view currently created messages.



You can add a new update message by clicking on the **Add New Update Message** hyperlink. You have an option to modify/delete the update messages at any time. You can add maximum of five Update messages at a time.



Tools

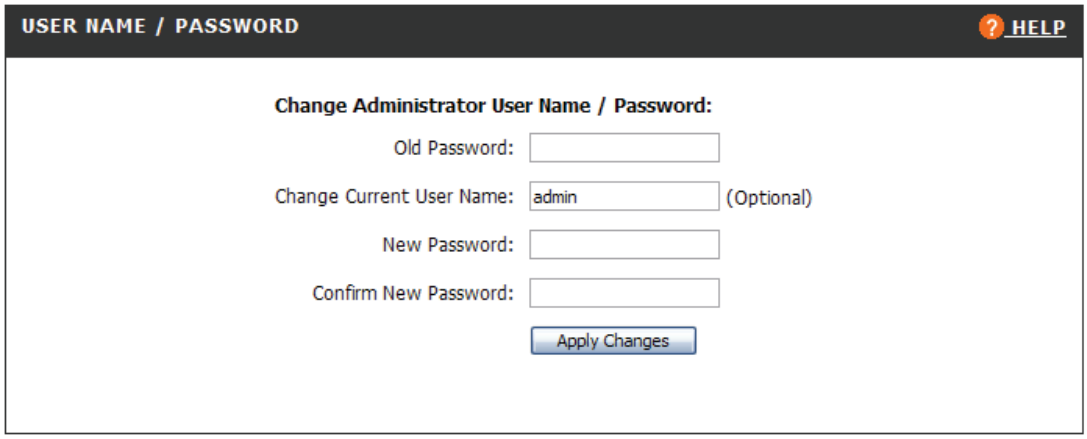
The Tools configuration pages in the DIR-430 provide the administrator access to system specific items.

Admin

Admin configurations allow the administrator account to be modified as well as enabling/disabling box access from the Internet.

User Name / Password

The default username/password of the Gateway can be overridden with your own for the security reasons. To change the user's password, click on **Tools** item in the top panel, then on **Admin** on the left hand menu to show the configuration as specified below. The User's password can be set using this, overriding the old password.



To change the password, enter the default or current password in the "Old Password:" field.

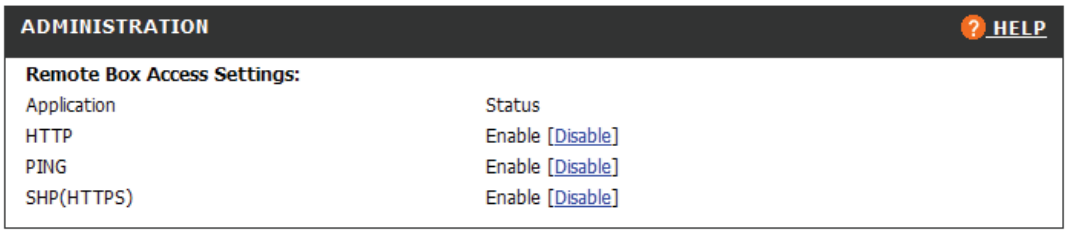
The user name can be changed from **admin** to any name you like. This is optional field. There is only one administrator user account for the DIR-430.

Your new password should be entered in "New password:" field. Re-type the new password in "Confirm new password:" field for confirmation. Press **Apply Changes** button to reflect your password changes.

User must remember the password or note it down in a safe place to access the DIR430 configuration further. In case, you forget the password to access the DIR-430, reset to factory defaults by holding in the reset button for 8 to 10 seconds.

Administration

By default, you will be able to 'ping' the DIR-430 as well as configure it from your local area network and the Internet. If you wish to disallow this traffic from the Internet, you need to configure Administration settings as shown below.

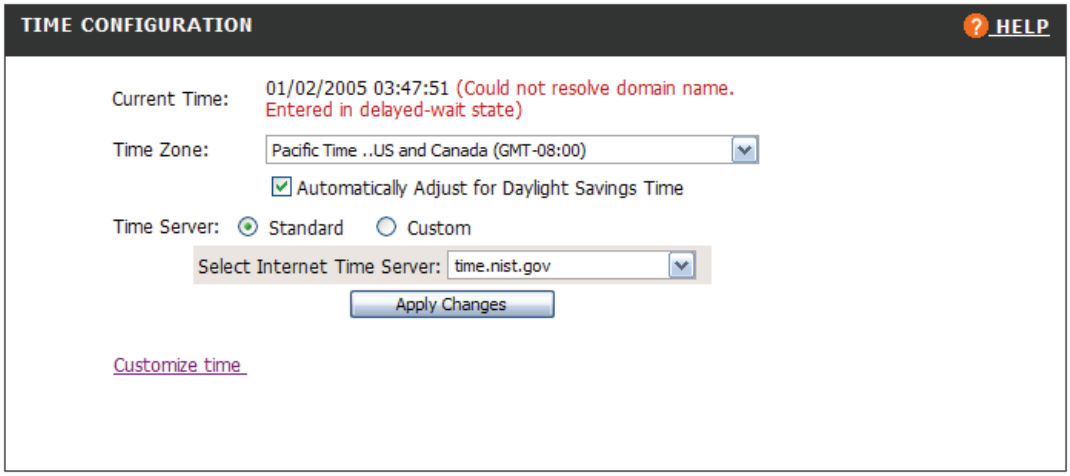


Box Access settings can be changed by clicking **Tools** item on the top pane, then clicking **Admin** on the left hand menu. The policies created cannot be deleted or modified. They may be disabled in case you know the respective feature is to be turned off on the DIR-430, by Disable hyperlink against the entry.

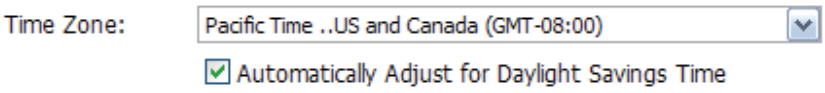
Time

Date and Time settings for the DIR-430 will be utilized by time-sensitive configurations such as Scheduling. The DIR-430 will synchronize the system time automatically from a standard timer server or any other configured time server so that you need not update the DIR-430 time settings manually. The configuration of date and time settings is shown below.

The current time is set in the Gateway in the form of MM/DD/YYYY HH:MM:SS, where MM is month (01-12), DD is date (01-31), YYYY is year represented in four digits, HH is hours in 24-hour format (00-23), MM represents minutes (00-59), and SS represents seconds (00-59).



You can select the appropriate Time zone information from the drop-down list. Also you can enable Daylight Saving Time (DST) support for particular time zone. By default DST support will be disabled.

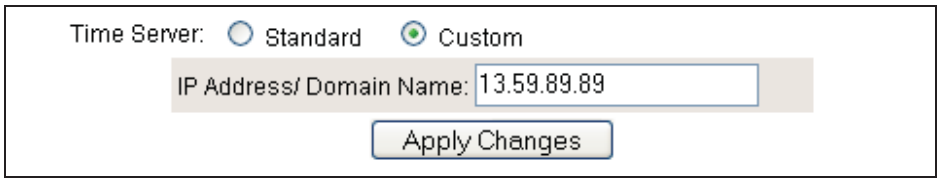


Currently DST support is available for only US and UK time zones. For all other time zones enabling of DST isn't applicable.

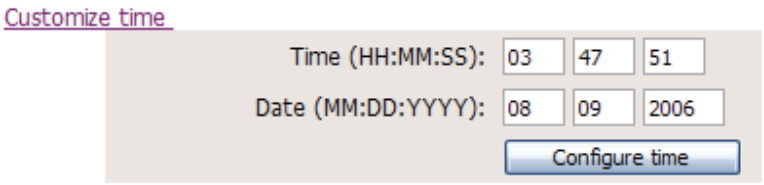
The timeserver can be selected from available **Standard** timeservers or you can choose your own **Custom** timeserver.

To select **Standard** timeserver, click on **Standard** timeserver radio button and choose one from the list of available **Standard** time servers by using drop-down list.

To select your own timeserver click on **Custom** radio button and enter **IP Address/ Domain Name** of the timeserver in the edit box provided.



You may set system time manually by clicking Customize time hyperlink and enter date and time in the edit box provided. The manually entered time information persists till the Gateway is power cycled.

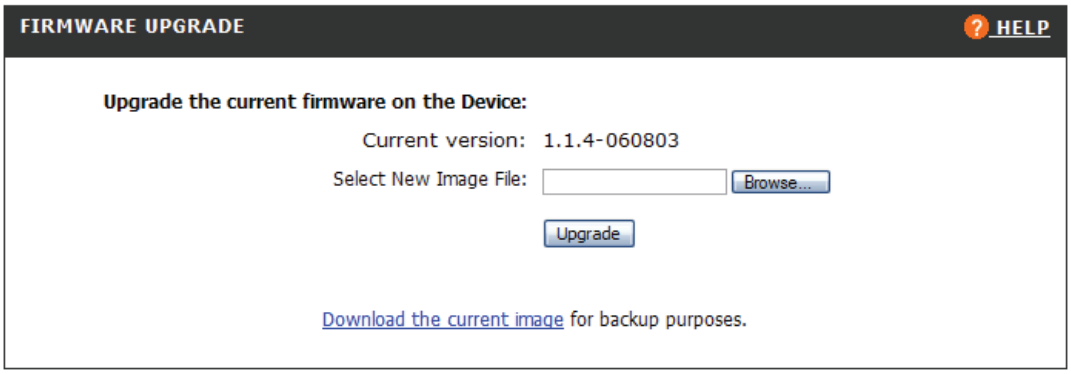


Firmware

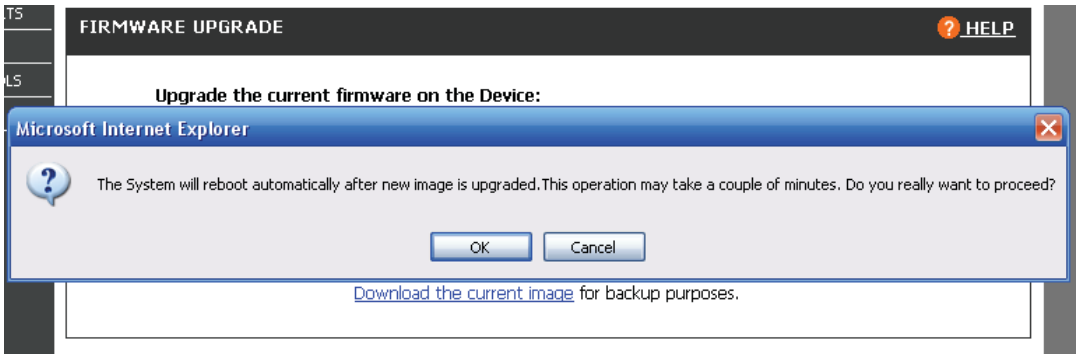
Before you can upgrade firmware, you must download the latest firmware version from the D-Link Support Website http://support.dlink.com.

It is highly recommended to store the current image on your PC before you perform firmware upgrade operation. DO NOT perform the upgrade over a wireless connection. Doing so may render the device unusable.

To upgrade firmware on the DIR-430, click on **Tools** on the top panel, and then click on **Firmware** on the left hand menu to show the configuration as outlined below.



Click on **Browse...** button, select the downloaded image and click on **Upgrade** button. The DIR-430 will be rebooted automatically in order to reflect your new image. A pop up window will be displayed to notify of the reboot. Clicking the Ok button will continue the upgrade process, cancel button will stop it.



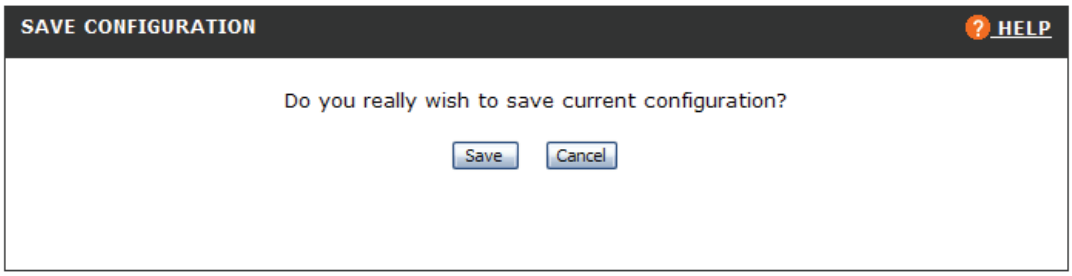
Once user enters the Ok button, you would observe the progress of the firmware upgrade as shown below. Please note that the operation takes a few minutes.

Once firmware upgrade is successful, you will see that the DIR-430 gets rebooted automatically. If it does not reboot and give you the web configuration login page, power cycle the DIR-430.

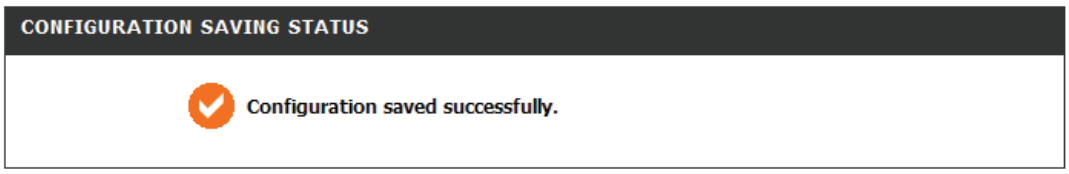
In case the DIR-430 is powered down, or disconnected from the network during firmware upgrade, the firmware may be corrupted. Please contact D-Link Technical Support for a resolution if within the factory warranty period.

Save Configuration

The user can save the current configuration to exist for the next reboots irrespective of any configuration changes done to the Gateway. This allows the user to configure the Gateway for customized behavior.



After making different configuration changes, once stable configuration exists on the Gateway, click on **Save Configuration** shown on the top frame of the HTML configuration page as in. In the resulting page as shown in, you will be prompted to press **Save** or **Cancel** buttons for saving the configuration.

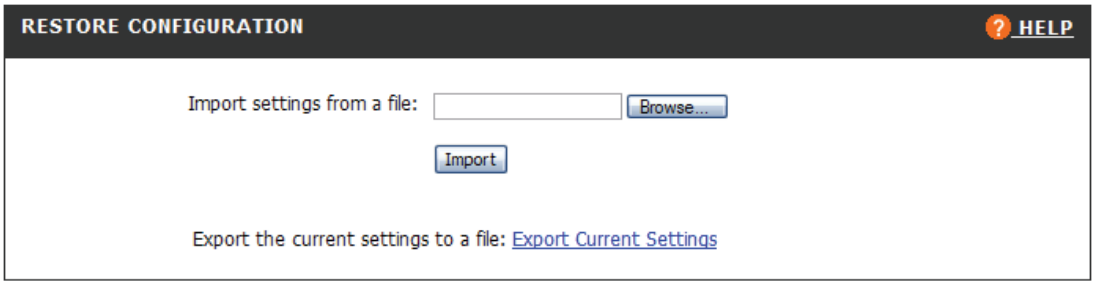


By pressing **save** button, the configuration will be saved onto the Gateway for next reboot overriding the configuration saved earlier. Press **Cancel** button to cancel the operation.

Restore Configuration

As a user you may like to take backup of configuration in cases like firmware upgrade, experimenting with configuration to customize Gateway's behavior.

Before you do such an operation, it is strongly advised to take a backup using **Backup configuration** facility. To take a backup of configuration, click on **System Settings** link, and then click on **Backup Configuration** hyperlink to open configuration page as shown below. To export current Gateway settings to a file, click on Export Current Settings hyperlink in the page. This opens a window for you to select the filename in the location you choose. Once you select **OK** button on the window, it shows the status of the operation.



To import previously stored Gateway settings in a file, type in the file name in the edit box provided on this page, or click on **Browse...** button next to it, to choose the file name. Click on the **Import** button to import settings to the DIR-430. The operation shows the final status as shown below.

Factory Defaults

This option is useful in a situation when, you are unable to revert back the configuration changes, or if you find the configuration saved onto the Gateway is not good to be used.

As shown in below, to set the factory defaults click on the **Tools** item on the top panel, and click on **Factory Defaults** on the left hand menu. You will be asked to respond to a question on whether to restore the factory defaults. Clicking on **Yes** button restores the factory default settings onto the Gateway.

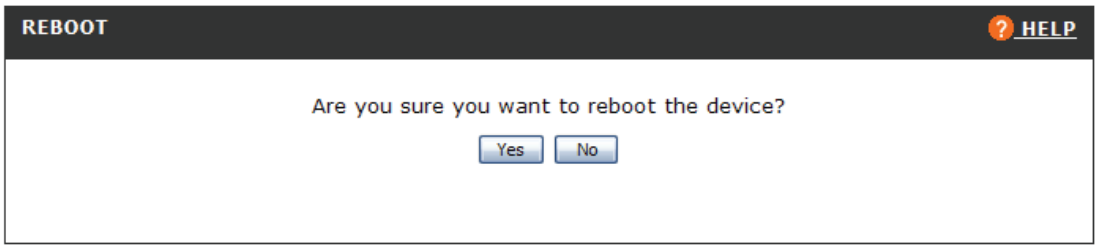
The entire manual configuration done by you earlier will be erased when factory defaults are set including the user's password.

Reboot

To reboot the Gateway for any reason, click on **Tools** on the top panel, and click on **Reboot** on the left hand menu. You will be asked for confirmation of the reboot with **Yes** or **No** buttons.

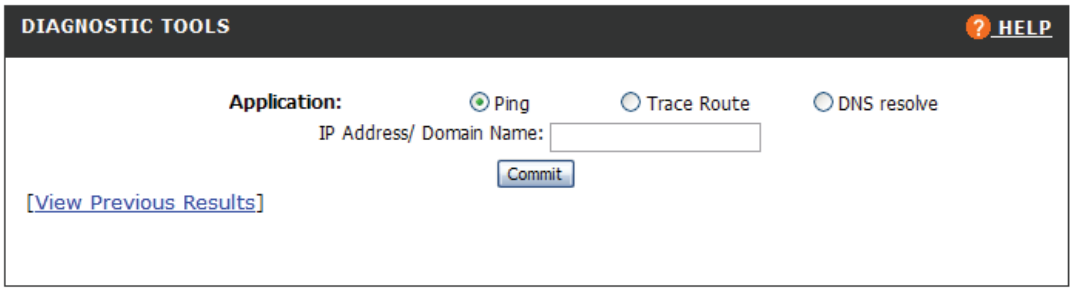
Press **Yes** button to reboot the box. Though there is a physical reset button on the Gateway, rebooting the box using HTML configuration is lot easier.

It is recommended to use this operation after firmware upgrade. This operation is specifically useful when the Gateway is not easily reachable physically.



Press **No** button if you do not want to reboot the box.

Diagnostic Tools



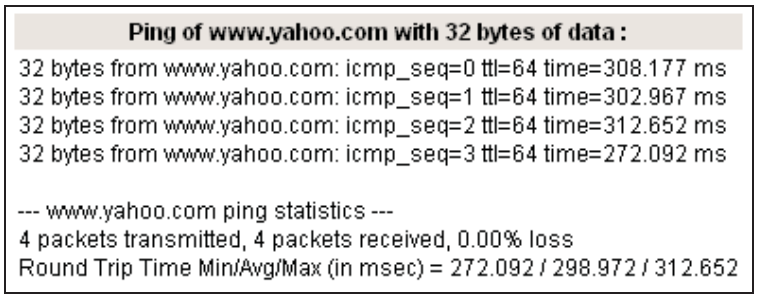
You may like to check whether there is connectivity to a particular website or a computer on the Internet from the DIR-430, or to evaluate whether there is certain delay in the network to reach your target host. There are two important diagnostic tools that help you identify and realize the behavior of the network.

To use these diagnostic tools, click on **Tools** hyperlink on the top panel, and then click on **Diagnostic Tools** on the left hand menu to open the configuration page.

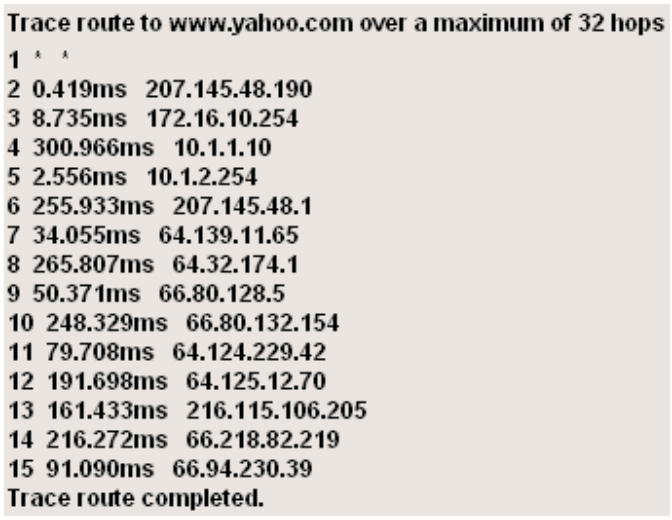
Ping can be used to check whether the host on the Internet can be reached from the DIR-430. Type an IP address (like 202.56.89.78) / domain name (like www.yahoo.com) in the edit box provided. Click on **Ping** button, and wait, to see the responses as shown below.

When Packets sent/received fields are greater than zero, then the connectivity exists.

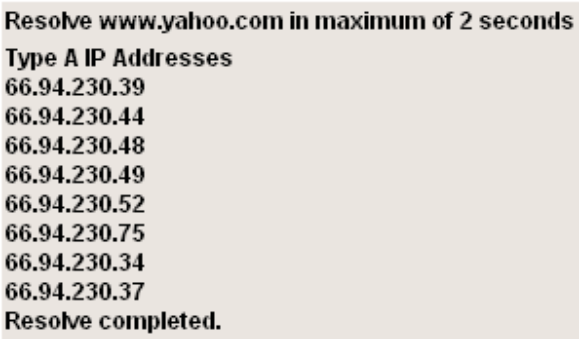
The data in the figure also shows the packet loss percentage in addition to minimum, maximum and average round trip times.



Trace Route option shows you the number of hops your data goes through for the specified remote host. You may input either IP address or domain name. The following figure shows the output format for Trace Route to domain www.yahoo.com.



DNS resolve option helps you find the IP address of a valid domain name. Select DNS resolve radio button, type in the domain name in the entry box provided, and click the **Commit** button. The following figure shows the output format for Trace Route to domain www.yahoo.com.

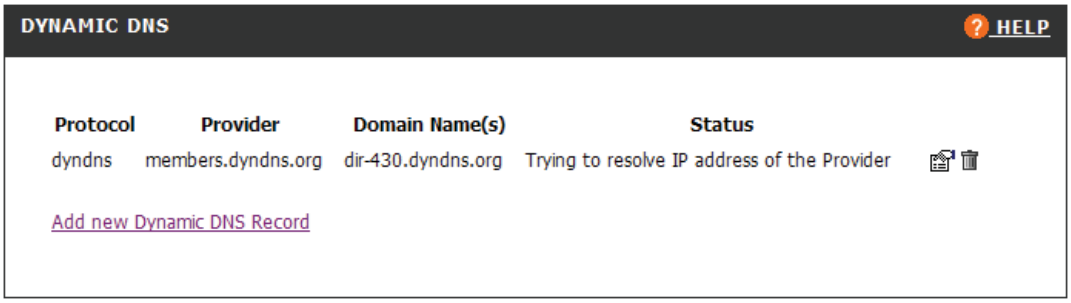


Dynamic DNS

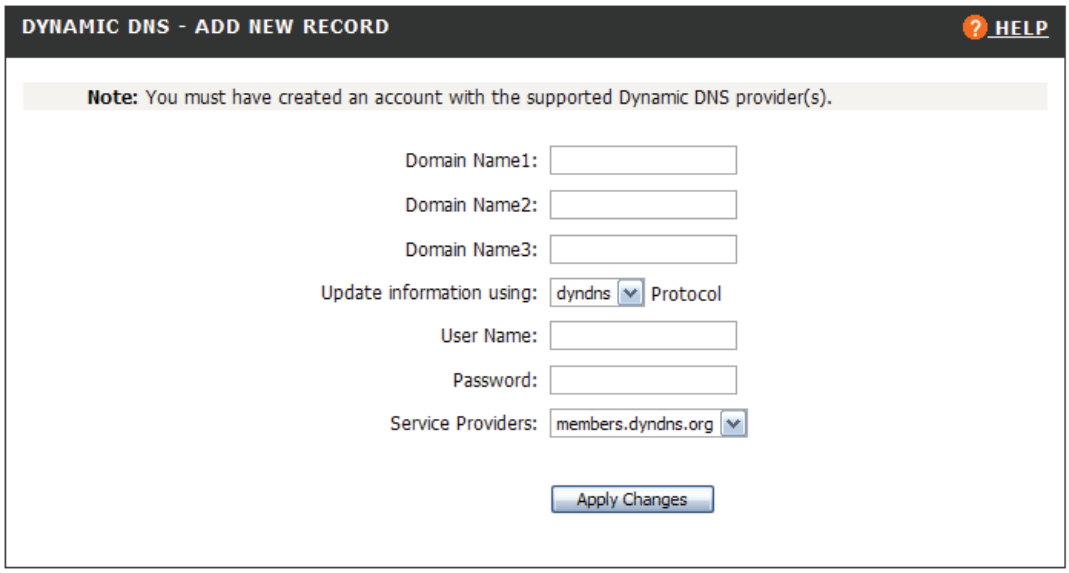
The DIR-430 features Dynamic Domain Name System (DDNS) support. This feature lets you assign a fixed host with a fixed domain name though IP address of the host changes dynamically. It is useful when you are hosting a website, running FTP service or any other service in your internal private network connected to the DIR-430, and make any useful information accessible anywhere on the Internet.

You must have Internet connectivity and you need to register with DDNS service provider using website http://DynDNS.org/. Create an account using URL https://www.dyndns.org/account/create.html after providing user name, password and domain name you require for hosting your server. Using the just created account, you can now create the five free domain names like xxxxx.dyndns.org when connected to http://members.dyndns.org.

Now, this information is to be used in the DIR-430 configuration in order to make your local PCs accessible from the Internet using the domain names you created. To configure, click on **Network Settings** hyperlink and then **Dynamic DNS** hyperlink on the left pane, to open up the configuration page as shown below. It shows the list of dynamic DNS entries, and their status. To modify an existing record, click on icon. To delete one, click the icon on the same line.



To create a new Dynamic DNS record, click on the Add New Dynamic DNS Record, to open a configuration page as shown below.



Domain Name 1, 2, 3 are the three domain names you registered with the dyndns.org website. You may like to specify the three domain names out of the domain names that you registered earlier.

Update information using: Currently only dyndns protocol is supported on this product.

Provide the **User Name** and **Password** with which the domain name accounts are created.

Choose **Service provider** field based on the website you used to create the DNS names. From the drop-down list against this field, choose members.dyndns.org.

Click on **Apply Changes** to add a DDNS service record.

To modify the existing record, click on the icon on the entry from the previous page.

Status

The Status section displays information relating to the Network interfaces and their current status as well as internal Logs that may help to debug/troubleshoot network issues.

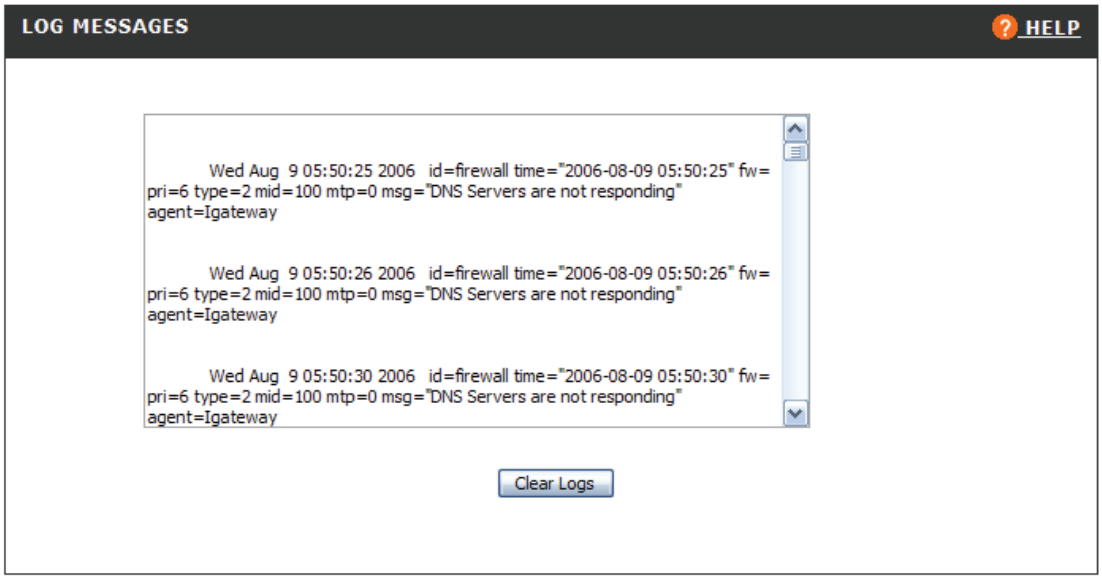
Device Info

The Device Info section provides information pertaining to your DIR-430 and its network Interfaces.

To access the Device Info section, click on Status on the top panel. The Device Info page will display as shown in the following figure.

Logs

The Logs section displays firewall attacks and authentication failure logs. Click on **Logs** of **Status** tab to view all the logged information



Logout

You may like to logout once your configuration is complete. You will find the **Logout** section by clicking the **Status** tab, then clicking **Logout** on the left hand menu. Clicking on the **Logout** prompts you with a question on how it should be logged out. This case is shown below.

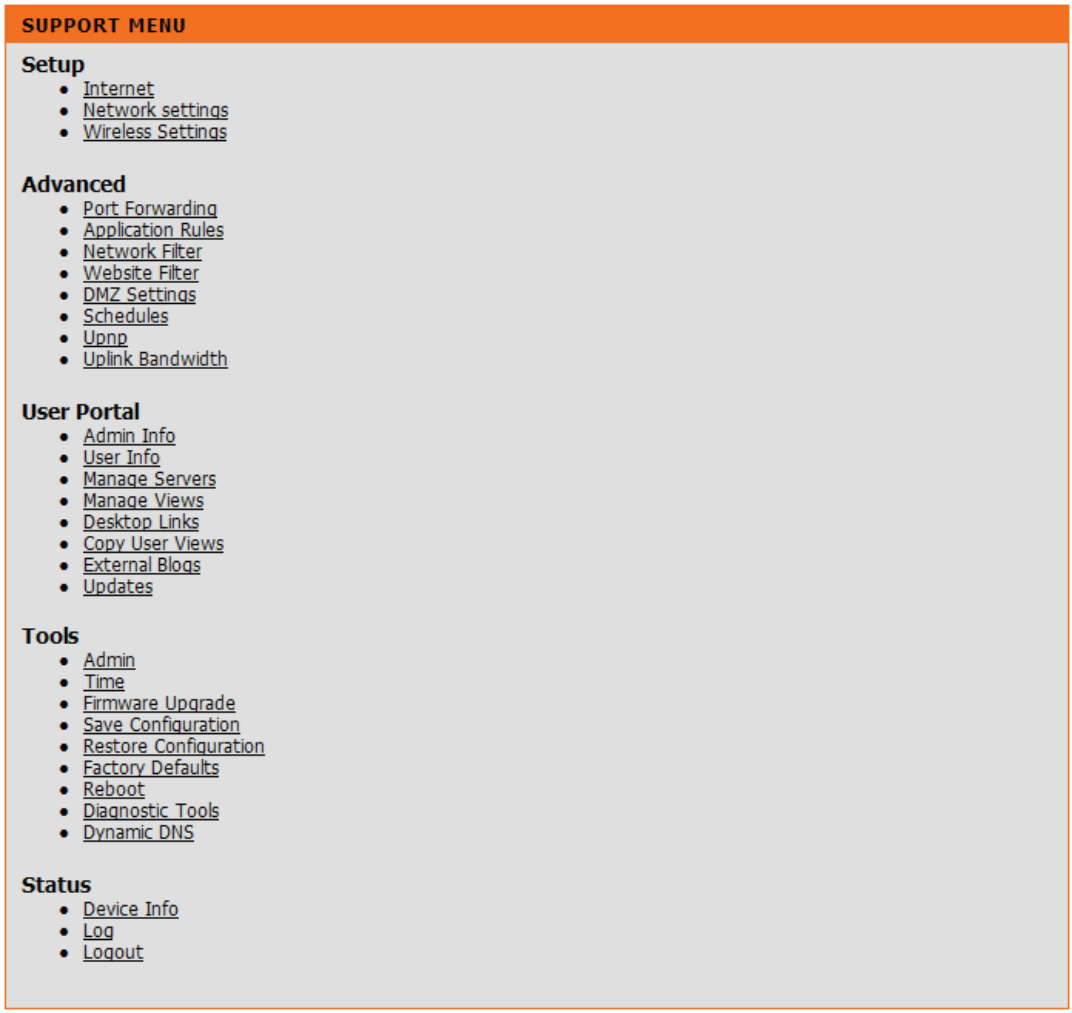
You should click on the **Save** and **Logout** if you require the current configuration on the DIR-430 to be used upon rebooting.

Else, you may click on **Logout without Saving** if you need this configuration for the time the DIR-430 is running, but not for next reboot.

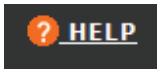
Cancel button cancels the logout operation and allows you to configure more.

Support

The Support section contains information pertaining to the DIR-430 features and configurations. To access the main index of all information contained within the DIR-430 click on the Support tab.



For context relevant information, click the **Help** Icon in the upper right corner of each configuration page.



Appendix A: Troubleshooting

I forgot my administrator password, what do I do?

Reset the DIR-430 to factory default settings by holding down the reset button for 8 seconds. Please note that all configurations will be lost. It is advised to keep a backup file of the configuration settings on a local PC in the event the DIR-430 needs to be reset.

Can my DIR-430 be a DSL modem as well?

No. Your DIR-430 provides firewall and VPN security to the internal network. Your DIR-430 should be connected behind your DSL or Cable modem. Your DIR-430 acts as a simple host towards the Internet.

Does the DIR-430 support protocols other than IP?

No. Your DIR-430 supports only Internet Protocol.

What is the Network Address Translation?

IP Address is translated for two purposes by a Gateway that connects two networks. One reason is to save number of IP addresses on one side, the other, to hide the internal IP addresses of the hosts.

Which Microsoft Windows platforms does the DIR-430 support?

The DIR-430 supports Windows 2000, XP, and 2003 versions. Others may work, but there is no support from D-Link for anything but the aforementioned.

Do I have DHCP address or static IP address?

By default, the DIR-430 uses DHCP client to connect to the Internet. Please ask your ISP if it is offering static IP. If static IP is offered, configure static IP using WAN hyperlink in the Web configuration pages.

What is the URL to configure my DIR-430?

Open browser, and type in http://192.168.0.1/ as URL.

What browsers may be used to configure the DIR-430?

Internet Explorer 6.0, Netscape Navigator 7.x, Mozilla Firefox 1.5, and Safari. Other browsers may work, but are not supported.

Any reasons why I don't get the DIR-430 configuration screens in my browser?

Check the connections and validate the connectivity using "ping" tool. You may like to run "ping 192.168.0.1" from your PC. If successful, check your browser settings; remove proxy settings if they are set.

For Internet Explorer 6.0, click **Tools** menu, and **Internet Options**. Click on **connection** tab. Make sure it is set to **Never Dial a connection**. Also, click on **LAN settings** button to open a window, and uncheck "**Use a proxy server for your LAN ….**"

Which modems work with my DIR-430?

Your DIR-430 can work with virtually all standard DSL and Cable modem available in the market.

What is the maximum Secure Portal connections supported?

5.

How do I know what IP address my PC has?

Click on **Start** button on the Windows task bar. In Start button menu, click on Run…. In the window opened, enter cmd to get the console window. On the console, run ipconfig /all command. This will display the IP address of your PC. If there are multiple interfaces, you may have more than one.

How do I know whether I can reach a machine from my PC?

Use Diagnostic tools from the configuration.

What applications does the Firewall have knowledge of?

Please refer to the section on configuring Port forwarding for the list of applications that the firewall is aware of.

How can I know what protocol is used currently for Internet?

The Device Info page in the Status section of the DIR-430 web configuration has information about the WAN connection status and type.

How will I be notified of new DIR-430 Firmware upgrades?

You may visit the D-Link Technical Support website periodically to check for updates.

What applications are supported by UPnP?

At present, MSN Instant Messenger is the only application that may use UPnP.

Please visit http://support.dlink.com for unanswered questions.

Appendix B: Glossary

Adapter – Electronic circuitry that converts one form of input to a different form of output so that it fits for your PC or Gateway. **Examples** are Power Adapter, Ethernet Adapter, and DSL Adapter.

Backbone – The part of a network that connects many systems and networks and handles high volume of data.

Bit – binary digit with values 0 or 1 in the binary numbering system.

Boot – When your Gateway or PC is powered on, the built-in instructions in a ROM chip that are automatically executed to search and load operating system and pass control to it.

Bridge – A device that provides connectivity between different networks.

Broadband Connection – Media that offers higher bandwidth that has capability to allow voice, video and data transmission. Now a days, Cable television network and Digital Subscriber Line (DSL) do offer residential broadband connections.

Browser - A browser is an application program that allows the user to browse through the web pages on your PC. For example, the browser can be used to look at web (html, shtml, xml) pages and download files that are available using FTP.

Cable Modem – A device that connects a computer to its Ethernet port and then to Internet through the Cable TV network. Once connected, cable modem users have a continuous connection to the Internet. Cable modems support bandwidth of 36 Mbps downstream (from the Internet to the computer), and from 200 Kbps to 2 Mbps upstream (from the computer to the Internet).

CAT 5 cable – ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of standards that specify "CATegories" of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. CAT 5 cable has a maximum throughput of 100 Mbps and is usually utilized for 100BaseTX networks.

Data Packet – It is a collection of bits sent over a network at once. For example, an Ethernet packet can be from 64 to 1518 bytes in length.

DDNS – Dynamic Domain Name System allows a network device with a dynamic Internet IP address to have a fixed host and domain name, such as abcd.mydomain.com. It is useful when you are hosting your own website, FTP server, or other server behind a router, so people can find your site no matter how often the Internet IP address changes. Using DDNS requires registering with a DDNS service provider on the Internet.

Default Gateway – The routing device used to forward all traffic that is not addressed to a station within the local subnet.

Denial of Service – When an attacker floods packets continuously to occupy the network bandwidth, your PC will not be able to respond to any other service requests. This leads to Denial of Service. The attack is called Denial of Service attack.

DES – Data Encryption Standard, a standard by which sender and receiver use a shared secret key to encrypt or decrypt the data. The key length used is 56-bits in this standard.

DHCP – Dynamic Host Configuration Protocol. All hosts/gateways that are in the network need to have an IP address to communicate. Without this protocol, you have to manually specify the IP address in a host/gateway. This protocol allows all IP address assignments to be centralized and automate the assignment of Internet Protocol (IP) addresses in an organization's network. The User of a DHCP server can configure the lease time of an IP address to be used by a DHCP client. It also supports static IP address assignment for fixed hosts/gateways if they run application servers.

DMZ (De Militarized Zone) - Allows one IP address (or computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP address if you want to use DMZ Hosting.

DNS – Domain Name System maps the domain name against an IP address. People remember meaningful domain names easily than the IP address that is in the form of numbers.

Domain – A sub network comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

Download – Receive the file from the network.

DSL – Digital Subscriber Line, Your telephone line is used as a digital carrier that can allow both data and your normal telephone. DSL can be always be powered on. It need not be dialed every time you are trying to connect to Internet.

Daylight saving time (DST) - time observed when clocks and other timepieces are set ahead so that the sun will rise and set later in the day. The amount of daylight on a given day of the year at given latitude is fixed, but over the year the hours of sunrise and sunset vary from day to day. During the summer months, the sun rises earlier and sets later and there are more hours of daylight. If clocks and other timepieces are set ahead in the spring by some amount (usually one hour), the sun will rise and set later in the day as measured by those clocks.

Dynamic IP Address - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that offer services like web, printer do not generally use DHCP. They are assigned with static IP addresses.

Encryption – A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

Ethernet - Supports 10 Mbps speed, this IEEE standard network protocol specifies how data is placed on and retrieved from a common transmission medium. This is the physical carrier for all TCP/IP protocol and its application messages.

Fast Ethernet – Same as Ethernet but supports 100 Mbps speed. Fast Ethernet uses CSMA/CD network access method.

Firewall – A firewall can be a software/hardware device that is located as network gateway to protect your private network from the attacks that can happen in the public Internet. It examines each packet to determine whether to forward it towards its destination.

Firmware – Binary code that is written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off.

FTP (File Transfer Protocol) – Protocol used to transfer the files across the TCP/IP network. For example, placing the files on to a web server uses FTP protocol.

Full Duplex – A device is capable of full duplex when it can send data simultaneously in both directions.

FQDN - A fully qualified domain name consists of a host and domain name, including top-level domain. For example, www.yahoo.com is a fully qualified domain name. www is the host, yahoo is the second-level domain, and.com is the top level domain.

Gateway – Device that can connect two different networks supporting two different communication protocols.

Half Duplex – A device is capable of half duplex when it can send data in both directions, but not simultaneously.

Hardware – All electronic component that are visible physically. Example, Electronic circuit boards in PCs, Gateway.

Hop - The link between two network elements.

HTTP (Hyper Text Transfer Protocol) – Protocol that allows web pages to be transferred over the Internet.

ISP (Internet Service provider) - A company that offers internet access, services such as web site building, virtual hosting to individuals and companies.

LAN (Local Area Network) – A group of computers/gateways/routers connected that can communicate each other in a small geographic area.

MAC (Media Access Control) – Every Ethernet networking device such as network adapter will be assigned with a unique number so that they can communicate.

MD5 – A type of one-way authentication scheme that uses passwords. The password is hashed and sent over the network so that only the sender and authenticator know about it. It is not very secure authentication mechanism when compared to others like EAP-TLS or EAP/TTLS.

NAT (Network Address Translation) – IP Address is translated for two purposes by a Gateway that connects two networks. One reason is to save number of IP addresses on one side, the other, to hide the internal IP addresses of the hosts. In the case of NAT, when the traffic is generated from your private network to public Internet, the source IP address of the packet generated will be transformed to the public address of your Gateway. The end user receiving the traffic perceives the packet to be generated by your Gateway.

Network Mask – Look at Subnet Mask.

Packet – A unit of data routed from an origin to its destination in a network.

Packet Filtering – Discarding unwanted network traffic based on its originating address or range of addresses or its type (e-mail, file transfer, etc.).

Ping (Packet INternet Groper) – Utility used at the network elements (PCs, routers) to determine whether a particular IP address is reachable and its delay to reach that network element.

Plug-n-Play – When a device or an expansion board is attached to a computer system they should be running without rebooting your computer system.

Port – A physical male or female sockets that can be hooked for plugging in communication lines, modems and printers.

PPP (Point to Point Protocol) - Protocol that is used by your dial-up modem for your PC to connect to the Internet. PPP protocol runs between dial-up modem and ISP. Once PPP connection is established, your PC gets Internet connectivity.

PPPoE (Point to Point Protocol over Ethernet) – It is a method that encapsulates PPP packets over Ethernet frames from the user to the ISP over the Internet. PPPoE is preferable by ISPs because it provides authentication (username and password) in addition to data transport. A PPPoE session can be initiated by either a client application residing on a PC, or by client firmware residing on a modem or router.

PPTP (Point to Point Tunneling Protocol) – The protocol defines the tunneling service in IP network to carry PPP protocol messages. One example of a tunneling service is secure access from a remote small office network to a headquarters corporate intranet via a Virtual Private Network (VPN) that traverses the Internet. They can also be used for residential purposes.

RJ – 45 (Registered Jack – 45) - A connector used for connecting Ethernet devices that holds up to eight wires.

Reverse Network Address Translation – When an Internet user tries to access a service at your Router/Gateway, the request made by the Internet user will be forwarded to an internal machine that serves the request. This is achieved by translating the destination IP address of the packet to private Local IP address of the PC where service is offered. This operation is exactly reverse of the NAT operation.

Router – Device that routes the packets across various sub networks that are attached to. It helps in managing the large networks in to smaller ones. They operate at IP layer of TCP/IP protocol suite.

Security Association – These are the parameters to be set for having a VPN tunnel.

Server – A computer that services the users on a network, may be to access files, web pages, printing.

Software – It is a series of instructions that control the behavior of the computer and its hardware.

Stateful Packet Inspection – Firewall that monitors the state of the transaction for the internal hosts. It looks at the internals of the packet and adjusts the firewall policies automatically based on the state but specific to the port requested/required. Hence this is more secured than the static packet filters which are not intelligent of states of transactions.

Static IP Address – Permanent IP address that is assigned to a host/router in an IP or TCP/IP network.

Switch – Device that connects host computers, large number of devices to share a limited number of ports. 2. It helps users to make, break, and change the connections physically on an electric circuit.

Subnet Mask – The method used for dividing IP networks into small networks called subnets. The division is determined by a binary pattern (called mask). Based on this mask (subnet mask), IP addresses of the hosts in that subnet can be assigned.

TCP (Transmission Control Protocol) - A setup of rules used to transmit data along with the IP (Internet Protocol) to split the data to be transmitted into small pieces. TCP creates connections with its peer to send the data. The protocol offers reliability of the packet transmission and adds delay in the network. Applications that assume unreliable networks generally use TCP.

TCP/IP – (Transmission Control Protocol / Internet Protocol) Set of protocols for communications over a network developed specifically for the Internet. TCP/IP defines a suite or group of protocols that involves many protocols like ICMP, RIP, DHCP, etc.

Throughput – The data sent successfully through the Internet in a given time period.

UDP (User Datagram Protocol) - A setup of rules used to transmit data along with the IP (Internet Protocol) to split the data to be transmitted into small pieces (called datagrams). UDP does not create a connection with its peer to send the data. Hence it is "connection-less", unreliable, but faster because there is no connection setup delay.

Upgrade – To replace the firmware version of the DIR-430 with a newer version.

URL (Universal Resource Locator) - It is the address that defines the route to a file on the Web or any other Internet resource. These can be accessed through typing the URLs in to the browser, or by clicking the hyperlinks on the existing web pages on the browser.

VoIP (Voice over Internet Protocol) – VoIP is a technology that makes use of your existing Internet connection instead of normal PSTN. When you connect your telephone on your RGS Gateway, the voice gets converted into digital information, which will be transmitted on the Internet. At the receiver's end, the reverse operation is performed.

VPN (Virtual Private Network) - A technology with which hosts communicate over public communication networks by creating private communication channels called tunnels. This is mostly achieved through encrypting the traffic at the originating point and decrypting the traffic at the destination point. Examples of VPN technology are, PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPSec (Internet Protocol Security).

VPN end point – A host connected to a router (or the router itself for the router related data traffic) has the ability to establish a VPN tunnel to some other host supporting VPN.

WAN (Wide Area Network) - Networks that cover communication over a large geographic area. These are through public networks like telephone (DSL) or cable Networks, through leased lines or satellites. Internet is a Wide Area Network.

Appendix C: Warranty Information

D-Link®
Building Networks for People

Limited Warranty
(USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in

the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

CE Mark Warning: This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: ***This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:***

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Appendix D: FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE: FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

We declare that the product is limited in CH1-CH11 for 2.4G band by specific firmware controlled by the manufacturer and is not user changeable.

IC statement

Operation is subject to the following two conditions:

1) This device may not cause interference and

2) This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

IMPORTANT NOTE:
IC Radiation Exposure Statement:
This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Reglement d'Industry Canada
Les conditions de fonctionnement sont sujettes a deux conditions:
1) Ce peripherique ne doit pas causer d'interference et.
2) Ce peripherique doit accepter toute interference, y compris les interferences pouvant perturber le bon fonctionnement de ce peripherique.