



# Conduit® AP Configuration Guide

---

Using mPower™ Edge Intelligence (v7.1.0)

## Conduit® AP Configuration Guide

This document applies to all models and regions on the device overview page. Go to <https://multitech.com/all-products/cellular/cellular-gateways/conduit-ap-300-series/#models>.

Document Part Number: S000831 Rev 1.0

## Copyright

This publication may not be reproduced, in whole or in part, without the specific and express prior written permission signed by an executive officer of Multi-Tech Systems, Inc. All rights reserved. **Copyright © 2025 by Multi-Tech Systems, Inc.**

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

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

## Trademarks

Multi-Tech and the Multi-Tech logo, DeviceHQ, SocketModem, and Conduit are registered trademarks of Multi-Tech Systems, Inc.

mPower, mCard, and mDot are trademarks of Multi-Tech Systems, Inc.

All other brand and product names are trademarks or registered trademarks of their respective companies.

## 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.

MULTITECH DOES NOT WARRANT THAT THE TRANSMISSION OF DATA BY A PRODUCT OVER A WIRELESS COMMUNICATIONS NETWORK WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE, NOR DOES MULTITECH WARRANT ANY CONNECTION OR ACCESSIBILITY TO ANY WIRELESS 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 WIRELESS 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

<b>1 Introduction.....</b>	<b>8</b>
Intended Audience .....	8
About the Conduit AP 300 .....	8
Intended Use.....	8
mPower™ Edge Intelligence .....	8
<b>2 Getting Started.....</b>	<b>9</b>
Installing a SIM Card.....	9
Removing a SIM Card .....	10
Attaching the Antenna .....	10
Cabling the Device.....	10
Commissioning Mode.....	11
Configure the Administrative User .....	11
First Time Setup Wizard .....	12
Configure Network Router Mode .....	12
Commissioning an Ethernet-Only MTCAP3 .....	13
Network Configuration .....	13
Locating the Device's IP Address .....	14
Connecting to the Device .....	14
<b>3 mPower Configuration Settings.....</b>	<b>15</b>
Home Menu .....	15
Dashboard Tab.....	15
Services Tab.....	16
Statistics Tab.....	16
LoRaWAN® .....	17
Network Settings.....	18
Network Server Mode.....	18
Status.....	19
LoRa Card Information.....	20
LoRaWAN Network Server Configuration .....	21
Network Configuration.....	24
Radio Bridge Console Configuration.....	25
Datarate Configuration .....	25
Duty Cycle Configuration.....	26
Database Configuration.....	26
Network Server Logging Configuration .....	27
Network Server Testing Configuration.....	27

Server Ports Configuration .....	28
Other Settings.....	28
Packet Forwarder Mode .....	29
Status.....	30
LoRa Card Information.....	31
Gateway Info.....	32
LoRa Packet Forwarder Configuration (Normal Mode) .....	32
Channel Plan .....	32
Basics .....	33
Server Settings.....	33
Forward CRC.....	34
Duty Cycle.....	35
Intervals.....	35
Other Settings.....	36
Basic Station Mode.....	36
Status.....	37
LoRa Card Information.....	38
Basic Station Configuration .....	38
Key Management.....	40
Gateways .....	44
Devices.....	45
Device Sessions .....	46
Device Groups .....	47
Profiles.....	47
Packets.....	51
Downlink Queue.....	53
Operations .....	54
Payload Management .....	56
BACnet Configuration.....	57
Definitions and Templates.....	58
Sensor Definitions .....	59
Filter the Sensor Definition List .....	60
Import Sensor Definitions .....	60
Templates Tab .....	62
Add a Sensor Type Template.....	62
Add a BACnet Object to a Template .....	64
Edit a BACnet Object in a Template .....	65
Delete a BACnet Object from a Template.....	65
Sensors.....	65
Sensors Tab .....	65
Filter Sensors List.....	66



View Sensor Details .....	66
Add Sensor .....	67
Apply Template .....	67
Sensors Data CSV Files .....	69
Edit Sensor Details .....	69
Delete Sensors .....	70
Sensor Map JSON Files .....	71
Import Sensor Map .....	71
Download the Sensor Map .....	72
BACnet Objects Tab .....	72
Filter BACnet Object Map .....	72
Edit a BACnet Object .....	73
Add a BACnet Object .....	73
Supported BACnet Object Types .....	75
Delete BACnet Objects .....	76
BACnet Object Map JSON Files .....	76
Import BACnet Object Map .....	79
Download the BACnet Objects Map .....	79
Setup Menu .....	79
Network Interface Configuration .....	80
Configure eth0 .....	80
Configure br0 .....	81
Ethernet Interface Configuration Parameters .....	82
Add a VLAN Interface .....	83
WAN Configuration .....	84
Global DNS .....	86
DDNS Configuration .....	87
DDNS Configuration Parameters .....	88
DHCP Configuration .....	89
DHCP Configuration Tab .....	89
Add IPv4 DHCP Server Tab .....	89
Add DHCPv6/RA Tab .....	90
Edit DHCPv6/RA Tab .....	91
LLDP Configuration .....	91
SMTP Configuration .....	91
Settings Tab .....	91
Mail Log Tab .....	92
SNMP Configuration .....	93
Time Configuration .....	96
Cellular Menu .....	97
Cellular Configuration .....	97

Cellular Configuration Tab.....	98
General Configuration.....	98
Connection Monitoring.....	98
Connection Recovery .....	99
Cellular Profiles Tab .....	100
Add Provider Profile Tab .....	100
Edit SIM Group .....	101
Add SIM Profile Tab.....	101
Diagnostics.....	102
Radio Status Tab.....	102
Diagnostics Tab.....	103
Cell Radio Firmware Upgrade Tab .....	104
SMS.....	104
Configuration Tab .....	105
Send/Received SMS Tab.....	105
Firewall Menu.....	106
Firewall Rules and Port Forwarding.....	106
Settings.....	107
Settings Tab.....	107
Port Forwarding .....	107
Status Tab.....	108
Trusted IP .....	109
Static Routes.....	110
Tunnels Menu .....	110
GRE Tunnels .....	111
GRE Configuration Tab .....	111
Add Tunnel Tab .....	111
IPSec Tunnels.....	112
IPSec Configuration Tab.....	113
Add Tunnel Tab.....	113
Configuration Parameters.....	114
OpenVPN Tunnels .....	116
OpenVPN Configuration Tab.....	117
Add Tunnel Tab .....	118
Configuration 1: OpenVPN Tunnel with TLS Authorization Mode (Device only) .....	118
Configuration 2: OpenVPN Tunnel with TLS Authorization Mode (Device and Connected PC) .....	121
Configuration 3: OpenVPN Tunnel with Static Key Authorization Mode (device server and client).....	121
Configuration 4: OpenVPN Tunnel with Static Key Authorization Mode and TCP .....	124
Administration Menu .....	126
User Accounts.....	126

SSH Key Management .....	127
Users Tab .....	129
Add User Tab .....	129
Password Complexity Rules Tab .....	131
Custom Roles Tab .....	131
Add Custom Role .....	132
Access Configuration .....	133
Radius Configuration .....	135
X.509 Certificate Tab .....	136
Web Certificate Tab .....	136
CA Certificates Tab .....	137
Remote Device Management .....	138
Notifications .....	139
Configuration Tab .....	139
Sent Tab .....	141
Web UI Customization .....	141
Firmware Upgrade .....	142
System Fallback .....	143
Package Management .....	143
Save/Restore .....	144
Debug Options .....	145
Usage Policy .....	146
Licensing .....	147
Apps Menu .....	147
Custom Apps .....	147
Installed Applications .....	148
View Application Details .....	149
Application Status .....	150
Extra Version Support .....	151
Install a Custom App .....	151
Installation Location .....	152
Send Notification Utility .....	153
<b>Warranty .....</b>	<b>155</b>
<b>Contact Information .....</b>	<b>155</b>
<b>Revision History .....</b>	<b>155</b>

# 1 Introduction

---

This guide provides information and procedures necessary to configure a Conduit AP (MTCAP3) using the mPower Edge Intelligence interface.

**Note:** For complete hardware information about the Conduit AP, refer to the Conduit AP Hardware Guide.

## Intended Audience

The intended audience of this guide is IT personnel tasked with installing, provisioning, and configuring a Conduit AP.

## About the Conduit AP 300

Conduit AP 300 Series (MTCAP3) securely connects thousands of LoRaWAN® wireless IoT sensors to the cloud using the LoRaWAN® protocol. It expands LoRa network coverage to difficult to reach areas and is capable of packet forwarding user data between LoRa end devices and a centrally located network server on the cloud, in a data center, or a public network. The Conduit AP Access Point packet forwarding gateway offers Ethernet and Cellular Wide Area Networks seamless connectivity options to connect to Cloud based applications in centrally located data centers.

## Intended Use

The Conduit AP is designed for indoor use and industrial applications, such as smart buildings, retail spaces, agricultural environments, and other deployments where reliability and secure long-range data communication is essential.

## 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

### Installing a SIM Card

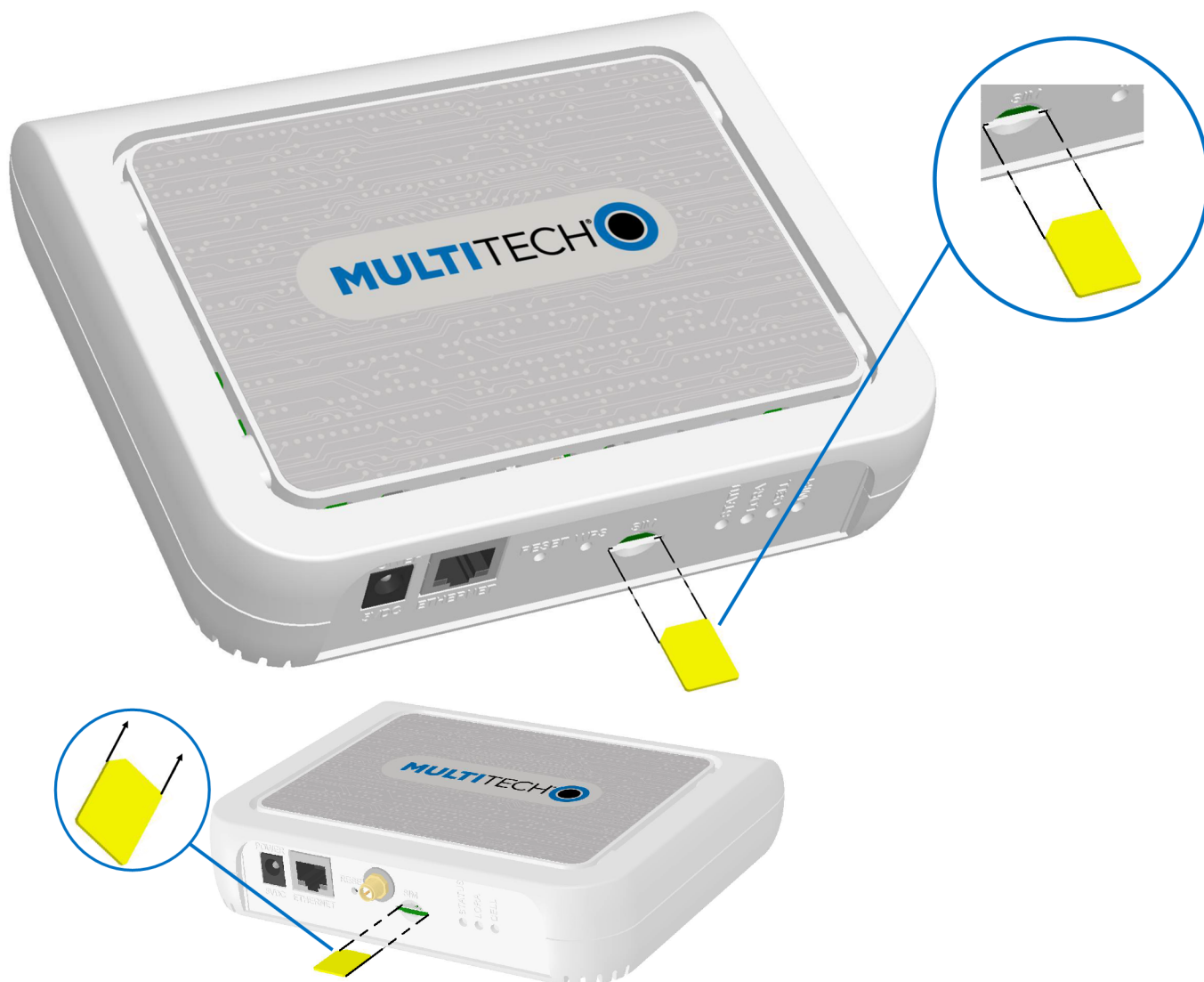
Models with cellular capability have a micro SIM slot, you'll need a micro (3FF) SIM card from your network provider.

**Note:** -LNA3 models work on both Verizon and AT&T networks. The device detects the carrier based on your SIM card.

**Note:** -LNA7D models work on both Verizon and AT&T networks. The device detects the carrier based on your SIM card.

To install the SIM card:

- With the contact side facing down, align the notched edge as shown and slide the SIM card completely into the SIM holder.



## Removing a SIM Card

To remove the SIM card, push the SIM card in. The device ejects the SIM card.

## Attaching the Antenna

(Models with external antenna only)

To connect the antenna:

- Finger-tighten the antenna to the antenna connector on your device.

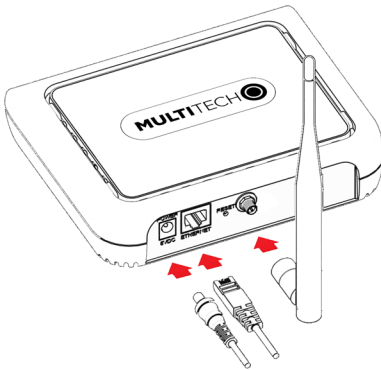
## Cabling the Device

To cable the device:

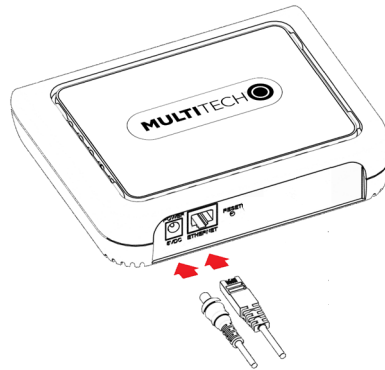
1. For Ethernet only models, connect the Ethernet cable to the Ethernet port on the device and to your computer.
2. Attach the plug for your country to the power supply.
3. Connect the power supply to the device's power jack and plug it into an electrical outlet. When the operating system is fully loaded, the STATUS LED blinks.

**Important:** The power supply is 5V at the connector. Verify you are connecting the power supply that shipped with the device. Using a power supply with higher voltage damages the device.

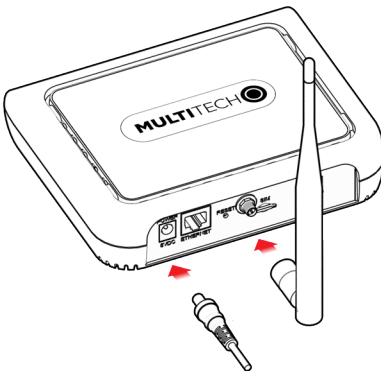
Ethernet only models with external LoRa antenna



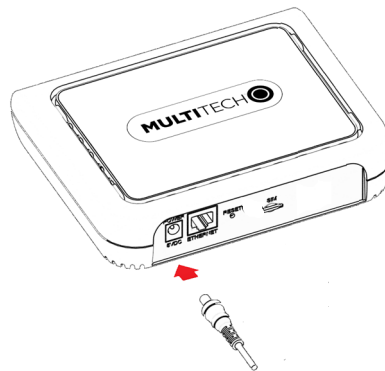
Ethernet only models, all internal antennas



Cellular models with external LoRa antenna



Cellular models, all internal antennas



## Commissioning Mode

The Conduit AP 300 ships in what is called Commissioning Mode. As soon as the Conduit AP 300 is reset to factory defaults or right after the manufacturing process is complete, the system is in Commissioning Mode.

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

**Important:** Beginning with mPower Release 7.1.0, if an MTCAP3 is a non-cellular device, the eth0 interface is configured as a WAN-DHCP client.

**Important:** Once the Conduit AP 300 has been powered up and is in Commissioning Mode, its Web UI 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.

Before proceeding, an Administrative User must be configured.

## Configure the Administrative User

Perform the following procedure to create and configure the Administrative user:

**Note:** MultiTech recommends using Firefox.

1. Open a browser and enter the default IP address in the URL field, **192.168.2.1**. Most browsers display a warning about HTTP addresses being unsafe because of a self-signed certificate:
  - For Edge, click **Advanced** and then **Continue** to **192.168.2.1**.
  - For Firefox, click **Advanced** and then click **Accept the Risk and Continue**.
  - For Chrome, click **Advanced** and then **Continue** to **192.168.2.1** (unsafe).

2. Enter a username for the Administrative User. Click **OK**. Follow on screen instructions for usernames.
3. Enter a password and click **OK**. Follow on screen instructions for a secure password.
4. Enter the password again to confirm. Click **OK**.
5. Log into the Conduit AP 300 using the new username and password.

The First-Time Setup Wizard will then launch.

## First Time Setup Wizard

Once commissioning is complete, the First Time Setup Wizard launches which enables users to configure:

- System date and time
- Cellular connectivity



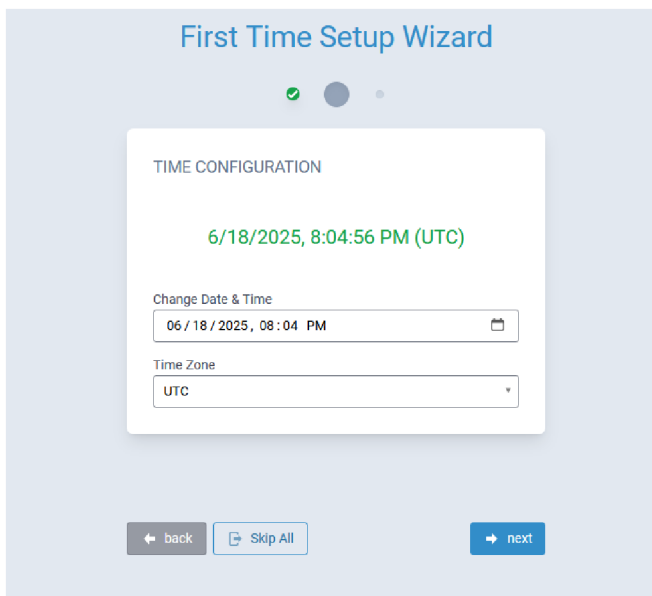
Click **Next** to begin configuring the Conduit AP 300.

## Configure Network Router Mode

Perform the following procedure to configure the Conduit AP 300 as a Network Router:

1. Configure **Date & Time** and **Time Zone** to reflect the Conduit AP 300's location.



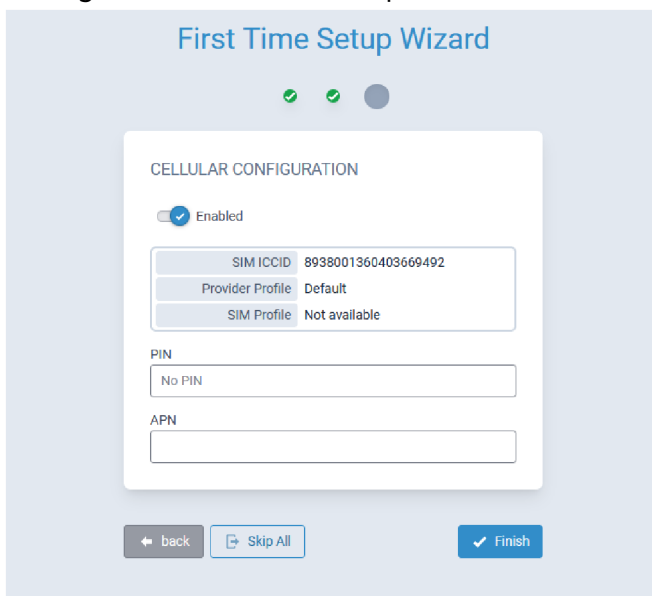


The screenshot shows the 'First Time Setup Wizard' with the 'TIME CONFIGURATION' step selected. The date and time are set to 6/18/2025, 8:04:56 PM (UTC). Below this, there are fields for 'Change Date & Time' (showing 06/18/2025, 08:04 PM) and 'Time Zone' (set to UTC). At the bottom, there are three buttons: 'back', 'Skip All', and 'next'.

2. Click **Next**.

**Note:** If the Conduit AP 300 is not equipped with a radio modem (i.e., does not support Cellular operation,) click **Finish**.

3. Configure **PIN** and **APN** if required.



The screenshot shows the 'First Time Setup Wizard' with the 'CELLULAR CONFIGURATION' step selected. The 'Enabled' toggle is checked. Below this, there is a table with cellular configuration details:

SIM ICCID	8938001360403669492
Provider Profile	Default
SIM Profile	Not available

Below the table, there are fields for 'PIN' (set to 'No PIN') and 'APN' (empty). At the bottom, there are three buttons: 'back', 'Skip All', and 'Finish'.

4. Click **Finish**.

## Commissioning an Ethernet-Only MTCAP3

### Network Configuration

The Ethernet interface on MTCAP3 (without cellular) operates as a DHCP client, meaning it does not use a predictable static IP (such as 192.168.2.1). Upon connection to a network, the device will request an IP from a DHCP server.

## Locating the Device's IP Address

The assigned IP can typically be found using one of the following methods:

- DHCP Server Logs - most IT departments can retrieve the IP via MAC address or hostname (mtcap3-<serial\_number>).
- Network Scanning Tools - utilities such as ARP, nmap, or similar tools may help identify the device's IP.

## Connecting to the Device

Once you've identified the assigned IP, you can access the device API or Web UI through that IP address in a browser.

# 3 mPower Configuration Settings

## 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.

Home

LoRaWAN

Payload Management

Setup

Cellular

Firewall

Tunnels

Administration

Apps

DashboardServicesStatistics

DEVELOPER

MULTITECH

Device Details

MODEL NUMBER

MTCAP3-LEU7-AC3EEA-LEM-DEV

SERIAL NUMBER

23050468

IMEI

862869032462249

FIRMWARE VERSION

7.2.0-dev1

CURRENT TIME

6/13/2025, 12:30:00 AM

UP TIME

00:05:15

Internet

Connected

WAN TRANSPORT

Cellular

WAN IP

10.74.123.254

CURRENT DNS

80.255.64.23

80.255.64.24

WAN

LAN

Cellular (ppp0)

STATE

Connected

CELLULAR SERVICE

LTE

NETWORK REGISTRATION

Registered

SIGNAL

-63 dBm

RSRP

-93 dBm

RSRQ

-10 dB

CONNECTED

00:01:59

APN

IPV4 ADDRESS

10.74.123.254

DNS

80.255.64.23, 80.255.64.24

PHONE NUMBER

0996366949

TOWER

57ESE21

Bridge (br0)

MAC ADDRESS

00:08:00:4D:A9:FB

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

Ethernet (eth0)

STATE

Enabled

BRIDGE

br0

MAC ADDRESS

00:08:00:4D:A9:FB

LoRa

MODEL NUMBER

MTCAP3-003E00

HARDWARE

MTCAP3-003-0.1

FREQUENCY BAND

868

EUI

00-80-00-00-00-14-39

Last update: 3:30:31 AM

Help

About

Contact Us

© 1995 - 2025 Multi-Tech Systems, Inc.

## Services Tab

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

**SERVICE STATISTICS**

Dashboard Services Statistics

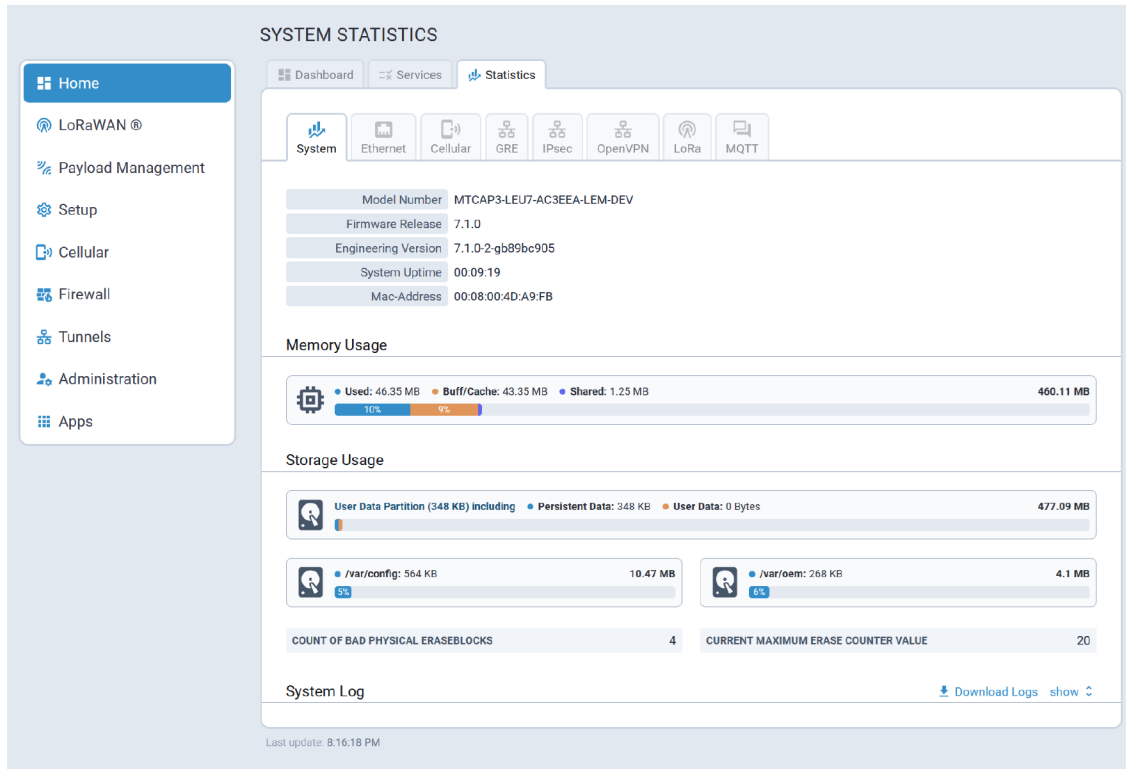
ENABLED	SERVICE	STATUS
×	DDNS	DDNS is disabled
✓	SNTP	Synchronized at Fri Sep 27 05:07:04 UTC 2024; NTPD is determining Polling Servers
×	TCP/ICMP Keep Alive	PING Keep alive is disabled
×	SMTP	SMTP is disabled
×	SMS	SMS is disabled
✓	Failover	Failover service is running
×	SNMP Server	SNMP Server is disabled
×	Reverse SSH Tunnel	Reverse SSH service is disabled
✓	Remote Device Management	Waiting for the connectivity before initiating checking-in procedure.
×	LLDP	LLDP is disabled
×	Continuous Ping	Continuous ping is disabled

Last update: 10:22:46 PM

## Statistics Tab

The System Statistics tab provides the following system information:

- System details, memory and storage usage, system log
- Ethernet interfaces statistics and logs
- Cellular statistics and logs
- GRE tunnels statistics and logs
- IPSec tunnels statistics and logs
- OpenVPN tunnels statistics and logs



## LoRaWAN®

A typical LoRaWAN® page is illustrated here:

**LORAWAN NETWORKING**

Home **LoRaWAN®** Network Settings

Payload Management Setup Cellular Firewall Tunnels Administration Apps

**LoRa Mode**

DISABLED

**LoRa Card Information** [hide](#)

Gateway EUI	00-80-00-00-D0-00-14-39
Frequency Band	868

[Submit](#) [Reset To Default](#)

Gateways such as the Conduit AP 300 can connect with end-devices/sensors to create an application network. Using the cloud-based Lens interface, LoRa application networks, including gateway and end-devices, can easily be managed.

When the LoRa Mode is set to **Network Server**, the Conduit AP 300 acts as a network server allowing end-points to join with the correct credentials on the correct frequency and sub-band.

LoRa can be configured for the following frequency bands:

- 915 (AS, AU, KR, IL, and US)

- In the US, the 915 band supports 8 sub-bands.
- 868 (EU, IN, and RU)
  - In the EU, the 868 band has three default channels and five configurable channels.
- Global 2400 (ISM)
  - For specific industrial, scientific, and medical applications globally, the ISM 2400 band has three default channels.

The transmit (TX) power setting controls the transmission power of the gateway.

The Rx 1 DR Offset and RX 2 Datarate are sent with a join response to configure the data rates used for receive windows.

The offset is applied to the downlink data rate for reception on the first window according to LoRa WAN standards.

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

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

Detailed LoRaWAN network configuration information is provided in the following sections.

## Network Settings

The set of network configuration parameters displayed depends on the selected **LoRa Mode**.

Supported LoRa Modes are:

- NETWORK SERVER
- PACKET FORWARDER
- BASIC STATION
- DISABLED

Configuration information for each of these modes is provided in the following sections.

### Network Server Mode

Typical Network Server mode configuration parameters are shown here:

Home

LoRaWAN

Network Settings

Payload Management

Setup

Firewall

Tunnels

Administration

Apps

LORAWAN NETWORKING

LoRa Mode

NETWORK SERVER

Status

Packet Forwarder

2.0.48-r14.0

STOPPED

Network Server

2.7.18

STOPPED

Lens Server

2.7.18

DISABLED

LoRa Card Information

show

LoRaWAN Network Server Configuration

Channel Plan

CHANNEL 0	CHANNEL 1	CHANNEL 2	CHANNEL 3	CHANNEL 4	CHANNEL 5	CHANNEL 6	CHANNEL 7	LORA STD
902.3MHz	902.5MHz	902.7MHz	902.9MHz	903.1MHz	903.3MHz	903.5MHz	903.7MHz	903MHz

Channel Plan

US915

Frequency Sub-Band 1

1

Channel Mask

Edit

Network

Network Mode

Public LoRaWAN

Join Delay (sec)

5

Lease Time

00:00:00

Address Range Start

00:00:00:01

NetID

000000

Rx1 Delay (sec)

1

Queue Size

16

Address Range End

FF:FF:FF:FE

Radio Bridge Console

show

Datarate

show

Duty Cycle

show

Database

show

Network Server Logging

show

Network Server Testing

show

Server Ports

show

Other Settings

show

Default App has been renamed to Cloud Connector and moved to the Apps section .

Submit

Reset To Default

Status

LoRaWan Network Server status information is shown here:

Status

Packet Forwarder

2.0.48-r14.0

STOPPED

Network Server

2.7.18

STOPPED

Lens Server

2.7.18

DISABLED

Conduit® AP Configuration Guide Using mPower™ Edge Intelligence (v7.1.0)

19

Parameter	Default Value	Description
Packet Forwarder	Depends on latest software version	Packet Forwarder software version
Packet Forwarder Status	If configured properly, RUNNING	Packet Forwarder status. Values include RUNNING, RESTARTED, or DISABLED.
Network Server	Depends on latest software version	Network Server software version
Network Server Status	If configured properly, RUNNING	Network Server status. Values include RUNNING, RESTARTED, or DISABLED.
Lens Server	Depends on latest software version	Lens Server software version
Lens Server Status	If configured properly, RUNNING	Lens Server status. Values include RUNNING, RESTARTED, or DISABLED.

### LoRa Card Information

Typical LoRa Card parameter information is provided here:

LoRa Card Information	
Gateway EUI	00-80-00-00-D0-00-14-39
Frequency Band	868

Parameter	Default Value	Description
Gateway EUI	N/A	Gateway ID of Conduit, queried from the LoRa card (if present).
Frequency Band	Depends on LoRa card	Frequency band set based on the installed LoRa peripheral.
FPGA Version	Depends on LoRa card	FPGA firmware version of the installed LoRa card.
Upgrade FPGA	N/A	Click on link to upgrade FPGA firmware on the LoRa card, if a later version is available.
Current Version	Depends on LoRa Card	Current FPGA firmware version of the installed LoRa card.



Parameter	Default Value	Description
Upgrade Version	Depends on LoRa Card	Upgrade version of FPGA firmware if available. If this field displays an upgrade version, click Start to upgrade the firmware. If this field displays No Options Available, then you already have the latest version and you can click Cancel.

### LoRaWAN Network Server Configuration

Typical LoRaWAN Network Server configuration parameters are shown here:

LoRaWAN Network Server Configuration

Channel Plan

CHANNEL 0	CHANNEL 1	CHANNEL 2	CHANNEL 3	CHANNEL 4	CHANNEL 5	CHANNEL 6	CHANNEL 7	LORA STD
902.3MHz	902.5MHz	902.7MHz	902.9MHz	903.1MHz	903.3MHz	903.5MHz	903.7MHz	903MHz

Channel Plan  
US915

Frequency Sub-Band 1  
1

Channel Mask

Parameter	Default Value	Description
Channel Plan	US915: 915, AU915: 915, AS923-1: 915, AS923-2: 915, AS923-3: 915, AS923-4: 915, KR920: 915, EU868: 868, IN865: 868, RU864: 868, ISM2400: 2400	LoRaWAN channel plan used for the upstream and downlink frequencies and datarates. Values are US915, EU868, IN865, AU915, AS923-1, AS923-2, AS923-3, AS923-4, KR920, RU864, or ISM2400. Available channel plans depend on the type of LoRa card installed. For more details about each Channel Plan, refer to the RP2-1.0.3 LoRaWAN® Regional Parameters document on the LoRa Alliance website, <a href="https://lora-alliance.org/">https://lora-alliance.org/</a> .

Parameter	Default Value	Description
Additional Channels	Depends on channel plan selected	A set of channels are configured based on this setting (MHz). Frequencies supported depends on channel plan selected. v2.1 Geolocation GW - default channels must be included in the configured range. The RU864 plan uses the following channels when configured with the default settings of 0: Radio 0: 868.9 MHz, 869.1 MHz Radio 1: 864.1 MHz, 864.3 MHz, 864.5 MHz, 864.7 MHz, 864.9 MHz.
Additional Channels 2	Depends on channel plan selected	A set of channels are configured based on this setting (MHz). Frequencies supported depends on channel plan selected. v2.1 Geolocation GW - Configurable for the range within the entire band. The RU864 plan will use the following channels when configured with the default settings of 0: Radio 0: 868.9 MHz, 869.1 MHz Radio 1: 864.1 MHz, 864.3 MHz, 864.5 MHz, 864.7 MHz, 864.9 MHz.

Parameter	Default Value	Description
Channel Mask	N/A	<p>Mask of available channels. Leave empty to enable only selected sub-band or set as desired. Click the Edit button to select your desired channel mask(s) by checking the box under the available list of channels. Override channel mask to include coverage provided by additional gateways.</p> <p>US/AU 64-channel:            00FFFFFFFFFFFFFFFFFFFF and            EU/AS/IN/KR: 00FF. Combine the following FSB masks to support more than 8 channels. Settings will be sent to end-devices on first downlink after OTA join:</p> <pre>           FSB0 :           00FFFFFFFFFFFFFFFFFFFF           FSB1 :           000100000000000000FF           FSB2 :           000200000000000000FF00           FSB3 :           000400000000000000FF0000           ...           FSB8 :           0080FF0000000000000000           FSB1 + FSB8 :           0081FF00000000000000FF           </pre>
Frequency Sub-Band	1	For US and AU only, 8 sub-bands are available.
Frequency Sub-Band 2	1	For US and AU only, 8 sub-bands are available (for extra LoRa Card).
Enable Diversity	Unchecked	Enable use of two LoRa cards.
Enable LBT	Unchecked	Enable Listen Before Talk.  <b>Note:</b> Requires FPGA v33 or v61.
Max EIRP	20	Maximum uplink transmit power of end-devices (in dBm)
Dwelltime Up	0 (no limit)	Maximum uplink dwell-time for region (ms). 0 : no limit and 1 : 400 ms (depends on region).

Parameter	Default Value	Description
Dwelltime Down	0 (no limit)	Maximum downlink dwell-time for region (ms). 0 : no limit and 1 : 400 ms (depends on region).

### Network Configuration

Typical Network configuration parameters are shown here:

Network			
Network Mode Public LoRaWAN	Join Delay (sec) 5	Lease Time 00-00-00	Address Range Start 00:00:00:01
NetID 000000	Rx1 Delay (sec) 1	Queue Size 16	Address Range End FF:FF:FF:FE

Parameter	Default Value	Description
Network Mode	Public LoRaWAN	Set Network Mode: Private MTS (sync word: 0x12 and US/AU) Downlinks per FrequencySubBand) Public LoRaWAN (sync word: 0x34) Private LoRaWAN (sync word: 0x12)
Join Delay (sec)	Depends on selected Network Mode value. <ul style="list-style-type: none"> <li>Private Mode: 1 (5 if user input value is outside of range.)</li> <li>Public Mode: 5 (Also if user input value is outside of range.)</li> </ul>	Number of seconds before receive windows are opened for join. Must match Dot settings. Range: 1-15
Lease Time (dd-hh-mm)	00-00-00	Amount of time until a successful join expires.
Address Range Start	00:00:00:01	Start address to assign to OTA joining motes.
NetID	000000	LoRaWAN NetID setting for assigning network address and beacons.
Rx1 Delay (sec)	1	Number of seconds before receive windows are opened. Must match Dot settings. Range: 1-15
Queue Size	16	Number of downlink messages to hold per node.

Parameter	Default Value	Description
Address Range End	FF:FF:FF:FE	End address to assign to OTA joining motes.

### Radio Bridge Console Configuration

Typical Radio Bridge Console configuration parameters are shown here:

Radio Bridge Console hide

☐ Enabled

Gateway Name

Region

Parameter	Default Value	Description
Enabled	TBD	TBD
Gateway Name	TBD	TBD
Region	TBD	TBD

### Datarate Configuration

Typical Datarate configuration parameters are shown here:

Datarate hide

Rx 1 DR Offset

Rx 2 Datarate

Max Datarate

Min Datarate

☒ Enable ADR

ADR Step (cB)

ADR Nb Trans

Max FUOTA Packet Size

Parameter	Default Value	Description
Rx 1 DR Offset	0	Offset applied to upstream data rate for downstream data rate on first receive window. US: 0-4, EU/RU: 0-5, AS/IN: 0-7, AU: 0-7, KR: 0-5.
Rx 2 Datarate	10 (For US/AU), 2 (For all others)	Datarate for second receive window. US: 8-13, EU/IN/AS: 0-7, AU: 8-13, KR: 0-5.
Max Datarate	0	Maximum datarate to use for ADR. US: 0-4, EU/AS/RU: 0-7, AU: 0-6, KR: 0-5, IN: 1-5,7.
Min Datarate	0	Minimum datarate to use for ADR. US: 0-4, EU/AS/RU: 0-7, AU: 0-6, KR: 0-5, IN: 1-5,7.
Enable ADR	<b>TBD</b>	<b>TBD</b>
ADR Step (cB)	30	Step between each datarate setting for ADR (minimum: 25).
ADR Nb Trans	<b>TBD</b>	<b>TBD</b>

Parameter	Default Value	Description
Max FUOTA Packet Size	N/A	Maximum packet size used for FUOTA downloads.

### Duty Cycle Configuration

Typical Duty Cycle configuration parameters are shown here:

Duty Cycle
hide

☐ Enable Duty-Cycle Limit
Duty-Cycle Period
60
Duty-Cycle Ratio

Parameter	Default Value	Description
Enable Duty-Cycle Limit	Disabled	Allows the gateway to configure and enforce duty-cycle window limits on transmissions.
Duty-Cycle Period	60	Number of minutes in sliding windows for duty cycle restrictions (for EU only).
Duty-Cycle Ratio	N/A	Amount of time on-air allowed per window.

### Database Configuration

Typical Database configuration parameters are shown below:

Database
hide

Database Path
/var/config/lora/lora-network-server.db
Trim Rows
100
☐ Reduce Uplink Writes

Backup Interval
3600
Trim Interval
600
☐ Skip Field Check

Parameter	Default Value	Description
Database Path	var/config/lora/lora-network-server.db	Path to backup database in non-volatile memory
Trim Size	100	Maximum size of packet tables to keep in database
Reduce Uplink Writes	Disabled (unchecked)	Write uplink data to database every 100 packets or 5 minutes to increase uplink throughput
Backup Interval	3600	Interval in seconds to backup the database to flash
Trim Interval	600	Interval in seconds to run the trim packet data tables command

Parameter	Default Value	Description
Skip Field Check	Disabled (unchecked)	Skip checking JSON fields of UDP packets from packet forwarder, may increase uplink throughput

### Network Server Logging Configuration

Typical Network Server Logging configuration parameters are shown here:

Parameter	Default Value	Description
Log Destination	Syslog	Select the type logging destination, either Syslog or File  <b>Note:</b> Select <b>File</b> only for debugging purposes to avoid running out of Conduit AP 300 RAM.
Log Level	INFO	Select the log level of the messages to be logged. Choose from drop-down: Info, Error, Warning, Debug, Trace, and Maximum. Maximum will provide all messages.
Path	blank	Specify the log file location.

### Network Server Testing Configuration

Typical Network Server Testing configuration parameters are shown here:

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

Parameter	Default Value	Description
Disable Rx1	Disabled	Disable sending downlink messages in Rx1.
Disable Join Rx2	Disabled	Disable sending join accept message in Rx2.
Disable Rx2	Disabled	Disable sending downlink messages in Rx2.
Disable Duty Cycle	Disabled	Disable duty cycle restrictions <b>(this is for testing purposes only - do not use for deployments)</b> .
Disable Strict Counter	<b>TBD</b>	<b>TBD</b>
Disable GPS	<b>TBD</b>	<b>TBD</b>

### Server Ports Configuration

Typical Server Port configuration parameters are shown here:

Server Ports hide

☐ Local Only

Network Lead Time: 500

Upstream Port: 1780

App Port Up: 1784

Downstream Port: 1782

App Port Down: 1786

Parameter	Default Value	Description
Local Only	Enabled (checked)	Configure local ports only
Network Lead Time	<b>TBD</b>	<b>TBD</b>
Upstream Port	1780	Upstream port
App Port Up	1784	Application port up
Downstream Port	1782	Downstream port
App Port Down	1786	Application port down

### Other Settings

Other configuration parameters are shown here:

Other Settings hide

☐ Trim Local MQTT Topic EUI

Max Tx Power EIRP (dBm): 26

Antenna Gain (dBi): 3

ACK Timeout (ms): 5000

Gateway Timeout Threshold (s): 120



Parameter	Default Value	Description
Trim Local MQTT Topic EUI	<b>TBD</b>	<b>TBD</b>
Max Tx Power EIRP (dBm)	N/A	Maximum transmitted power with antenna gain.
Antenna Gain (dBi)	3	Gain of the configured antenna Valid values: -128 to +128
ACK Timeout (ms)	<b>TBD</b>	<b>TBD</b>
Gateway Timeout Threshold (s)	<b>TBD</b>	<b>TBD</b>

## Packet Forwarder Mode

Typical Packet Forwarder mode configuration parameters are shown here:

Home

LoRaWAN

Network Settings

Payload Management

Setup

Firewall

Tunnels

Administration

Apps

## LORAWAN NETWORKING

LoRa Mode

PACKET FORWARDER

Status

Packet Forwarder

2.0.48-r14.0

STOPPED

LoRa Card Information

show

Gateway Info

UUID

4b7e172b-45cc-74fe-710f-e9a6a25a3915

Serial Number

22754348

LoRa Packet Forwarder Configuration (Normal Mode)

Show Manual Configuration

Channel Plan

CHANNEL 0	CHANNEL 1	CHANNEL 2	CHANNEL 3	CHANNEL 4	CHANNEL 5	CHANNEL 6	CHANNEL 7	LORA STD
902.3MHz	902.5MHz	902.7MHz	902.9MHz	903.1MHz	903.3MHz	903.5MHz	903.7MHz	903MHz

Network

Manual

Channel Plan

US915

Frequency Sub-Band

1

Basics

hide

Public LoRaWAN Sync Word

Packet Forwarder Path

/opt/lora/lora\_pkt\_fwd

Gateway ID Source

Hardware

Server Settings

hide

Server Address

127.0.0.1

Upstream Port

1780

Downstream Port

1782

Forward CRC

hide

Forward CRC Valid

Forward CRC Disabled

Forward CRC Error

Duty Cycle

hide

Enable Duty-Cycle

Duty-Cycle Period

Duty-Cycle Ratio

Intervals

hide

Keep Alive Interval (s)

10

Stat Interval (s)

20

Push Timeout (ms)

100

Autoquit Threshold

60

Other Settings

hide

Max Tx Power EIRP (dBm)

26

Antenna Gain (dBi)

3

Spreading Factors

Spreading Factor 5 - 12

ChirpStack Gateway Bridge Configuration

Chirpstack Gateway Bridge not installed. Instructions for installing the service can be found [here](#)

Enabled

Submit

Reset To Default

## Status

LoRaWan Packet Forwarder status information is shown here:

Status
Packet Forwarder <div>2.0.48-r14.0</div> <div>STOPPED</div>

Parameter	Default Value	Description
Packet Forwarder	Depends on latest software version	Packet Forwarder software version
Packet Forwarder Status	If configured properly, RUNNING	Packet Forwarder status. Values include RUNNING, RESTARTED, or DISABLED.

### LoRa Card Information

Typical LoRa Card parameter information is provided here:

LoRa Card Information
<div>Gateway EUI 00-80-00-00-D0-00-14-39</div> <div>Frequency Band 868</div>

Parameter	Default Value	Description
Gateway EUI	N/A	Gateway ID of Conduit, queried from the LoRa card (if present).
Frequency Band	Depends on LoRa card	Frequency band set based on the installed LoRa peripheral.
FPGA Version	Depends on LoRa card	FPGA firmware version of the installed LoRa card.
Upgrade FPGA	N/A	Click on link to upgrade FPGA firmware on the LoRa card, if a later version is available.
Current Version	Depends on LoRa Card	Current FPGA firmware version of the installed LoRa card.
Upgrade Version	Depends on LoRa Card	Upgrade version of FPGA firmware if available. If this field displays an upgrade version, click Start to upgrade the firmware. If this field displays No Options Available, then you already have the latest version and you can click Cancel.

## Gateway Info

Typical Gateway Info is shown here:

Gateway Info	
UUID	4b7e172b-45cc-74fe-710f-e9a6a25a3915
Serial Number	22754348

Parameter	Default Value	Description
UUID	N/A	Universally Unique Identifier (128-bit ID)
Serial Number	N/A	Serial number for the Conduit AP 300

## LoRa Packet Forwarder Configuration (Normal Mode)

To manually configure the Packet Forwarder, click on the **Show Manual Configuration** link as shown below.

LoRa Packet Forwarder Configuration (Normal Mode)								
<a href="#">Show Manual Configuration</a>								
Channel Plan								
CHANNEL 0	CHANNEL 1	CHANNEL 2	CHANNEL 3	CHANNEL 4	CHANNEL 5	CHANNEL 6	CHANNEL 7	LORA STD
902.3MHz	902.5MHz	902.7MHz	902.9MHz	903.1MHz	903.3MHz	903.5MHz	903.7MHz	903MHz

For a Dual Packet Forwarder, both cards may be manually configured provided two LoRa cards are installed. This allows different channel plans or network servers to be configured for each forwarder.

## Channel Plan

Typical Channel Plan configuration parameters are shown here:

Channel Plan								
CHANNEL 0	CHANNEL 1	CHANNEL 2	CHANNEL 3	CHANNEL 4	CHANNEL 5	CHANNEL 6	CHANNEL 7	LORA STD
902.3MHz	902.5MHz	902.7MHz	902.9MHz	903.1MHz	903.3MHz	903.5MHz	903.7MHz	903MHz
Network Manual		Channel Plan US915		Frequency Sub-Band 1				

Parameter	Default Value	Description
Network	Manual	Select the network for Packet Forwarder mode including Manual (user determined), Radio Bridge Chirpstack, The Things Network, Senet, and Loriot.  <b>Note:</b> For Manual configuration, if SR paths are not provided, the system automatically finds/specifies them.

Parameter	Default Value	Description
Channel Plan	US915: 915AU915: 915, AS923-1: 915, AS923-2: 915, AS923-3: 915, AS923-4: 915, KR920: 915, EU868: 868, IN865: 868, RU864: 868, ISM2400: 2400	LoRaWAN channel plan used for the upstream and downlink frequencies and datarates. Values are US915, EU868, IN865, AU915, AS923-1, AS923-2, AS923-3, AS923-4, KR920, RU864, or ISM2400. Available channel plans depend on the type of LoRa card installed.  For more details on each Channel Plan, refer the RP2-1.0.3 LoRaWAN® Regional Parameters document on the <a href="https://loro-alliance.org/">LoRa Alliance website, https://loro-alliance.org/</a> .
Frequency Sub-Band	1	For US and AU only, 8 sub-bands are available.

### Basics

Typical Basic configuration parameters are shown here:

Parameter	Default Value	Description
Public LoRaWAN Sync Word	Disabled	Enables/disables public mode: <ul style="list-style-type: none"> <li>■ Enable (public mode): sync word <math>0 \times 34</math></li> <li>■ Disable (private mode): sync word <math>0 \times 12</math></li> </ul>
Packet Forwarder Path	opt/loro/loro_pkt_fwd	Path to the packet forwarder binary file to execute.
Gateway ID Source	Manual	Valid values are: <ul style="list-style-type: none"> <li>■ Manual: specified in the configuration</li> <li>■ Hardware: queries from Conduit AP 300</li> </ul>

### Server Settings

Typical Server Settings configuration parameters are shown here:

Server Settings hide

Server Address  
127.0.0.1

Upstream Port  
1780

Downstream Port  
1782

Parameters	Default Value	Description
Server address	N/A	<p>Server IP address to forward received uplink packets and transmit received downlink packets. The system provides the default address for The Things Network (based on your channel plan) and Semtech Demo. Refer to the router addresses table of The Things Network for the list of specific addresses based on channel plan <a href="https://www.thethingsnetwork.org/docs/gateways/packet-forwarder/semtech-udp/">https://www.thethingsnetwork.org/docs/gateways/packet-forwarder/semtech-udp/</a>.</p> <p>If you choose The Things Network with the AS923 channel plan, there are four different addresses available.</p> <p><b>Note:</b> No server addresses are available for The Things Network when using IN865 or RU864 channel plans.</p>
Upstream Port	N/A	IP Port to send received uplinks to. The system provides default ports for The Things Network and Semtech Demo.
Downstream Port	N/A	IP Port to connect to network server for downlink packets. The system provides default ports for The Things Network and Semtech Demo.

### Forward CRC

Typical Forward CRC (cyclic redundancy check) configuration parameters are shown here:

Forward CRC hide

☒ Forward CRC Valid
 ☐ Forward CRC Disabled
 ☒ Forward CRC Error

Parameter	Default Value	Description
Forward CRC Valid	Enabled	When enabled, packets received with <b>CRC Valid</b> are sent to the network server.
Forward CRC Disabled	Disabled	When enabled, packets received with <b>CRC Disabled</b> are sent to the network server.
Forward CRC Error	Enabled	When enabled, packets received with <b>CRC Errors</b> are sent to the network server.

### Duty Cycle

Typical Duty Cycle configuration parameters are shown here:

Duty Cycle
hide

☐ Enable Duty-Cycle

Duty-Cycle Period

Duty-Cycle Ratio

Parameter	Default Value	Description
Enable Duty-Cycle	Disabled	When enabled, the gateway configures and enforces duty-cycle window limits on transmissions.
Duty-Cycle Period	60	Number of minutes in sliding windows for duty-cycle restrictions (for EU only).
Duty-Cycle Ratio	N/A	Amount of time on-air allowed per window.

### Intervals

Typical Intervals configuration parameters are shown here:

Intervals
hide

Keep Alive Interval (s)
 10

Stat Interval (s)
 20

Push Timeout (ms)
 100

Autoquit Threshold
 60

Parameter	Default Value	Description
Keep Alive Interval (s)	10	Interval to send a ping to the network server.
Stat Interval (s)	20	Interval to update the network server with gateway statistics.
Push Timeout (ms)	100	Timeout default.

Parameter	Default Value	Description
Autoquit Threshold	60	Number of messages sent without acknowledgment from the network server.

### Other Settings

Typical Other Settings configuration parameters are shown here:

Other Settings hide

Max Tx Power EIRP (dBm)

Antenna Gain (dBi)

Spreading Factors

26

3

Spreading Factor 5 - 12

Parameter	Default Value	Description
Max TX Power EIRP (dBm)	N/A	Transmit power limit with antenna gain (dBm)
Antenna Gain (dBi)	3	Gain of configured antenna Valid values are -128 to +128 dBi
Spreading Factors	Spreading Factors 5 - 12	<b>TBD</b>

### Basic Station Mode

Typical Basic Station mode configuration parameters are shown here:



Home

LoRaWAN

Network Settings

Payload Management

Setup

Firewall

Tunnels

Administration

Apps

LORAWAN NETWORKING

LoRa Mode

BASIC STATION

Status

Basic Station

2.0.6-24-r4.0

STOPPED

LoRa Card Information

show

Basic Station Configuration

Config Reboot Persistence

Non-persistent

Station Card 1

Credentials

LNS

URI

Station Config (example)

```
{
  "sx1301_conf": {
    "chan_FSK": {
      "bandwidth": 125000,
      "data_rate": 56000,
      "enable": false,
      "if": 300000,
      "radio": 0
    },
    "chan_Lora_std": {
      "bandwidth": 500000,
      "enable": true,
      "if": 300000,
      "radio": 0,
      "spread_factor": 8
    }
  }
}
```

Server Cert

Import

Gateway Key

Import

Gateway Cert

Import

Signature Key

Import

ChirpStack Gateway Bridge Configuration

Chirpstack Gateway Bridge not installed. Instructions for installing the service can be found [here](#)

Enabled

Submit

Reset To Default

Help

About

Contact Us

© 1995 - 2025 Multi-Tech Systems, Inc.

Status

LoRaWan Basic Station status information is shown here:

Status

Basic Station

2.0.6-24-r4.0

STOPPED

Parameter	Default Value	Description
Basic Station	Depends on latest software version	Basic Station software version (For LoRa cards - 868 and 915 only)

Parameter	Default Value	Description
Basic Station Status	If configured properly, RUNNING	Basic Station status. Values include RUNNING, RESTARTED, or DISABLED.

### LoRa Card Information

Typical LoRa Card parameter information is provided here:

LoRa Card Information	
Gateway EUI	00-80-00-00-D0-00-14-39
Frequency Band	868

Parameter	Default Value	Description
Gateway EUI	N/A	Gateway ID of Conduit, queried from the LoRa card (if present).
Frequency Band	Depends on LoRa card	Frequency band set based on the installed LoRa peripheral.
FPGA Version	Depends on LoRa card	FPGA firmware version of the installed LoRa card.
Upgrade FPGA	N/A	Click on link to upgrade FPGA firmware on the LoRa card, if a later version is available.
Current Version	Depends on LoRa Card	Current FPGA firmware version of the installed LoRa card.
Upgrade Version	Depends on LoRa Card	Upgrade version of FPGA firmware if available. If this field displays an upgrade version, click Start to upgrade the firmware. If this field displays No Options Available, then you already have the latest version and you can click Cancel.

### Basic Station Configuration

Typical Base Station Configuration parameters are shown here:

Basic Station Configuration
Config Reboot Persistence <input type="text" value="Non-persistent"/>

Parameter	Default Value	Description
Config Reboot Persistence	TBD	TBD

## Station Card \*\*\* level=6 not mapped

Typical Station Card configuration parameters are shown here:

Station Card 1

Credentials

LNS

URI

Station Config (example)

```
{
  "SX1301_conf": {
    "chan_FSK": {
      "bandwidth": 125000,
      "datarate": 50000,
      "enable": false,
      "if": 300000,
      "radio": 0
    },
    "chan_Lora_std": {
      "bandwidth": 500000,
      "enable": true,
      "if": 300000,
      "radio": 0,
      "spread_factor": 8
    }
  }
}
```

Server Cert

Import

Gateway Key

Import

Gateway Cert

Import

Signature Key

Import

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

## Key Management

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

### Join Server

Choose the location of your join server.

Parameter	Default Value	Description
Location	Cloud Key Store	Choose Remote or local Join Server to handle OTA join requests. Select from drop-down either <b>Cloud Key Store</b> or <b>Local Keys</b> .

### Add End Device Credentials

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

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

Once you enter the above values, click **Finish**. Your saved end-device information displays under the **Local End-Device Credentials**. To delete all credentials, click **Delete All**. To add new credentials, click **Add New**. And to upload credentials, click **Upload**. After clicking **Upload**, browse and select the file to upload by clicking **Choose CSV or JSON file**. To append to the current credential list, check **Append to current list**.

**Note:** If the file to be uploaded contains a device that already exists, the upload will fail and an error message will be returned.

### Settings (for Cloud Key Store)

Parameter	Default Value	Description
Join Server URL	https://join.devicehq.com/api/m1/joinreq	Join Server address (You can verify the join server by clicking the Test button.)

Parameter	Default Value	Description
Enable Lens API	Disabled (Unchecked)	Enable Lens API to use Lens portal to manage LoRaWAN network.
Lens API URL	<a href="https://lens.devicehq.com/api/">https://lens.devicehq.com/api/</a>	Lens API URL.
Check-In Interval	3600	Number of seconds between device check-in to Lens cloud.
Gateway EUI	N/A	Gateway EUI (Extended Unique Identifier)
UUID	N/A	Universally Unique Identifier (128-bit ID)
Serial Number	N/A	Device serial number

**Messages** (available using Cloud Key Store)

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

**Gateway Info** (available using Cloud Key Store)

Parameter	Default Value	Description
Gateway EUI	N/A	Gateway EUI (Extended Unique Identifier)
UUID	N/A	Universally Unique Identifier (128-bit ID)
Serial Number	N/A	Device serial number

**Traffic Manager** (available using Cloud Key Store)

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

### Local Network Settings

Parameter	Default Value	Description
Enabled	Checked (enabled)	Enable or disable Local Network Settings.
Default Device Profile	N/A	Default device profile to use for newly joined end-devices authenticated with the Local Network Settings, AppEUI and AppKey. For information about LoRaWAN profiles, refer to <a href="#">Profiles</a> .
Network ID (AppEUI)	Name	Specify Network ID format from local application network ID or App EUI. Select from drop-down: Name or EUI.
Name	Uses local device name	Gateway device name
Default Network Profile	DEFAULT-CLASS-A	Default network profile to use for newly joined end-devices authenticated with the Local Network Settings, AppEUI and AppKey. For information about LoRaWAN profiles, refer to <a href="#">Profiles</a> .
Network Key (AppKey)	Passphrase	Choose Network Key from Passphrase or Key.
Passphrase	N/A	Enter Passphrase if used.
Key	N/A	Enter Key if used (128-bit hexadecimal value).

### Spectral Scan Configuration

Parameter	Default Value	Description
Enabled	Unchecked (disabled)	Enable or disable Spectral Scan.
<b>Scan Settings</b>		
Samples	10000	Total number of RSSI points.
Bandwidth	250	Channel bandwidth in kHz.
Step	100000	Frequency step between start and stop (in Hz).
Offset	0	Offset in dB to be applied to resultant data
Floor	-120	Threshold in dB below which results are ignored.
<b>Scheduling</b>		
Start	9:00	Start time for scans in UTC time. Leave blank to use current time.
Interval	1	Time period, in minutes, between run sets.
Stop	Never	Stop criteria for scans. Valid values are: <ul style="list-style-type: none"> <li>■ Never</li> <li>■ After Duration</li> <li>■ After Number of Scans</li> </ul>
Duration	1	Duration, in hours, of continuous scans. When Stop=After Duration, configure Duration=0 to run one single scan.
Scan Sets to Run	0	Scan limit. This parameter is enabled when Stop=After Number of Scans.
<b>Scan Sets</b> - First set range is required and two default ranges are provided. Others are optional up to 5 max. Each range set is independent and flexible. Enter start and stop range and click Add to add that range as an additional set. Click Remove to delete one.		
Start 1	902100000	Required Start frequency 1 in Hz
Stop 1	903900000	Required Stop frequency 1 in Hz
Start 2	923000000	Optional Start frequency 2 in Hz
Stop 2	928000000	Optional Stop frequency 2 in Hz

Parameter	Default Value	Description
Start 3	N/A	Optional Start frequency 3 in Hz
Stop 3	N/A	Optional Stop frequency 3 in Hz
Start 4	N/A	Optional Start frequency 4 in Hz
Stop 4	N/A	Optional Stop frequency 4 in Hz
Start 5	N/A	Optional Start frequency 5 in Hz
Stop 5	N/A	Optional Stop frequency 5 in Hz

## Gateways

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

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

### Packets Received

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

### Network Statistics

Parameter	Description
Join Request Responses	Average Join Request Response in milliseconds: 90%, 70%, 30%



Parameter	Description
Join Packets	Number of Okay packets, Duplicates and MIC fails, Unknown, Late, Total
Transmitted Packets	Pkt (Packets) 1st Wnd (Window), Pkt 2nd Wnd, ACK Pkt, Total, Join 1st Wnd, Join 2nd Wnd, Join Dropped, Join Total
Received Packets	MIC Fails, Duplicates, CRC Errors, Total
Scheduled Packets	1st Wnd, 2nd Wnd, Dropped, Total

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

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

## Devices

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

1. Go to **LoRaWAN > Devices**.
2. Under **End Devices**, click **Add New**.
3. Enter the following fields:
  - a. **Dev EUI** - the end-device EUI (Extended Unique Identifier)
  - b. **Name** - the name of the end-device
  - c. **Class** - LoRaWAN operating class of end-device. Is communicated to network server on Join. The end-device must be configured out-of-band for operating class. A, B, or C are currently supported. (A, B, or C).
  - d. **Serial Number** - Serial number of end-device
  - e. **Product ID** - Product ID for end-device
  - f. **Hardware Version** - Hardware version for the end-device
  - g. **Firmware Version** - Firmware version for the end-device
  - h. **LoRaWAN Version** - Software version for LoRaWAN server
4. Click **Finish**.
5. The new end-device displays under the **End Devices** list including some device details and statistics.
6. To edit the device, click the pencil icon, or to delete it, click the **X** icon associated with that device.
7. To delete all devices, click the **Delete All** button.

## Device Sessions

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

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

To add a new session manually:

1. Go to **LoRaWAN > Devices**.
2. Under **Sessions**, click **Add New**.
3. Enter the following fields:
  - a. **Dev EUI** - End-device EUI (Extended Unique Identifier)
  - b. **Dev Addr** - Network device address assigned to end-device
  - c. **Class** - Device Class (B or C)
  - d. **App EUI** - Application EUI
  - e. **Join EUI** - Join Request EUI
  - f. **Net ID** - Network ID
  - g. **App Session Key** - Pre-shared application session key
  - h. **Net Session Key** - Derived network session key based on pre-shared application key
  - i. **Multicast Session** - Select from:
    - No (i.e., not a multicast session)
    - Class B
    - Class C
4. Click **Finish**.
5. The new session displays under the **Sessions** list including some device details and statistics.
  - a. **Dev EUI** - End-device EUI (Extended Unique Identifier)
  - b. **Dev Addr** - Network device address assigned to end-device
  - c. **Up FCnt** - Packet counter of last received packet
  - d. **Down FCnt** - Packet counter of last sent packet
  - e. **Last Seen** - Time of last packet received
  - f. **Joined** - What is the device joined to, Cloud or local version
  - g. **Details** - Additional session information (click on info icon)
  - h. **Multicast Session** - Select from:
    - No (i.e., not a multicast session)
    - Class B
    - Class C
6. To edit the session, click the pencil icon, or to delete it, click the **X** icon associated with that session.

7. To delete all sessions, click the **Delete All** button.

## Device Groups

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

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

To create a new device group:

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

To import your device group:

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

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

### Groups table fields

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

## Profiles

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

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

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

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

To add a new device profile:

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

#### End-Device Profiles (edit/add new)

Parameter	Description
Profile ID	Profile name
Max EIRP	Maximum transmit power of the end-device
Max Duty Cycle	Maximum duty-cycle of the end-device
MAC Version	LoRaWAN version supported by end-device <b>Note:</b> MAC commands and network messages are different for <b>LW1_0</b> and <b>LW1_1</b> .
RF Region	End-device region or channel plan
Region Version	Revision of Regional Parameters specification
Supports C	True when the end-device can use class C mode

Parameter	Description
Timeout C	Time for the end-device to reply to a confirmed downlink before retransmission
Supports B	<b>True</b> when the end-device can use class B mode
Timeout B	Time for the end-device to reply to a confirmed downlink before retransmission
Ping Slot Period	How often the end-device opens class B windows Valid value: 1 (once per second) up to 128 (once per beacon period)
Ping Slot Datarate	Data rate used for class B window
Ping Slot Frequency	Frequency used for class B window
Supports Join	<b>True</b> when the end-device supports OTA join
Rx1 Delay	Default delay between the end of the Tx window and the beginning of the first Rx window  <b>Note:</b> When <b>Rx1 Delay</b> is not specified, the LoRaWAN default for the selected channel plan is used.
Rx1 DR Offset	Default data rate offset of the first Rx window  <b>Note:</b> When <b>Rx1 DR Offset</b> is not specified, the LoRaWAN default for the selected channel plan is used.
Rx2 DR Index	Default data rate of second Rx window  <b>Note:</b> When <b>Rx2 DR Index</b> is not specified, the LoRaWAN default for the selected channel plan is used.
Rx2 Frequency	Default frequency of second Rx window  <b>Note:</b> When <b>Rx2 Frequency</b> is not specified, the LoRaWAN default for the selected channel plan is used.
Preset Frequencies	Additional channels configured at the end-device
Supports 32 Bit FCnt	<b>True</b> when the end-device supports 32 bit counters

## Network Profiles

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

**Note:** Network profile settings will override device profile and network settings.

To add a new network profile:

1. Go to **LoRaWAN > Profiles**.
2. Under **Network Profiles**, click **Add New**.
3. Configure the following parameters as required:
  - a. Profile ID – Enter the desired profile name
  - b. Max Duty Cycle - Select from the drop-down including DEFAULT or a range of options from 100% to 0.003%
  - c. Class- Select from the drop-down including A, B, or C
  - d. Timeout Class C
  - e. Rx1 Delay
  - f. Rx1 DR Offset - Select from drop-down which varies with your selected channel plan.
  - g. Rx2 DR Index - Select from drop-down which varies with your selected channel plan.
  - h. Rx2 Frequency
  - i. Channel Mask
  - j. Redundancy

#### Network Profiles (edit/add new)

Parameter	Description
Profile ID	Profile name
Max Duty Cycle	Maximum duty-cycle of the end-device
Class	Operating class for end-device Valid values are: <ul style="list-style-type: none"> <li>■ A</li> <li>■ B</li> <li>■ C</li> </ul>
Timeout C	Time for the end-device to reply to a confirmed downlink before retransmission
Rx1 Delay	Default delay between the end of the Tx window and beginning of the first Rx window  <b>Note:</b> When <b>Rx1 Delay</b> is not specified, the LoRaWAN default for the selected channel plan is used.
Rx2 DR Index	Default data rate of the second Rx window  <b>Note:</b> When <b>Rx2 DR Index</b> is not specified, the LoRaWAN default for the selected channel plan is used.
Rx2 Frequency	Default frequency of the second Rx window  <b>Note:</b> When <b>Rx2 Frequency</b> is not specified, the LoRaWAN default for the selected channel plan is used.

Parameter	Description
Channel Mask	<p>The bitmask to enable channels</p> <p>The United States uses a 20-character bitmask structured as follows:</p> <ul style="list-style-type: none"> <li>■ The first two characters are not used and are set to zero (0)</li> <li>■ The next two characters control the 50 kHz channels</li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>■ The mask to enable all channels is 00FFFFFFFFFFFFFFFFFFFFFF</li> <li>■ The mask to enable the bottom half 000F00000000FFFFFFFF</li> </ul> <p>Australia uses a 20-character bitmask.</p> <p>All others use a 4-character bitmask. For example, in the EU, the mask to enable all channels is FFFF.</p>
Redundancy	The number of times an unconfirmed uplink should be repeated

## Packets

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

### Packets (Transmitted)

Parameter	Description
Device EUI	End-device EUI (Extended Unique Identifier) transmitting the uplink packet or destination of the downlink packet
Freq	Frequency used to transmit packet
Datarate	Datarate used to transmit packet
SNR	Signal to noise ratio of received packet
CRC	Cyclic redundancy check failed
RSSI	Received signal strength
Size	Size in bytes of packet
FCnt	MAC packet counter
Type	<p>Type of packet includes these possible values:</p> <ul style="list-style-type: none"> <li>■ <b>JnAcc</b> - Join Accept Packet</li> <li>■ <b>JnReq</b> - Join Request Packet</li> <li>■ <b>UpUnc</b> - Uplink Unconfirmed Packet</li> <li>■ <b>UpCnf</b> - Uplink Confirmed Packet - ACK response from network requested</li> <li>■ <b>DnUnc</b> - Downlink Unconfirmed Packet</li> <li>■ <b>DnCnf</b> - Downlink Confirmed Packet- ACK response from end-device requested</li> </ul>
Tx/Rx Time	Time packet was sent or received

Parameter	Description
Details	Additional packet details <b>Note:</b> Click on the <b>Info</b> icon to view the dialog.

### Recent Join Requests

Parameter	Description
Join EUI	8-byte EUI (Extended Unique Identifier) found in the join request
Nonce	Join nonce provided by end-device in the Join Request
Elapsed	Round trip time in milliseconds for the Join Server to service the join request
Result	<p>If the result of the request is valid, it displays: <b>Success</b>.</p> <p>If the result is an error, one of the following is displayed:</p> <ul style="list-style-type: none"> <li>■ <b>MICFailed</b> - AppKey setting did not match the end-device record in Join Server</li> <li>■ <b>Dropped</b> - Downlink packet could not be scheduled for transmit on any available gateways</li> <li>■ <b>Duplicate Dev Nonce</b> - Nonce in join request has already been used</li> <li>■ <b>JoinReq Failed</b> - Other server error</li> <li>■ <b>UnknownDevEUI</b> - Device record was not found at Join Server</li> <li>■ <b>Gateway Mismatch</b> - Join Server configuration does not allow this device to join through this gateway</li> <li>■ <b>Server Error</b> - Join Server is not reachable possibly due to Internet connection settings or DNS resolution</li> </ul>

### Recent Rx Packets

Parameter	Description
Time	Time packet was received
Freq	Frequency used to transmit packet
Datarate	Data rate used to transmit packet
CRC	Cyclic redundancy check failed
SNR	Signal to noise ratio of received packet
RSSI	Received signal strength



Parameter	Description
Size	Size in bytes of packet
Type	Type of packet includes these possible values: <ul style="list-style-type: none"> <li>■ <b>JnAcc</b> - Join Accept Packet</li> <li>■ <b>JnReq</b> - Join Request Packet</li> <li>■ <b>UpUnc</b> - Uplink Unconfirmed Packet</li> <li>■ <b>UpCnf</b> - Uplink Confirmed Packet - ACK response from network requested</li> <li>■ <b>DnUnc</b> - Downlink Unconfirmed Packet</li> <li>■ <b>DnCnf</b> - Downlink Confirmed Packet- ACK response from end-device requested</li> </ul>
Data	Actual data in packet (payload)
Details	Additional packet details <b>Note:</b> Click on the <b>Info</b> icon to view the dialog.

## Downlink Queue

Downlink packets can be manually sent to an end-device.

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

To manually send a downlink packet:

1. Go to **LoRaWAN > Downlink Queue**. Click on **Add New**.
2. Configure the following information for the new Queue Item:
  - a. **Dev EUI** - receiving end-device EUI (Extended Unique Identifier)
  - b. **App Port** - port field set in the downlink packet
  - c. **Data Format** - encoding scheme for the packet (select either Hex or Base64).
  - d. **Data** - the payload (data being transmitted)
  - e. **Ack Attempts** - number of allowed downlink request `ack` retries
  - f. **RxWindow** - specify the Rx Window to use for downlink. Valid values are:
    - 0: no priority
    - 1: First Rx window
    - 2: Second Rx window
3. Click **Finish**.
4. The new **Queue Item** displays under the **Downlink Queue** list including some device details and statistics.
  - a. **Dev EUI** - receiving end-device EUI (Extended Unique Identifier)
  - b. **App Port** - port field set in the downlink packet
  - c. **Size** - total packet minus header
  - d. **Ack** - number of retries to receive ACK from end-device

- e. **RxWnd** - the Rx Window to use for downlink:
    - 0: no priority
    - 1: First Rx window
    - 2: Second Rx window
  - f. **Queued** - Time packet has been added to the queue
  - g. **Details** - additional statistics displayed related to the packet
5. To edit the item, click the pencil icon, or to delete it, click the **X** icon associated with that item.
  6. To delete all items, click the **Delete All** button.

## Operations

The LoRaWAN **Operations** page offers two different features on one page:

- **FOTA**
- **Multicast Messaging**

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

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

To perform **FOTA**:

1. Go to **LoRaWAN > Operations**.
2. Under **Operations Settings**, select **FOTA** in the **Operation Type** drop-down.
3. Click **Browse** and select your **Firmware Upgrade File** (.bin).
4. Under the **Fragment Description** field, enter the fragment description for the FOTA session in HEX format.
5. You have the option to specify a **Setup Time In** by clicking **Change**. Setup time specifies how long from the time scheduled before the Multicast Setup Process begins. Under **Setup Time Input** from the drop-down, select either:
  - a. **Countdown to Setup from Now**: Enter **Number of Days** plus hours, minutes and seconds in **HH:MM:SS** (default: 30 seconds) **OR**
  - b. **Specify Future Date and Time**: Select your desired **Date** and **Time**.
6. Otherwise, click **Hide** to hide **Setup Time Input** details. Click **Change** to show and modify.
7. You have the option to specify a **Launch Time In**. Launch time specifies how long the Multicast Process runs before starting firmware transmission. Under **Launch Time Input** from drop-down, select either:
  - a. **Countdown to Launch from Setup**: Enter **Number of Days** plus hours, minutes and seconds in **HH:MM:SS** (default: 90 seconds) **OR**
  - b. **Specify Future Date and Time**: Select your desired **Date** and **Time**.

8. Choose the desired **Target End-Devices** to receive the upgrade. Select either a previously-saved **End-Device Group** or **Individual Devices** from the drop-down on the right. Check the box near your desired device or group to designate it for upgrade. You can also check **Select/Deselect All box** to select or deselect all groups in the list.
9. Click the **Settings** tab, if you wish to change the defaults for the following FOTA parameters
  - a. **Delete Successful Logs** (default: checked)
  - b. **Multicast Group ID**
  - c. **Number of Parity Fragments per Session** (default: 100)
  - d. **Sleep Delay between Setup Messages** (default: 1000 microseconds)
  - e. **Sleep Delay between Data Fragments** (default: 1500 microseconds)
  - f. **Sleep Delay between Parity Fragments** (default: 3000 microseconds)
  - g. **Maximum Packet Size**
10. After configuring FOTA, click **Schedule** to finalize your FOTA update.
11. Once the scheduled upgrade is submitted, you can track its progress through the **Progress** tab. A progress bar appears at the top of the page. The progress bar shows the transfer of the file from the PC to the device. Once completed, the page switches to the Progress tab. The job displays in either **Scheduled**, **Active**, or **Completed Jobs** lists depending on the job phase and timing.

To perform the **Multicast Messaging**:

1. Go to **LoRaWAN > Operations**.
2. Under **Operations Settings**, select **Message** in the **Operation Type** drop-down.
3. Select from either **Textbox** or **File** under **Payload Source**.
4. Select from either **Hexadecimal** or **Base64** under **Payload Format**.
5. Enter the message contents under **Payload**.
6. Enter the **Port** from a range of **1-220** (default: 1).
7. Under **Transmission Setup**, you have the option to specify a **Setup Time Input** by clicking **Change**. Setup time specifies how long from the time scheduled before the Multicast Setup Process begins. Expand the **Setup Time Input** drop-down and select from the following options:
  - a. **Countdown to Setup from Now**: Enter **Number of Days** plus hours, minutes, and seconds formatted as **HH:MM:SS** (default value: 30 seconds)
  - b. **Specify Future Date and Time**: Configure the desired **Date** and **Time**.
8. Otherwise, click **Hide** to hide **Setup Time Input** details. Click **Change** to show and modify.
9. You have the option to specify a **Launch Time Input**. Launch time specifies how long the Multicast Process runs before starting message transmission. Expand the **Launch Time Input** drop-down and select from the following options:
  - a. **Countdown to Launch from Setup**: Enter **Number of Days** plus hours, minutes, and seconds formatted as **HH:MM:SS** (default value: 90 seconds)
  - b. **Specify Future Date and Time**: Configure the desired **Date** and **Time**.
10. Choose the desired **Target End-Devices** to receive the message. Select either a previously-saved **End-Device Group** or **Individual Devices** from the drop-down on the right. Check the box

near the desired device or group to designate it to receive the message. You can also check **Select/Deselect All** box to select or deselect all groups in the list.

11. Click the **Settings** tab to change the defaults for the following message parameters:

- a. **Delete Successful Logs** (default value: checked)
- b. **Multicast Group ID**
- c. **Sleep Delay between Setup Messages** (default value: 1000 microseconds)
- d. **Sleep Delay between Data Fragments** (default value: 1500 microseconds)
- e. **Maximum Packet Size**

**Note:** The following parameters are constants for Multicast Messaging and cannot be modified:

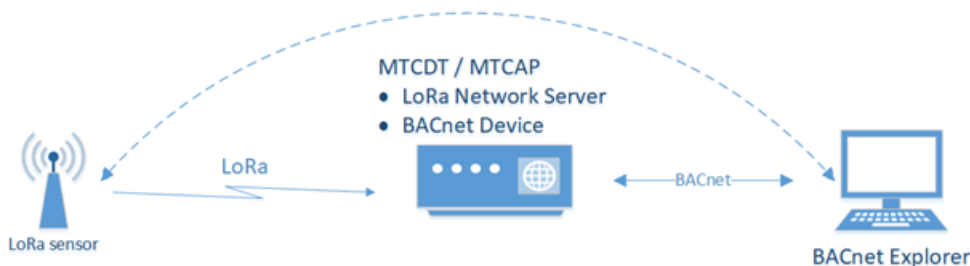
- **Number of Parity Fragments per Session:** value is **100**
- **Sleep Delay between Parity Fragments** value is **3000 microseconds**

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

## Payload Management

This chapter provides an overview about how to configure Payload Management settings such as BACnet Devices, sensors, and BACnet objects to receive BACnet data from LoRa sensors.

A typical application is illustrated here:



To get data from the LoRa sensor through mPower:

1. Verify the device has the BACnet license. BACnet payload management requires a license which is installed on your mPower device when it ships from the factory. If the Payload Management pages are not available, contact your account manager for a license.

**Note:** For information about adding a license, refer to [Licensing](#).

2. Configure the following [Network Settings](#):
  - a. Go to **Network Settings > Network Server**.
    - i. Set **LoRa Mode** to **Network Server**.
    - ii. Set the Channel Plan for your region.

- iii. Make sure the **Packer Forwarder** and the **Network Server** are running.
  - b. **Key Management** settings:
    - i. Set the **Join Server** to **Local Join Server**.
    - ii. Configure **Local Network Setting**.
    - iii. Configure **Local Network Setting**.
3. Set up and connect the sensor.

**Note:** This process is dependent upon the specific sensor being used. Refer to the sensor manufacturer's documentation for further information.
4. Open the **LoRaWAN > Packets** page. If the LoRaWAN network and sensor are configured properly, a Join Request from the sensor appears in the Recent Join Requests pane with the Success result. You will see Packets sent by the sensor in the Packets pane.
5. Click **Refresh** to update the data on the page.
6. Go to the **LoRaWAN > Devices** page. A new entry with the sensor Device EUI has been added to the End Devices and Sessions panes.
7. Configure **BACnet**.

**Note:** For complete information refer to [BACnet Configuration](#).
8. Add sensors.

**Note:** For complete information, refer to [Add Sensor](#).
9. Add/create BACnet objects.

**Note:** For complete information, refer to [Add a BACnet Object](#).
10. Configure a BACnet Explorer to get sensor data via BACnet.

**Note:** This process is dependent upon the specific BACnet Explorer is being used. Refer to the software developer's documentation for further information.

## BACnet Configuration

The BACnet Configuration page is illustrated here:

- Home
- LoRaWAN®
- Payload Management**
- BACnet Configuration
- Definitions and Templates
- Sensors
- Logs
- Setup
- Cellular
- Firewall
- Tunnels
- Administration
- Apps

### BACNET CONFIGURATION

#### General Settings

☒ Enabled

Vendor ID  
1331

Vendor Name  
Multi-Tech Systems, Inc.

#### BACnet Device Settings

Port  
47808

Interface  
br0

Device Object Identifier  
41943

APDU Timeout (seconds)  
3

Device Object Name  
Max Length is 128 characters

APDU Retries  
3

Device Description  
Device Description Max Length is 128 characters

Device Location  
Device Location Max Length is 128 characters

Parameter	Optional/Required	Value
<b>General Settings</b>		
Enabled	N/A	Enabled (slide to right)
<b>BACnet Device Settings</b>		
Port	Required	Numeric value: 1 to 65535
Interface	Required	Select the desired port from the pull-down list
Device Object Identifier	Required	Numeric value: 1 to 4194302
APDU Timeout (seconds)	Required	Numeric value: 1 to 65 Default value: 3
Device Object Name	Required	Character string Maximum length: 128 characters
APDU Retries	Required	Numeric value: 1 to 255 Default value: 3
Device Description	Optional	Character string Maximum length: 128 characters
Device Location	Optional	Character string Maximum length: 128 characters

## Definitions and Templates

The Definitions and Templates page lists information for all sensors that have been defined in the Conduit AP 300.

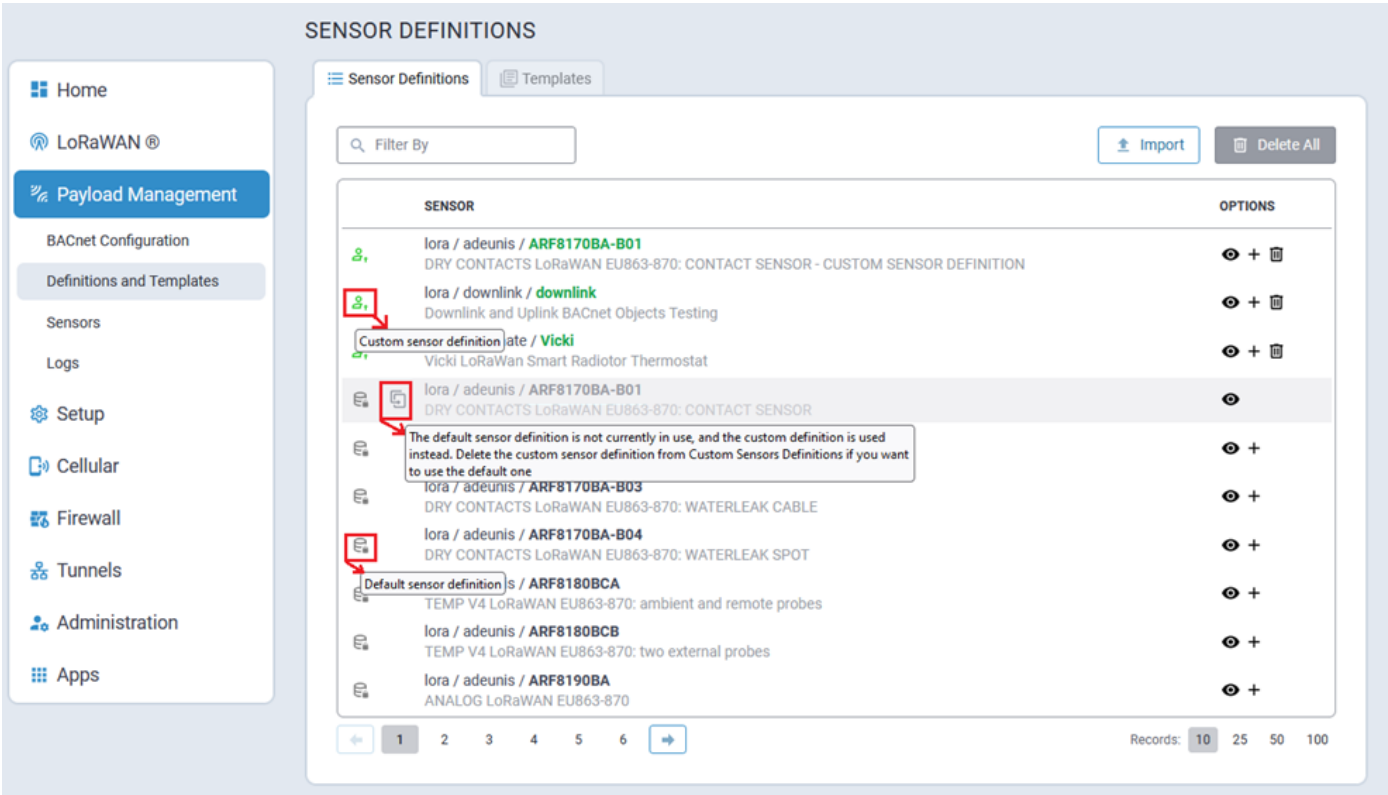
### Sensor Definitions

A Sensor Definition is a JSON file with a corresponding sensor decoder file.




The Sensor Definitions tab compiles the following sensor definitions:

- Current sensor definitions
- Default sensor definitions
- Custom sensor definitions
- Imported sensor definitions

The Sensor Definitions tab is illustrated here:





Each sensor definition is identified by one or more icons:


-  identifies default sensor definitions
-  identifies custom sensor definitions
-  identifies a custom sensor definition that is currently being overwritten by a custom sensor definition. When this is the case, as illustrated above, a tool tip is displayed when hovering the cursor over this icon.

**Note:** The Add Sensor control (+) will not be shown for these sensor definitions.

Available sensor definition **OPTIONS** are:

Icon	Option Information
	View detailed sensor definition information.

Icon	Option Information
+	Add Sensor control to the respective sensor definition.
	Delete the specified sensor control.

**Note:** Default sensors cannot be deleted. To delete all custom sensor definitions, click the  **Delete All** button and, when prompted, confirm deletion.

 **Delete All**

### *Filter the Sensor Definition List*

To filter the Sensor Definition list, enter the desired filter term in the **Filter By** field.

Sensor definitions may be filtered based on:

- Source
- Manufacturer
- Type
- Description

### *Import Sensor Definitions*

Importing custom sensor definitions is achieved by uploading a properly formatted Sensor Definition JSON file.

The Sensor Definition file describes the sensor data structure and corresponding sensor decoder that declares the decode Uplink function.

The Sensor Definition file for importing definitions must be in JSON format and include the following information:

- Description (optional)
- Properties (required)
- Decoder (required)

### **Example Sensor Definition JSON File Structure**

```
{
  "description" : "Optional description goes here",

  "properties" : {
    "DeviceID"           : {"type" : "string", "size" : 16},
    "DeviceStatus"       : {"type" : "uint8"},
    "BatteryVoltage"     : {"type" : "uint16", "units" : "amp"},
    "CounterA"           : {"type" : "uint16"},
    "CounterB"           : {"type" : "uint16"},
    "SensorStatus"       : {"type" : "uint8"},
    "TotalCounterA"      : {"type" : "uint16"},
    "TotalCounterB"      : {"type" : "uint16"},
    "PayloadCounter"     : {"type" : "uint8"}
  },

  "decoder": "SampleDecoder.js"
```



}

To import a custom sensor file, click on the  button. The **Details** pop-up dialog is displayed:

Details

Source

lora

Allow Overwrite

Manufacturer

Sensor Type

Files

Sensor Definition

No file selected

Sensor Decoder

No file selected

✓ Import

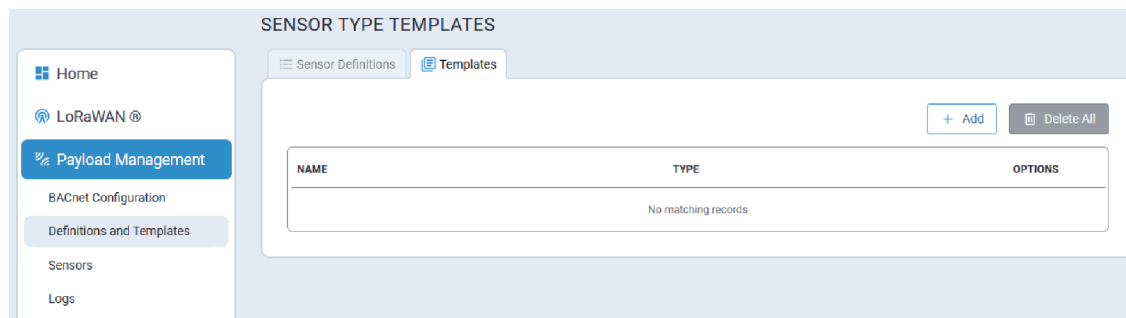
✕ Cancel

Parameter	Required/Optional	Value
Manufacturer	Required	<b>Case sensitive</b> character string Maximum length: 15 characters Must start with a letter and include only alphanumeric characters, hyphens, and underscores.
Sensor Type	Required	<b>Case sensitive</b> character string Maximum length: 32 characters Must start with a letter and include only alphanumeric characters, hyphens, and underscores.
Allow Overwrite	Optional	When importing a variation of an existing sensor type, enable this field to use the new sensor definition file.
Sensor Definition	Required	Path to the Sensor Definition JSON file to be imported

Parameter	Required/Optional	Value
Sensor Decoder	Required	Path to the Sensor Decoder file to be imported.

## Templates Tab

The Templates tab lists available user-defined Sensor Type Templates.



**Note:** By default there are no pre-defined templates provided.

Sensor Type Templates simplify and streamline the addition of multiple LoRaWAN sensors of the same type to the:

- Local Join Server (Local End-Device Credentials)
- Managed Sensors list

Additionally, Sensor Type Templates can be used to add the same set of BACnet Objects for each sensor.

### Add a Sensor Type Template

By default, there are no pre-defined templates provided. Users must add and configure their own templates in order to utilize templates.

Perform the following procedure to add a new Sensor Type template:

1. On the Sensor Type Templates page, click the **+ Add** button. The **Add Sensor Type Template** tab is displayed:

**ADD SENSOR TYPE TEMPLATE**

Sensor Definitions Templates + Add Sensor Type Template

**General Configuration**

Name

Sensor Definition

**LoRaWAN Device Details**

Class

Device Profile

Network Profile

**BACnet Objects** + Add Object

PROPERTY	OBJECT	OPTIONS
DOWNLINK-Test-BOOL bool	DOWNLINK-Test-BOOL - BV Binary Value	
UPLINK-Test-UINT8 uint8	UPLINK-Test-UINT8 - AV Analog Value	

Records: 10 25 50 100

2. Configure the following parameters for the new template:

Parameter	Required/Optional	Value
<b>General Configuration</b>		
Name	Required	Character string
Sensor Definition	Required	Sensor definition to which the template applies. Select the desired definition from the pull-down list.
<b>LoRaWAN Device Details</b>		
Class	Required	The LoRaWAN operating class of the end-device. This is transmitted to the network server on Join. The end-device must be configured out-of-band for operating class. Valid values are: <ul style="list-style-type: none"> <li>A</li> <li>B</li> <li>C</li> </ul>
Device Profile	Optional	
Network Profile	Optional	
<b>BACnet Objects</b>		
Property	N/A	Once a <b>Sensor Definition</b> has been selected, the system automatically adds all properties with a corresponding default Object Type. Refer to <a href="#">Supported BACnet Object Types</a> for complete information. If a different <b>Sensor Definition</b> is selected, this list will automatically be updated to reflect the new selection.

Parameter	Required/Optional	Value
Object	N/A	The system automatically generates the BACnet Object Name. <b>Format:</b> {PropertyName} - {BACnet_Object_Type_abbreviation}

- Click **Submit**.

### Add a BACnet Object to a Template

To add a BACnet Object to a Sensor Type template, click on the **+ Add Object** link above the list of BACnet objects.

The Add BACnet Object dialog is displayed:


Configure the following parameters:

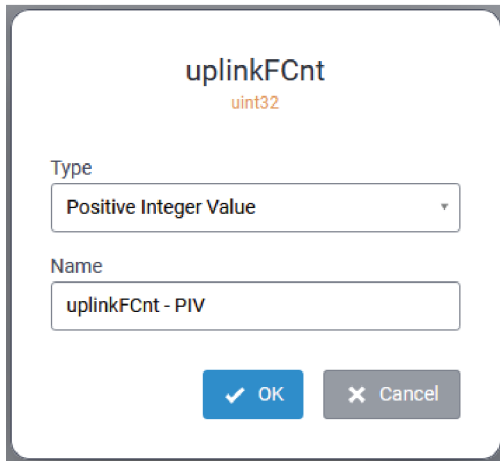
Parameter	Required/Optional	Value
Property	Required	Select the desired Property from the pull-down list.
Type	Required	Select the desired Type from the pull-down list. Refer to <a href="#">Supported BACnet Object Types</a> for complete information.
Name	Required	Format: {PropertyName} - {BACnet_Object_Type_abbreviation}  <b>Note:</b> The resulting BACnet Object Name will include the last four digits of the sensor Device EUI.

Once configured, click **OK** to save and add the object.

**Note:** Any number of BACnet objects may be added to a template.

### *Edit a BACnet Object in a Template*


BACnet Objects that are automatically added to a template may be edited. To edit a BACnet object, click the  associated with the object to be edited. The Edit BACnet Object dialog is displayed:



The dialog box is titled "uplinkFCnt" with "uint32" in orange text below it. It contains two input fields: "Type" with a dropdown menu showing "Positive Integer Value", and "Name" with a text box containing "uplinkFCnt - PIV". At the bottom are two buttons: "OK" (blue with a checkmark) and "Cancel" (grey with an X).

Update the **Type** and/or **Name** parameters as required, and click **OK** to save the changes.

### *Delete a BACnet Object from a Template*

To delete a BACnet object from a template, click the  associated with the object to be deleted. When prompted, confirm the deletion.

## Sensors

The Sensors page provides access to the following sensor-specific tabs:

- Sensors
- BACnet Objects

### Sensors Tab

The Sensors tab displays a list of all manages sensors, similar to that shown here:

### SENSORS

[Sensors](#)
[BACnet Objects](#)

[Download](#)
[Import](#)
[Apply Template](#)
[+ Add Sensor](#)
[Delete All](#)

DEVICE EUI	SOURCE	MANUFACTURER	TYPE	OPTIONS
70-b3-d5-2d-d3-01-91-b6	lora	mClimate	Vicki	
12-34-56-78-90-00-00-01	lora	downlink	downlink	
00-00-00-00-00-00-00-01	lora	downlink	downlink	

Records: 10 25 50 100

### Filter Sensors List

To filter the Sensors list, enter the desired filter term in the **Filter By** field.

Sensors may be filtered based on:

- Source
- Manufacturer
- Type
- Description

### View Sensor Details

To view sensor details for a sensor, on the Sensors page click the associated with the desired sensor. The **Sensor Details** page is displayed:

### Managed Sensor

Device EUI

70-b3-d5-2d-d3-01-91-b6

Source

lora

Type

mClimate/Vicki

BACnet Objects

[+ Add Object](#)

ID	PROPERTY	NAME	TYPE	OPTIONS
0	JoinRetryPeriod	test test	Analog Input	
11	JoinRetryPeriod	JoinRetry-PIV-Name JoinRetry-PIV-Description	Positive Integer Value	

Records: 10 25 50 100

OK

**Note:** The pages includes a link for adding new BACnet objects. For more information, refer to [Add a BACnet Object](#).

### Add Sensor

Perform the following procedure to add a managed sensor:

1. On the **Sensors** tab, click the **+ Add Sensor** link at the top of the page.
2. Enter the **Device EUI** in the format `XX-XX-XX-XX-XX-XX-XX-XX`.
3. Select the sensor **Manufacturer** from the drop-down list.
4. Select the sensor type from the **Type** drop-down list. These options depend on the Manufacturer selected in the previous step.
5. Click Finish to add the sensor.

### Apply Template

The use of Sensor Type templates streamlines the addition of LoRaWAN devices to the list of managed sensors.

**Note:** For complete information about creating Sensor Type templates, refer to the [Templates Tab](#).

**Note:** If there are no sensor type templates in the system, the **Apply Template** option on the [Sensors](#) tab will be disabled.

When applying a sensor type template to a list of sensors, the system makes the following changes:

- Local End-Device credentials are added. Note the following:
  - Credentials are added *only* if the Local Join Server is **enabled**.
  - Local End-Devices are not added, and a warning message is displayed, if:
    - The Local Join Server is **disabled**
    - There is at least one sensor with DevEUI already present in the Local End-Devices list.

**Note:** Refer to [Key Management](#) for additional information.

- Sensors are added to the [Sensors](#) list using the sensor definition specified by the selected **Sensor Type Template**.
  - If one or more sensors is being added with a DevEUI that is already in the sensors list, the system will display an error message and stop adding sensors. The user can delete the duplicate sensor and try again.
- BACnet Objects are added for each sensor on the list.

**Note:** Sensors are added to the Sensors list and BACnet Objects are created even if no Local End-Devices are added by the system.

A typical **Apply Template** tab is shown here:

### APPLY TEMPLATE

Sensors
BACnet Objects
**Apply Template**

---

#### General Configuration

Sensor Type Template  
Downlink Testing

BACnet Object Identifier Start Value  
100

---

#### Sensors

+ Add ↑ Import

DEVICE EUI	APP EUI	APP KEY	OPTIONS
70-B3-D5-2D-D3-01-91-11	70-B3-D5-2D-D3-00-00-01	2A-8C-C1-12-F0-E4-18-F9-A2-C1-AE-AE-1E-75-00-11	
70-B3-D5-2D-D3-01-91-12	70-B3-D5-2D-D3-00-00-02	6E-27-51-00-D9-D3-98-0F-A4-55-5C-DC-C9-8D-00-12	
70-B3-D5-2D-D3-01-8D-13	70-B3-D5-2D-D3-00-00-03	3C-DE-E5-C2-B5-49-FD-D9-9D-61-AB-CD-F1-1A-00-13	
ab-cd-ef-12-34-56-78-90	ab-cd-ef-12-34-56-78-90	AB-cd-ef-C2-B5-49-FD-D9-9D-61-AB-CD-F1-1A-00-04	

Records: 10 25 50 100

✓ Submit

✕ Cancel

To apply a Sensor Type template:

1. Select the desired **Sensor Type Template** from the pull-down.
2. Specify the **BACnet Object Identifier Start Value**.
  - The system will increment this value for each new BACnet object added while applying the template.
  - If the specified ID value is already in use, the system will skip it and apply a different value.
3. Add sensor details using one of the following methods:
  - Click **+ Add** to manually add the following sensor information:
    - Device EUI
    - App EUI
    - App Key

**Note:** Refer to [Key Management](#) for additional information.
  - Click **Import** to import sensor data from a CSV file.

**Note:** Refer to [Sensors Data CSV Files](#) for complete information.
4. Click **Submit**.

Once the template has been applied and the corresponding sensors/BACnet objects created, there is no dependency or connection between created items and the template. The template can be modified or deleted without affecting items created using the template.



## Sensors Data CSV Files

Sensor data can be formatted in a CSV file and then uploaded for use with templates. This is particularly helpful when applying a template to a large number of sensors.

Although the system does not require the CSV file to include a header, be aware of the following when creating sensor file:

- If the sensor CSV file includes a header, when the file is uploaded the system searches for the **DevEUI**, **AppEUI**, and **AppKey** columns, parses the file, and retrieves only those values that are required. For example:

#	SerialNumber	DevEui	AppEui	AppKey	DeviceType	Firmware Version	Date of manufacturing
1	1A1B2687547CD4	1111111111111401	1231231299992401	1231231212312312123FF31212312401	Vicki LoRaWAN	4.3	11/9/2023
2	2EFG268712HJKL	2222222222222402	1235533212312402	1231231212312312123FF31212312402	Vicki LoRaWAN	4.3	11/9/2023
3	3MNP26773715R3	3333333333333403	1235533123123403	123123121231232123FFE31212312403	Vicki LoRaWAN	4.3	11/9/2023
4	12345 ABCDEF1234567890		ABCDEF1234567890	123123121231232123FFE31212312404	N/A	N/A	N/A

#	SerialNumber	DevEui	AppEui	AppKey	DeviceType	Firmware Version	Date of manufacturing
1	1A1B2687547CD4	11:11:11:11:11:14:01	12:31:23:12:99:99:24:01	12:31:23:12:12:31:23:12:12:3F:F3:12:12:31:24:01	Vicki LoRaWAN	4.3	11/9/2023
2	2EFG268712HJKL	22:22:22:22:22:24:02	12:35:53:32:12:31:24:02	12:31:23:12:12:31:23:12:12:3F:F3:12:12:31:24:02	Vicki LoRaWAN	4.3	11/9/2023
3	3MNP26773715R3	33:33:33:33:33:34:03	12:35:53:31:23:12:34:03	12:31:23:12:12:31:23:21:23:FF:E3:12:12:31:24:03	Vicki LoRaWAN	4.3	11/9/2023
4	12345 AB:CD:EF:12:34:56:78:90		AB:CD:EF:12:34:56:78:90	12:31:23:12:12:31:23:21:23:FF:E3:12:12:31:24:04	N/A	N/A	N/A

- If the sensor CSV file does **NOT** include a header, the first three columns of sensor data must be:
  - DevEUI
  - AppEUI
  - AppKey

In the following example, the first three columns of data are added as DevEUI, AppEUI, and AppKey.

```
11111111111111401, 1231231299992401, 1231231212312312123FF31212312401, A, LW102-OTA-US915, DEFAULT-CLASS-A
2222222222222402, 1235533212312402, 1231231212312312123FF31212312402, B, LW102-OTA-US915, DEFAULT-CLASS-B
3333333333333403, 1235533123123403, 123123121231232123FFE31212312403, C, LW102-OTA-US915, DEFAULT-CLASS-C
```

## Edit Sensor Details

The following BACnet Object fields may be updated:

- Type
- Identifier
- Name
- Description

**Note:** The Property field is read-only.

Perform the following procedure to edit details for a sensor:

1. On the Sensors page, click on the pencil icon associated with the sensor to be edited. The Sensor Details dialog is displayed.

**Managed Sensor**

Device EUI: 70-b3-d5-2d-d3-01-91-b6

Source: loro

Type: mClimate/Vicki

**BACnet Objects** [+ Add Object](#)

ID	PROPERTY	NAME	TYPE	OPTIONS
0	JoinRetryPeriod	test	Analog Input	
11	JoinRetryPeriod	JoinRetry-PIV-Name JoinRetry-PIV-Description	Positive Integer Value	

Records: 10 25 50 100

- Expand the Device EUI pull-down and select the desired EUI from the list. The system will display all BACnet objects for the selected Device EUI.
- From the list of BACnet Objects, locate the object to be edited, and click on the corresponding pencil icon to display the BACnet Object details pop-up.

Property: UPLINK-Test-FLOAT (float)

Type: Analog Value

Identifier: 14

Name: FLOAT UPLINK - Analog Value

Description: FLOAT UPLINK - Analog Value Description

- Edit the fields as required.
- Click **OK** to save changes.

### Delete Sensors

To delete a specific sensor, on the Sensors tab, locate the sensor that is to be deleted and click on the corresponding icon. When prompted, confirm the deletion.

To delete all sensors, click the  **Delete All** icon/link on the top of the Sensors tab page. When prompted, confirm the deletion.

### Sensor Map JSON Files

mPower stores Sensor maps in JSON format.

Information for each sensor included in the system is structured as follows:

```
[
  {
    "id" : "",
    "sensor" : "",
    "src" : ""
  }
]
```

Parameter Name	Optional/Required	Value
id	Required	The 16-digit sensor Device EUI for the sensor in the format xx-xx-xx-xx-xx-xx-xx-xx
sensor	Required	The manufacturer's name and sensor model formatted as follows: {manufacturer_name}/{sensor_model}
src	Required	lora This is currently the only supported value. This value is case-sensitive and must be lower case.

A typical Sensor map with three sensors is shown here:

```
[
  {
    "id" : "11-22-33-44-55-66-77-80",
    "sensor" : "elsys/EMS",
    "src" : "lora"
  },
  {
    "id" : "11-22-33-44-55-66-77-81",
    "sensor" : "elsys/ERSCO2",
    "src" : "lora"
  },
  {
    "id" : "00-10-20-30-40-50-60-70",
    "sensor" : "manufacturer/test",
    "src" : "lora"
  }
]
```

### Import Sensor Map

LoRa sensors may be added by importing a JSON-formatted Sensor map.

**Note:** An imported Sensor map overwrites the existing Sensor map.

The Sensor map being imported must be a properly-formatted JSON file as defined in [Sensor Map JSON Files](#).

Perform the following procedure to import a JSON-formatted Sensor map:

1. On the [Sensors page](#), click the **Import** link at the top of the page.
2. Click the **Folder** icon under **Choose File** and navigate to the desired JSON file.
3. Click **Import**.
4. Click **Save and Apply**.

### Download the Sensor Map

Perform the following procedure to download the Sensor map as a JSON file:

1. Click the **Download** link on the top of the [Sensors page](#).
2. When prompted, navigate to the directory where the Sensor map JSON file is to be saved.
3. Click **OK**.

**Note:** Refer to [Sensor Map JSON Files](#) for information about how the downloaded Sensor data are formatted.

## BACnet Objects Tab

BACnet Objects define the data transferred from a sensor to the BACnet explorer.

The BACnet Object tab displays the current BACnet Objects Map similar to this:

**BACNET OBJECTS**

Sensors | **BACnet Objects**

BACnet Objects Map Download Import + Add Object Delete All

Type: All Filter By

ID	NAME	PROPERTY	SENSOR ID	OPTIONS
0	test	JoinRetryPeriod Analog Input	lora@70-b3-d5-2d-d3-01-91-b6	
0	Downlink_INT16_IntegerValue Changed to Analog Value Downlink_INT16_IntegerValue Changed to Analog Value Description	DOWNLINK-TEST-INT16 Analog Value	lora@00-00-00-00-00-00-01	
1	Uplink Int Test16 Integer Value Changed to Analog Value Uplink Int Test16 - descirptio Chnged to Analog Value	UPLINK-TEST-INT16 Analog Value	lora@00-00-00-00-00-00-01	

Records: 10 25 50 100

### Filter BACnet Object Map

To filter the BACnet object map, enter the desired filter term in the **Filter By** field.

The map may be filtered based on:

- Type
- ID

- Name
- Sensor ID
- Property

### *Edit a BACnet Object*

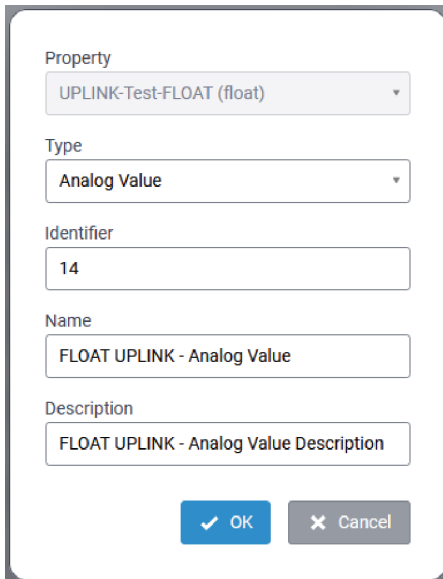
The following BACnet Object fields may be updated:

- Type
- Identifier
- Name
- Description

**Note:** The Property field is read-only.

Perform the following procedure to edit details for a BACnet object:

1. Within the BACnet Objects Map, click on the pencil icon associated with the object to be edited. The BACnet Object details pop-up is displayed.



The image shows a BACnet Object details pop-up dialog box. It contains the following fields:

- Property:** A dropdown menu showing "UPLINK-Test-FLOAT (float)".
- Type:** A dropdown menu showing "Analog Value".
- Identifier:** A text input field containing the number "14".
- Name:** A text input field containing "FLOAT UPLINK - Analog Value".
- Description:** A text input field containing "FLOAT UPLINK - Analog Value Description".

At the bottom of the dialog box, there are two buttons: a blue "OK" button with a checkmark icon and a grey "Cancel" button with an 'X' icon.

2. Edit the fields as required.
3. Click **OK** to save changes.

### *Add a BACnet Object*

**Note:** Before adding a BACnet Object, one or more sensors must first be added. Refer to [Add Sensor](#) for additional information.

Perform the following procedure to add a new BACnet object:

1. On the BACnet Objects tab page, click the **Add Object** link at the top of the page. The **Sensor Details** dialog is displayed.

Managed Sensor

Device EUI

70-b3-d5-2d-d3-01-91-b6

Source

lora

Type

mClimate/Vicki

BACnet Objects

+ Add Object

ID	PROPERTY	NAME	TYPE	OPTIONS
0	JoinRetryPeriod	test test	Analog Input	
11	JoinRetryPeriod	JoinRetry-PIV-Name JoinRetry-PIV-Description	Positive Integer Value	

Records: 10 25 50 100

OK

2. Expand the Device EUI pull-down and select the EUI for the new BACnet object.  
**Note:** A list of all BACnet objects for the selected EUI is then displayed.
3. Click **+ Add Object**. The New BACnet Object properties pop-up dialog is displayed.

Property

DOWNLINK-TEST-INT16 (int16)

Type

Integer Value

Identifier

0

Name

Description

OK

Cancel

4. Configure the following parameters:

Parameter	Required/Optional	Value
Property	Required	A list of properties corresponding to the selected Device EUI.
Type	Required	Available values are based on the configured <b>Property</b> value. Refer to <a href="#">Supported BACnet Object Types</a> for complete information.
Identifier	Required	Unique identifier for BACnet objects of the same type. Numeric value: 0 - 4194302

Parameter	Required/Optional	Value
Name	Required	Character string Maximum length: 128 characters
Description	Optional	Character string Maximum length: 128 characters

5. Click **OK**.

**Note:** If an object of the same type and identifier exists, or if a required field is empty, an error message is returned.

### *Supported BACnet Object Types*

Supported BACnet object types vary based on UPLINK and DOWNLINK properties.

**Note:** BACnet Objects Maps do not store uplink or downlink information. [Sensor definition](#) files distinguish between uplink and downlink properties.

#### **UPLINK BACnet Object Types**


Property Type	Supported BACnet Object Types
uint8	Analog Value, Analog Input, Positive Integer Value
uint16	Analog Value, Analog Input, Positive Integer Value
uint32	Positive Integer Value
int8	Analog Value, Analog Input, Integer Value
int16	Analog Value, Analog Input, Integer Value
int32	Integer Value
float	Analog Value, Analog Input
bool	Binary Value, Binary Input
string	Character String Value

#### **DOWNLINK BACnet Object Types**

Property Type	Supported BACnet Object Types
uint8	Positive Integer Value, Analog Value
uint16	Positive Integer Value, Analog Value
uint32	Positive Integer Value
int8	Integer Value, Analog Value
int16	Integer Value, Analog Value
int32	Integer Value
float	Analog Value
bool	Binary Value

Property Type	Supported BACnet Object Types
string	Character String Value

### Delete BACnet Objects

To delete a specific BACnet object, on the BACnet Objects page, locate the object that is to be deleted and click on the corresponding  icon. When prompted, confirm the deletion.

To delete all BACnet objects, click the  **Delete All** icon/link on the top of the BACnet Objects page. When prompted, confirm the deletion.

### BACnet Object Map JSON Files

mPower stores BACnet Object maps in JSON format. The JSON file includes any combination of the following object-type containers:

```
{
  "analog-inputs" : [],
  "analog-values" : [],
  "binary-inputs" : [],
  "binary-values" : [],
  "character-string-values" : [],
  "integer-values" : [],
  "positive-integer-values" : []
}
```

Each object-type container stores configuration details for each object of that type currently defined in the system.

**Note:** Refer to [Supported BACnet Object Types](#) for additional information.

Within each container, the BACnet object information is structured as follows:

```
[
  {
    "descr" : "",
    "key" : "",
    "name" : "",
    "oid" : 0
  }
]
```

Parameter	Optional/Required	Value
descr	Optional	Character string describing the object. This parameter may be empty.



Parameter	Optional/Required	Value
key	Required	<p>This value is formatted as follows:  {src}@{DeviceEUI}@{Name}</p> <p>where:</p> <ul style="list-style-type: none"> <li>■ src = lora</li> <li>■ DevEUI is the 16-digit Device EUI for the sensor in the format <b>xx-xx-xx-xx-xx-xx-xx-xx</b></li> <li>■ Name is the BACnet object's name.</li> </ul> <p>For example:  lora@00-10-20-30-40-50-60-70@UPLINK-TEST-INT16</p>
name	Required	User-assigned name for the BACnet object.
oid	Required	<p>Integer value.</p> <p>This value is unique <b>for each BACnet object within an object type</b> (e.g., analog-inputs, integer-values.)</p> <p>BACnet objects of different types may be configured with the same oid value.</p>

A typical BACnet Object map is shown here:

```
{
  "analog-inputs" :
  [
    {
      "descr" : "",
      "key" : "lora@00-10-20-30-40-50-60-70@UPLINK-TEST-INT16",
      "name" : "UPLINK-TEST-INT16 - AI-6070",
      "oid" : 0
    }
  ],
  "analog-values" :
  [
    {
      "descr" : "",
      "key" : "lora@00-10-20-30-40-50-60-70@DOWNLINK-Test-FLOAT",
      "name" : "DOWNLINK-Test-FLOAT - AV-6070",
      "oid" : 0
    },
    {
      "descr" : "",
      "key" : "lora@00-10-20-30-40-50-60-70@UPLINK-TEST-INT16",
      "name" : "UPLINK-TEST-INT16 - AV-6070",
      "oid" : 1
    }
  ],
  "binary-inputs" :
  [
    {
```

```
        "descr" : "",
        "key" : "lora@00-10-20-30-40-50-60-70@UPLINK-Test-BOOL",
        "name" : "UPLINK-Test-BOOL - BI-6070",
        "oid" : 0
    },
],
"binary-values" :
[
    {
        "descr" : "",
        "key" : "lora@00-10-20-30-40-50-60-70@DOWNLINK-Test-BOOL",
        "name" : "DOWNLINK-Test-BOOL - BV-6070",
        "oid" : 0
    },
    {
        "descr" : "",
        "key" : "lora@00-10-20-30-40-50-60-70@UPLINK-Test-BOOL",
        "name" : "UPLINK-Test-BOOL - BV-6070",
        "oid" : 1
    }
],
"character-string-values" :
[
    {
        "descr" : "",
        "key" : "lora@00-10-20-30-40-50-60-70@DOWNLINK-TEST-STRING",
        "name" : "DOWNLINK-TEST-STRING - CSV-6070",
        "oid" : 0
    },
],
"integer-values" :
[
    {
        "descr" : "",
        "key" : "lora@00-10-20-30-40-50-60-70@DOWNLINK-TEST-INT16",
        "name" : "DOWNLINK-TEST-INT16 - IV-6070",
        "oid" : 0
    },
    {
        "descr" : "",
        "key" : "lora@00-10-20-30-40-50-60-70@DOWNLINK-TEST-INT32",
        "name" : "DOWNLINK-TEST-INT32 - IV-6070",
        "oid" : 1
    },
    {
        "descr" : "",
        "key" : "lora@00-10-20-30-40-50-60-70@DOWNLINK-TEST-INT8",
        "name" : "DOWNLINK-TEST-INT8 - IV-6070",
        "oid" : 2
    }
]
```

```

    ],
    "positive-integer-values" :
    [
        {
            "descr" : "",
            "key" : "lora@00-10-20-30-40-50-60-70@DOWNLINK-Test-UINT16",
            "name" : "DOWNLINK-Test-UINT16 - PIV-6070",
            "oid" : 0
        },
        {
            "descr" : "",
            "key" : "lora@00-10-20-30-40-50-60-70@DOWNLINK-Test-UINT32",
            "name" : "DOWNLINK-Test-UINT32 - PIV-6070",
            "oid" : 1
        }
    ]
}

```

### Import BACnet Object Map

BACnet Objects may be added by importing a JSON-formatted BACnet Objects map.

**Note:** An imported BACnet Objects map overwrites the existing BACnet Objects map.

The BACnet Objects map being imported must be a properly-formatted JSON file as defined in [BACnet Object Map JSON Files](#).

Perform the following procedure to import a JSON-formatted BACnet Objects map file:

1. On the [BACnet Objects](#) page, click the **Import** link at the top of the page.
2. Click the **Folder** icon under **Choose File** and navigate to the desired JSON file.
3. Click **Import**.
4. Click **Save and Apply**.

### Download the BACnet Objects Map

Perform the following procedure to download the BACnet Objects map as a JSON file:

1. Click the **Download** link on the top of the [BACnet Objects](#) page.
2. When prompted, navigate to the directory where the BACnet Objects map JSON file is to be saved.
3. Click **OK**.

**Note:** Refer to [BACnet Object Map JSON Files](#) for information about how the downloaded BACnet Object data are formatted.

## Setup Menu

The Setup menu provides access to the following configuration settings:

- Network Interfaces

- WAN Configuration
- Global DNS
- DDNS Configuration
- DHCP Configuration
- LLDP Configuration
- SMTP Configuration
- SNMP Configuration
- Time Configuration

## Network Interface Configuration

By default:

- eth0 is configured as LAN

NAME	DIRECTION	TYPE	IP MODE	IP ADDRESS	BRIDGE	OPTIONS
eth0	LAN	Ethernet	Static	192.168.2.1/24	br0	
ppp0	WAN IPv4	Cellular	Auto	10.88.29.164		
br0	LAN IPv4	Bridge	Static	192.168.2.1/24		

### 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**.

NETWORK INTERFACE CONFIGURATION - ETH0

Direction: LAN Bridge: br0

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

NETWORK INTERFACE CONFIGURATION - ETH0

Direction: LAN Bridge: --

☐ Enable IPv6 Support

IPv4 Settings

Mode: Static Gateway:

IP Address:  Primary DNS Server:

Mask:  Secondary DNS Server:

802.1X Authentication

Authentication Method: NONE

## Configure br0

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

Direction

LAN

☐

Enable IPv6 Support

IPv4 Settings

Mode

Static

IP Address

192.168.2.1

Mask

255.255.255.0

Gateway

Primary DNS Server

Secondary DNS Server

✓ Submit

✕ Cancel

## Ethernet Interface Configuration Parameters

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

Parameter	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 or WLAN1 to use VLAN with the specified VLAN ID.

NETWORK INTERFACE CONFIGURATION - ADD VLAN

Direction  
LAN

VLAN ID

☐ Enable IPv6 Support

IPv4 Settings

Mode  
Static

Gateway

IP Address

Primary DNS Server

Mask

Secondary DNS Server

Submit

Cancel

Typical VLAN interfaces are illustrated here:

NETWORK INTERFACES CONFIGURATION

+ Add VLAN

Reset To Default

NAME	DIRECTION	TYPE	IP MODE	IP ADDRESS	BRIDGE	OPTIONS
eth0	VLAN	Ethernet	--			
ppp0	WAN IPv4	Cellular	Auto	10.88.29.164		
br0	LAN IPv4	Bridge	Static	192.168.2.1/24	br0	
vlan.20	LAN IPv4	VLAN	Static	192.168.20.1/24		

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	<input type="checkbox"/>	WAN IPv4	DHCP Client		
vlan.31	<input checked="" type="checkbox"/>	LAN IPv4	Static	192.168.3.1/24	

✓ Submit

✕ Cancel

## WAN Configuration

All WAN interfaces on the device should be configured for FAILOVER Mode.



Home

LoRaWAN®

Payload Management

Setup

Network Interfaces

WAN Configuration

Global DNS

DDNS Configuration

DHCP Configuration

LLDP Configuration

SMTP Configuration

SNMP Configuration

Time Configuration

Cellular

Firewall

Tunnels

Administration

Apps

WAN CONFIGURATION

General Configuration

Mode FAILOVER

WANs

STATE	NAME	TYPE	OPTIONS
Disabled	eth0	ETHERNET	^ v ✎
Enabled	ppp0	CELLULAR	^ v ✎

Reset To Default

Any VLANs added to the system will also be displayed as shown here:

Home

LoRaWAN®

Payload Management

Setup

Network Interfaces

WAN Configuration

Global DNS

DDNS Configuration

DHCP Configuration

LLDP Configuration

SMTP Configuration

SNMP Configuration

Time Configuration

Cellular

Firewall

Tunnels

Administration

Apps

WAN CONFIGURATION

General Configuration

Mode FAILOVER

WANs

STATE	NAME	TYPE	OPTIONS
Disabled	eth0	ETHERNET	^ v ✎
Enabled	ppp0	CELLULAR	^ v ✎
Disabled	vlan.20	VLAN	^ v ✎

Reset To Default

Each WAN interface can be configured for 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.

FAILOVER CONFIGURATION (ETH0)

Monitoring Mode

ACTIVE

Interval (secs)

60

Hostname

www.google.com

Mode Type

ICMP

ICMP Count

5

✓ Save

✕ Cancel

## Global DNS

A typical Global DNS Configuration page is illustrated here:

GLOBAL DNS CONFIGURATION

Global DNS Configuration

☒ Enable Forwarding Server

Primary Server

Secondary Server

Reset To Default

Hostname Configuration

Hostname

mtcap3-23067168

✓ Submit

Reset To Default

Global DNS enables user-defined DNS servers to be specified which are always used to resolve hostnames regardless of what WAN settings or interface are being used. If the **Primary Server** and

**Secondary Server** are not specified, the DNS servers will default to those specified in the [WAN Configuration](#) setup.

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.

Configuration scenarios for **Global DNS** and forwarding server, and their results (the device refers to a MultiTech device) include:

- If **Global DNS** is not configured and forwarding is enabled, the Conduit AP 300 acts as a proxy server for any devices on the LAN network(s).  
In this mode, the Conduit AP 300 uses WAN DNS settings.  
**Client Settings:** On the client, you must configure the Conduit AP 300 as the default gateway and DNS server. The easiest way to accomplish this is by using the DHCP server on the Conduit AP 300.
- If **Global DNS** is configured and forwarding is enabled, DNS requests are forwarded to servers configured in the **Global DNS** settings.  
The Conduit AP 300 acts as a proxy.  
**Client settings:** Clients must be configured the same as in the previous case above.
- If **Global DNS** is configured and forwarding is disabled, the default gateway and DHCP server on clients should point to the Conduit AP 300, and the DNS servers on the client must use the same DNS as the **Global DNS** settings.  
**Client settings:** The client device uses the Conduit AP 300 as a default gateway and DHCP server, but it must have DNS servers configured to the options that will be used.
- If neither item is configured/enabled, verify the Conduit AP 300 is properly configured to forward DNS.

## DDNS Configuration

Default DDNS configuration settings are illustrated here:

### DDNS 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
- Custom Apps

#### General Configuration

☐ Enabled

☒ Use External Check IP

Domain

Check IP Server

Service Provider

#### Authentication

Username

Password

#### Update Settings

Force Update Interval (days)

Check IP Interval (minutes)

#### Commands

DDNS Force Update

[Update](#)

DDNS Status

DDNS is disabled

[Submit](#)

[Reset To Default](#)

## DDNS Configuration Parameters

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

Parameter	Default Value	Value
Enabled	FALSE	True, False
Domain	empty	A valid domain name
<b>Custom Service</b>		
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

Parameter	Default Value	Value
Use External Check IP	TRUE	True, False
<b>Custom Check IP Server</b>		
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:

### DHCP CONFIGURATION

- Home
- Setup**
- Network Interfaces
- WAN Configuration
- Global DNS
- DDNS Configuration
- DHCP Configuration**
- LLDP Configuration
- GPS Configuration
- SMTP Configuration
- SNMP Configuration
- Time Configuration
- Digital I/O
- Cellular
- Wireless
- Firewall
- Tunnels
- Administration
- Apps

DHCP Configuration
+ Add IPv4 DHCP Server
+ Add DHCPv6/RA

#### DHCP

☒ Enabled

Interface: vlan.31

Gateway:

Domain:

Lease Range Start:

Subnet: 192.168.3.0

Mask: 255.255.255.0

Lease time (dd-hh-mm): 01-00-00

Lease Range End:

✓ Submit

#### Current Leases

NAME	MAC ADDRESS	IP ADDRESS	EXPIRATION	OPTIONS
No matching records				

#### Fixed Addresses + Add

MAC ADDRESS	IP ADDRESS	OPTIONS
No matching records		

## Add DHCPv6/RA Tab

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

### DHCPV6 AND ROUTER ADVERTISEMENT

- Home
- Setup**
- Network Interfaces
- WAN Configuration
- Global DNS
- DDNS Configuration
- DHCP Configuration**
- LLDP Configuration
- GPS Configuration
- SMTP Configuration
- Serial Configuration
- SNMP Configuration
- Time Configuration

DHCP Configuration
+ Add IPv4 DHCP Server
**+ Add DHCPv6/RA**

#### Router Advertisement Configuration

☒ Enabled

Interface: br0

Router Advertisement Mode: Stateless DHCP

Lease Time (dd-hh-mm): 01-00-00

✓ Submit

## Edit DHCPv6/RA Tab

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

The screenshot shows the 'DHCPv6 AND ROUTER ADVERTISEMENT' configuration page. On the left is a sidebar with a 'Setup' menu containing various network configuration options. The main panel is titled 'Router Advertisement Configuration' and includes the following settings:

- Enabled:** A toggle switch that is turned on.
- Interface:** A dropdown menu showing 'br0'.
- Router Advertisement Mode:** A dropdown menu showing 'Stateless DHCP'.
- Lease Time (dd-hh-mm):** A text input field containing '01-00-00'.
- Submit:** A blue button with a checkmark icon.

## LLDP Configuration

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

Typical LLDP configuration settings for eth0 are illustrated here:

The screenshot shows the 'LLDP CONFIGURATION' page. The sidebar on the left has 'LLDP Configuration' selected. The main panel contains the following settings:

- Enabled:** A toggle switch that is turned on.
- System Name:** A text input field containing 'mtr3'.
- System Description:** A text input field containing 'Multitech Systems mPower'.
- TX Interval:** A text input field containing '30'.
- TX Hold:** A text input field containing '4'.
- Submit:** A blue button with a checkmark icon.
- Reset To Default:** A button with a reset icon.

## 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:

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

SMTP CONFIGURATION

SettingsMail Log

Server Configuration

Enabled

Server

Port

465

TLS

StartTLS

Verify Server Certificate

Authentication

Enabled

Username

Password

Email

Send Test Email

Mail Log Settings

Entries To Keep

50

Submit

Reset To Default

## 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.



MAIL LOG





Settings

Mail Log


Mail Log


Refresh Log

Purge Log

DATE	RECIPIENT	STATUS	OPTIONS
03/25/2025 17:54:47	 @multitech.com	Sent	
03/25/2025 17:54:06	 @gmail.com	Sent	

Records: 10 25 50 100

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.





To: **alogvinova@multitech.com**

MultiTech Test Email

03/25/2025 17:54:47

This is a test email sent from mPower(TM)  
Edge MultiTech Router. Device ID: 23067168

 Sent

 OK

## SNMP Configuration

The typical SNMP Configuration settings are illustrated here:

Home

Setup

Network Interfaces

WAN Configuration

Global DNS

DDNS Configuration

DHCP Configuration

LLDP Configuration

GPS Configuration

SMTP Configuration

SNMP Configuration

Time Configuration

Digital I/O

Cellular

Wireless

Firewall

Tunnels

Administration

Apps

SNMP CONFIGURATION

Download MIB

SNMP Configuration + Add Server Configuration + Add Trap Destination

SNMP Server Configuration

Enabled

ALLOWED IP ADDRESSES (V1/V2C ONLY)

+ Add

Add IP address to limit access through SNMP v1/v2c. By default, all IP addresses are allowed.

Name

Location

Contact

ENABLED	NAME	VERSION	AUTH	ENCRYPTION	OPTIONS
No matching records.					

SNMP Trap Destinations

Enabled

Engine ID

0x800003e380f0a56c7d08d40f07

default

ENABLED	NAME	IP ADDRESS	VERSION	AUTH	ENCRYPTION	OPTIONS
No matching records.						

Submit

Help About Contact Us

© 1995 - 2024 Multi-Tech Systems, Inc.

The following MIB information is compatible with RFC1213 for the Conduit AP 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.

MIB Parameter	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: <ul style="list-style-type: none"> <li>Product ID</li> <li>Serial Number</li> <li>mPower Firmware Release</li> <li>vendor ID</li> </ul>

MIB Parameter	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".	The sysObjectID is <b>1.3.6.1.4.1.995.16.1.2.1</b>
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.

MIB Parameter	OID	OID Description	Comments
sysServices	1.3.6.1.2.1.1.7	<p>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, <math>2^{(L-1)}</math> is added to the sum. For example, a node which primarily performs routing functions has a value of <math>(2^{(3-1)})</math>, or 4.</p> <p>In contrast, a node which is a host offering application services has a calculated value of <math>[2^{(4-1)} + 2^{(7-1)}]</math>, or 72.</p> <p>Note that in the context of the Internet suite of protocols, values should be calculated accordingly:</p> <ul style="list-style-type: none"> <li>■ Layer 1: physical (repeaters)</li> <li>■ Layer 2: datalink/subnetwork (bridges)</li> <li>■ Layer 3: internet (IP gateways)</li> <li>■ Layer 4: end-to-end (IP hosts)</li> <li>■ Layer 7: applications (mail relays)</li> </ul> <p>For systems including OSI protocols, layers 5 and 6 may also be included.</p>	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:

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

TIME CONFIGURATION

Settings

Change Date & Time

12 / 03 / 2024 , 09 : 06 PM

Current Date and Time

12/3/2024, 9:06:03 PM (UTC)

Time Zone

UTC

NTP Configuration

Enabled

Minimum Poll Interval

6

Maximum Poll Interval

10

Pool Time Server

Server

north-america.pool.ntp.org

Custom Servers

Server 1

time.nist.gov

Server 2

Server 3

Server 4

Cellular Time

Enabled

Polling Time (5 to 1440 minutes)

120

Submit

Reset To Default

## Cellular Menu

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

**Note:** Conduit AP (MTCAP3) models that support cellular connectivity include a micro SIM slot. Refer to the Conduit AP Hardware Guide for additional information.

## Cellular Configuration

The Cellular Configuration page:

- Enables/disables cellular operation
- Configures Connection Monitoring parameters
- Configures Connection Recovery parameters.

Conduit® AP Configuration Guide Using mPower™ Edge Intelligence (v7.1.0)

97

The Cellular Configuration page is illustrated here:

**CELLULAR CONFIGURATION**

Cellular Configuration Cellular Profiles

**General Configuration**

☐ Enabled

PIN  
No PIN

APN

Active Slot	SIM 1 (Main)
SIM ICCID	[Masked]
Provider Profile	Default
SIM Profile	Not available

**Connection Monitoring** [show](#)

**Connection Recovery**

☒ Data Connection Reset

☐ Radio Reboot

☒ Service Reset

## Cellular Configuration Tab

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

### 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.

### 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.
- 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

☐ 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:

The screenshot displays the 'CELLULAR PROVIDER AND SIM PROFILES' configuration page. On the left is a sidebar with navigation links: Home, Setup, Cellular (highlighted), Cellular Configuration, Diagnostics, SMS, Wireless, Firewall, Tunnels, Administration, and Apps. The main panel has two tabs: 'Cellular Configuration' and 'Cellular Profiles' (selected). Under 'Cellular Profiles', there are two sections: 'SIM Details' and 'Provider Profiles'. The 'SIM Details' section shows fields for SIM Provider (Custom), Home PLMN ID (25503), SIM SPN (KYIVSTAR), ICCID, and IMSI. The 'Provider Profiles' section contains a table with one entry: 'Default' with a green checkmark in the 'CURRENT' column, 'Any SIM' in the 'ACTIVATION' column, and 'Auto' in the 'FIRMWARE IMAGE' column. Below this is a 'SIM Profiles' section with a table that is currently empty, displaying 'No SIM Profiles yet'. A '+ Add Provider Profile' link is located above the Provider Profiles table, and a '+ Add SIM Profile' link is above the SIM Profiles table. A 'Reset To Default' button is at the bottom right.

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.



ADD PROVIDER PROFILE
Cellular Configuration
Cellular Profiles
+ Add Provider Profile

General Configuration

Profile Name

Current SIM Activation

☐ Update Current SIM Profile on Submit

Automatic Profile Activation

Activation Mode
SIM Groups

SIM Groups

SIM PROVIDER	HOME PLMN ID	IMSI RANGE	SIM SPN	ICCID PREFIX	OPTIONS
No groups defined. This Provider Profile can only be selected manually via a SIM Profile.					

Modem Configuration

Cellular Mode
Auto

Firmware Image
Auto

TROUBLESHOOTING STRINGS
+ Add

Data Connection Configuration

PDP Context Mode
Auto

APN

Authentication
Authentication Type
NONE

Packet Size Settings
WWAN MTU
1500

LTE Registration Configuration
☐ Separate Registration APN

EDIT SIM GROUP

SIM Details

SIM Provider
Custom

Home PLMN ID
25503

SIM SPN
KYIVSTAR

ICCID

IMSI

Filter Configuration

SIM Provider
Custom

Home PLMN ID
Any

SIM SPN
Any

ICCID Prefix
Any

IMSI Range Start
Any

IMSI Range End
Any

### 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.

**ADD SIM PROFILE**

Cellular Configuration

Cellular Profiles

+ Add SIM Profile

**SIM Details**

SIM Provider

Custom

Home PLMN ID

25503

SIM SPN

KYIVSTAR

ICCID

IMSI

**SIM Profile Configuration**

Profile Name

PIN

No PIN

Check PIN

ICCID

8938003992741964975

Provider Profile

Auto

Submit

## Diagnostics

Cellular Diagnostics includes the following tabs:

- Radio Status
- Diagnostics
- Cell Radio Firmware Upgrade

### Radio Status Tab

Typical Radio Status information is illustrated here:

**RADIO STATUS**

Radio Status | Diagnostics | Cell Radio Firmware Upgrade

Home

Setup

**Cellular**

Cellular Configuration

Diagnostics

SMS

Wireless

Firewall

Tunnels

Administration

Apps

**Module Information**

IMEI	
IMSI	
MANUFACTURER	Telit
MODEL	LE910C4-WWxD
MDN (PHONE NUMBER)	
MSID	0609608352
FIRMWARE VERSION	M0F.603006
ICCID	

**Service Information**

HOME NETWORK	KYIVSTAR
CURRENT NETWORK	UA-KYIVSTAR
RSSI	-63 dBm
SERVICE	LTE
ROAMING	No
TOWER	50C512E

**Engineering Details**

TX PWR	
RSRP	-97
RSRQ	-11
RSSI	-66
MM STATE	3
RRC	0
SERVICE DOMAIN	CS+PS

**Options**

MDN (Phone Number) Update

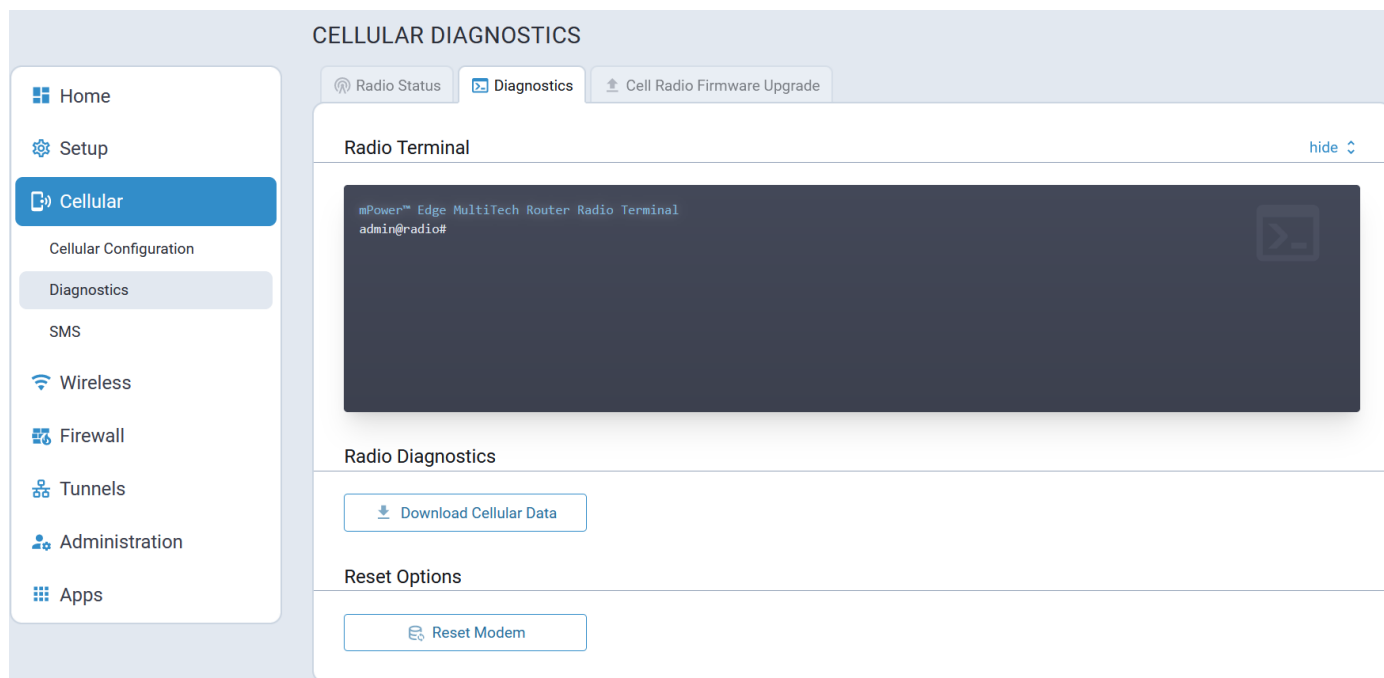
Last update: 7:48:55 PM

## 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

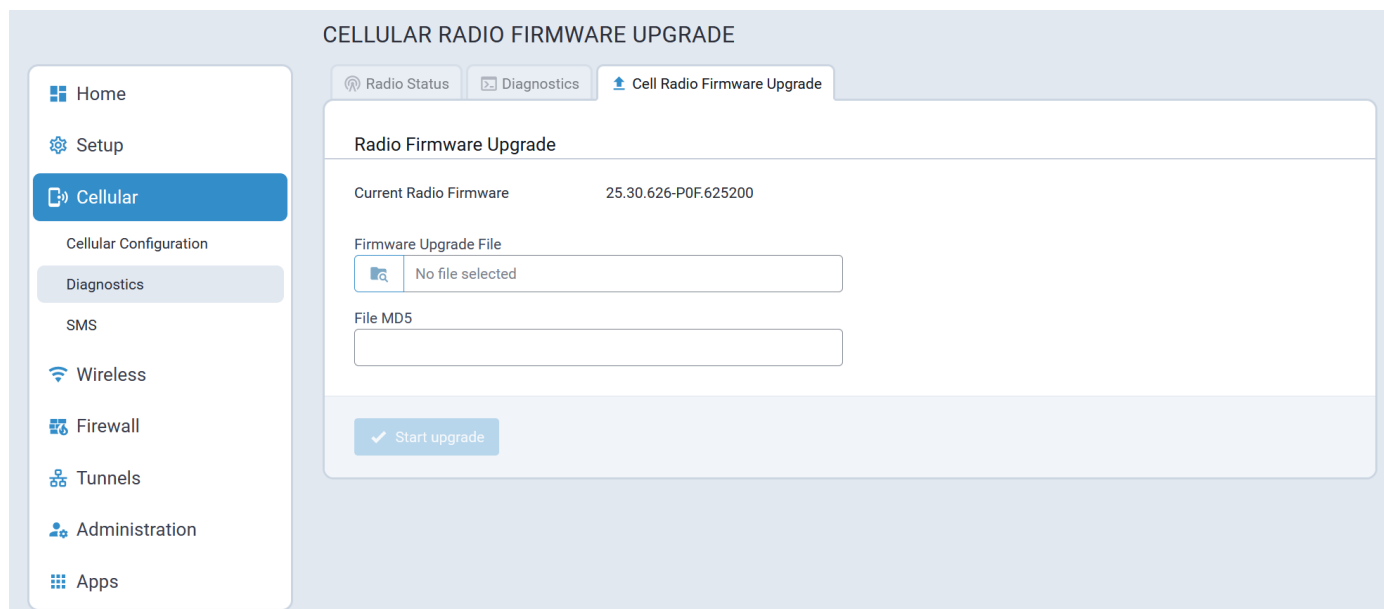
A typical Diagnostics tab is illustrated here:



## 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:

Home

LoRaWAN®

Payload Management

Setup

Cellular

Cellular Configuration

Diagnostics

SMS

Firewall

Tunnels

Administration

Apps

SMS CONFIGURATION

ConfigurationSend/Received SMS

SMS Settings

Enabled

Sent SMS to Keep

1000

Resend Failed SMS

0

Received SMS to Keep

1000

SMS Commands

#reboot

#apn

#checkin

#cellular

#rm <enable|disable>

#radio

#setcellular <enable|disable> [<APN>]

#ethernet

#ping [<interface>] [<count>] <address>

#wan

#wanips

#insrestart

Security Filters

Required SMS Command Format p password #command <parameter> from any number

Password

.....

Use custom password

Whitelist

+ Add Number

NUMBERS

OPTIONS

No numbers yet

Submit

Reset To Default

### Send/Received SMS Tab

A typical Send/Received SMS tab is illustrated here:

Conduit® AP Configuration Guide Using mPower™ Edge Intelligence (v7.1.0)

105

Home

Setup

Cellular

Cellular Configuration

Diagnostics

SMS

Wireless

Firewall

Tunnels

Administration

Apps

SEND AND RECEIVED SMS

Configuration

Send/Received SMS

Send SMS

Recipients

Specify multiple recipient phone numbers with comma(s).

Message

Characters: 0 (160 left)

Send

Sent SMS

Auto Refresh Delete All

STATUS	TIME	RECIPIENT	MESSAGE	OPTIONS
No matching records				

Received SMS

Auto Refresh Delete All

TIME	SENDER	MESSAGE	OPTIONS
No matching records			

## 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:

Home

Setup

Cellular

Wireless

Firewall

Settings

Trusted IP

Static Routes

Tunnels

Administration

Apps

FIREWALL SETTINGS

Settings

Status

Firewall Rules [+ Add Port Forwarding Rule](#)

Prerouting Rules [+ Add DNAT Rule](#)

NAME	SOURCE	DESTINATION	PROTOCOL	NAT IP	OPTIONS
No rules yet					

Input Filter Rules [+ Add Rule](#)

NAME	SOURCE	DESTINATION	PROTOCOL	TARGET	OPTIONS
No rules yet					

Forward Filter Rules [+ Add Rule](#)

NAME	SOURCE	DESTINATION	PROTOCOL	TARGET	OPTIONS
No rules yet					

Output Filter Rules [+ Add Rule](#)

NAME	SOURCE	DESTINATION	PROTOCOL	TARGET	OPTIONS
No rules yet					

Postrouting Rules [+ Add SNAT Rule](#)

NAME	SOURCE	DESTINATION	PROTOCOL	NAT IP	OPTIONS
No rules yet					

Connection Tracking Helper

☐ Enabled

Submit

### 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:

**PORT FORWARDING CONFIGURATION**

**Port Forwarding Rule**

Name

Description

WAN Port(s)

Protocol

Redirect to LAN Port

Redirect to LAN IP Address

**Advanced Settings** [hide](#)

Source Match

IP Address

Mask

Port(s)

NAT Loopback ☐ Enable NAT Loopback

## 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:



**FIREWALL STATUS**

Settings Status

Firewall Status [Refresh](#) [Download](#)

Filter Rules [hide](#)

```
table ip MTS-TABLE-FILTER {
    chain INPUT {
        type filter hook input priority filter + 5; policy drop;
        iifname "lo" accept
        counter packets 12483 bytes 1787966 jump KEEP_STATE_INPUT
        counter packets 4943 bytes 340818 jump DNS_SERVER_INPUT
        counter packets 972 bytes 64448 jump DHCP_SERVER_INPUT
        counter packets 969 bytes 63424 jump DHCP_CLIENT_INPUT
        counter packets 969 bytes 63424 jump HTTP_LAN_INPUT
        counter packets 969 bytes 63424 jump HTTPS_LAN_INPUT
        counter packets 730 bytes 50996 jump ICMP_LAN_INPUT
    }

    chain FORWARD {
        type filter hook forward priority filter + 5; policy drop;
    }
}
```

NAT Rules [hide](#)

```
table ip MTS-TABLE-NAT {
    chain PREROUTING {
        type nat hook prerouting priority dstnat + 5; policy accept;
    }

    chain POSTROUTING {
        type nat hook postrouting priority srcnat + 5; policy accept;
    }
}
```

IP Tables Dump [show](#)

## 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:

Home

Setup

Cellular

Wireless

**Firewall**

Settings

Trusted IP

Static Routes

Tunnels

Administration

Apps

TRUSTED IP

+ Add IP Range

Configuration

☐ Enabled

Trusted IP Mode

White List

NAME	IP RANGE	PORT	PROTOCOL	OPTIONS
No matching records				

✓ Submit

⚙️ Reset To Default

## Static Routes

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

A typical Static Route settings page is illustrated here:

Home

Setup

Cellular

Wireless

**Firewall**

Settings

Trusted IP

Static Routes

Tunnels

Administration

Apps

STATIC ROUTES

+ Add Route

NAME	IP ADDRESS	IP MASK	IP GATEWAY	OPTIONS
No matching records				

ADD STATIC ROUTE

Name

IP Address

IP Mask

Gateway

✓ Finish

✕ Cancel

## 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 Conduit AP 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:

The screenshot shows the 'GRE TUNNEL CONFIGURATION' page. On the left is a sidebar menu with options: Home, Setup, Cellular, Wireless, Firewall, Tunnels (highlighted), GRE Tunnels, IPSec Tunnels, OpenVPN Tunnels, Administration, and Apps. The main content area has a header with 'GRE Configuration' and an 'Add Tunnel' button. Below this is a table with columns: ENABLED, NAME, REMOTE IP, ROUTES, and OPTIONS. The table is currently empty, displaying 'No matching records'.

ENABLED	NAME	REMOTE IP	ROUTES	OPTIONS
No matching records				

### Add Tunnel Tab

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

The screenshot shows the 'GRE TUNNEL' configuration page in the mPower interface. On the left is a navigation menu with options: Home, Setup, Cellular, Wireless, Firewall, Tunnels (selected), GRE Tunnels, IPSec Tunnels, OpenVPN Tunnels, Administration, and Apps. The main content area is titled 'GRE TUNNEL' and has two tabs: 'GRE Configuration' and 'Add Tunnel'. The 'GRE Configuration' tab is active, showing a toggle switch for 'Enabled' which is turned on. Below this is a 'Name' input field. To the right is a 'Description' text area. Under the 'GRE Tunnel Settings' section, there are input fields for 'Remote WAN IP', 'Interface IP Address', and 'Interface Network Mask'. Below these is a 'Checking period (minutes)' field with the value '10'. At the bottom left of the settings area is a 'Submit' button with a checkmark icon. On the right side, there is a 'REMOTE NETWORK ROUTES' section with an '+ Add' button and a message stating 'Remote network routes list is empty'.

## 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:

The screenshot displays the mPower configuration interface for IPSec Tunnel Configuration. On the left, a sidebar lists various system settings, with 'Tunnels' selected and 'IPSec Tunnels' highlighted. The main panel shows the 'IPSEC TUNNEL CONFIGURATION' section with an active 'IPSec Configuration' tab and an 'Add Tunnel' button. A table with seven columns (ENABLED, NAME, AUTH, LOCAL NETWORKS, REMOTE WAN IP, REMOTE NETWORKS, OPTIONS) is shown, but it is currently empty, indicating 'No matching records'.

## Add Tunnel Tab

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

Home

Setup

Cellular

Wireless

Firewall

Tunnels

GRE Tunnels

IPSec Tunnels

OpenVPN Tunnels

Administration

Apps

IPSec Configuration

Add Tunnel

Enabled

Name

Remote WAN IP

LOCAL NETWORKS

+ Add

Local Networks list is empty

REMOTE NETWORKS

+ Add

Remote Networks list is empty

Authentication Method

Pre-Shared Key

Enable UID

Encryption Method

AES-128

Advanced Settings

show

Submit

Description

Tunnel Type

IKEv2

Allow All Traffic

Secret

## Configuration Parameters

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

Parameter	Description
<b>IPSec Tunnel</b>	
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.
<b>IPSec Remote Tunnel Endpoint</b>	
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 <b>Remote Network Mask</b> field and describes the remote endpoint's subnet. This is used to identify packets that are routed over the tunnel to the remote network.

Parameter	Description
Remote Network Mask	This field is used in conjunction with the <b>Remote Network Route</b> 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 <b>IKE</b> or <b>IKEv2</b> .
<b>IPsec Tunnel: IKE</b>	
Authentication Method	Choose between <b>Pre-Shared Key</b> or <b>RSA Signatures</b> . Authentication is performed using secret pre-shared keys and hashing algorithms (like SHA1 MD5) or RSA signatures (you provide the <b>CA Certificate</b> , <b>Local RSA Certificate</b> , and <b>Local RSA Private Key</b> in .pem format). If you check <b>Enable UID</b> , then <b>Local ID</b> and <b>Remote ID</b> 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 <b>Advanced</b> 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 <b>Phase 1 Authentication</b> .
Local RSA Private Key	The private key that the local endpoint uses during Phase 1 Authentication.
Encryption Method <sup>1</sup>	Choose an Encryption Method from the following list: <b>AES-128</b> , <b>AES-192</b> , <b>AES-256</b> , or <b>ADVANCED</b> . 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 <b>Advanced</b> option is used, in which case, all components of both phases 1 and 2 are specified by the user.
Phase 1 Encryption <sup>1</sup>	If <b>Advanced</b> is selected for <b>Encryption Method</b> , select <b>Phase 1 Encryption</b> from the drop-down: <b>AES-128</b> , <b>AES-192</b> , <b>AES-256</b> , or <b>ANY AES</b> .
Phase 1 Authentication <sup>1</sup>	If <b>Advanced</b> is selected for <b>Encryption Method</b> , select <b>Phase 1 Authentication</b> from the drop-down: <b>SHA-2</b> , <b>SHA2-256</b> , <b>SHA2-384</b> , <b>SHA2-512</b> , or <b>ANY</b> .
Phase 1 Key Group <sup>1</sup>	If <b>Advanced</b> is selected for <b>Encryption Method</b> , select the <b>Phase 1 Key Group</b> from the drop-down: <b>DH2 (1024-bit)</b> , <b>DH5 (1536-bit)</b> , <b>D14 (2048-bit)</b> , <b>DH15 (3072-bit)</b> , <b>DH16 (4096-bit)</b> , <b>DH17 (6144-bit)</b> , <b>DH18 (8192-bit)</b> , <b>DH22 (1024-bit)</b> , <b>DH23 (2048-bit)</b> , <b>DH24 (2048-bit)</b> , and <b>ANY</b> .

Parameter	Description
Phase 2 Encryption <sup>1</sup>	If <b>Advanced</b> is selected for <b>Encryption Method</b> , select <b>Phase 2 Encryption</b> from the drop-down: <b>AES-128</b> , <b>AES-192</b> , <b>AES-256</b> , <b>ANY AES</b> , or <b>ANY</b> .
Phase 2 Authentication <sup>1</sup>	If <b>Advanced</b> is selected for <b>Encryption Method</b> , select <b>Phase 2 Authentication</b> from the drop-down: <b>SHA-2</b> , <b>SHA2-256</b> , <b>SHA2-384</b> , <b>SHA2-512</b> , or <b>ANY</b> .
Phase 2 Key Group <sup>1</sup>	If <b>Advanced</b> is selected for <b>Encryption Method</b> , select the <b>Phase 2 Key Group</b> from the drop-down: <b>DH2 (1024-bit)</b> , <b>DH5 (1536-bit)</b> , <b>D14 (2048-bit)</b> , <b>DH15 (3072-bit)</b> , <b>DH16 (4096-bit)</b> , <b>DH17 (6144-bit)</b> , <b>DH18 (8192-bit)</b> , <b>DH22 (1024-bit)</b> , <b>DH23 (2048-bit)</b> , <b>DH24 (2048-bit)</b> , and <b>ANY</b> .
Enable UID	Unique Identifier String to enable the <b>Local ID</b> and <b>Remote ID</b> fields.
Local ID	String Identifier for the local security gateway (optional)
Remote ID	String Identifier for the remote security gateway (optional)
<b>IPSec Tunnel: Advanced</b>	
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.

<sup>1</sup> 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**):
  - a. **Interface Type** as **TUN** from the dropdown.
  - b. **Authorization Mode** as **TLS** from the dropdown.
  - c. **Protocol** as **UDP**.
  - d. **VPN Subnet**.
  - e. **Port** number.
  - f. **VPN Netmask**.
  - g. **LZO Compression** as **ADAPTIVE** from the dropdown.
  - h. **Hash Algorithm** as **DEFAULT**.
  - i. **NCP (Negotiable Crypto Parameters)** as **DEFAULT**.
  - j. **Min. TLS Version** as **1.2**.
  - k. **TLS Cipher Suite** as **DEFAULT**.
  - l. Enter the contents of the following files generated from the *easy-rsa* tool. You can copy and paste this content from the certificate files after opening from a text editor like Notepad (all required):
    - 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**:
  - a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
  - b. Enter the **Remote Network Mask** (usually 255.255.255.0).
  - c. You may enter **Gateway** (optional).
  - d. 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**:
  - a. Select **Client To Client** box if you want this optional feature (this establishes a connection between multiple clients that are connected to the server).
  - b. In the **Push Network Route**, select **Add**.
  - c. In the dialog box, enter the **Remote Network Route** (same address as the server subnet above).
  - d. Enter the **Remote Network Mask** (same as above).
  - e. *Optional:* You may enter **Gateway**.
  - f. 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**):
  - a. **Interface Type** as **TUN** from the dropdown.
  - b. **Authorization Mode** as **TLS** from the dropdown.
  - c. **Protocol** as **UDP**.
  - d. **Remote Host** (server public IP address).
  - e. **Remote Port** number.
  - f. **LZO Compression** as **ADAPTIVE** from the dropdown.
  - g. **Hash Algorithm** as **DEFAULT**.
  - h. **NCP (Negotiable Crypto Parameters)** as **DEFAULT**.
  - i. **Min. TLS Version** as **1.2**.
  - j. **TLS Cipher Suite** as **DEFAULT**.
  - k. Enter the contents of the following files generated from the easy-rsa tool. You can copy and paste this content from the certificate files after opening from a text editor like Notepad (all required):
    - 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:
  - a. **iroute [Client\_Subnet] [Mask]**
  - b. **example** -- echo "iroute 192.168.3.0 255.255.255.0" > mtrClient1
4. For each client, you must create a separate file in the folder `/var/config/ovpnccd/yourserverName`.
 

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

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

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

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

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

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

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. 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**):
  - a. **Interface Type** as **TUN** from the dropdown.
  - b. **Authorization Mode** as **STATIC KEY** from the dropdown.
  - c. **Protocol** as **UDP**.
  - d. **Local Address** as **DEFAULT**.
  - e. **Port** number.
  - f. **Remote Address** as **DEFAULT**.
  - g. **LZO Compression** as **ADAPTIVE** from the dropdown.
  - h. **Hash Algorithm** as **DEFAULT**.
  - i. **NCP (Negotiable Crypto Parameters)** as **DEFAULT**.
  - j. Generate and enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

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

```
3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875
215e20e80a2d59efd79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f5
5e7d8917a32bfe07d61591b7bbb43c7bad214482b8547ec9dca8910f514d9f4270cc
aef1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104e1968ed29b6c338871
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**:
    - a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
    - b. Enter the **Remote Network Mask** (usually 255.255.255.0).
    - c. 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**):
  - a. **Interface Type** as **TUN** from the dropdown.
  - b. **Authorization Mode** as **STATIC KEY** from the dropdown.
  - c. **Protocol** as **UDP**.
  - d. **Local Address** as **DEFAULT**.
  - e. **Remote Host**.
  - f. **Remote Address** as **DEFAULT**.
  - g. **Remote Port** number.
  - h. **LZO Compression** as **ADAPTIVE** from the dropdown.
  - i. Select the **NCP (Negotiable Crypto Parameters)** as **DEFAULT** from dropdown.
  - j. Select the **Hash Algorithm** as **DEFAULT** from dropdown.
  - k. **Min. TLS Version** as **1.2**.
  - l. **TLS Cipher Suite** as **DEFAULT**.
  - m. Enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:
 

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

3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875
215e20e80a2d59efd79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f5
5e7d8917a32bfe07d61591b7bbb43c7bad214482b8547ec9dca8910f514d9f4270cc
aef1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104e1968ed29b6c338871
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**:
  - a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.

- b. Enter the **Remote Network Mask** (usually 255.255.255.0).
    - c. 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**):
  - a. **Interface Type** as **TUN** from the dropdown.
  - b. **Authorization Mode** as **STATIC KEY** from the dropdown.
  - c. **Protocol** as **TCP**.
  - d. **Local Address** as **DEFAULT**.
  - e. **Remote Host**.
  - f. **Remote Address** as **DEFAULT**.
  - g. **Remote Port** number.
  - h. **Hash Algorithm** as **RSA-SHA1**.
  - i. **LZO Compression** as **ADAPTIVE** from the dropdown.
  - j. **NCP (Negotiable Crypto Parameters)** as **CAMELLIA-256-CBC**.
  - k. **Min. TLS Version** as **NONE**.
  - l. **TLS Cipher Suite** as **DEFAULT**.
  - m. Generate and enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

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

```
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**:
  - a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
  - b. Enter the **Remote Network Mask** (usually 255.255.255.0).
  - c. 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**):
  - a. **Interface Type** as **TUN** from the dropdown.
  - b. **Authorization Mode** as **STATIC KEY** from the dropdown.
  - c. **Protocol** as **TCP**.
  - d. **Local Address** as **DEFAULT**.
  - e. **Remote Host**.
  - f. **Remote Address** as **DEFAULT**.
  - g. **Remote Port** number.
  - h. **Hash Algorithm** as **RSA-SHA1**.
  - i. **LZO Compression** as **ADAPTIVE** from the dropdown.
  - j. **NCP (Negotiable Crypto Parameters)** as **CAMELLIA-256-CBC**.

- k. **Min. TLS Version** as **NONE**.
- l. **TLS Cipher Suite** as **DEFAULT**.
- m. Generate and enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

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

```
3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875
215e20e80a2d59efd79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f5
5e7d8917a32bfe07d61591b7bbb43c7bad214482b8547ec9dca8910f514d9f4270cc
aef1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104e1968ed29b6c338871
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**:
  - a. Enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
  - b. Enter the **Remote Network Mask** (usually 255.255.255.0).
  - c. 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.

**Note:** The Engineer and Monitor roles can only change their own account settings, while the Administrator role can update any account.

## SSH Key Management

SSH public keys are managed in this section of the Users page.

Users with an administrator role can view, add, and delete public keys for themselves as well as all other users with the following roles:

- Engineer
- Monitor
- Custom role

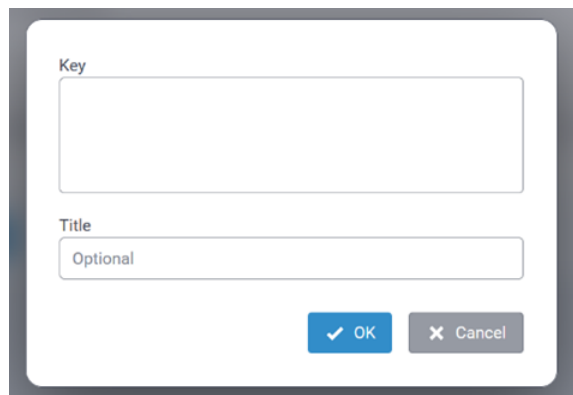
Only users with a local administrator role can add a public key for themselves.

Public keys that have been added to a user's account are listed in this section as well.

### Add a New Public Key

To create a new public key associated with a user account click **Add Public Key** as shown here:

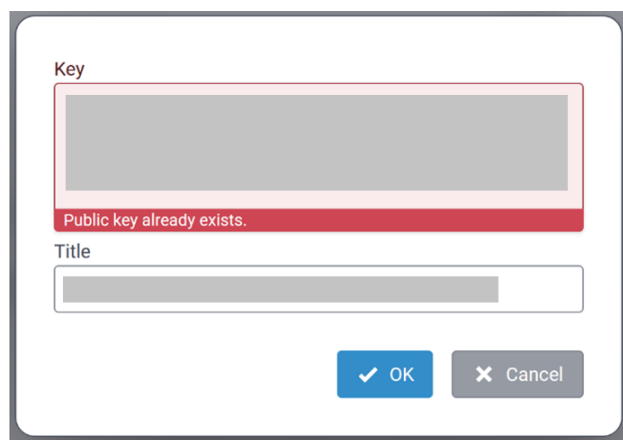
Paste the key into the Key field and assign a Title to the key:



A modal form with a title bar. It contains two text input fields: 'Key' and 'Title'. The 'Title' field has the placeholder text 'Optional'. At the bottom right, there are two buttons: 'OK' (blue with a checkmark) and 'Cancel' (grey with an 'X').

**Note:** The maximum length for a Public Key is 3000 characters.

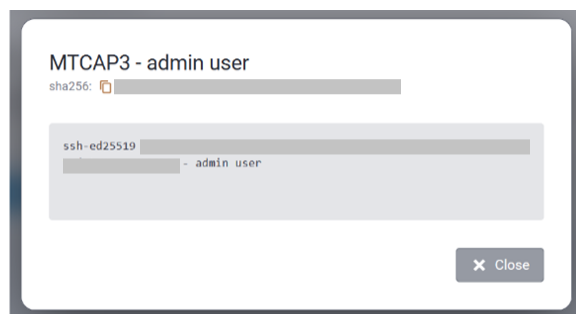
The system will not allow a public key to be added/created for a user if one has already been added.



A modal form identical to the one above, but with a red error message box below the 'Key' field that reads 'Public key already exists.' The 'OK' and 'Cancel' buttons are still present at the bottom.

### View a Public Key

To view a public key, click on the  icon associated with the key to be viewed.



A modal form titled 'MTCAP3 - admin user'. It displays a 'sha256:' label followed by a redacted key value. Below this, there is a code block showing 'ssh-ed25519' followed by another redacted key value and '- admin user'. A 'Close' button is at the bottom right.

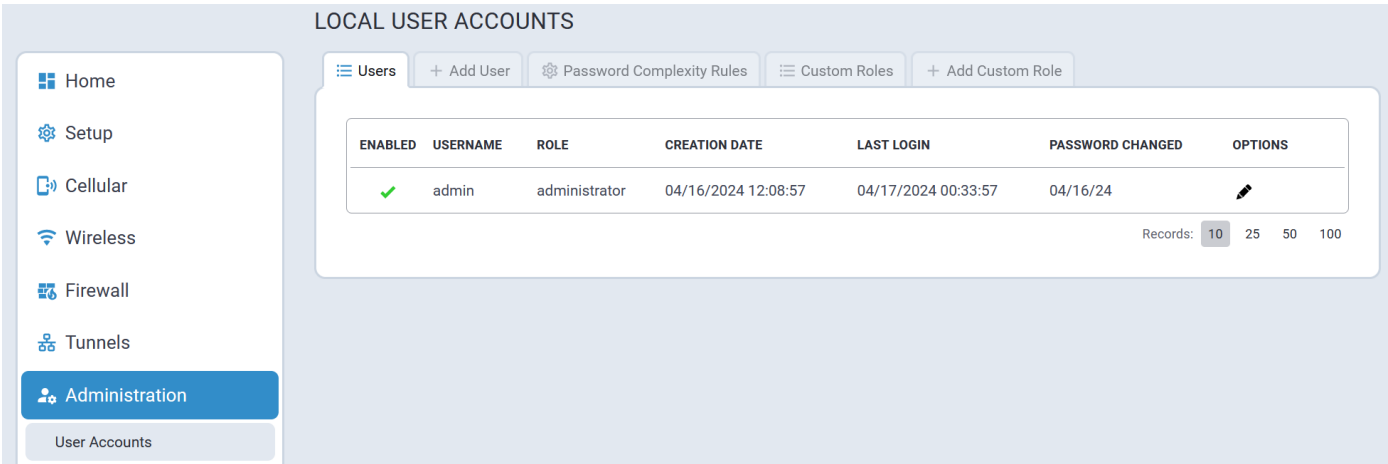
### Delete a Public Key

To delete a public key, click on the  icon associated with the key to be deleted.

**Note:** When a user account is deleted, all public keys associated with that account are also deleted by the system.

### Users Tab

A typical Users tab is illustrated here:



### Add User Tab

When adding a user, a User Role must be assigned to that user. By default, the system supports three user roles:

- Administrator
- Engineer
- Monitor

A typical Add User screen is shown here:

### ADD USER ACCOUNT

Users

+ Add User

Password Complexity Rules

Custom Roles

+ Add Custom Role

User Details

Username

First Name

Title

Employee Identification

Role

monitor

**Pre-Configured Roles**

administrator

engineer

monitor

Contact Information

Email

City

Country

Work Phone

Address

State

Postal Code

Mobile Phone

✓ Submit

When Custom Roles have been added to the system, they will be listed as well, as illustrated here:

### ADD USER ACCOUNT

Home

LoRaWAN®

Payload Management

Setup

Cellular

Firewall

Tunnels

**Administration**

User Accounts

Access Configuration

RADIUS Configuration

Users

+ Add User

Password Complexity Rules

Custom Roles

+ Add Custom Role

General Configuration

Username

User1

Role

CustomRole

Change Password

User Details

Contact Information

✓ Submit

**Pre-Configured Roles**

administrator

engineer

monitor

**Custom Roles**

Test

CustomRole

**Note:** For information about creating custom user roles, refer to [Add Custom Role](#).

### 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:

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

PASSWORD COMPLEXITY RULES

UsersAdd UserPassword Complexity RulesCustom RolesAdd Custom Role

Change Password Complexity Rules

Credit Complexity Mode

Default mode uses a minimum character length and may require a specific number of characters from each class. Credit Mode is recommended because requiring specific characters actually reduces the brute force search space. Nevertheless, it is fine to use this mode - just remember, the longer the password the better. Long passwords are nearly impossible to crack with brute force.

Minimum Password Length

8

Maximum Password Length

64

Minimum Upper Case Characters

0

Maximum Password Age (days)

0

Minimum Lower Case Characters

0

Minimum Password Age (days)

0

Minimum Numeric Characters

0

Password History Length

0

Minimum Special Characters

0

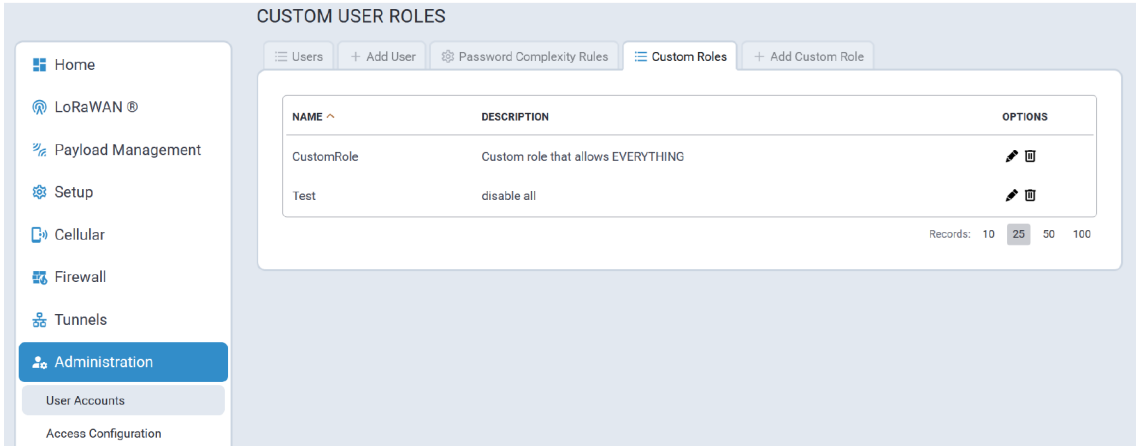
Characters Not Permitted

Submit

Reset To Default

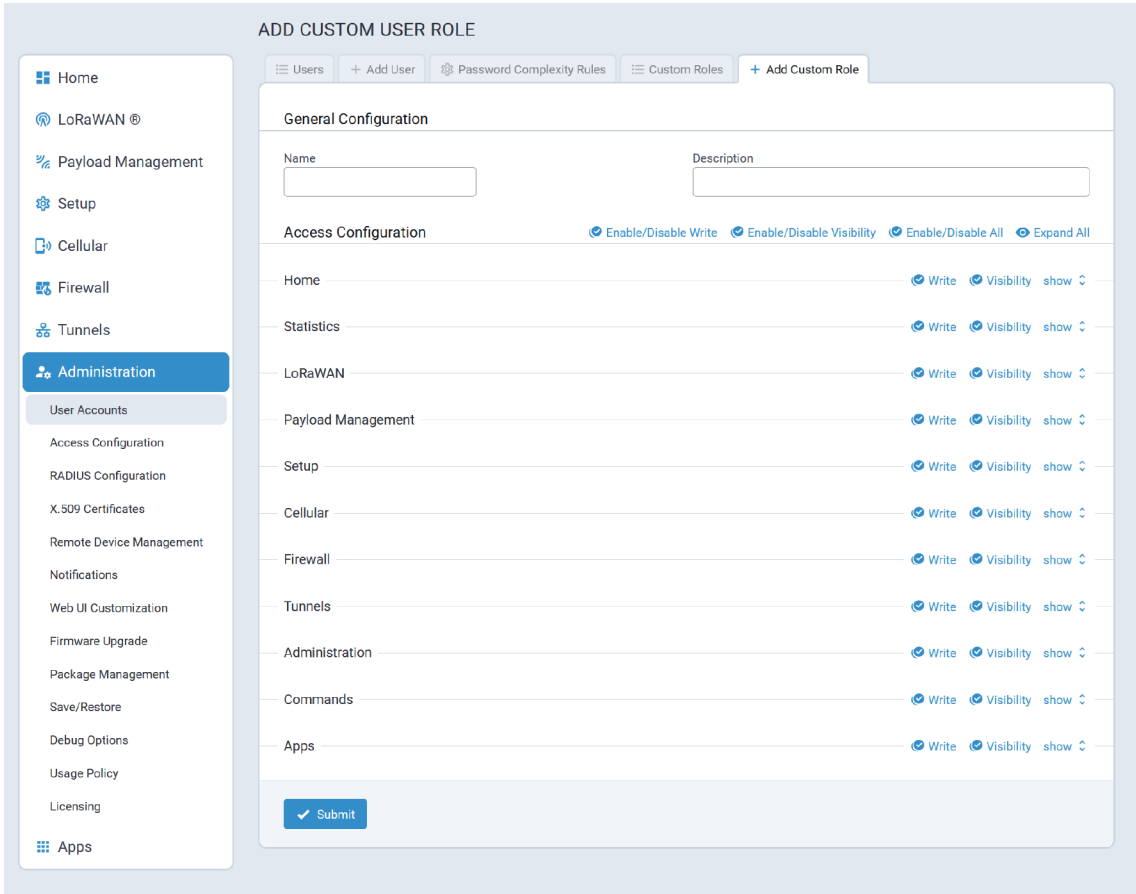
### Custom Roles Tab

The Custom Roles tab lists all Custom User Roles that have been added to the system. For example:



Add Custom Role

A typical Add Custom Role tab is illustrated here:



Sample custom User Role settings are illustrated here:



**ADD CUSTOM USER ROLE**

Users + Add User Password Complexity Rules Custom Roles + Add Custom Role

**General Configuration**

Name:  Description:

**Access Configuration** [Enable/Disable Write](#) [Enable/Disable Visibility](#) [Enable/Disable All](#) [Collapse All](#)

Home [Write](#) [Visibility](#) [show](#)

Statistics [Write](#) [Visibility](#) [show](#)

LoRaWAN [Write](#) [Visibility](#) [hide](#)

NAME	WRITE	VISIBILITY
Network Settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Key Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Gateways	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Profiles	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Packets	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Downlink Queue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Operations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Payload Management** [Write](#) [Visibility](#) [hide](#)

NAME	WRITE	VISIBILITY
Bacnet Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions and Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Logs	<input type="checkbox"/>	<input checked="" type="checkbox"/>

## Access Configuration

Access Configuration settings allow users to configure a variety of services on the device such as:

- The Web Server for the mPower API used by the mPower Web UI
- Responsiveness to Pings to the device on the LAN and WAN interfaces
- 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 limits
- SSH Authentication
- Reverse SSH Tunnel

A typical Access Configuration landing page is illustrated here:

The screenshot displays the 'ACCESS CONFIGURATION' settings page. On the left is a navigation sidebar with categories: Home, LoRaWAN, Payload Management, Setup (selected), Cellular, Firewall, Tunnels, Administration (expanded), and Apps. The 'Administration' section includes links for User Accounts, Access Configuration (selected), RADIUS Configuration, X.509 Certificates, Remote Device Management, Notifications, Web UI Customization, Firmware Upgrade, Package Management, Save/Restore, Debug Options, Usage Policy, and Licensing. The main content area is titled 'ACCESS CONFIGURATION' and has two tabs: 'Access Configuration' (active) and 'SSH Configuration'. A 'Reset To Default' button is in the top right. The 'Access Configuration' tab contains several sections: 'Web Server' (HTTP Port: 80, HTTPS Port: 443, Session Timeout: 300s, with toggles for HTTP Redirect to HTTPS, HTTP via LAN, HTTP via WAN, and HTTPS via WAN); 'HTTPS Security' (a 'show' link); '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: 300s); and a 'Submit' button at the bottom.

Access Configuration settings are presented on the following tabs:

- Access Configuration
- SSH Configuration

The following sections provide detailed information about each parameter used to configure device services.

## 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:

### RADIUS CONFIGURATION

[Download Dictionary](#)

- 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

☐ Enable Authentication

Primary Server

Secondary Server

☐ Enable Accounting

Authentication Port

Accounting Port

**Options**

Shared Secret Key

Authentication Protocol PAP

Timeout (seconds)

Retries

**Advanced Options**

☐ Use Anonymous ID

☒ Check Server Certificate Hostname

Anonymous ID

Submit

Reset To Default

## 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:

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 CERTIFICATE

Web Certificate

CA Certificates

Certificate



mts.example.com

Minneapolis, Minnesota, US

Issued By: mts.example.com, Minneapolis, Minnesota, US

Expiration Date: April 14, 2034 at 12:57:53 AM GMT+3

✓ This certificate is valid

⚠ Self Signed

Generate

Upload

Certificate Details

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

62:8d:c9:96:2b:90:71:b2:93:33:eb:86:89:31:b1:4a:50:e8:e2:0e

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = US, ST = Minnesota, L = Minneapolis, CN = mts.example.com

Validity

Not Before: Apr 15 21:57:53 2024 GMT

Not After : Apr 13 21:57:53 2034 GMT

Subject: C = US, ST = Minnesota, L = Minneapolis, CN = mts.example.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

GENERATE WEB CERTIFICATE

Common Name

Locality/City

Days

365

Organization

Country (2 letter code)

Email Address

State/Province

Generate

Cancel

UPLOAD WEB CERTIFICATE

Certificate

No file selected

A certificate with key size greater than 2048 bit will cause a delay in access to Web UI after the device starts.

A certificate with a key size less than 2048 bit is not recommended to use since this less secure and may become breakable in the near future.

Upload

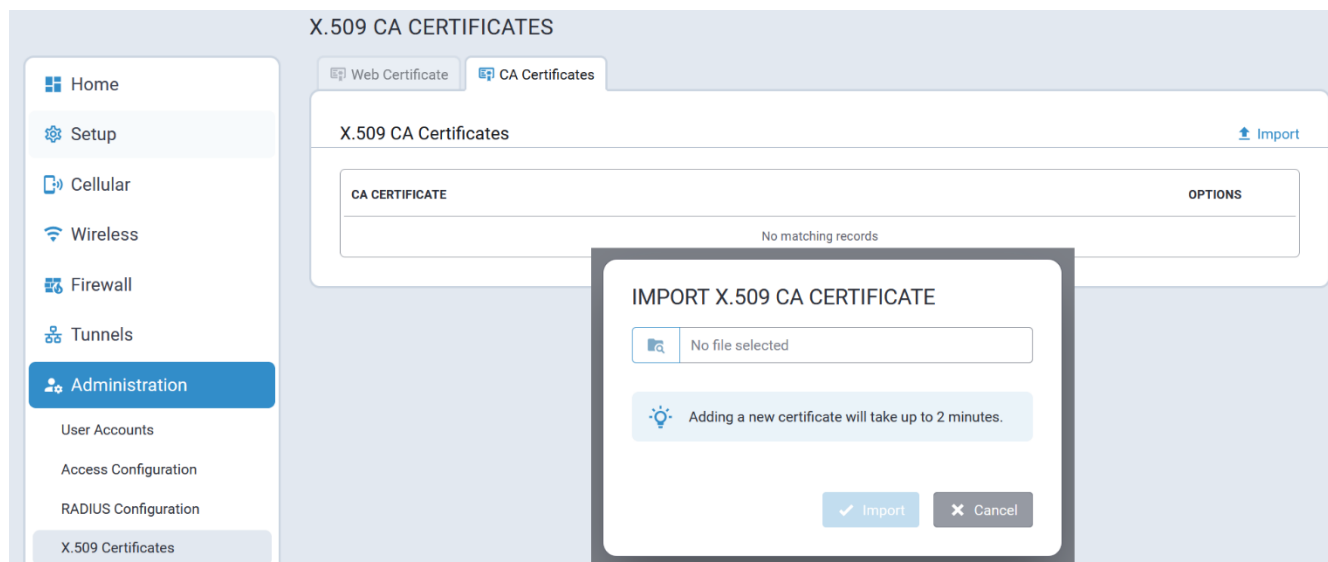
Cancel

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:

Conduit® AP Configuration Guide Using mPower™ Edge Intelligence (v7.1.0)

137



## Remote Device Management

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:

Home

Setup

Cellular

Wireless

Wi-Fi Configuration

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

REMOTE DEVICE MANAGEMENT

Remote Server

Enabled

Server Name

api.multitech.com

Check-In Settings

Intervals

Check-In Interval (minutes)

240

Schedule

Repeat

Daily

Time

--:--

Update Settings

Allow Firmware Upgrade

Allow Configuration Upgrade

Allow Configuration Upload

Check-In Status

Current Time

12/3/2024, 11:13:10 PM

Last Success

unknown

Last Attempt

12/3/2024, 11:11:59 PM

Next Attempt

12/3/2024, 11:14:58 PM

Current Status

Idle

Check-In

Trigger checkin via SMS by configuring SMS Commands

Submit

Reset To Default

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:

**NOTIFICATIONS**

Configuration Sent

Configuration

ENABLED	EVENT	NOTIFY	EMAIL	SMS	SNMP	OPTIONS
✓	High Data Usage	once per billing cycle	✓	✓	✓	
✓	Low Signal Strength	every 1 hours	✓	✓	✓	
✓	Device Reboots	always	✓	✓	✓	
✗	Ethernet Interface Failure	every 24 hours	✗	✗	✗	
✗	Cellular Interface Failure	every 24 hours	✗	✗	✗	
✗	Ethernet Data Traffic	every 24 hours	✗	✗		
✓	Cellular Data Traffic	every 24 hours	✗	✓		
✓	WAN Interface Failover	always	✓	✗	✗	
✗	Ping Failure	always	✗	✗	✓	

Recipient Groups [+ Add Group](#)

GROUP NAME	PHONE NUMBERS	EMAILS	OPTIONS
Test	1234-56-78	admin@test.test	

Records: 10 25 50 100

[Reset To Default](#)

To add a new Recipient Group, click on **+ Add Group** and configure the following information for the group:

**ADD RECIPIENT GROUP**

Group Name


Phone Number List [+ Add Phone](#)

NAME	PHONE NUMBER	OPTIONS
Admin	1234-56-78	

Email List [+ Add Email](#)

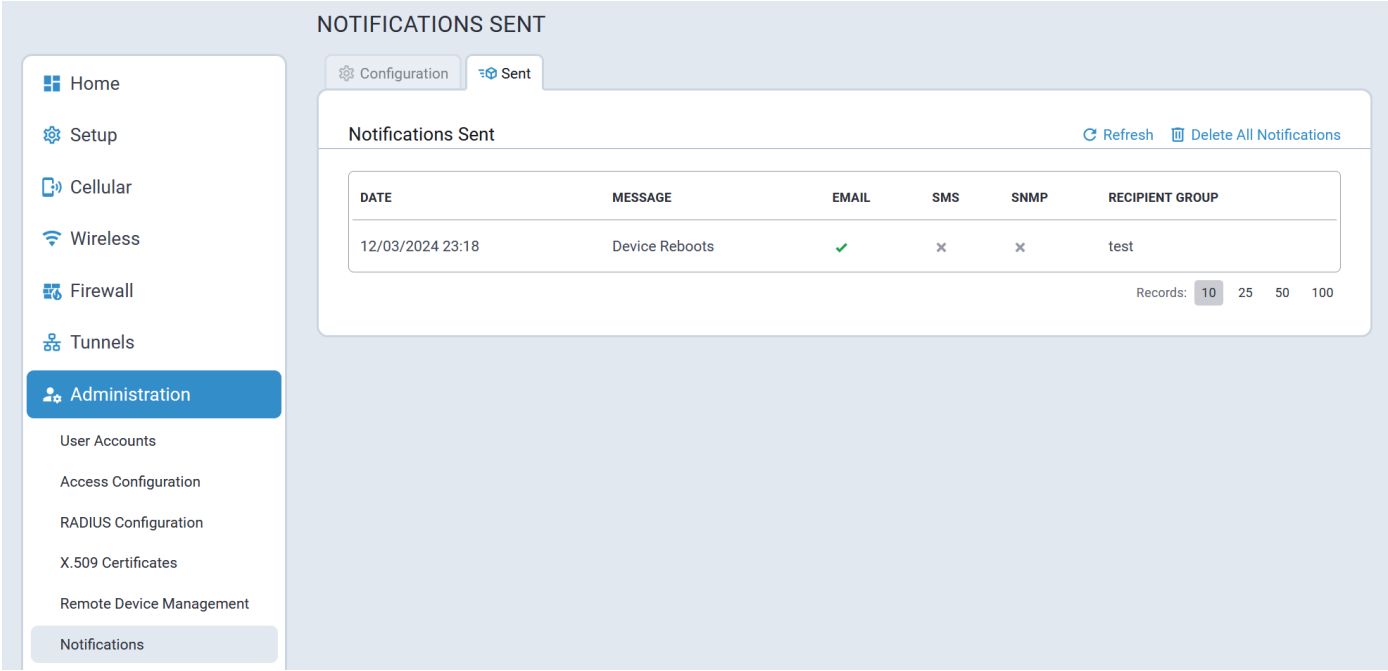
NAME	EMAIL	OPTIONS
admin	admin@test.test	



To edit an existing Recipient Group, click the  associated with the group to be edited. Add or delete contact information as required.

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:

### WEB UI CUSTOMIZATION

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

Footer Customization

Show Custom Info

Address 1

Address 2

City

State / Prv

Zip Code

Company Name

Country

Fax

Website

Phone Numbers

LABEL	PHONE	OPTIONS
No phones added yet		

Links

LABEL	URL	TEXT	OPTIONS
No links added yet			

Dashboard Customization

Device Name

Custom ID

Custom Image (310x180px) 30KB

No file selected

Upload

Remove

UI Customization

Button Color

Highlight Color

Button Font Color

Highlight Font Color

Custom Favicon (64x64px) 10KB

No file selected

Upload

Remove

Custom Logo (300x80px) 30KB

No file selected

Upload

Remove

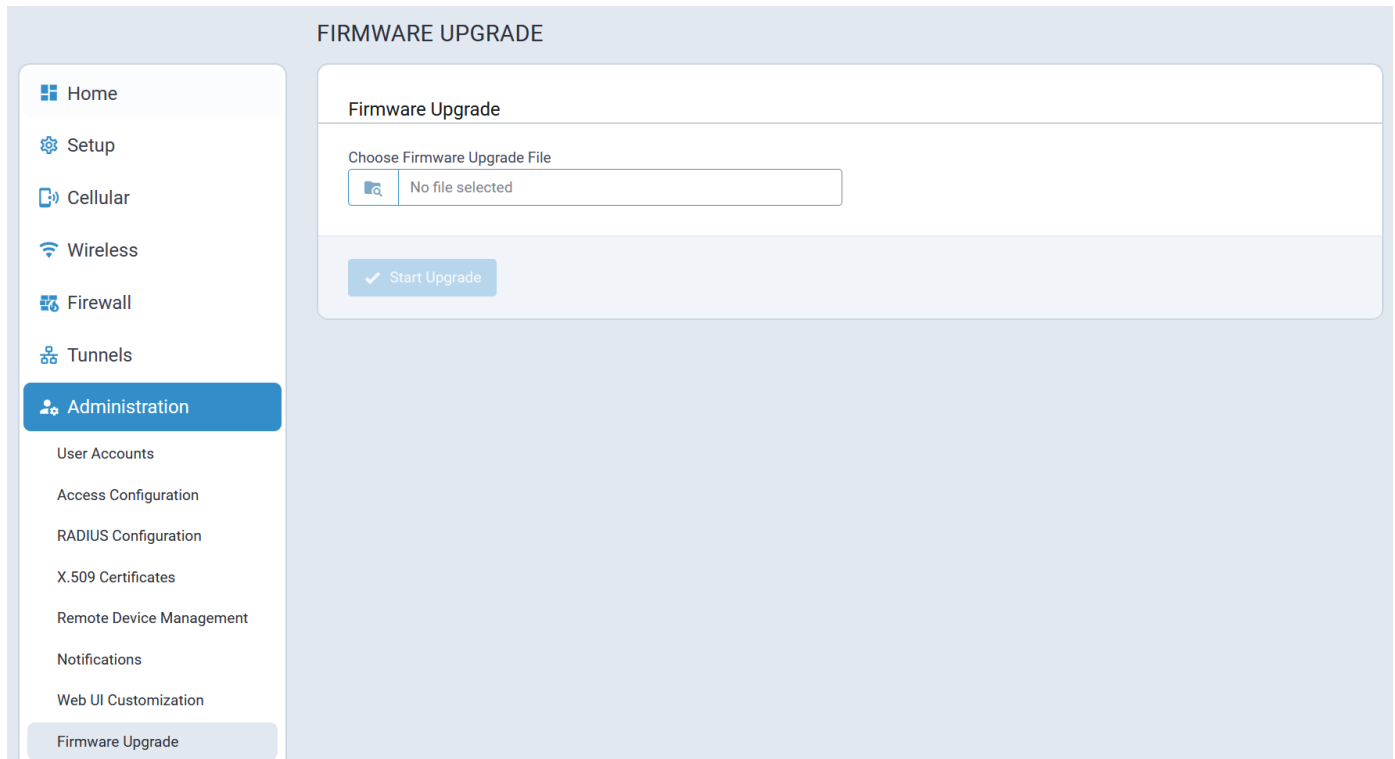
Submit

Reset To Default

## 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 screen is illustrated here:



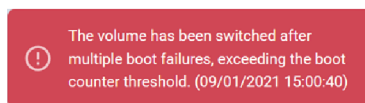
## System Fallback

To improve system reliability and ensure system recovery, the Conduit AP 300 employs a dual volume architecture.

If at any time the Conduit AP 300 fails to boot five consecutive times the system automatically reverts to the prior firmware version that is stored in the second volume.

**Note:** If the system successfully boots prior to triggering a fallback (e.g., during its fourth attempted reboot,) the boot counter is reset to zero.

Following a fallback, once the system successfully reboots the following message is displayed on the **Firmware Upgrade** screen to alert the user:



**Note:** This message will not be displayed if the system reverts to a firmware version prior to 7.1.0.

## 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:

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

PACKAGE MANAGEMENT

Install Package

No file selected

Install

Package List Update

Installed Packages

Filter packages

Storage: 424 KB

477.09 MB

PACKAGE	OPTIONS
No matching records	

## 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 page 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:

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

DEBUG OPTIONS

Auto Reboot Timer

Auto Reboot  
DISABLED

Remote Syslog

Enabled

Hostname  
mtr3-23067168

IP Address

Protocol  
UDP

Port  
514

Logging

Debug Log Level  
MAXIMUM

Download Logs

Data Traffic Statistics

Save Timeout (Seconds)  
300

Save Data Limit (MBytes)  
5

Ping

IP Address or URL

Number Of Requests  
4

Do Not Fragment

Network Interface  
ANY

Packet Size (Bytes)  
56

Ping

Continuous Ping

IP Address or URL

Packet Size (Bytes)  
56

Do Not Fragment

Network Interface  
ANY

Start Continuous Ping

Submit

Reset To Default

## Usage Policy

A typical Usage Policy tab is illustrated here:

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

USAGE POLICY

Usage Policy

This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Submit

Reset To Default

## Licensing

This page shows licenses on this device. Some licenses are factory installed. If you add a licensed feature after receiving the device and have a license file to add:

1. Go to **Administration > License**.
2. Click **Add New** in the upper right corner.
3. Add the **License Key** and **Password**.
4. Click **OK**.

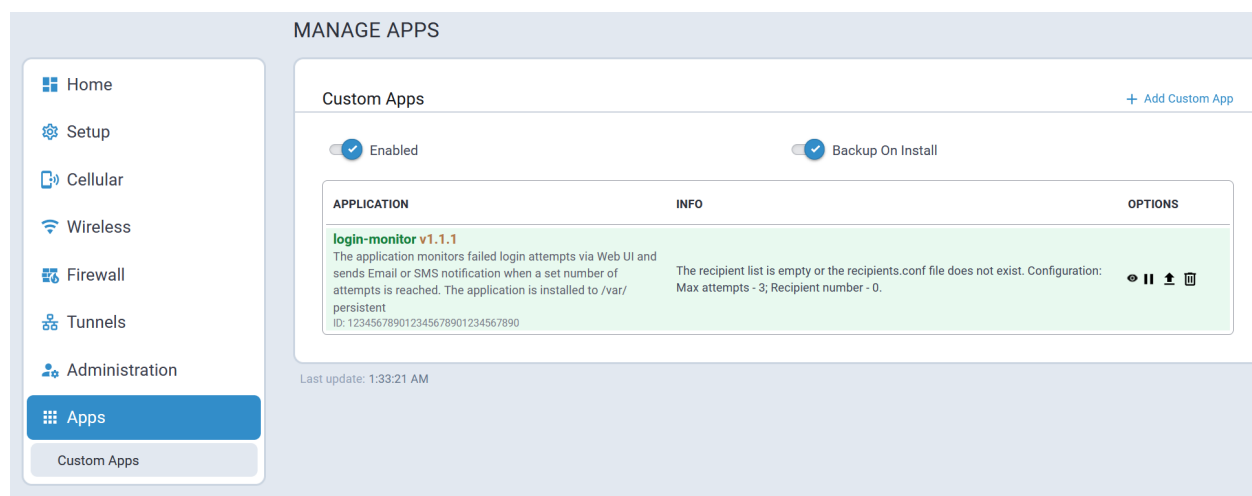
## Apps Menu

### Custom Apps


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

**Note:** For information about creating custom applications, refer to [Creating a Custom Application](#).

A typical Custom Apps page is illustrated here:



Parameter	Description
<b>Enabled</b>	<p>When <b>ENABLED</b>:</p> <ul style="list-style-type: none"> <li>The system launches all installed applications on boot.</li> <li>The system launches a custom application as soon as it has been installed.</li> </ul> <p>When <b>DISABLED</b>:</p> <ul style="list-style-type: none"> <li>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.</li> <li>The system allows the installation of custom applications, but it does not launch them.</li> <li>The system does not allow starting applications.</li> </ul>
<b>Backup on Install</b>	<p>When <b>ENABLED</b> (default setting) 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.</p>

**Note:** When a user disables the **Enabled** option and selects **Save and Apply**, the system does not stop any applications that are already running. To halt an application manually, locate the application in the list of installed applications and click the  button associated with the application to be stopped. For additional information, refer to [Installed Applications](#).

## Installed Applications

A list of custom applications that have been installed on the Conduit AP 300 is displayed on the Custom Apps page. A typical list is shown here:



APPLICATION	INFO	OPTIONS
<b>tomoyo_monitor_mtr v1.5</b> Track tomoyo violations and notify over Web UI ID: ac8bed96-3cf3-4b1b-9174-590f8af2a3c4	No security violations so far	
<b>cell-radio-set-cellauth v1.1.0</b> Custom application adds the "Cellular Authentication for LTE" support to mPower 6.3.x ID: c2e5640f-2c44-44bf-8dd1-e7fa87a531f5	App disabled. The current firmware natively supports Cellular Authentication for LTE	
<b>test_env_vars v0.1</b> An application that tests the presence of environment variables in start and stop scenarios. ID: 1111111111111111	Application started: CONFIG_DIR=/var/config/app/test_env_vars/config APP_DIR=/var/config/app/test_env_vars APP_ID=1111111111111111	
<b>test-several-pids v0.0.1 (1.1.3-alpha)</b> A simple app that runs two python scripts, that do nothing except sleeping ID: c2e5640f-2c44-44bf-8dd1-e7fa87a53321	Not Available	

Information about available application options is listed here:

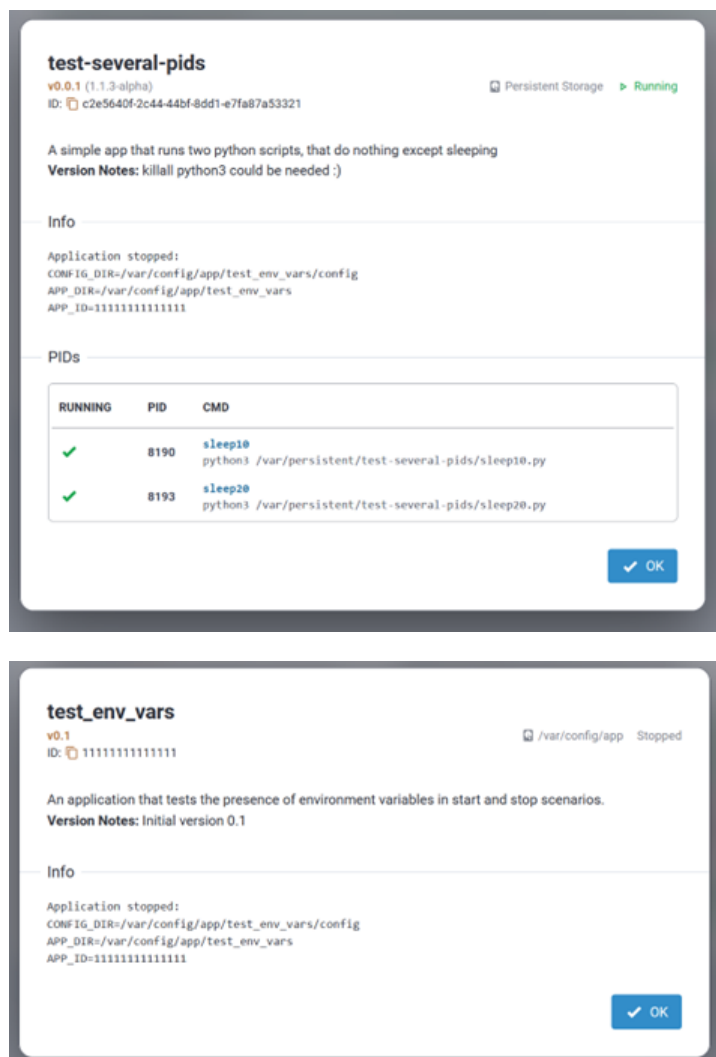
Icon	Function
	View application details
	Halt application
	TBD
	Delete the application

View Application Details

The following information about custom applications is displayed in a pop-up window when the respective option is selected:

- Application Name
- Application ID
- Application Version
- [Extra Version](#) [optional]
- Installation Location
  - Persistent Storage
  - /var/config/app
  - SD Card
- [Application Status](#)
- Application Description
- Version Notes
- Application Info; Not displayed if info is empty or "not available".
- Process IDs (PIDs)
  - Process ID
  - Running
  - Process Name
  - CMD

Typical Application Details pop-ups are displayed below:



### Application Status

The list of supported application statuses are provided below:

Status	Description
<b>STARTED</b>	The application is highlighted with green and there is a stop action in the Options column.
<b>RUNNING</b>	The application is highlighted with green and there is a stop action in the Options column.
<b>STOPPED</b>	The application is not highlighted and there is a start action in the Options column.
<b>FAILED</b>	The application is highlighted with red and the actual status is shown next to the app version.
<b>INSTALL FAILED</b>	The application is highlighted with red and the actual status is shown next to the app version.

Status	Description
<b>START FAILED</b>	The application is highlighted with red and the actual status is shown next to the app version.

### Extra Version Support

In addition to a custom application's version, which is stored in **manifest.json**, some applications may have an optional extra version which is managed by the custom application itself. The extra version is stored in the **[App Directory]/version\_extra** file.

If the **[App Directory]/version\_extra** file exists and is not empty, the extra version is displayed next to the application's current version.

#### MANAGE APPS

##### Custom Apps

[+ Add Custom App](#)

☒ Enabled
☒ Backup On Install

APPLICATION	INFO	OPTIONS
<b>tomoyo_monitor_mtr v1.5</b> Track tomoyo violations and notify over Web UI ID: ac8bed96-3cf3-4b1b-9174-590f8af2a3c4	No security violations so far	
<b>cell-radio-set-cellauth v1.1.0</b> Custom application adds the "Cellular Authentication for LTE" support to mPower 6.3.x ID: c2e5640f-2c44-44bf-8dd1-e7fa87a531f5	App disabled. The current firmware natively supports Cellular Authentication for LTE	
<b>test_env_vars v0.1</b> An application that tests the presence of environment variables in start and stop scenarios. ID: 1111111111111111	Application started: CONFIG_DIR=/var/config/app/test_env_vars/config APP_DIR=/var/config/app/test_env_vars APP_ID=1111111111111111	
<b>test-several-pids v0.0.1 (1.1.3-alpha)</b> A simple app that runs two python scripts, that do nothing except sleeping ID: c2e5640f-2c44-44bf-8dd1-e7fa87a53321	Not Available	

## Install a Custom App

Perform the following procedure 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 has been installed, the following information is displayed:

- The application's name
- Description
- Installed version
- App ID
- Current [status](#)
- Application information

## 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",
```

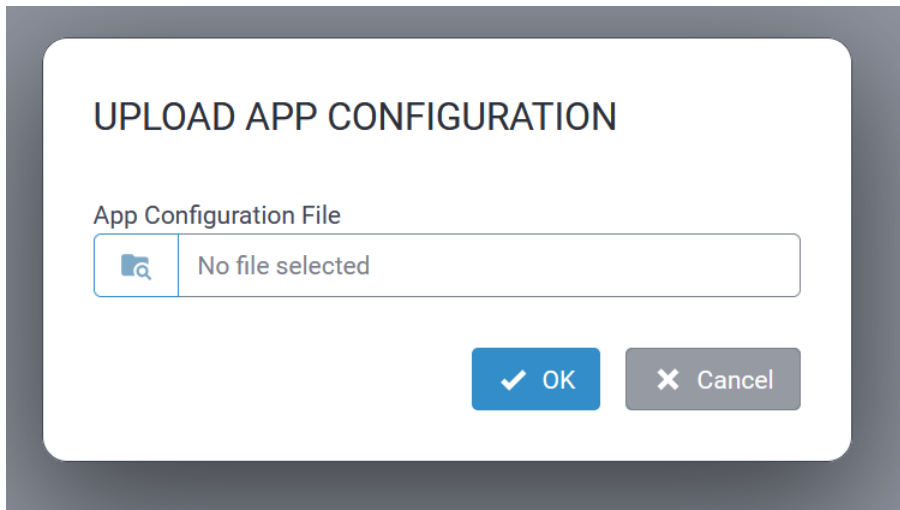
```

    "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

Send Notification is a command-line utility providing a simple method to send notifications via SMS and e-mail.

The path to the utility is: **/usr/bin/send-notification**

```

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#

```

Send Notifications supports sending notifications to one or more recipients allowing one notification to be sent to multiple recipients simultaneously.

---

## Warranty

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

## Contact Information

General Information	<a href="mailto:info@multitech.com">info@multitech.com</a> <a href="https://multitech.com/contact-us/">https://multitech.com/contact-us/</a>
Sales	+1 (763) 785-3500 <a href="mailto:sales@multitech.com">sales@multitech.com</a>
Technical Support Portal	+1 (763) 717-5863 <a href="https://support.multitech.com">https://support.multitech.com</a>
Website	<a href="http://www.multitech.com">www.multitech.com</a>
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 MTCAP3 Configuration Guide.	