Telco T1 Documentation

Version 1.0

RCM Certified

Table of Contents

1 Package Contents **3**

2 General Setup **4**

2.1 Firmware Upgrade 4

3 Mobile Data - Advanced Setup **5**

3.1 Authentication 5

3.2 Band Locking 6

Lock to Frequency Bands 6

4 Wifi - Advanced Setup **7**

4.1 Wifi Radio Configuration 7

4.1.1 General 7

4.2 Advanced Wifi Radio Configuration 8

4.3 Advanced Interface Options 10

4.3.1 General Tab 10

4.3.2 Wireless Security Tab 11

2.4.3.3 MAC Filter Tab 12

2.4.3.4 Advanced Settings 13

5 Advanced Commands **14**

5.0.1 Show all available commands 14

5.1 Signal Information 14

5.1.1 Show active band information 14

5.1.2 Get Signal Strength 14

1 Package Contents

Please ensure your package contains everything in the following list. In the event that anything is missing or damaged, please do not hesitate to contact us at sales@telcoantennas.com.au or +61 (07) 3393 9919 M-F 9am to 5pm AEST.

1. 1x Telco T1
2. 1x PoE adaptor
3. 1x LTE antenna
4. 1x Wifi antenna
5. 1x Ethernet cable
6. 2x stainless straps
7. 2x screws
8. 1x Mini-Quick Start Guide

Package contents

2 General Setup

2.1 Firmware Upgrade

Please visit www.telcoelectronics.com.au/downloads for the latest firmware, free for life, which contains new features, enhancements and fixes.

3 Mobile Data - Advanced Setup

3.1 Authentication

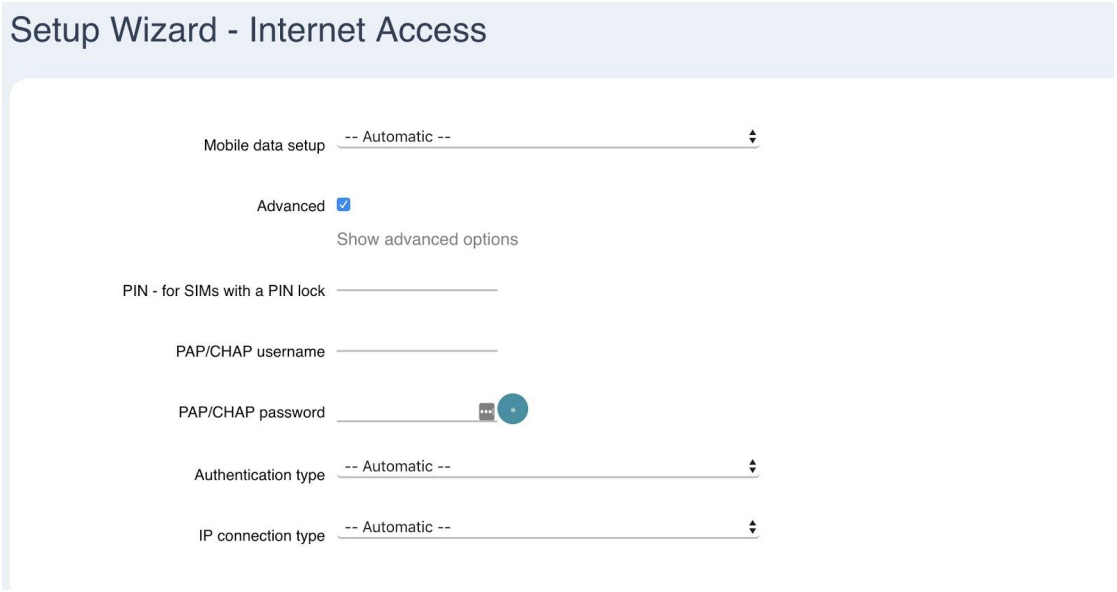
If your connection requires the use of extra parameters, these are located under the Advanced Setup options.

The following advanced options are revealed by ticking the ***Advanced*** box underneath *Mobile data setup*:

- PIN
- PAP/CHAP username
- PAP/CHAP password
- Authentication type: PAP/CHAP (both), PAP, CHAP
- IP connection type: IPv4/IPv6 (default to IPv4), IPv4 only, IPv6 only

Tip: Use of these options depend on your SIM card and mobile data plan. Please consult your mobile network operator (*e.g.* Telstra) for the details. These details are normally included with your SIM as accompanying documentation if they are required.

Note: Either incorrectly setting, or erroneously omitting any of these values, will result in a connection failure.



Advanced options revealed

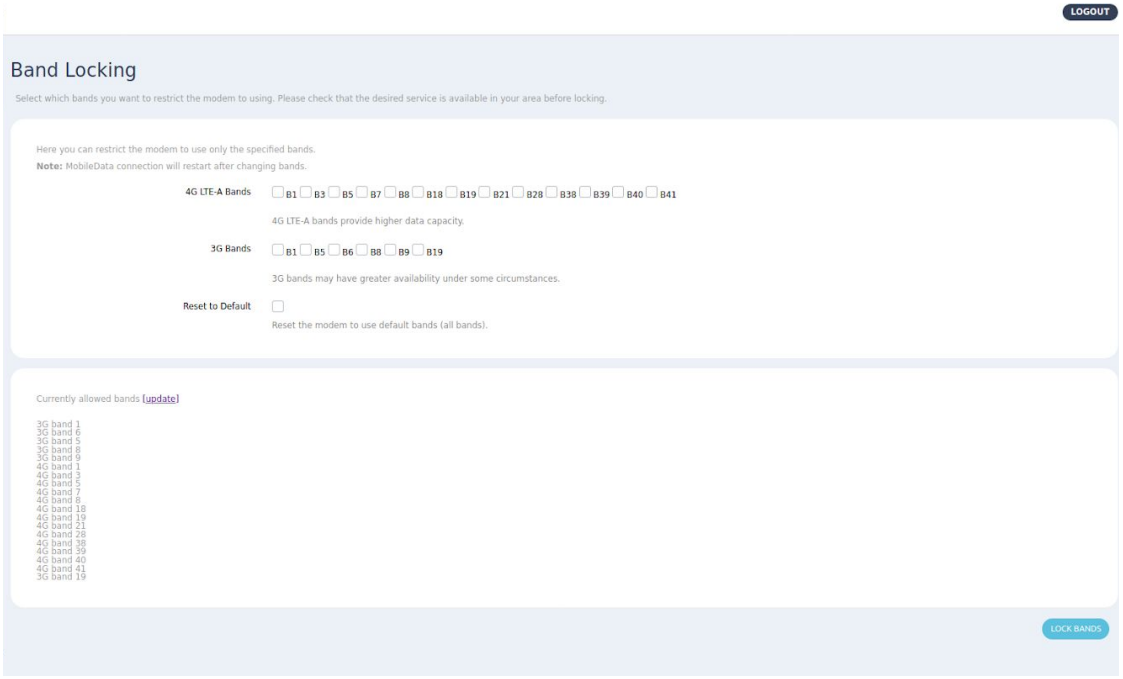
3.2 Band Locking

Lock to Frequency Bands

- Menu location: **Network** > **Band Locking**

You may set the T1 to only use any combination of selected 3G and 4G frequency bands. Note: please check beforehand that the desired frequency bands are indeed available in your area, else you may lock to bands that are not available and thus will not connect to the internet.

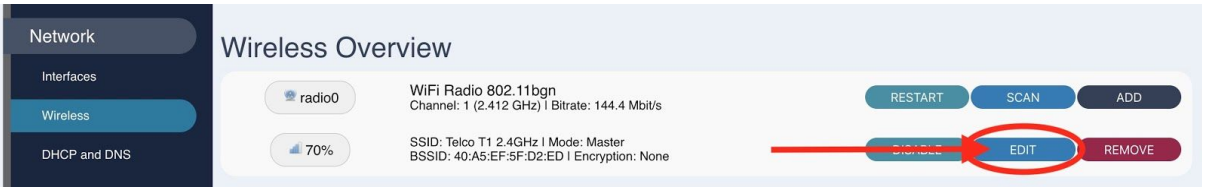
1. Select the desired bands
2. Click Lock Bands
3. Wait a moment as the T1 locks bands then restarts the mobile connection.
4. Check the Mobile Data Status page to confirm you are on the desired bands.



4 Wifi - Advanced Setup

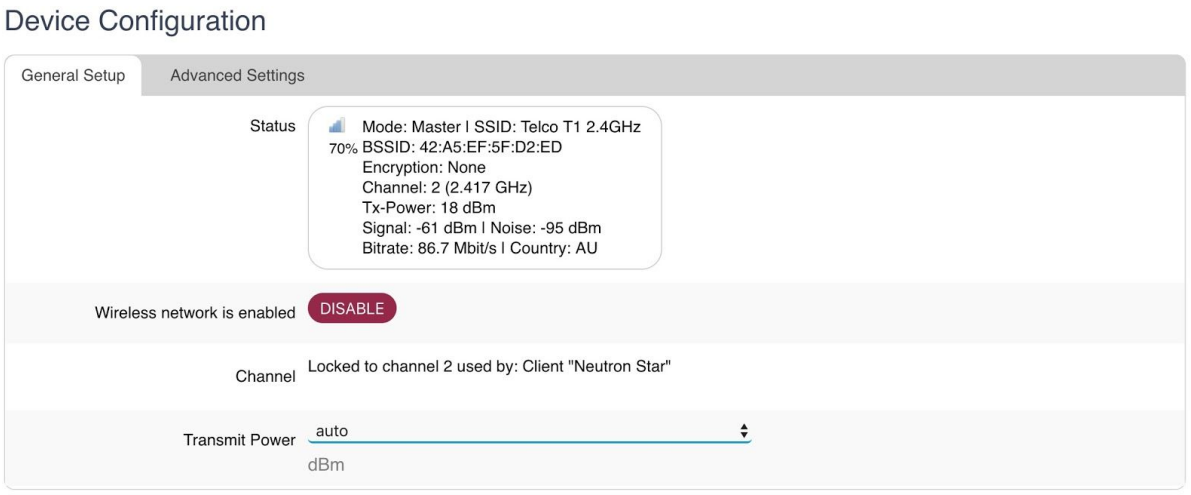
While it works great out of the box, T1 offers a wide array of options that give you complete control over the wireless LAN hardware.

Navigate to **Network** > **Wireless** and **Edit** the Wifi network



Wireless configuration options are distinguished by **Device** options, which are changeable parameters of the wifi radio for that network, and by **Interface** options, which are changeable parameters of a particular Wifi ESSID or Mesh ID that identifies that network. T1 supports multiple networks, all with different parameters*.

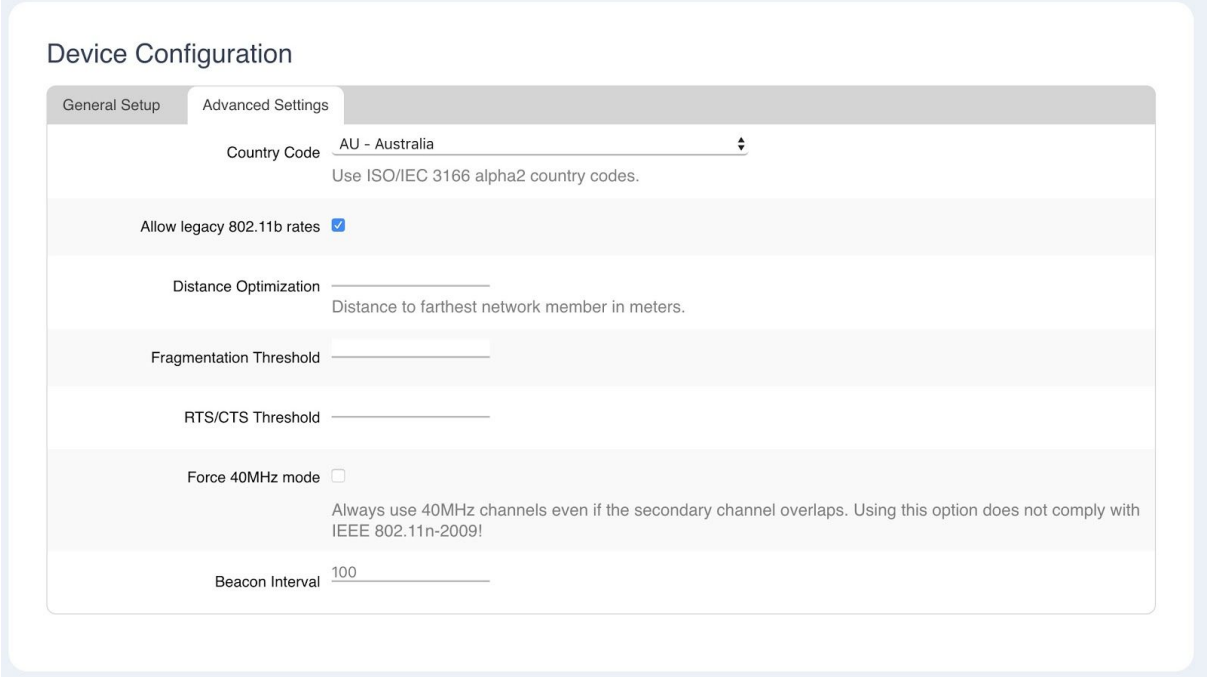
4.1 Wifi Radio Configuration



4.1.1 General

- **Transmit Power** - amount of power output by the radio, limited by the EIRP limit dictated by the Country Code
    - Default: auto
    - Unit: expressed as both dBm and mW

4.2 Advanced Wifi Radio Configuration



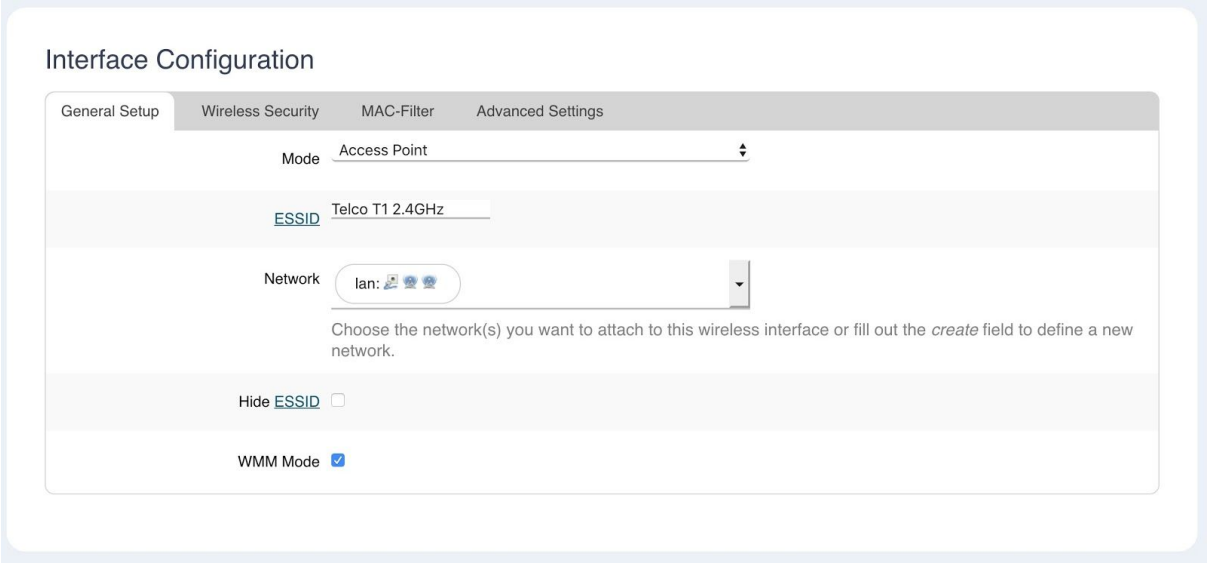
Advanced device options include the following:

- **Country Code** - the ISO/IEC 3166 country code which determines the frequencies and transmit power allowed to be used in that designated regulation domain. Please set this to the country you are operating the device in, in order to comply with local regulations.
    - Default: AU - Australia
- **Allow legacy 802.11b rates** - allow 802.11b devices to connect the expense of losing faster data rates. We recommend disabling this unless you explicitly need to support 802.11b devices.
    - Default: Enabled
- **Distance Optimisation** - Used by proprietary system to optimize transmission to the furthest client.
    - Default: blank
    - Unit: meters
- **Fragmentation Threshold** - specify the maximum size of a frame before it is broken into smaller frames. Useful when operating in areas with interference or long distance links. Setting to the maximum value of 2346 effectively disables this feature.
    - Default value: blank
    - Unit: 802.11 frame size (bytes, *i.e.* octets)
- **RTS/CTS Threshold** - Request To Send/Clear To Send threshold - use the 802.11 RTS/CTS protocol for frames above this size limit. Useful when operating in areas with a high concentration of other Access Points or clients,

though setting the value too low adds unnecessary overhead. Setting to the maximum value of 2346 effectively disables this feature.
    - Default: blank
    - Unit: 802.11 frame size (bytes, *i.e.* octets)
- **Force 40MHz mode** - force the radio to use 40MHz channels even if the bonded channel overlaps with the primary channel. This is not compliant with 802.11n-2009, but can increase the available bandwidth, however its use must be considered against the effects of self-interference.
    - Default: Disabled
- **Beacon Interval** - Time Units between broadcast of the 802.11 beacon (a management frame) which serves to synchronise devices connected to the AP. Setting a lower value can improve throughput at the expense of raised power usage by the clients. Setting too high a value could lower power consumption but may cause connectivity issues.
    - Default: 100
    - Unit: 802.11 Time Unit (100TU = 102.4ms)

4.3 Advanced Interface Options

The Wireless Interface section contains options for changing the operation of a wireless interface.

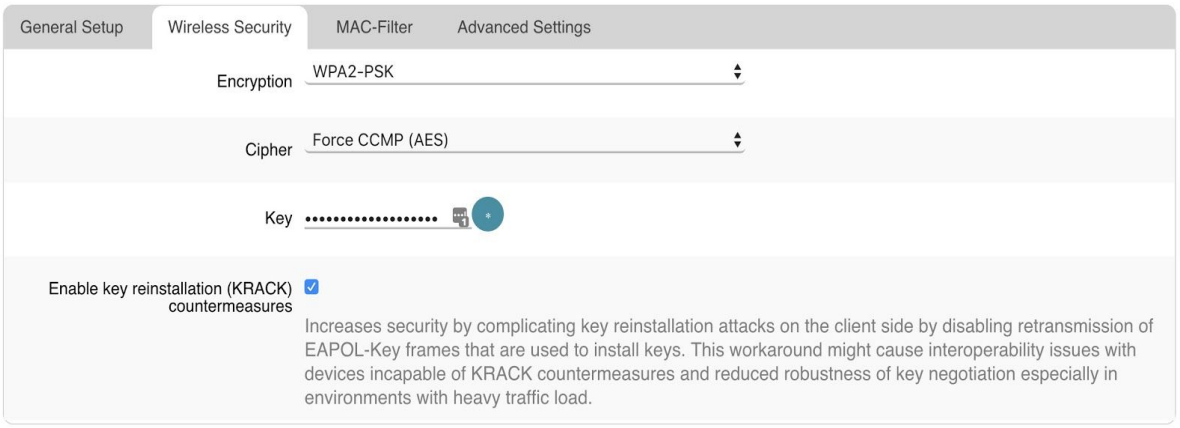


4.3.1 General Tab

- **Mode** - the primary function of this interface
  - **Access Point** - a complete, standard wireless access point which broadcasts an SSID and allows clients to connect
  - **Client** - allows connecting the T1 to another SSID as a client. Correct SSID and authentication credentials are required. See also: **Scan** for the recommended way of setting up a Client network
  - **802.11s** - mesh network support
  - **Ad-Hoc** - legacy mesh network support
  - **Pseudo Ad-hoc** - useful for PtP topology with no interference. Included for legacy support.
  - **Monitor** - monitor wireless traffic
  - **Access Point (WDS)** - useful for PtP relay networks, normally requiring 2 AP's.
    - *Tip: Prevent WDS throughput loss by connecting your devices to the LAN port of the T1.*
  - **Client (WDS)** - useful for PtP relay networks
- **ESSID** - Extended Service Set Identification, other devices will see this as the **SSID**.
- **Network** - the network to attach this interface to. Networks are where firewall rules and routing settings are managed.
- **Hide ESSID** - hide the broadcast of the ESSID (SSID)
  - Default: disabled
- **WMM Mode** - Toggle Wifi Multimedia Mode support
  - Default: enabled

4.3.2 Wireless Security Tab

Wireless Security options are where you will change the encryption and passwords used to secure your Wifi network.

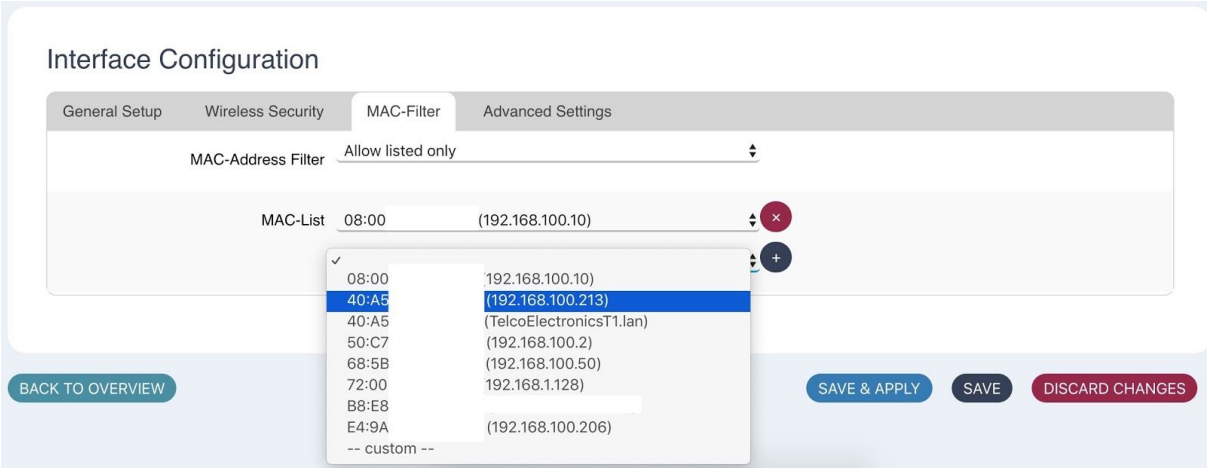


Tip: For the most secure Wifi access point use the following settings: *WPA2-PSK*, *Force CCMP (AES), Enable KRACK countermeasures* and a strong password.

- **Encryption**
  - No Encryption
  - WPA2-PSK - Wifi Protected Access v2 with Pre-shared Key
    - Pre-Shared key is the password
  - WPA-PSK - Wifi Protected Access v1 with Pre-shared Key
  - WEP Open System
  - WEP Shared Key
  - WPA-PSK/WPA2-PSK - Default to WPA2, but fall back to WPA if not supported by the client. Trade-off is security for backwards compatibility.
- **Cipher**
  - Various ciphers are included for backwards compatibility and state of the art security.
- **Key**
  - The wifi password, in technical terms known as a “key”
- **Enable key reinstallation (KRACK) countermeasures**
  - Countermeasure for the WPA2 KRACK vulnerabilities disclosed in late 2017. We recommend enabling this feature.

2.4.3.3 MAC Filter Tab

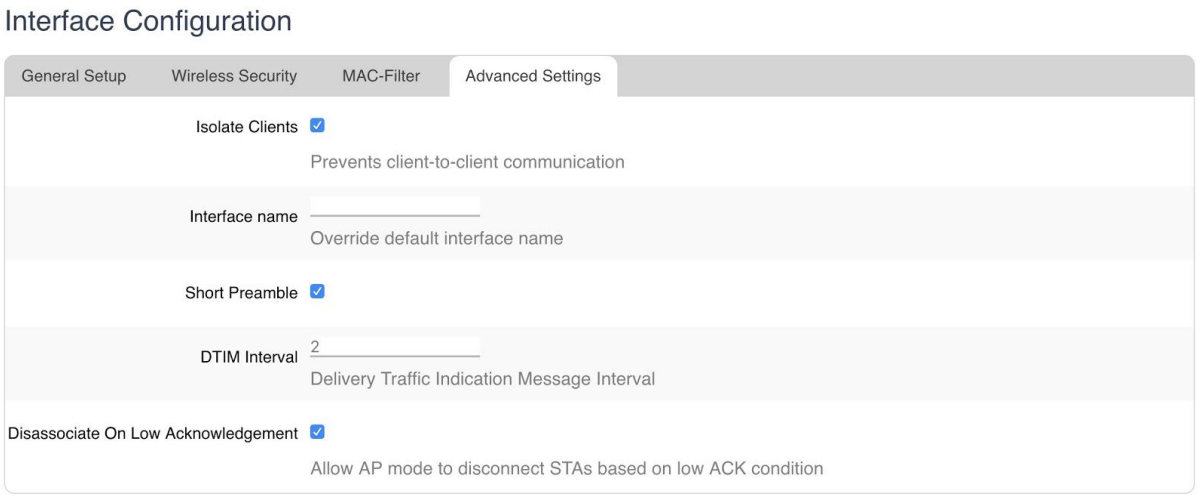
The **MAC-Filter** tab contains settings for controlling access to the Wifi based on a MAC address blacklist or whitelist.



- **Allow listed only** - basic whitelisting policy
- **Allow all except listed** - basic blacklisting policy
- **MAC-List** - Choose from a dropdown containing connected hosts, or select *--custom--* to enter one.

2.4.3.4 Advanced Settings

Advanced Settings contain options for fine tuning Wifi parameters.



- **Isolate Clients** - prevent client-to-client communication
  - Default: disabled
- **Interface name** - Override the default interface name
  - Default: blank
- **Short Preamble** - shorten the 802.11 preamble to reduce overhead
  - Default: enabled
- **DTIM Interval** - Delivery Time Indication Message Interval is used to aid power saving for wireless devices. A longer interval could save more power on mobile devices but could reduce performance in latency-sensitive applications such as VoIP.
  - Range: 1 to 255
  - Default: 2
- **Disassociate On Low Acknowledgement** - When the ACK from clients (stations) is low, disassociate, or kick the client from the AP. Recommended to leave enabled.

5 Advanced Commands

5.0.1 Show all available commands

Command
qmicli --help-all

5.1 Signal Information

These commands must be run from a shell on the device.

5.1.1 Show active band information

Command
qmicli -d /dev/cdc-wdm0 -p --nas-get-rf-band-info

Example Output
[/dev/cdc-wdm0] Successfully got RF band info
Radio Interface: 'lte'
Active Band Class: 'eutran-3'
Active Channel: '1725'

5.1.2 Get Signal Strength

Command
qmicli -d /dev/cdc-wdm0 -p --nas-get-signal-strength

Example Output
Current:
Network 'lte': '-65 dBm'
RSSI:
Network 'lte': '-65 dBm'
ECIO:
Network 'lte': '-2.5 dBm'
IO: '-106 dBm'
SINR (8): '9.0 dB'
RSRQ:
Network 'lte': '-16 dB'
SNR:
Network 'lte': '1.0 dB'
RSRP:
Network 'lte': '-96 dBm'