



SHIELD MegaFi 2

Software Manual

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 Mission Control.....	7
2.1 Accessing Mission Control via Ethernet Connection	8
2.2 Initial Connection to MegaFi 2 via Wi-Fi	12
2.3 Navigating Mission Control.....	18
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	35
3.3 Flash/Update Firmware	37
3.4 Backup Existing Configuration.....	42
3.5 Load Configuration from File	43
3.6 Change Password.....	46
3.7 Factory Defaults via Mission Control	48
3.8 Vehicle Shutdown Delay	50
3.9 Reboot.....	51
3.10 Wireless Settings.....	53
3.11 NAT vs. Passthrough Mode.....	63
3.12 Band Lock	68
3.13 SSH Access.....	71
3.14 GPS Output Configuration	74
3.15 WAN/LAN Port Mode	83
3.16 LCD Configuration	84
3.17 SNMP	87
3.18 Client Isolation.....	90

3.19 Failover Primary Connection	93
3.20 Network Scan.....	96
3.21 IPSec VPN.....	99
3.22 Modify Hostname.....	103
3.23 eSIM Configuration	107
3.24 Firewall	117

Revision History

Rev	Iteration	Description	Incorporated By	Date
1	1	Initial Release for v3.1.6	Lorenzo Porchas	5/21/2025
1	2	Release for v3.3.x	Lorenzo Porchas	7/24/2025
1	3	Release for v3.4.x	Lorenzo Porchas	10/6/2025
1	4	Release for v3.5.x	Lorenzo Porchas	12/9/2025
1	5	Release for v3.6.x	Lorenzo Porchas	1/9/2026

1 | Introduction

The purpose of this manual is to assist the user in operating the SHIELD MegaFi 2 wireless WAN HPUE router. This manual will help the user configure and operate the device using the device's Mission Control software.

- ⓘ For assistance in implementing or installing the MegaFi 2 device, please refer to the separate *MegaFi 2 User Manual*.
- ⚡ **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 2 for your use.
- to provide the necessary information to understand the device and the options available in the MegaFi 2; 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 2 User Manual*: <https://nextivityinc.com/wp-content/uploads/2024/01/SHIELD-MegaFi-2-User-Manual.pdf>
- 📄 The *MegaPortal User Manual*: <https://go.nextivityinc.com/shield-megaportal-manual>
- 📄 For other *MegaFi 2* documentation, please go to <https://nextivityinc.com/products/shield-MegaFi-2-hpue/>

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

Table 1: Abbreviations and Acronyms

1.5 About OpenWRT and Mission Control

The OpenWRT software that the MegaFi 2 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 2 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 Basic Configuration Settings and part 4 (forthcoming) 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, we recommend reading it in its entirety and reaching out with any questions.

Part 3 is Basic 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 (forthcoming) 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, please 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 2 router and allows the user to configure settings to their preferences. All configuration and management are done via your workstation or laptop 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. Remote access to Mission Control is also possible through MegaPortal. Please refer to the MegaPortal Manual for guidance on remote access to Mission Control.

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 2 or on the LCD display screen.

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

⌚ **Note:** Beginning in firmware release version 3.4.1, once the default password is changed, the password will no longer be displayed on the display screen. To re-enable this device password to be displayed back on the display screen, go to section 3.16 LCD Configuration for details.

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

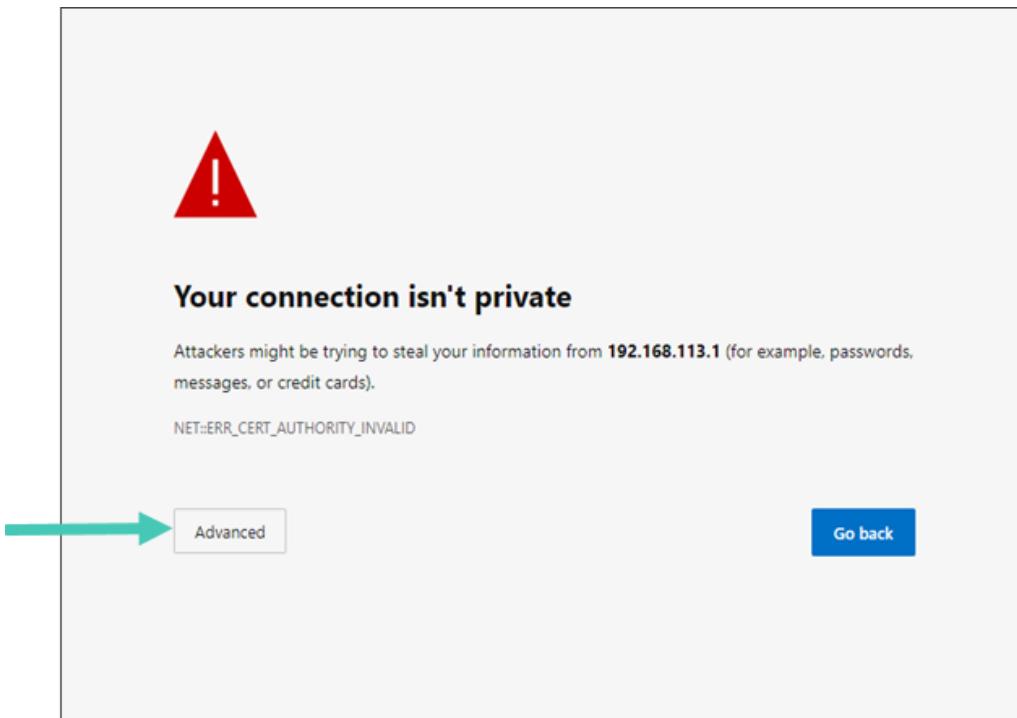


Figure 1: MegaFi 2 connection warning screen

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

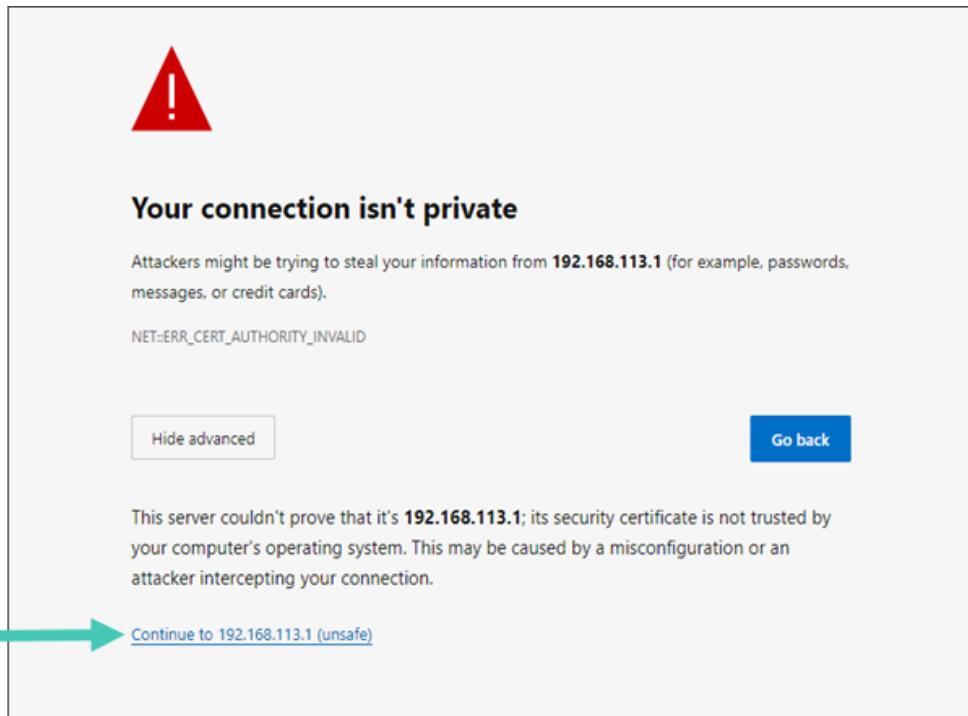


Figure 2: MegaFi 2 connection warning – second screen

5. The MegaFi 2's Mission Control GUI login page will now be displayed.
 - 5a. Enter the password as found on the bottom label or on the LCD display screen of the MegaFi 2 on the Mission Control login page.
 - 5b. Click **Login** to proceed.

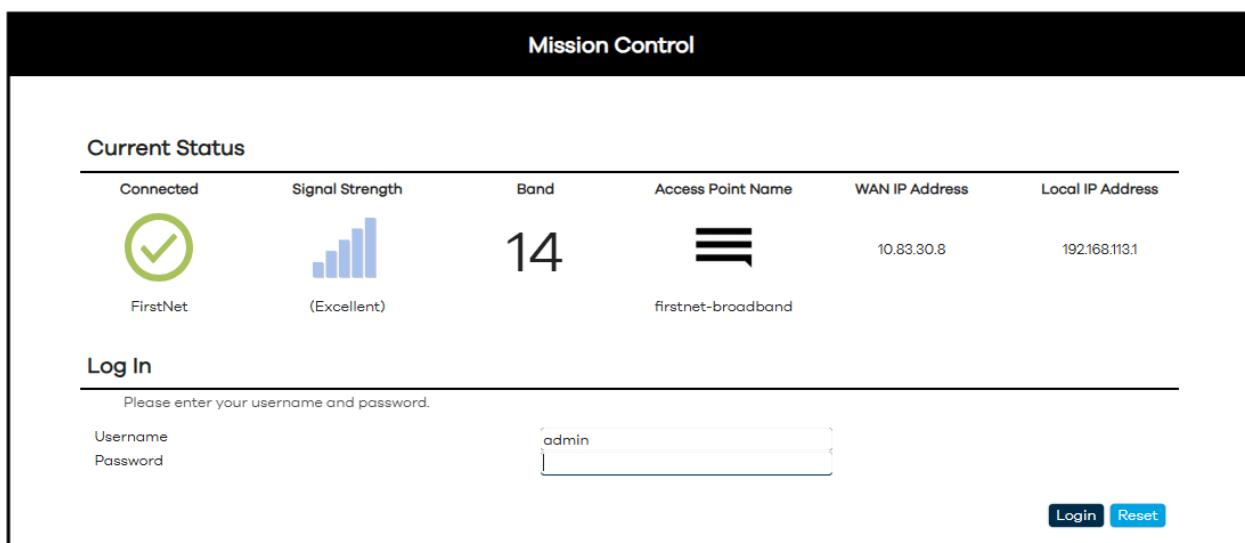


Figure 3: Mission Control Log-In screen

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.

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 initializes 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

Accept **Decline**

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

8. Also, as part of first-time login to MegaFi 2, the user will be required to change the default login password.
 - 8a. Proceed to change the default password to a 'Strong' password in the **Password** field.
 - 8b. Confirm the new password in the **Confirmation** field, then click on **Save**.

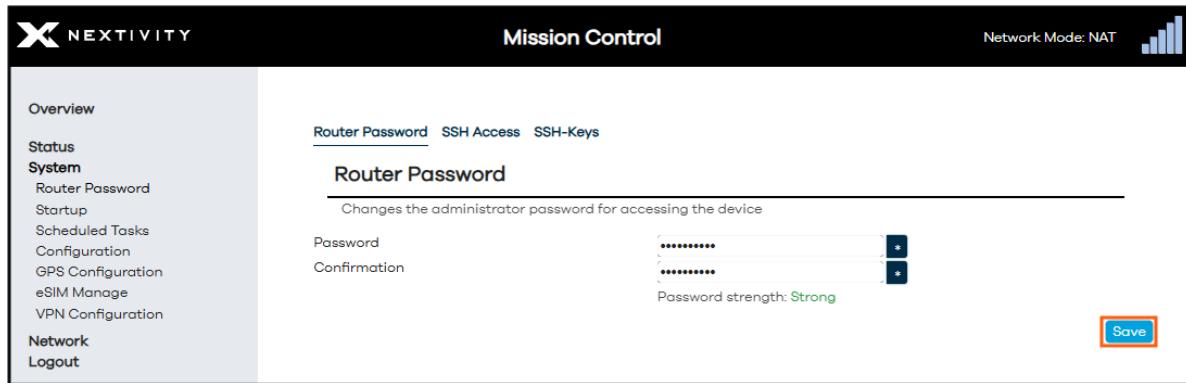


Figure 5: Change Router Password screen

9. The user will now be redirected to Mission Control's Overview page.

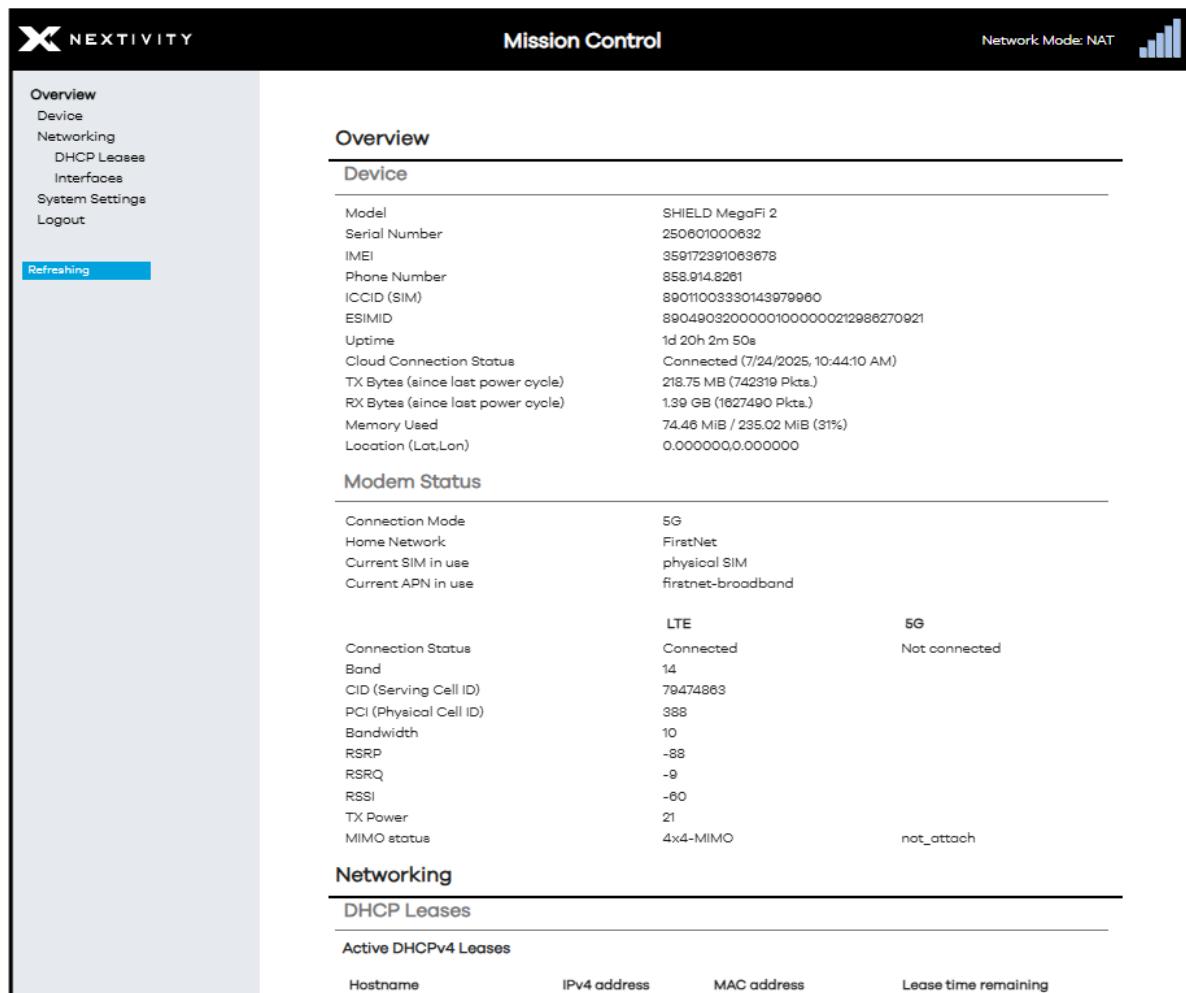


Figure 6: Mission Control – Overview page

10. First-time router configuration is now complete!

2.2 Initial Connection to MegaFi 2 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 2 or on the LCD display screen.

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.
- ⌚ Handheld devices can automatically connect to MegaFi 2's Wi-Fi by scanning the QR code from the LCD Display screen, but it may become difficult to configure certain settings. Therefore, it is highly recommended to configure settings using a computer workstation or laptop.

To connect to MegaFi 2 via Wi-Fi using a PC:

1. Go into your PC's **Network & internet > Wi-Fi** settings to add a new Wi-Fi connection.
2. Select your MegaFi 2 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 located underneath the device or it can be found on the LCD display screen.

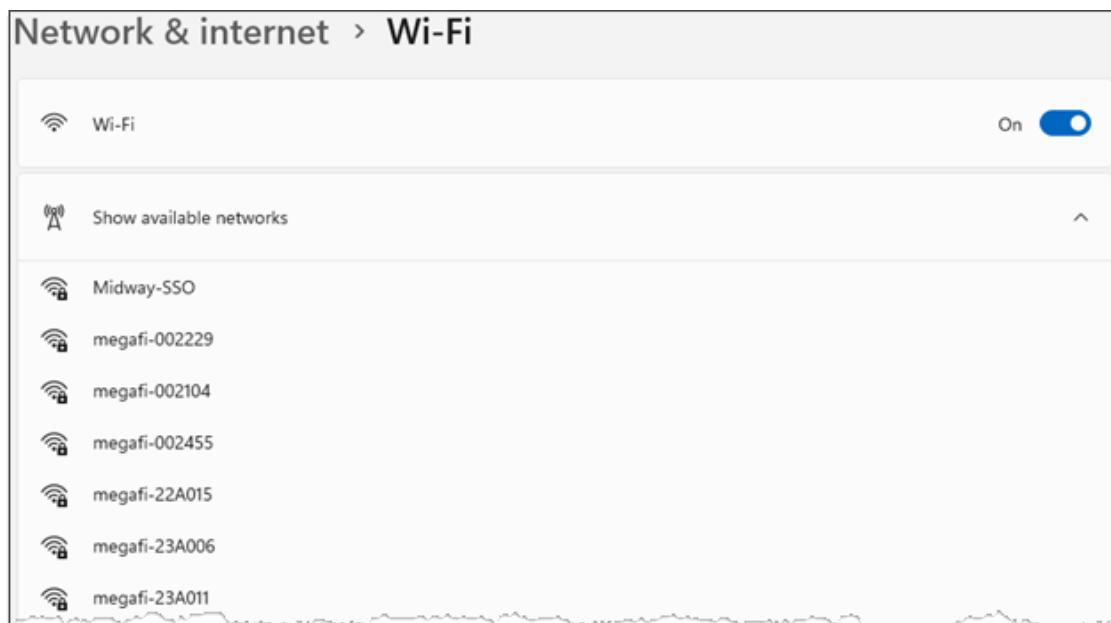


Figure 7: Windows network & internet window showing list of available Wi-Fi networks

3. The **Connect automatically** box may or may not be checked by default. Select as desired then 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**.

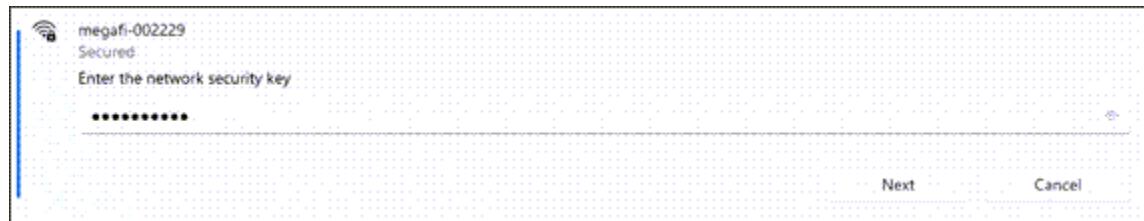


Figure 9: Wi-Fi Network Connection – Enter network security key

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 URL address: <https://192.168.113.1>
7. The first time you try to connect to MegaFi 2, a connection warning screen will display as shown below. Accept the connection warning by clicking on **Advanced**.

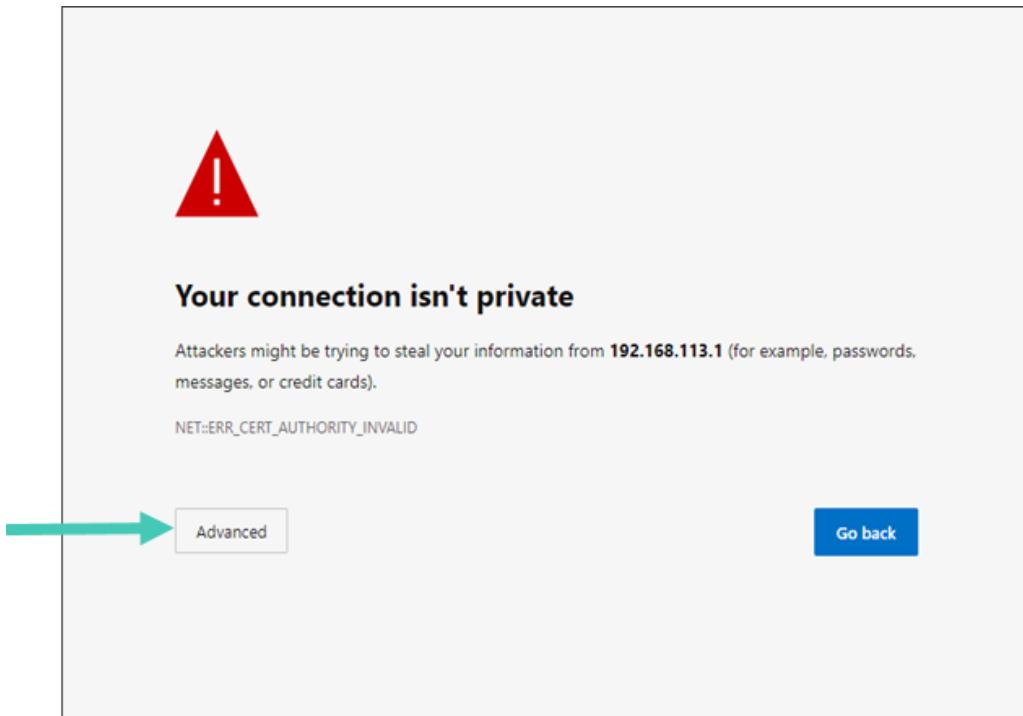


Figure 11: Warning message – Connection not private

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

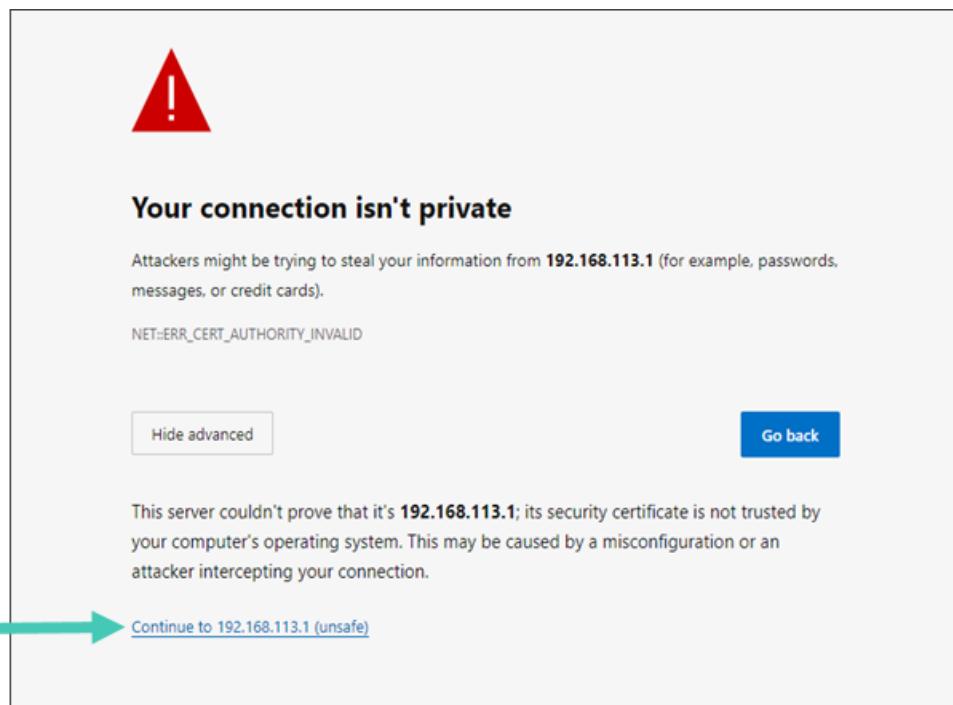


Figure 12: Warning message – Continue to IP address

9. The MegaFi 2's Mission Control GUI login page will now be displayed.

9a. Enter the password as found on the bottom label or on the LCD display of the MegaFi 2 on the Mission Control login page.

⌚ **Note:** The username always defaults to **admin**.

9b. Click **Login** to proceed.

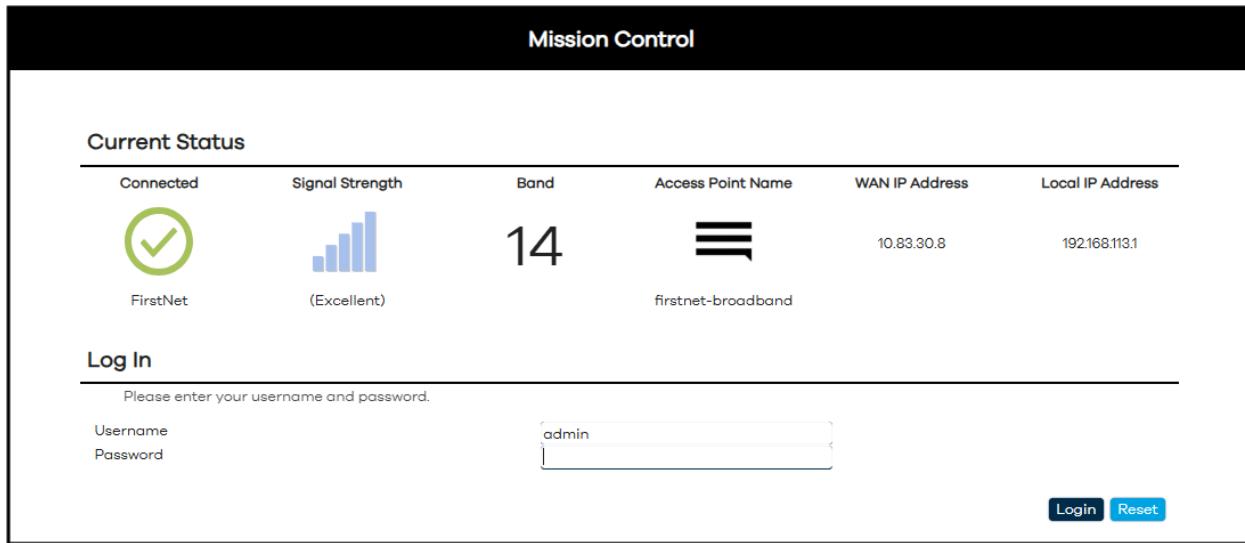


Figure 13: Mission Control – Log In page

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

Accept **Decline**

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

11. Also, as part of first-time login to MegaFi 2, the user will be required to change the default login password.

11a. Proceed to change the default password to a 'Strong' password in the **Password** field.

➲ **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 in the **Confirmation** field, then click on **Save**.

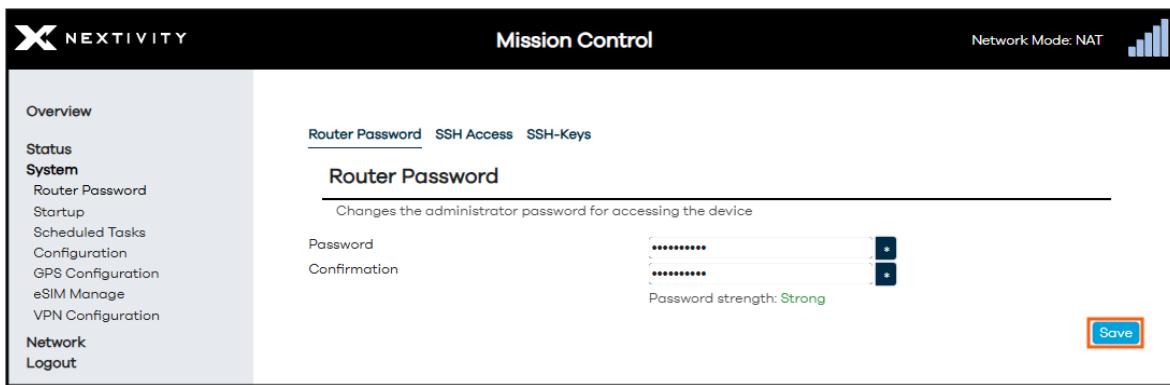


Figure 15: Change Router Password screen

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

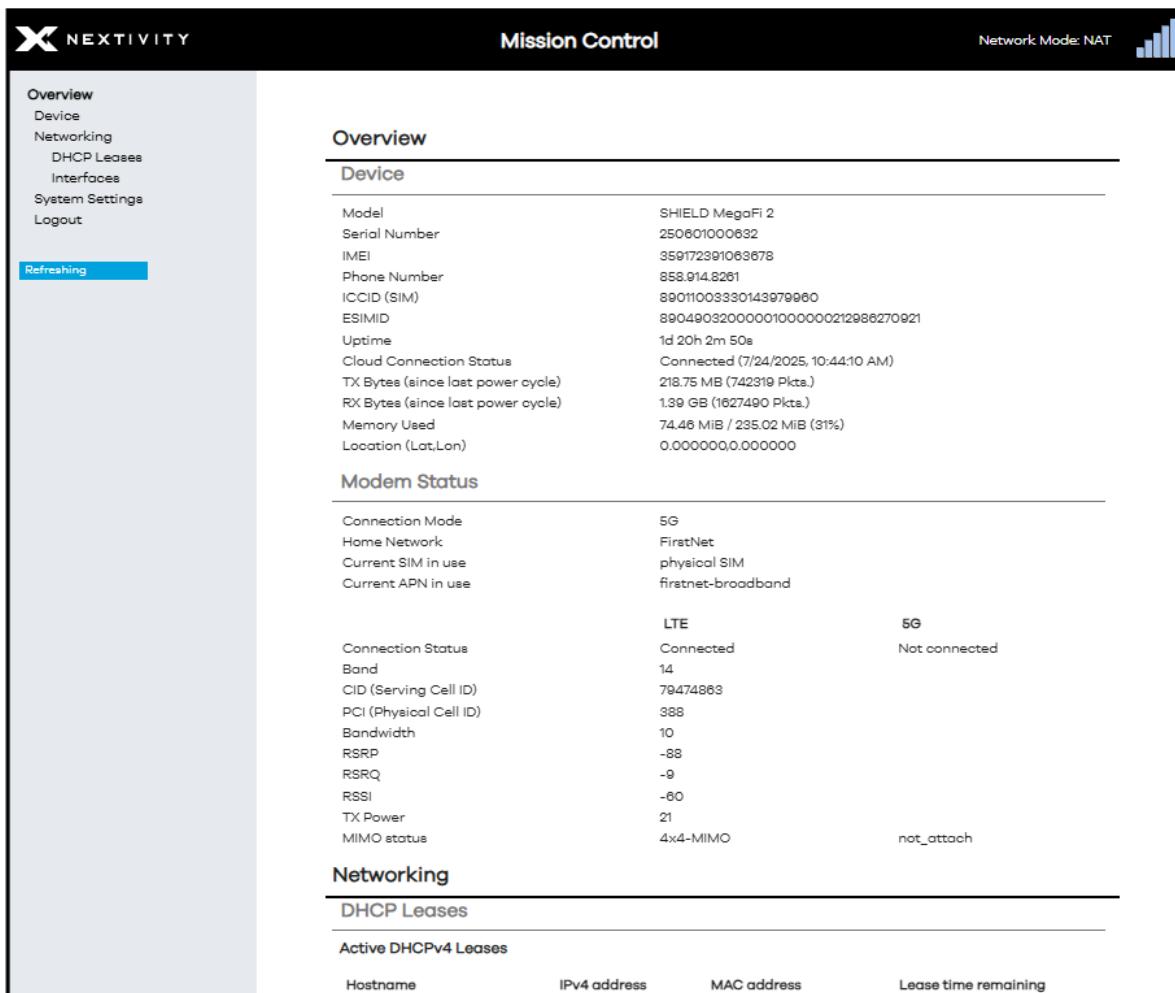


Figure 16: Mission Control – Overview page

14. First-time router configuration is now complete!

2.3 Navigating Mission Control

Once logged into Mission Control, the first page the user will see is the **Overview** page.

Overview

Device

Model	SHIELD MegaFi 2
Serial Number	250601000632
IMEI	359172391068678
Phone Number	858.914.8261
ICCID (SIM)	8901003330143979960
ESIMID	8904903200001000000212986270921
Uptime	1d 20h 2m 50s
Cloud Connection Status	Connected (7/24/2025, 10:44:10 AM)
TX Bytes (since last power cycle)	218.75 MB (742319 Pkts.)
RX Bytes (since last power cycle)	1.39 GB (1627490 Pkts.)
Memory Used	74.46 MiB / 235.02 MiB (31%)
Location (Lat,Lon)	0.000000,0.000000

Modem Status

Connection Mode	5G
Home Network	FireNet
Current SIM in use	physical SIM
Current APN in use	firenet-broadband
Connection Status	LTE
Band	Connected
CID (Serving Cell ID)	14
PCI (Physical Cell ID)	79474863
Bandwidth	388
RSRP	10
RSRQ	-88
RSSI	-9
TX Power	-60
MIMO status	21
	4x4-MIMO
	not_attach

Networking

DHCP Leases

Active DHCPv4 Leases

Hostname	IPv4 address	MAC address	Lease time remaining
----------	--------------	-------------	----------------------

Figure 17: Mission Control – Overview page

2.3.1 Top Banner

The top banner area, which is consistently displayed on every navigation page, will show the current Network mode and cellular signal strength information towards the top right area.



Figure 18: Mission Control – top banner

Network Mode	NAT (default) or Passthrough mode
Signal Strength	The number of cellular signal strength bars that should match up with the bars on the device LCD Display screen.

Table 2: Network Mode and Signal Strength

2.3.2 Navigation Pane

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



Figure 19: Mission Control Navigation Pane – Overview menu

- a:** In the main **Overview** page, the Top-level menu section consists of four on-page topics: **Device**, **Networking**, **System Settings**, and **Logout**.
- b:** If any, the second-level sub-menu contains on-page quick links.

For example, Figure 19 shows the top-level **Networking** menu item with its second-level sub-menu items of **DHCP Leases** and **Interfaces**. Clicking on any of those options will take you to that area of the current Top-level selection.

- c:** Selecting the **Logout** option will log you out of Mission Control.

When the user navigates into Expert Configuration mode by clicking on the **Expert Configuration** button, located in the **System Settings** under **Admin Tools**, the navigation pane on the left exposes different selectable options and lands the user inside the **General** page (Second-level page) under **Status** (Top-level menu).

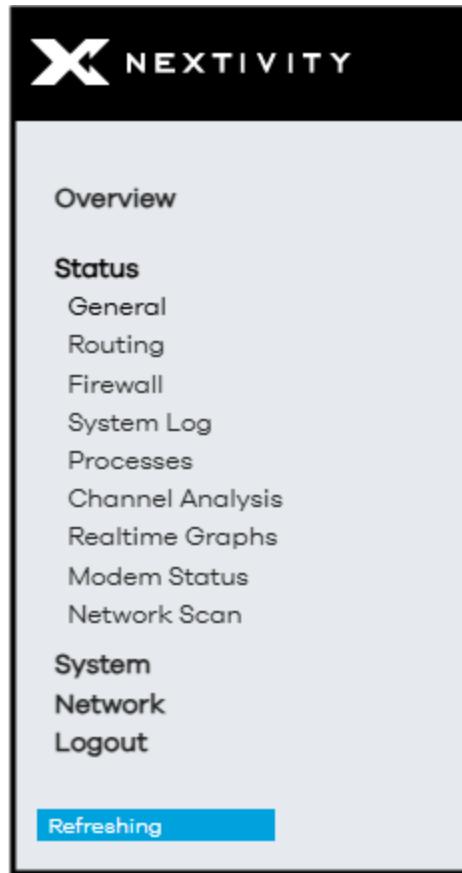


Figure 20: Mission Control Navigation Pane – Expert Configuration mode menu

- d: There is a link back to the main **Overview** page at the top. Click on it to go back to the main **Overview** page.
- e: The Top-level menu section consists of four new topics with links to different pages under each: **Status**, **System**, **Network**, and **Logout**.
- f: If any, the second-level sub-menu in this area contains a variable number of page links. For example, Figure 20 shows the top-level **Status** menu item with its second-level sub page links to **General**, **Routing**, **Firewall**, **System Log**, **Processes**, **Channel Analysis**, etc. Clicking on any of those page link options will take you to that page of the current Top-level selection.
- g: Selecting the **Logout** option will log you out of Mission Control.

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 and applied, reset/discard, 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, avoids slowing your workflow.

2.4.1 Save Options

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

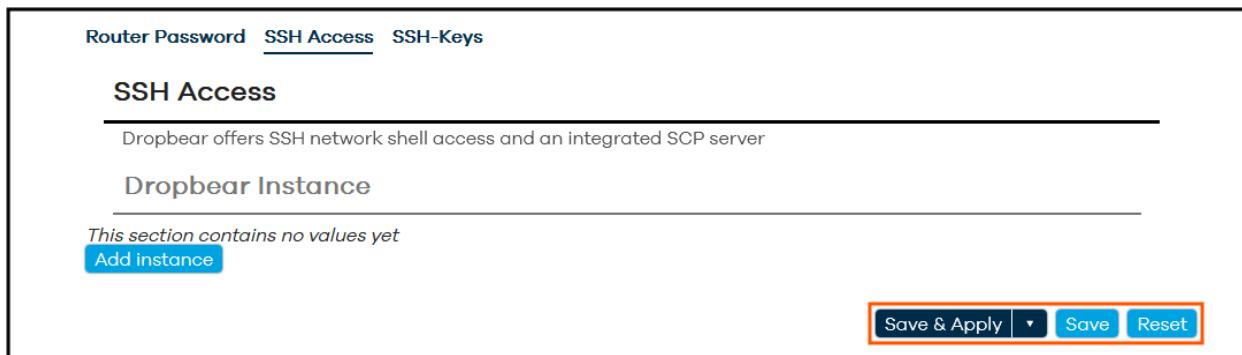


Figure 21: Mission Control – Save options

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**.

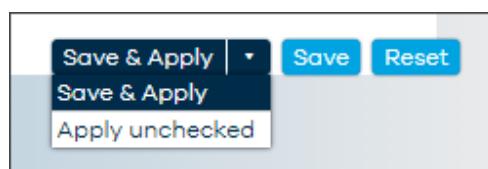


Figure 22: Mission Control – Save options

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 as a result of saving changes).

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



Figure 23: Navigation pane showing pending Unapplied 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 indicated by its color, 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**

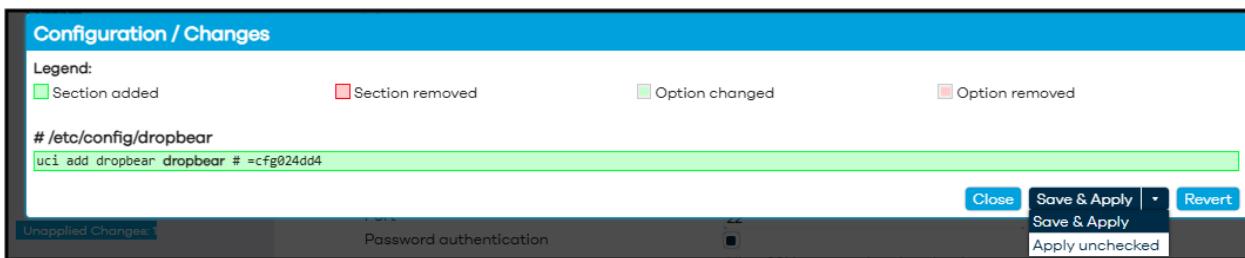


Figure 24: Configuration/Changes showing button options

- 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.
- 2c. **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, clears the list of any pending changes, and displays the “changes have been reverted” message as a popup, and then takes 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 2 during any updates.

2.4.5 Apply Unchecked

When updating certain attributes, such as the LAN IP address or other 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 are maintained. However, if, during this check, the system determines that either would be lost because of the change, it will 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.

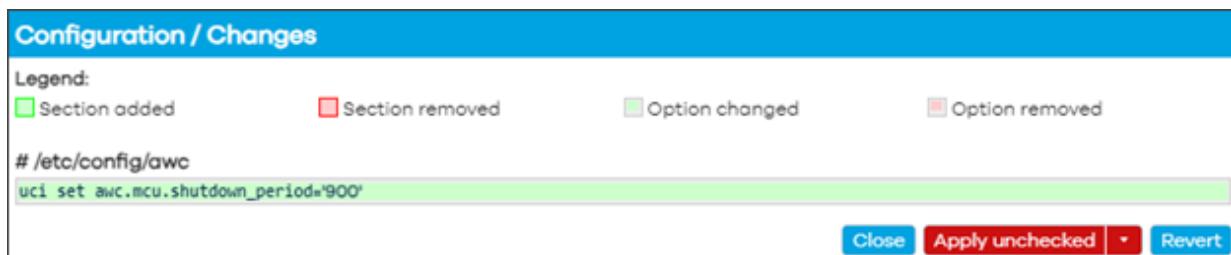


Figure 25: Configuration/Changes showing applied configuration changes

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.

Overview

Device

Model	SHIELD MegaFi 2
Serial Number	250601000632
IMEI	359172391063678
Phone Number	858.914.8261
ICCID (SIM)	89011003330143979060
ESIMID	8904903200001000000212986270921
Uptime	1d 20h 2m 50s
Cloud Connection Status	Connected (7/24/2025, 10:44:10 AM)
TX Bytes (since last power cycle)	218.75 MB (742319 Pkts.)
RX Bytes (since last power cycle)	1.39 GB (1627490 Pkts.)
Memory Used	74.46 MiB / 235.02 MiB (31%)
Location (Lat,Lon)	0.000000,0.000000

Modem Status

Connection Mode	5G
Home Network	FirstNet
Current SIM in use	physical SIM
Current APN in use	firtnet-broadband
LTE	5G
Connection Status	Connected
Band	14
CID (Serving Cell ID)	79474863
PCI (Physical Cell ID)	388
Bandwidth	10
RSRP	-88
RSRQ	-9
RSSI	-60
TX Power	21
MIMO status	4x4-MIMO
	not_attach

Networking

DHCP Leases

Hostname	IPv4 address	MAC address	Lease time remaining

Active DHCPv4 Leases

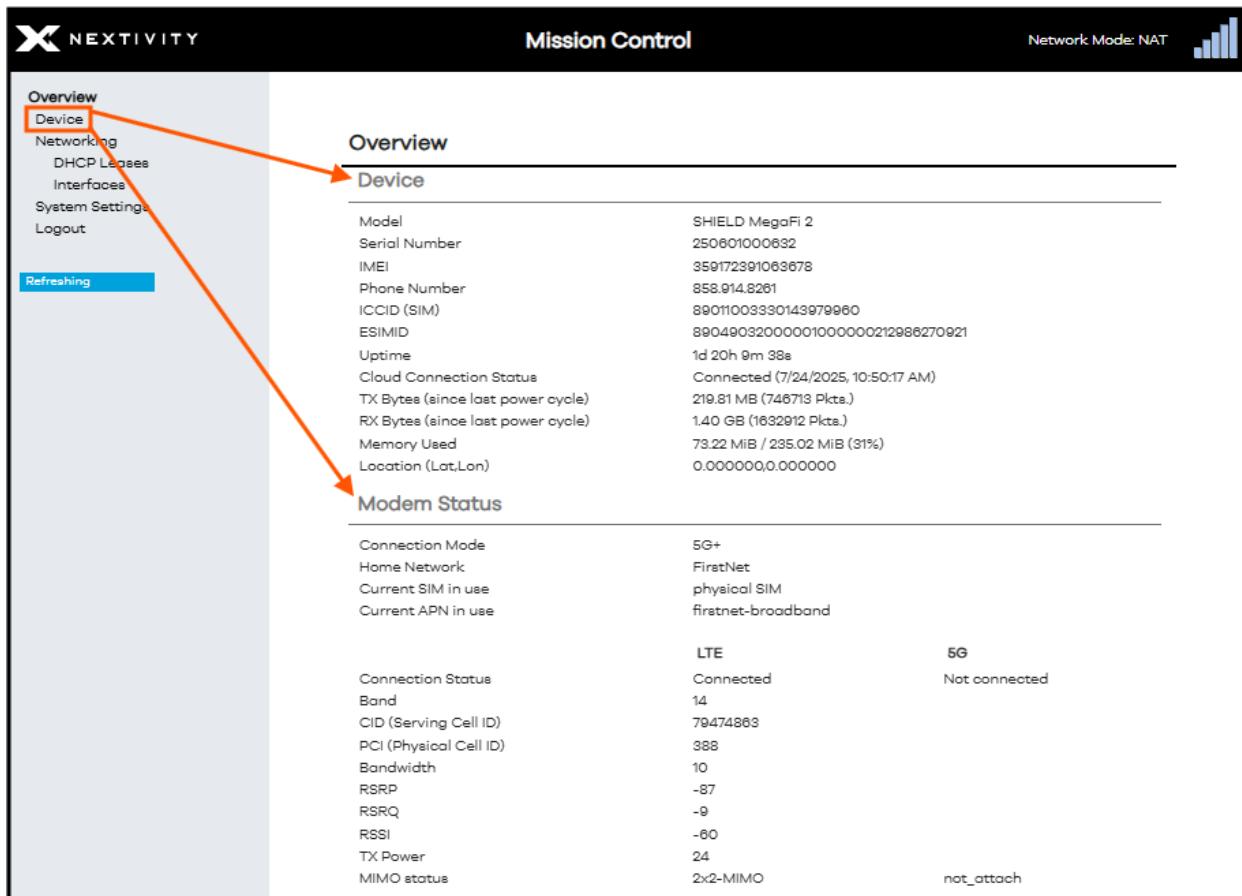
Hostname	IPv4 address	MAC address	Lease time remaining

Figure 26: Mission Control – Overview page

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

2.4.7.1 Device

For a detailed summary of the device, view the **Device** section. Right below is the **Modem Status** area for **Connection Mode** and **Connection Status**, as well as cellular network information and other statistics.



The screenshot shows the NEXTIVITY Mission Control interface. The left sidebar has a 'Refreshing' button and a menu with 'Overview', 'Device' (which is selected and highlighted with a red box), 'Networking', 'DHCP Leases', 'Interfaces', 'System Settings', and 'Logout'. The main content area is titled 'Mission Control' and 'Network Mode: NAT'. It shows 'Overview' and 'Device' sections. The 'Device' section contains detailed device information:

Model	SHIELD MegaFi 2
Serial Number	250801000632
IMEI	359172391063678
Phone Number	858.914.8281
ICCID (SIM)	8901003330143979960
ESIMID	890490320000100000212986270921
Uptime	1d 20h 9m 38s
Cloud Connection Status	Connected (7/24/2025, 10:50:17 AM)
TX Bytes (since last power cycle)	219.81 MB (746713 Pkts.)
RX Bytes (since last power cycle)	1.40 GB (1632912 Pkts.)
Memory Used	73.22 MiB / 235.02 MiB (31%)
Location (Lat,Lon)	0.000000,0.000000

The 'Modem Status' section shows LTE and 5G status:

Connection Mode	5G+
Home Network	FireNet
Current SIM in use	physical SIM
Current APN in use	firenet-broadband
Connection Status	Connected
Band	14
CID (Serving Cell ID)	79474863
PCI (Physical Cell ID)	388
Bandwidth	10
RSRP	-87
RSRQ	-9
RSSI	-60
TX Power	24
MIMO status	2x2-MIMO
	5G
	Not connected

Figure 27: Mission Control – Device

2.4.7.2 Networking

Clicking on **Networking** on the left-hand menu, the main window displays detailed information for **DHCP Leases** for connected hosts and **Interfaces: LAN, WAN, WAN6, WWAN, and Active Connections**.

Networking

DHCP Leases

Hostname	IPv4 address	MAC address	Lease time remaining
LPORCHAS-LT	192.168.113.140	BC:F4:D4:6F:D8:C1	0h 50m 12s
LPORCHAS-TEST	192.168.113.10	18:DB:F2:42:1A:80	unlimited
IBR1700-c2f	192.168.113.130	00:30:44:33:4C:2F	0h 41m 34s
Lorenzo-s-S25-Ultra	192.168.113.144	76:E2:CB:97:46:3E	0h 56m 8s

Active DHCPv6 Leases

Host	IPv6 address	DUID	Lease time remaining
There are no active leases			

Interfaces

Type	MAC	RX	TX	IPv4	IPv6
LAN	34:BA:9A:C3:68:B4	22.74 MB (81282 Pkts.)	146.46 MB (122949 Pkts.)	192.168.113.1/24	fdca:cd5b:b5b2::1/64
WAN	34:BA:9A:C3:68:B7	0 B (0 Pkts.)	0 B (0 Pkts.)		
WAN6	34:BA:9A:C3:68:B7	0 B (0 Pkts.)	0 B (0 Pkts.)		
WWAN	02:0F:5A:28:48:0D	43.93 MB (64684 Pkts.)	13.36 MB (54324 Pkts.)	10.209.129.136/28	2600:380:30e8:4e55:9898:a499:a5f7:120/64

Active Connections

287 / 15360 (1%)

Figure 28: Mission Control – Networking

2.4.7.3 System Settings

Clicking on **System Settings** on the left-hand menu, the main window displays Admin Tools for:

- **Primary SIM**
- **Physical SIM APN selection**
- **Physical SIM custom APN**
- **eSIM APN selection**
- **eSIM custom APN**
- **LAN IP**
- **WAN/LAN Port Mode**
- **Update Firmware**
- **Backup Existing Configuration**
- **Load Configuration from File**
- **Change Password**
- **Factory Defaults**
- **Vehicle Shutdown Delay**

- **Expert Configuration**
- **Reboot**

The user has complete access to all these configuration features from this environment without needing to be in **Expert Configuration** mode.

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

Admin Tools

System Settings

Primary SIM	physical SIM
Physical SIM APN selection	Automatic
Physical SIM custom APN	firstnet-broadband
eSIM APN selection	Automatic
eSIM custom APN	[dropdown]
LAN IP	192.168.113.1
WAN/LAN Port Mode	WAN
Update Firmware	Upload Firmware
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
Reboot	Reboot

Save & Apply
Save
Reset

Figure 29: Mission Control – System Settings

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 Configuration Mode located on the lefthand pane towards the bottom.



Figure 30: Logout from Overview mode

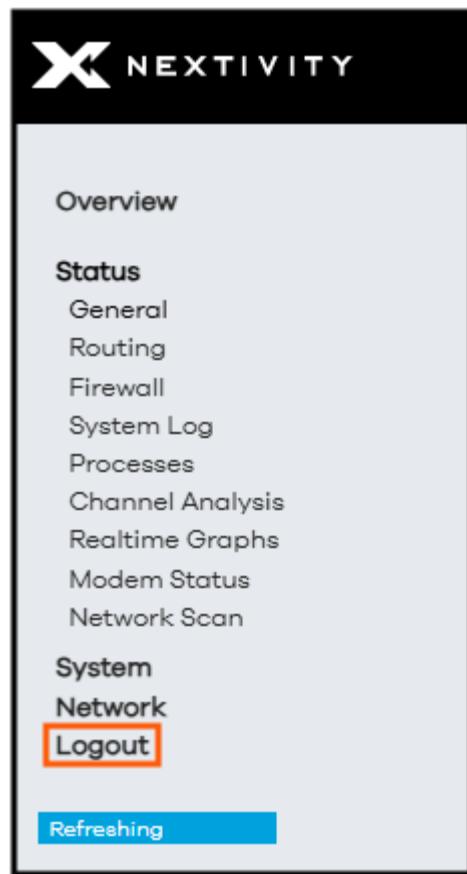


Figure 31: Logout from Expert Configuration mode

3 | Basic Configuration Settings

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

3.1 Changing APN (Access Point Name)

By default, the **Physical SIM APN selection** is set to **Automatic** and the **Physical SIM custom APN** will automatically detect and configure itself when a **firstnet-broadband** or an Enterprise **(broadband)** SIM is installed. If the user has a custom APN SIM card, do the following to manually change the **Physical SIM custom APN** in Mission Control:

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click the drop-down menu next to **Physical SIM APN selection** and select **Custom**.
3. Click on the **Save & Apply** button at the bottom to confirm the change.

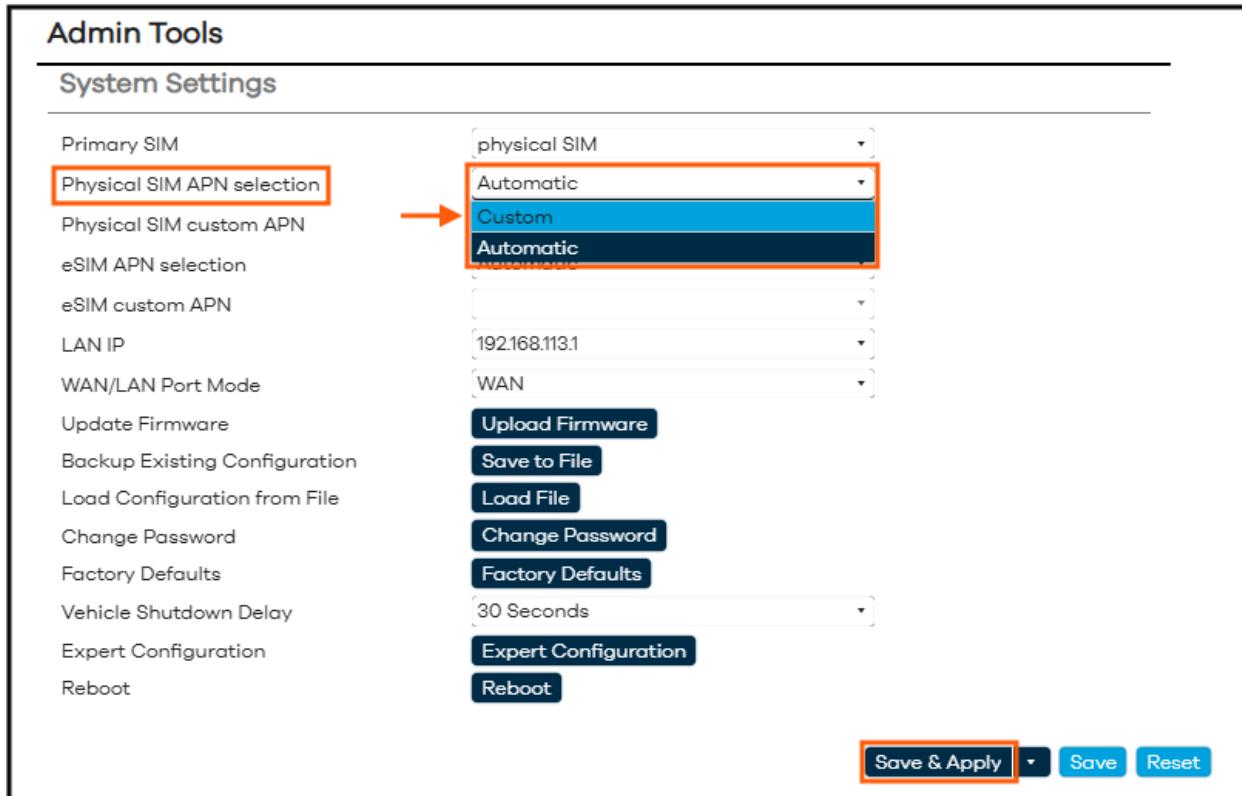


Figure 32: System Settings – Physical SIM APN selection

4. Now click the drop-down menu next to **Physical SIM custom APN** and click inside the custom field.
5. Correctly type in the APN name associated with the SIM card into the custom field and hit **Enter**. Otherwise, it will revert to its default setting, or pre-configured APN.
6. Click on the **Save & Apply** button at the bottom to confirm the change.

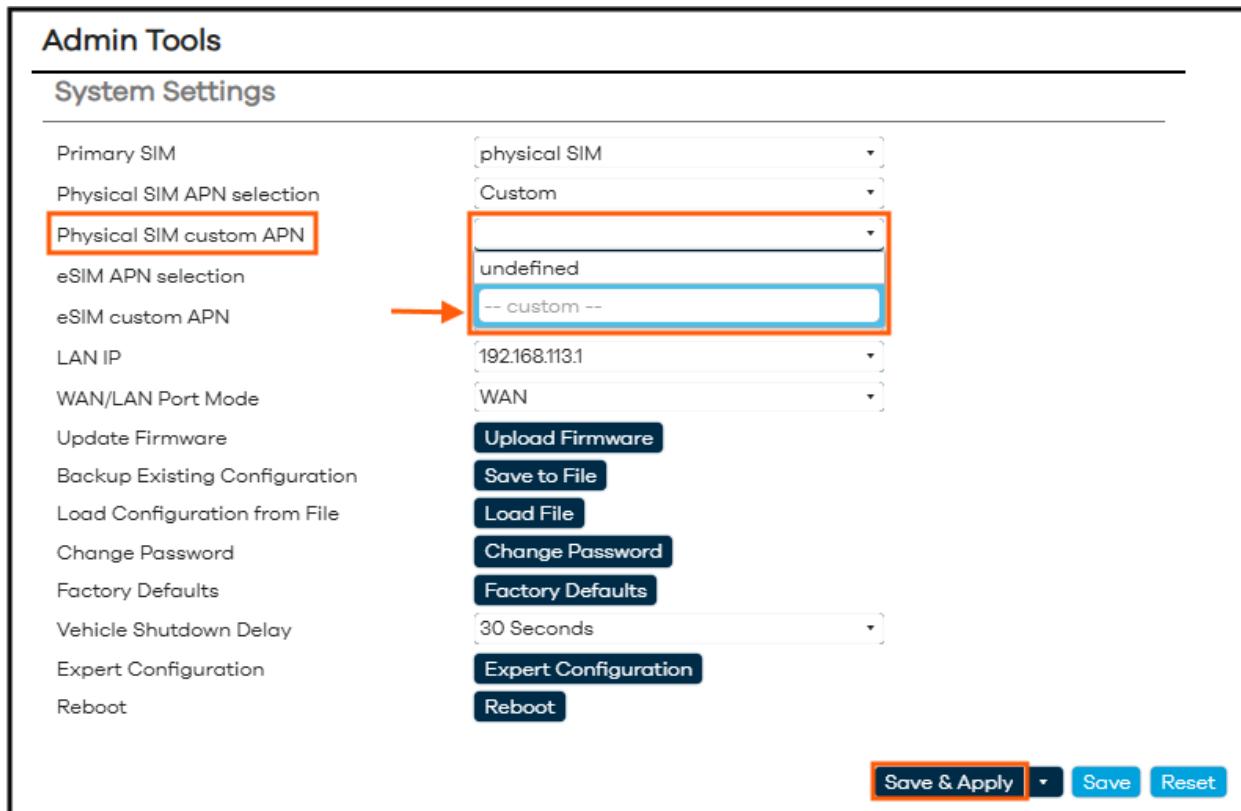


Figure 33: System Settings – Physical SIM custom APN

7. Give the device a few minutes to successfully regain network connectivity.
8. After the device becomes available, issue a **Reboot** so the device receives the correct IP address and any other provisioned network settings. See Section 3.9 for Reboot procedure.
9. To validate the custom IP address associated with your custom APN, navigate to **Overview > Networking** and verify the **WWAN IPv4** address under **Interfaces** and make sure it is what you are expecting.

Networking

DHCP Leases

Active DHCPv4 Leases

Hostname	IPv4 address	MAC address	Lease time remaining
LPORCHAS-LT	192.168.113.140	BC:F4:D4:6F:D8:C1	11h 59m 30s
LGgram	192.168.113.173	00:24:9B:2D:48:17	11h 55m 4s

Active DHCPv6 Leases

Host	IPv6 address	DUID	Lease time remaining
There are no active leases			

Interfaces

Type	MAC	RX	TX	IPv4	IPv6
LAN	34:BA:9A:C3:54:92	3.51 MB (14477 Pkts.)	18.81 MB (14354 Pkts.)	192.168.113.1/24	fdca:cd5b:b5b2:1/64
WAN	34:BA:9A:C3:54:95	0 B (0 Pkts.)	0 B (0 Pkts.)		
WAN6	34:BA:9A:C3:54:95	0 B (0 Pkts.)	0 B (0 Pkts.)		
WWAN	EA:F1:5D:46:CB:A4	2.45 MB (8121 Pkts.)	2.17 MB (8473 Pkts.)	107.89.21.27/29	

Active Connections  390 / 15360 (2%)

Figure 34: Networking – WWAN IPv4 Address

3.2 Changing LAN IP Address

By default, the **LAN IP** address of the device 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 in Mission Control:

➲ **Note:** In this environment, the system automatically sets a /24 or Class C network and will provide IP addresses to devices within this range.

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

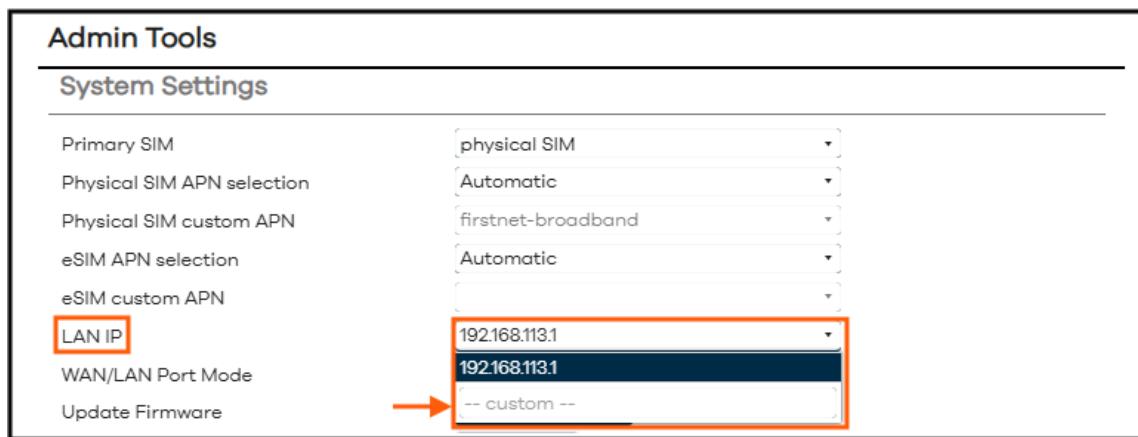


Figure 35: System Settings – Changing LAN IP Address

3. Enter the new IP address in the custom field and hit **Enter**. Otherwise, it will revert to its default setting, or pre-configured IP address.
4. After clicking on **Enter** above, a popup window will warn the user that the system will be temporarily unreachable and that a manual reconfiguration of the URL address in the web browser address bar will be required to regain access to the device as soon as the change is committed.

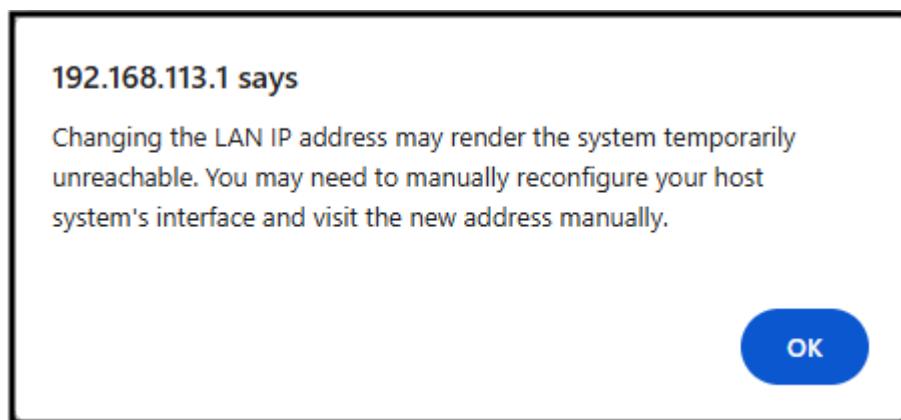


Figure 36: LAN IP address warning

5. Click on the **Save & Apply** button at the bottom to confirm the change.
6. A **Connectivity change** popup message will appear, warning the user that current access to the device will be interrupted if the user proceeds. The user is given options to either **Cancel**, **Apply with revert after connectivity loss**, or **Apply and keep settings**.

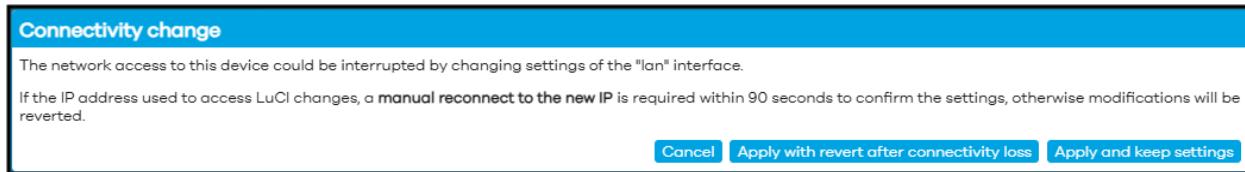


Figure 37: Connectivity change popup message

- 6a. **Cancel** – will not proceed with committing the change but will keep unapplied changes pending and take the user back to step 5.
- 6b. **Apply with revert after connectivity loss** – will begin to commit the change but the user will have 90 seconds to regain access to the device using the new IP address. Otherwise, the setting will automatically revert to the previous setting. Another popup window (**Configuration changes have been rolled back!**) will ask the user to select **Dismiss**, **Revert changes**, or **Apply unchecked**.
 - **Dismiss** – will dismiss this popup window and take the user back to step 5.
 - **Revert changes** – will revert changes and take the user back to step 2.
 - **Apply unchecked** – will commit the change. Skip to step 7.

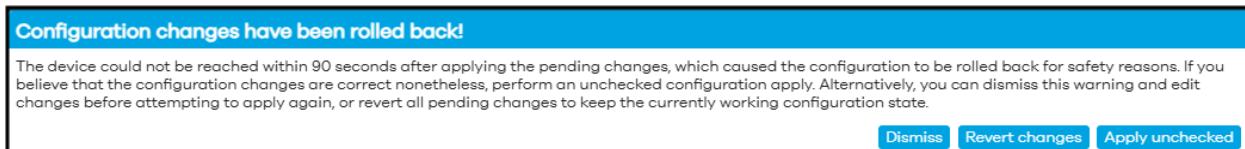


Figure 38: Configuration changes have rolled back! popup message

- 6c. **Apply and keep settings** – will commit the change.
7. Give the device a few minutes to successfully regain network connectivity before attempting to reconnect to MegaFi 2 via Mission Control.

⌚ **Note:** After proceeding with the LAN IP change, the user will need to retype the new IP address in the web browser address bar to regain access to the device.

3.3 Flash/Update Firmware

The user can either use Mission Control or MegaPortal (Nextivity's Cloud portal for MegaFi 2), to update MegaFi 2's firmware.

Notes:

- ⌚ Firmware updates for MegaFi 2 are primarily only supported via MegaPortal. 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 carry out the update. To update the device using MegaPortal, please refer to the *MegaPortal User Manual*.
- ⌚ For special needs or requirements, and only with the assistance of Nextivity Support, a user may update the firmware via Mission Control. To manually update the firmware for MegaFi 2 via Mission Control, the firmware version-specific **BIN** file needs to be obtained from Nextivity Support.

If the user cannot update from the Portal or requires an immediate update, do the following to update the device in Mission Control.

- ✓ **Assumption:** The user has obtained the appropriate firmware (**BIN** file) from Nextivity Support, it is loaded on a computer workstation or laptop, and it is directly connected to a LAN port on MegaFi 2 or via its Wi-Fi connection.
- ⌚ **Note:** Uploading an incorrect file can render your device inoperable and may void warranty.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Upload Firmware** or **Flash image...** button next to **Update Firmware**.

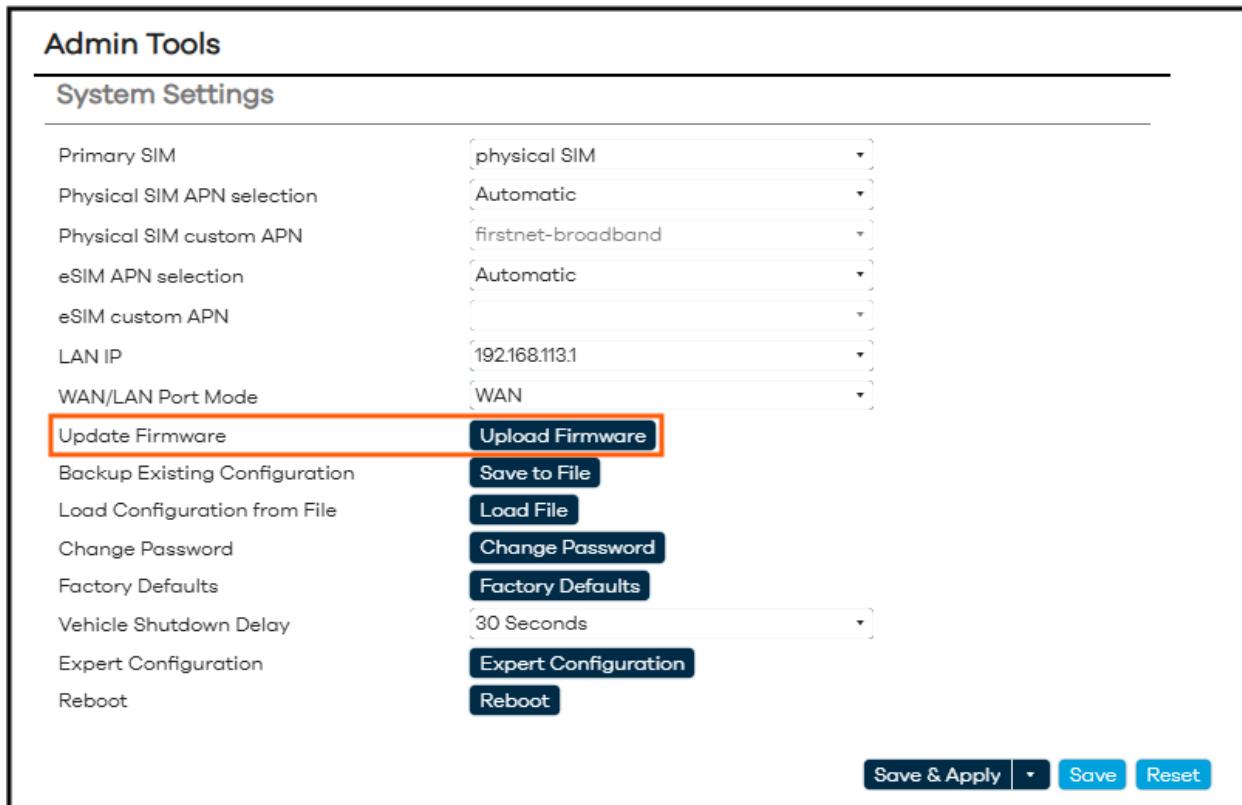


Figure 39: Firmware update – Upload Firmware button

3. On the pop-up **Uploading file...** window, click on **Browse** to locate the firmware file.



Figure 40: Uploading file... - Browse button

4. The firmware file should be a **BIN** type file, and, depending on the firmware version, around 47 MB or more.



Figure 41: Firmware update – Select the upgrade file

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



Figure 42: Firmware update – Uploading the selected upgrade file

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



Figure 43: 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 inside the checksum file. 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 3.4.1.

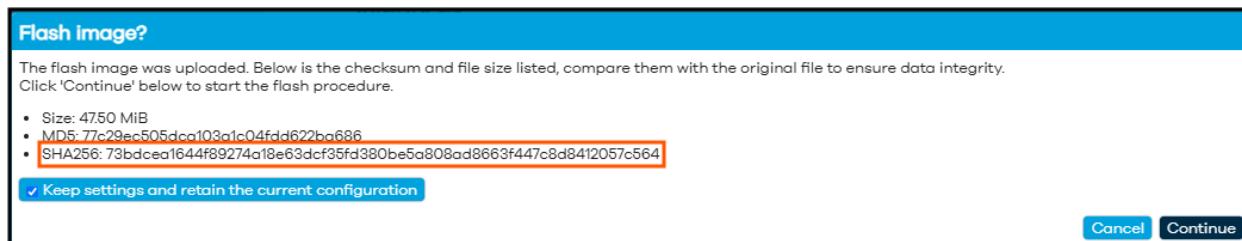


Figure 44: Flash image window – Compare checksum and file size with original

⌚ **Note:** By default, the **Keep settings and retain the current configuration** box is checked. If you uncheck this box, the current configuration will be erased after the update.

❗ **WARNING:** If you accidentally try to upload the wrong file format to the MegaFi 2 device, a warning screen will be displayed (see example below) with the error message in orange: **"The uploaded image file does not contain a supported format. Make sure that you choose the generic image format for your platform"**. If this happens, **STOP - DO NOT PROCEED**. Select **Cancel** to back out of this operation and avoid "bricking" your device.

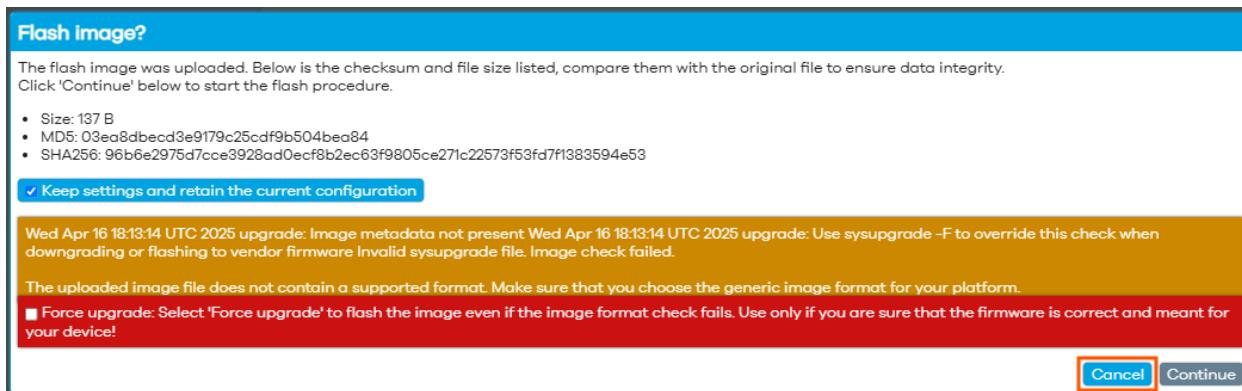


Figure 45: Flash image window – Image format check failure

⌚ **Note:** Updating from version 3.3.0 to version 3.4.1, there is a slightly different warning. In this case the size of the file is in question and the error message in yellow reads: "**It appears that you are trying to flash an image that does not fit into the flash memory, please verify the image file!**". This is a known issue, and if the checksum value matches proceed by checking the box: "**Force upgrade: Select 'Force upgrade' to flash the image even if the image format check fails. Use only if you are sure that the firmware is correct and meant for your device!**". Then proceed to the next step.

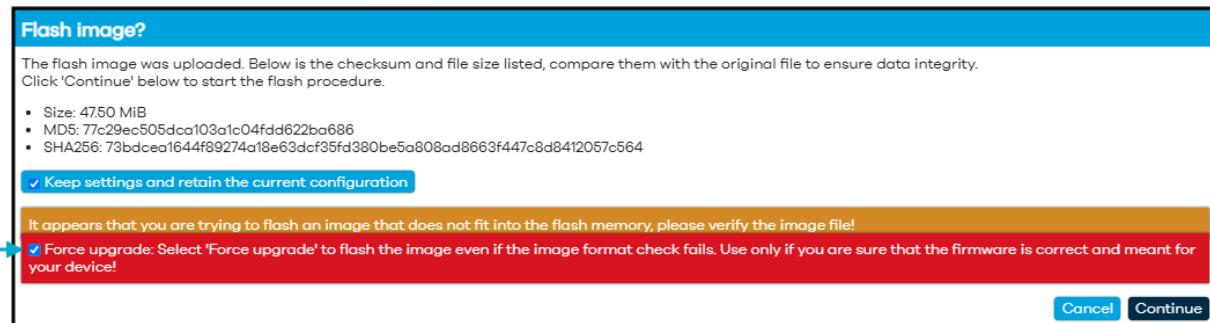


Figure 46: Flash image window – Image size

- Click on **Continue** on **Flash image?** only after the SHA256 values have been verified to match.
- The **Flashing...** window will display.

! WARNING: "Do not power off the unit until the image flashing is complete."

⌚ **Note:** The update will take 3-5 minutes.

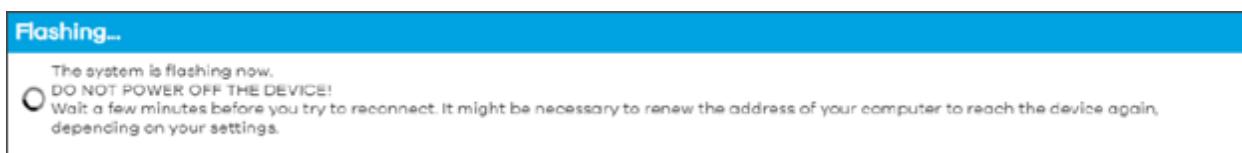


Figure 47: Flashing window – message indicating progress of the system flashing process

10. When the image flash is complete, you will be taken back to the login page.

11. Log in to continue.

Notes:

- ⌚ Current status may initially display **No Internet** and no signal strength bars. It will correct itself once the device properly boots up from the upgrade process.
- ⌚ Refresh the browser if the device has not gone back to the home screen after 10 minutes and re-login again.

12. Verify that the intended firmware upgrade successfully loaded by looking at the bottom right of any Mission Control page. Once verified, the firmware update is complete.



Figure 48: Mission Control page showing Firmware Version

3.4 Backup Existing Configuration

If the user wants to backup an existing configuration, do the following in Mission Control:

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Save to File** button next to **Backup Existing Configuration**.

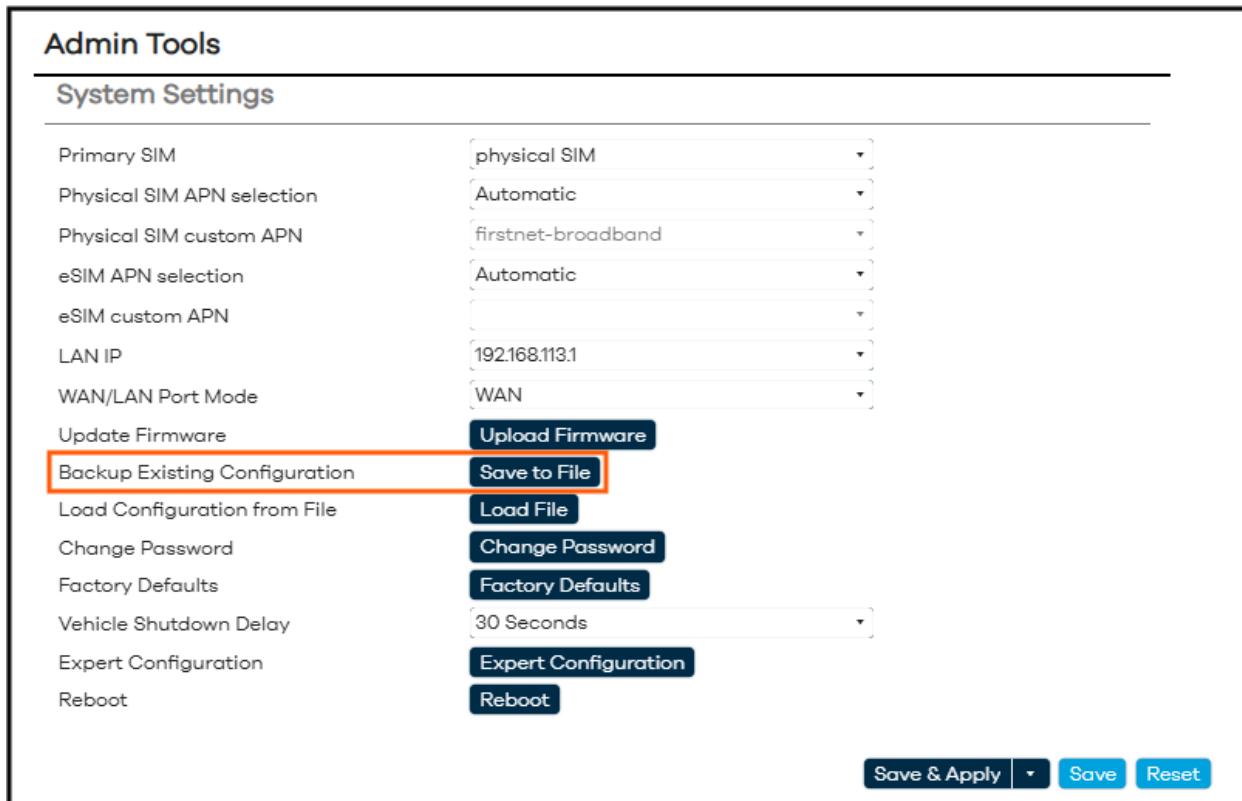


Figure 49: System Settings – Save to File button

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 50: Downloads folder showing downloaded tar.gz file

- ⌚ **Note:** The backup configuration file will **not** include the configured device password.

3.5 Load Configuration from File

If the user wants to load a backup/saved configuration (i.e., duplicate a configuration file onto other MegaFi 2 devices or restore a previous configuration file), do the following in Mission Control:

- ⌚ **Note:** The backup configuration file will **not** bring over the previous device password. All other Wi-Fi settings, and configuration settings from that MegaFi 2 device will be included.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Load File** button, sometimes referred to as **Upload archive...** next to **Load Configuration from File**.

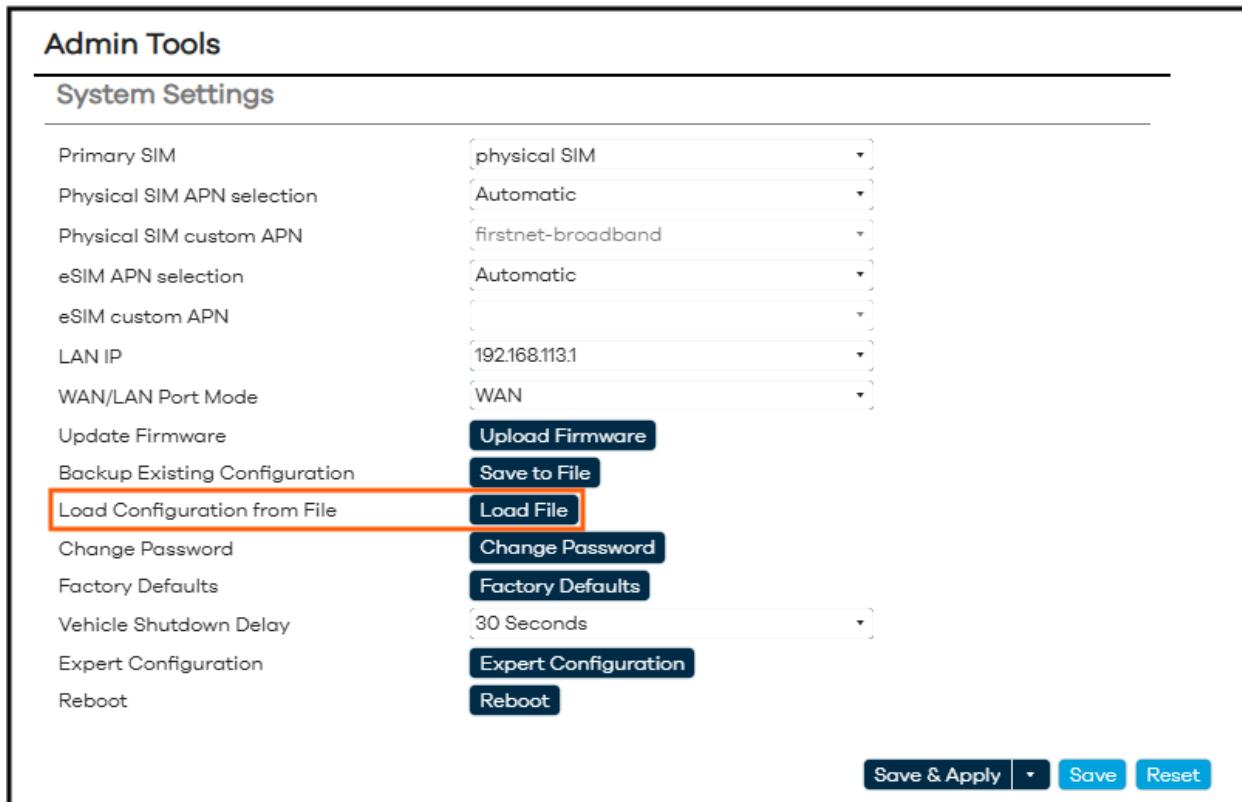


Figure 51: System Settings – Load File button

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



Figure 52: Uploading file – Browse to locate file button

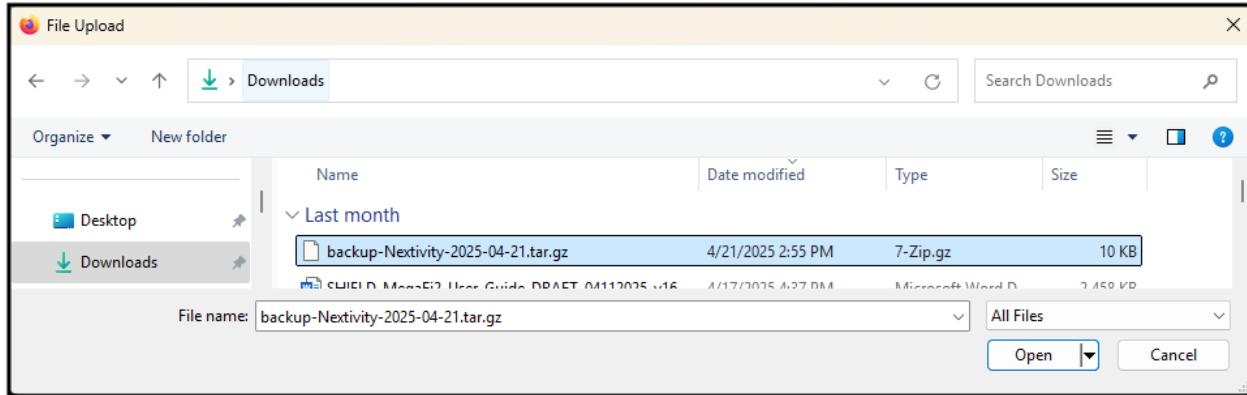


Figure 53: Uploading file and Browse to and select the tarball file

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



Figure 54: Load Configuration from File – Uploading selected file

5. 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.

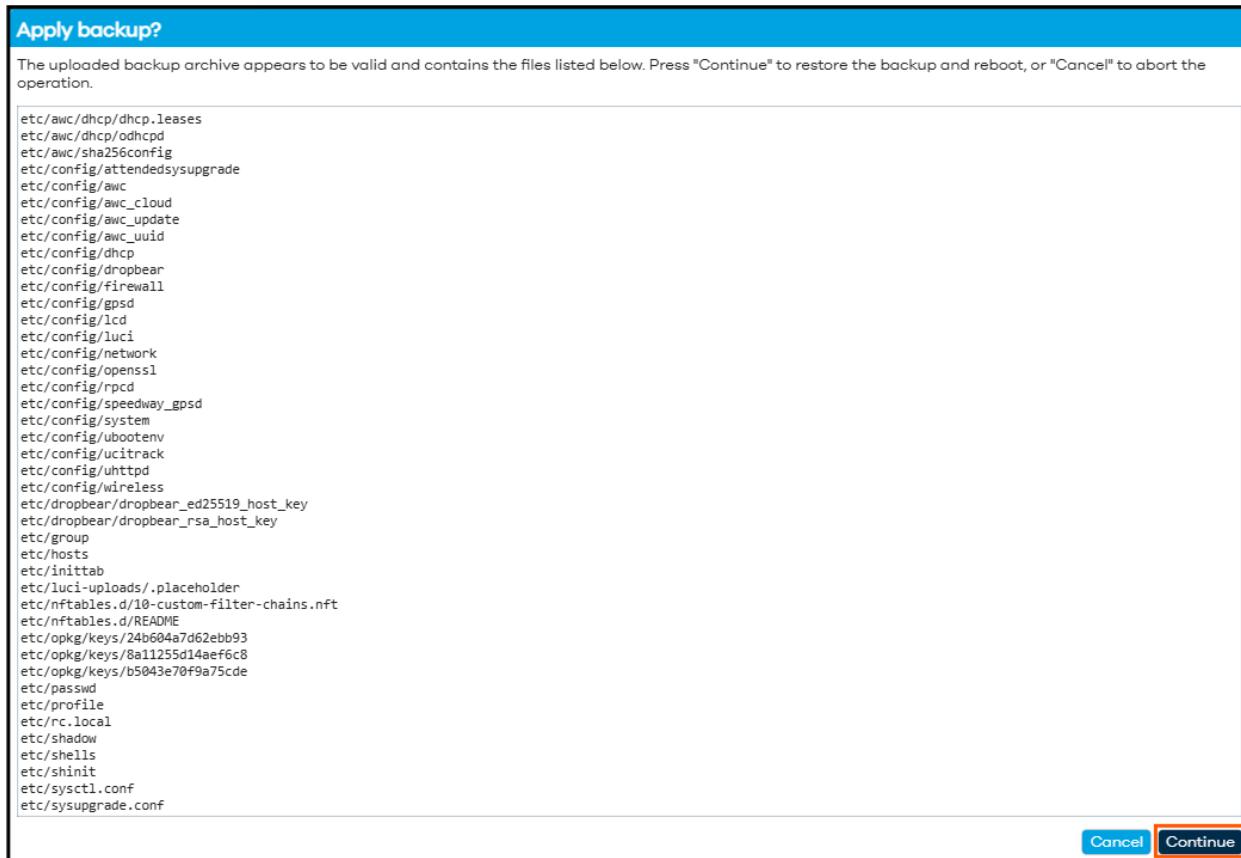


Figure 55: Apply backup – Confirmation to continue

6. Give the backup operation 3-5 minutes to finish as it reboots.

! 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 in Mission Control.

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

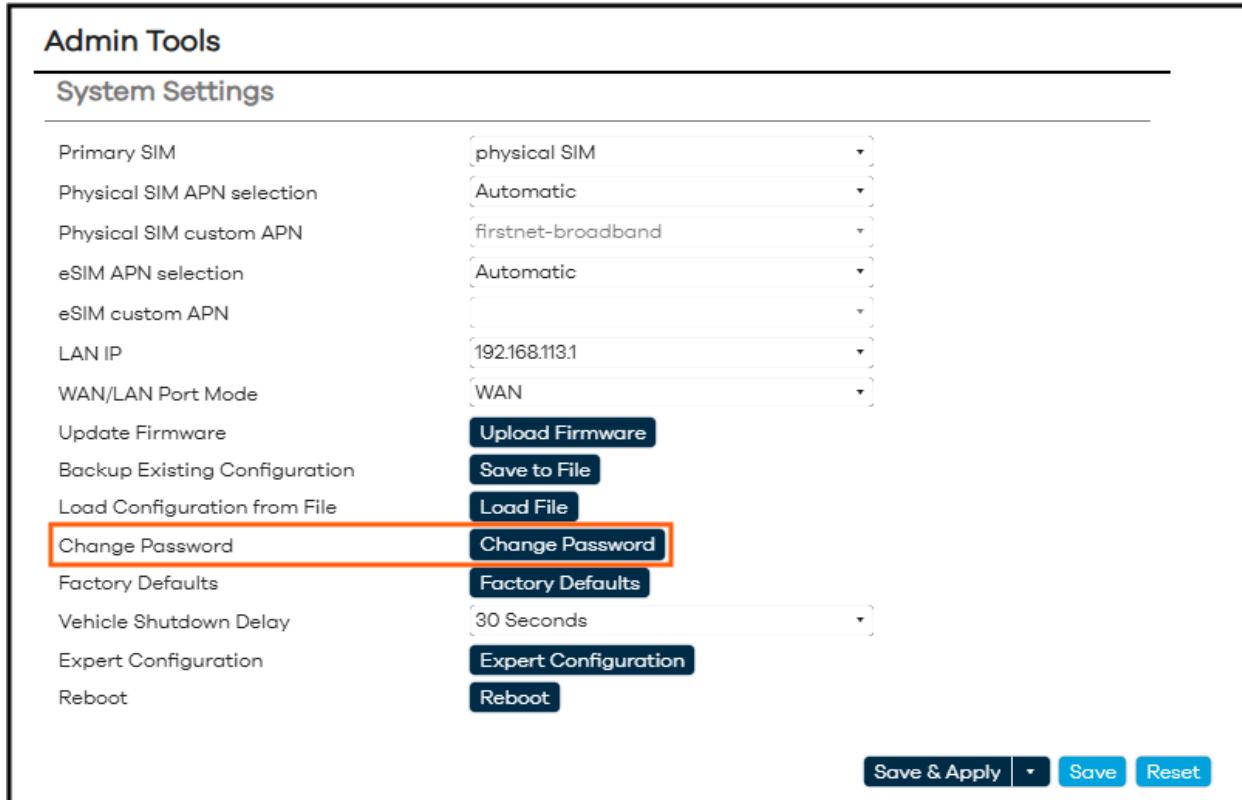


Figure 56: System Settings – Change Password button

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

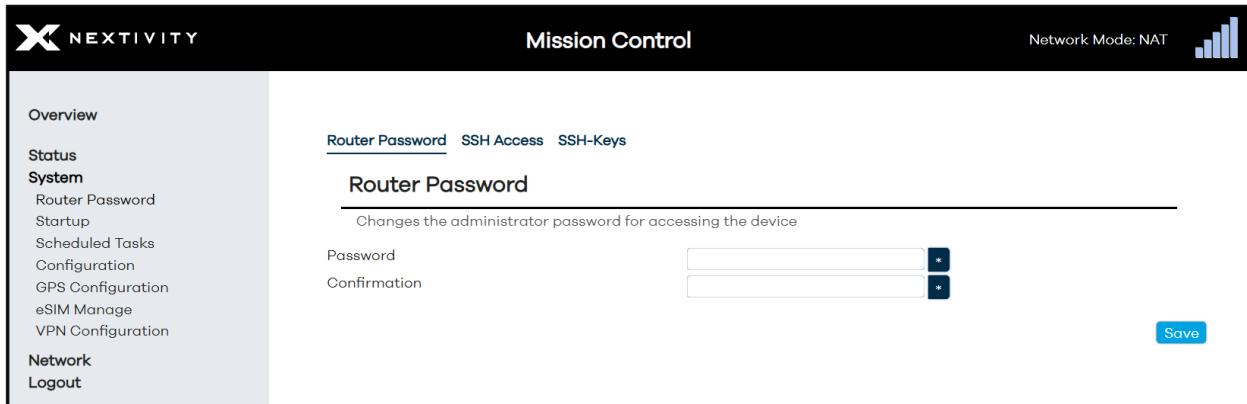


Figure 57: Router Password page – Expert Configuration Mode

4. Enter a new password in the **Password** field and re-type it in the **Confirmation** field as well.
- ⇒ **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.

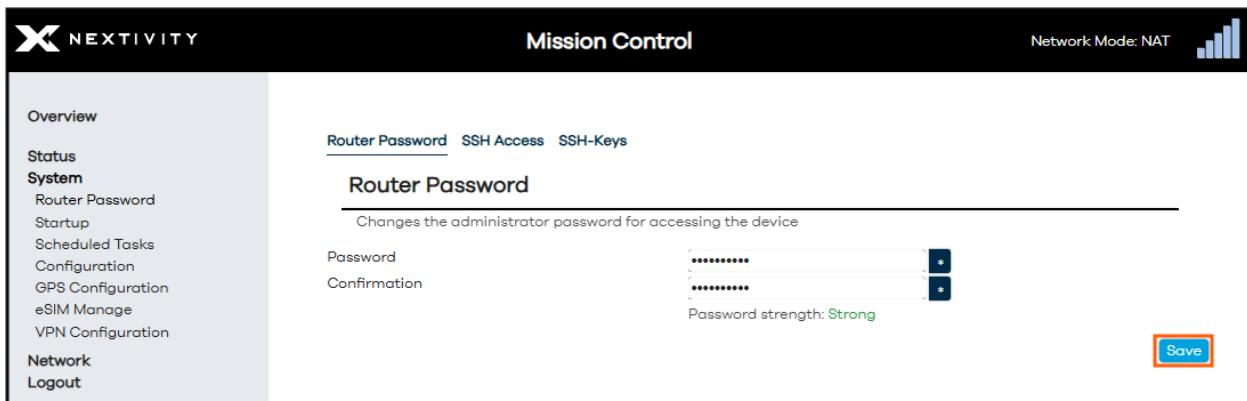


Figure 58: Router Password page – Enter new password

5. Click on the **Save** button.
6. Once the change is confirmed by the device, the user will be put back in the Overview page.

3.7 Factory Defaults via Mission Control

If the user wants to return to factory default settings, the user can perform a factory reset to the MegaFi 2 device in Mission Control as follows:

- ⌚ **Note:** Before proceeding with a factory reset, it is recommended to save a backup configuration of the device in case you need to revert to its previous settings. Follow the steps hi-lighted above in section 3.4 Backup Existing Configuration.
- ⌚ **Note:** After a factory reset, MegaFi 2's UUID may need to be reassigned for Cloud support. If cloud access breaks after a factory reset, contact the support team at support@nextivityinc.com for further assistance.

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

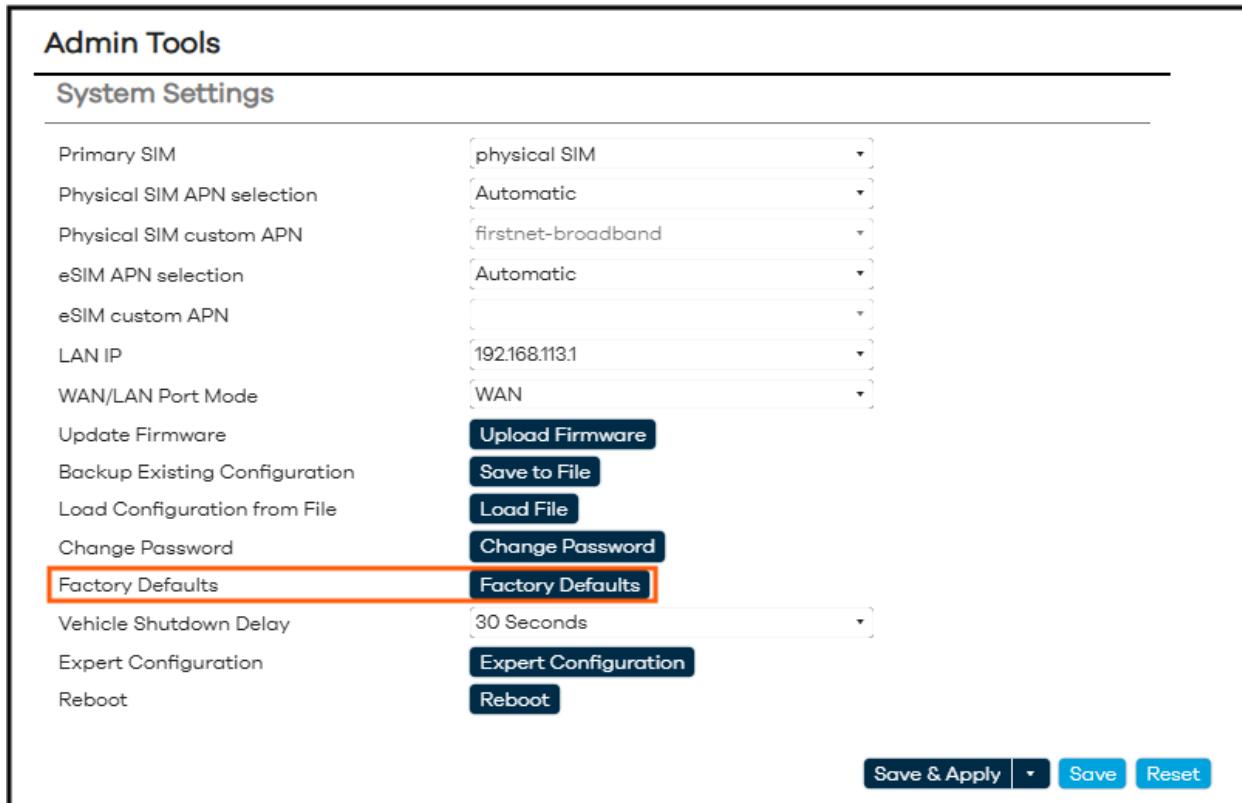


Figure 59: System Settings – Factory Defaults button

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

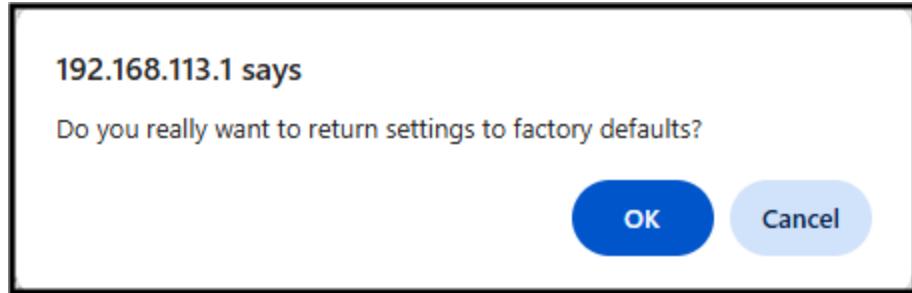


Figure 60: Confirmation to return settings back to factory defaults

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

i To factory default the MegaFi 2 using the **DISPLAY** button (in case of a forgotten password), press and hold the **DISPLAY** button for 20 seconds and release. The device will take a few minutes to recover, and all settings will now be set to factory default.

3.8 Vehicle Shutdown Delay

If the MegaFi 2 device is installed in a vehicle, the user can increase the **Vehicle Shutdown Delay** setting up to 2 hours. The default setting is 30 seconds. This ensures that the MegaFi 2 device will stay powered on after the vehicle is shut off and it will continue to provide services until the timer expires. To change this setting, do the following in Mission Control:

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

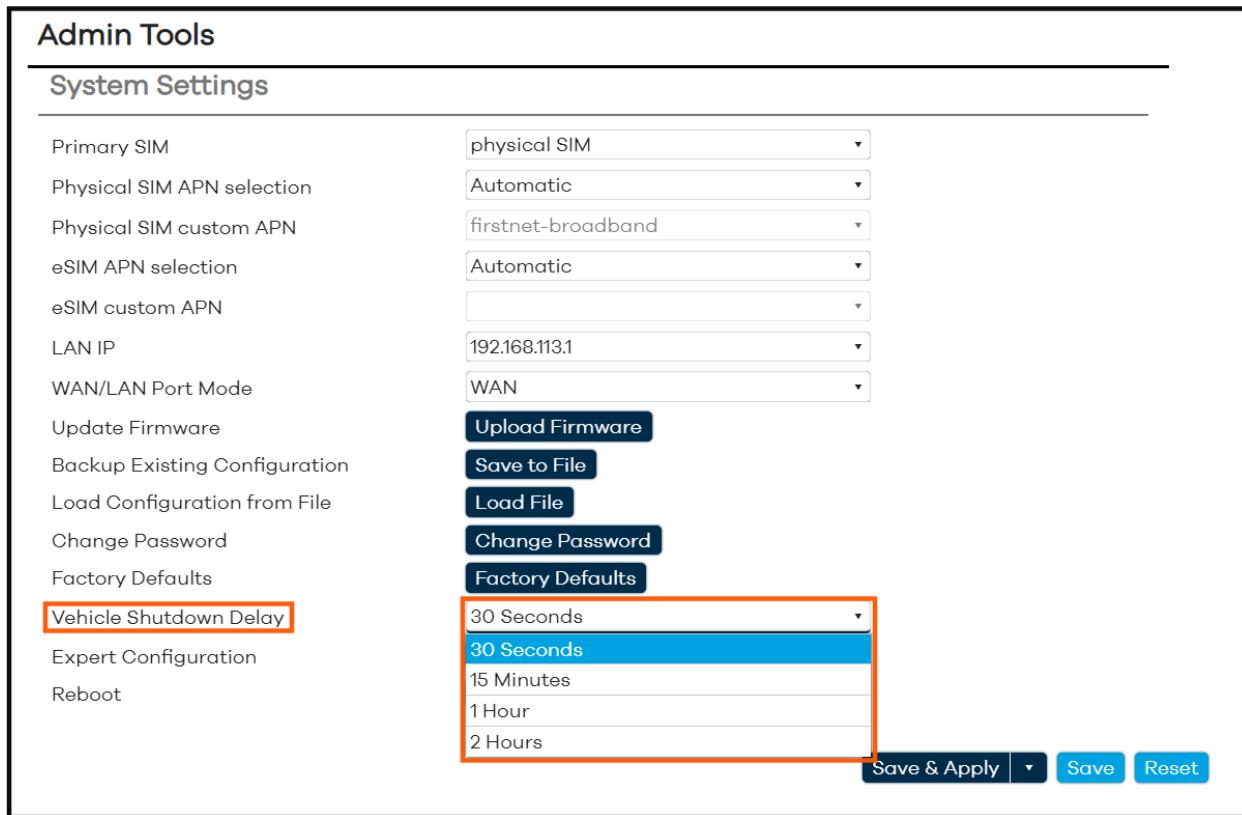


Figure 61: System Settings – Vehicle Shutdown Delay options

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

3.9 Reboot

If the user would like to reboot the MegaFi 2, do the following in Mission Control.

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

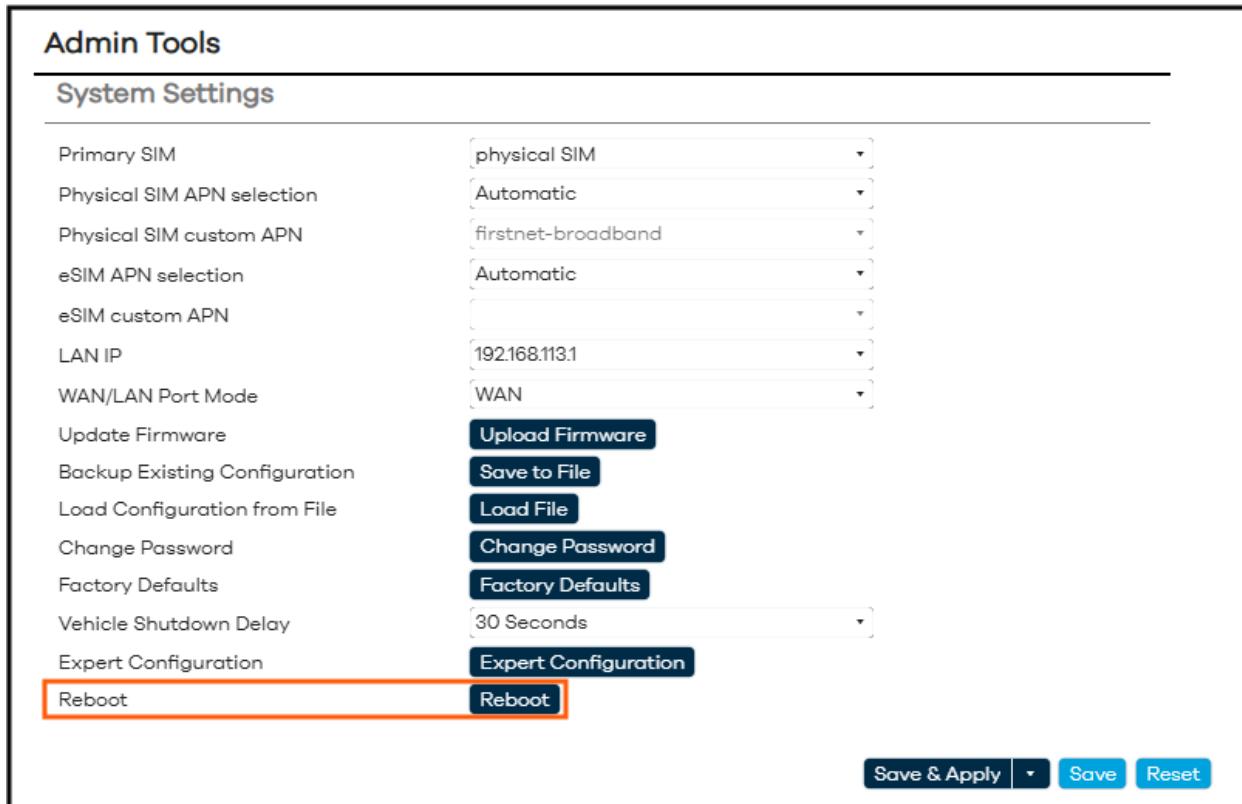


Figure 62: System Settings – Reboot button

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

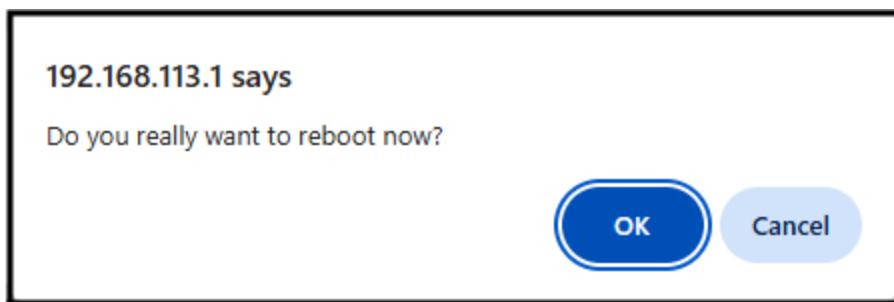


Figure 63: Confirmation message to reboot device

4. Wait for the device to reboot before continuing. The process will take 1 - 3 minutes.



Figure 64: Message indicating device is being rebooted

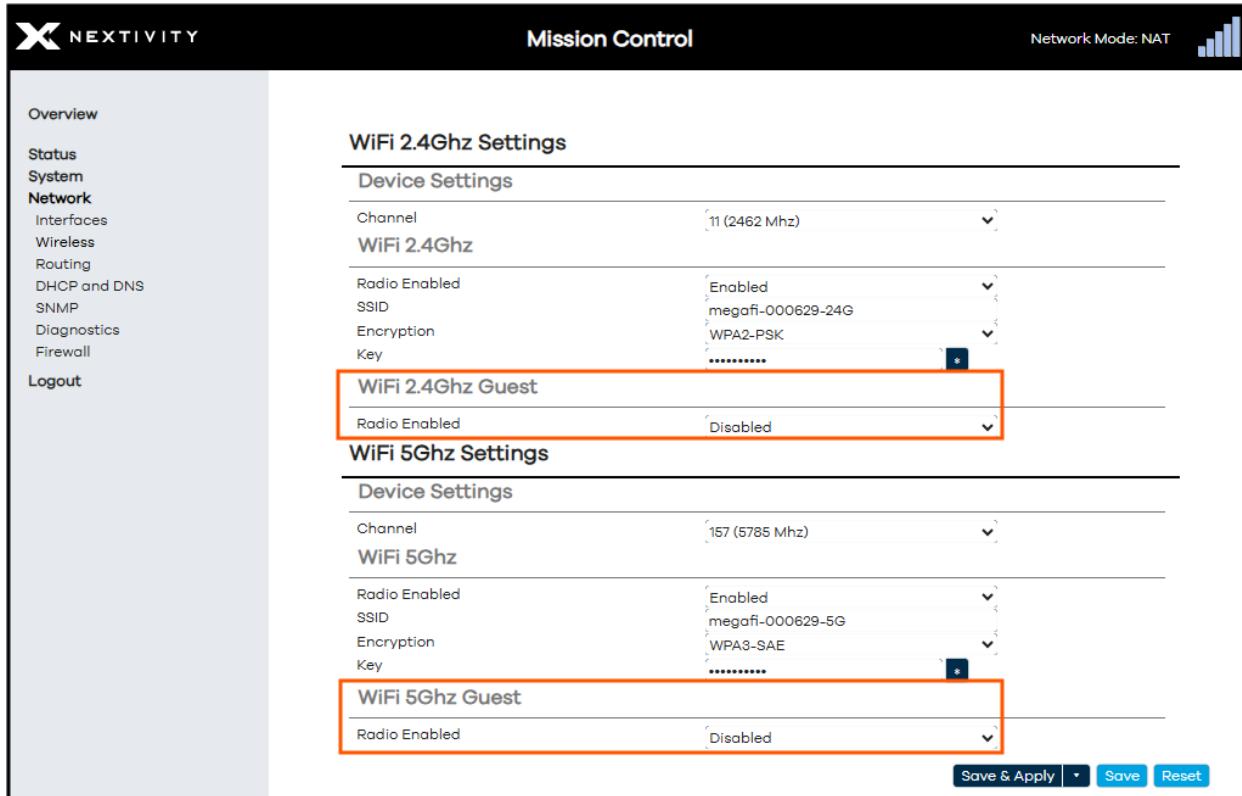
5. The user will be asked to log in again into Mission Control after the device reboots. Click on the **To login...** button to do so.



Figure 65: Prompt to log in after device reboots

3.10 Wireless Settings

Beginning with firmware version 3.4.1, two Guest Wi-Fi's or SSIDs have been introduced into Mission Control. There is one for 2.4 GHz and another for 5 GHz, for a total of 4 SSIDs that include the two primary SSIDs. Both Guest SSIDs are disabled by default while the two primary SSIDs are enabled by default.



The screenshot shows the 'Mission Control' interface with the 'Network Mode: NAT' status. The left sidebar includes links for Overview, Status, System, Network (selected), Interfaces, Wireless, Routing, DHCP and DNS, SNMP, Diagnostics, and Firewall, along with a Logout option. The main content area is titled 'WiFi 2.4Ghz Settings' and 'WiFi 5Ghz Settings'. Each section has a 'Device Settings' header and a list of parameters: Channel, Radio Enabled, SSID, Encryption, and Key. The 'WiFi 2.4Ghz Guest' and 'WiFi 5Ghz Guest' sections are highlighted with orange boxes. In the 'WiFi 2.4Ghz Guest' section, the 'Radio Enabled' dropdown is set to 'Disabled'. In the 'WiFi 5Ghz Guest' section, the 'Radio Enabled' dropdown is also set to 'Disabled'. At the bottom right are buttons for 'Save & Apply', 'Save', and 'Reset'.

Figure 66: System Settings – Expert Configuration button

To verify overall Wi-Fi settings, refer to section 3.10.1 below. To modify the primary SSIDs, refer to section 3.10.2. To enable and modify the Guest SSIDs, refer to section 3.10.3.

3.10.1 Verify Wi-Fi Settings

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

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.

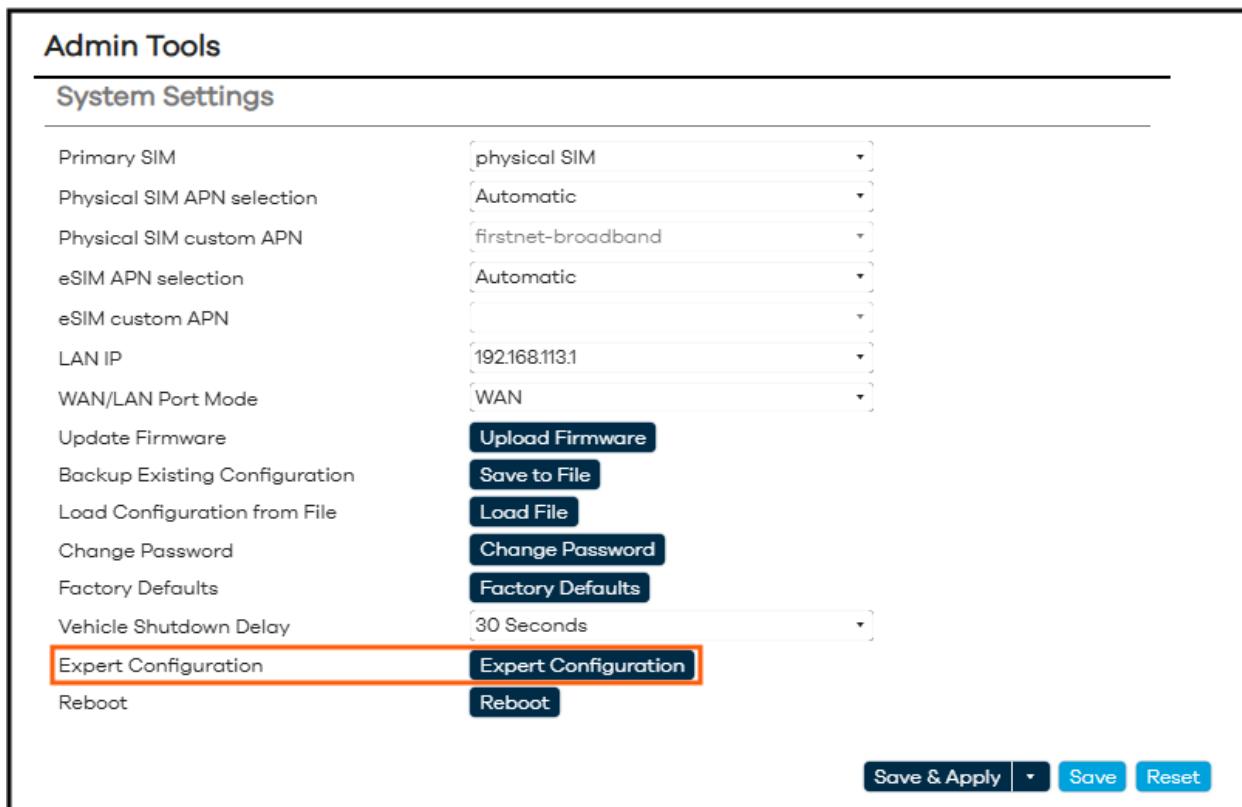


Figure 67: System Settings – Expert Configuration button

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

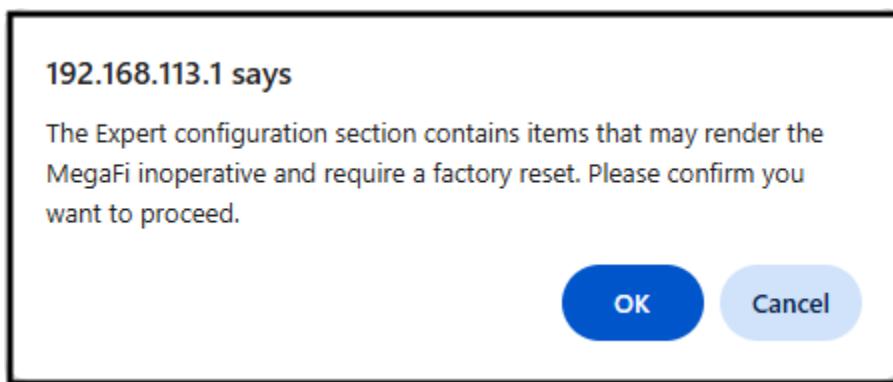


Figure 68: Confirmation message to enter Expert Configuration mode

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

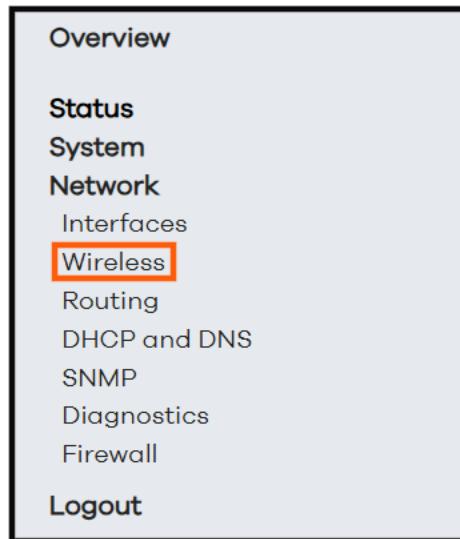


Figure 69: Navigation pane showing options available in Expert mode – Wireless

☞ **Note:** To view the primary SSID hidden Keys/Passwords, click on the * (asterisk) button next to the **Key** field to make it visible for either SSID. By default, the key/password is the same for both 2.4 GHz and 5 GHz settings and printed on the label or on the LCD display screen.

The image shows the 'Mission Control' interface with the 'Network Mode: NAT' status. The left sidebar includes:

- Overview
- Status
- System
- Network**
- Interfaces
- Wireless
- Routing
- DHCP and DNS
- SNMP
- Diagnostics
- Firewall
- Logout

The main content area is titled 'Mission Control' and shows 'WiFi 2.4Ghz Settings' and 'WiFi 5Ghz Settings' sections. Under 'WiFi 2.4Ghz Settings', the 'Device Settings' section shows:

- Channel: 11 (2462 Mhz)
- Radio Enabled: Enabled
- SSID: megafi-000629
- Encryption: WPA2-PSK
- Key: OCZpc34124 *

Under 'WiFi 5Ghz Settings', the 'Device Settings' section shows:

- Channel: 157 (5785 Mhz)
- Radio Enabled: Enabled
- SSID: megafi-000629
- Encryption: WPA3-SAE
- Key: OCZpc34124 *

At the bottom right are buttons: 'Save & Apply' (gray), 'Save' (blue), and 'Reset' (gray).

Figure 70: Wireless Settings – View hidden Keys

3.10.2 Change Wi-Fi Settings

The following options available for the primary 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	11 (2462 Mhz)	Auto and Channels 1-11	157 (5785 Mhz)	Auto and Channels 36, 40, 44, 48, 149, 153, 157, 161
SSID	default SSID name on label or LCD Display screen		default SSID name on label or LCD Display screen	
Encryption	WPA2-PSK	WPA2-EAP, WPA3-EAP, WPA2-EAP/WPA3-EAP, WPA2-PSK/WPA3-SAE, WPA3-SAE, and Disabled	WPA3-SAE	WPA2-EAP, WPA3-EAP, WPA2-EAP/WPA3-EAP, WPA2-PSK/WPA3-SAE, WPA2-PSK, and Disabled
Key	default key (password) on label or LCD Display screen		default key (password) on label or LCD Display screen	

Table 3: Wi-Fi Settings for 2.4 GHz and 5 GHz

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

- ➲ **Note:** If you attempt to make wireless changes while connected to the device via Wi-Fi, expect to be disconnected after committing the changes. You will then have to reconnect to Wi-Fi using the new settings.

1. For settings with a drop-down menu arrow, such as **Radio Enabled**, click the arrow and choose the preferred setting from the options.

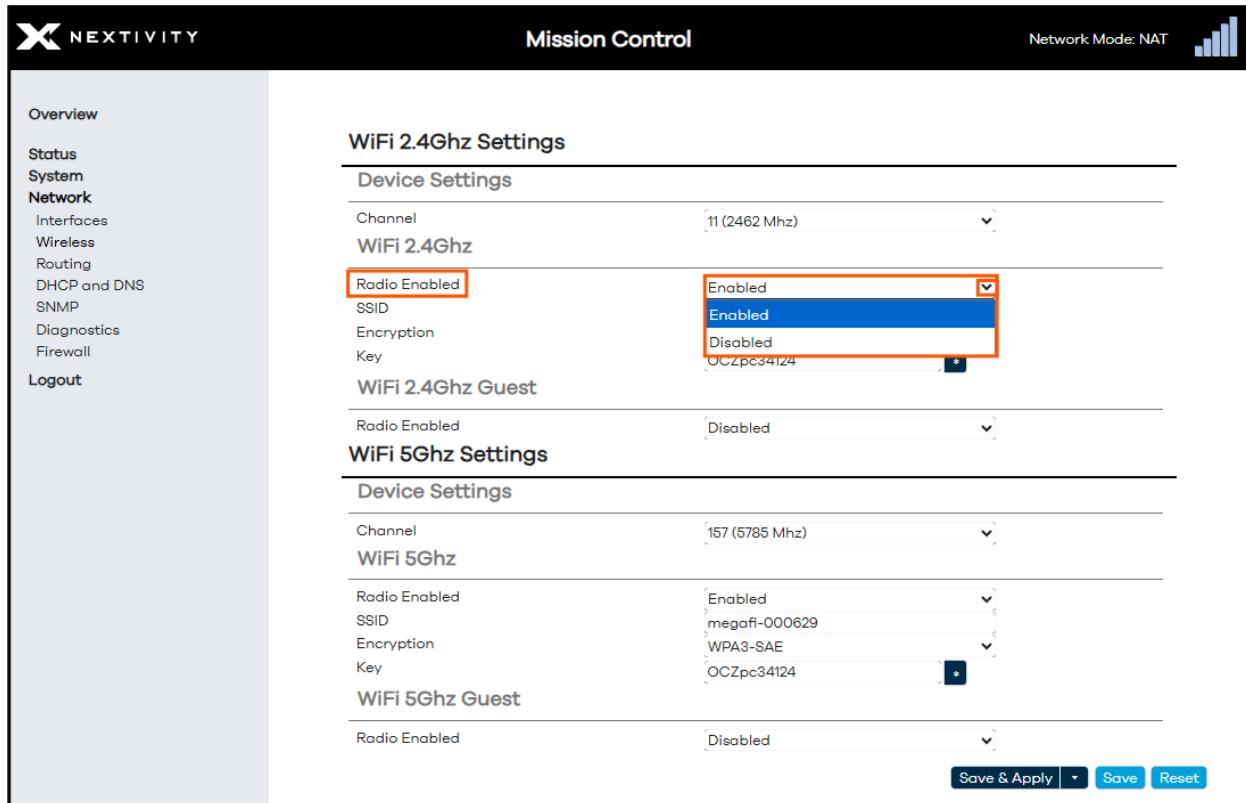


Figure 71: Wireless Settings – Selecting Drop-down Menu options

2. For **SSID** and **Key** modifications, remove/delete or change 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.

Figure 72: Wireless Settings – Modifying SSID and Key fields

3. Click on **Save** followed by **Save & Apply** to confirm the change(s).
- ⌚ **Note:** If the user selects either **WPA2-EAP** or **WPA3-EAP** encryption for **Wi-Fi 2.4 or 5 GHz** settings, the **Key** option goes away, and the user is presented with the following new options. Configure these settings as required for your Extensible Authentication Protocol (EAP) network environment.

- **RADIUS Server IP**
- **RADIUS Server Port**
 - Default setting - 1812
- **RADIUS Secret** - To view the hidden RADIUS Secret, click on the * (asterisk) button next to the field to make it visible for either SSID.

The screenshot shows the NEXTIVITY Mission Control interface. The left sidebar has a 'Network' section with 'Wireless' selected. The main area is titled 'Mission Control' and shows 'Basic Configuration Settings > Wireless Settings'. The 'WiFi 2.4Ghz Settings' section contains a 'Device Settings' table with rows for Channel (11), Radio Enabled (Enabled), SSID (megaf1-000629-24G), Encryption (WPA2-EAP), RADIUS Server IP, RADIUS Server Port (1812), and RADIUS Secret. The 'WiFi 5Ghz Settings' section contains a similar table with Channel (157), Radio Enabled (Enabled), SSID (megaf1-000629-5G), Encryption (WPA3-EAP), RADIUS Server IP, RADIUS Server Port (1812), and RADIUS Secret. The 'WiFi 2.4Ghz Guest' and 'WiFi 5Ghz Guest' sections show Radio Enabled as Disabled. At the bottom are 'Save & Apply', 'Save', and 'Reset' buttons. A red box highlights the 'Encryption', 'RADIUS Server IP', 'RADIUS Server Port', and 'RADIUS Secret' fields in both the WiFi 2.4Ghz and WiFi 5Ghz sections.

Figure 73: Wireless Settings – EAP fields

⇒ **Note:** Devices that connect to either primary SSID will be assigned to IP addresses within the default LAN subnet of 192.168.113.x/24 or whatever was subsequently configured as described in section 3.2 above.

3.10.3 Guest Wi-Fi Settings

The Guest Wi-Fi/SSIDs are disabled by default. The following options available for Guest Wi-Fi 2.4 GHz and 5 GHz settings are:

Guest Wi-Fi Setting	Guest WiFi 2.4 GHz Settings (Default)	Guest WiFi 2.4 GHz Settings -Other Options	Guest WiFi 5 GHz Settings (Default)	Guest WiFi 5 GHz Settings -Other Options
Radio Enabled	Disabled	Enabled	Disabled	Enabled
SSID	default SSID name is “ guest ”		default SSID name is “ guest5G ”	
Encryption	Disabled	WPA2-PSK, WPA2-EAP, WPA3-EAP, WPA2-EAP/WPA3-EAP, WPA2-PSK/WPA3-SAE, WPA3-SAE	Disabled	WPA2-PSK, WPA2-EAP, WPA3-EAP, WPA2-EAP/WPA3-EAP, WPA2-PSK/WPA3-SAE, WPA2-SAE
Key	none		none	

Table 4: Guest Wi-Fi Settings for 2.4 GHz and 5 GHz

To change current Guest Wi-Fi settings, do the following:

⇒ **Note:** If you attempt to make Guest Wi-Fi changes while connected to the device via Guest Wi-Fi, expect to be disconnected after committing the changes. You will then have to reconnect to Wi-Fi using the new settings. Any device connected to a Guest Wi-Fi will not have access to MegaFi’s Mission Control.

1. Enable the Guest Wi-Fi radio by selecting the Enabled option from the drop-down menu.

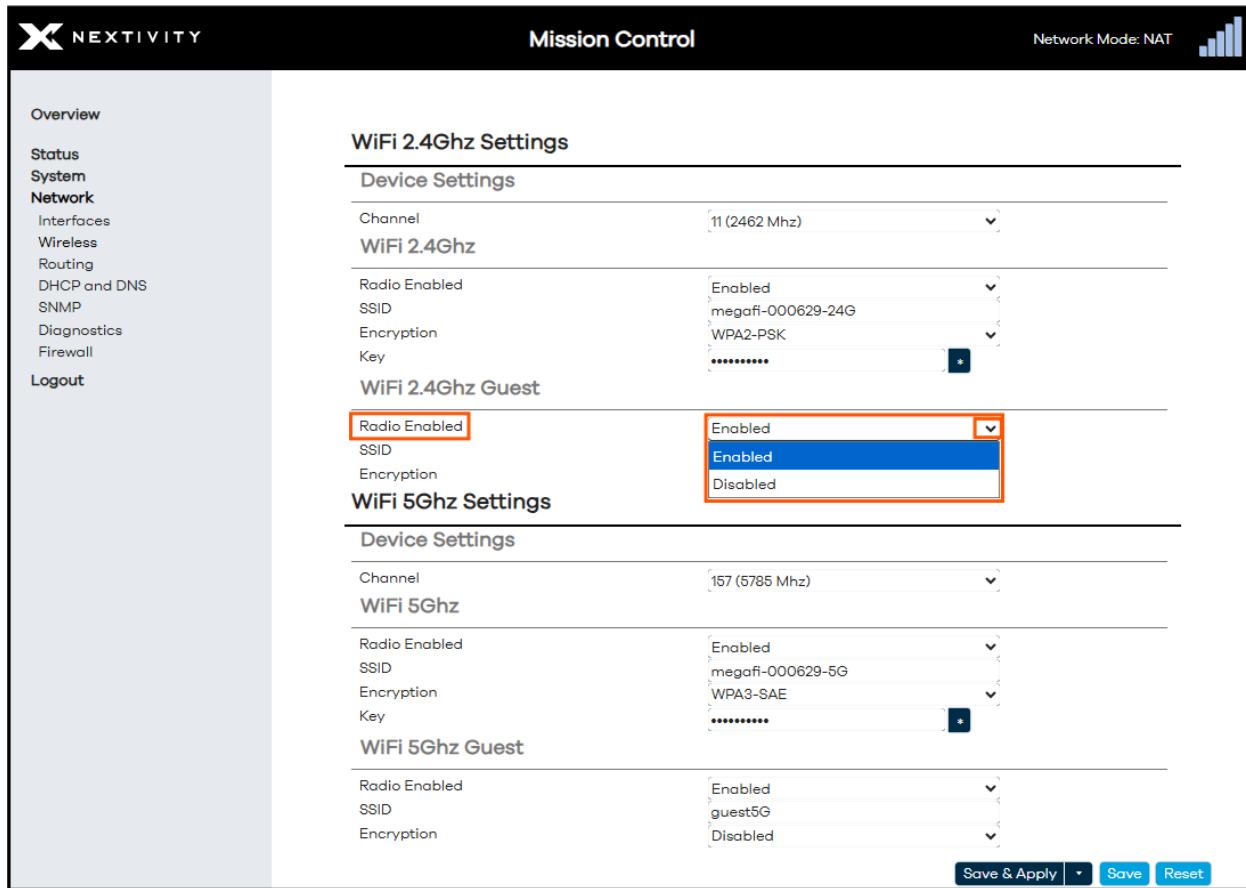


Figure 74: Guest Wireless Settings – Selecting Drop-down Menu options

2. Change the Guest SSID as needed by typing it into the SSID field.
3. Change the Encryption as needed from the default setting of Disabled to any of the available options in the drop-down menu.
4. Enter an appropriate **Key** (Must be at least 10 characters long) into its field. Click on the * (asterisk) button next to the **Key** field to make it visible for either SSID.
5. Click on **Save** followed by **Save & Apply** to confirm the change(s).

⌚ **Note:** If the user selects either **WPA2-EAP** or **WPA3-EAP** encryption for **Wi-Fi 2.4** or **5 GHz** settings, the **Key** option goes away, and the user is presented with the following new options. Configure these settings as required for your Extensible Authentication Protocol (EAP) network environment.

- **RADIUS Server IP**
- **RADIUS Server Port**

- Default setting - 1812
- **RADIUS Secret** - To view the hidden RADIUS Secret, click on the * (asterisk) button next to the field to make it visible for either SSID.

The screenshot shows the 'Mission Control' interface for a Nextivity device. The left sidebar has a 'Network' section with 'Wireless' selected. The main area is titled 'WiFi 2.4Ghz Settings' and 'WiFi 5Ghz Settings'. Each section has a 'Device Settings' tab and a 'Guest' tab. In the 'Guest' tab of the 2.4Ghz section, the 'Encryption' field is set to 'WPA2-EAP', 'RADIUS Server IP' is '1812', and 'RADIUS Secret' is visible as '*****'. In the 'Guest' tab of the 5Ghz section, the 'Encryption' field is set to 'WPA2-EAP/WPA3-EAP', 'RADIUS Server IP' is '1812', and 'RADIUS Secret' is visible as '*****'. Both the 'RADIUS Server IP' and 'RADIUS Secret' fields are highlighted with a red box.

Figure 75: Guest Wireless Settings – EAP fields

➲ **Note:** Devices that connect to either Guest SSID will be assigned to IP addresses within the subnet of 192.168.131.x/24 and are isolated from the main LAN subnet and from each other.

3.11 NAT vs. Passthrough Mode

The MegaFi 2 device can be set to either **NAT** (default setting) or **Passthrough Mode**. In **NAT Mode**, the device acts as an intermediary between a local network and the internet, translating private IP addresses into a single public IP address. This helps enhance security by hiding internal devices from external networks and allows multiple devices to share a single public IP. **Passthrough Mode** disables **NAT**, meaning the device does not modify IP addresses. It simply forwards traffic as-is, allowing a connected device (such as a firewall or router) to handle public IP assignments. **Passthrough** is often used when another device downstream is managing the network. Also, in **Passthrough Mode**, the carrier assigned IP address will be shared with the device directly connected behind the MegaFi 2 on the LAN 1 port. In some cases, computers with specific software will require this IP and can be the recipient of the passed through IP address. In addition, setting the device to **Passthrough Mode** will disable the WAN/LAN2 port as well as Wi-Fi.

Prior to implementing **Passthrough Mode**, the user needs to take the following steps:

- **Connection to MegaFi 2 Device** – the user will need to connect a computer workstation or laptop with an Ethernet cable 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) first 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 may proceed with implementing **Passthrough Mode** as instructed below.
 - **Manually refresh the 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 **LAN IP** address it has been configured to until the IP address is manually refreshed. If this occurs, go to Step 11 below for options to try to regain connection to Mission Control.

To change between **NAT** and **Passthrough** modes, do the following in Mission Control:

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.

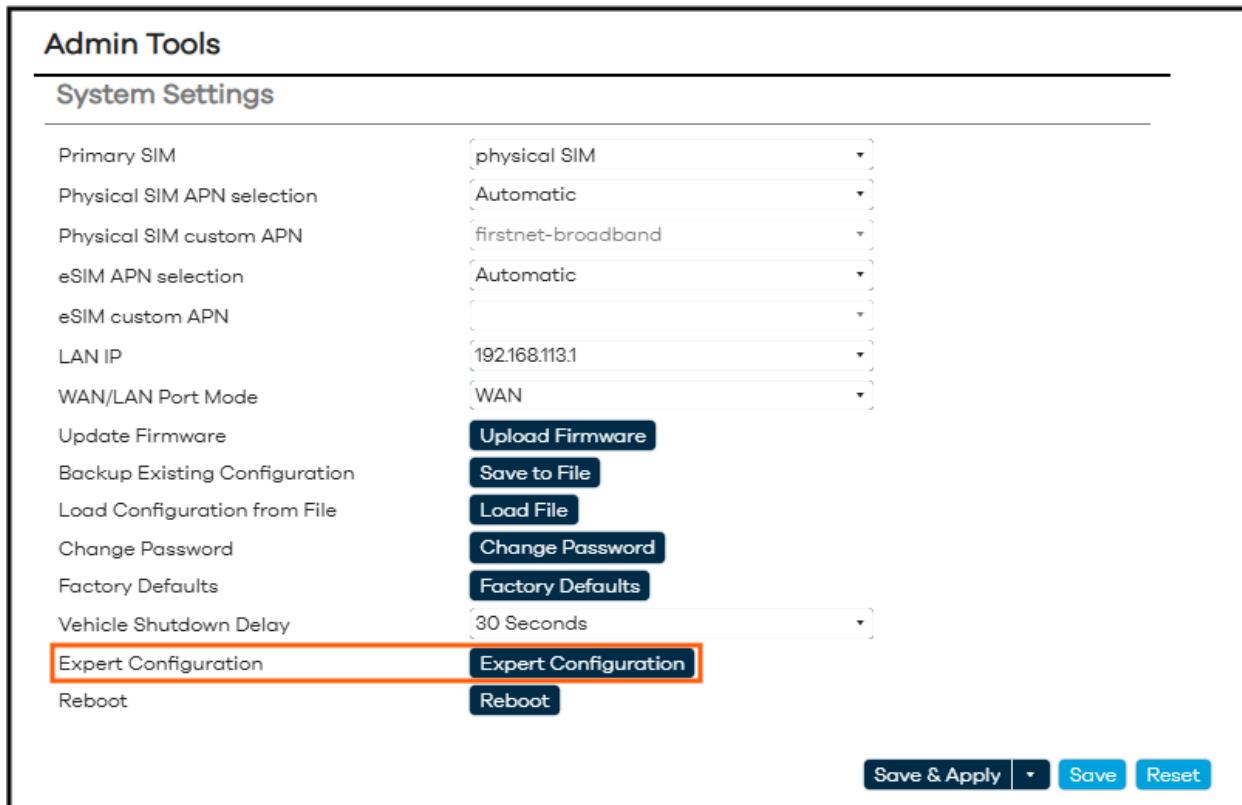


Figure 76: System Settings – Entering Expert Configuration mode

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

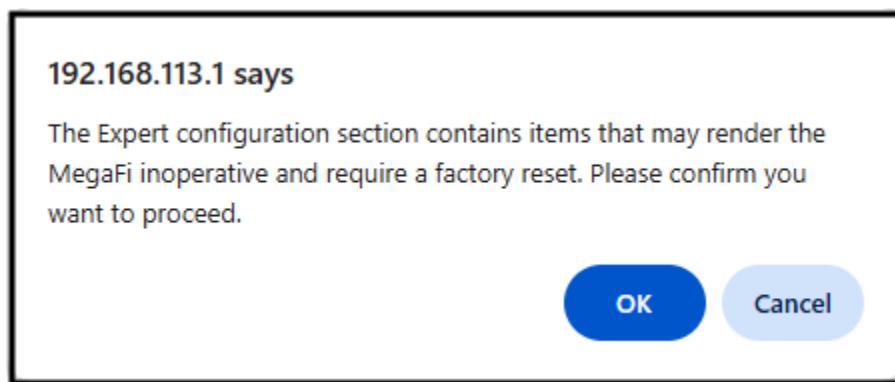


Figure 77: Confirmation message to enter Expert Configuration mode

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

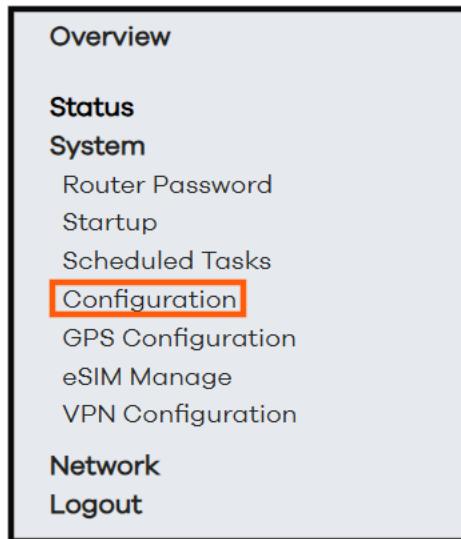


Figure 78: Navigation pane showing options available in Expert mode – Configuration

- Under the **Networking** area, click on the drop-down arrow and select the desired mode: **NAT Mode** (default), or **Passthrough Mode** from the **Passthrough vs NAT (changing causes reboot)** option.

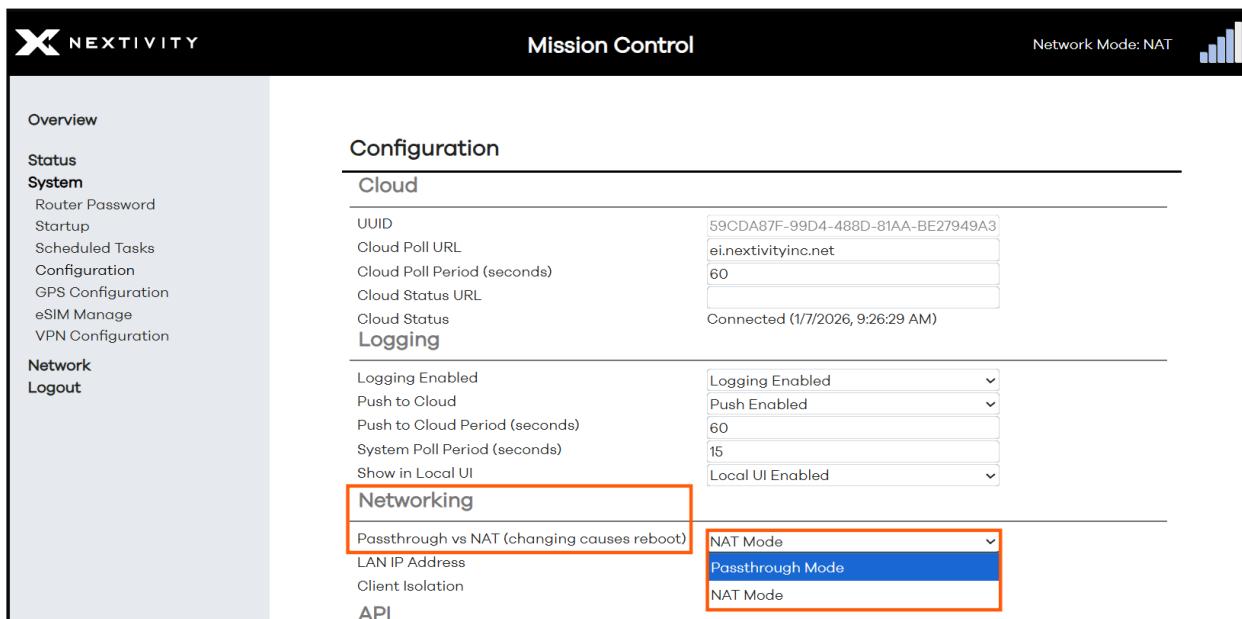


Figure 79: MegaFi 2 Configuration – Change modes (NAT or Passthrough)

- A pop-up window will warn the user that temporary access to Mission Control will be lost after committing to the mode change. After committing to the mode change, the user will have the option to restore the default configuration by holding the **Reset** button for 30 seconds if they don't wish to continue with the mode change. Click **OK** to continue with the mode change.

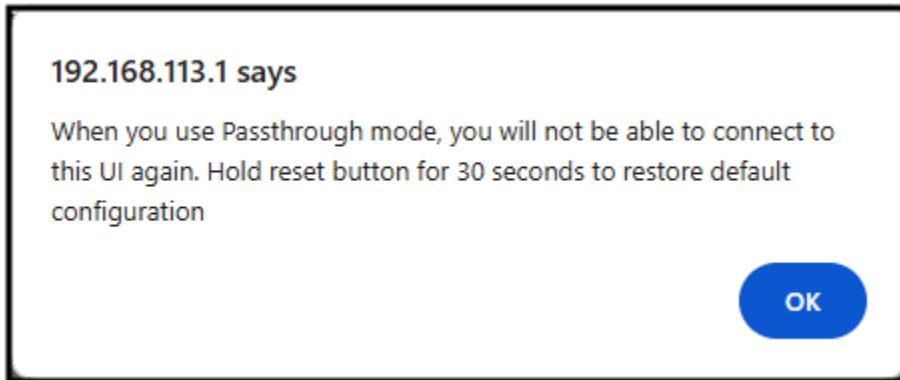


Figure 80: MegaFi 2 Configuration – Change modes (NAT or Passthrough)

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

! WARNING: Internet access, wireless connectivity and/or access to the MegaFi 2 will become disrupted or unavailable after committing the mode change. Please allow 1-3 minutes for the configuration to apply.

7. Once Mission Control access is re-established, login again to Mission Control.
8. It is highly recommended to issue a **Reboot** (Section 3.9) to make sure the new setting takes hold. Please proceed with a **Reboot** at this time.
9. If the MegaFi 2 is set to **Passthrough Mode**, and the desired device, such as a firewall or router or a different computer with special software is to be connected to LAN port 1 on MegaFi 2 other than the computer used to implement the mode change, follow these added steps:
 - 9a. Power down both the MegaFi 2 and the device that will interconnect with each other.
 - 9b. Using an Ethernet patch cable, interconnect the MegaFi 2 LAN port 1 interface and the device's **WAN** port. If the device is another computer, connect to its Ethernet port.
 - 9c. Power up both devices.
 - 9d. Ensure that the connected device receives the appropriate IP address. Follow instructions from the device manufacturer to validate the IP address.
10. If connectivity becomes an issue to Mission Control, try one of the following actions to regain access to MegaFi 2:
 - 10a. Refresh the web browser to Mission Control.
 - 10b. Connect an Ethernet cable to an enabled LAN port (LAN port 1 if in Passthrough mode) on the MegaFi 2 and re-access Mission Control as usual through a web browser.
 - 10c. Manually refresh connected computer IP address by opening a Windows PowerShell, or Command Prompt window on a PC with local access to MegaFi 2 and enter the following commands at the prompt:
 - **ipconfig /release <enter>** - this will release the existing IP addresses

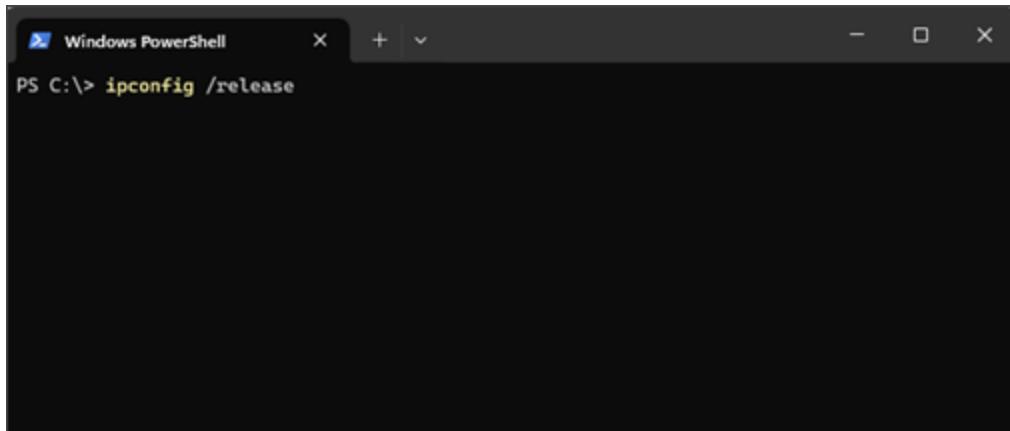


Figure 81: Windows PowerShell window – ipconfig /release <enter>

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

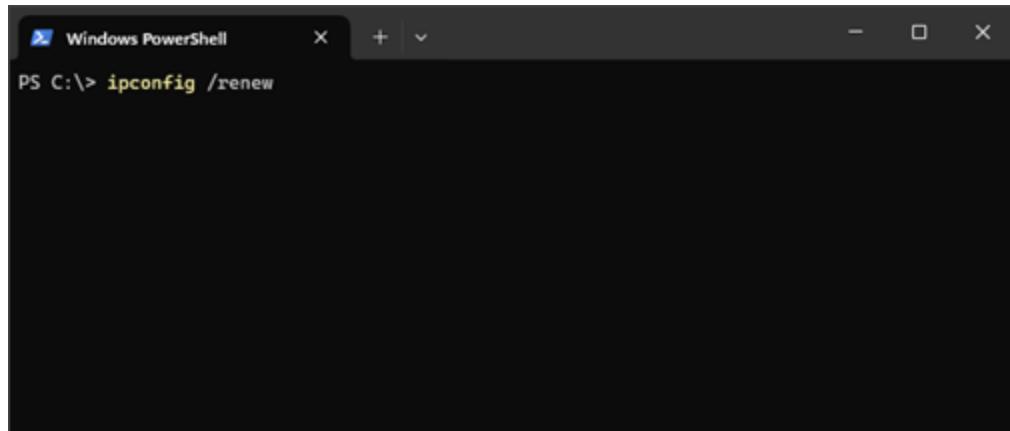


Figure 82: Windows PowerShell window – ipconfig /renew <enter>

11. 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

In certain situations, the user may need to **Band Lock** to band 14 or 28. To do so, do the following in Mission Control:

- ⌚ **Note:** Before committing to this change, please make sure to validate that band 14 or 28 is available in your area as not all areas are equipped for band 14 or 28.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.

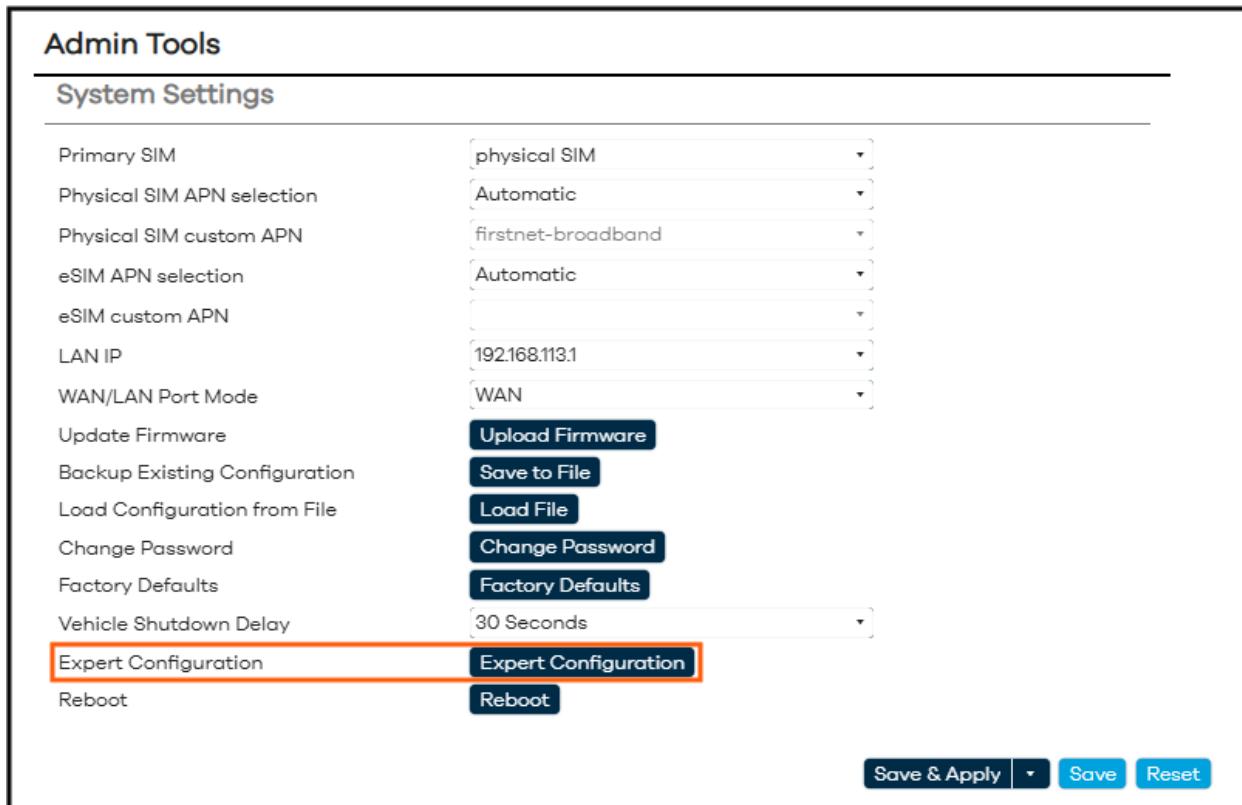


Figure 83: System Settings – Expert Configuration button

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

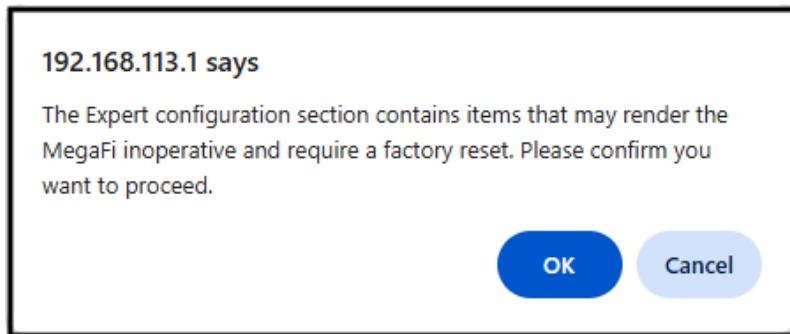


Figure 84: Confirmation to Enter Expert Configuration mode

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

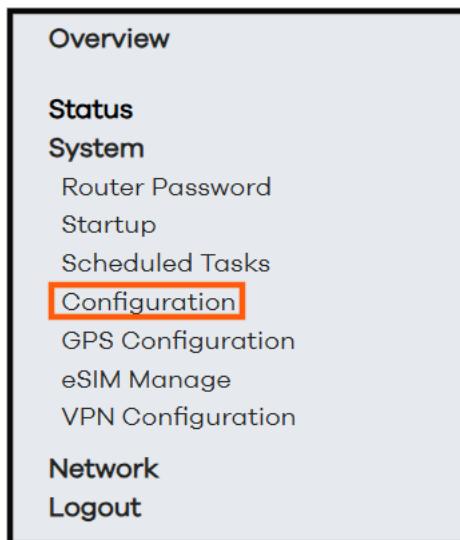


Figure 85: Navigation pane showing options available in Expert mode – Configuration

5. Under the **Other** area, use the drop-down arrow next to **Band Lock** to select **LTE B14 Only** or **LTE B28 Only**. Choose the **Default Band Configuration** option to set back to default setting in which the device relies on the Network to choose the appropriate band.

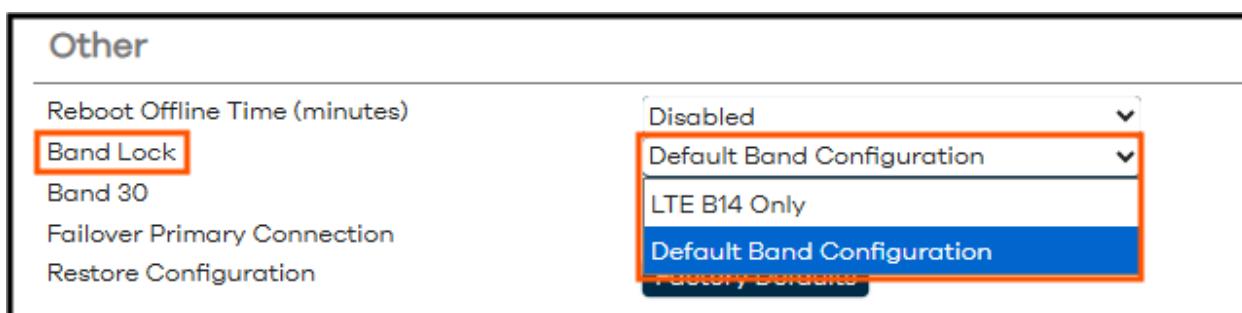


Figure 86: Band Lock Setting

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

3.13 SSH Access

The user-enabled SSH instance (**Dropbear**) offers SSH network shell access and an integrated SCP server. Access to SSH on the MegaFi 2 is turned off by default. To enable command line **SSH Access** to the device, do the following in Mission Control.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.

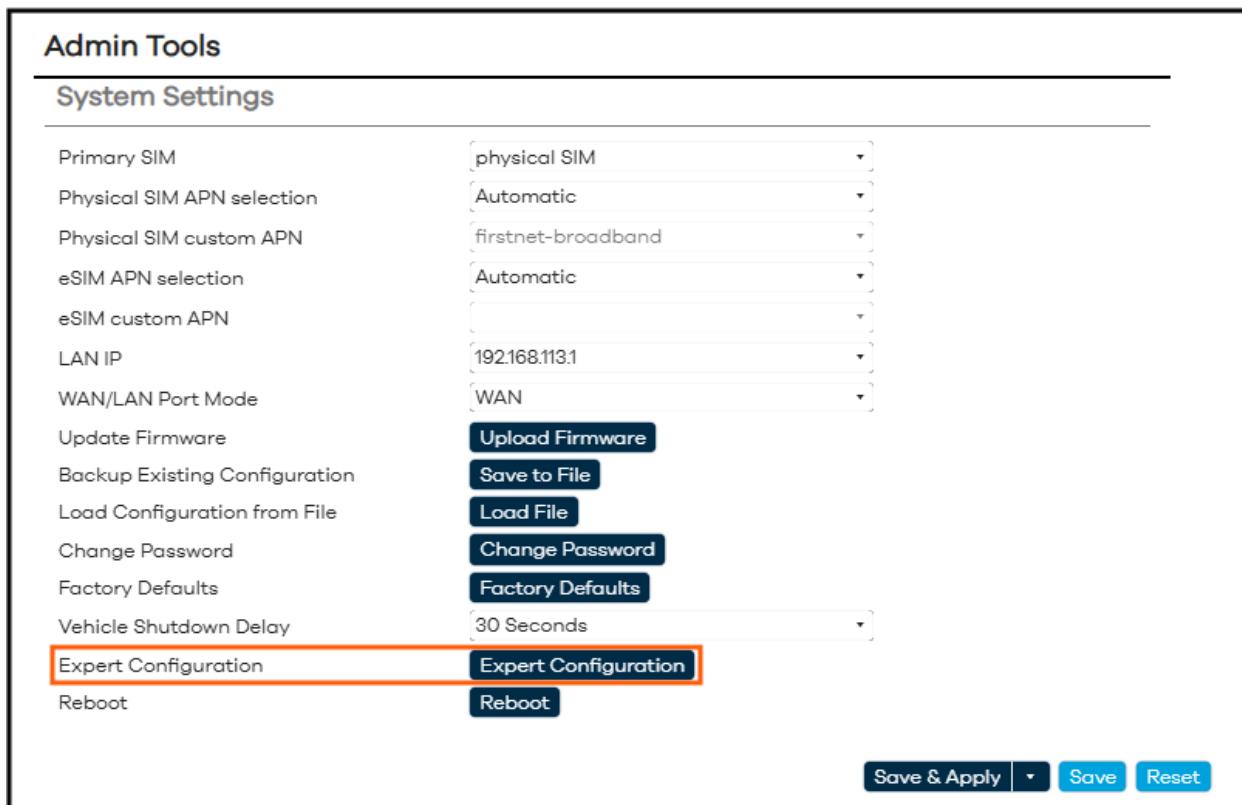


Figure 87: System Settings – Expert Configuration

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

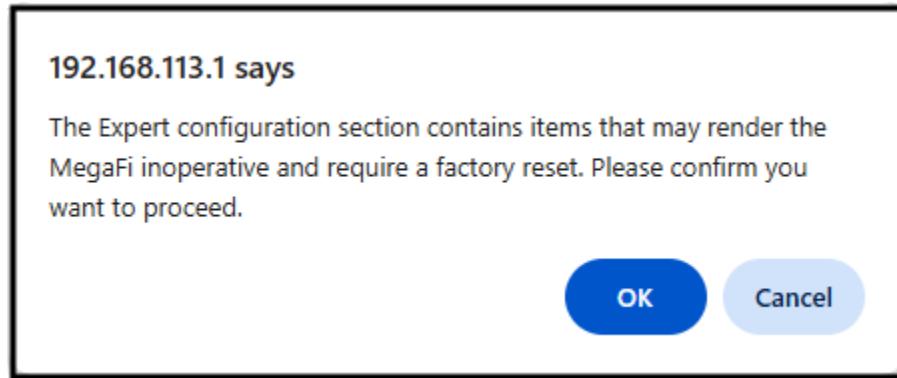


Figure 88: Confirmation to Enter Expert Configuration mode

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

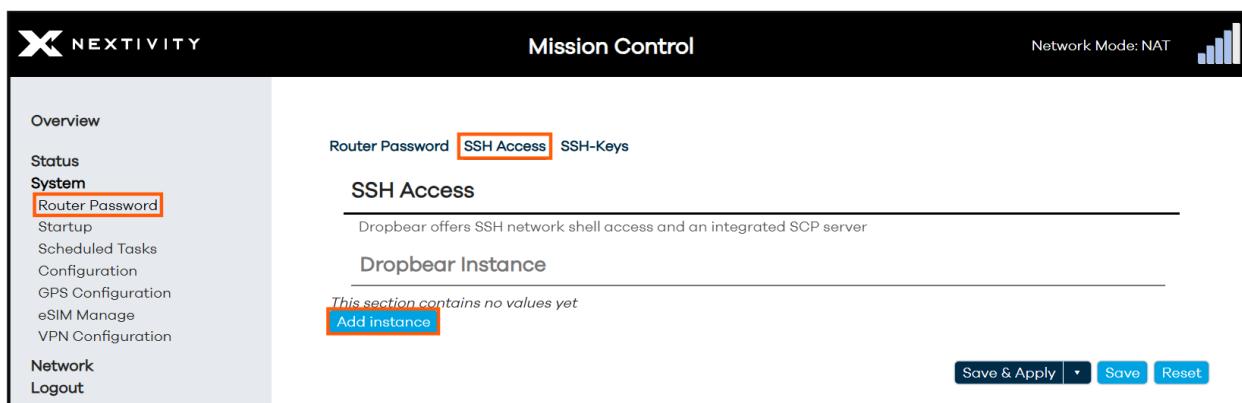


Figure 89: SSH Access – add new instance

5. Click on the **Add instance** button.
6. The **Interface** field will be pre-populated with the **LAN** interface by default and is the only option when needing local access to the device. The other options in the dropdown menu are **wan**, **wan6**, 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 for local access) or another port of your choosing that is not being used and hard for hackers to guess (typical for SSH wan access).
8. **Idle Timeout** is set to **300** seconds by default. Adjust for more or less time in seconds as needed.
9. All other settings are not required and are optional.
10. Click on **Save & Apply** to confirm changes.

SSH Access

Dropbear offers SSH network shell access and an integrated SCP server

Dropbear Instance

Interface: wan

Port: 22

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

Password authentication

Allow root logins with password

Allow remote hosts to connect to local SSH forwarded ports

Idle Timeout: 300

Add Instance

Save & Apply | **Save** | **Reset**

Figure 90: SSH Access – Change port number from 2022 to 22

11. Use your preferred SSH client to access MegaFi 2 on port **22** or whatever port configured and use **root** as the username along with the current router password.

⇒ **Note:** The SSH password will be the same as the Router Password.

12. **Optional:** If remote **SSH Access** to the device is required and the device has a custom static/public IP address, do the following to open the appropriate **wan** interface:

- 12a. Within the **SSH Access** page, click on **Add instance**.
- 12b. Choose the appropriate **wan** interface from the **Interface** drop-down menu.
 - **wwan** – most typical choice to access SSH from the cellular network
 - **wan** – only select if the device has internet connection through wan port
 - **wan6** – currently not widely used
- 12c. Choose a port such as 46556 or something similar that is not the typical SSH port 22.
- 12d. It is recommended to leave the **Idle Timeout** set to **300** or less for **wan** access for security reasons.
- 12e. All other settings are not required and are optional.
- 12f. Click on **Save & Apply** to confirm changes.

3.14 GPS Output Configuration

This is where the user can configure GPS settings on MegaFi 2 for a **GPS Server**, **GPS Internal Reporting**, and **GPS Output** in Mission Control.

- **GPS Server** – This option provides GPS data to applications or clients that request it using a predefined server port.
- **GPS Internal Reporting** – This is how the MegaFi 2 will process GPS data and display it on-device only. The user can choose the format and the optional NMEA station code or TAIP ID and Rate. The default format setting is NMEA.
- **GPS Output** – This most widely used option transmits or shares GPS data to other systems using a host's IP address, a port number, a defined format (NMEA or TAIP), and a TCP/IP connection method using UDP as the protocol of choice. NMEA station code or TAIP ID and Rate are other options available in this area.

The screenshot shows the 'Mission Control' interface for a Nextivity device. The left sidebar includes links for Overview, Status, System (Router Password, Startup, Scheduled Tasks), Configuration (GPS Configuration, eSIM Manage, VPN Configuration), and Network (Logout). The 'GPS Configuration' link is highlighted with a red box. The main content area is titled 'GPS Output Configuration' and contains sections for 'GPS Server' (Server Port), 'GPS Internal Reporting' (Output Format set to 'NMEA', NMEA station code or TAIP ID, Rate), and 'GPS Output' (status message: 'This section contains no values yet', 'Add output' button). At the bottom are 'Save & Apply', 'Save', and 'Reset' buttons.

Figure 91: GPS Output Configuration page

3.14.1 GPS Server

To set up the MegaFi 2 to act like a **GPS Server** where GPS clients can request GPS data from, do the following in Mission Control.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.

The screenshot shows the 'Admin Tools' interface with the 'System Settings' tab selected. The 'Expert Configuration' button is highlighted with an orange border. At the bottom right, there are buttons for 'Save & Apply', 'Save', and 'Reset'.

Setting	Value
Primary SIM	physical SIM
Physical SIM APN selection	Automatic
Physical SIM custom APN	firstnet-broadband
eSIM APN selection	Automatic
eSIM custom APN	
LAN IP	192.168.113.1
WAN/LAN Port Mode	WAN
Update Firmware	Upload Firmware
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
Reboot	Reboot

Figure 92: System Settings – Expert Configuration

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

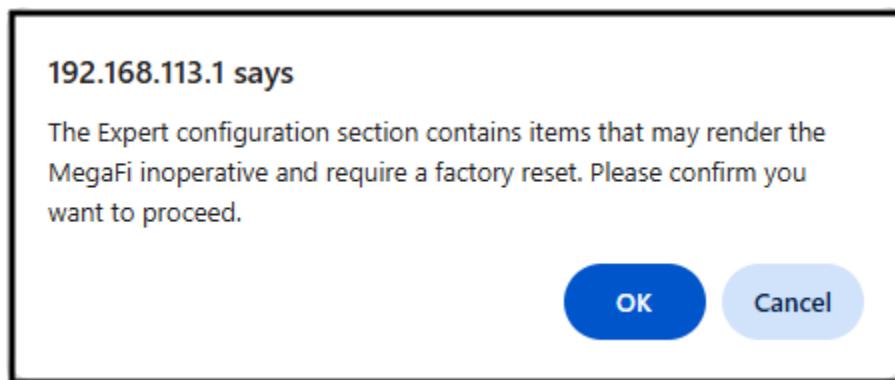


Figure 93: Confirmation to Enter Expert Configuration mode

4. The left-pane menu exposes pages only available in Expert Configuration mode. Navigate to **System > GPS Configuration > GPS Server**.
5. Enter the designated server port number for the **GPS Server** in the **Server Port** field, followed by hitting the **Enter** button. We entered **21000** in our example below:

A screenshot of the "GPS Output Configuration" page. The title is "GPS Output Configuration" with the subtitle "Configure GPS output in NMEA and TAIP format to hosts".

- GPS Server** section: "Server Port" field contains "21000", which is highlighted with a red box.
- GPS Internal Reporting** section: "Output Format" dropdown is set to "NMEA".
 - "NMEA station code or TAIP ID" field is empty.
 - "Rate" field contains "1".
- GPS Output** section: "This section contains no values yet".
 - "Add output" button.

At the bottom are three buttons: "Save & Apply" (with a dropdown arrow), "Save", and "Reset".

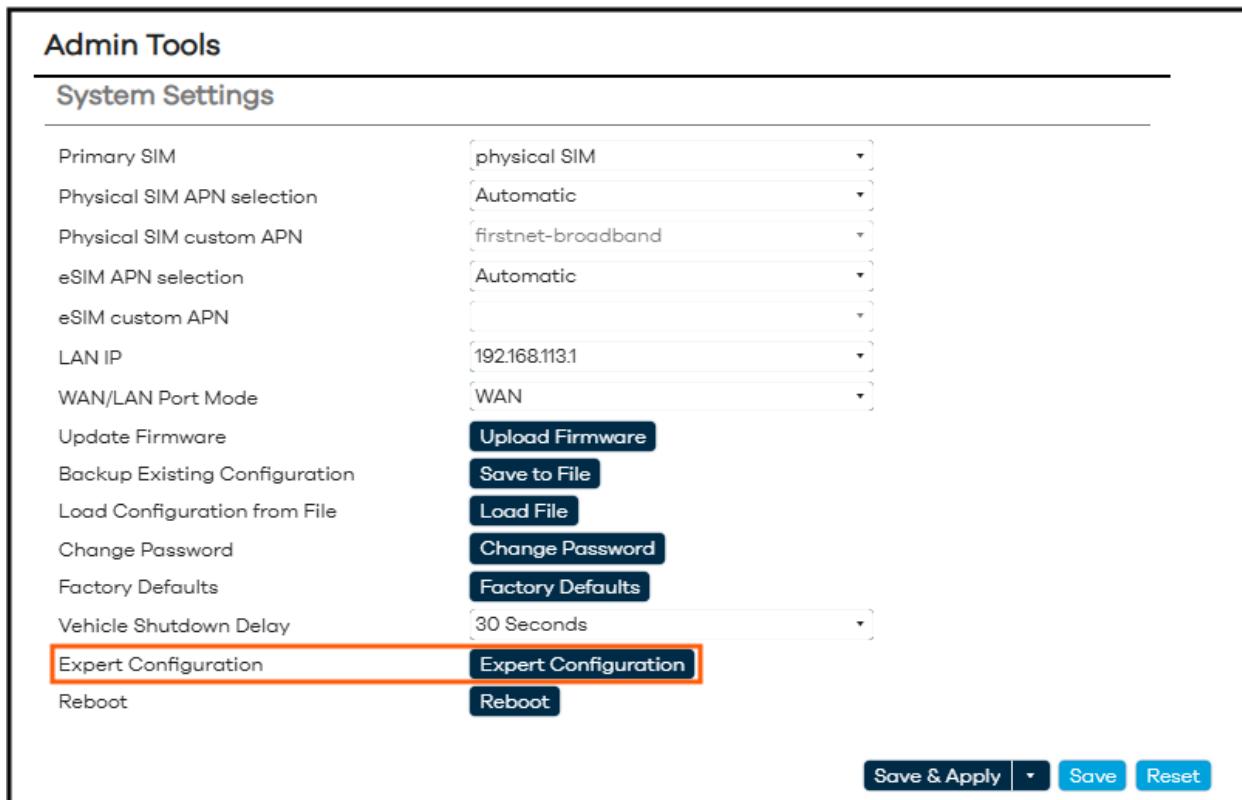
Figure 94: GPS Server Port Configuration

6. Click on **Save & Apply** to confirm the **GPS Server** setting.

3.14.2 GPS Internal Reporting

This section modifies the **GPS Internal Reporting** format and how it is displayed on MegaFi 2. To modify these settings, do the following in Mission Control.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.



The screenshot shows the 'System Settings' page under 'Admin Tools'. The 'Expert Configuration' button is highlighted with an orange border. Other buttons like 'Upload Firmware', 'Save to File', 'Load File', 'Change Password', and 'Factory Defaults' are also visible.

Setting	Value
Primary SIM	physical SIM
Physical SIM APN selection	Automatic
Physical SIM custom APN	firstnet-broadband
eSIM APN selection	Automatic
eSIM custom APN	
LAN IP	192.168.113.1
WAN/LAN Port Mode	WAN
Update Firmware	Upload Firmware
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
Reboot	Reboot

Buttons at the bottom: **Save & Apply** (dropdown), **Save**, **Reset**.

Figure 95: System Settings – Expert Configuration

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

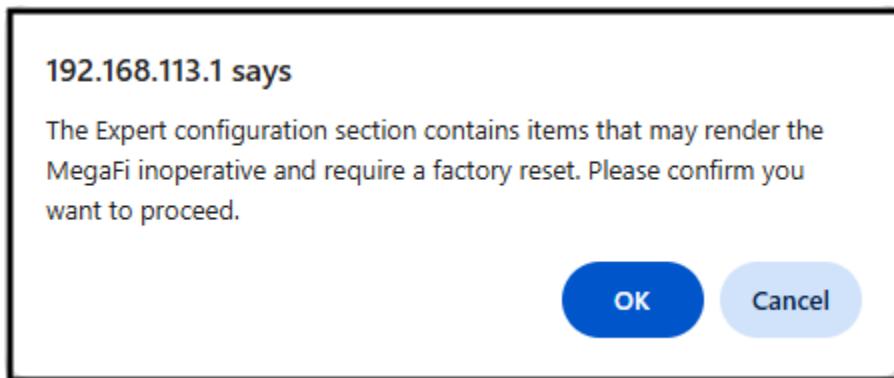


Figure 96: Confirmation to Enter Expert Configuration mode

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

GPS Output Configuration

Configure GPS output in NMEA and TAIP format to hosts

GPS Server

Server Port

GPS Internal Reporting

Output Format: NMEA

NMEA station code or TAIP ID: 1

Rate: Optional rate limit in seconds

GPS Output

This section contains no values yet

Add output

Save & Apply | Save | Reset

Figure 97: GPS Internal Reporting Configuration

5. **NMEA** is the default output format. Modify the following as needed for the MegaFi 2 to display the GPS message on-device.

- Output Format** – TAIP or NMEA
- NMEA station code or TAIP ID** (optional) – enter a valid alphanumeric value that is 4 characters long.
- Rate** (optional) – this parameter is in seconds. Leave as is or enter a rate between 1 – 3600.

6. Click on **Save & Apply** to confirm the **GPS Internal Reporting** settings.
7. To verify the on-device GPS settings, navigate to **Overview > System Settings** under **Admin Tools**.
8. Click on the **Expert Configuration** button to enter Expert Configuration mode.
9. A pop-up window asks the user to confirm going into Expert Configuration mode. Click **OK** to continue.
10. The left-pane menu exposes pages only available in Expert Configuration mode. Navigate to **Status > Modem Status** and verify the GPS as shown below for either **NMEA** or **TAIP** format.

Mission Control			
Overview	Modem Status		
Status	System Name: SHIELD Modem Software Version: A0R.001151_M0R160005 IMEI: 359172391104472 ICCID: 89011003330135141132 IMSI: 313100013545226 Phone Number: 858.310.6948 Latitude: 33.019592 Longitude: -117.087845 NMEA/TAIP Position: \$GPGGA,222510.000,3301.17559,N,11705.27056,W,1,15,0.7,231.9,M,-34.7,M,,1550*64 GPS UTC Timestamp: Tue Jan 06 2026 14:25:10 GMT-0800 (Pacific Standard Time)		
General	System Name	SHIELD	LTE Connection state
Routing	Modem Software Version	A0R.001151_M0R160005	Connected
Firewall	IMEI	359172391104472	Signal Percentage
System Log	ICCID	89011003330135141132	TX Bytes
Processes	IMSI	313100013545226	RX Bytes
Channel Analysis	Phone Number	858.310.6948	RX Packets
Realtime Graphs			TX Packets
Modem Status			24843
Network Scan			
System	Latitude	33.019592	
Network	Longitude	-117.087845	
Logout	NMEA/TAIP Position	\$GPGGA,222510.000,3301.17559,N,11705.27056,W,1,15,0.7,231.9,M,-34.7,M,,1550*64	
	GPS UTC Timestamp	Tue Jan 06 2026 14:25:10 GMT-0800 (Pacific Standard Time)	
	Mode	5G+	APN
	ID	79474696	Band
	PID	19	TAC
	EARFCN	700	RSRP
	Home Network MCC	313	RSRQ
	Home Network MNC	100	RSSI
	Home Network Name	FirstNet	SINR
			10.2 dB
			TX Power
			3 dBm

Figure 98: On-device GPS NMEA message format

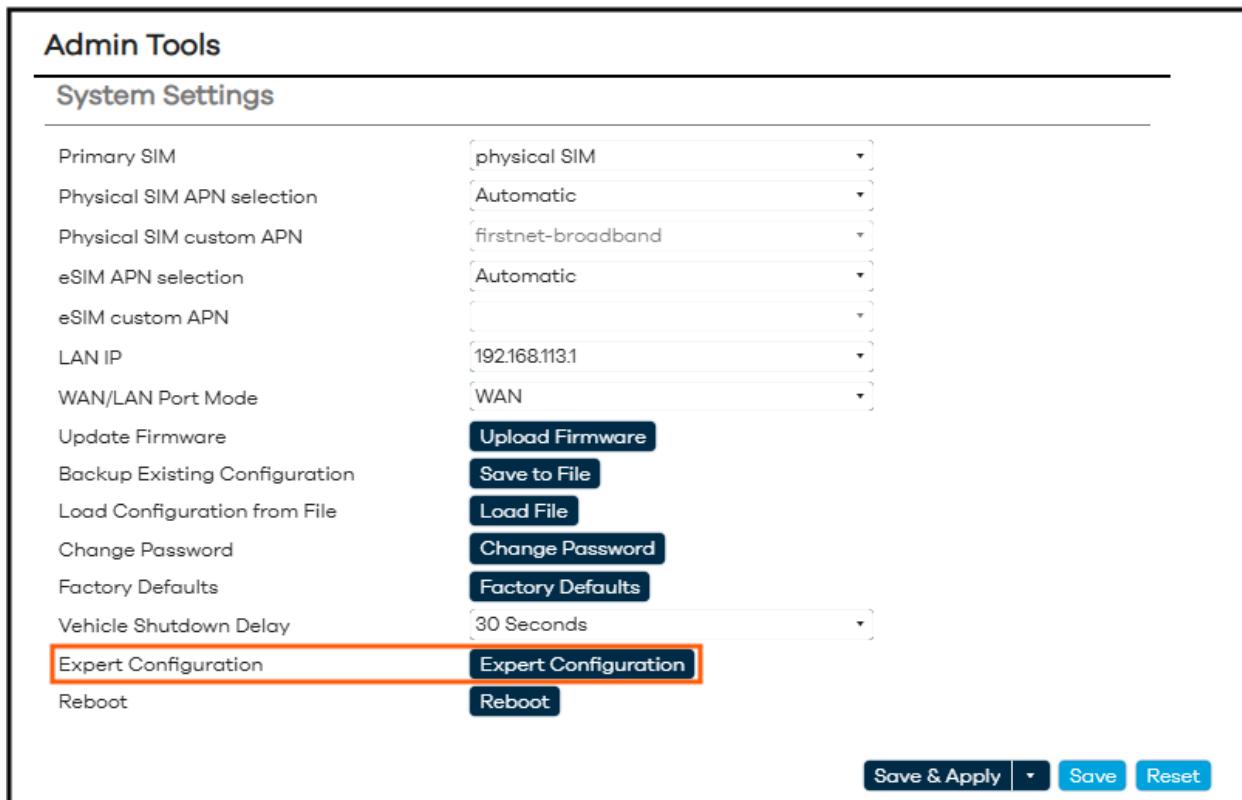
Overview		Mission Control		Network Mode: NAT
Status		Modem Status		
General	System Name	SHIELD	LTE Connection state	Connected
Routing	Modem Software Version	A0R.001151_M0R.160005	Signal Percentage	100%
Firewall	IMEI	359172391104472	TX Bytes	11432654
System Log	ICCID	89010003330135141132	RX Bytes	5245880
Processes	IMSI	313100013545226	TX Packets	35885
Channel Analysis	Phone Number	858.310.6948	RX Packets	24173
Realtime Graphs	Latitude	33.019592		
Modem Status	Longitude	-117.087845		
Network Scan	NMEA/TAIP Position	>RPV\$00616+3301959-1170878400000032;ID=1550,*7F<		
System	GPS UTC Timestamp	Tue Jan 06 2026 14:23:37 GMT-0800 (Pacific Standard Time)		
Network	Mode	5G+	APN	firstnet-broadband
Logout	ID	79474696	Band	2
	PID	19	TAC	33547
	EARFCN	700	RSRP	-69 dBm
	Home Network MCC	313	RSRQ	-9 dB
	Home Network MNC	100	RSSI	-38 dBm
	Home Network Name	FirstNet	SINR	9.6 dB
			TX Power	19 dBm

Figure 99: On-device GPS TAIP message format

3.14.3 GPS Output

This section will enable the MegaFi 2 to transmit or share GPS data to a single or multiple hosts running a GPS receiver or listener. Do the following to configure **GPS Output** in Mission Control.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.



The screenshot shows the 'System Settings' page under 'Admin Tools'. The 'Expert Configuration' button is highlighted with an orange box. Other buttons like 'Upload Firmware', 'Save to File', 'Load File', 'Change Password', and 'Factory Defaults' are also visible.

Setting	Value
Primary SIM	physical SIM
Physical SIM APN selection	Automatic
Physical SIM custom APN	firstnet-broadband
eSIM APN selection	Automatic
eSIM custom APN	
LAN IP	192.168.113.1
WAN/LAN Port Mode	WAN
Update Firmware	Upload Firmware
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
Reboot	Reboot

Buttons at the bottom: **Save & Apply** (dropdown), **Save**, **Reset**.

Figure 100: System Settings – Expert Configuration

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

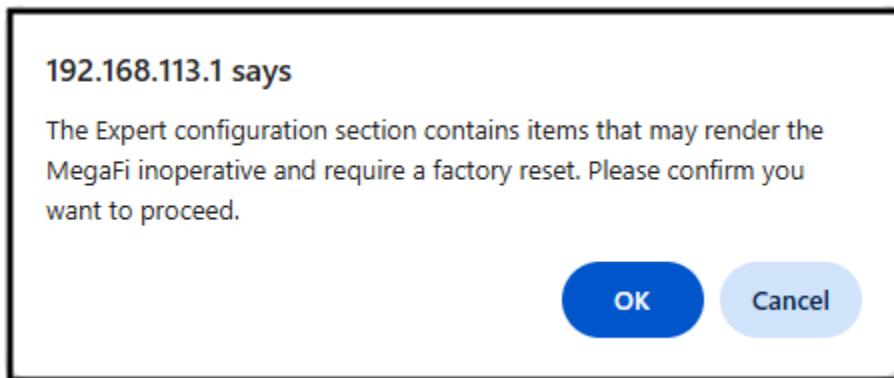


Figure 101: Confirmation to Enter Expert Configuration mode

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

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 102: GPS Output Configuration – Add output

5. Select **Add output** and enter the following information:

5a. **Host IP Address** – Enter the IP address of the workstation or laptop computer running a GPS client. Or select Broadcast to LAN for multiple locally connected devices that need to simultaneously receive GPS information.

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** (optional) – enter a valid alphanumeric value that is 4 characters long.

5e. **TCP/UDP** – UDP is typically the most widely used option. Check with your device to ensure what protocol it is set to.

5f. **Rate** – this parameter is in seconds. Leave as is or enter a rate between 1 – 3600.

⌚ **Note:** In some cases, and for certain systems to receive the proper GPS data, it is best practice to enter a value of 1 in this field or the matching rate value set on the GPS receiver.

GPS Output

Host IP Address: 192.168.113.104

Port: 5555

Output Format: TAIP

NMEA station code or TAIP ID: 1755

TCP/UDP: UDP

Rate: 1

Optional rate limit in seconds

Add output

Save & Apply | **Save** | **Reset**

Figure 103: GPS Output Configuration – Values for adding new output

6. Click on **Save & Apply** to confirm the GPS Output settings.

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 added and configured to transmit and share GPS data to individual clients. This is helpful if you use distinct port numbers, etc. Just repeat this process as needed. Otherwise, select Broadcast to LAN in the Host IP Address drop-down menu to send GPS information to multiple hosts using the same port number, etc. This is especially helpful when you do not know what IP address a host(s) will get assigned from the DHCP server.

⌚ **Note:** There is a **Delete** button to the top right of the **GPS Output**. If the output is no longer needed, click on the button to delete it followed by clicking on **Save & Apply**.

3.15 WAN/LAN Port Mode

The MegaFi 2 has two physical Ethernet ports. By default, the left port labeled **WAN/LAN2** is set to **WAN** mode. It can be set to function as a second LAN port if desired. To change the port mode on this port, do the following in Mission Control.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the drop-down menu next to **WAN/LAN Port Mode** and select **LAN**.

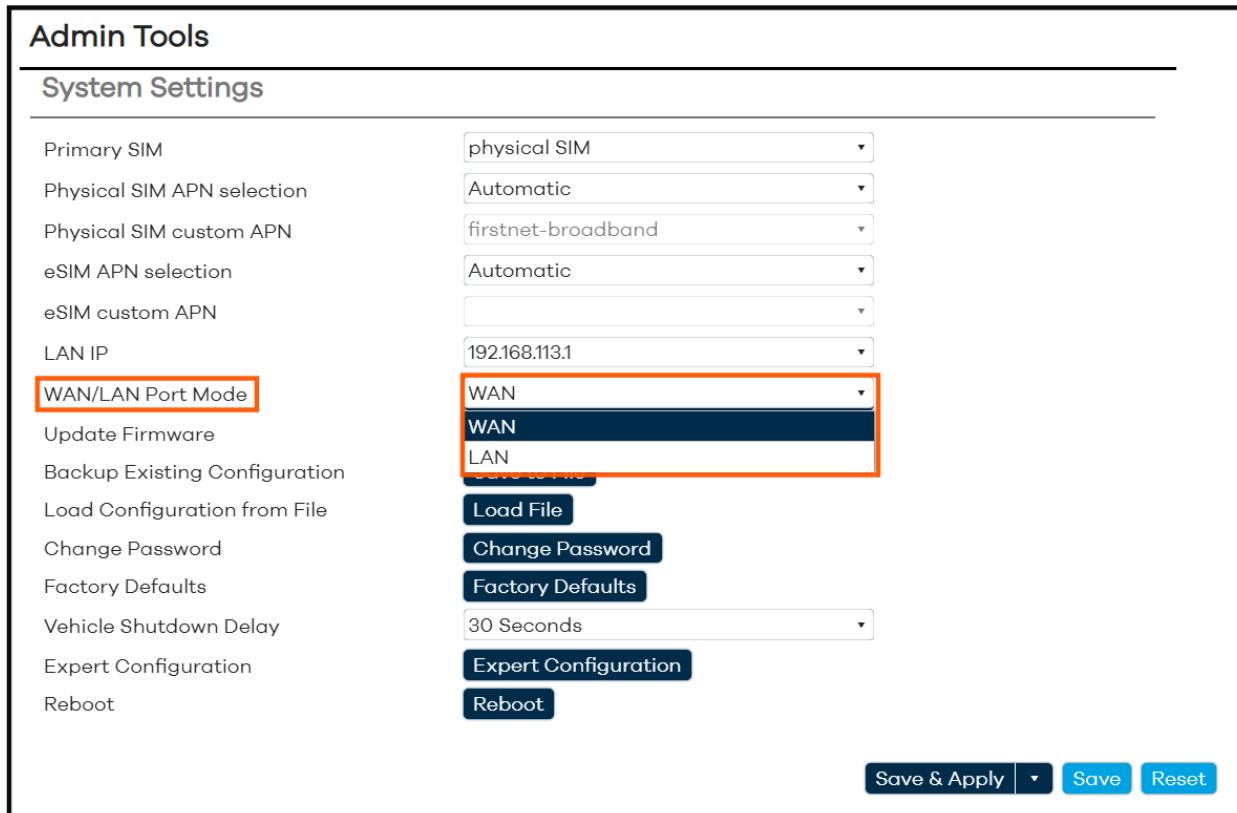


Figure 104: WAN/LAN Port Mode options

3. Click on **Save & Apply** to confirm the **WAN/LAN Port Mode** setting.

⌚ **Note:** The MegaFi 2 is capable of receiving **PoE** (Power over Ethernet) through the **WAN/LAN2** port. Check the MegaFi 2 User Manual for specifications.

3.16 LCD Configuration

The MegaFi 2 LCD display screen can be configured for the following settings:

LCD Setting	Fixed and Mobile Kit LCD Settings (Default)	LCD Settings - Other Options	MegaGo 2 LCD Settings (Default)
Screen Orientation	Portrait	Landscape	Landscape
Detail Level	Full	Minimal	Full
Turn off screen after (seconds)	600	Always On, custom (-1 – 3600)	Always On
Switch screen information (seconds)	15	1-60	15
Show Mission Control Password on the Display	Disabled	Enabled	Disabled

Table 5: LCD Screen Settings

To make any changes to the LCD Display screen, do the following in Mission Control.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.

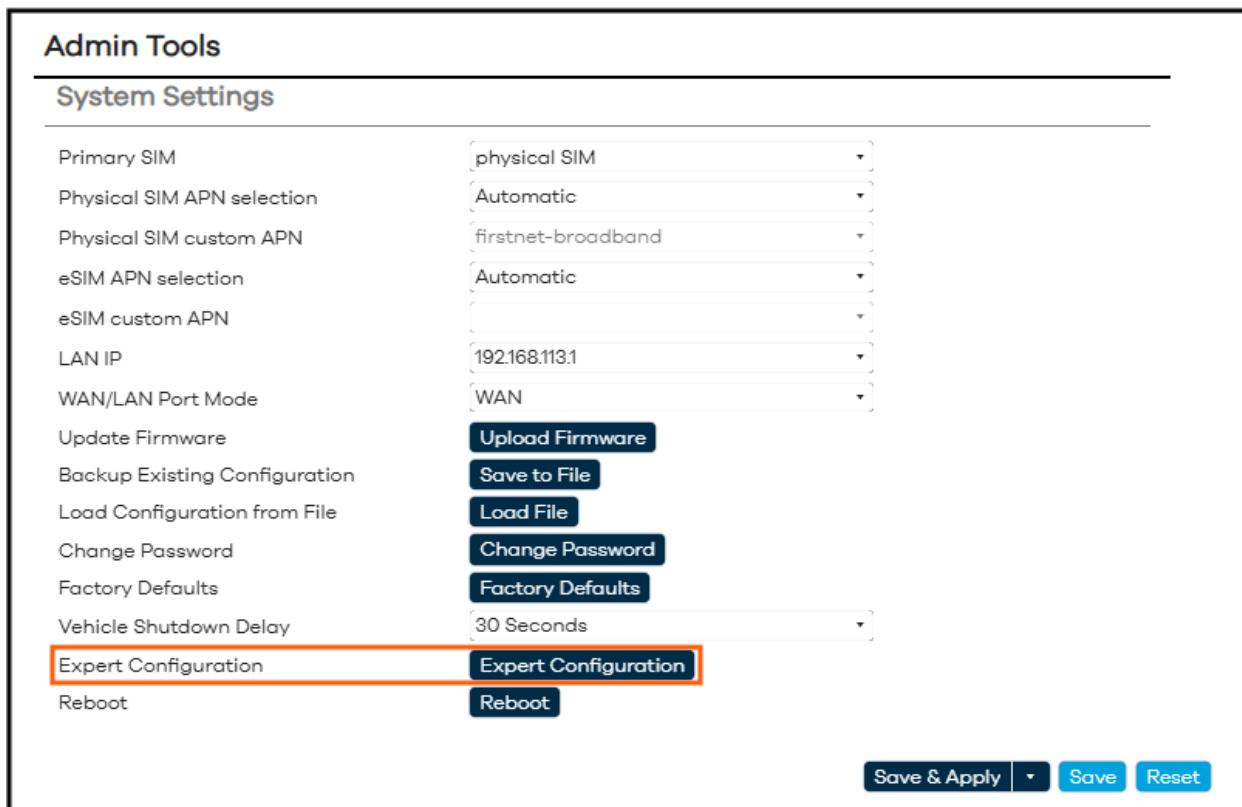


Figure 105: System Settings – Expert Configuration

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

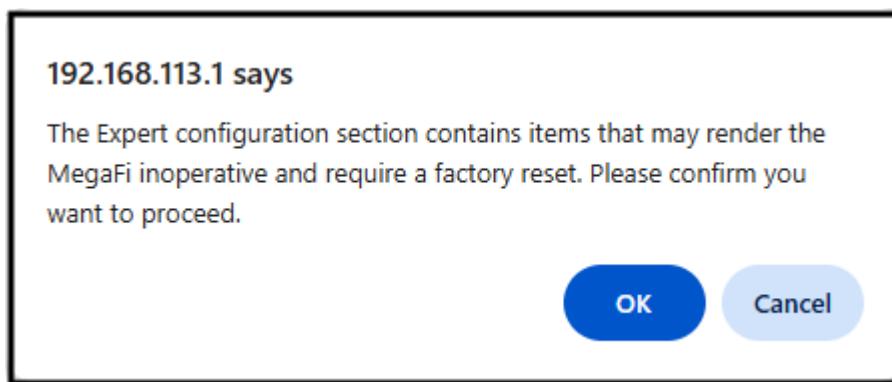


Figure 106: Confirmation to Enter Expert Configuration mode

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

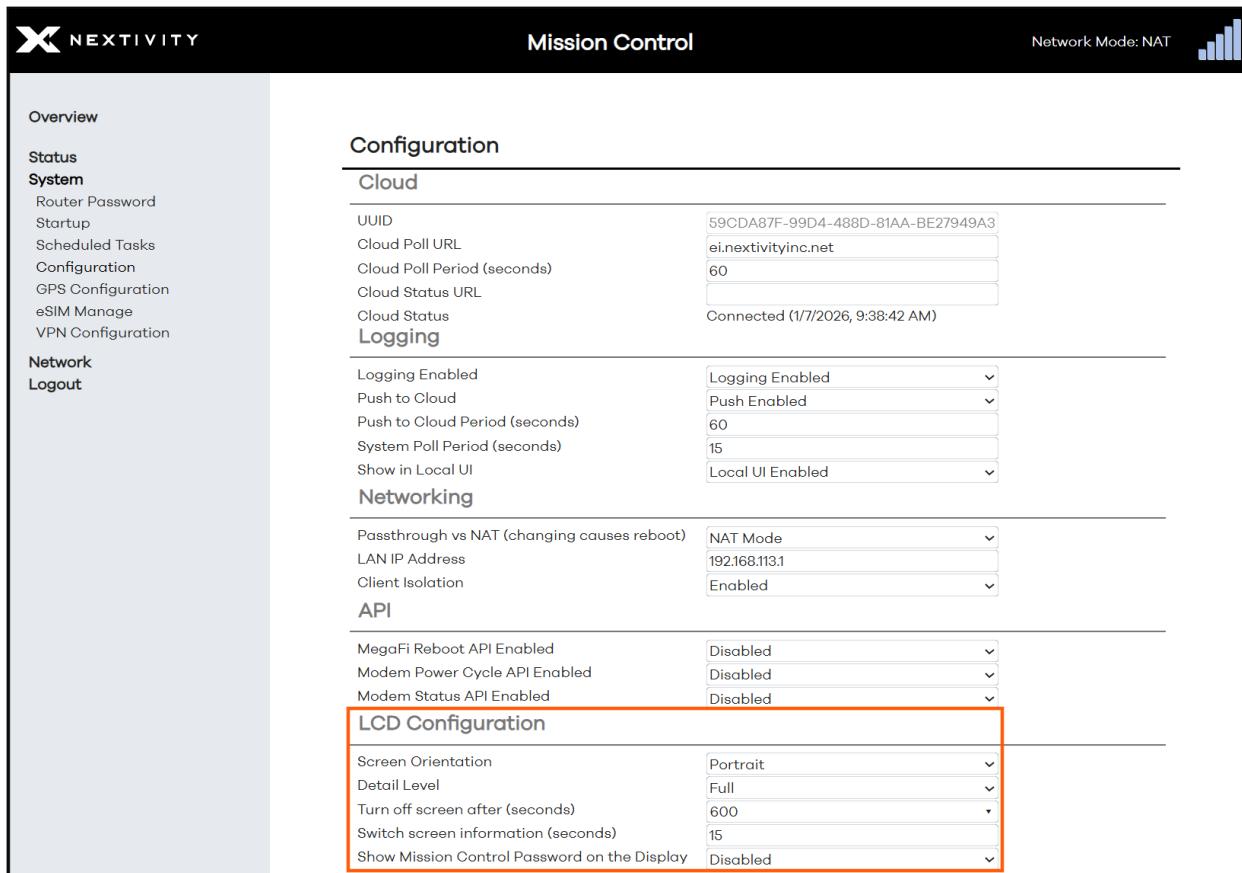


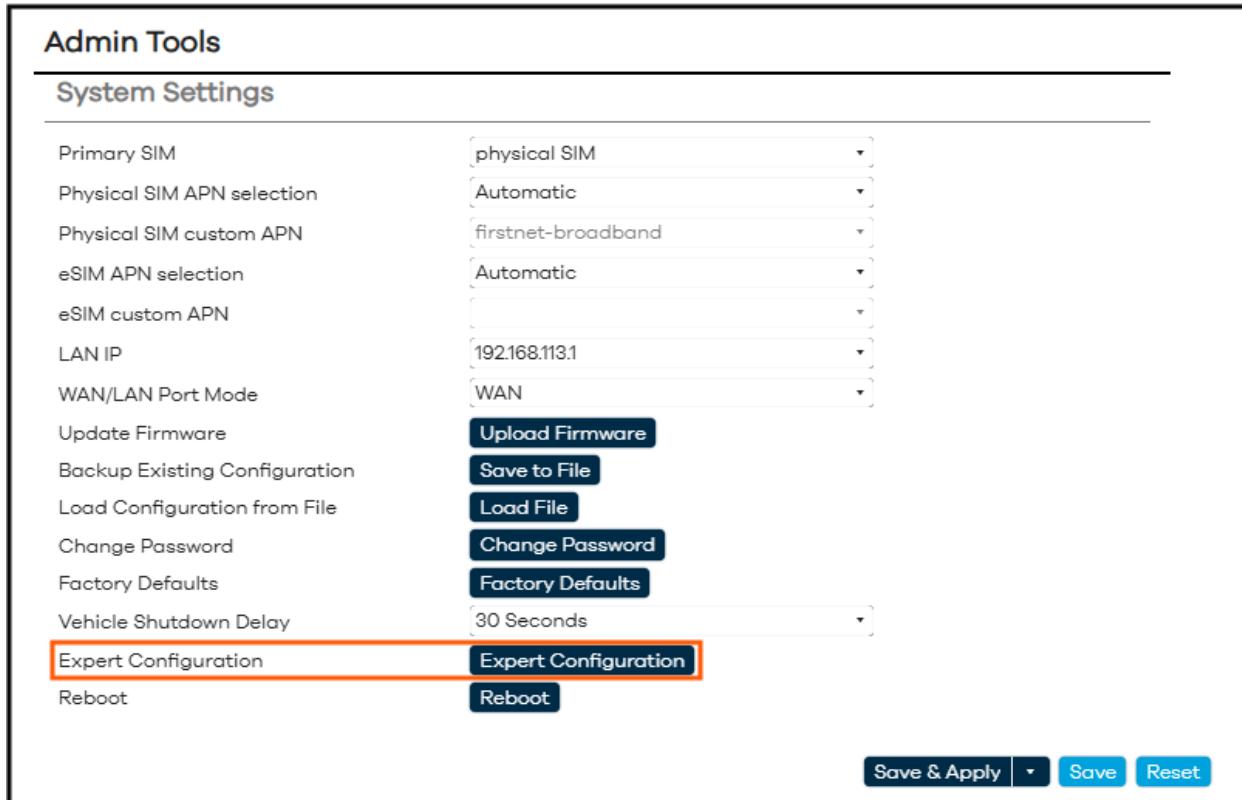
Figure 107: LCD Configuration – default settings

- For settings with a drop-down menu arrow, click the arrow and choose the preferred setting.
 - Screen Orientation** – select from Portrait (default) or Landscape
 - Detail Level** – select from Full (default) or Minimal
 - Turn off screen after (seconds)** – select from 600 (default), Always on, or enter a custom value in seconds between -1 and 3600.
 - Show Mission Control Password on the Display** – Beginning in firmware release version 3.4.1, changing the default password enables this feature and no longer displays the password on the display screen. Select from **Disabled** (default) or **Enabled** to display the device password on the display screen.
- To modify **Switch screen information (seconds)**, remove or delete the previous setting (default is set to 15) and enter a new setting between 1 and 60 in this field, and hit **Enter**. Otherwise, it will revert back to its default setting, or pre-configured setting.
- Click on **Save & Apply** to confirm the change(s).

3.17 SNMP

Beginning with firmware release version 3.4.1, SNMP was implemented into Mission Control. Though it is currently in an experimental feature. Please use this section with caution. To configure SNMP settings, do the following in Mission Control:

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.



The screenshot shows the 'System Settings' page under 'Admin Tools'. The 'Expert Configuration' button is highlighted with a red box. Other buttons like 'Upload Firmware', 'Save to File', 'Load File', 'Change Password', and 'Factory Defaults' are also visible.

Setting	Value
Primary SIM	physical SIM
Physical SIM APN selection	Automatic
Physical SIM custom APN	firstnet-broadband
eSIM APN selection	Automatic
eSIM custom APN	
LAN IP	192.168.113.1
WAN/LAN Port Mode	WAN
Update Firmware	Upload Firmware
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
Reboot	Reboot

Buttons at the bottom: Save & Apply, Save, Reset.

Figure 108: System Settings – Expert Configuration

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

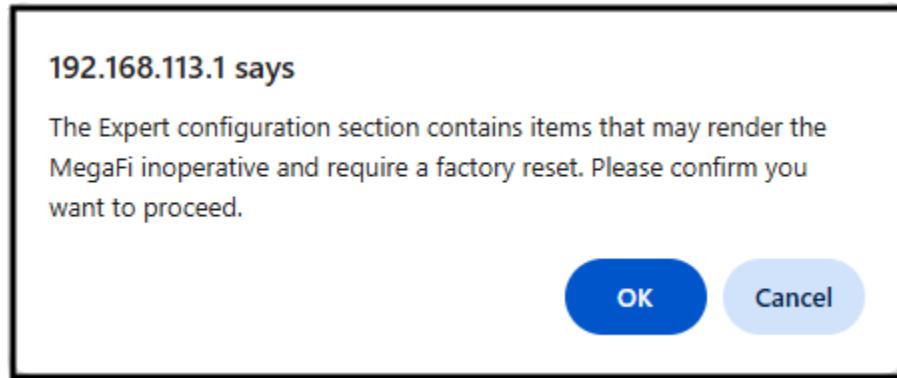


Figure 109: Confirmation to Enter Expert Configuration mode

4. The left-pane menu exposes pages only available in Expert Configuration mode. Navigate to **Network > SNMP**.

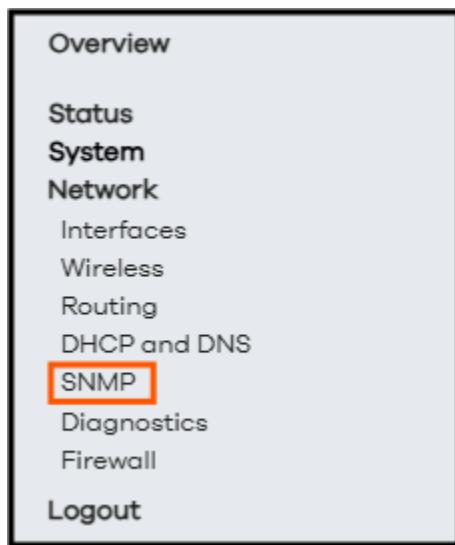


Figure 110: Navigation pane showing options available in Expert mode – Configuration

5. The following SNMP fields are available.

- **Service Enabled** – select from **Disabled** (default) or Enabled from the drop-down menu
- **User** – the default username is “**nexxtivity123**”. Change the username as needed for your environment
- **Authentication Protocol** – select from **SHA-512** (default), **MD5**, **SHA-1**, **SHA-224**, **SHA256**, **SHA-384** from the drop-down menu.
- **Encryption Protocol** – select from **AES-256** (default), **DES**, **AES-128**, **AES-192**
- **Authentication Password** – set to “**authpassword123**” by default. Change the authentication password as needed for your environment.

- **Encryption Password** - set to “**privpassword123**” by default. Change the encryption password as needed for your environment.

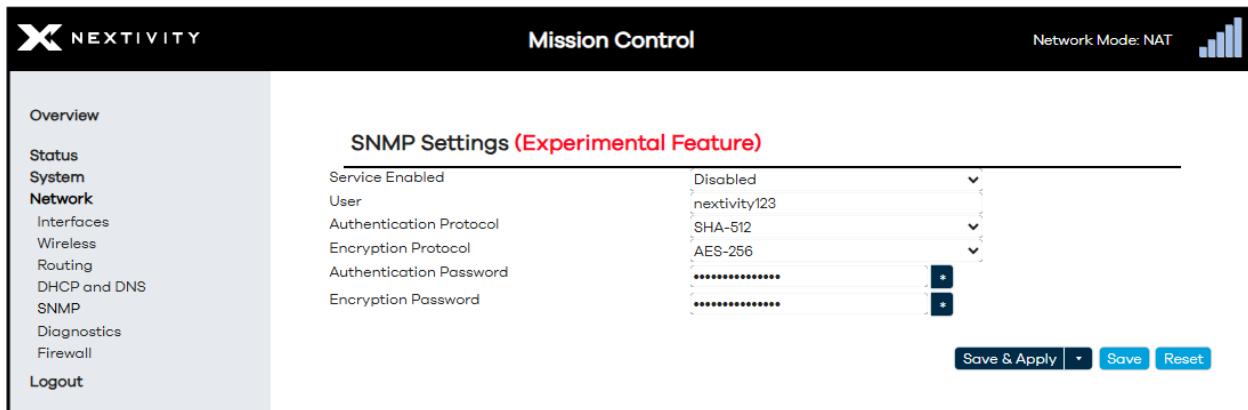
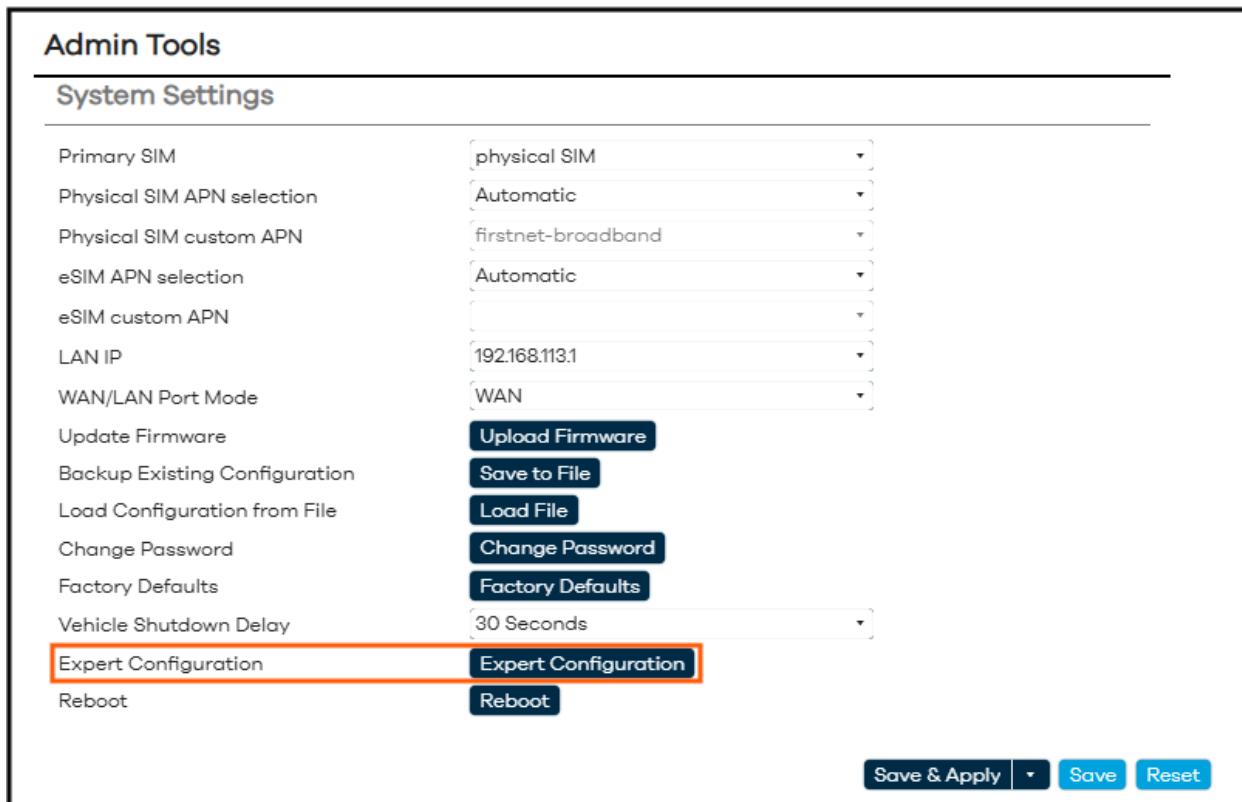


Figure 111: SNMP Settings

3.18 Client Isolation

Beginning with firmware release version 3.4.1, Client Isolation was implemented and enabled by default on both the main LAN subnet and Guest SSIDs. This feature in effect isolates client devices in which they cannot reach or communicate with each other within their respective network. To disable Client isolation for the main LAN subnet and let client devices reach or communicate with each other, do the following in Mission Control:

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.



The screenshot shows the 'System Settings' section of the 'Admin Tools' interface. It includes fields for Primary SIM (physical SIM), Physical SIM APN selection (Automatic), Physical SIM custom APN (firstnet-broadband), eSIM APN selection (Automatic), eSIM custom APN (empty), LAN IP (192.168.113.1), WAN/LAN Port Mode (WAN), and a section for firmware management with buttons for 'Upload Firmware', 'Save to File', 'Load File', 'Change Password', and 'Factory Defaults'. A dropdown for 'Vehicle Shutdown Delay' is set to '30 Seconds'. At the bottom, there are buttons for 'Expert Configuration' (which is highlighted with a red box), 'Reboot', and a 'Save & Apply' button with dropdown menus for 'Save' and 'Reset'.

Figure 112: System Settings – Expert Configuration

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

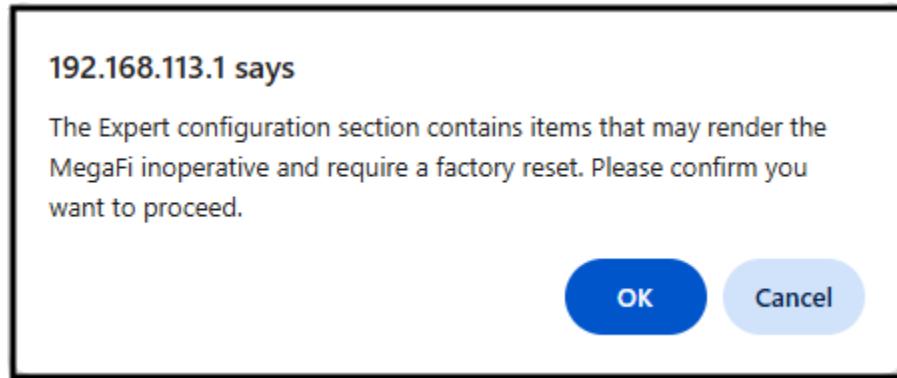


Figure 113: Confirmation to Enter Expert Configuration mode

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

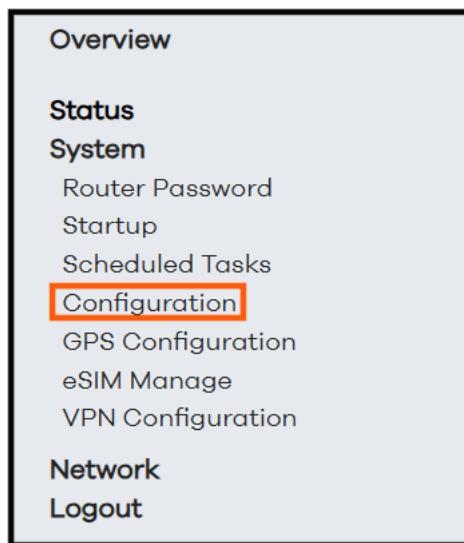
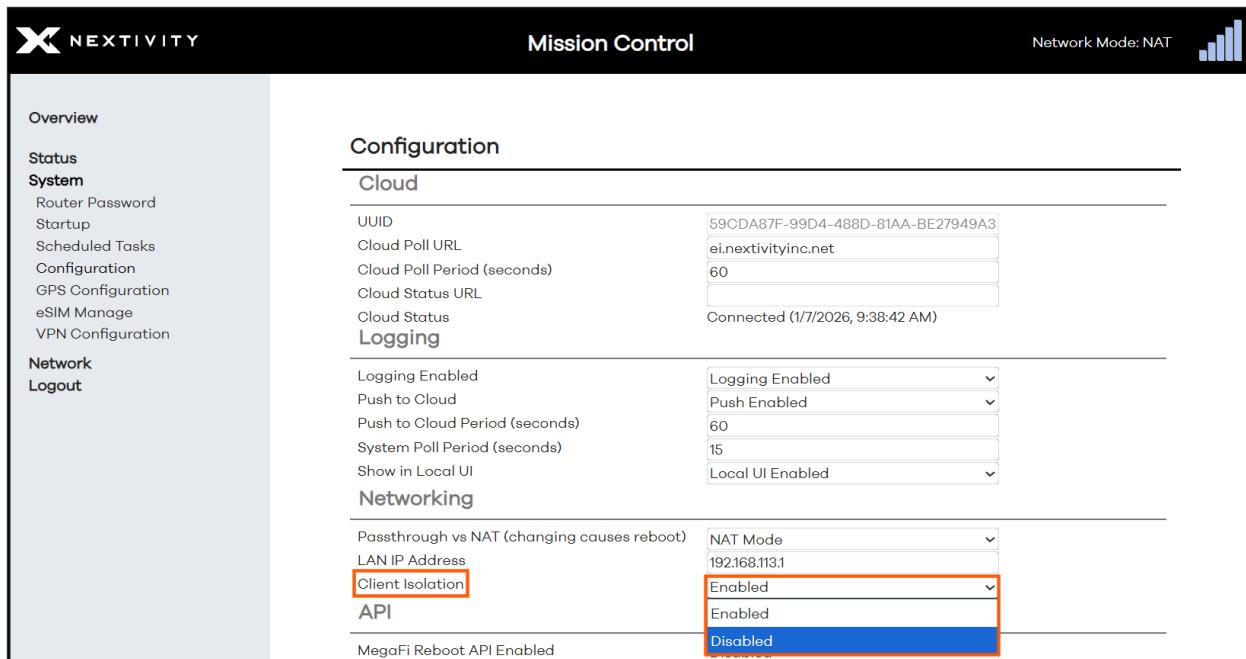


Figure 114: Navigation pane showing options available in Expert mode – Configuration

5. Select Disabled from the drop-down menu to Disable Client isolation.



The screenshot shows the Nextivity Mission Control interface. The left sidebar has sections for Overview, Status, System (with sub-options: Router Password, Startup, Scheduled Tasks, Configuration, GPS Configuration, eSIM Manage, VPN Configuration), and Network (Logout). The main area is titled 'Configuration' and contains sections for 'Cloud', 'Logging', and 'Networking'. In the 'Networking' section, there is a dropdown for 'Client Isolation' which is set to 'Enabled'. This dropdown is highlighted with a red box. Below it, there is another dropdown for 'MegaFi Reboot API Enabled' which is set to 'Disabled'. This second dropdown is also highlighted with a red box. The top right of the interface shows 'Network Mode: NAT' and a signal strength icon.

Figure 115: Client Isolation

6. Click on **Save & Apply** at the bottom to confirm the change.

3.19 Failover Primary Connection

Failover Primary Connection is set to **WAN – Internet Connection** by default. If you have both a WAN and WWAN connection, the physical WAN connection will be the preferred connection but if this connection is lost, the device will failover to the WWAN interface or cellular modem connection (**WWAN – Modem Connection**). If you prefer the WWAN interface, to be your primary connection, do the following in Mission Control:

- ⦿ **Note:** If you are only using the WWAN connection (most typical setup), there is no configuration needed and this setting can be left at default setting.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.

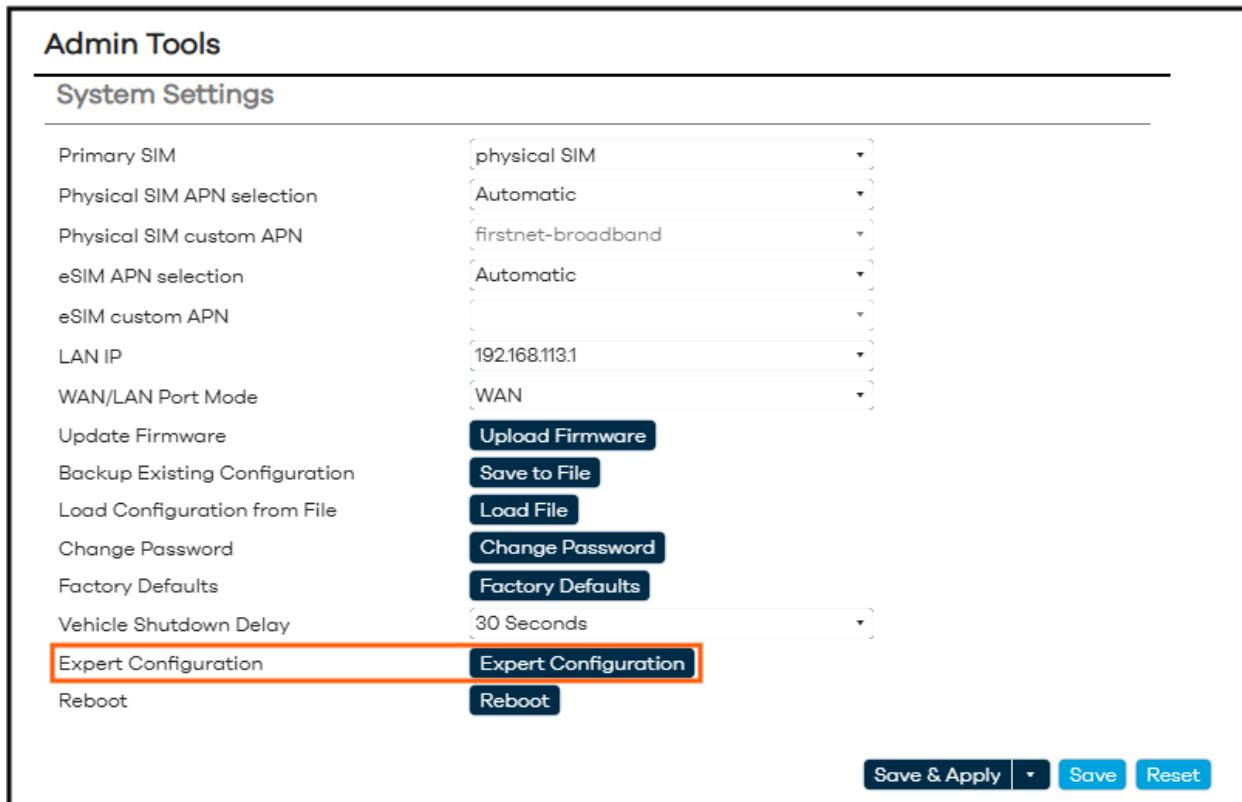


Figure 116: System Settings – Expert Configuration

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

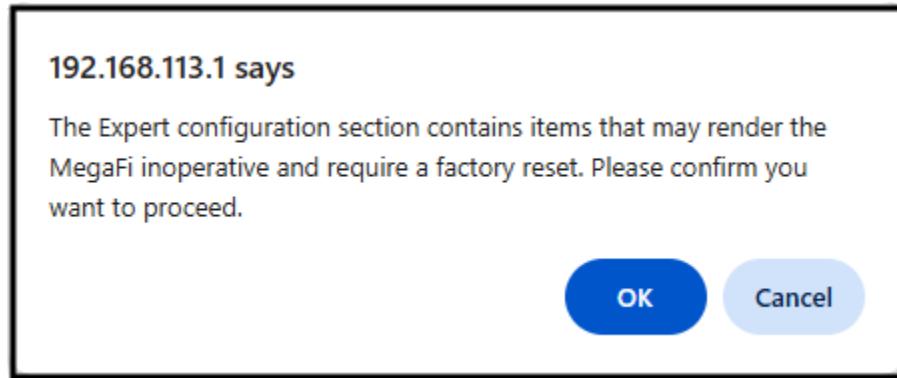


Figure 117: Confirmation to Enter Expert Configuration mode

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

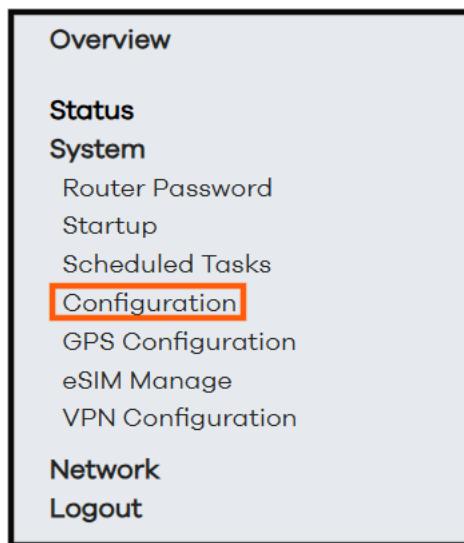
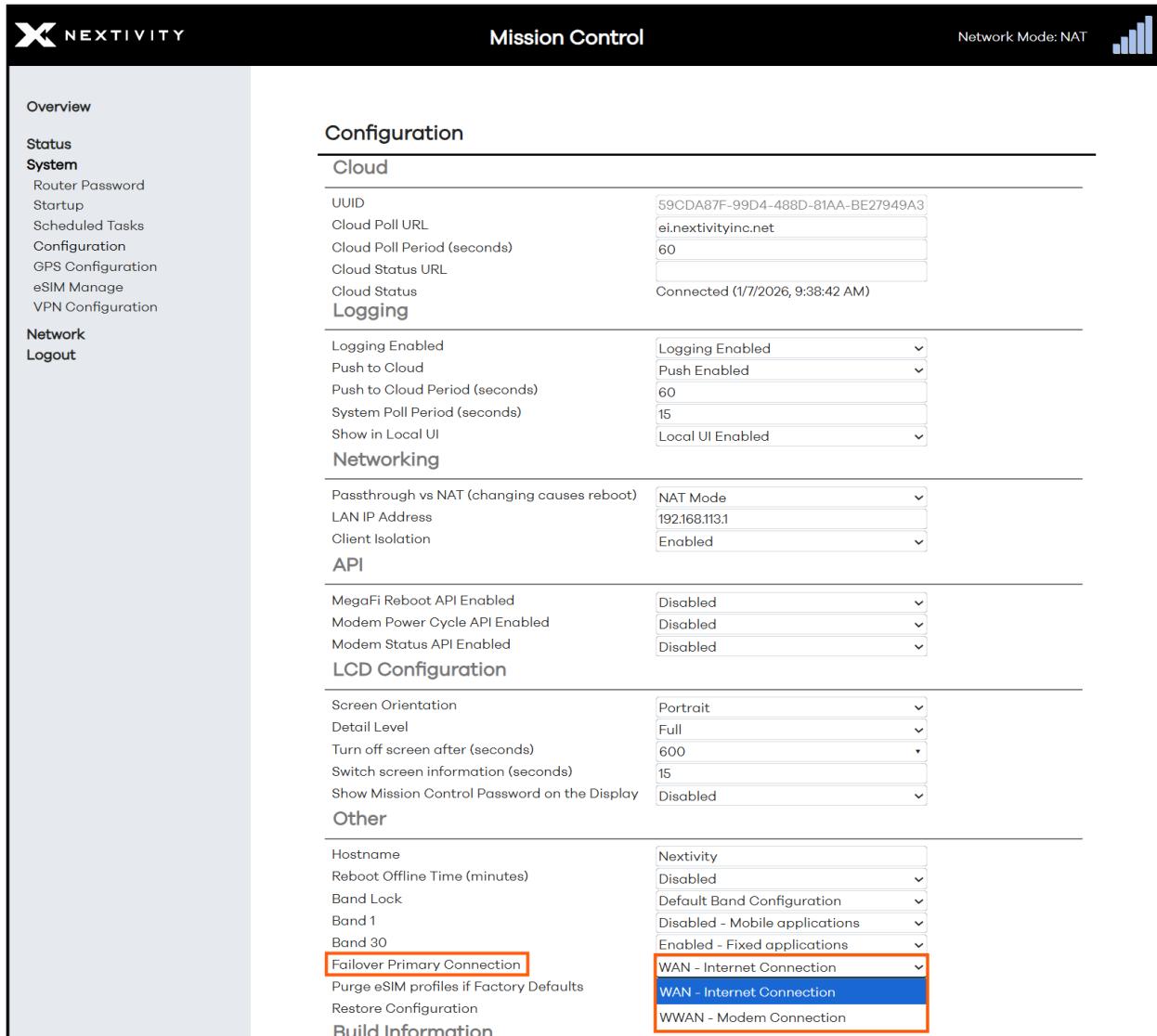


Figure 118: Navigation pane showing options available in Expert mode – Configuration

5. Scroll down to **Other** section and select **WWAN – Modem Connection** from the drop-down menu for **Failover Primary Connection**.



The screenshot shows the NEXTIVITY Mission Control interface. The left sidebar includes links for Overview, Status, System (Router Password, Startup, Scheduled Tasks, Configuration, GPS Configuration, eSIM Manage, VPN Configuration), and Network (Logout). The main 'Configuration' page has several sections: Cloud, Logging, Networking, API, LCD Configuration, and Other. In the 'Other' section, the 'Build Information' table has a row for 'Failover Primary Connection' with three options: 'WAN - Internet Connection' (selected and highlighted in blue), 'WAN - Internet Connection' (disabled), and 'WWAN - Modem Connection'.

Build Information	Failover Primary Connection
WAN - Internet Connection	Selected
WAN - Internet Connection	Disabled
WWAN - Modem Connection	

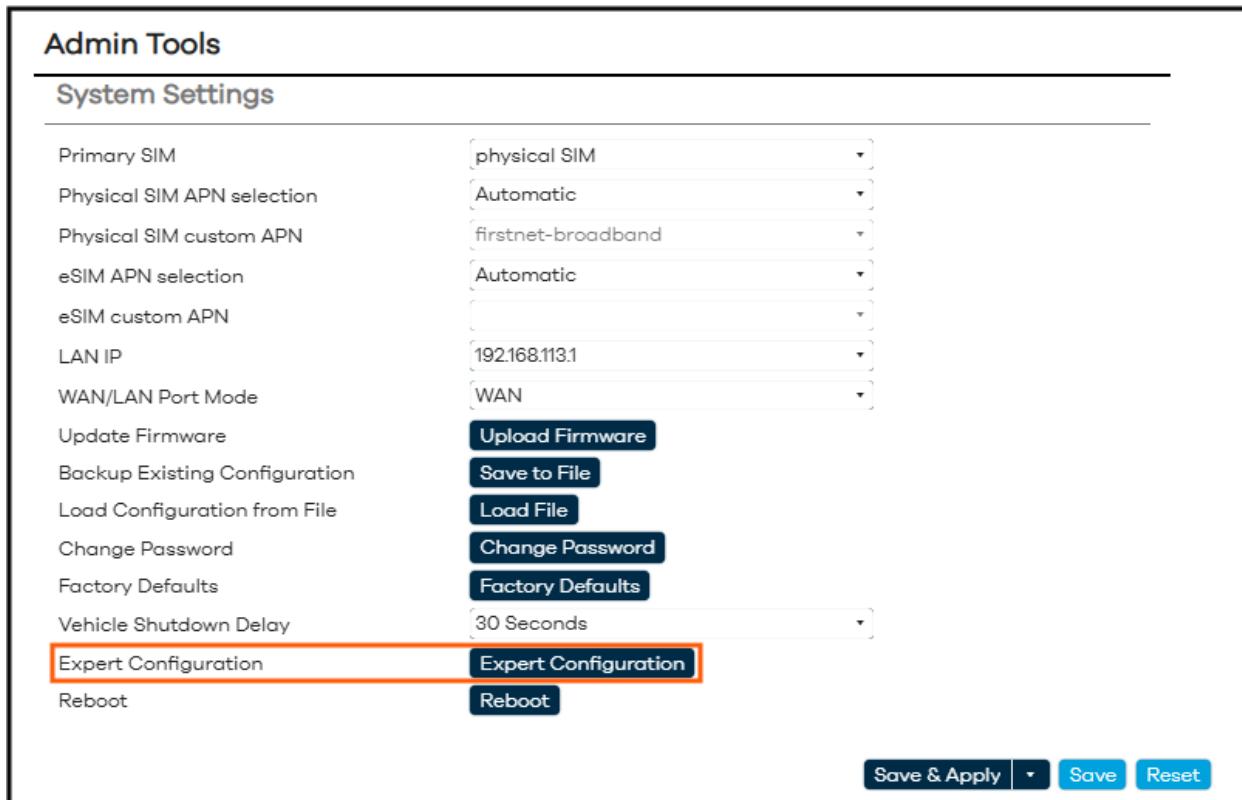
Figure 119: Failover Primary Connection

6. Click on **Save & Apply** at the bottom to confirm the change.

3.20 Network Scan

The MegaFi 2 is now capable of producing a manual scan list of available bands. A Network Scan menu page has been added to Mission Control under Expert Configuration / Status that enables the user to scan for available bands and export the result. To produce a manual scan, do the following in Mission Control:

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.



The screenshot shows the 'Admin Tools' interface with the 'System Settings' tab selected. The configuration page includes the following settings:

- Primary SIM: physical SIM
- Physical SIM APN selection: Automatic
- Physical SIM custom APN: firstnet-broadband
- eSIM APN selection: Automatic
- eSIM custom APN: (empty dropdown)
- LAN IP: 192.168.113.1
- WAN/LAN Port Mode: WAN
- Update Firmware: **Upload Firmware**
- 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** (highlighted with a red box)
- Reboot: **Reboot**

At the bottom right are buttons for **Save & Apply**, **Save**, and **Reset**.

Figure 120: System Settings – Expert Configuration

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

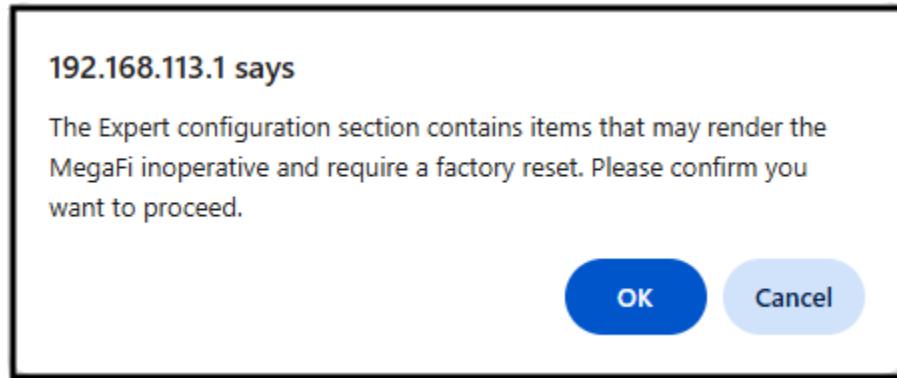


Figure 121: Confirmation to Enter Expert Configuration mode

4. The left-pane menu exposes pages only available in Expert Configuration mode. Navigate to **Status > Network Scan**.
5. Click on the Scan Now button to produce a list of available bands.

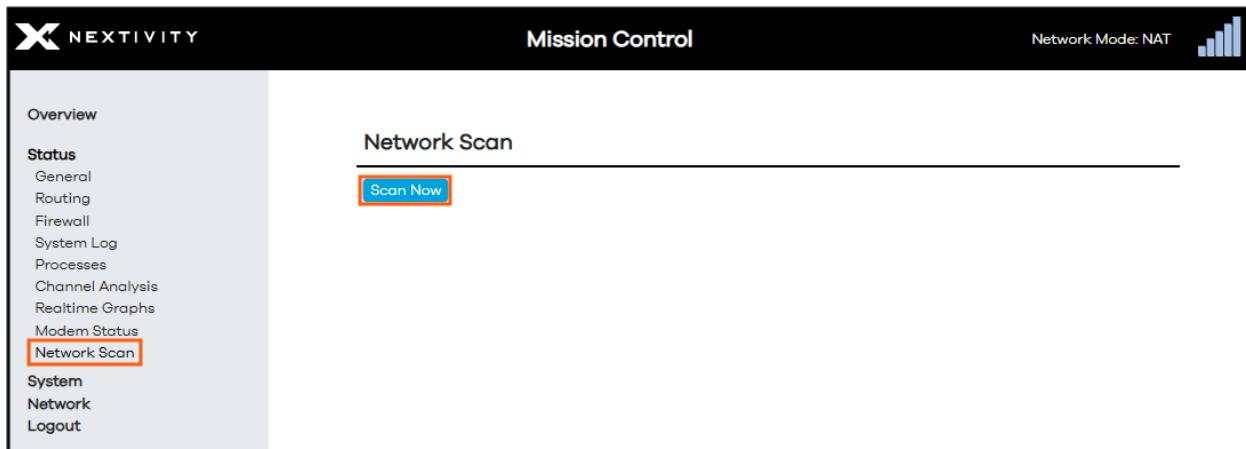


Figure 122: Network Scan

6. After the scan is complete, the results can be exported by clicking on the Export Results.

4G (LTE)											
EARFCN	RXLEV	MCC	MNC	CellID	CellStatus	TAC	PCI	RSRP	RSRQ	BW	
5330	-62	313	100	79474863	Suitable	33547	388	-91	-12	10	
700	-44	310	410	79474696	Suitable	33547	19	-75	-11	20	
5110	-60	310	410	79474703	Suitable	33547	321	-83	-6	10	
66686	-57	310	410	79474710	Suitable	33547	366	-91	-17	10	
9820	-59	310	410	79474837	Suitable	33547	275	-92	-16	10	
66986	-74	310	410	79474870	Suitable	33547	488	-98	-7	10	
66536	-59	310	260	226809090	Suitable	12101	-	-88	-9	20	
66911	-78	311	480	90670097	Suitable	13827	321	-104	-12	5	
66811	-63	311	480	90734604	Suitable	13827	283	-102	-20	15	
1000	-52	311	480	90734606	Suitable	13827	283	-85	-16	10	
68611	-67	310	260	226809405	Suitable	12101	-	-93	-12	5	
5035	-61	310	260	226809365	Suitable	12101	426	-89	-14	5	
875	-52	310	260	226809099	Suitable	12101	426	-86	-15	15	
2560	-61	311	480	13934611	Suitable	13827	283	-93	-15	10	

Figure 123: Export Results

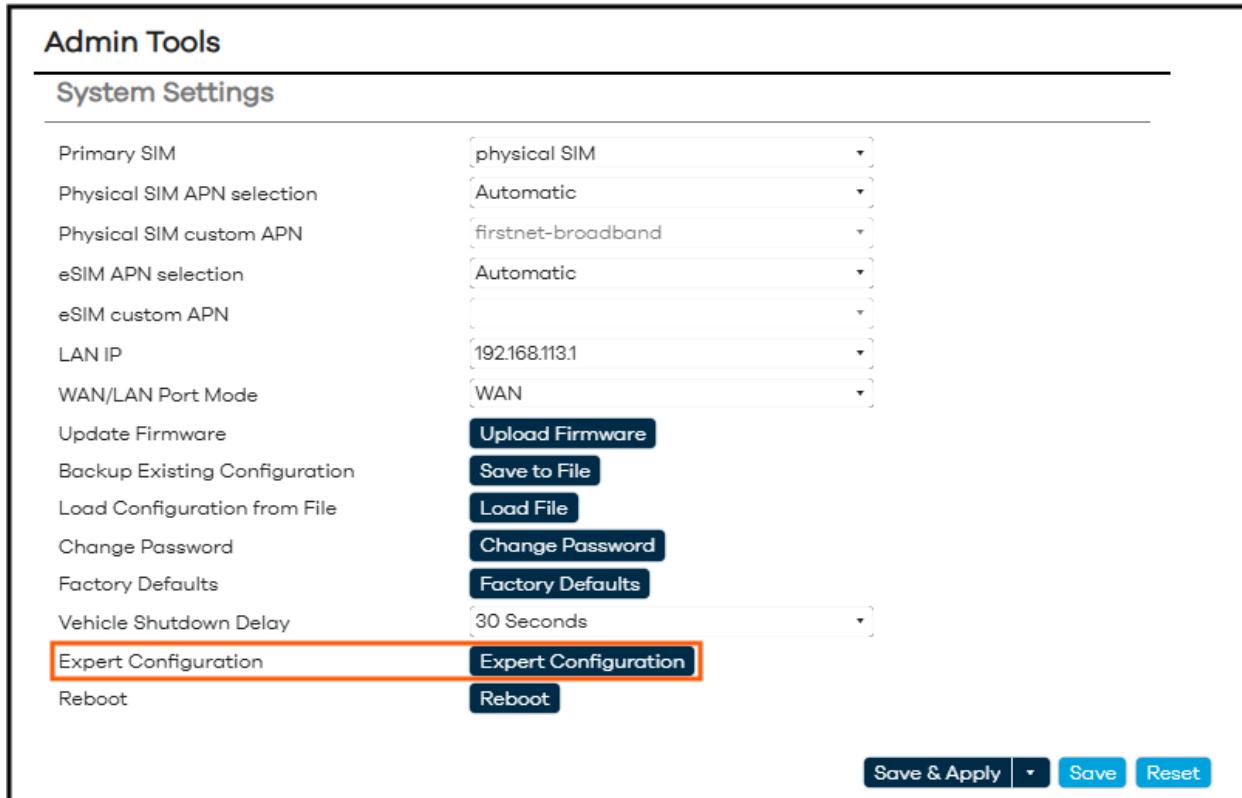
7. A csv file will be generated automatically saved to your local computer.

Figure 124: scan results csv file

3.21 IPSec VPN

The MegaFi 2 device can now serve as an endpoint for an IPSec VPN tunnel. Within Mission Control, a VPN Configuration menu page has been added within Expert Configuration that provides for VPN configuration and monitoring. To configure a VPN tunnel, do the following in Mission Control.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.



The screenshot shows the 'System Settings' page within the 'Expert Configuration' mode of the Admin Tools. The page includes fields for Primary SIM (physical SIM), Physical SIM APN selection (Automatic), Physical SIM custom APN (firstnet-broadband), eSIM APN selection (Automatic), eSIM custom APN (empty), LAN IP (192.168.113.1), WAN/LAN Port Mode (WAN), and a section for firmware management with buttons for 'Upload Firmware', 'Save to File', 'Load File', 'Change Password', and 'Factory Defaults'. The 'Vehicle Shutdown Delay' is set to '30 Seconds'. The 'Expert Configuration' button is highlighted with a red box. At the bottom, there are buttons for 'Save & Apply', 'Save', and 'Reset'.

Figure 125: System Settings – Expert Configuration

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

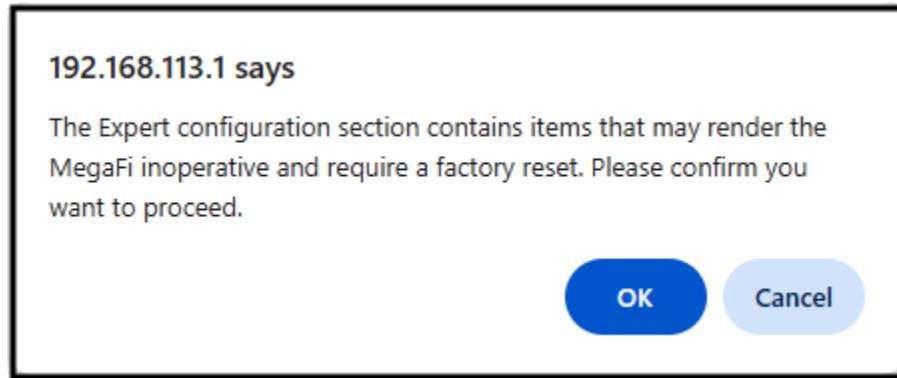


Figure 126: Confirmation to Enter Expert Configuration mode

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

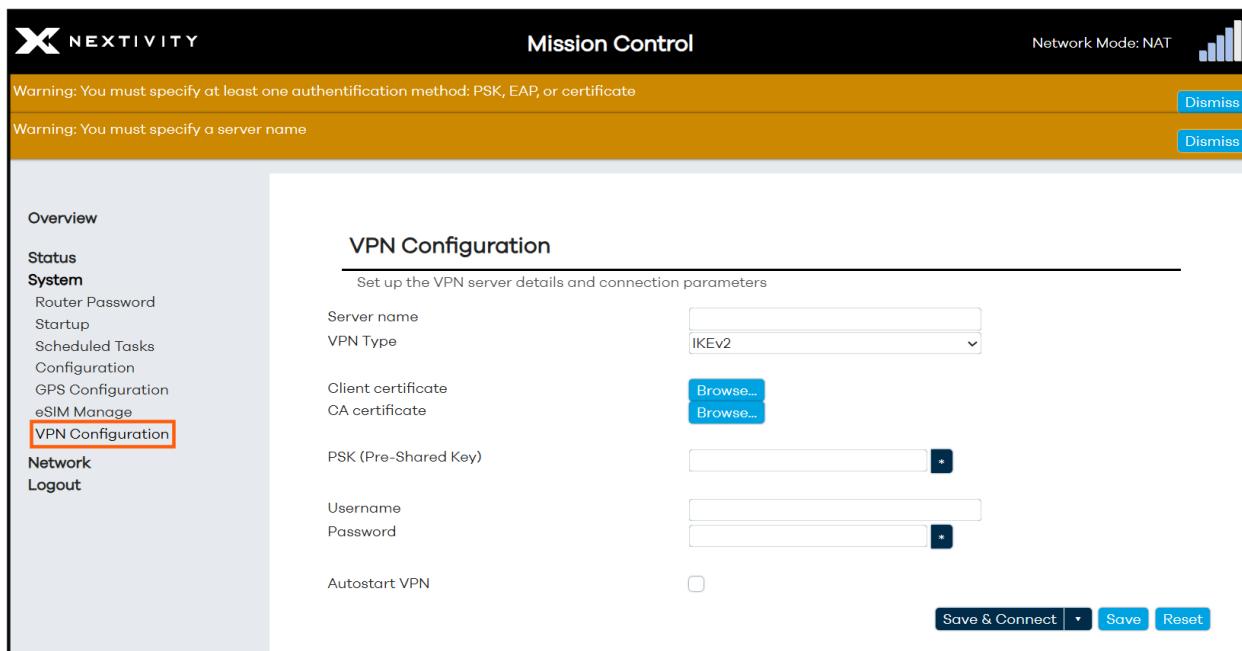


Figure 127: VPN Configuration

- ⌚ **Note:** The warnings at the top will disappear as you configure and commit the necessary parameters.
- ⌚ **Note:** Depending on the VPN Server setup, the following may or may not be needed in order to configure the VPN tunnel and both sides should match up. Relevant certificate files and parameters will be given to you by your VPN server administrator.
 - **Server name** – URL or IP address the VPN server (required)
 - **VPN Type** – choose either IKEv1 or IKEv2 from the drop-down menu (required)

- **Client certificate** – browse your local computer to find and upload the file
- **CA certificate** - browse your local computer to find and upload the file
- **PSK (Pre-Shared Key)** – enter the pre-shared key (click on the asterisk icon to the right to unhide the key)
- **Username and Password** – enter the username and password (click on the asterisk icon to the right to unhide the password)
- **Autostart VPN** – check the box if the VPN tunnel should automatically start upon reboot or restart
- **Save & Connect or Apply unchecked** – select **Save & Connect** to save the configuration and connect right away or select **Apply unchecked** once to pause full settings commit and press a second time to fully apply settings and commit from the drop-down menu
- **Save** – save current settings but do not fully apply or confirm the settings
- **Reset** – clear settings that have not been applied

5. In the example below, the VPN server administrator configured the VPN server such that the tunnel requires to be type IKEv2, both a client and CA certificates is required, as well as a pre-shared key, and user credentials.

VPN Configuration

Set up the VPN server details and connection parameters

Server name: vpn.server.url

VPN Type: IKEv2

Client certificate: /etc/swanctl/x509/client.crt

CA certificate: /etc/swanctl/x509ca/ca.crt

PSK (Pre-Shared Key): *

Username: user

Password: *

Autostart VPN:

Save & Connect | Save | Reset

Figure 128: VPN Configuration - Settings

6. If **Save & Connect** is selected, the VPN tunnel will begin to connect and the status of the connection will be shown at the top (**VPN Status** – either **Disconnected**, **Connecting to ...**).

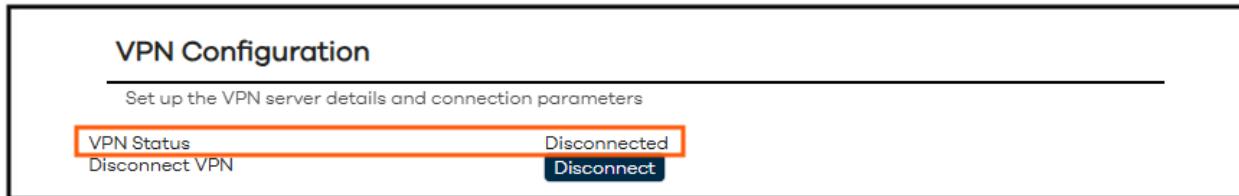


Figure 129: VPN Status - Disconnected

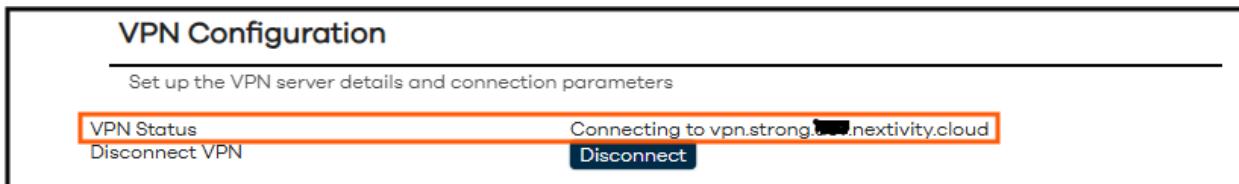


Figure 130: VPN Status – Connecting to...

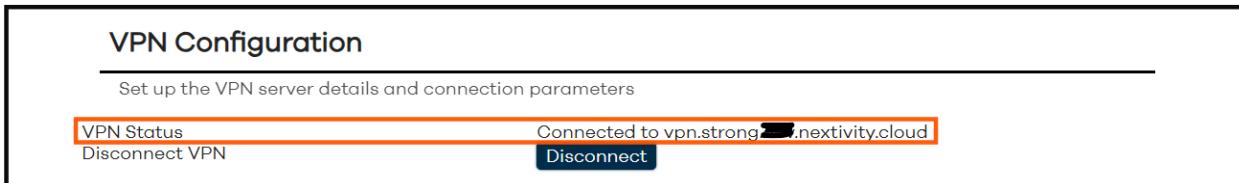


Figure 131: VPN Status – Connected

⌚ **Note:** If the connection is not successful, please contact your VPN server administrator to confirm the certificates and settings.

7. Click the **Disconnect** button to stop and disconnect the VPN tunnel.

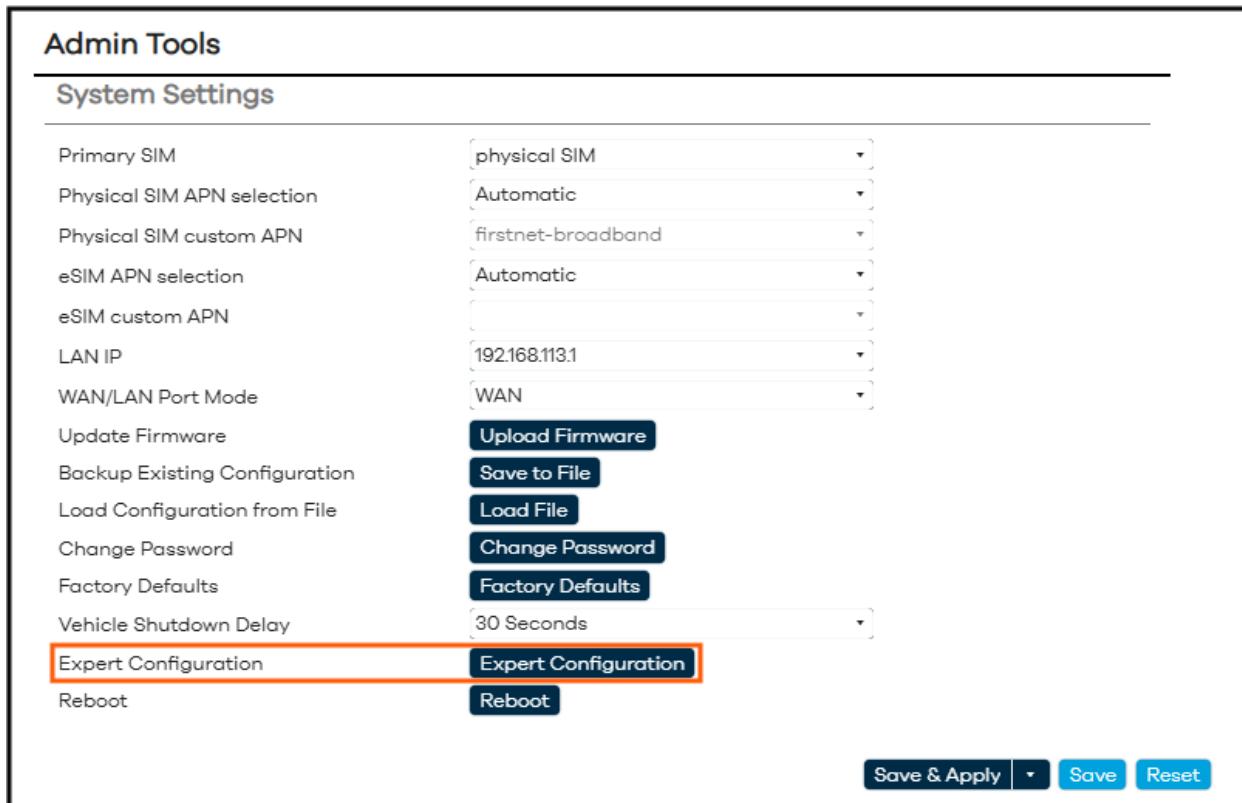


Figure 132: Disconnect VPN

3.22 Modify Hostname

By default, the MegaFi 2 device is configured with the hostname of Nextivity. To modify the hostname, do the following in Mission Control.

8. Navigate to **Overview > System Settings** under **Admin Tools**.
9. Click on the **Expert Configuration** button to enter Expert Configuration mode.



The screenshot shows the 'System Settings' page under 'Admin Tools'. The 'Expert Configuration' button is highlighted with a red box. Other buttons like 'Upload Firmware', 'Save to File', 'Load File', 'Change Password', and 'Factory Defaults' are also visible.

Setting	Value
Primary SIM	physical SIM
Physical SIM APN selection	Automatic
Physical SIM custom APN	firstnet-broadband
eSIM APN selection	Automatic
eSIM custom APN	
LAN IP	192.168.113.1
WAN/LAN Port Mode	WAN
Update Firmware	Upload Firmware
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
Reboot	Reboot

Buttons at the bottom: **Save & Apply**, **Save**, **Reset**.

Figure 133: System Settings – Expert Configuration

10. A pop-up window asks the user to confirm going into Expert Configuration mode. Click **OK** to continue.

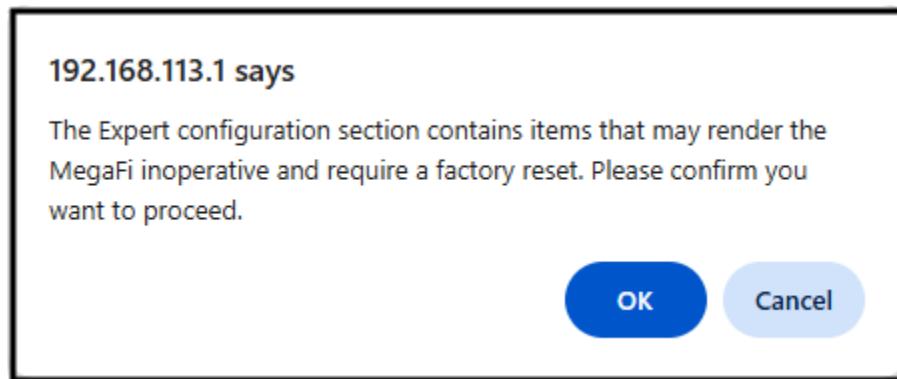


Figure 134: Confirmation to Enter Expert Configuration mode

11. The landing page is **Status > General**. The current Hostname of the device is listed at the top.

The image shows the "Status General" page of the NEXTIVITY interface. The top navigation bar includes the NEXTIVITY logo, "Mission Control", and "Network Mode: NAT" with a signal strength icon. The left sidebar has "Overview", "Status" (with "General" selected and highlighted in red), "Routing", "Firewall", "System Log", "Processes", "Channel Analysis", "Realtime Graphs", "Modem Status", and "Network Scan". The "System" section includes "Refreshing". The main content area is titled "General" and "System". The "System" section displays the following information:

Hostname	Nextivity
Model	MediaTek MT7981 RFB
Architecture	ARMv8 Processor rev 4
Target Platform	mediatek/filogic
Firmware Version	OpenWrt 23.05.5 r24106-10cc5fcd00 / SHIELD MegaFi 2 v3.5.1.11
Kernel Version	5.15.167
Local Time	2026-01-07 19:27:35
Uptime	1h 38m 58s
Load Average	0.26, 0.22, 0.25

Below this is a "Memory" section with three status bars:

- Total Available: 76.60 MIB / 235.02 MIB (32%)
- Used: 186.17 MIB / 235.02 MIB (79%)
- Cached: 67.20 MIB / 235.02 MIB (28%)

Figure 135: Status General - Hostname of the device

12. Now navigate to **System > Configuration**.

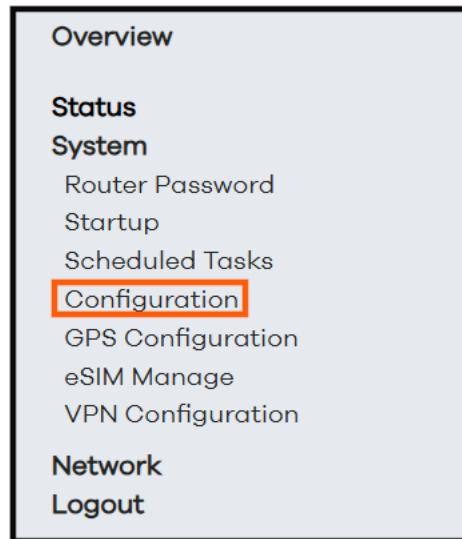


Figure 136: Navigation pane showing options available in Expert mode – Configuration

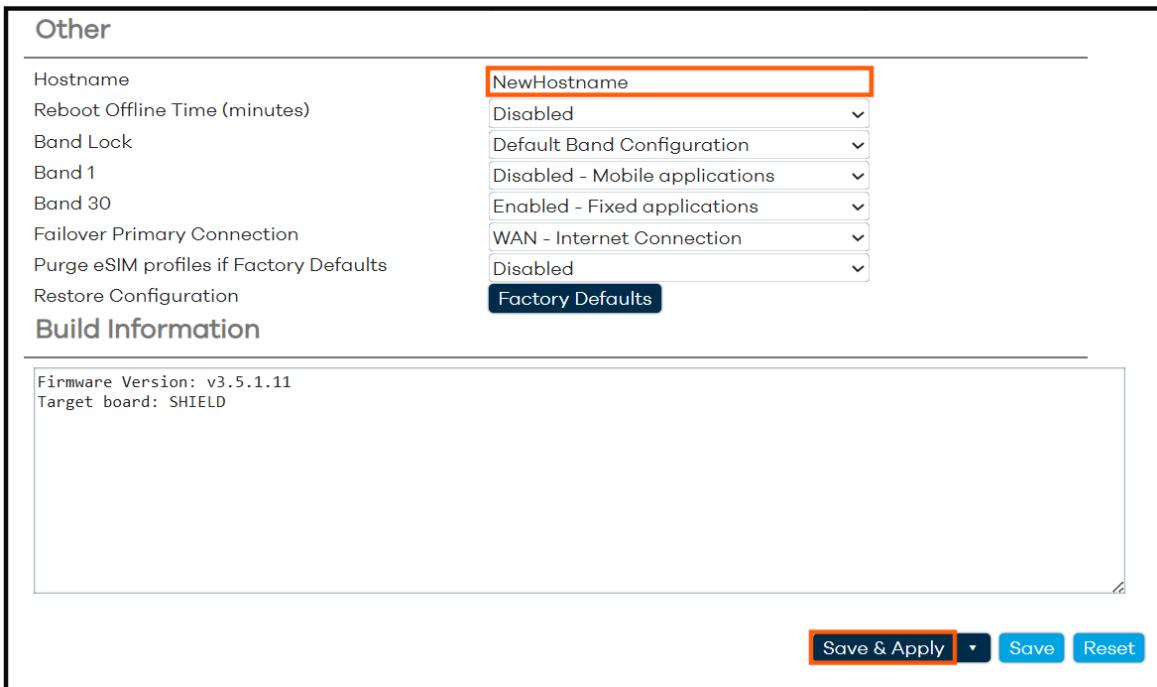
13. Towards the bottom of this page, in the **Other** section, the current **Hostname** configured is shown.

The image shows the 'Mission Control' interface with the following configuration details:

- Overview**
- System**
 - Router Password
 - Startup
 - Scheduled Tasks
 - Configuration**
 - GPS Configuration
 - eSIM Manage
 - VPN Configuration
- Network**
- Logout**
- Mission Control** (top right)
- Network Mode: NAT** (top right)
- Configuration** (highlighted)
- Cloud**
 - UUID: 59CDA87F-99D4-48BD-81AA-BE27949A3
 - Cloud Poll URL: ei.nextivityinc.net
 - Cloud Poll Period (seconds): 60
 - Cloud Status URL: Connected (1/7/2026, 11:41:38 AM)
- Logging**
 - Logging Enabled: Enabled
 - Push to Cloud: Enabled
 - Push to Cloud Period (seconds): 60
 - System Poll Period (seconds): 15
 - Show in Local UI: Local UI Enabled
- Networking**
 - Passthrough via NAT (changing causes reboot): NAT Mode
 - LAN IP Address: 192.168.1.1
 - Client Isolation: Enabled
- API**
 - MegaFi Reboot API Enabled: Disabled
 - Modem Power Cycle API Enabled: Disabled
 - Modem Status API Enabled: Disabled
- LCD Configuration**
 - Screen Orientation: Portrait
 - Detail Level: Full
 - Turn off screen after (seconds): 600
 - Switch screen information (seconds): 15
 - Show Mission Control Password on the Display: Disabled
- Other**
 - Hostname**: Nextivity (highlighted with a red box)
 - Reboot Offline Time (minutes): Disabled
 - Band Lock: Default Band Configuration
 - Band 1: Disabled - Mobile applications
 - Band 30: Enabled - Fixed applications
 - Failover Primary Connection: WAN - Internet Connection
 - Purge eSIM profiles if Factory Defaults: Disabled
 - Restore Configuration: Factory Defaults

Figure 137: Other – Hostname

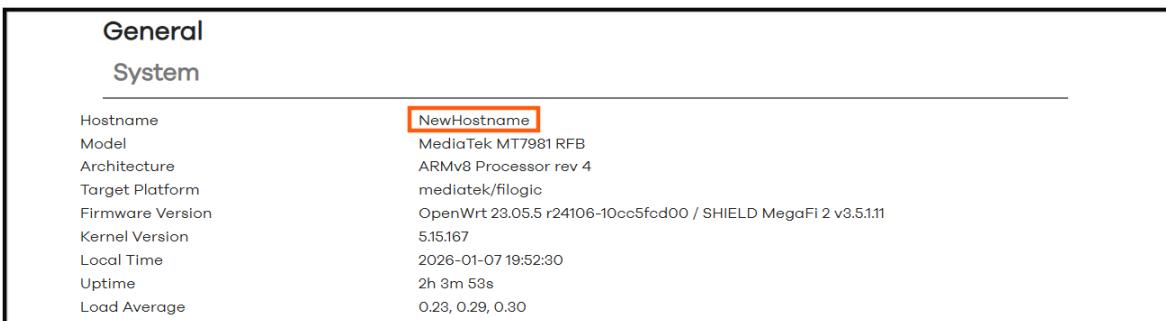
14. To change the **Hostname** of the device, type over the current hostname and click on **Save & Apply** at the bottom.



The screenshot shows the 'Other' configuration page. The 'Hostname' field is highlighted with a red box. The dropdown menu for 'Hostname' contains the following options: Disabled, Default Band Configuration, Disabled - Mobile applications, Enabled - Fixed applications, WAN - Internet Connection, and Disabled. A 'Factory Defaults' button is also visible. Below the configuration section, there is a 'Build Information' box containing 'Firmware Version: v3.5.1.11' and 'Target board: SHIELD'. At the bottom right are 'Save & Apply', 'Save', and 'Reset' buttons.

Figure 138: Other – New Hostname

15. Navigate back to **Status > General** to verify the new hostname.



The screenshot shows the 'Status General' page under the 'General' tab. The 'System' section is selected. The 'Hostname' field is highlighted with a red box. The table below shows the following system information:

Hostname	NewHostname
Model	MediaTek MT7981 RFB
Architecture	ARMv8 Processor rev 4
Target Platform	mediatek/filogic
Firmware Version	OpenWrt 23.05.5 r24106-10cc5fd00 / SHIELD MegaFi 2 v3.5.1.11
Kernel Version	5.15.167
Local Time	2026-01-07 19:52:30
Uptime	2h 3m 53s
Load Average	0.23, 0.29, 0.30

Figure 139: Status General – New Hostname

3.23 eSIM Configuration

Starting with firmware release version 3.6.0, eSIM will allow for dual network registration for better connectivity and reliability. A WAN source and a valid eSIM activation code will be needed to proceed. To enable this feature, do the following in Mission Control.

1. A WAN source connection will be required for eSIM configuration. If there is no physical connection on the WAN port, there will be no IP address assigned, and the **RX** and **TX** packet counters will not be actively incrementing or all zeroes as seen in Mission Control under the **Overview > Interfaces** section.

Modem Status								
Connection Mode	5G+							
Home Network	FirstNet							
Current SIM in use	physical SIM							
Current APN in use	firstnet-broadband							
	LTE		5G					
Connection Status	Connected		Connected					
Band	14		77					
CID (Serving Cell ID)	79474863		79474863					
PCI (Physical Cell ID)	388		85					
Bandwidth	10		80					
RSRP	-91		-112					
RSRQ	-11		-18					
RSSI	-65		-93					
TX Power	20		2					
MIMO status	1x1-SISO		1x1-SISO					
Networking								
DHCP Leases								
Active DHCPv4 Leases								
Hostname	IPv4 address	MAC address	Lease time remaining					
LGgram	192.168.113.173	00:24:9B:2D:48:17	11h 59m 18s					
LPORCHAS-LT	192.168.113.140	BC:F4:D4:6F:D8:C1	11h 54m 41s					
Active DHCPv6 Leases								
Host	IPv6 address	DUID	Lease time remaining					
There are no active leases								
Interfaces								
Type	MAC	RX	TX	IPv4	IPv6			
GUEST		0 B (0 Pkts.)	0 B (0 Pkts.)					
LAN	34:BA:9A:C3:5D:D0	692.52 KB (4388 Pkts.)	5.36 MB (3954 Pkts.)	192.168.113.1/24	fdca:cd5b:b5b2::1/64			
WAN	34:BA:9A:C3:5D:D3	0 B (0 Pkts.)	0 B (0 Pkts.)					
WAN6	34:BA:9A:C3:5D:D3	0 B (0 Pkts.)	0 B (0 Pkts.)					
WWAN	2E:B1:25:77:E6:02	549.27 KB (2139 Pkts.)	345.54 KB (2581 Pkts.)	10.22.119.146/30	2600:382:3916:6f4a:68f2:bdad:b4e2:cd85/64			

Figure 140: Interfaces – WAN Packet Counters at zero or not incrementing

2. Start by connecting a WAN source to the MegaFi 2 WAN/LAN2 port. This is required in order for the eSIM to download its profile. This will not work over a cellular connection (WWAN). Establishing a physical WAN connection will force a failover from WWAN to WAN, unless the device is already set to prefer the WAN interface as its primary connection. You will notice that packets will begin to increase along with an assigned IP address on the WAN interface.

Modem Status								
Connection Mode	5G							
Home Network	FirstNet							
Current SIM in use	physical SIM							
Current APN in use	firstnet-broadband							
	LTE	5G						
Connection Status	Connected	Not connected						
Band	14							
CID (Serving Cell ID)	79474863							
PCI (Physical Cell ID)	388							
Bandwidth	10							
RSRP	-90							
RSRQ	-10							
RSSI	-63							
TX Power								
MIMO status	1x1-SISO	not_attach						
Networking								
DHCP Leases								
Active DHCPv4 Leases								
Hostname	IPv4 address	MAC address	Lease time remaining					
LGgram	192.168.113.173	00:24:9B:2D:48:17	11h 52m 23s					
LPORCHAS-LT	192.168.113.140	BC:F4:D4:6F:D8:C1	11h 46m 47s					
Active DHCPv6 Leases								
Host	IPv6 address	DUID	Lease time remaining					
There are no active leases								
Interfaces								
Type	MAC	RX	TX	IPv4	IPv6			
GUEST		0 B (0 Pkts.)	0 B (0 Pkts.)					
LAN	34:BA:9A:C3:5D:D0	1.33 MB (7667 Pkts.)	10.89 MB (8216 Pkts.)	192.168.113.1/24	fdca:cd5b:b5b2:1/64			
WAN	34:BA:9A:C3:5D:D3	7.13 MB (49945 Pkts.)	447.12 KB (3956 Pkts.)	172.16.8.168/22				
WAN6	34:BA:9A:C3:5D:D3	7.13 MB (49945 Pkts.)	447.12 KB (3956 Pkts.)					
WWAN	2E:B1:25:77:E6:02	625.85 KB (2733 Pkts.)	1.30 MB (12355 Pkts.)	10.22.119.146/30	2600:382:3916:6f4a:68f2:bdad:b4e2:cd85/64			

Figure 141: Interfaces – WAN Packet Counters incrementing with assigned IP address

3. In Mission Control, navigate to **Overview > System Settings** under **Admin Tools**.
4. Click on the **Expert Configuration** button to enter Expert Configuration mode.

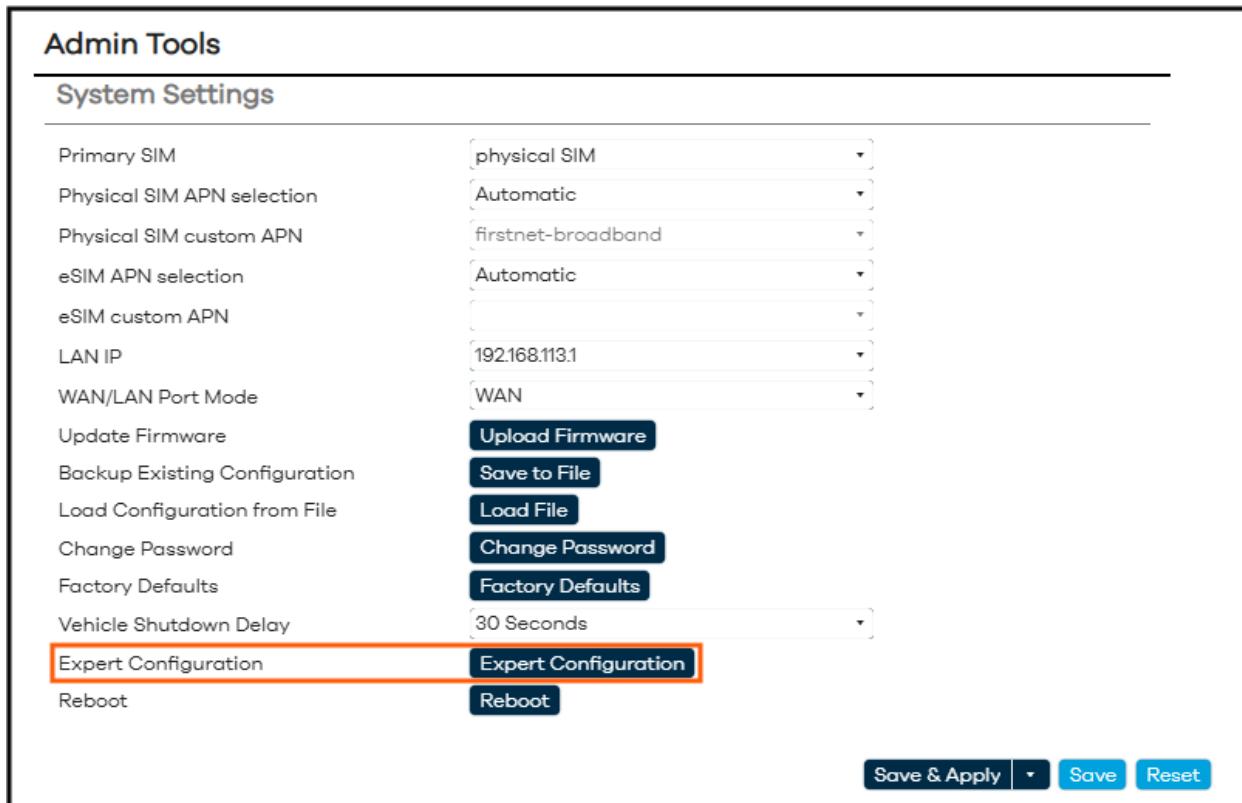


Figure 142: System Settings – Expert Configuration

5. A pop-up window asks the user to confirm going into Expert Configuration mode. Click **OK** to continue.

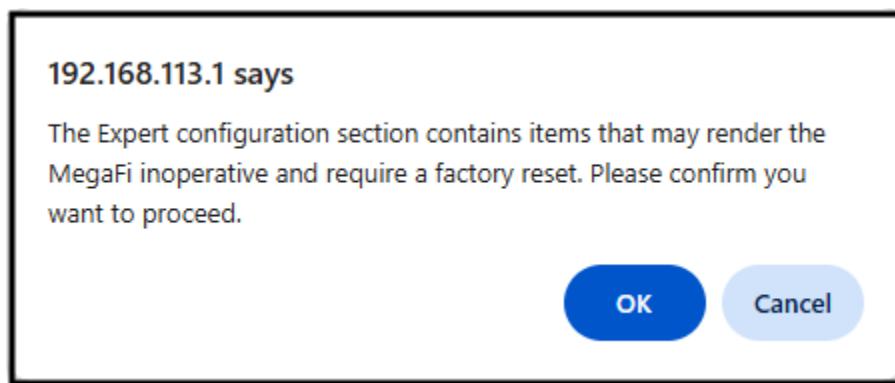


Figure 143: Confirmation to Enter Expert Configuration mode

6. The left-pane menu exposes pages only available in Expert Configuration mode. Navigate to **System > eSIM Manage**.

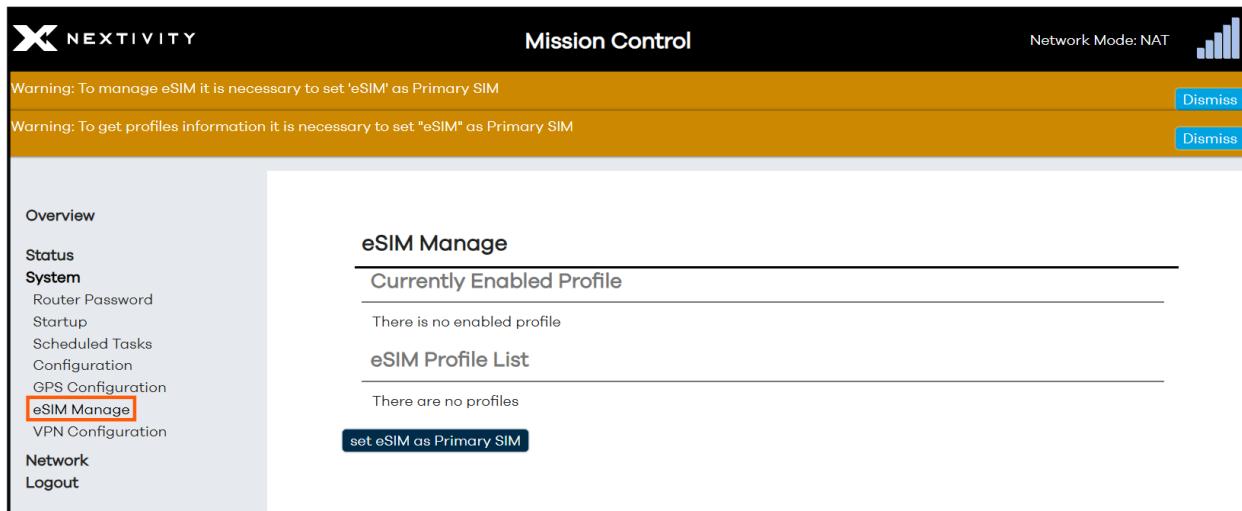


Figure 144: eSIM Manage

⌚ **Note:** The warnings at the top will disappear as you configure and commit the necessary parameters.

7. Click on the **set eSIM as Primary SIM** button and wait about a minute to allow for the device to switch to eSIM.

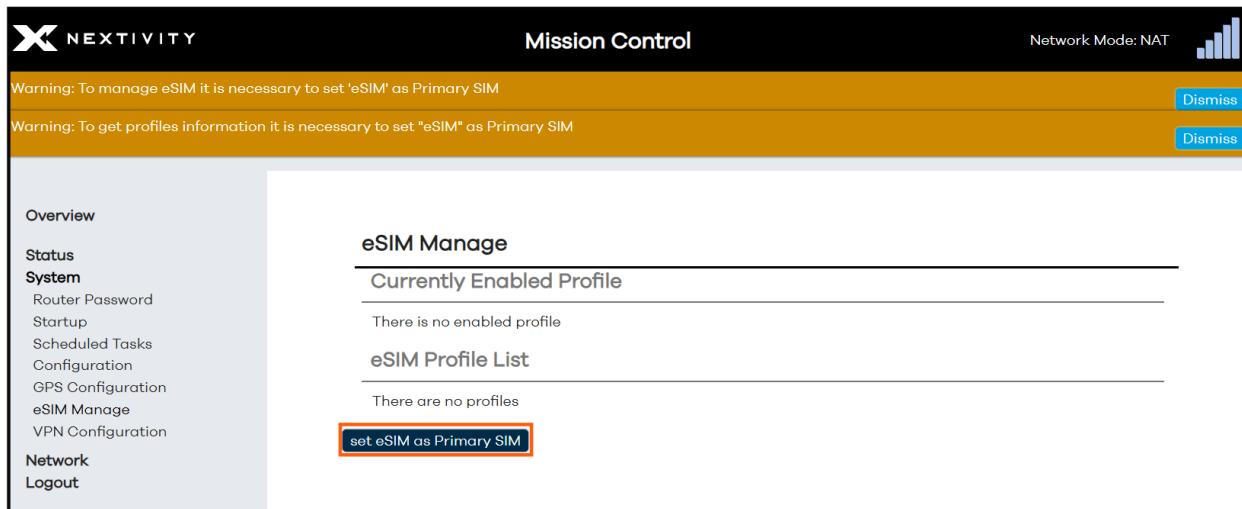


Figure 145: eSIM Manage – set eSIM as Primary SIM

8. After the short wait, you will see that there is no enabled profile, an internal eSIM Profile listed with ID = 0, and a button at the bottom to **Download eSIM profile**.

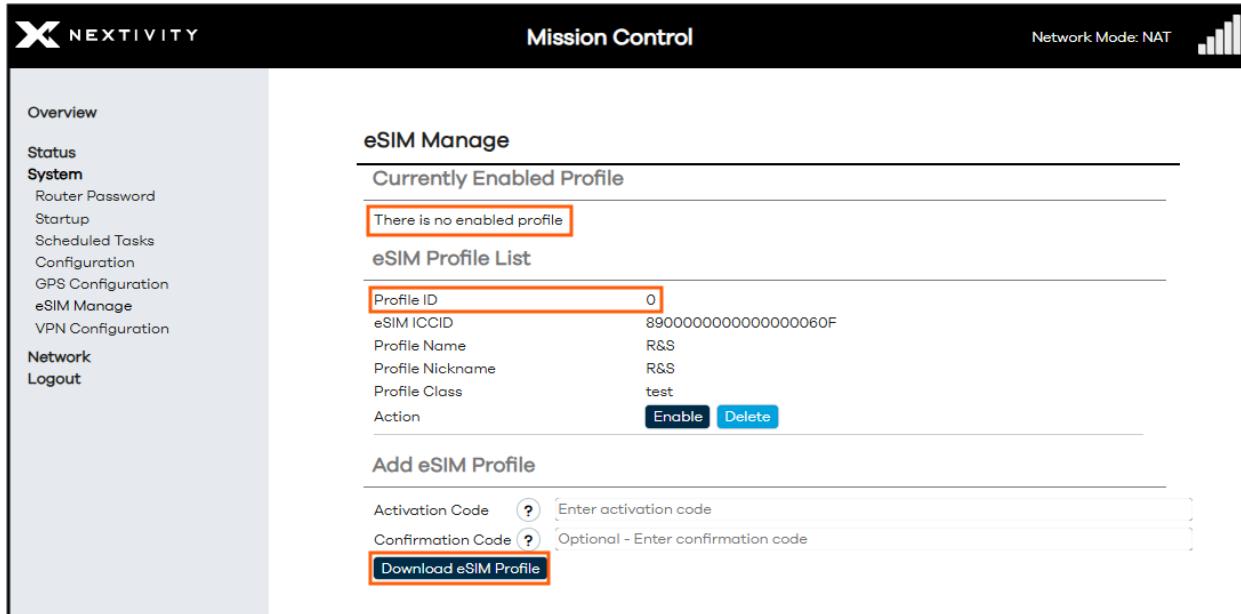


Figure 146: eSIM Manage – no enabled profile

- ⦿ **Note:** The cellular signal strength bars on the top right corner are gone, this is normal.

9. Enter your eSIM **Activation Code** and **Confirmation Code** (optional), then click on the **Download eSIM profile** button.

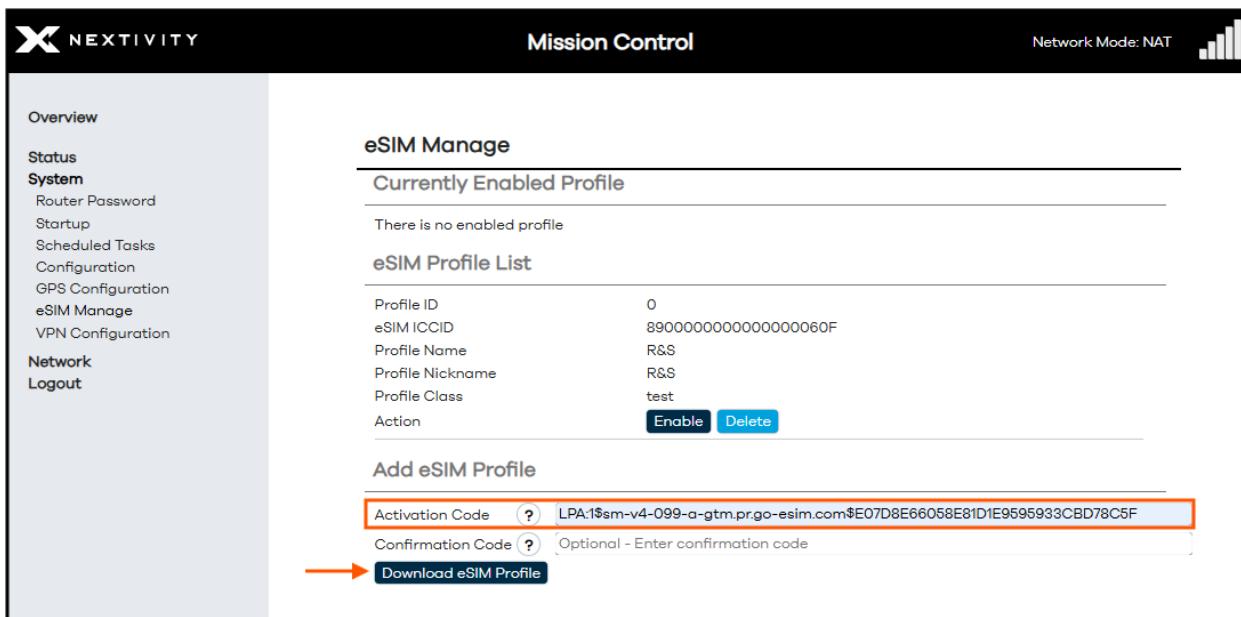


Figure 147: eSIM Manage – enter eSIM codes and download eSIM profile

- ⦿ **Note:** You may have received some instructions from the eSIM vendor. Please read and follow the instructions before proceeding with this step.

10. The eSIM profile begins to download and may take over 30 seconds to complete. Do not perform any other actions during this time.

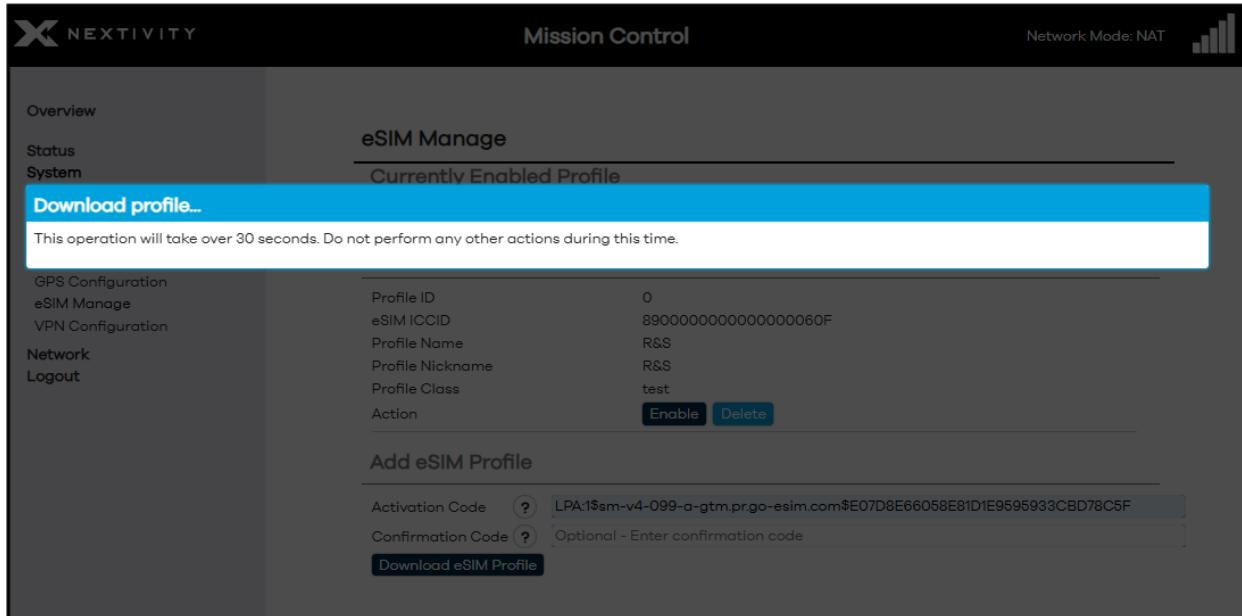


Figure 148: eSIM Manage – Downloading profile...

11. After the eSIM profile completes downloading, an informational message lets you know the **modem is rebooting... please wait**.

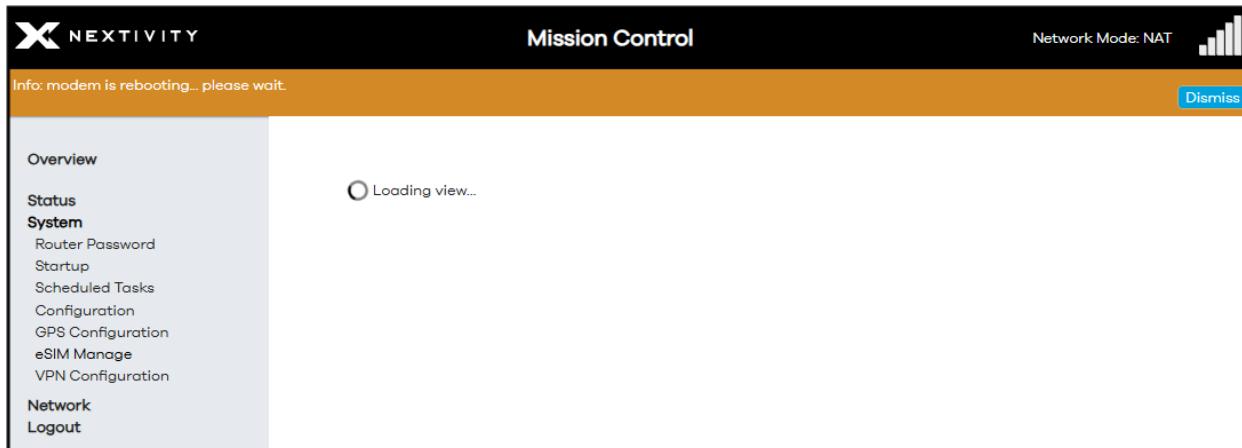


Figure 149: eSIM Manage – Info: modem is rebooting... please wait

After the modem completely reboots, the **Profile ID 1** should have the correct **eSIM ICCID** that pertains to the eSIM, and **Profile Class is operational**.

eSIM Manage

Currently Enabled Profile

There is no enabled profile

eSIM Profile List

Profile ID	0
eSIM ICCID	89000000000000000000000000000000
Profile Name	R&S
Profile Nickname	R&S
Profile Class	test
Action	Enable Delete
Profile ID	1
eSIM ICCID	89017901028902618411
Profile Name	89017901028902618411
Profile Nickname	operational
Profile Class	operational
Action	Enable Delete

Add eSIM Profile

Activation Code Enter activation code

Confirmation Code Optional - Enter confirmation code

Download eSIM Profile

Figure 150: eSIM Manage – Completed eSIM Profile and operational

12. Next to **Action**, click on the **Enable** button for **Profile ID 1** for your newly downloaded eSIM profile you wish to use.

eSIM Manage

Currently Enabled Profile

There is no enabled profile

eSIM Profile List

Profile ID	0
eSIM ICCID	89000000000000000000000000000000
Profile Name	R&S
Profile Nickname	R&S
Profile Class	test
Action	Enable Delete
Profile ID	1
eSIM ICCID	89017901028902618411
Profile Name	89017901028902618411
Profile Nickname	operational
Profile Class	operational
Action	Enable Delete

Add eSIM Profile

Activation Code Enter activation code

Confirmation Code Optional - Enter confirmation code

Download eSIM Profile

Figure 151: eSIM Manage – Enable eSIM

13. Wait about 10 seconds for the confirmation. Do not perform any other actions during this time.

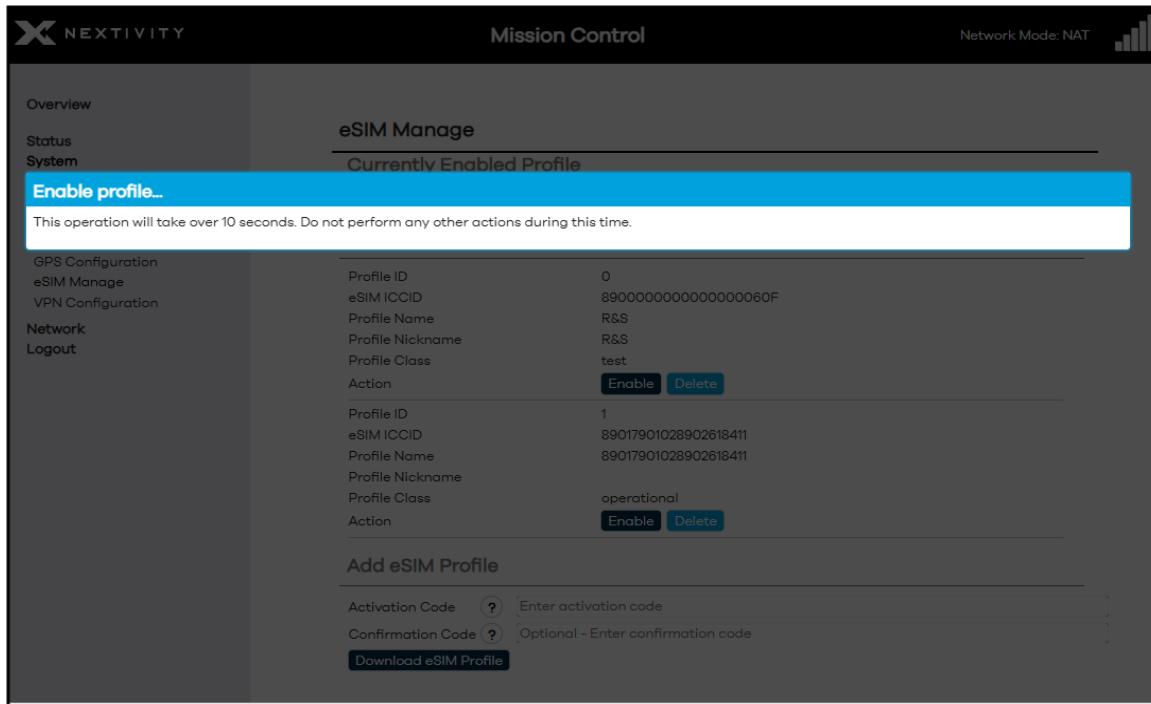


Figure 152: eSIM Manage – Wait for eSIM Profile to enable

14. After the wait, the **Currently Enabled Profile** reflects the eSIM profile in use. After about another minute, the cellular strength signal bars will come back, and the 'e' symbol on the LCD display is illuminated, indicating the device is using eSIM for connectivity.

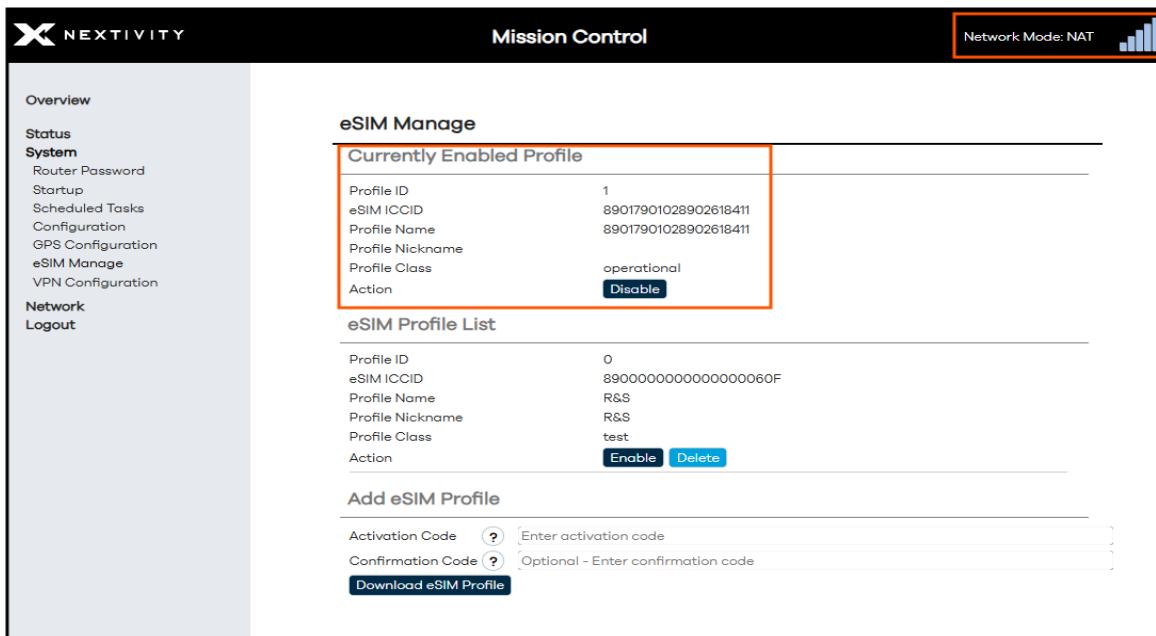


Figure 153: eSIM Manage – eSIM Profile in use

15. This process automatically configures the **eSIM custom APN** as shown in **Overview > Admin Tools** section and has made the eSIM the primary SIM over the physical SIM.

Admin Tools

System Settings

Primary SIM	eSIM
Physical SIM APN selection	Automatic
Physical SIM custom APN	firstnet-broadband
eSIM APN selection	Automatic
eSIM custom APN	internet
LAN IP	192.168.113.1
WAN/LAN Port Mode	WAN
Update Firmware	Upload Firmware
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
Reboot	Reboot

Save & Apply | Save | Reset

Figure 154: Admin Tools – eSIM custom APN

16. If no longer needed, the WAN source can be disconnected.

17. Above the **Admin Tools** section under **Overview > Modem Status**, verify **Current SIM in use**.

Mission Control

Network Mode: NAT

Overview

Device

Model	SHIELD MegaFi 2
Serial Number	250601000632
IMEI	359172391063678
Phone Number	858.310.7166
ICCID (SIM)	89017901028902618411
ESIMID	89049032000001000000212986270921
Uptime	0h 50m 16s
Cloud Connection Status	Connected (10/28/2025, 22:07:47 PM)
TX Bytes (since last power cycle)	13.03 MB (32231 Pkts.)
RX Bytes (since last power cycle)	92.90 MB (75160 Pkts.)
Memory Used	76.93 MIB / 235.02 MIB (32%)
Location (Lat,Lon)	0.000000,0.000000

Modem Status

Connection Mode	5G
Home Network	ATT
Current SIM in use	eSIM
Current APN in use	internet

Connection Status	LTE	5G
Band	Connected	Not connected
CID (Serving Cell ID)	14	
PCI (Physical Cell ID)	79474863	
Bandwidth	388	
RSRP	10	
RSRQ	-91	
RSSI	-9	
TX Power	-66	
MIMO status	9	
	1x1-SISO	not_attach

Figure 155: Modem Status – Current SIM in use

18. Further down **Overview > Interfaces** section, the IP address for the eSIM will be displayed under the **IPv4 WWAN** interface.

Interfaces					
Type	MAC	RX	TX	IPv4	IPv6
GUEST		0 B (0 Pkts.)	0 B (0 Pkts.)		
LAN	34:BA:9A:C3:5D:D0	41.17 MB (13917 Pkts.)	29.25 MB (19163 Pkts.)	192.168.113.1/24	fdca:cd5b:b5b2::1/64
WAN	34:BA:9A:C3:5D:D3	46.11 MB (168453 Pkts.)	4.65 MB (17323 Pkts.)		
WAN6	34:BA:9A:C3:5D:D3	46.11 MB (168453 Pkts.)	4.65 MB (17323 Pkts.)		
WWAN	BE:0E:AD:BD:EB:01	146.04 KB (792 Pkts.)	234.17 KB (1632 Pkts.)	100.76.115.193/30	

Active Connections 

Figure 156: Interfaces – WWAN IP address

19. If you prefer to make the physical SIM the primary SIM and the eSIM the standby SIM, do the following in Mission Control via **Overview > Admin Tools**. Go to the **Primary SIM** drop-down menu and select **physical SIM** from the list.

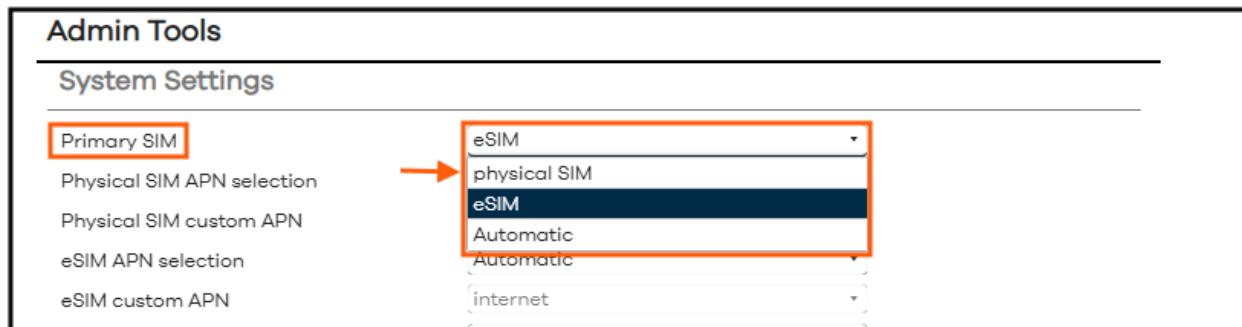


Figure 157: Admin Tools – Primary SIM

20. Click on **Save & Apply** at the bottom. The LCD display will indicate that the physical SIM is now active with a 'p' on the top right corner, but it may take Mission Control a few minutes to catch up and properly display this. After a few minutes, check in **Overview > Modem Status** and validate which **Current SIM in use**.

Modem Status	
Connection Mode	5G+
Home Network	FirstNet
Current SIM in use	physical SIM
Current APN in use	firstnet-broadband

Figure 158: Modem Status – Current SIM in use

3.24 Firewall

While in NAT mode, the Firewall of the MegaFi 2 device is active and blocks unsolicited incoming connections from the WWAN/WAN interfaces unless you explicitly allow them.

There are two methods in which you can allow incoming connections through the Firewall, either by a **Port Forward** or a **Traffic Rule**. Depending on the need, a Port Forward allows specific traffic from the WWAN/WAN to LAN and translate it to an internal host. A Traffic Rule allows, blocks, or redirects traffic without doing NAT. Do the following in Mission Control to create a Port Forward or Traffic Rule.

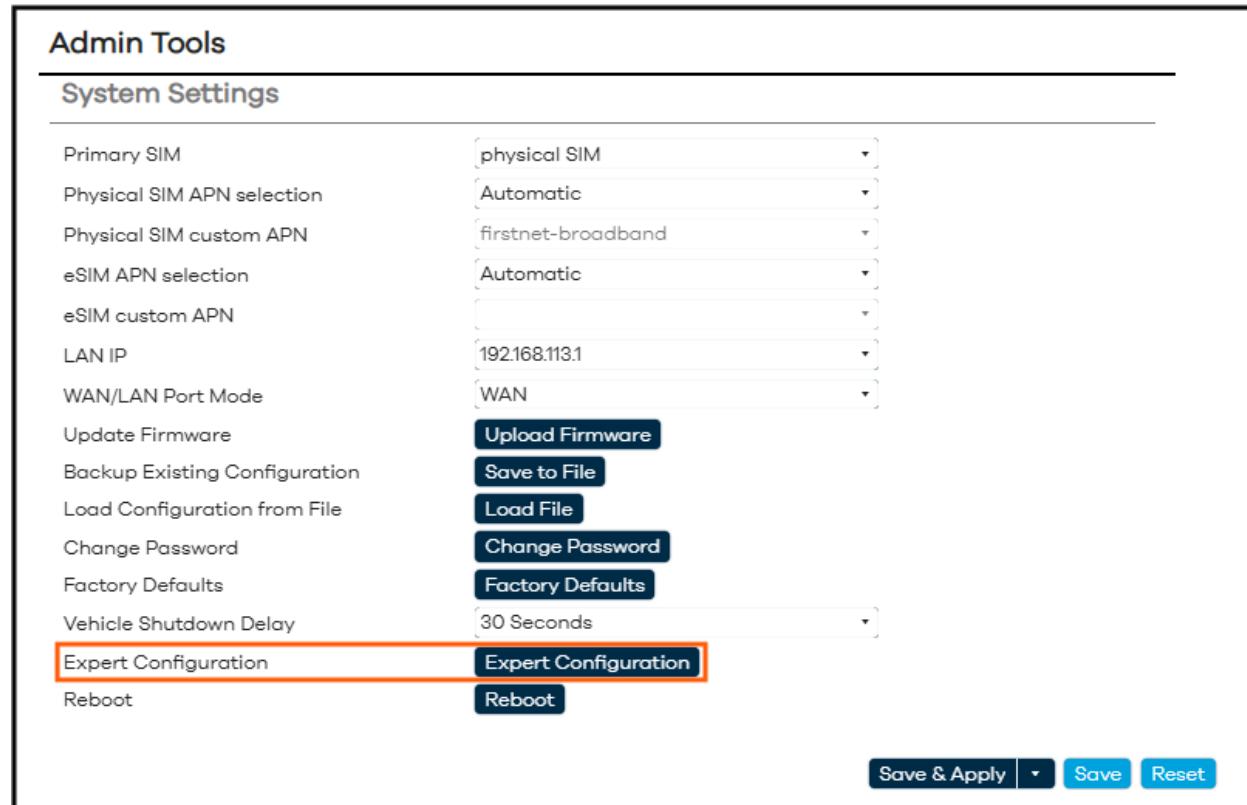
The typical caveats for implementing these rules are the following:

- The MegaFi 2 device is in NAT mode
- The MegaFi 2 device has a SIM card with a static and or public IP address

3.24.1 Port Forward

A Port Forward creates a NAT rule that takes traffic arriving on the WAN interface and forwards it to a device inside your LAN. To create a Port Forward rule, do the following in Mission Control.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.



The screenshot shows the 'Admin Tools' interface with the 'System Settings' tab selected. The 'Expert Configuration' button is highlighted with a red box. Other visible buttons include 'Upload Firmware', 'Save to File', 'Load File', 'Change Password', 'Factory Defaults', and 'Reboot'. At the bottom, there are 'Save & Apply' and 'Save' buttons.

Setting	Value
Primary SIM	physical SIM
Physical SIM APN selection	Automatic
Physical SIM custom APN	firstnet-broadband
eSIM APN selection	Automatic
eSIM custom APN	
LAN IP	192.168.113.1
WAN/LAN Port Mode	WAN
Update Firmware	Upload Firmware
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
Reboot	Reboot

Figure 159: System Settings – Expert Configuration

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

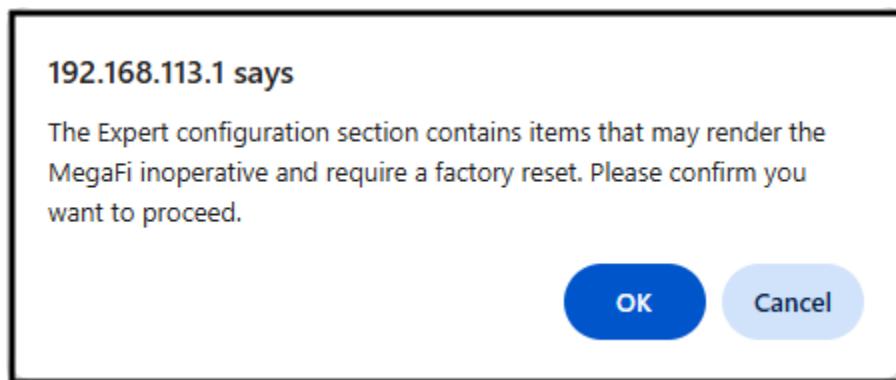


Figure 160: Confirmation to Enter Expert Configuration mode

4. Navigate to **Network > Firewall**. The landing page is General Settings. Select **Port Forwards** at the top.

Zone → Forwardings	Input	Output	Forward	Masquerading	Actions
lan → wan svvpn	accept	accept	accept	<input type="checkbox"/>	Edit Delete
wan → ACCEPT	accept	accept	accept	<input type="checkbox"/>	Edit Delete
guest → wan	reject	accept	reject	<input type="checkbox"/>	Edit Delete
svvpn → lan	accept	accept	accept	<input type="checkbox"/>	Edit Delete

Figure 161: Firewall – General Settings

5. Click the Add button to add a Port Forward rule.

General Settings Port Forwards Traffic Rules NAT Rules IP Sets

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Action	Enable
	<i>This section contains no values yet</i>		

Add

Save & Apply ▾ Save Reset

Figure 162: Firewall – Port Forwards Add

6. Within General Settings of the Port Forwards pop-up window the following options are available:
 - **Name** – name of the Port Forward rule
 - **Restrict to address family** – options are **automatic** (default), **IPv4 only**, **IPv6 only**
 - **Protocol** – options are **Any**, **TCP**, **UDP**, **ICMP**, and **custom**. Both **TCP** and **UDP** are selected by default
 - **Source zone** – options are **guest**, **lan**, **swvpn**, **wan** (wan, wan6, wwan); **wan** is selected by default
 - **External port** – enter the port number or range of port numbers expected
 - **Destination zone** - options are **unspecified**, **guest**, **lan** (default), **swvpn**, **wan** (wan, wan6, wwan)
 - **Internal IP address** – select **any** or the desired destination device by internal IP address, MAC address or hostname from the drop-down menu. There is an option to enter a custom value as well.
 - **Internal port** – enter the expected port number or port number range or redirect to a different port number on the internal host

Firewall - Port Forwards - Unnamed forward

[General Settings](#) [Advanced Settings](#)

Name	Unnamed forward	
Restrict to address family	automatic	
Protocol	TCP UDP	
Source zone	wan wan: wan6: wwan:	
External port	Match incoming traffic directed at the given destination port or port range on this host	
Destination zone	lan lan: <input checked="" type="checkbox"/>	
Internal IP address	any	
Internal port	any	Redirect matched incoming traffic to the specified internal host
	any	Redirect matched incoming traffic to the given port on the internal host

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

Figure 163: Firewall – Port Forwards General Settings

7. In the following example, we created a Port Forward rule to allow an incoming RDP (Remote Desktop Protocol) connection, which uses the TCP protocol, to a specific PC computer on the LAN using the typical RDP port of 3389. We match the external and internal port to 3389 as it will not change.

Firewall - Port Forwards - Unnamed forward

[General Settings](#) [Advanced Settings](#)

Name	Allow-RDP-Hostname	
Restrict to address family	automatic	
Protocol	TCP	
Source zone	wan wan: wan6: wwan:	
External port	3389	Match incoming traffic directed at the given destination port or port range on this host
Destination zone	lan lan: <input checked="" type="checkbox"/>	
Internal IP address	192.168.113.134 (LPORCHAS-LT.lan)	
Internal port	3389	Redirect matched incoming traffic to the specified internal host
	3389	Redirect matched incoming traffic to the given port on the internal host

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

Figure 164: Firewall – Port Forwards RDP example

8. Click on **Save** then **Save & Apply** on the main Firewall - Port Forwards page.
9. A remote user should now be able to successfully connect to the local PC computer via an RDP connection. In the RDP connection image example below, the user is entering the public-static IP address of the MegaFi 2 device which comes from the SIM card.

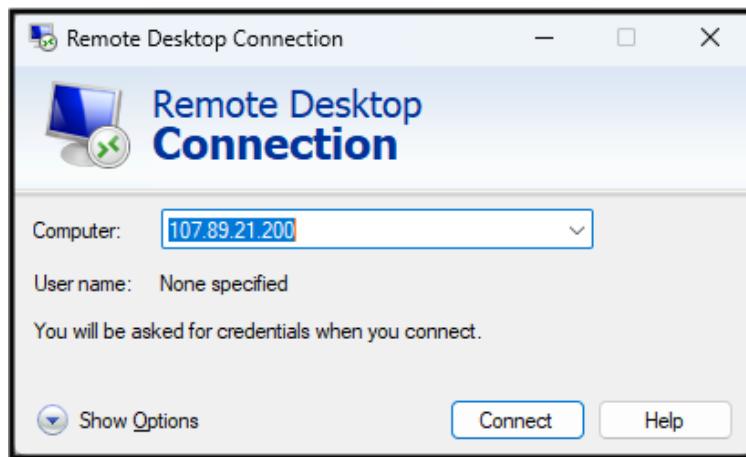
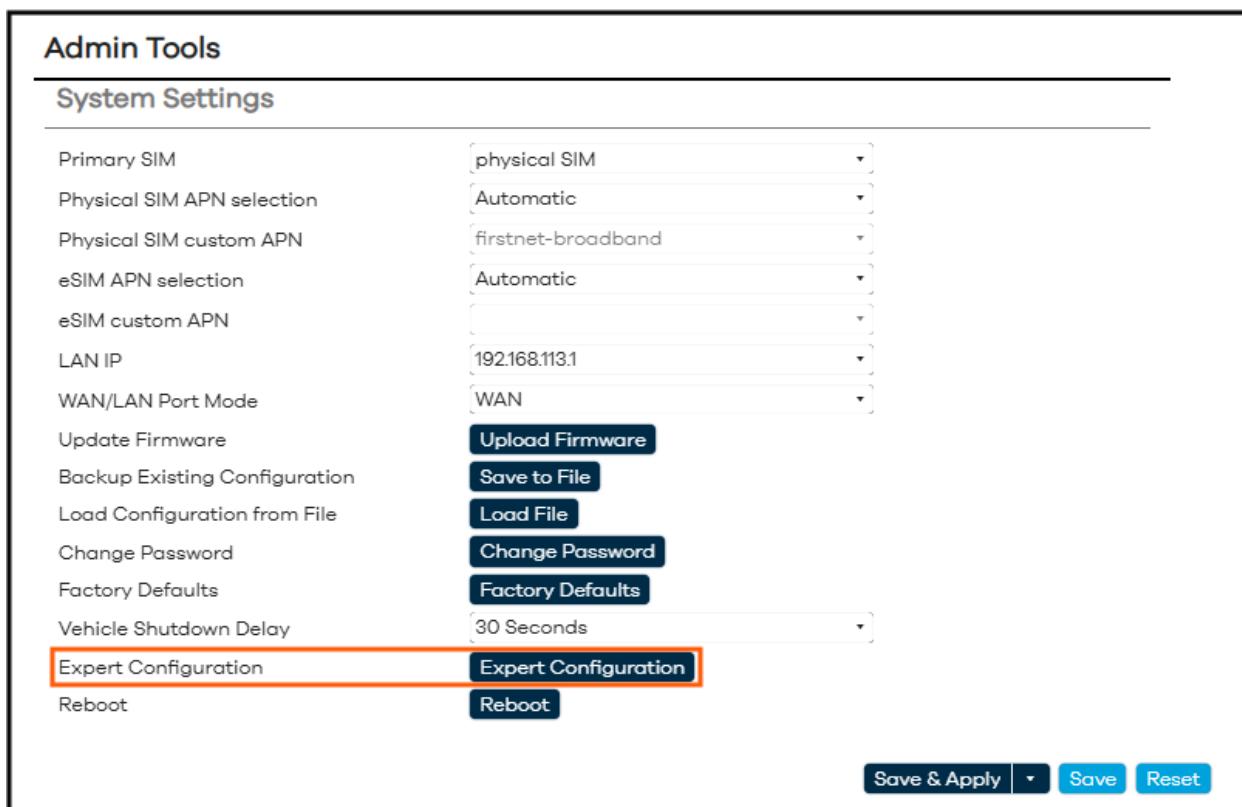


Figure 165: Remote user preparing an RDP connection

3.24.2 Traffic Rule

A Traffic Rule simply allows, blocks or redirects traffic between firewall zones. For example, is the IPSec VPN endpoint and we need to create a traffic rule to ensure VPN traffic can pass through NAT. NAT-T or NAT-Traversal protocols UDP port 4500 and UDP port 500 will need to be allowed inbound. We'll show how to create one of these rules. The other rule can be similarly created using the other port number.

1. Navigate to **Overview > System Settings** under **Admin Tools**.
2. Click on the **Expert Configuration** button to enter Expert Configuration mode.



The screenshot shows the 'System Settings' section of the 'Admin Tools' interface. The 'Expert Configuration' button is highlighted with a red box. The interface includes fields for Primary SIM, Physical SIM APN selection, Physical SIM custom APN, eSIM APN selection, eSIM custom APN, LAN IP, WAN/LAN Port Mode, Update Firmware, Backup Existing Configuration, Load Configuration from File, Change Password, Factory Defaults, Vehicle Shutdown Delay, and a 'Reboot' button. At the bottom are 'Save & Apply' and 'Save' buttons.

Figure 166: System Settings – Expert Configuration

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

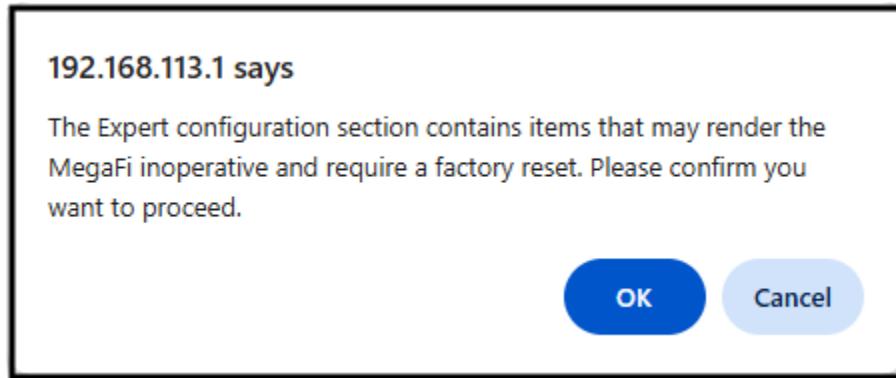


Figure 167: Confirmation to Enter Expert Configuration mode

4. Navigate to **Network > Firewall**. The landing page is General Settings. Select **Traffic Rules** at the top.

Overview

Status

System

Network

- Interfaces
- Wireless
- Routing
- DHCP and DNS
- SNMP
- Diagnostics
- Firewall**
- Logout

Mission Control

Network Mode: NAT

General Settings Port Forwards **Traffic Rules** NAT Rules IP Sets

Firewall - Zone Settings

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

General Settings

Enable SYN-flood protection

Drop invalid packets

Input: accept

Output: accept

Forward: reject

Routing/NAT Offloading

Experimental feature. Not fully compatible with QoS/SQM.

Software flow offloading

Software based offloading for routing/NAT

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	Actions
lan ⇒ wan swvpn	accept	accept	accept	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
wan ⇒ REJECT	accept	accept	reject	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
guest ⇒ wan	reject	accept	reject	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
swvpn ⇒ lan	accept	accept	accept	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Add **Save & Apply** **Save** **Reset**

Figure 168: Firewall – General Settings

5. A preset of Traffic Rules are already configured by default. Scroll to the bottom and click on the **Add** button to add a new Traffic Rule.

Mission Control

Network Mode: NAT

Overview

Status

System

Network

Interfaces

Wireless

Routing

DHCP and DNS

SNMP

Diagnostics

Firewall

Logout

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.

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 To this device , 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	Accept input	<input type="checkbox"/> Edit Delete
Allow-ICMPv6-Forward	Limit matching to 1000 packets per second Forwarded IPv6 , protocol ICMP From wan To any zone	Accept forward	<input type="checkbox"/> Edit Delete
Allow-IPSec-ESP	Limit matching to 1000 packets per second 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
Support-UDP-Traceroute	Incoming IPv4 , protocol UDP From wan To this device , port 33434:33689	Reject input	<input type="checkbox"/> Edit Delete
Allow-Remote-HTTPS	Incoming IPv4 and IPv6 , protocol TCP From wan To this device , port 443	Reject input	<input type="checkbox"/> Edit Delete
Allow-DNS-guest	Incoming IPv4 and IPv6 , protocol TCP, UDP From guest To this device , port 53	Accept input	<input type="checkbox"/> Edit Delete
Allow-DHCP-guest	Incoming IPv4 , protocol UDP From guest To this device , port 67	Accept input	<input type="checkbox"/> Edit Delete

[Add](#)

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

Figure 169: Firewall - Traffic Rules

6. Within General Settings of Traffic Rules pop-up window the following options are available:

- **Name** – name of the Traffic Rule
- **Protocol** – options are **Any**, **TCP**, **UDP**, **ICMP**, **IGMP**, **IPSEC-ESP**, and **custom**. Both **TCP** and **UDP** are selected by default
- **Source zone** – options are **Device(output)**, **Any zone(forward)**, **guest**, **lan**, **swvpn**, **wan** (wan, wan6, wwan); **Device(output)** is selected by default
- **Source address** – choose from the drop-down menu or enter a custom IP address
- **Source port** – enter a source port number
- **Output zone** – options are **Any zone** (default), **guest**, **lan**, **swvpn**, **wan** (wan, wan6, wwan); **Any zone** is selected by default
- **Destination address** - choose from the drop-down menu or enter a custom IP address
- **Destination port** – enter a source port number
- **Action** – options are **accept** (default), **drop**, **reject**, **don't track**, **assign conntrack helper**, **apply firewall mark**, **XOR firewall mark**, **DSCP classification**

Firewall - Traffic Rules - Unnamed rule

General Settings Advanced Settings Time Restrictions

Name	Unnamed rule
Protocol	TCP <input type="button" value="UDP"/>
Source zone	Device(output) <input type="button"/>
Source address	any <input type="button"/>
Source port	any
Output zone	Any zone <input type="button"/>
Destination address	any <input type="button"/>
Destination port	any
Action	accept <input type="button"/>

Dismiss Save

Figure 170: Firewall – Traffic Rules General Settings

7. In the following example, we created a Traffic Rule to allow or accept inbound NAT-T traffic on port 4500, which uses the UDP protocol, to the LAN zone.

Firewall - Traffic Rules - Unnamed rule

General Settings Advanced Settings Time Restrictions

Name	Allow-NAT-T
Protocol	UDP
Source zone	wan wan: wan6: wwan: wan wan: wan6: wwan:
Source address	-- add IP --
Source port	any
Destination zone	lan lan: lan lan:
Destination address	-- add IP --
Destination port	4500
Action	accept

Buttons: Dismiss Save

Figure 171: Firewall – Traffic Rules NAT-T (port 4500) example

8. Click on **Save** then **Save & Apply** on the main **Firewall - Traffic Rules** page.
9. Following the same steps, create another Traffic Rule for port 500, only change the name and this will complete what is needed for NAT-T.