



# MultiConnect<sup>®</sup> CBRS Wi-Fi AP

---

MTCAPW-L12G2 Admin Guide



## MultiConnect® CBRS WiFi AP Admin Guide

Models: MTCAPW-L12G2

Part Number: S000792 version 1.1

### 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 © 2021 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.

### 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:	<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 <https://www.multitech.com/legal/warranty>. 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>5</b>
MultiConnect CBRS Wi-Fi AP.....	5
About this document .....	5
Package Contents.....	5
Package Contents.....	5
System Requirements .....	5
MTCAPW Specifications .....	5
All Models .....	5
LED Indicators .....	7
Antenna.....	8
Antenna Specifications .....	8
<b>Chapter 2 – Installation.....</b>	<b>9</b>
.....	9
<b>Chapter 3 – Setting Up and Onboarding Devices .....</b>	<b>12</b>
Using the Setup Wizard.....	12
Using DeviceHQ for Device Management.....	12
System Management (DeviceHQ).....	12
Signing Up with DeviceHQ and Setting Up MTCAPW to Communicate with DeviceHQ .....	12
Setting Up MTCAPW UI for DeviceHQ .....	13
Setting Up a New Firmware File on DeviceHQ .....	13
Pushing a Firmware Update to All Devices .....	13
Pushing a Firmware Update to One Device .....	13
Setting Up a Configuration File on DeviceHQ.....	14
Pushing a Configuration File to a Single Device.....	14
Requesting Device Log Files.....	14
Requesting a Device Reboot .....	14
MTCAPW Data Usage with DeviceHQ.....	14
System Management (TR-069) .....	15
DeviceHQ Onboarding .....	16
Local Bulk Onboarding .....	16
Device Onboard Troubleshooting .....	17
<b>Chapter 4 – Device Management .....</b>	<b>18</b>
WiFi Setup.....	18
Wireless Client List.....	19
Advanced Configuration.....	19
Status .....	19
Network Status .....	19

WiFi Status .....	19
LAN Client List .....	20
WAN and Internet Setup for 4G .....	20
Ethernet LAN .....	21
NAT.....	21
Routing.....	22
Static Routing .....	22
Dynamic DNS.....	22
DHCP Server .....	22
Advanced Network.....	23
Configuration .....	23
Packet Filters.....	23
MAC Control.....	23
Options.....	24
<b>Chapter 5 – System .....</b>	<b>25</b>
System.....	25
Change Password.....	25
System Information.....	25
System Status.....	25
System Tools .....	25
Scheduling.....	26
External Servers .....	26
<b>Chapter 6 – Safety/Regulatory Information .....</b>	<b>27</b>
Ethernet Ports .....	27
Radio Frequency (RF) Safety .....	27
Interference with Pacemakers and Other Medical Devices .....	27
Potential interference .....	27
Precautions for pacemaker wearers .....	27
47 CFR Part 15 Regulation Class B Devices .....	28
FCC Interference Notice.....	28
FCC Grant Information .....	29
FCC Class B Part 15.....	29
FCC Part 96.....	29
Restriction of the Use of Hazardous Substances (RoHS) .....	31
Waste Electrical and Electronic Equipment Statement .....	31
WEEE Directive.....	31
Instructions for Disposal of WEEE by Users in the European Union .....	31

# Chapter 1 – Product Overview

## MultiConnect CBRS Wi-Fi AP

This Admin Guide provides information on the MultiConnect® CBRS Wi-Fi AP. The Multiconnect CBRS Wi-Fi AP is a 4G/LTE CBRS Wi-Fi to Cellular access point used to enable devices with internet service. It is an alternative to cellular routers in applications where there is a need for remote access without using local wired networks.

### About this document

This document contains regulatory, and safety notices only for the following MultiConnect CBRS Wi-Fi AP models.

- MTCAPW-L12G2-A600VA-CUA

## Package Contents

### Package Contents

Description	Quantity
MultiConnect CBRS Wi-Fi AP modem and Stand	1
Cellular Antenna	2
Power Adapter	1
Ethernet Cable	1
Four Rubber Feet	1
Quick Start	1
Mounting Template	1

## System Requirements

Network Requirements	<ul style="list-style-type: none"> <li>■ CBRS Private LTE</li> </ul>
Browser Requirements	<ul style="list-style-type: none"> <li>■ Microsoft Edge 83 or higher</li> <li>■ Internet Explorer 9.0 or higher</li> <li>■ Chrome 2.0 or higher</li> <li>■ Firefox 3.0 or higher</li> <li>■ Safari 3.0 or higher</li> </ul>

## MTCAPW Specifications

MTCAPW specifications depend on the hardware configuration for your model.

### All Models

<b>Performance</b>
--------------------






Standards	CBRS 4G LTE Cat 12
	TDD LTE Bands 42, 43, and 48 for CBRS/private LTE
	2xCA (UL) B42+B42
	2xCA (DL) B42+B42, B48+B48
	3xCA (DL) B42+B42+B42; B48+B48+B48
	DL 256QAM: Y
	3FF Micro SIM
Wi-Fi (2 - Internal Antennas)	2.4GHz 802.11bgn
<b>Physical Description</b>	
Dimensions	5.3 x 6.5 x 1.4 (in)
Weight	0.6 lbs
<b>Connectors</b>	
Connectors	1 RJ-45 Ethernet port
	2 LTE antenna connectors
<b>Power Requirements</b>	
Input Voltage	12V DC (2.5mm connector)
Power Consumption	2.64Watts = 0.22A @ 12V
<b>Environment</b>	
Operating Environment	-10° to +50° C*
Storage Environment	-40° to +85° C
Relative Humidity	20 to 90% non-condensing
<b>Certifications</b>	
EMC Radio Compliance	FCC Part 15 Class B
	OnGo FCC Part 96 CBRS

UL listed at 40° C, limited by AC power supply. Product has been tested to +50° C excluding power supply.

## LED Indicators

### Device LED Status Indicators

Page 6

LED	Icon	Description
POWER		<p><b>On:</b> Device is in normal operational mode</p> <p><b>Off:</b> No power</p> <p><b>Flashing:</b> Device is in firmware upgrade mode, recovery mode, or needs troubleshooting</p>
SIM		<p><b>On:</b> SIM card detected and ready</p> <p><b>Off:</b> SIM card not present or not detected</p> <p><b>Flashing:</b> Detecting and querying SIM card information</p>
INTERNET		<p><b>On:</b> Device 4G is established and active</p> <p><b>Off:</b> No active cellular connection</p> <p><b>Flashing:</b> Active data transferred via cellular</p>
SIGNAL		<p><b>On:</b> Device has a strong cellular signal</p> <p><b>Off:</b> No cellular signal</p> <p><b>Fast Flash:</b> Medium cellular signal</p> <p><b>Slow Flash:</b> Weak cellular signal</p>
WIFI		<p><b>On:</b> Device Wi-Fi enabled and active</p> <p><b>Off:</b> Wi-Fi disabled</p> <p><b>Flashing:</b> Active data transferred via Wi-Fi</p>
LAN (LED on the LAN port)	N/A	<p><b>On:</b> Device has a LAN connection</p> <p><b>Off:</b> No LAN connection</p> <p><b>Flashing:</b> Data actively transmitting via the connection</p>

## 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

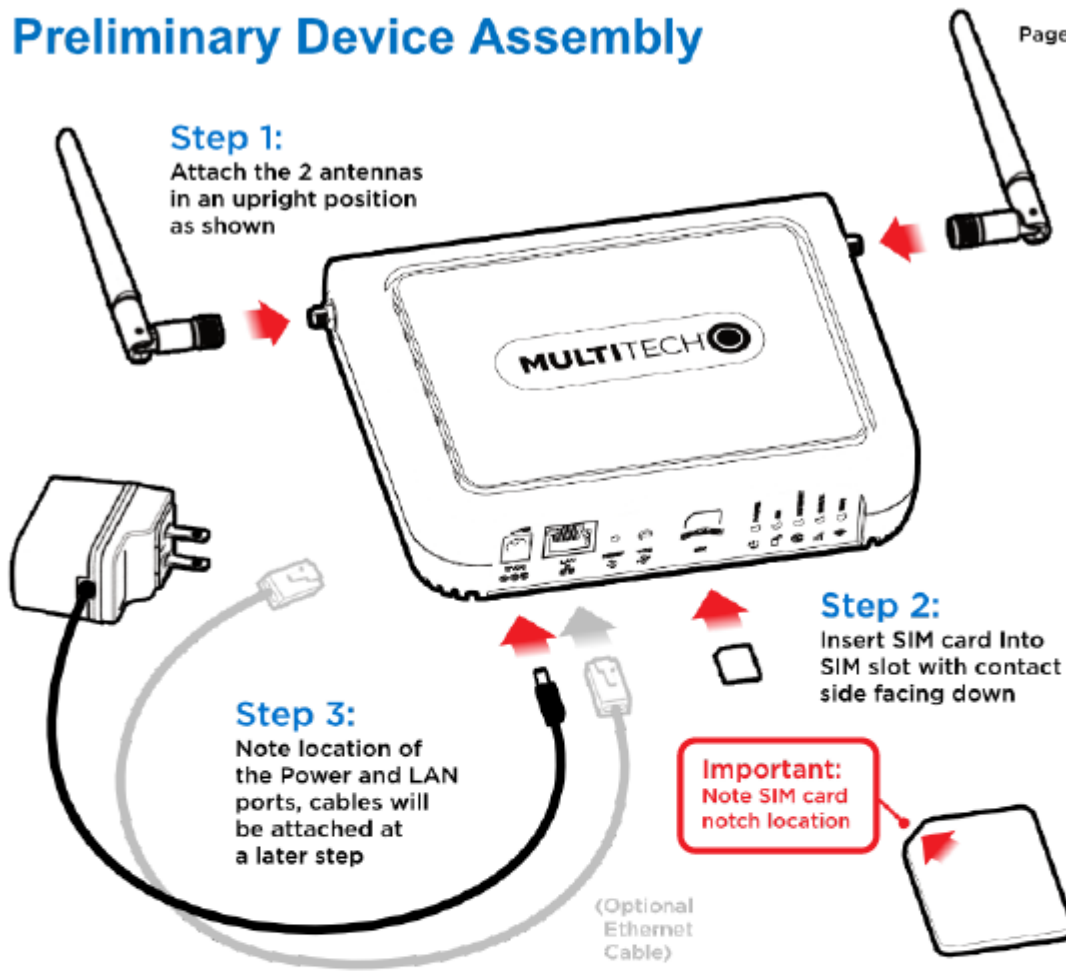
Category	Description
Frequency Range	3.5 - 3.8 GHz
VSWR	3:1 maximum
Gain	1.27 dBi
Impedance	50Ω nominal
Radiation	Omni-directional
Polarization	Linear, vertical



## Chapter 2 – Installation

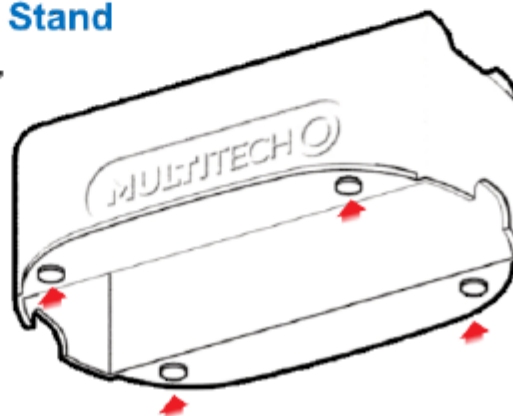
### Preliminary Device Assembly

Page 3



### Prepare Vertical Stand

If using the vertical stand, attach the 4 rubber feet to the bottom of flanges as shown



## Establish a Wireless Connection

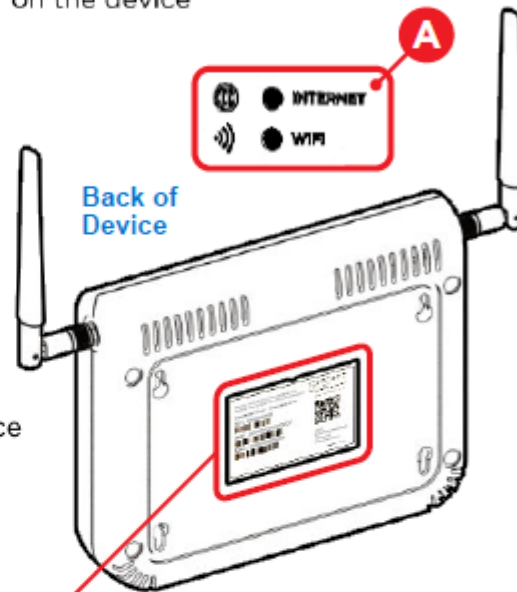
Be certain the following steps have been completed prior to wireless connection:

- Attach two cellular antennas to the two SMA threaded connectors
- Insert 3FF micro SIM card into SIM slot with contact side facing down
- Attach power blade to power adapter and power adapter to the device
- Plug power adapter into outlet to power on the device

### Using Wi-Fi to Connect Device

To perform Wi-Fi connection on your Wi-Fi client:

- Confirm INTERNET and WIFI LEDs are active,
- Scan Wi-Fi QR code with a compatible mobile device, or
- Select the Wi-Fi SSID and enter password printed on the back of device or, follow the instructions provided with a WPS compatible Wi-Fi client and use the device WPS push-button



MODEL: MTCAPW-L12G2-A600VA-CUA  
ORDER P/N: MTCAPW-L12G2-A600VA-CUA

SKU#92507151LF DOM:0000.00.00

S/N: 000000000

IMEI: 0000000000000000

MAC: 000000000000

Power Requirements  
12Vdc @1A

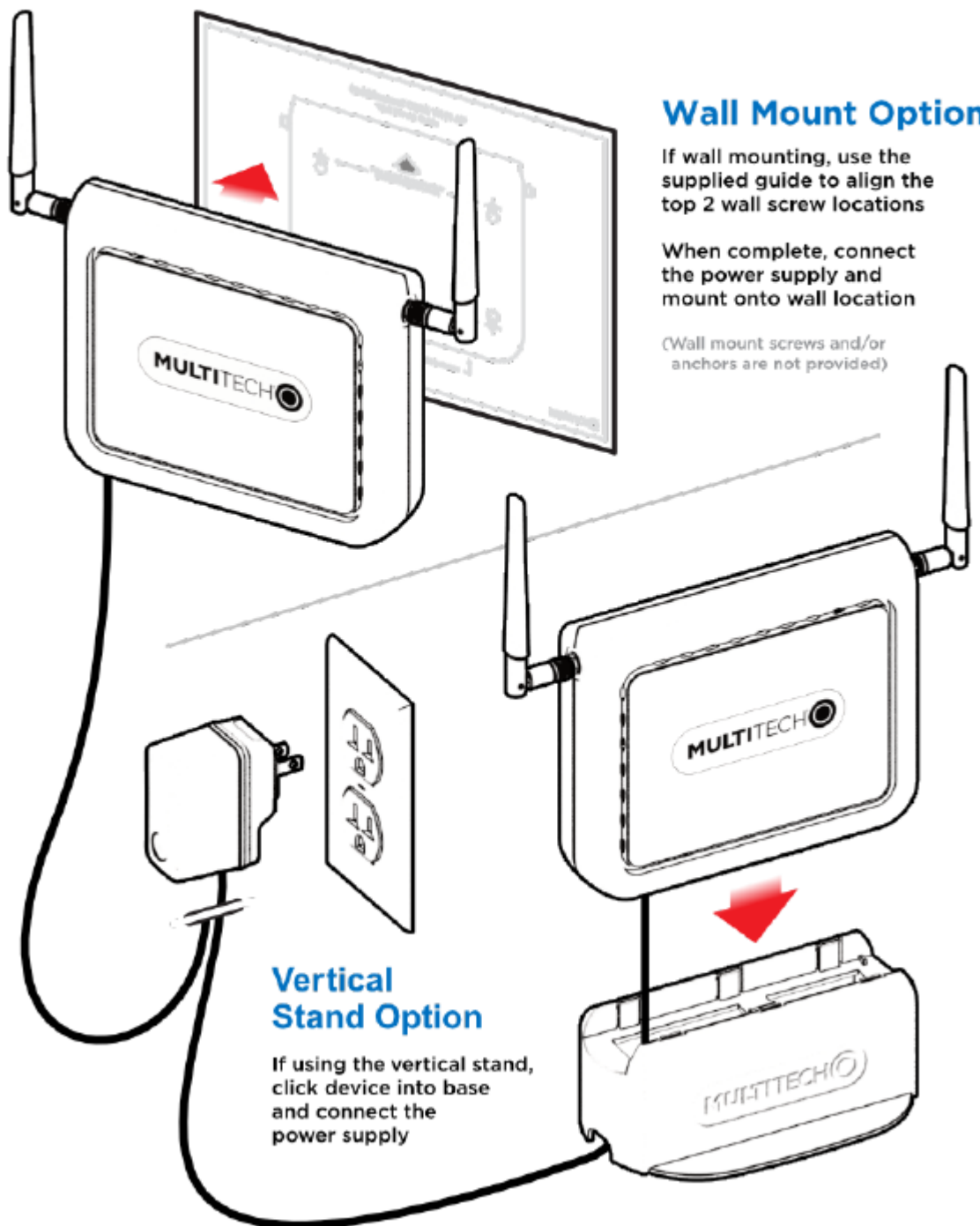
www.multitech.com

SSID:  
MTCAPW-00000000  
Password:  
XXXXXXXXXXXXXX

Made In Taiwan

## Choose Wall Mount or Vertical Stand to Support Device

Page 4



## Chapter 3 – Setting Up and Onboarding Devices

---

### Using the Setup Wizard

**Note:** When using a 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.

### Using DeviceHQ for Device Management

DeviceHQ is a cloud-based device management tool for remote monitoring, upgrades, and configuration mPower devices. For information on creating and using a DeviceHQ account, go to the

<http://www.multitech.net/developer/software/devicehq/>.

**Note:** If you are not using DeviceHQ as the management system, disable DeviceHQ as the management system within the software. Once the Setup Wizard has been completed, from the left menu select **Basic Network > System Management** then deselect the "Enable" box on the top row of the configuration table.

### System Management (DeviceHQ)

#### Signing Up with DeviceHQ and Setting Up MTCAPW 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 MTCAPW device setup.

**Note:** **DO NOT** lose these keys since there is no way to see them again.

## Setting Up MTCAPW UI for DeviceHQ

MTCAPW must be running firmware version 4.03 or above for DeviceHQ support. If new firmware becomes available, download firmware from the website and upgrade the device before proceeding.

<https://www.multitech.com/models/92507151LF>

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 MTCAPW has an active cellular internet connection, it automatically checks in and registers with DeviceHQ. Log in to DeviceHQ and make sure the new MTCAPW 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. **Log In:** Log in into device. Change default password on first log in.
2. **Change Settings:** Navigate web UI settings and make changes based on use case and applications.
3. **DeviceHQ:** Setup DeviceHQ with individual API key pair and change the check-in interval.
4. **SSID / Password :** Updated WiFi SSID and password if required. WiFi QR code on physical device will become invalid if changes are made to the SSID and password
5. **Telnet / SSH:** Disable Telnet / SSH if not in use.
6. **Download** Click **Backup** to download the configuration file
7. **Rename:** Rename configuration file as needed.
8. **Zip:** Zip up configuration file before upload to DeviceHQ.
9. Upload device configuration ZIP file to DeviceHQ.
  - a. Login to [www.devicehq.com](http://www.devicehq.com)
  - b. click on Files button
  - c. click on New Configuration Button
  - d. enter Name, Description, Model = MTCAPW, Choose File, and upload configuration ZIP file that is created in **step 8**

## 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.

## MTCAPW 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.
- MTCAPW firmware file size is approximately 9 MB.

## System Management (TR-069)

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices, like this gateway device. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). The Security Gateway is such CPE.

TR-069 is a customized feature and require working with ISP and ACS provider in order to be fully compatible.

In "TR-069" setup page, you must specify the related information for your security gateway to connect to the ACS. Drive the function to work by specifying the URL of the ACS server, the account information to login the ACS server, the service port and the account information for connection requesting from the ACS server, and the time interval for job inquiry. Except the inquiry time, there are no activities between the ACS server and the gateways until the next inquiry cycle. But if the ACS server has new jobs that are expected to do by the gateways urgently, it will ask these gateways by using connection request related information for immediate connection for inquiring jobs and executing.

TR-069 Settings		
TR-069	The box is unchecked by default	Check the <b>Enable</b> box to activate TR-069 function
ACS URL	A must be filled setting	You can ask ACS manager to provide ACS URL and manually set
ACS Username	A must be filled setting	You can ask ACS manager to provide ACS username and manually set
ACS Password	A must be filled setting	You can ask ACS manager to provide ACS password and manually set
Connection Request Port	A must be filled setting By default 8099 is set	You can ask ACS manager to provide ACS Connection Request Port and manually set. Value Range : 0-65535
Connection Request User Name	A must be filled setting	You can ask ACS manager to provide AVS Connection Request User Name and manually set
Connection Request Password	A must be filled setting	You can ask ACS manager provide ACS Connection Request Password and manually set
Inform	The box is checked by default The interval value is 300 by default	When the Enable box is checked, the gateway (CPE) will periodically send inform messages to ACS Server according to the interval setting. Value Range: 0-86400 for Inform interval
STUN Settings		
STUN	The box is unchecked by default	Check the <b>Enable</b> box to activate STUN function

STUN Settings		
Server Address	String format: any IPv4 address It is an optional Item	Specify the IP address for the expected STUN Server
Server Port	An optional setting 3478 is set by default	Specify the port number for expected STUN Server. Value Range: 1-65535
Keep Alive Period	An optional setting 0 is set by default	Specify the keep alive time period for the connection with STUN Server. Value Range : 0-65535
Save	N/A	Click <b>Save</b> to save the settings
Undo	N/A	Click <b>Undo</b> to cancel the modification

## DeviceHQ Onboarding

Initial factory out of the box setup and using DeviceHQ onboarding process

### DeviceHQ account setup

1. End user login, sign up and register to DeviceHQ with new account
2. End user need to generate a new Device / Machine API key pair
3. End user need to create a MTCAPW configuration file with the machine API key pair in step 2
4. End user upload MTCAPW zipped configuration file created in step 3 to DeviceHQ

### MTCAPW device setup require only power on and check LED status

5. Install CBRS SIM card
6. Attach two LTE antennas
7. Power on the device
8. Wait for two minutes and check all the LEDs on the device to indicate active wifi and internet connection
9. MTCAPW will automatically register to DeviceHQ after active internet connection

### End user claiming the MTCAPW on DeviceHQ

10. Login to DeviceHQ
11. Go to URL <https://www.devicehq.com/devices/claiming#/>
12. Enter the serial number of the MTAPW that just checked in above
13. Assign device configuration file in step 4 to the device serial number selected
14. Power off/on the device and wait for a few minutes so device will auto check in, get the new configuration file, apply the new configuration file and auto reboot. If everything is successful, the device will now show up in the end customer DeviceHQ account

## Local Bulk Onboarding

Initial factory out of the box setup and local onboarding process: Windows 10 PC setup and third parties SW need to be installed.

- Install Windows terminal SW: <https://tssh2.osdn.jp/index.html.en>
- Install Windows web server SW: <http://nginx.org/en/docs/windows.html>



- setup PC Ethernet with static IP 192.168.2.2

### DeviceHQ account setup

1. Login, sign up and register to DeviceHQ with a new account
2. Need to generate a new Device / Machine API key pair
3. Need to create a MTCAPW mater configuration file with the machine API key pair in step 2 and all other settings
4. Test out device with the master configuration file to make sure everything is working based on customer requirements
5. After master configuration file is create, copy the configuration BIN file to the web server folder that was created above with the Windows Web server

### MTCAPW device setup

1. Connect Windows PC to device via Ethernet.
2. Make sure Windows web server is running.
3. Power on device.
4. Wait for 40 seconds, run Windows Terminal SW and Telnet into device on IP 192.168.2.1 / port 23, login with default = admin and password = admin
5. At the device command prompt, issue command: reset —o http://192.168.2.2/configname.bin
6. Power down the device.

## Device Onboard Troubleshooting

1. Connect Windows PC to device via Ethernet.
2. Install SIM and antennas.
3. Ensure live CBRS network is available.
4. Power on device, ensure all LEDs indicate active cellular and wifi signals.
5. Login to device and check all settings to ensure they match the relative master configuration file.
6. If DeviceHQ is configured, ensure device is displayed on DeviceHQ.

# Chapter 4 – Device Management

## WiFi Setup

The WiFi settings allow you to set the wireless LAN configuration. Once the configurations is complete, your device will be ready to support your local WiFi devices.

This allows you to connect wired and wireless devices with NAT. In this mode, the gateway is a WiFi AP and a hotspot. With NAT, all wireless clients don't need public IP addresses. The following settings are available under WiFi configuration for AP Router Mode:

- **WiFi Module:** Enables the wireless function.
- **Green AP:** When there is no wireless traffic, enable **Green AP** to reduce power consumption.
- **Time Schedule:** The wireless radio can be turned off on a schedule. By default, it is always on when the wireless module is enabled. To add a schedule rule, go to **System > Scheduling**.
- **Network ID (SSID) & Broadcast:** Network ID identifies the wireless LAN. Client stations can roam freely over this and other access points with the same Network ID. If the Broadcast option is unchecked, wireless clients can't find the gateway through a wireless network scan.
- **WLAN Partition:** Enabling this option separates the wireless clients so they can't communicate with each other but can access the internet and other Ethernet LAN devices.
- **Channel:** The default radio channel number is set to **Auto**. To reduce radio interference, choose a channel that is not used in your environment.
- **WiFi System:** The default setting is **B/G/N mixed**. You can also choose **N only** or **G/N Mixed**.
- **Authentication and Encryption:** Select one of the following authentications to secure your wireless network:

Authentication Type	Description
Open	This mode consists of two communications, an authentication request by the client and an authentication response from the AP/router. In this mode, only <b>None</b> or <b>WEP</b> are available for encryption type.
Shared	Both stations in a shared authentication must have the same shared key or passphrase. This key must be manually set on both the client and the AP/router.
Auto	Automatically sets the appropriate authentication method based on the WiFi client.
WPA-PSK	The available encryption types for this authentication are <b>TKIP</b> , <b>AES</b> , or <b>TKIP/AES</b> . In this mode, you don't need an additional RADIUS server for user authentication.
WPA	In this mode, specify the IP address and port number for the RADIUS server. The key value is shared by the device and RADIUS server. The available encryption modes are <b>TKIP</b> , <b>AES</b> , or <b>TKIP/AES</b> .
WPA2-PSK	The available encryption types for this authentication are <b>TKIP</b> , <b>AES</b> , or <b>TKIP/AES</b> . In this mode, you don't need an additional RADIUS server for user authentication.
WPA2	In this mode, specify the IP address and port number for the RADIUS server. The key value is shared by the device and RADIUS server. The available encryption modes are <b>TKIP</b> , <b>AES</b> , or <b>TKIP/AES</b> .

Authentication Type	Description
WPA-PSK/WPA2-PSK	This mode is used when some clients only support WPA-PSK and others use WPA2-PSK. You don't need an additional RADIUS server for user authentication.
WPA/WPA2	This mode is used when some clients only support WPA and others use WPA2. The key value is shared by the device and RADIUS server. Specify the RADIUS server IP address and port number.

## Wireless Client List

The Wireless Client List displays the connected wireless clients. Choose to see all connected clients or only clients on a specific AP.

## Advanced Configuration

Advanced wireless setup is used to optimize the wireless performance under the specific installation environment.

1. **Beacon Interval:** Beacons are broadcast packets that are sent by a wireless AP/router.
2. **DTIM Interval:** Delivery Traffic Indication Message Interval. When the wireless router has buffered a broadcast or multicast message for clients, it sends a DTIM with a DTIM interval value.
3. **RTS Threshold:** Adjust the Request To Send Threshold value and you can improve wireless performance if there is an excessive number of wireless packet collisions.
4. **Fragmentation:** Wireless frames are divided into smaller units to improve performance in the presence of RF interference.
5. **WMM:** WiFi Multimedia helps control latency and jitter when transmitting multimedia content over a wireless connection.
6. **TX Rate:** Choose **Best** for auto-adjustment based on WiFi signal quality in the current environment.
7. **Transmit Power:** You can lower the power ratio to prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

## Status

The status window shows different kinds of system status: Network Status, WiFi Status, and LAN Client List.

### Network Status

- **WAN Interface IPv4 Network Status:** This shows the current status of all the WAN interfaces that are set up with IPv4 addresses. Click **Edit** to configure the WAN internet settings.
- **4G Modem Status:** This shows the current status of the 4G mobile WAN interfaces. Click **Details** to view details of the cellular radio and network information.
- **Internet Traffic Statistics:** This shows the amount of data being sent and received on all the WAN interfaces.
- **Data Usage Monitoring:** This shows the amount of data being sent and received periodically on 4G mobile WAN interface.

### WiFi Status

- **WiFi Virtual AP List:** This shows the current status of all the Virtual WiFi access point. Click **Edit** to configure the virtual WiFi access point settings.
- **WiFi Traffic Statistics:** This shows the amount of data being sent and received on all the virtual WiFi access point. Click **Refresh** to see the latest amount of data usage. Click **Reset** to start counting data from 0.

## LAN Client List

- **LAN Client List:** This shows a list of all the current Ethernet and WiFi client devices that are detected and active on the LAN and WiFi interfaces.

## WAN and Internet Setup for 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 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 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 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**.

## 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 5 – 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. Port settings apply to WAN web UI access only.

## 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. **Syslog:** 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:** Perform firmware upgrade.
- 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 6 – Safety/Regulatory Information

### 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).

## 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

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

### FCC Part 96

<b>FCC Identifier:</b>	XMR201909EG12GT
<b>Equipment Class:</b>	Citizens Band End User Devices
<b>Notes:</b>	LTE-A Cat 12 LGA Module
<b>Approval:</b>	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 3).

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

- 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)

<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

**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

