MultiConnect® eCell

MTE2-L12G2 User Guide

MultiConnect® eCell User Guide

Models: MTE2-L12G2

Part Number: S000767 Rev 1.0

Copyright

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.

The MultiTech products and the final application of the MultiTech products should be thoroughly tested to ensure the functionality of the MultiTech products as used in the final application. The designer, manufacturer and reseller has the sole responsibility of ensuring that any end user product into which the MultiTech product is integrated operates as intended and meets its requirements or the requirements of its direct or indirect customers. MultiTech has no responsibility whatsoever for the integration, configuration, testing, validation, verification, installation, upgrade, support or maintenance of such end user product, or for any liabilities, damages, costs or expenses associated therewith, except to the extent agreed upon in a signed written document. To the extent MultiTech provides any comments or suggested changes related to the application of its products, such comments or suggested changes is performed only as a courtesy and without any representation or warranty whatsoever.

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:	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others:	support@multitech.com	(800) 972-2439 or (763) 717-5863

Warranty

To read the warranty statement for your product, visit https://www.multitech.com/legal/warranty. For other warranty options, visit 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

Chapter 1 – Product Overview

About the MultiConnect eCell

The Multiconnect eCell (MTE2) is an affordable LTE and/or CBRS Private LTE Ethernet to Cellular Bridge used to enable devices with Internet service. It is a simple alternative to complex and expensive cellular routers in applications where advanced networking capabilities are already in place or are not required, but there is a need for remote access without using local wired networks.

Package Contents

Description	Quantity
MultiConnect eCell	1
Antenna	2
Power Adapter	1
Ethernet Cable	1
Four Rubber Feet	1
Mounting Stick	1
Quick Start	1

System Requirements

Network Requirements	▪ An external Ethernet device ▪ LTE and/or CBRS Private LTE ▪ Network ▪ Ethernet connection
Browser Requirements	▪ Microsoft Edge 83 or higher ▪ Internet Explorer 9.0 or higher ▪ Chrome 2.0 or higher ▪ Firefox 3.0 or higher ▪ Safari 3.0 or higher

LED Indicators

Item	Description
Power	**On:** Solid when the device is in normal operational mode.
	Off: No power.
	Flashing: Device is in firmware upgrade mode, recovery mode or needs troubleshooting.
SIM	**On:** SIM card detected and ready.
	Off: SIM card not present or not detected.
	Flashing: Detecting and Querying SIM card information.
Internet	**On:** Connection is established and active.
	Off: No active cellular connection.
	Flashing: Active data transferred via cellular.
Signal	**On:** Solid when there is a strong cellular signal.
	Off: No cellular signal.
	Flashing fast: Medium cellular signal.
	Flashing slow: Weak cellular signal.
Ethernet (On the Ethernet port)	**On:** Solid when there is an Ethernet connection.
	Off: No Ethernet connection.
	Flashing: Data is actively transmitting via the Internet.

Using DeviceHQ for Device Management

DeviceHQ is a cloud-based device management tool for remote monitoring, upgrades, and configuration AEP devices. For information on creating and using a DeviceHQ account, go to the http://www.multitech.net/developer/software/devicehq/.

Chapter 2 – Specifications

Category	Description
General	
Performance	4G LTE Cat 12
Frequency Bands	TDD B42/B43/B48
Radio	
Cellular	4G LTE CBRS
4G LTE Speed	
Packet Data	Up to 600 Mbps downlink/150 Mbps uplink (Actual speed measured at up to 300 Mbps downlink /up to 90 Mbps uplink)
Connectors	
Cellular	Two female SMA connectors
SIM Holder	Mini-SIM 2FF push push SIM
Power Requirements	
Voltage	9VDC to 32VDC (12 VDC @ 1A)
Physical Description	
Dimensions	3.74" x 2.76" x 1.2" (95 x 70 x 30.5 millimeters)
Weight	1.2 lbs. (0.54 Kg)
Environment	
Operating Temperature	-30° C to +70° C
Humidity	Relative humidity 10% to 93% non-condensing
Certifications, Compliance, Warranty	
FCC Compliance	FCC Part 15B and Part 96 (Band 48)
Network Compliance	LTE and/or CBRS Private LTE
Warranty	Two years

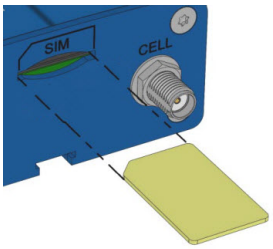
Chapter 3 – Installing and Using the eCell

Installing the SIM Card

This device requires a SIM card, which is supplied by your service provider. Install the SIM card before connecting antennas and cabling the device.

To install the SIM card:

1. Locate the SIM card slot on the side of the device. The slot is labeled SIM.
2. Slide the SIM card into the SIM card slot with the contact side facing down as shown. When the SIM card is installed, it locks into place.



Attaching Antennas and Cables

Note: Before powering up the device, enable DHCP on your computer's Ethernet port.

1. Connect the provided antennas to the connectors labeled CELL and AUX. Finger tighten. For best cellular performance, position the top of the antennas as far apart as possible.
2. Connect the Ethernet cable between the Ethernet ports on your computer and the device.
3. Connect 12V power adapter to the 2-pin terminal block power connector.
4. To power up the device, plug the power adapter into an electrical outlet.


MULTITECH

Using the Setup Wizard

Note: When using a 3G/4G network, verify a SIM card has been installed before powering on and starting setup.

Configure the device using the web UI. To access the web UI, enter the IP Address into your browser. The default IP Address is 192.168.2.1. If this has been changed, type in the new IP Address.

From the menu on the left, click **Wizard**.

1. Wait 60 seconds after connecting power. The computer gets IP address 192.168.2.100 via DHCP.
2. In a web browser, enter IP address 192.168.2.1.
3. Login using **admin** as both the **Username** and **Password**. If you are using the default password, it will prompt you to change it for future logins.
4. Click **Wizard** on the left.
5. Click **Next**.
6. **Change password**, if desired and click **Next**. (Recommended)
7. Set the device's **Time Zone** and click **Next**.
8. Enter and configure **APN**.
    a. Select **Manual Configuration**.
    b. Set **Country** to **Others**.
    c. Enter the **APN** provided by the SIM provider.
    d. Click **Next**.
9. Click **Apply**.
10. Wait a few minutes and check LED status. Power, SIM, Internet, and Signal LEDs are on when there is a live Internet connection. For more information on the LEDs, refer to *LED Indicators*.

After the device has a valid Internet connection, your computer automatically renews to the new IP address assigned to cellular connection and has full access to the Internet.

Chapter 4 – Basic Network

WAN and Internet Setup for 3G/4G

This device has Cellular WAN interfaces. Configure these individually to maximize Internet connection setup.

To configure Cellular WAN settings go to **Basic Network** > **WAN** on the menu on the left.

1. **Dial-up Profile**: Use information given by your 3G/4G data service provider to setup your connection including APN, dialed number, and account/password. Choose from **Manual Configuration** or **Auto-Detection**. When selecting **Manual Configuration**, configure the following:

   Country: Select the country. If using custom APN, select **Others**.

   Service Provider: Select the service provider. If using custom APN, select **Others**.

   APN: Verify predefined APN name or manually enter a custom APN name.

   PIN code: If your card needs to be unlocked before making a data connection, enter the SIM card PIN code (optional).

   Dial Number: Enter the ISP-provided dial number (optional).

   Account/Password: Enter the ISP-provided Account/Password (optional).

   Authentication: Choose **Auto, PAP,** or **CHAP** according to your ISP's authentication approach. If unsure, choose **Auto**.
2. **Roaming**: Allow internet connection when roaming.
3. **Data Usage Monitor**: Controls how much data is allowed for the 3G/4G connection during a defined cycle period. This helps avoid data overage charges from your service provider.

   Carrier Name: Name of the carrier or provider.

   Cycle Period: Cycle period duration in hours, weeks, or months.

   Cycle Start Date: Cycle period start date and time.

   Data Allowance: Set amount of data allowed during the cycle period.

   Halting Internet: Stop internet connection when the maximum data allowance is reached during the cycle period.
4. **Connection Control**: Setup WAN connection to be **Always on, Connect-On-Demand,** or **Connect Manually**.
5. **Time Schedule**: Set the WAN connection to be active for a certain predefined period. Choose from **Always** or **By Schedule**. If you choose **By Schedule**, add a new schedule at **System > Scheduling**.
6. **MTU**: Maximum Transmit Unit. Different WAN connections have different values. If unsure, use default value of **0** (Auto).
7. **IP Passthrough**: This is a bridge mode between a LAN device and a WAN interface. For security, assign a WAN interface IP Address to a fixed MAC address on the LAN device. In this mode, only one device is allowed on the LAN.
   - **Cellular Consecutive fails times:** Automatically reboots the modem when the cellular connection can't obtain an IP address after consecutive attempts. Enter the number of allowed cellular IP address failures before modem auto reboot.
   - **Network Monitoring:** To monitor the WAN interface connection status, check **Enable**. The system monitors when there is no activity for a defined period of time and resets the cellular connection.

- **Data Load Check**: Enable this option if there are continuous incoming and outgoing data packets passing through the WAN connection. If no data traffic is detected for the duration of the check interval, it disconnects and reconnects the cellular WAN connection.
- **Check Interval**: Indicate how often to check the data traffic on the WAN connection.

8. **NAT**: Enable or disable the NAT mechanism between the LAN and WAN interfaces. The default is disable, bridge mode only. In this mode, multiple LAN devices are supported.
   - **Cellular Consecutive fails times:** Automatically reboots the modem when the cellular connection can't obtain an IP address after consecutive attempts. Enter the number of allowed cellular IP address failures before modem auto reboot.
   - **Network Monitoring (keep alive):** To monitor cellular connection status, check **Enable**. The system prevents the embedded 3G/LTE modem from auto-timeout and disconnects after a period of inactivity.
   - **DNS Query or ICMP Checking:** Performs DNS query or ICMP on the cellular connection to determine if an active cellular connection is still valid.
   - **Data Load Check:** Enable this option if there are continuous incoming and outgoing data packets passing through the WAN connection. If no data traffic is detected for the duration of the check interval, it disconnects and reconnects the cellular WAN connection.
   - **Check Interval:** Indicates how often to perform DNS query or ICMP check on the WAN connection.
   - **Target 1/Target2:** Sets host for network monitoring keep alive check including **DNS1, DNS2,** or **Other** host (input IP address manually).
9. **AT Command:** Enable to allow an external TCP application to have direct access to an internal LTE radio using AT commands. The TCP port number needs to be set up between 1 to 65535.
10. **Init String 1 to 4:** Sets up custom AT commands to be sent to the LTE radio before making a cellular WAN connection.

Ethernet LAN

This device has one Ethernet LAN port to connect to one external Ethernet device. To configure, on the menu on the left go to **Basic Network** > **LAN**.

1. **Site Name:** Enter the Site name to identify the location when setting up DeviceHQ.
2. **LAN IP Address**: Enter the LAN's IP address. This IP address must be used as the computer's default gateway. This is also the IP address of the web UI. If you change this, type in the new IP address into a web browser to see the web UI.
3. **Subnet Mask**: Enter the LAN's subnet mask. This defines how many clients are allowed in one network or subnet. The default subnet is 255.255.255.0 and allows for a maximum of 254 IP addresses.

NAT

This option appears when NAT mode is selected in the WAN internet setup page. This mode allows multiple LAN devices to share one cellular WAN connection.

1. **Configuration:** Check option for NAT loopback. Allows you to access the WAN IP address from inside your LAN network.
2. **Virtual Server:** Allows you to setup the WAN IP to LAN IP mapping in order for remote access to LAN devices.
   a. **Public Port:** Enter the public IP port number.

b. **Server IP:** Enter the LAN device IP address.
c. **Private Port:** Enter the LAN device IP port number.
d. **Protocol:** Select TCP or UDP or both.
e. **Time Schedule:** Select a time schedule when this rule will take effect.
f. **Rule:** Check to enable the rule.

3. **DMZ (Demilitarized Zone) Host:** This is a host without the protection of a firewall. It allows a computer to be exposed to unrestricted 2-way communication from the Internet. If a specific application is blocked by NAT mechanism, you can designate that LAN computer as a DMZ host to solve this problem.
Note: This feature should only be used when necessary.

Routing

If there is more than one router and subnet, enable the routing function to allow packets to find proper routing paths and allow different subnets to communicate with each other.

Static Routing

For static routing, you can specify up to 16 routing rules. These rules allow you to determine which physical interface addresses are being used for outgoing data. For each rule, enter the destination IP address, subnet mask, gateway, and hop. Check **Enable** or **Disable**.

Dynamic DNS

To host a server on a changing IP address, you have to use dynamic domain name service (DDNS). DDNS maps the name of your host to the current IP address, which changes each time you connect to your ISP. Before you enable DDNS, you need to register an account on one of the DDNS servers in the provider list. To configure, from the menu on the left choose **Basic Network** > **Client/Server**.

1. **DDNS**: Check **Enable**.
2. **Provider**: The DDNS provider supports a service to bind your IP with a certain domain name.
3. **Host Name**: Register a domain name to the DDNS provider.
4. **Username/email**: Enter a username or email based on the DDNS provider requirements.
5. **Password/Key**: Enter a password or key based on the DDNS provider requirements.

DHCP Server

The gateway supports DHCP server to serve the DHCP requests from a LAN device. There is one default LAN IP address that is the same as the gateway LAN interface. The subnet mask is 255.255.255.0, and the IP Pool ranges from .100 to .200 as shown on the following DHCP Server List. To edit one DHCP server configurations, click **Edit** at the end of the DHCP server information.

There is one additional option to show the DHCP client list and IP addresses of local client hosts.

To configure, from the menu on the left choose **Basic Network** > **Client/Server**.

1. **DHCP Server Name**: Name of the DHCP server. This is optional.
2. **LAN IP Address**: Specify the local IP address of the enabled DHCP Server. This is the LAN IP address of this gateway for the DHCP server. Normally, this IP address is also the default gateway of local computers and devices.

3. **Subnet Mask**: Select the subnet mask for the DHCP server. The subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0/24. This means a maximum of 254 IP addresses are allowed in the subnet. However, the gateway's LAN IP occupies one of them.
4. **IP Pool Starting/Ending Address**: Specify the IP address pool's starting/ending addresses. When there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer.
   Note: The number of IP addresses in this IP pool must be less than the maximum number of subnet networks according to the set subnet mask.
5. **Lease Time**: DHCP lease time to the DHCP client.
6. **Domain Name**: This information is passed to the clients. This is optional.
7. **Primary DNS/Secondary DNS**: Assign DNS Servers. This is optional.
8. **Primary WINS/Secondary WINS**: Assign WINS Servers. This is optional.
9. **Gateway**: This is the alternate Gateway IP address. Assign another gateway to your computer when the DHCP server offers an IP address. For example, the gateway will assign an IP address to local computers but they will access the Internet through another gateway. This is optional.
10. **Server**: To activate the DHCP server, check **Enable**.

System Management (DeviceHQ)

Signing Up with DeviceHQ and Setting Up MTE2 to Communicate with DeviceHQ

1. Register and sign up a new account at https://www.devicehq.com.
2. Log in to https://www.devicehq.com and generate a device API key using the following steps:
   a. Select **Account info** (to the right of the account email address) and click **Edit**.
   b. Check **Device API Enabled** and click **Update Account**.
   c. Click **Generate new Device API Keys**.
   d. Write down and save "Device API Secret" and "Device API Auth Token", these two keys are required during MTE2 device setup.
      Note: **DO NOT** lose these keys since there is no way to see them again.

Setting Up MTE2 UI for DeviceHQ

MTE2 must be running firmware version 3.03 or above for DeviceHQ support. Download firmware from the website and upgrade the device before proceeding. https://www.multitech.com/models/92506980LF

1. In Basic Network, on the LAN Setup Screen: Enter and Define Site Name so it shows as Description in DeviceHQ
2. In Basic Network, on the System Management Setup Screen: DeviceHQ access setup requires:
   a. Check the **Enable** option.
   b. Enter **DeviceHQ account API secret** and **API Auth Token**.
   c. Click **Save**.

Wait for a few minutes. If MTE2 has an active cellular internet connection, it automatically checks in and registers with DeviceHQ. Log in to DeviceHQ and make sure the new MTE2 device shows up on your account.

Setting Up a New Firmware File on DeviceHQ

This is performed after logging in to DeviceHQ.

1. Click Files and click the **New Firmware** button.
2. Select model = **Unspecified**.
3. Enter the name and version number of the firmware file.
4. Choose the firmware BIN file.
5. Click the **Upload** button.
6. Make sure MD5 checksum matches on the firmware BIN file.

Pushing a Firmware Update to All Devices

This is performed after logging in to DeviceHQ.

1. Check all the devices.
2. Click **Tasks** and select **Upgrade Firmware**.
3. Select the firmware file you want to push to the devices.
4. Click **OK**.
   This schedules a new firmware push to all devices the next time they check in.

Pushing a Firmware Update to One Device

This is performed after logging in to DeviceHQ.

1. Click on the individual device to view more details.
2. Click **Schedule**, select **Upgrade Firmware**, and select the firmware file.
3. Click **OK** when prompted.

Setting Up a Configuration File on DeviceHQ

This is performed after logging in to DeviceHQ.

1. Click the **Files** tab.
2. Click **New Configuration**.
3. Enter the configuration file's name and description.
4. Choose the configuration ZIP file (zip up the configuration BIN file into a .zip file).
5. Click **Upload**.
   Note: MTE2 configuration BIN files must be created using an external device and saved as backup, then the BIN file must be a .zip file when uploaded to DeviceHQ. Name the ZIP file based on device description or serial number so it can be easily identified.

Pushing a Configuration File to a Single Device

1. Click on the individual device to view more details.
2. Click **Schedule**, select **Upgrade Config**, and select the config file.
3. Click **OK** when prompted.

Requesting Device Log Files

1. Click on the individual device to view more details.
2. Click **Schedule** and select **Request Device Logs**.
3. Click **OK** when prompted.

Requesting a Device Reboot

1. Click on the individual device to view more details.
2. Click **Schedule** and select **Reboot**.
3. Click **OK** when prompted.

MTE2 Data Usage with DeviceHQ

- Each time a device checks in, it can take up to 23 KB.
- Log file upload can vary depending on the size of the log files.
- Configuration file size can be up to 12 KB.
- MTE2 firmware file size is approximately 9 MB.

Chapter 5 – Advanced Network

Advanced Network

This section is only available when NAT mode is selected in the WAN cellular internet setup. Enable/disable firewall, Stealth Mode, SPI, and Discard PING from the WAN interface.

Configuration

- **Firewall:** Enable / Disable Firewall.

Packet Filters

Enable: When enabled, the router will perform IP packet filter based on rules defined.

Black List / White List: Select option to create black list to allow all traffics except for defined deny rules. White list is to deny all traffics except for the defined allow rules

Log Alert: When enabled, it will create log messages when it detect traffics matching with defined rules

Packet filter List: Enter and define rule based on black list / white list option selected above. The rule should be defined with rule name, from interface, to interface, source IP, destination IP, destination port, protocol, time schedule, rule enable.

MAC Control

Enable: When enabled, the router will perform Ethernet MAC address filter based on rules defined.

Black List / White List: Select option to create black list to allow all MAC addresses except for defined deny rules. White list is to deny all MAC addresses except for the defined allow rules.

Log Alert: When enabled, it will create log messages when it detect MAC address matching with defined rules

Known MAC address for LAN PC list: Select and clone MAC address that are known and detected by the eCell device

MAC Control Rule List: Enter and define rule based on black list / white list option selected above. The rule should be defined with rule name, MAC address, time schedule, rule enable.

Options

- **Stealth Mode:** When enabled, the router will not respond to port scans from the WAN. This makes the router less susceptible to discovery and attacks.
- **SPI (Stateful Packet Inspection):** Also known as dynamic packet filtering. This helps to prevent cyber attacks by tracking more states per session. It validates that the traffic passing through that session conforms to the protocol.
- **Discard PING from WAN side:** When enabled, this gateway won't reply to any ICMP request packets from the WAN side.

Chapter 6 – System

System

This section includes system information, system logs, system tools (i.e. firmware updates), scheduling, and external syslog server setup.

Change Password

1. **Old, New, and Confirmation Password**: To change your password, type in your old password, then enter in the new password in the new password and confirm password fields. Click **Save** to store your settings or **Undo** to cancel the changes.
2. **Administrator Time-out**: Other options allow you to set when there are no activities on the web user interface.
3. **Telnet with CLI**: Check to **Enable** CLI access via LAN or WAN.
4. **Connection Type**: Check to **Enable** Telnet or SSH access via LAN or WAN. The Telnet and SSH access IP port number can be configured to use custom port.
5. **Options**: Setup local or remote HTTP or HTTPS web UI access. Enter unique remote IP address and subnet mask to restrict remote web UI access. Enable web UI access for LAN and/or WAN interfaces.

System Information

This section displays System Information for the WAN interface, current date and time, device serial number and MAC address.

System Status

System Status displays and captures log information. It also allows log files to be sent to an external syslog server.

1. **Web Log**: Check **Enable** for System, Attacks, Drop, and Debug categories, then click **Save**. Click **View** to display or download log files.
2. **Syslogd**: Check to **Enable** logging to an external syslog server. The external syslog server's IP address can be configured using the **External Servers** option.

System Tools

Options to setup system time, perform firmware updates, ping test, trace route test, reboot or schedule a reboot, reset to factory defaults, wake up on LAN, and backup configuration settings.

- **System Time**: Configure the time zone. You can select sync current time and date with external time server or local PC time.
- **Firmware Upgrade/Configuration Restore**: Perform firmware upgrade or restore a backup configuration file.

Note: To check the current firmware version, refer to the top of the page after login.

- **Ping Test (NAT mode only)**: Enter external host IP address and perform ping test.
- **Tracert Test (NAT mode only)**: Enter external host IP address and perform trace route test.
- **Reboot**: Select reboot now or set a schedule for an auto-reboot to occur.
- **Reset to Default**: Resets all settings back to factory defaults.

- **Backup/Restore Configuration Settings**: Save all current settings to a configuration file or restore a backup configuration file.

Scheduling

1. **Enable** the schedule function and setup a rule for each schedule. The rule can be used in many other functions, such as scheduling an auto-reboot, scheduling an auto WAN connectivity, etc.
2. Click **Save** to store all schedule settings.

External Servers

1. Click **Add** to add and configure an external syslog server. The server will allow logging to be captured via an external syslog server.
2. Click **Save** to save all the server settings.

Chapter 7 – Antenna

Devices were approved with the following antenna:

Manufacturer:	Wieson
Description:	LTE Antenna with SMA-Male Connector
Model Number	GY115IE002-001

MultiTech ordering information:

Model	Quantity
ANLTE4-1HRA	1
ANLTE4-2HRA	2
ANLTE4-10HRA	10
ANLTE4-50HRA	50

Antenna Specifications

Category	Description
Frequency Range	0.698 - 0.96 GHz 1.710 - 2.170 GHz 2.30 - 2.69 GHz
VSWR	3:1 maximum
Gain	2.06 dBi
Impedance	50Ω nominal
Radiation	Omni-directional
Polarization	Linear, vertical

Chapter 8 – Safety Warnings

Ethernet Ports

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

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.

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).

Chapter 9 – 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.

FCC Interference Notice

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.

FCC Grant Information

FCC Class B Part 15

FCC Identifier:	XMR201909EG12GT
Equipment Class:	Part 15 Class B Computing Device Peripheral
Notes:	LTE-A Cat 12 LGA Module
Approval:	Single Modular

FCC Part 96

FCC Identifier:	XMR201909EG12GT
Equipment Class:	Citizens Band End User Devices
Notes:	LTE-A Cat 12 LGA Module
Approval:	Single Modular

Grant Notes	FCC Rule Part	Frequency Range (MHz)	Output Watts	Frequency Tolerance	Emission Designator
EP	96	3560.0 - 3590.0	0.052	0.001 PM	37M3G7D
EP	96	3560.0 - 3590.0	0.05	0.001 PM	37M3D7W
EP	96	3552.5 - 3697.5	0.125	0.001 PM	4M46G7D
EP	96	3552.5 - 3697.5	0.107	0.001 PM	4M46D7W
EP	96	3552.5 - 3697.5	0.086	0.001 PM	4M46D7W
EP	96	3555.0 - 3695.0	0.129	0.001 PM	8M90G7D
EP	96	3555.0 - 3695.0	0.107	0.001 PM	8M91D7W
EP	96	3555.0 - 3695.0	0.086	0.001 PM	8M91D7W
EP	96	3557.5 - 3692.5	0.13	0.001 PM	13M4G7D
EP	96	3557.5 - 3692.5	0.107	0.001 PM	13M4D7W
EP	96	3557.5 - 3692.5	0.087	0.001 PM	13M4D7W
EP	96	3560.0 - 3690.0	0.135	0.001 PM	17M8G7D
EP	96	3560.0 - 3690.0	0.111	0.001 PM	17M8D7W
EP	96	3560.0 - 3690.0	0.09	0.001 PM	17M8D7W

Output power listed is EIRP. Single modular approval for mobile RF exposure conditions. Co- transmission of this module with other transmitters requires a separate evaluation according to FCC multi-transmitter procedures. The host integrator must follow the integration instructions provided by the module manufacturer and ensure that the composite-system end product complies with the FCC requirements by a technical assessment or evaluation to the FCC rules and to KDB Publication 996369. The module antenna(s) must be installed to meet the RF exposure compliance separation distance of 20 cm and any additional testing and authorization process as required. The module grantee is responsible for providing the documentation to the system integrator on restrictions of use, for continuing compliance of the module. The host integrator installing this module into their product must ensure

that the final composite product complies with the FCC requirements by a technical assessment or evaluation to the FCC rules, including the transmitter operation and should refer to guidance in KDB 996369. Approval is limited to OEM installation only. This grant is valid only when the device is sold to OEM integrators and the OEM integrators are instructed to ensure that the end user has no manual instructions to remove or install the device. This device supports 5/10/15/20 MHz bandwidth modes for LTE B42/B43/B48 and uplink intra-band carrier aggregation for LTE B42.

Restriction of the Use of Hazardous Substances (RoHS)

Multi-Tech Systems, Inc.

Certificate of Compliance

2015/863

Multi-Tech Systems, Inc. confirms that its embedded products comply with the chemical concentration limitations set forth in the directive 2015/863 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[1]:

- Lead, [Pb] < 1000 PPM
- Mercury, [Hg] < 100 PPM
- Cadmium, [Cd] < 100 PPM
- Hexavalent Chromium, [Cr+6] < 1000 PPM
- Polybrominated Biphenyl, [PBB] < 1000 PPM
- Polybrominated Diphenyl Ethers, [PBDE] < 1000 PPM
- Bis(2-Ethylhexyl) phthalate (DEHP): < 1000 ppm
- Benzyl butyl phthalate (BBP): < 1000 ppm
- Dibutyl phthalate (DBP): < 1000 ppm
- Diisobutyl phthalate (DIBP): < 1000 ppm

Environmental considerations:

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

[1]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

Note: This statement may be used in documentation for your final product applications.

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