MOFI6500-5GXeLTE User Manual

(Non SIM, EM7411, EM7411-DUAL, RM520-HP, RM520-HP-DUAL)

User Guide

Advanced High Performance Cellular Router

MoFi Network Inc.

www.mofinetwork.com | +1-888-499-0123 (Tech Support open 7 days a week)

Table of Contents

Getting Started

Quick Reference — Common Tasks

---

1. Welcome

The MoFi 6500 is an enterprise-grade cellular router designed for reliable internet connectivity in any environment. Depending on which model you have, it can support 4G/LTE, 5G SA/NSA, and wired WAN connections with automatic failover, load balancing, and remote management.
These features can also be set and managed via the MoFi ACS cloud platform.

Key Features

- **5G & LTE Connectivity** — With the RM520-HP models, it supports 5G SA, 5G NSA, and LTE with carrier aggregation
- **LTE only option** — Sierra Wireless EM7411 model supporting 4G/LTE with 2 x carrier aggregation

- **Dual Module Support** — Some models include two cellular modems for redundancy both LTE and 5G
- **Automatic Failover** — Seamlessly switches between cellular, WAN, WiFi repeater, and USB connections
- **Load Balancing** — Combine multiple internet connections for increased bandwidth (more work done in less time, like have 2 routers in 1)
- **WiFi 6 with Embedded Boosters**— Dual-band 2.4 GHz and 5 GHz wireless (802.11ax) with build in WiFi boosters to give the best speed and range
- **VPN Server** — Built-in WireGuard and Open VPN servers for secure remote access
- **VPN Client Support** — ProtonVPN, ExpressVPN, NordVPN, IPVanish, PIA, CyberGhost, PureVPN, OpenVPN, OpenConnect, Tailscale, ZeroTier, L2TP/IPSec, and MoFi-to-MoFi VPN
- **Remote Management** — Cloud-based ACS portal for managing routers from anywhere
- **CloudLink** — Static public IP service for cellular connections without a public IP
- **IP Passthrough** — Pass the modem's IP directly to a connected device
- **Captive Portal** — Guest network with splash page authentication
- **Enterprise Security** — Firewall, port filtering, attack defense (banIP), MAC filtering, country blocking
- **VLAN Support** — Segment your network into isolated virtual LANs
- **Bandwidth Management** — Speed limiters, usage monitoring, ad blocking, website blocking, WiFi scheduling
- **SIM Failover** — Automatic switching between dual SIM slots

What's in the Box (depends on which model)

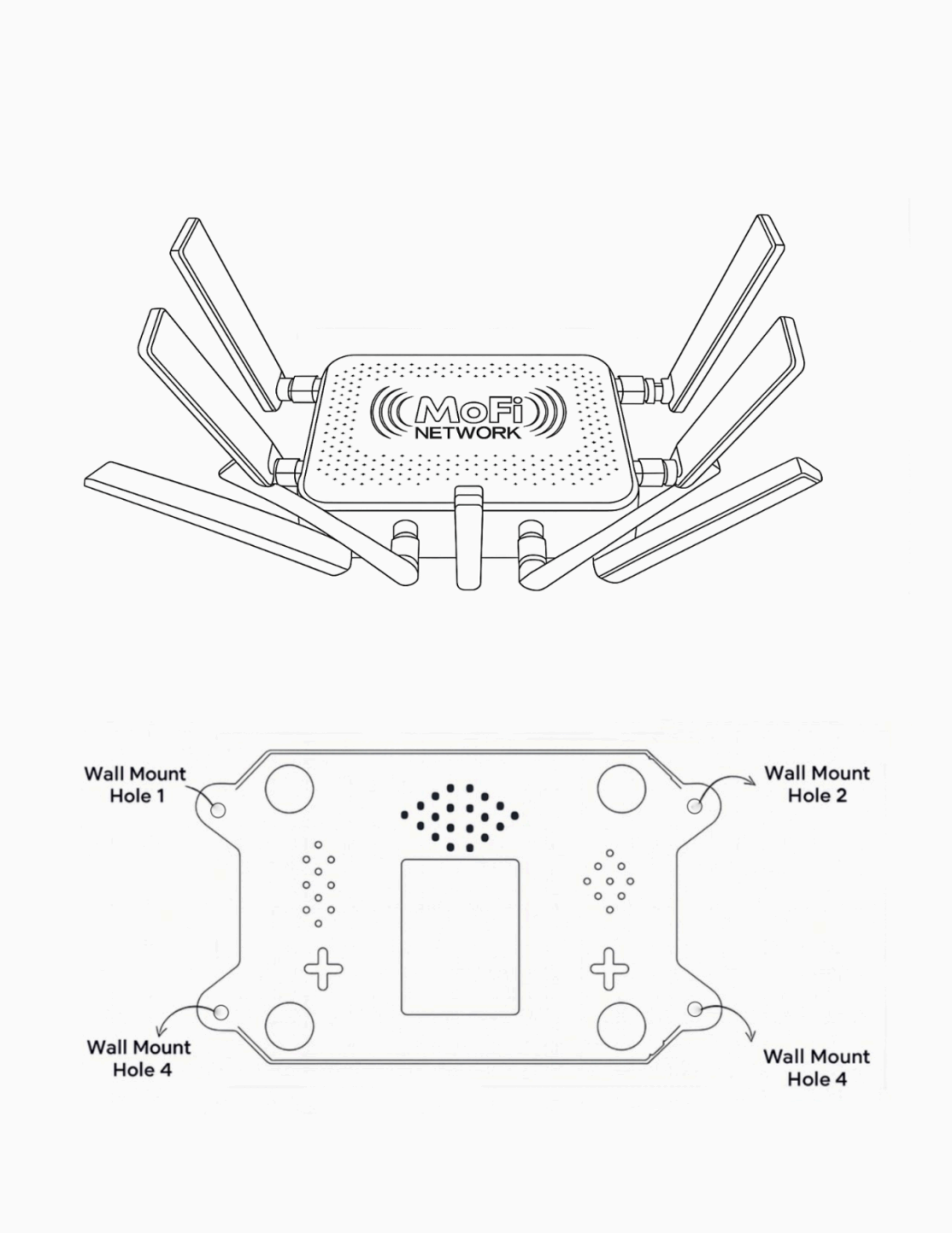
- MoFi 6500 Router
- 12V DC power adapter (3.5AMP Rating)
- 10 Feet Ethernet cable (Cat6e)
- If cellular model, 2, 4 or 8 External cellular antennas (SMA connectors)
- 5 External WiFi antennas
- Quick start guide

---

2. Hardware Overview

Device Design — Front Panel

Figure 1: MOFI6500-5GXeLTE-5GXeLT-RM520-HP Front View



MoFi6500-5GXeLTE-RM520-HP Top View and Wall Mount Holes

Figure 2: Top View and Wall Mount Hole Locations

The MOFI6500-5GXeLTE features a rugged metal casing with the MoFi Network logo on top. The MOFI6500-5GXeLTE-RM520-HP router has up to 9 detachable external antennas: 4 cellular antennas (for 5G

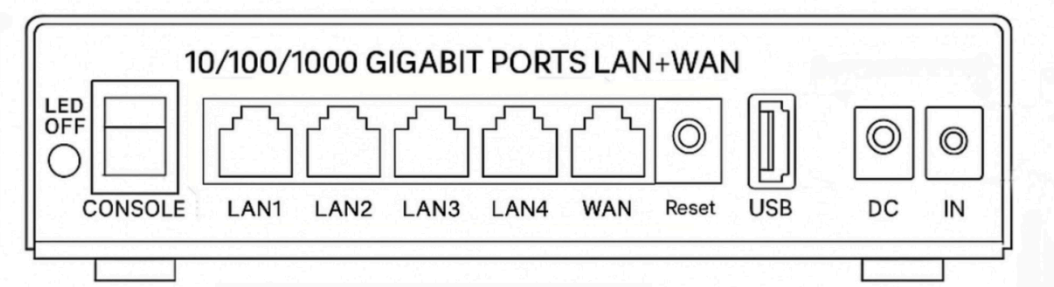
MIMO) and 5 WiFi antennas (for extended Wi-Fi 6 coverage). The number of cellular antennas depends on your model (LTE models may have 2 cellular antennas, 5G models have 4).

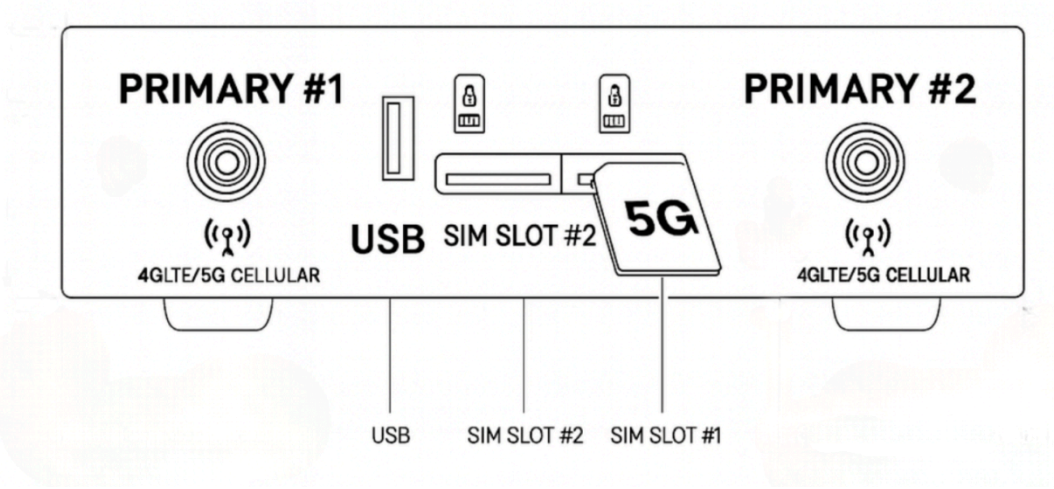
The front panel has a row of LED indicators (see table below). An **LED ON/OFF** switch on the back panel allows you to turn off all LEDs — useful for dark environments like bedrooms or RVs.

LED Indicators

LED	Behavior	Description
Power/Boot Status	Blink	Router is booting up
	Solid	Boot complete — router is ready
Internet	ON	Internet is active using the SIM card (cellular)
	BLINKING	Internet is active using the WAN ethernet port
	OFF	No internet access
Wi-Fi	ON	Wireless is enabled (blinks during data transfer)
	OFF	Wireless is disabled
	Blinking	Normal use — data is being transmitted
	Very Fast blink	Unit is in recovery mode
WAN	ON	Connected to a Cable/DSL/Satellite modem
	OFF	No modem connection on WAN port
Ethernet 1-4	ON	An active ethernet device is connected to this port
	OFF	No device connected
	Blinking	Transmitting/receiving data
RED Ethernet	ON/OFF	Serial Access to router (normally left unused)

Device Design — Back Panel





MoFi 6500 Back Panel and Bottom View

Figure 3: Back Panel Ports and Bottom Panel (SIM Slots, Antennas)
If you are using a non sim model, SIM1/SIM2 will not be used

The back panel provides all physical connections, laid out left to right:


```
[LED OFF/ON] [Console] [LAN1] [LAN2] [LAN3] [LAN4] [WAN] [Reset] [USB] [DC]
[DC IN]
              (serial)  ←— 10/100/1000 Gigabit Ports LAN+WAN —→       12
VOLTS
```

Label	Description
LED OFF/ON	Switch to turn front panel LEDs on or off
Console (RED PORT)	Serial console port for advanced debugging (115200 baud, 8N1)
LAN1 — LAN4	Four 10/100/1000 Gigabit Ethernet ports for connecting computers, switches, IP cameras, or NAS drives
WAN	Gigabit Ethernet port for connecting to a Cable/DSL/Satellite modem or upstream router
Reset	Press and hold for 10 seconds to reset the router to factory default settings after router is booted up with power LED solid
USB	USB port for iPhone tethering, USB cellular modems, or USB storage.
DC / DC IN	12V 3.5A power input — use only the included power adapter. The router supports two power inputs: a standard barrel connector and a 4-pin Molex connector for permanent installations.

Bottom Panel — SIM Slots and Antennas (Not applicable for non SIM models)

The bottom of the router contains:

Label	Description
SIM Slot #1	Primary Nano SIM card slot (4FF) — insert your main cellular SIM here
SIM Slot #2	Secondary Nano SIM card slot (4FF) — for dual-SIM failover
PRIMARY #1	Primary cellular antenna connector #1 (4G/LTE/5G) — SMA female
PRIMARY #2	Primary cellular antenna connector #2 (4G/LTE/5G) — SMA female
USB	Additional USB port (5G model)

SIM Card Installation: 1. Power off the router
2. Locate the SIM card slots on the bottom panel
3. Insert the Nano SIM card into Slot #1 with the gold contacts facing down
4. If using dual-SIM failover, insert a second SIM into Slot #2
5. Power on the router — the modem will detect the SIM automatically

Wall Mounting

The router has 4 wall mount holes on the bottom of the case (see diagram). Use appropriate screws and anchors for your wall type. Mount the router with the antennas pointing upward for best signal coverage.

Antennas

The MOFI6500-5GXeLTE has up to 13 external antenna connectors depending on the sub model.
MOFI6500-5GXeLTE (Non Cellular) - 0 cellular and 5 WiFi antennas
MOFI6500-5GXeLTE-EM7411 - 2 Cellular and 5 WiFi antennas
MOFI6500-5GXeLTE-EM7411-DUAL - 4 Cellular and 5 WiFi antennas
MOFI6500-5GXeLTE-RM520-HP - 4 Cellular and 5 WiFi antennas
MOFI6500-5GXeLTE-RM520-HP-DUAL - 8 Cellular and 5 WiFi antennas

MOFI6500-5GXeLTE-RM520-HP	Connector	Purpose
Cellular PRIMARY #1	SMA female	Primary cellular antenna (required)
Cellular PRIMARY #2	SMA female	Secondary cellular antenna
Cellular MIMO #3	SMA female	Additional MIMO antenna
Cellular MIMO #4	SMA female	Additional MIMO antenna
WiFi 2.4 GHz (x2)	SMA female	2.4 GHz wireless antennas with built-in power amplification
WiFi 5 GHz (x3)	SMA female	5 GHz wireless antennas with built-in power amplification

Antenna Placement Tips: - Keep antennas at least 12 inches (30 cm) from metal objects, walls, and other electronics - The router features built-in power amplification for both 2.4 GHz and 5 GHz bands, providing extended range compared to standard routers - All antennas are detachable.

External Connectors and Specifications

Power Input: - DC Jack: 110-220V input, 12V DC output, 12-30V DC range - Recommended inline fuse for vehicle installations: min 3A fast-blow - AC Power Adapter: 12V DC output, 110/120V, 3.5A, fully UL certified

Ports: - 4 x RJ45 LAN ports (10/100/1000 Gigabit, can function as multi-WAN ports) - 1 x RJ45 WAN port (10/100/1000 Gigabit, can also be used as a LAN port) - 1 x USB 2.0 port (rear) - 1 x USB 3.0 port (side/bottom) - 1 x Factory Default Reset button - 1 x Serial Console port

Antennas: - 5 x 5 dBi premium external SMA antennas for WiFi - 4 x 5 dBi premium wide-band external SMA antennas for 3G/4G/LTE/5G cellular signals

SIM Slots: - 2 x 4FF SIM slots (Nano SIM cards)

Performance: - CPU: 1.3 GHz dual-core - RAM: 1 GB (DDR4, 2400 MT/s) - ROM: 128 MB (system memory)

Physical Dimensions: - Size: 260 mm x 140 mm x 33 mm (10 in x 5.5 in x 1.3 in) - Weight: 340 grams (1.6 lb) — router body only, without antennas

Operating Temperature: -30 C to +75 C (-22 F to +167 F)

Storage Temperature: -40 C to +90 C (-40 F to +194 F)

Molex Power Connector: The router includes a 4-pin Molex power connector in addition to the standard barrel jack. This is useful for permanent vehicle or marine installations where the router can be wired directly to a 12V DC power source.

Cellular Module Specifications

The MOFI6500-5GXeLTE can use various modules depending on the model
For the 6500-5GXeLTE-RM520-HP, here are the specs

Module Antenna Mapping: The module has 4 antenna connectors (ANT0-ANT3) mapped to the external enclosure as follows:

Module Pin	External Label	Function
ANT0	PRIMARY #1	Primary TX/RX antenna (required for any cellular connection)
ANT1	SECONDARY #1	MIMO diversity antenna
ANT2	SECONDARY #2	MIMO diversity antenna
ANT3	PRIMARY #2	Secondary TX/RX antenna

Important: There must be an antenna connected to the **PRIMARY #1** cellular antenna port for the unit to establish a cellular connection. PRIMARY #2 is required for 5G MIMO performance and highly recommended

Supported Frequency Bands:

Band	Description
LB (Low Band)	617-960 MHz
MHB (Mid-High Band)	1452-2690 MHz
UHB (Ultra-High Band)	3400-3800 MHz
n77/n78	3300-4200 MHz
n79	4400-5000 MHz
LAA	5150-5925 MHz

Data Rates:

Mode	Download	Upload
5G SA	2.4 Gbps	900 Mbps
5G NSA	3.4 Gbps	550 Mbps
LTE Cat 19	1.6 Gbps	200 Mbps
HSPA+	42 Mbps	5.76 Mbps

Supported LTE Bands: B1, B2, B3, B4, B5, B6, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B43, B46, B48, B66, B71

Supported 5G NR Bands: N1, N2, N3, N5, N7, N8, N12, N13, N14, N18, N20, N25, N26, N28, N29, N30, N38, N40, N41, N48, N66, N70, N71, N75, N76, N77, N78, N79

Common US Carrier Bands: - **AT&T:** B2, B4, B5, B12/B17, B14, B30, B66, ATT 5G: N2, N5, N29, N30, N48, N66, N77, N78 - **T-Mobile:** B2, B4, B5, B12/B17, B66, B71. TMobile 5G: N2, N25, N41, N66, N71, N77, N78- **Verizon:** B2, B4, B5, B13, B66, Verizon 5G: N2, N5, N48, N66, N77, N78

---

3. First-Boot Setup Wizard

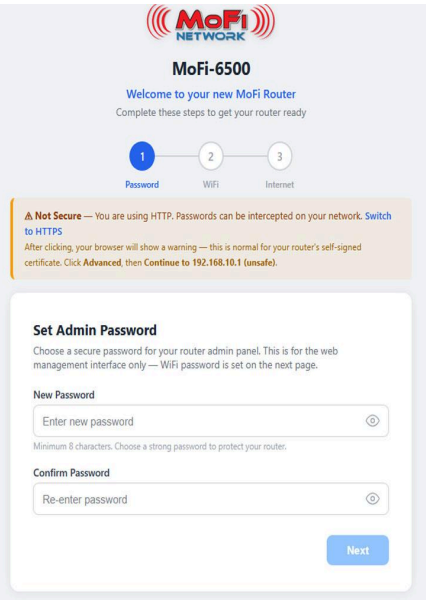
When you power on the MoFi 6500 for the first time (or after a factory reset), a setup wizard guides you through essential configuration.

Connecting to the Router

1. **Insert SIM card(s):** Power off the router. Insert your activated cellular SIM card into SIM Slot 1. If you have a second SIM, insert it into SIM Slot 2. If you have a single module router, only 1 SIM card can be used at a time. If you have a Dual Module router, both SIM's can be used but need to ensure you set up fail over or load balancing.
2. **Connect antennas:** Attach all included antennas to their labeled ports. Hand-tighten only — do not use tools.
3. **Power on:** Connect the 12V power adapter and plug it in. Wait approximately 90 seconds for the router to fully boot. You will know when the booting status LED is solid.
4. **Connect your device:** Connect a computer to one of the LAN ports (1-4) using the included ethernet cable. Alternatively, connect to the default WiFi network (SSID will be printed on the router label, typically `Mofi_Fast-5G-AX-XXXXXX`).
5. **Open the setup page:** Launch a web browser and navigate to: **http://192.168.10.1**
6. The setup wizard will appear automatically on first boot.

Step 1: Set Admin Password

- **New Password:** Enter a strong password (minimum 8 characters recommended). Use a mix of uppercase, lowercase, numbers, and symbols.
- **Confirm Password:** Re-enter the same password.
- This password protects access to the router's web management interface.
- **Important:** Write this password down and store it securely. If forgotten, a factory reset is required



Step 2: Configure WiFi

The router broadcasts two WiFi networks:

• 2.4GHz – Longer range and better compatibility with older devices, but generally slower speeds.

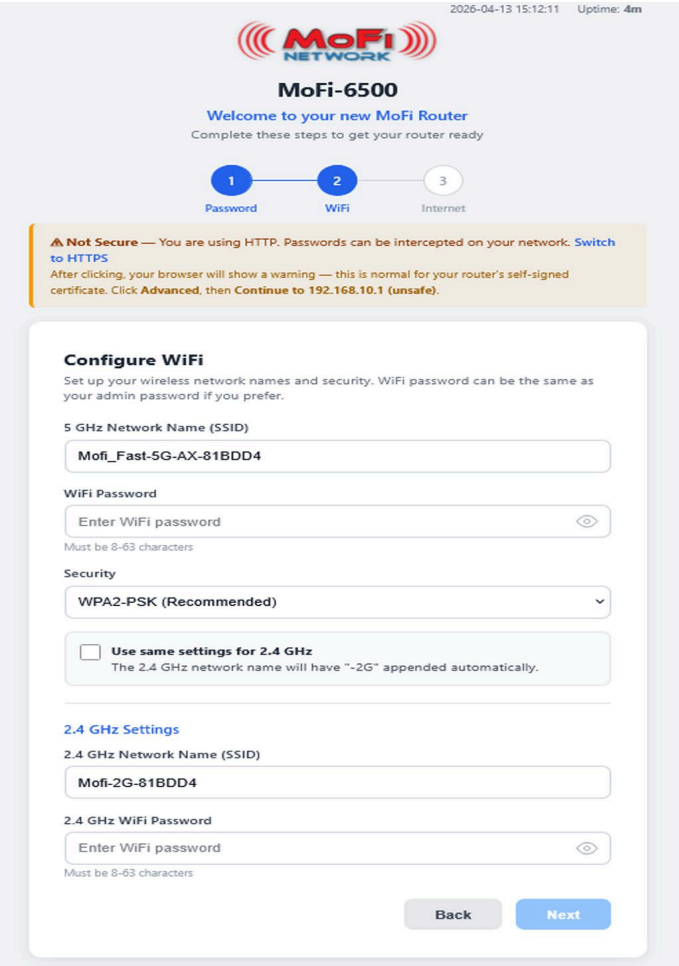
• 5GHz – Faster speeds and less interference, making it ideal for streaming, gaming, video calls, and other high-bandwidth activities.

Some older devices may not support 5GHz and will only be able to connect to the 2.4GHz network.

For the best performance, connect to the 5GHz network whenever possible.

- **5 GHz Network Name (SSID):** Enter your preferred WiFi network name (up to 32 characters). This is the name your devices will see when scanning for WiFi.
- **WiFi Password:** Enter a password (8-63 characters). Use a strong, unique password.
- **Security:** Select the encryption type:

Use the same settings for 2.4 GHz: Check this box to automatically create a matching 2.4 GHz network with “-2G” appended to the SSID name. Uncheck to configure 2.4 GHz settings separately.



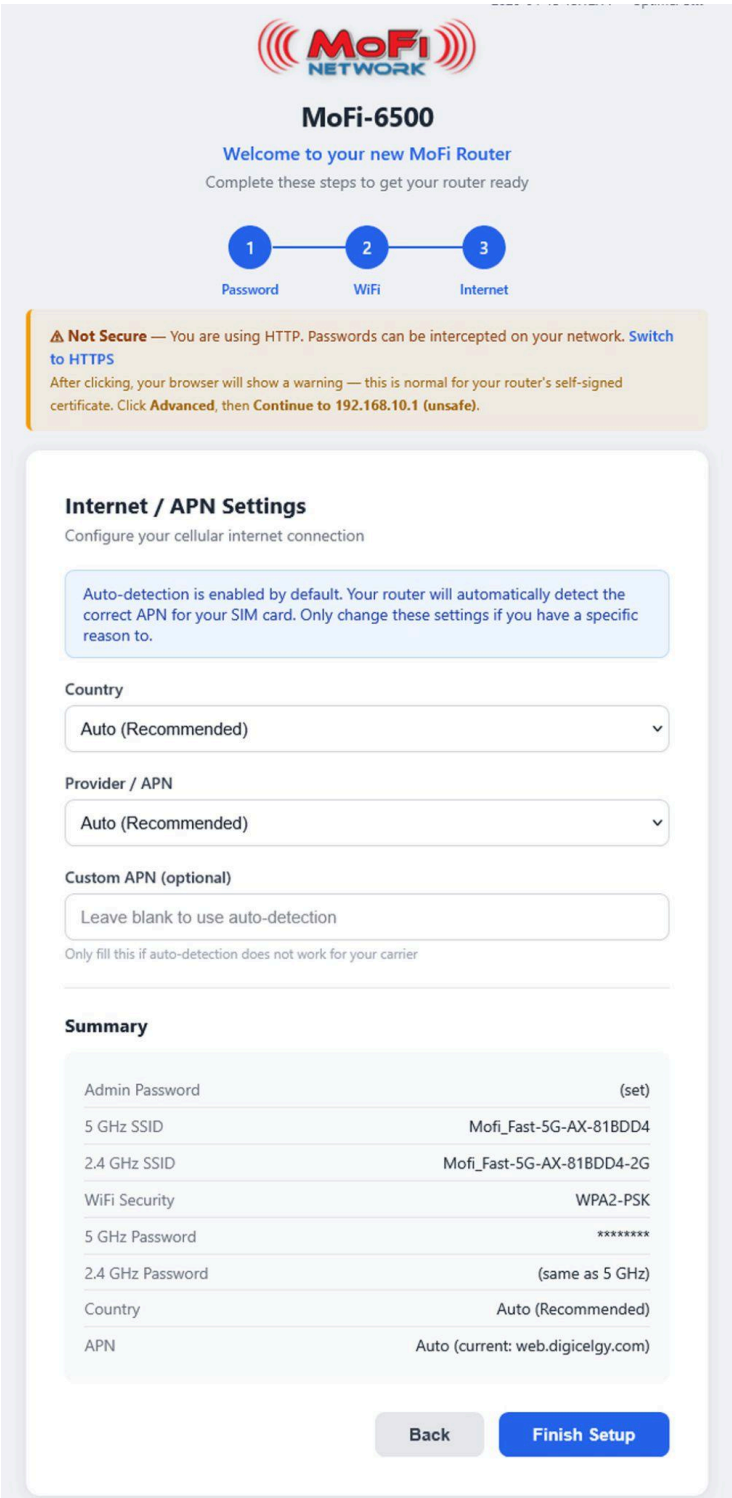
Step 3: Internet / APN Settings

In most cases, the APN is automatically detected by your router when using a cellular provider in Canada or the USA, and no manual configuration is required.

If the router is unable to connect to the internet, verify the correct APN settings with your cellular provider and enter them manually if needed.

An incorrect APN can prevent the router from establishing a data connection, even if the SIM card is detected.

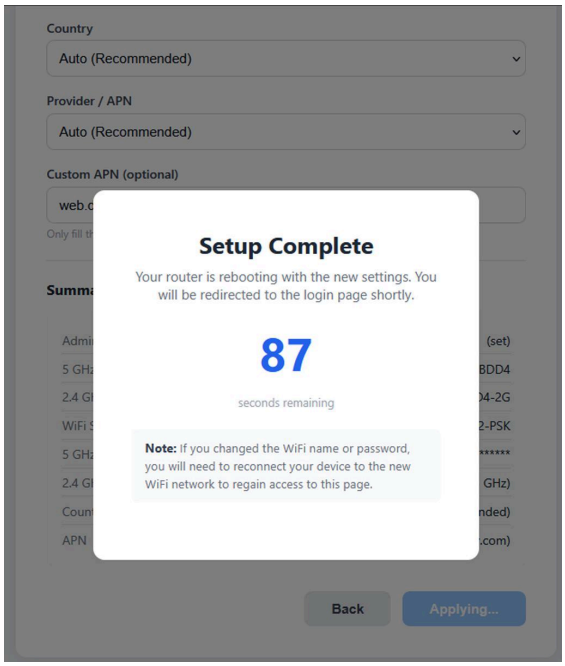
- **Country:** Select your country from the dropdown. This auto-populates the list of known carriers and their APN settings.
    - Available countries: United States, Canada, Mexico, Costa Rica, Jamaica, Nigeria, Bahamas, UK, Germany, India, France, and Custom APN.
- **Provider:** Select your cellular carrier, or leave as “Auto” for automatic detection.
- **APN:** If your carrier requires a specific APN, enter it here. Otherwise, leave blank for auto-detection.



Finishing Setup

A summary page displays all your chosen settings. Review them carefully, then click **Finish Setup**.

The router will reboot with your new settings. This takes approximately 90 seconds.
When the router is booting up, the power LED will flash. When it is fully booted, it will go solid.
After rebooting:
1. Connect to your new WiFi network using the SSID and password you configured
2. Navigate to **http://192.168.10.1**
3. Log in with the admin password you set in Step 1



Connecting to the Internet via 4G/LTE/5G (Cellular)

1. Insert an activated SIM card into SIM Slot #1 (see bottom panel)
2. Attach the cellular antennas to the PRIMARY antenna connectors
3. Power on the router and wait for boot to complete (Power LED solid)
4. The router will automatically detect the SIM and connect to the cellular network
5. The Internet LED will turn solid ON when connected
6. If the router does not connect automatically, navigate to **MoFi Internal Modem-1 > Configuration** and
7. verify the APN settings for your carrier and if needed, set APN in the custom APN settings option

Connecting via Cable/DSL/Fiber (WAN Ethernet)

1. Connect an Ethernet cable from your Cable/DSL/Fiber modem to the router's **WAN port** (blue port on the back)
2. Power on the modem first then wait until its fully online then power on the router
3. The WAN LED will turn ON when a connection is detected

4. The Internet LED will blink when internet is active via WAN
5. The router uses DHCP by default — it will automatically obtain an IP from your modem
6. For PPPoE connections (some DSL providers), navigate to **Network > Router IP/DNS** and set the WAN Protocol to “PPPoE” with your ISP-provided username and password

Using Starlink Satellite Internet

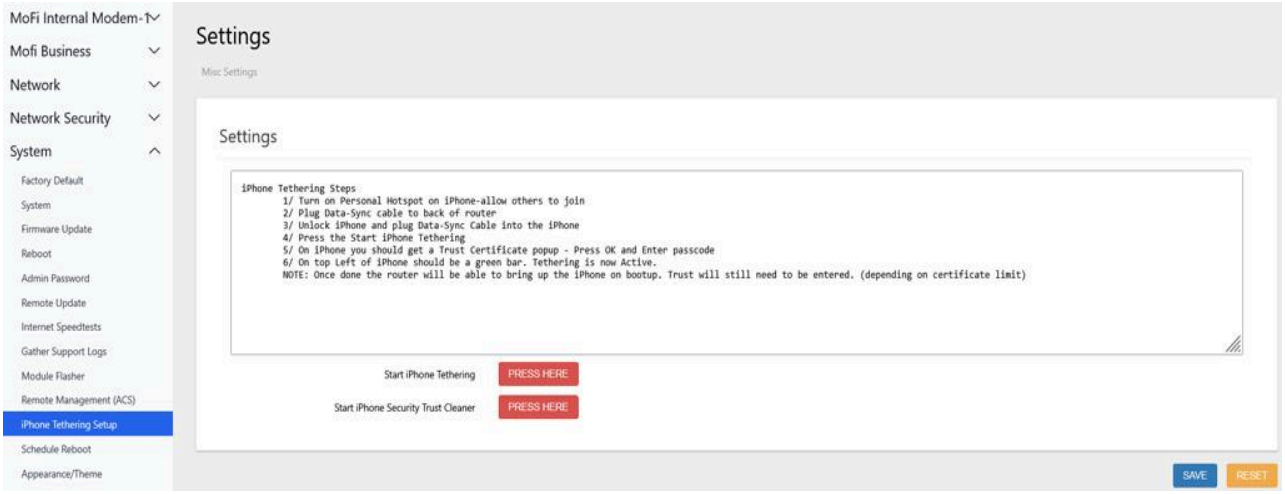
If you are using Starlink as your internet source:

1. Use the Starlink Ethernet adapter cable to connect your Starlink to the router’s **WAN port**
2. Using the Starlink app on your phone, put the Starlink modem into **Bridge mode** (also called IP Passthrough mode)
3. Power off both the Starlink and the MoFi router, then power them back on
4. Connect your PC to any available LAN port using an Ethernet cable, or connect via WiFi
5. The router will obtain an IP address from Starlink and provide internet to all connected devices

Note: Ensure that the router’s LAN IP address (default 192.168.10.1) does not conflict with the Starlink modem’s IP range. If there is a conflict, change the router’s IP at **Network > Router IP/DNS**.

Using iPhone USB Tethering

1. Connect your iPhone to the router’s USB port using a Lightning or USB-C cable
2. On your iPhone, go to **Settings > Personal Hotspot** and enable it
3. When prompted on the iPhone, tap **Trust** to trust the router
4. On the router, navigate to **System > iPhone Tethering Setup** and click **Start iPhone Tethering**
5. The router will use your iPhone’s cellular connection as an internet source



Requirements

To set up and use the MoFi 6500 router, you need: - An internet browser to access the web interface (Chrome, Firefox, Safari, or Edge) - An Ethernet network adapter or a WiFi network adapter on your computer - An

activated SIM card from a cellular carrier (for 4G/LTE/5G internet) - OR an Ethernet cable and Cable/DSL/Fiber/Starlink modem (for wired internet) - The MoFi router is compatible with virtually any operating system and device.
To set up and use the MoFi 6500 router, you will need:

- A web browser to access the router's management interface, such as Google Chrome, Mozilla Firefox, Safari, or Microsoft Edge
- An Ethernet adapter or WiFi adapter on your computer or device
- An activated SIM card from a cellular provider for 4G/LTE/5G internet access

OR

- An Ethernet connection to a Cable, DSL, Fiber, or Starlink modem for wired internet access

The router is compatible with virtually all modern operating systems and connected devices.

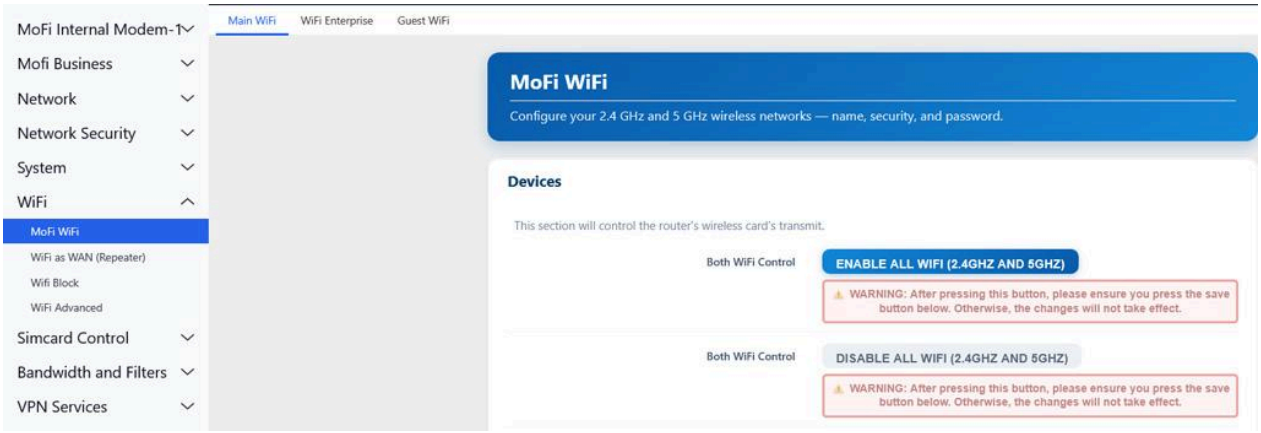
Quick Reference — Common Tasks

This section provides quick step-by-step guides for the most frequently needed tasks. Each task includes a direct URL you can paste into your browser.

How to Change the WiFi Password

1. Go to **WiFi** → **Mofi WiF**i or you can click below:
   http://192.168.10.1/cgi-bin/luci/admin/wireless/mofi-wifi
2. You can change the SSID and Password for both 2.4GHz and the 5GHz WiFi but note they can't have the same SSID (network name)
3. Choose your **WiFi Security** type — WPA2-PSK is recommended for best device compatibility
4. Click **Save.**
5. All connected devices will be disconnected and will need to reconnect using the WiFi name and new password
   If your device previously was connected to the new WiFi name and password as what you are setting now, it should reconnect on its own after you save.
   If you can't connect to the new wifi, try to forget the network and connect again.

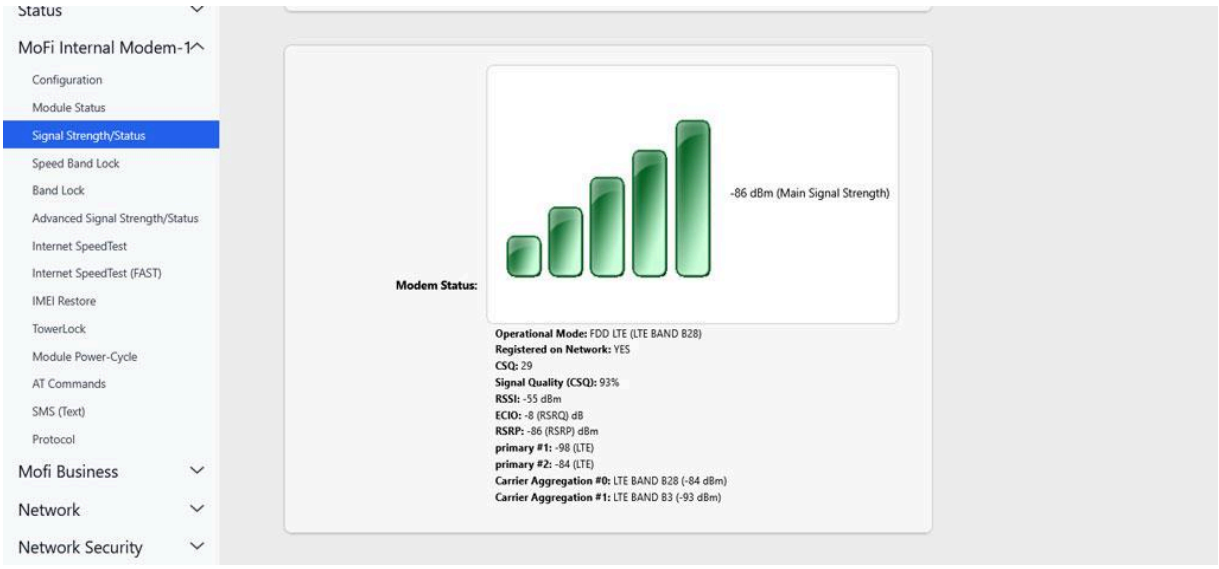
To change the Guest WiFi password, click the **Guest WiFi** tab and repeat the same steps.



See Section 9.1 for full details on all WiFi options.

How to Check Signal Strength and Run a Speed Test

1. Go to **Mofi Internal Modem** → **Signal Strength / Status** or click the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/module_status.
2: Click **Refresh** under current connection
3:Check the **Signal DStrength (RSRP)** bar: - Lower that -90 dBm = Excellent signal, -90 to -105 dBm = Good to Fair signal - Higher -105 dBm = Poor signal — reposition antennas or try a different location.
The higher the dB, the weaker the signal. Most locations are between 95-105 dB
4: Check **SINR** (Signal-to-Noise): 20+ dB is excellent, below 0 dB is poor.
5: Click **Refresh Status** to update the readings.



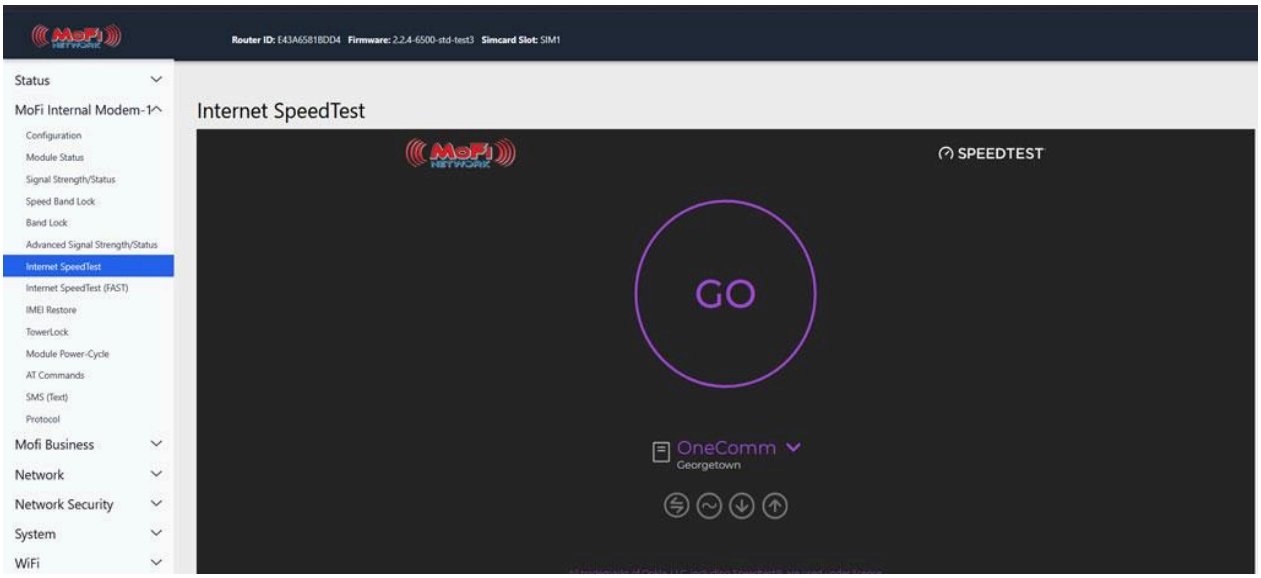
Run Speed Test:

1. Go to **Mofi Internal Modem** → **Internet Speed Test** or click the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/speed.

2: Click the **GO** button.

3: Wait for the test to complete — results show Ping (ms), Download (Mbps), and Upload (Mbps).

4: For a quick Netflix-based test, use **http://192.168.10.1/cgi-bin/luci/admin/jmodule1/netflixspeed**

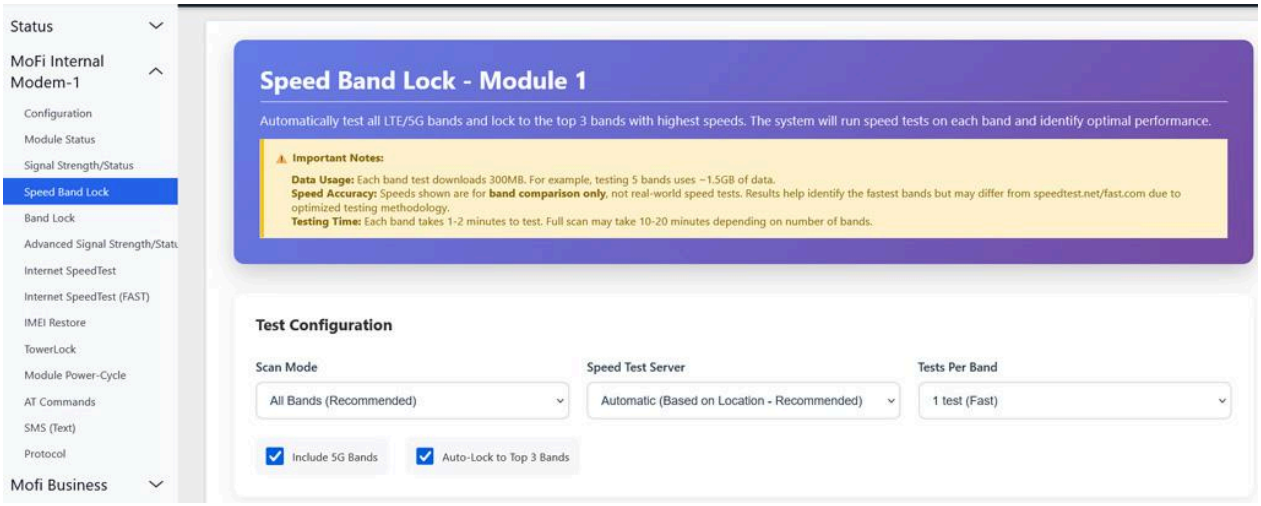


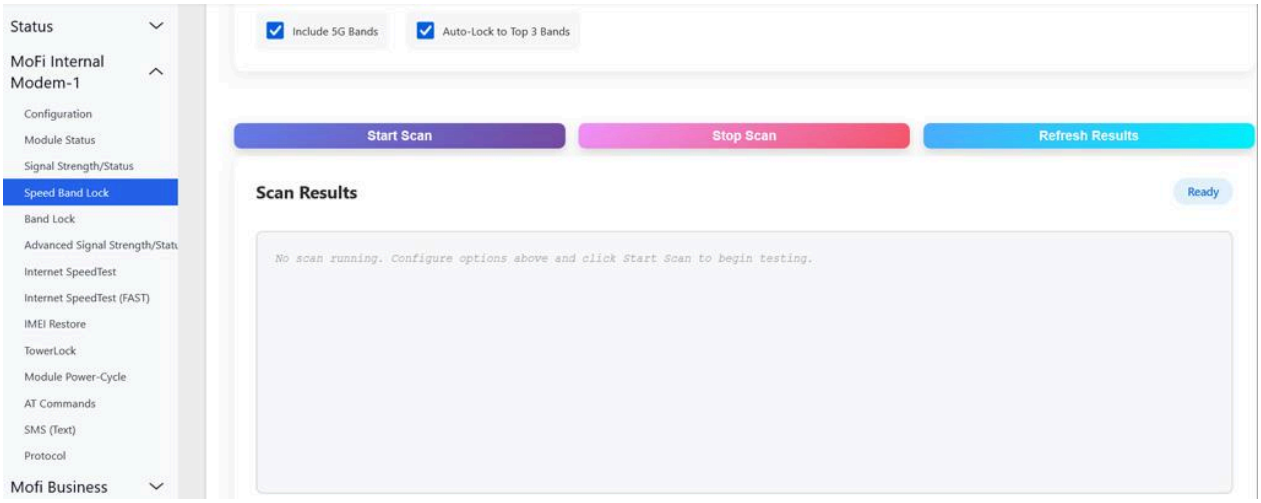
How to Run Speed Band Lock (Find the Fastest Bands)

Speed Band Lock automatically tests each cellular band's speed and locks to the fastest ones for your location.

1. Go to **Mofi Internal Modem** → **Speed Band Lock** or click the link below: http://192.168.10.1/cgi-bin/luci/admin/jmodule1/speedbandlock
2. Select **Scan Mode**:
    - Choose your carrier (e.g., "AT&T Optimized", "T-Mobile Optimized", "Verizon Optimized") to only test bands your carrier uses to only scan the bands needed
    - Or choose "All Bands" to test everything (uses more data and takes longer)
3. Select a **Speed Test Server** close to your location (automatic is recommended)
4. Set **Tests Per Band** to "2 Recommended" for accurate results
5. Toggle **Include 5G Bands** to ON if you have 5G service is using a 5G model
6. Toggle **Auto-Lock to Top 3 Bands** to ON if you want the router to automatically lock to the best bands after scanning (normally want to lock on 3 bands)
7. Click **Start Scan**
8. Wait for the scan to complete — this can take 10-30 minutes depending on how many bands are tested
9. The router will disconnect and reconnect to each band individually during testing so when doing this process, do not use the router under this is completed
10. When done, a results table shows each band along with the speed for each band
11. If you enabled Auto-Lock, the router is now locked to the top 3 fastest bands

Important: Each band test uses approximately 300 MB of data. A full "All Bands" scan can use 5-15 GB. Use carrier-optimized mode to reduce data usage.





See Section 5.4 for full details.

How to Set Up Failover (Automatic Backup Connection)

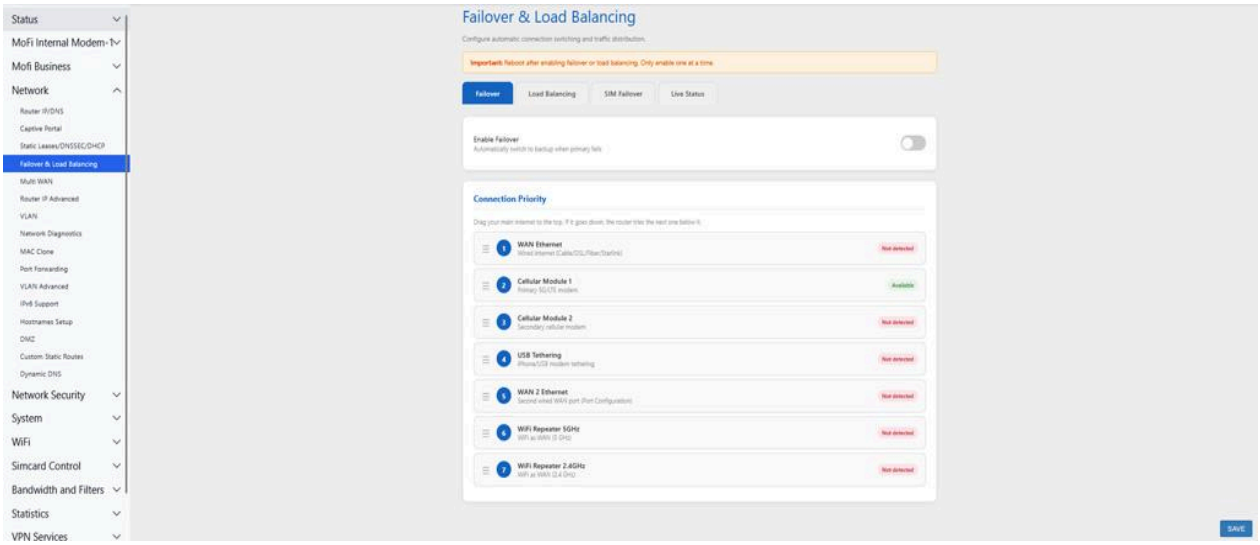
Failover automatically switches to a backup internet connection when the primary fails. For example, if your WAN ethernet/Starlink goes down, the router switches to cellular then back to main when it is back up.

What is Failover vs Load Balancing? - **Failover** = One connection active at a time. If the primary fails, the router switches to the backup. Only the backup is used until the primary recovers. - **Load Balancing** = Multiple connections active simultaneously. Traffic is distributed across all connections for combined speed. If one fails, the remaining connections handle all traffic. - You can only enable **one** — Failover OR Load Balancing, not both.

Setting Up Failover:

http://192.168.10.1/cgi-bin/luci/admin/business/failover-new

1. Go to **Mofi Business** → **Fail Over** / **Load Balancing**
2: Click the Failover tab.
3: Toggle Enable Failover to ON.
4: Select the priority that you want (you drag to change) then Click Save
6. Reboot the router — failover changes require a reboot to take effect
7. After reboot, the router monitors all connections and switches automatically if the primary fails.

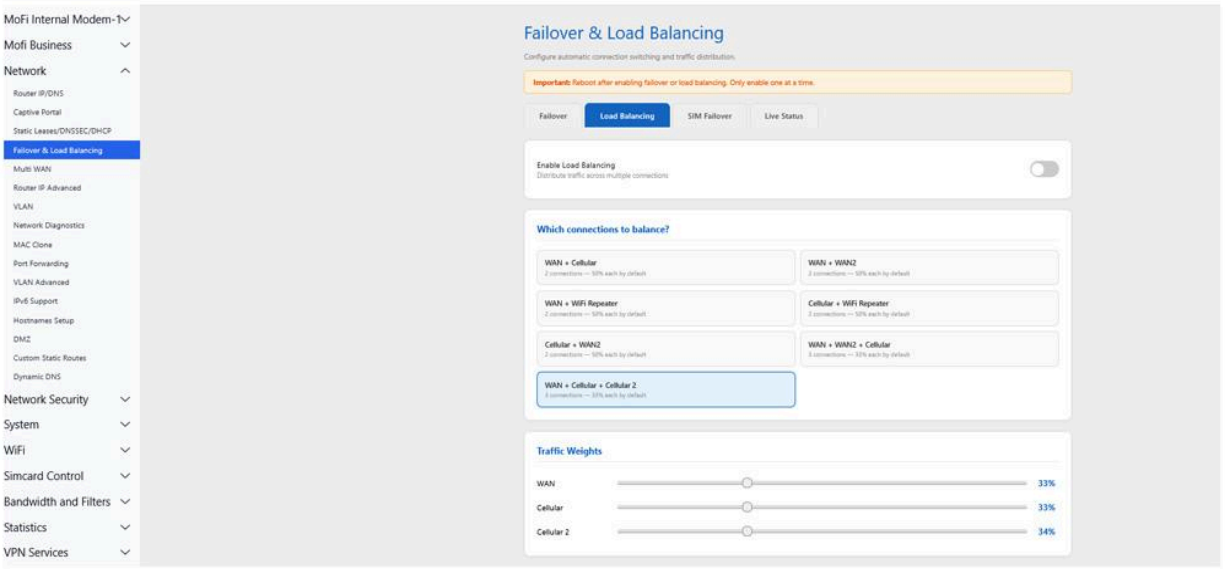


See Section 7.6 for full details including SIM failover.

How to Set Up Load Balancing (Combine Connections)

Load Balancing distributes traffic across multiple internet connections simultaneously for increased total speed. Here is a video to explain this more https://youtu.be/L3N2mcUmeuA

1. Go to **Mofi Business** → **Fail Over** / **Load Balancing** or click on the link below: **http://192.168.10.1/cgi-bin/luci/admin/business/failover-new**
2. Click the **Load Balancing** tab
3. Make sure **Failover is disabled** on the Failover tab first (you cannot use both)
4. Toggle **Enable Load Balancing** to ON
5. Select a **Load Balancing Profile**:
    - **WAN + Cellular** — Balance between WAN ethernet and cellular modules
    - **WAN + Module1** — Balance between WAN and Module 1 only
    - **WAN + Module2** — Balance between WAN and Module 2 only
6. Set **WAN Weight** and **Module Weight** percentages (e.g., 50/50 for equal distribution, or 70/30 to favor one connection), normally 50% is recommended
7. Click **Save**
8. **Reboot the router**
9. After reboot, traffic is distributed across both connections



How to Set Up SIM Failover (Dual SIM Automatic Switching)

If you have two SIM cards, either from different carriers or the same carrier, SIM Failover can automatically switch to the backup SIM if the primary SIM loses signal or experiences some other issues.

On a single-module router, only one SIM can be active at a time. Because of this, once the router switches to the secondary SIM, it cannot continuously monitor the primary SIM while connected to the backup SIM.

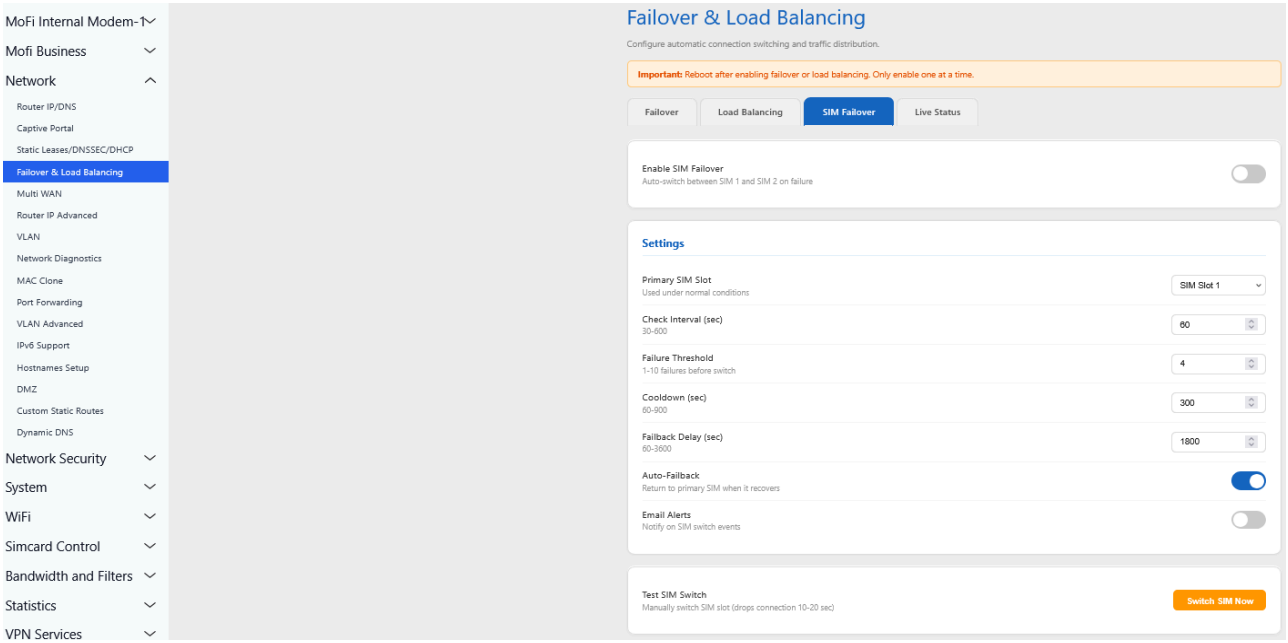
To check whether the primary SIM connection has been restored, the router must briefly disconnect from the secondary SIM and test the primary SIM again.

By default, the router is configured to recheck the primary SIM every 30 minutes. This helps minimize interruptions. If the recheck interval is set too low, users may notice brief disconnections every few minutes while the router checks whether the primary SIM is available again.

Go to **Mofi Business** → **Fail Over** / **Load Balancing** or click the link below:
http://192.168.10.1/cgi-bin/luci/admin/business/failover-new

1. Click the **SIM Failover** tab
2. Toggle **Enable SIM Failover** to ON
3. Set **Primary SIM Slot** to your main SIM (usually “SIM Slot 1”)
4. Set **Check Interval** — how often to test connectivity (60 seconds recommended)
5. Set **Failure Threshold** — how many consecutive failures before switching (4 recommended)
6. Set **Cooldown Time** — minimum wait between switches (300 seconds / 5 minutes recommended)
7. Toggle **Enable Auto-Failback** to ON — this automatically returns to your primary SIM when it recovers

8. Set **Failback Delay** — how long to wait before switching back (1800 seconds / 30 minutes recommended)
9. Click **Save**
10. Click **Switch SIM Now** to test that both SIMs work before relying on failover



How to Set Up WiFi as WAN (WiFi Repeater)

Use an existing WiFi network — such as at a hotel, campground, office, or public hotspot — as your internet source. The MOFI router connects to the external WiFi network and then securely shares that connection with all of your devices through your own private network.
If you are setting up the Wifi as WAN via a wireless connection, suggest connecting the WiFi type opposite than you want to connect to. For example, if your main source internet is on a 2.4GHz WiFi, then connect to Mofi's 5GHz WiFi to set this up and vice versa.

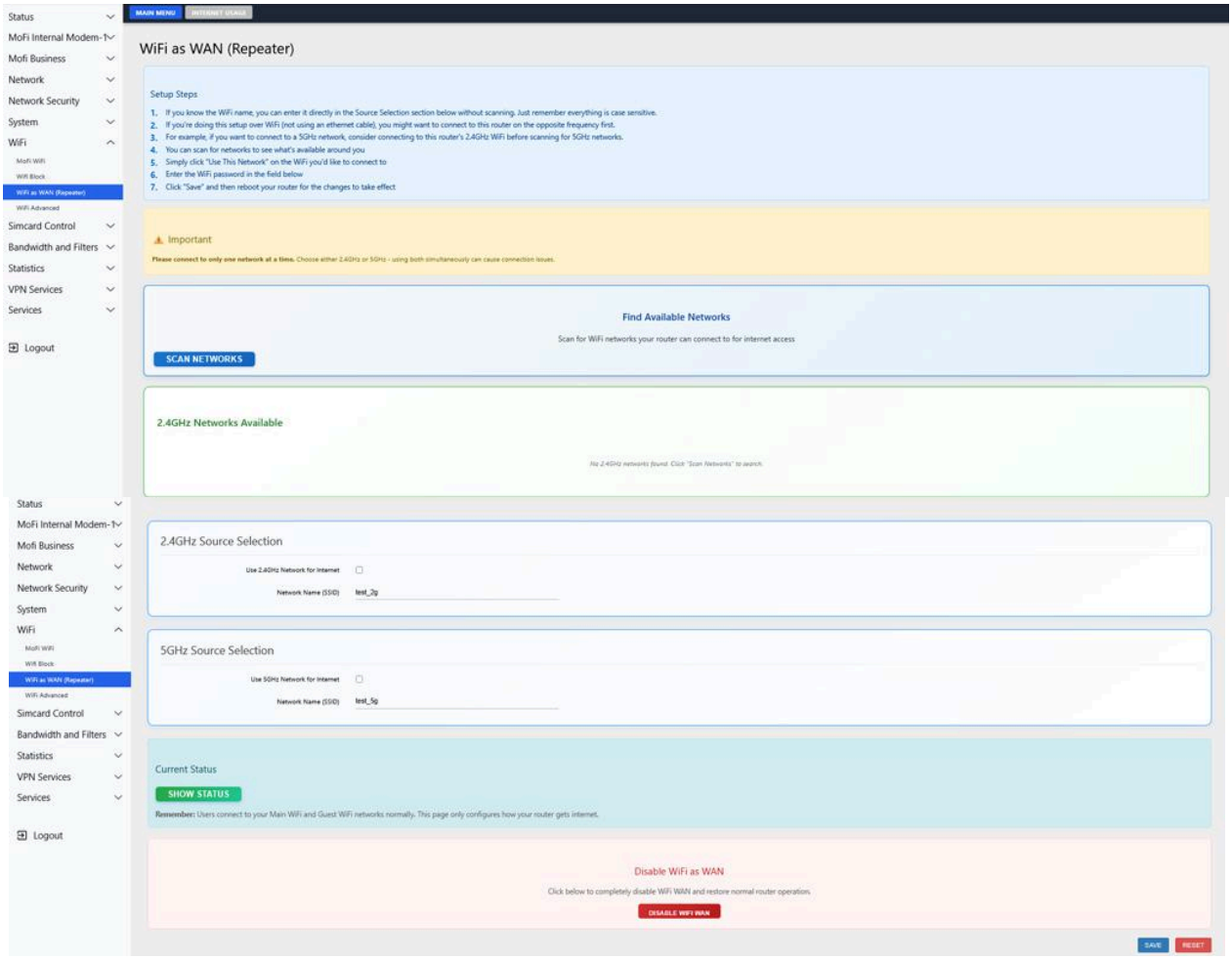
1. Go to **Wifi** → **Wifi As Wan** or click on the link below:
   http://192.168.10.1/cgi-bin/luci/admin/wireless/wifi-repeater
2. Click **Scan Networks** — the router scans for available WiFi networks nearby
3. Wait 5-15 seconds for the scan to complete
4. Find the WiFi network you want to connect to in the **2.4 GHz** or **5 GHz** list
   Only connect to one network at a time

   - 5 GHz is faster and recommended
   - 2.4 GHz has better range but slower speeds

5. Click **Use This Network** next to the desired network
6. The **Network Name (SSID)** field will auto-fill with the network name
7. Enter the network's **Password** in the **Network Password** field
8. Click **Save**
9. Wait 30-60 seconds for the router to connect
10. Click **Show Status** to verify the connection is established
11. All your devices connected to the MoFi router now share the upstream WiFi

To disconnect and stop using WiFi as WAN: - Return to this page and click **Disable WiFi WAN**

Tip: If using WiFi as WAN with cellular failover, set the failover profile to "WiFi as WAN" so the router automatically switches to cellular if the WiFi network goes down.

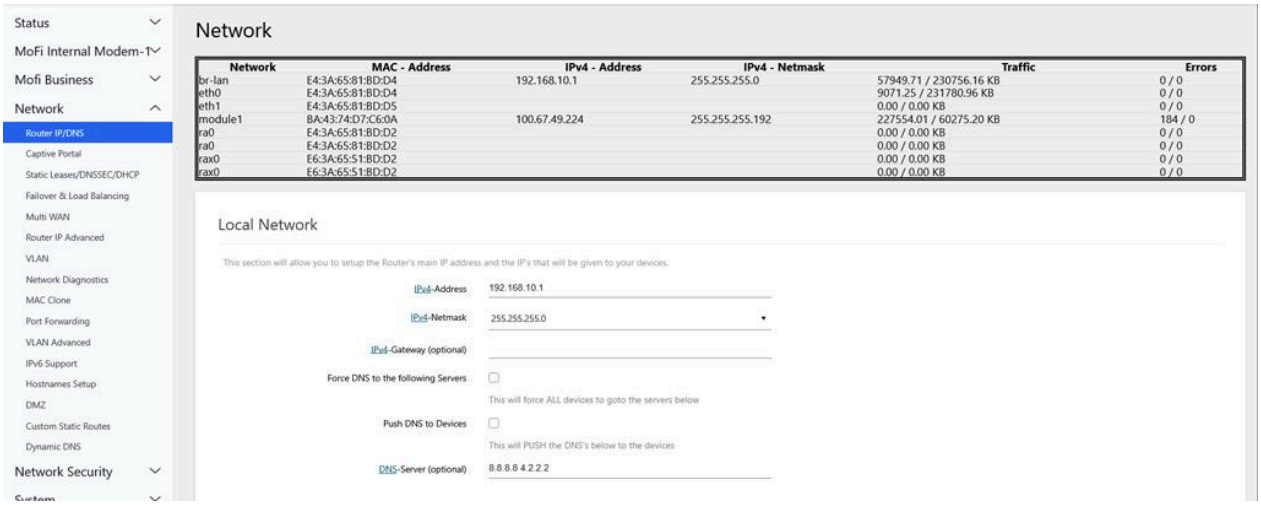


See Section 9.2 for full details.

How to Change the Router IP and DNS Settings

The router's default LAN IP is 192.168.10.1. You can change this if it conflicts with another network, or configure custom DNS servers.

1. Go to **Network** → **Router ID/DNS** or click on the link below:
   http://192.168.10.1/cgi-bin/luci/admin/network/routeripjs
2. Under **Local Network**:
   - Change **IPv4 Address** if you need a different LAN IP (e.g., 192.168.1.1)
   - Change **IPv4 Netmask** if you need a different subnet size
3. To force specific DNS servers for all devices:
   - Toggle **Force DNS to following Servers** to ON
   - Toggle **Push DNS to Devices** to ON
   - Enter your preferred **DNS Server** (e.g., 8.8.8.8 for Google, 1.1.1.1 for Cloudflare)
4. Click **Save**
5. **Important:** If you change the IP address, your browser will lose connection. Reconnect to the router using the new IP address.



See Section 8.2 for full details including WAN settings.

How to Set Up Port Forwarding

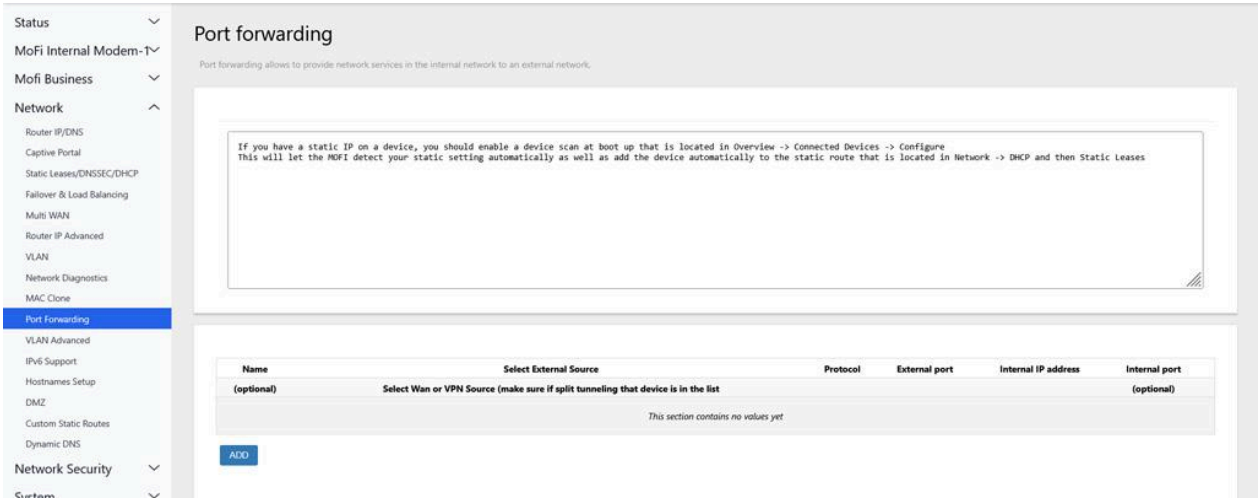
Port Forwarding allows external internet traffic to reach a specific device on your local network. This is commonly used for applications such as security cameras, game servers, remote desktop access, and other services that require access from outside your network.

1. Go to **Network** → **Router IP/DNS** or click on the link below:
   http://192.168.10.1/cgi-bin/luci/admin/network/portfw-js
2. Enter a **Name** for the rule (e.g., "Security Camera", "Minecraft Server")

3. Set **Select External Source**:
    - Choose **"Cellular/Wan/Repeater"** for traffic coming in through your cellular or WAN connection
    - Choose **"Cloudlink/Vpn"** if you're using CloudLink for a static public IP
4. Set **Protocol**: TCP, UDP, or TCP+UDP (check your application's requirements)
5. Enter the **External port** — the port number visible from the internet
6. Enter the **Internal IP address** — the device on your LAN to forward to (e.g., 192.168.10.100)
7. Enter the **Internal port** — the port on the device (leave blank to use the same as external)
8. Click **Add** to create the rule
9. Click **Save** to apply

Example — Forward port 8080 to a security camera at 192.168.10.100: Name: "Camera", Source: "Cellular/Wan/Repeater", Protocol: TCP+UDP, External port: 8080, Internal IP: 192.168.10.100, Internal port: 80

Tip: For port forwarding to work, you need a public IP address. Most cellular carriers use CGNAT which blocks incoming connections. Use **CloudLink** to get a static public IP.



See Section 8.7 for full details.

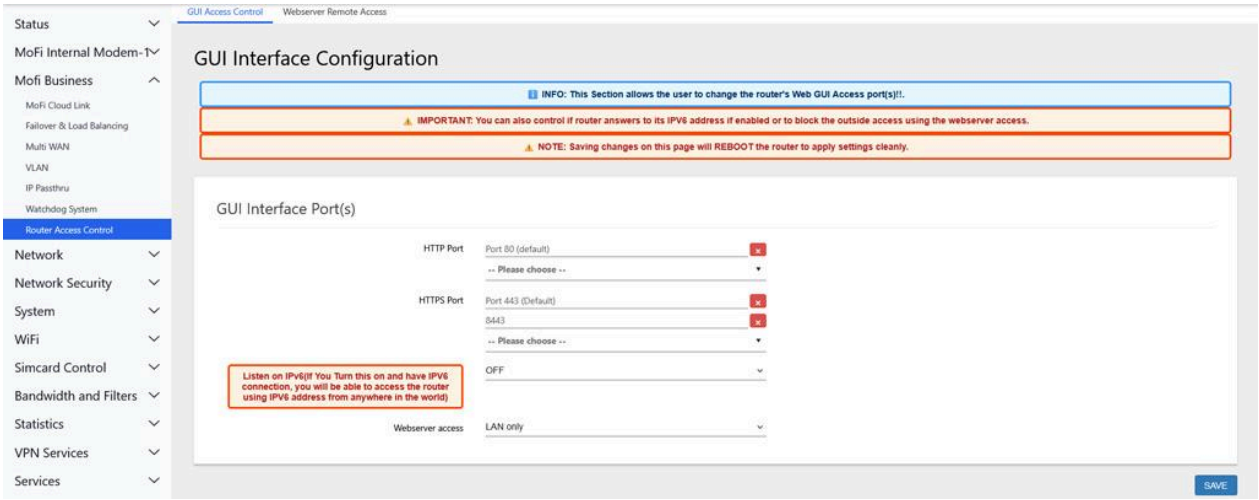
How to Make the Router GUI Accessible Over the Internet (WAN)

By default, the router admin interface is only accessible from the LAN (local network). You can open it to WAN access for remote management.

1. Go to **Mofi Business → Router Access Control** or click on the link below: **http://192.168.10.1/cgi-bin/luci/admin/business/webserver**
2. Change **Web server access** from "LAN only" to **"Allow access from LAN/WAN"**
3. Optionally change the **HTTP Port** (default 80) and **HTTPS Port** (default 443) to non-standard ports for security (e.g., 8080 and 8443)

4. Click **Save**
5. The router admin is now accessible from the WAN/cellular side at your public IP

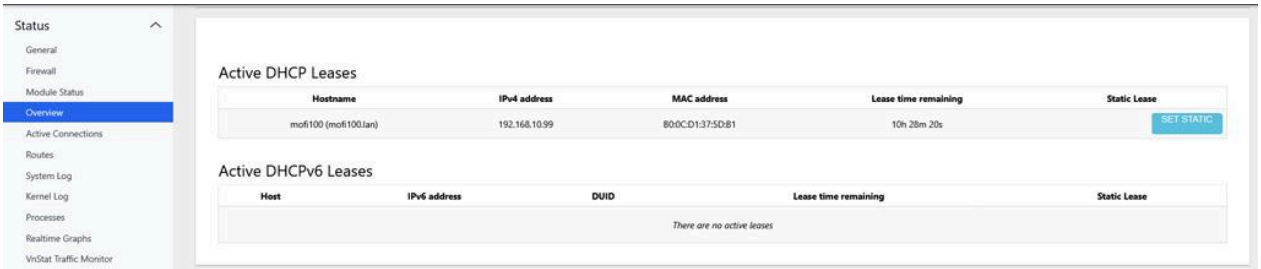
Security Warning: Opening the GUI to the WAN exposes it to the entire internet. To reduce risk: - Use a strong admin password - Change the HTTP/HTTPS ports to non-standard numbers - Consider using **Webserver Remote Access** whitelist (Network Security > Webserver Remote Access) to only allow specific IPs - A safer alternative is using **CloudLink** or **WireGuard VPN** for remote access — these encrypt the connection and don't expose the admin page directly



See Section 7.5 for full details.

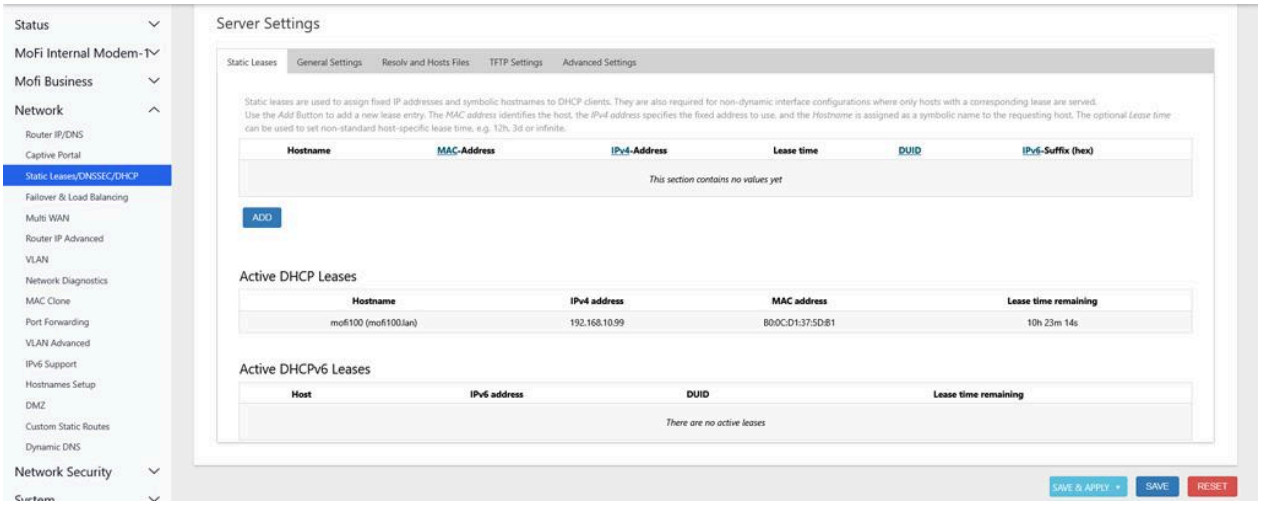
How to Assign a Static IP Address to a Device

Method 1 — From the Status Overview Page (fastest):
1. Go to **Status** → **Overview** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/status/overview
2. Scroll down to the **Active DHCP Leases** table
3. Find the device you want to assign a static IP to
4. Click **Set Static** next to that device
5. The device's hostname, MAC address, and current IP will be automatically filled in as a static lease
6. Click **Save & Apply**
7. That device will now always receive the same IP address



Method 2 — From the DHCP Settings Page (manual):

1. Go to **Network** → **Static Leases/ DNSSEC/DHCP** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/dhcp
2. Click the **Static Leases** tab
3. Click **Add**
4. Enter the **Hostname**, **MAC Address**, and desired **IPv4 Address**
5. Click **Save & Apply**



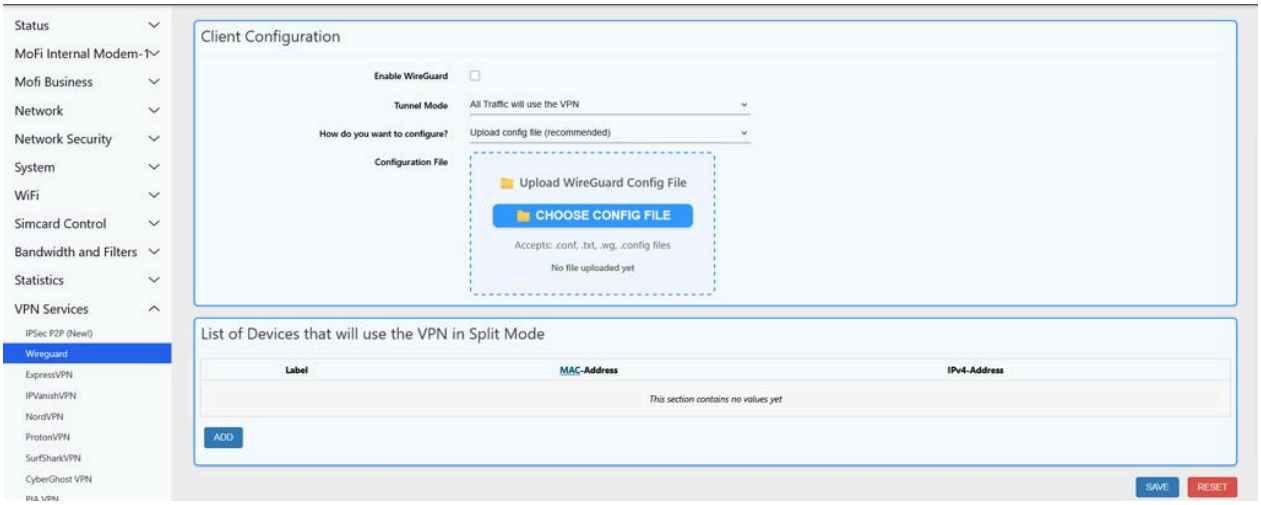
See Section 8.3 for full details.

How to Set Up WireGuard VPN Server

WireGuard VPN lets you securely connect to your router and home/office network from anywhere in the world.

1. Go to **VPN Services** → **WireGuard** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/wireguard-mofi-js
2. Toggle **Enable** to ON
3. Set **Listen Port** — default is 6677 (you can change this)
4. Set **Server Address** — default 10.110.0.1/24 is fine for most setups
5. Enter your **Endpoint Address** — this is the public IP or hostname that clients will connect to:
    - If using CloudLink: enter your CloudLink IP
    - If you have a public IP from your carrier: enter that IP
    - If using Dynamic DNS: enter your DDNS hostname
6. Toggle **Enable LAN Access** to ON if you want VPN clients to access devices on your local network (192.168.10.x)
7. Click **Save** to start the WireGuard server
8. Click **Add Peer** — the router generates a complete client configuration
9. Click **Download** next to the peer to get the `.conf` file

10. On your phone/laptop, install the **WireGuard app** (available for iOS, Android, Windows, macOS, Linux)
11. Import the `.conf` file into the WireGuard app
12. Activate the VPN — you're now securely connected to your router



Note: If your cellular carrier doesn't provide a public IP (most don't), you need **CloudLink** to make the WireGuard server reachable. Without a public IP, external devices cannot connect to your VPN.

Note: If your cellular carrier does not provide a public IP address — which is common with most carriers — CloudLink is required to make the WireGuard server accessible from the internet. Without a public IP, external devices will not be able to connect directly to your VPN server.

See Section 12.1 for full details.

How to Set Up NordVPN

Route all your internet traffic through NordVPN for privacy and security.

1:Go to **VPN Services** → **NordVPN** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/nordvpn

2: Toggle **Enable NordVPN** to ON

3: Enter your **NordVPN service credentials**:

- Log in to your NordVPN account at nordvpn.com
- Go to **Services > NordVPN** in your account dashboard
- Find your **Service credentials** (username and password) — these are NOT your login email/password

4: Enter the **Username** and **Password** from step 3

5: Enter a **Server** hostname:

- Go to **nordvpn.com/servers/tools/** in your browser
- Select your preferred country and click "Show available protocols"

- Copy the server hostname (e.g., `us1234.nordvpn.com`)

Set **Protocol** to “UDP” (faster) or “TCP” (more reliable on restricted networks)

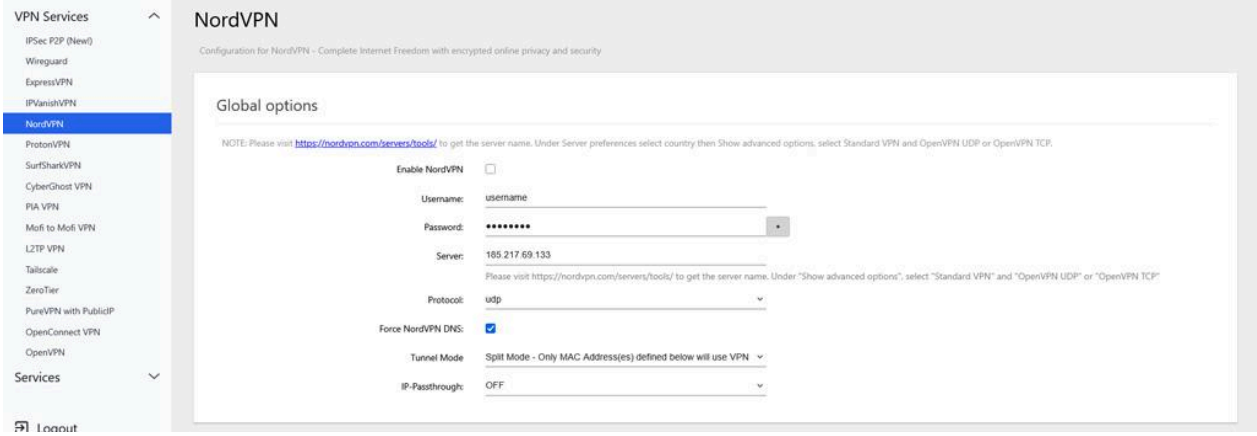
Toggle **Force NordVPN DNS** to ON (prevents DNS leaks)

Set **Tunnel Mode**:

- **All Traffic** — route everything through NordVPN
- **Split Mode** — only route specific devices through VPN (add them by MAC address below)

6: Click **Save**

7: Check **NordVPN Status** at the bottom of the page — it should show “Connected” within 30-60 seconds



See Section 12.4 for full details.

How to Set Up OpenVPN (Any Provider)

OpenVPN works with many VPN providers. You need an `.ovpn` configuration file from your provider.

1. Go to **VPN Services** → **OpenVPN** or click on the link below: http://192.168.10.1/cgi-bin/luci/admin/vpnservice/openvpn
2. Scroll down to **OVPN configuration file upload**:
   - Enter an **Instance name** (e.g., “MyVPN”)
   - Click the file selector and choose the `.ovpn` file from your VPN provider
   - Click **Upload**
3. The VPN instance will appear in the **OpenVPN Instances** table at the top
4. Click the **Enabled** toggle to turn it on
5. Click the **Start** button to connect
6. Check the **Status** column — it should show the connection as active

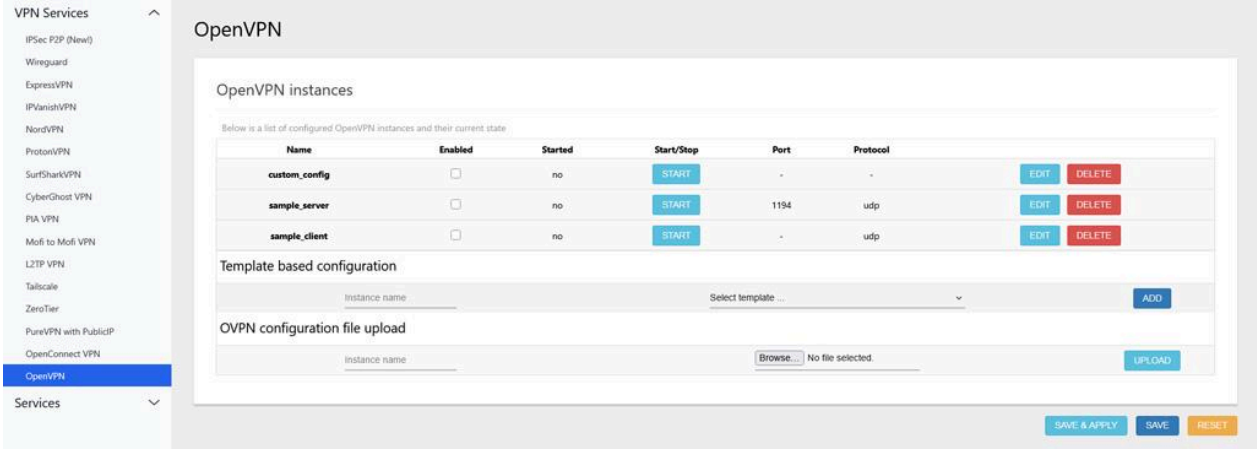
Getting a .ovpn file from your provider: - Most VPN providers offer `.ovpn` files on their website under Downloads or Manual Configuration - Download the file for your preferred server/country - Some providers

require you to enter a username and password — these are usually separate from your login credentials

Getting a .ovpn File from Your VPN Provider:

- Most VPN providers offer `.ovpn` files on their website under sections such as Downloads, Setup Guides, or Manual Configuration
- Download the `.ovpn` file for the server or country you want to connect to
- Some VPN providers require a separate VPN username and password for manual setup, which may be different from your account login credentials

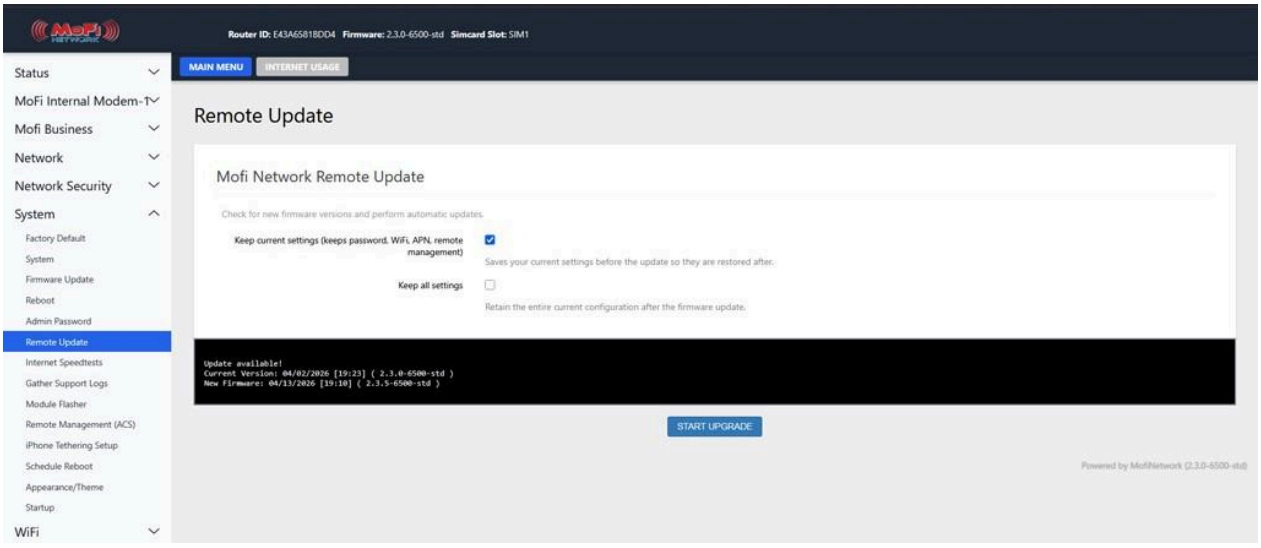
Alternatively, set up from a template: 1. Under **Add New Instance**, enter an **Instance Name** 2. Select a **Template** (e.g., “Client configuration for a routed multi-client VPN”) 3. Edit the configuration with your provider’s server details



See Section 12.11 for full details.

How to Update Router Firmware

Method 1 — One-Click Remote Update (recommended):
1. Go to **System** → **Remote Update** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/remote-update-js
2. The page shows your **current firmware version** and checks for updates
3. Check **Keep Configuration** to preserve your settings during the update
4. Click **Start Upgrade**
5. The router downloads the latest firmware from MoFi’s servers and installs it automatically
6. Wait 3-5 minutes — do NOT power off the router
7. The router reboots automatically with the new firmware

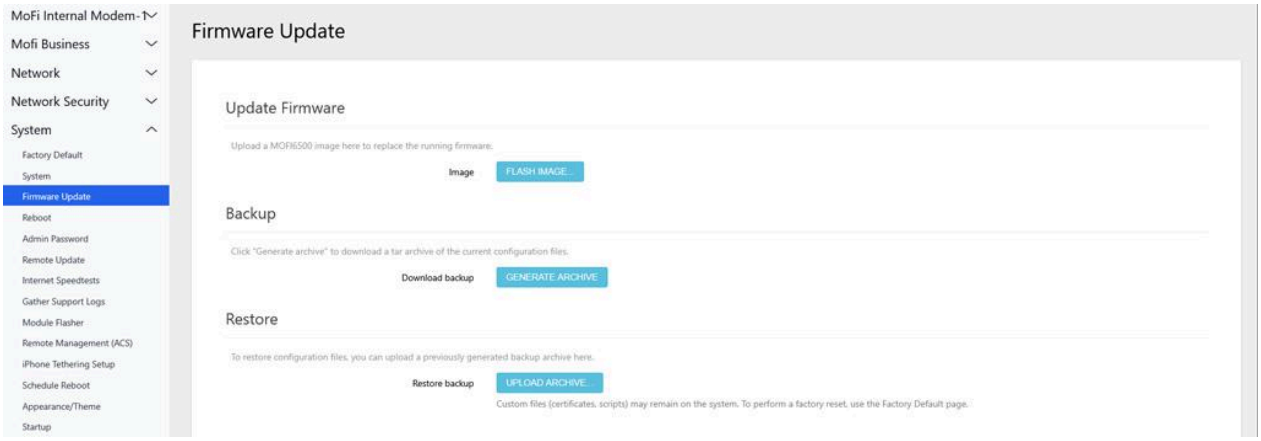


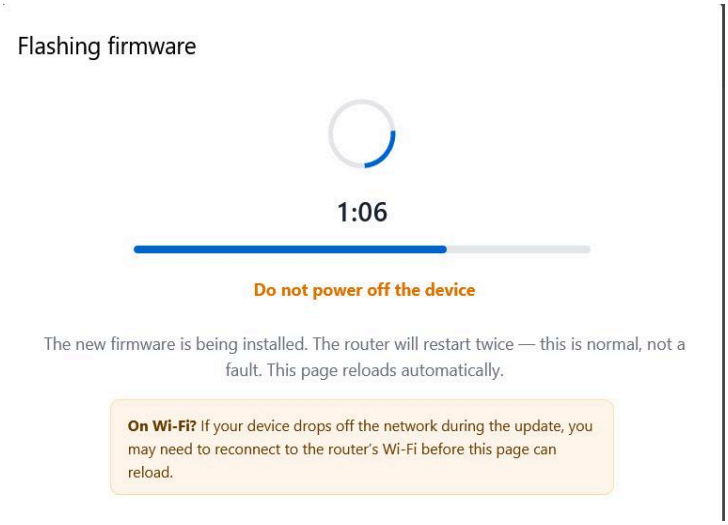
Method 2 — Manual Firmware Upload:

1. Download the firmware .bin file from MoFi or your reseller
2. Go to **System** → **Firmware Update** or click on the link below:

http://192.168.10.1/cgi-bin/luci/admin/system/flash

3. Select the firmware file and click **Flash image**
4. Wait for the update to complete — do NOT power off the router

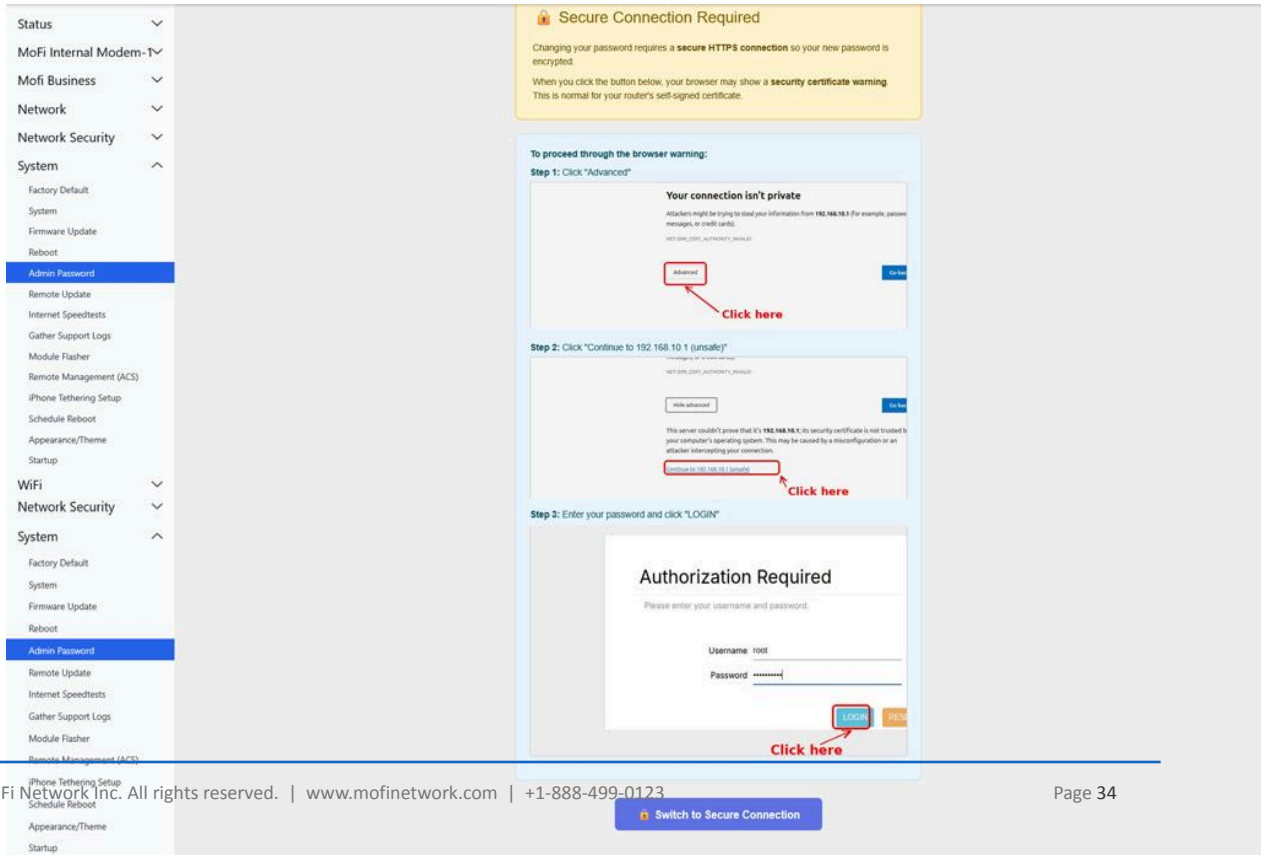




See Section 14.3 and Section 14.6 for full details.

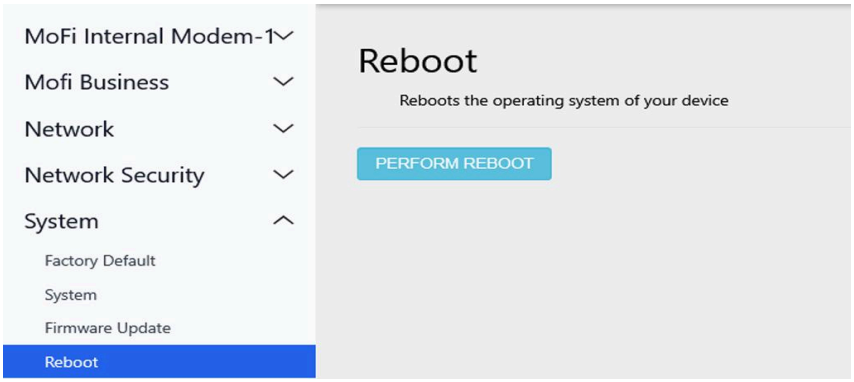
How to Change the Router Admin Password

1. Go to **System** → **Admin Password** or click on the link below: **http://192.168.10.1/cgi-bin/luci/admin/system/admin_password**
2. Click **Switch to Secure Connection** to use HTTPS (recommended for security)
3. Enter your **New Password** and **Confirm New Password**
4. Click **Save**



How to Reboot the Router=

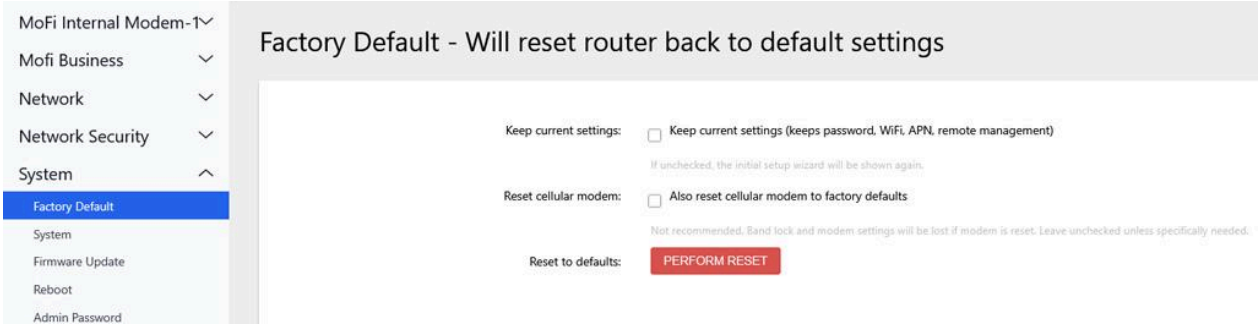
1. Go to **System** → **Reboot** or click on the link below:
   http://192.168.10.1/cgi-bin/luci/admin/system/reboot
2. Click **Perform reboot**
3. Wait approximately 90 seconds for the router to restart

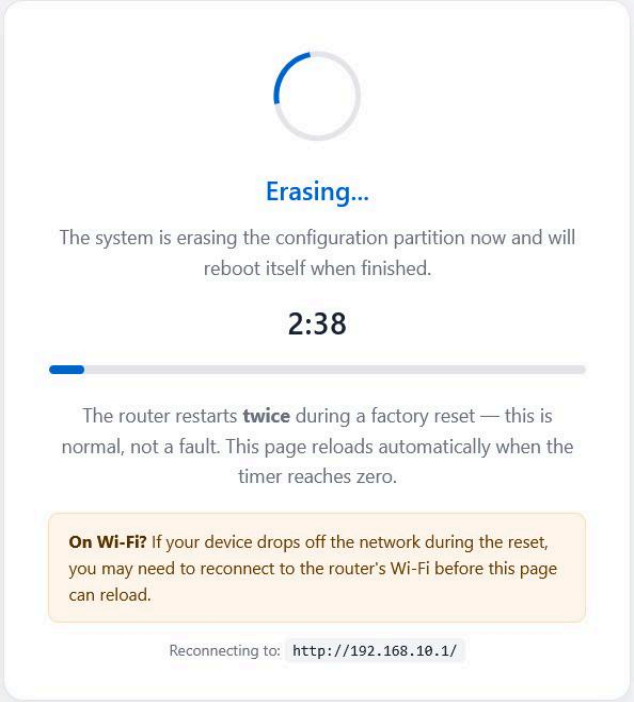


How to Factory Reset the Router

Method 1 — From the Web Interface:

1. Go to **System** → **Factory Reset** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/factory_reset
2. Click **Factory Default**
3. The router erases all settings and reboots with defaults





Method 2 — Using the Reset Button (if you can't access the web interface):
1. With the router powered on, press and hold the **Reset** button on the back for 10+ seconds
2. Release when the LEDs blink
3. The router restarts with factory default settings

After reset: Default IP is 192.168.10.1, default WiFi password is on the router label, the setup wizard will appear on first access.

How to Control the Router Remotely

The MoFi 6500 supports cloud-based remote management through the **MoFi ACS (Auto Configuration Server)** portal. This allows you to monitor and configure your router from anywhere in the world using a web browser — no VPN or public IP required.
If you are looking to manage multiple routers in a single portal, contact us and we can make a custom firmware with your own specialized ACS and all settings in the router customized with your requirements

What you can do remotely via ACS: - View router status, signal strength, and bandwidth usage - Change WiFi SSID and password - Change router admin password - Reboot or factory reset the router - Update firmware remotely - Adjust band lock settings - Configure failover and SIM failover - Push configuration changes to multiple routers simultaneously ETC.
The MOFI 6500 supports cloud-based remote management through the MOFI ACS (Auto Configuration Server) portal. This allows you to monitor, manage, and configure your router from anywhere in the world using a web browser — no VPN or public IP address required.

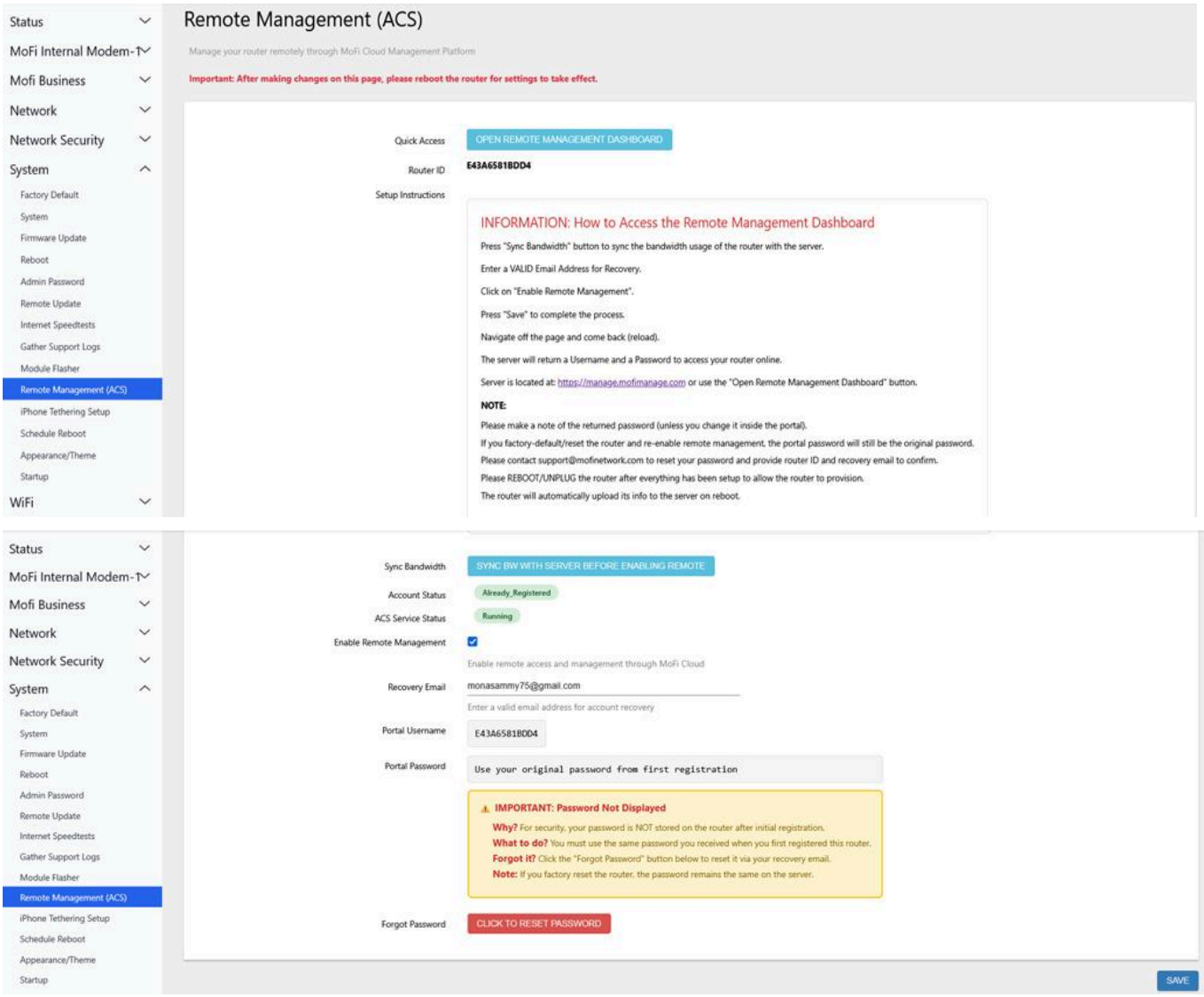
What you can do remotely through ACS:

- View router status, cellular signal strength, and bandwidth usage
- Change WiFi SSID and password
- Change the router admin password
- Reboot or factory reset the router remotely
- Update router firmware remotely
- Adjust cellular band lock settings
- Configure failover and SIM failover settings
- Push configuration changes to multiple routers simultaneously
- Monitor connected devices and network activity
- Manage router settings without needing on-site access

This makes ACS ideal for remote deployments, fleet management, business locations, RV setups, and unattended installations.

How to set it up:

1. Go to **System** → **Remote Management** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/remserver
2. Note your **Router ID** — this is your login username for the ACS portal
3. Enter a valid **Recovery Email** address (used for password resets)
4. Click **Enable Remote Management**
5. Click **Save**
6. Navigate away from the page and then return (reload the page)
7. The server will return a **Username** and **Password** — make a note of this password
8. Reboot the router to allow it to provision with server
9. After reboot, open **https://manage.mofimanage.com** in your browser
10. Log in with the Username and Password displayed on the Remote Management page



Important notes: - **Write down the returned password.** If you factory reset the router and re-enable remote management, the original password will still apply. - To reset a forgotten password, contact support@mofinetwork.com and provide your Router ID and recovery email for confirmation. - You can also change your password inside the ACS portal after logging in. - The router checks in with the ACS server periodically to receive any queued configuration changes. No special IP configuration is needed — ACS works with both public and private IP addresses.

For the complete ACS Remote Management Portal User Guide, contact MoFi Network or visit www.mofinetwork.com. The ACS guide is available as a separate document.

Important Notes:

- Be sure to write down the generated password. If the router is factory reset and remote management is enabled again, the original ACS password will still remain active.

- If you forget your ACS password, contact MOFI Network Support at support@mofinetwork.com and provide your Router ID along with the registered recovery email for verification.
- You can also change your ACS password at any time after logging into the ACS portal.
- The router periodically checks in with the ACS server to receive any pending configuration updates or commands.
- No special IP configuration is required. ACS remote management works with both public and private IP addresses.

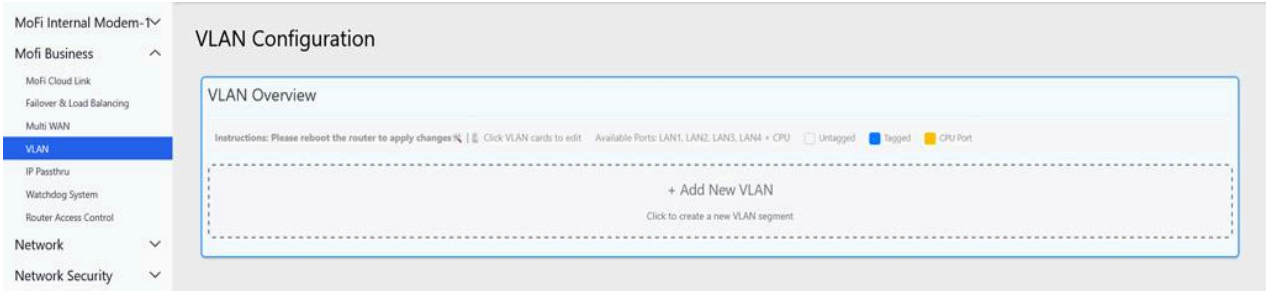
For the complete ACS Remote Management Portal User Guide, contact MOFI Network or visit www.mofinetwork.com for additional documentation. The ACS guide is provided as a separate document.

See Section 14.10 and Section 16 for full details.

How to Create a VLAN (Isolate Devices on Separate Networks)

A VLAN (Virtual LAN) creates an isolated network segment. Devices on different VLANs cannot communicate with each other. This is useful for separating IoT devices, guest networks, or security cameras from your main network.

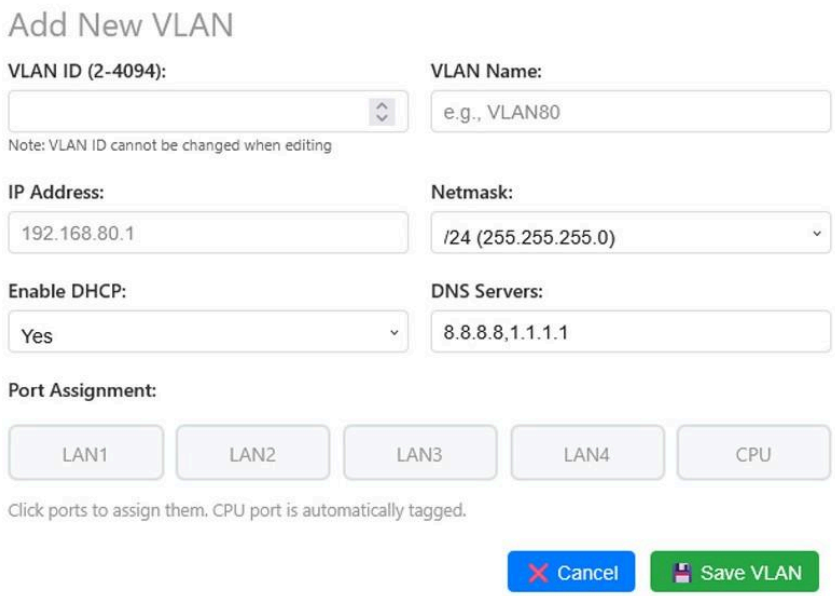
1. Go to **Mofi Business** → **VLAN** or click on the link below:
   http://192.168.10.1/cgi-bin/luci/admin/business/vlan
2. You'll see the **VLAN Overview** showing any existing VLANs as visual cards
3. Click **+ Add New VLAN**



4. Fill in the VLAN details:
   - **VLAN ID** — a unique number between 2 and 4094 (e.g., 10 for IoT, 20 for Cameras)
   - **VLAN Name** — a friendly label (e.g., "IoT Devices", "Security Cameras")
   - **IP Address** — the router's IP on this VLAN (e.g., 192.168.20.1) — must be a different subnet from your main LAN
   - **Netmask** — usually /24 (supports up to 254 devices)
   - **Enable DHCP** — set to "Yes" so devices get IP addresses automatically
   - **DNS Servers** — leave blank to use the router's DNS, or enter specific DNS servers
5. Under **Port Assignment**, click the LAN port(s) you want to assign to this VLAN (e.g., click **LAN4** to put port 4 on the VLAN)

6. Click **Save VLAN**
7. Any device plugged into the assigned LAN port will now be on the isolated VLAN network

Example: Create a VLAN for IoT devices on LAN port 4 with IP range 192.168.20.x — your IoT devices can access the internet but cannot see your computers on the main 192.168.10.x network.



See Section 7.3 for full details.

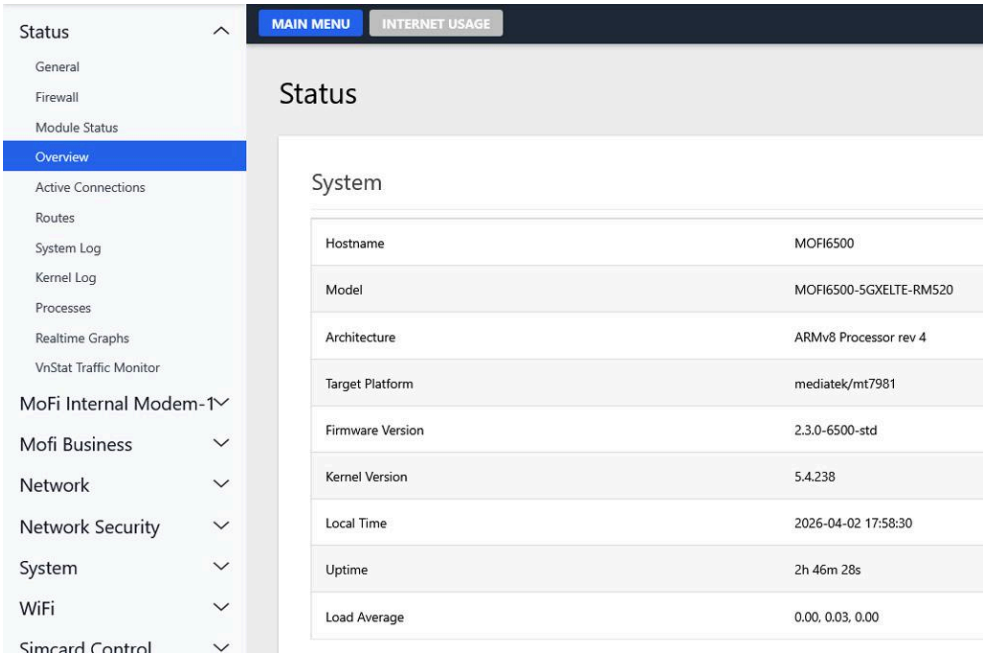
---

4. Dashboard & Status

General Status (Welcome Page)

Menu: Status → **Overview** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/status/overview

The welcome page provides a quick overview of your router's current state including: - Router model and firmware version - Network interface status - Quick links to common settings pages - Uptime and system load ETC.

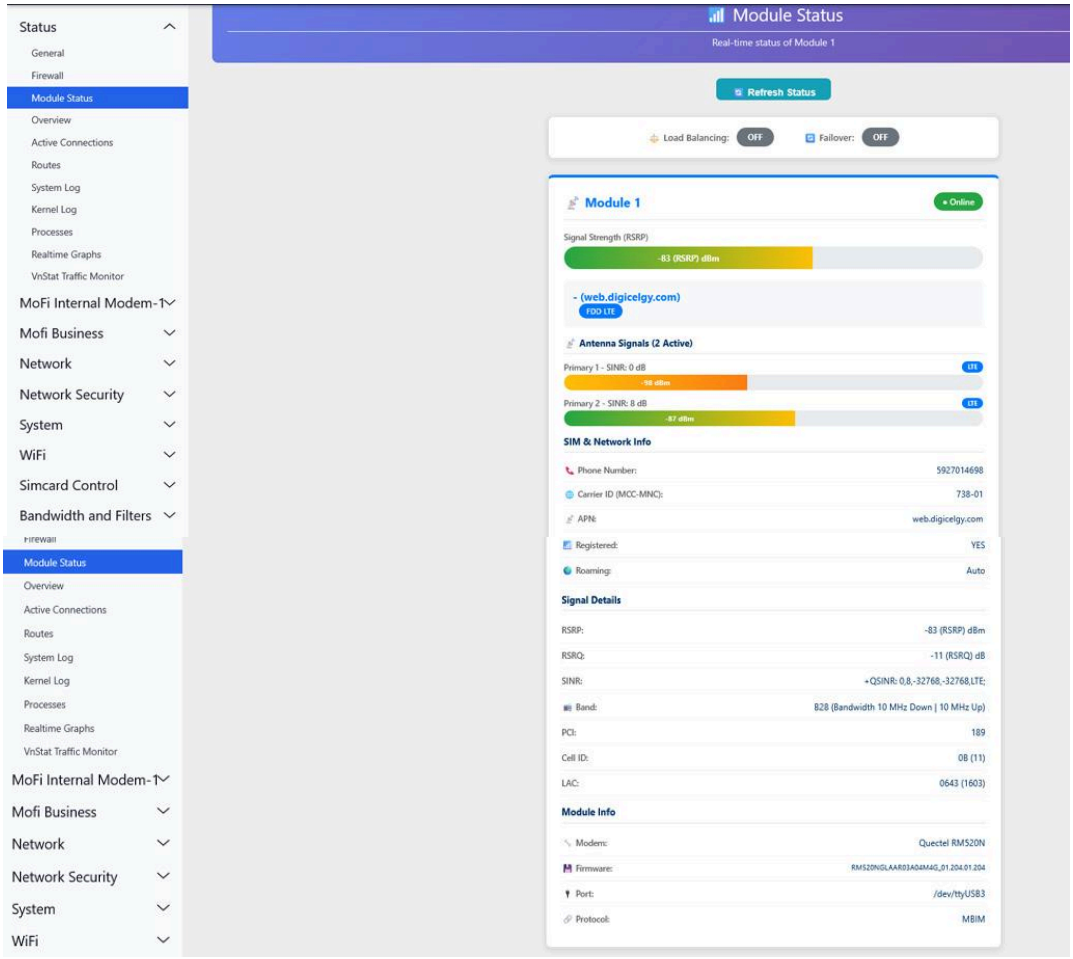


Module Status

Menu: Go to **Status** → **Module Status** or click on the link below:
(also accessible at **MoFi Internal Modem-1** > Module Status)
http://192.168.10.1/cgi-bin/luci/admin/status/module_status

Displays real-time cellular connection status with visual indicators:

- **Load Balancing** indicator — shows ON or OFF
- **Failover** indicator — shows ON or OFF
- **Module 1** status badge — Online (green) or Offline (red)
- **Signal Strength (RSRP)** — visual bar showing signal power in dBm
- **Carrier/Network** — displays carrier name and connection technology (e.g., “T-Mobile TDD NR5G”, “AT&T FDD LTE”)
- **Antenna Signals** — individual antenna readings:
    - Primary Antenna 1: SINR value + dBm bar with 5G/4G label
    - Primary Antenna 2: SINR value + dBm bar with 5G/4G label
    - Secondary Antenna 1: SINR value + dBm bar with 5G/4G label
    - Secondary Antenna 2: SINR value + dBm bar with 5G/4G label

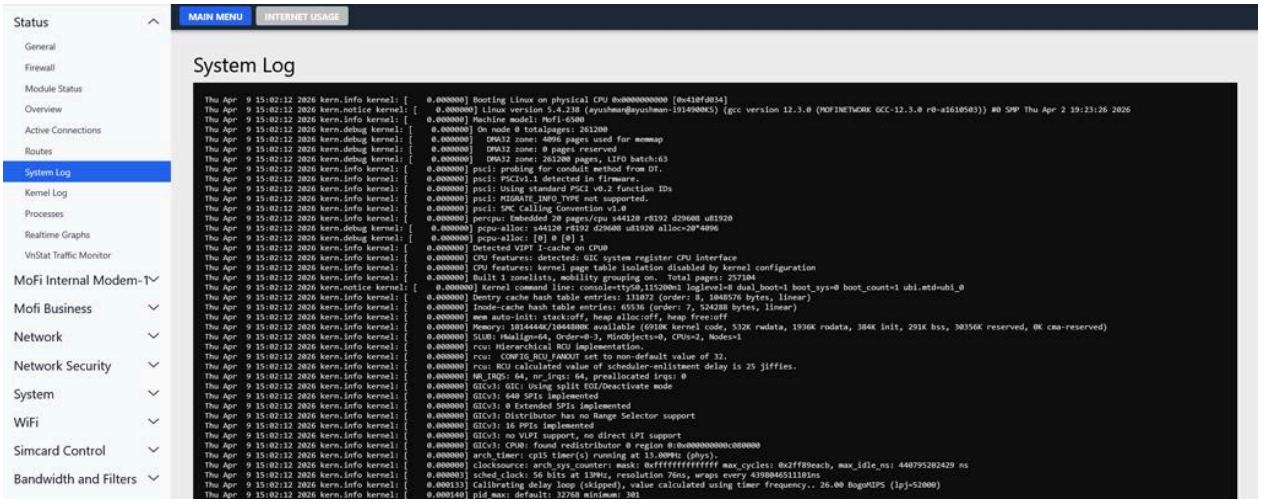


Click **Refresh Status** to update all displayed values.

System Log

Menu: Go to **Status** → **System Log** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/status/syslog

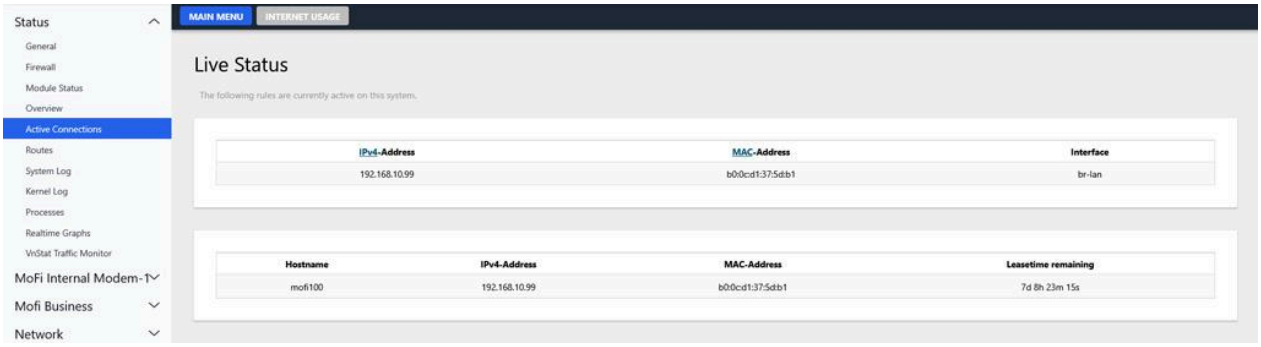
Displays the real-time system log output. Useful for: - Troubleshooting connectivity issues - Viewing cellular modem connection/disconnection events - Monitoring ACS communication - Watching firewall and security events - Diagnosing boot problems



Active Connections

Menu: Go to **Status** → **Active Connections** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/status/live

Shows all active network connections currently passing through the router: - Source IP address and port - Destination IP address and port - Protocol (TCP, UDP, ICMP) - Connection state - Bytes transferred



---

5. Cellular Modem — Module 1

This section covers all pages under the **MoFi Internal Modem-1** menu. Module 1 is the primary built-in cellular modem (Quectel RM520N-GL).

5.1 Configuration

Menu: Go to **MoFi Internal Modem-1** → **Configurations** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/module1_config_js

This is the primary cellular modem setup page. All settings here control how Module 1 connects to your cellular carrier.

Basic Settings:

Setting	Options	Description
Enabled	Toggle ON/OFF	Turn the cellular modem on or off. When disabled, the modem is powered down and no cellular connection is made.
Country	Canada, Costa Rica, Jamaica, Nigeria, United States, Mexico, Bahamas, Tether, UK, Germany, India, France, Custom APN	Select your country to auto-populate carrier APN settings. Select “Custom APN” to manually enter an APN.
Provider	Auto / carrier list	Your cellular carrier. “Auto” lets the router detect the carrier automatically.
APN	Text field	The Access Point Name for your carrier’s data network. Usually auto-detected. Common examples: “broadband” (Verizon), “fast.t-mobile.com” (T-Mobile), “iot.att.com” (AT&T IoT).

ISP Credentials:

Setting	Options	Description
Authentication	none / pap / chap / mschapv2	Authentication method required by your carrier. Most carriers use “none”.
Username	Text field	ISP-provided username (if required).
Password	Text field	ISP-provided password (if required).
Pincode	Text field	SIM card PIN code (if your SIM has PIN lock enabled).

MTU / MSS Settings:

Setting	Options	Description
Auto MTU	Toggle	When ON, the router automatically determines the optimal Maximum Transmission Unit size.
ISP Preferred MTU	Checkbox	Use the MTU value advertised by your carrier.
MTU	Numeric value	Manually set the MTU (typically 1500 for most carriers, 1428 for some). Only editable when Auto MTU is off.
Auto MSS	Toggle	Automatically calculate the Maximum Segment Size from the MTU.

Setting	Options	Description
Override MSS	Numeric value	Manually set the MSS value. Only used when Auto MSS is off.

Connection Settings:

Setting	Options	Description
TTL	No TTL / 64 / 65 / 117 / others	Override the Time-To-Live value on outgoing packets. Setting TTL to 65 can help bypass some carriers' hotspot detection. "No TTL" leaves the default value.
IPv6 PDP Type	IPv4 Only / IPv6 Only / IPv4v6	Controls the IP protocol version used on the cellular connection. "IPv4 Only" is recommended for broadest compatibility. "IPv4v6" enables dual-stack if your carrier supports it.
Reconnection Time	unspecified / 1 min / 2 min / 3 min / 4 min / 5 min / Off	How long to wait before attempting to reconnect after a connection drop. "Unspecified" uses the system default.
Web Check	Toggle	When ON, the router periodically loads a web page to verify the internet connection is actually working (not just connected). Triggers reconnection if the check fails.
Service Mode	Module Default / LTE only / 5G Only SA / 4G/LTE / 4G Only / LTE/5G	Controls which cellular technologies the modem is allowed to use. See table below.
Phone Number	Text field	Your SIM card's phone number (informational, used for SMS features).

Service Mode Options Explained:

Mode	Description	When to Use
Module Default	Modem chooses the best available technology automatically	Default — recommended for most users
LTE/5G	Allow both LTE and 5G connections	Recommended for 5G coverage areas
5G Only SA	Force 5G Standalone only — will not fall back to LTE	Only use if you have confirmed strong 5G SA coverage
LTE Only	Force LTE only — disables 5G	Useful for troubleshooting, or if 5G performance is poor in your area
4G/LTE	Use 4G LTE bands only	Same as LTE Only
4G Only	Restrict to 4G bands	Legacy option

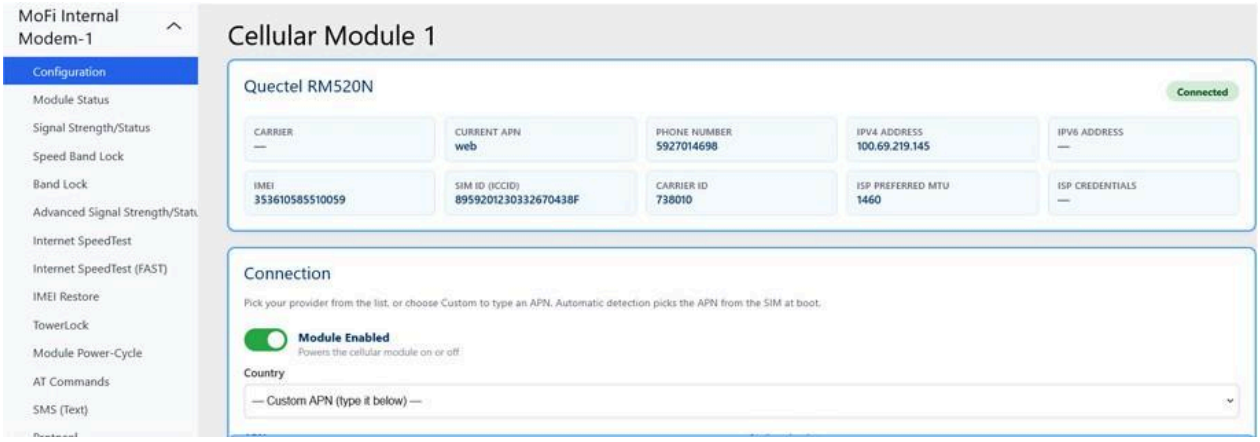
Module Watchdog:

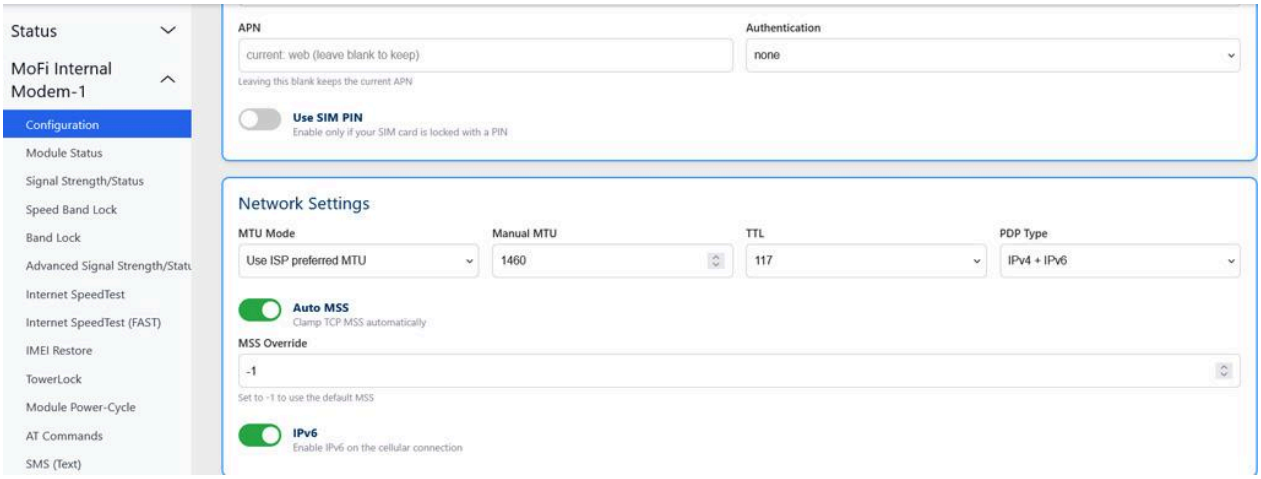
Setting	Options	Description
Watchdog Ping Attempts	Numeric	Number of ping attempts before considering the module offline. The watchdog periodically checks if the modem has a working internet connection.

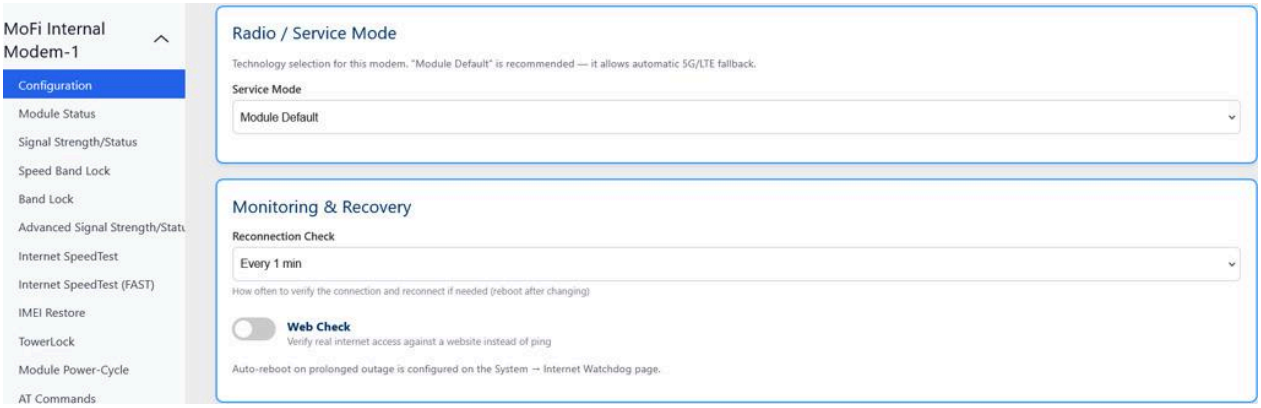
Read-Only Information (displayed at bottom of page): - **IMEI** — The modem's unique hardware identifier (International Mobile Equipment Identity) - **SIM ID (ICCID)** — The SIM card's unique identifier - **Carrier ID** — The detected carrier name - **Current APN** — The APN currently in use

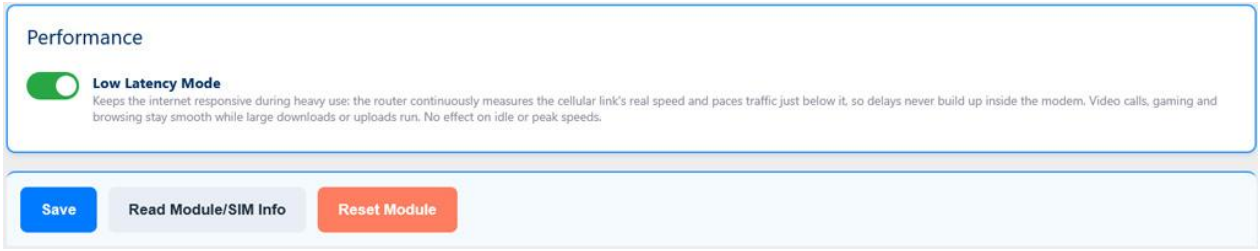
Step-by-Step: Configuring the Cellular Modem for a New SIM Card:
1. Insert your activated SIM card into SIM Slot 1 (power off the router first)
2. Power on the router and wait for it to fully boot (90 seconds)
3. Navigate to MoFi Internal Modem-1 > Configuration
4. Ensure **Enabled** is set to ON
5. Select your **Country** from the dropdown
6. The **APN** field should auto-populate. If not, enter your carrier's APN manually: - AT&T: `broadband` or `iot.att.com` - T-Mobile: `fast.t-mobile.com` - Verizon: `vzwinternet`
7. Set **Service Mode** to "LTE/5G" (recommended)
8. Set **TTL** to "65" if you want to bypass hotspot detection (optional)
9. Set **IPv6 PDP Type** to "IPv4 Only" for simplest setup
10. Click **Save**
11. Click **Read Module/SIM Info** to verify the SIM is detected
12. Wait 30-60 seconds for the modem to connect
13. Check Module Status page to verify connectivity

Buttons: - **Read Module/SIM Info** — Refreshes the read-only information fields - **Reset Module** — Power-cycles the cellular modem (does not reboot the router) - **Save** — Saves and applies changes immediately (modem reconnects with new settings) - **Reset** — Discards unsaved changes









5.2 Module Status

Menu: Go to **MoFi Internal Modem-1** → **Module Status** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/module_status

See Section 4 — Module Status for full details. This is the same page accessible from both the Status menu and the Modem-1 menu.

5.3 Signal Strength / Status

Menu: Go to **MoFi Internal Modem-1** → **Signal Strength/Status** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/quectel_stat

Displays comprehensive cellular signal information. Press **Refresh** to update.

General Information: - Modem model (e.g., RM520N-GL) - Currently connected LTE/NR5G Band - Roaming status (Home / Roaming)

Modem/SIM Information: - IMEI (modem hardware ID) - ICCID (SIM card ID) - Phone Number (if provisioned)

Signal Metrics:

Metric	Excellent	Good	Fair	Poor	Description
RSRP (dBm)	-80 or better	-80 to -90	-90 to -100	Below -110	Reference Signal Received Power — primary measure of signal strength
RSRQ (dB)	-10 or better	-10 to -15	-15 to -20	Below -20	Reference Signal Received Quality — signal quality relative to interference
SINR (dB)	20+	13-20	0-13	Below 0	Signal-to-Interference-plus-Noise Ratio — signal clarity
RSSI (dBm)	-65 or better	-65 to -75	-75 to -85	Below -85	Received Signal Strength Indicator — overall signal power

Modem Status Fields: - Operational Mode (Online/Offline) - Registered on Network (Yes/No) - ECIO/RSRQ value - RSRP value - Primary antenna signal and Secondary antenna signal - Carrier Aggregation info (shows if multiple bands are combined)

Cell Information: - MCC (Mobile Country Code) — identifies the country - MNC (Mobile Network Code) — identifies the carrier - RNC/eNB ID — identifies the base station - LAC/TAC (Location/Tracking Area Code) - Cell ID — specific cell sector

BandLock Current Bands: - Displays any currently locked bands (if band lock is configured)

5.4 Speed Band Lock

Menu: Go to **MoFi Internal Modem-1** → **Speed Band Lock** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/cellbandlock

Automatically tests each cellular band's speed and optionally locks to the fastest ones. This is an automated tool that disconnects, tests each band individually, and reports the results.

Settings:

Setting	Options	Description
Scan Mode	All Bands / AT&T Optimized / T-Mobile Optimized / Verizon Optimized / Bell / Rogers / Telus / Freedom / Jio / Airtel / Custom Bands	Determines which bands to test. Carrier-optimized modes only test bands used by that carrier, saving time and data.
Speed Test Server	Automatic / US Central Dallas / US South Atlanta / US East Newark / US West Fremont / Europe London / India Mumbai / UAE Dubai	Select the closest speed test server for accurate results. "Automatic" picks the best server.
Tests Per Band	1 Fast / 2 Recommended / 3 Thorough	Number of speed tests to run per band. More tests = more accurate results but more data usage and time.
Include 5G Bands	Toggle	When ON, also tests 5G NR bands in addition to LTE bands.
Auto-Lock to Top 3 Bands	Toggle	When ON, automatically locks the modem to the 3 fastest bands after testing completes.

Select Bands to Test (Custom Mode): - LTE Bands: B2, B4, B5, B12, B13, B14, B17, B25, B26, B30, B41, B48, B66, B71 - 5G Bands: n2, n5, n7, n12, n25, n41, n48, n66, n71, n77, n78, n79

Buttons: - **Start Scan** — Begins the speed test scan. The router will disconnect and reconnect to each band. - **Stop Scan** — Aborts the scan in progress. - **Refresh Results** — Updates the results display.

Scan Results Display: After scanning completes, a table shows each tested band with its download speed, upload speed, and latency. Bands are ranked from fastest to slowest.

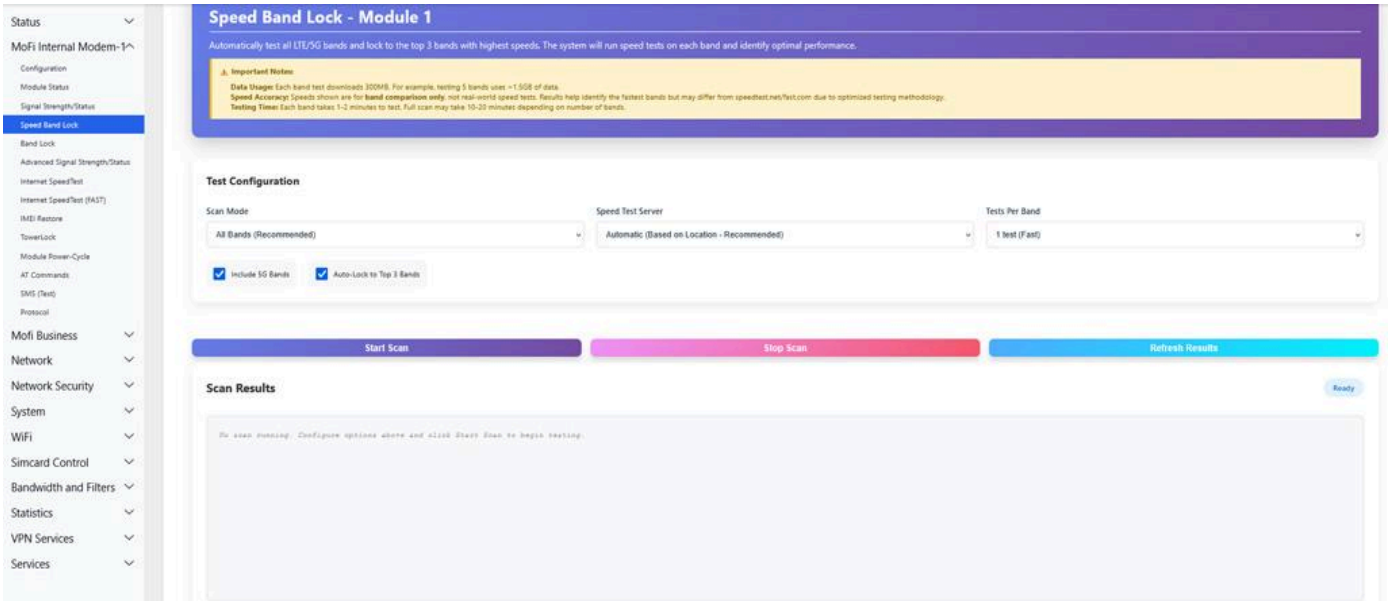
Important Warnings: - Each band test downloads approximately 300 MB of data - A full scan of all bands can use 5-15 GB of cellular data - The router will be offline during testing (each band test takes 30-60 seconds) - Do not navigate away from the page during scanning

Important Warnings:

- Each individual band test downloads approximately 300 MB of cellular data
- A complete scan of all supported bands may consume between 5–15 GB of data depending on the router and network conditions
- The router will temporarily go offline during testing, with each band test typically taking 30–60 seconds
- Do not close the browser, refresh the page, or navigate away from the scanning page while the test is in progress

Step-by-Step: Running a Speed Band Lock Scan:

1. Navigate to MoFi Internal Modem-1 > Speed Band Lock
2. Select your carrier under **Scan Mode** (or use “All Bands”)
3. Choose a **Speed Test Server** close to your location
4. Set **Tests Per Band** to “2 Recommended” for a good balance
5. Enable **Include 5G Bands** if you have 5G service
6. Enable **Auto-Lock to Top 3 Bands** if you want automatic optimization
7. Click **Start Scan**
8. Wait for all bands to be tested (may take 10-30 minutes depending on band count)
9. Review the results table — the fastest bands are listed first
10. If you did not enable auto-lock, you can manually lock to preferred bands on the Band Lock page



5.5 Band Lock

Menu: Go to **MoFi Internal Modem-1** → **Band Lock** or click ont the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/quectel-bandlock-js

Manually lock the modem to specific LTE and/or 5G bands. This forces the modem to only connect using the selected bands, ignoring all others.

Current Configuration Display: Shows the currently active band lock filters for WCDMA, LTE, and NR5G.

Network Mode:

Mode	Description
AUTO LTE+5G	Modem uses both LTE and 5G bands automatically (default)
LTE Only	Restrict to LTE bands only
5G Only	Restrict to 5G NR bands only
LTE+5G Prefer 5G	Use both, but prefer 5G when available
AT&T	AT&T-optimized band selection
T-Mobile	T-Mobile-optimized band selection
Verizon	Verizon-optimized band selection

LTE Bands (check/uncheck individual bands): - **Select All** / **Clear All** buttons - Available: B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B43, B46, B48, B66, B71

5G NR Bands (check/uncheck individual bands): - **Select All** / **Clear All** buttons - Available: n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n66, n70, n71, n75, n76, n77, n78, n79

Buttons: - **Save** — Saves the band lock settings and applies them to the modem immediately - **Get Current Band Lock Status** — Query the modem for currently locked bands

Warning: Only lock bands if you know which bands your carrier uses in your area. Locking to incorrect bands will cause the modem to lose cellular connectivity entirely. If this happens, return to this page and click **Select All** then **Save** to unlock all bands.

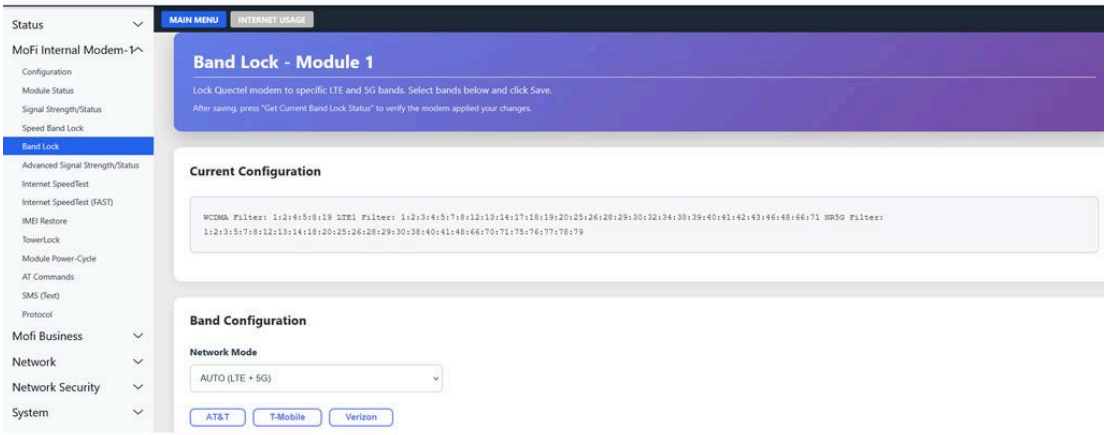
Step-by-Step: Locking to T-Mobile Bands:
1. Navigate to MoFi Internal Modem-1 > Band Lock
2. Set **Network Mode** to “T-Mobile” for automatic selection, OR:
3. Click **Clear All** under LTE Bands
4. Check: B2, B4, B12, B25, B41, B66, B71
5. Click **Clear All** under 5G NR Bands
6. Check: n25, n41, n71, n77
7. Click **Save**
8. The modem will reconnect using only the selected bands

Step-by-Step: Unlocking All Bands (Recovery):

1. Navigate to MoFi Internal Modem-1 > Band Lock
2. Set **Network Mode** to “AUTO LTE+5G”
3. Click **Select All** under LTE Bands
4. Click **Select All** under 5G NR Bands
5. Click **Save**

Common US Carrier Bands:

Carrier	Primary LTE Bands	Primary 5G Bands
AT&T	B2, B4, B5, B12, B14, B30, B66	n2, n5, n77
T-Mobile	B2, B4, B12, B25, B41, B66, B71	n25, n41, n71, n77
Verizon	B2, B4, B5, B13, B48, B66	n2, n5, n77

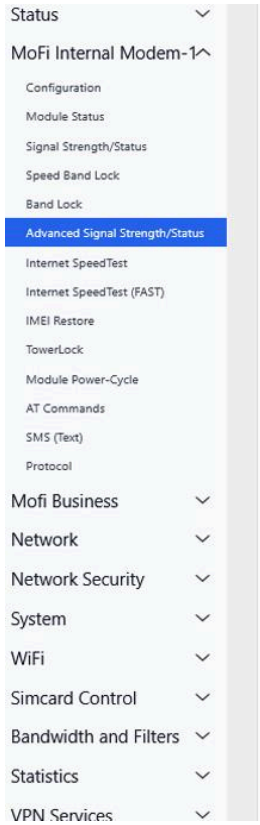


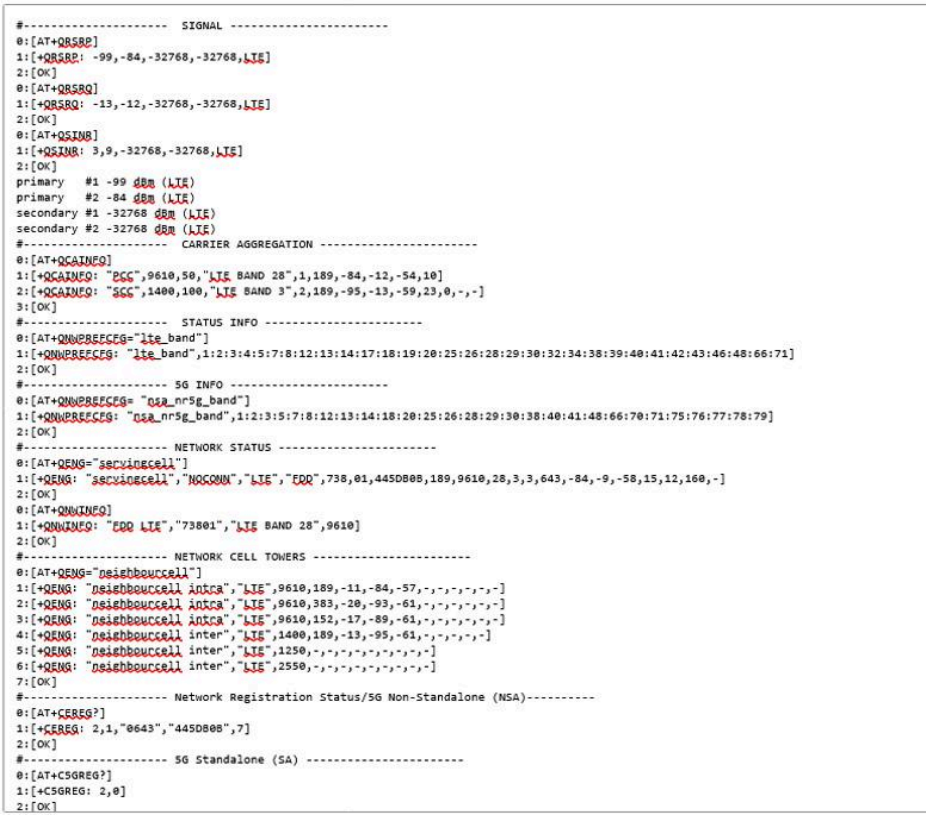
5.6 Advanced Signal Strength / Status

Menu: Go to **MoFi Internal Modem-1** → **Advanced Signal Strength/Status** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/quectel_adv_signal

Displays raw AT command output from the modem for advanced troubleshooting. This is a display-only page showing:

- **SIGNAL** — Per-antenna RSRP, RSRQ, SINR values (QRSRP, QRSRQ, QSINR commands)
- **CARRIER AGGREGATION** — Active carrier aggregation info (QCAINFO command), showing primary and secondary component carriers
- **STATUS INFO** — Current LTE band configuration details
- **5G INFO** — NR5G band configuration, frequency, bandwidth
- **NETWORK STATUS** — Serving cell info and network info (QNWINFO)
- **NETWORK CELL TOWERS** — Neighbor cell measurements for signal comparison
- **Network Registration Status** — EPS (CEREG) and 5G (C5GREG) registration states
- **5G Status** — EN-DC (EUTRA-NR Dual Connectivity) support status (QENDC)





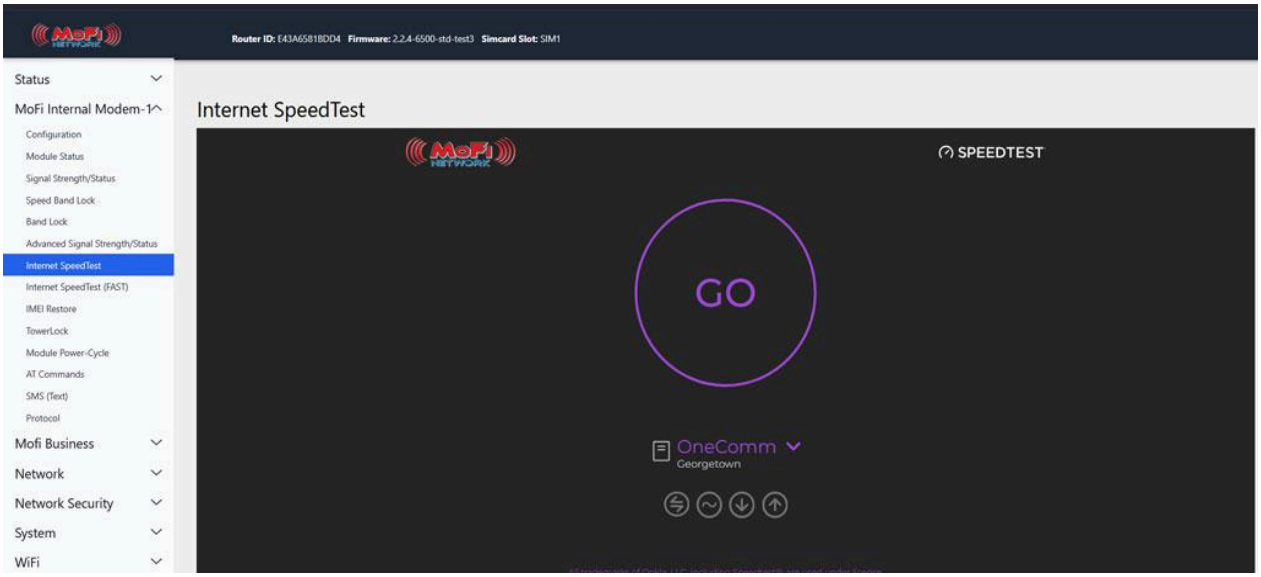
This page is primarily for MoFi technical support and advanced users.

5.7 Internet SpeedTest

Menu: Go to **MoFi Internal Modem-1** → **Internet SpeedTest** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/speed

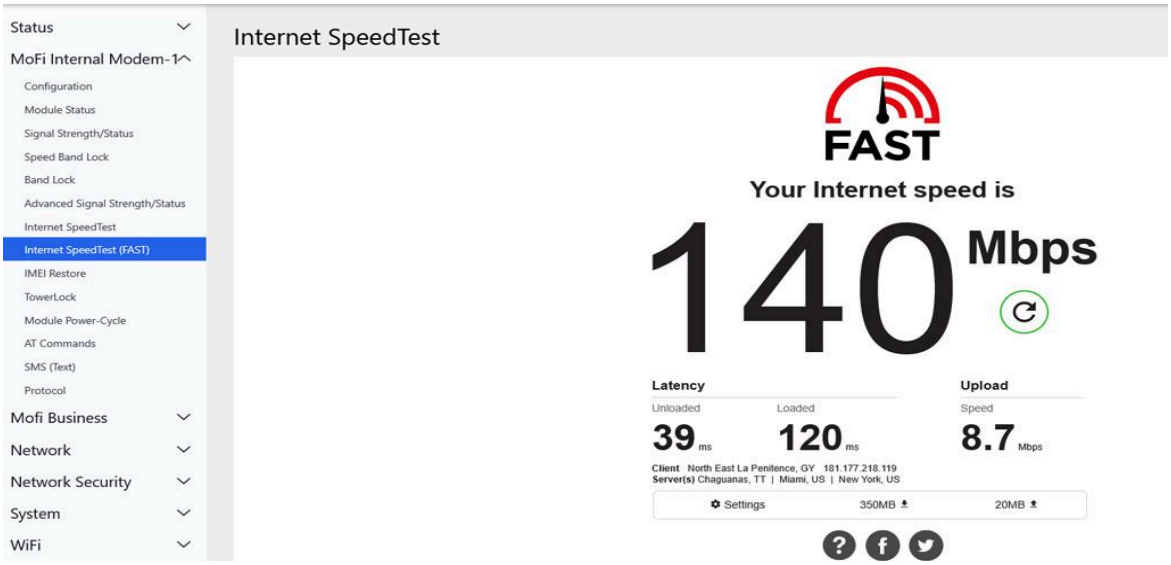
Embedded Speedtest.net widget for testing your current internet speed.

- Click the **GO** button to start a speed test
- Select a nearby server from the dropdown for most accurate results
- Results display: **Ping** (ms), **Download** (Mbps), **Upload** (Mbps)



5.8 Internet SpeedTest (FAST)
Uses fast.com for speed test

Menu: Go to **MoFi Internal Modem-1** → **Internet SpeedTest (FAST)** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/netflixspeed



Embedded fast.com widget powered by Netflix for a quick single-button speed test. Click the button and wait for results. This tests your connection speed to Netflix's servers specifically.

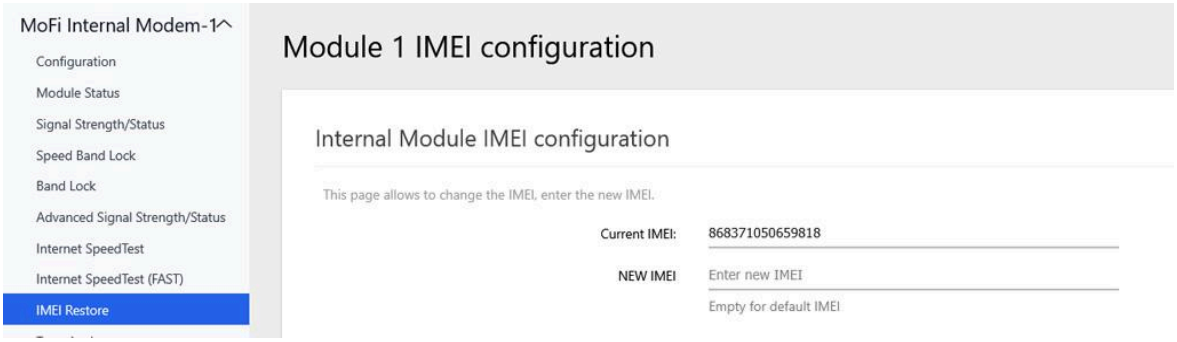
5.9 IMEI Restore

Menu: Go to **MoFi Internal Modem-1** → **IMEI Restore** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/imei-js

Restore or change the modem's IMEI number.

- **Current IMEI** — Displays the modem's current IMEI (read-only)
- **NEW IMEI** — Enter a new IMEI value, or leave empty to restore the factory default IMEI

Buttons: - **Save** — Write the new IMEI to the modem - **Reset** — Discard changes



Warning: Changing the IMEI to an unauthorized value may violate regulations in your country. This feature is intended for restoring the original factory IMEI if it becomes corrupted.

5.10 Tower Lock

Menu: Go to **MoFi Internal Modem-1** → **TowerLock** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/tower_scanjs

Lock the modem to a specific cell tower. This prevents the modem from switching to other towers, which can be useful in areas where a nearby tower provides better performance than the one the modem automatically selects.

How to Use:

1. Click **Show All** to start a tower scan. The modem will search for all visible cell towers in your area. This may take 1-3 minutes.
2. **Carrier Table** — After scanning, a table displays all discovered towers:

Column	Description
Mode	Connection type (LTE or NR5G)
MCC	Mobile Country Code
MNC	Mobile Network Code (identifies carrier)
LAC	Location Area Code
Signal	Signal strength reading
Frequency	Operating frequency of the tower
PCI	Physical Cell ID — unique identifier for the cell sector
SCS	Subcarrier Spacing (5G only)
Band	LTE band or NR band number

3. **Current Cell Information** — Shows the tower you are currently connected to (auto-populated).
4. **Tower Lock Settings:**

Setting	Options	Description
Enable	Checkbox	Enable or disable tower lock
Mode	LTE / NR5G	Select the technology type of the tower you want to lock to
Frequency	From scan results	The frequency of the desired tower
PCI	From scan results	The Physical Cell ID of the desired tower
SCS	From scan results	Subcarrier spacing (5G only)
Band	From scan results	The band of the desired tower

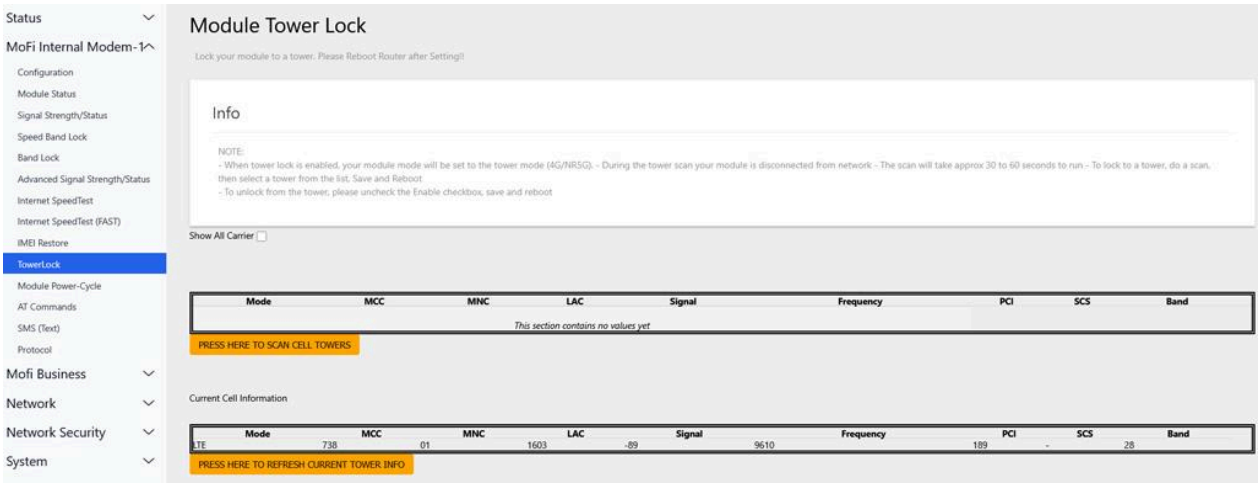
5. Click **Save** to apply the tower lock.

Step-by-Step: Locking to a Specific Tower:
1. Navigate to MoFi Internal Modem-1 > TowerLock
2. Click **Show All** to start scanning for towers (wait 1-3 minutes)
3. Review the Carrier Table — look for towers with the best signal strength

4. Note the **Mode**, **Frequency**, **PCI**, **SCS**, and **Band** values of your preferred tower
5. In the Tower Lock section, check **Enable**
6. Set **Mode** to match (LTE or NR5G)
7. Enter the **Frequency**, **PCI**, **SCS**, and **Band** values from the scan
8. Click **Save**

Step-by-Step: Disabling Tower Lock:

1. Navigate to MoFi Internal Modem-1 > TowerLock
2. Uncheck **Enable**
3. Click **Save**
4. The modem will automatically select the best available tower.



Note: If the locked tower goes offline or becomes unreachable, the modem will have no internet connectivity until the tower comes back online or you disable the tower lock.

5.11 Module Power-Cycle

Menu: Go to **MoFi Internal Modem-1** → **Module Power-Cycle** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/mpowercycle

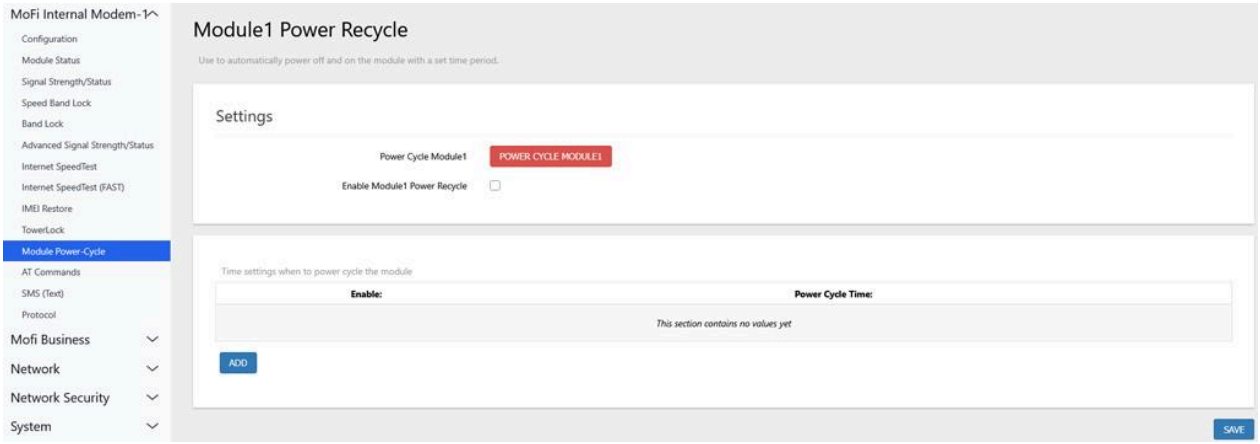
Schedule automatic power-cycling (restart) of the cellular modem at regular intervals. This can help maintain stable connectivity in environments where the modem occasionally loses connection.

Settings:

Setting	Options	Description
Enable Module1 Power Recycle	Checkbox	Enable or disable scheduled power cycling
When to Cycle	1-23 Hours	How often to power-cycle the modem

Time Settings Table: - Add specific times for power cycling using the table - Each row has: **Enable** checkbox and **Power Cycle Time** selector - Click **Add** to add additional time slots

Buttons: Save.



5.12 AT Commands

Menu: Go to **MoFi Internal Modem-1** → **AT Commands** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/sendat

Send AT commands directly to the cellular modem. This is an advanced tool for diagnostics and configuration.

How to Use:
1. Select a preset command from the **Preset Command** dropdown (e.g., “Signal Quality/Strength → AT+CSQ”)
2. Or type a custom AT command in the **Command to send** field
3. Click **Send command**
4. View the modem’s response in the **Reply** area

Common Preset Commands: - `AT+CSQ` — Signal quality (returns RSSI and BER) - `AT+COPS?` — Current operator - `AT+QENG="servingcell"` — Serving cell information - `AT+QNWINFO` — Network information - `AT+CFUN?` — Phone functionality mode

Click **Clear form** to reset the command field and reply area.

Warning: Sending incorrect AT commands can disrupt modem operation. Only use this if you understand AT command syntax or are directed by MoFi support.

5.13 SMS (Text Messages)

Menu: Go to **MoFi Internal Modem-1** → **SMS (Text)** Or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/sms-simple

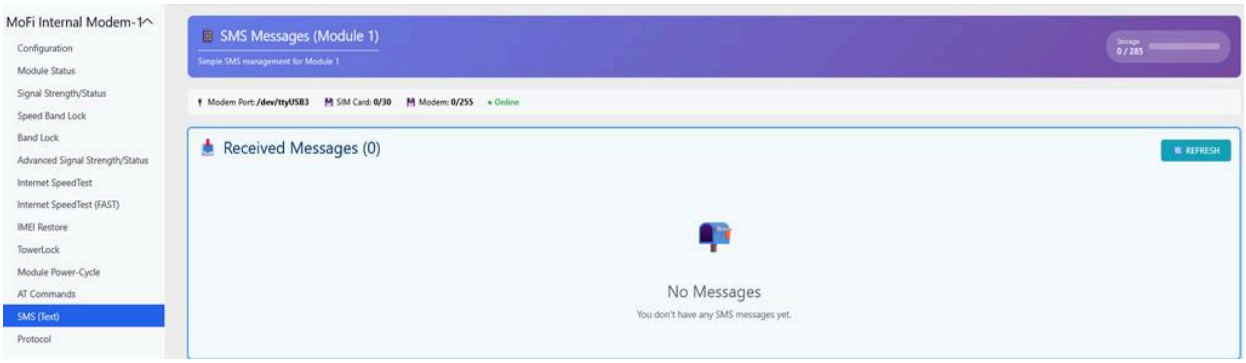
Send and receive SMS text messages through the cellular modem's SIM card.

Storage Display: - Shows current message count vs. capacity (e.g., "9/265") - Modem port, SIM card slot, and modem memory status (read-only)

Received Messages: - List of all received SMS messages - Each message shows: sender number, timestamp, message text - **Reply** button — opens a reply form pre-filled with the sender's number - **Delete** button — removes individual messages - **Delete All** button — clears all received messages - **Refresh** button — checks for new messages

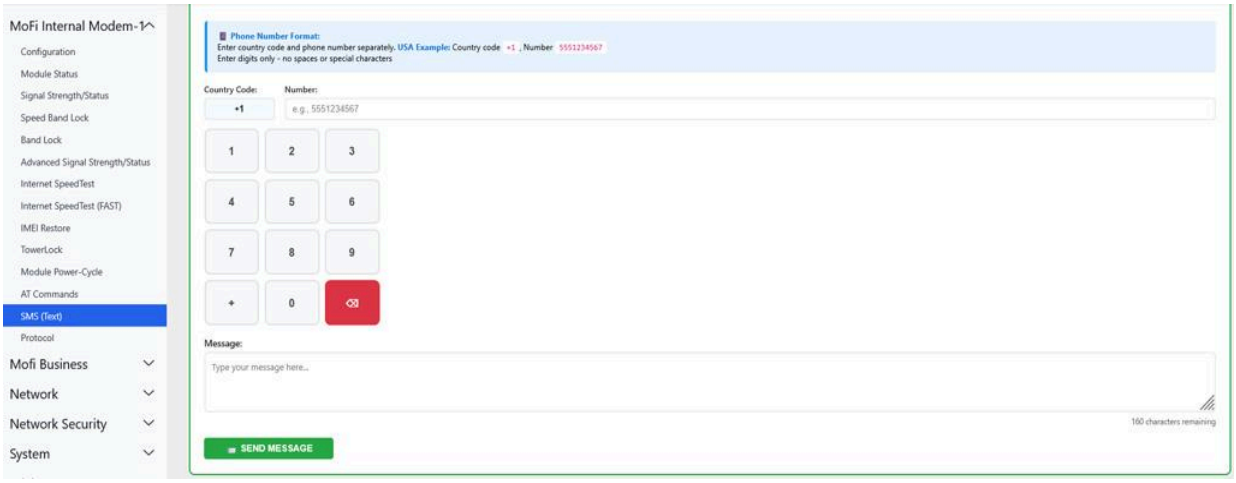
Received Messages

- View all received SMS messages
- See sender number, timestamp, and message text
- Reply button opens a pre-filled reply form with the sender's number
- Delete individual messages
- Delete All clears all received messages
- Refresh checks for new messages



Send SMS:

Field	Description
Country Code	Numeric country code (e.g., 1 for US/Canada, 44 for UK, 91 for India)
Number	Recipient's phone number (without country code)
Message	Message text (maximum 160 characters for a single SMS)



Click **Send Message** to send.

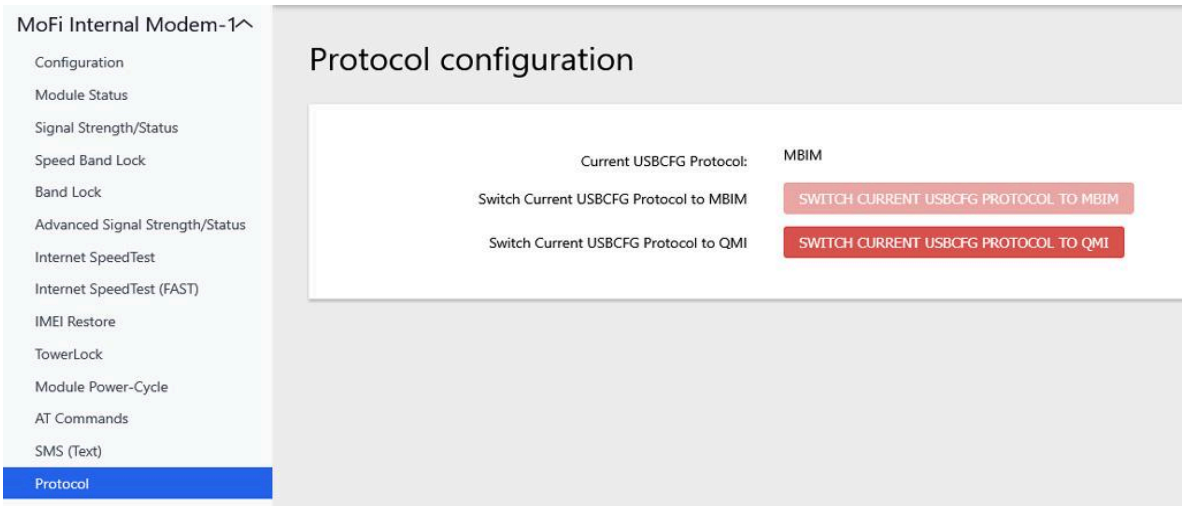
5.14 Protocol

Menu: Go to **MoFi Internal Modem-1** → **Protocol** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/jmodule1/protocolq

Switch the USB communication protocol between the modem and the router.

- **Current USBCFG Protocol** — Displays the active protocol (MBIM or QMI)
- **Switch to MBIM** button — Changes the protocol to MBIM (Mobile Broadband Interface Model)
- **Switch to QMI** button — Changes the protocol to QMI (Qualcomm MSM Interface)

Which Protocol to Use: - **MBIM** — Default. Recommended for most configurations. Better IPv6 support. - **QMI** — Alternative protocol. May provide better performance in some scenarios. Required by some carrier configurations.



Note: Changing the protocol will restart the modem connection. The router will briefly lose internet connectivity during the switch.

---

6. Cellular Modem — Module 2

Menu: MoFi Internal Modem-2

Module 2 is available on dual-module MoFi 6500 models. It provides a second independent cellular connection for redundancy or load balancing.

Module 2 has the same configuration pages and options as Module 1 (see Section 5). All sub-pages mirror the Module 1 interface:

- Configuration
- Module Status
- Signal Strength/Status
- Speed Band Lock
- Band Lock
- Advanced Signal Strength/Status
- Internet SpeedTest / FAST SpeedTest
- IMEI Restore
- TowerLock

- Module Power-Cycle
- AT Commands
- SMS (Text)
- Protocol

The key difference is that Module 2 uses a separate SIM card slot and antenna connections. It operates independently from Module 1 and can be on a different carrier.

Typical Use Cases for Dual Modules: - **Failover:** Module 2 automatically takes over if Module 1 loses connectivity - **Load Balancing:** Traffic is distributed across both modules for higher combined throughput - **Different Carriers:** Use AT&T on Module 1 and T-Mobile on Module 2 for coverage redundancy

The main difference is that Module 2 uses its own dedicated SIM card slot and antenna connections. It functions independently from Module 1 and can connect to a separate carrier if needed.

Common Dual-Module Applications

- **Automatic Failover:** Module 2 takes over automatically if Module 1 loses its connection
- **Load Balancing:** Network traffic is shared between both modules to improve overall performance and throughput
- **Multi-Carrier Redundancy:** Use different carriers, such as AT&T on Module 1 and Verizon on Module 2, for stronger coverage and backup connectivity

---

7. MoFi Business

This section covers enterprise-grade features accessible under the **Mofi Business** menu.

7.1 MoFi CloudLink

Menu: Go to **Mofi Business** → **MoFi Cloud Link** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/business/cloudlink-js

CloudLink provides a static public IP address for your router, even when using a cellular connection that does not have a public IP. This enables remote access, port forwarding, and hosting services behind cellular connections.

How CloudLink Works: CloudLink creates a VPN tunnel from your router to a MoFi datacenter. The datacenter assigns a static public IP to your tunnel. All traffic to that IP is forwarded to your router.

CloudLink provides your router with a static public IP address, even when using a cellular/starlink connection that normally does not offer a public IP. This allows you to enable remote access, port forwarding, and hosted

services over cellular networks. Most important is this IP will be the same even while using different internet connection types.

How CloudLink Works

CloudLink establishes a secure VPN tunnel between your router and a MoFi Network datacenter. The datacenter assigns a static public IP address to the tunnel, and all traffic sent to that IP is securely forwarded to your router.

Settings:

Setting	Options	Description
Enable CloudLink	Toggle ON/OFF	Activate or deactivate the CloudLink connection
Server	See server list below	Select the CloudLink datacenter closest to your location
Wireguard Server	Location provided by MoFi	WireGuard-based CloudLink server (if using WireGuard mode)

Available CloudLink Servers:

Server	Protocol	Description
us1-datacentre.mofimanage.com	PPTP	US Datacenter 1
us2-datacentre.mofimanage.com	PPTP	US Datacenter 2
us5-datacentre.mofimanage.com	SoftEther	US Datacenter 5
Additional servers	SoftEther/PPTP	Other regional datacenters
WireGuard Server	WireGuard	Modern protocol option (requires config file)
Username	Text field	Your CloudLink account username (provided by MoFi)
Password	Text field	Your CloudLink account password
Configuration File	File upload	Upload a WireGuard .conf file provided by MoFi
IP-Passthrough	Toggle OFF/ON	When ON, passes the CloudLink public IP directly to a connected LAN device
DMZ	IP address field	When set, all incoming traffic on the CloudLink IP is forwarded to this single LAN device

Server	Protocol	Description
Router GUI (Remote Access)	Toggle OFF/ON	When ON, allows access to the router's web interface from the CloudLink IP

Advanced Settings:

Setting	Options	Description
Tunnel Mode	All Traffic / Split Mode by MAC	"All Traffic" routes everything through CloudLink. "Split Mode" only routes traffic for specific devices (identified by MAC address).
Fix TTL	Toggle OFF/ON	Modify TTL values on packets going through the CloudLink tunnel
Auto Find Best MTU	Toggle	Automatically determine the optimal MTU for the tunnel
MTU	Numeric	Manual tunnel MTU (only if auto MTU is off)
Auto Calc Best MSS	Toggle	Automatically calculate MSS
Override MSS	Numeric	Manual MSS value

VPN Status: Displays the current CloudLink connection status (Connected / Disconnected).

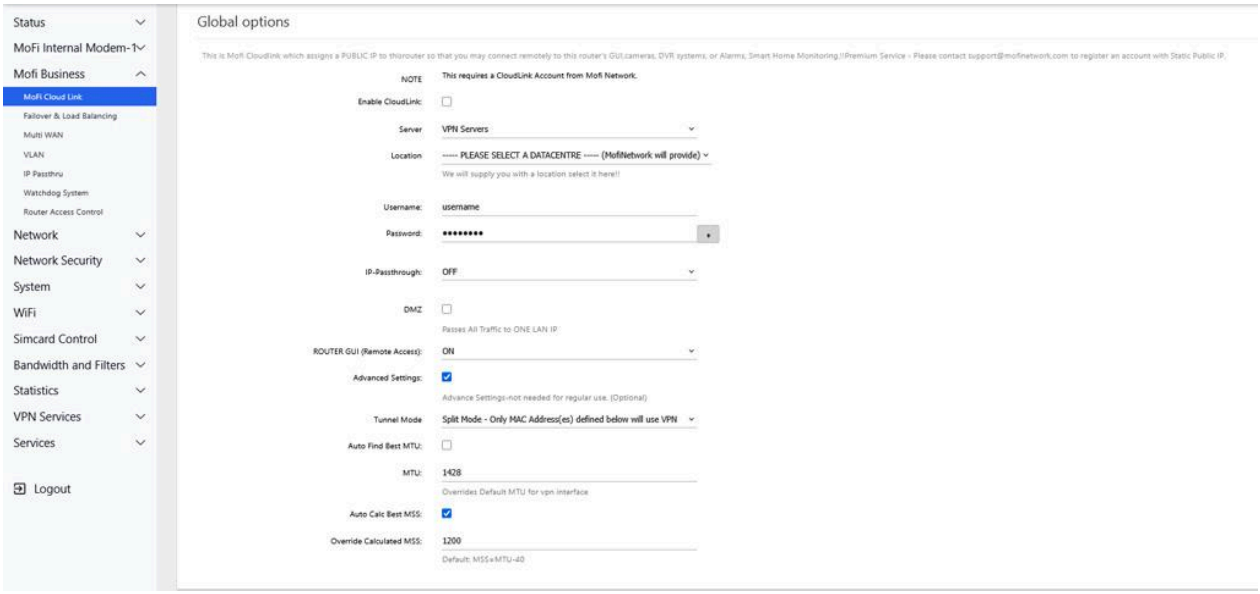
Split Mode Devices Table (only shown when Tunnel Mode = Split Mode): Add devices that should route traffic through CloudLink:

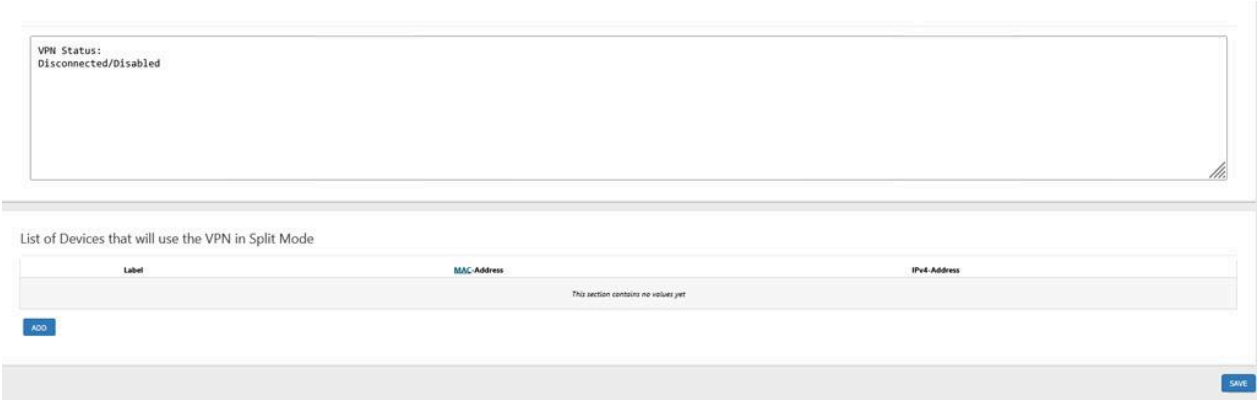
Column	Description
Label	Friendly name for the device
MAC Address	Device's MAC address
IPv4 Address	Device's current IP address

Click **Add** to add devices. Click **Save** to apply.

Step-by-Step: Setting Up CloudLink:
1. Contact MoFi to purchase a CloudLink subscription
2. Navigate to Mofi Business > MoFi Cloud Link
3. Toggle **Enable CloudLink** to ON
4. Select the nearest **Server** datacenter
5. Enter your **Username** and **Password** provided by MoFi
6. Upload the **Configuration File** if provided
7. Click **Save**
8. Wait 30-60 seconds for the tunnel to establish
9. Check the **VPN Status** — it should show "Connected"
10. Your CloudLink public IP is now active and reachable from the internet

Important: Port Forwarding with CloudLink: When forwarding ports to devices behind CloudLink, you must select **"Cloudlink/Vpn"** (not "Cellular/Wan/Repeater") as the external source in the Port Forwarding settings. CloudLink traffic arrives on the VPN firewall zone, not the WAN zone.





7.2 IP Passthrough

Menu: Go to **Mofi Business** → **IP Passthru** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/business/ippass

IP Passthrough passes the modem's public IP address directly to a single connected device, bypassing the router's NAT. The connected device receives the carrier-assigned IP as its own.

Settings:

Setting	Options	Description
Enable IP Passthrough	Checkbox	Turn IP passthrough on or off

Setting	Options	Description
Primary Connection	Built-IN MOFI Modem #1 / #2 / WAN Ethernet / USB RNDIS Tethering	Select which internet source to pass through
Current MTU	Display only	Shows the current MTU of the selected connection
IP Mode	DHCP Automatic / Static Manual	How the passthrough IP is assigned to the connected device
Static IP Address	Text field	Manual IP (only for Static Manual mode)
Primary DNS	Text field	DNS server 1 (only for Static Manual mode)
Secondary DNS	Text field	DNS server 2 (only for Static Manual mode)

Auto-Detected Settings (display only): - Gateway address - Netmask

Advanced Settings:

Setting	Options	Description
MSS	Auto / 1200 / 1436	Maximum Segment Size for the passthrough connection
Cisco Device Mode	Toggle	Enable compatibility mode for Cisco equipment
Use Carrier Netmask	Toggle	Use the netmask provided by the carrier instead of the default
TTL	Default / Linux 64 / Linux-2 65 Recommended / Linux-3 117 / Windows 128 / Cisco 255 / Other 32	Override TTL value on passthrough traffic

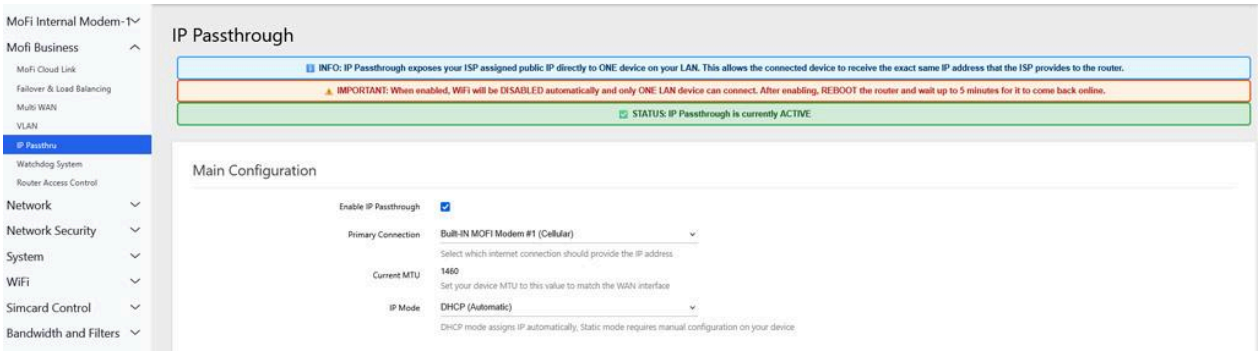
DNS Configuration:

Setting	Options	Description
DNS Selection	Use ISP Provided DNS / Use Custom DNS	Choose between carrier-provided DNS or custom DNS servers
Custom DNS Servers	Text field	Enter custom DNS server addresses (only when using Custom DNS)

Buttons: Save.

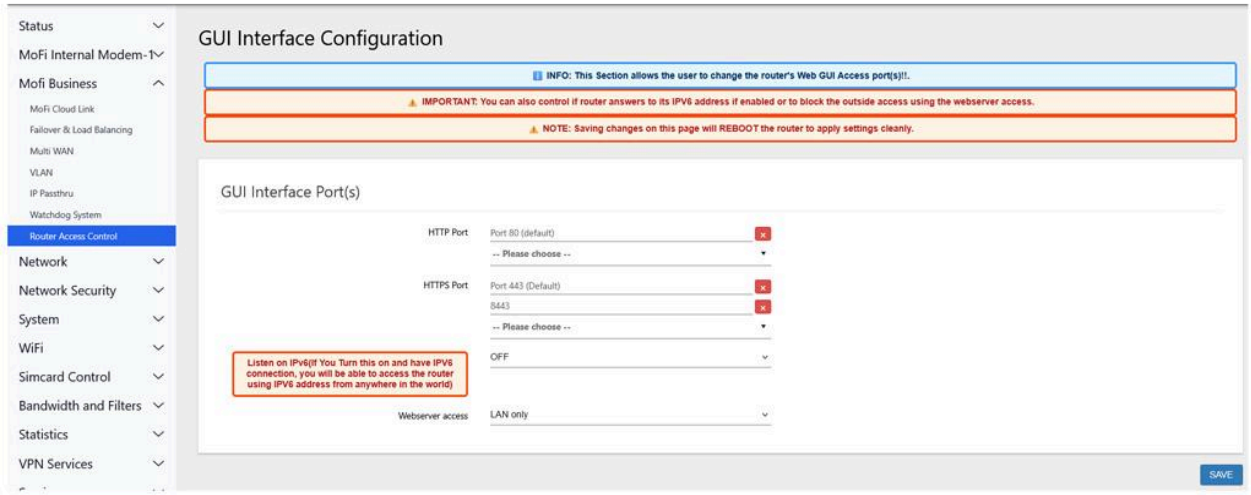
Step-by-Step: Setting Up IP Passthrough to a Firewall:

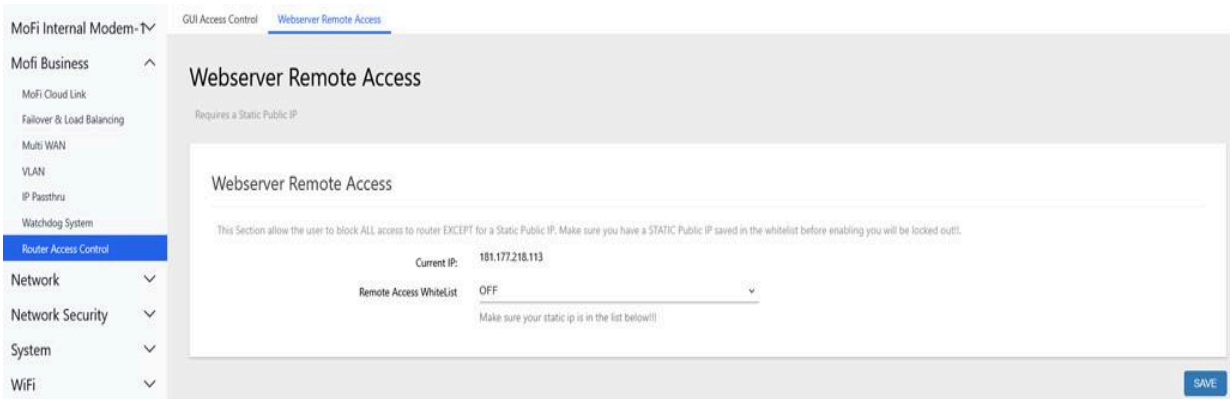
1. Navigate to Mofi Business > IP Passthru
2. Check **Enable IP Passthrough**
3. Select **Primary Connection** — choose “Built-IN MOFI Modem #1” for cellular
4. Set **IP Mode** to “DHCP Automatic”
5. Under Advanced Settings, set **TTL** to “Linux-2 65 Recommended”
6. Under DNS Configuration, choose “Use ISP Provided DNS” or enter custom DNS
7. Set **HTTP Web Port** to 8080 and **HTTPS Web Port** to 8443 (these allow remote access to the router through the passthrough IP)
8. Click **Save**
9. Connect your firewall/device to LAN port 1
10. The connected device will receive the carrier’s public IP address via DHCP
11. Access the router admin from LAN at `http://192.168.10.1` (port 80, unchanged). For remote access through the passthrough public IP, use port 8080.



Remote Access Configuration: When IP passthrough is active, the router's LAN management interface remains accessible at `http://192.168.10.1` (port 80) as normal. These settings configure *remote* access to the router through the passthrough public IP:

Setting	Description
HTTP Web Port	Remote access port for HTTP (default: 8080). Traffic to this port on the public IP is redirected to the router's port 80. Set to 0 to disable.
HTTPS Web Port	Remote access port for HTTPS (default: 8443). Traffic to this port on the public IP is redirected to the router's port 443. Set to 0 to disable.





Use Cases: - Pass a public IP directly to a firewall device (Cisco, Ubiquiti, etc.) - Allow a server to have a real public IP from the cellular carrier - Enable peer-to-peer applications that require a public IP

7.3 VLAN

Menu: Go to Mofi Business → VLAN or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/business/vlan

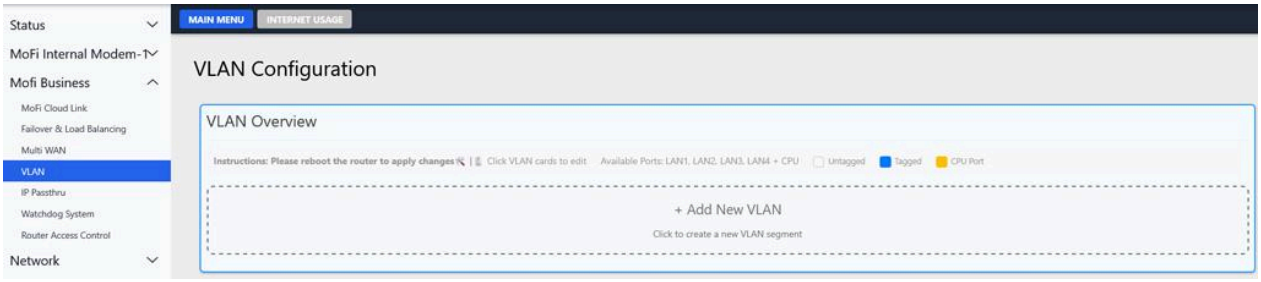
Create virtual LANs to segment your network into isolated groups. Devices on different VLANs cannot communicate with each other unless explicitly allowed.

VLAN Overview: Visual card display showing all existing VLANs. Click a card to edit its settings.

Available Physical Ports: LAN1, LAN2, LAN3, LAN4, CPU (router's internal connection)

Each VLAN card shows: - VLAN ID - VLAN Name - Assigned ports (Untagged / Tagged / CPU)

Creating a New VLAN: Click **+ Add New VLAN** to open the creation form:



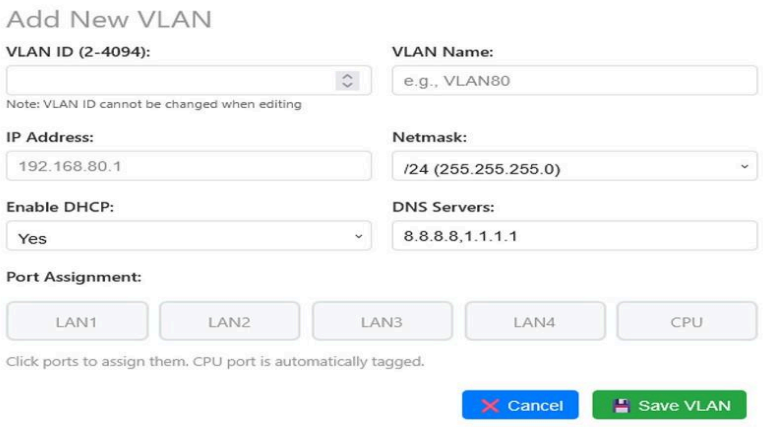
Setting	Options	Description
VLAN ID	2-4094	Unique numeric identifier for this VLAN
VLAN Name	Text field	Friendly name (e.g., "Guest", "IoT", "Cameras")

Setting	Options	Description
IP Address	Text field	The router's IP address on this VLAN (e.g., 192.168.20.1)
Netmask	/24, /23, /22	Subnet size. /24 = 254 devices, /23 = 510, /22 = 1022
Enable DHCP	Yes / No	Automatically assign IP addresses to devices on this VLAN
DNS Servers	Text field	DNS servers to push to devices on this VLAN
Port Assignment	Click LAN1-LAN4 and CPU	Assign physical ports to this VLAN

Click **Save VLAN** to create it, or **Cancel** to discard.

Step-by-Step: Creating an IoT VLAN:

1. Navigate to Mofi Business > VLAN
2. Click **+ Add New VLAN**
3. Set VLAN ID to `10`, Name to `IoT`
4. Set IP Address to `192.168.20.1`, Netmask to `/24`
5. Set Enable DHCP to `Yes`
6. Click LAN4 to assign LAN port 4 to this VLAN
7. Click **Save VLAN**
8. Devices plugged into LAN port 4 will now be on the isolated IoT VLAN (192.168.20.x)



7.4 Watchdog System

Menu: Go to **Mofi Business** → **Watchdog System** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/business/watchdog

Automatically monitor internet connectivity and take corrective action when it fails.

Settings:

Setting	Options	Description
Enable Watchdog	Toggle	Turn the watchdog on or off
Response Mode	Normal / Mission-Critical	**Normal:** Verifies the failure with a second check before taking action (reduces false positives). **Mission-Critical:** Takes immediate action on first failure detection (fastest recovery, but may trigger on brief outages).
Check Interval	Every 10 / 15 / 20 / 30 / 45 / 60 minutes	How often the watchdog pings the test servers
Primary Test Server	IP or hostname	First server to ping (default: 1.1.1.1 or 8.8.8.8)
Secondary Test Server	IP or hostname	Backup server to ping if primary is unreachable
Recovery Action	Full Reboot / Restart WAN / USB Reset / Network Reset	What to do when connectivity failure is confirmed

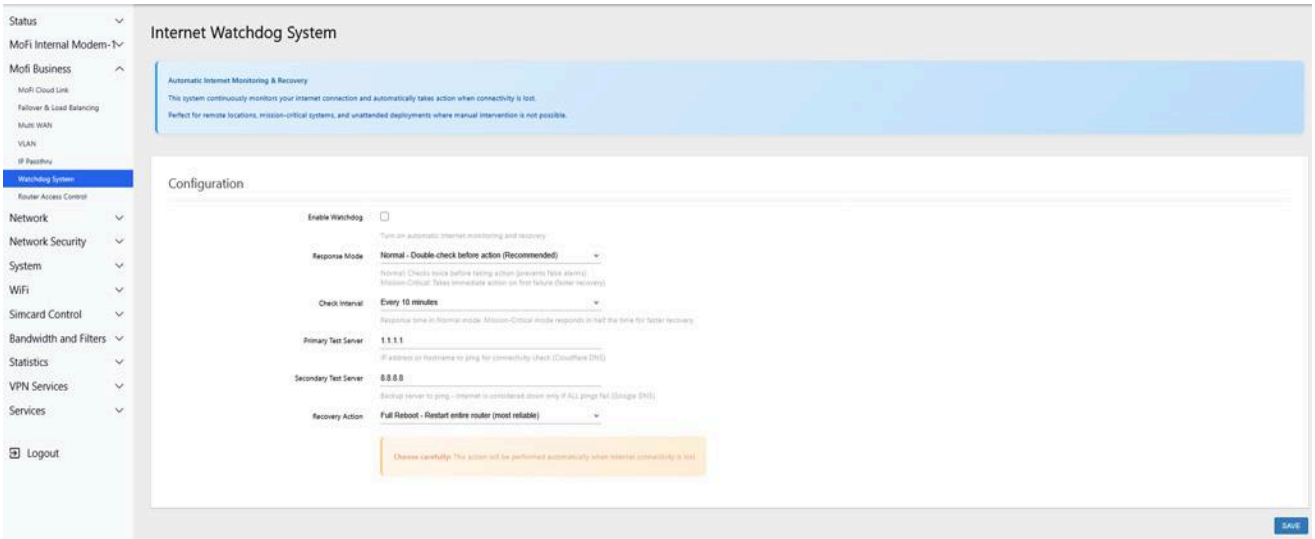
Recovery Actions Explained:

Action	Description	Severity
Full Reboot	Restarts the entire router	Most thorough but causes 90-second downtime
Restart WAN	Restarts only the WAN/cellular interfaces	Moderate — attempts to reconnect without full reboot
USB Reset	Power-cycles the cellular modems only	Minimal impact to other services
Network Reset	Restarts the network stack and firewall	Resets all network connections

Buttons: Save.

Step-by-Step: Setting Up Watchdog for Cellular Connections:
1. Navigate to Mofi Business > Watchdog System
2. Toggle **Enable Watchdog** to ON
3. Set **Response Mode** to “Normal” (recommended — verifies failure before acting)
4. Set **Check Interval** to “Every 15 minutes”
5. Set **Primary Test Server** to `1.1.1.1` (Cloudflare DNS)
6. Set **Secondary Test Server** to `8.8.8.8` (Google DNS)

7. Set **Recovery Action** to “Restart WAN” (tries to reconnect without full reboot)
8. Click **Save**
9. The watchdog will now check connectivity every 15 minutes by pinging the test servers. In Normal mode, it verifies the failure twice before taking action to prevent false alarms.



For mission-critical deployments: Set Response Mode to “Mission-Critical” and Recovery Action to “Full Reboot” for the fastest recovery (at the cost of a 90-second reboot).

7.5 Router Access Control

Menu: Go to **Mofi Business** → **Router Access Control** (also at **Network Security > GUI Access Control**) or click the link below:

http://192.168.10.1/cgi-bin/luci/admin/business/webserver

Control how the router’s web management interface is accessed.

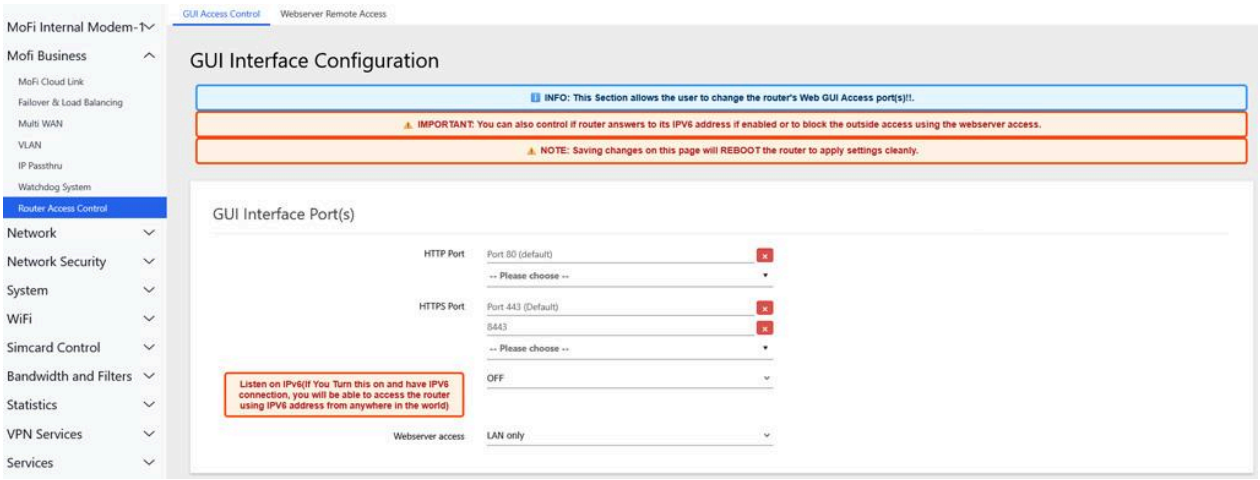
Settings:

Setting	Options	Description
HTTP Port	80 / 81 / 8080 / 3821 / 8001 / others	Port for unencrypted web access. Default: 80.
HTTPS Port	443 / 4443 / 8443 / others	Port for encrypted web access. Default: 443.
Listen on IPv6	Toggle ON/OFF	Whether the web server listens on IPv6 addresses
Web server access	LAN only / Allow access from LAN/WAN	**LAN only** (recommended): Only devices on the local network can access the router GUI.

Setting	Options	Description
		LAN/WAN: Also allows access from the WAN/cellular side (use with caution).

Buttons: Save.

Step-by-Step: Changing the Router Admin Port:
1. Navigate to Mofi Business > Router Access Control
2. Change **HTTP Port** from 80 to your desired port (e.g., 8080)
3. Change **HTTPS Port** from 443 to your desired port (e.g., 8443)
4. Keep **Web server access** set to “LAN only”
5. Click **Save**
6. After saving, access the router at `http://192.168.10.1:8080` (using your new port)



Security Recommendation: Always keep webserver access set to “LAN only” unless you specifically need remote management. If you need remote access, use CloudLink or a VPN instead of opening the GUI to the WAN.

7.6 Failover / Load Balancing

Menu: Go to **Mofi Business** → **Failover/Load Balancing** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/failover

This page has three tabs: **Failover**, **Load Balancing**, and **SIM Failover**.

Important: Only enable Failover OR Load Balancing — not both at the same time. The router will automatically disable both if you try to enable both simultaneously.

Important: Reboot the router after changing failover or load balancing settings for changes to take full effect.

Failover Tab

Automatically switch to a backup internet connection when the primary fails.

Enable Failover: Toggle ON/OFF

Primary Connection Profiles:

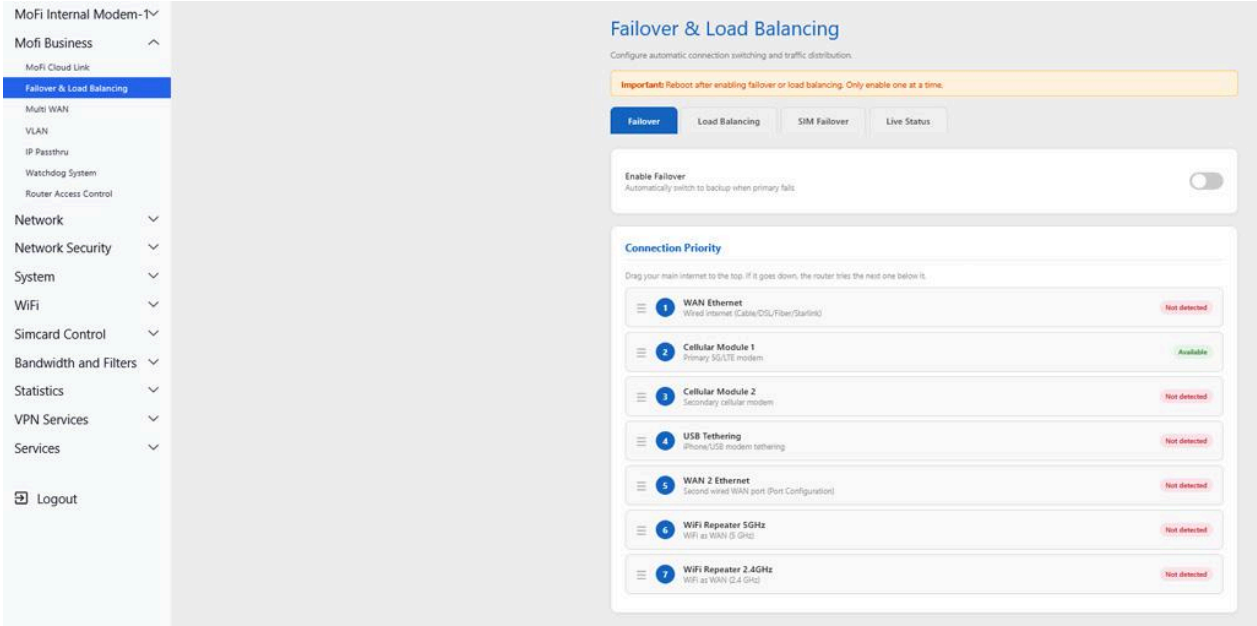
Profile	Label	Priority Order
Default	WAN ethernet (primary) → Module1 → Module2 → USB	WAN first, then cellular, then USB
Cellular Primary	Module (primary) → WAN ethernet	Cellular first, ethernet backup
Module1 Primary	Module1 → Module2 → WAN	Module 1 first, Module 2 second, WAN last
Module2 Primary	Module2 → Module1 → WAN	Module 2 first, Module 1 second, WAN last
Cellular/WiFi Primary	Module/WiFi → WAN (secondary)	Cellular and WiFi primary, WAN secondary
WiFi as WAN	5GHz → 2.4GHz → Cellular → WAN	WiFi repeater first, cellular backup, WAN last
Cellular Primary (with WiFi)	Module → WiFi 5GHz → 2.4GHz → WAN	Cellular first, WiFi repeater backup, WAN last

The router continuously monitors each connection by pinging test servers (8.8.8.8, 8.8.4.4, 208.67.222.222, 208.67.220.220). When the primary connection fails 3 consecutive checks, the router switches to the next priority connection within seconds.

Step-by-Step: Setting Up Cellular Failover with WAN Primary:
1. Navigate to Mofi Business > Failover/Load Balancing
2. Click the **Failover** tab
3. Toggle **Enable Failover** to ON
4. Select **Primary Connection**: “Default: WAN ethernet (primary) → Module1 → Module2 → USB”
5. Click **Save**
6. **Reboot the router** (required for failover changes)
7. After reboot, if the WAN ethernet loses internet, the router automatically switches to Module 1 cellular

Step-by-Step: Setting Up Cellular-Primary Failover:
1. Navigate to Mofi Business > Failover/Load Balancing
2. Click the **Failover** tab
3. Toggle **Enable Failover** to ON
4. Select **Primary Connection**: “Cellular Primary: Module (primary) → WAN ethernet”
5. Click **Save**

6. **Reboot the router**
7. The router now uses cellular as the main connection, with WAN ethernet as backup



Load Balancing Tab

Distribute traffic across multiple connections simultaneously for increased total bandwidth.

Enable Load Balancing: Toggle ON/OFF

Load Balancing Profiles:

Profile	Description
WAN + Cellular	Balance traffic between WAN ethernet and all cellular modules
WAN + Module1	Balance traffic between WAN ethernet and Module 1 only
WAN + Module2	Balance traffic between WAN ethernet and Module 2 only
WAN + WiFi Repeater	Balance between WAN and WiFi as WAN (shown only if WiFi repeater is enabled)
Cellular + WiFi Repeater	Balance between cellular and WiFi as WAN (shown only if WiFi repeater is enabled)

Weight Controls: Adjust the percentage of traffic on each connection (10%-90% in 10% increments): - **WAN Weight** — Percentage of traffic routed through WAN ethernet - **Module1 Weight** — Percentage of traffic routed through Module 1 (shown if Module 1 connected) - **Module2 Weight** — Percentage of traffic routed through Module 2 (shown if Module 2 connected) - **WiFi 2G Repeater Weight** — Percentage for 2.4 GHz WiFi repeater (shown if enabled) - **WiFi 5G Repeater Weight** — Percentage for 5 GHz WiFi repeater (shown if enabled)

Weight Controls

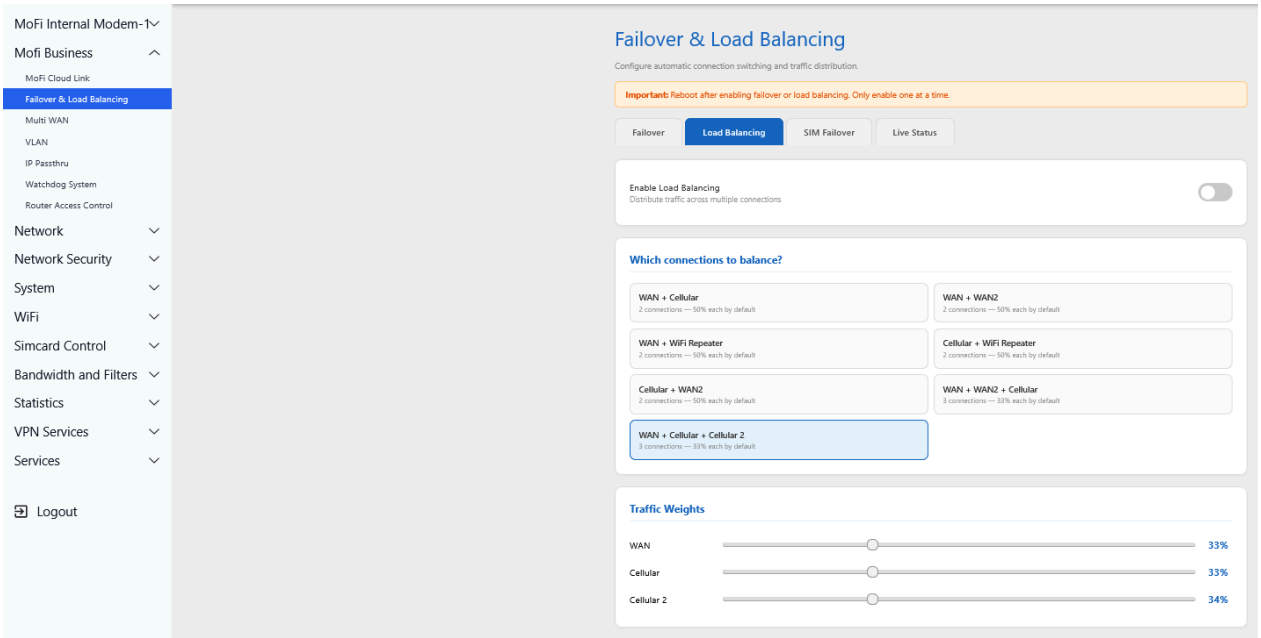
Weight controls determine how traffic is distributed across available internet connections. Each connection can be assigned a percentage from 10% to 90% in 10% increments.

Available weight settings include:

- **WAN Weight** — Percentage of traffic routed through the WAN ethernet connection
- **Module1 Weight** — Percentage of traffic routed through Module 1 (displayed when Module 1 is connected)
- **Module2 Weight** — Percentage of traffic routed through Module 2 (displayed when Module 2 is connected)
- **WiFi 2G Repeater Weight** — Percentage of traffic routed through the 2.4 GHz WiFi repeater connection (displayed when enabled)
- **WiFi 5G Repeater Weight** — Percentage of traffic routed through the 5 GHz WiFi repeater connection (displayed when enabled)

The default weight for all connections is 50%.

Step-by-Step: Setting Up Load Balancing (WAN + Cellular):
1. Navigate to Mofi Business > Failover/Load Balancing
2. Click the **Load Balancing** tab
3. Make sure **Failover is disabled** on the Failover tab first
4. Toggle **Enable Load Balancing** to ON
5. Select **Load Balancing Profile**: “WAN + Cellular: Balance between ethernet and cellular”
6. Set **WAN Weight** to 50% and **Module1 Weight** to 50% (or adjust as desired)
7. Click **Save**
8. **Reboot the router**
9. Traffic will now be distributed across both WAN and cellular connections



SIM Failover Tab

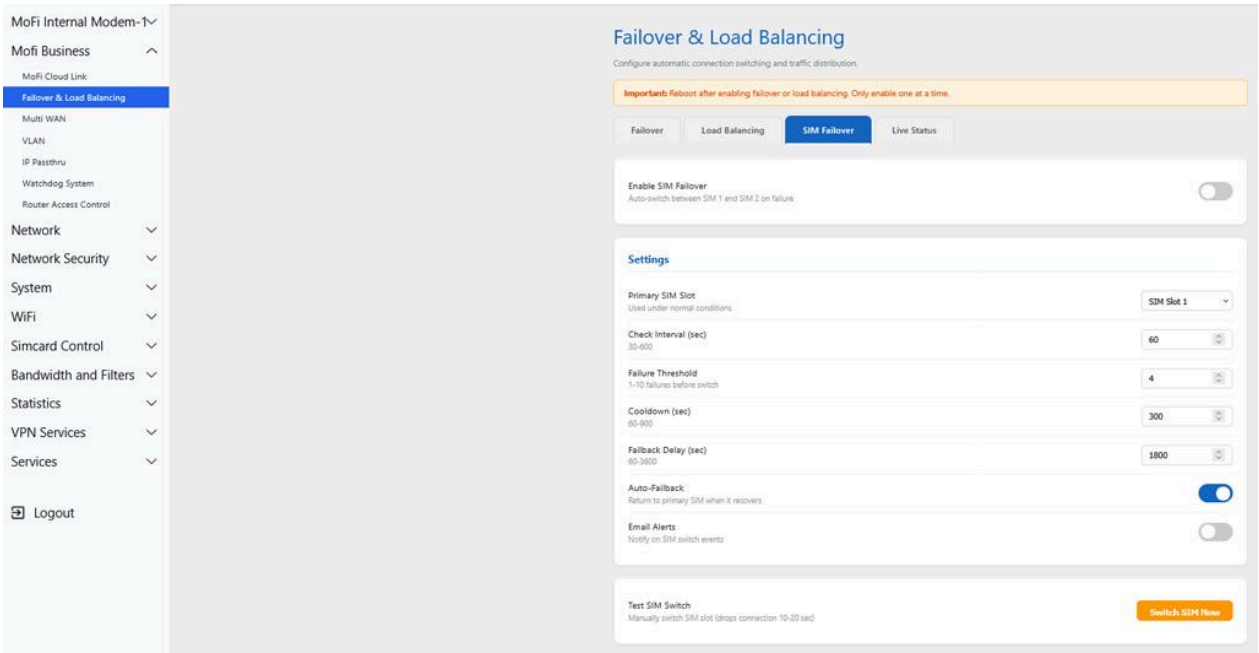
Automatically switch between SIM Slot 1 and SIM Slot 2 when the active SIM loses cellular connectivity. Requires both SIM slots to have active SIM cards.

Setting	Options	Default	Description
Enable SIM Failover	Toggle	OFF	Master enable for automatic SIM switching
Primary SIM Slot	SIM Slot 1 / SIM Slot 2	SIM Slot 1	Which SIM slot to use under normal conditions
Check Interval	30-600 seconds	60 seconds	How often to test cellular connectivity
Failure Threshold	1-10	4	Number of consecutive failures before switching SIM slots
Cooldown Time	60-900 seconds	300 seconds (5 min)	Minimum wait time after switching before checking again (prevents rapid toggling)
Enable Auto-Failback	Toggle	ON	Automatically return to the primary SIM when it recovers
Failback Delay	60-3600 seconds	1800 seconds (30 min)	How long to wait on the backup SIM before attempting to switch back to primary
Enable Email Alerts	Toggle	OFF	Send email notifications when SIM failover events occur

Test SIM Switch: Click **Switch SIM Now** to manually trigger a SIM slot switch for testing. This will briefly drop the cellular connection for 10-20 seconds while the modem switches SIM slots and reconnects.

Step-by-Step: Setting Up SIM Failover:

1. Insert active SIM cards into both SIM Slot 1 and SIM Slot 2
2. Navigate to Mofi Business > Failover/Load Balancing
3. Click the **SIM Failover** tab
4. Toggle **Enable SIM Failover** to ON
5. Set **Primary SIM Slot** to “SIM Slot 1” (your main SIM)
6. Set **Check Interval** to 60 seconds (checks connectivity every minute)
7. Set **Failure Threshold** to 4 (switches after 4 consecutive failures)
8. Set **Cooldown Time** to 300 seconds (5-minute cooldown between switches)
9. Enable **Auto-Failback** so the router returns to your primary SIM when it recovers
10. Set **Failback Delay** to 1800 seconds (wait 30 minutes before switching back)
11. Optionally enable **Email Alerts** for notifications
12. Click **Save**
13. Click **Switch SIM Now** to test that both SIMs work.



Multi Wan

Menu: Go to **Mofi Business** → **Multi Wan** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/business/dualwan

Multi WAN — Port Assignment

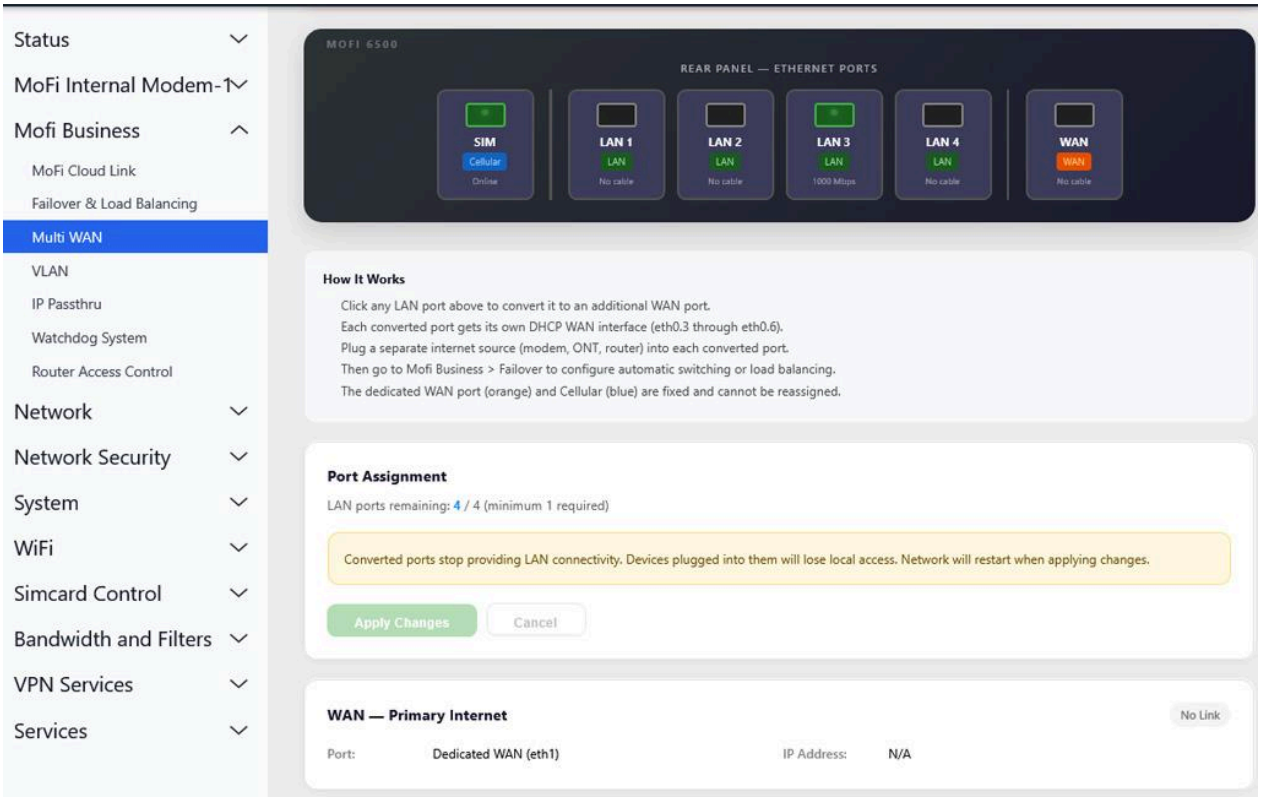
Convert up to 3 LAN ports into additional WAN ports for multiple internet connections. At least 1 LAN port must remain for local network access.

IMPORTANT — Convert FIRST, Plug Cable AFTER

Always convert the LAN port to WAN on this page BEFORE plugging in the upstream internet cable. Do NOT do it the other way around.

Right way: Click the LAN port → Apply Changes → wait for reload → then plug the cable into that port.

Why: If you plug the upstream cable into a LAN port first and the router reboots before you convert it, the GUI can become inaccessible. Convert-first avoids that risk entirely.



After Adding WAN Ports

- **Failover:** Go to Mofi Business > Failover to set automatic switching between connections.
- **Load Balancing:** Combine multiple WANs for higher total bandwidth.
- **DHCP:** Each new WAN port uses DHCP. Connect it to a device that assigns IPs (modem, ONT, router).
- **Port Forwarding:** Traffic rules using "Cellular/Wan/Repeater" source already cover all extra WAN ports.

8. Network

This section covers all pages under the **Network** menu.

8.1 Captive Portal

Menu: Go to **Network** → **Captive Portal** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/splash-js

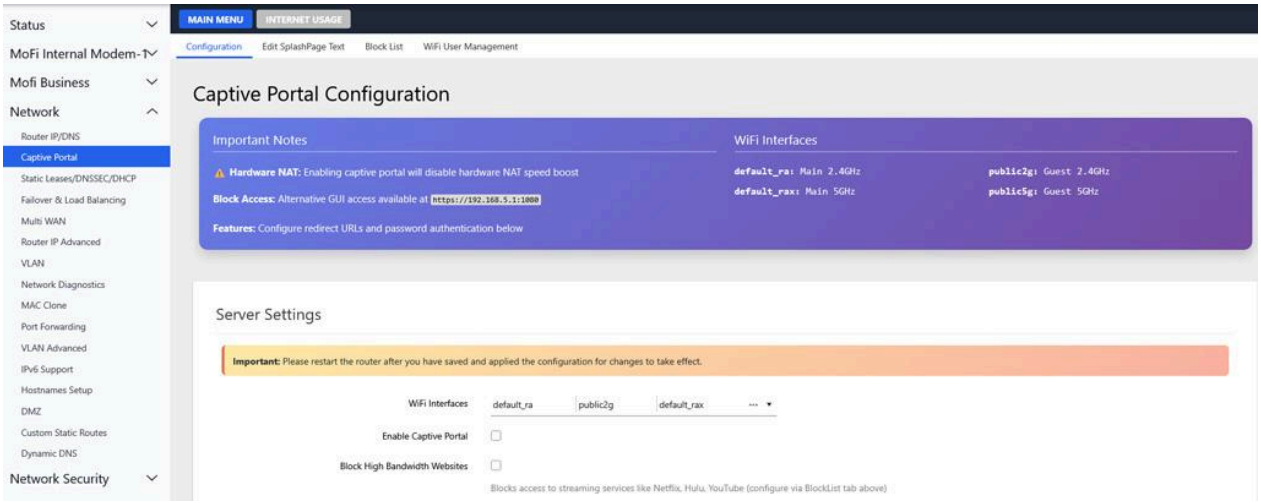
Create a guest network with a splash page that users must accept before gaining internet access (similar to hotel or airport WiFi).

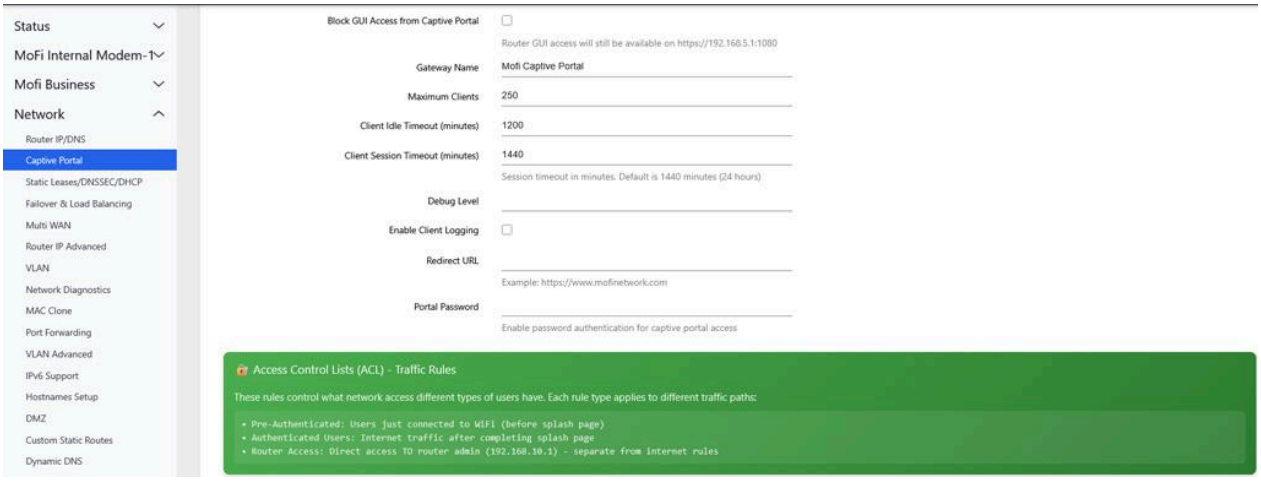
This page has four sub-tabs: **Configuration**, **Edit SplashPage Text**, **Block List**, and **WiFi User Management**.

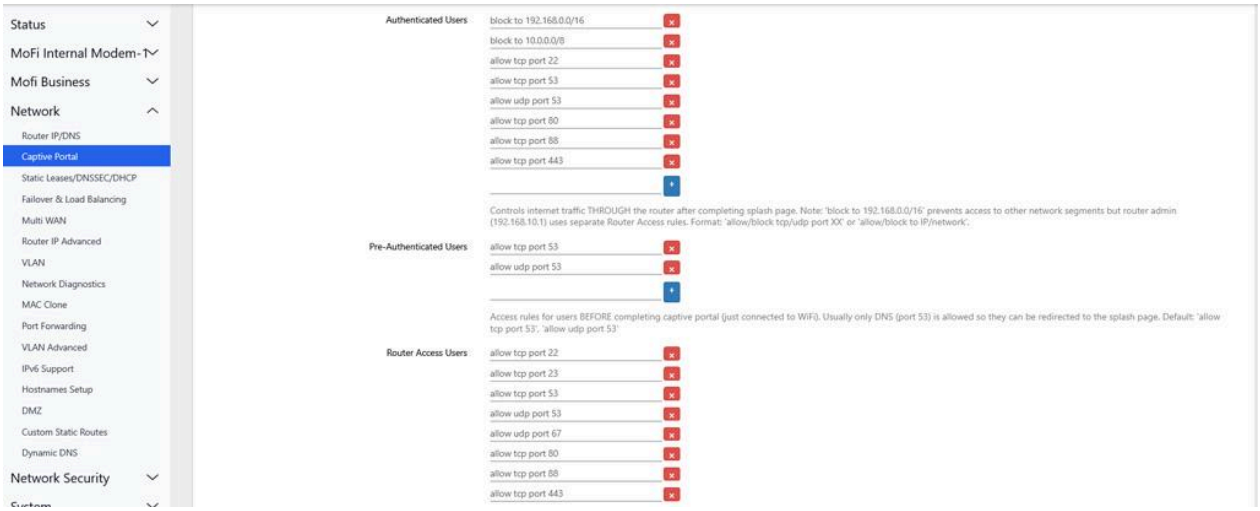
Important: You must reboot the router after saving captive portal changes for them to take effect. Enabling the captive portal will also disable hardware NAT acceleration, which may reduce maximum throughput.

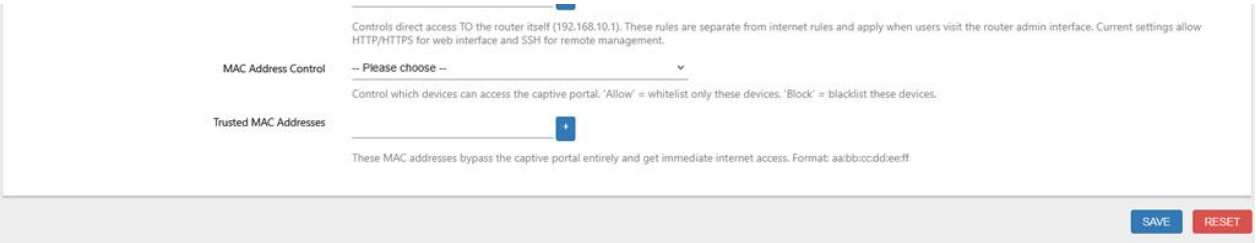
How the Captive Portal Works:
1. A guest connects to the selected WiFi network
2. The router intercepts their first web request and redirects to a splash page
3. The guest sees a welcome page with terms and an "Accept" button (or a password field if password mode is enabled)
4. After accepting (or entering the password), the guest gets internet access for the configured session duration
5. The captive portal network uses a separate subnet (192.168.5.0/24) isolated from your main LAN (192.168.10.0/24)

Step-by-Step: Setting Up a Guest Captive Portal:
1. Navigate to Network > Captive Portal
2. Select which WiFi interfaces should use the portal (e.g., "public2g Guest 2.4GHz" and "public5g Guest 5GHz")
3. Toggle **Enable Captive Portal** to ON
4. Set a **Gateway Name** (e.g., "Welcome to MyBusiness WiFi")
5. Set **Maximum Clients** (e.g., 50)
6. Set **Client Session Timeout** (e.g., 1440 minutes = 24 hours)
7. Optionally enable **Block High Bandwidth Websites** to prevent streaming
8. Optionally enable **Block GUI Access from Captive Portal** for security
9. Optionally set a **Portal Password** for password-protected access
10. Click **Save**
11. **Reboot the router** (System > Reboot) for the captive portal to take effect









Accessing the Router Admin While Captive Portal is Active: If you enabled "Block GUI Access from Captive Portal," you can still reach the router admin at: https://192.168.5.1:1080 or via any wired LAN connection at http://192.168.10.1.

Configuration Tab

WiFi Interface Selection:

Interface	Description
default_ra 2.4GHz	Main WiFi 2.4 GHz network
public2g Guest 2.4GHz	Guest WiFi 2.4 GHz network
default_rax 5GHz	Main WiFi 5 GHz network
public5g Guest 5GHz	Guest WiFi 5 GHz network

Select which WiFi interface(s) should use the captive portal.

General Settings:

Setting	Options	Description
Enable Captive Portal	Toggle	Turn the captive portal on or off
Block High Bandwidth Websites	Toggle	When ON, blocks Netflix, Hulu, YouTube, and other streaming sites for captive portal users
Block GUI Access from Captive Portal	Toggle	When ON, prevents captive portal users from accessing the router's admin interface
Gateway Name	Text field	The name displayed on the splash page
Maximum Clients	Numeric	Maximum number of simultaneous captive portal users
Client Idle Timeout	Minutes	Disconnect idle clients after this many minutes
Client Session Timeout	Minutes	Maximum session length before requiring re-authentication
Debug Level	Numeric	Logging verbosity (higher = more verbose)
Enable Client Logging	Toggle	Log all captive portal client connections
Redirect URL	URL	After authentication, redirect users to this URL (leave blank for no redirect)

Password Authentication:

Setting	Options	Description
Enable password authentication	Toggle	Require a password to pass through the splash page
Portal Password	Text field	The password users must enter

Access Control Lists (ACLs):

- **Authenticated Users** — Rules for users who have passed through the splash page. Add allow/block rules by IP or MAC address.
- **Pre-Authenticated Users** — Rules for users who haven't yet authenticated. Controls what resources they can access before login.
- **Router Access Users** — Rules for users who can access the router's management interface through the captive portal.

MAC Address Control:

Setting	Options	Description
MAC Filter Mode	Allow / Block	"Allow" = only listed MACs can use captive portal. "Block" = listed MACs are denied.
Allowed MAC Addresses	List	Devices that are always allowed
Blocked MAC Addresses	List	Devices that are always blocked
Trusted MAC Addresses	List	Devices that bypass the captive portal entirely (no splash page shown)

Edit SplashPage Text Tab

Customize the HTML content of the splash page that users see before gaining internet access.

Block List Tab

Manage lists of blocked websites, domains, or IP addresses for captive portal users.

WiFi User Management Tab

View and manage currently connected captive portal users. Disconnect users or view their session details.

8.2 Router IP / DNS

Menu: Go t**o Network** → **Router IP/DNS o**r click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/routeripjs

Change the router's local IP address, subnet, and DNS settings.

Network Interface Table (display only): Shows all network interfaces with their MAC address, IPv4 address, and traffic statistics: - br-lan (LAN bridge) - eth0 (WAN physical) - eth1 (LAN physical) - module1 (cellular) - ra0 (WiFi 2.4 GHz) - rax0 (WiFi 5 GHz)

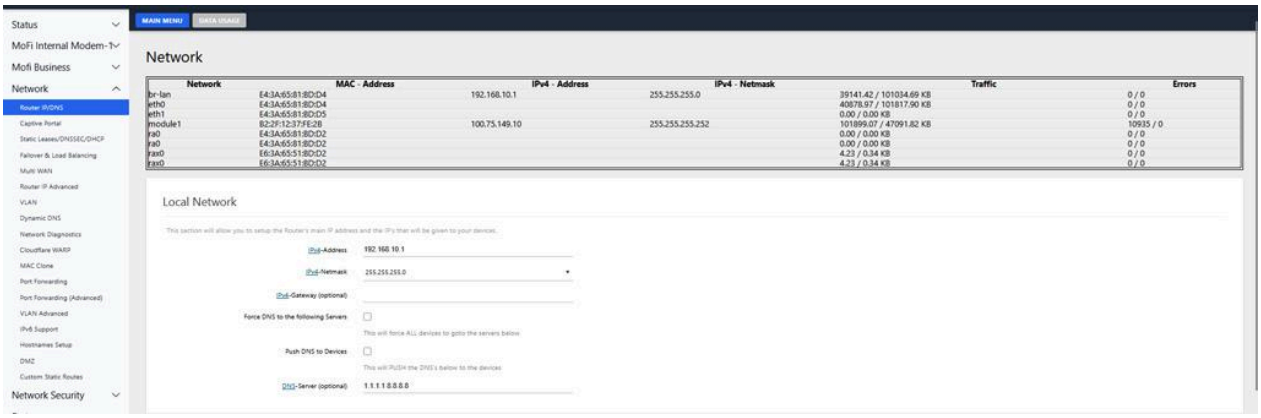
Local Network Settings:

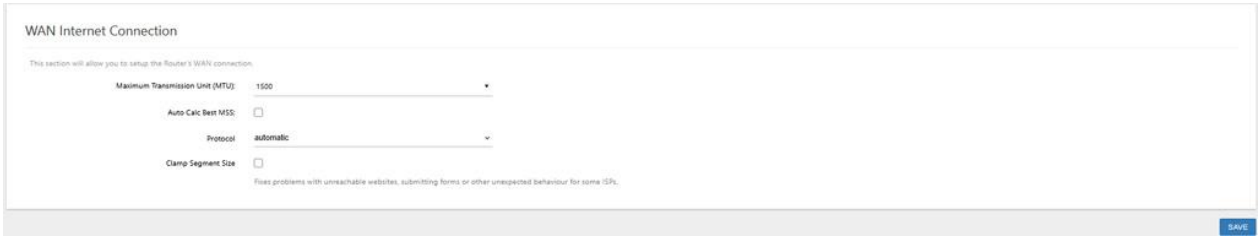
Setting	Options	Description
IPv4 Address	IP address	The router's LAN IP address. Default: 192.168.10.1. All your LAN devices use this as their gateway.
IPv4 Netmask	Dropdown (255.255.255.0, etc.)	Subnet mask. Default: 255.255.255.0 (/24 = 254 devices).
IPv4 Gateway	IP address (optional)	Only needed in special routing scenarios. Leave blank for normal operation.
Force DNS to following Servers	Toggle	When ON, forces all DNS queries from LAN devices through the specified DNS server instead of letting devices use their own DNS.
Push DNS to Devices	Toggle	Send DNS server information to devices via DHCP.
DNS Server	IP address (optional)	Custom DNS server address to push to clients.

WAN Internet Connection Settings:

Setting	Options	Description
MTU	1500 / 1492 / 1472 / 1428 / others	Maximum Transmission Unit for the WAN interface. 1500 is standard for ethernet; 1492 for PPPoE.
Auto Calc Best MSS	Toggle	Automatically calculate the Maximum Segment Size
Override Calculated MSS	Numeric	Manually set MSS value
Protocol	disabled / manual / automatic	How the WAN port obtains its IP. "automatic" = DHCP. "manual" = static IP.
IPv4 Address	IP address	Static WAN IP (manual mode only)
IPv4 Netmask	Subnet mask	Static netmask (manual mode only)
IPv4 Gateway	IP address	Upstream gateway (manual mode only)
DNS-Server	IP address	DNS for WAN (manual mode only)
Username / Password	Text fields	Credentials for PPPoE connections
Clamp Segment Size	Toggle	Enable TCP MSS clamping
Auto reconnect	Toggle	Automatically reconnect WAN if disconnected

Setting	Options	Description
Disconnect when idle	Seconds	Drop WAN connection after this many seconds of inactivity (0 = never)
PPTP-Server	Text field	PPTP server address (if using PPTP as WAN protocol)





Buttons: Save.

Warning: Changing the router's LAN IP address will disconnect your browser. You will need to reconnect to the new IP address.

8.3 Static Leases / DNSSEC / DHCP

Menu: Go to **Network** → **Static Leases/DNSSEC/DHCP** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/dhcp

Configure the DHCP server, set static IP assignments for specific devices, and manage DNS settings.

This page has multiple tabs: **General Settings**, **Static Leases**, **Resolv and Hosts Files**, **TFTP Settings**, **Advanced Settings**.

Note: The **Resolv and Hosts Files** tab manages custom DNS resolution files. The **TFTP Settings** tab configures a TFTP server for network booting (PXE). These are advanced tabs rarely needed for standard operation.

Static Leases Tab

Assign fixed IP addresses to specific devices so they always get the same IP when they connect.

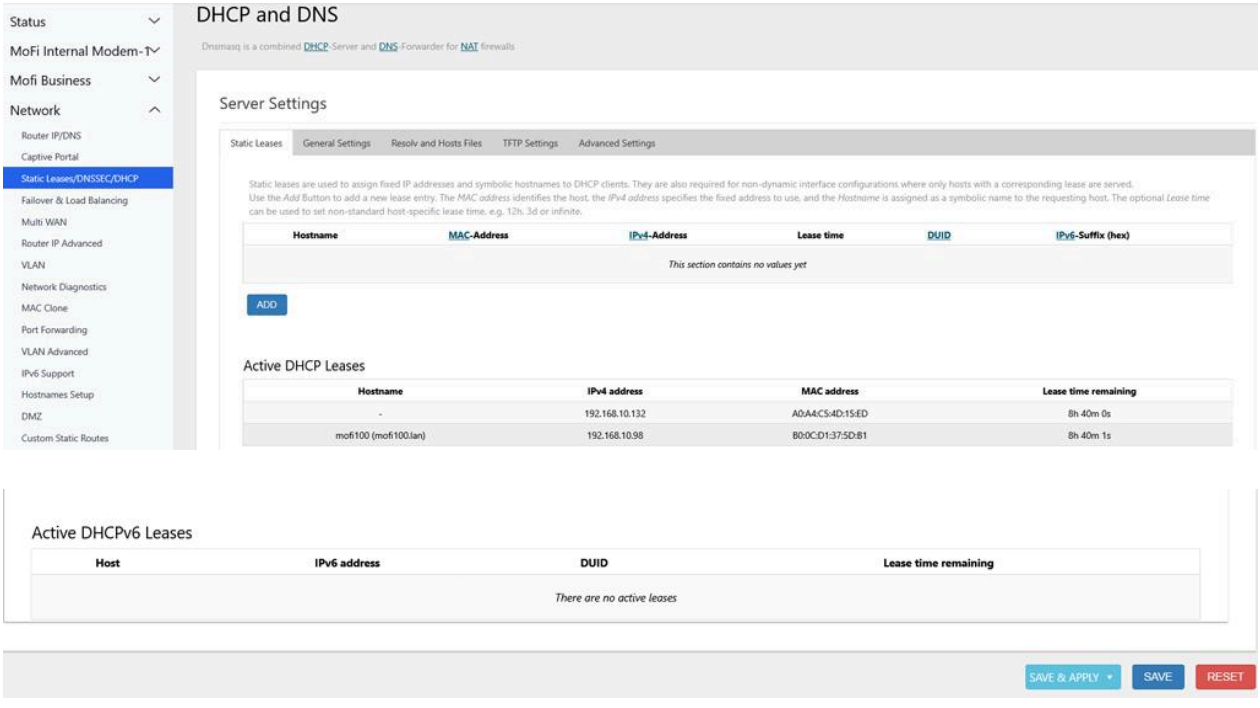
Static Lease Table:

Column	Description
Hostname	Device's network name
MAC Address	Device's hardware address (format: AA:BB:CC:DD:EE:FF)
IPv4 Address	The fixed IP to assign
Lease time	How long the lease is valid
DUID	DHCPv6 device identifier (optional)
IPv6 Suffix	IPv6 address suffix (optional)

Click **Add** to create a new static lease.

Step-by-Step: Assigning a Static IP to a Device:

1. Navigate to Network > Static Leases/DNSSEC/DHCP
2. Click the **Static Leases** tab
3. Look at the **Active DHCP Leases** table at the bottom to find your device's current MAC and hostname
4. Click **Add** at the top of the Static Leases table
5. Enter the **Hostname** (e.g., "SecurityCamera")
6. Enter the **MAC Address** (e.g., AA:BB:CC:DD:EE:FF — copy from active leases)
7. Enter the **IPv4 Address** you want to assign (e.g., 192.168.10.100)
8. Click **Save & Apply**
9. The device will receive this IP address every time it connects



Active DHCP Leases (display only): Shows all devices that currently have a DHCP lease: - Hostname, IPv4 address, MAC address, lease time remaining

Active DHCPv6 Leases (display only): Shows active IPv6 leases.

General Settings Tab

Setting	Description
Domain required	Don't forward DNS requests without a domain part
Authoritative	Make DHCP server authoritative on this network
Local server	Local DNS suffix (e.g., /lan/)
Local domain	Domain name for the local network
Log queries	Write DNS queries to the system log
DNS forwardings	Forward specific domains to custom DNS servers
Addresses	Override DNS responses for specific domains (e.g., block domains by returning 0.0.0.0)
Rebind protection	Reject DNS responses containing private IP ranges from upstream DNS
Allow localhost	Allow DNS rebind responses for localhost (127.0.0.0/8)
Domain whitelist	Domains exempt from rebind protection
Local Service Only	Only respond to DNS queries from local network
Non-wildcard	Only resolve hostnames in /etc/hosts that have a domain part
Listen interfaces	Only listen for DHCP/DNS on selected interfaces
Exclude interfaces	Don't listen on these interfaces
Use /etc/ethers	Read static DHCP lease entries from /etc/ethers
Leasefile	Path to store DHCP lease database file

Advanced Settings Tab

Setting	Description
Suppress logging	Disable DNS query logging to reduce log volume
Allocate IP sequentially	Assign IPs in sequential order instead of random
Filter private	Filter useless/private DNS results from upstream
Localise queries	Return DNS results based on the requesting interface subnet
DNSSEC	Enable DNS Security Extensions for validated DNS responses
DNSSEC check unsigned	Reject DNS responses that are not DNSSEC-signed
Expand hosts	Add the local domain to hostnames in /etc/hosts
No negative cache	Don't cache failed DNS lookups
Additional servers file	Path to extra dnsmasq configuration
Strict order	Query DNS servers in the order listed (don't try all simultaneously)
All Servers	Query all DNS servers simultaneously and use the first reply

Setting	Description
Bogus NX Domain Override	List of IPs to ignore in “not found” responses from upstream DNS
DNS server port / query port	Custom port numbers for DNS
Max DHCP leases	Maximum number of simultaneous DHCP leases
Max EDNS0 packet size	Maximum size for EDNS0 UDP packets
Max concurrent queries	Maximum DNS queries processed simultaneously
DNS query cache size	Number of cached DNS query results

8.4 Router IP Advanced

Menu: Go to **Network** → **Router IP Advanced** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/network

Full LuCI network interface editor for advanced users. Shows all network interfaces: - **br-lan** — LAN bridge (combines all LAN ports and WiFi) - **wan** — WAN ethernet interface - **wan6** — WAN IPv6 interface - **module1** — Cellular module 1 - **module2** — Cellular module 2 - **vpn** — VPN/CloudLink interface

For each interface, you can configure: protocol, IPv4/IPv6 addresses, gateway, DNS servers, MTU, MAC address override, and advanced options.

Advanced Network Interfaces

This section provides the full LuCI network interface editor for advanced network configuration and management.

Available Interfaces

The following network interfaces are displayed:

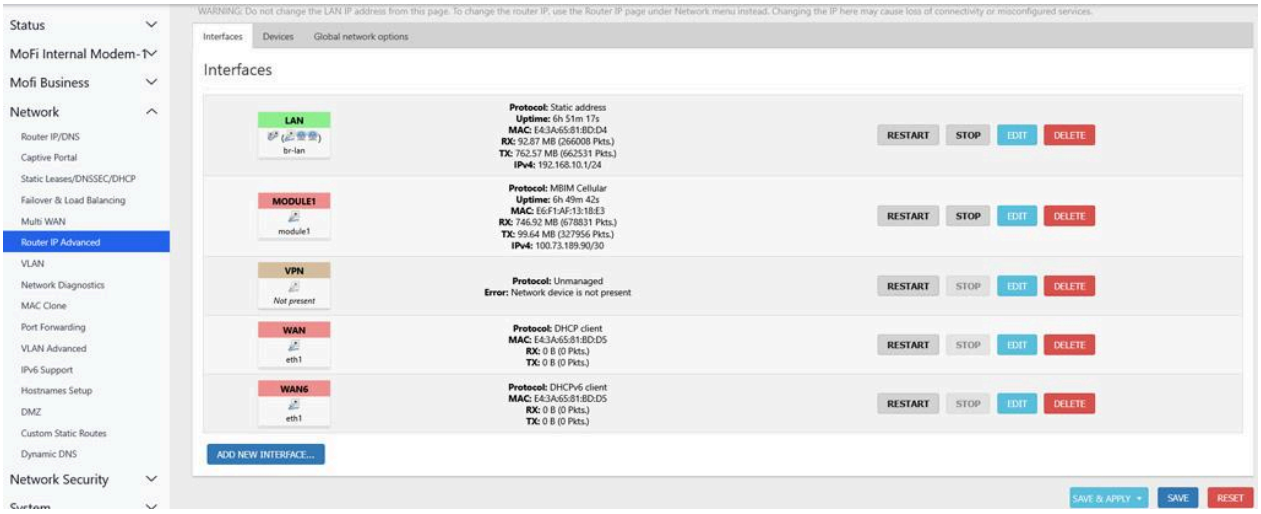
- **br-lan** — LAN bridge combining all LAN ethernet ports and WiFi networks
- **wan** — Primary WAN ethernet interface
- **wan6** — WAN IPv6 interface
- **module1** — Cellular Modem 1 interface
- **module2** — Cellular Modem 2 interface
- **vpn** — VPN or CloudLink interface

Interface Configuration Options

Each interface includes advanced configuration settings such as:

- Protocol selection
- IPv4 and IPv6 address settings

- Gateway configuration
- DNS server configuration
- MTU adjustment
- MAC address override
- Additional advanced networking options (CHATGPT)



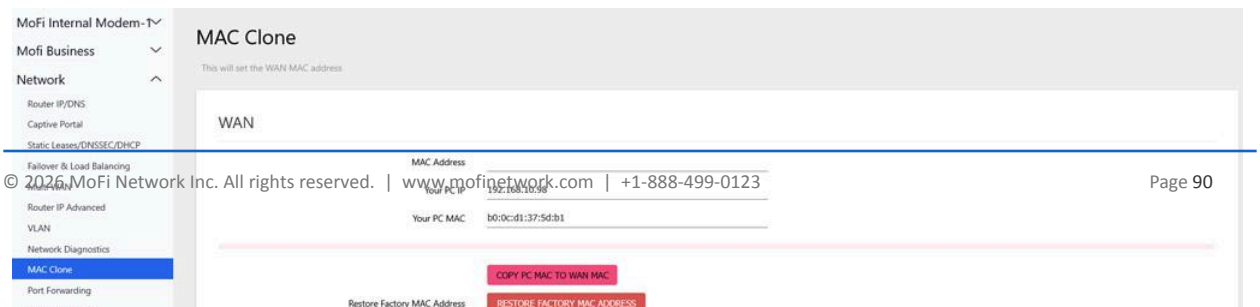
Note: This is an advanced page. Most users should use the simpler Router IP/DNS page instead.

8.5 MAC Clone

Menu: Go to **Network** → **MAC Clone** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/macclone

Change the WAN port's MAC address. Some ISPs lock service to specific MAC addresses; this feature lets you copy your computer's MAC to the router.

Setting	Description
WAN MAC Address	Enter a custom MAC address for the WAN port
Your PC IP	Auto-detected IP of the computer accessing this page (click to copy)
Your PC MAC	Auto-detected MAC of the computer accessing this page (click to copy to WAN MAC field)



Button: Restore Factory MAC Address — resets the WAN MAC to the original hardware address.

8.6 Port Filtering

Menu: Network > Port Filtering **URL:** `/cgi-bin/luci/admin/network/pfiltering`

Whitelist mode: block ALL incoming traffic except on specified ports. This is a simple but powerful security tool.

Setting	Options	Description
Enable Port Filtering (Whitelist Mode)	Toggle	When ON, ALL incoming ports are blocked except those listed below

Allowed Ports Table:

Column	Description
Service Name	Friendly name (e.g., “Web”, “HTTPS”)
Port Number	The port to allow (e.g., 22, 443, 8080)
Protocol	TCP+UDP / TCP only / UDP only

Quick-Add Reference for Common Ports: - HTTP: 80 - HTTPS: 443 - Alt-HTTP: 8080 - FTP: 21 - WireGuard: 51820 (standard) or 6677 (MoFi default) - OpenVPN: 1194 - RDP: 3389

Click **Add** to add a new port rule. Click **Save** to apply.

Step-by-Step: Allowing Only Web and VPN Traffic:
1. Navigate to Network > Port Filtering
2. Toggle **Enable Port Filtering (Whitelist Mode)** to ON
3. Click **Add** and enter: Service Name “HTTP”, Port “80”, Protocol “TCP+UDP”
4. Click **Add** and enter: Service Name “HTTPS”, Port “443”, Protocol “TCP+UDP”
5. Click **Add** and enter: Service Name “DNS”, Port “53”, Protocol “TCP+UDP”
6. Click **Add** and enter: Service Name “WireGuard”, Port “6677” (or your WireGuard listen port), Protocol “UDP only”
7. Click **Save**
8. Now only web browsing, DNS, and WireGuard VPN traffic is allowed — all other ports are blocked

CONFIRM WE TOOK THIS OUT AND THEN REMOVE FROM THE MANUAL

8.7 Port Forwarding

Menu: Go to **Network** → **Port Forwarding** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/portfw-js

Forward incoming traffic on specific ports to devices on your local network. Required for hosting services, accessing security cameras remotely, gaming servers, etc.

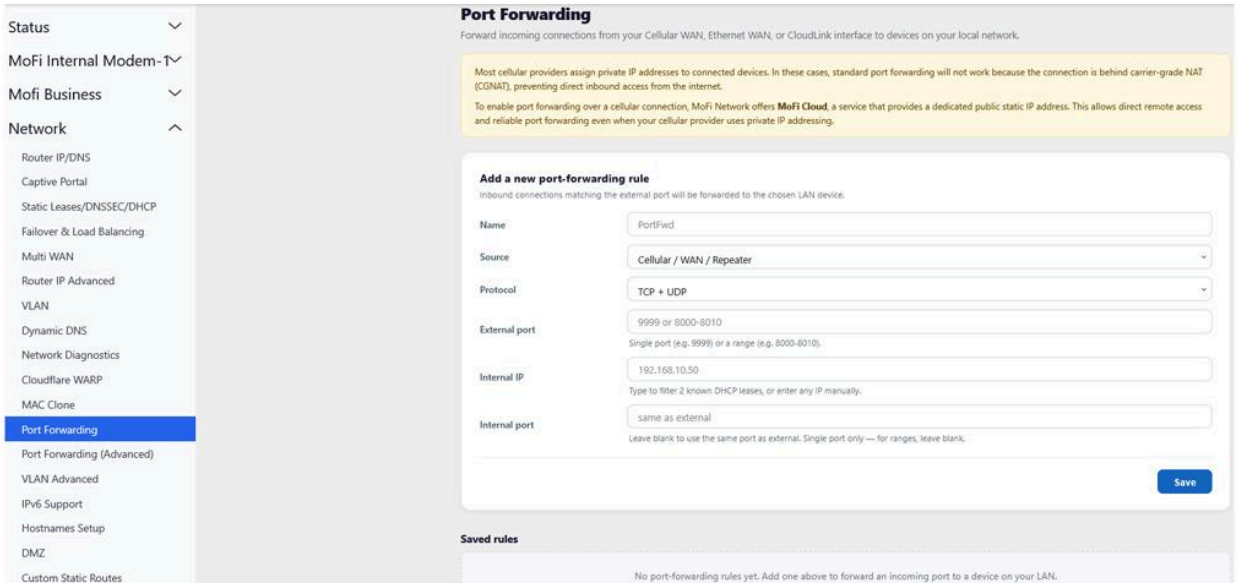
Settings per Rule:

Field	Description
Name	Descriptive name for this rule (e.g., “Security Camera”, “Game Server”)
Select External Source	Which WAN interface receives the traffic: **Cellular/Wan/Repeater** (for traffic from the internet via cellular, WAN, or WiFi repeater) or **Cloudlink/Vpn** (for traffic arriving via CloudLink tunnel)
Protocol	TCP / UDP / TCP+UDP
External port	The port number visible from the internet
Internal IP address	The LAN device to forward traffic to
Internal port	The port on the LAN device (leave blank to use same as external)

Click **Add** to create the rule. Click **Save** to apply.

Step-by-Step: Forward Port 8080 to a Security Camera at 192.168.10.100:

1. Navigate to Network > Port Forwarding
2. Enter Name: “Security Camera”
3. External Source: “Cellular/Wan/Repeater”
4. Protocol: TCP+UDP
5. External port: 8080
6. Internal IP: 192.168.10.100
7. Internal port: 8080
8. Click **Add**, then **Save**



8.8 QoS (Quality of Service)

Menu: Network > QOS Simple **URL:** `/cgi-bin/luci/admin/network/qos-simple`

Prioritize network traffic to ensure smooth performance for important applications.

- **Mode selector:** Radio buttons for Disabled or enabled QoS modes
- **Active Interface:** Shows which WAN interface QoS is applied to
- **Mode display:** Shows the current QoS mode (e.g., “Simple — All Equal”)

Click **Save** to apply.

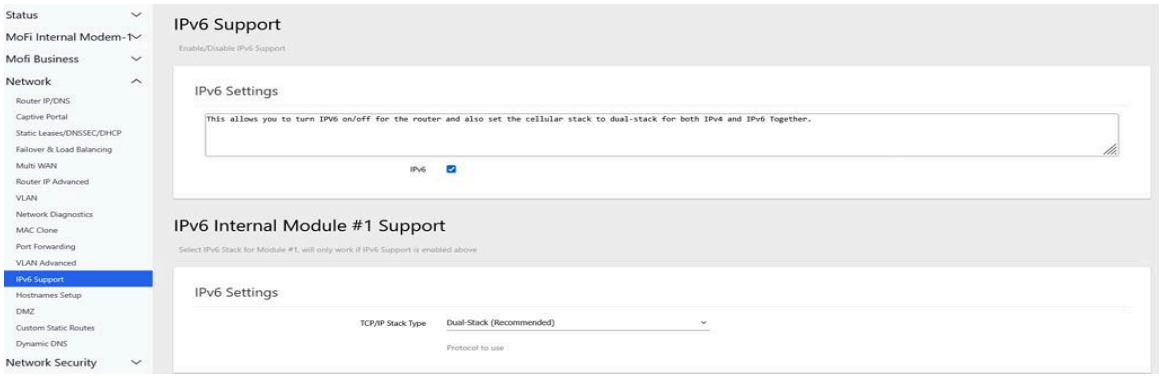
This was removed from the GUI

8.9 IPv6 Support

Menu: Go to **Network** → **IPv6 Support** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/IPV6

Enable or disable IPv6 networking.

Setting	Options	Description
IPv6	Toggle ON/OFF	Master IPv6 enable/disable
IPv6 Internal Module #1 Support	IPv4 / Dual-Stack Recommended / IPv6	TCP/IP stack type for the cellular connection. “Dual-Stack Recommended” enables both



Click **Save** to apply. The router may need to reboot for IPv6 changes to take effect.

8.10 Hostnames Setup

Menu: Go to **Network** → **Hostnames Setup** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/hosts

Create custom hostname-to-IP mappings. These work like a local DNS override — when any device on your network tries to reach the hostname, the router resolves it to the configured IP.

Host Entries Table:

Column	Description
Hostname	The domain name to resolve (e.g., myserver.local)
IP Address	The IP to return for that hostname

Default entry: `mofilogin.com` → `192.168.10.1` (allows accessing the router by typing “mofilogin.com” in any browser)

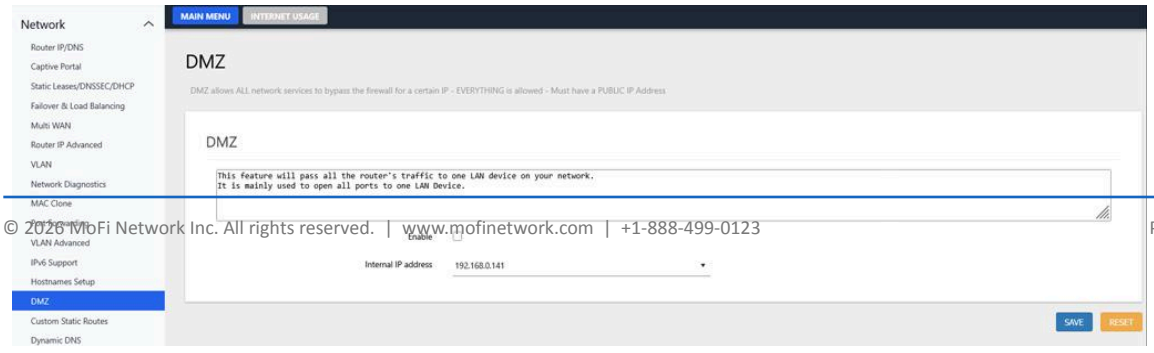
Click **Add** to create new entries. Click **Save & Apply** to activate.

8.11 DMZ

Menu: Go to **Network** → **DMZ** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/DMZ

Forward ALL incoming traffic to a single device on your network. DMZ stands for “Demilitarized Zone.”

Setting	Options	Description
Enable	Checkbox	Turn DMZ on or off
Internal IP address	Dropdown of connected devices	Select the device to receive all incoming traffic



Click **Save** to apply.

Warning: DMZ exposes the target device to all internet traffic. Ensure the device has its own firewall and security measures. Do not DMZ devices that don't need it.

Step-by-Step: Setting Up DMZ for a Gaming Console:
1. First, assign a static IP to your console (Network > Static Leases — see Section 8.3)
2. Navigate to Network > DMZ
3. Check **Enable**
4. Select your gaming console from the **Internal IP address** dropdown (or type its static IP)
5. Click **Save**
6. All incoming internet traffic is now forwarded to your console — all ports are open

Step-by-Step: Disabling DMZ:
1. Navigate to Network > DMZ
2. Uncheck **Enable**
3. Click **Save**

Use Cases: - Gaming consoles that need all ports open - Security DVR/NVR systems - Business servers behind the router

---

8.12 Custom Static Routes

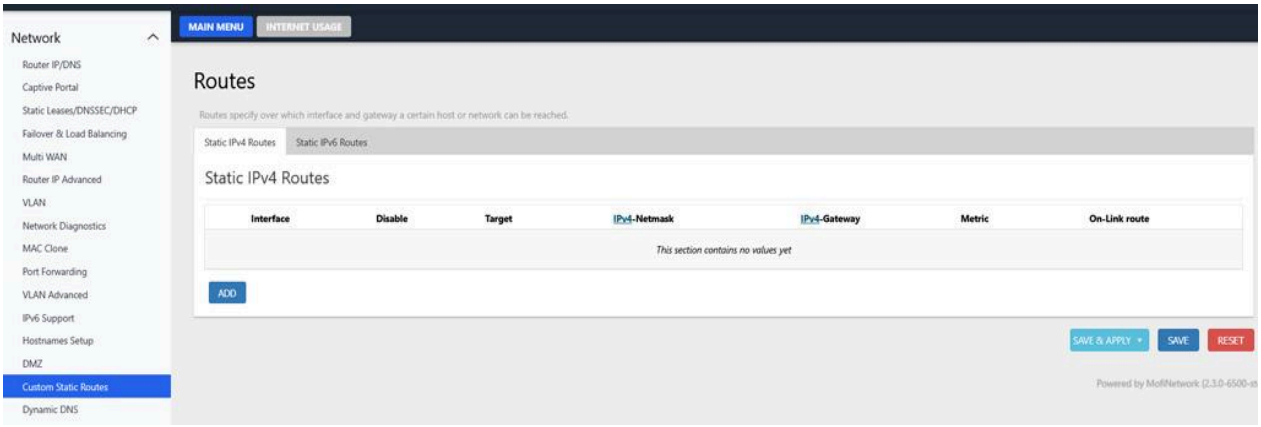
Menu: Go to **Network** → **Custom Static Routes** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/routes

Add custom routing rules to direct specific traffic through specific network interfaces or gateways.

Static IPv4 Routes Table:

Column	Description
Interface	Which network interface to use for this route
Disable	Toggle to temporarily disable this route
Target	Destination network (e.g., 10.0.0.0)
Netmask	Destination subnet mask (e.g., 255.255.255.0)
Gateway	Next-hop IP address
Metric	Route priority (lower = preferred)
On-Link route	Whether the gateway is directly connected

Static IPv6 Routes Table: Same structure but for IPv6 addresses.



Click **Add** to create new routes. Click **Save & Apply** to activate.

8.13 Dynamic DNS

Menu: Go to **Network** → **Dynamic DNS** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/ddns-js

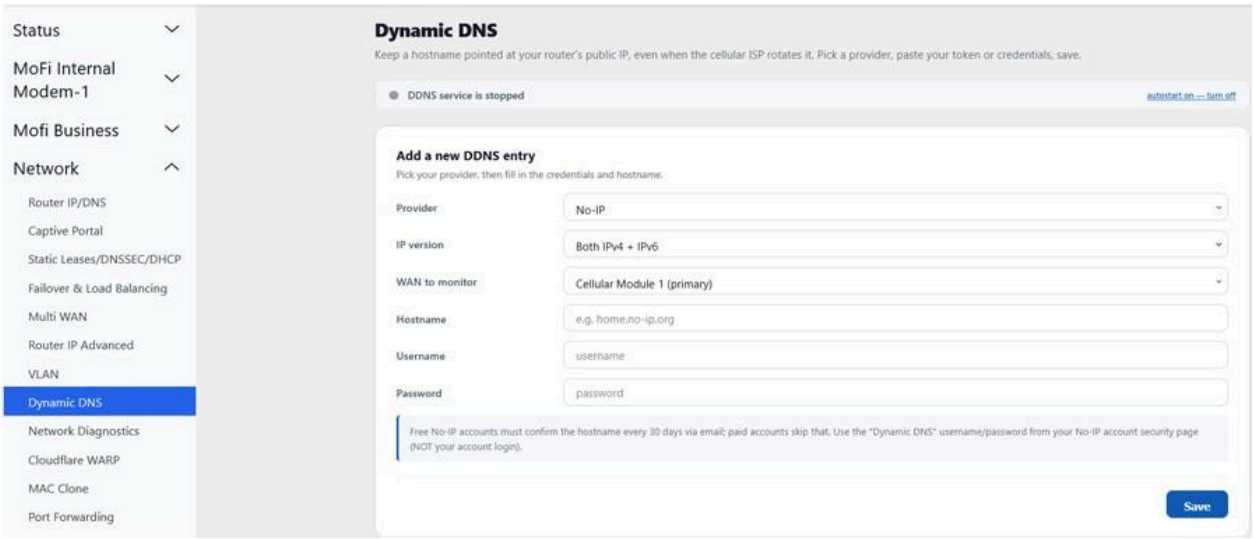
Configure a dynamic DNS service to access your router with a hostname (e.g., myrouter.duckdns.org) instead of a changing IP address.

Information Tab: - DynDNS version and state information - Available services list

Services Table: Shows configured DDNS services with: - Status (running/stopped) - Service name - Lookup hostname - Registered IP - Enable/disable toggle - Last and next update times - Start/Stop/Reload/Edit/Delete buttons

Global Settings: - Date format, directories, logging options - Use cURL toggle - CA certificates path

Click **Add new services** to configure a new Dynamic DNS provider.



Supported DDNS Providers: DuckDNS, No-IP, DynDNS, FreeDNS, Cloudflare, and many more.

Dynamic DNS (DDNS)

Dynamic DNS allows you to connect to your router using a hostname, such as `myrouter.duckdns.org`, instead of relying on a public IP address that may change over time.

Information Section

The information tab displays:

- DDNS software version and current status
- Available Dynamic DNS service providers

Configured Services

The services table lists all configured DDNS entries and includes:

- Service status (running or stopped)
- Provider/service name
- Hostname being updated
- Current registered public IP address
- Enable or disable toggle
- Last update timestamp
- Next scheduled update time
- Management controls:
    - Start

- Stop
- Reload
- Edit
- Delete

Global Configuration Options

System-wide DDNS settings include:

- Date and time formatting
- Directory and storage paths
- Logging configuration
- Optional **Use cURL** setting
- CA certificate path configuration

Adding a New DDNS Service

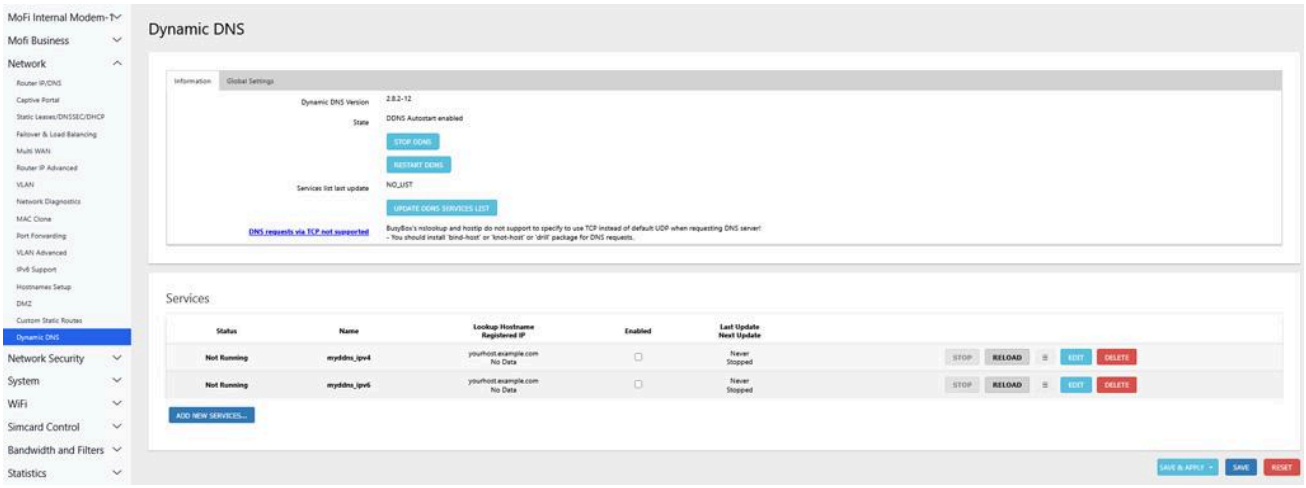
Use the **Add new services** button to configure a new Dynamic DNS provider.

Supported Providers

The router supports many Dynamic DNS services, including:

- DuckDNS
- No-IP
- DynDNS
- FreeDNS
- Cloudflare
- and many other compatible DDNS providers

Step-by-Step: Setting Up DuckDNS Dynamic DNS:
1. Go to https://www.duckdns.org and create a free account
2. Create a subdomain (e.g., “mymofi.duckdns.org”) and note your token
3. On the router, navigate to Network > Dynamic DNS
4. Click **Add new services**
5. Enter a name (e.g., “DuckDNS”)
6. Select “duckdns.org” as the DDNS provider
7. Enter your domain: “mymofi” (without .duckdns.org)
8. Enter your DuckDNS token as the password
9. Set the lookup hostname to “mymofi.duckdns.org”
10. Enable service 11. Click **Save & Apply** 12. You can now reach your router at mymofi.duckdns.org (if you have a public IP)



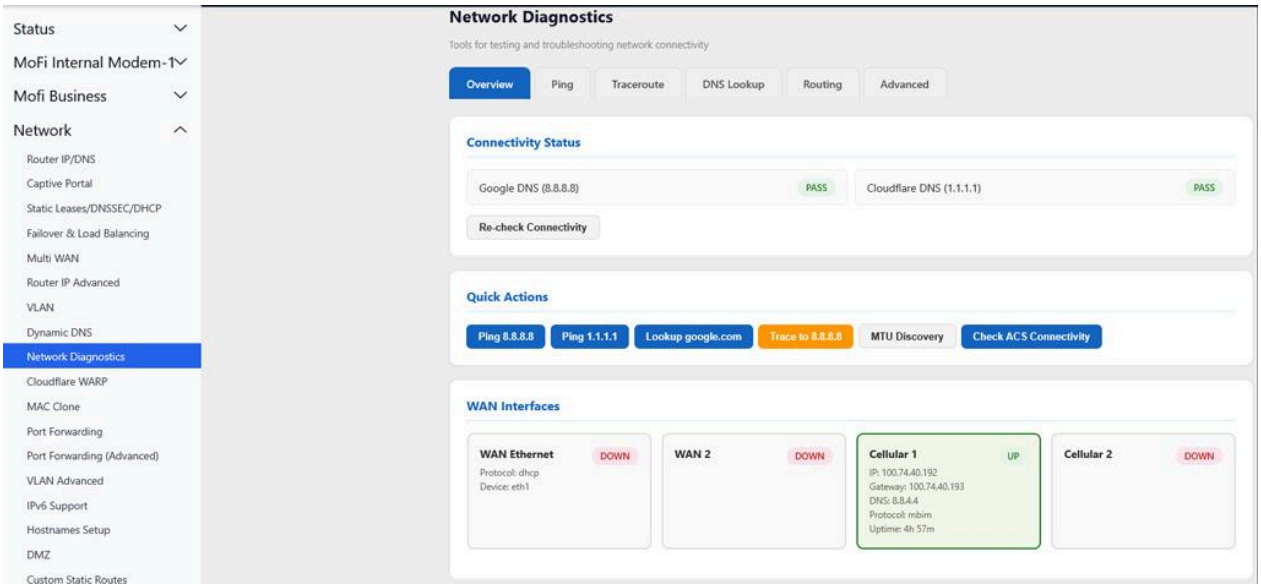
8.14 Diagnostics

Menu: Go to **Network** → **Network Diagnostics** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/ddns-js

Built-in network diagnostic tools:

Tool	Description
IPv4 Ping	Send ICMP echo requests to test connectivity to a specific IP or hostname
IPv6 Ping	Same as above but using IPv6
IPv4 Traceroute	Trace the network path to a destination, showing each hop
IPv6 Traceroute	Same as above but using IPv6

For each tool: enter the target address/hostname and click the Run button.

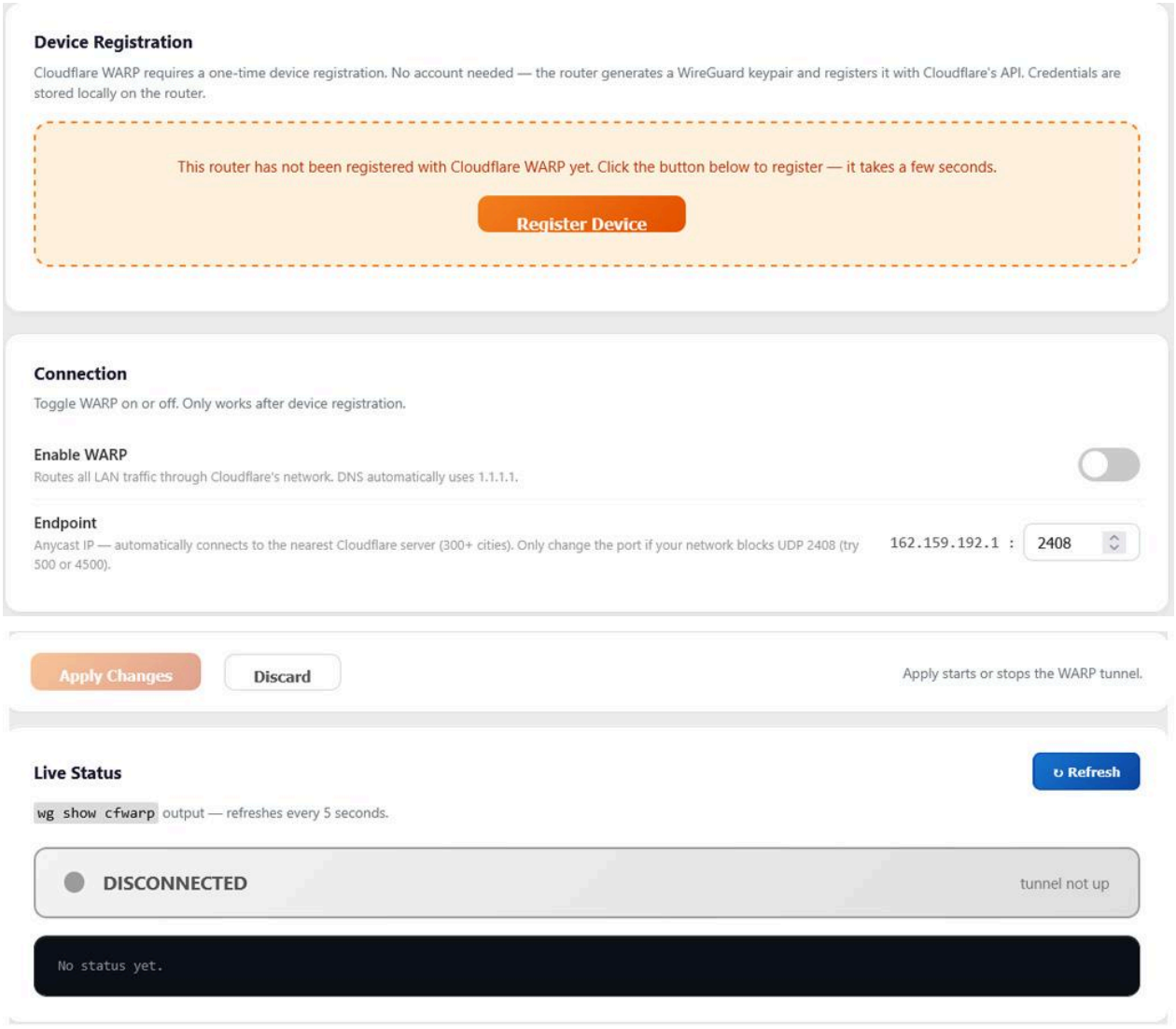


Cloudflare WARP

Menu: Go to **Network** → **Cloudflare WARP** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/cloudflare-warp-js

Cloudflare WARP

Cloudflare WARP encrypts and routes all your internet traffic through Cloudflare's global network using WireGuard. **Free, no account required, no data caps.** One-click registration, then toggle on.



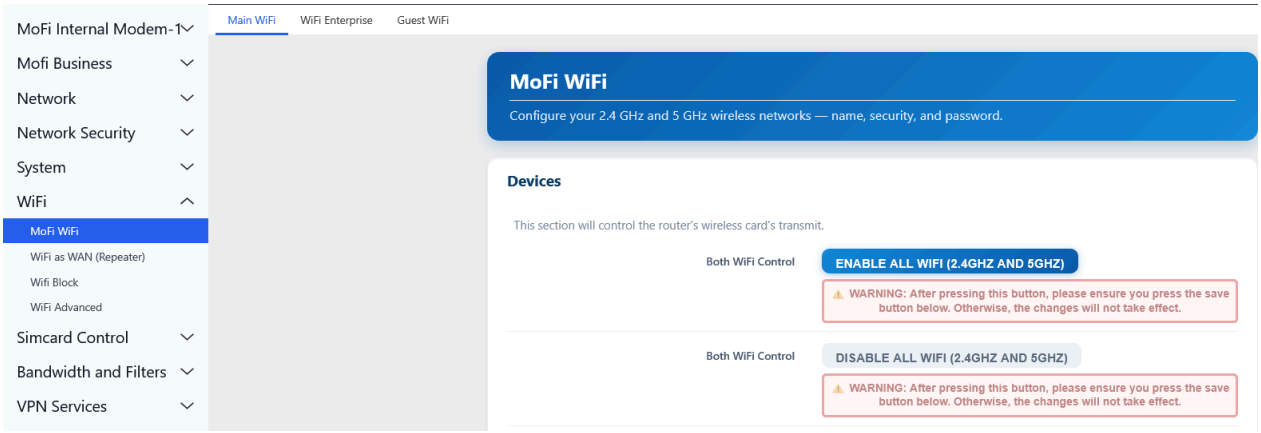
9. WiFi

This section covers all pages under the **WiFi** menu.

9.1 MoFi WiFi

Menu: Go to **WiFi** → **MoFi WiFi** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/wireless/mofi-wifi

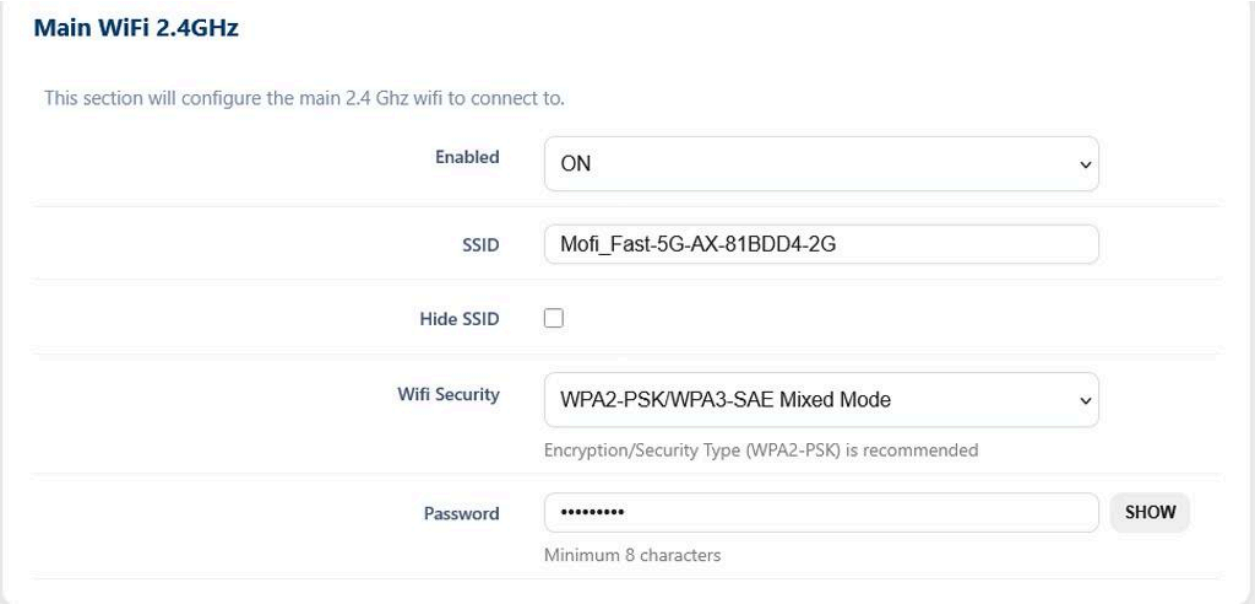
This page has two sub-tabs: **Main WiFi** and **Guest WiFi**.



Main WiFi Tab

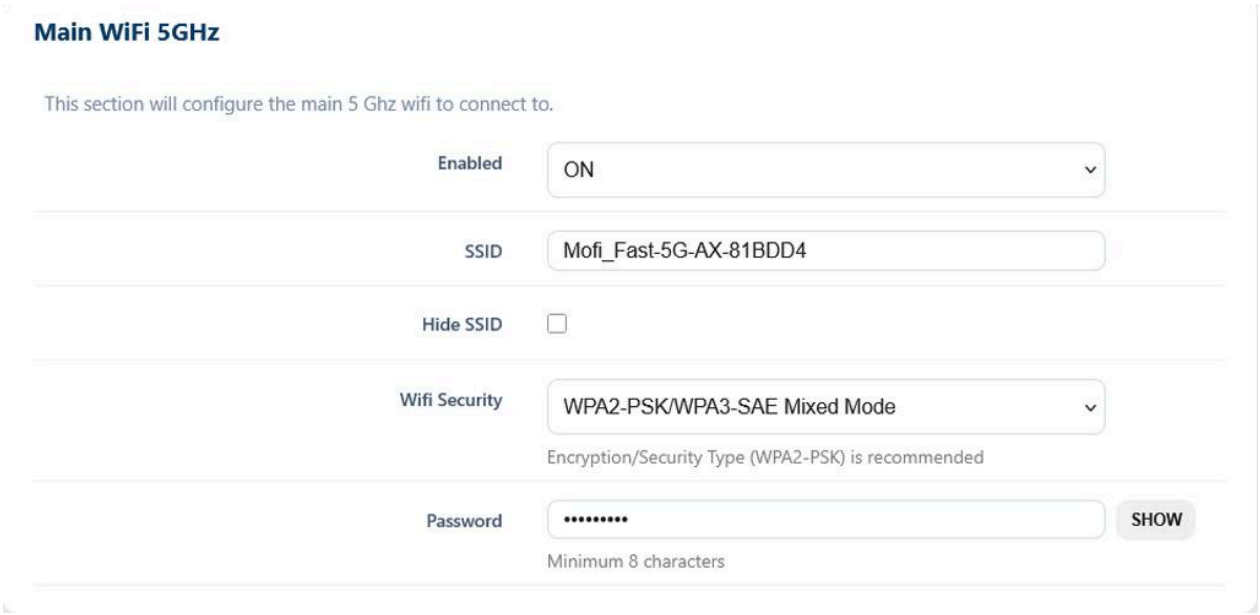
Quick Controls: - **Enable ALL WiFi** button — Turns on both 2.4 GHz and 5 GHz radios - **Disable ALL WiFi** button — Turns off all WiFi (router becomes wired-only)

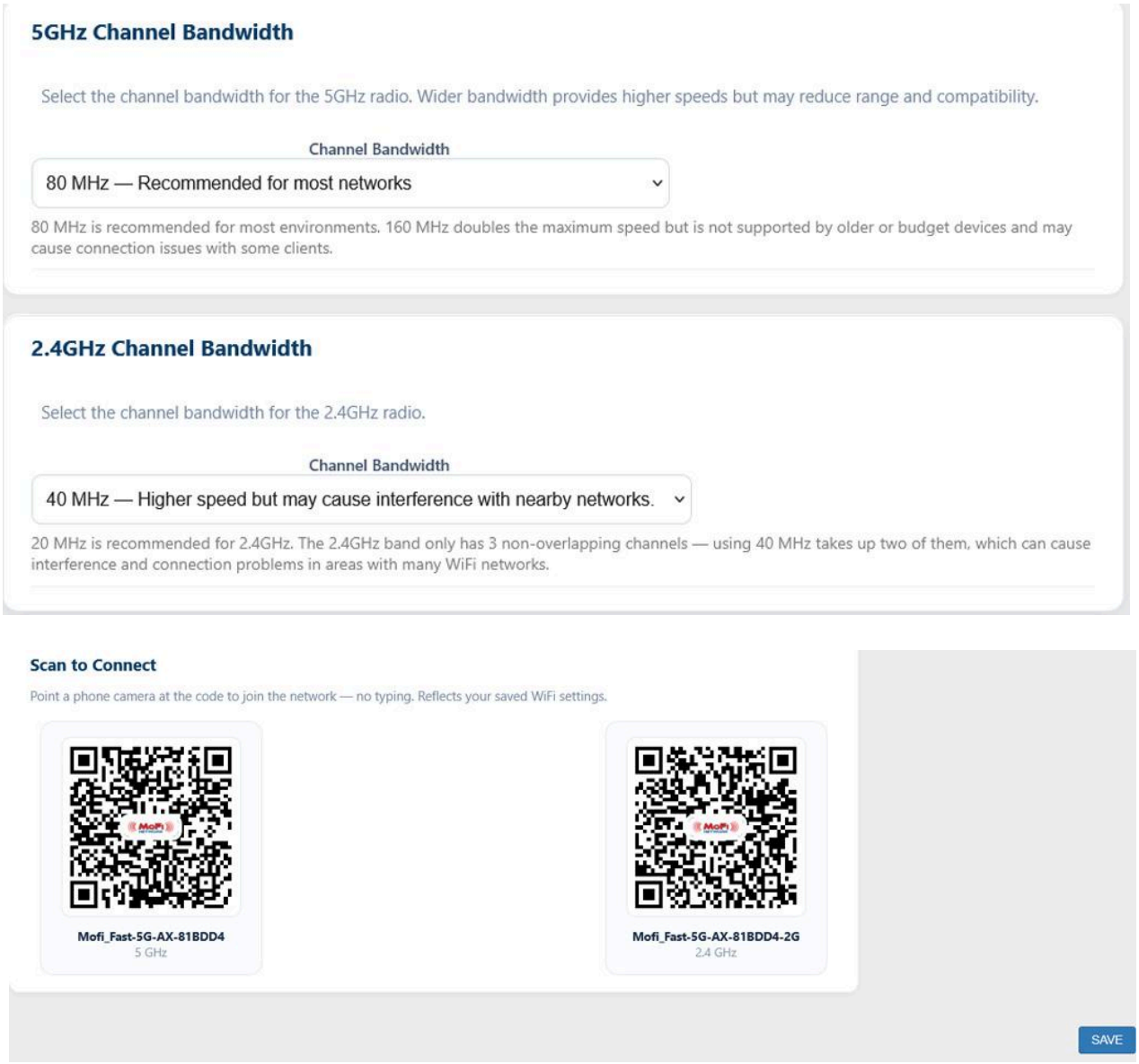
Main WiFi 2.4 GHz Settings:



Setting	Options	Description
Enabled	Toggle ON/OFF	Enable or disable the 2.4 GHz radio
SSID	Text (up to 32 chars)	Your 2.4 GHz WiFi network name
Hide SSID	Toggle	When ON, the network won't appear in WiFi scans. Devices must manually enter the network name to connect.
WiFi Security	No Encryption / WPA-PSK / WPA2-PSK / WPA-PSK/WPA2-PSK Mixed Mode	Encryption type for the network. WPA2-PSK is recommended.
Cipher	Force AES / Force TKIP / Force TKIP and CCMP	Encryption cipher. AES is recommended and most secure.
Password	Text (8-63 chars)	WiFi password

Main WiFi 5 GHz Settings: Same fields as 2.4 GHz above, but for the 5 GHz radio.



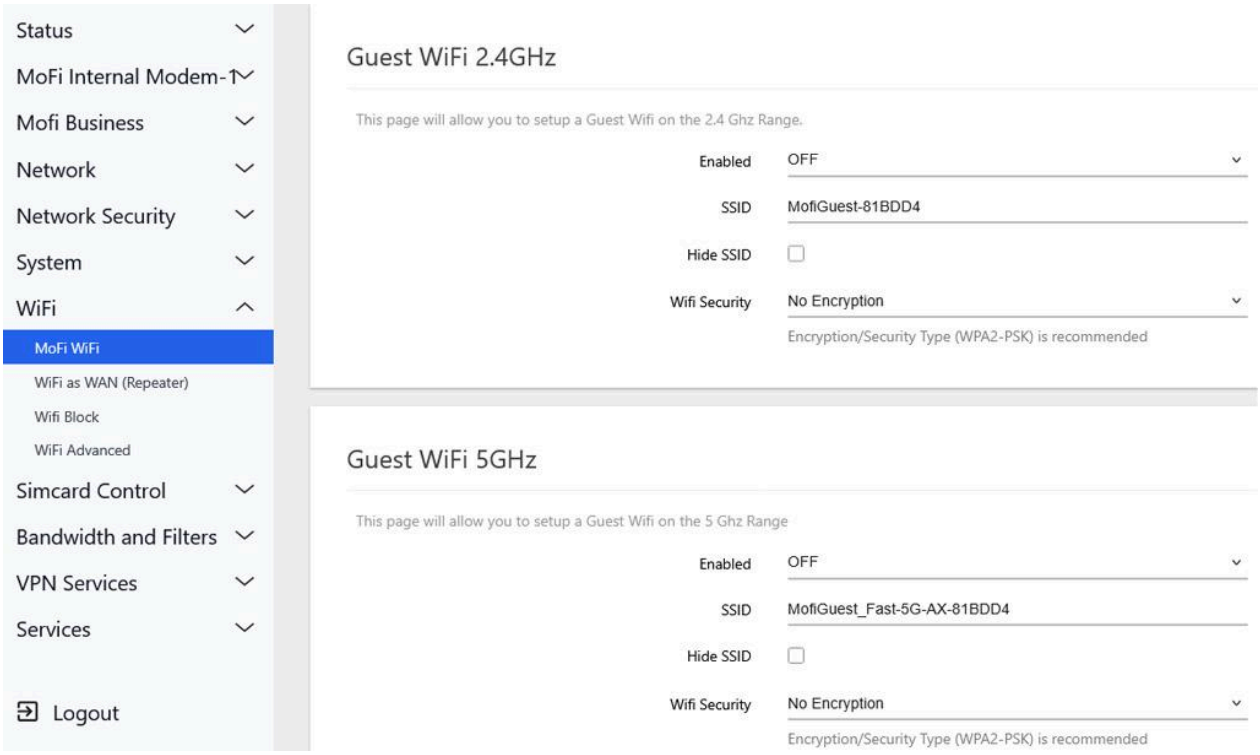


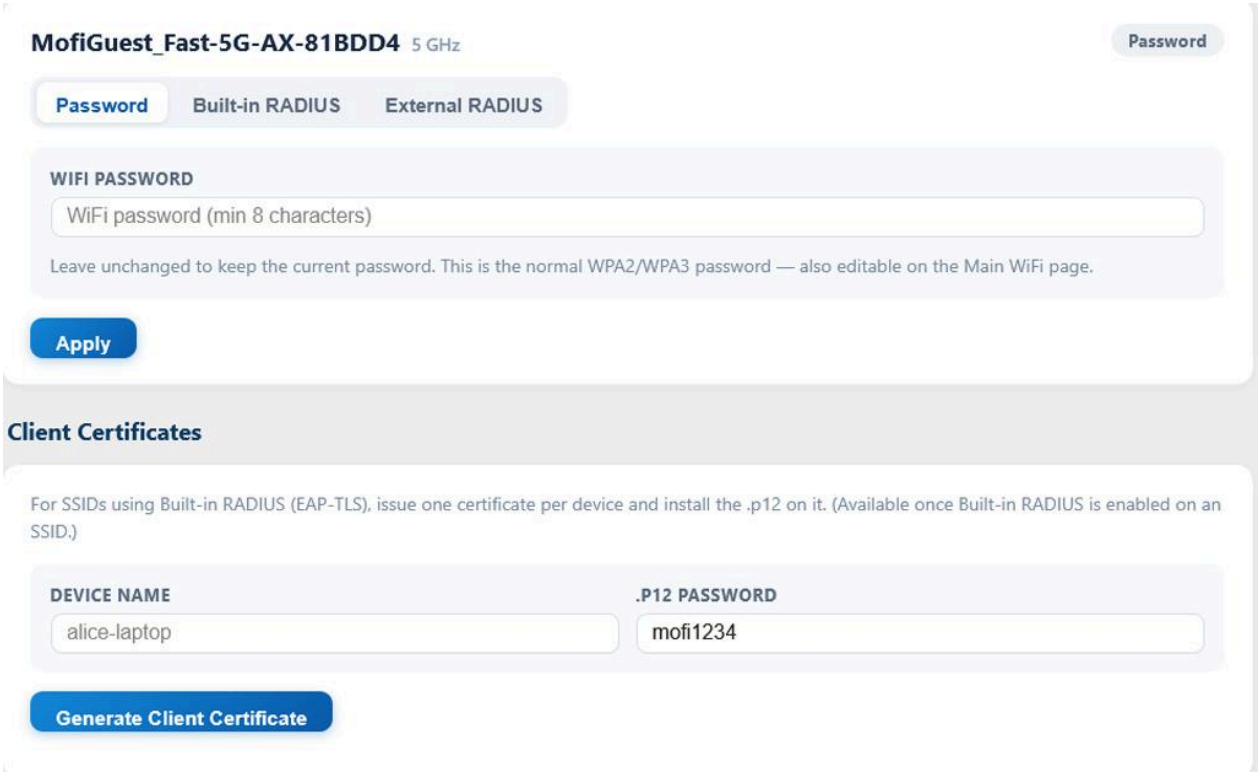
Buttons: Save.

Guest WiFi Tab

Same settings structure as Main WiFi, but for the guest networks (public2g and public5g SSIDs).

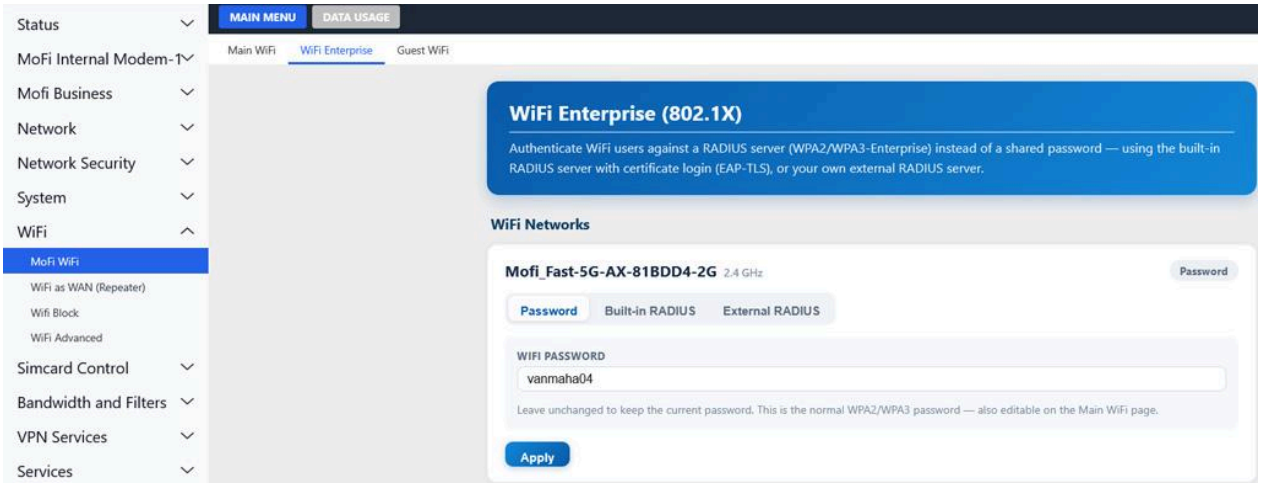
Guest networks are isolated from the main network — guest users can access the internet but cannot see or communicate with devices on the main LAN or other SSIDs.

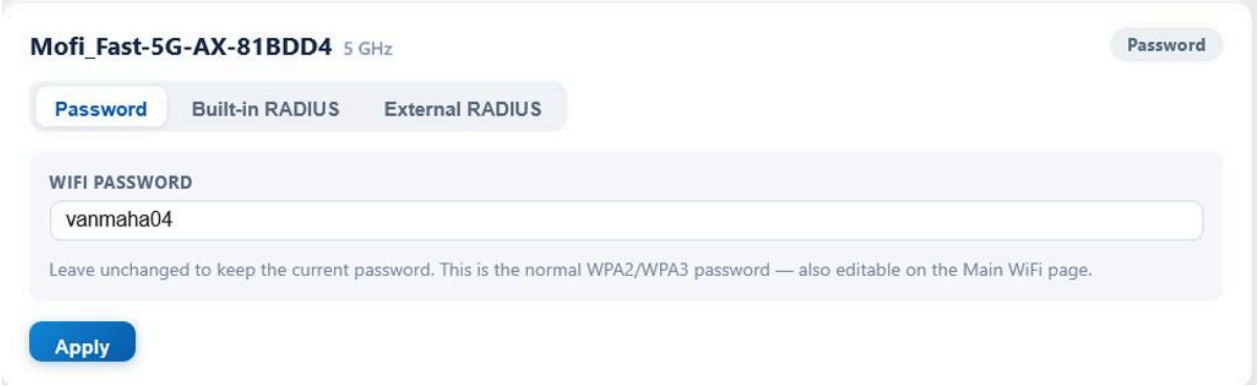




WiFi Enterprise (802.1X)

Authenticate WiFi users against a RADIUS server (WPA2/WPA3-Enterprise) instead of a shared password — using the built-in RADIUS server with certificate login (EAP-TLS), or your own external RADIUS server.





Tips: - Use 5 GHz for faster speeds when possible. Use 2.4 GHz for better range and compatibility with older devices - Keep Main WiFi and Guest WiFi passwords different for security - Guest WiFi is ideal for visitors, IoT devices, or temporary access

---

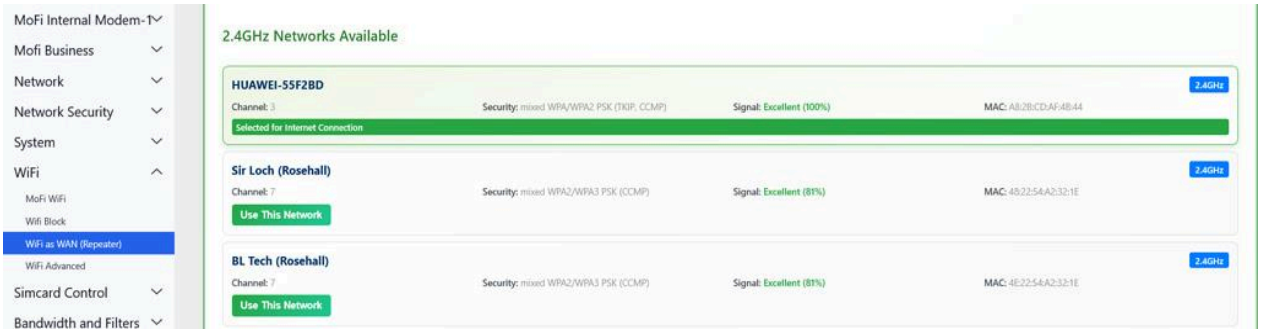
9.2 WiFi as WAN (Repeater)

Menu: Go to **WiFi** → **WiFi as WAN (Repeater)** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/wireless/wifi-repeater

Use an existing WiFi network as your internet source. The router connects to an upstream WiFi network and shares that internet connection with all your devices via ethernet and your own WiFi networks.

Step-by-Step Setup:

1. Click **Scan Networks** — the router scans for available WiFi networks (takes 5-15 seconds)
2. **2.4 GHz Networks Available** — List of discovered 2.4 GHz networks. Each entry shows SSID name, signal strength, and encryption type, with a **Use This Network** button.



3. **5 GHz Networks Available** — Same list for 5 GHz networks, each with a **Use This Network** button.
4. Click **Use This Network** next to the desired network, or manually enter the details below:

2.4 GHz Source Selection:

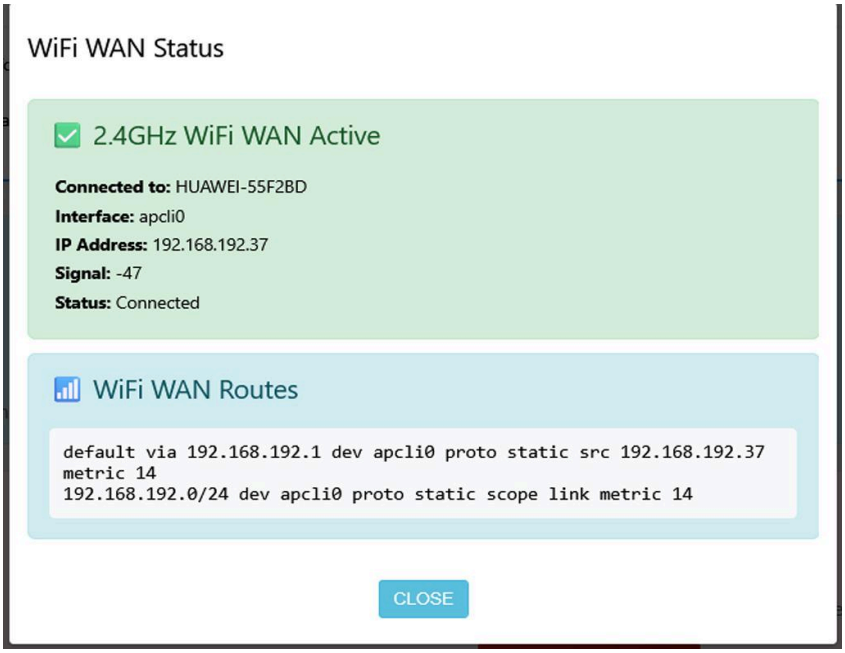
Setting	Description
Use 2.4GHz Network for Internet	Toggle ON to enable using a 2.4 GHz WiFi network as your internet source
Network Name (SSID)	The SSID of the upstream 2.4 GHz network to connect to
Network Password	The password for the upstream network

5 GHz Source Selection:

Setting	Description
Use 5GHz Network for Internet	Toggle ON to enable using a 5 GHz WiFi network as your internet source
Network Name (SSID)	The SSID of the upstream 5 GHz network to connect to
Network Password	The password for the upstream network

5. Click **Save**

Status and Controls: - **Current Status** display — shows connection status - **Show Status** button — refresh the status display - **Disable WiFi WAN** button — disconnect from the upstream network and disable repeater mode



Step-by-Step: Connecting to a Hotel WiFi via Repeater:

1. Navigate to WiFi > WiFi as WAN (Repeater)
2. Click **Scan Networks** and wait for the scan to complete
3. Find the hotel's WiFi network in the 5 GHz or 2.4 GHz list
4. Click **Use This Network** next to it
5. The SSID field will auto-populate with the hotel's network name
6. Enter the hotel WiFi **password** in the Network Password field
7. Click **Save**
8. Wait 30-60 seconds for the router to connect to the hotel WiFi
9. Click **Show Status** to verify the connection
10. All devices connected to your MoFi router now share the hotel WiFi through your own secure network

Step-by-Step: Disabling WiFi Repeater:

1. Navigate to WiFi > WiFi as WAN (Repeater)
2. Click **Disable WiFi WAN**
3. The router will stop using the upstream WiFi and revert to cellular/WAN

Use Cases: - Extend hotel, campground, or RV park WiFi through your router - Use a neighbor's shared WiFi as a backup internet source - Bridge two networks wirelessly

---

9.3 WiFi Block

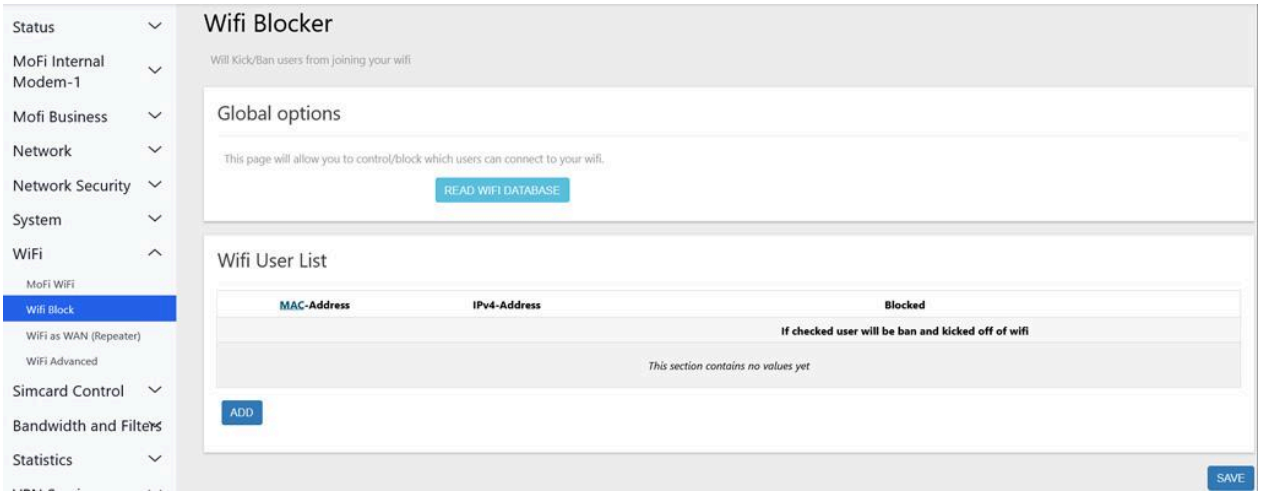
Menu: Go to **WiFi** → **Wifi Block** or click on the line below:
http://192.168.10.1/cgi-bin/luci/admin/wireless/wifiblockjs

Block specific devices from connecting to your WiFi networks by their MAC address.

1. Click **Read Wifi Database** to populate the list of known WiFi clients
2. **WiFi User List Table:**

Column	Description
MAC Address	The device's hardware address
IPv4 Address	The device's current IP address
Blocked	Checkbox — check to block this device

3. Click **Add** to manually add a MAC address to block
4. Click **Save** to apply changes



9.4 WiFi Advanced

Menu: Go to **WiFi** → **WiFi Advanced** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/wireless/wireless

Full LuCI wireless configuration editor for advanced users. Shows all radio interfaces and their associated SSIDs.

Radio ra (2.4 GHz): - Hardware: Mediatek MT7981 802.11bgnax - Configurable: Channel, TX power, country code, bandwidth (20/40 MHz) - SSIDs: Main WiFi 2.4 GHz, Guest WiFi 2.4 GHz, WiFi repeater client

Radio rax (5 GHz): - Hardware: Mediatek MT7981 802.11anacax - Configurable: Channel, TX power, country code, bandwidth (20/40/80/160 MHz) - SSIDs: Main WiFi 5 GHz, Guest WiFi 5 GHz, WiFi repeater client

Per-SSID Controls: - **Disable/Enable** — Toggle individual SSIDs on/off - **Edit** — Open full SSID configuration (SSID name, encryption, key, MAC filtering, advanced options) - **Remove** — Delete the SSID

Associated Stations Table: Shows all currently connected WiFi clients: - Network (which SSID) - MAC Address - Hostname - Signal / Noise (dBm) - RX Rate / TX Rate (Mbps)

Buttons: Save & Apply, Apply unchecked, Save, Reset

Radio ra (2.4 GHz)

- **Chipset:** Mediatek MT7981 with 802.11b/g/n/ax wireless support
- **Configurable Options:** Channel, transmit power, country code, and channel width (20 MHz or 40 MHz)
- **Supported SSIDs:**
    - Main 2.4 GHz WiFi network
    - Guest 2.4 GHz WiFi network
    - WiFi repeater client mode

Radio rax (5 GHz)

- **Chipset:** Mediatek MT7981 with 802.11a/n/ac/ax wireless support
- **Configurable Options:** Channel, transmit power, country code, and channel width (20 MHz, 40 MHz, 80 MHz, or 160 MHz)
- **Supported SSIDs:**
    - Main 5 GHz WiFi network
    - Guest 5 GHz WiFi network
    - WiFi repeater client mode

SSID Management Controls

Each SSID can be managed individually with the following options:

- **Enable / Disable** — Turn the SSID on or off
- **Edit** — Access detailed SSID settings including network name, security mode, password, MAC filtering, and advanced wireless settings
- **Remove** — Delete the SSID configuration

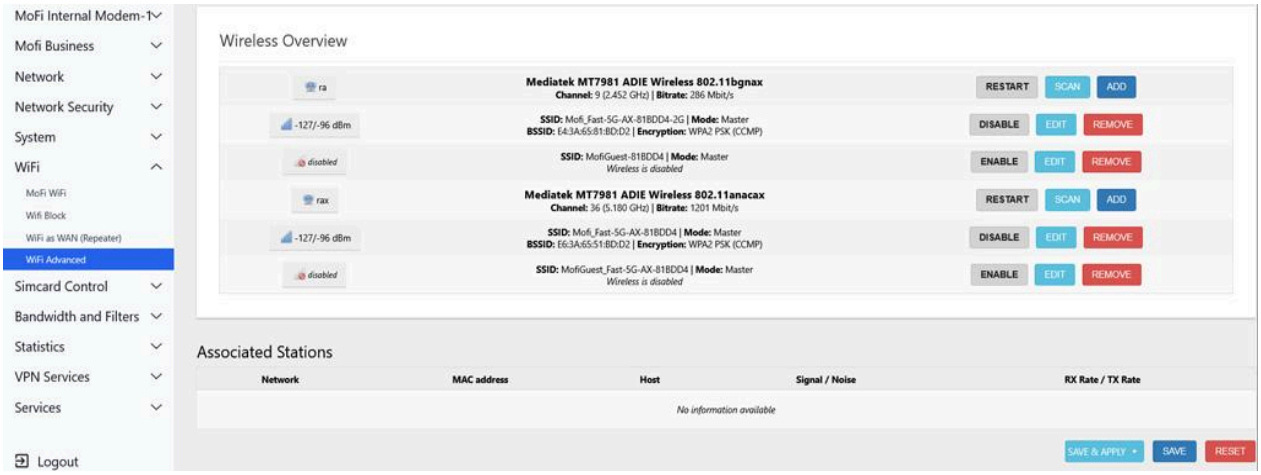
Connected Devices Table

Displays all active WiFi clients connected to the router, including:

- SSID/network name
- MAC address
- Hostname
- Signal and noise levels (dBm)
- RX and TX connection speeds (Mbps)

Action Buttons

- **Save & Apply** — Save settings and apply changes immediately
- **Apply Unchecked** — Apply settings without validation checks
- **Save** — Save changes without applying them
- **Reset** — Restore the previous unsaved configuration changes



---

10. SIM Card Control

SIM Slot Selector

Menu: Go to **Simcard Control** → **SIM Slot Selector** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/simcard/simcard

Switch between SIM card slots and configure separate APN profiles for each slot.

Active SIM Slot display — shows which SIM slot is currently active (Slot 1 or Slot 2).

Slot Selector Buttons: - **Slot 1** — Switch to SIM Slot 1 - **Slot 2** — Switch to SIM Slot 2

Current APN: Displays the APN in use for the active slot.

Slot #1 Profile:

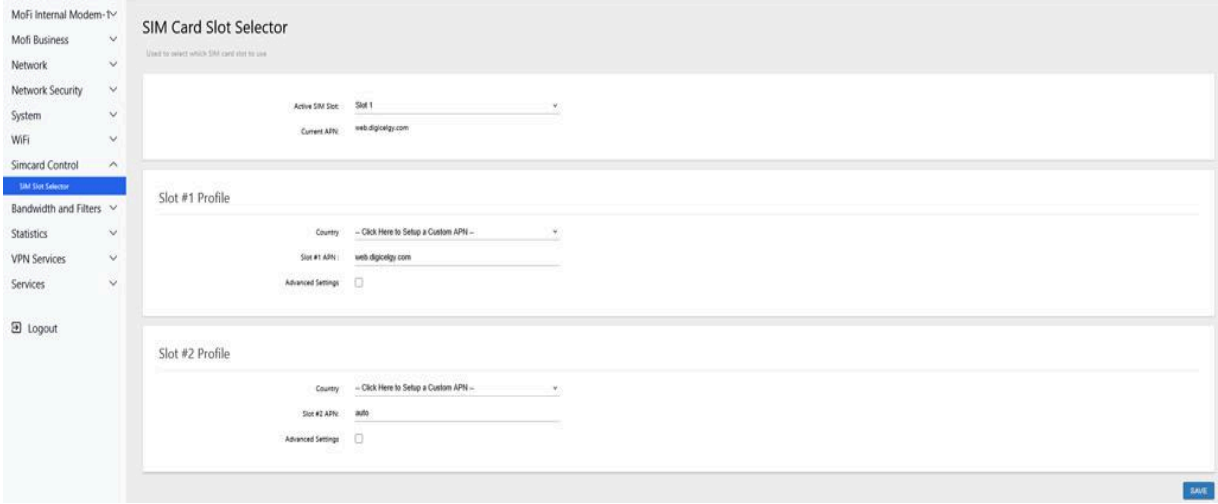
Setting	Options	Description
Country	Dropdown	Country for APN auto-detection
Provider	Auto / carrier list	Carrier selection
Slot #1 APN	Text field	APN for SIM slot 1

Advanced Settings for Slot #1:

Setting	Options	Description
MTU	Numeric	Maximum Transmission Unit
TTL	Dropdown	Time-To-Live override
PDP Type	IPv4 Only / IPv6 Only / IPv4v6	IP protocol version

Slot #2 Profile: Same fields as Slot #1, but for the second SIM.

Buttons: Save.



Note: Switching SIM slots will briefly interrupt the cellular connection (10-20 seconds) while the modem reinitializes with the new SIM card.

---

11. Network Security

This section covers all pages under the **Network Security** menu.

11.1 Firewall Basic Settings

Menu: Go to **Network Security** → **Firewall Basic Settings** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/security/zones

Configure the router's firewall zones, default policies, and NAT offloading.

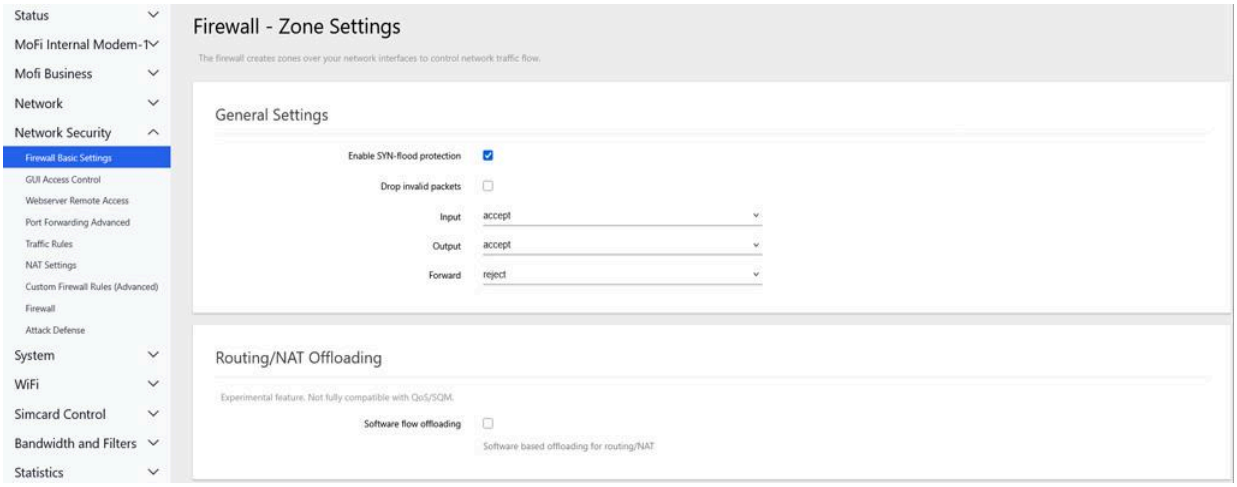
Global Settings:

Setting	Options	Description
Enable SYN-flood protection	Toggle	Protects against SYN flood denial-of-service attacks

Setting	Options	Description
Drop invalid packets	Toggle	Reject malformed network packets
Input	reject / drop / accept	Default policy for incoming traffic to the router itself
Output	reject / drop / accept	Default policy for outgoing traffic from the router
Forward	reject / drop / accept	Default policy for forwarded traffic (LAN to WAN)

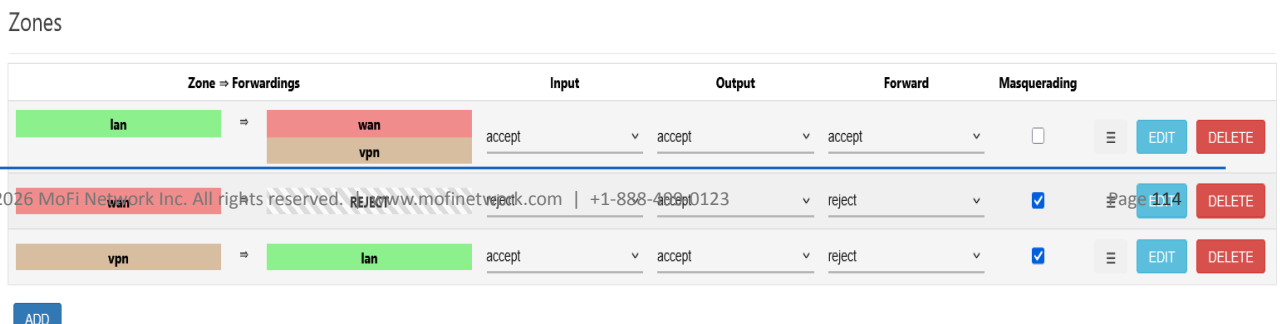
Routing/NAT Offloading:

Setting	Description
Software flow offloading	Accelerates packet forwarding using software optimization
Hardware flow offloading	Accelerates packet forwarding using the SoC's hardware NAT engine (faster, but may conflict with some VPN and QoS



Firewall Zones Table: Shows configured zones (typically: lan, wan, vpn). Each zone has:

Column	Description
Name	Zone name
Input	Policy for traffic entering this zone
Output	Policy for traffic leaving this zone
Forward	Policy for forwarding between this zone and others
Masquerading	Toggle — enables NAT for this zone (required for WAN)



Click **Edit** on a zone to modify its settings. Click **Add** to create new zones.

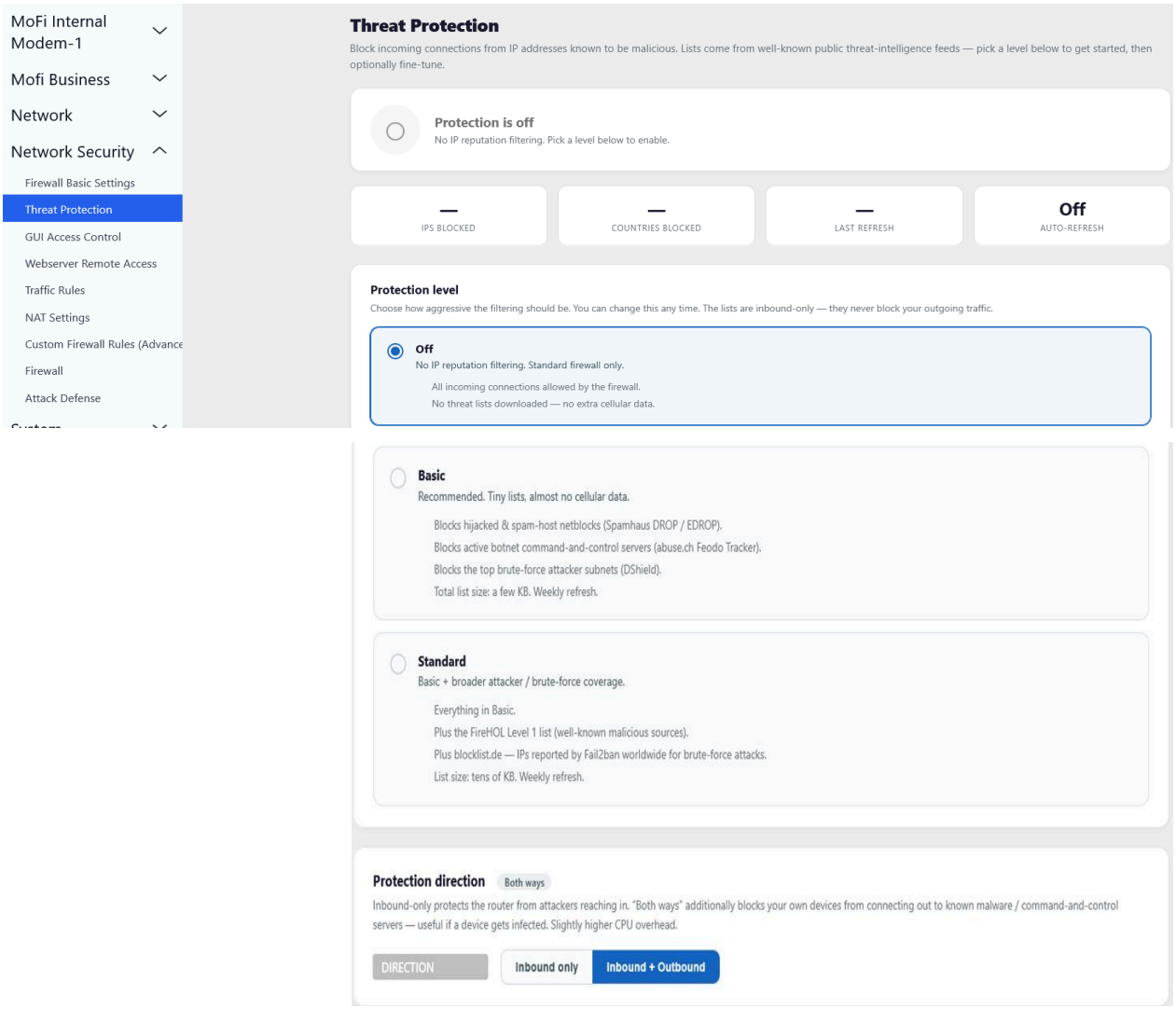
Buttons: Save & Apply, Save, Reset

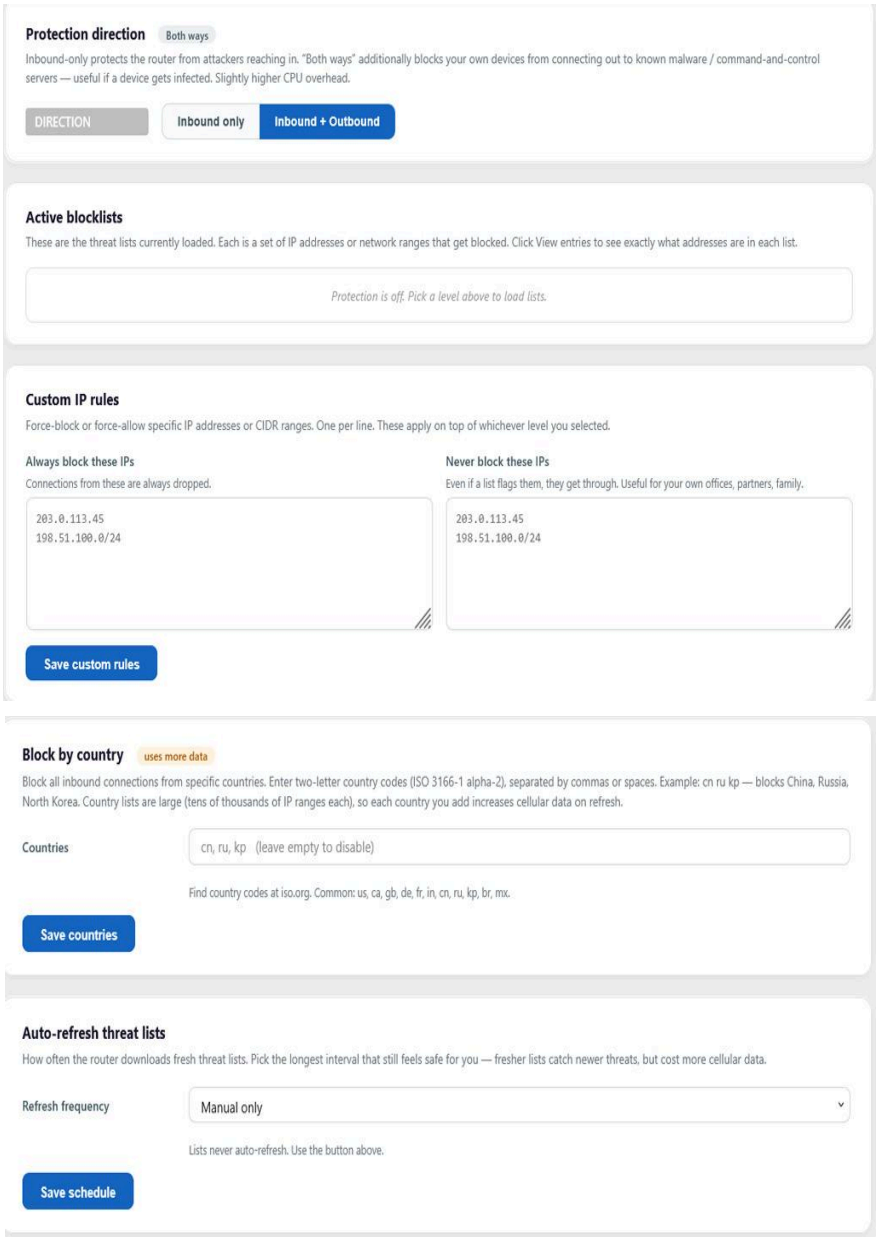
Threat Protection

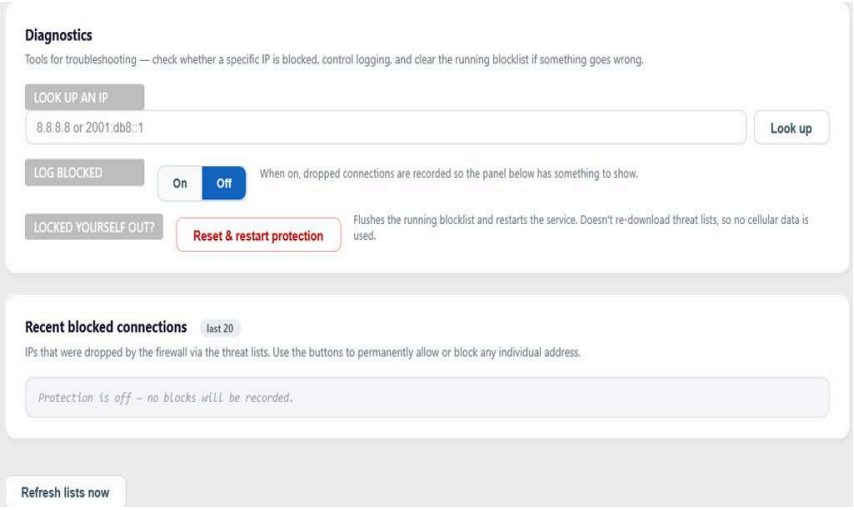
Menu: Go to Network Security → Threat Protection or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/security/threat-protection

Threat Protection

Block incoming connections from IP addresses known to be malicious. Lists come from well-known public threat-intelligence feeds — pick a level below to get started, then optionally fine-tune.







A note on cellular data: Threat lists download whenever Protection is changed or the scheduled refresh runs. Basic uses a few KB, Standard tens of KB, Daily refresh is roughly 7× more than Weekly, and country blocking can use much more (country lists are large). Pick what fits your data plan.

11.2 GUI Access Control

Menu: Go to **Network Security** → **GUI Access Control** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/security/gui

Same as Section 7.5 — Router Access Control. Controls HTTP/HTTPS ports and LAN-only vs. LAN+WAN access.

11.3 Webserver Remote Access

Menu: Go to **Network Security** → **Webserver Remote Access** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/security/webserver-remote

Whitelist specific IP addresses for remote management access to the router's web interface.

Setting	Options	Description
Current IP	Display only	Your current IP address
Remote Access WhiteList	Toggle ON/OFF	Enable IP-based access control
Interface	Module / Module2 / VPN Tunnel / Cloudlink /	Which interface the whitelist applies to

Setting	Options	Description
	Wireguard / WAN Port / Broadband / RNDIS / others	
WhiteList entries	IP address list	Add specific IP addresses that are allowed remote access

Buttons: Save.

11.4 Port Filtering THIS IS NOT IN THE GUI ATM

Menu: Network Security > Port Filtering **URL:** `/cgi-bin/luci/admin/security/port-filtering`

Same interface as Section 8.6 — Port Filtering. Enable whitelist mode and specify allowed ports.

11.5 Port Forwarding Advanced

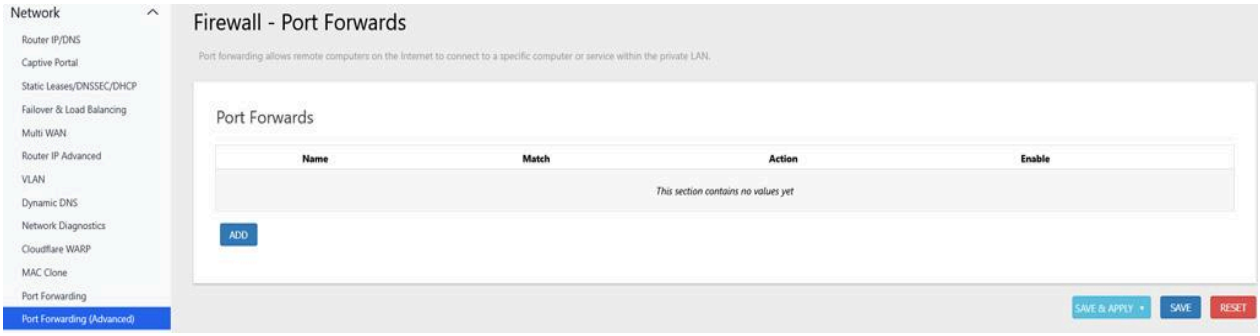
Menu: Go to **Network** → **Port Forwarding Advanced** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/network/portfw-adv

Advanced port forwarding interface (full LuCI format):

Port Forwards Table:

Column	Description
Match	Source zone, protocol, and port match conditions
Action	Destination IP and port
Enable	Toggle to enable/disable individual rules

Click **Add** to create new rules with full control over source zone, source IP, source port, destination zone, destination IP, destination port, and protocol.



Buttons: Add, Save & Apply, Save, Reset

11.6 Traffic Rules

Menu: Go to **Network Security** → **Traffic Rules** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/security/traffic-rules

Pre-configured and custom firewall rules that control which traffic is allowed or blocked.

Traffic Rules Table: Each row contains a firewall rule with: - Rule description (e.g., “Allow-DHCP-Renew”, “Allow-ICMP”, “Allow-HTTP”) - Match conditions (source zone, port, protocol) - Action (Accept, Drop, Reject) - Enable toggle - Edit/Delete buttons

Default Rules Include: - DHCP (port 68 UDP) - ICMP (ping) - IGMP (multicast) - IPSec (ports 500, 4500 UDP) - OpenVPN (port 1194) - HTTP (port 80) - HTTPS (port 443)

Firewall Rules

This section manages the firewall rules that determine which network traffic is permitted or blocked. Both default system rules and user-created custom rules are supported.

Traffic Rules Table

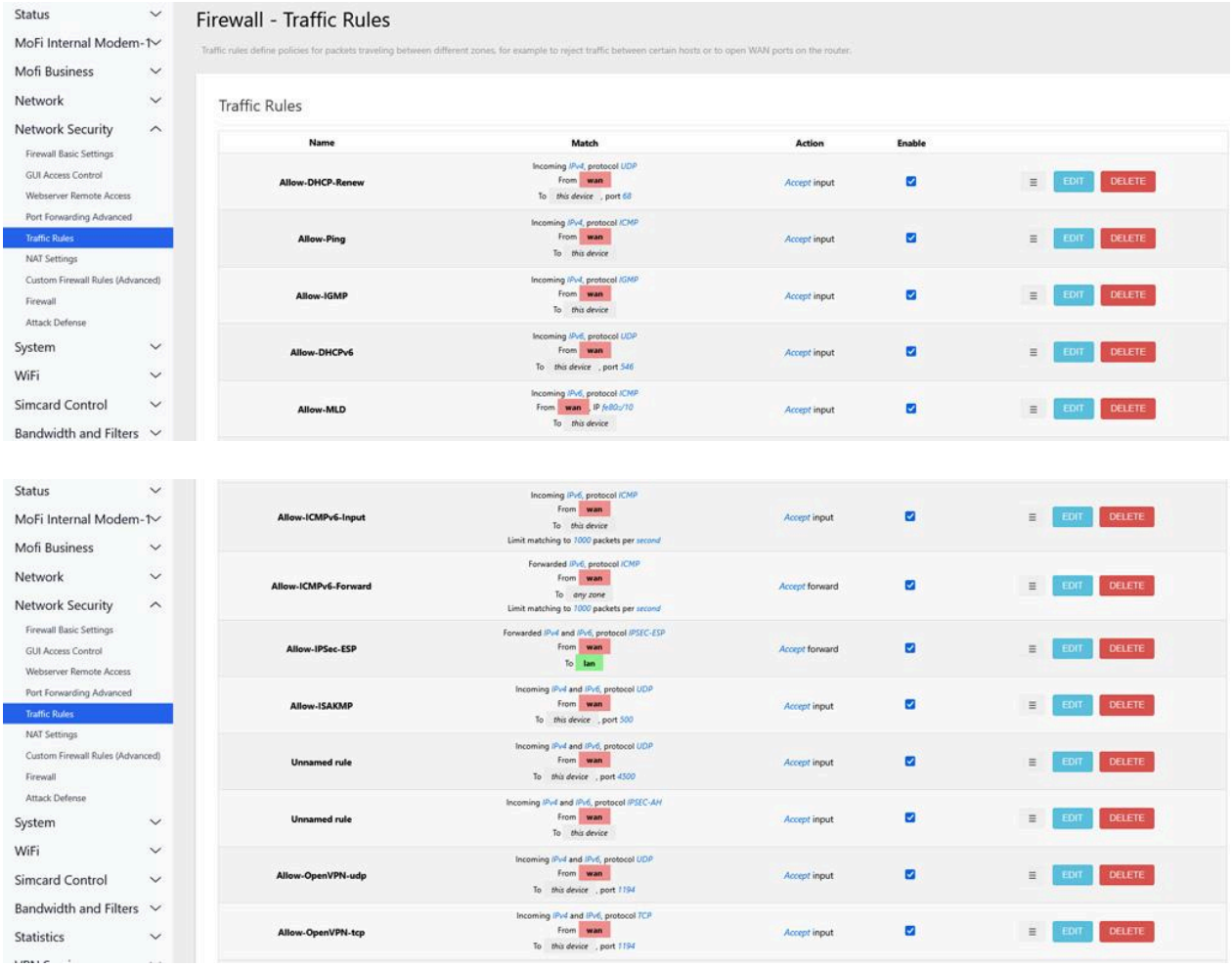
Each rule entry displays:

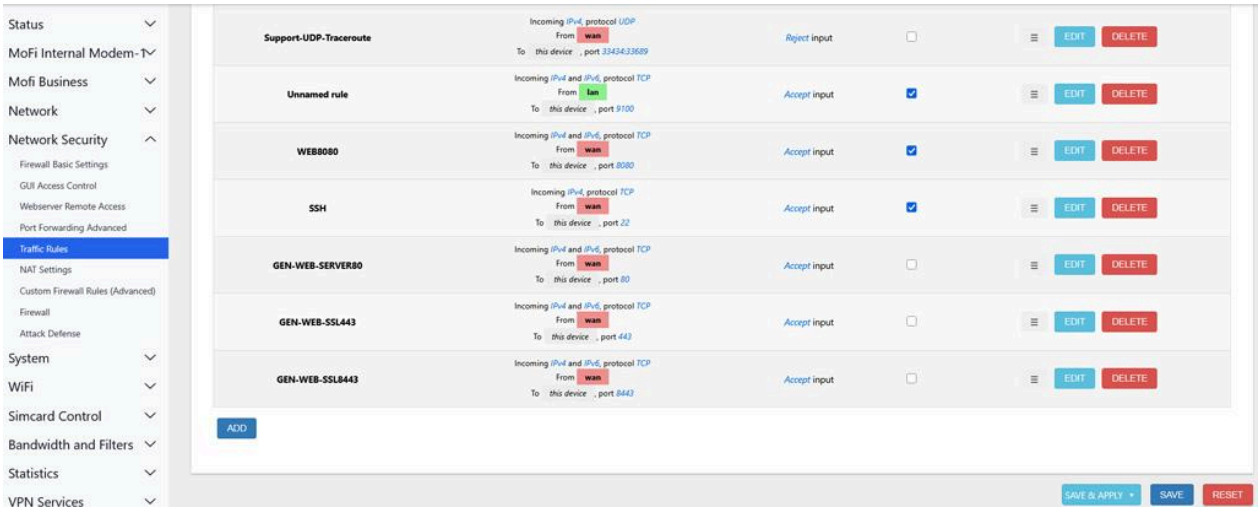
- A rule name or description (for example: “Allow-DHCP-Renew”, “Allow-ICMP”, or “Allow-HTTP”)
- Matching criteria such as source zone, protocol, and port number
- The selected action: **Accept**, **Drop**, or **Reject**
- An enable/disable switch
- Edit and Delete options

Included Default Rules

The router includes several predefined firewall rules, including:

- **DHCP** — Allows UDP port 68 traffic
- **ICMP** — Allows ping and network diagnostic traffic
- **IGMP** — Supports multicast traffic
- **IPSec** — Allows VPN traffic on UDP ports 500 and 4500
- **OpenVPN** — Allows VPN connections on port 1194
- **HTTP** — Allows web traffic on port 80
- **HTTPS** — Allows secure web traffic on port 443 (Chatgpt)





Click **Add** to create custom rules. Click **Save & Apply** to activate changes.

11.7 NAT Settings

Menu: Go to Network Security → NAT Settings or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/security/snats

Configure Source NAT (SNAT) rules for advanced routing scenarios.

NAT Rules Table:

Column	Description
Match	Source IP/port and destination IP/port conditions
Action	The NAT translation to apply
Enable	Toggle to enable/disable Click **Add** to create new SNAT rules. **Buttons:** Add, Save & Apply, Save, Reset

Column	Description

11.8 Custom Firewall Rules (Advanced)

Menu: Go to **Network Security** → **Custom Firewall Rules** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/security/custom

Raw iptables rule editor. Enter custom iptables commands that will be executed after the standard firewall rules.

This is a plain text editor where you can type iptables commands, one per line. Rules are executed in order on every firewall restart.

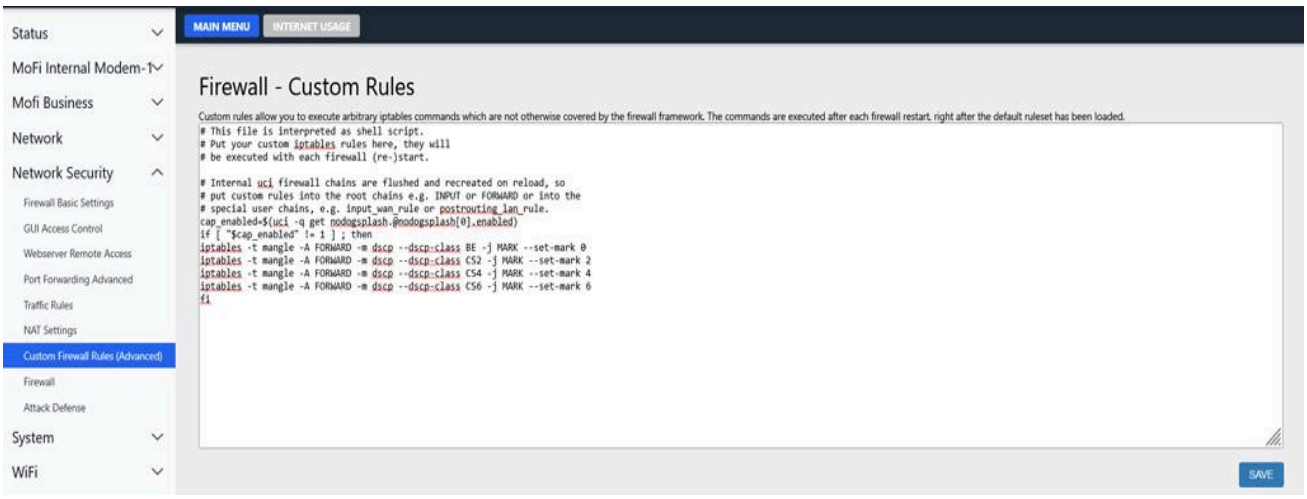
Warning: Incorrect iptables rules can lock you out of the router or break connectivity. Only use this if you are experienced with Linux iptables. A factory reset will clear custom rules.

Custom iptables Rules

This section provides a raw iptables rule editor for advanced firewall customization. Any commands entered here are executed after the standard firewall rules are applied.

The editor is a plain text field where you can enter custom iptables commands, one command per line. All rules are processed in order each time the firewall restarts.

> **Warning:** Incorrect iptables rules may block router access or disrupt network connectivity. This feature is intended for advanced users familiar with Linux iptables. Performing a factory reset will remove all custom rules.



11.9 Firewall Overview

Menu: Go to **Network Security** → **Firewall** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/security/firewall

Standard LuCI firewall overview combining zones, forwarding rules, and traffic rules in a single view. This is an alternative view of the same firewall configuration accessible through the other security pages.

11.10 Attack Defense (banIP)

Menu: Go to Network Security → Attack Defense or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/security/banip

Automated threat blocking using community-maintained IP blocklists, country blocking, and login attempt monitoring.

This page has six tabs: **Overview**, **IPSet Report**, **Edit Blacklist**, **Edit Whitelist**, **Edit Maclist**, **Log View**.

Overview Tab

Information Panel (display only): - Status, version, active sources, active devices, active interfaces - Run information, flags, last run time, refresh timer

Action Buttons: Suspend, Refresh, Restart

General Settings:

Setting	Options	Description
Enabled	Toggle	Enable/disable the banIP service
Startup Trigger Interface	Dropdown	Network interface that triggers banIP startup
Auto Detection	Toggle	Auto-detect interfaces, devices, subnets, and protocols
Network Interfaces	Multi-select	Manually select interfaces (if auto-detect is off)
IPv4 Support	Toggle	Enable IPv4 blocking
IPv6 Support	Toggle	Enable IPv6 blocking
Log Monitor	Toggle	Block suspicious login attempts (web interface)
Enable SRC logging	Toggle	Log suspicious incoming packets
Enable DST logging	Toggle	Log suspicious outgoing packets
Whitelist Only	Toggle	Restrict internet to only whitelisted IPs/websites

Setting	Options	Description
E-Mail Notification	Toggle	Send email when blocks occur
E-Mail Receiver Address	Text field	Notification email recipient
Verbose Debug Logging	Toggle	Detailed logging for troubleshooting

Additional Settings:

Setting	Options	Description
Service Priority	Highest / High / Normal / Less / Least	Processing priority for the banIP service
Trigger Delay	Numeric (seconds)	Additional seconds before banIP processing begins after boot
Download Queue	1 / 2 / 4 / 8 / 16 / 32	Number of concurrent blocklist downloads
Base Temp Directory	Text	Temporary working directory path
Backup Directory	Text	Where to store blocklist backups
Report Directory	Text	Where to save banIP reports
Download Utility	uclient-fetch / wget / curl / aria2c	Tool used to download blocklists
Download Insecure	Toggle	Skip SSL certificate verification on downloads
Download Parameters	Text	Manually override pre-configured download options

Advanced Chain Settings:

Setting	Options	Description
Global IPSet Type	src+dst / src / dst	Which direction to apply blocklists
SRC Target	DROP / REJECT	Action for blocked incoming traffic
DST Target	REJECT / DROP	Action for blocked outgoing traffic
Maclist/Whitelist/Blacklist Timeout	30 min / 1 hr / 6 hrs / 12 hrs / 24 hrs	How long entries remain active
SRC IPSet Type	Multi-select per list	Assign specific blocklists to SRC (incoming) filtering
DST IPSet Type	Multi-select per list	Assign specific blocklists to DST (outgoing) filtering
SRC+DST IPSet Type	Multi-select per list	Assign specific blocklists to both-direction filtering
IPv4 Chains	LAN Input / LAN Forward / WAN Input / WAN Forward	Select which firewall chains to apply IPv4 blocking

Setting	Options	Description
IPv6 Chains	LAN Input / LAN Forward / WAN Input / WAN Forward	Select which firewall chains to apply IPv6 blocking

Advanced Log Settings:

Setting	Options	Description
Log Limit	50 / 100 / 250 / 500	Maximum log entries per run
Log Terms	Multi-select: luci / nginx	Which services to monitor for suspicious login attempts
LuCI Log Count	Numeric	Number of failed web login attempts before blocking
NGINX Log Count	Numeric	Number of failed nginx attempts before blocking
SRC Log Options	unspecified / rate-limited 2/sec / rate-limited 10/sec	Logging rate for blocked incoming packets
DST Log Options	unspecified / rate-limited 2/sec / rate-limited 10/sec	Logging rate for blocked outgoing packets

Advanced E-Mail Settings:

Setting	Options	Description
E-Mail Sender Address	Text	From address for notification emails
E-Mail Topic	Text	Subject line prefix for notification emails
E-Mail Profile	Text	msmtp profile name to use for sending
E-Mail Actions	Multi-select: start / reload / restart / refresh	Which banIP actions trigger email notifications

Blocklist Sources: Enable/disable individual threat intelligence feeds:

Source	Description	Approximate Entries
darklist	Composite threat list	Varies
debl	Dynamic Emerging Blocklist	Varies
doh	DNS-over-HTTPS servers	Varies
drop	Spamhaus DROP list	~1,000
dshield	DShield.org recommended block list	~20
edrop	Spamhaus Extended DROP	~500
feodo	Feodo Tracker (banking trojans)	~300
firehol1-4	FireHOL threat lists (level 1-4)	500-15,000
greensnow	GreenSnow.co attack list	~3,000

Source	Description	Approximate Entries
iblockads	Ad-serving networks	Varies
iblockspy	Known spyware networks	Varies
myip	MyIP.ms blacklist	Varies
nixspam	NiXSpam IP blocklist	~10,000
proxy	Known proxy/VPN exit nodes	Varies
sslbl	SSL Blacklist (malicious SSL)	~300
talos	Cisco Talos threat list	~1,000
threat	Emerging Threats	Varies
tor	Tor exit node list	~7,000
uceprotect1-2	UCE Protect spam lists	Varies
voip	VoIP abuse list	Varies
yoyo	Ad server list	~2,500

Country Selection: Block traffic from/to specific countries using a multi-select dropdown of all world countries.

ASN Selection: Block specific Autonomous System Numbers (ISPs/organizations).

Local Sources: - Multi-select: maclist / whitelist / blacklist — enable locally maintained lists

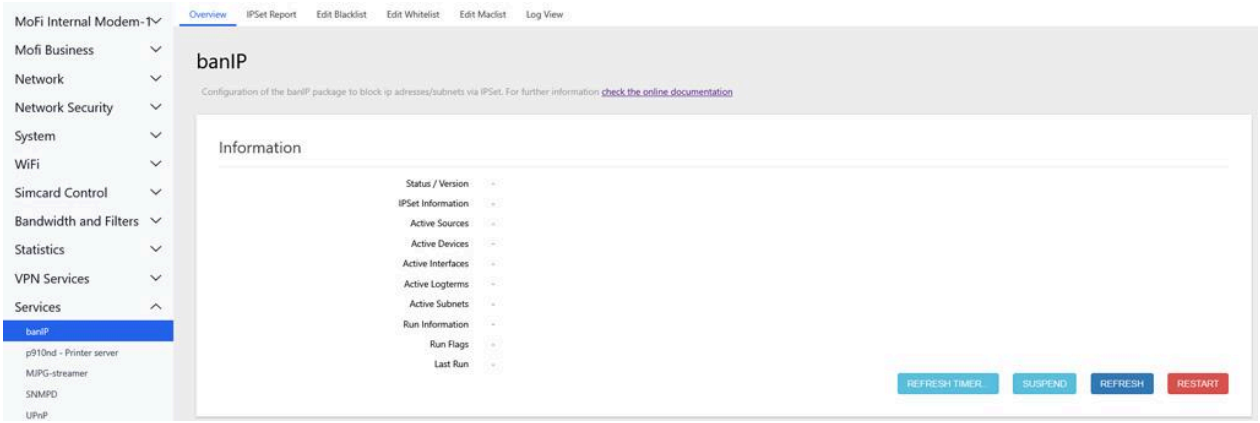
Extra Sources: - Add additional non-banIP IPSets from other packages

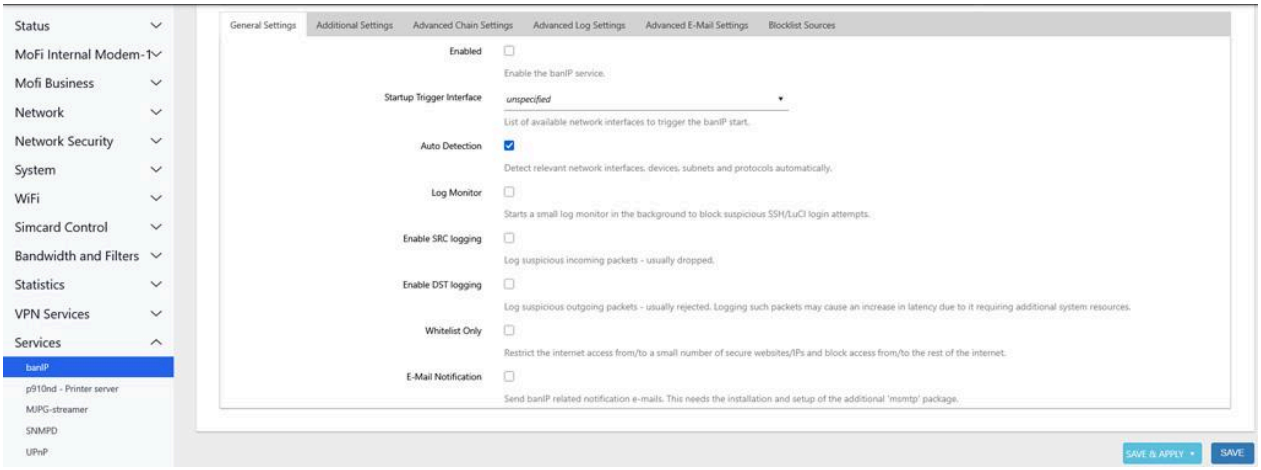
Auto Blacklist/Whitelist: - **Auto Blacklist** — Automatically transfers suspicious IPs from log to blacklist during runtime - **Auto Whitelist** — Automatically transfers your uplink IPs to whitelist during runtime

Step-by-Step: Enabling Basic Threat Protection:
1. Navigate to Network Security > Attack Defense
2. Click the **Overview** tab
3. Toggle **Enabled** to ON
4. Toggle **Auto Detection** to ON
5. Enable **IPv4 Support**
6. Toggle **Log Monitor** to ON (blocks suspicious login attempts)
7. Under **Blocklist Sources**, enable these recommended lists: - **drop** — Spamhaus DROP (known criminal networks) - **dshield** — DShield recommended block list - **feodo** — Banking trojan command servers - **threat** — Emerging threats
8. Click **Save & Apply**
9. Click **Restart** to activate the blocklists
10. The router will now automatically block traffic from known malicious IP addresses

Step-by-Step: Blocking Traffic from Specific Countries:
1. Navigate to Network Security > Attack Defense
2. Under Blocklist Sources, enable **country**
3. Under **Country Selection**, select the countries you want to block

4. Click **Save & Apply**
5. Click **Restart**





Edit Blacklist Tab

Manually add IP addresses or CIDR ranges to the blocklist.

Edit Whitelist Tab

Manually add IP addresses or CIDR ranges that should never be blocked.

Edit Maclist Tab

Block or allow specific MAC addresses.

Log View Tab

View banIP activity logs showing blocked connections, rule matches, and events.

12. VPN Services

This section covers all VPN options available under the **VPN Services** menu.

12.1 WireGuard VPN Server

Menu: Go to **VPN Services** → **Wireguard** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/wireguard-mofi-js

Built-in WireGuard VPN server for secure remote access to your router and local network.

Server Configuration:

Setting	Options	Description
Enable	Toggle	Turn the WireGuard server on or off
MTU	Numeric, range 1280-1400 (default: 1400)	Tunnel Maximum Transmission Unit. Lower values (e.g., 1280) may be needed if you experience connection drops over cellular.
Listen Port	Numeric (default: 6677)	UDP port the server listens on. Must be allowed through your firewall. Common alternative: 5566.
Server Address (IP Addresses)	CIDR (default: 10.110.0.1/24)	The VPN tunnel IP address and subnet. The first address is the gateway for clients. If no subnet mask is specified, /24 is automatically appended.
Endpoint Address (Public IP)	IP or hostname	The public IP or hostname clients will connect to (e.g., your CloudLink IP, DDNS hostname, or WAN IP).
Enable LAN Access	Toggle	When ON, VPN clients can access devices on the local network (192.168.10.0/24). When OFF, clients can only access the internet through the VPN tunnel. LAN subnet is automatically detected from the br-lan interface.

Peer Management: Add VPN clients (peers) that can connect to the server:

- Click **Add Peer** to create a new client
- The router automatically generates: public key, private key, preshared key, and a complete .conf file
- Download the generated .conf file and import it into any WireGuard client app (available for Windows, macOS, Linux, iOS, Android)

Generated Peer Configuration Includes: - Client private key (auto-generated) - Client IP address within the VPN subnet (auto-assigned, starting from .2) - Server public key and endpoint (your router's public IP + port) - Preshared key (for additional security) - Allowed IPs: `10.110.0.0/24` (VPN subnet) + `192.168.10.0/24` (LAN, if LAN Access enabled) - PersistentKeepalive: 25 seconds (keeps the tunnel alive behind NAT) - MTU: matches server MTU setting (default 1400)

Peer Files Created (on the router): - `/etc/wireguard/peer_00.conf` — First peer configuration file - `/etc/wireguard/peer_00.key` — Peer private key - `/etc/wireguard/peer_00.pub` — Peer public key - Peers are sequentially numbered: peer_00, peer_01, peer_02, etc.

Download Options: - Download individual peer .conf files - **Download ALL peers** — Downloads `all_peers.tar.gz` bundle containing all peer configs - **Flush old peer files** — Remove all generated peer configurations (requires confirmation)

Generated Peer Configuration

When a new WireGuard peer is created, the router automatically generates a complete client configuration that includes:

- Client private key (automatically generated)
- Client VPN IP address within the VPN subnet (automatically assigned starting at `.2`)
- Server public key and endpoint (your router's public IP address and WireGuard port)
- Preshared key for additional encryption security
- Allowed IPs:
  - `10.110.0.0/24` — VPN subnet
  - `192.168.10.0/24` — LAN subnet (included when LAN Access is enabled)
- `PersistentKeepalive: 25` — Keeps the tunnel active behind NAT connections
- MTU value matching the server MTU setting (default: `1400`)

Peer Files Stored on the Router

The router creates individual configuration and key files for each peer, including:

- `/etc/wireguard/peer_00.conf` — Peer configuration file
- `/etc/wireguard/peer_00.key` — Peer private key
- `/etc/wireguard/peer_00.pub` — Peer public key

Peer files are numbered sequentially:

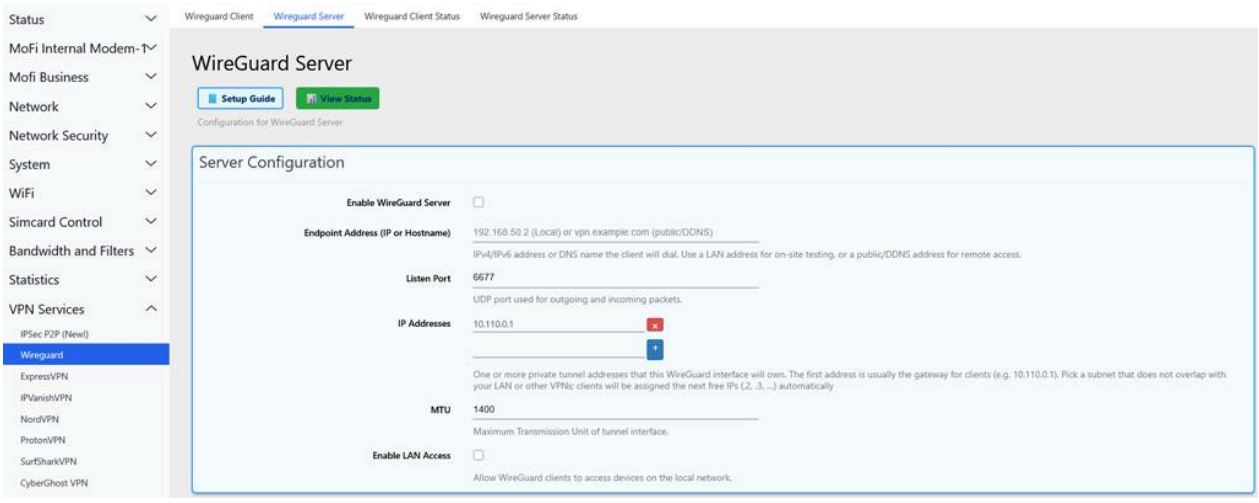
- `peer_00`
- `peer_01`
- `peer_02`
- and so on

Download and Management Options

Available peer management actions include:

- Download individual peer `.conf` files
- **Download ALL Peers** — Downloads an `all_peers.tar.gz` archive containing every generated peer configuration
- **Flush Old Peer Files** — Deletes all generated peer configuration files (confirmation required)

Step-by-Step: Setting Up WireGuard VPN:
1. Navigate to VPN Services > Wireguard
2. Toggle **Enable** to ON
3. Set **Listen Port** (default 6677, or change to your preferred port)
4. Set **Server Address** (default 10.110.0.1/24 is fine)
5. Enter your **Endpoint Address (Public IP)** (or the CloudLink IP if using CloudLink)
6. Enable **LAN Access** if you want VPN clients to reach your local devices
7. Click **Save** to start the WireGuard server
8. Click **Add Peer** to create a client configuration
9. Click **Download** next to the peer to get the .conf file
10. Install the WireGuard app on your device (phone, laptop, etc.)
11. Import the .conf file into the WireGuard app
12. Activate the VPN connection



Note: If your router is behind a cellular carrier that doesn't provide a public IP, you will need CloudLink to make the WireGuard server reachable from the internet.

12.2 ProtonVPN

Menu: Go to **VPN Services** → **ProtonVPN** or click on the link below:

http://192.168.10.1/cgi-bin/luci/admin/vpnservice/protonovpn

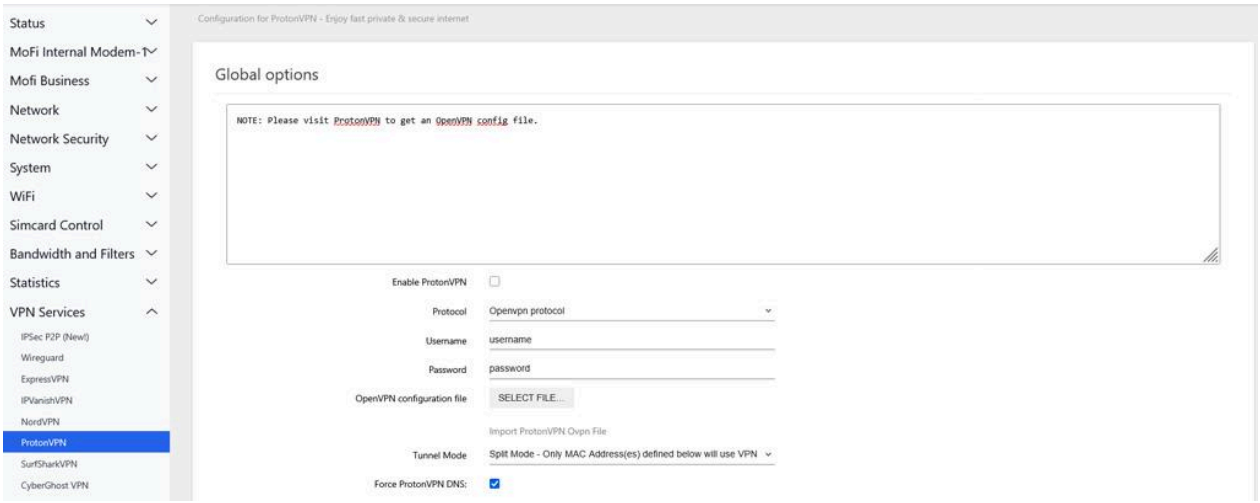
Route your internet traffic through ProtonVPN's privacy-focused network.

Setting	Options	Description
Enable ProtonVPN	Toggle	Activate or deactivate ProtonVPN
Protocol	OpenVPN	VPN protocol (OpenVPN)
Username	Text	ProtonVPN username (from your ProtonVPN account settings, NOT your email)
Password	Text	ProtonVPN password (from account settings)
OpenVPN configuration file	File upload	Upload the .ovpn file downloaded from ProtonVPN
Tunnel Mode	All Traffic / Split Mode by MAC	Route all traffic through VPN, or only specific devices
Force ProtonVPN DNS	Toggle	Use ProtonVPN's DNS servers (prevents DNS leaks)

Split Mode Device List: When Tunnel Mode = Split Mode, add devices by Label, MAC Address, and IPv4 Address.

ProtonVPN Status: Shows current connection status.

Step-by-Step: Setting Up ProtonVPN:
1. Log in to your ProtonVPN account at account.protonvpn.com
2. Go to Downloads > OpenVPN configuration files
3. Download a .ovpn file for your preferred server/country
4. Get your OpenVPN/IKEv2 username and password from account settings
5. On the router, navigate to VPN Services > ProtonVPN
6. Toggle **Enable ProtonVPN** to ON
7. Enter your **Username** and **Password** from step 4
8. Upload the .ovpn file under **OpenVPN configuration file**
9. Set **Tunnel Mode** (All Traffic or Split Mode)
10. Toggle **Force ProtonVPN DNS** to ON
11. Click **Save**
12. Check **ProtonVPN Status** — it should show "Connected" after 30-60 seconds

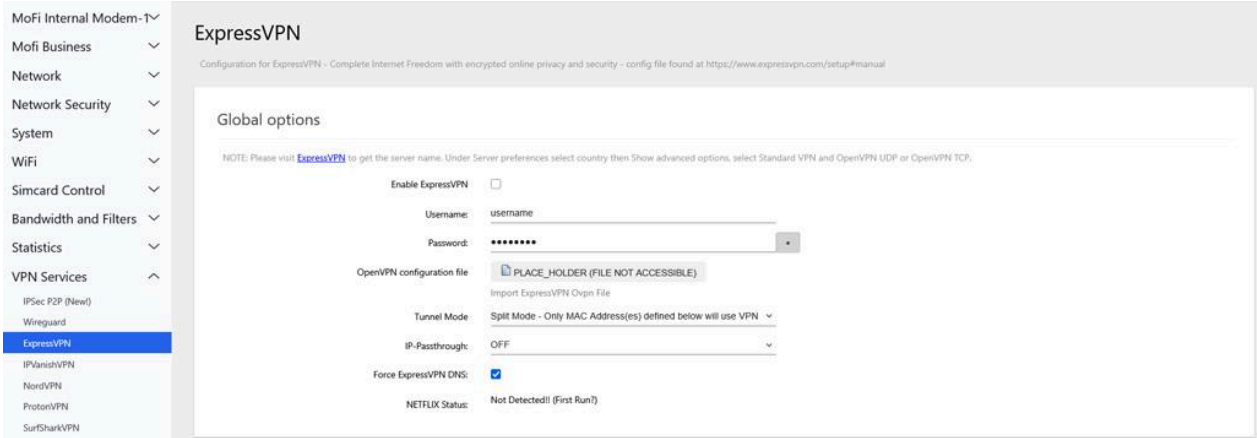


12.3 ExpressVPN

Menu: Go to **VPN Services** > **ExpressVPN** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/expressvpnjs

Setting	Options	Description
Enable ExpressVPN	Toggle	Activate or deactivate
Username	Text	ExpressVPN manual config username
Password	Text	ExpressVPN manual config password
OpenVPN configuration file	File upload	Upload .ovpn file from ExpressVPN
Tunnel Mode	All Traffic / Split Mode by MAC	Route all or selected traffic
IP-Passthrough	Toggle	Pass VPN IP to a single device
DMZ mode	Toggle	Forward all VPN traffic to one device
DMZ IP address	Text	Target device IP for DMZ
Enable Web	Toggle	Allow web management through the VPN
Force ExpressVPN DNS	Toggle	Use ExpressVPN DNS servers

NETFLIX Status: Detects if Netflix is accessible through the VPN connection.



Split Mode Device List: Add devices by Label, MAC, and IPv4.

12.4 NordVPN

Menu: Go to **VPN Services** → **NordVPN** or click on the link below:

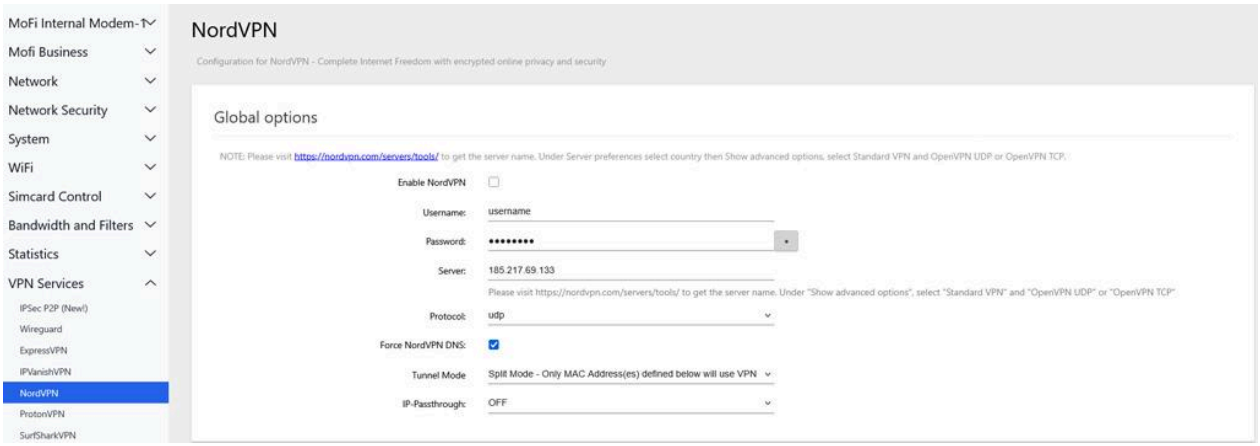
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/nordvpn

Setting	Options	Description
Enable NordVPN	Toggle	Activate or deactivate
Username	Text	NordVPN service credentials username
Password	Text	NordVPN service credentials password
Server	Text	Server hostname from nordvpn.com/servers/tools/ (e.g., us1234.nordvpn.com)
Protocol	UDP / TCP	UDP is faster; TCP is more reliable on restrictive networks
Force NordVPN DNS	Toggle	Use NordVPN DNS servers
Tunnel Mode	All Traffic / Split Mode by MAC	Route all or selected traffic
IP-Passthrough	Toggle	Pass VPN IP to a single device

Split Mode Device List: Add devices by Label, MAC, and IPv4.

Step-by-Step: Setting Up NordVPN:
1. Log in to your NordVPN account at nordvpn.com
2. Go to NordVPN > Service Credentials and copy your service username and password (these are different from your login email/password)

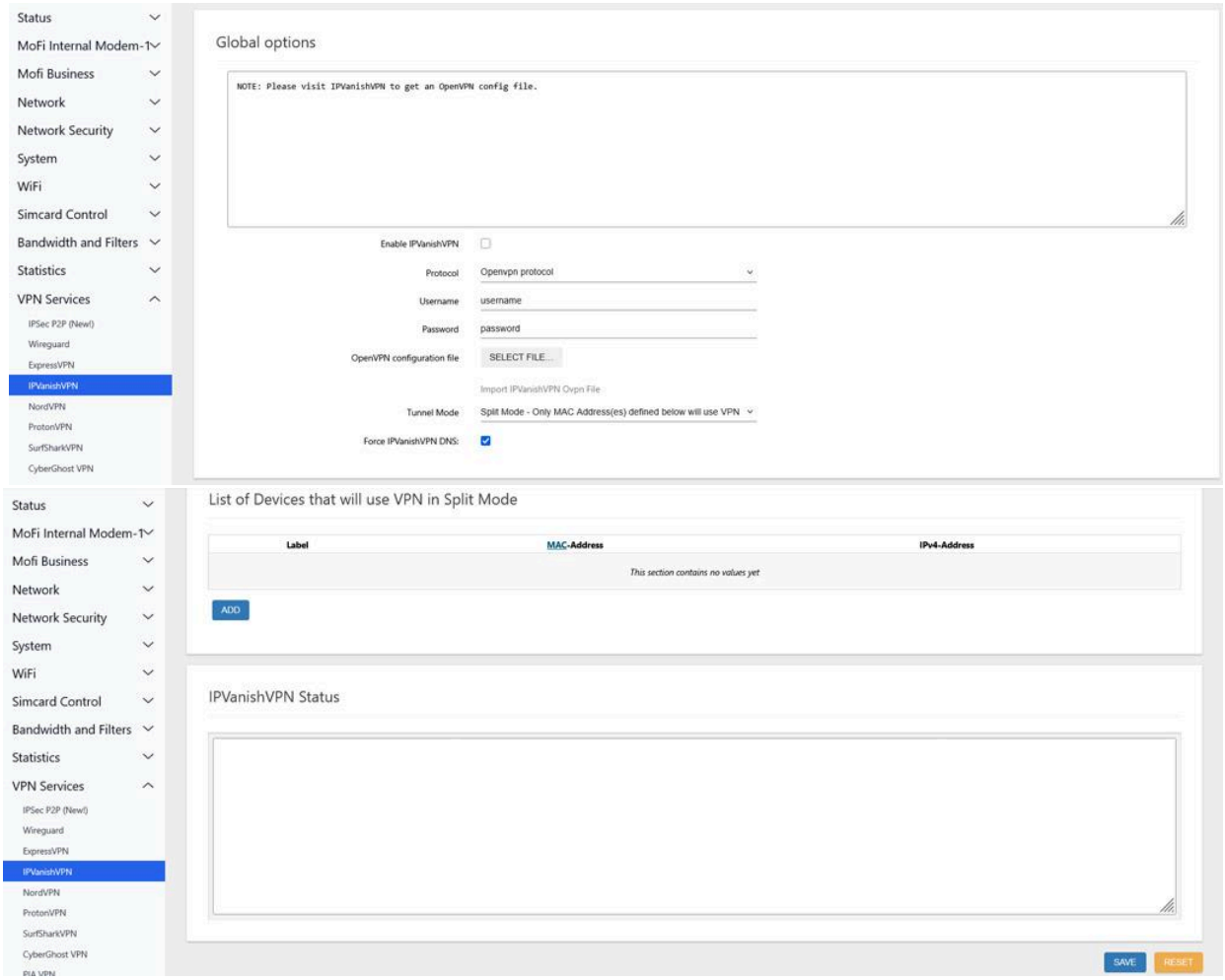
3. Go to nordvpn.com/servers/tools/ and find a recommended server (e.g., “us1234.nordvpn.com”)
4. On the router, navigate to VPN Services > NordVPN
5. Toggle **Enable NordVPN** to ON
6. Enter your **NordVPN service username**
7. Enter your **NordVPN service password**
8. Enter the **Server** hostname (e.g., us1234.nordvpn.com)
9. Set **Protocol** to “UDP” (faster) or “TCP” (more reliable)
10. Toggle **Force NordVPN DNS** to ON (prevents DNS leaks)
11. Select **Tunnel Mode**: “All Traffic” routes everything through VPN, or “Split Mode” to only route specific devices
12. Click **Save**
13. Check **NordVPN Status** — it should show “Connected” after 30-60 seconds



12.5 IPVanish VPN

Menu: Go to **VPN Services** → **IPVanishVPN** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/ipvanishvpn

Setting	Options	Description
Enable IPVanishVPN	Toggle	Activate or deactivate
Protocol	OpenVPN	VPN protocol
Username	Text	IPVanish credentials
Password	Text	IPVanish credentials
OpenVPN configuration file	File upload	Upload .ovpn file from IPVanish
Tunnel Mode	All Traffic / Split Mode by MAC	Route all or selected traffic
Force IPVanishVPN DNS	Toggle	Use IPVanish DNS servers

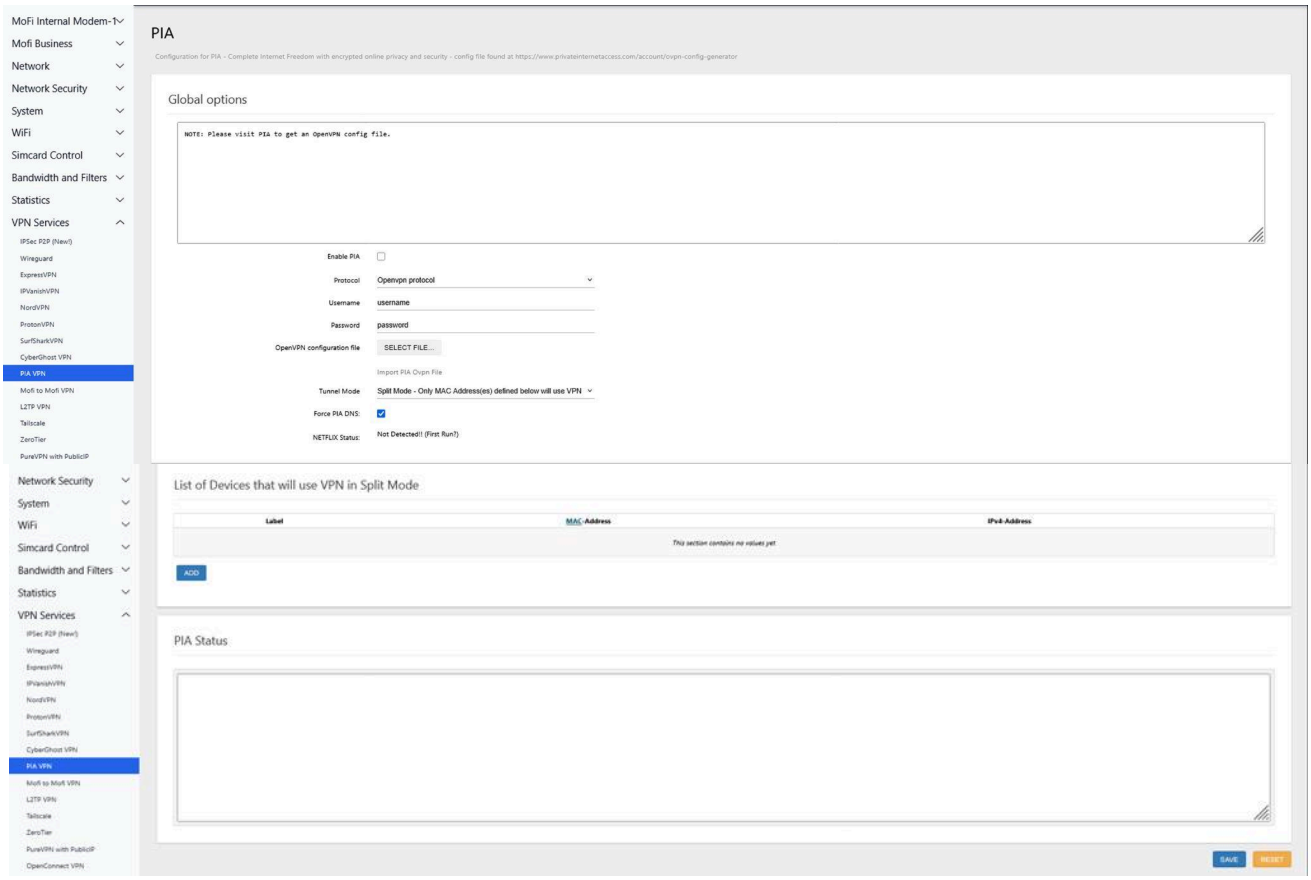


12.6 PIA (Private Internet Access) VPN

Menu: Go to **VPN Services** → **PIA VPN** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/pia

Setting	Options	Description
Enable PIA	Toggle	Activate or deactivate
Protocol	OpenVPN	VPN protocol
Username	Text	PIA credentials
Password	Text	PIA credentials
OpenVPN configuration file	File upload	Upload .ovpn file from PIA
Tunnel Mode	All Traffic / Split Mode by MAC	Route all or selected traffic
Force PIA DNS	Toggle	Use PIA DNS servers

NETFLIX Status: Detects if Netflix is accessible.



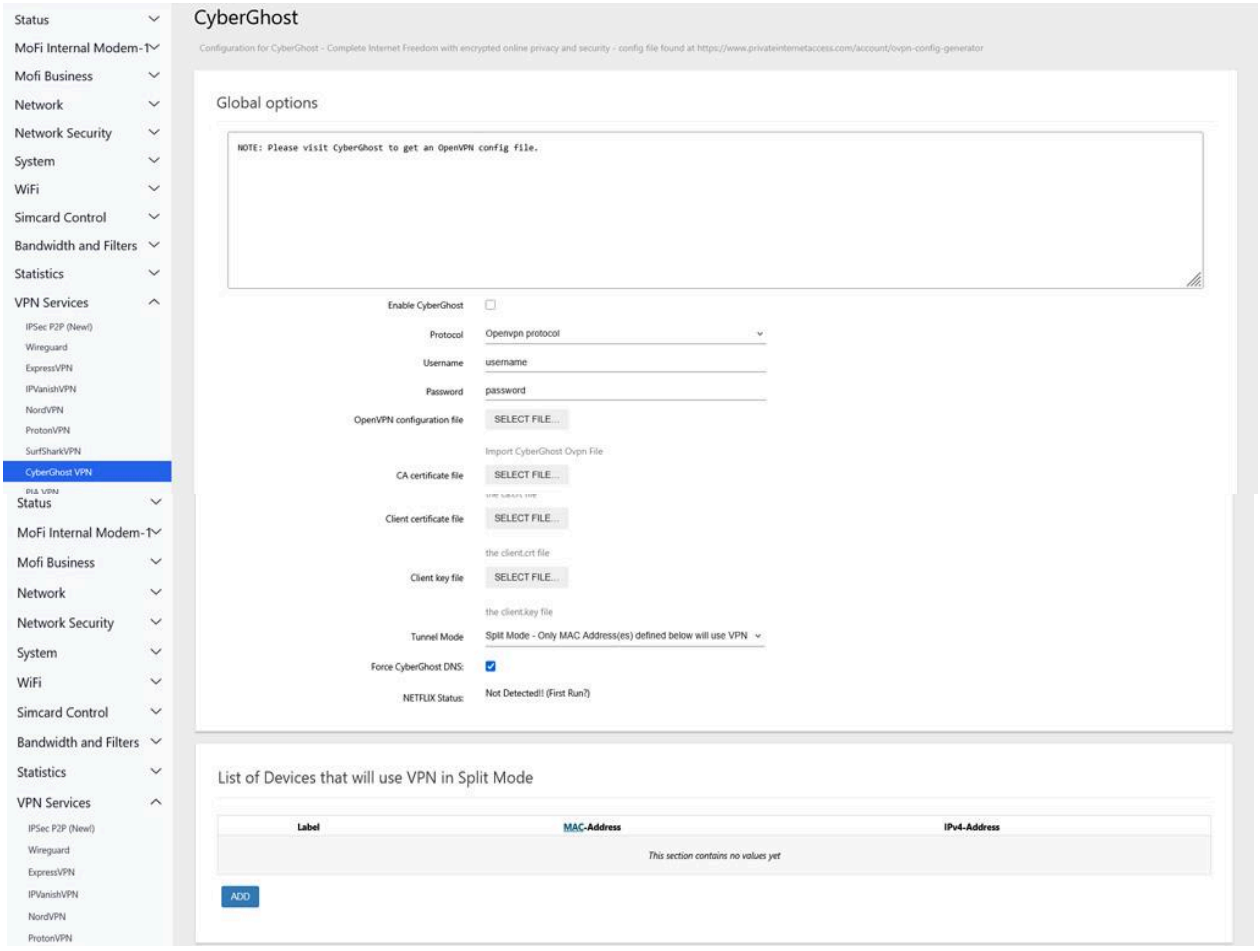
12.7 CyberGhost VPN

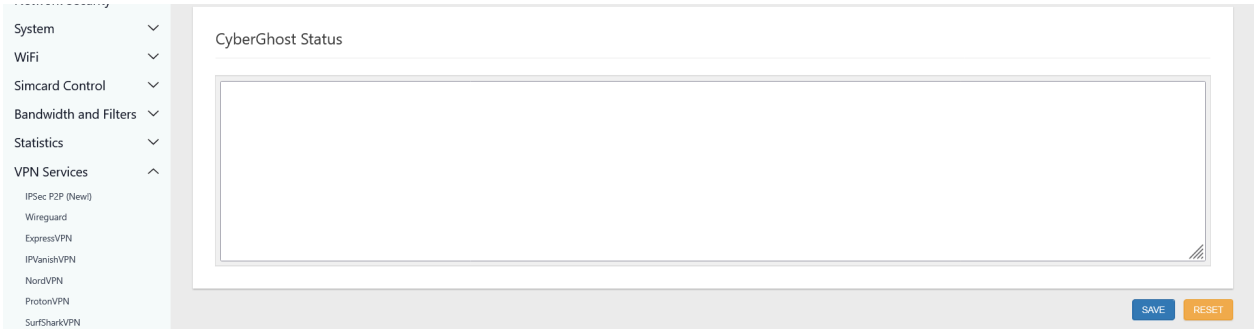
Menu: Go to **VPN Services** ⟶ **CyberGhost** or click on the line below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/cyberghost

Setting	Options	Description
Enable CyberGhost	Toggle	Activate or deactivate

Setting	Options	Description
Protocol	OpenVPN	VPN protocol
Username	Text	CyberGhost credentials
Password	Text	CyberGhost credentials
OpenVPN configuration file	File upload	Upload .ovpn file
CA certificate file	File upload	Upload ca.crt file
Client certificate file	File upload	Upload client.crt file
Client key file	File upload	Upload client.key file
Tunnel Mode	All Traffic / Split Mode by MAC	Route all or selected traffic
Force CyberGhost DNS	Toggle	Use CyberGhost DNS servers

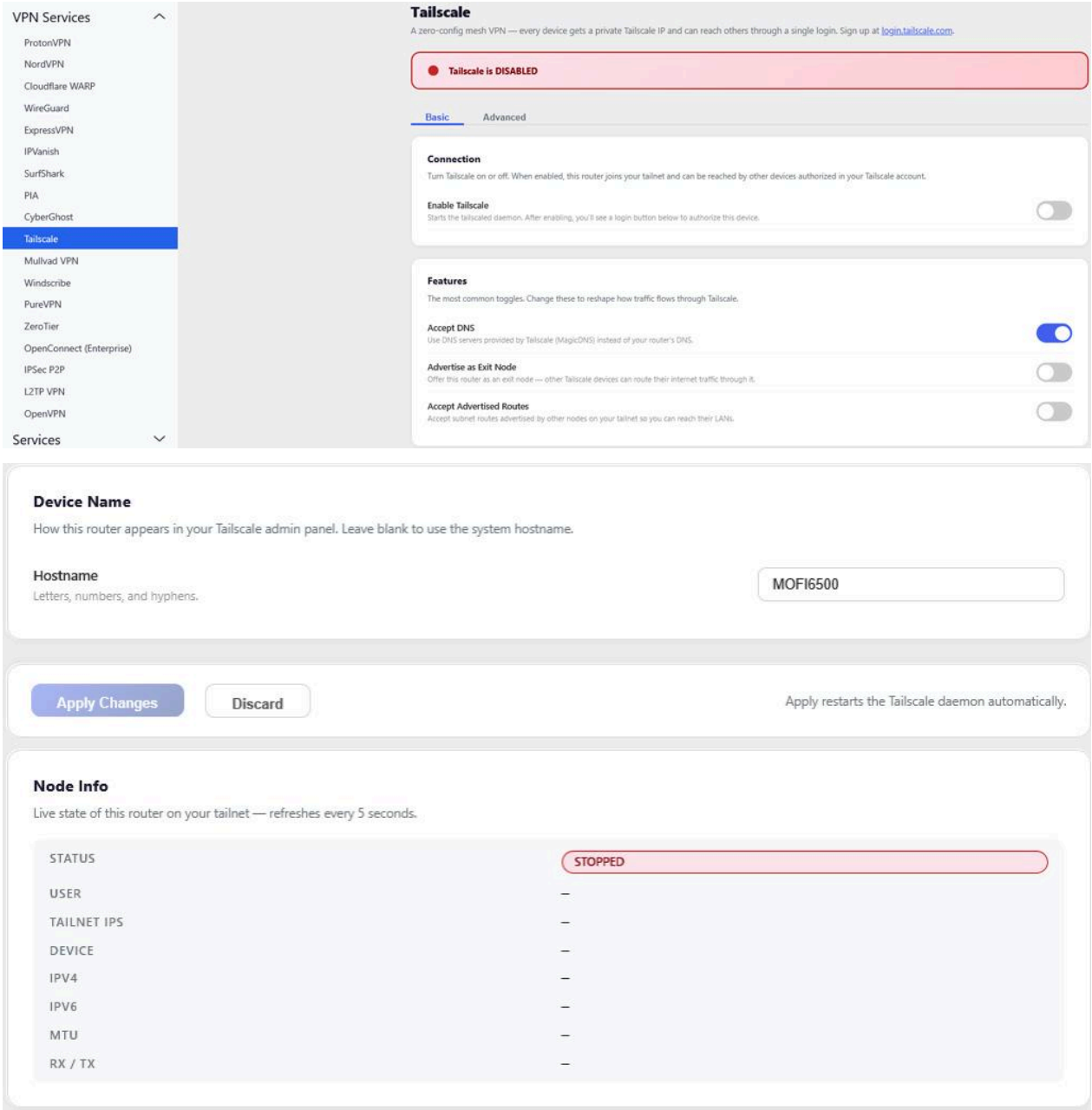
NETFLIX Status: Detects if Netflix is accessible.




System
WiFi
Simcard Control
Bandwidth and Filters
Statistics
VPN Services
IPSec P2P (New!)
Wireguard
ExpressVPN
IPVanishVPN
NordVPN
ProtonVPN
SurfSharkVPN
CyberGhost Status
SAVE
RESET

12.8 Tailscale VPN

Menu: Go to **VPN Services** → **Tailscale** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/tailscale

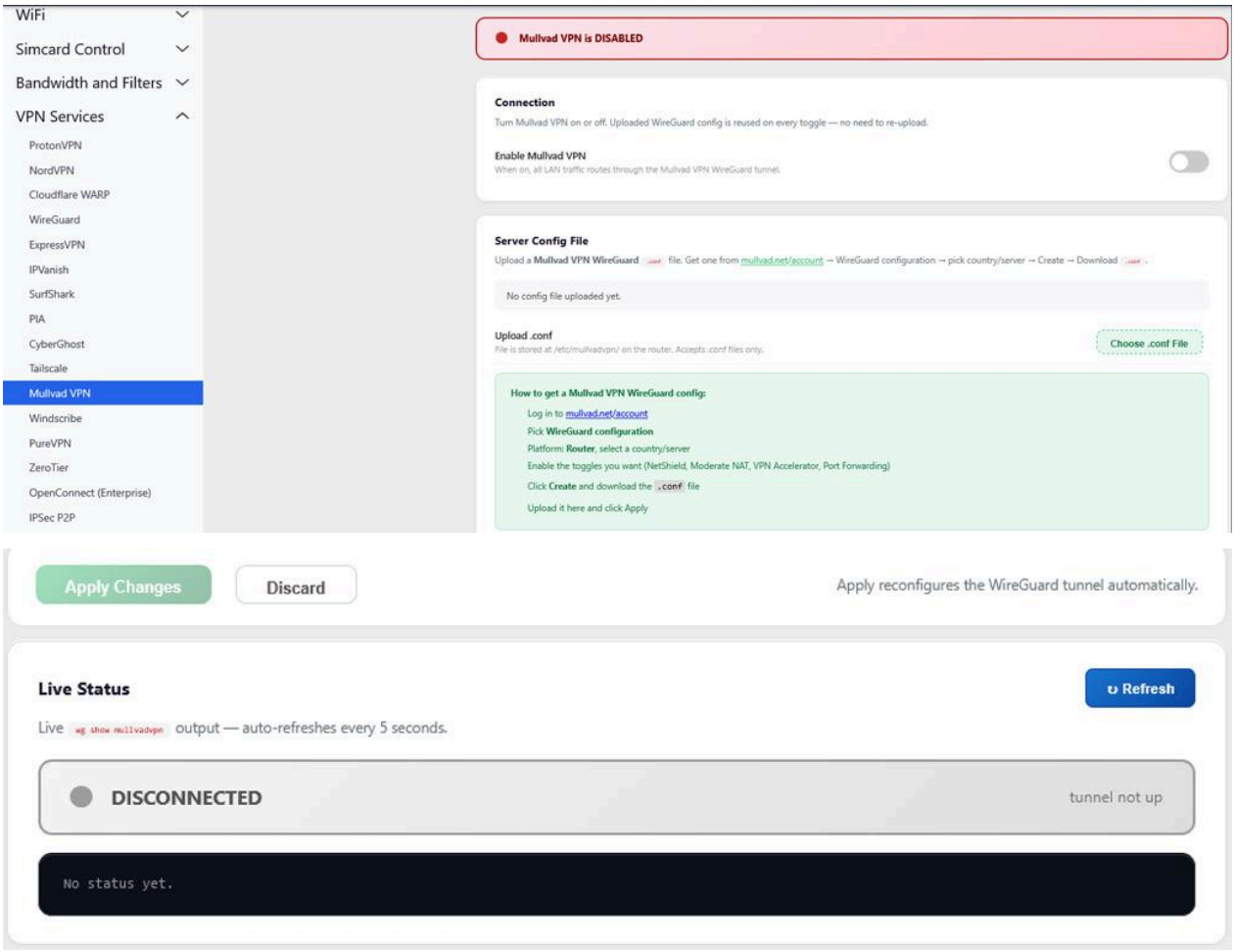


Mullvad VPN

Menu: Go to **VPN Service** → **Mullvad VPN** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/mullvad

Mullvad VPN

Mullvad VPN via WireGuard — faster, simpler, and more efficient than OpenVPN. Get a WireGuard `.conf` file from your Mullvad VPN account.

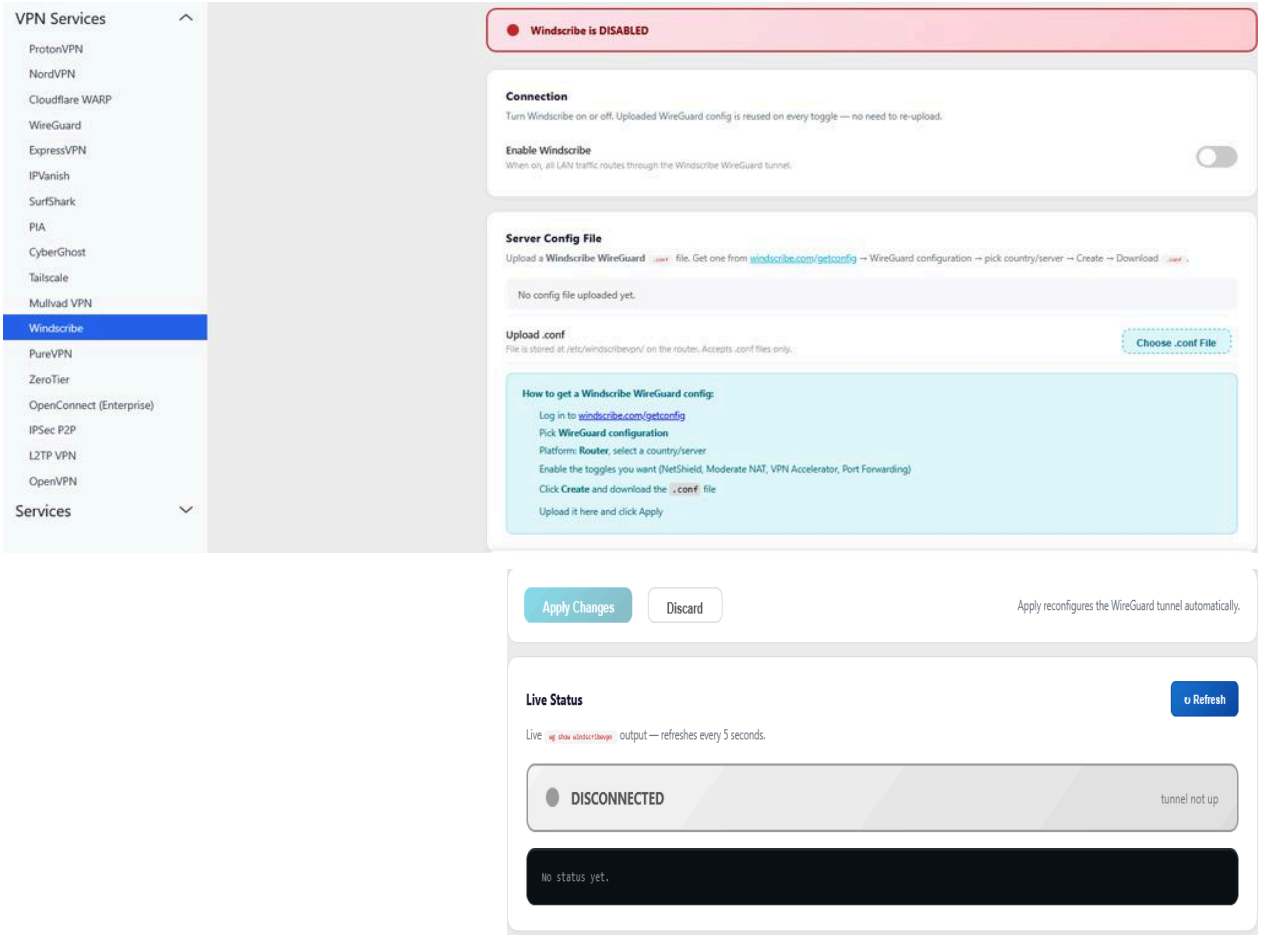


Windscribe VPN

Menu: Go to **VPN Services** → **Windscribe VPN** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/windscribe

Windscribe

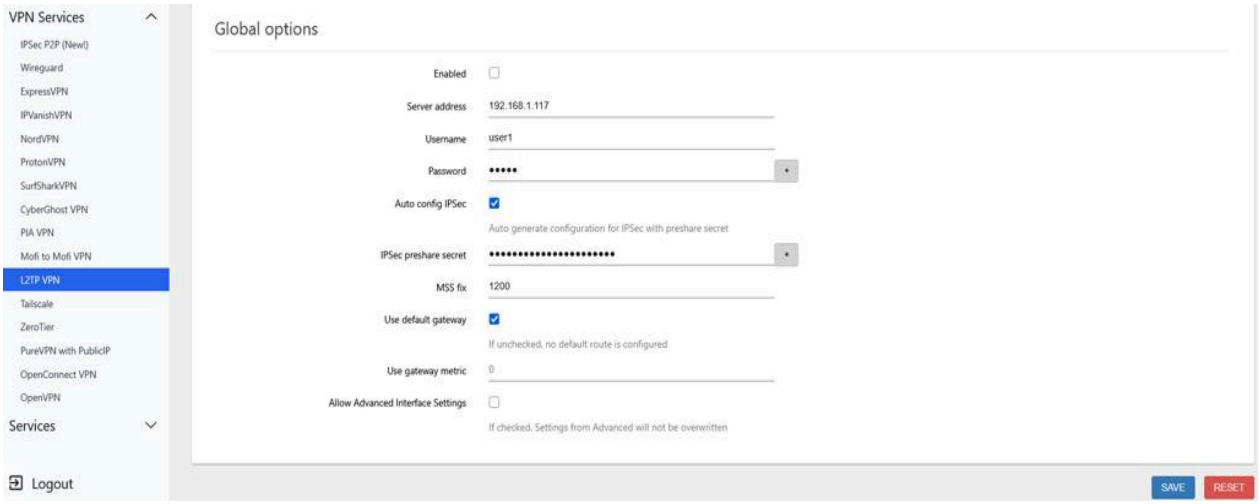
Windscribe via **WireGuard** — faster, simpler, and more efficient than OpenVPN. Get a WireGuard `.conf` file from your Windscribe account.



12.9 L2TP VPN

Menu: Go to **VPN Services** → **L2TP VPN** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/mofixl2tp

L2TP (Layer 2 Tunneling Protocol) VPN with optional IPSec encryption. Has two tabs: **Client L2TP VPN** and **Server L2TP VPN**.



Client L2TP VPN Tab

Setting	Options	Description
Enabled	Toggle	Enable the L2TP client
Server address	Text	Remote L2TP server IP or hostname
Username	Text	L2TP account username
Password	Text	L2TP account password
Auto config IPSec	Toggle	Automatically generate IPSec configuration
IPSec preshare secret	Text	Pre-shared key for IPSec encryption
MSS fix	Toggle	Enable TCP MSS clamping
Use default gateway	Toggle	Route all traffic through the L2TP tunnel. If unchecked, only traffic destined for the remote network uses the tunnel.
Use gateway metric	Numeric	Routing priority for the L2TP tunnel
Allow Advanced Interface Settings	Toggle	Prevent auto-overwrite of advanced settings

Server L2TP VPN Tab

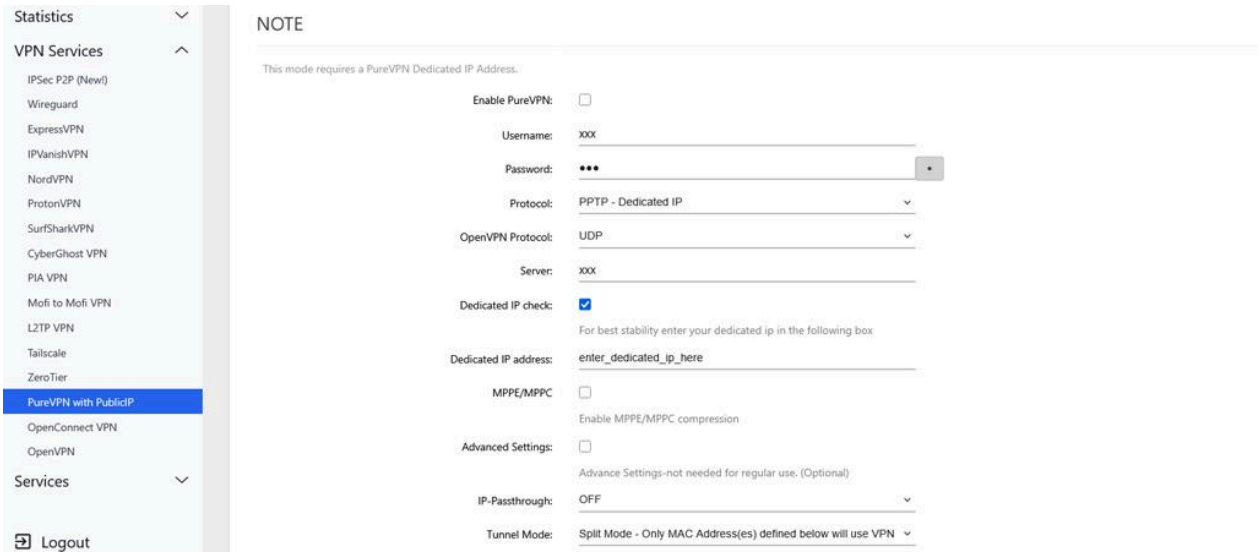
Setting	Options	Description
Enabled	Toggle	Enable the L2TP server
Port	Numeric (default: 1701)	L2TP listening port
Local IP	Text (e.g., 10.9.30.1)	Server's IP within the VPN tunnel
Remote IP range	Text (e.g., 10.9.30.2-100)	IP range to assign to connecting clients
Auto config IPSec	Toggle	Enable IPSec encryption
IPSec preshare secret	Text	Pre-shared key
MSS fix	Toggle	TCP MSS clamping

L2TP Client Accounts Table:

Column	Description
Username	Client account username
Password	Client account password
Assign IP	Fixed IP to assign to this client

12.10 PureVPN (with Public IP)

Menu: Go to **VPN Services** → **PureVPN** with PublicIP or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/purevpn



Setting	Options	Description
Enable PureVPN	Toggle	Activate or deactivate
Username	Text	PureVPN credentials
Password	Text	PureVPN credentials
Protocol	PPTP – Dedicated IP / OpenVPN	Connection protocol
OpenVPN Protocol	TCP / UDP	Sub-protocol when using OpenVPN
Server	Text	PureVPN server address
Dedicated IP address	Text	Your PureVPN dedicated IP (if applicable)
MPPE/MPPC	Toggle	Enable compression (PPTP only)
IP-Passthrough	Toggle	Pass VPN IP to a device
Tunnel Mode	All Traffic / Split Mode by MAC	Route all or selected traffic

Split Mode Device List includes DMZ option:

Column	Description
Label	Device name
MAC Address	Device MAC
IPv4 Address	Device IP
DMZ	Toggle — pass all VPN traffic to this device

12.11 OpenVPN

Menu: Go to **VPN Services > OpenVPN** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/openvpn

Full OpenVPN client and server configuration.

OpenVPN Instances Table: Shows configured VPN instances with Enabled, Started, Start/Stop, Port, and Protocol columns.

Add New Instance:

Field	Description
Instance Name	Unique name for this VPN instance
Template	Pre-configured template (see options below)

Template Options: - Client configuration for an ethernet bridge VPN - Client configuration for a routed multi-client VPN - Simple client configuration for a routed point-to-point VPN - Server configuration for an ethernet bridge VPN - Server configuration for a routed multi-client VPN - Simple server configuration for a routed point-to-point VPN

Upload OVPN File: Alternatively, upload a pre-configured .ovpn file: - Enter an **Instance Name** - Select the .ovpn file using the file upload button

---

12.12 OpenConnect VPN

Menu: Go to **VPN Services → OpenConnect VPN** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/openconnect-client

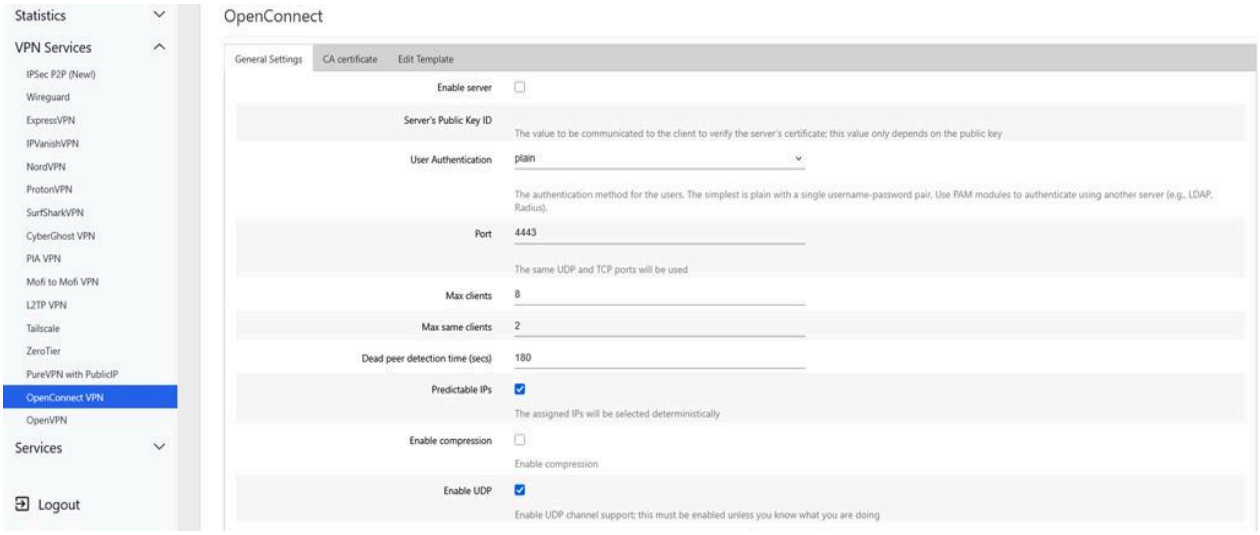
OpenConnect VPN server (compatible with Cisco AnyConnect clients). Has two tabs: **Server Settings** and **User Settings**.

Server Settings Tab

Setting	Options	Description
Enable server	Toggle	Start the OpenConnect VPN server
Server's Public Key ID	Text	Communicated to clients to verify server certificate
User Authentication	plain / PAM	Authentication method
Port	Numeric	Same port used for both TCP and UDP
Max clients	Numeric	Maximum simultaneous connections
Max same clients	Numeric	Max connections from the same user
Dead peer detection time	Seconds	Timeout for inactive peers
Predictable IPs	Toggle	Assign deterministic IPs based on username
Enable compression	Toggle	Compress tunnel traffic
Enable UDP	Toggle	Enable UDP channel (recommended)
AnyConnect client compatibility	Toggle	Support Cisco AnyConnect clients
Enable proxy arp	Toggle	Provide addresses from LAN subnet
VPN IPv4-Network-Address	Text	Tunnel subnet (e.g., 10.10.10.0)
VPN IPv4-Netmask	255.255.255.0 / 255.255.0.0 / 255.0.0.0	Tunnel subnet mask
VPN IPv6-Network-Address	CIDR	IPv6 tunnel subnet

DNS servers table: Add DNS servers to push to VPN clients. **Routing table:** Add routes to push to VPN clients.

CA certificate and **Edit Template** links for SSL/TLS configuration.



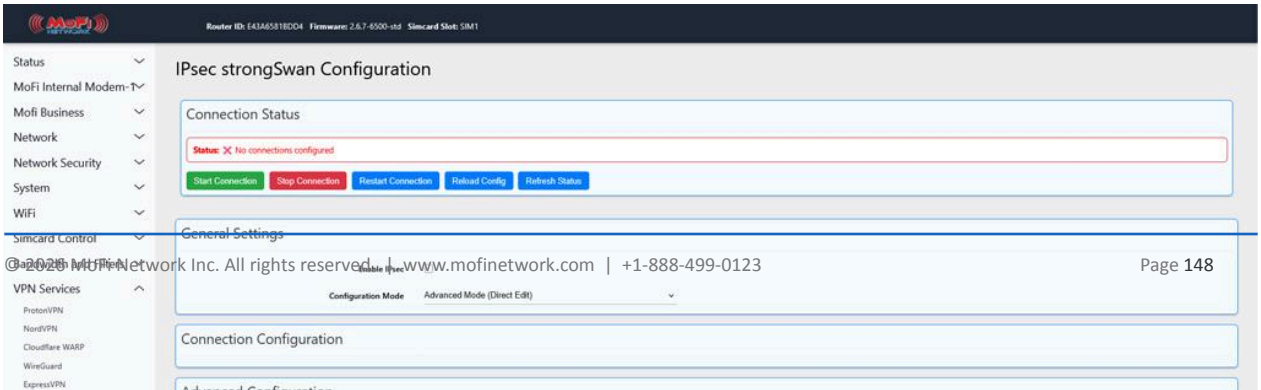
User Settings Tab

Active Users Table:

Column	Description
ID	Session ID
Username	Connected user
Group	User group
IP	Real IP
VPN IP	Assigned tunnel IP
Device	Client device type
Time	Connection duration
Cipher	Encryption in use
Status	Connection status

IPSEC P2P

Menu: Go to **VPN Services > IPsec P2P** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/vpnservice/ipsec-js



13. Bandwidth and Filters (Review)

This section covers all pages under the **Bandwidth and Filters** menu.

13.1 Internet Usage Set Date

Menu: Go to **Bandwidth and Filters** → **Internet Usage Set Date** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/parental/data-usage

Set the billing cycle reset date for bandwidth usage tracking.

Setting	Options	Description
Day of Reset	1-31	Day of the month when usage counters reset

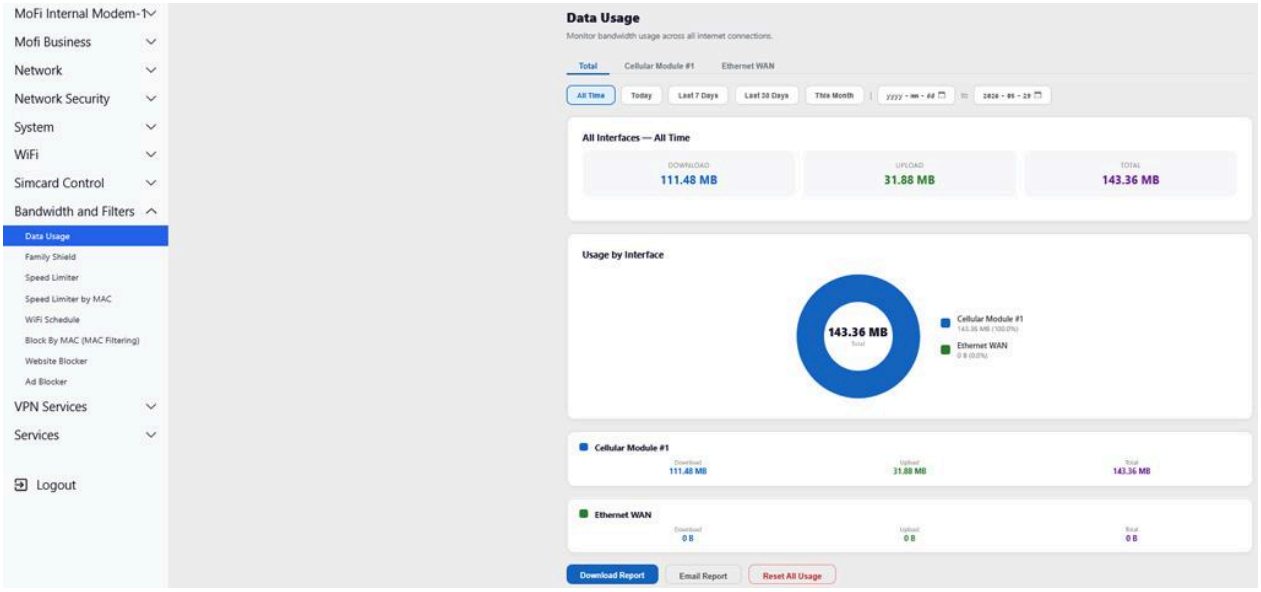
Note: Setting this date will reset the current usage database. Click **Save** to apply.

13.2 Internet Usage

Menu: Go to **Bandwidth and Filters** → **DataUsage** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/parental/data-usage

View bandwidth consumption per device on your network for the current billing period.

- **Usage Table:** Shows download and upload data per device (hostname, IP, MAC address)
- **Reset** button to clear current usage counters



13.3 MoFi Family Shield

Menu: Go to **Bandwidth and Filters** → **Mofi Family Shield** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/parental/family-shield

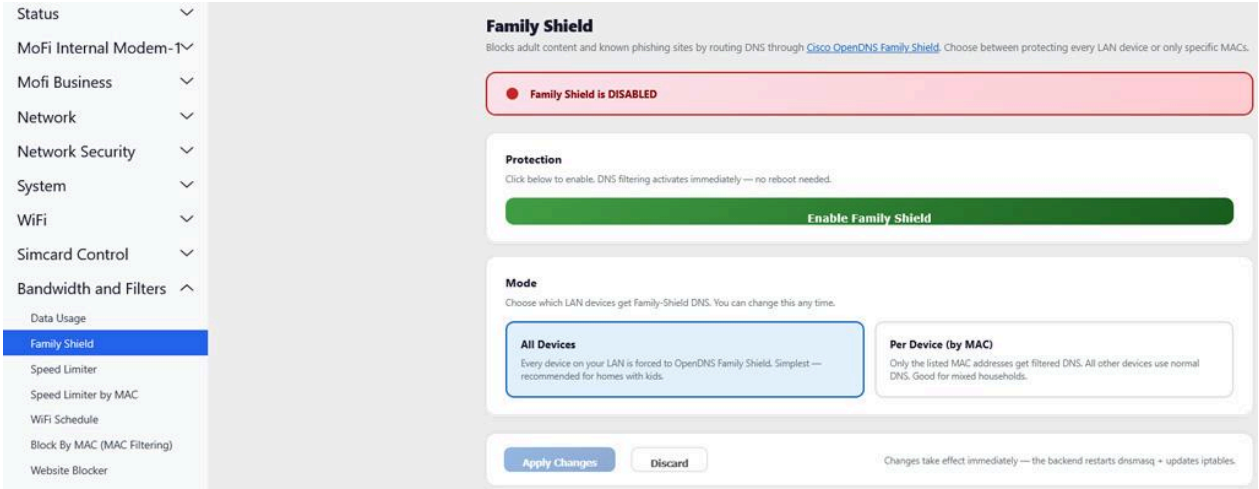
DNS-based content filtering powered by Cisco OpenDNS. Blocks inappropriate content, adult websites, and known malicious domains.

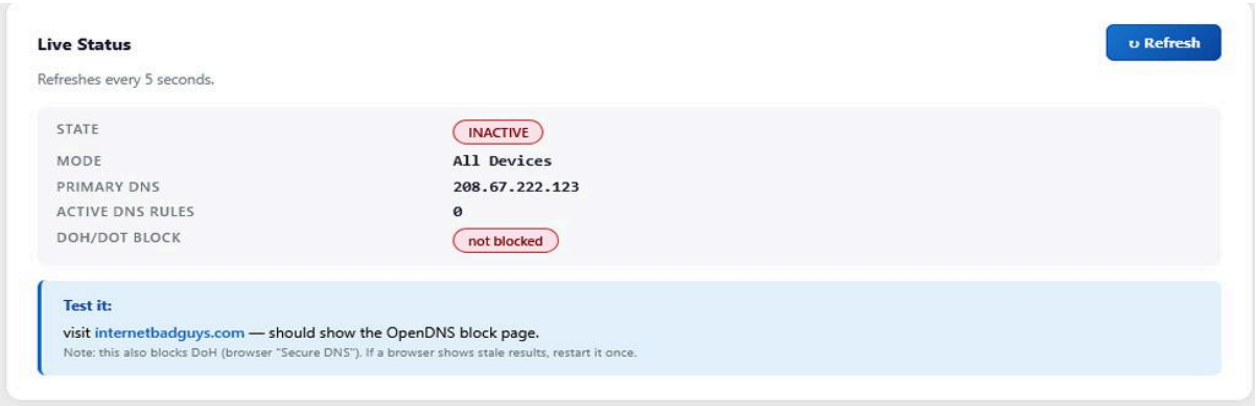
Setting	Options	Description
Apply Family Shield to All Devices	Checkbox	Force all devices on the network to use OpenDNS Family Shield DNS servers
Family Shield by MAC Only	Toggle	Apply filtering only to specific devices (by MAC address) instead of all devices

Per-Device Table (when using MAC mode):

Column	Description
Name	Device name/label
MAC Address	Device MAC
IP address	Device IP
Enable	Checkbox to enable filtering for this device

Click **Add** to add devices. Click **Apply Changes**





13.4 Bandwidth Monitoring (This is not in the GUI)

Menu: Bandwidth and Filters > Bandwidth Monitoring **URL:** `/cgi-bin/luci/admin/parental/monitor`

Track total bandwidth usage per interface and optionally block the internet when a threshold is exceeded.

Global Settings:

Setting	Options	Description
Enabled	Checkbox	Enable bandwidth monitoring
Track interfaces	WAN / Module1 / Module2 checkboxes	Which connections to monitor
Reset Time	Daily Basis / Monthly Basis	How often usage counters reset
Reset Hour	Every Hour / specific hour	What time to reset
Internet block on exceeded bandwidth	Toggle	Block internet access when threshold is exceeded

Setting	Options	Description
Bandwidth Threshold	Numeric	The usage limit
Unit	KB / MB / GB	Unit for the threshold

Bandwidth Usage Totals (display only): - Uploaded, Downloaded, Total, Previous Period

Internet Block Status: Shows whether the internet is currently blocked due to exceeded bandwidth (Active / Inactive).

Button: Reset Usage Database

Individual User Bandwidth Table:

Column	Description
User IP	Device IP address
MAC	Device MAC address
Upload	Upload data used
Download	Download data used
Total	Combined usage

User Limits Section:

Setting	Options	Description
Enabled	Toggle	Enable per-user limits
Policy	Allow All / Block All	Default policy for unlisted users
Auto Limit	Toggle	Automatically apply limits

User Bandwidth Configuration Table:

Column	Description
Hostname	Device name
MAC	Device MAC
Bandwidth Limit	Maximum allowed bandwidth
Limit Size	Unit (KB/MB/GB)
Action	What to do when limit is reached
Throttle Up/Down kbps	Speed throttle values
Reset	Reset this user's counter
Status	Current status

13.5 Speed Limiter

Menu: Go to **Bandwidth and Filters** → **Speed Limiter** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/parental/blimits-js

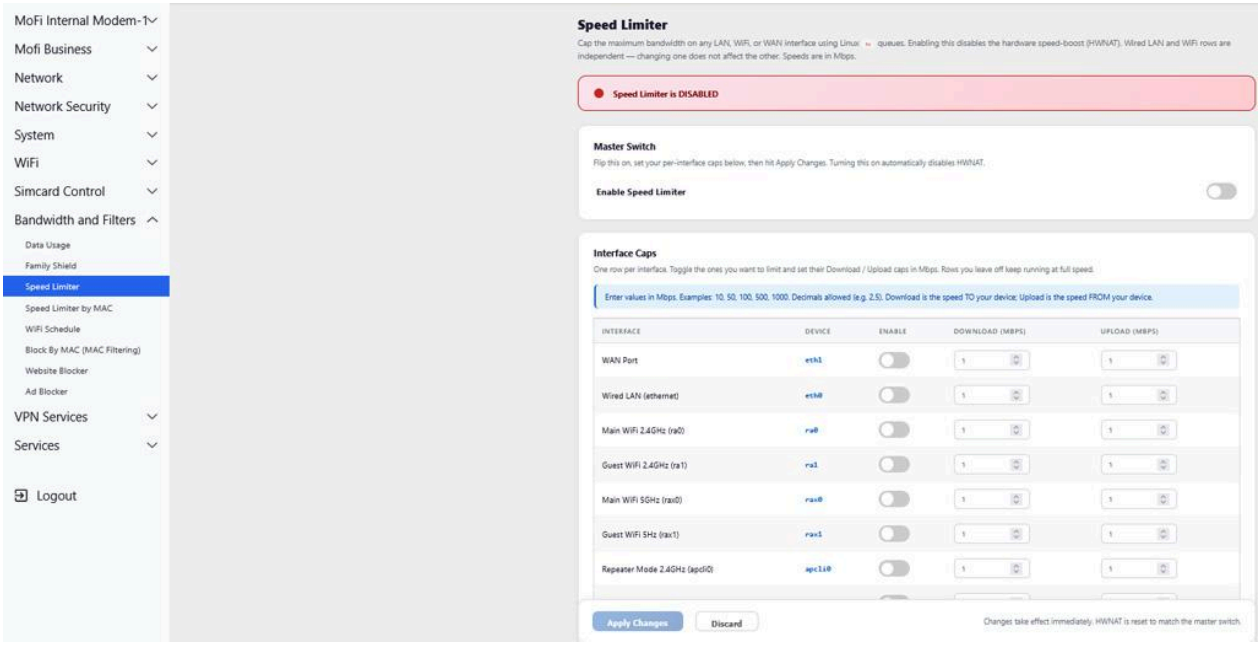
Limit upload and download speeds per WiFi interface.

Setting	Options	Description
Master Enable	Toggle OFF/ON	Enable or disable all speed limits

Interfaces Table:

Column	Description
Description	Interface name (Main WiFi 2.4GHz, Main WiFi 5GHz, Guest 2.4GHz, Guest 5GHz, LAN)
Interface	Technical interface name
Enabled	Toggle ON/OFF per interface
Upload Limit	Maximum upload speed in kbps
Download Limit	Maximum download speed in kbps

Buttons: Save, Reset



Step-by-Step: Limiting Guest WiFi to 10 Mbps:
1. Navigate to Bandwidth and Filters > Speed Limiter
2. Toggle **Master Enable** to ON
3. Find “Guest WiFi 2.4GHz” in table

4. Set its **Enabled** to ON
5. Set **Download Limit** to 10000 (kbps = 10 Mbps)
6. Set **Upload Limit** to 5000 (kbps = 5 Mbps)
7. Repeat for “Guest WiFi 5GHz” 8. Click **Save**
9. All guest WiFi users are now limited to
10 Mbps download / 5 Mbps upload

13.6 Speed Limiter by MAC

Menu: Go to **Bandwidth and Filters** → **Speed Limiter by MAC** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/parental/mac_bw_limit

Set individual speed limits for specific devices by their MAC address.

Setting	Description
Enable MAC Speed Limiter	Checkbox to enable per-device speed limiting

Users Table:

Column	Description
Enabled	Checkbox per device
MAC Address	Dropdown showing connected devices
Upload Limit (kbps)	Maximum upload speed
Download Limit (kbps)	Maximum download speed

13.7 WiFi Schedule

Menu: Go to **Bandwidth and Filters** → **Wifi Schedule** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/parental/wifi_schedule

Schedule WiFi to automatically turn on and off at specific times.

Setting	Description
Enable Wifi Schedule	Toggle to enable/disable the scheduler

Schedule Table:

Column	Description
Day of week	Monday through Sunday
Start Time	Hour:minute when the rule begins
End Time	Hour:minute when the rule ends
WiFi Network	Which SSID is affected

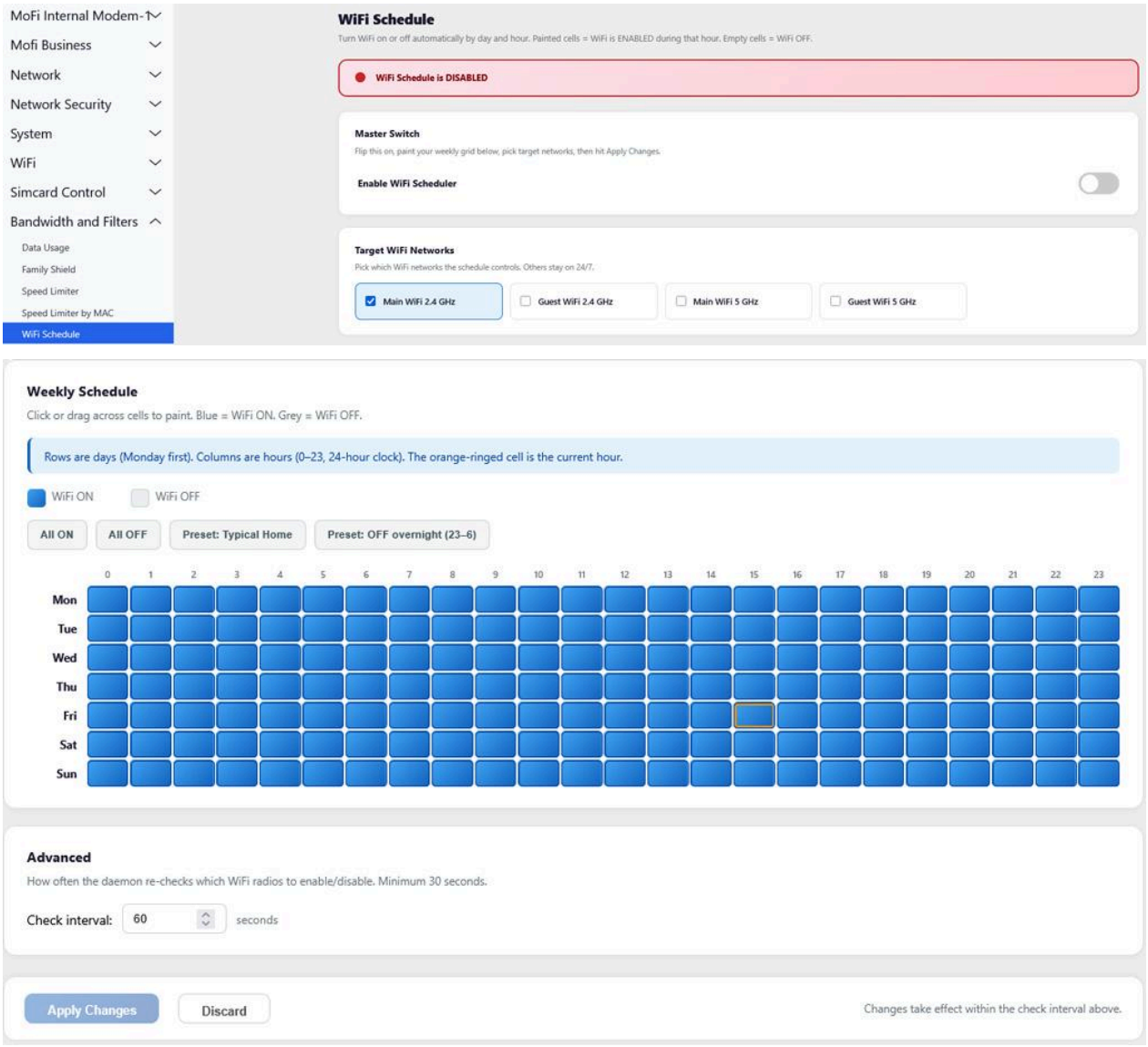
Column	Description
Action	Enable WiFi / Disable WiFi during this period

Click **Add** to create new schedule entries. Click **Save & Apply** to activate.

Step-by-Step: Disabling WiFi at Night (10 PM - 6 AM):
1. Navigate to Bandwidth and Filters > Wifi Schedule
2. Toggle **Enable Wifi Schedule** to ON
3. Click **Add** to create a new schedule entry
4. Set **Day of week** to every day you want (e.g., Monday through Sunday)
5. Set **Start Time** to 22:00 (10 PM)
6. Set **End Time** to 06:00 (6 AM)
7. Select the **WiFi Network** to affect (e.g., Main WiFi 2.4GHz)
8. Set **Action** to “Disable WiFi”
9. Repeat steps 3-8 for other WiFi networks (Main 5GHz, Guest, etc.)
10. Click **Save & Apply**

Step-by-Step: Business Hours Only Guest WiFi (OFF after 6 PM):
1. Navigate to Bandwidth and Filters > Wifi Schedule
2. Toggle **Enable Wifi Schedule** to ON
3. Click **Add** to create an “after hours” rule
4. Set days to Monday through Sunday
5. Start Time: 18:00, End Time: 07:59 6. WiFi Network: Guest 2.4GHz
7. Action: “Disable WiFi” (guest WiFi turns off at 6 PM, back on at 8 AM)
8. Repeat steps 3-7 for Guest 5GHz
9. Click **Save & Apply**
10. Test by checking that guest WiFi is available during business hours and disabled after 6 PM

Use Cases: - Automatically disable WiFi at bedtime (e.g., 10 PM - 6 AM) - Turn off guest WiFi during non-business hours - Limit children’s internet access to specific hours



13.8 Block by MAC (MAC Filtering)

Menu: Go to **Bandwidth and Filters** → **Block By MAC** or click on the line below:
http://192.168.10.1/cgi-bin/luci/admin/parental/wifi_schedule_adv

Control internet access by device MAC address.

Setting	Options	Description
Enable MAC Filtering	Toggle	Enable or disable MAC-based filtering
Filter Mode	Blacklist / Whitelist	**Blacklist:** Allow all devices, block listed MACs. **Whitelist:** Block all devices, allow only listed MACs.

Device List Table:

Column	Description
Label / Device Name	Friendly name
MAC Address	Device MAC
Enabled	Toggle per device

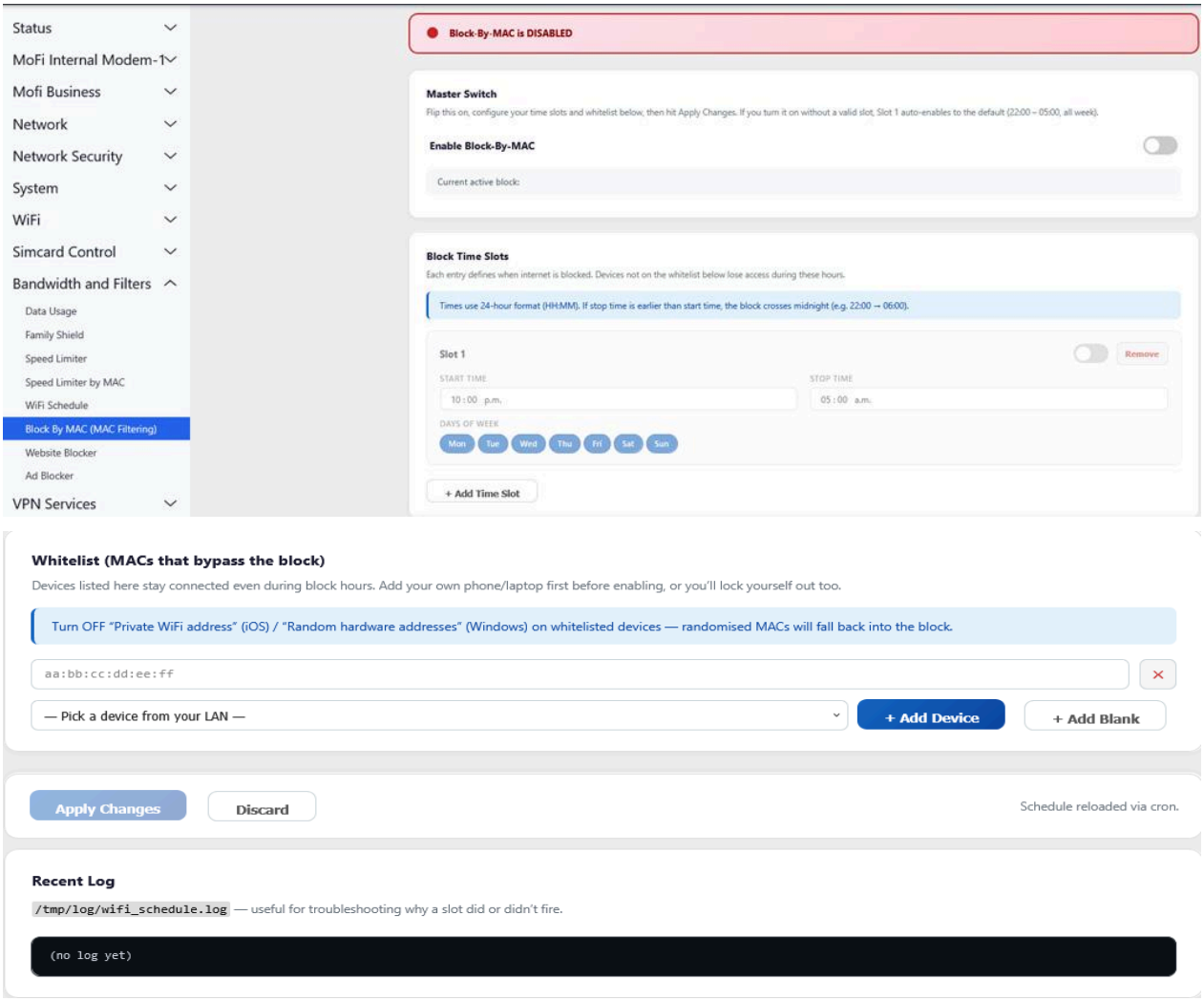
Click **Add** to add devices. Click **Save & Apply** to activate.

Step-by-Step: Blocking a Specific Device from the Internet:

1. Navigate to Bandwidth and Filters > Block By MAC
2. Toggle **Enable MAC Filtering** to ON
3. Set **Filter Mode** to “Blacklist” (block specific devices)
4. Click **Add**
5. Enter a **Label** (e.g., “Old Laptop”)
6. Enter the device’s **MAC Address** (find it in Status > Active Connections or the device’s network settings)
7. Toggle **Enabled** to ON
8. Click **Save & Apply**
9. That device will no longer be able to access the internet

Step-by-Step: Allowing Only Approved Devices (Whitelist):

1. Navigate to Bandwidth and Filters > Block By MAC
2. Toggle **Enable MAC Filtering** to ON
3. Set **Filter Mode** to “Whitelist” (only listed devices get internet)
4. Click **Add** for each approved device
5. Enter each device’s MAC address and toggle **Enabled** to ON
6. Click **Save & Apply**
7. Only the listed devices will have internet — all others are blocked



13.9 Website Blocker

Menu: Go to **Bandwidth and Filters** → **Website Blocker** or click on the line below:
http://192.168.10.1/cgi-bin/luci/admin/parental/website-blocker

Block access to specific websites for all devices on your network.

Setting	Options	Description
Enable Website Blocker	Toggle	Turn website blocking on or off
Block Policy	Blacklist / Whitelist	**Blacklist:** All sites work normally, listed domains are blocked. **Whitelist:** All sites are blocked, only listed domains are allowed.

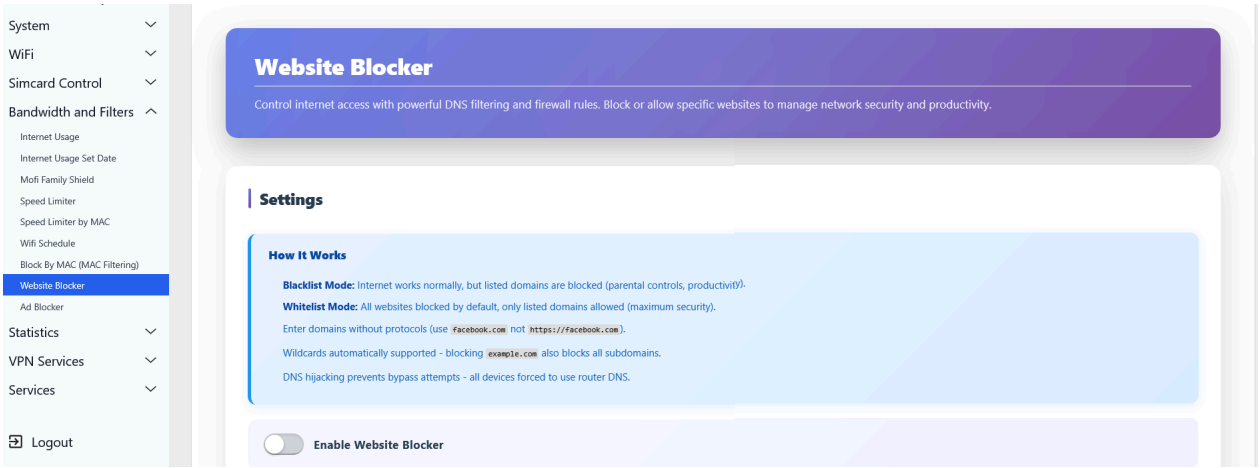
Domain List: Large text area for entering domains (one per line): - Lines starting with # are treated as comments - Blank lines are allowed for organization - Shows current count: “X domains in list”

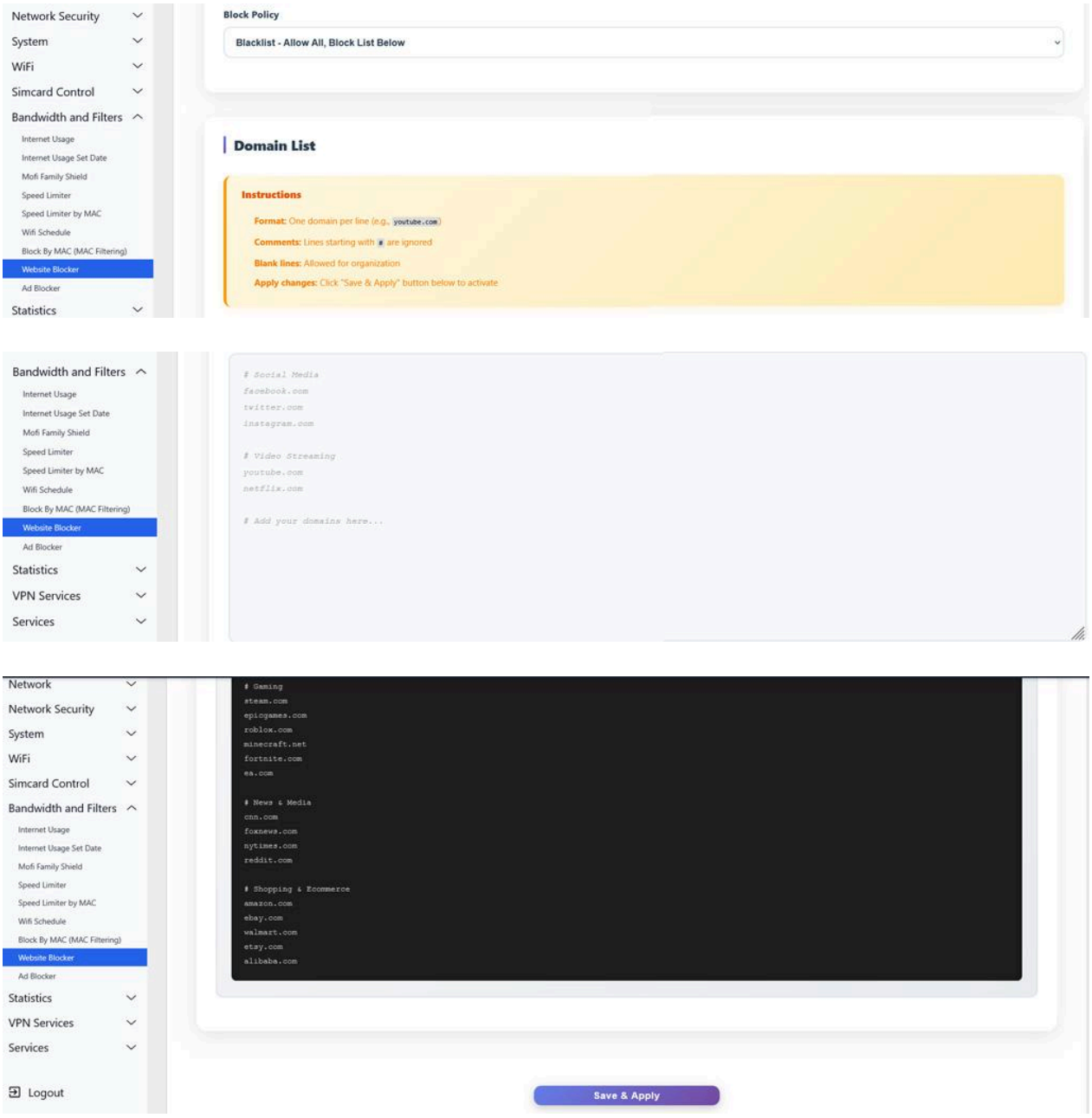
How It Works: - Blocking `example.com` automatically blocks all subdomains (e.g., `www.example.com`, `mail.example.com`) - DNS hijacking prevents bypass — all devices are forced to use the router’s DNS - Pre-filled example categories include: social media, video streaming, gaming, news, shopping domains

Click **Save & Apply** to activate changes.

Step-by-Step: Blocking Social Media and Streaming Sites:
1. Navigate to Bandwidth and Filters > Website Blocker
2. Toggle **Enable Website Blocker** to ON
3. Set **Block Policy** to “Blacklist” (allow all, block specific sites)
4. In the Domain List text area, enter one domain per line: `facebook.com` `instagram.com` `tiktok.com` `youtube.com` `netflix.com` `twitter.com` 5. Click **Save & Apply** 6. All devices on the network will now be blocked from accessing these sites

Step-by-Step: Creating a Kids-Only Whitelist:
1. Navigate to Bandwidth and Filters > Website Blocker
2. Toggle **Enable Website Blocker** to ON
3. Set **Block Policy** to “Whitelist” (block all, allow specific sites)
4. Enter only the approved sites in the Domain List: `google.com` `wikipedia.org` `khanacademy.org` `pbskids.org` 5. Click **Save & Apply** 6. Only the listed sites will be accessible — everything else is blocked





13.10 Ad Blocker

Menu: Go to **Bandwidth and Filters** → **Ad Blocker** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/parental/adblock

Network-wide ad blocking. When enabled, ads are blocked for all devices without requiring software on each device.

Status Panel (display only): - Status: Disabled / Enabled - Blocked Lists: count of active lists - Force DNS: Yes / No

Configuration:

Setting	Options	Description
Enable Ad Blocker	Toggle	Turn ad blocking on or off
Force DNS to Router	Toggle	Force all devices to use the router's DNS (prevents bypass via custom DNS settings on devices). Recommended: ON.
Update Lists Now	Button	Download the latest versions of all enabled ad-blocking lists

Ad Blocking Source Lists:

List Name	Description	Approx. Entries
ADAWAY	Focus on mobile ads	~400
SOCIAL	Blocks Facebook, Twitter, Myspace, LinkedIn, Classmates	Varies
BLACKLIST	Static local domain blacklist (always deny)	Custom
DISCONNECT	Mozilla content blocklist	~6,500
MALWARE	Broad malware domain blocklist	~16,000
MALWARELIST	Generic malware blocklist	~1,500
OPENPHISH	Focus on phishing domains	~1,800
ROLIST	Romanian ad-related domains + easylist	~600
RUADLIST	Russian ad-related domains + easylist	~2,000
SHALLA	Broad blocklist (ads, costtraps, spyware, trackers, warez)	~32,000
SPAM404	Suspicious domains	~5,000
SYSCTL	Ad-related domains	~21,000
WHOCARESABOUT	Broad suspicious domain blocklist	~12,000
WINHELP	Broad suspicious domains	~15,000
YOYO	Ad-related domains	~2,500

Enable/disable each list individually using the toggle next to each name.

Whitelist: Text area for domains that should NOT be blocked (one per line, no `http://`). Use this if ad blocking breaks a specific website.

Custom Blacklist: Text area for additional domains to block beyond the standard lists (one per line, no `http://`).

Bypass Devices: Devices that will NOT have ads blocked:

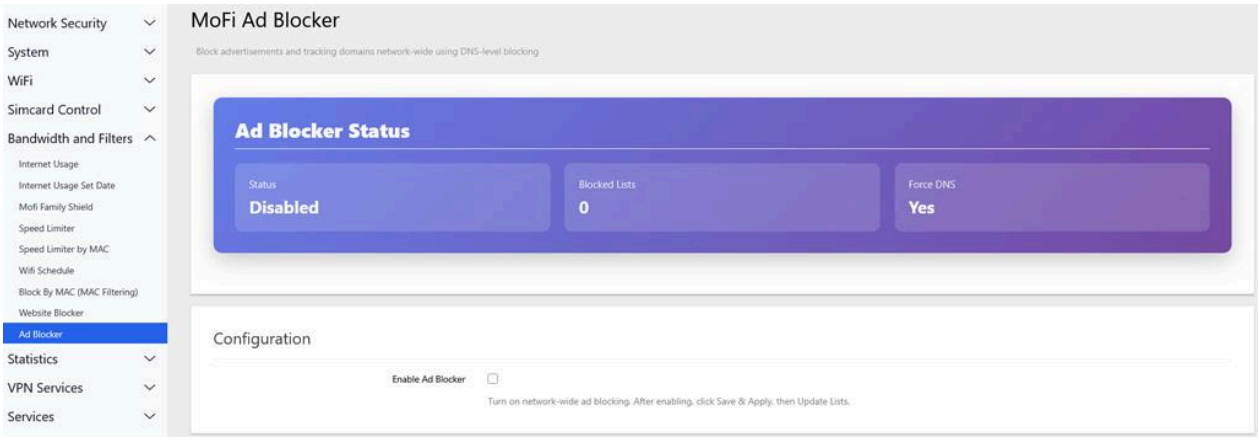
Column	Description
Device Name	Friendly name
MAC Address	Device MAC
Enabled	Toggle

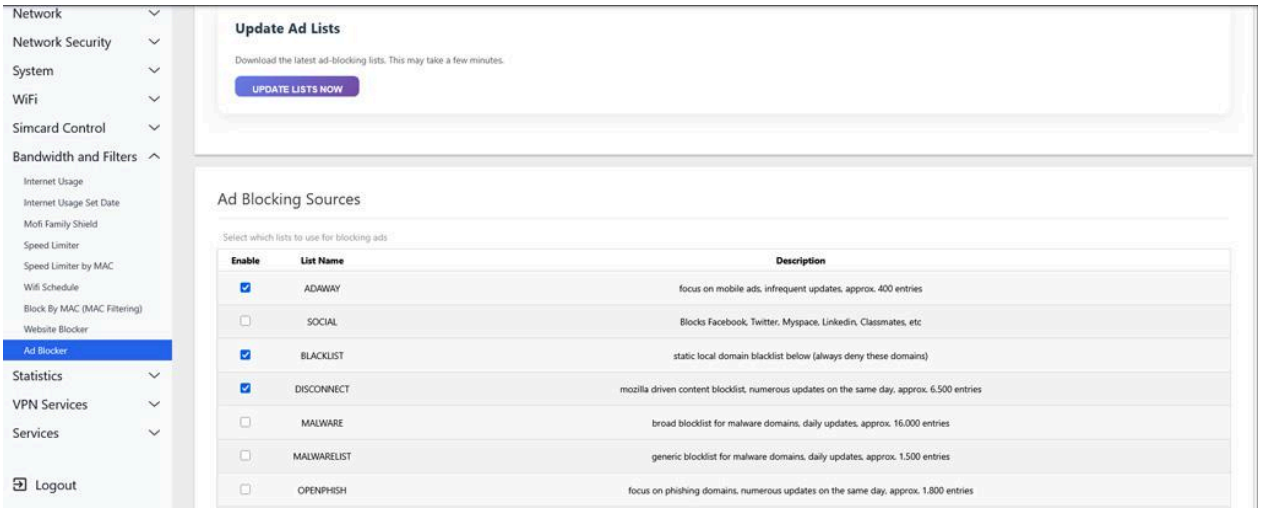
Click **Add** to add bypass devices. Click **Save** to apply.

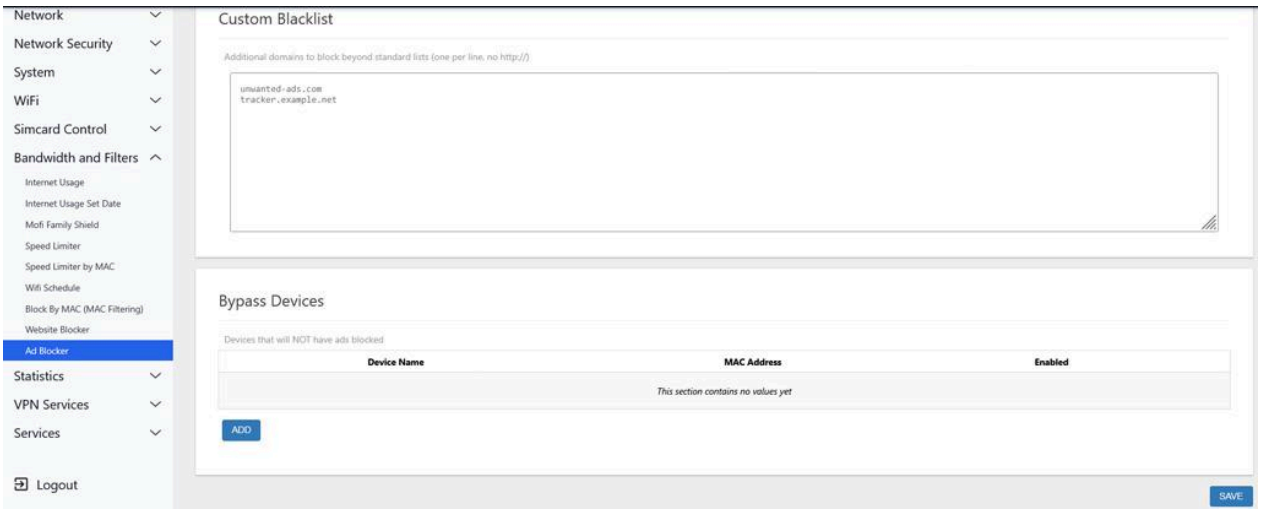
Step-by-Step: Enabling Network-Wide Ad Blocking:
1. Navigate to Bandwidth and Filters > Ad Blocker
2. Toggle **Enable Ad Blocker** to ON
3. Toggle **Force DNS to Router** to ON (important — prevents devices from bypassing the ad blocker using their own DNS)
4. Enable the ad blocking lists you want: - **YOYO** — Good general-purpose ad list (~2,500 domains) - **DISCONNECT** — Mozilla's content blocklist (~6,500 domains) - **MALWARE** — Blocks known malware domains (~16,000 domains)
5. Click **Update Lists Now** to download the latest blocklists
6. Click **Save**
7. Ads will now be blocked across all devices on the network

Step-by-Step: Whitelisting a Website That Ad Blocking Breaks:
1. Navigate to Bandwidth and Filters > Ad Blocker
2. Scroll down to the **Whitelist** text area
3. Enter the domain that's not working properly (e.g., `example.com`)
4. Click **Save**
5. That domain will no longer be blocked

Step-by-Step: Exempting a Device from Ad Blocking:
1. Navigate to Bandwidth and Filters > Ad Blocker
2. Scroll to **Bypass Devices**
3. Click **Add**
4. Select the device's **MAC Address** from the dropdown
5. Enter a **Device Name** (e.g., "Work Laptop")
6. Check **Enabled**
7. Click **Save**
8. That device will now receive ads normally while all other devices remain ad-free







---

14. System Administration

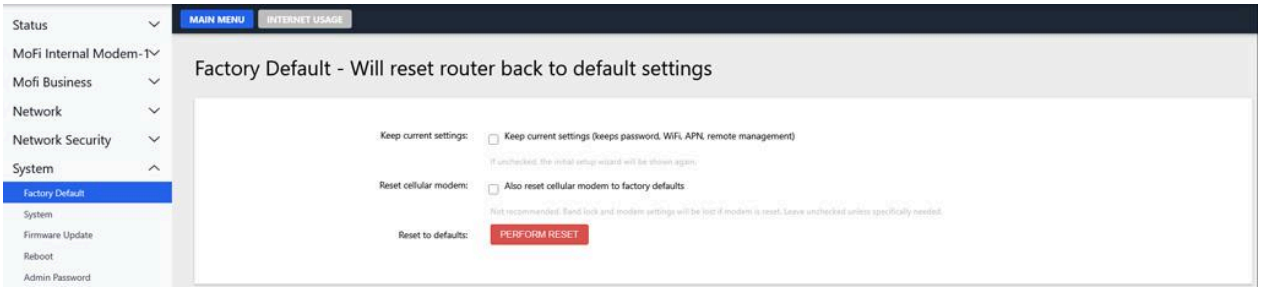
This section covers all pages under the **System** menu.

14.1 Factory Default

Menu: Go to **System** → **Factory Default** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/factory_reset

Reset the router to factory default settings. This erases all configuration (WiFi passwords, firewall rules, VPN settings, etc.) and restores the router to its out-of-box state.

Single action: Click **Factory Default** to perform the reset.



Warning: This action cannot be undone. All custom settings will be permanently deleted. The router will reboot and the setup wizard will appear.

14.2 System Settings

Menu: Go to **System** → **System** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/system

General system configuration. Has tabs: **General Settings**, **Logging**, **Time Synchronization**, **Language and Style**.

General Settings

Setting	Options	Description
Local Time	Display + Sync buttons	Current router time. Click “Sync with browser” to set from your computer, or “Sync with NTP-Server” to set from internet time.
Hostname	Text	Router’s network hostname (default: MoFi)
Description	Text (optional)	Description label for this router (visible in ACS portal)
Notes	Free-form text	Personal notes about this router (not shared externally)
Timezone	Full world timezone dropdown	Set your local timezone for accurate time display

Logging

Setting	Options	Description
System log buffer size	KiB	Memory allocated for system logs
External system log server	IP address	Send logs to a remote syslog server
Log server port	Numeric	Remote syslog port
Log server protocol	UDP / TCP	Protocol for remote logging
Write system log to file	Toggle	Save logs to a file on the router
Log output level	Debug / Info / Notice / Warning / Error / Critical / Alert / Emergency	Minimum severity for logged messages
Cron Log Level	Debug / Normal / Warning	Logging verbosity for scheduled tasks

Time Synchronization

Setting	Options	Description
Enable NTP client	Toggle	Synchronize time from internet NTP servers
Provide NTP server	Toggle	Let LAN devices sync time from this router
Bind NTP server	Interface dropdown	Which network interface the NTP server listens on
Use DHCP advertised servers	Toggle	Use NTP servers provided by your ISP
NTP server candidates	List	NTP server addresses (add/remove)

Language and Style

Setting	Options	Description
Language	auto / Deutsch / English / 简体中文	Web interface language
Design/Theme	Argon / Bootstrap / BootstrapDark / BootstrapLight / Material	Visual theme for the web interface

Buttons: Save & Apply, Save, Reset

14.3 Firmware Update

Menu: Go to **System** → **Firmware Update** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/flash

Upload new firmware, backup/restore configuration, or factory reset.

Update Firmware: - Select a firmware image file (.bin) from your computer - Click **Flash image** to upload and install - The router will verify the image, then reboot with the new firmware

Backup: - Click **Generate archive** to download a .tar.gz backup of all current settings - Store this file safely — you can use it to restore settings later

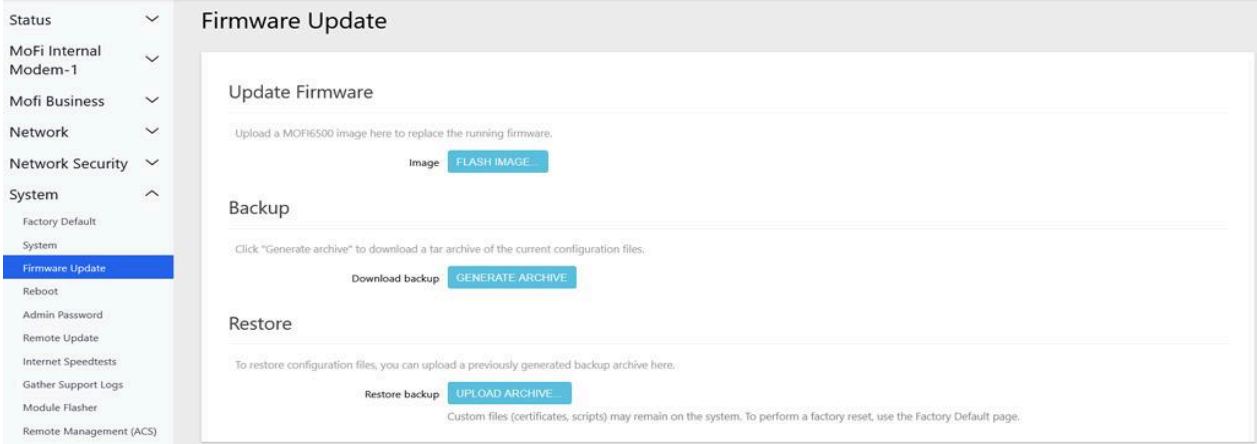
Restore: - Upload a previously saved backup archive to restore settings - Click **Perform reset** for a factory reset (same as System > Factory Default)

Warning: Do not interrupt the firmware update process. Disconnecting power during a firmware flash can permanently damage the router (“bricking”).

Step-by-Step: Updating Firmware Manually:
1. Download the latest firmware .bin file from MoFi’s website or your reseller
2. Navigate to System > Firmware Update
3. Click **Generate archive** first to download a backup of your current settings
4. Under **Update Firmware**, click the file selector and choose the .bin firmware file
5. Click **Flash image**
6. The router will verify the firmware image (checksum validation)
7. Confirm the update when prompted
8. Wait 3-5 minutes — do NOT turn off the router or close the browser
9. The router will reboot with the new firmware
10. Reconnect to the router and verify the firmware version under Status > General

Step-by-Step: Backing Up and Restoring Settings:
1. Navigate to System > Firmware Update
2. Click **Generate archive** to download your configuration backup (.tar.gz file)
3. Store this file safely on your computer

4. To restore: click **Upload archive**, select the .tar.gz file, and click upload
5. The router will apply the saved configuration and reboot



14.4 Reboot

Menu: Go to S**ystem** → **Reboot** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/reboot

Click **Perform reboot** to restart the router. The reboot takes approximately 90 seconds. All active connections will be temporarily interrupted.

14.5 Admin Password

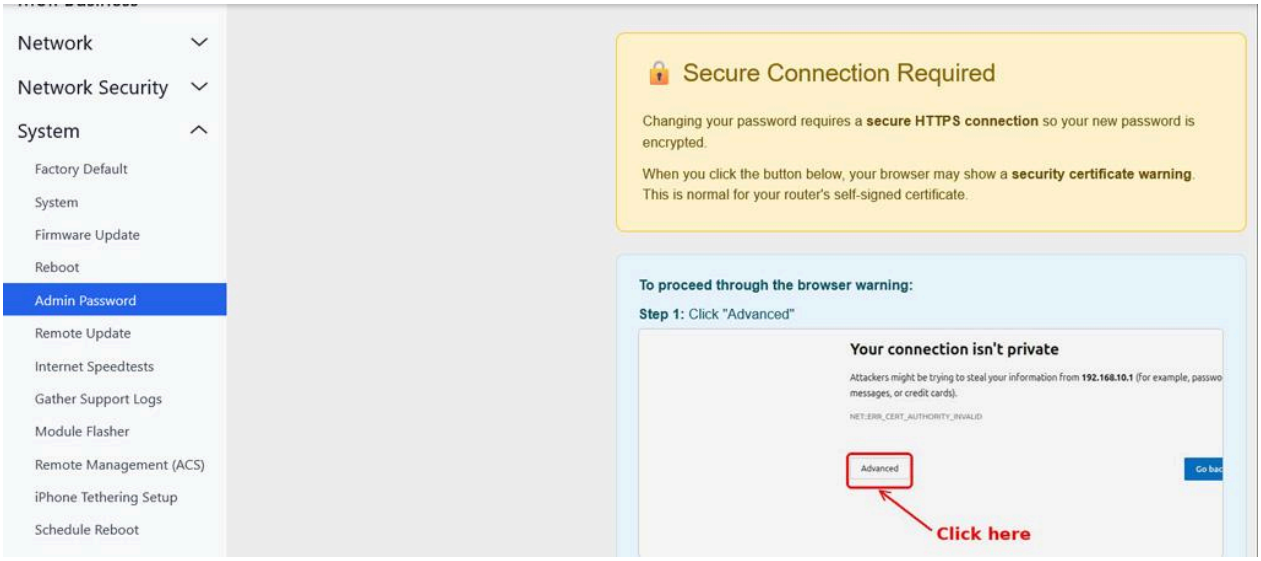
Menu: Go to **System** → **Admin Password** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/admin_password

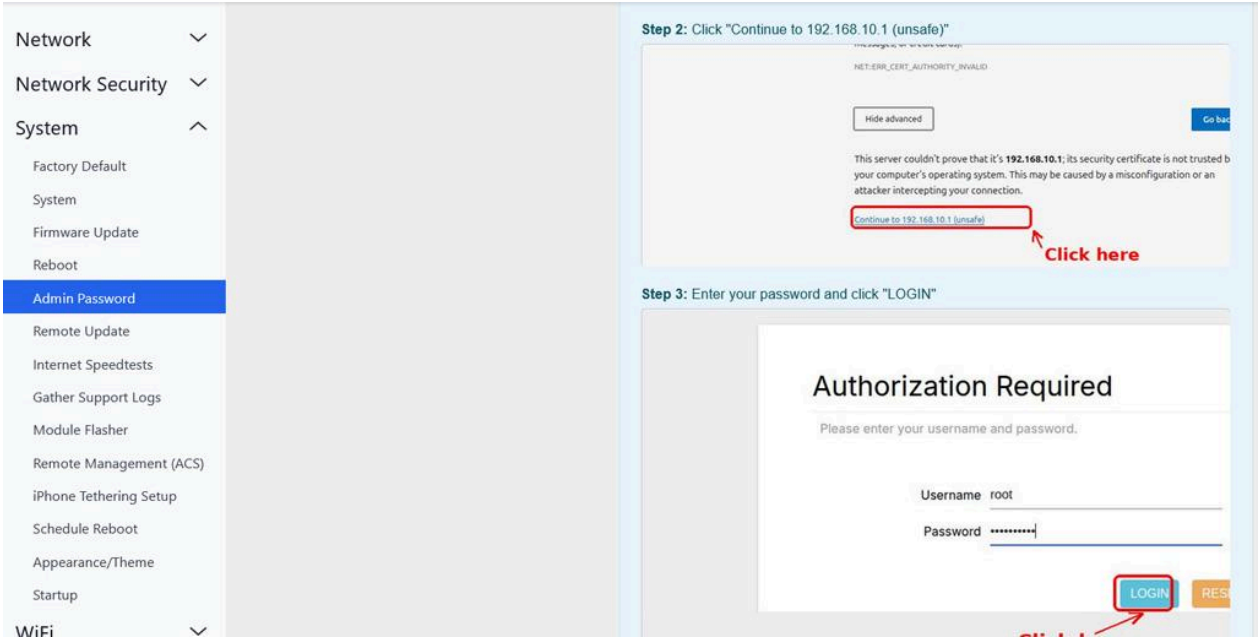
Change the router's admin password.

Important: You will see an HTTPS notice with a button to **Switch to Secure Connection**. Always change your password over HTTPS to prevent interception.

On HTTPS: - **New Password** — Enter your new password - **Confirm New Password** — Re-enter to confirm

Click **Save** to apply.





14.6 Remote Update

Menu: Go to **System** → **Remote Update** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/remote-update-js

Check for and install firmware updates from MoFi's servers.

Setting	Description
Keep Configuration	Checkbox — when checked, your settings are preserved after the firmware update
Version status	Shows your current firmware version and whether an update is available

Click **Start Upgrade** to download and install the latest firmware from MoFi's update server.

14.7 Internet Speedtests

Menu: Go to **System** → **Internet Speedtests** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/speeds

System-level embedded internet speed test tools (similar to the modem-specific speed test pages).

14.8 Gather Support Logs

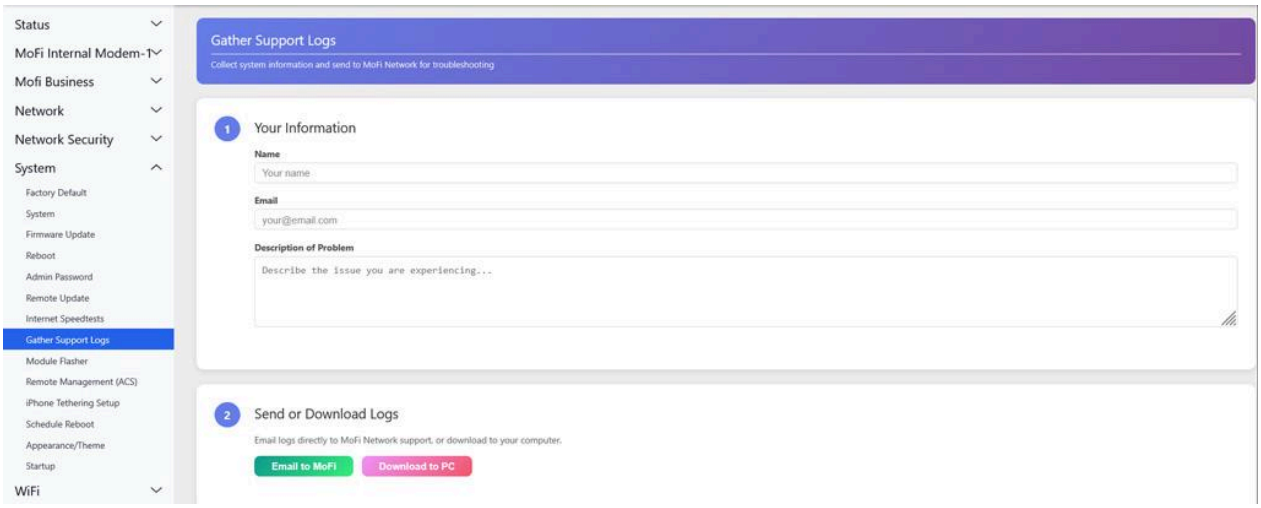
Menu: Go to **System** → **Gather Support Logs** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/supportlog

Collect diagnostic information to send to MoFi support.

3-Step Wizard:

1. **Step 1:** Enter your information:
    - **Name** — Your name
    - **Email** — Your email address
    - **Description of Problem** — Describe the issue you're experiencing
    - Click **Next**
2. **Step 2:** The router gathers system logs, configuration files, and diagnostic data

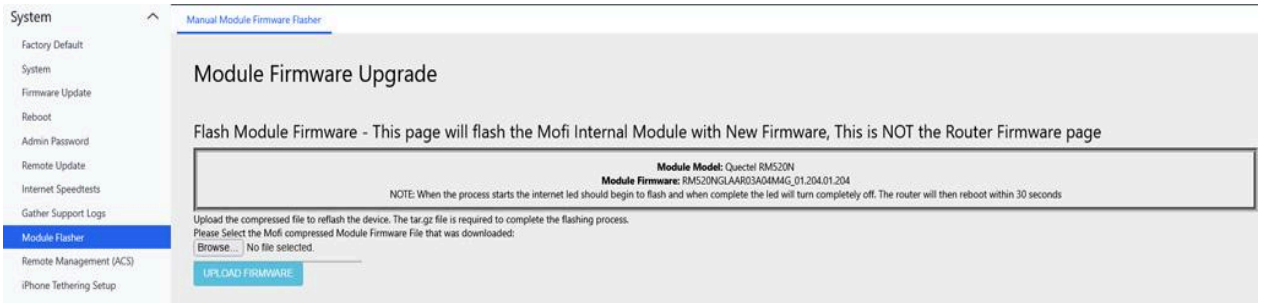
Step 3: Download the log package (.tar.gz) and send it to MoFi support



14.9 Module Flasher (module update)

Menu: Go to **System** → **Module Flasher** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/quectel_modupd

Flash/update the cellular modem's internal firmware. This updates the Quectel RM520N-GL modem itself, not the router's firmware.



Warning: Do not interrupt the modem firmware update. This process can take several minutes. Disconnecting power during a modem flash can permanently damage the cellular module.

14.10 Remote Management (ACS) Set up

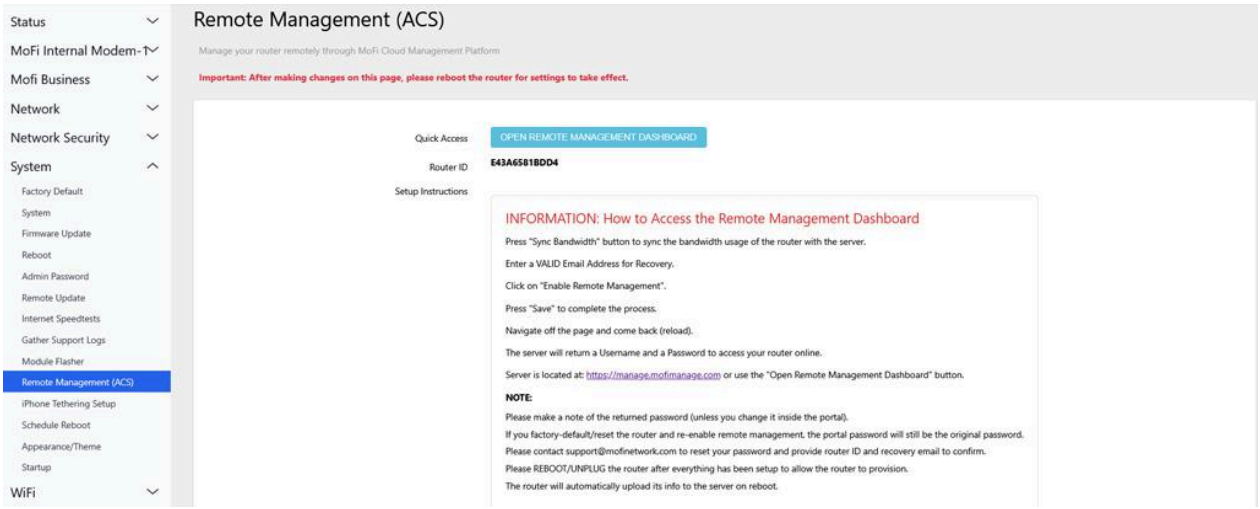
Menu: Go to **System** → **Remote Management (ACS)** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/remserver

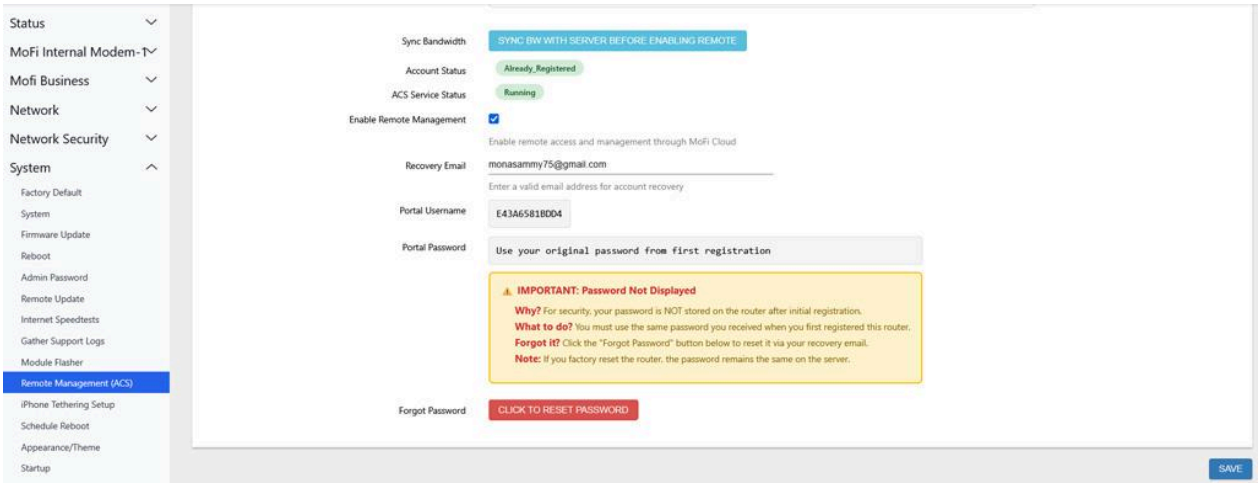
Connect your router to the MoFi ACS (Auto Configuration Server) cloud management platform.

Setting	Description
Open Remote Management Dashboard	Button — opens the ACS portal in a new browser tab
Router ID	Your unique router identifier (serial number) — this is your ACS login username
Sync Bandwidth	Button — manually sync bandwidth data to ACS
Account Status	Current ACS account status
ACS Service Status	Connection status to the ACS server
Enable Remote Management	Toggle — enable or disable ACS reporting
Recovery Email	Email address for password resets
Portal Username	Display only — your Router ID (auto-assigned)
Portal Password	Display only — auto-generated by the server on first registration. Write this down.
Forgot Password	Button — contact support@mofinetwork.com with your Router ID and recovery email to reset

Buttons: Save.

Important: Reboot the router after enabling or modifying ACS settings for changes to take full effect.





Step-by-Step: Connecting to ACS:

1. Navigate to System > Remote Management
2. Note your **Router ID** — this is your ACS login username
3. Enter a valid **Recovery Email** for password resets
4. Click **Enable Remote Management**
5. Click **Save**
6. Navigate away from the page and then return (reload)
7. The server will return a **Username** and **Password** — write down the password
8. Reboot the router to allow it to provision
9. After reboot, click **Open Remote Management Dashboard** to access https://manage.mofimanage.com
10. Log in with the returned Username and Password

14.11 iPhone Tethering Setup

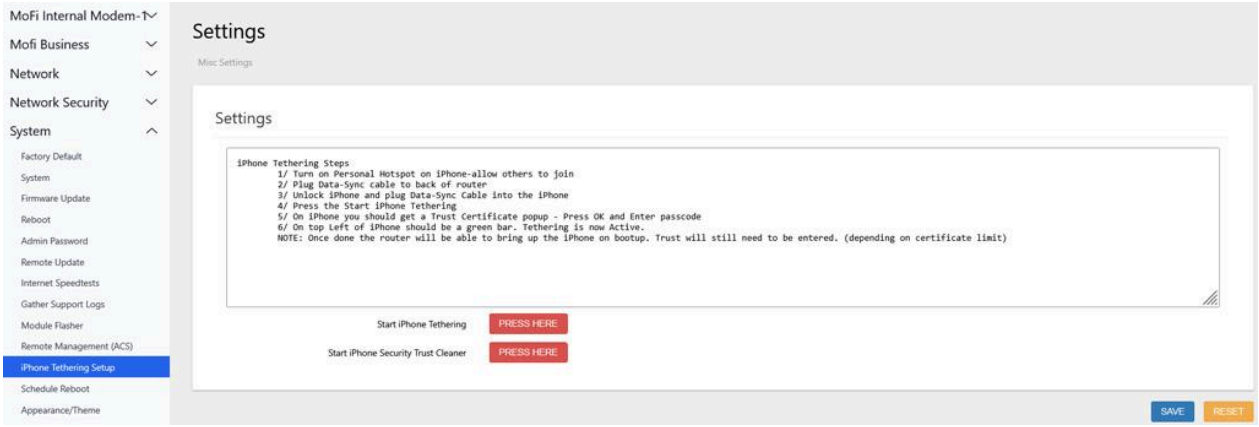
Menu: Go to **System** → **iPhone Tethering** Setup or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/iphone

Use your iPhone's cellular data connection through the MoFi router via USB tethering.

Step-by-step instructions displayed (6 steps):

1. Connect your iPhone to the router's USB port using a Lightning/USB-C cable
2. On your iPhone, go to Settings > Personal Hotspot and enable it
3. When prompted on the iPhone, tap "Trust" to trust the router
4. Click **Start iPhone Tethering** on this page
5. The router will detect the iPhone and use its cellular connection as an internet source

Buttons: - **Start iPhone Tethering** — Begin the tethering process - **Start iPhone Security Trust Cleaner** — Clear stored trust certificates (use if the iPhone doesn't detect the router)



14.12 Scheduled Reboot

Menu: Go to **System** → **Schedule Reboot** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/rebooter-js

Configure automatic periodic reboots to keep the router running smoothly.

Setting	Options	Description
Enabled	Checkbox	Enable or disable scheduled reboots
Reset Hour	Every Hour / Every 1 Hour / Every 2 Hours / 1am-12pm (all 24 hours in AM/PM format)	Hour to reboot
Reset Minutes	Every Minute / Every 2/5/10/20/50 Minutes / 00, 05, 10, 15, 20, 25, 30, 35, 40, 45, 50, 59	Minute to reboot (5-minute increments for specific times)
Reset Day of the Month	Every Day / Every 2 Days / Every 3 Days / Every 10 Days / Every 20 Days	Day of month
Reset Day of Week	Every Day / Every Monday-Sunday	Day of week

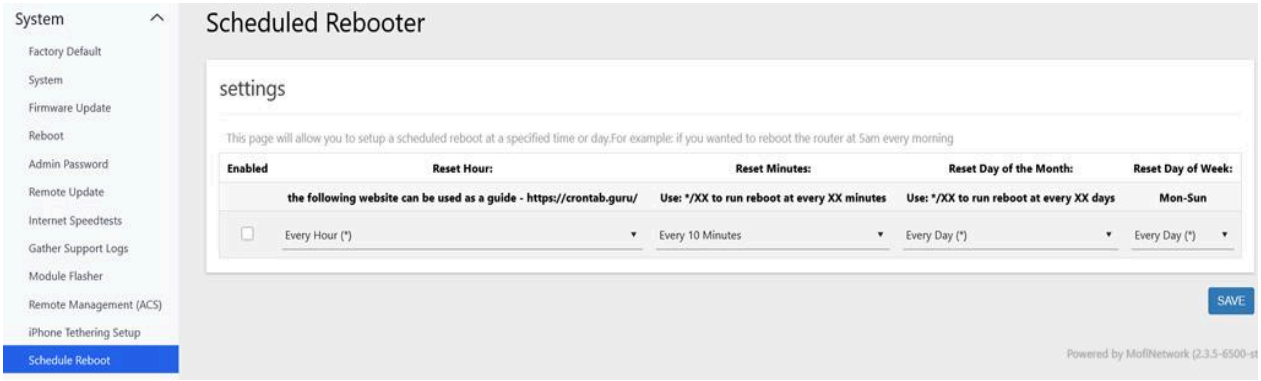
Buttons: Save, Reset

Step-by-Step: Setting Up a Daily 3 AM Reboot:
1. Navigate to System > Schedule Reboot
2. Check **Enabled**
3. Set **Reset Hour** to “3am”
4. Set **Reset Minutes** to “00”

5. Set **Reset Day of the Month** to “Every Day (*)”
6. *Set **Reset Day of Week** to ”Every Day (*)”*
7. Click **Save**
8. The router will now automatically reboot at 3:00 AM every day

Step-by-Step: Weekly Sunday Night Reboot:

1. Navigate to System > Schedule Reboot
2. Check **Enabled**
3. Set **Reset Hour** to “2am”
4. Set **Reset Minutes** to “00”
5. Set **Reset Day of the Month** to “Every Day (*)”
6. Set **Reset Day of Week** to “Every Sunday (Sun)”
7. Click **Save**



Tip: For most deployments, a daily reboot at 3:00 AM provides a good balance between uptime and stability.

Audit Log Menu : Go to **System** → **Audit Log** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/audit-log

Record of admin logins, configuration changes, failover events, reboots, and firmware upgrades. Kept in memory; the most recent entries are also written to flash so they survive a reboot.

Audit Logging

Recording all supported events.
The Audit Log on the MOFI6500-5GXeLTE tracks important router events in a structured format separate from the normal system log.

It records:

- Admin logins/logouts
- Configuration changes
- New devices joining/leaving
- WAN failover and reconnect events
- Reboots and firmware updates

Each entry includes:

- Time
- Event type
- User
- Source IP
- Summary
- Technical details

Examples:

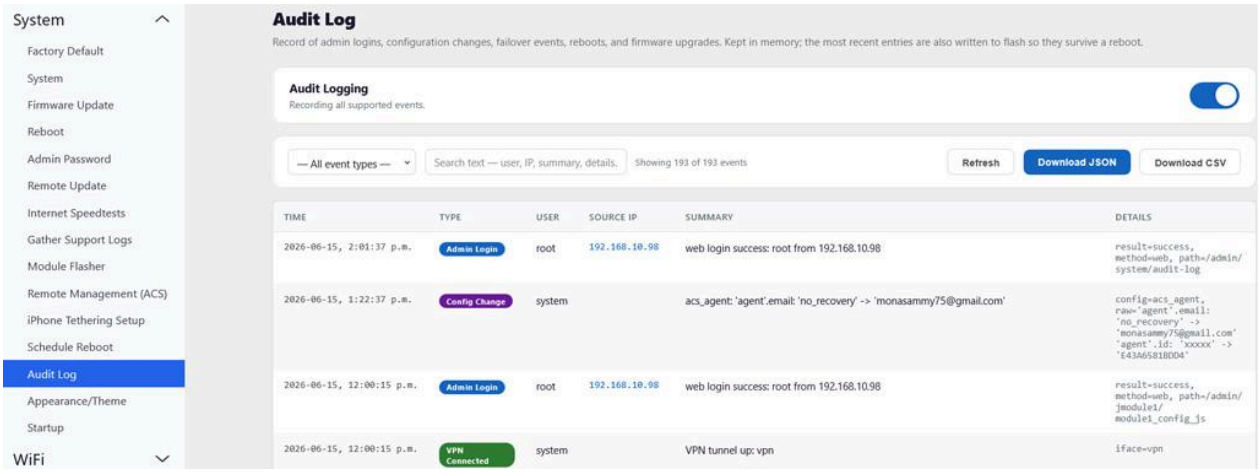
- web login success: root from 192.168.10.99
- network: 'module1'.conn_retry: '1' -> '2'
- new device: mofi100 @ 192.168.10.99

Useful features:

- Filter by event type
- Search by IP/user/text
- Export as JSON or CSV
- Recent logs survive reboot

The Audit Log is mainly for:

- Admin accountability
- Change tracking
- Device monitoring
- Troubleshooting
- MSP/remote management support



14.13 Module Reset (There is no Module reset in SYSTEM)

Menu: System > Module Reset **URL:** `/cgi-bin/luci/admin/system/module_reset_js`

Reset the cellular modem module to factory defaults.

Click **Module1 Reset** to reset. The router will reboot automatically in approximately 35 seconds.

Note: This resets the modem's internal configuration, not the router's configuration. Band locks, tower locks, and custom AT command settings on the modem will be cleared.

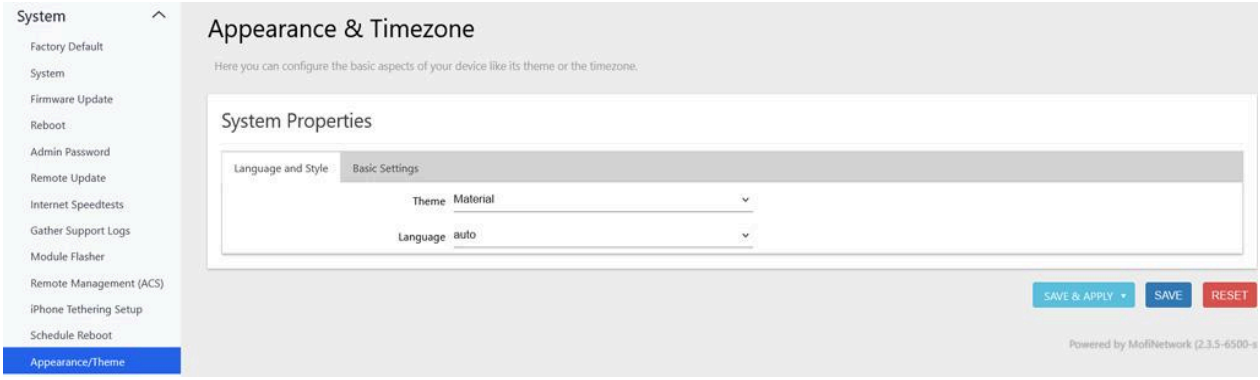
14.14 Appearance / Theme

Menu: Go to **System** → **Appearance/Theme** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/theme

Customize the look of the router's web interface.

Setting	Options	Description
Theme	Argon / Bootstrap / BootstrapDark / BootstrapLight / Material	Visual theme
Language	auto / Deutsch / English / 简体中文	Interface language
Local Time	Display + Sync button	Current time with browser sync
Hostname	Text	Router hostname
Timezone	Full dropdown	Time zone

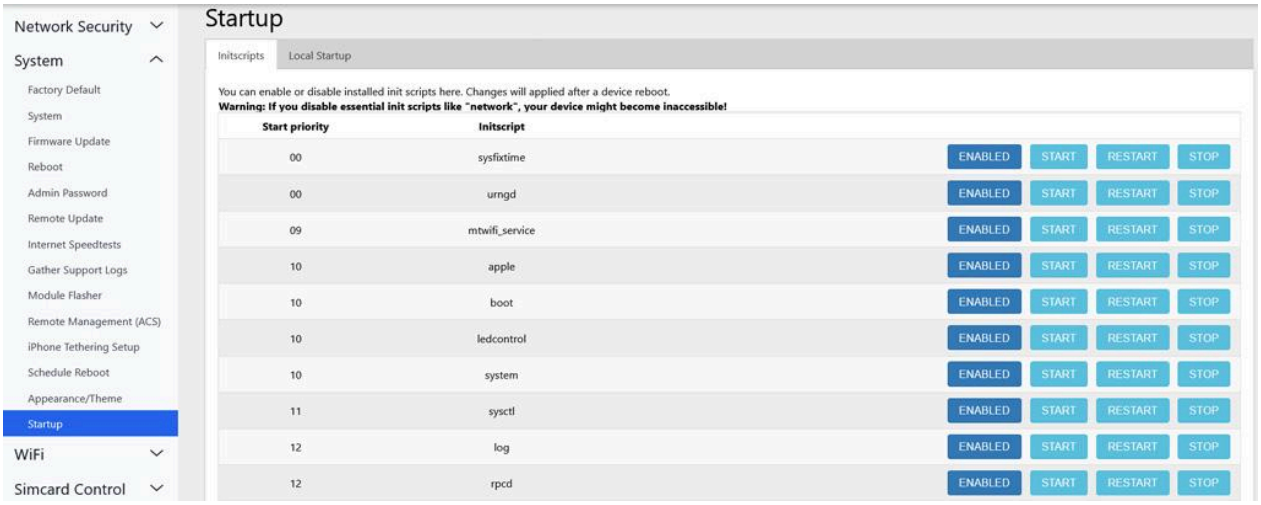
Buttons: Save & Apply, Save, Reset



14.15 Startup (Init Scripts)

Menu: Go to **System** → **Startup** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/system/startup

View and manage all system services (init scripts). Each service has: - **Enable** / **Disable** buttons — Control whether the service starts at boot - **Start** / **Stop** / **Restart** buttons — Control the service immediately



Warning: Disabling critical services can make the router inaccessible. Do not disable services unless you know what they do.

---

15. Services

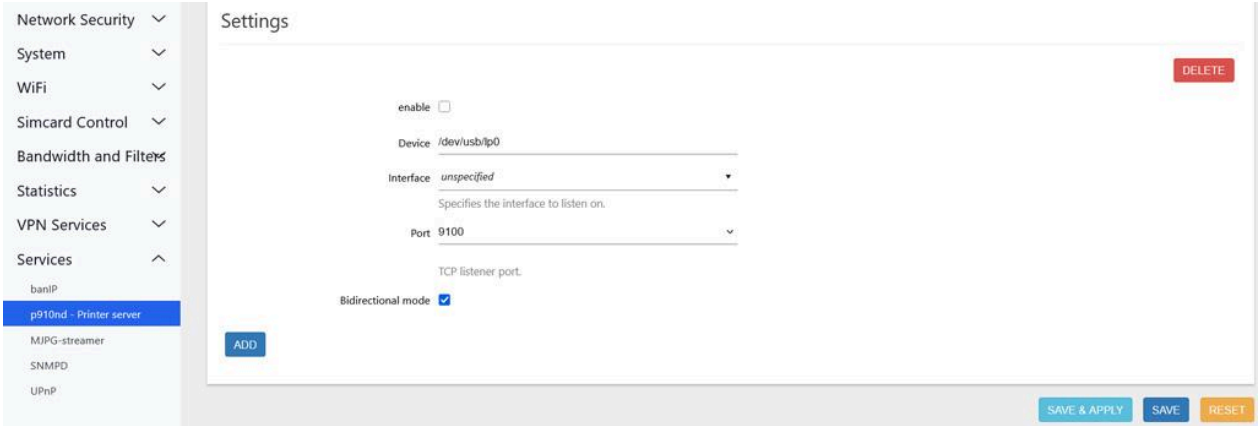
15.1 Printer Server (p910nd)

Menu: Go to **Services** → **p910nd** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/services/p910nd

Share a USB-connected printer with all devices on the network.

Setting	Options	Description
Enable	Toggle	Enable the print server
Device	Text (e.g., /dev/usb/lp0)	USB printer device path
Interface	unspecified / lan / module1 / vpn / wan / wan6	Network interface to listen on
Port	9100-9109	TCP port for print jobs
Bidirectional mode	Toggle	Enable two-way communication with the printer

Note: Requires `kmod-usb-printer` kernel module to be installed.



15.2 MJPG-Streamer

Menu: Go to **Services** → **MJPG-streamer** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/services/mjpg-streamer

Stream video from a USB camera over the network.

General:

Setting	Description
Enable	Enable MJPG-streamer service

HTTP Output Settings:

Setting	Description
Port	TCP port for the video stream
Authentication required	Require username/password to view the stream
WWW folder	Folder containing the web viewer

File Output Settings:

Setting	Description
Folder	Save captured images to this folder
Interval	Time between image captures (milliseconds)
Ring buffer size	Maximum stored images
Command to run	Execute a command after each capture

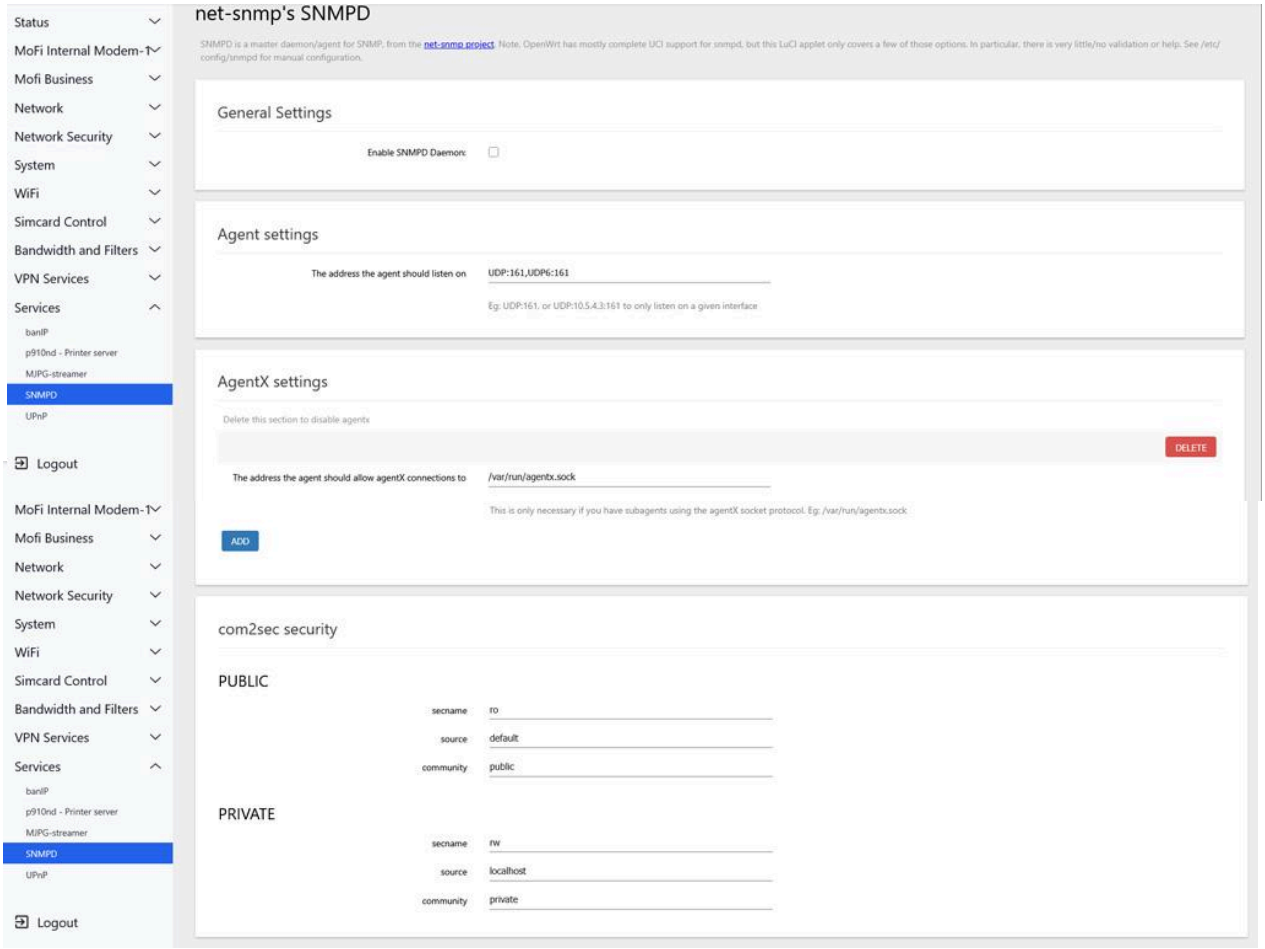
UVC Input Settings:

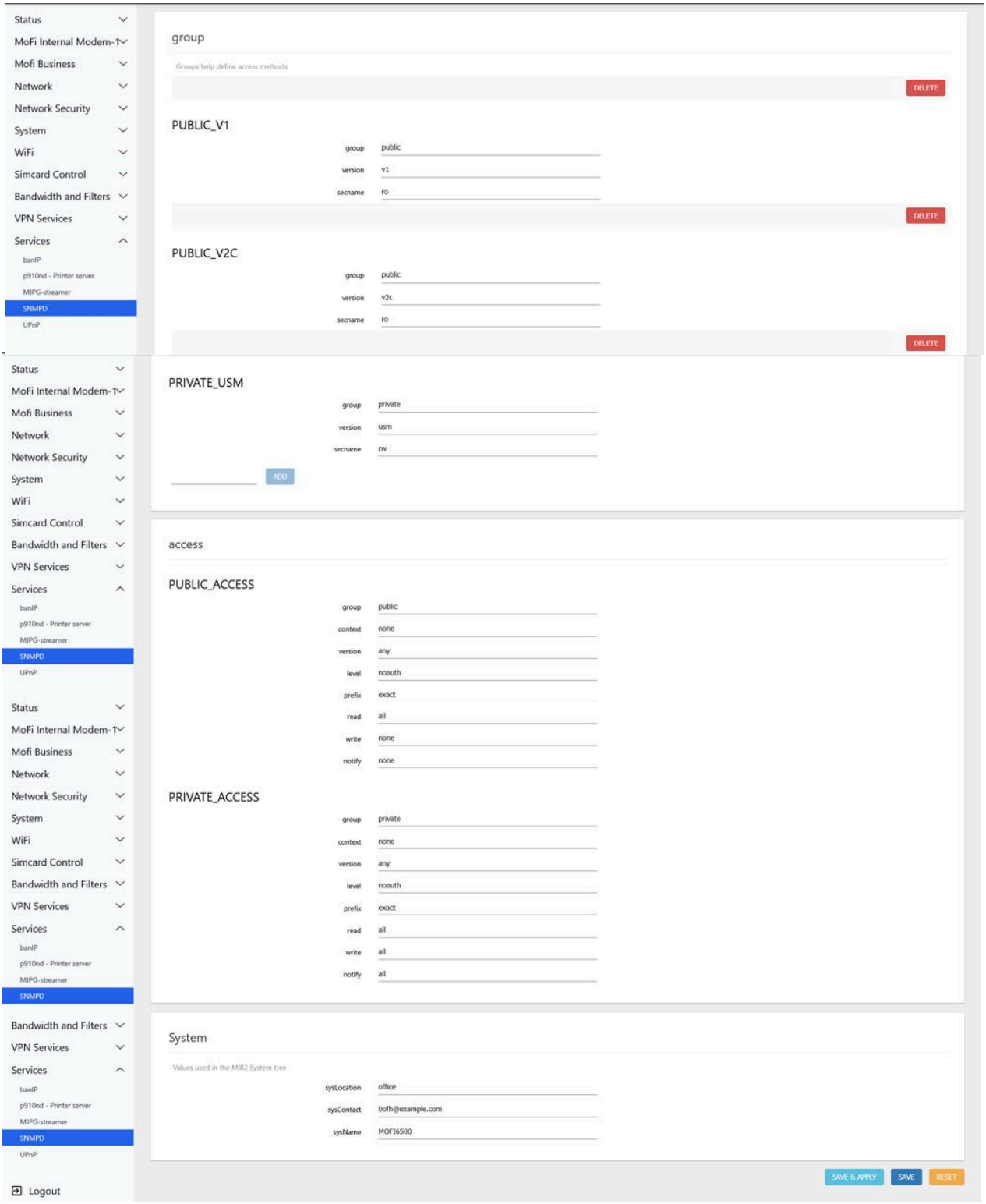
Setting	Options	Description
Device	/dev/video0, video1, video2	USB camera device
Resolution	320x240 through 1920x1080	Video resolution
Frames per second	Numeric	Video framerate
	Percentage	Image quality

SNMPB Menu: **Services** → **SNMPB** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/services/snmpd

net-snmp's SNMPD

SNMPD is a master daemon/agent for SNMP, from the net-snmp project. Note, OpenWrt has mostly complete UCI support for snmpd, but this LuCI applet only covers a few of those options. In particular, there is very little/no validation or help. See /etc/config/snmpd for manual configuration.




Status
MoFi Internal Modem-1
Mofi Business
Network
Network Security
System
WiFi
Simcard Control
Bandwidth and Filters
VPN Services
Services
banIP
p910nd - Printer server
MJPG-streamer
SNMPD
UPnP
Logout
group
Groups help define access methods
DELETE
PUBLIC_V1
group public
version v1
secname ro
DELETE
PUBLIC_V2C
group public
version v2c
secname ro
DELETE
PRIVATE_USM
group private
version usm
secname rw
ADD
access
PUBLIC_ACCESS
group public
context none
version any
level noauth
prefix exact
read all
write none
notify none
PRIVATE_ACCESS
group private
context none
version any
level noauth
prefix exact
read all
write all
notify all
System
Values used in the MIB2 System tree
sysLocation office
sysContact both@example.com
sysName MOFI6500
SAVE & APPLY
SAVE
RESET

15.3 banIP (Services View)

Menu: Go to **Services** → **banIP** or click on the link below:
http://192.168.10.1/cgi-bin/luci/admin/services/banip

Same as Section 11.10 — Attack Defense (banIP). Full banIP configuration with all six tabs.

---

16. ACS Remote Management Portal

To view the full user manual on the ACS, click on link
https://mofinetwork-firmware.s3.dualstack.us-east-1.amazonaws.com/manual/MoFi_ACS_Portal_Guide.pdf

The MoFi ACS (Auto Configuration Server) is a cloud-based management portal for monitoring and configuring your router remotely from any web browser. The ACS works with both public and private IP addresses — no special network configuration is required.

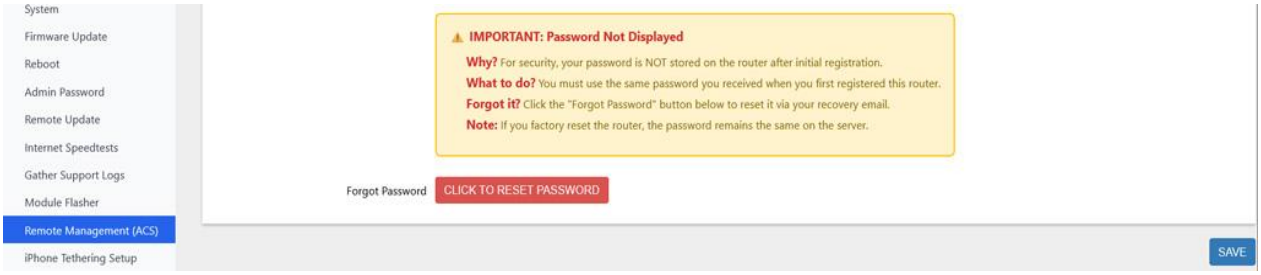
Portal URL: https://manage.mofimanage.com

> **The complete ACS Remote Management Portal User Guide is available as a separate document.** The section below provides an overview. For detailed ACS instructions including multi-device management, bulk operations, and advanced features, contact MoFi Network or visit www.mofinetwork.com.

16.1 Logging In

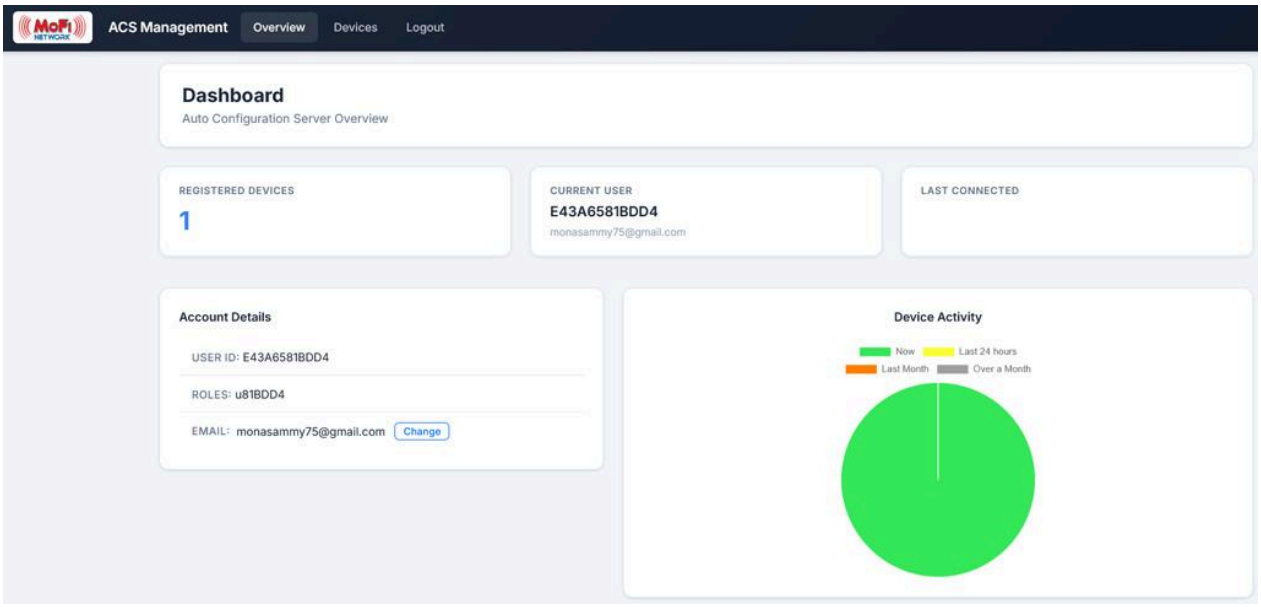
Field	Value
Username	Your Router ID (serial number printed on the router, e.g., E43A6581B660)
Password	The password you set on the Remote Management page

Forgot Password:
1. Click **Forgot password?** on the login page
2. Enter your Router ID
3. A reset link is sent to your registered recovery email
4. Click the link and set a new password
5. The reset link expires in 1 hour and can only be used once



16.2 Dashboard

After logging in, the dashboard shows: - Total registered devices - Your account details (username, email) - Most recently connected device - Device activity summary with timestamps



16.3 Device List

View all your managed routers in a sortable, searchable table:

Column	Description
Serial	Router’s unique ID
Description	Custom label for the router
Last Online	When the router last checked in
SIM ID (ICCID)	Active SIM card ID
IMEI	Modem hardware ID
Carrier	Active cellular carrier
Signal	Signal strength (RSRP)

Column	Description
Firmware	Installed firmware version
IP Address	Router's public/cellular IP
Uptime	How long since last reboot
Download / Upload	Bandwidth usage

Bulk Actions: Select multiple devices for group operations: - Reboot all selected - Factory reset all selected - Run speed test on all selected - Export selected to CSV file

16.4 Device Detail

Click a device serial number to view its full configuration. Available sections:

Common Settings: - Change hostname and description - Set router admin password remotely - Toggle Captive Portal, Watchdog, HWNAT, Internet Enable - Set ACS check-in interval (how often the router reports to ACS) - Configure failover policy and SIM failover

Module Information: - View: APN, carrier, signal strength, band, temperature, IMEI, ICCID - Change APN settings remotely - Reset modem remotely

WiFi Settings: - Change SSID and password for all radios (Main 2.4G, Main 5G, Guest 2.4G, Guest 5G) - Change encryption type - Reload WiFi configuration remotely

Band Lock: - Select specific LTE and 5G bands - Apply carrier presets (AT&T, T-Mobile, Verizon)

Bandwidth: - View download/upload/total usage per interface - Set bandwidth limits and thresholds - Reset bandwidth counters

Actions: - Reboot, Factory Reset, Run Speed Test - Run Speed Band Lock, Email Band Lock Report - Push Firmware Updates (admin only)

16.5 Data Usage

View daily bandwidth breakdown by interface (WAN, Module 1, Module 2): - Filter by date range - Export reports via email

16.6 Connected Devices

View all devices currently connected to the router: - Hostname, IP address, MAC address - Active/inactive status

16.7 Tasks

View pending configuration tasks queued for the device. Tasks are applied automatically when the router checks in with the ACS server (default: every 10 minutes).

---

17. Troubleshooting

No Internet Connection

1. **Check LEDs:** Is the Internet Status LED on? Refer to the LED table in Section 2.
2. **Check Signal:** Go to 'Mofi Internal Modem' then Module Status — is RSRP above -140 dBm? Is SINR above 0 dB? Suggest to swap the primary and secondary antenna and then reboot and check
3. **Check SIM:** Ensure the SIM card is properly seated. Try removing and reinserting it.
   Log into the router, go to mofi internal modem and ensure the carrier ID and SIM is being read.
4. **Verify SIM activation:** Contact your carrier to confirm the SIM is activated for data service.
   When SIM is activated, it should also show a phone number under mofi internal modem
5. **Check APN:** Go to Configuration and verify the APN matches your carrier's requirements. Try "Auto" if unsure.
6. **Reboot:** System > Reboot
7. **Reset Modem:** System > Factory Reset / Default
8. **Hard Reset:** Hold the reset button for 10+ seconds (last resort)

Slow Speeds

1. **Check signal quality:** RSRP should be above lower than -110, if numbers are higher, you have a signal issue.
2. **Run Speed Band Lock:** Automatically finds and locks to the fastest bands in your area.
3. **Check band lock:** If bands are manually locked, ensure they include your carrier's bands.
4. **Try different Service Mode:** Switch between LTE/5G, 5G Only, or LTE Only to compare.
5. **Check for interference:** Move cellular antennas away from metal objects and electronics.
6. **Check connected devices:** Another device may be consuming bandwidth. Check Internet Usage.

WiFi Issues

1. **Can't see network:** Check if SSID is hidden (WiFi > MoFi WiFi). Check if WiFi is disabled.
2. **Can't Connect:** Verify the WiFi password. Try WPA2-PSK if using WPA-PSK/WPA2-PSK Mixed doesn't work.
3. **Slow WiFi:** Use 5 GHz for faster speeds. Check WiFi channel for congestion in WiFi Advanced.
4. **Limited Range:** Ensure WiFi antennas are properly connected and positioned vertically.
5. **Devices Disconnecting:** Check if WiFi Schedule is enabled. Check MAC filtering.

Router Not Responding

1. **Check power:** Is the Power LED on? Try a different power outlet.
2. **Try a different browser:** Clear cache or use incognito/private mode.
3. **Check IP:** Default is 192.168.10.1. Ensure your computer is set to DHCP (automatic IP).
4. **Try a different LAN port:** Connect to a different LAN port (1-4).
5. **Hard reset:** Hold the reset button for 10+ seconds. The router will restart with default settings.
6. **Check if IP was changed:** If someone changed the router IP, you may need to factory reset.

VPN Not Connecting

1. **Check port forwarding:** WireGuard needs the configured listen port (default 6677 UDP) open.
2. **Check public IP:** Cellular carriers often don't provide public IPs. Use CloudLink.
3. **Check firewall:** Ensure the VPN port is allowed in Traffic Rules.
4. **Check credentials:** Verify username/password for third-party VPN providers.
5. **Try a different protocol:** For OpenVPN, switch between TCP and UDP.

Failover Not Working

1. **Reboot required:** Always reboot after changing failover settings.
2. **Check both connections:** Each connection must be able to reach the internet independently.
3. **Don't enable both:** Failover and Load Balancing cannot be active simultaneously.
4. **Check MWAN3 status:** The system log shows failover switching events.

ACS Portal Issues

1. **Can't log in:** Use your Router ID (serial number) as username, not your email.
2. **Forgot password:** Click "Forgot password?" and check your email (including spam folder).
3. **Device not showing:** Ensure Remote Management is enabled on the router. Reboot after enabling.
4. **Changes not applying:** Changes apply on the next check-in (default every 10 minutes). Reboot the router for immediate application.
5. **Status not updating:** Click "Sync Bandwidth" on the ACS page, then wait for next check-in.

CloudLink Issues

1. **Not connecting:** Verify your CloudLink username and password.
2. **Port forwarding not working:** Use "Cloudlink/VPN" as the external source, NOT "Cellular/Wan/Repeater."
3. **Slow speeds:** CloudLink adds some latency. This is normal for tunneled connections.
4. **IPSec through CloudLink:** CloudLink may block UDP 500/4500. Contact MoFi support for IPSec compatibility.

MoFi Recovery (Boot Recovery from Bad Firmware)

If your router becomes non-functional after a failed firmware update or other issue (router won't boot up, can't access the web interface, stuck in a boot loop), use this boot recovery procedure to restore the router.

When to Use Recovery Mode: - Router won't boot (Power LED keeps blinking, never goes solid) - Router boots but web interface is inaccessible - Bad firmware was flashed and router is unresponsive - WiFi LED blinks very fast (indicates recovery mode)

Step 1: Set Router to Recovery Mode

1. Connect your PC to **LAN port 1:** on the back of the router using an Ethernet cable.
2: Unplug the router's power cable.
3: Press and hold the **Reset** button on the back of the router
4. While holding the Reset button, plug the power cable back in.

5: Continue holding the Reset button for 15 seconds.
6: Release the Reset button when you see only two blue LEDs flashing — the router is now in Recovery Mode

Step 2: Configure Your Computer's Network Connection to a Static IP.
1: On your PC, go to Control Panel > Network and Internet > Network and Sharing Center.
2: Click Change adapter settings
3. Right-click on Local Area Connection (or Ethernet) and choose Properties.
4: Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
5: Select Use the following IP address and enter: - IP Address: **192.168.10.7** - Subnet Mask: **255.255.255.0** - Default Gateway: **192.168.10.1** Click OK to save

Step 3: Access the MoFi Recovery Interface
1. Open your web browser and go to: **http://192.168.10.1**
2. You should see the recovery interface (a simple upload page)
3: Browse to select the firmware file you want to install and start the recovery process .
4: The recovery will take approximately 1-2 minutes. The Power/Boot LED will turn off, flash, and then become solid when complete.

Step 4: Revert Your Computer's Network Connection to Automatic.
1: Go back to your network adapter Properties > TCP/IPv4 Properties.
2: Select Obtain an IP address automatically.
3: Select Obtain DNS server address automatically.
4: Click OK

Step 5: Log Into the Router
1. Open your web browser and go to: **http://192.168.10.1**
2: The setup wizard will appear — set your admin password and configure basic settings.
3: Upload the latest firmware if needed via System > Firmware Update

Note: After recovery, all settings are reset to factory defaults. The setup wizard will guide you through initial configuration (admin password, WiFi, APN). You will need to reconfigure any custom settings (failover, VPN, port forwarding, etc.).

---

18. Specifications

Feature	Specification for the MOFI6500-5GXeLTE-RM520-HP model
Cellular Modem	Quectel RM520N-GL-HP
Cellular Standards	5G SA, 5G NSA, LTE Cat 20
5G NR Bands	n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n66, n70, n71, n75, n76, n77, n78, n79
LTE Bands	B1-B5, B7, B8, B12-B14, B17-B20, B25, B26, B28-B30, B32, B34, B38-B43, B46, B48, B66, B71

Feature	Specification for the MOFI6500-5GXeLTE-RM520-HP model
Max Cellular Download	Up to 3.4 Gbps (5G NSA) / 2.4 Gbps (5G SA) / 1.6 Gbps (LTE Cat 19)
Max Cellular Upload	Up to 900 Mbps (5G SA) / 550 Mbps (5G NSA) / 200 Mbps (LTE)
WiFi Standard	802.11ax (WiFi 6)
WiFi Bands	2.4 GHz (802.11b/g/n/ax) + 5 GHz (802.11a/n/ac/ax)
WiFi Max Speed	286 Mbps (2.4 GHz) / 1201 Mbps (5 GHz)
WiFi Security	WPA2-PSK, WPA-PSK/WPA2/3-PSK Mixed, WPA-PSK, Open
CPU	1.3 GHz dual-core processor
RAM	1 GB high-speed DDR
Flash Storage	128 MB
Ethernet Ports	1x WAN + 4x LAN (all 10/100/1000 Gigabit)
USB	2x USB ports (tethering, storage, USB modem)
SIM Slots	2x Nano SIM (4FF) for dual-SIM failover
SoC / Chipset	MediaTek MT7981
Console Port	External serial console port (115200 baud, 8N1)
Antenna Connectors	SMA female — 4x cellular + 5x WiFi (9 total on 5G model)
Power Input Options	Standard barrel connector + 4-pin Molex connector
LED Control	LED ON/OFF switch on back panel
Casing	Rugged metal enclosure
VPN Protocols	WireGuard, OpenVPN, L2TP/IPSec, OpenConnect, PPTP (CloudLink)
VPN Throughput	Up to 200+ Mbps (WireGuard)
Failover	WAN, Cellular (Module 1 & 2), WiFi Repeater, USB Tethering
Load Balancing	Per-connection weight-based distribution
NAT	Hardware NAT offloading supported
VLAN	IEEE 802.1Q, up to 4094 VLANs
QoS	SQM-based traffic shaping
Firewall	iptables with zone-based configuration
Operating Temperature	-30 C to +75 C (-22 F to +167 F)
Storage Temperature	-40 C to +90 C (-40 F to +194 F)
Power Input	12V DC, 3.5A (barrel jack + 4-pin Molex), 12-30V DC input range
Power Adapter	110/120V AC to 12V DC, 3.5A, UL certified
Dimensions	260 mm x 140 mm x 33 mm (10.2 in x 5.5 in x 1.3 in)
Weight	2.8 lb (with supplied antennas)
Certifications	Verizon, FCC, IC, PTCBR

19. Support & Contact

Resource	Details
Website	www.mofinetwork.com
ACS Portal	https://manage.mofimanage.com
Email Support	support@mofinetwork.com
Phone Support	+1-888-499-0123
Support Ticket	Open a ticket at https://support.mofinetwork.com

How to Contact MoFi Support:
1. **Open a support ticket** at www.mofinetwork.com — fastest response for technical issues https://support.mofinetwork.com
2. **Email** support@mofinetwork.com with your Router ID (serial number), firmware version, and a description of the issue
3. **Call** +1-888-499-0123 for phone support 7 days a week with a live rep

Before contacting support: - Note your **Router ID** is found at the bottom of the unit or above on the main GUI page next to the **Firmware Version** (shown on the Status > General page) - Gather **Support Logs** by going to System > Gather Support Logs — enter your name, email, and problem description, then download the log package and attach it to your ticket or email

Warranty Information

1 Year Manufacture defect, visit www.mofinetwork.com for warranty terms and conditions.

Regulatory Information

FCC Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15, 22 and 24 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by MoFi Network Inc. could void the user’s authority to operate the equipment.

RF Exposure Information: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

This device complies with Industry Canada licence-exempt RSS standard(s).

European Regulations: This product has been designed, tested and manufactured according to the European R&TTE directive 1999/5/EC.

Copyright Notice

Disclaimer: Information in this document is subject to change without notice. MoFi Network Inc. reserves the right to change specifications, features, and hardware design without prior notice. The information provided is believed to be accurate and reliable; however, MoFi Network Inc. assumes no responsibility for any errors or omissions.

> **ACS Remote Management Portal User Guide** — Available separately. Contact MoFi Network or visit www.mofinetwork.com.

MOFI6500-5GXeLTE User Guide
Document Version 2.0
June 2026

MoFi Network Inc.
www.mofinetwork.com
support@mofinetwork.com
+1-888-499-0123

Rugged Enterprise Extended Range Router