NEXTIVITY
Smarter by Design

SHIELD MegaFi 2

Software Manual

Rev Date: Feb 2026

Table of Contents

Revision History iii

1 | Introduction 1

1.1 Objectives 1

1.2 Conventions 1

1.3 Related Documents 2

1.4 Abbreviations and Acronyms 3

1.5 About OpenWRT and Mission Control 5

1.6 About this Document 5

1.7 Support 5

2 | Misson Control 7

2.1 Accessing Mission Control via Ethernet Connection 8

2.2 Initial Connection to MegaFi 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, Band 1, and Band 30 Settings 69

3.13 SSH Access 72

3.14 GPS Output Configuration 75

3.15 WAN/LAN Port Mode 84

3.16 LCD Configuration 85

3.17 SNMP 88

3.18 Client Isolation 91

3.19 Failover Primary Connection 94
3.20 Network Scan 97
3.21 IPSec VPN 100
3.22 Modify Hostname 104
3.23 eSIM Configuration 108
3.24 Download Troubleshooting Files 123
3.25 Firewall 124
3.26 Firewall Diagnostics 134

Revision History

Rev	Iteration	Description	Date
1	1	Initial Release for v3.1.6	5/21/2025
1	2	Release for v3.3.x	7/24/2025
1	3	Release for v3.4.x	10/6/2025
1	4	Release for v3.5.x	12/9/2025
1	5	Release for v3.6.x	1/9/2026
1	6	Release for v3.7.x	2/18/2026

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 | Misson 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**.

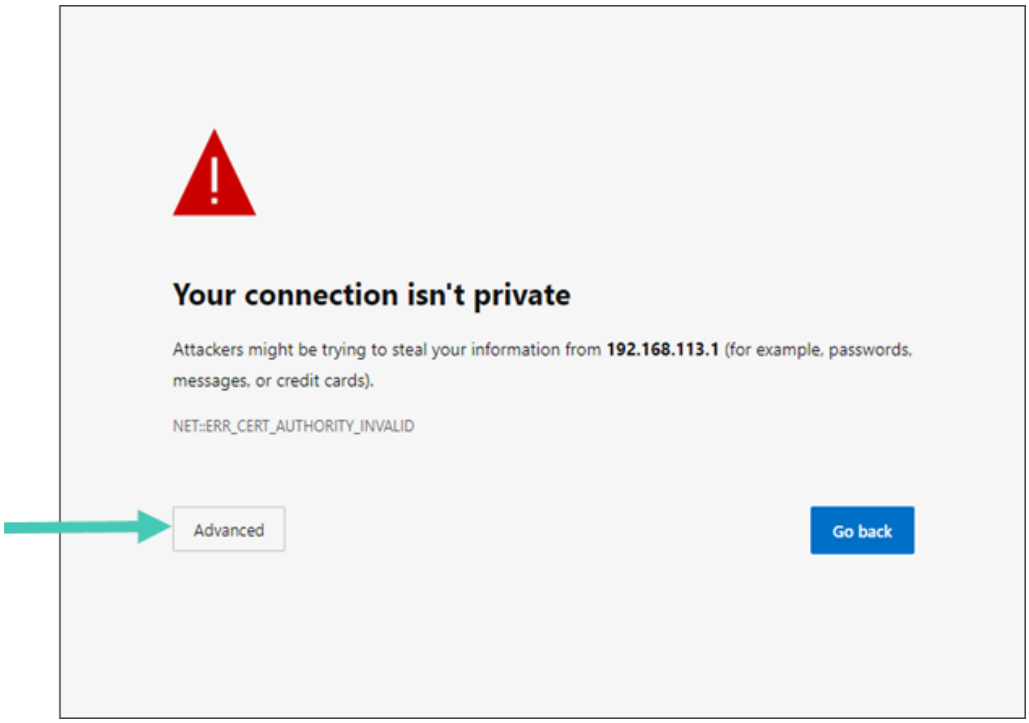


Figure 1: MegaFi 2 connection warning screen

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

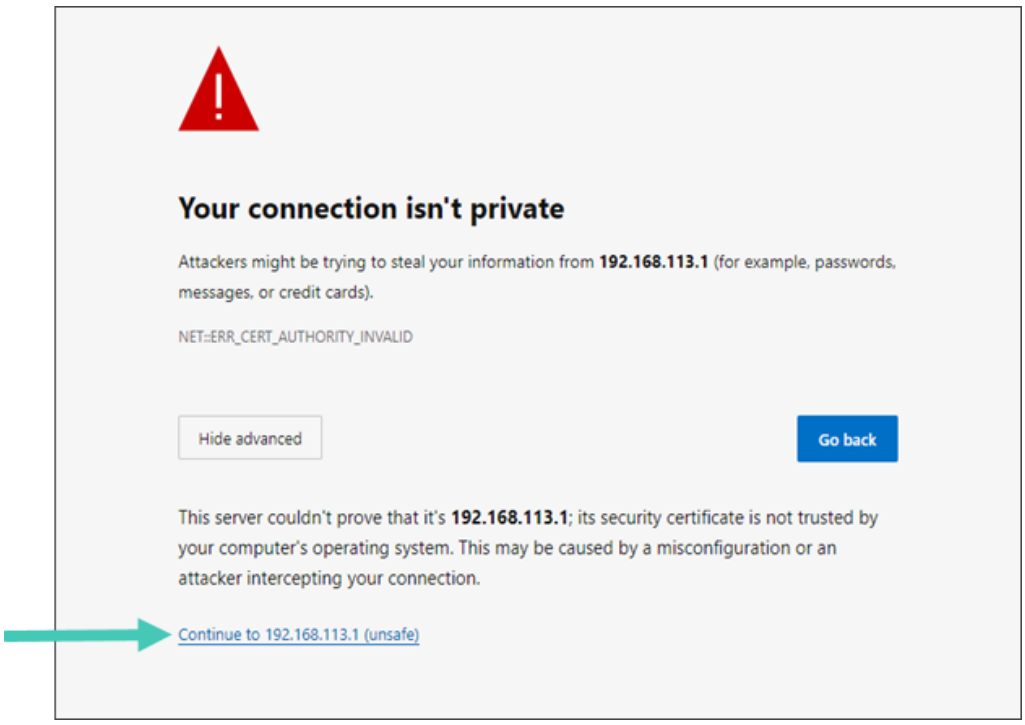


Figure 2: MegaFi 2 connection warning – second screen

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.

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

   5b. Click **Login** to proceed.

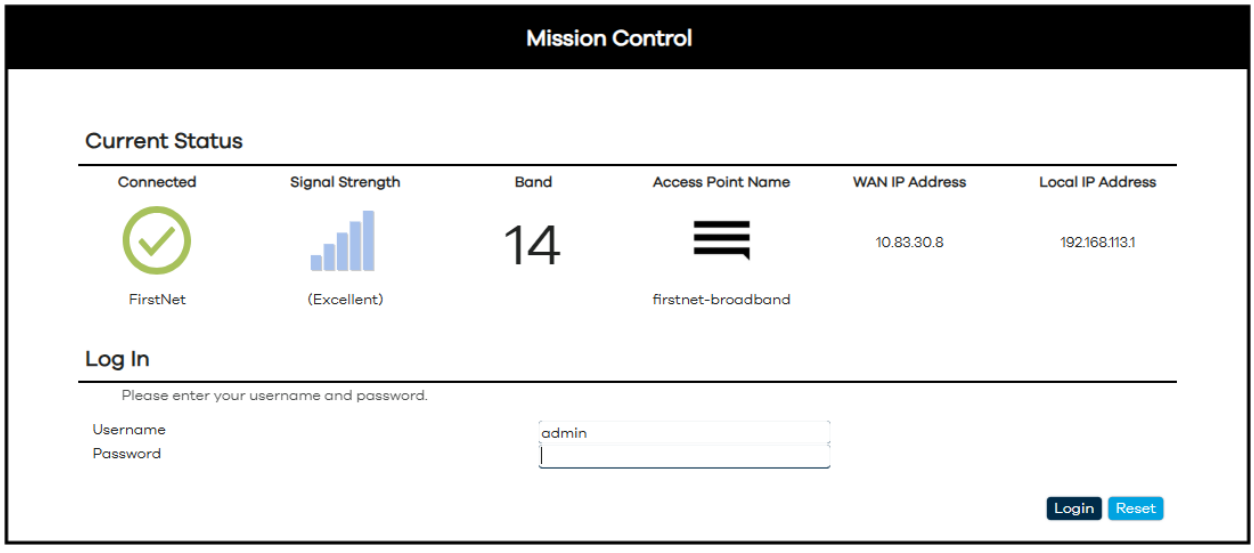


Figure 3: Mission Control Log-In screen

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.

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.

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

   8b. Confirm the new password in the **Confirmation** field, then click on **Save**.

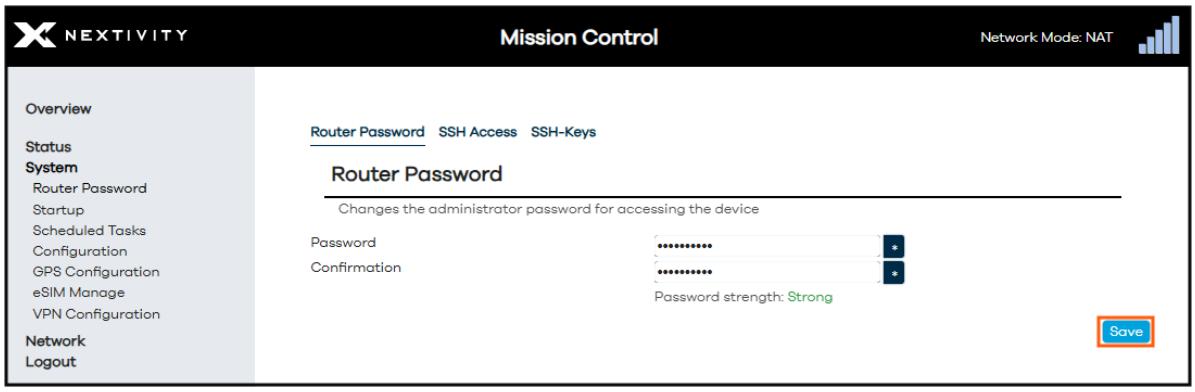


Figure 5: Change Router Password screen

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

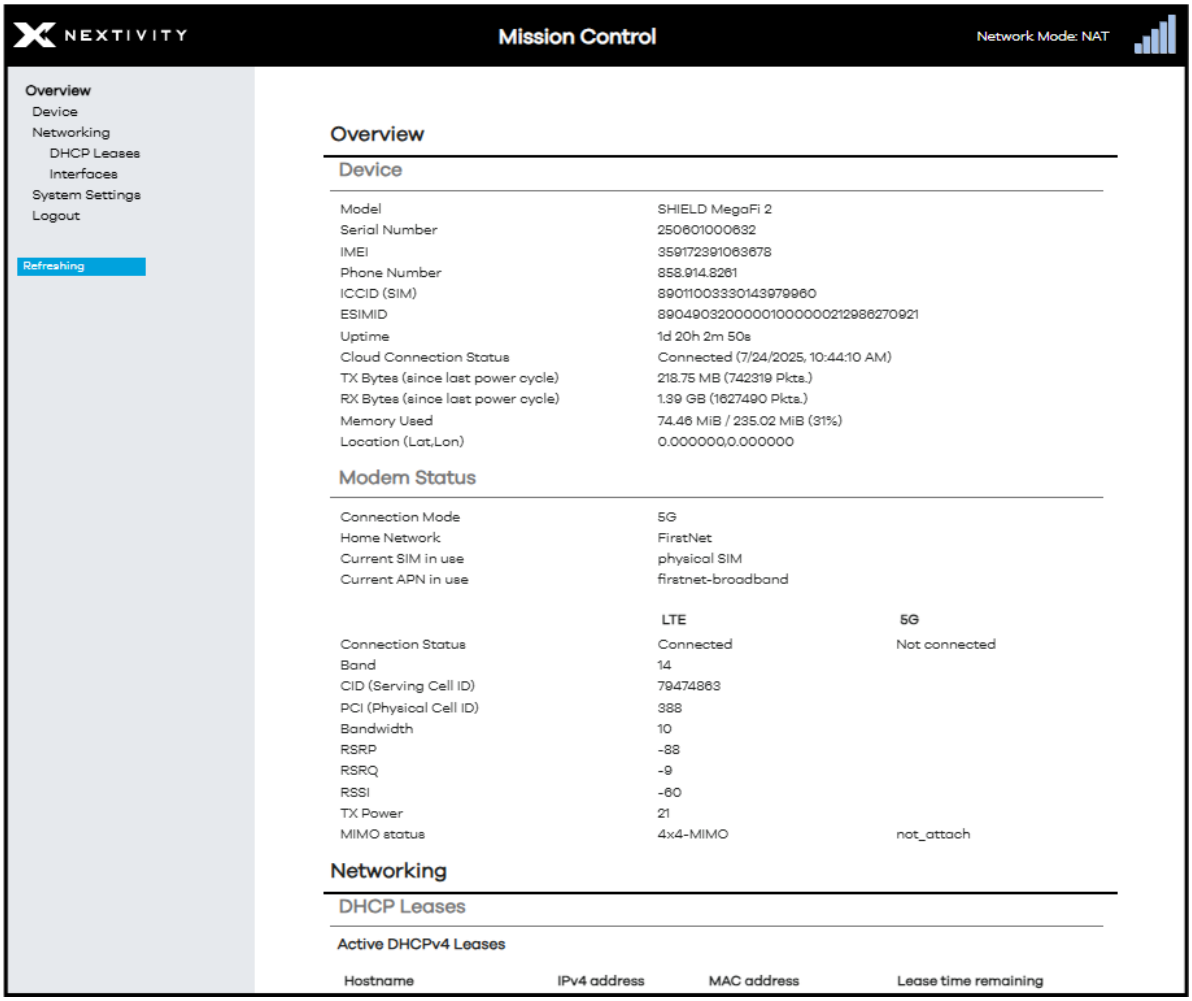


Figure 6: Mission Control – Overview page

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.

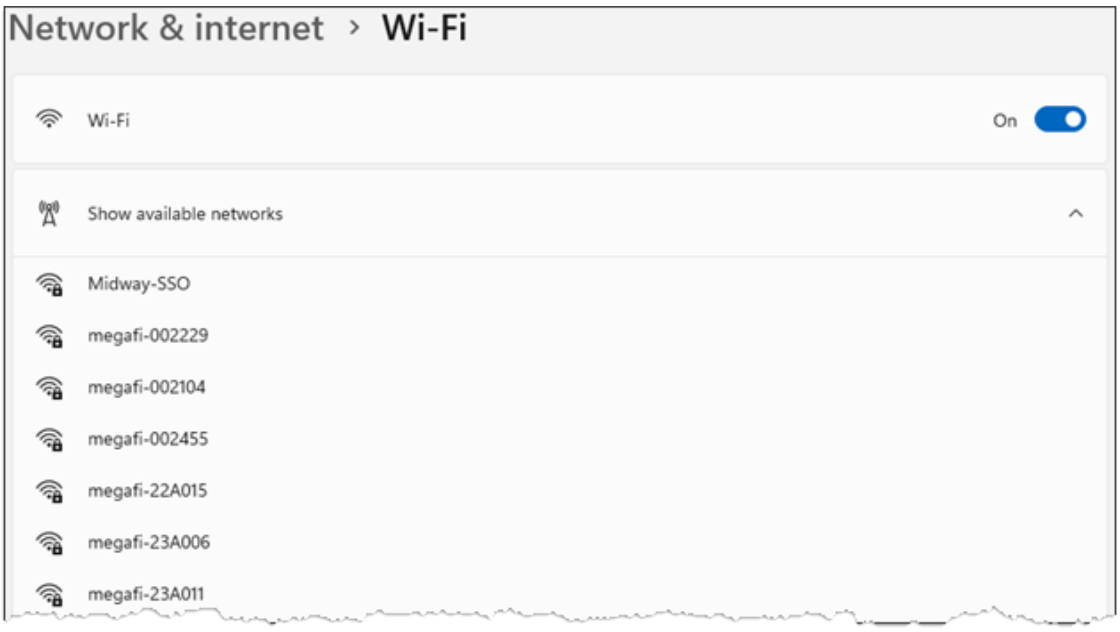


Figure 7: Windows network & internet window showing list of available Wi-Fi networks

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**.

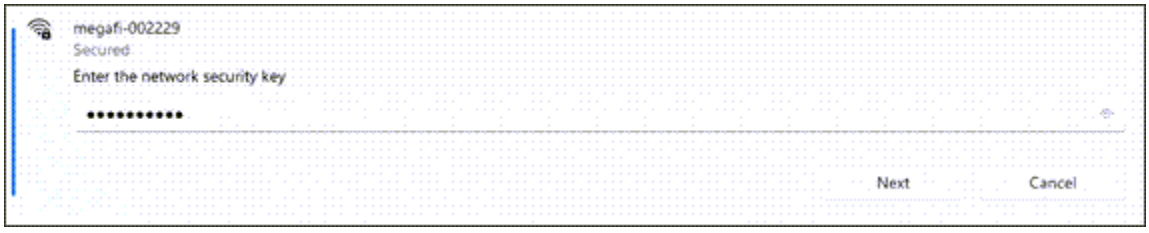


Figure 9: Wi-Fi Network Connection – Enter network security key

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**.

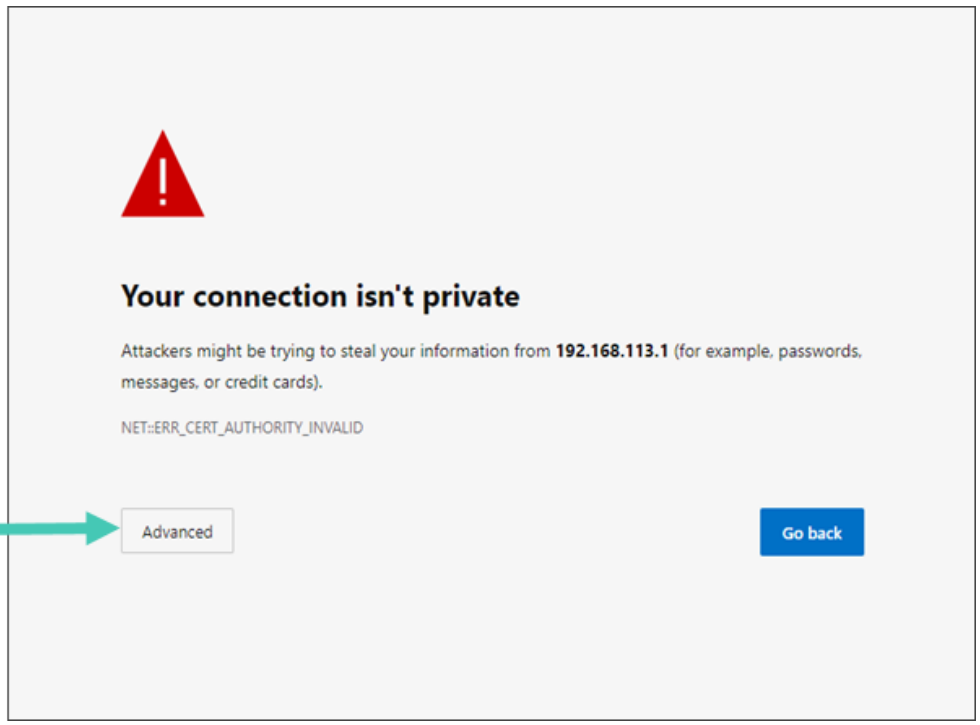


Figure 11: Warning message – Connection not private

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

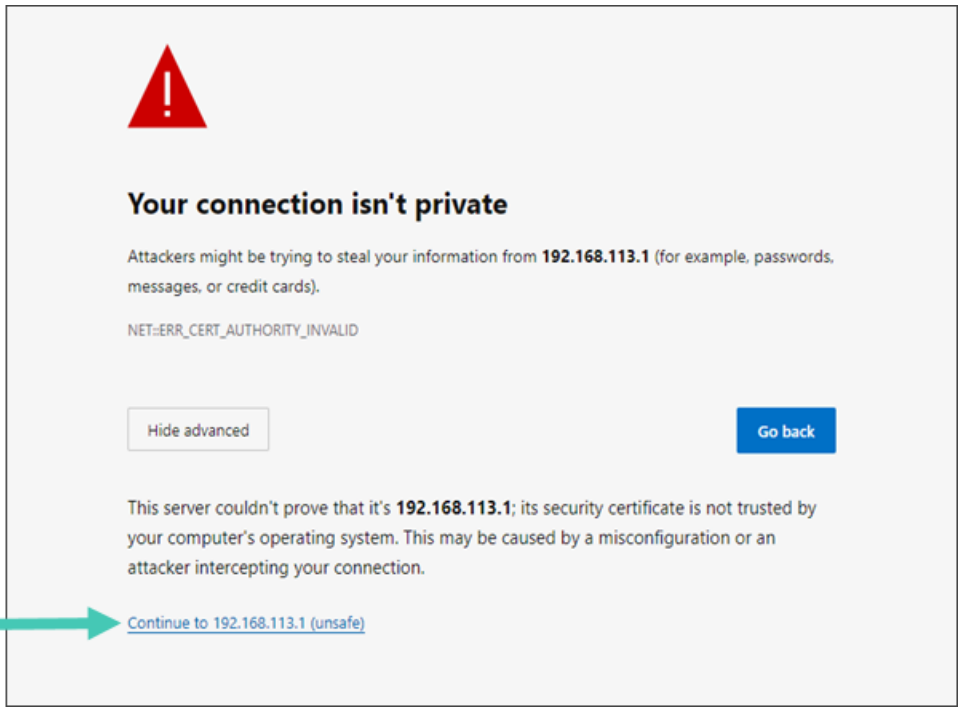


Figure 12: Warning message – Continue to IP address

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.

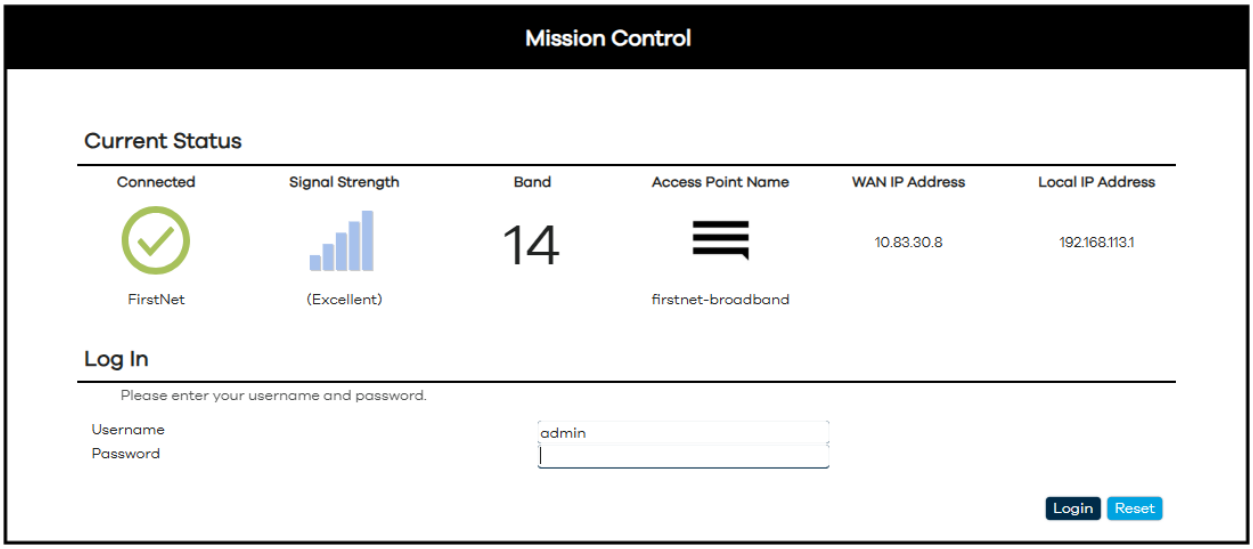


Figure 13: Mission Control – Log In page

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.

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**.

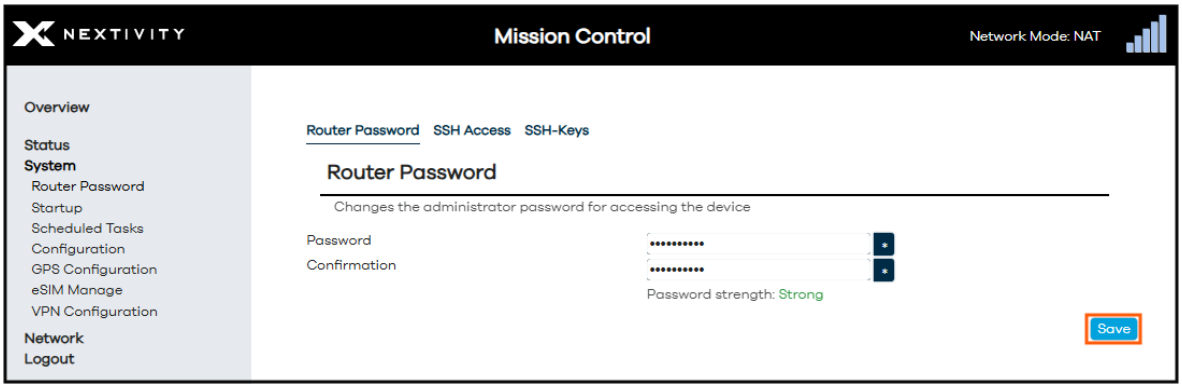


Figure 15: Change Router Password screen

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

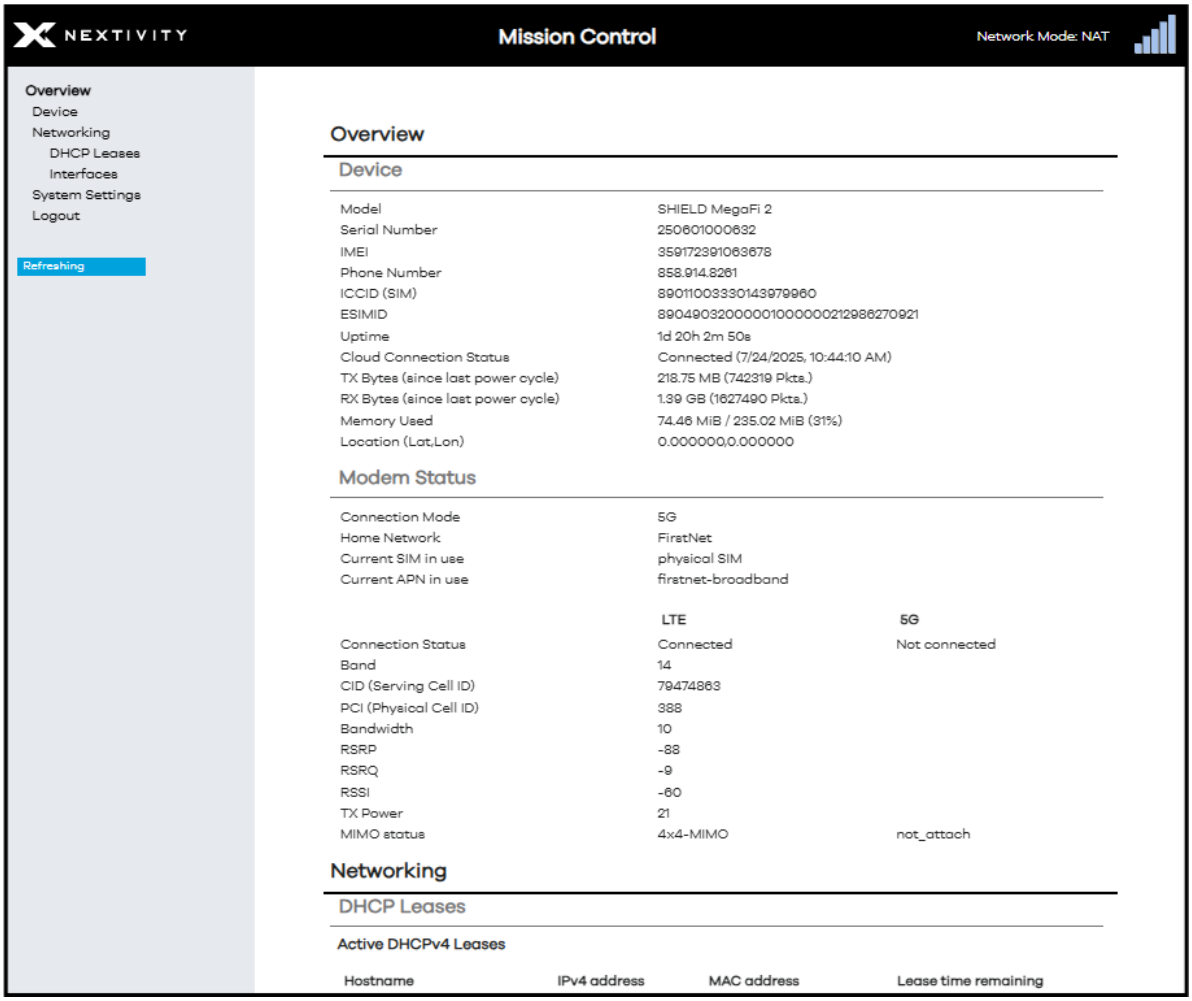


Figure 16: Mission Control – Overview page

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.

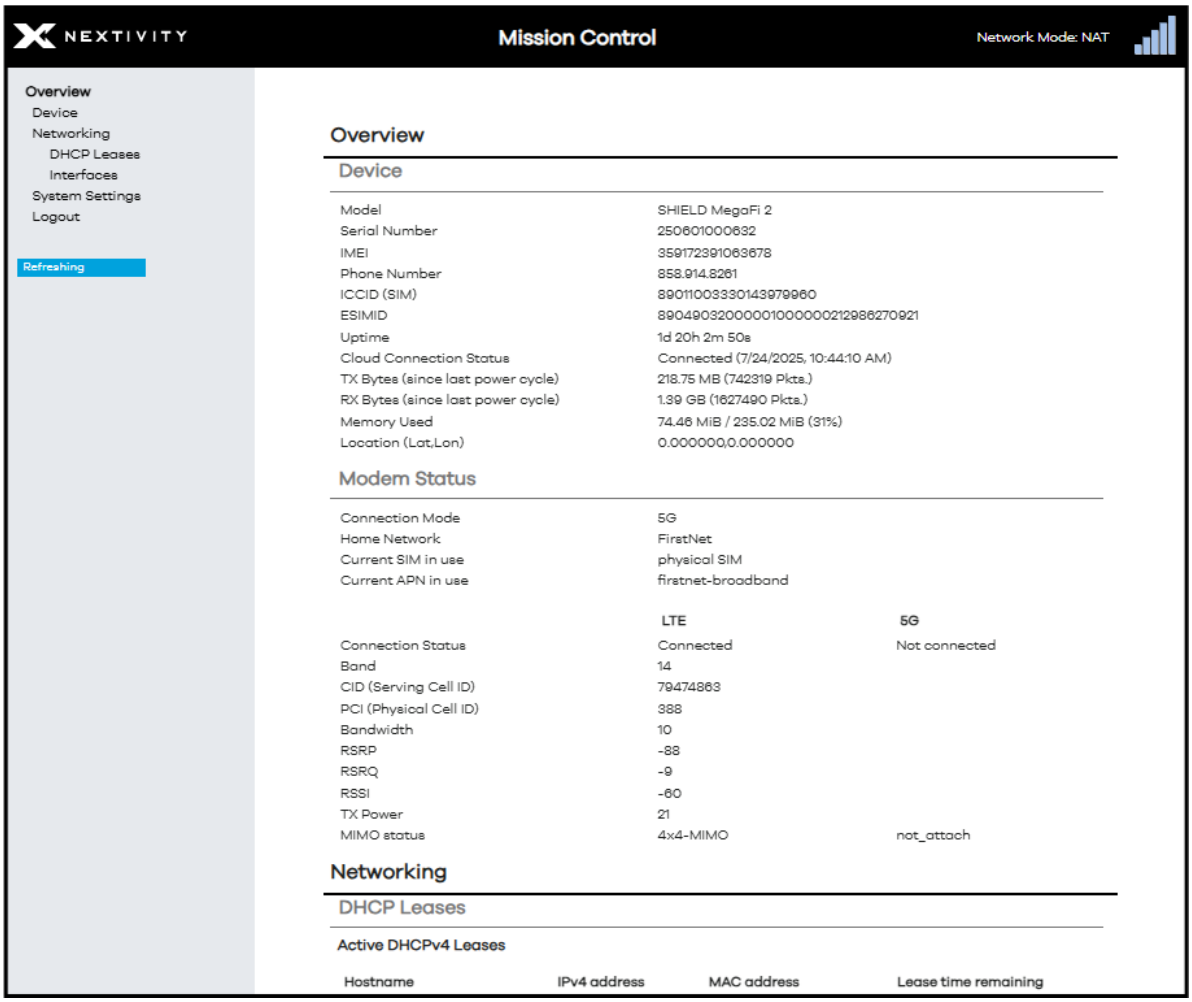


Figure 17: Mission Control – Overview page

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).

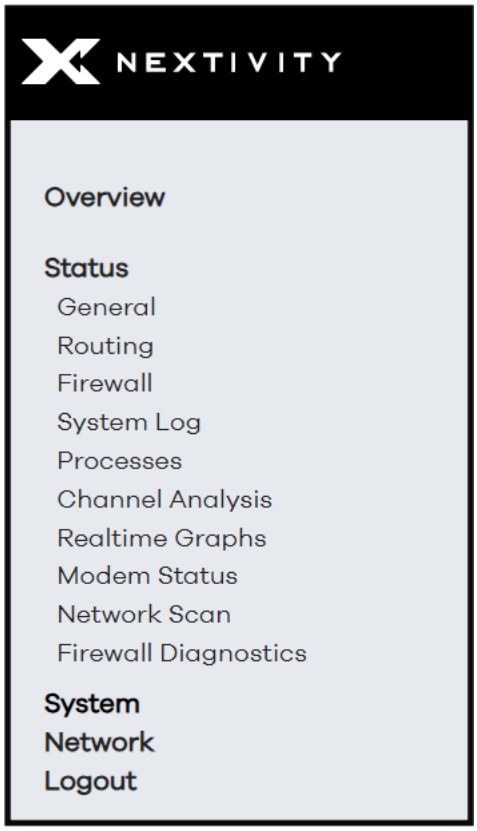


Figure 20: Mission Control Navigation Pane – Expert Configuration mode menu

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/discarded, or revert/cancelled in one stroke rather than piecemeal, one at a time. This process also lets you check, verify, and manage the list of queued changes prior to updating the system, and, depending on the changes required, 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.

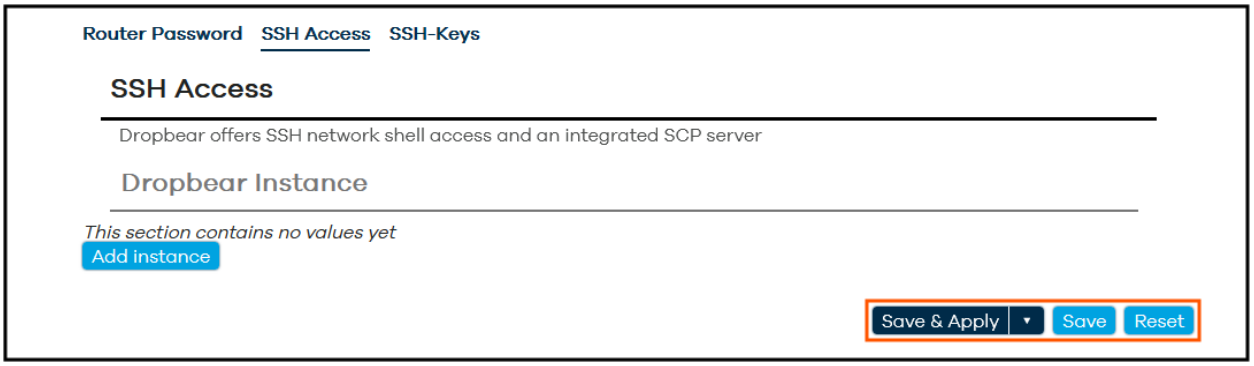


Figure 21: Mission Control – Save options

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**.

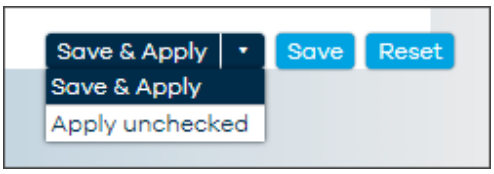


Figure 22: Mission Control – Save options

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.

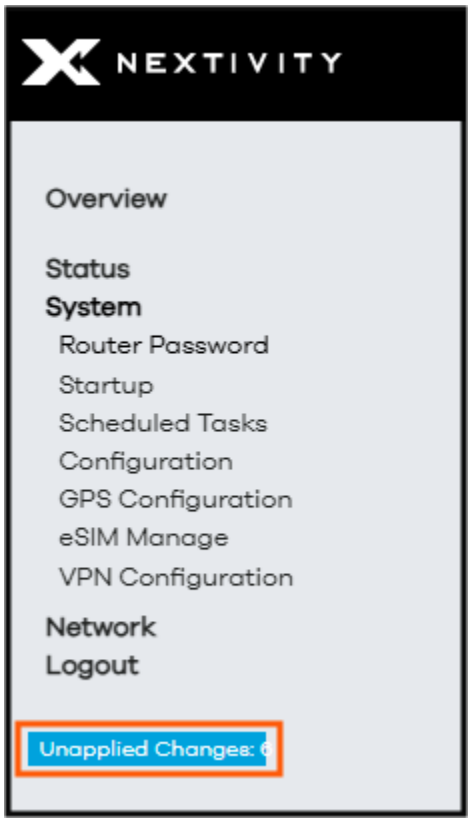


Figure 23: Navigation pane showing pending Unapplied Changes

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**

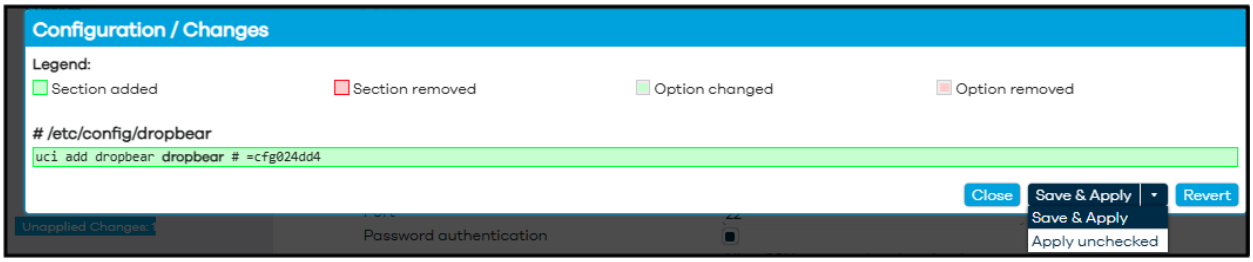


Figure 24: Configuration/Changes showing button options

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.

➲ **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.

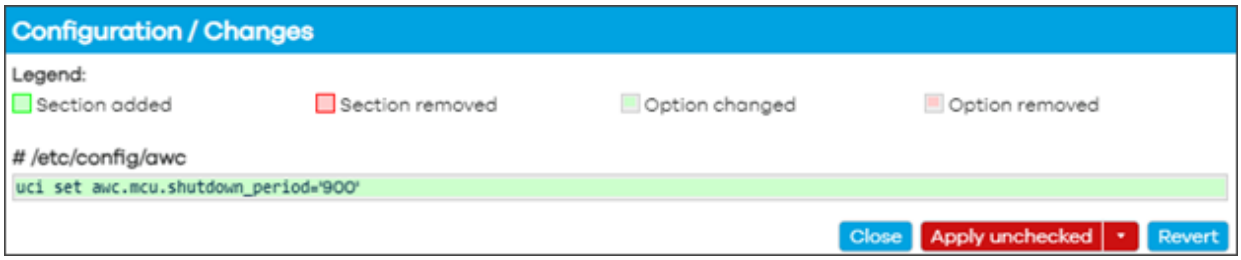


Figure 25: Configuration/Changes showing applied configuration changes

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.

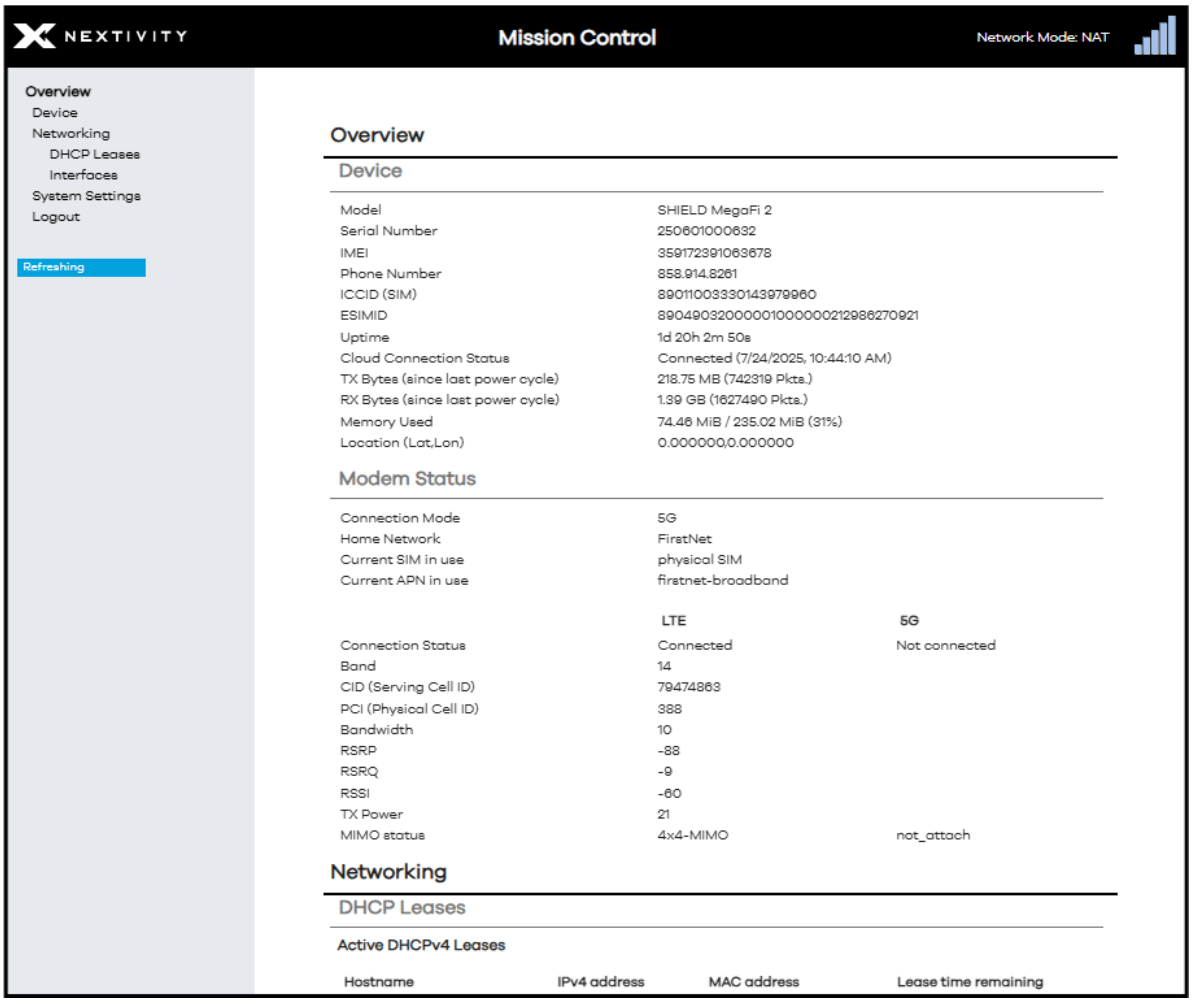


Figure 26: Mission Control – Overview page

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.

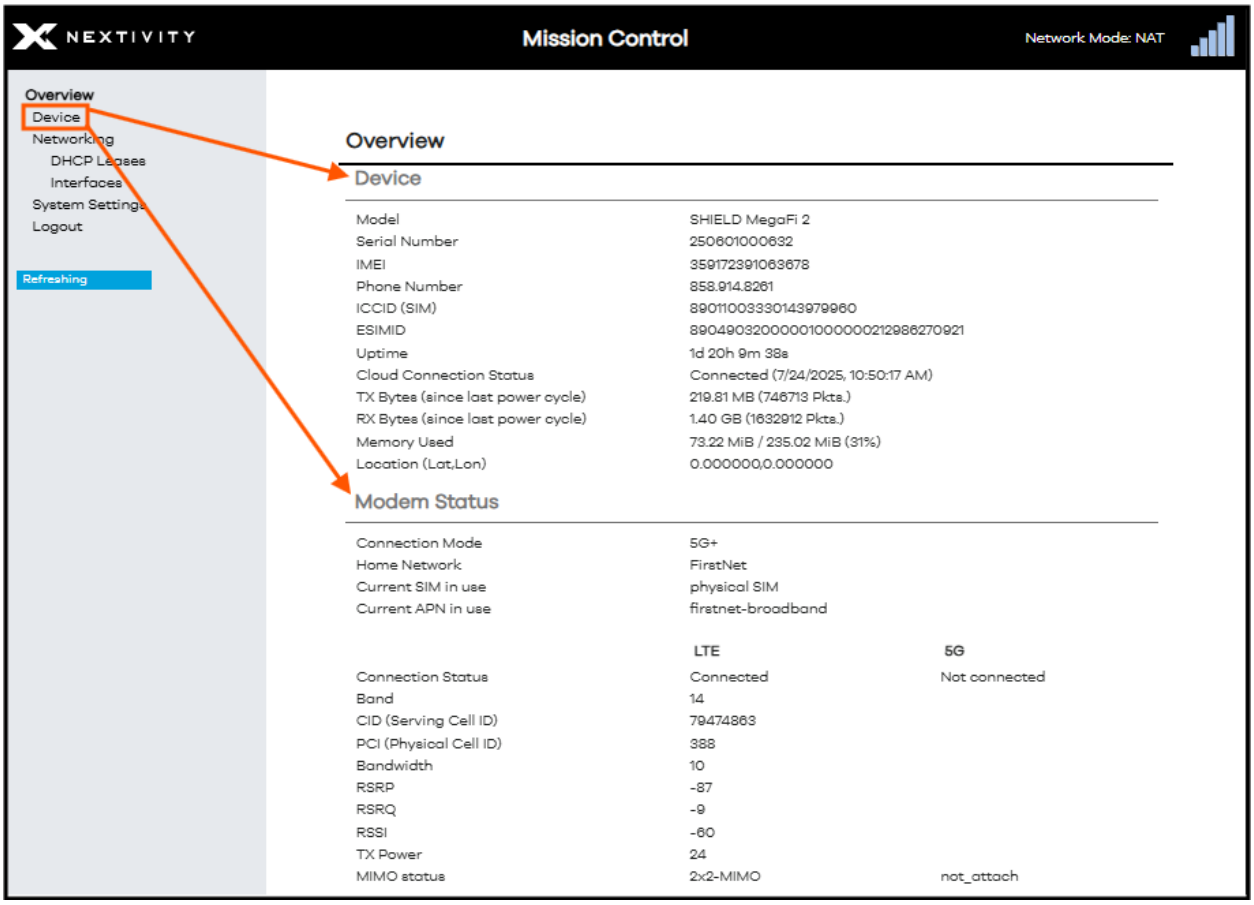


Figure 27: Mission Control – Device

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**.

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**
- **Download Troubleshooting Files**
- **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.

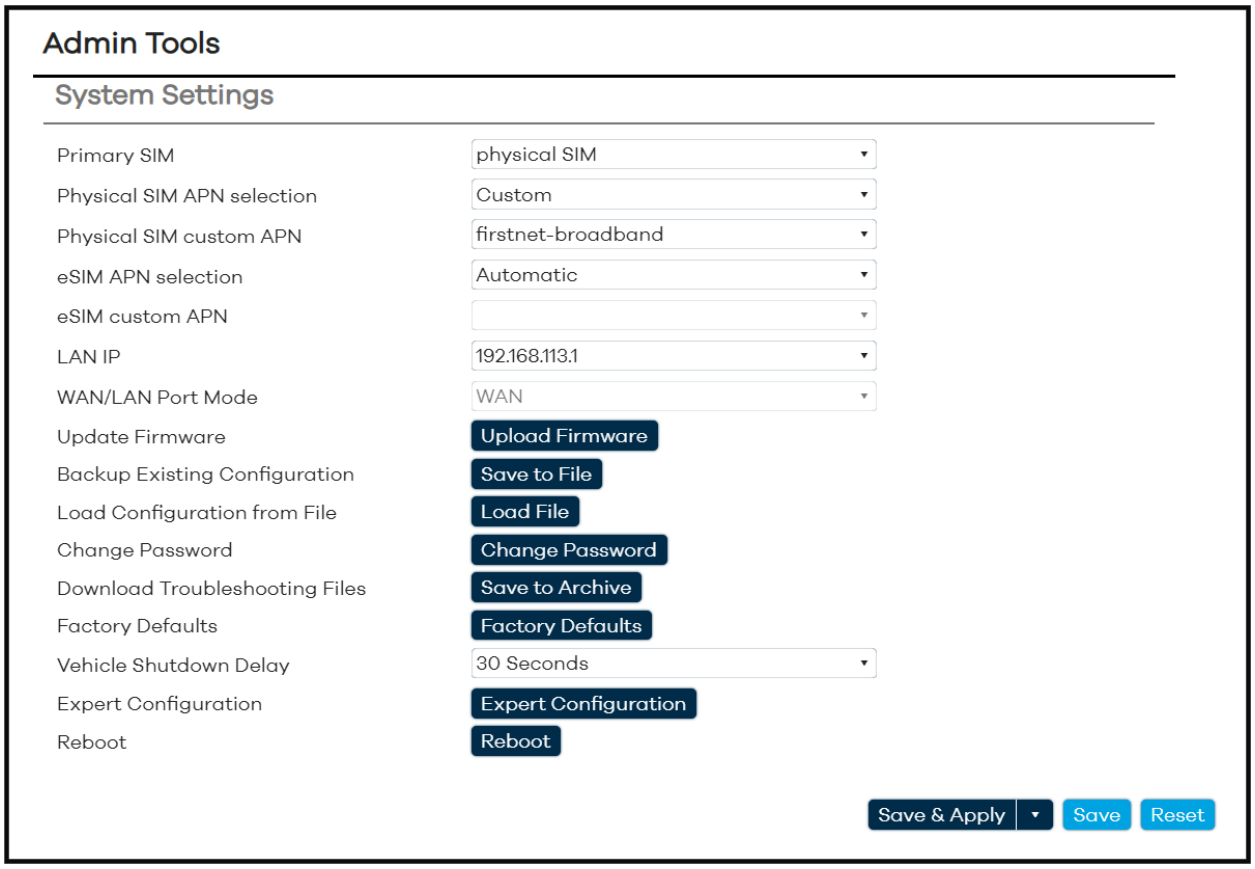


Figure 29: Mission Control – System Settings

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

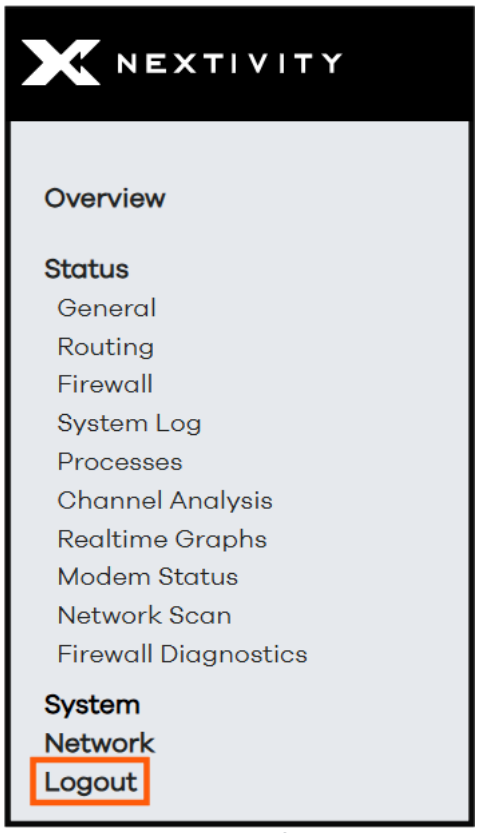


Figure 31: Logout from Expert Configuration mode

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.

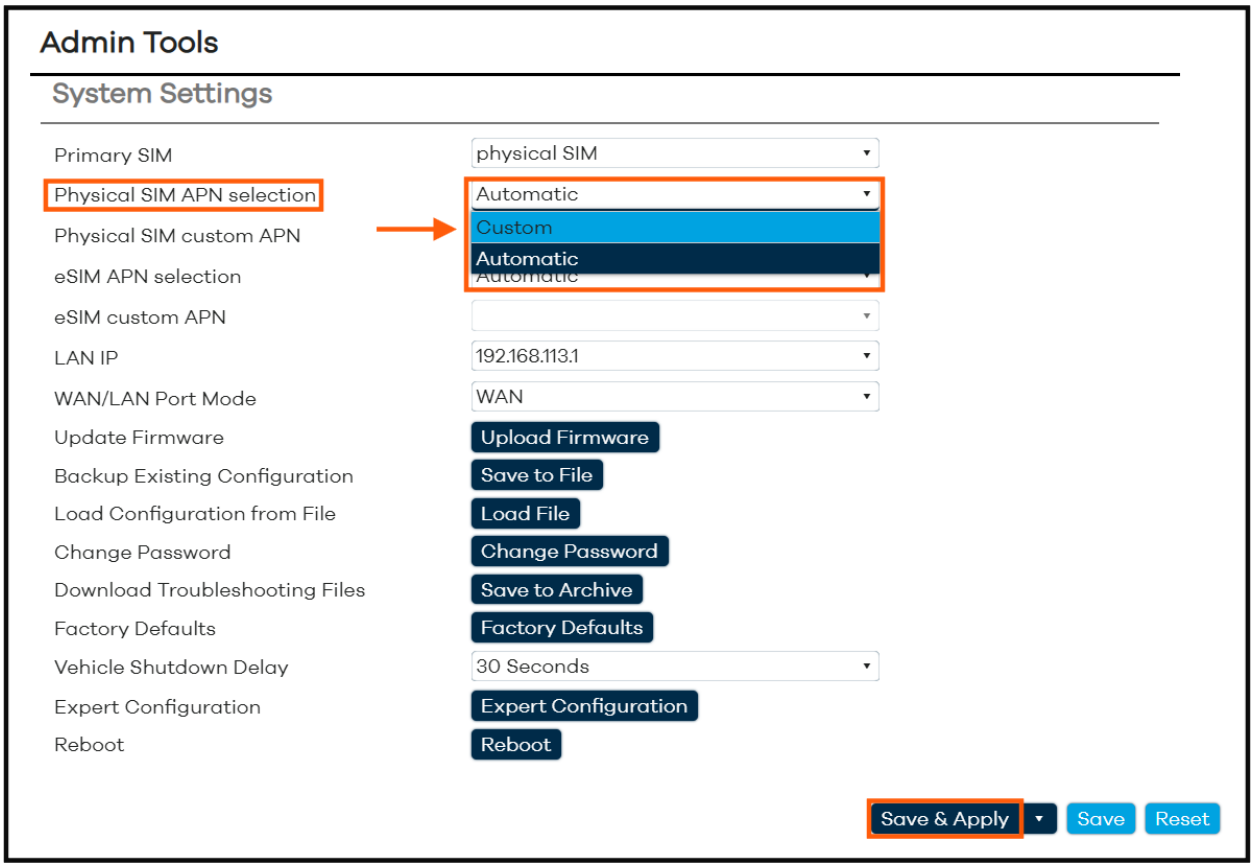


Figure 32: System Settings – Physical SIM APN selection

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.

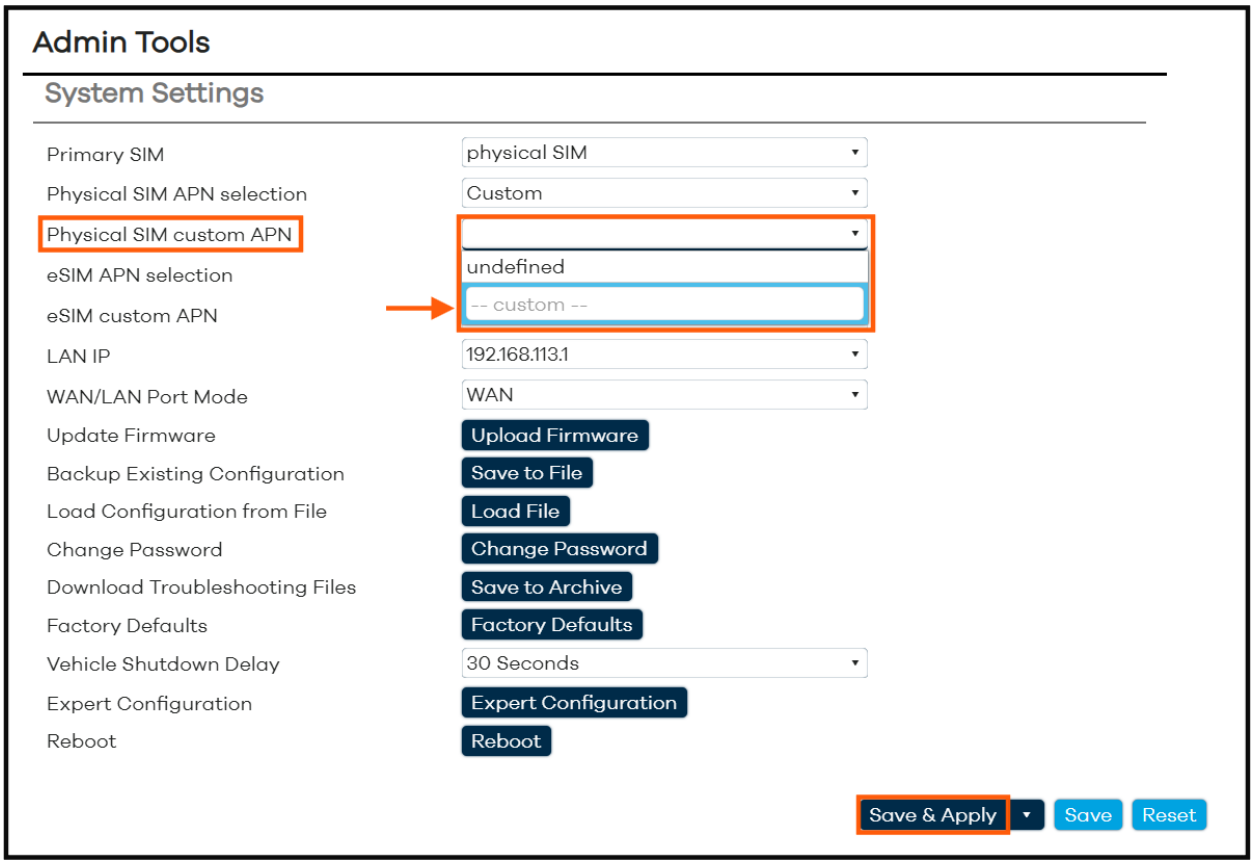


Figure 33: System Settings – Physical SIM custom APN

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.

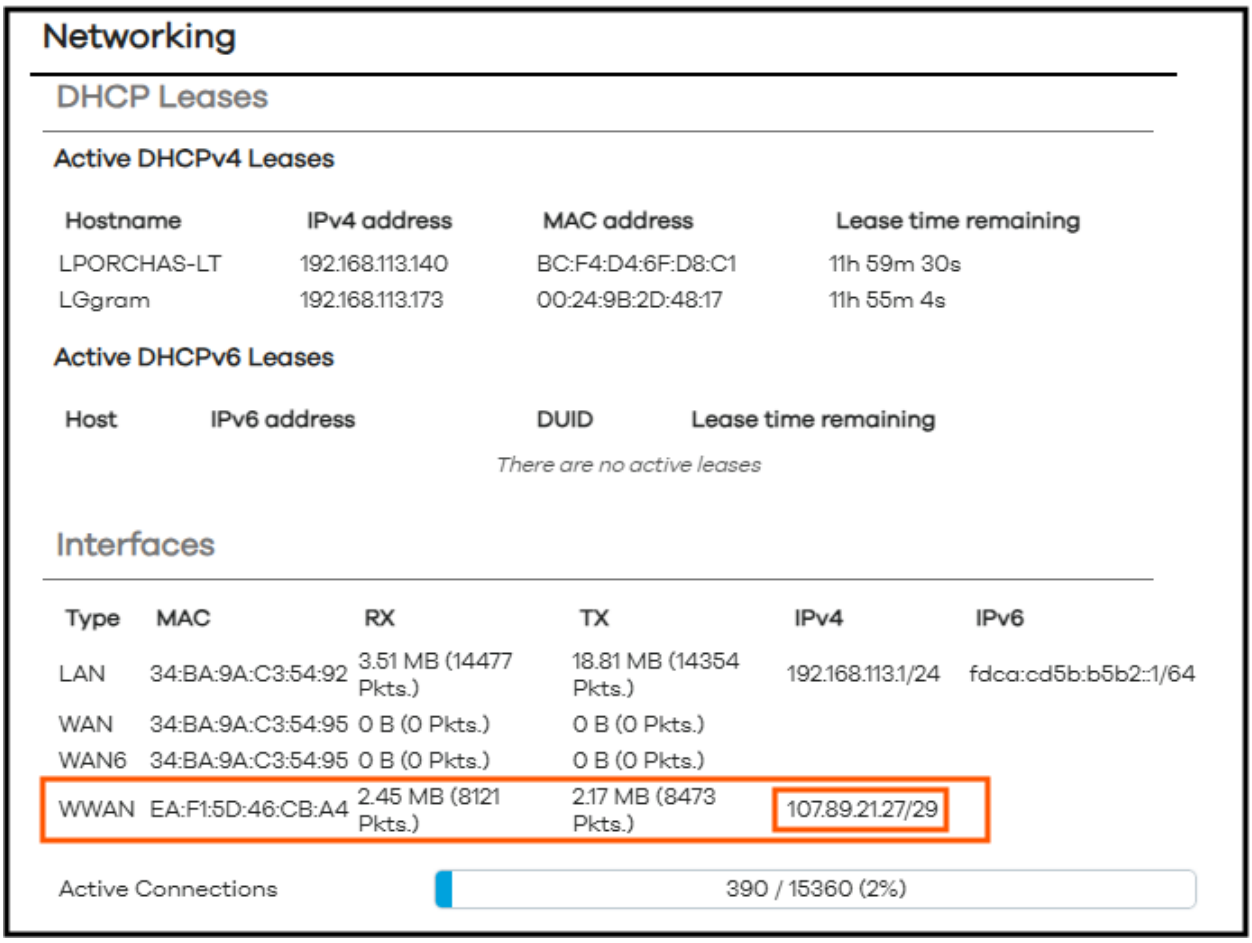


Figure 34: Networking – WWAN IPv4 Address

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.

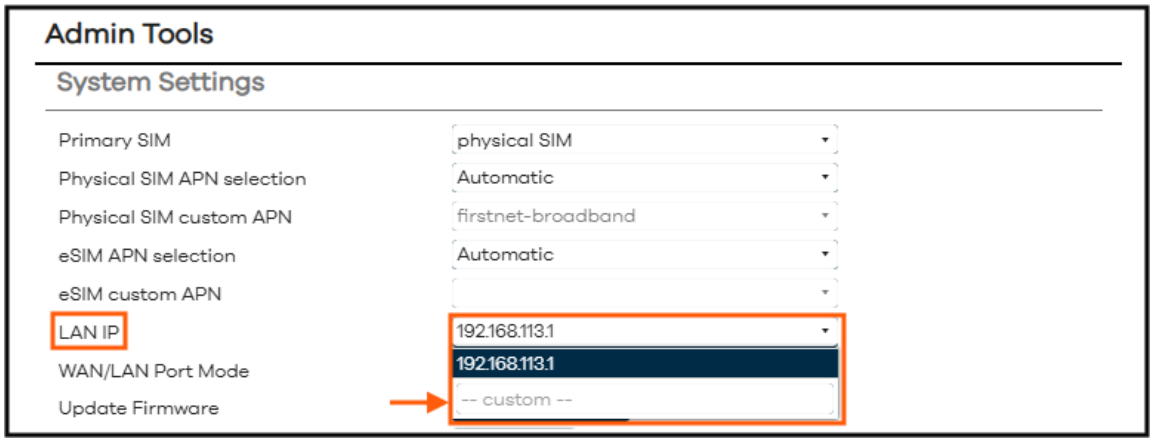


Figure 35: System Settings – Changing LAN IP Address

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.

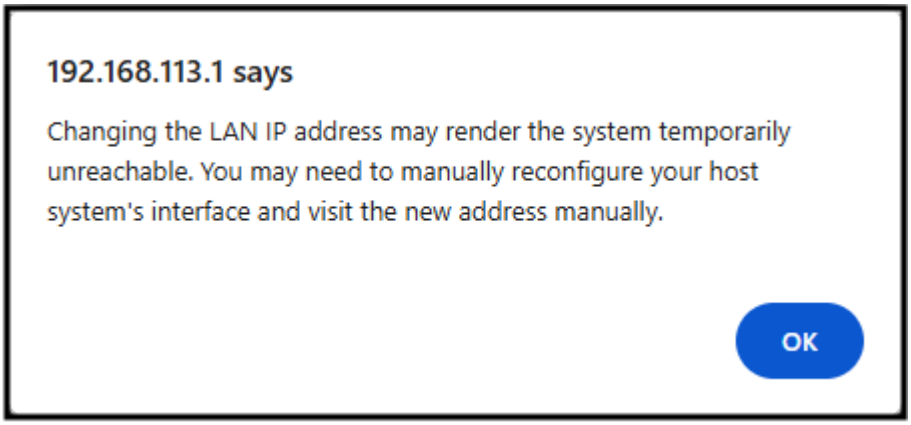


Figure 36: LAN IP address warning

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.

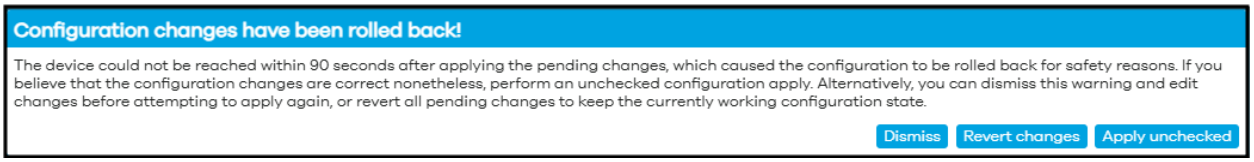


Figure 38: Configuration changes have rolled back! popup message

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**.

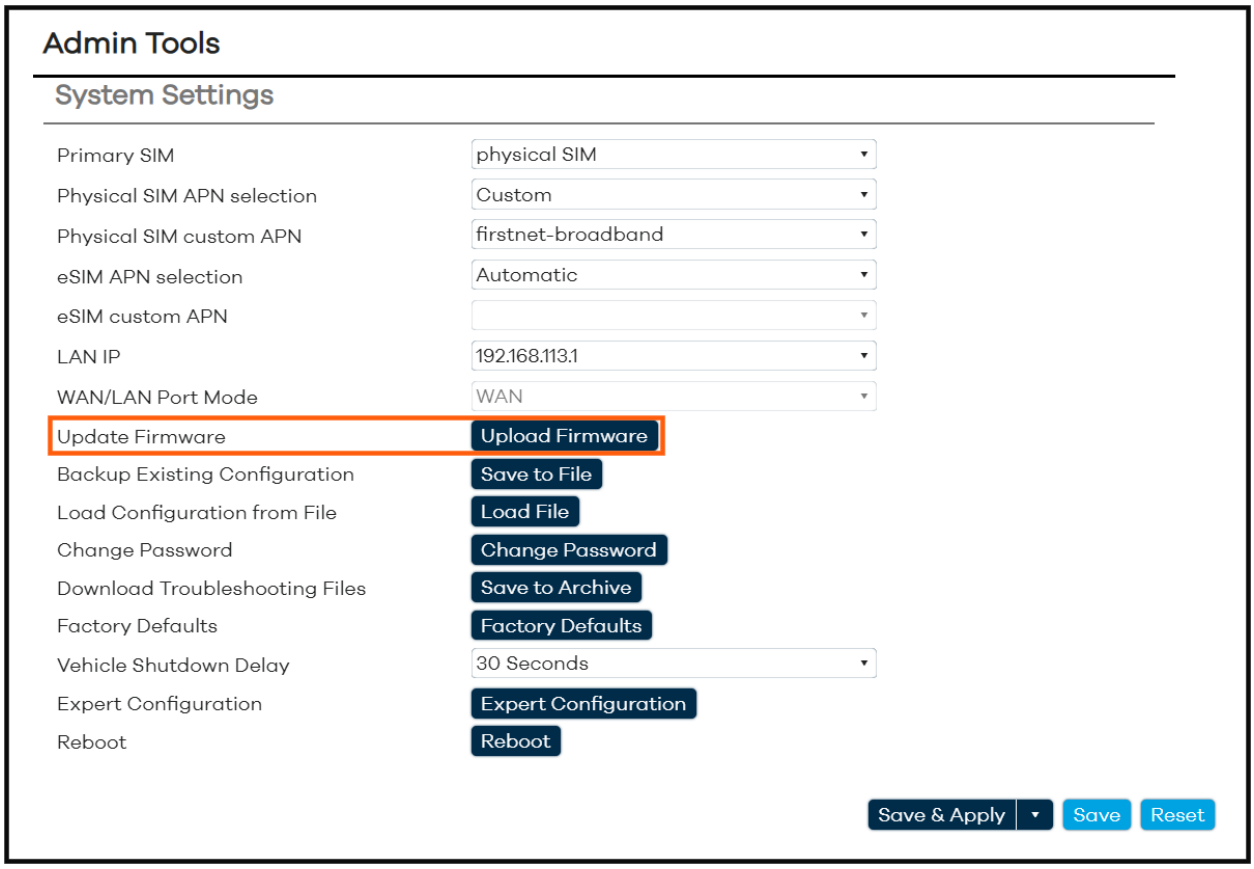


Figure 39: Firmware update – Upload Firmware button

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.

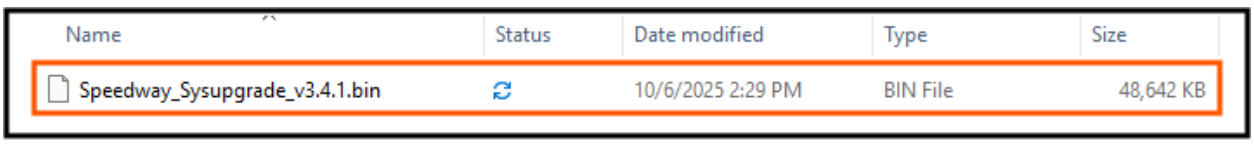


Figure 41: Firmware update – Select the upgrade file

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.

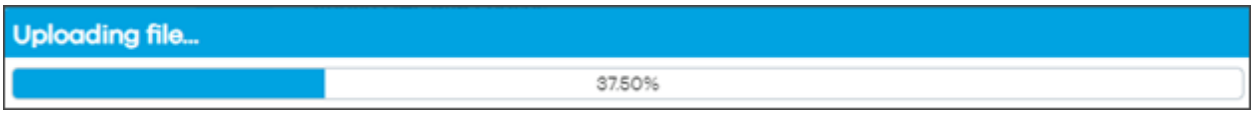


Figure 43: Firmware update – Status of upgrade file upload

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.

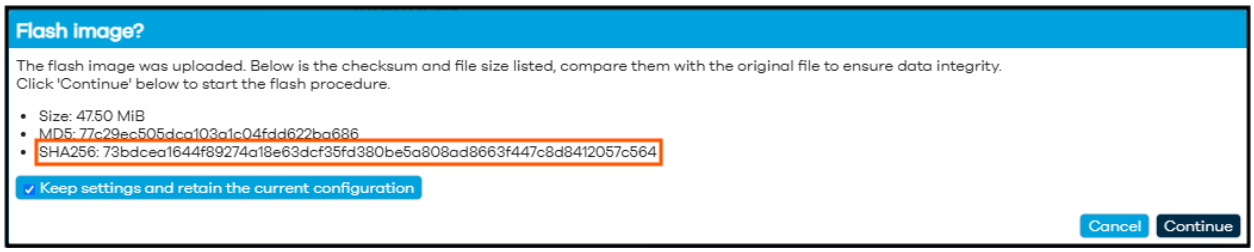


Figure 44: Flash image window – Compare checksum and file size with original

➲ **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.

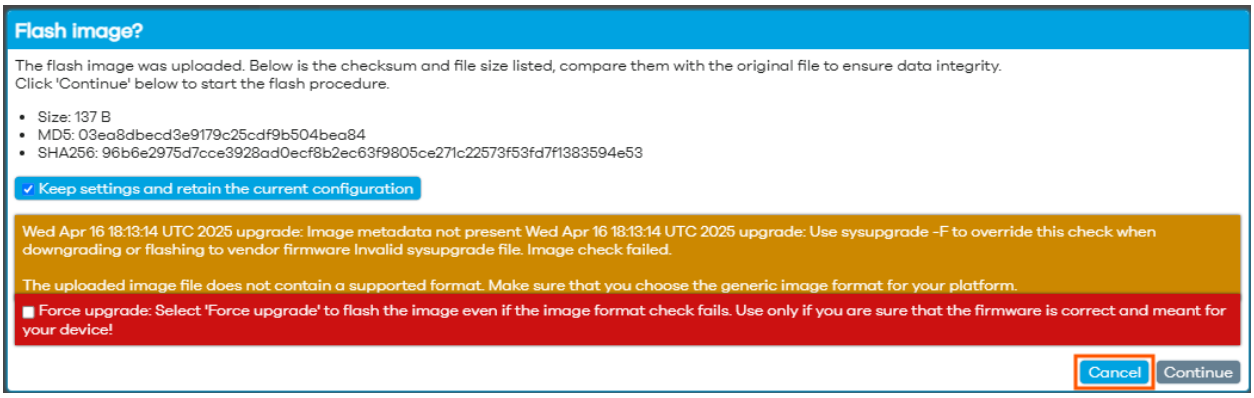


Figure 45: Flash image window – Image format check failure

➲ **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.

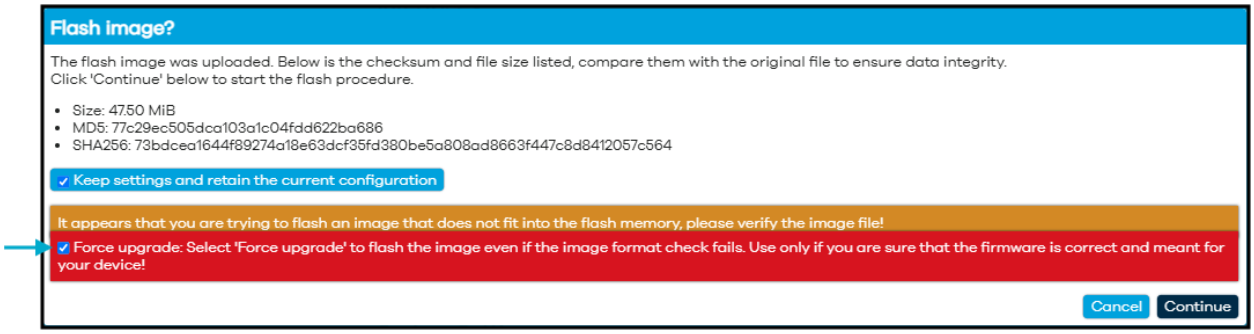


Figure 46: Flash image window – Image size

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

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

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

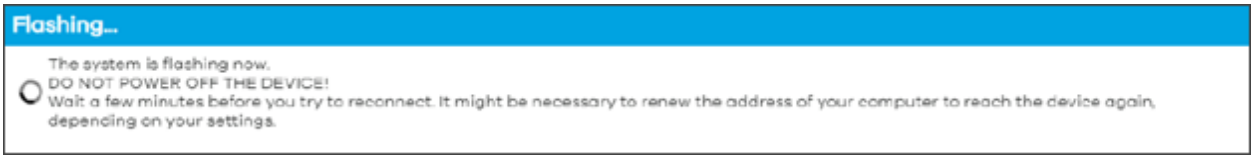


Figure 47: Flashing window – message indicating progress of the system flashing process

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**.

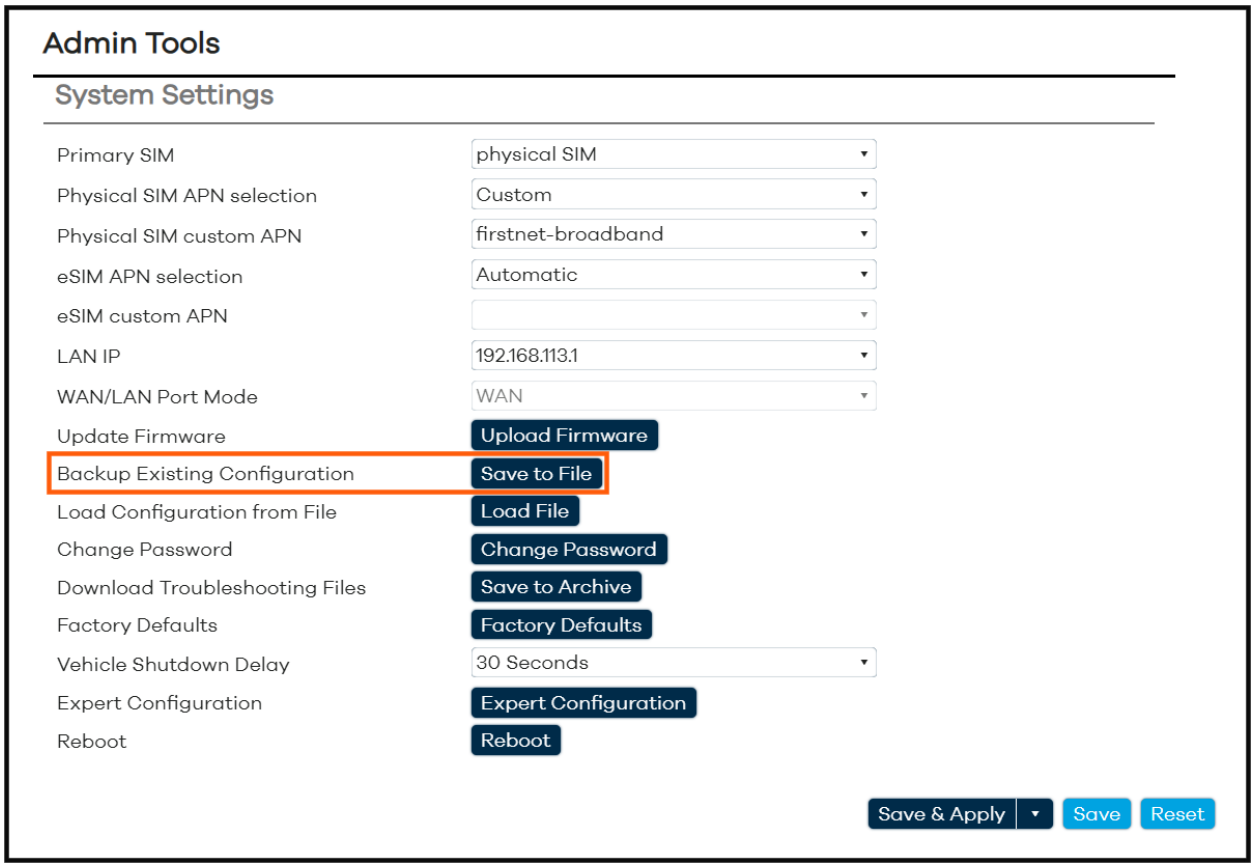


Figure 49: System Settings – Save to File button

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.

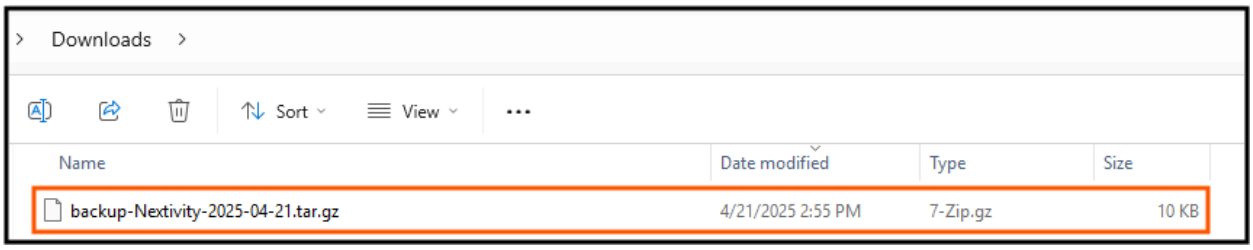


Figure 50: Downloads folder showing downloaded tar.gz file

➲ **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**.

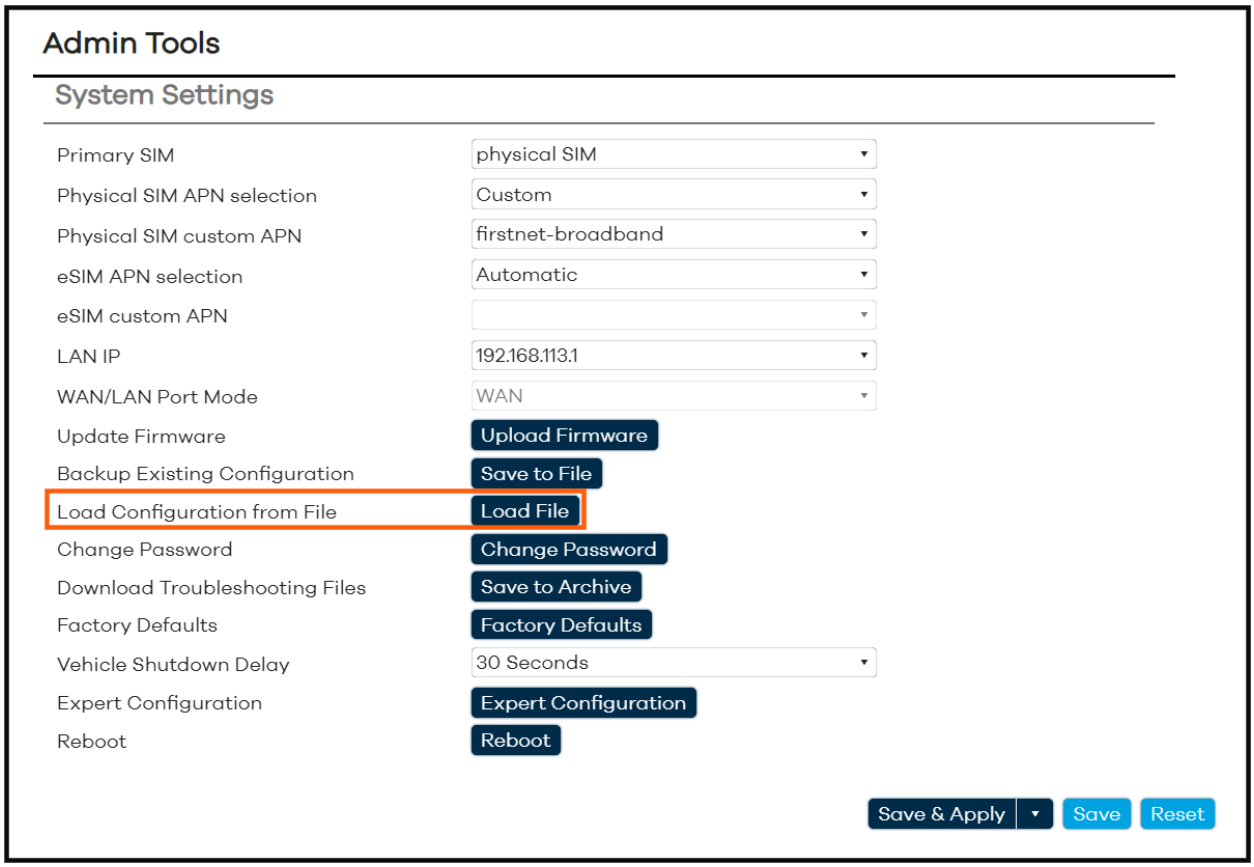


Figure 51: System Settings – Load File button

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

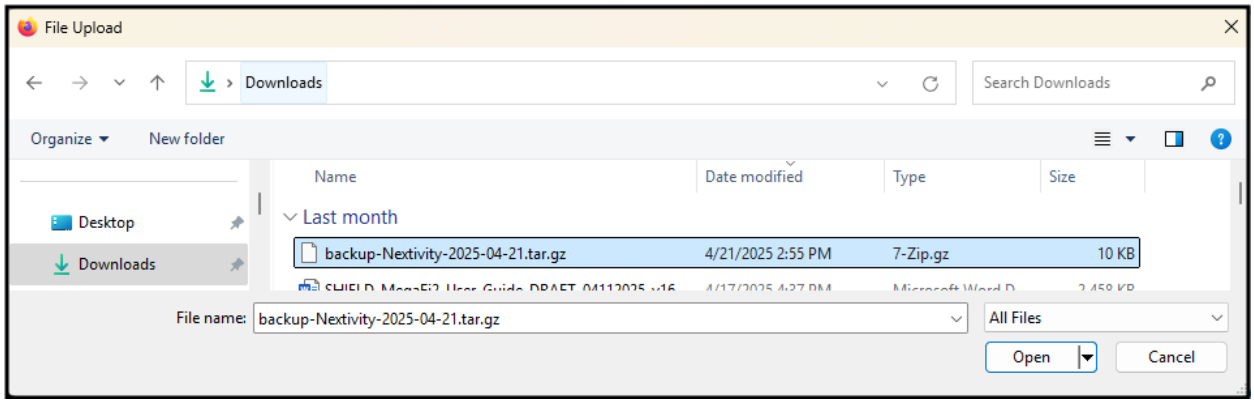


Figure 53: Uploading file and Browse to and select the tarball file

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.

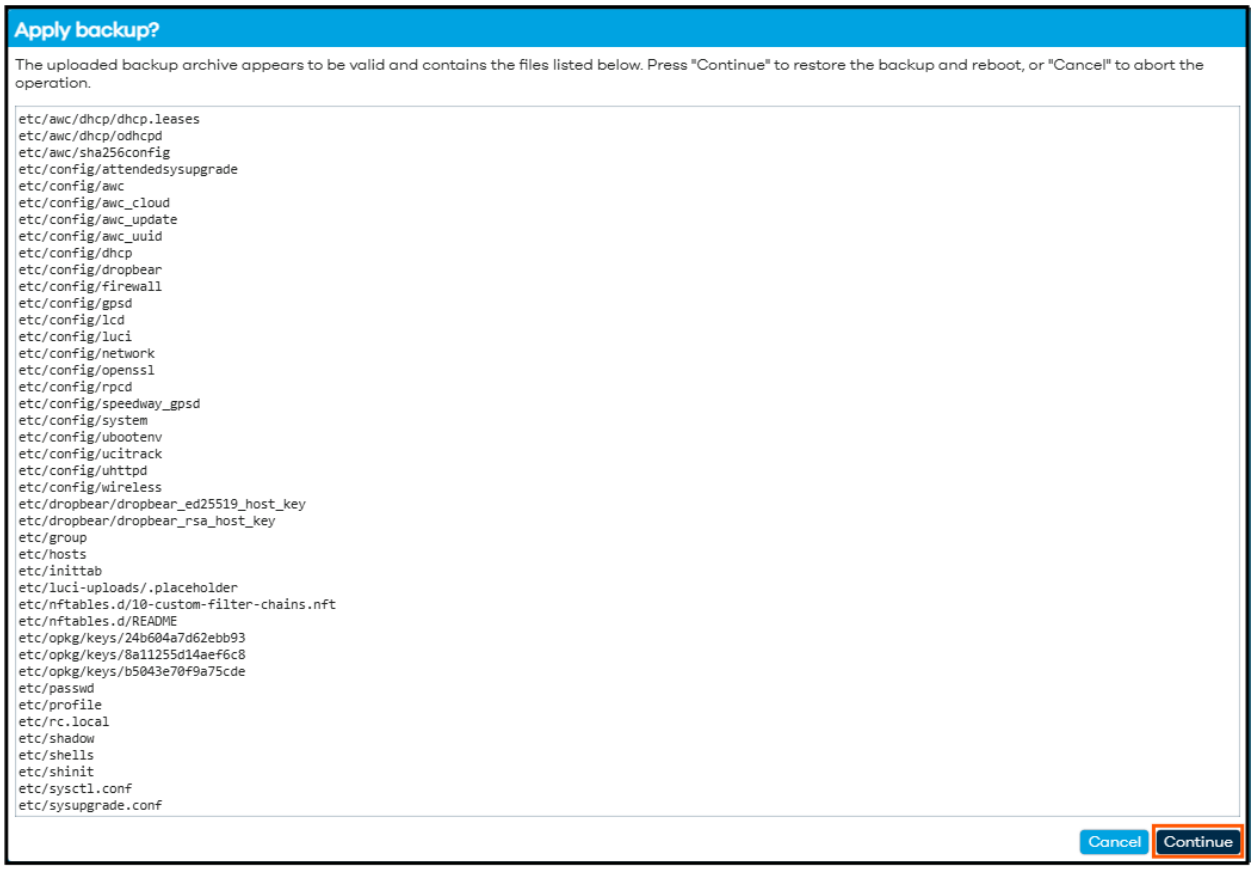


Figure 55: Apply backup – Confirmation to continue

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**.

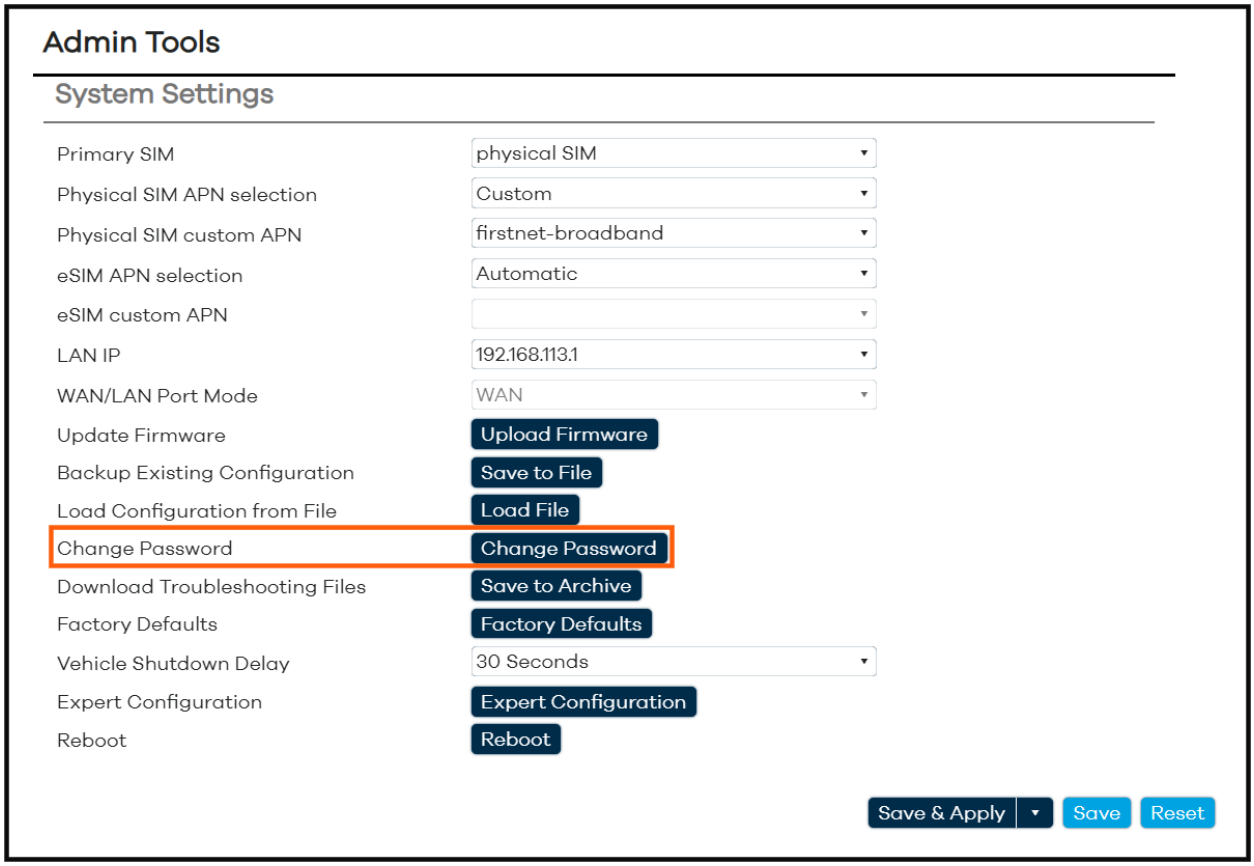


Figure 56: System Settings – Change Password button

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

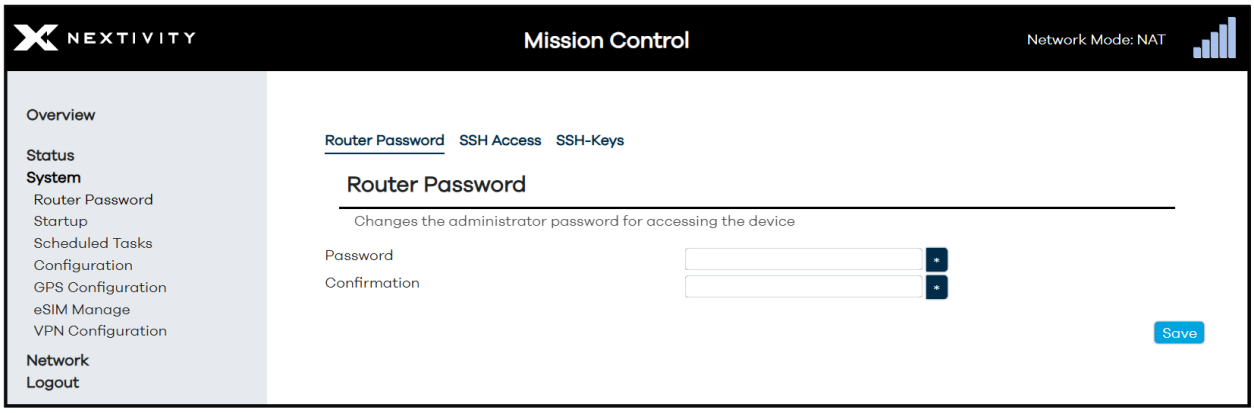


Figure 57: Router Password page – Expert Configuration Mode

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.

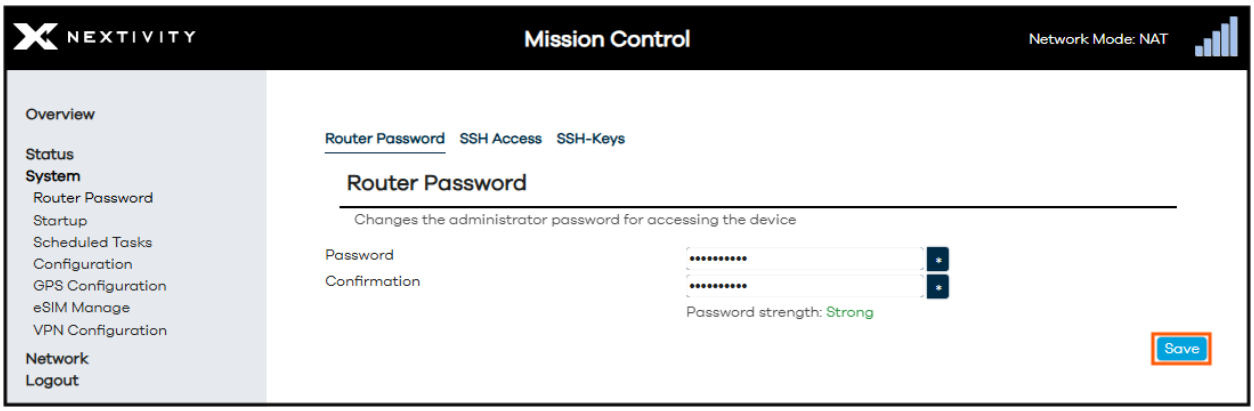


Figure 58: Router Password page – Enter new password

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**.

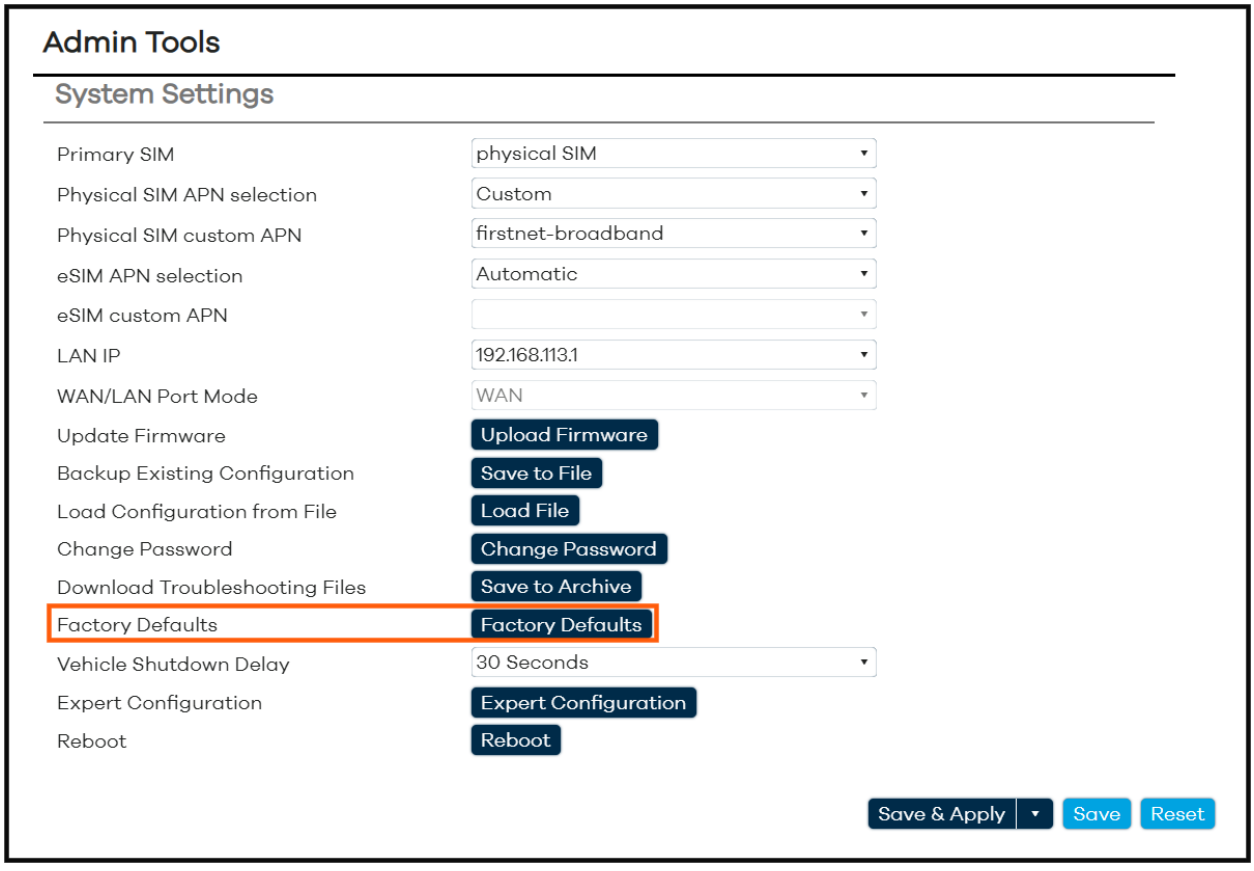


Figure 59: System Settings – Factory Defaults button

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

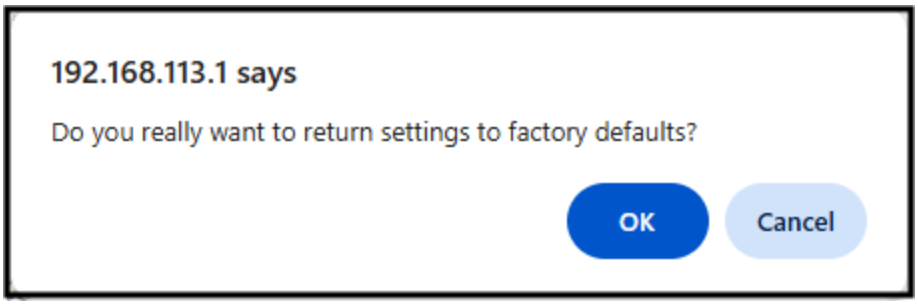


Figure 60: Confirmation to return settings back to factory defaults

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.

ⓘ 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**.

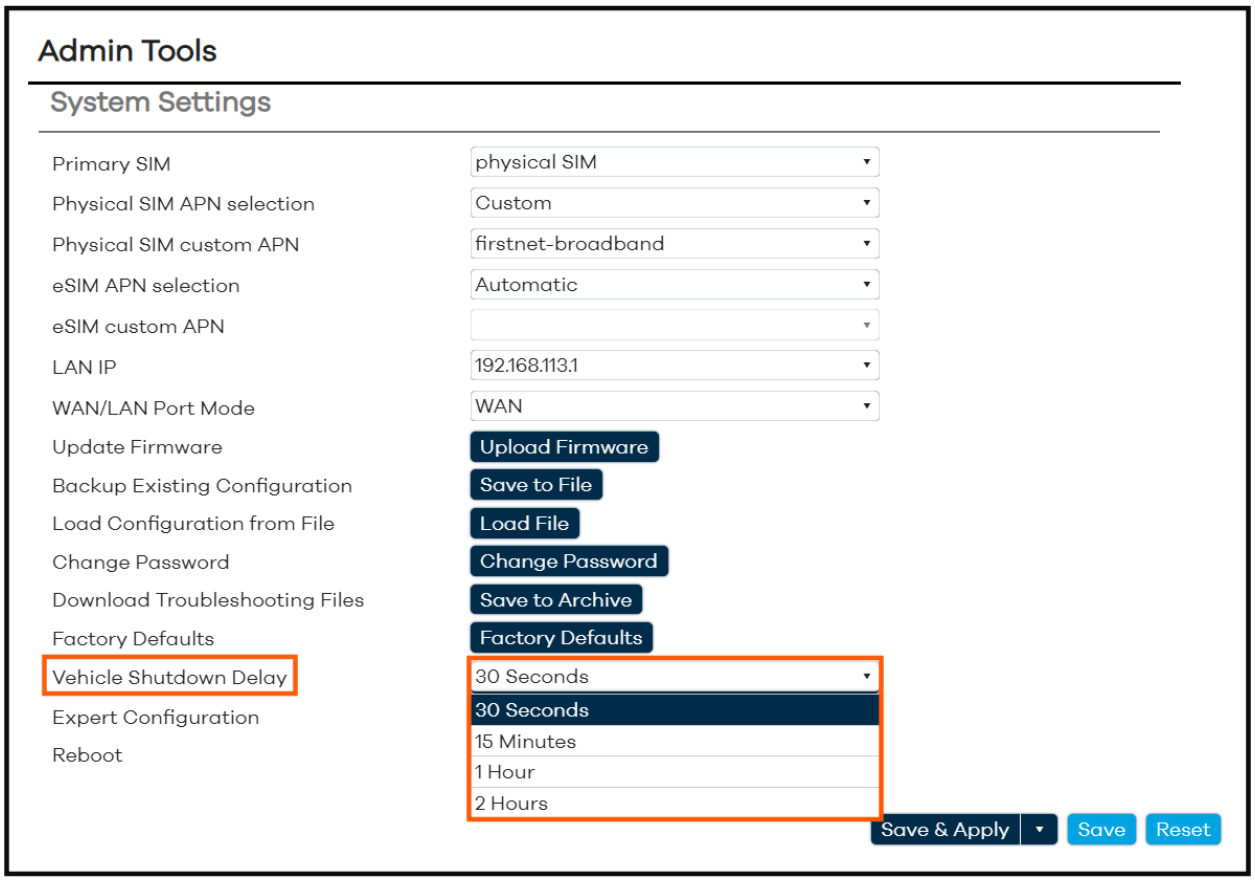


Figure 61: System Settings – Vehicle Shutdown Delay options

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.

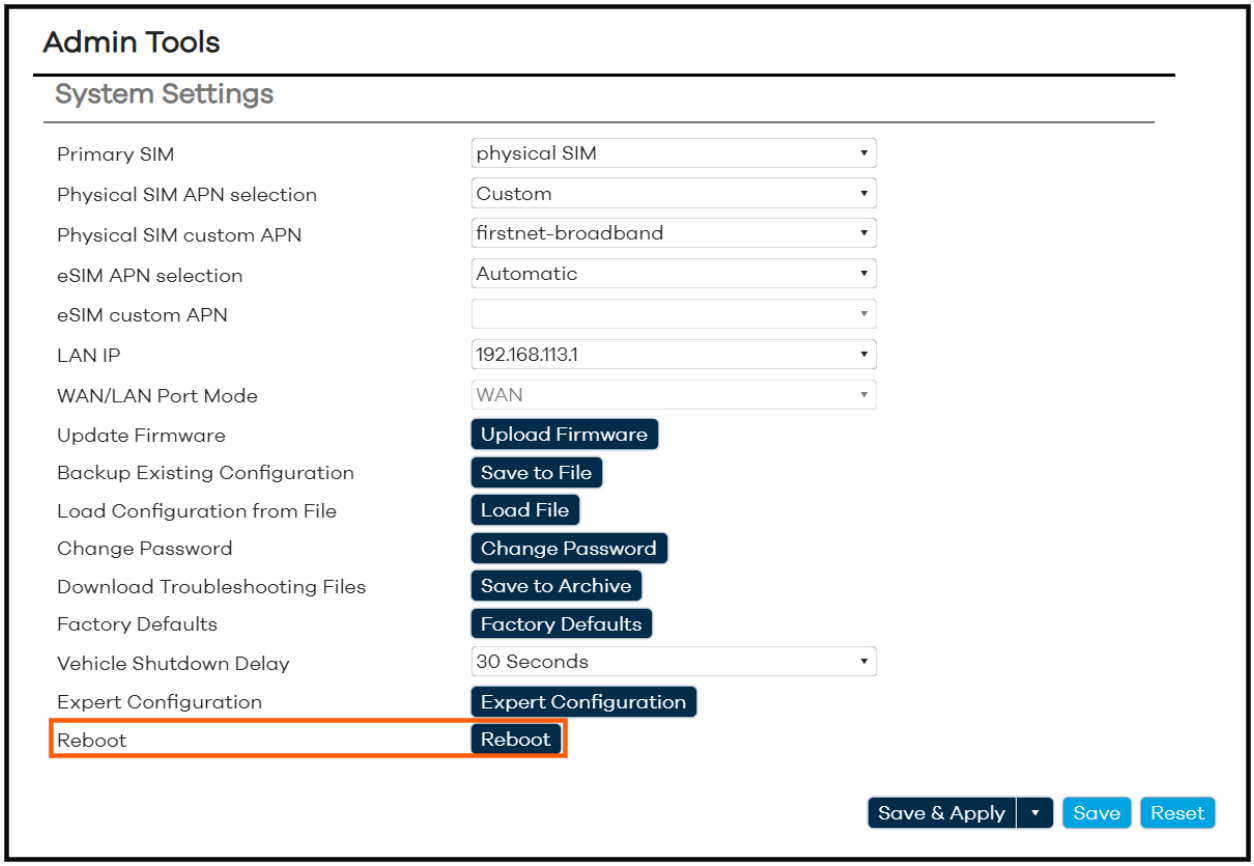


Figure 62: System Settings – Reboot button

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

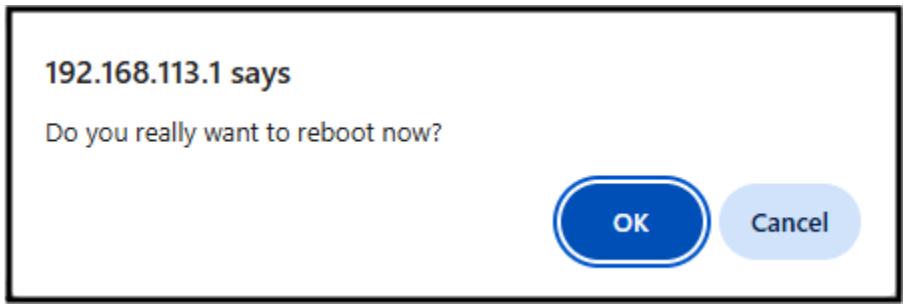


Figure 63: Confirmation message to reboot device

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.

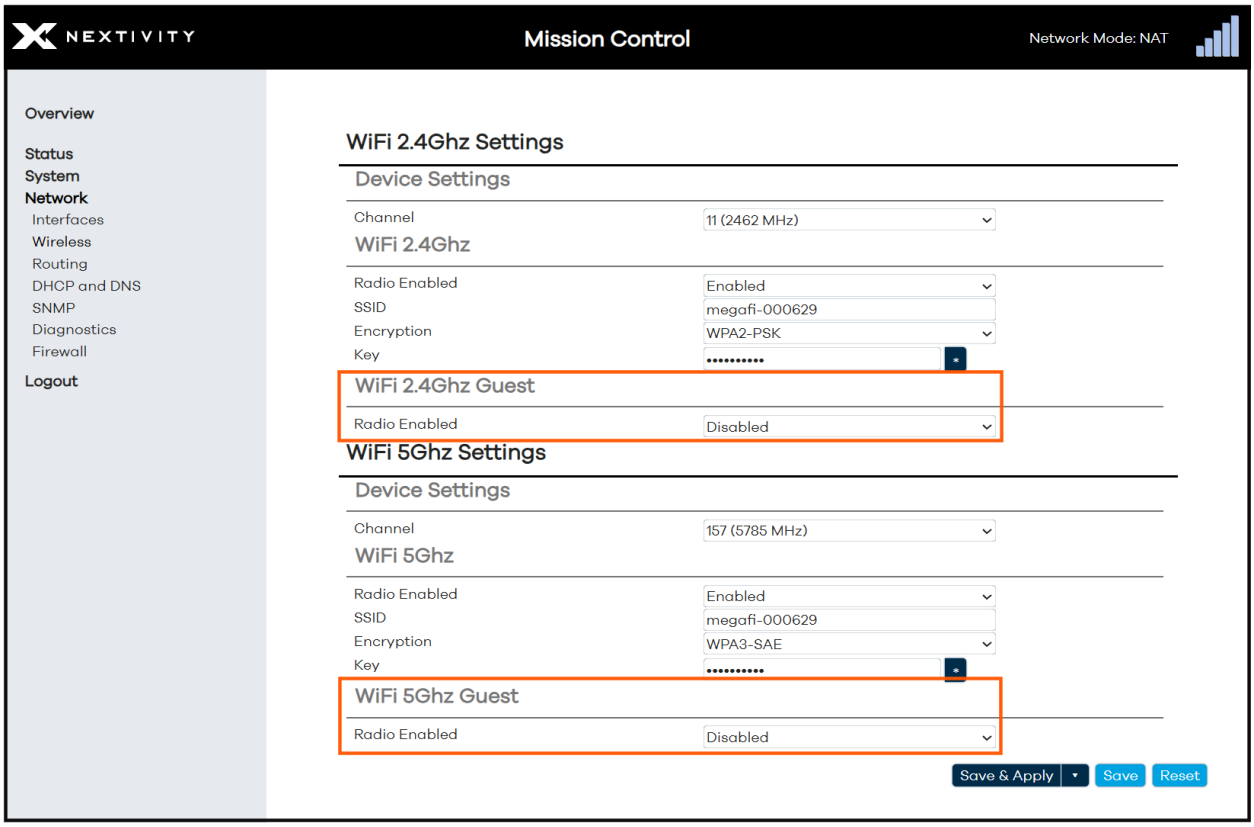


Figure 66: System Settings – Expert Configuration button

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.

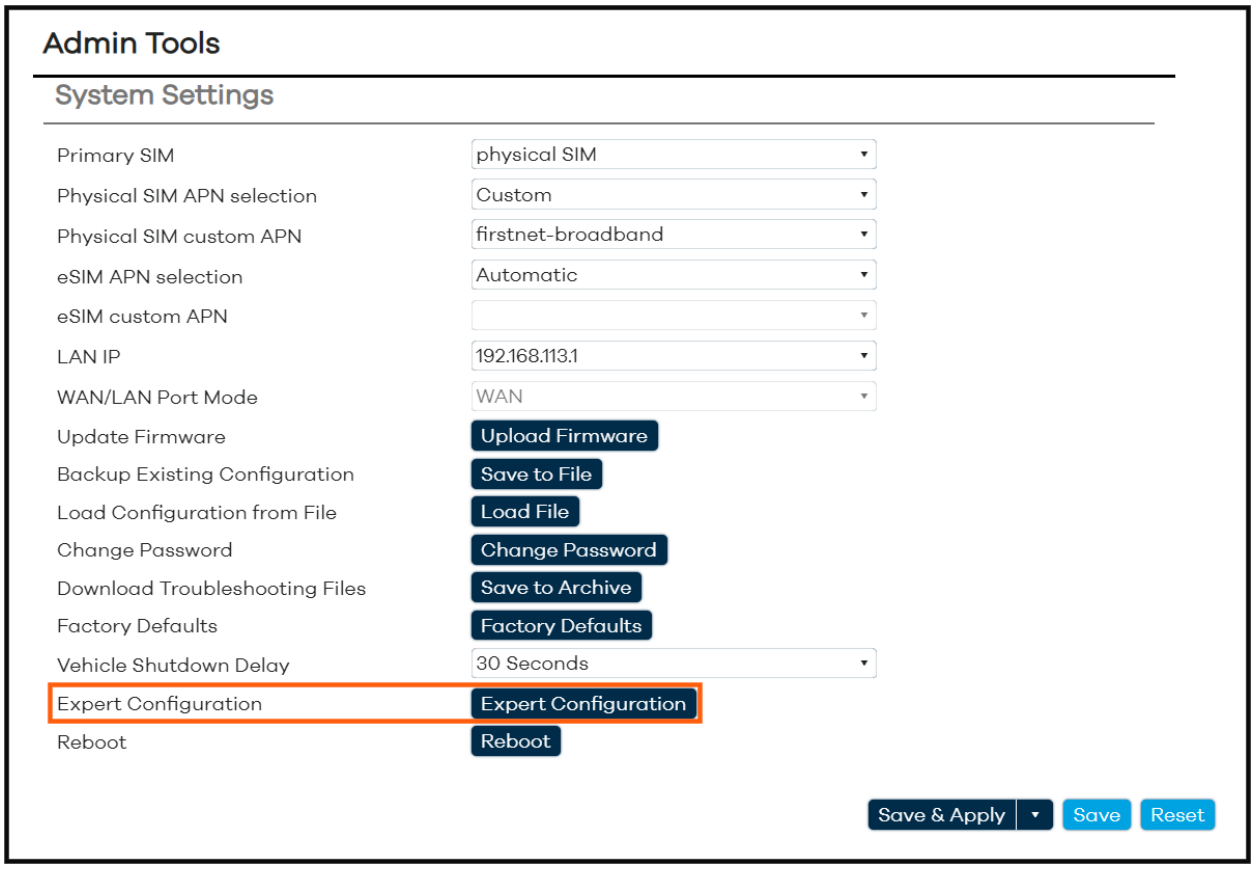


Figure 67: System Settings – Expert Configuration button

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

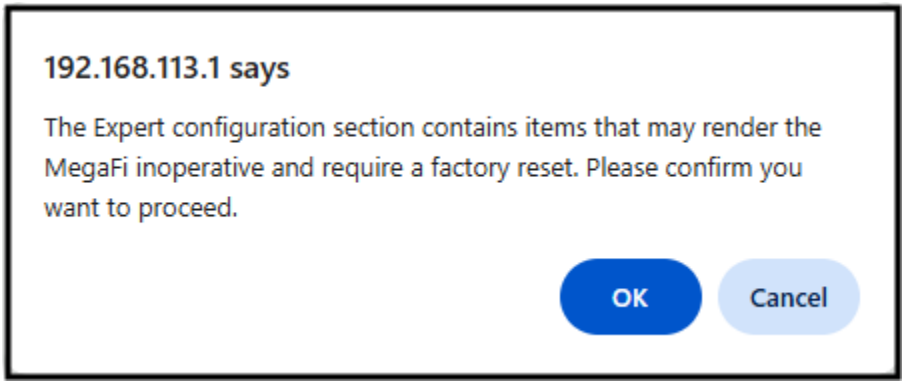


Figure 68: Confirmation message to enter Expert Configuration mode

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

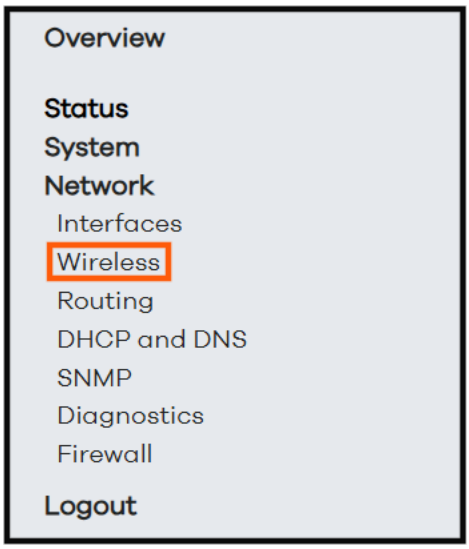


Figure 69: Navigation pane showing options available in Expert mode – Wireless

➲ **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.

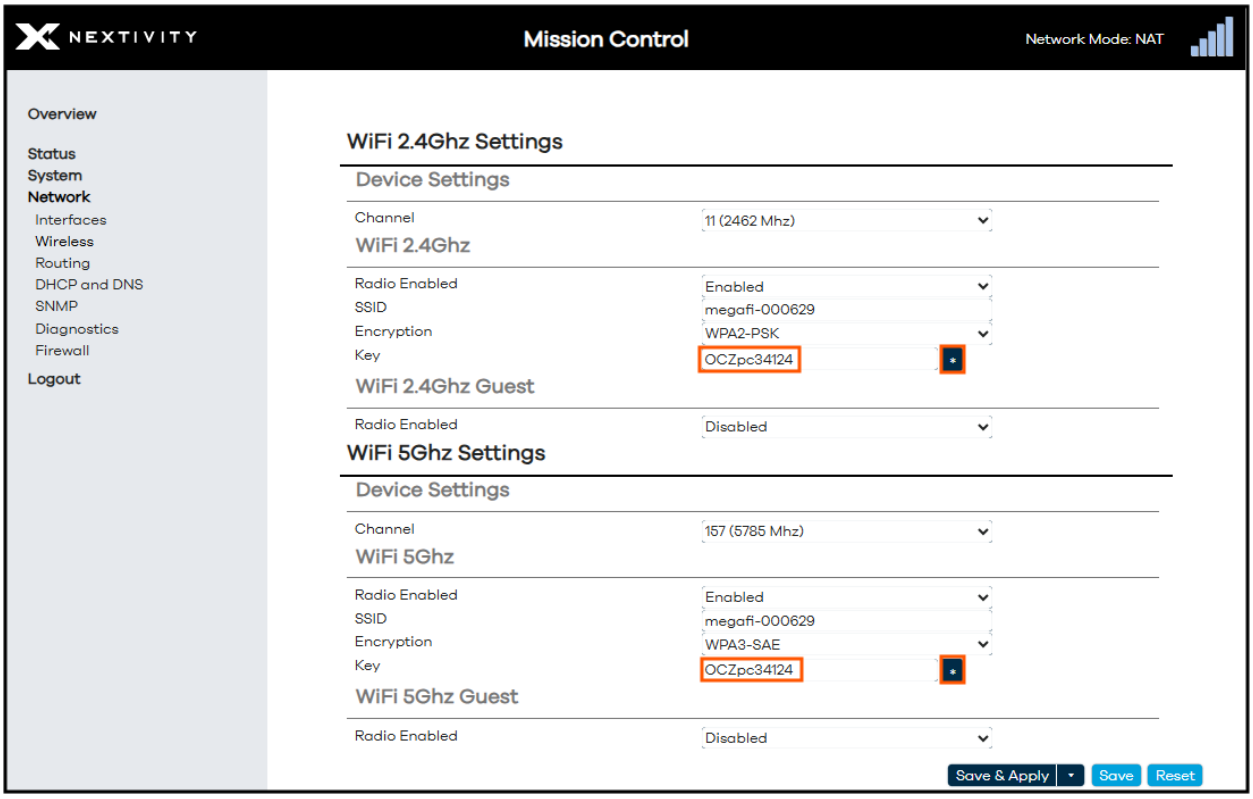


Figure 70: Wireless Settings – View hidden Keys

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.

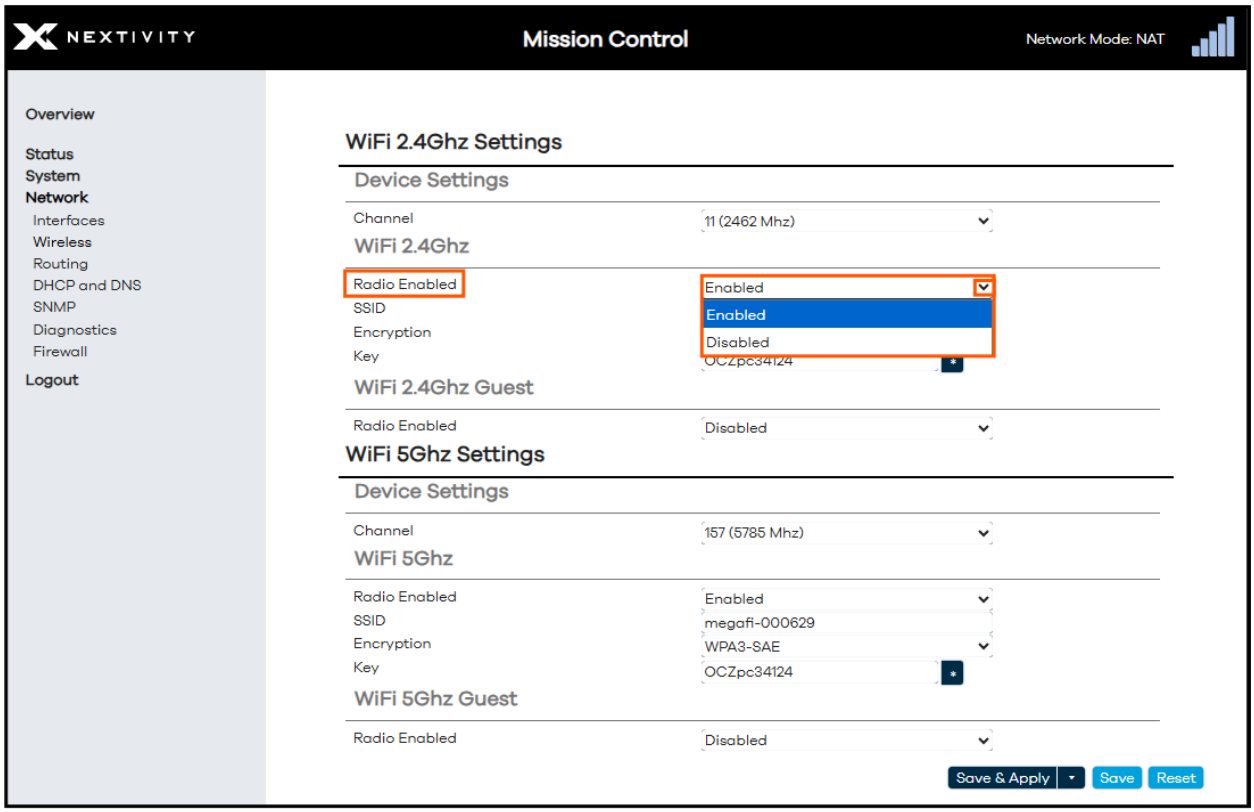


Figure 71: Wireless Settings – Selecting Drop-down Menu options

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.

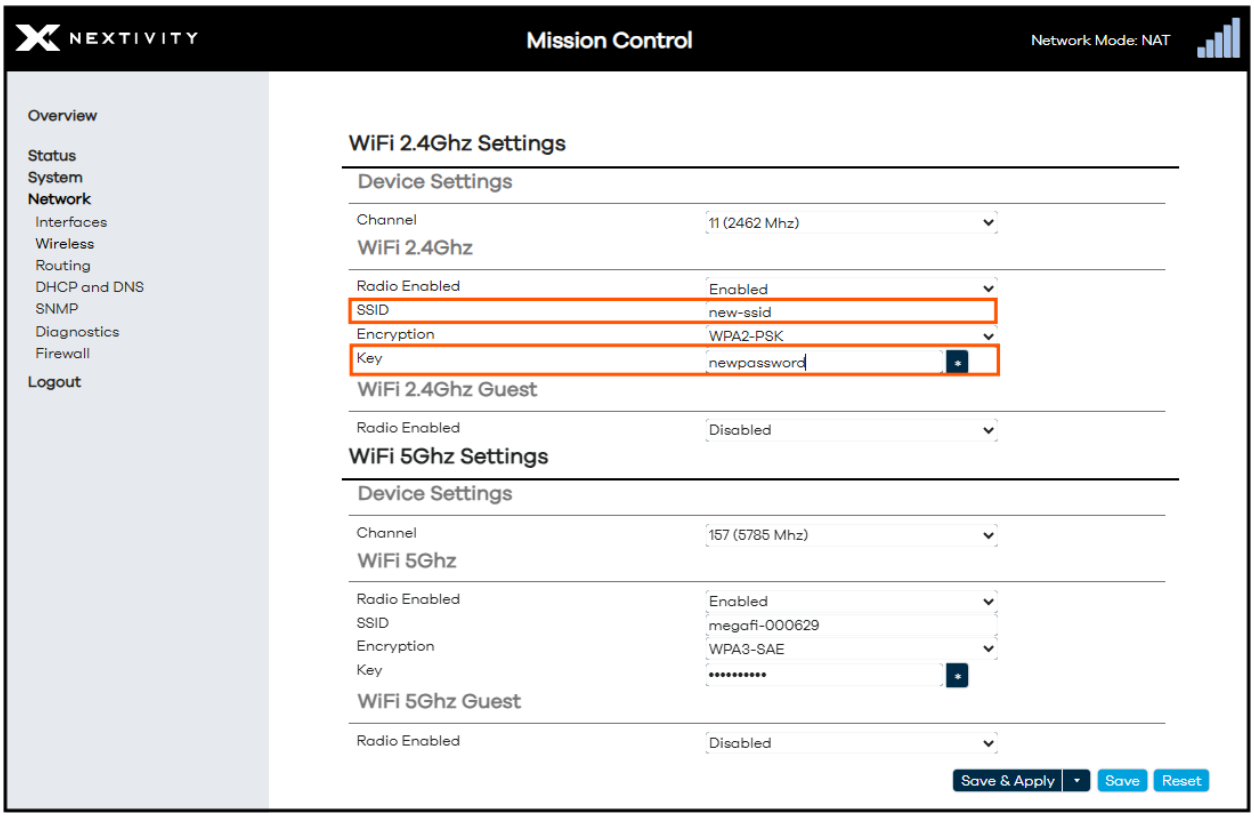


Figure 72: Wireless Settings – Modifying SSID and Key fields

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.

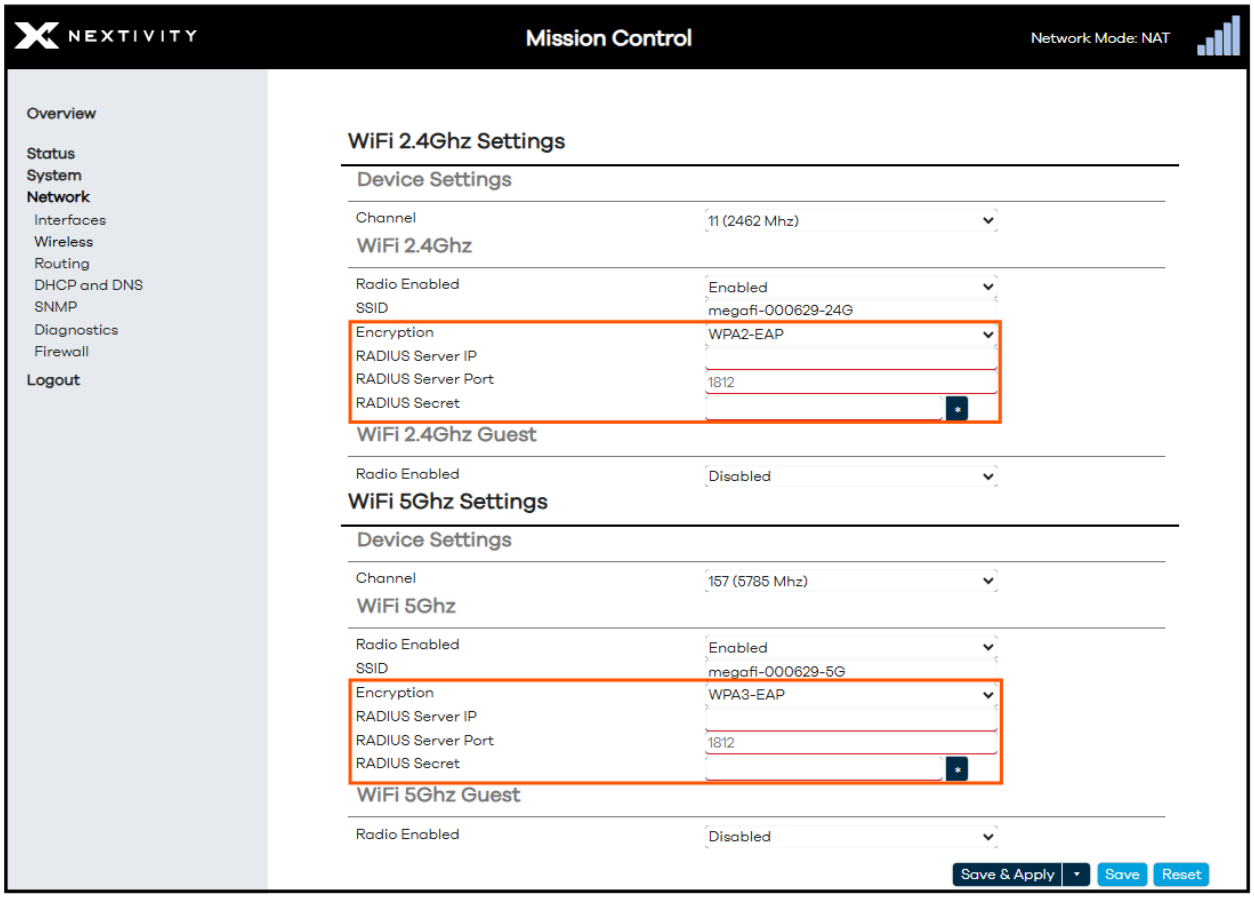


Figure 73: Wireless Settings – EAP fields

➲ **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.

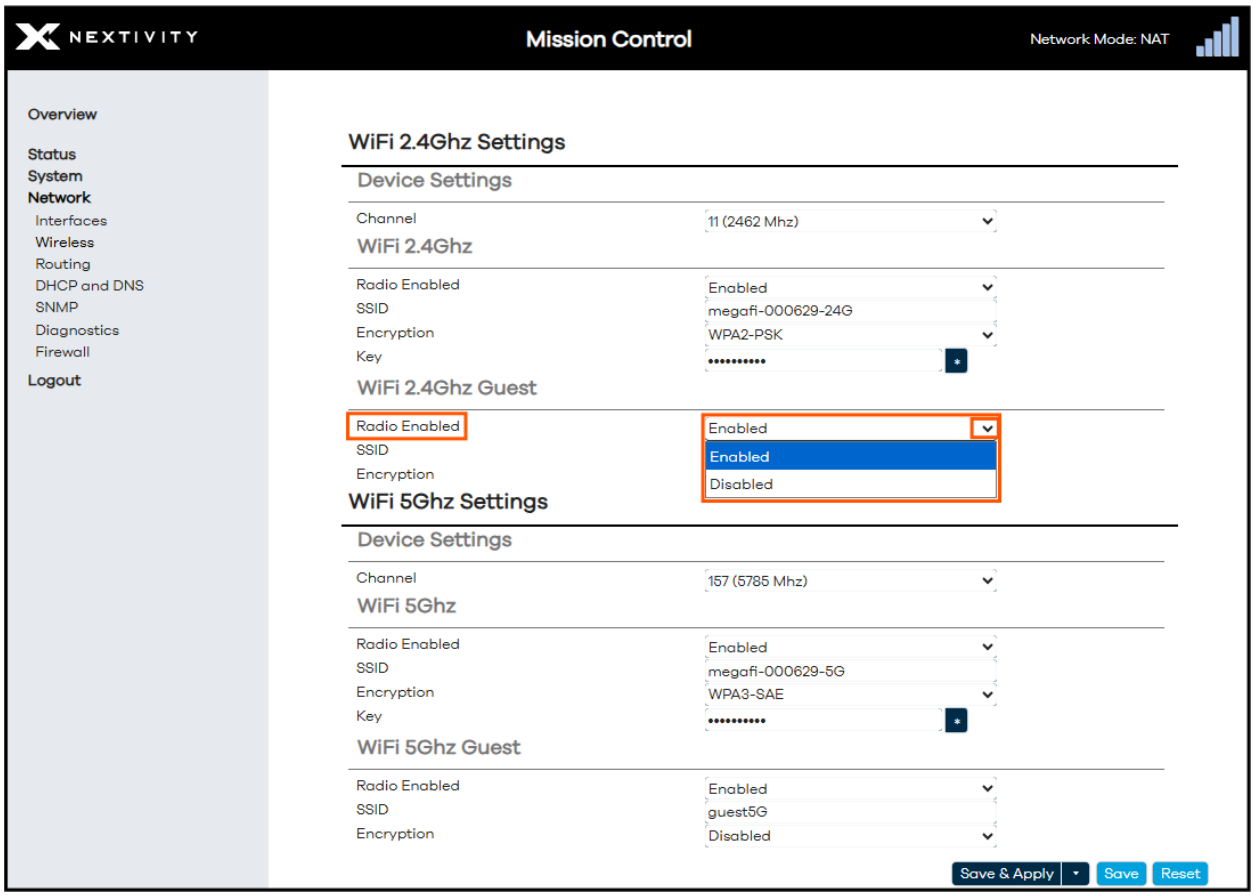


Figure 74: Guest Wireless Settings – Selecting Drop-down Menu options

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.

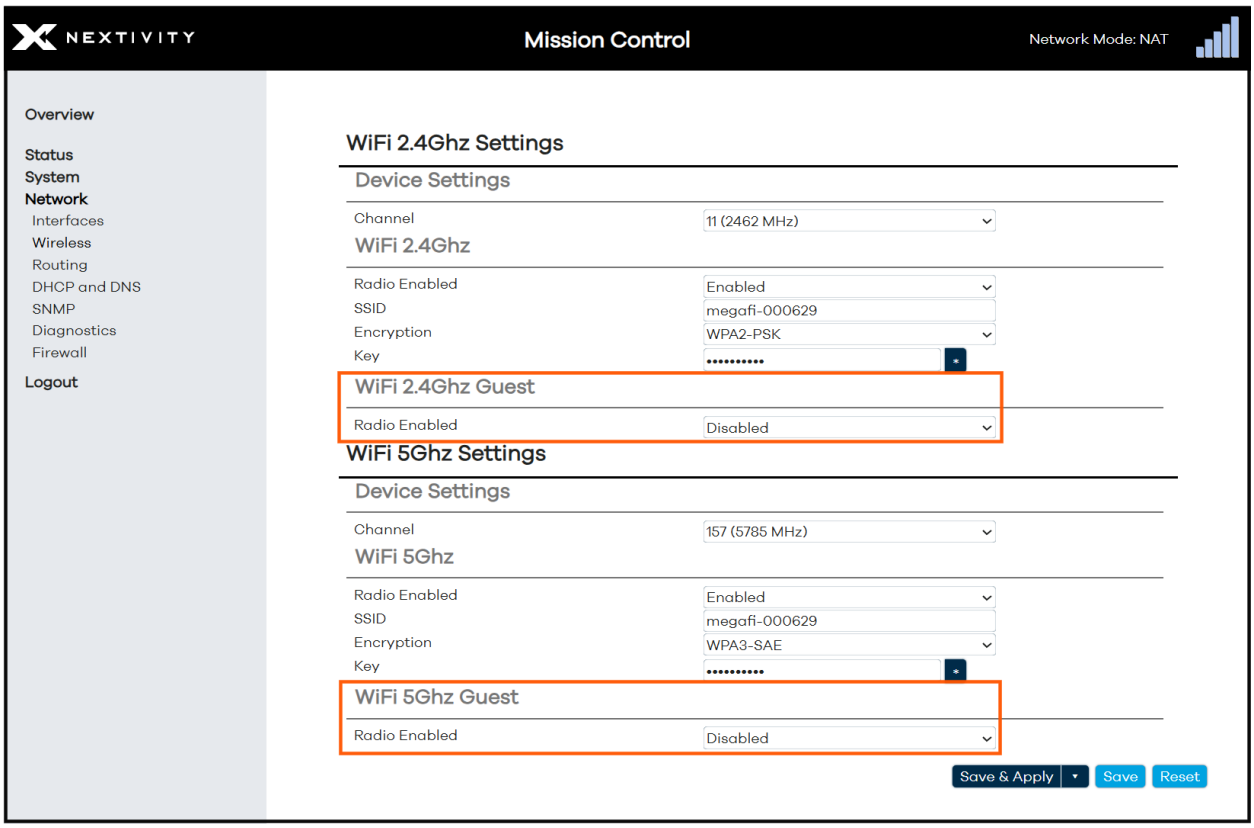


Figure 75: Guest Wireless Settings – EAP fields

➲ **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** and typical router functions. In this mode, the MegaFi will simply act as a bridge and forwards traffic as-is, allowing a connected device (such as a firewall or router) to handle the carrier assigned IP assignments and manage the network. The carrier assigned IP address will be assigned to the device directly connected behind the MegaFi 2 on the LAN 1 port, but the Subnet mask and Gateway can be modified as described below. 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, Wi-Fi, Firewall, and IPSec VPN functions.

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 connection to Mission Control cannot be resolved after a couple of minutes, 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.

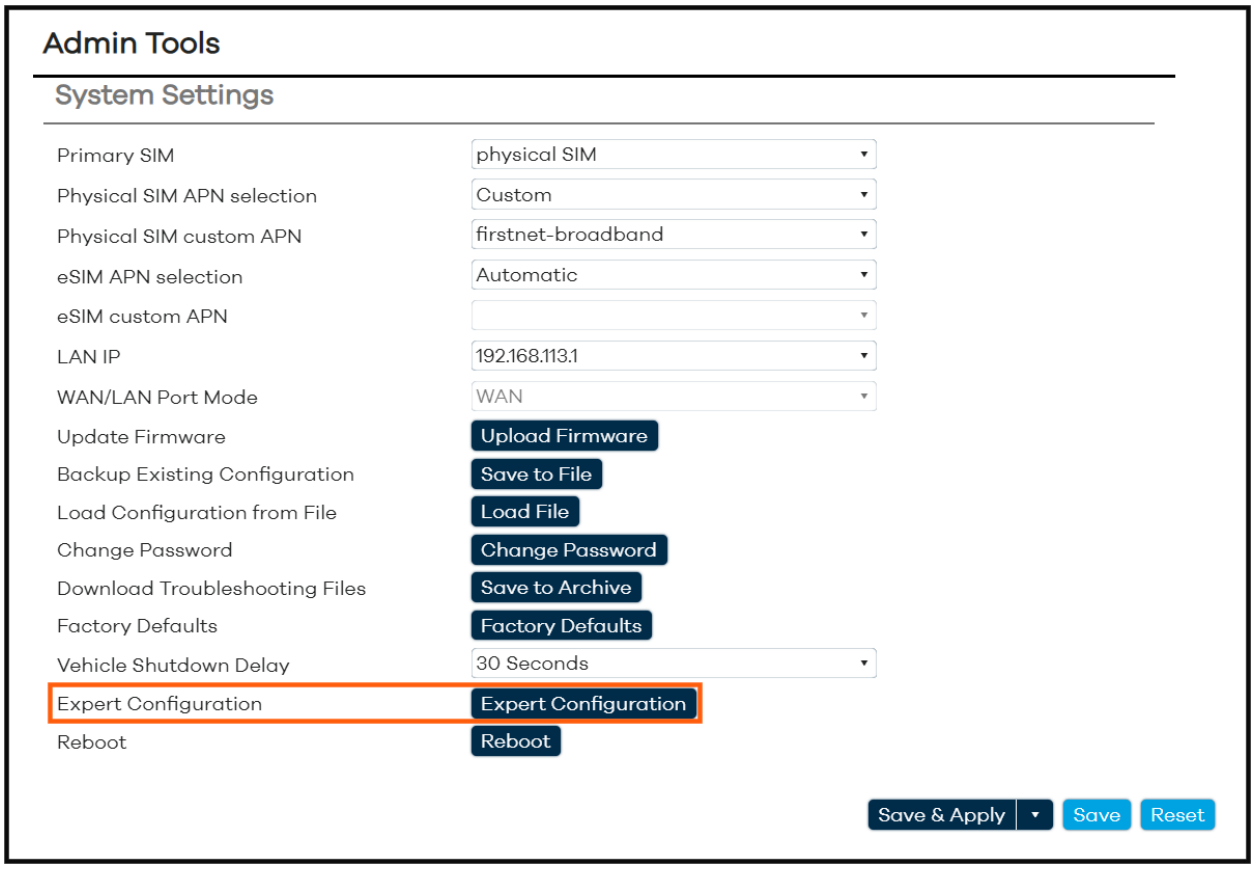


Figure 76: System Settings – Entering Expert Configuration mode

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

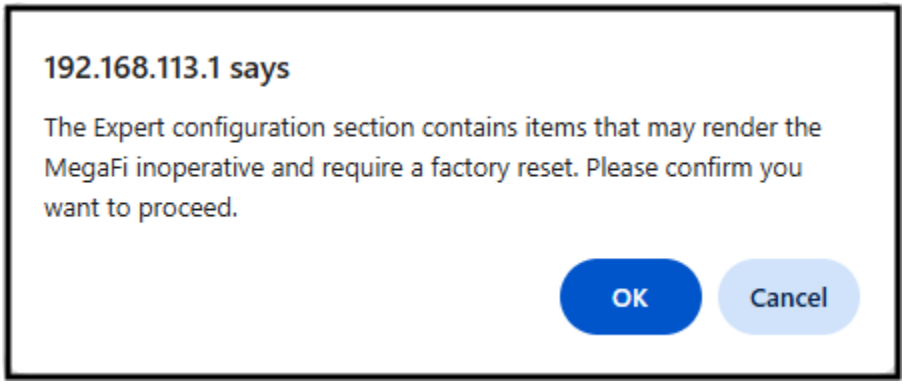


Figure 77: Confirmation message to enter Expert Configuration mode

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

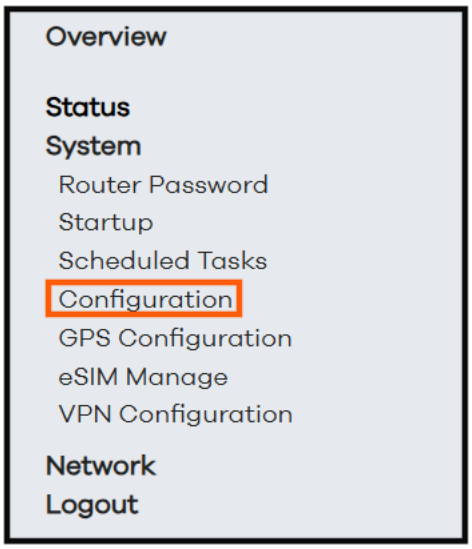


Figure 78: Navigation pane showing options available in Expert mode – Configuration

5. 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.

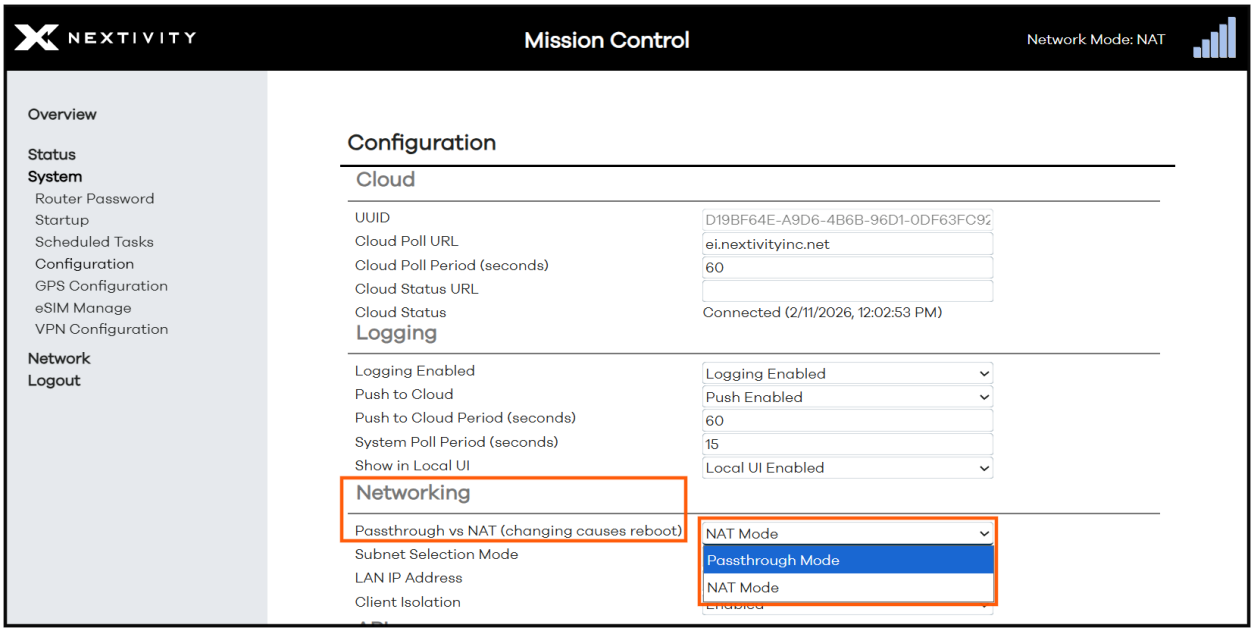


Figure 79: MegaFi 2 Configuration – Change modes (NAT or Passthrough)

6. 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.

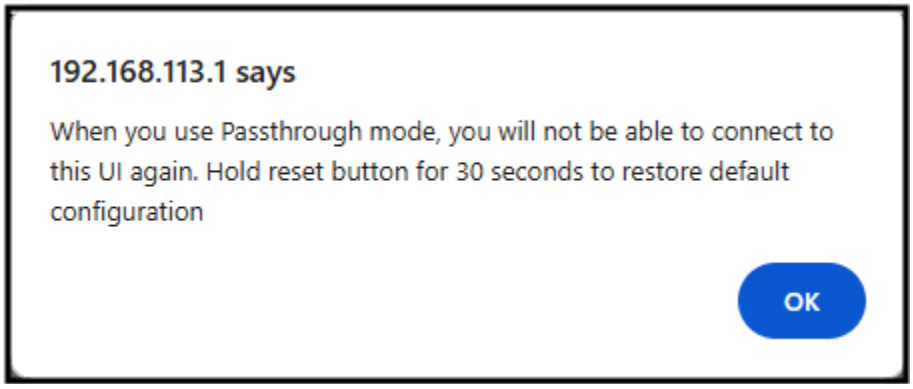


Figure 80: MegaFi 2 Configuration – Change modes (NAT or Passthrough)

7. Select the desired **Subnet Selection Mode** from the dropdown menu (**Force 24 Subnet (Compatibility Mode)** or **Automatically Create Subnet**).

    - **Force 24 Subnet (Compatibility Mode)** – this is the default selection. This selection forces a class C subnet (i.e. 255.255.255.0 or /24 in CIDR form) regardless of what the carrier has assigned. This will also use the first available IP address in the /24 block as the Gateway IP address.

      Use case:

        - Only use this if the downstream device **cannot operate** with the carrier's native subnet. For example, downstream devices cannot handle small or non-standard WAN subnets like /31 or /30.
        - Helpful in environments where firewalls insist on a /24 WAN network.
        - This compatibility mode avoids issues where the carrier's assigned IP/mask combination:
            - falls into a non-usable network/broadcast range, or
            - results in overlapping networks at multiple sites.
    - Automatically Create Subnet – This selection dynamically creates the subnet mask based on whatever subnet the carrier assigns to the modem. This also designates the server that assigned the IP address to the modem as the Gateway IP address.

      Use case:

        - Works best when the carrier assigns /31, /30, /29 or unusual subnet masks.
        - Ensures IP Passthrough functions correctly without manual intervention.

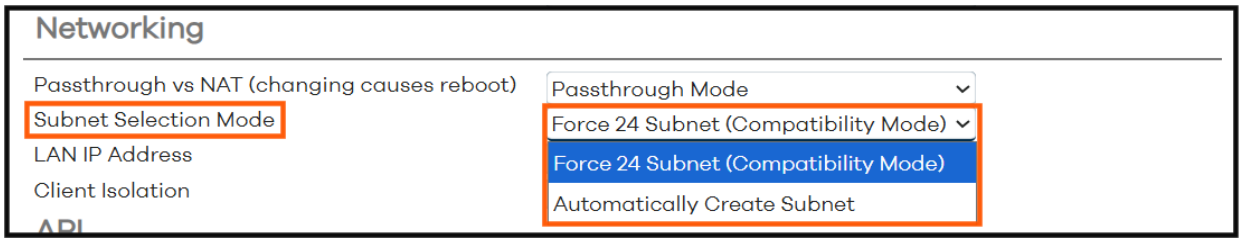


Figure 81: MegaFi 2 Configuration – Subnet Selection Mode

8. 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.

9. Once Mission Control access is re-established, login again to Mission Control.
10. 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.
11. Once in **Passthrough Mode**, connect the desired device to LAN port 1. Give the MegaFi and the device a couple of minutes to properly reconfigure themselves. If the device does not properly obtain the expected IP address information, follow these added steps:
    - 11a. Power down both the MegaFi 2 and the device connected to LAN port 1.
    - 11b. Verify that the Ethernet patch cable is properly interconnecting both the MegaFi 2 via its LAN port 1 interface and the device's **WAN** port. If the device is another computer, it will be its Ethernet port.
    - 11c. Power up both devices.
    - 11d. Ensure that the connected device receives the appropriate IP address. Follow instructions from the device manufacturer to validate the IP address.
12. If connectivity becomes an issue to Mission Control, try one of the following actions to regain access to MegaFi 2:
    - 12a. Refresh the web browser to Mission Control.
    - 12b. 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.
    - 12c. 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

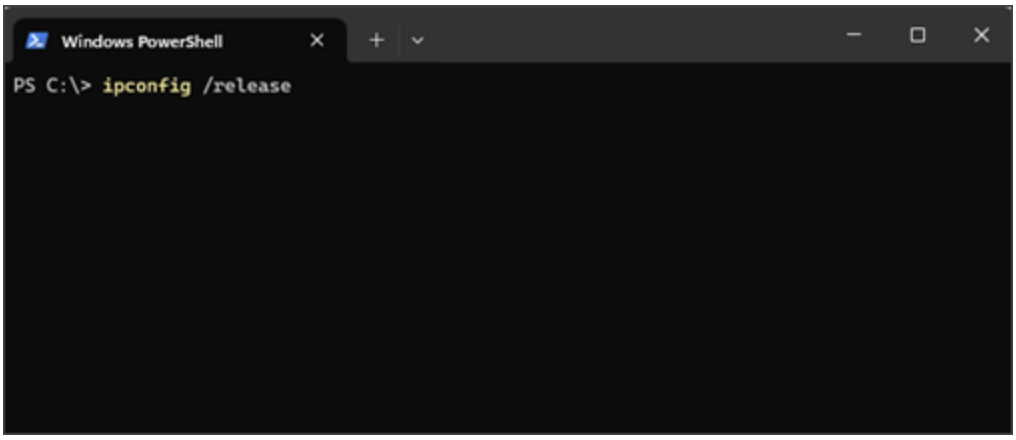


Figure 82: Windows PowerShell window – ipconfig /release <enter>

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

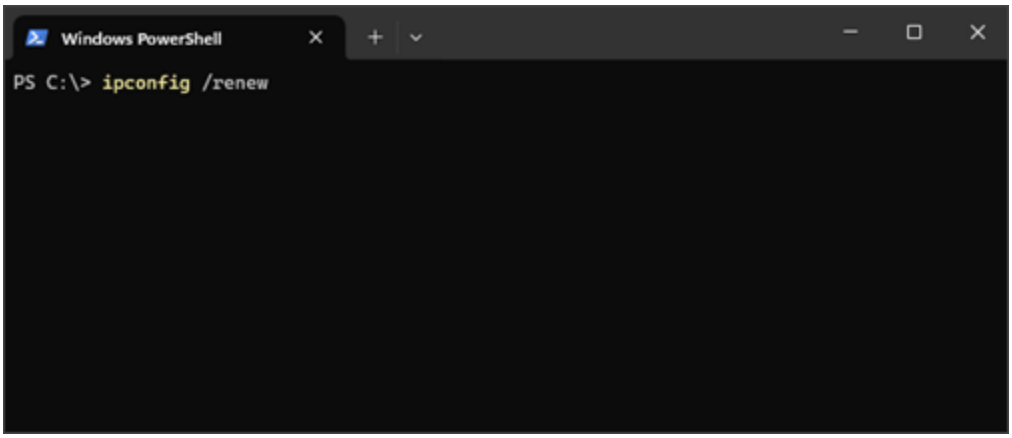


Figure 83: Windows PowerShell window – ipconfig /renew <enter>

13. 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, Band 1, and Band 30 Settings

In certain situations, the user may need to **Band Lock** to band 14 or 28. Also, Band 1 and Band 30 can be either enabled or disabled as needed depending on Mobile or Fixed setups. To do so, do the following in Mission Control:

3.12.1 Band Lock Setting

➲ **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.

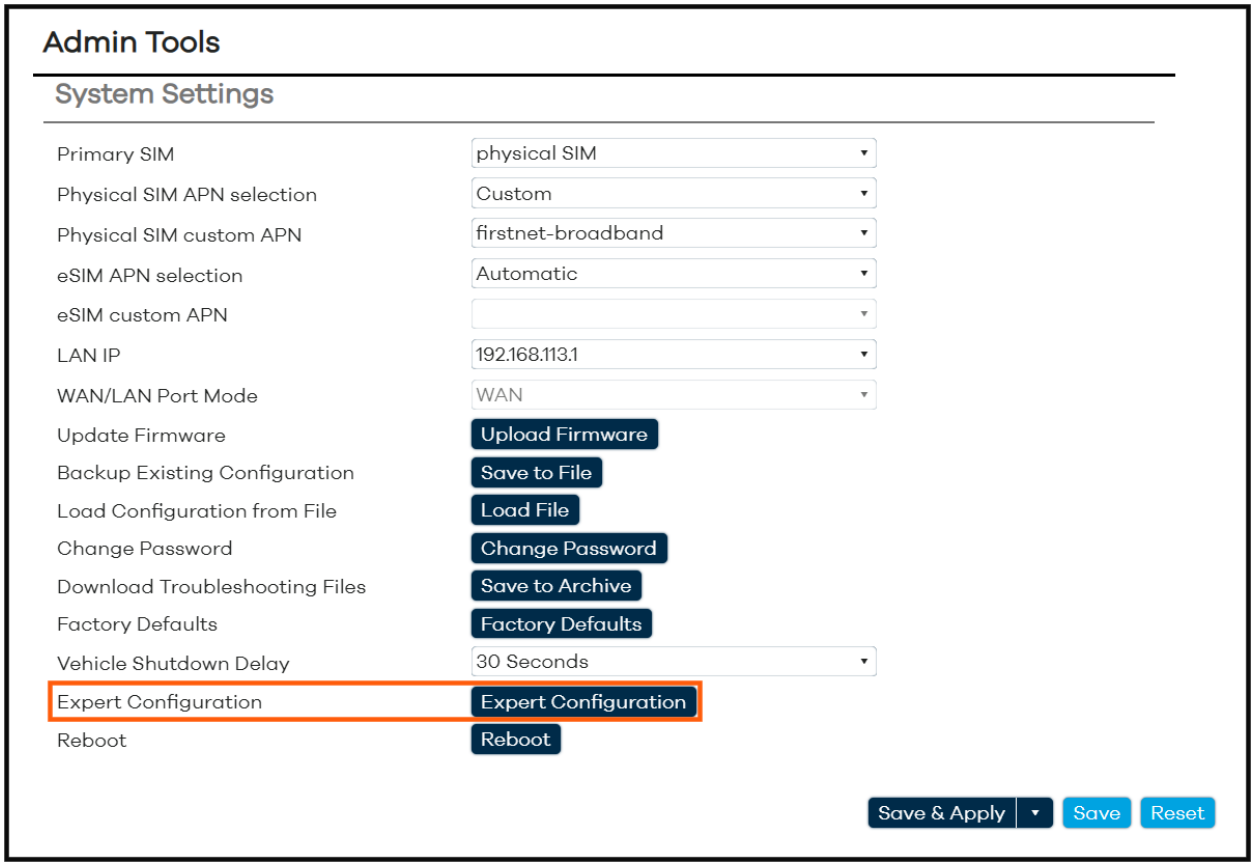


Figure 84: System Settings – Expert Configuration button

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

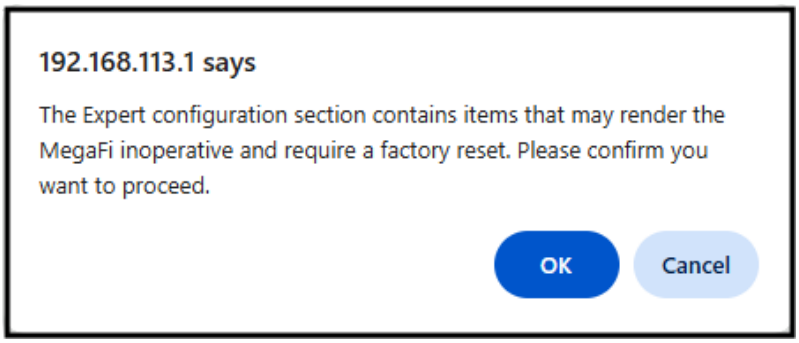


Figure 85: Confirmation to Enter Expert Configuration mode

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

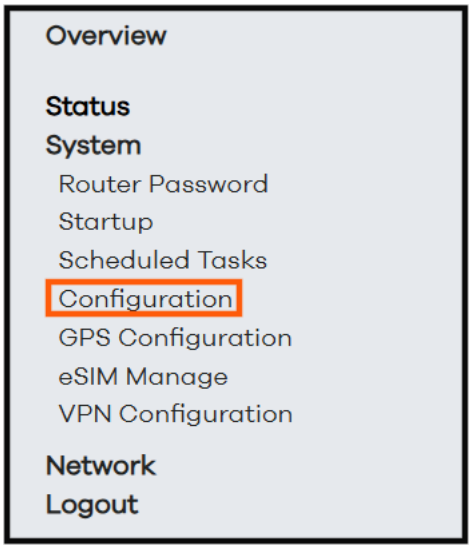


Figure 86: Navigation pane showing options available in Expert mode – Configuration

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.

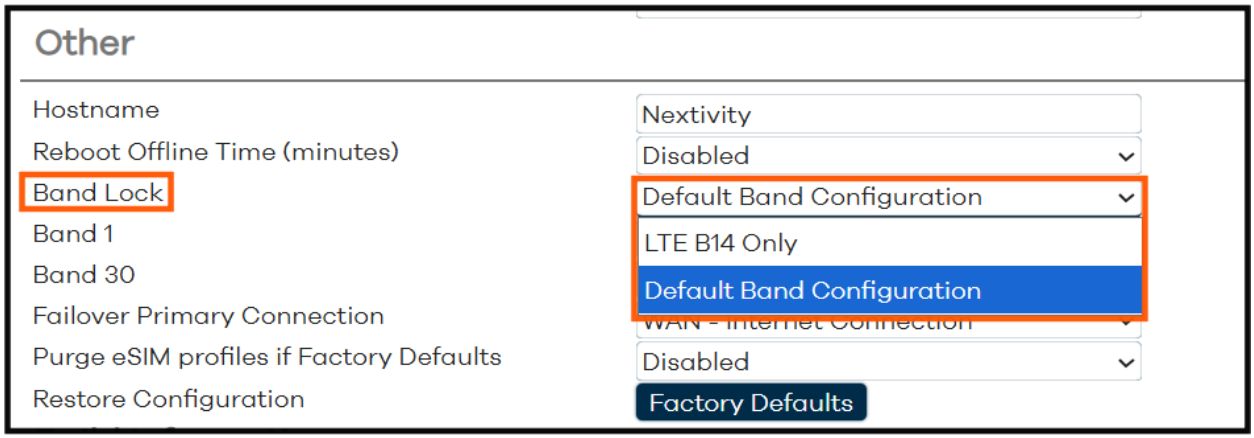


Figure 87: Band Lock Setting

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.

3.12.2 Band 1 and Band 30 Settings

By default, Band 1 is disabled (Mobile applications) and Band 30 is enabled (Fixed applications). So by default, the settings are set to a Fixed application.

To enable or disable these settings per your specific application, do the following in Mission Control:

1. These settings are located right below the Band Lock setting.

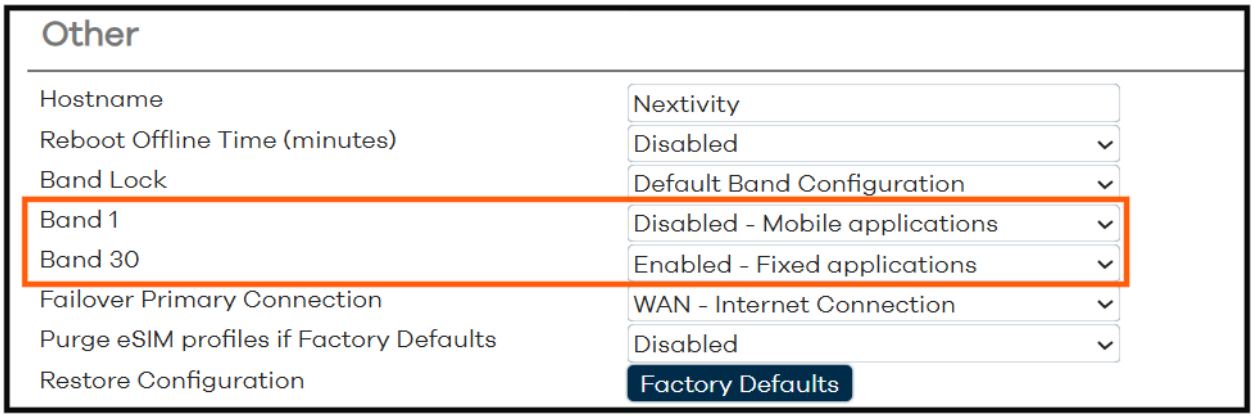


Figure 88: Band 1 and Band 30 Settings

2. Select the dropdown menu on either setting and select the opposite setting for either a Mobile or Fixed application.
3. Click on **Save & Apply** to confirm the change.
4. 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.

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

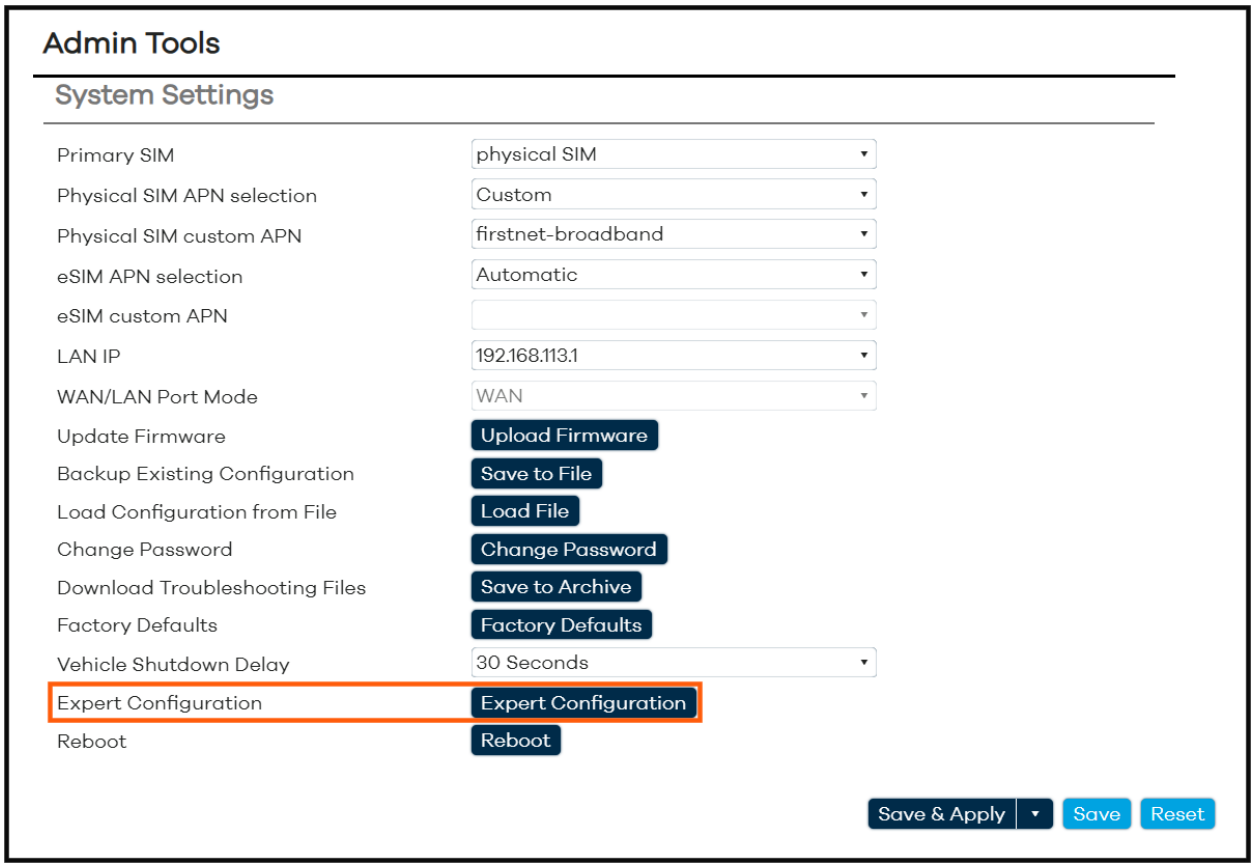


Figure 89: System Settings – Expert Configuration

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

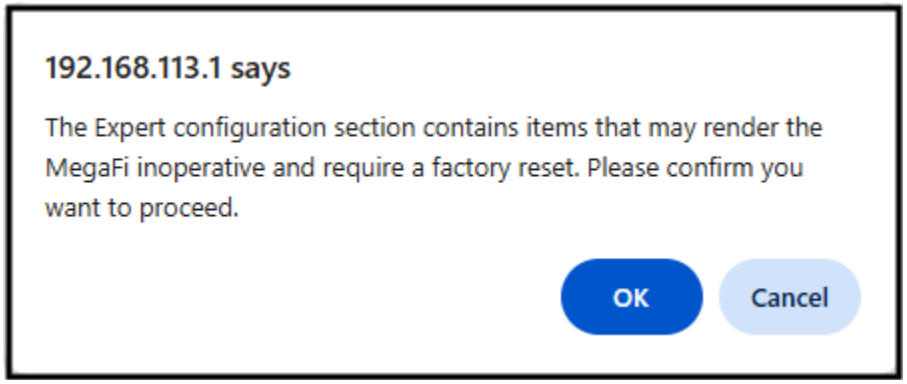


Figure 90: Confirmation to Enter Expert Configuration mode

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

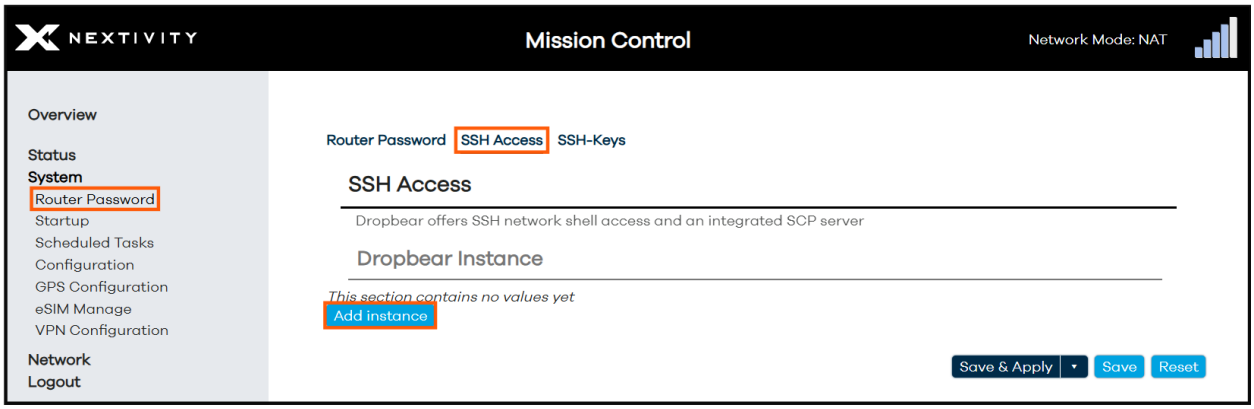


Figure 91: SSH Access – add new instance

10. Click on the **Add instance** button.
11. 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.
12. 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).
13. **Idle Timeout** is set to **300** seconds by default. Adjust for more or less time in seconds as needed.
14. All other settings are not required and are optional.
15. Click on **Save & Apply** to confirm changes.

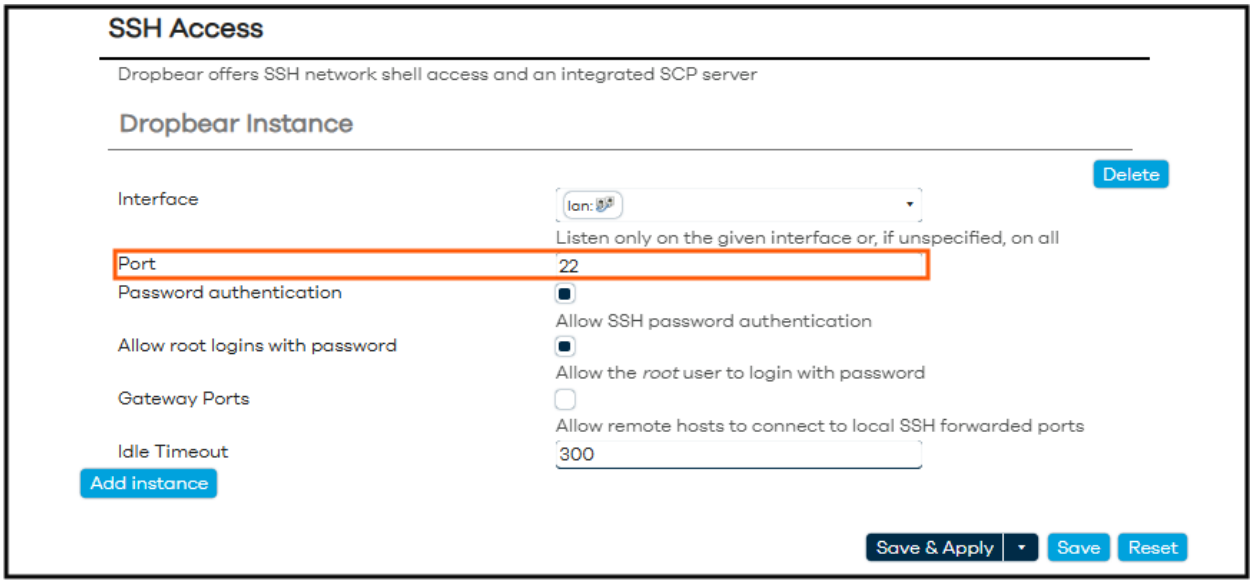


Figure 92: SSH Access – Change port number from 2022 to 22

16. 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.

17. **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:

    17a. Within the **SSH Access** page, click on **Add instance**.

    17b. 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

    17c. Choose a port such as 46556 or something similar that is not the typical SSH port 22.

    17d. It is recommended to leave the **Idle Timeout** set to **300** or less for **wan** access for security reasons.

    17e. All other settings are not required and are optional.

    17f. 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.

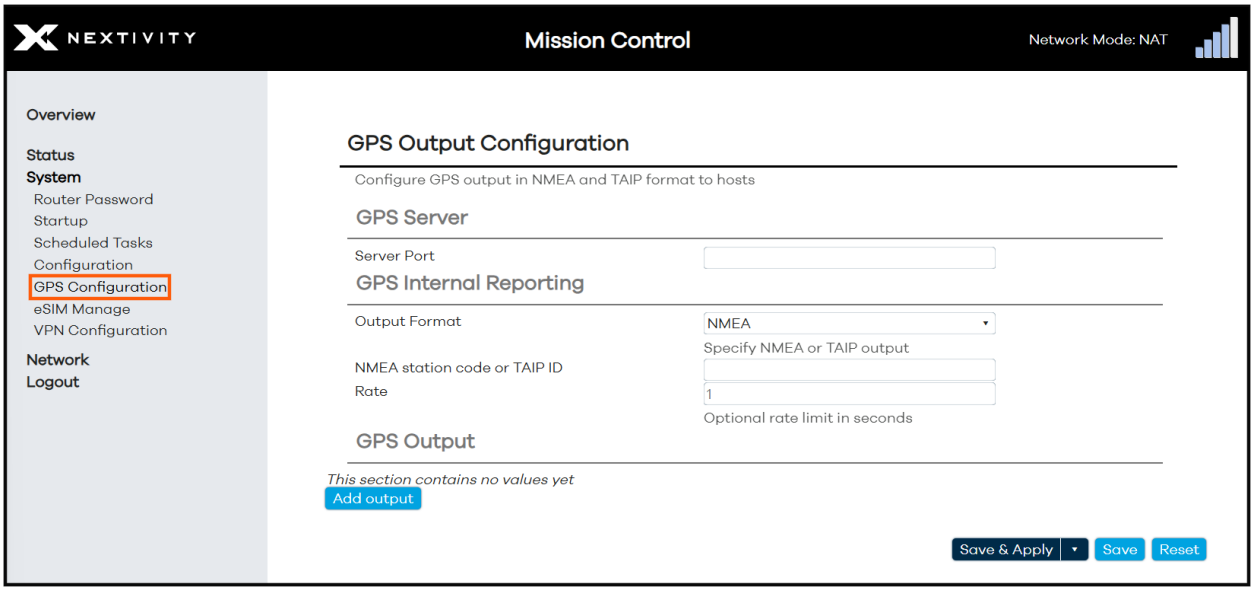


Figure 93: GPS Output Configuration page

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.

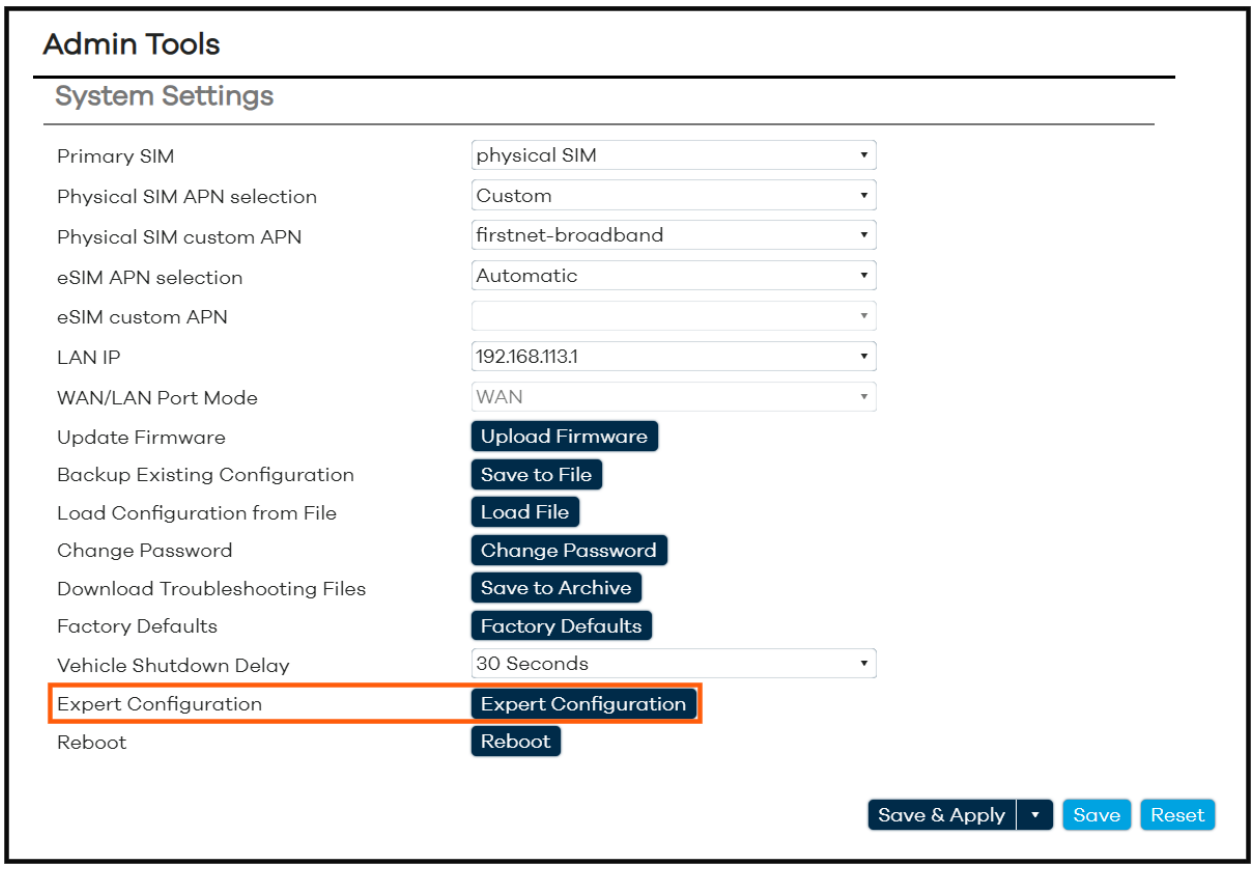


Figure 94: System Settings – Expert Configuration

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

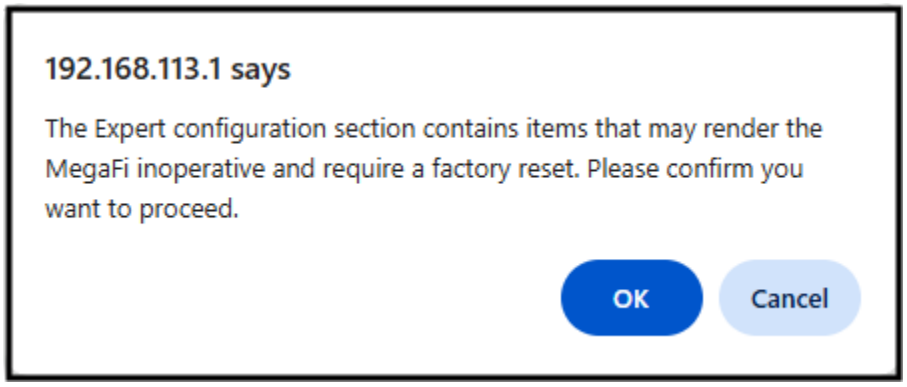


Figure 95: Confirmation to Enter Expert Configuration mode

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:

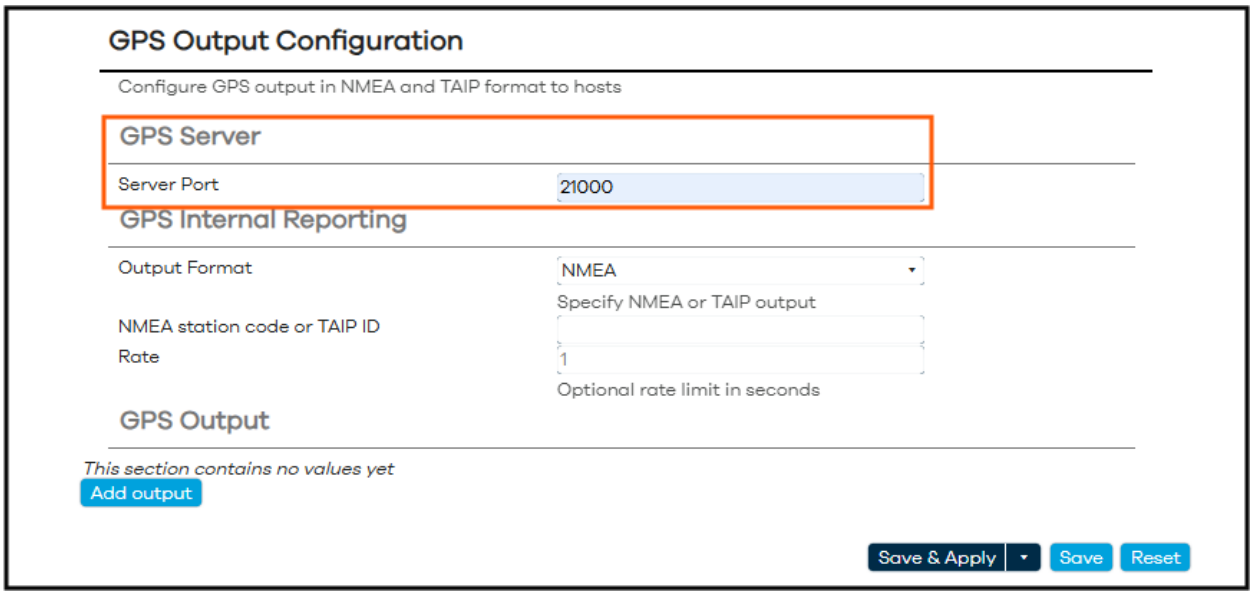


Figure 96: GPS Server Port Configuration

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.

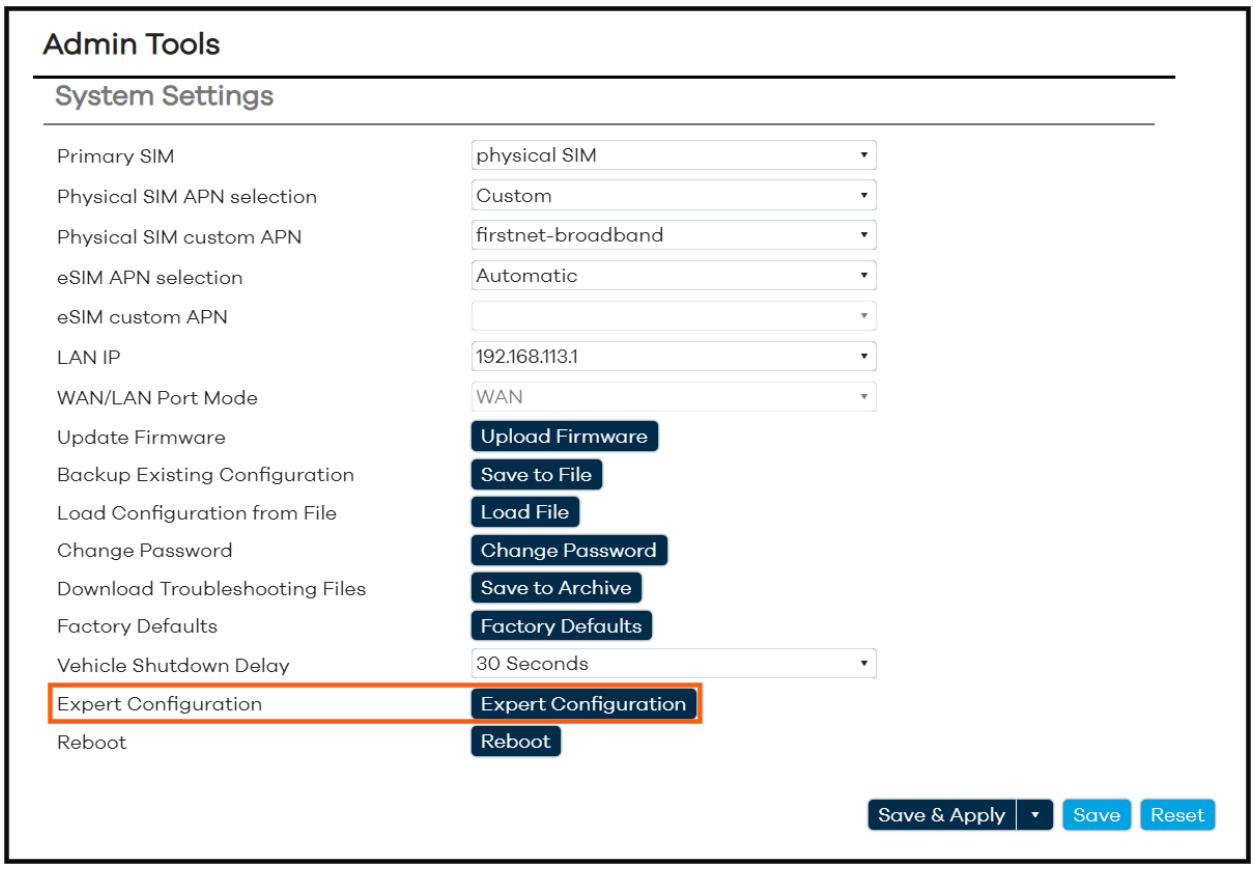


Figure 97: System Settings – Expert Configuration

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

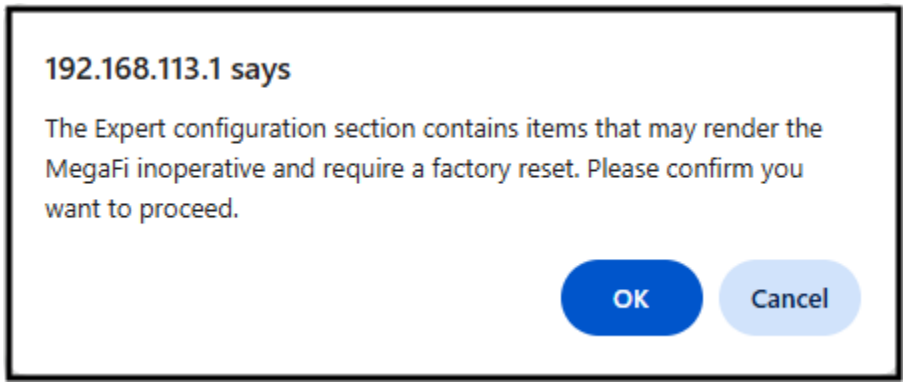


Figure 98: Confirmation to Enter Expert Configuration mode

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

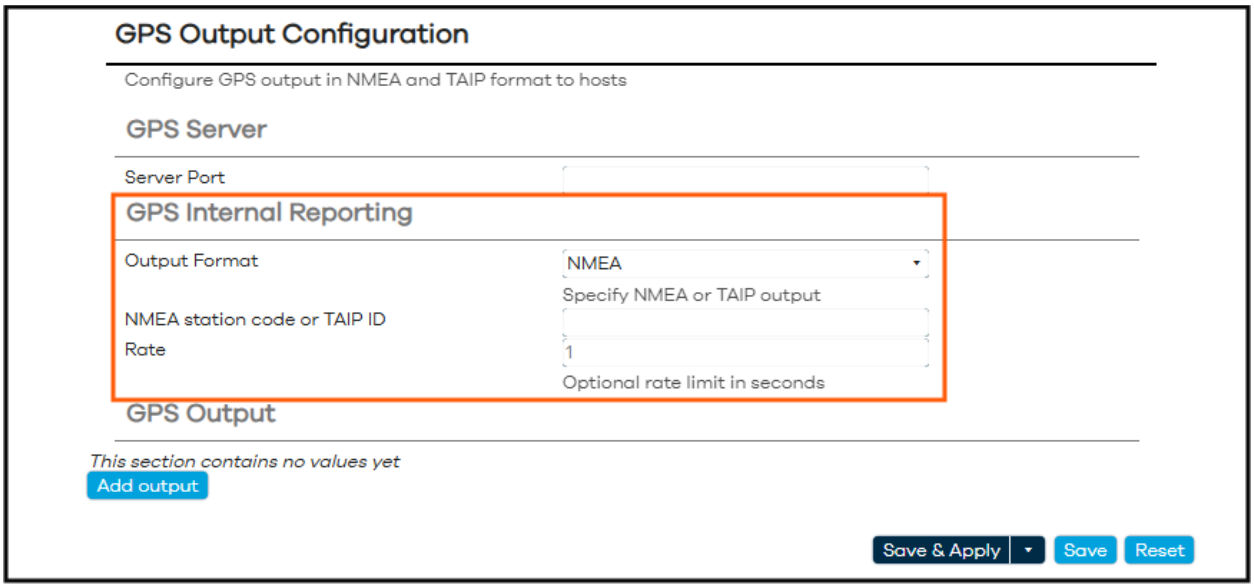


Figure 99: GPS Internal Reporting Configuration

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

   5a. **Output Format** – TAIP or NMEA

   5b. **NMEA station code or TAIP ID** (optional) – enter a valid alphanumeric value that is 4 characters long.

   5c. **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.

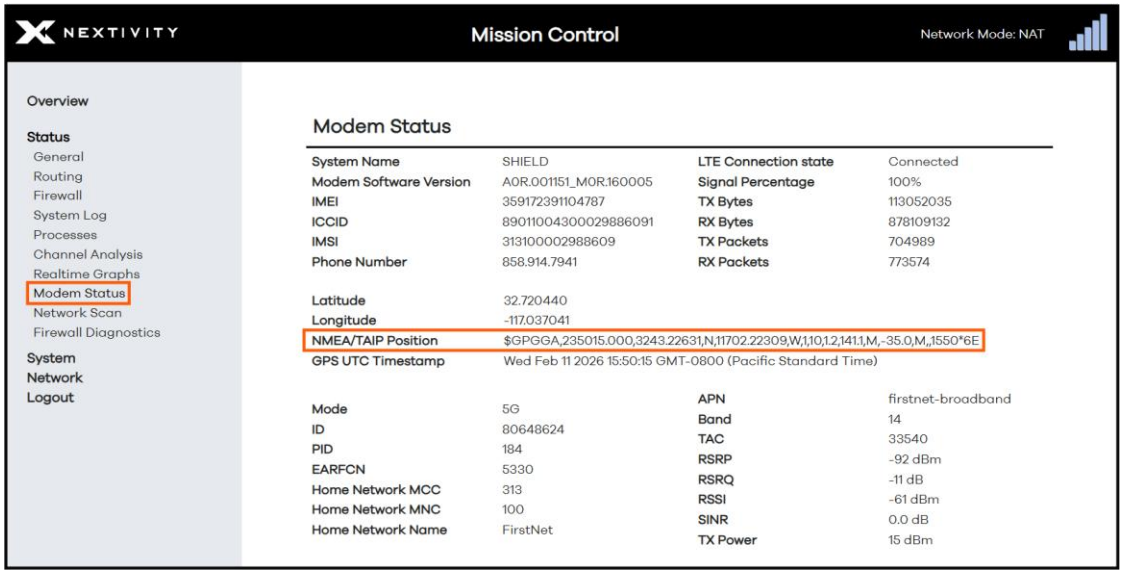


Figure 100: On-device GPS NMEA message format

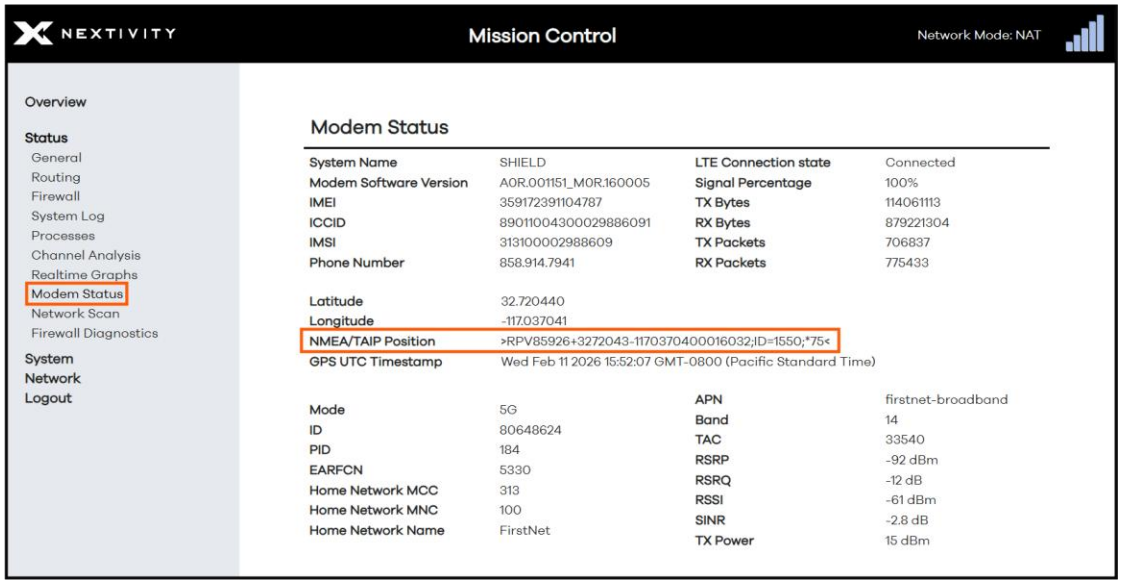


Figure 101: On-device GPS TAIP message format

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.

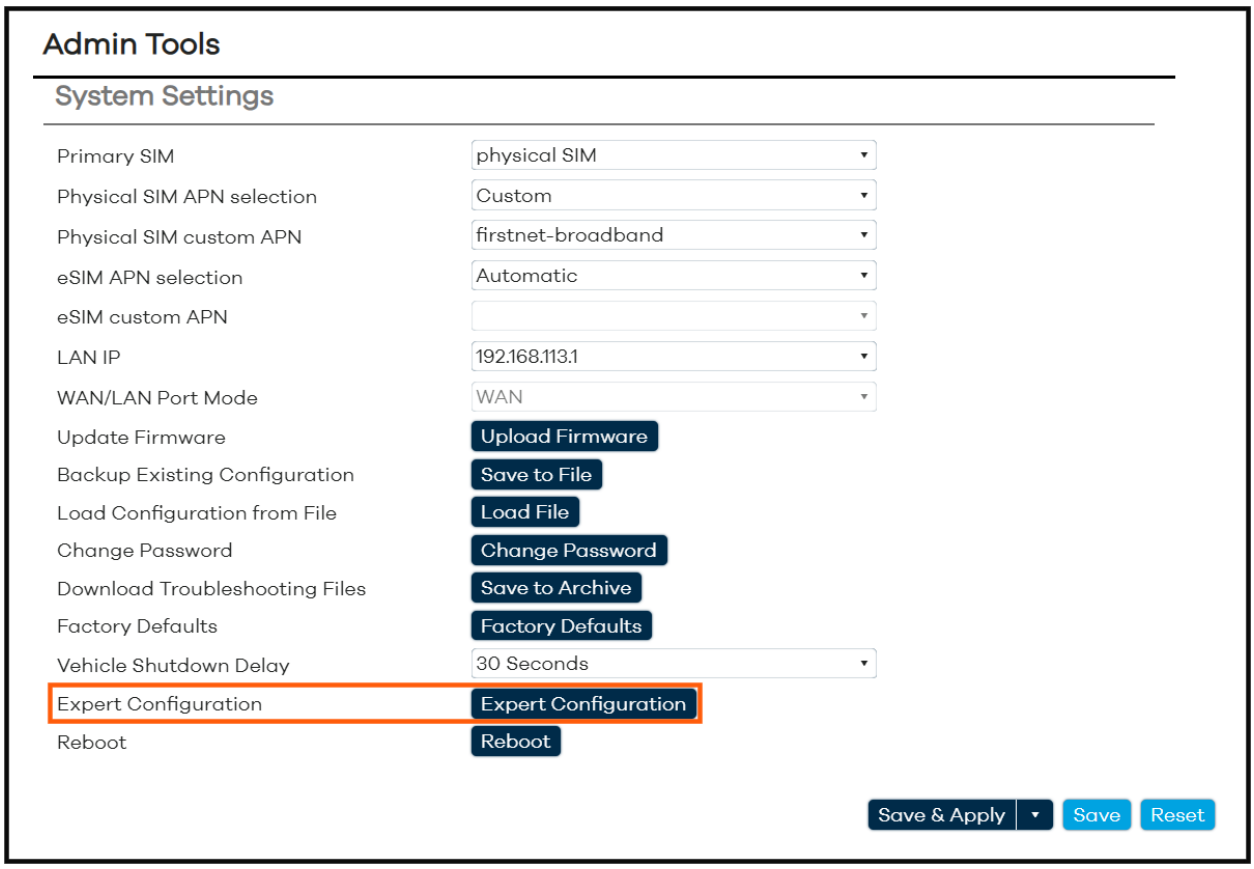


Figure 102: System Settings – Expert Configuration

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

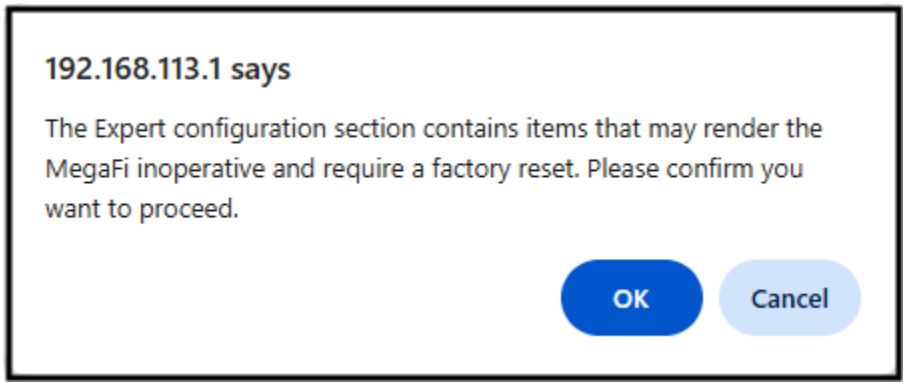


Figure 103: Confirmation to Enter Expert Configuration mode

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

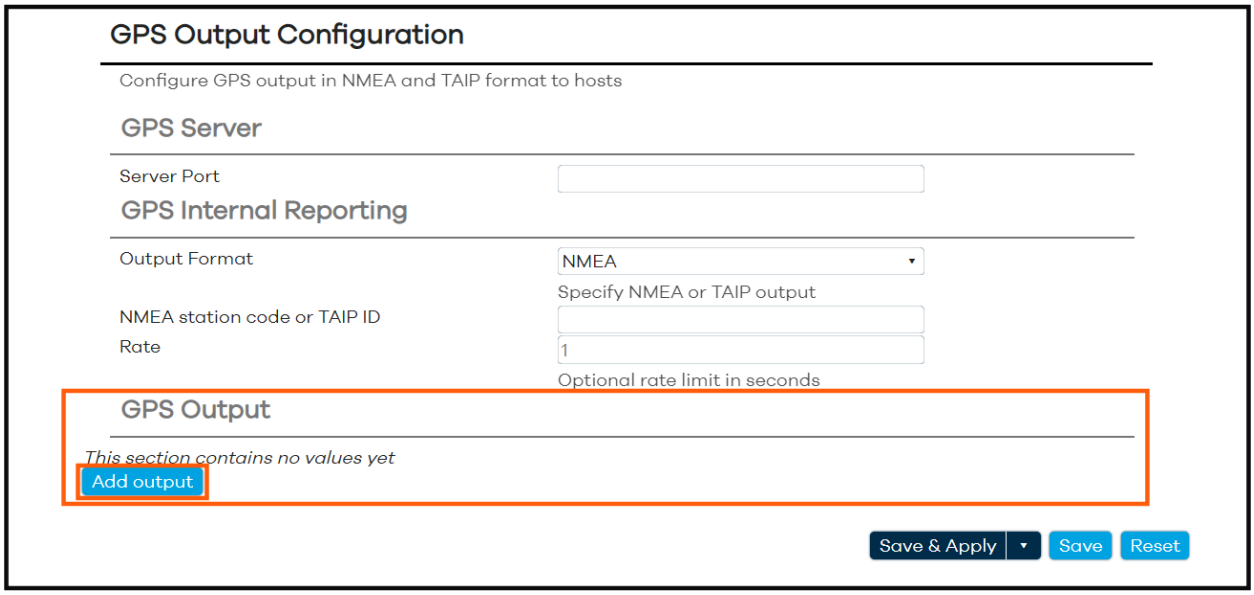


Figure 104: GPS Output Configuration – Add output

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.

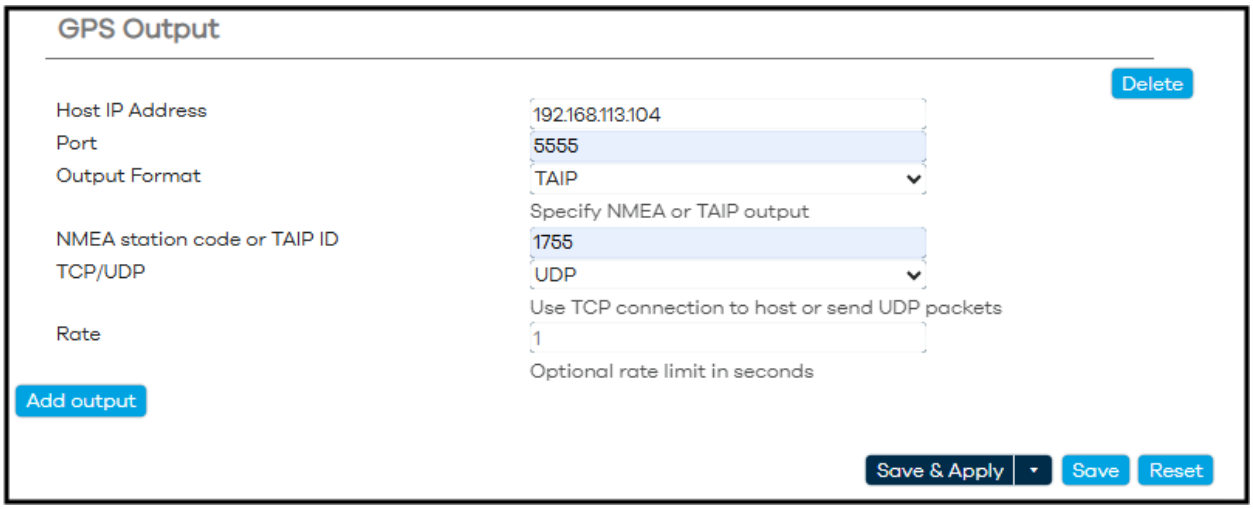


Figure 105: GPS Output Configuration – Values for adding new output

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**.

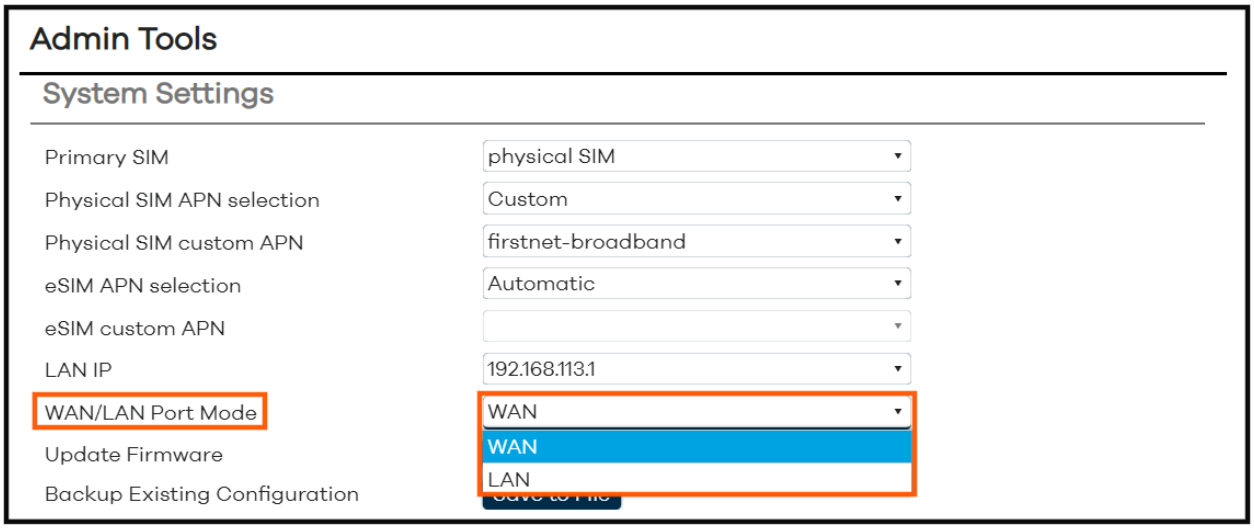


Figure 105: WAN/LAN Port Mode options

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.

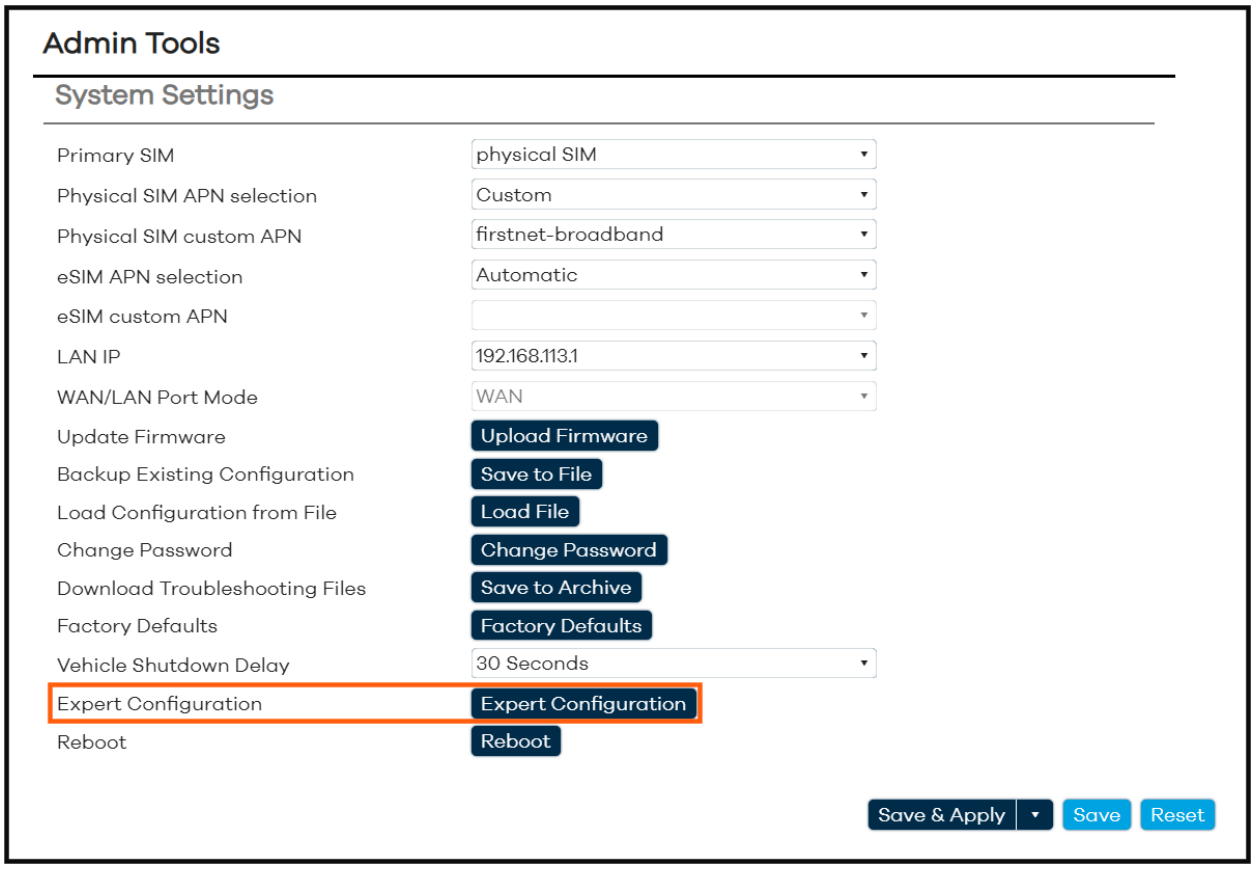


Figure 106: System Settings – Expert Configuration

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

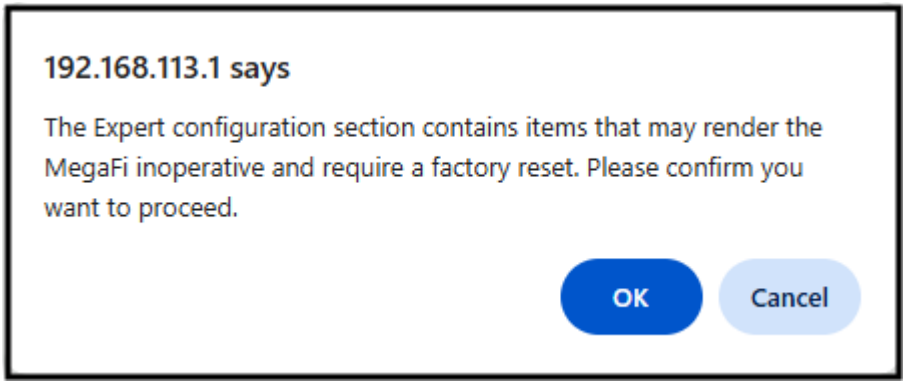


Figure 107: Confirmation to Enter Expert Configuration mode

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

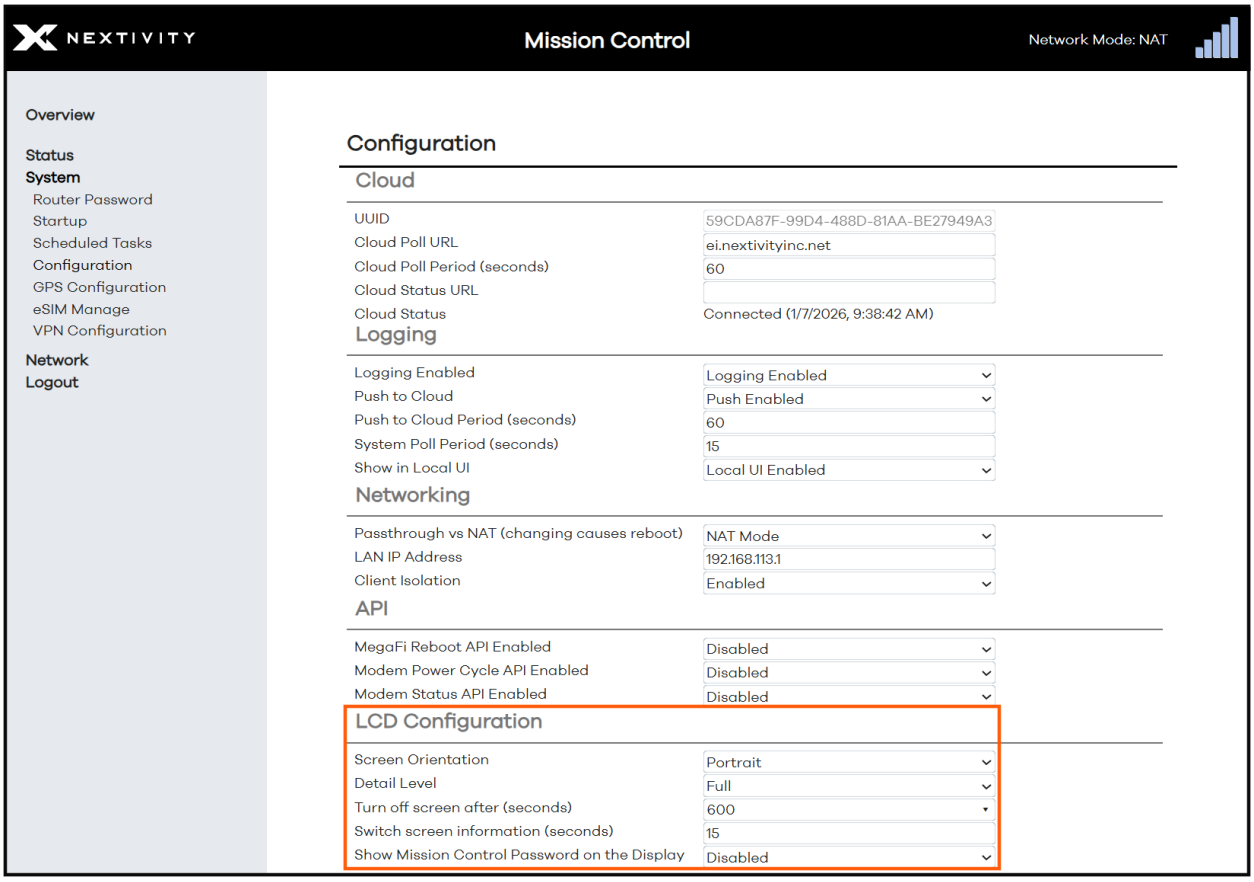


Figure 108: LCD Configuration – default settings

5. 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.

6. 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.
7. 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.

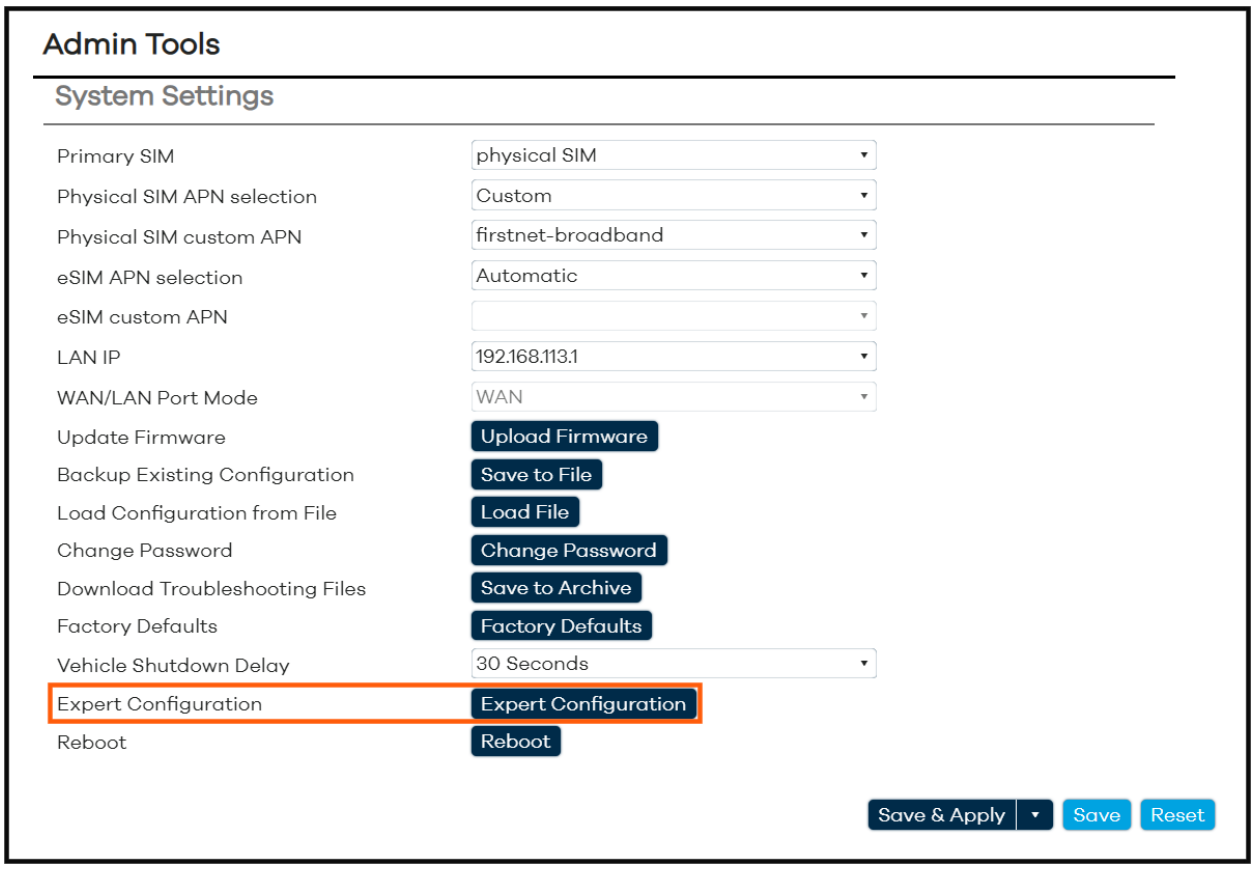


Figure 109: System Settings – Expert Configuration

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

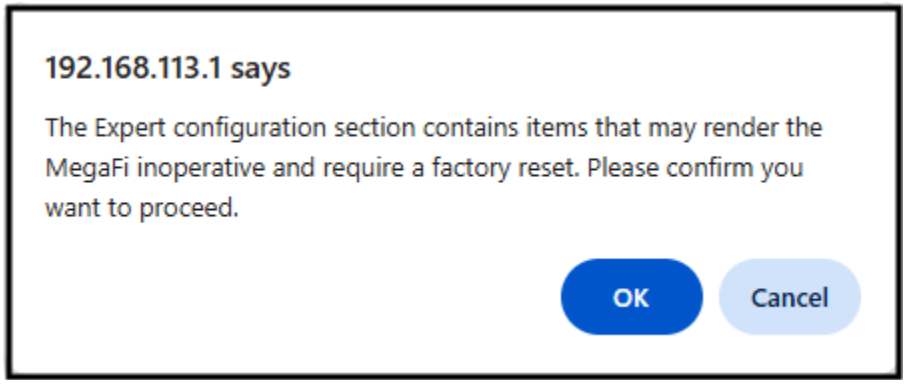


Figure 110: Confirmation to Enter Expert Configuration mode

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

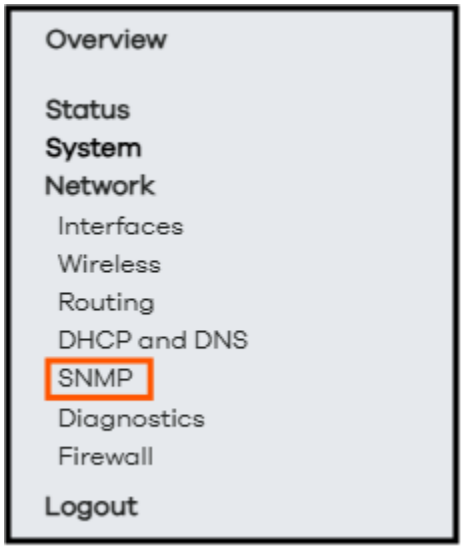


Figure 111: Navigation pane showing options available in Expert mode – Configuration

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 "**nextivity123**". 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.

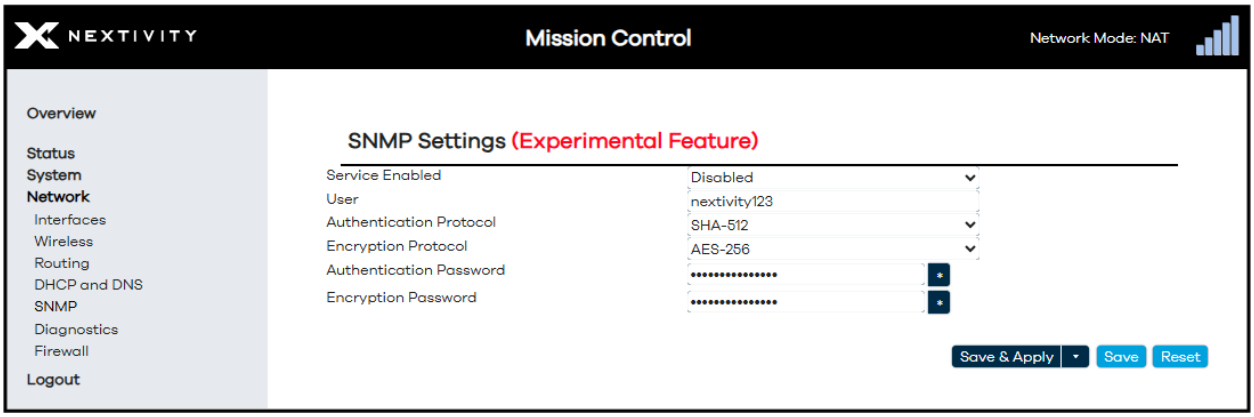


Figure 112: SNMP Settings

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.

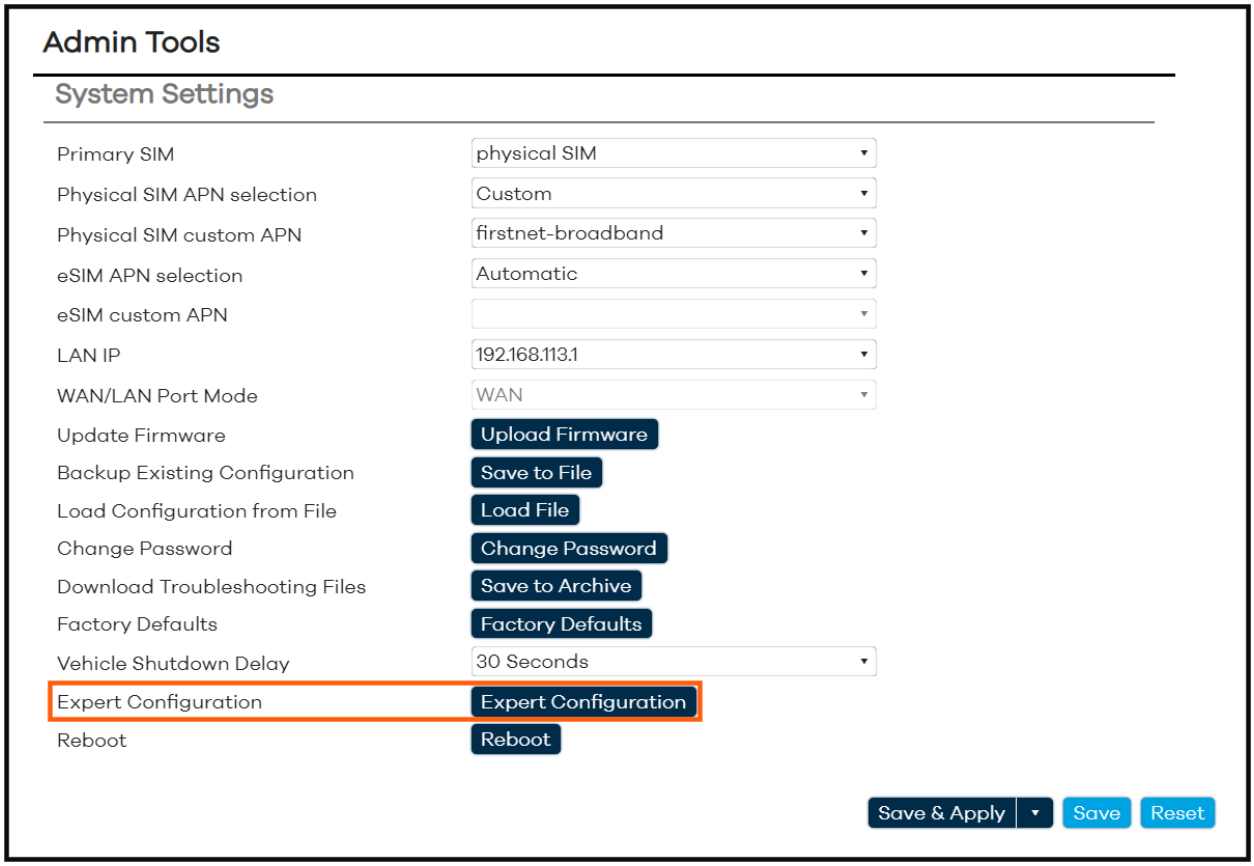


Figure 113: System Settings – Expert Configuration

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

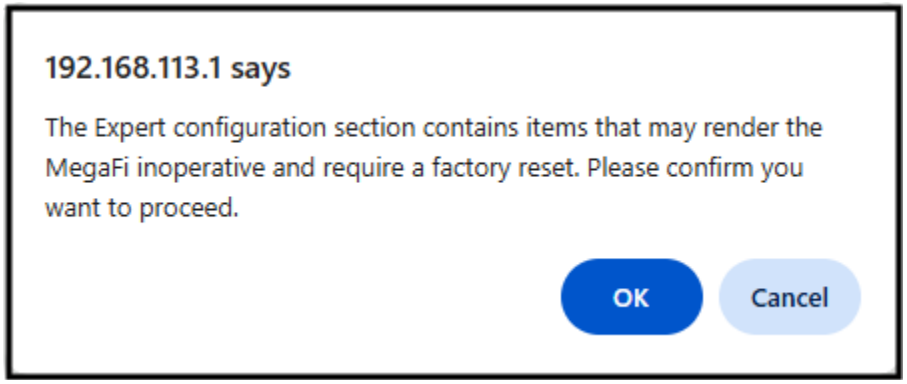


Figure 114: Confirmation to Enter Expert Configuration mode

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

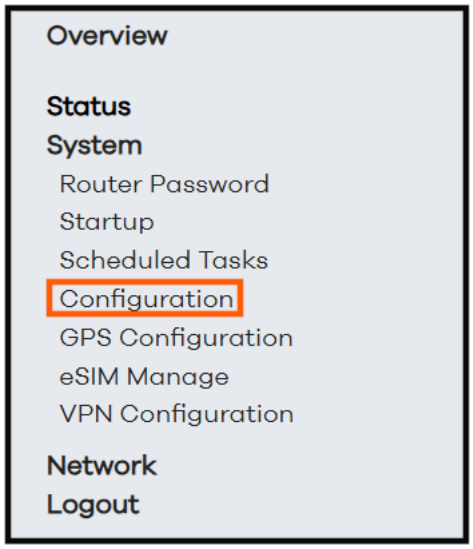


Figure 115: Navigation pane showing options available in Expert mode – Configuration

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

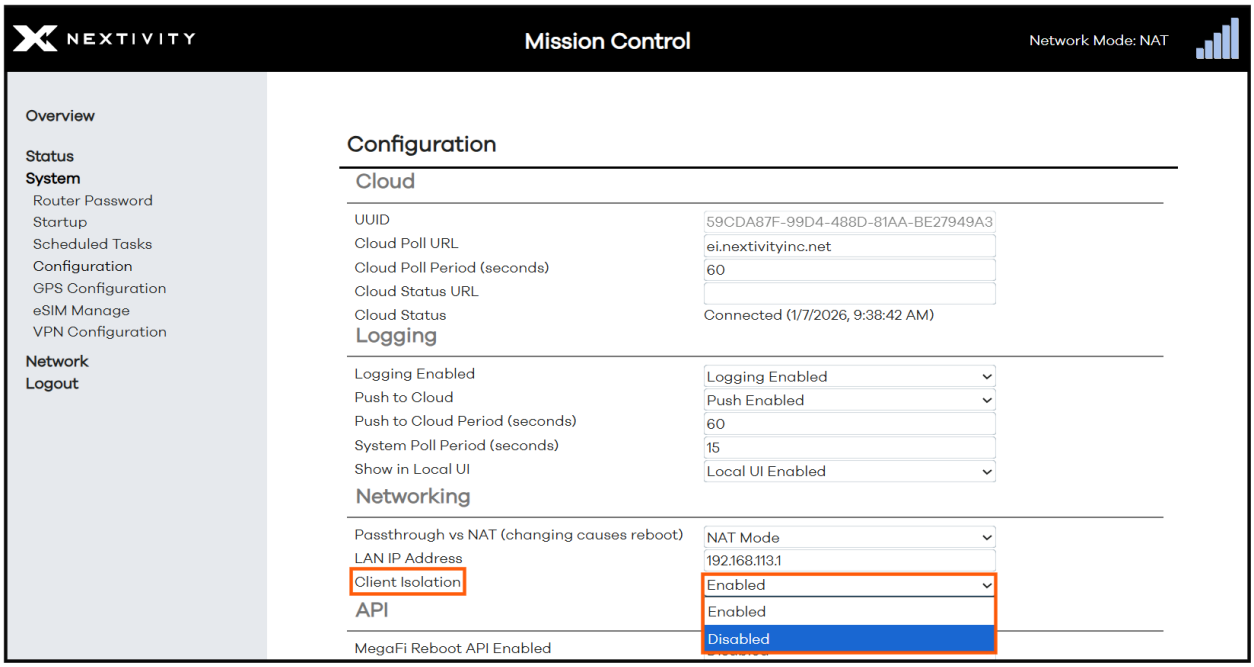


Figure 116: Client Isolation

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.

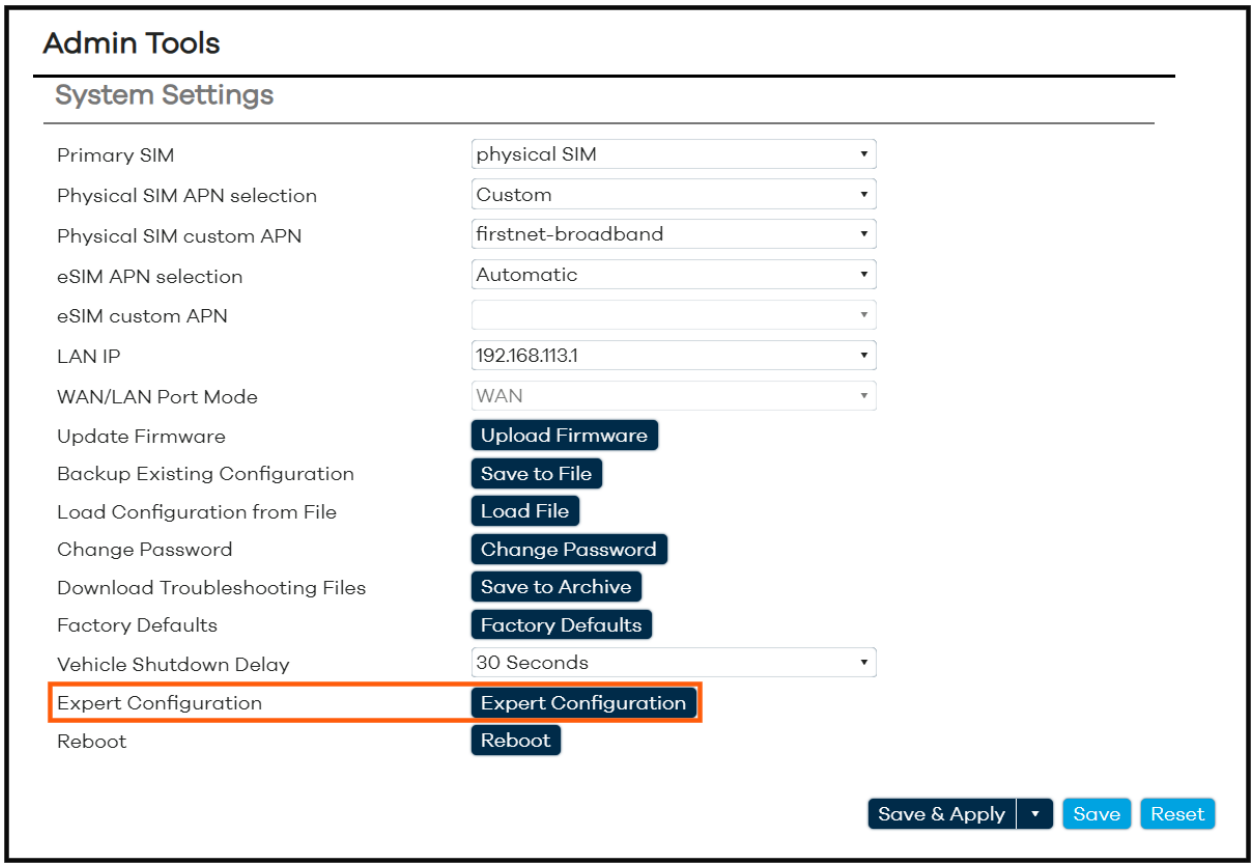


Figure 117: System Settings – Expert Configuration

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

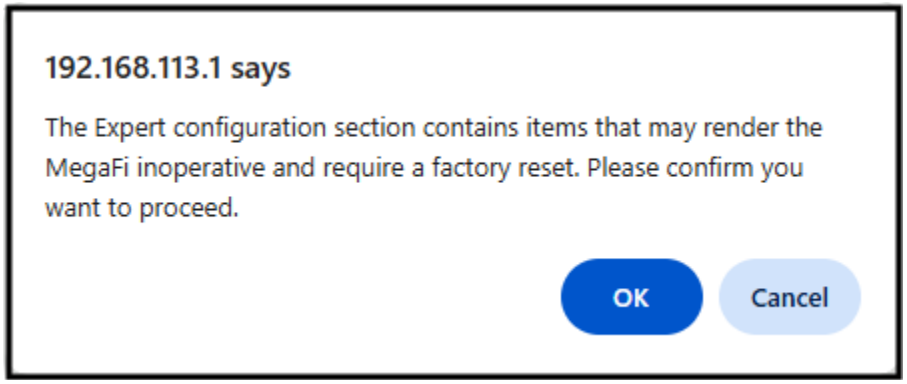


Figure 118: Confirmation to Enter Expert Configuration mode

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

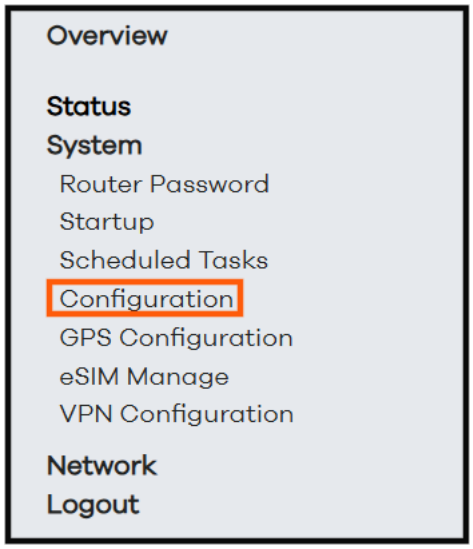


Figure 119: Navigation pane showing options available in Expert mode – Configuration

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

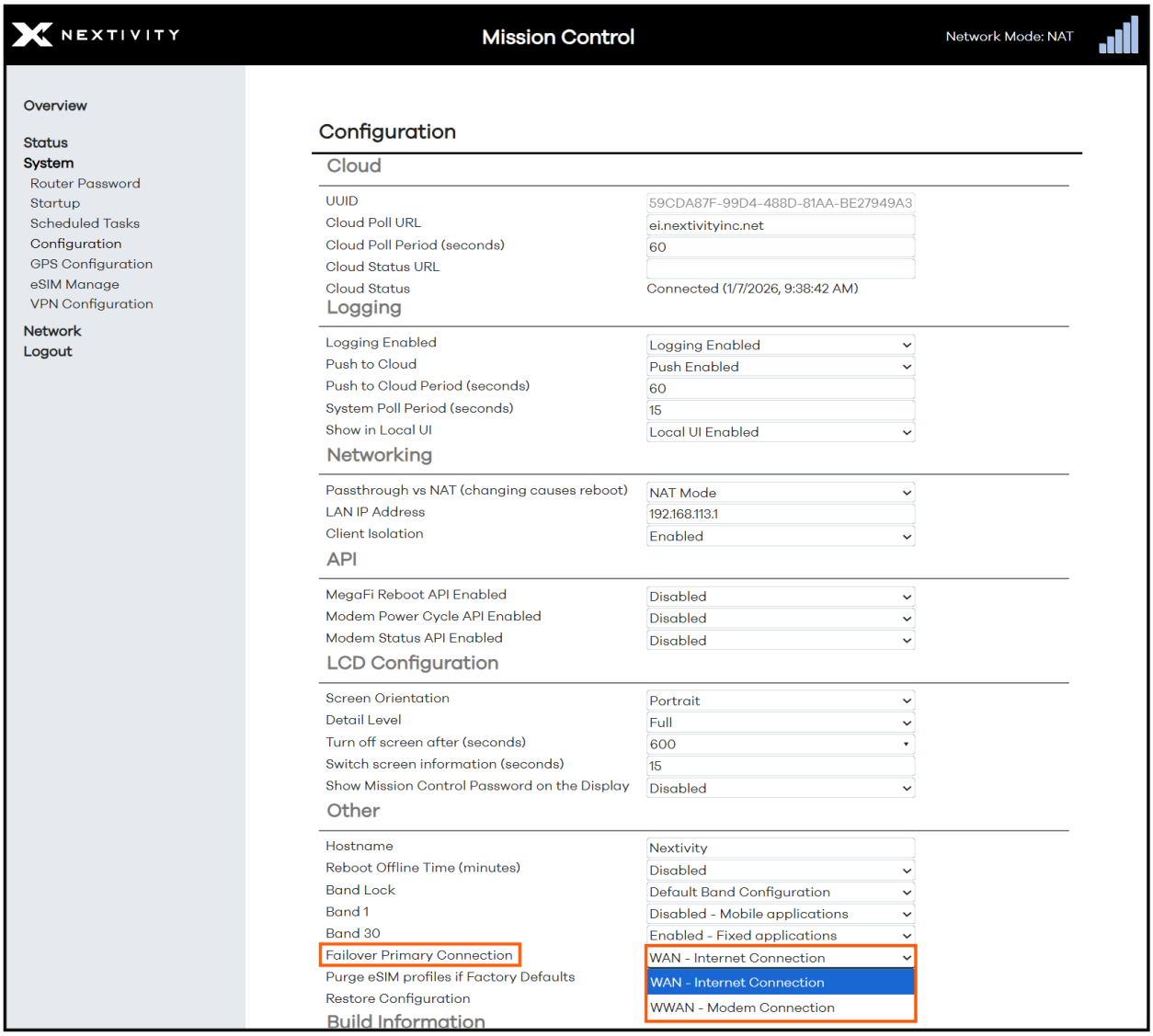


Figure 120: Failover Primary Connection

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.

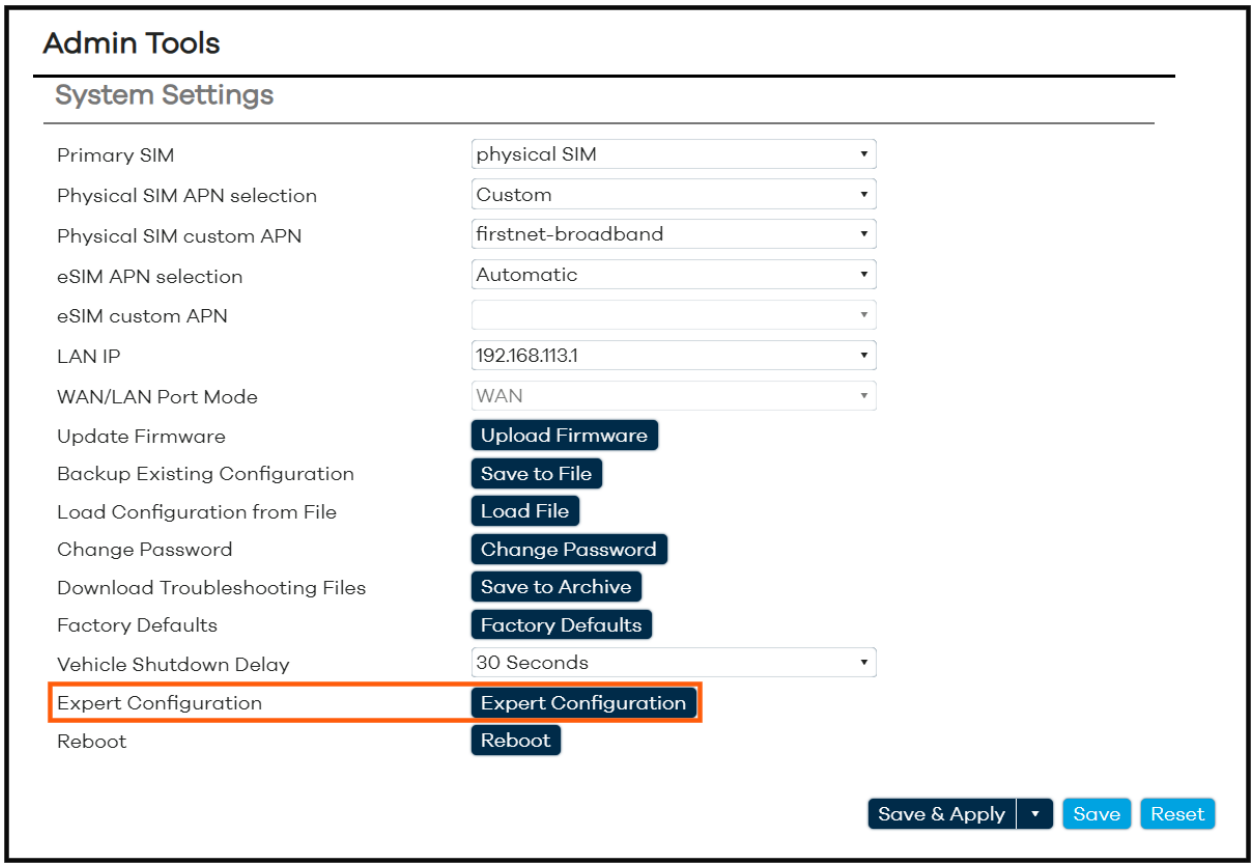


Figure 121: System Settings – Expert Configuration

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

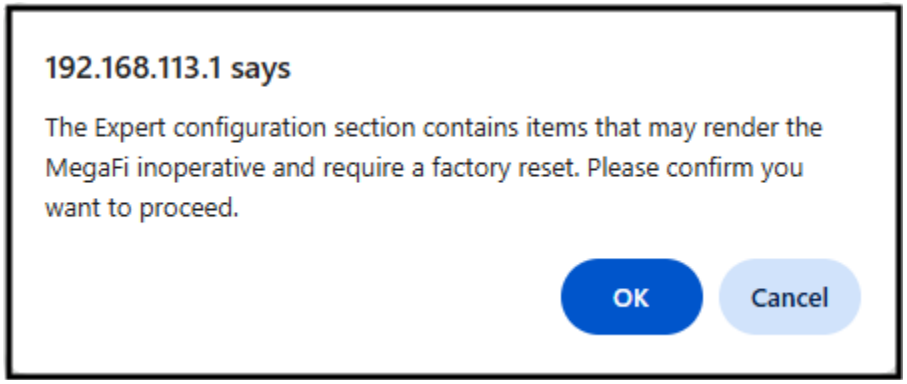


Figure 122: Confirmation to Enter Expert Configuration mode

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.

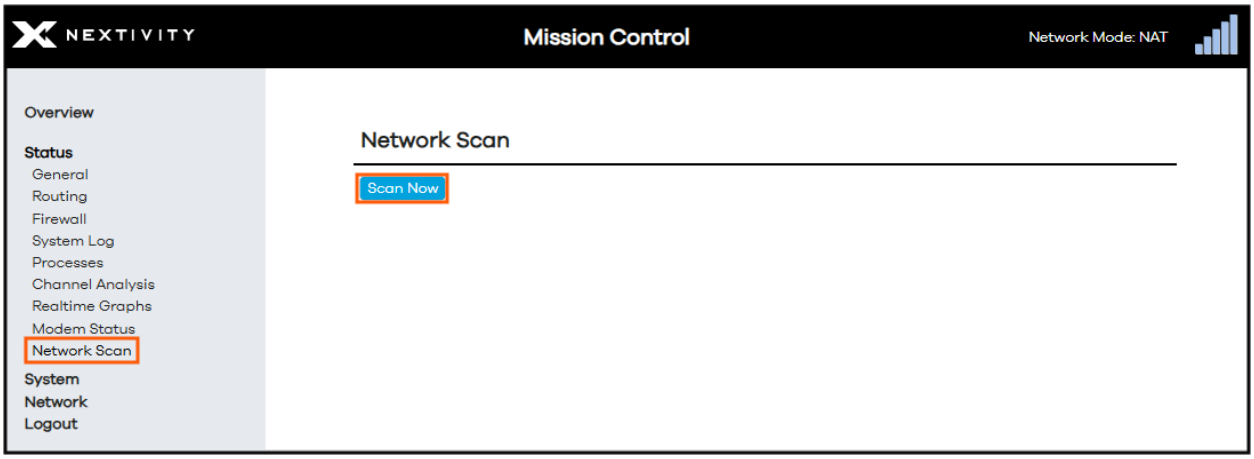
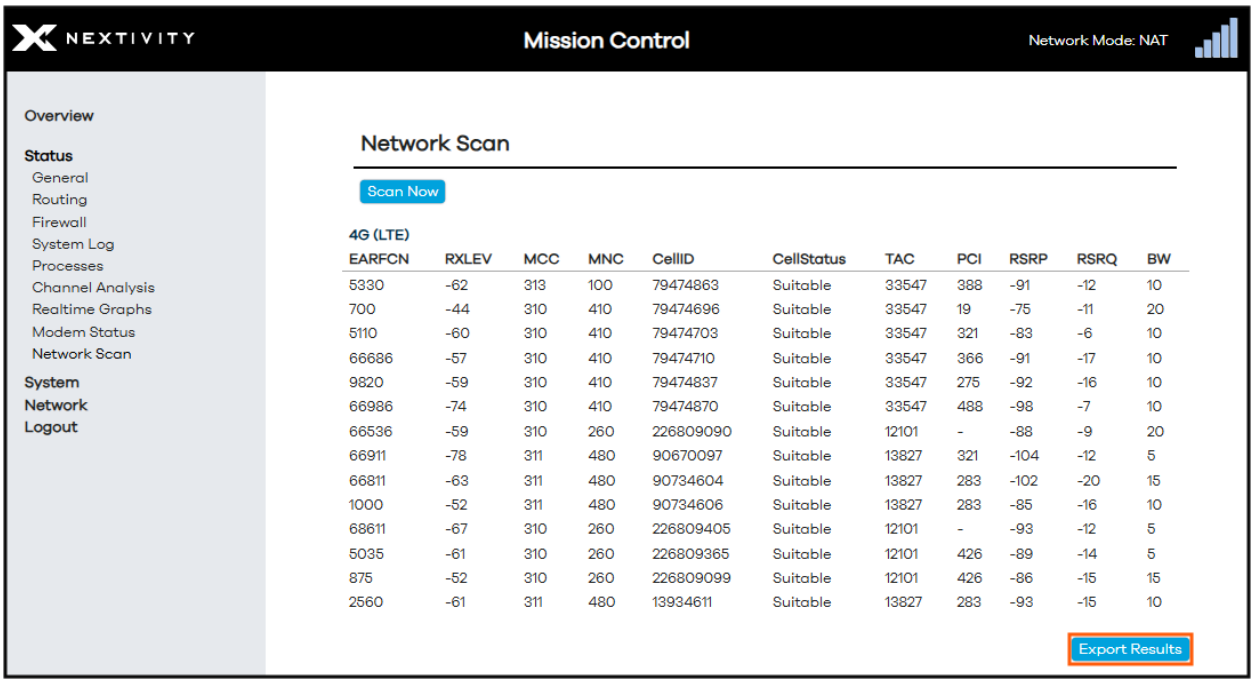


Figure 123: Network Scan

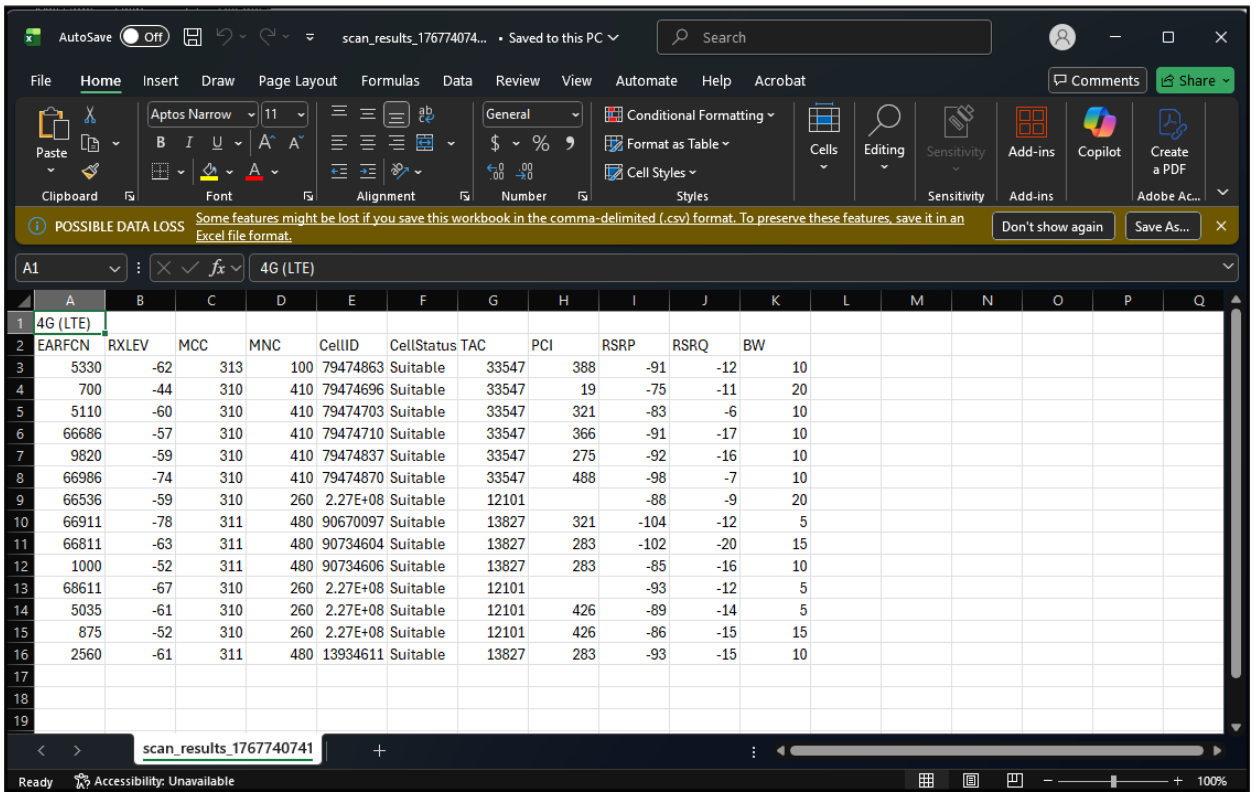
6. After the scan is complete, the results can be exported by clicking on the Export Results.



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 124: Export Results

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



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	2.27E+08	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	2.27E+08	Suitable	12101		-93	-12	5
5035	-61	310	260	2.27E+08	Suitable	12101	426	-89	-14	5
875	-52	310	260	2.27E+08	Suitable	12101	426	-86	-15	15
2560	-61	311	480	13934611	Suitable	13827	283	-93	-15	10

Figure 125: 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. 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.

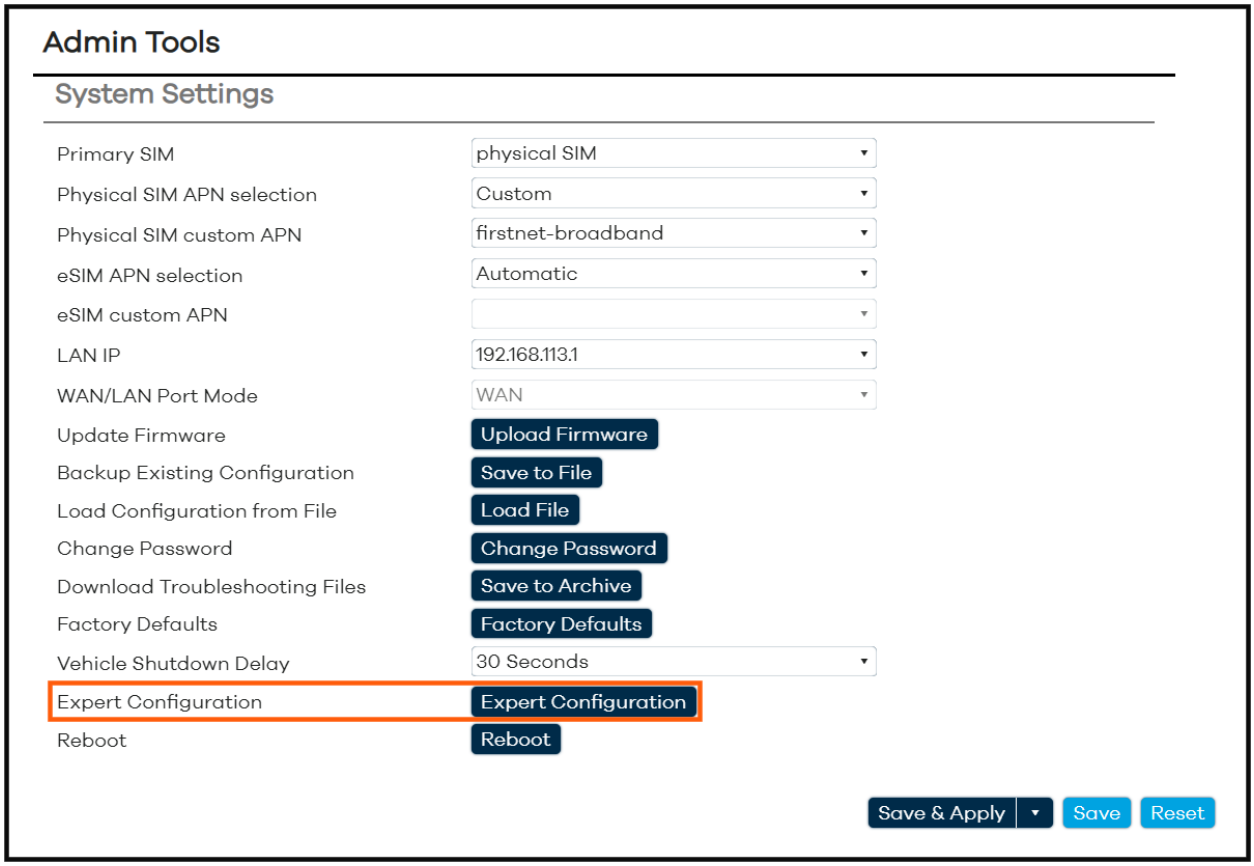


Figure 126: System Settings – Expert Configuration

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

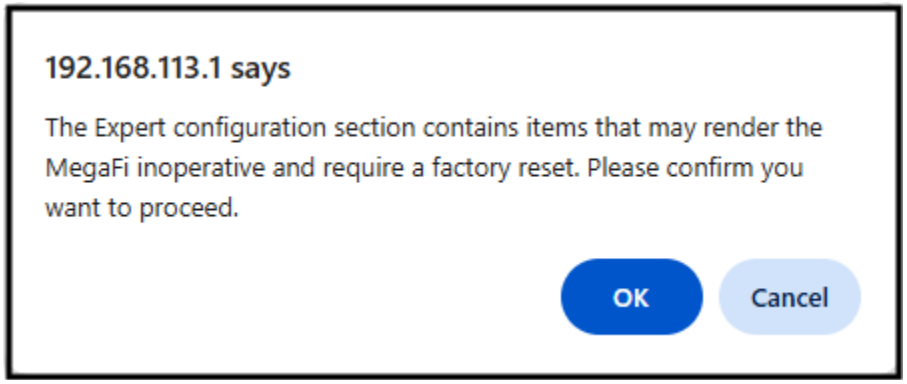


Figure 127: Confirmation to Enter Expert Configuration mode

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

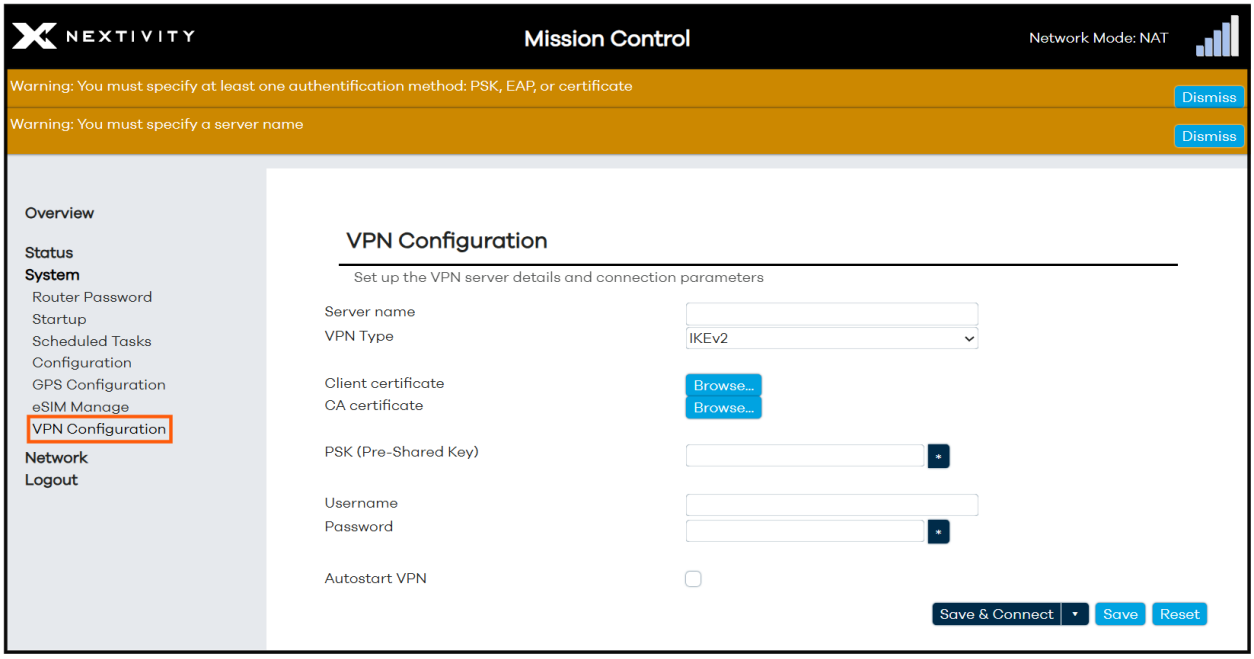


Figure 128: VPN Configuration

➲ **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 account credentials.

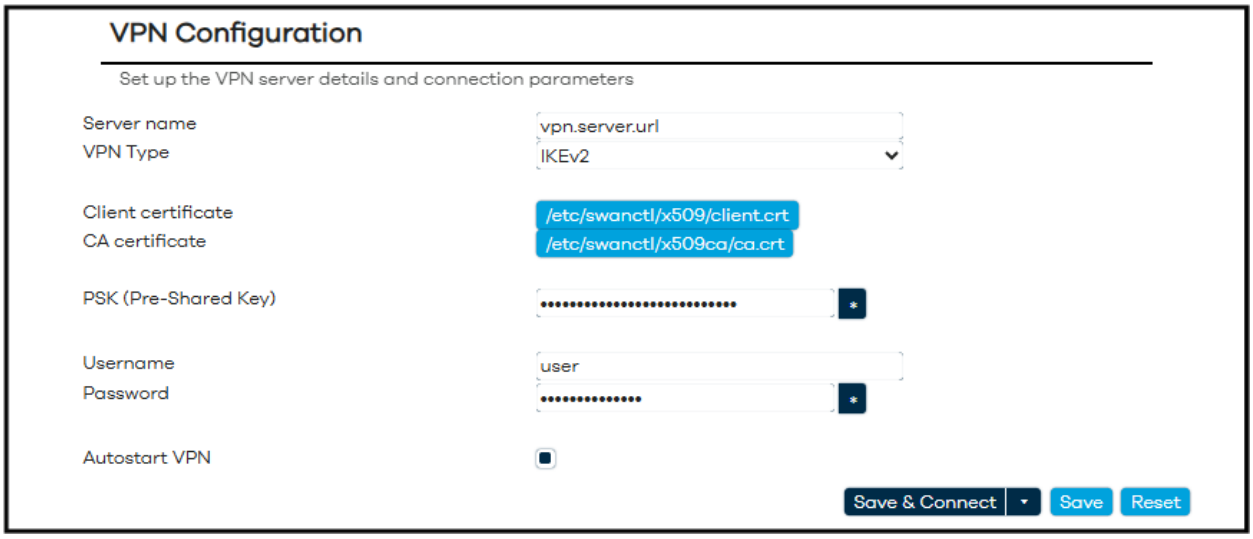


Figure 129: VPN Configuration - Settings

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 …** or **Connected to …**).

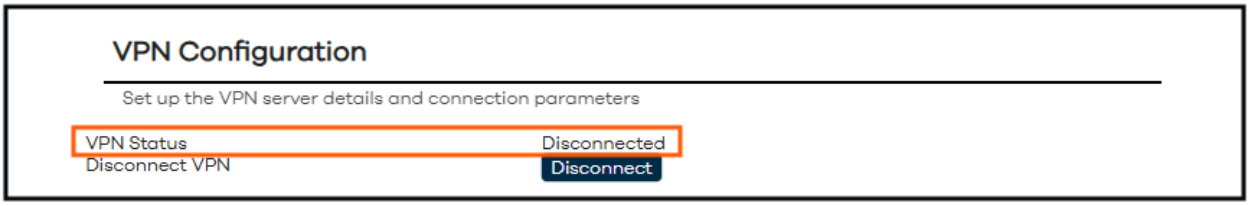


Figure 130: VPN Status - Disconnected

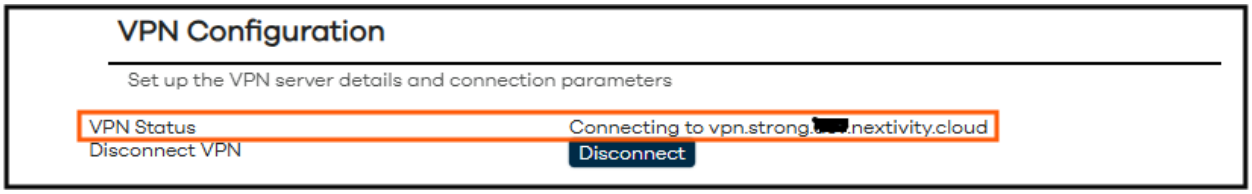


Figure 131: VPN Status – Connecting to…

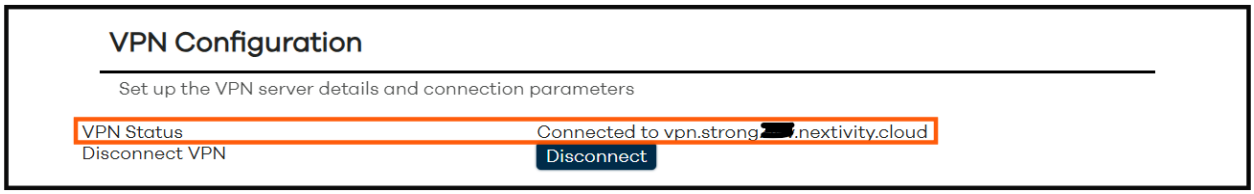


Figure 132: VPN Status – Connected

➲ **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 133: 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.

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

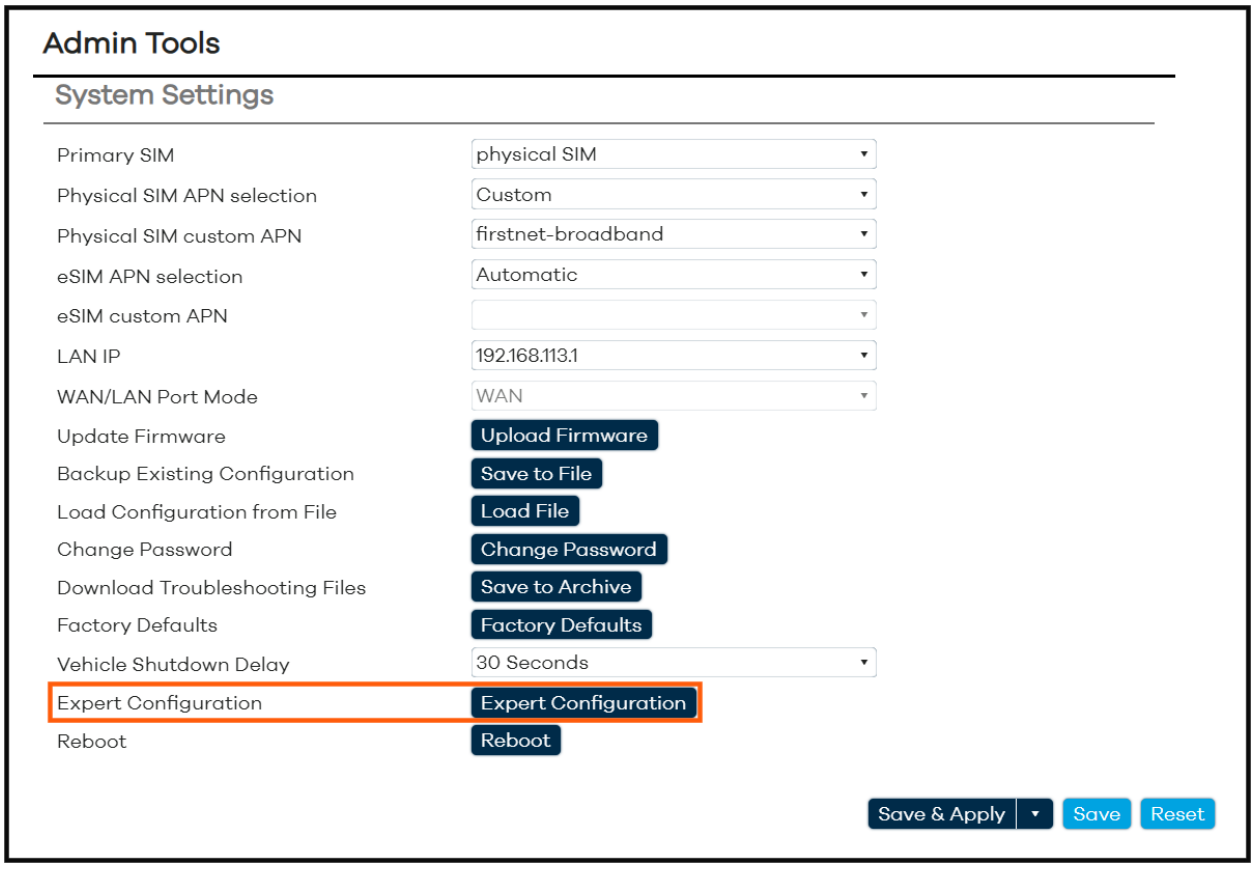


Figure 134: System Settings – Expert Configuration

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

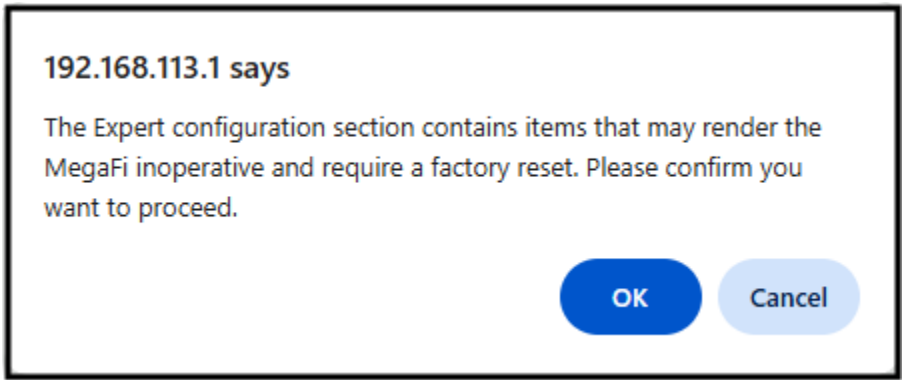


Figure 135: Confirmation to Enter Expert Configuration mode

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

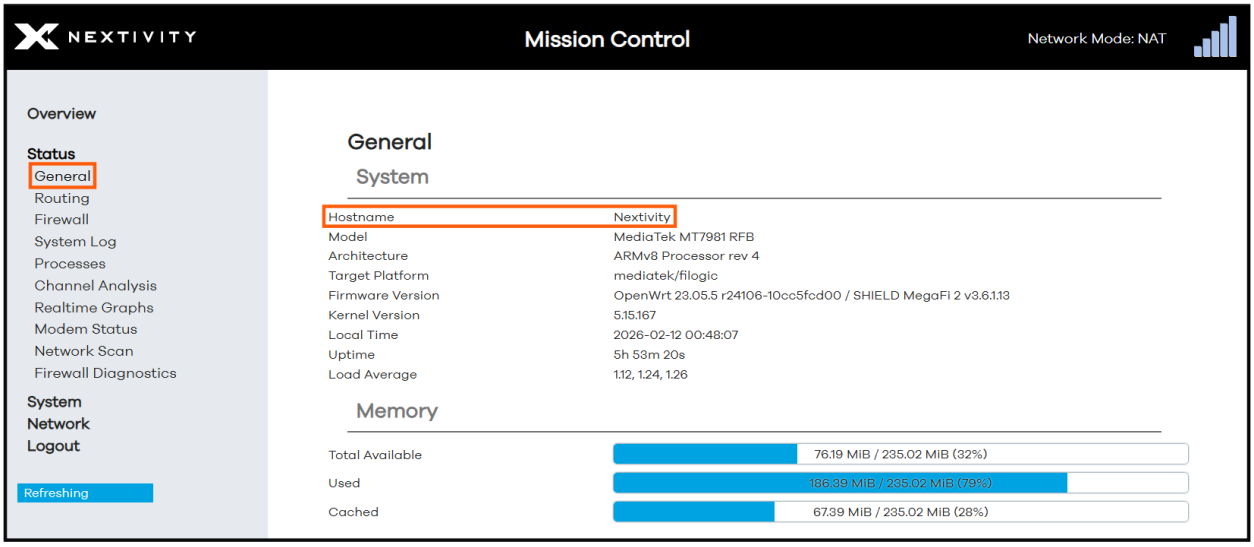


Figure 136: Status General - Hostname of the device

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

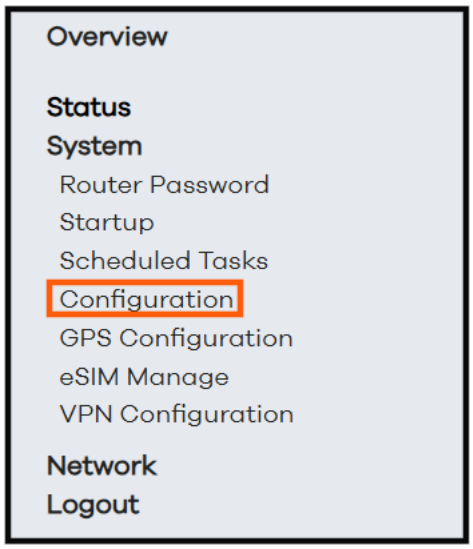


Figure 136: Navigation pane showing options available in Expert mode – Configuration

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

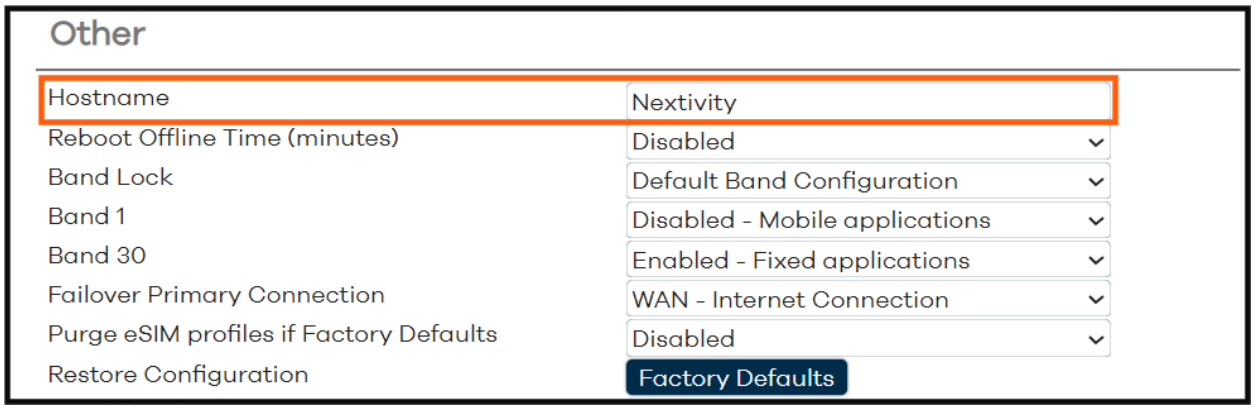


Figure 137: Other – Hostname

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

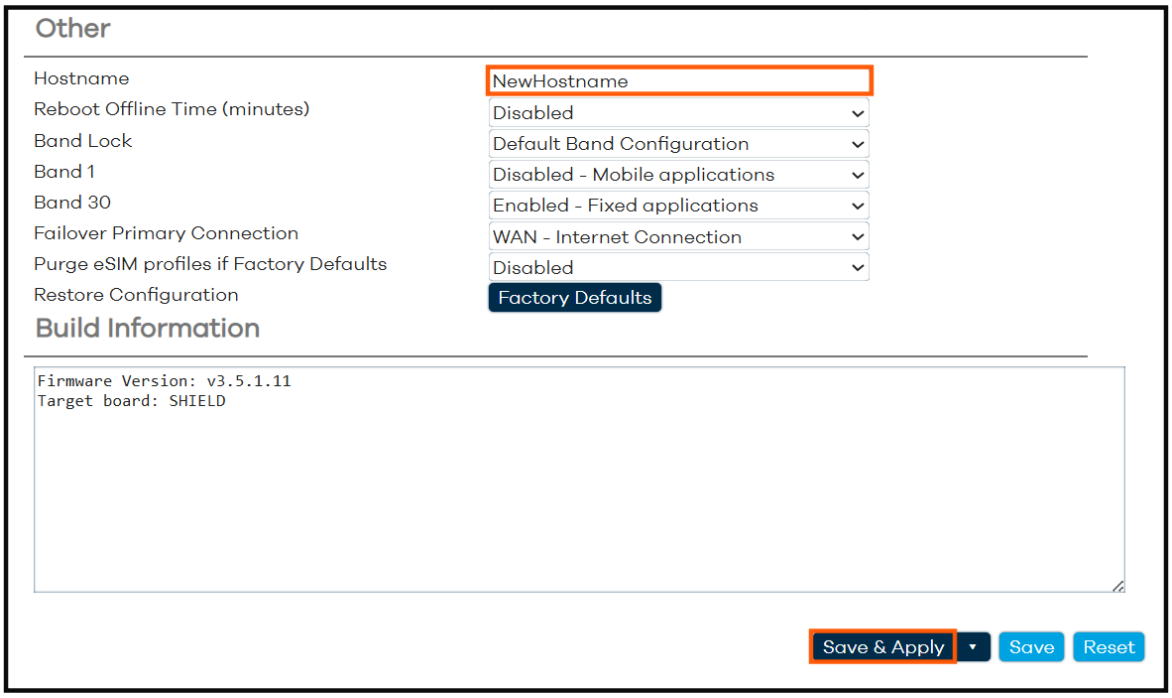


Figure 138: Other – New Hostname

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

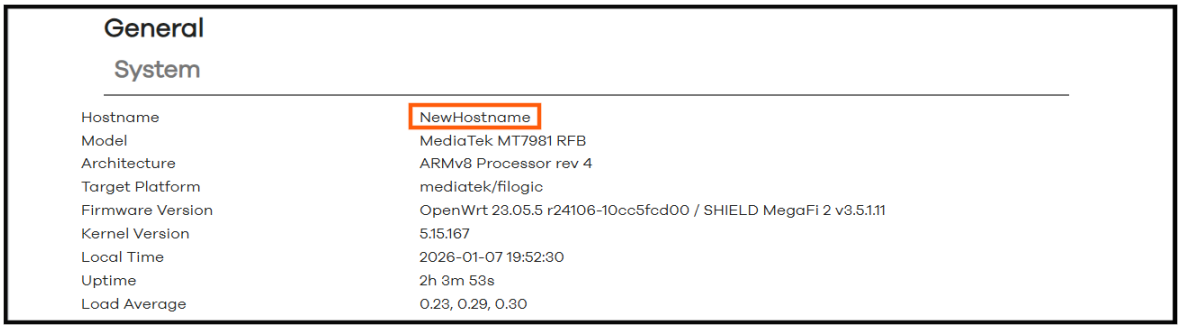


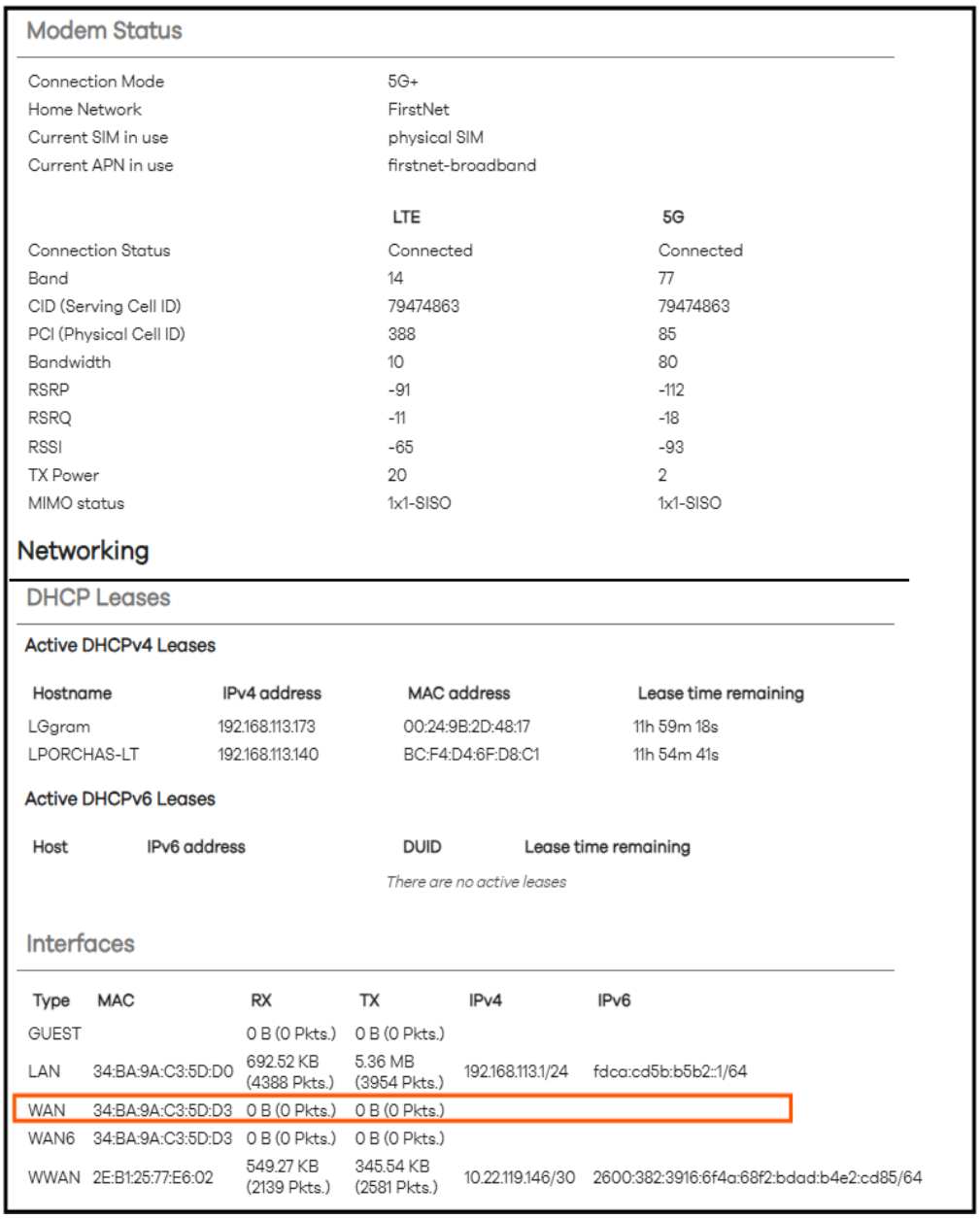
Figure 139: Status General – New Hostname

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.

3.23.1 eSIM Manage

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

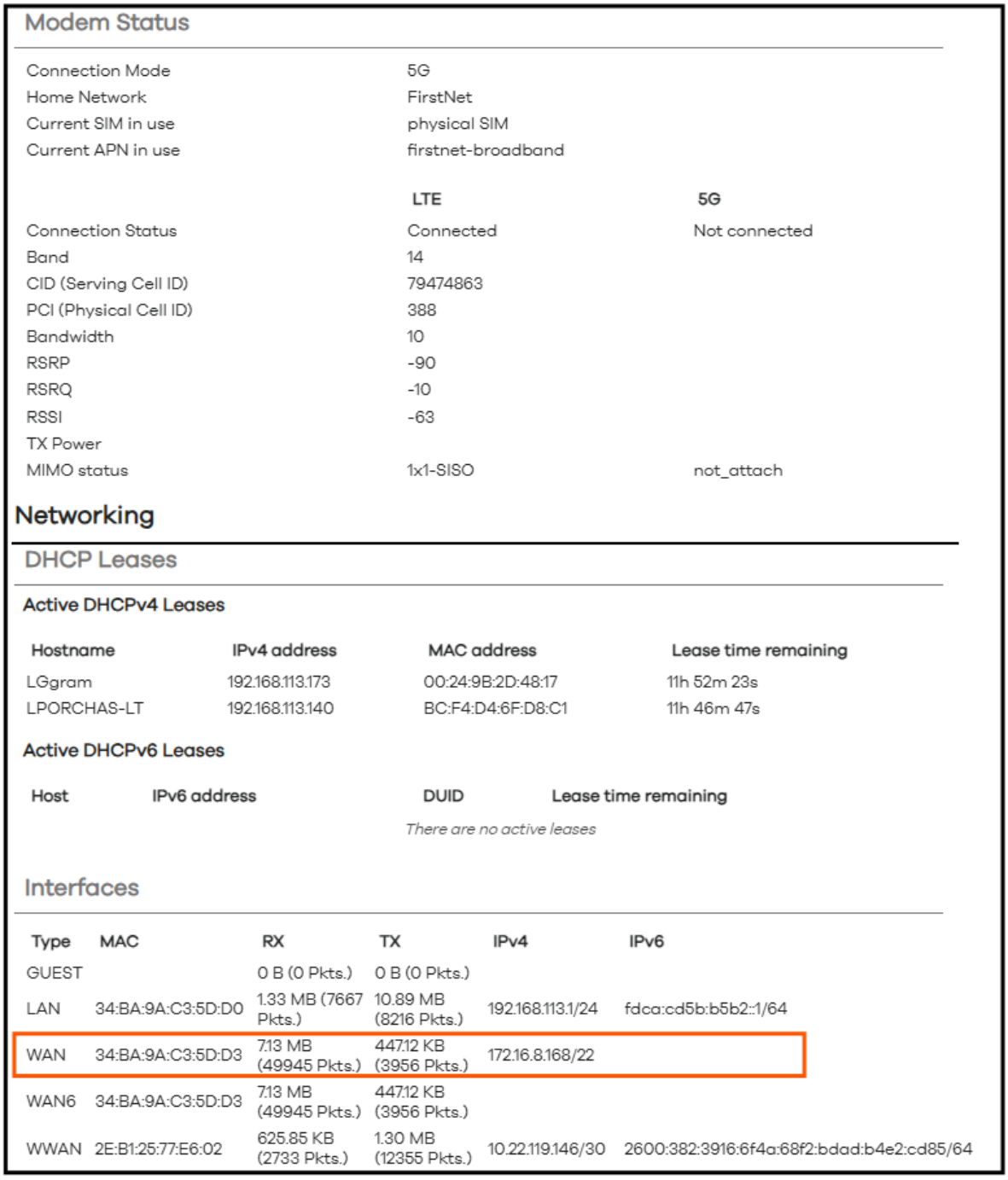
Host	IPv6 address	DUID	Lease time remaining
There are no active leases			

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

1. 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

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

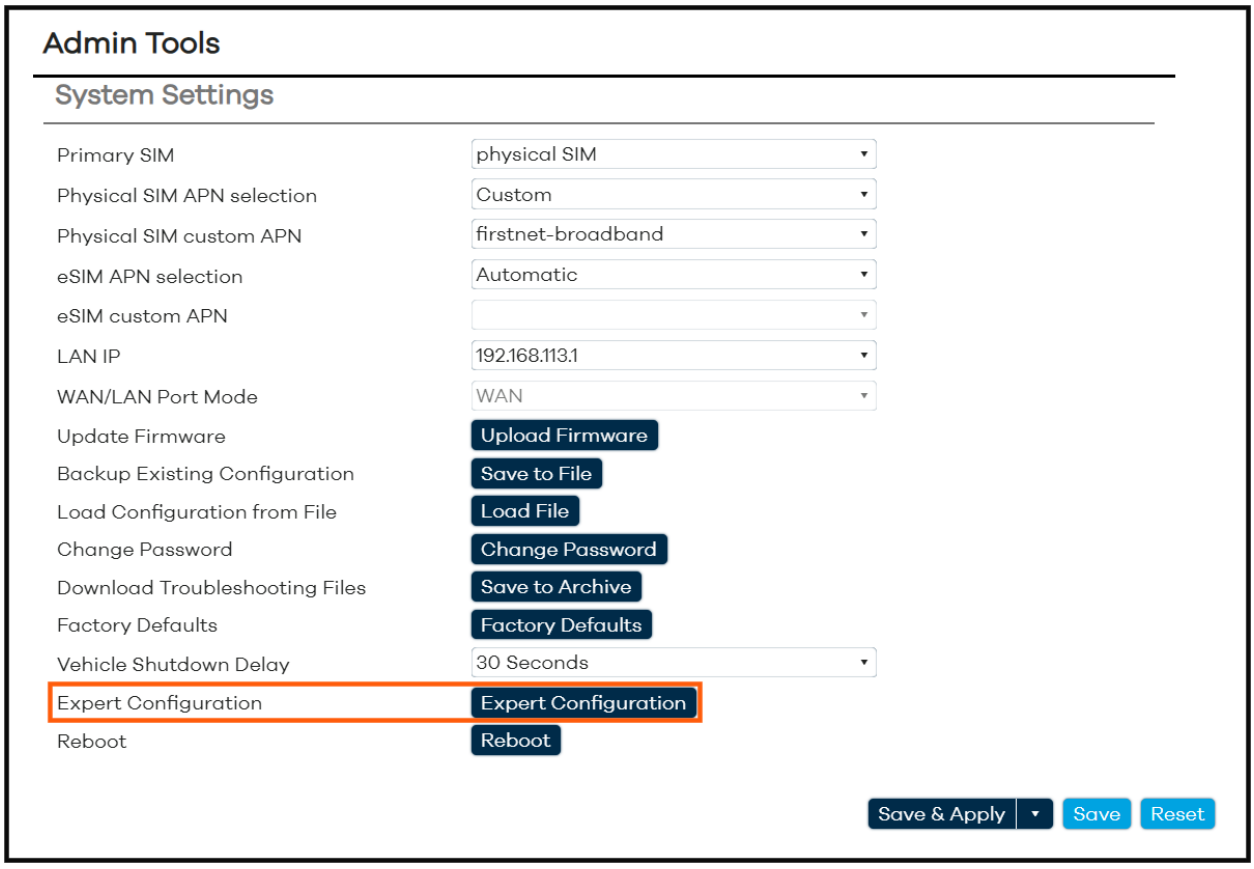


Figure 142: System Settings – Expert Configuration

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

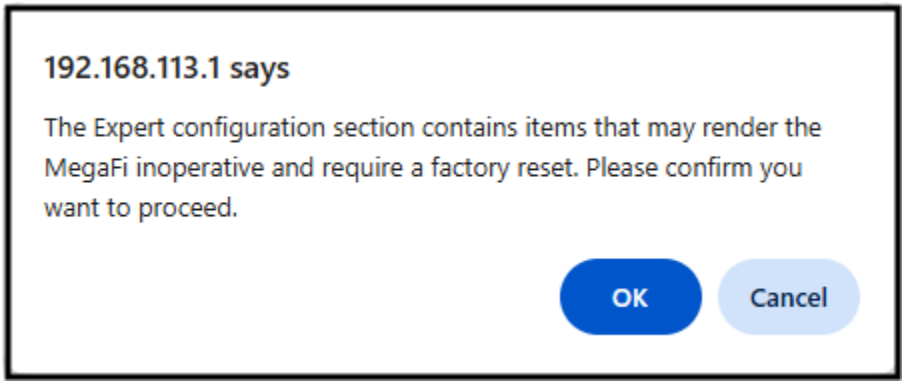


Figure 143: Confirmation to Enter Expert Configuration mode

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

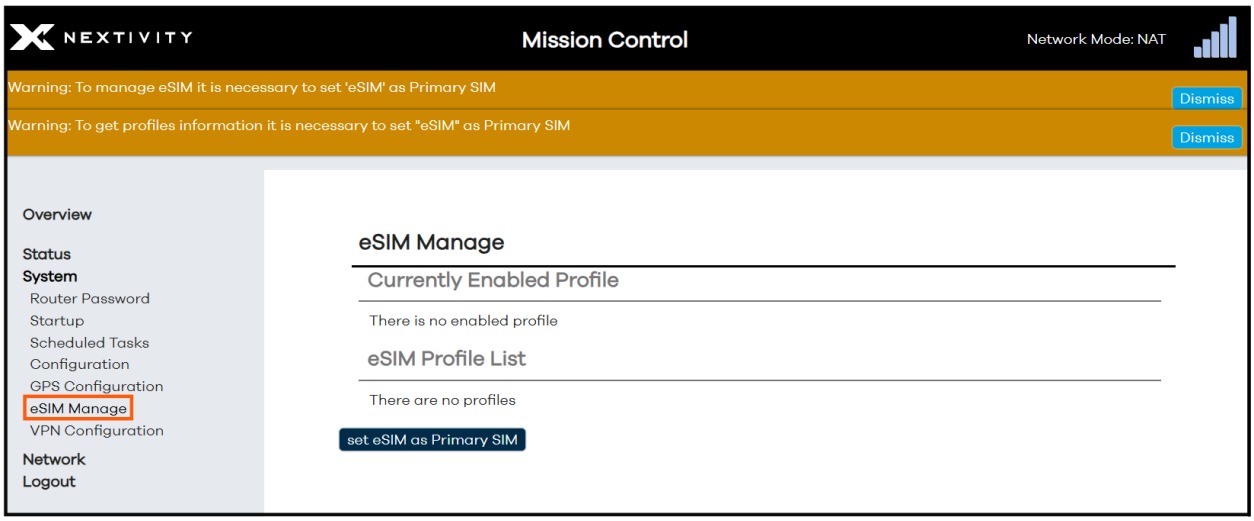


Figure 144: eSIM Manage

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

6. Click on the **set eSIM as Primary SIM** button and wait about a minute to allow for the device to switch to eSIM. This may take a few minutes. The informational message at the top will indicate **Switching to eSIM… please wait**.

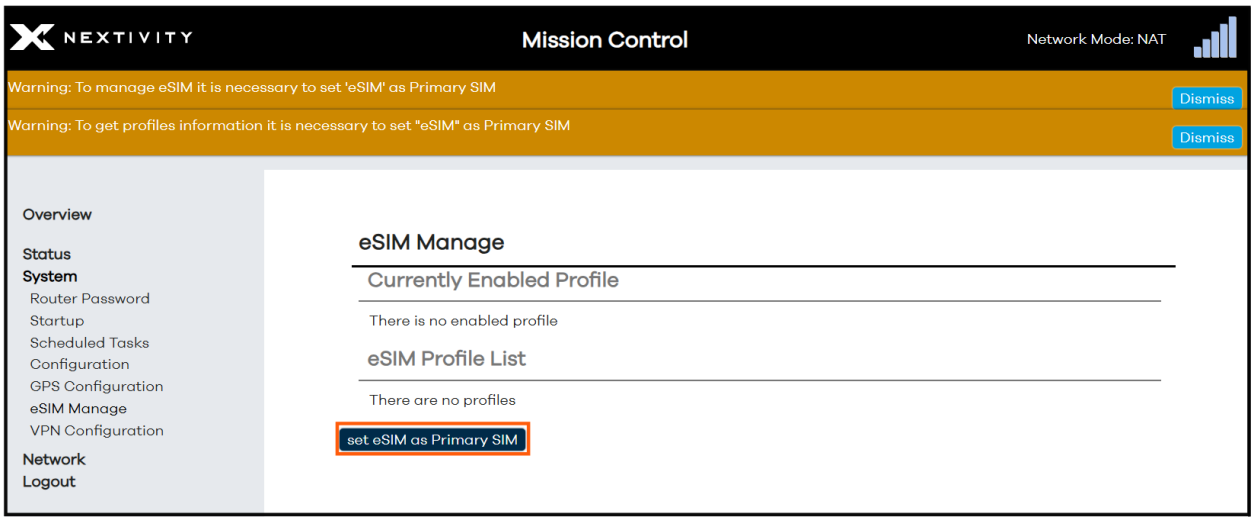


Figure 145: eSIM Manage – set eSIM as Primary SIM

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

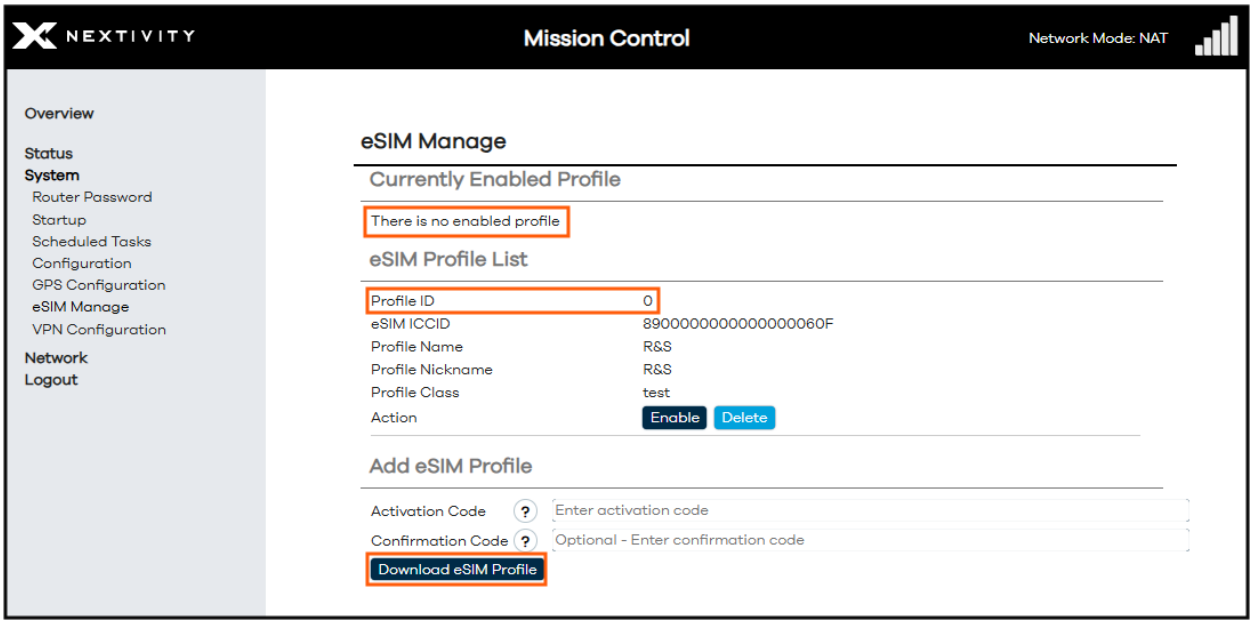


Figure 146: eSIM Manage – no enabled profile

- **Note**: If after several minutes, you do not see the above, refresh the page.
- **Note**: The cellular signal strength bars on the top right corner will disappear. This is normal.

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

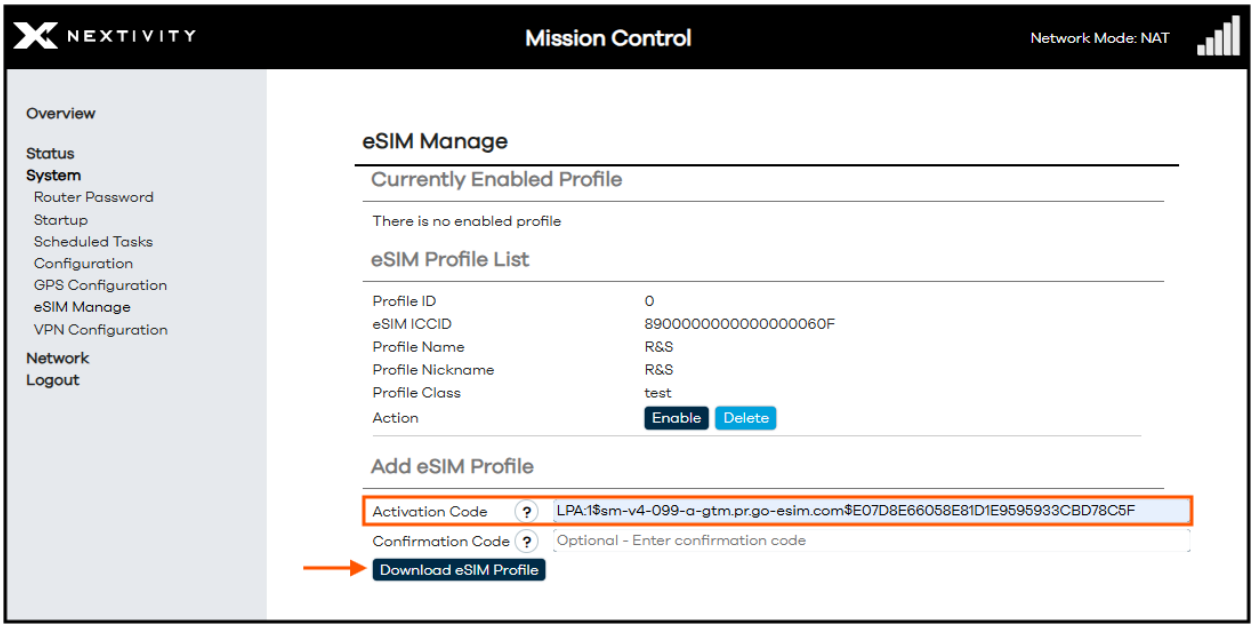


Figure 147: eSIM Manage – enter eSIM codes and download eSIM profile

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

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

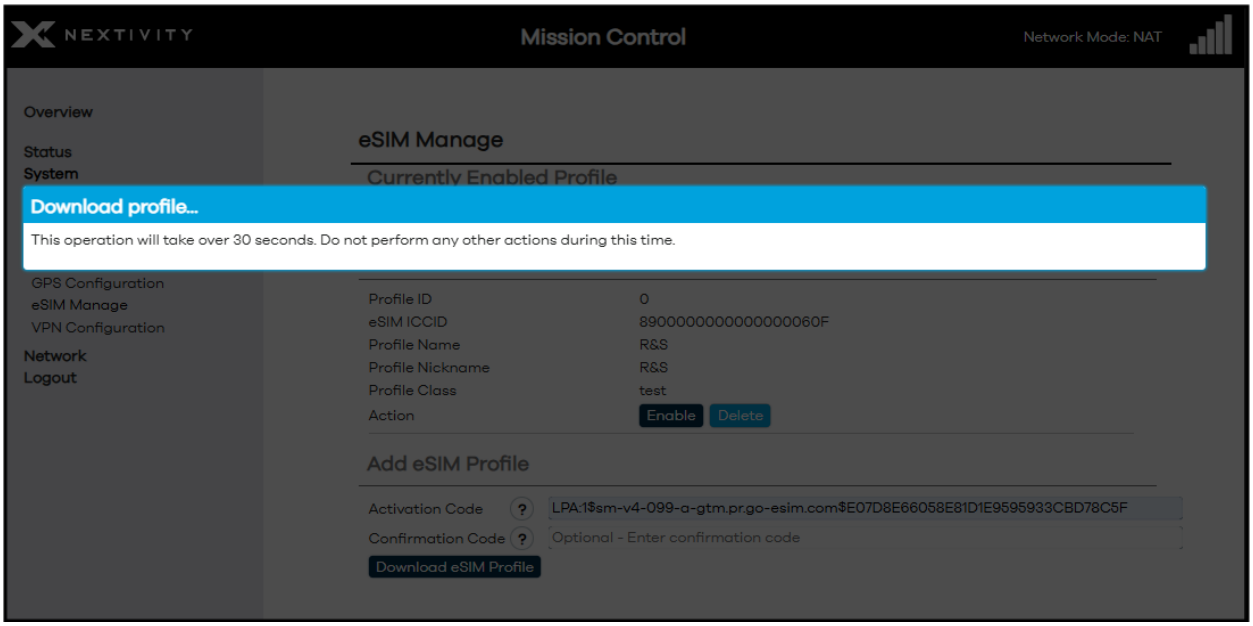


Figure 148: eSIM Manage – Downloading profile...

10. 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 completes rebooting, a new profile will appear. In this example, **Profile ID 1** appears. Validate the **eSIM ICCID** with your eSIM provider. Notice that the **Profile Class** is **operational** for this profile. The **Profile Name** may vary by provider with an actual name, or it may be represented with the **eSIM ICCID** number as shown in this example.

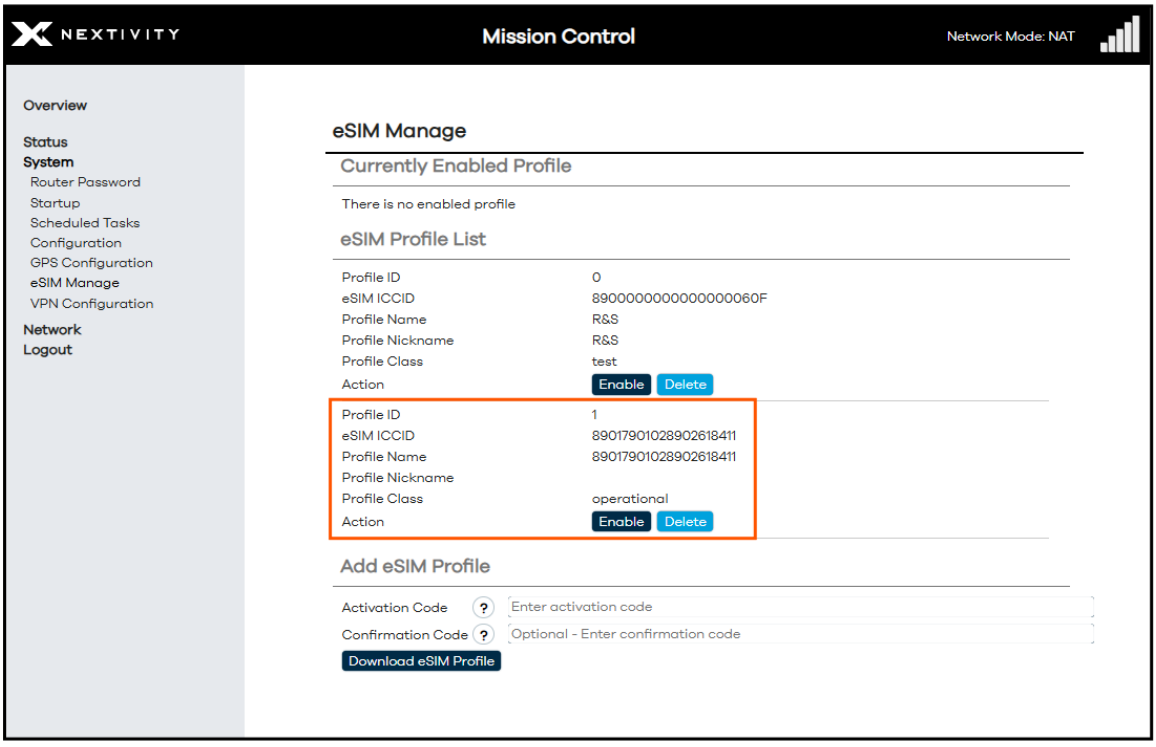


Figure 150: eSIM Manage – Completed eSIM Profile and operational

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

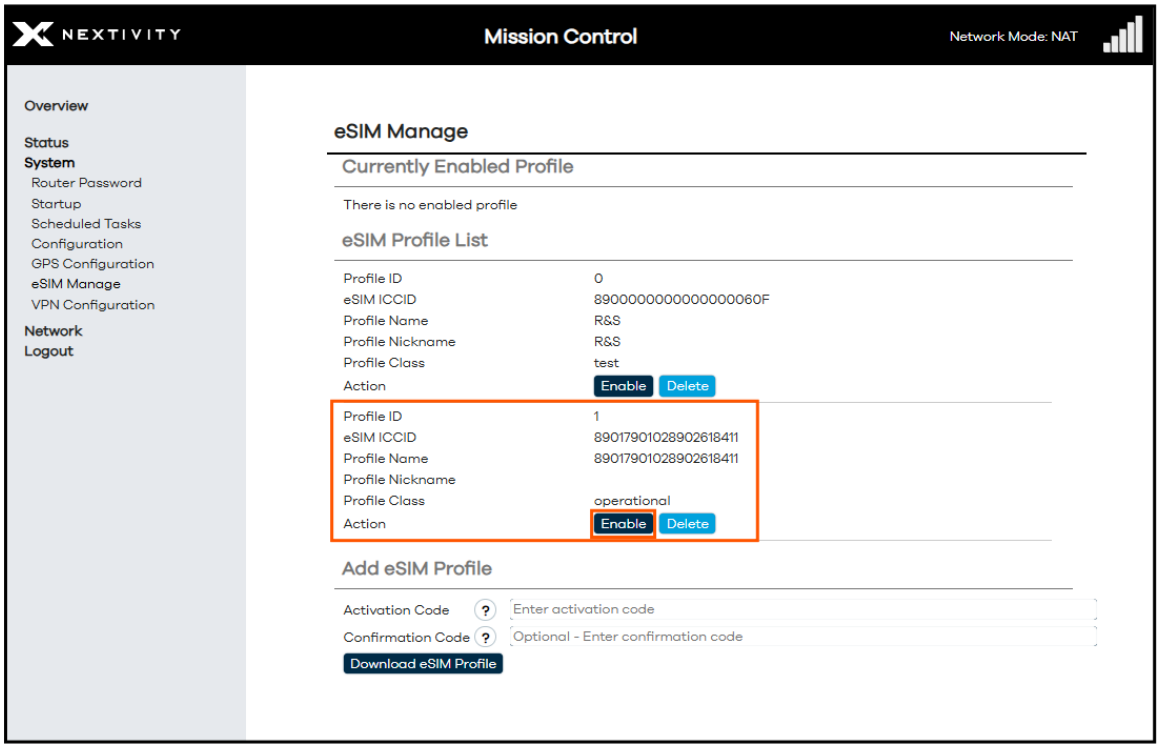


Figure 151: eSIM Manage – Enable eSIM

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

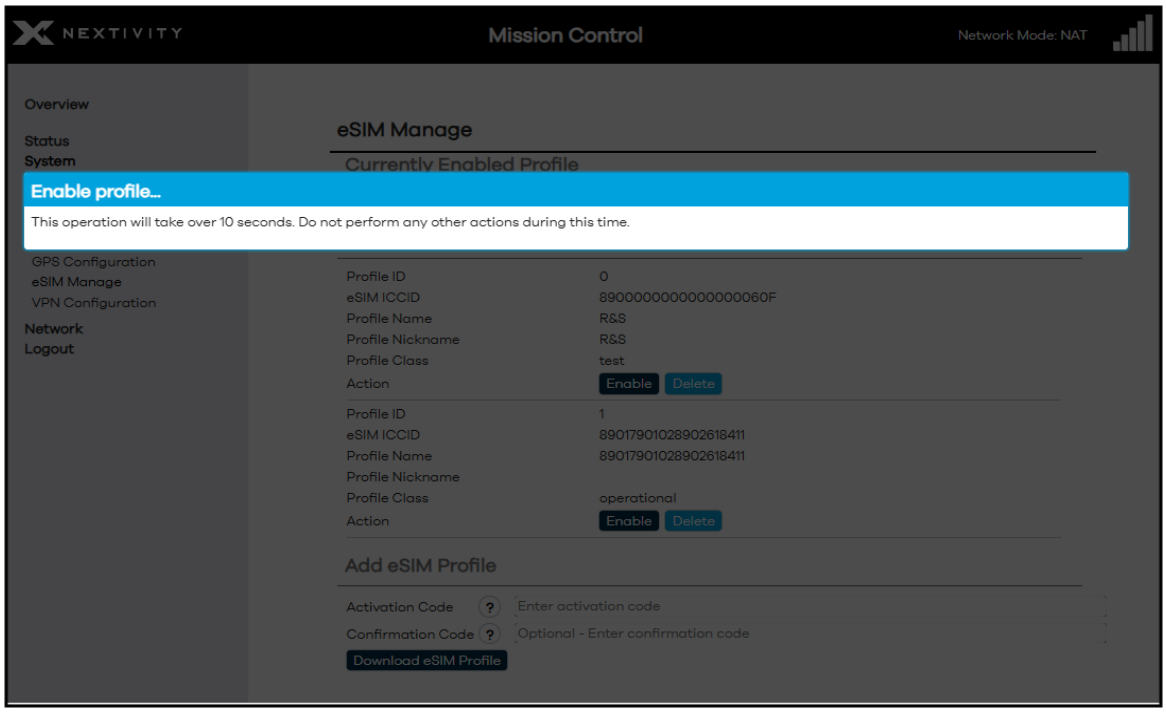


Figure 152: eSIM Manage – Wait for eSIM Profile to enable

13. 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 eSIM ready.

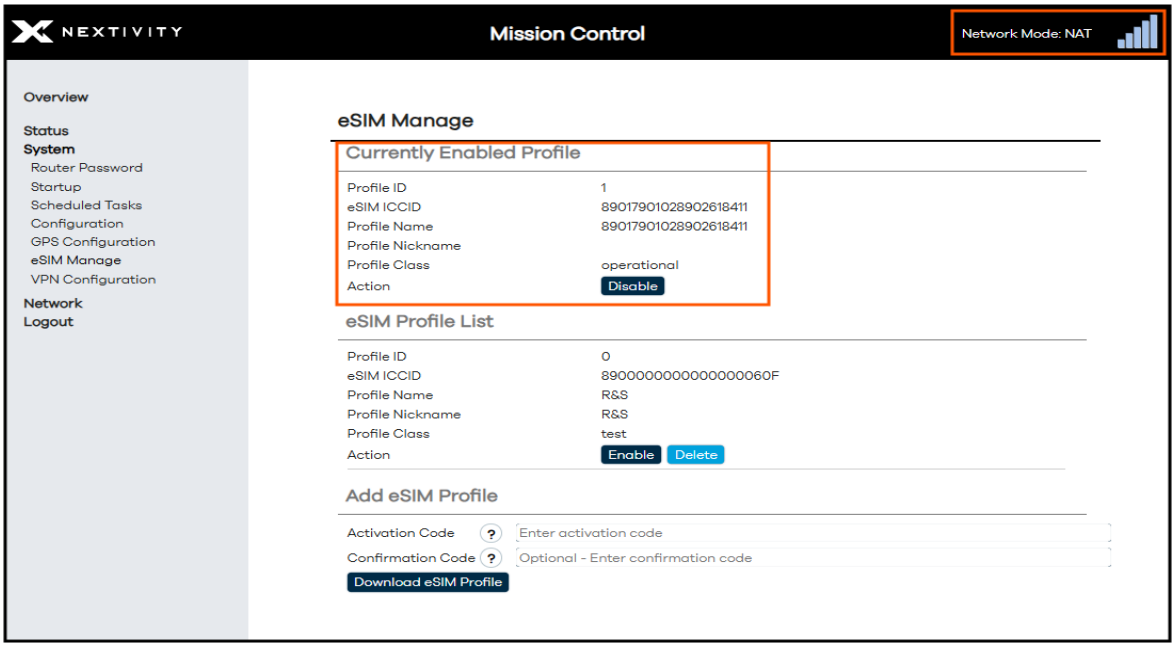


Figure 153: eSIM Manage – eSIM Profile in use

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

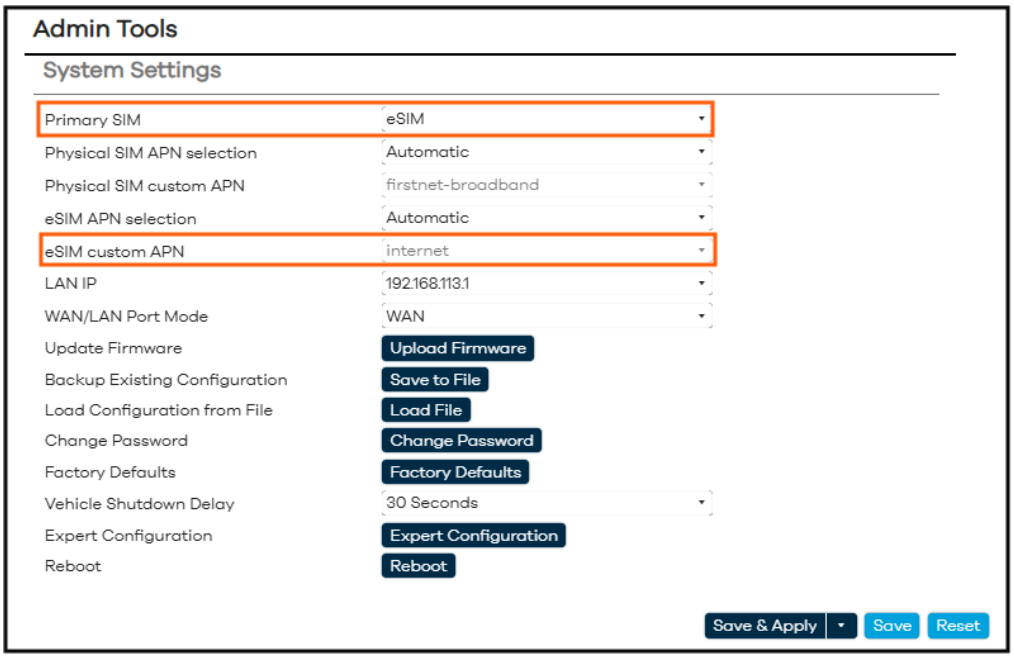


Figure 154: Admin Tools – eSIM custom APN

15. The WAN source can be disconnected, and internet connectivity will flow through the eSIM.

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

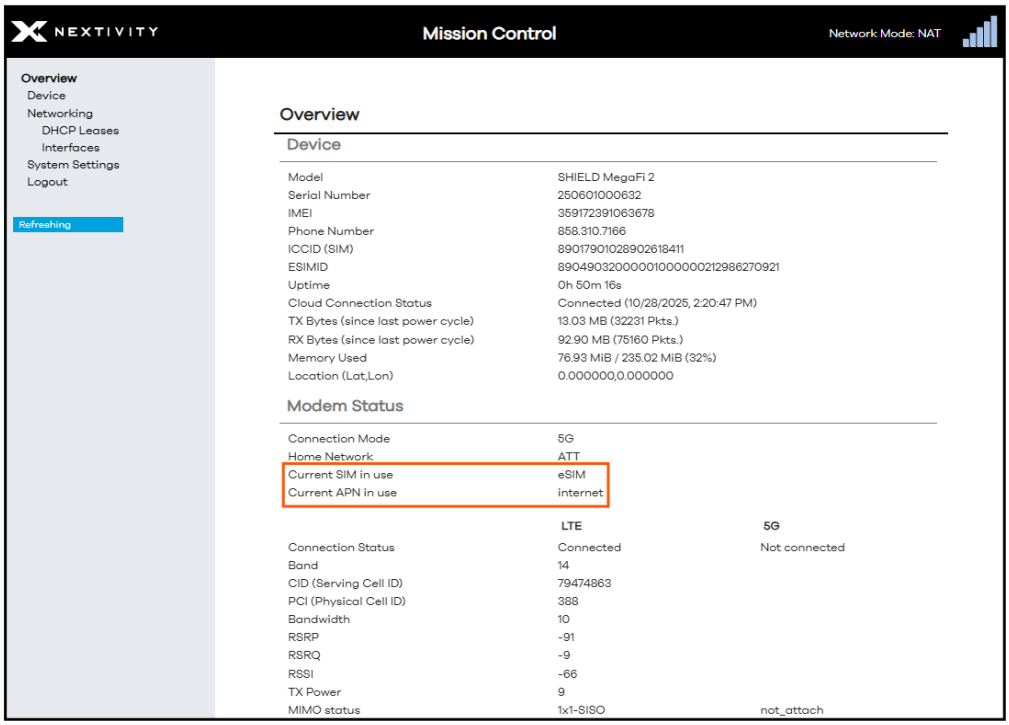


Figure 155: Modem Status – Current SIM in use

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

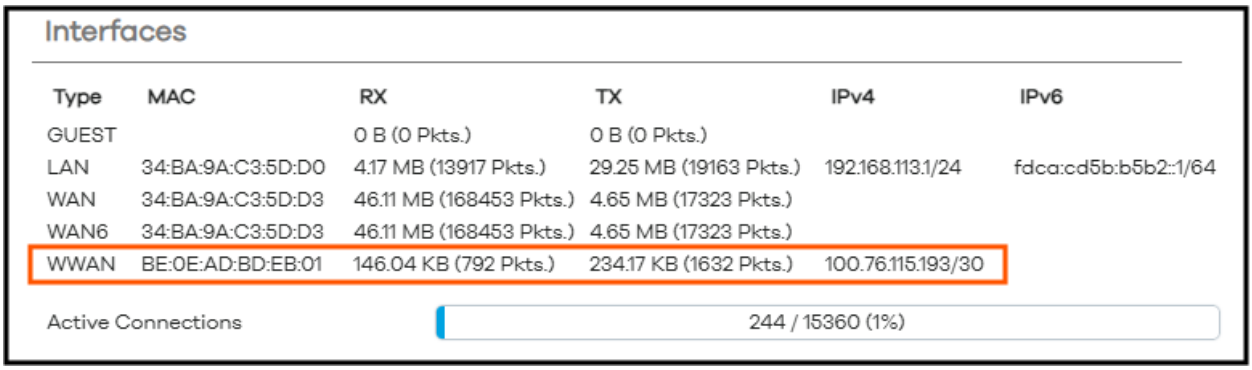


Figure 156: Interfaces – WWAN IP address

18. 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 **Automatic** from the list.

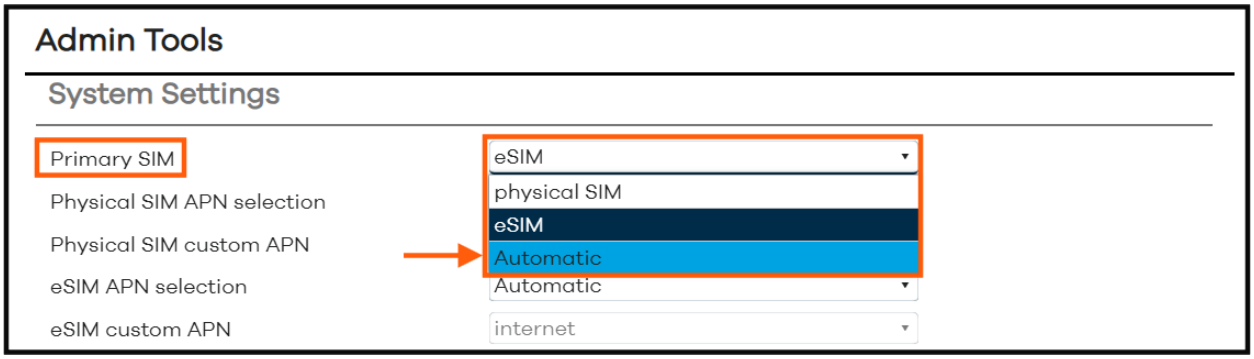


Figure 157: Admin Tools – Primary SIM set to Automatic

19. 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** is **physical SIM**.

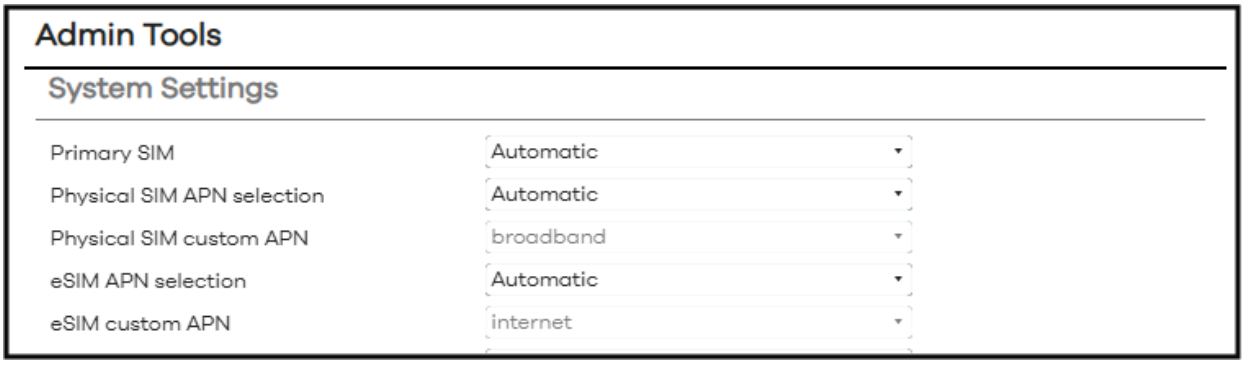


Figure 158: Admin Tools – SIM Settings

3.23.2 Disable and Delete eSIM Profile

If a currently enabled eSIM profile is no longer needed or you would like to use a different profile, do the following in Mission Control to disable it.

➲ **Note**: Proceed with deletion of eSIM profiles with caution. Deleting the eSIM profile requires an active internet connection to notify the eSIM management server. If the device is offline, the deletion will only occur locally, and the operator may still treat the profile as active. In this case the profile may not be recoverable or downloadable again.

1. Navigate to the **eSIM Manage** page.
2. If the **Primary SIM** setting is set to **Automatic** as described above or set to **physical SIM**, it is necessary to **set eSIM as Primary SIM** to manage eSIM profiles. Click on **set eSIM as Primary SIM** to begin.

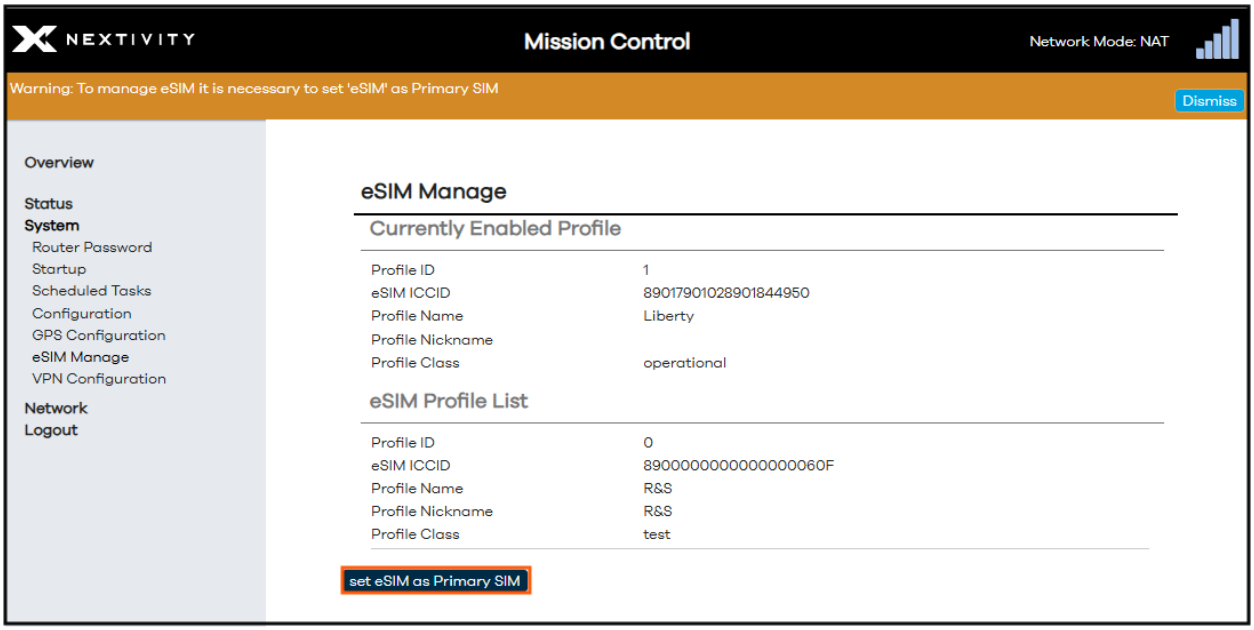


Figure 159: eSIM Manage – set eSIM as Primary SIM

3. Select the **Disable** button next to **Action** of the **Currently Enabled Profile**.

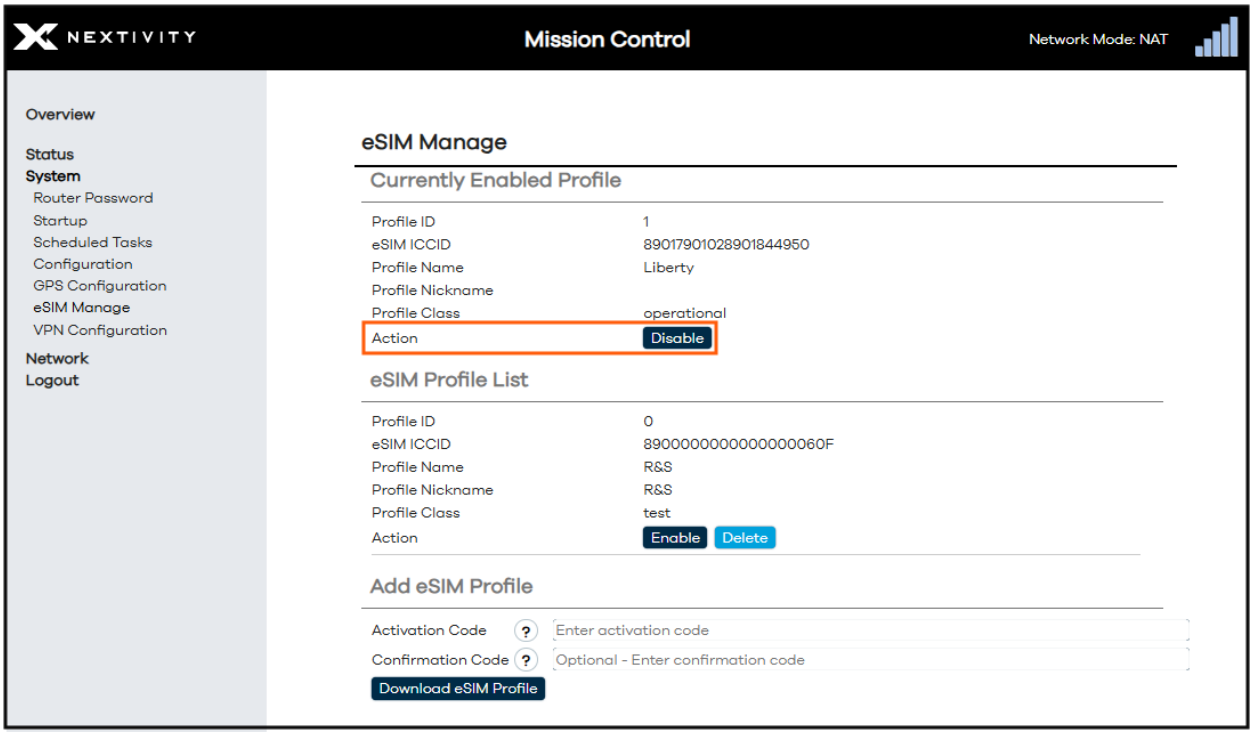


Figure 160: eSIM Manage – Disable Currently Enabled Profile

4. This action will take about 10 seconds to complete. If the MegaFi was currently active on eSIM, failover to physical SIM will take a longer.

Figure 161: Disable Currently Enabled Profile – 10 seconds

5. Delete the eSIM profile from the **eSIM Profile List**. **Note** that an active internet connection is required to notify the eSIM management server. Otherwise, the eSIM may become unrecoverable or downloadable again.

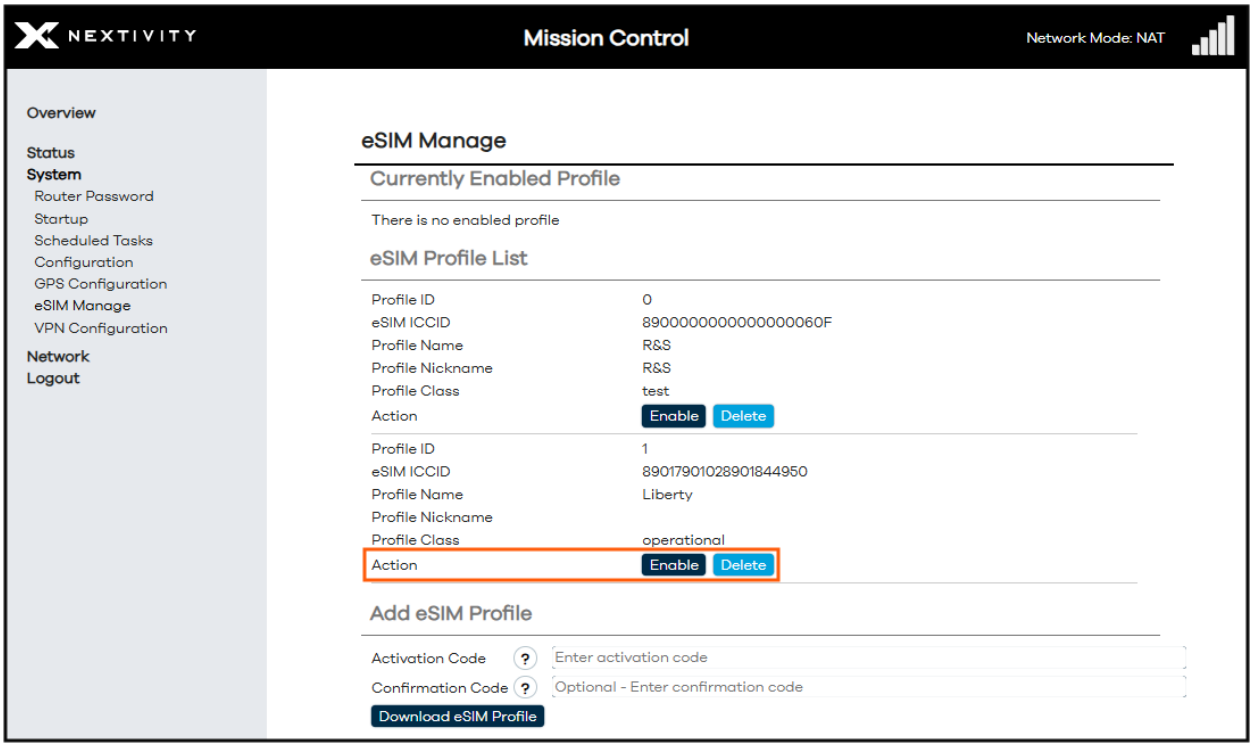


Figure 162: Delete eSIM Profile

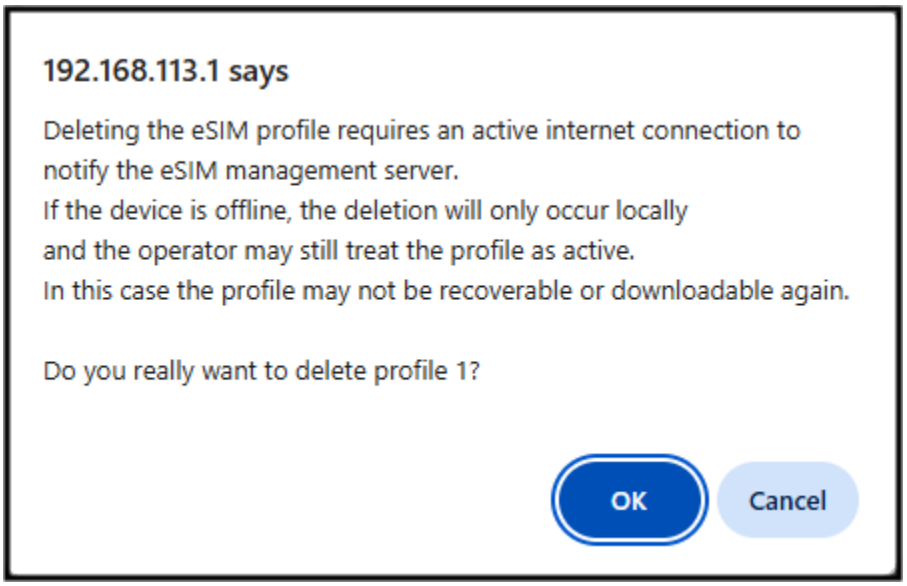


Figure 163: Delete eSIM Profile Warning

3.23.3 Purge eSIM Profile

In case a MegaFi is repurposed or needs to be returned for repair or replacement, the eSIM profile can be purged from the MegaFi device. Do the following in Mission Control.

➲ **Note**: Proceed with purge of eSIM profiles with caution. Purging the eSIM profile requires an active internet connection to notify the eSIM management server. If the device is offline, the purge will only occur locally, and the operator may still treat the profile as active. In this case the profile may not be recoverable or downloadable again.

1. Connect a WAN source to the WAN port of the MegaFi device. A purge of the eSIM profile requires this.
2. Login to Mission Control and navigate to **Expert Configurations > System > eSIM Manage**.
3. Locate the target eSIM profile and select **Disable**.
4. Now select the **Delete** button next to the target eSIM profile.
5. Navigate to **System > Configuration**.
6. Under the **Other** section, select **Enabled** from the drop-down menu for the **Purge eSIM profiles if Factory Defaults** setting.

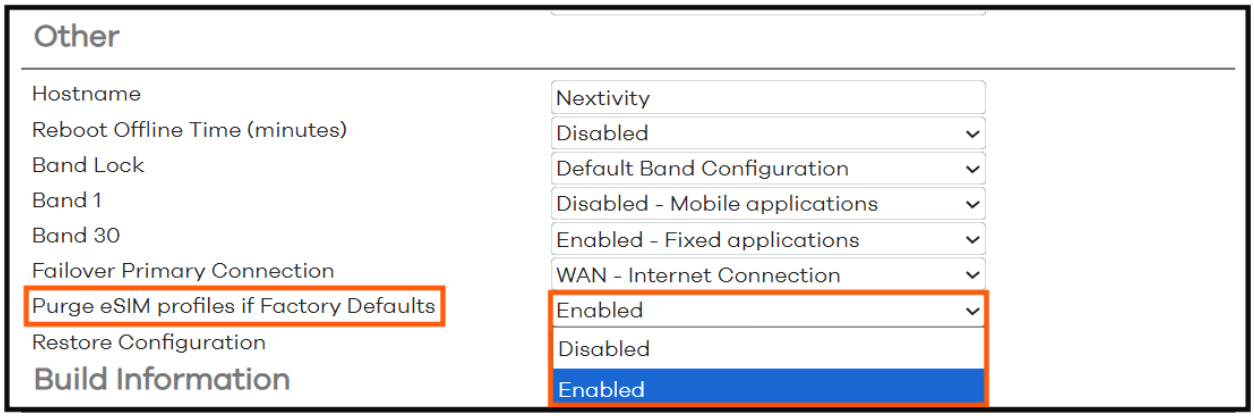


Figure 166: eSIM Profile Purge setting

7. Click **Save & Apply** at the bottom.
8. Make sure the MegaFi has a WAN internet source connected.
9. Right under **Purge eSIM profiles if Factory Defaults**, click on the **Factory Defaults** button next to **Restore Configuration** and confirm by clicking on OK on the popup box to proceed with this action.

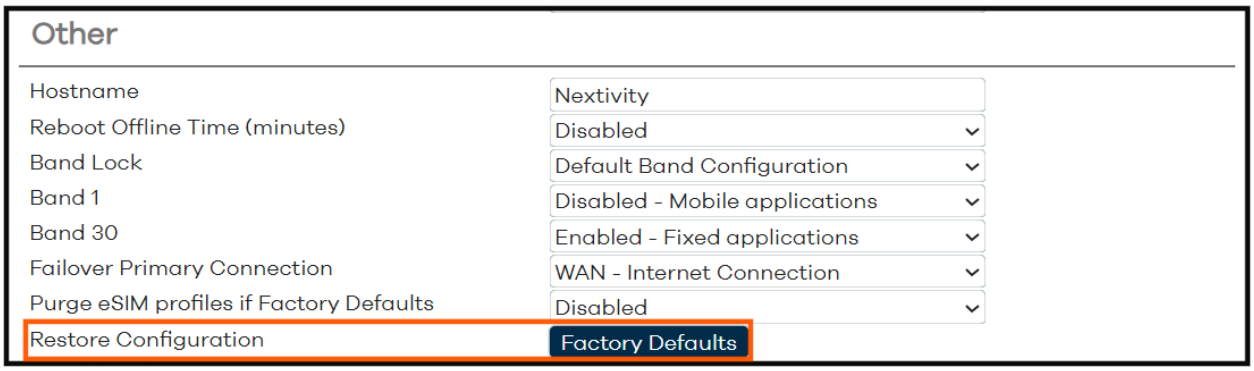


Figure 167: Restore Configuration – Factory Defaults button

10. After the device boots up check the **eSIM Manage** page. Set eSIM as Primary SIM and verify that the eSIM profiles are deleted, they are all removed with the exception of the test eSIM. Check the configuration tab, the Purge eSIM profiles if Factory Default = Disabled by default.

3.24 Download Troubleshooting Files

A feature was added to the Admin Tools area where a collection of troubleshooting files can be downloaded from the MegaFi. A tarball file is created and this can then be easily forwarded to the Nextivity support team for further analysis. Do the following in Mission Control to download this file.

1. In Mission Control, navigate to **Overview > System Settings** under **Admin Tools**.

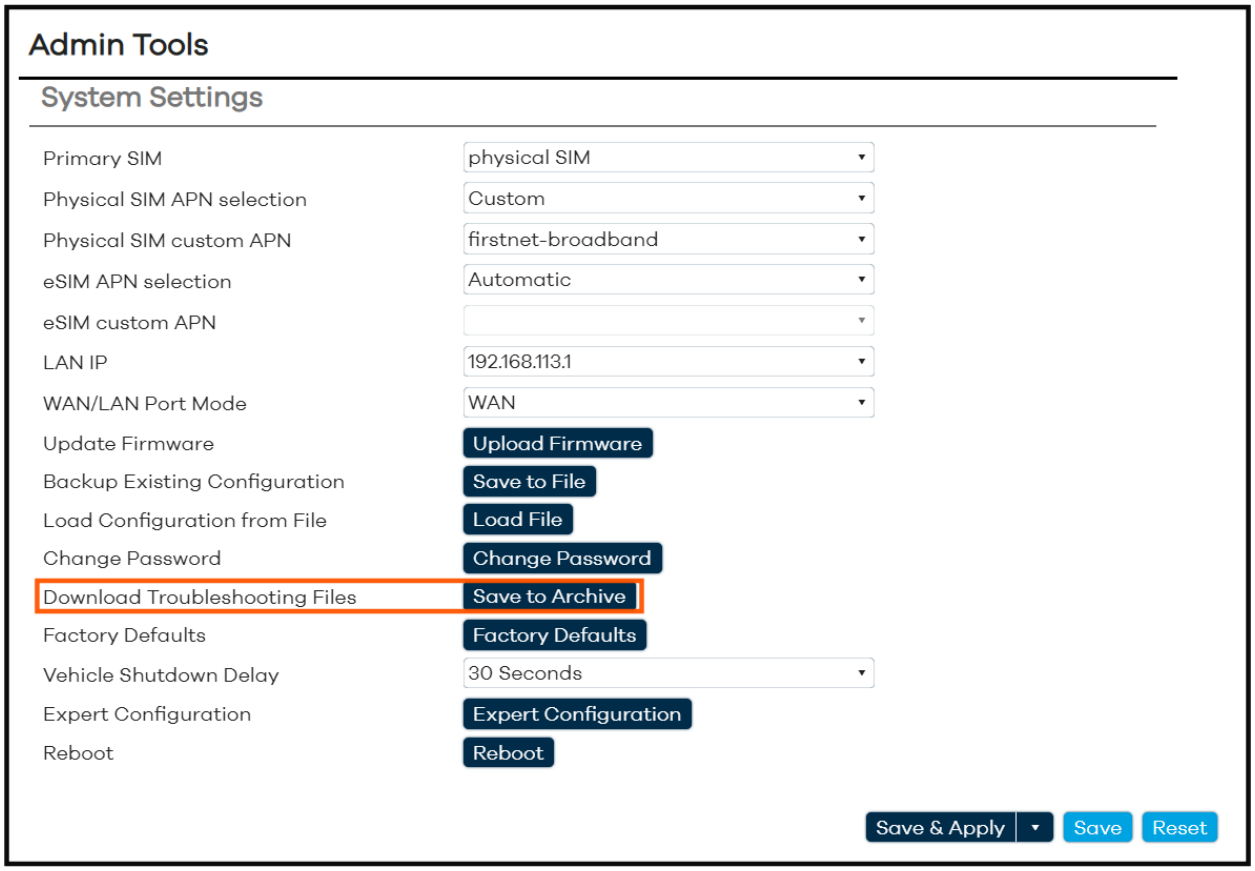


Figure 168: System Settings – Expert Configuration

2. Click on **Save to Archive** next to **Download Troubleshooting Files** to download the collection of files.
3. Look in the Downloads folder of your computer. The file will be called **troubleshooting.files.tar.gz**.

3.25 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

3.25.1 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.

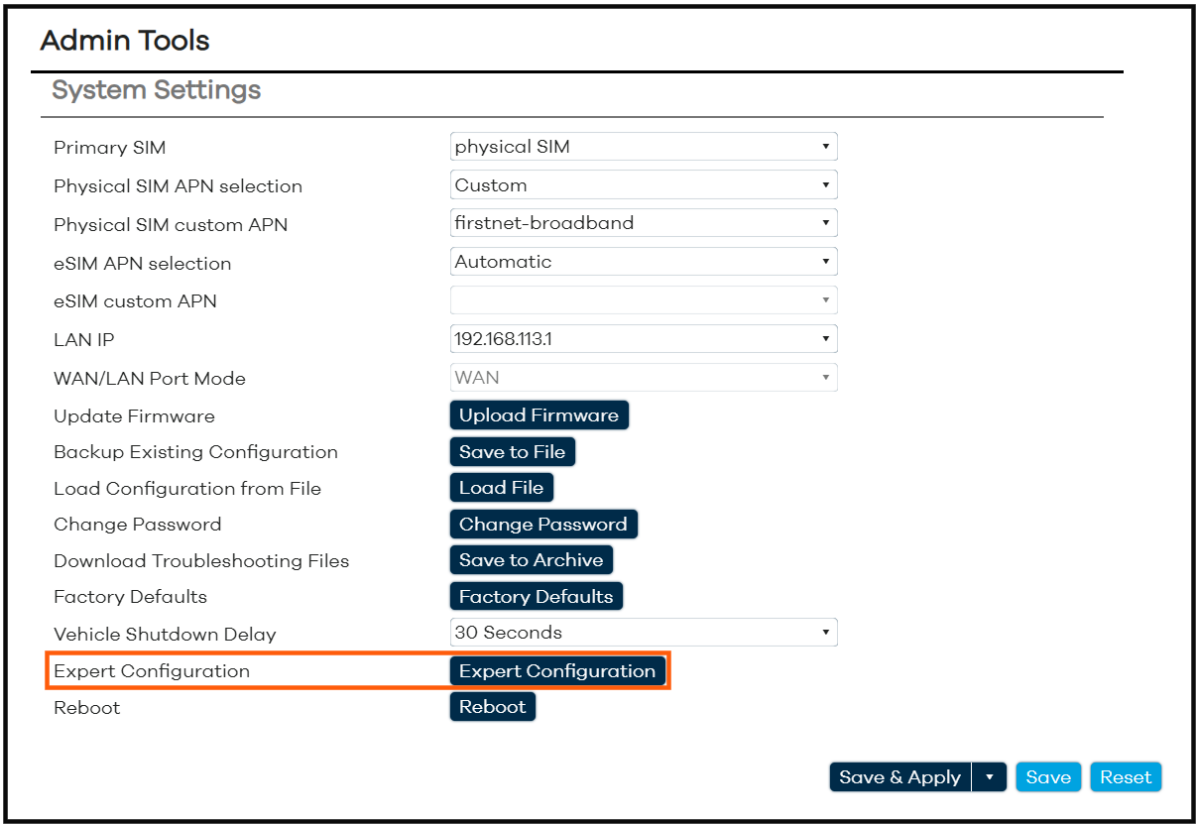


Figure 169: System Settings – Expert Configuration

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

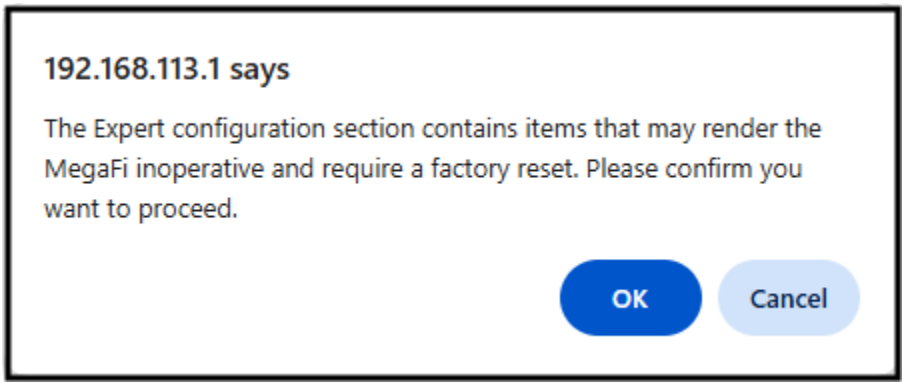


Figure 170: Confirmation to Enter Expert Configuration mode

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

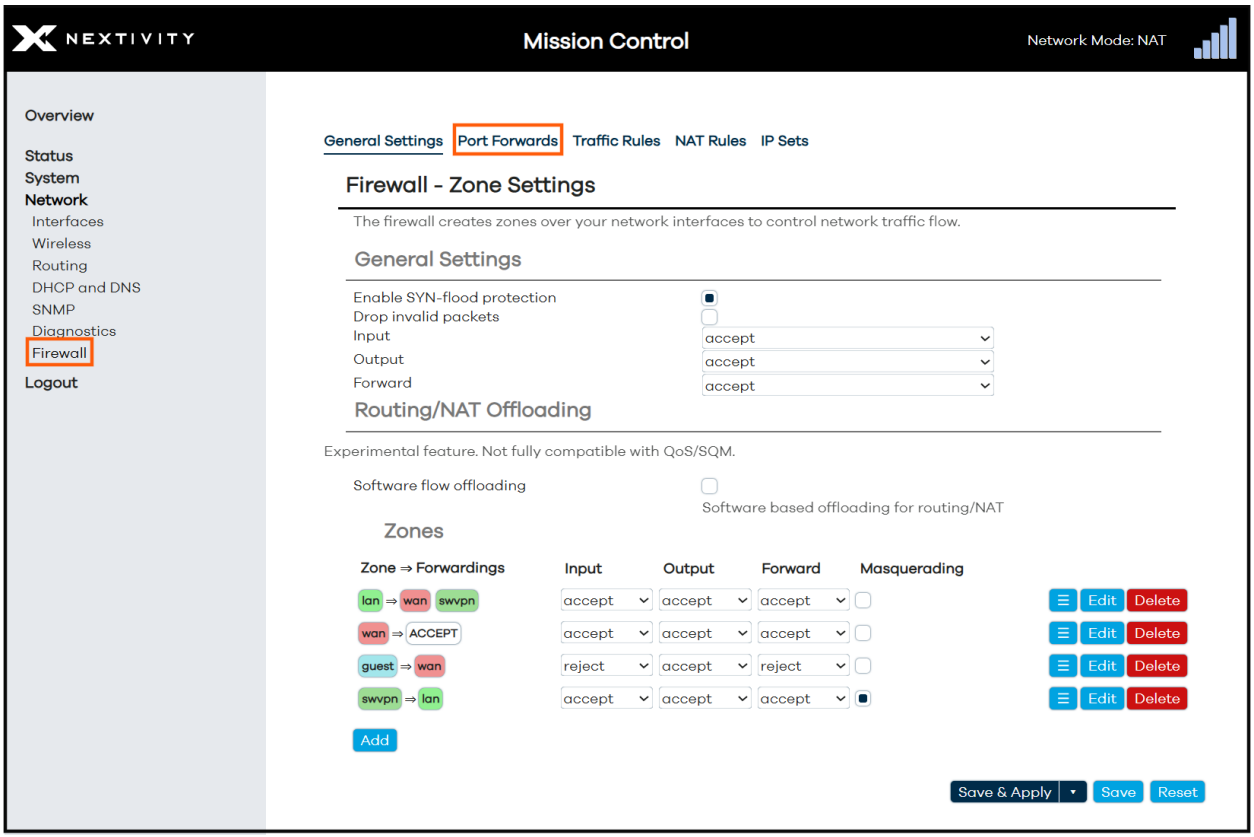


Figure 171: Firewall – General Settings

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

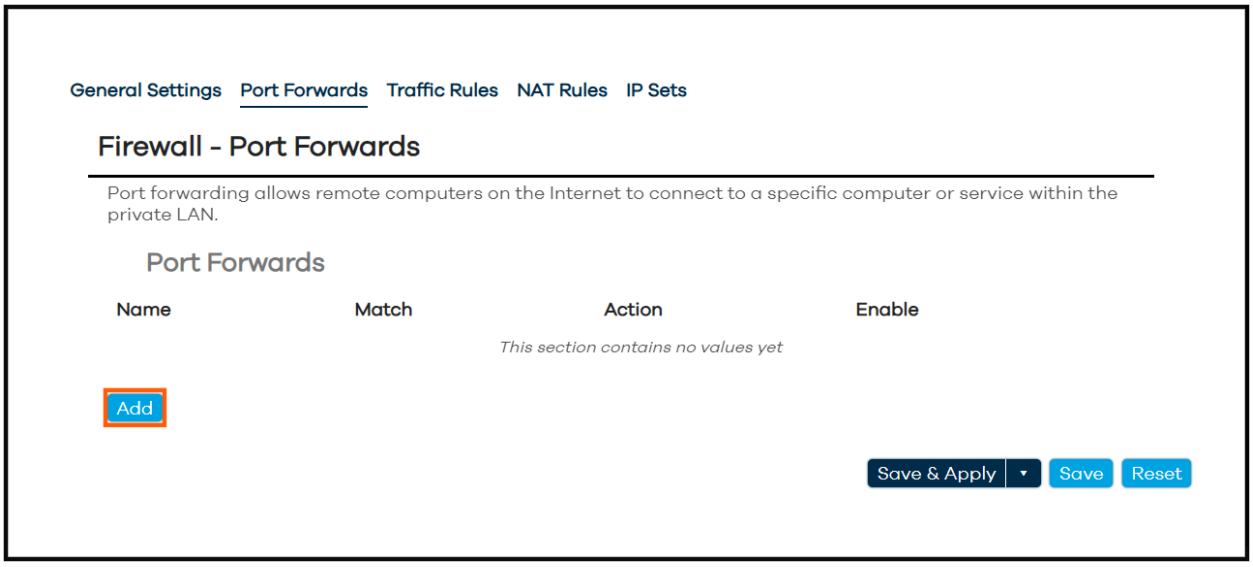


Figure 172: Firewall – Port Forwards Add

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

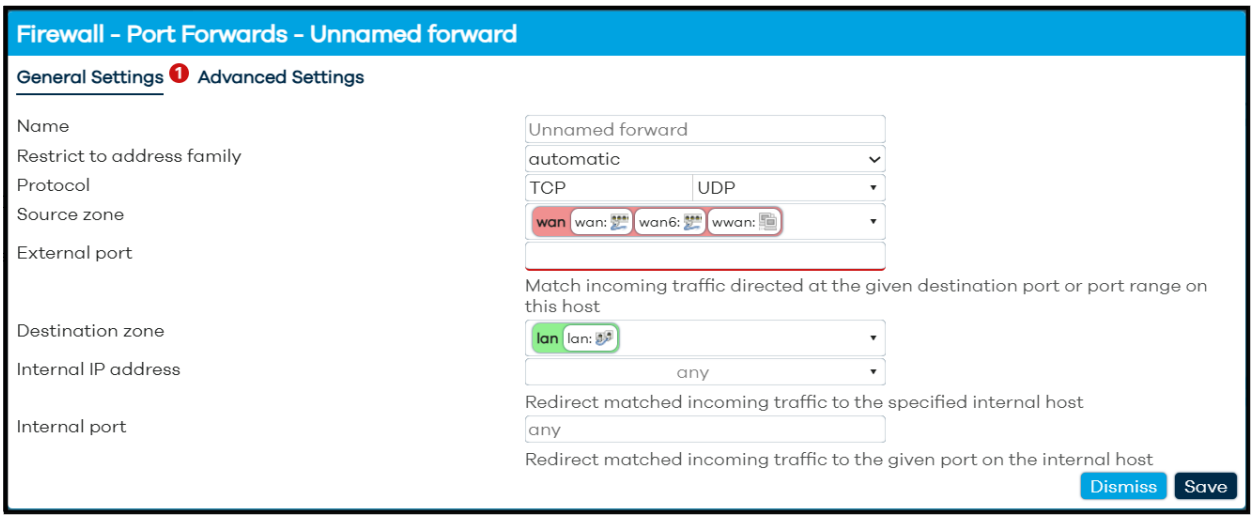


Figure 174: Firewall – Port Forwards General Settings

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.

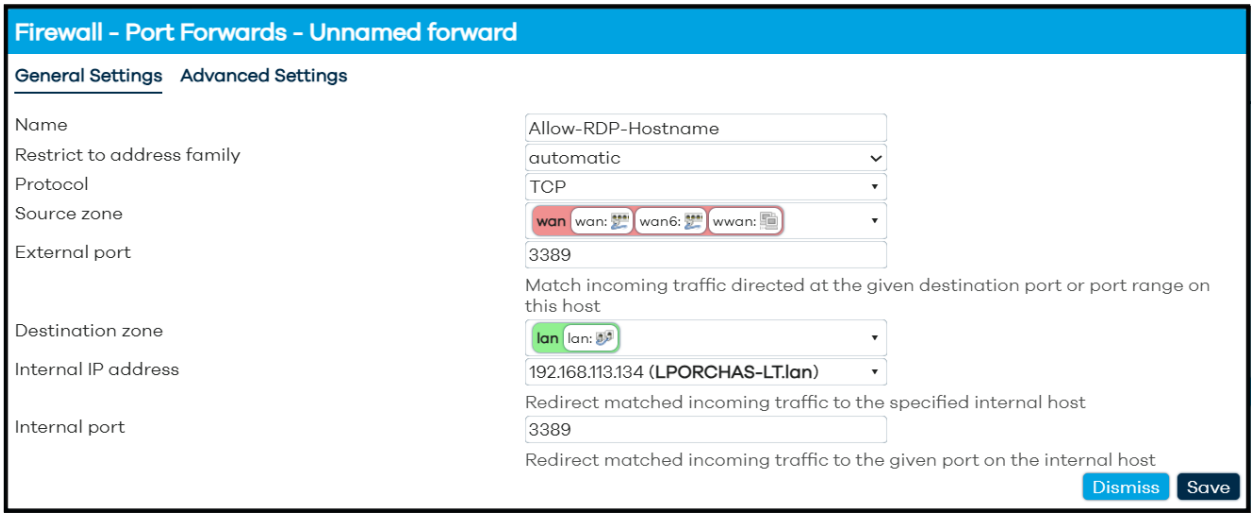


Figure 175: Firewall – Port Forwards RDP example

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.

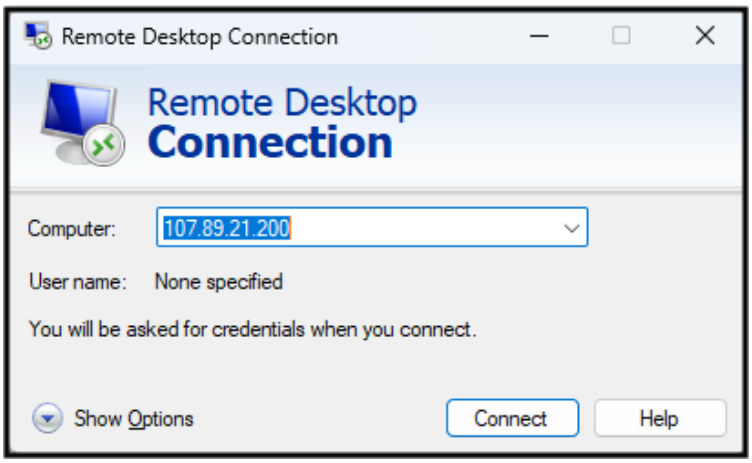


Figure 176: Remote user preparing an RDP connection

3.25.2 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.

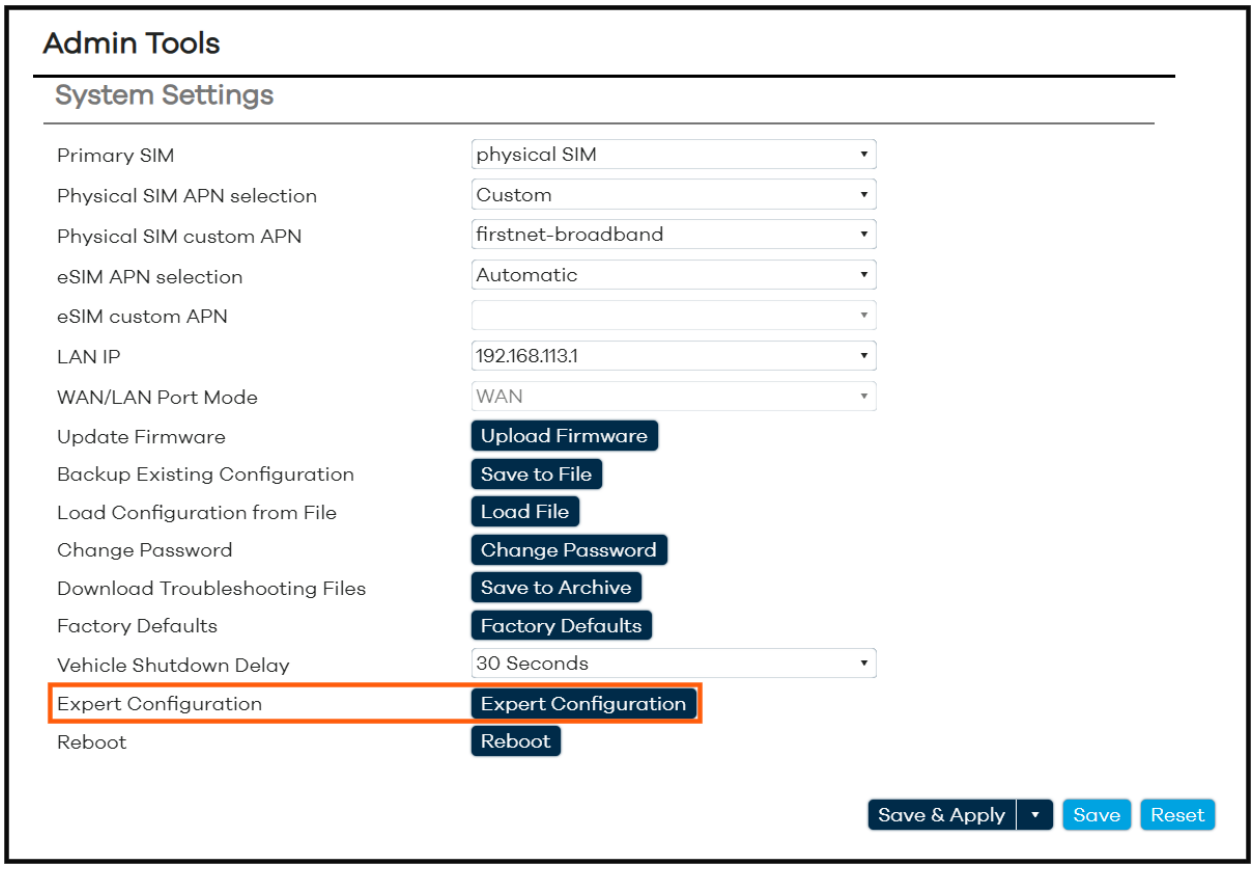


Figure 177: System Settings – Expert Configuration

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

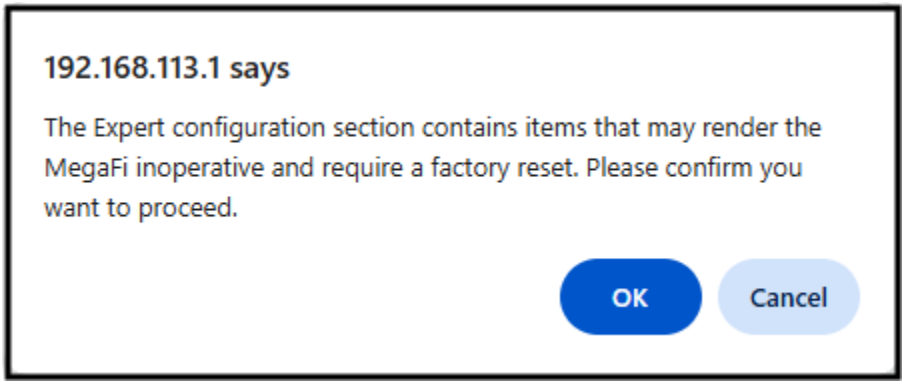


Figure 178: Confirmation to Enter Expert Configuration mode

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

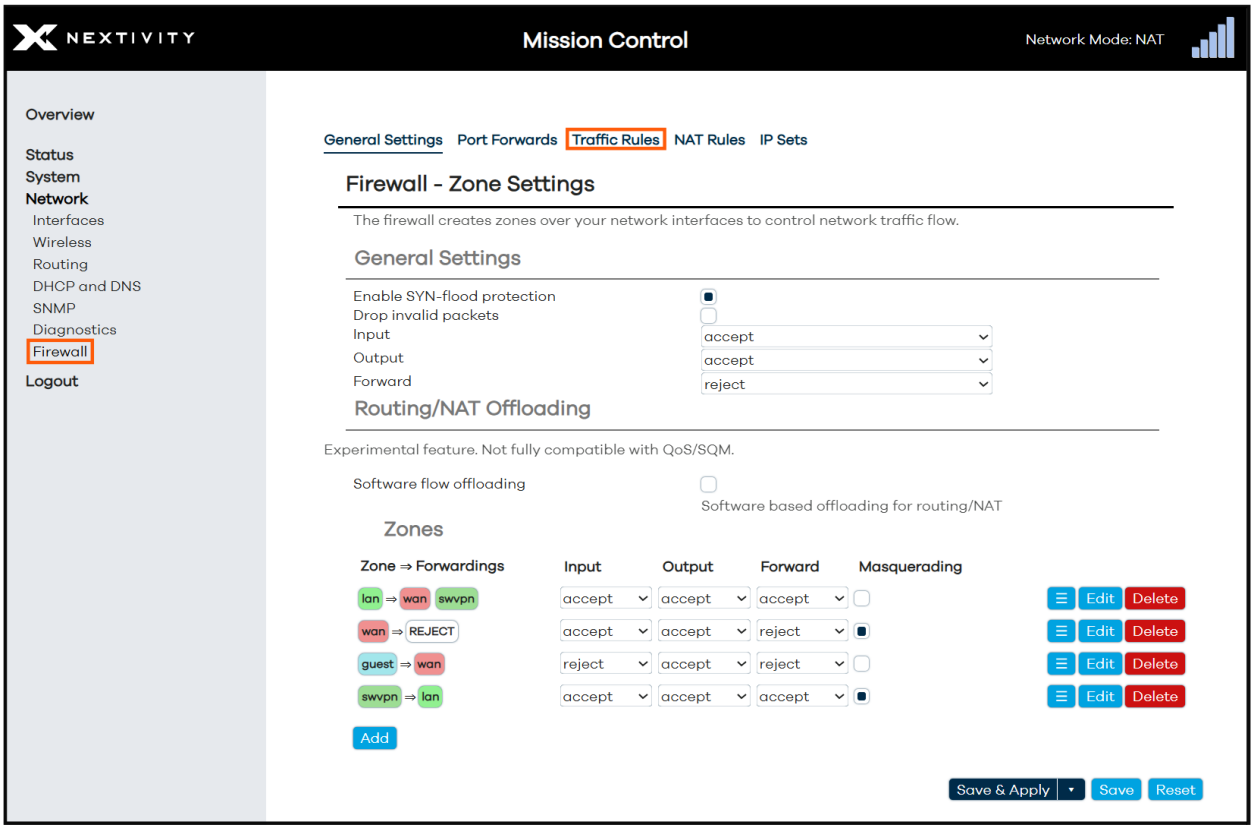


Figure 179: Firewall – General Settings

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

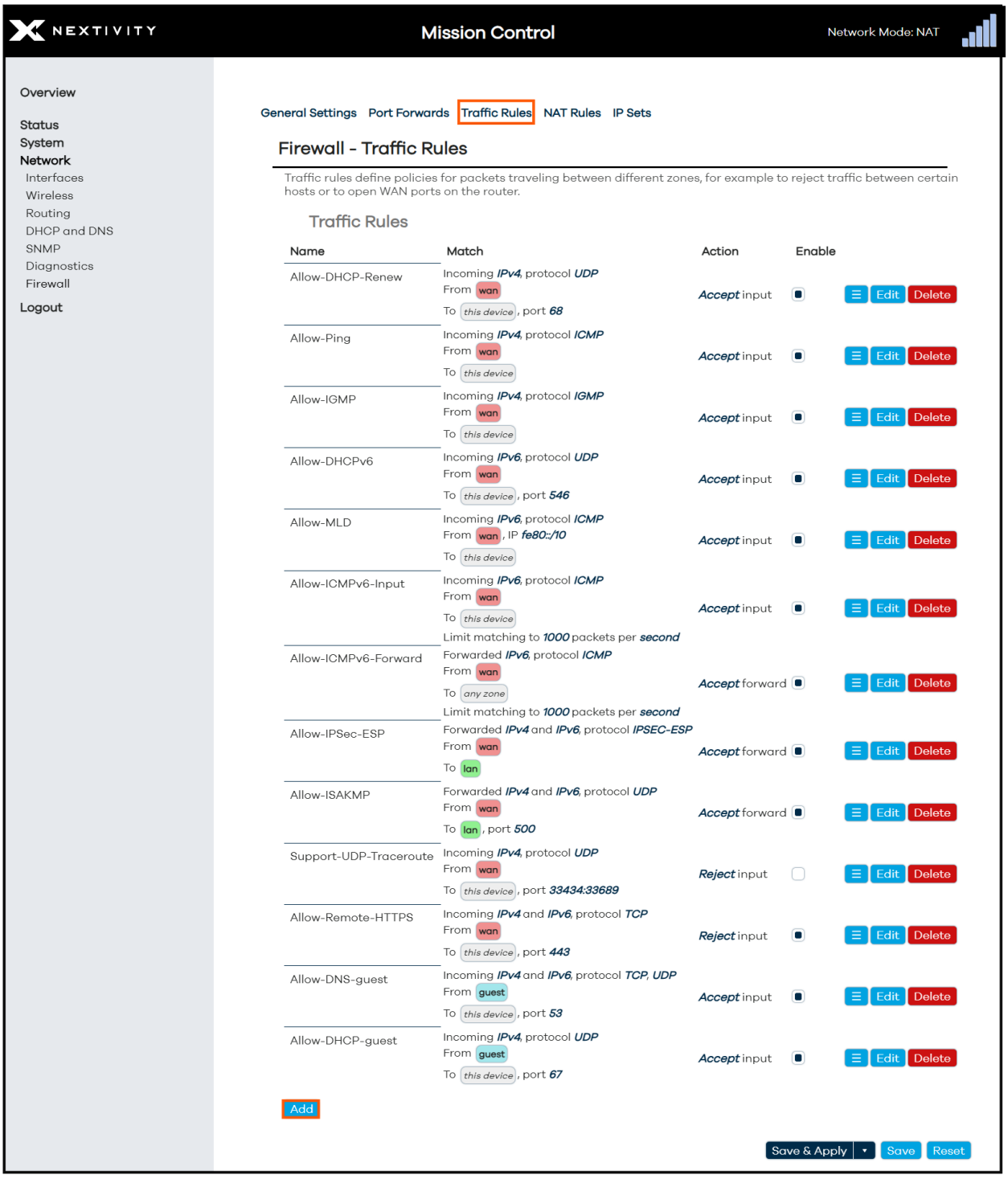


Figure 180: Firewall – Traffic Rules

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**

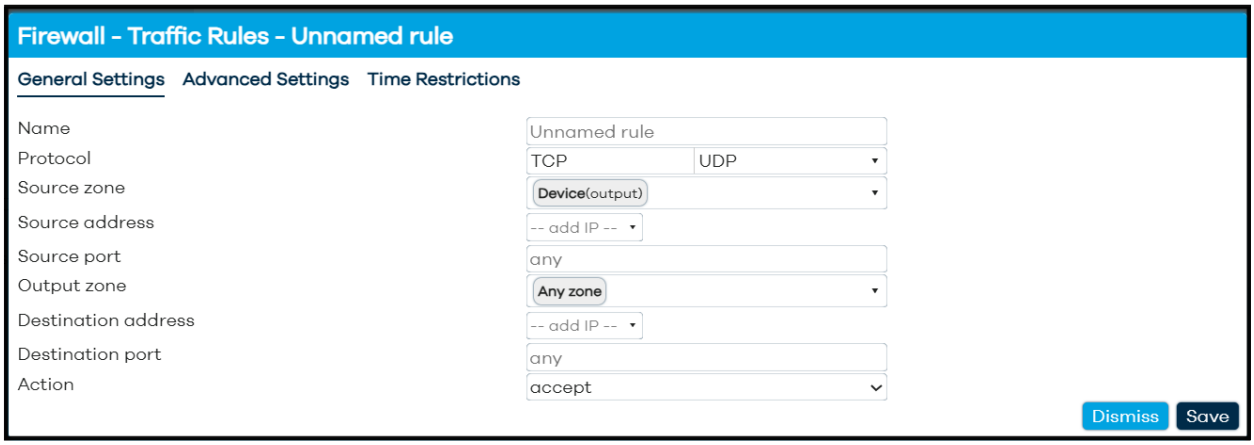


Figure 181: Firewall – Traffic Rules General Settings

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.

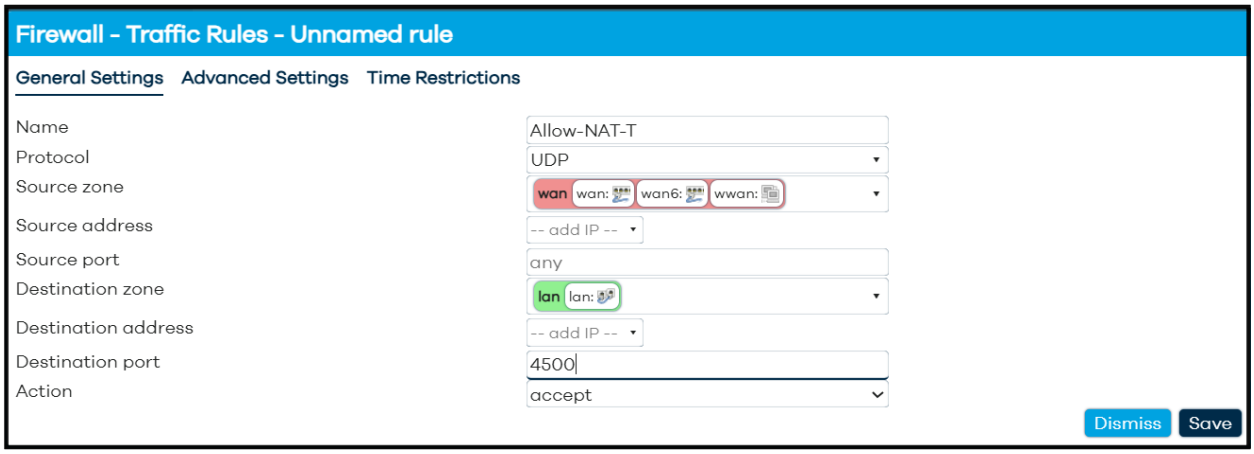


Figure 182: Firewall – Traffic Rules NAT-T (port 4500) example

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.

3.26 Firewall Diagnostics

Firewall Diagnostics can be used to help troubleshoot blocked traffic that is expected inbound through the MegaFi firewall. Turn this feature on for the selected duration to help analyze this traffic that is not normally recorded in the system log. 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.

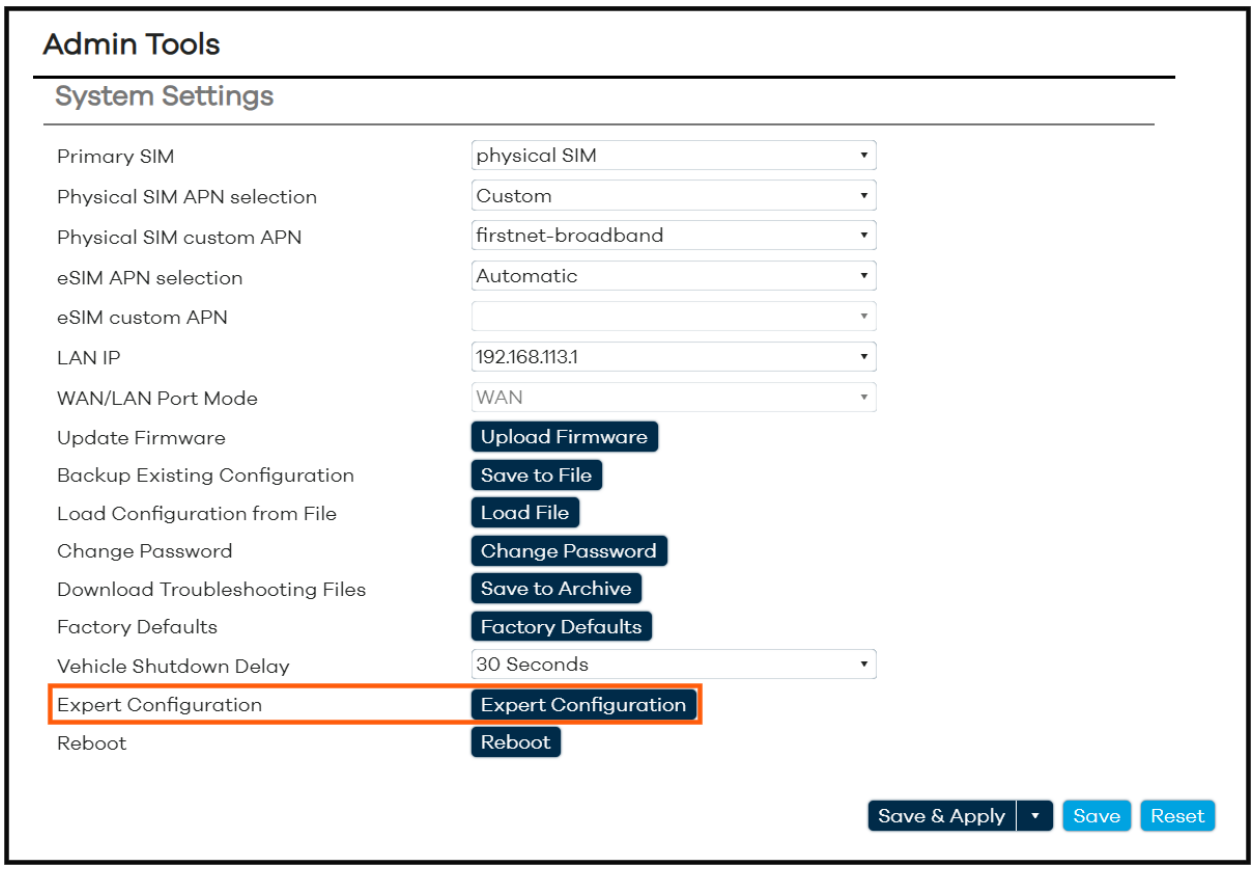


Figure 183: System Settings – Expert Configuration

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

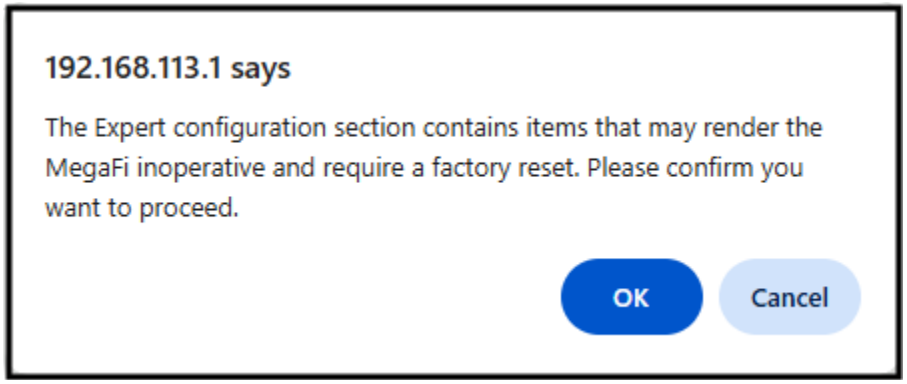


Figure 184: Confirmation to Enter Expert Configuration mode

4. Navigate to **Status > Firewall Diagnostics.**

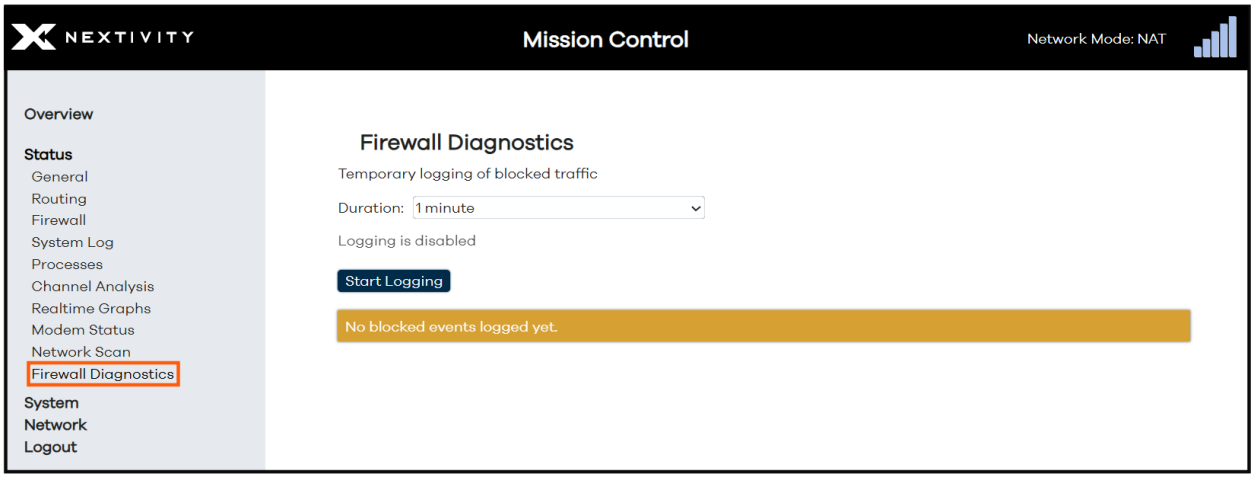


Figure 185: Firewall Diagnostics

5. Select the duration from the drop-down menu from the 1, 3, 5, 10, 15, or 30 minutes.

Figure 186: Firewall Diagnostics – Duration options

6. Then click on **Start Logging** to start. A timer will commence and start to count down. Press **Stop Logging** to prematurely stop the action. Induce perceived incoming traffic during this time frame to see any blocked traffic.

Figure 187: Firewall Diagnostics – Count down timer and Stop Logging – no blocked events

7. If there are any blocked events, the blocked events will be displayed below under Recently Blocked Events as well as in the System Log.

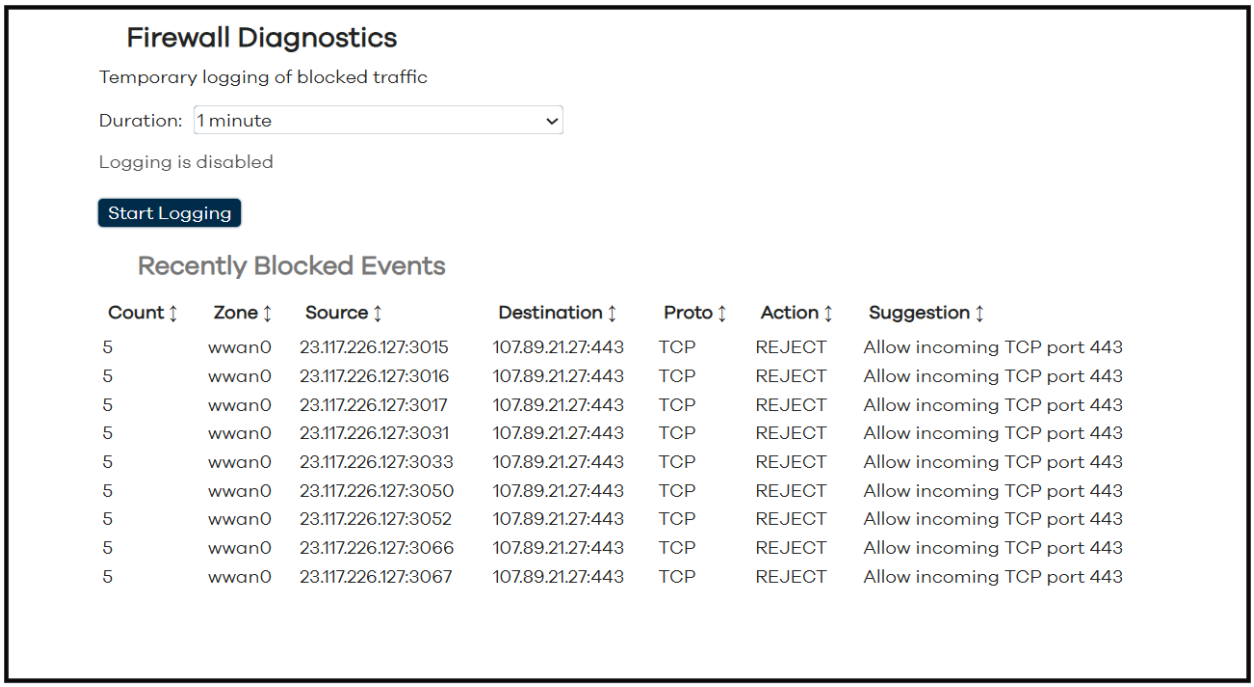


Figure 188: Firewall Diagnostics – Recently Blocked events

Navigate to **Status > System Log** and scroll all the way down the System Log to review any rejected entries.

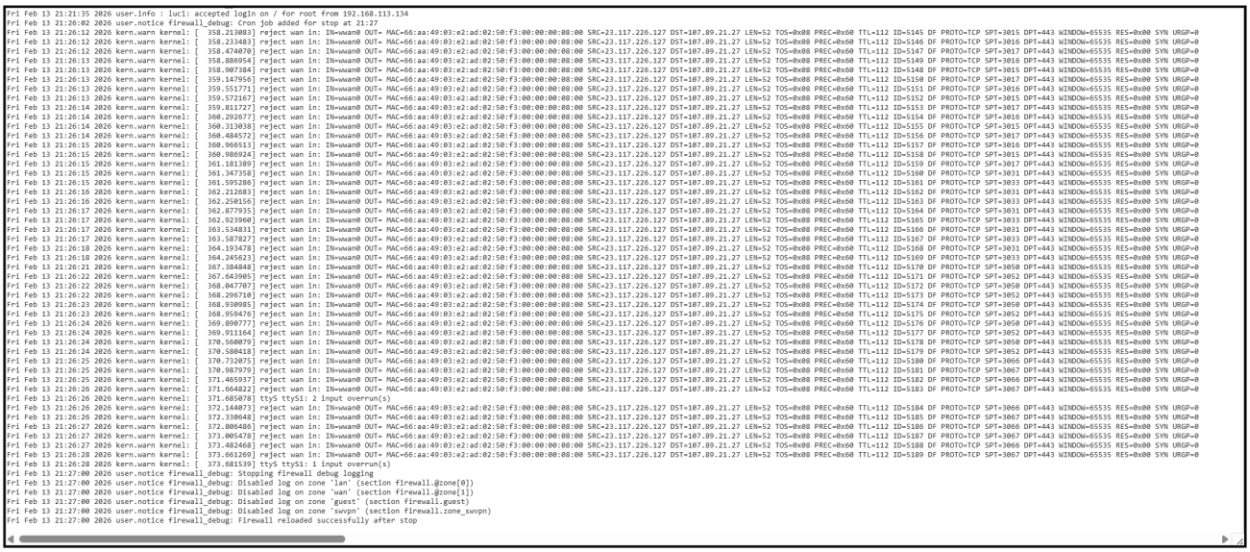


Figure 189: System Log – Blocked events

In the example above, the rejected or blocked events were blocked at the wwan0 interface and destined to IP address 107.89.21.27 on port 443 using TCP protocol. The source of this traffic was noted as coming from an IP address of 23.117.226.127.

This type of traffic is typical of an incoming HTTPS remote access request to the destined device. The suggestion is given as to **Allow incoming TCP port 443**, but only do so if you trust the source.

Hint: There is a predefined Traffic Rule to **Allow-Remote-HTTPS** in the MegaFi Firewall – Traffic Rules table that is set to **Reject**. The rule can easily be modified to **Accept** by unchecking the box next to **Reject input** and **Save & Apply**.

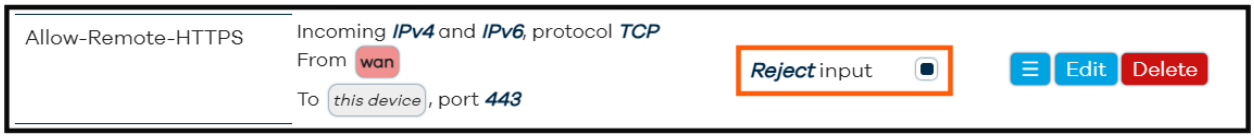


Figure 190: Firewall Traffic Rules – Allow-Remote-HTTPS