

USER GUIDE

Verizon Jetpack™
4G LTE Mobile Hotspot
Model#: 890L
Global Ready™



LEGAL INFORMATION

Copyright © 2012 ZTE CORPORATION.

All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without the prior written permission of ZTE Corporation.

The manual is published by ZTE Corporation. We reserve the right to make modifications on print errors or update specifications without prior notice.

Version No. : 1.0

Edition Time : 03-2012

CONTENTS

Welcome	4
Thank You for Choosing Verizon Wireless	4
Getting Started.....	5
Screen Indicators	6
Hardware Installation.....	8
Installing the 4G SIM Card	8
Inserting and Charging the Battery.....	9
Removing the 4G SIM Card	11
Connecting to the Internet	12
Connecting Wi-Fi Enabled Devices To Your Jetpack	12
Follow these Steps.....	13
Accessing the Internet.....	13
Advanced Configuration.....	14
PIN Code Verification.....	15
Basic Setup	16
WAN Settings.....	17
Router	20
Wi-Fi Settings.....	21
Firewall.....	26
SMS	31

Navigating the Device	32
WAN Info	33
WLAN Info	33
Settings.....	34
Message	36
Usage of WPS	36
Glossary.....	37
How to Get Help.....	41
Health and Safety Information	41
General Guidelines	41
Aircraft Safety	46
Hospital Safety	47
Road Safety	47
Vehicles Equipped with an Airbag	48
Third Party Equipment.....	48
Efficient Use.....	49
CTIA Requirements.....	49
Radio Frequency (RF) Exposure	50
FCC Compliance	52
Consumer Limited Warranty	55

Welcome

Thank You for Choosing Verizon Wireless

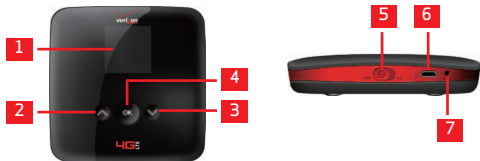
You're now connected to the blazingly fast, powerfully brilliant Verizon 4G LTE Network. This guide will help you understand your new mobile hotspot and all the things you can do with it at home or abroad. So let's get started.

This guide will show you how to unleash the potential of your new Verizon Jetpack™. Assistance is at your fingertips at **verizonwireless.com/support**. Customer Service is at your disposal at **1-800-922-0204** or in any Verizon Wireless Communications Store.

Device Introduction

The Verizon Jetpack™ - 890L is a newly developed 4G LTE Mobile Hotspot. It is Global Ready™ providing flexible access for users to enjoy high-speed internet applications around the globe. When connected to the Verizon 4G LTE Network, the Jetpack can support simultaneous connections to up to 10 Wi-Fi enabled devices. When connected in 2G or 3G mode the Jetpack can support simultaneous connections to 5 Wi-Fi enabled devices.






Getting Started


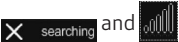









BUTTONS AND INTERFACE	DESCRIPTION
1. SCREEN	Displays the menus and the status of your Jetpack.
2. UP BUTTON	Scroll up to select the options.
3. DOWN BUTTON	Scroll down to select the options.

4. OK BUTTON	<ul style="list-style-type: none"> • Confirm highlighted selection. • When the Jetpack button is locked, press once to light up the screen, and press again to unlock.
5. POWER SWITCH	Power on/off your Jetpack.
6. MICRO USB PORT	Charge your Jetpack.
7. RESET BUTTON	Press and hold to restore your Jetpack to the factory default settings.

Screen Indicators

Icon	Description
	Battery Status
	4G Network
	3G Network
	2G Network
	Data Connected

Icon	Description
	Signal Strength
	No Network Service
	Roaming Signal Strength
	Roaming
	SMS
	New SMS
	SMS Full
	Number of current Wi-Fi connections
	Settings

Hardware Installation

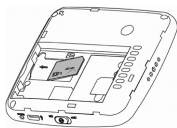
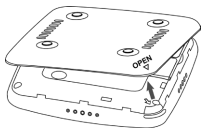
Installing the 4G SIM Card

If you have not already done so, please follow these instructions for the installation of your new 4G SIM Card:

1. Remove 4G SIM Card from the outer card, being careful not to touch the gold contacts.

CAUTION: Do not bend or scratch your 4G SIM Card. Avoid exposing your 4G SIM Card to static electricity, water or dirt.

2. Turn the power off. Remove the battery cover and take the battery out. Locate the 4G SIM card slot. Hold the card so the Verizon Wireless logo on the card is facing you and the gold contact points are properly aligned with the 4G SIM Card slot.



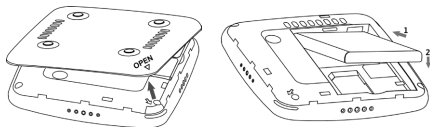
3. Insert 4G SIM Card with the Verizon Wireless logo facing you into the slot until it is fully inserted.

NOTE: Your 4G SIM (Subscriber Identity Module) Card is a small rectangular plastic card that stores your phone number and important information about your wireless service.

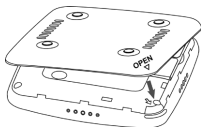
The 4G SIM Card **MUST** remain in the Jetpack when in use.

Inserting and Charging the Battery

1. Use the thumb catch at the bottom of the device to open the battery cover and align the battery contacts with the terminals in the battery compartment as shown. Push the battery down until it clicks into place.

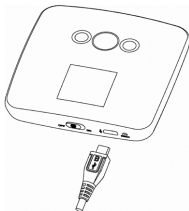


2. Place the battery cover over the battery compartment ensuring that the arrow on the device and the arrow on battery cover are aligned. Then press the battery cover downward until it clicks into place.



Your device comes with wall charger. To charge:

1. Plug one end of the wall charger into an electrical outlet and the the other end into the device's **MICRO USB PORT**.



2. It is recommended the battery be fully charged before you use your Jetpack for the first time.

NOTE: The charge time varies depending upon the battery level. The device will stop charging if the temperature of the battery exceeds 113 °F/45 °C.

Removing the 4G SIM Card

1. Turn the Verizon Jetpack power off. Remove the battery cover and take out the battery.
2. Gently remove the SIM Card from the SIM Card slot.

NOTE: Should your 4G SIM Card be lost or damaged please call **1-800-922-0204** to speak with a Customer Service Representative. From outside the U.S. call **+ 1-908-559-4899** for 24/7 Global Support.

You can move the 4G SIM Card from one device to another and your wireless service will work seamlessly as long as you have a compatible device and service plan. To see which devices are compatible with the Verizon Wireless 4G SIM Card, visit **verizonwireless.com/certifieddevice**.

For additional information about 4G SIM Cards, visit **verizonwireless.com/4GSIM**.



Connecting to the Internet

With your new Verizon Jetpack, a wireless Internet connection can always be at your fingertips.

Connecting Wi-Fi Enabled Devices To Your Jetpack

NOTE: It is recommended the battery be fully charged in order to use your Jetpack via Wi-Fi for the first time, or connect your Jetpack to the wall adapter for power.

The following should occur once you power on your Jetpack:

- Your Jetpack is powered as soon as you slide the **Power Switch** to **On** and the display lights up.
- Once your Jetpack is powered on and has been activated, it automatically connects to the Internet provided that Mobile Broadband service is available and one or more Wi-Fi devices are connected to the Jetpack.
- The Service(4G LTE, 3G, 2G), Signal Strength , and Data Connected  icons on your Jetpack indicate it is in service and ready to connect.

Follow these Steps

1. Ensure the Wi-Fi enabled device you wish to connect to your Jetpack has Wi-Fi turned on, then use the Wi-Fi application to establish a connection to your Jetpack.
2. Look for the network (SSID) named “**Verizon-890L**”. There are XXXX digits unique to your device following the network (SSID) name displayed.
3. Click **Connect** and enter the default password printed on the back of your Jetpack .

NOTE: Your password will also be displayed on the Jetpack screen each time the Jetpack is powered on.

Accessing the Internet

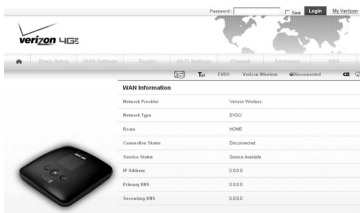
After successfully establishing the connection between your Jetpack and computer, you can access the Internet in the **Auto Connect, Manual Connect** mode. The default mode is **Auto Connect**.

Advanced Configuration

1. Make sure your computer is connected to the Jetpack.
2. Launch the internet browser and enter **http://192.168.1.1** or **http://vz.hotspot** in the address bar.

NOTE: It is recommended that you use IE (7.0 or later), Firefox (3.0 or later), Opera (10.0 or later), Safari (4.0 or later) or Chrome (5.0 or later).

3. The login page appears as follows:



Input the case-sensitive default password printed on the back of your Jetpack, and then click **Login** to access the Web User Interface.

NOTE: Do not put anything on the top of your Jetpack. Do not lay devices to overlap each other when using. The Jetpack takes 1-2 minutes to initialize, and attach to the network.

PIN Code Verification

If the PIN code of your SIM card is enabled, you will need to input the PIN code after you logging in.

Verify PIN

PIN

PIN Remaining Times

3

Apply

NOTE: The SIM card will be locked if you enter wrong PIN code consecutively for three times. If you want to change the PIN status or modify the PIN code, please select **WAN Settings > SIM PIN** to do the actions.

SIM PIN

PIN Status

Enable

Action

Disable

Enable

PIN

Disable

Modify

PIN Remaining Times

3

Apply

Basic Setup

After logging in, select **Basic Setup > Quick Setup** to configure the Wi-Fi settings, including **Wi-Fi Network Name**, **Wi-Fi Security Policy** and **Sleep Time**.

The screenshot shows the 'Basic Setup' configuration page with the 'Quick Setup' tab selected. The page is divided into three main sections: 'Wi-Fi Network Name', 'Wi-Fi Security Policy', and 'Sleep Time'. In the 'Wi-Fi Network Name' section, the 'SSID' field contains 'Verizon-Euf-B0D-63AE' with a note '(1-30 characters)' and the 'Broadcast SSID' is set to 'Enabled'. In the 'Wi-Fi Security Policy' section, the 'Wi-Fi Security Type' is set to 'NONE'. In the 'Sleep Time' section, the 'Sleep Time' is set to '10 Minutes'. At the bottom of the page is a 'Next' button.

Basic Setup		Quick Setup	Password
Wi-Fi Network Name			
SSID	Verizon-Euf-B0D-63AE (1-30 characters)		
Broadcast SSID	Enabled		
Wi-Fi Security Policy			
Wi-Fi Security Type	NONE		
Sleep Time			
Sleep Time	10 Minutes		
Next			

Select **Basic Setup > Password** to change the login password for the Web User Interface.

The screenshot shows the 'Basic Setup' configuration page with the 'Password' tab selected. The page is titled 'Set Administration Password'. It contains three input fields: 'Current Password', 'New Password' (with a note '(8-20 characters)'), and 'Confirm New Password'. At the bottom of the page are 'Apply' and 'Cancel' buttons.

Basic Setup		Quick Setup	Password
Set Administration Password			
Current Password			
New Password	(8-20 characters)		
Confirm New Password			
Apply Cancel			

WAN Settings

After logging in, select **WAN Settings > Wireless Info** to display the information of WAN wireless. Click **Refresh** to update the information.

WAN Settings **Wireless Info** Network Select WAN Connection SIM PIN

WAN Wireless Information

Network Provider	Verizon Wireless
Network Type	EVDO
Roam	HOME
RSSI	-76 dBm
Ec/Io	-7.0 dBm
Cell ID	EVDO 004dc008c00000000edbf11974028e6
LAC Code	CDMA7

Refresh

Select **WAN Settings > Network Select** to select the proper network mode, including **Global Mode**, **LTE/CDMA Mode**, and **GSM Mode(Automatic/Manual)**. Click **Apply** to confirm your choice.

WAN Settings Wireless Info **Network Select** WAN Connection SIM PIN

Network Selection Mode

G	Global Mode
C	LTE/CDMA Mode
C	GSM Mode Automatic

Apply

NOTE: In **GSM Mode**, you can either set your device to automatic network selection or manual network selection. If you choose the manual, you will be prompted to select what GSM network you would like to connect to.

WAN Settings Wireless Info **Network Select** WLAN Connection SIM PIN

Network Selection Mode

☐ Global Mode

☐ LTE/CDMA Mode

☒ GSM Mode **Manual**

Apply

WAN Settings Wireless Info **Network Select** WLAN Connection SIM PIN

Network Selection Mode

Accessing data during trips outside the US may result in significantly higher charges. Do you want to allow data access?

Apply **Cancel**

Index	MCC	MNC	Network Name	Registration Status	Network Mode	Operation
1	460	00	CHINA MOBILE	available for registration	GSM	Connect
2	460	02	CHINA MOBILE	available for registration	WCDMA	Connect
3	460	01	CHINA MOBILE	forbidden registration	WCDMA	Connect
4	460	01	CHINA MOBILE	forbidden registration	GSM	Connect

Return

Select **WAN Settings > WAN Connection** to choose the WAN Connection mode according to your requirement.

The screenshot shows the 'WAN Settings' menu with four tabs: 'Wireless Info', 'Network Select', 'WAN Connection' (which is selected and highlighted), and 'SIM PIN'. Below the tabs, the 'WAN Connection' section is visible. It contains two rows: the first row has a radio button labeled 'A' and the text 'Auto Connect'; the second row has a radio button labeled 'C' and a dropdown menu labeled 'Manual Connect' with 'connect_internet' selected. Below these rows, it shows 'WAN Connection Status' as 'Disconnected'. At the bottom left, there is an 'Apply' button.

WAN Settings	
Wireless Info	Network Select
WAN Connection	SIM PIN
WAN Connection	
A	Auto Connect
C	Manual Connect connect_internet
WAN Connection Status	
Disconnected	
Apply	

Auto Connect: The device will connect to the Internet automatically when it is powered on.

Manual Connect: Connect/disconnect to the Internet connection manually.

Select **WAN Settings > SIM PIN** to enable/disable/modify the PIN code of your SIM card.

The screenshot shows the 'WAN Settings' menu with four tabs: 'Wireless Info', 'Network Select', 'WAN Connection', and 'SIM PIN' (which is selected and highlighted). Below the tabs, the 'SIM PIN' section is visible. It contains three rows: the first row has 'PIN Status' set to 'Disable'; the second row has 'Action' with a dropdown menu showing 'Enable'; the third row has 'PIN' with an empty input field. Below these rows, it shows 'PIN Remaining Times' as '2'. At the bottom left, there is an 'Apply' button.

WAN Settings	
Wireless Info	Network Select
WAN Connection	SIM PIN
SIM PIN	
PIN Status	Disable
Action	Enable
PIN	
PIN Remaining Times	2
Apply	

Router

After logging in, select **Router > LAN** to access the interface below:

Router

LAN

DMZ

LAN Interface Setup

IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
MAC Address	38-45-08-10-63-aa
DHCP Server	<input type="button" value="Enable"/>
DHCP IP Pool	<input type="text" value="192.168.1.2"/> - <input type="text" value="192.168.1.99"/>

IP Address: IP address for LAN interface.

Subnet Mask: Subnet mask for the IP address.

MAC Address: MAC address for the LAN interface.

DHCP Server: Enable/disable DHCP server function.

DHCP IP Pool: Allocate start and end IP address for IP pool.

Select **Router > DMZ** to access the interface below:

Router

LAN

DMZ

DMZ Setting (DMZ means demilitarized zone)

IP Address	<input type="text"/>
------------	----------------------

DMZ means demilitarized zone, click **Add** to add the Wi-Fi client in DMZ, and click **Apply** to confirm. Click **Delete** to erase the Wi-Fi client from DMZ. An external computer or device can access to the Wi-Fi client which is in DMZ, rather than any other part of the network.

Wi-Fi Settings

After logging in, select **Wi-Fi Settings > Connected Devices** to display the information about the devices connected to your Jetpack.

The screenshot shows the 'Wi-Fi Settings' page with the 'Connected Devices' tab selected. Below the tabs is a table titled 'Wireless Network' with columns for Station, Address Type, MAC Address, IP Address, Host Name, and Nickname. One device is listed with a 'Disconnect' button. An 'Apply' button is at the bottom right of the table. Below the table, there is a note about reconnection and a 'Refresh' button.

Station	Address Type	MAC Address	IP Address	Host Name	Nickname	
Disconnect	1	dhcp	00-13-07-06-5a-11	192.168.1.2	PCANDEERS-SP1	<input type="text"/>

[Apply](#)

If you want the user who has been disconnected to connect to this device again, please operate according to notes in ACL tab.
The max length of nickname is 30.

[Refresh](#)

You can click **Refresh** to update the information, or click **Disconnect** to terminate the wireless connection between these Wi-Fi enabled devices and your Jetpack.

Select **Wi-Fi Settings > Basic** to set the configuration of the wireless network.

Wi-Fi Settings	Connected Devices	Basic	Security	ACL	Firmware
Wireless Network					
Sleep Time	[10 Minutes ▾]				
Network Mode	[11n/gn ▾]				
SSID	[Jetpack-Euf880-83AE (1~30 characters)]				
Broadcast SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
Country Code	[US ▾]				
Frequency (Channel)	[Auto Select ▾]				
MAX Station Number	[5 ▾]				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

Sleep Time: Set the time before the Jetpack enters sleep mode, The Jetpack will enter sleep mode if no Wi-Fi clients (devices) are connected to the Jetpack for a given period of time.

Network Mode: If all of the wireless devices connect with the Jetpack in the same transmission mode, performance will be improved by choosing the appropriate wireless mode.

SSID: Service Set Identifier(SSID). Enter a string less than 30 characters as the name for your wireless local area network(WLAN).

Broadcast SSID: Disable or Enable(Default) this function. If Enable is selected, the Jetpack broadcasts the SSID, and other devices can search and connect to it. When you select Disable, other devices can not search out the SSID. If you want someone to connect, you need tell them the SSID, and let them to setup manually.

AP Isolation: When Enable is selected, each of your wireless clients will not be able to communicate with each other.

Country Code: Choose the right country code.

Frequency(Channel): Choose the appropriate channel to optimize the performance and coverage of your wireless network.

MAX Connections: Choose the maximum number of the Wi-Fi enabled devices which are able to connect to the Jetpack simultaneously.

Click **Apply** to save your settings.

Select **Wi-Fi Settings > Security** to set the Wi-Fi security settings.

The screenshot shows the 'Wi-Fi Settings' page with the 'Security' tab selected. The 'Security Policy' section has 'Security Type' set to 'WPA2-PSK'. The 'WPA' section shows 'WPA Algorithm' set to 'AES' (selected over TKIP), 'GTK' set to 'GCM' (selected over CCMP), and 'Password' set to '1107044'. A small disclaimer at the bottom states: 'The WPA2 password should not contain personal and private information. Because this password will be released to other WPA2 users to establish WPA2 connection. And users can also get it from the device display while connecting on a Wi-Fi connection mode.' An 'Apply' button is at the bottom left.

Wi-Fi Settings				
Connected Devices	Basic	Security	ACL	Firmware
Security Policy				
Security Type	WPA2-PSK			
WPA				
WPA Algorithm	C TKIP AES			
GTK	GCM (1000-95400)			
Password	1107044 (6-63 character)			
<small>The WPA2 password should not contain personal and private information. Because this password will be released to other WPA2 users to establish WPA2 connection. And users can also get it from the device display while connecting on a Wi-Fi connection mode.</small>				
Apply				

The security modes are described below:

NONE: In this mode, no password is required.

WEP: The WLAN clients who have the same key with wireless gateway can pass the authentication and access the wireless network.

WPA-PSK: WPA Pre-Shared Key, Enter the Pre-Shared key as a plain text (ASCII) pass-phrase of at least 8 characters.

WPA2-PSK: A securer version of WPA with implementation of the 802.11i standard.

WPA-PSK/WPA2-PSK: Apply both the WPA-PSK and WPA2-PSK scheme.

If the Security type is **WEP**, the following configuration page will appear:

Security Policy			
Security Type	[WEP]		
Authentication Type	[OPEN]		
Encrypt Type	[WEP-40]		

Wire Equivalence Protection (WEP)			
Default Key	[Key 1]		
Password	WEP Key 1 :	[234567890]	[Hex]
	WEP Key 2 :	[234567890]	[Hex]
	WEP Key 3 :	[234567890]	[Hex]
	WEP Key 4 :	[234567890]	[Hex]

The WPA2 password should not contain personal and private information. Because this password will be released to other WPA2 users to establish WPA2 connection. And users can also get it from the device display while powering on or in SSD information menu.

[Apply]

Authentication Type: Two types of authentication can be used: **OPEN** and **SHARE**. In the **OPEN** authentication type, the WLAN client (device) doesn't need to provide the correct credentials

to the Jetpack in order to connect to it. However, if the credentials are incorrect, data won't be transferred successfully between the WLAN clients and Jetpack. In effect, no authentication occurs. And in the **SHARE** authentication type, the WLAN client cannot connect to the Jetpack with the incorrect credentials.

Encrypt Type: Select the encrypt type(**WEP-40** and **WEP-104**).

Password: You can set at most four keys. Choose one of them as the default key, which is the only key in use at any given time. You must enter the default keys on the Wi-Fi client in order to connect to the Jetpack.

Select **Wi-Fi Settings > ACL** to access:

The screenshot shows the 'Wi-Fi Settings' interface with the 'ACL' tab selected. The 'ACL Setting' section includes a radio button for 'Accept' (selected) and a radio button for 'Deny'. Below this is a 'MAC Address' input field with a placeholder example: '00:00:00:00:00:00, eg. a0-a0-a0-a0-a0-a0'. A small note explains the policy: 'If the ACL policy is Deny, the user in MAC list can't connect to this device. If the ACL policy is Accept, the user in MAC list can connect to this device. You can allow or refuse other's user according to different ACL policy.' There is an 'Apply' button. Below the settings is a 'MAC List' section with a table header: 'No.', 'MAC Address', 'Policy', and 'Delete'. The table is currently empty. There is a 'Delete' button at the bottom of the table area.

No.	MAC Address	Policy	Delete
-----	-------------	--------	--------

If the ACL(**Access Control List**) policy is **Deny**, the user in MAC list can't connect to this device. If the ACL policy is **Accept**, the user in MAC list can connect to this device. You can allow or refuse a Wi-Fi user according to different ACL policy.

Select **Wi-Fi Settings > Firmware** to display the Wlan Chip Firmware Version.



Firewall

After logging in, select **Firewall > IP/Port Filtering** to access:



If you select **Enable**, the filter settings will appear:

Basic Settings

IP/Port Filtering

Enable

Default Policy – The packet that match with any rule would be:

Dropped

Apply

IP/Port Filter Settings

Source IP Address

(000.000.000.000, eg. 10.120.80.1)

Source Submask

(/Nn accept or drop IP address in network segment calculated by source IP address and source submask.)

Protocol

NONE

The maximum rule count is 5.

Add

Current IP/Port filtering rules in system:

No.	Source IP Address	Source Submask	Protocol	Source Port Range/Type	Dest Port Range/Code	Action	Delete
-----	-------------------	----------------	----------	------------------------	----------------------	--------	--------

Delete

Default Policy: Set how to handle the packet if any of the rules matches.

Source IP Address: Set the source IP address that will be filtered.

Source Submask: Set the source submask that will be filtered.

Protocol: Set which protocol will be used for filtering.

Source Port Range: Set the source port numbers that will be filtered.

Dest Port Range: Set the destination port numbers that will be filtered.

How to add a new rule:

1. Select **Enable** and click **Apply** in the **Basic Settings** area.
 2. Input the detail information in the **Ip/Port Filtering** area.
 3. Click **Add** in the **Ip/Port Filtering** area.
- In the **Current IP/Port filtering rules** area, click **Delete** to delete the rules that you selected.

Select **Firewall > Port Forwarding** to access:

Firewall IP/Port Filtering **Port Forwarding** VPN

Virtual Server Settings

Virtual Server Settings Disable ▾

Apply

If you select **Enable**, the Virtual Server Settings will appear:

Virtual Server Settings

Virtual Server Settings Enable ▾

IP Address (000.000.000.000, eg. 192.168.1.101/80)

Port

Protocol TCP+UDP ▾

The maximum rule count is 10.

Apply

Current Virtual Servers in system:

No.	IP Address	Port	Protocol	Delete
-----	------------	------	----------	--------

Delete

IP Address: Set IP address for the virtual server.

Port: Set port number for the virtual server.

Protocol: Set the protocol for the virtual server.

How to add a virtual server:

1. Select **Enable** and input the detailed information in the **Virtual Server Settings** area.
2. Click **Apply** to save your settings.

In the **Current Virtual Servers** area, click **Delete** to delete the virtual servers that you selected.

Select **Firewall > VPN** to enable/disable the VPN Connection.

Firewall IP Port Filtering Port Forwarding **VPN**

VPN Connection

IPSec VPN Pass Through ☒ Enable ☐ Disable

Apply

Advanced

After logging in, select **Advanced > Status** to display the system information.

Advanced **Status** Statistics Restore/Reboot Sound Alert Config File

Status

Network Selection Mode	Global Mode
IMEI	9900005800029180
Wireless Access Module Software Version	VZW_EuF000V1.0.2012
System Up Time	2 hours, 41 mins, 15 secs

Select **Advanced > Statistics** to check your WAN usage. Click **Refresh** to update the usage, and click **My Verizon** to visit Verizon website to check your monthly total data.

The screenshot shows the 'Advanced' settings menu with 'Statistics' selected. Under the 'WAN' section, there are four rows of statistics, all showing '0' values: WAN Receive data rate (0 bits/s), WAN Transmit data rate (0 bits/s), WAN Total Data Received (0 KB), and WAN Total Data Transmitted (0 KB). A small note below states: 'Attention: WAN usage (as counted by the device on the Statistics page) is estimated and may not be accurate for billing purposes.' A 'Refresh' button is located below the statistics. At the bottom, under 'Monthly Total Data', there is a 'Visit Verizon Website' link and a 'My Verizon' button.

Advanced	
Status	Statistics
WAN	
WAN Receive data rate	0 bits/s
WAN Transmit data rate	0 bits/s
WAN Total Data Received	0 KB
WAN Total Data Transmitted	0 KB
Attention: WAN usage (as counted by the device on the Statistics page) is estimated and may not be accurate for billing purposes.	
Refresh	
Monthly Total Data	
Visit Verizon Website	My Verizon

Select **Advanced > Restore&Reboot** to restart your device, or restore your device to the factory default settings.

The screenshot shows the 'Advanced' settings menu with 'Restore&Reboot' selected. There are two main options: 'Reboot device' with a 'Reboot' button, and 'Restore to Factory Default' with a 'Restore' button.

Advanced	
Status	Statistics
Restore&Reboot	
Reboot device	Reboot
Restore to Factory Default	Restore

Select **Advanced > Sound Alert** to turn on/off the sound alert.

The screenshot shows the 'Advanced' settings menu with 'Sound Alert' selected. There is a 'Sound Alert' toggle switch currently set to 'Off'. Below the toggle is an 'Apply' button.

Advanced	
Status	Statistics
Sound Alert	
Sound Alert	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Apply	

Select **Advanced > Config File** to import/export the configuration file of the device.

The screenshot shows a web interface with a top navigation bar containing tabs: 'Advanced', 'Status', 'Statistics', 'Restored&Reboot', 'Sound Alert', and 'Config file'. The 'Config file' tab is active. Below the navigation bar, there is a section titled 'Import' with a 'Path' input field and a 'Browse...' button. A note below states: 'It will modify the configuration of this device to import configuration file. Please make sure the parameters in the configuration file are correct.' Below this note is an 'Apply' button. Underneath the 'Import' section is an 'Export' section with an 'Export file' button.

NOTE: It will modify the configuration of this device to import configuration file. Please make sure the parameters in the configuration file are correct.

SMS

This function allows you to view, save, send and receive text messages. After logging in, select **Message** to perform the related operations.

The screenshot shows a web interface with a top navigation bar containing tabs: 'Message', 'Inbox', 'Outbox', 'Drafts', and 'New Message'. The 'Message' tab is active. Below the navigation bar, there is a section titled 'Inbox'. Below this section is a table with columns: 'No', 'Number', 'Date', and 'Contents'. Below the table are five buttons: 'Delete', 'Delete All', 'View', 'Select All', and 'cancel'.


Navigating the Device

Slide the **Power Switch** to the **ON** position to turn on the device. The screen lights up. After the initialization of the device, the SSID and default password will display on the screen. Press the **OK button**, the following icons will appear:



NOTE: Devices and software are constantly evolving — the screen images and icons displayed are for reference only and may differ from your device.

WAN Info

Select  and press the **OK button** to check the WAN information. Use the **UP** and **DOWN buttons** to scroll to the desired menu. Press the **OK button** to view information about the following WAN settings:


Network Provider: Displays the name of your service provider.

Network Type: Displays your network type.

Roam: Displays whether or not your device is roaming.

WAN Connection: Check your connection status.

WLAN Info

Select  using the **UP** and **DOWN buttons** and press the **OK button** to check the WLAN information. Use the **UP** and **DOWN buttons** to scroll to the desired menu. Press the **OK button** to view information about the following WLAN settings:


SSID Information: Displays the SSID and password.

Connected Device: Displays the information about connected Wi-Fi devices.

Start WPS: Launch the Wi-Fi Protection Setup.

Read the prompt on the display and refer to the **Usage of WPS** chapter.

Settings

Select  using the **UP** and **DOWN buttons** and press the **OK button** to check the settings. Use the **UP** and **DOWN buttons** to scroll to the desired menu. Press the **OK button** to view information about the following settings:

Device Info: Displays the basic information about your device: **Phone Number**, **SIM ID**, **MEID**, **SW Version** and **RSSI**.

Mobile Network: Use the **UP** and **DOWN buttons** to scroll to the desired menu. Press the **OK button** to view the following operations related to your network:

- **Data Connection:** Connect or disconnect the WAN connection.
- **Network Select:** Choose the desired network from the following options: **Global Mode**, **LTE/CDMA Mode**, and **GSM Mode**.

Wi-Fi: Press the **OK button** to select Proceed to adjusting your Wi-Fi settings or **Back** to return to the previous menu.

The following Wi-Fi settings appear when you

select **Proceed**:

- **Wi-Fi Network Mode:** Change the Wi-Fi standard.(It is recommended that you do not change the default setting, **11 b/g**.)
- **SSID Broadcast:** Enable or disable discovery mode, allowing your device to be found by other Wi-Fi compatible devices.
- **AP Isolation:** Enable or Disable the connection between connected Wi-Fi devices communicating with each other.
- **Channel:** Choose the appropriate channel frequency to optimize the performance and coverage of your wireless network.
- **MAX Connections:** Choose the maximum number of Wi-Fi devices that can be connected to your device simultaneously.


Web User Interface: Indicates you how to access the web-based Configuration Page for your device.

Software Update: Select **Check New** to check for new software.

Button Lock: Set the lock duration for your device by selecting on of the following options: **30Secs/15Secs/Never**.

Sound Alert: Mute or unmute the system alert.

Message


Select  using the **UP** and **DOWN buttons** and press the **OK button** to check messages. Select one of the following options:

New Messages: Displays your unread messages.

Inbox: Displays the messages in your inbox.

Usage of WPS

If your client device supports WPS, you need not input the password manually after WPS has been available. Please do the following:

1. Start up your Jetpack.
2. Launch the client device.
3. Select the icon , and then choose **Start WPS** to enable the WPS function of your Jetpack.
4. Enable the WPS function of the client.

NOTE: For the detailed operations about the client, please refer to the client's instruction.

Glossary

3G: Third Generation. 3G refers to the third generation of mobile telephony technology.

4G: Fourth Generation. 4G refers to the third generation of mobile telephony technology.

802.11(b, g, n): A set of WLAN communication standards in the 2.4, 3.6 and 5 GHz frequency bands.

Broadband: High-capacity high-speed, transmission channel with a wider bandwidth than conventional modem lines. Broadband channels can carry video, voice, and data simultaneously.

DHCP: Dynamic Host Configuration Protocol. Software found in servers and routers that automatically assigns temporary IP addresses to clients logging into an IP network.

DHCP Server: A server or service with a server that assigns IP addresses.

Firewall: A hardware or software boundary that protects a network or single computer from unwanted outside traffic.

Firmware: A computer program embedded in an electronic device. Firmware usually contains operating code for the device.

Hotspot: A WiFi (802.11) access point or the area covered by an access point. Used for connecting to the Internet.

HTTP: Hypertext Transfer Protocol. An application-level protocol for accessing the World Wide Web over the Internet.

IEEE: Institute of Electrical and Electronics Engineers. An international technical/professional society that promotes standardization in technical disciplines.

LAN: Local Area Network. A type of network that lets a group of computers, all in close proximity (such as inside an office building), communicate with one another. It does not use common carrier circuits though it can have gateways or bridges to other public or private networks.

MAC Address: Media Access Control. A number that uniquely identifies each network hardware device. MAC addresses are 12-digit hexadecimal numbers. This is also known as the physical or hardware address.

Port: A virtual data connection used by programs to exchange data. It is the endpoint in a logical connection. The port is specified by the port number.

Port Forwarding: A process that allows remote devices to connect to a specific computer within a private LAN.

Port Number: A 16-bit number used by the TCP and UDP protocols to direct traffic on a TCP/IP host. Certain port numbers are standard for common applications.

Protocol: A standard that enables connection, communication, and data transfer between computing endpoints.

Router: A device that directs traffic from one network to another.

SIM: Subscriber Identification Module. Found in GSM network technology, the SIM is a card containing identification information for the subscriber and their account. The SIM card can be moved to different devices.

SMS: Short Messaging Service. Short text messages of generally no more than 140-160 characters sent and received by wireless devices.

SSID: Service Set Identifier. The name assigned to a WiFi network.

TCP/IP: Transmission Control Protocol/Internet Protocol. The set of communications protocols used for the Internet and other similar networks.

USB: Universal Serial Bus. A connection type for computing device peripherals such as a printer, mobile device, etc.

VPN: Virtual Private Network. A way to communicate through a dedicated server securely to a corporate network over the Internet.

WAN: Wide Area Network. A public network that extends beyond architectural, geographical, or political boundaries (unlike a LAN, which is usually a private network located within a room, building, or other limited area).

WEP: Wired Equivalent Privacy. An IEEE standard security protocol for 802.11 networks. Superseded by WPA and WPA2.

Wi-Fi: Wireless Fidelity. Any system that uses the 802.11 standard developed and released in 1997 by the IEEE.

Wi-Fi Client: A wireless device that connects to the Internet via Wi-Fi.

WPA/WPA2: Wi-Fi Protected Access. A security protocol for wireless 802.11 networks from the Wi-Fi Alliance.

How to Get Help

Assistance is at your fingertips at **verizonwireless.com**. Customer Service is at your disposal at **1-800-922-0204** or in any Verizon Wireless Communications Store.

If you have questions about how to use ZTE mobile devices or your device needs repair services, please access to our support website, contact our services hotline or email for more information.

Website Address: **<http://www.zteusa.com/support/>**

Service Hotline: **877-817-1759** (9:00 am – 9:00 pm CST)

Service Email: devicesupport@zteusa.com

Health and Safety Information

General Guidelines

- Some electronic devices may be susceptible to electromagnetic interference. Locate the device away from TV set, radio and other electronic equipment to avoid electromagnetic interference.

- The device may interfere with medical devices like hearing aids and pacemakers. Consult a physician or the manufacturer of the medical device before using the device.
- Please keep yourself at least 20 centimeters away from the device.
- Do not use your device in dangerous environments such as oil terminals or chemical factories where there are explosive gases or explosive products being processed.
- Please use original accessories or accessories that are authorized by ZTE. Unauthorized accessories may affect the device performance, damage the device or cause danger to you.
- Do not attempt to dismantle the device. There are no user serviceable parts.
- Do not allow the device or accessories to come into contact with liquid or moisture at any time. Do not immerse the device in any liquid.
- Do not place objects on top of the device. This may lead to overheating of the device.
- The device must be used in ventilated environment.
- Do not expose the device to direct sunlight or store it in hot areas. High temperature can

shorten the life of electronic devices.

- Do not allow children to play with the device or charger.
- Use an antistatic cloth to clean the device. Do not use chemical or abrasive cleanser as these could damage the plastic case. Turn off your device before you clean it.
- Use the device within the temperature range of -10°C ~ $+35^{\circ}\text{C}$, and the storage temperature range is -20°C ~ $+60^{\circ}\text{C}$. The humidity range is 5%-90%.
- Do not use your device during a thunderstorm. Remove the charger from the mains socket.
- Do not take out your (U)SIM card unnecessarily. The (U)SIM card may be easily lost or it can be damaged by static electricity.
- Do not place the device alongside computer disks, credit cards, travel cards or other magnetic media. The information contained on the disks or cards may be affected by the device.
- Do not paint the device.
- Do not remove the device battery while the device is switched on.
- Take care not to allow metal objects, such as

coins or key rings, to contact or short circuit the battery terminals.

- Do not dispose of batteries in fire. The device's Li-ION batteries may be safely disposed of at a Li-ION recycling point. Follow local requirements for recycling.
- Do not put the device's battery in your mouth, as battery electrolytes are toxic.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, expose to fire, explosion or other hazard.
- Only use the battery for the system for which it is specified.
- Only use the battery with a charging system that has been qualified with the system per this standard. Use of an unqualified battery or charger may present a risk of fire, explosion, leakage, or other hazard.
- Do not short circuit a battery or allow metallic conductive objects to contact battery terminals.
- Replace the battery only with another battery that has been qualified with the system per this standard, IEEE-Std-1725-200x. Use of an

unqualified battery may present a risk of fire, explosion, leakage or other hazard.

- Promptly dispose of used batteries in accordance with local regulations.
- Battery usage by children should be supervised.
- Avoid dropping the device or battery. If the device or battery is dropped, especially on a hard surface, and the user suspects damage, take it to a service center for inspection.
- Improper battery use may result in a fire, explosion, or other hazard.
- Do not put a battery into a microwave oven, dryer or high-pressure container.
- Do not connect the battery directly into an electric outlet or cigarette lighter charger. Use only authorized chargers.
- Do not puncture the battery with a sharp object such as a needle.
- When the battery is disposed, be sure it is non-conducting by applying vinyl tape to the (+) and (-) terminals.
- Do not drop, throw, or subject the device to rough treatment.

- Stop using the battery if abnormal heat, odor, discoloration, deformation, or abnormal condition is detected during use, charge or storage.
- Do not use your device with a damaged or deformed battery.
- Do not solder the battery directly.
- Remove the battery whose life cycle has expired from equipment immediately.
- Remember to recycle: The cardboard packing supplied with this device is ideal for recycling.

Warnings: In the unlikely event of a battery leak, take care to keep the leakage away from your eyes and skin. If the leakage does come into contact with the eyes or skin, flush thoroughly with clean water and consult with a doctor.

Aircraft Safety

Switch off your device before the airplane takes off. In order to protect airplane's communication system from interference, it is never allowed to use the device when in flight. Get aircrew's permission if you want to use the device prior to take-off.

Hospital Safety

- Switch off your device and remove its battery in areas where device use is prohibited.
- Follow the instructions given by any respective medical facility regarding the use of Wireless devices on their premises.

Road Safety

- You must exercise proper control of your vehicle at all times. Give your full attention to driving.
- Observe all of the recommendations contained in your local traffic safety documentation.
- Please check if local laws and/or regulations restrict the use of wireless devices while driving.
- Switch off your device at a refueling point, such as a gas station, even if you are not refueling your own car.
- Do not store or carry flammable or explosive materials in the same compartment as the device.
- Electronic systems in a vehicle, such as anti-lock brakes, speed control and fuel injection systems are not normally affected by radio transmissions. The manufacturer of such

equipment may advise if it is adequately shielded from radio transmissions. If you suspect vehicle problems caused by the radio transmitter in the device, consult your dealer and do not switch on the device until your device has been checked by a qualified technician.

Vehicles Equipped with an Airbag

An airbag inflates with great force. Do not place objects, including either installed or portable wireless equipment, in the area over the airbag or in the airbag deployment area. If in-vehicle wireless equipment is improperly installed and the airbag inflates, serious injury could result.

Third Party Equipment

The use of third party equipment, cables or accessories, not made or authorized by ZTE, may invalidate the warranty of the device and also adversely affect the device's operation. For example, use only the ZTE charger supplied with the device.

Efficient Use

For optimum performance with minimum power consumption, do not cover the device with anything. Covering the device may cause the device to operate at higher power levels than needed, and may shorten the using time of the battery.

CTIA Requirements

- a. Do not disassemble or open crush, bend or deform, puncture or shred.
- b. Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, expose to fire, explosion or other hazard.
- c. Only use the battery for the system for which it is specified.
- d. Only use the battery with a charging system that has been qualified with the system per this standard. Use of an unqualified battery or charger may present a risk of fire, explosion, leakage, or other hazard.
- e. Do not short circuit a battery or allow metallic conductive objects to contact battery terminals.

- f. Replace the battery only with another battery that has been qualified with the system per this standard, IEEE-Std-1725-2006. Use of an unqualified battery may present a risk of fire, explosion, leakage or other hazard.
- g. Promptly dispose of used batteries in accordance with local regulations
- h. Battery usage by children should be supervised.
- i. Avoid dropping the phone or battery. If the device or battery is dropped, especially on a hard surface, and the user suspects damage, take it to a service center for inspection.
- j. Improper battery use may result in a fire, explosion or other hazard.

For those host devices that utilize a USB port as a charging source, the host device's user manual shall include a statement that the device shall only be connected to CTIA certified adapters, products that bear the USB-IF logo or products that have completed the USB-IF compliance program.

Radio Frequency (RF) Exposure

This device meets the government's requirements for exposure to radio waves.

This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government:

The exposure standard for wireless mobile devices employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit set by the FCC is 1.6W/kg. *Tests for SAR are conducted using standard operating positions accepted by the FCC with the device transmitting at its highest certified power level in all tested frequency bands. Although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. This is because the device is designed to operate at multiple power levels so as to use only the power required to reach the network. In general, the closer you are to a wireless base station antenna, the lower the power output.

The highest SAR value for the device as reported to the FCC is **1.39** W/kg (Body-worn measurements differ among device models, depending upon available enhancements and FCC requirements.)

While there may be differences between the SAR levels of various devices and at various positions, they all meet the government requirement.

The FCC has granted an Equipment Authorization for this device with all reported SAR levels evaluated as in compliance with the FCC RF exposure guidelines. SAR information on this device is on file with the FCC and can be found under the Display Grant section of <http://www.fcc.gov/oet/ea/fccid/> after searching on:

FCC ID: Q78-EUFI890

For body worn operation, this device has been tested and meets the FCC RF exposure guidelines for use with an accessory that contains no metal and the positions the handset a minimum of 1.5 cm from the body. Use of other enhancements may not ensure compliance with FCC RF exposure guidelines. If you do not use a body-worn accessory and are not holding the device at the ear, position the handset a minimum of 1.5 cm from your body when the device is switched on.

FCC Compliance

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.

Caution: Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

NOTE: 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.
- Consult the dealer or an experienced radio/TV technician for help.

Consumer Limited Warranty

ZTE (“Seller”) offers you a limited warranty that the enclosed product or products (the “Product”) will be free from defects in material and workmanship for a period that expires one year from the date of sale of the Product to you, provided that you are the original end-user purchaser of the Product and provided that your purchase was made from a supplier authorized by the Seller. Transfer or resale of a Product will automatically terminate warranty coverage with respect to that Product. This limited warranty is not transferable to any third party, including but not limited to any subsequent purchaser or owner of the Product. This limited warranty is applicable only to end users in the United States.

Seller will, at its sole and absolute discretion, either repair or replace a Product (for which Seller may use refurbished parts of similar quality and functionality) if found by Seller to be defective in material or workmanship, or if Seller determines that it is unable to repair or replace such Product, Seller will refund the purchase price for such Product, provided that the subject Product (i) is returned to a Seller authorized service center

within the one year warranty period, and (ii) is accompanied by a proof of purchase in the form of a bill of sale or receipted invoice which evidences that the subject Product is within the one year warranty period. After the one year warranty period, you must pay all shipping, parts and labor charges. In the event that the Product is deemed un-repairable or has been removed from the list of products supported by the Seller, you will only be liable for shipping and labor charges.

This limited warranty does not cover and is void with respect to the following: (i) any Product which has been improperly installed, repaired, maintained or modified; (ii) any Product which has been subjected to misuse (including any Product used in conjunction with hardware electrically or mechanically incompatible or used with accessories not approved by Seller), abuse, accident, physical damage, abnormal operation, improper handling, neglect, exposure to fire or liquid; (iii) any Product operated outside published maximum ratings; (iv) cosmetic damage; (v) any Product on which warranty stickers or Product serial numbers have been removed, altered, or rendered illegible; (vi) cost of installation, removal or reinstallation; (vii) signal reception

problems (unless caused by defects in material and workmanship); (viii) damage as a result of fire, flood, acts of God or other acts which are not the fault of Seller and which the Product is not specified to tolerate, including damage caused by mishandling, shipping and blown fuses; (ix) consumables (such as fuses); or (x) any Product which has been opened, repaired, modified or altered by anyone other than Seller or a Seller authorized service center.

USE ONLY SELLER APPROVED ACCESSORIES WITH SELLER DEVICES. USE OF ANY UNAUTHORIZED ACCESSORIES MAY BE DANGEROUS AND WILL INVALIDATE THE DEVICE WARRANTY IF SAID ACCESSORIES CAUSE DAMAGE OR A DEFECT TO THE DEVICE.

SELLER SPECIFICALLY DISCLAIMS LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, PUNITIVE, EXEMPLARY, AGGRAVATED, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE OF ANY KIND WHATSOEVER, INCLUDING BUT NOT LIMITED TO LOSS OF PROFITS, UNANTICIPATED BENEFITS OR REVENUE, ANTICIPATED PROFITS ARISING OUT

OF USE OF OR INABILITY TO USE ANY PRODUCT (FOR EXAMPLE, WASTED AIRTIME CHARGES DUE TO THE MALFUNCTION OF A PRODUCT) OR CONTRIBUTION OR INDEMNITY IN RESPECT OF ANY CLAIM RELATED TO A PRODUCT.

REPAIR OR REPLACEMENT OF A DEFECTIVE PRODUCT OR REFUND OF THE PURCHASE PRICE RELATING TO A DEFECTIVE PRODUCT, AS PROVIDED UNDER THIS WARRANTY, ARE YOUR SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THE LIMITED WARRANTY, AND SUBJECT TO THIS WARRANTY, THE PRODUCTS ARE APPROVED AND ACCEPTED BY YOU "AS IS". SELLER MAKES NO OTHER WARRANTIES, REPRESENTATIONS OR CONDITIONS OF ANY KIND, ORAL OR VERBAL, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OR ANY IMPLIED WARRANTY OR CONDITION ARISING OUT OF TRADE USAGE OR OUT OF A COURSE OF DEALING OR COURSE OF PERFORMANCE. NO DEALER, DISTRIBUTOR, AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE

ANY MODIFICATION OR ADDITION TO THIS WARRANTY.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, or allow limitations on how long an implied warranty lasts, so the above limitations or exclusions may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from jurisdiction to jurisdiction.

For warranty service information, please call the following telephone number: **1-877-817-1759, 1-212-444-0502** or return to the point of sale for the products.

