rCell 300 Configuration Guide

Using mPower™ Edge Intelligence

rCell 300 Configuration Guide

Model: MTR3-L4G2D

Document Part Number: S000829 Rev 1.0

Copyright

Trademarks

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.

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Multi-Tech Systems, Inc. Multi-Tech Systems, Inc. provides this document "as is," without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Multi-Tech Systems, Inc. may make improvements and/or changes in this manual or in the product(s) and/or the software described in this manual at any time.

Contents

1 Introduction

This guide provides information and procedures necessary to configure an rCell 300 Series router using the mPower Edge Intelligence interface.

The rCell 300 router provides secure data communication between many devices that use legacy as well as current communication technologies.

Note: For complete hardware information about the rCell 300 router, refer to the rCell 300 Series Router Hardware Guide.

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

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

Intended Audience

The intended audience of this guide is IT personnel tasked with installing, provisioning, and configuring an rCell 300 router.

About the rCell 300

The MultiTech rCell 300 router is both an industrial router and a specialized network device designed to connect internet-of-things (IoT) devices. The rCell 300 provides enhanced security to protect against cyber threats, includes edge intelligence to run local applications, and offers secure data communication between many types of devices that use legacy or the latest communication technologies. The rCell 300 can be remotely managed via MultiTech Device Manager.

Intended Use

The rCell 300 is designed for a variety of industrial and IoT applications. Some of its intended uses include:

- **Remote monitoring and control**: This device is ideal for remote monitoring and control of equipment and systems in industries such as oil and gas, utilities, and agriculture. The rCell 300 allows for real-time data collection and management of remote locations.
- **Smart cities and infrastructure**: This device can be used in smart-city applications, including traffic management, environmental monitoring, and electric vehicle charging stations.
- **Industrial automation**: This device works with current industrial automation equipment (such as RTU) for remote data collection, fault notifications, control/manage field equipment.

The rCell 300 can be used in applications that require equipment to operate in harsh environments. For outdoor deployments, the rCell 300 must be installed in a waterproof enclosure.

Operating Modes

rCell 300 routers can operate in the following modes:

- Network Router
- Cellular IP Passthrough mode

Once the initial commissioning process for the rCell 300 has been completed, the mPower Setup Wizard allows administrators to select the desired operating mode upon logging in to mPower via the LAN.

mPower™ Edge Intelligence

mPower™ Edge Intelligence is an embedded software offering to deliver programmability, network flexibility, enhanced security, and manageability for scalable Industrial Internet of Things (IIoT) solutions. mPower represents the unification and evolution of well-established MultiTech smart router and gateway firmware platforms.

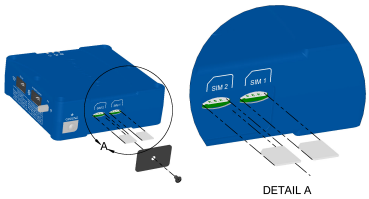
mPower Edge Intelligence simplifies integration with a variety of popular upstream IoT platforms to streamline edge-to-cloud data management and analytics, while also providing the programmability and processing capability to execute critical tasks at the edge of the network to reduce latency; control network and cloud services costs, and ensure core functionality – even in instances when network connectivity may not be available. In response to evolving customer security requirements, mPower Edge Intelligence incorporates a host of new security features including signed firmware validation, secure boot, new Cloud management, programmability of custom apps, DI/DO, and more.

2 Getting Started

Install the SIM Card(s)

To operate the device on a particular wireless network, install a micro (3FF) SIM card rated for industrial use.

1. Using a #1 Phillips screwdriver, remove the SIM card cover.



2. In the **SIM 1** slot, insert the SIM card for the primary cellular network and push until it snaps into place.
3. *Optional:* In the **SIM 2** slot, insert the SIM card for the secondary cellular network and push until it snaps into place.
4. Reinstall the SIM card cover.

Add the Device to Your Cloud Account

Prerequisite: You must have a MultiTech Cloud Service Platform Account. To create an account, go to https://cloud.multitech.com. Refer to the rCell 300 Quick Start Guide to connect and manage your device.

You can choose to add the rCell 300 device either via QR code or manually:

- **QR Code**
  a. Using a smartphone camera, scan the onboard QR code from the device serial label. See rCell 300 Serial Label.
  b. Follow the instructions to sign in to your cloud account and quickly onboard the device.
- **Manually**
  a. Sign in to your cloud account.
  b. Select **Gateways**.
  c. Under **Actions**, select **Add device**.
  d. Enter the PID number from the device serial label. See rCell 300 Serial Label.

Install the Device

To begin using the rCell 300:

1. Connect the cellular, GNSS, and Wi-Fi antennas.
2. Connect the local configuration port (ETH0/LAN) on the rCell 300 to the networked device on the LAN network. The LAN port has a static IP of 192.168.2.1.
3. *Optional:* If using a serial device, use the 8-wire terminal block connectors to connect to the RS-232 or RS-485 serial port:
   a. Wire the push-in spring 8-wire terminal plug per your application needs.

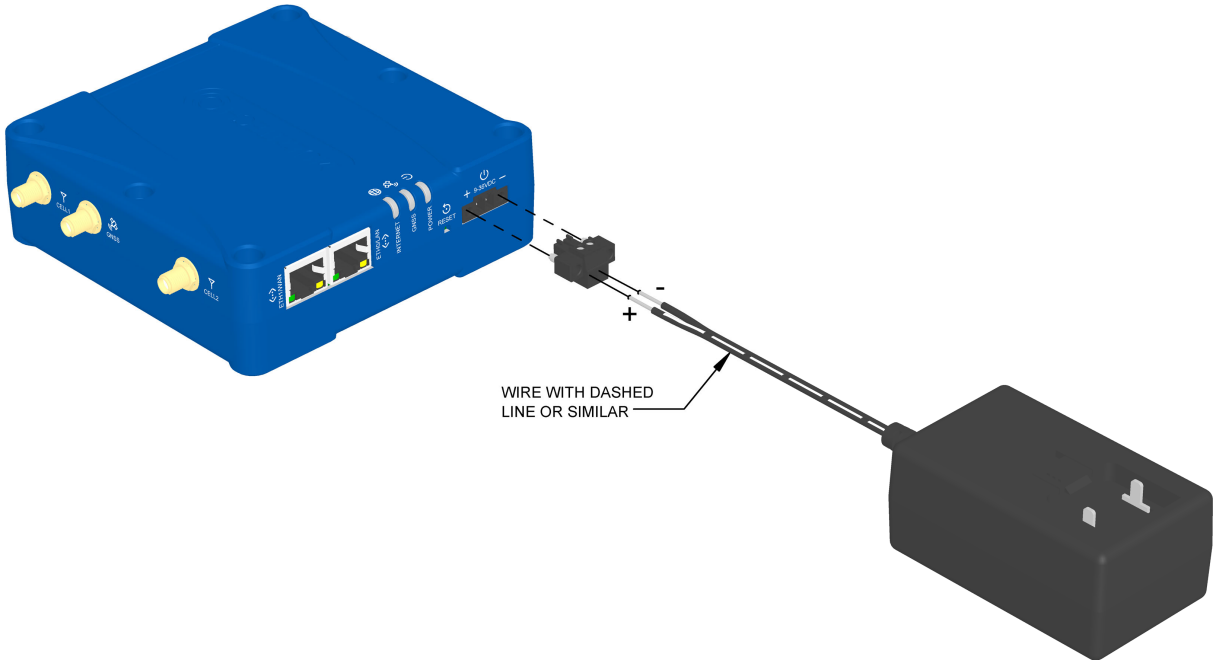
      Note: Refer to Terminal Block Connector Pinout in the rCell 300 Series Router Hardware Guide for complete information.

   b. Secure the 8-wire terminal plug to the device using a 2.5 mm slotted screwdriver.

   Note: The RS-232 port on the rCell 300 is not a local configuration port.
4. Connect the power supply:
   a. Using a 2.0 mm slotted screwdriver, screw the power supply wires into the 2-wire terminal plug.
   b. Secure the 2-wire terminal plug to the 9–36 VDC 2-pin terminal block on the device using a 2.5 mm slotted screwdriver.
   c. Connect the power supply to a power source. The POWER LED turns solid green when the device is ready for use.

   The proper polarity is shown below.

   Note: The customer should take steps to prevent any potential reverse polarity connections.

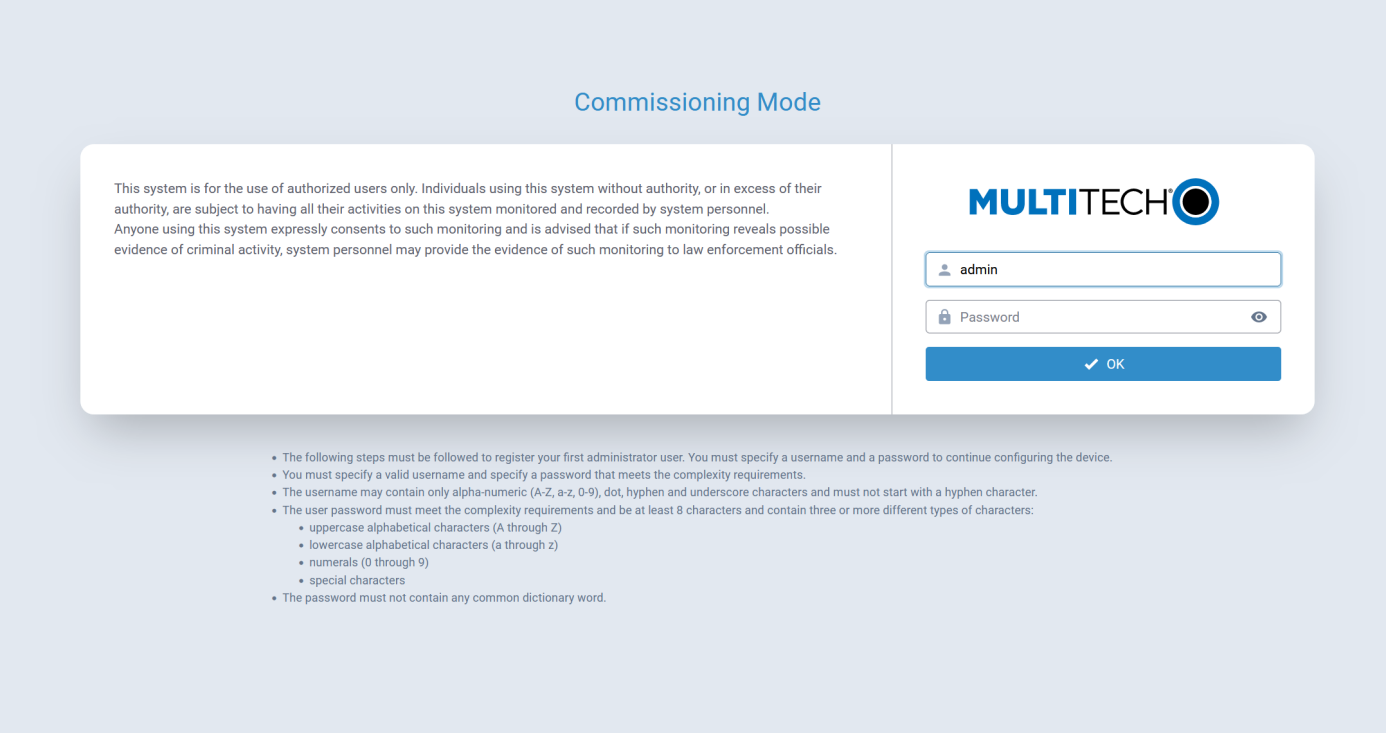


5. Use the device web user interface to configure the device.

- The default IP address for the ETH0/LAN port is 192.168.2.1.
- A DHCP server is enabled on the LAN interface to provision an IP to any device making a request for one. The range of addresses being assigned by this server is 192.168.2.100 to 192.168.2.254, with a subnet mask of 255.255.255.0.
- When you log in for the first time, the device is in commissioning mode, which requires you to set up a username and password for an administrator user account. Enter and submit your desired username and password.

Commissioning Mode

The device ships in what is called Commissioning Mode. As soon as the device is reset to factory defaults or right after the manufacturing process is complete, the system is in Commissioning Mode.



In this mode, the ETH1 /WAN is configured as WAN DHCP Client and the system attempts to connect to Device Manager (MT Cloud) as soon as there is internet connection.

The ETH0/LAN interface is configured with an IP of 192.168.2.1 and a netmask of 255.255.255.0.

Important: To access the Web UI once the device has been powered up and is in Commissioning Mode, the device can be accessed directly through the LAN interface at 192.168.2.1. The LAN interface has a DHCP server running on it to provide addresses in the range of 192.168.2.100 - 192.168.2.254, netmask 255.255.255.0.

First Time Setup Wizard

The First Time Setup Wizard allows setting up the operating mode (Network Router or Cellular IP Passthrough) configuring the system date and time, and configuring cellular connection.

SIM Card Has Been Installed

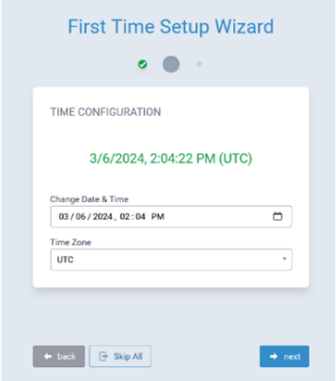
When a SIM card has been installed, the system allows users to set a PIN code and APN for the installed SIM card.

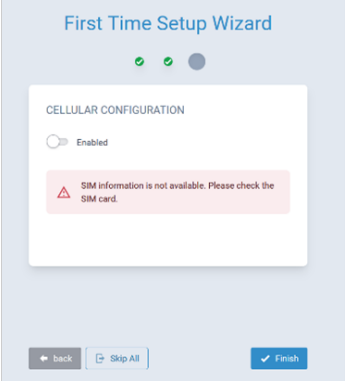
Note: By default, the system will only detect a SIM card that has been installed into the SIM1 slot. Users must install a SIM card into the SIM1 slot, otherwise the system will not see the SIM card. When installing a SIM card into the SIM2 slot, users must manually enable and configure the SIM2 slot separately when configuring mPower.

In this case, the system creates a corresponding provider profile and SIM profile that are linked to the installed SIM card.

SIM Card Has Not Been Installed

If no SIM card has been installed, the system will only allow cellular to be enabled.





3 Network Router Mode

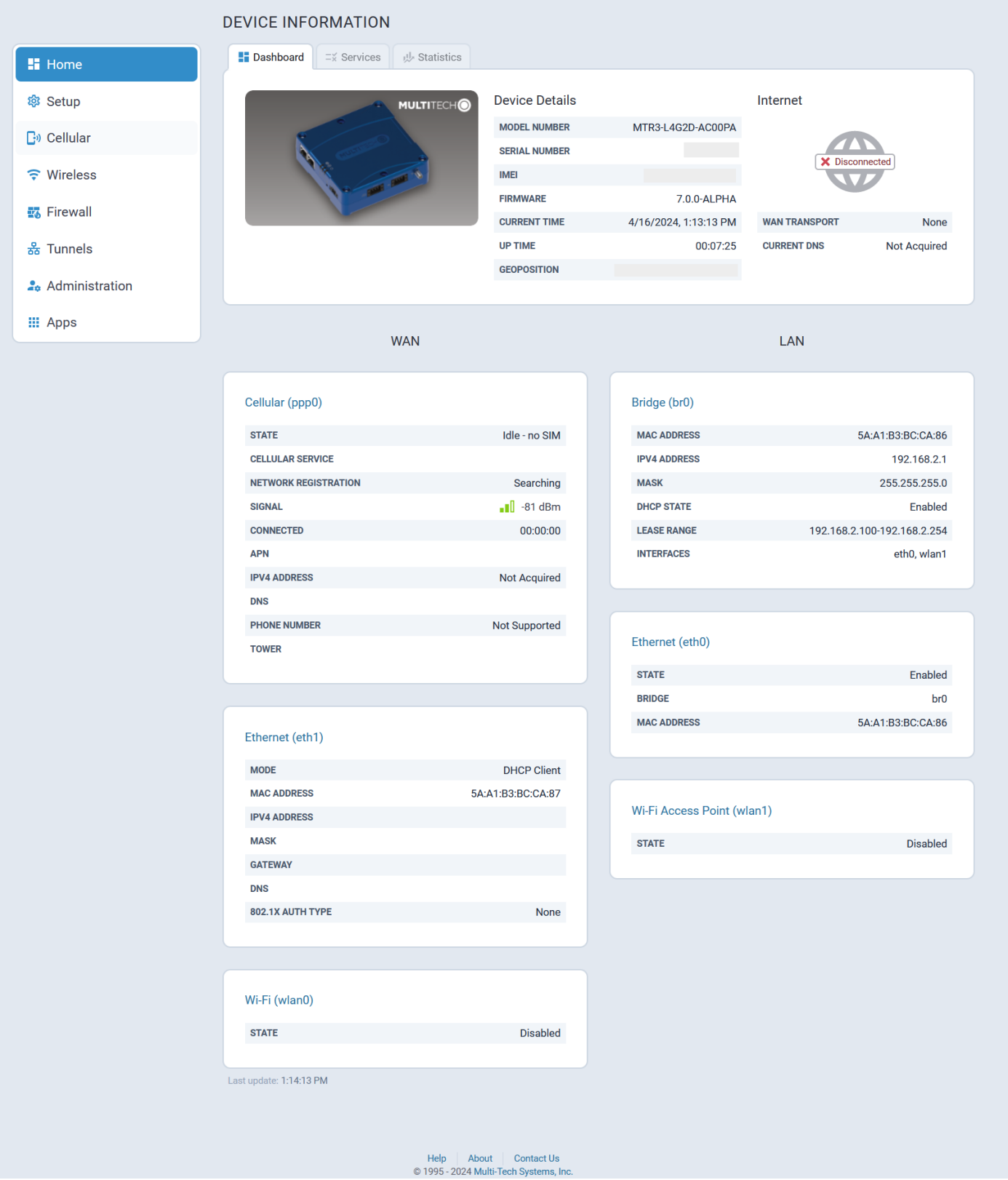
Home Menu

The Home menu comprises the following tabs:

- Dashboard
- Services
- Statistics

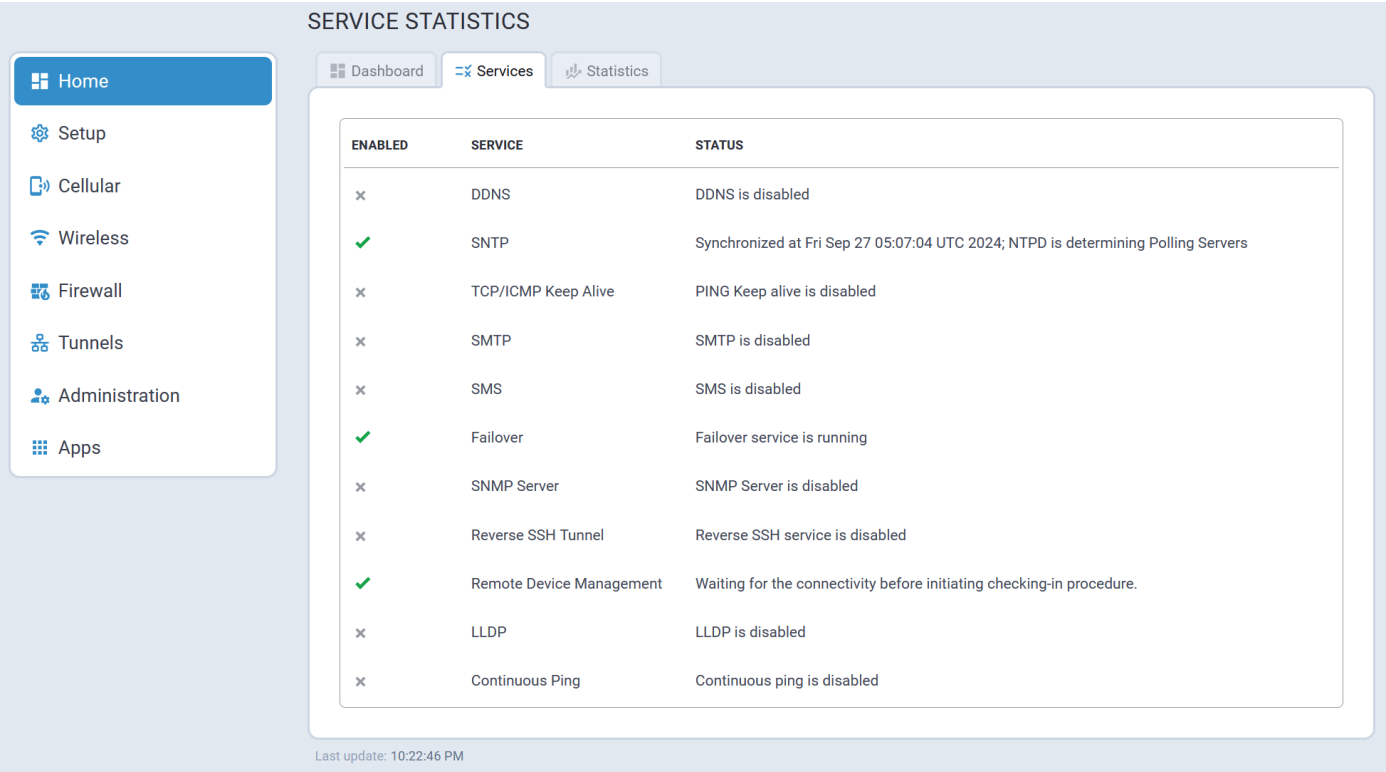
Dashboard Tab

The Dashboard tab provides a brief overview of the system state and configuration.


DEVICE INFORMATION
Home
Setup
Cellular
Wireless
Firewall
Tunnels
Administration
Apps
Dashboard
Services
Statistics
MULTITECH
Device Details
MODEL NUMBER MTR3-L4G2D-AC00PA
SERIAL NUMBER
IMEI
FIRMWARE 7.0.0-ALPHA
CURRENT TIME 4/16/2024, 1:13:13 PM
UP TIME 00:07:25
GEOPOSITION
Internet
Disconnected
WAN TRANSPORT None
CURRENT DNS Not Acquired
WAN
LAN
Cellular (ppp0)
STATE Idle - no SIM
CELLULAR SERVICE
NETWORK REGISTRATION Searching
SIGNAL -81 dBm
CONNECTED 00:00:00
APN
IPV4 ADDRESS Not Acquired
DNS
PHONE NUMBER Not Supported
TOWER
Ethernet (eth1)
MODE DHCP Client
MAC ADDRESS 5A:A1:B3:BC:CA:87
IPV4 ADDRESS
MASK
GATEWAY
DNS
802.1X AUTH TYPE None
Wi-Fi (wlan0)
STATE Disabled
Last update: 1:14:13 PM
Bridge (br0)
MAC ADDRESS 5A:A1:B3:BC:CA:86
IPV4 ADDRESS 192.168.2.1
MASK 255.255.255.0
DHCP STATE Enabled
LEASE RANGE 192.168.2.100-192.168.2.254
INTERFACES eth0, wlan1
Ethernet (eth0)
STATE Enabled
BRIDGE br0
MAC ADDRESS 5A:A1:B3:BC:CA:86
Wi-Fi Access Point (wlan1)
STATE Disabled
Help | About | Contact Us
© 1995 - 2024 Multi-Tech Systems, Inc.

Services Tab

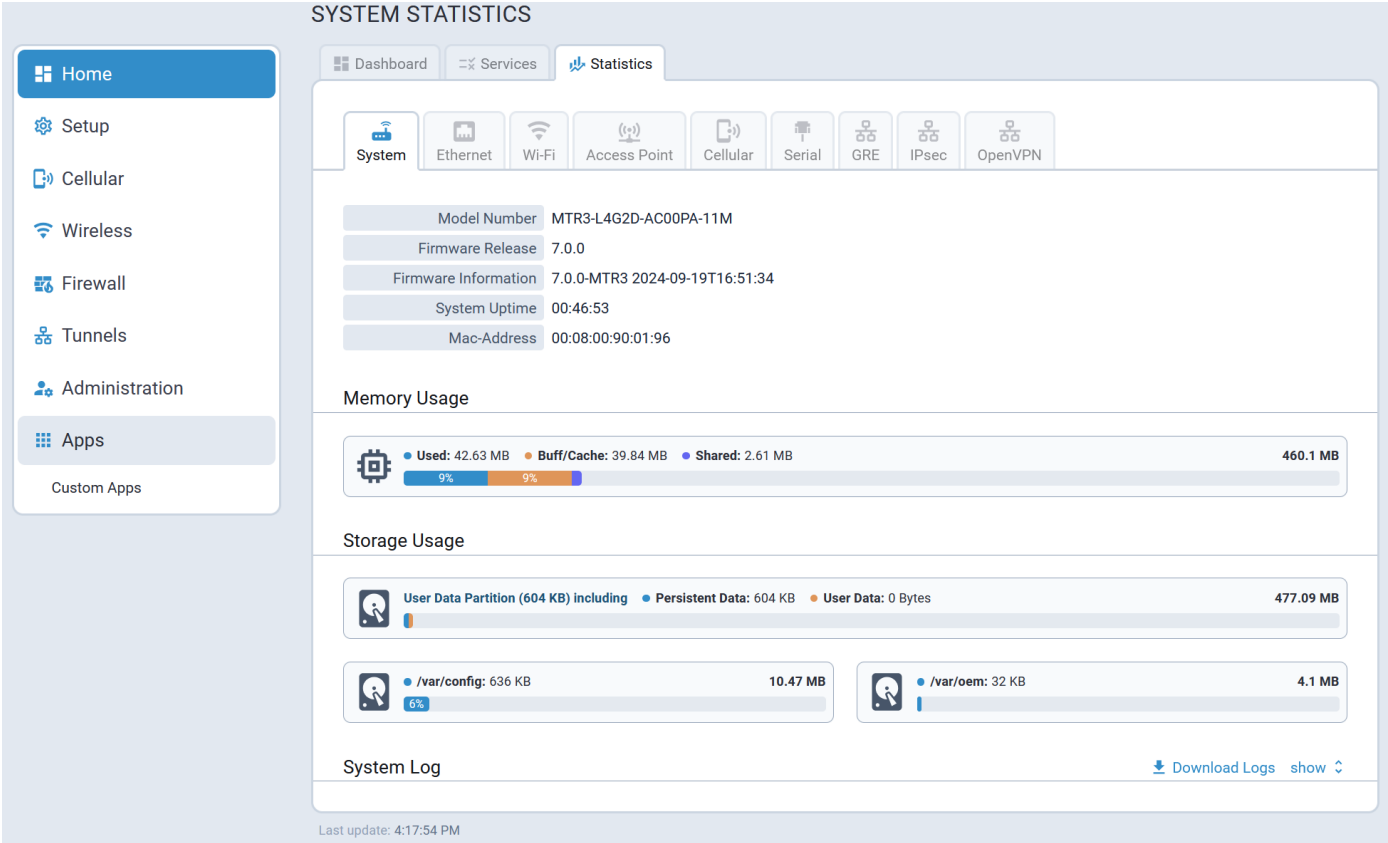
The Service Statistics tab lists the available services and their respective status.



Statistics Tab

The System Statistics tab provides the following system information:

- System details, memory and storage usage, system log
- Ethernet interfaces statistics and logs
- Wi-Fi as WAN statistics and logs
- Wi-Fi Access Point statistics and logs
- Cellular statistics and logs
- Serial statistics and logs
- GRE tunnels statistics and logs
- IPSec tunnels statistics and logs
- OpenVPN tunnels statistics and logs



Setup Menu

The Setup menu provides access to the following configuration settings:

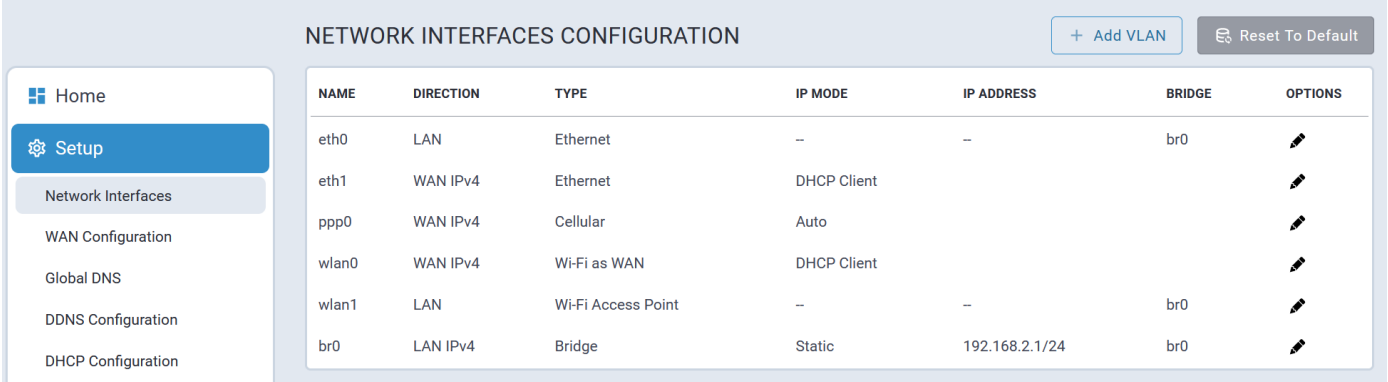
- Network Interfaces
- WAN Configuration
- Global DNS
- DDNS Configuration
- DHCP Configuration
- LLDP Configuration
- GPS Configuration
- SMTP Configuration
- Serial Configuration
- SNMP Configuration
- Time Configuration
- Digital I/O

Network Interface Configuration

By default:

- eth0 is configured as LAN

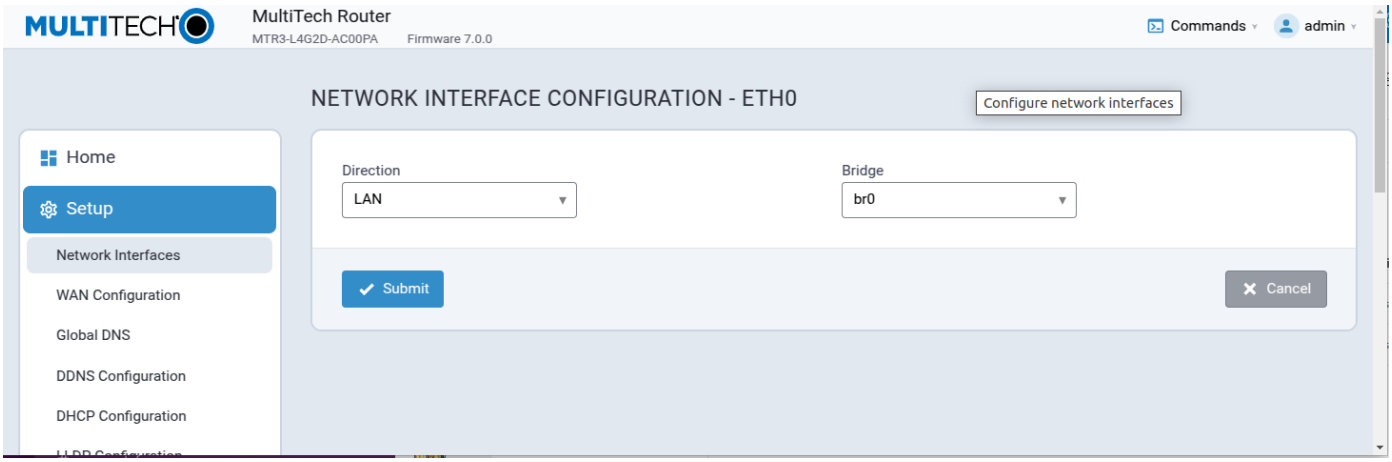
- eth1 is configured as DHCP Client



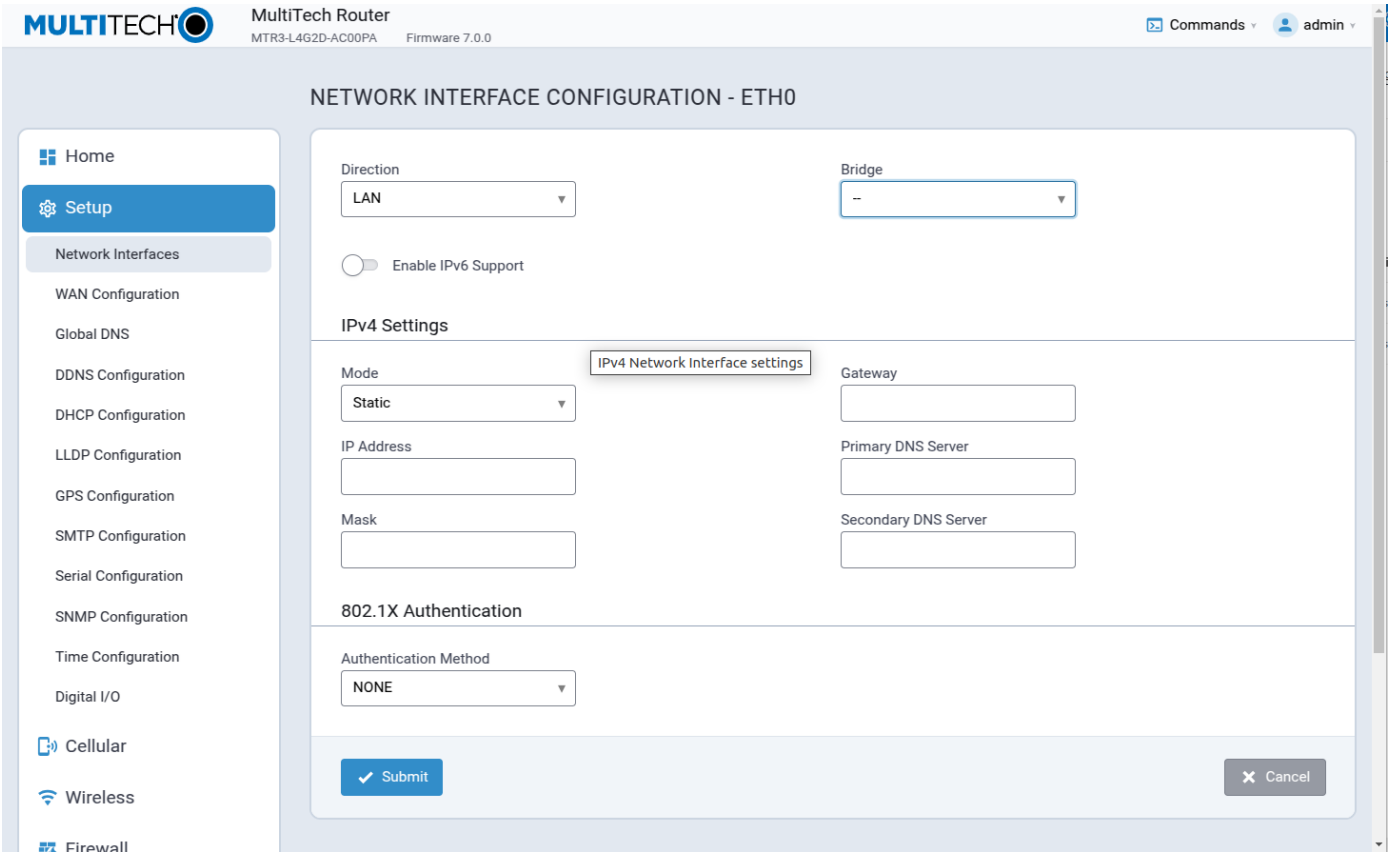
Configure eth0

To update the **eth0** interface configuration, select the corresponding pencil icon in the OPTIONS column.

Note: By default the eth0 interface is configured "under" the bridge interface. **br0**.

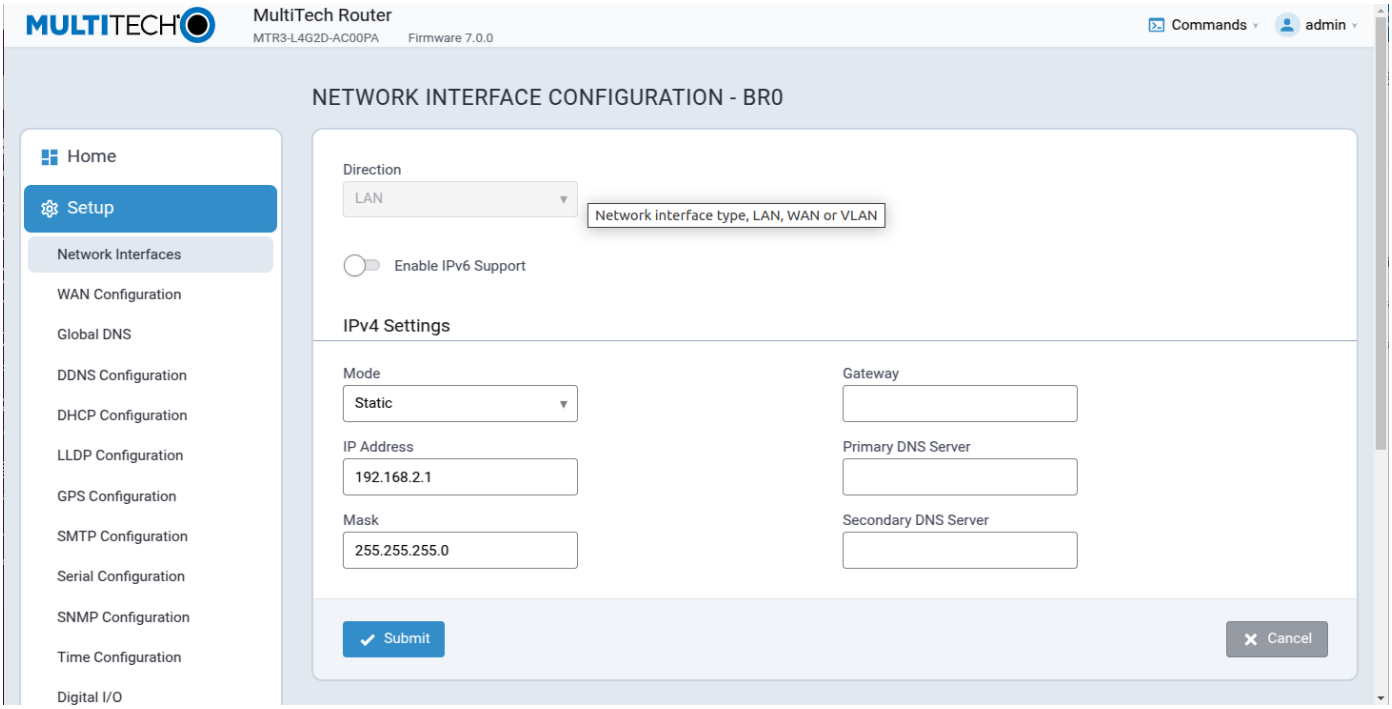


The eth0 interface can be removed from the bridge interface and configured independently by updating the **Bridge** field:



Configure br0

The bridge (br0) interface has the following configuration options to manage all the LAN interfaces assigned to it:



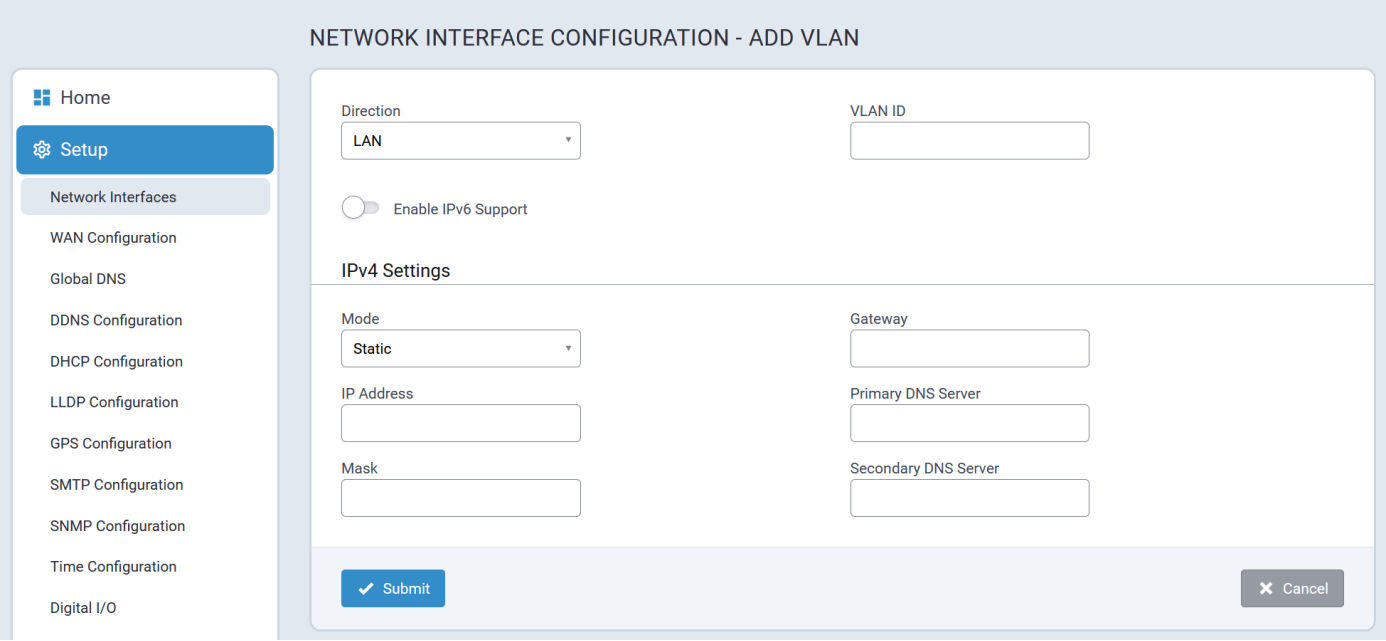
Ethernet Interface Configuration Parameters

The following is a description of each of the fields in the interface configuration for the Ethernet interfaces:

Field Name	Description
Direction	LAN, WAN or VLAN. WAN requires configured settings for gateway and DNS for the device to function effectively. VLAN indicates a VLAN interface associated with the Eth0 interface.
Bridge	br0 for Eth0 to be under the bridge. '-' for it to be independent of the bridge.
Enable IPv6 Support	Enable IPv6 on the interface allowing delegated prefix or static IPv6 address settings.
Mode	Static for static IP and Mask settings, DHCP Client for obtaining address information via DHCP
IP Address	Static IPv4 address to assign to the interface
Mask	The network mask for the network that the interface will be assigned to.
Gateway	Default Route Gateway
Primary DNS Server	DNS server for the network the interface is connected to
Secondary DNS Server	Backup DNS server for the network the interface is connected to
802.1X Authentication	Enable support for EAP-PWD, EAP-TLS, EAP-TTLS, or EAP-PEAP authentication of the device on the network connected to the interface.

Add a VLAN Interface

Create a new VLAN interface, and then configure eth0, eth1, or WLAN1 to use VLAN with the specified VLAN ID.



Typical VLAN interfaces are illustrated here:

NETWORK INTERFACES CONFIGURATION

+ Add VLAN | Reset To Default

NAME	DIRECTION	TYPE	IP MODE	IP ADDRESS	BRIDGE	OPTIONS
eth0	LAN	Ethernet	--	--	br0	
eth1	WAN IPv4	Ethernet	DHCP Client			
ppp0	WAN IPv4	Cellular	Auto			
wlan0	WAN IPv4	Wi-Fi as WAN	DHCP Client			
wlan1	LAN	Wi-Fi Access Point	--	--	br0	
br0	LAN IPv4	Bridge	Static	192.168.2.1/24	br0	
vlan.31	LAN IPv4	VLAN	Static	192.168.3.1/24		
vlan.41	LAN IPv4	VLAN	Static	192.168.4.1/24		
vlan.100	WAN IPv4	VLAN	DHCP Client			

To configure an existing ethernet interface to use VLAN (eth0) select VLAN from the Direction pull-down list as shown here:

NETWORK INTERFACE CONFIGURATION - ETH0

Direction

VLAN

LAN
WAN
VLAN

NAME	DIRECTION	IP MODE	IP ADDRESS	OPTIONS
vlan.41	LAN IPv4	Static	192.168.4.1/24	+

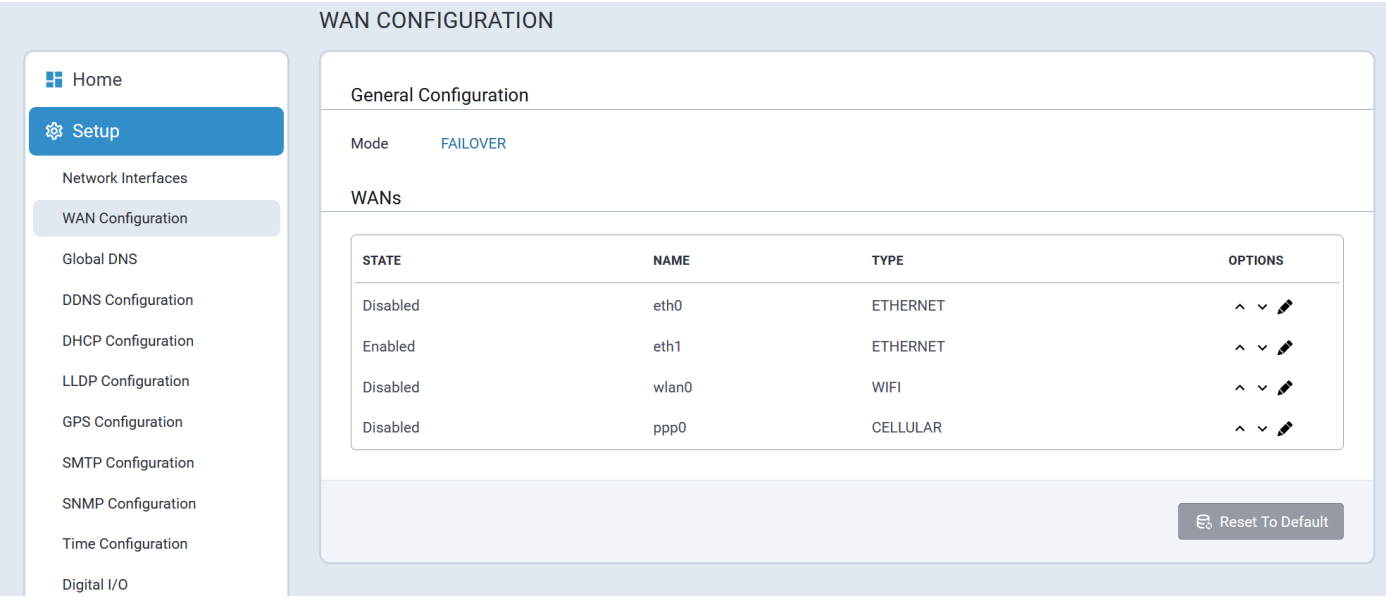
Used VLANs

NAME	TAGGED	DIRECTION	IP MODE	IP ADDRESS	OPTIONS
vlan.100		WAN IPv4	DHCP Client		
vlan.31	✓	LAN IPv4	Static	192.168.3.1/24	

Submit | Cancel

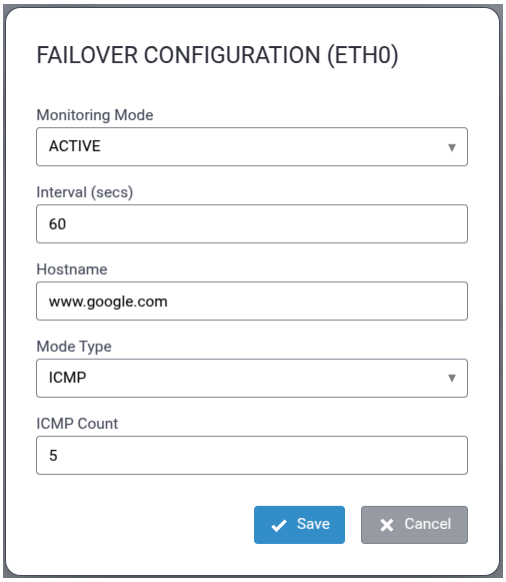
WAN Configuration

All WAN interfaces on the device should be configured with the desired priorities for WAN failover.



Each WAN interface can be configured to Active or Passive failover with a timeout interval to trigger failover to the next prioritized WAN interface.

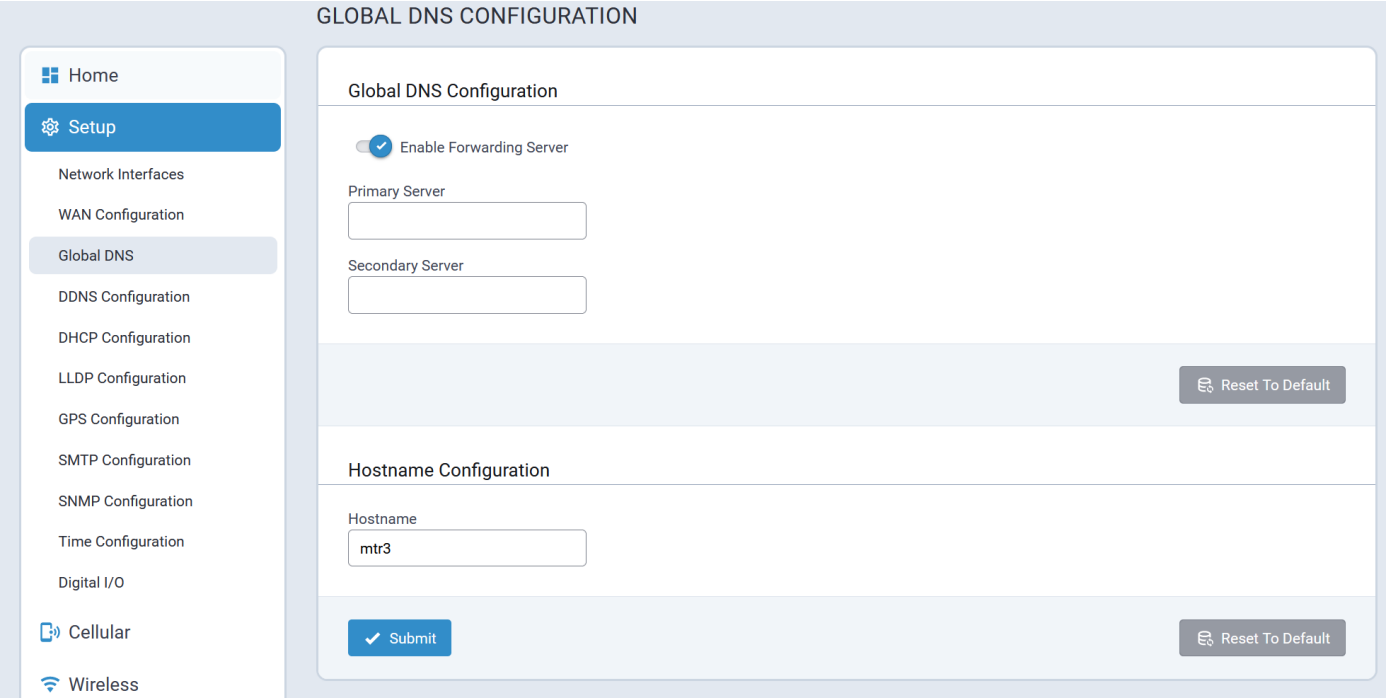
Hostname must be specified and **Mode Type** selected (for example: ICMP for ping, TCP for an actual TCP connect attempt) to verify connectivity. The number of failures is controlled by the ICMP Count setting.



Global DNS Configuration

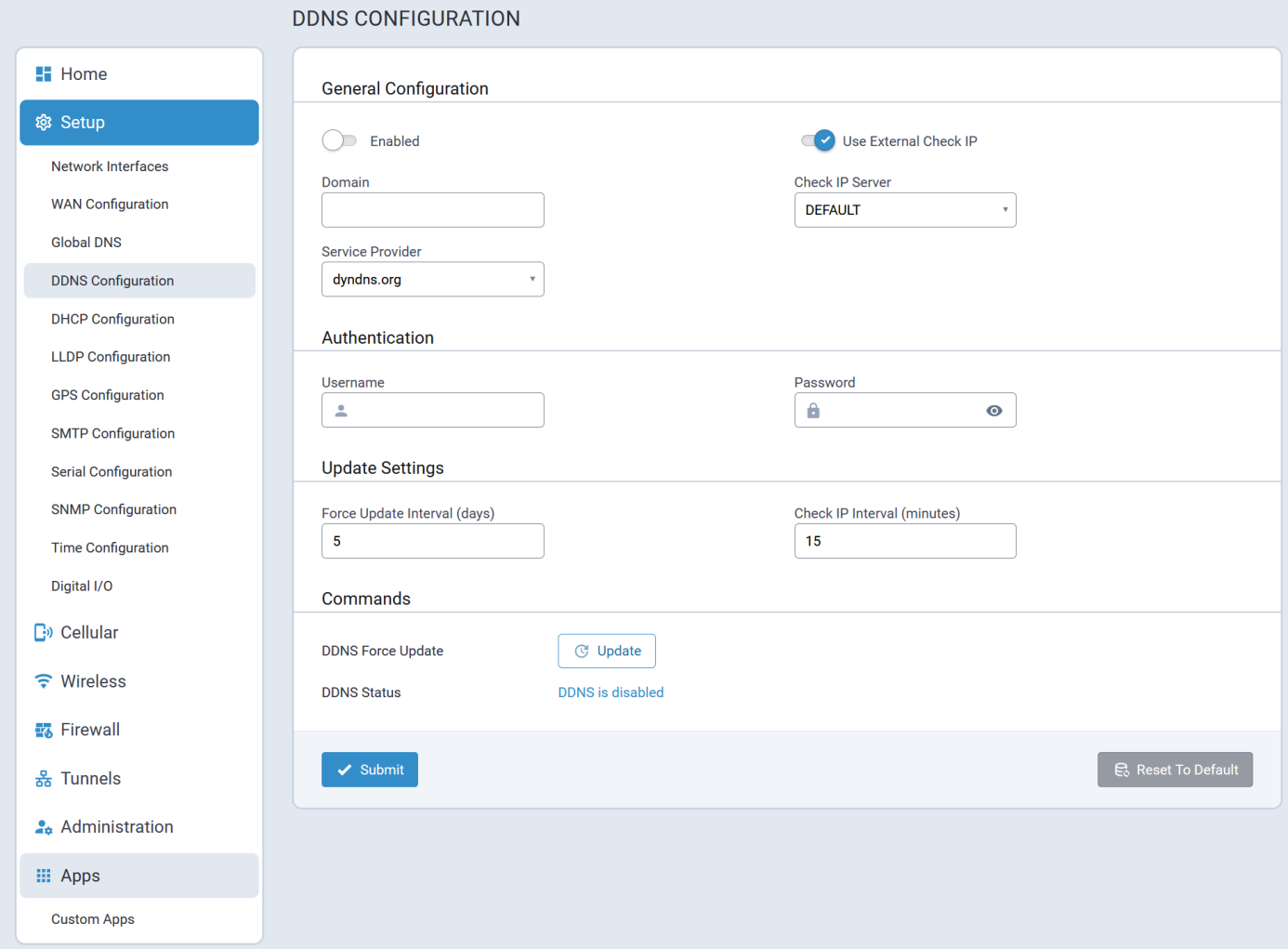
Global DNS Configuration is a means to override the DNS settings obtained for the active WAN interface.

For example, if cellular is the active WAN interface and the DNS settings are obtained from the provider, enabling this feature overrides the DNS server settings obtained from the provider with the settings that are specified here.



DDNS Configuration

Default DDNS configuration settings are illustrated here:



DDNS Configuration Fields

Refer to the following table for complete information about each DDNS configuration field:

Input Field	Default Value	Validation Rules
Enabled	FALSE	True, False
Domain	empty	A valid domain name
Custom Service		
Server	empty	A valid server name or IP Address, max length is 250 characters
Path	/nic/update?hostname=%h	Max length is 256 characters. Must start with "/". Allowed characters: a-z, A-Z, 0-9, and special characters: ~@#%&_-=+.:/?
Port	443	1 - 65535
Use SSL	TRUE	True, False

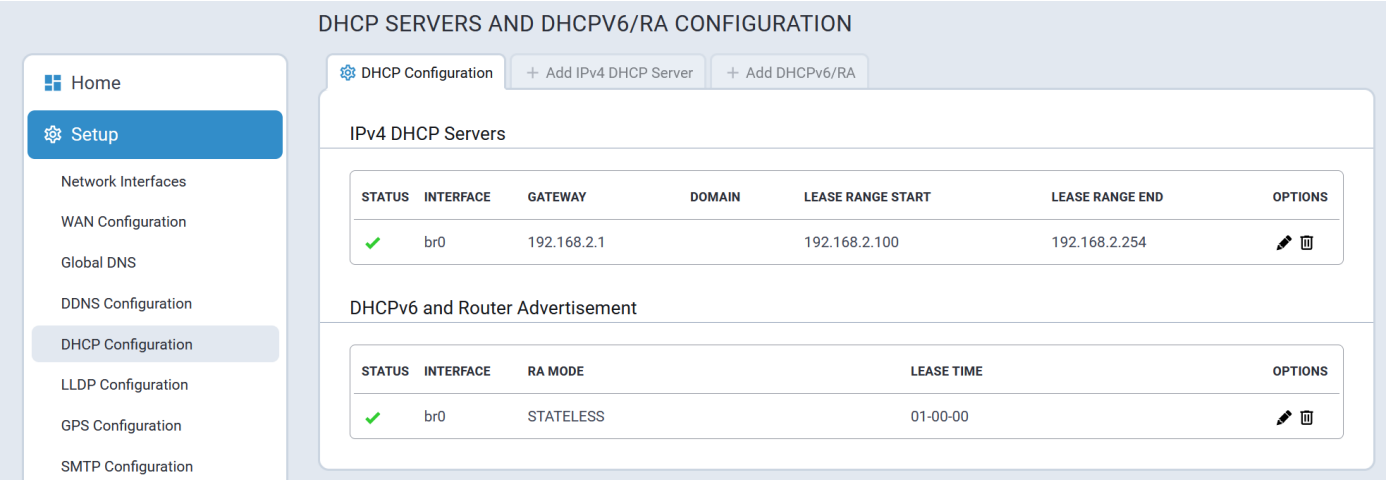
Input Field	Default Value	Validation Rules
Use External Check IP	TRUE	True, False
Custom Check IP Server		
Check IP Server	checkip.dyndns.org	A valid server name or IP Address, max length is 250 characters
Path	/	Max length is 256 characters. Must start with "/". Allowed characters: a-z, A-Z, 0-9, and special characters: ~@#%&_-=+.:/?
Port	80	1 - 65535
Use SSL	FALSE	True, False
Username	empty	Max length is 128 characters
Password	empty	The value must be from 6 to 64 characters long
Force Update Interval	5	Range is 1 - 30 days
Check IP Interval	15	Range is 1 - 14400 minutes (10 days)

DHCP Configuration

The system supports the configuration of IPv4 and IPv6 DHCP servers for all network interfaces that are configured as LAN, including new user-created VLAN interfaces.

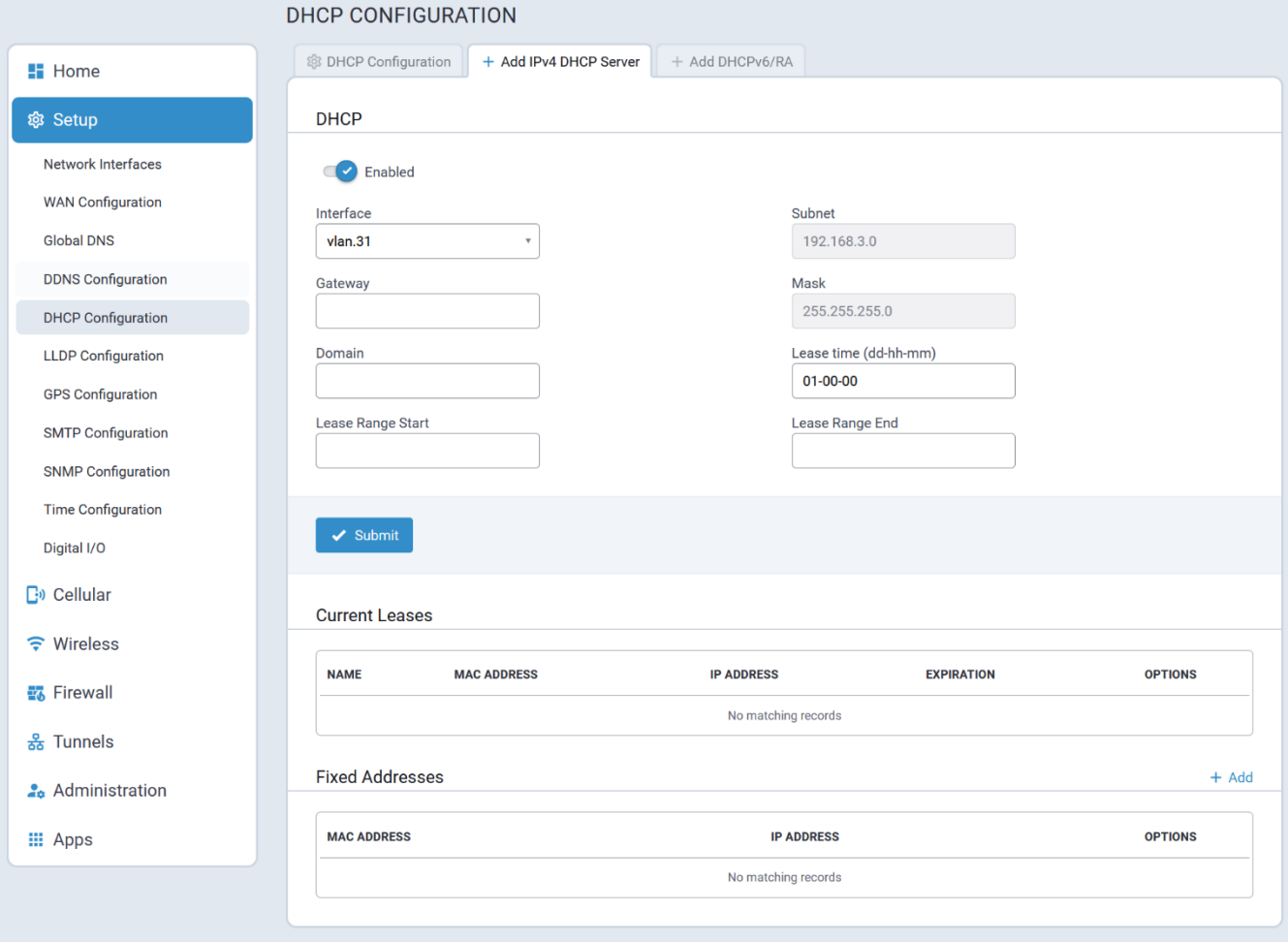
DHCP Configuration Tab

Default DHCP configuration settings are illustrated here:



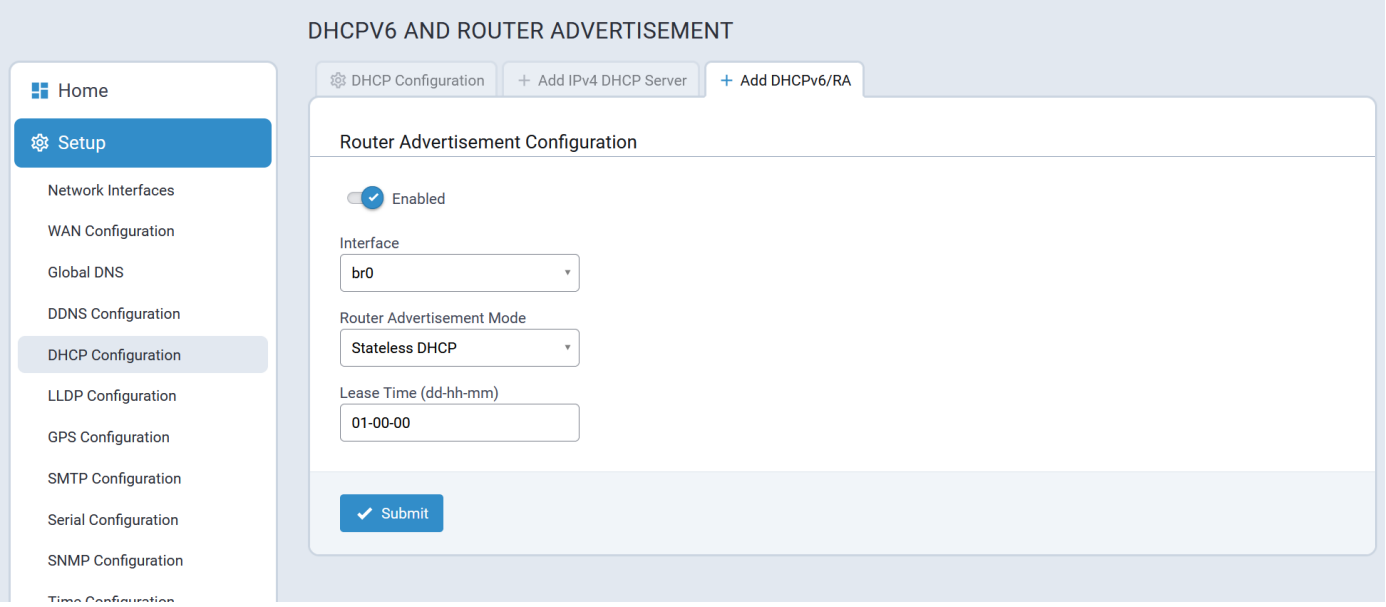
Add IPv4 DHCP Server Tab

Typical DHCP configuration information for a new VLAN interface is illustrated here:



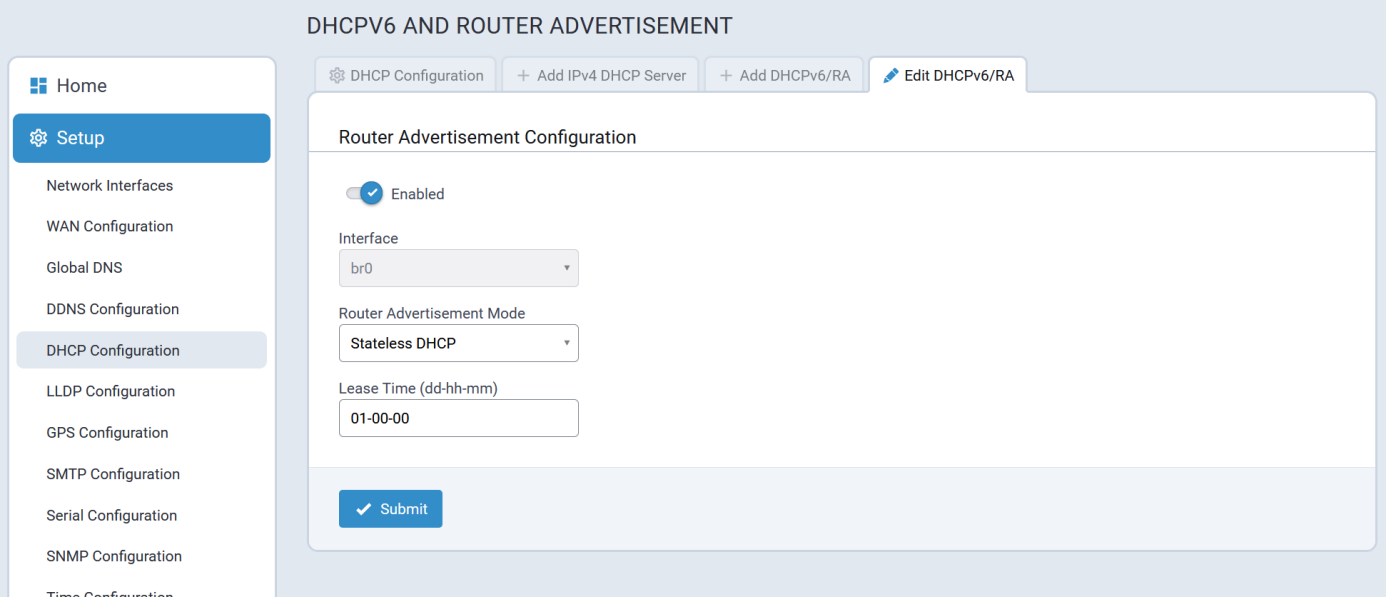
Add DHCPv6/RA Tab

Typical DHCPv6 Router Advertisement (RA) configuration information is illustrated here:



Edit DHCPv6/RA Tab

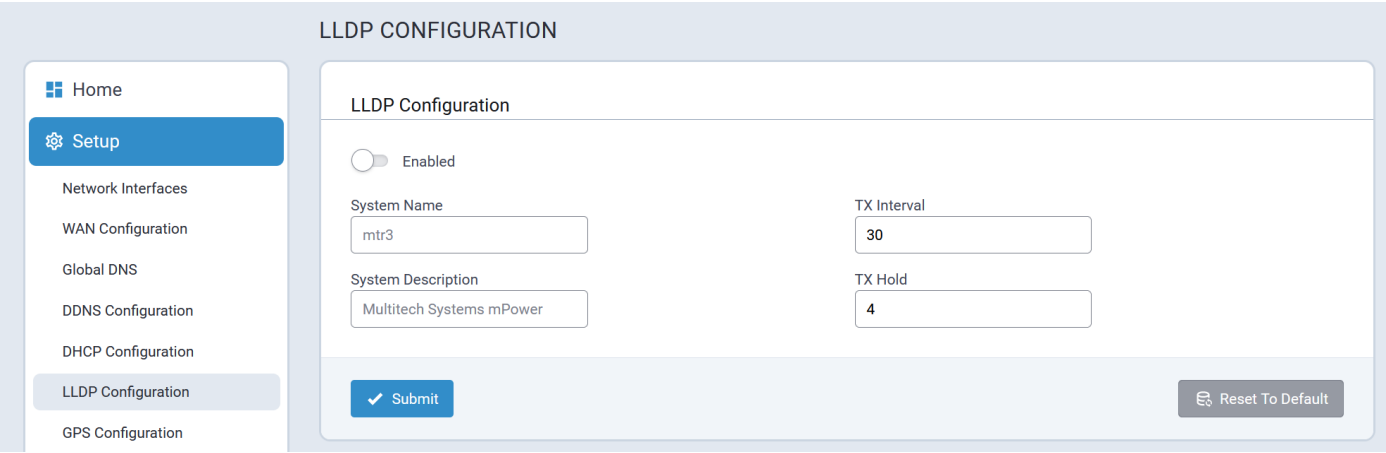
Information for an existing DHCPv6/RA configuration is modified on this tab. Typical RA settings are illustrated here:



LLDP Configuration

Note: LLDP (Link Layer Discovery Protocol) is supported only on the eth0 interface.

Typical LLDP configuration settings for eth0 are illustrated here:

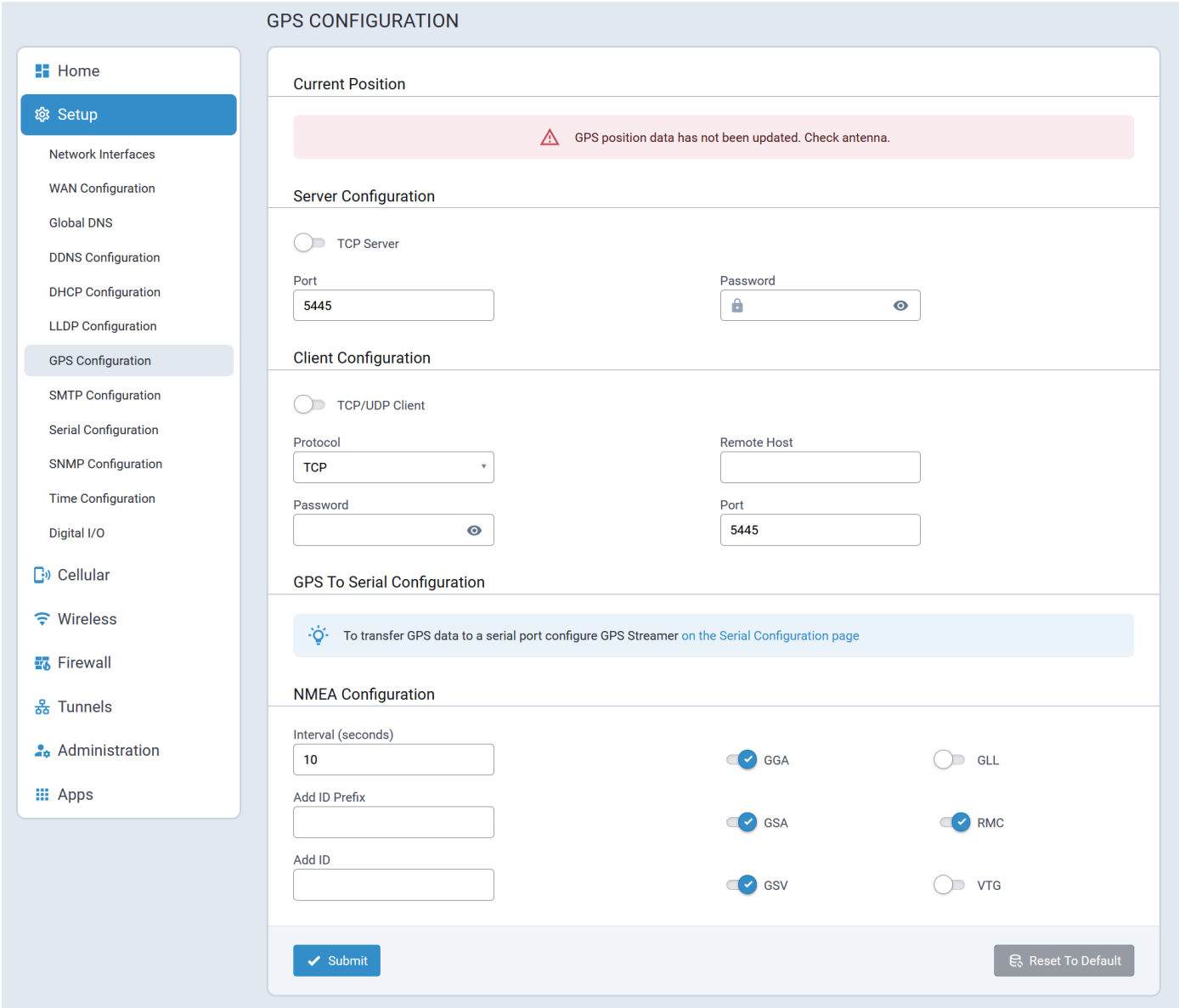


GPS Configuration

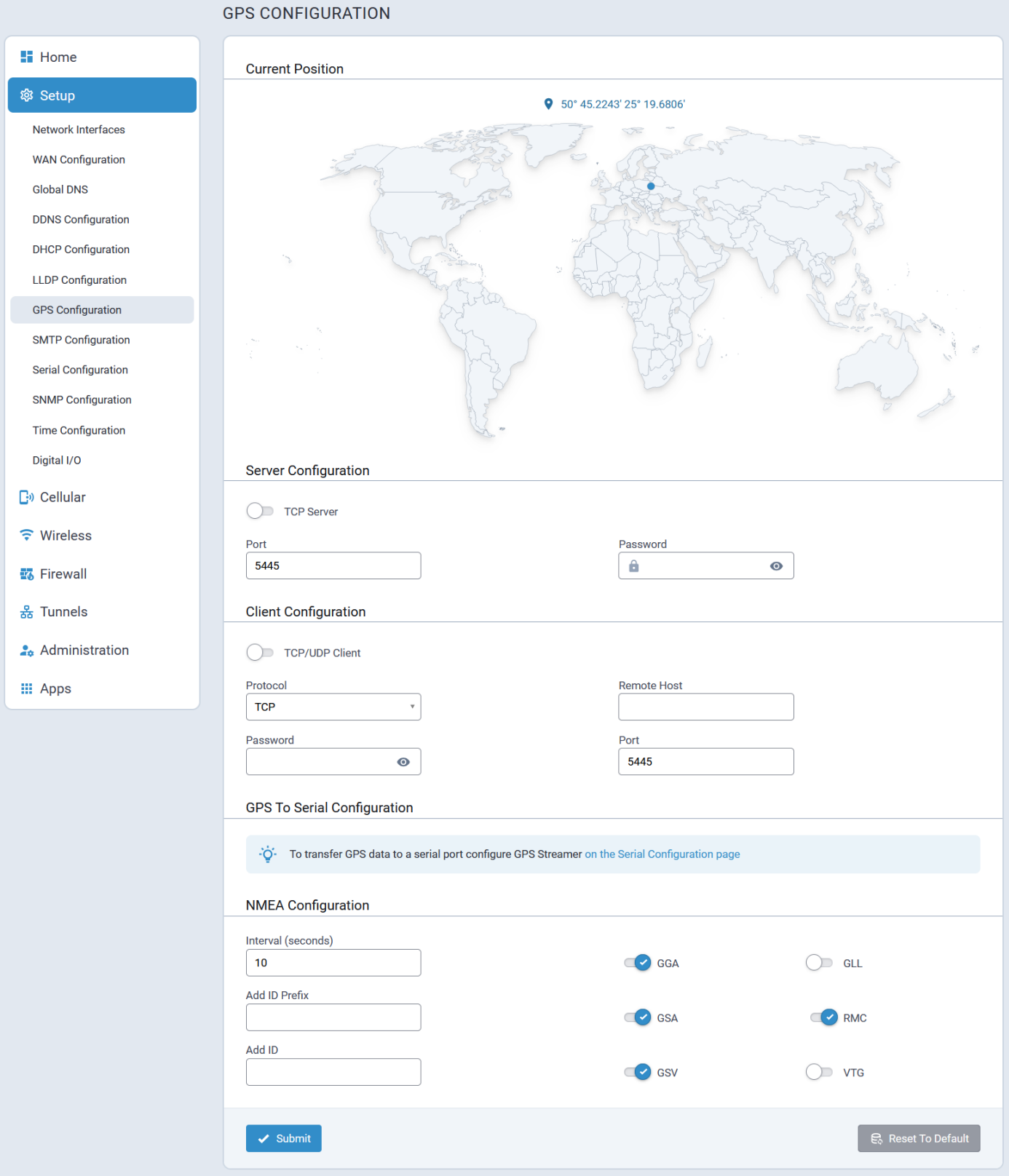
rCell 300 IoT Router hardware uses the radio modem to receive GPS data.

The system configuring a TCP Server sends NMEA strings to a client, and/or a TCP/UDP Client to stream NMEA strings to a server application.

To transfer GPS data to a serial port, configure GPS Streamer parameters on the Serial Configuration page.



Once GPS Position data have been updated, the current position is shown on map as illustrated here:

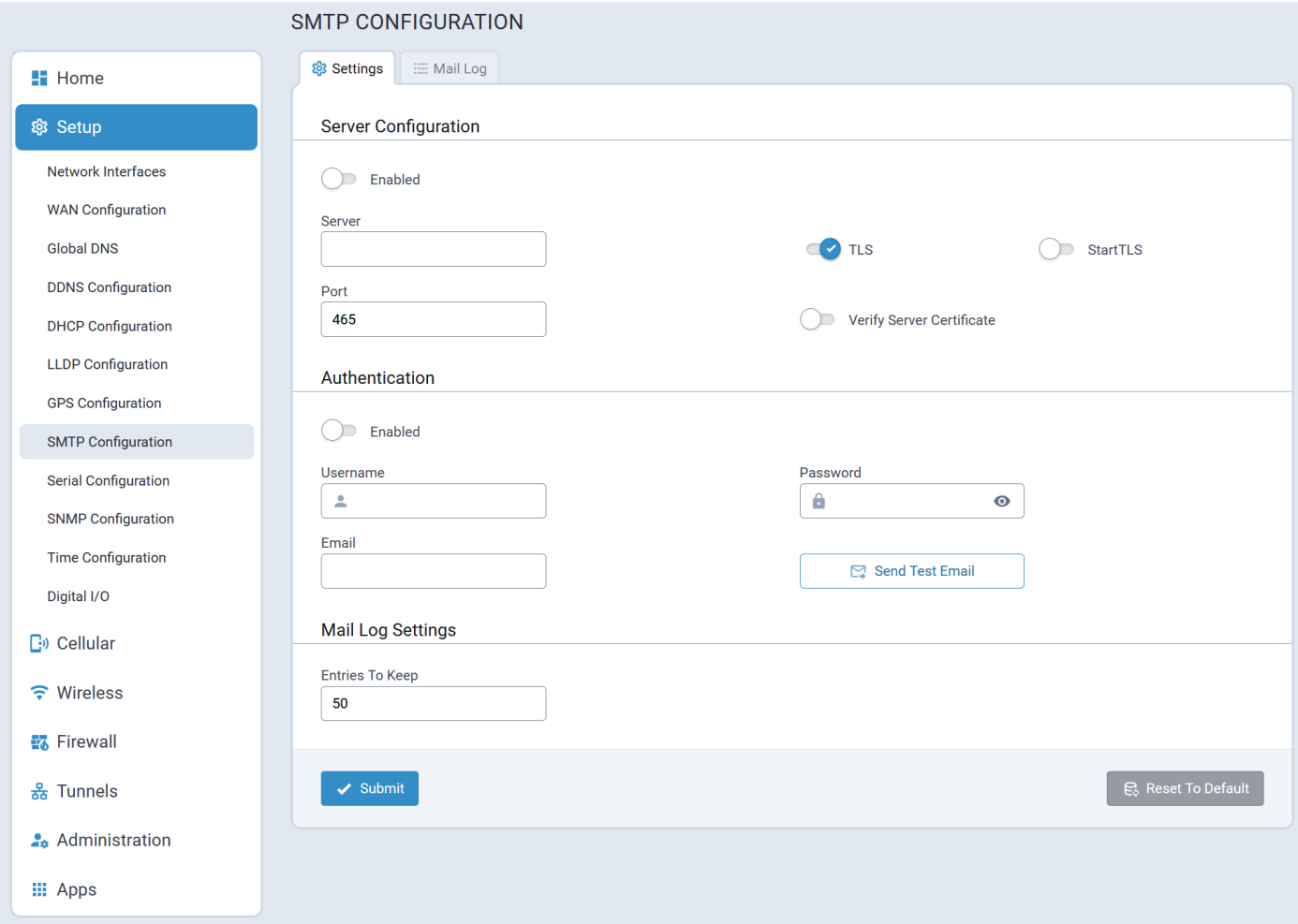

GPS CONFIGURATION
Home
Setup
Network Interfaces
WAN Configuration
Global DNS
DDNS Configuration
DHCP Configuration
LLDP Configuration
GPS Configuration
SMTP Configuration
Serial Configuration
SNMP Configuration
Time Configuration
Digital I/O
Cellular
Wireless
Firewall
Tunnels
Administration
Apps
Current Position
50° 45.2243' 25° 19.6806'
Server Configuration
TCP Server
Port
5445
Password
Client Configuration
TCP/UDP Client
Protocol
TCP
Remote Host
Password
Port
5445
GPS To Serial Configuration
To transfer GPS data to a serial port configure GPS Streamer on the Serial Configuration page
NMEA Configuration
Interval (seconds)
10
Add ID Prefix
Add ID
GGA
GLL
GSA
RMC
GSV
VTG
Submit
Reset To Default

SMTP Configuration

The SMTP client can be configured to send notifications via email to a configured server.

Settings Tab

Typical SMTP configuration values are illustrated here:

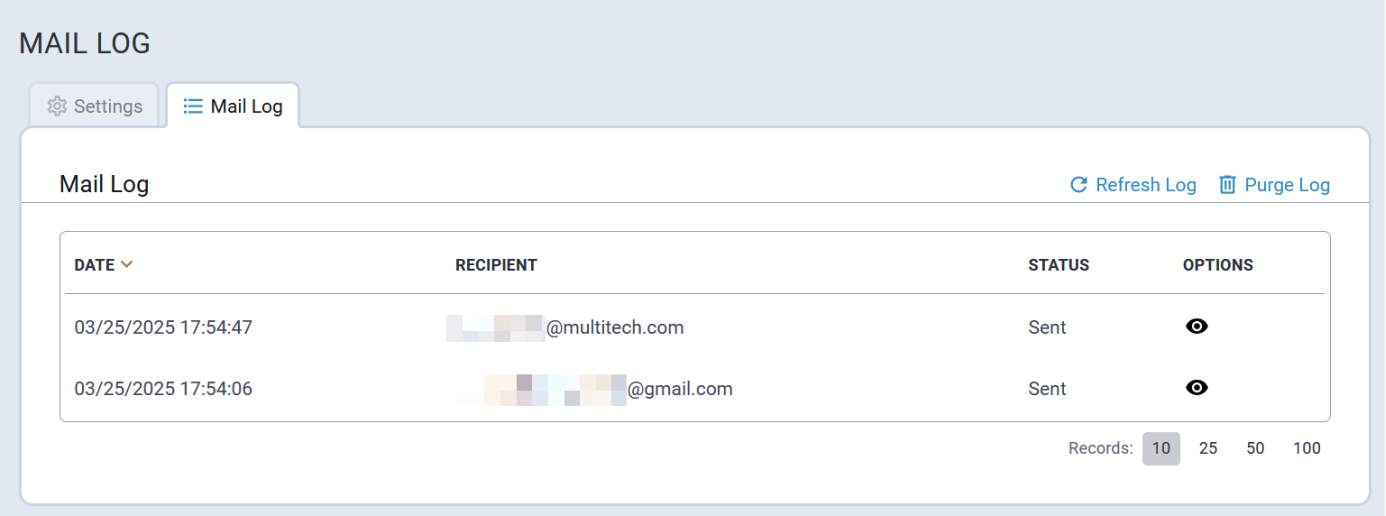


Mail Log Tab

The Mail Log displays:

- Messages that are queued for sending
- Deferred messages
- Sent messages

For example, the Mail Log illustrated here shows two messages have been sent.



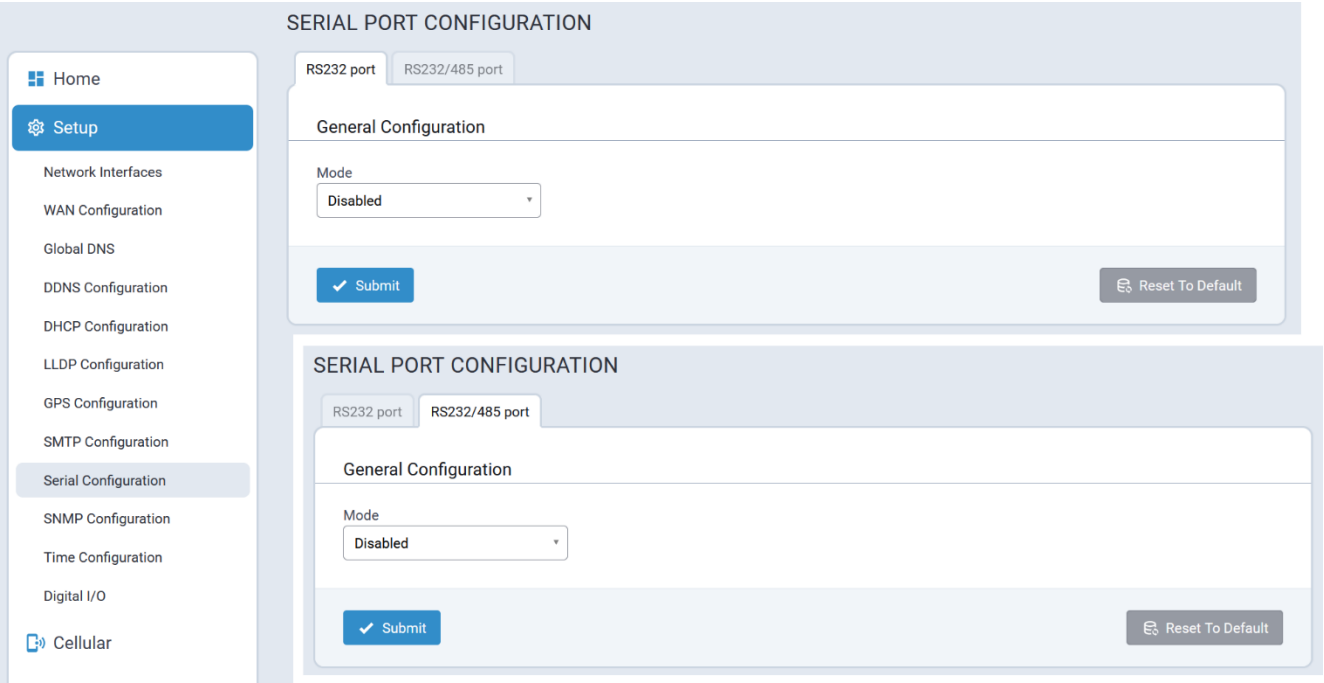
To view the details of a message, click on the icon in the OPTIONS column that corresponds with the desired message. A dialog similar to the following will include the message details.

Serial Configuration

As illustrated below, rCell 300 is equipped with two serial ports:

- RS232
- RS232/485 GPIO

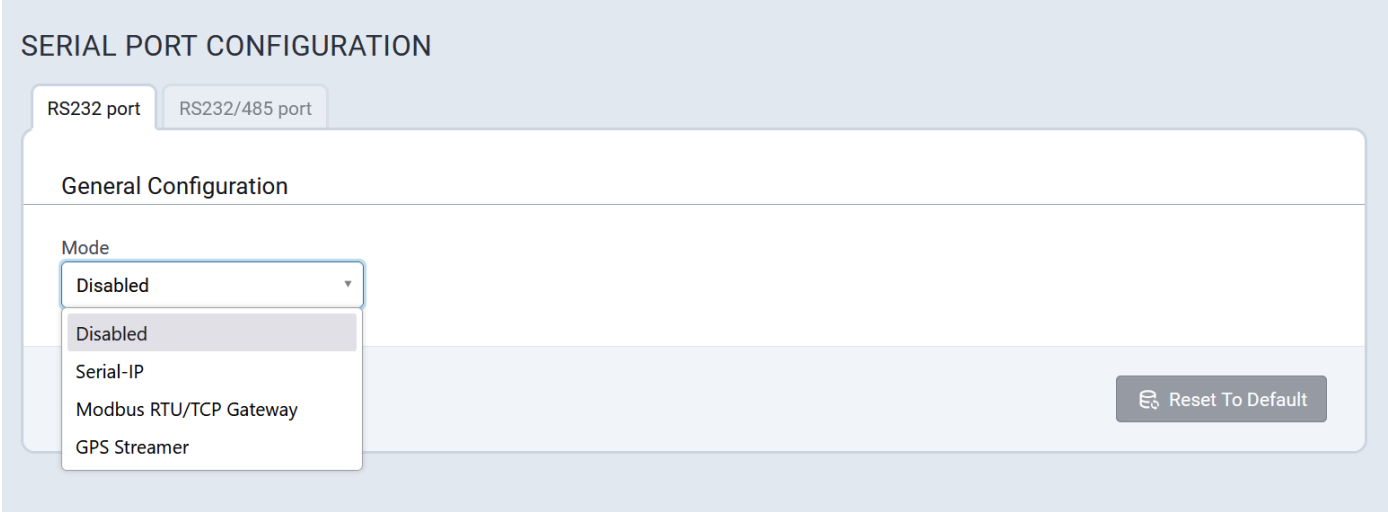
Note: By default, both serial ports are disabled.



Each serial port may be configured for one of the following modes:

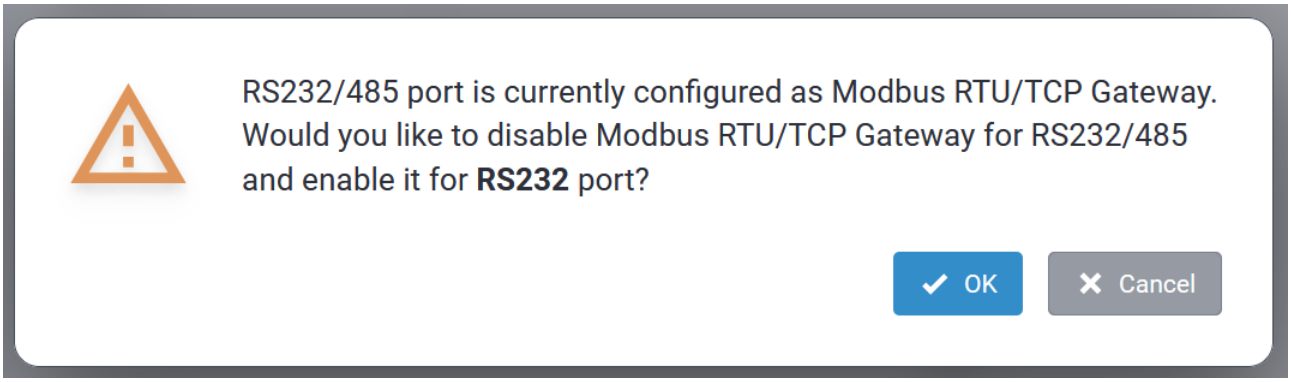
- Serial-IP
- Modbus RTU/TCP Gateway
- GPS Streamer

To configure either serial port, expand the **Mode** pull-down list and select the desired mode as illustrated here:



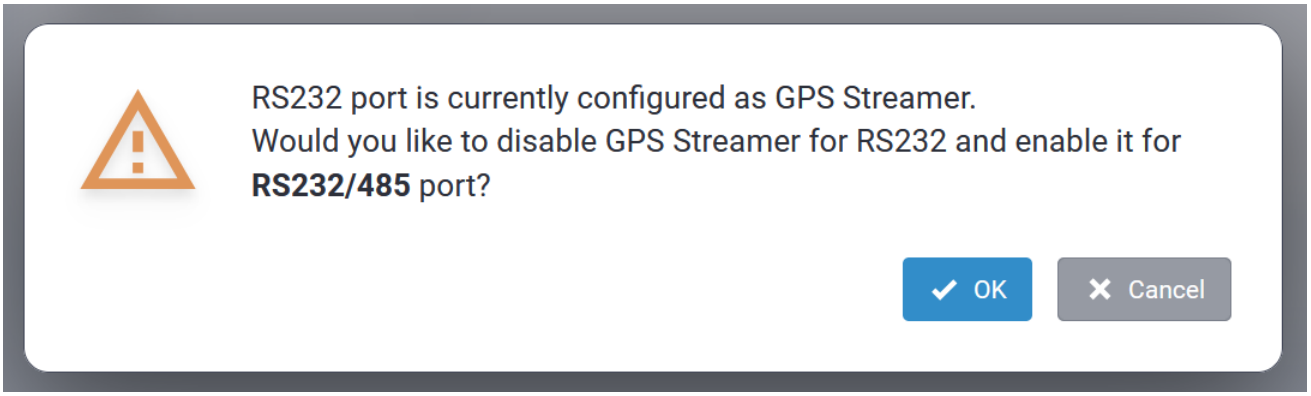
Note: Only one port may be configured for Modbus RTU/TCP Gateway at a time.

The system shows a warning message on submit when a user tries to configure a port as Modbus RTU/TCP Gateway while the other port is already configured as Modbus RTU/TCP Gateway.



Note: Only one port may be configured for GPS Streamer at a time.

The system shows a warning message on submit when a user tries to configure a port as GPS Streamer while the other port is already configured as GPS Streamer.



Note: The RS232 and RS232/485 ports may be configured for Serial-IP simultaneously.

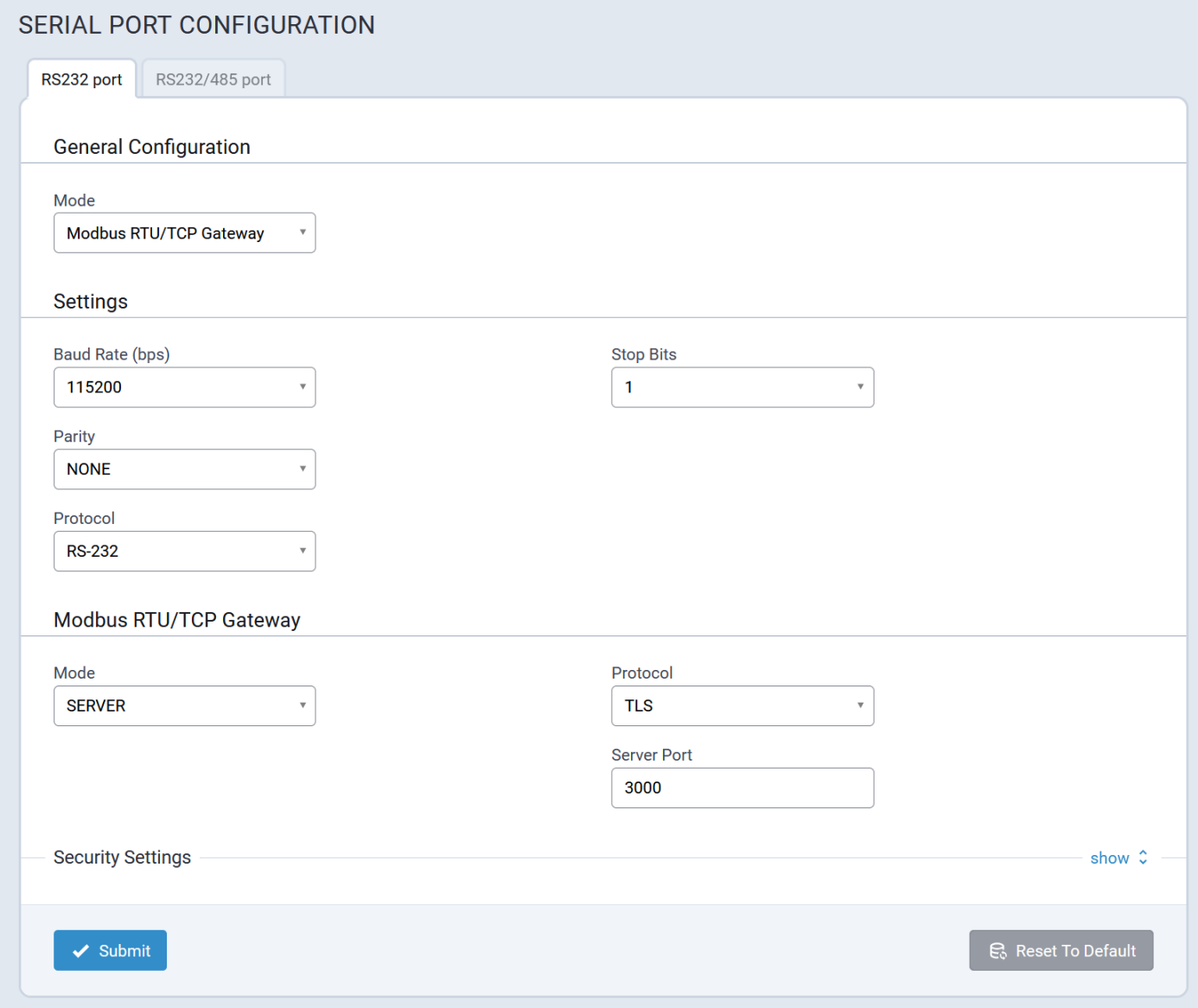
Modbus RTU/TCP Gateway

The system allows users to configure one of the serial ports as Modbus RTU/TCP Gateway.

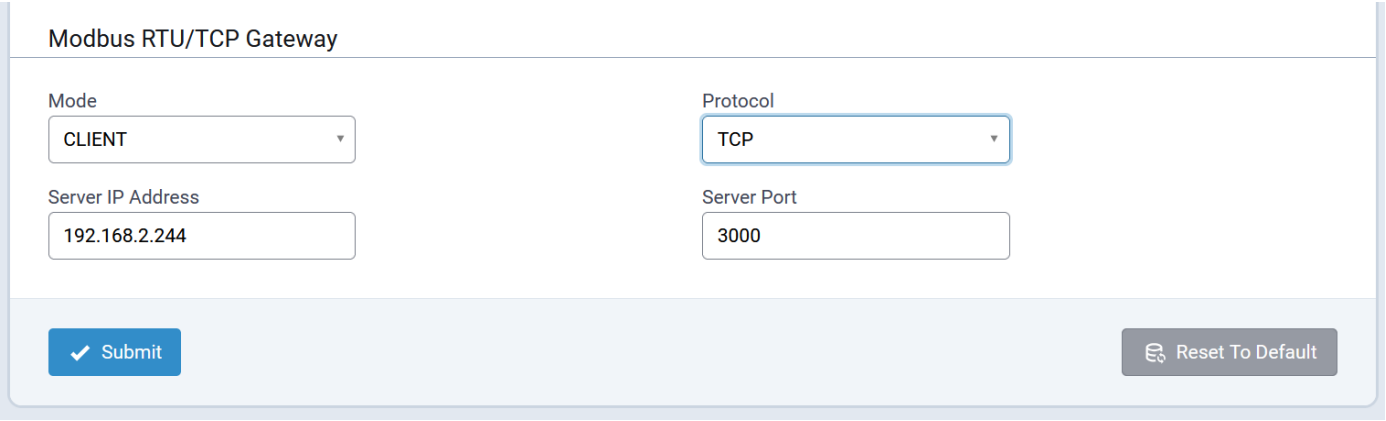
Compared to the previous mPower releases, the Modbus RTU/TCP Gateway feature has not been changed from the user requirements and general functionality standpoint.

Modbus RTU slave is connected to the Serial Port and a remote Modbus TCP Master. Modbus Gateway application works as a translator between Modbus RTU (slave) and Modbus-TCP (master) devices. When the Modbus Gateway is enabled, its application runs in the system. The application works as a translator converting between the Modbus-TCP and Modbus RTU protocols. The Modbus Gateway passes data between an RTU connected to the serial port and a Modbus TCP remote client/server.

An example of the Modbus RTU/TCP Gateway Settings for the server is illustrated here:



An example of the Modbus RTU/TCP Gateway Settings for the client is illustrated here:



GPS Streamer Mode

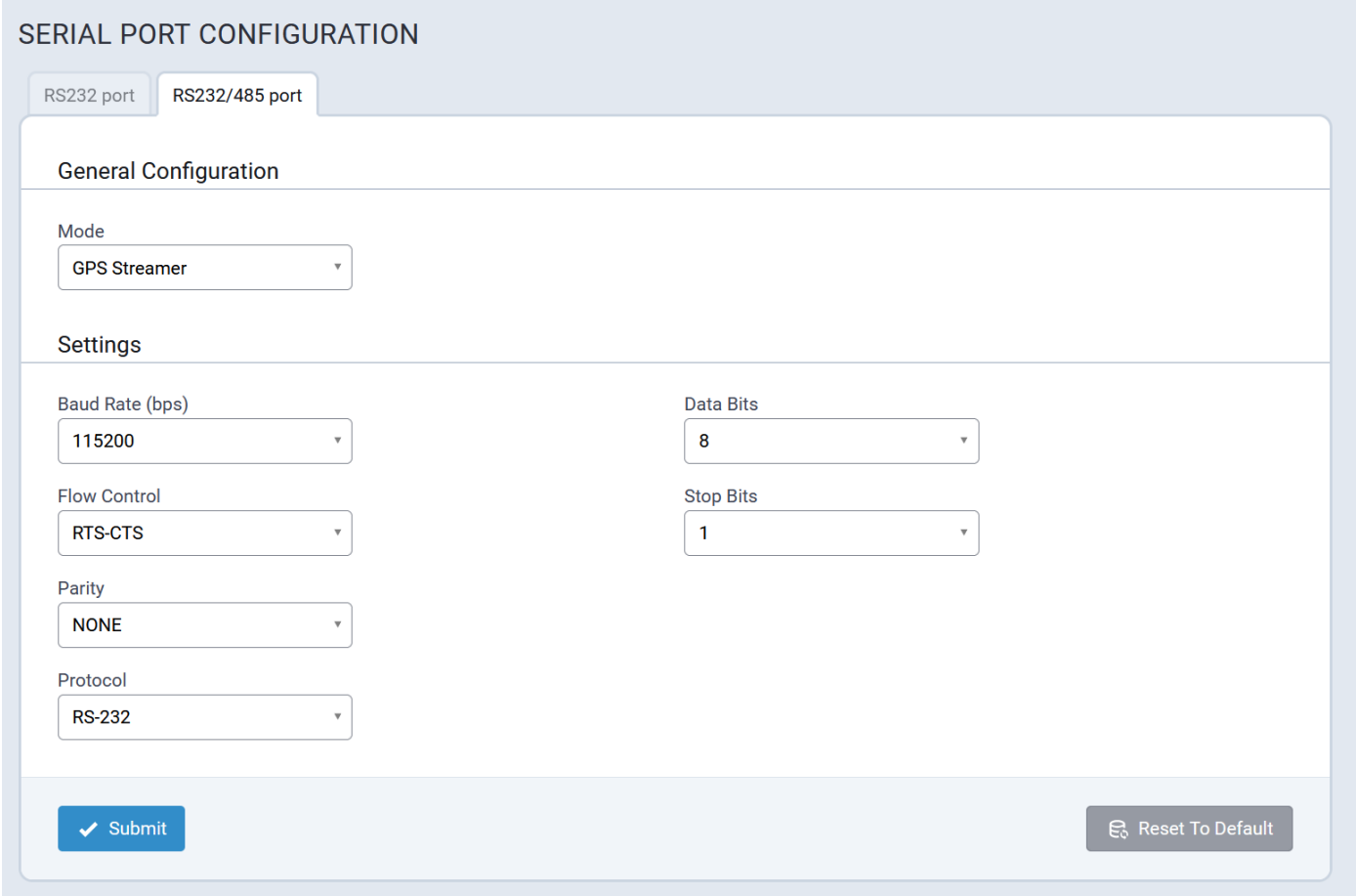
rCell 300 has two serial ports, and GPS Streamer to a serial port configuration is a part of the Serial Port functionality. The system allows configuring any of the Serial ports as a GPS streamer, but only one Serial port can be configured as a GPS streamer at a time.

Important: GPS Streamer supports data transfer when the baud rate is between 4800 and 115200 bps. If the baud rate is not in this range, the data transfer will not be performed.

The GPS Configuration page allows configuring what **NMEA messages** must be sent as GPS data, the **interval**, **prefix and ID**. The GPS configuration page does not have settings for configuring Serial port. However, it has the **GPS To Serial Configuration** section that refers to the Serial Configuration page.

To configure GPS data transfer to a serial port, on the GPS Configuration page configure the NMEA messages, interval, add prefix and ID if required, and then go to the Serial Configuration page to configure a serial port as a GPS Streamer.

An example of the GPS Streamer Configuration for the server is illustrated here:



Logging

Serial-IP

The system uses a separate file **/var/log/messages/ser-cli.log** for logging Serial-IP events.

RS232 and RS232/485 serial ports can be configured and operate as Serial-IP simultaneously, and logs are added to the same event log file: ser-cli.log. RS232 uses the source "**serial0**" in the logged messages; RS232/485 uses the source "**serial1**" in the logs.

```
root@mtr3:/var/log# tail -f /var/log/ser-cli.log
15:18:17:520|ERROR| serial0|pid:11478|Error connection: No route to host
15:18:17:520|ERROR| serial0|pid:11478|Failed to connect to the primary server address
15:18:17:521|ERROR| serial0|pid:11478|Error connection: No route to host
15:18:17:521|ERROR| serial0|pid:11478|Failed to connect to the secondary server address
15:18:17:521|INFO| serial0|pid:11478|Sleeping for 5 seconds...
15:18:17:760|ERROR| serial1|pid:11487|Error connection: No route to host
15:18:17:760|ERROR| serial1|pid:11487|Failed to connect to the primary server address
15:18:17:760|ERROR| serial1|pid:11487|Error connection: No route to host
15:18:17:761|ERROR| serial1|pid:11487|Failed to connect to the secondary server address
15:18:17:761|INFO| serial1|pid:11487|Sleeping for 5 seconds...
15:18:22:521|INFO| serial0|pid:11478|Reinitiating the client...
15:18:22:522|INFO| serial0|pid:11478|Start trigger is Always-on.Trying to connect to a remote server
15:18:22:524|INFO| serial0|pid:11478|Cellular Link is up
15:18:22:524|INFO| serial0|pid:11478|Trying to connect: 192.168.2.242, port 3000
15:18:22:761|INFO| serial1|pid:11487|Reinitiating the client...
15:18:22:762|INFO| serial1|pid:11487|Start trigger is Always-on.Trying to connect to a remote server
15:18:22:764|INFO| serial1|pid:11487|Cellular Link is up
15:18:22:764|INFO| serial1|pid:11487|Trying to connect: 192.168.2.13, port 3001
```

Modbus RTU/TCP Gateway

The system uses a separate file to store logs when a serial port is configured as Modbus RTU/TCP Gateway: **/var/log/messages/modbus-gateway.log**.

GPS Streamer

The **mtsgpsstreamer** services logs events to **/var/log/messages**

```
admin@mtr3:/var/log$ tail -f /var/log/messages | grep mtsgpsstreamer
2024-08-13T12:41:23.088886+00:00 mtr3 mtsgpsstreamer: serial:$GPGSV,3,1,12,01,,,52,03,56,111,33,04,87,336,39,06,43,295,53,1*5C#015#012$GPGSV,3,2,12,09,49,248,30
,11,09,322,51,26,14,074,46,28,04,033,50,1*6A#015#012$GPGSV,3,3,12,31,30,052,55,02,04,171,,07,07,192,,19,12,261,,1*64#015#012$GPGGA,124123.00,5045.215060,N,02519
.681548,E,1,07,0.7,218.9,M,33.0,M,,*64#015#012$GPRMC,124123.00,A,5045.215060,N,02519.681548,E,0.0,,130824,4.6,E,A,V*65#015#012$GPGSA,A,3,03,04,06,09,11,26,31,,,
,,,1.0,0.7,0.7,1*20#015
2024-08-13T12:41:24.089339+00:00 mtr3 mtsgpsstreamer: serial:$GPGSV,3,1,12,01,,,52,03,56,111,33,04,87,336,39,06,43,295,53,1*5C#015#012$GPGSV,3,2,12,11,09,322,51
,26,14,074,46,28,04,033,50,31,30,052,55,1*65#015#012$GPGSV,3,3,12,02,04,171,,07,07,192,,09,49,248,,19,12,261,,1*68#015#012$GPGGA,124124.00,5045.215077,N,02519.6
81558,E,1,07,0.7,218.9,M,33.0,M,,*64#015#012$GPRMC,124124.00,A,5045.215077,N,02519.681558,E,0.0,,130824,4.6,E,A,V*65#015#012$GPGSA,A,3,03,04,06,09,11,26,31,,,,,
,1.0,0.7,0.7,1*20#015
2024-08-13T12:41:25.089886+00:00 mtr3 mtsgpsstreamer: serial:$GPGSV,3,1,12,01,,,52,03,56,111,33,04,87,336,38,06,43,295,53,1*5D#015#012$GPGSV,3,2,12,09,49,248,32
,11,09,322,52,26,14,074,45,28,04,033,49,1*60#015#012$GPGSV,3,3,12,31,30,052,53,02,04,171,,07,07,192,,19,12,261,,1*62#015#012$GPGGA,124125.00,5045.215089,N,02519
.681566,E,1,07,0.7,218.9,M,33.0,M,,*69#015#012$GPRMC,124125.00,A,5045.215089,N,02519.681566,E,0.0,,130824,4.6,E,A,V*68#015#012$GPGSA,A,3,03,04,06,09,11,26,31,,,
,,,1.0,0.7,0.7,1*20#015
2024-08-13T12:41:26.090360+00:00 mtr3 mtsgpsstreamer: serial:$GPGSV,3,1,12,01,,,52,03,56,111,34,04,87,336,37,06,43,295,53,1*55#015#012$GPGSV,3,2,12,09,49,248,32
,11,09,322,51,26,14,074,45,28,04,033,49,1*63#015#012$GPGSV,3,3,12,31,30,052,55,02,04,171,,07,07,192,,19,12,261,,1*64#015#012$GPGGA,124126.00,5045.215099,N,02519
.681572,E,1,07,0.7,218.9,M,33.0,M,,*6E#015#012$GPRMC,124126.00,A,5045.215099,N,02519.681572,E,0.0,,130824,4.6,E,A,V*6F#015#012$GPGSA,A,3,03,04,06,09,11,26,31,,,
,,,1.0,0.7,0.7,1*20#015
2024-08-13T12:41:27.090832+00:00 mtr3 mtsgpsstreamer: serial:$GPGSV,3,1,12,01,,,52,03,56,111,34,04,87,336,36,06,43,295,53,1*54#015#012$GPGSV,3,2,12,09,49,248,32
```

Serial Port Statistics

The Serial Port Statistics page provides information regarding data transferred through the serial port (RX/TX), DCD status (if available), and corresponding logs (if available). The information that is shown on the Statistics page is stored in **/api/stats/serial**.

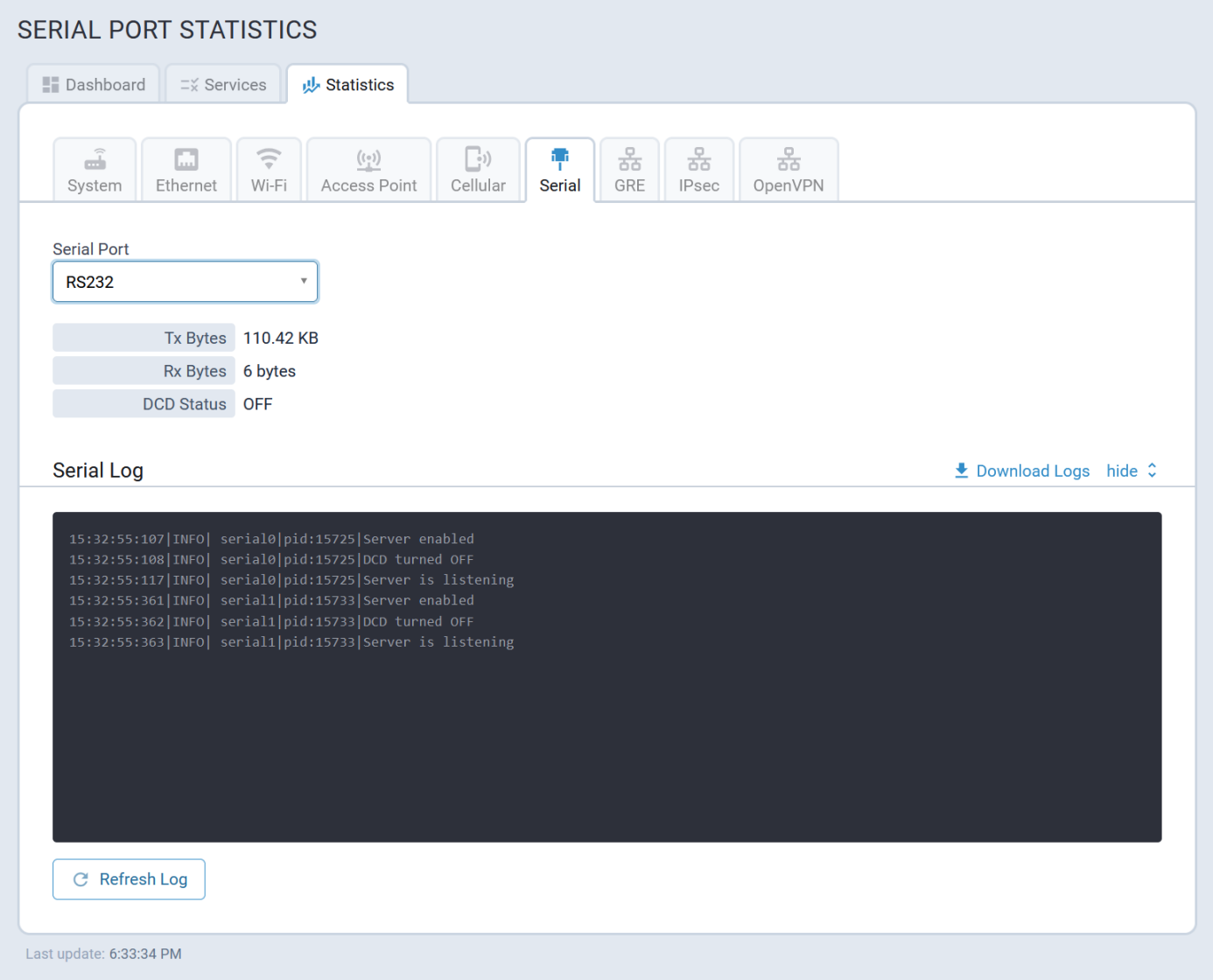
The Serial Port dropdown allows switching between available Serial Ports to see corresponding statistics and logs.

The system stores the serial port data transfer statistics (RX/TX) when a user reconfigures the serial port and restarts corresponding services.

The system does not preserve the serial port data transfer statistics (RX/TX) over a reboot. When the system reboots, the serial port statistics are reset.

DCD Status is not available for RS232/485 port; and the DCD Status is hidden on the Serial Port Statistics page.

The Serial Log pane shows the device logs that correspond to the current mode of the selected serial port.

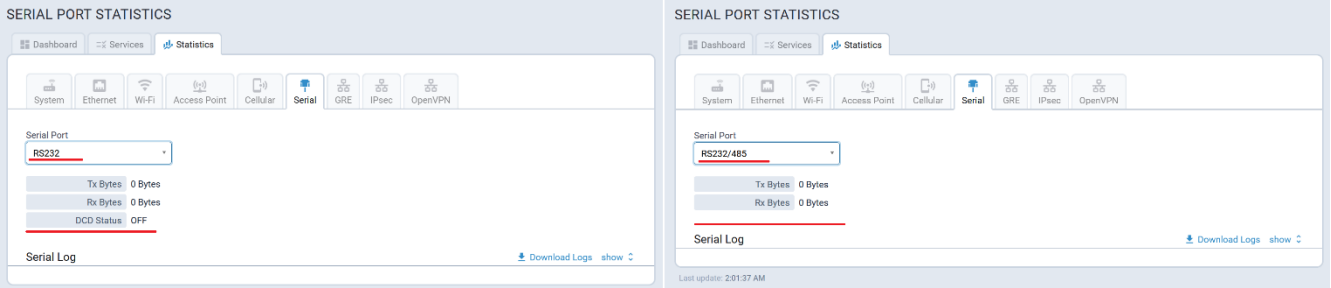


DCD (Data Carrier Detect) Status

Data Carrier Detect (DCD) is a control signal that is present inside an RS-232 serial communications cable and that goes between a computer and another device. The DCD is available in RS-232 serial port only, and is not available in RS232/485 serial port.

DCD Status is available on the Serial Port Statistics page:

- When RS232/485 is selected, the DCD Status is not shown.
- When RS232 is selected, the DCD status is available.



The DCD status depends on the serial port mode configuration.

DCD Status when the serial port is disabled.

DCD Status is always OFF when RS232 is disabled.

DCD Status when the serial port is configured as GPS Streamer.

When RS232 is configured as GPS Streamer, the DCD Status changes to ON.

When you change the mode from GPS Streamer to Disabled, the DCD Status changes to OFF.

DCD Status when the serial port is configured as Serial-IP.

In the Server Mode, the DCD Status is OFF until a connection with a client is established.

In the Client Mode, the DCD Status is OFF if the connection with the server has not been established.

When the connection with the server is established, the DCD status depends on the Connection Activation setting.

If the Connection Activation is ALWAYS-ON, the DCD Status sets to ON immediately.

If the Connection Activation is On-Demand, DTR-ASSERT, or CR, the DCD Status is OFF unless the corresponding trigger is received.

If the Connection Activation is On-Demand, DTR-ASSERT, or CR, the DCD Status changes to ON as soon as the corresponding connection activation trigger is received.

DCD Status when the serial port is configured as Modbus RTU/TCP Gateway.

The DCD Status is always ON when the RS232 port is configured as Modbus RTU/TCP Gateway.

Example #1:

- The Serial Port is disabled. **DCD Status is OFF**.
- Enable **Modbus RTU/TCP Gateway**.
- Select **Submit**.
- Select **Save and Apply**.
- After saving and applying the changes the **DCD Status is ON**.
- Change the Modbus RTU/TCP Gateway to **Disabled**. Submit, Save and Apply the changes.
- After saving and applying the changes the **DCD Status is OFF**.

Example #2:

- The Serial Port is configured as **GPS Streamer**. **DCD Status is ON**.

- Enable **Modbus RTU/TCP Gateway**.
- Select **Submit**.
- Select **Save and Apply**.
- After saving and applying the changes the **DCD Status is ON**.
- Change the Modbus RTU/TCP Gateway to **Disabled**. Submit, Save and Apply the changes.
- After saving and applying the changes the **DCD Status is OFF**.

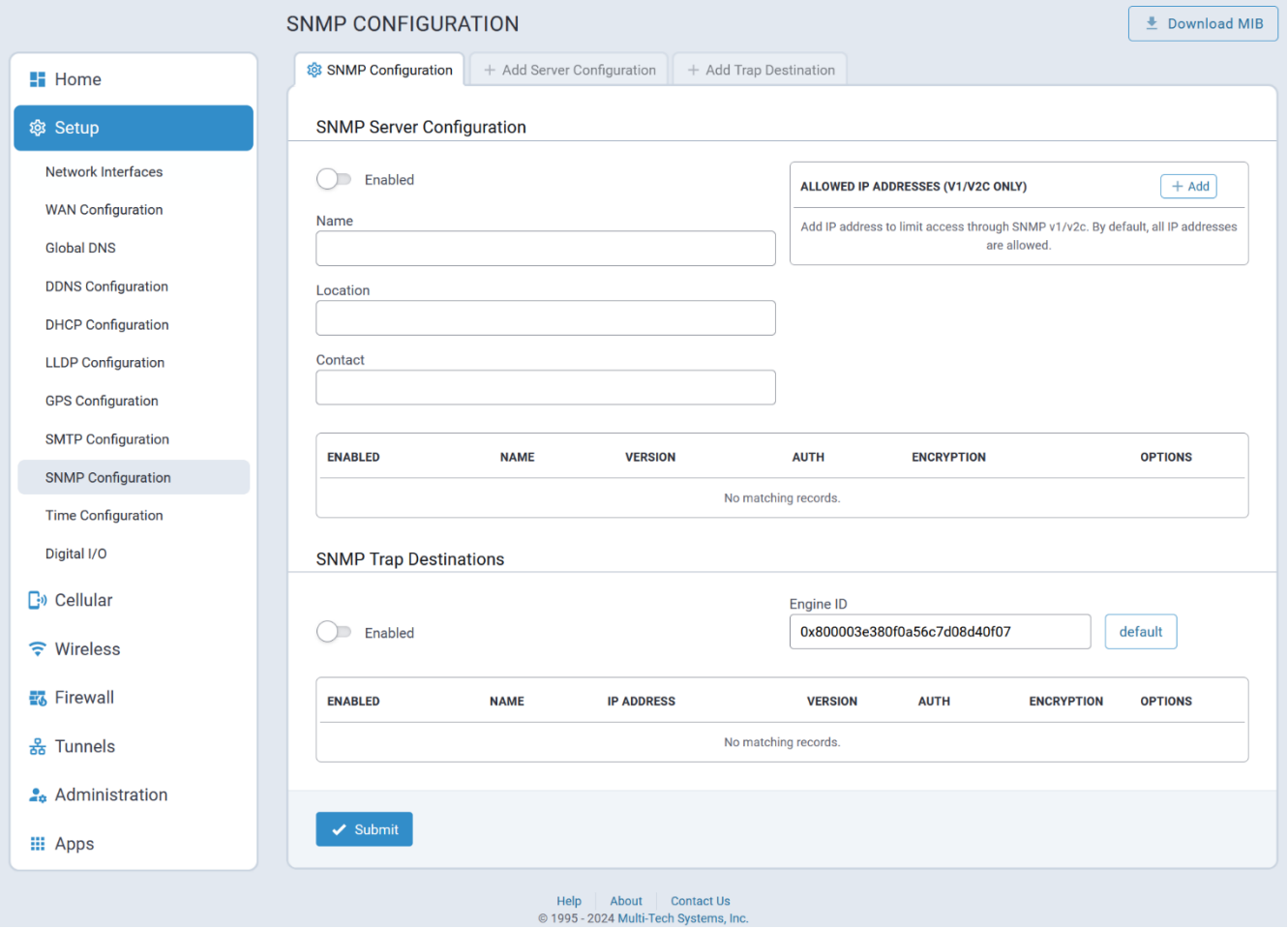
When you enable Modbus RTU/TCP Gateway mode, the system remembers the current DCD Status (it can be ON or OFF) and changes the DCD Status to ON. When you change the Modbus RTU/TCP Gateway mode to something else, the system restores the DCD Status to the value that was before the Modbus RTU/TCP Gateway was enabled.

Example #3:

- The Serial Port is configured as **Serial IP server**. **DCD Status is ON** (the connection with a client should be established).
- Change the Serial-IP mode to **Modbus RTU/TCP Gateway**.
- Select **Submit**.
- Select **Save and Apply**.
- After saving and applying the changes the **DCD Status is ON**.
- Change the Modbus RTU/TCP Gateway to **Disabled**. Submit, Save and Apply the changes.
- After saving and applying the changes the **DCD Status may be ON for a short moment, but then it changes to OFF**.

SNMP Configuration

The typical SNMP Configuration settings are illustrated here:



The following MIB information is compatible with RFC1213 for the rCell 300:

Note: By default, the values for **sysContact**, **sysName**, and **sysLocation** are empty. However, they may be configured by populating the **Contact**, **Name**, and **Location** fields (respectively) on the SNMP Configuration page.

Name	OID	OID Description	Comments
sysDescr	1.3.6.1.2.1.1.1	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.	The system returns the following information: ▪ Product ID ▪ Serial Number ▪ mPower Firmware Release ▪ vendor ID

Name	OID	OID Description	Comments
sysObjectID	1.3.6.1.2.1.1.2	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for identifying the type of box being managed. For example, if vendor "Flintstones, Inc." is assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to "Fred Router".	For rCell 300, the sysObjectID is **1.3.6.1.4.1.995.16.1.1.1**
sysUpTime	1.3.6.1.2.1.1.3	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.	The uptime of the snmp service.
sysContact	1.3.6.1.2.1.1.4	The textual identification of the contact person for this managed node, together with information on how to contact this person.	Empty by default. Configurable.
sysName	1.3.6.1.2.1.1.5	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	Empty by default. Configurable.
sysLocation	1.3.6.1.2.1.1.6	The physical location of this node ("telephone closet on 3rd floor").	Empty by default. Configurable.

Name	OID	OID Description	Comments
sysServices	1.3.6.1.2.1.1.7	A value which indicates the set of services that this entity primarily offers. The value is a sum which initially has the value zero (0). Then, for each layer, L, in the range 1 - 7, for which a node performs transactions, $2^{(L - 1)}$ is added to the sum. For example, a node which primarily performs routing functions has a value of ($2^{(3-1)}$), or 4. In contrast, a node which is a host offering application services has a calculated value of [$2^{(4-1)} + 2^{(7-1)}$], or 72. Note that in the context of the Internet suite of protocols, values should be calculated accordingly: ■ Layer 1: physical (repeaters) ■ Layer 2: datalink/subnetwork (bridges) ■ Layer 3: internet (IP gateways) ■ Layer 4: end-to-end (IP hosts) ■ Layer 7: applications (mail relays) For systems including OSI protocols, layers 5 and 6 may also be included.	mPower devices will return 76.

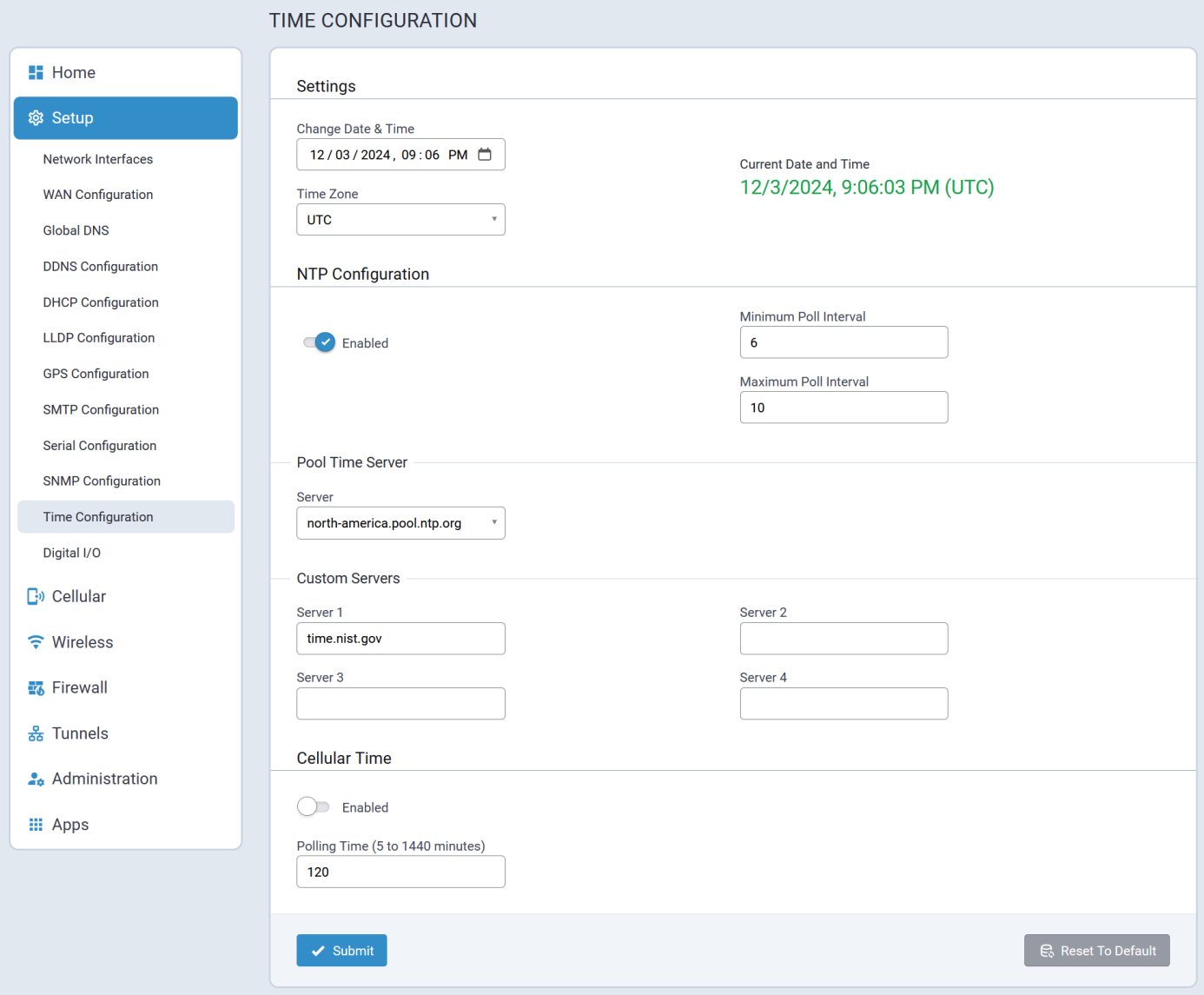
Time Configuration

The time synchronization feature sets up device time according to the specified system settings. Two different options are used to get the correct time:

- NTP Synchronization
- Cellular Synchronization

If using the Cellular Synchronization exclusively, verify that the device is successfully synchronizing time with the provider where the device has been placed. Some networks do not synchronize time on the Cellular radio correctly in some areas.

The typical Time Configuration settings are illustrated here:



Digital I/O

The system allows users to configure and control digital input and output pin states directly from the Web UI, API, and via SMS commands.

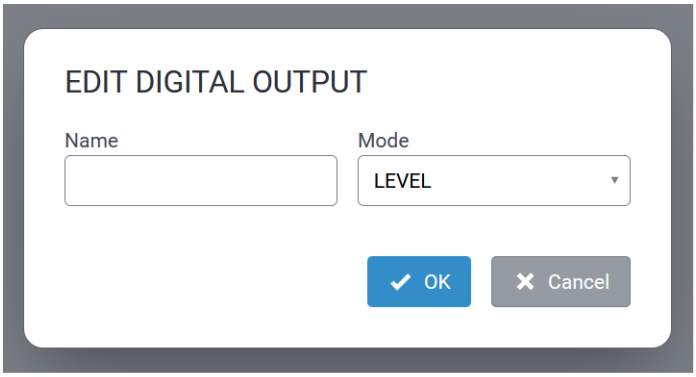
Digital I/O allows users to:

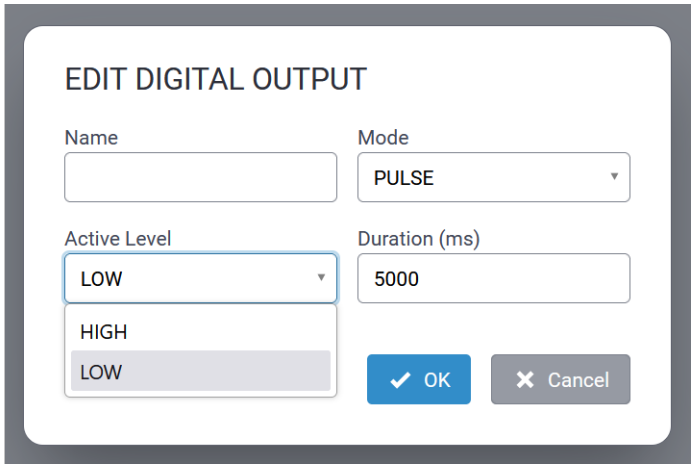
- Observe the actual state of the Input and Output pins in the STATE column.
- Set a user-friendly name for the Input and Output pins. This name may include alphanumeric characters only and has a maximum length of 10 characters.
- Change the mode of the output pin from Web UI.

By default, the mode is **LEVEL**, which means that the output pin stays at the same voltage level: LOW or HIGH. Select **Set High** or **Set Low** to change the current state.

The system allows configuring the output pin mode in the **PULSE** mode. In this mode, the system changes the current voltage level to another level (**Active Level**) for a user-configurable period of time (**Duration (ms)**) before returning to its original level.

- Valid values for **Active Level** are:
  - **LOW**
  - **HIGH**
- **Duration (ms)** is an integer value. Valid values are:
  - 1 (minimum)
  - 86400000 (maximum corresponding to 24 hours)

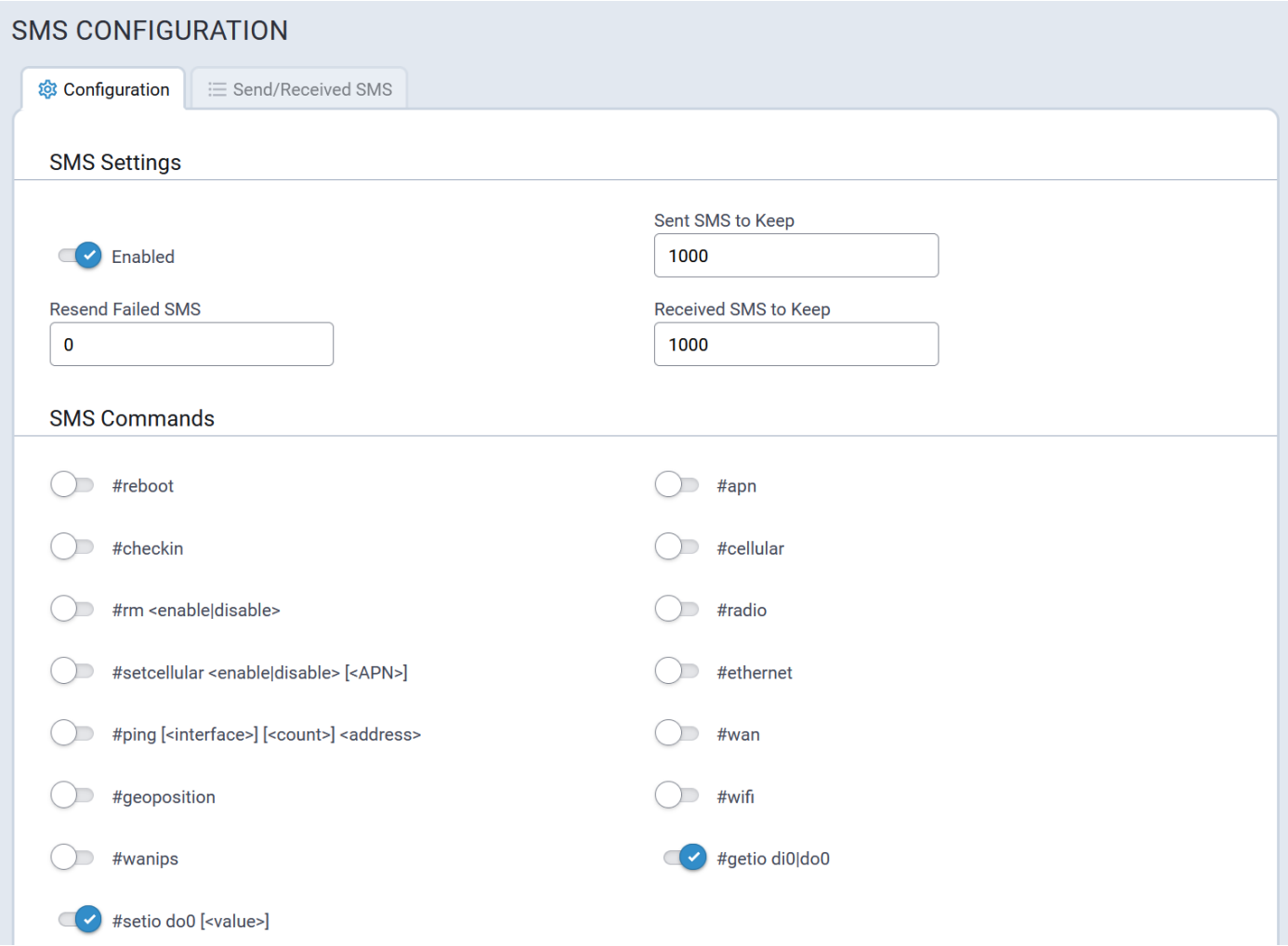




SMS Configuration and Commands

The following SMS commands are supported:

- #getio di0|do0
- #setio do0 [<value>]



#getio di0|do0

When the system receives the SMS command, it sends back the current state of the digital input (di0) or digital output (do0).

SMS Command	Custom PIN Name	SMS Response
#getio di0	Not set	*The state of the digital output is HIGH. YYYY-MM-DD HH:MM*
#getio di0	OUTPUTNAME	*The state of the digital output 'OUTPUTNAME' is HIGH. YYYY-MM-DD HH:MM*
#getio do0	Not set	*The state of the digital input is LOW. YYYY-MM-DD HH:MM*
#getio do0	INPUT0NAME	*The state of the digital input 'INPUT0NAME' is LOW. YYYY-MM-DD HH:MM*

#setio do0 [<value>]

The system allows users to change the current state of the output pin by sending a corresponding SMS command.

Level Mode

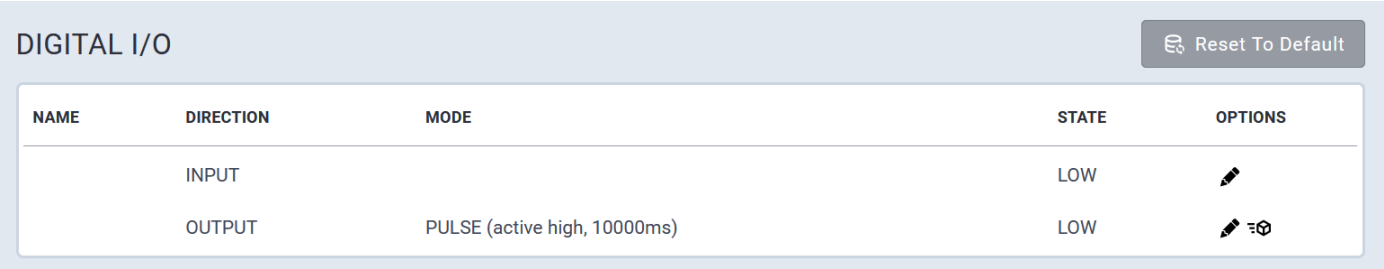
If the mode is **LEVEL**, add the value "0" to set the voltage level to LOW and "1" to set the voltage level to HIGH. If you do not add a value, the system will set the voltage to LOW.

Examples of SMS Command when the output pin mode is LEVEL:

Mode	SMS Command	SMS Response
LEVEL	#setio do0 **0**	The state of the digital output 'OUTPUTNAME' has been changed to **LOW**. YYYY-MM-DD HH:MM
LEVEL	#setio do0 **1**	The state of the digital output 'OUTPUTNAME' has been changed to **HIGH**. YYYY-MM-DD HH:MM
LEVEL	#setio do0	The state of the digital output 'OUTPUTNAME' has been changed to **LOW**. YYYY-MM-DD HH:MM

Pulse Mode

If the mode is **PULSE**, the received SMS command will make the system to change the state of the digital output based on the Pulse mode configuration. Do no add a value parameter, and the system will use the duration configured in the system. You can change the duration by setting a custom interval in the SMS command. To specify a custom duration of the pulse signal in ms, add an integer value. For example, the command #setio do0 15000 will send a signal to change the digital output state for 15 seconds.



Mode	SMS Command	SMS Response
PULSE	#setio do0	A signal to change the state of the digital output 'OUTPUTNAME' to HIGH for **10000ms** (PULSE mode) has been sent. YYYY-MM-DD HH:MM
PULSE	#setio do0 **15000**	A signal to change the state of the digital output 'OUTPUTNAME' to HIGH for **15000ms** (PULSE mode) has been sent. YYYY-MM-DD HH:MM

Cellular Menu

All Cellular features such as Cellular connection, cellular diagnostics, and SMS related functionality are configured within this menu.

rCell 300 is equipped with two SIM slots and supports DUAL SIM functionality.

The following cellular profiles are supported by the rCell 300:

- Provider Profiles
- SIM Profiles

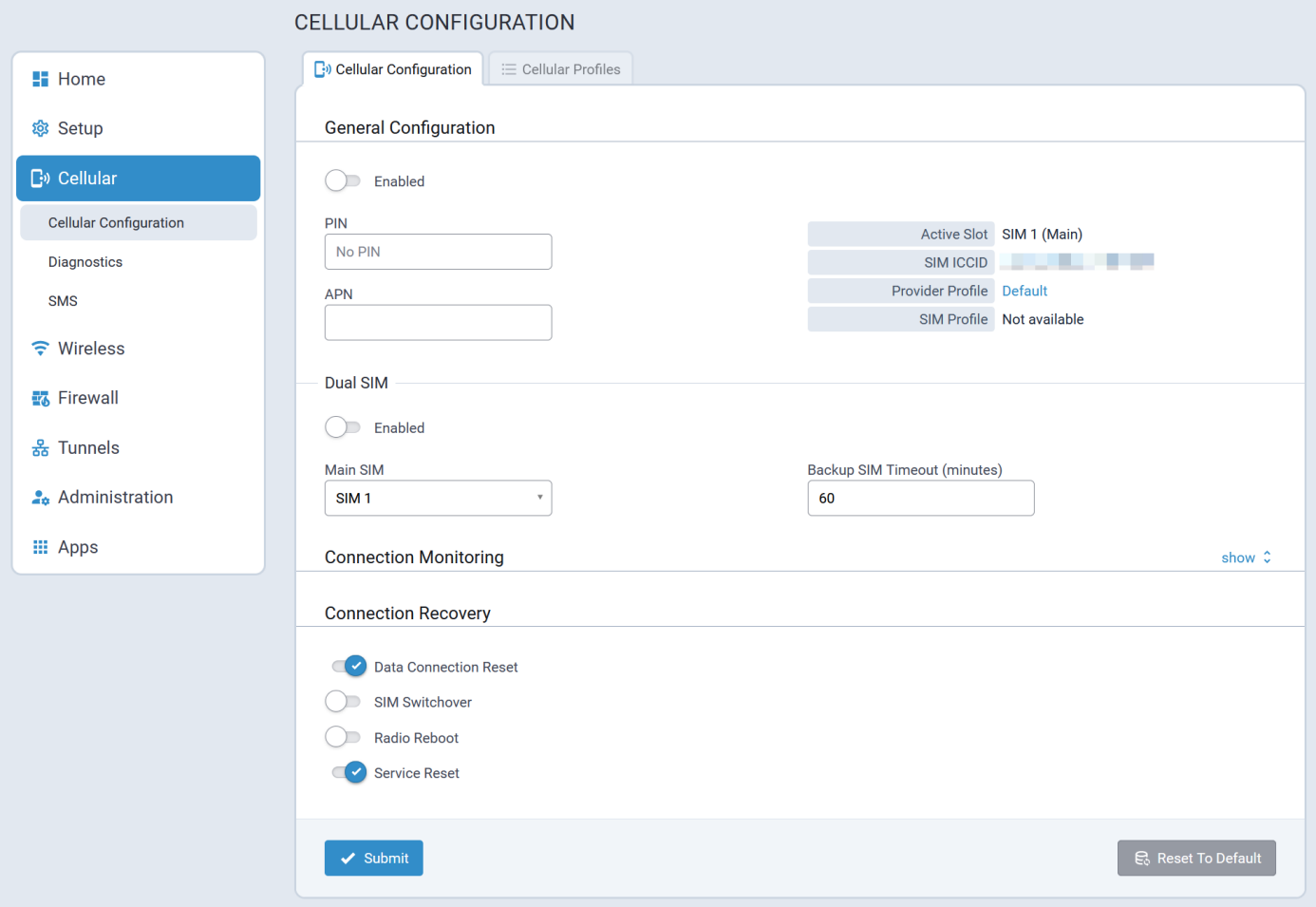
Cellular Configuration

Cellular Configuration page enabling or disabling the Cellular feature, set the main SIM slot, enable or disable the Dual SIM support, and configure the parameters that the system should monitor when Cellular connection is established and connection recovery options.

Cellular Configuration Tab

The Cellular Configuration tab includes settings that users must manage in order for their Cellular Connection to work.

Default cellular configuration settings are illustrated here:



General Configuration

The following General Configuration settings are configured in this area:

- Cellular operation is enabled/disabled.
- If the SIM is locked, the PIN must be configured for it.
- If the customer has a custom APN or is using an MVNO, they may be required to manually configure the APN.
- Dual SIM functionality is enabled/disabled.

Connection Monitoring

Connection Monitoring settings are configured in this area:

- Max Connection Failures – This setting, when enabled, tracks up to the maximum attempts before the additional connection recover activities begin.
- Keep Alive – This is essentially a Ping keep-alive to verify that the data connection is still established and data can be transmitted and received.
- Data Receive Monitor – This is a passive monitor. If the device has not received any packets over the Cellular connection in the configured window it will trigger connection re-establishment activities.

- Network Registration Timeout – If enabled, and the radio is unable to register with the Cellular network in the timeout specified, the Cellular recovery procedures are triggered.
- Roaming Network Timeout – If enabled, if the radio is connected in roaming it will attempt to reconnect to its home network per the timeout setting.
- Signal Quality Timeout – If the RSSI remains below the specified DBm for the timeout period, the recovery procedures are started in order to attempt to find better signal.

Connection Recovery

Connection Recovery settings are enabled/disabled in this area:

- Data Connection Reset – If it is determined that the data connection is not passing traffic the connection will be re-established.
- SIM Switchover – This enables a failover behavior to the other SIM during connection recover after a certain number of attempts or time has elapsed since the last successful data connection.
- Radio Reboot – If this is enabled, after all back-off timers have been exercised, and if the data connection has not been re-established successfully during that time, the radio is rebooted.
- Service Reset – Per algorithm, the entire set of processes, counters, etc. Will be restarted at a point if Cellular data connectivity cannot be re-established.

Connection Monitoring

hide

Max Connection Failures

Enabled

Max Attempts: 8

Keep Alive

ICMP/TCP Check

Interval (seconds): 60

Hostname:

Keep Alive Type: ICMP

ICMP Count: 4

Packet Size (Bytes): 56

Data Receive Monitor

Enabled

Window (minutes): 60

Network Registration Reset Timeout

Enabled

Timeout (minutes): 2

Roaming Network Timeout

Enabled

Timeout (minutes): 2

Signal Quality Timeout

Enabled

Minimum RSSI (dBm): -113

Timeout (minutes): 10

Connection Recovery

Data Connection Reset

SIM Switchover

Radio Reboot

Service Reset

Submit

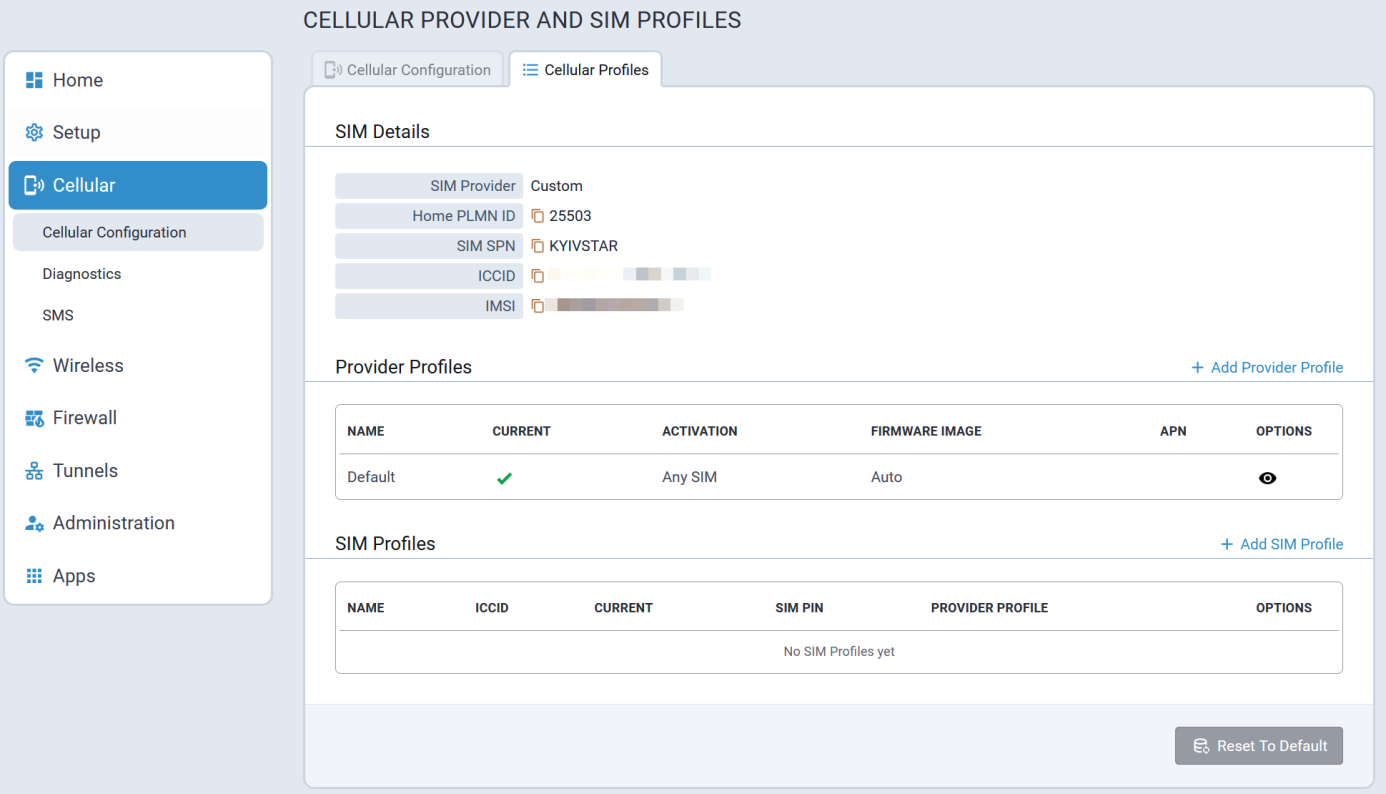
Reset To Default

Cellular Profiles Tab

The system supports the configuration of Cellular Provider Profiles and SIM profiles.

The system applies a corresponding Provider Profile and SIM profile based on the settings configured by users.

Default Cellular Profile configuration settings are illustrated here:

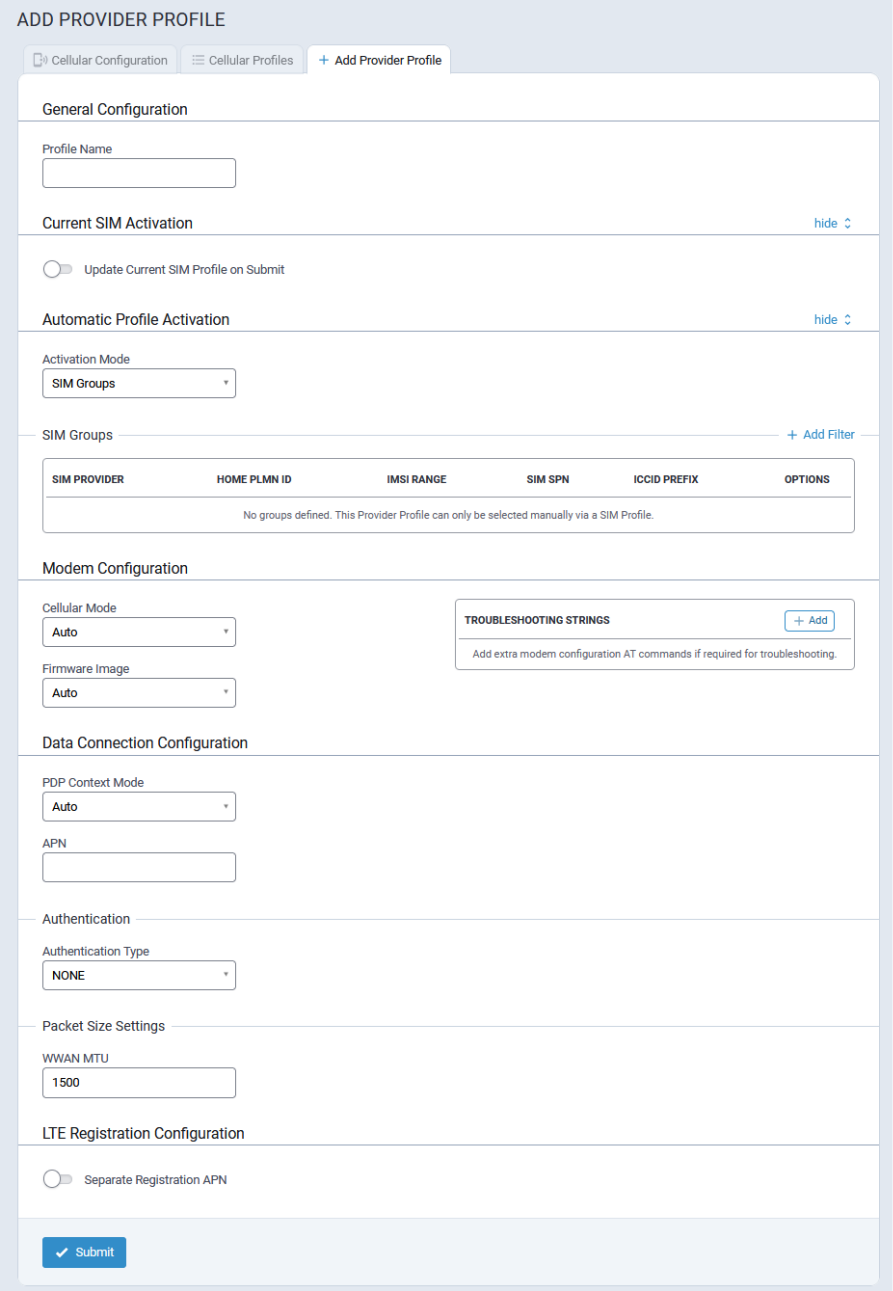


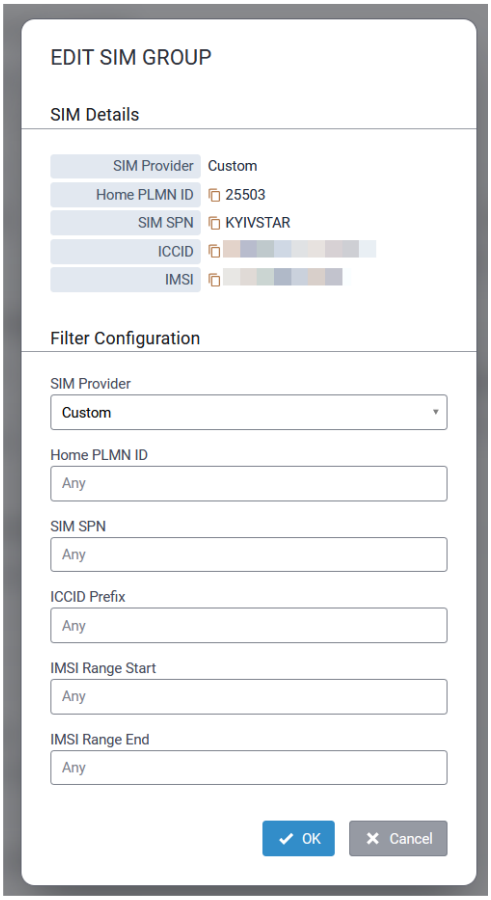
Provider profiles support the configuration of Cellular Management settings such as private network APNs, specific settings for different types of SIMs, etc. What is powerful about these profiles is the ability to customize on a provider basis the configuration values that are not defaults or supported through default behavior.

Add Provider Profile Tab

To create a new Provider Profile, select **+ Add Provider Profile** on the **Cellular Profiles** tab.

The **Add Provider Profile** tab is then displayed allowing users to configure the new provider profile.





Edit SIM Group

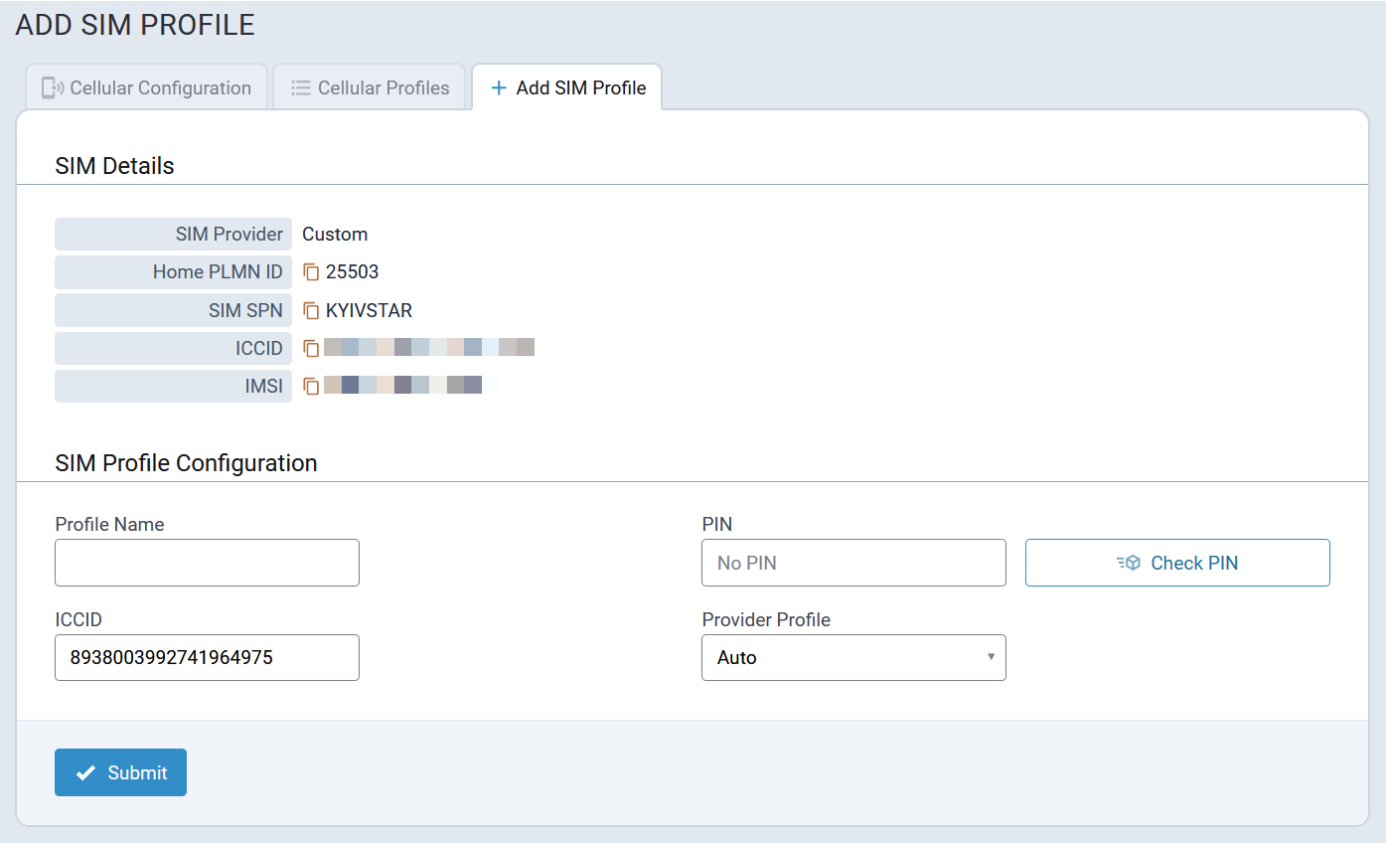
When updating the SIM groups for a profile, what is happening is that each group added is a filter to match only the SIM profiles to be used with the provider profile you are defining groups for. It is possible to have multiple groups which are multiple filters that match different groups of SIMs.

Add SIM Profile Tab

When adding a new provider profile, it is possible to create a SIM group that will be used with that provider profile.

To create a new SIM Profile, select **+ Add SIM Profile** on the **Cellular Profiles** tab.

The **Add SIM Profile** tab is then displayed allowing users to configure the new SIM profile.



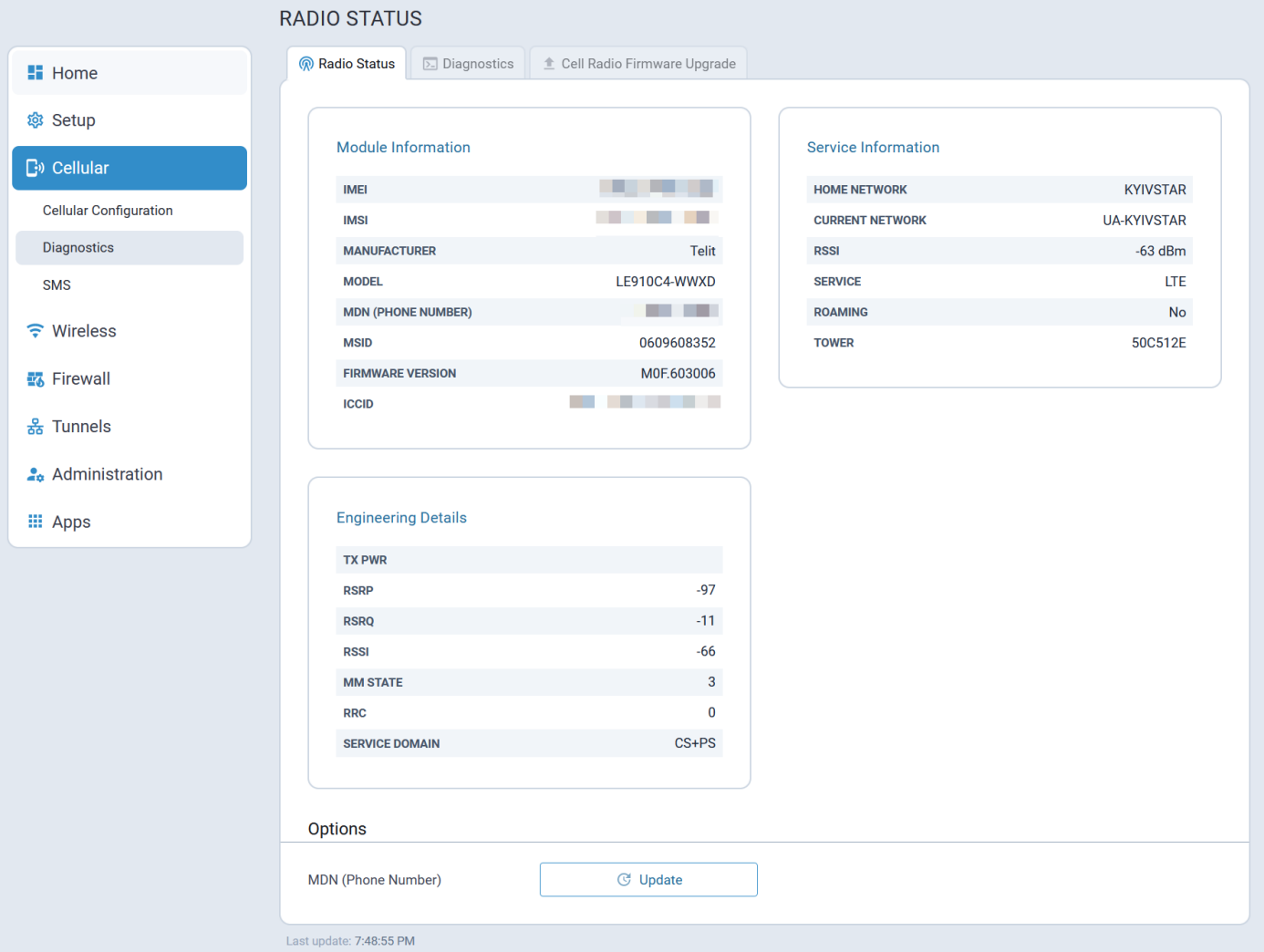
Diagnostics

Cellular Diagnostics includes the following tabs:

- Radio Status
- Diagnostics
- Cell Radio Firmware Upgrade

Radio Status Tab

Typical Radio Status information is illustrated here:

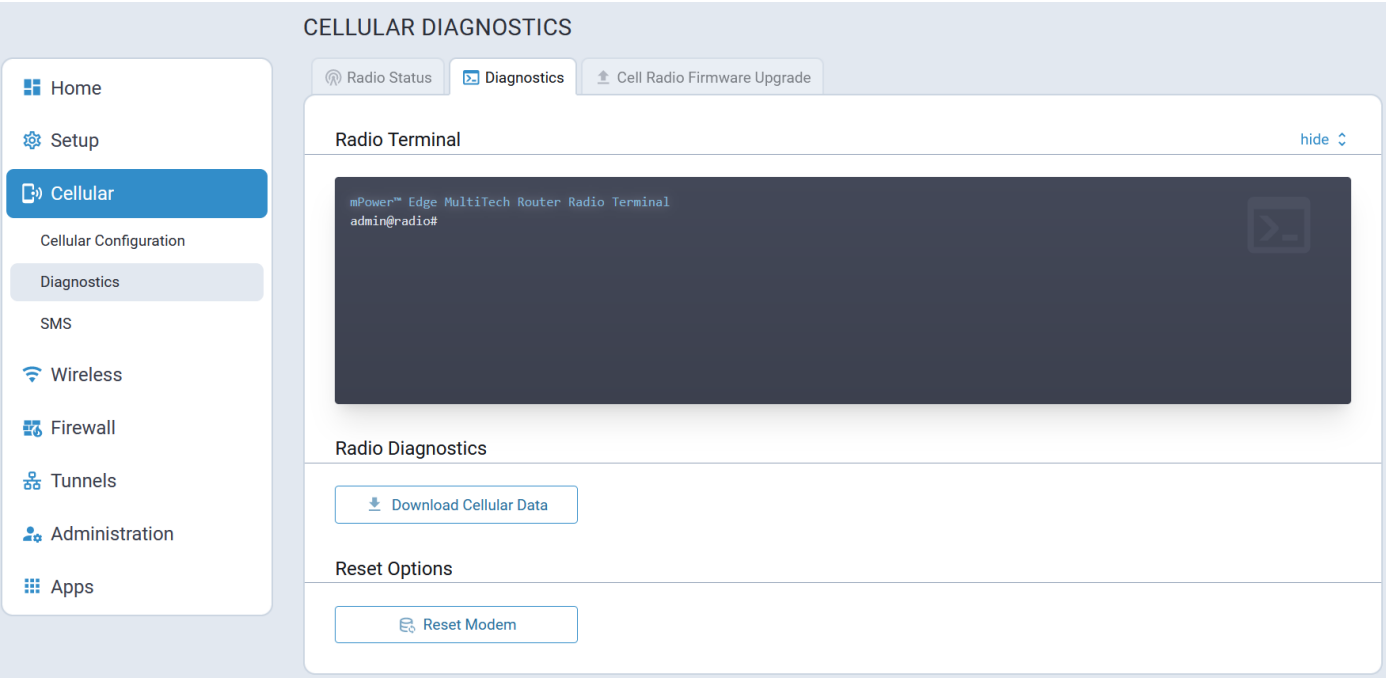


Diagnostics Tab

The Diagnostics tab includes:

- The Radio Terminal in which users can execute AT commands
- Radio Diagnostics feature which allows users to download cellular related logs and details
- Reset Options which allow the modem to be reset

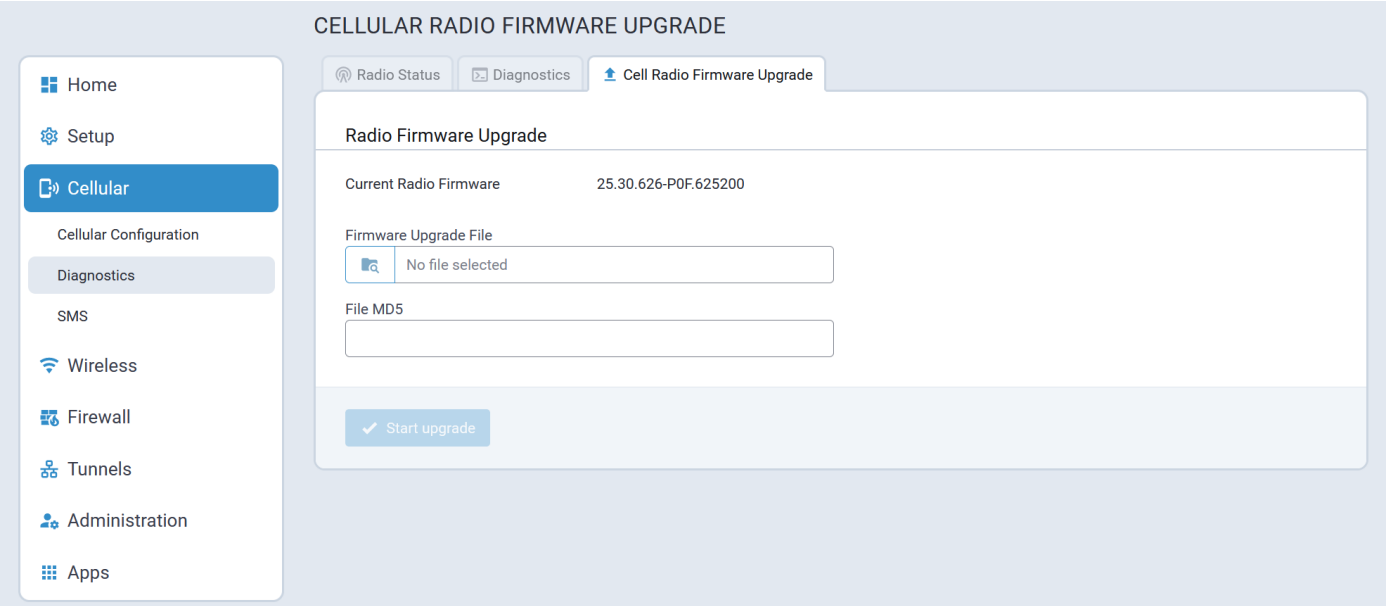
A typical Diagnostics tab is illustrated here:



Cell Radio Firmware Upgrade Tab

The system allows users to perform a cellular radio firmware upgrade.

A typical Cell Radio Firmware Upgrade tab is illustrated here:



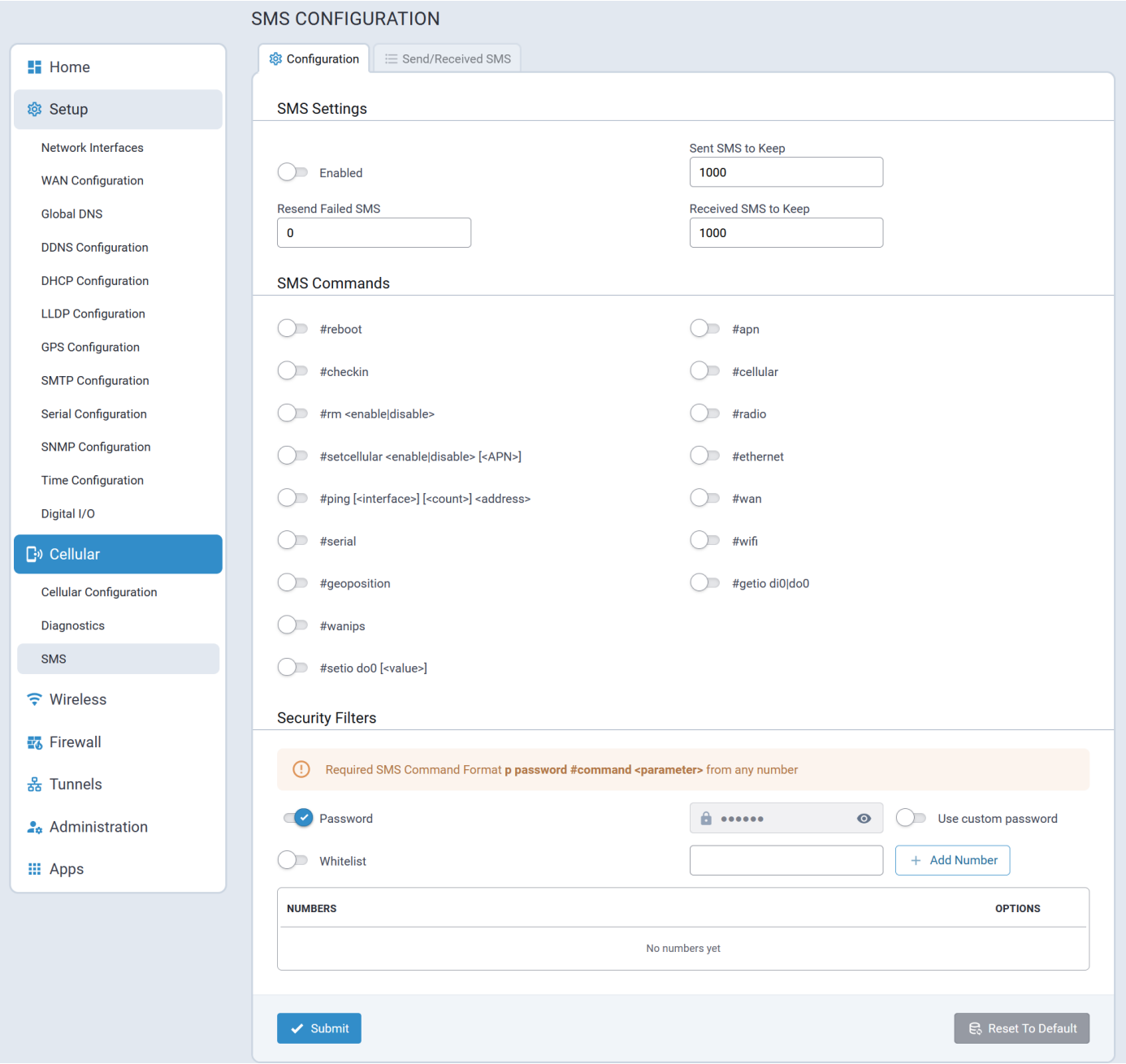
SMS

The SMS menu includes tabs for the following:

- SMS Configuration
- Send/Received SMS

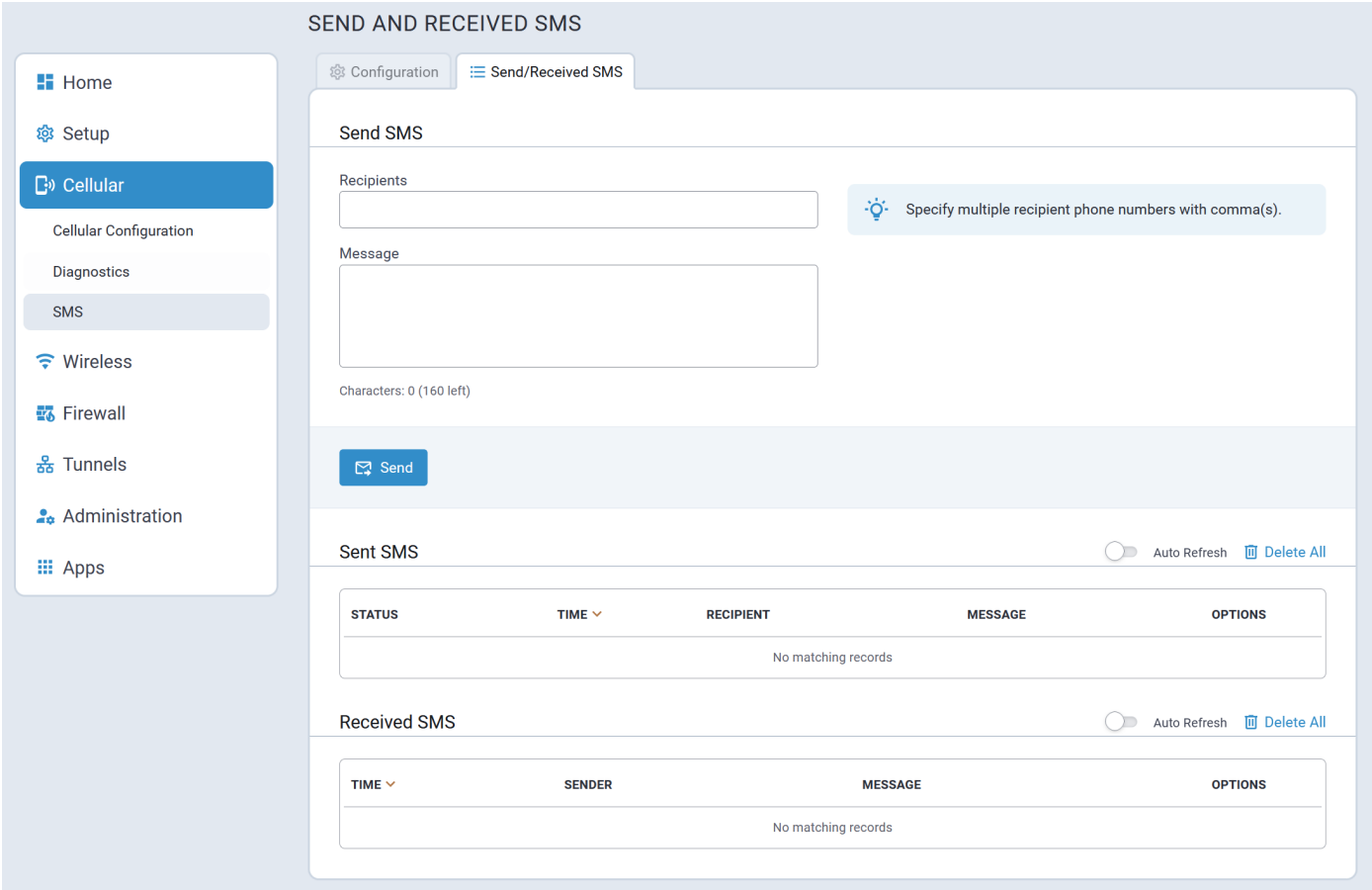
Configuration Tab

A typical SMS Configuration tab showing all supported SMS Commands is illustrated here:



Send/Received SMS Tab

A typical Send/Received SMS tab is illustrated here:



Wireless Menu

Wi-Fi Access Points and Wi-Fi Stations are supported by rCell 300.

Wi-Fi Configuration

The Wi-Fi Configuration menu includes Wi-Fi Access Point and Wi-Fi as WAN configuration pages.

Note: Wi-Fi 6 is supported by rCell 300. The Security Options support **WPA3-SAE** authentication method.

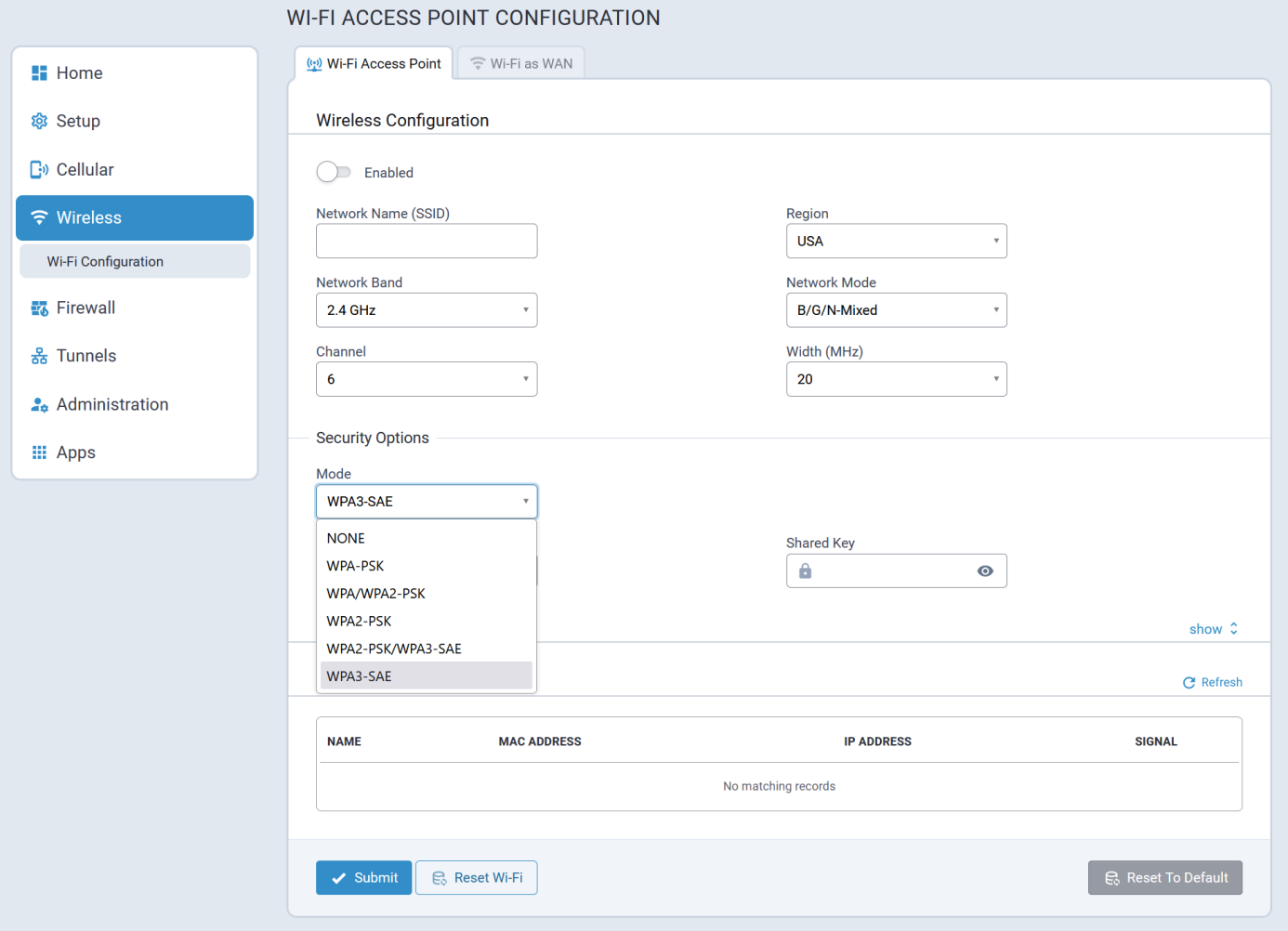
Note: The system does not currently support Wi-Fi Concurrent mode nor Dual Homing. If Wi-Fi as WAN is enabled, the system does not allow enabling Wi-Fi Access Point, and vice versa.

Wi-Fi Access Point Tab

rCell 300 supports **up to 16 clients connected to the Wi-Fi Access Point**.

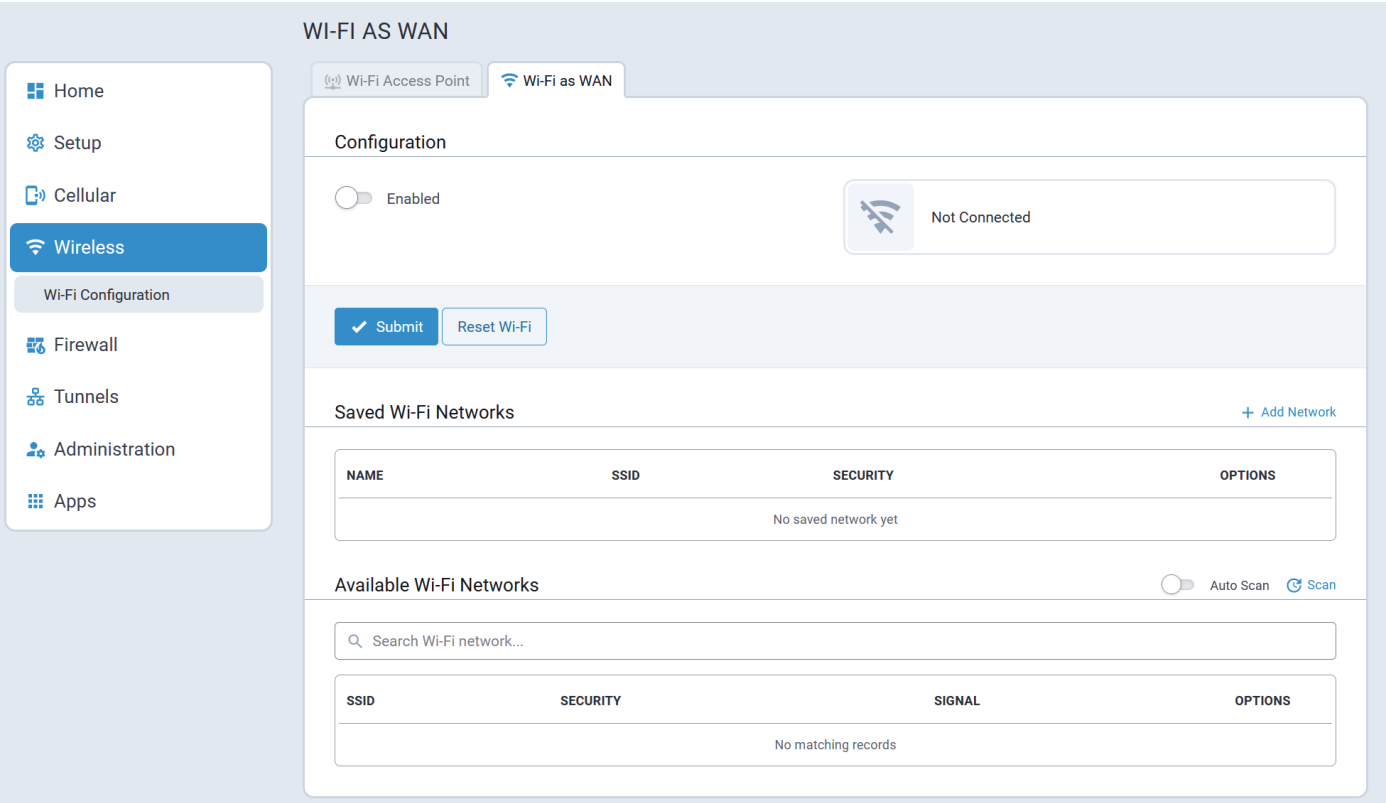
Supported regions are limited to **USA and Canada**.

Typical Wi-Fi Access Point configuration values are illustrated here:



Wi-Fi as WAN Tab

Typical Wi-Fi as WAN configuration values are illustrated here:



Firewall Menu

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 following parameters are configured under the Firewall menu:

- Settings
- Trusted IP
- Static Routes

Note: As a best security practice, the device employs minimum firewall rules by default. This means that the Output Filter Rules are configured to permit all outbound traffic to be transmitted. (Traffic through the device is handled by Port Forwarding Rules.) However, all inbound traffic to the device via WAN interfaces is blocked using 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.

Firewall Rules and Port Forwarding

Firewall Rules and Port Forwarding are performed using nftables.

To print Firewall Rules in the device console use **nft list ruleset**.

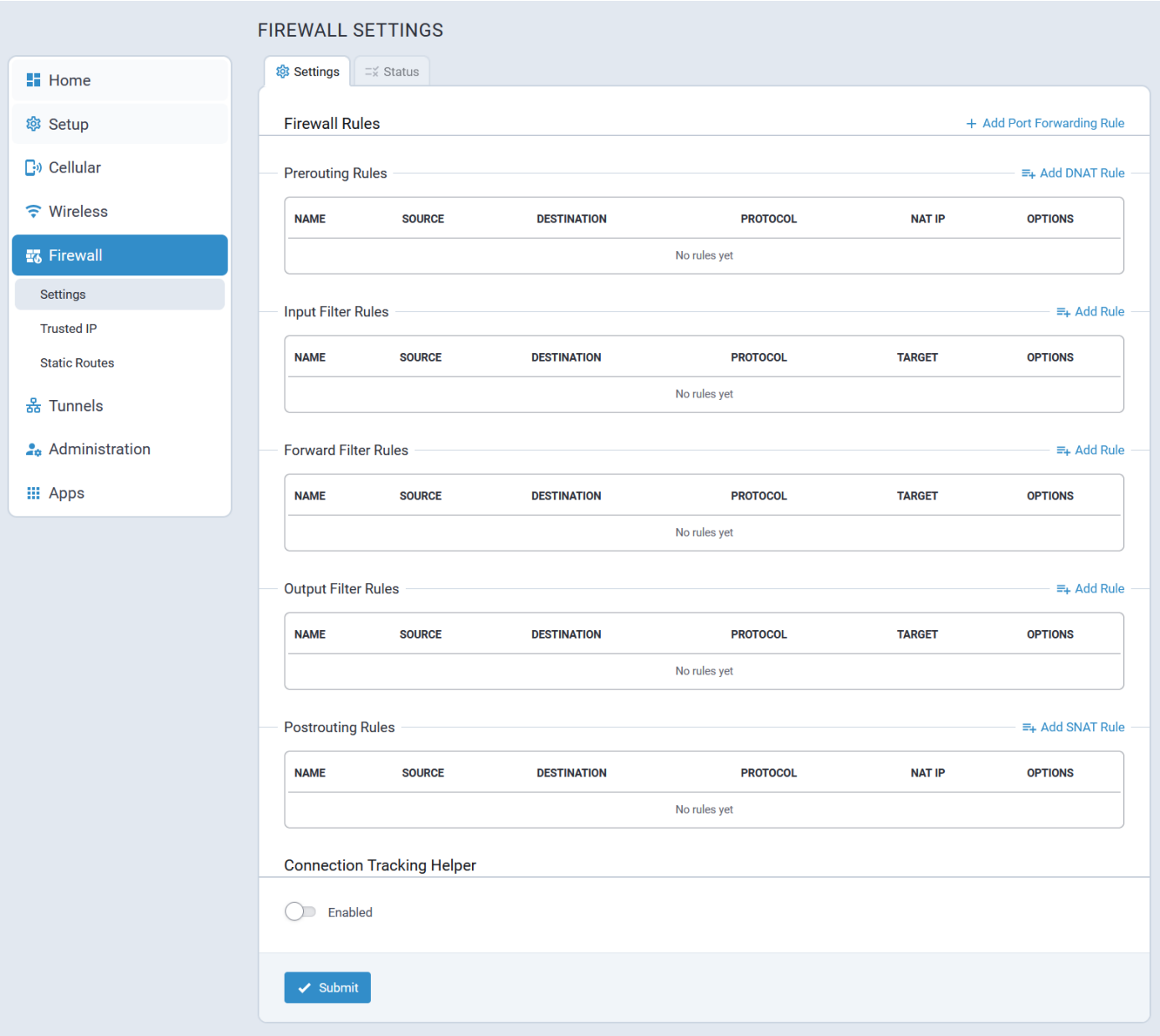
Settings

Firewall Rules and Port Forwarding configuration and status is performed on the following tabs:

- Settings
- Status

Settings Tab

Typical firewall rule configuration settings are illustrated here:



Port Forwarding

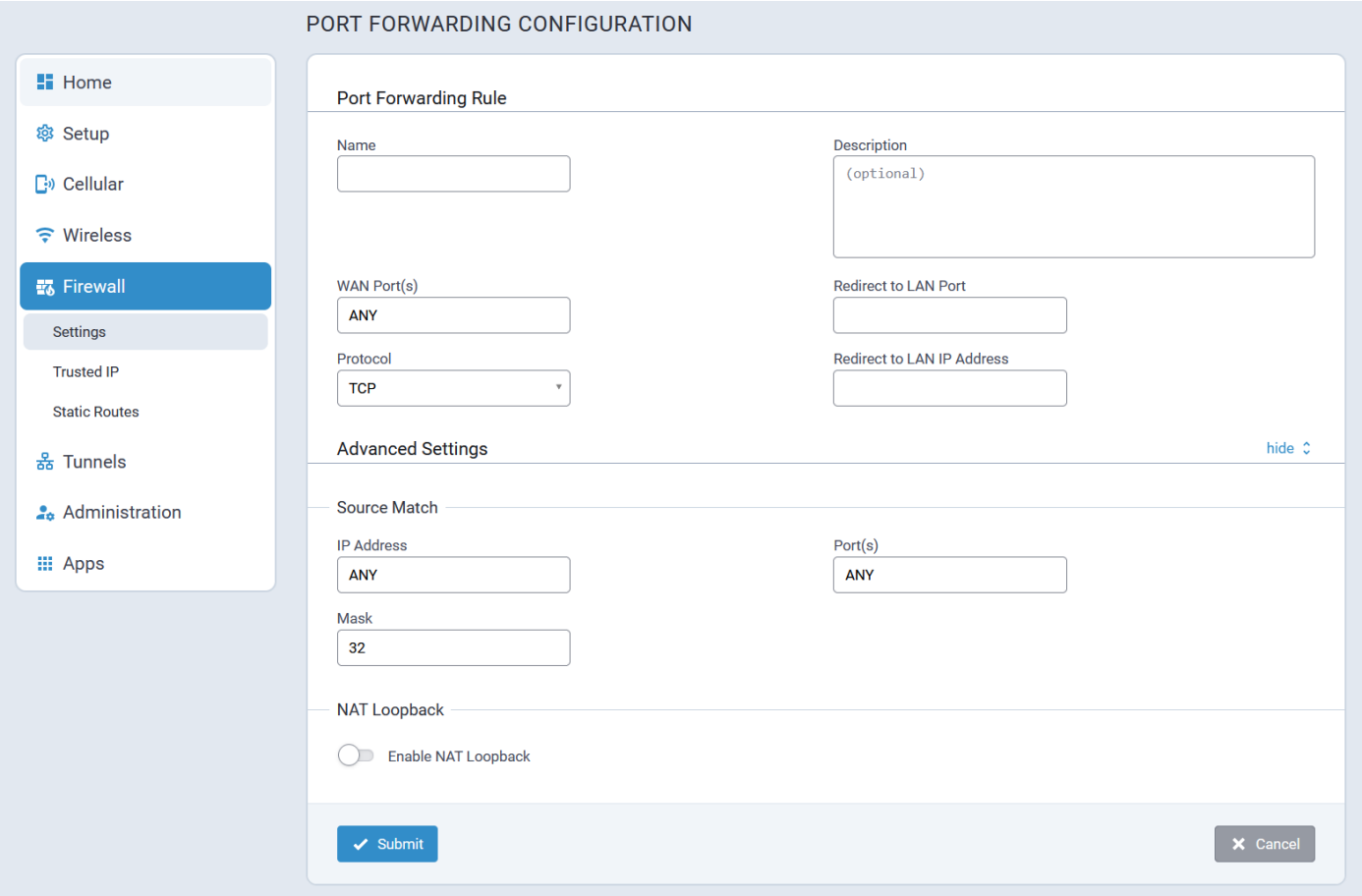
The **Add Port Forwarding Rule** option allows users to create a Port Forwarding rule which comprises two separate firewall rules:

- A prerouting rule
- A forward filter rule

As soon as a user selects **Add Port Forwarding Rule,** the system automatically creates two separate rules.

If changes to the port forwarding rules are required, each of the corresponding rules should be updated individually. Alternatively, the incorrect rules can be deleted and a new port forwarding rule created by selecting the **Add Port Forwarding Rule** button.

Typical port forwarding configuration settings are illustrated here:

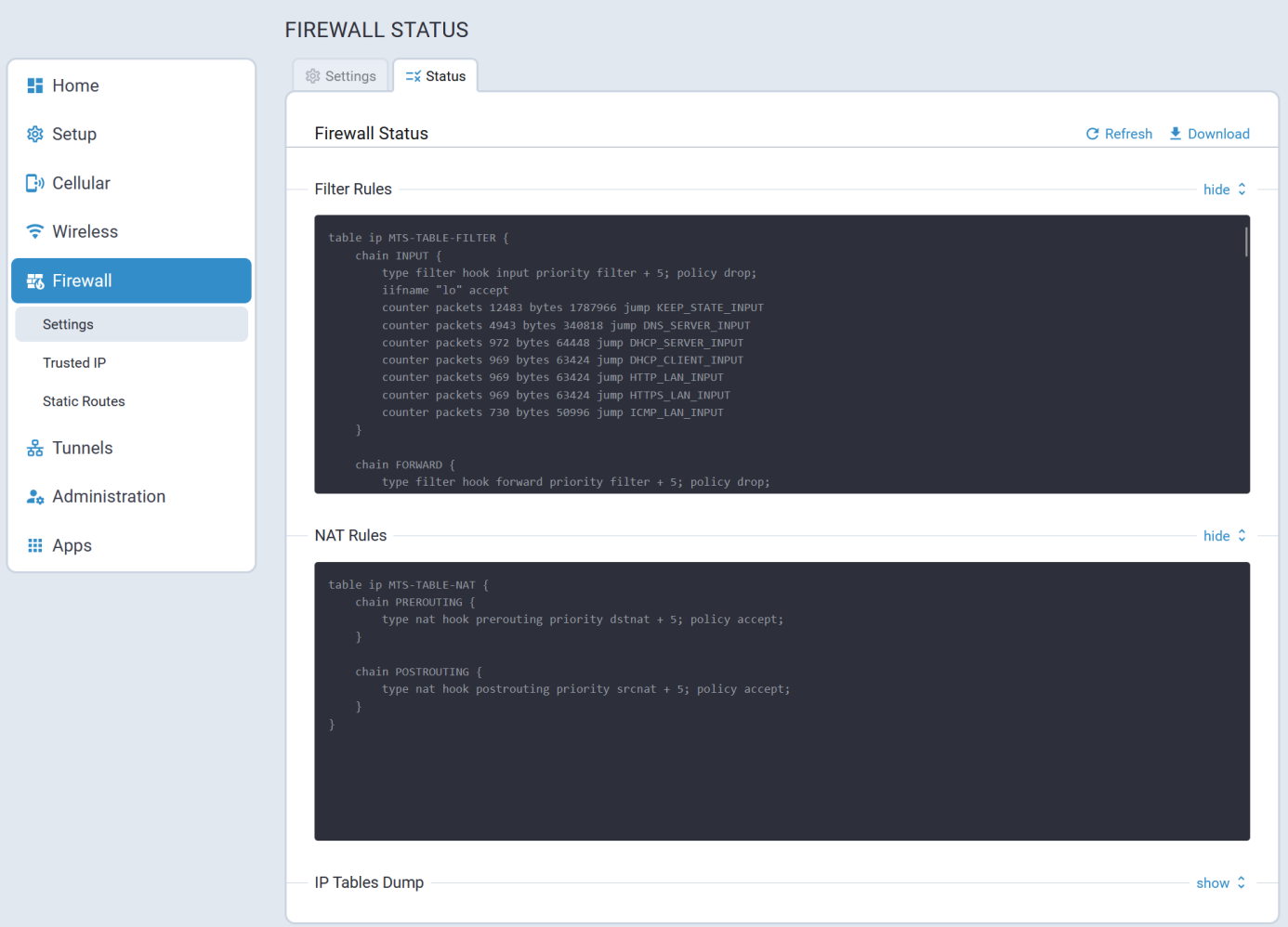


Status Tab

The Firewall Status allows users to review the Firewall rules that are currently being applied within the system.

When a user selects **Download**, the system creates an archive with a **firewall-ruleset.log** file.

A typical firewall Status tab is illustrated here:

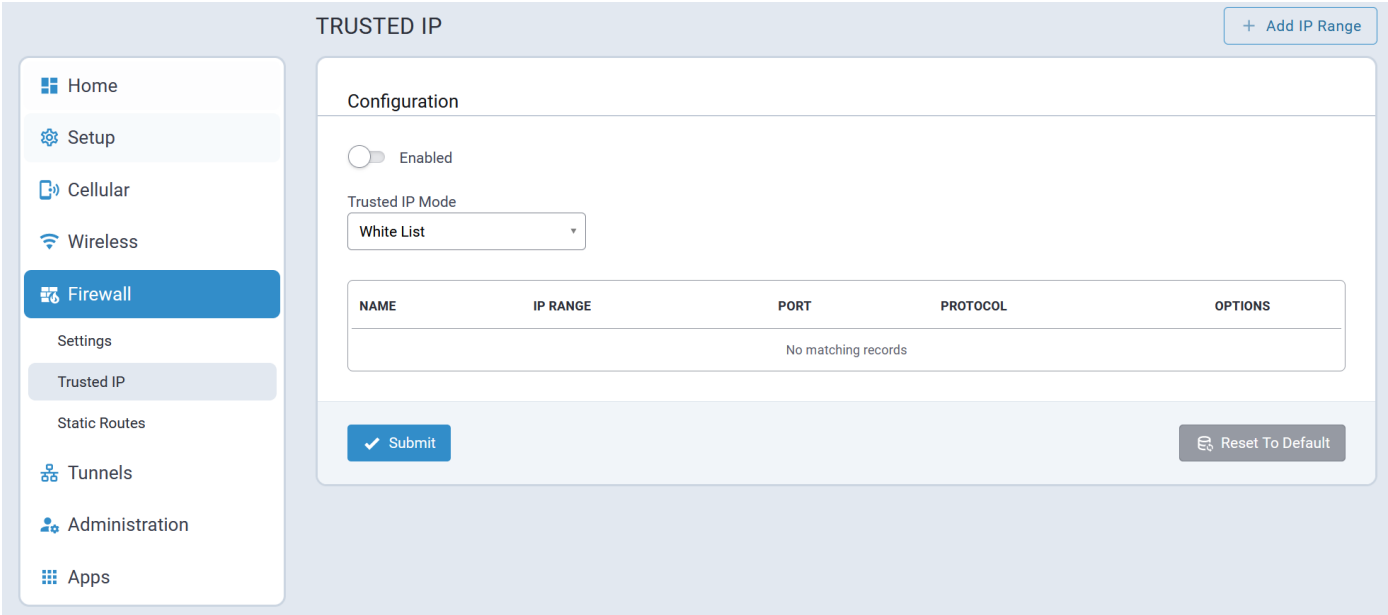


Trusted IP

Trusted IP is a simplified interface to create nftables 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 do not set any IP range, no traffic will be allowed.
- If you select Black List as Trusted IP Mode and do not set any IP range, all traffic will be allowed.

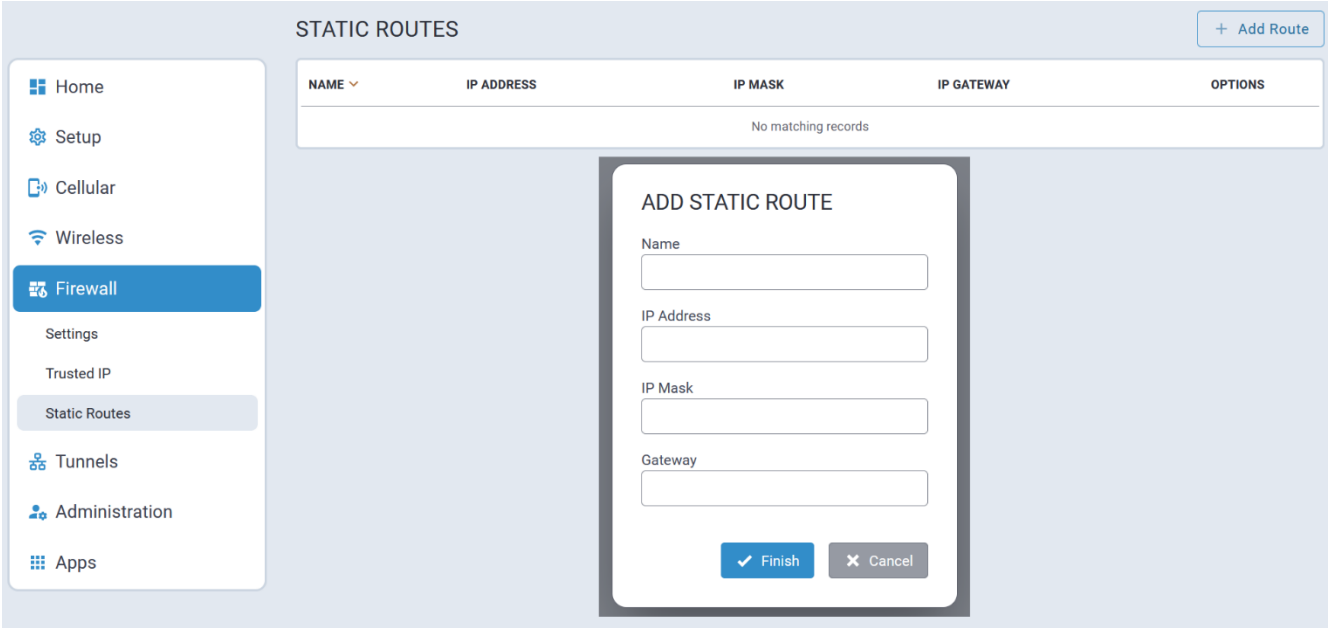
Typical Trusted IP settings are illustrated here:



Static Routes

Configuring static routes adds persistent routes to remote devices that are automatically recreated when the rCell 300 is rebooted.

A typical Static Route settings page is illustrated here:



Tunnels Menu

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.

The rCell 300 supports the following tunnel mechanisms:

- GRE Tunnels
- IPSec Tunnels
- OpenVPN Tunnels

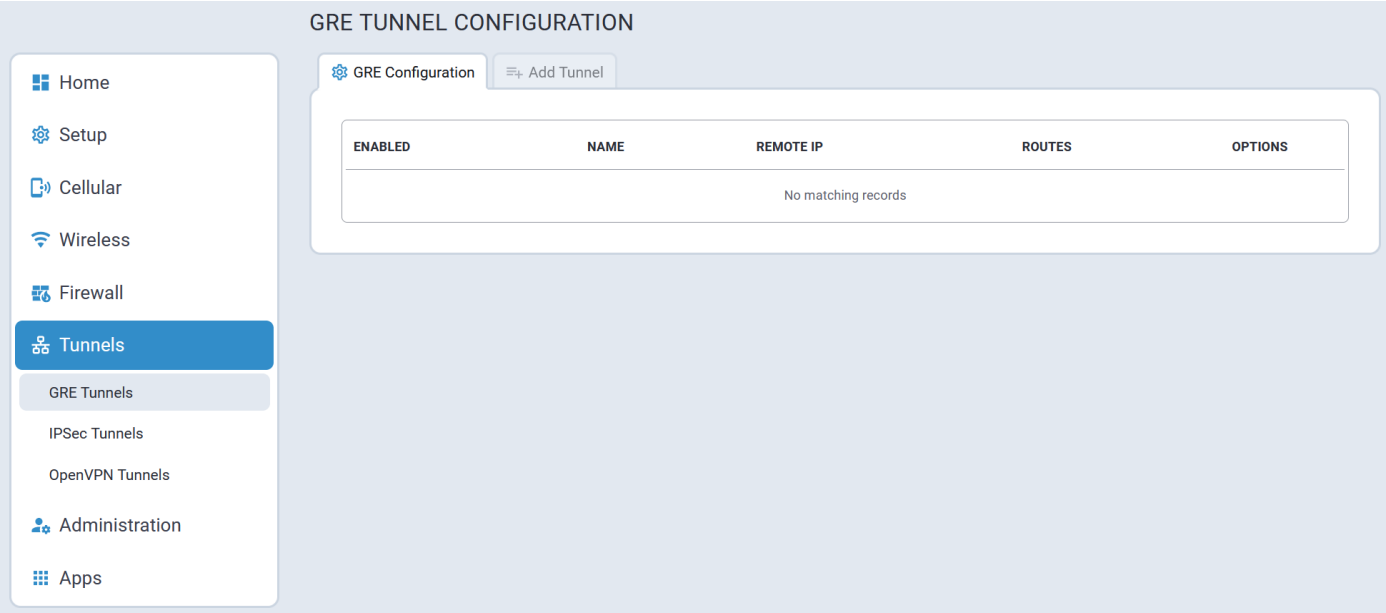
GRE Tunnels

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.

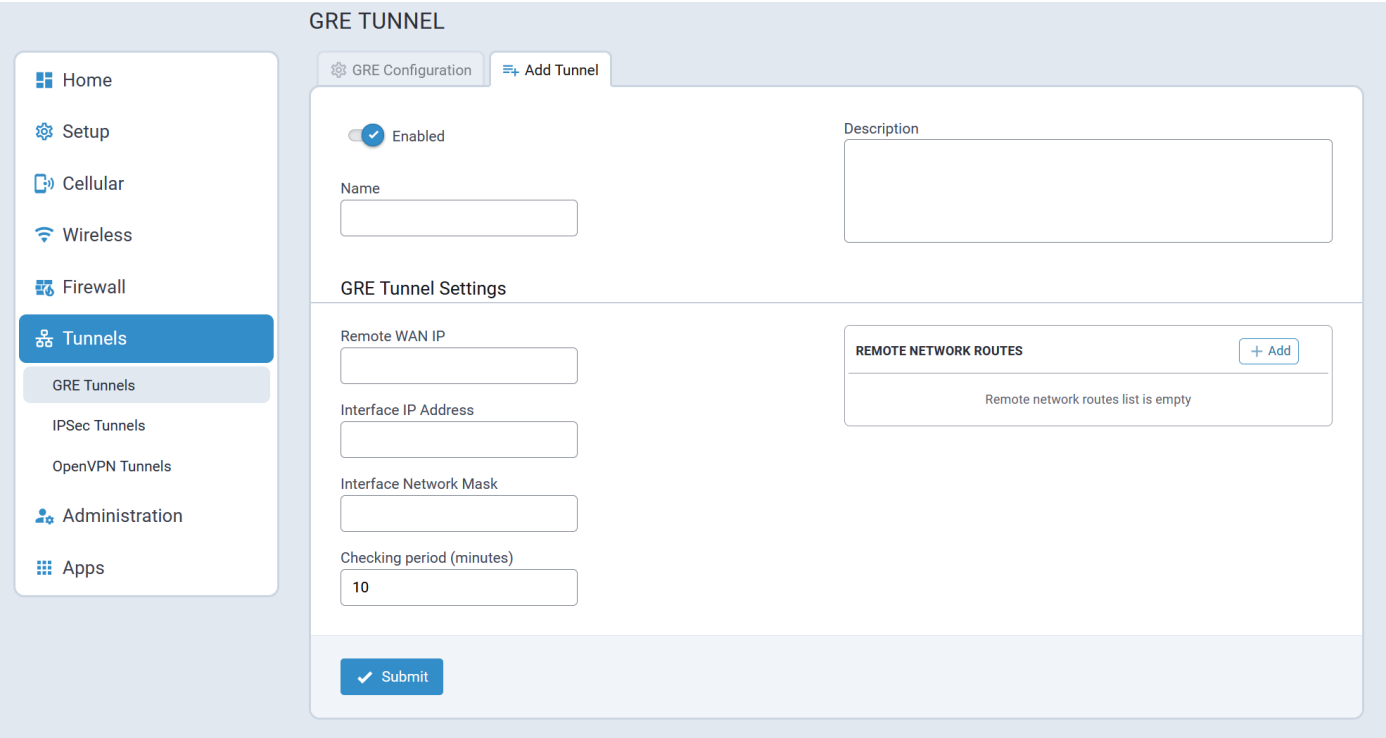
GRE Configuration Tab

A typical GRE Configuration page is illustrated here:



Add Tunnel Tab

To add a GRE tunnel, navigate to the **Add Tunnel** tab. Once all parameters have been configured, select **Submit**.



IPSec Tunnels

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)
- DH24(2048-bit)

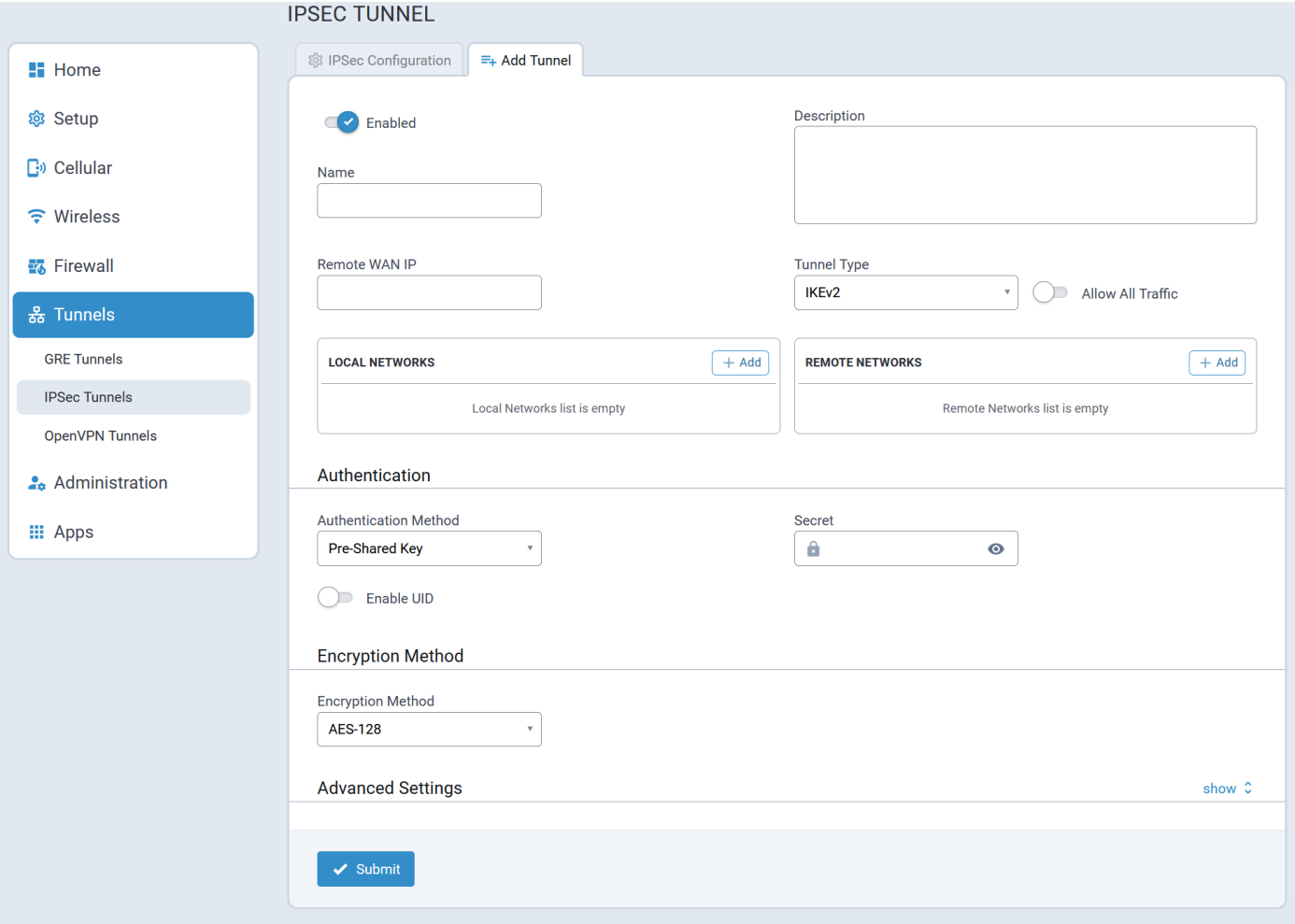
There is the option to add multiple local and remote networks. These additional subnets can provide more complexity, flexibility, efficiency, and redundancy to the VPN. Using multiple networks allows different endpoints in different LAN subnets to securely communicate through the same tunnel. Users do not have to configure an additional tunnel for those subnets saving time and effort.

IPSec Configuration Tab

A typical IPSec Configuration tab is illustrated here:

Add Tunnel Tab

To add an IPSec tunnel, navigate to the **Add Tunnel** tab. Once all parameters have been configured, select **Submit**.



Configuration Parameters

Refer to the following table for information about each IPSec configuration parameter.

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.

Field	Description
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.
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[1]	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[1]	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[1]	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[1]	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**.

Field	Description
Phase 2 Encryption[1]	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[1]	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[1]	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	
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.

[1] *For mPower 5.3 and higher, 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.

To use OpenVPN, install an OpenVPN application along with an easy-rsa tool and configure OpenVPN on your computer. Then, 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:

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

Note:

- When you configure OpenVPN server and client, make sure both sides use the same settings and certificates.
- For mPower 5.3 and higher, some encryption and hash configurations are deprecated and not available for creating new tunnels. Any tunnels 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.
- Some encryption and hash configurations are too weak and NOT supported at all in mPower 5.3 or higher.

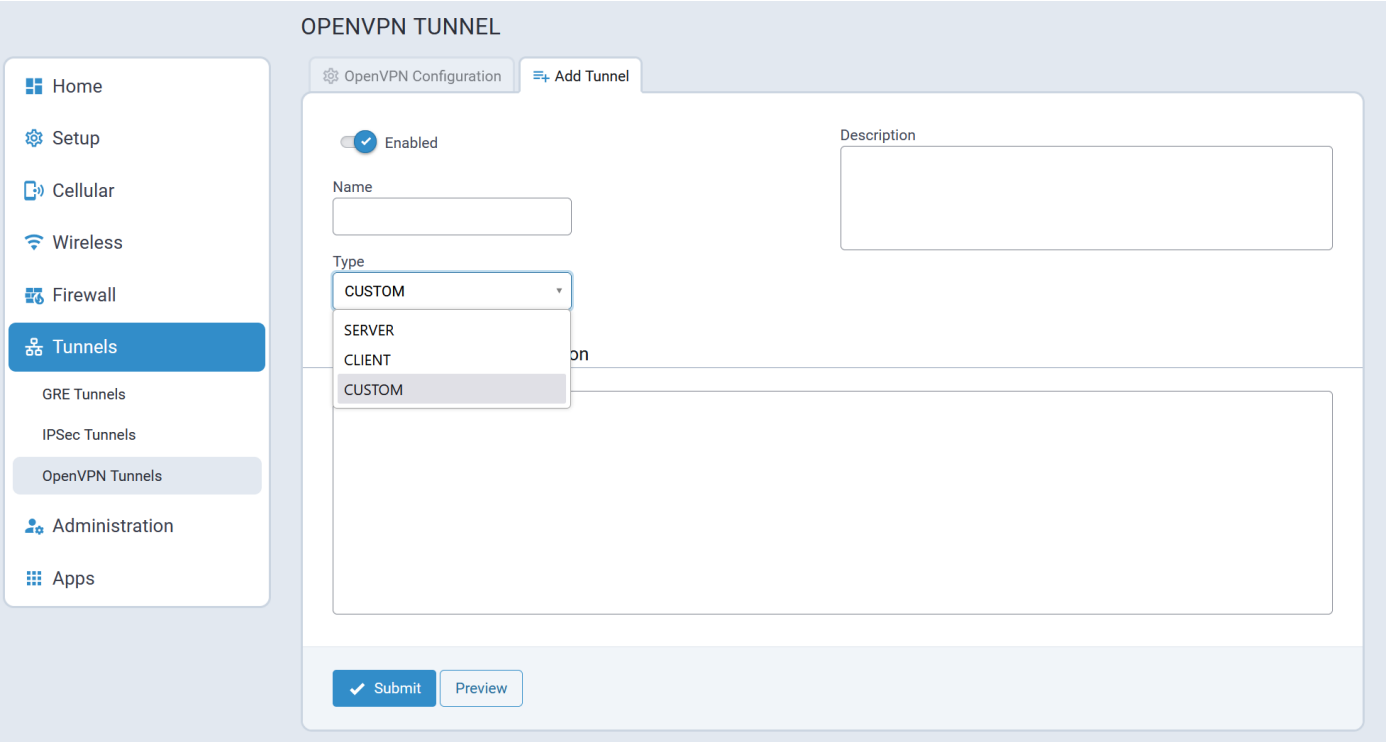
These settings do not function when performing an upgrade to mPower 5.3. The system provides a warning message during upgrade and replaces them with Default. The following TLS cipher suites are not supported: TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA and TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA. Also, the following hash algorithms are not supported: DSA, DSA-SHA, DSA-SHA1, DSA-SHA1-old, ECDSA-with-SHA1, RSA-SHA, RSA-SHA1-2, and SHA.

OpenVPN Configuration Tab

A typical OpenVPN Configuration page is illustrated here:

Add Tunnel Tab

To add a OpenVPN tunnel, navigate to the **Add Tunnel** tab. Once all parameters have been configured, select **Submit**.



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. Select **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **SERVER** from the dropdown.
5. You can also enter an optional **Description**.
6. Under OpenVPN Tunnel Configuration, enter the following fields (using **TLS** as **Authorization Mode**):
   i. **Interface Type** as **TUN** from the dropdown.
   ii. **Authorization Mode** as **TLS** from the dropdown.
   iii. **Protocol** as **UDP**.
   iv. **VPN Subnet**.
   v. **Port** number.
   vi. **VPN Netmask**.
   vii. **LZO Compression** as **ADAPTIVE** from the dropdown.
   viii. **Hash Algorithm** as **DEFAULT**.
   ix. **NCP (Negotiable Crypto Parameters)** as **DEFAULT**.
   x. **Min. TLS Version** as **1.2**.
   xi. **TLS Cipher Suite** as **DEFAULT**.
   xii. 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):
      - CA PEM (.crt)
      - Diffie Hellman PEM (.pem)
      - Server Certificate PEM (.crt)
      - 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**, select **Add**:
   i. 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.
   ii. Enter the **Remote Network Mask** (usually 255.255.255.0).
   iii. You may enter **Gateway** (optional).
   iv. Select **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**:
   i. Select **Client To Client** box if you want this optional feature (this establishes a connection between multiple clients that are connected to the server).
   ii. In the **Push Network Route**, select **Add**.
   iii. In the dialog box, enter the **Remote Network Route** (same address as the server subnet above).
   iv. Enter the **Remote Network Mask** (same as above).
   v. *Optional:* You may enter **Gateway**.
   vi. Select **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. Select **Preview** to view the tunnel configuration.
12. Select **Submit**.
13. Select **Save and Apply** to save your changes

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

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Select **Add Tunnel**.
3. Enter the **Name** of the tunnel.
4. Select the **Type** as **CLIENT** from the dropdown.
5. *Optional:* Enter a **Description**.
6. Under OpenVPN Tunnel Configuration, enter the following fields (using **TLS** as **Authorization Mode**):
   i. **Interface Type** as **TUN** from the dropdown.
   ii. **Authorization Mode** as **TLS** from the dropdown.
   iii. **Protocol** as **UDP**.
   iv. **Remote Host** (server public IP address).
   v. **Remote Port** number.
   vi. **LZO Compression** as **ADAPTIVE** from the dropdown.
   vii. **Hash Algorithm** as **DEFAULT**.
   viii. **NCP (Negotiable Crypto Parameters)** as **DEFAULT.**
   ix. **Min. TLS Version** as **1.2.**
   x. **TLS Cipher Suite** as **DEFAULT**.
   xi. 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):
      - CA PEM (.crt)
      - Client Certificate PEM (.crt)

- 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. Select **Preview** to view the tunnel configuration.
9. Select **Submit**.
10. Select **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:
   i. **iroute [Client_Subnet] [Mask]**
   ii. **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. Select **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **SERVER** from the dropdown.
5. *Optional:* Enter a **Description**.
6. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
   i. **Interface Type** as **TUN** from the dropdown.
   ii. **Authorization Mode** as **STATIC KEY** from the dropdown.
   iii. **Protocol** as **UDP**.
   iv. **Local Address** as **DEFAULT**.
   v. **Port** number.
   vi. **Remote Address** as **DEFAULT**.
   vii. **LZO Compression** as **ADAPTIVE** from the dropdown.
   viii. **Hash Algorithm** as **DEFAULT**.
   ix. **NCP (Negotiable Crypto Parameters)** as **DEFAULT**.
   x. 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-----

3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875
215e20e80a2d59efd79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f5
5e7d8917a32bfe07d61591b7bbb43c7bad214482b8547ec9dca8910f514d9f4270cc
aeff1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104e1968ed29b6c338871
9226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07087
81fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c7531
2375b4bd09876e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd
00305c7cb30beef66ad33f43dacc2e662128

-----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**, select **Add**:
   i. 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.
   ii. Enter the **Remote Network Mask** (usually 255.255.255.0).
   iii. Select **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. Select **Preview** to view the tunnel configuration.

10. Select **Submit**.
11. Select **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. Select **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **CLIENT** from the dropdown.
5. *Optional:* Enter a **Description**.
6. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
   i. **Interface Type** as **TUN** from the dropdown.
   ii. **Authorization Mode** as **STATIC KEY** from the dropdown.
   iii. **Protocol** as **UDP**.
   iv. **Local Address** as **DEFAULT**.
   v. **Remote Host**.
   vi. **Remote Address** as **DEFAULT**.
   vii. **Remote Port** number.
   viii. **LZO Compression** as **ADAPTIVE** from the dropdown.
   ix. Select the **NCP (Negotiable Crypto Parameters)** as **DEFAULT** from dropdown.
   x. Select the **Hash Algorithm** as **DEFAULT** from dropdown.
   xi. **Min. TLS Version** as **1.2.**
   xii. **TLS Cipher Suite** as **DEFAULT**.
   xiii. Enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

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

3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875
215e20e80a2d59efd79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f5
5e7d8917a32bfe07d61591b7bbb43c7bad214482b8547ec9dca8910f514d9f4270cc
aeff1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104e1968ed29b6c338871
9226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07087
81fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c7531
2375b4bd09876e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd
00305c7cb30beef66ad33f43dacc2e662128

-----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**, select **Add**:
   i. 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.

   ii. Enter the **Remote Network Mask** (usually 255.255.255.0).
   iii. Select **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. Select **Preview** to view the tunnel configuration.
10. Select **Submit**.
11. Select **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. Select **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **SERVER** from the dropdown.
5. *Optional:* Enter a **Description**.
6. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):

   i. **Interface Type** as **TUN** from the dropdown.
   ii. **Authorization Mode** as **STATIC KEY** from the dropdown.
   iii. **Protocol** as **TCP**.
   iv. **Local Address** as **DEFAULT**.
   v. **Remote Host**.
   vi. **Remote Address** as **DEFAULT**.
   vii. **Remote Port** number.
   viii. **Hash Algorithm** as **RSA-SHA1**.
   ix. **LZO Compression** as **ADAPTIVE** from the dropdown.
   x. **NCP (Negotiable Crypto Parameters)** as **CAMELLIA-256-CBC**.
   xi. **Min. TLS Version** as **NONE.**
   xii. **TLS Cipher Suite** as **DEFAULT**.
   xiii. 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-----

3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875
215e20e80a2d59efd79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f5
5e7d8917a32bfe07d61591b7bbb43c7bad214482b8547ec9dca8910f514d9f4270cc
```

```
aeff1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104e1968ed29b6c338871
9226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07087
81fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c7531
2375b4bd09876e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd
00305c7cb30beef66ad33f43dacc2e662128

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

7. Select **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**, select **Add**:
   i. 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.
   ii. Enter the **Remote Network Mask** (usually 255.255.255.0).
   iii. Select **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. Select **Preview** to view the tunnel configuration.
11. Select **Submit**.
12. Select **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. Select **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **CLIENT** from the dropdown.
5. *Optional:* Enter a **Description**.
6. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
   i. **Interface Type** as **TUN** from the dropdown.
   ii. **Authorization Mode** as **STATIC KEY** from the dropdown.
   iii. **Protocol** as **TCP**.
   iv. **Local Address** as **DEFAULT**.
   v. **Remote Host**.
   vi. **Remote Address** as **DEFAULT**.
   vii. **Remote Port** number.
   viii. **Hash Algorithm** as **RSA-SHA1**.
   ix. **LZO Compression** as **ADAPTIVE** from the dropdown.
   x. **NCP (Negotiable Crypto Parameters)** as **CAMELLIA-256-CBC**.

xi. **Min. TLS Version** as **NONE.**

xii. **TLS Cipher Suite** as **DEFAULT**.

xiii. 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-----

3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875
215e20e80a2d59efd79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f5
5e7d8917a32bfe07d61591b7bbb43c7bad214482b8547ec9dca8910f514d9f4270cc
aeff1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104e1968ed29b6c338871
9226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07087
81fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c7531
2375b4bd09876e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd
00305c7cb30beef66ad33f43dacc2e662128

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

7. Select **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**, select **Add**:

   i. 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.

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

   iii. Select **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. Select **Preview** to view the tunnel configuration.

11. Select **Submit**.

12. Select **Save and Apply** to save your changes.

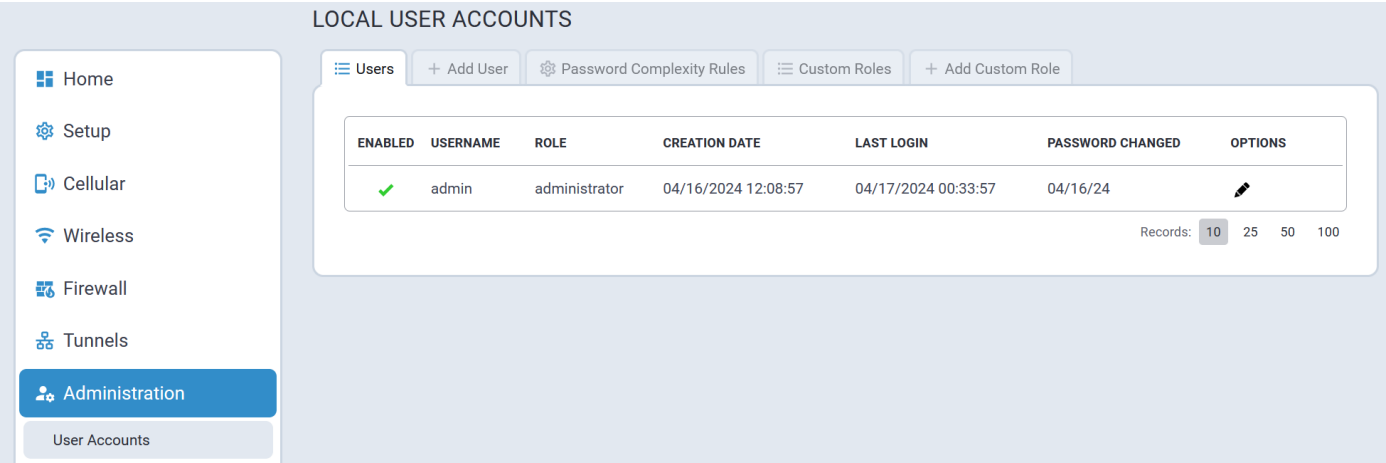
Administration Menu

User Accounts

The Local User Accounts page supports activities to add, remove, and update user accounts on the device including changing passwords. The Engineer and Monitor roles can only change their own account settings, while the Administrator role can update any account.

Users Tab

A typical Users tab is illustrated here:

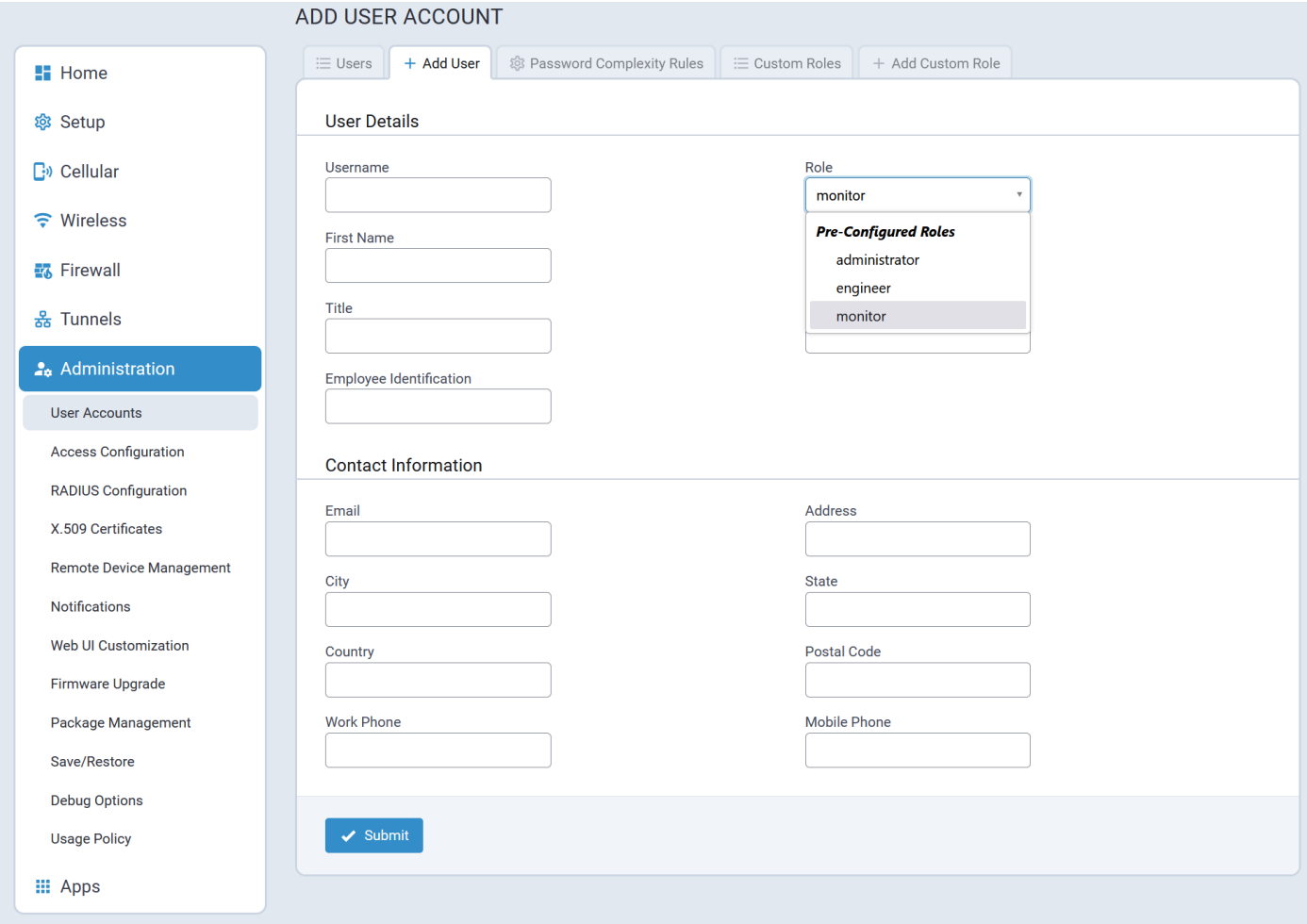


Add User Tab

By default, the system supports three user roles:

- Administrator
- Engineer
- Monitor

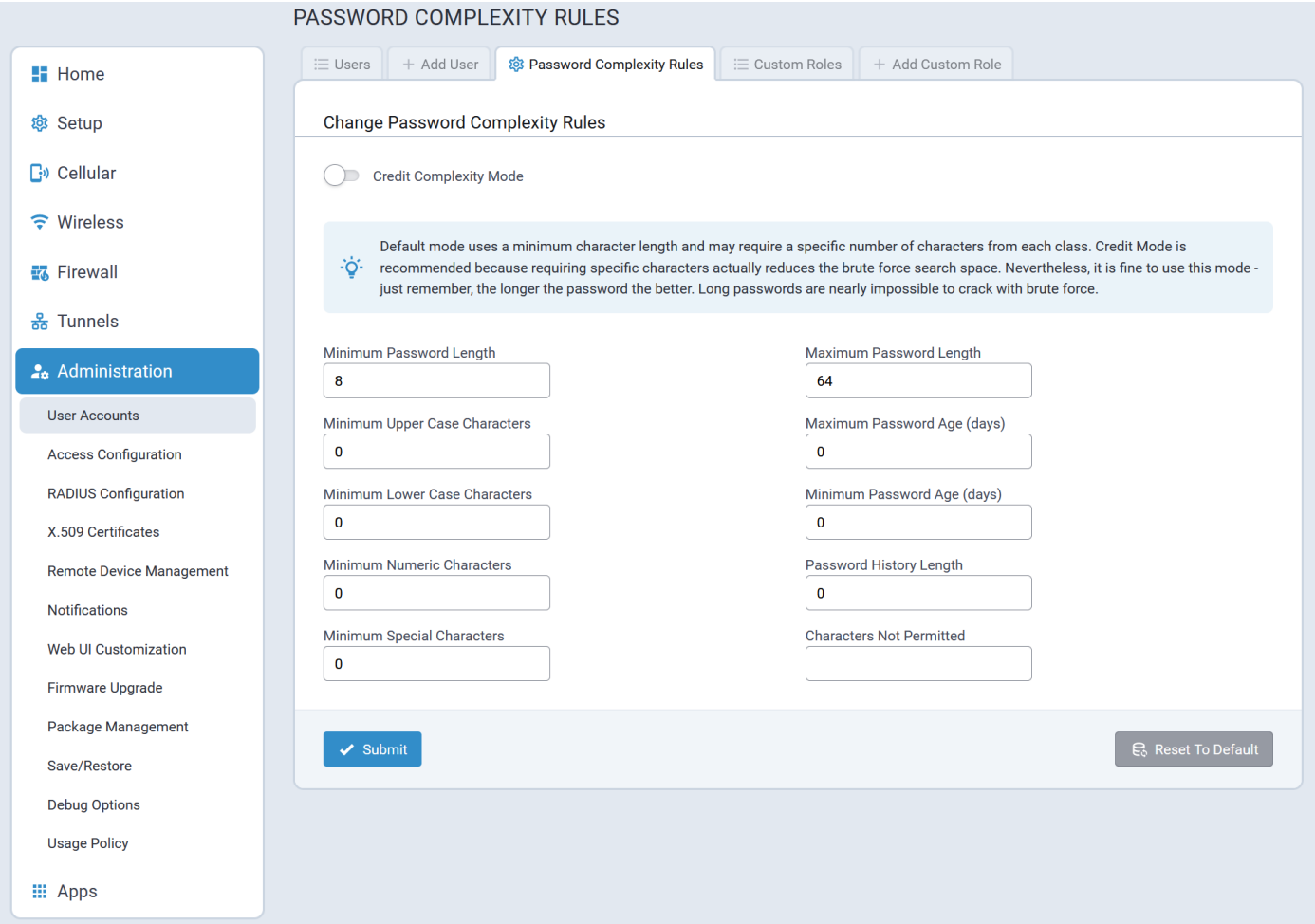
A typical Add User tab is illustrated here:



Password Complexity Rules Tab

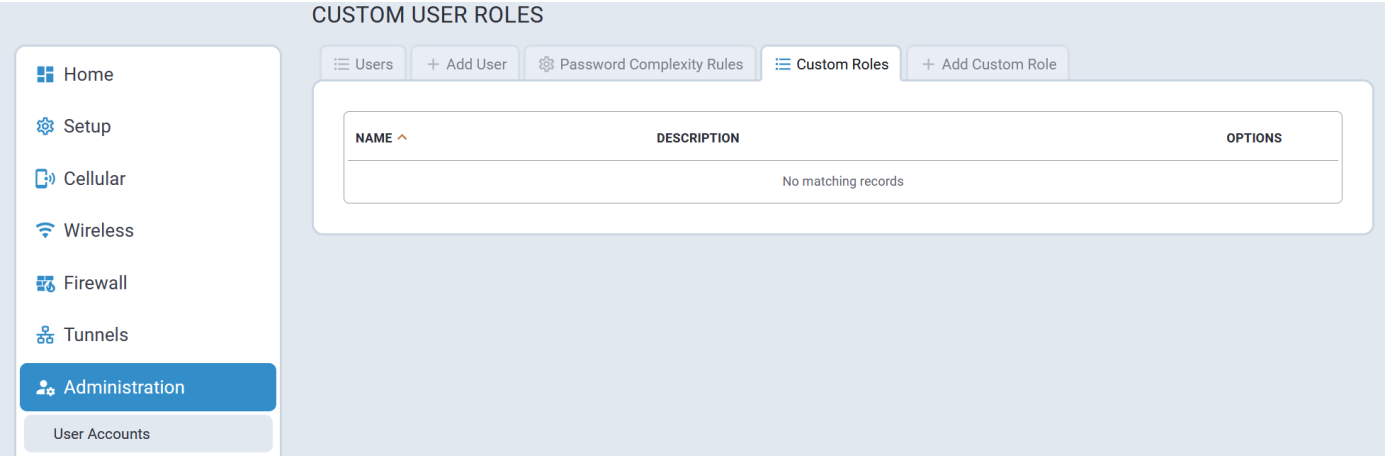
Password complexity is managed through the facilities in Linux and PAM. There is a default complexity mode that is configurable. There is also the credit mode that is available in Linux distributions configurable to require a minimum credit score on a new password.

A typical Password Complexity Rules tab is illustrated here:



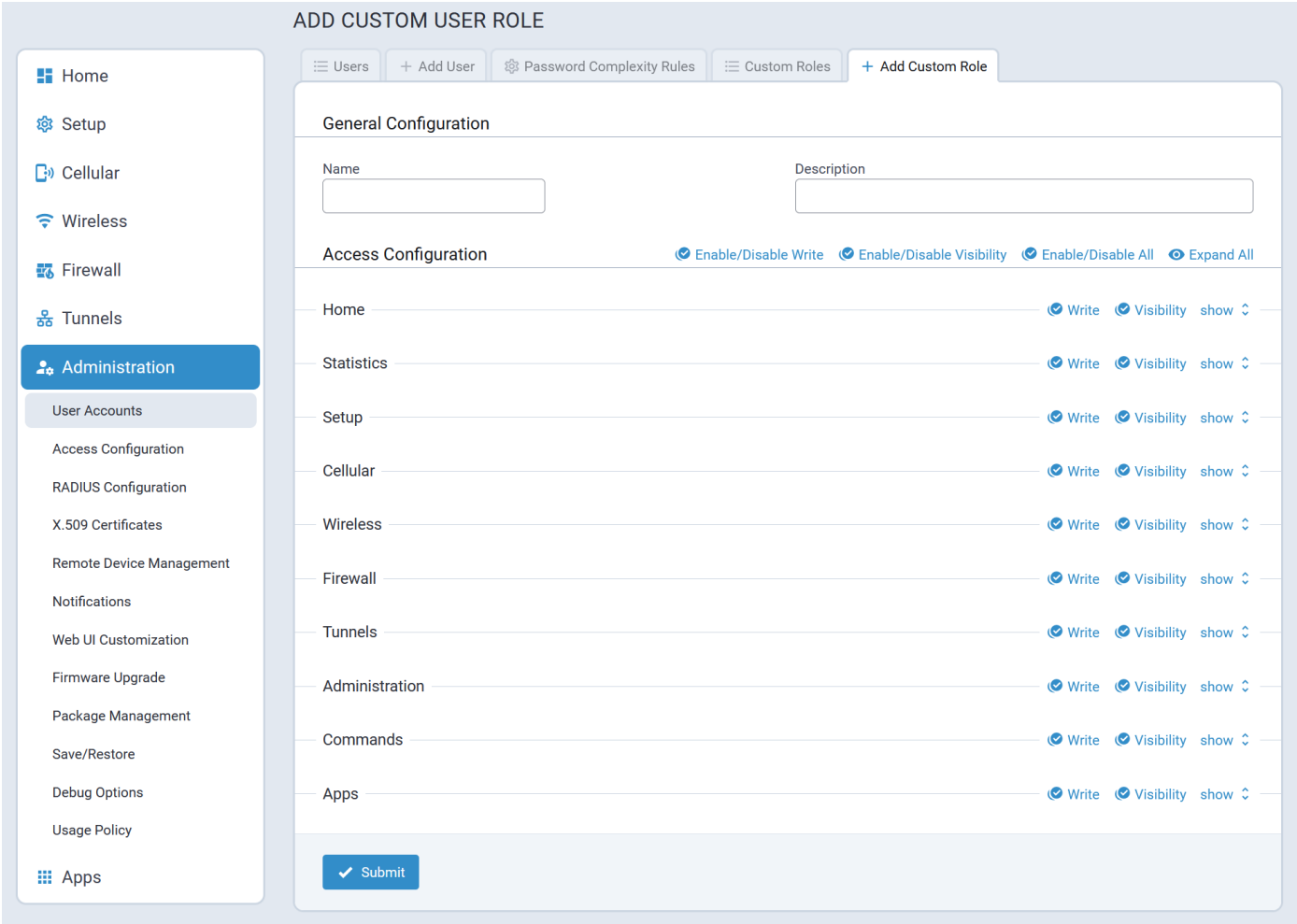
Custom Roles Tab

A typical Custom Roles tab is illustrated here:



Add Custom Role

A typical Add Custom Role tab is illustrated here:

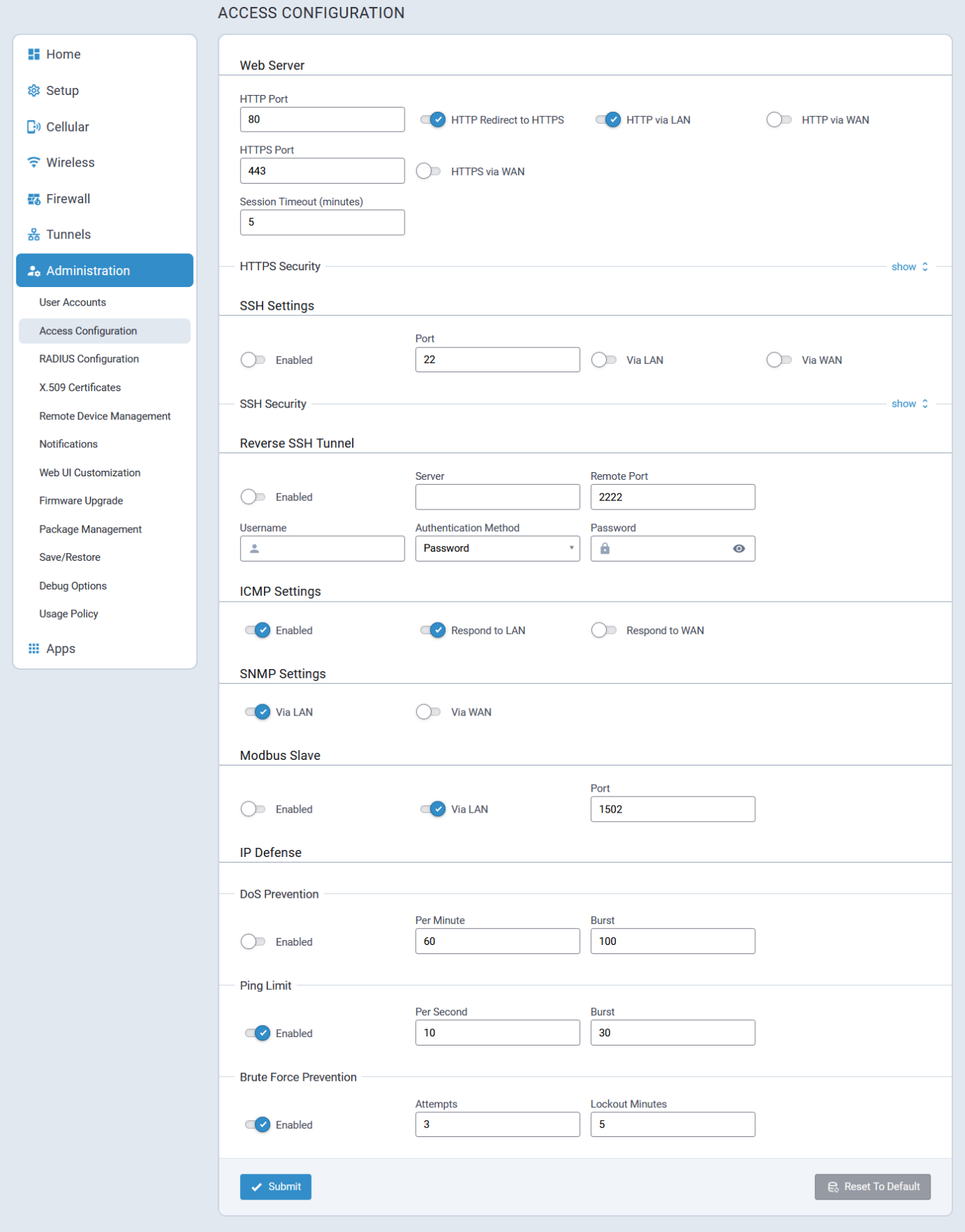


Access Configuration

Access Configuration supports configuring access for different services on the device:

- The Web Server for the mPower API used by the mPower Web UI
- SSH access to the device
- Responsiveness to Pings to the device on the LAN and WAN interfaces
- Enabling the Reverse SSH port forwarding capability
- The SNMP server
- The Modbus server
- Enabling and limited configuration of:
  - DoS prevention
  - Ping Limiting
  - Brute Force Prevention to lock out user accounts that exceed the password failure limit

The default settings for the Access Configuration page is illustrated here:


ACCESS CONFIGURATION
Home
Setup
Cellular
Wireless
Firewall
Tunnels
Administration
User Accounts
Access Configuration
RADIUS Configuration
X.509 Certificates
Remote Device Management
Notifications
Web UI Customization
Firmware Upgrade
Package Management
Save/Restore
Debug Options
Usage Policy
Apps
Web Server
HTTP Port
80
HTTP Redirect to HTTPS
HTTP via LAN
HTTP via WAN
HTTPS Port
443
HTTPS via WAN
Session Timeout (minutes)
5
HTTPS Security
show
SSH Settings
Enabled
Port
22
Via LAN
Via WAN
SSH Security
show
Reverse SSH Tunnel
Enabled
Server
Remote Port
2222
Username
Authentication Method
Password
Password
ICMP Settings
Enabled
Respond to LAN
Respond to WAN
SNMP Settings
Via LAN
Via WAN
Modbus Slave
Enabled
Via LAN
Port
1502
IP Defense
DoS Prevention
Enabled
Per Minute
60
Burst
100
Ping Limit
Enabled
Per Second
10
Burst
30
Brute Force Prevention
Enabled
Attempts
3
Lockout Minutes
5
Submit
Reset To Default

Radius Configuration

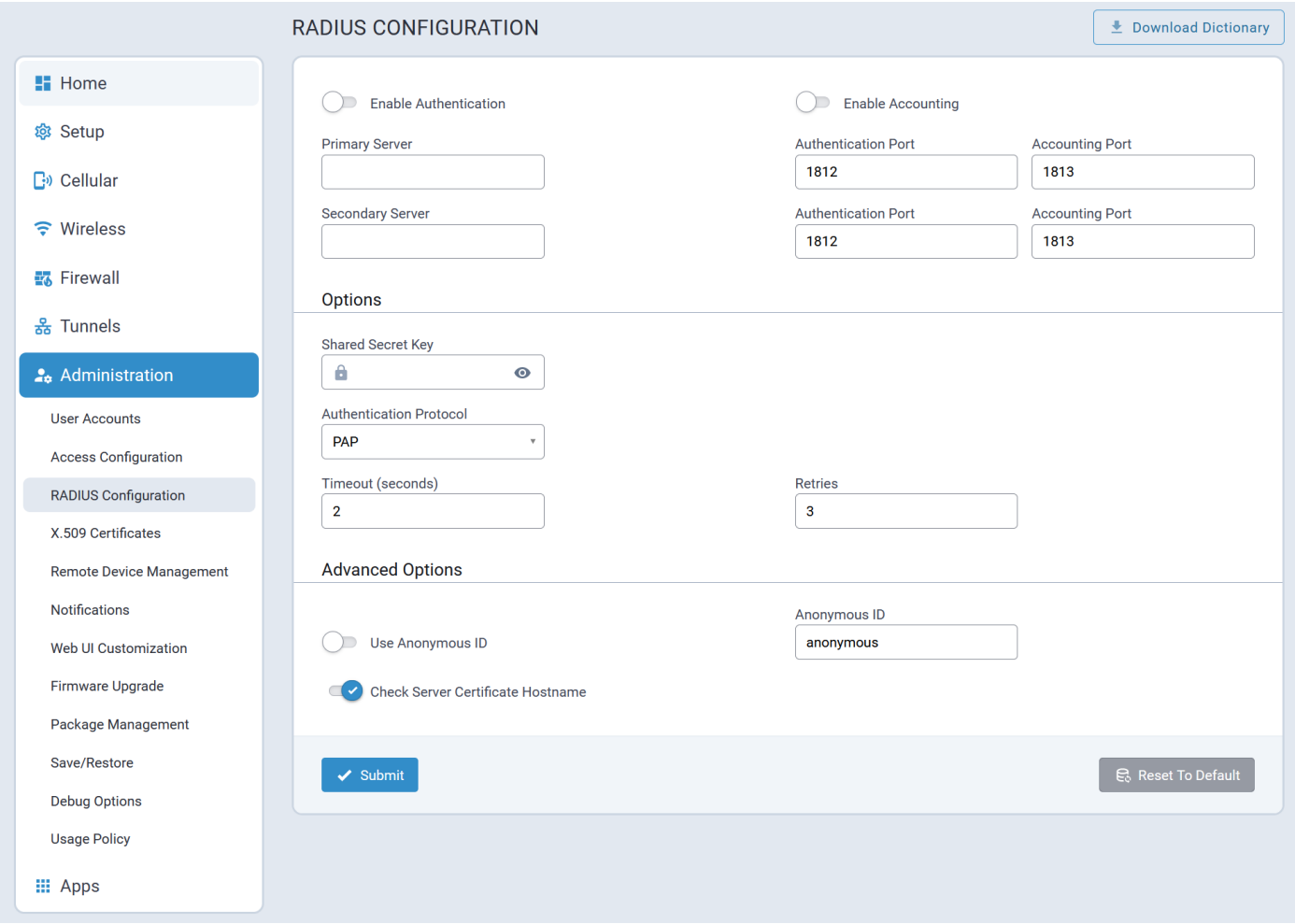
The RADIUS protocol supports authentication, user session accounting, and authorization of users to the device.

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.

A typical Radius Configuration page is illustrated here:



X.509 Certificate Tab

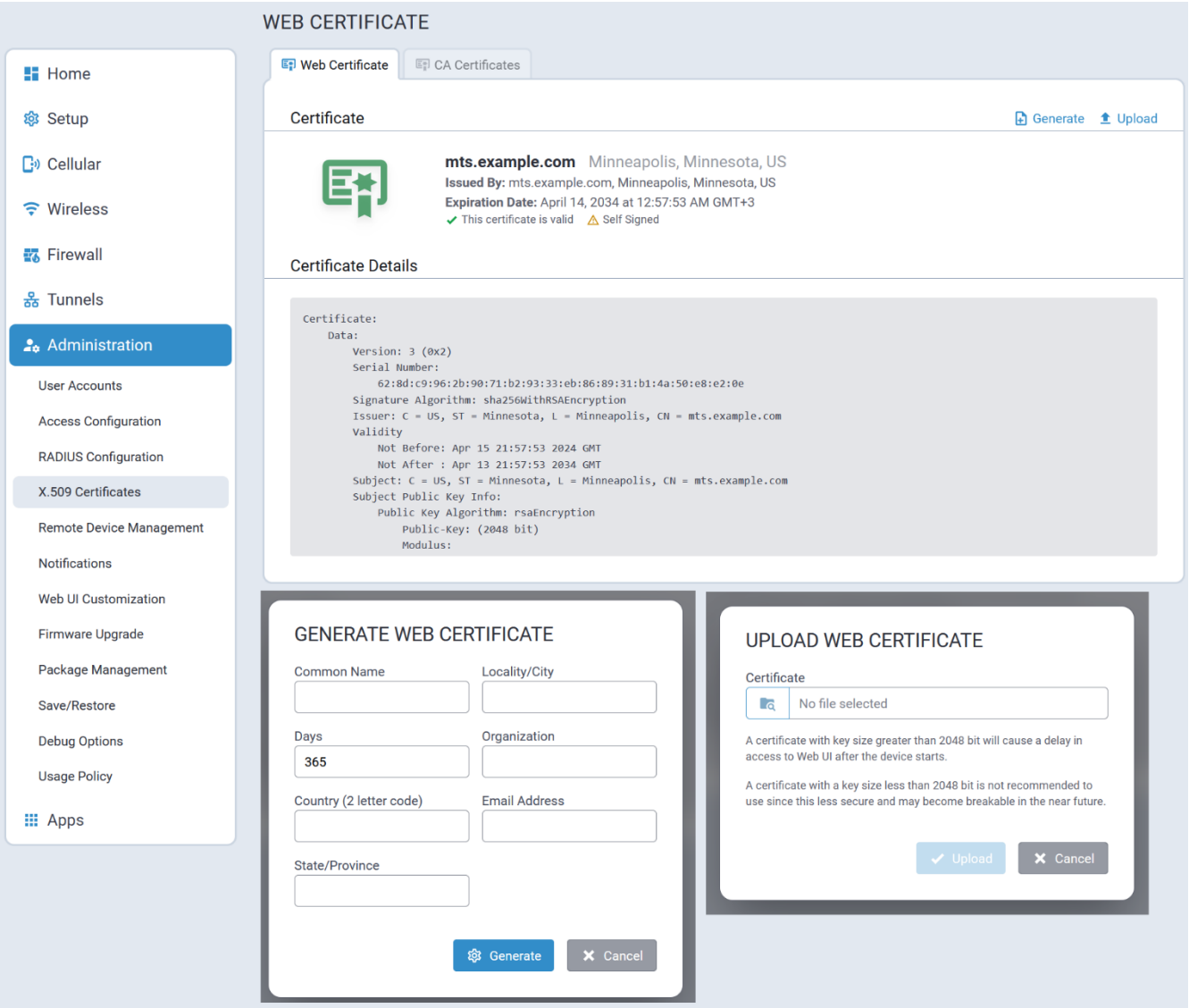
X.509 Certificate tab includes settings for the following:

- Web Certificate
- CA Certificates

Web Certificate Tab

The system supports generating and uploading a new Web Certificate in **.pem** format.

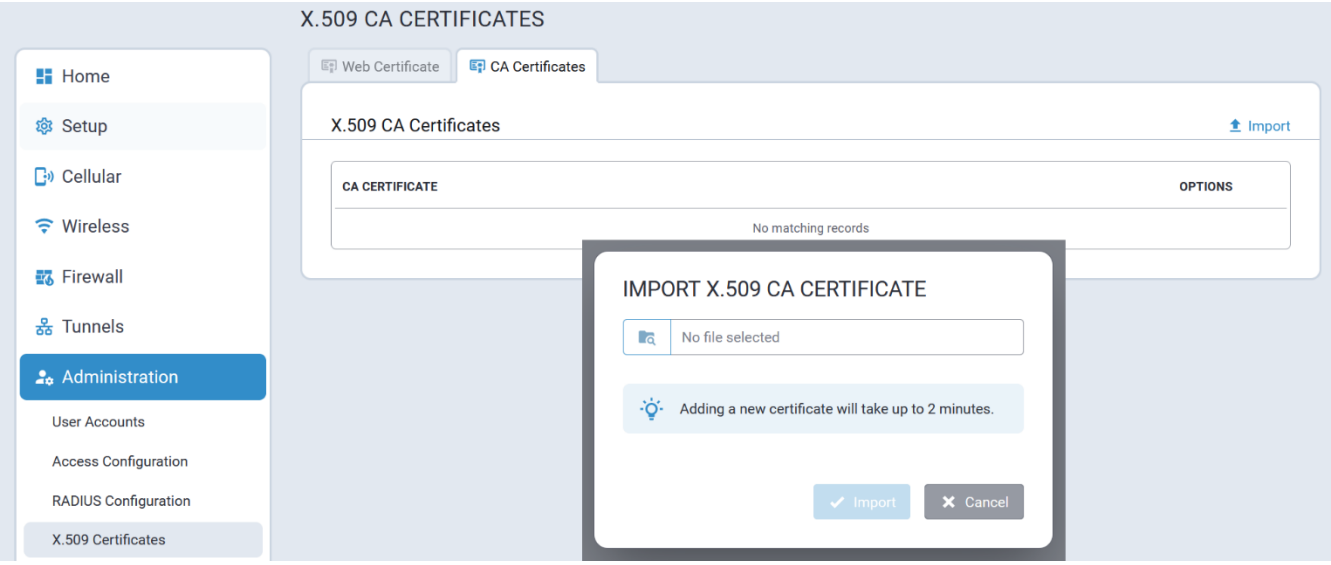
A typical Web Certificate tab is illustrated here:



CA Certificates Tab

The system supports importing X.509 CA Certificates. Imported certificates must be in **.pem** format.

A typical CA Certificates tab is illustrated here:

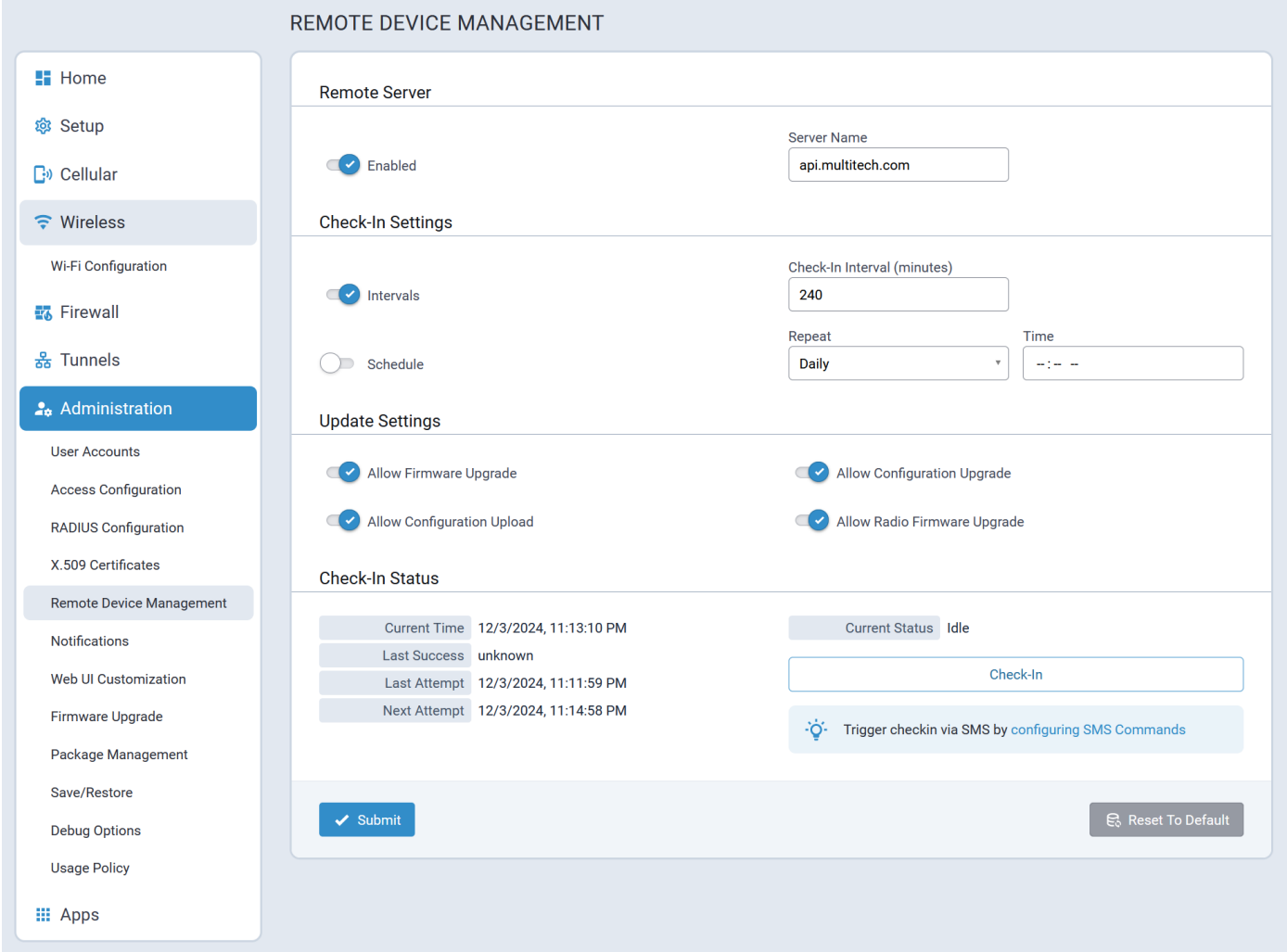


Remote Device Management Tab

The following Remote Device Management operations are supported:

- Check-in based on a specified interval, and repeated at a particular time and day(s) of the week
- Upload device configuration to the remote server
- Commands execution:
  - Configuration upgrade
  - Firmware upgrade
  - Device Logs Upload
  - Reboot

A typical Remote Device Management tab is illustrated here:



Notifications

The Notification tab includes settings for users to manage the following:

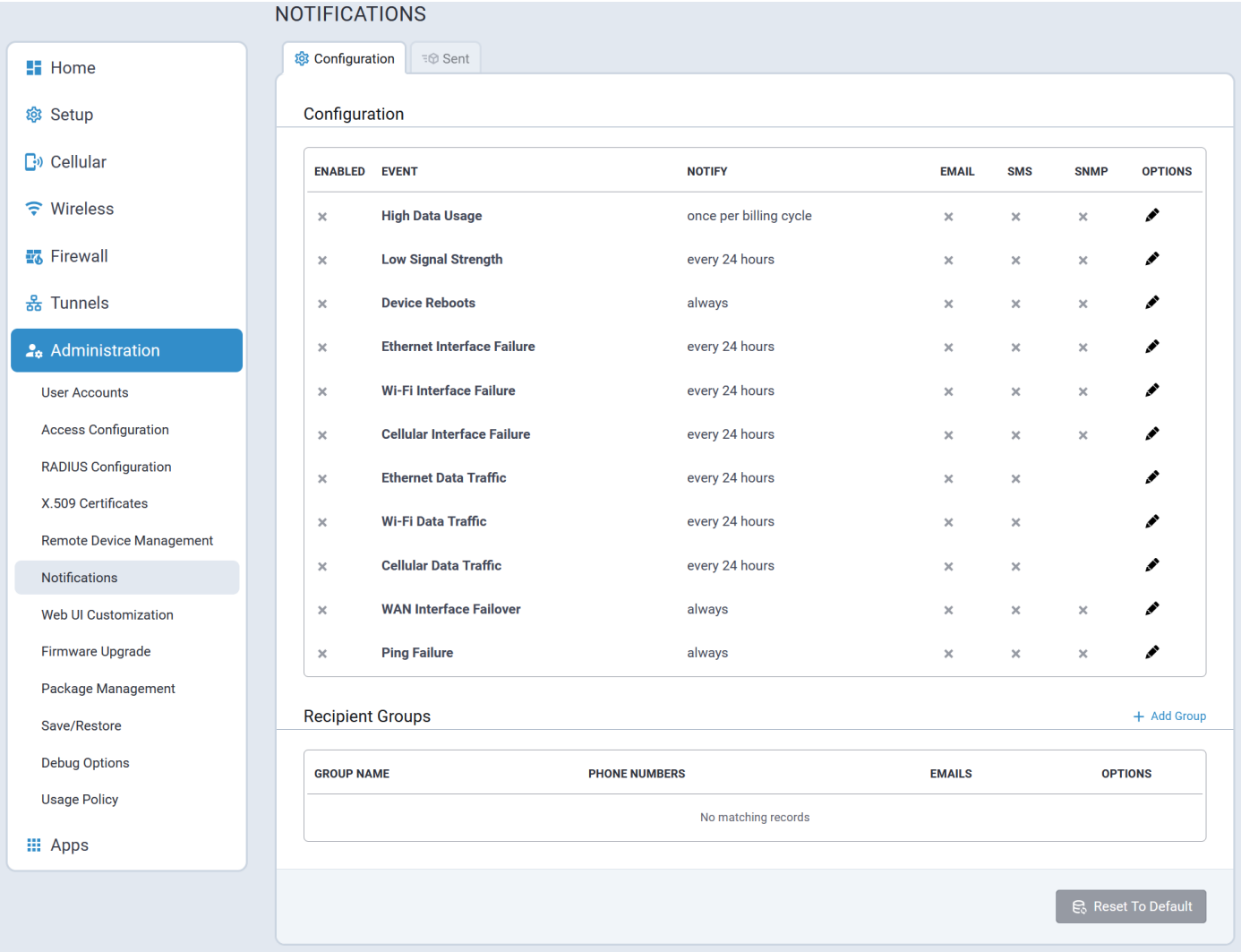
- Notifications Configuration
- Notifications Sent

The device can send alerts via:

- email
  To send alerts via email, the SMTP server must be enabled.
- SMS
  To send alerts via SMS, refer to SMS Configuration and Commands.
- SNMP
  To enable SNMP traps, refer to SNMP Configuration.

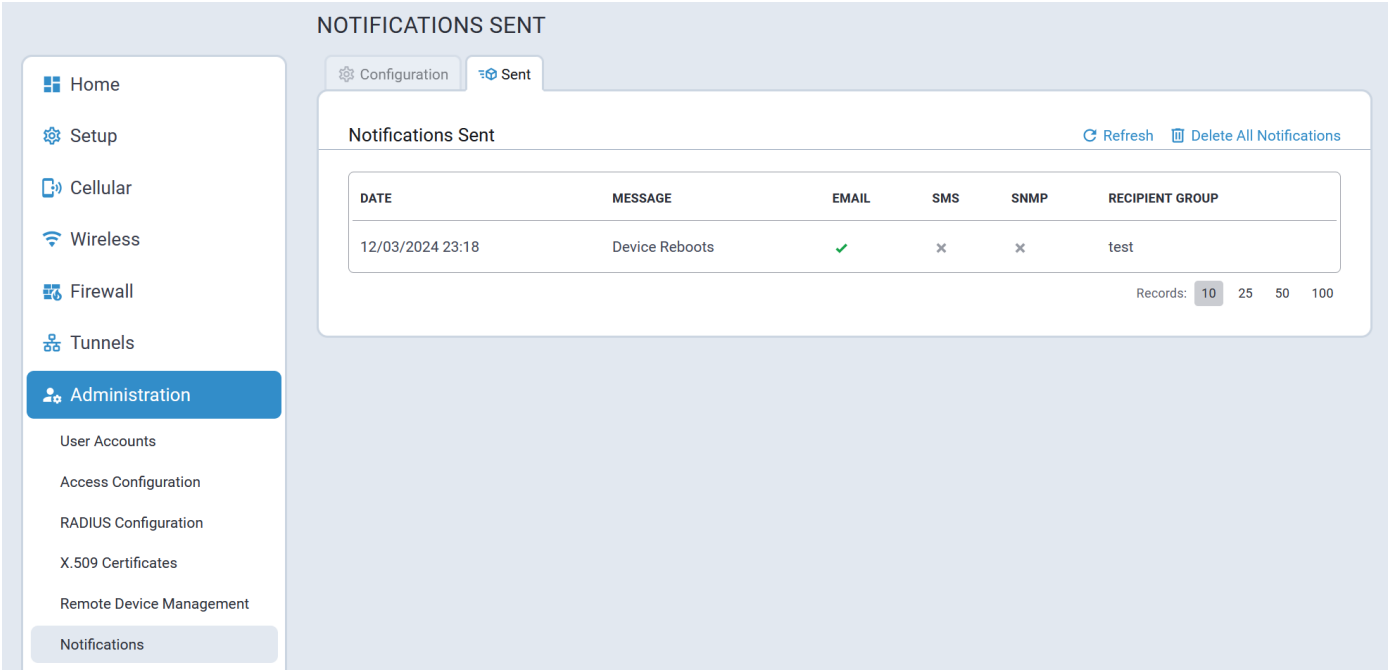
Configuration Tab

A typical Configuration tab for notifications is illustrated here:



Sent Tab

A typical Sent tab for notifications is illustrated here:

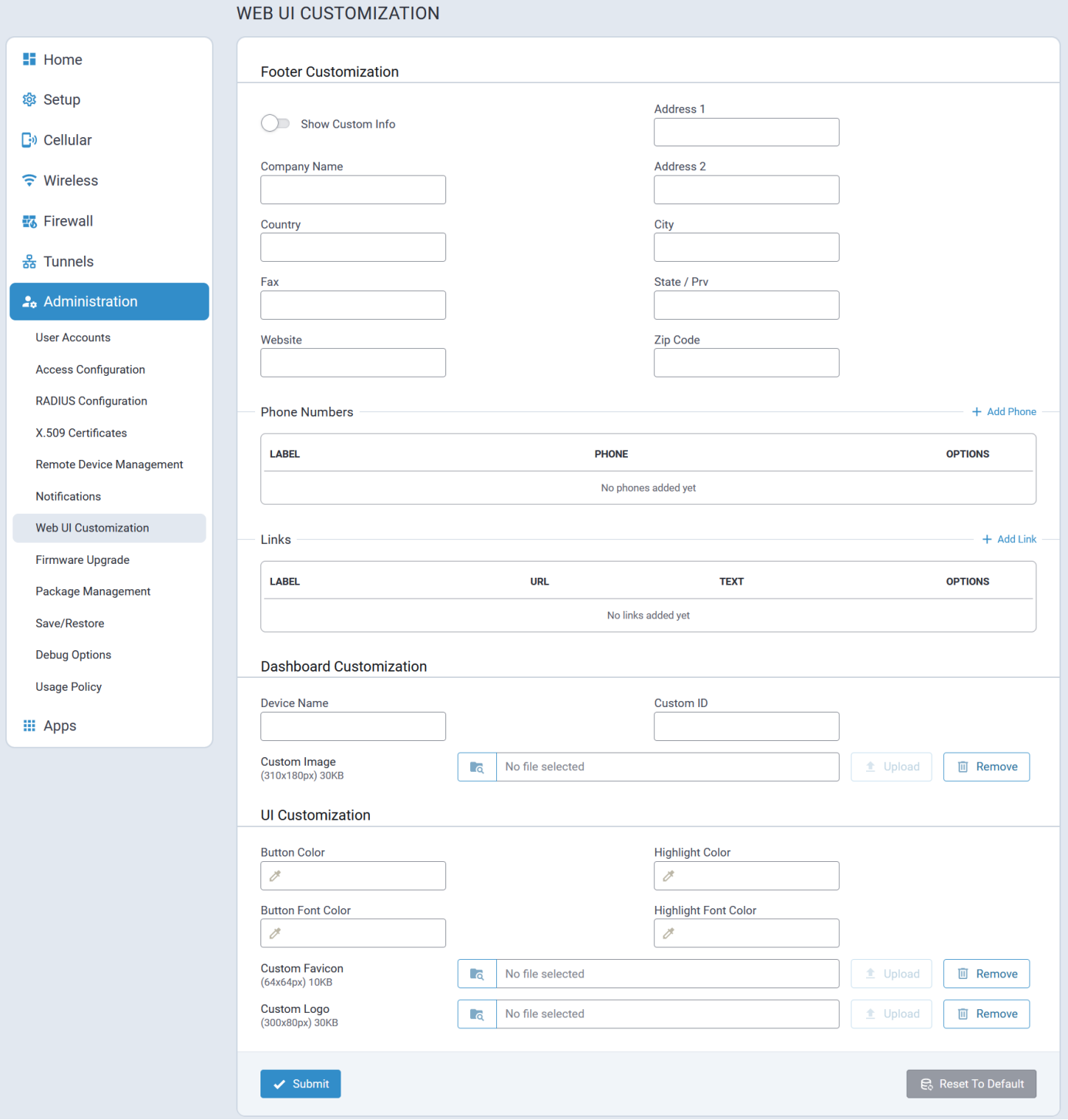


Web UI Customization

Users can configure the following on the Web UI Customization tab:

- Footer Customization allows the user to add custom organization details to the footer.
- Dashboard Customization allows the user to upload a new image and specify Device Name and Custom ID that will be shown on the Dashboard page.
- UI Customization allows the user to modify the color schema of the buttons, and upload a custom logo and favicon.

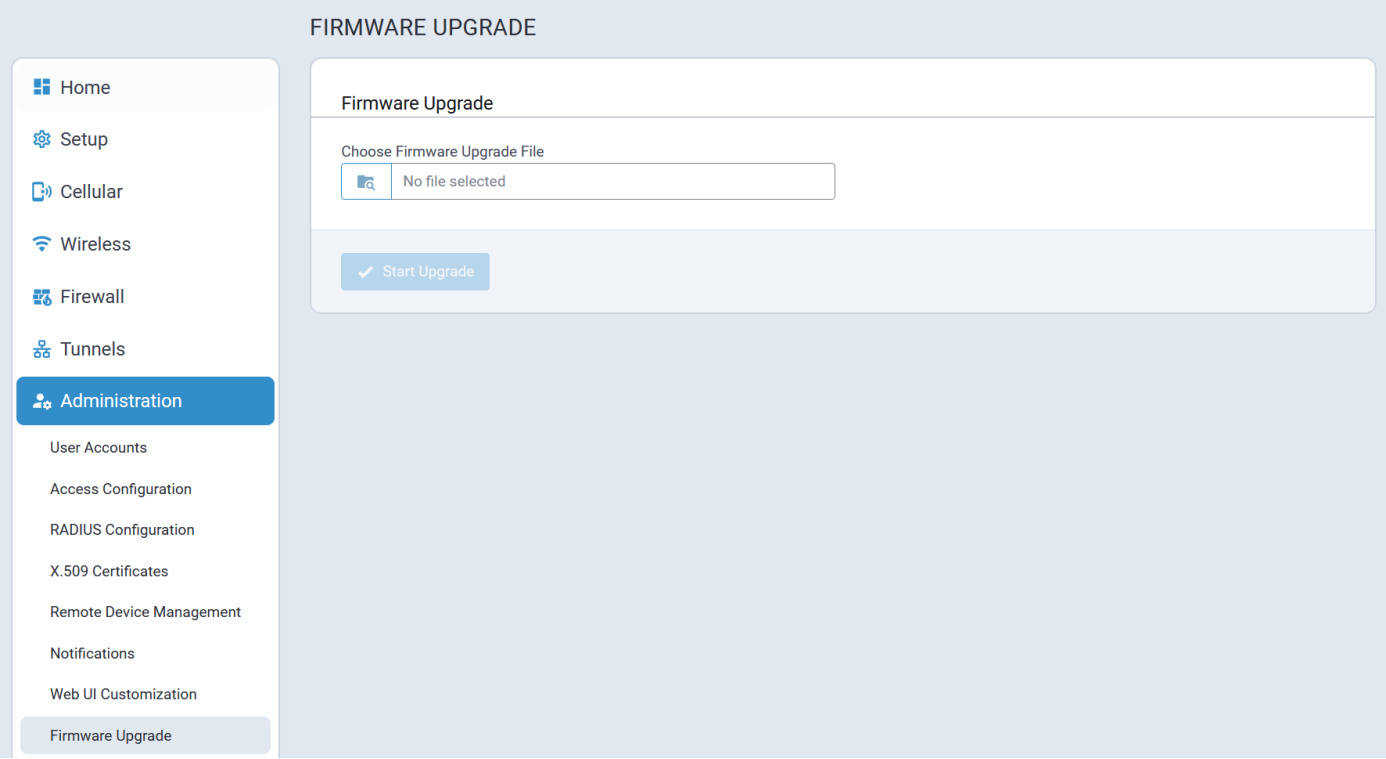
A typical Web UI Customization tab is illustrated here:



Firmware Upgrade

Firmware from MultiTech is signed by MultiTech's private key and the signatures on the artifacts in the firmware must verify successfully for the firmware to be applied to the device flash.

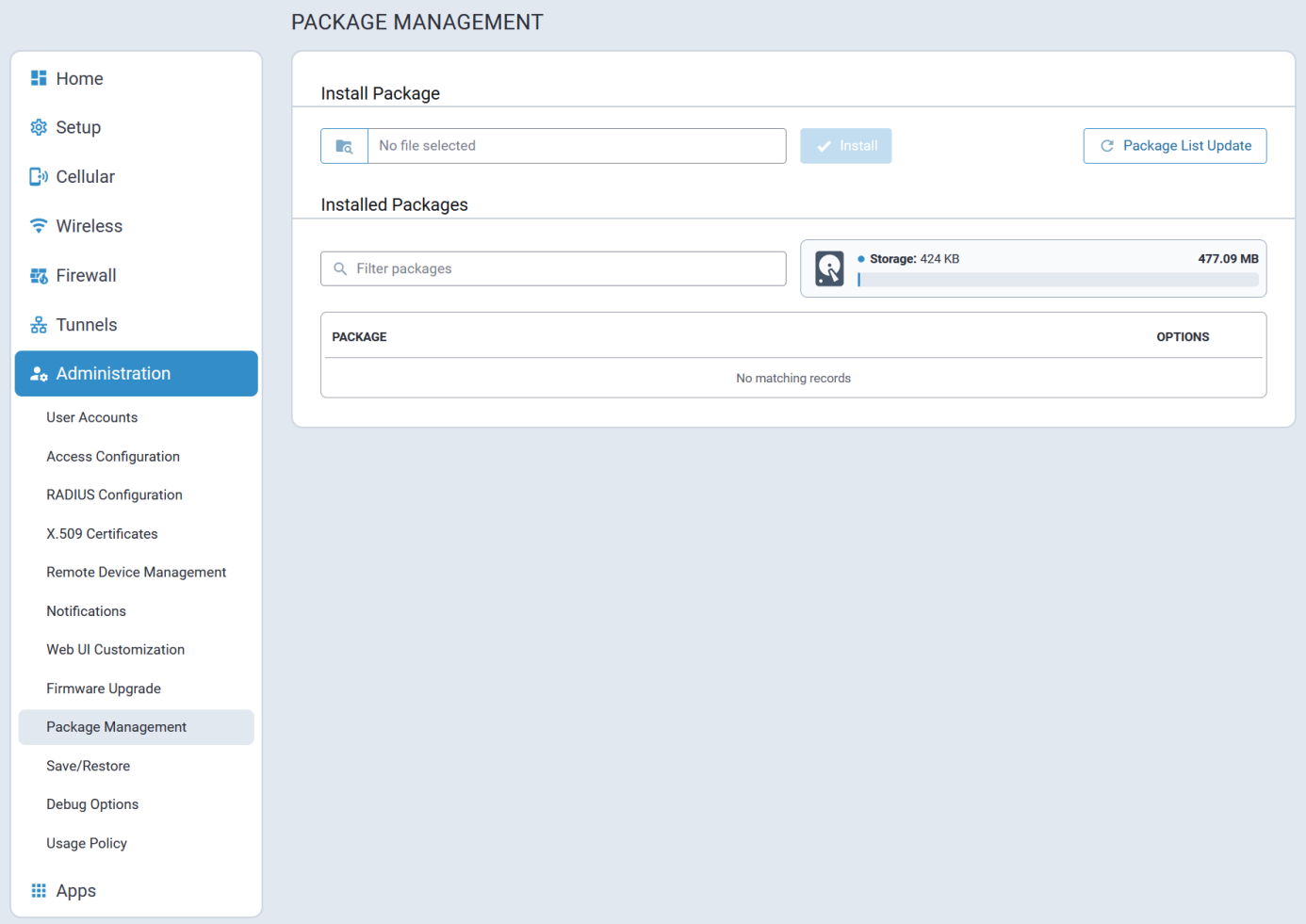
A typical Firmware Upgrade tab is illustrated here:



Package Management

The Package Management feature supports importing and installing packages from the MultiTech online mLinux feeds.

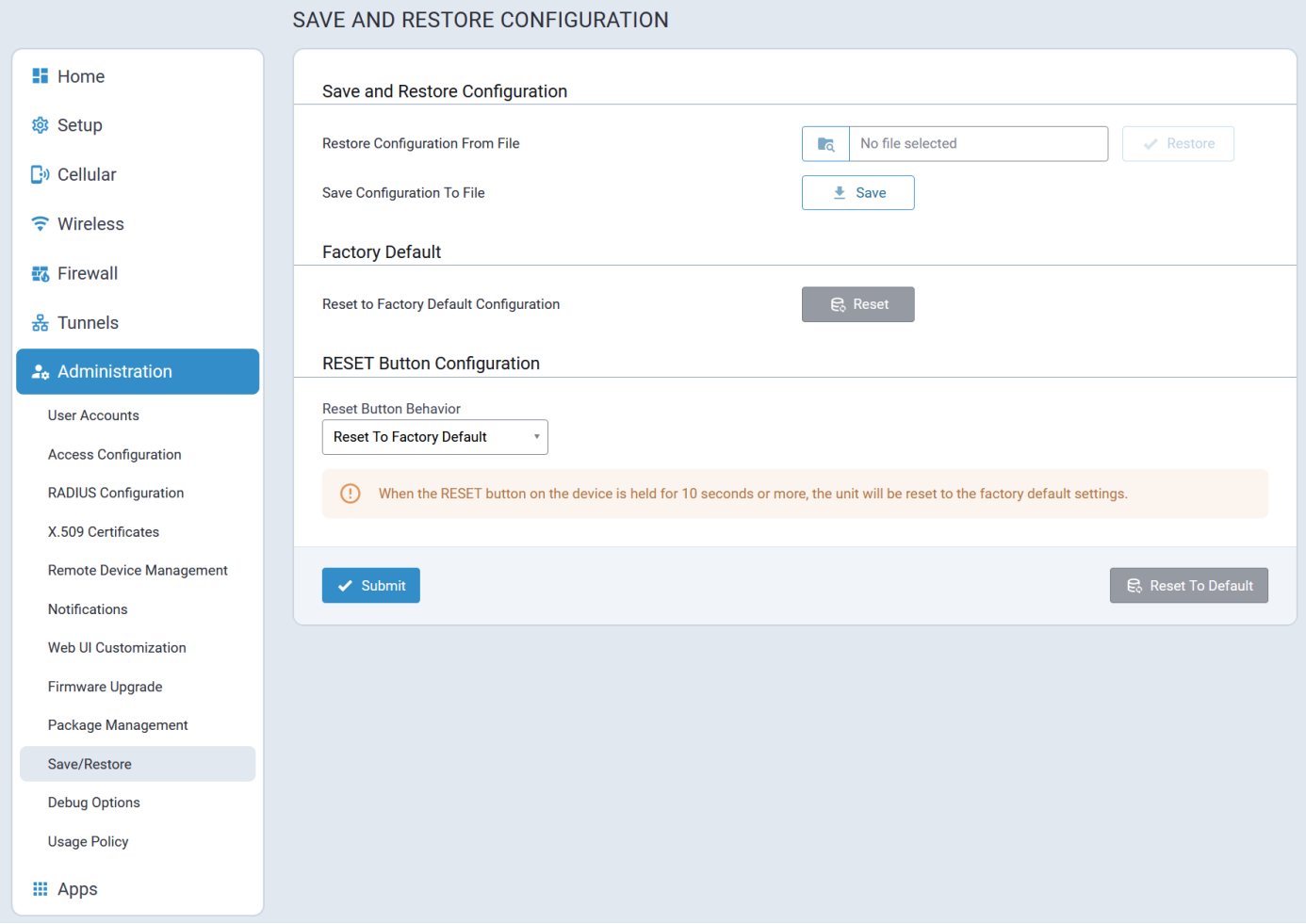
A typical Package Management tab is illustrated here:



Save/Restore

Save/Restore supports restoring from a uploaded configuration file, saving the current configuration to a file, and defaulting the device back to factory settings. The RESET button can be configured to enable it, disable it, or disable factory reset so that the device only resets when the button is pressed.

A typical Save/Restore tab is illustrated here:

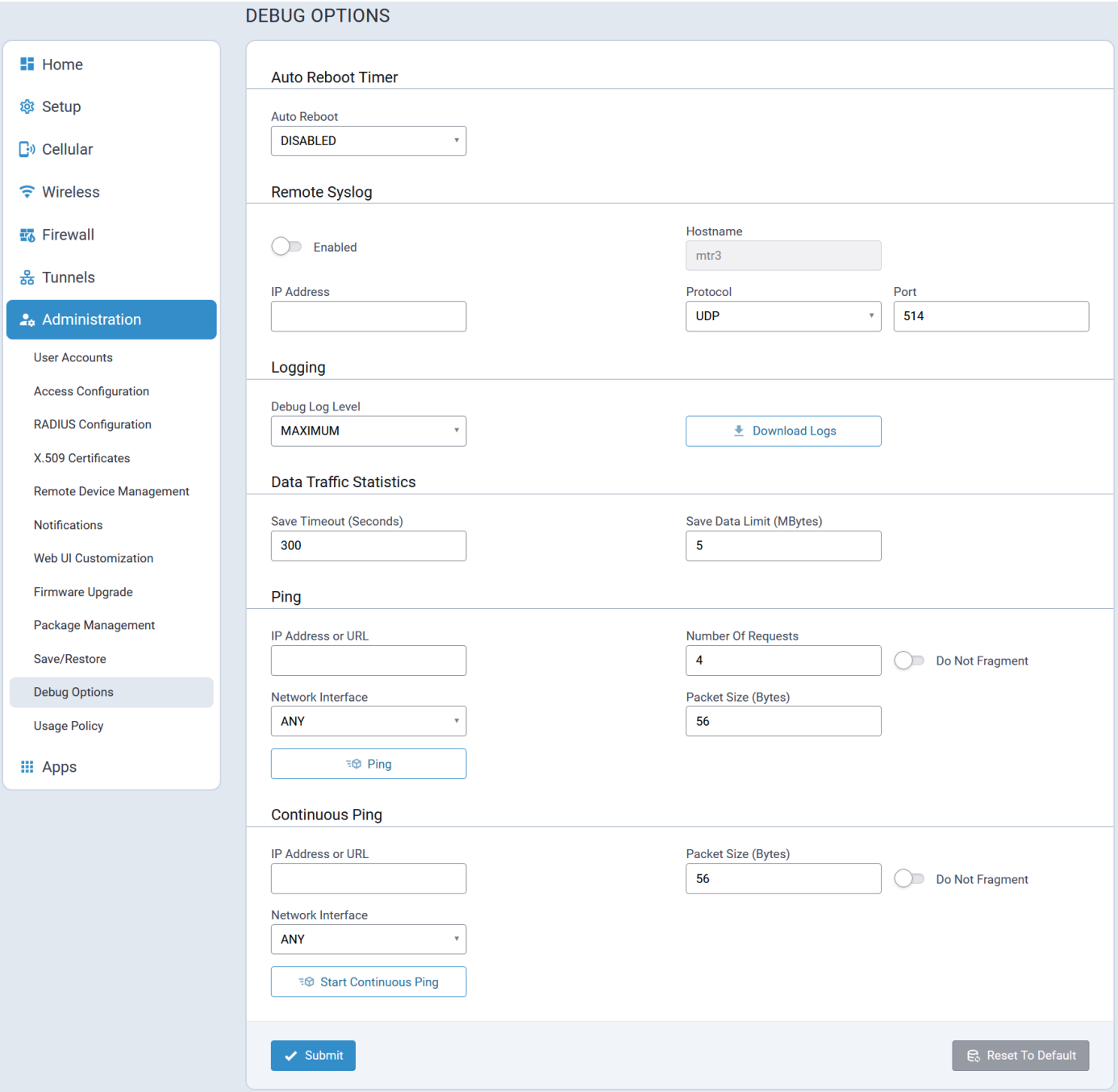


Debug Options

The Debug Options tab contains a miscellaneous set features and options for debugging and rebooting the device:

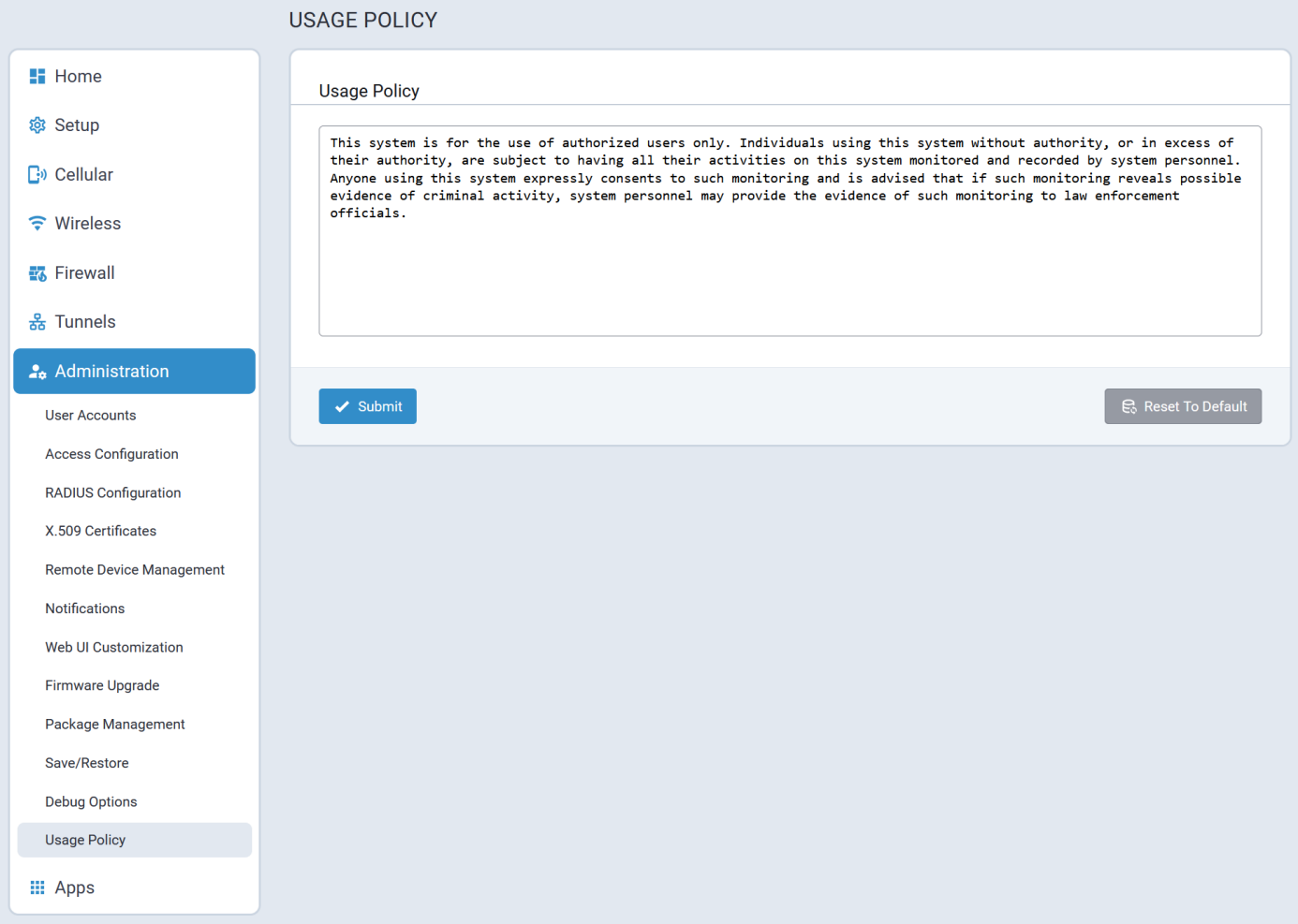
- When enabled, the Auto Reboot Timer feature will reboot per the configured timeout.
- When enabled and configured, the Remote Syslog feature will stream the syslog output to the remote server.
- Logging is a global setting to increase or decrease the device logging level.
- The Data Traffic Statistics feature controls the periodicity and data threshold when statistics are saved to persistent storage.
- The Ping feature pings or connects via TCP to the target remote host.
- The Continuous Ping feature pings the target remote host continuously.

A typical Debug Options tab is illustrated here:



Usage Policy

A typical Usage Policy tab is illustrated here:



Apps Menu

Custom Apps

The system allows installing custom applications and uploading configuration files for the installed custom apps.

For details regarding custom application creation, refer to: https://www.multitech.net/developer/software/aep/creating-a-custom-application/.

The **Backup On Install** setting is enabled by default. When enabled, the currently running custom application is backed up in case a new version of the application is being downloaded and installed. If the install fails, the backup is reinstalled. Disable this option only if there is not enough space to backup custom apps.

When **Enabled** is on (in the right-most position):

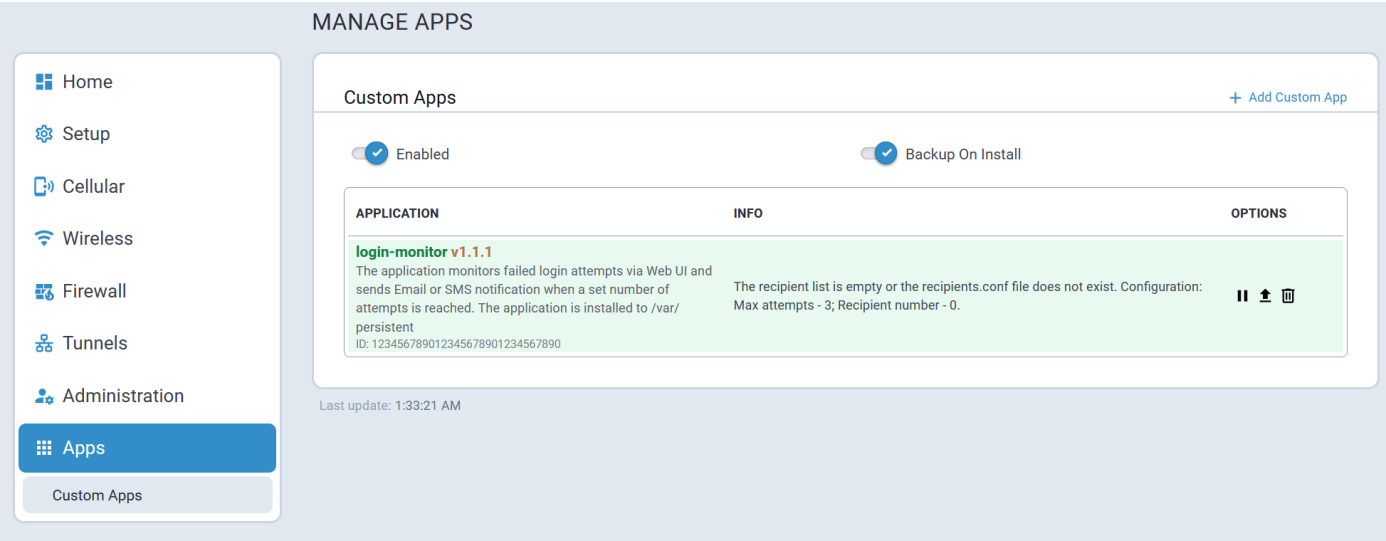
- The system launches all installed custom application on boot.
- The system launches a custom application as soon as it has been installed.

When **Enabled** is off (in the left-most position):

- The system does not launch custom application that are installed. The Run action icon is not available on UI and user cannot run the application manually.
- The system allows the installation of custom applications, but it does not launch them.
- The system does not allow starting applications.

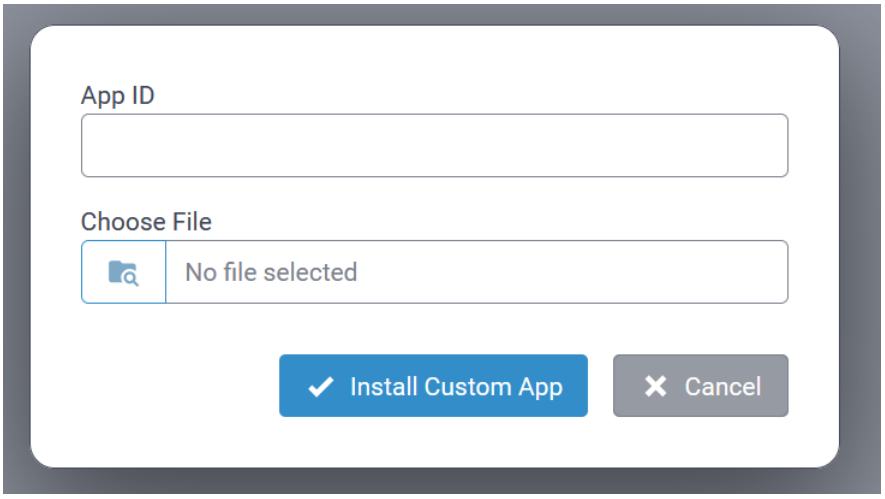
When a user disables the Enabled option and selects **Save and Apply**, the system does not stop applications that are running. A user can stop the running application manually by selecting the stop action button, in which case the run action button will not be available.

A typical Custom Apps tab is illustrated here:



To install a custom application:

1. Go to the Custom Apps page, select **Add Custom App**.
2. Specify an App ID and an choose an application file in the pop up. The App ID must be a hexadecimal value with a maximum length of 32 characters.



When adding a custom app, the following information applies:

- The application name must be unique. The system does not allow installing two different apps with the same name. The system retrieves the **App Name** value from the **manifest.json**.
- The installed application has a corresponding unique App ID. When installing an app, the system verifies if the app with the same name is already installed. If this is true, the system does not allow specifying a different App ID.
- If a user installs a new version of the application that is already installed, the user has to specify the App ID of the installed application. If the user specifies a different App ID, the application installation will fail and corresponding error message will be displayed.
- When installing an app, the system does not allow specifying an App ID that is already used by another application.

When the application is installed, the system displays its name, description, version, ID, current status, and application information.

The application statuses are:

- STARTED: The application is highlighted with green and there is a stop action in the Options column
- RUNNING: The application is highlighted with green and there is a stop action in the Options column
- STOPPED: The application is not highlighted and there is a start action in the Options column
- FAILED: The application is highlighted with red and the actual status is shown next to the app version
- INSTALL FAILED: The application is highlighted with red and the actual status is shown next to the app version
- START FAILED: The application is highlighted with red and the actual status is shown next to the app version

Installation Location

The location where the system installs a custom application is defined in the manifest.json file. The application can be installed to /var/config/app, /var/persistent, or to the SD card.

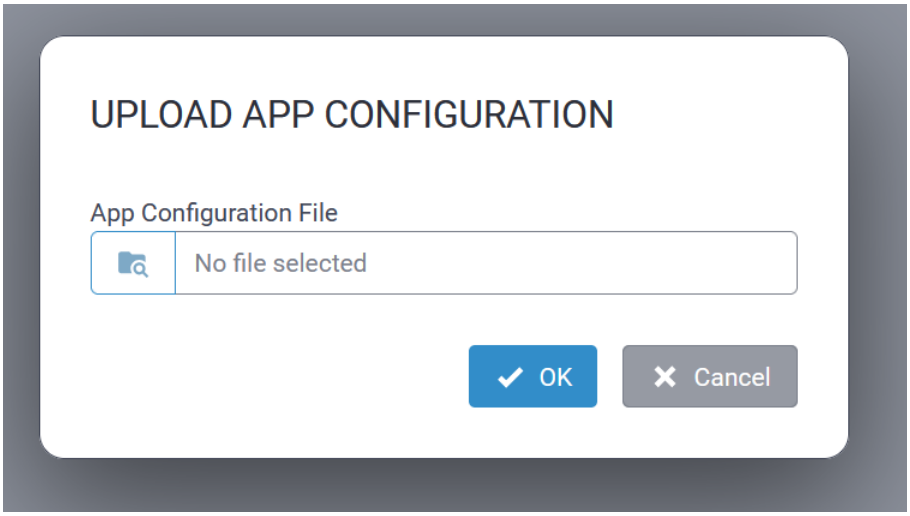
To install the application to /var/persistent, the manifest.json file shall have the “PersistentStorage” field set to true. If it is absent or set to false, then the app will be installed to the **/var/config/app** directory.

Example:

```
{
  "AppName": "Application Name" ,
  "AppVersion": "Application Version" ,
  "AppDescription": "Description to be displayed for the custom app",
  "AppVersionNotes":"Any applicable notes for this version of the app.",
  "PersistentStorage": true
}
```

The system allows uploading one or more configuration files for the installed custom application.

To upload a new configuration file, select the Upload App Configuration icon in the Actions column.



The files will be uploaded to the **/[AppName]/config** directory.

Note:

- If the /[AppName]/config directory does not exist, the system will create a “config” directory in the application directory.
- You have to specify files with a correct file name that the application supposes to use. If the application uses **general.conf**, and you upload **general_v1.conf** and **general_v3.conf**, all these files will be present in the /config directory, and it depends on the app how to use them. If the file name of the file you upload corresponds to a file from the /config directory, new file will replace the existing one.

Send Notification Utility

The “send-notification” utility is a simple method for users to send notifications via SMS and email.

```
root@mtcap3:/usr/bin# send-notification --help
Send notification utility v.1.0-3-gebcac32
Usage:
  send-notification -r <recipient> [-r <recipient> ...] [-s <subject>] -m <message>
Options:
  -r, --rcpt <recipient>  Recipient
  -s, --subj <subject>    Message subject
  -m, --msg <message>     Message body
  -v, --ver               Print version and exit
  -h, --help              Print this help and exit

root@mtcap3:/usr/bin#
```

4 Cellular IP Passthrough Mode

In **Cellular IP Passthrough mode**, the rCell 300 is configured to negotiate a cellular data link and an IP address is directly linked to a connected device.

Note: Not all routing and firewall features are available in Cellular IP Passthrough Mode.

Enable IP Passthrough Mode

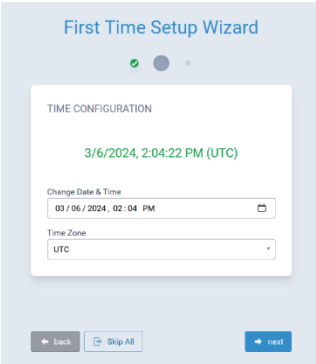
Once the rCell 300 has been successfully commissioned, the **First Time Setup Wizard** is automatically launched and Cellular IP Passthrough Mode may be configured.

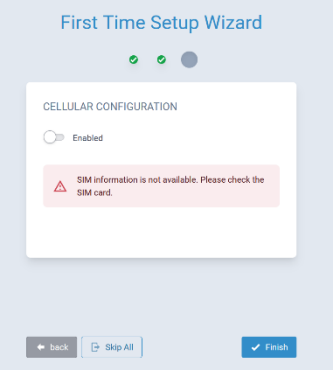
1. Expand the **Mode** pull-down list and, select **Cellular IP Passthrough**.
2. Select **next**.
3. Configure the **Date and Time** and select the appropriate **Time Zone** for the location where the rCell 300 is to be located.

   Note: Because the system does not have an Internet connection in this mode, the automatic synchronization of system time is not supported.
4. Select **next**.

There are three screens in the First Time Setup Wizard in the Cellular IP Passthrough mode:

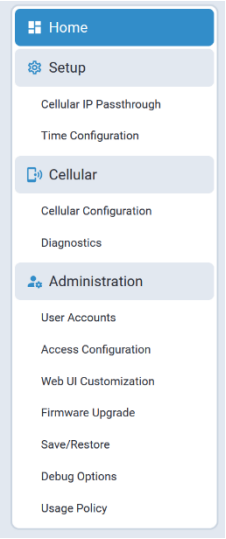
- Mode selection
- Time Configuration
- Cellular Configuration (the page content depends on the presence of a SIM card in the SIM1 slot)





1. Install a SIM card in the SIM1 slot.
2. Enter the correct date and time on the **TIME CONFIGURATION** dialog and select Next.
3. On the **CELLULAR CONFIGURATION** dialog slide the **Enabled** slider to the right to enable cellular mode.
4. Enter PIN, if necessary.
5. Enter APN, if necessary.
6. Select **Finish**.
7. Click **Save and Apply**. The system will reboot to apply the changes. Once restarted, the rCell 300 will begin operating in Cellular IP Passthrough mode.

The following configuration pages are available in the Cellular IP Passthrough Mode:



- Home
  - Dashboard
  - Statistics (System, Ethernet, Cellular)
- Setup
  - Cellular IP Passthrough
  - Time Configuration

- Cellular
  - Cellular Configuration (Cellular Configuration and Cellular Profiles)
  - Diagnostics (Radio Status, Diagnostics, Cell Radio Firmware Upgrade)
- Administration
  - User Accounts (Users, Add User, Password Complexity Rules)
  - Access Configuration
  - Web UI Configuration
  - Firmware Upgrade
  - Save/Restore
  - Debug Options
  - Usage Policy

Use Case Configuration

Cellular IP Passthrough mode can be configured to support IPv4 and IPv6, DNS, and different netmasks for the connected device. Refer to the following table for information about configuring various Use Cases.

Note: A working Cellular connection is required.

Use Case	Configuration	Expected Behavior
1	Protocol Support: IPv4 IPv4 DNS Server: empty Public IPv4 Mask: 32	▪ The system obtains the network settings from the rCell 300 and cellular network. ▪ When the Internet (cellular) connection is NOT established, the IPv4 Address is assigned from the local subnet (192.168.2.0/24 by default). ▪ IPv4 Default Gateway and IPv4 DHCP Server correspond to the IPv4 Address of the rCell 300. ▪ When the Internet (cellular) connection is established, the IPv4 Address corresponds to the IP Address that the cellular network provided. ▪ The IPv4 DNS Server address(es) are obtained from the cellular network. ▪ There is an Internet connection on the user's computer that is connected to the rCell 300. ▪ Ping to **google.com** from the user's computer is successful. ▪ The mPower Web UI is accessible via the IPv4 address that is configured on the Cellular IP Passthrough Configuration page. ▪ Identical behavior is observed when the user's computer is connected to the rCell 300 via the ETH0 and ETH1 ports. Both ethernet ports work the same.

Use Case	Configuration	Expected Behavior
2	Protocol Support: IPv4 IPv4 DNS Server: 8.8.8.8 Public IPv4 Mask: 32	▪ The system obtains the network settings from the rCell 300 and cellular network. ▪ When the Internet (cellular) connection is NOT established, the IPv4 Address is assigned from the local subnet (192.168.2.0/24 by default). ▪ IPv4 Default Gateway and IPv4 DHCP Server correspond to the IPv4 Address of the rCell 300. ▪ When the Internet (cellular) connection is established, the IPv4 Address corresponds to the IP Address that the cellular network provided. ▪ The IPv4 DNS Server address is **8.8.8.8**. ▪ There is an Internet connection on the user's computer that is connected to the rCell 300. ▪ Ping to **google.com** from the user's computer is successful. ▪ The mPower Web UI is accessible via the IPv4 address that is configured on the Cellular IP Passthrough Configuration page. ▪ Identical behavior is observed when the user's computer is connected to the rCell 300 via the ETH0 and ETH1 ports. Both ethernet ports work the same.
3	Protocol Support: IPv4 IPv4 DNS Server: empty Public IPv4 Mask: 24	▪ The system obtains the network settings from the rCell 300 and cellular network. ▪ When the Internet (cellular) connection is NOT established, the **IPv4 Address** is assigned from the local subnet (192.168.2.0/24 by default). ▪ **IPv4 DHCP Server** corresponds to the IPv4 Address of the rCell 300. ▪ When the Internet (cellular) connection is established, the IPv4 Address corresponds to the IP Address that the cellular network provided. ▪ **IPv4 Default Gateway** is obtained from the cellular network ▪ The **IPv4 DNS Server** addresses are obtained from the Cellular network. ▪ There is an Internet connection on the user's computer that is connected to the rCell 300. ▪ Ping to **google.com** from the user's computer is successful. ▪ The mPower Web UI is accessible via the IPv4 address that is configured on the Cellular IP Passthrough Configuration page. ▪ Identical behavior is observed when the user's computer is connected to the rCell 300 via the ETH0 and ETH1 ports. Both ethernet ports work the same.

Use Case	Configuration	Expected Behavior
4	Protocol Support: IPv4 IPv4 DNS Server: 8.8.4.4 Public IPv4 Mask: 24	▪ The system obtains the network settings from the rCell 300 and cellular network. ▪ When the Internet (cellular) connection is NOT established, the **IPv4 Address** is assigned from the local subnet (192.168.2.0/24 by default). ▪ **IPv4 DHCP Server** corresponds to the IPv4 Address of the rCell 300. ▪ When the Internet (cellular) connection is established, the IPv4 Address corresponds to the IP Address that the cellular network provided. ▪ **IPv4 Default Gateway** is obtained from the cellular network ▪ The **IPv4 DNS Server** address is **8.8.4.4** ▪ There is an Internet connection on the user's computer that is connected to the rCell 300. ▪ Ping to **google.com** from the user's computer is successful. ▪ The mPower Web UI is accessible via the IPv4 address that is configured on the Cellular IP Passthrough Configuration page. ▪ Identical behavior is observed when the user's computer is connected to the rCell 300 via the ETH0 and ETH1 ports. Both ethernet ports work the same.

Use Case	Configuration	Expected Behavior

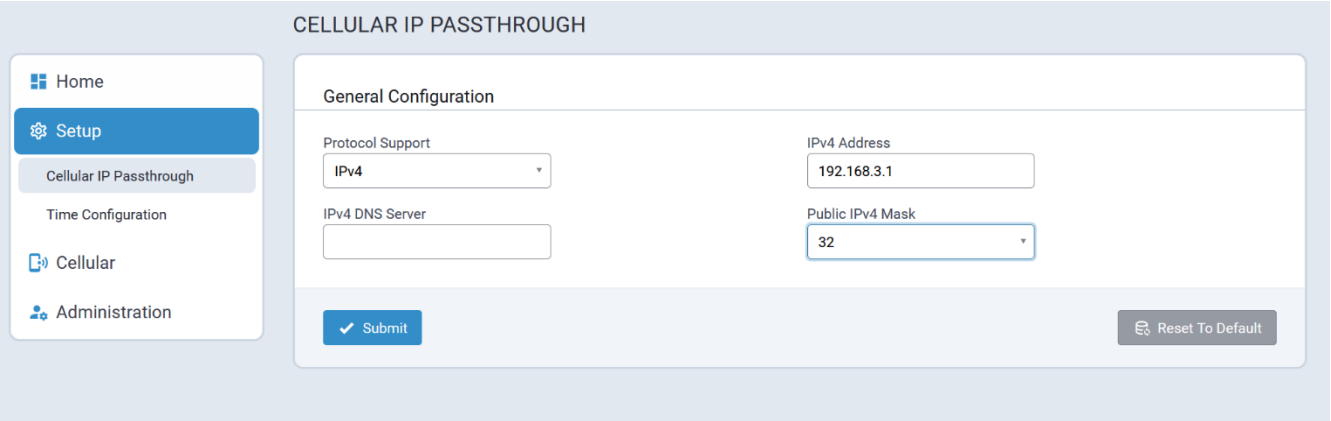
6	Protocol Support: IPv6
	IPv6 DNS Server: empty
		▪ The system obtains the network settings from the rCell 300 and cellular network.
		▪ IPv4 Address is obtained from the local IPv4 subnet of the rCell 300.
		▪ IPv4 Default Gateway and IPv4 DHCP Server correspond to the IPv4 IP Address of the rCell 300.
		When the Internet (cellular) connection is established:
		▪ The IPv6 Address on the Dashboard corresponds to the br0 network interface IPv6 address (issue **ifconfig** in the device console to see the **inet6 addr** for **br0**).
		▪ The device Web UI can be accessed via the IPv6 address.
		Example: https://[fe80::58a1:b3ff:febc:ca86]/
		▪ The ethernet interface on the user's PC obtains the following IPv6 network settings from the cellular network:
		  ▪ IPv6 Address
		  ▪ IPv6 Default Gateway
		  ▪ IPv6 DNS Servers
		▪ There is an Internet connection on the user's computer that is connected to the rCell 300.
		▪ Ping to **ipv6.google.com** from the user's computer is successful.
		▪ The mPower Web UI is accessible via the IPv4 address that is configured on the Cellular IP Passthrough Configuration page.
		▪ Identical behavior is observed when the user's computer is connected to the rCell 300 via the ETH0 and ETH1 ports. Both ethernet ports work the same.

Use Case	Configuration	Expected Behavior

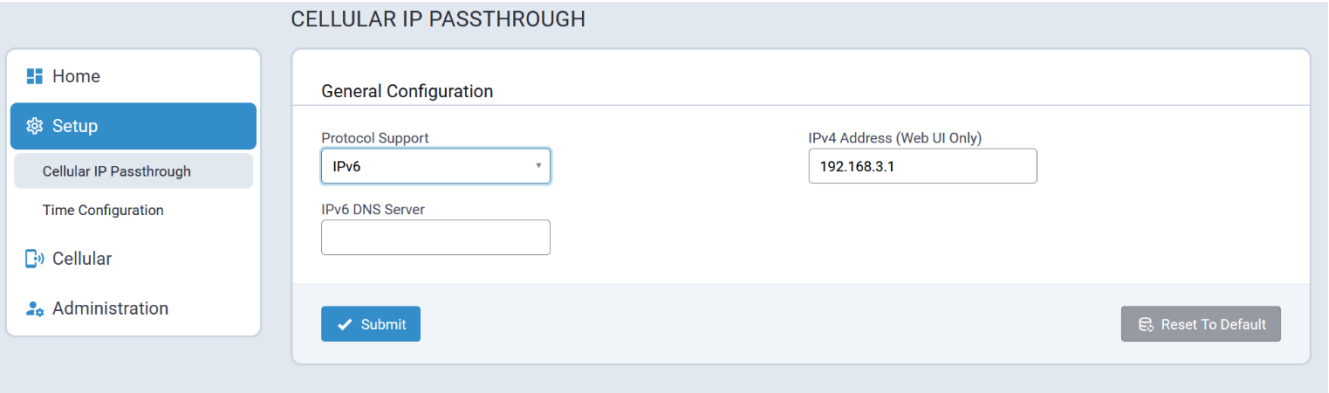
7	Protocol Support: IPv6
	IPv6 DNS Server:
	2001:4860:4860::8888
		▪ The system obtains the network settings from the rCell 300 and cellular network.
		▪ IPv4 Address is obtained from the local IPv4 subnet of the rCell 300.
		▪ IPv4 Default Gateway and IPv4 DHCP Server correspond to the IPv4 IP Address of the rCell 300.
		When the Internet (cellular) connection is established:
		▪ The IPv6 Address on the Dashboard corresponds to the br0 network interface IPv6 address (issue **ifconfig** in the device console to see the **inet6 addr** for **br0**)
		▪ The device Web UI is accessible via the IPv6 address.
		Example: https://[fe80::58a1:b3ff:febc:ca86]/
		▪ The ethernet interface on the user's PC obtains the following IPv6 network settings from the cellular network:
		  ▪ IPv6 Address
		  ▪ IPv6 Default Gateway
		▪ The IPv6 DNS Server is **2001:4860:4860::8888** .
		▪ There is an Internet connection on the user's computer that is connected to the rCell 300.
		▪ Ping to **ipv6.google.com** from the user's computer is successful.
		▪ The mPower Web UI is accessible via the IPv4 address that is configured on the Cellular IP Passthrough Configuration page.
		▪ Identical behavior is observed when the user's computer is connected to the rCell 300 via the ETH0 and ETH1 ports. Both ethernet ports work the same.

Cellular IP Passthrough

An example for setting up the Cellular IP Passthrough configuration for IPv4 is illustrated here:

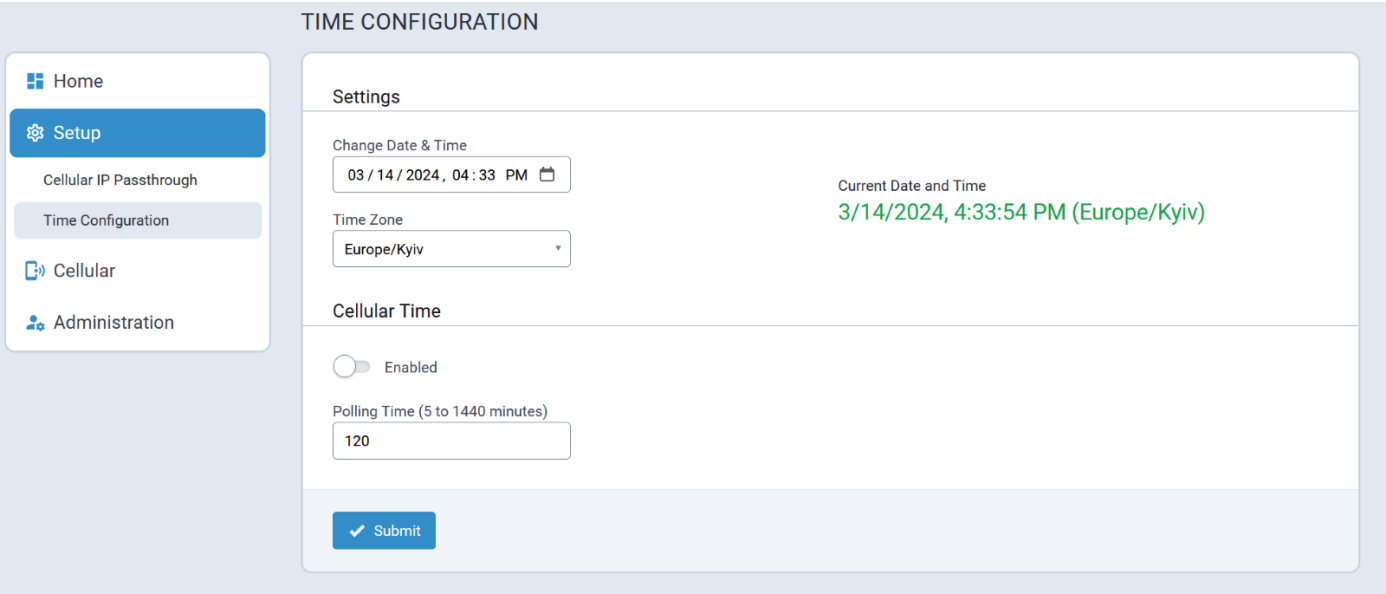


An example for setting up the Cellular IP Passthrough configuration for IPv6 is illustrated here:



Time Configuration

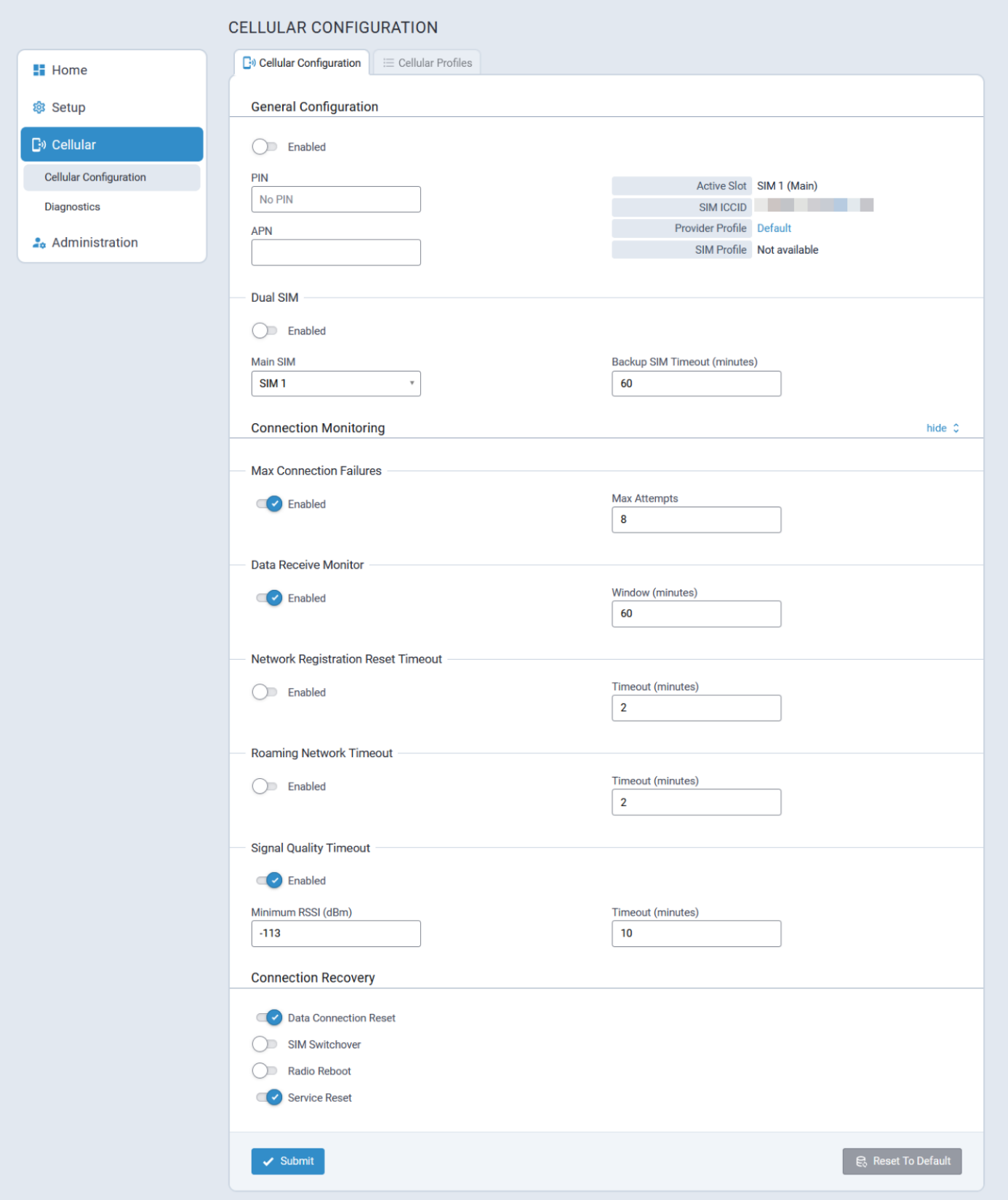
An example of the Time Configuration settings is illustrated here:



Cellular Configuration

In Cellular IP Passthrough mode, the Keep Alive feature is not supported and not present in the Connection Monitoring section. The rest of the Connection Monitoring features are available and operate the same way they work in the Network Router mode.

The Cellular Configuration tab in Cellular IP Passthrough mode is illustrated here:


CELLULAR CONFIGURATION
Home
Setup
Cellular
Cellular Configuration
Diagnostics
Administration
Cellular Configuration
Cellular Profiles
General Configuration
Enabled
PIN
No PIN
APN
Active Slot
SIM 1 (Main)
SIM ICCID
Provider Profile
Default
SIM Profile
Not available
Dual SIM
Enabled
Main SIM
SIM 1
Backup SIM Timeout (minutes)
60
Connection Monitoring
hide
Max Connection Failures
Enabled
Max Attempts
8
Data Receive Monitor
Enabled
Window (minutes)
60
Network Registration Reset Timeout
Enabled
Timeout (minutes)
2
Roaming Network Timeout
Enabled
Timeout (minutes)
2
Signal Quality Timeout
Enabled
Minimum RSSI (dBm)
-113
Timeout (minutes)
10
Connection Recovery
Data Connection Reset
SIM Switchover
Radio Reboot
Service Reset
Submit
Reset To Default

Warranty

To read the warranty statement for your product, go to https://www.multitech.com/warranty.

Contact Information

General Information	info@multitech.com https://multitech.com/contact-us/
Sales	+1 (763) 785-3500 sales@multitech.com
Technical Support Portal	+1 (763) 717-5863 https://support.multitech.com
Website	www.multitech.com
World Headquarters	2205 Woodale Drive Mounds View, MN 55112 USA

Revision History

Revision Number	Description	Revision Date
1.0	This is the initial release of the rCell 300 Configuration Guide.	April 2025