SWR-8225 USER MANUAL

EPIVALLEY

WiMAX Mobile Hotspot Router

WiMAX Mobile Hotspot Guide

Version 04.27.2010

Table of Contents

The Browser Interface and Settings 2
Home 3
WiMAX 3
    Status. 3
    Configuration. 4
Network 4
    Local Network 4
    Network Address Server 5
WiFi 5
    Status. 6
    Basic 6
    Multi SSID 7
    Secure Profile 7
    Trusted MAC Filtering. 9
Advanced 9
    Firewall. 9
        Port Filtering 10
        VPN Passthrough 10
    Traffic Control. 11
        Port Forwarding 11
        DMZ. 11
    Management 12
        Account 12
        Backup & Restore 12
        Power Management. 13
        Factory Default 13
    Firmware Upgrade 13

Help 13

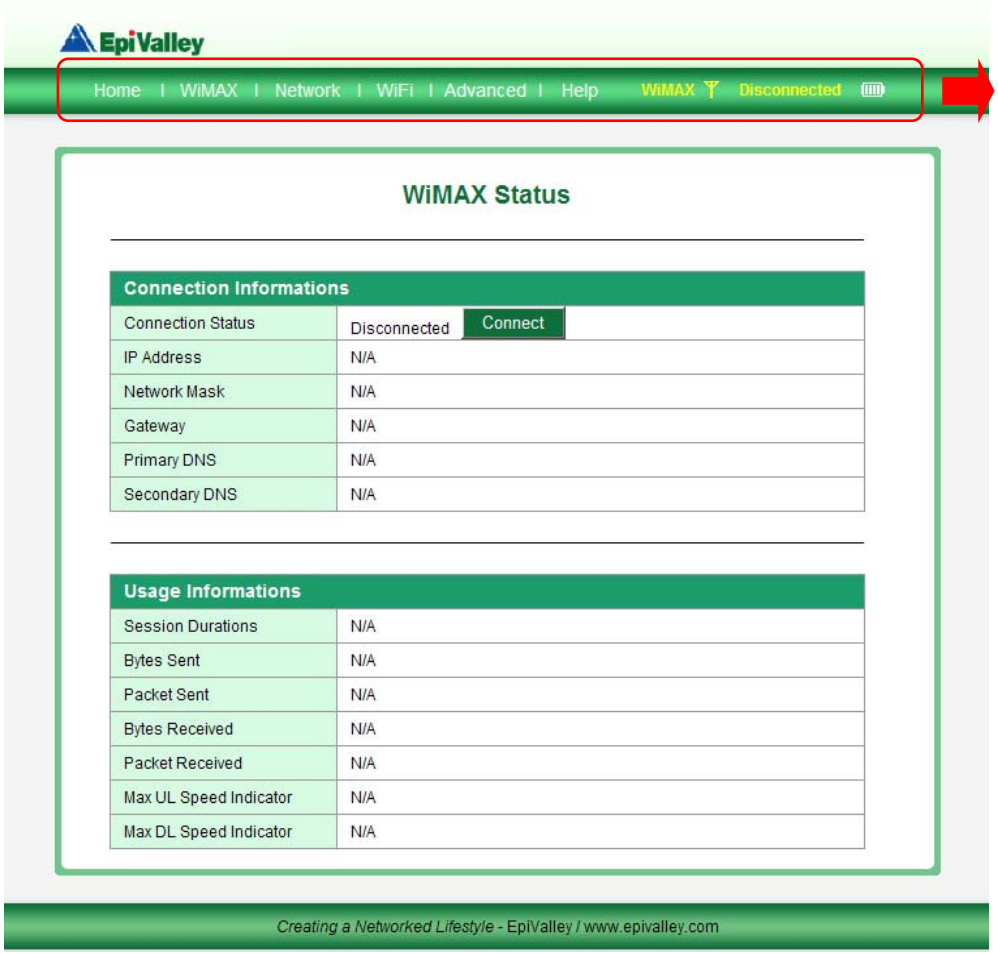
The Browser Interface and Settings

Open your Web browser and enter *http://192.168.5.1/*or *http://wimax_ap.hotspot/* into the address window. The browser interface will open.

Your WiMAX and WiFi use a browser interface to configure the device.

The browser interface lets you:

- View the status of aspects of your network.
- Set up DHCP, WEP or WPA security, MAC filtering, port filtering, port forwarding, DMZ, and VPN pass through.
- Set up a hotspot to allow a maximum of 255 connections to your device without having to share your network name and network key.



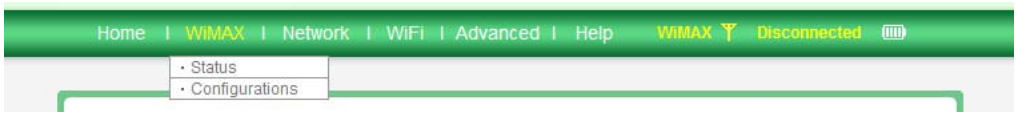
Home

The Home screen is the first screen you see after logging in to the browser interface. It is the main point of entry for all your work in the browser interface. The menu bar runs horizontally along the top of the browser interface. It shows WiFi embedded devices are connected. It also displays information about your device's connection strength and battery level.

WiMAX

The WiMAX menu allows you to set your authentication or WiMAX auto connection option.

It also provides internet connection information as well and traffic counters.



- *Status*

The WiMAX status screen is divided into two sections.

The Connection Informations section also displays the following information:

- Duration of the current connection.
- The device's IP address and subnet mask.
- Gateways IP address.
- Primary, secondary DNS server's IP address.

Connection Informations	
Connection Status	Disconnected Connect
IP Address	N/A
Network Mask	N/A
Gateway	N/A
Primary DNS	N/A
Secondary DNS	N/A

Click *Connect* to connect to your 3G network.

It will not normally require any additional configuration to the basic settings unless you are using the device behind a corporate firewall, and this may require the appropriate proxy server settings to be modified.

The Usage Informations section displays the following:

- Total duration of connection
- Total data bytes sent and received, total data packets sent and received.
- Max uplink(UP) speed and downlink(DN) speed.

Usage Informations	
Session Durations	N/A
Bytes Sent	N/A
Packet Sent	N/A
Bytes Received	N/A
Packet Received	N/A
Max UL Speed Indicator	N/A
Max DL Speed Indicator	N/A

This section displays a count for the current session.

- *Configurations*

The Configurations menu allows you to set your WiMAX username and password, also enabling *Auto connect* allows your device to connect to your 3G network automatically when it is turned on.

Authentication	
WiMAX Username	
WiMAX Password	

Options	
Auto Connection	Enable Disable

Apply

Network

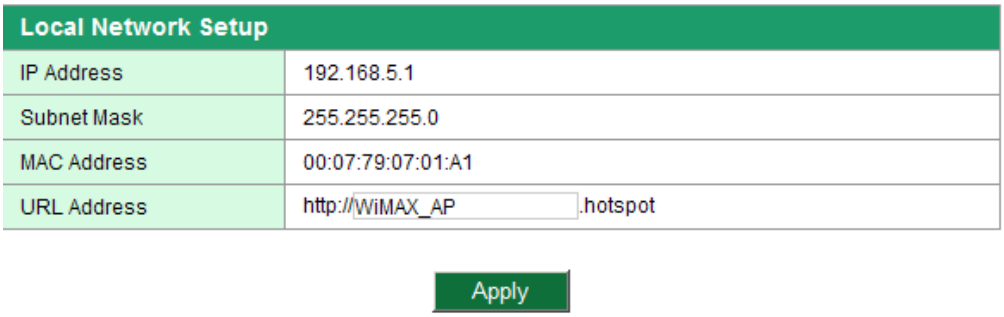
The Network menu allows you to set domain name of the wireless browser interface and set DHCP.

- *Local Network*

This Local Network menu gives you following status information:

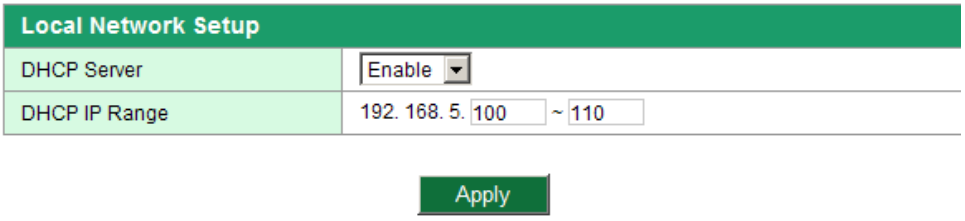
- IP address and subnet mask of the wireless browser interface.

- Device's MAC address.
- The wireless browser interface's current URL address. (which can be change.)



- *Network Address Server*

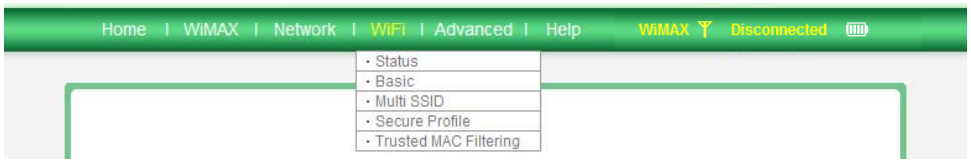
This menu allows you to modify WiFi DHCP IP range.



- DHCP Server: Enabling the DHCP server allows the device to automatically assign a local IP address to a new device joining your network (such as a wireless printer or an additional laptop). When the DHCP server is disabled, you will have to assign static IP addresses to all devices on your network.

WiFi

The WiFi menu allows you to view status information for your WiFi network and configure your hotspot.

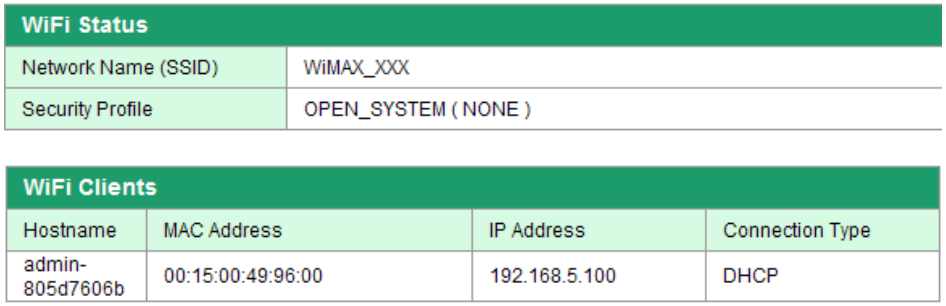


- *Status*

This Status menu gives you following status information:

- Network Name. (also known as SSID)

- Security profile in use.
- Users(clients) information currently connected to the device.

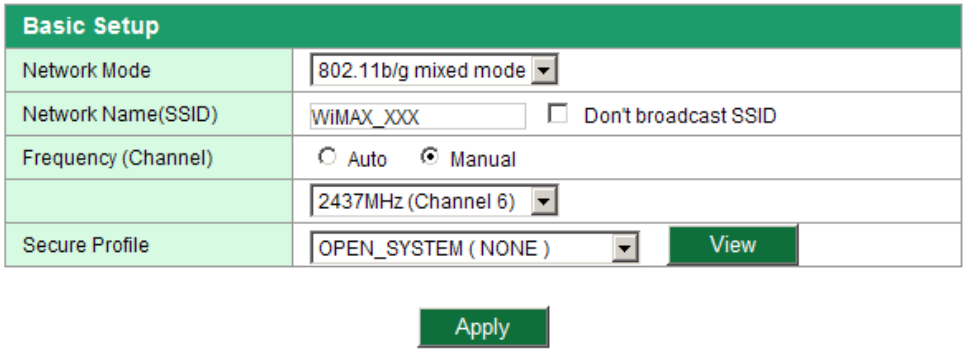


WiFi Status	
Network Name (SSID)	WiMAX_XXX
Security Profile	OPEN_SYSTEM (NONE)

WiFi Clients			
Hostname	MAC Address	IP Address	Connection Type
admin-805d7606b	00:15:00:49:96:00	192.168.5.100	DHCP

- *Basic*

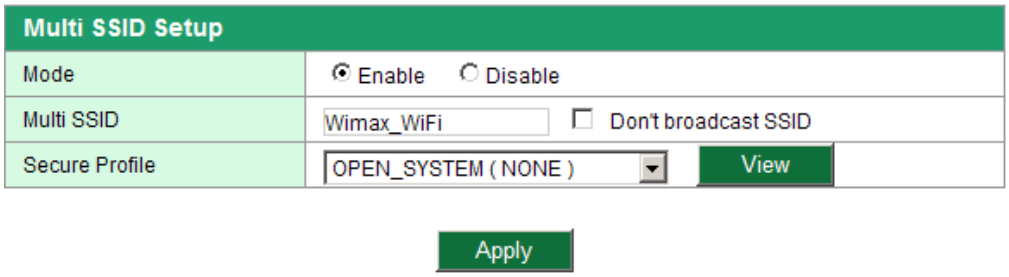
This menu allows you to modify WiFi and Secure Profile.



- Network mode: The type of wireless networking you are currently using. You can choose either mode among 802.11b only, 802.11g only, 802.11b/g mixed mode. The default mode is 802.11b/g mixed mode.
- Network Name (SSID): You can change or input new Network Name (SSID). System default SSID is WiMAX_XXX. If you check *Don't broadcast* box, WiFi clients who try to access the WiMAX mobile hotspot can not see this SSID.
- Frequency (Channel): The radio channel is divided into Auto and Manual. This should be usually set to Auto and left unchanged. Available channels are Auto and 1 to 14.
- Secure Profile: The type of security the router is using. This applies to the Secure and the Temporary hotspot profiles. You can modify(add/edit/delete) Secure Profile using *View* button.

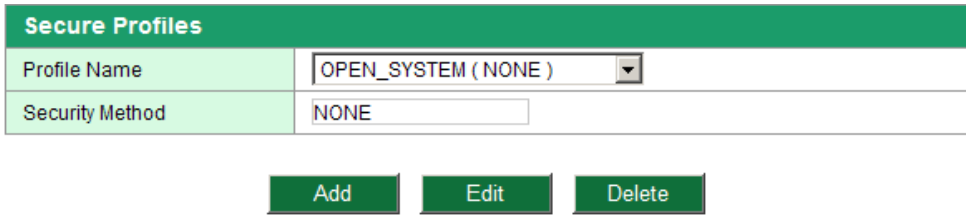
- *Multi SSID*

You can use Multi SSID with secure profile. Enabling Mode allows your device to logically divide into two devices. Also you can set Multi SSID and Secure Profile.

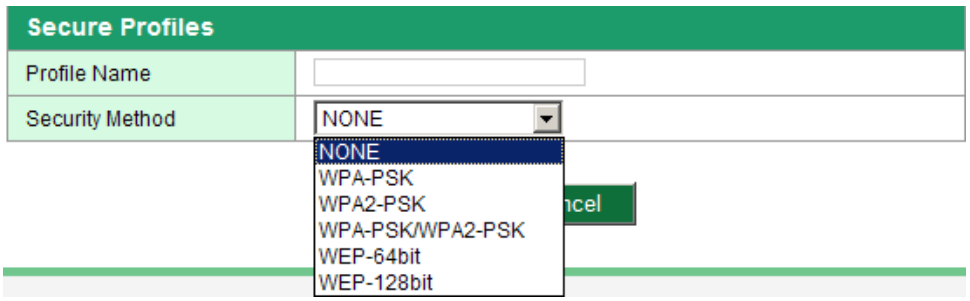


- *Secure Profile*

This menu allows you to modify(add/edit/delete) Secure Profile.

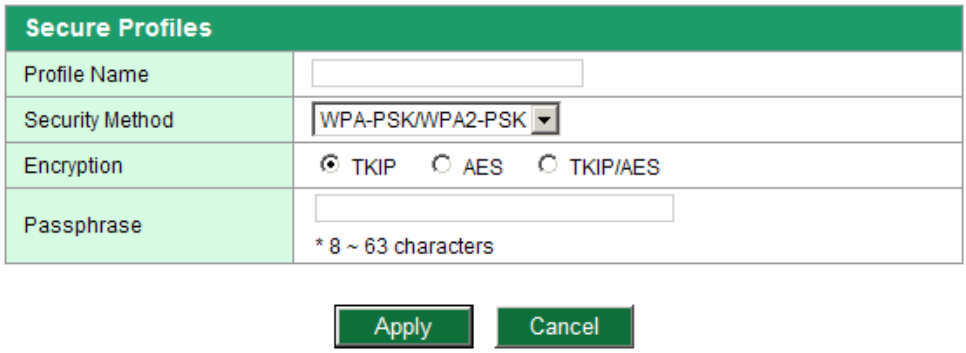


Click *Add*, define Secure Profile. You can set Profile Name, Security Method, Encryption, and Passphrase.



- WPA-PSK/WPA2-PSK: New WiFi certification program mode.
- WEP(64bit or 128bit): Traditional WiFi certification program mode.

After Security Method selected, you can choose the Encryption mode and set the Passphrase.



- TKIP/AES: Data encryption mode.

1. Select a Security Method from the security list.
2. Select the Encryption mode.
3. Enter a new network key in the Passphrase box. (Permissible characters are listed in gray just under the box.)
4. Click *Apply*.

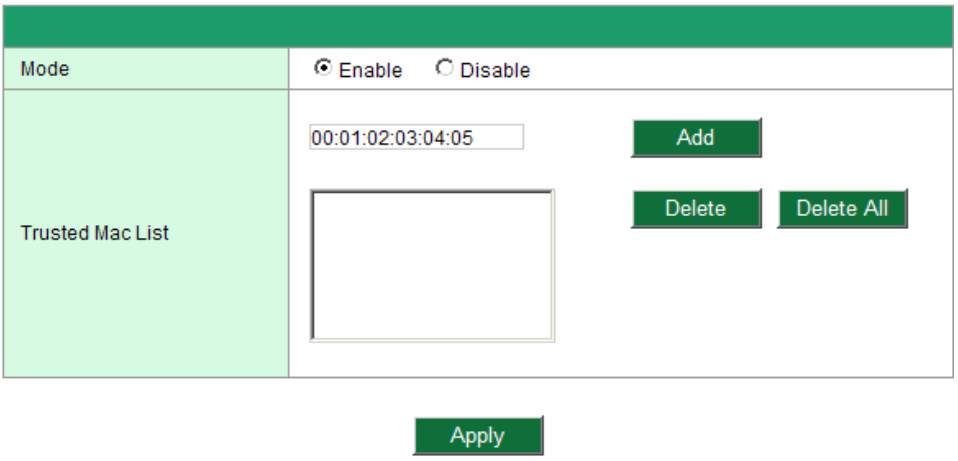
Click *Edit,* you can redefine Security Profile. Also click *Delete*, delete Security Profile from the security list. But you can not *Edit* or *Delete* to *OPEN_SYSTEM (NONE)* Profile. This profile has set as the default Secure Profile.

Note.

When you click Apply, you will need to reconnect to your router by closing your current view and re-opening a browser connection to http://192.168.5.1/

- *Trusted MAC Filtering*

MAC Filter allows you to limit access to your device to only those devices with a specified MAC address (a unique code assigned to hardware such as network adapters).



Finding the MAC Address

The MAC Address is also known as a hardware or physical address for a device, usually a network adapter.

It consists of six pairs of numbers and letters (for example, 00:21:9B:1C:64:34).

You can view the MAC address for any device connected to the WiMAX Mobile device in the WiFi Clients section of the WiFi Status screen. (See "WiFi Clients" on page 6.)

Note.

When you enable this feature for the first time, ensure you add your wireless MAC first, then click Apply.

Advanced

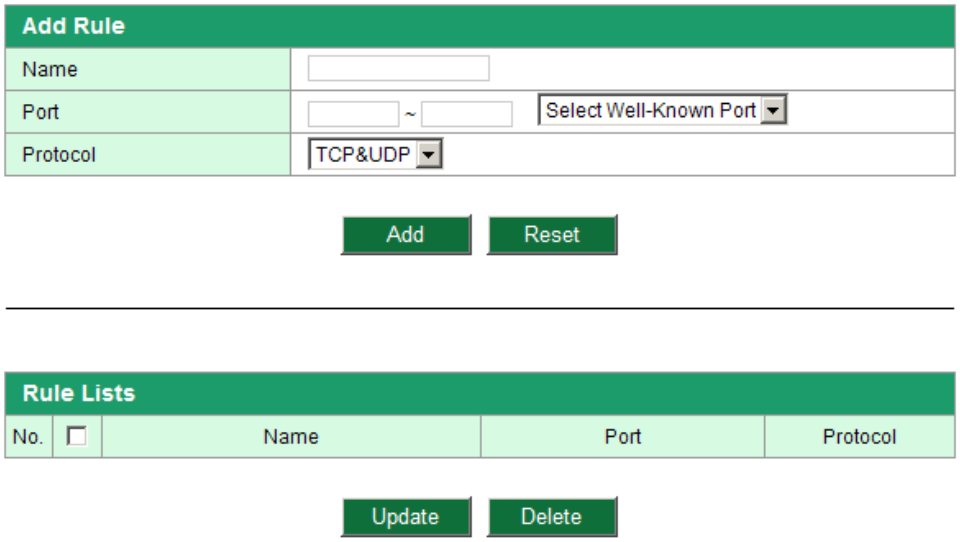
This menu allows you to configure your device to enable Port Filtering, VPN Passthrough, Port Forwarding, DMZ, Backup Configuration, Power Saving, Firmware Upgrade, and so on.

- *Firewall*

The *Firewall* menu allows you to set Port Filtering and VPN Passthrough function.

1) Port Filtering

Port filtering allows you to conserve bandwidth by preventing non-business applications from accessing the Internet, and to prevent applications such as online games from accessing the Internet.



1. Selecting the list box for the applications for which you want to allow access to the Internet.
2. or enter the application value in the Name, Port, and Protocol boxes.
3. Click *Apply*.

2) VPN Passthrough

VPN Passthrough is required if you are going to connect to a VPN.

(Such as a corporate system.)

- L2TP/IPSEC/PPTP: VPN tunneling protocols.

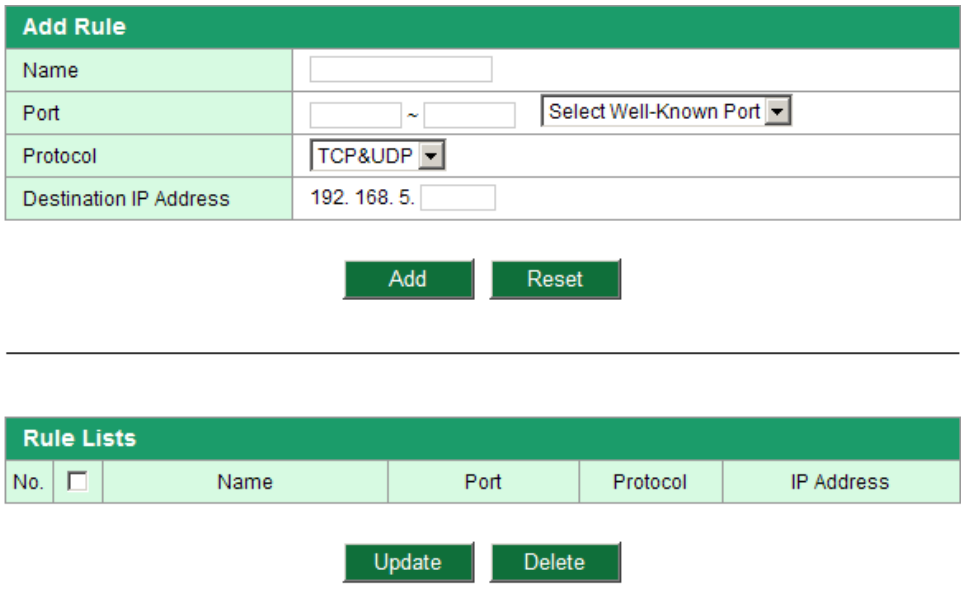
- *Traffic Control*

This menu allows you to set Port Forwarding and DMZ function.

1) Port Forwarding

Port forwarding allows designated users or applications to reach specified servers, such as FTP and DNS servers,

on your computer. Also, some online games require incoming access to work properly.



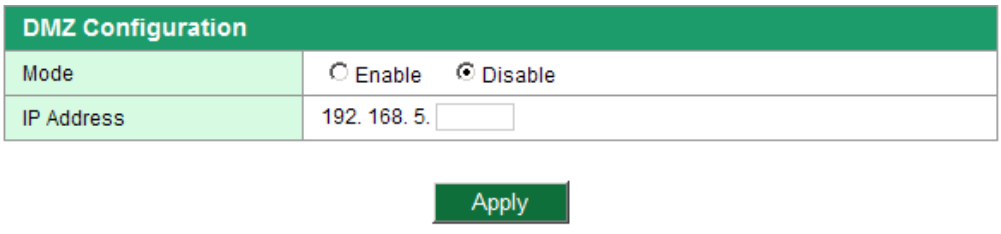
1. Selecting the list box and typing local static IP address of the device hosting the application IP.
2. or enter the value in the Name, Port, Protocol, and Destination IP Address boxes.
3. Click *Apply***.**

Note.

You cannot use port forwarding with some standard data accounts. To use port forwarding, you may need to request a static IP address from your carrier / service provider..

2) DMZ

DMZ function is a host on the internal network that has all ports exposed, except those ports otherwise forwarded. The Mode set enable and enter the local static IP address.



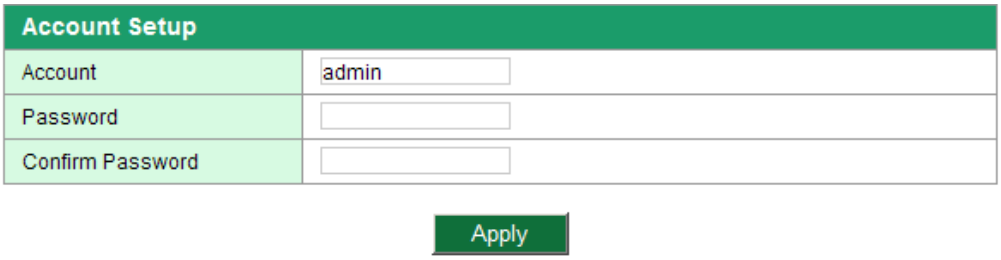
- *Management*

You can create a new administrator's name and password. Also you configure your device to apply Backup Configuration, Power Saving, and Firmware upgrade in this category.

Note.

When you change the default settings, keep you new information in a safe place.

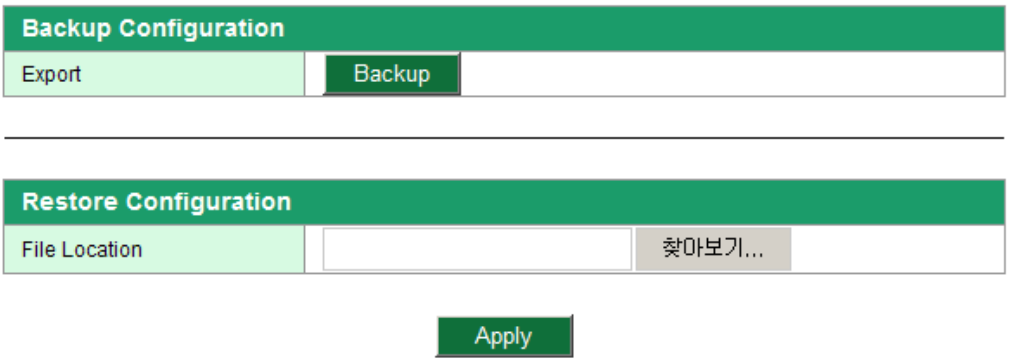
1) Account



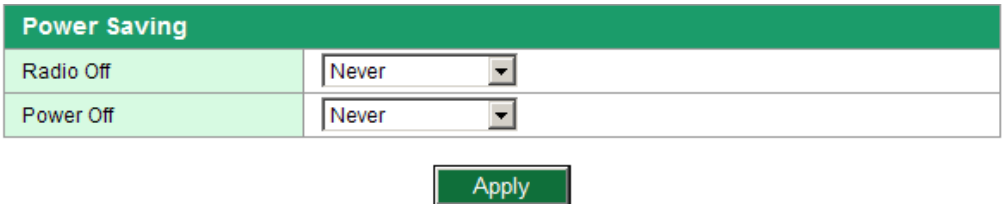
Create administrator's name and password.

2) **Backup & Restore**

The Backup Configuration allows you to backup your settings save to your PC, memory stick, CD, etc. And the Restore Configuration allows you to restore previously saved/backed up settings.



3) **Power Management**



- Radio Off: You can use the Radio Off mode to customize your device to switch to a low power mode when not in use. There are 10 minute increments from 10-60 minutes. Select *Never* to disable this power saving feature. If you want to switch the WiFi Radio on earlier than the time you set in this

menu, you can easily push the power button one time lightly. A blue WiFi LED of indicates that WiMAX Mobile device is ready to connect.

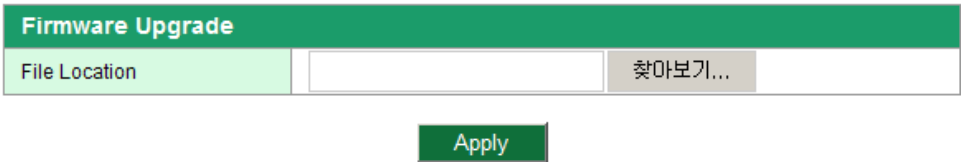
- Power Off - The Power Off mode allows you to choose when your device will automatically power off, to save battery life, due to inactivity. There are 10 minute increments from 10-60 minutes you can select. Select *Never* to disable this power saving feature.

4) Factory Default

Click *Update* to reset your device to the defualt factory settings.

- *Firmware Upgrade*

You can upgrade your device's configuration file to your computer.



Help

Help menu gives you the information about customer service, the Quick Start Guide, full User Guide, Frequently Asked Questions, & Troubleshooting.

- *Customer Service*
- *User Guide*
- *FAQ*
- *Troubleshooting*

User Information

This device complies with part 15 of 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.

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 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

WARNING:

During transmitter operation, in order to meet RF Maximum permissible Exposure Safety Guidelines, a minimum distance of 20cm shall be maintained between this device and personnel.

This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.