

FWT Wifi AP_USB x 4

User's Guide

Version: 1.0

Date: August 14, 2013

3JTech Co., Ltd.
2F, No. 342, Fu-Shing N. Rd.
Taipei, Taiwan
Tel: +886-2-2500 6916
e-mail: info@3jtech.com.tw

Revision History

Version	Date	Changes
1.0	08/14/2013	First Release of FWT Wifi AP_USB x 4 User's Manual

Table of Contents

Revision History	2
TABLE OF CONTENTS.....	3
CHAPTER 1. PRODUCT OVERVIEW	5
1.1 INTRODUCTION	5
1.2 FEATURES	6
1.3 PACKAGE CONTENTS	7
CHAPTER 2. PHYSICAL DESCRIPTION	8
2.1 PANELS	8
2.1.1 Front Panel.....	8
2.1.2 Rear Panel.....	9
2.2 ILLUSTRATION	10
2.2.1 Front Panel Information.....	11
Phone Connector	11
3G ANT SMA Connector	11
SIM Card Slot.....	11
Power Supply Connector.....	11
WAN Port	11
LAN Network Connectors	11
USB 1~USB 3 Connectors	11
RESET Button	11
2.2.2 Rear Panel Information.....	11
LEDs	11
2.2.3 LED Description on the Rear Panel	12
CHAPTER 3. WEB-BASED MANAGEMENT.....	13
3.1. INTERNET SETTINGS	15
3.1.1 WAN	15
3.1.1.1 Static(Fixed IP) WAN Mode	16
3.1.1.2 DHCP(Auto Config) WAN Mode.....	16
3.1.1.3 PPPoE (ADSL) WAN Mode	17
3.1.1.4 3G Settings	18
3.1.2 LAN.....	19
3.1.3 DHCP Client	21
3.1.4 VPN (GRE)	22
3.1.5 Advanced Routing Settings.....	23

3.2 WIRELESS SETTINGS	24
3.2.1 Basic Wireless Settings	24
3.2.2 Wireless Security/Encryption Settings	29
3.2.2.1 Disable Mode	29
3.2.2.2 WEPAUTO(WEP) Mode	30
3.2.2.3 WPA-PSK / WPA2-PSK Mode	32
3.2.3 Station List	34
3.2.4 Wireless Statistics	35
3.3 FIREWALL SETTINGS	36
3.3.1 MAC/IP/Port Filtering Settings	36
3.3.2 Port Forwarding Settings	38
3.3.2.1 Create a Port Forwarding	38
3.3.3 DMZ Settings	41
3.3.4 System Security Settings	42
3.4 MANAGEMENT	44
3.4.1 System Management	44
3.4.2 SIM Card Control	46
3.4.3 SMS Sending/Receiving	49
3.4.4 TR-069	51
3.4.5 Fax Sending/Receiving via FWT	52
3.4.5.1 Usage of FAX	52
3.4.5.2 Fax Settings	54
3.4.6 Firmware Upgrade	55
3.4.7 Configuration Management	56
3.4.8 Status	57
3.4.9 Statistic	58
CHAPTER 4. GSM SETUP	59

1. Product Overview

1.1 Introduction

FWT Wifi AP_USB x 4, a 3G WiFi Router with a WAN port and multiple cellular modems, is the perfect option to connect a small group of PCs to a high-speed broadband Internet connection or to an Ethernet backbone. Configurable as a DHCP server, FWT Wifi AP_USB x 4 acts as the only externally recognized Internet device on your local area network (LAN). The FWT Wifi AP_USB x 4 also serves as an Internet firewall to protect your network from being accessed by outside users.

In addition, this AP is a Fixed Wireless Terminal (FWT). A simple desk phone can be connected to the phone jack to make and receive calls. The SIM card inserted in the device is used for GSM calls.



1.2 Features

- Router Mode
 - 3G Dial-up
 - 3 WAN Modes (It includes Static(Fixed IP), DHCP(Auto Config) and PPPoE (ADSL))
 - DHCP Sever
 - NAPT (Network Address and Port Translation)
 - NAT (Network Address Translation)
- Internet Access
 - TCP/IP,UDP, ICMP, ARP, PPP, NAT, DHCP (Server), Static IP assignment
- Security Features
 - Password protected configuration access
 - User authentication (PAP/CHAP) for PPP connection
- Wireless Features
 - Support 802.11b/g, 802.11n draft 3.0 Wireless Access Point
 - Support 128-Bit and 64-Bit WEP encryption, WPA-PSK, WPA2-PSK
- Security
 - Support packet inspection and filtering
 - Intrusion detection and protection
 - Password protected system management
- Ethernet Interface
 - Compliant with IEEE 802.3 and 802.3u 10/100 Mbps
- HTTP Web-Based Management
 - Firmware upgrade by UI
 - WAN and LAN side connection statistics
 - Password protected access
 - Wireless LAN
- Support TR-069 management function
- Support the Fax function
- Support the load balance function with multiple 3G

1.3 Package Contents

- 1 x FWT Wifi AP_USB x 4
- 1 x RJ45 Ethernet Cable
- External 3G Antenna with 3M Antenna Cable
- RJ11 Phone Cable
- 3G USB Dongle (*Optional*)
- 1 x Power Adapter
- 1 x CD with this User's Manual
- Quick Setup Guide

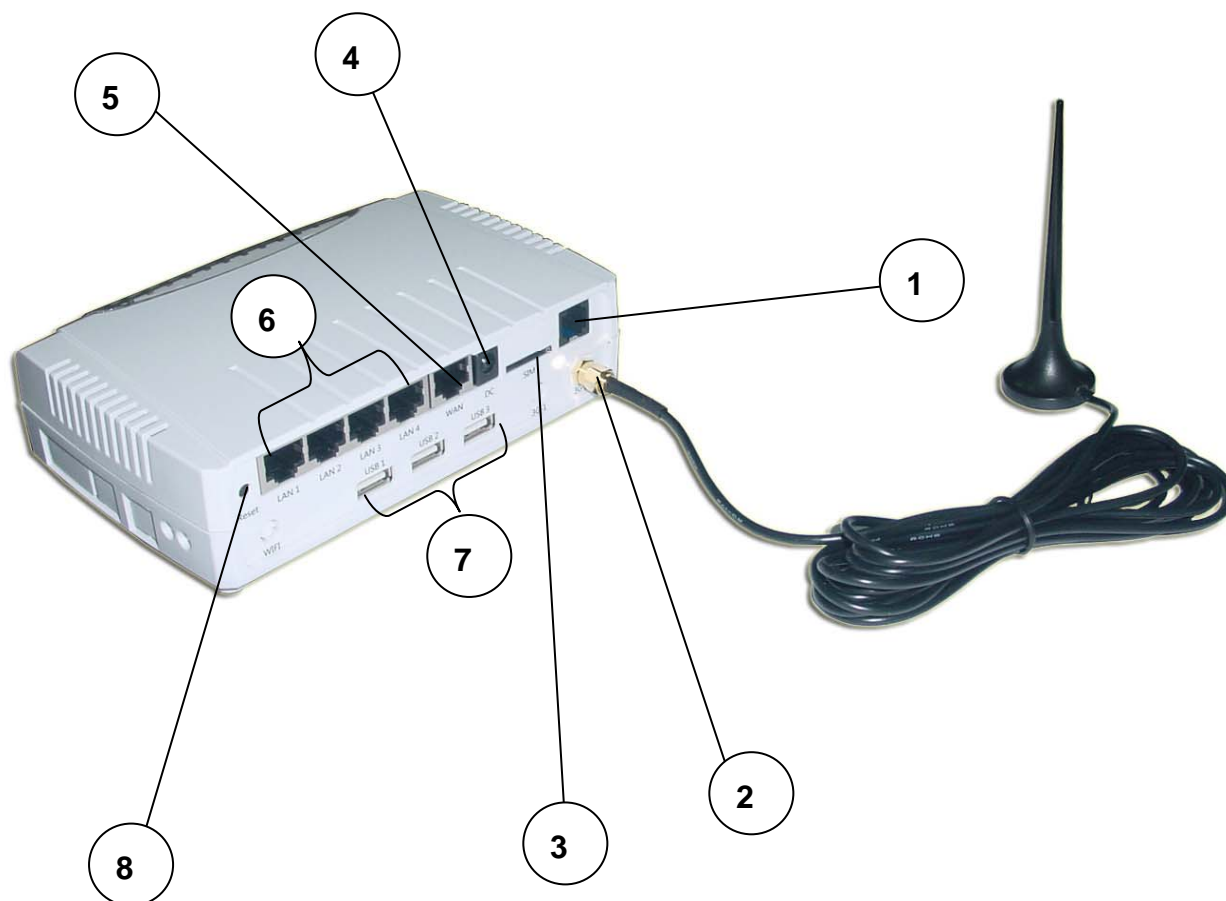
2. Physical Description

The following information contains the physical description of the FWT Wifi AP_USB x 4. This includes the functions and the locations of each connector and indicator. This information provides useful reference when installing the product. Please familiarize yourself with the FWT Wifi AP_USB x 4.

2.1 Panels

2.1.1 Front Panel

For more related description, please refer to the Section 2.2 and Section 2.2.1.



2.1.2 Rear Panel

For more detailed description, please refer to the Section 2.2 and Section 2.2.2.



2.2 Illustration

No. in Figures	Name on FWT Wifi AP_USB x 4	Description	Remark
1	Phone Connector	To connect with an analog phone via a RJ-11 cable	Refer to Section 2.2.1 for front panel information
2	3G ANT SMA Connector	To externally connect with the 3G Antenna	Refer to Section 2.2.1 for front panel information
3	SIM Card Slot	To connect with the internal modem	Refer to Section 2.2.1 for front panel information
4	Power Supply Connector	To connect with the FWT Wifi AP_USB x 4 and the power adapter	Refer to Section 2.2.1 for front panel information
5	WAN Port	For the access of Internet	Refer to Section 2.2.1 for front panel information
6	LAN Network Connectors	To connect to the device and Ethernet port via RJ45 cable	Refer to Section 2.2.1 for front panel information
7	USB 1~USB 3 Connectors	To externally connect with the 3G dongle(s)	Refer to Section 2.2.1 for front panel information
8	Reset Button	To reset the FWT Wifi AP_USB x 4 to its factory defaults	Refer to Section 2.2.1 for front panel information
9	LEDs	To display the status of FWT Wifi AP_USB x 4	Refer to Section 2.2.2 for rear panel information and Section 2.2.3 for LED description on the rear panel

2.2.1 Front Panel Information

Phone Connector

Offer the Voice FWT function.

3G ANT SMA Connector

Support 3G mode for the access of Internet.

SIM Card Slot

Plug the SIM card chip.

Power Supply Connector

Plug the power adapter. The specifications of FWT Wifi AP_USB x 4's power adapter are as follows:

- Input: 100 ~ 240V AC, 50/60Hz
- Output: 12V DC / 1.5A

WAN Port

Offer the access of Internet.

LAN Network Connectors

FWT Wifi AP_USB x 4 is designed for 10/100Mbps Ethernet networks. FWT Wifi AP_USB x 4 connects to the network via category 5 cable.

USB 1~USB 3 Connectors

Plug the 3G USB dongle for the load balance.

Note: Please plug the 3G USB dongle when the router is powered off.

RESET Button

Support the hardware reset function. Press this button 2 seconds around, and the settings of the device will return to the factory defaults.

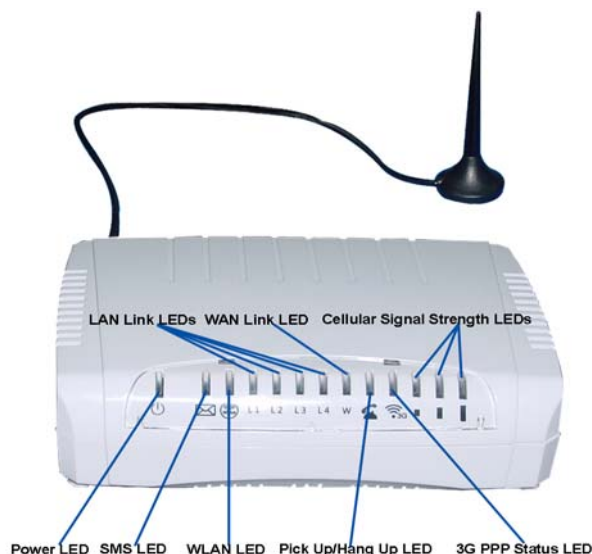
Note: Please do not power off the router while resetting it to the factory default.











2.2.2 Rear Panel Information

LEDs

Include the LEDs of POWER, SMS, WLAN (Wireless LAN), LAN Link, WAN Link, Pick Up/Hang Up, 3G PPP Status, and Cellular Signal Strength.

2.2.3 LED Description on the Rear Panel

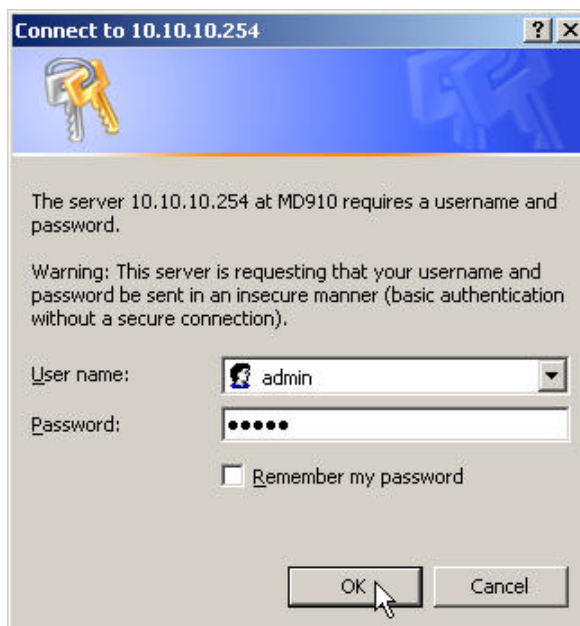


LED	Color	Status
POWER ()	Yellow	Lit when +12V DC power is on and working.
SMS ()	Yellow	Lit when receiving any new SMS(s). Off at any status except the incoming of new SMS(s).
WLAN (Wireless LAN )	Yellow	Lit when the WiFi function is enabled. Flash when the data is transmitting. Off when the WiFi function is disabled.
LAN Link ()	Yellow	Lit when the cable connection with device exists. Flash when the data is transmitting. Off when no cable connection exists.
WAN Link ()	Yellow	Lit when the cable connection with device exists. Flash when the data is transmitting. Off when no cable connection exists.
Pick Up/Hang Up ()	Yellow	Lit when picking up the connected analog phone. Off when hanging up the connected analog phone.
3G PPP Status ()	Yellow	Lit when dialup is connected. Flash when the data is transmitting. Off when dialup is disconnected.
3 Cellular Signal Strength LEDs		
Low ()	Yellow	All 3 LEDs lit when the signal strength is good. (The LEDs lit would decrease progressively upon the signal strength)
Medium ()		
High ()		

3. Web-Based Management

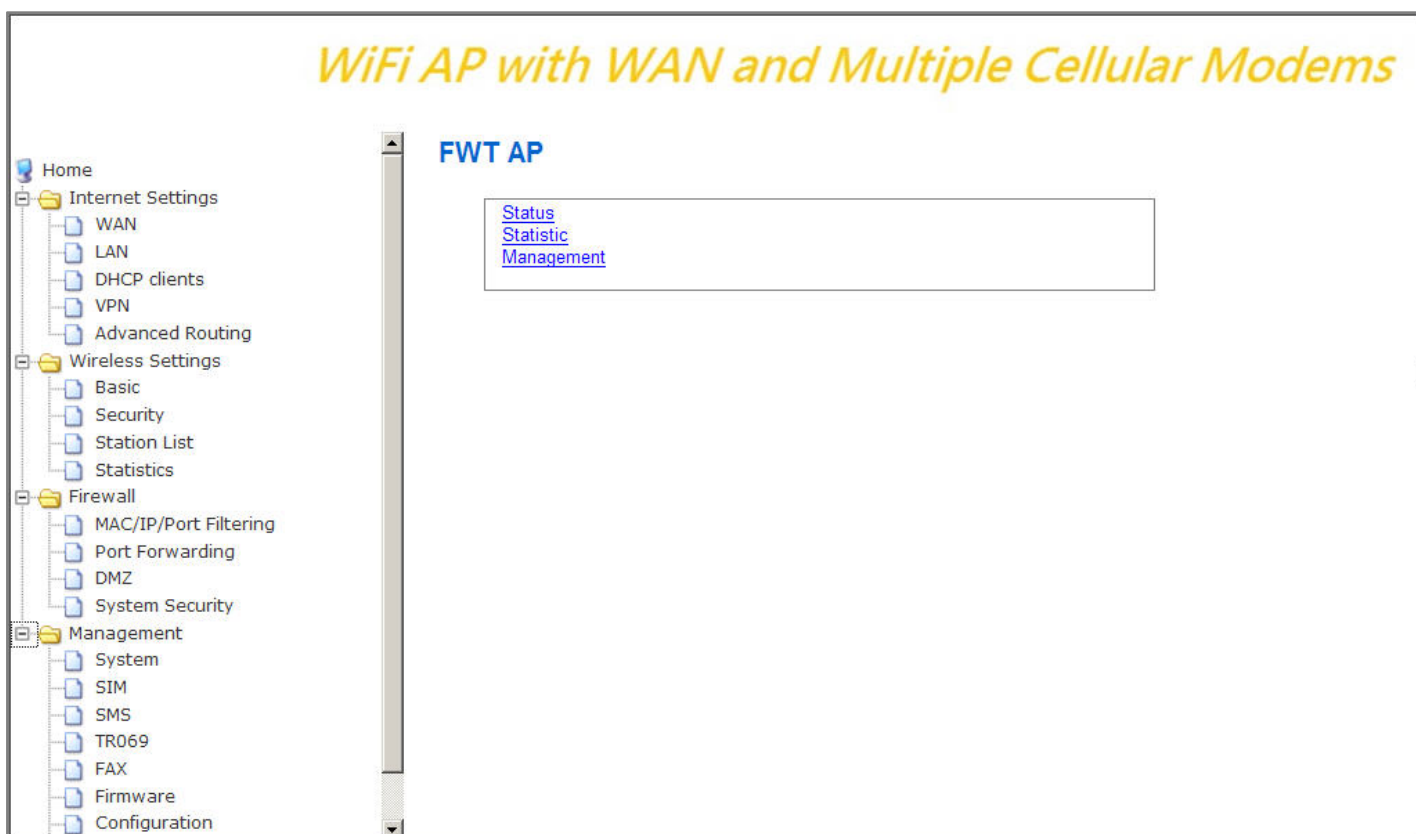
This chapter instructs you how to configure and manage the FWT Wifi AP_USB x 4 through the web user interface it supports. With this facility, you can easily access and monitor through the LAN port of the FWT Wifi AP_USB x 4.

After the FWT Wifi AP_USB x 4 has been connected to your PC via RJ45 network cable, type <http://10.10.10.254> in IE browser, it will show the following screen and ask you to input the user name and password in order to login and access authentication. The default user name and the password are both “**admin**”. For the first time to use, please enter this default user name and the password, then click the **OK** button. The root setup page for FWT Wifi AP_USB x 4 will be displayed once the login process is successful. The user will be able to fully access and configure the system.



In the FWT Wifi AP_USB x 4, it supports a simple user management function to configure the system. As the figure below shows, for example, left section is the whole function tree with web user interface while each of main functions, including INTERNET SETTINGS, WIRELESS SETTINGS, FIREWALL, and MANAGEMENT is selected.

By means of the hyperlink of Status, Statistic or Management in this root setup page, you can directly jump to the related pages if you would like to realize the basic information of the system.



3.1. Internet Settings

3.1.1 WAN

The WAN (Wide Area Network) section is where you configure your Internet connection type. Besides supporting 3G dialup connection type to access Internet, there are three WAN connection modes to choose from: Static (Fixed IP), DHCP(Auto Config) and PPPoE(ADSL). If you are unsure of your connection method, please contact your Internet Service Provider before configuring the required parameters. Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers is removed or disabled.

Through the **Wan Weight** function on this WAN setting webpage, you can set up the transmission ratio among the Ethernet WAN and each 3Gs (WAN1: WAN2: WAN3: WAN4: WAN5) for the router's load balance. Default is 1:1:1:1:1.

Note: If the external dongle is not connected, the wan weight for it must be either 0 or empty.

Wide Area Network (WAN) Settings

WAN Connection Type: (Dropdown menu options: DHCP (Auto config), STATIC (fixed IP), DHCP (Auto config), PPPoE (ADSL))

DHCP Mode

Hostname (optional):

3G Mode

APN:

Dial Number:

Username:

Pasword:

Auth Mode: (Dropdown)

Connection Type: (Dropdown)

3G Mode:1

APN:

Dial Number:

⋮

⋮

3G Mode:3

APN:

Dail Number:

Username:

Password:

Auth Mode: (Dropdown)

Connection Type: (Dropdown)

WAN Weight

WAN1 (Ether Cable):

WAN2 (3G Internal):

WAN3 (3G USB1):

WAN4 (3G USB2):

WAN5 (3G USB3):

3.1.1.1 Static(Fixed IP) WAN Mode

Used when your ISP provides you a set IP address that does not change. The IP information is manually entered in your IP configuration settings. You must enter the **IP address**, **Subnet Mask**, **Default Gateway**, **Primary DNS Server**, and **Secondary DNS Server**. Your ISP provides you with all of this information.

WAN Connection Type:		STATIC (fixed IP) ▼
Static Mode		
IP Address	<input type="text"/>	
Subnet Mask	<input type="text"/>	
Default Gateway	<input type="text"/>	
Primary DNS Server	<input type="text"/>	
Secondary DNS Server	<input type="text"/>	

3.1.1.2 DHCP(Auto Config) WAN Mode

A method of connection where the ISP assigns your IP address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the Internet.

WAN Connection Type:		DHCP (Auto config) ▼
DHCP Mode		
Hostname (optional)	<input type="text"/>	

Hostname: Some ISP's may check your computer's hostname. The hostname identifies your system to the ISP's server. This way they know your computer is eligible to receive an IP address. In other words, they know that you are paying for their service.

3.1.1.3 PPPoE (ADSL) WAN Mode

Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. DSL providers typically use this option. This method of connection requires you to enter a **User Name** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

WAN Connection Type:		PPPoE (ADSL) ▼
PPPoE Mode		
User Name	<input type="text"/>	
Password	<input type="password"/>	
Verify Password	<input type="password"/>	
Operation Mode	Keep Alive ▼	
	Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds	

Operation Mode: Typically, connections are not always on. The router allows you to set the reconnection mode. The setting is:

- **Keep Alive:** A connection to the Internet is always maintained. When this option is selected, please enter a value in the field of **Redial Period** which is the time interval the machine will be redialed before the PPPoE connection is disconnected.

3.1.1.4 3G Settings

This section is where you configure your dialup connection type. There are 2 modem types to choose from: Cellular 2G and 3G.

Up to four 2G/3G are allowed to be used at a time through one internal 2G/3G module and three external USB ports for the connection of 3G dongles. With these multiple 2G/3G, they will balance the load of WAN transmission for the router. Based on your USB1/USB2/USB3 hardware configuration on FWT WIFI AP_USB x 4, sequentially set up these cellular modems (See the figure below).

2G/3G ISP Settings: Your 2G/3G service provider will provide you with the values to fill in for the required fields of **Access Point Name (APN Gateway)**, **PPP User Name**, **PPP Password** and **Dial Number**.

Dial Number: The 2G/3G dial command. Default is *99#.

Authentication Mode: The mode for PPP authentication. Default is Auto.

Connection Type: There are four types of operation mode supported: 3G only, 3G+2G(3G Preferred), 2G only, and 2G+3G(2G Preferred). Default is 3G + 2G (3G Preferred).

3G Mode	
APN	internet
Dial Number	*99#
Username	user
Password	password
Auth Mode	Auto
Connection Type	3G + 2G(3G Preferred)

For Internal Modem 2G/3G Settings

3G Mode:1	
APN	internet
Dial Number	*99#
Username	user
Password	password
Auth Mode	Auto
Connection Type	3G+2G(3G Preferred)

For External USB Port 1 2G/3G Settings

3G Mode:2	
APN	internet
Dial Number	*99#
Username	user
Password	password
Auth Mode	Auto
Connection Type	3G+2G(3G Preferred)

For External USB Port 2 2G/3G Settings

3G Mode:3	
APN	internet
Dial Number	*99#
Username	user
Password	password
Auth Mode	Auto
Connection Type	3G+2G(3G Preferred)

For External USB Port 3 2G/3G Settings

3.1.2 LAN

These are the settings of the LAN (Local Area Network) interface for the AP. The AP's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

LAN Setup	
IP Address	10.10.10.254
Subnet Mask	255.255.255.0
MAC Address	00:0A:EB:38:B8:85
DHCP Type	Server
Start IP Address	10.10.10.100
End IP Address	10.10.10.200
Subnet Mask	255.255.255.0
Primary DNS Server	168.95.1.1
Secondary DNS Server	8.8.8.8
Lease Time	86400
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>

Apply Cancel

IP Address: The IP address of your router's LAN port. Default: 10.10.10.254.

Subnet Mask: Subnet Mask of your LAN (default: 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.

DHCP Type: DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN). When you select **Server** item from this pull-down list to enable this function, the following parameters will be displayed. You must enter the IP address, Subnet Mask, Primary DNS Server and/or Secondary DNS Server.

Start IP Address: Specify the DHCP Client IP address that will start.

End IP Address: Specify the DHCP Client IP address that will end.

Note: The number of the “End IP” must be greater than “Start IP”, and cannot be the same as the router’s IP address.

DHCP Lease Time: Designate the amount of the time for the device to recycle and give out the IP addresses to the devices in your network (default: 86400).

Statically Assigned: You can statically assign the client MAC and IP address. Up to three IPs and MACs can be assigned.

3.1.3 DHCP Client

In this section, you can see clearly which devices are currently leasing IP addresses that you had defined for the DHCP Server's allocation of addresses to computers and devices on your Local Area Network.

DHCP Client List			
DHCP Clients			
Hostname	MAC Address	IP Address	Expires in
iris	00:0C:6E:AB:9B:E6	10.10.10.100	17:21:11

Host Name: A name for each computer or device that is given an IP address by the DHCP Server. This may help you keep track of which computers are assigned this way.

MAC Address: A MAC address is usually located on a sticker at the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33.

IP Address: The address which is obtained from the DHCP Server.

Expires in: The remaining time of the IP address's lease. A specific LAN device no longer needs the leased IP address when the time ends up, and this device will also free the IP address it had leased.

3.1.4 VPN (GRE)

FWT WIFI AP_USB x 4 supports GRE VPN (Virtual Private Network) communication protocol. VPN is a technology commonly used in different private networks between companies or groups. It allows the intranet message to be transmitted using the public network such as Internet. Through VPNs, the user is able to access resources on remote networks, for example, files, printers, databases, internal websites and so on. You can refer to the following description of parameters to set up your VPN.

VPN (GRE)	
<hr/>	
GRE Mode	
GRE Enable	<input type="checkbox"/>
Remote IP Address	<input type="text"/>
Gateway	<input type="text"/>
IP/Subnet Mask	<input type="text"/> / <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

GRE Enable: Enable/Disable the VPN function for the FWT WIFI AP_USB x 4.

Remote IP Address: The IP address of the remote VPN host.

Gateway: The IP address of Gateway in VPN.

IP/Subnet Mask: Set up the IP/Subnet Mask for VPN. The valid range for Subnet Mask is 8~32.

3.1.5 Advanced Routing Settings

In Static Routing Settings, the user can set up a route rule (table) here. Refer to the description of the following parameters to set up the necessary route rule, and click the **Apply** button when you complete.

Add a routing rule

Destination	<input type="text"/>
Range	Host <input type="text"/>
Gateway	<input type="text"/>
Interface	LAN <input type="text"/>
Comment	<input type="text"/>

Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	10.10.10.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	

Destination: The IP address of packets that will take this route.

Range: Includes **Host** and **Net** options. When selecting “Net”, there is another “Netmask” column that needs to be filled out.

Netmask: The bits in the mask specify which bits of the IP address must match.

Gateway: The gateway for the routing.

Interface: Specifies the interface -- **LAN** or **WAN** -- that the IP packet must use to transit out of the router when this route is used. Or you can choose the user-defined way by selecting the **Custom** option.

Comment: Memo for the routing rule.

Routing Table: Lists the current route rules you have added before. Click on the **Delete** button to delete the selected route rule.

3.2 Wireless Settings

The wireless section is used to configure the wireless settings for your router. Please note that changes made on this section may also need to be duplicated on your wireless client.

To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP(WEPAUTO), WPA-PSK, and WPA2-PSK. WEP is the original wireless encryption standard. WPA provides a higher level of security. In WPA encryption, it supports TKIP or AES of WPA-PSK/WPA2-PSK.

3.2.1 Basic Wireless Settings

Through the basic wireless setting page, the user can control the ON/OFF status of WiFi function, and set up the 802.11 mode, Network Name (SSID) as well as Channel. Besides, you can do the further settings related to the HT Physical Mode.

Basic Wireless Settings	
You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.	
Wireless Network	
WiFi On/Off	WiFi OFF
Network Mode	11b/g/n mixed mode
Network Name(SSID)	default <input type="checkbox"/> Hidden
Multiple SSID1	<input type="text"/> <input type="checkbox"/> Hidden
Multiple SSID2	<input type="text"/> <input type="checkbox"/> Hidden
Multiple SSID3	<input type="text"/> <input type="checkbox"/> Hidden
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Frequency (Channel)	2437MHz (Channel 6)

HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2457MHz (Channel 10)
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Wireless Network Settings:

WiFi On/Off: This option turns on and off the wireless connection feature of the router. Simply click on the **WiFi ON / WiFi OFF** button. The system will automatically detect the current status of the router and switch the button accordingly.

Network Mode: There are 5 modes including, 802.11b/g mixed mode, 802.11b only, 802.11g only, 802.11/b/g/n mixed mode, and 802.11n only(2.4G) can be chosen.

Network Name(SSID): When you are browsing for available wireless networks, this is the name that will appear in the list (unless you set it to Hidden, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. Default is "default".

Hidden: The option allows you to hide your wireless network. When this option is unchecked, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When you click on this checkbox to enable this function, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

Multiple SSID 1 ~ 3: Up to three SSIDs you can additionally set up for this wireless network.

Broadcast Network Name (SSID): Enable/Disable the SSID broadcast function. This function is used to control the broadcast status of all SSIDs. If this function is disabled, all SSIDs you had set up for the router will be hidden. To cancel the hidden status for the specific SSID, you can uncheck the "Hidden" option in the back of your desired SSID.

AP Isolation: Enable/Disable this function. Create a separate virtual network for your wireless network. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. You may want to utilize this feature if you have many guests that frequent your wireless network.

MBSSID AP Isolation: Enable/Disable the MBSSID AP Isolation function. The router supports multiple SSIDs. You can decide whether the clients associated to different SSIDs on the device can see each other or not. Enable the option to block it. Default is "Disable".

Frequency (Channel): A wireless network uses specific channels in the 2.4GHz wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network. If you select **AutoSelect**, the router automatically finds the channel with least interference and uses that channel for wireless networking.

Rate: Exist only when selecting 802.11b/g mixed mode, 802.11b only, 802.11g only as the Network Mode for the router. You can set up the desired transmitting rate for these network modes. Default is Auto.

HT Physical Mode Settings: This mode settings exist only when 802.11b/g/n mixed mode or 802.11n only(2.4G) is chosen as your router's Network Mode.

Operating Mode: Select the option to enable the Mixed Mode or the Green Field Mode for physical layer transceivers. Default: Mixed Mode.

Mixed mode: In this mode the device transmits the packets with preamble compatible legacy (802.11g), so they can be decoded by legacy devices. The device receives and decodes both Mixed Mode packets and legacy packets.

Green Field mode: The device transmits HT packets without legacy compatible part. But the device receives and decodes both Green Field and legacy packets.

Channel BandWidth: This option only works when selecting Network mode in 11b/g/n mixed mode and 11n mode. Select the option to choose 20 MHz or 20/40MHz. This option affects the Phy data rate of radio. Please refer to the table below, which shows the relationship among Phy data rate, Bandwidth and Guard Interval.

Guard Interval: The 11n device inserts the Guard Interval into the signal. You can choose the interval between "Long" and "Auto". This option affects the Phy data rate of radio. For more details, please refer to the table below.

MCS: It means "Modulation Coding Scheme". The available options are "Auto, 0, 1, ...15, and 32". It changes the modulation of this device and effect the maximum Phy data rate. We recommend "Auto" setting. For more details, please refer to the table below.

The table below shows the relationship among Phy data rate, Bandwidth and Guard Interval.

Data Rate Mbps MCS	Bandwidth = 20MHz		Bandwidth = 40MHz	
	Short Guard Interval	Long Guard Interval	Short Guard Interval	Long Guard Interval
0 (1S)	7.2	6.5	15	13.5
1	14.4	13	30	27
2	21.7	19.5	45	40.5
3	28.9	26	60	54
4	43.3	39	90	81
5	57.8	52	120	108
6	65	58.5	135	121.5
7	72.2	65	150	135
8 (2S)	14.4	13	30	27
9	28.9	26	60	54
10	43.3	39	90	81
11	57.8	52	120	108
12	86.7	78	180	162
13	115.6	104	240	216
14	130	117	270	243
15	144.4	130	300	270
32	Not Supported	Not Supported	6.7	6

MCS: Modulation Coding Scheme
MCS=0~7 (1S, One Tx Stream)
MCS=8~15 (2S, Two Tx Stream)
MCS 32: BPSK

Reverse Direction Grant(RDG): This is the 11n performance parameter. Enable it if needed.

Extension Channel: Exist only when selecting “20/40” as the Channel BandWidth for the router. For example, if channel 6 is selected, it means you can select channel 2 or channel 10 as the extension channel. Choose the unused channel as the extension channel.

Aggregation MSDU(A-MSDU): The multiple HT packets can be transmitted with single ACK reply packet. Enable it to apply this function and reduce the network congestion.

Auto Block ACK: It is another aggregation technique which prevents sending ACK in the communication to increase the throughput. If this option is enabled, the device will activate this function when transmitting massive data.

Decline BA Request: Enable this option to decline the Block ACK request addressed by the other devices.

3.2.2 Wireless Security/Encryption Settings

In this section, you can configure the wireless security and encryption to prevent from unauthorized access and monitoring. Please choose a SSID you had created for this router in the *Wireless Settings* → *Basic* setting page from the **SSID Choice** pull-down list.

There are 4 encryption modes, including **Disable**, **WEPAUTO(WEP)**, **WPA-PSK** and **WPA2-PSK** offered for your selection. Please also pull down the **Security Mode** list and select the desired mode for your router's wireless security. For more details about the setup in these different modes, please refer to the following sections.

3.2.2.1 Disable Mode

In this mode, wireless clients can directly connect to the router without inputting any key.

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID

SSID choice: FWT AP

"FWT AP"

Security Mode: Disable

Apply Cancel

3.2.2.2 WPAUTO(WEP) Mode

WEP is a method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F(a-f)) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network.

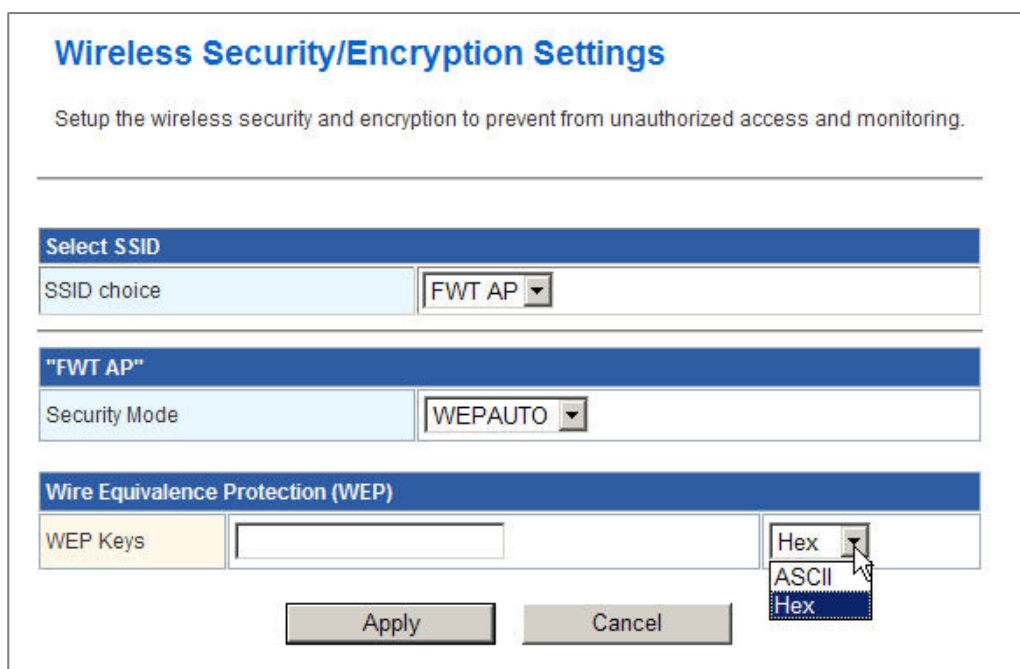
Example,

64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)

128-bit hexadecimal keys are exactly 26 characters in length.
(456FBCDF12340012225271730 is a valid string of 26 characters for 128-bit encryption.)

64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)

128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)



WEP Keys: Select “ASCII” or “Hex” from the pull-down list to set up the key value. ASCII (American Standard Code for Information Interchange) is a code for representing char as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F (a-f).

3.2.2.3 WPA-PSK / WPA2-PSK Mode

WPA (Wi-Fi Protected Access) is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard.

PSK(Pre-Shared Key) is the key which is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format or 64 digits in HEX format at both ends of the wireless connection. When inputting ASCII strings, it cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Wireless Security/Encryption Settings	
Setup the wireless security and encryption to prevent from unauthorized access and monitoring.	
Select SSID	
SSID choice	FWT AP
"FWT AP"	
Security Mode	WPA-PSK
WPA	
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
Pass Phrase	FWT352347030413115
Key Renewal Interval	3600 seconds (0 ~ 4194303)
Apply Cancel	

WPA Algorithms: Mark the option to enable modes of TKIP or AES.

Pass Phrase: This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8-63 ASCII characters or 64 digits in HEX format.

Key Renewal Interval: Enter a value to set up the WPA key renewal interval. The device regenerates the key in every interval seconds that you have setup without disconnection. The WPA Algorithm will regroup the key for a period. The default value is 3600 seconds, and you can adjust the time interval (Valid Range: 0 ~ 4194303).

3.2.3 Station List

From the list of Station, you can see which devices are currently connecting to your FWT Wifi AP_USB x 4 in the wireless way through the MAC address. You also can have a clear realization of status, including Aid, PSM, MimoPS, MCS, BW(Bandwidth), SGI and STBC for each Wifi connection.

Station List

You could monitor stations which associated to this AP here.

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
74:2F:68:90:35:F4	1	0	0	7	20M	0	0

3.2.4 Wireless Statistics

The FWT Wifi AP_USB x 4 offers the counter function to collect all wireless traffic counting information about the transmitting/ receiving packets of this router. The system will automatically update these wireless data per 3 seconds. To restart the counting, please click on the **Reset Counters** button.

Transmit Statistics	
Tx Success	54
Tx Retry Count	0, PER=0.0%
Tx Fail after retry	0, PLR=0.0e+00
RTS Successfully Receive CTS	0
RTS Fail To Receive CTS	0

Receive Statistics	
Frames Received Successfully	313760
Frames Received With CRC Error	243, PER=0.1%

SNR	
SNR	n/a, n/a, n/a

Tx Success: Display the transmitted number of the successful packets.

Tx Retry Count: Display the transmitted number of the retry packets.

Tx Fail after retry: Display the transmitted number of the unsuccessful packets after retry.

RTS Successfully Receive CTS: Display the transmitted number of RTS(Request To Send) packets which receive CTS(Clear To Send) packets successfully.

RTS Fail To Receive CTS: Display the transmitted number of RTS(Request To Send) packets which receive CTS(Clear To Send) packets unsuccessfully.

Frames Received Successfully: Display the received number of the successful frames.

Frames Received With CRC Error: Display the received number of frames with CRC error packets.

SNR: Signal-to-Noise ratio (SNR). It stands that how fast wireless data of the router can travel and how far a wireless signal of the router can reach.

3.3 FireWall Settings

3.3.1 MAC/IP/Port Filtering Settings

The router could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet. The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users. Port filter restricts certain type of data packets from your LAN to Internet through the router.

MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus, worm and malicious activity on the Internet.

Basic Settings

MAC/IP/Port Filtering:

Default Policy -- The packet that doesn't match with any rules must be:

MAC/IP/Port Filter Settings

Source MAC address	<input type="text"/>
Dest IP Address	<input type="text"/>
Source IP Address	<input type="text"/>
Protocol	<input type="text" value="None"/>
Dest Port Range	<input type="text"/> - <input type="text"/>
Source Port Range	<input type="text"/> - <input type="text"/>
Action	<input type="text" value="Accept"/>
Comment	<input type="text"/>

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:

No.	Source MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Packets dropped that don't match with any rules above									-

Basic Settings:

MAC/IP/Port Filtering: Enable/Disable the function of MAC/IP/Port Filtering.

Default Policy - The packet that doesn't match with any rules must be: Dropped/Accepted. For example, if you select "Dropped", all packets that do not match the rule you set up in the following **MAC/IP/Port FilteringSettings** would be dropped.

MAC/IP/Port Filtering Settings:

Source MAC address: Fill out the MAC address that you wish to filter.

Dest IP Address: Fill in the destination IP address that you wish to filter.

Source IP Address: Fill in the source IP address that you wish to filter.

Protocol: Select the protocol type of TCP, UDP or ICMP.

Dest Port Range: Fill in the destination port range that you wish to filter.

Source Port Range: Fill in the source port range that you wish to filter.

Action: You can either choose "Accept" or "Drop" to permit or prevent the action.

Comment: Input any text to describe this mapping, up to 16 alphanumerical characters.

IP/Port Filter Rule List: Lists the IP / Port Filter Settings you have added before. Click on the **Delete Selected** button to delete the selected list.

3.3.2 Port Forwarding Settings

This function offers the way of Port Forwarding / Virtual Server in order to help redirect requests from computers on the LAN to a server set up on the LAN. You can set up an Internet service on the computer on local network, without exposing it on Internet directly. You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address.

3.3.2.1 Create a Port Forwarding

In this section, you can add a new port forwarding to the port forwarding table below or delete an existing entry from this table.

Port Forwarding				
Port Forwarding	Enable			
IP Address				
Port Range				
Protocol	TCP&UDP			
Comment				
(The maximum rule count is 32.)				
Apply Reset				
Current Port Forwarding in system:				
No.	IP Address	Port Range	Protocol	Comment
1	10.10.10.10	100 - 111	TCP + UDP	
Delete Selected Reset				

Port Forwarding: Enable/Disable the function of Port Forwarding.

IP Address: Fill in the IP address of your LAN Server.

Port Range: Fill in the port range that you wish to filter.

Protocol: Select the protocol type, including TCP, UDP or TCP&UDP used by the service.

Comment: Input any text to describe this mapping. Up to 16 alphanumeric characters can be filled in.

Port Forwarding Mapping List: After completing the above settings, please click on the **Apply** button. The entry of Port Forwarding you had added will be listed on this table if it is created successfully. Clicking on the **Delete Selected** button will remove the existing entry you select from this table.

3.3.2.2 Create a Virtual Server

In this section, you can add a new virtual server to the virtual server table below or delete an existing entry from this table.

The Virtual Server option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and LAN port. For Example,

You are hosting a Web Server on a PC that has LAN IP Address of 10.10.10.50 and your ISP is blocking Port 80.

1. Enter the IP Address of the machine on your LAN (for example: **10.10.10.50**)
2. Enter the Public Port as [8888]
3. Enter the Private Port as [80]
4. Select the Protocol - TCP
5. Click the **Apply** button to add the settings to the Virtual Server Table
6. Repeat these steps for each Virtual Server Rule you wish to add. With this Virtual Server entry, all Internet traffic on Port 8888 will be redirected to your internal web server on port 80 at IP Address 10.10.10.50.

Virtual Server					
Virtual Server	Enable ▾				
IP Address	<input type="text"/>				
Public Port	<input type="text"/>				
Private Port	<input type="text"/>				
Protocol	TCP&UDP ▾				
Comment	<input type="text"/>				
(The maximum rule count is 32.)					
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					
Current Virtual Servers in system:					
No.	IP Address	Public Port	Private Port	Protocol	Comment
1 <input type="checkbox"/>	10.10.10.50	8888	80	TCP	Web
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>					

Virtual Server: Enable/Disable the function of Virtual Server.

IP Address: The IP address of the system on your internal network that will provide the virtual service, for example, **10.10.10.50**.

Public Port: The port that will be accessed from the Internet.

Private Port: The port that will be used on your internal network.

Protocol: Select the protocol type, including TCP, UDP or TCP&UDP used by the service.

Comment: Input any text to describe this mapping. Up to 16 alphanumeric characters can be filled in.

Virtual Server Mapping List: After completing the above settings, please click on the **Apply** button. The entry of Virtual Server you had added will be listed on this table if it is created successfully. Clicking on the **Delete Selected** button will remove the existing entry you select from this table.

3.3.3 DMZ Settings

The DMZ (Demilitarized Zone) is used to enable protocols, which needs to open ports on the router. The router will forward all unspecified incoming traffic to the host specified in this setting page. To configure it, mark to enable virtual DMZ and then enter the Host IP (private IP address) and click the **Apply** button to enact the setting.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

DMZ Settings	
DMZ Settings	Disable
DMZ IP Address	<input type="text"/>

Except TCP port 80

Apply Reset

DMZ Settings: Enable/Disable the function of DMZ.

DMZ IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its address automatically using DHCP, then you may want to make a static reservation in the field of **Statically Assigned** on the *Internet Settings* → *LAN* setting page so that the IP address of the DMZ machine does not change.

Except TCP port 80: If you click on the checkbox in front of **Except TCP port 80** function, it means that TCP port 80 cannot be used for DMZ; otherwise, you can use this port for DMZ.

3.3.4 System Security Settings

To improve the safety of the internal network environment, FWT Wifi AP_USB x 4 offers a variety of basic firewall management functions, including Remote management (via WAN), Ping from WAN Filter, Block port scan, Block SYN Flood and SPI Firewall. By the configuration the following system security settings, you can protect the router itself from being attacked, scanned or intruded.

The screenshot shows the 'System Security Settings' web interface. At the top, there is a title 'System Security Settings' and a subtitle 'You may configure the system firewall to protect AP/Router from unauthorized access.' Below this, there are five sections, each with a blue header and a light blue background:

- Remote management**: 'Remote management (via WAN)' is set to 'Deny'.
- Ping from WAN Filter**: 'Ping from WAN Filter' is set to 'Disable'.
- Block Port Scan**: 'Block port scan' is set to 'Disable'.
- Block SYN Flood**: 'Block SYN Flood' is set to 'Disable'.
- Stateful Packet Inspection (SPI)**: 'SPI Firewall' is set to 'Disable'.

At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

Remote management (via WAN): Allow or Not Allow the user to log in the system with the WAN IP.

Ping from WAN Filter: Enable/Disable the function of Ping from WAN Filter. If the function is enabled, the system will reject to response the ICMP(ping) packets coming from the WAN.

Block port scan: Enable/Disable the function of Block port scan. The port scan actions will be dropped if you enable this function.

Block SYN Flood: Block TCP SYN Flood or not. If this function is enabled, it can prevent the system from being attacked by a large amount of SYN packets.

SPI Firewall: SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyberattacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol.

3.4 Management

3.4.1 System Management

You may configure language, administrator's account and password, and NTP settings here.

The screenshot displays three configuration sections:

- Language Settings:** A dropdown menu for 'Select Language' is set to 'English'. Below are 'Apply' and 'Cancel' buttons.
- Administrator Settings:** The 'Account' field contains 'admin' and the 'Password' field contains six dots. Below are 'Apply' and 'Cancel' buttons.
- NTP Settings:** The 'Current Time' is 'Sat Jan 1 01:28:47 UTC 2000'. The 'Time Zone' dropdown is set to '(GMT-11:00) Midway Island, Samoa'. The 'NTP Server' field is empty, with examples: 'time.nist.gov', 'ntp0.broad.mit.edu', and 'gps.ntp.br'. The 'NTP synchronization' field is empty, followed by the unit 'hours'. Below are 'Apply' and 'Cancel' buttons.

Language Settings: Select the language which you would like. Currently, only English is included.

Administrator Settings: Modify the account and password to set up and manage the FWT Wifi AP_USB x 4. The default settings for administrator are as follows:

Username: admin

Password: admin

NTP Settings: Set up the system time by syncing from the NTP server.

Current Time: Show the system time of the router. Its format: day of week, month, day, hours : minutes : seconds, year. For instance, Wed, Aug. 29, 12:10:10, 2012.

Time Zone: It is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the router will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The router supports configurable time zone from -11 to +12 step 1 hour. Default Time zone: -11 Hrs.

NTP Sever: NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If you manually specify an IP address of user-defined NTP server as well as Time Zone, the router will sync the time immediately after pressing the **Apply** button.

NTP Synchronization: Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing. You can set up the time interval (Valid range: 1 ~ 300 hours) to have the assigned NTP server do the synchronization of time for your router.

3.4.2 SIM Card Control

(Note: This Section is also Suitable for the USB1 /USB2/USB3 SIM Functions.)

On this SIM Card Control settings page, you can set up the password for SIM card's authentication. FWT Wifi AP_USB x 4 will detect automatically the current limit times of PIN code and PUK input for your SIM card. If the remaining times of PIN code input are less than 3 times, the system will stop all related functions. You should configure the PIN code of the SIM card on this web setting page, and enter the correct PIN code again before the reboot of the device.

Note 1: The wrong input of PIN code and PUK in the following setup will decrease the allowable input times of PIN code and PUK.

Note 2: Any changes on this webpage, the user needs to reset to power to have all related functions work normally.

Information	
SIM Card Status	READY
Remaining attempts to enter PIN	3
Remaining attempts to enter PUK	10

<input type="checkbox"/> Automatic PIN CODE insertion on boot	
Type the PIN CODE for automatic insertion:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Enable PIN request for inicalization	
Enable	No <input type="button" value="v"/>
PIN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Enter PIN	
PIN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Change PIN	
Old PIN	<input type="text"/>
New PIN	<input type="text"/>
Confirm New PIN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

PIN Unlock	
PUK	<input type="text"/>
New PIN	<input type="text"/>
Confirm New PIN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Information Table: This table will show all information about the SIM card used in your FWT Wifi AP_USB x 4. For more details, please refer to the following parameters below:

SIM Card Status: It includes “SIM not inserted”, “READY”, “SIM PIN”, “SIM PUK”, “ERROR” five statuses.

- **SIM not inserted:** It stands that the SIM card has not been inserted into the router yet.
- **READY:** It stands that the SIM card works normally.
- **SIM PIN:** It stands that the user needs to input the correct PIN code due to the wrong PIN code value of system.
- **SIM PUK:** It stands that the SIM card has already been locked. The user needs to request ISP and input the correct PUK to unlock the SIM card.
- **ERROR:** This message will be shown if the system fails to detect the information of the SIM card.

Remaining attempts to enter PIN: It shows the remaining times that you are allowed to input the PIN code for the SIM card inserted into the router. Once the times exceeds 3 times, the SIM card will be locked.

Remaining attempts to enter PUK: It shows the remaining times that you are allowed to input the PUK for the SIM card inserted into the router. Once the times exceeds 10 times, the SIM card will be useless.

Automatic PIN CODE insertion on boot: Decide that whether to use the value filled in the field of **Type the PIN CODE for automatic insertion** to do the authentication of SIM card or not while the router is powered on. To enable it, please click on the checkbox in front of this function.

Enable PIN request for initialization: Enable/Disable the PIN code function. In case this function is enabled and your SIM card has the PIN code setup, you must input the correct pin code and press the **Apply** button for the authentication. Three successively incorrect input of Pin Code will make the SIM card locked.

Enter PIN: In case the field of SIM Card Status in the Information Table is at the “SIM PIN” status, you should enter the correct PIN code in the **PIN** field of this function and press the **Apply** button for authentication. The system will return the message in the pop-up window for you to realize whether your setting is successful or not.

Change PIN: Besides the cell phone, you are also allowed to modify your PIN code of the SIM card through this function. To modify this password, please fill in your old password and your desired new password accordingly, then re-key this new password into the **Confirm New PIN** field. The new settings will be taken effect immediately after you press the **Apply** button. You also can realize whether this change is successful or not from the message returned by the system in the pop-up window.

PIN Unlock: As we had mentioned above the “SIM PUK” status displayed in the field of SIM Card Status in the Information Table, it means that the SIM card is locked. To unlock the SIM card, you should enter the correct PUK in the **PUK** field of this function and new PIN code accordingly. Also re-key this new PIN into the **Confirm New PIN** field of this function before pressing the **Apply** button for authentication. The system will return the message in the pop-up window for you to realize whether your setting is successful or not.

3.4.3 SMS Sending/Receiving

Like the mobile phones, the user is able to send/receive the SMS through the FWT WIFI AP_USB x 4. After the edition of your message on the SMS webpage, this SMS will be sent out easily to the given mobile phone number by clicking on the **Send** button. Besides, you also can read the SMS(s) sending from any mobile phones in the folder of InBox on this webpage.

	Phone Number	Date	SMS Message
<input type="checkbox"/>	1 +886934187676	12/12/21 14:25:16	Test
<input type="checkbox"/>	2 +886975435123	12/11/21 15:51:54	FWT SMS Test from 3JTech

Send To: The assigned mobile phone number that will receive the message edited by the user.

Content: The text of the message that the user would like to send out. Up to 160 characters can be filled in. Valid letters are A-Z, a-z, 0-9 characters as well as the symbols shown on the keyboard. Please note that it will only accommodate 70 characters if any Chinese is included.

In Box: The folder of all SMS(s) that had been sent to the phone number of SIM card inserted into the FWT WIFI AP W_WAN. Please also note that the SMS function does not support the automatic refresh function, the user needs to refresh this webpage by pressing the **Refresh** button to see that if there is any new SMS(s) received.

Sent Box: The folder of the SMS copies that had been sent out from the phone number of SIM card inserted into the FWT WIFI AP W_WAN.

Delete: To remove any SMS(s) from the folder of In Box/Sent Box. Just click on the checkbox in front of the desired SMS(s) and press this button, the selected SMS(s) will be deleted immediately.

3.4.4 TR-069

Due to the built-in TR-069 function, FWT WIFI AP W_WAN will allow the administrator to remotely do the firmware upgrade, system configuration, management, troubleshooting via the Auto-Configuration Server (ACS) in the method of HTTP Internet network connection. ACS is a TR-069_based automatic configuration server, implementing CPE WAN Management Protocol (CWMP). For more details on the ACS, please refer to our ACS Administrator's User Manual.

ACS Server	
URL	<input type="text" value="http://61.56.193.38:8080/openacs/acs"/>
Periodic Inform Settings	
Enable	<input type="text" value="Enable"/>
Interval Time	<input type="text" value="120"/> Sec
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

URL of ACS Server: For the FWT WIFI AP W_WAN 's access of TR-069 service from ACS through the web browser, please fill in the path in which the ACS is built. For example, `http://61.56.193.38:8080/openacs/acs`)

Enable: Activate/Deactivate the FWT WIFI AP W_WAN 's TR-069 functionality.

Interval Time of Periodic Inform Settings: Enter a value to set up or change the Periodic Inform Interval of the FWT WIFI AP W_WAN. Upon this time interval you had set up, FWT WIFI AP W_WAN will communicate with ACS periodically and automatically. Please note that the value of **Periodic Inform Interval Time** must be more than 30 seconds, and the maximum of this Interval Time can be 4294967295 in seconds.

3.4.5 Fax Sending/Receiving via FWT

Not only does FWT Wifi AP_USB x 4 support an analog phone to be connected to its phone jack to make and receive calls, but it allows the user to connect a fax machine for the sending/receiving of the facsimile.

3.4.5.1 Usage of FAX

Use the procedures listed below for step-by-step instructions to send your facsimile separately based on your case. Also be sure that you had enabled the fax function on the Fax webpage for your FWT Wifi AP_USB x 4 and have it registered to the fax server built by 3Jtech while doing the following setup. For more details on the software setup, please refer to Section 3.4.5.2.

■ ***In the case of sending the facsimile from the FWT to FWT:***

- 1) Connect a fax machine to the phone jack of your FWT Wifi AP_USB x 4 using a RJ-11 cable. Make sure the SIM card, U6100 module and antenna has been installed on your router.
- 2) Power on the fax machine and your FWT Wifi AP_USB x 4.
- 3) Wait for the dial tone on the fax handset. The router is ready when you hear the dial tone.
- 4) Insert pages you would like to send into the fax machine.
- 5) Dial the command of ***329#*destination FWT number#** on the fax machine connected to the FWT Wifi AP_USB x 4. Wait to hear a long ring. About this dial command, you can refer to the **FAX Number** parameter described in Section 3.4.5.2.
- 6) Immediately, you will hear the fax modem sound after long ring. Press the "**Send**" button on your fax machine.
- 7) Wait for the transmission to complete. At the end, the fax machine will display "page sent" or "error" message. It will print out the report in case any error occurs.

■ ***In the case of sending the facsimile from the FWT to PSTN line:***

- 1) Connect a fax machine to the phone jack of your FWT Wifi AP_USB x 4 using a RJ-11 cable. Make sure the SIM card, U6100 module and antenna has been installed on your router.
- 2) Power on the fax machine and your FWT Wifi AP_USB x 4.
- 3) Wait for dial tone on the fax handset. The router is ready when you hear the dial tone.
- 4) Insert pages you would like to send into the fax machine.
- 5) Dial the command of ***329#destination Fax number#** on the fax machine connected to the FWT Wifi AP_USB x 4. Wait to hear a long ring.

Note: Area code needs to be added when dialing the destination Fax number if your destination PSTN line is located in different city/county.

- 6) Immediately, you will hear the fax modem sound after long ring. Press the "**Send**" button on your fax machine.
- 7) Wait for the transmission to complete. At the end, the fax machine will display "page sent" or "error" message. It will print out the report in case any error occurs.

■ ***In the case of sending the facsimile from PSTN line to the FWT:***

- 1) Connect the PSTN line to the fax machine.
- 2) Power on the fax machine and insert pages you would like to send into the fax machine.
- 3) Contact our 3Jtech to request the server's fax number, and dial this number on the fax machine connected with the PSTN line.
- 4) Just follow the voice instructions you had heard, then dial the command **destination FWT number#** on the fax machine connected with the PSTN line. About the FWT number, you can refer to Section 3.4.5.2.

Note: Area code needs to be added when dialing the fax number of the server if your city/county is different from the one in which 3Jtech's fax sever is located.

- 5) Press the "**Send**" button on your fax machine.
- 6) Wait for the transmission to complete. At the end, the fax machine will display "page sent" or "error" message. It will print out the report in case any error occurs.

3.4.5.2 Fax Settings

FAX Server	
FAX Number	*329#*10000004#
Enable	Enable
Domain Name/ IP address	116.205.70.84
Interval Time	10 Sec

Apply Cancel

FAX Number: *329#*destination FWT number# dial command will be shown in this parameter upon your FWT Wifi AP_USB x 4's registration from our fax sever. It means the facsimile is transmitted to other FWT. You may refer to our Fax Sever User's Manual for further information on the fax sever we offer.

Enable: Activate/Deactivate the FWT Wifi AP_USB x 4's fax functionality. FWT Wifi AP_USB x 4 will not automatically register to the fax server for the obtainment of the facsimile if this function is disabled. Please note that the router will fail to gain the number from the dial command of *329#*destination FWT number# and be unable to send the facsimile out through this command if its registration is unsuccessful.

Domain Name/ IP address: The IP address or DNS that belongs to the fax server.

Interval Time: Like the interval time of TR-069 function as we had mentioned above, please enter a value to set up or change the periodic inform interval for the request of the connection between the FWT Wifi AP_USB x 4 and the fax server. Thus, the FWT Wifi AP_USB x 4 will periodically and automatically communicate with the fax server based on this time interval you had set up. Please note that the value of **Interval Time** must be more than 10 seconds.

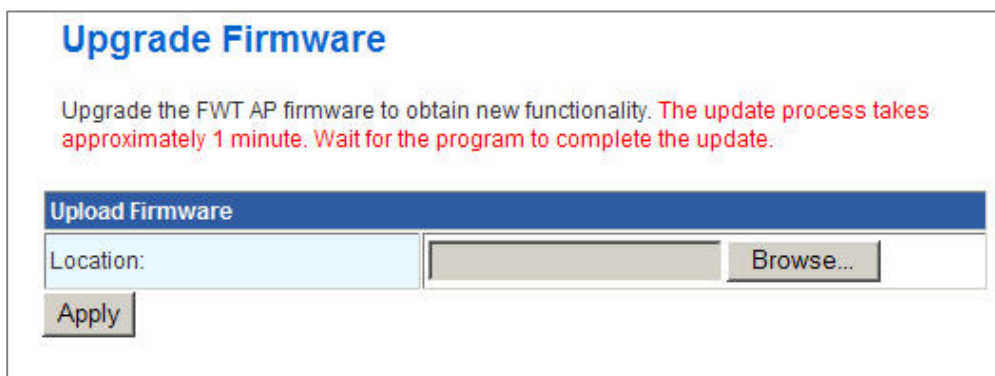
3.4.6 Firmware Upgrade

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. User can upgrade the firmware in this page. Please note that power cannot be off in the process of the software upgrade. You must do it carefully.

Specify the filename and directory where the file is located via the **Browse...** button, and click on the **Apply** button when it is completed. When the upload is finished, the router will start upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the router to have the new software worked.

If your upload is unsuccessful, an error message will be shown in the webpage, and it will not upgrade the software as well.

For FWT WIFI AP_USB x 4's NVRAM value update, you should press the **Reset** button (more than 2 seconds) when the device is on and have it restart. And then power off the router and power on for its normal working.



Location: File path and filename stored the image file you would like to upgrade.

3.4.7 Configuration Management

With this function, user can back up or reload the config files by exporting/ importing settings.

Besides through the press of the **RESET** button in the front panel to execute the hardware reset function as we had mentioned in Section 2.2.1 for the router. The software reset function provided here takes the same effect as the **RESET** button on the front panel of the router. It will take about 30~60 seconds to complete the system boot.

Settings Management

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

Export

Click here to export current configuration

Import

Locate import file

Factory Defaults

Click here to load factory defaults

Export: To export the current settings stored in the flash to a config file, just press the **Export** button.

Import: Import the config file into your router. Specify the filename and directory where the file is located via the **Browse...** button, and press the **Import** button when completed.

Factory Defaults: Restoring the unit to the factory default settings will erase all settings, including any rules that you had created. To have the router's settings be returned to the factory default, just press the **Load Default** button. Please note that the router cannot be powered off while resetting to the factory default.

3.4.8 Status

In the Status page, it tells you the basic information of the system. You can check the device status, including the firmware version, system up time, WAN/Local IP address, MAC address and so on. They will be refreshed per 3 seconds. With these information, it is helpful while malfunctioning.

FWT AP Status	
System Info	
Firmware Version	6.0.0.2
System Up Time	21 mins, 52 secs
Operation Mode	Gateway Mode
Internet Configurations	
WAN IP Address	192.168.100.187
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.1
Primary Domain Name Server	168.95.1.1
Secondary Domain Name Server	168.95.1.1
3G Internal WAN IP Address	111.80.25.96
3G Internal Subnet Mask	255.255.255.255
3G Internal Default Gateway	10.64.64.64
3G USB0 WAN IP Address	
3G USB0 Subnet Mask	
3G USB0 Default Gateway	
3G USB1 WAN IP Address	
3G USB1 Subnet Mask	
3G USB1 Default Gateway	
3G USB2 WAN IP Address	
3G USB2 Subnet Mask	
3G USB2 Default Gateway	
VPN IP Address	
VPN Subnet Mask	
VPN Default Gateway	
Local Network	
Local IP Address	10.10.10.254
Local Netmask	255.255.255.0
MAC Address	00:09:B5:12:06:89
IMEI	352347030406341
Registration Network	Local
CSQ	13
PLMN	Chunghwa Telecom
Connection Type	HSUPA
MyLoc (MCC:MNC:LAC:CI)	466:92:10291:74731

3.4.9 Statistic

FWT Wifi AP_USB x 4 offers the counter function to collect all counting information about the memory status and all interfaces' receiving/transmitting packets of this router.

Statistic	
Memory	
Memory total:	28572 kB
Memory left:	10780 kB
All interfaces	
Name	ra0
Rx Packet	7143
Rx Byte	1083841
Tx Packet	66
Tx Byte	0
Name	eth2.2
Rx Packet	0
Rx Byte	0
Tx Packet	22
Tx Byte	2146
Name	br0
Rx Packet	324
Rx Byte	22871
Tx Packet	144
Tx Byte	86510

4. GSM Setup

This chapter will instruct you how to set up the code of PIN/Call Barring as well as the functions of Call Barring, Call Forwarding/Diversion, Call Waiting and Number Presentation for MD910 via the analog phone. You can refer to the commands listed below and dial these buttons on the analog phone connected to MD910 upon your needs.

Type	Command Strings	Function Description
Code Management	**03*OldCode*NewCode*NewCode#	Change code for call barring
	**03*330*OldCode*NewCode*NewCode#	Change code for call barring
	**04*OldPIN*NewPIN*NewPIN#	Change PIN code
	**042*OldPIN2*NewPIN2*NewPIN2#	Change PIN2 code
	**05*PUK*NewPIN*NewPIN#	Unlock PIN code
	**052*PUK2*NewPIN2*NewPIN2#	Unlock PIN2 code
Call Barring	**33*code#	Activate barr all outgoing calls (for code see "Safety" above)
	#33*code#	Deactivate barr all outgoing calls
	**330*code#	Activate barr all calls
	#330*code#	Deactivate barr all calls
	**331*code#	Activate barr all outgoing international calls
	#331*code#	Deactivate barr all outgoing international calls
	**332*code#	Activate barr all outgoing international calls except home
	#332*code#	Deactivate barr all outgoing international calls except home
	**333*code#	Activate barr all outgoing calls
	#333*code#	Deactivate barr all outgoing calls
	**35*code#	Activate barr all incoming calls
	#35*code#	Deactivate barr all incoming calls
	**351*code#	Activate barr all incoming calls when roaming
	#351*code#	Deactivate barr all incoming calls when roaming
	**353*code#	Activate barr all incoming calls
	#353*code#	Deactivate barr all incoming calls

Call Forwarding/ Diversion	##002#	Unregister all call diversions
	**004*PhoneNumber#	Set all configured call diversions to PhoneNumber
	##004#	Unregister all configured call diversions
	**21*PhoneNumber#	Register and activate divert all calls to PhoneNumber
	*21#	Activate divert all calls
	#21#	Deactivate divert all calls
	##21#	Unregister divert all calls
	**61*PhoneNumber#	Register and activate divert on no answer to PhoneNumber
	*61#	Activate divert on no answer
	#61#	Deactivate divert on no answer
	##61#	Unregister divert on no answer
	**62*PhoneNumber#	Register and activate divert on not reachable
	*62#	Activate divert on not reachable
	#62#	Deactivate divert on not reachable
	##62#	Unregister divert on not reachable
	**67*PhoneNumber#	Register and activate divert on busy
	*67#	Activate divert on busy
	#67#	Deactivate divert on busy
##67#	Unregister divert on busy	
Call Waiting	*43#	Activate call waiting
	#43#	Deactivate call waiting
	#1	Hang up current call, make waiting or on-hold call active
	#2	Put the call on hold, make waiting or on-hold call active
	#3	Put the call and on-hold call active in conference

Number presentation	*30#PhoneNumber	Activate CLIP
	#30#PhoneNumber	Deactivate CLIP
	*31#PhoneNumber	Activate CLIR for this call
	#31#PhoneNumber	Deactivate CLIR for this call
	*76#	Activate COLP
	#76#	Deactivate COLP