STRONG

ATRIA MESH AX3000

MESHAX3000

Table of Contents

I. Introduction ---- 4
1. General Introduction ---- 4
2. Presentation of the Device and its LEDs ---- 4
3. Presentation of the Web UI ---- 4
II. Configuring your Device and Network ---- 6
1. Setting Up your mesh network ---- 6
2. Optimizing your mesh network ---- 9
3. Adding mesh units to your network ---- 10
4. Connecting to the Wi-Fi and Accessing the Web UI ---- 11
5. Changing the administrator password in the Web UI ---- 13
6. Resetting the device to its factory configuration ---- 15
III. Using the Web UI ---- 18
1. Changing the SSID (Wi-Fi Network Name) and password ---- 18
2. Updating the device Firmware ---- 20
IV. Customized Settings ---- 23
1. LAN Info ---- 23
1.1. Wi-Fi Basic Info ---- 23
1.2. LAN Ethernet Info ---- 23
1.3. Connected Device Info ---- 23
2. Network ---- 24
2.1. WAN Configuration ---- 24
2.1.1. Static ---- 24
2.1.2. PPPoE ---- 25
2.2. LAN Configuration ---- 26
2.2.1. IPv4 Configuration ---- 26
2.2.2. IPv6 Configuration ---- 28
2.3. Speed Limit Configuration ---- 28
3. WLAN ---- 29
3.1. 2.4 G ---- 29
3.1.1. Multiple SSID ---- 29
3.1.2. WPS ---- 30
3.1.3. Advanced Settings ---- 33
3.2. Advanced ---- 34
3.2.1. Access Control ---- 34
3.2.2. Scheduler ---- 36
3.2.3. Easy Mesh ---- 37
3.2.4. Band Steering ---- 38
4. Security ---- 39
4.1. Firewall Settings ---- 39

4.1.1. Firewall Level ---------- 39
4.1.2. DoS Settings ---------- 39
4.2. Parental Control ---------- 40
4.2.1. Schedule ---------- 40
4.2.2. Mac Filter ---------- 41
4.2.3. URL Filter ---------- 42
4.2.4. IP Filter ---------- 45
4.3. ACL ---------- 46
5. Application ---------- 48
5.1. NAT ---------- 48
5.1.1. ALG ---------- 48
5.1.2. DMZ ---------- 49
5.1.3. Port Forwarding ---------- 49
5.2. VPN ---------- 50
5.3. SNTP ---------- 51
5.4. DDNS ---------- 52
5.5. UPnP ---------- 53
5.6. IPTV Configuration ---------- 55
5.6.1. Snooping ---------- 55
5.6.2. Proxy ---------- 55
6. System Tools ---------- 56
6.1. Device Management ---------- 56
6.1.1. Reboot ---------- 56
6.1.2. Settings Backup ---------- 57
6.1.3. Settings Upgrade ---------- 57
6.1.4. Restore Default ---------- 58
6.1.5. LED control ---------- 59
6.2. Diagnostic ---------- 59
6.2.1. Ping Test ---------- 59
6.2.2. Tracer Test ---------- 60
6.2.3. TR069 Inform ---------- 62
V. Accessing the FAQs ---------- 62

I. Introduction

1. General Introduction

The following user manual is meant to guide you in the installation process of your ATRIA MESH AX3000. For this purpose, we will detail the process to set up your device and network. In addition, we will present you the process to connect to Web UI and the different parameters that you can set, as well as the meaning of the LEDs that you can see on your device.

2. Presentation of the Device and its LEDs

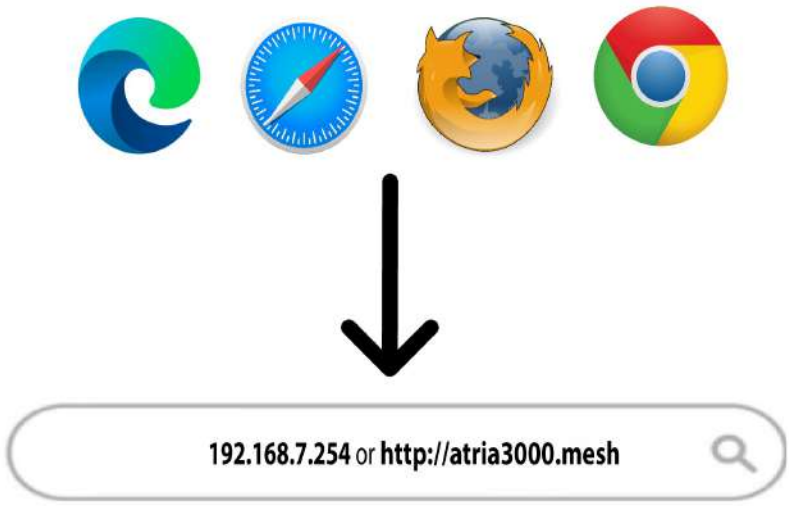
Congratulations, you bought one of our mesh product, now it is the time to present the device before configuring it for its first use.
The Atria Mesh AX3000 works with a RJ45 Connection to your router/modem. Then, you must pair the two mesh units together.

There are 5 different LEDs on the front of your AX3000 Mesh. The floowing image shows the different statuses of the LEDs.

3. Presentation of the Web UI

The Web UI is the place where you can set up advanced parameters for your device but also customize your SSID, password and so much more.

The Web UI is accessible after connecting to the Wi-Fi of the device or to the internet connection of the mesh unit by using the Ethernet cable and entering the following IP Address in your browser:

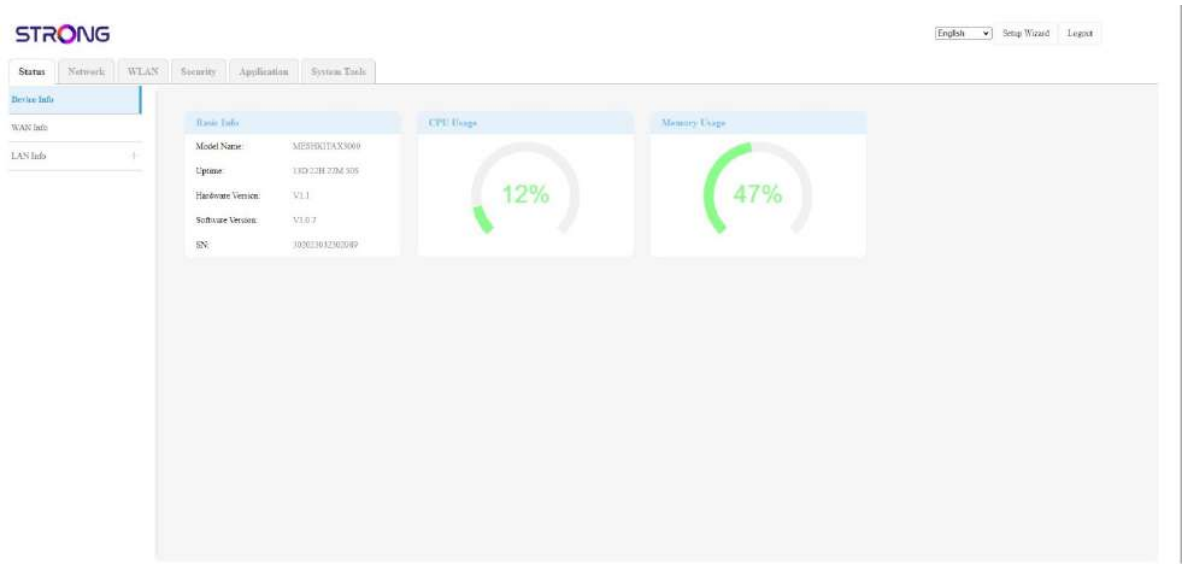


Once you have entered the password, you can see that the Web UI is organised into different sections:

The Web UI is divided into 6 sections:

Status: Where you can find all the informations about the Mesh device and Network.

- Network: where you can configure the WAN, the LAN settings (IPv4 / IPv6) and set up a Speed Limit.
- WLAN: where you choose between 2.4G and 5G network, set up multiples SSID, the WPS, manage the internet access of the different mac address, modify the SSID and Wi-Fi Passwords and set up a Mesh.
- Security: where you can set up a firewall, DoS Settings, URL/MAC filters, IP filters, parental/service control and Schedule the Mesh Network activation.
- Application: where you can configure the NAT settings (ALG, DMZ, Port Forwarding), a VPN, the SNTP (Time zone), a VPN, a Dynamic DNS, the UPnP and access the IPTV Configuration.
- System Tools: where you can change the login credentials, reboot the device, update the firmware, save and restore a backup, reset to factory settings, manage the LEDs, access the logs and launch diagnostics.



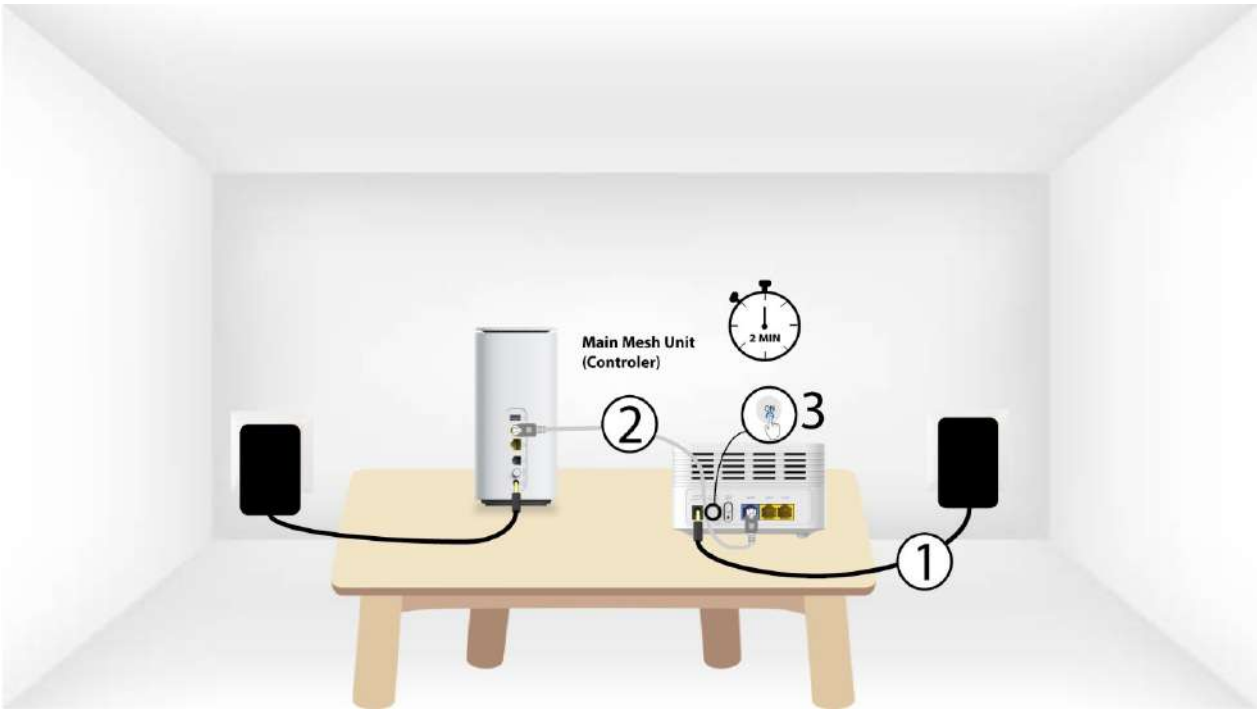
II. Configuring your Device and Network

1. Setting Up your mesh network

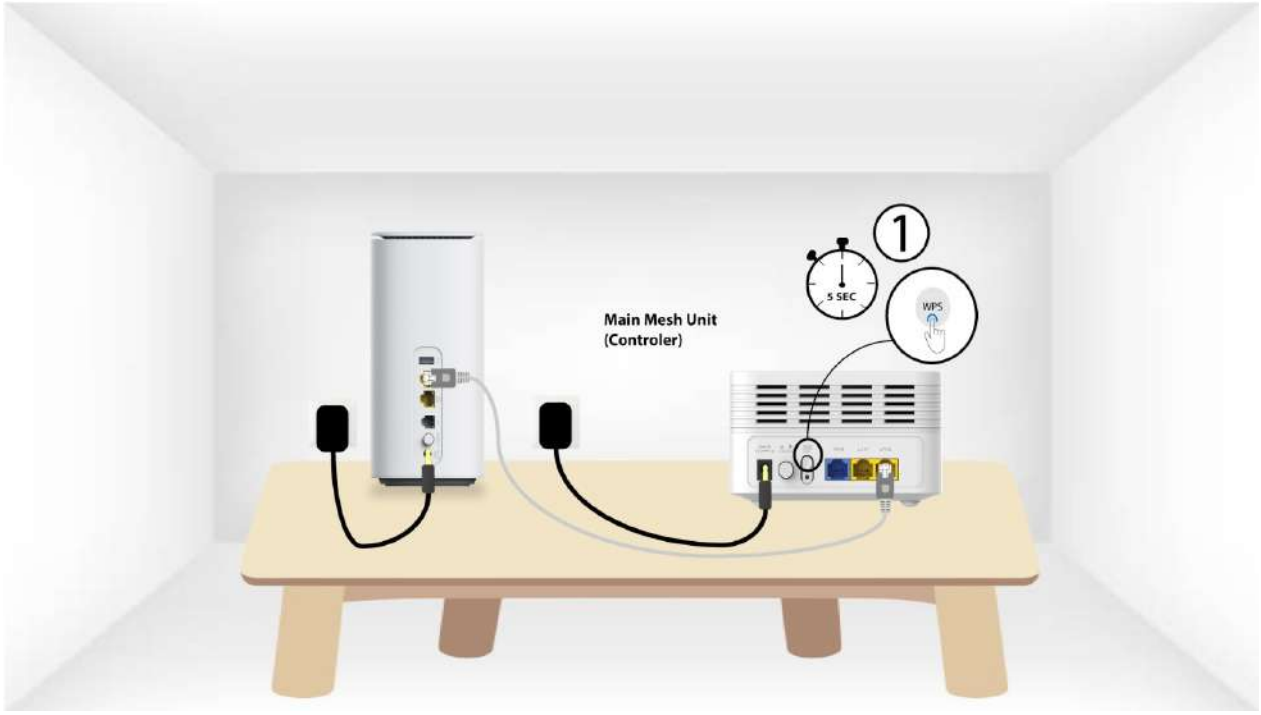
To configure your Mesh network please refer to the QIG provided in the box of your product.

Case 1: WPS Button

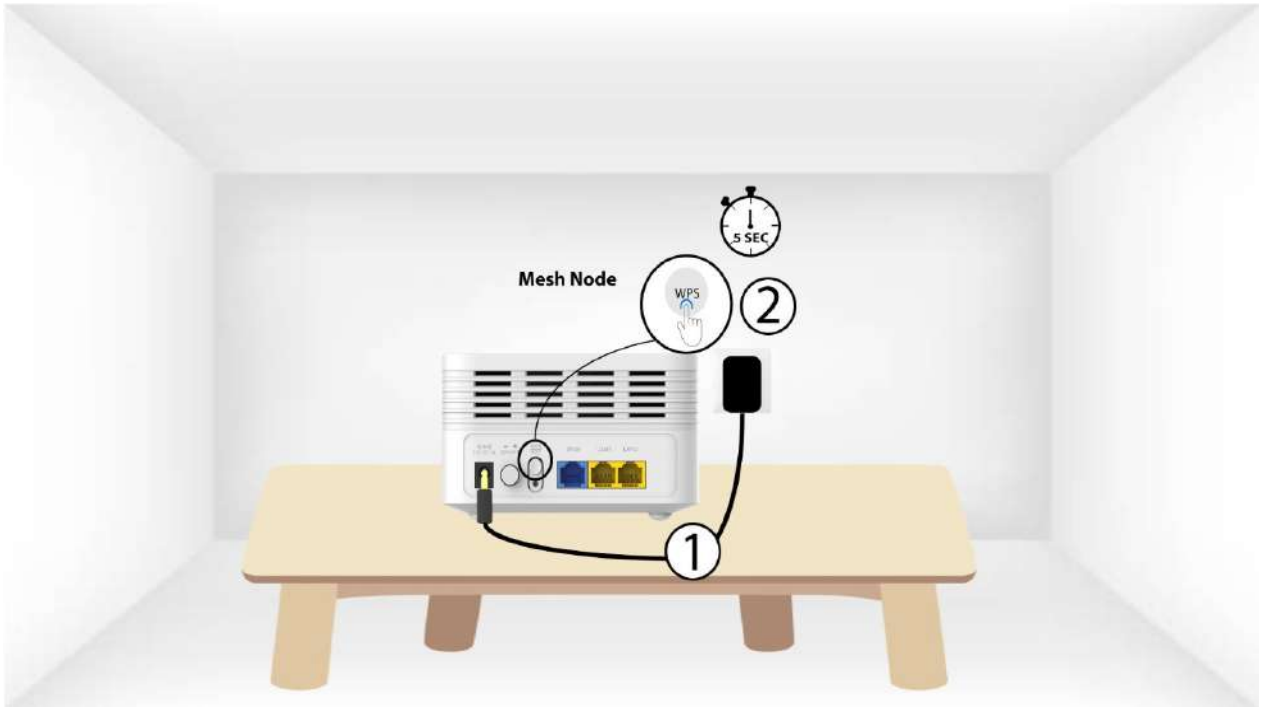
1. You must plug in the mesh unit and connect it to your modem by using an RJ45 cable before pressing the power button.



2. Press the WPS button on the mesh connected to your modem for 5 seconds.



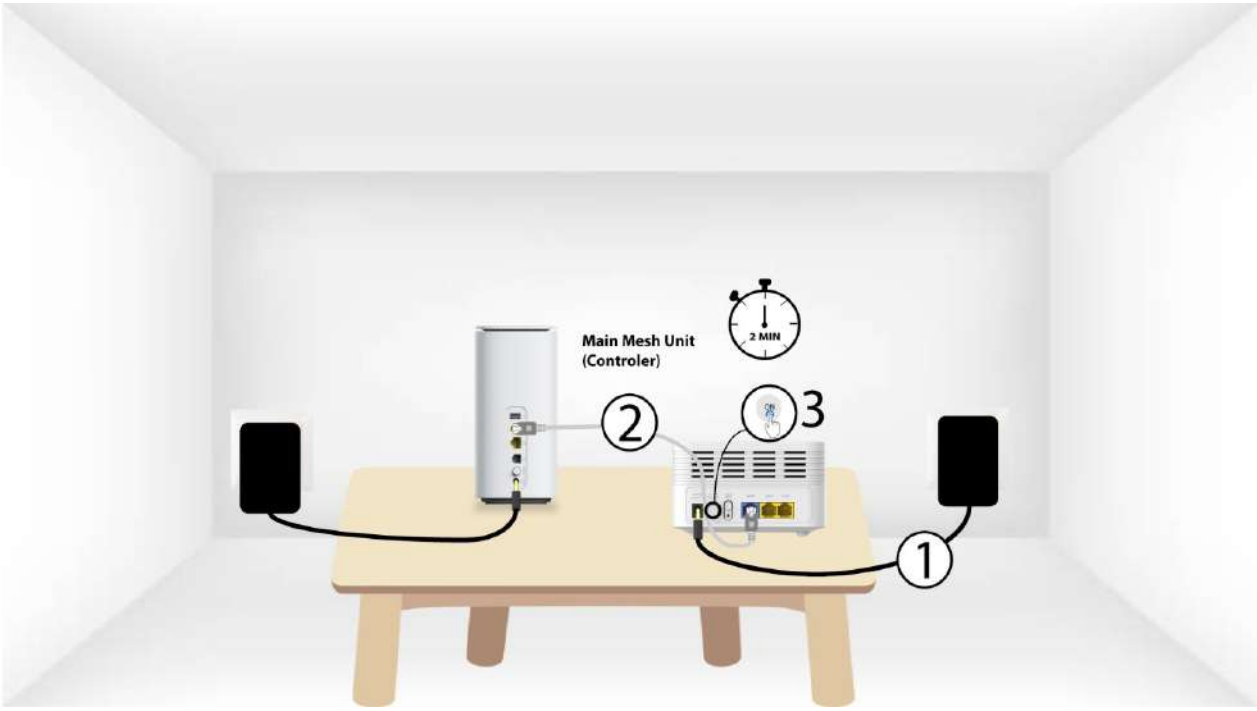
3. Plug the second mesh unit to a socket and press the WPS button for 5 seconds.



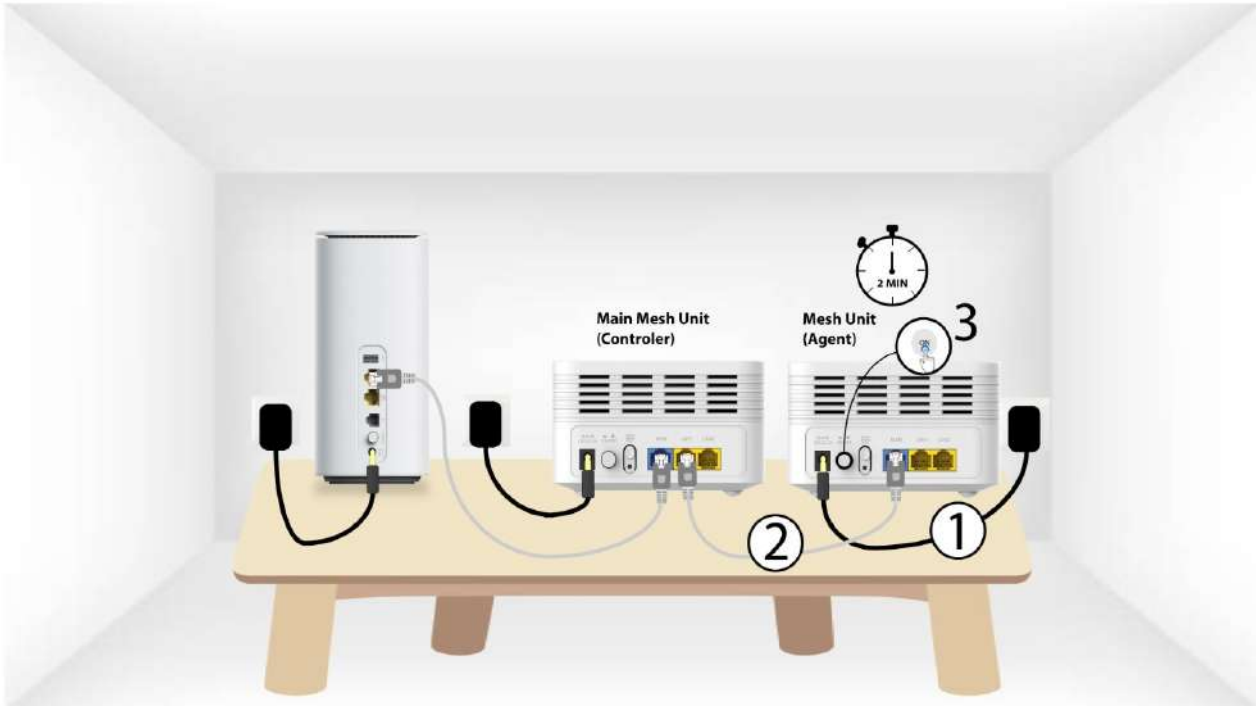
⚠ WARNING: Please note that you need to repeat this operation for each Mesh unit you wish to add to your Mesh network.

Case 2: RJ45 cable

1. You must plug in the mesh unit and connect it to your modem by using a RJ45 cable in the WLAN port before pressing the power button.



2. Plug the Main Mesh Unit (Controler) to the Mesh Unit (Agent) via RJ45 in both LAN port of the two mesh units.



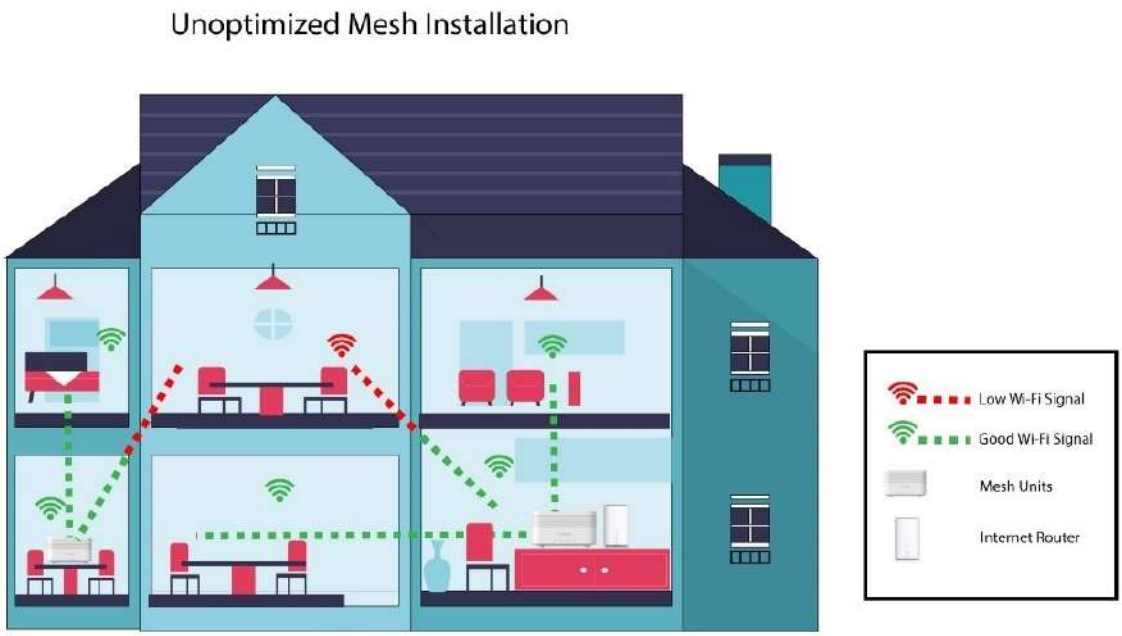
⚠ WARNING: Please note that you need to repeat this operation for each Mesh unit

you wish to add to your Mesh network.

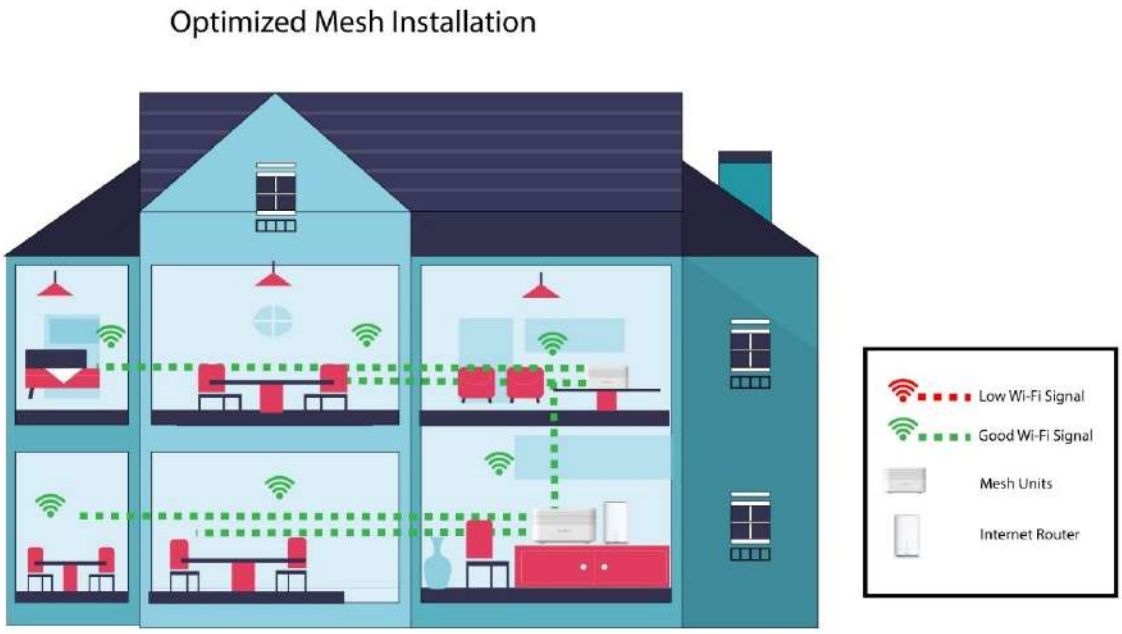
2. Optimizing your mesh network

To optimize you coverage you should install the mesh in the location where you have coverage issues in order to cover the widest area possible in your home. Please make sure that the mesh units are not located in a room where there is a load bearing wall, as the wall is thicker the Wi-Fi signal can have issues getting through it.

The following schema shows Wi-Fi coverage inside a house where mesh nodes are not located in the right area of the house to have a proper coverage.



The following schema shows Wi-Fi coverage inside a house where mesh nodes are located in the right area of the house to have a proper coverage.



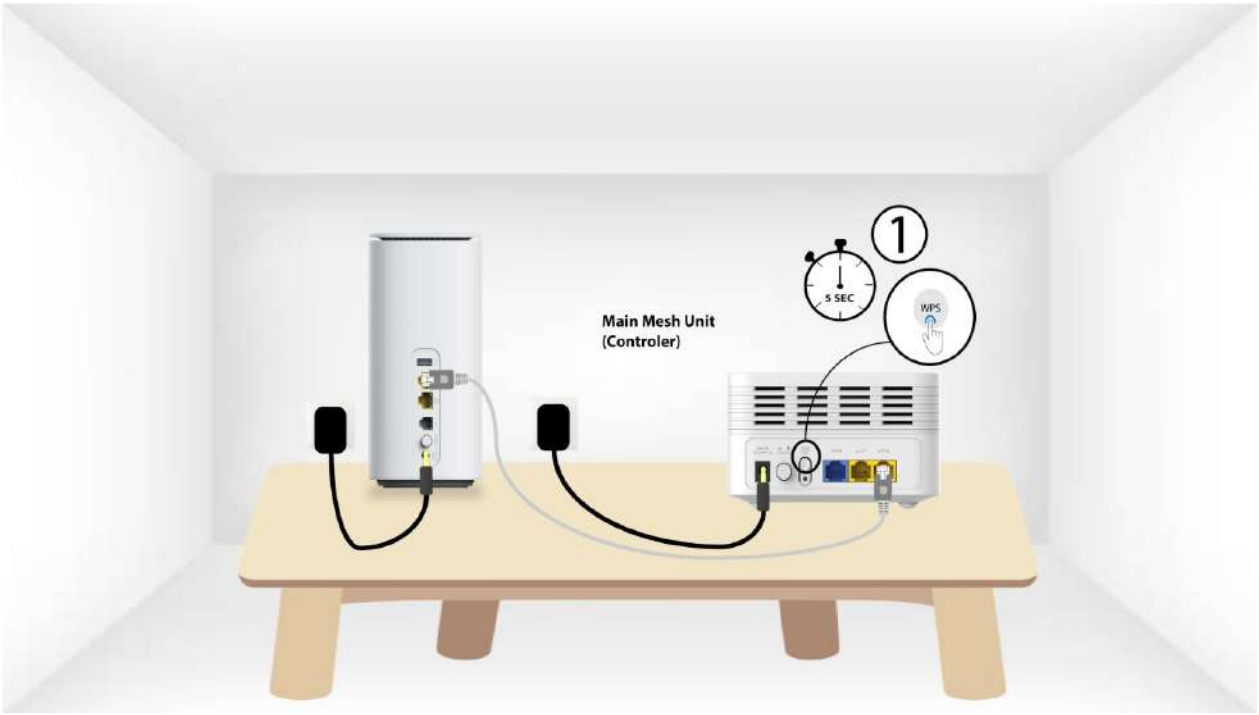
If you have a big house, you can install several mesh units to cover all the rooms.

You can see if the coverage provided by your mesh nodes in your home is OK in the app.

3. Adding mesh units to your network

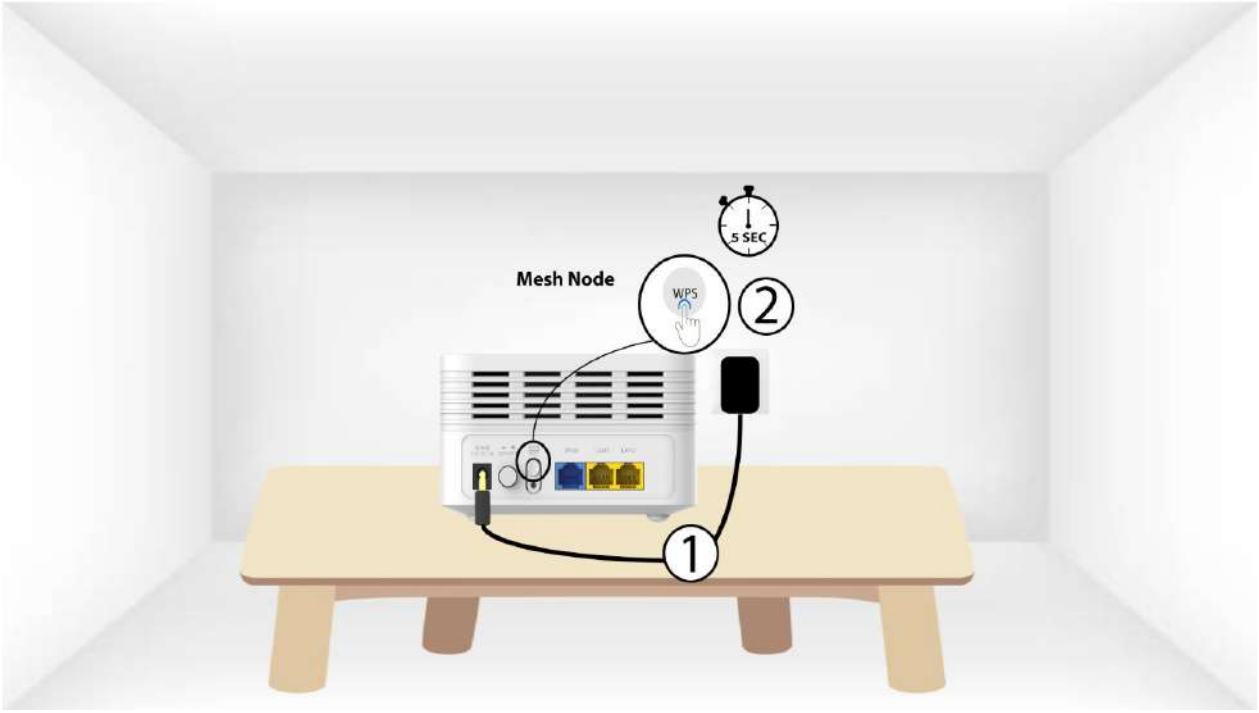
It is very easy to add new mesh units to your existing Mesh network.

1. To do so, press the WPS button for 5 seconds on the Mesh unit that is connected to your router/modem by RJ45.



1.

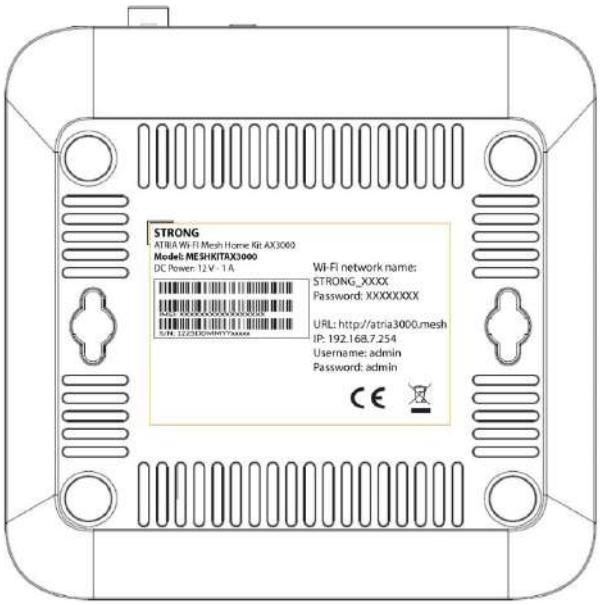
2. Then, press the WPS button on the new unit for 5 seconds.



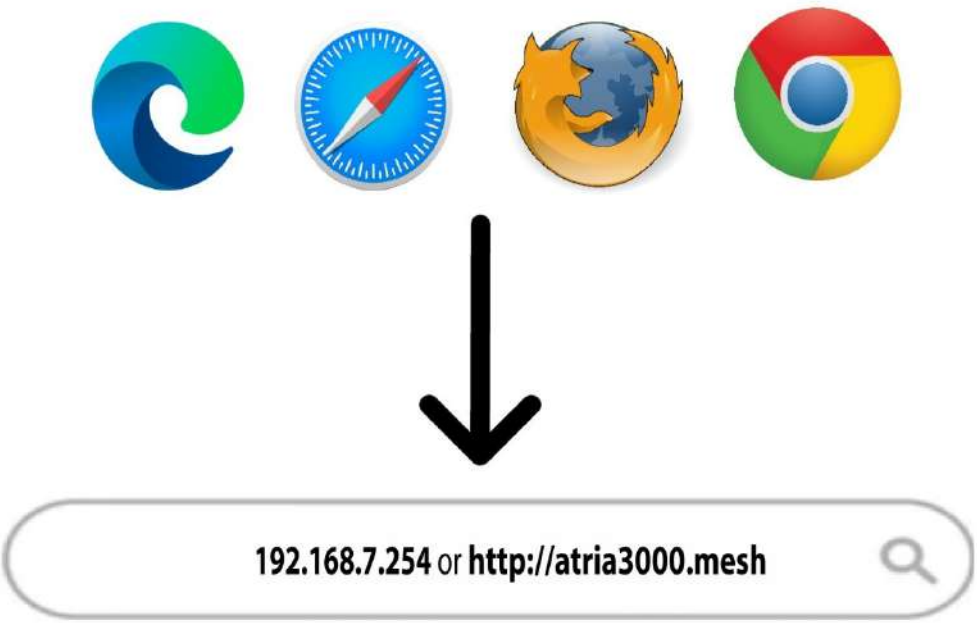
4. Connecting to the Wi-Fi and Accessing the Web UI

You can connect any compatible device to the Wi-Fi of your device and access the Web UI to customize your configuration.

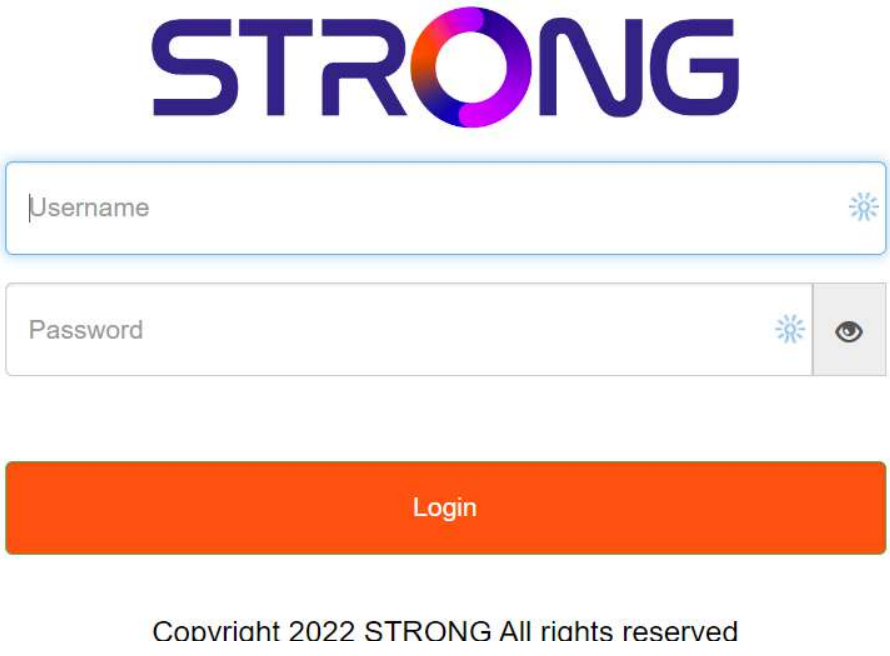
1. To connect to the Wi-Fi, look at the rear side of your router and locate the sticker where the **SSID** and **Password** are written. Then, enter the information in your device.



2. Then, enter the following IP address in your browser:□192.168.7.254 or type the following address: http://atria3000.mesh

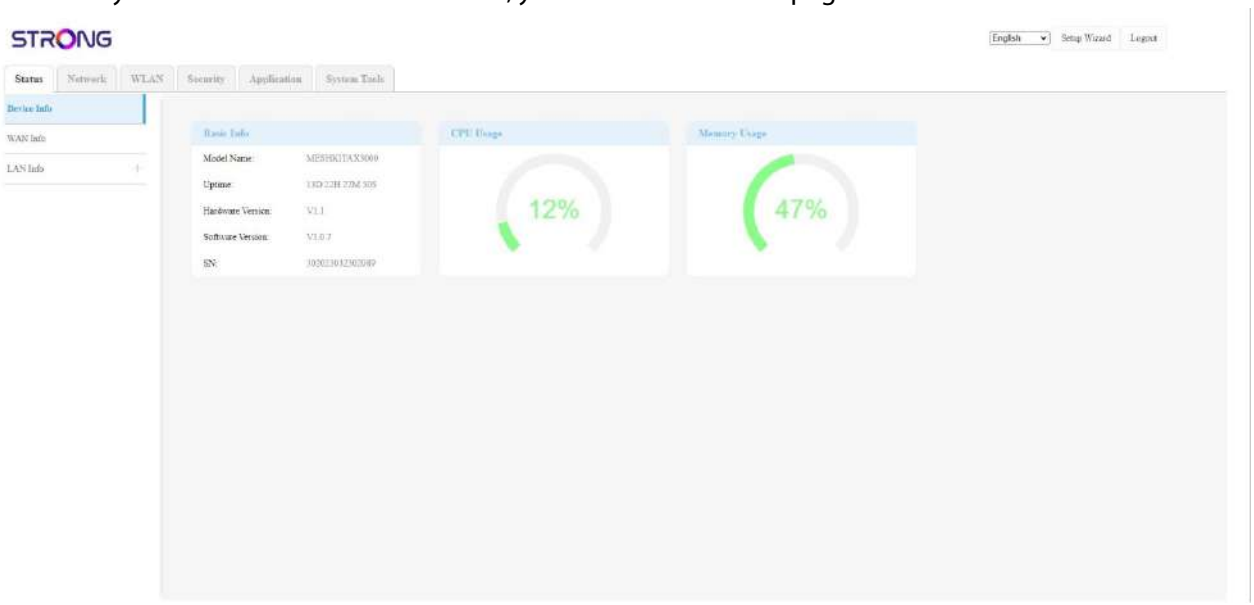


3. A new page opens in which you must enter the **Password** before clicking the **Login** button.



ⓘTIPS: Please note that we strongly advise you to change the admin password. If you decide to change it, your new password must contain at least 8 characters with upper and lower cases, number, and special characters. We strongly suggest using the same password as the one used for the Wi-Fi connection, as this password is unique for your device.

4. Once you are connected to the Web UI, you will see this home page

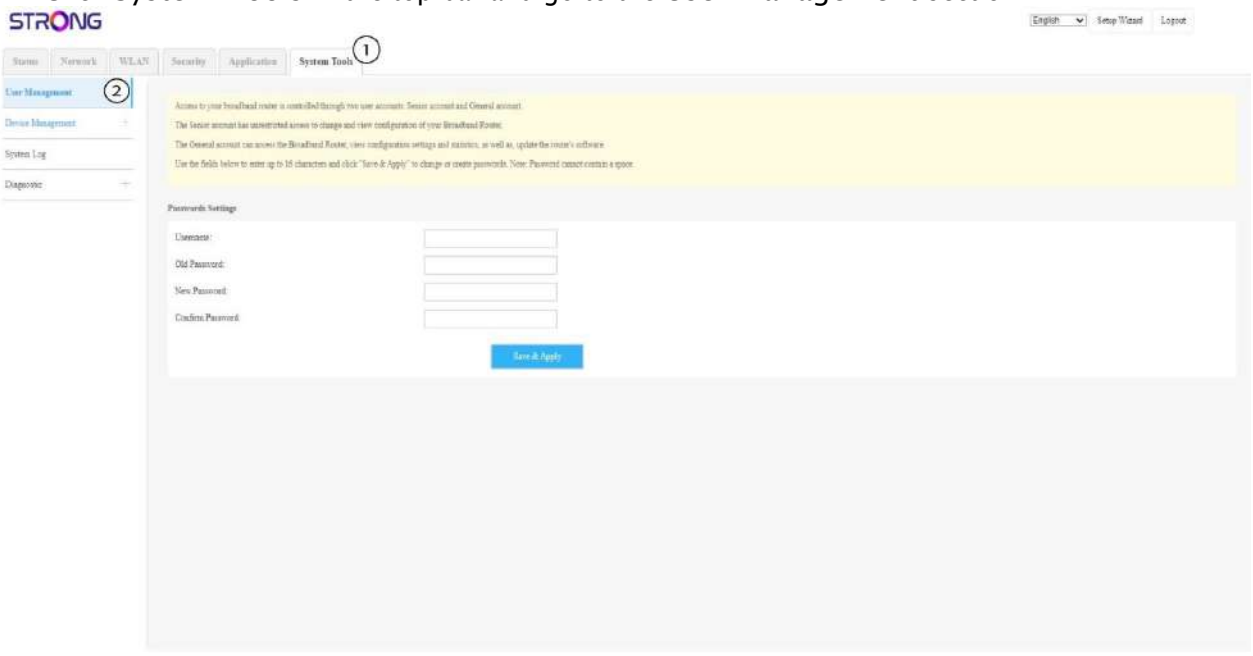


5. Changing the administrator password in the Web UI

We strongly recommend updating the administrator password and username once you're connected to the Web UI, and after you set up all the necessary parameters for your device.

ⓘTIPS: Please note that we strongly advise you to change the admin password. If you decide to change it, your new password must contain at least 8 characters with upper and lower cases, number, and special characters. We strongly suggest using the same password as the one used for the Wi-Fi connection, as this password is unique for your device.

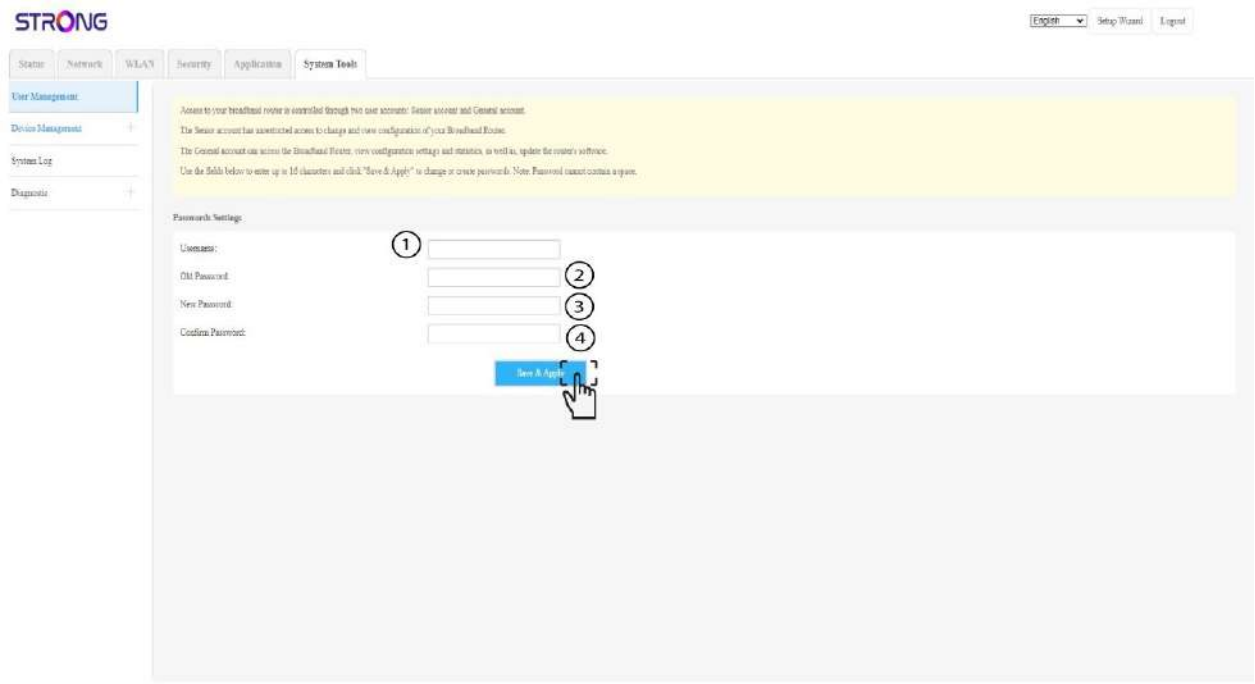
1. Click System Tools in the top bar and go to the User Management section.



3.

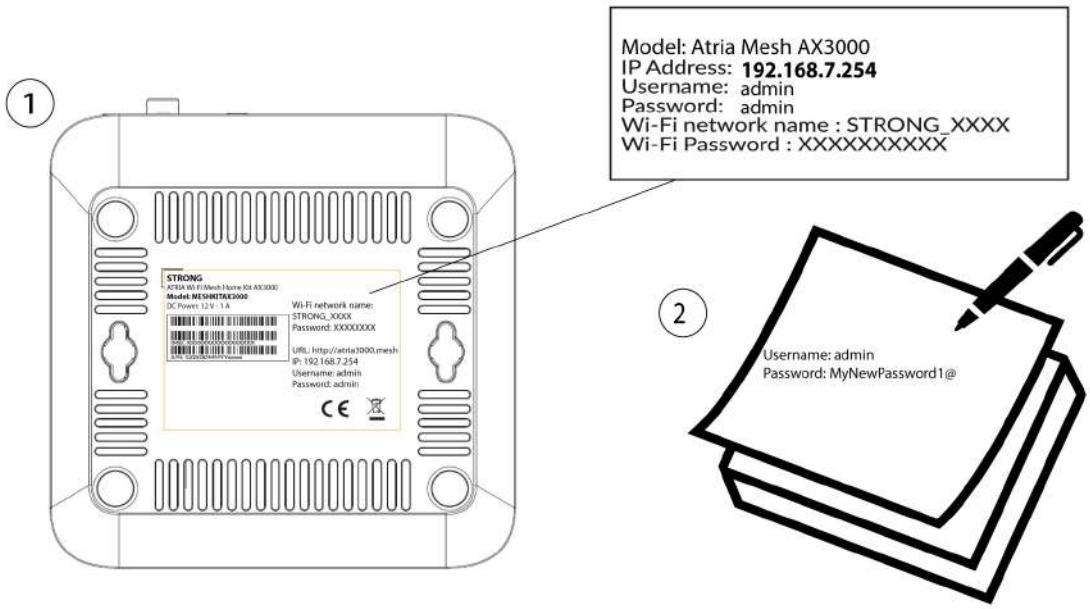
2. Type the Username (admin) and the Old Password. Then in New Password and Confirm Password, enter your new personal password for the Web UI. Then, click on Save & Apply.

⚠WARNING: Please note that you need to enter a password between 8 and 32 characters containing uppercase, lowercase, number and at least one special character (@, $, !, %, *, ?, &)



4.

3. Write down the information a piece of paper and tape it under your device.

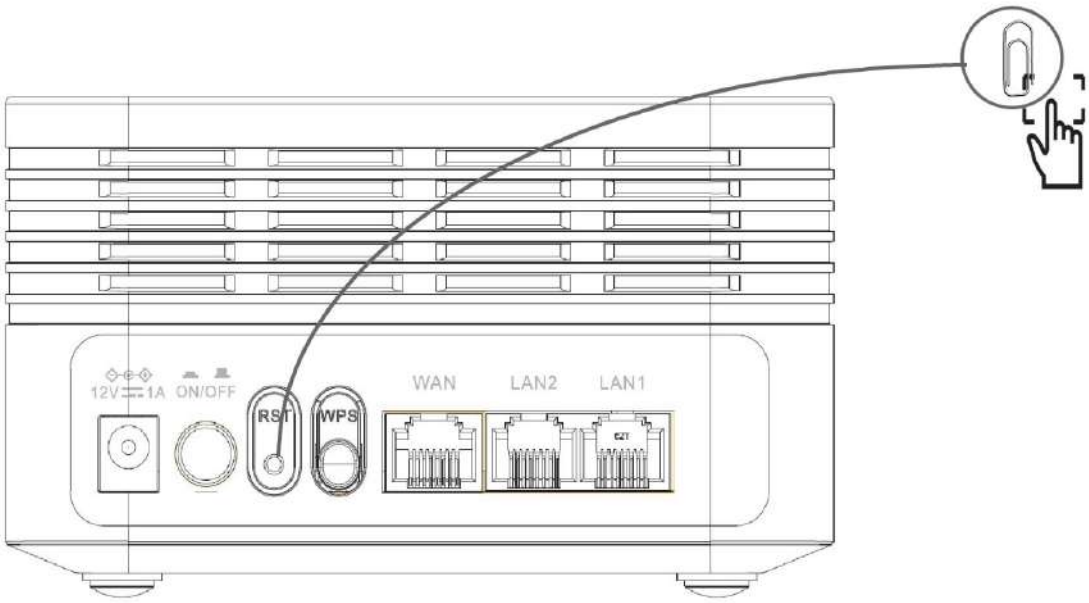


6. Resetting the device to its factory configuration

Sometimes, it is possible that your device is not working properly and that you don't have internet access. In this case, we suggest resetting your device to its factory settings and updating it afterward if necessary. You have two ways to do it; you can reset the device by pressing the reset button or doing it in the Web UI.

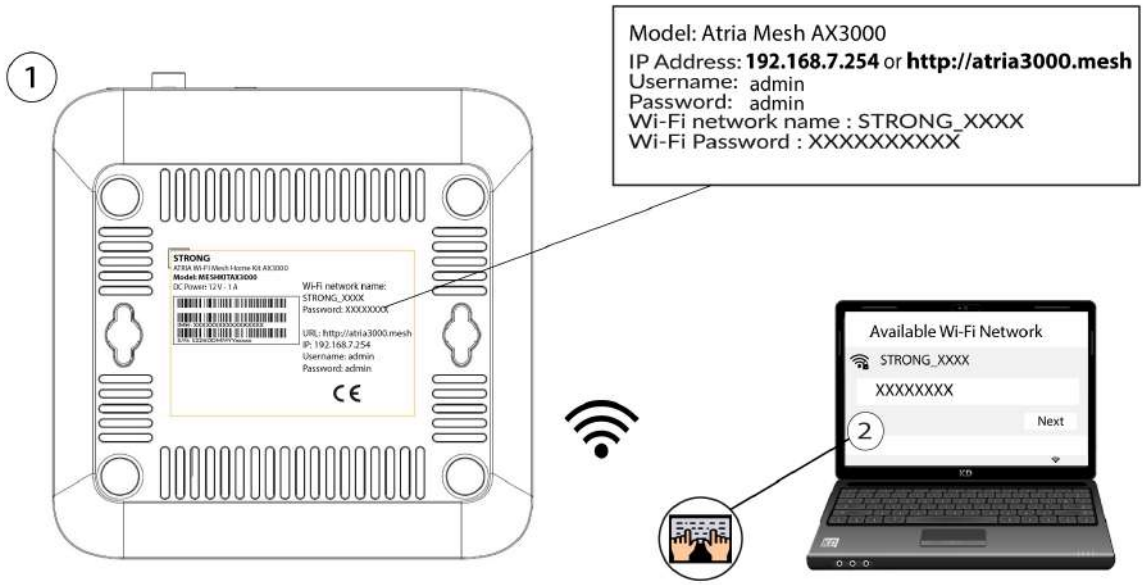
Case 1 : Reset Button

1. To do so, insert a paper clip in the RST hole at the back of the device to press the reset button. Press the reset button for 10 seconds. The LEDS will switch off and turn back on again.

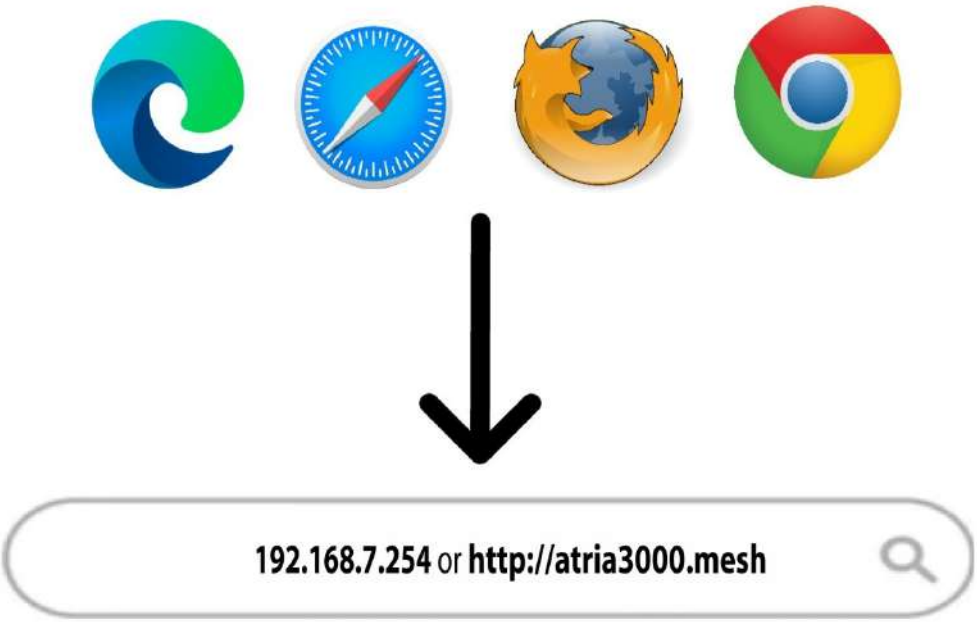


Case 2: Web UI

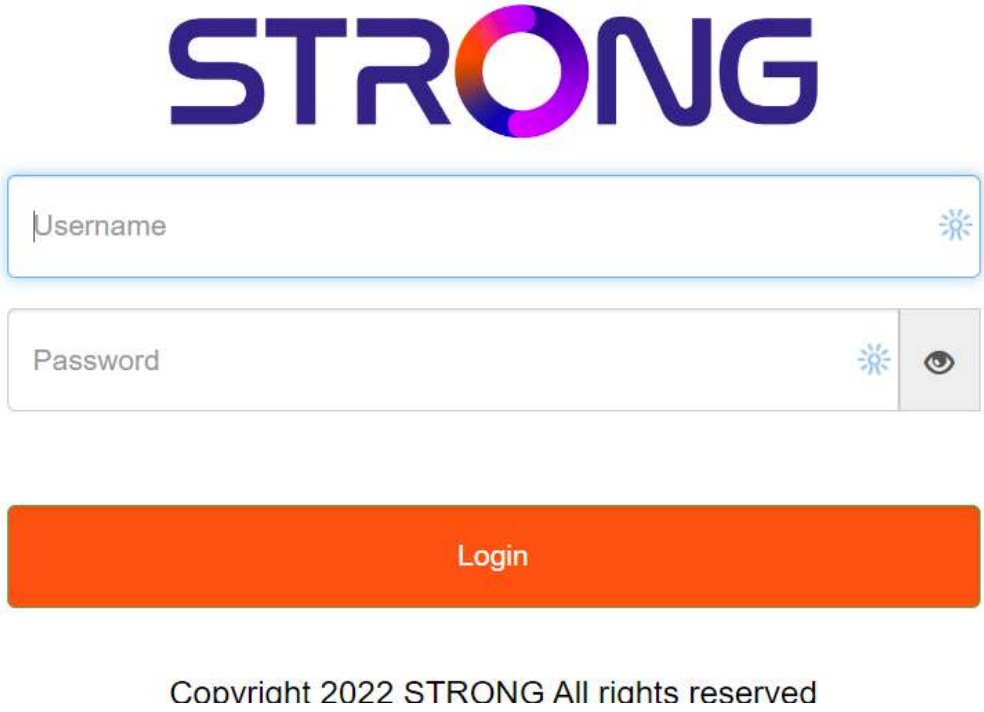
1. To do so, enter the SSID (Wi-Fi Network Name) and Wi-Fi password of the router in your device:



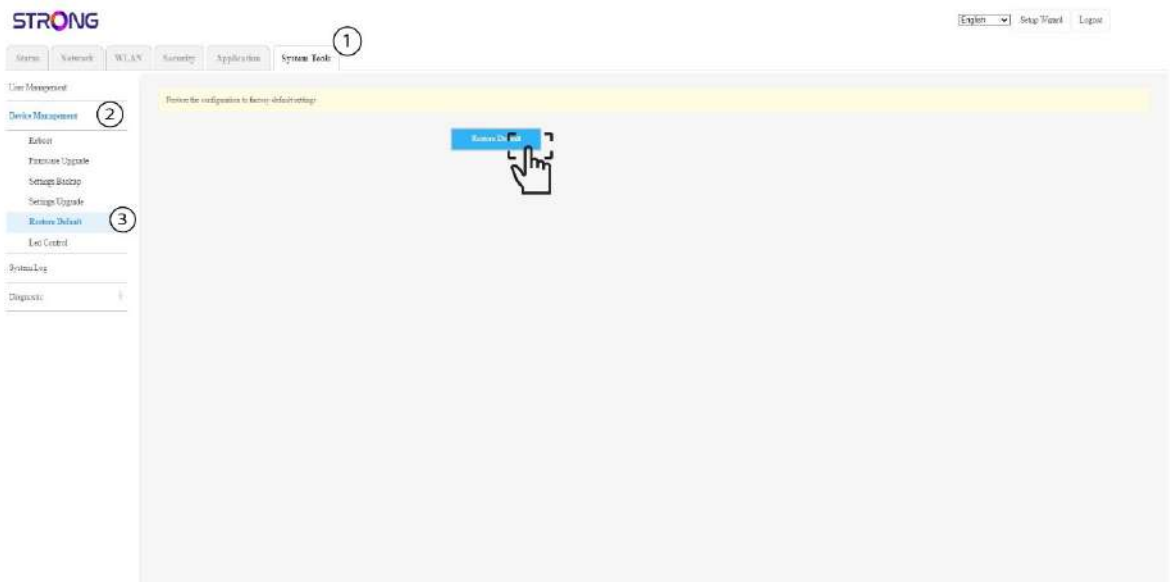
2. Then, enter the following IP address in your browser: 192.168.7.254 or type the following address : http://atria3000.mesh



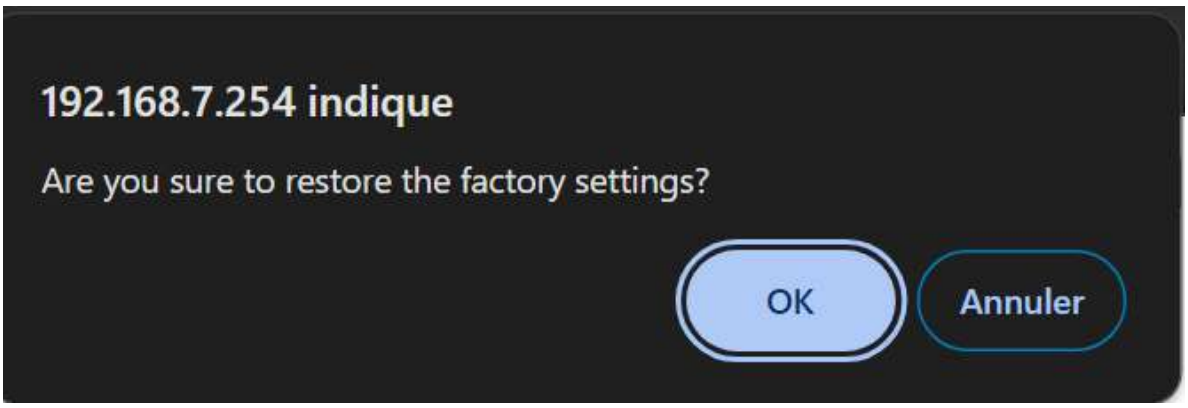
3. You must enter the Username (admin) and Password (admin) (please note that after the first connection you will create your personal admin password which means that the password written on the product label will not work any more). Then, click Login.



4. Then, in the top bar, click System Tools, then go on the Device Management section and click on Restore Default.



5. Then, click OK in the pop-up window.



III. Using the Web UI

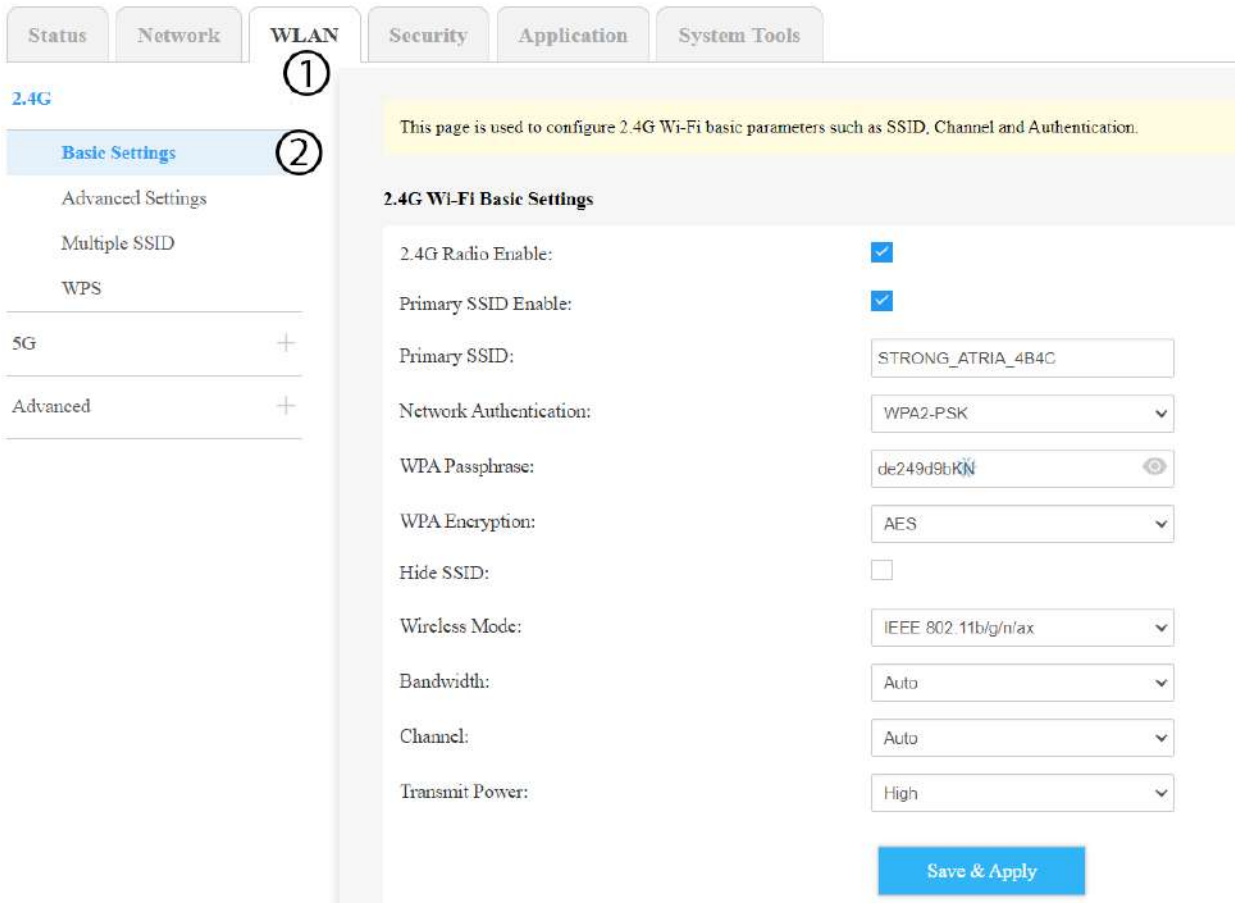
Once you have configured your device and network, you can customize some settings. For instance, you can decide to deactivate/edit your PIN code, edit the SSID and password, and update the firmware.

1. Changing the SSID (Wi-Fi Network Name) and password

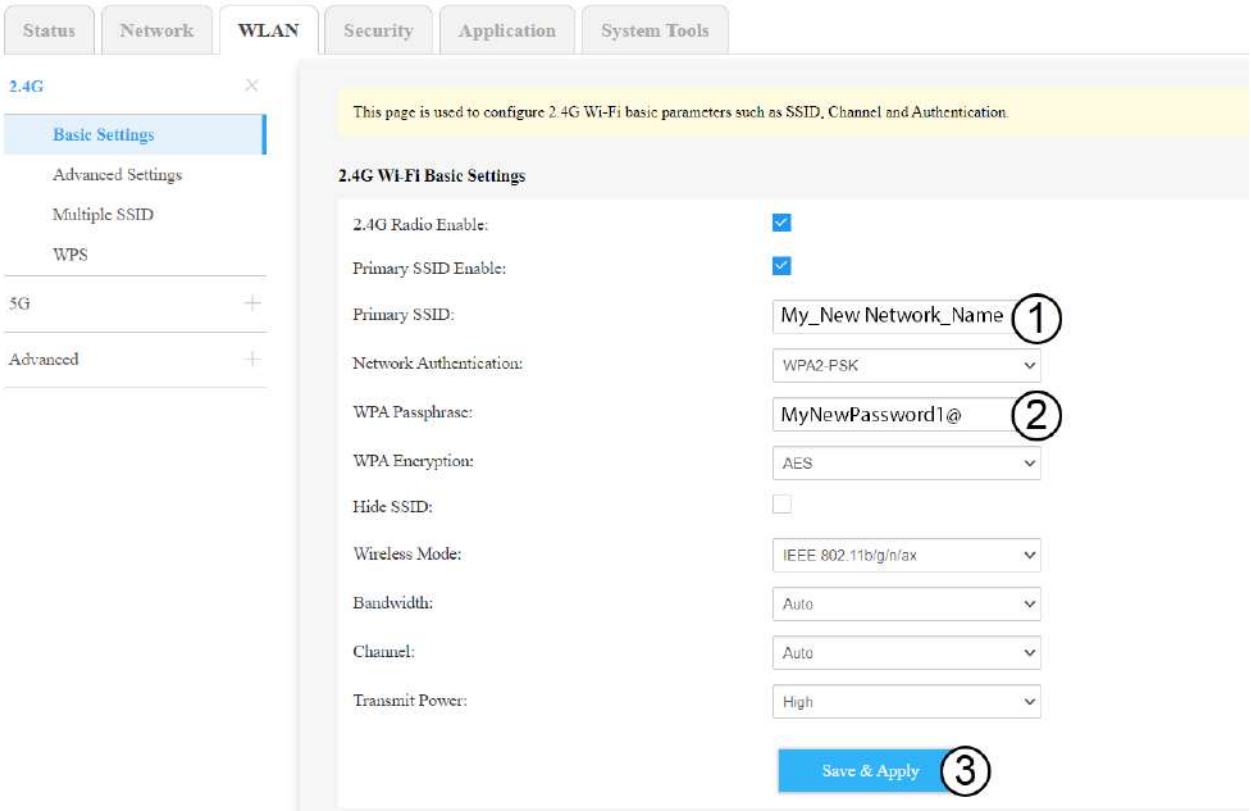
After setting up your device and connecting to it for the first time, it is possible for you to change the SSID, also known as the name of your Wi-Fi Network and its password.

⚠ WARNING: Please note that we strongly recommend using a network name and password that is different from the one of your Internet box. Why? As you may know, your devices automatically connect to the known networks, so if you put the same names and password for your router network and your Internet box, you will not be able to differentiate them.

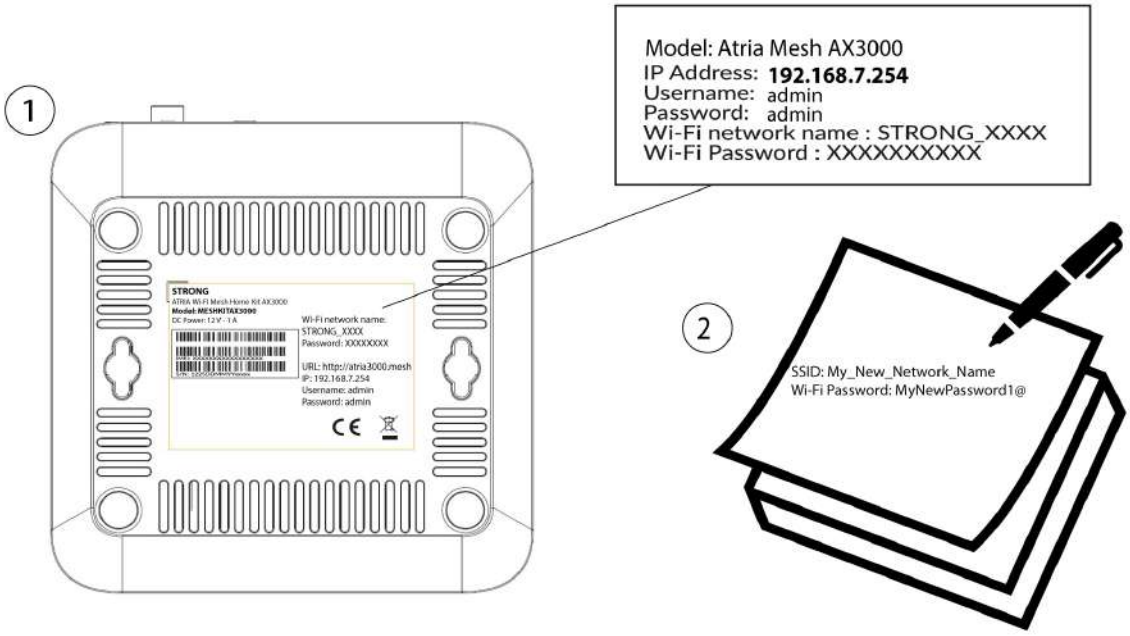
1. Click **WLAN** and **Basic Settings**.



2. Enter the new **primary SSID** and clikc the eye icon to display the **WPA Passphrase**. Enter a new passphrase and click **Save & Apply**.



3. Write down the new network information on a piece of paper.



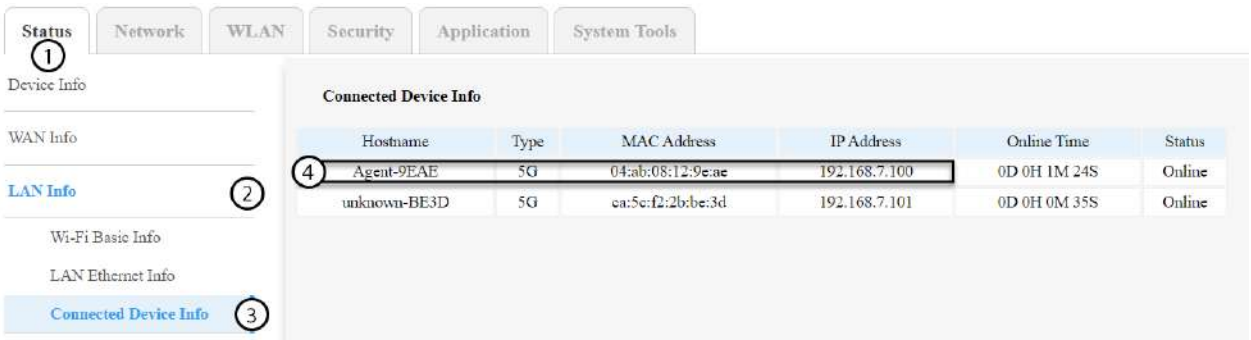
Warning: After changing the Wi-Fi network information all the devices that were connected to the network will be automatically disconnected.

2. Updating the device Firmware

1. To update the firmware of the device, you must browse to this page. You will find the firmware file. Click on the name to download it.

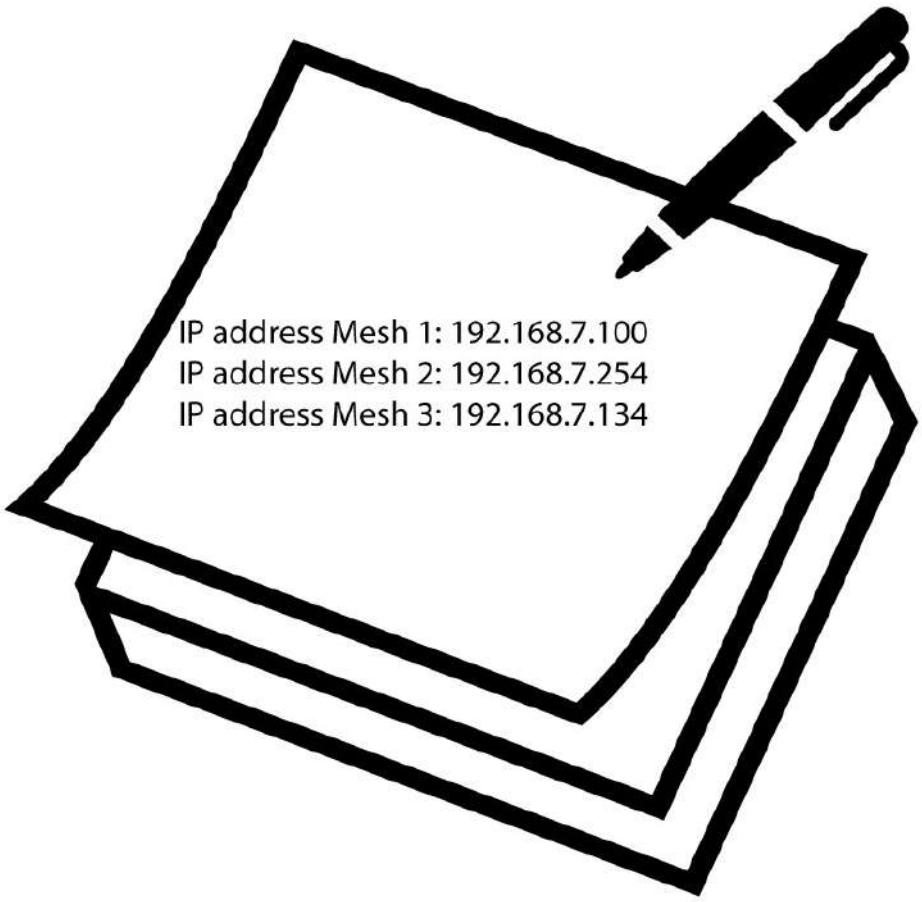
2. To do so, connect to the Web UI, please follow this procedure: Connecting to the Wi-Fi and Accessing the Web UI

3. You must identify the IP addresses of the other mesh nodes. You can do this by clicking **Status, LAN info** and **Connected Device Info.**

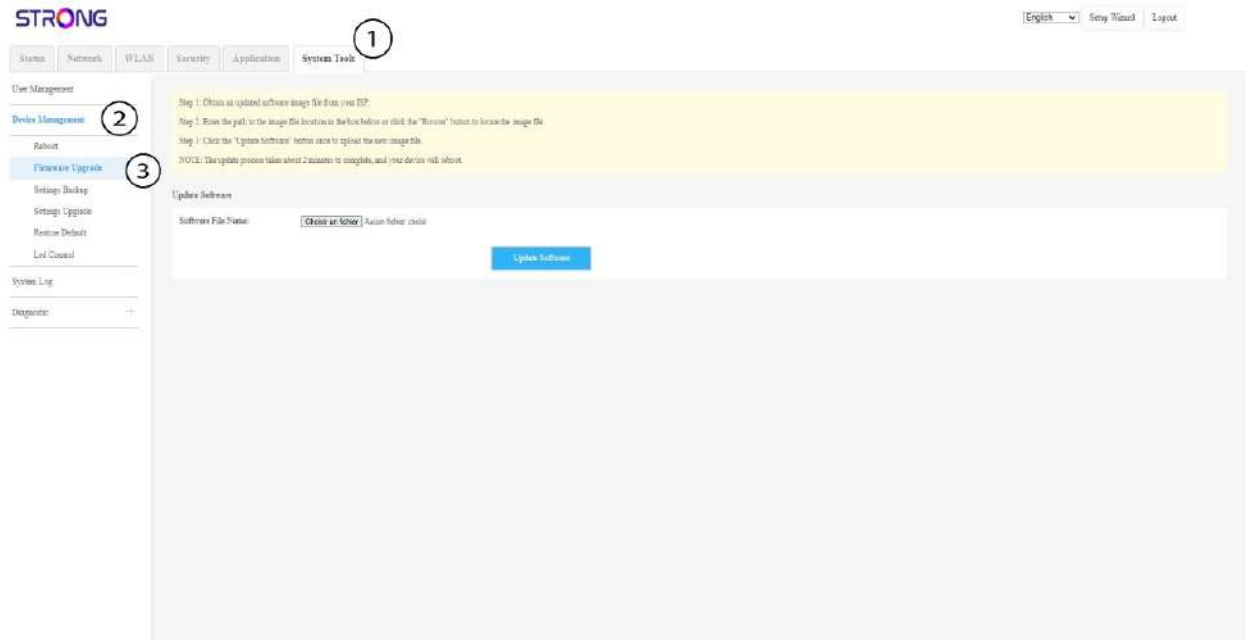


ⓘTIPS: The name of the second mesh units will be Agent-XXXX.

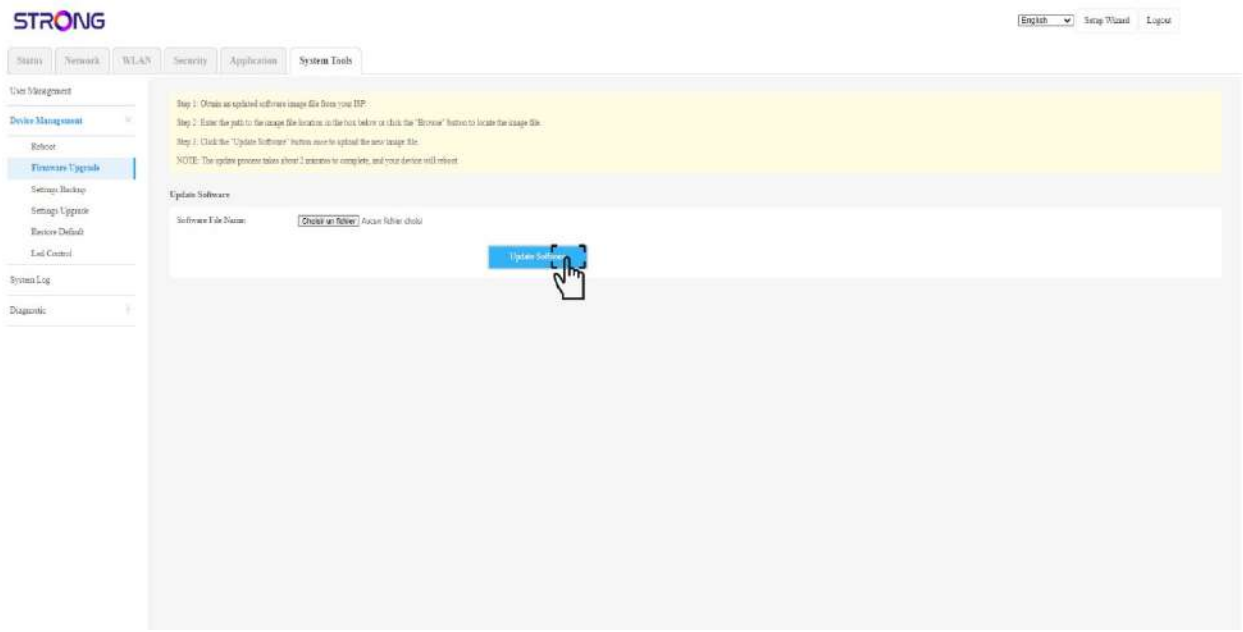
4. Write down the IP Address on a piece of paper.



5. Click **System Tools**, select **Device Management** and **Firmware Update**.



6. Select the fileby clicking **choose file** and click **Update Software**.

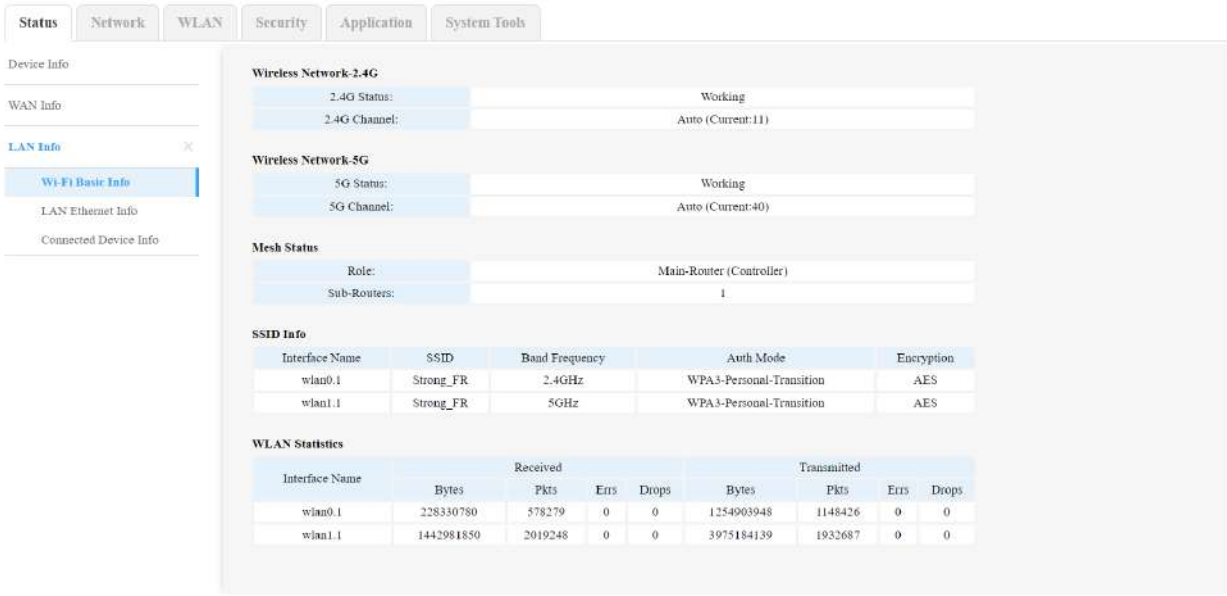


IV. Customized Settings

1. LAN Info

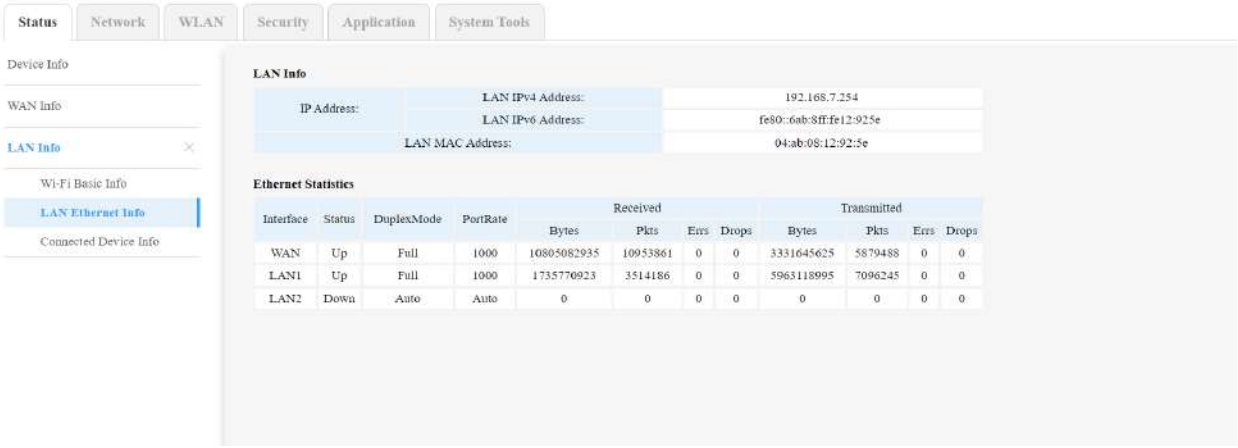
1.1. Wi-Fi Basic Info

You can see the information of the Wi-Fi configuration of your LAN network.



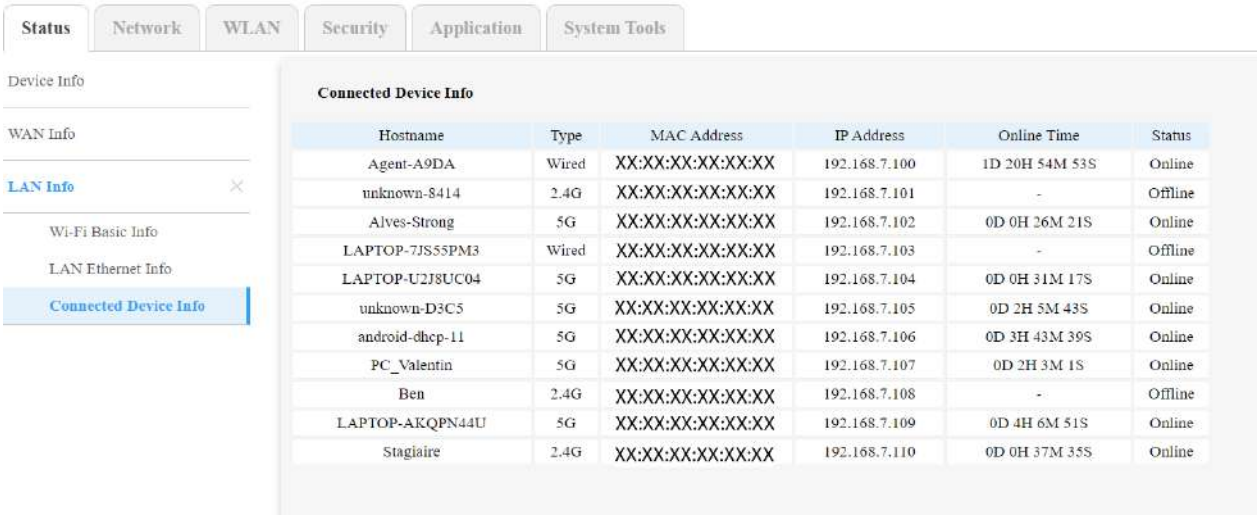
1.2. LAN Ethernet Info

You can see the information of the devices connected to the WAN and LAN ports



1.3. Connected Device Info

You can see the list of connected devices with their name, MAC Address, IP Addresses.
:



Hostname	Type	MAC Address	IP Address	Online Time	Status
Agent-A9DA	Wired	XX:XX:XX:XX:XX:XX	192.168.7.100	1D 20H 54M 53S	Online
unknown-8414	2.4G	XX:XX:XX:XX:XX:XX	192.168.7.101	-	Offline
Alves-Strong	5G	XX:XX:XX:XX:XX:XX	192.168.7.102	0D 0H 26M 21S	Online
LAPTOP-7JS55PM3	Wired	XX:XX:XX:XX:XX:XX	192.168.7.103	-	Offline
LAPTOP-U2J8UC04	5G	XX:XX:XX:XX:XX:XX	192.168.7.104	0D 0H 31M 17S	Online
unknown-D3C5	5G	XX:XX:XX:XX:XX:XX	192.168.7.105	0D 2H 5M 43S	Online
android-dhcp-11	5G	XX:XX:XX:XX:XX:XX	192.168.7.106	0D 3H 43M 39S	Online
PC_Valentin	5G	XX:XX:XX:XX:XX:XX	192.168.7.107	0D 2H 3M 1S	Online
Ben	2.4G	XX:XX:XX:XX:XX:XX	192.168.7.108	-	Offline
LAPTOP-AKQPN44U	5G	XX:XX:XX:XX:XX:XX	192.168.7.109	0D 4H 6M 51S	Online
Stagiaire	2.4G	XX:XX:XX:XX:XX:XX	192.168.7.110	0D 0H 37M 35S	Online

2. Network

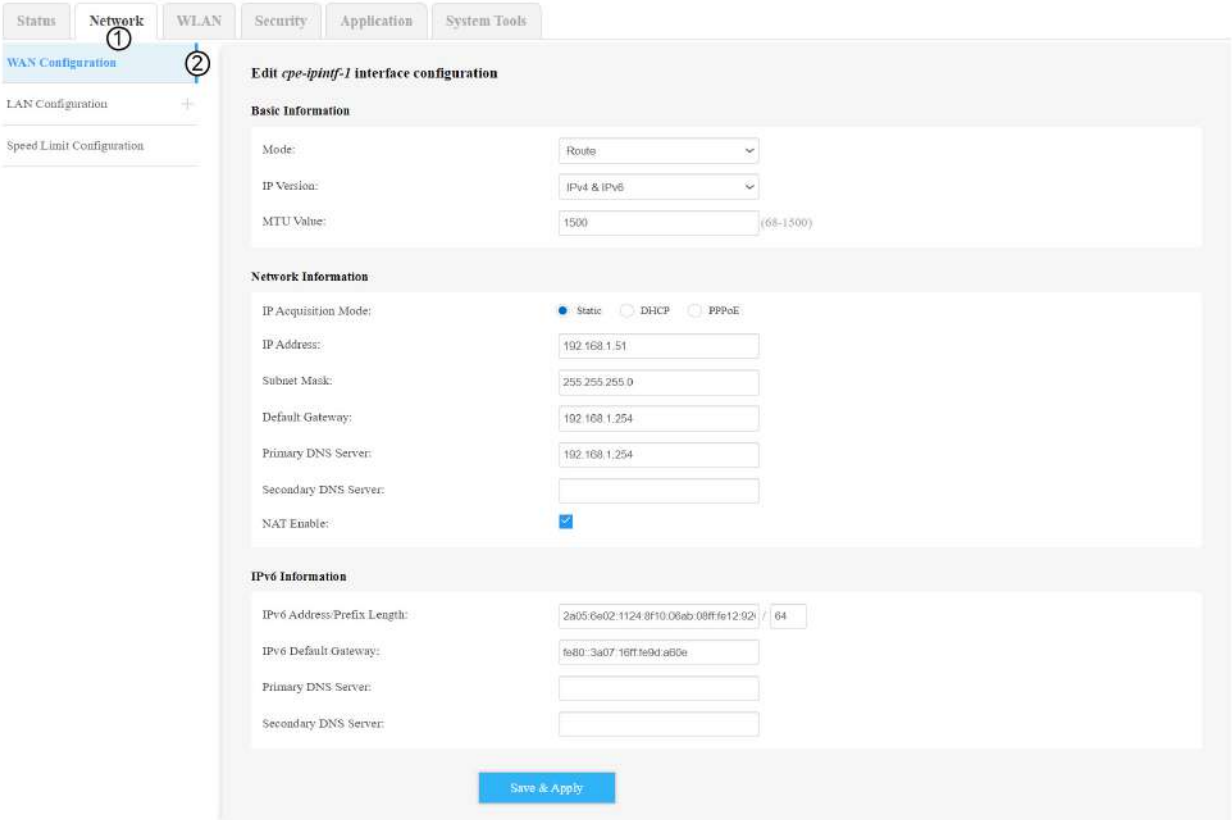
2.1. WAN Configuration

This section enables you to edit the settings of your WAN configuration. By default the WAN configuration is set up to DHCP.

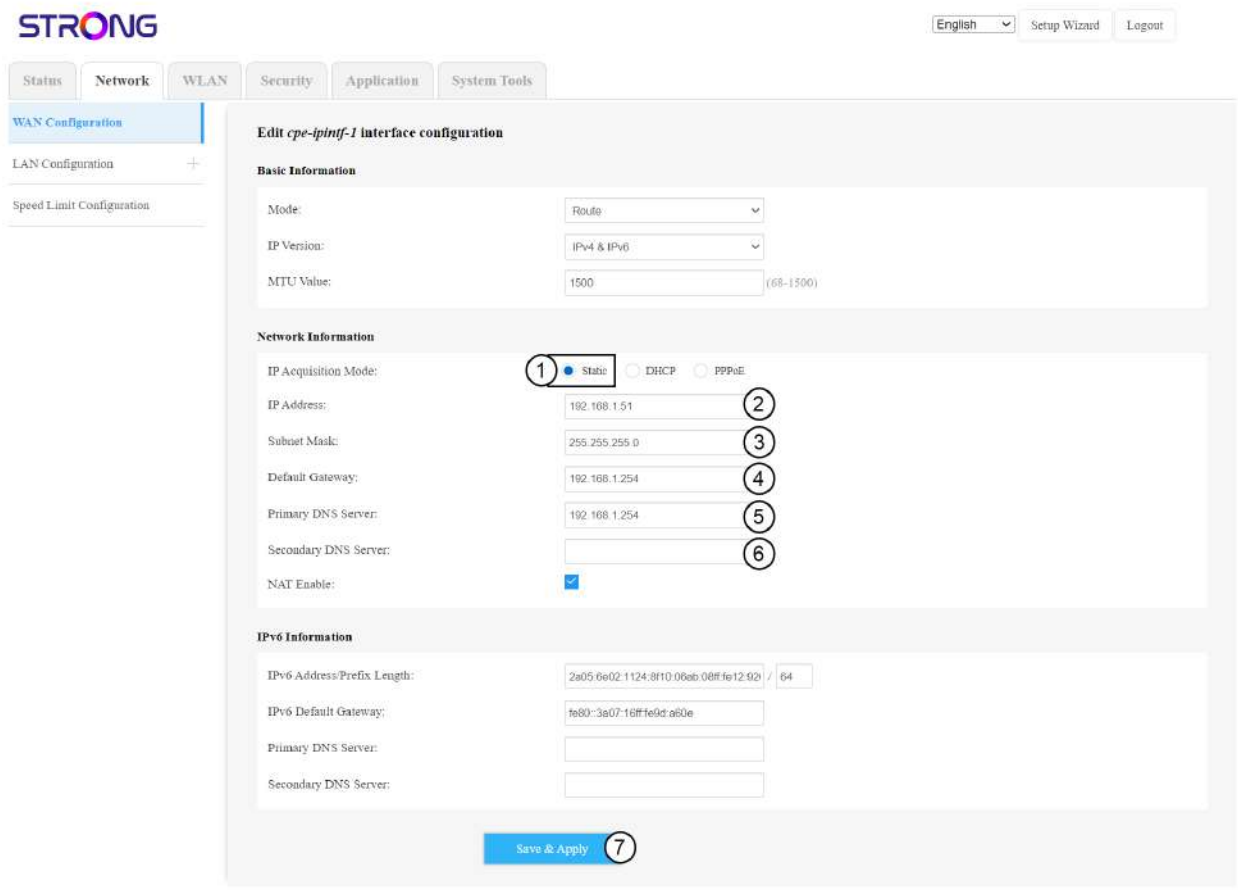
2.1.1. Static

You can configure a Static IP for your mesh units.

1. To do so, click **Network** and **WAN Configuration**.



2. Click **Static**, the mesh units automatically gets the IP Address, Subnet Mask, Default Gateway and Primary DNS Server. Then, click **Save & Apply**.



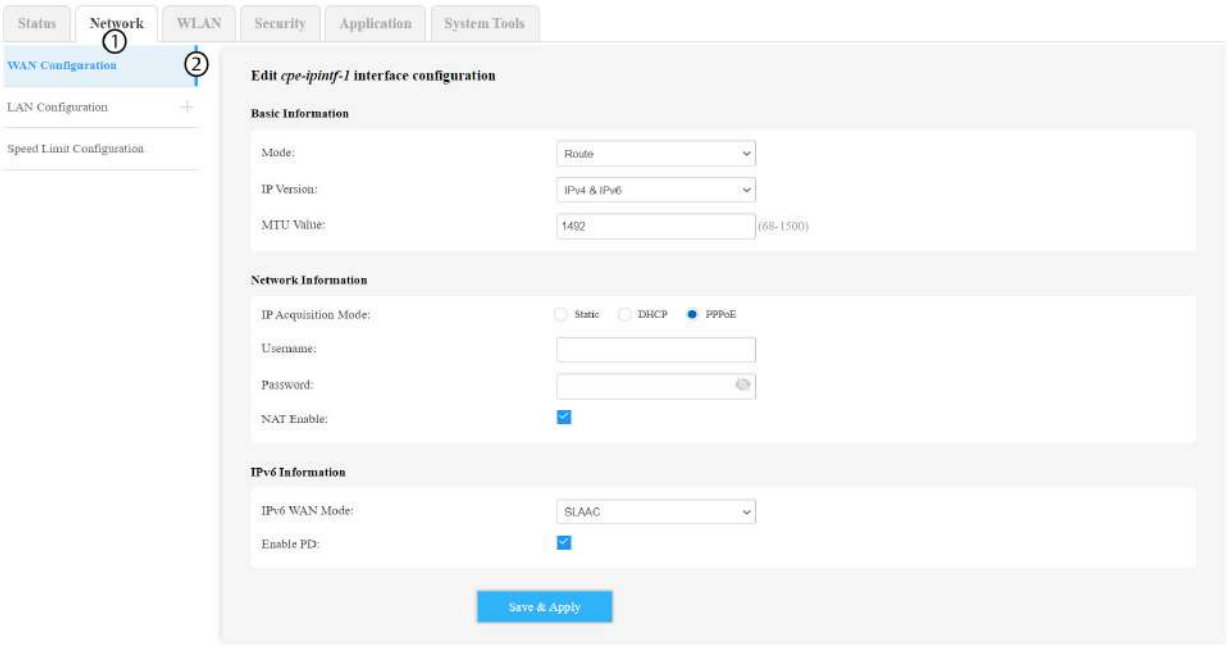
ⓘTIPS: You can set up the mesh controller address to the same IP as the one used to connect to the Web UI. For the mesh agents you can set up a static IP by connecting to the IP address you wrote down.

2.1.2. PPPoE

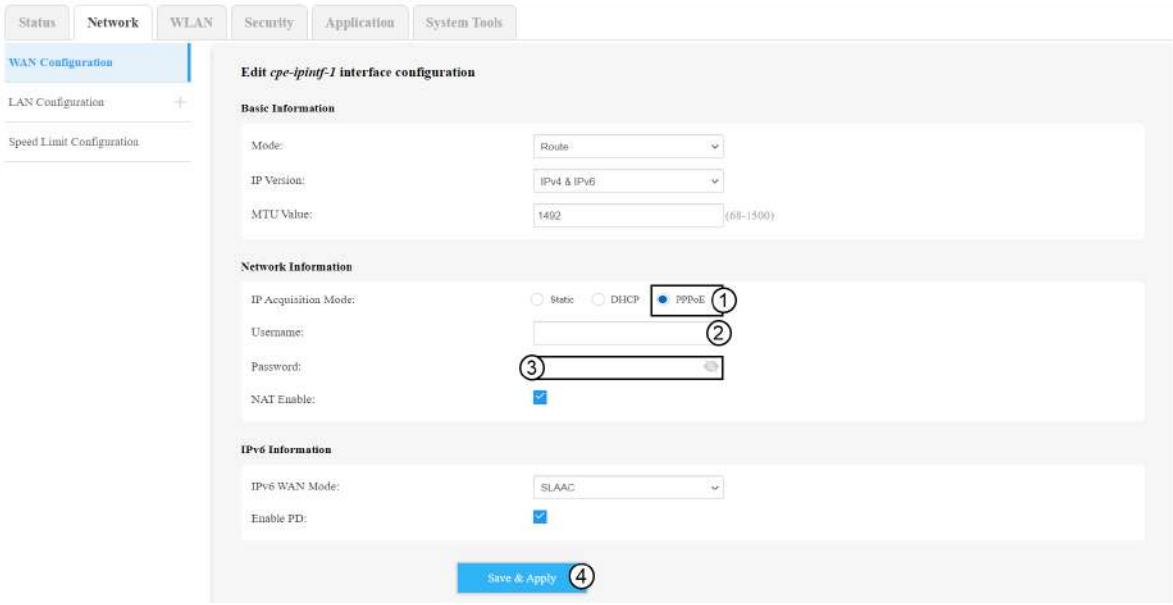
This section enables you to edit the settings of your WAN configuration. By default the WAN configuration is set up to DHCP.

PPPoE (Point to point protocol over Ethernet) can be set up on your mesh network by entering the administration credentials given by your Internet Service Provider. The credentials are the ones used to connect to the administration interface of the modem/router.

1. To do so, click **Network** and **WAN Configuration**.



2. Click **PPoE** and enter the username and password given by your internet service provider to access the administration interface of the router/modem. Then, click **Save & Apply.**



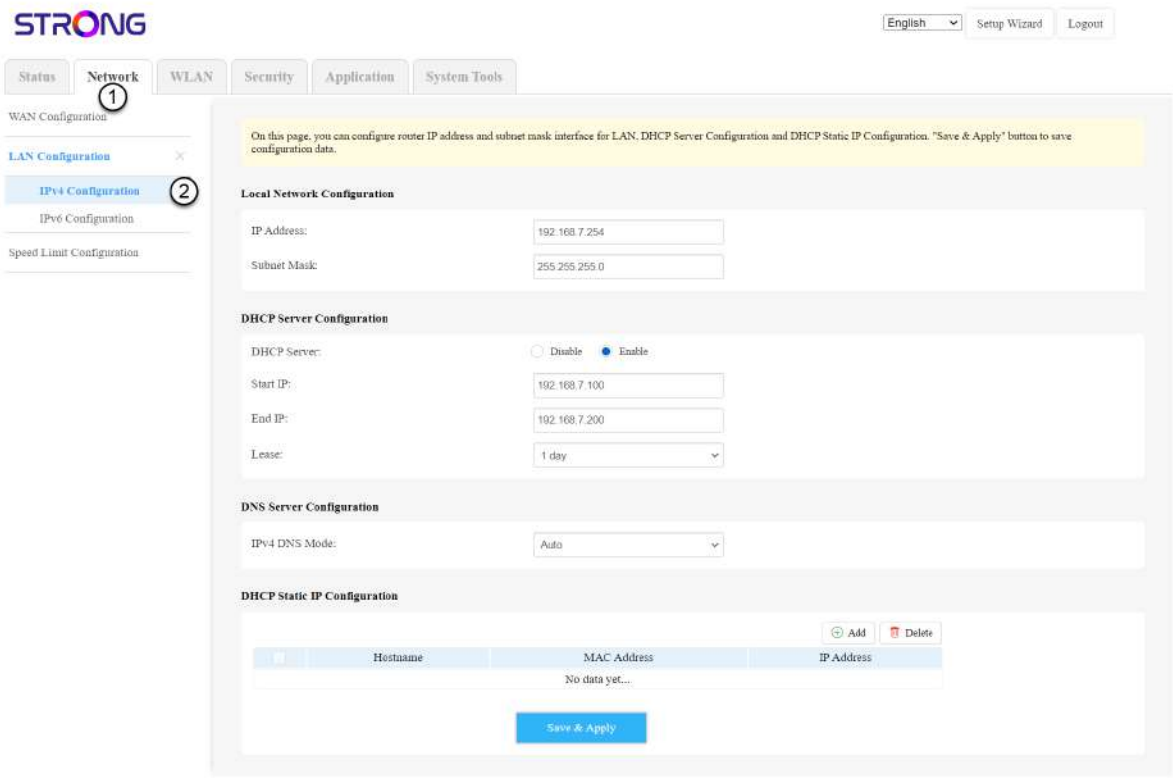
3.

2.2. LAN Configuration

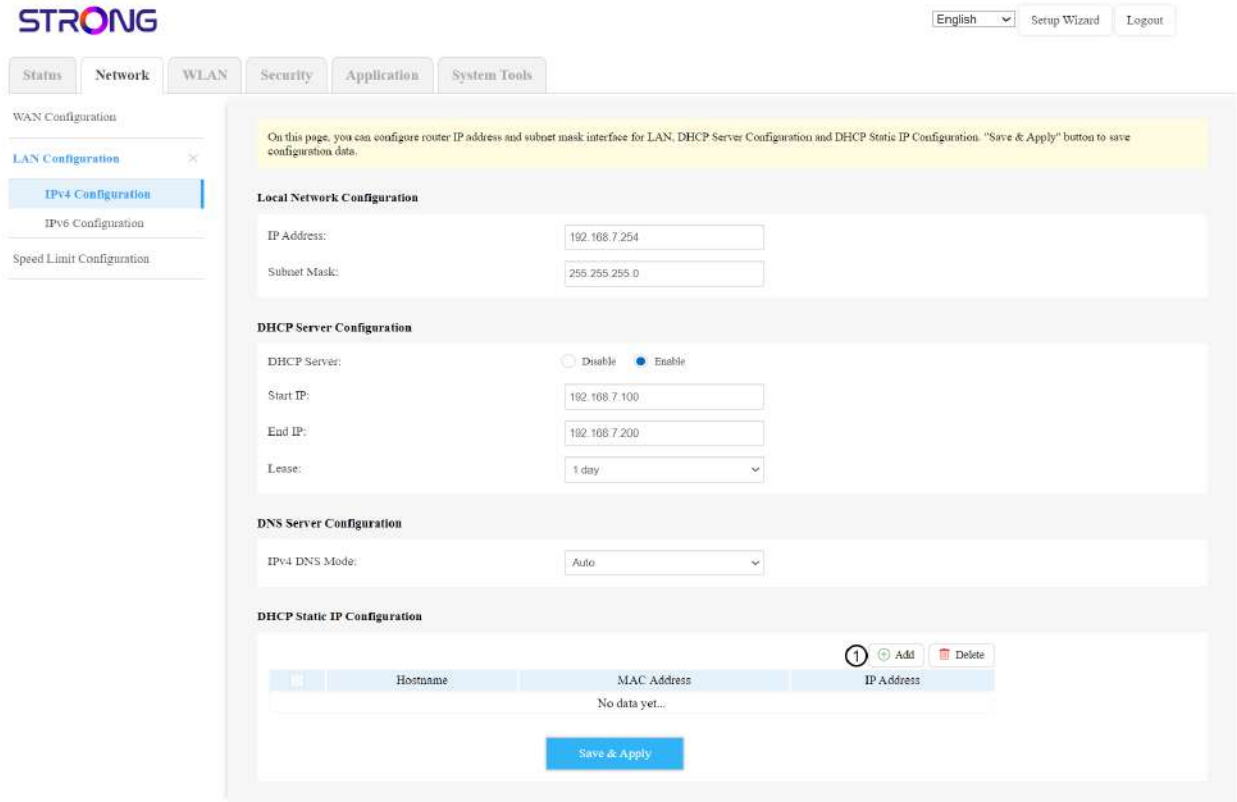
2.2.1. IPv4 Configuration

You can set up a static IP Address for your devices or router.

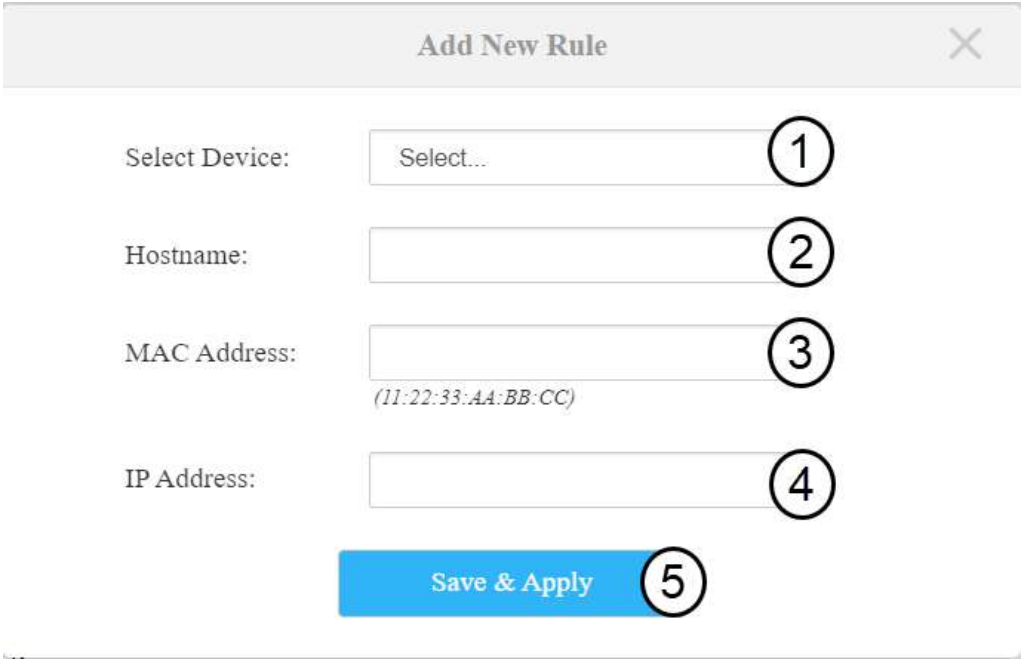
1. To do so, click **Network** and **LAN Configuration.** Then, select **IPV4 Configuration**.



2. In the **DHCP Static Configuration** section, click **Add.**



3. And enter the following information before clicking **Save & Apply**:
    - **Select Device:** Select the device name from the list.
    - **Hostname:** The field is automatically populated with the device name.
    - **MAC Address:** The field is automatically populated with the device IP Address.
    - **IP Address**: A new IP Address is automatically assigned to the device.

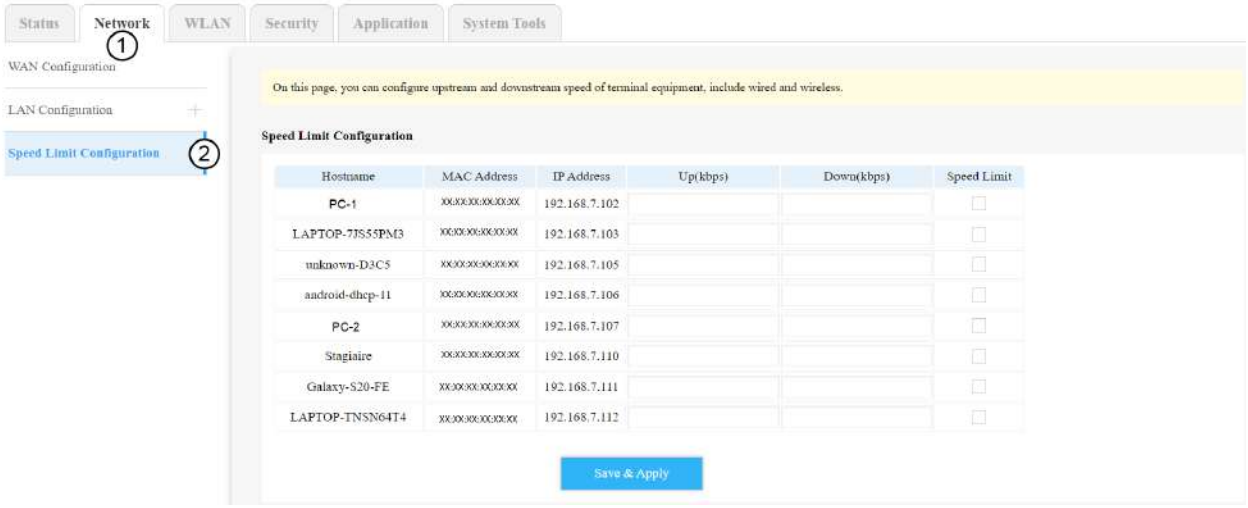


2.2.2. IPv6 Configuration

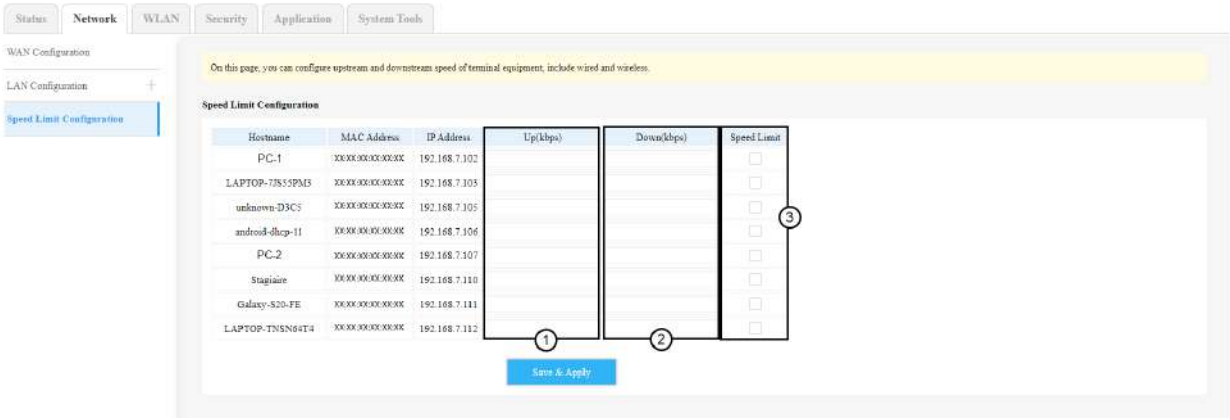
2.3. Speed Limit Configuration

You can set up the speed limit for the different devices connected to your network.

1. To do so, click **Network** and **Speed Limit Configuration**.



2. Enter the following information before clicking **Save & Apply**:
    - **Up (Kbps):** Enter the maximum up speed limit.
    - **Down (Kbps):** Enter the maximum down speed limit.
    - **Speed Limit:** Check the box to activate the rule.



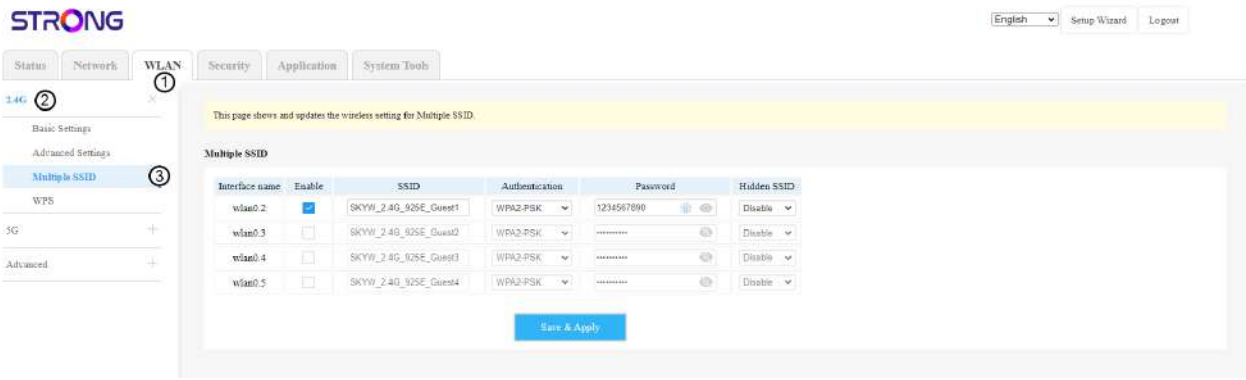
3. WLAN

3.1. 2.4 G

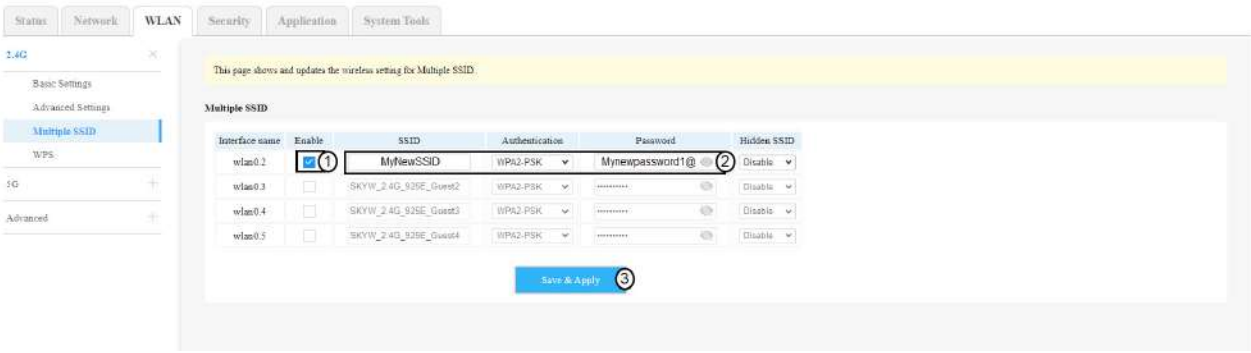
3.1.1. Multiple SSID

You can use this setting if you need to have several SSIDs on your network.

1. To do so, click **WLAN, 2.4G** and **Multiple SSID.**



2. Check the **enable** box next to the name of the SSID that you want to activate. Then, enter a New **SSID** and **Password** (click the eye icon to display the password) and click **Save & Apply**.

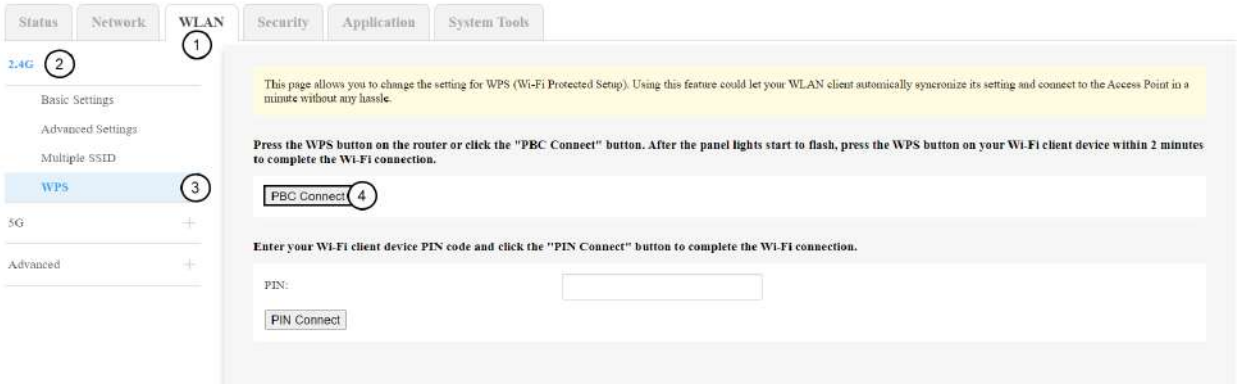


3. Write down the new network information on a piece of paper.

3.1.2. WPS

You can set up the WPS connection method that you want to use. We advise to use the PBC method, once you clicked the button in the UI your devices can connect automatically (Computers).

1. To do so, click **WLAN, 2.4G** and **WPS.** Then click the **PBC Connect** button.



2. When the WPS is activated the WPS starts blinking.

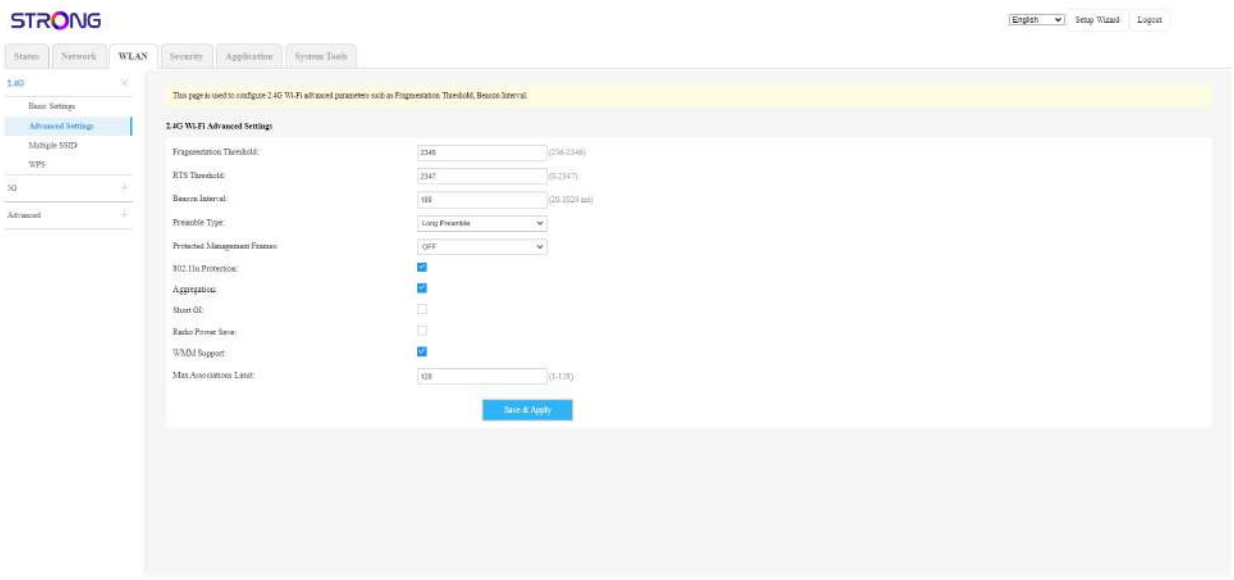
WPS Blinking: TWPS is on. The WPS pairing is ongoing, wait until the end of the procedure.

3. In your device settings, select the Wi-Fi network and press the connect button.

3.1.3. Advanced Settings

You can edit the settings such as Beacon Interval, RTS Treshold and so on..

⚠ WARNING: If you edit the settings without having suffiicient knowledge it can prevent your device from working properLy. We highly discourage changing the parameters.

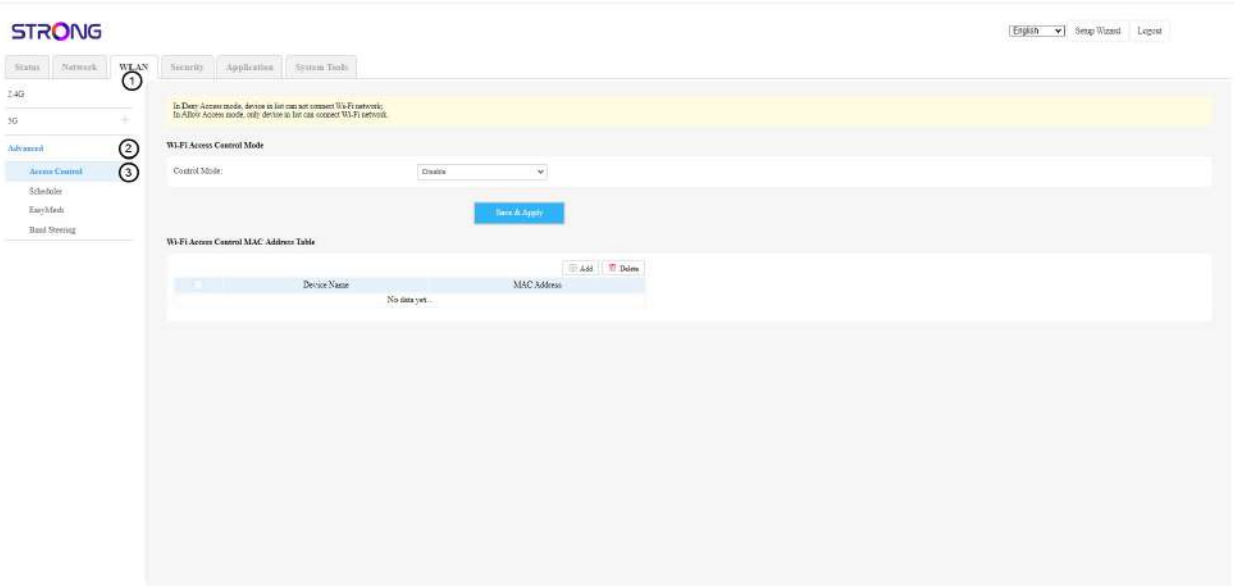


3.2. Advanced

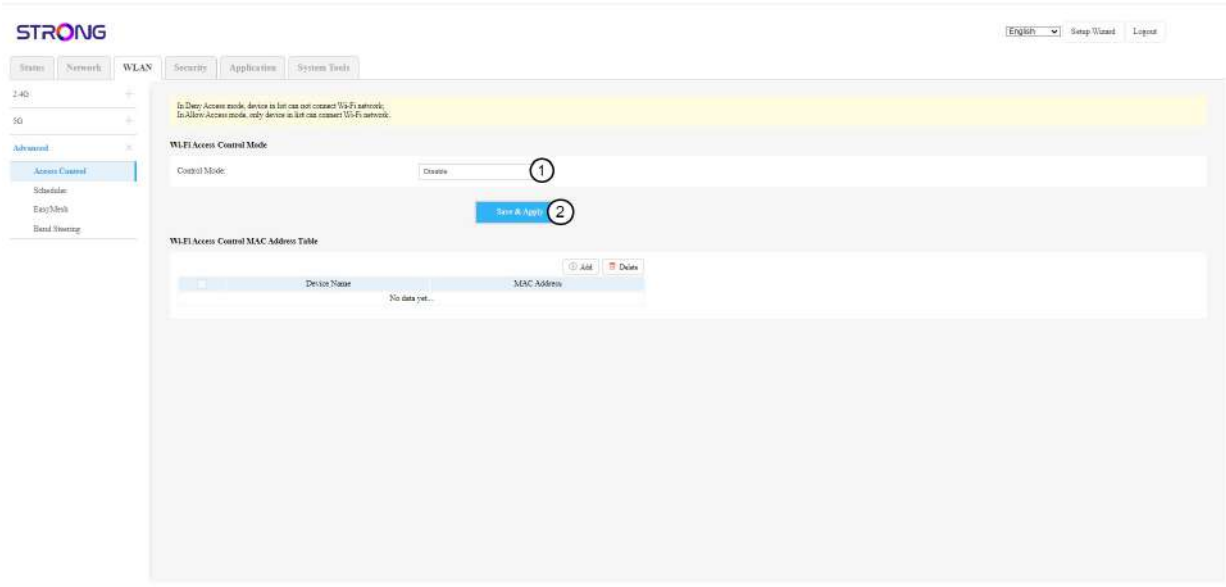
3.2.1. Access Control

You can set up the MAC Addresses of the devices that are allowed to connect to your Wi-Fi Network.

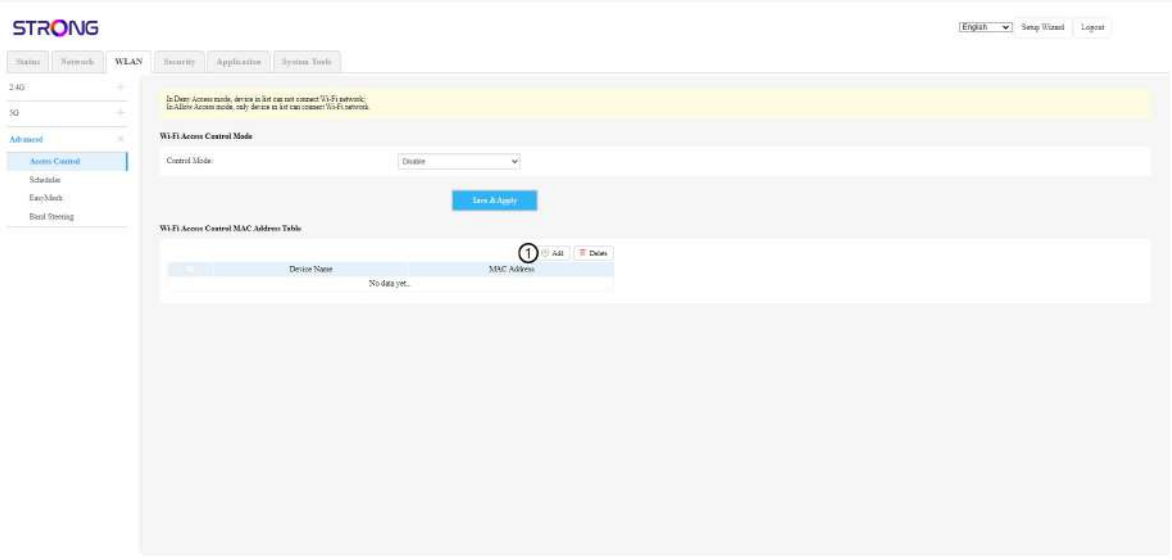
1. To configure the access control, click **WLAN** and **Advanced**. Then select **Access Control.**



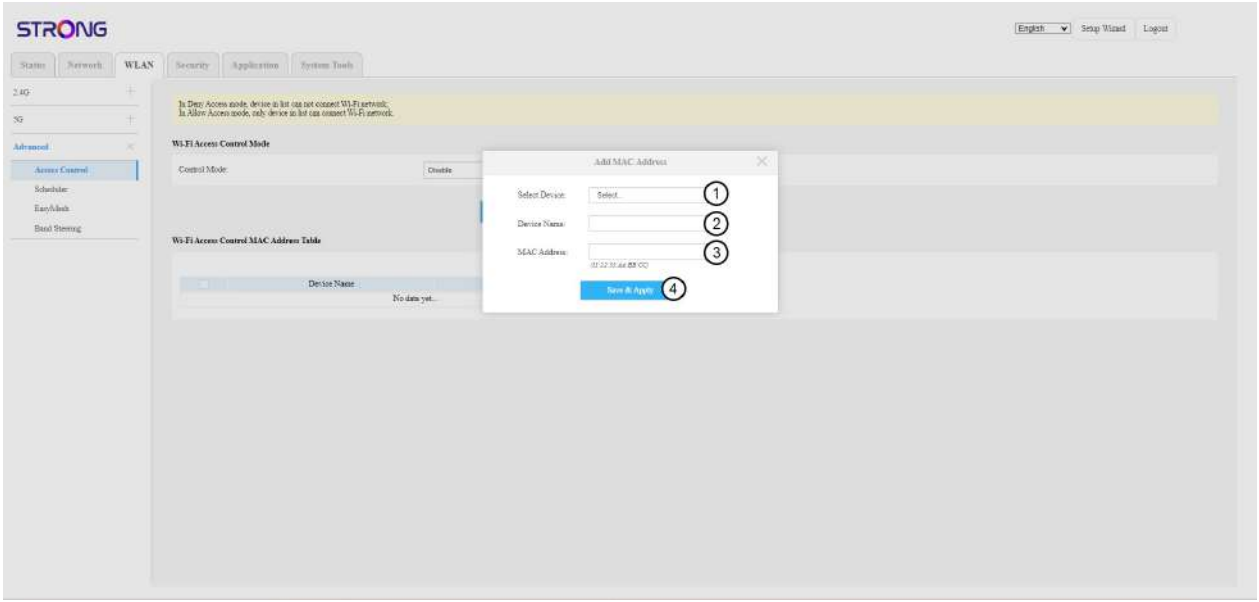
2. In the **Control Mode** drop down list, select a value between **Allow Access** and **Deny Access.** Then, click **Save & Apply**.



3. Click **Add**



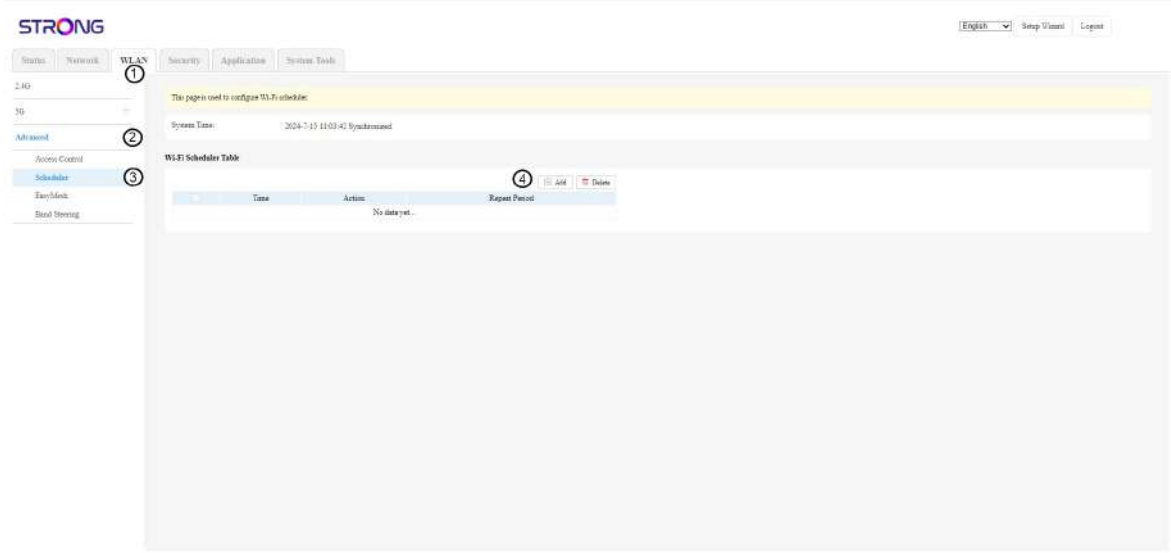
4. Enter the following information before clicking **Save & Apply**:
    - **Select Device: Select** the name of the device in the list
    - **Device Name:** The field is automatically populated with the device name.
    - **MAC Address:** The field is automatically populated with the Mac Address of the device.



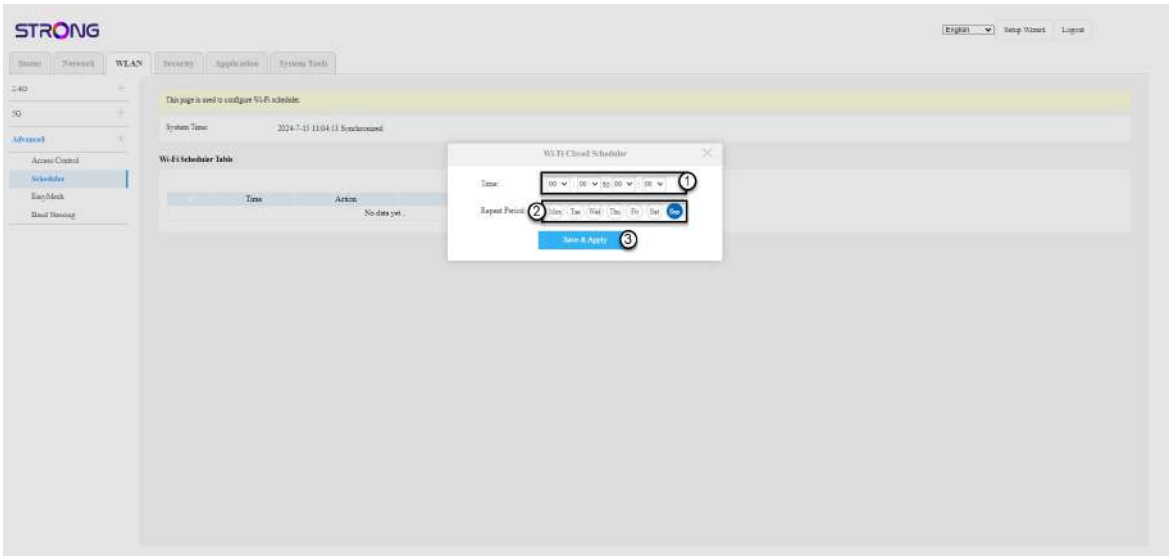
3.2.2. Scheduler

You can set up the day and times to stop the router automatically.

1. Click **WLAN** and **Advanced**. Then, select **Scheduler** and click **Add.**



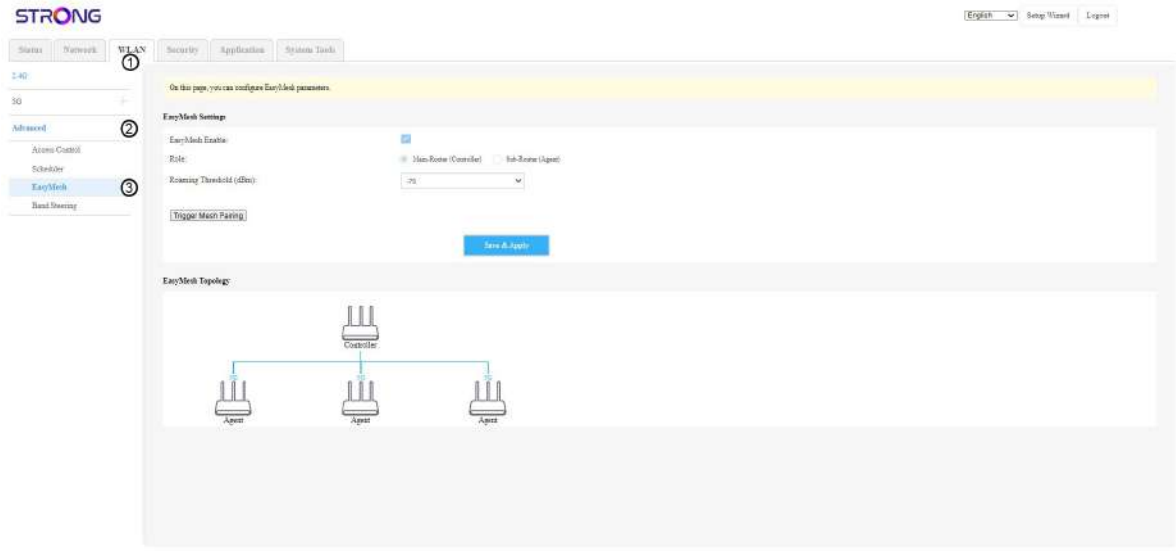
2. Select the days and times when you want to switch off the router and click **Save & Apply**.



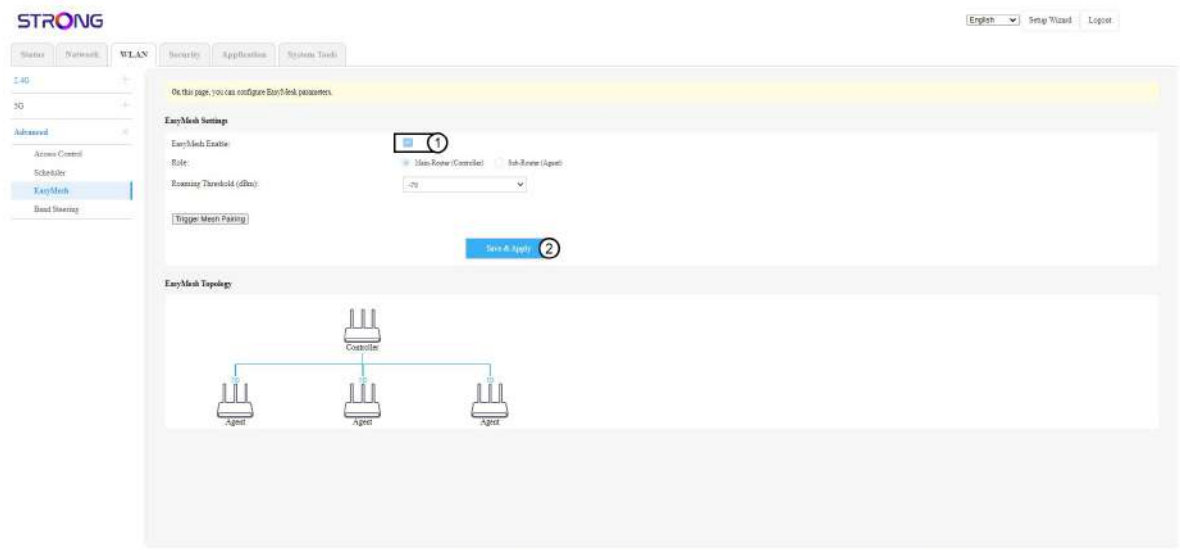
3.2.3. Easy Mesh

This parameter enables you to connect mesh of different brands together in a same network if they are also set up with this option.

1. To do so, click **WLAN** and **Advanced**. Then select, **Easy Mesh**.



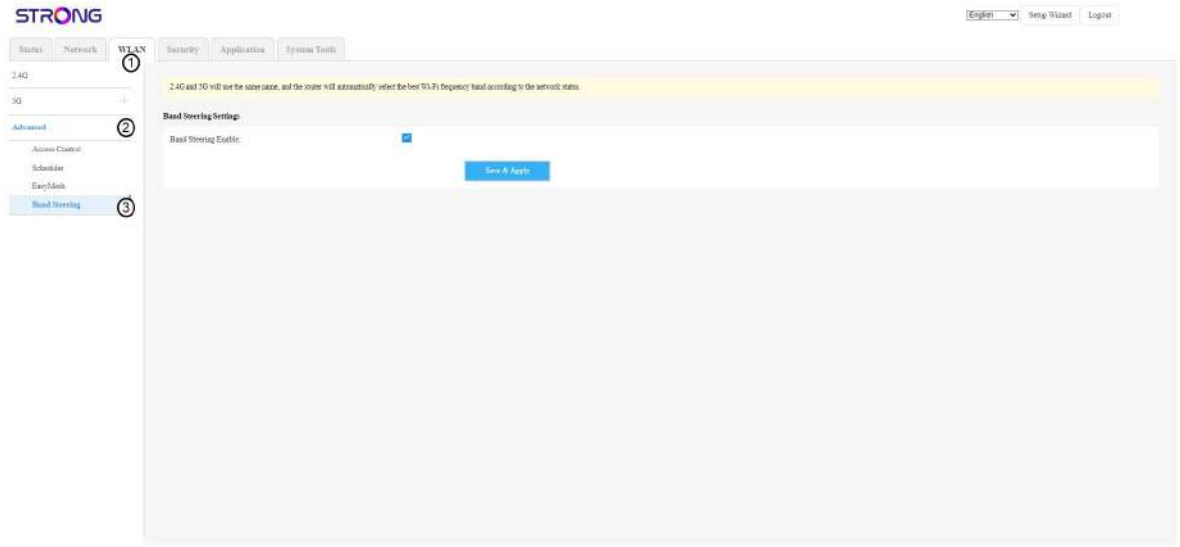
2. Uncheck the **Enable** box and click **Save & Apply**.



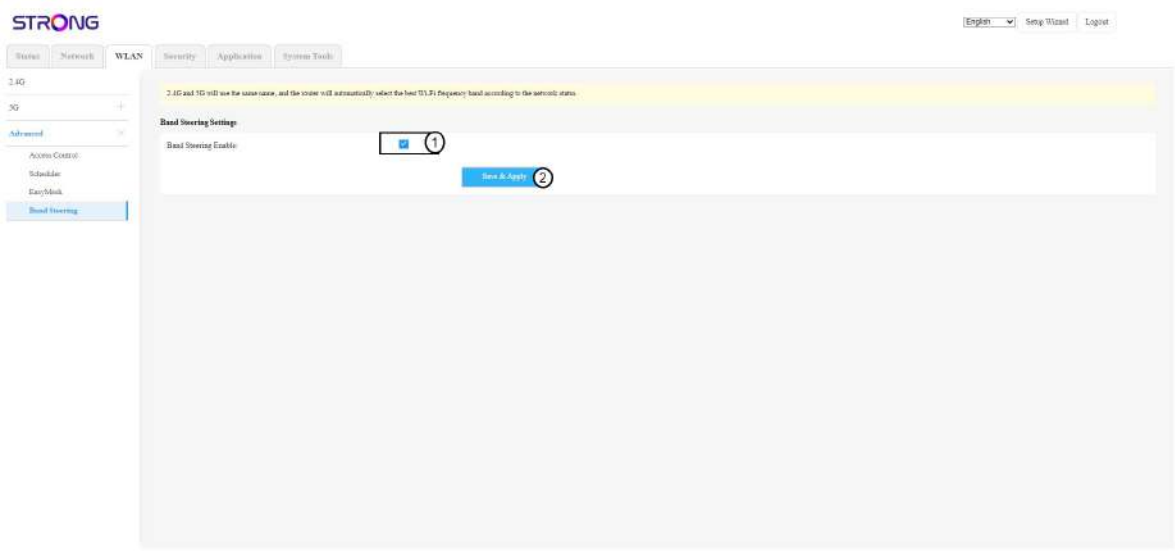
3.2.4. Band Steering

You can deactivate this parameter if you need your 2.4 GHz and 5 GHz Wi-Fi Networks to be separated. By default, our router 2.4 and 5G networks are not separated.

1. To do so, click **WLAN** and **Advanced**. Then select, **Band Steering**.



2. Uncheck the **Enable** box and click **Save & Apply**.



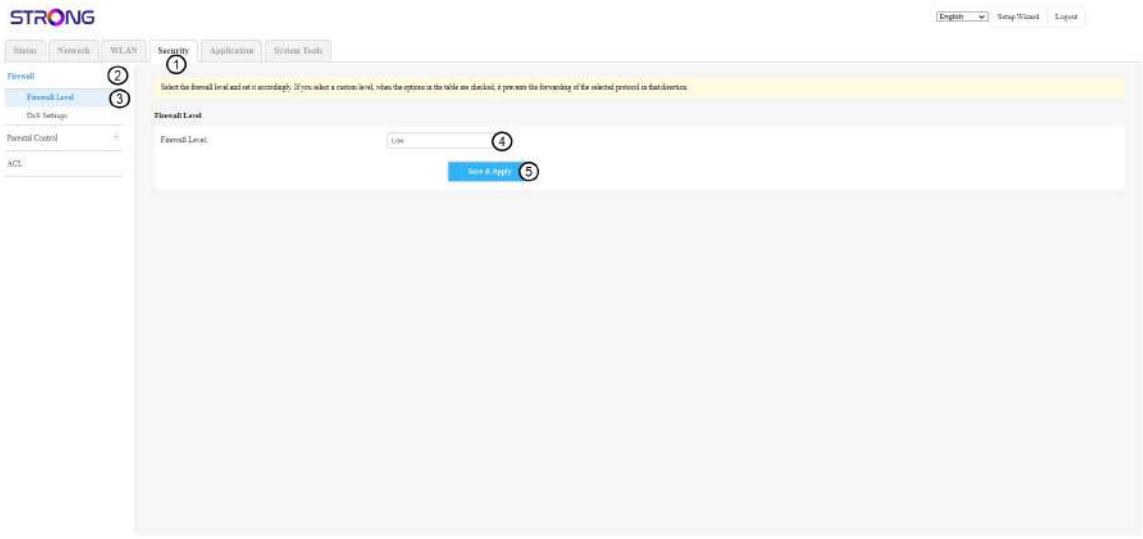
4. Security

4.1. Firewall Settings

4.1.1. Firewall Level

You can choose the security level for the firewall of the router

1. To do so, click **Security** and **Firewall Level**. Then, select the appropriate value in the **Firewall Level** drop down list and click **Save & Apply**.



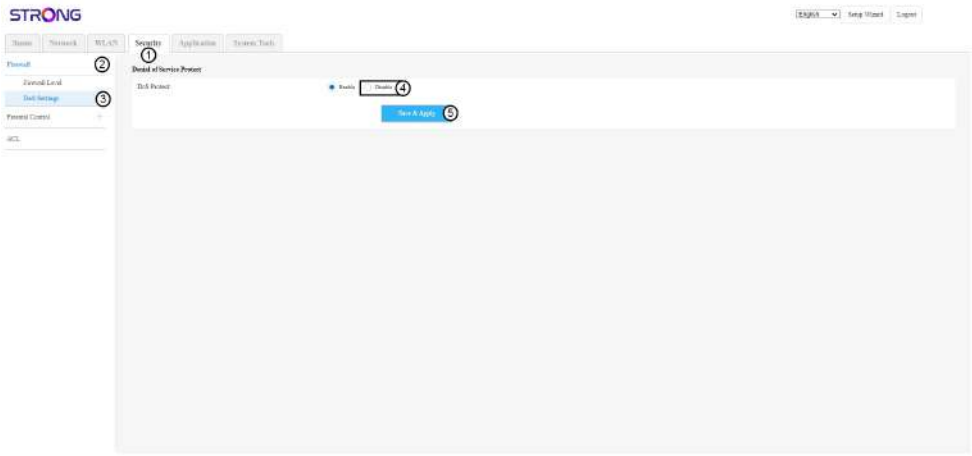
4.1.2. DoS Settings

Denial of Service (DoS) protection is a setting used to prevent cyber-attacks on your network that makes your resources and services unavailable.

You can deactivate this setting that is enabled by default in the mesh unit.

⚠ WARNING: It is not recommended to deactivate it because it can make your router vulnerable to DoS attacks.

1. To do so, click **Security**, **Firewall** and **DoS Settings**. Then, click **Disable** and **Save & Apply**



4.2. Parental Control

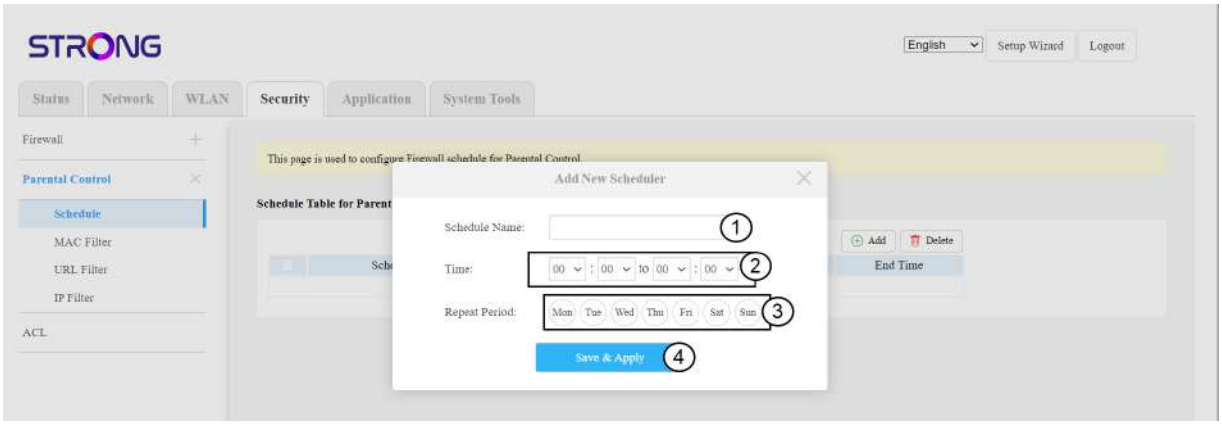
4.2.1. Schedule

You can schedule when the parental control is activated (day and time).

1. To do so, click **Security** and **Parental Control**. Then, select **Schedule** and **Add.**

2. Enter the following information before clicking **Save & Apply:**

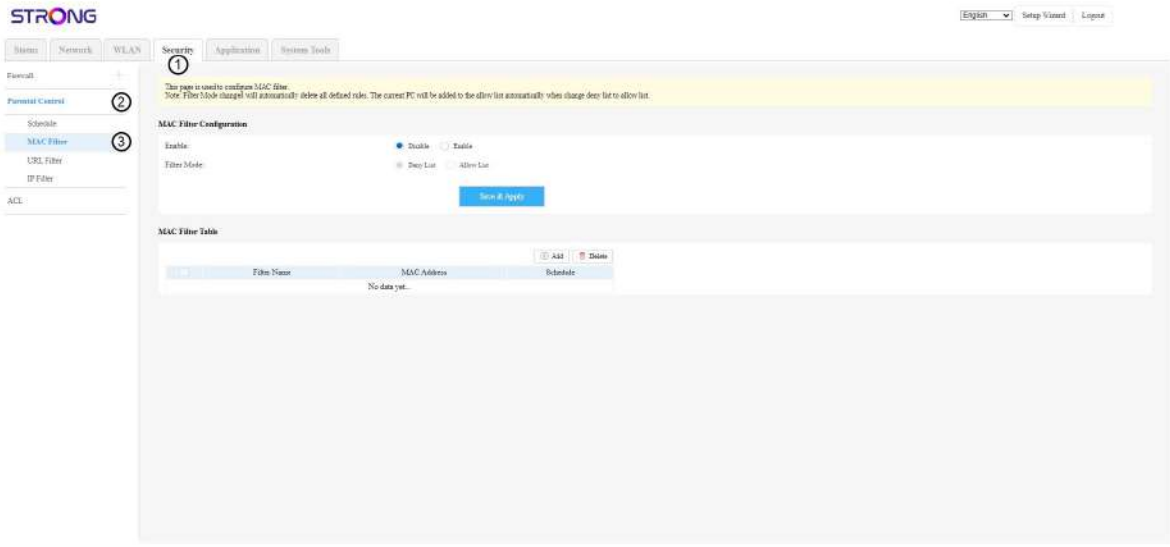
- **Schedule Name:** Enter a name for your scheduling rule
- **Time:** Enter the time period during which the parental control must be activated.
- **Repeat Period:** Select the days when the router must switch on parental control.



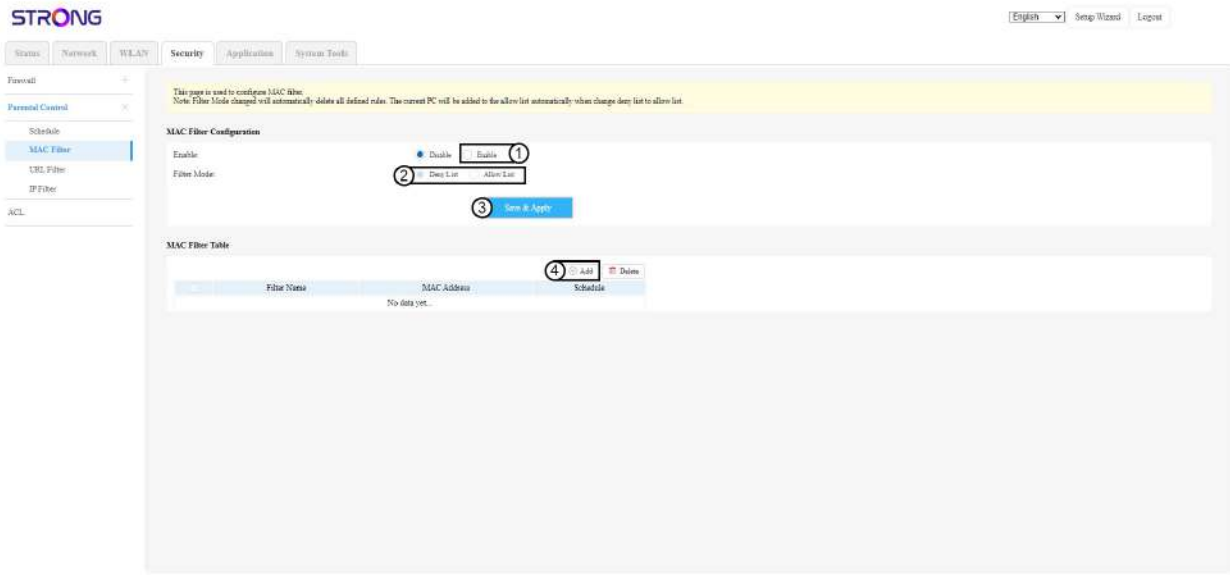
4.2.2. Mac Filter

You can configure a list of devices that are allowed or denied to use the Wi-Fi network.

1. To do so, click **Security** and **Parental Control**. Then, select **MAC Filter.**

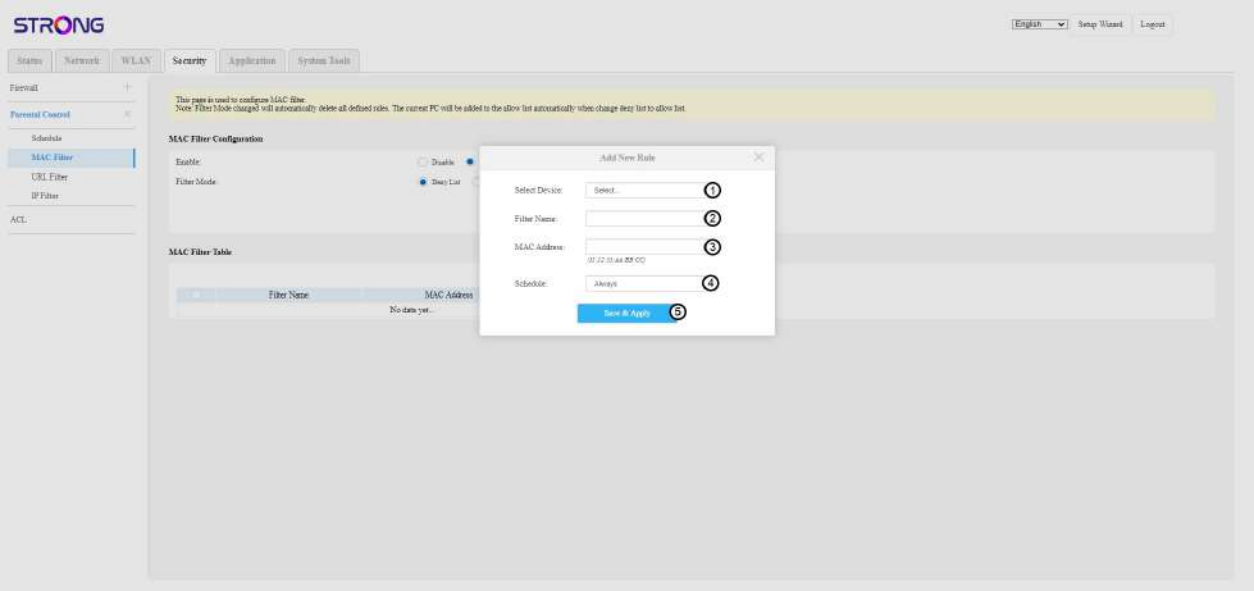


2. Click the **Enable** and **Save & Apply. Then,** elect the **Filter Mode** between **Deny List** and **Allow List**, before clicking **Add.**



3. Enter the following information before clicking **Save & Apply:**

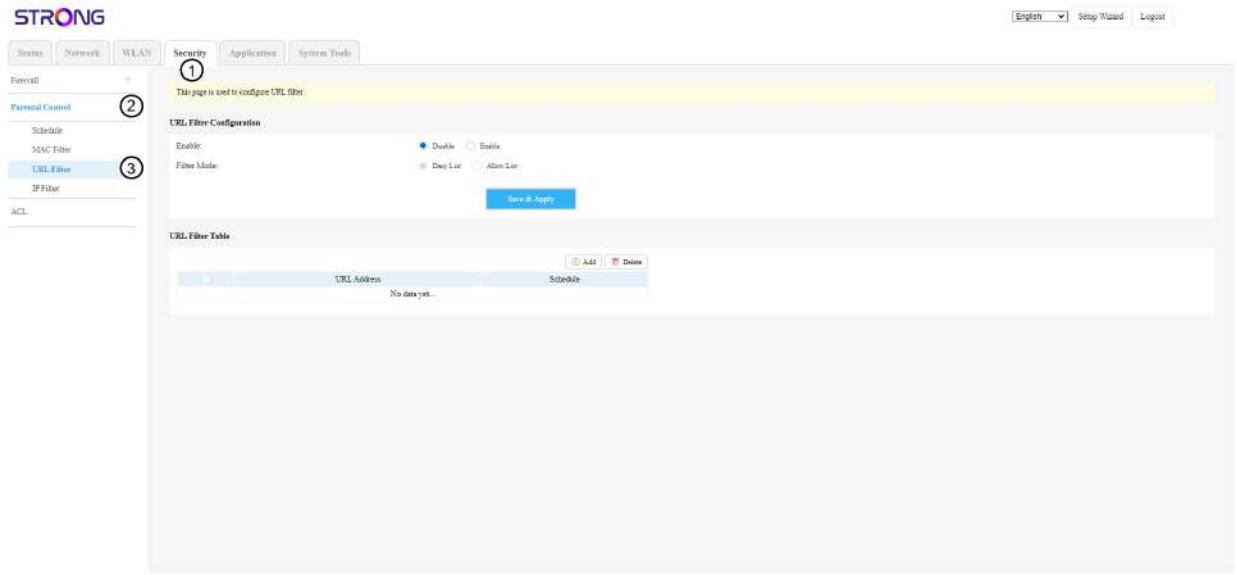
- **Select Device:** Select your device from the drop-down list.
- **Filter Name:** The field is automatically populated with the Device Name.
- **MAC Address:** The field is automatically populated with the MAC Address of the device.



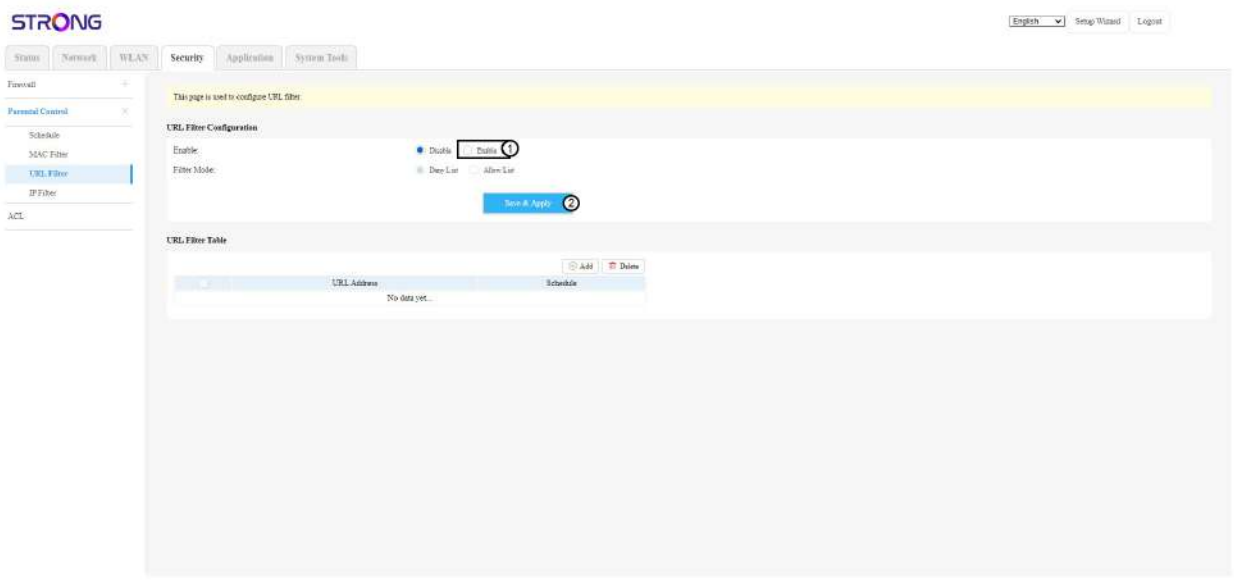
4.2.3. URL Filter

You can set up a list of allowed or denied websites.

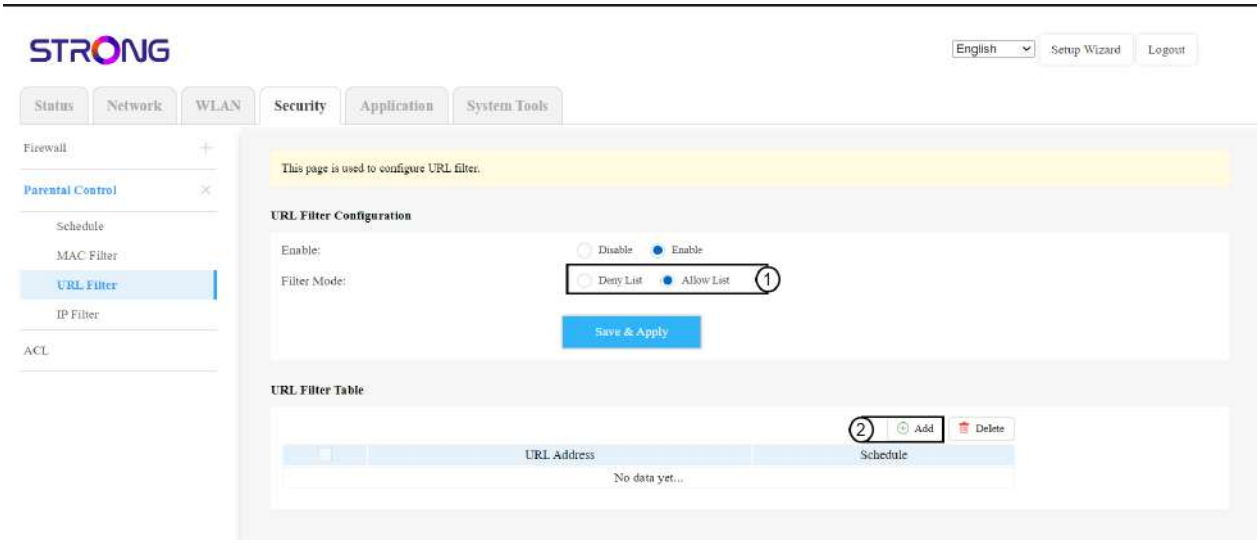
1. To do so, click **Security** and **Parental Control**. Then, select **URL Filter.**



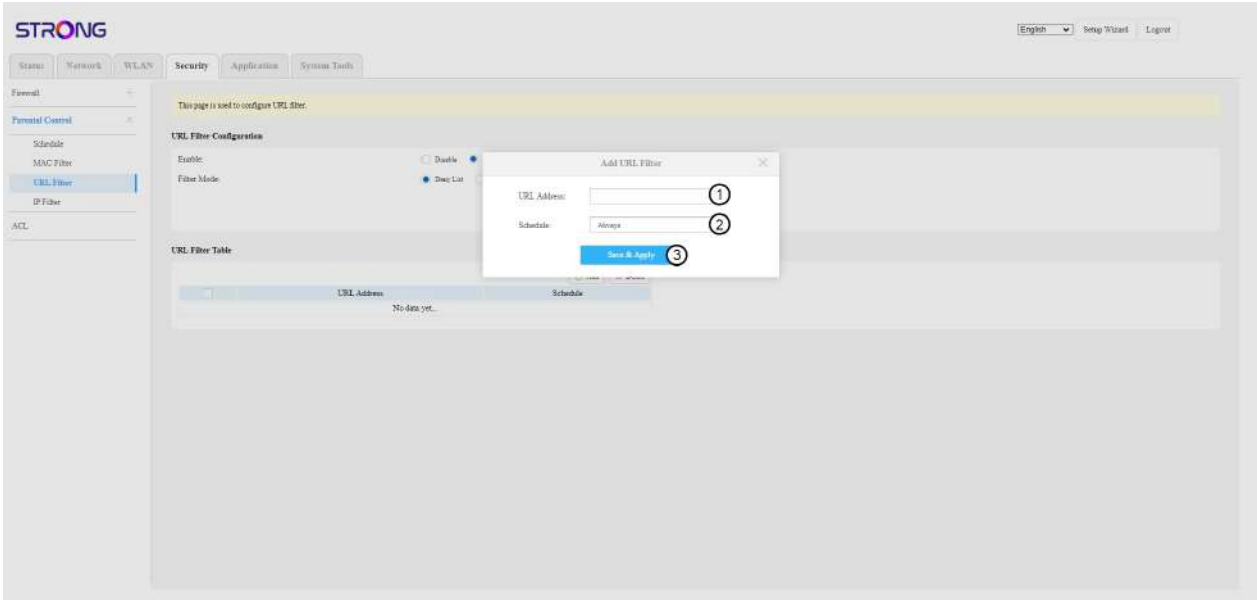
2. Click the **Enable** and **Save & Apply.**



3. Then, select the **Filter Mode** between **Deny List** and **Allow List**, before clicking **Add.**



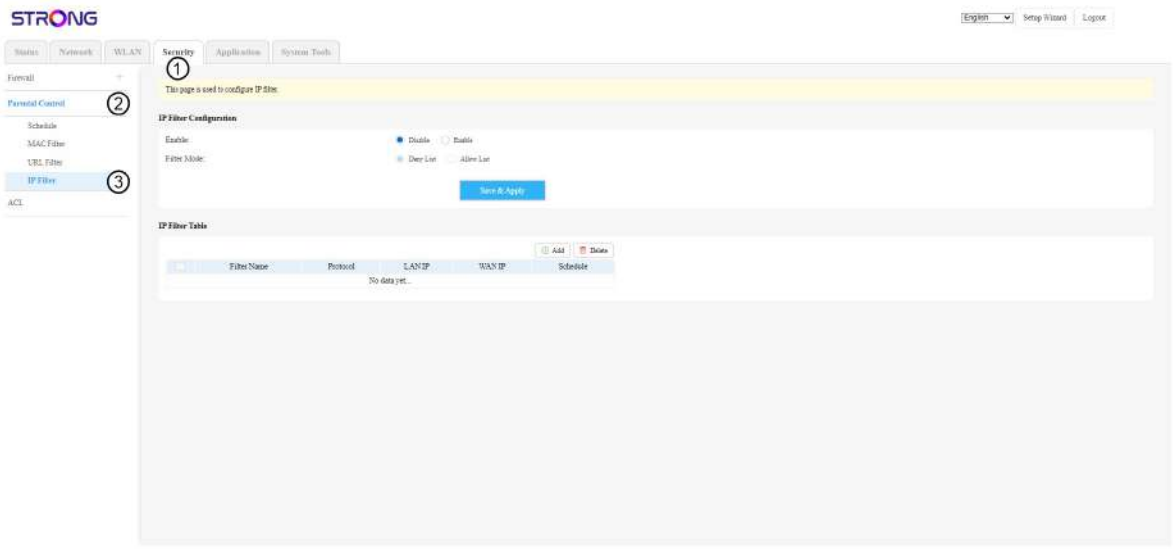
4. Enter the following information before clicking **Save & Apply:**
   - **URL Address:** Enter the URL of the website that you want to allow or block.
   - **Schedule:** Select a value for the scheduling rule.



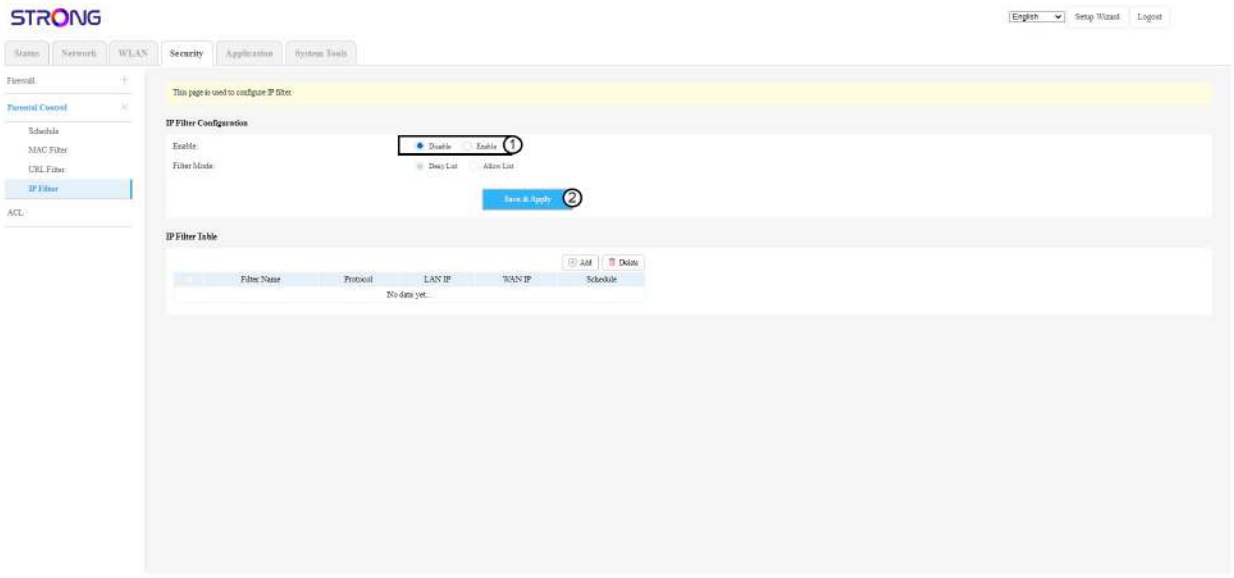
4.2.4. IP Filter

This section enables you to configure IP Filters for you WAN and LAN connection.

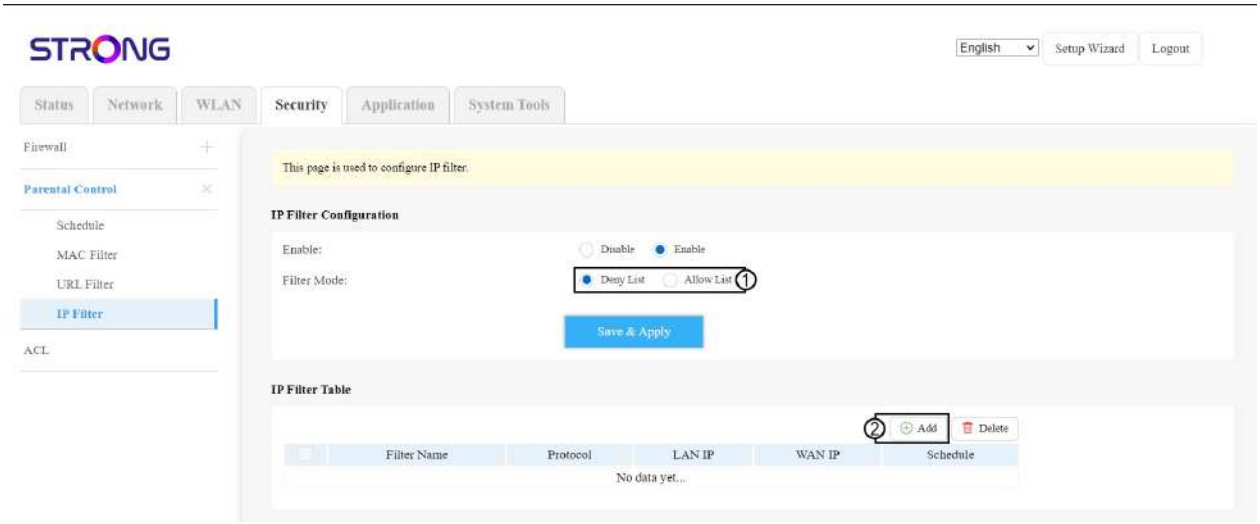
1. To do so, click **Security** and **Parental Control**. Then, select **IP Filter.**



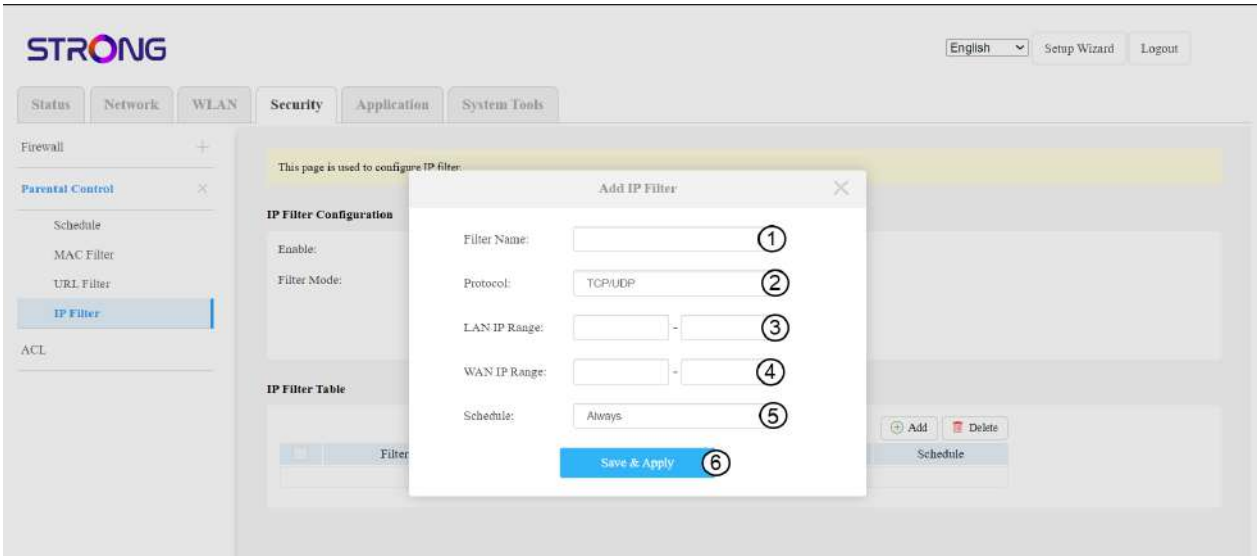
2. Click the **Enable** and **Save & Apply.**



3. Then, select the **Filter Mode** between **Deny List** and **Allow List**, before clicking **Add.**



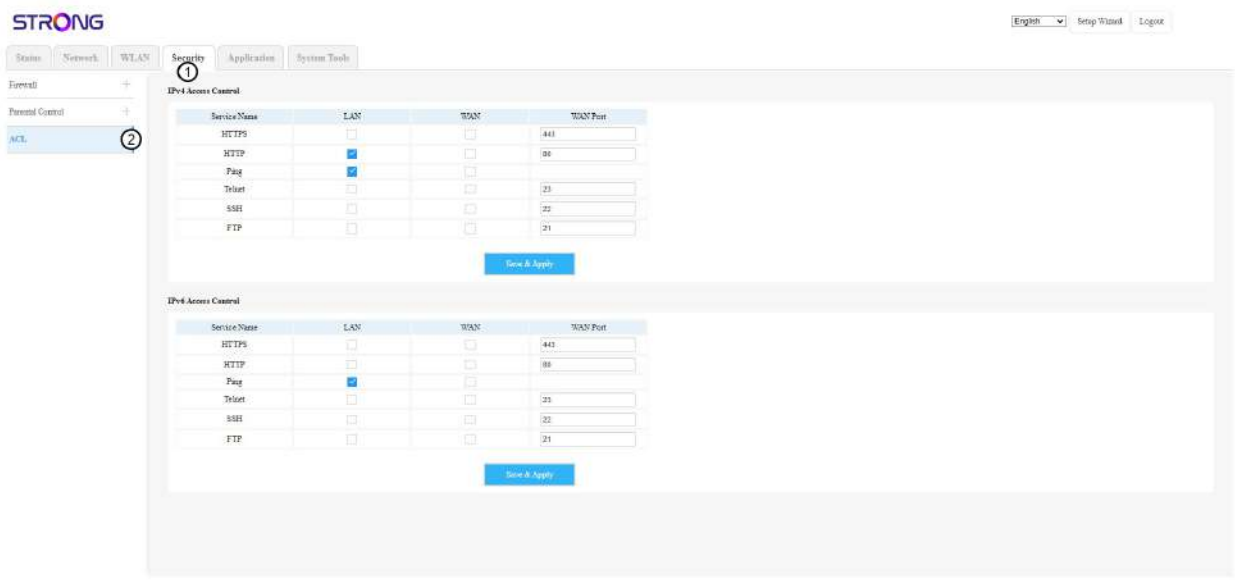
4. Enter the following information before clicking **Save & Apply** :
    - **Filter Name**: Enter a name for the filter .
    - **Protocol:** Select the type of protocol for the filter.
    - **LAN IP Range :** Enter the LAN IP pool.
    - **WAN IP Range :** Enter the LAN IP pool.



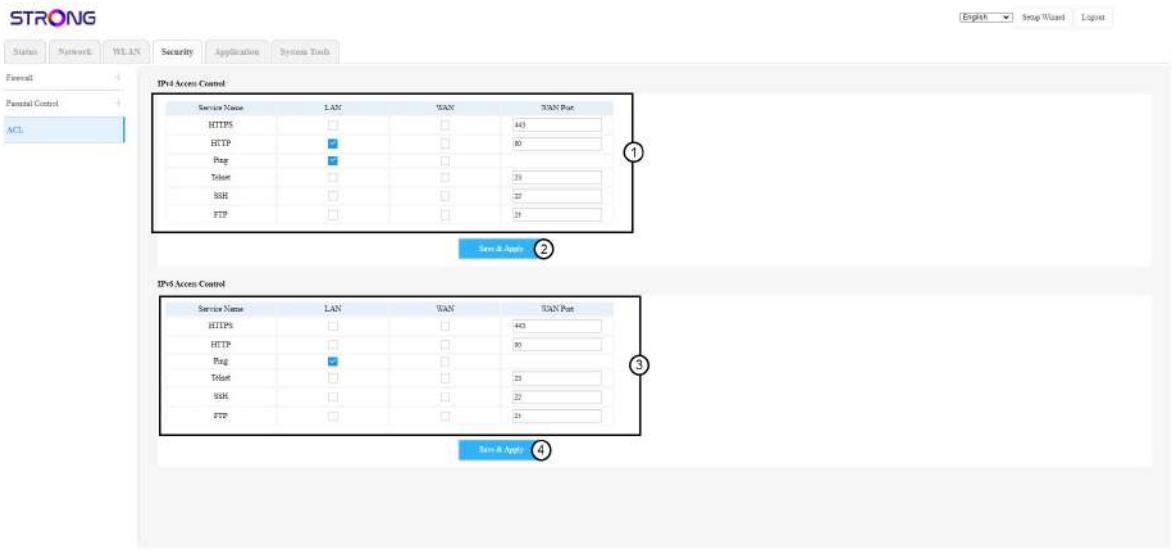
4.3. ACL

You can set up the parameters to define which IPv4 and IPv6 access types are allowed.

1. To do so, click **Security** and **ACL.**



2. Check the boxes of the authorized protocols for your **WAN** and **LAN** networks for IPv6 & IPv4 configuration and click **Save & Apply.**



5. Application

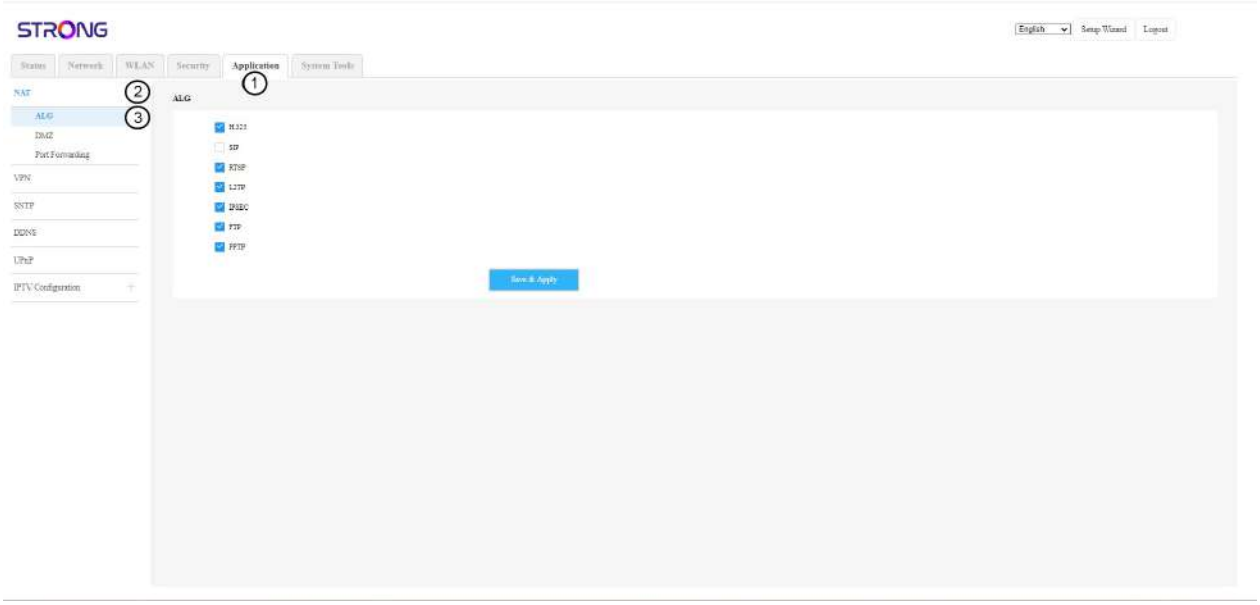
In the Application Settings section of the UI, you can set different basic parameters regarding your network and advanced parameters according to your needs.

5.1. NAT

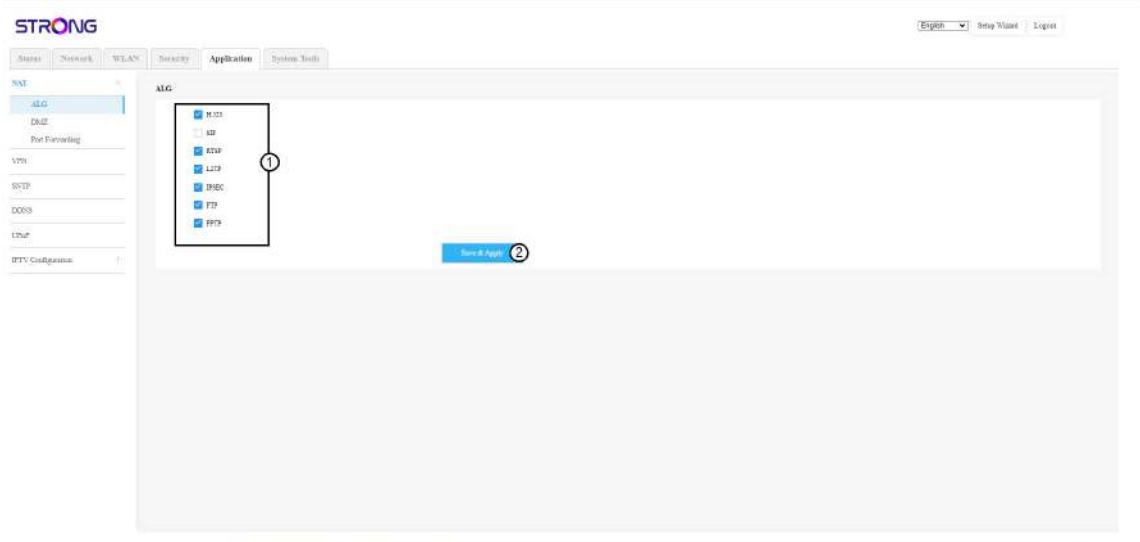
5.1.1. ALG

Application Layer Gateway (ALG) is protocol that is used to control the authorisation or deny of traffic to a specific application of a server it is mainly used for SIP or FTP.

1. To configure the allowed protocols, click **Application** and **NAT**. Then, select **ALG**.



2. Select the values for the protocol that you want to allow and click **Save & Apply**



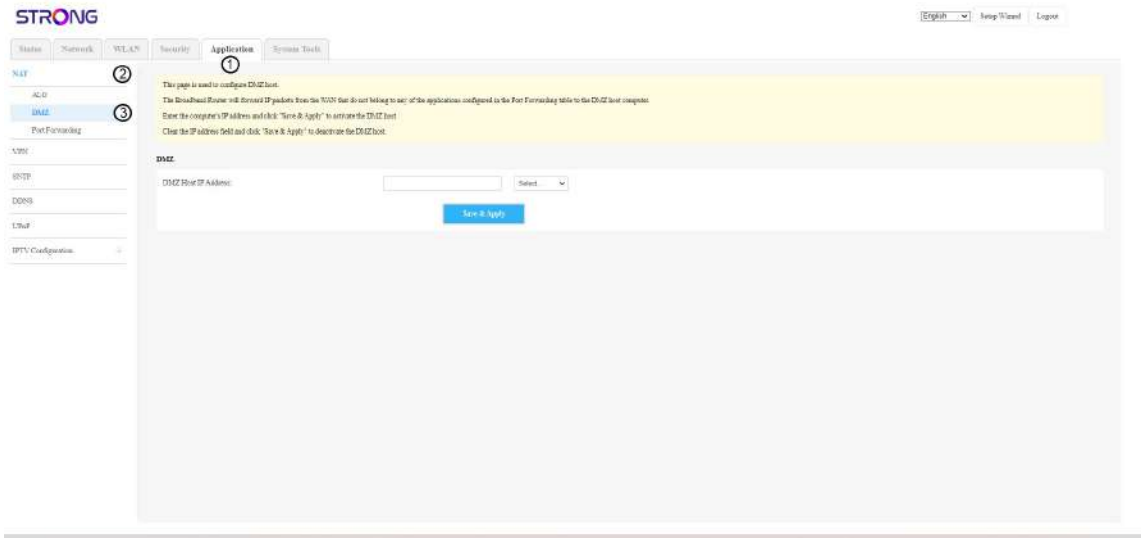
5.1.2. DMZ

A Demilitarized Zone (DMZ) is a subnetwork that is separated and isolated from the main local network (LAN) and from Internet by a Firewall. On this network, you can configure the devices that needed to access the Internet without accessing your LAN.

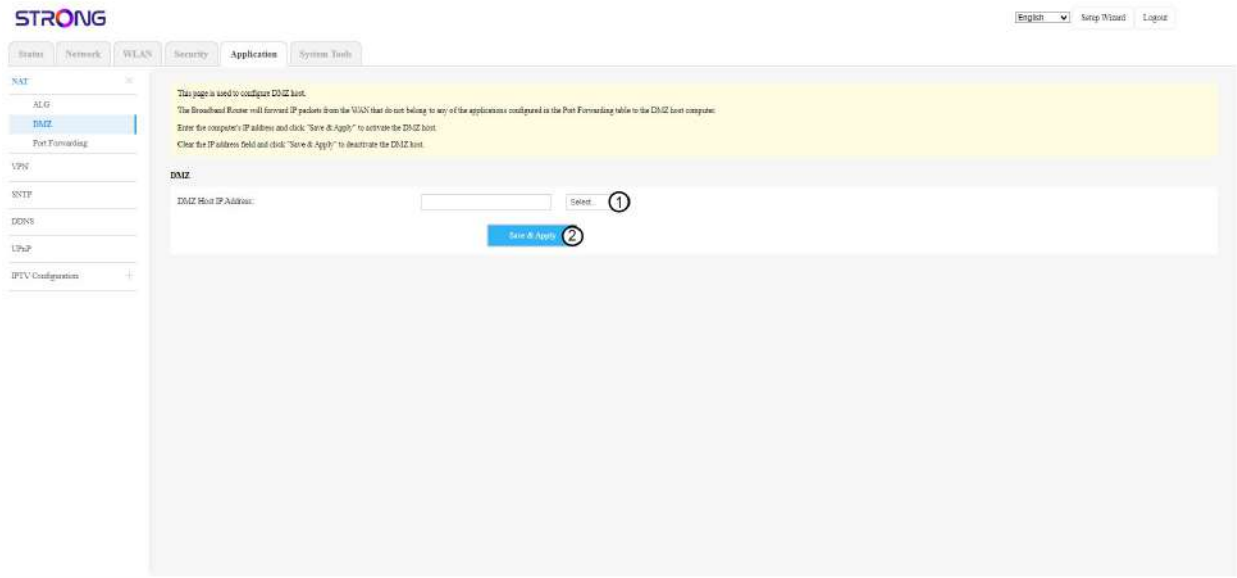
1. To configure DMZ on your router, you must be connected to the Wi-Fi of the router and access the Web UI. Please refer to the following procedures to connect to Web UI:

- Connecting to the Wi-Fi and Accessing the Web UI

2. Click **Application** in the top bar, then the **NAT** section and **DMZ.**



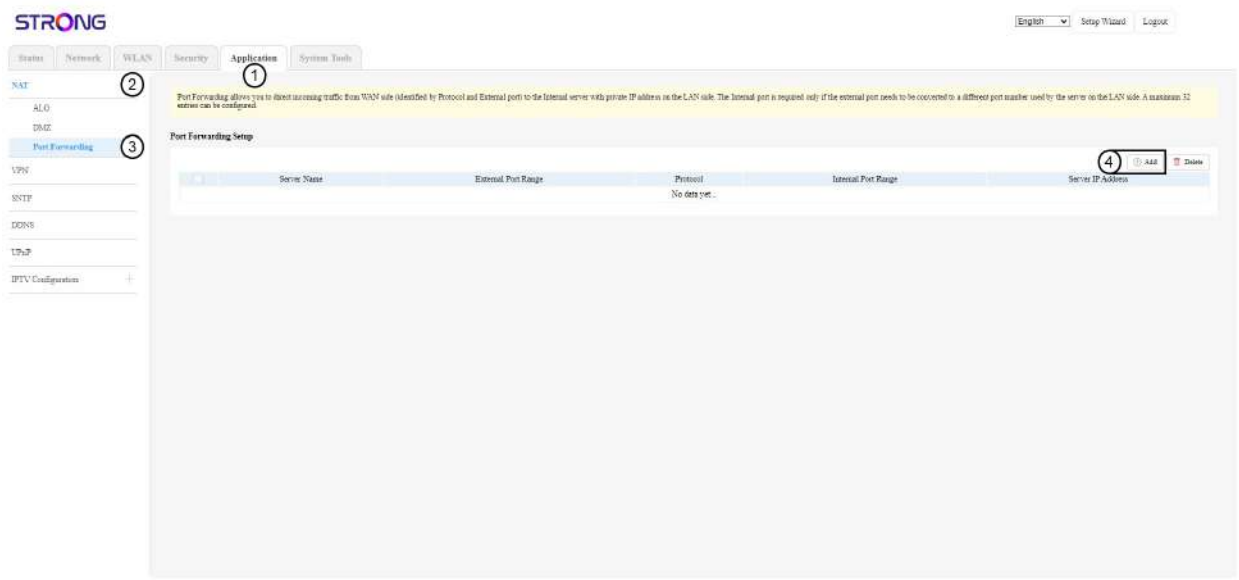
3. Enter the IP Address of your device, you can select the settings with the Select Option and click on **Save & Apply**.



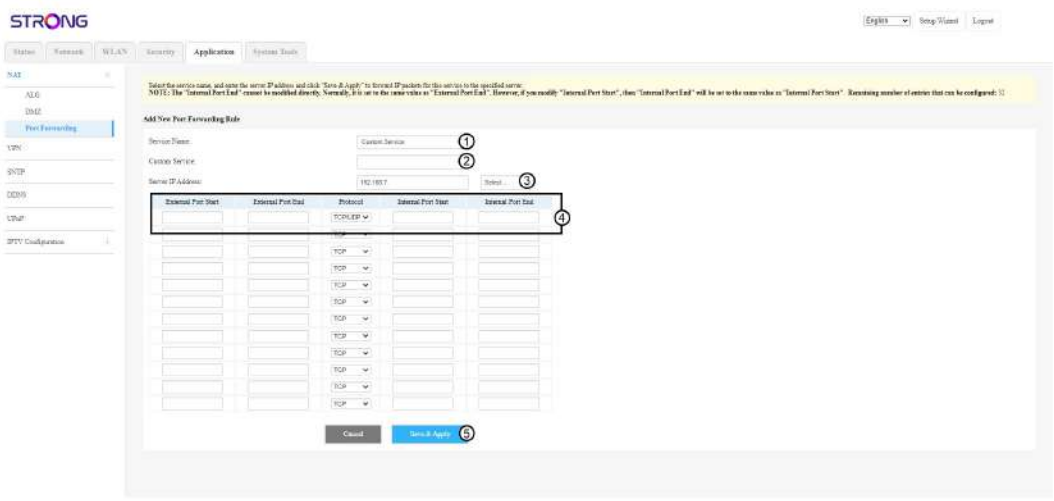
5.1.3. Port Forwarding

Port Forwarding is used to forward queries from internet to a specific device. This feature can be used to forward queries to a game console for instance when you are hosting a peer-to-peer game.

1. To do so, click **Application** and **Port Forwarding**. Then, click **add** to create a new rule.



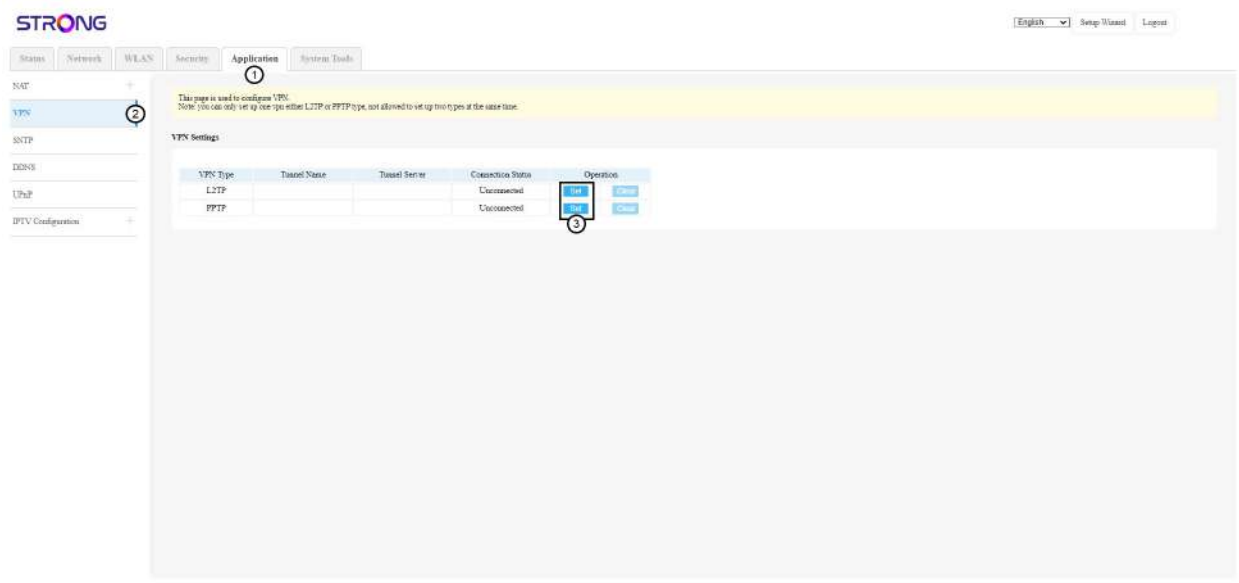
2. Enter the following information before clicking **Save & Apply:**
    - **Service Name**: Select the appropriate value in the list.
    - **Custom Service:** Enter a name for the service you are configuring.
    - **Server IP Address:** Select your device in the drop-down menu.
    - **External Port Start and External Port End:** *: For a HTTP service enter 80. For more information about the different port services, see.
    - **Protocol:** Select the protocol from the drop-down list.
    - **Internal Port Start** and **Internal Port End**: Enter the port number.



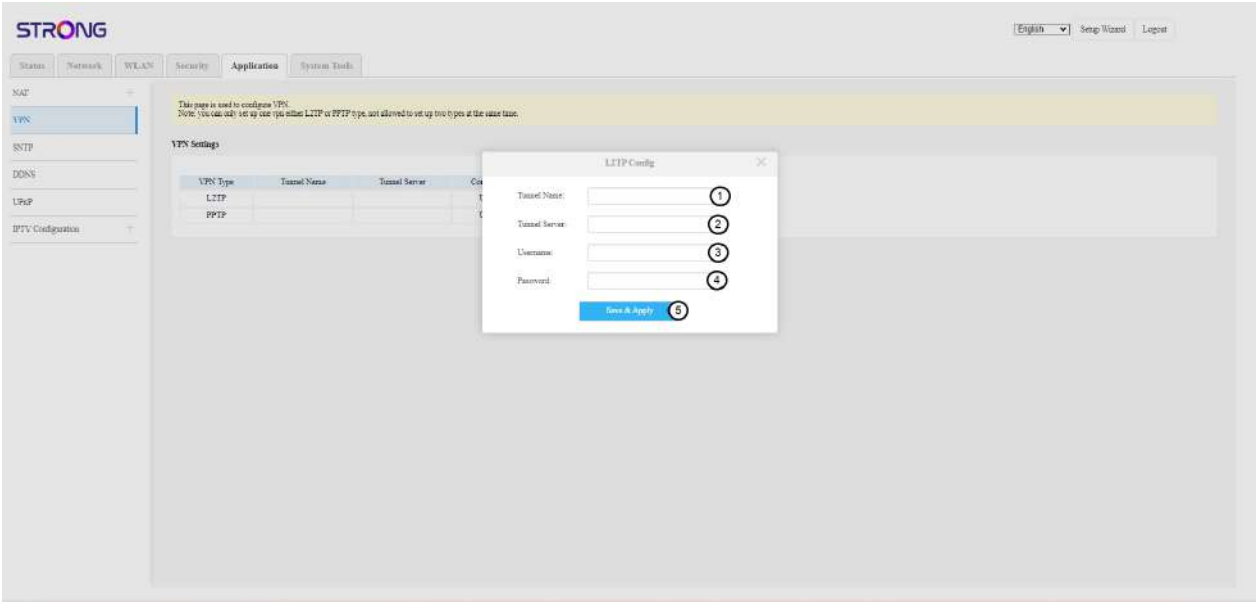
5.2. VPN

You can configure a VPN Network on your router.

1. To do so, click **Application** and **VPN.**



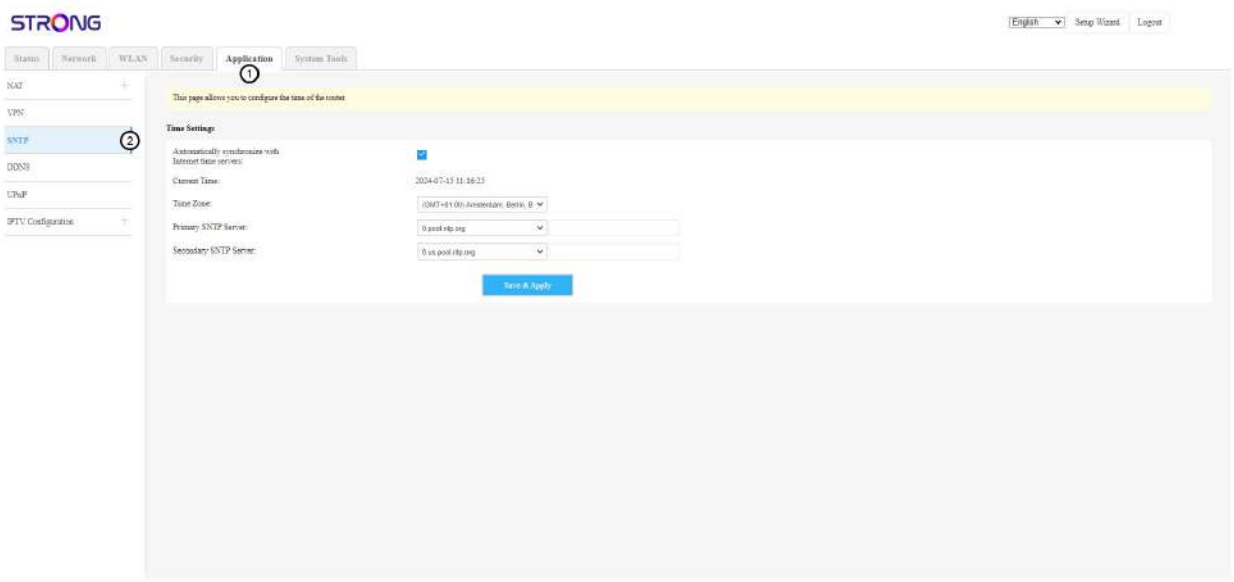
2. If you have a **L2TP** or **PPTP** account, click the **Set** button next to it. then enter the following information before clicking **Save & Apply:**
   - **Tunnel Name:** Enter a name for your VPN connection.
   - **Tunnel Server:** Enter the address of the tunnel.
   - **Username:** Enter your username.
   - **Password:** Enter your password.



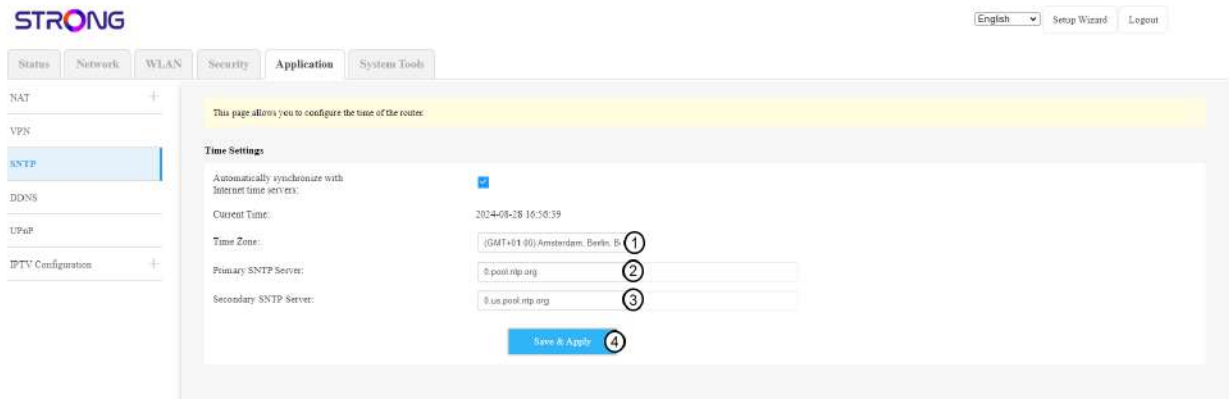
5.3. SNTP

In this part of the Web UI you can set up the time zone settings as well as the SNTP Servers.

1. To do so, click **Application** and **SNTP**.



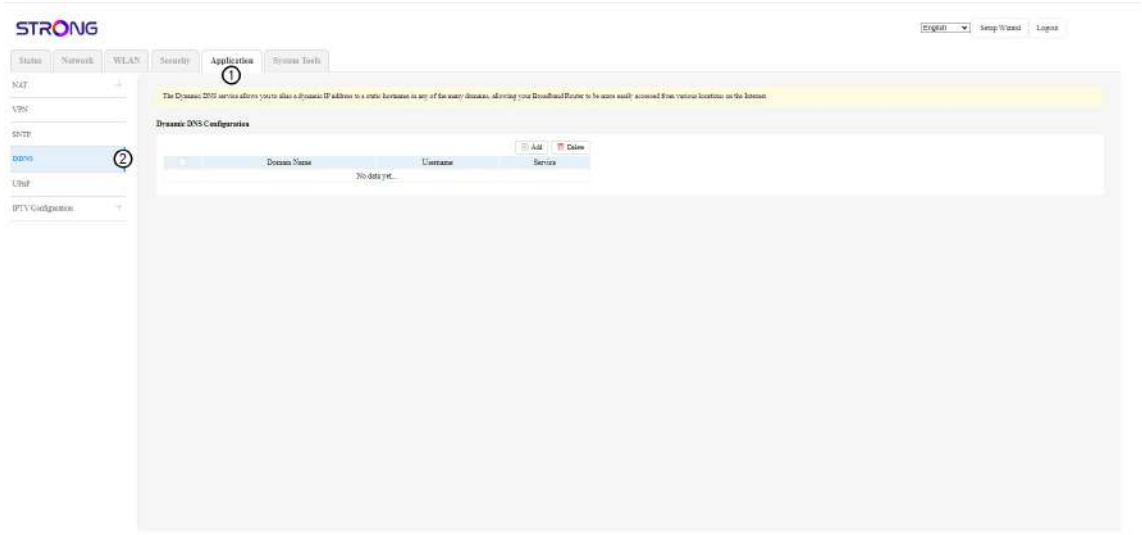
2. Enter the following information before clicking **Save & Apply:**
    - **Time Zone:** Select your time zone from the drop-down list
    - **Primary SNTP Server**: Select a SNTP Server from the list
    - **Secondary SNTP Server:** Select a SNTP Server from the list



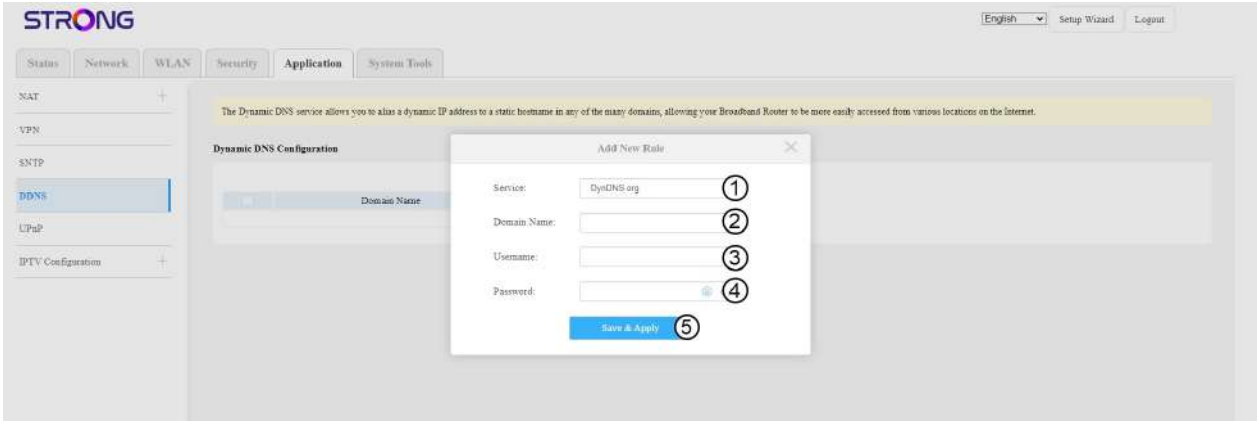
5.4. DDNS

Dynamic DNS (DDNS) is used to automatically update a DNS Server. You can choose between two DDNS provider in the Web UI, you will have to create an account and register before being able to set up the DDNS for the router.

1. Click **Application** and **DDNS**. Then, click **Add**.



2. Enter the following information before clicking **Save & Apply**:
    - **Service:** Select the DDNS service provider from the list
    - **Domain Name:** Enter the domain name
    - **Username:** Enter your username provided by the DNS Service provider.
    - **Password:** Enter your password provided by the DNS Service provider.



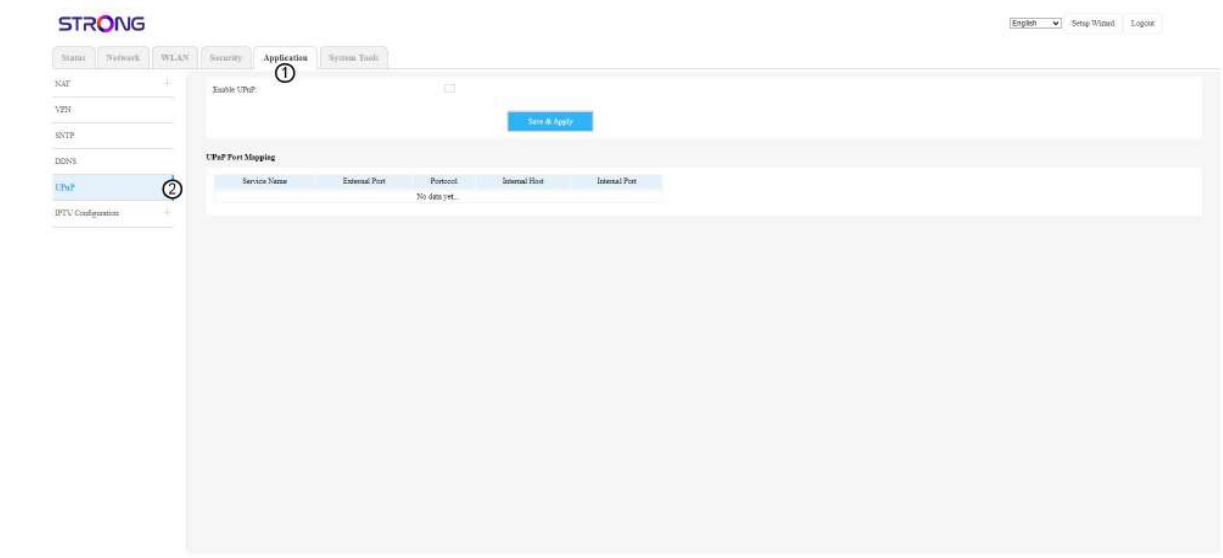
5.5. UPnP

Universal Plug and Play (UPnP) enables the devices of your network to detect compatible devices and to communicate with them automatically.

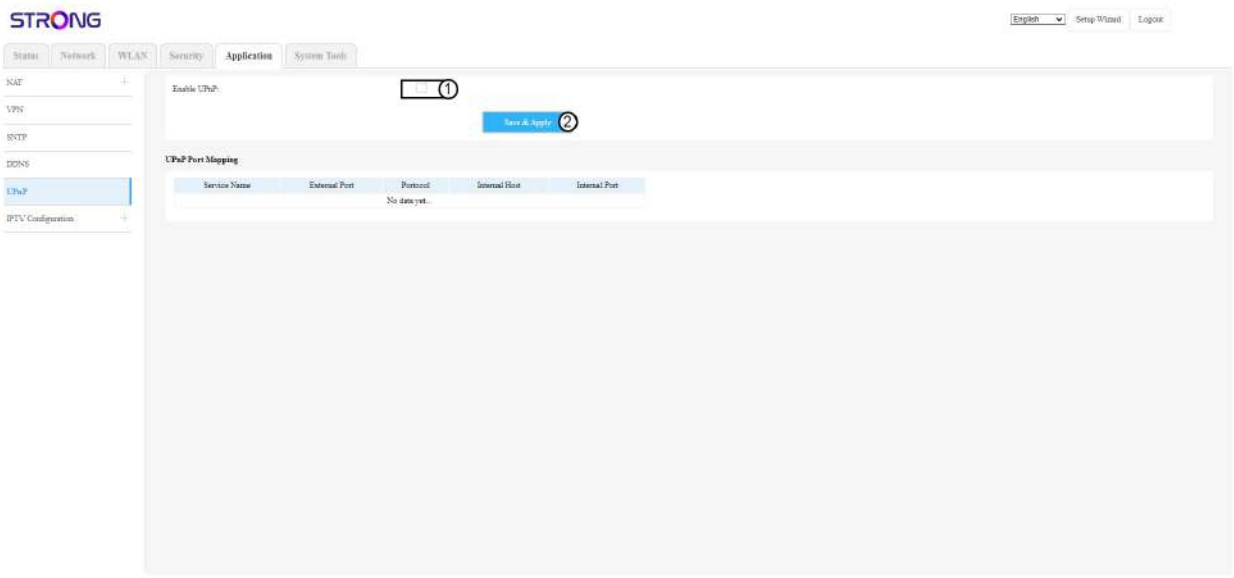
1. To activate the UPnP feature, you must be connected to the Wi-Fi of your device and access the Web UI. To do so, follow one of the procedures below:

- Connecting to the Wi-Fi and Accessing the Web UI

2. Click **Application** and **UPnP.**



3. Check the **Enable option** and **Save & Apply.**

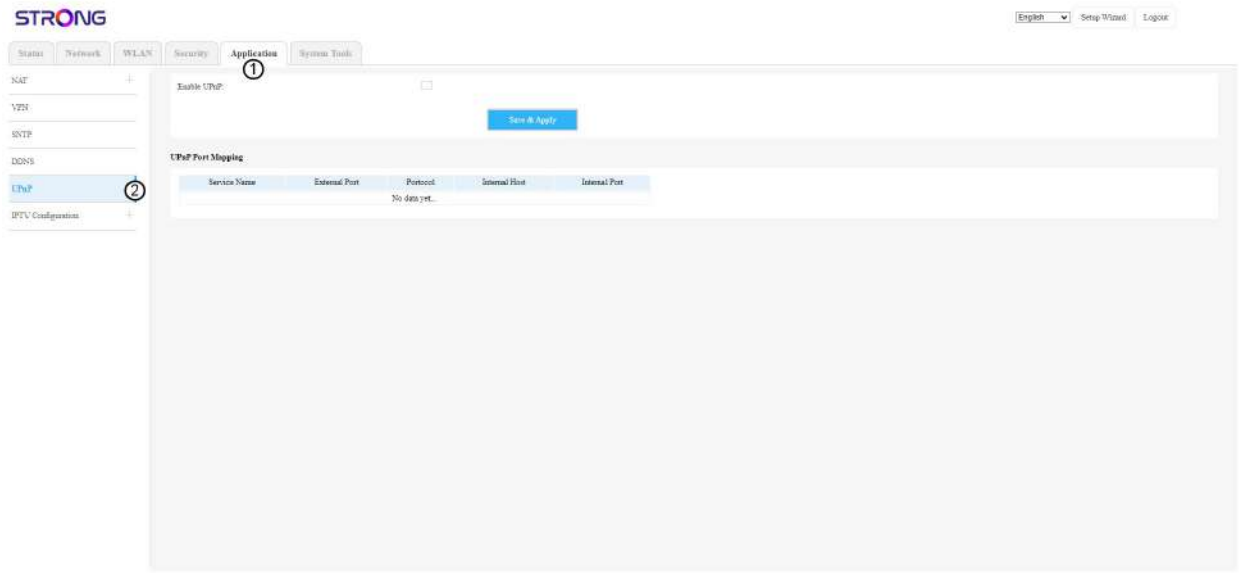


5.6. IPTV Configuration

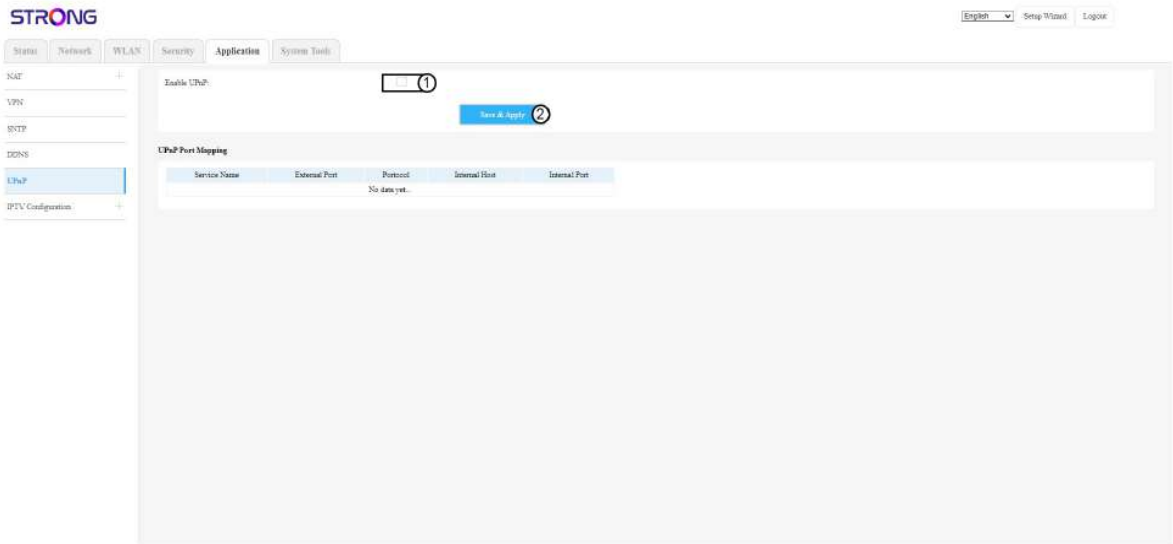
5.6.1. Snooping

In a Mesh Network, the IGMP snooping function ensure that the information (like videos or music) are send to those that need it and not to everyone. It allows a better and faster transfer.

1. Click **Application**, **IPTV Configuration** and **Snooping**.



2. Check the **IPTV Snooping Enable** box and click **Save & Apply**.

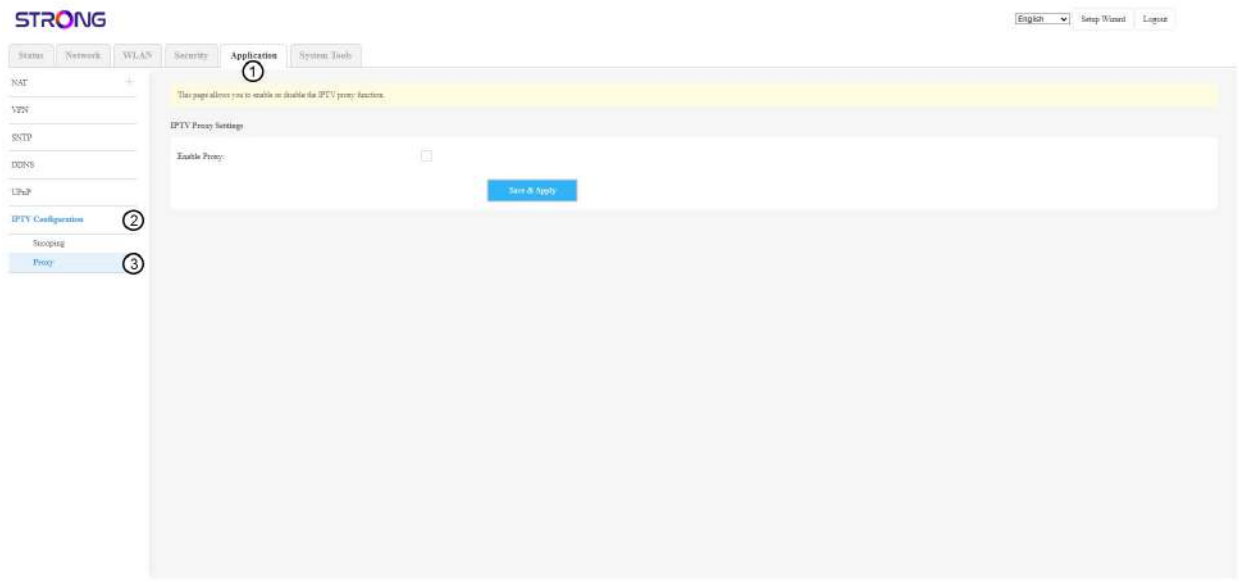


3.

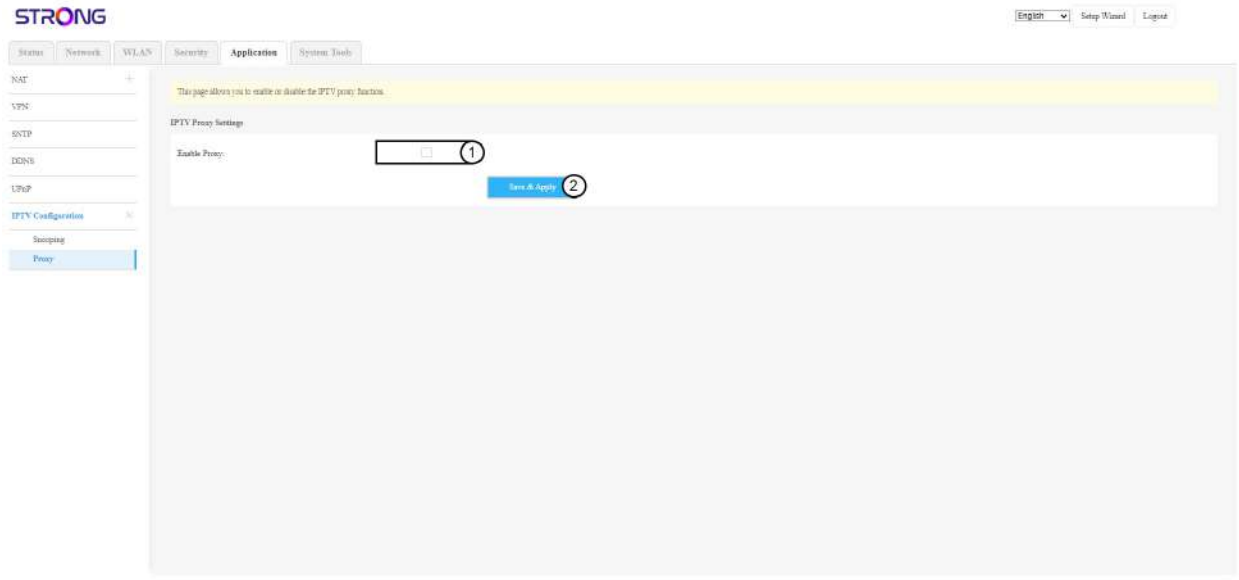
5.6.2. Proxy

IGMP Proxy: It is a parameter that enables the proxy function, which acts as an intermediary between 2 hosts to save or facilitate their communication.

1. Click **Application, IPTV Configuration** and **Proxy**.



2. Check the **Enable DHCP** box and click **Save & Apply**.



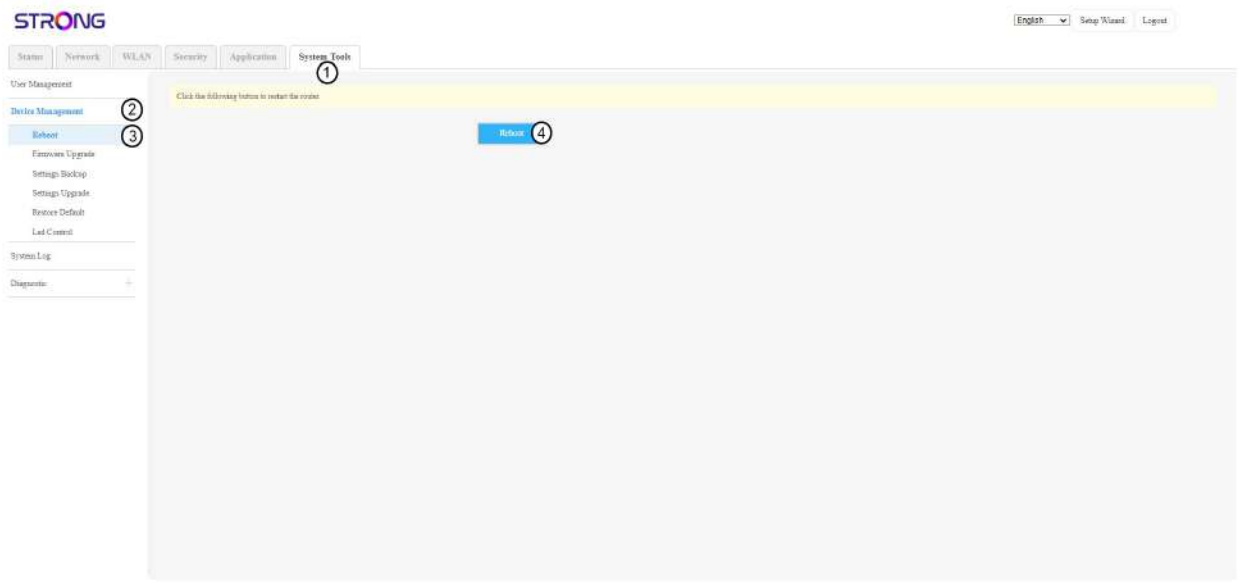
6. System Tools

6.1. Device Management

6.1.1. Reboot

You can reboot the device.

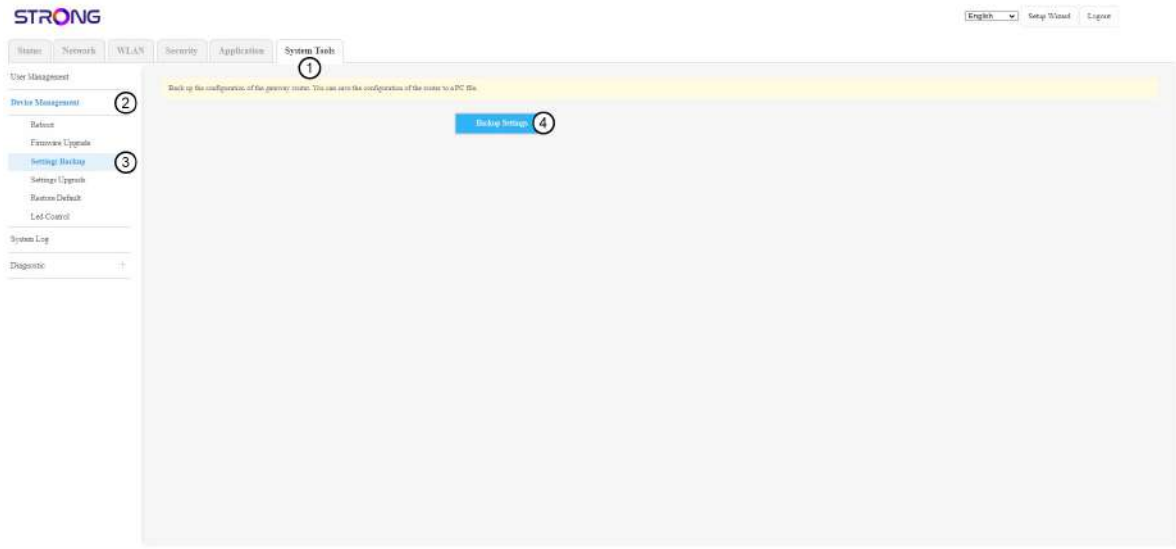
1. Click **System Tools** in the top bar, then click on the **Device Management** section and **Reboot.** Then, click the **reboot** button.



6.1.2. Settings Backup

You can save the settings of your routers in a file.

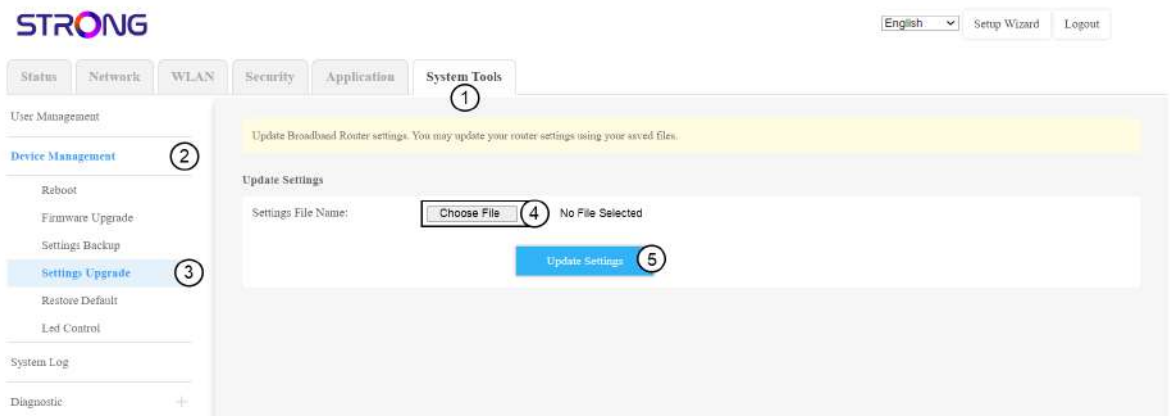
1. Click **System Tools** in the top bar, then click on the **Device Management** section and **Settings Backup.** Then, click **Backup Settings.**



6.1.3. Settings Upgrade

Here you can restore the configuration of your router with a file containing all the parameters.

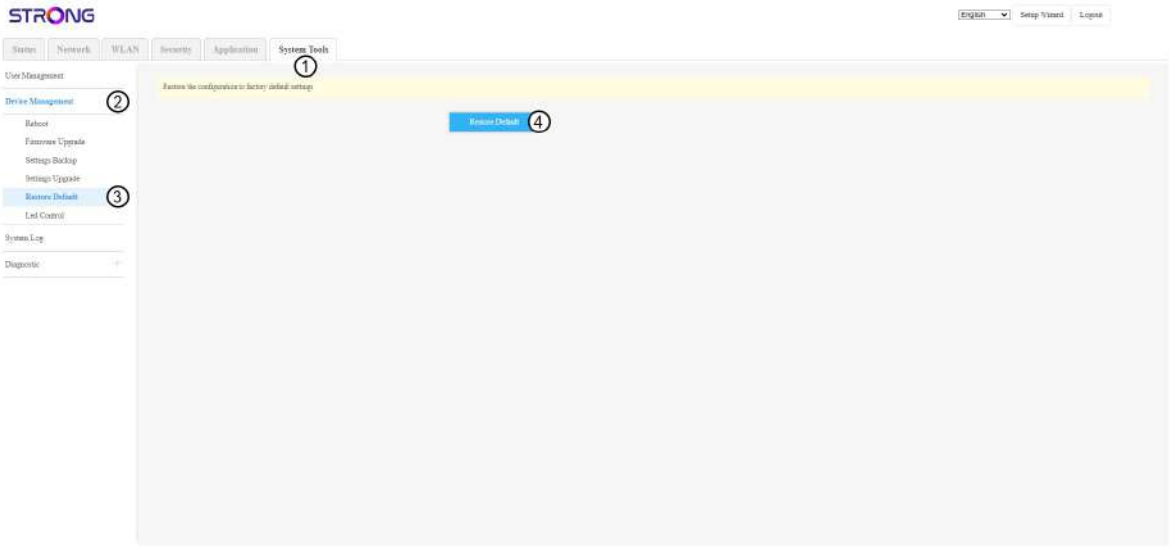
1. Click **System Tools** in the top bar, then click on the **Device Management** section and **Settings Upgrade.** Then, click the **choose file** button and select you file. Finally, click **Upgrade Settings**.



6.1.4. Restore Default

You can restore your router to its default settings.

1. Click **System Tools** in the top bar, then click on the **Device Management** section and **Restore Default.** Then, click the **Restore Default** button.

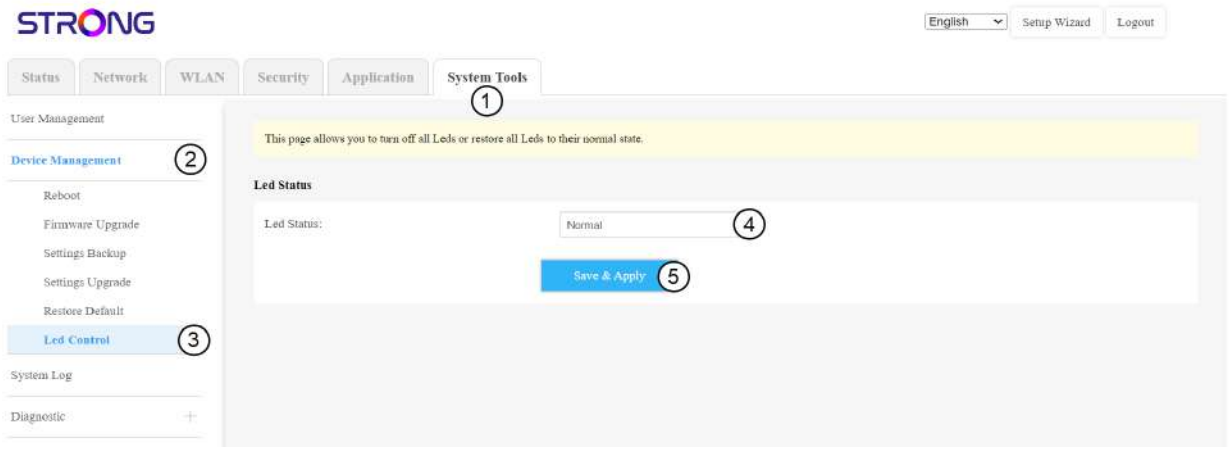


2. Click **Ok** in the message that appears.

6.1.5. LED control

You can deactivate the LED of your router.

1. Click **System Tools** in the top bar, then click on the **Device Management** section and **LED Control.** Then, uncheck the **Led Indicators on** box and click **Save & Apply.**

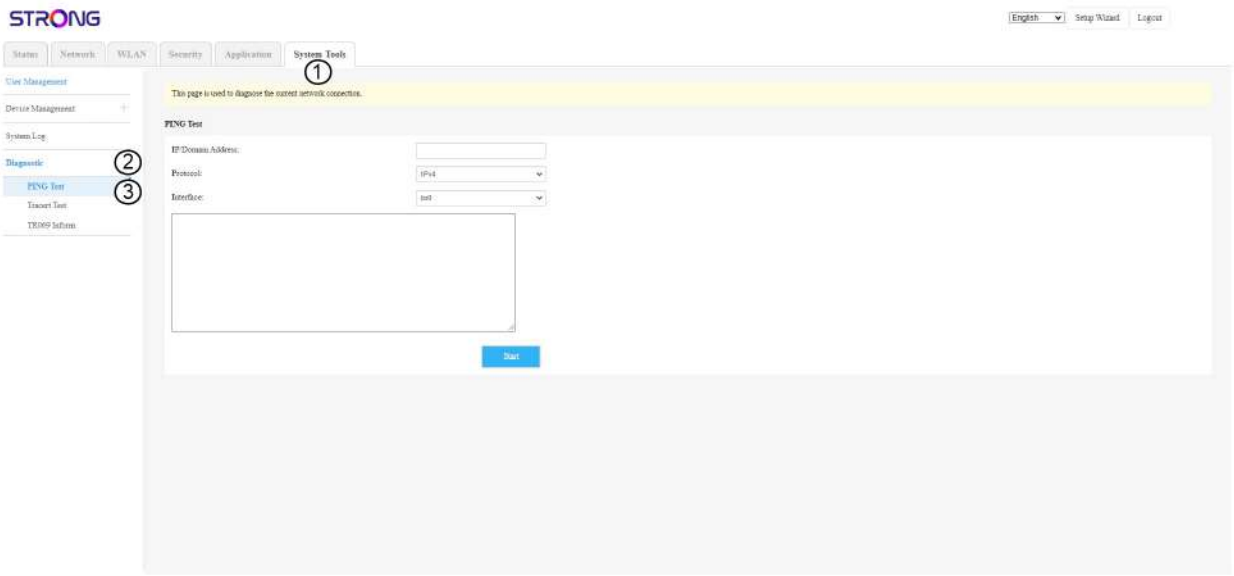


6.2. Diagnostic

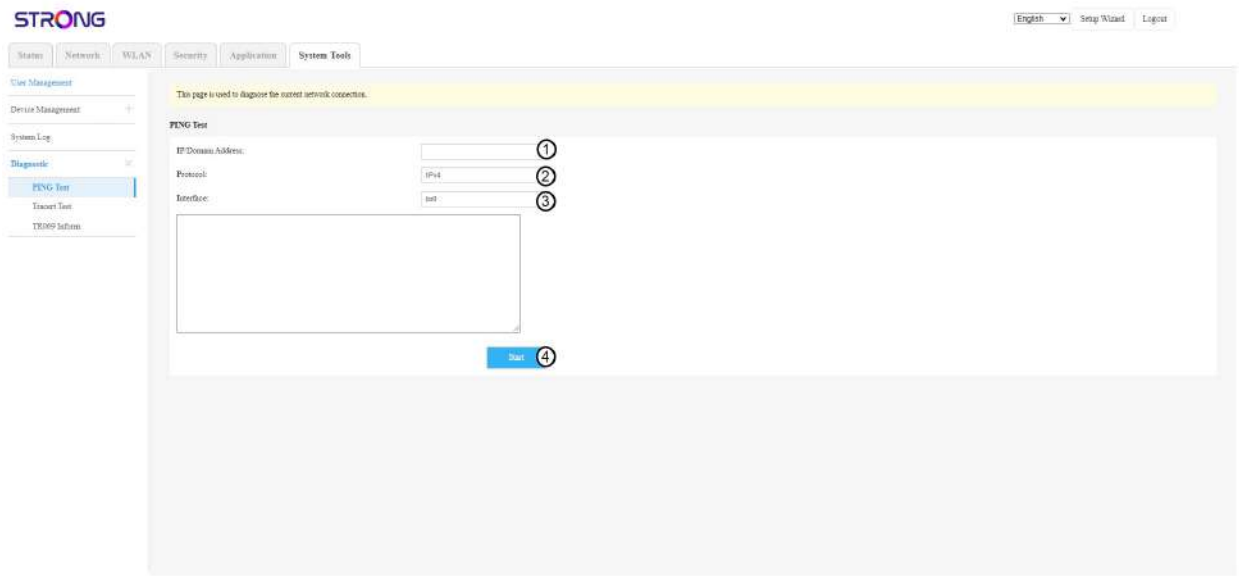
6.2.1. Ping Test

You can perform a ping test

1. Click **System Tools** in the top bar, then click on the **Diagnostic** and **PING Test.**



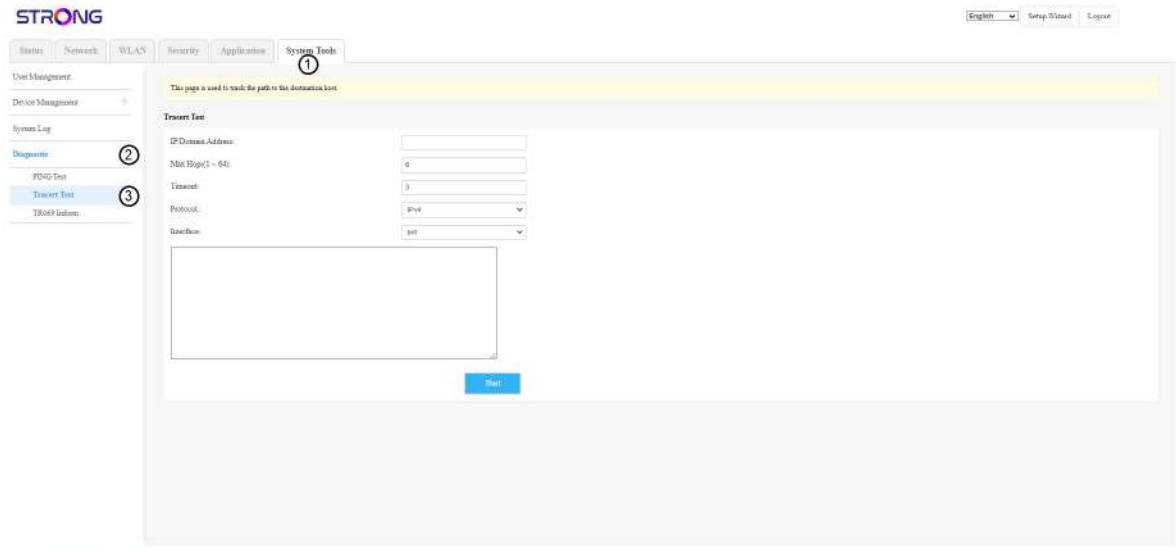
2. Enter the following information before clicking **Start**:
   - **IP/Domain Address**: Enter the IP address.
   - **Protocol:** Select the type of protocol in the drop down list.
   - **Interface :** Select the appropriate value in the list.



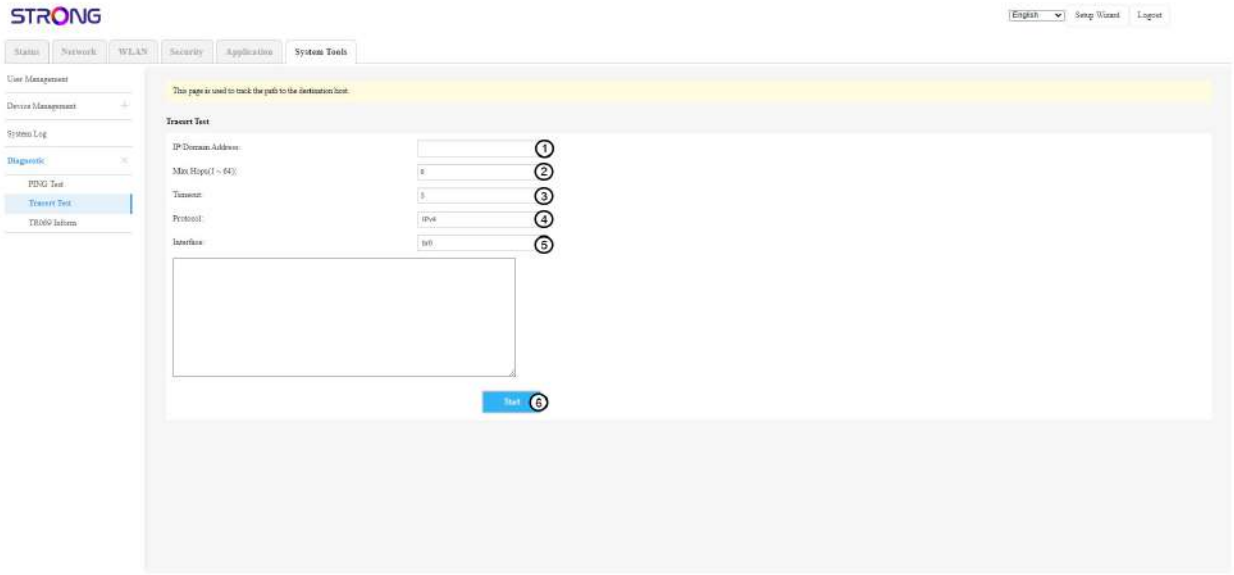
6.2.2. Tracer Test

You can perform a trace route test.

1. Click **System Tools** in the top bar, then click on the **Diagnostic** and **Tracert Test.**



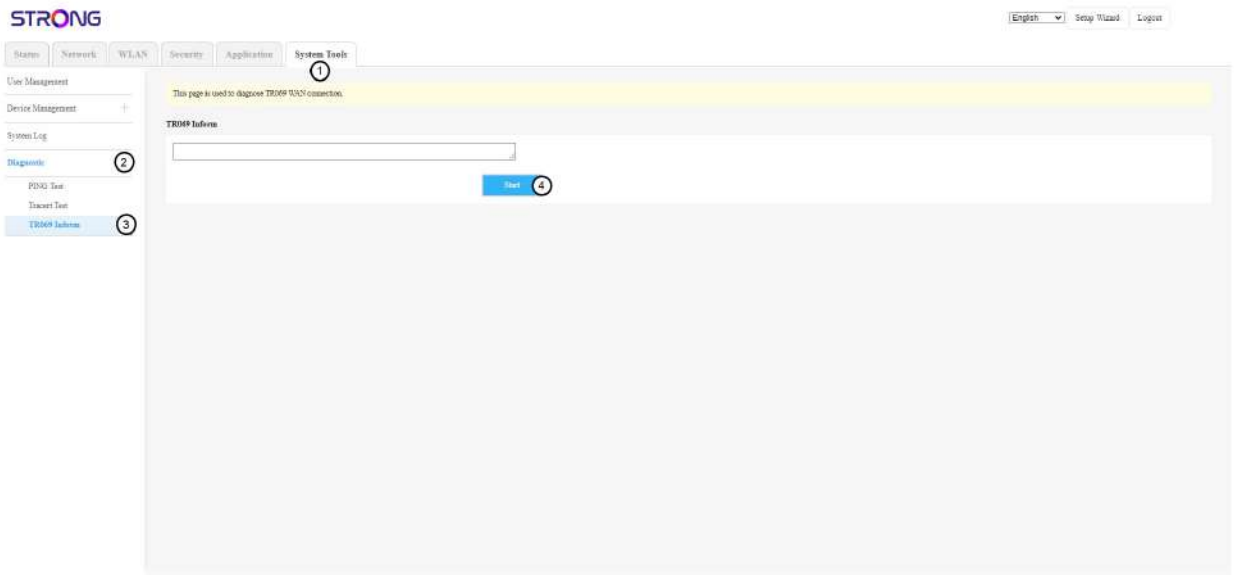
2. Enter the following information before clicking **Save & Apply**:
    - **IP/Domain Address**: Enter the IP address.
    - **Max Hops:** Enter a value between 1 and 64.
    - **Timeout :** Enter a value.
    - **Protocol:** Select the protocol in the drop down list.
    - **Interface:** Select the appropriate value in the drop-down list.



6.2.3. TR069 Inform

TR-069, also known as CWMP (CPE WAN Management), is a technical specification that provides structured remote management of local customer equipment (CPE).

1. Click **System Tools**, **Diagnostic** and **TR069 Inform**. Then, click **Start**.



V. Accessing the FAQs

You can access the Atria Mesh AX3000 FAQs , here:

Atria Mesh AX3000 Duo	Atria Mesh AX3000 Duo UK
Atria Mesh AX3000 ADD ON	Atria Mesh AX3000 ADD ON UK
Atria Mesh AX3000 Trio	Atria Mesh AX3000 Trio UK

