

# Industrial Router 624 Product User Manual

## ^ Table of contents

- ▲ 1. Overview
- ▲ 2. Hardware
  - ▲ 2.1 LED Indicators
  - ▲ 2.2 Restore to Factory Defaults
- ▲ 3. Default Settings
- ▲ 4. Quick Guide
  - ▲ 4.1 Environment Setup
  - ▲ 4.2 Access the Internet
    - 4.2.1 5G/4G
    - **4.2.2 Wired Connection**
    - 4.2.3 Wi-Fi STA
- ▲ 5. Configuration
  - ▲ 5.1 Dashboard
    - 5.1.1 Device Information
    - 5.1.2 Interface Status
    - 5.1.3 Traffic Statistics
    - 5.1.4 Wi-Fi Connections
    - 5.1.5 Clients Traffic Top5
  - ▲ 5.2 Status
    - 5.2.1 Link Monitor
    - 5.2.2 Cellular Signal

- 5.2.3 Clients
- 5.2.4 VPN
- 5.2.5 Events
- 5.2.6 Logs
- ▲ 5.3 Internet
  - 5.3.1 Wired Connection
  - 5.3.2 Wireless Connection
  - 5.3.3 5G/4G Connection
  - 5.3.4 Uplink Table
  - 5.3.5 Uplink Settings
- ▲ 5.4 Local Network
- ▲ 5.5 Wi-Fi
  - 5.5.1 SSIDs
  - 5.5.2 Portal
- ▲ 5.6 VPN
  - 5.6.1 IPSec VPN
  - 5.6.2 L2TP VPN
    - 5.6.2.1 Work as Client
    - **5.6.2.2 Work as Server**
- ▲ 5.7 Security
  - 5.7.1 Firewall
    - 5.7.1.1 Inbound/Outbound Rules
    - 5.7.1.2 Port Forwarding
    - **5.7.1.3 MAC Address Filter**
    - 5.7.1.4 NAT
    - 5.7.1.5 Domain Name Filtering
  - 5.7.2 Policy-Based Routing

- 5.7.3 Traffic Shaping

#### ▲ 5.8 Service

- 5.8.1 Interface Management
- 5.8.2 DHCP Server
- 5.8.3 DNS Server
- 5.8.4 Fixed Address List
- 5.8.5 Static Routes
- 5.8.6 Dynamic DNS

#### ▲ 5.9 Industrial Interface

#### ▲ 5.10 System

- 5.10.1 Cloud Management
- 5.10.2 Remote Access Control
- 5.10.3 System Clock
- 5.10.4 Device Option
- 5.10.5 Configuration Management
- 5.10.6 Device Alarms
- 5.10.7 Tools
  - 5.10.7.1 Ping
  - 5.10.7.2 Traceroute
  - **5.10.7.3 Capture**
- 5.10.8 Scheduled Reboot
- 5.10.9 Log Server
- 5.10.10 Account Management
- 5.10.11 Other Settings
  - 5.10.11.1 Web Login Management
  - 5.10.11.2 Automatically Restart

#### ▲ 6. Security Precautions

## Deceleration

Thank you for choosing our company's product! Before use, please carefully read this user manual. By complying with the following statements, you will help maintain intellectual property rights and legal compliance, ensuring that your user experience aligns with the latest product information. If you have any questions or need written permission, please feel free to contact our technical support team.

- **Copyright Statement**

This user manual contains copyrighted content, and the copyright belongs to InHand Networks and its licensors. Without written permission, no organization or individual may excerpt, copy any part of the content of this manual, or distribute it in any form.

- **Disclaimer**

Due to ongoing updates in product technology and specifications, the company cannot guarantee that the information in the user manual is entirely consistent with the actual product. Therefore, no disputes arising from any discrepancies between the actual technical parameters and the user manual are accepted. Any changes to the product will not be notified in advance, and the company reserves the right to make the final changes and interpretations.

- **Copyright Information**

## Conventions

Symbol	Indication
[ ]	Referring to function modules or menus, such as in the [ Status ] menu."
" "	Referring to a button name, such as Clicking the "Add" button.
>	Multiple levels of menus are separated by "> ". For example, "File> New> Folder" represents the "Folder" menu item under the "New" submenu, which is under the "File" menu.
Cautions	Please be mindful of the following points during the operation, as improper actions may result in data loss or device damage.
Note	Supplement and provide necessary explanations for the description of the operation.

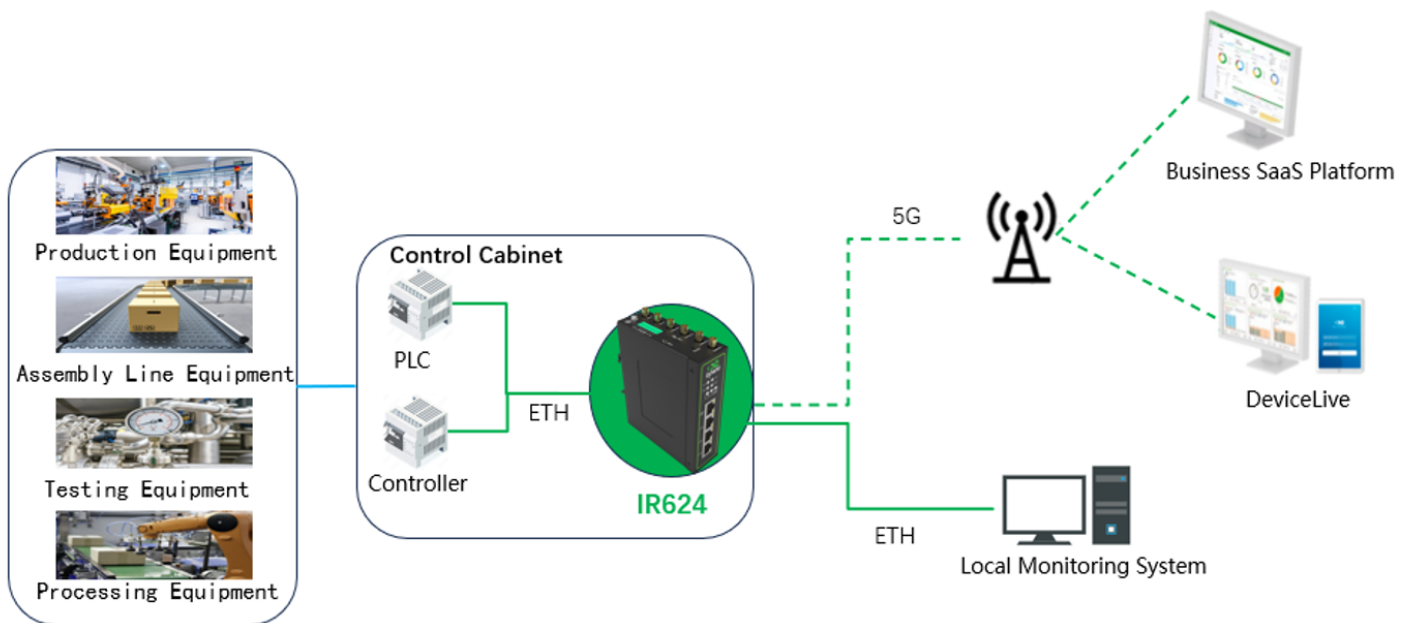
## Technical Support

E-mail : [support@inhandnetworks.com](mailto:support@inhandnetworks.com)

# 1. Overview

The IR624 series products are industrial router product that integrates 4G/5G, Wi-Fi, virtual private network (VPN) and other technologies. It provides uninterrupted network access capabilities, comprehensive security features, and intelligent software services for various IoT industry applications, providing a secure and reliable business data link for enterprises to achieve digital networking.

The IR624 series products are suitable for the networking of unattended devices and sites. It is embedded with watchdog and multi-layer link detection mechanisms to ensure reliable and stable communications. Meanwhile, combined with the InHand DeviceLive cloud platform, it is easy for enterprise users to conduct unified cloud management centrally, grasp status of devices effortlessly, save deployment costs and improve management efficiency, providing one-stop solutions for your large-scale IoT deployment.



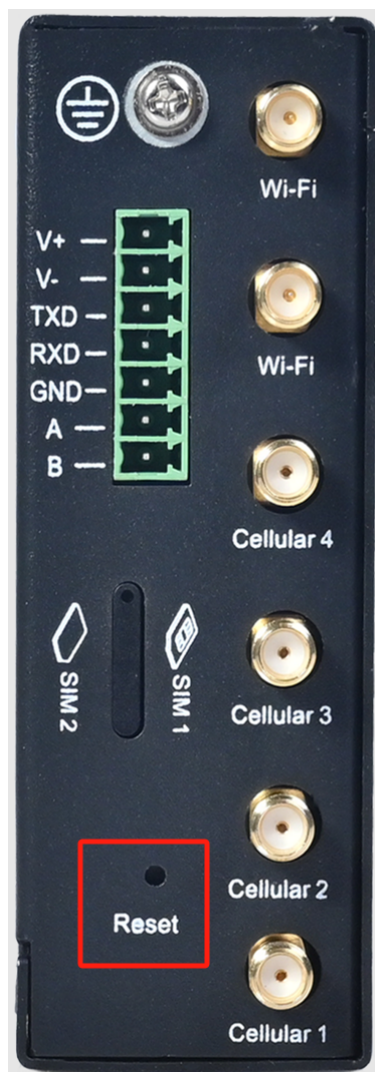
# 2. Hardware

## 2.1 LED Indicators

LED Indicators	Status and Description
SYS	Off --- Power off Steady in red --- Device starting Blink in red --- System error Steady in red --- Working properly Blink in red --- Firmware updating
NET	Off --- The WAN port is not connected Steady in green --- The WAN port is connected normally

	Blink in green --- Data Transferring
Cellular	Steady in green with one indicator --- Poor cellular signal Steady in green with two indicators --- Medium cellular signal Steady in green with three indicators --- Good cellular signal
Wi-Fi 2.4G	Off --- AP&STA is disabled Blink in green --- Working properly Steady in green --- Work as STA and AP is not associated
Wi-Fi 5G	Off --- AP&STA is disabled Blink in green --- Working properly Steady in green --- Work as STA and AP is not associated Steady in green --- Other abnormalities

## 2.2 Restore to Factory Defaults



To reset to factory default settings using the Reset button:

Step 1: After powering on, press and hold the reset button for 5~10 seconds, and the red will be solid.

Step 2: Release the button, red flashes.

Step 3: Press and hold the reset button again, release it after the red is solid and enter the system boot stage.

## 3. Default Settings

No.	Function	Default Settings
1	Cellular Dialing	Default dialing is set to "SIM1"
2	Wi-Fi	<ol style="list-style-type: none"><li>1. Wi-Fi 2.4G access point enabled, SSID: Prefixed with "IR624-", followed by the last 6 digits of the wireless MAC address.</li><li>2. Wi-Fi 5G access point enabled, SSID: Prefixed with "IR624-5G-", followed by the last 6 digits of the wireless MAC address.</li><li>3. The authentication method is WPA2-PSK.</li><li>4. The password for both is the last 8 digits of the serial number.</li></ol>
3	Ethernet	<ol style="list-style-type: none"><li>1. Enable all 3 LAN ports.</li><li>2. IP Address: 192.168.2.1 Subnet Mask: 255.255.255.0</li><li>3. DHCP server enabled, with an address pool from 192.168.2.2 to 192.168.2.100 for automatic IP address assignment to connected devices.</li></ol>
4	Network Access Control	Local HTTP and HTTPS are enabled with port numbers 80 and 443 respectively. Disable access from the cellular network.
5	Username/Password	adm/123456

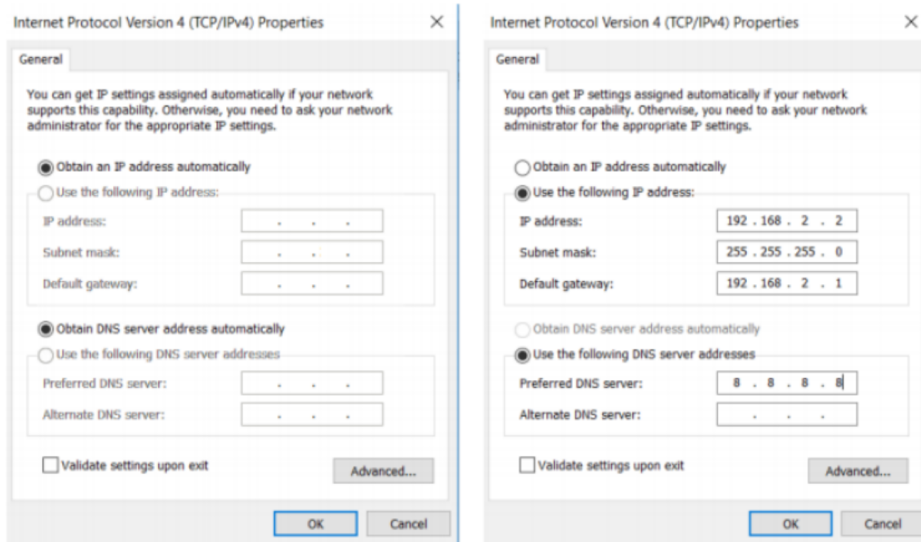
## 4. Quick Guide

### 4.1 Environment Setup

**Step 1:** Install the 4G/5G and Wi-Fi antennas and insert the SIM card.

**Step 2:** Connect the power cable and an Ethernet cable; connect any LAN port to your PC.

**Step 3:** Set your PC's IP address to be on the same subnet as the edge router.

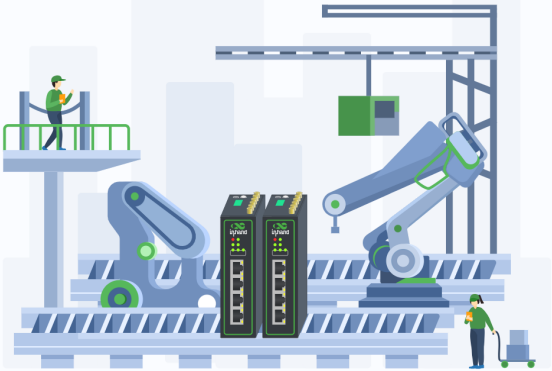



The device's LAN port has DHCP Server functionality enabled by default. Once the PC has automatically obtained an IP address, please ensure that your PC and router are in the same address range. If your PC fails to obtain an IP address automatically, please configure it with a static IP address and the following parameters: IP Address: **192.168.2.x** (Choose an available address within the range of 192.168.2.2 to 192.168.2.254). Subnet Mask: 255.255.255.0. Default Gateway: 192.168.2.1. DNS Servers: 8.8.8.8 (or your ISP's DNS server address)

**Step 4:** Enter the default device address **192.168.2.1**, in the browser's address bar. After entering the username and password (**adm/123456**), access the device's web management interface. If the page shows a security warning, click on the "Hide" or "Advanced" button and select "Proceed" to continue.

## Embrace 5G

### Co-Create the Digital Era





Login

Copyright © 2024 InHand Networks All rights reserved

## 4.2 Access the Internet



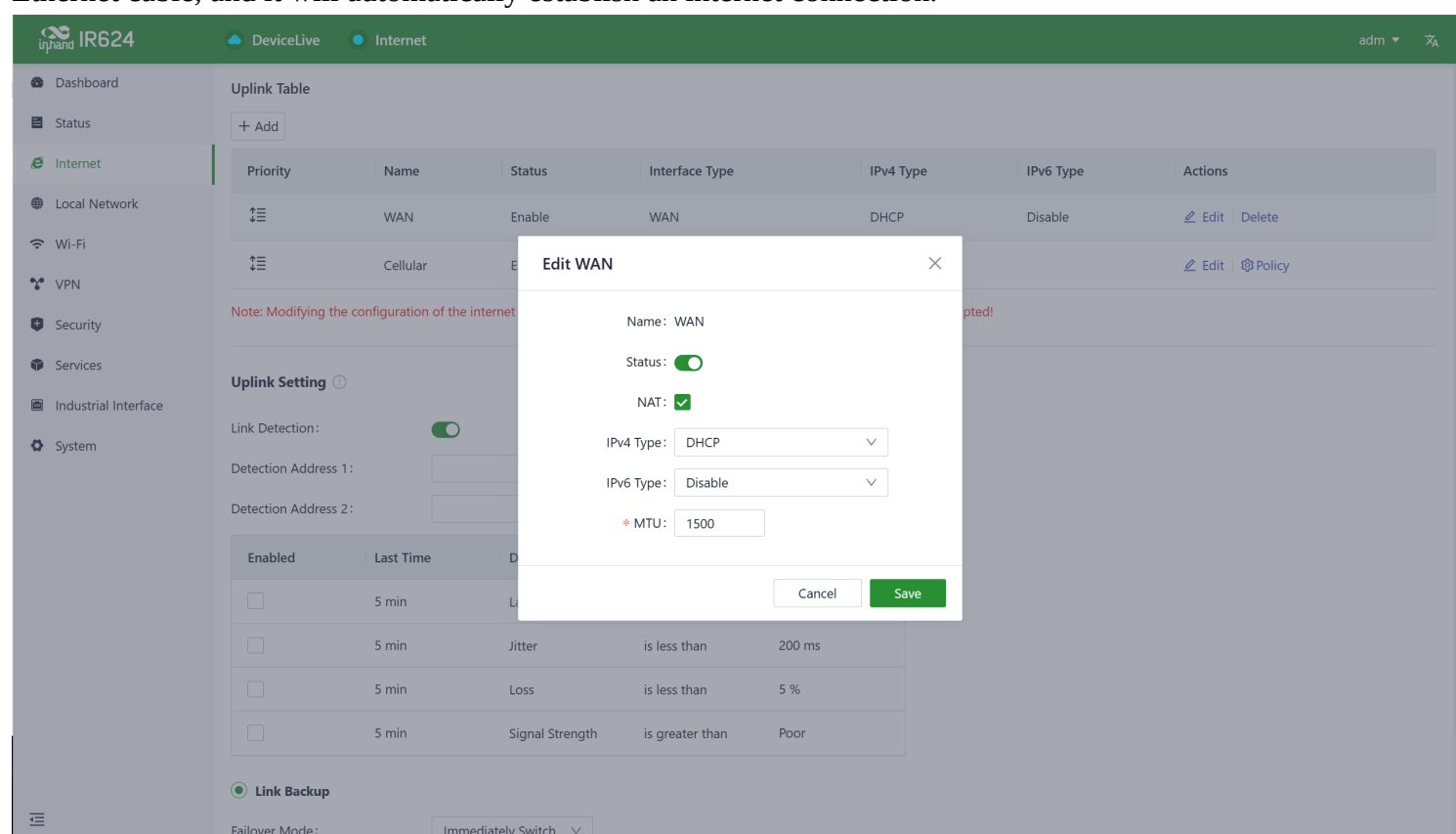
The IR624 supports three access network modes, including wired, cellular, and Wi-Fi. The device's WAN interface has DHCP service enabled by default. Simply connect the WAN interface to the internet using an Ethernet cable, and it will automatically establish an internet connection.

## 4.2.1 5G/4G

In the usual scenario, as per the instructions, upon inserting the SIM card and connecting the Wi-Fi antennas, the IR624 router will automatically establish a dial-up connection and connect to the network when powered on.

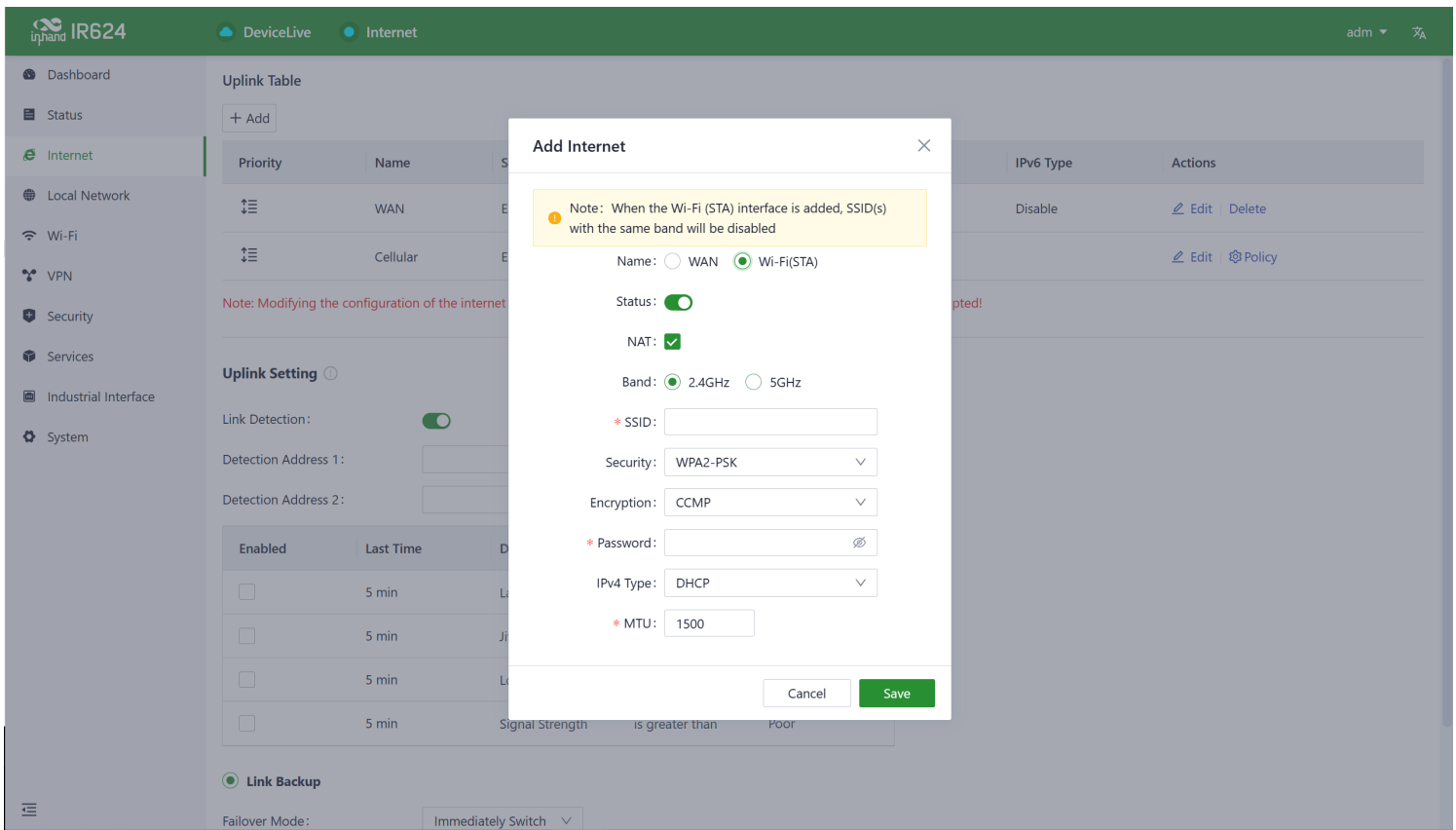
## 4.2.2 Wired Connection

The IR624 supports three wired internet connection methods: DHCP, Static IP, and PPPoE. The device's WAN interface has DHCP service enabled by default. Simply connect the WAN interface to the internet using an Ethernet cable, and it will automatically establish an internet connection.



## 4.2.3 Wi-Fi STA

The IR624 supports connecting as a client to an on-site AP's network. To do this, click on the "Add" button as shown in the illustration, select "Wi-Fi (STA)," and fill in the required parameters, including the SSID name and password.

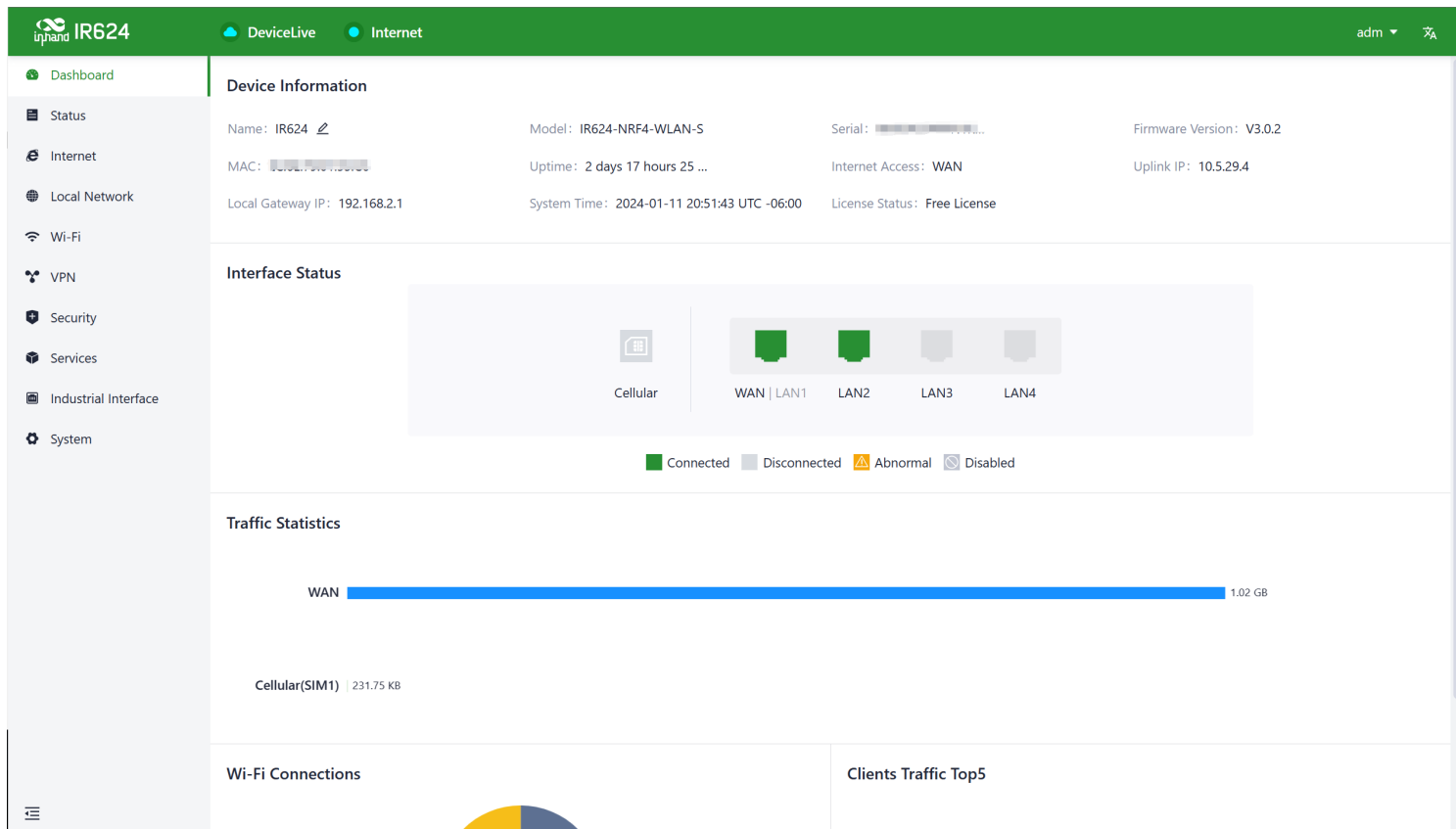


## 5. Configuration

### 5.1 Dashboard

#### 5.1.1 Device Information

In the [ Dashboard ] interface, users can find basic device information at the top, including the device name, device model, device serial number, MAC address, online duration, and upstream interface address.



- **Name:** Identifies the device's name, which is initially set to "IR624" but can be customized.
- **MAC Address:** Identifies the device's physical MAC address.
- **Local Gateway Address:** The default gateway address of the device's subnet.
- **Model:** Specifies the device's specific model, which can help determine if it supports cellular and WLAN features.
- **Uptime:** Reflects the device's running time since it was powered on.
- **System Time:** Displays the device's time zone and system time.
- **Serial:** A unique code that serves as an identifier for the device and can be used for indexing or adding the device to a platform account.
- **Internet Access:** The upstream interface used by the device for internet connectivity.
- **License Status:** Information about the applied license on the device, distinguishing between Small Star Cloud Manager Basic and Small Star Cloud Manager Professional.
- **Firmware Version:** Shows the device's current software version.
- **Uplink IP:** The IP address of the upstream interface used for device internet connectivity.

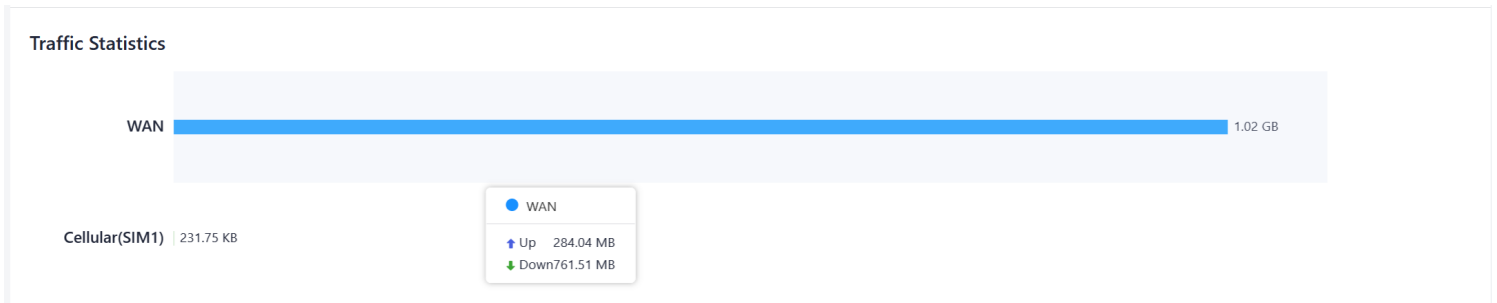
## 5.1.2 Interface Status

In the "Dashboard > Interface Status" feature, you can visually inspect the operational status of each interface. By clicking on the "Interface Icon," you can access detailed information for each interface in a pop-up box on the right-hand side of the interface.

The screenshot displays the InHand IR624 web interface. The top navigation bar includes 'DeviceLive' and 'Internet' status indicators. The left sidebar contains menu items: Dashboard, Status, Internet, Local Network, Wi-Fi, VPN, Security, Services, Industrial Interface, and System. The main content area is divided into three sections: 'Device Information' (Name: IR624, Model: IR624-NRF4-WLAN-S, Serial: RN62423499N1K..., MAC: EC:6E:79:01:55:C6, Uptime: 2 days 17 hours 33 ..., Internet Access: WAN, Local Gateway IP: 192.168.2.1, System Time: 2024-01-11 20:59:54 UTC -06:00, License Status: Free License), 'Interface Status' (Cellular, WAN | LAN1, LAN2, LAN3, LAN4), and 'Traffic Statistics' (WAN, Cellular(SIM1) | 231.75 KB, Wi-Fi Connections, Clients Traffic Top5). A right-hand panel titled 'Interface Status' provides detailed configuration for the WAN interface, including Status (Connected), Work Mode (Active), IPv4 Type (DHCP), IPv4 Address (10.5.29.4/24), IPv4 Gateway Address (10.5.29.254), Lease Acquisition Time (2024-01-11 14:31:28), Lease Timeout (2024-01-12 14:31:28), Primary DNS, Secondary DNS, IPv6 Type (Disable), IPv6 Address, IPv6 Gateway Address, Main IPv6 DNS, Secondary IPv6 DNS, and Test Connectivity to.

### 5.1.3 Traffic Statistics

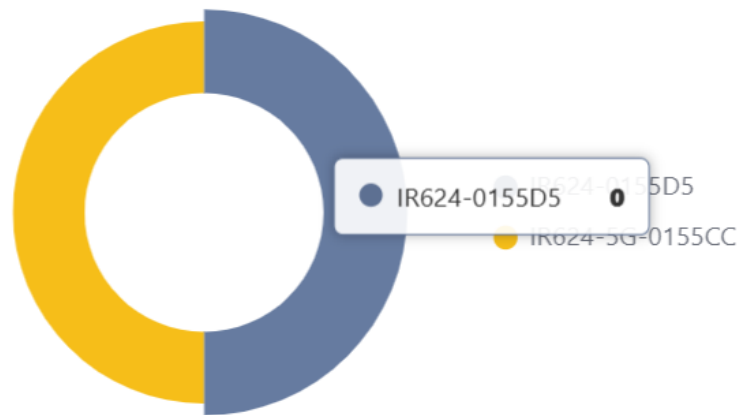
Users can monitor the usage of traffic on each upstream interface since the router was powered on through the "Dashboard > Traffic Statistics" feature. The data in traffic statistics will reset after the device is rebooted. If you need to review historical traffic records, you can access this information on the device's details page within InCloud Manager.



### 5.1.4 Wi-Fi Connections

In the "Dashboard > Wi-Fi Client Count" feature, users can check the number of active SSIDs on the IR624 and the number of connected clients under each SSID.

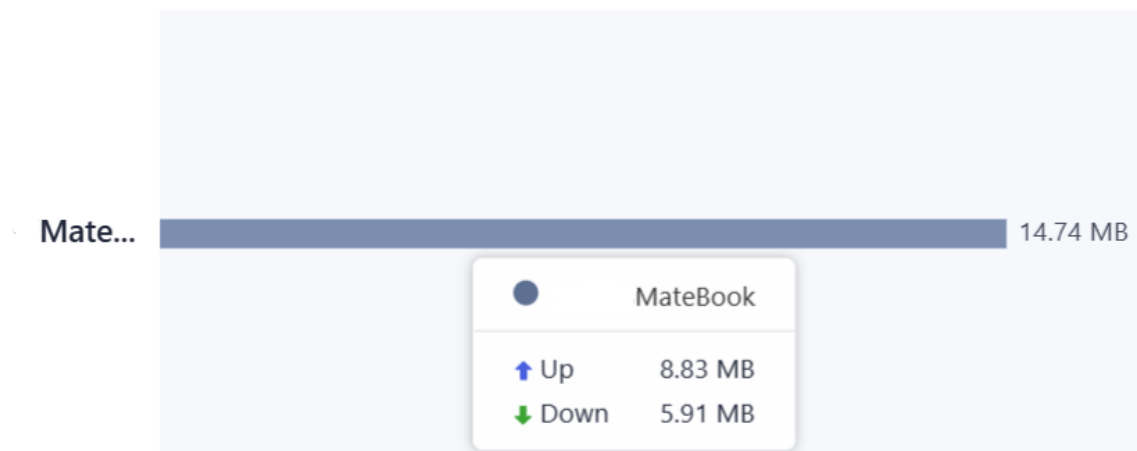
## Wi-Fi Connections



### 5.1.5 Clients Traffic Top5

In the "Dashboard > Top 5 Client Traffic" feature, users can view the current ranking of client traffic usage for devices connected to the router. It displays up to 5 records, and when a client disconnects, its statistical data will be cleared.

#### Clients Traffic Top5

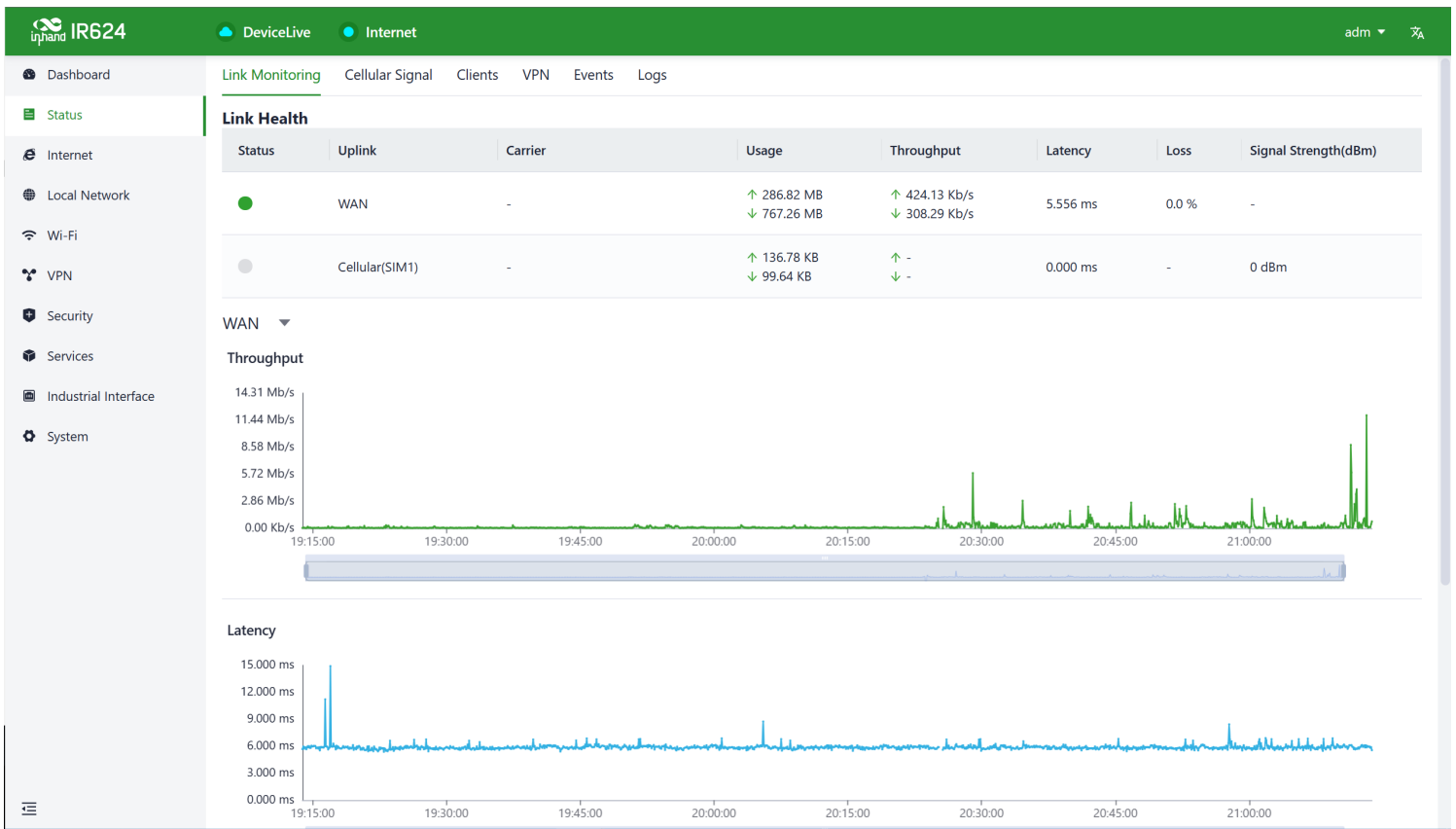


## 5.2 Status

Under the [Status] function, you can view the uplink status of the device, device operation logs, events, etc., which helps to grasp the device operation status more accurately

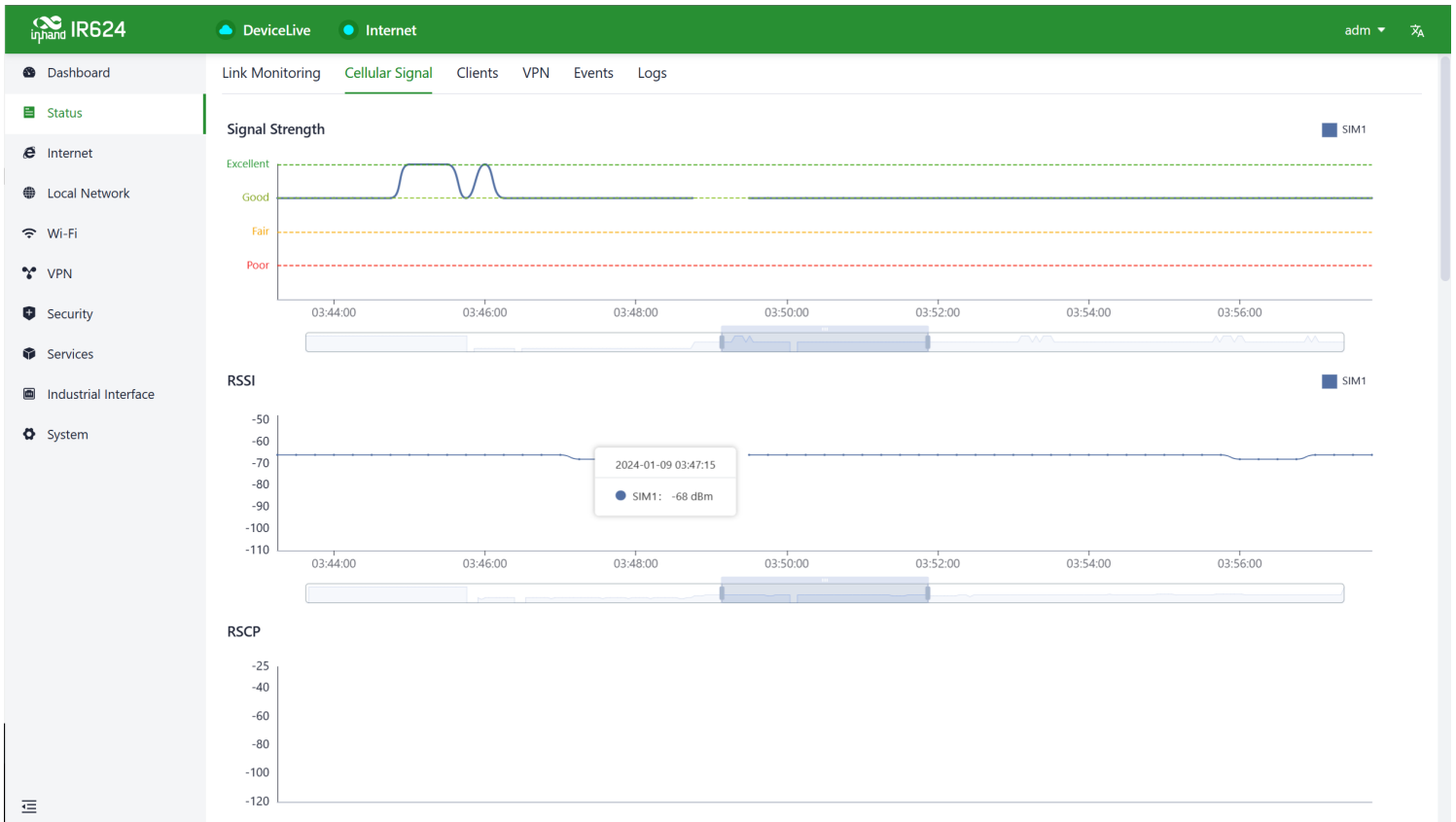
### 5.2.1 Link Monitor

You can utilize the "Status > Link Monitoring" feature to check the health status of each upstream link and access information about throughput, latency, packet loss, signal strength, and more for each interface.



## 5.2.2 Cellular Signal

You can access the "Status > Cellular Signal" feature to check the signal strength of SIM cards under the cellular interface, along with parameters such as RSSI, SINR, RSRP, and more.



## 5.2.3 Clients

Through the "Status > Clients" feature, users can view detailed information about both wired and wireless clients connected to the router. This includes details such as names, addresses, MAC addresses, VLANs, connected subnets, traffic usage, online duration, and more.

The screenshot shows the inhand IR624 web interface. The top navigation bar includes 'DeviceLive' and 'Internet' status indicators. The main menu on the left lists various system features. The 'Status' section is active, and the 'Clients' tab is selected. A filter bar shows 'All 1', 'Wired 1', and 'Wireless 0' counts. Below the filter is a table of connected clients.

Name	IP Address	MAC Address	VLAN	Connection	Traffic	UP	Down	Uptime
[REDACTED]	192.168.2.147	[REDACTED]	1	Default	26.57 MB	12.76 MB	13.80 MB	55 minutes

1-1 of 1 items < 1 >

## 5.2.4 VPN

You can access the "Status > VPN" feature to view information about IPSec VPN and L2TP VPN, including their status, traffic, and the duration of the most recent connection.

## 5.2.5 Events

You can use the "Status > Events" feature to check event information related to the device's operation, helping users understand the device's operational status.

Currently supported event types:



- Successful/Failed User Logins.
- High CPU Utilization in the Last 5 Minutes.
- High Memory Utilization in the Last 5 Minutes.
- Cellular Traffic Reaches Threshold.
- VPN Status Changes.
- Uplink Status Changes.
- Uplink Switching.
- WAN2/LAN1 Switching.
- Reboot.
- Upgrade.

## 5.2.6 Logs

Through the "Status > Logs" feature, users can examine the system logs, which contain information about the device's operational history. When the device encounters issues, technical personnel can use these logs for troubleshooting and diagnosis.

The screenshot displays the 'Logs' page in the inhand IR624 web interface. The top navigation bar shows 'DeviceLive' and 'Internet' status. The left sidebar contains a menu with 'Status' selected. The main area features a search bar with 'Level: ALL' and a 'Key:' field. Below this is a table of log entries:

Level	Time	Content
Information	Jan 11 21:23:04	redial[1026]: modem response (6): ^M OK^M
Information	Jan 11 21:23:04	redial[1026]: detecting modem register status (1/30)...
Information	Jan 11 21:23:04	redial[1026]: send to modem (12): AT+C5GREG?^M
Information	Jan 11 21:23:04	redial[1026]: modem response (46): ^M +C5GREG: 2,8,"280413","901515003",11^M ^M OK^M
Information	Jan 11 21:23:07	redial[1026]: detecting modem register status (2/30)...
Information	Jan 11 21:23:07	redial[1026]: send to modem (11): AT+CEREG?^M
Information	Jan 11 21:23:07	redial[1026]: modem response (21): ^M +CEREG: 2,0^M ^M OK^M
Information	Jan 11 21:23:10	redial[1026]: detecting modem register status (3/30)...
Information	Jan 11 21:23:10	redial[1026]: send to modem (11): AT+CGREG?^M
Information	Jan 11 21:23:10	redial[1026]: modem response (21): ^M +CGREG: 2,0^M ^M OK^M
Information	Jan 11 21:23:13	redial[1026]: detecting modem register status (4/30)...
Information	Jan 11 21:23:13	redial[1026]: send to modem (12): AT+C5GREG?^M
Information	Jan 11 21:23:13	redial[1026]: modem response (46): ^M +C5GREG: 2,8,"280413","901515003",11^M ^M OK^M

At the bottom right of the log table, there are three buttons: 'Clear Logs', 'Download Logs', and 'Diagnostic Logs'.

- **Download Logs:** Download the device's operational logs.
- **Download Diagnostic Logs:** Download the device's diagnostic logs, which include system operation logs, device information, and device configurations.
- **Clear Logs:** Clear the device's operational logs; this does not clear the device's diagnostic logs.

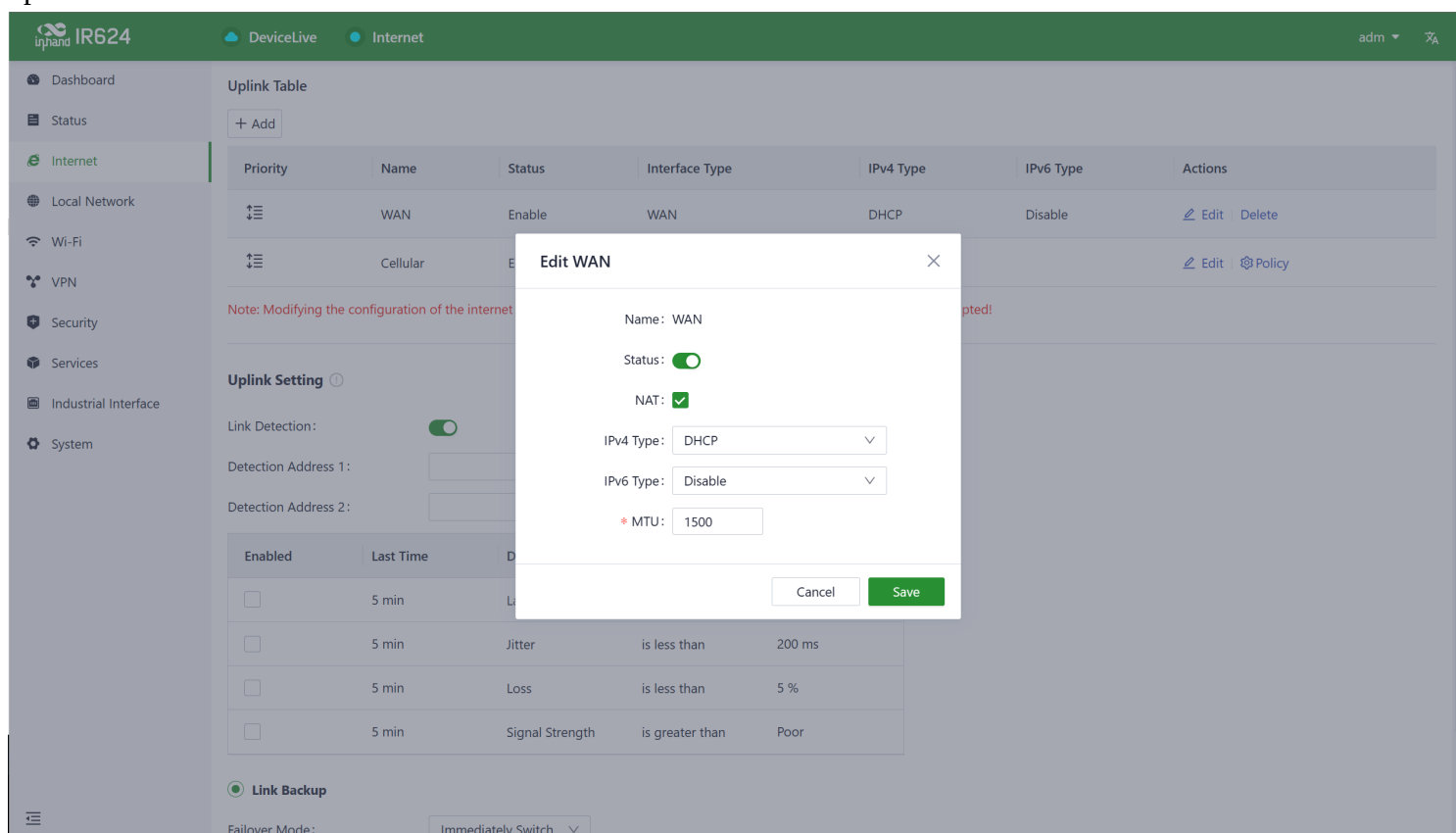
## 5.3 Internet

You can configure the parameters and operational modes of each upstream interface under the "Internet" feature. The IR624 supports three access network modes, including wired, cellular, and Wi-Fi. The device comes with two non-removable upstream links by default, WAN1, and Cellular. It can support up to four upstream links, including WAN1, Cellular, and Wi-Fi (STA). Wi-Fi (STA) interfaces need to be manually added and can be removed as needed.

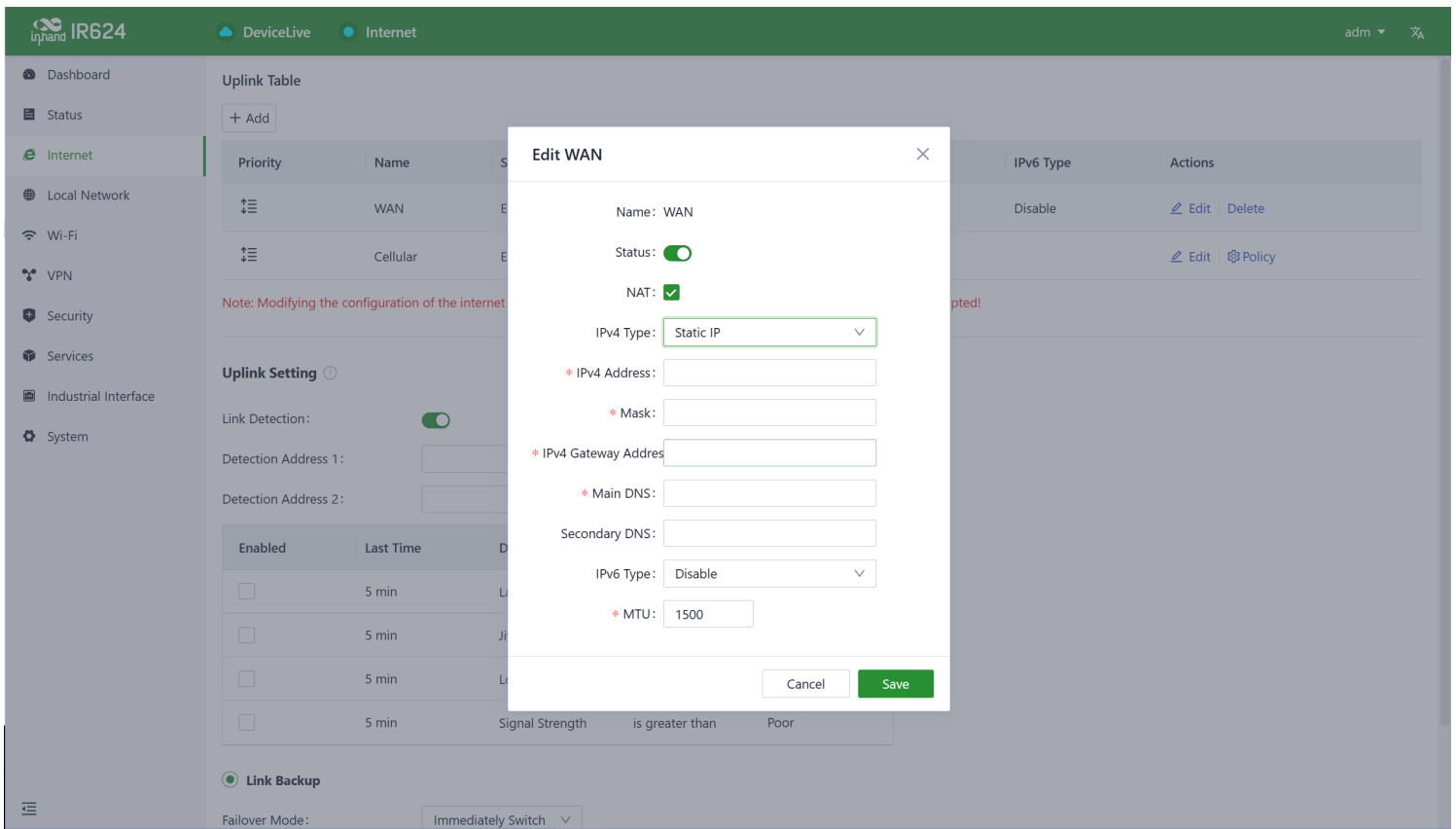
### 5.3.1 Wired Connection

You can configure the parameters and operation modes for each upstream interface under the "Internet" function. IR624 supports three access network modes: wired, cellular, and Wi-Fi. It can support up to three upstream links, including WAN, cellular, and Wi-Fi (STA).

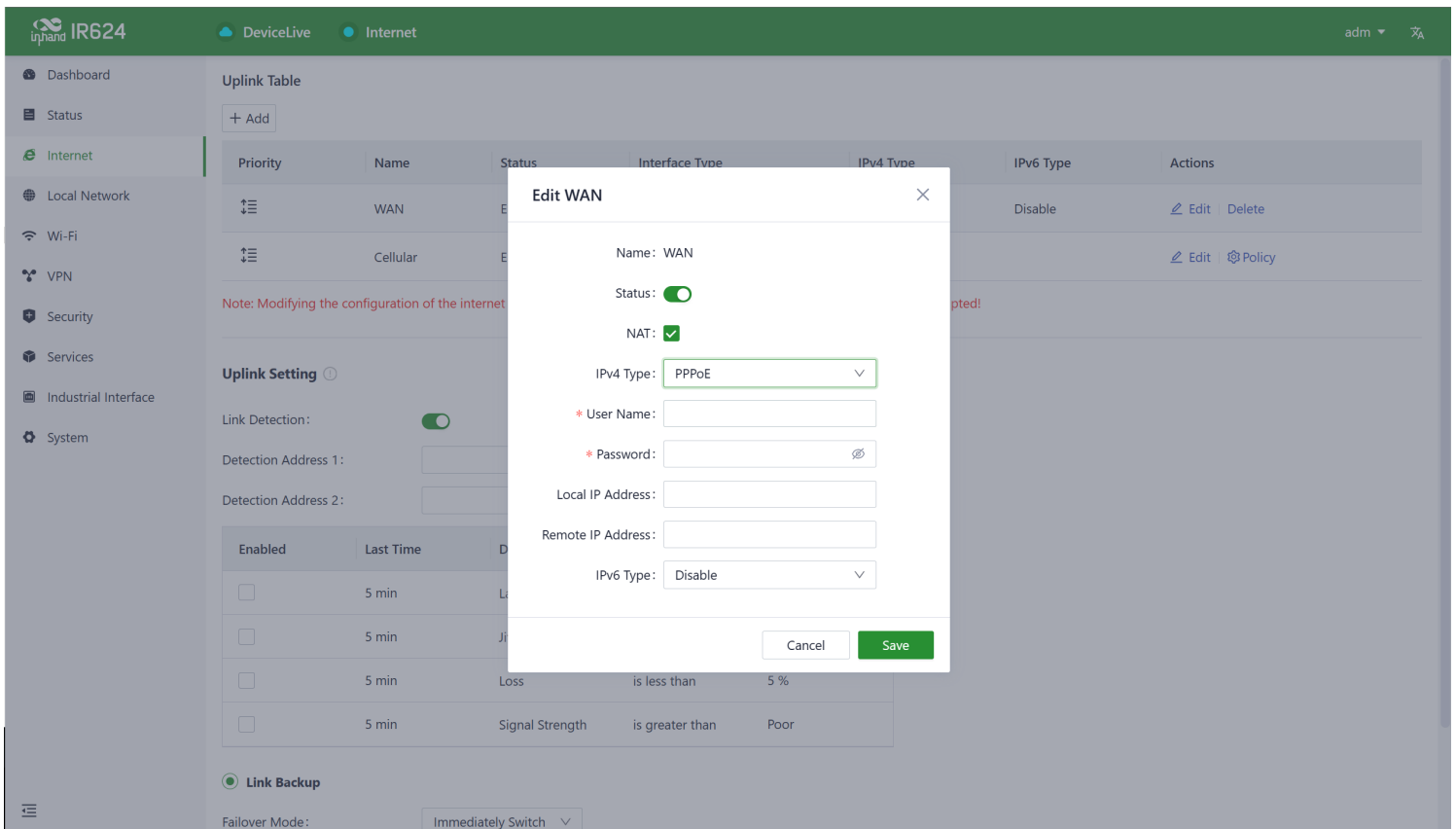
The WAN and Wi-Fi (STA) interfaces need to be manually added and can be deleted as needed; the cellular upstream link cannot be deleted.



- **DHCP:** The device's WAN interface has DHCP service enabled by default. Simply connect the WAN interface to the internet using an Ethernet cable, and it will automatically establish an internet connection.
- **Static IP:** Users have the option to manually configure an address either obtained from their internet service provider or one that is within the same network segment as their upstream device. Once the configuration is complete, the router will access the network via the specified static IP address.

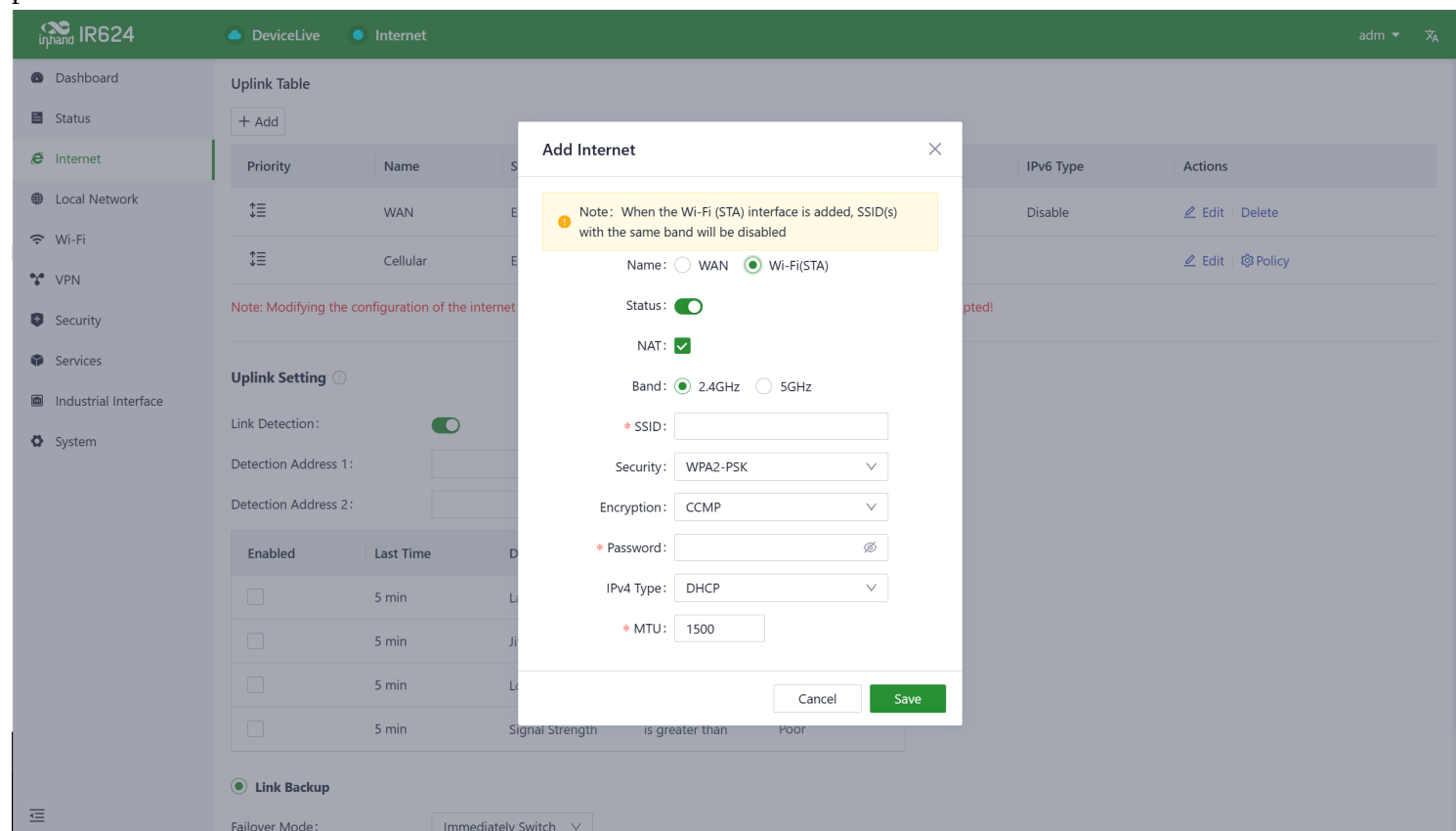


- **PPPoE:** Users have the option to configure broadband dial-up. Once the configuration is complete, the router will establish an internet connection through the broadband dial-up.



## 5.3.2 Wireless Connection

The IR624 supports connecting as a client to an on-site AP's network. To do this, click on the "Add" button as shown in the illustration, select "Wi-Fi (STA)," and fill in the required parameters, including the SSID name and password.

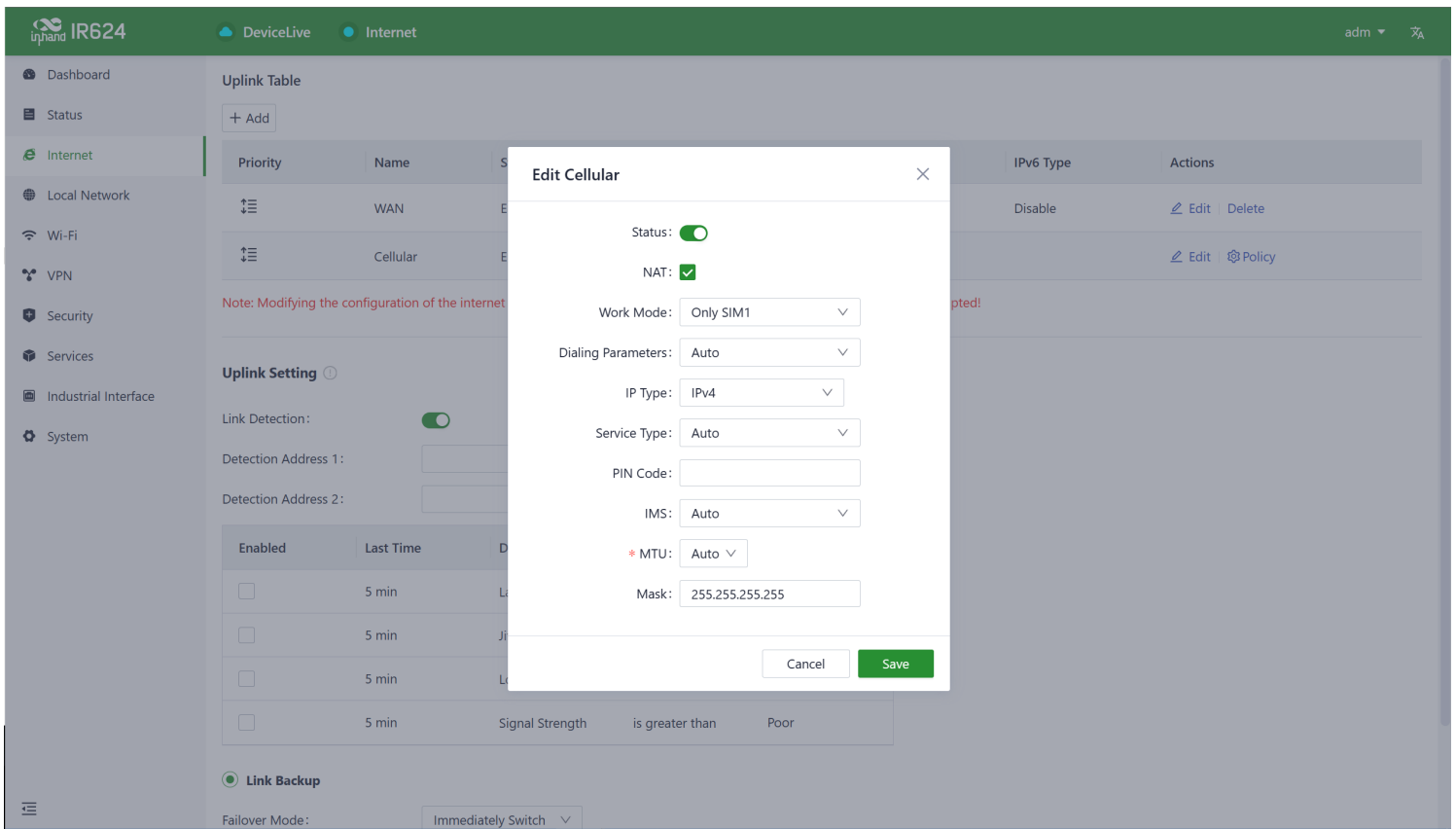


### Cautions:

- Upon adding Wi-Fi (STA), IR624 will automatically disable SSIDs in the same frequency band within the Wi-Fi settings, and the status field for those SSIDs cannot be modified.
- After removing Wi-Fi (STA), the "Status" field and SSIDs in the same frequency band within the Wi-Fi settings can be modified.
- When Wi-Fi (STA) is deleted, all configuration associated with the Wi-Fi (STA) interface, including static routes, inbound/outbound rules, port forwarding, policy routing, and traffic shaping settings, will be removed.

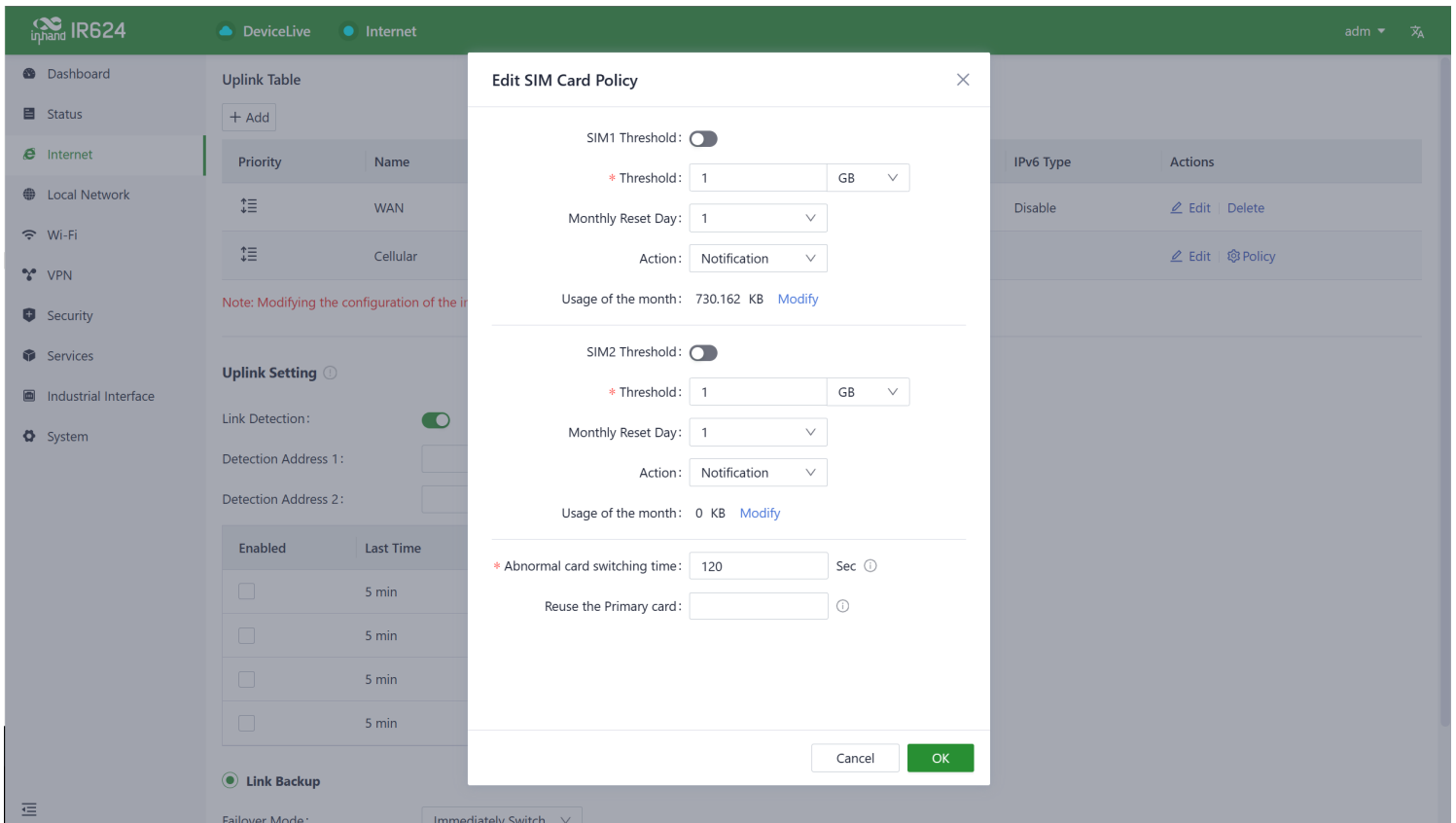
### 5.3.3 5G/4G Connection

In the usual scenario, as per the instructions, upon inserting the SIM card and connecting the Wi-Fi antennas, the IR624 router will automatically establish a dial-up connection and connect to the network when powered on. To configure APN (Access Point Name) parameters, users can select the "Cellular" interface in the [ Internet ] menu and click the "Edit" button to access the APN parameter configuration interface.



The IR624, in addition to supporting cellular internet access, now includes a traffic policy feature. Once the policy is enabled, the SIM card will take specific actions when the traffic reaches a threshold. Traffic usage statistics will reset at the beginning of the next month.

You can select the "Cellular" interface in the [ Internet ] menu and click the "Policy" button to access the SIM card's policy parameter configuration interface.



- **Actions:** These are the actions triggered when SIM card traffic reaches a threshold.
  - **Notification:** It generates an event when traffic reaches the threshold but does not stop forwarding regular business traffic.
  - **Cloud Management Only:** It generates an event when traffic reaches the threshold, allowing only the forwarding of cloud-based management traffic while blocking access to the internet for regular business traffic.
  - **Switch the SIM card:** It generates an event when traffic reaches the threshold and switches to another SIM card for internet access.

### Cautions:

- In certain dedicated network scenarios, it may be necessary to manually disable the "Link Detection" function under the [ Internet ] menu to prevent cellular connectivity issues caused by unsuccessful detection.
- In some cases, manual configuration of the subnet mask for the cellular interface may be required to ensure the proper functioning of the ARP (Address Resolution Protocol) feature.
- When inserting or removing a SIM card, it is essential to disconnect the power to prevent data loss or damage to the device.

## 5.3.4 Uplink Table

You can add/edit/remove the WAN and Wi-Fi (STA) interfaces in the "Internet > Uplink Table." You can also adjust the priority of each interface by dragging the "Priority" icon. Interfaces are arranged from top to bottom based on their priority, with higher priority interfaces taking precedence in determining the current upstream interface for device operation.

Priority	Name	Status	Interface Type	IPv4 Type	IPv6 Type	Actions
☰	WAN	Enable	WAN	DHCP	Disable	<a href="#">Edit</a>   <a href="#">Delete</a>
☰	Cellular	Enable	Cellular: SIM1	Auto		<a href="#">Edit</a>   <a href="#">Policy</a>

Note: Modifying the configuration of the internet interface or adjusting the priority may cause the device network to be interrupted!

## 5.3.5 Uplink Settings

You can configure link detection settings and establish collaboration modes between different upstream interfaces through the "Internet > Upstream Link Settings" feature.

## Uplink Setting !

Link Detection:

Detection Address 1:  !

Detection Address 2:

Enabled	Last Time	Detection Item	Constraint	Value
<input type="checkbox"/>	5 min	Latency	is less than	200 ms
<input type="checkbox"/>	5 min	Jitter	is less than	200 ms
<input type="checkbox"/>	5 min	Loss	is less than	5 %
<input type="checkbox"/>	5 min	Signal Strength	is greater than	Poor

### Link Backup

Failover Mode:  ▼

### Load balancing

**Link Detection Switch:** The device has link detection functionality enabled by default. However, in certain specialized network environments where external communication is not possible, users may need to manually disable link detection. When link detection is turned off, users won't be able to view latency, jitter, packet loss, signal strength, and other information for upstream interfaces in the [ Status ] menu.

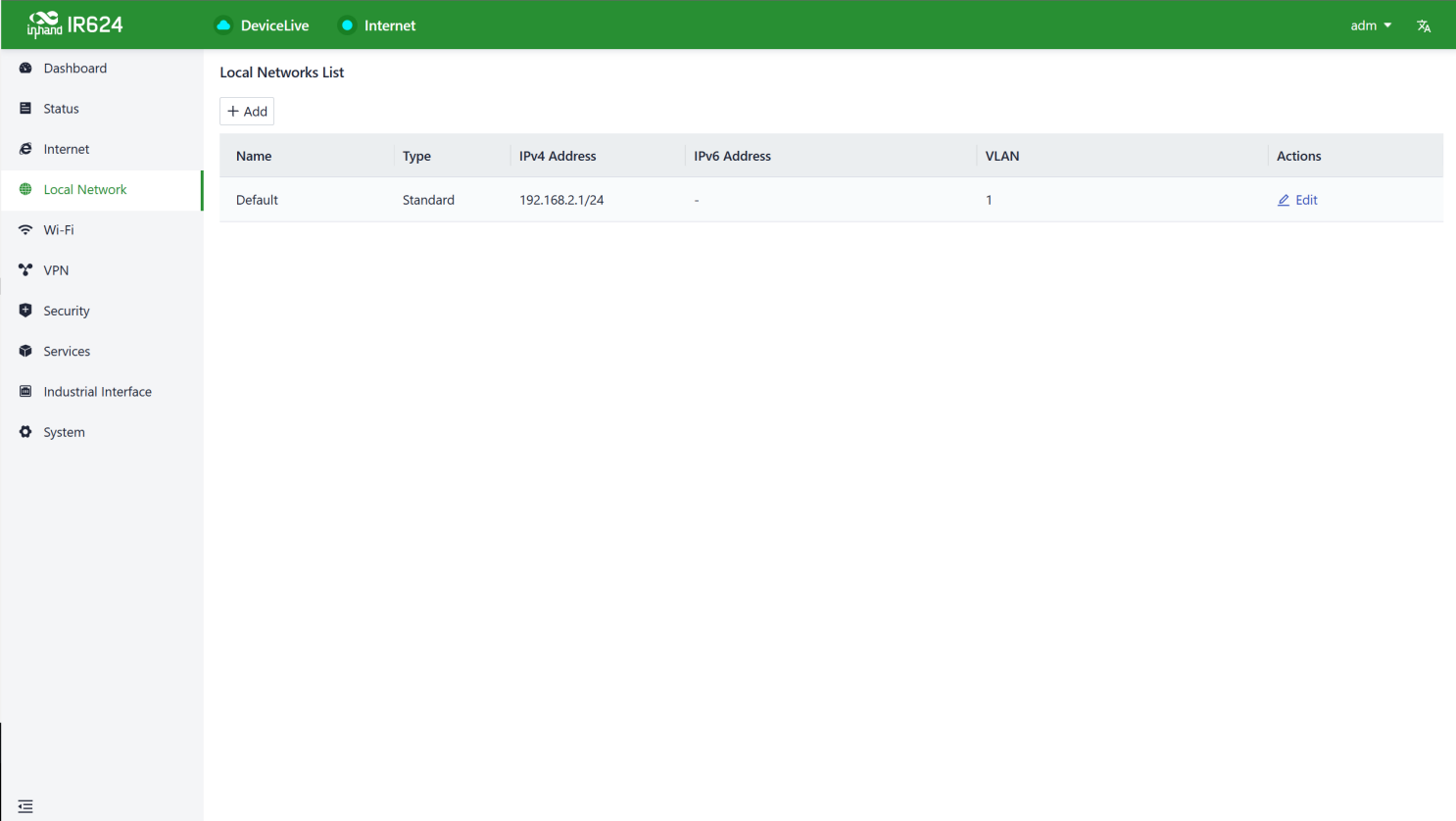
### Notes:

- Modifying settings in the Internet menu can potentially lead to a disruption in device connectivity. Exercise caution when making changes.
- When the link detection address is left empty, the default behavior is to detect the DNS address via the upstream interface. If you specify a detection address, all upstream interfaces will only detect the address you provided.
- In the router's link backup mode, users can customize detection parameters, and the device will switch links based on the enabled detection items. When detection items are not enabled, upstream link switching will only occur based on priority and link connectivity.

- In the device's load balancing mode, all operational upstream links will forward business traffic, provided they are functioning correctly.

## 5.4 Local Network

In the [ Local Network ] feature, users have the flexibility to define their local subnets. This includes configuring the address range, VLAN ID, DHCP services, and other related parameters for the local LAN. Once the configuration is complete, users need to further apply these settings to the device's LAN port through [ Interface Management ] or apply them to the desired SSID in the Wi-Fi settings. This series of operations is intended to ensure that client devices can smoothly connect to the local network according to the planned network addresses.

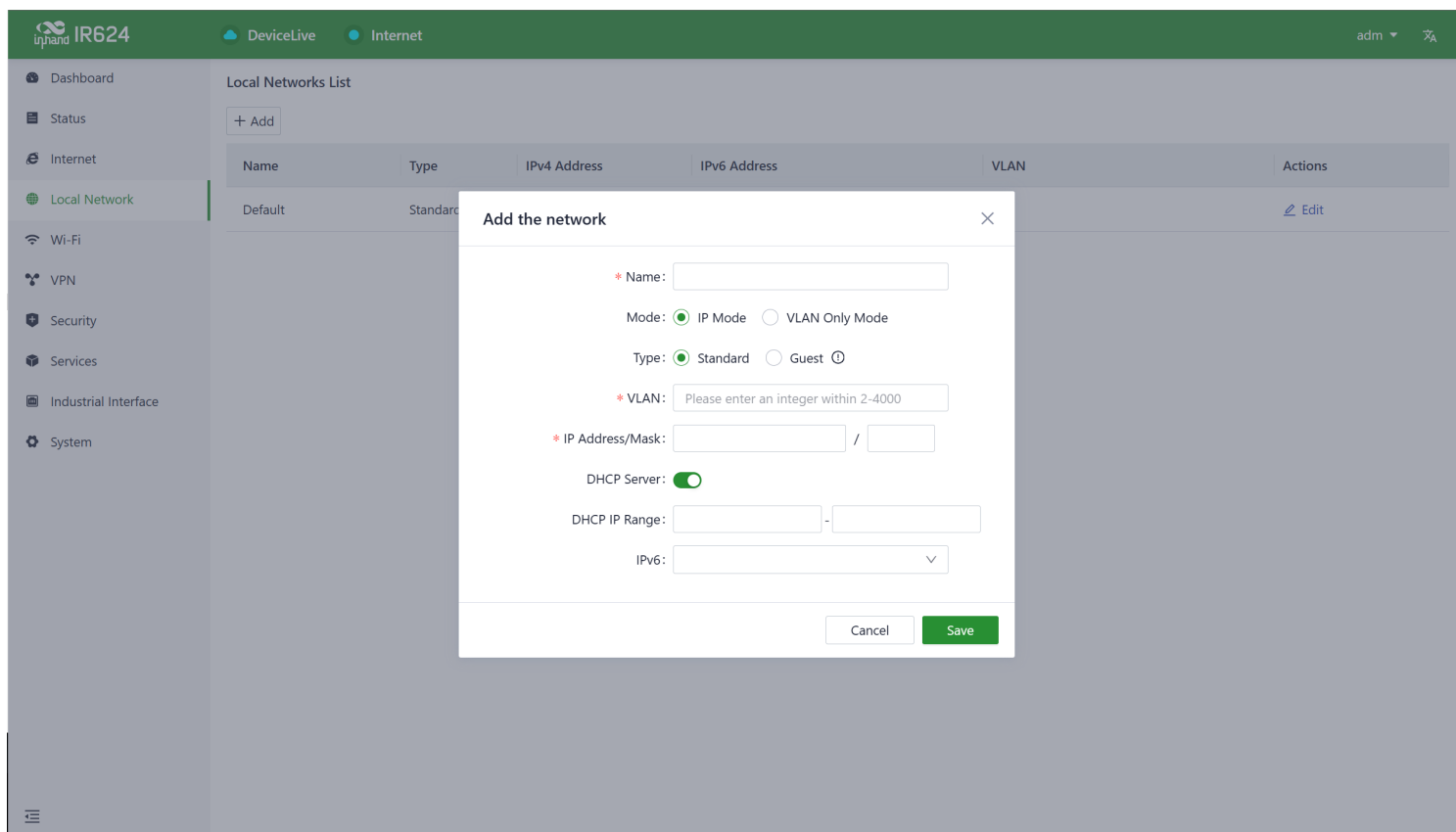


The screenshot displays the InHand IR624 web interface. The top navigation bar is green and contains the InHand logo, the model number 'IR624', and status indicators for 'DeviceLive' and 'Internet'. A user profile dropdown is visible on the right. A left sidebar menu lists various system settings: Dashboard, Status, Internet, Local Network (highlighted), Wi-Fi, VPN, Security, Services, Industrial Interface, and System. The main content area is titled 'Local Networks List' and features a '+ Add' button. Below this is a table with the following data:

Name	Type	IPv4 Address	IPv6 Address	VLAN	Actions
Default	Standard	192.168.2.1/24	-	1	<a href="#">Edit</a>

Click the "Add/Edit" button to add a new local network or edit an existing one.





**Name:** Used to identify the network. Users can select this name to apply the network in both [ Wi-Fi ] and [ Interface Management ].

**Mode:** Choose whether the current subnet operates in 2-layer transparent mode or 3-layer IP mode. The default is "IP mode."

**VLAN:** This allows for the division of the local network into different virtual logical networks. The default VLAN for all interfaces and Wi-Fi is "default (VLAN1)."

**IP Address/Subnet Mask:** This is the gateway address for accessing the router through the LAN port or Wi-Fi. The default is "192.168.2.1."

**DHCP Server:** Clients connecting to the router can obtain IP addresses through this function. It is enabled by default, and the address range is generated based on the "IP Address/Subnet Mask."

**Note:**

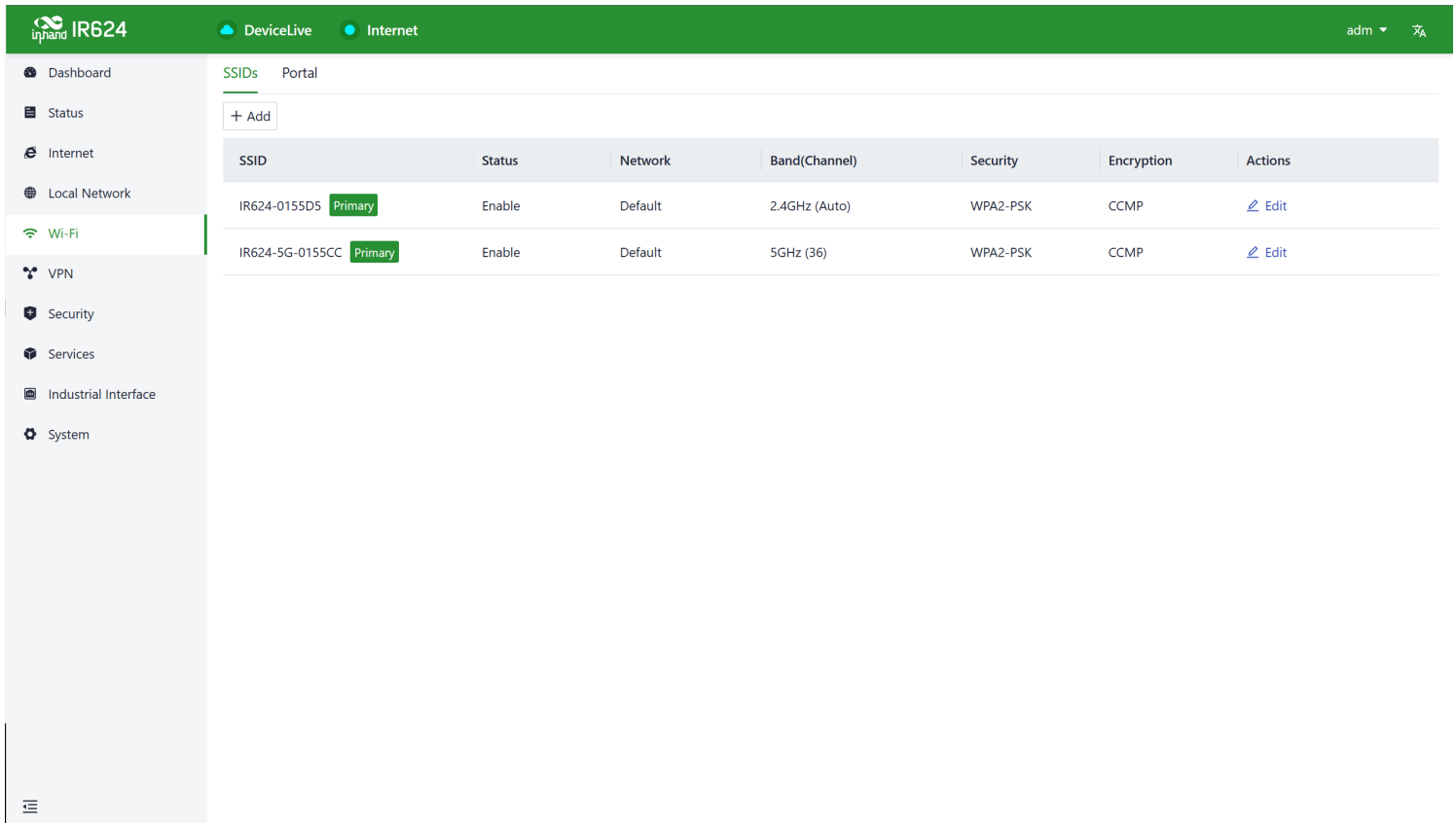
- The default local network cannot be deleted, and you can only modify the IP address/subnet mask and DHCP server settings.
- Once a local network is added, you cannot change its mode.
- The VLAN Only mode is designed for 2-layer transparent operation and doesn't require configuration of IP address/subnet mask or DHCP server settings.

## 5.5 Wi-Fi

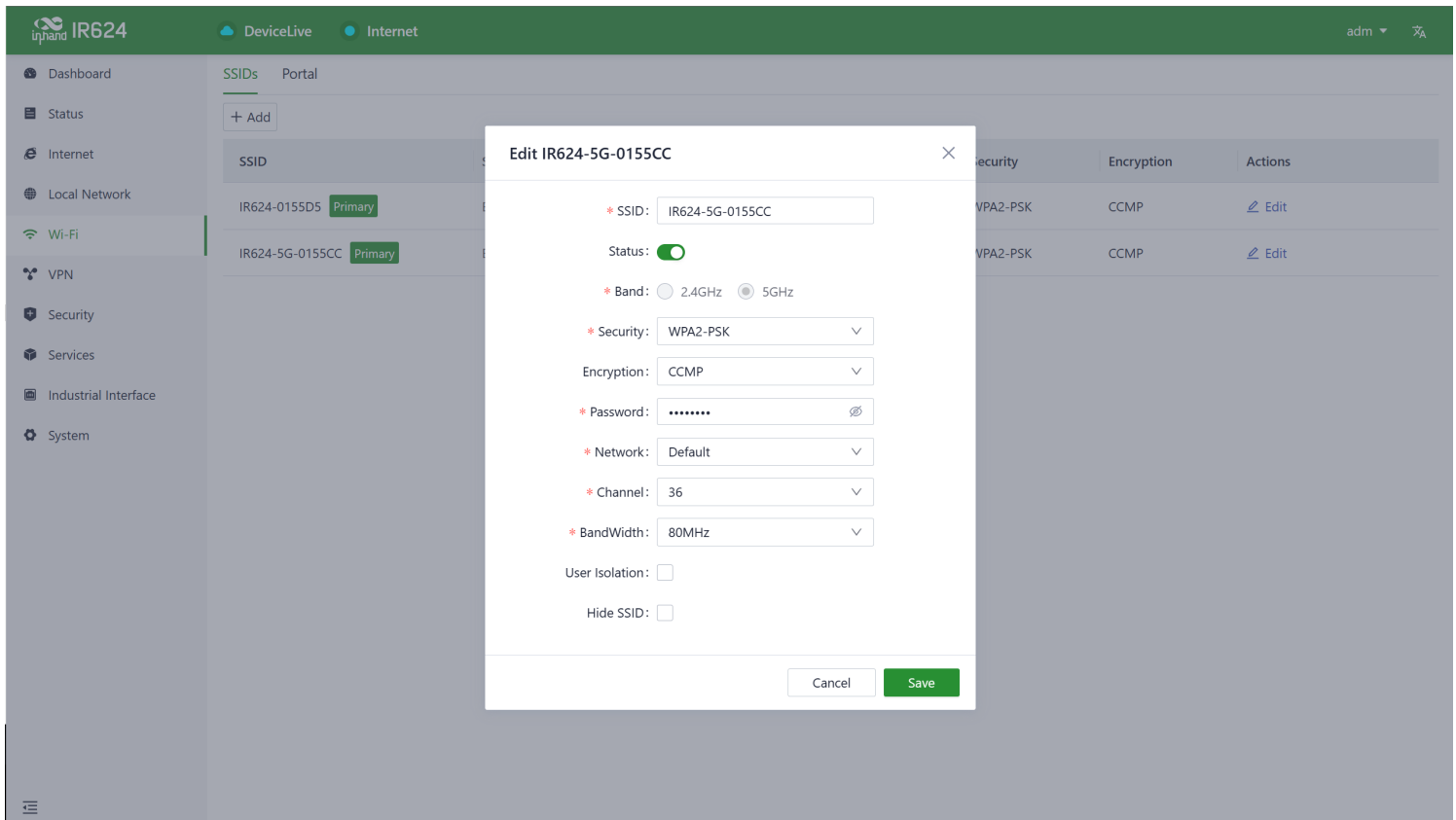
Wi-Fi is a widely used wireless communication technology that enables computers, smartphones, tablets, and other devices to connect to the internet or a local network. Wi-Fi technology allows devices to transmit data over a certain range through wireless signals, providing the convenience of accessing networks without the need for physical connections.

## 5.5.1 SSIDs

The IR624 can function as an Access Point (AP) to provide multiple SSID wireless network access. Users have the flexibility to customize different SSIDs for various purposes and configurations.



By clicking the "Add/Edit" button under "Wi-Fi > Wi-Fi List," you can add a new SSID or edit an existing one.



- The device comes with default 2.4GHz and 5GHz main SSIDs. The frequency bands of these main SSIDs cannot be modified and cannot be deleted.
- Once an SSID is added, its frequency band cannot be changed, and it will automatically use the same channel as its corresponding main SSID.
- If a user creates a Wi-Fi (STA) interface in the "Internet" menu with the same frequency band as an existing SSID, that SSID cannot be enabled until the Wi-Fi (STA) interface is deleted.

## 5.5.2 Portal

In scenarios where hotels and restaurants provide zero-hour Wi-Fi for customers, the Wi-Fi portal function can ensure the security of wireless access to a certain extent, and merchants can customize slogans and backgrounds on the authentication page for publicity.

The screenshot shows the 'Add Portal' configuration page in the InHand IR624 web interface. The page is organized into two main sections: 'Portal Setting' and 'Guest Login Page'.

**Portal Setting:**

- Name:** A text input field.
- Authentication Type:** A dropdown menu currently set to 'Click-Passthrough'.
- Target SSID:** A text input field.

**Guest Login Page:**

- Background Image:** A dropdown menu currently set to 'None'.
- Logo:** A dropdown menu currently set to 'None'.
- Splash Language:** A dropdown menu currently set to 'English'.
- Color Scheme:** A section with five color pickers:
  - Background Color:** A light gray color.
  - Title Color:** A dark blue/black color.
  - Text Color:** A dark blue/black color.
  - Box Color:** A light gray color.
  - Button Color:** A green color.
- Title:** A text input field containing 'Welcome to the InHand network'.
- Welcome Message:** A large text area for a custom message.
- Button Text:** A text input field containing 'Continue to the Internet !'.
- Box opacity:** A text input field containing '90'.

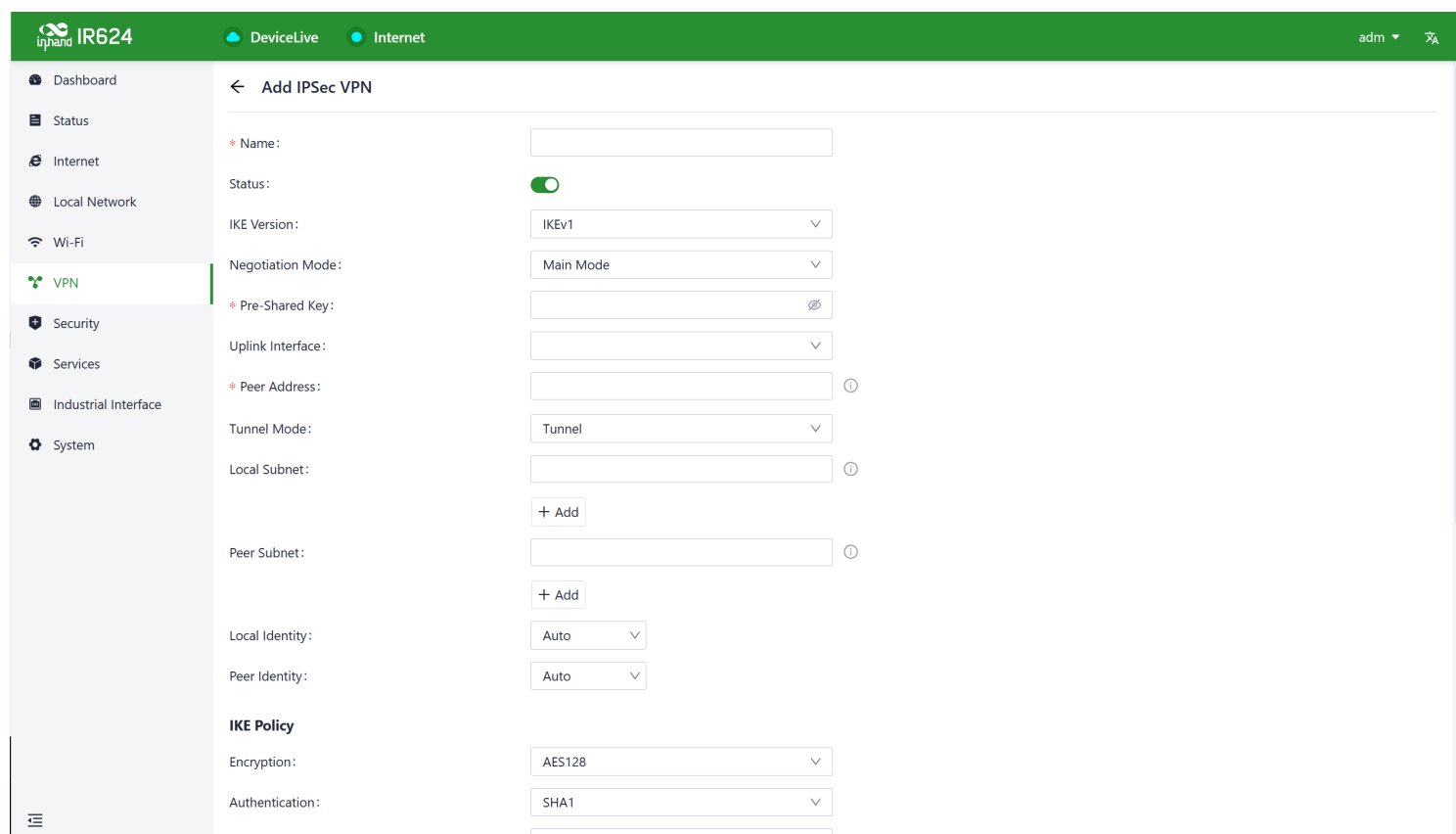
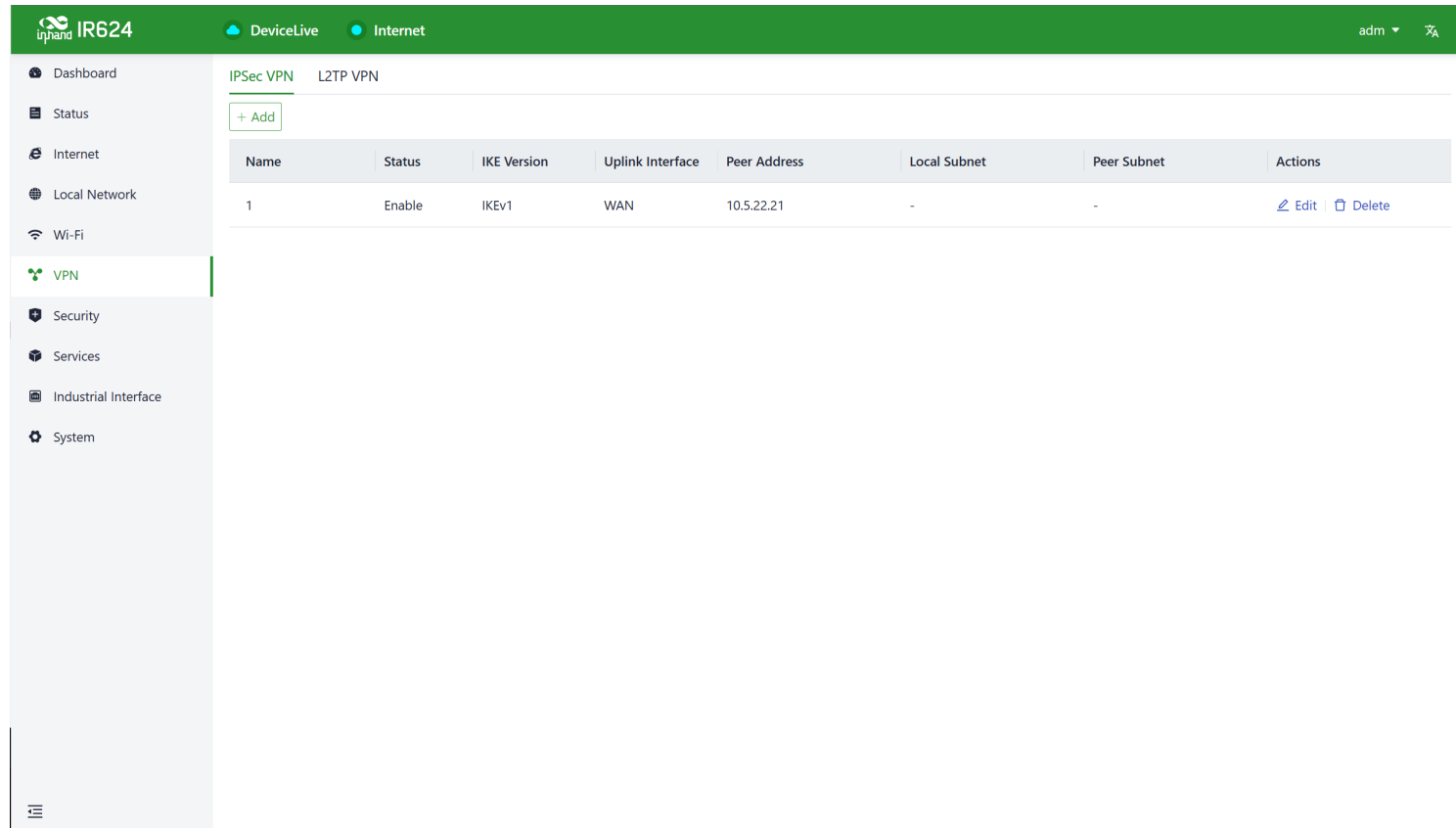
## 5.6 VPN

A Virtual Private Network (VPN) is an encryption technology used to establish a secure, private network connection over the public internet. It enables users to securely access private network resources over the internet from anywhere. VPNs achieve this by encrypting communication data, ensuring the confidentiality and security of the communication and preventing unauthorized access. This technology is highly valuable for connecting to corporate networks, maintaining online privacy, and accessing restricted content. VPNs have a wide range of applications, including in the corporate, personal, and mobile device sectors, making them a crucial tool for safeguarding privacy and data security.

### 5.6.1 IPSec VPN

IPsec (Internet Protocol Security) VPN is a protocol suite designed to enhance network communication security by encrypting and authenticating data transmission. It is widely used for establishing secure remote access, site-to-site connections, and Virtual Private Networks (VPNs). IPsec VPN ensures data protection and security through encryption and authentication methods.

Click the "Add" button under "VPN > IPsec VPN" to add a new IPsec VPN.



Once configurations are completed at both ends, the tunnel can be established. Users can check the tunnel establishment status in the "Status > VPN" menu.

- **Name:** This is the user-assigned name for the IPsec VPN to identify it for local management purposes.
- **IKE Version:** You can set the version of the Internet Key Exchange (IKE) protocol to be used. It supports both IKEv1 and IKEv2.
- **Pre-Shared Key:** This is a secret shared key that must be configured the same on both devices for authentication during IKE negotiation.
- **Internet Interface:** Choose the upstream interface used to establish the IPsec VPN locally.
- **Tunnel Mode:** This sets the encapsulation mode for IPsec on IP packets. It supports both tunnel mode and transport mode.
- **Peer Address:** This is the address of the remote endpoint with which IR624 establishes the IPsec tunnel.

#### Notes:

This setup allows the device with the public IP address to act as the server, and the client devices connect to it using the server's public IP address. If you have more specific questions or need further assistance with IPsec VPN configuration, please let me know.

- **Local Subnet:** Specify the subnet addresses that need to communicate through the IR624 IPsec VPN tunnel.
- **Remote Subnet:** Specify the subnet address on the other end of the tunnel that needs to communicate through the IPsec VPN tunnel.
- **IKE Policy:** Supports configuring the IKE protocol.
- **Encryption Method:** Sets the encryption algorithm used by IKE.
  - **Options:** DES, 3DES, AES128, AES192, AES256 (default: AES128)
- **Authentication Method:** Set the authentication algorithm used by IKE.
  - **Options:** MD5, SHA1, SHA2-256, SHA2-384, SHA2-512 (default: SHA1)
- **DH Group:** Configure the DH exchange parameters used during the IKE phase key negotiation.
  - **Options:** 1, 2, 5, 14, 15, 16, 19, 20
- **Timeout:** Set the IKE SA (Security Association) lifetime, defaulting to 86400 seconds.
- **IPsec Policy:** This allows you to configure IPsec parameters.
- **Security Protocol:** Sets the security protocol used by the ESP protocol.
  - **Options:** DES, 3DES, AES128, AES192, AES256 (default: AES128)
- **Encryption Method:** Sets the encryption algorithm used by the ESP protocol.
  - **Options:** MD5, SHA1, SHA2-256, SHA2-384, SHA2-512 (default: SHA1)
- **PFS Group:** In IPsec, during the negotiation of a security policy, an additional key exchange is performed in Phase 2 to enhance communication security.
  - **Options:** 1, 2, 5, 14, 15, 16, 19, 20
- **Timeout:** Sets the IPsec SA aging time, default is 86400 seconds.

## 5.6.2 L2TP VPN

The Layer 2 Tunneling Protocol (L2TP) is a Layer 2 VPN protocol designed to establish secure point-to-point or site-to-site Virtual Private Network (VPN) connections. It is commonly used for remote access and branch office

connectivity, creating secure communication channels for users or networks to protect the privacy and integrity of data transmission.

### 5.6.2.1 Work as Client

The IR624 can act as an L2TP client and establish a tunnel with a remote L2TP server. Click on the "L2TP VPN" menu, then navigate to "Client," and use the "Add" button to configure an L2TP client.

The screenshot shows the 'Add L2TP Client' configuration page in the IR624 web interface. The page has a green header with the 'inhand IR624' logo and status indicators for 'DeviceLive' and 'Internet'. A sidebar on the left lists various system settings, with 'VPN' highlighted. The main configuration area includes the following fields:

- Name:** A text input field.
- Status:** A toggle switch, currently turned on.
- NAT:** A checkbox, currently checked.
- Uplink Interface:** A dropdown menu with 'Any' selected.
- Server Address:** A text input field.
- User Name:** A text input field.
- Password:** A text input field with a copy icon.
- Authentication Mode:** A dropdown menu with 'AUTO' selected.
- Enable Tunnel Verification:** A checkbox, currently unchecked.

At the bottom of the form, there are two buttons: 'Save' (green) and 'Cancel' (white).

- **Name:** The name of the L2TP client for local identification.
- **Status:** The switch to enable or disable the L2TP client tunnel.
- **NAT:** The switch for NAT functionality when forwarding with the L2TP client.
- **Upstream Interface:** The upstream interface used for communication between the L2TP client and the server.
- **Server Address:** The communication address of the remote L2TP server.
- **Username/Password:** Usernames and passwords that need to be configured the same on both ends during L2TP negotiation.
- **Authentication Mode:** Setting the L2TP authentication mode.
- **Enable Tunnel Authentication:** When enabled, both ends need to configure the same username and password for tunnel authentication.

### 5.6.2.2 Work as Server

A typical L2TP server is usually deployed at the headquarters of an enterprise, serving as a remote access server for mobile office or branch offices. To configure the L2TP server settings, please click on "VPN > L2TP VPN > Server" to access the L2TP server editing page.

The screenshot shows the configuration page for L2TP VPN on an inhand IR624 device. The interface includes a sidebar with navigation options like Dashboard, Status, Internet, Local Network, Wi-Fi, VPN, Security, Services, Industrial Interface, and System. The main content area is titled 'IPSec VPN' and 'L2TP VPN'. It features a 'Server' tab and a 'Client' tab. The configuration fields are as follows:

- Name:** L2TP Server
- Status:** A toggle switch currently turned off.
- Uplink Interface:** A dropdown menu set to 'Any'.
- VPN Connection Address:** An empty text input field.
- IP Pool:** Two empty text input fields separated by a hyphen.
- User Name:** An empty text input field.
- Password:** An empty text input field with a password icon.
- Authentication Mode:** A dropdown menu set to 'AUTO'.
- Enable Tunnel Verification:** An unchecked checkbox.

At the bottom of the configuration area, there are two buttons: 'Save' (highlighted in green) and 'Reset'.

- **Name:** The name of the L2TP server, not editable.
- **Status:** The on/off switch for the L2TP server function, default is off.
- **Upstream Interface:** The upstream interface used by the L2TP server.
- **VPN Communication Address:** The gateway address for L2TP clients, which can be assigned to devices within the IP address pool.
- **Address Pool:** The IP address pool is used for communication when L2TP clients connect.
- **Username/Password:** Usernames and passwords that need to be the same on both ends for L2TP negotiation.
- **Authentication Mode:** Setting the L2TP authentication mode.
- **Enable Tunnel Verification Function:** When enabled, the usernames/passwords for tunnel verification on both ends need to be the same.

## 5.7 Security

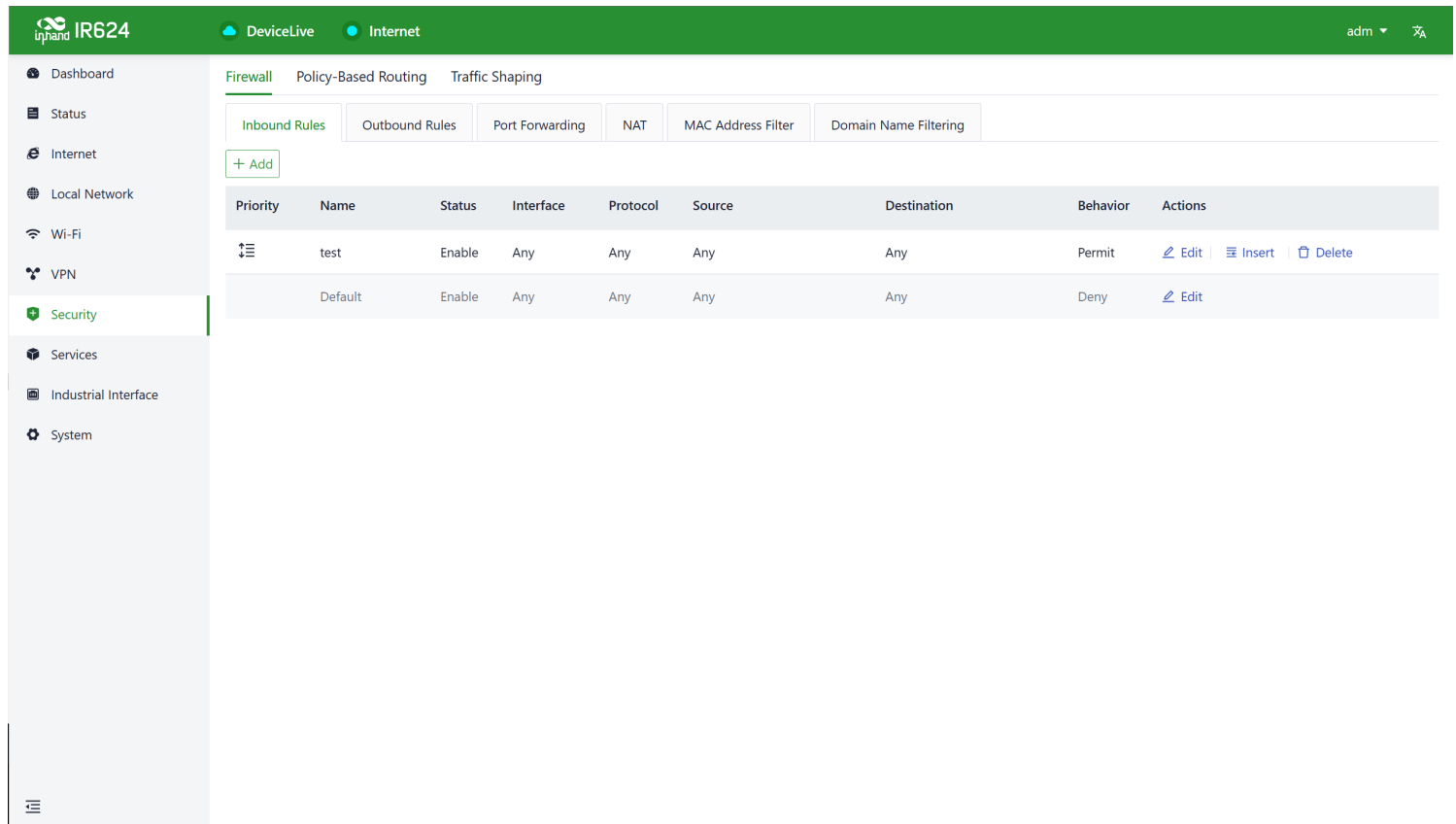
In the [ Security ] menu, users can configure advanced features related to firewalls, policy routing, and traffic shaping.

### 5.7.1 Firewall

The firewall currently includes functions such as inbound rules, outbound rules, port forwarding, MAC address filtering, and more.

#### 5.7.1.1 Inbound/Outbound Rules

You can implement traffic in/out control based on interfaces through the "Security > Firewall > Outbound Rules/Inbound Rules" feature. For example, if a user is subjected to a significant amount of attacks from a specific source IP address, they can use inbound firewall rules to restrict traffic from that IP address.



Furthermore, IT personnel can utilize outbound firewall rules to restrict certain users' access to external networks. Inbound and outbound rules share the same configurable content, with the only distinction being the default rules.

- **Name:** Set the name of the inbound/outbound rule for local identification.
- **Status:** Rule function switch.
- **Interface:** For outbound rules, it specifies the upstream interface where traffic leaves the router. For inbound rules, it specifies the upstream interface where traffic enters the router
- **Protocol:** Match traffic based on the protocol type, with options like Any, TCP, UDP, ICMP, or custom.
- **Source:** Match the source address for traffic, supporting custom, with the default as Any.
- **Destination:** Match the destination address for traffic, supporting custom, with the default as Any.
- **Action:** Action taken for matching traffic in inbound/outbound rules, supporting allow and deny.
- **Inbound Rules:** Traffic management rules for external network accessing the router, with the default as deny all.
- **Outbound Rules:** Traffic management rules for traffic going out through the router, with the default allowing all.
- Support for adjusting the priority of inbound and outbound rules.

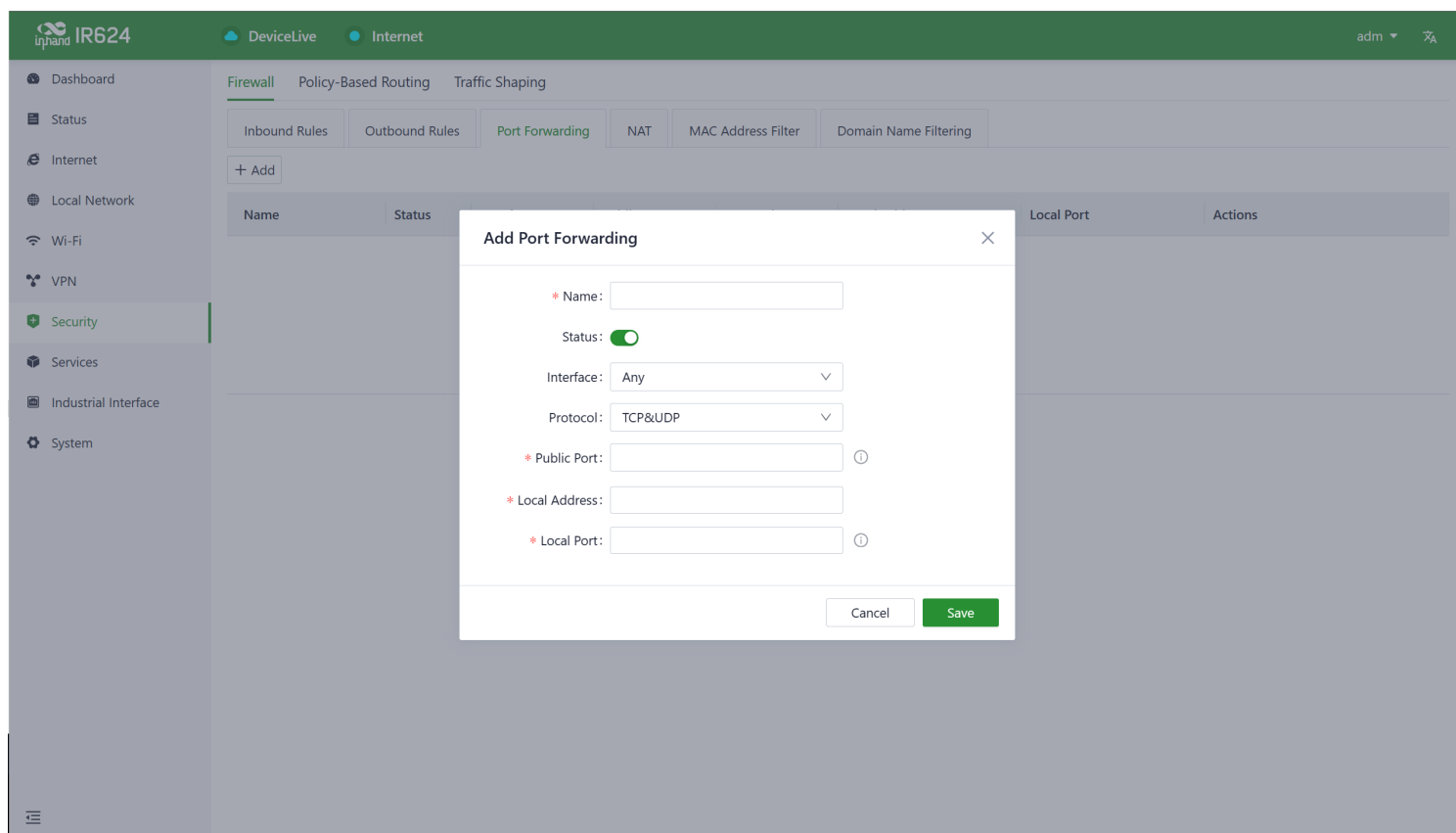
### 5.7.1.2 Port Forwarding

Port forwarding, also known as port mapping or port redirection, is used to redirect network packets from one network port (or address) to another network port or address. Users can configure port forwarding rules under "Security > Firewall > Port Forwarding." When external traffic accesses a specific port on the router, the device



forwards the data to the corresponding port of an internal client, enabling external access to services inside the router.

For example, when a user needs to access the service on port 1024 of the internal client at 192.168.2.10 from the external network, they can map this client's port to port 1024 under the WAN1 interface. External users only need to enter "<https://WAN address:1024>" in their browser to access the target device's data, where the "WAN address" is the IP address of the WAN interface.



- **Name:** The name of the port forwarding rule, used for local identification.
- **Status:** The on/off switch for the port forwarding rule.
- **Interface:** The upstream interface that provides mapping functionality for internal clients. The upstream interface needs public IP address support.
- **Protocol:** The protocol type of the traffic for port mapping, supports TCP, UDP, and TCP & UDP.
- **Public Port:** The port number on the upstream interface that provides mapping
- **Local Address:** The address of the target device located under the router that the external network needs to access.
- **Local Port:** The port of the target device that the external network needs to access. It needs to be consistent with the public port input range.

### 5.7.1.3 MAC Address Filter

MAC address filtering involves allowing or disallowing devices in a MAC address list to access the internet, which means controlling LAN devices' internet access requests through MAC address filtering on the router. Users can configure MAC address filtering rules in "Security > Firewall > MAC Address Filtering."

You can create multiple MAC addresses in the list, add address descriptions, and set it to allow only the MAC addresses to access the network (whitelist), or you can block MAC addresses in the list from accessing the

## network (blacklist).

The screenshot shows the inhand IR624 web interface. The top navigation bar includes 'DeviceLive' and 'Internet'. The left sidebar lists various system components, with 'Security' highlighted. The main content area is titled 'Firewall' and contains sub-tabs for 'Inbound Rules', 'Outbound Rules', 'Port Forwarding', 'NAT', 'MAC Address Filter', and 'Domain Name Filtering'. The 'MAC Address Filter' tab is selected, displaying a 'MAC Address Filter Table' with radio buttons for 'Unlimited', 'Blacklist', and 'Whitelist'. The 'Blacklist' option is selected. There are 'Save' and 'Reset' buttons. Below the options is a '+ Add' button and a table with columns for 'MAC Address', 'Status', 'Description', and 'Actions'. The table is currently empty, showing 'No data'.

### 5.7.1.4 NAT

NAT (Network Address Translator) is a technology used to use a private address in a local network and switch to a global IP address when connecting to the Internet. You can set source or destination address translation as needed in "Security > Firewall > NAT".

The screenshot shows the inhand IR624 web interface with the 'Add NAT Rule' dialog box open. The dialog box is titled 'Add NAT Rule' and has a close button (X). It contains the following fields and options:

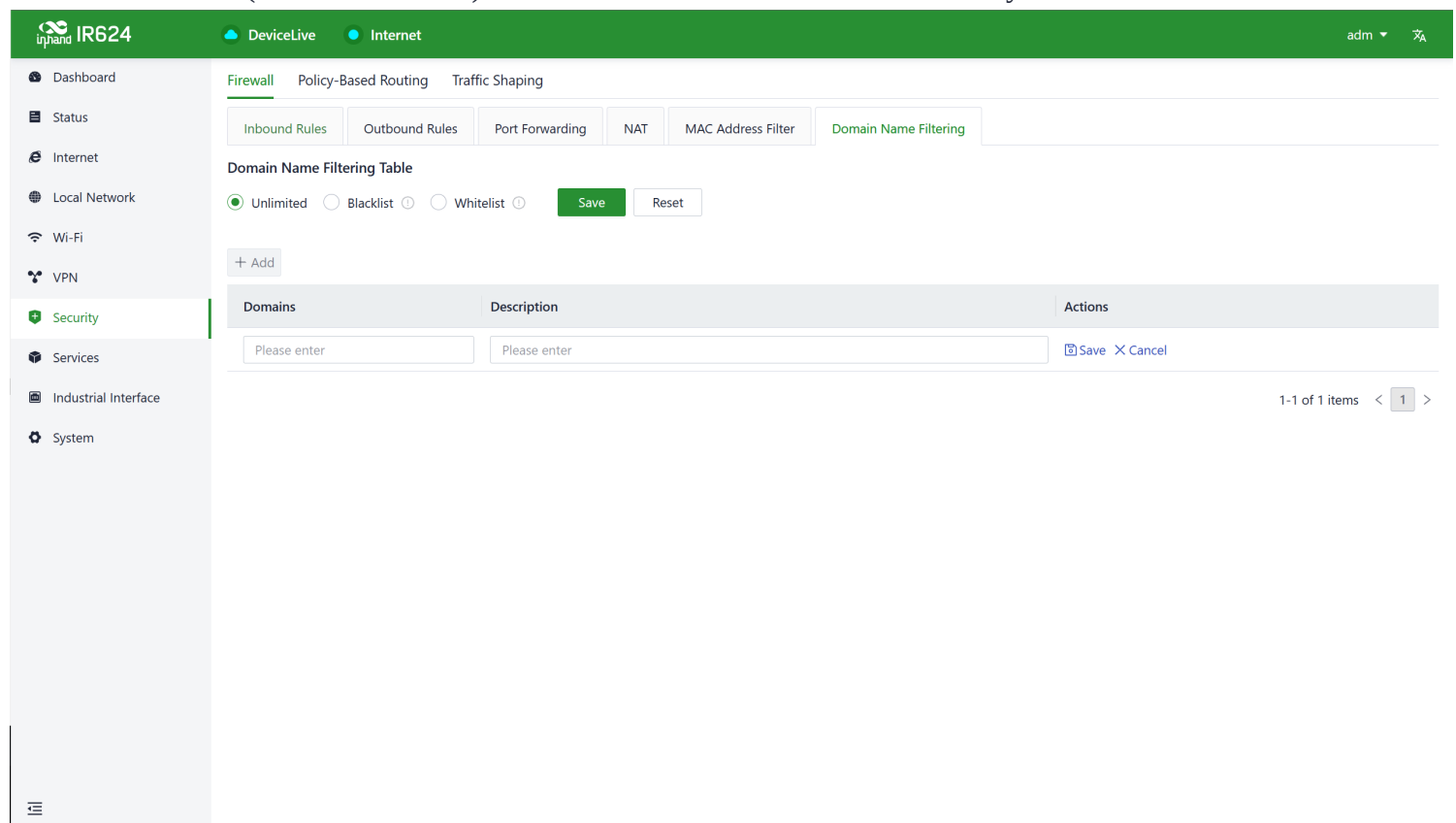
- \* Name: [Text input field]
- Status:
- Type: SNAT (dropdown menu)
- Protocol: Any (dropdown menu)
- Source: Any (dropdown menu)
- Destination: Custom (dropdown menu) [Text input field]
- \* Converted Address: [Text input field]

At the bottom of the dialog box, there are 'Cancel' and 'Save' buttons.

- **Name:**The user sets a name for the rule.
- **Type:** The type of this rule.
  - **SNAT:** Translate the source IP address.
  - **DNAT:** Translate the destination IP address
- **Protocol:** The scope of the rule.
  - **Any:** This rule is effective for all agreements.
  - **TCP:** This rule takes effect only for TCP protocol.
  - **UDP:** This rule takes effect only for UDP protocol.
  - **TCP&UDP:** This rule takes effect only for TCP and UDP protocols.
- **Source:** The source IP address that needs to be translated.
- **Destination:** The destination IP address that needs to be translated.
- **Converted Address:** Translated address.

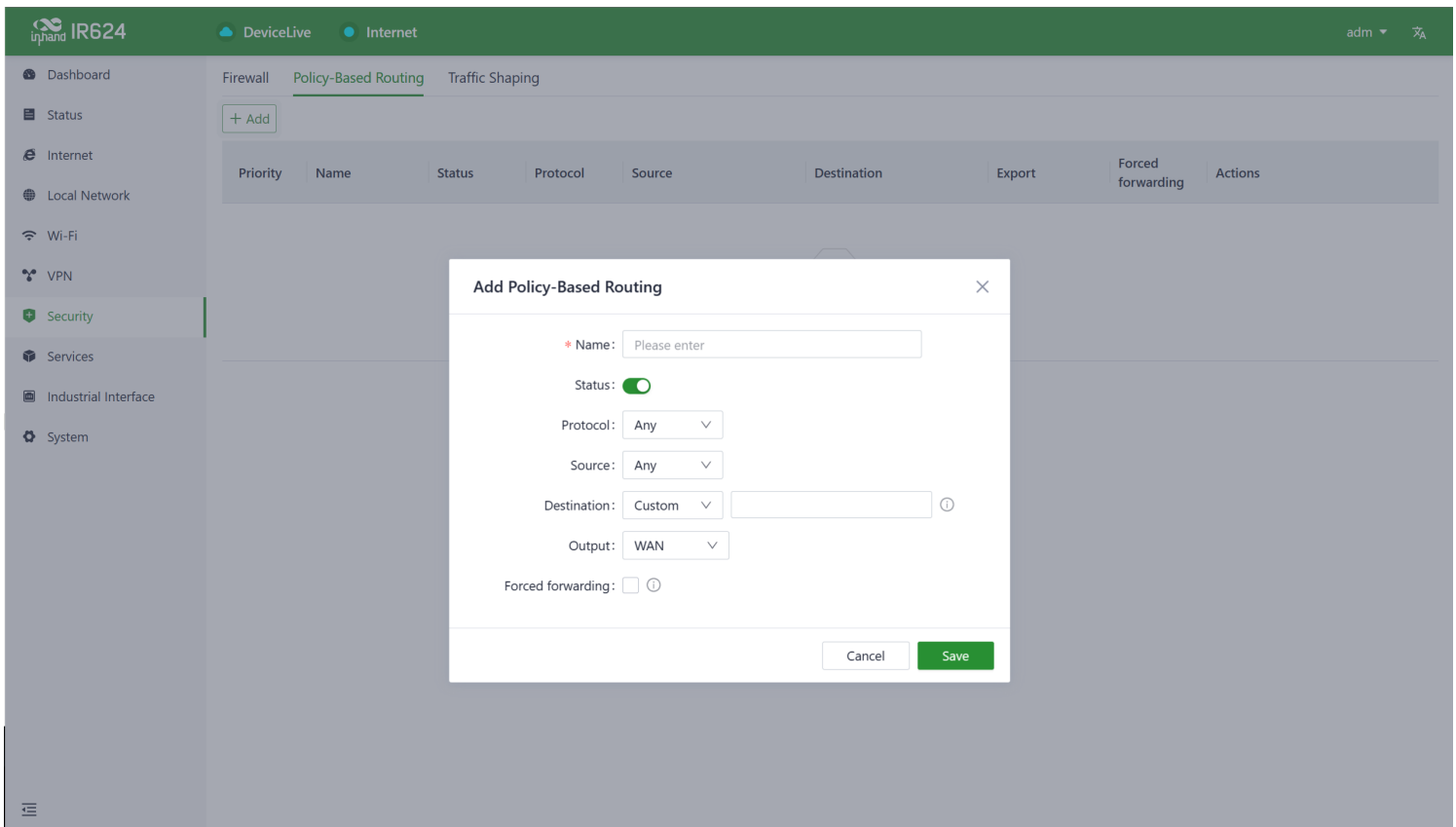
### 5.7.1.5 Domain Name Filtering

Allow or disallow (White/Black List) the domain names that can be accessed by clients as needed.



### 5.7.2 Policy-Based Routing

Policy routing is a feature that allows users to create policies based on their specific needs, enabling them to route different data flows through different links. This improves the flexibility and control of routing decisions, enhances link utilization efficiency, and reduces enterprise costs. Click the "Add" button under "Security > Policy Routing" to create a new policy routing rule.



## Cautions:

- The source address and destination address in a policy routing rule cannot both be set as "Any."

## 5.7.3 Traffic Shaping

Create a traffic shaping policy to optimize your network based on each protocol, giving users control and prioritizing critical business traffic. This feature can also reduce the bandwidth allocated to entertainment traffic. You can configure traffic shaping rules in "Security > Traffic Shaping > Add/Edit."

Traffic shaping policies consist of a series of rules executed sequentially, similar to custom firewall rules. Each rule comprises two main components: the type of traffic to restrict or adjust and how to limit or adjust that traffic.

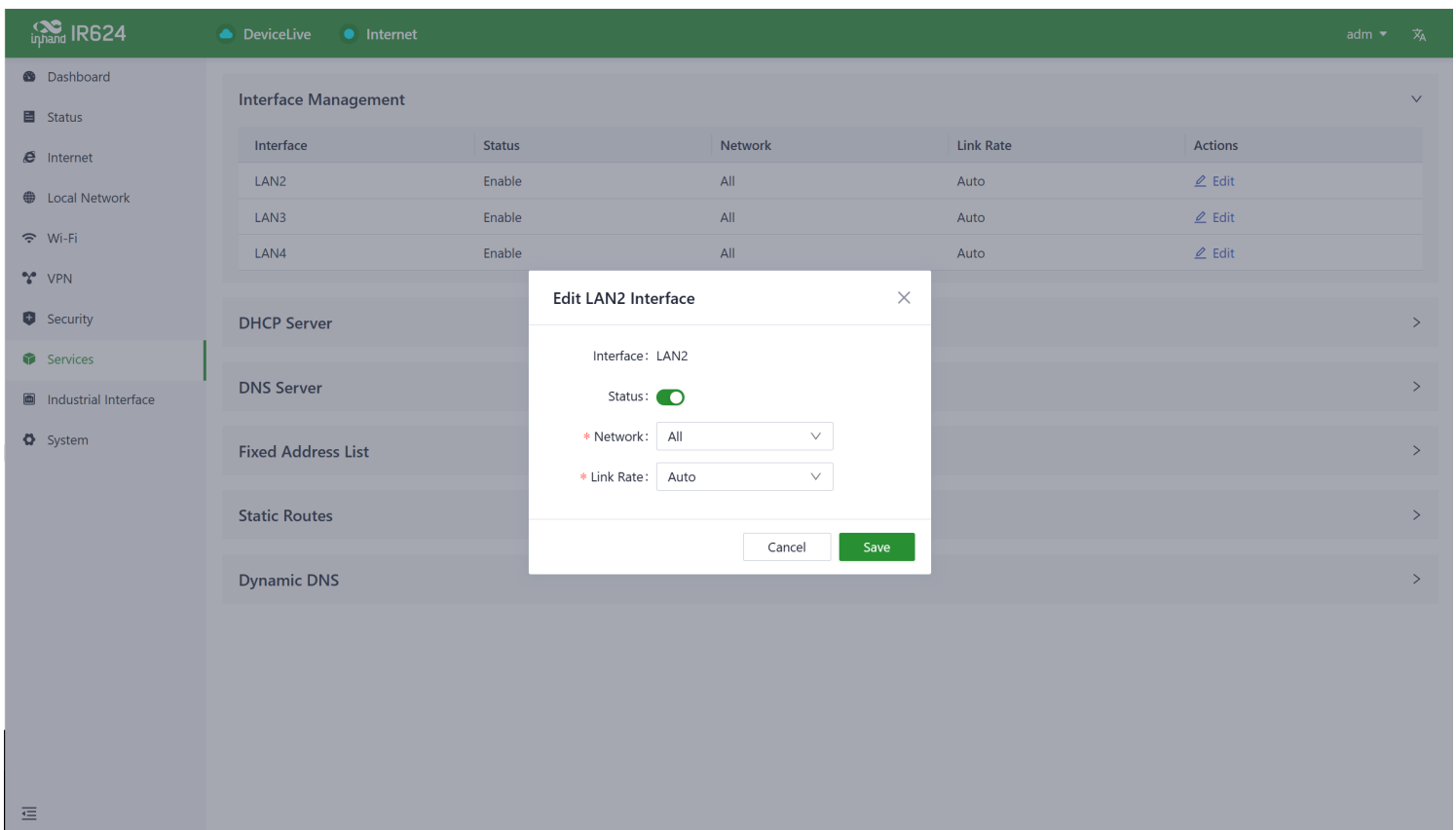
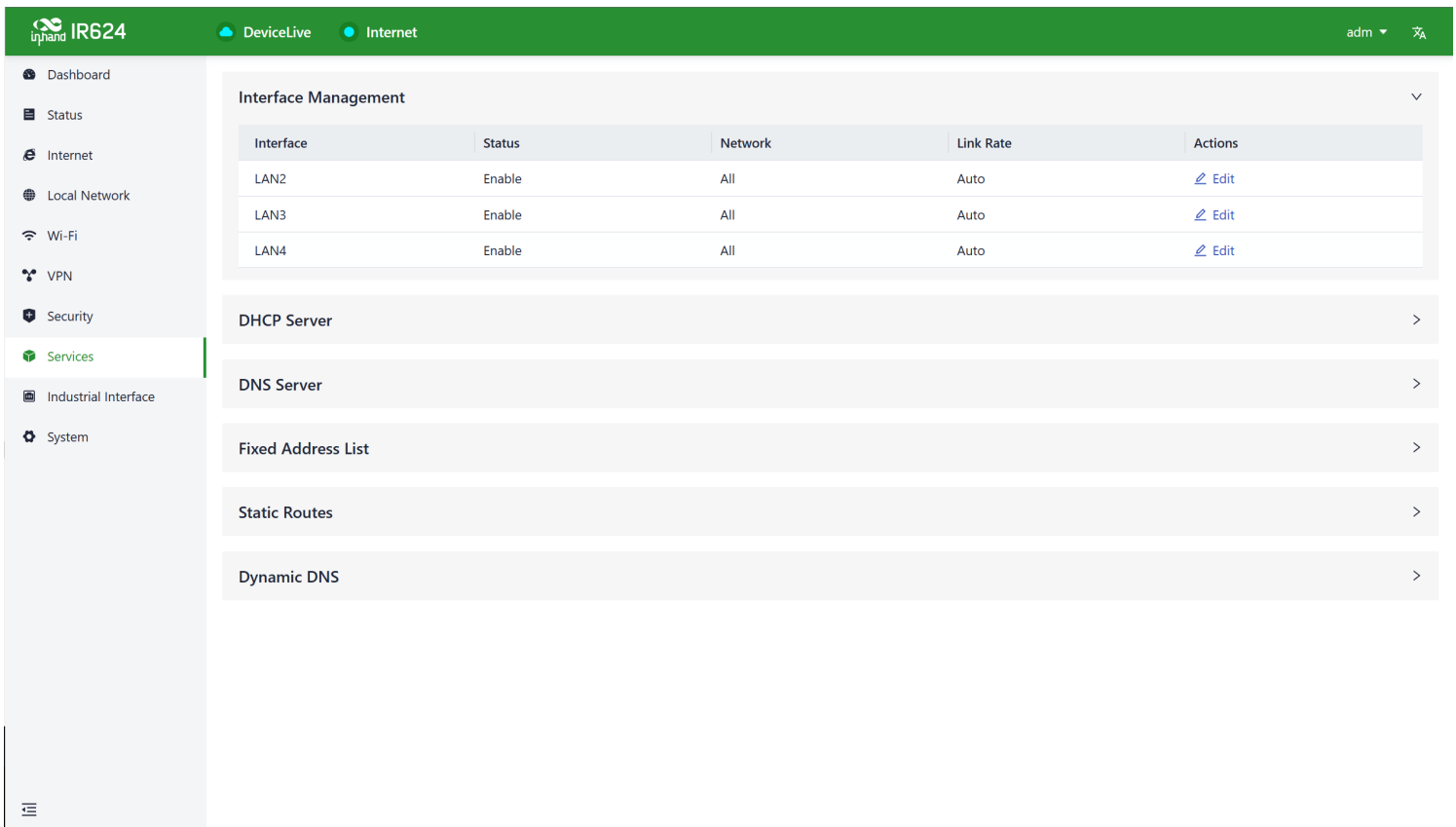
#### Notes:

- Traffic forwarding priority for unmatched rules is medium.
- When Limit Bandwidth is set to 0, the system will not limit the bandwidth.
- The value of Reserved Bandwidth should not be greater than the Limit Bandwidth.

## 5.8 Service

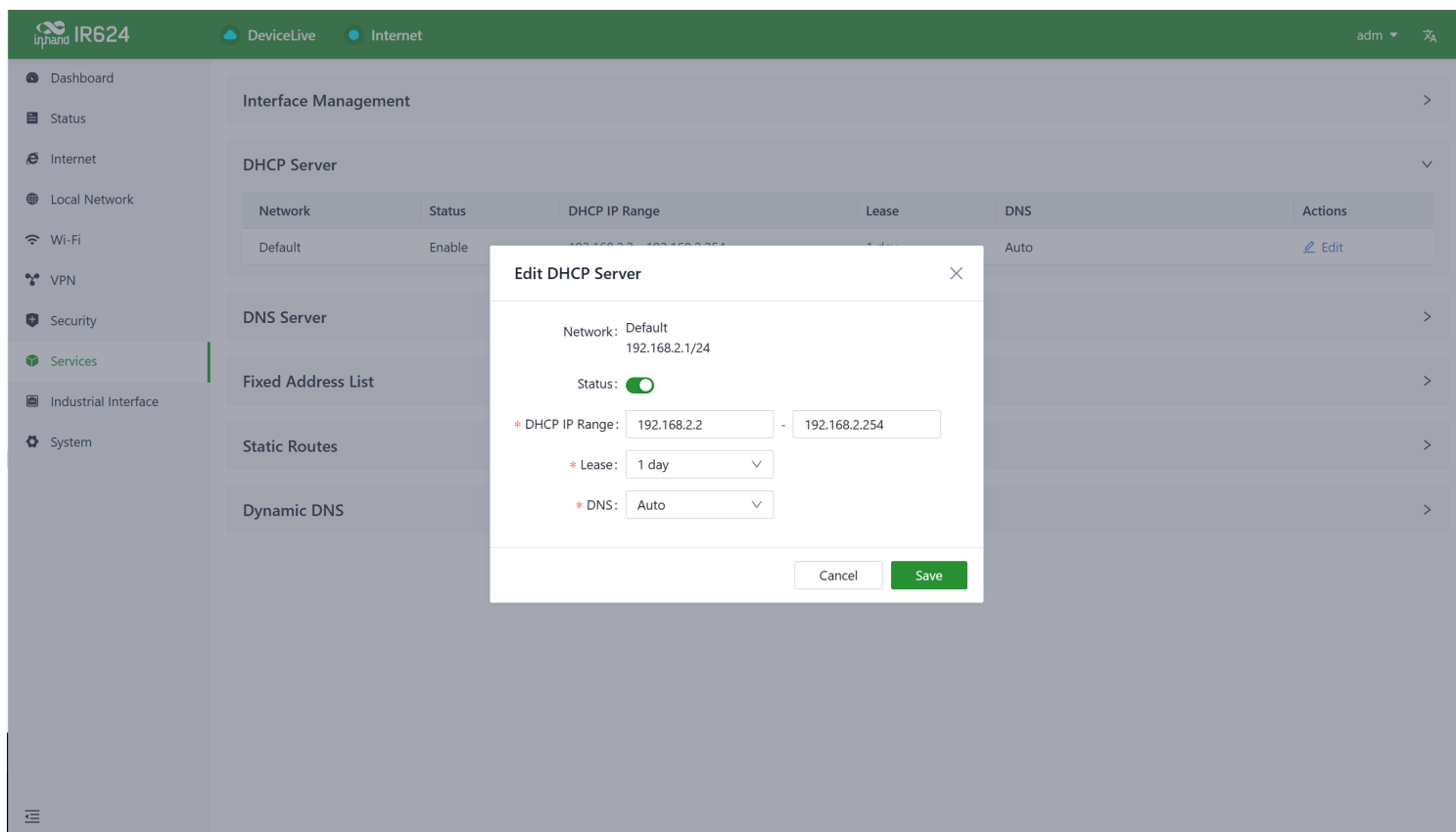
### 5.8.1 Interface Management

You can configure local networks allowed through a specific interface and set the interface's speed in the "Services > Interface Management" function.



## 5.8.2 DHCP Server

The DHCP (Dynamic Host Configuration Protocol) service operates in a client/server communication mode, where clients request IP addresses from servers, and servers respond to these requests by assigning IP addresses dynamically to clients. You can configure the DHCP server's IP address pool using the "Services > DHCP Server" feature.



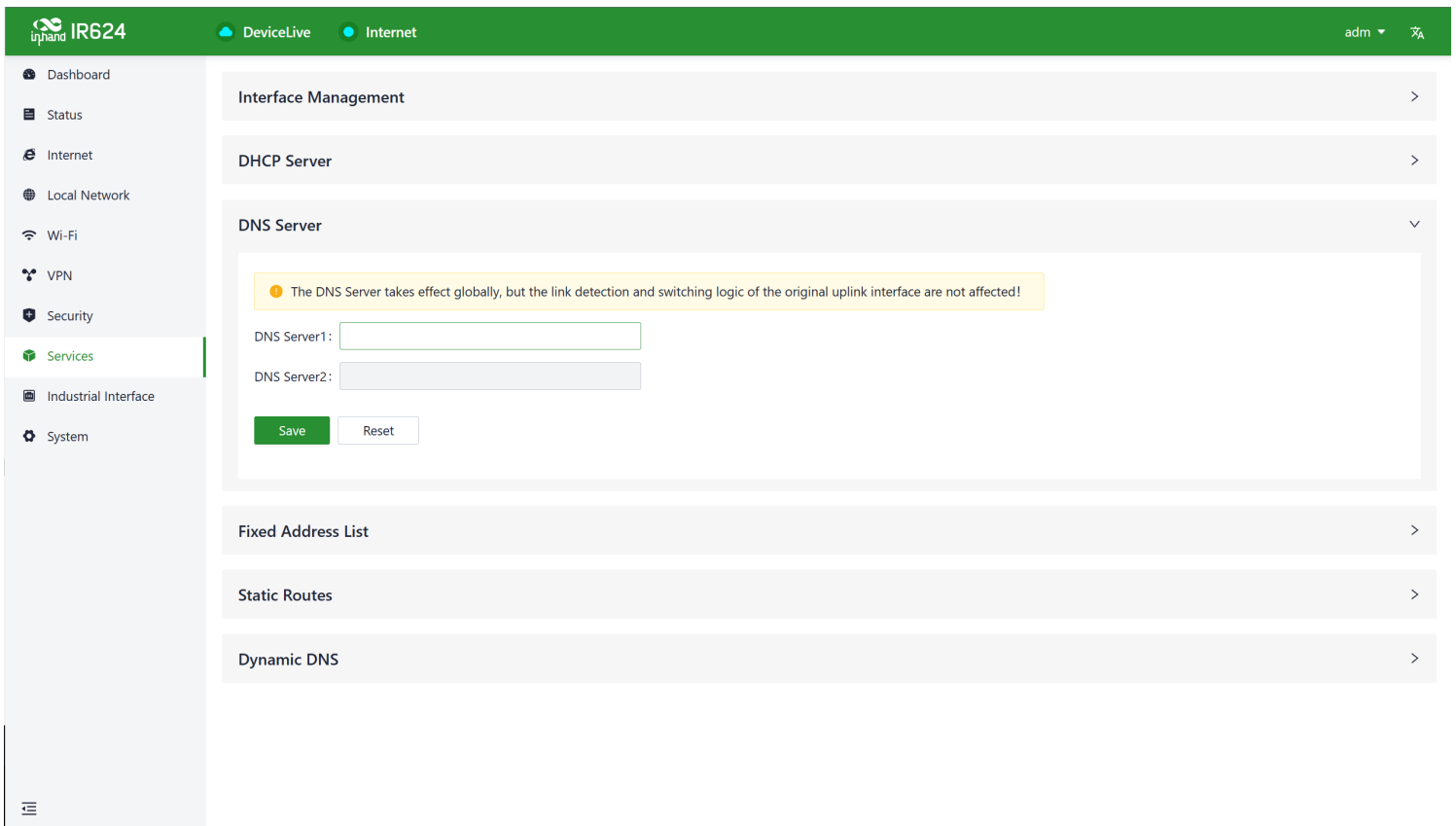
## Notes:

- The device's DHCP service is generated based on the network information in the local network. If you remove a local subnet from the "Local Network List," the DHCP Server for that local subnet will also be deleted.
- Local network entries need to be set in "IP" mode for the DHCP server function to take effect. Networks in "VLAN Only" mode are not within the selectable range.

## 5.8.3 DNS Server

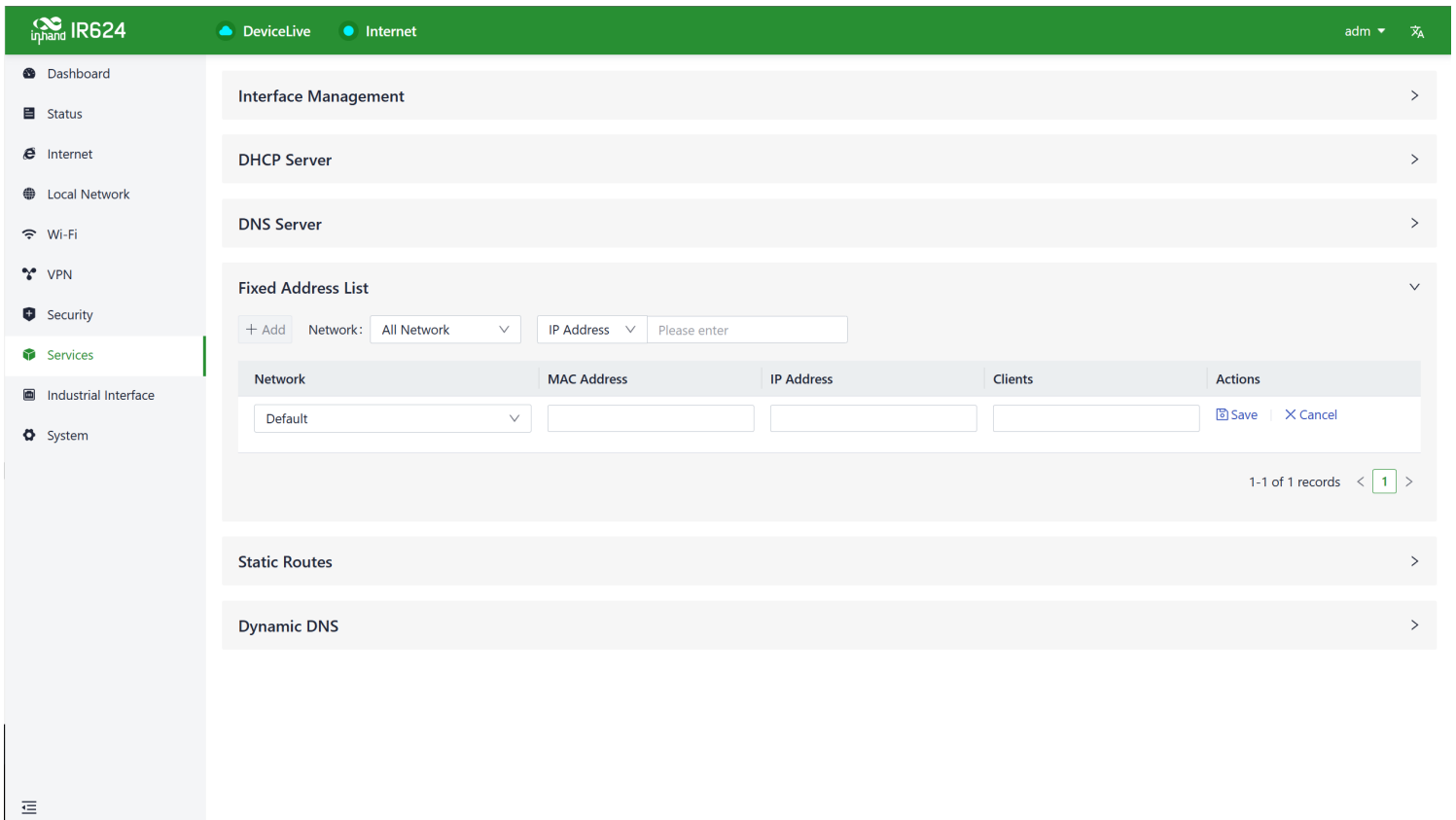
DNS (Domain Name System) servers are a crucial network component responsible for translating human-readable domain names (e.g., [www.example.com](http://www.example.com)) into computer-understandable IP addresses (e.g., 192.168.1.1). DNS servers act as the address book of the internet, helping computers and devices find the locations of other devices and ensuring that information can be correctly delivered across the network.

When users don't set DNS server addresses in "Services > DNS Server," the DNS addresses obtained from the device's upstream interface will be used for domain name resolution. When users configure DNS server addresses, the configured DNS addresses will be used for domain name resolution.



## 5.8.4 Fixed Address List

You can use the "Services > Fixed Address List" function to allocate a fixed IP address to a device based on its MAC address. This means that the device will consistently receive the same IP address every time it connects to the IR624.



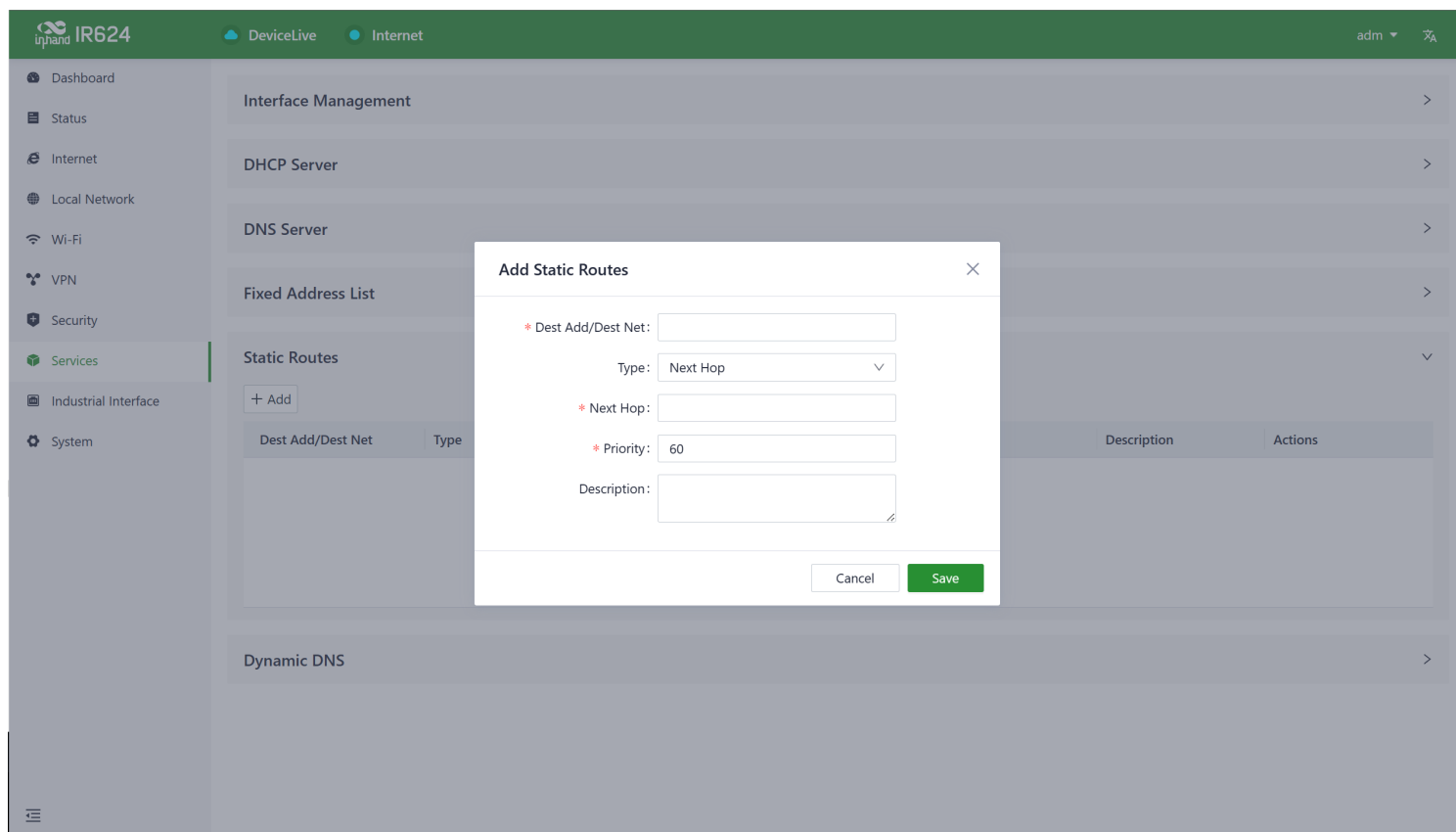


## Cautions:

- The available addresses for allocation must fall within the address range of the local network in IP mode, or else the configuration will not take effect
- When the local network is deleted, all fixed address allocation rules within the local network's address range will be removed.

## 5.8.5 Static Routes

You can configure static routing entries using the "Services > Static Routing" feature to enable data to be forwarded through specified paths and interfaces. The contents of the static routing table are manually created by users, and routing entries generated by other services, such as VPN functionality, will not be displayed in this table.



## Cautions:

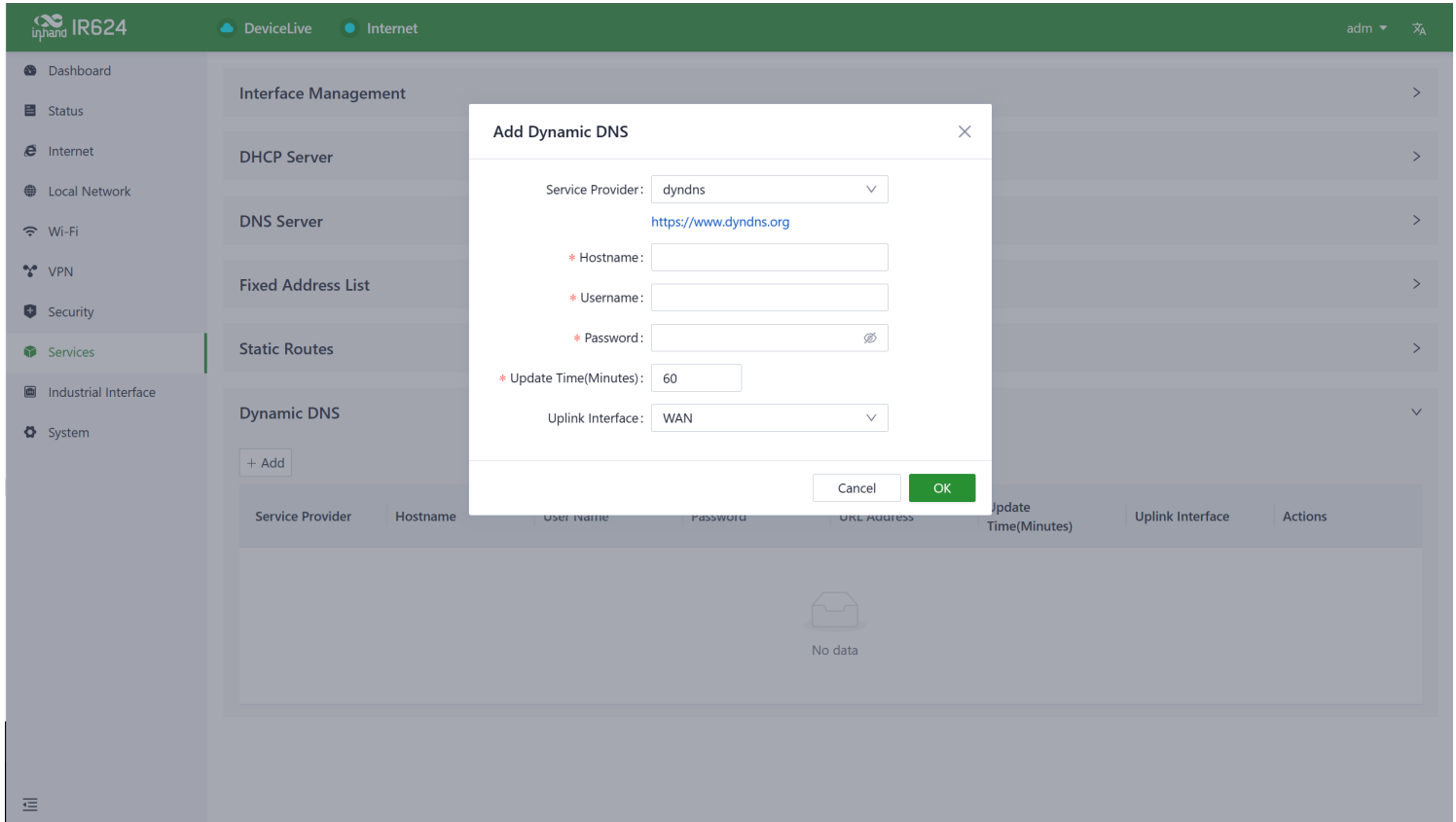
- For static routes with the same destination address/network, the next-hop address, interface, or priority cannot be the same; otherwise, it will result in a non-functional route.
- When Wi-Fi (STA), or L2TP Client VPN is deleted, the corresponding static routes using those interfaces will also be removed.

## 5.8.6 Dynamic DNS

Dynamic DNS (Dynamic Domain Name System) is used to automatically update the name server content in the domain system. According to internet domain rules, domain names are typically associated with fixed IP

addresses. Dynamic DNS technology allows users with dynamic IP addresses to have a fixed name server. This enables external users to connect to the URL of users with dynamic IP addresses through regular updates.

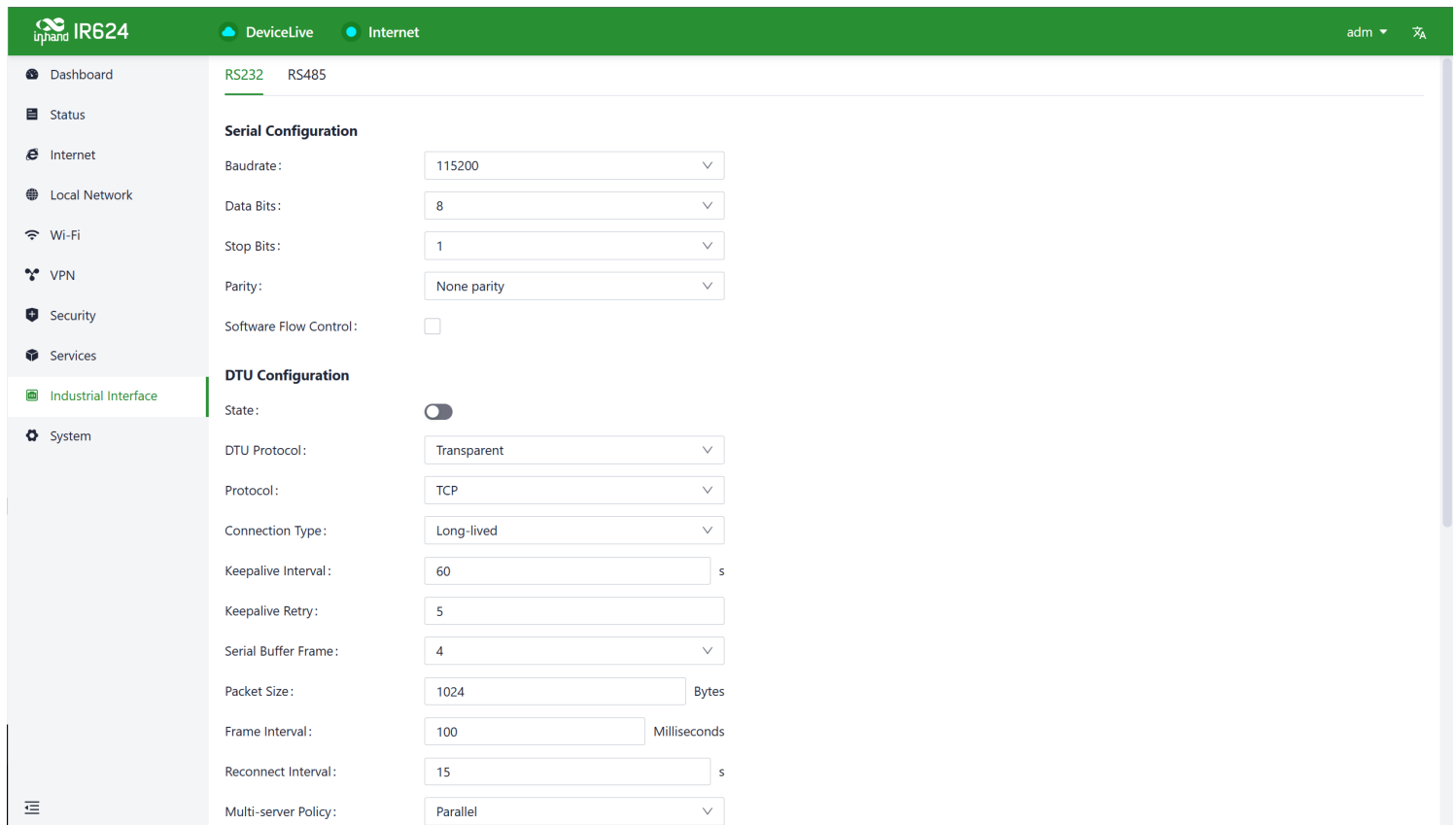
You can manually configure the Dynamic DNS server address under the "Services > Dynamic DNS" feature.



- **Service Provider:** Provided by the Dynamic DNS service operator, you can choose from dyndns, 3322, oray, no-ip, or use a custom option (requires a URL).
- **Hostname:** Register for a hostname by clicking on the URL below the service provider.
- **Username:** Register for a username by clicking on the URL below the service provider.
- **Password:** The password set by the user during registration.

## 5.9 Industrial Interface

IR624 supports RS232 and RS485 industrial serial port protocols, which can be used for PLCs, industrial equipment, etc. to access IR624 and send data back.



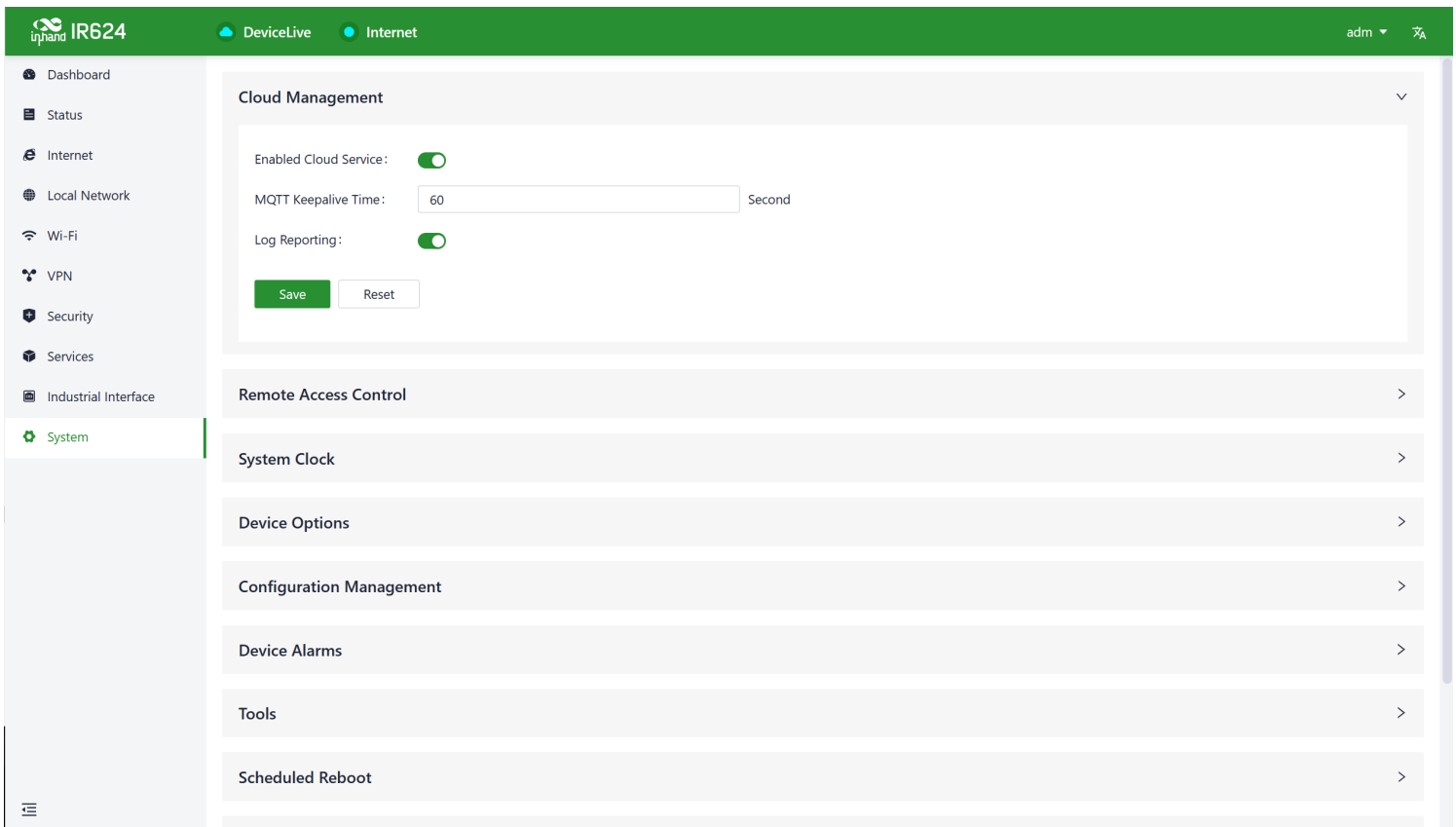
## 5.10 System

In the "System" menu, users can configure settings related to cloud management, remote access control, clock settings, device options, configuration management, device alerts, tools, and log servers, among other functions.

### 5.10.1 Cloud Management

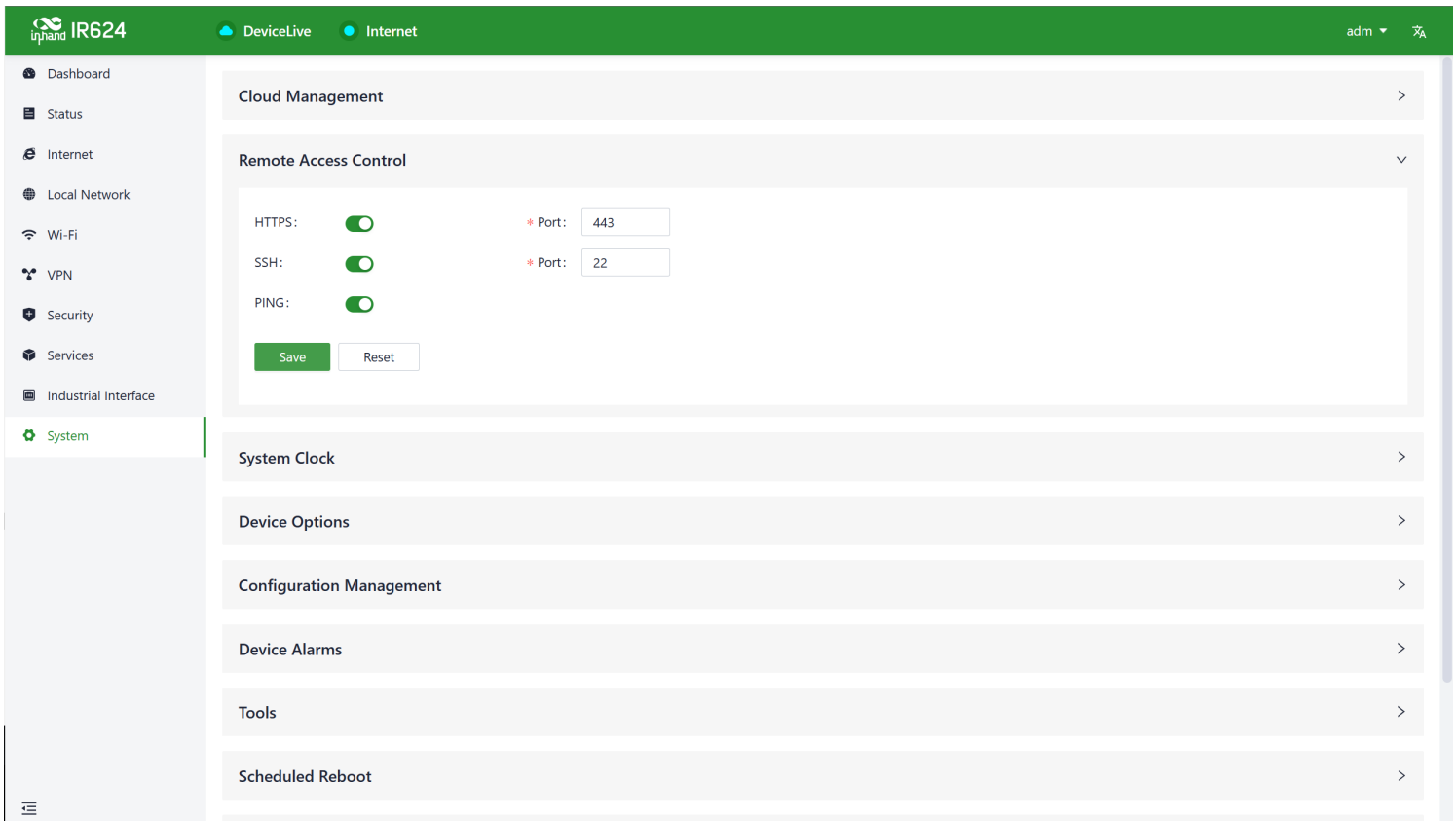
The Device Live ([device.inhandcloud.com](https://device.inhandcloud.com)) is a cloud platform developed by InHand Networks to address the challenges faced by Industrial networks, such as slow deployment, complex operations, and poor user experiences. This platform is designed with a focus on user needs and integrates features like zero-touch deployment, intelligent operations and maintenance, security protection, and excellent user experience capabilities. Once devices are connected to the cloud platform, users can perform remote management, batch configuration, traffic monitoring, and other operations through the platform, making network device management more convenient and efficient.

IR624 automatically connects to the Device Live after establishing an internet connection by default. If you do not wish to use the cloud management function, you can disable it manually in the "System > Cloud Management" function.



## 5.10.2 Remote Access Control

You can configure whether to allow external access to the router's web configuration interface from the Internet through the "System > Remote Access Control" function. You can also set the service port for this purpose.

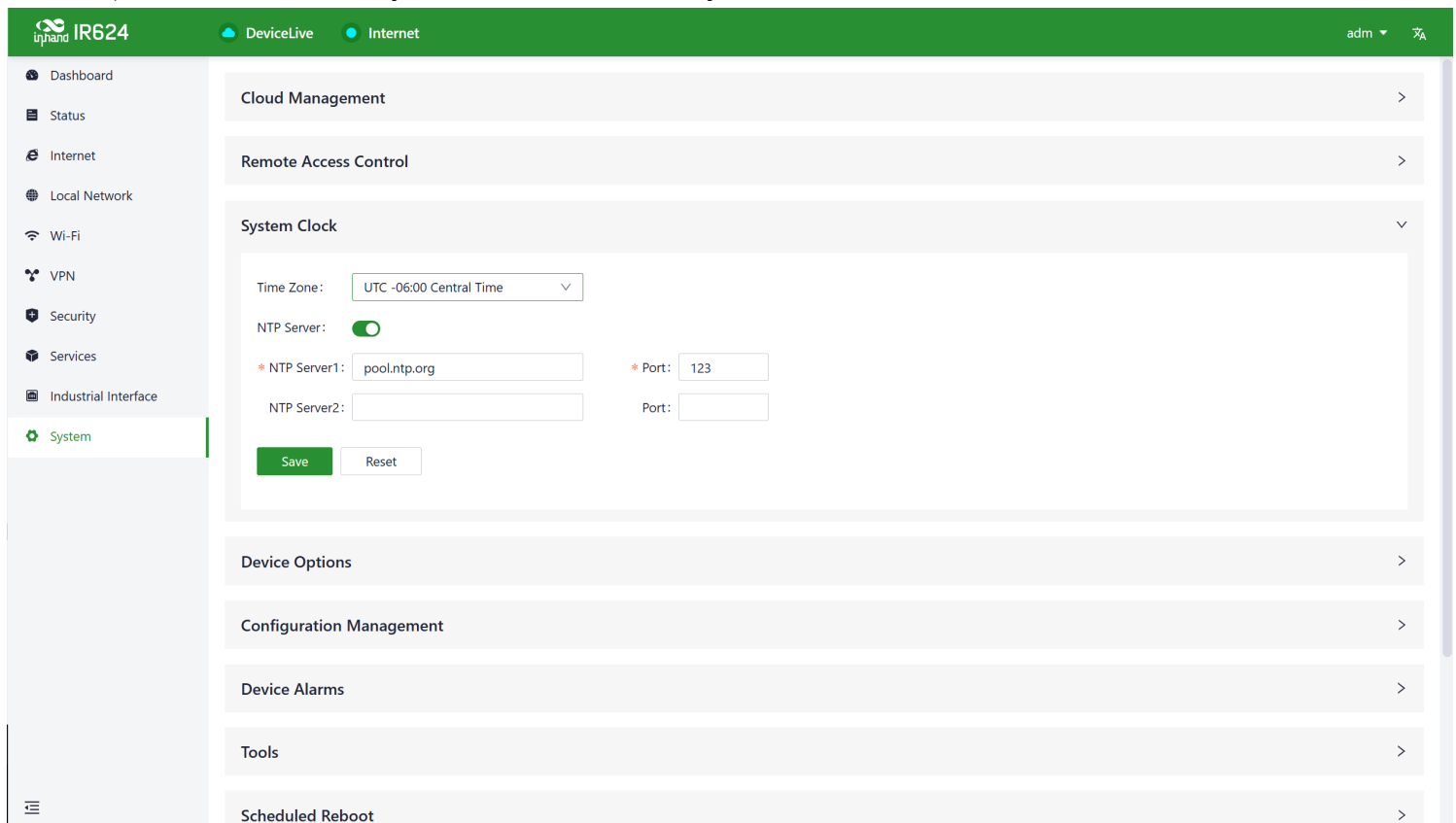


- **HTTPS:** When enabled, users can access the router's web interface remotely by entering the public IP address and port number of the upstream interface in a web browser.
- **SSH:** When enabled, users can remotely log in to the router's backend using remote tools (such as CRT) by providing the public IP address, port number, username, and password.
- **Ping:** When enabled, the upstream interface allows external networks to initiate Ping requests.

### 5.10.3 System Clock

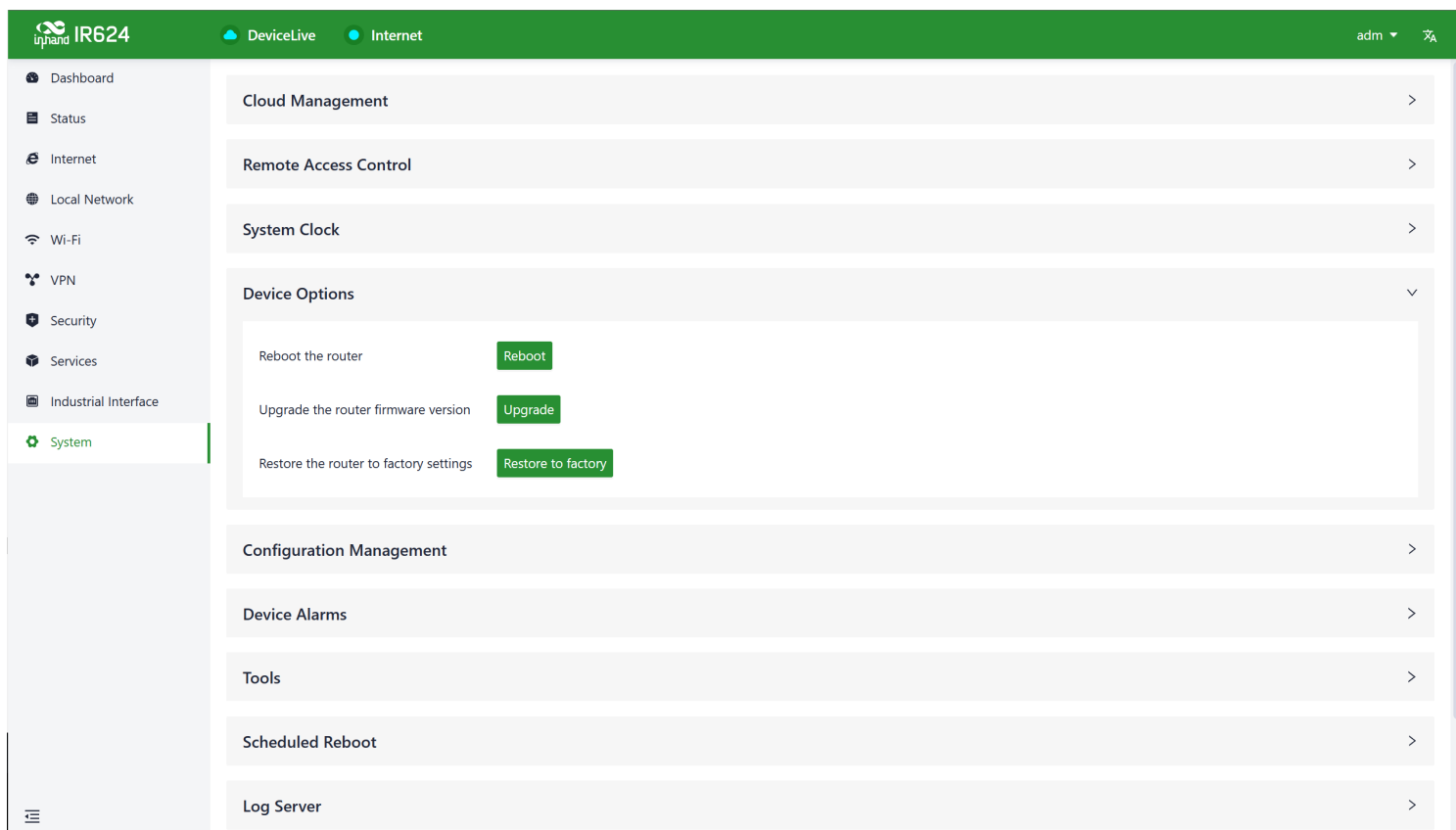
In network functionality, the clock function refers to the capability used to coordinate and synchronize the time between network devices. Clock functionality within a network is crucial for data transmission, log recording, security, coordination, and troubleshooting. It ensures that various devices in the network are operating with synchronized times, which is essential for efficient and secure network operations.

You can use the "System > Clock" function to select their current time zone and configure NTP (Network Time Protocol) server addresses to synchronize the device's system time with an NTP server.



### 5.10.4 Device Option

In the "System > Device Options" section, users can perform various device operations such as rebooting, upgrading firmware, and restoring factory settings.



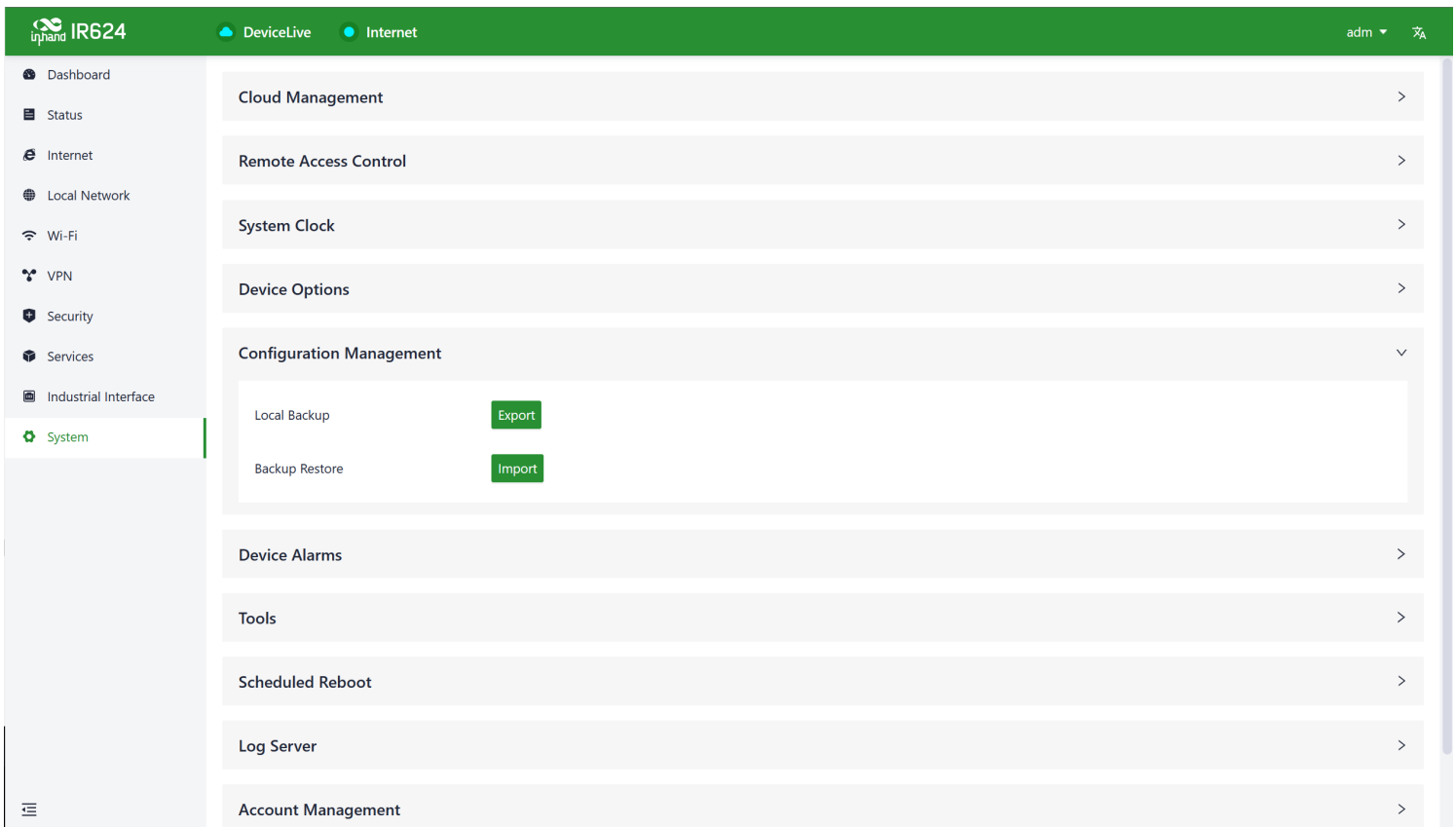
## Cautions:

- When performing a local firmware upgrade, it is essential to ensure that the firmware is obtained from a legitimate source to avoid rendering the device inoperable due to incorrect firmware imports.
- When a device is connected to the cloud platform, the platform will synchronize the previous configuration to the device again due to cloud-based configuration synchronization. The device will only clear historical data during the factory reset.

## 5.10.5 Configuration Management

Configuring backups and backup recovery are critical tasks in network management and maintenance. They involve saving the configuration information of network devices so that it can be quickly restored or transferred when needed.

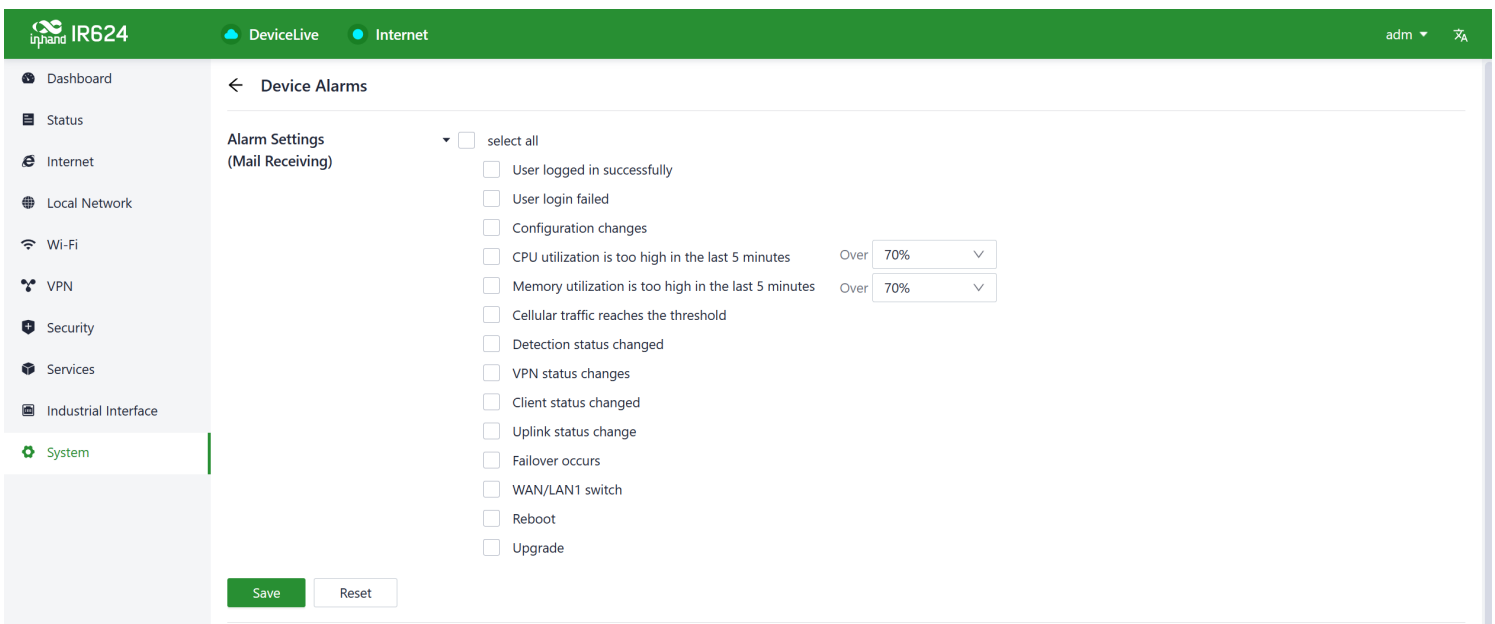
Users can export device configurations to local storage in the "System > Configuration Management" menu. This backup can be imported into the device in case of configuration loss or when you need to overwrite the existing configuration.



## 5.10.6 Device Alarms

You can choose to focus on specific events that may occur on the device by selecting the corresponding alarm events and configuring the email address for receiving alerts. When an alarm event occurs, the device will automatically send an email notification. It's important to note that even if a user doesn't select certain alarm options, related alarm events will still be recorded in the device's local logs.

You can configure alarm event types and email addresses for alarm notifications in the "System > Device Alarms" menu.



After configuring the outgoing email server address, port, username, and password, the device will use this email account to send alarm notifications. You can use the "Send Test Email" option to verify whether the outgoing

email configuration is correct. This test email will help you ensure that the device can successfully send alarm notifications to the specified email address.

Receive Mail Settings

Enable:

\* Mail Server Address:

\* Mail Server Port:

\* Username:

\* Password:

TLS:

\* Receiving Email Address:

+ Add

Send a test email to:

## 5.10.7 Tools

### 5.10.7.1 Ping

You can use ICMP (Internet Control Message Protocol) to check the device's external network connectivity. In the "Target" field, enter any domain name or IP address you want to test the device's connectivity to, and then click "Start" to check the connectivity status between the device and the specified target. This can help you determine whether the device can reach the target over the internet.

You can perform a network ping test on a target by going to "System > Tools > Ping." This allows to send ICMP echo requests to the specified target IP address or domain name and receive ICMP echo replies to check network connectivity and latency to that target.

inhand IR624 DeviceLive Internet adm 文

Tools

Ping

\* Target:

Interface:

Source:

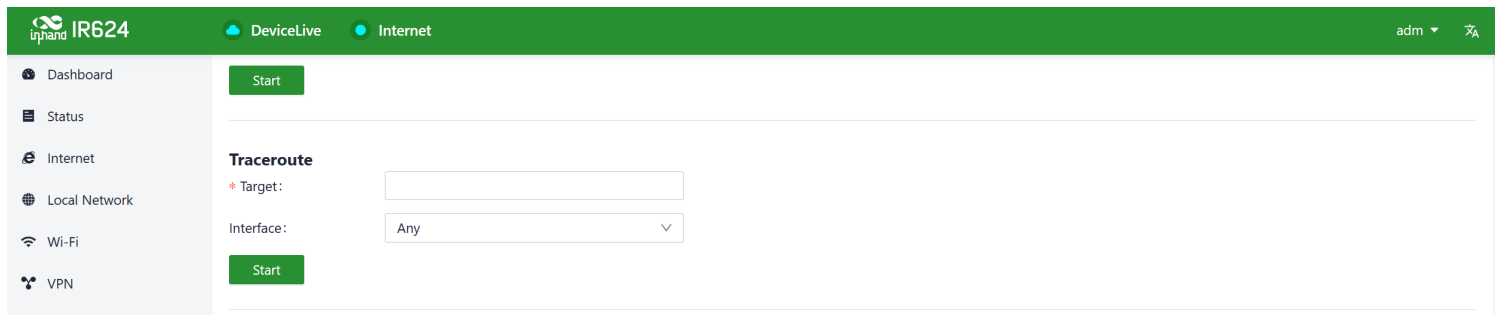
\* Packet Size:  Bytes

\* Packet numbers:

### 5.10.7.2 Traceroute

Traceroute is a network diagnostic tool used to determine the network path that data packets take from the source to the destination, as well as the intermediate routers or hops along that path. You can enter the target host's IP address in "System > Tools > Traceroute," choose the outgoing interface for the traffic, click "Start," and check the device's connectivity to the target IP by tracing the route.

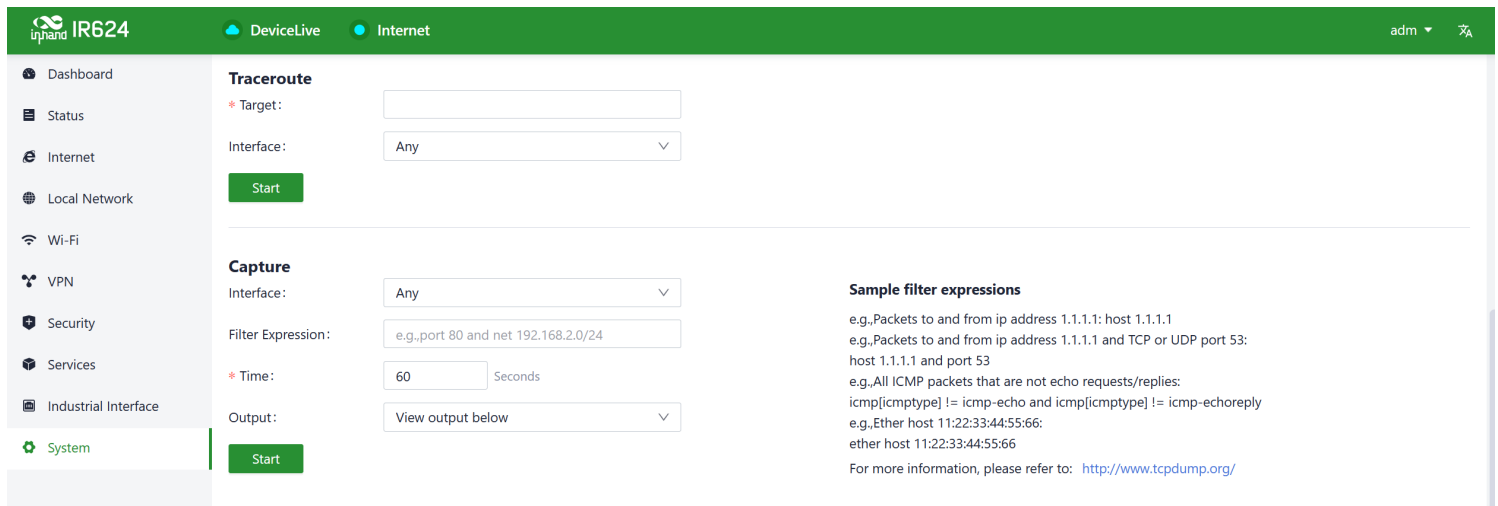




### 5.10.7.3 Capture

Packet capturing is a network monitoring and analysis technique used to capture and record data packets transmitted over a computer network. Packet capture tools are typically used for network troubleshooting, network performance analysis, security auditing, and protocol analysis, among other purposes.

Users can capture packets passing through a specific interface in "System > Tools > Packet Capture." By selecting the "Output" option, users can choose to display the captured data within the interface or export it locally for further analysis.



### 5.10.8 Scheduled Reboot

Scheduled reboot is a network device management strategy that allows administrators to automatically restart a device at a specific time or under certain conditions to ensure the device's normal operation and performance.

In practice, users can set up scheduled reboots in the "System > Scheduled Reboot" function based on their business requirements. The device supports scheduled reboots at fixed times daily, weekly, or monthly.

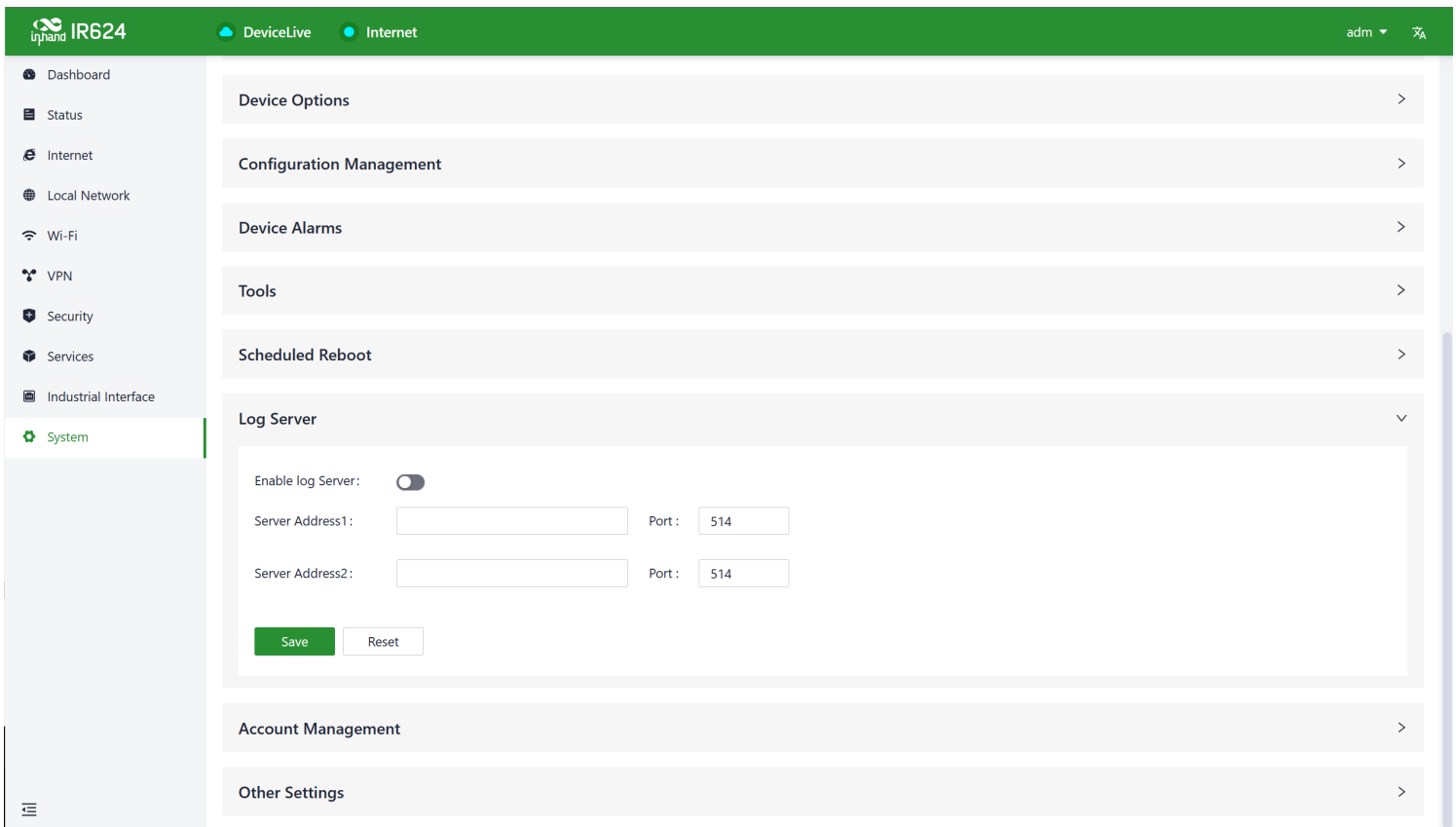
In the case of monthly reboots, if the selected reboot day exceeds the actual number of days in the month, the device will reboot on the last day of the month. For example, if you choose to reboot on the 31st of every month, it will reboot on the 30th in a month with only 30 days.

The screenshot displays the Inhand IR624 web management interface. The top navigation bar includes the Inhand logo, the model number IR624, and status indicators for DeviceLive and Internet. A user profile 'adm' is visible in the top right. The left sidebar contains a menu with options: Dashboard, Status, Internet, Local Network, Wi-Fi, VPN, Security, Services, Industrial Interface, and System (highlighted). The main content area shows a list of system management options: Remote Access Control, System Clock, Device Options, Configuration Management, Device Alarms, Tools, Scheduled Reboot (expanded), Log Server, and Account Management. The 'Scheduled Reboot' section is active, showing a configuration form with the following fields: 'Scheduled Reboot' set to 'Monthly', '\* Start Time' set to '00:00', and 'Day of Month' set to '7'. There are 'Save' and 'Reset' buttons at the bottom of the form.

## 5.10.9 Log Server

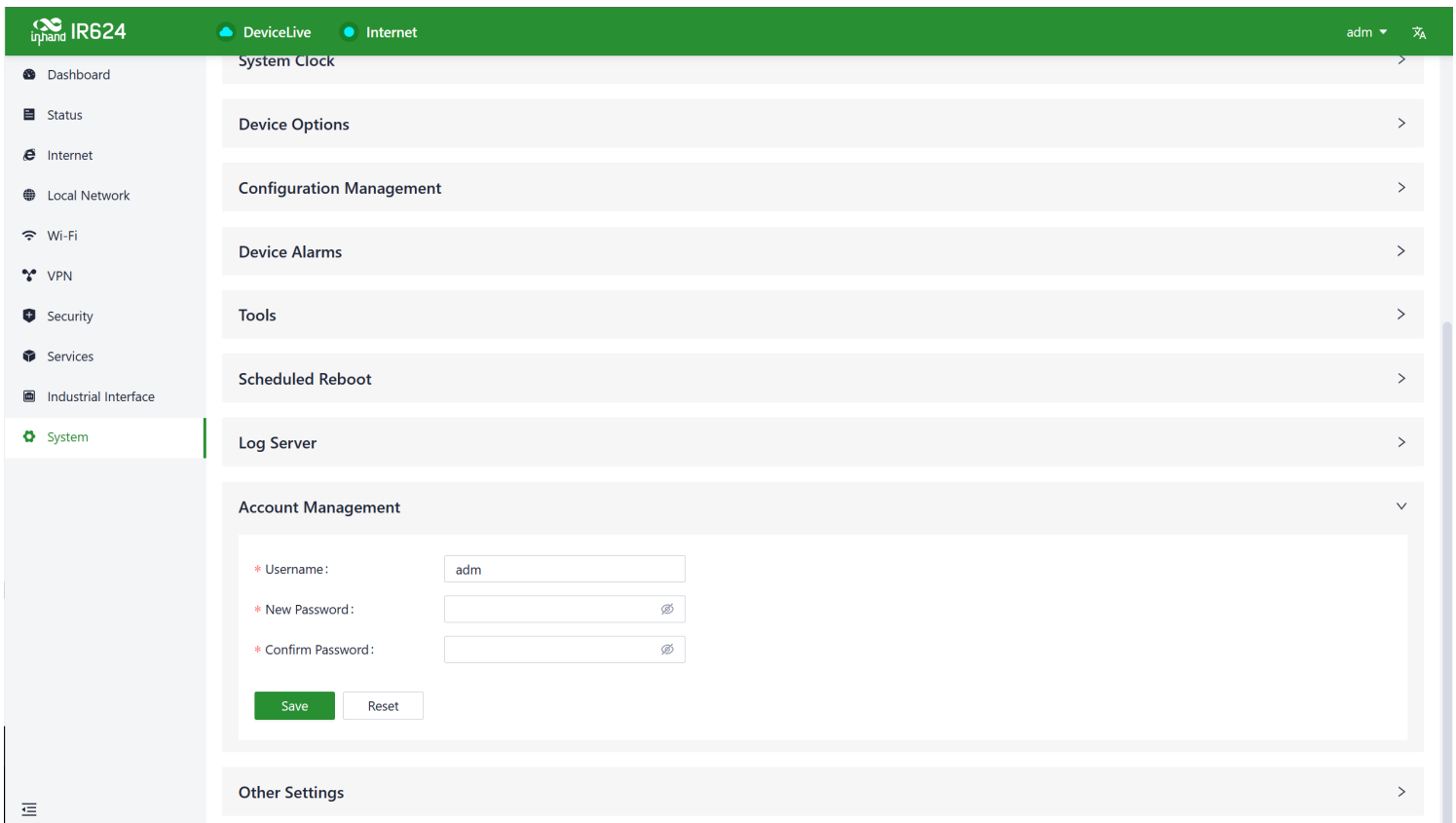
A log server is a dedicated server or software application used to collect, store, and manage log information generated by network devices, applications, and operating systems. These log records include events, warnings, errors, activities, and other relevant information and are crucial for monitoring, troubleshooting, and performance optimization.

When users enable the log file server function in the "System > Log Server" feature, the device will periodically upload log files to the specified log server.



## 5.10.10 Account Management

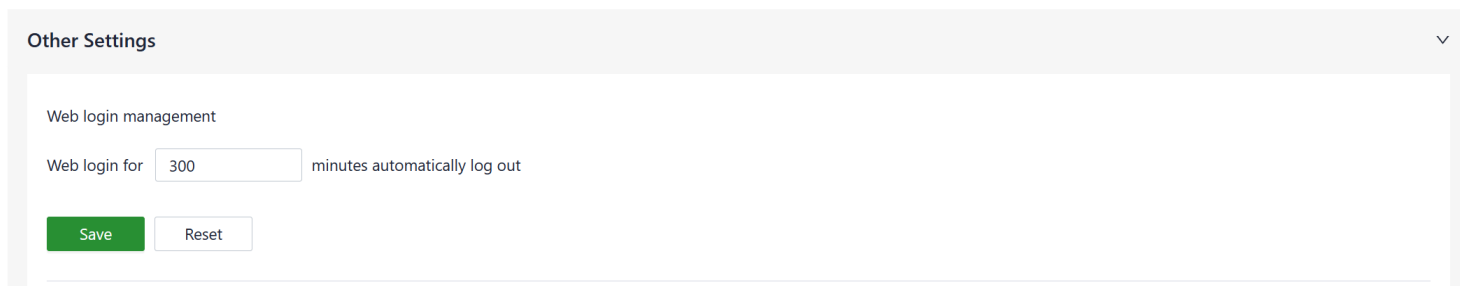
You can change the username and password for logging in to the web page of the device in the "System > Log Server"



## 5.10.11 Other Settings

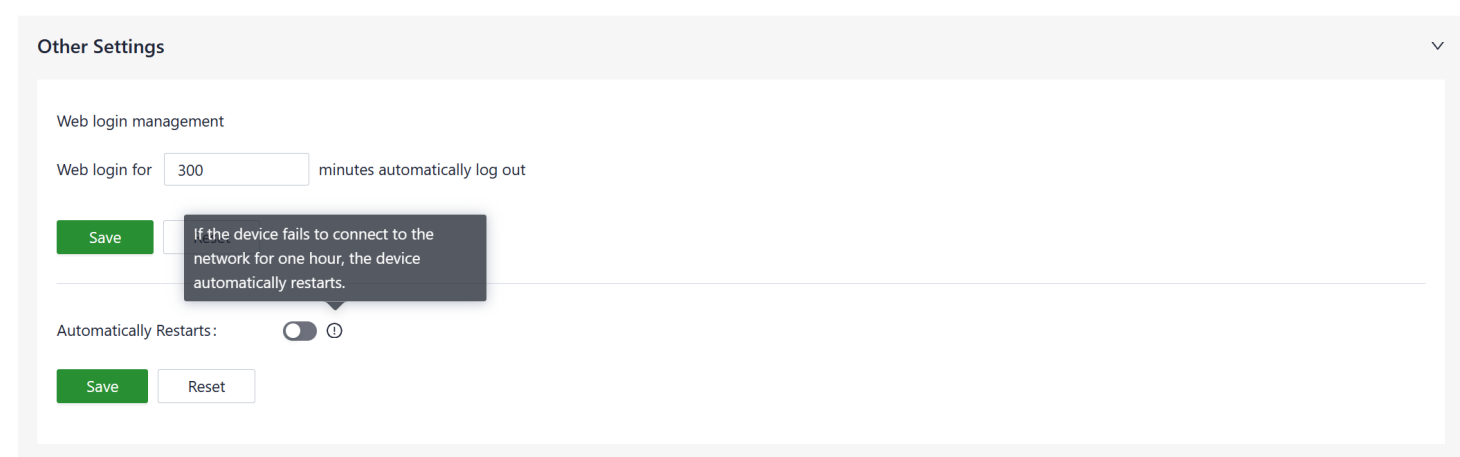
### 5.10.11.1 Web Login Management

When a user logs in to the local interface of the device through the web and the session remains active for a certain period, it will automatically log out or disconnect to protect the user's privacy and security. You can configure the logout time in "System > Other Settings > Web Login Management." If the online time during a single login session on the device's web page exceeds the configured time, the system will automatically log the user out, and they will need to log in again to continue their operations.



### 5.10.11.2 Automatically Restart

This feature can be used to quickly forward packets, improving network performance. By default, it is turned off. When users enable this feature in "System > Other Settings > Fast Forward," the device's data forwarding rate will significantly increase.



## 6. Security Precautions

1. Please use the original power adapter to avoid damaging the device due to mismatched power adapters.
2. When installing the device, avoid placing it in an environment with strong electromagnetic interference, and keep it at a safe distance from high-power equipment. After installation, ensure that the device is stable to prevent accidental drops and potential damage.
3. Ensure that the device's operating environment meets the temperature and humidity requirements specified in the user manual.
4. Regularly inspect the device's cables, including Ethernet cables and power adapter connections. Keep the cables clean, and replace them if any damage is detected.
5. When cleaning the device, avoid spraying chemical agents directly on the device's surface to prevent damage to the housing or internal components. Use a soft cloth for cleaning.

6. Do not attempt to disassemble or modify the device on your own, as this can pose safety risks and may void the device's warranty.

# Appendix A

## EU Declaration of Conformity

**IR624 supported frequency bands and transmit power are as follows:**

WCDMA B1:

Tx(MHz): 1920-1980, Rx(MHz): 2110-2170, Power: 25dBm

WCDMA B3:

Tx(MHz): 1710-1785, Rx(MHz): 1805-1880, Power: 25dBm

WCDMA B5:

Tx(MHz): 824-849, Rx(MHz): 869-894, Power: 25dBm

WCDMA B8:

Tx(MHz): 880-915, Rx(MHz): 925-960, Power: 25dBm

LTE B1:

UL(MHz): 1920-1980, DL(MHz): 2110-2170, Power: 24.5dBm

LTE B3:

UL(MHz): 1710-1785, DL(MHz): 1805-1880, Power: 24.5dBm

LTE B5:

UL(MHz): 824-849, DL(MHz): 869-894, Power: 24.5dBm

LTE B7:

UL(MHz): 2500-2570, DL(MHz): 2620-2690, Power: 24.5dBm

LTE B8:

UL(MHz): 880-915, DL(MHz): 925-960, Power: 24.5dBm

LTE B20:

UL(MHz): 832-862, DL(MHz): 791-821, Power: 24.5dBm

LTE B28:

UL(MHz): 703-748, DL(MHz): 758-803, Power: 24.5dBm

LTE B38:

UL(MHz): 2570-2620, DL(MHz): 2570-2620, Power: 24.5dBm

LTE B40:

UL(MHz): 2300-2400, DL(MHz): 2300-2400, Power: 24.5dBm

LTE B41:

UL(MHz): 2496-2690, DL(MHz): 2496-2690, Power: 24.5dBm

5G NR n1:

UL(MHz): 1920-1980, DL(MHz): 2110-2170, Power: 24.5dBm

5G NR n3:

UL(MHz): 1710-1785, DL(MHz): 1805-1880, Power: 24.5dBm

5G NR n5:

UL(MHz): 824-849, DL(MHz): 869-894, Power: 24.5dBm

5G NR n7:

UL(MHz): 2500-2570, DL(MHz): 2620-2690, Power: 24.5dBm

5G NR n8:

UL(MHz): 880-915, DL(MHz): 925-960, Power: 24.5dBm

5G NR n20:

UL(MHz): 832-862, DL(MHz): 791-821, Power: 24.5dBm

5G NR n28:

UL(MHz): 703-748, DL(MHz): 758-803, Power: 24.5dBm

5G NR n38:

UL(MHz): 2570-2620, DL(MHz): 2570-2620, Power: 24.5dBm

5G NR n40:

UL(MHz): 2300-2400, DL(MHz): 2300-2400, Power: 24.5dBm

5G NR n41:

UL(MHz): 2496-2690, DL(MHz): 2496-2690, Power: 27.5dBm

5G NR n77:

UL(MHz): 3300-4200, DL(MHz): 3300-4200, Power: 27.5dBm

5G NR n78:

UL(MHz): 3300-3800, DL(MHz): 3300-3800, Power: 27.5dBm


2.4G Wi-Fi:

2412MHz-2472MHz, Power: 19.92dBm

5G Wi-Fi:

5150MHz-5250MHz, 5725MHz-5825MHz, Power: 19.19dBm

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

	AT	BE	BG	HR	CY	CZ	DK
	EE	FI	FR	DE	EL	HU	IE
	IT	LV	LT	LU	MT	NL	PL
	PT	RO	SK	SI	ES	SE	UK(NI)

The operation temperature range of IR624: -20°C- +70°C °

This equipment should be installed and operated with minimum distance of 30 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Warning: Operation of this equipment in a residential environment could cause radio interference.

Hereby, Beijing InHand Networks Technology Co., Ltd. declares that the radio equipment type [IR624,IR6X4 Where X represents the numbers 0-9] is in compliance with Directive 2014/ 53/EU. The full text of the EU

declaration of conformity is available at the following internet address:<https://www.inhand.com.cn>