



SHIELD MegaFi

Software Guide

Table of Contents

Revision History	iii
1 Introduction	1
1.1 Objectives	1
1.2 Conventions.....	1
1.3 Related Documents.....	2
1.4 Abbreviations and Acronyms.....	3
1.5 About OpenWRT and Mission Control.....	5
1.6 About this Document.....	5
1.7 Support	5
2 Misson Control.....	7
2.1 Accessing Mission Control via Ethernet Connection	8
2.2 Initial Connection to MegaFi via Wi-Fi	13
2.3 Navigating Mission Control.....	19
2.4 Working within Mission Control.....	22
3 Basic Configuration Settings	31
3.1 Changing APN (Access Point Name)	32
3.2 Changing LAN IP Address	32
3.3 Flash/Update Firmware	33
3.4 Backup Existing Configuration.....	37
3.5 Load Configuration from File	38
3.6 Change Password.....	40
3.7 Factory Defaults via Mission Control	42
3.8 Vehicle Shutdown Delay	44
3.9 Reboot.....	45
3.10 Wi-Fi Settings.....	47
3.11 NAT vs. Passthrough Mode.....	50
3.12 Band Lock	55
3.13 SSH Access.....	57
3.14 GPS Output Configuration	60
4 Expert Configuration Settings.....	67
4.1 Enter Expert Mode.....	68
4.2 Status.....	69
4.3 System	86

4.4 Network.....	103
4.5 Logout.....	159
5.1 Appendix 1 – Firewall Traffic Rule for Remote SSH Example	160

Revision History

Rev	Iteration	Description	Incorporated By	Date
1	1	Initial Release	Lorenzo Porchas	1/16/2024
1	2	WiFi encryption enhancements, Passthrough mode feature with introduction of firmware version 2.4.44, and manual software update instructions	Lorenzo Porchas	4/9/2024
1	3	With firmware version release 2.4.95 and above, and the subsequent release of version 2.5.0, this guide includes improvements to GPS, and other minor setting changes	Lorenzo Porchas	7/30/2024

1 | Introduction

The purpose of this guide is to assist the user in operating the SHIELD MegaFi wireless WAN HPUE router. This guide will help the user configure and operate the device using the device's-built Mission Control software.

- ❗ For assistance in implementing or installing the MegaFi device, please refer to the separate *MegaFi User Guide*.
- ➡ **Note:** All images used in this document are used only for displaying examples of configurations and may not reflect the users' current device.

1.1 Objectives

The objectives of this document are:

- to describe the software environment and basic understanding of interacting and configuring MegaFi for your use.
- to provide the necessary information to understand the device and the options available in the MegaFi, and
- to support implementing the necessary configuration for your communications environment and for your continued use.
- This document expects the user to have basic computer skills and to be familiar with using and navigating with a web browser, to be knowledgeable in networking concepts, and to be able to configure a traditional wired or wireless router for their communications environment.

1.2 Conventions

This document follows certain typographic conventions, outlined below:

Bold

Is used for directories, filenames, commands, and options. All terms shown in bold are typed literally.

Bold Italic

Is used to show generic arguments and options; these should be replaced with user-supplied values.

Italic

Is used to highlight comments in examples.

Constant Width

Is used to show the contents of files or the output from commands.

1.3 Related Documents

- 📄 The *MegaFi User Guide*: <https://nextivityinc.com/wp-content/uploads/2024/01/SHIELD-MegaFi-User-Guide.pdf>
- 📄 The *MegaPortal User Guide*: <https://go.nextivityinc.com/shield-megaportal-guide>
- 📄 The *MegaFi Software Update Guide*: <https://nextivityinc.com/wp-content/uploads/2023/11/SHIELD-MegaFi-Software-Update-Guide.pdf>
- 📄 For other MegaFi documentation, go to www.nextivityinc.com/support and select the FirstNet HPUE tab.

1.4 Abbreviations and Acronyms

The following table provides a list of abbreviations and acronyms that are referenced throughout this manual.

APN	Access Point Name	NTPD	Network Time Protocol Daemon
DHCP	Dynamic Host Configuration Protocol	PD	Prefix Delegation
DNS	Domain Name System	PID	Process Identification Number
DDNS	Dynamic Domain Name System	PIN	Personal Identification Number
GNSS	Global Navigation Satellite System	Ping	Packet Internet Groper
GPS	Global Positioning System	PoE	Power over Ethernet
HTTPS	Hypertext Transfer Protocol Secure	PPP	Point-to-Point Protocol
ICCID	Integrated Circuit Card Identifier	PPPoE	Point-to-Point Protocol over Ethernet
ICMP	Internet Control Message Protocol	RA	Route Advertisement
IGMP	Internet Group Management Protocol	SIM	Subscriber Identity Module
IMEI	International Mobile Equipment Identity	SLAAC	Stateless Address Auto Configuration
IMSI	International Mobile Subscriber Identity	SSH	Secure Shell
IP	Internet Protocol	SSID	Service Set Identifier
IPSEC	Internet Protocol Security	STP	Spanning Tree Protocol
LAN	Local Area Network	TAIP	Trimble ASCII Interface Protocol
LTE	Long-Term Evolution	TFTP	Trivial File Transfer Protocol
MAC address	Media Access Control address	UDP	User Datagram Protocol
MCBV	Modem Configuration Band Values	UTC	Coordinated Universal Time

MCLBV	Modem Configuration LTE Band Values	UUID	Universally Unique Identifier
MTU	Maximum Transmission Unit	VLAN	Virtual LAN
NAT	Network Address Translation	VPN	Virtual Private Network
NDP Proxy	Neighbor Discovery Protocol Proxy	HPUE	High Power User Equipment

1.5 About OpenWRT and Mission Control

The OpenWRT software that the MegaFi system uses is an open-source project that provides a full-featured operating system for embedded devices. Nextivity's implementation of OpenWRT LuCI—the dashboard that allows you to configure and manage the MegaFi suite of software and devices from a single computer—is known as Mission Control.

1.6 About this Document

This document is in 4 parts: part 1 is the Introduction, part 2 is Mission Control, part 3 is Most Frequent Configuration Settings and part 4 is Expert Configuration Settings.

You are currently in the introduction. Part 2, Mission Control, provides information on accessing, navigating, and working within the system, including how to save your work. We cannot emphasize enough how important it is that you understand how to navigate and work within the system as it is a new experience for many. Indeed, if this is your first time using this document and/or accessing the dashboard, then we recommend reading it in its entirety.

Part 3 is Most Frequent Configuration Settings. Most users can simply use this section to complete the most frequent and basic configuration settings such as password, wi-fi, firmware updates, APN, IP address and others.

Part 4 is Expert Configuration Settings. This is where you will view and manage your device at a more advanced level. The user can schedule tasks, configure interfaces, set firewall rules, etc.

1.7 Support

Nextivity's support desk is always ready to help you with any support issues or requests. If you encounter any problems, need clarification, or have feedback, recommendations, or suggestions then feel free to contact us at support@nextivityinc.com.

For additional assistance: +1 (858) 485-9442 **OPTION 1**
Support Business Hours: 6:00 AM – 5:00 PM PST

We look forward to being of service.

2 | Mission Control

Mission Control is the built-in web interface that provides information about the SHIELD MegaFi router and allows the user to configure settings to their preferences. All configuration and management are done via your computer's web browser, and you will need to be locally connected to the device via Ethernet to a LAN port, or by utilizing its Wi-Fi capability in the admin dashboard.

Refer to the following topics to get started with using Mission Control.

2.1 Accessing Mission Control via Ethernet Connection.....	8
2.2 Initial Connection to MegaFi via Wi-Fi.....	13
2.3 Navigating Mission Control	19
2.4 Working within Mission Control	22

2.1 Accessing Mission Control via Ethernet Connection

To access Mission Control, you will need both your **admin Password**, and the default factory **LAN IP, 192.168.113.1**. The Password is printed on the label on the bottom of your MegaFi.

➤ **Note:** Use the defined password and/or IP address if it has been changed for your environment.

1. Connect an Ethernet cable between your computer and any LAN port (1-4) on the MegaFi.
2. Open a web browser to the following address: <https://192.168.113.1>
3. The first time you try to connect to MegaFi, a connection warning screen will display as shown below. Accept the connection warning by clicking on '**Advanced**'.

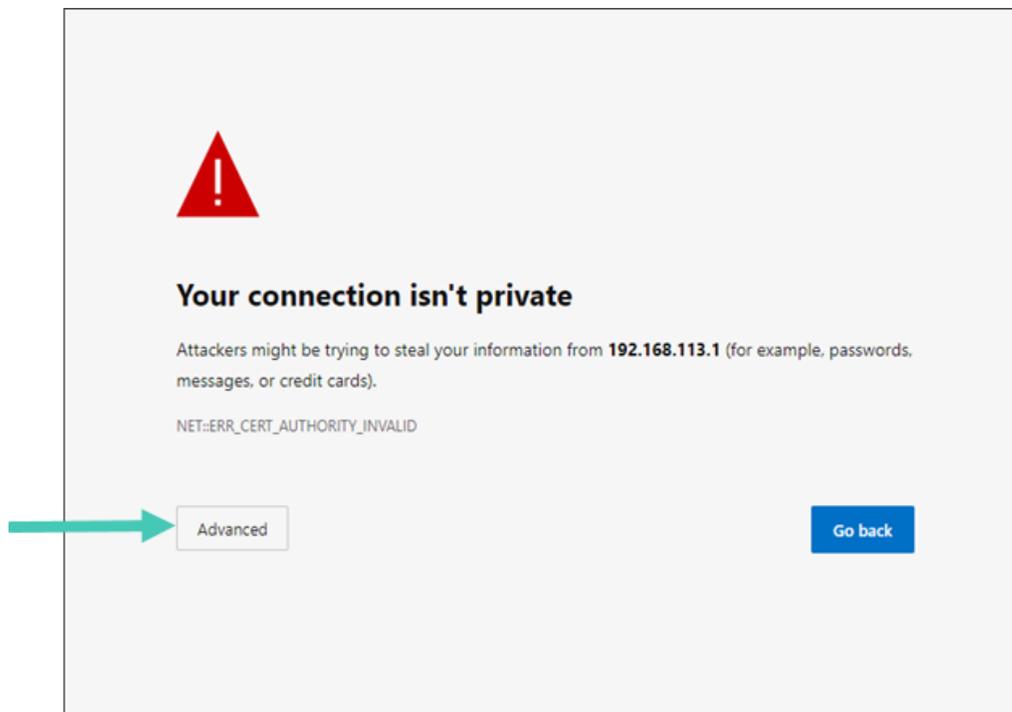


Figure 1: MegaFi connection warning screen

4. A second warning screen will be displayed as shown below. Click on '**Continue to 192.168.113.1 (unsafe)**' link to proceed.

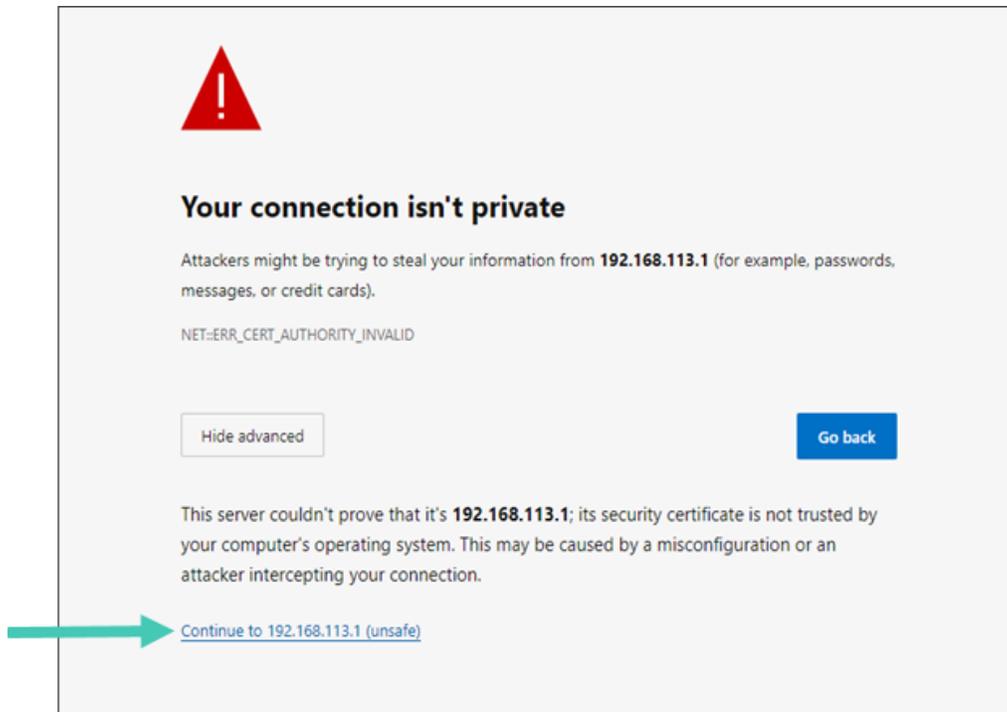


Figure 2: MegaFi connection warning – second screen

5. The MegaFi's Mission Control GUI login page will now be displayed.
 - 5a. Enter the password as found on the bottom label of the MegaFi on the Mission Control login page.
 - **Note:** username always defaults to 'admin'.
 - 5b. Click '**Login**' to proceed.

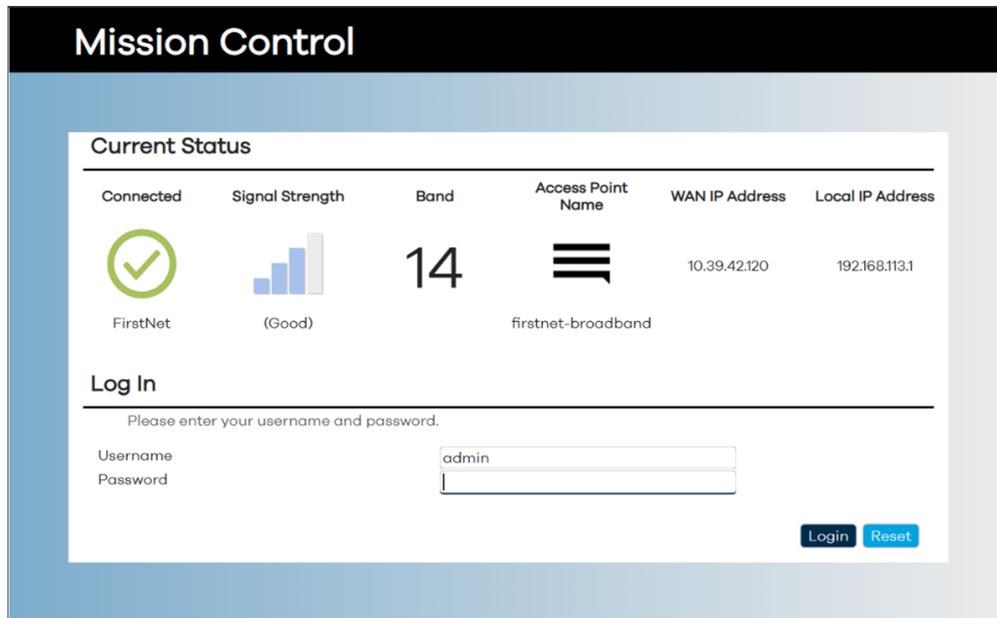


Figure 3: Mission Control login screen

6. When logging in for the first time, the EULA (End User License Agreement) will be displayed.
7. Fill out the requested information and click 'Accept' to continue.



Figure 4: Nextivity, Inc. End User License Agreement screen

8. Also, part of first-time login to MegaFi, the user will be required to change the default login password.
 - 8a. Proceed to change the default password to a 'Strong' password.
 - ➔ **Note:** The device will not accept weak passwords. Password must meet the following requirements: a minimum length of 10 characters and a randomized complexity of lowercase letters, uppercase letters, and numbers.
 - 8b. Confirm the new password change by clicking on '**Save**'.

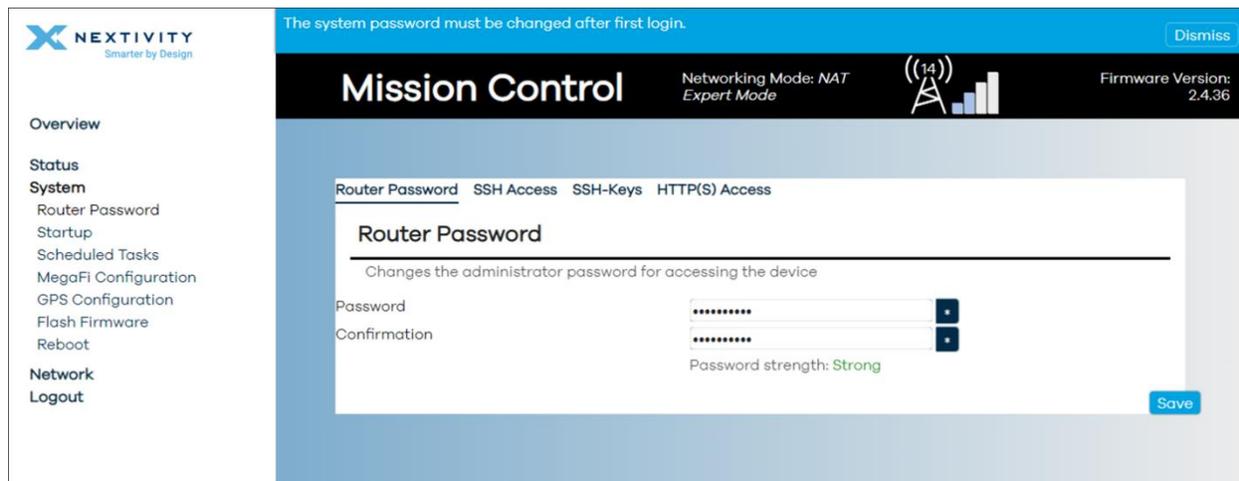


Figure 5: Change router password screen

9. The user will now be re-directed to Mission Control's Overview page.



Figure 6: Mission Control – Overview, Device page

10. First-time router configuration is now complete!

2.2 Initial Connection to MegaFi via Wi-Fi

To access Mission Control, you will need both your admin Password, and the default factory LAN IP, 192.168.113.1. The Password is printed on the label on the bottom of your MegaFi.

Notes:

- Use the defined password and/or IP address if it has been changed for your environment.
- The example shown below was accomplished using a Windows (10/11) PC. The steps should be similar using a different OS.

To connect to MegaFi via Wi-Fi:

1. Go into your PC computer's **Network & internet > Wi-Fi** settings to add a new Wi-Fi connection.
2. Add the MegaFi device by looking for its default SSID under '**Show available networks**' by selecting it. The default SSID and its password are printed on the device's label.



Figure 7: Windows Network & Internet window showing list of available Wi-Fi networks

3. The '**Connect automatically**' box will be checked by default. Click on '**Connect**'.



Figure 8: Wi-Fi Network Connection – Connect automatically option

4. 'Enter the network security key' (default SSID password), then click on 'Next'. The default SSID and its password are printed on the device's label.

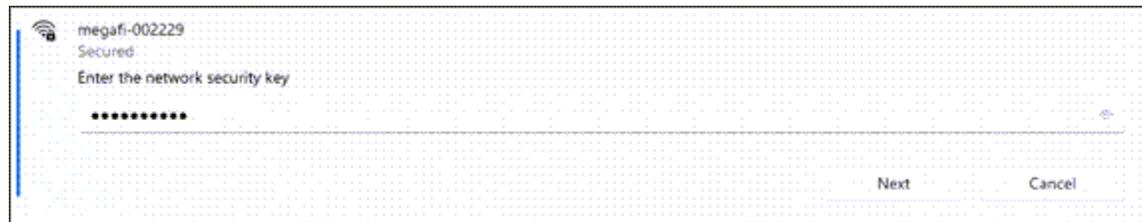


Figure 9: Wi-Fi Network Connection – Enter network security key

5. If the connection is successful, it will say 'Connected, secured'.



Figure 10: Wi-Fi Network Connection – Successful connection

6. Open a web browser to the following address: <https://192.168.113.1>
7. The first time you try to connect to MegaFi, a connection warning screen will display as shown below. Accept the connection warning by clicking on 'Advanced'.

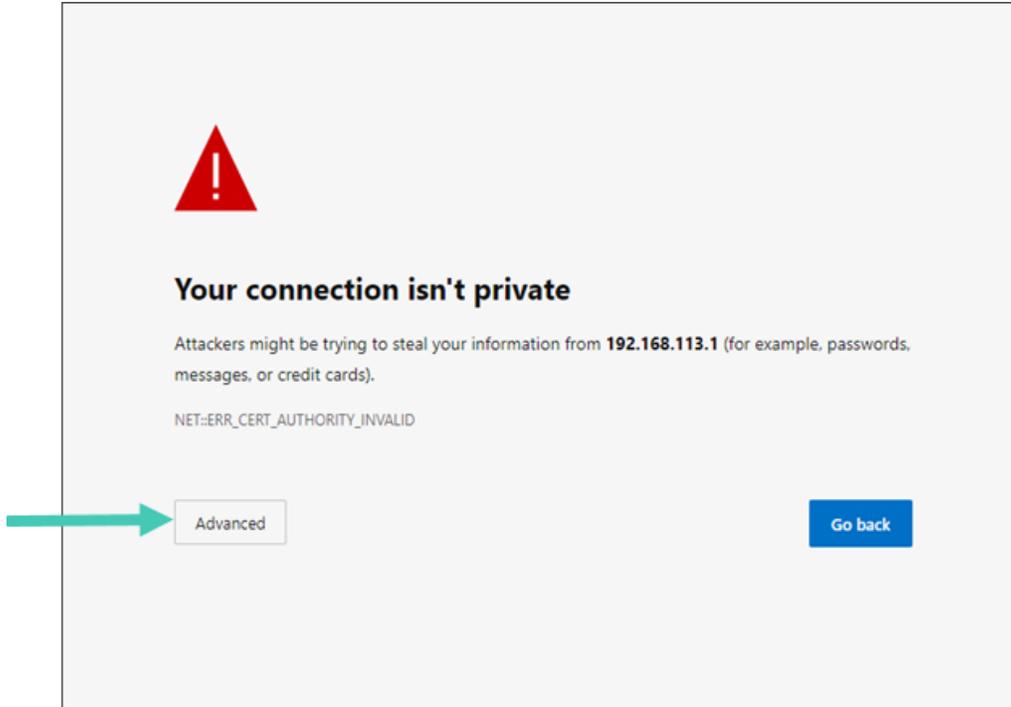


Figure 11: Warning message – Connection not private

8. A second warning screen will be displayed as shown below. Click on 'Continue to 192.168.113.1 (unsafe)' link to proceed.

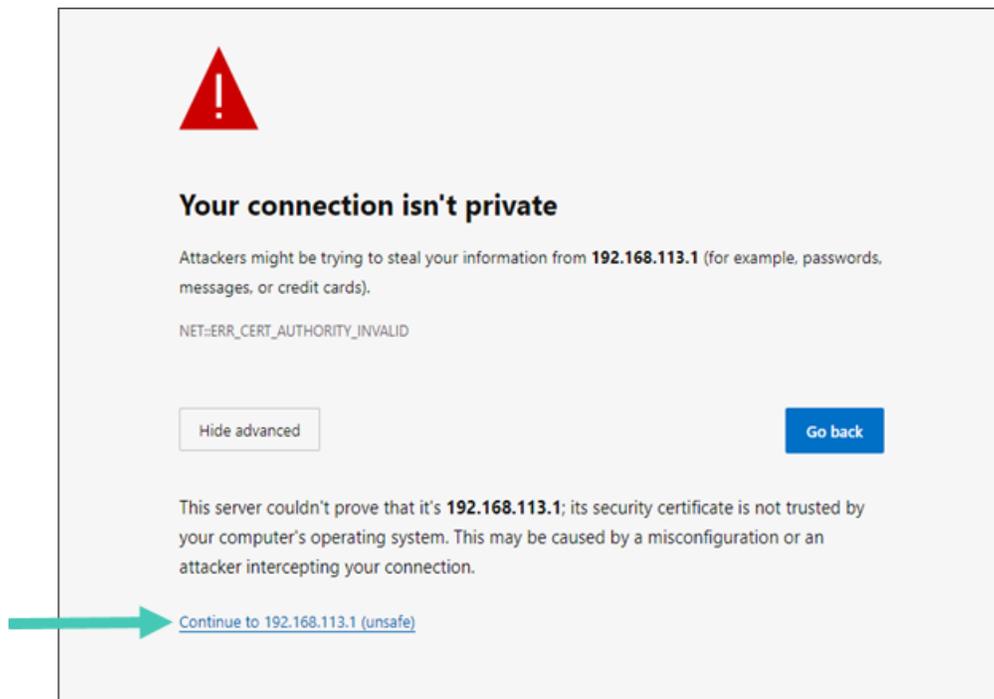


Figure 12: Warning message – Continue to IP address

9. The MegaFi's Mission Control GUI login page will now be displayed.
 - 9a. Enter the password as found on the bottom label of the MegaFi on the Mission Control login page.
- **Note:** username always defaults to 'admin'.
- 9b. Click '**Login**' to proceed.

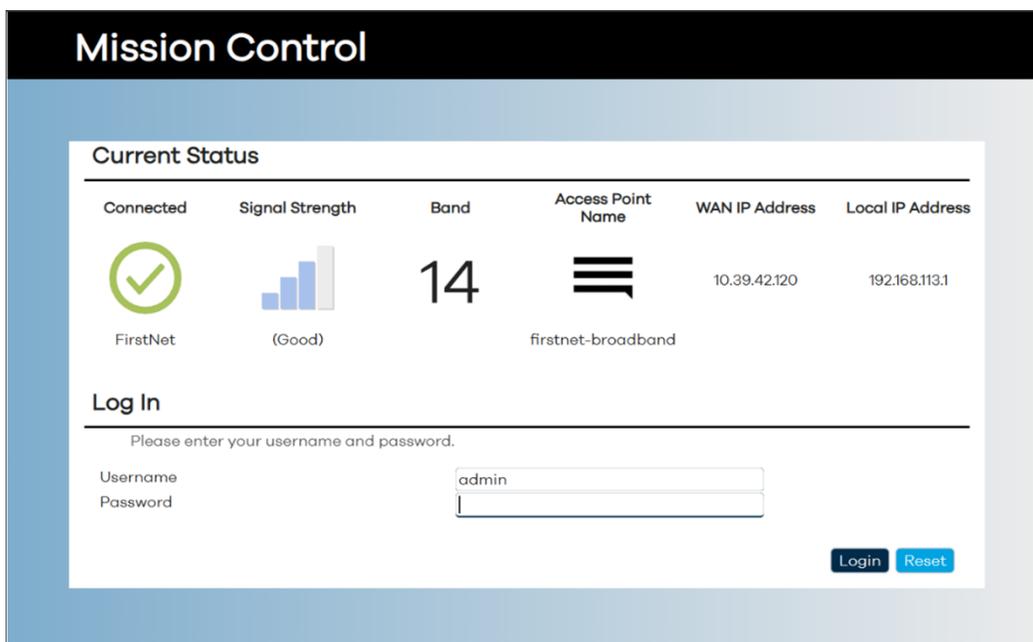


Figure 13: Mission Control – Login page

10. When logging in for the first time, the EULA (End User License Agreement) will be displayed.
 - 10a. Fill out the requested information and click '**Accept**' to continue.

End User Licence Agreement

Nextivity Inc. ("Nextivity")
End User License Agreement ("EULA")

Version Date: July 25, 2023

BY ACCEPTING THIS EULA, EITHER BY INDICATING YOUR ACCEPTANCE, BY EXECUTING A QUOTE OR ORDERING EQUIPMENT OR SERVICES DIRECTLY WITH US OR THROUGH AN APPROVED NEXTIVITY DISTRIBUTOR OR RESELLER (HOWEVER TITLED, REFERRED TO HEREIN AS AN "ORDER"), OR BY DOWNLOADING, INSTALLING AND/OR UTILIZING ANY OF THE SERVICES (DEFINED BELOW), YOU AGREE TO THE TERMS AND CONDITIONS OF THIS EULA. THIS EULA IS A LEGALLY BINDING CONTRACT BETWEEN YOU AND NEXTIVITY AND SETS FORTH THE TERMS THAT GOVERN THE LICENSES PROVIDED TO YOU HEREUNDER. IF YOU ARE ENTERING INTO THIS EULA ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THIS EULA. ANY CHANGES, ADDITIONS OR DELETIONS BY YOU TO THIS EULA WILL NOT BE ACCEPTED AND WILL NOT BE A PART OF THIS EULA. IF YOU DO NOT AGREE TO THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SERVICES.

This Nextivity End User License Agreement ("EULA") is between Nextivity (or "we" or "us") and the user ("User" or "You" or "Your") of the Services, as defined below. This EULA applies to Your use of:

- (1) the Nextivity equipment ("Equipment");
- (2) the Nextivity on-premises, installed software that initialize and enables the Equipment ("Installed Software");
- (3) the Nextivity cloud-based software that allows You to manage and configure Your Equipment ("Cloud Software");
- (4) the written and visual materials Nextivity may provide to aid You in Your use of the Equipment, Installed Software and Cloud Software ("Documentation"); and
- (5) any training or support services performed, either remotely or in person, by Nextivity ("Support"). The Installed Software and Cloud Software may be referred to together as the "Software." The Software, Equipment, Documentation and Support may be referred to collectively as the "Services." This EULA also incorporates any Equipment-specific terms that may apply to the Equipment You acquire ("Supplemental Terms").

Section 1. Using the Services

1.1 License and Right to Use. Nextivity grants You a non-exclusive, non-transferable, non-sublicensable, revocable (a) license to use the Installed Software; (b) right to use the Cloud Software; and (c) right to use the Documentation solely in connection with Your use of the Software and Equipment, each as acquired from Nextivity or an approved reseller or distributor of Nextivity ("Approved Provider"), solely for Your internal business purposes during the Usage Term (as defined in Section 1.6 below), subject to the terms of this EULA and the applicable Order (collectively, the "Usage Rights"). Nextivity reserves all rights, title, and interest in and to the Services, including all related intellectual property rights, subject to the limited rights expressly granted hereunder.

First Name

Last Name

Company (optional)

Phone (optional)

E-Mail

Figure 14: Nextivity, Inc. End-User License Agreement (EULA)

11. Also, part of first-time login to MegaFi, the user will be required to change the default login password.

11a. Proceed to change the default password to a strong password.

➤ **Note:** The device will not accept weak passwords. Password must meet the following requirements: a minimum length of 10 characters and a randomized complexity of lowercase letters, uppercase letters, and numbers.

12. Confirm the new password change by clicking on 'Save'.

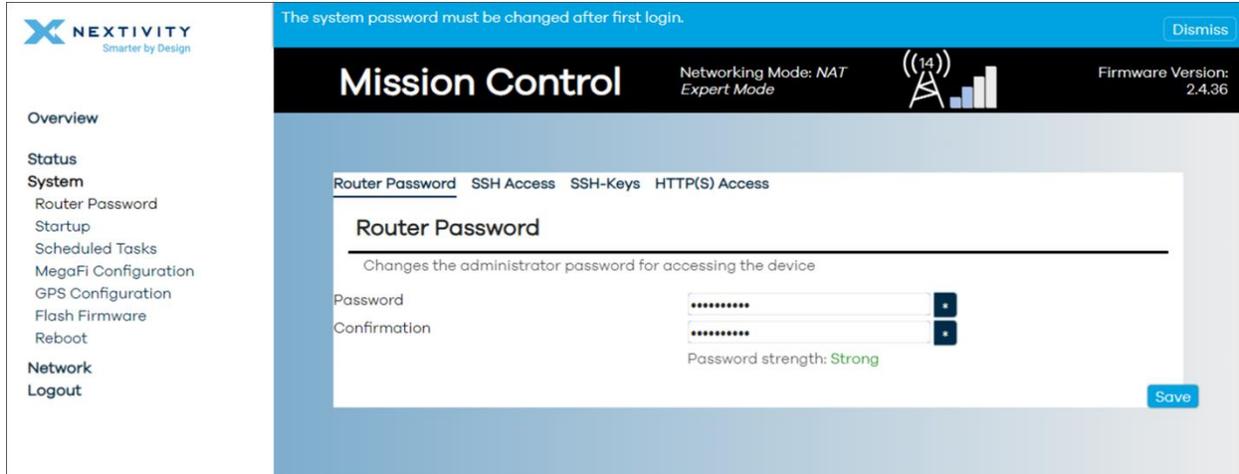


Figure 15: Mission Control – Reset password page

13. The user will now be re-directed to Mission Control’s Overview page.

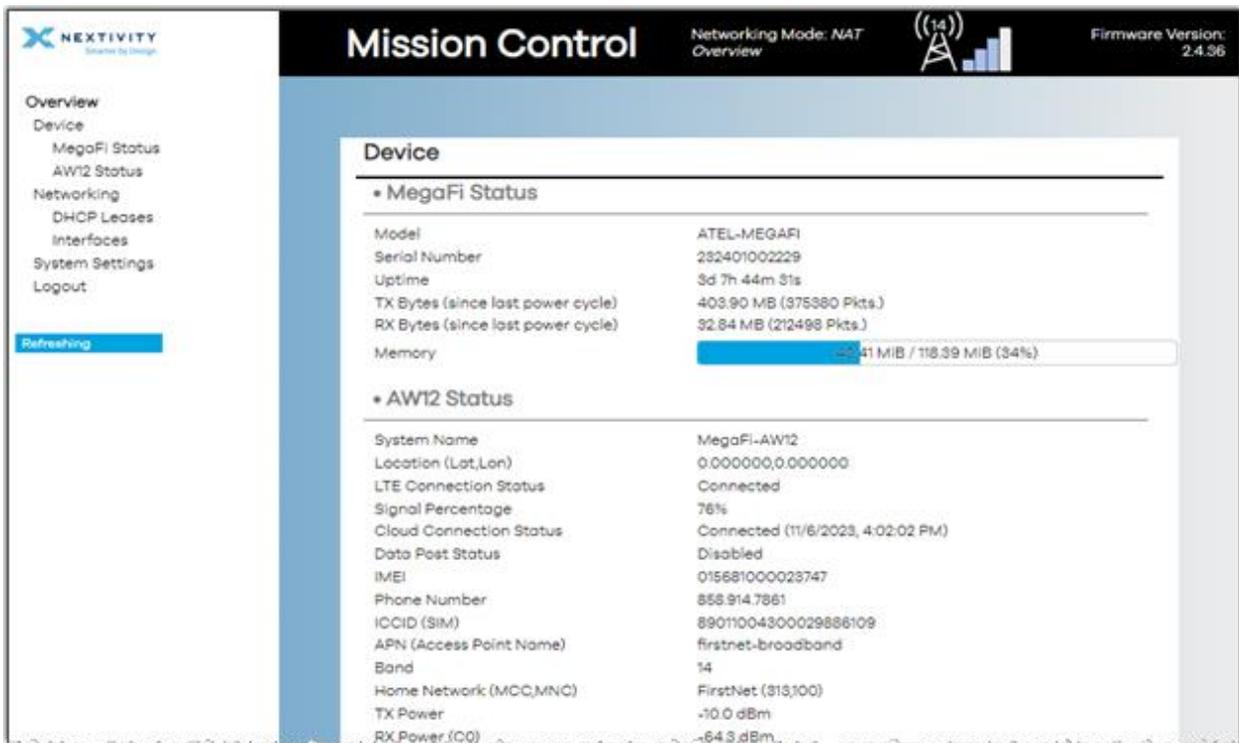


Figure 16: Mission Control – Overview page

14. First-time router configuration is now complete!

2.3 Navigating Mission Control

Once logged in, the first page the user will see is the **Overview > Device** page of Mission Control.

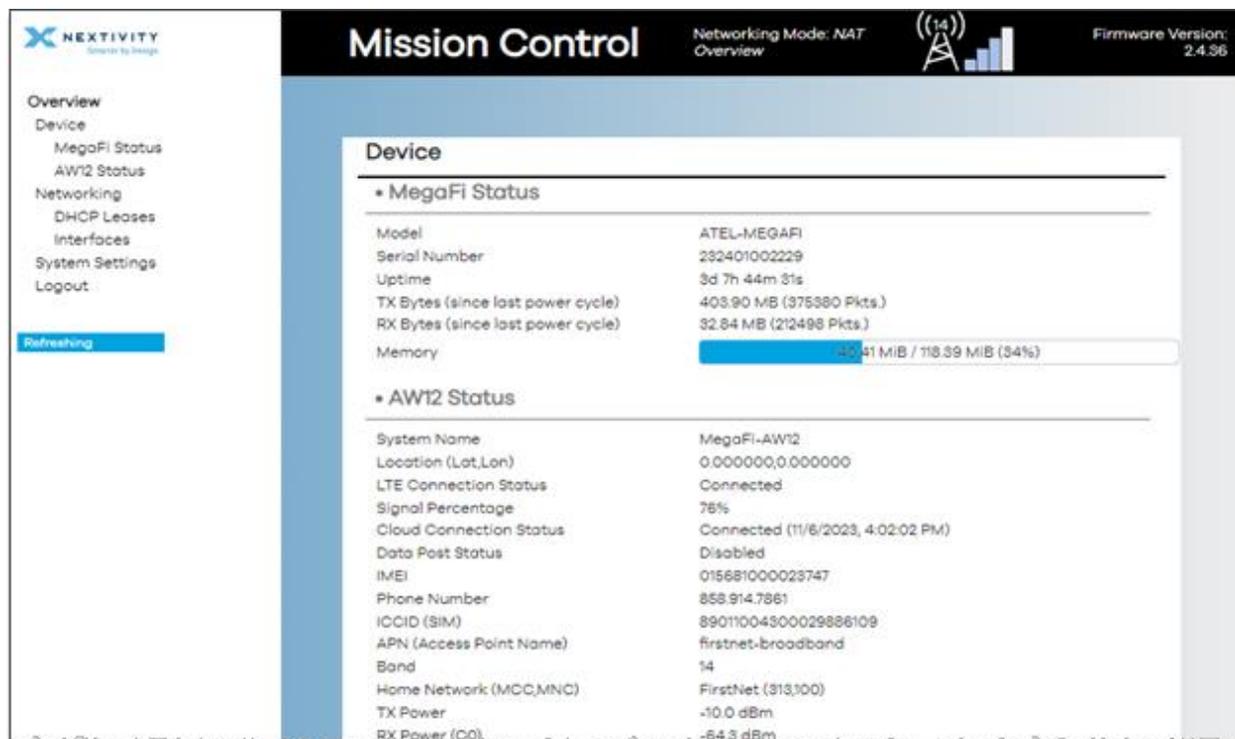


Figure 17: Mission Control – Overview, Device page

2.3.1 Top Banner

The top banner area, which is persistent on every and any page the user navigates to, will show the current information:



Figure 18: Mission Control – top banner

a	<p>Software mode Overview or Expert</p> <ul style="list-style-type: none"> ▪ Overview mode – In this mode, the user can view status pages, logs, and do certain operations such as upgrading the firmware, change APN, reboot, etc. ▪ Expert mode – In this mode, the user can configure more advanced settings such as: Scheduled tasks, interfaces, firewall, etc.
b	<p>Networking Mode</p> <ul style="list-style-type: none"> ▪ NAT (default) or Passthrough ▪ Passthrough replaced Bridge mode in firmware version 2.4.44
c	<p>Band</p> <p>The band shows what band the system is currently operating on. Megafi operates on the best band available on the network. In remote areas at the edge of the network, Megafi typically operates on band 14 in High Power mode.</p>
d	<p>Signal Strength</p> <p>In bars that should match up with the Signal Strength LED bars on top of the device</p>
e	<p>Firmware Version</p> <p>Current running firmware version</p>

2.3.2 Navigation Pane

The navigation pane on the left consists of a 2-level menu system:

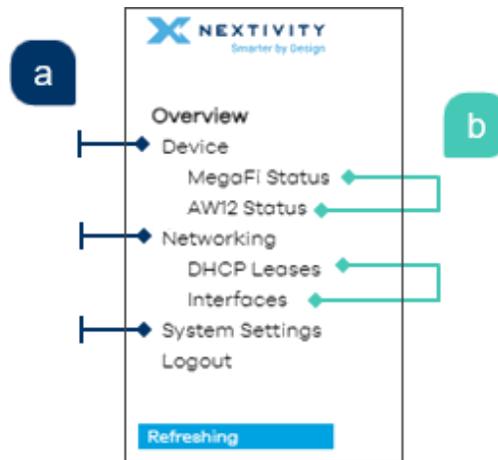


Figure 19: Mission Control Navigation Pane – menus

- a:** Top-level main menu section consists of 4 topics: **Device**, **Networking**, **System Settings**, and **Logout**.
- b:** Second-level sub-menu contains a variable number of on-page quick links.

For example, Figure 19 shows the top-level **Device (a)** menu item with its second-level sub menu items of **MegaFi Status** and **AW12 Status (b)**. Where MegaFi Status reflects router status and AW12 Status reflects modem status.

2.4 Working within Mission Control

When working within Mission Control, you will need to perform actions such as edit, save, discard, reset, etc. To both ease this process and to ensure efficiency of workflow, changes made are stored as **unapplied changes** rather than being actioned and implemented immediately. In doing so, if your workflow is interrupted or if you inadvertently navigate away from a page without applying your changes, any work done to date is not discarded and accidentally lost.

Subsequently, when you are ready to apply these unapplied changes, they can either be saved & applied, reset/discarded, or revert/cancelled in one stroke rather than piecemeal, one-at-a-time. This process also lets you check, verify, and manage the list of queued changes prior to updating the system and, depending on the changes required, where updates take time, avoids slowing your workflow.

2.4.1 Save Options

Within Mission Control, all changes and saves must be applied manually—there is no automatic save or apply options. Typically, there are 3 save options: **Save**, **Save & Apply**, and **Apply Unchecked**; plus, non-save options such as **Reset**, **Dismiss**, **Revert**, etc.

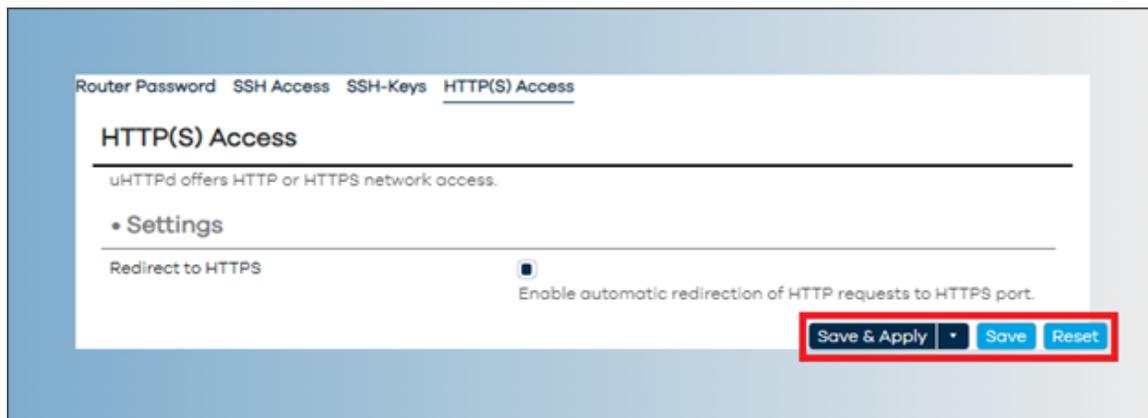


Figure 20: Mission Control – Save options

The action buttons you see will depend on where you are in the system and what changes you have made. We will look at these in more detail, below, starting with **Save**.

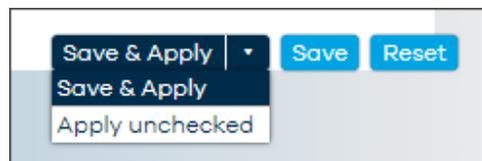


Figure 21: Mission Control – Save options

2.4.2 Save

Though the **Overview** page presents most of the basic admin functionality in a single scrolling page, you may need to navigate between, and make changes to, multiple pages within Mission Control itself. The **Save** button allows you to save your changes as you go. In contrast, without this save option, if you navigated away from a page without saving your changes, these would then be discarded and lost, and current applied settings and values would remain unchanged. However, it is important to note that saving changes *does not* apply/commit them to the system, i.e., no updates occur at this stage.

Instead, saving any changes adds them as pending to the Unapplied Changes list as shown below.



Figure 22: Navigation pane showing pending changes

Once saved as **Unapplied Changes**, you can then:

- carry out additional work on the current page or navigate away to a different page and continue your tasks until you are ready to apply all changes
- manage your unapplied changes
- save and apply your unapplied changes

2.4.3 Managing Unapplied Changes

To view or manage your unapplied changes:

1. Click on the **Unapplied Changes** button and the **Configuration/Changes** dialog will show, listing all queued changes as shown below. Also, the status of each item is determined by its color and as per the legend.
 2. From here, you have several buttons: **Close**, **Save & Apply** (Apply unchecked is in the drop-down menu), and **Revert** or **Reset**.
 - 2a. **Close** – will close this dialog window.
 - 2b. **Save & Apply** – will apply the changes, clear the Configuration/Changes list, close the dialog window, and you will then see the Apply configuration changes countdown popup.
- ⇒ **Note:** Unlike performing a '**Save & Apply**' from the main dashboard, because these items have already been saved once (the initial save added them to the unapplied changes queue), no second click is required to initiate these changes. A single click on the **Save & Apply** button will commit all changes and the countdown will commence.
- 2c. **Revert/Reset** – will cancel all unapplied changes, clear this list, display the changes have been reverted popup, and then take you back to the Mission Control dashboard where all settings remain unchanged.

2.4.4 Save & Apply

When you are ready to apply your unapplied changes, click on **Save & Apply**. This will then apply all unapplied changes to the system and update your current configuration.

- ✘ **IMPORTANT:** Please allow adequate time for changes to update and ensure continuous power is supplied to the MegaFi during any updates.

2.4.5 Apply Unchecked

When updating certain attributes, such as IP or other addresses/configurations, there is often a time-delay between events, (e.g., a change in the LAN IP that uses DHCP) so there may be a delay between connecting to the new IP and subsequent assignment of new DHCP addresses. In such cases, the system will attempt to check that both communication and function is maintained. However, if during this check, the system determines that either would be lost because of the change, it would trigger the “Configuration has been rolled back!” alert. **Apply unchecked** allows us to avert this by applying pending changes without performing communication and function checks.

1. Click on the **Save & Apply** button arrow and the popup, as shown below, will open:
2. Click on **Apply unchecked** and the dropdown will close, the button label will change to **Apply unchecked**, and the button color will change to **red** as shown below.
3. A second click, on the now **Apply unchecked** button, will apply the changes and the Applying configuration changes countdown will initiate:

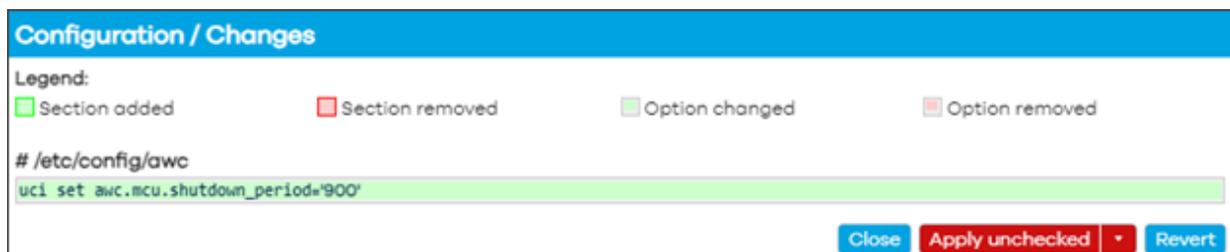


Figure 23: Configuration/Changes showing applied configuration changes

2.4.5.1 Cancelling Apply Unchecked

To cancel the Apply unchecked button (and revert to the default Save & Apply):

1. Click on the arrow on the **Apply unchecked** button to display the popup as shown above.
2. Click on **Save & Apply**. The button’s label will revert to **Save & Apply**, and the button’s color will change to blue.

2.4.6 Reset or Revert

Clicking on **Reset** or **Revert** will cancel all unapplied changes, clear this list, return on-page settings to their current values, and leave the current settings and configuration in their present state.

2.4.7 Overview Page

As previously pointed out above, the top-level menu, the user can see direct links to **Device**, **Networking**, **System Settings** all listed in the left-hand pane and detailed information and statistics for each of these pages within the main window. The **Logout** button function is also listed at the bottom.

The screenshot shows the Mission Control interface. The top navigation bar includes the Nextivity logo, 'Mission Control' title, 'Networking Mode: NAT', 'Overview' (highlighted in red), a signal strength icon, and 'Firmware Version: 2.4.39'. The left sidebar has a menu with 'Overview' selected, containing 'Device', 'Networking', 'System Settings', and 'Logout'. Under 'Device', 'MegaFi Status' and 'AW12 Status' are listed. A green arrow points from 'MegaFi Status' to the main content area. The main content area displays the 'Device' page with a 'MegaFi Status' section containing a table of device information and a memory usage bar.

+ MegaFi Status	
Model	ATEL-MEGAFI
Serial Number	232401002229
Uptime	2h 36m 25s
TX Bytes (since last power cycle)	90.42 MB (100255 Pkts.)
RX Bytes (since last power cycle)	17.34 MB (79446 Pkts.)
Memory	39.79 MiB / 118.39 MiB (33%)

Figure 24: Mission Control – Overview page

The user may need to scroll down the main window to see all that is presented in each page under **Overview**. Each of these pages are detailed below.

2.4.7.1 Device Page

For a detailed summary of the device, this section shows **MegaFi Status**, including the modem's **AW12 Status**, GPS, SIM, cellular network information and other statistics.

The screenshot shows the 'Mission Control' interface. At the top, it displays 'Networking Mode: NAT Overview' and 'Firmware Version: 2.4.38'. The main content area is titled 'Device' and contains two sections: 'MegaFi Status' and 'AW12 Status'.

MegaFi Status

Model	ATEL-MEGAFI
Serial Number	282401002229
Uptime	20h 25m 46s
TX Bytes (since last power cycle)	466.84 MB (447069 Pkts.)
RX Bytes (since last power cycle)	54.72 MB (235754 Pkts.)
Memory	36.72 MIB / 118.39 MIB (31%)

AW12 Status

System Name	MegaFi-AW12
Location (Lat,Lon)	0.000000,0.000000
LTE Connection Status	Connected
Signal Percentage	84%
Cloud Connection Status	Connected (11/9/2023, 10:55:53 AM)
Data Post Status	Disabled
IMEI	015681000023747
Phone Number	858.914.7861
ICCID (SIM)	89011004300029886109
APN (Access Point Name)	firstnet-broadband
Band	14
Home Network (MCC,MNC)	FirstNet (313,100)
TX Power	14.0 dBm
RX Power (C0)	-62.4 dBm
RX Power (C1)	-63.1 dBm
CID (Serving Cell ID)	79474863
PCI (Physical Cell ID)	388
RSRQ (Reference Signal Received Quality)	-10 dB
RSRP (Reference Signal Received Power)	-90 dBm
RSSI (Received Signal Strength Indicator)	-61 dBm
SNR (Signal to Noise Ratio)	14.0 dB

Figure 25: Mission Control – Device page

2.4.7.2 Networking Page

Clicking on **Networking** on the left-hand menu, the main window displays detailed information for **DHCP Leases** for connected hosts and **Interfaces**: LAN, WAN, WWAN, and Active Connections.

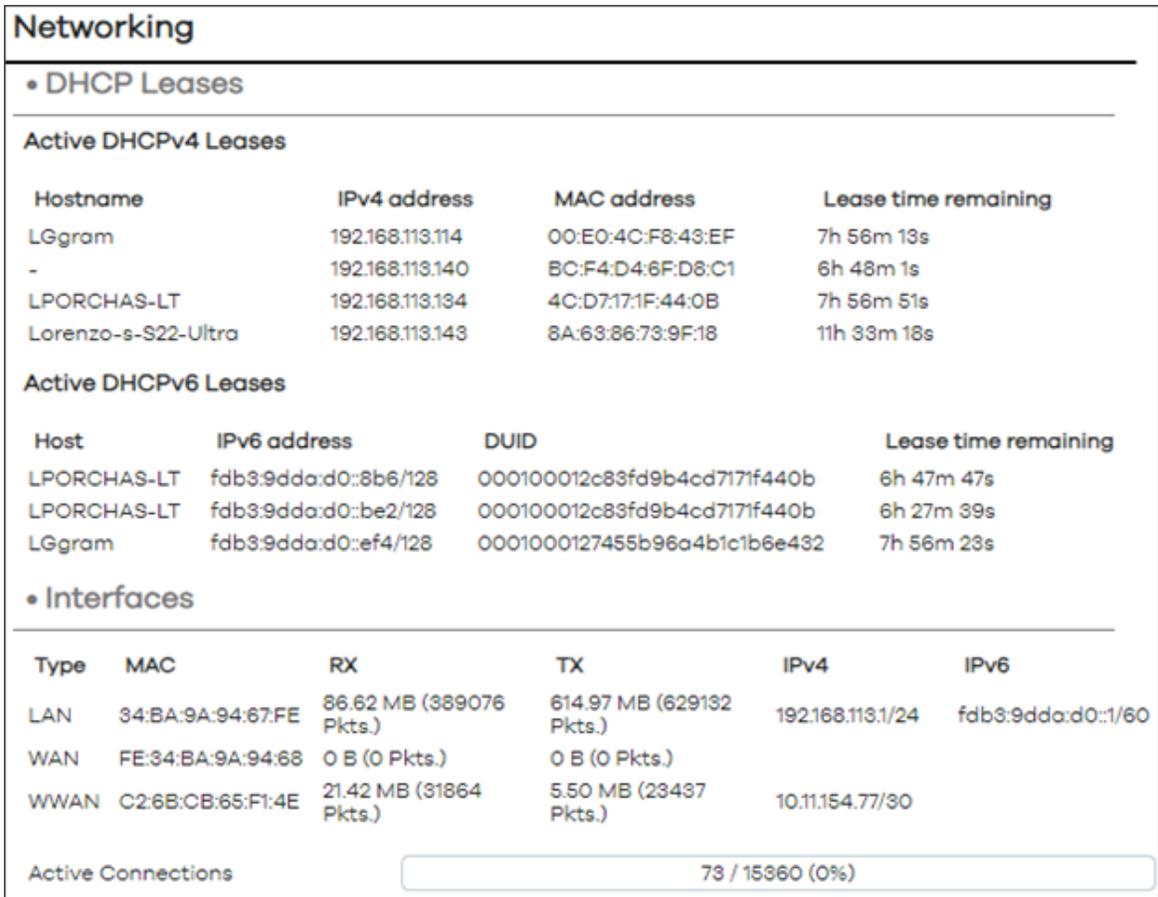


Figure 26: Mission Control – Networking page

2.4.7.3 System Settings Page

Clicking on **System Settings** on the left-hand menu, the main window display's Admin Tools for **APN (Access Point Name), LAN IP, Cycle LAN upon WWAN IP change, Report to Cloud, Automatically Update Firmware, Automatically Update Configuration, Update Firmware, Backup Existing Configuration, Load Configuration from File, Change Password, Factory Defaults, Vehicle Shutdown Delay, Expert Configuration, and Reboot**. The user has complete access to all these configuration features from this environment without the need of being in **Expert mode**.

Further details on how to use these settings will be discussed later in this document.

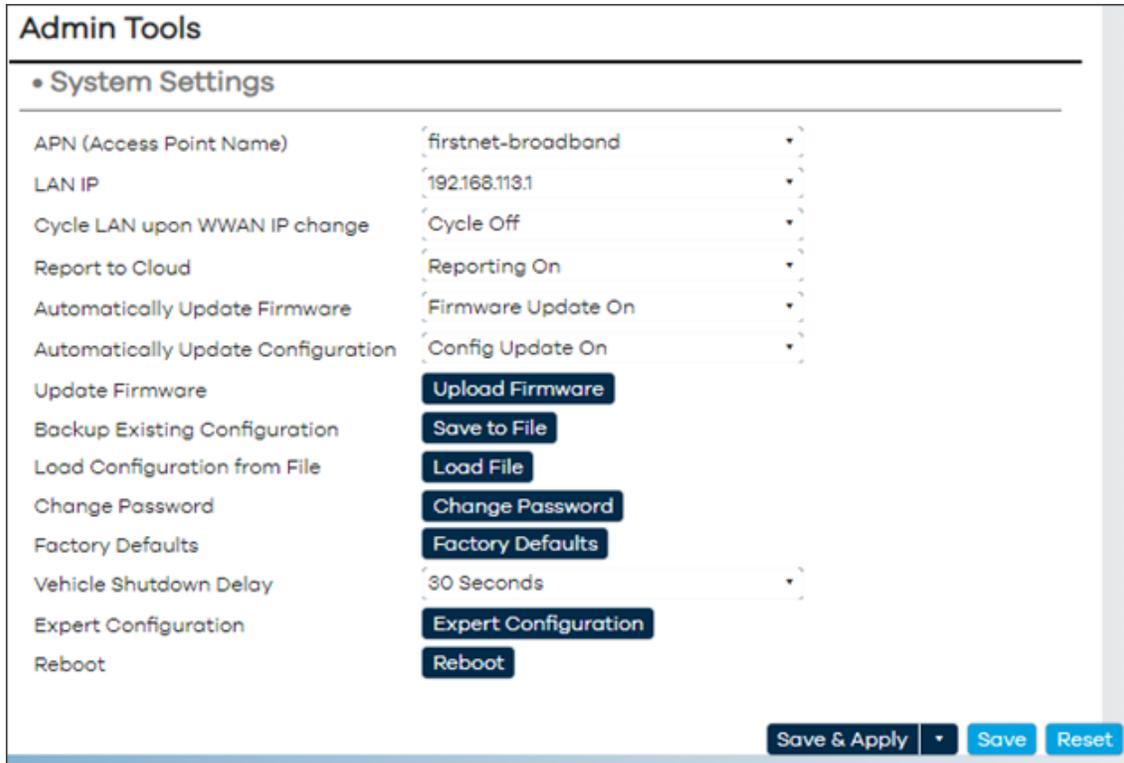


Figure 27: Mission Control – System Settings page

2.4.7.4 Logout

The user can log out of Mission Control by clicking on this button. This button is always visible in either Overview or Expert Mode on the left-hand pane towards the bottom.

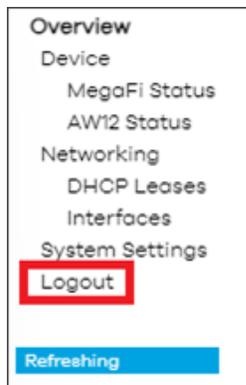


Figure 28: Logout from Overview mode



Figure 29: Logout from Expert mode

3 | Basic Configuration Settings

This section details the most frequent configuration settings that typical users need to make.

3.1 Changing APN (Access Point Name).....	32
3.2 Changing LAN IP Address.....	32
3.3 Flash/Update Firmware	33
3.4 Backup Existing Configuration	37
3.5 Load Configuration from File.....	38
3.6 Change Password	40
3.7 Factory Defaults via Mission Control.....	42
3.8 Vehicle Shutdown Delay.....	44
3.9 Reboot	45
3.10 Wi-Fi Settings.....	47
3.11 NAT vs. Passthrough Mode.....	50
3.12 Band Lock	55
3.13 SSH Access	57
3.14 GPS Output	60

3.1 Changing APN (Access Point Name)

By default, the APN (Access Point Name) is set to **firstnet-broadband**. If the user has a custom APN, do the following to make the change.

1. Navigate to **Overview > System Settings**
2. In the **APN (Access Point Name)** field, click on the drop-down arrow and choose custom.



Figure 30: System Settings – APN (Access Point Name)

3. Enter the custom APN in the field and hit **'Enter'**, otherwise it will revert back to its default setting or pre-configured APN.
4. Click on **Save & Apply** to confirm the change.
5. Give the device a few minutes for it to successfully regain network connectivity.
6. After the device becomes available, issue a **Reboot** so the device receives the correct IP address. See Section 3.9 for Reboot procedure.
7. Refer to *Networking page (Section 2.4.7.2)* and verify correct IPv4 address for WWAN or WAN interface.

3.2 Changing LAN IP Address

By default, the LAN IP address is set to 192.168.113.1. If the user needs to configure this setting to fit their network environment, do the following to make the change.

1. Navigate to **Overview > System Settings**.
2. In the **LAN IP** field, click on the drop-down arrow and choose custom.



Figure 31: System Settings – Changing LAN IP Address

3. Enter the new IP address in the field and hit '**Enter**', otherwise it will revert back to its default setting or pre-configured IP address.
 4. Click on **Save & Apply** to confirm change.
 5. Give the device a few minutes for it to successfully regain network connectivity, and before attempting to reconnect to MegaFi via Mission Control or SSH.
- ⇒ **Note:** In this environment, the system automatically sets a /24 or Class C network and will provide IP addresses to devices within this range.

3.3 Flash/Update Firmware

The user can either use Mission Control, or MegaPortal (Nextivity's Cloud portal for MegaFi), to update MegaFi's firmware.

To update the firmware via Mission Control (manually), the firmware version-specific **BIN** file needs to be downloaded from Nextivity's Support site at <https://nextivityinc.com/support/> and locate the firmware under the FirstNet HPUE tab. If manually updating the firmware, it is recommended to also download the **SHIELD MegaFi Software Update Guide** and follow the detailed step-by-step instructions in that guide. This document can be found under the same location as the firmware.

Notes:

- ⇒ To update the device using MegaPortal, please refer to the *MegaPortal User Guide*.
- ⇒ For more details on updating the MegaFi via Mission Control, refer to the *MegaFi Software Update Guide* or contact Nextivity support for further assistance.

By default, the device is set to Automatically Update its firmware whenever there is a new version available in the cloud. This feature does not necessarily auto-update the device, but it acknowledges a new update is available and requires some user intervention to do so.

If the user requires an immediate update, do the following to update the device via Mission Control:

- ✓ **Assumption:** User has the firmware (BIN file) loaded on a PC and it is directly connected to a LAN port on the MegaFi.
1. Navigate to **Overview > System Settings**.
 2. Click on the **Upload Firmware** or **Flash image** button.

System Settings

APN (Access Point Name)	firstnet-broadband
LAN IP	192.168.113.1
Cycle LAN upon WWAN IP change	Cycle Off
Report to Cloud	Reporting On
Automatically Update Firmware	Firmware Update On
Automatically Update Configuration	Config Update On
Update Firmware	Upload Firmware
Backup Existing Configuration	Save to File

Figure 32: Firmware update – Upload Firmware button

- On the pop-up **Uploading file...** window, click on **Browse** to locate the firmware file.
- The firmware file should be the BIN type file and depending on the firmware version, around 14 MB:

Name	Date modified	Type	Size
Checksum-MegaFi-v2.4.39	11/20/2023 10:39 AM	SHA256SUM File	1 KB
MegaFi Software Update Guide Nov 2023	11/20/2023 4:01 PM	Adobe Acrobat Document	1,190 KB
Software-MegaFi-v2.4.39.bin	11/20/2023 10:41 AM	BIN File	14,850 KB

Figure 33: Firmware update – Select the upgrade file

- Select the firmware file. The **Uploading file...** window now shows the selected file.

Uploading file...

- Name: Software-MegaFi-v2.4.39.bin
- Size: 14.50 MiB

Browse... Cancel **Upload**

Figure 34: Firmware update – Uploading the selected upgrade file

- Click on **Upload**, the file will begin to upload.

Uploading file...

37.50%

Figure 35: Firmware update – Status of upgrade file upload

7. A new pop-up window **Flash image?** will ask the user to manually verify the checksum **SHA256** value displayed here, with the checksum **SHA256** value displayed next to firmware file from where it was downloaded. Only continue if the values match.
- **Note:** The **SHA256** value is unique to each version. In this example, this is the **SHA256** value for firmware version 2.4.39.



Figure 36: Flash image window – Compare checksum and file size with original

- ! WARNING:** If you accidentally try to upload the wrong file to the MegaFi device, a warning screen will be displayed (see example below). If this happens, **STOP - DO NOT PROCEED**. Select '**Cancel**' to back out of this operation and avoid "bricking" your device.

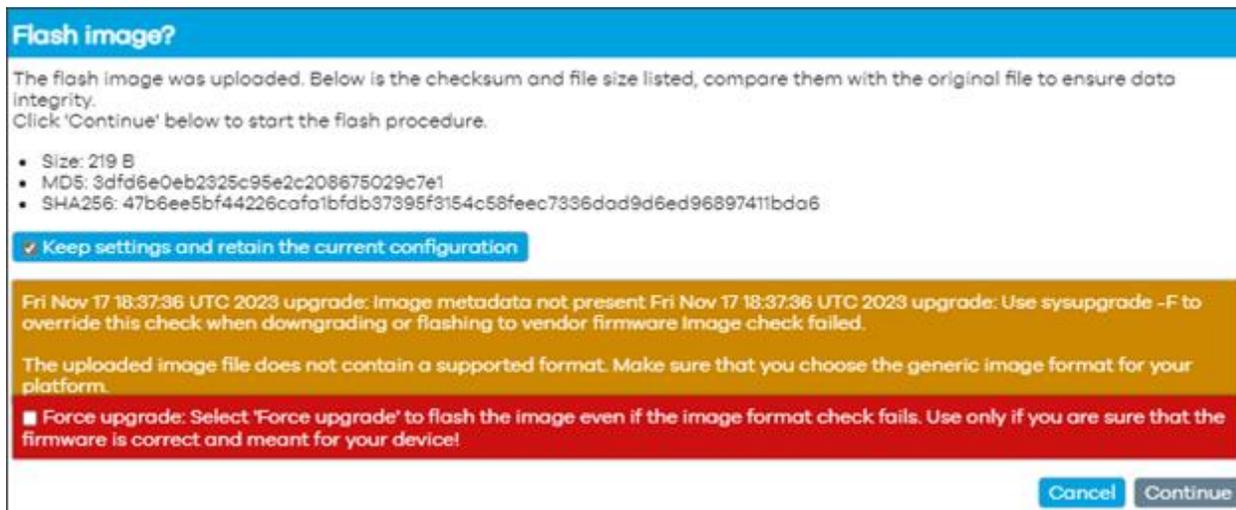


Figure 37: Flash image window – Image format check failure

8. Click on **Continue** on **Flash image?** only after the SHA256 values have been verified to match.
 9. The **Flashing...** window will display.
 - ! WARNING:** "Do not power off the unit until the image flashing is complete."
- **Note:** The update will take between 5 to 15 minutes.

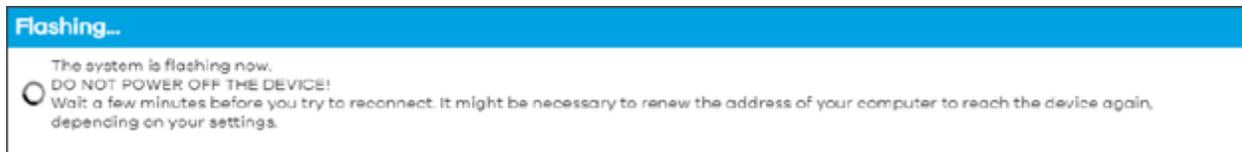


Figure 38: Flashing window – message indicating progress of the system flashing process

10. When the image flash is complete, you will be taken back to the login page.
11. Log in to continue.
 - **Note:** Current status may initially display 'Not Connected' and no 'Signal Strength'. It will correct itself once the device properly boots up from the upgrade process.
 - **Note:** Refresh the browser if the device has not gone back to home screen after 10 minutes.
12. Verify that the intended firmware upgrade successfully loaded by looking at the top right cover of Mission Control. Once verified, firmware update is complete.

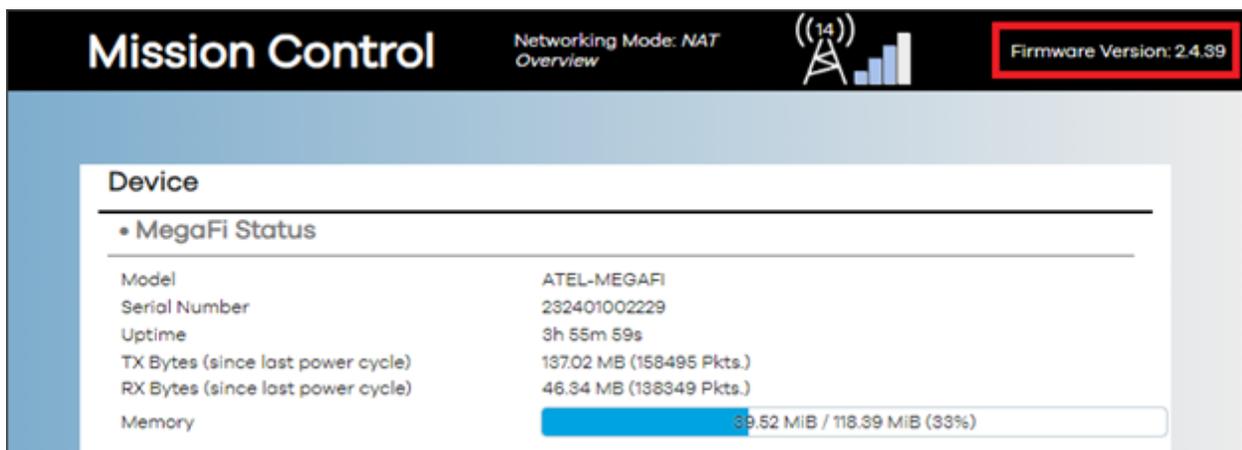


Figure 39: Mission Control page showing Firmware Version

3.4 Backup Existing Configuration

If the user requires to backup an existing configuration, do the following via Mission Control:

1. Navigate to **Overview > System Settings**.
2. Click on the **Save to File** button.

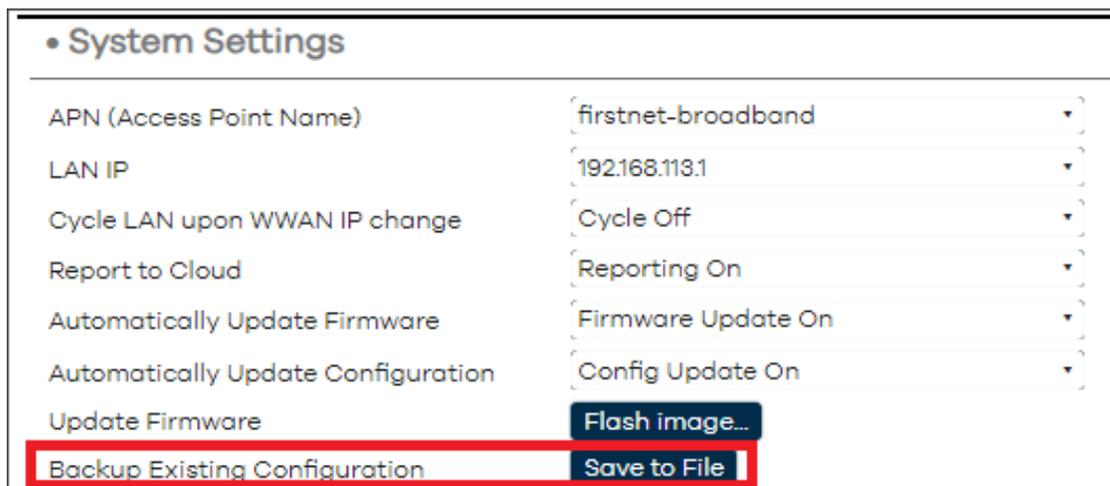


Figure 40: System Settings – Save to File button

3. A tar.gz (tarball) file is created and stored in Downloads. Take note of the date of the file for future reference if needed.

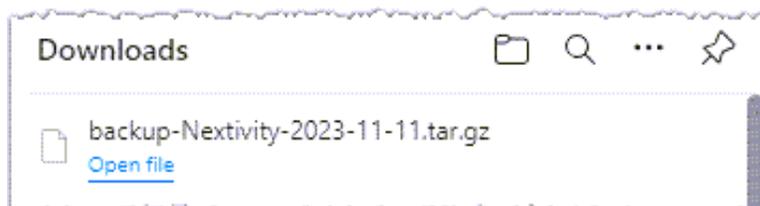


Figure 41: Downloads folder showing downloaded tar.gz file

3.5 Load Configuration from File

If the user requires to load a backup/saved configuration (i.e. duplicate a configuration file onto other MegaFi devices or restore a previous configuration file), do the following via Mission Control:

1. Navigate to **Overview > System Settings**.
2. Click on the **Load File** button, sometimes referred to as **Upload archive...**

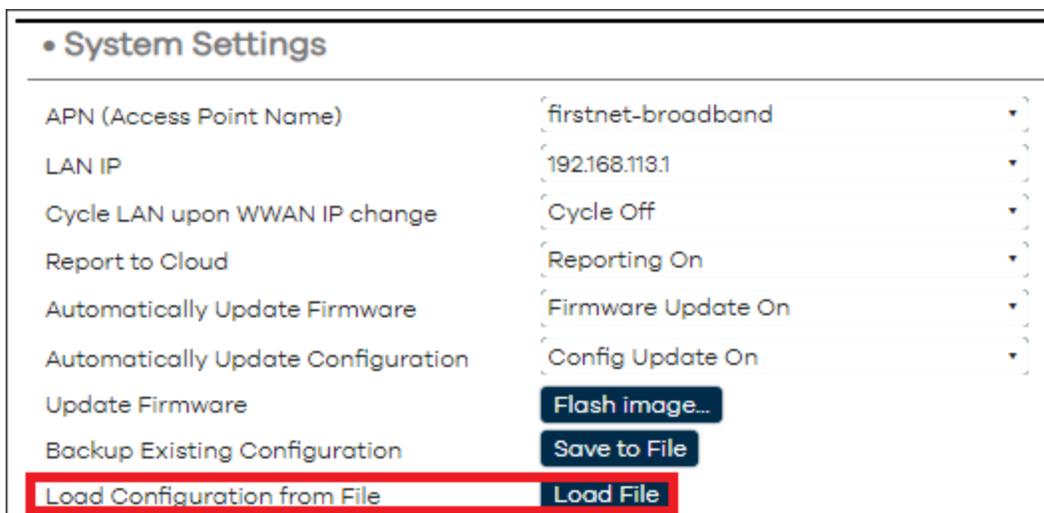


Figure 42: System Settings – Load file button

3. The **Uploading file...** window pop ups, select **Browse** to locate the appropriate tarball file and **Open**.

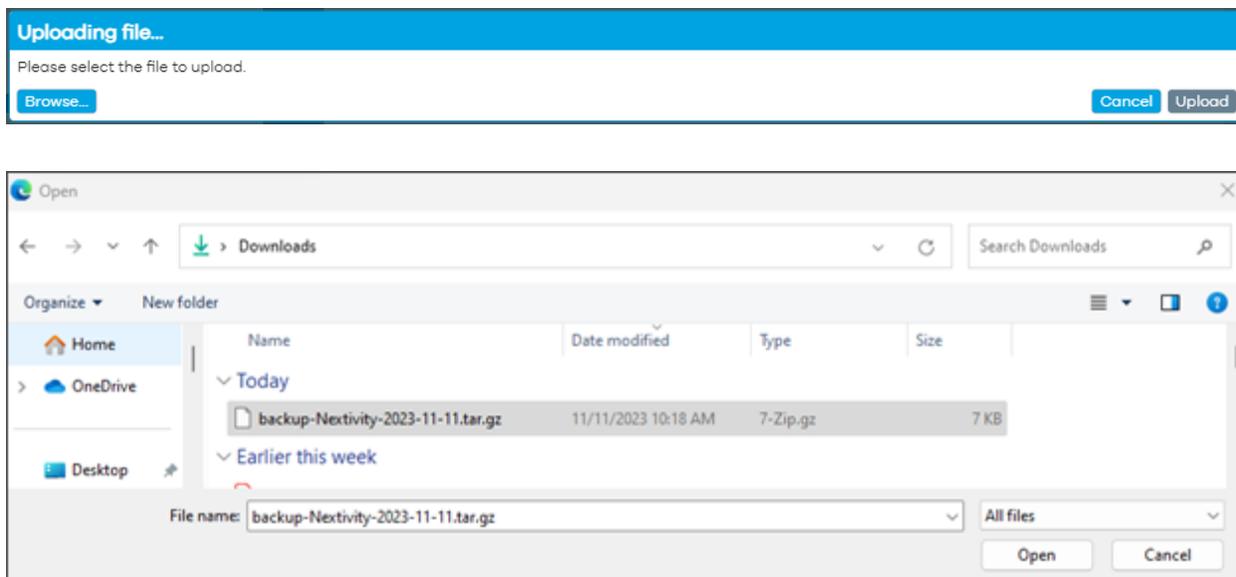


Figure 43: Uploading file and Browse to and select the tarball file

- The **Uploading file...** pop up window shows the file chosen to load. Verify if it is the intended file before selecting **Upload** to continue with loading the file.



Figure 44: Load Configuration from File – Uploading selected file

- In the **Apply backup?** pop up window, press **Continue** at the bottom to proceed with restoring the backup file and reboot. Otherwise, **Cancel** to abort the operation.

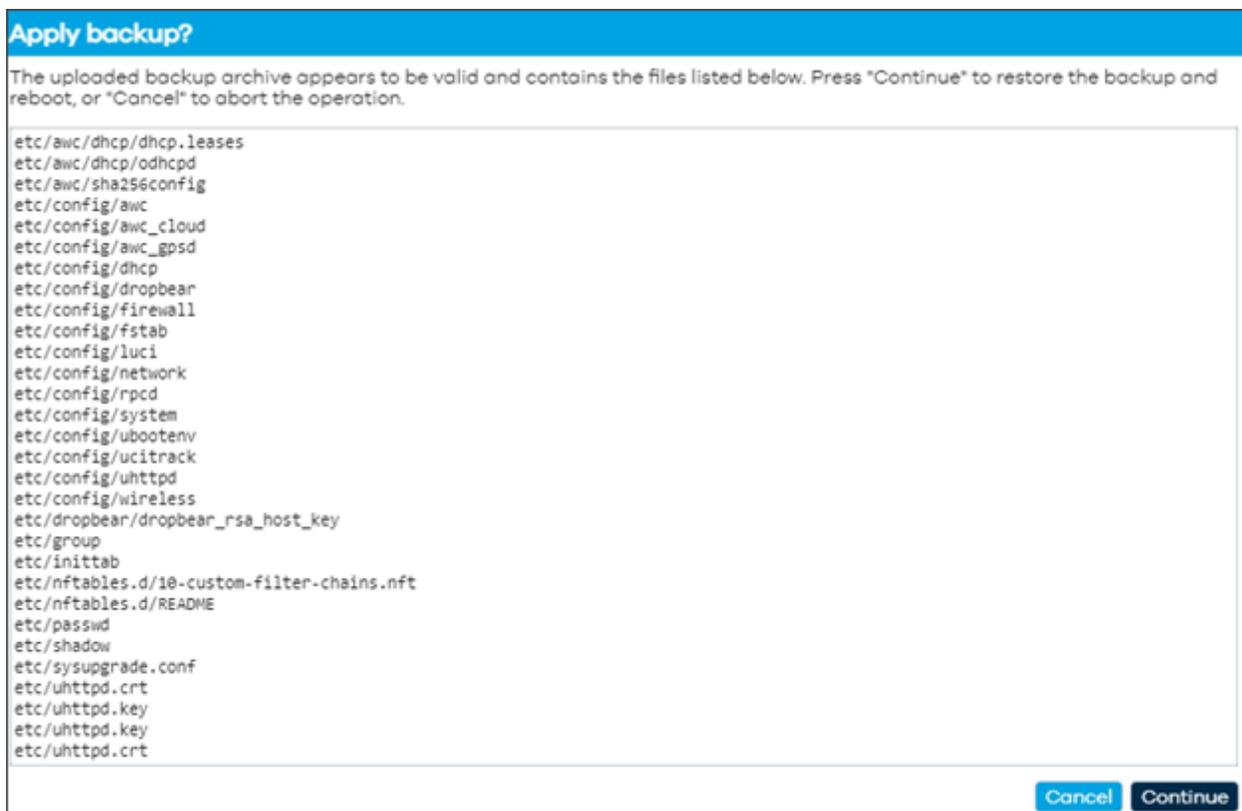


Figure 45: Apply backup – Confirmation to continue

- Give the backup operation 5-15 minutes to finish.

! WARNING: Do not power off the device during this time.

3.6 Change Password

If the user requires to change the current password, do the following via Mission Control:

1. Navigate to **Overview > System Settings**.
2. Click on the **Change Password** button.

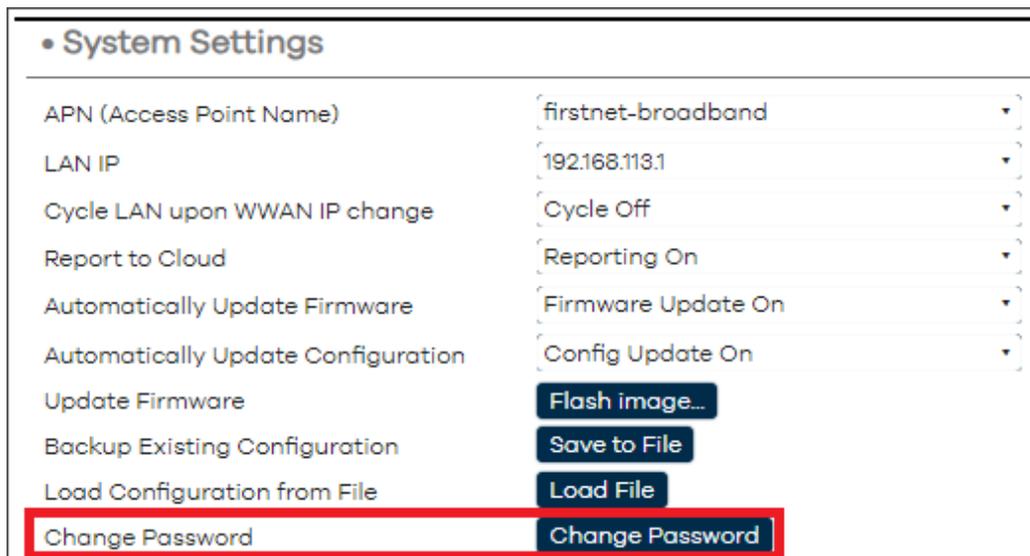


Figure 46: System Settings – Change Password button

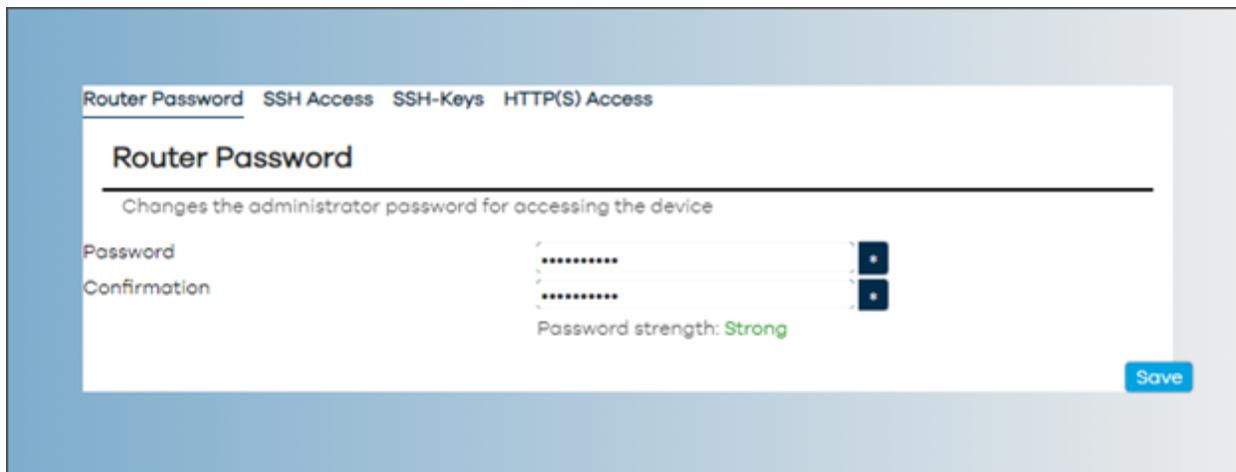
3. The user is automatically put into Expert Mode and taken to the **System > Router Password** page.



Figure 47: Router Password page – Expert Mode

4. Enter a new desired password.

- **Note:** The device will not accept weak passwords. Password must meet the following requirements: a minimum length of 10 characters and a randomized complexity of lowercase letters, uppercase letters, and numbers.



Router Password SSH Access SSH-Keys HTTP(S) Access

Router Password

Changes the administrator password for accessing the device

Password

Confirmation

Password strength: **Strong**

Save

Figure 48: Router Password page – Enter new password

5. Click on the **Save** button.

3.7 Factory Defaults via Mission Control

If the user requires to factory default the MegaFi device, do the following in Mission Control.

- ➔ **Note:** After a factory reset, the MegaFi's UUID must be reassigned for Cloud support. Contact the support team at support@nextivityinc.com for further assistance.

To Factory Reset MegaFi:

1. Navigate to **Overview > System Settings**.
2. Click on the **Factory Defaults** button.

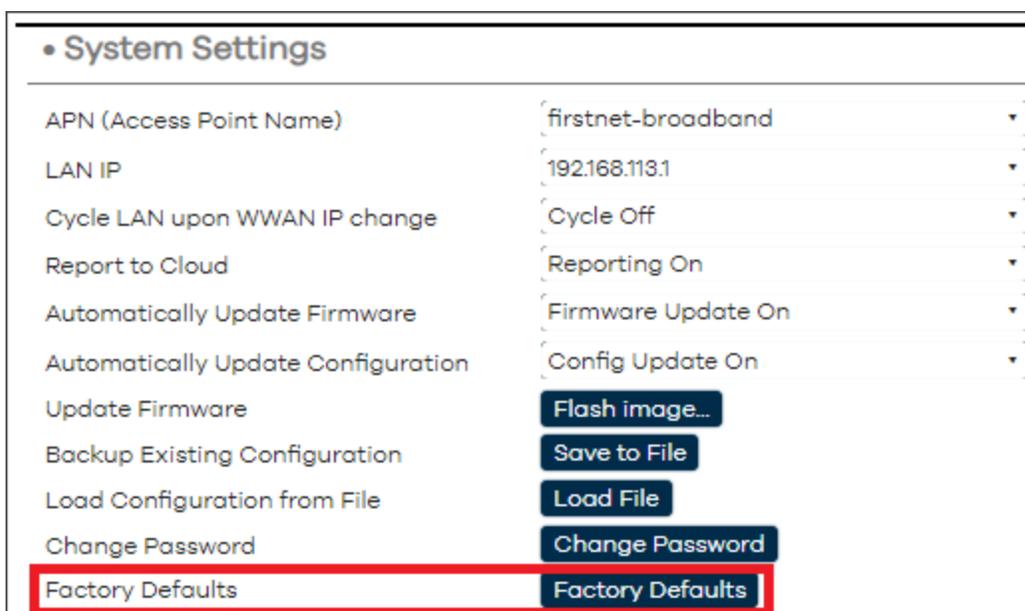


Figure 49: System Settings page – Factory Defaults button

3. A window will pop up and ask the user to confirm the operation. Click **OK** to continue.

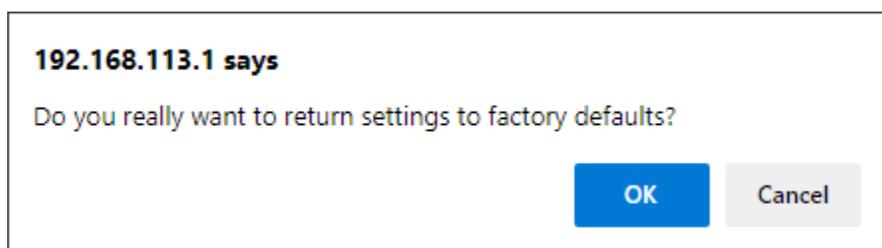


Figure 50: Confirmation to return settings to factory defaults

4. Give the device 5-15 minutes to complete the operation.

5. Once the device recovers, the user will be asked to log in to Mission Control again, using the default password located on the device's label.
 6. The user will then be asked to accept the EULA agreement and change the default password.
- ① For more details on Factory Defaulting the device via Mission Control or for instructions on how to factory default using the reset button on the device (in case of a forgotten password), refer to the *MegaFi User's Guide* for more information.

3.8 Vehicle Shutdown Delay

If the user requires to change the Vehicle Shutdown Delay (default is set to 30 seconds), do the following in Mission Control:

1. Navigate to **Overview > System Settings**.
2. Click the drop-down arrow to expose the other pre-fined settings and select from 15 minutes, 1 Hour, or 2 Hours.

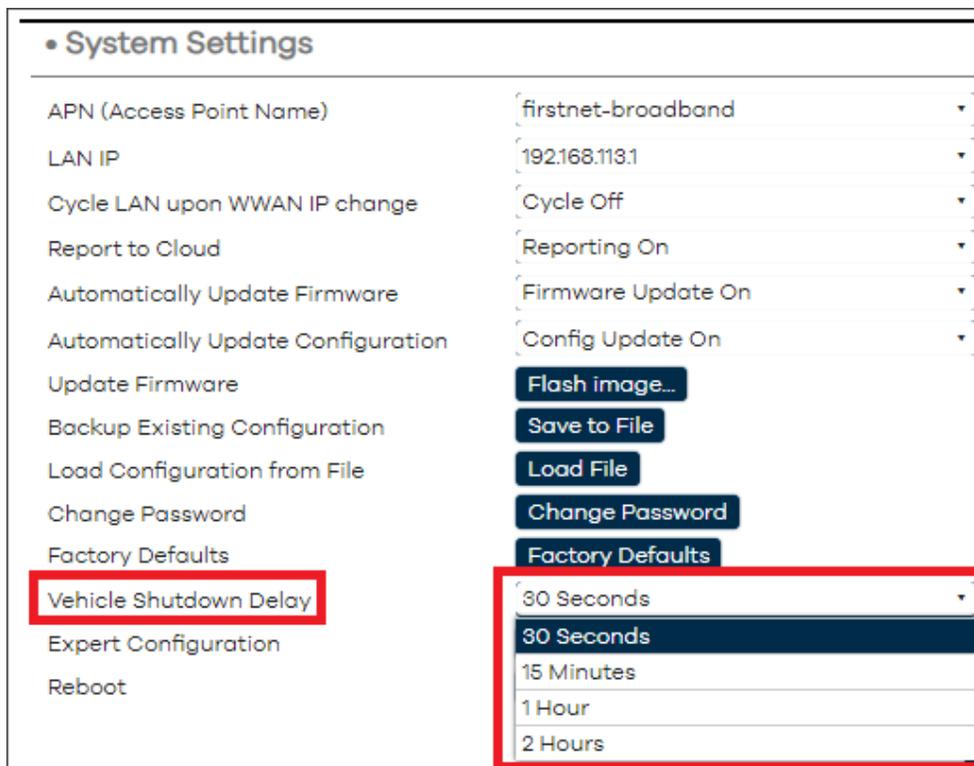


Figure 51: System Settings – Vehicle Shutdown Delay options

3. Click on **Save & Apply** to confirm the new setting.

3.9 Reboot

If the user would like to initiate a reboot of the device, do the following in Mission Control:

1. Navigate to **Overview > System Settings**.
2. Click on the **Reboot** button.

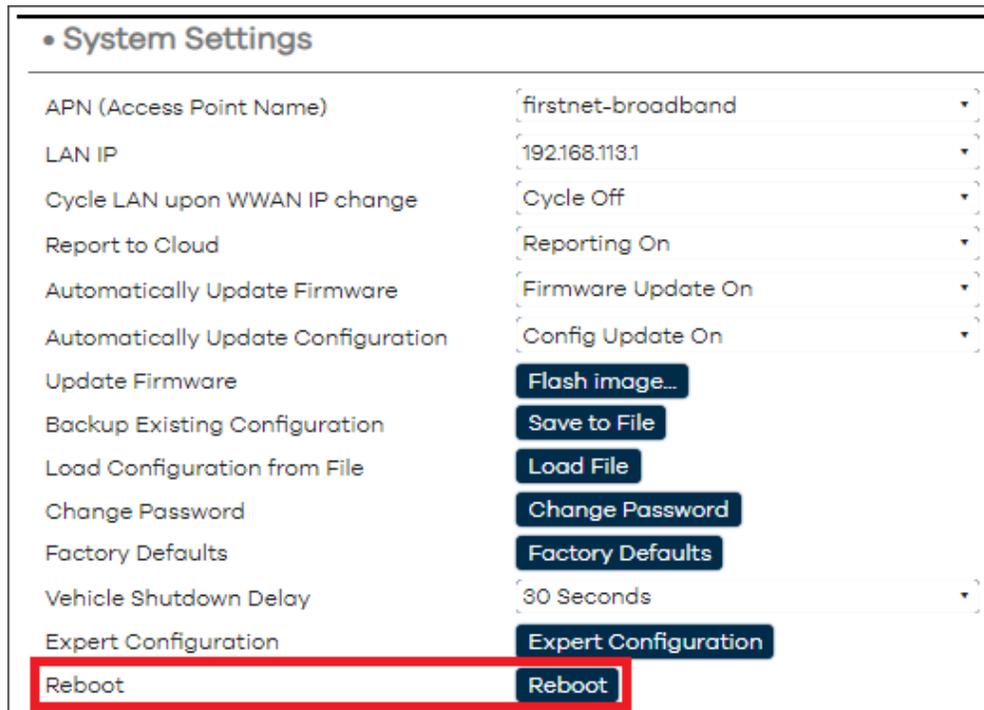


Figure 52: System Settings – Reboot button

3. A pop-up window asks the user to confirm the operation. Click on **OK** to continue.

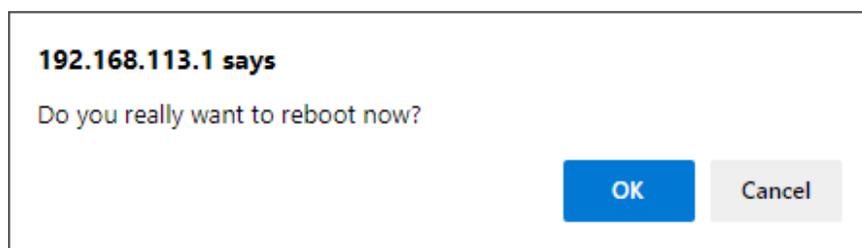


Figure 53: Confirmation message to reboot device

4. Wait for the device to reboot before continuing. The process will take 1 - 5 minutes.



Figure 54: Message indicating device is being rebooted

5. The user will be asked to log in again into Mission Control after the device reboots. Click on the **To login...** button to do so.



Figure 55: Prompt to log in after device reboots

3.10 Wi-Fi Settings

To verify current Wi-Fi settings, do the following in Mission Control:

3.10.1 Verify Wi-Fi Settings

To view current Wi-Fi settings, do the following:

1. Navigate to **Overview > System Settings**.
2. Click on **Expert Configuration** to enter Expert Mode.

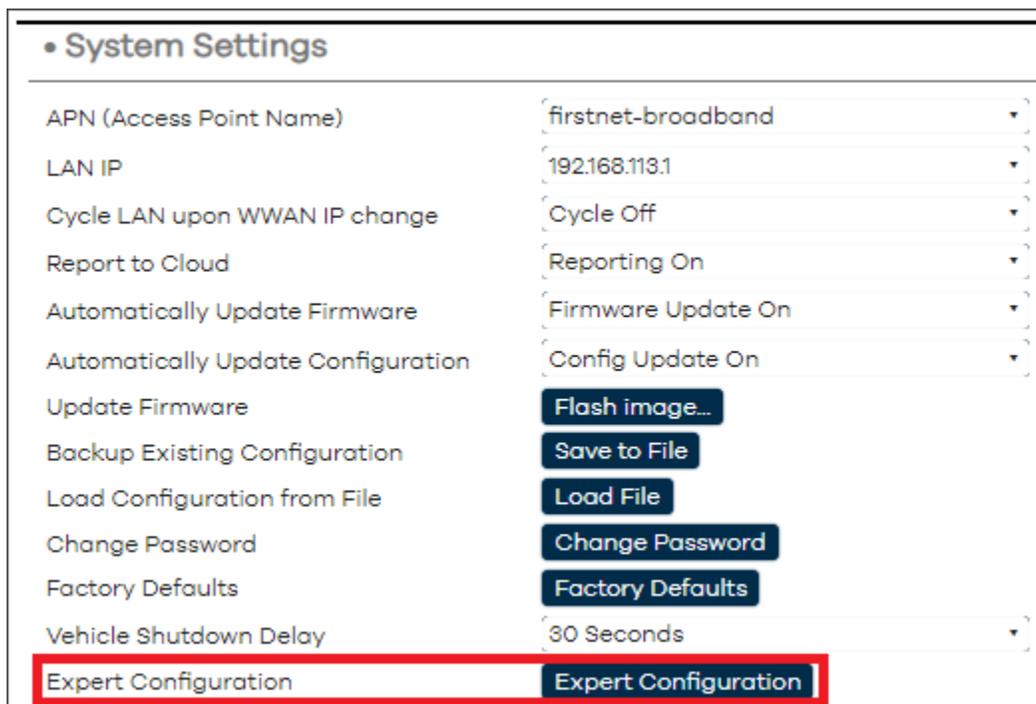


Figure 56: System Settings – Expert Configuration button

3. A pop-up window asks the user to confirm going into Expert Mode. Click **OK** to continue.

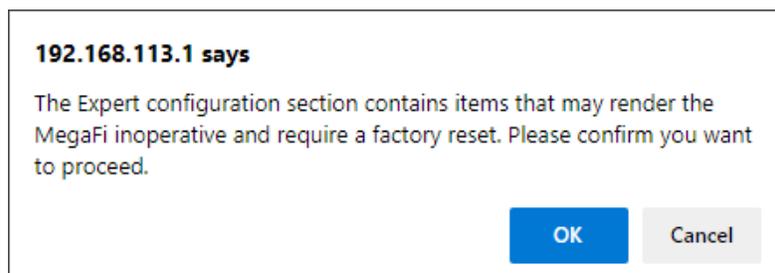


Figure 57: Confirmation message to enter Expert Mode

- The left-pane menu exposes pages only available in Expert Mode. Navigate to **Network > Wireless**.

➤ **Note:** To view the hidden Wi-Fi Key/Password, click on the * (asterisk) button next to the Key field to make it visible for either setting. By default, the key/password is the same for both 2.4 and 5 GHz settings and printed on the label as well.



Figure 58: Mission Control navigation pane showing Expert Mode menu options

- To make any changes in this page, continue to the next section: **Change Wi-Fi- Settings**.

3.10.2 Change Wi-Fi Settings

The following available options for WiFi 2.4GHz and 5 GHz Settings are:

Wi-Fi Setting	WiFi 2.4 GHz Settings (Default)	WiFi 2.4 GHz Settings -Other Options	WiFi 5 GHz Settings (Default)	WiFi 5 GHz Settings -Other Options
Radio Enabled	Enabled	Disabled	Enabled	Disabled
Channel	1 (2412 Mhz)	Auto and Channels 2-11	36 (5180 Mhz)	Auto and Channels 40, 44, 48, 149, 153, 157, 161
Mode	N	Legacy	AC	Legacy, N
SSID	default SSID name on label		default SSID name on label	
Encryption	WPA2-PSK	WPA2-EAP, WPA3-EAP, WPA2-EAP/WPA3-EAP, WPA2-PSK/WPA3-SAE, WPA3-SAE, and Disabled	WPA2-PSK	WPA2-EAP, WPA3-EAP, WPA2-EAP/WPA3-EAP, WPA2-PSK/WPA3-SAE, WPA3-SAE, and Disabled
Key	default key (password) on label		default key (password) on label	

Table 1: Wi-Fi Settings for 2.4 GHz and 5 GHz

1. For settings with a drop-down menu arrow, click the arrow and choose the preferred setting. For **SSID** and **Key** changes, remove/delete the previous setting and enter the new SSID and/or new and appropriate Key (Must be at least 10 characters long) into their respective fields.
2. Click on **Save** followed by **Save & Apply** to confirm the change(s).
3. When changes have been completed, and to prevent any more setting changes, click on the **Logout** button to exit out of Mission Control and be taken back to the Log In page.

3.11 NAT vs. Passthrough Mode

In the NAT or Passthrough Mode configuration section, the device can be put into NAT (default setting) or Passthrough Mode. Passthrough Mode will disable the router capability of the MegaFi without disabling its modem and pass the carrier assigned IP address to the device directly connected behind the MegaFi.

Prior to implementing Passthrough mode, the user needs to do the following steps:

- **Connection to MegaFi Device** – the user will need to connect a computer via ethernet to LAN port 1. The user will also need to make sure the computer is NOT connected to Wi-Fi.
- **Note:** Only LAN port 1 is usable and all other LAN ports are disabled in Passthrough Mode.
- **Implement Custom APN/Static IP first** – Though not always the case, if the user is using a custom APN, the user will need to input the custom APN (Section 3.1), save, and reboot the device to make sure the device receives the correct IP address prior to implementing Passthrough Mode. If the correct IP address does not appear on the device, please review SIM provisioning with the carrier. If the correct IP address does appear, then, the user can implement Passthrough Mode as instructed below.
- **Manually refresh connected computer IP address** – Once in Passthrough Mode, the Mission Control software management interface will briefly be unreachable at <https://192.168.113.1> or whatever IP address it has been configured to until the IP address is manually refreshed. If this occurs, go to Step 8 below for options to try to regain connection to Mission Control.

To change between modes, do the following in Mission Control:

1. Navigate to **Overview > System Settings**.
2. Click on **Expert Configuration** to enter *Expert Mode*.

The screenshot shows the 'System Settings' page with the following items:

APN (Access Point Name)	firstnet-broadband
LAN IP	192.168.113.1
Cycle LAN upon WWAN IP change	Cycle Off
Report to Cloud	Reporting On
Automatically Update Firmware	Firmware Update On
Automatically Update Configuration	Config Update On
Update Firmware	Flash image...
Backup Existing Configuration	Save to File
Load Configuration from File	Load File
Change Password	Change Password
Factory Defaults	Factory Defaults
Vehicle Shutdown Delay	30 Seconds
Expert Configuration	Expert Configuration

Figure 59: System Settings page – Entering Expert mode

3. A pop-up window asks the user to confirm going into Expert Mode. Click **OK** to continue.

The dialog box contains the following text:

192.168.113.1 says

The Expert configuration section contains items that may render the MegaFi inoperative and require a factory reset. Please confirm you want to proceed.

Buttons: **OK** (blue), **Cancel** (grey)

Figure 60: Confirmation message to enter Expert Mode

4. The left-pane menu exposes pages only available in Expert Mode. Navigate to **System > MegaFi Configuration**.



Figure 61: Navigation pane showing options available in Expert Mode

- Under the NAT or Passthrough Mode area, click on the drop-down arrow and select the desired mode: **NAT Mode** (default), or **Passthrough Mode**.

The screenshot shows the MegaFi Configuration page with the following sections:

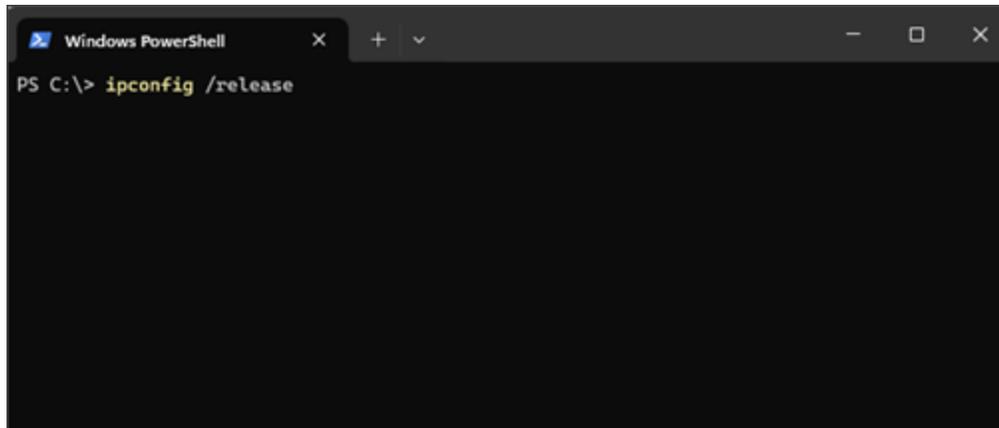
- Cloud**
 - UUID: C9E3F2EC-C84B-421B-B615-0E8EE926F0
 - Cloud Poll URL: ei.awcone.com
 - Cloud Poll Period (seconds): 60
 - Cloud Status URL: [Redacted]
 - Cloud Status: Connected (3/29/2024, 1:18:42 PM)
- MegaFi Logging**
 - Logging Enabled: Logging Enabled
 - Push to Cloud: Push Enabled
 - Push to Cloud Period (seconds): 60
 - System Poll Period (seconds): 15
 - Show in Local UI: Local UI Enabled
- NAT or Passthrough Mode**
 - MegaFi Mode (Changing causes reboot): **NAT Mode**
 - LAN IP Address: [Redacted]
- MegaFi and Modem Configuration**

Figure 62: MegaFi Configuration – Change modes (NAT or Passthrough)

- Click on **Save & Apply** to confirm the change.

! WARNING: Internet access, Wireless connectivity and/or access to the MegaFi will become disrupted or unavailable after changing modes. Please allow 1-5 minutes for the configuration to apply.

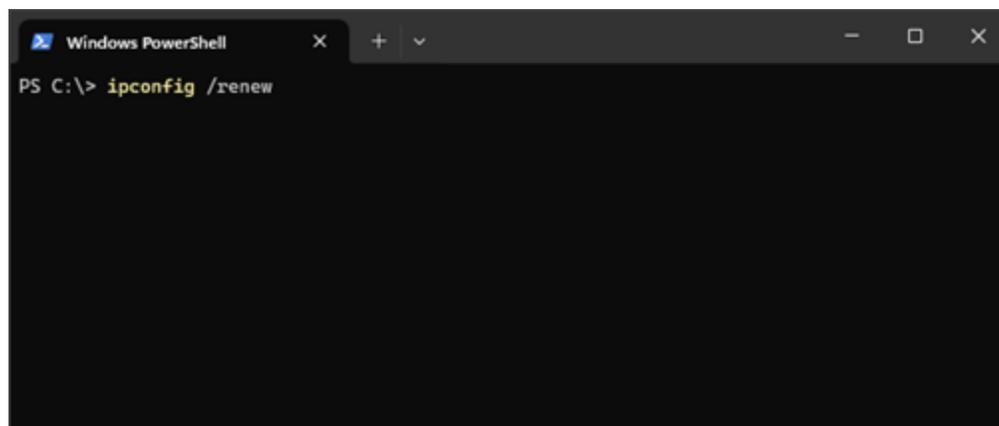
7. It is highly recommended to issue a **Reboot** (Section 3.9) to make sure the new setting takes hold.
8. If connectivity becomes an issue, try one of the following actions to regain access to MegaFi:
 - 8a. Refresh the web browser to Mission Control.
 - 8b. Connect an Ethernet cable to an enabled LAN port (LAN port 1 if in Passthrough) on the MegaFi and re-access Mission Control as usual through a web browser.
 - 8c. Manually refresh connected computer IP address by opening a Windows PowerShell, or Command Prompt window on a PC with local access to MegaFi and enter the following commands at the prompt:
 - **ipconfig /release** <enter> - this will release the existing IP addresses



```
Windows PowerShell
PS C:\> ipconfig /release
```

Figure 63: Windows PowerShell window – `ipconfig /release` <enter>

- **ipconfig /renew** <enter> - this will refresh the IP addresses on the connected computer.



```
Windows PowerShell
PS C:\> ipconfig /renew
```

Figure 64: Windows PowerShell window – `ipconfig /renew` <enter>

9. When changes have been completed, and to prevent any more setting changes, click on the **Logout** button to exit out of Mission Control and be taken back to the Log In page.

3.12 Band Lock

The user may briefly change the Band Lock from **Default Band Configuration** to **LTE B14 Only** until the device is rebooted. Do the following in Mission Control:

1. Navigate to **Overview > System Settings**.
2. Click on **Expert Configuration** to enter Expert Mode.

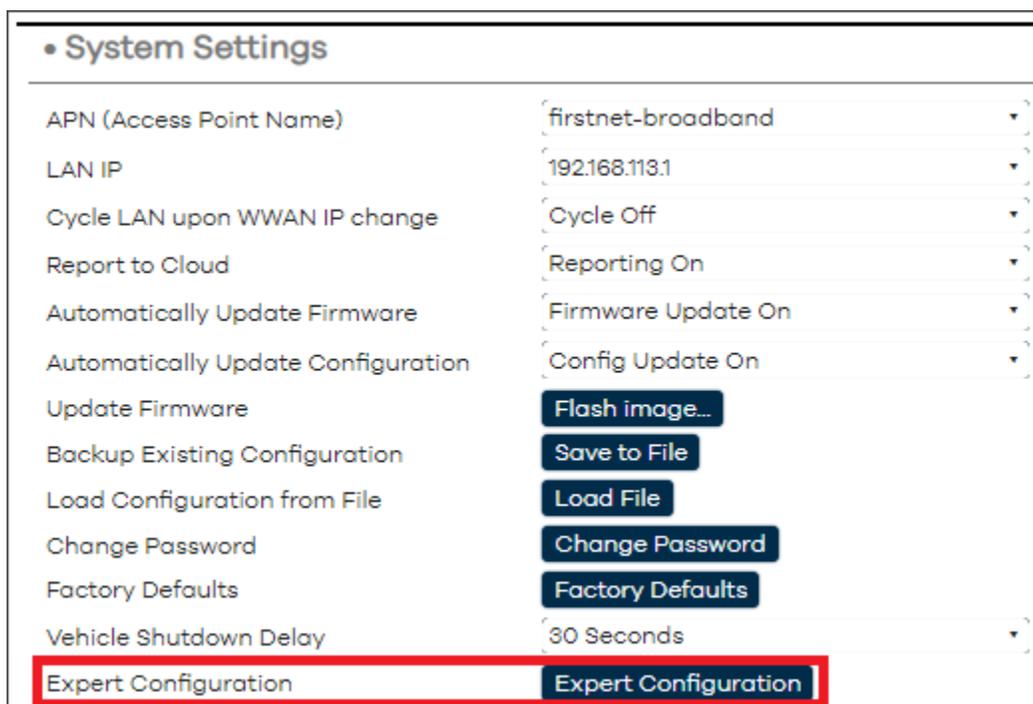


Figure 65: System Settings – Expert Configuration button

3. A pop-up window asks the user to confirm going into Expert Mode. Click **OK** to continue.

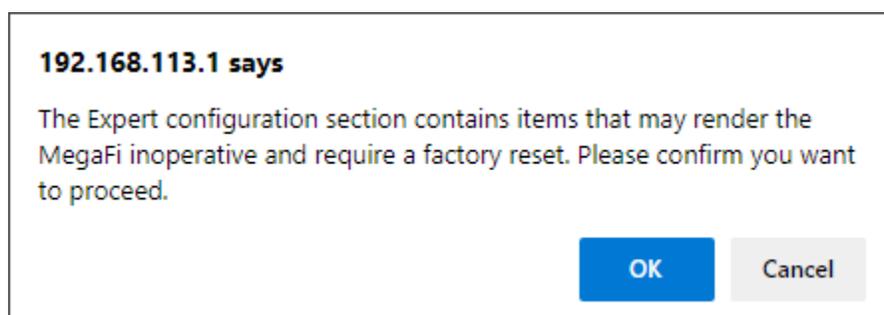


Figure 66: Confirmation to Enter Expert mode

4. The left-pane menu exposes pages only available in Expert Mode. Navigate to **System > MegaFi Configuration**.

- Under the **MegaFi and Modem Configuration** area, use the drop-down arrow to select **LTE B14 only** or **Default Band Configuration**. Choose the **Set Default Band Configuration** button to set back to default setting in which the device relies on the Network to choose the appropriate band.

The screenshot displays the 'MegaFi Configuration' interface. It is divided into several sections: 'Cloud', 'MegaFi Logging', 'NAT or Bridge Mode', and 'MegaFi and Modem Configuration'. The 'MegaFi and Modem Configuration' section is highlighted with a red border. Within this section, the 'Band Lock' setting is highlighted with a yellow border. The 'Band Lock' is currently set to 'Default Band Configuration', and a 'Set Default Band Configuration' button is visible next to it.

MegaFi Configuration	
• Cloud	
UUID	97F8B7D4-609D-4514-9F6C-A03FB694A
Cloud Poll URL	ei.awcone.com
Cloud Poll Period (seconds)	60
Cloud Status URL	
Cloud Status	Connected (12/1/2023, 12:43:27 PM)
• MegaFi Logging	
Logging Enabled	Logging Enabled
Push to Cloud	Push Enabled
Push to Cloud Period (seconds)	60
System Poll Period (seconds)	15
Show in Local UI	Local UI Enabled
• NAT or Bridge Mode	
MegaFi Mode (Changing causes reboot)	NAT Mode
LAN IP Address	192.168.113.1
• MegaFi and Modem Configuration	
Reboot Offline Time (minutes)	Disabled
Band Lock	Default Band Configuration
	Set Default Band Configuration

Figure 67: Band Lock Setting

- **Note:** Choosing the LTE B14 Only is temporary until the device reboots.
- Click on **Save & Apply** to confirm the change.
 - When changes have been completed, and to prevent any more setting changes, click on the **Logout** button to exit out of Mission Control and be taken back to the Log In page.

3.13 SSH Access

Access to SSH is turned off by default. To enable command line SSH access to the device, add a Dropbear SSH instance(s) by selecting the **SSH Access** tab and following the menu prompts. The user enabled SSH instance offers SSH network shell access and an integrated SCP server.

- ➔ **Note:** The default Port is set to 2022, but the user can change it to the typical port of 22. Make sure to Save & Apply to confirm the Dropbear SSH instance and change of port if any.

1. Navigate to **Overview > System Settings**.
2. Click on **Expert Configuration** to enter Expert Mode.

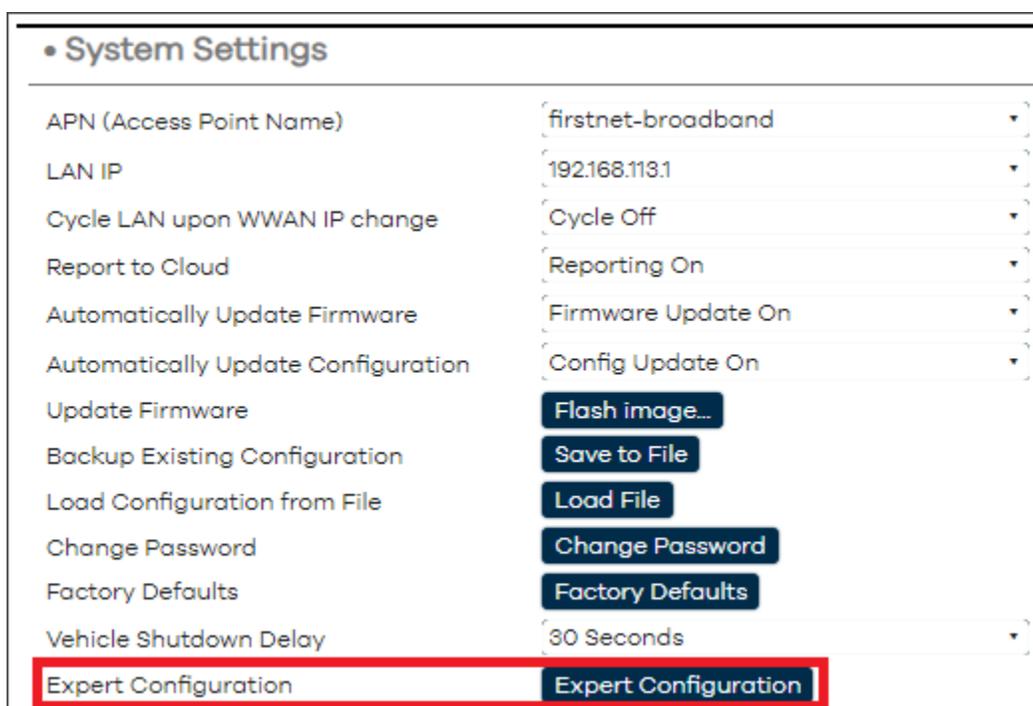


Figure 68: System Settings – Expert Configuration

3. A pop-up window asks the user to confirm going into Expert Mode. Click **OK** to continue.

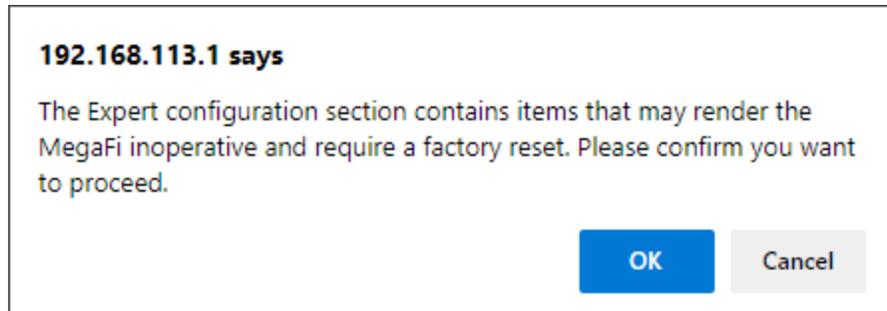


Figure 69: Confirmation to Enter Expert mode

4. The left-pane menu exposes pages only available in Expert Mode. Navigate to **System > Router Password > SSH Access**.



Figure 70: SSH Access page – add new instance

5. Click on the **Add Instance** button.
6. The Interface field will be pre-populated with the lan port by default and is typical when needing local access to the device. The other options in the dropdown menu are wan and wwan when remote SSH access is required.
7. In the **Port** field, change the port number from the default **2022** to **22** (well-known SSH port) and click on **Save & Apply**.

Router Password SSH Access SSH-Keys HTTP(S) Access

SSH Access

Dropbear offers SSH network shell access and an integrated SCP server

• Dropbear Instance

Interface Delete

Port Listen only on the given interface or, if unspecified, on all

Password authentication Allow SSH password authentication

Allow root logins with password Allow the root user to login with password

Gateway Ports Allow remote hosts to connect to local SSH forwarded ports

Idle Timeout

Add instance Save & Apply Save Reset

Figure 71: SSH Access page – Change port number from 2022 to 22

8. When changes have been completed, and to prevent any more setting changes, click on the **Logout** button to exit out of Mission Control and be taken back to the **Log In** page.
9. Use your preferred SSH client to access MegaFi on port **22** and use '**root**' as the username along with the current router password.
 - **Note:** The SSH password will be the same as the Router Password.
10. **Optional:** If remote SSH access to the device is required and the device has a custom static/public IP address, do the following:
 - 10a. **Add Interface** and choose wan or wwan depending on how the device is connected.
 - 10b. Choose a non-well-known port such as 46556.
 - 10c. A Firewall Traffic Rule will need to be implemented to allow incoming traffic on this port. An example of this is shown in section 5.1.

3.14 GPS Output Configuration

This is where the user can configure GPS settings for a GPS Server, GPS Internal Reporting, and GPS Output.

Mission Control Networking Mode: NAT Expert Mode ((14)) Firmware Version: 2.5.0.E.8

GPS Output Configuration

Configure GPS output in NMEA and TAIP format to hosts

- **GPS Server**
- Server Port
- **GPS Internal Reporting**
- Output Format Specify NMEA or TAIP output
- NMEA station code or TAIP ID
- Rate Optional rate limit in seconds
- **GPS Output**

This section contains no values yet
[Add output](#)

[Save & Apply](#) [Save](#) [Reset](#)

Figure 72: GPS Output Configuration page

3.14.1 GPS Server

To set up the MegaFi to act like a GPS Server to forward the GPS information to GPS Clients, do the following.

1. Navigate to **Overview > System Settings**.
2. Click on **Expert Configuration** to enter Expert Mode.

• System Settings

APN (Access Point Name)	firstnet-broadband
LAN IP	192.168.113.1
Cycle LAN upon WWAN IP change	Cycle Off
Report to Cloud	Reporting On
Automatically Update Firmware	Firmware Update On
Automatically Update Configuration	Config Update On
Update Firmware	Flash image...
Backup Existing Configuration	Save to File
Load Configuration from File	Load File
Change Password	Change Password
Factory Defaults	Factory Defaults
Vehicle Shutdown Delay	30 Seconds
Expert Configuration	Expert Configuration

Figure 73: System Settings – Expert Configuration

3. A pop-up window asks the user to confirm going into Expert Mode. Click **OK** to continue.

192.168.113.1 says

The Expert configuration section contains items that may render the MegaFi inoperative and require a factory reset. Please confirm you want to proceed.

OK **Cancel**

Figure 74: Confirmation to Enter Expert mode

4. The left-pane menu exposes pages only available in Expert Mode. Navigate to **System > GPS Configuration > GPS Server**.
5. Enter the port that the GPS server will be available on in the Server Port field followed by hitting the 'Enter' button. We entered 21000 as our example:

• GPS Server

Server Port	21000
-------------	-------

Figure 75: Configuration of GPS Server Port

6. **Save & Apply.**
7. When changes have been completed, and to prevent any more setting changes, click on the **Logout** button to exit out of Mission Control and be taken back to the Log In page.

3.14.2 GPS Internal Reporting

This section modifies the internal GPS formation and how it is reported. This section is discussed in more detail in section 4.3.5.2.

3.14.3 GPS Output

This section will enable the MegaFi to forward GPS information to a server. When adding an output, the available fields are:

- **Host IP Address** – Typically the IP address of the computer running a GPS client
- **Port** – can be any network port number from 1024 on, as long as it is not blocked and not already in use (stay away from well-known port numbers in the range between 0-1023)
- **Output Format** – TAIP or NMEA
- **NMEA station code or TAIP ID** – typically not required, but if needed, enter an appropriate and valid 4-digit number
- **TCP/UDP** – most typical option is UDP (Currently, only UDP works!)
- **Rate** – this parameter is in seconds

1. Navigate to **Overview > System Settings**.
2. Click on **Expert Configuration** to enter Expert Mode.

• System Settings	
APN (Access Point Name)	firstnet-broadband
LAN IP	192.168.113.1
Cycle LAN upon WWAN IP change	Cycle Off
Report to Cloud	Reporting On
Automatically Update Firmware	Firmware Update On
Automatically Update Configuration	Config Update On
Update Firmware	Flash image...
Backup Existing Configuration	Save to File
Load Configuration from File	Load File
Change Password	Change Password
Factory Defaults	Factory Defaults
Vehicle Shutdown Delay	30 Seconds
Expert Configuration	Expert Configuration

Figure 76: System Settings – Expert Configuration

3. A pop-up window asks the user to confirm going into Expert Mode. Click **OK** to continue.

192.168.113.1 says

The Expert configuration section contains items that may render the MegaFi inoperative and require a factory reset. Please confirm you want to proceed.

Figure 77: Confirmation to Enter Expert mode

4. The left-pane menu exposes pages only available in Expert Mode. Navigate to **System > GPS Configuration > GPS Output**.

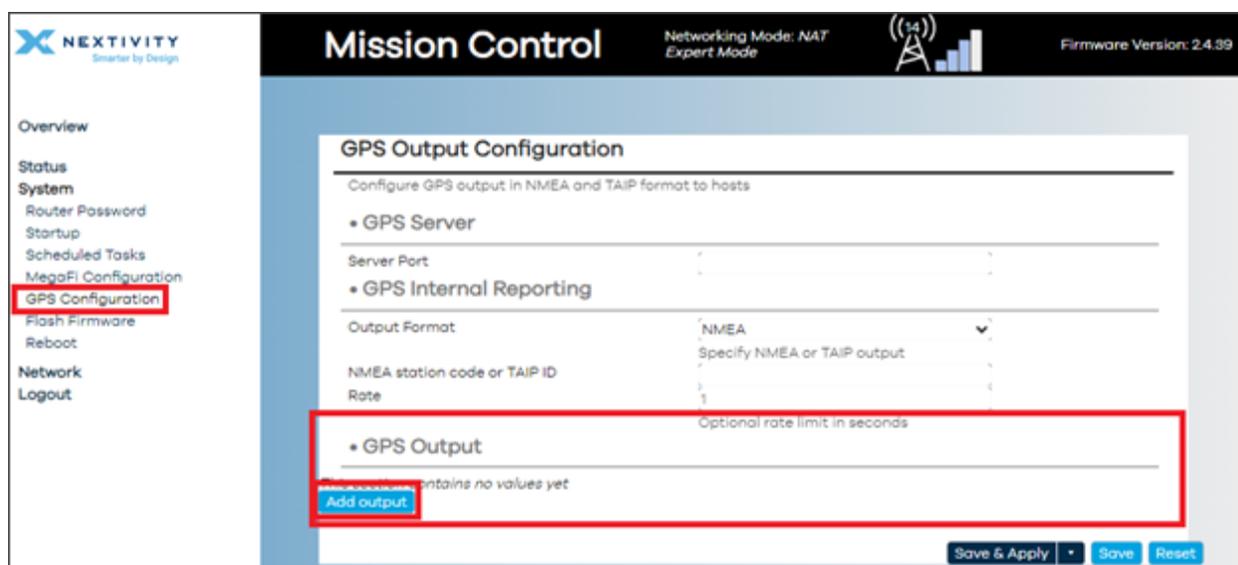


Figure 78: GPS Output Configuration – Add output

5. Select **Add output** and enter the following information:
 - 5a. **Host IP Address** – Typically the IP address of the computer running a GPS client
 - 5b. **Port** – can be any network port number from 1024 on, as long as it is not blocked and not already in use (stay away from well-known port numbers in the range between 0-1023)
 - 5c. **Output Format** – TAIP or NMEA
 - 5d. **NMEA station code or TAIP ID** – typically not required, but if needed, enter an appropriate and valid 4-digit number
 - 5e. **TCP/UDP** – most typical option is UDP (Currently, only UDP works!)
 - 5f. **Rate** – this parameter is in seconds

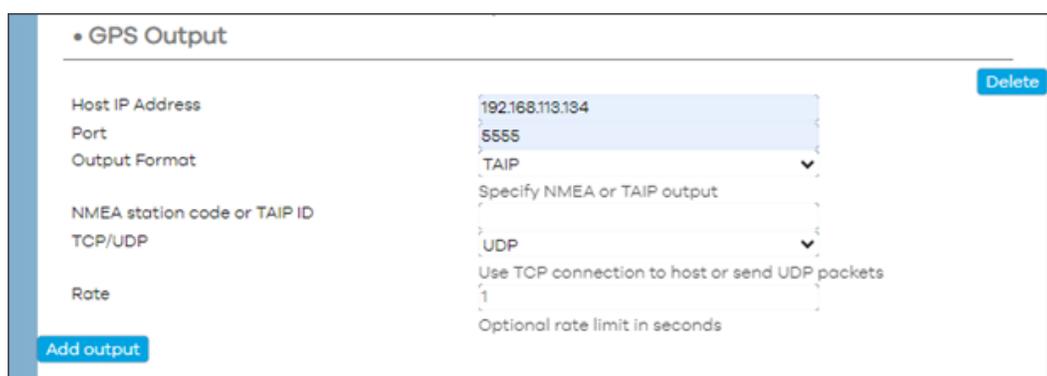


Figure 79: GPS Output page – Values for adding new output

6. **Save & Apply.**

7. When changes have been completed, and to prevent any more setting changes, click on the **Logout** button to exit out of Mission Control and be taken back to the Log In page.

🔄 **Note:** Multiple outputs can be configured to multiple clients. Just repeat this process as needed.

4 | Expert Configuration Settings

For more advanced settings, the user will need to first access Expert Mode. More detailed information into other Expert Mode configuration settings not yet discussed will be high-lighted in this section.

4.1 Enter Expert Mode	68
4.2 Status	69
4.3 System.....	86
4.4 Network	103
4.5 Logout	159

4.1 Enter Expert Mode

1. Navigate to **Overview > System Settings**.
2. Click on **Expert Configuration** to enter **Expert Mode**.

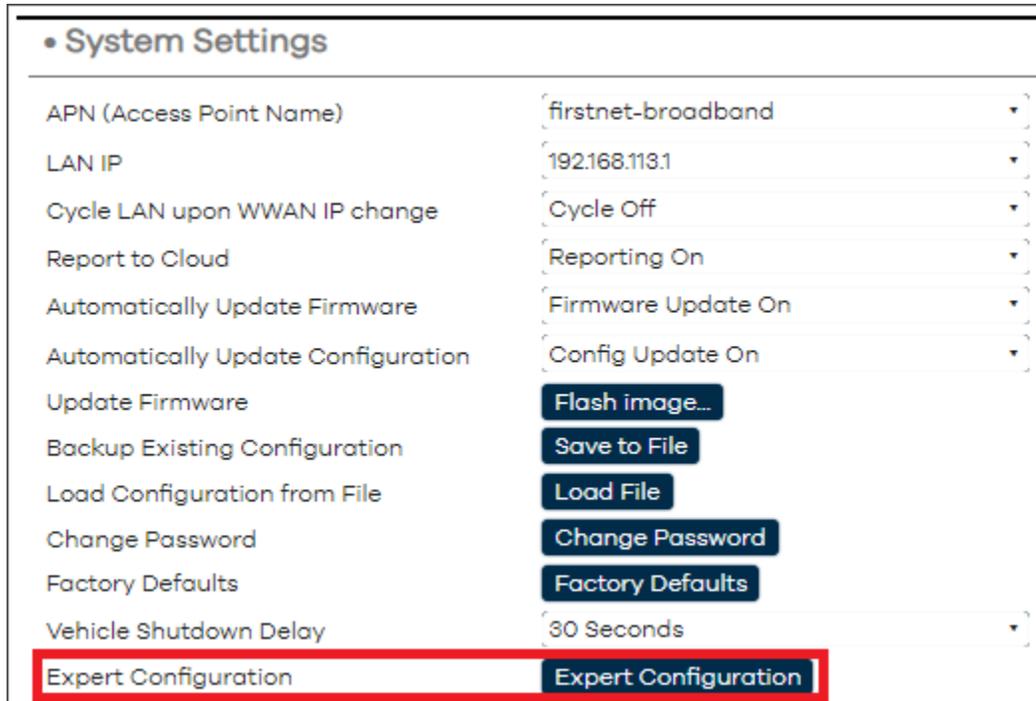


Figure 80: System Settings – Expert Configuration

3. A pop-up window asks the user to confirm going into Expert Mode. Click **OK** to continue.

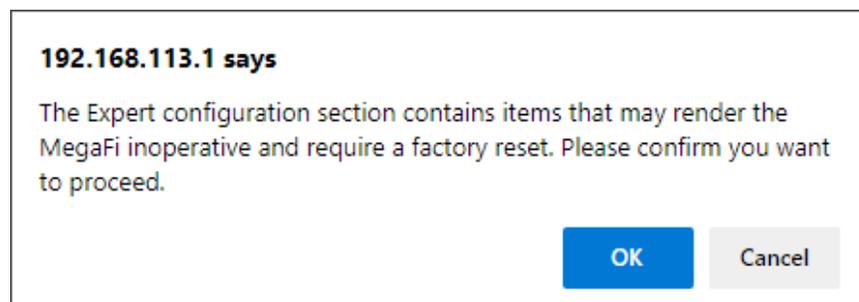


Figure 81: Confirmation message – Enter Expert Mode

4.2 Status

The left-pane menu exposes pages only available in **Expert Mode**. In the main window, the **Status > General** page will be displayed where the Status page provides a quick overview of the device's environment, health, and current standing. Links to sub-sections are **General, Routing, Firewall, System Log, Processes, Channel Analysis, Realtime Graphs, and Modem Status**. Each of these pages will be further discussed in detail below.

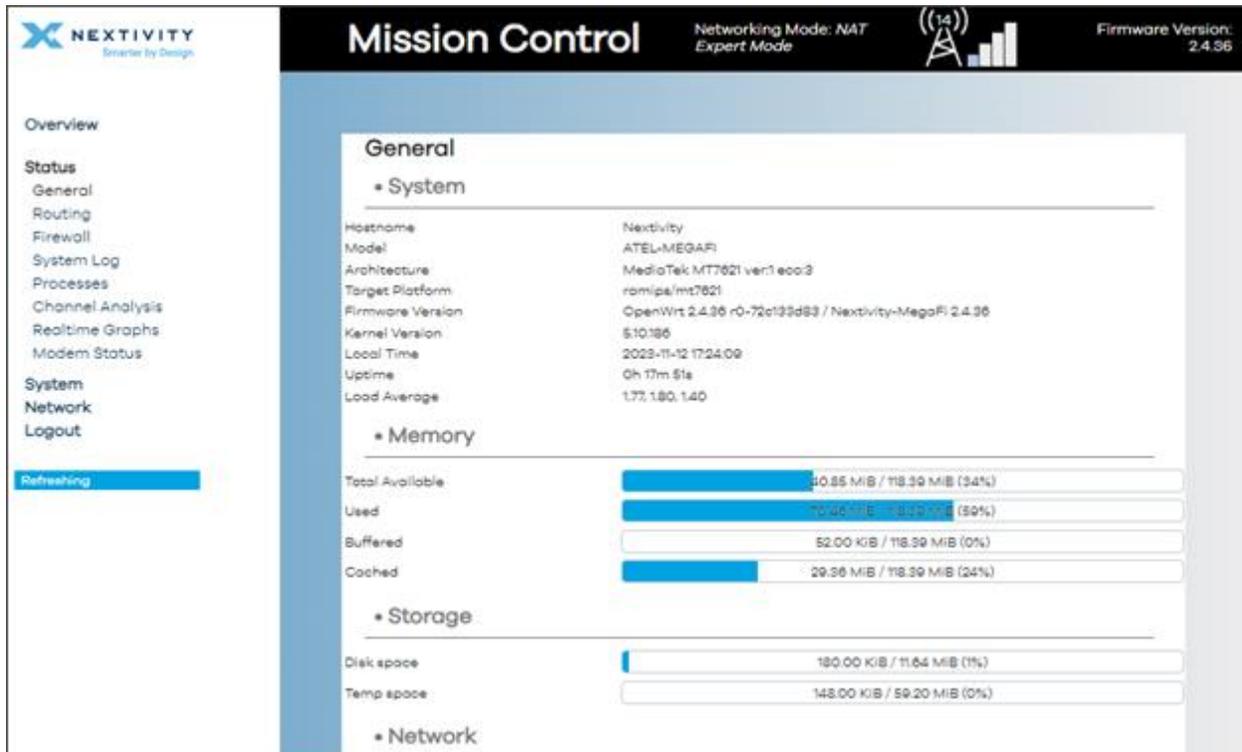


Figure 82: Status page showing overview of the device's environment, health, and current standing

4.2.1 General

The **General** section displays a summary of the devices' **System, Memory, Storage, Network, Active DHCP Leases, and Wireless** environments.

4.2.1.1 System

The System environment contains a list of attributes and parameters of the device such as:

- Hostname
- Model
- Architecture
- Target Platform
- Firmware Version

- Kernel Version
- Local time
- Uptime
- Load Average

General	
• System	
Hostname	Nextivity
Model	ATEL-MEGAFI
Architecture	MediaTek MT7621 ver:1 eco:3
Target Platform	ramips/mt7621
Firmware Version	OpenWrt 2.4.36 r0-72c133d83 / Nextivity-MegaFi 2.4.36
Kernel Version	5.10.186
Local Time	2023-10-18 17:29:00
Uptime	0h 56m 4s
Load Average	1.78, 1.85, 1.86

Figure 83: General page – System environment

4.2.1.2 Memory

The Memory environment displays the real time view of the memory of the device. This includes:

- Total Available
- Used
- Buffered
- Cached

• Memory	
Total Available	40.53 MiB / 118.39 MiB (34%)
Used	70.79 MiB / 118.39 MiB (59%)
Buffered	52.00 KiB / 118.39 MiB (0%)
Cached	29.37 MiB / 118.39 MiB (24%)

Figure 84: General page – Memory environment

4.2.1.3 Storage

The Storage environment displays disk space and temporary space available on the device.

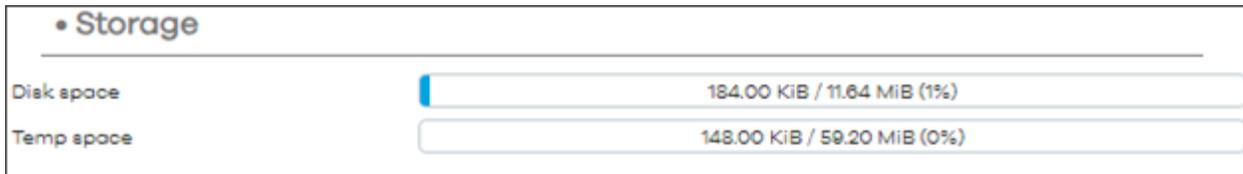


Figure 85: General page – Storage environment

4.2.1.4 Network

The **Network** environment contains:

- Protocol
- Cellular WWAN network connections (specifically IPv4 and IPv6 addresses assigned by the wireless network provider)
- Gateway
- Connected (device connection uptime)
- Device interface name
- MAC address
- Active Connections



Figure 86: General page – Network environment

4.2.1.5 Active DHCP/DHCPv6 Leases

The Active DHCP/DHCPv6 Leases environments includes the following information:

- Current Active DHCPv4 and Active DHCPv6 leases
- There is a “**Set Static lease**” option which, if selected and applied, will cause the MegaFi to maintain an association between the MAC and IP address assigned by DHCP on the LAN side, creating static routing to the designated device.

Active DHCP Leases				
Hostname	IPv4 address	MAC address	Lease time remaining	Static Lease
Lorenzo-s-S22-Ultra	192.168.113.143	8A:63:86:73:9F:18	11h 59m 43s	Set Static
LPORCHAS-LT	192.168.113.140	BC:F4:D4:6F:D8:C1	11h 33m 5s	Set Static
LGgram	192.168.113.110	A4:B1:C1:B6:E4:32	10h 58m 17s	Set Static

Active DHCPv6 Leases				
Host	IPv6 address	DUID	Lease time remaining	Static Lease
LPORCHAS-LT	2600:380:309d:1f42::be2/128 fdb3:9dda:d0::be2/128	000100012c83fd9b4cd7171f440b	11h 33m 16s	Set Static
LGgram	2600:380:309d:1f42::ef4/128 fdb3:9dda:d0::ef4/128	0001000127455b96a4b1c1b6e432	10h 51m 34s	Set Static

Figure 87: General page – Active DHCP Leases environments

4.2.1.6 Wireless

The **Wireless** environment provides a summary of Wi-Fi details from the 2.4 GHz radio (radio0) and the 5 GHz radio (radio1). In this environment, the user can also see the Associated Stations section which displays a list of Wi-Fi connected devices. Parameters to note are:

- Type – 802.11x
- Channel – 2.4 and 5GHz
- SSID
- Encryption
- Associations – current connections
- MAC Address
- Host
- Signal / Noise
- RX/TX Rates
- Option to Disconnect hosts

• Wireless

radio0

Type: MediaTek MT7603E 802.11bgn
Channel: 1 (2.412 GHz)
Bitrate: -

SSID: megafi-002229
Mode: Master
BSSID: 34:BA:9A:94:67:FF
Encryption: WPA3 SAE (CCMP)
Associations: -

radio1

Type: MediaTek MT76x2E 802.11acbg
Channel: 36 (5.180 GHz)
Bitrate: 811 Mbit/s

SSID: megafi-002229
Mode: Master
BSSID: 34:BA:9A:94:68:01
Encryption: WPA3 SAE (CCMP)
Associations: 3

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate	
megafi-002229 (...)	A4:B1:C1:B6:E4:32	LGgram (192.168.113.110, 2600:380:309d:1f42:ef4)	-34 dBm	6.0 Mbit/s, 20 MHz 866.7 Mbit/s, 80 MHz, VHT- MCS 9, VHT-NSS 2, Short GI	Disconnect
megafi-002229 (...)	BC:F4:D4:6F:D8:C1	LPORCHAS-LT (192.168.113.140, 2600:380:309d:1f42:38d6:9357:1c65:6045)	-42 dBm	866.7 Mbit/s, 80 MHz, VHT- MCS 9, VHT-NSS 2, Short GI 780.0 Mbit/s, 80 MHz, VHT- MCS 8, VHT-NSS 2, Short GI	Disconnect
megafi-002229 (...)	8A:63:86:73:9F:18	Lorenzo-s-S22-Ultra (192.168.113.143, 2600:380:309d:1f42:5ce1:e43d:d92f:6e3b)	-51 dBm	6.0 Mbit/s, 20 MHz 866.7 Mbit/s, 80 MHz, VHT- MCS 9, VHT-NSS 2, Short GI	Disconnect

Figure 88: General page – Wireless environment

4.2.2 Routing

In the **Routing** section, the user can track currently active IPv4 and IPv6 routing that shows **Neighbors**, **Routes**, and **Rules** on the system.

Routing

The following rules are currently active on this system.

IPv4 Routing IPv6 Routing

IPv4 Neighbours

IP address	MAC address	Interface
192.168.113.127	7C:8A:E1:80:E6:40	lan

Active IPv4 Routes

Network	Target	Gateway	Metric	Table	Protocol
wwan	0.0.0.0/0	10.39.42.121	10	main	static
wwan	10.39.42.112/28	-	10	main	static
lan	192.168.113.0/24	-	0	main	kernel

Active IPv4 Rules

Priority	Rule
0	from all lookup local
32766	from all lookup main
32767	from all lookup default

Figure 89: Routing page – IPv4 routing

IPv6 Neighbours

IP address	MAC address	Interface
2600:380:30fc:b93d:d51c:b83e:2bf0:115	A4:B1:C1:B6:E4:32	(br-lan)
2600:380:309d:1f42:5ce1e43d:d92f:6e3b	8A:63:86:73:9F:18	lan
2600:380:309d:e1ca:a8f2:9642:442d:dc9a	A4:B1:C1:B6:E4:32	(br-lan)
2600:380:30cd:af87:a8f2:9642:442d:dc9a	A4:B1:C1:B6:E4:32	(br-lan)
2600:380:309d:1f42:38d6:9357:1c65:6045	BC:F4:D4:6F:D8:C1	lan
fdb3:9dda:d0:0:d51c:b83e:2bf0:115	A4:B1:C1:B6:E4:32	lan
2600:380:309d:1f42:f04e:b639:2979:7806	BC:F4:D4:6F:D8:C1	lan
fdb3:9dda:d0:0:38d6:9357:1c65:6045	BC:F4:D4:6F:D8:C1	lan
fdb3:9dda:d0:0:61c4:902d:5798:95ff	8A:63:86:73:9F:18	lan
fdb3:9dda:d0:0:f04e:b639:2979:7806	BC:F4:D4:6F:D8:C1	lan

Active IPv6 Routes

Network	Target	Source	Metric	Table	Protocol
wwan	::/0	2600:380:309d:1f42::/64	10	main	static
wwan	2600:380:309d:1f42:110b:893e:301c:684	-	10	main	static
wwan	2600:380:309d:1f42:7419:1c42:282f:9931	-	10	main	static
lan	2600:380:309d:1f42::/64	-	1024	main	static
(br-lan)	2600:380:309d:e1ca::/64	-	256	main	kernel
(br-lan)	2600:380:30cd:af87::/64	-	256	main	kernel
(br-lan)	2600:380:30fc:b93d::/64	-	256	main	kernel
lan	fdb3:9dda:d0::/64	-	1024	main	static

Active IPv6 Rules

Priority	Rule
0	from all lookup local

Figure 90: Routing page – IPv6 routing

4.2.3 Firewall

The **Firewall** section displays the list of active chains across both IPv4 and IPv6 firewalls.

- **Note:** Hover over '#' with the mouse pointer for rule comments that gives more information on each rule.

IPv4/IPv6 traffic table "fw4"

Traffic filter chain "input"

- Hook: **input** (Capture incoming packets routed to the local system), Priority: 0
- Policy: **accept** (Continue processing unmatched packets)

Rule matches	Rule actions
# <i>Ingress device name</i> is lo	Accept packet
# <i>Conntrack state</i> is one of established, related	Accept packet
# <i>TCP flags & (fin syn rst ack)</i> is syn	Continue in syn_flood
# <i>Ingress device name</i> is br-lan	Continue in input_lan
# <i>Ingress device name</i> in set { wan, wwan0 }	Continue in input_wan

Traffic filter chain "forward"

- Hook: **forward** (Capture incoming packets addressed to other hosts), Priority: 0
- Policy: **drop** (Drop unmatched packets)

Rule matches	Rule actions
# <i>Conntrack state</i> is one of established, related	Accept packet
# <i>Ingress device name</i> is br-lan	Continue in forward_lan
# <i>Ingress device name</i> in set { wan, wwan0 }	Continue in forward_wan
<i>Any packet</i>	Continue in handle_reject

Traffic filter chain "output"

- Hook: **output** (Capture outgoing packets originating from the local system), Priority: 0
- Policy: **accept** (Continue processing unmatched packets)

Figure 91: Firewall page – IPv4 and IPv6 firewalls

4.2.4 System Log

The **System Log** page provides a list of notifications within the system and the kernel. These entries are important for troubleshooting and understanding the state of the device.

- **Note:** If asked to provide a log for troubleshooting purposes, the user can select the entire log by hovering over the entries in the log, and right click the mouse, and then select all from the list. Then, right click again and select copy to make it available on the clipboard. Then open Notepad, or a similar text program, and press control-V to paste the log. Then, save the pasted log as a text file on your PC. The text file can then be emailed as needed. This is true for either the System or Kernel logs.

The screenshot shows a terminal window with a tabbed interface. The 'System Log' tab is active, displaying a list of system messages. The messages include kernel information, daemon notices, and user notices, all timestamped 'Wed Oct 18 00:11:32 2023' or 'Wed Oct 18 00:11:34 2023'. The log entries describe the configuration and initialization of network interfaces (lan1, lan2, lan3, lan4, wan, wwan) and the network service.

```

System Log Kernel Log

System Log

Wed Oct 18 00:11:32 2023 user.notice ucitrack: Setting up /etc/config/miniupnpd reload dependency on /etc/config/firewall
Wed Oct 18 00:11:32 2023 user.notice ucitrack: Setting up /etc/config/odhcpd reload dependency on /etc/config/dhcp
Wed Oct 18 00:11:32 2023 kern.info kernel: [ 54.198519] mtk_soc_eth 1e100000.ethernet eth0: configuring for fixed/rgmii 1:
Wed Oct 18 00:11:32 2023 kern.info kernel: [ 54.293784] mtk_soc_eth 1e100000.ethernet eth0: Link is Up - 1Gbps/Full - flow
Wed Oct 18 00:11:32 2023 kern.info kernel: [ 54.298649] device eth0 entered promiscuous mode
Wed Oct 18 00:11:32 2023 kern.info kernel: [ 54.451408] mt7530 mdio-bus:1f lan1: configuring for phy/gmii link mode
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 54.532037] 8021q: adding VLAN 0 to HW filter on device lan1
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 54.603286] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 54.679612] br-lan: port 1(lan1) entered blocking state
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 54.742424] br-lan: port 1(lan1) entered disabled state
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 54.807028] device lan1 entered promiscuous mode
Wed Oct 18 00:11:33 2023 daemon.notice netifd: Interface 'lan' is enabled
Wed Oct 18 00:11:33 2023 daemon.notice netifd: Interface 'lan' is setting up now
Wed Oct 18 00:11:33 2023 daemon.notice netifd: Interface 'lan' is now up
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 54.897981] mt7530 mdio-bus:1f lan2: configuring for phy/gmii link mode
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 54.978533] 8021q: adding VLAN 0 to HW filter on device lan2
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 55.051232] br-lan: port 2(lan2) entered blocking state
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 55.114049] br-lan: port 2(lan2) entered disabled state
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 55.178748] device lan2 entered promiscuous mode
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 55.256005] mt7530 mdio-bus:1f lan3: configuring for phy/gmii link mode
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 55.339327] 8021q: adding VLAN 0 to HW filter on device lan3
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 55.412853] br-lan: port 3(lan3) entered blocking state
Wed Oct 18 00:11:33 2023 kern.info kernel: [ 55.475899] br-lan: port 3(lan3) entered disabled state
Wed Oct 18 00:11:34 2023 kern.info kernel: [ 55.542295] device lan3 entered promiscuous mode
Wed Oct 18 00:11:34 2023 kern.info kernel: [ 55.619904] mt7530 mdio-bus:1f lan4: configuring for phy/gmii link mode
Wed Oct 18 00:11:34 2023 kern.info kernel: [ 55.701969] 8021q: adding VLAN 0 to HW filter on device lan4
Wed Oct 18 00:11:34 2023 kern.info kernel: [ 55.774428] br-lan: port 4(lan4) entered blocking state
Wed Oct 18 00:11:34 2023 kern.info kernel: [ 55.837291] br-lan: port 4(lan4) entered disabled state
Wed Oct 18 00:11:34 2023 kern.info kernel: [ 55.903025] device lan4 entered promiscuous mode
Wed Oct 18 00:11:34 2023 daemon.notice netifd: Interface 'loopback' is enabled
Wed Oct 18 00:11:34 2023 daemon.notice netifd: Interface 'loopback' is setting up now
Wed Oct 18 00:11:34 2023 daemon.notice netifd: Interface 'loopback' is now up
Wed Oct 18 00:11:34 2023 kern.info kernel: [ 55.906974] mt7530 mdio-bus:1f wan: configuring for phy/gmii link mode
Wed Oct 18 00:11:34 2023 kern.info kernel: [ 56.069799] 8021q: adding VLAN 0 to HW filter on device wan
Wed Oct 18 00:11:34 2023 daemon.notice netifd: Interface 'wan' is enabled
Wed Oct 18 00:11:34 2023 daemon.notice netifd: Interface 'wwan' is setting up now
Wed Oct 18 00:11:34 2023 daemon.notice netifd: Network device 'eth0' link is up
Wed Oct 18 00:11:34 2023 daemon.notice netifd: Network device 'lo' link is up
Wed Oct 18 00:11:34 2023 daemon.notice netifd: Interface 'loopback' has link connectivity
Wed Oct 18 00:11:34 2023 user.notice ucitrack: Setting up non-init /etc/config/fstab reload handler: /sbin/block mount
Wed Oct 18 00:11:35 2023 daemon.notice netifd: wwan (3974): error: couldn't find the ModemManager process in the bus
Wed Oct 18 00:11:35 2023 daemon.notice netifd: wwan (3974): Device not managed by ModemManager
Wed Oct 18 00:11:35 2023 user.notice ucitrack: Setting up /etc/config/system reload trigger for non-procd /etc/init.d/led
Wed Oct 18 00:11:35 2023 daemon.info ModemManager[3761]: hotplug: no need to wait for modem at sysfs path /sys/devices/plat
Wed Oct 18 00:11:35 2023 daemon.notice netifd: wwan (4083): stopping network

```

Figure 92: System Log page

4.2.4.1 Kernel Log

The Kernel Log can be found as a tab to the right of the System Log in the middle of the screen and displays kernel information such as:

- Operating system and version
- Data cache
- Type information
- Memory
- Nodes

```

System Log  Kernel Log

Kernel Log

[ 0.000000] Linux version 5.10.186 (root@34fbaf1d1532) (mipsel-openwrt-linux-musl-gcc (OpenWrt GCC 11.2.0 r0-72c133d83) : ^
[ 0.000000] SoC Type: MediaTek MT7621 ver:1 eco:3
[ 0.000000] printk: bootconsole [early0] enabled
[ 0.000000] CPU0 revision is: 0001992f (MIPS 1004Kc)
[ 0.000000] MIPS: machine is ATEL-MEGAFI
[ 0.000000] Initrd not found or empty - disabling initrd
[ 0.000000] VPE topology (2,2) total 4
[ 0.000000] Primary instruction cache 32kB, VIPT, 4-way, linesize 32 bytes.
[ 0.000000] Primary data cache 32kB, 4-way, PIPT, no aliases, linesize 32 bytes
[ 0.000000] MIPS secondary cache 256kB, 8-way, linesize 32 bytes.
[ 0.000000] Zone ranges:
[ 0.000000]   Normal [mem 0x0000000000000000-0x0000000007ffffff]
[ 0.000000]   HighMem empty
[ 0.000000] Movable zone start for each node
[ 0.000000] Early memory node ranges
[ 0.000000]   node 0: [mem 0x0000000000000000-0x0000000007ffffff]
[ 0.000000] Initmem setup node 0 [mem 0x0000000000000000-0x0000000007ffffff]
[ 0.000000] On node 0 totalpages: 32768
[ 0.000000]   Normal zone: 256 pages used for memmap
[ 0.000000]   Normal zone: 0 pages reserved
[ 0.000000]   Normal zone: 32768 pages, LIFO batch:7
[ 0.000000] percpu: Embedded 15 pages/cpu s29968 r8192 d23280 u61440
[ 0.000000] pcpu-alloc: s29968 r8192 d23280 u61440 alloc=15*4096
[ 0.000000] pcpu-alloc: [0] 0 [0] 1 [0] 2 [0] 3
[ 0.000000] Built 1 zonelists, mobility grouping on.  Total pages: 32512
[ 0.000000] Kernel command line: rootfstype=squashfs,jffs2
[ 0.000000] Dentry cache hash table entries: 16384 (order: 4, 65536 bytes, linear)
[ 0.000000] Inode-cache hash table entries: 8192 (order: 3, 32768 bytes, linear)
[ 0.000000] Writing ErrCtl register=00021491
[ 0.000000] Readback ErrCtl register=00021491
[ 0.000000] mem auto-init: stack:off, heap alloc:off, heap free:off
[ 0.000000] Memory: 119924K/131072K available (6357K kernel code, 600K rwdata, 1196K rodata, 1308K init, 232K bss, 11148K
[ 0.000000] SLUB: HWalign=32, Order=0-3, MinObjects=0, CPUs=4, Nodes=1

```

Figure 93: Kernel Log page

4.2.5 Processes

The **Processes** section provides an overview list of all currently running system processes and their status, which include:

- PID
- Owner
- Command
- CPU usage (%)
- Memory usage (%)

There are three (3) action options for each process:

- **Hang Up:** shut down the process and restart it
- **Terminate:** shut down the process
- **Kill:** the kernel will stop the process

Processes

This list gives an overview over currently running system processes and their status.

PID	Owner	Command	CPU usage (%)	Memory usage (%)			
1	root	/sbin/procd	0%	1%	Hang Up	Terminate	Kill
2	root	[kthreadd]	0%	0%	Hang Up	Terminate	Kill
9	root	[rcu_tasks_trace]	0%	0%	Hang Up	Terminate	Kill
10	root	[ksoftirqd/0]	0%	0%	Hang Up	Terminate	Kill
12	root	[migration/0]	0%	0%	Hang Up	Terminate	Kill
13	root	[cpuhp/0]	0%	0%	Hang Up	Terminate	Kill
14	root	[cpuhp/1]	0%	0%	Hang Up	Terminate	Kill
15	root	[migration/1]	0%	0%	Hang Up	Terminate	Kill
16	root	[ksoftirqd/1]	0%	0%	Hang Up	Terminate	Kill
19	root	[cpuhp/2]	0%	0%	Hang Up	Terminate	Kill
20	root	[migration/2]	0%	0%	Hang Up	Terminate	Kill
21	root	[ksoftirqd/2]	0%	0%	Hang Up	Terminate	Kill
24	root	[cpuhp/3]	0%	0%	Hang Up	Terminate	Kill
25	root	[migration/3]	0%	0%	Hang Up	Terminate	Kill
26	root	[ksoftirqd/3]	0%	0%	Hang Up	Terminate	Kill
193	root	[oom_reaper]	0%	0%	Hang Up	Terminate	Kill
196	root	[kcompactd0]	0%	0%	Hang Up	Terminate	Kill
246	root	[watchdogd]	0%	0%	Hang Up	Terminate	Kill
270	root	[kswapd0]	0%	0%	Hang Up	Terminate	Kill

Figure 94: Process page showing system processes and status

4.2.6 Channel Analysis

In the **Channel Analysis** section, a graphing environment of each radio is shown and displays all available Wi-Fi routers available nearby. The radios are radio0 (2.4 GHz), radio1 (2.4GHz), and radio1 (5 GHz). In each radio graph, the user can see each router's **Signal**, **SSID**, **Channel**, **Channel Width**, **Mode**, and **BSSID** along with other Wi-Fi radios currently online and their frequencies. The radio1 (2.4GHz) radio only shows your device.

Utilizing this tool can reveal which channels are used least, allowing the user to switch to a less crowded part of the spectrum. Doing so will help to reduce interference, increasing speed, and enhance overall network reliability. If there is significant contention noted, the MegaFi Wi-Fi channel assignment can be updated. See section 3.10.2 *Change Wi-Fi Settings*.

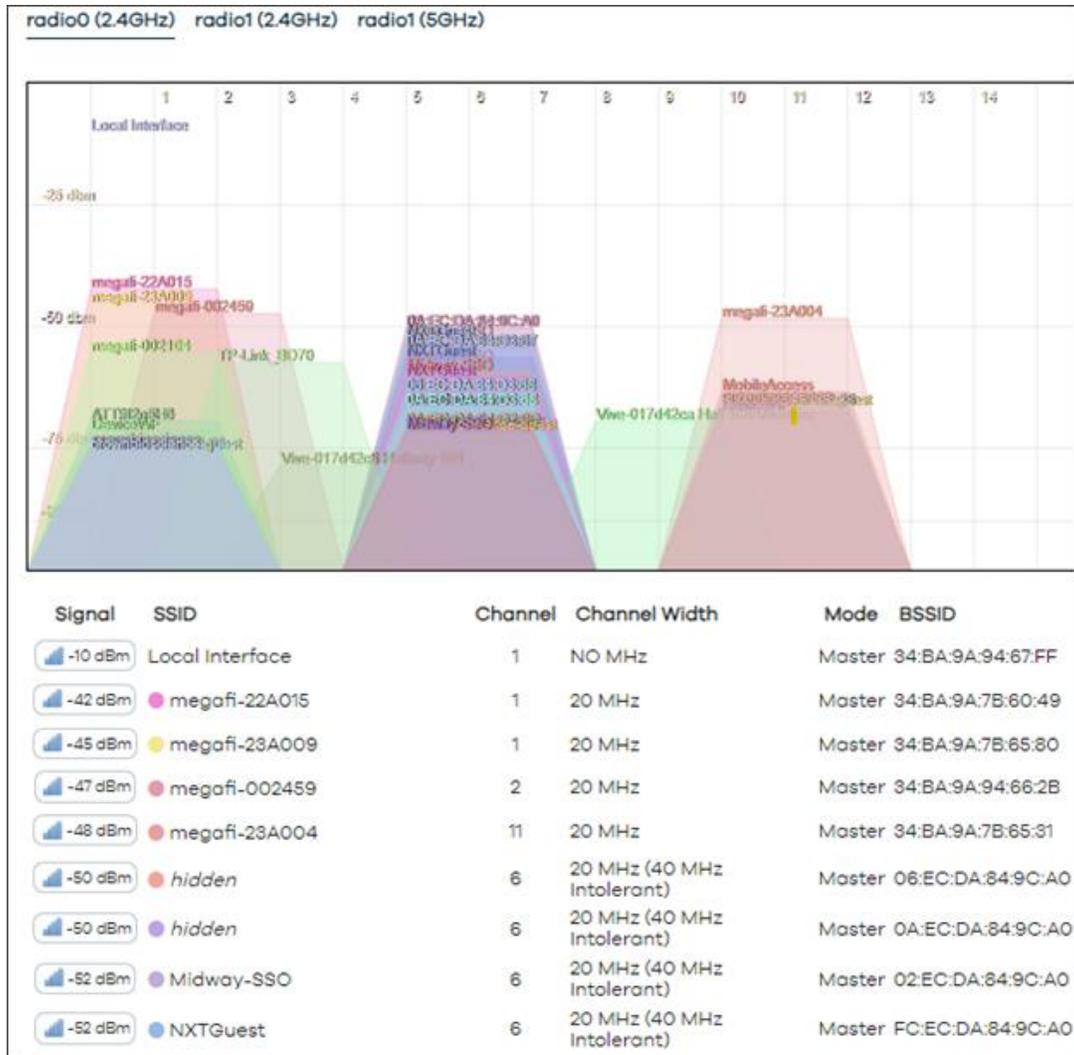


Figure 95: Channel Analysis showing graph radio0 (2.4GHz)

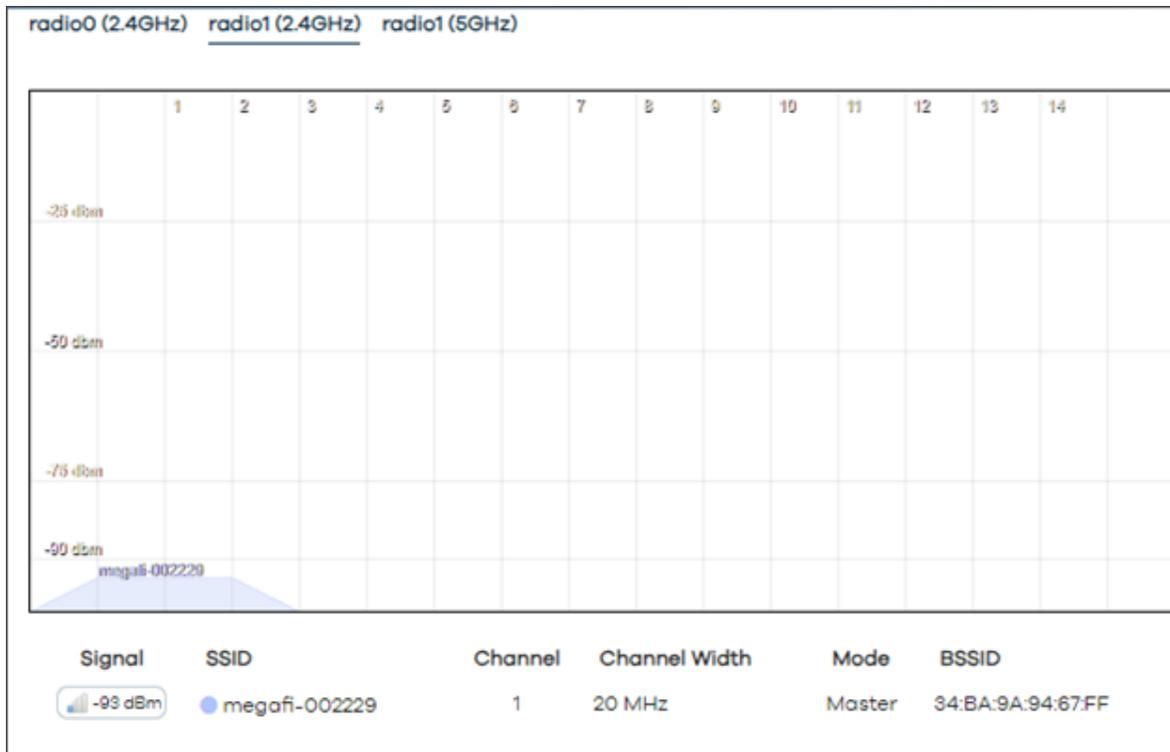


Figure 96: Channel Analysis showing graph for radio1 (2.4GHz)

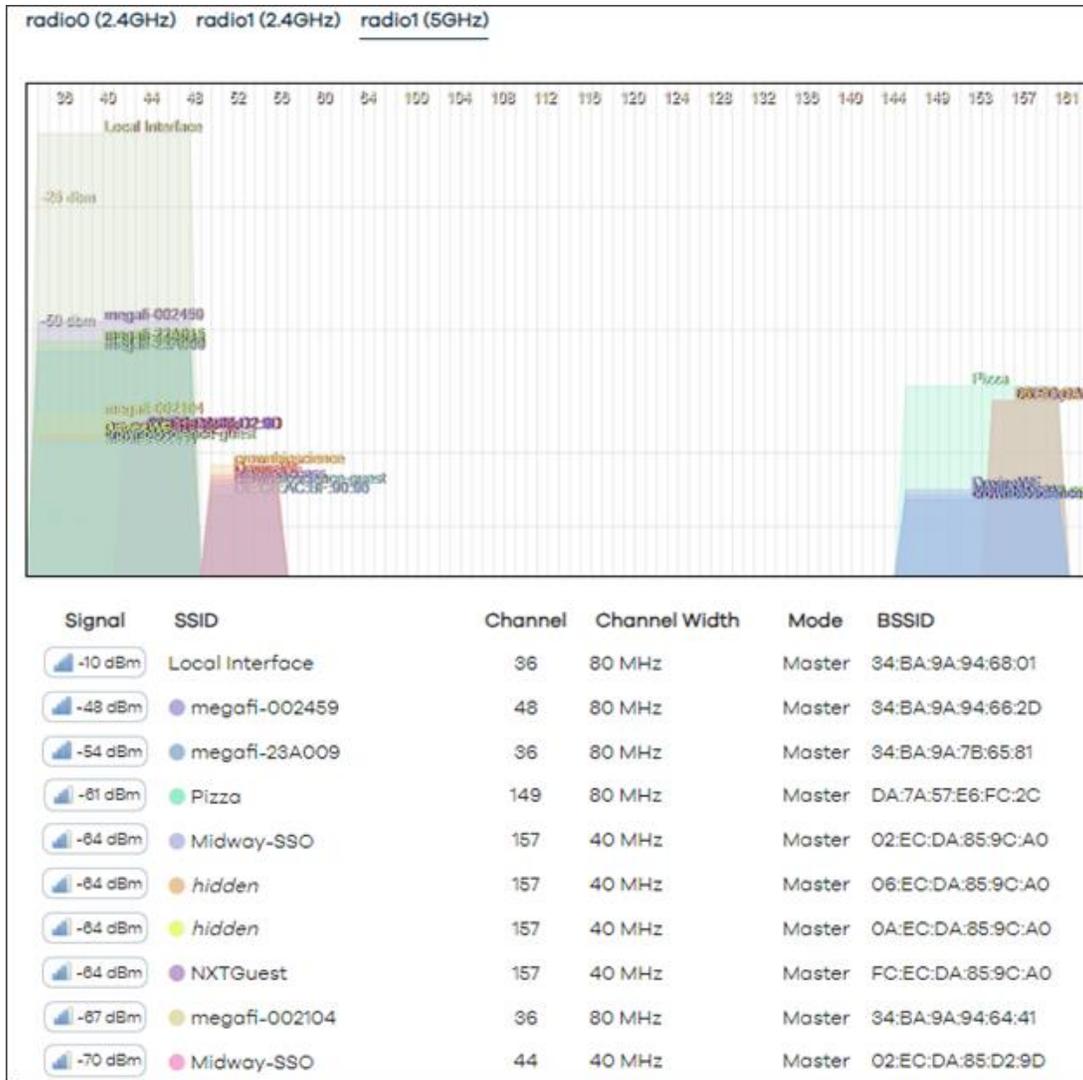


Figure 97: Channel Analysis showing graph for radio1 (5GHz)

4.2.7 Realtime Graphs

The Realtime Graphs section provides more aid in information gathering and diagnostic evaluations. The graphs provides:

- **Load:** network load is shown as filled colored elements in 1, 5, and 15 minute load segments.

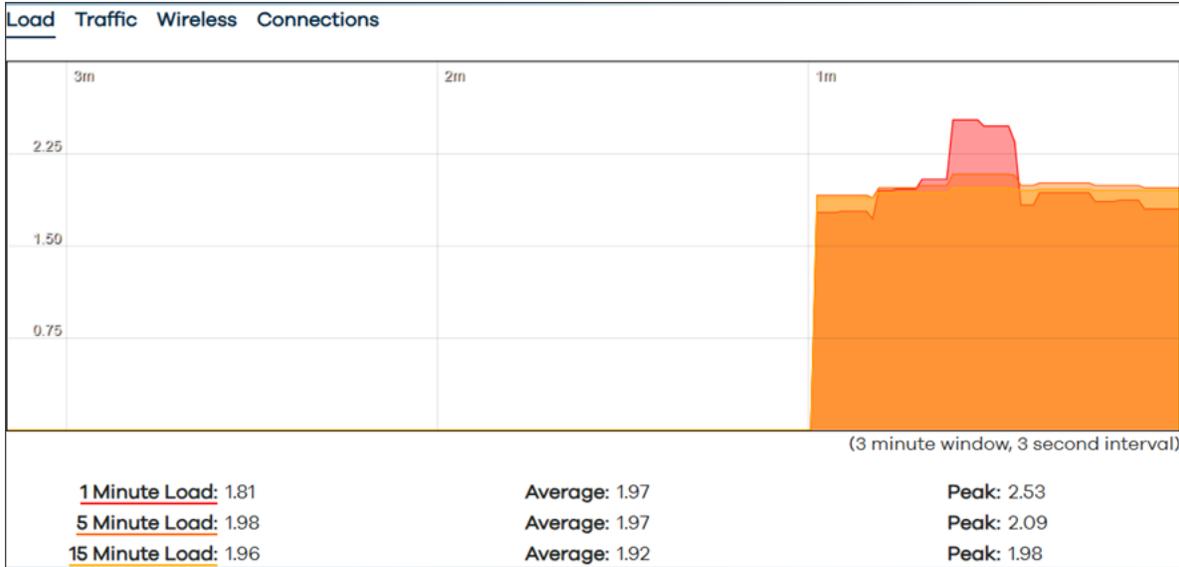


Figure 98: Realtime Graphs – Load graph

- Traffic:** real time information about the current traffic load is shown for each interface with inbound and outbound traffic statistics available in graph and tabular form. The Traffic tab section below shows route segments configured: br-LAN, erspan0, eth0, LAN1, LAN2, LAN3, LAN4, wan, wwan0, wlan0, and wlan1, however, the user may have more, or fewer segments based upon their implementation.

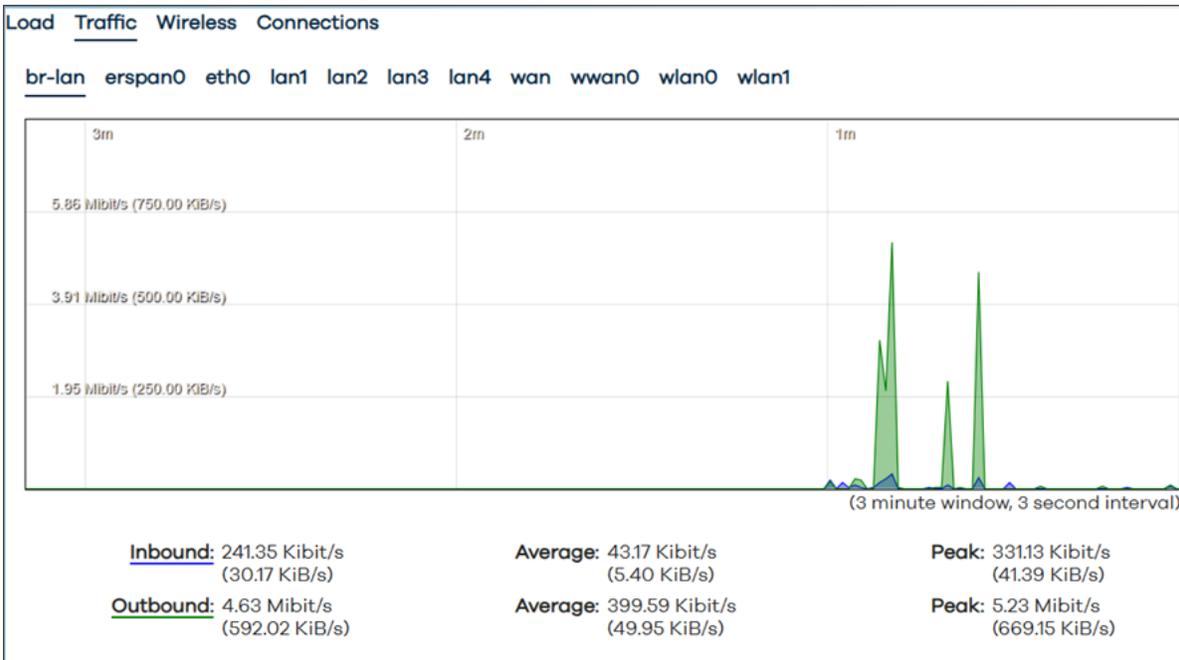


Figure 99: Realtime Graphs – Traffic graph

- **Wireless:** provides Signal and Noise graphs (peak and averages) as well as peak and average use for the 2.4GHz Wi-Fi (wLAN0) and 5GHz Wi-Fi (wLAN1).



Figure 100: Realtime Graphs – Wireless graph

- **Connections:** real time numbers of current active connections. Provides a summary of connections by protocol (UDP, TCP, or Other) with peaks and averages. Other packet traversal information such as Network, Protocol, Source, Destination, and Transfer is available.

There is button to **Enable DNS lookups** if needed.

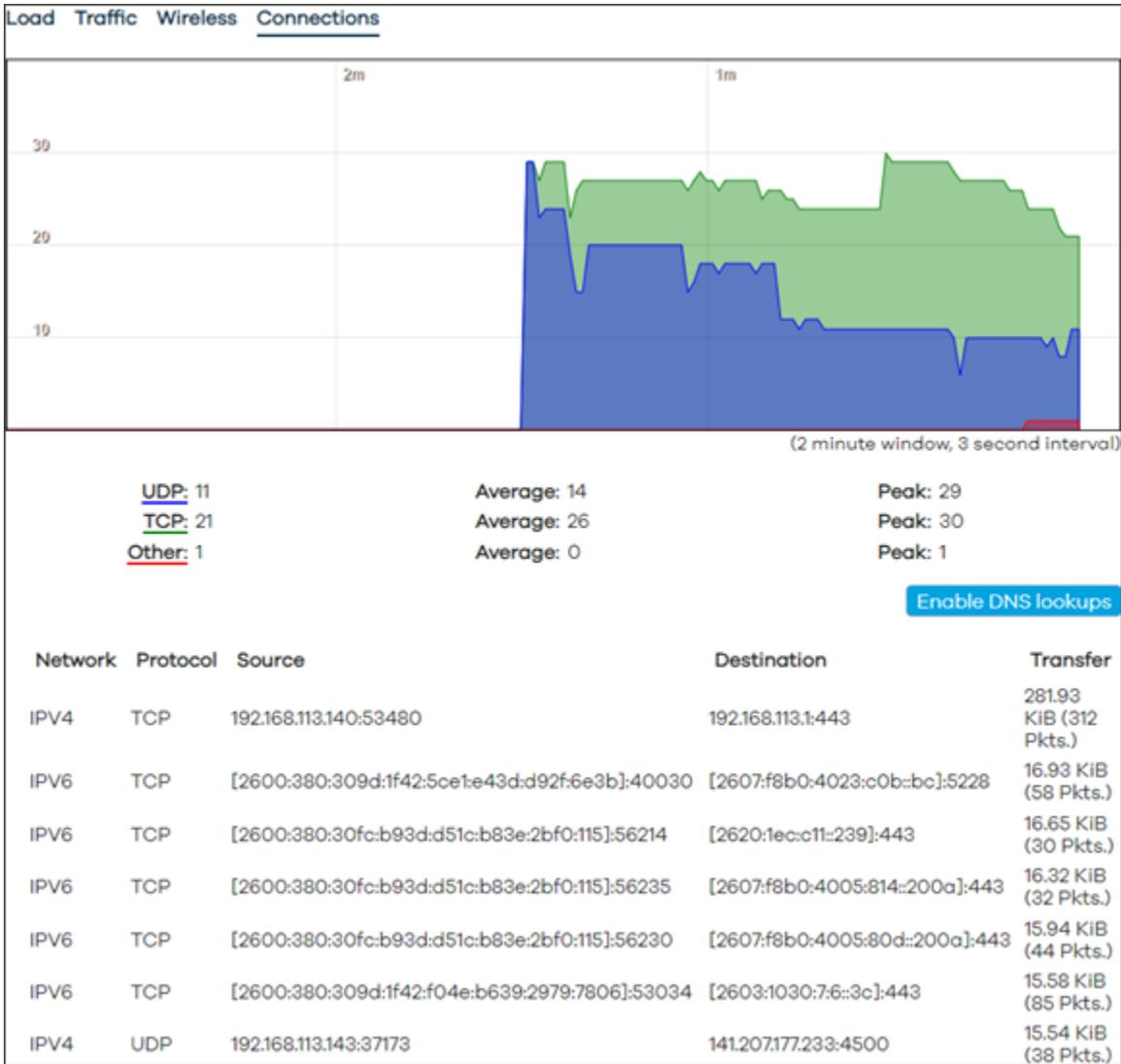


Figure 101: Realtime Graphs – Connections graph

4.2.8 Modem Status

The **Modem Status** page lists the information based on the latest polling of the modem. The most important details that most users will be interested in are **IMEI, Phone Number, LTE Connection State, Signal Percentage, Tx and Rx Bytes, GPS, APN, Band, Tx Power, RSRP, RSRQ, RSSI, and SINR** values.

Modem Status			
System Name	MegaFi-AW12	LTE Connection state	Connected
Modem Software Version	EM12AWPAR01A07M4G	Signal Percentage	75%
IMEI	015681000000596	TX Bytes	16527313
ICCID	89011003300033550304	RX Bytes	53182994
IMSI	313100003355030	TX Packets	38332
MCBV	0x260	RX Packets	57118
MCLBV	0x2000000003000281a	AT RX Bytes	25433292
Phone Number	858.310.7548	AT TX Bytes	138813208
Modem Protocol	QMI		
Latitude	0.000000		
Longitude	0.000000		
NMEA/TAIP Position	\$GPGGA,010321.000,0000.00000,N,00000.00000,E,0,00,0.0		
GPS UTC Timestamp	Tue Aug 29 2023 18:03:21 GMT-0700 (Pacific Daylight Time)		
APN	firstnet-broadband	Mode	LTE
Home Network MCC	313	ID	79474863
Home Network MNC	100	PID	388
Home Network Name	FirstNet	EARFCN	5330
		FB	14
		ULB	10
		DLB	10
PDP IP Address	10.39.42.120	TAC	33547
UE RSSI	-63 dBm	RSRP	-94 dBm
UE Qual	99	RSRQ	-10 dB
QMI SC SNR	3.4 dB	RSSI	-65 dBm
QMI CA Band	30	SINR	6.0 dB
		TX Power	0.0 dBm

Figure 102: Modem Status – Latest modem polling information

4.3 System

The **System** section provides the user with the ability to configure the internal settings of the MegaFi. Sub-sections under System include **Router Password**, **Startup**, **Scheduled Tasks**, **MegaFi Configuration**, **GPS Configuration**, **Flash Firmware**, and **Reboot**.

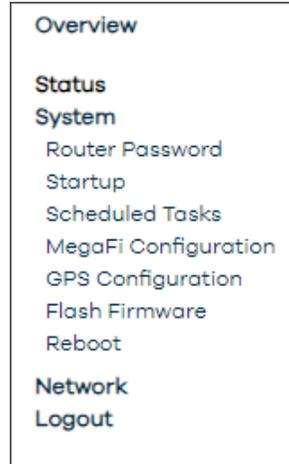


Figure 103: Navigation pane – System menu

4.3.1 Router Password

The user will be able to change or reset the device password, as well as manage **SSH Access**, **SSH Keys**, and **HTTP(S) Access**. Please note the additional tabs for SSH Access, SSH Keys, and HTTP(S) Access are shown to the right of the Router Password, not in the list on menu on the left side of the screen.

! WARNING: If the user has forgotten the password set, a reset of the unit is available. However, this will revert the password to the default password, which can be found on the label beneath the device. All other settings will also default to factory settings.

4.3.1.1 Change Password

Refer to section 3.6 *Change Password* for details on changing the Router Password.

4.3.1.2 SSH Access

Access to SSH is turned off by default. To enable command line SSH access to the device, add a Dropbear SSH instance(s) by selecting the **SSH Access** tab and following the menu prompts. The user enabled SSH instance offers SSH network shell access and an integrated SCP server. Refer to section 3.13 *SSH Access* for more details on setting up SSH Access.

4.3.1.3 SSH-Keys

For higher security, **SSH-Keys**, an OpenSSH public key line or .pub file, can be required.

Paste or drag the SSH key file into the supplied field and click on **'Add Key'** to upload the required keys and enable empty password SSH logins with higher security.

The screenshot shows the 'SSH-Keys' section of a configuration interface. At the top, there are tabs for 'Router Password', 'SSH Access', 'SSH-Keys' (which is selected), and 'HTTP(S) Access'. Below the tabs, the title 'SSH-Keys' is displayed. A paragraph explains that public keys allow for passwordless SSH logins with higher security. Below this, it states 'No public keys present yet.' At the bottom, there is a text input field with the placeholder 'Paste or drag SSH key file...' and a blue 'Add key' button to its right.

Figure 104: SSH-Keys section – Adding a key

If an SSH-Key is no longer needed, or needs to be updated, simply click on the '-' button, followed by **'Delete key'** to delete it.

The first screenshot shows the 'SSH-Keys' section with a list of keys. One key is selected, showing its name 'Unnamed key', its type 'RSA, 2048 Bit / Options: 192.168.113.1', and its public key text. A blue '-' button is visible to the right of the key. Below the list is the 'Add key' button. The second screenshot is a modal dialog titled 'Delete key'. It asks 'Do you really want to delete the following SSH key?' and displays the key's details: '192.168.113.1 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ6wRUazI+JFhR3y1tBspYZka72MD4qGCHYrNxcFitq4M3yT0sMMUPc8g1AWLqmtEhGuFDHx1P'. At the bottom right of the dialog are 'Cancel' and 'Delete key' buttons.

Figure 105: SSH-Keys – Delete key

4.3.1.4 HTTP(S) Access

HTTP(S) Access causes a redirect from HTTP to HTTPS for access to the device. It is highly recommended that this be left checked as included in the default configuration.

Router Password SSH Access SSH-Keys HTTP(S) Access

HTTP(S) Access

uHTTPd offers HTTP or HTTPS network access.

- Settings

Redirect to HTTPS Enable automatic redirection of HTTP requests to HTTPS port.

Save & Apply Save Reset

Figure 106: HTTPS Access

4.3.2 Startup

The **Startup** page shows the user the scripts that run when the system loads. There are two scripts on this page: **Initscripts** and **Local Startup** scripts.

4.3.2.1 Initscripts

In the Initscripts tab, there are some action buttons such as:

- **Enabled** – click once to disable the script and again to enable
- **Start** – initiates a stopped service
- **Restart** – stops and then starts the selected service
- **Stop** – stops a started service

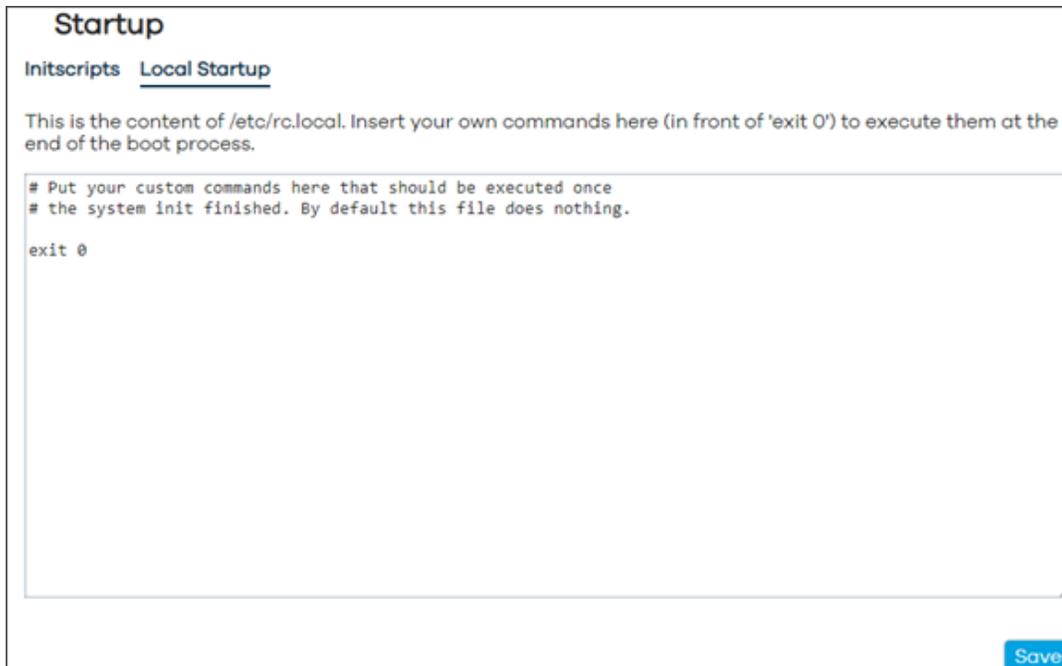
Startup			
		Initscripts	Local Startup
You can enable or disable installed init scripts here. Changes will be applied after a device reboot. Warning: If you disable essential init scripts like "network", your device might become inaccessible!			
Start priority	Initscript	Enabled	Start Restart Stop
00	urngd	Enabled	Start Restart Stop
00	sysfixtime	Enabled	Start Restart Stop
10	system	Enabled	Start Restart Stop
10	boot	Enabled	Start Restart Stop
11	fstab	Enabled	Start Restart Stop
11	sysctl	Enabled	Start Restart Stop
12	log	Enabled	Start Restart Stop
12	rpcd	Enabled	Start Restart Stop
13	awc-usb-fixup	Enabled	Start Restart Stop
14	mcu	Enabled	Start Restart Stop
15	lvm2	Enabled	Start Restart Stop
19	dropbear	Enabled	Start Restart Stop
19	wpad	Enabled	Start Restart Stop
19	firewall	Enabled	Start Restart Stop
19	dnsmasq	Enabled	Start Restart Stop
20	usbmode	Enabled	Start Restart Stop
20	network	Enabled	Start Restart Stop
35	odhcpd	Enabled	Start Restart Stop
50	cron	Enabled	Start Restart Stop

Figure 107: Startup page – Initscripts

4.3.2.2 Local Startup

In the Local Startup scripts tab, the user can add their own custom scripts or commands to the system.

! WARNING: Any additional scripts or commands should only be added by very experienced users.



Startup

[Initscripts](#) Local Startup

This is the content of `/etc/rc.local`. Insert your own commands here (in front of 'exit 0') to execute them at the end of the boot process.

```
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.

exit 0
```

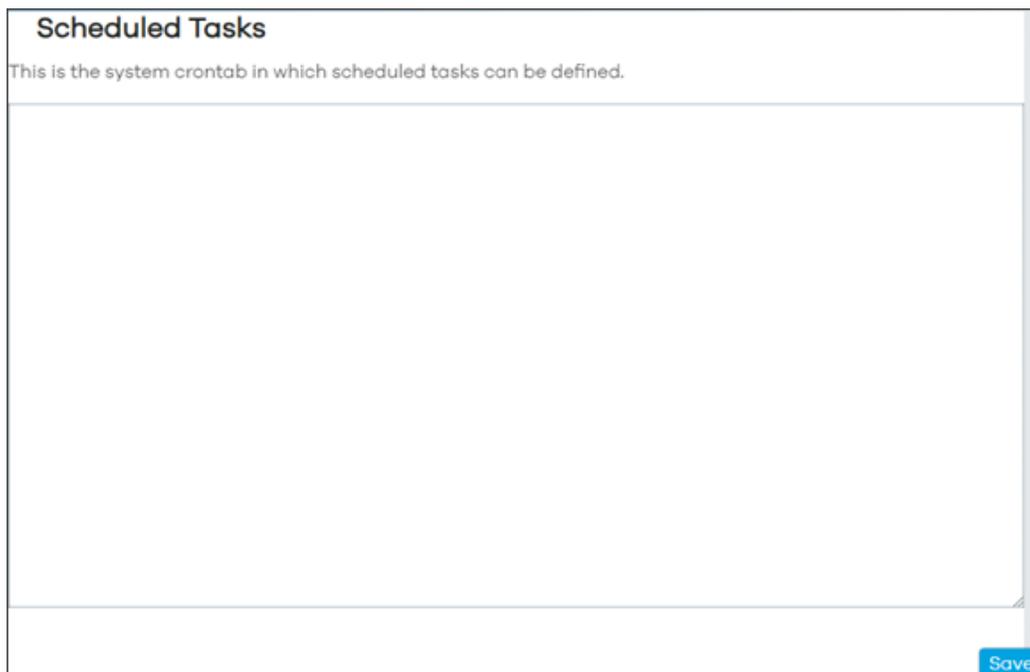
Save

Figure 108: Startup page – Local Startup

4.3.3 Scheduled Tasks

The **Scheduled Tasks** page allows the user to add their own cron jobs.

! WARNING: Cron jobs should only be added by experienced users.



Scheduled Tasks

This is the system crontab in which scheduled tasks can be defined.

Save

Figure 109: Scheduled Tasks page

4.3.4 MegaFi Configuration

This page is where the MegaFi device has most of its user configurations. There are eight sections: **Cloud**, **MegaFi Logging**, **IP Configuration**, **MegaFi and modem Configuration**, **API Configuration**, **Configuration**, **Serial Number**, and **Build Information**.

4.3.4.1 Cloud

In the Cloud section, there are multiple configurations that include:

- **UUID** – this is the device’s Universally Unique Identifier. This is a one-time assignment by the Nextivity cloud service and cannot be changed. If no UUID is present and the user wants to work with the device in the cloud, the user can contact Nextivity support team at support@nextivityinc.com.
- **Cloud Poll URL** – a URL is assigned prior to the user receiving their device and should not be changed.
- **Cloud Poll Period (seconds)** - time delay between polls. The default value is 60 seconds which is the recommended interval.
- **Cloud Status URL** – is not currently used and should be blank.
- **Cloud Status** – current connection status and reports if the Cloud is enabled and communicating.

• Cloud	
UUID	97F8B7D4-609D-4514-9F6C-A03FB694A
Cloud Poll URL	ei.awcone.com
Cloud Poll Period (seconds)	60
Cloud Status URL	
Cloud Status	Connected (10/18/2023, 12:45:13 PM)

Figure 110: MegaFi Configuration – Cloud section

4.3.4.2 MegaFi Logging

In the **MegaFi Logging** section, there are different types of logging settings that can be enabled/disabled. Though these default settings can be changed, it is strongly recommended to leave them as is:

- **Logging Enabled:** Logging enabled is the default setting
- **Push to Cloud:** Push Enabled is the default setting
- **Push to Cloud Period (seconds):** 60 seconds is the default setting
- **System Poll Period (seconds):** 15 seconds is the default setting
- **Show in Local UI:** Local UI Enabled is the default setting

• MegaFi Logging	
Logging Enabled	Logging Enabled ▼
Push to Cloud	Push Enabled ▼
Push to Cloud Period (seconds)	60
System Poll Period (seconds)	15
Show in Local UI	Local UI Enabled ▼

Figure 111: MegaFi Configuration – MegaFi Logging

4.3.4.3 NAT or Passthrough Mode

In the NAT or Passthrough Mode configuration section, the device can be put into NAT (default setting) or Passthrough Mode and the user can also update the devices' LAN IP address which sets the range.

- **Note:** Refer to section 3.11 *NAT vs. Passthrough Mode* for detailed information on configuring the mode of MegaFi.

• NAT or Passthrough Mode	
MegaFi Mode (Changing causes reboot)	NAT Mode ▼
LAN IP Address	192.168.113.1

Figure 112: MegaFi Configuration – NAT or Passthrough Mode

4.3.4.4 LAN IP Address

The LAN IP address can be updated by entering the new LAN IP address in the field.

- **Note:** Changing the LAN IP Address in this area is the same procedure that was described in *Section 3.2 Changing LAN IP Address*.
1. Enter the new IP Address in the field and hit **'Enter'**, otherwise it will revert back to default or pre-configured setting.
 2. Click on **Save & Apply** to confirm change.
 3. Give the device a few minutes for it to successfully regain network connectivity, and before attempting to reconnect to MegaFi via Mission Control or SSH.
- **Note:** The system automatically sets a Class C network and will provide IP Addresses to devices within that range as it is set as a DHCP server by default.

4.3.4.5 MegaFi and Modem Configuration

In the **MegaFi and Modem Configuration** section, the **Band Lock** can be configured to either "LTE B14 Only" or "Default Band Configuration" (default setting and involves other bands corresponding to FirstNet). Changing this setting using the **'Set Default Band Configuration'**

button will require confirmation from the user to proceed since it will cause a brief connection interruption.

- **Note:** Refer to section 3.12 *Band Lock* for more detailed information for Band Locking.

The Reboot Offline Time can be configured here 3, 5, or 10 minutes. It is disabled by default.

• **MegaFi and Modem Configuration**

Reboot Offline Time (minutes)

Band Lock

Figure 113: MegaFi Configuration – MegaFi and Modem Configuration

4.3.4.6 API Configuration

In the **API Configuration** section, there are three options that can be enabled/disabled. These APIs allow external systems to use https to gather modem status, reboot, or power cycle the MegaFi.

- **MegaFi Reboot API Enabled:** Disabled by default
- **Modem power Cycle API Enabled:** Disabled by default
- **Modem Status API Enabled:** Disabled by default

• **API Configuration**

MegaFi Reboot API Enabled

Modem Power Cycle API Enabled

Modem Status API Enabled

Figure 114: MegaFi Configuration – API Configuration

Each of these settings can be enabled via the dropdown menu and applied as follows. To change:

1. Click on the dropdown for the settings you wish to change and select the required option of **Enabled** or **Disabled**.
2. Click on the **Save** button to add this change to the list of **Unapplied Changes** and carry on making additional modifications as required; or on the **Save & Apply** button to commit the changes.
3. Once the desired API has been enabled, append the appropriate string to the end of the MegaFi's url's on a web browser or to the following curl command as follows.
 - `/cgi-bin/actions/reboot` – (will reboot MegaFi and power cycle modem)
 - `/cgi-bin/actions/power-cycle` – (will power cycle modem)

- `/cgi-bin/actions/modem-status` – (will return modem status as json)
4. Example: To get modem status with default MegaFi IP address:
 - 4a. Open a web browser and enter the following url:
<https://192.168.113.1/cgi-bin/actions/modem-status>
 - 4b. In an ssh session, enter the following command: `curl -k https://192.168.113.1/cgi-bin/actions/modem-status`

4.3.4.7 Configuration

In the **Configuration** section, the user can restore the device to default factory settings. This is the same procedure as described in *Factory Defaults via Mission Control Section 3.7*.

- 🔔 **Note:** After a factory reset, the MegaFi's UUID must be reassigned for Cloud support. Contact the support team at support@nextivityinc.com for further assistance.

To Factory Reset MegaFi:

1. Click on the **Factory Defaults** button.



Figure 115: MegaFi Configuration – Configuration

2. Confirm on the pop-up window by clicking on 'OK'.

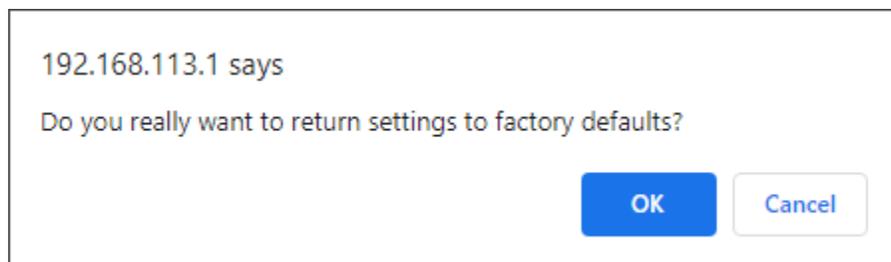


Figure 116: Confirmation message – Return to factory defaults

3. Give the device 5-15 minutes to complete the operation.
4. Once the device recovers, the user will be asked to log in to Mission Control again, using the default password located on the device's label.
5. The user will then be asked to accept the EULA agreement and change the default password.

- **Note:** For more details on Factory Defaulting the device via Mission Control or for instructions on how to factory default using the reset button on the device (in case of a forgotten password), refer to the *MegaFi User's Guide* for more information.

4.3.4.8 Serial Number

The Serial Number section provides the devices' serial number.



Figure 117: MegaFi Configuration – Serial Number

4.3.4.9 Build Information

The Build Information section provides the user with where the device was built, when it was built, skin, firmware version, git tag, and other related information.



Figure 118: MegaFi Configuration – Build Information

4.3.5 GPS Output Configuration

On this page, the user will be able to configure **GPS Server**, **GPS Internal Reporting**, and **GPS Output** (multiple outputs can be added).

GPS Output Configuration

Configure GPS output in NMEA and TAIP format to hosts

- **GPS Server**

Server Port
- **GPS Internal Reporting**

Output Format

Specify NMEA or TAIP output

NMEA station code or TAIP ID

Rate

Optional rate limit in seconds
- **GPS Output**

This section contains no values yet

[Add output](#)

[Save & Apply](#) [Save](#) [Reset](#)

Figure 119: GPS Output Configuration page

4.3.5.1 GPS Server

The user can configure a GPS Server Port in the field provided. Make sure to **'Save & Apply'** after doing so.

- **Note:** Refer to section 3.14.1 *GPS Output Configuration* for detailed instructions on how to configure a GPS Server.

4.3.5.2 GPS Internal Reporting

In this section, the user can configure the GPS Internal Reporting within MegaFi to output the GPS format in either NMEA or TAIP format, NMEA station code or TAIP ID, and Rate in seconds. By default the output format is NMEA.

• **GPS Internal Reporting**

Output Format

Specify NMEA or TAIP output

NMEA station code or TAIP ID

Rate

Optional rate limit in seconds

Figure 120: GPS Internal Reporting

1. If the user prefers to see the output format in TAIP format, click on the drop-down menu and select TAIP. The other option is Disabled.
2. To add a NMEA station code or TAIP ID, add a digit number in this field, and hit the 'Enter' button.
3. To change the rate, enter the desired rate in this field in seconds, and hit the 'Enter' button.
4. After any modifications above, click on '**Save & Apply**' to commit the changes.
5. To verify any changes made above or if in fact the output format is set to the desired language, do the following:
 - 5a. In **Expert mode**, go to **Status**, then **Modem Status**. Towards the middle of this page the information is being reported in **NMEA/TAIP Position**.

Mission Control
Networking Mode: NAT
Expert Mode


Firmware Version: 2.5.0.E.8

Modem Status

System Name	megafi-AW12	LTE Connection state	Connected
Modem Software Version	EM12AWPAR01A08M4G	Signal Percentage	90%
IMEI	015681000023929	TX Bytes	19411345
ICCID	89011003300033549470	RX Bytes	10462481
IMSI	313100003354947	TX Packets	30382
MCBV	0x260	RX Packets	26192
MCLBV	0x2000000003000281a	AT RX Bytes	19369235
Phone Number	858.914.8404	AT TX Bytes	10103120
Modem Protocol	QMI		
Latitude	32.771530		
Longitude	-117.053398		
NMEA/TAIP Position	\$GPGGA,001152.000,3246.29164,N,11703.20437,W,2,14,0.8,144.7,M,-34.9,M,0.000,*43		
GPS UTC Timestamp	Fri Jul 19 2024 17:11:59 GMT-0700 (Pacific Daylight Time)		
APN	firstnet-broadband	Mode	LTE
Home Network MCC	310	ID	79498159
Home Network MNC	410	PID	248
Home Network Name	FirstNet	EARFCN	5330
		FB	14
		ULB	10MHz
		DLB	10MHz
PDP IP Address	10.226.240.109	TAC	33545
UE RSSI	-61 dBm	RSRP	-90 dBm
UE Qual	26	RSRQ	-14 dB
QMI SC SNR	12.00 dB	RSSI	-61 dBm
QMI CA Band	66	SINR	-18.0 dB
		TX Power	11.0 dBm
QMI RX C0 Power	-58.0 dBm	QMI RX C1 Power	-62.6 dBm
QMI RX C0 ECIO	14.30 dB	QMI RX C1 ECIO	12.50 dB
QMI RX C0 RSRP	89.30 dBm	QMI RX C1 RSRP	92.00 dBm
QMI RX C0 Phase	0.00 degrees	QMI RX C1 Phase	0.00 degrees

Figure 121: NMEA/TAIP Position

4.3.5.3 GPS Output

To enable a remote server to receive the GPS information, start by clicking the **'Add output'** as shown in light blue on the lower left of the screen and follow the prompts to implement the format needed for your remote server environment. When adding an output, the available fields are:

- **Note:** Refer to section 3.14.3 *GPS Output* for detailed instructions on how to configure a GPS Output.

4.3.6 Flash Firmware

All firmware-related actions can be performed on this page and is similar to another area withing Mission Control where these same actions can be accomplished.

- **Note:** Backup, Restore, and Flash new firmware image were already previously described in sections 3.4 – Backup Existing Configuration, 3.5 – Load Configuration from File, and 3.3 – Flash/Update Firmware.

Flash operations

Actions

- **Backup**

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup Generate archive

- **Restore**

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Restore backup Upload archive...

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

- **Flash new firmware image**

Upload a sysupgrade-compatible image here to replace the running firmware.

Image Flash image...

- **Available Firmware**

Firmware available in the Cloud

None Available

Save & Apply Save Reset

Figure 122: Flash Operations page

4.3.6.1 Backup

Backup – generate a backup and download/save current configuration files. The '**Generate archive**' button will compile the configuration files as a .tar file and will automatically download to the default download folder.

4.3.6.2 Restore

Restore – user can restore from a previously generated backup. The user would simply browse for the .tar file that was generated during a Backup action as previously shown. Click on **Upload archive** button, browse for the preferred .tar file and select 'Upload' to start the process.



Figure 123: Flash Firmware – After clicking Upload Archive button

The system validates the contents of the archive and asks the user to confirm by selecting 'Continue'.

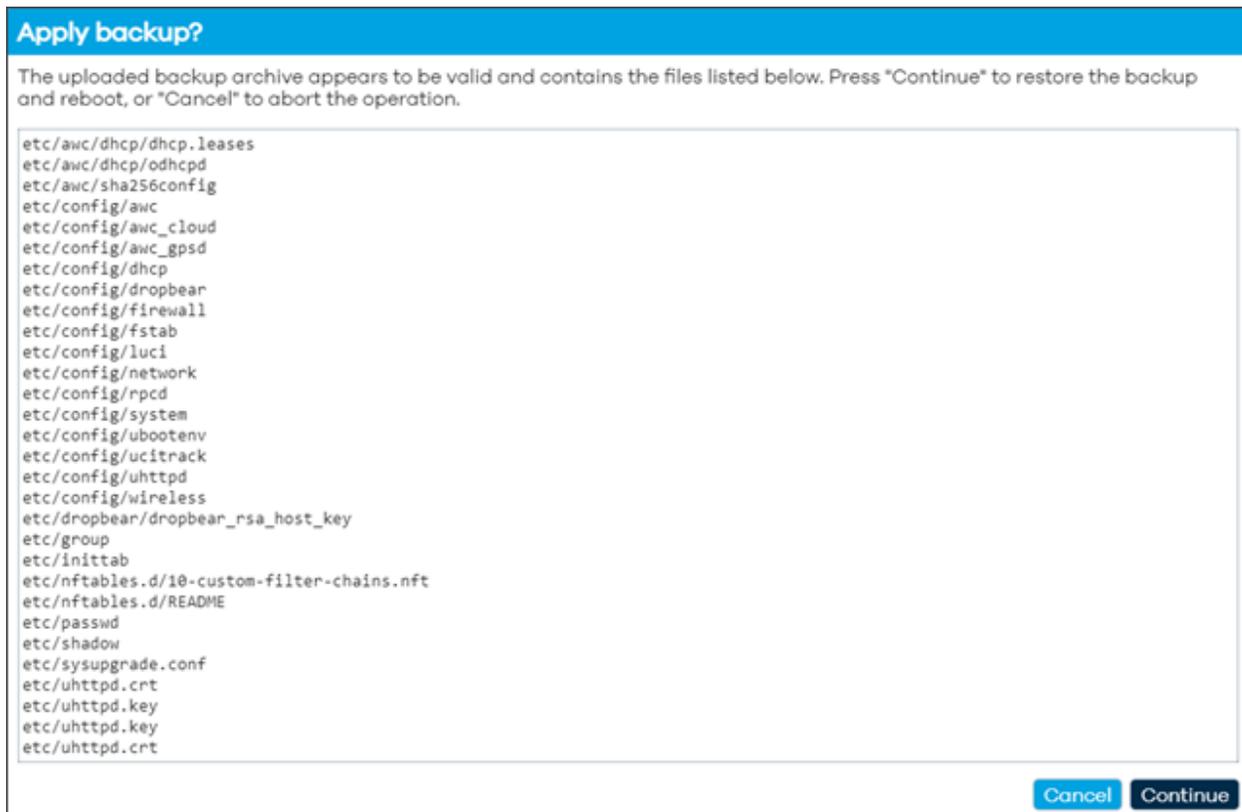


Figure 124: Apply backup? page – prompting to continue to restore the backup

- **Note:** Some custom files, such as certificates or scripts, may remain on the system; therefore, it is recommended to perform a Factory Reset before restoring/deploying a backup.

4.3.6.3 Flash new firmware image

The user will be able to update firmware manually if they have an available firmware file downloaded onto their personal computer. To do so:

1. Click on **Flash image...**
2. Select **Browse** to locate the appropriate firmware file on your computer (BIN file).



Figure 125: Uploading file window prompting user to select the file to upload

3. Select **Upload** to begin the update.
4. A status bar will briefly indicate the upload of the file, followed by a '**Flash image?**' pop-up message. The pop-up cautions the user to validate that the firmware file is corrupt-free by comparing the original file size and SHA256 checksum. Select **Continue** only if the file size and SHA256 checksum match. Notice that by default, the 'Keep settings and retain the current configuration' box is checked. It is recommended to leave this box checked.



Figure 126: Message prompting user to compare original file size and checksum

5. The unit will begin 'Flashing...'

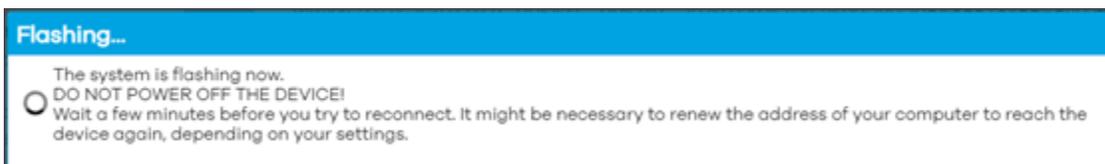


Figure 127: Message indicating flashing is in progress

! WARNING: DO NOT POWER OFF THE DEVICE! – The update process will take about 5 minutes to complete.

6. After the upload completes, the user may need to refresh their web browser and/or reconnect to MegaFi's Wi-Fi connection to regain access.

4.3.6.4 Available Firmware

If there is a new version of firmware available to download from the cloud, it will show up listed here. Follow the prompts to update the firmware of the device. Otherwise, the button will be labeled as '**None Available**'.

4.3.7 Reboot

This page contains a “Perform reboot” option that will restart the unit.

- ➔ **Note:** Clicking the **Perform reboot** button will perform an immediate reboot with no warning.
- ➔ **Note:** This is similar to what was previously detailed in section 3.9.



Figure 128: Reboot page – Perform reboot button

If there are unsaved changes, a message will indicate this as such:

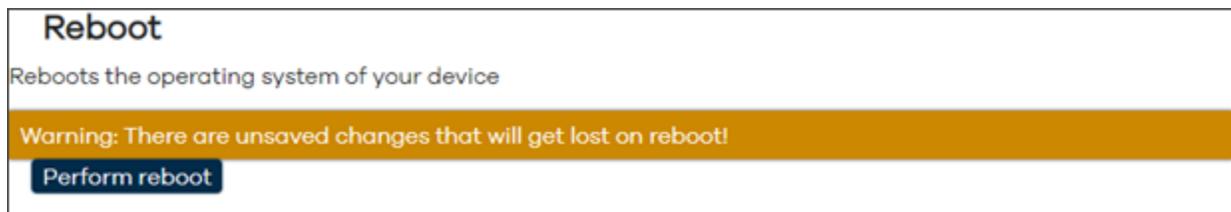


Figure 129: Warning Message – Unsaved changes

4.4 Network

The **Network** section will allow the user to setup, configure, and manage the devices' network. Sub-sections under this page include **Interfaces**, **Wireless**, **Routing**, **DHCP and DNS**, **Diagnostics**, and **Firewall**.



Figure 130: Navigation pane – Network menu

4.4.1 Interfaces

The Interfaces page has three tabs: **Interfaces**, **Devices**, and **Global network options**.

The screenshot shows the 'Interfaces' tab with the following details:

Interface	Protocol	Uptime	MAC	RX	TX	IPv4	IPv6	IPv6-PD	Actions
lan	Static address	2h 19m 3s	34:BA:9A:7B:65:2F	12.56 MB (60458 Pkts.)	104.53 MB (92427 Pkts.)	192.168.113.1/24	2600:380:3080:cd4a::1/64		Restart, Stop, Edit
wan	DHCP client		34:BA:9A:7B:65:30	0 B (0 Pkts.)	0 B (0 Pkts.)				Restart, Stop, Edit
wwan	ModemManager	2h 18m 19s	3A:AA:10:84:9B:C9	87.05 MB (75086 Pkts.)	10.45 MB (48219 Pkts.)	10.222.229.171	2600:380:3080:cd4a:74d1:d43e:4a0f:be3e		Restart, Stop, Edit

Figure 131: Interfaces page – Interfaces tab

4.4.1.1 Interfaces

Within the **Interfaces** tab, there should be a **lan**, **wan**, and **wwan** interface shown by default. Each interface will show some statistics for each interface such as:

- **Protocol** currently configured for the interface
- **Uptime** for the interface
- **MAC** address for the interface
- **RX** and **TX** data
- **IPv4** and **IPv6** addresses if any

Next to each interface, there are three actions that are available: **Restart**, **Stop**, and **Edit**.

- **Restart**: selecting this option will immediately reconnect that interface – take caution before selecting this option as it will momentarily disrupt connectivity.
- **Stop**: selecting this option will immediately shut down that particular – take caution as this will disrupt connectivity.
- **Edit**: choose this option to edit the port

Ian Edit

Under **Edit**, there are four tabs available: **General Settings**, **Advanced Settings**, **Firewall Settings**, and **DHCP Server** for each interface.

In **General Settings** for the LAN interface, it shows the following information:

! WARNING: This is an Edit page from the LAN interface. The other interfaces (WAN and WWAN) have a number of different configuration options under their respective **Edit** pages and should only be updated by experienced users.

- **Status:** Device, Uptime, MAC address, RX and TX data, IPv4 and IPv6 IP addresses
- **Protocol:** defaults to the Static address of **192.168.113.1**.
 - Other options are **DHCP client**, **DHCPv6 client**, **GRE tunnel over IPv4**, **GRETAP tunnel over IPv4**, **GRE tunnel over IPv6**, **GRETAP tunnel over IPv6**, **ModemManager**, and **Unmanaged**.
- **Device:** defaults to **Bridge: "br-lan" (LAN)**. Other options are available to change the type of interface, though it is not recommended to make any changes as doing so may render your device unusable.
- **Bring up on boot:** checked by default
- **IPv4 address:** default is **192.168.113.1/24**
- **IPv4 netmask:** default is **255.255.255.0**. Other options are available in the drop-down menu as well as configuring a custom netmask.
- **IPv4 gateway:** this is automatically derived from the carrier and not configurable
- **IPv4 broadcast:** this is automatically derived from the IPv4 address setting above and not configurable.

The screenshot shows the configuration page for the LAN interface. The 'General Settings' tab is active. The configuration fields are as follows:

Field	Value
Status	Device: br-lan Uptime: 2h 20m 10s MAC: 34:BA:9A:78:65:2F RX: 13.04 MB (60936 Pkts.) TX: 104.90 MB (93035 Pkts.) IPv4: 192.168.113.1/24 IPv6: 2600:380:3080:cd4a::1/64 IPv6: fdb3:9ddad0::1/60
Protocol	Static address
Device	br-lan
Bring up on boot	<input checked="" type="checkbox"/>
IPv4 address	192.168.113.1
IPv4 netmask	255.255.255.0
IPv4 gateway	10.222.229.172 (wwan)
IPv4 broadcast	192.168.113.255

Buttons: Dismiss, Save

Figure 132: Interfaces > lan – General Settings tab

In **Advanced Settings** for the LAN interface, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Force link:** box is checked by default. Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).
- **Use default gateway:** box is checked by default. If unchecked, no default route is configured.
- **Use custom DNS servers:** None configured by default
- **DNS search domains:** None configured by default
- **DNS weight:** set to 0 by default. The DNS server entries in the local resolv.conf are primarily sorted by the weight specified here.
- **Use gateway metric:** set to **0** by default
- **Override IPv4 routing table:** set to '**unspecified**' by default. Other options are: **prelocal (128)**, **local (255)**, **main (254)**, **default (253)**, and custom setting
- **Override IPv6 routing table:** set to 'unspecified' by default. Other options are: **prelocal (128)**, **local (255)**, **main (254)**, **default (253)**, and custom setting
- **Delegate IPv6 prefixes:** checked by default. Enable downstream delegation of IPv6 prefixes available on this interface.
- **IPv6 assignment length:** set to **60** by default.
 - Other options are: disabled, 64, or custom setting. Assign a part of given length of every public IPv6-prefix to this interface.
- **IPv6 assignment hint:** set to **0** by default. Assign prefix parts using this hexadecimal subprefix ID for this interface.
- **IPv6 prefix filter:** no value set by default. Options are **local (Local ULA)**, **wwan**, or custom setting. If set, downstream subnets are only allocated from the given IPv6 prefix classes.
- **IPv6 suffix:** set to **::1** by default. Optional. Allowed values: 'eui64', 'random', fixed value like '::1' or '::1:2'. When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like '::1') to form the IPv6 address ('a:b:c:d::1') for the interface.
- **IPv6 preference:** set to **0** by default. When delegating prefixes to multiple downstreams, interfaces with a higher preference value are considered first when allocating subnets.

Interfaces > lan

General Settings Advanced Settings Firewall Settings DHCP Server

Force link Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).

Use default gateway If unchecked, no default route is configured

Use custom DNS servers +

DNS search domains +

DNS weight The DNS server entries in the local resolv.conf are primarily sorted by the weight specified here

Use gateway metric

Override IPv4 routing table ▼

Override IPv6 routing table ▼

Delegate IPv6 prefixes Enable downstream delegation of IPv6 prefixes available on this interface

IPv6 assignment length Assign a part of given length of every public IPv6-prefix to this interface

IPv6 assignment hint Assign prefix parts using this hexadecimal subprefix ID for this interface.

IPv6 prefix filter ▼ If set, downstream subnets are only allocated from the given IPv6 prefix classes.

IPv6 suffix Optional. Allowed values: 'eui64', 'random', fixed value like ':1' or ':1:2'. When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like ':1') to form the IPv6 address ('a:b:c:d:1') for the interface.

IPv6 preference When delegating prefixes to multiple downstreams, interfaces with a higher preference value are considered first when allocating subnets.

Dismiss Save

Figure 133: Interfaces > lan – Advanced Settings

In **Firewall Settings** for the lan interface, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Create/Assign firewall-zone:** set to **lan** by default. Other options are: **wan**, **wwan**, **unspecified**, and custom setting. Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the custom field to define a new zone and attach the interface to it.



Figure 134: Interfaces > lan – Firewall Settings

In **DHCP Server, General Setup** settings for the lan interface, it shows the following information:

! **WARNING:** Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Ignore interface:** unchecked by default. If checked, disables DHCP for this interface.
- **Start:** set to 100 by default. Lowest leased address as offset from the network address.
- **Limit:** set to 150 by default. Maximum number of leased addresses.
- **Lease time:** set to 12h by default. Expiry time of leased addresses, minimum is 2 minutes (2m).

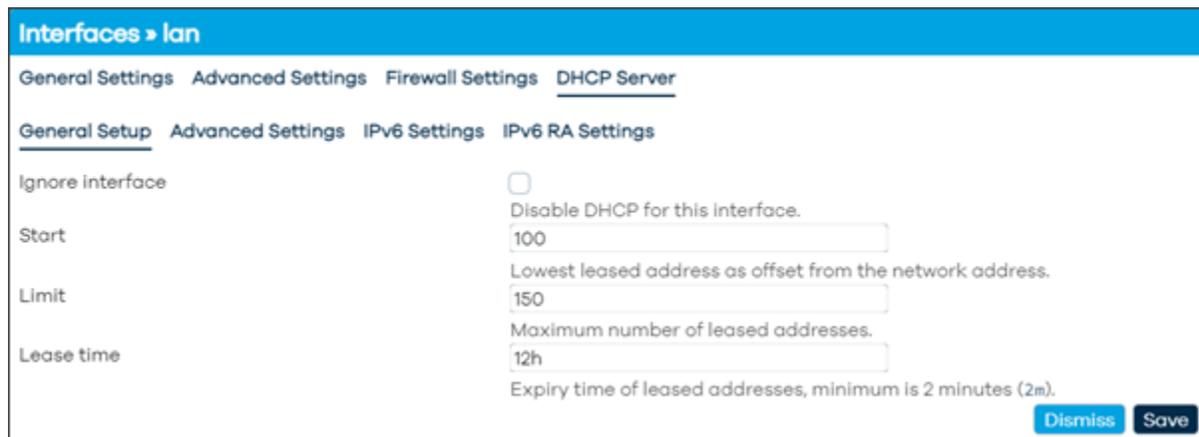


Figure 135: Interfaces > lan – DHCP Server, General Setup

In **DHCP Server, Advanced Settings** for the **lan** interface, it shows the following information:

! **WARNING:** Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Dynamic DHCP:** checked by default. Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
- **Force:** unchecked by default. Force DHCP on this network even if another server is detected.

- **IPv4-Netmask:** set to **255.255.255.0** by default. Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
- **DHCP-Options:** left blank by default. Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

The screenshot shows the configuration page for the DHCP Server on the 'lan' interface. The 'Advanced Settings' tab is selected. The 'Dynamic DHCP' checkbox is checked. The 'Force' checkbox is unchecked. The 'IPv4-Netmask' is set to '255.255.255.0'. The 'DHCP-Options' field is empty. There are 'Dismiss' and 'Save' buttons at the bottom right.

Figure 136: Interfaces > lan – DHCP Server, Advanced Settings

In **DHCP Server, IPv6 Settings** for the **lan** interface, it shows the following information:

! **WARNING:** Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Designated master:** unchecked by default. Set this interface as master for RA and DHCPv6 relaying as well as NDP proxying.
- **RA-Service:** set to **server mode** by default which sends RA messages advertising this device as IPv6 router.
 - Other options are: **disabled** which does not send any RA messages on this interface; **relay mode** which forwards RA messages received on the designated master interface to downstream interfaces; **hybrid mode** which operates in **relay mode** if a designated master interface is configured and active, otherwise fall back to server mode.
- **DHCPv6-Service:** set to server mode by default which provides a DHCPv6 server on this interface and reply to DHCPv6 solicitations and requests.
 - Other options are: **disabled** which does not offer DHCPv6 service on this interface; **relay mode** which forwards DHCPv6 messages between the designated master interface and downstream interfaces; **hybrid mode** which operates in **relay mode** if a designated master interface is configured and active, otherwise fall back to server mode.

- **Announced IPv6 DNS servers:** left blank by default. Specifies a fixed list of IPv6 DNS server addresses to announce via DHCPv6. If left unspecified, the device will announce itself as IPv6 DNS server unless the Local IPv6 DNS server option is disabled.
- **Local IPv6 DNS server:** checked by default. Announce this device as IPv6 DNS server.
- **Announced DNS domains** – left blank by default. Specifies a fixed list of DNS search domains to announce via DHCPv6. If left unspecified, the local device DNS search domain will be announced.
- **NDP-Proxy:** Configures the operation mode of the NDP proxy service on this interface. Set to disabled by default which does not proxy any NDP packets.
 - Other options are: **relay mode** which forwards NDP NS and NA messages between the designated master interface and downstream interfaces; **hybrid mode** which operates in **relay mode** if a designated master interface is configured and active, otherwise disable NDP proxying.

Interfaces > lan

General Settings
Advanced Settings
Firewall Settings
DHCP Server

General Setup
Advanced Settings
IPv6 Settings
IPv6 RA Settings

Designated master	<input type="checkbox"/>	Set this interface as master for RA and DHCPv6 relaying as well as NDP proxying.
RA-Service	<input type="text" value="server mode"/>	Configures the operation mode of the RA service on this interface.
DHCPv6-Service	<input type="text" value="server mode"/>	Configures the operation mode of the DHCPv6 service on this interface.
Announced IPv6 DNS servers	<input type="text" value=""/>	Specifies a fixed list of IPv6 DNS server addresses to announce via DHCPv6. If left unspecified, the device will announce itself as IPv6 DNS server unless the <i>Local IPv6 DNS server</i> option is disabled.
Local IPv6 DNS server	<input checked="" type="checkbox"/>	Announce this device as IPv6 DNS server.
Announced DNS domains	<input type="text" value=""/>	Specifies a fixed list of DNS search domains to announce via DHCPv6. If left unspecified, the local device DNS search domain will be announced.
NDP-Proxy	<input type="text" value="disabled"/>	Configures the operation mode of the NDP proxy service on this interface.

Figure 137: Interfaces > lan – DHCP Server, IPv6 Settings

In **DHCP Server, IPv6 RA Settings** for the **lan** interface, it shows the following information:

! **WARNING:** Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Default router** - Configures the default router advertisement in RA messages. Set to automatic by default which announces this device as the default router if a local IPv6 default route is present.
 - Other options are: **on available prefix** which announces this device as default router if a public IPv6 prefix is available, regardless of local default router availability; **forced** which announces this device as default router regardless of whether a prefix or default route is present.
- **Enable SLAAC:** checked by default. Set the autonomous address-configuration flag in the prefix information options of sent RA messages. When enabled, clients will perform stateless IPv6 address autoconfiguration.
- **RA Flags:** Specifies the flags sent in RA messages, for example to instruct clients to request further information via stateful DHCPv6. Is set to both **managed config (M)** which indicates that the IPv6 addresses are available via DHCPv6 and **other (O)** which indicates that other information, such as DNS servers, is available via DHCPv6 by default.
 - Other option is: **mobile home agent (H)** which indicates that the device is also acting as Mobile IPv6 home agent on this link.
- **Max RA interval** (seconds) : set to **600** by default. Maximum time allowed between sending unsolicited RA.
- **Min RA interval** (seconds) : set to **200** by default. Minimum time allowed between sending unsolicited RA.
- **RA Lifetime** (seconds) : set to **1800** by default. Router Lifetime published in RA messages. Maximum is 9000 seconds.
- **RA MTU** (bytes) : set to **1342** by default. The MTU to be published in RA messages. Minimum is 1280 bytes.
- **RA Hop Limit:** set to **64** by default. The maximum hops to be published in RA messages. Maximum is 255 hops.

Interfaces > lan

General Settings Advanced Settings Firewall Settings DHCP Server

General Setup Advanced Settings IPv6 Settings IPv6 RA Settings

Default router: automatic
Configures the default router advertisement in RA messages.

Enable SLAAC:
Set the autonomous address-configuration flag in the prefix information options of sent RA messages. When enabled, clients will perform stateless IPv6 address autoconfiguration.

RA Flags: managed config (M) | other config (O)
Specifies the flags sent in RA messages, for example to instruct clients to request further information via stateful DHCPv6.

Max RA interval: 600
Maximum time allowed between sending unsolicited RA. Default is 600 seconds.

Min RA interval: 200
Minimum time allowed between sending unsolicited RA. Default is 200 seconds.

RA Lifetime: 1800
Router Lifetime published in RA messages. Maximum is 9000 seconds.

RA MTU: 1342
The MTU to be published in RA messages. Minimum is 1280 bytes.

RA Hop Limit: 64
The maximum hops to be published in RA messages. Maximum is 255 hops.

[Dismiss](#) [Save](#)

Figure 138: Interfaces > lan – DHCP Server, IPv6 RA Settings tab

wan Edit

In **General Settings** for the wan interface, it shows the following information:

! WARNING: This is an **Edit** page from the WAN interface. The other interfaces (LAN and WWAN) have a number of different configuration options under their respective Edit pages and should only be updated by experienced users.

- **Status:** Device, MAC address, RX and TX data
- **Protocol:** Defaults to **DHCP client**.
 - Other options are **DHCPv6 client**, **GRE tunnel over IPv4**, **GRETAP tunnel over IPv4**, **GRE tunnel over IPv6**, **GRETAP tunnel over IPv6**, **ModemManager**, **Unmanaged**, and **Static Address**.
- **Device:** Defaults to **Switch port: “wan” (wan)**. Other options are available to change the type of interface, though it is not recommended to make any changes as doing so may render your device unusable.
- **Bring up on boot:** Box is checked by default.
- **Hostname to send when requesting DHCP:** Default value is ‘**Send the hostname of this device**’.

- Other options are '**Do not send a hostname**' and the user can specify a custom value a well.

The screenshot shows the configuration page for the 'wan' interface. The 'General Settings' tab is active. The 'Status' field is empty. The 'Protocol' is set to 'DHCP client'. The 'Device' is set to 'wan'. The 'Bring up on boot' checkbox is checked. The 'Hostname to send when requesting DHCP' is set to 'Send the hostname of this device'. A tooltip for the 'Device' field displays: Device: wan, MAC: FE:34:BA:9A:94:68, RX: 0 B (0 Pkts.), TX: 0 B (0 Pkts.).

Figure 139: Interfaces > wan – General Settings tab

In **Advanced Settings** for the wan interface, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

- Force link:** box is unchecked by default. Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).
- Use broadcast flag:** box is unchecked by default. Required for certain ISPs, e.g. Charter with DOCSIS 3.
- Client ID to send when requesting DHCP:** left blank by default
- Vendor Class to send when requesting DHCP:** left blank by default
- Use default gateway:** box is checked by default. If unchecked, no default route is configured.
- Use DNS servers advertised by peers:** box is checked by default. If unchecked, the advertised DNS server addresses are ignored.
- DNS weight:** set to **0** by default. The DNS server entries in the local resolv.conf are primarily sorted by the weight specified here.
- Use gateway metric:** set to **0** by default
- Override IPv4 routing table:** set to '**unspecified**' by default. Other options are: prelocal (128), local (255), main (254), default (253), and custom setting
- Override IPv6 routing table:** set to '**unspecified**' by default. Other options are: prelocal (128), local (255), main (254), default (253), and custom setting
- Delegate IPv6 prefixes:** box is checked by default. Enable downstream delegation of IPv6 prefixes available on this interface.
- IPv6 assignment length:** set to **disabled** by default. Other options are: 64, or custom setting. Assign a part of given length of every public IPv6-prefix to this interface.

- **IPv6 prefix filter:** no value set by default. Options are local (Local ULA), wwan, or custom setting. If set, downstream subnets are only allocated from the given IPv6 prefix classes.
- **IPv6 suffix:** set to `::1` by default. Optional. Allowed values: 'eui64', 'random', fixed value like `::1` or `::1:2`. When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like `::1`) to form the IPv6 address ('a:b:c:d::1') for the interface.
- **IPv6 preference:** set to `0` by default. When delegating prefixes to multiple downstreams, interfaces with a higher preference value are considered first when allocating subnets.

Interfaces > wan

General Settings
Advanced Settings
Firewall Settings
DHCP Server

Force link	<input type="checkbox"/>	Set interface properties regardless of the link carrier (if set, carrier sense events do not invoke hotplug handlers).
Use broadcast flag	<input type="checkbox"/>	Required for certain ISPs, e.g. Charter with DOCSIS 3
Client ID to send when requesting DHCP	<input type="text"/>	
Vendor Class to send when requesting DHCP	<input type="text"/>	
Use default gateway	<input checked="" type="checkbox"/>	If unchecked, no default route is configured
Use DNS servers advertised by peer	<input checked="" type="checkbox"/>	If unchecked, the advertised DNS server addresses are ignored
DNS weight	<input type="text" value="0"/>	The DNS server entries in the local resolv.conf are primarily sorted by the weight specified here
Use gateway metric	<input type="text" value="0"/>	
Override IPv4 routing table	<input type="text" value="unspecified"/>	
Override IPv6 routing table	<input type="text" value="unspecified"/>	
Delegate IPv6 prefixes	<input checked="" type="checkbox"/>	Enable downstream delegation of IPv6 prefixes available on this interface
IPv6 assignment length	<input type="text" value="disabled"/>	
IPv6 prefix filter	<input type="text" value="-- Please choose --"/>	Assign a part of given length of every public IPv6-prefix to this interface
IPv6 suffix	<input type="text" value="::1"/>	If set, downstream subnets are only allocated from the given IPv6 prefix classes. Optional. Allowed values: 'eui64', 'random', fixed value like <code>::1</code> or <code>::1:2</code> . When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like <code>::1</code>) to form the IPv6 address ('a:b:c:d::1') for the interface.
IPv6 preference	<input type="text" value="0"/>	When delegating prefixes to multiple downstreams, interfaces with a higher preference value are considered first when allocating subnets.

Dismiss
Save

Figure 140: Interfaces > wan – Advanced Settings tab

In **Firewall Settings** for the **wan** interface, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

Create/Assign firewall-zone: set to **wan** and **wwan** by default. Other options are: **lan**, **unspecified**, and custom setting. Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the custom field to define a new zone and attach the interface to it.

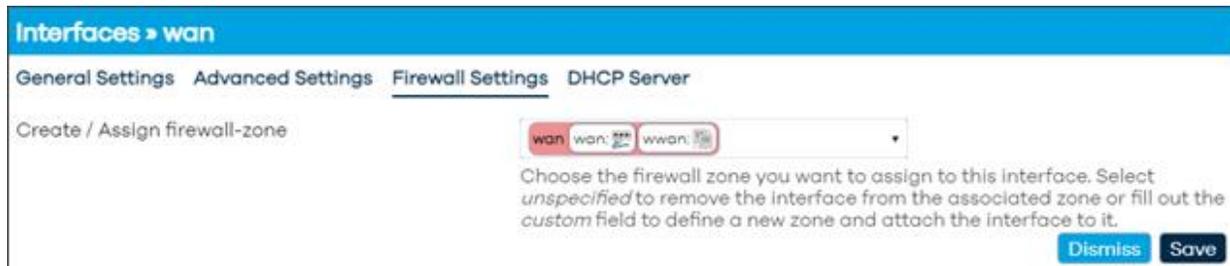


Figure 141: Interfaces > wan page – Firewall Settings tab

In **DHCP Server, General Setup** settings for the wan interface, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Ignore interface:** box is checked by default. If checked, disables DHCP for this interface.

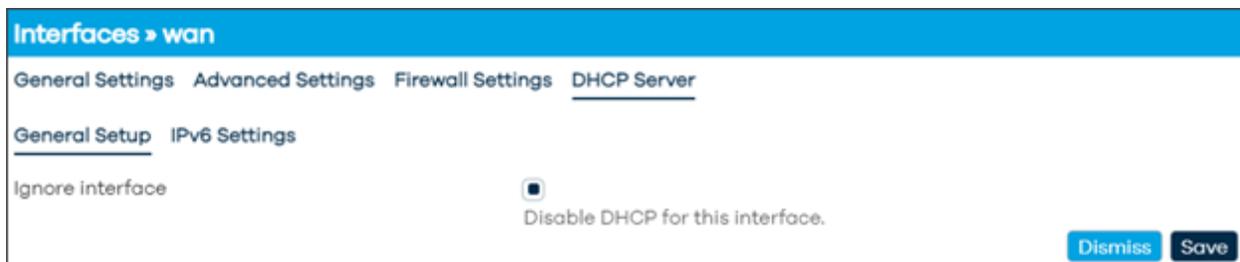


Figure 142: Interfaces > wan page – DHCP Server tab

In **DHCP Server, IPv6 Settings** for the wan interface, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Designated master:** box is unchecked by default. Set this interface as master for RA and DHCPv6 relaying as well as NDP proxying.

- **RA-Service:** set to disabled by default which does not send any RA messages on this interface. Other options are: server mode which sends RA messages advertising this device as IPv6 router; relay mode which forwards RA messages received on the designated master interface to downstream interfaces; hybrid mode which operates in relay mode if a designated master interface is configured and active, otherwise fall back to server mode.
- **DHCPv6-Service:** set to disabled by default which does not offer DHCPv6 service on this interface. Other options are: server mode which provides a DHCPv6 server on this interface and reply to DHCPv6 solicitations and requests; relay mode which forwards DHCPv6 messages between the designated master interface and downstream interfaces; hybrid mode which operates in relay mode if a designated master interface is configured and active, otherwise fall back to server mode.
- **NDP-Proxy:** Configures the operation mode of the NDP proxy service on this interface. Set to disabled by default which does not proxy any NDP packets.
 - Other options are: **relay mode** which forwards NDP NS and NA messages between the designated master interface and downstream interfaces; **hybrid mode** which operates in **relay mode** if a designated master interface is configured and active, otherwise disable NDP proxying.

The screenshot shows the configuration page for the 'wan' interface, specifically the 'DHCP Server' tab and 'IPv6 Settings' sub-tab. The 'Designated master' checkbox is unchecked. The 'RA-Service', 'DHCPv6-Service', and 'NDP-Proxy' dropdown menus are all set to 'disabled'. The 'Dismiss' and 'Save' buttons are visible at the bottom right.

Figure 143: Interfaces > wan – DHCP Server – IPv6 Settings tab

wwan Edit

In **General Settings** for the **wwan** interface, it shows the following information:

! WARNING: This is an Edit page from the WWAN interface. The other interfaces (LAN and WAN) have a number of different configurations under their respective Edit pages and should only be updated by experienced users.

- **Status:** Device, Uptime, MAC address, RX and TX data, IPv4, IPv6, and IPv6-PD
- **Protocol:** defaults to **ModemManager**.
 - Other options are **DHCP client**, **DHCPv6 client**, **GRE tunnel over IPv4**, **GRETAP tunnel over IPv4**, **GRE tunnel over IPv6**, **GRETAP tunnel over IPv6**, **Unmanaged**, and **Static Address**
- **Bring up on boot:** box is checked by default
- **Modem device:** defaults to Nextivity Inc. – AW-12
- **APN:** firstnet-broadnet or user may configure to a customer specific APN
- **PIN:** default is blank
- **Authentication Type:** default is set to 'None'.
 - Other choices are: **PAP/CHAP(both)**, **PAP**, or **CHAP**
- **IP Type:** default is **IPv4/IPv6 (both – defaults to IPv4)**.
 - Other choices are: **IPv4 only**, **IPv6 only**
- **Signal Refresh Rate (in seconds):** default is blank.

The screenshot shows the 'wwan' configuration page with the following settings:

- Status:** Device: modemmanager-wwan, RX: 0 B (0 Pkts.), TX: 0 B (0 Pkts.), Error: Network device is not present.
- Protocol:** ModemManager
- Bring up on boot:**
- Modem device:** Nextivity Inc. – AW-12
- APN:** firstnet-broadband
- PIN:** (blank)
- Authentication Type:** None
- IP Type:** IPv4/IPv6 (both - defaults to IPv4)
- Signal Refresh Rate:** (blank) In seconds

Buttons: Dismiss, Save

Figure 144: Interfaces > wwan page – General Settings tab

In **Advanced Settings** for the **wwan** interface, it shows the following information:

! **WARNING:** Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Force link:** box is unchecked by default. Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).
- **Override MTU:** default is set to **1342**
- **Use default gateway:** box is checked by default. If unchecked, no default route is configured.
- **Use custom DNS servers:** left blank by default
- **DNS weight:** set to **0** by default. The DNS server entries in the local resolv.conf are primarily sorted by the weight specified here.
- **Use gateway metric:** set to **10** by default
- **Override IPv4 routing table:** set to 'unspecified' by default. Other options are: **prelocal (128)**, **local (255)**, **main (254)**, **default (253)**, and custom setting
- **Override IPv6 routing table:** set to 'unspecified' by default. Other options are: **prelocal (128)**, **local (255)**, **main (254)**, **default (253)**, and custom setting
- **Delegate IPv6 prefixes:** box is checked by default. Enable downstream delegation of IPv6 prefixes available on this interface.
- **IPv6 assignment length:** set to disabled by default. Other options are: **64**, or custom setting. Assign a part of given length of every public IPv6-prefix to this interface.
- **IPv6 prefix filter:** no value set by default. Options are local (Local ULA), wwan, or custom setting. If set, downstream subnets are only allocated from the given IPv6 prefix classes.
- **IPv6 suffix:** set to **::1** by default. Optional.
 - Allowed values: 'eui64', 'random', fixed value like '::1' or '::1:2'. When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like '::1') to form the IPv6 address ('a:b:c:d::1') for the interface.
- **IPv6 preference:** set to **0** by default. When delegating prefixes to multiple downstreams, interfaces with a higher preference value are considered first when allocating subnets.

Interfaces > wwan

General Settings
Advanced Settings
Firewall Settings
DHCP Server

Force link	<input type="checkbox"/>	Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).
Override MTU	<input type="text" value="1342"/>	
Use default gateway	<input checked="" type="checkbox"/>	If unchecked, no default route is configured
Use custom DNS servers	<input type="text" value=""/>	<input style="background-color: #0070c0; color: white; border: none; padding: 2px 5px; font-size: 10px; vertical-align: middle;" type="button" value="+"/>
DNS weight	<input type="text" value="0"/>	The DNS server entries in the local resolv.conf are primarily sorted by the weight specified here
Use gateway metric	<input type="text" value="10"/>	
Override IPv4 routing table	<input type="text" value="unspecified"/>	▼
Override IPv6 routing table	<input type="text" value="unspecified"/>	▼
Delegate IPv6 prefixes	<input checked="" type="checkbox"/>	Enable downstream delegation of IPv6 prefixes available on this interface
IPv6 assignment length	<input type="text" value="disabled"/>	▼
IPv6 prefix filter	<input type="text" value="-- Please choose --"/>	▼
IPv6 suffix	<input type="text" value="::1"/>	Optional. Allowed values: 'eui64', 'random', fixed value like ':1' or ':1:2'. When IPv6 prefix (like 'a:b:c:d:') is received from a delegating server, use the suffix (like ':1') to form the IPv6 address ('a:b:c:d::1') for the interface.
IPv6 preference	<input type="text" value="0"/>	When delegating prefixes to multiple downstreams, interfaces with a higher preference value are considered first when allocating subnets.

Figure 145: Interfaces > wwan page – Advanced Settings tab

In **Firewall Settings** for the **wwan** interface, it shows the following information:

! **WARNING:** Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Create/Assign firewall-zone:** set to **wan** and **wwan** by default. Other options are: **lan**, **unspecified**, and custom setting. Choose the firewall zone you want to assign to this interface. Select **unspecified** to remove the interface from the associated zone or fill out the custom field to define a new zone and attach the interface to it.

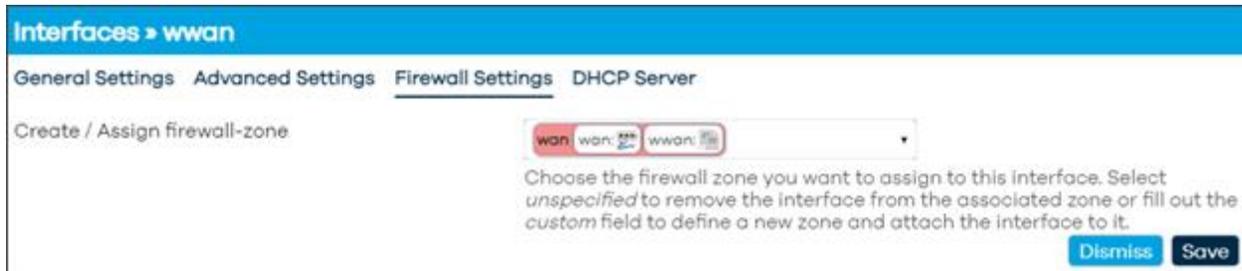


Figure 146: Interfaces > wwan page – Firewall Settings tab

In **DHCP Server** settings for the **wwan** interface, there is no DHCP Server configured for this interface by default.

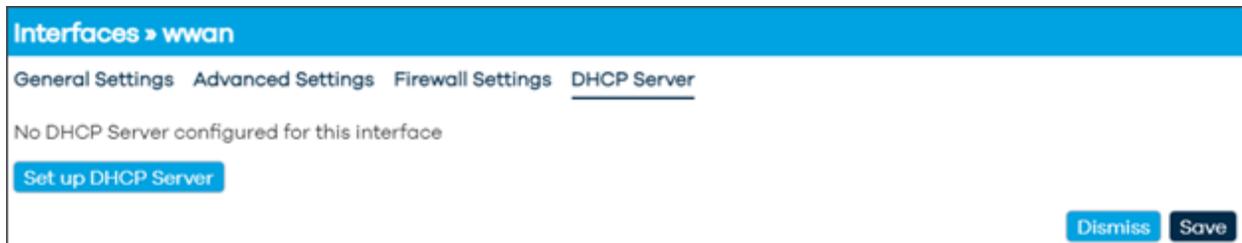


Figure 147: Interfaces > wwan page – DHCP Server settings tab

However, a user can configure one if they wish. They may do so by clicking on 'Set up DHCP Server'.

The **DHCP Server, General Setup** settings for the **wwan** interface, shows the following information:

! **WARNING:** Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Ignore interface:** box is checked by default. If checked, disables DHCP for this interface.

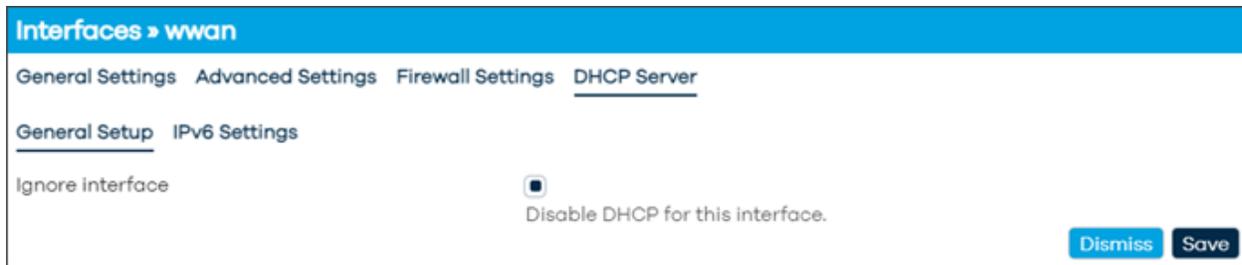


Figure 148: Interfaces > wwan page – General Setup for DHCP Server

In **DHCP Server, IPv6 Settings** for the **wwan** interface, it shows the following information:

! **WARNING:** Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Designated master:** box is unchecked by default. Set this interface as master for RA and DHCPv6 relaying as well as NDP proxying.
- **RA-Service:** set to **disabled** by default which does not send any RA messages on this interface.
 - Other options are: **server mode** which sends RA messages advertising this device as IPv6 router; relay mode which forwards RA messages received on the designated master interface to downstream interfaces; hybrid mode which operates in relay mode if a designated master interface is configured and active, otherwise fall back to server mode.
- **DHCPv6-Service:** set to **disabled** by default which does not offer DHCPv6 service on this interface.
 - Other options are: **server mode** which provides a DHCPv6 server on this interface and reply to DHCPv6 solicitations and requests; relay mode which forwards DHCPv6 messages between the designated master interface and downstream interfaces; **hybrid mode** which operates in **relay mode** if a designated master interface is configured and active, otherwise fall back to server mode.
- **NDP-Proxy:** Configures the operation mode of the NDP proxy service on this interface. Set to **disabled** by default which does not proxy any NDP packets.
 - Other options are: **relay mode** which forwards NDP NS and NA messages between the designated master interface and downstream interfaces; hybrid mode which operates in **relay mode** if a designated master interface is configured and active, otherwise disable NDP proxying.

4.4.1.2 Devices

In the **Devices** tab, there are listed devices that have corresponding information that include: Device name, Type, MAC Address, MTU. Next to each device, there are some action buttons such as Configurations and Unconfigure (and “Add device configuration...” at the bottom). By default, **br-lan** and **wan** are hi-lighted.

Device	Type	MAC Address	MTU	Configure...	Unconfigure
br-lan	Bridge device	34:BA:9A:7B:65:2F	1342	Configure...	Unconfigure
wan	Network device	34:BA:9A:7B:65:30	1500	Configure...	Unconfigure
erspan0	Network device	00:00:00:00:00:00	1450	Configure...	Unconfigure
eth0	Network device	3E:A5:F4:55:65:95	1504	Configure...	Unconfigure
lan1	Network device	34:BA:9A:7B:65:2F	1500	Configure...	Unconfigure
lan2	Network device	34:BA:9A:7B:65:2F	1500	Configure...	Unconfigure
lan3	Network device	34:BA:9A:7B:65:2F	1500	Configure...	Unconfigure
lan4	Network device	34:BA:9A:7B:65:2F	1500	Configure...	Unconfigure
wwan0	Network device	3A:AA:10:84:9B:C9	1342	Configure...	Unconfigure
wlan0	Network device	34:BA:9A:7B:65:31	1342	Configure...	Unconfigure
wlan1	Network device	34:BA:9A:7B:65:32	1342	Configure...	Unconfigure

Add device configuration...

Save & Apply Save Reset

Figure 149: Devices tab showing list of device properties

br-lan Configure

Each device has its own configuration, and after selecting “**Configure...**,” a configurations page will be displayed with 3-tabs of settings if applicable: **General device options**, **Advanced device options**, and **Bridge VLAN filtering**.

! WARNING: The **Unconfigure** option can lead to unfavorable results. Only use this if you are an experienced user.

In **General device options** for **br-lan**, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Device type:** Bridge device is set by default
- **Device name:** br-lan

- **Bridge ports:** Lists: lan1, lan2, lan, lan4. Specifies the wired ports to attach to this bridge. In order to attach wireless networks, choose the associated interface as network in the wireless settings.
- **Bring up empty bridge:** box not checked by default.
- **MTU:** set to **1342** by default
- **MAC address:** mac address of the device
- **TX queue length:** set to **1000** by default.
- **Enable IPv6:** set to automatic (enabled) by default. Other option is disabled.
- **IPv6 MTU:** set to **1342**
- **DAD transmits:** set to **1** by default. Amount of Duplicate Address Detection probes to send.

Bridge device: br-lan

General device options Advanced device options Bridge VLAN filtering

Device type: br-lan

Device name: br-lan

Bridge ports: lan1 lan2 lan3 lan4

Bring up empty bridge:

MTU: 1342

MAC address: 34:BA:9A:7B:65:2F

TX queue length: 1000

Enable IPv6: automatic (enabled)

IPv6 MTU: 1342

DAD transmits: 1

Amount of Duplicate Address Detection probes to send

[Dismiss](#) [Save](#)

Figure 150: Configuration page for br-lan device – General device options tab

In **Advanced** device options for **br-lan**, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Priority:** set to **32767**
- **Ageing time:** **30**. Timeout in seconds for learned MAC addresses in the forwarding database.
- **Enable STP:** box unchecked by default. Enables the Spanning Tree Protocol on this bridge if checked.
- **Enable IGMP snooping:** box unchecked by default. Enables IGMP snooping on this bridge if checked.
- **Enable multicast querier:** box unchecked by default.

- **Enable promiscuous mode:** set to automatic (disabled) by default. Other option is **enabled**.
- **Reverse path filter:** set to **disabled** by default. Other options are: Loose filtering and Strict filtering.
- **Accept local:** set to **automatic (disabled)** by default. Other option is **enabled**. Accept packets with local source addresses.
- **Send ICMP redirects:** set to **automatic (enabled)** by default. Other option is disabled.
- **Honor gratuitous ARP:** set to **automatic (disabled)** by default. Other option is enabled. When enabled, new ARP table entries are added from received gratuitous APR requests or replies, otherwise only preexisting table entries are updated, but no new hosts are learned.
- **Drop gratuitous ARP:** set to **automatic (disabled)** by default. Other option is enabled. Drop all gratuitous ARP frames, for example if there's a known good ARP proxy on the network and such frames need not be used or in the case of 802.11, must not be used to prevent attacks.
- **Neighbor cache validity:** set to **30000**. Time in milliseconds
- **Stale neighbor cache timeout:** set to **60**. Timeout in seconds
- **Minimum ARP validity time:** set to **0**. Minimum required time in seconds before an ARP entry may be replaced. Prevents ARP cache thrashing.
- **Enable IPv6 segment routing:** set to **automatic (disabled)** by default. Other option is enabled.
- **Drop unsolicited NA:** set to **automatic (disabled)** by default. Other option is enabled. Drop all unsolicited neighbor advertisements, for example if there's a known good NA proxy on the network and such frames need not be used or in the case of 802.11, must not be used to prevent attacks.
- **Enabled multicast support:** set to **automatic (enabled)** by default. Other option is disabled.
- **Force IGMP version:** set to **No enforcement** by default. Other options are Enforce IGMPv1, Enforce IGMPv2, and Enforce IGMPv3.
- **Force MLD version:** set to **No enforcement by default**. Other options are Enforce MLD version 1, and Enforce MLD version 2.

Bridge device: br-lan

General device options **Advanced device options** Bridge VLAN filtering

Priority: 32767

Ageing time: 30
Timeout in seconds for learned MAC addresses in the forwarding database

Enable STP:
Enables the Spanning Tree Protocol on this bridge

Enable IGMP snooping:
Enables IGMP snooping on this bridge

Enable multicast querier:

Enable promiscuous mode: automatic (disabled)

Reverse path filter: disabled

Accept local: automatic (disabled)
Accept packets with local source addresses

Send ICMP redirects: automatic (enabled)

Honor gratuitous ARP: automatic (disabled)
When enabled, new ARP table entries are added from received gratuitous ARP requests or replies, otherwise only preexisting table entries are updated, but no new hosts are learned.

Drop gratuitous ARP: automatic (disabled)
Drop all gratuitous ARP frames, for example if there's a known good ARP proxy on the network and such frames need not be used or in the case of 802.11, must not be used to prevent attacks.

Neighbour cache validity: 30000
Time in milliseconds

Stale neighbour cache timeout: 60
Timeout in seconds

Minimum ARP validity time: 0
Minimum required time in seconds before an ARP entry may be replaced. Prevents ARP cache thrashing.

Enable IPv6 segment routing: automatic (disabled)

Drop unsolicited NA: automatic (disabled)
Drop all unsolicited neighbor advertisements, for example if there's a known good NA proxy on the network and such frames need not be used or in the case of 802.11, must not be used to prevent attacks.

Enable multicast support: automatic (enabled)

Force IGMP version: No enforcement

Force MLD version: No enforcement

Dismiss Save

Figure 151: Configuration page for br-lan device – Advanced device options tab

In **Bridge VLAN filtering** for br-lan, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Enable VLAN filtering:** box is unchecked by default and no VLAN values are set. Other option is to enable by checking the box which turns on this feature on.
- The **Add** button below allows the user to add ports to a VLAN to the users' discretion with options to create VLAN ID number, whether it is Not a member, Untagged, Tagged, or Is Primary VLAN.

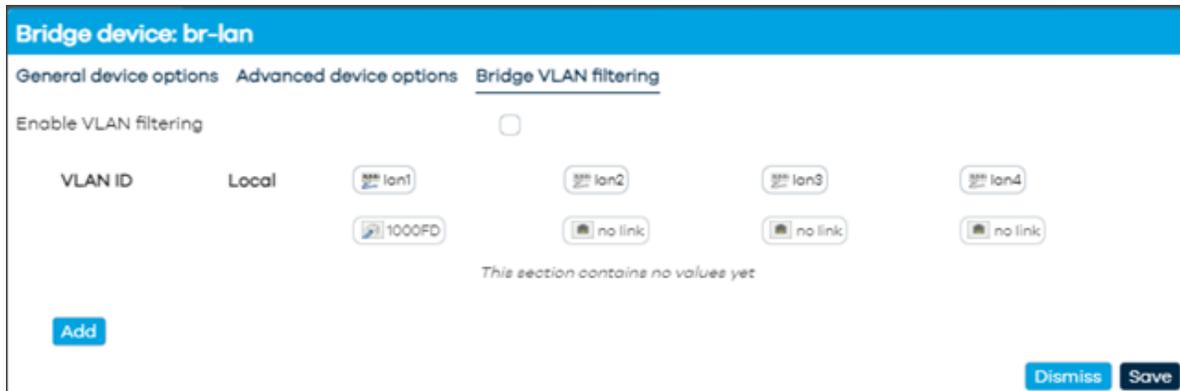


Figure 152: Configuration page for `br-lan` device – Bridge VLAN Filtering

wan Configure

In **General device options** for `wan`, it shows the following information:

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Device type:** Network device is set by default
- **Existing device:** `wan`
- **MTU:** set to 1500 by default
- **MAC address:** mac address of the device
- **TX queue length:** set to 1000 by default.
- **Enable IPv6:** set to automatic (enabled) by default. Other option is disabled.
- **IPv6 MTU:** set to 1500
- **DAD transmits:** set to 1 by default. Amount of Duplicate Address Detection probes to send.

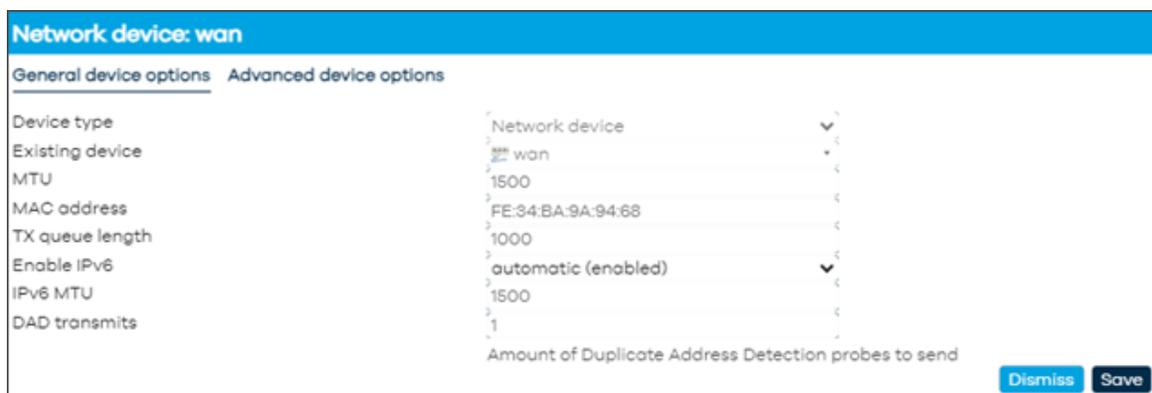


Figure 153: General device options for `wan`

In **Advanced device options** for wan, it shows the following information:

! **WARNING:** Settings in this area should be left at default values and any changes should only be made by experienced users.

- **Enable promiscuous mode:** set to **automatic (disabled)** by default. Other option is enabled.
- **Reverse path filter:** set to **disabled** by default. Other options are: Loose filtering and Strict filtering.
- **Accept local:** set to **automatic (disabled)** by default. Other option is enabled. Accept packets with local source addresses.
- **Send ICMP redirects:** set to **automatic (enabled)** by default. Other option is disabled.
- **Honor gratuitous ARP** - set to **automatic (disabled)** by default. Other option is enabled. When enabled, new ARP table entries are added from received gratuitous APR requests or replies, otherwise only preexisting table entries are updated, but no new hosts are learned.
- **Drop gratuitous ARP** - set to **automatic (disabled)** by default. Other option is enabled. Drop all gratuitous ARP frames, for example if there's a known good ARP proxy on the network and such frames need not be used or in the case of 802.11, must not be used to prevent attacks.
- **Neighbor cache validity:** set to **30000**. Time in milliseconds
- **Stale neighbor cache timeout:** set to **60**. Timeout in seconds
- **Minimum ARP validity time:** set to **0**. Minimum required time in seconds before an ARP entry may be replaced. Prevents ARP cache thrashing.
- **Enable IPv6 segment routing:** set to **automatic (disabled)** by default. Other option is enabled.
- **Drop unsolicited NA:** set to **automatic (disabled)** by default. Other option is enabled. Drop all unsolicited neighbor advertisements, for example if there's a known good NA proxy on the network and such frames need not be used or in the case of 802.11, must not be used to prevent attacks.
- **Enabled multicast support:** set to **automatic (enabled)** by default. Other option is disabled.
- **Force IGMP version:** set to **No enforcement** by default. Other options are Enforce IGMPv1, Enforce IGMPv2, and Enforce IGMPv3.
- **Force MLD version:** set to **No enforcement** by default. Other options are Enforce MLD version 1 and Enforce MLD version 2.

Network device: wan

General device options Advanced device options

Enable promiscuous mode automatic (disabled) ▼

Reverse path filter disabled ▼

Accept local automatic (disabled) ▼

Accept packets with local source addresses

Send ICMP redirects automatic (enabled) ▼

Honor gratuitous ARP automatic (disabled) ▼

When enabled, new ARP table entries are added from received gratuitous APR requests or replies, otherwise only preexisting table entries are updated, but no new hosts are learned.

Drop gratuitous ARP automatic (disabled) ▼

Drop all gratuitous ARP frames, for example if there's a known good ARP proxy on the network and such frames need not be used or in the case of 802.11, must not be used to prevent attacks.

Neighbour cache validity 30000 ▼

Time in milliseconds

Stale neighbour cache timeout 60 ▼

Timeout in seconds

Minimum ARP validity time 0 ▼

Minimum required time in seconds before an ARP entry may be replaced. Prevents ARP cache thrashing.

Enable IPv6 segment routing automatic (disabled) ▼

Drop unsolicited NA automatic (disabled) ▼

Drop all unsolicited neighbor advertisements, for example if there's a known good NA proxy on the network and such frames need not be used or in the case of 802.11, must not be used to prevent attacks.

Enable multicast support automatic (enabled) ▼

Force IGMP version No enforcement ▼

Force MLD version No enforcement ▼

Dismiss Save

Figure 154: Advanced device options for wan

4.4.1.3 Global network options

In the **Global network options** tab, there are two settings that can be configured:

- **IPv6 ULA-Prefix:** prepopulated by default. Unique Local Address - in the range fc00::/7. Typically only within the 'local' half fd00::/8. ULA for IPv6 is analogous to IPv4 private network addressing. This prefix is randomly generated at first install.
- **Packet Steering:** box checked by default. Enable packet steering across all CPUs. May help or hinder network speed.

Interfaces Devices Global network options

• Global network options

IPv6 ULA-Prefix fdb3:9dda:00d0::/48

Unique Local Address - in the range fc00::/7. Typically only within the 'local' half fd00::/8. ULA for IPv6 is analogous to IPv4 private network addressing. This prefix is randomly generated at first install.

Packet Steering

Enable packet steering across all CPUs. May help or hinder network speed.

Save & Apply Save Reset

Figure 155: Global network options

4.4.2 Wireless

On this page, Wi-Fi settings can be configured based on the users' preferences. There are two available Wi-Fi radios, one for 2.4 GHz and one for 5 GHz. In each setting, the user has the option to enable the radio, change the channel, configure the mode, change the SSID, configure the encryption, and configure the key.

- **Note:** Please refer to section 3.10 *Wi-Fi Settings* for details on verifying and changing these settings.

4.4.3 Routing

On this page, the user will be able to route over which interface and gateway a certain host or network can be reached. There are four tabs: **Static IPv4 Routes**, **Static IPv6 Routes**, **IPv4 Rules**, and **IPv6 Rules**.

These sections contain no values by default. The **Static IPv4** and **IPv6 Routes** tabs are similar as are the IPv4 and IPv6 Rules tabs.

There is an **Add** button at the bottom to add routes and rules as needed.

Routing

Routing defines over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes Static IPv6 Routes IPv4 Rules IPv6 Rules

Static IPv4 Routes

Interface	Target	Gateway	Metric	Table	Disable
<i>This section contains no values yet</i>					

[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

Figure 156: Routing page – Static IPv4 Routes

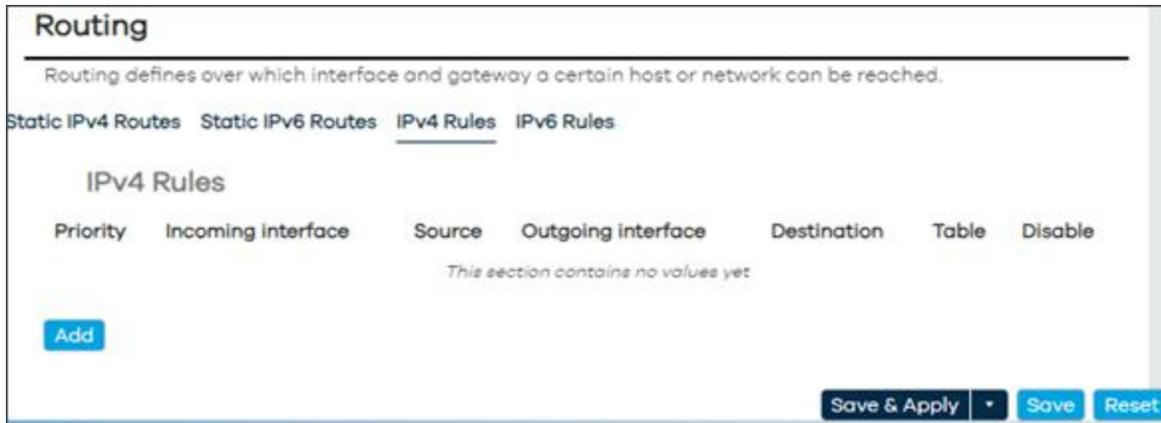


Figure 157: Routing page – IPv4 Rules tab

4.4.3.1 Adding Routes

When adding routes, the user will be presented with **General Settings** and **Advanced Settings**.

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

Under **General Settings**, the following parameters are available:

- **Interface:** set to **unspecified**. Options are lan, loopback, wan, and wwan. Specifies the logical interface name of the parent (or master) interface this route belongs to.
- **Route Type:** set to **unicast**. Options are: local, broadcast, multicast, unreachable, prohibit, blackhole, and anycast. Specifies the route type to be created.
- **Target:** set to **0.0.0.0/0**. Network address.
- **Gateway:** set to **192.168.0.1**. Specifies the network gateway. If omitted, the gateway from the parent interface is taken if any, otherwise creates a link scope route. If set to 0.0.0.0 no gateway will be specified for the route.



Figure 158: Routing page – General Settings tab

Under **Advanced Settings**, the following parameters are available:

- **Metric:** set to **0**. Specifies the route metric to use.
- **MTU:** set to **1500**. Defines a specific MTU for this route.
- **Table:** set to **unspecified**. Options are: prelocal (128), local (255), main (254), default (253), and custom. The rule target is a table lookup ID: a numeric table index ranging from 0 to 65535 or symbol alias declared in /etc/iproute2/rt_tables. Special aliases local (255), main (254) and default (253) are also valid.
- **Source:** set to **auto**. Options are 192.168.113.1 or local IP address of device, derived IP address for wwan, or custom. Specifies the preferred source address when sending to destinations covered by the target.
- **On-Link:** box is unchecked. When enabled, gateway is on-link even if the gateway does not match any interface prefix.

The screenshot shows the 'Routing' configuration page with the 'Advanced Settings' tab selected. The form contains the following fields and values:

- Metric:** 0. Description: Specifies the route metric to use.
- MTU:** 1500. Description: Defines a specific MTU for this route.
- Table:** unspecified. Description: The rule target is a table lookup ID: a numeric table index ranging from 0 to 65535 or symbol alias declared in /etc/iproute2/rt_tables. Special aliases local (255), main (254) and default (253) are also valid.
- Source:** auto. Description: Specifies the preferred source address when sending to destinations covered by the target.
- On-link:** . Description: When enabled, gateway is on-link even if the gateway does not match any interface prefix.

Buttons for 'Dismiss' and 'Save' are visible at the bottom right of the form.

Figure 159: Routing page – Advanced Settings tab

4.4.3.2 Adding Rules

When adding rules, the user will be presented **General Settings** and **Advanced Settings**.

! WARNING: Settings in this area should be left at default values and any changes should only be made by experienced users.

Under **General Settings**, the following parameters are available:

- **Priority:** set to **30000**
- **Rule type:** set to **unicast**. Specifies the ordering of the IP rules. Other options are: unreachable, prohibit, blackhole, and throw.
- **Incoming interface:** set to **unspecified**. Other options are: lan, loopback, wan, and wwan. Specifies the incoming logical interface name.
- **Source:** set to **0.0.0.0/0**. Specifies the source subnet to match (CIDR notation).

- **Outgoing interface:** set to unspecified. Specifies the outgoing logical interface name.
- **Destination:** set to **0.0.0.0/0**. Specifies the destination subnet to match (CIDR notation).
- **Table:** set to **unspecified**. Options are: prelocal (128), local (255), main (254), default (253), and custom. The rule target is a table lookup ID: a numeric table index ranging from 0 to 65535 or symbol alias declared in /etc/iproute2/rt_tables. Special aliases local (255), main (254) and default (253) are also valid.

The screenshot shows the 'Routing' configuration page with the 'General Settings' tab selected. The parameters are as follows:

Parameter	Value	Description
Priority	30000	Specifies the ordering of the IP rules
Rule type	unicast	Specifies the rule target routing action
Incoming interface	unspecified	Specifies the incoming logical interface name
Source	0.0.0.0/0	Specifies the source subnet to match (CIDR notation)
Outgoing interface	unspecified	Specifies the outgoing logical interface name
Destination	0.0.0.0/0	Specifies the destination subnet to match (CIDR notation)
Table	unspecified	The rule target is a table lookup ID: a numeric table index ranging from 0 to 65535 or symbol alias declared in /etc/iproute2/rt_tables. Special aliases local (255), main (254) and default (253) are also valid

Buttons: Dismiss, Save

Figure 160: Routing page – General settings tab

Under **Advanced Settings**, the following parameters are available:

- **Jump to rule:** set to **80000**. The rule target is a jump to another rule specified by its priority value.
- **Firewall mark:** set to **0x1/0xf**. Specifies the fwmark and optionally its mask to match, e.g. 0xFF to match mark 255 or 0x0/0x1 to match any even mark value.
- **Type of service:** set to **10**. Specifies the TOS value to match in IP headers.
- **User identifier:** set to **1000-1005**. Specifies an individual UID or range of UIDs to match, e.g. 1000 to match corresponding UID or 1000-1005 to inclusively match all UIDs within the corresponding range.
- **Prefix suppressor:** set to **24**. Reject routing decisions that have a prefix length less than or equal to the specified value.
- **Invert match:** box is unchecked. If set, the meaning of the match options is inverted.

Routing

General Settings Advanced Settings

Jump to rule	80000 The rule target is a jump to another rule specified by its priority value
Firewall mark	0x1/0xf Specifies the fwmark and optionally its mask to match, e.g. 0xFF to match mark 255 or 0x0/0x1 to match any even mark value
Type of service	10 Specifies the TOS value to match in IP headers
User identifier	1000-1005 Specifies an individual UID or range of UIDs to match, e.g. 1000 to match corresponding UID or 1000-1005 to inclusively match all UIDs within the corresponding range
Prefix suppressor	24 Reject routing decisions that have a prefix length less than or equal to the specified value
Invert match	<input type="checkbox"/> If set, the meaning of the match options is inverted

Dismiss
Save

Figure 161: Routing page – Advanced Settings

4.4.4 DHCP and DNS

This page contains all the device information and attributes to manage servers, leases, and other settings:

In **General Settings**, configurable options are:

- **Domain required:** boxed is checked by default. Do not forward DNS queries without dots or domain parts.
- **Authoritative:** boxed is checked by default. This is the only DHCP server in the local network.
- **Local server:** set to **/lan/**. Never forward matching domains and subdomains, resolve from DHCP or hosts files only.
- **Local domain:** set to **lan**. Local domain suffix appended to DHCP names and hosts file entries.
- **Log queries:** boxed unchecked by default. Write received DNS queries to syslog.
- **DNS forwardings:** set to **/example/10.1.2.3**. Can add more as needed. List of upstream resolvers to forward queries to.
- **Addresses:** set to **/router.local/router.lan/192.168.0.1**. Resolve specified FQDNs to an IP.
 - Syntax: `/fqdn[/fqdn...]/[ipaddr]`.
 - `/#/` matches any domain. `/example.com/` returns NXDOMAIN.
 - `/example.com/#` returns NULL addresses (0.0.0.0 and ::) for example.com and its subdomains. Can add more as needed.
- **IP sets:** set to **/example.org/ipset6**. List of IP sets to populate with the IPs of DNS lookup results of the FQDNs also specified here. Can add more as needed.
- **Rebind protection:** box is unchecked by default. Discard upstream responses containing RFC1918 addresses.
- **Local service only:** box is checked by default. Accept DNS queries only from hosts whose address is on a local subnet.
- **Non-wildcard:** box is checked by default. Bind dynamically to interfaces rather than wildcard address.
- **Listen interfaces:** set to **lan** by default. Listen only on the specified interfaces, and loopback if not excluded explicitly. Can add more as needed.
- **Exclude interfaces:** set to **loopback**. Do not listen on the specified interfaces. Can add more as needed.

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

General Settings **Relay** Resolv and Hosts Files PXE/TFTP Settings Advanced Settings Static Leases Hostnames

SRV MX IP Sets

Domain required Do not forward DNS queries without dots or domain parts.

Authoritative This is the only DHCP server in the local network.

Local server Never forward matching domains and subdomains, resolve from DHCP or hosts files only.

Local domain Local domain suffix appended to DHCP names and hosts file entries.

Log queries Write received DNS queries to syslog.

DNS forwardings + List of upstream resolvers to forward queries to.

Addresses + Resolve specified FQDNs to an IP.
Syntax: /fqdn[/fqdn...]/[ipaddr].
/#/ matches any domain. /example.com/ returns NXDOMAIN.
/example.com/# returns NULL addresses (0.0.0.0 and ::) for example.com and its subdomains.

IP sets + List of IP sets to populate with the IPs of DNS lookup results of the FQDNs also specified here.

Rebind protection Discard upstream responses containing RFC1918 addresses.

Local service only

Figure 162: DHCP and DNS page – General Settings

In **Relay**, there are no values set by default.

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

General Settings **Relay** Resolv and Hosts Files PXE/TFTP Settings Advanced Settings Static Leases Hostnames

SRV MX IP Sets

Relay DHCP requests elsewhere. OK: v4↔v4, v6↔v6. Not OK: v4↔v6, v6↔v4.
Note: you may also need a DHCP Proxy (currently unavailable) when specifying a non-standard Relay To port(addr#port).
You may add multiple unique Relay To on the same Listen addr.

ID	Interface	Listen address	Relay To address
<i>This section contains no values yet</i>			

Figure 163: DHCP and DNS page – Relay tab

There is the ability to Add relay entries as follows:

- **ID:** Enter the ID
- **Interface:** set to unspecified. Options are lan, wan, wwan, and custom.
- **Listen address:** choose an IP address or mac address from the drop-down menu or enter a custom one.
- **Relay To address:** set to 192.168.10.1#535. Change as necessary.

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

General Settings **Relay** Resolv and Hosts Files PXE/TFTP Settings Advanced Settings Static Leases

Hostnames SRV MX IP Sets

Relay DHCP requests elsewhere. OK: v4→v4, v6→v6. Not OK: v4→v6, v6→v4.
 Note: you may also need a DHCP Proxy (currently unavailable) when specifying a non-standard Relay To port(addr#port).
 You may add multiple unique Relay To on the same Listen addr.

ID	Interface	Listen address	Relay To address
	unspecified	-- Please choose --	192.168.10.1#535

Add

Save & Apply Save Reset

Figure 164: DHCP page – Add Relay

In **Resolv** and **Hosts Files**, these are the parameters that are configurable:

- **Use /etc/ethers:** box is checked by default. Read /etc/ethers to configure the DHCP server.
- **Lease file:** set to /etc/awc/dhcp/dhcp.leases. File to store DHCP lease information.
- **Ignore resolv file:** box is unchecked by default.
- **Resolv file:** set to /tmp/resolv.conf.d/resolv.conf.auto. File with upstream resolvers.
- **Ignore /etc/hosts:** box is unchecked by default.
- **Additional hosts files:** set to /etc/dnsmasq.hosts, Can add more as needed.

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

General Settings Relay Resolv and Hosts Files PXE/TFTP Settings Advanced Settings Static Leases Hostnames

SRV MX IP Sets

Use /etc/ethers Read /etc/ethers to configure the DHCP server.

Lease file File to store DHCP lease information.

Ignore resolv file Resolv file File with upstream resolvers.

Ignore /etc/hosts Additional hosts files +

Save & Apply Save Reset

Figure 165: DHCP and DNS page – Resolv and Hosts Files tab

In **PXE/TFTP Settings**, these are the parameters that are configurable:

- **Enable TFTP server:** box is not checked by default. Check the box to enable the built-in single-instance TFTP server.

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

General Settings Relay Resolv and Hosts Files PXE/TFTP Settings Advanced Settings Static Leases Hostnames

SRV MX IP Sets

Enable TFTP server Enable the built-in single-instance TFTP server.

Special PXE boot options for Dnsmasq.

Filename	Server name	Server address	DHCP Options	Network-ID	Force	Instance
<i>This section contains no values yet</i>						

Add

Save & Apply Save Reset

Figure 166: DHCP and DNS page – PXE/TFTP Settings tab

- **Special PXE boot options for Dnsmasq:** there are no values in this area. The ability to add will provide further configuration options:
 - **Filename:** set to **pxelinux.0**. Host requests this filename from the boot server.
 - **Server name:** set to **myNAS**. The hostname of the boot server.
 - **Server address:** set to **192.168.1.2**. The IP address of the boot server.

- **DHCP Options:** set to **42.192.168.14**. Options for the Network-ID. (Note: needs also Network-ID.) E.g. "42,192.168.1.4" for NTP server, "3,192.168.4.4" for default route. 0.0.0.0 means "the address of the system running dnsmasq". Can add more as needed.
- **Network-ID:** set to **unspecified**. Use the drop-down menu to choose a specific option. Apply DHCP Options to this net. (Empty = all clients).
- **Force:** box is unchecked. Always send DHCP Options. Sometimes needed, with e.g. PXELinux.
- **Instance:** set to **unspecified**. Options are 0 (Domain: lan, Local: /lan/), or custom. Dnsmasq instance to which this boot section is bound. If unspecified, the section is valid for all dnsmasq instances.

DHCP and DNS

Filename	pxelinux.0 Host requests this filename from the boot server.
Server name	myNAS The hostname of the boot server
Server address	192.168.1.2 The IP address of the boot server
DHCP Options	42,192.168.1.4 Options for the Network-ID. (Note: needs also Network-ID.) E.g. "42,192.168.1.4" for NTP server, "3,192.168.4.4" for default route. 0.0.0.0 means "the address of the system running dnsmasq".
Network-ID	unspecified Apply DHCP Options to this net. (Empty = all clients).
Force	<input type="checkbox"/> Always send DHCP Options. Sometimes needed, with e.g. PXELinux.
Instance	unspecified Dnsmasq instance to which this boot section is bound. If unspecified, the section is valid for all dnsmasq instances.

Dismiss Save

Figure 167: DHCP and DNS page – Special PXE boot options for Dnsmasq

In **Advanced Settings**, these are the available configuration options:

- **Suppress logging:** box unchecked by default. Suppress logging of the routine operation for the DHCP protocol.
- **Allocate IPs sequentially:** box unchecked by default. Allocate IP addresses sequentially, starting from the lowest available address.
- **Filter private** - box checked by default. Do not forward reverse lookups for local networks.
- **Filter SRV/SOA service discovery** - box unchecked by default. Filters SRV/SOA service discovery, to avoid triggering dial-on-demand links. May prevent VoIP or other services from working.
- **Filter IPv6 AAAA records** - box unchecked by default. Remove IPv6 addresses from the results and only return IPv4 addresses. Can be useful if ISP has IPv6 nameservers but does not provide IPv6 routing.
- **Filter IPv4 A records:** box unchecked by default. Remove IPv4 addresses from the results and only return IPv6 addresses.

- **Localise queries:** box checked by default. Return answers to DNS queries matching the subnet from which the query was received if multiple IPs are available.
- **Expand hosts:** box checked by default. Add local domain suffix to names served from hosts files.
- **No negative cache:** box unchecked by default. Do not cache negative replies, e.g. for non-existent domains.
- **Additional servers file:** set to `/etc/dnsmasq.servers`. File listing upstream resolvers, optionally domain-specific, e.g. `server=1.2.3.4, server=/domain/1.2.3.4`.
- **Strict order** - box unchecked by default. Upstream resolvers will be queried in the order of the resolv file.
- **All servers** - box unchecked by default. Query all available upstream resolvers.
- **Ips to override with NXDOMAIN:** set to `64.94.110.11`. List of IP addresses to convert into NXDOMAIN responses. Can add more as needed.
- **DNS server port:** set to **53**. Listening port for inbound DNS queries.
- **DNS query port:** set to **any**. Fixed source port for outbound DNS queries.
- **Max. DHCP leases:** set to **unlimited**. Maximum allowed number of active DHCP leases.
- **Max. EDNSO packet size:** set to **1232**. Maximum allowed size of EDNSO UDP packets.
- **Max. concurrent queries:** set to **1024**. Maximum allowed number of concurrent DNS queries.
- **Size of DNS query cache:** set to **1024**. Number of cached DNS entries, 10000 is maximum, 0 is no caching.

General Settings	Relay	Resolv and Hosts Files	PXE/TFTP Settings	<u>Advanced Settings</u>	Static Leases
Hostnames SRV MX IP Sets					
Suppress logging	<input type="checkbox"/>	Suppress logging of the routine operation for the DHCP protocol.			
Allocate IPs sequentially	<input type="checkbox"/>	Allocate IP addresses sequentially, starting from the lowest available address.			
Filter private	<input checked="" type="checkbox"/>	Do not forward reverse lookups for local networks.			
Filter SRV/SOA service discovery	<input type="checkbox"/>	Filters SRV/SOA service discovery, to avoid triggering dial-on-demand links. May prevent VoIP or other services from working.			
Filter IPv6 AAAA records	<input type="checkbox"/>	Remove IPv6 addresses from the results and only return IPv4 addresses. Can be useful if ISP has IPv6 nameservers but does not provide IPv6 routing.			
Filter IPv4 A records	<input type="checkbox"/>	Remove IPv4 addresses from the results and only return IPv6 addresses.			
Localise queries	<input checked="" type="checkbox"/>	Return answers to DNS queries matching the subnet from which the query was received if multiple IPs are available.			
Expand hosts	<input checked="" type="checkbox"/>	Add local domain suffix to names served from hosts files.			
No negative cache	<input type="checkbox"/>	Do not cache negative replies, e.g. for non-existent domains.			
Additional servers file	<input type="text" value="/etc/dnsmasq.servers"/>	File listing upstream resolvers, optionally domain-specific, e.g. server=1.2.3.4, server=/domain/1.2.3.4.			
Strict order	<input type="checkbox"/>	Upstream resolvers will be queried in the order of the resolv file.			
All servers	<input type="checkbox"/>	Query all available upstream resolvers.			
IPs to override with NXDOMAIN	<input type="text" value="64.94.110.11"/> <input checked="" type="checkbox"/>	List of IP addresses to convert into NXDOMAIN responses.			
DNS server port	<input type="text" value="53"/>	Listening port for inbound DNS queries.			
DNS query port	<input type="text" value="any"/>	Fixed source port for outbound DNS queries.			
Max. DHCP leases	<input type="text" value="unlimited"/>	Maximum allowed number of active DHCP leases.			
Max. EDNS0 packet size	<input type="text" value="1232"/>	Maximum allowed size of EDNS0 UDP packets.			
Max. concurrent queries	<input type="text" value="1024"/>	Maximum allowed number of concurrent DNS queries.			
Size of DNS query cache	<input type="text" value="1024"/>	Number of cached DNS entries, 10000 is maximum, 0 is no caching.			
					<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>

Figure 168: DHCP and DNS page – Advanced Settings tab

In **Static Leases**, there is a list of Active DHCP and DHCPv6 Leases.

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

[General Settings](#)
[Relay](#)
[Resolv and Hosts Files](#)
[PXE/TFTP Settings](#)
[Advanced Settings](#)
[Static Leases](#)
[Hostnames](#)

[SRV](#)
[MX](#)
[IP Sets](#)

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the *Add* Button to add a new lease entry. The *MAC address* identifies the host, the *IPv4 address* specifies the fixed address to use, and the *Hostname* is assigned as a symbolic name to the requesting host. The optional *Lease time* can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC address	IPv4 address	Lease time	DUID	IPv6 suffix (hex)
<i>This section contains no values yet</i>					

[Add](#)

Active DHCP Leases

Hostname	IPv4 address	MAC address	Lease time remaining
LAPTOP-UIRN6RVQ	192.168.113.127	7C:8A:E1:80:E6:40	8h 15m 37s

Active DHCPv6 Leases

Host	IPv6 address	DUID	Lease time remaining
LAPTOP-UIRN6RVQ	2600:380:3080:cd4a::8e6/128 fdb3:9dda:d0::8e6/128	00010001285dc5fe7c8ae180e640	8h 15m 50s

[Save & Apply](#)
[Save](#)
[Reset](#)

Figure 169: DHCP and DNS page – Static Leases tab

There are values configured in this area by default, but there is an option to **Add** as follows:

- **Hostname:** enter hostname
- **MAC address:** set to unspecified. Choose one from the drop-down menu or choose custom.
- **IPv4 address:** set to unspecified. Choose one from the drop-down menu or choose custom.
- **Lease time:** set the lease time
- **DUID:** set to unspecified. Choose one from the drop-down menu or choose custom.
- **IPv6 suffix (hex):** enter the IPv6 suffix in hex value.

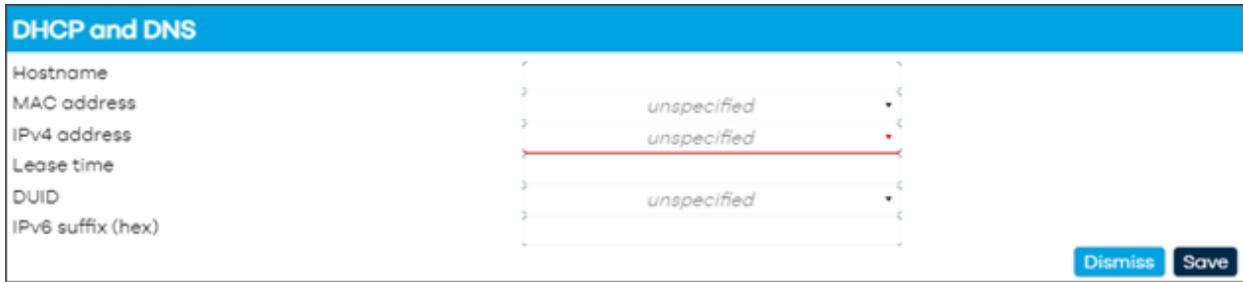


Figure 170: DHCP and DNS page – Add Static Lease

In **Hostnames**, there are no values configured.

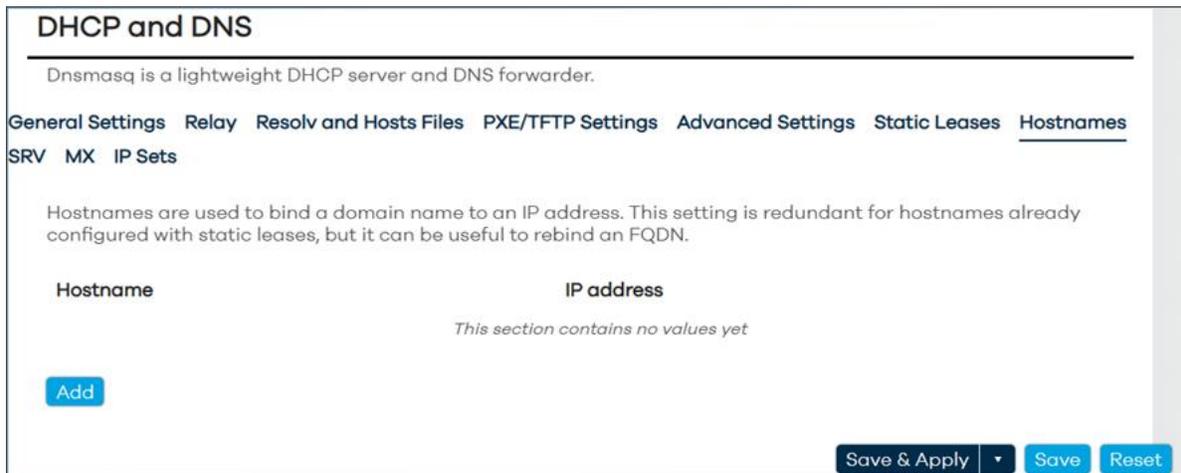


Figure 171: DHCP and DNS page – Hostnames tab

There is an option to Add as follows:

- **Hostname:** enter the hostname
- **IP address** - Choose one from the drop-down menu or choose custom.

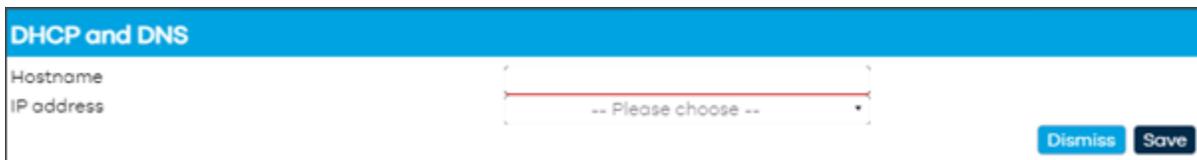


Figure 172: DHCP and DNS page – Adding a hostname

In **SRV**, there are no values configured in this area by default.

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

General Settings Relay Resolv and Hosts Files PXE/TFTP Settings Advanced Settings Static Leases Hostnames

SRV MX IP Sets

Bind service records to a domain name: specify the location of services. See RFC2782.
 _service: _sip, _ldap, _imap, _stun, _xmpp-client, ... (Note: while _http is possible, no browsers support SRV records.)
 _proto: _tcp, _udp, _sctp, _quic, ...
 You may add multiple records for the same Target.
 Larger weights (of the same prio) are given a proportionately higher probability of being selected.

SRV	Target	Port	Priority	Weight
Syntax: <code>_service._proto.example.com</code>	CNAME or fqdn		Ordinal: lower comes first.	

This section contains no values yet

Add

Save & Apply Save Reset

Figure 173: DHCP and DNS page – SRV tab

There is an option to Add as follows:

- **SRV:** example is given. Enter appropriate domain
- **Target:** enter target value (CNAME or fqdn)
- **Port:** set to 5060
- **Priority:** set to 10
- **Weight:** set to 50

DHCP and DNS

Dnsmasq is a lightweight DHCP server and DNS forwarder.

General Settings Relay Resolv and Hosts Files PXE/TFTP Settings Advanced Settings Static Leases

Hostnames **SRV** MX IP Sets

Bind service records to a domain name: specify the location of services. See RFC2782.
 _service: _sip, _ldap, _imap, _stun, _xmpp-client, ... (Note: while _http is possible, no browsers support SRV records.)
 _proto: _tcp, _udp, _sctp, _quic, ...
 You may add multiple records for the same Target.
 Larger weights (of the same prio) are given a proportionately higher probability of being selected.

SRV	Target	Port	Priority	Weight
Syntax: <code>_service._proto.example.com</code>	CNAME or fqdn		Ordinal: lower comes first.	
<code>_sip_tcp.example.com</code>	<code>sip.example.com</code>	<code>5060</code>	<code>10</code>	<code>50</code>

Add

Save & Apply Save Reset

Figure 174: DHCP and DNS page – SRV tab

In **MX**, there are no values configured in this area by default.

Figure 175: DHCP and DNS page – MX tab

There is an option to Add as follows:

- **Domain:** enter domain
- **Relay:** enter relay
- **Priority:** set to 0

In **IP Sets**, there are no values configured in this area by default.

Figure 176: DHCP and DNS page – IP Sets tab

There is an option to Add as follows:

- **IP set:** add IP sets as needed
- **Domain:** add domains as needed

Figure 177: DHCP and DNS page – Adding an IP Set

4.4.5 Diagnostics

This page will allow the user to execute various network commands to check the connection and name resolution to other systems.

The options are:

- **IPv4 Ping:** ping remote device to verify connectivity
 - **IPv4 Traceroute:** traceroute to remote device to verify connectivity, hops, etc
 - **Nslookup:** verify name resolution
- ➔ **Note:** the default server in the fields “openwrt.org”, can be modified as needed.

Figure 178: Diagnostics page – Checking connection and name resolution to other systems

4.4.6 Firewall

This page has five tabs: **General Settings**, **Port Forwards**, **Traffic Rules**, **NAT Rules**, and **IP Sets**.

4.4.6.1 Firewall – Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

In **General Settings**, the following settings are:

- **Enable SYN-flood protection:** box checked by default
 - **Drop invalid packets:** box unchecked by default
 - **Input:** set to accept. Other options are to reject or drop.
 - **Output:** set to accept. Other options are to reject or drop.
 - **Forward:** set to reject. Other options are to accept or drop.
- ⇒ **Note:** The following are experimental features. Not fully compatible with QoS/SQM:
- **Software flow offloading:** box unchecked by default.
 - **Zone forwardings setup:**
 - **lan → wan:** Adjust Input, Output, Forward, and Masquerading as needed.
 - **wan → REJECT**

The screenshot shows the 'Firewall - Zone Settings' page with the following configuration:

- General Settings:**
 - Enable SYN-flood protection:
 - Drop invalid packets:
 - Input: accept
 - Output: accept
 - Forward: reject
- Routing/NAT Offloading:**
 - Software flow offloading: (Software based offloading for routing/NAT)
- Zones:**

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading
lan ⇒ wan	accept	accept	accept	<input type="checkbox"/>
wan ⇒ REJECT	reject	accept	reject	<input checked="" type="checkbox"/>

Figure 179: Firewall – Zone Settings page – General Settings tab

Edit button these zone forwards reveals further settings: **General Settings, Advanced Settings** and **Conntrack Settings**.

In **General Settings**:

- **Name:** set to **lan**.
 - **Input:** set to **accept**. Other options are reject and drop.
 - **Output:** set to **accept**. Other options are reject and drop.
 - **Forward:** set to **accept**. Other options are reject and drop.
 - **Masquerading:** box is unchecked. Enable network address and port translation IPv4 (NAT4 or NAPT4) for outbound traffic on this zone. This is typically enabled on the wan zone.
 - **MSS clamping** - box is unchecked
 - **Covered networks:** set to **lan**. Other options are wan, wwan, and custom.
- 🔄 **Note:** The options below control the forwarding policies between this zone (lan) and other zones. Destination zones cover forwarded traffic originating from lan. Source zones match forwarded traffic from other zones targeted at lan. The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.
- **Allow forward from destination zones:** set to **wan** and **wwan**
 - **Allow forward from source zones:** set to **unspecified**. Other options are: wan and wwan.

Firewall - Zone Settings

General Settings Advanced Settings Conntrack Settings

This section defines common properties of "lan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name: lan

Input: accept

Output: accept

Forward: accept

Masquerading:

MSS clamping:

Covered networks: lan

The options below control the forwarding policies between this zone (lan) and other zones. *Destination zones* cover forwarded traffic originating from lan. *Source zones* match forwarded traffic from other zones targeted at lan. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.

Allow forward to destination zones: wan, wwan

Allow forward from source zones: unspecified

Dismiss Save

Figure 180: Firewall Zone – Zone properties

In Advanced Settings:

- ⇒ **Note:** The options below control the forwarding policies between this zone (lan) and other zones. Destination zones cover forwarded traffic originating from lan. Source zones match forwarded traffic from other zones targeted at lan. The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.
- **Covered devices:** set to **unspecified**. Choose from drop-down menu to choose device. Use this option to classify zone traffic by raw, non-uci managed network devices.
- **Covered subnets:** Use this option to classify zone traffic by source or destination subnet instead of networks or devices. Add as needed.
- **IPv6 Masquerading:** box is unchecked by default. Enable network address and port translation IPv6 (NAT6 or NAPT6) for outbound traffic on this zone.
- **Restrict to address family:** set to **IPv4** and **IPv6**. Other options IPv4 only or IPv6 only.
- **Restrict Masquerading to given source subnets:** set to **0.0.0.0/0**. Can add subnets as needed.
- **Restrict Masquerading to given destination subnets:** set to **0.0.0.0/0**. Can add subnets as needed.
- **Enable logging on this zone:** box is unchecked by default

Firewall - Zone Settings

General Settings Advanced Settings Conntrack Settings

The options below control the forwarding policies between this zone (lan) and other zones. Destination zones cover forwarded traffic originating from lan. Source zones match forwarded traffic from other zones targeted at lan. The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.

Covered devices: unspecified

Use this option to classify zone traffic by raw, non-uci managed network devices.

Covered subnets: +

Use this option to classify zone traffic by source or destination subnet instead of networks or devices.

IPv6 Masquerading:

Enable network address and port translation IPv6 (NAT6 or NAPT6) for outbound traffic on this zone.

Restrict to address family: IPv4 and IPv6

Restrict Masquerading to given source subnets: 0.0.0.0/0 +

Restrict Masquerading to given destination subnets: 0.0.0.0/0 +

Enable logging on this zone:

Dismiss Save

Figure 181: Firewall Zone Settings – Advanced Settings tab

In Contrack Settings:

- **Allow “invalid” traffic:** box is unchecked by default. Do not install extra rules to reject forwarded traffic with contrack state invalid. This may be required for complex asymmetric route setups.
- **Automatic helper assignment:** box is checked by default. Automatically assign contrack helpers based on traffic protocol and port.

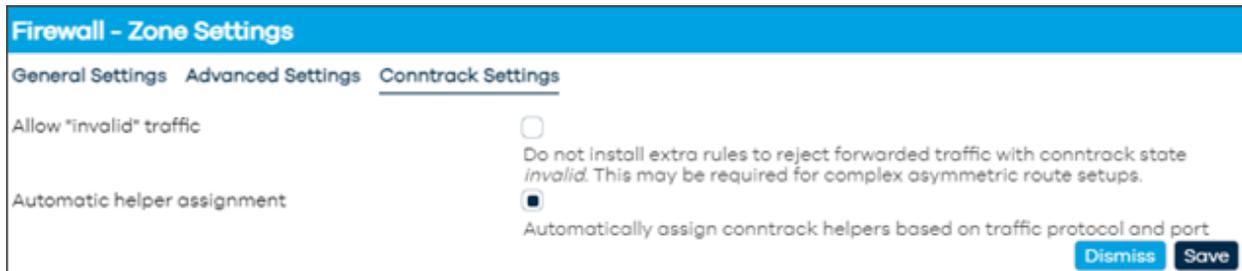


Figure 182: Firewall Zone Settings – Contrack Settings tab

More Zones can be added as needed using the **Add** button and will be similar configuration pages as just discussed in 4.4.6.1 Firewall – Zone Settings.

4.4.6.2 Firewall – Port Forwards

In Port Forwards, the user can add the ability to allow remote computers on the Internet to connect to a specific computer or service within the private LAN.

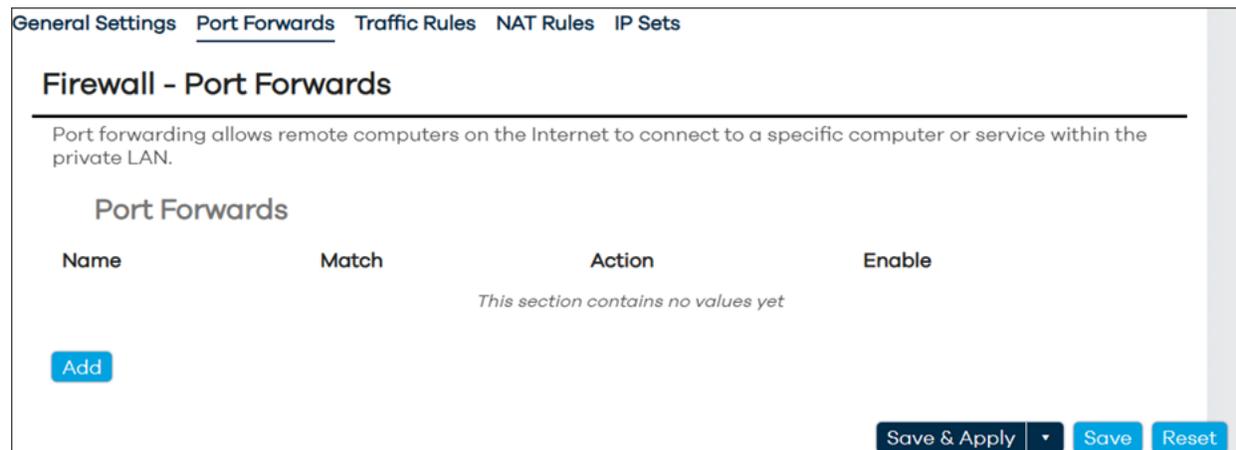


Figure 183: Firewall – Port Forwards page

Click on the '**Add**' button to enter Port Forwarding rule. Settings in **General Settings**:

- **Name:** Enter a name for the Port Forwarding rule
- **Restrict to address family:** set to **automatic**. Other options are IPv4 only and IPv6 only
- **Protocol:** set to **TCP** and **UDP**. Other options are Any, ICMP and custom

- **Source zone:** set to **wan** and **wwan**. Other options are unspecified and lan.
- **External port:** set the external port. Match incoming traffic directed at the given destination port or port range on this host.
- **Destination zone:** set to **lan**. Other options are unspecified, wan, and wwan
- **Internal IP address:** set to **any**. Other options are specified in the drop down menu. Redirect matched incoming traffic to the specified internal host.
- **Internal port:** set to **any**. Redirect matched incoming traffic to the given port on the internal host.

The screenshot shows the 'Firewall - Port Forwards - Unnamed forward' configuration window. The 'General Settings' tab is active. The configuration is as follows:

Field	Value
Name	Unnamed forward
Restrict to address family	automatic
Protocol	TCP UDP
Source zone	wan wan: wwan:
External port	
Destination zone	lan lan:
Internal IP address	any
Internal port	any

Below the fields, there are two explanatory lines: 'Match incoming traffic directed at the given destination port or port range on this host' and 'Redirect matched incoming traffic to the specified internal host'. At the bottom right, there are 'Dismiss' and 'Save' buttons.

Figure 184: Firewall Port Forwards – General Settings tab

In **Advanced Settings**, the following settings are:

- **Use ipset:** enter ipset to use
- **Source MAC address:** choose from drop down menu. Only match incoming traffic from these MACs.
- **Source IP address:** set to **any**. Other options are displayed in the drop-down menu. Only match incoming traffic from this IP or range.
- **Source port:** set to **any**. Only match incoming traffic originating from the given source port or port range on the client host.
- **External IP address:** set to **any**. Other options are displayed in the drop-down menu.
- **Enable NAT Loopback:** box checked by default.
- **Loopback source IP:** set to **Use internal IP address**. Other option is external IP address
- **Match helper:** set to **any**. Other options in the drop-down menu are: AMANDA, FTP, RAS, Q.931, IRC, NETBIOS-NS, PPTP, SANE, SIP, SNMP, TFTP, RSTP, or custom. Match traffic using the specified connection tracking helper.

- **Match mark:** enter a match mark that matches a specific firewall mark or a range of different marks.
- **Limit matching:** set to **unlimited**. Other options are 10/second, 60/minute, 3/hour, 500/day, or custom. Limits traffic matching to the specified rate.

Firewall - Port Forwards - Unnamed forward

General Settings Advanced Settings

Use ipset

Source MAC address

Source IP address

Source port

External IP address

Enable NAT Loopback

Loopback source IP

Match helper

Match mark

Limit matching

Dismiss Save

Figure 185: Firewall Port Forwards – Advanced Settings tab

4.4.6.3 Firewall – Traffic Rules

In **Traffic Rules**, define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router. Traffic Rule options are:

- **Allow-DHCP-Renew:** set to match incoming **IPv4**, protocol **UDP** from **wan** to this device, port **68**. Action set to **Accept input** and **Enabled** (box checked).
- **Allow-Ping:** set to match incoming **IPv4**, protocol **ICMP** from **wan** to *this device*. Action set to **Accept input** and **Enabled** (box checked).
- **Allow-IGMP:** set to match incoming **IPv4**, protocol **IGMP** from **wan** to this device. Action set to **Accept input** and **Enabled** (box checked).
- **Allow-DHCPv6:** set to match incoming **IPv6**, protocol **UDP** from **wan**, IP **fc00::/6** to this device, IP **fc00::/6**, port **546**. Action set to **Accept input** and **Enabled** (box checked).
- **Allow-MLD:** set to match incoming **IPv6**, protocol **ICMP** from **wan**, IP **fe80::/10** to this device. Action set to **Accept input** and **Enabled** (box checked).

- **Allow-ICMPv6-Input:** set to match incoming **IPv6**, protocol **ICMP** from **wan** to this device. Limit matching to 1000 packets per second. Action set to **Accept input** and **Enabled** (box checked).
- **Allow-ICMPv6-Forward:** set to match incoming **IPv6**, protocol **ICMP** from **wan** to **any zone**. Limit matching to 1000 packets per second. Action set to **Accept input** and **Enabled** (box checked).
- **Allow-IPSEC-ESP:** set to match Forwarded **IPv4** and **IPv6**, protocol **IPSEC-ESP** from **wan** to **lan**. Action set to **Accept input** and **Enabled** (box checked).
- **Allow-ISAKMP:** set to match Forwarded **IPv4** and **IPv6**, protocol **UDP** from **wan** to **lan**, port **500**. Action set to **Accept input** and **Enabled** (box checked).
- **Add your own:** select to add a rule not listed above.

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable
Allow-DHCP-Renew	Incoming IPv4, protocol UDP From wan To this device, port 68	Accept input	<input type="checkbox"/> Edit Delete
Allow-Ping	Incoming IPv4, protocol ICMP From wan To this device	Accept input	<input type="checkbox"/> Edit Delete
Allow-IGMP	Incoming IPv4, protocol IGMP From wan To this device	Accept input	<input type="checkbox"/> Edit Delete
Allow-DHCPv6	Incoming IPv6, protocol UDP From wan, IP fc00::/6 To this device, IP fc00::/6, port 546	Accept input	<input type="checkbox"/> Edit Delete
Allow-MLD	Incoming IPv6, protocol ICMP From wan, IP fe80::/10 To this device	Accept input	<input type="checkbox"/> Edit Delete
Allow-ICMPv6-Input	Incoming IPv6, protocol ICMP From wan To this device Limit matching to 1000 packets per second	Accept input	<input type="checkbox"/> Edit Delete
Allow-ICMPv6-Forward	Forwarded IPv6, protocol ICMP From wan To any zone Limit matching to 1000 packets per second	Accept forward	<input type="checkbox"/> Edit Delete
Allow-IPSec-ESP	Forwarded IPv4 and IPv6, protocol IPSEC-ESP From wan To lan	Accept forward	<input type="checkbox"/> Edit Delete
Allow-ISAKMP	Forwarded IPv4 and IPv6, protocol UDP From wan To lan, port 500	Accept forward	<input type="checkbox"/> Edit Delete

[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

Figure 186: Firewall Traffic Rules page

Use the **Edit** button next to a specific Traffic Rule to adjust and fine tune:

General Settings:

The screenshot shows the configuration page for a firewall rule named 'Allow-DHCP-Renew'. The 'General Settings' tab is active. The configuration is as follows:

Field	Value
Name	Allow-DHCP-Renew
Protocol	UDP
Source zone	wan wan:wan wwan:wan
Source address	-- add IP --
Source port	any
Destination zone	Device(input)
Destination address	-- add IP --
Destination port	68
Action	accept

Buttons: Dismiss, Save

Figure 187: Firewall Traffic Rules – Showing the Allow DHCP Renew rule General Settings

Advanced Settings:

The screenshot shows the configuration page for a firewall rule named 'Allow-DHCP-Renew'. The 'Advanced Settings' tab is active. The configuration is as follows:

Field	Value
Match device	unspecified
Restrict to address family	IPv4 only
Use ipset	
Source MAC address	-- add MAC --
Match helper	any
Match mark	
Match DSCP	any
Limit matching	unlimited

Buttons: Dismiss, Save

Figure 188: Firewall Traffic Rules – Showing the Allow DHCP Renew rule Advanced Settings

Time Restrictions:

The screenshot shows the 'Firewall - Traffic Rules - Allow-DHCP-Renew' configuration page. The 'Time Restrictions' tab is active. The fields are as follows:

- Week Days: Any day
- Month Days: Any day
- Start Time (hh:mm:ss):
- Stop Time (hh:mm:ss):
- Start Date (yyyy-mm-dd):
- Stop Date (yyyy-mm-dd):
- Time in UTC:

Buttons: Dismiss, Save

Figure 189: Firewall Traffic Rules Showing the Allow DHCP Renew rule Time Restrictions

4.4.6.4 Firewall – NAT Rules

In **NAT Rules**, allows fine grained control over the source IP to use for outbound or forwarded traffic.

The screenshot shows the 'Firewall - NAT Rules' configuration page. The page title is 'Firewall - NAT Rules'. Below the title is a description: 'NAT rules allow fine grained control over the source IP to use for outbound or forwarded traffic.' There is a table with columns: Name, Match, Action, and Enable. The table is empty, with the text 'This section contains no values yet' below it. There is an 'Add' button on the left and 'Save & Apply', 'Save', and 'Reset' buttons on the right.

Figure 190: Firewall NAT Rules page

Click on the '**Add**' button to enter a NAT Rule. Settings in **General Settings**:

- **Name:** Enter a name for the NAT rule
- **Restrict to address family:** set to **automatic**. Other options are IPv4 only and IPv6 only
- **Protocol:** set to **ANY**. Other options are TCP, UDP, ICMP, and custom
- **Outbound zone:** set to **lan**. Other options are Any zone, wan, and wwan.
- **Source address:** set to **any**. Other options are displayed in the drop-down menu.
- **Destination address:** set to **any**. Other options are displayed in the drop-down menu. Match forwarded traffic directed at the given IP address.
- **Action:** set to **SNAT** – Rewrite to specific source IP or port. Other options are MASQUERADE – Automatically rewrite to outbound interface IP, or ACCEPT – Disable address rewriting.

- **Rewrite IP address:** set to **unspecified**. Other options are specified in the drop-down menu. Redirect matched incoming traffic to the specified internal host.

The screenshot shows the 'General Settings' tab for a Firewall NAT Rule named 'Unnamed NAT'. The configuration is as follows:

Field	Value
Name	Unnamed NAT
Restrict to address family	automatic
Protocol	Any
Outbound zone	lan (highlighted)
Source address	any
Destination address	any
Action	SNAT - Rewrite to specific source IP or port
Rewrite IP address	unspecified

Buttons: Dismiss, Save

Figure 191: Firewall NAT Rules – General Settings tab

In Advanced Settings:

- **Outbound device:** set to **unspecified**. Other options are displayed in the drop-down menu. Matches forwarded traffic using the specified outbound network device.
- **Match mark:** enter a match mark that matches a specific firewall mark or a range of different marks.
- **Limit matching:** set to **unlimited**. Other options are **10/second**, **60/minute**, **3/hour**, **500/day**, or **custom**. Limits traffic matching to the specified rate.

The screenshot shows the 'Advanced Settings' tab for the same Firewall NAT Rule. The configuration is as follows:

Field	Value
Outbound device	unspecified
Match mark	
Limit matching	unlimited

Buttons: Dismiss, Save

Figure 192: Firewall NAT Rules – Advanced Settings tab

In Time Restrictions:

- **Week Days:** set to **Any day**. Choose specific days in the drop-drop menu.
- **Month Days** - set to **Any day**. Choose specific days in the drop-drop menu.
- **Start Time (hh:mm:ss)** – enter start time
- **Stop time (hh:mm:ss)** – enter stop time
- **Start Date (yyyy-mm-dd)** – enter start date
- **Stop Date (yyyy-mm-dd)** – enter stop date
- **Time in UTC** – Check box to set time in UTC

The screenshot shows the 'Time Restrictions' tab for an unnamed NAT rule. It features several input fields: 'Week Days' and 'Month Days' are dropdown menus both set to 'Any day'; 'Start Time (hh:mm:ss)', 'Stop Time (hh:mm:ss)', 'Start Date (yyyy-mm-dd)', and 'Stop Date (yyyy-mm-dd)' are empty text input fields; and 'Time in UTC' is an unchecked checkbox. At the bottom right, there are 'Dismiss' and 'Save' buttons.

Figure 193: Firewall NAT Rules – Time Restrictions tab

4.4.6.5 Firewall – IP Sets

In IP Sets, firewall4 supports referencing and creating IP sets to simplify matching of large address lists without the need to create one rule per item to match. Port ranges in ipsets are unsupported by firewall4.

The screenshot shows the 'IP Sets' configuration page. It includes a header with navigation tabs: 'General Settings', 'Port Forwards', 'Traffic Rules', 'NAT Rules', and 'IP Sets'. Below the header, there is a title 'Firewall - IP sets' and a descriptive paragraph: 'firewall4 supports referencing and creating IP sets to simplify matching of large address lists without the need to create one rule per item to match. Port ranges in ipsets are unsupported by firewall4.' A note states 'Your device runs firewall4.' Below this is a table titled 'IP Sets' with columns: 'Name', 'Family', 'Packet Field Match', 'IPs/Networks/MACs', 'Include File', and 'Enabled'. The table is currently empty, with the text 'This section contains no values yet' centered below it. An 'Add' button is located at the bottom left of the table area. At the bottom right, there are 'Save & Apply', 'Save', and 'Reset' buttons.

Figure 194: Firewall IP Sets

Click **'Add'** to add an IP Set rule.

- **Name:** enter a name for the IP Set
- **Comment:** add a comment
- **Family:** set to **IPv4**. Other option is **IPv6**
- **Packet Field Match:** Choose an option from the drop-down menu. Packet fields to match upon.
 - Syntax: `direction_datatype`. e.g.: `src_port, dest_net`.
 - Directions: `src, dst`. Datatypes: `ip, port, mac, net, set`.
 - Direction prefixes are optional.
- ↻ **Note:** datatype `set` is unsupported in fw4.
- **IPs/Networks/MACs:** enter a mac address: `macaddr|ip[/cidr]`
- **Max Entries:** enter max entries up to 65536
- **Include File:** Select file and upload. Path to file of CIDRs, subnets, host IPs, etc.
- **Timeout:** set timeout. Unit: seconds. Default 0 means the entry is added permanently to the set. Max: 2147483 seconds.
- **Counters:** check box to enable packet and byte count tracking for the set.

Firewall - IP sets

Name: Unnamed set

Comment: Comment

Family: IPv4

Packet Field Match: -- Please choose --

Packet fields to match upon.
 Syntax: `direction_datatype`. e.g.: `src_port, dest_net`.
 Directions: `src, dst`. Datatypes: `ip, port, mac, net, set`.
 Direction prefixes are optional.
 *Note: datatype `set` is unsupported in fw4.

IPs/Networks/MACs: macaddr|ip[/cidr]

Max Entries: up to 65536 entries.

Include File: Select file...
 Path to file of CIDRs, subnets, host IPs, etc.

Timeout: 0
 Unit: seconds. Default 0 means the entry is added permanently to the set.
 Max: 2147483 seconds.

Counters:
 Enables packet and byte count tracking for the set.

Dismiss Save

Figure 195: Firewall IP Sets – Adding a new IP Set

4.5 Logout

The user can log out of Mission Control by clicking on this button. This button is always visible in either **Overview** or **Expert Mode** on the left-hand pane towards the bottom.

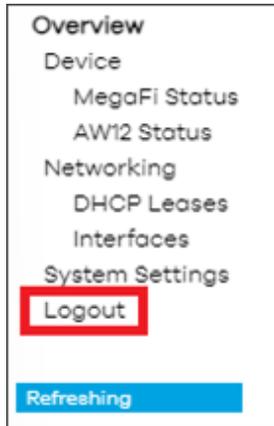


Figure 196: Overview menu in Overview mode



Figure 197: Overview menu in Expert mode

5.1 Appendix 1 – Firewall Traffic Rule for Remote SSH Example

If remote SSH access to the device is required and the device has a custom static/public IP address, do the following.

The first piece of setting remote SSH Access was described in section 3.13. The following will finalize what is required to allow traffic on this port to pass through the Firewall.

1. Navigate to **Overview > System Settings**.
2. Click on **Expert Configuration** to enter Expert Mode.

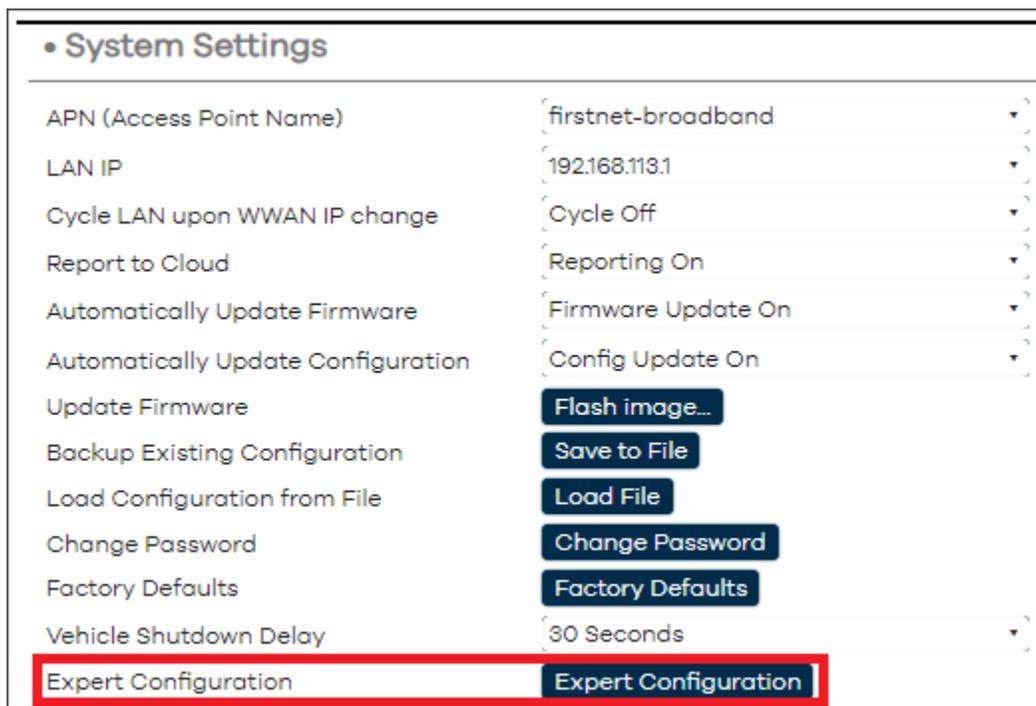


Figure 198: System Settings – Expert Configuration

3. A pop-up window asks the user to confirm going into Expert Mode. Click **OK** to continue.

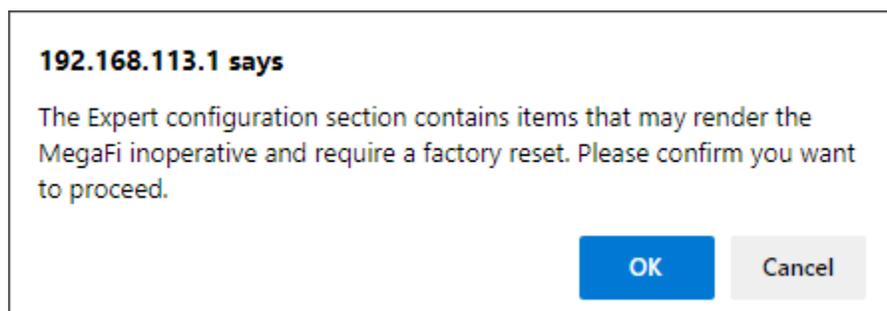


Figure 199: Confirmation to Enter Expert mode

The left-pane menu exposes pages only available in Expert Mode. Navigate to **Network > Firewall > Traffic Rules**.

4. Click on 'Add' at the bottom.

Mission Control Networking Mode: NAT Expert Mode Firmware Version: 2.5.0.E.8

General Settings Port Forwards Traffic Rules NAT Rules IP Sets

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Name	Match	Action	Enable
Allow-DHCP-Renew	Incoming IPv4, protocol UDP From wan To this device, port 68	Accept input	<input type="checkbox"/> Edit Delete
Allow-Ping	Incoming IPv4, protocol ICMP From wan To this device	Accept input	<input type="checkbox"/> Edit Delete
Allow-IGMP	Incoming IPv4, protocol IGMP From wan To this device	Accept input	<input type="checkbox"/> Edit Delete
Allow-DHCPv6	Incoming IPv6, protocol UDP From wan, IP fc00::/6 To this device, IP fc00::/6, port 546	Accept input	<input type="checkbox"/> Edit Delete
Allow-MLD	Incoming IPv6, protocol ICMP From wan, IP fe80::/10 To this device	Accept input	<input type="checkbox"/> Edit Delete
Allow-ICMPv6-Input	Incoming IPv6, protocol ICMP From wan To this device Limit matching to 1000 packets per second	Accept input	<input type="checkbox"/> Edit Delete
Allow-ICMPv6-Forward	Forwarded IPv6, protocol ICMP From wan To any zone Limit matching to 1000 packets per second	Accept forward	<input type="checkbox"/> Edit Delete
Allow-IPSec-ESP	Forwarded IPv4 and IPv6, protocol IPSEC-ESP From wan To lan	Accept forward	<input type="checkbox"/> Edit Delete
Allow-ISAKMP	Forwarded IPv4 and IPv6, protocol UDP From wan To lan, port 500	Accept forward	<input type="checkbox"/> Edit Delete

Add Save & Apply Save Reset

Figure 200: Firewall – Traffic Rules page

5. In **General Settings**, enter the following parameters:

- Give the Firewall Traffic Rule a descriptive name. We named it “Remote SSH”.
- Choose only **TCP** for the Protocol in the drop-down menu. Un-check **UDP** from its drop-down menu.
- Choose **wan/wwan** for Source zone in the drop-down menu.
- Choose **Device(input)** for Destination zone from the drop-down menu.
- For Destination address, select the drop-down arrow and enter the static/public IP address in the ‘–custom–’ field box at the bottom. Hit ‘Enter’ after entering the IP address.
- Enter port number **46556** in the Destination port field.
- **Save**
- **Save & Apply**

The screenshot shows the 'Firewall - Traffic Rules - Remote SSH' configuration page. The 'General Settings' tab is active. The configuration fields are as follows:

Field	Value
Name	Remote SSH
Protocol	TCP
Source zone	wan
Source address	-- add IP --
Source port	any
Destination zone	Device(input)
Destination address	107.89.21.27 (52:24:7F:7F:33:3B)
Destination port	46556
Action	accept

Buttons for 'Dismiss' and 'Save' are visible at the bottom right of the configuration area.

Figure 201: Firewall – Traffic Rules – Remote SSH

6. Once this is done, a remote client should be able to connect via a terminal, PowerShell, or Command prompt window with the following command:

- `ssh root@<static ip> -p <chosen port>`
- When prompted for the password, use the same password used to login to Misson Control.