# ZTE Unite
# User Guide

## LEGAL INFORMATION

The guide 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: 07 23, 2011

# Contents

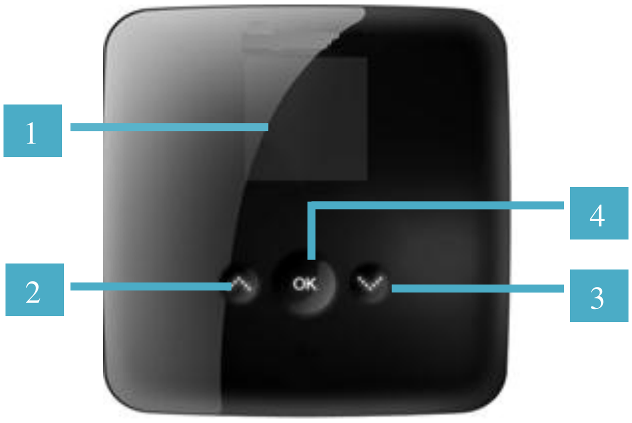
# Thank You For Choosing ZTE Unite

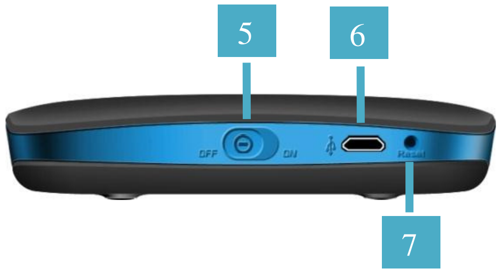
The ZTE Unite is a newly developed 4G LTE Mobile Hotspot, providing flexible LTE/EVDO/CDMA 1X access for users to enjoy high-speed Internet applications. When connected to the U.S. Cellular® 4G LTE Network, the ZTE Unite can support simultaneous connections with up to 10 Wi-Fi enabled devices. When connected in 2G or 3G mode the ZTE Unite can support simultaneous connections with 5 Wi-Fi enabled devices.

You're now connected to the blazingly fast, powerfully brilliant 4G 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.

# Getting Started

The following figure shows the appearance of your ZTE Unite, it is only for your reference. The actual device may be different.





| BUTTONS AND INTERFACE | DESCRIPTION |
|---|---|
| 1. SCREEN | Displays the menus and the status of your ZTE Unite. |
| 2. UP BUTTON | Scroll up to select the options. |
| 3. DOWN BUTTON | Scroll down to select the options. |
| 4. OK BUTTON | ● Confirm the highlighted selection.<br>● When the ZTE Unite button is locked, press once to light up the screen, and press again to unlock. |
| 5. POWER SWITCH | Power on/off your ZTE Unite. |
| 6. MICRO USB PORT | Charge your ZTE Unite. |
| 7. RESET BUTTON | Press and hold to restore your ZTE Unite to the factory default settings. |

## *Screen Indicators*

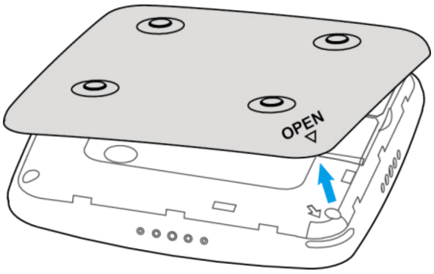
| Icon | Description | Icon | Description |
|---|---|---|---|
| 🔋 | Battery Status | 4G | 4G Network |
| 3G | 3G Network | 1X | CDMA 1X Network |
| ⇅ | Data Connected | 📶 | Signal Strength |
| 📶 | Roaming Signal Strength | ▲ | Roaming |
| X No SIM | No SIM Card Inserted | X Invalid SIM | PIN enabled SIM card or Incorrect SIM card inserted |
| X searching and 📶 | No Network Service | 10 | Number of current Wi-Fi connections |
| 🖵 | System Message | ! | New System Message |
| full | System Message Full | ⚙ | Settings |

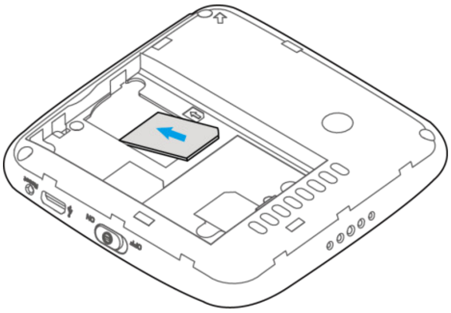
# *Hardware Installation*

## Installing the SIM Card

If you have not already done so, please follow these instructions for the installation of your new SIM Card which is in the package:

1. Remove SIM Card from the outer card, being careful not to touch the gold contacts.
2. Turn the power off. Remove the battery cover and take the battery out. Locate the SIM card slot. Hold the card so the writing on the back of the card is facing you and the gold contact points are properly aligned with the SIM Card slot.





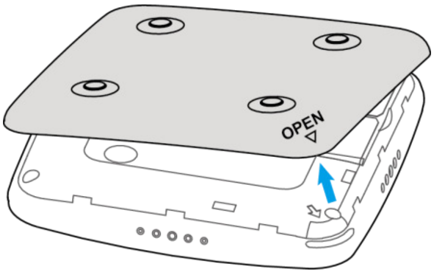
3. Insert SIM Card into the slot until it is fully inserted.

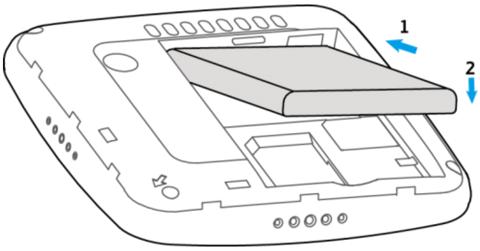
**ATTENTION!**

- The SIM Card MUST remain in your ZTE Unite when in use. Once the SIM card has been inserted into the ZTE Unite, do not remove!
- Do not bend or scratch your SIM Card. Avoid exposing your SIM Card to static electricity, water or dirt.
- If your SIM card is separated from the ZTE Unite or damaged, your ZTE Unite will not work. If you encounter any issue with your ZTE Unite, contact Customer Service at 1-888-944-9400 or visit your nearest U.S. Cellular® retail location.

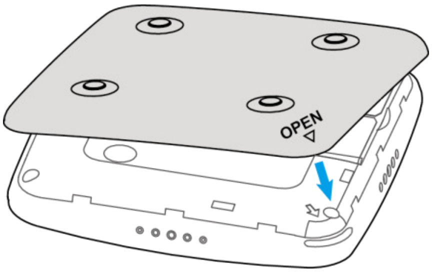
## Inserting and Charging the Battery

1. Use the thumb catch at the bottom of your ZTE Unite 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.

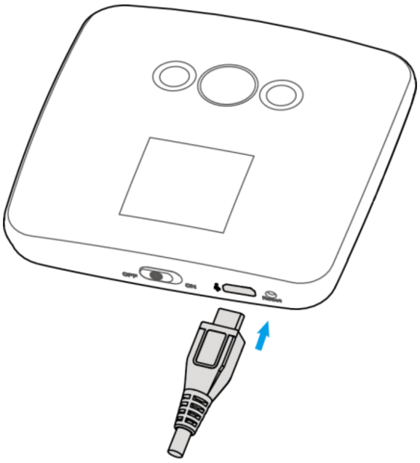




2. Place the battery cover over the battery compartment and press it downward until it clicks into place.



3. Your ZTE Unite comes with wall charger. To charge: Plug one end of the wall charger into an electrical outlet and the the other end into the ZTE Unite’s **MICRO USB PORT**.



**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 SIM Card

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

# Connecting to the Internet

With your ZTE Unite, a wireless Internet connection can always be at your fingertips.

## *Connecting Wi-Fi Enabled Devices To Your ZTE Unite*

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

The following should occur once you power on your ZTE Unite:

- Your ZTE Unite is powered as soon as you slide the **Power Switch** to **On** and the display lights up.
- Once your ZTE Unite 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.
- The Service (4G LTE, 3G, and 1X), Signal Strength 📶, and Data Connected ⇅ icons on your ZTE Unite indicate it is in service and ready to connect.

**Follow these Steps**:

1. Use your normal Wi-Fi application on your computer to establish a connection to your ZTE Unite.
2. Look for the network (SSID) named "**USCC-EuFi891**". There are XXXX digits unique to your ZTE Unite following the network (SSID) name displayed.
3. Click **Connect** and enter the default password printed beside the battery compartment of your ZTE Unite.

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

## *Accessing the Internet*

After successfully establishing the connection between your ZTE Unite and Wi-Fi clients, you can access the Internet in the **Auto Connect**, **Manual Connect** mode. The default mode is **Auto Connect**.

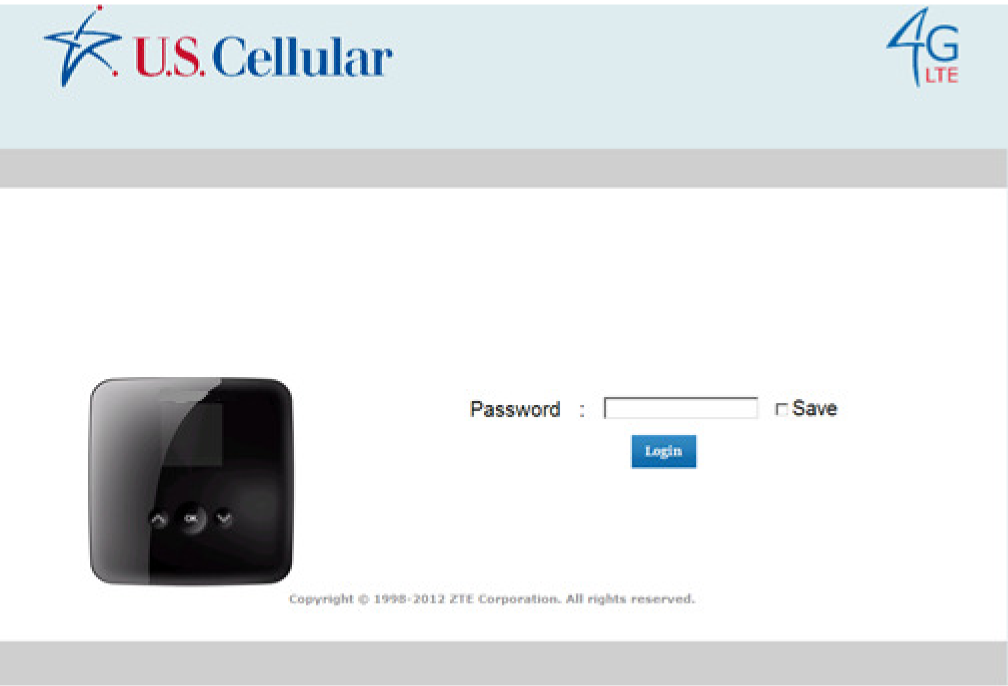
## Advanced Configuration

1. Make sure your computer is connected to the ZTE Unite.

2. Launch the Internet Browser and enter **http://uscc.hotspot** or **http://192.168.1.1** 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 (10.0 or later).

3. The login page appears as follow:



Password : □ Save

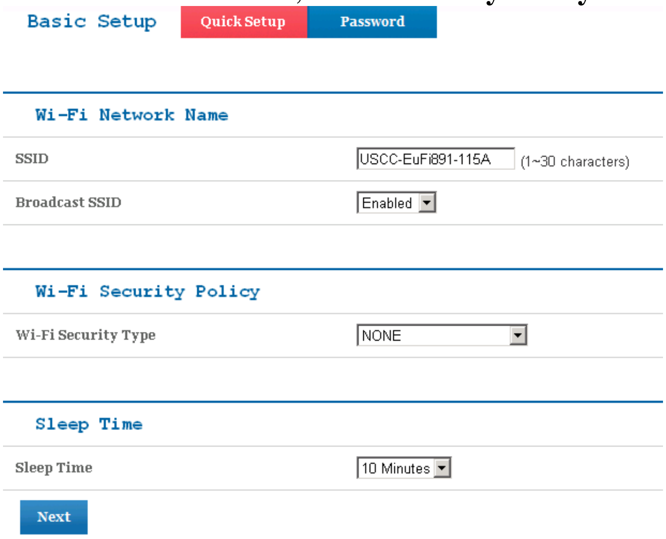
Copyright © 1998-2012 ZTE Corporation. All rights reserved.

Input the case-sensitive default password printed beside the battery compartment of your ZTE Unite, and then click **Login** to access the Web User Interface.

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

### *Basic Setup*

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



Wi-Fi Network Name

| | |
|---|---|
| SSID | USCC-EuFi891-115A (1~30 characters) |
| Broadcast SSID | Enabled |

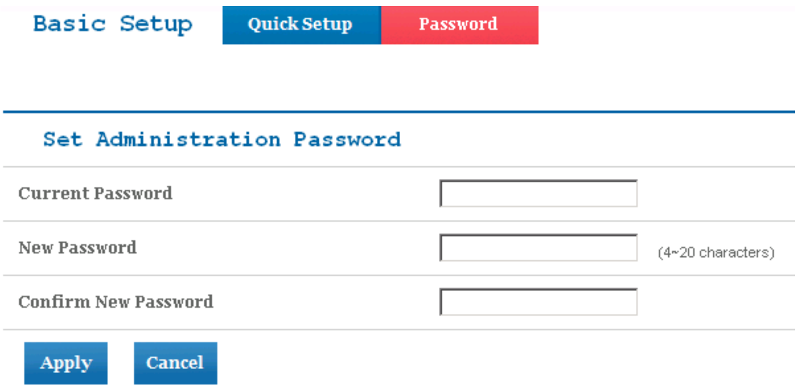
Wi-Fi Security Policy

| | |
|---|---|
| Wi-Fi Security Type | NONE |

Sleep Time

| | |
|---|---|
| Sleep Time | 10 Minutes |

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

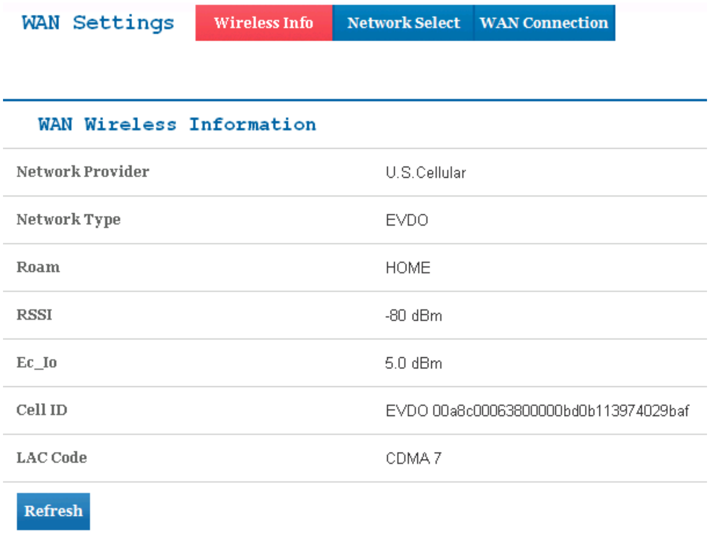


Set Administration Password

| | | |
|---|---|---|
| Current Password | | |
| New Password | | (4~20 characters) |
| Confirm New Password | | |

## WAN Settings

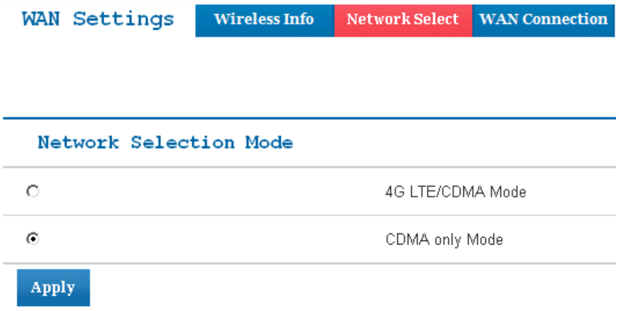
After logging in, select **WAN Settings > Wireless Info** to display the infomation of WAN wireless. Click **Refresh** to update the information.



WAN Wireless Information

| | |
|---|---|
| Network Provider | U.S.Cellular |
| Network Type | EVDO |
| Roam | HOME |
| RSSI | -80 dBm |
| Ec_Io | 5.0 dBm |
| Cell ID | EVDO 00a8c00063800000bd0b113974029baf |
| LAC Code | CDMA 7 |

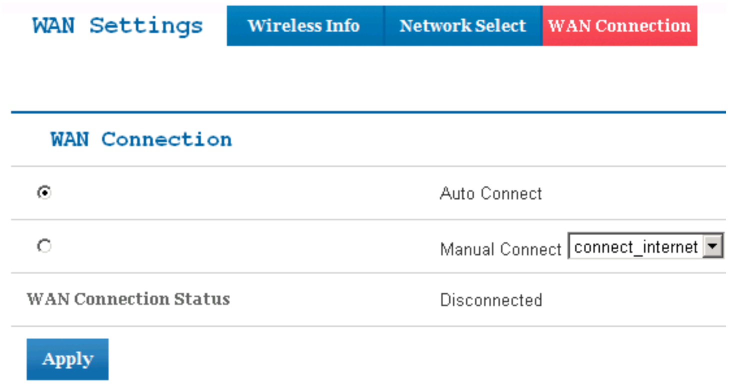
Select **WAN Settings > Network Select** to select the proper network mode, including **4G LTE/CDMA Mode** and **CDMA only Mode**. Click **Apply** to comfirm your choice.



Network Selection Mode

| | |
|---|---|
| ○ | 4G LTE/CDMA Mode |
| ● | CDMA only Mode |

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



WAN Connection

● Auto Connect

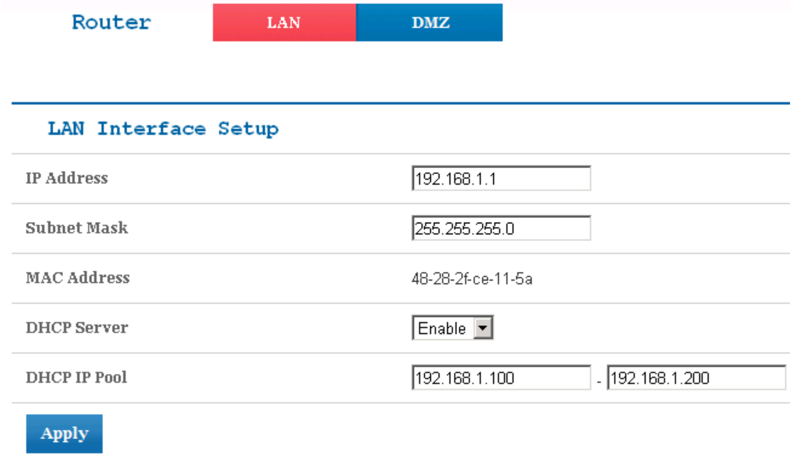
○ Manual Connect connect_internet

WAN Connection Status: Disconnected

**Auto Connect:** The ZTE Unite will connect to the Internet automatically when it is powered on.
**Manual Connect:** Connect/disconnect to the Internet connection manually.

## *Router*

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

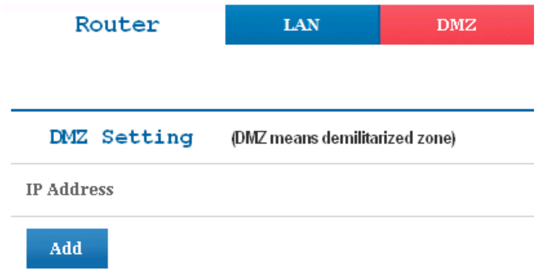


LAN Interface Setup

| | |
|---|---|
| IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| MAC Address | 48-28-2f-ce-11-5a |
| DHCP Server | Enable |
| DHCP IP Pool | 192.168.1.100 - 192.168.1.200 |

**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:



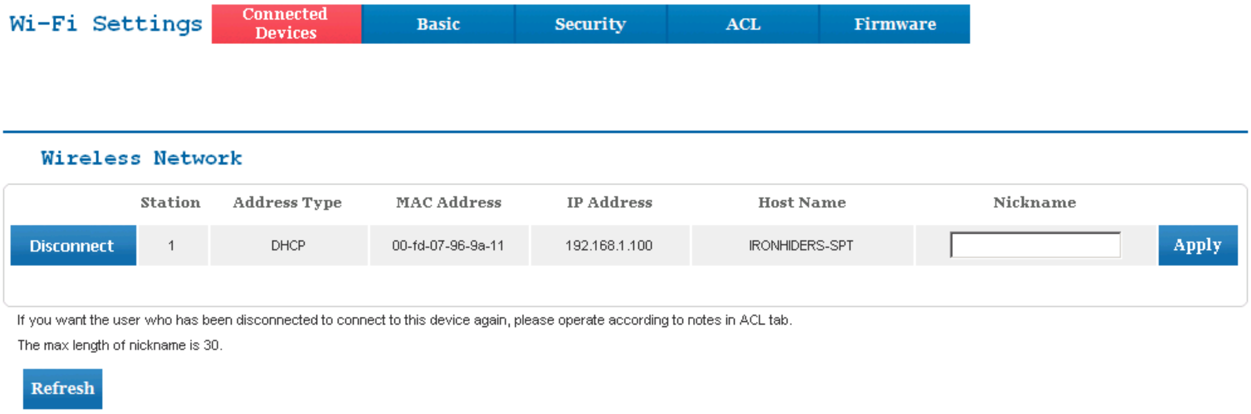
DMZ Setting (DMZ means demilitarized zone)

IP Address

**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 ZTE Unite.



Wireless Network

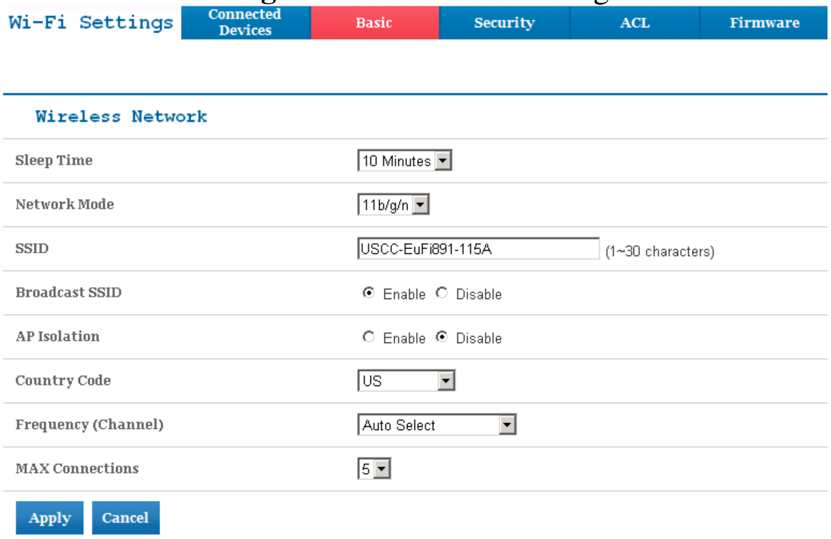
| | Station | Address Type | MAC Address | IP Address | Host Name | Nickname | |
|---|---|---|---|---|---|---|---|
| Disconnect | 1 | DHCP | 00-fd-07-96-9a-11 | 192.168.1.100 | IRONHIDERS-SPT | | Apply |

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.

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

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



Wireless Network

| | |
|---|---|
| Sleep Time | 10 Minutes |
| Network Mode | 11b/g/n |
| SSID | USCC-EuFi891-115A (1~30 characters) |
| Broadcast SSID | ● Enable ○ Disable |
| AP Isolation | ○ Enable ● Disable |
| Country Code | US |
| Frequency (Channel) | Auto Select |
| MAX Connections | 5 |

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

**Network Mode:** If all of the wireless devices connect with the ZTE Unite 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 ZTE Unite 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.

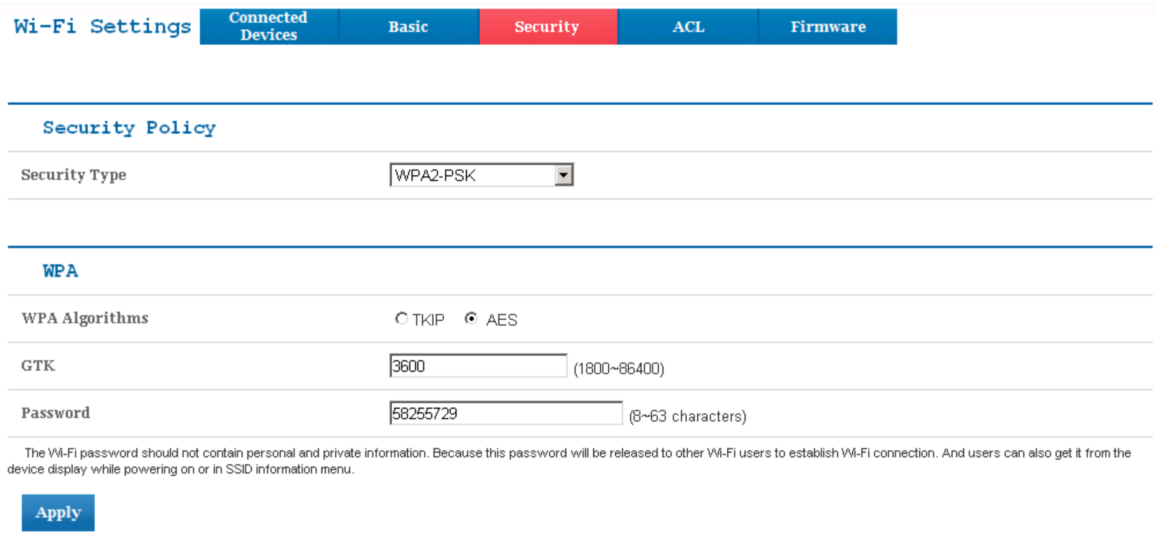
**Country Code:** Choose the right country code.

**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 ZTE Unite simultaneously.

Click **Apply** to save your settings.

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



Security Policy

Security Type: WPA2-PSK

WPA

WPA Algorithms: ○ TKIP ● AES

GTK: 3600 (1800~86400)

Password: 58255729 (8~63 characters)

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

The security modes are described below:

**NONE:** In this mode, no password is required.

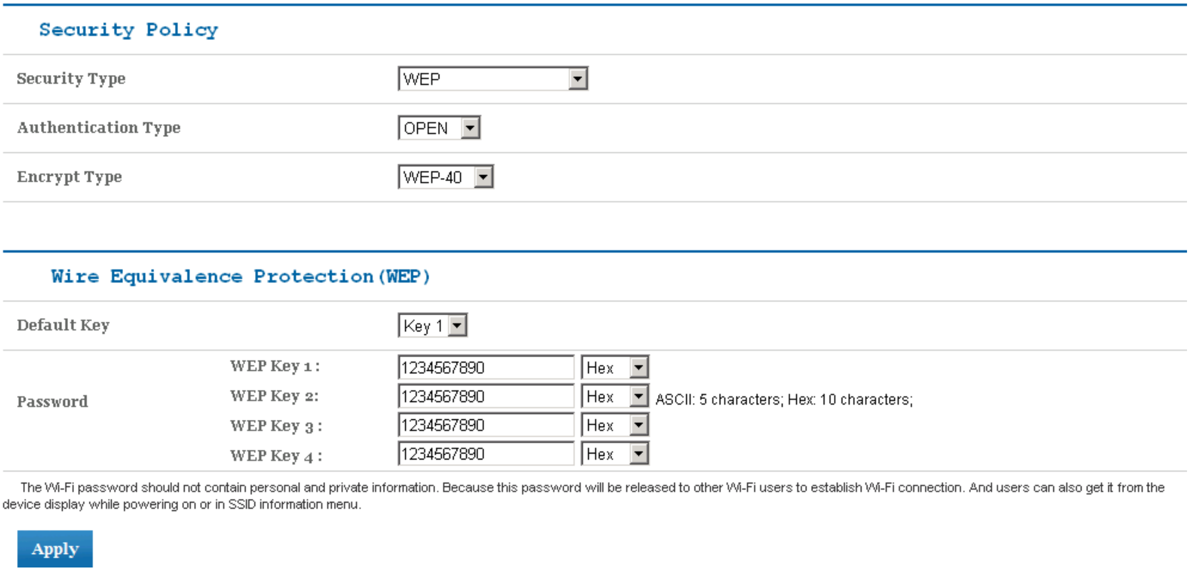
**WEP:** The WLAN clients who have the same key with wireless gateway can pass the authentication and access the wireless network.

**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 : | 1234567890 | Hex |
| WEP Key 2: | 1234567890 | Hex |
| WEP Key 3 : | 1234567890 | Hex |
| WEP Key 4 : | 1234567890 | Hex |

ASCII: 5 characters; Hex: 10 characters;

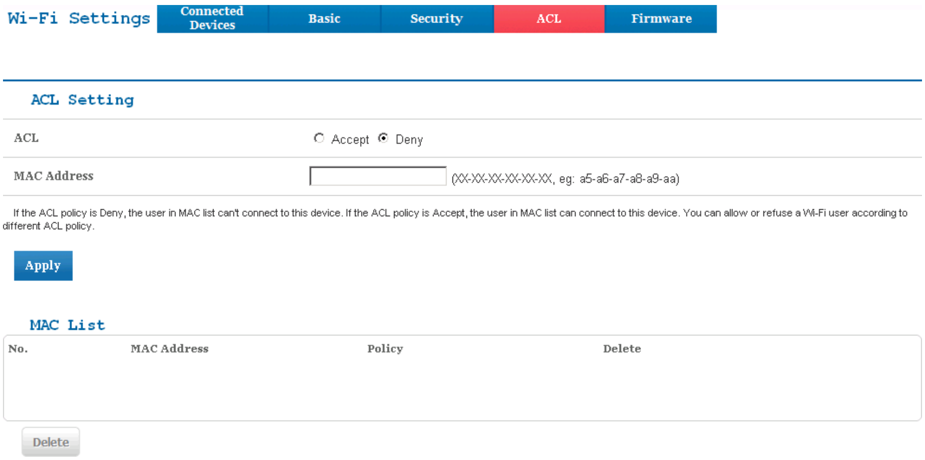
The Wi-Fi password should not contain personal and private information. Because this password will be released to other Wi-Fi users to establish Wi-Fi connection. And users can also get it from the device display while powering on or in SSID information menu.

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

**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 ZTE Unite.

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



ACL Setting

| | |
|---|---|
| ACL | ○ Accept ● Deny |
| MAC Address | (XX-XX-XX-XX-XX-XX, eg: a5-a6-a7-a8-a9-aa) |

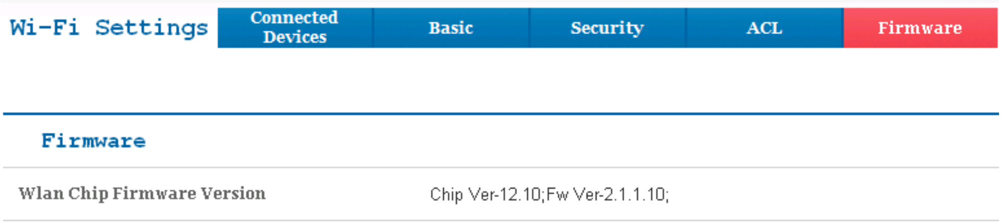
If the ACL policy is Deny, the user in MAC list can't connect to this device. If the ACL policy is Accept, the user in MAC list can connect to this device. You can allow or refuse a Wi-Fi user according to different ACL policy.

MAC List

| 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 theWlan Chip Firmware Version.

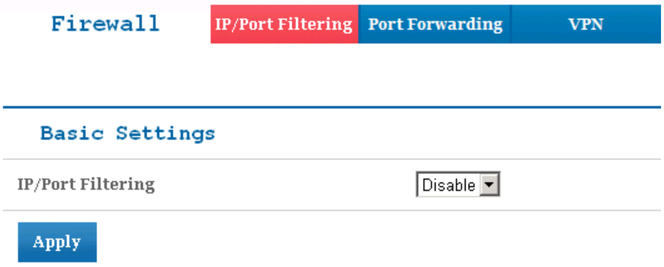


Firmware

| | |
|---|---|
| Wlan Chip Firmware Version | Chip Ver-12.10;Fw Ver-2.1.1.10; |

## *Firewall*

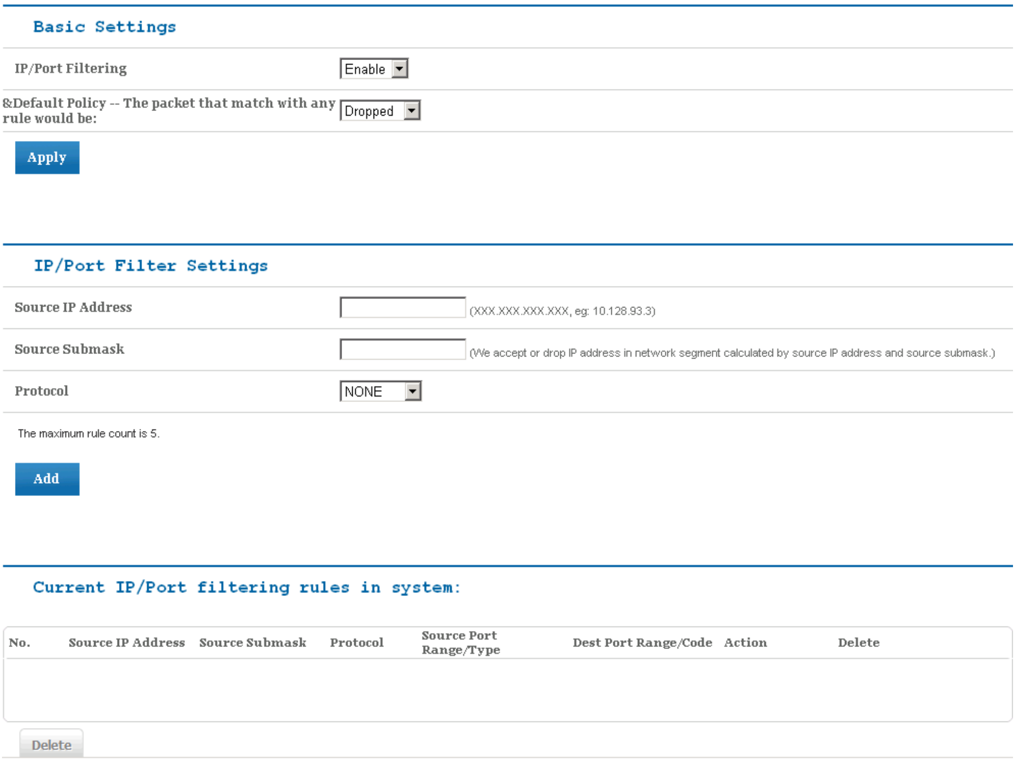
After logging in, select **Firewall > IP/Port Filtering** to access:



Basic Settings

| | |
|---|---|
| IP/Port Filtering | Disable |

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 |

IP/Port Filter Settings

| | |
|---|---|
| Source IP Address | (XXX.XXX.XXX.XXX, eg: 10.128.93.3) |
| Source Submask | (We accept or drop IP address in network segment calculated by source IP address and source submask.) |
| Protocol | NONE |

The maximum rule count is 5.

Current IP/Port filtering rules in system:

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

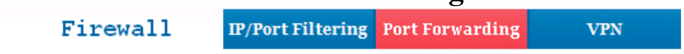
**Default Policy:** Set how to handle the packet if any of the rules matches.
**Source IP Address:** Set the source IP address that will be filtered.
**Source Submask:** Set the source submask that will be filtered.
**Protocol:** Set which protocol will be used for filtering.
**Source Port Range:** Set the source port numbers that will be filtered.
**Dest Port Range:** Set the destination port numbers that will be filtered.

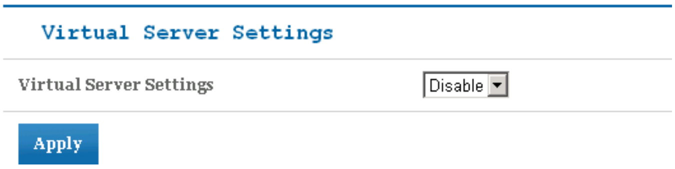
**How to add a new rule:**

1. Select **Enable** and click **Apply** in the **Basic Settings** area.
2. Input the detail information in the **Ip/Port Filter Settings** area.
3. Click **Add** in the **Ip/Port Filtering Settings** area.

In the **Current IP/Port filtering rules in system** area, click **Delete** to delete the rules that you selected.

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

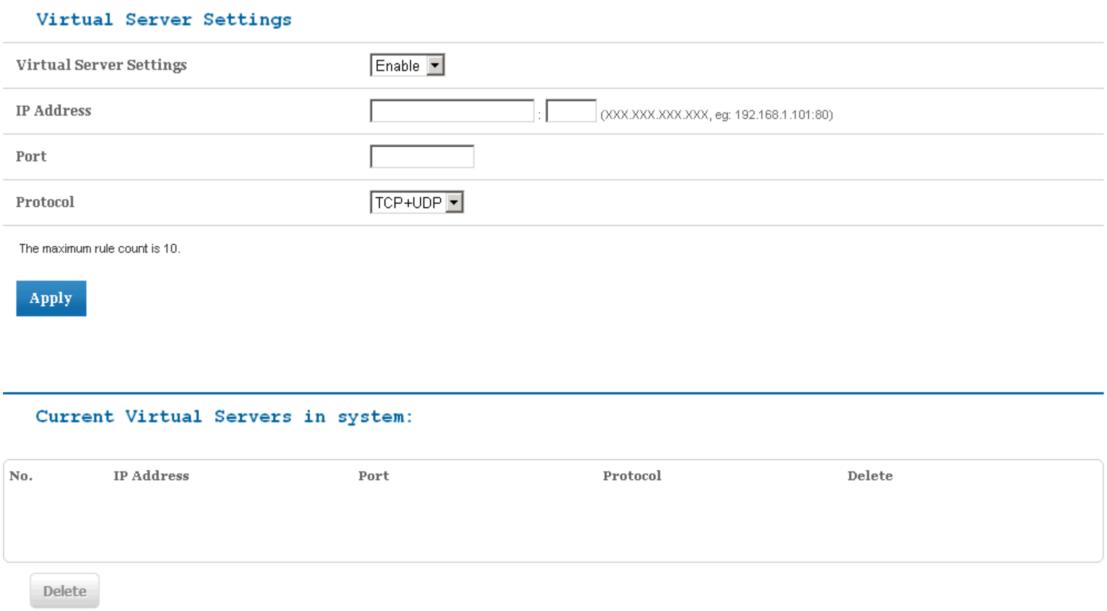




Virtual Server Settings

| | |
|---|---|
| Virtual Server Settings | Disable |

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



Virtual Server Settings

| | |
|---|---|
| Virtual Server Settings | Enable |
| IP Address | : (XXX.XXX.XXX.XXX, eg: 192.168.1.101:80) |
| Port | |
| Protocol | TCP+UDP |

The maximum rule count is 10.

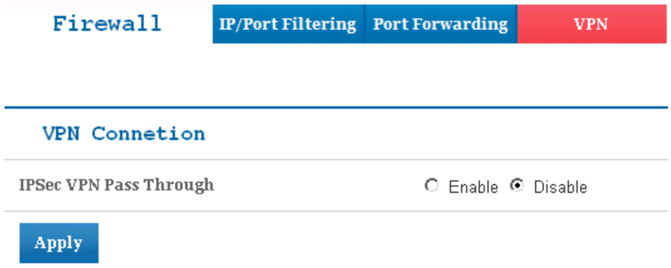
Current Virtual Servers in system:

| No. | IP Address | Port | Protocol | 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 in system** area, click **Delete** to delete the virtual servers that you selected.

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

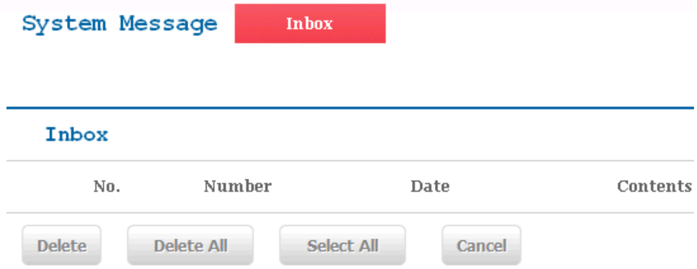


VPN Connetion

IPSec VPN Pass Through ○ Enable ● Disable

## *SYS Message*

After logging in, select **SYS Message** to view or delete your messages stored in the **Inbox**.

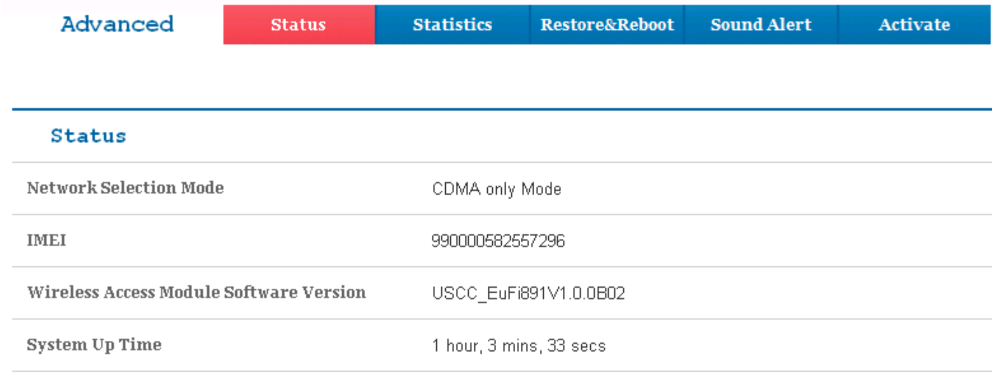


Inbox

| No. | Number | Date | Contents |
|---|---|---|---|

## *Advanced*

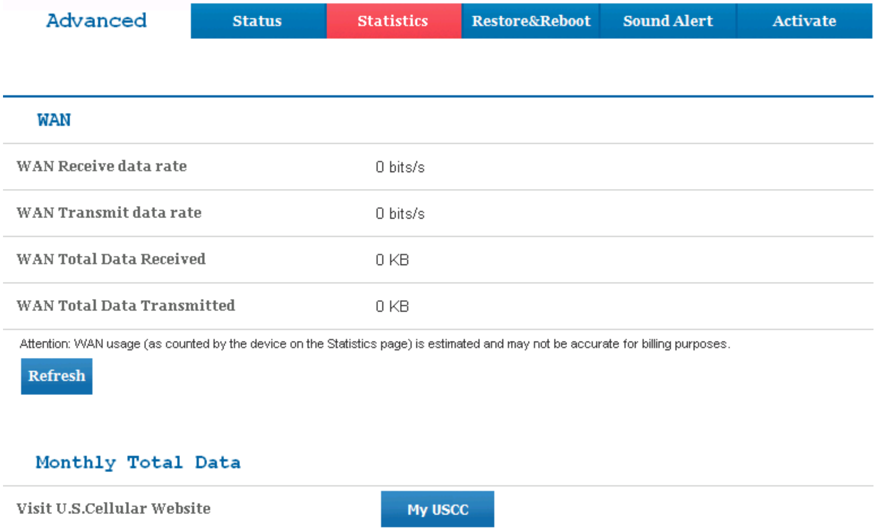
After logging in, select **Advanced > Status** to display the system information.



Status

| | |
|---|---|
| Network Selection Mode | CDMA only Mode |
| IMEI | 990000582557296 |
| Wireless Access Module Software Version | USCC_EuFi891V1.0.0B02 |
| System Up Time | 1 hour, 3 mins, 33 secs |

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



WAN

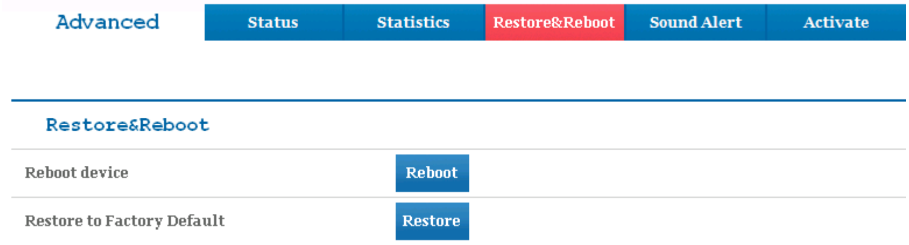
| | |
|---|---|
| WAN Receive data rate | 0 bits/s |
| WAN Transmit data rate | 0 bits/s |
| WAN Total Data Received | 0 KB |
| WAN Total Data Transmitted | 0 KB |

Attention: WAN usage (as counted by the device on the Statistics page) is estimated and may not be accurate for billing purposes.

Monthly Total Data

Visit U.S.Cellular Website

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

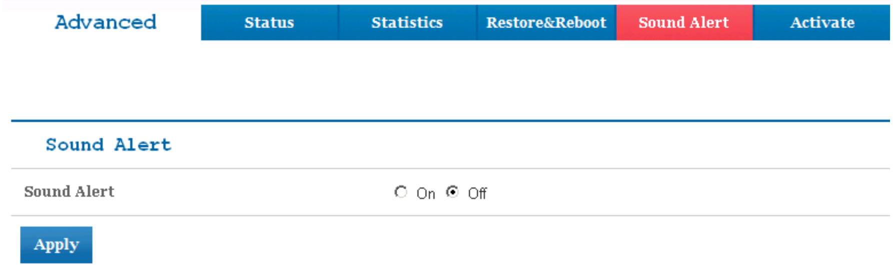


Restore&Reboot

Reboot device

Restore to Factory Default

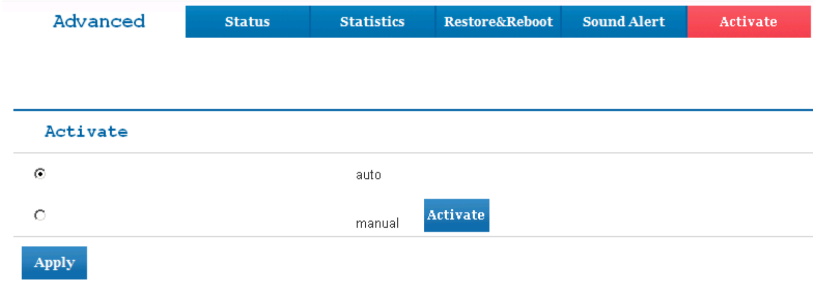
Select **Advanced > Sound Alert** to turn on/off the sound alert.



Sound Alert

Sound Alert ○ On ● Off

Select **Advanced > Activate** to choose how the SIM card is activated. You can either activate it once ZTE Unite is powered on, or activate manually by clicking the **Activate** button.



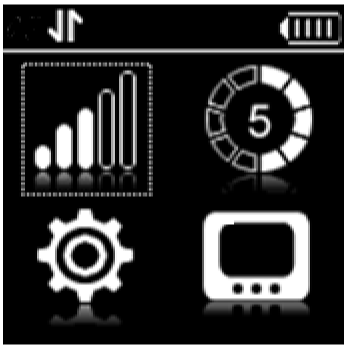
Activate

● auto

○ manual

## Navigating the Device

Slide the **Power Switch** to the **ON** position to turn on the ZTE Unite. The screen lights up. After the initialization of the ZTE Unite, 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 ZTE Unite is roaming.
- **WAN Connection:** Check your connection status.

### *WLAN Info*

Select ⑤ using the **UP** and **DOWN buttons** and press the **OK button** to check the following information. Use the **UP** and **DOWN buttons** to scroll to the desired menu. Press the **OK button** to view information 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 following information. Use the **UP** and **DOWN buttons** to scroll to the desired menu. Press the **OK button** to view information settings:

- **Device Info:** Displays the basic information about your device: **Phone Number**, **SIM ID**, **MEID**, **SW Version**, **PRI Version** and **RSSI**.
- **Data Connection:** Connect or disconnect the WAN connection.
- **Data Roaming:** Enable or disable the WAN connection when your ZTE Unite is roaming.

- **Network Select:** Choose the desired network from the following options: **4G LTE/CDMA Mode** and **CDMA Only 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 defualt setting, **11 b/g/n**.)
- ➢ **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 Station Number:** 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 ZTE Unite.
- **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.

## *System 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 already 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 ZTE Unite.
2. Launch the client device.
3. Select the icon ⚙, and then choose Start WPS to enable the WPS function of your ZTE Unite.
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 Wi-Fi (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.

**SSID:** Service Set IDentifier. The name assigned to a Wi-Fi 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.

# 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 °C, and the storage temperature range is -20 °C ~ +60 °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 SIM card unnecessarily. The 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.

## *Device Heating*

Do not use the device in an enclosed environment or where heat dissipation is poor. Prolonged work in such space may cause excessive heat and raise ambient temperature, which may lead to automatic shutdown of the device for your safety. In the case of such event, cool the device in a well-ventilated place before turning on for normal use.

## *Faulty and Damaged Products*

- Do not attempt to disassemble the device or its accessory.
- Only qualified personnel must service or repair the device or its accessory.
- If your device or its accessory has been submerged in water, punctured, or subjected to a severe fall, do not use it until you have taken it to be checked at an authorized service centre.

## *Explosive environments*

### Petrol stations and explosive atmospheres

- In locations with potentially explosive atmospheres, obey all posted signs to turn off wireless mobile phones such as your phone or other radio equipment.
- Areas with potentially explosive atmospheres include fuelling areas, below decks on boats, fuel or chemical transfer or storage facilities, areas where the air contains chemicals or particles, such as grain, dust, or metal powders.

### Blasting Caps and Areas

Turn off your mobile phone or wireless device when in a blasting area or in areas posted turn off “two-way radios” or “electronic devices” to avoid interfering with blasting operations.

## *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.

## *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 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 poser required to reach the network. In general, the closer you are to a wireless base station antenna, the lower the power output.

The device was tested according to FCC RF exposure procedures to address hand and near-body exposure conditions, and the highest SAR value as reported to the FCC is 1.33 W/kg

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 www.fcc.gov/oet/ea/fccid after searching on FCC ID: **Q78-EUFI891**.

This device has been tested and meets the FCC RF exposure guidelines.

## *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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

●The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## Consumer Limited Warranty

Personal Communications Devices, LLC (the "Company") warrants to the original retail purchaser of this cellular handset or wireless device (Product), that should this Product or any part thereof during normal consumer usage and conditions, be proven defective in material or workmanship that results in the Product's failure within the first twelve (12) month period from the date of purchase (proof of purchase required), such defect(s) will be repaired or replaced (with new or rebuilt parts) at the Company's option, without charge for parts or labor directly related to the defect(s).

The antenna, keypad, display, rechargeable battery and battery charger, if included with the Product, are similarly warranted for twelve (12) months from the date of purchase.

This Warranty extends only to consumers who purchase the product in the United States or Canada and it is not transferable or assignable.

This Warranty does not apply to:

(a) Product subjected to abnormal use or conditions, accident, mishandling, neglect, unauthorized alteration, misuse, improper installation or repair or improper storage;

(b) Product whose mechanical serial number or electronic serial number has been removed altered or defaced;

(c) Damage from exposure to moisture, humidity, excessive temperatures or extreme environmental conditions;

(d) Damage resulting from connection to, or use of any accessory or other product not approved or authorized by the Company;

(e) Defects in appearance, cosmetic, decorative or structural items such as framing and non-operative parts;

(f) Product damaged from external causes such as fire, flooding, dirt, sand, weather conditions, battery leakage, blown fuse, theft or improper usage of any electrical source;

(g) Product subjected to unauthorized modifications to the software of the Product or to the Product itself;

(h) Product subjected to the unauthorized opening or repair of the Product;

(i) Product subjected to hacking, password-mining, jail breaking, the unlocking of the boot loader using the fast boot program or the tampering with or short-circuiting of the battery; or

(j) Product that has been modified to alter functionality or capability of the Product without the written permission of the Company.

The Company disclaims liability for removal or reinstallation of the Product, for geographic coverage, for inadequate signal reception by the antenna or for communications range or operation of the cellular system as a whole.

When sending your wireless device to the Company for repair or service, please note that any personal data or software stored on the Product may be inadvertently erased or altered. Therefore, we strongly recommend you make a back up copy of all data and software contained on your Product before submitting it for repair or service. This includes all contact lists, downloads (i.e. third-party software applications, ringtones, games and graphics) and any other data added to your Product. In addition, if your Product utilizes a SIM or Multimedia card, please remove the card before submitting the Product and store for later use when your Product is returned. The Company is not responsible for and does not guarantee restoration of any third-party software, personal information or memory data contained in, stored on, or integrated with any other wireless device, whether under warranty or not, returned to the Company for repair or service.

To obtain repairs or replacement within the terms of this Warranty, the Product should be delivered with proof of Warranty coverage (e.g. dated bill of sale), the consumer's return address, daytime phone number and/or fax number and complete description of the problem.

Transportation repaid, to the Company at the address shown below or to the place of purchase for repair or replacement processing. In addition, for reference to an authorized Warranty station in your area, you may telephone in the United States (800) 229-1235, and in Canada (800) 465-9672 (in Ontario call 416-695-3060).

THE EXTENT OF THE COMPANY'S LIABILITY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT PROVIDED ABOVE AND, IN NO EVENT, SHALL THE COMPANY'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY PURCHASER FOR THE PRODUCT.

ANY IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, SHALL BE LIMITED TO THE DURATION OF THIS WRITTEN WARRANTY. ANY ACTION FOR BREACH OF ANY WARRANTY MUST BE BROUGHT WITHIN A PERIOD OF 18 MONTHS FROM DATE OF ORIGINAL PURCHASE. IN NO CASE SHALL THE COMPANY BE LIABLE FOR AN SPECIAL CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, WHATSOEVER. THE COMPANY SHALL NOT BE LIABLE FOR THE DELAY IN RENDERING SERVICE UNDER THIS WARRANTY OR LOSS OF USE DURING THE TIME THE PRODUCT IS BEING REPAIRED OR REPLACED.

No person or representative is authorized to assume for the Company any liability other than expressed herein in connection with the sale of this product.

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

**IN USA:**  
Personal Communications Devices, LLC.  
555 Wireless Blvd.  
Hauppauge, NY 11788  
(800) 229-1235

**IN CANADA:**  
PCD Communications Canada Ltd.  
5535 Eglington Avenue West Suite #210  
Toronto, ON M9C 5K5  
(800) 465-9672