



# MultiConnect™ A2EW

---

## MT200A2EW User Guide

## MultiConnect A2EW User Guide

MT200A2EW-H5-GLOBAL

Part Number S000655

### Copyright

This publication may not be reproduced, in whole or in part, without the specific and express prior written permission signed by an executive officer of Multi-Tech Systems, Inc. All rights reserved. **Copyright © 2017 by Multi-Tech Systems, Inc.**

Multi-Tech Systems, Inc. makes no representations or warranties, whether express, implied or by estoppels, with respect to the content, information, material and recommendations herein and specifically disclaims any implied warranties of merchantability, fitness for any particular purpose and non-infringement.

Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

### Trademarks and Registered Trademarks

Multi-Tech, and the Multi-Tech logo, and SocketModem are trademarks and registered trademarks of Multi-Tech Systems, Inc. All other products and technologies are the trademarks or registered trademarks of their respective holders.

### Legal Notices

The MultiTech products are not designed, manufactured or intended for use, and should not be used, or sold or re-sold for use, in connection with applications requiring fail-safe performance or in applications where the failure of the products would reasonably be expected to result in personal injury or death, significant property damage, or serious physical or environmental damage. Examples of such use include life support machines or other life preserving medical devices or systems, air traffic control or aircraft navigation or communications systems, control equipment for nuclear facilities, or missile, nuclear, biological or chemical weapons or other military applications ("Restricted Applications"). Use of the products in such Restricted Applications is at the user's sole risk and liability.

MULTITECH DOES NOT WARRANT THAT THE TRANSMISSION OF DATA BY A PRODUCT OVER A CELLULAR COMMUNICATIONS NETWORK WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR FREE, NOR DOES MULTITECH WARRANT ANY CONNECTION OR ACCESSIBILITY TO ANY CELLULAR COMMUNICATIONS NETWORK. MULTITECH WILL HAVE NO LIABILITY FOR ANY LOSSES, DAMAGES, OBLIGATIONS, PENALTIES, DEFICIENCIES, LIABILITIES, COSTS OR EXPENSES (INCLUDING WITHOUT LIMITATION REASONABLE ATTORNEYS FEES) RELATED TO TEMPORARY INABILITY TO ACCESS A CELLULAR COMMUNICATIONS NETWORK USING THE PRODUCTS.

### Contacting MultiTech

#### Knowledge Base

The Knowledge Base provides immediate access to support information and resolutions for all MultiTech products. Visit <http://www.multitech.com/kb.go>.

#### Support Portal

To create an account and submit a support case directly to our technical support team, visit: <https://support.multitech.com>.

#### Support

Business Hours: M-F, 8am to 5pm CT

Country	By Email	By Phone
Europe, Middle East, Africa:	<a href="mailto:support@multitech.co.uk">support@multitech.co.uk</a>	+(44) 118 959 7774
U.S., Canada, all others:	<a href="mailto:support@multitech.com">support@multitech.com</a>	(800) 972-2439 or (763) 717-5863

#### Warranty

To read the warranty statement for your product, visit [www.multitech.com/warranty.go](http://www.multitech.com/warranty.go). For other warranty options, visit [www.multitech.com/es.go](http://www.multitech.com/es.go).

#### World Headquarters

Multi-Tech Systems, Inc.  
2205 Woodale Drive, Mounds View, MN 55112  
Phone: (800) 328-9717 or (763) 785-3500  
Fax (763) 785-9874

# Contents

<b>Chapter 1: Product Overview</b> .....	<b>6</b>
Product Overview.....	6
Package Contents .....	6
<b>Chapter 2: Hardware</b> .....	<b>8</b>
LED Indicators .....	8
Specifications .....	9
Power Draw.....	11
Antenna System Cellular Devices.....	11
HEPTA Antenna Information .....	12
Authorized Antenna/Antenna Specifications for Cellular Bands .....	12
3G Antenna Requirements/Specifications .....	12
<b>Chapter 3: Safety Information</b> .....	<b>13</b>
Radio Frequency (RF) Safety .....	13
Sécurité relative aux appareils à radiofréquence (RF).....	13
Interference with Pacemakers and Other Medical Devices .....	14
Potential interference .....	14
Precautions for pacemaker wearers .....	14
Handling Precautions .....	14
Device Maintenance .....	14
Ethernet Ports .....	15
Ports Ethernet .....	15
Dial Port .....	15
Dial Port Caution .....	15
UL notice LPS or Class 2 .....	15
Power Supply Caution .....	15
UL Note English and French .....	15
<b>Chapter 4: Getting Started</b> .....	<b>16</b>
Mounting the Device on a Flat Surface.....	16
Installing/Removing the SIM Card .....	17
Installing the Converter .....	18
Resetting the Device .....	18
Upgrading Firmware .....	19
<b>Chapter 5: Device Configuration</b> .....	<b>20</b>
First-Time Setup Wizard.....	20
Home Page (Dashboard) .....	21
Configuring Network Interfaces .....	22
WAN Setup.....	22

Editing Failover Configuration.....	22
Failover Configuration Fields .....	23
Configuring Dynamic Domain Naming System (DDNS) .....	23
Entering authentication information .....	24
Forcing a DDNS server update .....	24
Configuring Dynamic Host Configuration Protocol (DHCP) Server .....	24
Assigning Fixed Addresses .....	24
Configuring the Dial Port.....	25
Dial Port Configuration Fields .....	25
Time Configuration .....	26
Setting the Date and Time .....	26
Configuring Cellular RTC to Update Date and Time.....	26
Configuring SNTP to Update Date and Time .....	27
<b>Chapter 6: Cellular Configuration .....</b>	<b>28</b>
Configuring Cellular.....	28
Cellular Configuration Fields.....	28
Radio Status .....	30
<b>Chapter 7: Firewall Setup.....</b>	<b>31</b>
Defining Firewall Rules .....	31
Adding Port Forwarding Rules .....	31
Setting up Static Routes.....	31
<b>Chapter 8: Tunnels.....</b>	<b>32</b>
Setting Up VPN Tunnels .....	32
VPN Tunnel Configuration Field Descriptions.....	32
<b>Chapter 9: Administration.....</b>	<b>34</b>
Configuring Device Access .....	34
HTTP Redirect to HTTPS.....	34
HTTPS .....	34
SSH .....	34
ICMP .....	35
IP Defense .....	35
Generating a New Certificate.....	36
Uploading a New Certificate .....	37
Saving and Restoring Settings .....	37
Using the Debugging Options .....	38
Configuring Remote Syslog .....	38
Statistics Settings .....	38
Statistics Configuration Fields.....	39
Ping and Reset Options.....	39

---

<b>Chapter 10: Status and Logs</b> .....	<b>40</b>
Viewing Device Statistics .....	40
Service Statistics.....	41
<b>Chapter 11: Regulatory Information</b> .....	<b>42</b>
47 CFR Part 15 Regulation Class B Devices .....	42
Industry Canada Class B Notice.....	42
EMC, Safety, and R&TTE Directive Compliance .....	43
EMC, Safety, and R&TTE Directive Compliance .....	43
Approvals and Certifications .....	43
Canadian Limitations.....	44
Limitations canadiennes .....	44
<b>Chapter 12: Environmental Notices</b> .....	<b>45</b>
REACH Statement .....	45
Registration of Substances.....	45
Substances of Very High Concern (SVHC) .....	45
Restriction of the Use of Hazardous Substances (RoHS) .....	46
Waste Electrical and Electronic Equipment Statement .....	46
WEEE Directive.....	46
Instructions for Disposal of WEEE by Users in the European Union .....	46
<b>Index</b> .....	<b>48</b>

# Chapter 1: Product Overview

## Product Overview

The MultiConnect™ A2EW Analog converter is a convenient turnkey solution that allows legacy equipment with built-in analog modems to connect via cellular network or ethernet connection. By emulating the traditional dial-up PSTN network and using a cellular modem or ethernet connection, the affordable MultiConnect A2EW converter gives new life to devices currently using traditional analog dial-up communications.

The MultiConnect A2EW converter operates on standards-based communication networks and can be desktop or panel mounted.

## Package Contents







Your MultiConnect A2EW package includes the following:

Contents	Description	Order Part Number
	MultiConnect A2EW Converter	MT200A2EW-H5-WW
	1 - Power Supply	PS-9VCB-SBC-U-Global
	1 - NAM Blade	PB-NAM
	1 - Euro Blade	PB-EU
	1 - UK Blade	PB-GB

Contents	Description	Order Part Number
	1 - Ethernet Cable RJ-45 6-ft.	CA-RJ-45
	1 - Telephone Cable RJ-11	01100207 L
	1 - Hepta Band Antenna	ANHB-1HRA
Customer Notices	Legal and Support Information	
	Extended Services	
	4 - Rubber Dome Feet	

## Chapter 2: Hardware

### LED Indicators

Indicator	Label	Description
Power Source		<b>Continuously ON:</b> Device is powered.
Device Status		<b>Continuously ON:</b> Device is initializing.
		<b>Flashing:</b> Device is in normal operation.
Carrier Detect Status		<b>Continuously ON:</b> There is a call online.
		<b>Flashing:</b> There is a call coming in.
		<b>OFF:</b> There is no call.
Internet Status		<b>Continuously ON:</b> Internet is connected.
Cellular Signal Strength		<b>One Light:</b> Minimal signal.
		<b>Two Lights:</b> Moderate signal.
		<b>Three Lights:</b> Strong signal.
		<b>Lights Flashing:</b> An error has occurred.
Link Status		<b>Continuously ON:</b> The unit is registering with the network.
		<b>Flashing:</b> The unit is registered with the network.



## Specifications

Category	Description
<b>General</b>	
Performance	HSPA+
Frequency Band (MHz)	WCDMA/FDD 800/850 (B5) 900 (B8) AWS1700 (B4) 1900 (B2) 2100 (B1) GSM850, GSM900, DCS1800, PCS1900
Packet Data	HSDPA data service of up to 21.0 Mbps HSUPA data service of up to 5.76 Mbps
Cellular	Telit HE910-D H5
<b>Speed</b>	
Data Speed	HSPA+: Up to 21.0 Mbps downlink/5.76 Mbps uplink EDGE: Up to 296 Kbps downlink/236.8 Kbps uplink GPRS: Up to 107 KBPS downlink/85.6 Kbps uplink
<b>Connectors</b>	
Rf Antenna Connector	50 ohm SMA (female connector)
IP Ethernet	WAN: RJ-45, 10/100 Base T
SIM Connector	Standard 1.8 and 3V SIM receptacle
Dial Connector	RJ-11
Power	2.5 mm miniature
<b>Power Requirements</b>	
Voltage	9V to 18V DC @ 400mA
<b>Physical Description</b>	
Dimensions (L x W x H)	2.89" x 4.75" x 1.58" (73.4 x 120.6 x 40.1 millimeters)
Weight	0.325 lbs (0.147 Kg)
<b>Environment</b>	
Operating Temperature	-22° to 167° F (-30° to 75° C)
Storage Temperature	-40° to 185° F (-40° to 85° C)
Humidity	Relative humidity 20% to 90% non-condensing
<b>Certifications and Compliance</b>	
Safety Compliance	UL 60950-1, 2nd edition cUL 60950-1, 2nd edition IEC 60950-1, 2nd edition, Am.1 and AM.2

Category	Description
Radio and EMC Compliance	FCC Part 15 Class B
	EN 55032 Class B
	ETSI EN 301-489-1
	ETSI EN 301-489-7
	ETSI EN 301-489-24

\*UL Listed @ 40° C, limited by power supply. UL Certification does not apply or extend to an ambient above 40° C and has not been evaluated by UL for ambient greater than 40° C.

UL has evaluated this device for use in ordinary locations only. Installation in a vehicle or other outdoor locations has not been evaluated by UL. UL Certification does not apply or extend to use in vehicles or outdoor applications or in ambient above 40° C.

Note: The radio's performance may be affected at the temperature extremes. This is considered normal. There is no single cause for this function. Rather, it is the result of an interaction of several factors, such as the ambient temperature, the operating mode and the transmit power.

## Power Draw

Multi-Tech Systems, Inc. recommends that you incorporate a 10% buffer into your power source when determining product load.

Voltage and Connection	Device Powered On and Idle with No Modem Connection or Ethernet Traffic	(AVG) Measure Current at Max Power	IP Connection to Cellular Call Box with Data (AVG Measured Current at Max Power)	TX Pulse (AVG) Amplitude Current for GSM850 or Peak Current for HSDPA	Total Inrush Charge Measured in MilliCoulombs (mC)
<b>9 Volts:</b> Simulated GSM850 Wireless Connection	155 mA	425 mA	640 mA	2.0 Amps	.175 mC
<b>9 Volts:</b> Simulated HSDPA Wireless Connection	152 mA	475 mA	763 mA	560 mA	.175 mC
<b>18 Volts:</b> Simulated GSM850 Wireless Connection	85 mA	212 mA	605 mA	1.03 Amps	.133 mC
<b>18 Volts:</b> Simulated HSDPA Wireless Connection	80 mA	199 mA	271 mA	288 mA	.133 mC

**Tx Pulse:** The average peak current during a GSM850 transmission burst period or HSDPA connection. The transmission burst duration for GSM850 can vary depending on what transmission scheme is being deployed (GPRS Class 8, Class 10, GSM, etc.).

**Maximum Power:** The continuous current during maximum data rate with the radio transmitter at maximum power

**Inrush Charge:** The total inrush charge at power on.

## Antenna System Cellular Devices

The cellular/wireless performance depends on the implementation and antenna design. The integration of the antenna system into the product is a critical part of the design process; therefore, it is essential to consider it early so the performance is not compromised. If changes are made to the device's certified antenna system, then recertification will be required by specific network carriers.

## HEPTA Antenna Information

### Authorized Antenna/Antenna Specifications for Cellular Bands

The cellular radio portion of the device is approved with the following antenna or for alternate antennas meeting the given specifications.

Manufacturer:	Laird Technologies.
Description:	HEPTA-SM
Model Number:	MAF94300
Multi-Tech Part Number:	45009735L

#### MultiTech Ordering Information:

Model	Quantity
ANHB-1HRA	1
ANHB-10HRA	10
ANHB-50HRA	50

### 3G Antenna Requirements/Specifications

Category	Description	
Frequency Range	824 – 960 MHz / 1710 – 1990 MHz / 1920 – 2170 MHz	
Impedance	50 Ohms	
VSWR	VSWR should not exceed 2.0:1 at any point across the bands of operation	
Typical Radiated Gain	850 MHz	3.17 dBi
	950 MHz	3.51 dBi
	1800 MHz	3.55 dBi
	1900 MHz	3.0 dBi
	2100 MHz	3.93 dBi
Radiation	Omni-directional	
Polarization	Linear Vertical	

## Chapter 3: Safety Information

### Radio Frequency (RF) Safety

Due to the possibility of radio frequency (RF) interference, it is important that you follow any special regulations regarding the use of radio equipment. Follow the safety advice given below.

- Operating your device close to other electronic equipment may cause interference if the equipment is inadequately protected. Observe any warning signs and manufacturers' recommendations.
- Different industries and businesses restrict the use of cellular devices. Respect restrictions on the use of radio equipment in fuel depots, chemical plants, or where blasting operations are in process. Follow restrictions for any environment where you operate the device.
- Do not place the antenna outdoors.
- Switch OFF your wireless device when in an aircraft. Using portable electronic devices in an aircraft may endanger aircraft operation, disrupt the cellular network, and is illegal. Failing to observe this restriction may lead to suspension or denial of cellular services to the offender, legal action, or both.
- Switch OFF your wireless device when around gasoline or diesel-fuel pumps and before filling your vehicle with fuel.
- Switch OFF your wireless device in hospitals and any other place where medical equipment may be in use.

### Sécurité relative aux appareils à radiofréquence (RF)

À cause du risque d'interférences de radiofréquence (RF), il est important de respecter toutes les réglementations spéciales relatives aux équipements radio. Suivez les conseils de sécurité ci-dessous.

- Utiliser l'appareil à proximité d'autres équipements électroniques peut causer des interférences si les équipements ne sont pas bien protégés. Respectez tous les panneaux d'avertissement et les recommandations du fabricant.
- Certains secteurs industriels et certaines entreprises limitent l'utilisation des appareils cellulaires. Respectez ces restrictions relatives aux équipements radio dans les dépôts de carburant, dans les usines de produits chimiques, ou dans les zones où des dynamitages sont en cours. Suivez les restrictions relatives à chaque type d'environnement où vous utiliserez l'appareil.
- Ne placez pas l'antenne en extérieur.
- Éteignez votre appareil sans fil dans les avions. L'utilisation d'appareils électroniques portables en avion est illégale: elle peut fortement perturber le fonctionnement de l'appareil et désactiver le réseau cellulaire. S'il ne respecte pas cette consigne, le responsable peut voir son accès aux services cellulaires suspendu ou interdit, peut être poursuivi en justice, ou les deux.
- Éteignez votre appareil sans fil à proximité des pompes à essence ou de diesel avant de remplir le réservoir de votre véhicule de carburant.
- Éteignez votre appareil sans fil dans les hôpitaux ou dans toutes les zones où des appareils médicaux sont susceptibles d'être utilisés.

## Interference with Pacemakers and Other Medical Devices

### Potential interference

Radio frequency energy (RF) from cellular devices can interact with some electronic devices. This is electromagnetic interference (EMI). The FDA helped develop a detailed test method to measure EMI of implanted cardiac pacemakers and defibrillators from cellular devices. This test method is part of the Association for the Advancement of Medical Instrumentation (AAMI) standard. This standard allows manufacturers to ensure that cardiac pacemakers and defibrillators are safe from cellular device EMI.

The FDA continues to monitor cellular devices for interactions with other medical devices. If harmful interference occurs, the FDA will assess the interference and work to resolve the problem.

### Precautions for pacemaker wearers

If EMI occurs, it could affect a pacemaker in one of three ways:

- Stop the pacemaker from delivering the stimulating pulses that regulate the heart's rhythm.
- Cause the pacemaker to deliver the pulses irregularly.
- Cause the pacemaker to ignore the heart's own rhythm and deliver pulses at a fixed rate.

Based on current research, cellular devices do not pose a significant health problem for most pacemaker wearers. However, people with pacemakers may want to take simple precautions to be sure that their device doesn't cause a problem.

- Keep the device on the opposite side of the body from the pacemaker to add extra distance between the pacemaker and the device.
- Avoid placing a turned-on device next to the pacemaker (for example, don't carry the device in a shirt or jacket pocket directly over the pacemaker).

## Handling Precautions

To avoid damage due to the accumulation of static charge, use proper precautions when handling any cellular device. Although input protection circuitry has been incorporated into the devices to minimize the effect of static build-up, use proper precautions to avoid exposure to electronic discharge during handling and mounting the device.

## Device Maintenance

When maintaining your device:

- Do not attempt to disassemble the device. There are no user serviceable parts inside.
- Do not expose your device to any extreme environment where the temperature or humidity is high.
- Do not expose the device to water, rain, or spilled beverages. It is not waterproof.
- Do not place the device alongside computer discs, credit or travel cards, or other magnetic media. The information contained on discs or cards may be affected by the device.
- Using accessories, such as antennas, that MultiTech has not authorized or that are not compliant with MultiTech's accessory specifications may invalidate the warranty.

If the device is not working properly, contact MultiTech Technical Support.

## Ethernet Ports

**CAUTION:** Ethernet ports and command ports are not designed to be connected to a public telecommunication network.

## Ports Ethernet

**CAUTION:** Les ports Ethernet et de commande ne sont pas conçus pour être raccordés à un réseau de télécommunications public.

## Dial Port

### Dial Port Caution



**CAUTION:** The dial port **is not** designed to be connected to a Public Telecommunications Network (PSTN/phone line) or used outside the building.



**CAUTION:** L'accès à commutation directe n'est pas conçu pour être raccordé à un réseau de télécommunications public (RTPC/ligne téléphonique) ou utilisé à l'extérieur du bâtiment.

## UL notice LPS or Class 2

**Note:** This product is intended to be supplied a listed power Module marked L.P.S. or Class 2 and rates from 5V dc 1.4A.

## Power Supply Caution

**CAUTION:** Do not replace the power supply with one designed for another product; doing so can damage the modem and void your warranty.

**CAUTION:** Pour garantir une protection continue contre les risques d'incendie, remplacez les fusibles uniquement par des fusibles du même type et du même calibre.

## UL Note English and French

UL Listed at 40° C, limited by power supply. UL Certification does not apply or extend to an ambient above 40° C and has not been evaluated by UL for ambient greater than 40° C.

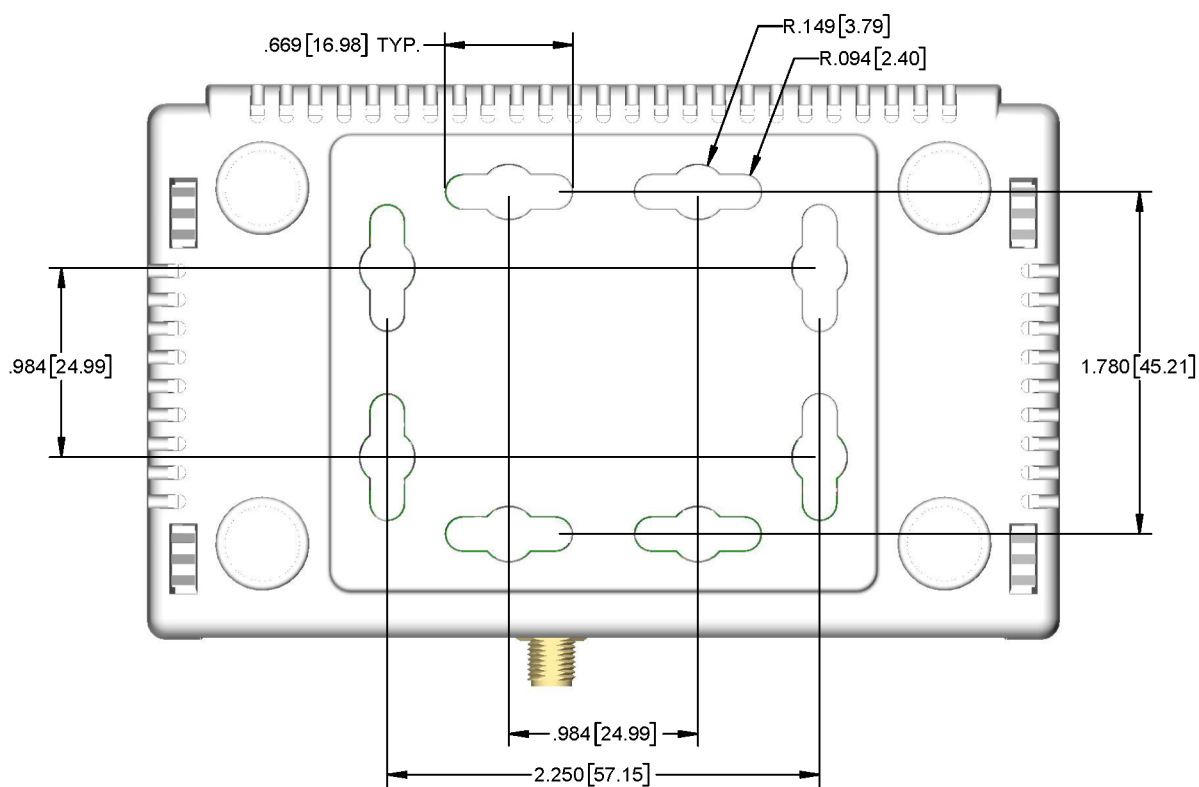
Listé UL à 40° C, limité par l'alimentation. La certification UL ne s'applique pas ou ne s'étend pas à des températures dépassant 40° C, et le produit n'a pas été évalué par UL pour une température ambiante dépassant 40° C.

## Chapter 4: Getting Started

### Mounting the Device on a Flat Surface

To mount the device:

- Verify the location has a strong signal strength.
- Position the device so the antenna is always vertical and pointing upward.
- Use the dimensions in the following image to space screw holes.
- Use either #4 or #6 pan head screws.



DIMENSIONS IN In [mm]



## Installing/Removing the SIM Card

This device requires a SIM card to operate on a GPRS/GSM and HSPA+ network.

Note: Disconnect power from the unit before installing the SIM card.

To install the SIM card:

1. Open the SIM door by pressing down on the tab at the top of the door and pulling it outward.
2. Insert the SIM card into the card holder either by hand or with a needle-nose pliers. See the graphic for the correct orientation of the notch on the SIM card.
3. Make sure that the SIM card fits properly and then close the door.
4. To activate the SIM card, refer to the GSM Modem Activation Notice at [www.multitech.com](http://www.multitech.com).

To remove the SIM card:

1. Open the SIM door.
2. Remove the SIM card either by hand or with a needle-nose pliers.
3. Close the SIM door.

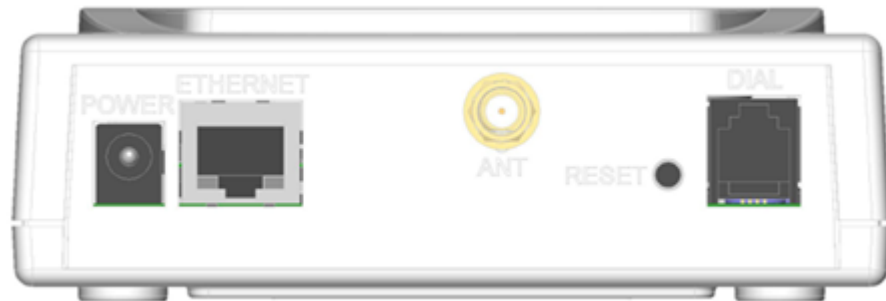


## Installing the Converter

1. Connect one end of the Ethernet cable to the **Ethernet** port on the back of the converter and the other end to the Ethernet port on your computer, either directly or through a switch or hub.
2. Connect the RJ11 phone cable to the **Dial** port on the converter and connect the other end of the cable to the analog modem.
3. Connect the antenna to the antenna connector.
4. Attach the power cable to the **Power** port on the converter and plug the other end of the cable into your power source.

When the Power LED remains on, the device is powered.

When the Device Status LED begins to blink, the device is ready for use.



5. Perform the following steps if your computer's IP address is not in the same IP and subnet mask range as the device.
  - a. Open a web browser. In the browser's address field, type the default address for the converter: <http://192.168.2.1>. (If the browser displays a message that there is a problem with the website's security certificate, ignore this and click **Continue to the webpage**).
  - b. A login page opens. In the **username** field, type the default user name: admin (all lower-case).
  - c. In the **password** field, type the default password: admin (all lower-case).
  - d. Click **Login**. The Web Management Home page opens. Online documentation included with the web management interface describes how to configure your converter.
6. Configure your device using the web management interface. See the Device Configuration chapter for more information.

## Resetting the Device

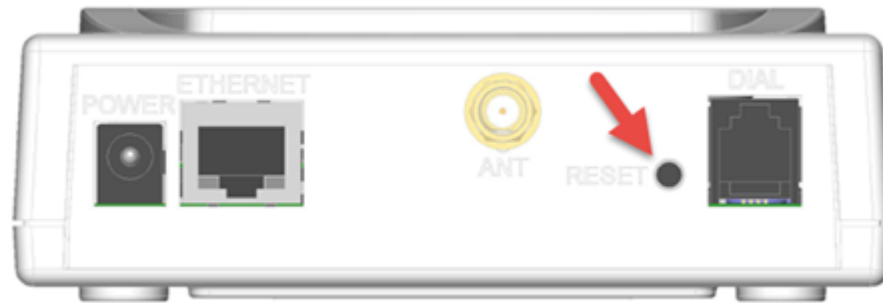
You need:

- A pin, paperclip, or similar thin object that can fit into the reset hole.

The following is the default condition for the RESET button on the device. You can program a change to the behavior of the button if needed.

To reset the device:

1. Find the hole labeled RESET. The reset button is recessed into the case.
2. Use the pin to press and release the RESET button as follows:



- To reboot, press RESET for less than 3 seconds.
- To reboot and restore user-defined defaults (if previously set), press RESET for 3 to 29 seconds.
- To reboot, restore factory settings, and erase user-defined defaults, press RESET for 30 seconds or longer.

**Note:** The device reboots when restoring settings.

## Upgrading Firmware

Upgrade the device's firmware to the latest version.

You can download firmware upgrades from the MultiTech website.

First, check your firmware version. Refer to the upper right corner of your configuration software window. To upgrade the firmware on your device:

1. Before you upgrade your firmware, save your present configuration as a backup.
2. Go to the MultiTech website, locate the firmware upgrade file you want for your device, and download this file to a known location.
3. From **Administration**, select **Firmware Upgrade**. The Administration: Firmware Upgrade pane opens.
4. In the **Firmware Upgrade File** field, point to the area where the upgrade file resides, and select the firmware file. To do so:
  - a. Click **Browse** to find where the firmware file resides that you want to apply.
  - b. Select the file and click **Open**. The file appears in the **Firmware Upgrade File** field. Make sure you select the correct BIN file; otherwise, your device can become inoperable.
5. Click **Start Upgrade**.
6. A message about time needed to upgrade appears. Click **OK**. A progress bar appears indicating the status of the upgrade. When upgrade is completed, your device reboots.
7. After the firmware upgrade is complete, verify your configuration to make sure it is what you expected.

**Note:**

- The new firmware is written into flash memory.
- It may take up to five minutes to upgrade the firmware. Do not interfere with the device's power or press the reset button during this time.

# Chapter 5: Device Configuration

## First-Time Setup Wizard

The first-time setup wizard walks you through the initial setup. Other than when you first power up the device, you must reset the device and accept factory default settings to see the first-time setup.

1. Click **Next**.
2. To change the password, enter the following. If you do not want to change your password, click **Skip**.  
**Note:** Multi-Tech highly recommends changing your password.
  - a. Enter in the **Current Password**. The initial password is **admin**.
  - b. Enter in the **New Password**.
  - c. Re-enter the new password in the **Confirm Password** field.
  - d. Click **Next**.
3. Time Configuration. Set the date, time, and time zone.
  - a. Enter the desired **Date** in the format **MM/DD/YYYY**.
  - b. Enter the desired **Time** in the format **HH:MM** (24hr).
  - c. Select the **Time Zone** in which the device operates.
  - d. Click **Next**.
4. IP Setup - eth0
  - a. **Mode:** Choose from **Static**, **DHCP Client**, or **DHCP Client - Addresses Only**.
  - b. In the **IP Address** field, type the device's IP address.
  - c. In the **Mask** field, type the mas for the network. The default is **255.255.255.0**.
  - d. In the **Gateway** field, type the IP address of the network's gateway (device).
  - e. In the **Primary DNS Server**field, type the address of the primary DNS.
  - f. In the **Secondary DNS Server**field, type the address of the secondary DNS.
  - g. Click **Next**.
5. Cellular PPP Configuration
  - a. Enabled: **Check** to enable. This is enabled by default.
  - b. To enable the dial-on-demand feature, check **Dial-on-Demand**. This indicates to the device to bring up the PPP connection when there is outgoing IP traffic, and take down the PPP connection after a given idle timeout.
  - c. Enter the **APN** (Access Point Name). The APN is assigned by your wireless service provider.
  - d. Click **Next**.
6. Cellular PPP Authentication
  - a. Select the authentication protocol **Type** used to negotiate with the remote peer: **PAP**, **CHAP**, or **PAP-CHAP**. The default value is **NONE**.
  - b. Click **Next**.
7. Dial Port Settings

- a. Mode: **Select** from **PPP** or **RAW**
- b. Click **Finish**.

## Home Page (Dashboard)

The Home page (dashboard) displays a summary of the device's configuration settings. The following settings, where applicable, include the area of the Web Management interface where they can be accessed and changed.

Click **Home** to display the following information:

- **Common::**
  - **Model Number:** The MultiConnect A2EW model ID.
  - **Serial Number:** The MultiTech device ID.
  - **IMEI:** International Mobile Station Equipment Identity.
  - **Firmware:** MultiConnect A2EW firmware version.
  - **Current Time:** The device's current date and time. For information on setting the date and time, go to **Setup > Time Configuration**.
  - **Up Time:** Amount of time the device has been continuously operating.
  - **WAN Transport:** Current transport for IP traffic leaving the LAN. If two WAN interfaces are configured for use (Wi-Fi and cellular), the current WAN will be set based on the WAN configurations at *Setup > WAN Configuration*.
- **Cellular:**
  - **State:** Current state of the cellular PPP link. For more information, go to **Cellular > Cellular Configuration**.
  - **Signal:** Current signal strength of the cellular link. Mouse hover provides dBm value.
  - **Connected:** Total time connected for the current PPP session.
  - **IP Address:** Current cellular WAN IP address issued to this device by the cellular carrier.
  - **Roaming:** Indicates whether or not this device's cellular link is currently connected to its home network.
  - **Phone number:** Device's cellular phone number also known as Mobile Directory Number (MDN).
  - **Tower:** Tower ID of the cellular tower currently providing cellular service to this device.
- **Ethernet/LAN:**
  - **Type:** This will always be **LAN**.
  - **Mode:** This will be either **static** or **DHCP** (dynamic host configuration protocol).
  - **MAC Address:** Media Access Control Address used to uniquely identify the device's LAN Ethernet interface.
  - **IP Address:** LAN IP address of this device. To configure the IP address, go to **Setup > Network Configuration**.
  - **Mask:** Network mask of the LAN. To configure the mask, go to **Setup > Network Configuration**.
  - **Gateway:** Default gateway IP address of the LAN. To configure the default gateway, go to **Setup > Network Configuration**.
  - **DNS:** Current DHCP Lease range of this device's DHCP server. To configure, go to **Setup > DHCP Configuration**.

## Configuring Network Interfaces

Your device manages traffic for your local area network (LAN). To change the IP address and DNS configuration:

1. From **Setup**, select **Network Interfaces**.
2. To configure the address LAN information, select the pencil icon to edit the LAN network details:  
 In the **IP Address** field, type the device's IP address. The default is 192.168.2.1.  
 In the **Mask** field, type the mask for the network. The default is 255.255.255.0.  
 In the **Gateway** field, type the IP address of the network's gateway (device). If this device is the gateway, leave this field blank.
3. To resolve domain names, configure domain name server information (DNS).  
 To allow the device to behave as a local DNS forwarder, check **Enable Forwarding Server**.  
**Note:** When a DNS request is received, the device forwards the request to a remote DNS server if there is no record in the device's cache. New requests are cached in the device for future requests.  
 In the **Primary Server** field, type the address of the primary DNS.  
 In the **Secondary Server** field, type the address of the secondary DNS.  
 The **WAN DNS Servers** field displays information about DNS servers, if any, that have been detected on the WAN link of the device.
4. Click **Submit**.
5. To save your changes, click **Save and Restart**.

## WAN Setup

### Configuring WAN Failover Priority

Failover mode regulates which WAN is used for the Internet connection and switches the WAN if a connectivity failure is detected.

Failover mode enables the WAN with the highest priority as displayed on the **WAN Configuration** page. If the WAN with priority 1 is disabled or a connection failure is detected, the WAN with priority 2 is automatically selected for establishing connection to the Internet.

If Ethernet is used as WAN, the DHCP server must be disabled.

1. Click **Setup > WAN Configuration**.
2. Under **Options**, click the up and down arrows to change the priority of the appropriate WAN.
3. Click **Save and Restart** to save the change.

For field descriptions see Failover Configuration Fields

For information on editing WAN Failover see Editing Failover Configuration

## Editing Failover Configuration

The device can use the active or passive mode to monitor the Internet availability in WAN. The default condition is active mode.

Active mode can be type ICMP (ping) or TCP. ICMP periodically pings the designated host at the specified interval. TCP tries to make a connection to the designated host at the interval specified.

For both ICMP and TCP, if a response is not received, the device switches to the WAN with lower priority. The device continues to ping the designated host at the interval specified for WAN with the higher priority and switches back when the ping is successful. When passive mode is enabled, the device switches the WANs when the network interface is down. The currently active WAN is displayed on the home page under the label WAN Transport.

To edit failover configuration:

1. Click **Setup > WAN Configuration**.
2. Under the **Options** column at the right, click the pencil icon (edit) for the selected WAN. The **Failover Configuration** page is displayed.
3. Make the desired changes. Refer to Failover Configuration Fields for details.
4. Click **Finish**.
5. If you are finished making changes, click **Save and Restart**.

## Failover Configuration Fields

Field	Description
<b>Monitoring Mode</b>	Use the drop-down list to select the mode to connect to the host: PASSIVE or ACTIVE.
<b>Interval</b>	Enter the number of seconds between each check. Default is 60 seconds.
<b>Host Name</b>	Enter the host name or IP address to use for the check. Default is www.google.com.
<b>Mode Type</b>	Use the drop-down list to select the mode type: ICMP or TCP. Default is ICMP. (Active Monitoring Mode)
<b>TCP Port</b>	Enter the TCP Port number to connect to the host. (Mode TCP)
<b>ICMP Port</b>	Enter the number of ICMP pings to be sent to the specified host. Default is 10. (Mode ICMP)

## Configuring Dynamic Domain Naming System (DDNS)

This feature allows your device to use a DDNS service to associate a hosted server's domain name with a dynamically changing internet address. To configure your device to use DDNS:

1. From **Setup**, select **DDNS Configuration**.
2. In the **Configuration** group, check **Enabled**.
3. In the **Service** drop-down list, select a DDNS service. To define a service that isn't listed choose **Custom**.
  - a. For custom DDNS service, in the **Service** field, type the DDNS server's URL.
  - b. For custom DDNS service, in the **Port** field, type the DDNS server's port.
4. In the **Domain** field, type the registered Domain name.
5. In the **Update Interval** field, type the days that can pass with no IP Address change. At the end of this interval, the existing IP Address is updated on the server so that the address does not expire. The range of the interval you can enter is between 1 and 99 days. The default is 28 days.
6. Check **Use Check IP**, if you want to query the server to determine the IP address before the DDNS update. The IP address is still assigned by the wireless provider and the DDNS is updated based on the address

returned by Check IP Server. If disabled, the DDNS update uses the IP address from the PPP link. The default is **Use Check IP**.

7. In the **Check IP Server** field, type the name to which the IP Address change is registered. Example: checkip.dyndns.org .
8. In the **Check IP Port** field, type the port number of the Check IP Server. The default is 80.
9. From the **System** drop-down list, select the desired system registration type, either Dynamic or Custom. The default is Dynamic.
10. Enter the **Username** of the server.
11. Enter the **Password** of the server.
12. To force update of DDNS, click **Update**.
13. Click **Submit**.
14. To save your changes, click **Save and Restart**.

## Entering authentication information

Your DDNS server requires you to identify yourself before you can make changes.

1. In the **Username** field, type the name that can access the DDNS Server. The default is NULL. You receive your name when you register with the DDNS service.
2. In the **Password** field, type the password that can access the DDNS Server. The default is NULL. You receive your password when you register with the DDNS service.
3. Click **Submit**. If you are finished making changes click **Save and Restart**.

## Forcing a DDNS server update

To update the DDNS server with your IP address, click **Update**.

## Configuring Dynamic Host Configuration Protocol (DHCP) Server

You can configure your device to function as a DHCP server that supplies network configuration information, such as IP address, subnet mask, and broadcast address, to devices on the network. To configure the DHCP server:

1. From **Setup**, select **DHCP Configuration**.
2. To use the DHCP feature, check **Enabled**.
3. The **Subnet** field displays the subnet address.
4. The **Mask** field displays the network's subnet mask.
5. In the **Lease Range Start** field and in the **Lease Range End** field, type the range of IP addresses to be assigned by DHCP.
6. In the **Lease Time** field, type the DHCP lease time. Lease time is set in days, hours, and minutes.
7. Click **Submit**. If you are finished making changes, click **Save and Restart**.

## Assigning Fixed Addresses

To add fixed addresses for the DCHP server:

1. In the **Fixed Address** group, click **Add**. A dialog box opens, where you define the address.
2. In the **MAC Address** field, type the MAC address to which the specified IP address binds.
3. In the **IP Address** field, type the fixed IP address to be assigned.



4. Click **Finish**.
5. To save your changes, click **Save and Restart**.

## Configuring the Dial Port

To configure the dial port:

1. From **Setup**, select **Dial Port Configuration**.
2. From the **Mode** drop-down list, select PPP (passthrough mode) or RAW.
3. Make the desired changes. Refer to Dial Port Configuration Fields for details.
 

**Note:** Click **Reset to Default** in the top right corner to return all values to their default settings.
4. Click **Submit**.
5. To save your changes, click **Save and Restart**.

## Dial Port Configuration Fields

Field	Description
<b>Dial Port Mode</b>	
<b>RAW</b>	Allows external device serial raw data to be converted to a TCP packet and transmitted over a standard IP network.
<b>PPP</b>	Allows an external device to use the PPP protocol to connect to the converter.
<b>PPP Configuration</b>	
<b>Connect Timeout</b>	The amount of time that the connection can remain idle before it disconnects.
<b>Authentication Type</b>	The appropriate PPP authentication type (none, PAP, CHAP, or PAP-CHAP).
<b>Init String1</b>	Allows the user to enter initialization commands into the internal analog modem.
<b>Init String2</b>	Allows the user to enter initialization commands into the internal analog modem.
<b>Server IP Address</b>	Internal PPP IP address for the device connection.
<b>Client IP Address</b>	Internal PPP IP address provided to the external PPP client.
<b>Internet Connection Check</b>	
<b>Enable</b>	When checked, monitors and maintains an active internet connection at all times.
<b>Mode</b>	The mode in which to check that the internet connection is active (ICMP or TCP).
<b>Hostname</b>	The remote host IP.
<b>ICMP Count</b>	The amount of times that the connection is checked before determined a failure.

Field	Description
<b>IP Pipe</b>	
<b>Client Mode</b>	When the external modem dials into the device, the TCP client initiates a TCP connection to the remote TCP server.
<b>Server Mode</b>	When the external modem is waiting to answer a modem call, the TCP server waits for the remote TCP client to connect.
<b>TCP Protocol</b>	For data without encryption.
<b>SSL/TLS Protocol</b>	For data with encryption.
<b>Server Port</b>	Remote server TCP port number.
<b>Modem Configuration</b>	
<b>Connect Timeout</b>	The amount of time that the connection can remain idle before it disconnects.
<b>On Demand</b>	In TCP <b>client</b> mode, allows TCP the connection to remain when analog modem is active. In TCP <b>server</b> mode, allows analog modems to remain connected when the TCP connection is active.
<b>Init String1</b>	Allows the user to enter initialization commands into the internal analog modem.
<b>Init String2</b>	Allows the user to enter initialization commands into the internal analog modem.

## Time Configuration

You can configure how your device manages the setting of time on its domain of systems. The system date and time display in these formats: **MM/DD/YYYY / HH:MM**. You can set the date and time manually, or you can configure the device to get this information from a cellular RTC (real time clock) or an SNTP server.

## Setting the Date and Time

To set the device's date and time:

1. From **Setup**, select **Time Configuration**.
2. In the **Date** field, type in the date you desire, or select the date from the pop-up calendar that opens.
3. In the **Time** field, type the time.
4. From the **Time Zone** drop-down list, select your time zone. The default selection is UTC (Universal Coordinated Time, Universal Time).

**Note:** To learn more about time zones, visit the following website :  
<http://www.greenwichmeantime.com/info/current-time.htm>

5. Click **Submit**.
6. To save your changes, click **Save and Restart**.

## Configuring Cellular RTC to Update Date and Time

This device defaults to the cellular RTC (real time clock) setting to update the date and time.

1. To enable the cellular RTC, check **Enabled**.
2. In the **Polling Time** field, enter the time (in minutes) that passes, after which the cellular RTC updates the time. Default is 120 minutes.
3. Click **Submit**.
4. To save your changes, click **Save and Restart**.

## Configuring SNTP to Update Date and Time

To configure the server from which the SNTP date and time information is taken, and how often:

1. To enable SNTP to update the date and time, check **Enabled**.
2. In the **Server** field, type the SNTP server name or IP address that is contacted to update the time.
3. In the **Polling Time** field, type the time that passes (in minutes), after which the SNTP client requests the server to update the time. Default is 120 minutes.
4. Click **Submit**.
5. To save your changes, click **Save and Restart**.

# Chapter 6: Cellular Configuration

## Configuring Cellular

To configure how cellular is used on your device:

1. On the Web Management interface, go to **Cellular > Cellular Configuration** to display the **Cellular Configuration** window. If you choose IPv6 Passthrough mode, you must select **Administration > Initial Setup**.
2. Check **Enabled**.
3. Check and change the Cellular Configuration fields as desired. For field descriptions, see Cellular Configuration Fields.
4. Click **Submit**.
5. To save your changes, click **Save and Restart**.

## Cellular Configuration Fields

Field	Description
<b>General Configuration</b>	
Enabled	Allows the device to establish a cellular PPP connection (Cellular WAN).
Dial-on-Demand	Enables the Dial-on-Demand feature. If enabled, the device brings up and maintains a cellular connection while network activity on the LAN requires WAN access. The device brings down the cellular connection when outgoing network traffic ceases for the given Idle Timeout duration.
Connect Timeout	The time (in seconds) that the device waits before it deems that the connection attempt has failed. The value used is the amount of time that elapses between each dialing retry.
Dialing Max Retries	Number of dialing retries allowed; the default is zero, which means an infinite number is allowed.
<b>Modem Configuration</b>	
Dial Number	The modem dial string is: <ul style="list-style-type: none"> <li>■ <b>*99***1#</b> for GSM/GPRS/LTE devices</li> <li>■ <b>#777</b> for CDMA/EVDO devices</li> <li>■ <b>*99***3#</b> for Verizon SIM based LTE devices</li> </ul>
Connect String	The modem response to initiate a PPP connection, usually <b>CONNECT</b> .
Dial Prefix	The modem AT command that initiates a PPP connection, usually <b>ATDT</b> or <b>ATD</b> .
SIM Pin	The pin used to unlock the SIM for use (only required if the SIM is locked). This does not apply to CDMA radios.
APN	The Access Point Name assigned by the wireless service provider (carrier specific).

Field	Description
Init String#	Optional fields to apply additional AT commands that execute just before every PPP connection attempt. Use these fields to expand functionality and to troubleshoot.
<b>Authentication</b>	
Authentication Type	The type of authentication to use when establishing a PPP connection: <b>NONE, PAP, CHAP, or PAP-CHAP</b> (either). Authentication may not be required by the cellular service provider.
Username	Name of the user that the remote PPP peer uses to authenticate.
Password	Password that the remote PPP peer uses to authenticate.
<b>Keep Alive</b>	
Used to periodically check if the cellular link is up; if not, the device tries to establish the link.	
<b>ICMP/TCP Check</b>	
An active check that provides the most reliable and reactive diagnosis of the cellular link, but requires sending data through the cellular link.	
Enabled	Enables the Active Keep Alive check. Depending on the plan type and data usage, this may result in additional data charges.
Keep Alive Type	Protocol type for active keep alive, either <b>TCP</b> or <b>ICMP</b> . <b>ICMP</b> periodically pings the designated host at the specified interval. <b>TCP</b> tries to make a connection to the designated host at the interval specified.
Interval	Time in seconds between active checking of the cellular link.
Hostname	Host name or IP address for the keep alive check.
TCP Port	TCP port number to connect with the TCP server (only visible when <b>Keep Alive Type TCP</b> is selected).
ICMP Count	Number of sequential, unsuccessful ping attempts to the specified host to declare that the link needs to be re-established (only visible when <b>Keep Alive Type ICMP</b> is selected).
<b>Data Receive Monitor</b>	
A passive check that observes the absence of packets received over a given amount of time. This check cannot reliably determine if the link is down; no network traffic may cause the monitor to signal to shutdown and re-establish the cellular link even though the link was in a good state.	
Enabled	Enable or disable the passive monitoring of the cellular link.
Window	The amount of time that can pass without receiving network traffic before the cellular link is torn down and re-established.

## Radio Status

Field	Description
<b>Module Information</b>	
IMEI	International Mobile Station Equipment Identifier
IMSI	International Mobile Subscriber Identifier
Manufacturer	Company that developed the cellular module
Model	Cellular module model number
Hardware Revision	Module's hardware revision
MDN (Phone Number)	Mobile Directory Number. In some SIM/carriers, the value may not be present and therefore not displayed.
MSID	Mobile Station ID. Some SIM/carriers do not contain this value and therefore the value is not displayed.
Firmware Version	Module's firmware version
<b>Service Information</b>	
Home Network	Cellular service provider associated with the module's data account
Current Network	Current cellular service operator (Not available for C2 or EV3 models)
RSSI	Received Signal Strength Indication
Service	Cellular service connection type
Roaming	Indicates whether or not the current service is provided by the Home Network carrier
<b>Update Options</b>	
MDN (Phone Number)	Update the cellular module's phone number. This number is updated only on the device. The MDN that the carrier has associated with this device does not change.

# Chapter 7: Firewall Setup

## Defining Firewall Rules

The device's firewall enforces a set of rules that determine how incoming and outgoing packets are handled. By default, all outbound traffic originating from the LAN is allowed to pass through the firewall, and all inbound traffic originating from external networks is dropped. This effectively creates a protective barrier between the LAN and all other networks.

## Adding Port Forwarding Rules

For a device within the LAN to be visible from the internet or from an outside network, create a forwarding rule to allow incoming packets to reach the device.

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Port Forwarding** group, click **Add Rule**.
3. In the **Port Forwarding Rule** dialog box, enter a name for the rule and optionally, a description. Click **Next**.
4. In the **External WAN Port(s)** field, type the port(s) to be forwarded. Common ports are listed in the field's attached drop-down list and are exposed once you enter a character. Type **ANY** to forward all ports.
5. In the **Destination LAN Port(s)** field, type the port to which packets are translated. If there is a range of ports, the ending port is automatically set. The Destination LAN ending port is based on the Destination LAN starting port and the range provided in the **External WAN Port(s)** field.
6. From the **Protocol** drop-down list, select the protocol of the messages that can be forwarded.
7. Click **Finish**.
8. To save your changes, click **Save and Restart**.

## Setting up Static Routes

To set up a manually configured mapping of an IP address to a next-hop destination for data packets:

1. Go to **Firewall > Static Routes**.
2. In the **Static Routes** window, click **Add Route**.
3. In the **Name** field of the **Add Route** dialog box, type the name of the route.
4. In the **Address** field, type the remote network IP address of the remote location.
5. In the **Mask** field, type the network mask that is assigned on the remote location.
6. In the **Gateway** field, type the IP address of the routing device that supports the remote IP Network.
7. Click **Finish**.
8. To save your changes, click **Save and Restart**.

## Chapter 8: Tunnels

### Setting Up VPN Tunnels

Tunneling allows the use of a public network to convey data on behalf of two remote private networks. It is also a way to transform data frames to allow them to pass networks with incompatible address spaces or even incompatible protocols. VPN (virtual private network) is a tunneling mechanism that extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network.

1. From **Tunnels**, select **OpenVPN Tunnels**.
2. Click **Add Tunnel**.
3. In the **Name** field, enter the tunnel name.
4. From the **Type** drop-down menu, select the tunnel type.
5. In the **Description** field, enter a description of the tunnel (optional).
6. Click **Next**.
7. Make the necessary menu selections and field entries. See **VPN Tunnel Configuration Field Descriptions** for more information.
8. Click **Finish** to finish adding the tunnel, or click **Back** to return to the previous window and make edits.
9. To save your changes, click **Save and Restart**.

### VPN Tunnel Configuration Field Descriptions

Field	Description
<b>Open VPN Tunnel</b>	
<b>Name</b>	Name used to identify the tunnel in configurations and logs.
<b>Tunnel Types</b>	<b>Server:</b> Waiting for remote OpenVPN client to connect. <b>Client:</b> Originate the OpenVPN connection to the remote openVPN server. <b>Custom:</b> Manually configure Open VPN Settings.
<b>Description</b>	Optional text to describe the tunnel. This description shows up in the UI while hovering over the summary of a tunnel.
<b>Interface Types</b>	<b>TAP</b> works at the Ethernet level (layer 2) and acts as a switch or bridge. <b>TUN</b> works at the network level (layer 3) and routes packets on the VPN.
<b>TLS Authorization</b>	Establishes control and data channels which are multiplexed over a single TCP/UDP port. OpenVPN initiates a TLS session over the control channel and uses it to exchange cipher and HMAC keys to protect the data channel. TLS mode uses a reliability layer over the UDP connection for all control channel communication, while the data channel (over which encrypted tunnel data passes) is forwarded without mediation.
<b>Static Key Authorization</b>	Less secure than TLS mode, the static key mode does not require certificates or handshake protocols. It does require a preexisting secure channel with your peer to initially copy the key.



Field	Description
<b>Protocol</b>	Select UDP or TCP for the OpenVPN connection.
<b>Tunnel Type: Client</b>	
<b>Remote Host</b>	Remote OpenVPN server IP address.
<b>Remote Port</b>	Remote OpenVPN server port number.
<b>LZO Compression</b>	Compression method use for the VPN tunnel. Must match up with the OpenVPN remote server setup.
<b>CA PEM</b>	Certificate Authority (CA) file in PEM format. Also referred to as the root certificate.
<b>Client Certificate PEM</b>	Local peer's signed certificate in PEM format. Must be signed by a certificate authority whose certificate is in the <b>CA PEM file</b> . Each peer in an OpenVPN link running in TLS mode should have its own certificate and private key file.
<b>Client Key PEM</b>	Local peer's signed certificate in PEM format. Must be signed by a certificate authority whose certificate is in the <b>CA PEM file</b> . Each peer in an OpenVPN link running in TLS mode should have its own certificate and private key file.
<b>Tunnel Type: Server</b>	
<b>VPN Subnet</b>	Sets up an OpenVPN server that allocates addresses to clients out of the given network/netmask.
<b>VPN Netmask</b>	Sets up an OpenVPN that allocates addresses to clients out of the given network/netmask.
<b>Port</b>	Port number used for establishing the OpenVPN tunnel.
<b>CA PEM</b>	Certificate Authority (CA) file in PEM format. Also referred to as the root certificate.
<b>Diffie Hellman PEM</b>	Diffie Hellman parameters in PEM format. Use: <b>openssl dhparam -out dh1024.pem 1024</b> to generate you own, or use the existing dh1024.pem file included with the OpenVPN distribution. Diffie Hellman parameters may be considered public.
<b>Server Certification PEM</b>	Local peer's signed certificate in PEM format. Must be signed by a certificate authority whose certificate is in the <b>CA PEM file</b> . Each peer in an OpenVPN link running in TLS mode should have its own certificate and private key file.
<b>Server Key PEM</b>	Local peer's signed certificate in PEM format. Must be signed by a certificate authority whose certificate is in the <b>CA PEM file</b> . Each peer in an OpenVPN link running in TLS mode should have its own certificate and private key file.
<b>Tunnel Type: Custom</b>	
<b>Config</b>	User custom OpenVPN configuration. Refer to standard OpenVPN website <a href="https://openvpn.net">https://openvpn.net</a> for more information.

# Chapter 9: Administration

## Configuring Device Access

This section contains configurations that determine how the device can be accessed as well as security features that decrease susceptibility to malicious activity.

To display the **Access Configuration** window containing the fields described below, go to **Administration > Access Configuration**.

### HTTP Redirect to HTTPS

The device allows only secure access to its Web UI. This set of rules provides the optional convenience of automatically redirecting HTTP requests to the device's secure HTTPS port.

The device can be configured to allow HTTP access to its RESTFUL JSON API. Embedded devices that do not have SSL/TLS or HTTPS capabilities can then configure, monitor, and control the device.

See the [MTR API Developer Guide](#) for more information.

Field	Description
<b>Enabled</b>	Enables HTTP to HTTPS redirect which automatically redirects users trying to access the device via HTTP to HTTPS.
<b>Port</b>	The port on which the device listens for HTTP requests.
<b>Via LAN/Ethernet</b>	If checked, the device listens and responds to HTTP requests from the LAN.
<b>Via WAN/Cellular</b>	If checked, the device listens and responds to HTTP requests from the WAN.

### HTTPS

The device provides secure Web UI access to modify its configurations and execute actions.

Field	Description
<b>Port</b>	The port on which the device will listen for HTTPS requests.
<b>Via WAN/Cellular</b>	If checked, the device will listen and respond to HTTPS requests from the WAN. This increases susceptibility to malicious activity.
<b>Timeout Minutes</b>	Amount of time a user's session can remain dormant before automatically being logged out.
<b>Change Password</b>	Utility to change the user's password.

### SSH

The device's internal system can be accessed securely via SSH. This is intended for advanced troubleshooting and/or custom deployment solutions.

Field	Description
<b>Enabled</b>	Enables SSH redirect which automatically redirects users trying to access the device via SSH.
<b>Port</b>	The port on which the device listens for SSH requests.
<b>Via LAN/Ethernet</b>	If checked, the device listens and responds to SSH requests from the LAN.
<b>Via WAN/Cellular</b>	If checked, the device listens and respond to SSH requests from the WAN.

## ICMP

Internet Control Message Protocol (ICMP) is used by devices to send error messages such as that a requested service is not available or a host or device could not be reached. ICMP can also relay query messages.

Field	Description
<b>Enabled</b>	Enables ICMP responses.
<b>Respond to LAN/Via Ethernet</b>	If checked, the device will respond to ICMP traffic from the LAN, such as ping requests.
<b>Respond to WAN/Via Cellular</b>	If checked, the device will respond to ICMP traffic from the WAN, such as ping requests. This increases susceptibility to malicious activity.

## IP Defense

A set of rules that decreases susceptibility to malicious activity. If these settings are configured too strictly, they may interfere with non-malicious activity.

### DoS Prevention

This area of the Access Configuration window engages a set of rules at the firewall that prevents Denial-of-Service attacks by limiting the amount of new connection requests to the device.

Field	Description
<b>Enabled</b>	Enables DoS prevention.
<b>Per Minute</b>	Allowed number of new connections per minute until burst points are consumed. For example, if 60 new connections are received in a minute, decrement one burst point. If no more burst points, drop the packet.
<b>Burst</b>	Number of allowed burst for traffic spikes. A burst occurs when the Per Minute limit is reached. On a period where the Per Minute limit is not reached, one burst point is regained, up to the maximum.

### Ping Limit

This area of the Access Configuration window engages a set of rules at the firewall that aims to prevent ping flood attacks by limiting the number of ICMP requests to the device. These rules that mitigate the effects of a ping DoS on your device do not apply if ICMP is disabled.

Field	Description
<b>Enabled</b>	Enables the Ping Limit feature.
<b>Per Second</b>	Allowed number of pings per second before burst points are consumed. Once burst points run out, ICMP packets will be dropped.
<b>Burst</b>	Number of burst points. On a period where the Per Second limit is not reached, one burst point is regained, up to this maximum.

### Brute Force Protection

This feature tracks login attempts at the RESTFUL API level. Its purpose is to prevent Dictionary attacks that attempt to brute force the user's password.

Field	Description
<b>Enabled</b>	Enables the Brute Force Prevention feature.
<b>Attempts</b>	The number of failed attempts allowed before the user's account is locked out.
<b>Lockout Minutes</b>	The number of minutes an account is locked out before a new login attempt will be accepted.

After making all your desired changes, click **Submit**, then click **Save and Restart**.

## Generating a New Certificate

Because the device uses a self-signed website certificate, your browser shows a certificate error or warning. Ignore the warning and add an exception or add your device IP address to the trusted sites.

To generate a new certificate:

1. Go to **Administration > Certificate Management**. The **Certificate** window displays the details of the certificate that is currently used.
2. Click **Create** to open the **Generate Certificate** window.
3. In the **Common Name** field, enter the name, hostname, or IP address, depending on what you use to connect to the device. The web browser uses this field to check for a valid certificate.
4. In the **Days** field, enter the amount of days before the certificate will expire.
5. In the **Country** field, enter the 2-letter code for the country name.
6. In the **State/Province** field, enter the state or province for which the certificate is valid.
7. In the **Locality/City** field, enter the locality or the city for which the certificate is valid.
8. In the **Organization** field, enter the organization name for which the certificate is valid.
9. In the **Email Address** field, enter the email address of the person responsible for the device. Typically this is the administrator. This field may be left blank.
10. Click **Generate**. Wait until the certificate is generated. You may have to reboot to complete the operation.
11. To save your changes, click **Save and Restart**.

## Uploading a New Certificate

To upload a new certificate:

1. Go to **Administration > Certificate Management**. The Certificate window displays the details of the certificate that is currently used.
2. Click **Upload** to open **Upload Certificate** window.
3. Click **Choose File** to select a valid certificate to be uploaded.
4. Click **Save**. Wait until the file is uploaded.
5. To save your changes, click **Save and Restart**.

## Saving and Restoring Settings

To restore previous configuration settings to your device, to restore settings to their factory defaults, or to save the current configuration:

1. Go to **Administration > Save/Restore > Upload Configuration**.
2. To restore a configuration from a previously saved file, go to **Restore Configuration From File**:
  - a. Next to the **Restore Configuration** field, click **Browse**.
  - b. Navigate to the location where the configuration file is stored and select the desired file.
  - c. Click **Restore**. The device reboots.
3. To save your current configuration to a file, go to **Save Configuration To File**:
  - a. Click **Save**.
  - b. Navigate to the location where you wish to save the file and select location.
4. This option is only available if you had reset to user-defined configuration. (Also, holding the reset button on the device for 30 seconds overrides user-defined settings and resets to factory default.) To reset the device's configuration to the factory settings, go to **Reset to Factory Default Configuration**:
  - a. Click **Reset**.
  - b. A dialog box appears prompting you to confirm that you want to restore to factory default settings.
  - c. Click **OK**.
5. This option is only available if you set user-defined settings first. (Also, holding the reset button on the device for 5 seconds sets user-defined defaults) To restore the device's configuration to the user-defined configuration settings, go to **Reset to User-Defined Configuration**:
  - a. Click **Restore**.
  - b. A dialog box appears prompting you to confirm that you want to restore to a set of user-defined settings.
  - c. Click **OK**.
6. To set deployment-specific default settings, click **Set Current Configuration As User-Defined Default**.
  - a. A dialog box appears prompting you to confirm that you want to restore to a set of user-defined settings.
  - b. Click **OK**.
7. To save a current configuration:

- a. Click **Save**.
- b. A dialog box appears asking you if you want to open or save the configuration file. Click **Save**.
- c. Navigate to the location where you want to store the configuration. Click **Save**.
- d. A progress dialog box appears to indicate that the configuration is being saved. Click **Close**.

## Using the Debugging Options

The device has utilities to help troubleshoot and solve technical problems. You can set up your device:

- To automatically reboot itself at a particular time of day or use a particular offset in hours from boot.
- To record and report Syslog messages that can help you resolve potential issues with your device.

You can also communicate directly with the device's cellular radio. To do this:

1. From **Administration**, select **Debug Options**.
2. Click the down arrow to the far right of the Radio Terminal screen to view the terminal window.
3. Enter AT commands to the radio.

See also: Statistics Configuration Fields

## Configuring Remote Syslog

To enable and configure Remote Syslog to capture and send log data from your device, you must have local syslog software installed.

1. To activate **Remote Syslog**, go to **Administration > Debug Options > Logging** under **Remote Syslog**, check **Enabled**.
2. To enable a remote server to receive and store the device's log data, in the **IP Address** field, type the IP address of the desired server.
3. To determine the amount of log information that is collected, in the **Debug Log Level**, select the type of information from the values in the dropdown menu which includes: **Minimum**, **Error**, **Warning**, **Info**, **Debug**, and **Maximum**. The system will collect the type of information you specify. For example, **Maximum** will collect all the log data available while **Warning** will collect anything that is a warning or above that level.
4. To download syslog information directly from the device, click **Download**.
5. Click **Submit**.
6. To save your changes, click **Save and Restart**.

## Statistics Settings

To configure **Statistics**:

1. Go to **Administration > Debug Options > Statistics**.
2. Enter the **Save Timeout** in seconds.
3. Enter the **Save Data Limit** in megabytes.
4. To delete cell activity history, click **Delete Cellular History**.
5. To delete ethernet history, click **Delete Ethernet History**.
6. Click **Submit**.
7. To save your settings, click **Save and Restart**.

## Statistics Configuration Fields

The device saves the statistics periodically depending on the configured timeout and data limit. By default, the Save Timeout is set to 300 seconds and the Data Limit is set to 5 MB. For the default scenario, the device saves the data if more than 5 minutes has elapsed, or if more than 5 MB has been sent or received from the last check. The device checks these conditions every minute, but the data is saved only if one of the conditions is met.

Field	Description
Save Timeout	The device saves the statistical data when the desired timeout period has elapsed. Default is 300 seconds (5 minutes).
Save Data Limit	The device saves the statistical data if the data limit is reached. Default is 5 MB.
Delete Cellular History	Deletes all Cellular history on the device.
Delete Ethernet History	Deletes all Ethernet history on the device.

## Ping and Reset Options

### Perform a Ping Test

Ping allows you to test the IP address or URL to ensure it is operational.

To perform a ping test:

1. Go to **Administration > Debug Options > Ping**.
2. Enter the **IP address or URL** of the site you wish to ping.
3. Under **Network Interface**, choose from the available drop-down list options including: **ANY, CELLULAR, ETHERNET, and DIAL-UP**.
4. Click **Ping**.

### Reset Options

To reset the modem, go to **Administration > Debug Options > Reset Options**, click **Reset Modem**. If successful, the system displays a message confirming a successful reset.

# Chapter 10: Status and Logs

## Viewing Device Statistics

The device collects sent/received traffic data for WAN, Cellular, and Ethernet networks. The daily statistical data is stored on the device for a 365-day period. All data that is older than 365 days is automatically deleted.

1. From **Status & Logs** on the left side of the Web Management interface, select **Statistics**.
2. The application categorizes statistics about your device. To see statistics that appear in a particular category, click the appropriate tab.

**System**

**Ethernet**

**Cellular**

### Definitions

A data usage bar chart and a cumulative usage line chart are available for Ethernet and Cellular. The Data Usage bar chart also shows statistics for data sent and data received. The following list includes some definitions to help you understand some of the data. Not all of the available statistics are listed here or shown in every tab.

- **Total:** Total number of sent/received bytes for a 365-day period.
- **Today:** Total number of sent/received bytes for today.
- **Sessions:** Bytes
- **Packets:** Number of successfully transmitted (TX) and received (RX) packets.
- **Errors:** Number of errors that occurred. Possibly due to connection issues or network congestion.
- **Dropped:** Number of dropped packets. Possibly due to memory constraints.
- **Overruns:** Number of overruns that occurred. Possibly due to processing constraints.
- **Frame:** Number of invalid packets.
- **Carrier:** Number of signal modulation errors that occurred (possibly due to physical connection).
- **Collisions:** Number of packet collisions that occurred due to network congestion.
- **Queue Length:** Length of the transmit queue.

### Cumulative and Daily Usage

Click **Show Cumulative Usage** or **Show Daily Usage** to display the desired view. Default chart view is Daily Usage for 30-day period.

### Timeframe of Chart

Change the time frame for the chart by clicking **Configure**. In the dialog that appears, set the **Start Date** and **End Date**, then click **Finish**.

### Show Log

The associated run-time logs for this section.



## Service Statistics

On the Web Management interface side menu, click **Status & Logs > Services** to display the **Service Statistics** window. This window shows the configuration (enabled or disabled) and the status of the following services:

- DDNS
- SNTP
- Cellular RTC
- TCP/ICMP Keep Alive
- Dial-on-Demand
- Failover

# Chapter 11: Regulatory Information

---

## 47 CFR Part 15 Regulation Class B Devices

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.

**Warning:** Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## Industry Canada Class B Notice

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement Canadien sur le matériel brouilleur.

This device complies with Industry Canada license-exempt RSS standard(s). The operation is permitted for the following two conditions:

1. the device may not cause harmful interference, and
2. the user of the device must accept any interference suffered, even if the interference is likely to jeopardize the operation.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

## EMC, Safety, and R&TTE Directive Compliance



The CE mark is affixed to this product to confirm compliance with the following European Community Directives:

Council Directive 2014/30/EU on the approximation of the laws of Member States relating to electromagnetic compatibility;

and

Council Directive 2014/35/EU on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;

and

Council Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment;

and

Council Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

## EMC, Safety, and R&TTE Directive Compliance



The CE mark is affixed to this product to confirm compliance with the following European Community Directives:

Council Directive 2014/30/EU on the approximation of the laws of Member States relating to electromagnetic compatibility;

and

Council Directive 2014/35/EU on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;

and

Council Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment;

and

Council Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

## Approvals and Certifications

This device is an industry and/or carrier approved modem. In most cases, when integrated and used with an antenna system that was part of the MultiTech modem certification, additional approvals or certifications are not required for the device that you develop as long as the following requirements are met:

- **PTCRB Requirements:** The antenna system cannot be altered.
- **Model Identification:** The MultiTech model identification allows the carrier to verify the modem as one of its approved models. This information is located on the modem's label below the bar code.

## Canadian Limitations

**Notice:** This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

**Notice:** The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

## Limitations canadiennes

**Avis:** Cet équipement respecte les spécifications techniques des équipements terminaux d'Industrie Canada. Cette conformité est confirmée par le numéro d'enregistrement. L'abréviation IC précédant le numéro d'enregistrement signifie que l'enregistrement a été effectué conformément à une Déclaration de Conformité indiquant que les spécifications techniques d'Industrie Canada ont été respectées. Ceci n'indique pas que cet équipement a été approuvé par Industrie Canada.

**Avis:** L'IES (indice d'équivalence de la sonnerie) attribué à chaque terminal fournit une indication du nombre maximal de terminaux pouvant être connectés à une interface téléphonique. La terminaison d'une interface peut être constituée de n'importe quelle combinaison d'appareils à la seule condition que la somme des indices d'équivalence de sonnerie de l'ensemble des appareils ne dépasse pas cinq.

---

## Chapter 12: Environmental Notices

---

### REACH Statement

#### Registration of Substances

After careful review of the legislation and specifically the definition of an “article” as defined in EC Regulation 1907/2006, Title II, Chapter 1, Article 7.1(a)(b), it is our current view that Multi-Tech Systems, Inc. products would be considered as “articles.” In light of the definition in § 7.1(b) which requires registration of an article only if it contains a regulated substance that “is intended to be released under normal or reasonably foreseeable conditions of use,” our analysis is that Multi-Tech Systems, Inc. products constitute nonregisterable articles for their intended and anticipated use.

#### Substances of Very High Concern (SVHC)

Per the candidate list of Substances of Very High Concern (SVHC) published October 28, 2008 we have reviewed these substances and certify the Multi-Tech Systems, Inc. products are compliant per the EU “REACH” requirements of less than 0.1% (w/w) for each substance. If new SVHC candidates are published by the European Chemicals Agency, and relevant substances have been confirmed, that exceeds greater than 0.1% (w/w), Multi-Tech Systems, Inc. will provide updated compliance status.

Multi-Tech Systems, Inc. also declares it has been duly diligent in ensuring that the products supplied are compliant through a formalized process which includes collection and validation of materials declarations and selective materials analysis where appropriate. This data is controlled as part of a formal quality system and will be made available upon request.

## Restriction of the Use of Hazardous Substances (RoHS)



**Multi-Tech Systems, Inc.**

### **Certificate of Compliance**

#### **2011/65/EU**

Multi-Tech Systems, Inc. confirms that its embedded products comply with the chemical concentration limitations set forth in the directive 2011/65/EU of the European Parliament (Restriction of the use of certain Hazardous Substances in electrical and electronic equipment - RoHS).

These MultiTech products do not contain the following banned chemicals<sup>1</sup>:

- Lead, [Pb] < 1000 PPM
- Mercury, [Hg] < 1000 PPM
- Hexavalent Chromium, [Cr+6] < 1000 PPM
- Cadmium, [Cd] < 100 PPM
- Polybrominated Biphenyl, [PBB] < 1000 PPM
- Polybrominated Diphenyl Ether, [PBDE] < 1000 PPM

Environmental considerations:

- Moisture Sensitivity Level (MSL) =1
- Maximum Soldering temperature = 260C (in SMT reflow oven)

<sup>1</sup>Lead usage in some components is exempted by the following RoHS annex, therefore higher lead concentration would be found in some modules (>1000 PPM);

- Resistors containing lead in a glass or ceramic matrix compound.

## Waste Electrical and Electronic Equipment Statement

### **WEEE Directive**

The WEEE Directive places an obligation on EU-based manufacturers, distributors, retailers, and importers to take-back electronics products at the end of their useful life. A sister directive, ROHS (Restriction of Hazardous Substances) complements the WEEE Directive by banning the presence of specific hazardous substances in the products at the design phase. The WEEE Directive covers all MultiTech products imported into the EU as of August 13, 2005. EU-based manufacturers, distributors, retailers and importers are obliged to finance the costs of recovery from municipal collection points, reuse, and recycling of specified percentages per the WEEE requirements.

### **Instructions for Disposal of WEEE by Users in the European Union**

The symbol shown below is on the product or on its packaging, which indicates that this product must not be disposed of with other waste. Instead, it is the user's responsibility to dispose of their waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information

about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or where you purchased the product.

July, 2005



# Index

<b>A</b>		
antenna		
cellular devices.....	11	
HSPA+.....	12	
<b>C</b>		
Class B .....	42	
Industry Canada .....	42	
<b>D</b>		
device		
maintenance .....	14	
<b>E</b>		
Ethernet ports .....	15	
<b>F</b>		
FCC Notice		
Class B .....	42	
<b>H</b>		
hazardous substances .....	46	
HSPA+		
antenna.....	12	
<b>I</b>		
Industrie Canada .....	44	
Industry Canada .....	44	
Class B .....	42	
interférence des radiofréquences.....	13	
<b>L</b>		
LED Indicators .....	8	
<b>M</b>		
maintenance .....	14	
model location .....	43	
<b>P</b>		
packing list .....	6	
Ports Ethernet .....	15	
<b>R</b>		
radio frequency interference.....	13	
RoHS.....	46	
<b>S</b>		
safety.....	15	
RF interference .....	13	
service statistics .....	41	
static.....	14	
Statistics		
configuration fields .....	39	
sécurité.....	15	
interférences RF.....	13	
<b>U</b>		
UL listed power notice .....	15	