mPower™ Edge Intelligence

Conduit® 300 Software Guide

mPower Edge Intelligence Software Guide

Models: MTCDT3AC

Part Number: S000786 rev. 5.4

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.

Trademarks and Registered Trademarks

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 mPower Edge Intelligence

This guide reviews the mPower Edge Intelligence software for Conduit 300 devices.

For hardware details, refer to the appropriate hardware guide. Use your device to provide secure data communication between many types of devices that use legacy and the latest communication technologies.

Some device models support (varies with model-refer to your specific hardware guide for details):

- Bluetooth communication to devices with this technology
- Wi-Fi communication to devices with this technology
- GPS capability
- Diversity

What's New in This Release

Manual version	Update description
5.4	Switch Configuration and Docker.

Chapter 2 – Using the Wizard to Configure Your Device

First-Time Setup

Setting Up Your Device using Setup Wizard (After Choosing Reset and Factory Default Settings)

Other than when you first power up the device, you must configure the device to factory default settings, reset it and then, access it through the default 192.168.2.1 IP address to see the first-time setup. To reset the device to factory default settings, go to **Administration > Save/Restore > Reset to Factory Default Configuration** and click the **Reset** button. This wizard helps you configure the main features of your device for initial setup.

Here are the steps for first-time setup:

1. Upon power up for the first time or after you set factory default settings, the device goes into commissioning mode. The system requires you to set up an admin user. Enter your desired username and click **OK**.
2. Enter a desired password for the admin user and click **OK**. This password must be of sufficient length and strength (with a mix of character classes such as letters, numbers, and symbols). Enter the password again to confirm. Click **OK**.
3. Log into your device using your new username and password.
4. On the first page, the system allows you set up the device as a **Network Router** device.
    a. The default mode establishes the device as a cellular **Network Router**.
    b. Click **Next**.

For Default Mode (set up as a Network Router):

1. Configure **Call Home**
    a. Check **Enabled.** (You must have an existing DeviceHQ™ account.)
    b. Click the **Call Home** button to activate Call Home (which enables the device to call home for configuration files, firmware updates, custom applications, and adds your DeviceHQ account key to the device). **NOTE:** Clicking the **Call Home** button, results in the device being reset to factory defaults.
    c. Click **Next.**
2. Set the date, time, and time zone.
    a. Enter the desired **Date**.
    b. Enter the desired **Time**.
    c. Select the **Time Zone** in which the device operates.
    d. Click **Next**.
3. Configure LAN network interfaces Eth0 and Br0. Enter the device address and network information for Network Router mode only. (**Note:** If you do not accept default settings, after applying changes to **Network Interface Configuration (br0** or **eth0)**, the device reboots.):

a. In the **Network Interface Configuration – eth0** section, leave the **eth0** assigned to the bridge **br0**, or unassign **eth0** from bridge and enter network settings for the **eth0** interface - **IPv4 Address** and **Mask.**
b. In the **Network Interface Configuration – br0** section, enter network settings for the **br0** interface - **IPv4 Address** and **Mask**.

4. Configure your device's **PPP**.

a. To use PPP, check **Enable**. When enabled, your device functions as a router.
b. Check **Diversity** to enable the use of two cellular antennas for better performance. (For devices that use two antennas, Diversity is enabled by default. See *Installing the Router* in your User Guide for more details).
c. To enable the dial-on-demand feature, check **Dial-on-Demand**. This indicates to the device to bring up the PPP connection when there is outgoing IP traffic, and take down the PPP connection after a given idle timeout. **Note:** This field is only available on specific models where the device defaults to PPP instead of WWAN.
d. Enter the **APN** (Access Point Name). The APN is assigned by your wireless service provider. (This field is not available on all models.)
e. Click **Next**.

5. Set up **PPP Authentication**:

a. Select the authentication protocol **Type** used to negotiate with the remote peer: **PAP, CHAP, or PAP-CHAP**. The default value is **NONE**.
b. Enter the **Username** with which the remote peer authenticates. Optional. Username is limited to 60 characters.
c. Enter the **Password** with which the remote peer authenticates. Optional. Password is limited to 60 characters.

6. Set up **Remote Management:**

a. Check **Enabled** to configure the device to check in at the next scheduled check-in time.
b. Check **SSL Enabled** to activate SSL on the annex protocol.
c. **Server Name** for DeviceHQ is provided.
d. **Server Port** for DeviceHQ is provided.
e. **App Store URL** for DeviceHQ is provided.
f. Enter your **DeviceHQ Account Key**. (**NOTE:** You must already have a DeviceHQ account.)
g. Click **Next.**

7. Configure **HTTP/HTTPS Access**.

a. In the **HTTP Redirect to HTTPS** panel define how the device handles HTTP traffic. Check **Enabled** to enable HTTP and redirect to HTTPS.
b. Configure HTTP **Port**. By default, 80.
c. Check **Via LAN** (enabled by default) to allow traffic from local area network.
d. Check **Via WAN** (disabled by default) to allow traffic from the wide area network.
e. In the **HTTPS** panel, define how the device handles secure HTTP traffic.
f. Check **Via WAN** to allow traffic from the wide area network. Note: HTTPS traffic via LAN is enabled by default and cannot be changed.

g. Configure HTTPS **Port**. By default, 443.

8. Set up **Bootloader Protection** by setting a u-boot password.
   a. Enter a password and click **Enable**. The password will be set immediately.
   b. To change the password, enter a new password and click **Change Password**.
   c. To disable the password, click **Disable**.
9. Click **Finish**.
10. To save your changes, click **Save and Apply**.

Note: The **Bootloader Protection** settings depend on the previous u-boot configuration and are preserved when device is reset to factory defaults.

Chapter 3 – Home

Device Information

This page provides a high-level view of the device. It shows the configuration for one or more network interfaces including a cellular interface. Click **Home** to display the following information:

1. **Device**:
    - **Model Number**: The Conduit 300 model ID.
    - **Serial Number**: The MultiTech device ID.
    - **IMEI**: International Mobile Station Equipment Identity.
    - **Firmware**: mPower Edge Intelligence firmware version.
    - **Current Time**: Current date and time of the device. For information on setting the date and time, go to **Setup > Time Configuration**.
    - **Up Time**: Amount of time the device has been continuously operating.
    - **WAN Transport**: Current transport for IP traffic leaving the LAN. If two WAN interfaces are configured for use (Wi-Fi and cellular), the current WAN will be set based on the WAN configurations at ***Setup > WAN Configuration***.
    - **Current DNS**: the actual DNS IP addresses that are used by the current WAN.
    - **GeoPosition**: the GPS coordinates of the device (provided a GPS satellite fix is acquired).
2. **LAN (**LAN network interfaces, **br0, eth0, eth1, eth2,** and **wlan1**):
    - **Bridge** (**br0**)

      MAC Address: Media Access Control Address used to uniquely identify the devices LAN Ethernet interface.

      IPv4 Address: IP address of this device. To configure the IP address, go to **Setup > Network Interfaces Configuration**.

      Mask: Network mask of the bridge (**br0**). To configure the network mask, go to **Setup > Network Interfaces Configuration**.

      DHCP State: Current state of the DHCP server configured for the bridge (br0). To configure, go to **Setup > DHCP Configuration**.

      Interfaces: lists all the interfaces added to the bridge **(br0).**

    - **Ethernet (eth0, eth1, and eth2)**

      Bridge: specifies if the network interface is added into the bridge (**br0**).

      MAC Address: Media Access Control Address used to uniquely identify the devices LAN Ethernet interface.

      IPv4 Address: LAN IP address of the **Ethernet** interface. To configure the IP address, go **Setup > Network Interfaces Configuration**.

      Mask: Network mask of the **Ethernet** interface. To configure the network mask, go to **Setup > Network Interfaces Configuration.**

      DHCP State: Current state of the DHCP server configured for the bridge (**br0**). To configure, go to **Setup > DHCP Configuration**.

Lease Range: Current DHCP lease range of the **Ethernet** interface. To configure, go to **Setup > DHCP Configuration**.

DHCP State: Current state of this device's DHCP server. To configure go to **Setup > DHCP Configuration**.

Lease Range: Current DHCP lease range of this device's DHCP server. To configure go to **Setup > DHCP Configuration**.

- **Wi-Fi Access Point (wlan1)**:

  State: Current state of the Access Point. To configure go to **Wireless > Wi-Fi Access Point**.

  Bridge: specifies if the network interface is added into the bridge (**br0**).

  MAC Address: Media Access Control Address used to uniquely identify the devices LAN Ethernet interface.

  IPv4 Address: LAN IP address of the wlan1 interface. To configure the IP address, go **Setup > Network Interfaces Configuration**.

  Mask: Network mask of the Access Point (wlan1). To configure the network mask, go to **Setup > Network Interfaces Configuration**.

  DHCP State: Current state of the DHCP server configured for the wlan1 network interface. To configure, go to **Setup > DHCP Configuration**.

  SSID: the Service Set Identifier (SSID) for this device's Wi-Fi Access Point. For configuration go to **Wireless > Wi-Fi Access Point**.

  Security: the current security protocol of this device's Wi-Fi Access Point. To configure go to **Wireless > Wi-Fi Access Point**.

3. **Bluetooth Classic**
   - **State**: Current state of the Bluetooth link. To configure go to **Wireless > Bluetooth-IP**.
   - **MAC Address**: Media Access Control Address used to uniquely identify the Bluetooth interface.
   - **Device Name**: Name of Bluetooth device configured to link to. For configuration go to **Wireless > Bluetooth-IP.**
   - **Device MAC**: Media Access Control Address of the Bluetooth device configured to link to. To configure go to **Wireless > Bluetooth-IP**.
4. **WAN** (WAN network interfaces, **ppp0**, **wlan0, eth0, eth1,** and **eth2**):
   - **Cellular (ppp0) :**

     State: Current state of the cellular PPP link.

     Connection Mode: PPP or **WWAN** (only visible on LTE devices)

     Cellular Mode: LTE, 3G, and **2G**.

     Mode: PPP or **PPP - Addresses Only**.

     Protocol Support: Choose from **IPv4** or **IPv6**. If you choose **IPv6**, also enter the **Connect Timeout**.

     Signal: Current signal strength of the cellular link. Mouse hover provides dBm value.

     Ec/Io: Signal to Noise Ratio (used to calculate RSSI in 3G devices).

     RSCP: Received Signal Code Power (used to calculate RSSI in 3G devices)

     RSRP: Reference Signal Received Power (used to calculate RSSI in LTE devices)

RSRQ: Reference Signal Received Quality (used to calculate RSSI in LTE devices)

Connected: Total time connected for the current PPP session.

IPv4 Address: Current cellular WAN IP address issued to this device by the cellular carrier.

DNS: DNS IP addresses retrieved from the cellular network or configured by user in the Setup > Network Interfaces Configuration.

Roaming: Indicates whether or not this device's cellular link is currently connected to its home network.

Phone number: Device's cellular phone number also known as Mobile Directory Number (MDN). This field is blank if the MDN is not stored in the SIM card.

Tower: Tower ID of the cellular tower currently providing cellular service to this device.

- **Ethernet (eth0, eth1, and eth2):**

  Mode: Static, DHCP Client or DHCP Client – Addresses Only

  MAC Address: Media Access Control Address used to uniquely identify the devices LAN Ethernet interface.

  IPv4 Address: IP address of the Ethernet interface. To configure the IP address, go to **Setup > Network Interfaces Configuration**.

  Mask: Network mask of the network to which the device is currently connected.

  Gateway: Gateway IP address of the network to which the device is currently connected.

  DNS: DNS IP addresses retrieved from the cellular network or configured by user in the Setup > Network Interfaces Configuration.

- **Wi-Fi (wlan0)**:

  State: Current state of the Wi-Fi

  Mode: DHCP Client or DHCP Client – Addresses Only

  MAC Address: Media Access Control Address used to uniquely identify the Wi-Fi interface.

  IPv4 Address: The IP address that is obtained from the Wi-Fi network to which the device is currently connected.

  Mask: Network mask of the Wi-Fi network to which the device is currently connected.

  Gateway: Gateway IP address that is retrieved from the Wi-Fi network to which the device is currently connected.

  DNS: DNS IP addresses retrieved from the cellular network or configured by user in the **Setup > Network Interfaces Configuration**.

  SSID: the Service Set Identifier (SSID) of the Wi-Fi Access Point to which the device is currently connected.

5. **Accessory Cards** (if installed)
   - **Card1 (AP1)**

     Model Number: Model number of accessory card 1.

     Serial Number: Serial number of accessory card 1.

Hardware: Hardware version of accessory card 1.

- **Card2 (AP2)**

  Model Number: Model number of accessory card 2.

  Serial Number: Serial number of accessory card 2.

  Hardware: Hardware version of accessory card 2.

Chapter 4 – LoRaWAN

LoRaWAN Network Settings

The LoRaWAN Network Settings screen contains settings for the LoRaWAN network server, Lens Server and LoRa packet forwarder. A grouping of a gateway (like your device) and end-devices (sensors) can be connected to create an application network. Through the cloud-based Lens interface, you can manage your LoRa application networks including gateway and end-devices. When the LoRa Network Server is enabled, the gateway device acts as a network server allowing end-points to join with the correct credentials on the correct frequency and sub-band. LoRa can be configured for the 915 frequency band (AS, AU, KR, and US), the 868 frequency band (EU, IN, and RU), or the global 2400 frequency band (ISM). For the US, the 915 band allows 8 sub-bands. For the EU, the 868 band has three default channels and five configurable channels. For specific industrial, scientific, and medical applications globally, the ISM 2400 band has three default channels.

The TX (transmit power) setting is used to control the transmission power of the gateway. The Rx 1 DR Offset and RX 2 Datarate are sent with a join response to configure the data rates used for receive windows. The offset is applied to the downlink data rate for reception on the first window according to LoRa WAN standards.

If two cards are installed, the system displays information for both cards: FPGA Version and Frequency Band using (ap1) and (ap2) labels.

- The system chooses the card to activate based on the selected channel plan.
- This allows 868 and 915 cards to be installed. Only one card is be active at any time.
- Two v1.5 915 or 868 cards can be used as long as they are the same frequency band.

After you change any of these settings, click **Submit**. Then, click **Save and Apply** to save your changes.

LoRa Mode

The LoRa Configuration pane contains the configuration values for the LoRa network server that acts as a gateway for the LoRa endpoint devices.

Item	Default Value	Description
Mode	Network Server	Choose from Network Server, LoRa Packet Forwarder, Basic Station, or Disabled.
Packet Forwarder	Depends on latest software version	Packet Forwarder software version
Packet Forwarder Status	If configured properly, RUNNING	Packet Forwarder status. Values include RUNNING, RESTARTED, or DISABLED.
Network Server	Depends on latest software version	Network Server software version
Network Server Status	If configured properly, RUNNING	Network Server status. Values include RUNNING, RESTARTED, or DISABLED.
Lens Server	Depends on latest software version	Lens Server software version
Lens Server Status	If configured properly, RUNNING	Lens Server status. Values include RUNNING, RESTARTED, or DISABLED.

Basic Station	Depends on latest software version	Basic Station software version (For MTAC-LORA-H 868 and 915 cards only)
Basic Station Status	If configured properly, RUNNING	Basic Station status. Values include RUNNING, RESTARTED, or DISABLED.
FPGA version	Depends on latest software version	Shows the FPGA firmware version for the installed MTAC-LORA cards.
Frequency Band (MHz)	N/A	Frequency band used which is determined by the type of MTAC-LORA card installed. Values are 868 or 915 MHz.

LoRaWAN Network Server Configuration

The LoRaWAN Server Configuration pane contains the configuration values for the LoRa network server that acts as a gateway for the LoRa endpoint devices.

Item	Default Value	Description
Channel Plan		
Channel Plan	US915: 915, AU915: 915, AS923-1: 915, AS923-2: 915, AS923-3: 915, KR920: 915, EU868: 868, IN865: 868, RU864: 868, ISM2400: 2400	LoRaWAN channel plan used for the upstream and downlink frequencies and datarates. Values are US915, EU868, IN865, AU915, AS923-1, AS923-2, AS923-3, KR920, RU864, or ISM2400. Available channel plans depend on the type of MTAC-LORA card installed. For more details on each Channel Plan, refer to the RP2-1.0.1 LoRaWAN® Regional Parameters document on the LoRa Alliance website, https://lora-alliance.org/.

Channel Mask	N/A	Mask of available channels. Leave empty to enable only selected sub-band or set as desired. Click the Edit button to select your desired channel mask(s) by checking the box under the available list of channels. Override channel mask to include coverage provided by additional gateways. US/AU 64-channel: 00FFFFFFFFFFFFFFFF and EU/AS/IN/KR: 00FF. Combine the following FSB masks to support more than 8 channels. Settings will be sent to end-devices on first downlink after OTA join:
		FSB0: 00FFFFFFFFFFFFFFFF FSB1: 00010000000000000FF FSB2: 00020000000000FF00 FSB3: 00040000000000FF0000 ... FSB8: 0080FF00000000000000 FSB1 + FSB8: 0081FF000000000000FF
Frequency Sub-Band	1	For US and AU only, 8 sub-bands are available.
Frequency Sub-Band 2	1	For US and AU only, 8 sub-bands are available (for extra LoRa Card).
Enable Diversity	Unchecked	Enable use of two LoRa cards.
Enable LBT	Unchecked	Enable Listen Before Talk. Note: Requires FPGA v33 or v61.
Max EIRP	20	Maximum uplink transmit power of end-devices (in dBm)
Dwelltime Up	0 (no limit)	Maximum uplink dwell-time for region (ms). 0 : no limit and 1 : 400 ms (depends on region).
Dwelltime Down	0 (no limit)	Maximum downlink dwell-time for region (ms). 0 : no limit and 1 : 400 ms (depends on region).

Additional Channels	Depends on channel plan selected	A set of channels are configured based on this setting (MHz). Frequencies supported depends on channel plan selected. v2.1 Geolocation GW - default channels must be included in the configured range. The RU864 plan uses the following channels when configured with the default settings of 0: Radio 0: 868.9 MHz, 869.1 MHz Radio 1: 864.1 MHz, 864.3 MHz, 864.5 MHz, 864.7 MHz, 864.9 MHz.
Additional Channels 2	Depends on channel plan selected	A set of channels are configured based on this setting (MHz). Frequencies supported depends on channel plan selected. v2.1 Geolocation GW - Configurable for the range within the entire band.The RU864 plan will use the following channels when configured with the default settings of 0: Radio 0: 868.9 MHz, 869.1 MHz Radio 1: 864.1 MHz, 864.3 MHz, 864.5 MHz, 864.7 MHz, 864.9 MHz.
Duty Cycle Period	60	Number of minutes in sliding windows for duty cycle restrictions (for EU only)
Class B Settings		
Enable Beaconing	Checked	Enable beacon broadcasting.
Beacon Frequency	0	Beacon frequency (MHz).
Beacon Power	27	Beacon power (dBm). Select from drop-down: 0, 3, 6, 10, 11, 12, 13, 14, 16, 20, 23, 24, 25, 26, or 27.
Disable Ping Slot Frequency Hopping	Unchecked	Disable frequency hopping on beacons (only available in regions that support frequency hopping).
Ping Slot Frequency	0: uses the Channel Plan default	Frequency to use on ping slots (MHz).

Ping Slot Datarate	DEFAULT	Datarate to use on ping slots. US: 8-13, EU/IN/AS: 0-7, AU: 8-13, KR: 0-5. When using DEFAULT, the datarate matches the Rx2 Datarate setting and the ranges match the Rx2 Datarate ranges.
Info Descriptor	0	Info Descriptor of beacon. Select from drop-down: 0, 1, or 2.
Beacon Latitude	0	GPS latitude of antenna specified by Info Descriptor (degrees).
Beacon Longitude	0	GPS longitude of antenna specified by Info Descriptor (degrees).
Network		
Network Mode	Public LoRaWAN	Set Network Mode: Private MTS (sync word: 0x12 and US/AU) Downlinks per FrequencySubBand) Public LoRaWAN (sync word: 0x34) Private LoRaWAN (sync word: 0x12)
Lease Time (dd-hh-mm)	00-00-00	Amount of time until a successful join expires.
Join Delay (Private mode)	1 (5 if user input value is outside of range.)	Number of seconds before receive windows are opened for join. Must match Dot settings. Range: 1-15
Join Delay (Public mode)	5 (Also if user input value is outside of range.)	Number of seconds before receive windows are opened for join. Must match Dot settings. Range: 1-15
Address Range Start	00:00:00:01	Start address to assign to OTA joining motes.
Address Range End	FF:FF:FF:FE	End address to assign to OTA joining motes.
Rx1 Delay	1	Number of seconds before receive windows are opened. Must match Dot settings. Range: 1-15
NetID	000000	LoRaWAN NetID setting for assigning network address and beacons.
Queue Size	16	Number of downlink messages to hold per node.
Settings		

Tx Power (dBm)	26	Transmit power of the device. Value range is from 1 to 27.
ADR Step (cB)	30	Step between each datarate setting for ADR (minimum: 25).
Antenna Gain (dBi)	3	Gain of configured antenna (-128 to 128).
Min Datarate	0	Minimum datarate to use for ADR. US: 0-4, EU/AS/RU: 0-7, AU: 0-6, KR: 0-5, IN: 1-5,7.
Rx 1 DR Offset	0	Offset applied to upstream data rate for downstream data rate on first receive window. US: 0-4, EU/RU: 0-5, AS/IN: 0-7, AU: 0-7, KR: 0-5.
Max Datarate	0	Maximum datarate to use for ADR. US: 0-4, EU/AS/RU: 0-7, AU: 0-6, KR: 0-5, IN: 1-5,7.
Rx 2 Datarate	10 (For US/AU), 2 (For all others)	Datarate for second receive window. US: 8-13, EU/IN/AS: 0-7, AU: 8-13, KR: 0-5.
ACK Timeout	5000	Time in milliseconds to wait for ACK before retry of confirmed downlink
Database		
Database Path	var/config/lora/lora-network-server.db	Path to backup database in non-volatile memory
Reduce Uplink Writes	Disabled (unchecked)	Write uplink data to database every 100 packets or 5 minutes to increase uplink throughput
Backup Interval	3600	Interval in seconds to backup the database to flash
Skip Field Check	Disabled (unchecked)	Skip checking JSON fields of UDP packets from packet forwarder, may increase uplink throughput
Trim Interval	600	Interval in seconds to run the trim packet data tables command
Trim Size	100	Maximum size of packet tables to keep in database
Fine TimeStamp		
FTS Version	1	The default version of the encrypted/main fine timestamp (for FPGA >= v59). Select from drop-down: 0 or 1.

DSPs	1	Number of DSPs (Digital Signal Process) on the board to be booted.
DSP Stat Interval	10	DSP's reporting interval (seconds).
FSK SYNC	N/A	An hexadecimal string, 2 to 16 digits long, setting the "sync word" for FSK transmissions in TX and RX (most significant bit first).
Room Temperature	22	Reference room temperature Tref used for calibration (°C)
AD9361 Code	77	Temperature code returned by AD9361 radio when room temperature is Tref [0..255]
Match CRC Error	Unchecked	Enable/disable fine timestamp matching for packets with CRC error.
GPS Receiver	Checked	Whether or not to use the GPS receiver in conjunction with the packet forwarder.

Network Server Logging (hidden by default, click Show to see settings)

The logging pane specifies what format, the location and what level of server logs to save for the LoRa Server Network.

Item	Default Value	Description
Log Destination	Syslog	Select the type logging destination, either Syslog or File (use only for debug purposes to avoid filling up device RAM).
Path	blank	Specify the log file location.
Log Level	INFO	Select the log level of the messages to be logged. Choose from drop-down: Info, Error, Warning, Debug, Trace, and Maximum. Maximum will provide all messages.

Network Server Testing (hidden by default, click Show to see settings)

The testing pane provides testing and debugging functions for the LoRa server.

Item	Default Value	Description
Disable Join Rx1	Disabled	Disable sending join accept message in Rx1.
Disable Join Rx2	Disabled	Disable sending join accept message in Rx2.

Disable Rx1	Disabled	Disable sending downlink messages in Rx1.
Disable Rx2	Disabled	Disable sending downlink messages in Rx2.
Disable Duty Cycle	Disabled	Disable duty cycle restrictions (**this is for testing purposes only -** do not use for deployments).

Server Ports (hidden by default, click Show to see settings)

To configure the server ports, enter the following:

Item	Default Value	Description
Local Only	Enabled (checked)	Configure local ports only
Upstream Port	1780	Upstream port
Downstream Port	1782	Downstream port
App Port Up	1784	Application port up
App Port Down	1786	Application port down

Payload Broker

To configure the payload broker, enter the following:

Item	Default Value	Description
Enabled	Enabled (checked)	Enable MQTT protocol
Hostname	127.0.0.1	Hostname of payload broker
Port	1883	Port used by MQTT
Username	N/A	Username
Password	N/A	Password

Default App (hidden by default, click Show to see settings)

A default application is provided to communicate LoRaWAN network messages to remote servers. HTTP and MQTT protocols are supported. For information about the defined API and an example service, see here: https://github.com/MultiTechSystems/lorawan-app-connect

To configure the default app, enter the following:

Item	Default Value	Description
Enabled	Disabled (Unchecked)	Enable/disable default application.
Check Hostname	Disabled (Unchecked)	Enable/disable hostname check of app.
Server URL	N/A	Server URL for MQTT(s) and HTTP(s) services.

App EUI	N/A	EUI of the default application.
Server Cert	N/A	The certificate to authenticate the server.
Client Cert	N/A	The certificate used to authenticate the client.
Client Key	N/A	The key used to authenticate the client.
Username	N/A	Authentication username for MQTT.
Password	N/A	Authentication password for MQTT.

LoRa Packet Forwarder Configuration

The LoRaWAN Packet Forwarder pane contains the configuration values for the Packet Forwarder mode.

Item	Default Value	Description
SX1301		
Frequency Band (MHz)	N/A	Frequency band used which is determined by the type of MTAC-LORA card installed. Values are 868 or 915 MHz.
Channel Plan		
Channel Plan	US915: 915AU915: 915, AS923-1: 915, AS923-2: 915, AS923-3: 915, KR920: 915, EU868: 868, IN865: 868, RU864: 868, ISM2400: 2400	LoRaWAN channel plan used for the upstream and downlink frequencies and datarates. Values are US915, EU868, IN865, AU915, AS923-1, AS923-2, AS923-3, KR920, RU864, or ISM2400. Available channel plans depend on the type of MTAC-LORA card installed. For more details on each Channel Plan, refer the RP2-1.0.1 LoRaWAN® Regional Parameters document on the LoRa Alliance website, https://lora-alliance.org/.
Enable Diversity	Unchecked	Enable use of two LoRa cards.

Additional Channels	Depends on channel plan selected	A set of channels are configured based on this setting (MHz). Frequencies supported depends on channel plan selected. v2.1 Geolocation GW - default channels must be included in the configured range. The RU864 plan uses the following channels when configured with the default settings of 0: Radio 0: 868.9 MHz, 869.1 MHz Radio 1: 864.1 MHz, 864.3 MHz, 864.5 MHz, 864.7 MHz, 864.9 MHz
Additional Channels 2	Depends on channel plan selected	A set of channels are configured based on this setting (MHz). Frequencies supported depends on channel plan selected. v2.1 Geolocation GW - Configurable for the range within the entire band.The RU864 plan will use the following channels when configured with the default settings of 0: Radio 0: 868.9 MHz, 869.1 MHz Radio 1: 864.1 MHz, 864.3 MHz, 864.5 MHz, 864.7 MHz, 864.9 MHz.
Frequency Sub-Band	1	For US and AU only, 8 sub-bands are available.
Listen-Before-Talk (LBT) - Available for AS923 and KR920 only		
Enabled LBT	Unchecked (disabled)	Enable (check) LBT (Listen-Before-Talk) when supported by hardware. Note: Requires FPGA v33 or v61.
LBT RSSI Offset	-128 dB	Adjustment value for RSSI during LBT.
LBT RSSI Target	-65 dBm	Target RSSI level for LBT, if RSSI level is above the target, then transmit is not possible.
Scan Time	128 **µs**	Amount of clear time below threshold needed to allow transmission. Select from 128 or 5000 microseconds (**µs)**.
Add LBT channels	Check	Set the LBT channels automatically.
Basics		

Public	Unchecked (disabled)	Enable public mode: sync word 0×34, Disable for private mode: sync word 0×12.
Gateway ID Source	Manual	Either specified in configuration (Manual) or queried from device (Hardware).
Gateway ID	N/A	Installed LoRa card EUI (Extended Unique Identifier).
Gateway ID 2	N/A	Second Installed LoRa card EUI (Extended Unique Identifier).
Packet Forwarder Path	opt/lora/lora_pkt_fwd	Path to packet forwarder binary file to execute.
Beacon Configuration		
Enable Beaconing	Checked	Enable beacon broadcasting.
Disabled Beacon Frequency Hopping	Unchecked	Disable frequency hopping on beacons (only available in regions that support frequency hopping.
Beacon Frequency	0: uses the Channel Plan default	Beacon frequency (MHz).
Beacon Power	27	Beacon power (dBm). Select from drop-down: 0, 3, 6, 10, 11, 12, 13, 14, 16, 20, 23, 24, 25, 26, or 27.
Info Descriptor	0	Info Descriptor of beacon. Select from drop-down: 0, 1, or 2.
Beacon Latitude	0	GPS latitude of antenna specified by Info Descriptor (degrees).
Beacon Longitude	0	GPS longitude of antenna specified by Info Descriptor (degrees).
Intervals		
Keep Alive Interval	10 seconds	Interval to send a ping to the network server.
Stat Interval	20 seconds	Interval to update the network server with gateway statistics.
Push Timeout	100 ms	Timeout default.
Autoquit Threshold	60	Number of messages sent without acknowledgment from the network server
Server		
Network	Manual	Select the network for Packet Forwarder mode including Manual (user determined), The Things Network, or Semtech Demo.

Server address	N/A	Server IP address to forward received uplink packets and transmit received downlink packets. The system provides the default address for The Things Network (based on your channel plan) and Semtech Demo. Refer to the router addresses table of The Things Network for the list of specific addresses based on channel plan: https://www.thethingsnetwork.org/docs/gateways/packet-forwarder/semtech-udp.html If you choose The Things Network with the AS923 channel plan, there are four different addresses available. **NOTE:**No server addresses are available for The Things Network when using IN865 or RU864 channel plans.
Upstream Port	N/A	IP Port to send received uplinks to. The system provides default ports for The Things Network and Semtech Demo.
Downstream Port	N/A	IP Port to connect to network server for downlink packets. The system provides default ports for The Things Network and Semtech Demo.
Forward CRC		
Forward CRC Disabled	Unchecked	Enable (check) to send packets received with CRC disabled to the network server.
Forward CRC Error	Checked	Enable (check) to send packets received with CRC errors to the network server.
Forward CRC Valid	Checked	Enable (check) to send packets received with CRC valid to the network server.

Basic Station Configuration

To configure Basic Station, use the following settings:

Item	Default Value	Description

Station Card 1		
Credentials	LNS	Choose connection method to reach network server. Select from LNS or CUPS.
URI	N/A	URI to connect to CUPS or LNS server.
Station Configuration	Example	Station configuration for the gateway. See included example file.
Server Cert	N/A	Server certificate used to authenticate CUPS or LNS server.
Gateway Cert	N/A	Client certificate used by server to authenticate gateway.
Gateway Key	N/A	Client key used by server to authenticate gateway.

Key Management

For Local Network Settings, after you change these fields, click **Submit**. Then, click **Save and Apply** to save your changes.

Join Server

Choose the location of your join server.

Item	Default Value	Description
Location	Cloud Key Store	Choose Remote or local Join Server to handle OTA join requests. Select from drop-down either **Cloud Key Store** or **Local Keys**.

Add End Device Credentials

In order to use this section, you must choose **Local Keys** under **Join Server** and click on **Add New** to add new end-device credentials.

Item	Default Value	Description
Dev EUI	N/A	Enter Device EUI.
App EUI	N/A	Enter App EUI.
App Key	N/A	Enter App Key.
Class	A	Select Device Class from A, B, or C.
Device Profile	N/A	Select Device Profile from drop-down.

Network Profile	N/A	Select Network Profile from drop-down.

Once you enter the above values, click **Finish**. Your saved end-device information displays under the **Local End-Device Credentials**.

Settings (for Cloud Key Store**)**

Item	Default Value	Description
Join Server URL	https://join.devicehq.com/api/m1/joinreq	Join Server address (You can verify the join server by clicking the Test button.)
Enable Lens API	Disabled (Unchecked)	Enable Lens API to use Lens portal to manage LoRaWAN network.
Lens API URL	https://lens.devicehq.com/api/	Lens API URL.
Check-In Interval	3600	Number of seconds between device check-in to Lens cloud.
Gateway EUI	N/A	Gateway EUI (Extended Unique Identifier)
UUID	N/A	Universally Unique Identifier (128-bit ID)
Serial Number	N/A	Device serial number

Messages (available using Cloud Key Store)

Item	Default Value	Description
Network Stats	Enabled	Send periodic network stats to Lens servers.
Packet Metadata	Enabled	Send metadata on uplink and downlink packets to Lens servers.
Packet data	Disabled	Send data from uplink and downlink packets to Lens servers.
Gateway Stats	Enabled	Send periodic gateway stats to Lens servers.
Local Join Metadata	Enabled	Send periodic gateway stats to Lens servers.
DeviceHQ	Enabled	Allows Lens to control DeviceHQ connectivity settings (optional).

Gateway Info (available using Cloud Key Store)

Item	Default Value	Description
Gateway EUI	N/A	Gateway EUI (Extended Unique Identifier)

UUID	N/A	Universally Unique Identifier (128-bit ID)
Serial Number	N/A	Device serial number

Traffic Manager (available using Cloud Key Store)

Item	Default Value	Description
JoinEUI Filter	N/A	Applied to received Join Requests to limit the number of messages sent to Join Server from unwanted devices (Read-only display of logic downloaded from Lens settings).
DevEUI Filter	N/A	Applied to received Join Requests to limit the number of messages sent to the Join Server from unwanted devices (Read-only display of logic downloaded from Lens settings).

Local Network Settings

Item	Default Value	Description
Enabled	Checked (enabled)	Enable or disable Local Network Settings.
Network ID (AppEUI)	Name	Specify Network ID format from local application network ID or App EUI. Select from drop-down: Name or EUI.
Name	Uses local device name.	Gateway device name.
Default Profile	DEFAULT-CLASS-A	Default network profile to use for newly joined end-devices. Choose from Class A, B, or C.
Network Key (AppKey)	Passphrase	Choose Network Key from Passphrase or Key.
Passphrase	N/A	Enter Passphrase if used.
Key	N/A	Enter Key if used. (128-bit hexadecimal value)

Spectral Scan Configuration

Item	Default Value	Description
Enabled	Unchecked (disabled)	Enable or disable Spectral Scan.
Scan Settings		
Samples	10000	Total number of RSSI points.
Bandwidth	250	Channel bandwidth (in KHz).

Step	100000	Frequency step between start and stop (in Hz).
Offset	0	Offset to be applied to resultant data (in db).
Floor	-120	Threshold below which results are ignored (in db).
Scheduling		
Start	9:00	Start time for scans in UTC time (leave blank if you want current time).
Interval	1	Time period between run sets (minutes).
Stop	Never	Stop criteria for scans. Select from drop-down: Never, After Duration, and After Number of Scans
Duration	1	Time period to run continuous scans (in hours). Use 0 for once. (Shows up if you choose After Duration under Stop.)
Scan Sets to Run	0	Scan limit (Shows up if you choose After Number of Scans under Stop.)
Scan Sets - First set range is required and two default ranges are provided. Others are optional up to 5 max. Each range set is independent and flexible. Enter start and stop range and click Add to add that range as an additional set. Click Remove to delete one.		
Start 1	902100000	Start frequency 1 (in Hz) - Required.
Stop 1	903900000	Stop frequency 1 (in Hz) - Required.
Start 2	923000000	Start frequency 2 (in Hz) - Optional.
Stop 2	928000000	Stop frequency 2 (in Hz) - Optional.
Start 3	N/A	Start frequency 3 (in Hz) - Optional.
Stop 3	N/A	Stop frequency 3 (in Hz) - Optional.
Start 4	N/A	Start frequency 4 (in Hz) - Optional.
Stop 4	N/A	Stop frequency 4 (in Hz) - Optional.
Start 5	N/A	Start frequency 5 (in Hz) - Optional.
Stop 5	N/A	Stop frequency 5 (in Hz) - Optional.

Gateways

This section displays all active and configured gateways. The following information displays:

Item	Description

Gateway EUI	Gateway EUI (Extended Unique Identifier)
IP address	Gateway IP address
IP Port	Port used for LoRaWAN Gateway
Version	Protocol version of Packet Forwarder
Last Seen	Time of last update, Minutes or hours ago
Options	Additional statistics and details for Gateway option in last five minutes. Click info icon for details.

Packets Received

Item	Description
Gateway EUI	Gateway EUI (Extended Unique Identifier)
Channels 1 -10	Number of packets received on this channel
CRC	Cyclic Redundancy Check failed
Adding Total	Count of packets on all channels including CRC errors

Network Statistics

Item	Description
Join Request Responses	Average Join Request Response in milliseconds: 90%, 70%, 30%
Join Packets	Number of Okay packets, Duplicates and MIC fails, Unknown, Late, Total
Transmitted Packets	Pkt (Packets) 1st Wnd (Window), Pkt 2nd Wnd, ACK Pkt, Total, Join 1st Wnd, Join 2nd Wnd, Join Dropped, Join Total
Received Packets	MIC Fails, Duplicates, CRC Errors, Total
Scheduled Packets	1st Wnd, 2nd Wnd, Dropped, Total

Duty Cycle Time-On-Air Available (seconds - only available for EU)

Item	Description
Gateway EUI	Gateway EUI (Extended Unique Identifier)
Bands 0-3	Channel bands

Devices

This section allows users to add new end-devices. To add a new end-device:

1. Go to **LoRaWAN** > **Devices**.
2. Under **End Devices**, click **Add New**.
3. Enter the following fields:

a. **Dev EUI** - the end-device EUI (Extended Unique Identifier)
b. **Name** - the name of the end-device
c. **Class** - LoRaWAN operating class of end-device. Is communicated to network server on Join. The end-device must be configured out-of-band for operating class. A, B, or C are currently supported. (A, B, or C).
d. **Serial Number** - Serial number of end-device
e. **Product ID** - Product ID for end-device
f. **Hardware Version** - Hardware version for the end-device
g. **Firmware Version** - Firmware version for the end-device
h. **LoRaWAN Version** - Software version for LoRaWAN server

4. Click **Finish**.
5. The new end-device displays under the **End Devices** list including some device details and statistics.
6. To edit the device, click the pencil icon, or to delete it, click the x icon next to that device.

Device Sessions

The normal join process involving properly configured and registered gateways and end-devices creates sessions FOTA (Firmware Over-the-Air) automatically.

However, you can use the Device Sessions section, if you want to create a session manually, otherwise known as ABP (Activation by Personalization). The manual session includes only the gateway and end-devices. The server is not involved.

To add a new session manually:

1. Go to **LoRaWAN** > **Devices**.
2. Under **Sessions**, click **Add New**.
3. Enter the following fields:

a. **Dev EUI** - End-device EUI (Extended Unique Identifier)
b. **Dev Addr** - Network device address assigned to end-device
c. **Class -** Device Class (B or C)
d. **App EUI** - Application EUI
e. **Join EUI** - Join Request EUI
f. **Net ID** - Network ID
g. **App Session Key** - Pre-shared application session key
h. **Net Session Key** - Derived network session key based on pre-shared application key
i. **Multicast Session** - Select from the drop-down: No (not multicast session), Class B, or Class C

4. Click **Finish**.
5. The new session displays under the **Sessions** list including some device details and statistics.

a. **Dev EUI** - End-device EUI (Extended Unique Identifier)
b. **Dev Addr** - Network device address assigned to end-device
c. **Up FCnt** - Packet counter of last received packet
d. **Down FCnt** - Packet counter of last sent packet
e. **Last Seen** - Time of last packet received

f. **Joined** - What is the device joined to, Cloud or local version
g. **Details** - Additional session information (click on info icon)
h. **Multicast Session** - Select from the drop-down: No (not multicast session), Class B, or Class C

6. To edit the session, click the pencil icon, or to delete it, click the x icon next to that session.

Device Groups

This page allows you to create **Device Groups** in order to perform mass firmware upgrade OTA and multicast messaging to all devices in that group.

The **Groups** table displays existing groups. Use the **View**, **Edit,** or **Remove** buttons to see, modify, or delete an existing group in the table.

To create a new device group:

1. Go to **LoRaWAN > Device Groups**.
2. Click the **Add New** button.
3. The Add Group dialog box appears. Enter your desired **Group Name**.
4. You can also enter an optional **Group EUI**. If you do not provide one, the system generates a Group EUI automatically.
5. Select the desired end device(s) to include in your group by clicking the box next to each **Device EUI**.
6. Click **Add**.

To import your device group:

1. Click **Import**.
2. Click **Choose File** and browse to select your desired file.
3. Click **Import**.

To export all your device groups, click **Export All**.

Groups table fields

Item	Description
Name	Device Group Name (user-defined)
EUI	Optional Device Group EUI (the system generates one for you if undefined)
Size	Number of devices in the group
Options	Edit and Delete options

Profiles

When connected to the LoRaWAN server, the profiles can be downloaded from the cloud. There are two-kinds of profiles: End-Device and Network.

Make profile changes in the Lens cloud and the device updates during a periodic check-in or when end-device associated with the profile joins or rejoins the network.

See existing profiles under the End-Device Profiles and Network Profiles lists. Refer to tables for profile details. Click Refresh to update the list.

Settings provided in the device profile must reflect the default settings of the end-device when it is first joined to the network. The end-device should be in this default configuration. Any deviation between the device profile and the actual default end-device settings may result in lost downlinks to the end-device due to non-matching Rx window parameters.

To add a new device profile:

1. Go to **LoRaWAN > Profiles**.
2. Under **End-Devices Profiles**, click **Add New**.
3. Enter the fields or check the following boxes:
    a. Profile ID - Enter your desired profile name.
    b. Max EIRP
    c. Max Duty Cycle - Select from the drop-down including DEFAULT or a range of options from 100% to 0.003%.
    d. MAC Version.
    e. RF Region - Select from the drop-down including DEFAULT, US915, AU915, AS923, KR920, EU868, IN865, and RU864.
    f. Region Version.
    g. Supports Class C (Check box to enable. If this is enabled, then you may enter a value for the following field.)
        i. Timeout Class C
    h. Supports Class B (Check box to enable. If this is enabled, the following fields appear and you may enter values for them.)
        i. Ping Slot Period
        ii. Ping Slot Datarate
        iii. Ping Slot Frequency
    i. Supports Join (check box to enable)
    j. Support 32 Bit FCnt (check box to enable)

End-Device Profiles (edit/add new)

Parameter	Description
Profile ID	name of profile
Max EIRP	maximum transmit power of the end-device
Max Duty Cycle	maximum duty-cycle of the end-device
MAC Version	LoRaWAN version supported by end-device, LW1_0 has different MAC commands, and network messages from LW1_1
RF Region	end-device region or channel plan
Region Version	revision of Regional Parameters specification

Supports C	true if end-device can use class C mode
Timeout C	time for the end-device to reply to a confirmed downlink before retransmission
Supports B	true if end-device can use class B mode
Timeout B	time for the end-device to reply to a confirmed downlink before retransmission
Ping Slot Period	how often the end-device opens class B windows – 1 (once per second) up to 128 (once per beacon period)
Ping Slot Datarate	datarate used for class B window
Ping Slot Frequency	frequency used for class B window
Supports Join	true if end-device supports OTA join
Rx1 Delay	default delay between end of Tx and beginning of the first Rx window, if not provided the LoRaWAN default for the selected channel plan will be used.
Rx1 DR Offset	default datarate offset of first Rx window, if not provided the LoRaWAN default for the selected channel plan will be used
Rx2 DR Index	default datarate of second Rx window, if not provided the LoRaWAN default for the selected channel plan will be used
Rx2 Frequency	default frequency of second Rx window, if not provided the LoRaWAN default for the selected channel plan will be used
Preset Frequencies	additional channels configured at the end-device
Supports 32 Bit FCnt	true if end-device supports 32 bit counters

Network Profiles

Settings provided in the network profile reflect the settings of the end-device to be received in MAC commands after it is first joined to the network. These are the desired settings for the end-device to operate with. Any deviation between the network profile and the default end-device settings are sent to the end-device in successive MAC commands until all settings have been relayed.

NOTE: Network profile settings will override device profile and network settings.

To add a new network profile:

1. Go to **LoRaWAN > Profiles**.
2. Under **Network Profiles**, click **Add New**.
3. Enter the fields or check the following boxes:
    a. Profile ID – Enter your desired profile name.
    b. Max Duty Cycle - Select from the drop-down including DEFAULT or a range of options from 100% to 0.003%
    c. Class- Select from the drop-down including A, B, or C.

d. Timeout Class C
e. Rx1 Delay
f. Rx1 DR Offset - Select from drop-down which varies with your selected channel plan.
g. Rx2 DR Index - Select from drop-down which varies with your selected channel plan.
h. Rx2 Frequency
i. Channel Mask
j. Redundacy

Network Profiles (edit/add new)

Parameter	Description
Profile ID	name of profile
Max Duty Cycle	maximum duty-cycle of the end-device
Class	operating class for end-device: A, B or C
Timeout C	time for the end-device to reply to a confirmed downlink before retransmission
Rx1 Delay	default delay between end of Tx and beginning of the first Rx window, if not provided the LoRaWAN default for the selected channel plan will be used
Rx1 DR Offset	default datarate offset of first Rx window, if not provided the LoRaWAN default for the selected channel plan will be used
Rx2 DR Index	default datarate of second Rx window, if not provided the LoRaWAN default for the selected channel plan will be used
Rx2 Frequency	default frequency of second Rx window, if not provided the LoRaWAN default for the selected channel plan will be used
Channel Mask	bitmask of enabled channels, US/AU use a twenty character mask, other use a four character mask
US	first 2 characters are not used, the next two control the 500 KHz channels: ■ enable all channels – 00FFFFFFFFFFFFFFFF ■ enable bottom half - 000F00000000FFFFFFFF
EU	enable all channels - FFFF
Redundancy	number of times an unconfirmed uplink should be repeated

Packets

This section shows three lists: transmitted, recent join requests, and recently received packets on the LoRa network. Each packet includes relevant packet details.

Packets (Transmitted)

Item	Description
Device EUI	End-device EUI (Extended Unique Identifier) transmitting the uplink packet or destination of the downlink packet
Freq	Frequency used to transmit packet
Datarate	Datarate used to transmit packet
SNR	Signal to noise ratio of received packet
CRC	Cyclic redundancy check failed
RSSI	Received signal strength
Size	Size in bytes of packet
FCnt	MAC packet counter
Type	Type of packet includes these possible values: ■ **JnAcc** - Join Accept Packet ■ **JnReq** - Join Request Packet ■ **UpUnc** - Uplink Unconfirmed Packet ■ **UpCnf** - Uplink Confirmed Packet - ACK response from network requested ■ **DnUnc** - Downlink Unconfirmed Packet ■ **DnCnf** - Downlink Confirmed Packet- ACK response from end-device requested
Tx/Rx Time	Time packet was sent or received
Details	Additional packet details (click on info icon to view popoup)

Recent Join Requests

Item	Description
Join EUI	8-byte EUI (Extended Unique Identifier) found in the join request
Nonce	Join nonce provided by end-device in the Join Request
Elapsed	Round trip time in milliseconds for the Join Server to service the join request

Result	If the result of the request is valid, it displays: **Success**. If the result is an error, one of the following displays: ■ **MICFailed** - AppKey setting did not match the end-device record in Join Server ■ **Dropped** - Downlink packet could not be scheduled for transmit on any available gateways ■ **Duplicate Dev Nonce** - Nonce in join request has already been used ■ **JoinReq Failed** - Other server error ■ **UnknownDevEUI** - Device record was not found at Join Server ■ **Gateway Mismatch** - Join Server configuration does not allow this device to join through this gateway ■ **Server Error** - Join Server is not reachable possibly due to Internet connection settings or DNS resolution

Recent Rx Packets

Item	Description
Time	Time packet was received
Freq	Frequency used to transmit packet
Datarate	Datarate used to transmit packet
CRC	Cyclic redundancy check failed
SNR	Signal to noise ratio of received packet
RSSI	Received signal strength
Size	Size in bytes of packet
Type	Type of packet includes these possible values: ■ **JnAcc** - Join Accept Packet ■ **JnReq** - Join Request Packet ■ **UpUnc** - Uplink Unconfirmed Packet ■ **UpCnf** - Uplink Confirmed Packet - ACK response from network requested ■ **DnUnc** - Downlink Unconfirmed Packet ■ **DnCnf** - Downlink Confirmed Packet- ACK response from end-device requested
Data	Actual data in packet (payload)
Details	Additional packet details (click on info icon to view popup)

Downlink Queue

You can manually send a downlink packet to an end-device.

The packet remains in the queue until sent. Once it has been transmitted/received, the packet displays under **Packets**.

To manually send a downlink packet:

1. Go to **LoRaWAN > Downlink Queue**. Click on **Add New**.
2. Enter the following fields for the new Queue Item:
    a. **Dev EUI** - receiving end-device EUI (Extended Unique Identifier)
    b. **App Port** - port field set in the downlink packet
    c. **Data Format** - encoding scheme for the packet (select either Hex or Base64).
    d. **Data** - the payload (data being transmitted)
    e. **Ack Attempts** - number of allowed downlink request ack retries
    f. **RxWindow** - specify the Rx Window to use for downlink (0 - no priority, 1- first Rx Window, 2- second Rx Window)
3. Click **Finish**.
4. The new **Queue Item** displays under the **Downlink Queue** list including some device details and statistics.
    a. **Dev EUI** - receiving end-device EUI (Extended Unique Identifier)
    b. **App Port** - port field set in the downlink packet
    c. **Size** - total packet minus header
    d. **Ack** - number of retries to receive ACK from end-device
    e. **RxWnd** - the Rx Window to use for downlink (0 - no priority, 1- first Rx Window, 2- second Rx Window)
    f. **Queued** - Time packet has been added to the queue
    g. **Details** - additional statistics displayed related to the packet
5. To edit the item, click the pencil icon, or to delete it, click the x icon next to that item.

Operations

The LoRaWAN **Operations** page offers two different features on one page: **FOTA** or **Multicast Messaging**.

The device offers the option of FOTA using your LoRaWAN network. To use this feature, you must properly configure your LoRa network and end-devices (must be joined to the network). You may set a countdown for an immediate update or schedule the upgrade for a specific time. You can also update multiple devices on your LoRa network.

The device also offers the option of Multicast Messaging over the LoRaWAN network.

To perform **FOTA**:

1. Go to **LoRaWAN > Operations**.
2. Under **Operations Settings**, select **FOTA** in the **Operation Type** drop-down.
3. Click **Browse** and select your **Firmware Upgrade File** (.bin).
4. Under the **Fragment Description** field, enter the fragment description for the FOTA session in HEX format.

5. You have the option to specify a **Setup Time In by clicking Change**. Setup time specifies how long from the time scheduled before the Multicast Setup Process begins. Under **Setup Time Input** from the drop-down, select either:
    a. **Countdown to Setup from Now:** Enter **Number of Days** plus hours, minutes and seconds in **HH:MM:SS** (default: 30 seconds) **OR**
    b. **Specify Future Date and Time:** Select your desired **Date** and **Time**.
6. Otherwise, click **Hide** to hide **Setup Time Input** details. Click **Change** to show and modify.
7. You have the option to specify a **Launch Time In**. Launch time specifies how long the Multicast Process runs before starting firmware transmission. Under **Launch Time Input** from drop-down, select either:
    a. **Countdown to Launch from Setup:** Enter **Number of Days** plus hours, minutes and seconds in **HH:MM:SS** (default: 90 seconds) **OR**
    b. **Specify Future Date and Time:** Select your desired **Date** and **Time**.
8. Choose the desired **Target End-Devices** to receive the upgrade. Select either a previously-saved **End-Device Group** or **Individual Devices** from the drop-down on the right. Check the box near your desired device or group to designate it for upgrade. You can also check **Select/Deselect All box** to select or deselect all groups in the list.
9. Click the **Settings** tab, if you wish to change the defaults for the following FOTA parameters
    a. **Delete Successful Logs** (default: checked)
    b. **Number of Parity Fragments per Session** (default: 100)
    c. **Sleep Delay between Setup Messages** (default: 1000 microseconds)
    d. **Sleep Delay between Data Fragments** (default: 1500 microseconds)
    e. **Sleep Delay between Parity Fragments** (default: 3000 microseconds)
10. After configuring FOTA, click **Schedule** to finalize your FOTA update.
11. Once the scheduled upgrade is submitted, you can track its progress through the **Progress** tab. A progress bar appears at the top of the page. The progress bar shows the transfer of the file from the PC to the device. Once completed, the page switches to the Progress tab. The job displays in either **Scheduled, Active**, or **Completed Jobs** lists depending on the job phase and timing.

To perform the Multicast **Messaging**:

1. Go to **LoRaWAN > Operations**.
2. Under **Operations Settings**, select **Message** in the **Operation Type** drop-down.
3. Select from either **Textbox** or **File** under **Payload Source**.
4. Select from either **Hexadecimal** or **Base64** under **Payload Format**.
5. Enter the message contents under **Payload**.
6. Enter the **Port** from a range of **1-220** (default: 1).
7. Under **Transmission Setup**, you have the option to specify a **Setup Time In by clicking Change**. Setup time specifies how long from the time scheduled before the Multicast Setup Process begins. Under **Setup Time Input** from the drop-down, select either:
    a. **Countdown to Setup from Now:** Enter **Number of Days** plus hours, minutes and seconds in **HH:MM:SS** (default: 30 seconds) **OR**
    b. **Specify Future Date and Time:** Select your desired **Date** and **Time**.

8. Otherwise, click **Hide** to hide **Setup Time Input** details. Click **Change** to show and modify.
9. You have the option to specify a **Launch Time In**. Launch time specifies how long the Multicast Process runs before starting message transmission. Under **Launch Time Input** from drop-down, select either:

    a. **Countdown to Launch from Setup:** Enter **Number of Days** plus hours, minutes and seconds in **HH:MM:SS** (default: 90 seconds) **OR**

    b. **Specify Future Date and Time:** Select your desired **Date** and **Time**.

10. Choose the desired **Target End-Devices** to receive the message. Select either a previously-saved **End-Device Group** or **Individual Devices** from the drop-down on the right. Check the box near your desired device or group to designate it to receive the message. You can also check **Select/Deselect All box** to select or deselect all groups in the list.
11. Click the **Settings** tab, if you wish to change the defaults for the following message parameters

    a. **Delete Successful Logs** (default: checked)

    b. **Sleep Delay between Setup Messages** (default: 1000 microseconds)

    c. **Sleep Delay between Data Fragments** (default: 1500 microseconds)

    These parameters are constants for multicast messaging and cannot be modified:

    a. **Number of Parity Fragments per Session** (value: 100)

    b. **Sleep Delay between Parity Fragments** (value: 3000 microseconds)

12. After configuring Mulitcast **Messaging**, click **Schedule to schedule your message**.
13. Once the message is submitted, you can track its progress through the **Progress** tab. A progress bar appears at the top of the page. The progress bar shows the transfer of the message from the PC to the device. Once completed, the page switches to the Progress tab. The job displays in either **Scheduled, Active**, or **Completed Jobs** lists depending on the job phase and timing.

Chapter 5 – Setup

Network Interfaces

For configuration management of network interfaces, go to **Setup > Network Interfaces > Network Interfaces Configuration**. This section displays the list of network interfaces. Click on the pencil icon to the right of a particular interface in order to edit its configuration. Refer to possible configurations in the table below.

Bridge

This section allows you to create a bridge between network interfaces. All LAN network interfaces are added into the bridge (br0) by default.

Just LAN interfaces are allowed under bridge including **Ethernet** (**eth0, eth1, eth2)** and **Wi-Fi Access Point** (**wlan1)**. With this bridge interface added, it is possible to assign any number of LAN interfaces (of both **Ethernet** and **Wi-Fi AP** types) to a specified bridge. Only one bridge interface is supported. **IPv6** support is also available under the bridge using **Static** IP mode.

Slave Interfaces

Slave interfaces such as **Ethernet (eth0, eth1, eth2)** or **Wi-Fi AP** (**wlan1**) do not have their own IP addresses and are not configured as DHCP clients by default. Static IP address mode is implemented on the bridge level.

Ethernet Interface

The Ethernet interface can be configured as either **LAN** or **WAN**. Ethernet interface as **LAN** can be set to use static pre-set IPv4 or IPv6 addresses or dynamically obtain an IPv4/IPv6 address over DHCP in DHCP client mode. When configured as **WAN**, only IPv4 is available.

PPP interface

The **PPP** interface is only allowed to be **WAN**. The **PPP** interface listed in the **Network Interfaces** page can only have its mode changed. Options are **PPP** and **PPP addresses-only** modes. IPv6 WAN support is also an option with the PPP interface (configurable fields vary with network carrier).

Wi-Fi integration (depends on model)

Wi-Fi integration is enabled by adding two network interfaces: **wlan0** (used exclusively for **Wi-Fi as WAN (STATION)** mode) and **wlan1** (used exclusively for **AP** mode). The Web UI as well as API back-end has been modified to add support and validation rules in order to assign **LAN** interface(s) to a bridge, and removing them from under the bridge. **NOTE:** Wi-Fi availability depends on model. Consult the appropriate manual for details.

Switch Interface

Before configuring your switch interface (**swi***), you must first add it to the **Switch Configuration**. In default configuration, all four Ethernet Switch ports are tied to one sw1 interface (**swi***) that is, in turn, included in Bridge (**br0**). The system supports configuration of each switch interface as either **WAN** or **LAN**, under the Bridge (**br0**) or not, and with a mode of either **static**, **DHCP**, or **DHCP Addresses Only (WAN only)**. **LAN** supports both **IPv4** and **IPv6**. **WAN** only supports **IPv4**. There can be up to four switch interfaces.

Network configurations

Refer to the following table for the possible network configurations:

Interface	Direction	Type	IP Mode	Bridge Mode	IPv4/IPv6 Support
Br0	N/A	BRIDGE	STATIC	Br0	Both
Eth0, Eth1, Eth2	LAN	Ethernet	STATIC	N/A	Both
Eth0, Eth1, Eth2	LAN	Ethernet	DHCP Client	N/A	Both
Eth0, Eth1, Eth2	LAN	Ethernet	N/A	Br0	N/A
Eth0, Eth1, Eth2	WAN	Ethernet	STATIC	N/A	IPv4 only
Eth0, Eth1, Eth2	WAN	Ethernet	DHCP Client	N/A	IPv4 only
Eth0, Eth1, Eth2	WAN	Ethernet	DHCP Client - Addresses Only	N/A	IPv4 only
Wlan0	WAN	Wi-Fi as WAN	DHCP Client	N/A	IPv4 only
Wlan0	WAN	Wi-Fi as WAN	DHCP Client - Addresses Only	N/A	IPv4 only
Wlan1	LAN	Wi-Fi AP	STATIC	N/A	IPv4 only
Wlan1	LAN	Wi-Fi AP	N/A	Br0	IPv4 only
ppp0	WAN	Cellular	PPP	N/A	Both
ppp0	WAN	Cellular	PPP - Addresses Only	N/A	Both
swi1, swi2, swi3, swi4	LAN	Ethernet	STATIC	Br0	Both
swi1, swi2, swi3, swi4	LAN	Ethernet	DHCP Client	Br0	Both
swi1, swi2, swi3, swi4	WAN	Ethernet	STATIC	Br0	IPv4 only
swi1, swi2, swi3, swi4	WAN	Ethernet	DHCP Client	Br0	IPv4 only
swi1, swi2, swi3, swi4	WAN	Ethernet	DHCP Client - Addresses Only	Br0	IPv4 only

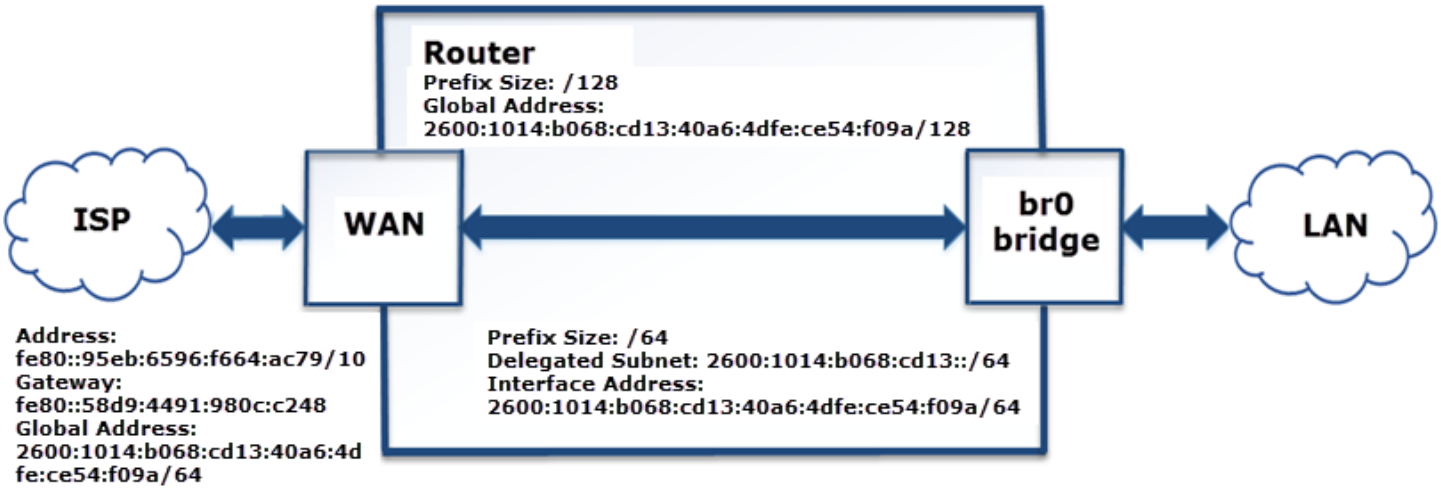
IPv6 Example Configurations

Configuration Example #1: Cellular WAN, Delegated LAN

This example is the most typical configuration. The admin user enables IPv6 on the Cellular Configuration, configures the bridge interface on the device in Delegated Prefix mode and, configures all LAN interfaces that will perform IPv6 as slaves of the bridge interface. The LAN networks “under” the bridge will all have the whole 64 bit

prefix delegated to them. The bridge and Cellular WAN interfaces will have the same IPv6 address. In this manner, the router will act as the gateway to the Internet for all the LAN devices that have delegated addresses.

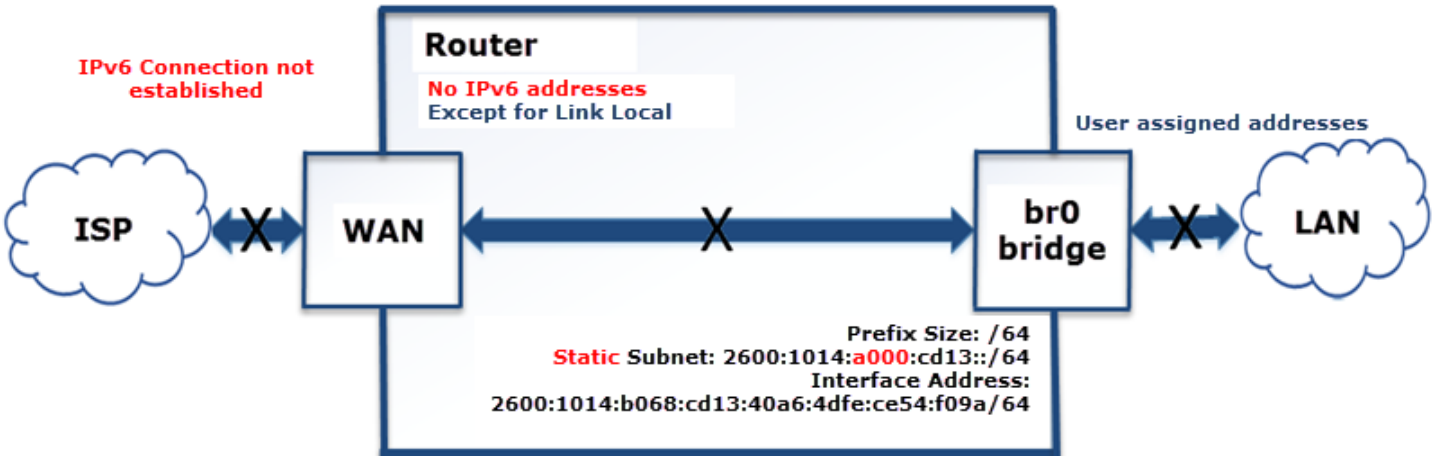
- WAN interface is configured in Automatic Client IPv6 Mode.
- All LAN interfaces are connected to the bridge interface.
- The bridge interface is configured in the Delegated Prefix mode.
- The whole /64 prefix is delegated to the LAN network.
- The Bridge interface and Cellular WAN interface have the same IPv6 address.



Configuration Example #2: No IPv6 WAN, Static LAN

This example is essentially the same as the old mode where IPv6 was not supported. The devices have Internet access via IPv4, but not via IPv6. On the LAN side, the admin user assigns a static IPv6 address to the br0 (bridge) interface and all the IPv6 addresses on the LAN side will be assigned by the user. In this case, the device may be managed through the LAN interface over IPv6.

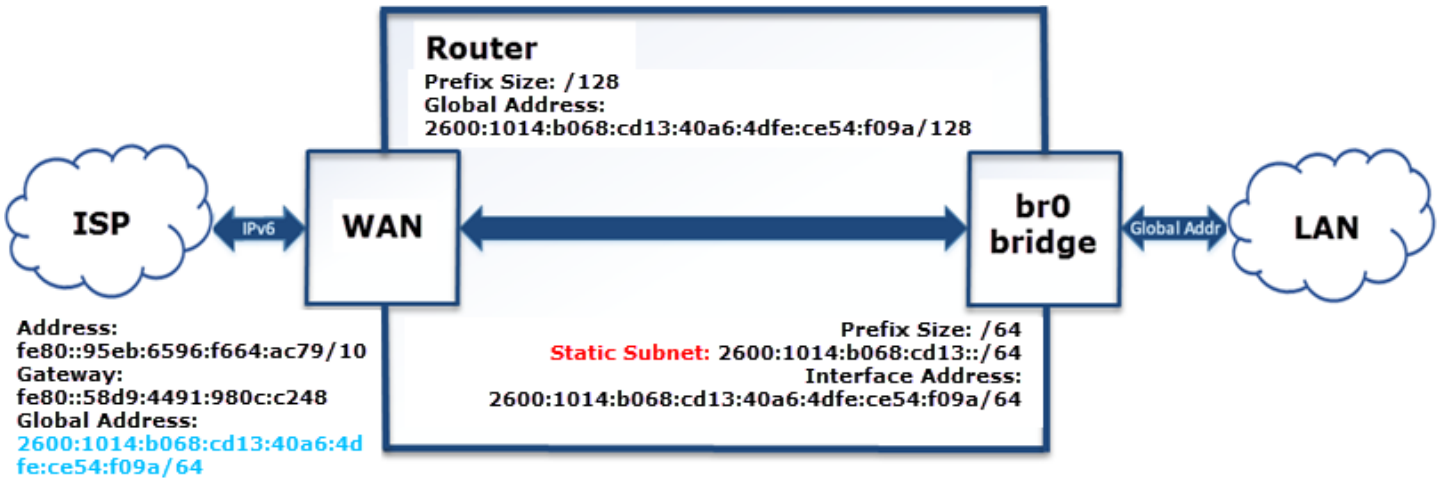
- IPv6 support disabled on WAN interface or IPv6 is not supported on cellular provider.
- Devices in LAN1 will see each other.
- Devices in LAN1 will not have Internet access over IPv6.



Configuration Example #3: Cellular WAN, Static LAN with valid addresses

This example is typically the second most widely used IPv6 scenario since not all ISPs support prefix delegation automatically. In this case, the cellular provider or ISP provides the admin user with global address of the device is and the IPv6 prefix that needs to be assigned to the LAN devices. The LAN devices are all programmed with a valid IPv6 address statically by the admin user with the knowledge of what IPv6 prefix to use provided by the Cellular Provider / ISP. All the LAN devices can access the Internet via IPv6 if they have a global IPv6 address configured.

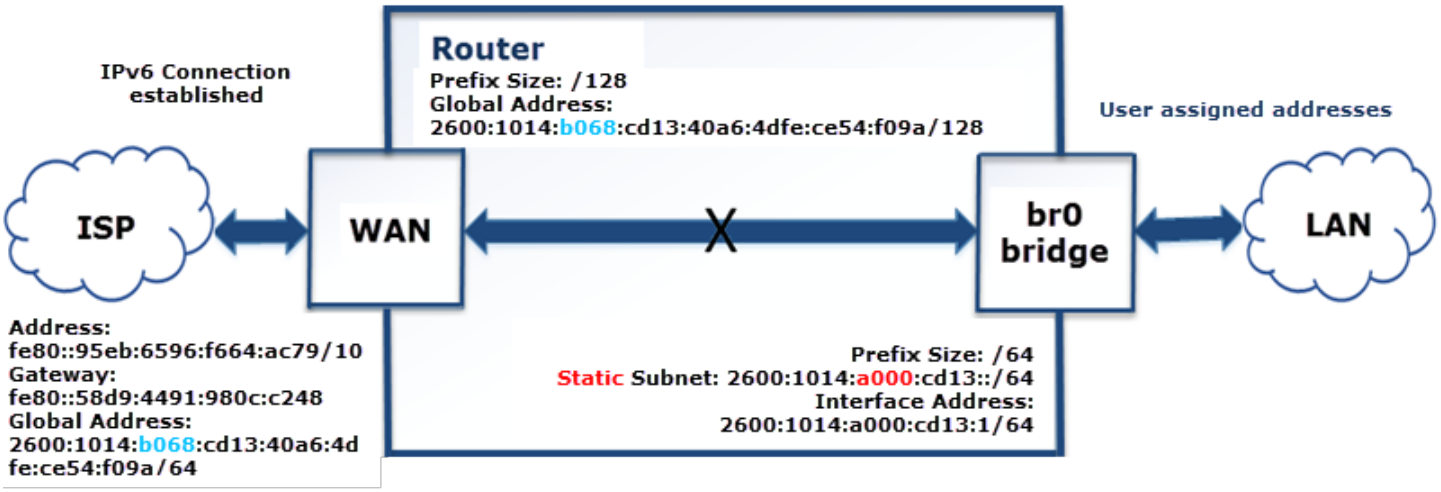
- It is known exactly what IPv6 subnet is assigned to the device by the cellular provider/ISP.
- All devices in LAN1 will have IPv6 Internet access.



Configuration Example #4: Cellular WAN, Static LAN with user-selected addresses

For this example, the LAN has IPv6 addresses, but they're not in the recognized range of addresses the cellular provider/ISP have specified with a prefix. The LAN devices will network with each other over IPv6, but do not have Internet access via IPv6. The device can ping IPv6 addresses on the Cellular WAN. However, since the LAN devices don’t have globally routable addresses recognized by the cellular provider/ISP, they get their packets dropped on the WAN link.

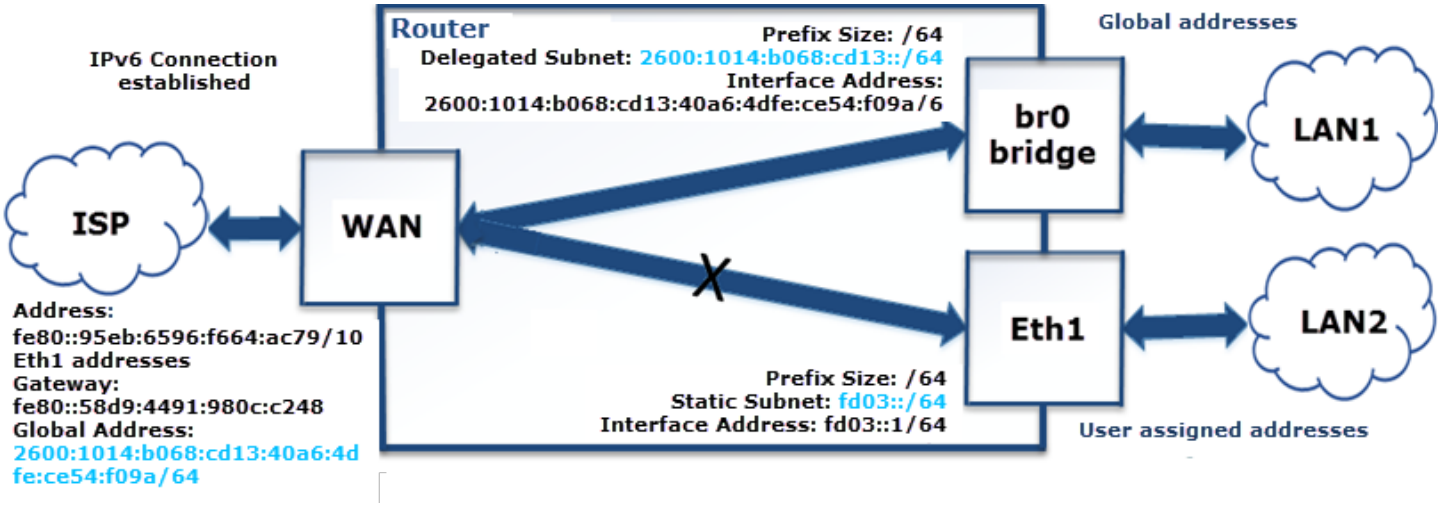
- LAN subnet is outside of the range of addresses provided by the cellular provider/ISP.
- Devices in LAN can see each other via IPv6.
- Devices in LAN do not have Internet access via IPv6.
- The router can ping IPv6 addresses.
- All packets with invalid IPv6 addresses are dropped on the WAN link.



Configuration Example #5: Cellular WAN, Static LAN, Delegated Prefix LAN

This scenario is a combination of examples #1 and #3. The difference is the Static LAN2 does not have Internet access because the prefix for the statically assigned addresses on that LAN do not match the delegated prefix from the cellular provider/ISP. The devices on LAN1 got their IPv6 addresses from the router that is using the delegated prefix from the cellular provider/ISP, so those devices have Internet access via IPv6. This example demonstrates the difference in behavior for the LAN networks based on the prefix delegation.

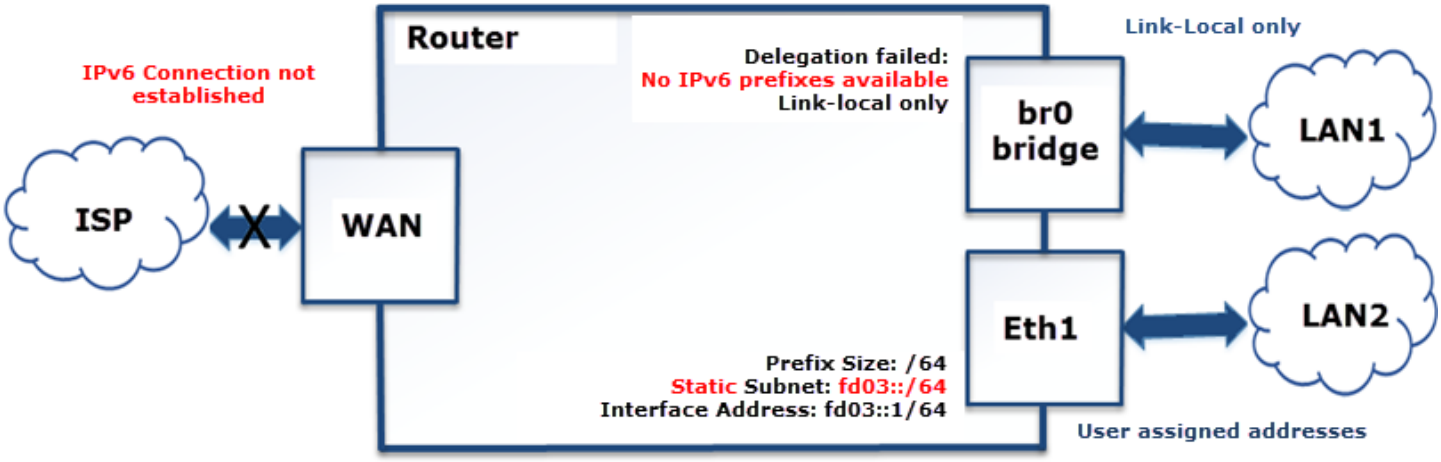
- User configured LAN1 in Delegated Prefix IPv6 mode.
- User configured LAN2 in Static IPv6 mode with user-selected addresses
- Devices in LAN2 will see each other.
- Devices in LAN1 will have Internet access via IPv6.
- Devices in LAN2 will not have Internet access via IPv6.



Configuration Example #6: No IPv6 WAN, Static LAN

For this example, IPv6 is enabled on the LAN interface but disabled on the WAN side or not supported by the cellular provider/ISP. The delegation fails. This results in LAN1 not receiving delegated IPv6 addresses as it should, but only link-local IPv6 addresses. LAN2 has statically defined IPv6 addresses, but does not have Internet access since the device does not have an established IPv6 connection.

- IPv6 support disabled on WAN interface or IPv6 is not supported by cellular provider/ISP.
- Delegation fails.
- Devices in LAN1 will not get any IPv6 addresses (except link-local).
- Devices in LAN2 will see each other and have IPv6 addresses.
- No IPv6 Internet access.



Switch Configuration

This device contains a four-port Ethernet Switch. Support for the Ethernet ports and interface configurations is implemented on this **Switch Configuration** page. The system supports adding and removing an Ethernet interface to/from Bridge (br0).

In default configuration, all four Ethernet Switch ports are tied to one sw1 interface (swi*) that is, in turn, included in Bridge (br0). You can reset the Switch Configuration to default settings using the **Reset to Default** button.

If you choose to configure a switch interface with less that the total four ports, you must create another interface with the remaining ports. Switch Configuration does not allow for any ports to be left out of the configuration (either covered all in one or under separate interfaces). Also, each Ethernet port can only be assigned to one switch interface.

The four port numbers (1-4) are labeled on the front of the device below each of their corresponding physical Ethernet ports.

The system supports configuration of each switch interface through **Setup > Network Interfaces** as either **WAN** or **LAN**, and with a mode of either **static**, **DHCP**, or **DHCP Addresses Only**.

There can be up to four switch interfaces.

You can view currently configured switch interfaces, add a new interface, modify an existing interface, remove one, or reset to default settings.

To view the current switch interfaces:

1. Go to **Setup > Switch Configuration**.
2. The **Switch Configuration** list displays the active switch interfaces and shows the following for each interface: Interface, Ports, and Options which include Edit (pencil icon) and Delete (trash can icon).

To add a switch interface:

1. Go to **Setup > Switch Configuration**.
2. Click **Add Interface**.
3. Under the **Add Interface** window, select the **Interface Name** from the drop-down which includes swi1, swi2, swi3, or swi4. **Note**: Switch Configuration does not allow for any ports to be left out of the configuration (either covered all in one or under separate interfaces). Check that all four ports are configured in either one or multiple interfaces.
4. Select the ports to be associated with this interface. Check any or all ports (1-4).
5. Click **OK**.
6. Go to **Setup > Network Interfaces** to configure network settings for your new interface. Under the **Network Interfaces Configuration** list, find the switch interface that you just added (swi1-4).
7. Click on the interface you just added (swi1-4) and set up its network configuration under **Network Interface Configuration-swi1-4** including **Direction** (**LAN** or **WAN**), **Bridge** (by default it's assigned to **br0**), and other details (refer to **Network Interfaces** for more information).

To modify an existing switch interface:

1. Go to **Setup > Switch Configuration**.
2. Under the **Switch Configuration** list, click **Edit** (pencil icon) under Options for the interface you wish to modify.

3. Under **Edit Interface**, you may modify the ports tied to this interface. Check those you wish to add and/or uncheck any you wish to remove. **Note**: Switch Configuration does not allow for any ports to be left out of the configuration (either covered all in one or under separate interfaces). Check that all four ports are configured in either one or multiple interfaces.
4. Click **OK**.
5. Go to **Setup > Network Interfaces** to modify the network settings for your edited interface. Under the **Network Interfaces Configuration** list, find the switch interface that you just added (swi1-4).
6. Click on the interface you just added (swi1-4) and modify network configuration under **Network Interface Configuration-swi1-4** including

   Direction (**LAN** or **WAN**), **Bridge** (by default it's assigned to **br0**), and other details (refer to **Network Interfaces** for more information).

To remove an existing switch configuration:

1. Go to **Setup > Switch Configuration**.
2. Under the **Switch Configuration** list, click **Delete** (trash can icon) under **Options** for the interface you wish to remove.
3. A confirmation message appears. Click **OK** to confirm deletion.

To reset switch configuration to default settings:

1. Click the **Reset to Default** button.
2. A confirmation message appears. Click **OK** to proceed.

Global DNS

The **Global DNS** Configuration page allows the user to set user-defined DNS servers. User-defined DNS servers in this page are always used to resolve hostnames regardless of what the WAN settings are and what WAN interface is being used. If the **Global DNS** primary and secondary servers are not configured here, the DNS servers used default to the servers configured for the current WAN.

Here are the key configuration scenarios for both **Global DNS** and forwarding server and their results (the device refers to a MultiTech device):

- If you do not configure **Global DNS** and enable forwarding, the device acts as a proxy server for any devices on the LAN network(s). In this mode, the device uses WAN DNS settings. Client settings: On the client, you must configure the device as the default gateway and DNS server. The easiest way to accomplish this is by using the DHCP server on the device.
- If you configure **Global DNS** and enable forwarding, DNS requests are forwarded to servers configured in the **Global DNS** settings. The device still acts as a proxy. Client settings: Clients must be configured the same as in the previous case above.
- If you configure **Global DNS** and disable forwarding, the default gateway and DHCP server on clients should point to the device and the DNS servers on the client must use the same DNS as the **Global DNS** settings. Client settings: The client device uses the device as default gateway and the DHCP server, but must have DNS servers configured to what options you plan to use.
- If neither item is configured/enabled, make sure to configure your device properly to forward DNS.

To configure **Global DNS**:

1. Click **Setup > Global DNS.**

2. Under **Global DNS Configuration**, leave **Enable Forwarding Server** unchecked. (If you check this, the forwarding server is active and global DNS is not configured).
3. To set global DNS servers, enter IP addresses for the both **Primary** and **Secondary Servers**. (These servers override any DNS servers specified elsewhere in the UI. If none are entered, the system defaults to servers configured for the current WAN.)
4. Under **Hostname Configuration**, enter the **Hostname** for your device.
5. Click **Submit**.
6. Click **Save and Apply** to save your changes **OR** click **Reset to Default** to return to default settings.

Hostname Configuration allows the user to change the hostname of the device to distinguish the device from other devices on the network.

To modify the default hostname:

1. Under **Hostname Configuration**, enter the **Hostname** for your device.
2. Click **Save and Apply** to save your changes **OR** click **Reset to Default** to return to default settings.

WAN Setup

Configuring WAN Failover Priority

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

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

Ethernet (eth0) is priority 1 by default.

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

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

For field descriptions see Failover Configuration Fields

For information on editing WAN Failover see Editing Failover Configuration

Editing Failover Configuration

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

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

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

To edit failover configuration:

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

Failover Configuration Fields

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

Configuring IP Address for LAN

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

1. Go to **Setup** > **Network Interfaces** > **br0** and click the **pencil icon** to edit.
2. To configure the address LAN information:
   In the **IP Address** field, type the device's IP address. The default is 192.168.2.1.
   In the **Mask** field, type the mask for the network. The default is 255.255.255.0.
3. To resolve domain names, configure domain name server information (DNS), go to **Setup > Global DNS** and refer to the Global DNS section (WAN DNS) for options and instructions on how to properly configure this feature.
4. Click **Submit**.
5. To save your changes, click **Save and Apply**.

Configuring Dynamic Domain Naming System (DDNS)

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

1. From **Setup**, select **DDNS Configuration**.
2. In the **Configuration** group, check **Enabled**.
3. In the **Service** drop-down list, select a DDNS service. To define a service that isn't listed choose **Custom**.
   a. For custom DDNS service, in the **Service** field, type the DDNS server's URL.

b. For custom DDNS service, in the **Port** field, type the DDNS server's port.

4. In the **Domain** field, type the registered Domain name.
5. In the **Update Interval** field, type the days that can pass with no IP Address change. At the end of this interval, the existing IP Address is updated on the server so that the address does not expire. The range of the interval you can enter is between 1 and 99 days. The default is 28 days.
6. Check **Use Check IP**, if you want to query the server to determine the IP address before the DDNS update. The IP address is still assigned by the wireless provider and the DDNS is updated based on the address returned by Check IP Server. If disabled, the DDNS update uses the IP address from the PPP link. The default is **Use Check IP**.
7. In the **Check IP Server** field, type the name to which the IP Address change is registered. Example: checkip.dyndns.org
8. In the **Check IP Port** field, type the port number of the Check IP Server. The default is 80.
9. Click **Submit**.
10. To save your changes, click **Save and Restart**.

Entering authentication information

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

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

Forcing a DDNS server update

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

Configuring Dynamic Host Configuration Protocol (DHCP) Server

To view, add, or edit DHCP servers, see the **IPv4 DHCP Servers** (IPv4 support) or **DHCPv6 and Router Advertisement** (for IPv6 support) list under **Setup > DHCP Configuration.**

You can configure multiple DHCP servers. Only one DHCP server can be created per LAN network interface. You can configure your device to function as a DHCP server that supplies network configuration information, such as IP address, subnet mask, and broadcast address, to devices on the network.

By default, the DHCP server is configured and enabled for Bridge (**br0**) network interface. If a LAN network interface is NOT under the bridge, DHCP server can be configured and enabled for it..

DHCP Server is disabled automatically if you modify the network interface under **Setup > Network Interface** including:

- changes to the interface subnet
- adding network interface under the bridge
- changing the interface from LAN to WAN (Ethernet interface only)
- removing all LANs from under the bridge (DHCP for **br0** will be disabled in this case)

DHCP Server cannot be enabled if the network interface is under the bridge, or is not enabled or configured properly (for example, when **eth0** is configured as WAN, or Wi-Fi Access Point is disabled).

To edit the configuration of an existing IPv4 DHCP server or add a new one:

1. Go to **Setup > DHCP Configuration**. See the **IPv4 DHCP Servers** list.
2. To edit a **DHCP Server**, click the pencil icon (edit) for the selected interface, **OR** to add a **DHCP Server**, click the **Add IPv4 DHCP Server** button.
3. The **DHCP Configuration** fields appear. To use the **DHCP** feature, check **Enabled**.
4. In the **Interface** field, select the network interface. Note: The Interface field is read-only when you edit DHCP Server.
5. The **Subnet** field displays the subnet address.
6. The **Mask** field displays the network's subnet mask.
7. In the **Gateway** field, type the gateway address.
8. In the **Domain** field, type your network domain, if any.
9. In the **Lease Time** field, enter the DHCP lease time. Lease time is set in days, hours, and minutes (dd-hh-mm). A Lease Time of 00-00-00 is an infinite lease time.
10. In the **Lease Range Start** field and in the **Lease Range End** field, type the range of IP addresses to be assigned by DHCP.
11. Click **Submit**. If you are finished making changes, click **Save and Apply**.

To edit the configuration of an existing DHCPv6 and Router Advertisement server or add a new one:

1. Go to **Setup > DHCP Configuration**. See the **DHCPv6 and Router Advertisement** list.
2. To edit a **DHCP Server**, click the pencil icon (edit) for the selected interface, **OR** to add a **DHCP Server**, click the **Add DHCPv6/RA** button.
3. The **DHCP Configuration** fields appear. To use the **DHCP** feature, check **Enabled**.
4. In the **Interface** field, select the network interface from the drop-down including **eth0** and **wlan1**. **Note:** Interface field is read-only when you edit DHCP Server.
5. In the **Router Advertisement Mode,** select from the drop-down the DHCP IPv6 mode including **SLAAC** or **Stateless DHCP**.
6. In the **Lease Time** field, type the DHCP lease time. Lease time is set in days, hours, and minutes (dd-hh-mm). A Lease Time of 00-00-00 is an infinite lease time.
7. Click **Submit**. If you are finished making changes, click **Save and Apply**.

To add fixed addresses for the DCHP server, see **Assigning Fixed Addresses**.

Assigning Fixed Addresses

To add fixed addresses for the DCHP server make the changes under the **Fixed Addresses** section on the **DCHP Configuration** page:

1. In the **MAC Address** field, type the MAC address to which the specified IP address binds.
2. In the **IP Address** field, type the fixed IP address to be assigned.
3. Click **Add**.
4. To save your changes, click **Save and Apply**.

Configuring SNMP

The device offers Simple Network Management Protocol (SNMP) which is used for collecting information from network devices on an IP network.

You also have the option to configure SNMP traps which are alerts sent from SNMP-enabled devices to an SNMP agent or manager typically providing device status or condition information.

You can also access the **MIB** file which is a management information base. This file is a formal description of a set of network objects managed using the Simple Network Management Protocol (SNMP). The format of the **MIB** is defined as part of the SNMP. (All other **MIBs** are extensions of this basic management information base.)

Click **Download MIB**, to download the MIB file.

To configure SNMP:

1. Go to **Setup > SNMP Configuration**.
2. Under **SNMP Server Configuration**, check **Enabled** to activate the SNMP server. Click **Submit**.
3. If needed, click **Add** under **Allowed IP Addresses** for **SNMP v1/v2c**.
4. Click **Add Server Configuration**.
    a. Make sure that **Enabled** is checked.
    b. Under **Version**, select from the drop-down either **SNMP v1/v2c** or **SNMP v3**.
    c. For **SNMP v1** and **SNMP v2c**:
        i. Enter the **Configuration Name** for your SNMP configuration.
        ii. Enter **Community String** which is a read-only string used to authenticate incoming SNMP requests.
    d. For **SNMP v3**:
        i. Enter the **Authentication Protocol** from the drop-down, including **NONE, MD5**, or **SHA1**.
        ii. Enter the **Security Name** which is a username used to authenticate incoming SNMP v3 requests. If you selected **MD5** or **SHA1** for Authentication Protocol:
            - Enter the **Authentication Password**, which is a password used to authenticate incoming SNMPv3 requests.
            - Confirm the password.
        iii. Enter the **Encryption Protocol** for SNMPv3 messages from the drop-down, including **NONE, DES** or **AES-128**. If you selected **DES or AES-128** for **Encryption Protocol**:
            - Enter the **Encryption Password**.
            - Confirm the password.
    e. Click **Submit**.
5. The **SNMP Configuration** list displays your recently added SNMP Server Configuration. To edit the configuration, click the pencil icon under **Options**.
6. To delete an existing configuration, click the trash can icon under **Options**.
7. To save your changes, click **Save and Apply**. Or continue to **SNMP Trap Destinations** and **Add Trap Destinations**.

To configure SNMP Traps:

1. Go to **Setup > SNMP Configuration > SNMP Trap Configuration**, check **Enabled** to enable sending SNMP traps on the device..
2. The engine ID displays to the right of **Enabled**. Modify the engine ID or use the default value.
3. Click **Submit.**

4. Click **Add Trap Destination**.
    a. Make sure that **Enabled** box is checked.
    b. Enter the **Destination Name.**
    c. Select from the drop-down the **Version** of SNMP (**SNMP v1/v2c** or **SNMP v3**).
    d. For **SNMP v1** or **SNMP v2c**
        i. Enter the **Destination IP Address**.
        ii. Enter the **Community String**.
    e. For **SNMPv3**:
        i. Enter the **Destination IP Address**.
        ii. Enter **Security Name**.
        iii. Enter the **Authentication Protocol** from the drop-down, including **NONE, MD5,** or **SHA1**. If you selected **MD5** or **SHA1** for **Authentication Protocol**:
            i. Enter the **Authentication Password**, which is a password used to authenticate incoming SNMPv3 requests.
            ii. Confirm the password.
        iii. Enter the **Encryption Protocol** for SNMPv3 messages from the drop-down, including **NONE, DES**, or **AES-128**. If you selected **DES** or **AES-128** for Encryption Protocol:
            i. Enter the **Encryption Password**.
            ii. Confirm the password.
    f. Click **Submit**.
5. The **SNMP Trap Destination** list displays your recently added SNMP Trap Destination. To edit the destination, click the pencil icon under **Options**.
6. To delete an existing destination, click the **trash can** icon under **Options**.
7. To save your changes, click **Save and Apply**.

To download the MIB file:

1. Click **Download MIB** in the far right corner of the device display.
2. Download/save the file from your browser.

Configuring the Global Positioning System (GPS)

This GPS information applies only to the device models that support GPS.

Some devices have a built-in GPS receiver. If your device has a GPS receiver, the device can forward NMEA (National Marine Electronics Association) sentences from the GPS receiver to another device connected to the device. You can also send the GPS data over the network to a remote computer.

The key areas of GPS configuration include: **Server Configuration**, **Client Configuration** and **NMEA Configuration** along with **Current Position** information.

Notes:

- All enabled sentences are forwarded periodically using the interval specified in the **NMEA Configuration** section. Before forwarding, the device adds an ID prefix and ID to each enabled NMEA sentence. If set, the NMEA sentences available are those provided by the built-in receiver which are: GPGGA, GPGSA, GPGSV, GPGLL, GPRMC, GPVTG.
- You can simultaneously enable the TCP Server, and TCP/UDP client.

GPS Server Configuration

To setup the GPS Server Configuration:

1. Go to **Setup > GPS Configuration > Server Configuration**.
2. To enable server configuration, check **TCP Server**.
3. In the **Port** field, type the port number on which the TCP server is listening for connections. The default is **5445**. You can use up to five digits. Each digit itself must be between **0** and **9**. Numbers above **65,535** are illegal as the port identification fields are 16 bits long in the TCP header.
4. Enter **Password** and confirm **Password**.
5. Click **Submit**.
6. To save your changes, click **Save and Apply**.

Sending GPS information to a remote server

The **Client Configuration** allows the device to connect to a remote server using the IP and port information for uploading GPS data.

1. To allow the device to connect, go to **Setup > GPS Configuration > Client Configuration**.
2. Check **TCP/UDP Client**.
3. From the **Protocol** drop-down list, select the protocol of the client (**TCP or UDP**).
4. In the **Remote Host** field, type the IP address of the remote host.
5. In the **Port**, field type the port number of the remote host.
6. If your remote host requests a password, type that password in the **Password** field. The password is sent to the server in response.
7. Click **Submit**.
8. To save your changes, click **Save and Apply**.

Configuring NMEA Sentences

To configure the time interval, additional prefix or ID information, and which NMEA sentences that can be sent:

1. Go to **Setup > GPS Configuration > NMEA Configuration**.
2. **If Enable NMEA Mode** exists (disabled by default), check to enable. **NOTE:**GLL and VTG sentences cannot be enabled when NMEA Mode is disabled.
3. In the **Interval** field, type the amount of time, in seconds, that passes before the NMEA information is sent. The default is **10** seconds. The range is **1** to **255** seconds.
4. You can further identify the device, also called a remote asset, that is collecting and sending the GPS information. To do so:

   Add ID: The ID is an unique remote asset identification string. The ID string can be any length up to 20 characters. The *&* and *$* are invalid characters. The ID must follow the standard NMEA sentence structure. Refer to the Universal IP AT Commands Reference Guide for sentence structure.

   To add more information to the beginning of the ID, in the Add ID Prefix field, type the information.

5. For devices that do not have **Enable NMEA Mode**, you can select which NMEA sentence types you want to send. Check any combination of the available options: **GGA, GSA, GSV, GLL, RMC,** and **VTG**.

SMTP Settings

The following table lists the configuration fields in the SMTP window.

Field	Description
SMTP Configuration	
Enabled	Click to use the SMTP feature.
Server	Enter the SMTP server address.
Port	Enter the port number that the SMTP server uses.
Email	Enter the sender email address. This address will be added as the sender email address to the sent emails.
Username	Enter the name that can access the SMTP server.
Password	Enter the password that can access the SMTP server.
Mail Log Settings	
Entries to Keep	Enter the desired number of mail log entries that are to be stored in the device. The range of values is **10** to **1000**. If you click **Submit**, this setting is not applied to the emails that are in progress or deferred. Note that logs are not saved on the device. Also, logs do not persist through power cycles.
Send a Test Email	
Address	To make sure that the SMTP is configured properly, enter a destination email address, then click **Send Test Email**.

Configuring the Serial Port in Serial IP Mode

This features requires installation and configuration of mCard Accessory Card (such as an MTAC-MFSER) into your device first. To configure the serial terminal connected to the RS-232 connector on your accessory card:

1. Go to **Setup > Serial IP Configuration > Serial Port Settings**, check **Enabled**.
2. From the **Baud Rate** drop-down list, select the baud-rate at which the serial terminal communicates. The default is **115200**.
3. From the **Flow Control** drop-down list, select the flow control for the serial port. The options are **NONE** or **RTS-CTS**. The default is **NONE**.
4. From the **Parity** drop-down list, select the parity for the serial port. The options are **NONE, EVEN,** or **ODD**. The default is **NONE**.
5. To use the Modbus protocol as the protocol the serial devices use to communicate, check **Modbus Gateway** to the right of **Enabled**. **NOTE:** You may have the TCP connection encrypted with TLS. Make sure to check **Protocol** under **IP Pipe** and select **SSL/TLS**.
6. From the **Data Bits** drop-down list, select the data bits for the serial port. Data bit options are **7** or **8**. The default is **8**.

7. From the **Stop Bits** drop-down list, select the stop bits for the serial port. The options are **1** or **2**. The default is 1.
8. Click **Submit**.
9. To save your changes, click **Save and Apply**. If the device is set to **Serial Modem Mode**, the device reboots after applying any changes.

Configuring Device to Act as Client for Serial IP

You can set up the device to act as a client.

The TCP, UDP, SSL/TLS client feature enables the device to act as a proxy TCP, UDP, or SSL/TLS client to the serial terminal connected to the RS-232 port on the device. This helps the serial terminal access any TCP, UDP, or SSL/TLS server on the LAN/WAN allowing two-way traffic between the serial device and the remote server.

To use this function, you must first check **Enabled** under **Serial Port Settings**. To configure the IP Pipe in TCP, UDP, or SSL/TLS client mode:

1. Go to **Setup > Serial-IP Configuration > Serial Port Settings > IP Pipe** group.
2. From the **Mode** drop-down list, select **CLIENT**.
3. From the **Protocol** drop-down list, select the desired protocol: **TCP**, **UDP**, or **SSL/TLS**.
4. In the **Server IP Address** field, enter the address of the far-end TCP, UDP, or SSL/TLS server.
5. In the **Server Port** field, enter the port value used by the far-end TCP, UDP, or SSL/TLS server.
6. If the primary server is unavailable, in the **Secondary IP Address** field, enter the address of the alternate TCP, UDP, or SSL/TLS server.
7. If the primary server is unavailable, in the **Secondary Port** field, enter port number value of the alternate TCP, UDP, or SSL/TLS server.
8. From the **Connection Activation** drop-down list, select a connection method. Options are:

   ALWAYS-ON.

   CR. Three carriage returns must be received before the TCP, UDP, or SSL/TLS connection is established to the remote server.

   ON-DEMAND. Set the connection as available on-demand.
9. From the **Connection Termination** drop-down list, select a disconnect method for the IP pipe. Options are:

   ALWAYS-ON.

   TIMEOUT. The IP pipe connection disconnects if the configured timer expires with no data sent or received. In the **Timeout** field, enter the desired number of seconds for this timeout. The valid timeout range is from **0 to 900 seconds**. Timeout of zero seconds disables the timeout and it is equivalent to **ALWAYS-ON**.

   SEQUENCE. A sequence of received characters disconnects the IP pipe.
10. In the **Buffer Timeout** field, enter the timeout after which data is sent to the network if the buffer is not full (in milliseconds).
11. In the **Buffer Size** field, enter the size of the buffer for reading data from the serial port and sending to the network (in bytes). Data is sent when the buffer is full.
12. Click **Submit**.
13. To save your changes, click **Save and Apply**. If the device is set to **Serial Modem Mode**, the device reboots after applying any changes.

To configure security settings:

1. Make sure you select **SSL/TLS** under **Protocol**.
2. Under **Security Settings**, click the **Show** to the right.
3. Select any TLS version. Check **TLSv1.3, TLSv1.2** and/or **TLSv1.1 (deprecated)**. Default: **TLSv1.3** and **TLSv1.2** are enabled.
4. Check any preferred Cipher Suite from the following list: **TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-GCM-SHA256,TLS_AES_128_GCM_SHA256,** and also including the following deprecated ciphers: **ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA,** and/or **AES128-SHA.** Default: **All.** (You can also set the priority order of the ciphers).
5. Click **Submit**.
6. To save your settings, click **Save and Apply**.

Configuring Device to Act as Server for Serial IP

You can set up the device to act as a server.

The TCP, UDP, SSL/TLS server feature enables a TCP, UDP, SSL/TLS client on the Ethernet network to connect to the remote serial terminal that is connected to the RS-232 port on the device. The device acts as a TCP, UDP, SSL/TLS server which allows two-way traffic between the TCP, UDP, SSL/TLS client and the remote terminal on the serial port.

To use this function, you must first check **Enabled** under **Serial Port Settings**. To configure the IP Pipe in TCP, UDP, SSL/TLS server mode:

1. Go to **Setup > Serial-IP Configuration > Serial Port Settings > IP Pipe** group.
2. In the **Mode** drop-down list, select **SERVER**.
3. From the **Protocol** drop-down list, select the desired protocol: **TCP**, **UDP**, or **SSL/TLS**.
4. In the **Buffer Timeout** field, enter the timeout after which data is sent to the network if the buffer is not full (in milliseconds).
5. In the **Server Port** field, type the desired port value in the range **1** to **65535**.
6. In the **Buffer Size** field, enter the size of the buffer for reading data from the serial port and sending to the network (in bytes). Data is sent when the buffer is full.
7. From the **Connection Termination** drop-down list, select a disconnect method for the IP pipe. Options are:

   ALWAYS-ON.

   TIMEOUT. The IP pipe connection disconnects if the configured timer expires with no data sent or received. In the **Timeout** field, enter the desired number of seconds for this timeout. The valid timeout range is from **0 to 900 seconds**. Timeout of zero seconds disables the timeout and it is equivalent to ALWAYS-ON.

   SEQUENCE. A sequence of received characters disconnects the IP pipe.
8. Click **Submit**.
9. To save your changes, click **Save and Apply**. If the device is set to **Serial Modem Mode**, the device reboots after applying any changes.

To configure security settings:

1. Make sure you select **SSL/TLS** under **Protocol**.
2. Under **Security Settings**, click the **Show** to the right.
3. Select any **TLS version**. Check **TLSv1.3, TLSv1.2** and/or **TLSv1.1 (deprecated)**. Default: **TLSv1.3** and **TLSv1.2** are enabled.
4. Check any **Cipher Suite** from the following list: **TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-GCM-SHA256,TLS_AES_128_GCM_SHA256**, and also including the following deprecated ciphers: **ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA**, and/or **AES128-SHA**. Default: **All.**
5. Click **Submit**.
6. To save your settings, click **Save and Apply**.

Time Configuration

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

Setting the Date and Time

To set the device's date and time:

1. From **Setup**, select **Time Configuration**.
2. In the **Date** field, select today's date from the pop-up calendar that opens.
3. In the **Time** field, type the time (24-hour).
4. From the **Time Zone** drop-down list, select your time zone. The default selection is UTC (Universal Coordinated Time, Universal Time).

   Note: To learn more about time zones, visit the following website : http://www.https://greenwichmeantime.com/time-zone/
5. Click **Submit**.
6. To save your changes, click **Save and Apply**.

Configuring SNTP Client to Update Date and Time

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

1. To enable SNTP to update the date and time, check **Enabled**.
2. In the **Polling Time** field, type the time that passes (in minutes), after which the SNTP client requests the server to update the time. Default is 120 minutes.
3. In the **Server** field, type the SNTP server name or IP address that is contacted to update the time.
4. In the **Backup Server 1 - 4** fields, you may enter the SNTP server name or IP address of up to four backup SNTP servers. These fields are optional.
5. Click **Submit**.

6. To save your changes, click **Save and Apply**.

Chapter 6 – Wireless

Setting Up Wi-Fi Access Point

If you ordered a device with Wi-Fi capability, it can be configured as a wireless access point (AP). This allows Wi-Fi enabled devices to connect to your device using Wi-Fi. The Wi-Fi access point can have up to 5 clients at a time. To set up your device as an access point:

1. Go to **Wireless > Wi-Fi Access Point**.
2. To enable Wi-Fi Access Point mode, check **Enabled**.
3. To set the SSID (service set identifier) for the access point supported by your device, in the **SSID** field, type the name. The Wi-Fi devices look for this ID in order to join the wireless network. All wireless devices on a WLAN must use the same SSID in order to communicate with the access point.
4. To specify the data rates supported, in the **Network Mode** drop-down list, select the desired option. Possible values are B/G/N-Mixed, B/G-Mixed, B-Only, and N-Only.
5. From the **Channel** drop-down list, select the channel on which the device operates. Channels 1-11 are available.
6. In the **Beacon Interval** field, enter the period of time, in milliseconds, when the access point sends a beacon packet. Beacons help synchronize a wireless network. For most applications, the default value of 100 provides good performance.
7. In the **DTIM Interval** field, enter how often a beacon frame includes a Delivery Traffic Indication Message, and this number is included in each beacon frame. It is generated within the periodic beacon at a frequency specified by the DTIM Interval. A delivery traffic indication message is a kind of traffic indication message (TIM) which informs the clients about the presence of buffered multicast/broadcast data on the access point. The default value of 1 provides good performance for most applications. You might want to increase this value when using battery powered Wi-Fi devices, which can sleep (at reduced power consumption) during the longer DTIM interval period. You must balance the power savings from increasing the DTIM interval against possible reduced communication throughput.
8. In the **RTS Threshold** field, type the frame size at which the AP transmissions must use the RTS/CTS protocol. This is often used to solve hidden node problems. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth. However, the more RTS packets that are sent, the quicker the system can recover from interference or collisions.

For related information, see Setting Security Options and Viewing Information About Wi-Fi Clients Using Your Wireless Network.

Setting Security Options

Specify the security protocol that your device uses to secure the communications from it to the connected devices under **Security Options**.

1. From the **Mode** drop-down list, select the security protocol you want to use. Options include:

   None

   WEP: Use Wired Equivalent Privacy protocol to allow a group of devices on the network to exchange coded messages.

   WPA-PSK: Use Wi-Fi protected access to secure data exchanged on your network.

   WPA2-PSK: Use Wi-Fi protected access version 2 to secure data exchanged on your network.

   WPA/WPA2-PSK: Use Wi-Fi protected access version 1 and 2 to secure data exchanged on your network.

2. To select **WEP** mode:
   a. From the **Encryption** drop-down list, select the encryption to be used. Choose from **64 bit 10 hex digits** or **128 bit 26 hex digits**.
   b. To generate a key from a phrase, in the **Passphrase** field, type a phrase. Click **Generate**.
   c. To manually enter keys, type the keys in the Key 1, Key 2, Key 3 or Key 4 fields.
3. To select **WPA-PSK, WPA2-PSK** or **WPA-PSK/WPA2-PSK** modes:
   a. Select the WPA Algorithm from the drop-down list. Choose from **TKIP, AES** or **TKIP+AES**.
   b. In the **Shared Key** field, type the key that is used for encrypting and decrypting the data.
   c. To remove the mask characters, thereby making the Shared Key visible, check **Unmask**.
4. When done, click **Submit**.
5. To save your changes, click **Save and Apply**.

Viewing Information About Wi-Fi Clients Using Your Wireless Network

To view information about clients (such as computers, tablets, and smart phones) that are connected to your device's Wi-Fi access point:

1. The Clients group displays a list of clients using your device's Wi-Fi.
2. To update the list, click **Refresh**.

Setting Up Wi-Fi as WAN

To setup the device's Wi-Fi as WAN:

1. Go to **Wireless > Wi-Fi as WAN.**
2. To enable Wi-Fi as WAN mode, check **Enabled**. (**Note:** After you enable or disable **Wi-Fi as WAN** and apply that change, the device reboots.)
3. Click **Save and Apply**. **Note**: **Save and Apply** the device to get a list of available Wi-Fi Networks.
4. Go to **Wireless > Wi-Fi as WAN**.
5. Searching for available Wi-Fi networks starts automatically. After 30 to 60 seconds, a list of detected Wi-Fi Access Points appears in the **Available Networks** group.
6. In the **Available Wi-Fi Networks** group, click the SSID for the Wi-Fi access point you want to use. The **Add Saved Network** window opens. Here are the available fields to enter information:

   Network Name

   Hidden Network(only check if your target network is currently hidden)

   SSID

   Security Mode: None, WEP, WPA, WPA-PSK, WPA-2, or **WPA-2-PSK**

   Username

   Password

   Unmask (Check, Uncheck)

   WPA Algorithm: TKIP, +AES, TKIP, or **AES**

   Shared Key

   Key Index: 0 - 3

   Network Key

IEEE 802.1x

7. Review the information, enter any required security info, then click **Finish**. The Wi-Fi access point you just added appears in the **Saved Wi-Fi Networks** group.
8. If desired, add additional access points to the list of Saved Networks. The device tries to connect to **Saved Wi-Fi Networks** in the order they are listed. You can change the order by clicking the up or down arrows shown under **Options**.
9. When finished, click **Save and Apply**. The Status field displays "Connected" if you have successfully connected to the Wi-Fi access point.

Note: You cannot edit the network name and you cannot delete a network if it is used in another configuration.

Setting up Bluetooth

The Bluetooth-IP feature allows a data connection between a remote TCP/UDP client or server and a local Bluetooth device. To set up the Bluetooth connection:

1. Go to **Wireless > Bluetooth-IP**
2. To enable the feature, check **Enabled**. Click **Submit**.
3. Confirm that the far-end Bluetooth device is powered on and waiting for a connection.
4. In the **Available Devices** group, click **Refresh**. A list of detected Bluetooth devices appears.
5. Click the name of the Bluetooth device that you want to use. The name and MAC address appear under the **Selected Device**.
6. To add a device, click **Add Device** and enter the device name and the **MAC address**.
7. Click **Finish**.
8. To save your changes, click **Save and Apply**.

Note: You cannot edit the network name and you cannot delete a network if it is used in another configuration.

IP Pipe in TCP/UDP Server mode

1. In the **IP Pipe** group, from the **Mode** drop-down list, select **SERVER**.
2. From the **Protocol** drop-down list, select the desired protocol, either **TCP** or **UDP**.
3. In the **Server Port** field, type the desired port value in the range **1** to **65535**.
4. From the **Connection Termination** drop-down list, select a disconnect method for the IP pipe. Options are:
   - **ALWAYS-ON**
   - **SEQUENCE:** A sequence of characters received from the Bluetooth side used to disconnect the IP pipe.
   - **TIMEOUT:** The IP pipe connection disconnects if the configured timer expires with no data sent or received. A timeout of zero seconds disables the timeout, it is equivalent to **ALWAYS-ON**.

To configure the IP Pipe in TCP/UDP Client mode

1. In the **IP Pipe** group, from the **Mode** drop down list, select **CLIENT**.
2. From the **Protocol** drop-down list, select the desired protocol, either **TCP** or **UDP**.
3. In the **Server IP Address** field, type the address of the far-end TCP-UDP server.
4. In the **Server Port** field, type the port value used by the far-end TCP/UDP Server.
5. In case the primary server is unavailable, in the **Secondary IP Address** field and in the **Secondary Port** field, type the IP address and port number, respectively, of the alternate TCP/UDP server.

6. From the **Connection Activation** drop-down list, select a connection method. Options are:
    - **ALWAYS-ON**
    - **ON-DEMAND**
    - **CR:** Three carriage returns must be received from the Bluetooth side before TCP/UDP connection is established to the remote server.
7. From the **Connection Termination** drop-down list select a disconnect method for the IP pipe. Options are:
    - **ALWAYS-ON:**
    - **TIMEOUT:** The IP pipe connection disconnects if the configured timer expires with no data sent or received. A timeout of zero seconds disables the timeout, it is equivalent to **ALWAYS-ON**.
    - **SEQUENCE:** A sequence of characters received from the Bluetooth side used to disconnect the IP pipe.
8. Click **Submit**.
9. To save your changes, click **Save and Apply**.
    - The device immediately connects to the local Bluetooth device. If successful the **Status** field displays **Connected**. If **IP Pipe** is configured for **SERVER**, the IP connection is initiated by the far-end TCP/UDP client.
    - If **Mode** is set to **CLIENT**, the device initiates connections for the far-end TCP/UDP server based on the configured **Connection Activation** conditions are met.

To configure security settings:

1. Make sure you select **SSL/TLS** under **Protocol**.
2. Under **Security Settings**, click the **Show** to the right.
3. Select any TLS version. Check **TLSv1.3, TLSv1.2** and/or **TLSv1.1 (deprecated)**. Default: **TLSv1.3** and **TLSv1.2** are enabled.
4. Check any preferred Cipher Suite from the following list: **TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256**, **TLS_AES_128_GCM_SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-GCM-SHA256,TLS_AES_128_GCM_SHA256,** and also including the following deprecated ciphers: **ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA,** and/or **AES128-SHA.** Default: **All**.
5. Click **Submit**.
6. To save your settings, click **Save and Apply**.

Bluetooth Low Energy (BLE)

Bluetooth Low Energy allows you to search and/or scan for BLE devices. You can connect with selected BLE device to obtain the list of UUIDs for services and characteristics that are supported on the device.

A python library called gattlib is integrated into the device and can be used for scans, reads, writes, and handling notifications.

You must develop a custom application to read and accept the data from a BLE device. Please refer to the example on the BLE for mLinux page as well as the Creating a Custom Application page.

1. Go to **Wireless > Bluetooth Low Energy > Settings**, check the **Enabled** box.
2. Under **Power Mode**, select from the drop-down including **Custom, High, Medium** or **Low**.

3. Click **Submit.**
4. Under the **Available Device Servers**, the detected BLE devices appear.
5. To choose a device from the **Available Device Servers**, click on the name of your desired device.
6. If you do not see your desired device, click **Add Device.** Enter the **Name** and **MAC Address** of your BLE device.
7. Click **OK**. Your device appears under **Saved Devices**.
8. Click **Save and Restart** to save your changes.

You may also restart BLE by clicking **Reset Bluetooth** above **Saved Devices** section.

Chapter 7 – Firewall

Defining Firewall Rules

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

The firewall is built on top of iptables. The different rule groups correspond to their respective chains in iptables.

Note: As a best security practice, the device employs minimum firewall rules by default. This means by default the device allows all outbound traffic from it in the Output Filter Rules. (Traffic through the device is handled by the Port/Inbound Forwarding Rules.) But all traffic to the device via WAN interfaces is blocked by default in the Input Filter Rules. Users may create their own specific and targeted input filter rules to allow certain traffic to the device based on their specific needs. For additional information, see:

- Adding Port Forwarding Rules
- Adding Input Filter Rules
- Adding Output Filter Rules
- Advanced Settings

Trusted IP

Trusted IP is a simplified interface to create iptables rules to allow or block specific IPs, IP ranges, or subnets. This feature allows users to create whitelists (which are allowed or trusted IPs) or black lists (which are blocked or unwanted IPs). You can add, edit, and delete IP addresses as needed.

If you select **White List** as **Trusted IP Mode** and you do not set any IP range, no traffic will be allowed. If you select **Black List** as **Trusted IP Mode** and you do not set any IP range, all traffic will be allowed.

To set up a Trusted IP range:

1. Go to **Firewall > Trusted IP**.
2. Check the **Enabled** box to turn on Trusted IP.
3. Select the **Trusted IP Mode** from the drop-down, either **White List** or **Black List**. (**NOTE**: Be aware of the behavior of each list and its consequences based on your specific configuration. For example, if you select **White List** as **Trusted IP Mode**, you should include the device **IP Address Range** or **IP Address** and **Subnet Mask** to maintain your local device LAN access.)
4. To add IP addresses, click **Add IP Range** in the upper right corner.
5. Under the **Add IP Range**, enter or select the following parameters:
    a. **Name**
    b. Mode from drop-down, either **Subnet** or **IP Range**.
    c. For **Subnet**:
        i. **IP Address**
        ii. **Subnet Mask**
    d. For **IP Range**:

i. **IP Address Start**
ii. **IP Address End**

e. **Destination Port** (default: **ANY**)
f. **Protocol** from drop-down including **ANY, TCP/UDP, TCP**, or **UDP**
g. Click **Finish**.

6. The system displays your recently added and existing IP ranges in a list. The list includes the relevant details. You may edit any IP ranges by clicking on the pencil icon under **Options**.
7. You may delete any IP ranges by clicking on the trash can icon under **Options**.
8. If you want to revert back to default settings (where **Trusted IP** is disabled and all IP ranges are removed), click the **Reset to Default** button in the lower right corner
9. Click **Submit**.
10. To save your changes, click **Save and Apply**.

Prerouting Rule

Add a DNAT rule

To add prerouting or DNAT rule to your firewall:

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Prerouting Rules** group, click **Add DNAT Rule**.
3. In the **Filter Rule** section, enter a name for the rule and optionally, a description.
4. In the **Destination IP** field, enter the destination IP address that applies to this rule.
5. In the **Destination Port** field, enter the destination port that applies to this rule. If there is a range of ports, the ending port is automatically set.
6. In the **Destination Mask** field, enter the subnet mask of the destination that applies to this rule.
7. In the **Destination Interface** field, select the interface used by the destination that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN**.
8. In the **Source IP** field, enter the source IP address that applies to this rule.
9. In the **Source Port** field, enter the source port that applies to this rule.
10. In the **SourceMask** field, enter source subnet mask that applies to this rule.
11. In the **SourceMAC** field, enter the source MAC address for the device that applies to this rule.
12. In the **SourceInterface** field, select the source interface that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN**.
13. In the **Protocol** drop-down list, select the protocol of the messages that apply to this rule. Select from **TCP/UDP**, **TCP**, **UDP**, or **ANY**.
14. In the **NAT IP** field, enter the local IP address for the Network Address Translation.
15. In the **NAT Port** field, enter the port used for the Network Address Translation.
16. **Check Enable NAT Loopback if you want to redirect LAN packets destined for the WAN's public IP address.**
17. Click **Submit**.
18. To save your changes, click **Save and Apply**.

Postrouting Rule

Add a SNAT rule

To add postrouting or SNAT rule to your firewall:

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Postrouting Rules** group, click **Add SNAT Rule**.
3. In the **Postrouting Rule** section, enter a name for the rule and optionally, a description.
4. In the **Destination IP** field, enter the destination IP address that applies to this rule.
5. In the **Destination Port** field, enter the destination port that applies to this rule. If there is a range of ports, the ending port is automatically set.
6. In the **Destination Mask** field, enter the subnet mask of the destination that applies to this rule.
7. In the **Destination Interface** field, select the interface used by the destination that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN**.
8. In the **Source IP** field, enter the source IP address that applies to this rule.
9. In the **Source Port** field, enter the source port that applies to this rule.
10. In the **SourceMask** field, enter source subnet mask that applies to this rule.
11. In the **SourceInterface** field, select the source interface that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN**.
12. In the **Protocol** drop-down list, select the protocol of the messages that apply to this rule. Select from **TCP/UDP**, **TCP**, **UDP**, or **ANY**.
13. In the **NAT IP** field, enter the public IP address for the Network Address Translation.
14. In the **Target** field, select the desired action of the firewall based on this rule from the drop-down menu. Choose from **SNAT** or **MASQUERADE**.
15. In the **NAT Port** field, enter the port used publicly for the Network Address Translation.
16. Click **Submit**.
17. To save your changes, click **Save and Apply**.

Input Filter Rules

To add an input filter rule to your firewall:

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Input Filter Rules** group, click **Add Rule**.
3. In the **Filter Rule** section, enter a name for the rule and optionally, a description.
4. In the **Destination IP** field, enter the destination IP address that applies to this rule.
5. In the **Destination Port** field, enter the destination port that applies to this rule. If there is a range of ports, the ending port is automatically set.
6. In the **Destination Mask** field, enter the subnet mask of the destination that applies to this rule.
7. In the **Destination Interface** field, select the interface used by the destination that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN**.
8. In the **Source IP** field, enter the source IP address that applies to this rule.
9. In the **Source Ports** field, enter the source port range that applies to this rule.
10. In the **Source Mask** field, enter source subnet mask that applies to this rule.

11. In the **Source MAC** field, enter the source MAC address for the device that applies to this rule.
12. In the **Source Interface** field, select the source interface that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN**.
13. In the **Protocol** drop-down list, select the protocol of the messages that apply to this rule. Select from **TCP/UDP**, **TCP**, **UDP**, or **ANY**.
14. In the **Chain** field, select the grouping based on the type of traffic affected by the rule from the drop-down menu. Select from **INPUT, FORWARD,** or **OUTPUT**.
15. In the **Target** field, select the desired action of the firewall based on this rule from the drop-down menu. Choose from **ACCEPT, REJECT, DROP,** or **LOG**.
16. Click **Submit**.
17. To save your changes, click **Save and Apply**.

Adding Port Forwarding Rules

Inbound Forwarding Rule

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

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Port Forwarding** group, click **Add Rule**.
3. In the **Filter Rule section**, enter a name for the rule and optionally, a description.
4. In the **Destination IP** field, enter the destination IP address that applies to this rule.
5. In the **Destination Port** field, enter the destination port that applies to this rule. If there is a range of ports, the ending port is automatically set.
6. In the **Destination Mask** field, enter the subnet mask of the destination that applies to this rule.
7. In the **Destination Interface** field, select the interface used by the destination that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN.**
8. In the **Source IP** field, enter the source IP address that applies to this rule.
9. In the **Source Ports** field, enter the source port range that applies to this rule.
10. In the **Source Mask** field, enter source subnet mask that applies to this rule.
11. In the **Source MAC** field, enter the source MAC address for the device that applies to this rule.
12. In the **Source Interface** field, select the source interface that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN**.
13. In the **Protocol** drop-down list, select the protocol of the messages that apply to this rule. Select from **TCP/UDP**, **TCP**, **UDP**, or **ANY**.
14. In the **Chain** field, select the grouping based on the type of traffic affected by the rule from the drop-down menu. Select from **INPUT, FORWARD,** or **OUTPUT**.
15. In the **Target** field, select the desired action of the firewall based on this rule from the drop-down menu. Choose from **ACCEPT, REJECT, DROP,** or **LOG**.
16. Click **Submit**.
17. To save your changes, click **Save and Apply**.

A default filter allowing forwarded packets through the firewall is automatically created. If desired, you can use the **Advanced Settings** mode of the Port Forwarding configuration to further restrict packets based on source address and source ports using the **Inbound Filter Rule**. In most cases, this is not necessary.

Output Filter Rules

To prevent a device within the LAN from communicating with a device in an external network, you must establish a firewall rule to drop packets destined to the external device.

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. Click **Add Rule** in the **Output Filter Rules** section.
3. Enter a **Name** for the rule and optionally, a **Description**.
4. In the **Destination IP** field, type the IP address of the device or network that packets are to be sent to. Type **ANY** if the destination address does not matter.
5. In the **Destination Port** field, type the port for which that the packets are destined. Common destination ports are listed in the Destination Port field's attached drop-down. Type **ANY** if the destination port does not matter.
6. In the **Destination Mask** field, type the network mask of the destination network.
7. In the **Destination Interface** field, select the interface used by the destination that applies to this rule from the drop-down. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN**.
8. In the **Source IP** field, type the IP address of the device or network that the traffic originates from. Type **ANY** if the source address does not matter.
9. In the **Source Port** field, type the port that is the origin of the traffic. Type **ANY** if the source port does not matter.
10. In the **Source Mask** field, type a network mask for the origin of the traffic.
11. In the **SourceMAC** field, enter the source MAC address for the device that applies to this rule.
12. In the **Source Interface** field, select the source interface that applies to this rule from the drop-down. Select from **ANY, LAN, WAN, ETHERNET, CELLULAR, WI-FI WAN, WI-FI AP,** or **OPENVPN**.
13. From the **Protocol** drop-down, select the protocol of the messages that apply to this rule. Choose from **TCP/UDP**, **TCP**, **UDP**, or **ANY**.
14. In the **Chain** field, select the grouping based on the type of traffic affected by the rule from the drop-down. Select from **INPUT, FORWARD,** or **OUTPUT**.
15. In the **Target** field, select the desired action of the firewall based on this rule from the drop-down. Choose from **ACCEPT, REJECT, DROP,** or **LOG**.
16. Click **Submit**.
17. To save your changes, click **Save and Apply**.

Advanced Settings

The **Firewall's Advanced Settings** mode lets you manipulate **DNAT, SNAT**, and **Filter** rules directly. **DNAT** rules can manipulate the destination address and port of a packet; similarly **SNAT** rules can manipulate the source address and port of a packet.

Filter rules apply an **ACCEPT, REJECT, DROP**, or **LOG** action to a packet. A **DNAT or SNAT** rule with the same name as a **Forwarding** rule will be associated under **Normal Settings** for **Port Forwarding/NAT** rules.

- Adding Prerouting Rules
- Adding Postrouting Rules

Setting up Static Routes

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

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

Chapter 8 – Cellular

Configuring Cellular

To configure how cellular is used on your device:

1. Go to **Cellular > Cellular Configuration** to display the **Cellular Configuration** window.
2. Check **Enabled**.
3. Check and change the Cellular Configuration fields as desired. For field descriptions, see Cellular Configuration Fields.
4. Click **Submit**.
5. To save your changes, click **Save and Apply**.

Cellular Configuration Fields

Field	Description
General Configuration	
Enabled	Allows the device to establish a cellular PPP or WWAN connection. After you enable or disable PPP and apply that change, the device reboots.
Mode (varies with model)	Choose from either PPP or WWAN for the cellular connection mode. (NOTE: For some models, this field is not available and the device defaults to PPP. Some fields described here are not used in WWAN mode.)
Protocol Support	Select the IP protocol from the drop-down (either IPv4 or IPv6).
Dial-on-Demand[1]	Enables the Dial-on-Demand feature. If enabled, the device brings up and maintains a cellular connection while network activity on the LAN requires WAN access. The device brings down the cellular connection when outgoing network traffic ceases for the given Idle Timeout duration. Enable this feature when Wakeup-on-Call is enabled to allow the device to "sleep" after it has been "woken up." See **Configuring Wakeup-on-Call** for more information.
Diversity (For H5, H6, LTE)	Allows the use of two antennas to increase receive signal quality. Not all models support diversity. If diversity is enabled, connect a second cellular antenna to the AUX port on the device. Otherwise, the cellular performance of the device may degrade.
Connect Timeout	The time (in seconds) that the device waits before it deems that the connection attempt has failed. The value used is the amount of time that elapses between each dialing retry.
Dialing Max Retries	Number of dialing retries allowed; the default is zero, which means an infinite number is allowed.
Cellular Mode (varies with model)	Select the Cellular Mode from the drop-down based on the cellular radio module in your device including: **Auto (default), LTE Only, LTE prefer, 2G only, 3G only,** or **3G prefer**. NOTE: Values vary based on model. For some models, this field is not available.
IPv4/IPv6 Address	The IP address of the device.

Field	Description
IPv4/IPv6 Primary DNS	The IP address of the primary DNS server (optional).
Public IPv4 Mask	The public mask for IPv4 (either 32 or 24).
Packet Size Settings	
MTU	Specifies the maximum transmit unit. The value must be between 128 and 16834 (default: 1500).
MRU	Specifies the maximum receive unit. The value must be between 128 and 16834 (default: 1500).
Modem Configuration	
Firmware Image (Only available for specific models)	Only available for specific radio models including -L4N1, -LNA3, or -MNG2. Allows user to switch from one network carrier to another. Select from the drop-down either **AT&T Compatible** (default)**,** or **Verizon** for -L4N1. Select from the drop-down either **Auto** (default), **AT&T Compatible,** or **Verizon** for -LNA3. Select from **Auto** (default), **AT&T Compatible, Verizon,** or **World-Wide** for -MNG2. The **Auto** option automatically detects your SIM and configures the device for the appropriate carrier.
Dial Number	The modem dial string is: ▪ ***99***1#** for GSM/GPRS/non-Verizon LTE devices If the Dial Number is empty, the system uses the dial string based on the detected provider (**AUTO**).
Connect String	The modem response to initiate a PPP connection, usually **CONNECT**.
Dial Prefix	The modem AT command that initiates a PPP connection, usually **ATDT** or **ATD**.
SIM Pin	The pin used to unlock the SIM for use (only required if the SIM is locked). This does not apply to CDMA radios.
PDP Context Mode	A value used to establish a cellular connection. Value is determined automatically and depends on the carrier. Select from drop-down either: **AUTO** (default), **IP, IPV4V6**, or **IPV6.**
APN	The Access Point Name assigned by the wireless service provider (carrier specific).
Init String#	Optional fields to apply additional AT commands that execute just before every PPP connection attempt. Use these fields to expand functionality and to troubleshoot.
Authentication	
Authentication Type	The type of authentication to use when establishing a PPP connection: **NONE, PAP, CHAP, or PAP-CHAP** (either). Authentication may not be required by the cellular service provider. After you select and apply that change, the device reboots.
Username	Name of the user that the remote PPP peer uses to authenticate.
Password	Password that the remote PPP peer uses to authenticate.

Field	Description
Keep Alive[1] Used to periodically check if the cellular link is up; if not, the device tries to establish the link.	
ICMP/TCP Check[1] An active check that provides the most reliable and reactive diagnosis of the cellular link, but requires sending data through the cellular link.	
Enabled[1]	Enables the Active Keep Alive check. Depending on the plan type and data usage, this may result in additional data charges.
Keep Alive Type[1]	Protocol type for active keep alive, either **TCP** or **ICMP**. **ICMP** periodically pings the designated host at the specified interval. **TCP** tries to make a connection to the designated host at the interval specified.
Interval[1]	Time in seconds between active checking of the cellular link.
Hostname[1]	Host name or IP address for the keep alive check.
TCP Port[1]	TCP port number to connect with the TCP server (only visible when **Keep Alive Type TCP** is selected).
ICMP Count[1]	Number of sequential, unsuccessful ping attempts to the specified host to declare that the link needs to be re-established (only visible when **Keep Alive Type ICMP** is selected).
Data Receive Monitor A passive check that observes the absence of packets received over a given amount of time. This check cannot reliably determine if the link is down; no network traffic may cause the monitor to signal to shutdown and re-establish the cellular link even though the link was in a good state.	
Enabled	Enable or disable the passive monitoring of the cellular link.
Window	The amount of time that can pass without receiving network traffic before the cellular link is torn down and re-established.
Network Registration Reset Timeout Checks for the network registration every 10 seconds, and if no network registration occurs during the set interval, the radio modem is reset.	
Enabled	If enabled, radio will reset if no network registration occurs before the timeout period has elapsed.
Timeout (minutes)	Amount of time (in minutes) that passes before the radio is reset in case the modem is not registered in a network.

[1]If you choose **PPP-IP Passthrough** and **Serial Modem** mode, this field is not available.

Configuring Wake Up On Call

This feature allows the device to wake up and initiate a cellular connection when there is an incoming call, SMS, or LAN activity.

The Wake Up on Call function is not available for the LVW2 or Cat M1 devices (even though you can access those settings in the device software.)

1. Go to **Cellular > Wake Up On Call** to display the configurations.
2. Check the **Wake Up On Call** box.
3. Select a Wake Up setting. For wakeup methods, see Wake Up On Call Method Settings.
4. Click **Submit**.
5. To save your changes, click **Save and Apply**.

Note: This feature only defines when the device brings up its cellular link, not when the device takes it down. See the **Dial on Demand** option on the **Cellular Configuration** page at **Cellular > Cellular Configuration** to configure the criteria for bringing the cellular link down.

Wake Up On Call Method Settings

The triggers that wake up the device to re-establish the cellular link are:

- On Ring:

  Any incoming call will bring up the cellular link.

  Enabled: Check to allow any incoming call to wake up the device.

  Message: The expected response from the integrated cellular modem to an incoming call.

- On Caller ID:

  Only incoming calls in the caller ID list will bring up the cellular link.

  Enabled: Check to allow a specific caller to wake up the device.

  Caller ID: Field to specify a caller ID. Enter the ID then click **Add** to add the caller to the approved caller ID trigger list.

- On SMS (not available if you enabled SMS through **SMS > General Configuration**):

  Only specific SMS messages will bring up the cellular link.

  Enabled: Check to allow specific SMS messages to wake up the device.

  Message: Field to specify the SMS message contents. Click **Add** to add the SMS message to the approved SMS trigger list.

For Wake-Up-On-Call field descriptions, see Wake Up On Call General Configurations.

Wake Up On Call General Configurations

Field	Description
Wake Up on Call check box	Enables the Wake Up On Call feature.
Dial On Demand LAN	When checked, the device allows network activity on the LAN that needs WAN access to trigger the Wake Up and establish the cellular link. If this configuration is not checked, the device will only establish a cellular connection when the selected Wake Up method is triggered via incoming call, caller ID, and/or short message service (SMS).
Time Delay	Time that passes between a receiving call and initiating the Wake Up On Call connection.
Acknowledgment String to Caller	String used to acknowledge to the delivering SMSC (short message service center) the receipt of an SMS.

Field	Description
Init String Number	Device initialization strings specific to the integrated cellular modem required for the Wake Up On Call feature.

Radio Status

Field	Description
Module Information	
IMEI	International Mobile Station Equipment Identifier
IMSI	International Mobile Subscriber Identifier.
Manufacturer	Company that developed the cellular module.
Model	Cellular module model number.
Hardware Revision	Module's hardware revision.
MDN (Phone Number)	Mobile Directory Number. In some SIM/carriers, the value may not be present and therefore not displayed.
MSID	Mobile Station ID. Some SIM/carriers do not contain this value and therefore the value is not displayed.
Firmware Version	Module's firmware version.
Service Information	
Home Network	Cellular service provider associated with the module's data account.
Current Network	Current cellular service operator (Not available for C2 or EV3 models).
RSSI	Received Signal Strength Indication (RSSI is pure wide band power including intracell power, interference, and noise): RSSI [dBm] = RSCP[dBm] - Ec/Io[dB].
Service	Cellular service connection type.
Roaming	Indicates whether or not the current service is provided by the Home Network carrier.
Engineering Details	
Tx Pwr	Transmit Power.
PCS	3G Service.
Ec/Io	Signal to Noise Ratio (used to calculate RSSI in 3G devices).
RSCP	Received Signal Code Power (used to calculate RSSI in 3G devices).
RSRP	Reference Signal Received Power (used to calculate RSSI in LTE devices).
RSRQ	Reference Signal Received Quality (used to calculate RSSI in LTE devices): RSRQ = (N * RSRP) / RSSI where N is the number of Physical Resource Blocks (BRBs) over which RSSI is measured, typically equal to system bandwidth.
DRX	Discontinuous Reception.
Mobility Management State	State of cellular radio.
Radio Service State	On/off status of cellular radio.
Network Operator Mode	Cellular provider's Network Operation Mode.
Block Error Rate	Number of erroneous blocks / total number of received blocks.

Field	Description
Service Domain	Network Domain/Service Area.
Update Options	
MDN (Phone Number)	Update the cellular module's phone number. This number is updated only on the device. The MDN that the carrier has associated with this device does not change.

Radio Firmware Upgrade

Applies to specific models only

Radio firmware upgrades are available for some specific Telit and Quectel cellular radios. Refer below for details on specific models.

There are two types of radio firmware upgrades:

1. **Full Firmware Image Upgrade:** When applied, the full firmware update replaces the current firmware image with the new image of the new version.
2. **Delta Firmware Upgrade:** When applied, the current firmware image is updated with the differences between it and the new version, and effectively becomes the new version of firmware.

You can distinguish between upgrade types by looking for the term **FULL** or **DELTA** in the radio firmware upgrade filename.

Those models that support both full firmware and delta upgrades include: **LNA7, LEU7, L4N1, L4E1,** and **L4G1**.

Those models that support only full firmware upgrades include: **H5, H6, LAT1, LAT3, LDC3, LEU1, LSB3,** and **LVW2**.

Refer to your product model number on the product label usually found on the bottom or back of your device or also at the top of the page of the device UI.

Note: If you have LoRa capability, you must have it disabled to perform the radio firmware upgrade.

There are two methods for updating the cellular firmware offered: 1) Upgrading using DeviceHQ® and 2) Upgrading using the device UI only.

Upgrading Cellular Firmware Using DeviceHQ (Remote Management)

DeviceHQ can manage the Radio Firmware upgrade to your device when annex-client checks in. **NOTE:** You must first enable and properly configure Remote Management in the device UI (refer to **Managing Your Device Remotely**).

1. Open **DeviceHQ**.
2. Select **Device > Your Device Name > Schedule > Upgrade Radio Firmware**.
3. **DeviceHQ** provides a list of eligible Telit and Quectel module firmware that a particular device can queue for download and install. Select the appropriate firmware.
4. The device checks in, downloads the firmware, automatically verifies the MD5 sum of the firmware to check the integrity of the upgrade file, and applies it to the modem module.
   Note: Allow at least 10 minutes after the device has downloaded the firmware file before taking any action. The system should reboot on its own after a successful download. Otherwise, after 10 minutes, you may reboot the device manually.

5. Once you have refreshed or the device checks in again, verify that the cellular radio firmware has been updated in DeviceHQ.

In the device UI, you can also check that the cellular radio firmware has been updated. Refer to the **Current Radio Firmware** on the **Radio Firmware Upgrade** page (see step 1 of Upgrading Cellular Firmware Using UI only) or also see the firmware version on the **Radio Status** page under **Cellular**.

Upgrading Cellular Firmware using UI only

You can also use the device UI to upgrade your radio firmware. You must first obtain the appropriate binary upgrade file for the cellular radio in your device.

NOTE: If you use the firmware upgrade via Cellular using the UI and you get a timeout failure, first try to boost the signal strength and attempt it again. Otherwise, update via an Ethernet connection or use **DeviceHQ**.

1. Open the **Radio Firmware Upgrade** page under **Cellular**.
2. Enter the MD5 Check Sum or hash under **File MD5**.
3. Place the downloaded binary or delta file on your local computer. Browse for the file and select it.
4. Click **Start Upgrade**. The system should reboot automatically after a successful download. Otherwise, after ten minutes, you may reboot the device manually.
5. Check that the cellular radio firmware has been updated. Refer to the **Current Radio Firmware** on the **Radio Firmware Upgrade** page (see step 1 of Upgrading Cellular Firmware Using UI only) or also see the firmware version on the **Radio Status** page under **Cellular**.

Chapter 9 – SMS

Configuring SMS

This function is not available if you enable SMS through **Cellular > Wake Up On Call**. To enable short message service (SMS) via the Web Management interface or API:

1. From the Web Management interface, go to **SMS > SMS Configuration > SMS Settings**.
2. Check **Enabled**.
3. In the **Sent SMS to Keep** field, enter the total number of sent SMS messages to keep in the device's history.
4. In the **Received SMS to Keep** field, enter the total number of received SMS messages to keep in the device's history.
5. In the **Resend Failed SMS** field, enter the total number of resend attempts for SMS messages that failed to send.
6. Set messages to keep and resend options.
7. Click **Submit.**
8. To save your changes, click **Save and Apply**.

For field descriptions see SMS Field Descriptions.

SMS Field Descriptions

Field	Description
Enabled	Enables the SMS utilities required to send SMS via API and the Web Management interface.
Sent SMS to Keep	The total number of sent SMS messages to keep in the device's history.
Received SMS to Keep	The total number of received SMS messages to keep in the device's history.
Resend Failed SMS	The total number of resend attempts for SMS messages that failed to send.

SMS Commands

SMS commands are disabled by default.

First, make sure to enable SMS under **SMS > SMS Configuration > SMS Settings**.

To enable these available commands (for status and debugging purposes) and set security filters:

1. Go to **SMS > SMS Configuration > SMS Commands**, check the SMS commands you wish to enable. Refer to the table of **SMS Command Descriptions** for details on available commands.
2. Check the security filters, you wish to use (can be one or both):
   - **Password:** If enabled, SMS commands will require **p password** in the syntax. For example: **p 123456 #serial** where 123456 is your password.

     Use the **default password** (last six digits of the radio's IMEI or last six digits of the MEID).

     Or click on **Use custom password** and enter your own password.

     You can also toggle the eye icon to make the password visible or hidden.

- **Whitelist**: If enabled, SMS commands can only be received from a number in the whitelist (you must enter a phone number).

  Enter the phone number and click **Add Number**.

  Note: Due to differences between service providers, for every US number you add to the **Whitelist**, create two separate entries: 1) one using the **phone number** and 2) the other using **1 + phone number**. Tip: Since the number format varies with provider, you can send your device an SMS message from the number in question and see what format is used.

3. Refer to the **Required SMS Command Format** field to see the format based on your chosen settings.
4. Click **Submit**.
5. To save your changes, click **Save and Apply**.

Here is an example SMS Command (#serial – Server mode):

Serial-IP Port Status:

Mode: **Server**

Protocol: SSL/TLS

Port: 3000

TX Bytes: 1234567

RX Bytes: 123456789

DCD Status: ON

2016-11-20 19:22

The response message to all SMS commands includes a time stamp. The time stamp format is **YYYY-MM-DD HH:MM**.

The system adds the time stamp to the existing commands at the end of the SMS message. In case the message exceeds the 160 character limit, the device information and the occurred event are not truncated. Only the time stamp is lost.

SMS Command Descriptions

The following table describes available SMS Commands under **SMS Configuration** > **SMS Commands**. All SMS Commands are disabled by default. Check to enable.

SMS Command	Description
#reboot	reboot the device
#checkin	check in to DeviceHQ
#rm <enable|disable> <AccountKey>	enable or disable remote management using DeviceHQ (You must specify AccountKey when enabling Remote Management if not previously configured.)
#setcellular <enable|disable> [<APN>]	enable or disable Cellular and allows setting of the APN

SMS Command	Description
#ping [<interface>] [<count>] <address>	ping IP address <count> times (range: 1-20, default = 4) through <interface> (choose from cellular, wifi, and ethernet or if not specified, the default gateway interface is used)
#apn	get APN string
#cellular	get cellular connection status
#radio	get radio status
#ethernet	get Ethernet interface configuration
#wan	get actual WAN transport and WAN priority configuration
#serial	get serial details: Mode (Server or Client), RX bytes, TX bytes, DCD Status, Protocol, Port (Server mode only), Server IP Address (Client mode only), and Server Port (Client Mode only)
#wifi	get Wi-Fi details: Date and time in format YYYY-MM-DD HH:MM, mode (WAN or Access Point), MAC address, status (for WAN mode only), SSID, Security settings (for Access Point only, None, WEP, WPA, WPA2-PSK, and WPA/WPA2-PSK)
#geoposition	get GPS coordinates, latitude and longitude (only available on devices with a GPS module acquiring sufficient GPS signal)
#lnsrestart	Upon reception, the device restarts the LoRa network server

Note: Arguments in square brackets [ ] are optional. Those in angle brackets < > are values.

Sending an SMS Message

To send an SMS message from the device:

1. Go to **SMS > Send SMS** to display the **Send SMS** window.
2. In the **Recipient** field, enter a phone number and click **Add**. You can add up to 100 phone numbers.
3. In the **Message** field, enter a text message up to 160 characters long.
4. Click **Send**. The system displays a confirmation indicating whether the message has been successfully sent or not.

Viewing Received SMS Messages

To view received SMS messages from the device:

1. Go to **SMS > Received** to display the **Received SMS** window. The messages are sorted by date with the most recent messages on top. The table shows up to 30 characters for each message.
2. To view the full message, click the **eye** icon to the right of the message entry.

3. To delete an SMS message, click the **trash can** icon under **Options** to the right of the message. A dialog box asks you to confirm that you want to delete the SMS message. Click **OK**.
4. To delete all the received SMS messages, click **Delete All**. A dialog box asks you to confirm that you want to delete all SMS messages. Click **OK**.
5. To configure, the receive list to automatically update, check the **Auto Refresh** box in the upper right corner.

Viewing Sent SMS Messages

To view sent SMS messages from the device:

1. Go to **SMS > Sent** to display the **Sent SMS** window. The messages are sorted by date with the most recent messages on top. The table shows up to 30 characters for each message.
2. To view a full message, click the **eye** icon to the right of the message entry.
3. To delete a sent SMS message, click the **trash can** icon to the right of the message entry. A dialog box asks you to confirm that you want to delete the SMS message. Click **OK**.
4. To delete all the sent SMS messages, click **Delete All**. A dialog box asks you to confirm that you want to delete all the SMS messages. Click **OK**.
5. To configure, the receive list to automatically update, check the **Auto Refresh** box in the upper right corner.

Chapter 10 – Tunnels

Setting Up GRE Tunnels

Tunneling allows the use of a public network to convey data on behalf of two remote private networks. It is also a way to transform data frames to allow them to pass networks with incompatible address spaces or even incompatible protocols. Generic Routing Encapsulation (GRE) is a tunneling mechanism that uses IP as the transport protocol and can be used for carrying many different passenger protocols.

The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint. Configuring a GRE tunnel involves creating a tunnel interface, which is a logical interface, then configuring the tunnel endpoints for the tunnel interface. To set up GRE tunnels:

1. From the Web Management interface, go to **Tunnels > GRE Tunnels**.
2. Click **Add Tunnel**.
3. In the **Tunnel Name** field, enter a name for the new tunnel.
4. (Optional) In the **Description** field, you can enter a description that helps you further identify the tunnel.
5. In the **GRE Tunnel Settings** section:
    a. In the **Remote WAN IP** field, type the IP address of the gateway to which you want to connect.
    b. Click **Add** in the **Remote Network Routes** table.
    c. In the **Remote Network Route** field, type the IP address of the network that is routed through the tunnel.
    d. In the **Remote Network Mask** field, type the mask of the network.
    e. Click **Add**. The defined **Remote Network Route** is added and appears in the **Network Routes** list.
6. In the **Interface IP Address**, specify the IP address of the virtual GRE network interface. It should be equal to the IP address of the LAN interface that is used for establishing the Tunnel connection.
7. In the **Interface Network Mask**, specify the network mask of the virtual GRE network interface.
8. (Optional) In the **Checking period (minutes)** specify the interval to resolve the Remote WAN hostname by DynDNS. Recommended for hostnames that have dynamic IP addresses.
9. Click **Submit**.
10. The defined GRE tunnel configuration is added and appears in the **GRE Tunnels list**.
11. To save your changes, click **Save and Apply**.

IPsec Tunnels

Configuring Network-to-Network Virtual Private Networks (VPNs)

The device supports site-to-site VPNs via IPsec tunnels for secure network-to-network communication. Both tunnel endpoints should have static public IP addresses and must be able to agree on the encryption and authentication methods to use. Setting up an IPsec tunnel is a two-stage negotiation process. The first stage negotiates how the key exchange is protected. The second stage negotiates how the data passing through the tunnel is protected. For endpoints that do not have public static IP addresses, additional options may help such as **NAT Traversal** and **Aggressive Mode**.

By default, based on the encryption method chosen, the device negotiates ISAKMP hash and group policies from a default set of secure algorithms with no known vulnerabilities. This allows flexibility in establishing connections

with remote endpoints. There is an **ADVANCED** mode that provides a way to specify a strict set of algorithms to use per phase, limiting the remote endpoint's negotiation options.

The default Encryption Method is: **AES-128**.

The default set of DH Group Algorithms is: **DH2(1024-bit), DH5(1536-bit), DH14(2048-bit), DH15(3072-bit), DH16(4096-bit), DH17(6144-bit), DH18(8192-bit), DH22(1024-bit), DH23(2048-bit)**, and **DH24(2048-bit)**.

To set up a Network-to-Network VPN tunnel on your device:

1. From the Web Management interface, go to **Tunnels > IPsec Tunnels**.
2. Click **Add Tunnel** in upper right.
3. Enter a **Name** for the tunnel and an optional **Description**.
4. Click **Next**. The **IPsec Remote Tunnel Endpoint** pane opens.
5. Enter a network manually by entering the **Remote Network Route** (LAN IP) and **Remote Network Mask** (Subnet).
6. Choose **Tunnel Type** from the drop-down. Values are **IKE** and **IKEv2**.
7. The public IP address and LAN of this device do not need to be configured because they are already known by this device.
8. Select the **Authentication Method** from the drop-down either **Pre-Shared Key** or **RSA Signatures**. Authentication is performed using secret pre-shared keys and hashing algorithms (like **SHA1 MD5**) or RSA signatures.
9. If you select **Pre-Shared Key**, then enter the **Secret**. This key needs to be the same on both endpoints.
10. If you select **RSA Signatures**, enter the following (in .pem format):
    a. **CA Certificate**
    b. **Local RSA Certificate**
    c. **Local RSA Private Key**
11. Select the **Encryption Method** from the drop-down including **AES-128, AES-192, AES-256** or **ADVANCED**. The encryption method needs to be the same on both endpoints. IKE encryption algorithm is used for the connection (**phase 1 -** ISAKMP SA). Based off of **Phase 1**, a secure set of defaults are used for phase 2, unless the **Advanced** option is used, in which case, you must specify all components of both **phases 1** and **2** including **Encryption, Authentication**, and **Key Group**. When you choose **Advanced** Encryption Method, you select the following (see **IPsec Fields** for field values) :
    a. **Phase 1 Encryption**
    b. **Phase 1 Authentication**
    c. **Phase 1 Key Group**
    d. **Phase 2 Encryption**
    e. **Phase 2 Authentication**
    f. **Phase 2 Key Group**

NOTE: For mPower 5.3 and above, deprecated encryption and hash algorithms are not available for creating new tunnels. But old tunnels that were created in 5.2 or lower will retain the deprecated settings unless changed. Those deprecated settings include: **3DES, ANY, MD5**, and **SHA-1**.

12. If the remote endpoint is set up with unique IDs, check the **Enable UID** box, and enter the **Local** and **Remote IDs**.
13. Click **Show** for **IPSec Tunnel: Advanced** features that limit the remote endpoint's negotiation options.

14. In the **IKE Lifetime** field, enter the duration in which ISAKMP SA lasts (in hours).
15. In the **Max Retries** field, enter the number of retries for the IPSec Tunnel. Enter zero for unlimited retries.
16. In the **Key Life** field, duration in which the IPSec SA lasts (in hours).
17. In the **Checking Period** field, enter the timeout interval (in minutes).
18. Check **Compression** to enable IPComp (compression algorithm).
19. Check **Aggressive Mode** to enable exchange identification in plain text (unencrypted for faster negotiation). NOTE: This mode is less secure and prone to dictionary and brute force attacks.
20. Click **Submit**.
21. To save your changes, click **Save and Apply**.

For field descriptions, see IPsec Tunnel Configuration Field Descriptions.

IPsec Tunnel Configuration Field Descriptions

Field	Description
IPSec Tunnel	
Name	Name used to identify the IPsec tunnel in configurations and logs.
Description	Optional text to describe the IPsec tunnel. This description shows up in the UI while hovering over the summary of an IPsec tunnel.
IPSec Remote Tunnel Endpoint	
Remote WAN IP	External IP address of the remote tunnel endpoint. The remote device is typically a router.
Remote Network Route	This field is used in conjunction with the **Remote Network Mask** field and describes the remote endpoint's subnet. This is used to identify packets that are routed over the tunnel to the remote network.
Remote Network Mask	This field is used in conjunction with the **Remote Network Route** field, to describe the remote endpoint's subnet. It identifies packets that are routed over the tunnel to the remote network.
Tunnel Type	Internet Key Exchange (IKE) for host-to-host, host-to-subnet, or subnet-to-subnet tunnels. Choose from **IKE** or **IKEv2**.
IPsec Tunnel: IKE	
Authentication Method	Choose between **Pre-Shared Key** or **RSA Signatures**. Authentication is performed using secret pre-shared keys and hashing algorithms (like SHA1 MD5) or RSA signatures (you provide the **CA Certificate, Local RSA Certificate**, and **Local RSA Private Key** in .pem format). If you check **Enable UID**, then **Local ID** and **Remote ID** become available as options.
Pre-Shared Key	Authentication is performed using a secret pre-shared key and hashing algorithms on both sides.
Secret	Secret key that is known by both endpoints.
Encryption Method	IKE encryption algorithm used for the connection (phase 1 - ISAKMP SA). Based off of phase 1, a secure set of defaults are used for phase 2, unless the **Advanced** option is used, in which case, all components of both phases 1 and 2 are specified by the user.

Field	Description
RSA Signatures	Authentication is performed using digital RSA signatures.
CA Certificate	Certificate Authority certificate used to verify the remote endpoint's certificate.
Local RSA Certificate	Certificate the local endpoint uses during **Phase 1 Authentication**.
Local RSA Private Key	The private key that the local endpoint uses during Phase 1 Authentication.
Encryption Method*	Choose an Encryption Method from the following list: **AES-128, AES-192, AES-256**, or **ADVANCED.** IKE encryption algorithm is used for the connection (phase 1 - ISAKMP SA). Based off of phase 1, a secure set of defaults are used for phase 2, unless the **Advanced** option is used, in which case, all components of both phases 1 and 2 are specified by the user.
Phase 1 Encryption*	If **Advanced** is selected for **Encryption Method**, select **Phase 1 Encryption** from the drop-down: **AES-128, AES-192, AES-256**, or **ANY AES**.
Phase 1 Authentication*	If **Advanced** is selected for **Encryption Method**, select **Phase 1 Authentication** from the drop-down: **SHA-2, SHA2-256, SHA2-384, SHA2-512,** or **ANY.** .
Phase 1 Key Group*	If **Advanced** is selected for **Encryption Method**, select the **Phase 1 Key Group** from the drop-down: **DH2 (1024-bit), DH5 (1536-bit), D14 (2048-bit), DH15 (3072-bit), DH16 (4096-bit), DH17 (6144-bit), DH18 (8192-bit), DH22 (1024-bit), DH23 (2048-bit), DH24 (2048-bit),** and **ANY**.
Phase 2 Encryption*	If **Advanced** is selected for **Encryption Method**, select **Phase 2 Encryption** from the drop-drown: **AES-128, AES-192, AES-256, ANY AES,** or **ANY**.
Phase 2 Authentication*	If **Advanced** is selected for **Encryption Method**, select **Phase 2 Authentication** from the drop-drown: **SHA-2, SHA2-256, SHA2-384, SHA2-512,** or **ANY**.
Phase 2 Key Group*	If **Advanced** is selected for **Encryption Method**, select the **Phase 2 Key Group** from the drop-down: **DH2 (1024-bit), DH5 (1536-bit), D14 (2048-bit), DH15 (3072-bit), DH16 (4096-bit), DH17 (6144-bit), DH18 (8192-bit), DH22 (1024-bit), DH23 (2048-bit), DH24 (2048-bit),** and **ANY**.
Enable UID	Unique Identifier String to enable the **Local ID** and **Remote ID** fields.
Local ID	String Identifier for the local security gateway (optional)
Remote ID	String Identifier for the remote security gateway (optional)
IPSec Tunnel: Advanced	

Field	Description
IKE Lifetime	Duration for which the ISAKMP SA exists from successful negotiation to expiration.
Key Life	Duration for which the IPsec SA exists from successful negotiation to expiration.
Max Retries	Number of retry attempts for establishing the IPsec tunnel. Enter zero for unlimited retries.
Checking Period	Timeout interval in minutes. If Remote WAN IP address is a hostname that can be resolved by DynDNS, the hostname will be resolved at the set interval. Recommended for dynamic IP addresses.
Compression	Enable IPComp. This protocol increases the overall communication performance by compressing the datagrams. Compression requires greater CPU processing.
Aggressive Mode	Whether to allow a less secure mode that exchanges identification in plain text. This may be used for establishing tunnels where one or more endpoints have a dynamic public IP address. Although this mode is faster to negotiate phase 1, the authentication hash is transmitted unencrypted. You can capture the hash and start a dictionary or use brute force attacks to recover the PSK.

*__NOTE__: For mPower 5.3 and above, deprecated encryption and hash algorithms are not available for creating new tunnels. But old tunnels that were created in 5.2 or lower will retain the deprecated settings unless changed. Those deprecated settings include: **3DES, ANY, MD5,** and **SHA-1**.

OpenVPN Tunnels

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. You can use and setup OpenVPN tunnels with this device.

To use OpenVPN, you must first install an OpenVPN application along with an easy-rsa tool and configure OpenVPN on your computer. Then you must also generate the certificates for the OpenVPN server and client before configuring the device.

To configure OpenVPN client and server on this device the following files are required:

- **The CA PEM file or CA certificate (.crt)**
- **The Diffie Hellman PEM file (.pem)**
- **The Server Certificate to be used by the device endpoint (.crt)**
- **The Server/Client Key to be used by the device endpoint (.key)**

Note 1: When you configure OpenVPN server and client make sure both sides use the same settings, and certificates.

Note 2: For mPower 5.3 and above, some encryption and hash configurations are deprecated and not available for creating new tunnels. But old tunnels that were created in 5.2 or lower will retain the deprecated settings unless changed. Deprecated settings for hash algorithms include: **MD4, MD5, RSA-MD4, RSA-MD5, and SHA-1.**

Deprecated settings for encryptions ciphers include: **BF-CBC, CAST5-CBC, DES-CBC, DES-EDE-CBC, DES-EDE3-CBC, DESX-CBC, IDEA-CBC, RC2-40-CBC, RC2-64-CBC,** and **RC2-CBC**. Deprecated setting for Minimum TLS version is **1.1.**

Note 3: Some encryption and hash configurations are too weak and NOT supported at all in mPower 5.3 or higher. These settings do not function when performing an upgrade to mPower 5.3. The system provides a warning message during upgrade and replaces them with **Default**. The following TLS cipher suites are not supported: **TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA** and **TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.** Also, the following hash algorithms are not supported: **DSA, DSA-SHA, DSA-SHA1, DSA-SHA1-old, ECDSA-with-SHA1, RSA-SHA, RSA-SHA1-2,** and **SHA**.

Configuration 1: OpenVPN Tunnel with TLS Authorization Mode (Device only)

This first configuration establishes the OpenVPN Tunnel connection from a device client to a device server using TLS as Authorization Mode. This involves adding and configuring both OpenVPN Server and Client sides within the device UI.

To add an **OpenVPN Server using TLS**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **SERVER** from the drop-down.
5. You can also enter an optional **Description**.
6. Under OpenVPN Tunnel Configuration, enter the following fields (using **TLS** as **Authorization Mode**):
    a. **Interface Type** as **TUN** from the drop-down.
    b. **Authorization Mode** as **TLS** from the drop-down.
    c. **Protocol** as **UDP**.
    d. **VPN Subnet**.
    e. **Port** number.
    f. **VPN Netmask**.
    g. **LZO Compression** as **ADAPTIVE** from the drop-down.
    h. **Hash Algorithm** as **DEFAULT**.
    i. **NCP (Negotiable Crypto Parameters)** as **DEFAULT**.
    j. **Min. TLS Version** as **1.2**.
    k. **TLS Cipher Suite** as **DEFAULT**.
    l. Enter the contents of the following files generated from the easy-rsa tool. You can copy and paste this content from the certificate files after opening from a text editor like Notepad. (all required):
        i. **CA PEM (.crt)**
        ii. **Diffie Hellman PEM (.pem)**
        iii. **Server Certificate PEM (.crt)**
        iv. **Server Key PEM (.key)**

        Note: Use the same **CA PEM** certificate and parameters as the server for the OpenVPN clients .
7. **Remote Network Routes** create a route from the server network to the client network. This allows the server to get access to the client's network. In the **OpenVPN Tunnel Network Routes**, click **Add**:

a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
b. Enter the **Remote Network Mask** (usually 255.255.255.0).
c. You may enter **Gateway** (optional).
d. Click **Add**.

8. The system displays your recently-added **Push Route** with the client subnet (remote network route + mask).
9. **Push Routes** create a route from client's network to the server's network. This allows clients to get access to the server's network. Under **Push Routes**:

a. Click **Client To Client** box if you want this optional feature (this establishes a connection between multiple clients that are connected to the server).
b. In the **Push Network Route**, click **Add**.
c. In the dialog box, enter the **Remote Network Route** (same address as the server subnet above).
d. Enter the **Remote Network Mask** (same as above).
e. You may enter **Gateway** (optional).
f. Click **Add**.

Note: If you use **Static Key Authorization Mode**, the **Push Routes** do not work.

10. The system displays your recently-added **Push Route** with the client subnet (remote network route + mask).
11. Click **Preview** to view the tunnel configuration.
12. Click **Submit**.
13. Click **Save and Apply** to save your changes

To add an **OpenVPN Client using TLS**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name** of the tunnel.
4. Select the **Type** as **CLIENT** from the drop-down.
5. You can also enter an optional **Description**.
6. Under OpenVPN Tunnel Configuration, enter the following fields (using **TLS** as **Authorization Mode**):

a. **Interface Type** as **TUN** from the drop-down.
b. **Authorization Mode** as **TLS** from the drop-down.
c. **Protocol** as **UDP**.
d. **Remote Host** (server public IP address).
e. **Remote Port** number.
f. **LZO Compression** as **ADAPTIVE** from the drop-down.
g. **Hash Algorithm** as **DEFAULT**.
h. **NCP (Negotiable Crypto Parameters)** as **DEFAULT.**
i. **Min. TLS Version** as **1.2.**
j. **TLS Cipher Suite** as **DEFAULT**.

k. Enter the contents of the following files generated from the easy-rsa tool. You can copy and paste this content from the certificate files after opening from a text editor like Notepad. (all required):

   i. **CA PEM (.crt)**
   ii. **Client Certificate PEM (.crt)**
   iii. **Client Key PEM (.key)**

7. If you use **TLS** as **Authorization Mode**, you do not need configure or add **Remote Network Routes**. The server adds the routes if the server's **Push Routes** are already configured. If you use **Static Key** as **Authorization Mode**, you must add and configure **Remote Network Routes**.
8. Click **Preview** to view the tunnel configuration.
9. Click **Submit**.
10. Click **Save and Apply** to save your changes.

Now the device client can access the device server subnet. You can ping the IP address of the device server subnet from the client console to test this.

Note: The PC connected to the device does not have access to the device server subnet.

Configuration 2: OpenVPN Tunnel with TLS Authorization Mode (Device and Connected PC)

This second configuration provides access between a device server and its subnet and device client and its subnet. An additional configuration is needed on the device server side. This also allows your PC to connect with the device server and ultimately to the device client through that server.

1. Configure the device server as shown under how to add an **OpenVPN Server using TLS**.
2. Open device console, go to **/var/config/ovpnccd/openVPNServerName**. Create the folder if not present in the device.
3. Create a file that has the client certificate name with the following information:

   a. **iroute [Client_Subnet] [Mask*/***
   b. **example** -- echo “iroute 192.168.3.0 255.255.255.0” > mtrClient1

4. For each client, you must create a separate file in the folder **/var/config/ovpnccd/yourserverName**.

   Note: Make the file name the same as the Common Name value used to create the certificate.
5. Configure device client as shown under how to add an **OpenVPN Client**.

Once properly configured, you should have a connection between the device server and device client and their subnets. Your PC can also connect with the device server and thus the device client through that server.

Configuration 3: OpenVPN Tunnel with Static Key Authorization Mode (device server and client)

This third configuration establishes the OpenVPN Tunnel connection from a device client to a device server using Static Key as Authorization Mode. This involves adding and configuring both OpenVPN Server and Client sides within the device UI.

When using Static Key, the OpenVPN tunnel is created between only two end-points, the client and server. You cannot connect more than one client to the server in this mode. Remote Network Route must be specified in both configurations, client and server, in order to establish the connection between subnets.

To add an **OpenVPN Server using Static Key**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.

2. Click **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **SERVER** from the drop-down.
5. You can also enter an optional **Description**.
6. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
    a. **Interface Type** as **TUN** from the drop-down.
    b. **Authorization Mode** as **STATIC KEY** from the drop-down.
    c. **Protocol** as **UDP**.
    d. **Local Address** as **DEFAULT**.
    e. **Port** number.
    f. **Remote Address** as **DEFAULT**.
    g. **LZO Compression** as **ADAPTIVE** from the drop-down.
    h. **Hash Algorithm** as **DEFAULT**.
    i. **NCP (Negotiable Crypto Parameters)** as **DEFAULT**.
    j. Generate and enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

    -----BEGIN OpenVPN Static key V1-----

    3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875215e20e80a2d59efd
    79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f55e7d8917a32bfe07d61591b7bbb43c7ba
    d214482b8547ec9dca8910f514d9f4270ccaeff1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104
    e1968ed29b6c3388719226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07
    08781fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c75312375b4bd098
    76e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd00305c7cb30beef66ad33f43dac
    c2e662128

    -----END OpenVPN Static key V1-----

7. **Remote Network Routes** create a route from the server network to the client network. This allows the server to get access to the client's network. In the **OpenVPN Tunnel Network Routes**, click **Add**:
    a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
    b. Enter the **Remote Network Mask** (usually 255.255.255.0).
    c. Click **Add**.
8. The system displays your recently-added **Remote Network Route** with the client subnet (remote network route + mask).

    Note: **Push Routes are not required with Static Key as Authorization Mode.**
9. Click **Preview** to view the tunnel configuration.
10. Click **Submit**.
11. Click **Save and Apply** to save your changes.

To add an **OpenVPN Client using Static Key**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name**.

4. Select the **Type** as **CLIENT** from the drop-down.
5. You can also enter an optional **Description**.
6. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
   a. **Interface Type** as **TUN** from the drop-down.
   b. **Authorization Mode** as **STATIC KEY** from the drop-down.
   c. **Protocol** as **UDP**.
   d. **Local Address** as **DEFAULT**.
   e. **Remote Host**.
   f. **Remote Address** as **DEFAULT**.
   g. **Remote Port** number.
   h. **LZO Compression** as **ADAPTIVE** from the drop-down.
   i. Select the **NCP (Negotiable Crypto Parameters)** as **DEFAULT** from drop-down.
   j. Select the **Hash Algorithm** as **DEFAULT** from drop-down.
   k. **Min. TLS Version** as **1.2.**
   l. **TLS Cipher Suite** as **DEFAULT**.
   m. Enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

      -----BEGIN OpenVPN Static key V1-----

      3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875215e20e80a2d59efd
      79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f55e7d8917a32bfe07d61591b7bbb43c7ba
      d214482b8547ec9dca8910f514d9f4270ccaeff1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104
      e1968ed29b6c3388719226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07
      08781fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c75312375b4bd098
      76e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd00305c7cb30beef66ad33f43dac
      c2e662128

      -----END OpenVPN Static key V1-----.

7. **Remote Network Routes** create a route from the server network to the client network. This allows the server to get access to the client's network. In the **OpenVPN Tunnel Network Routes**, click **Add**:
   a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
   b. Enter the **Remote Network Mask** (usually 255.255.255.0).
   c. Click **Add**.
8. The system displays your recently-added **Remote Network Route** with the client subnet (remote network route + mask).

   Note: **Push Routes** are not required with **Static Key** as **Authorization Mode.**
9. Click **Preview** to view the tunnel configuration.
10. Click **Submit**.
11. Click **Save and Apply** to save your changes.

Configuration 4: OpenVPN Tunnel with Static Key Authorization Mode and TCP

This fourth configuration establishes the OpenVPN Tunnel connection from a device client to a device server using Static Key as Authorization Mode and TCP protocol (instead of UDP for the third configuration). This involves adding and configuring both OpenVPN Server and Client sides within the device UI.

To add an **OpenVPN Server using Static Key and TCP**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **SERVER** from the drop-down.
5. You can also enter an optional **Description**.
6. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
    a. **Interface Type** as **TUN** from the drop-down.
    b. **Authorization Mode** as **STATIC KEY** from the drop-down.
    c. **Protocol** as **TCP**.
    d. **Local Address** as **DEFAULT**.
    e. **Remote Host**.
    f. **Remote Address** as **DEFAULT**.
    g. **Remote Port** number.
    h. **Hash Algorithm** as **RSA-SHA1**.
    i. **LZO Compression** as **ADAPTIVE** from the drop-down.
    j. **NCP (Negotiable Crypto Parameters)** as **CAMELLIA-256-CBC**.
    k. **Min. TLS Version** as **NONE.**
    l. **TLS Cipher Suite** as **DEFAULT**.
    m. Generate and enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

        -----BEGIN OpenVPN Static key V1-----

        3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875215e20e80a2d59efd
        79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f55e7d8917a32bfe07d61591b7bbb43c7ba
        d214482b8547ec9dca8910f514d9f4270ccaeff1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104
        e1968ed29b6c3388719226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07
        08781fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c75312375b4bd098
        76e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd00305c7cb30beef66ad33f43dac
        c2e662128

        -----END OpenVPN Static key V1-----

7. Click **Next**.
8. **Remote Network Routes** create a route from the server network to the client network. This allows the server to get access to the client's network. In the **OpenVPN Tunnel Network Routes**, click **Add**:
    a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
    b. Enter the **Remote Network Mask** (usually 255.255.255.0).
    c. Click **Add**.

9. The system displays your recently-added **Remote Network Route** with the client subnet (remote network route + mask).

   Note: **Push Routes are not required with Static Key as Authorization Mode.**
10. Click **Preview** to view the tunnel configuration.
11. Click **Submit**.
12. Click **Save and Apply** to save your changes.

To add an **OpenVPN Client using Static Key and TCP**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **CLIENT** from the drop-down.
5. You can also enter an optional **Description**.
6. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):

   a. **Interface Type** as **TUN** from the drop-down.
   b. **Authorization Mode** as **STATIC KEY** from the drop-down.
   c. **Protocol** as **TCP**.
   d. **Local Address** as **DEFAULT**.
   e. **Remote Host**.
   f. **Remote Address** as **DEFAULT**.
   g. **Remote Port** number.
   h. **Hash Algorithm** as **RSA-SHA1**.
   i. **LZO Compression** as **ADAPTIVE** from the drop-down.
   j. **NCP (Negotiable Crypto Parameters)** as **CAMELLIA-256-CBC**.
   k. **Min. TLS Version** as **NONE.**
   l. **TLS Cipher Suite** as **DEFAULT**.
   m. Generate and enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

      -----BEGIN OpenVPN Static key V1-----

      3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875215e20e80a2d59efd
      79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f55e7d8917a32bfe07d61591b7bbb43c7ba
      d214482b8547ec9dca8910f514d9f4270ccaeff1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104
      e1968ed29b6c3388719226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07
      08781fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c75312375b4bd098
      76e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd00305c7cb30beef66ad33f43dac
      c2e662128

      -----END OpenVPN Static key V1-----
7. Click **Next**.
8. **Remote Network Routes** create a route from the server network to the client network. This allows the server to get access to the client's network. In the **OpenVPN Tunnel Network Routes**, click **Add**:

   a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.

b. Enter the **Remote Network Mask** (usually 255.255.255.0).

c. Click **Add**.

9. The system displays your recently-added **Remote Network Route** with the client subnet (remote network route + mask).

   Note: **Push Routes are not required with Static Key as Authorization Mode.**

10. Click **Preview** to view the tunnel configuration.
11. Click **Submit**.
12. Click **Save and Apply** to save your changes.

Chapter 11 – Administration

User Accounts

Use this feature to add user accounts or change the password.

The system offers three roles or user types: administrator, engineer, and monitor. Administrators have full rights and permissions including change settings on the device. Engineers have read/write privileges and some access to controls on the device. Monitors have read-only access. Note: the system automatically checks for a strong password and tells you how to improve it.

Username requirements include:

- Must be unique.
- Is case-sensitive (for example, admin and ADMIN are treated as two different usernames).
- Acceptable characters: uppercase alphabetic, lowercase alphabetic, numeric, and non-alphanumeric (symbols like #).
- A hyphen (-) should not be used as the first character.

Password requirements include:

- User account is disabled if password is not set up.
- Must be at least eight characters in length.
- Contains three or more different types of characters such as: uppercase alphabetic, lowercase alphabetic, numeric, and non-alphanumeric (symbols like #).

Administrator details:

- Able to delete any local users. (Engineer and Monitor cannot delete any users.)
- Able to modify any other user details, except username.
- Can not modify another administrator user account if it is the only enabled local administrator user on the device.
- Able to modify own account details except Role, Username, and Enabled values.
- Able to disable and enable any local users except their own account. Also, not able to disable local user account if this is only local administrator.
- Able to change own password and other user passwords.

Engineer and Monitor details:

- Able to view and modify own user account details except Role, Username, and Enabled values.
- Access to only their own user account.
- Not able to delete users.
- Able to change own password.

To add new users:

1. Go to **Administration** > **User Accounts**.
2. Click **Add New User**.
3. Under **User Details**, enter the following fields:

a. Username (required)
b. Role (required). Select the user role from the drop-down menu including **administrator**, **engineer**, or **monitor**.
c. First Name
d. Last Name
e. Title
f. Division
g. Employee Identification

4. Under **Contact Information**, enter the following fields:

a. Email
b. Address
c. City
d. State
e. Country
f. Postal Code
g. Work Phone
h. Mobile Phone

5. Click **Submit**.
6. The **Change Password** page opens. Enter **New Password**. Click **Submit**.
7. The **Change Password** page opens. Enter **New Password**. Click **Submit**.

If the password is not set up for the new user, the user is disabled until the password is set.

Password Complexity

Password Complexity Rules allow an administrative user to choose rules and limitations on user passwords. You can determine various password parameters such as the minimum length of passwords, upper and lower case requirements, and characters not permitted.

Before choosing your options, you must first select between two different complexity modes: **Default** or **Credit**.

Default mode uses a minimum character length and may require a specific number of characters from each class. But requiring specific classes of characters actually makes brute force attacks easier because it reduces the search space.

For this reason, we recommend using **Credit** mode. This mode grants one credit per password character plus one extra credit for certain character classes up to their respective extra credit cap. You can still specify a minimum number of classes, but the strongest passwords come from their length.

In either mode, you should use longer passwords for increased security.

1. Go to **Administration > User Accounts**.
2. Click **Change Password Complexity Rules** button.
3. Under the **Change Password Complexity Rules** window, select from the drop-down between **Default** or **Credit** mode.
4. For **Default** mode**,** you may enter the following:

a. **Minimum Password Length** (default = 8)
b. **Minimum Upper Case Characters** (default = 0)
c. **Minimum Lower Case Characters** (default = 0)
d. **Minimum Numeric Characters** (default = 0)
e. **Minimum Special Characters** (default = 0)
f. **Maximum Password Length** (default = 64)*
g. **Characters Not Permitted** (enter restricted characters in any order with no separators)

5. For **Credit** mode**,** you may enter the following:

a. **Minimum Password Credits** (default = 8)
b. **Minimum Character Classes** (default = 3)
c. **Upper Case Extra Credit Cap** (default = 0)
d. **Lower Case Extra Credit Cap** (default = 0)
e. **Numeral Extra Credit Cap** (default = 0)
f. **Special Extra Credit Cap** (default = 0)
g. **Maximum Password Length** in number of characters (default = 64)*
h. **Characters Not Permitted** (enter restricted characters in any order with no separators)

* **Note:** Entering a value of 0 indicates no maximum.

Self-Diagnostics

The device offers self-diagnostics or periodic monitoring of certain issues such as memory errors or leaks, and security violations by applications. The following self-diagnostic features are available with this device (varies with model) :

- Security Violation
- Resource Overuse

This monitoring is intended detect corruption, or help prevent malicious activity. After an event is detected, the system disables the cellular radio module, sends an alarm or notification, logs the event, and sends a record of it via SMS, Email, or to the SNMP server. To receive notifications for specific diagnostic features, configure them under **Administration > Notifications**.

For the self-diagnostic features, go to **Administration > Self-Diagnostics** and refer to the following sections.

To turn on the **Resource Overuse** diagnostic that detects memory leaks or errors:

1. Check **Enabled** under **Resource Overuse**.
2. If you want the system to reboot the device after a **Resource Overuse** is detected, check **Reboot the device** under **Actions.**

To turn on the **Security Violation** diagnostic that detects security rule violations by applications:

1. Check **Enabled** under **Security Violation**.
2. If you want the system to disable WAN interfaces after a **Security Violation** is detected, check **Disable WAN Interfaces** under **Actions**.
3. If you want the system to disable user-defined firewall rules after a **Security Violation** is detected, check **Disable User-Defined Firewall Rules** under **Actions**.

After you completed your **Self-Diagnostic** configuration (selecting any or all of the above):

1. Click **Submit**.
2. To save changes, click **Save and Apply**.

If at any time you want to return the device to the default setting, click the **Reset to Default** button in the bottom right corner. (This disables or removes all enabled **Self-Diagnostic** features.)

Configuring Device Access

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

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

HTTP Redirect to HTTPS

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

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

HTTPS

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

Field	Description
Port	The port on which the device will listen for HTTPS requests.
Via WAN/Cellular	If checked, the device will listen and respond to HTTPS requests from the WAN. This increases susceptibility to malicious activity.
Session Timeout (under **Authorization)**	Amount of time a user's session can remain dormant before automatically being logged out (minutes). Note: Changing this item requires the device to reboot.

HTTPS Security

Configure the HTTPS security settings (like version and cipher suite). Click the **Show** link to the right under **HTTPS Security**. To enable the Web server to authenticate the client via the client's public key certificate, check **Client Authentication** under the **Authentication** section.

Note: Enabling **Client Authentication** can prevent users from accessing the Web UI. When **Client Authentication** is enabled it is required that a web browser has a valid client certificate that is signed by a CA that the server can verify. The CA certificate needs to be uploaded to the device using the upload feature at **Administration > X.509 CA Certificates**. Configure TLS version and cipher suites under the **TLS Settings** section.

NOTE: For mPower 5.3 and above, deprecated encryption and ciphers are not available for creating new tunnels. But old tunnels that were created in 5.2 or lower will retain the deprecated settings unless changed.

Field	Description
Authentication	
Client Authentication	Requires web browsers to have a valid client certificate that is signed by a Certifying Authority (CA) that the server can verify. Otherwise, user access to the UI is blocked. **NOTE:** You must first upload a CA certificate at **Administration > X.509 CA Certificates.**
TLS Settings	
TLSv1.3, TLSv1.2, and/or TLSv1.1	Check any version of the TLS protocol you want to use: **TLSv1.3, TLSv1.2, and/or TLSv1.1 (Deprecated)**. Default: **TLSv1.3 and TLSv1.2**
Cipher Suite Name	Check any preferred **Cipher Suite** from the following: **TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-GCM-SHA256,TLS_AES_128_GCM_SHA256**, and also including the following deprecated ciphers: **ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA**, and/or **AES128-SHA**. Default: **All.** (You can also set the priority order of the ciphers).

SSH

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

Field	Description
Enabled	Enables SSH redirect which automatically redirects users trying to access the device via SSH (disabled by default).
Port	The port on which the device listens for SSH requests.

Field	Description
Via LAN/Ethernet	If checked, the device listens and responds to SSH requests from the LAN.
Via WAN/Cellular	If checked, the device listens and respond to SSH requests from the WAN.

Reverse SSH Tunnel

Enable and configure a reverse SSH tunnel.

Field	Description
Enabled	Enable **Reverse SSH tunnel** to get SSH access to the device with a public IP address.
Server	Remote SSH server IP address or hostname to which the reverse SSH tunnel connection is established.
Remote Port	Tunnel remote port that opens on the remote end of the reverse SSH tunnel connection (2222 by default).
Username	Remote SSH server username.
Authentication Method	Defines Authentication method to use for **Reverse SSH Tunnel**. Select from drop-down including **Password**, **Public Key**, or **Private Key**.
Password	User's password on the remote SSH server (when you select **Password** for Authentication Method).
Public Key	The public key that the Remote SSH server uses to authorize your device and establish the tunnel connection (when you select **Public Key** for Authentication Method).
Private Key	The private key provided by the remote SSH server (when you select **Private Key** for Authentication Method).

SSH Security

Configure the **SSH security settings** (like ciphers and HMAC). Click **Show** to the right under **Security Settings**. Must select **SSL/TLS** under **Protocol**.

NOTE: For mPower 5.3 and above, deprecated hash algorithms are not available for creating new tunnels. But old tunnels that were created in 5.2 or lower will retain the deprecated settings unless changed.

Field	Description
Ciphers	Check any Cipher you want to use: CHACHA20-POLY1305@OPENSSH.COM (no HMAC required), AES128-CTR, and/or AES256-CTR.
HMAC	Check any hash-based message authentication code, you want to use: SHA1 (deprecated), SHA2-256, and/or SHA2-512.

ICMP

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

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

Node-RED

The device can be configured to accept connections to the Node-RED browser editor to either/both LAN and/or WAN.

Field	Description
Via LAN	If checked, the device allows connection to Node-RED from the LAN.
Via WAN	If checked, the device allows connection to Node-RED from the WAN. This may increase susceptibility to malicious activity.

NOTE: Support for Node-RED/Node.js on Multitech AT91SAM9G25-based products has been discontinued.

SNMP

The device offers Simple Network Management Protocol (SNMP) which is used for collecting information from, and configuring network devices on an IP network. For more details, refer to **Configuring SNMP**.

Field	Description
Via LAN	If checked, the device allows access to the SNMP server via LAN.
Via WAN	If checked, the device allows access to the SNMP server via WAN.

Modbus Slave

The Modbus feature allows the user to enable the Modbus query server. You can query this server over Modbus-TCP for status information.

Field	Description
Enabled (under **Modbus Slave**)	Enables the Modbus Query Server.
Via LAN	If checked, the device can query the Modbus server via LAN.
Port	Port number configured for Modbus.

NOTE: Modbus Slave is not available on devices with Quectel cellular radios (-L4G1, -LEU7, -LNA7).

For Modbus query information, refer to the MTR Modbus Information page on our Developer Resources website (on .net) for details: http://www.multitech.net/developer/software/mtr-software/mtr-modbus-information/

IP Defense

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

Go to **Administration > Access Configuration > IP Defense** to find these features.

DoS Prevention

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

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

Ping Limit

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

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

Brute Force Protection

This feature tracks login attempts at the RESTFUL API level. Its purpose is to prevent Dictionary attacks that attempt to brute force the user's password. The device reboots after applying changes in this section.

Field	Description
Enabled	Enables the Brute Force Prevention feature (enabled by default).

Field	Description
Attempts	The number of failed attempts allowed before the user's account is locked out.
Lockout Minutes	The number of minutes an account is locked out before a new login attempt will be accepted.

Bootloader Protection

To see or set these features, go to **Administration > Access Configuration > Bootloader Protection** and click **Show.**

Bootloader Password

This feature enables password authentication to access the device bootloader. It is disabled by default.

Field	Description
Enable	Enables the Bootloader Password feature to the right of Authentication Status (enabled by default).
Password	Enter password to access the device bootloader.
Confirm	Enter the password again to confirm.

Debug Console

This feature allows the customer to run **Silent Mode** which turns off the output to the **Debug Console**. The console output is enabled by default (i.e. **Silent Mode** is disabled).

When **Silent Mode** is enabled, **Debug Console** is turned off. (**NOTE:** During boot, the device does not output any information after the notice that the Linux Kernel is being decompressed including no login prompt, etc.)

Field	Description
Enable	Enables Silent Mode which turns off output to the Debug Console (disabled by default meaning Debug Console output is on).

After making all your desired changes, click **Submit**, then click **Save and Apply**. (Changes to specific sections may require reboot.)

RADIUS Configuration

The RADIUS protocol supports authentication, user session accounting, and authorization of users to the device. This authentication, accounting, and authorization is independent of the local users created on the device. The user can enable Authentication, Accounting, or both options.

RADIUS user details:

- Access to device if role is one of those in the provided list (Administrator, Engineer, or Monitor).
- All RADIUS users do not have SSH access to the device.
- RADIUS creates a temporary session instead of a local account like local users.
- RADIUS uses shared key encryption.

- Local users shall take priority over RADIUS user (if a RADIUS user has the same username as a local user, the RADIUS user cannot log in even if the local user is disabled).
- RADIUS user with Administrator role can view and modify all local users (but cannot delete a local Administrator if it is the only local admin user on the device).
- RADIUS users with Engineer and Monitor role cannot view or modify user details. They do not have access to the **User Accounts** page.
- RADIUS users cannot change their own password in the Web UI.

To set up the RADIUS server configuration:

1. Go to **Administration** > **RADIUS Configuration**.
2. To enable authentication, check **Enable Authentication**.
3. To enable accounting, check **Enable Accounting**.
4. Enter the following fields for **RADIUS configuration**:
   a. Primary Server
   b. Authentication Port (for Primary Server)
   c. Accounting Port (for Primary Server)
   d. Secondary Server
   e. Authentication Port (for Secondary Server)
   f. Accounting Port (for Secondary Server)
5. Under **Options**, enter the following fields:
   a. **Shared Secret Key** value is used to: 1) encrypt packets between the RADIUS Server and device, 2) encrypt RADIUS attributes such as user password, and 3) verify that RADIUS messages have not been modified in transit. This value must be equal to the shared secret that is set up in RADIUS server. The Shared Secret Key can be up to 128 characters long. You can click the eye icon to hide the key.
   b. Authentication Protocol: select from drop-down list including **PAP**, **EAP-PEAPv0/MSCHAPv2**, or **EAP-TTLS/PAPv0**
   c. Timeout is the interval in seconds between tries to connect to RADIUS server in case of communication failure. Maximum is 10 seconds.
   d. Retries is the number of tries to connect to RADIUS server in case of communication failure.
6. Advanced Options are used when Authentication Protocol is EAP-PEAPv0/MSCHAPv2 or EAP-TTLS/PAPv0. If Protocol is PAP, these settings are ignored:
   a. Check **Use Anonymous ID** if you want to enable identity privacy. The device does not send its identity in plain text before the device has authenticated the RADIUS server.
   b. Anonymous ID is a name or value that the device will use in the identity response when “Use Anonymous ID” is enabled.
   c. Check **Check Server Certificate Hostname** to allow the server certificate CN (common name) to be validated by the device.
7. Click **Submit**.
8. To save your changes, click **Save and Apply**.

Generating a New Certificate

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

To generate a new certificate:

1. Go to **Administration > X.509 Certificate**. The **X.509 Certificate** window displays the details of the certificate that is currently used.
2. Click **Generate** to open the **Generate Certificate** window.
3. In the **Common Name** field, enter the name, hostname, or IP address, depending on what you use to connect to the device. The web browser uses this field to check for a valid certificate.
4. In the **Days** field, enter the amount of days before the certificate will expire.
5. In the **Country** field, enter the 2-letter code for the country name.
6. In the **State/Province** field, enter the state or province for which the certificate is valid.
7. In the **Locality/City** field, enter the locality or the city for which the certificate is valid.
8. In the **Organization** field, enter the organization name for which the certificate is valid.
9. In the **Email Address** field, enter the email address of the person responsible for the device. Typically this is the administrator. This field may be left blank.
10. Click **Generate**. Wait until the certificate is generated. You may have to reboot to complete the operation.
11. If you are finished making changes, click **Save and Apply**. The device reboots after applying those changes.

Importing a Certificate

To import a certificate (in **.pem** format):

1. Go to **Administration > X.509 Certificate**. The Certificate window displays the details of the certificate that is currently used.

NOTE: A certificate with a key size greater than 2048 bits causes a delay accessing the Web UI after the device starts. A certificate with a key size less than 2048 bits is not recommended since it is less secure and may become breakable in the near future.

2. Click **Import** to open **Upload Certificate** window.
3. Click **Browse** to select a valid certificate to be uploaded. Check that your certificate file format is **.pem**.
4. Click **Upload**. Wait until the file is uploaded.
5. To save your changes, click **Save and Apply**. The device reboots after applying those changes.

NOTE: Your certificate file must be in **.pem** format.

Uploading CA Certificate

This page allows a user to upload an X.509 CA (Certifying Authority) Certificate. This is also where you upload root CA certificates for the on-premises Device HQ server to the device.

To upload a CA certificate:

1. Go to **Administration > X.509 CA Certificates**.
2. Click **Choose File** and browse for your CA certificate file.

3. Click **Open**.
4. Once your file is selected, click **Import**.
5. Click **Save and Apply** to save your changes. The device reboots.
6. Your CA certificate file displays in the certificate list along with relevant details.
7. You may delete or remove a certificate by clicking the trash can icon to the right under **Options**.

Note: Both add and remove functions may take up to two minutes to update. Once updated, the changes are applied immediately. There is no need to restart the device after CA certificate is added or removed. For bi-directional certificate authentication or client authentication, go to **Device Administration > Access Configuration > HTTPS Security > Authentication** and check **Client Authentication.** See **HTTPS Security** on the**Access Configuration** page for more details**.**

Setting up the Remote Management

To modify DeviceHQ automatic update settings, go to options under **Auto-Update Settings** and refer to Managing Your Device Remotely.

1. Go to **Administration > Remote Management > Remote Server**. To allow the device to connect to the Remote Management Server, check **Enabled**.
2. If you want the device to use a secure connection, check **SSL Enabled**.
3. The **Server Name** field is pre-populated with the address of the Remote Management Server.
4. The **Server Port** field is pre-populated with the port the Remote Management Server listens on. You likely do not need to change this.
5. In the **Account Key** field, type the account key received from the Remote Management administrator. The device is not allowed to connect to the Remote Management Server without a valid account key.
6. For MTCAP only, in the **Device API Secret** field, enter the API Secret for the device from your Device HQ account to send backup battery data so that DeviceHQ can display it.
7. For MTCAP only, in the **Device API Authentication Token** field, enter the API Authentication Token for the device from your Device HQ account to send backup battery data so that DeviceHQ can display it.
8. Click **Submit**.
9. To save your changes, click **Save and Apply**.

Managing Your Device Remotely

DeviceHQ® can monitor devices, reboot devices, and perform remote software and configuration updates.

NOTE: Reboot the device before performing any firmware updates.

To configure your device to use DeviceHQ:

1. Go to **Administration > Remote Management** and check **Enabled**.
2. Go to options under **DeviceHQ Check-In Settings**.
3. Enable the **Intervals** check box to check in to DeviceHQ periodically at the specified interval.**If you do not select **Intervals**, certain DeviceHQ features will NOT be available**.** See note at the end for this topic for details.*

    a. To define how often the device connects to DeviceHQ to check in and request any pending updates, set the **Check-In Interval** field to the desired number of minutes between 240-10080 (240 minutes

to 1 week). **Note:**The minimum check-in interval is 4 hours. If you set a device's check-in interval to less than 4 hours, the change is ignored.

b. To define how often the device connects to DeviceHQ to send GPS data, set the **GPS Data Interval** field to the desired number of minutes, between 240-10080 (240 minutes to 1 week). **Note:** Some MTR models do not have GPS. Then this field does not display.

4. Enable **Single Check-In** to configure your device to check-in to DeviceHQ at the specific date and time. If you enable **Single Check-In**, click the **Date** field to select the date from the calendar picker, and then enter the **Time** (HH:MM) for your device to check-in.
5. Enable **Repeatable** to check-in to DeviceHQ periodically at the specified time daily or at the specific days of the week.

   a. Select **Daily** from the **Repeat** drop-down to check in to DeviceHQ every day, and enter the **Time** (HH:MM) for your device to check-in.

   b. Select **Custom** from the **Repeat** drop-down, then specify the days of the week, and enter the **Time** (HH:MM) for your device to check-in.

6. Go to options under **Update Settings**
7. If **Sync with Dial-On-Demand** is checked and cellular dial-on-demand is enabled, the connection is not dialed solely for the purpose of connecting to DeviceHQ. The device will connect to DeviceHQ only when other traffic brings up the link.
8. Check **Allow Firmware Upgrade** if you want DeviceHQ to make automatic updates of your firmware.
9. Check **Allow Configuration Upgrade** if you want DeviceHQ to make automatic updates of your configuration software.
10. Check **Allow Radio Firmware Upgrade** if you want DeviceHQ to make automatic updates of your cellular radio firmware.
11. Click **Submit**.
12. Click **Save and Apply** to save your changes.

***NOTE**: If you do not select **Intervals**, certain DeviceHQ features will NOT be available including:

- missed check-in alerts
- device rebooted alerts
- automatically scheduled device log uploads
- home page notices for rebooted or missed check-in devices

Notifications

The device can send alerts via email, SMS, and/or SNMP. To use these options, enable SMTP (see SMTP Settings for details), SMS (see Configuring SMS for details), and SNMP Traps (see Configuring SNMP for details).

A time stamp is added to the actual notifications. The format is **YYYY-MM-DD HH:MM**.

To setup notifications:

1. Go to **Administration > Notifications > Configuration**.
2. Under **Recipient Group**, click **Add Group** (you must add a group before you can edit/save your alert).
3. In the **Create Recipient Group** window, enter your **Group Name**.
4. Enter the person's **Name** and **Phone Number**. Click **Add Phone**.
5. Enter the person's **Name** and **Email**. Click **Add Email**.

6. Add name, phone number and email for each person in your group. When done, click **Submit**.
7. Click **Save and Apply** if you have no additional changes. Otherwise, skip to step 9.
8. See the list of available alerts:
    - **High Data Usage**
    - **Low Signal Strength**
    - **Device Reboots**
    - **Ethernet Interface Failure**
    - **Cellular Interface Failure**
    - **Ethernet Data Traffic**
    - **Cellular Data Traffic**
    - **WAN Interface Failover**
    - **Ping Failure**
    - **Security Violation**
    - **Resource Overuse**
    - **Wi-Fi Interface Failure***
    - **Wi-Fi Data Traffic***

    ***Only available on models with Wi-Fi capabilities
9. Click on the pencil icon under the **Edit** column for the alert you want to use and configure. The **Edit** dialog box appears for your chosen alert.

For **High Data Usage**:

1. Check **Enabled**.
2. Under **Data Plan Details**, select the **Plan Type** from the drop down menu which includes **Monthly** or **Custom Interval**.
3. If you choose **Custom Interval**, enter the **Interval** length in days.
4. Select the **Start Date** from the calendar picker.
5. Enter the **Limit** in **MB** for data usage.
6. In **Notify At**, enter the percentage of the limit that triggers notification to be sent.
7. Select alert recipients from **Recipient Group**.
8. Select how you want to send alerts by clicking **Email**, **SMS**, or **SNMP**.
9. Click **OK**.
10. To save your changes, click **Save and Apply**.

For **Low Signal Strength**:

1. Check **Enabled**.
2. Enter the **Signal Threshold** in **dBm**.
3. Enter the **Duration** in seconds.
4. Under **Alerts**, select the recipients under **Recipient Group**.
5. In **Notify**, enter the frequency of notification (in hours). Default is **24**.
6. Select how you want to send alerts by clicking **Email**, **SMS**, or **SNMP**.
7. Click **OK**.

8. To save your changes, click **Save and Apply**.

For **Device Reboots**:

1. Check **Enabled**.
2. Under **Alerts**, select the recipients under **Recipient Group**.
3. In **Notify**, the field for frequency of notification is shown. The predefined value is **Always** and cannot be modified by the user.
4. Select how you want to send alerts by clicking **Email**, **SMS**, or **SNMP**.
5. Click **OK**.
6. To save your changes, click **Save and Apply**.

For **Ethernet Interface Failure**:

1. Check **Enabled**.
2. Enter the **Duration** in seconds.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, enter the frequency of notification (in hours). Default is **24**.
5. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.
6. Click **OK**.
7. To save your changes, click **Save and Apply**.

For **Cellular Interface Failure**:

1. Check **Enabled**.
2. Enter the **Duration** in seconds.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, enter the frequency of notification (in hours). Default is **24**.
5. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.
6. Click **OK**.
7. To save your changes, click **Save and Apply**.

For **Ethernet Data Traffic**:

1. Check **Enabled**.
2. Enter **Interval** in hours when alert is sent.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, the constant value is **Always**.
5. Select how you want to send alerts by clicking **Email**, **SMS** or **both**.
6. Click **OK**.
7. To save your changes, click **Save and Apply**.

For **Cellular Data Traffic**:

1. Check **Enabled**.
2. Enter **Interval** in hours when alert is sent.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, the constant value is **Always**.

5. Select how you want to send alerts by clicking **Email**, **SMS** or **both**.
6. Click **OK**.
7. To save your changes, click **Save and Apply**.

For **WAN Interface Failover**:

1. Check **Enabled**.
2. Enter the **Timeout** in seconds.
3. Select what to **Notify On** from the drop-down.
4. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
5. In **Notify**, the constant value is **Always**.
6. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.
7. Click **OK**.
8. To save your changes, click **Save and Apply**.

For **Ping Failure**:

1. Check **Enabled**.
2. Under **Ping Details**, select the **Network Interface** from the drop-down.
3. Enter the **IP Address** or **URL** that you want to ping.
4. Enter the **Count**.
5. Enter the **Failure Threshold**.
6. Enter the **Ping Interval**.
7. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
8. In **Notify**, the constant value is **Always**.
9. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.
10. Click **OK**.
11. To save your changes, click **Save and Apply**.

For **Security Violation**:

1. Check **Enabled**.
2. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
3. In **Notify**, the constant value is **Always**.
4. Select how you want to send alerts by clicking **Email, SMS** , or **SNMP.**
5. Click **OK.**

For **Resource Overuse**:

1. Check **Enabled**.
2. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
3. In **Notify**, the constant value is **Always**.
4. Select how you want to send alerts by clicking **Email, SMS** , or **SNMP.**
5. Click **OK.**

The following notifications are only available on models with Wi-Fi capabilities:

For **Wi-Fi Interface Failure**:

1. Check **Enabled**.
2. Enter the **Duration** in seconds.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, enter the frequency of notification (in hours). Default is **24**.
5. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.
6. Click **OK**.
7. To save your changes, click **Save and Apply**.

For **Wi-Fi Data Traffic**:

1. Check **Enabled**.
2. Enter **Interval** in hours when alert is sent.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, the constant value is **Always**.
5. Select how you want to send alerts by clicking **Email** or **SMS**.
6. Click **OK**.
7. To save your changes, click **Save and Apply**.

Customizing the User Interface

You can change how the user interface on your device appears. To change the interface:

1. From the Navigation pane, select **Administration > Web UI Customization**.
2. To define what information appears on the **Administration: Support** page, use the Support group. See Customizing Support Information.
3. To define other settings, use the **Device Settings** group. See Specifying Device Settings.

Customizing Support Information

To customize the interface displaying information that can be used to support users:

1. To enable display of the custom support information, go to **Administration > Web UI Customization > Support Information** and check **Show Custom Info**.
2. Type the desired information into the optional fields including:
   - **Company Name**
   - **Country**
   - **Fax**
   - **Address 1**
   - **Address 2**
   - **City**
   - **State/ Prv**
   - **Zip Code**
   - **City**
3. To add a phone number:
   a. Click **Add Phone**.

   b. A label can appear next to the phone number, for example **Fax** or **Phone** or **International**. In the **Label** field, enter text that describes the phone number.
   c. In the **Number** field, type the phone number.

4. To add a link to a website, click **Add Link**.
   a. To label the website, type label text in **Label** field.
   b. In the **URL** field, type the website's link.
   c. To add further descriptive text about the site, type the information in the **Text** field.
5. To add an image, click **Upload Image:**
   a. Click **Browse**, go to the location of the image, and select the image.
   b. Click **OK.**
6. To delete an existing image, click **Remove Image**.
7. Click **Submit**.
8. To save your changes, click **Save and Apply**.

Specifying Device Settings

To define other custom settings for devices:

1. Go to **Administration > Web UI Customization > Device Settings**.
2. Enter desired information in the optional fields including:
   - **Device Name**
   - **Custom ID**
   - **Button Color**
   - **Button Font Color**
   - **Highlight Color**
   - **Highlight Font Color**

Note: To define color fields, use **#rrggbb** format.

3. To add a favorite icon, also known as a shortcut icon or bookmark icon, in the **Custom Favicon** field, click **Browse** to find where the Favicon file resides, select the desired file, and click **Upload Icon**.
4. To remove an existing favorite icon, click **Remove Icon**.
5. To add a custom logo, next to the **Custom Logo** field, click **Browse** to find where the logo file resides, select the desired file, and click **Upload Logo**.
6. To remove an existing logo, click **Remove Logo**.
7. Click **Submit**.
8. To save your changes, click **Save and Apply**.

Upgrading Firmware

Before upgrading: reboot the device.

Upgrade the device's firmware to the latest version. You can download firmware upgrades from the MultiTech website or update your firmware automatically through MultiTech's DeviceHQ™ system.

For added security, Signed Firmware Validation is automatically used once it's enabled after upgrading from version 5.1 and higher. This authentication method prevents attempts to load invalid or damaged firmware files in order to defeat possible tampering. The module does not load any firmware that MultiTech did not digitally sign.

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

There are two types of device firmware upgrades based on the upgrade file:

1. **Full Firmware Image Upgrade**: When applied, the full firmware update replaces the current firmware image with the new image of the new version.
2. **Differential Firmware Upgrade:** When applied, the current firmware image is updated with the differences between it and the new version, and effectively becomes the new version of firmware. **NOTE**: This type is only available in mPower 5.3 or later.

   NOTE: When selecting the appropriate file, the differential upgrade files use diff in the filename. Full upgrade files do not contain diff in the filename.

To upgrade the firmware locally on your device:

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

Note:

- The new firmware is written into flash memory.
- It may take up to 10 minutes to upgrade the firmware. Do not interfere with the devices's power or press the reset button during this time.
- The DeviceHQ is a cloud platform that provides the ability to remotely manage and upgrade devices. Please see the **Remote Management** section or visit www.devicehq.com for more information.

Package Management

The Package Management feature installs packages and displays already-installed packages for the user. The system allows you to install only packages signed by MultiTech. You also have the option to remove currently installed packages.

Package Management is only available to users with an Administrator role.

Note: If you reset the device to factory default settings or perform a device firmware upgrade (either full or differential), all installed packages are removed.

To install a new package:

1. Verify that the target package is signed by MultiTech.
2. Go to **Administration > Package Management**.
3. Click **Choose File** and browse to select your package file.
4. Click **Install**. The system provides the status of the installation.
5. After the system successfully installs your package, it displays the package details along with previously installed packages. The package details include: Package Name,Version, and Options (with a trash can icon for delete).

To remove an existing package:

1. Go to **Administration > Package Management**. See the **Installed Packages** list.
2. Click the **Trash Can** icon for the package entry you wish to remove.
3. The system displays a confirmation message asking if you want to uninstall the target package. If you want to proceed, click **OK**. If not, click **Cancel**.
4. If you proceed, the system provides the status of removal.
5. Once the system successfully uninstalls the package, verify its removal from the **Installed Packages** list.

Saving and Restoring Settings

Before using these settings and features, we recommend you clearly understand their behaviors and effects.

To restore previous configuration settings to your device, to restore settings to their factory or user-defined defaults, or to save the current configuration, see the following.

User-defined Default Settings

When you reset your device to user-defined default settings, the following actions occur:

- Your device restarts
- All settings modified by the user (not saved in the user-defined default configuration) are removed/returned to user-defined default settings
- Any custom applications saved under this configuration are restored (however, custom applications are not saved in configurations uploaded to DeviceHQ or restored when downloaded from it)
- Any Node-RED applications saved under this configuration are restored (including configurations uploaded to DeviceHQ)
- Installed packages are not included in user-defined default configurations but are not deleted (when you reset to user-defined default configuration, they are not restored this way)

Factory Default Settings

When you reset your device to factory default settings, the following actions occur:

- Your device restarts
- User-defined default configuration is deleted (if set)
- All settings modified by the user are removed/returned to factory default settings

- All custom applications are deleted
- All Node-RED applications are deleted
- All installed packages are deleted
- Customer images, favicons, and logos are deleted
- CA certificates are deleted and new certificates are generated
- Your web server's SSL certificate is deleted and a new certificate is generated
- SSH certificates are removed and new certificates are generated

Save and Restore Configuration

1. From the navigation bar, go to **Administration > Save/Restore > Save and Restore Configuration**.
2. To restore a configuration from a previously saved file:
   a. Next to the **Restore Configuration** field, click **Browse**.
   b. Navigate to the location where the configuration file is stored and select the desired file.
   c. Click **Restore**. The device reboots.
3. To save your current configuration to a file:
   a. Next to the **Save Configuration to File**, click **Save**.
   b. Navigate to the location where you wish to save the file and select location.

Factory Default

To reset the device's configuration to the factory default settings:

1. Click **Reset**.
2. A dialog box appears prompting you to confirm that you want to restore to factory default settings.
3. Click **OK**.

User-Defined Default

To restore the device to user-defined default settings, you must first set a current configuration as user-defined default.

1. To set deployment-specific default settings as user-defined defaults, under **Set Current Configuration As User-Defined Default**:
   a. Click **Set**.
   b. A dialog box appears prompting you to confirm that you want to save the current configuration as user-defined settings.
   c. Click **OK**.
2. To restore the device's configuration to the user-defined configuration settings, go to **Reset to User-Defined Configuration** under **User-Defined Default**:
   a. Click **Restore**.
   b. A dialog box appears prompting you to confirm that you want to restore to a set of user-defined settings.
   c. Click **OK**. The device reboots.
3. To clear user-defined defaults, under **Clear User-Defined Defaults**:

a. Click **Clear**.
b. A dialog box appears asking you if you want to clear user-defined defaults.
c. Click **OK**.

Reset Button Configuration

To enable reset to factory default settings:

1. Check **Enable Reset to Factory Default** under **Reset Button Configuration** (enabled by default).
2. Click **Submit**.
3. Then click **Save and Apply** to save your changes. No restart required.

   When you enable this option and press the reset button on the device for 5 seconds or more, the device will reset to factory default settings.

To enable reset to user-defined default settings:

1. Check **Enable Reset to User-Defined Default** under **Reset Button Configuration** (disabled by default).
2. Click **Submit**.
3. Then click **Save and Apply** to save your changes. No restart required.

   When you enable this option and press the reset button on the device 5 seconds or more, the device will reset to user-defined default settings.

To enable reset of **BOTH** factory default and user-defined default settings:

1. Check both options, **Enable Reset to Factory Default** and **Enable Reset to User-Defined Default** under **Reset Button Configuration**.
2. Click **Submit**.
3. Then click **Save and Apply** to save your changes. No restart required.

   To **Reset to User-Defined Configuration**:

   When you enable both options and press the reset button on the device for 5 seconds or more, the device will reset to user-defined default settings.

   To **Reset to Factory Default Configuration**:

   To override user-defined default configurations and restore the device to factory default settings, press and hold the reset button on the device for more than 30 seconds.

To disable **BOTH** factory default and user-defined default settings:

1. Uncheck both options, **Enable Reset to Factory Default** and **Enable Reset to User-Defined Default** under **Reset Button Configuration**.
2. Click **Submit.**
3. Then click **Save and Apply** to save your changes. No restart required.

   In this case, the reset button on the device only restarts the device and will not restore it to either factory default or user-defined default settings.

NOTE: Disabling factory default settings will mean there is no mechanism to restore the device to commissioning mode. Once the factory default has been disabled, do not lose track of your access credentials or access to the device will be lost.

Using the Debugging Options

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

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

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

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

See other topics for additional Debug Options:

- Auto Reboot Timer (automatically reboot device)
- Remote Syslog (configuring syslog)
- Ping and Reset Options
- Statistics Settings

See also: Statistics Configuration Fields

Automatically rebooting the device

To choose a specific time to reboot daily, the amount of time that passes before the device automatically reboots itself, or to disable this function:

1. Go **Administration > Debug Options > Auto Reboot Timer**, select **DAILY, TIMER,** or **DISABLED** from the drop-down under **Auto Reboot**.
2. If you chose **DAILY**, enter the **Time** of day you want device to reboot (in HH:MM format).
3. If you chose **TIMER**, enter the Interval (in hours) for the amount of time that passes before the device automatically reboots itself.
4. If you do NOT want the device to automatically reboot, select **DISABLED** (default).

Configuring Remote Syslog

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

To set up a log request in DeviceHQ, under **Devices**, select your device. Then click on Tasks and select **Request Device Logs**. After the request has been completed, return to the device administration software.

Note: If you change **Debug Log Level**, it does not require reboot. However, you must reboot the system in order for the log level in **/var/log/api.log** to be changed.

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

4. To download syslog information directly from the device, click **Download Logs**.
5. Click **Submit**.
6. To save your changes, click **Save and Apply**.

Statistics Settings

To configure **Statistics**:

1. Go to **Administration > Debug Options > Statistics**.
2. Enter the **Save Timeout** in seconds.
3. Enter the **Save Data Limit** in megabytes.
4. Click **Submit**.
5. To save your settings, click **Save and Apply**.

Statistics Configuration Fields

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

Field	Description
Save Timeout	The device saves the statistical data when the desired timeout period has elapsed. Default is 300 seconds (5 minutes).
Save Data Limit	The device saves the statistical data if the data limit is reached. Default is 5 MB.

Ping and Reset Options

Perform a Ping Test

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

To perform a ping test:

1. Go to **Administration > Debug Options > Ping**.
2. Enter the **IP address or URL** of the site you wish to ping.
3. Under **Network Interface**, choose from the available drop-down options including: **ANY, LAN, CELLULAR,** and **ETHERNET**. (Some models also support **WI-FI**).
4. Click **Ping**.

Reset Options

For various reset options, go to **Administration > Debug Options > Reset Options:**

- To reset the modem, click **Reset Modem.**
- To reset Wi-Fi, click **Reset Wi-Fi**.
- If you use a Verizon SIM only, click **Reset Class 3 APN (Verizon)** to initiate the OMA DM procedure, retrieve APN settings from Verizon, and apply them automatically to your modem settings.
- To reset Bluetooth, click **Reset Bluetooth**

Usage Policy

The device shall provide a Usage Policy for the system. The default usage policy reads as follows:

This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

This policy displays on the login page. You may modify or add language to the policy as needed.

To view or modify the **Usage Policy**:

1. Go to **Administration > Usage Policy**.
2. The default language appears. You may edit the language directly in the text box.
3. When completed, click **Submit**.
4. To save your changes, click **Save and Apply**.

If at any time you want to return the device to the default setting, click the **Reset to Default** button in the bottom right corner. (This reverts the **Usage Policy** back to the default language.)

Chapter 12 – Status & Logs

Viewing Device Statistics

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

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

   System

   Ethernet

   Wi-Fi

   Access Point

   Cellular

   Serial

   Bluetooth

   GRE

   IPSec

   OpenVPN

   LoRa

Definitions

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

- **Total**: Total number of sent/received bytes for a 365-day period.
- **Today**: Total number of sent/received bytes for today.
- **Sessions**: Bytes.
- **Packets**: Number of successfully transmitted (TX) and received (RX) packets.
- **Errors**: Number of errors that occurred. Possibly due to connection issues or network congestion.
- **Dropped**: Number of dropped packets. Possibly due to memory constraints.
- **Overruns**: Number of overruns that occurred. Possibly due to processing constraints.
- **Frame**: Number of invalid packets.
- **Carrier**: Number of signal modulation errors that occurred (possibly due to physical connection).
- **Collisions**: Number of packet collisions that occurred due to network congestion.
- **Queue Length**: Length of the transmit queue.
- **MTU** (Maximum Transmission Unit): the maximum size of packet content (Bluetooth only).
- **ACL** (Asynchronous Connection-Less): the typical protocol used for data packets (Bluetooth only).
- **SCO** (Synchronous Connection-Oriented): the typical protocol used for voice (Bluetooth only).
- **Events**: Number of events that occurred on a Bluetooth connection (Bluetooth only).
- **Commands**: Number of commands given to devices on a Bluetooth connection (Bluetooth only).

Cumulative and Daily Usage

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

Timeframe of Chart

Change the time frame for the chart by clicking **Start Date** or **End Date** using calendar to set a different date.

Show Log

The associated run-time logs for this section.

LoRa Statistics

The **LoRa** statistics tab contains Received and Sent statistics for LoRa packets received and sent by the LoRa network server. These statistics can be cleared with the **Clear History** button. This tab also contains the list of nodes that have joined the network the device is supporting. There are statistics for each node and also status information in this table. This list can be refreshed by clicking on the **Refresh Node List** button.

Service Statistics

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

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

Mail Log

Mail Log shows the recent email delivery attempts and the mail log details. Mail log entries are sorted by date with the most recent on top. You can select the number of emails to display in the queue. Possible values are **5, 10, 25, 50**, or **All emails**.

1. Go to **Status & Logs > Mail Log** to display the **Mail Log** window.
2. To see the delivery details, click the eye icon under **Options** for the desired email entry.
3. To delete all mail log entries, click **Purge Log**.
   Note: Logs do not persist through power cycles.

Mail Queue

Mail Queue shows the emails that are waiting to be sent. The most recent email delivery attempts are on top. You can select the number of emails to display in the queue. Possible values are **5, 10, 25, 50**, and **All emails. Note:** Logs do not persist through power cycles.

1. Go to **Status & Logs > Mail Queue** to display the **Mail Queue** window.
2. To view the delivery details for an individual email, click the eye icon under **Options** for the desired email entry.

Notifications Sent

This page displays attempts to send Notifications via email, SMS, or SNMP.

The list includes the following details of each attempted notification: **Date, Message, Recipient Group**, and the status of the notification under each communication method including **Email, SMS**, and **SNMP**. A check indicates success via that method. An **X** means failure. No symbol or a blank space indicates that method was not attempted.

To view **Notifications Sent**:

1. Go to **Status & Logs > Notifications Sent**.
2. In the upper right corner, click **Refresh** to update the list.
3. To the right of **Refresh**, click **Delete All Notifications** if you want to remove all items in the list.

RF Survey

RF survey is not available for LTE models.

If you have a non-LTE device with a SIM card and want to perform an RF Survey, enter this address: 192.168.2.1/rf_survey and follow the instructions below. (The link uses the default IP address for the device upon log in. If you change the IP address of the device, make sure to use that new IP address in the link).

After the RF Survey, you must reset the device in order to restore cellular radio functionality.

The RF Survey tool allows you to view the list of the cell towers that belong to the carrier and their signal quality details such as Signal Level and Signal Noise Ratio. You need a SIM card to acquire the list of available cell towers.

Note: Selecting this tool terminates any existing PPP connection

1. Enter this address: 192.168.2.1/rf_survey to open the **RF Survey** page.
   - The search for the cell towers takes up to 2 minutes. The wait icon displays while the search is in progress.
   - The cell tower to which the device is currently connected displays at the top of the list.
2. To view the Signal Strength chart of a carrier, under **Options**, click the eye icon for the carrier.
   - The **Carrier Details** window appears.
   - This feature helps you decide which area has better signal strength and thus a better location for the device.
3. After the RF survey, reset your device. Go to **Commands > Restart Device**.

Chapter 13 – Apps

Manage Apps

Manage Apps

The **Manage Apps** screen under **Apps** provides information on installed custom applications including the status and version of all the installed applications.

Node-RED Apps

NOTE: Support for Node-RED/Node.js on Multitech AT91SAM9G25-based products has been discontinued within mPower 5.3.0. For mPower 5.3.3 or higher, users can install Node-RED as a custom application. See Install Node-RED as a Custom App. For details on other methods to create applications, see Creating a Custom Application.

The **Node-RED Apps** section displays information for the currently running Node-RED application. Only one Node-RED application can be running at a time on the device.

Node-RED is disabled by default to save system resources. First, check **Enabled** to enable **Node-Red**.

If you want to launch Node-RED, click the **Launch Node-RED** button at the top.

You can also upload applications to **DeviceHQ™** either as a new application or a new version of an existing application. To upload Node-RED applications to DeviceHQ:

1. Click **Upload**. Then select **a new app** or **an update** from the drop-down.
2. Enter the **application name**
3. Enter the **version**.
4. Enter your DeviceHQ login credentials including **email** and **password**. **Note:** For security purposes, the credentials are not saved on the device.
5. Click **Upload**.

DeviceHQ Login Credentials

Item	Default Value	Description
Email	Blank	Email address used to login to DeviceHQ account that administers apps.
Password	Blank	Password used to login to DeviceHQ account that administers apps.

Custom Apps

Check **Enabled** to enable custom applications.

Uncheck **Backup On Install** if you do not want to backup the currently running application while installing a new version of the application. When checked, the backup is re-installed if the installation of a new version of the app fails.

The **Custom Apps** section contains the list of custom applications currently installed on the device. Each listing contains the information for a particular application including the **name, version, status, and info** of the application. The status value can be **Started, Running, Stopped, Failed, Install Failed,** and **Start Failed**.

Refer to Creating a Custom Application on the MultiTech Developer Resources website for complete instructions on developing, installing, and deploying custom applications.

To install a new Custom app, click **Add Custom App**:

1. In the **App ID** field, enter Application ID.
2. In the **App Name** field, enter Application Name.
3. Click **Browse**, go to the location of the custom app, and select the file.
4. To install the app, click **Install Custom App**.

After any changes to this section, click **Save and Apply** to apply those changes.

Chapter 14 – Docker

Docker

Docker is a client-server application technology which manages containers. Containerization is an efficient way to encapsulate applications and its dependencies in a lightweight, portable environment. Docker enables you to separate your applications from your infrastructure so you can develop, test, and deploy software more quickly.

You can use Docker on MTCDT3AC devices with mPower 5.4x software or higher. The UI provides a view of what is currently active, installed, and/or running on the device with regards to Docker.

You can view the following Docker items in the device UI if they are already active, installed, and/or running on the device:

- Containers
- Images
- Networks
- Volumes
- Host

But in order to perform key Docker tasks such as building images, removing images, creating containers, and other functions, you must log into your device over SSH/debug console, move to the user_data directory, and execute them at the command prompt.

Prior to testing any Docker containers, check:

- your internet connection
- the current date-time
- that your device has enough disk space

NOTE: Docker makes changes to the system firewall rules and IP tables. Docker adds its own rules on daemon start and can add/remove/modify rules while the docker daemon is running.

Docker Resources

For general information on Docker, see: docs.docker.com

Please note that the following instructions require:

1. Registered accounts with third-party providers such as Docker, AWS, and MS Azure.
2. Use of a separate Docker application (see link on Docker for Conduit3 Devices for further details).

For details on how to use Docker on this device, refer to the following: Docker for Conduit3 Devices -- How To Instructions and Examples

Docker Containers

To see currently installed and running Docker containers on the device:

1. Go to **Docker > Containers.**
2. See the list of active **Docker Containers** showing State, Name, Image, Created, IP Address, Published Ports, and Details (eye icon) for each container.
3. Click on the eye icon to view **Container Details** of each container. The system displays the following:

a. Container Status

   i. ID
   ii. Name
   iii. Status
   iv. Created (date and time created)
   v. Start Time

b. Container Details

   i. Image
   ii. Port Configuration
   iii. CMD
   iv. ENV

c. Connected Networks

   i. Network
   ii. IP Address
   iii. Gateway
   iv. MAC Address
   v. Details (eye icon)

4. Click **Back** to return to the previous selection.

Docker Images

To see currently installed and running Docker images on the device:

1. Go to **Docker > Images.**
2. See the list of active **Docker Images** showing ID, Tags, Size, Created, and Details (eye icon) for each image.
3. Click on the eye icon to view **Image Details** of each image. The system displays the following:

   a. Image Details

      i. Tag
      ii. ID
      iii. Size
      iv. Created (date and time created)
      v. Build

   b. Dockerfile Details

      i. CMD
      ii. Expose
      iii. Volume
      iv. Env

   c. Image Layers

4. Click **Back** to return to the previous selection.

Docker Networks

To see currently active Docker network interfaces on the device:

1. Go to **Docker > Networks.**
2. See the list of active **Docker Networks** showing Name, Driver, Attachable, Internal, IPAM driver, IPAM Subnet, IPAM Gateway, and Details (eye icon) for each container.
3. Click on the eye icon to view Network **Details** of each network interface. The system displays the following:
    a. Network Details
        i. Tag
        ii. ID
        iii. Driver
        iv. Scope
        v. Attachable
        vi. Internal
        vii. Subnet
        viii. Gateway
    b. Containers in Network
        i. Container Name
        ii. IPv4 Address
        iii. IPv6 Address
        iv. MAC Address
        v. Details (eye icon)
4. Click **Back** to return to the previous selection.

Docker Volumes

To see currently used Docker Volumes on the device:

1. Go to **Docker > Volumes.**
2. See the list of active **Docker Volumes** showing Name, Driver, Used, Mount Point, Created, and Details (eye icon) for each volume.
3. Click on the eye icon to view **Volume Details** of each Volume. The system displays the following:
    a. Volume Details
        i. ID
        ii. Created (date and time)
        iii. Mount Path
        iv. Driver

b. Containers using volume

i. Container Name
ii. Mounted At
iii. Read-only
iv. Details (eye icon)

4. Click **Back** to return to the previous selection.

Docker Host

To view the current Docker Host details:

1. Go to **Docker > Host**.
2. Under **Docker Host Details**, the system displays the following:

a. Host overview

i. Hostname
ii. OS Information
iii. Kernel Version
iv. Total CPU
v. Total memory

b. Engine Details

i. Version
ii. Root directory
iii. Storage Driver
iv. Logging Driver
v. Volume Plugins
vi. Network Plugins

3. Click **Back** to return to the previous selection.