K3

AC3150 Dual-band Gigabit

Wireless Router

User Guide

PHICOMM

Table of Contents

Notification of Compliance

CE

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Operating Frequency

2.4G: 2402 - 2482 MHz / 5G: 5150 - 5250 MHz Maximum

Maximum Transmit Power

2.4G: 20 dBm / 5G: 23 dBm

This device may be operated in all EU countries (and other countries following the EU directive RED 2014/53/EU) for home and office use.

The band 5150 - 5250 MHz is restricted to indoor-only operation.

RF Exposure Information

This device meets the EU requirements (RED 2014/53/EU) on the limitation of exposure of the general electromagnetic fields by way of health protection.

The device complies with RF specifications when the device used at 20 cm from your body.

DISCLAIMER

Any pre-installed software or data provided as a bundle to this device is subject to the applicable law under the responsibility of the issuing software / service provider. The hardware manufacturer cannot be held liable for any breach, malfunction or other occurrence raised by using this third-party software. Only the issuing providers can lawfully be held responsible. Phicomm (Shanghai) Co., Ltd. does not own the intellectual property of the third-party software and applications that are delivered with this product. Therefore, Phicomm (Shanghai) Co., Ltd. will not provide any warranty of any kind for these third-party software and applications. Neither will Phicomm (Shanghai) Co., Ltd. provide support to customers who use these third-party software and applications nor be responsilbe or liable for the functions of these third-party software and applications. Third-party software and applications services may be interrupted or terminated at any time. Phicomm (Shanghai) Co., Ltd. does not guarantee that any content or service would be maintained for any period during its availability. Third-party service providers provide content and services through network or transmission tools outside of the control of Phicomm (Shanghai) Co., Ltd. to the greatest extent permitted by applicable law, it is explicitly stated that Phicomm (Shanghai) Co., Ltd. shall not compensate or be liable for services provided by third-party service providers or the interruption or termination of third-party contents or services. Phicomm (Shanghai) Co., Ltd. shall be not responsible for the legality, quality or any other aspects of any software installed on this product, or for any uploaded or downloadad third-party works, such as texts, images, videos or software. Customers shall bear the risk for any and all effects including incompatibility between the software and this product, which result from installing software or uploading or downloading the third-party works.

LIMITATION OF DAMAGES

To the maximum extent permitted by applicable law, in no event shall Phicomm (Shanghai) Co., Ltd. be liable for any special incidental, indirect or consequential damages or lost profits, business, revenue, data, goodwill or anticipated savings. The maximum liability (this limitaion shall not apply to liability for personal injury to the extent applicable law prohibits such a limitation) of Phicomm (Shanghai) Co., Ltd. arising from the use of the product described in this document shall be limited to the amount paid by customers for the purchase of this product.

IMPORTANT HEALTH INFORMATION AND SAFETY PRECAUTIONS

When using this product, the safety precautions below must be taken to avoid possible legal liabilities and damages. Retain and follow all product safety and operating instructions. Observe all warnings in the operating instructions on the product.

To reduce the risk of bodily injury, electric shock, fire and damage to the equipment, observes the following precautions.

SAFETY PRECAUTIONS FOR PROPER INSTALLATION

CAUTION: Connecting to an inappropriate charger can result in an electric shock to your device.

SAFETY PRECAUTIONS FOR PROPER SUPPLY UNIT

Use the correct power source!

This product can only be charged with matching standard external power source appointed by Phicomm (Shanghai) Co., Ltd.

Phicomm (Shanghai) Co., Ltd. is not liable for any device breakdown or safety accident arising from the use of unauthorized external power source.

SAFETY PRECAUTION FOR DIRECT SUNLIGHT

Keep this product away from excessive moisture and extreme temperatures. The device is designed to be operated in temperatures between 0°C and 40°C. Low- or high-temperature conditions might cause the device to temporarily stop working properly. Do not leave the product in a vehicle or in places where the temperature may exceed 70°C (window sill or behind glass). Avoid dramatic changes in temperature or humidity when using the device as condensation may form on or within the device.

When you are using the device, it is normal for the device to get warm. The exterior of the device functions as a cooling surface that transfers heat from inside the unit to the cooler air outside.

ENVIRONMENT RESTRICTIONS

Do not use this product in gas stations, fuel depots, chemical plants or where blasting operations are in process, or in potentially explosive atmospheres such as below deck on boats, fuel or chemical transfer or storage facilities, and areas where the air contains chemicals or particles, such as grain, dust or metal powders. Please be aware that sparks in such areas could cause an explosion or fire resulting in bodily injury or even death.

EXPLOSIVE ATMOSPHERES

In any area with a potentially explosive atmosphere or where flammable materials exist, the product should be turned off and the user should obey all signs and instructions. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Users are advised not to use the equipment at refueling areas such as service or gas stations, and are reminded of the need to observe restrictions on the use or radio equipment in fuel depots, chemical plants or where blasting operations are in progress. Areas with a potentially explosive atmosphere are often, but not always, clearly marked. These include fueling areas, below deck on boats, fuel or chemical transfer or storage facilities, and areas where the air contains chemicals or particles, such as dust or metal powders.

SAFETY PRECAUTIONS FOR RADIO FREQUENCY EXPOSURE

- Avoid using your device near metal structures (e. g. the steel frame of a building).
- Avoid using the device near strong electromagnetic sources, such as microwave ovens, sound speakers, TV and radio.
- Use only original manufacturer-approved accessories.
- Use of non-original manufacturer-approved accessories may violate your local RF exposure guidelines and should be avoided.

INTERFERENCES WITH MEDICAL EQUIPMENT FUNCTIONS

This product may cause medical equipment to malfunction. The use of this device is forbidden in most hospitals and medical clinics.

If you use any other personal medical device, consult the manufacturer of your device to determine if they are adequately shielded from external RF energy.

HEARING AID DEVICES

Some devices may interfere with some hearing aid devices. In the event of such interference, you may want to consult your service provider, or call customer service line to discuss alternatives.

NON-IONIZING RADIATION

Your device has external antennas. This product should be operated in its normal-use position to ensure the radiative performance and safety of the interference. Users are advised that for satisfactory operation of the equipment and for the safety of personnel, it is recommended that no part of the human body be allowed to come too close to the antenna during operation of the equipment.

Use only the supplied antennas. Use of unauthorized or modified antennas may impair transfer quality and damage the device, causing loss of performance and SAR levels exceeding the recommended limits as well as result in noncompliance with local regulatory requirements in your country.

To assure optimal device performance and ensure human exposure to RF energy is within the guidelines set forth in the relevant standards, always use your device only its normal-use position. Contact with the antennas may impair quality and cause your device to operate at a higher power level than needed. Avoiding contact with the antenna area when the device is in use optimizes the antenna performance.

GENERAL PRECAUTIONS

AVOID APPLYING EXCESSIVE PRESSURE TO THE DEVICE

Do not apply excessive pressure on the device to prevent damage.

DEVICE IS GETTING WARM AFTER PROLONGED USE

When using your device for prolonged periods the device may become warm. In most cases this condition is normal and therefore should not be interpreted as a problem with the device.

HEED SERVICE MARKING

Except as explained in the user manual, do not repair any product yourself. Service needed on components inside the device should be done by an authorized service outlet or provider.

Phicomm (Shanghai) Co., Ltd. is entitled to use new or reconditioned replacements parts or boards for repairs under warranty, provided they have the same functionality as the parts to be replaced.

DAMAGE REQUIRING SERVICE

Unplug the device from the electrical outlet and refer servicing to an authorized service center or provider under the following conditions:

- Liquid has been spilled or an object has fallen onto the product.
- The product has to been exposed to rain or water.
- There are noticeable signs of overheating.
- The product does not operate normally when you follow the operating instructions.

AVOID HOT AREAS

The product should be placed away from heat sources such as radiators, heat registers, stoves, or other products (including amplifiers) that products heat.

AVOID WET AREAS

Never use the product in a wet location.

AVOID USING YOUR DEVICE AFTER A DRAMATIC CHANGE IN TEMPERATURE

When you move your device between environments with very different temperature and/or humidity ranges, condensation may form on or within the device. To avoid damaging the device, allow sufficient time for the moisture to evaporate before using the device.

NOTICE: When taking the device from low-temperature conditions into a warmer environment or from high-temperature conditions into a cooler environment, allow the device to acclimate to room temperature before turning on power.

AVOID PUSHING OBJECTS INTO THE DEVICE

Never push objects of any kind into cabinet slots or other openings in the product. Slots

and openings are provided for ventilation. These openings must not be blocked or covered.

MOUNTING ACCESSORIES

Do not use the product on an unstable table, cart, tripod or bracket. Any mounting of the product should follow the manufacturer's instructions, and should use a mounting accessory recommended by the manufacturer.

AVOID UNSTABLE MOUNTING

Do not place the product with an unstable base.

USE PRODUCT WITH APPROVED EQUIPMENT

This product should be used only with personal computers and options identified as suitable for use with your equipment.

CLEANING

Unplug the product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning, but NEVER use water to clean the device. The device has been provided with special treatments featuring that it could dispose dirt and sweat on its surface. The device itself does not have a stain-resistant function. In case of smudginess and dyeing, please wipe it with clean damp sponge immediately. Please keep the device dry when necessary.

PACEMAKER

The device may cause disturbance to pacemakers. Please keep the device a proper distance of least 5 centimeters away from pacemakers.

If you need detailed information about other active implantable medical devices, please consult your doctor to ensure the magnetic interference of such active implantable medical devices.

CAUTION

Update your operating system with caution

- Improper operation or unforeseen external factors may cause an operating system update fails; the device will not work properly. If such a situation occurs, you need to send the unit in for repair.

- An unofficial operating system can cause security risks. Please install only official updates provided by Phicomm (Shanghai) Co., Ltd., if not you will void the warranty and a repair is chargeable.

FCC User Information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

1 About this guide

This user guide includes a complete overview of the configuration and functions of PHICOMM K3 router on Web Management interface.

Note

- It is suggested to use Firefox, Google Chrome, IE 9.0 or above to login in Web Management. Software interface might vary by browsers.
- Software interface and functions might vary by firmware versions.

1.1 Structure of this guide

This guide is structured as follows:

Chapter	Title	Subject
1	About this guide	Basic description of document content, definition of symbols and conventions
2	Introduction	Description of basic functions
3	Hardware connections	Description of the way connecting the router to your devices
4	Get started	Description of the way to set up your router for the first time
5	General configurations	Description of router's general functions
6	Advanced configurations	Description of router's advanced functions
7	Administration	Description of router's administration features
	Appendix	FAQs and technical support information

1.2 Symbols and conventions

The following symbols are used in the user guide:

WARNING!
May result in severe damage to your device or database.

Note
Useful additional information

The following editorial conventions are used in the guide:

Convention	Explanation
Bold	Field names / button names are written in bold Example: click menu **View**
Italic	Commands, screen output, file names and paths are written in *Italic*. Example: Input *192.168.2.1* in **IP address** text box.
<…>	<…> keyboard or actual names are represented in angle brackets Example: Click <Ctrl> + <Alt> + <Delete> to open the task manager.
>	Used for menu sequence Example: Click **File > Print** to print.

2 Introduction

Phicomm K3 AC3150 Dual-band Gigabit wireless Router is an all-in-one router for home and SOHO users to share broadband internet connection over a wired or a wireless network.

The simultaneous dual-band speed of up to 3167 Mbps (2.4G 1000 Mbps and 5G 2167 Mbps) provides users with extraordinary smooth internet surfing, internet phone calling and online gaming.

Phicomm K3 router support the following features:

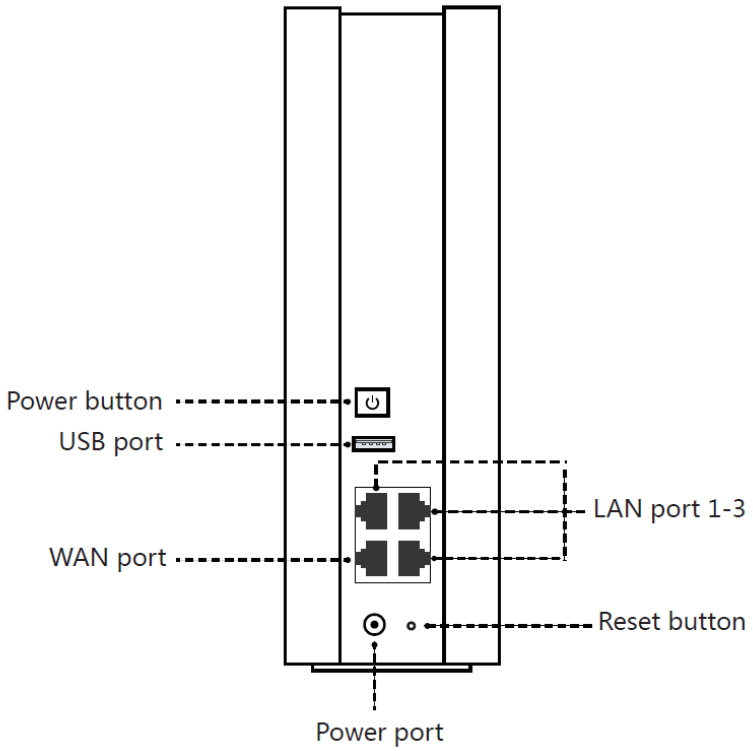
- Dedicated processor for each band to manage Wi-Fi traffic, freeing up the router's 1.4GHz dual-core Broadcom CPU to tackle more demanding tasks
- 512 MB RAM and optimized software prevent network congestion, assuring smooth and fast internet surfing
- 8 Built-in high-gain array omni-directional antennas greatly increase the PHICOMM K3's range and signal stability.
- Simultaneous dual-band speed up to 3167 Mbps (2.4G 1000 Mbps and 5G 2167 Mbps)
- 1 Gigabit WAN + 3 Gigabit LAN with up to 1000 Mbps WAN-LAN throughput
- USB 3.0 interface for file share in external storage device
- VPN offers secure access for remote users
- Parental Control allows parents or administrators to establish restricted access policies for children or staff
- Device Management allows administrators to control the bandwidth for each individual device.
- Create separate network for guest users to enhance network security
- You can access internet with only three steps

3 Hardware connections

3.1 Package contents

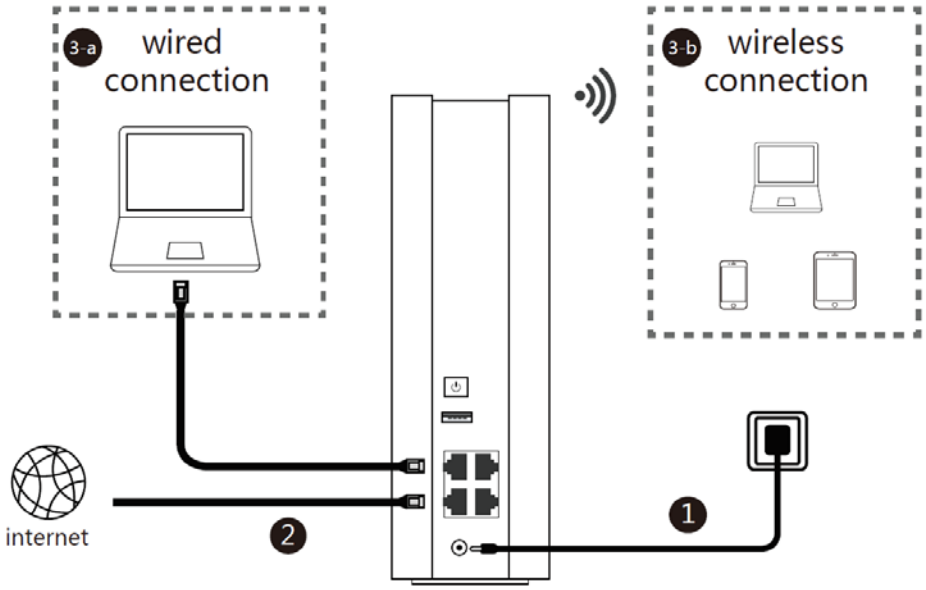
Please check the package content before the installation of the router:

- 1 x Wireless Router
- 1 x power adapter
- 1 x RJ-45 cable
- 1 x Quick Installation Guide
- GPL license
- 1 x Warranty Card



3.2 Connect your devices

Follow these steps below to connect your devices.



1. Connect the power adapter into an electrical socket, connect the other end to the router, and switch it on.

2. Connect your modem to the WAN port on the router using a RJ-45 cable.

> **Note**
>
> - Make sure your modem has proper internet connection.
> - If you have a wired Ethernet connection to internet instead of a modem, connect the RJ-45 cable directly to the WAN port on the router, then continue with the following instructions to complete the router setup.

3. Connect your device to the router (wired or wireless):

3-a. **Wired**: Connect your PC to the LAN port on the router with a RJ-45 cable.

3-b. **Wireless**: Turn on WLAN on your wireless device and connect to **@PHICOMM_XX** or **@PHICOMM_XX_5G**.

XX represents the last two digits of the router's MAC address that can be found on the label at the bottom of the router.

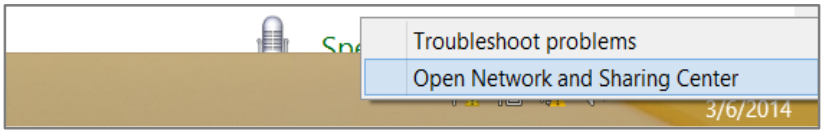
4 Get started

This section gives instructions of the procedures that must be performed to enable the wireless router.

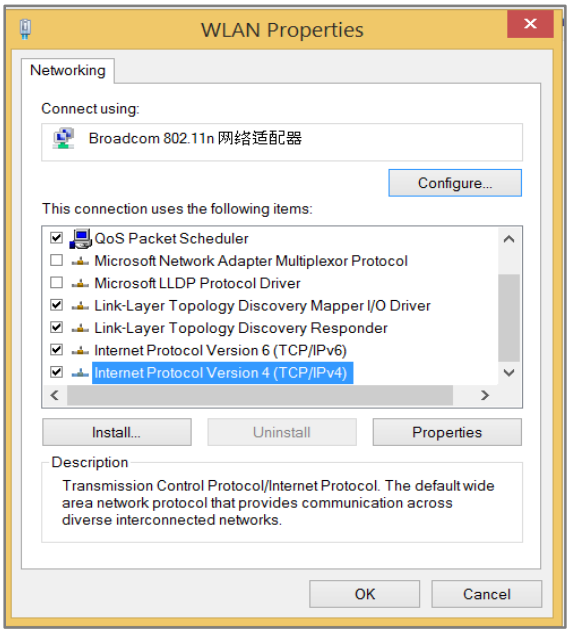
4.1 TCP/IP settings

The IP address has to be obtained automatically before starting the configuration of the router. Please follow these steps:

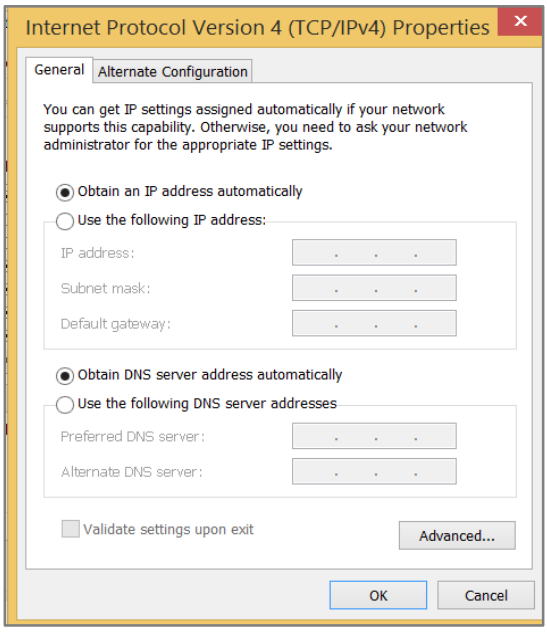
1. With the right mouse button please click on the right bottom corner. Click **Open Network and Sharing Center** and select **Change adapter settings** on the upper left of the screen.



2. Right-click network connection type and select **Properties**. In the **Properties** window double click **Internet Protocol Version 4 (TCP/IPv4)**.



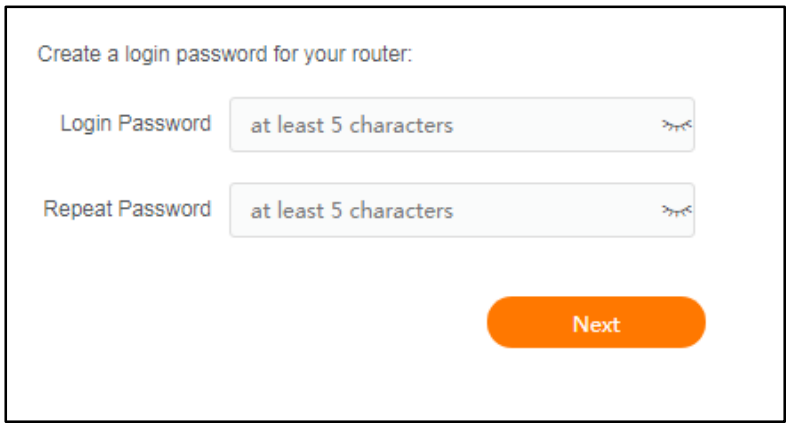
3. Select both **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK** to confirm the configuration.



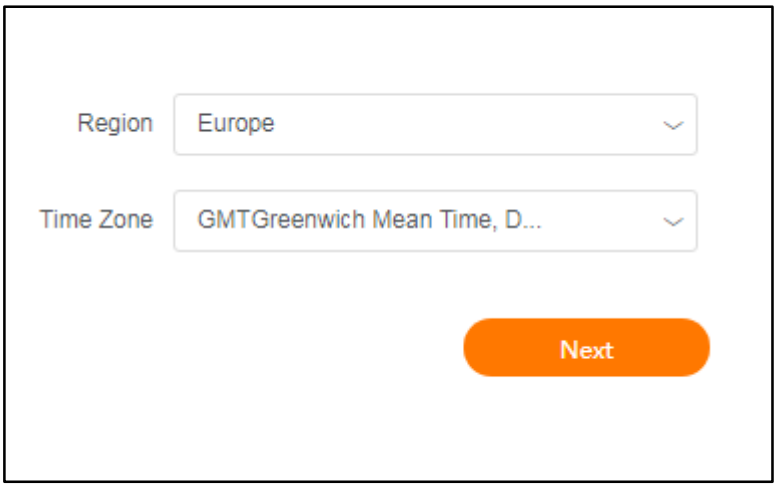
4.2 Set up router via web browser

1. On your web browser, enter ***p.to*** or ***192.168.2.1*** in address bar and click **Start Setup** to run the setup wizard.

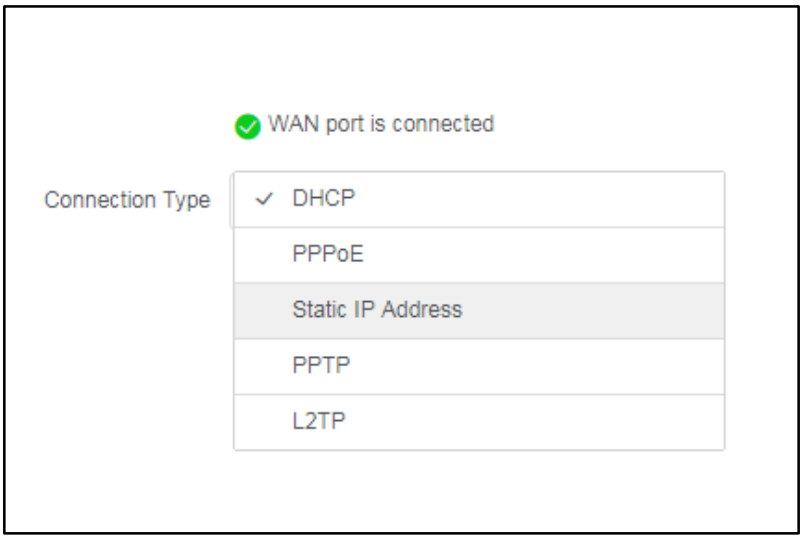
2. Create a login password for your router and click **Next**.



3. Select your local time zone and click **Next**.



4. Specify your internet connection type, enter the relevant account information as required and click **Next**.

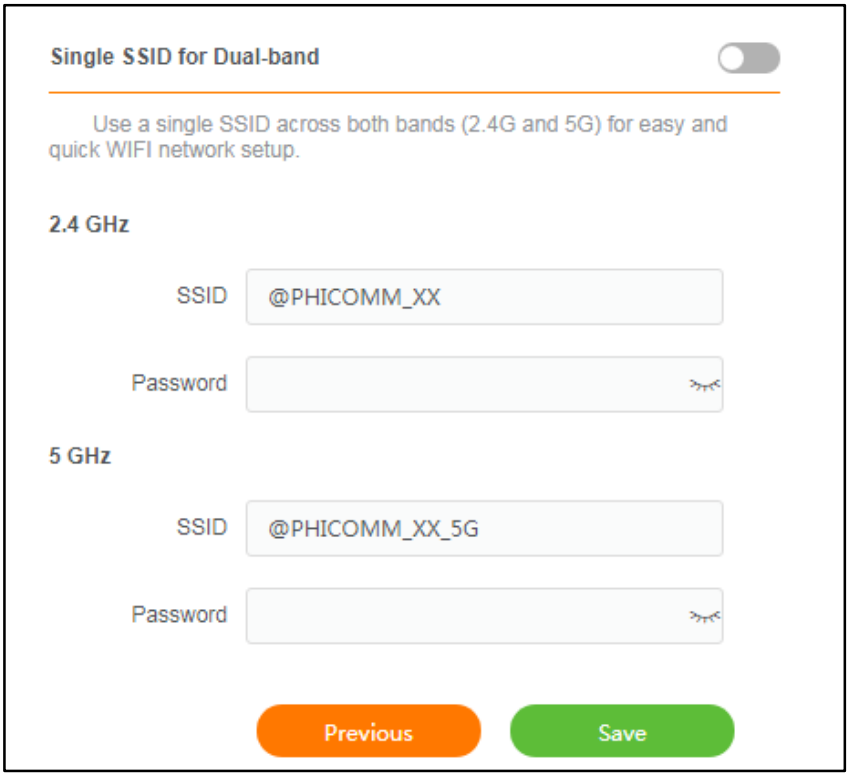


DHCP	DHCP is commonly used if internet service provider does not provide any IP to use. Router will obtain IP address information automatically.
PPPoE	PPPoE is typically used for DSL services. Enter the username and password provided by your internet service provider.
Static IP address	Select Static IP if internet service provider provides the static IP address, subnet mask, default gateway and DNS server address.
PPTP/L2TP	Select PPTP or L2TP if ISP provides the username, password, and VPN server IP.

Note

Contact your ISP if you are not sure about your internet connection type.

5. Set SSID and password (no less than 8 characters) for your wireless network or use the default settings. You can choose to use the **Single SSID for Dual-band** (2.4G and 5G) for easy and quick WIFI network setup. Click **Save** to complete the setup.

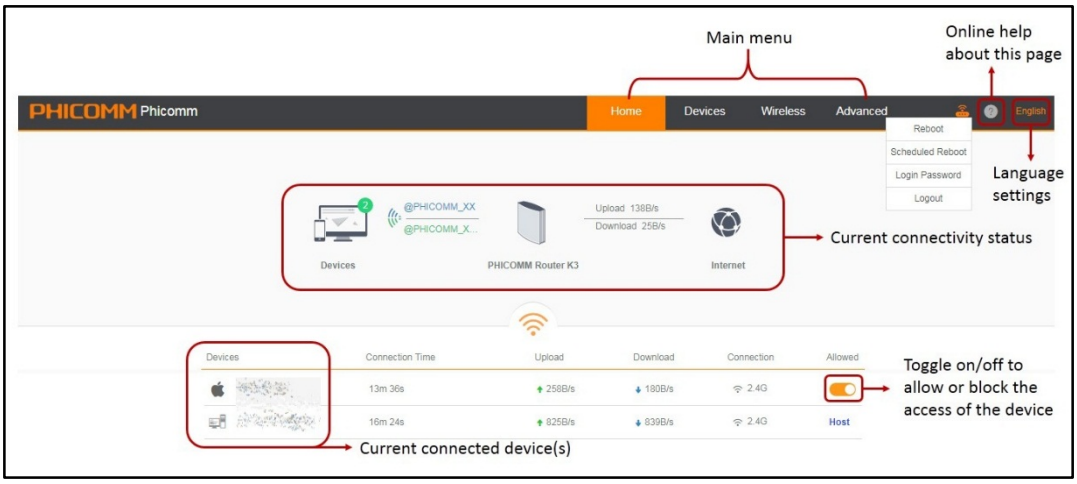


6. Now Wi-Fi has been successfully set up on your router. If your device does not automatically connect to the wireless network, please connect manually. You can also click **More Settings** for further advanced configuration.

4.3 Log into Web Management

On your web browser, enter ***p.to*** or ***192.168.2.1*** in address bar, and enter the login password that is set when you set up the router for the first time.

You can now use the Web Management for further configurations on the router.



4.4 Configuring router via Phicomm app

To install and set up your router via Phicomm app, follow these steps:

1. Scan the barcode below, download and install PhiWiFi from Apple App Store or Google Play.

> **Note**
>
> Alternatively, you can search “PhiWiFi” on Apple App Store or Google Play Store.

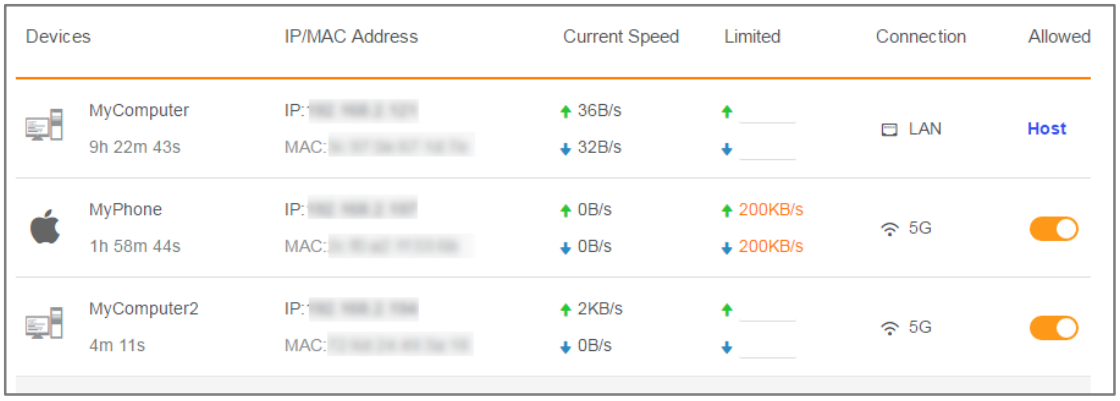
2. Make sure your router is powered on and connected to internet properly. Turn on WLAN on your smartphone and connect to Phicomm’s wireless network **@PHICOMM_XX** or **@PHICOMM_XX_5G**.

3. Launch PhiWiFi and follow the step-by-step instructions to complete the setup.

5 General configurations

5.1 Manage devices

To manage the devices on your local network, go to **Main menu > Devices** on Web Management, all devices connected to your local network will be listed on this screen.



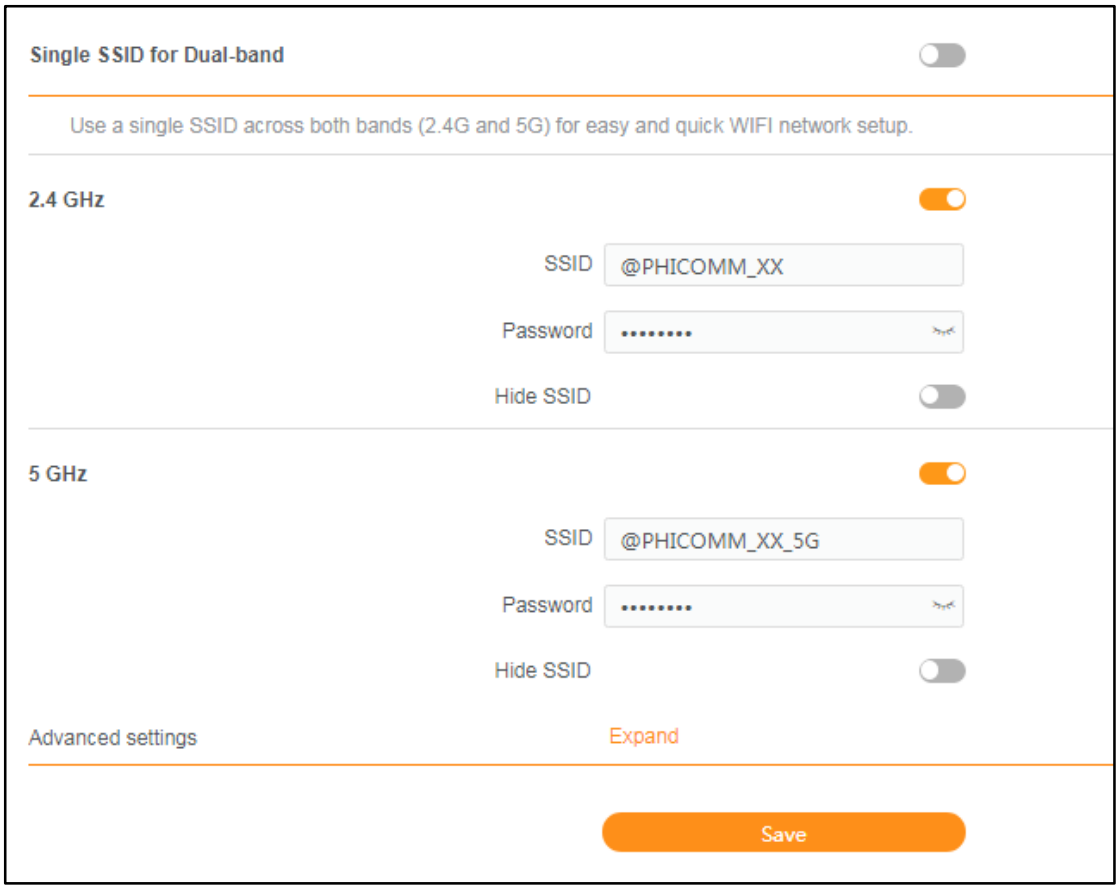
To block a computer or device from connecting to your home network, toggle off the **Allowed** switch. To allow the computer or device to continue access the network, toggle on the **Allowed** switch.

You can specify the maximum upload/download bandwidth in the **Limited** field.

The device can be renamed by clicking **Devices** field and entering the new name.

5.2 Wireless settings

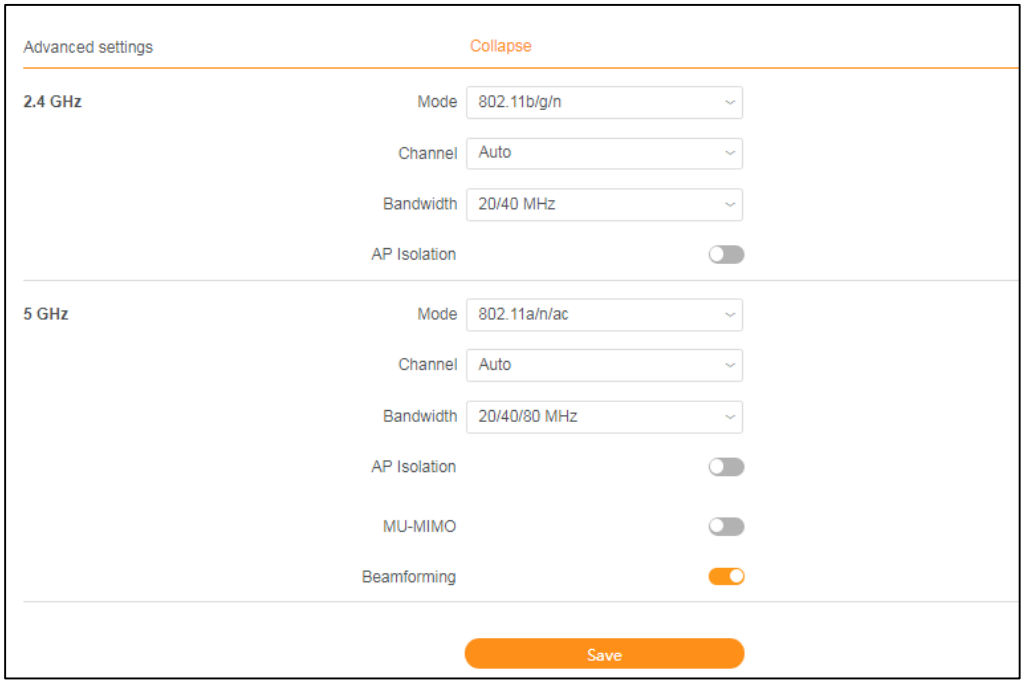
To configure the basic wireless settings, go to **Main menu** > **Wireless** on Web Management.



You can switch on/off wireless network, or modify the SSID/password for 2.4G and 5G separately.

Single SSID for Dual-band	If **Single SSID for Dual-band** is enabled, both 2.4G and 5G will apply the same SSID and password.
Hide SSID	If **Hide SSID** is enabled, the wireless network with this SSID will not be discovered by other Wi-Fi devices.

Click **Expand** to have more advanced settings displayed.



Mode Select the Wi-Fi mode you want to use. For more information about IEEE802.11, please refer to *http://www.ieee.org*.

Channel Channel determines which operating frequency will be used. If you notice a severe interference problems with another nearby access point, you may try to manually select a fixed channel. Otherwise you can leave it as *Auto*.

Bandwidth Different Wi-Fi mode has different bandwidth. Normally a higher bandwidth provides faster network speed, but it will be much easier interfered by other radio signal. The default value is recommended.

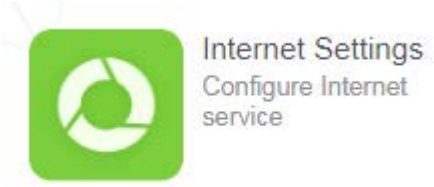
AP Isolation If enabled, the devices under this SSID can only access internet and it cannot communicate with other devices in the same Wi-Fi network.

MU-MIMO When Multi-User Multiple-Input Multiple-Output (MU-MIMO) is enabled, the router can utilize the wireless bandwidth in the most efficient way to achieve a faster network speed.

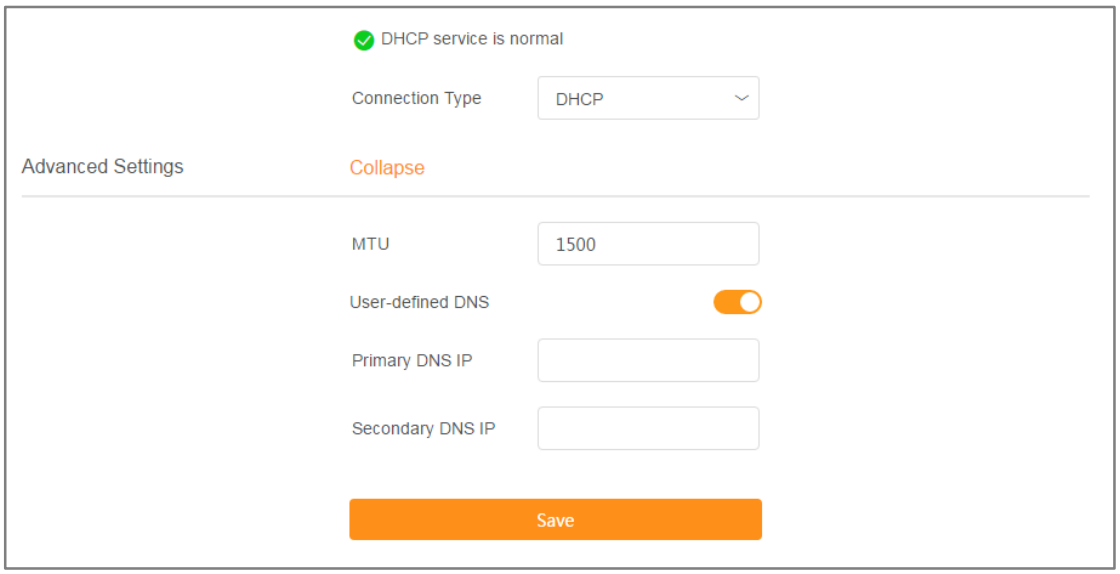
Beamforming When Beamforming is enabled, the radio energy can be better utilized between the router and the connected devices to achieve a faster network speed.

Click **Save** to save the settings.

5.3 WAN settings



To configure WAN settings, go to **Main menu > Advanced > Internet Settings** on Web Management.



For **Connection Type**, refer to Section 4.2.

Click **Expand** to have more advanced settings displayed.

MTU MTU defines the maximum length of your data packet.

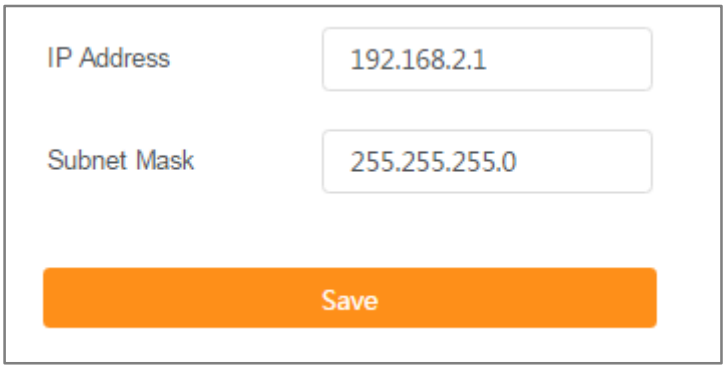
- *DHCP*: The range of maximum length is between 576 and 1500. 1500 is the default value.
- *PPPoE*: The range of maximum length is between 576 and 1492. 1480 is the default value.
- *Static IP Address*: The range of maximum length is between 576 and 1500. 1500 is the default value.
- *PPTP*: The range of maximum length is between 576 and 1420. 1420 is the default value.
- *L2TP*: The range of maximum length is between 576 and 1460. 1460 is the default value.

User-defined DNS	If any specific server is required, toggle on this switch and enter the IP address of primary DNS server and secondary DNS server (if available).

Click **Save** to save the settings.

5.4 LAN settings

To configure LAN settings, go to **Main menu > Advanced > LAN Settings** on Web Management. Current LAN IP address and subnet mask are displayed.



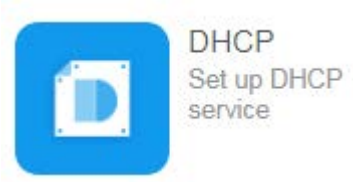
IP address	Enter LAN IP address of the router.
Subnet Mask	Enter the subnet mask associated with the LAN IP address.

Note

If you change the LAN IP address of the router, please log on Web Management with the new IP address or *p.to*.

6 Advanced settings

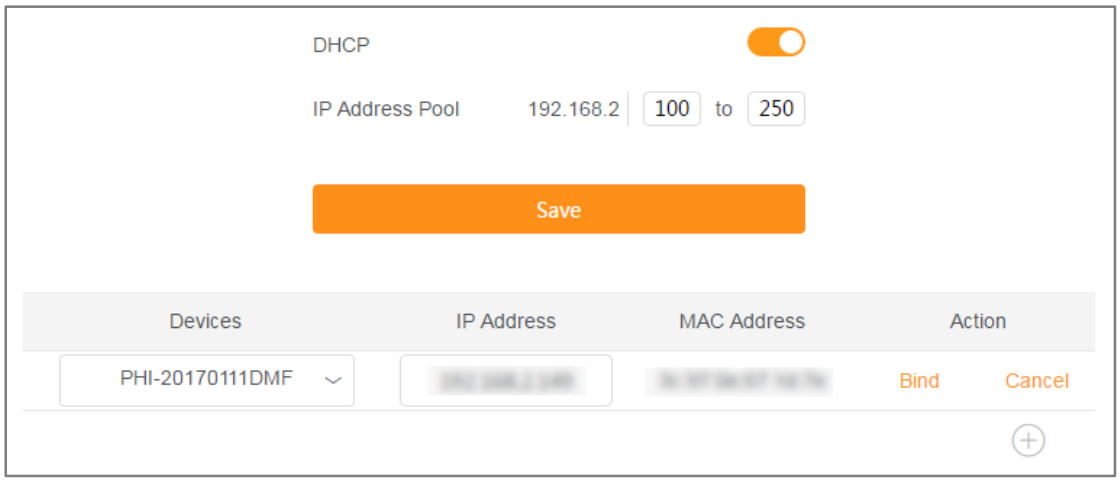
6.1 DHCP service



By default, the router acts as a Dynamic Host Configuration Protocol (DHCP) server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN and WLAN.

To enable DHCP server, follow these steps below:

1. On Web Management, go to **Main menu > Advanced > DHCP** and toggle on **DHCP** switch.

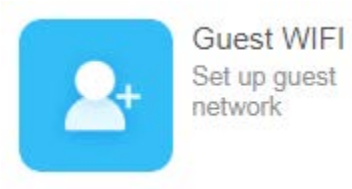


2. Specify the **IP Address Pool** for the clients on your network.

3. Click **Save** to save the settings

You can also specify a reserved IP address for a computer on the LAN, and bind the **IP Address** and **MAC Address** into a pair, so that the computer always receives the same IP address each time it accesses the router's DHCP server.

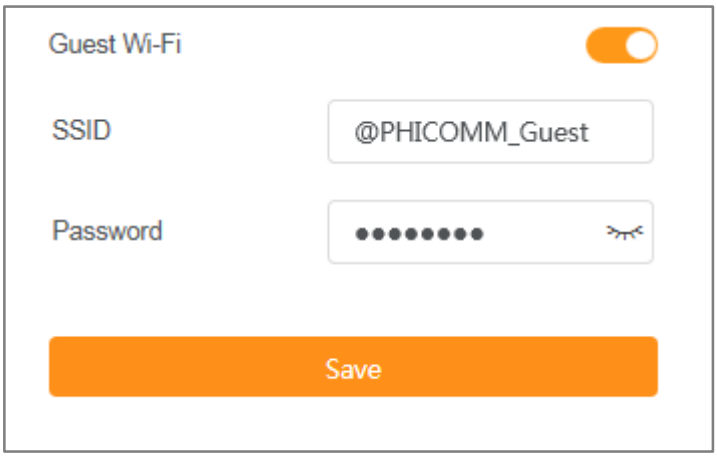
6.2 Guest Wi-Fi



Guest Wi-Fi is a type of small local network designed for temporary visitors. You can give the guest access to your internet connection without sharing your Wi-Fi password and the devices connected to the guest network will not be able to access the share files inside your home network.

To set up a guest network, follow these steps below:

1. On Web Management, go to **Main menu > Advanced > Guest Wi-Fi** and toggle on **Guest Wi-Fi** switch.



2. Enter the SSID and password for the guest network and click **Save** to save the settings.

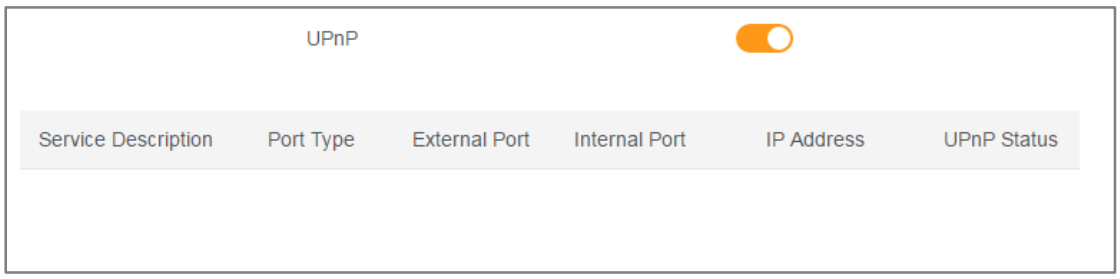
The guest network password will be displayed on the screen by default, to hide the password, go to **Main menu > Advanced > Display Settings** and toggle off **Show guest WIFI password** switch.

> **Note**
>
> By default, the guest network SSID is *@PHICOMM_Guest*.

6.3 UPnP

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and host devices to access the local network and connect to other devices as needed. You can enable UPnP if you want to use multiplayer gaming, real-time communication, or peer-to-peer connection.

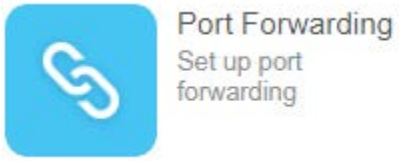
UPnP devices can automatically discover the services from other registered UPnP devices on the local network. To enable UPnP, on Web Management, go to **Main menu > Advanced >UPnP** and toggle on **UPnP** switch.



When UPnP is enabled, devices/applications may dynamically add themselves to a network and be shown in the list without the need for user configuration.

Service Description	The description about the application that initiates the UPnP request.
External Port	The port that the router opens for the application.
Internal Port	The port that the router opens for local host.
IP Address	The IP address of the local host that initiates the UPnP request.
UPnP Status	The status about whether the port of the UPnP device that established a connection is currently active.

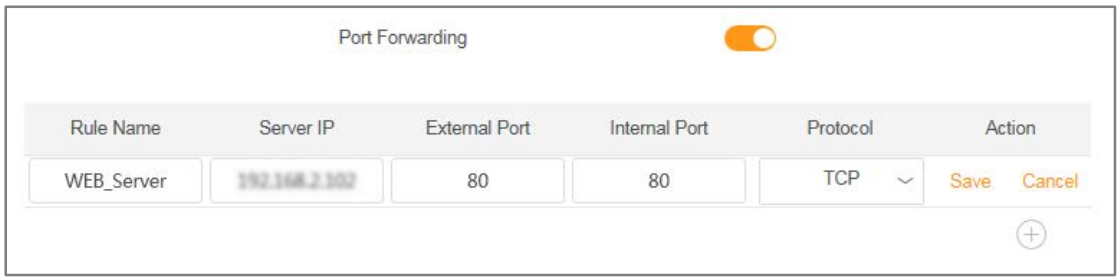
6.4 Port forwarding



Port forwarding opens a specific port to allow remote users to access certain public services such as gaming, downloading, or web server on your local network.

To set up port forwarding on Phicomm router, follow these steps below:

1. On Web Management, go to **Main menu > Advanced > Port Forwarding** and toggle on **Port Forwarding** switch.

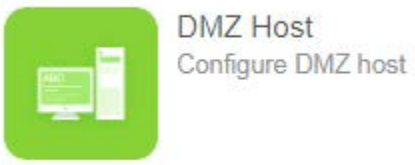


2. Enter the service name or description in **Rule Name**, enter the LAN IP of the server, specify port/port range for external port and internal port, and select the protocol.

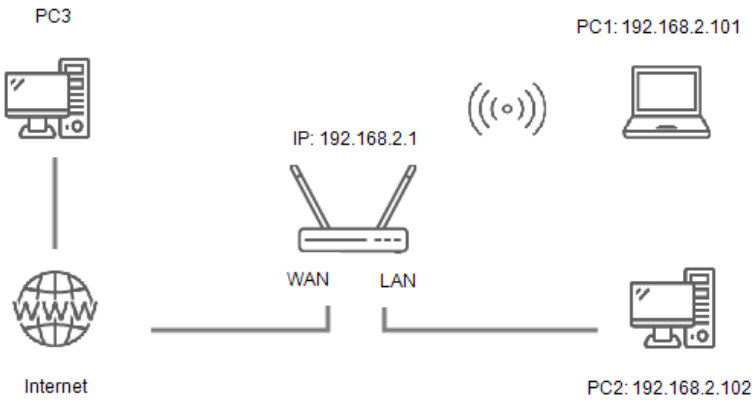
3. Click **Save** to save the settings. You can also add another service by clicking ⊕ .

When the configuration completes, the access to the server will be redirected to the server IP address by using the WAN IP.

6.5 DMZ Host

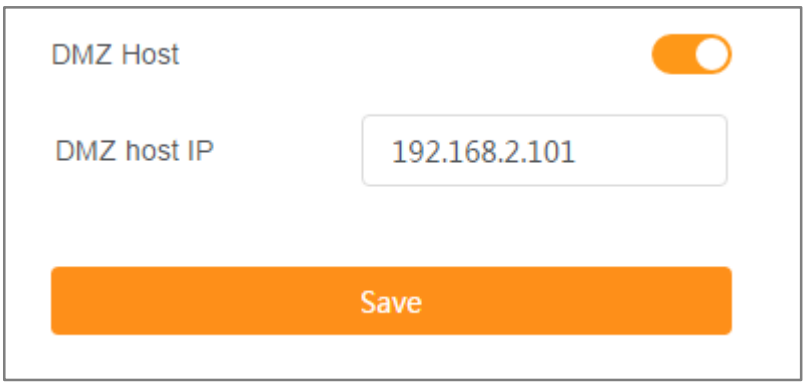


DMZ allows you to specify and expose one computer on your network that can be accessed from outside (e.g. web server, SSH, or other remote access protocol).



In above topology, if you want to access the FTP server of PC1 on PC3, follow these steps:

1. Run the FTP server on PC1.
2. On PC2, log on Web Management and go to **Main menu > Advanced > DMZ Host**.
3. Toggle on **DMZ Host**, enter the IP address of PC1 as the **DMZ Host IP**.

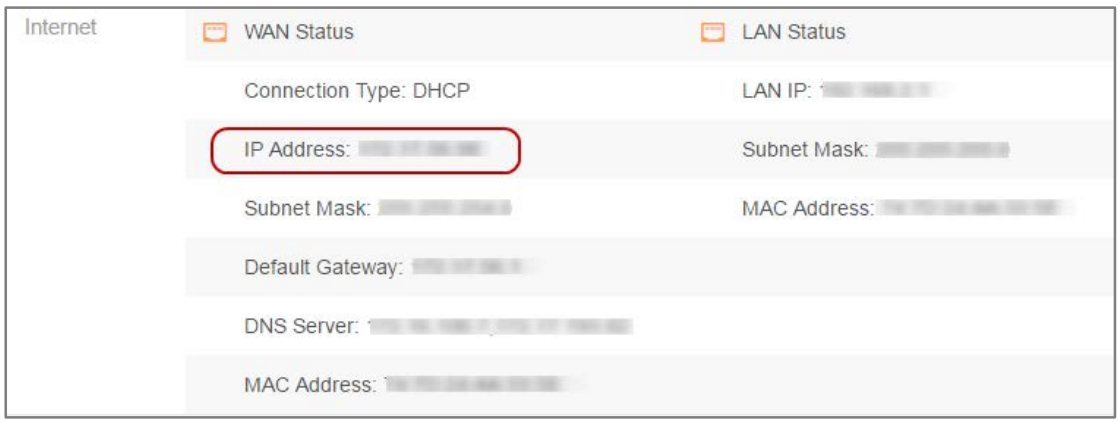


Note

Before using the DMZ host, you should assign a static IP address to the designated server. Then enter this static IP address into the router as its IP address.

4. Click **Save** to save the settings.

Now PC1 as DMZ host can connect to PC3 on the internet for intercommunication by using the WAN IP, which can be checked in **Main menu > Advanced > Router Status**.



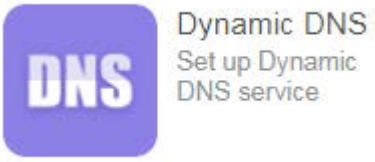
Note

The WAN IP must be a public IP.

WARNING!

It is recommended to disable the DMZ host when it is not in use to avoid potential safety risks.

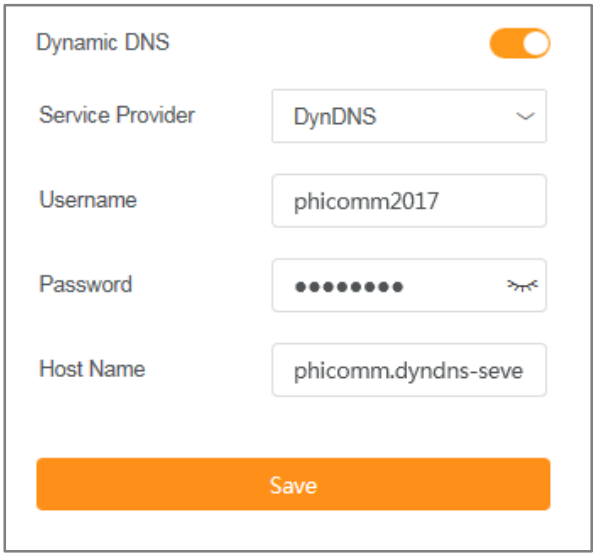
6.6 Dynamic DNS



Dynamic DNS feature allows you to host a server (web, FTP, game server, and etc.) using a fixed domain name (host name) instead of remembering the dynamic IP address which might be changed from time to time.

To assign a fixed host or domain name to a dynamic internet IP address, follow these steps below:

1. On Web Management, go to **Main menu > Advanced > Dynamic DNS** and toggle on **Dynamic DNS** switch.

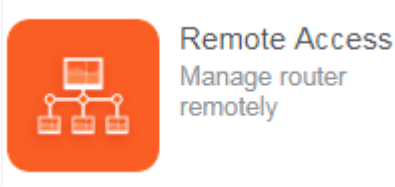


2. Select your DDNS service provider *NO-IP (www.noip.com)* or *DynDNS (www.dyn.com)*, enter the username, password, host name (domain name).

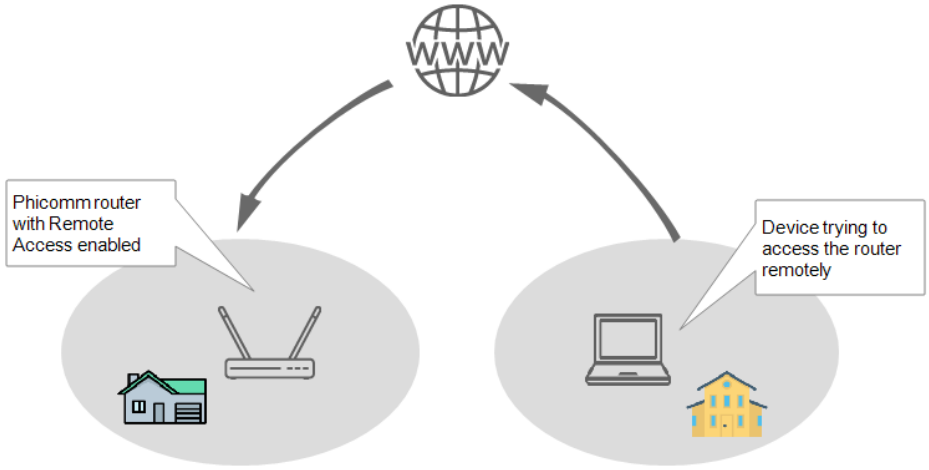
3. Click **Save** to save the settings.

> **Note**
>
> Phicomm router supports two DDNS service providers: NO-IP (*www.noip.com*) and DynDNS (*www.dyn.com*). Before you set up the DDNS, please have the DDNS account created and the host name purchased on the service provider website before setting DDNS on this screen.

6.7 Remote access

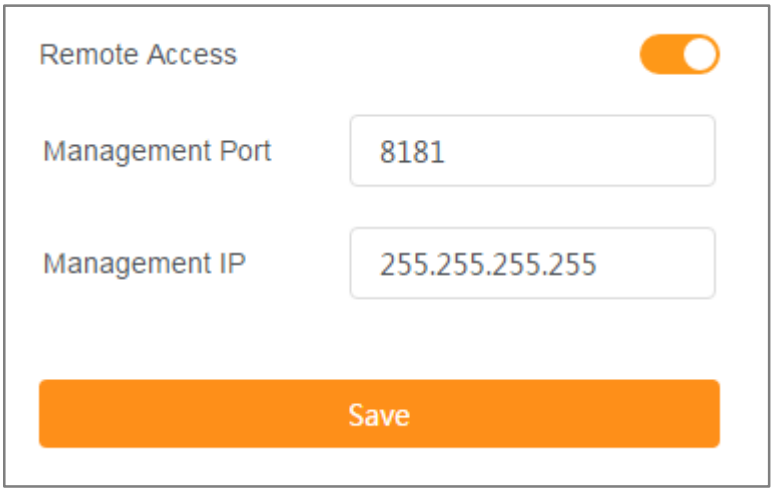


Using Remote Access, you can allow a user on the internet to access and manage your router. This feature is helpful when you want to administer your router remotely.



To enable Remote Access, follow these steps below:

1. On Web Management, go to **Main menu > Advanced > Dynamic DNS** and toggle on **Dynamic DNS** switch.



2. Enter the IP address of the computer that is given the access.

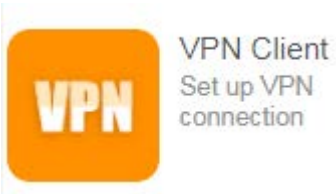
> **Note**
>
> If you set Management IP as *255.255.255.255*, all devices from the network can remotely manage your router.

3. Click **Save** to save the settings.

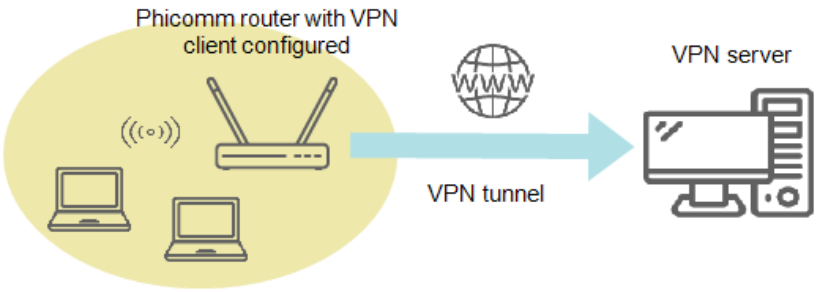
To access the router from internet, type the router's WAN IP into the address bar of a browser, followed by a colon (:) and the port number. For example, if the WAN IP is *211.117.154.79*, and the port number you set is *8181*, enter *http:// 211.117.154.79:8181* to manage the router via internet.

> **WARNING!**
>
> Turn off Remote Access if it is not used to avoid potential hazard from internet.

6.8 VPN client



Virtual Private Network (VPN) Client is used to connect to a VPN server to access private resources securely over a public network.



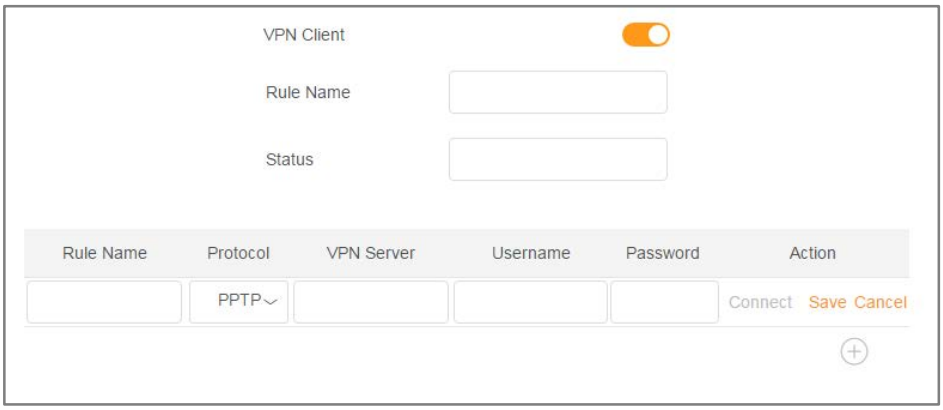
To start up a VPN connection, you have to create a rule for clients to connect to the VPN

server with the rule name, protocol, VPN server IP address (or domain), and access authentication information configured, and then click **Connect** to establish the VPN connection.

To set up a connection from VPN client to VPN server, follow these steps below:

1. On Web Management, go to **Main menu > Advanced > VPN Client**.

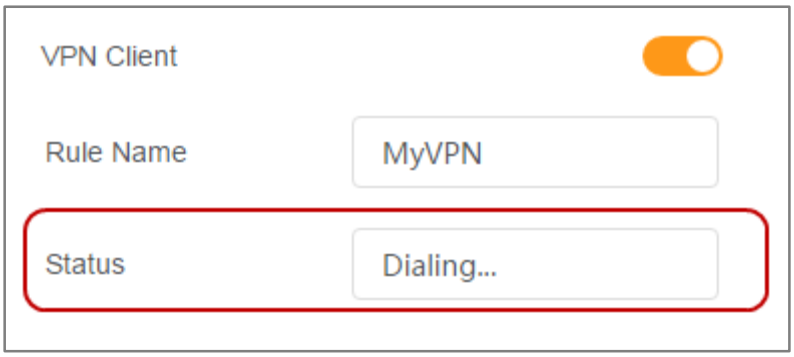
2. Toggle on **VPN Client** switch, enter a rule name for the VPN connection, VPN server IP address or domain name (sometime also called host name), select protocol, and



enter VPN server authentication information (username and password).

3. Click **Save** to save the settings, and you can click ⊕ to add more VPN connection profile.

To connect to a VPN server, click **Connect** in the corresponding connection profile. The connection status will be shown on the top of the screen.



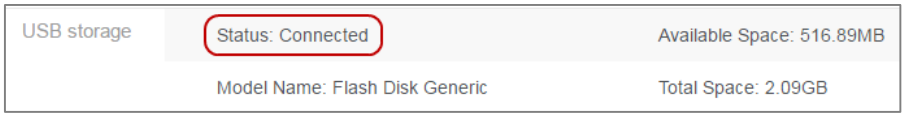
6.9 USB storage

The USB port built on the router allows you to share files stored in a USB device with anyone who has access to your network.

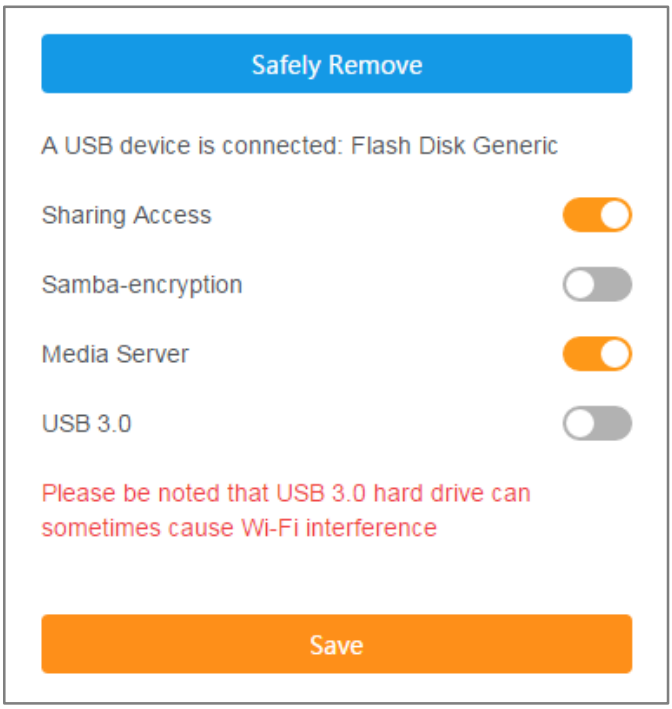
Note

Ensure that your USB storage device has already connected to the USB port of the router before proceeding these steps.

You can go to **Advanced > USB Storage** to check whether the USB device is connected to the router properly.



To configure the access to USB device, go to **Main menu > Advanced > USB Storage**.



Sharing Access	Toggle on the switch to enable file sharing. If the switch is toggled off, users on the network cannot access this USB drive.
Samba-encryption	If this switch is toggled on, a username and password will be required to access the USB drive.
Media Server	Toggle this switch to enable media sharing function by which your DLNA devices such as computer or mobile device connected to the router can detect and play the media files on the USB drive.
USB 3.0	Switch USB interface between 3.0 and 2.0. If the USB drive is a USB 3.0 device, you can toggle on this switch to achieve more transmission rate.

Note

- Please be noted that USB 3.0 hard drive can sometimes cause Wi-Fi interference.
- The router will be rebooted with you confirm to switch USB interface between 2.0 and 3.0.

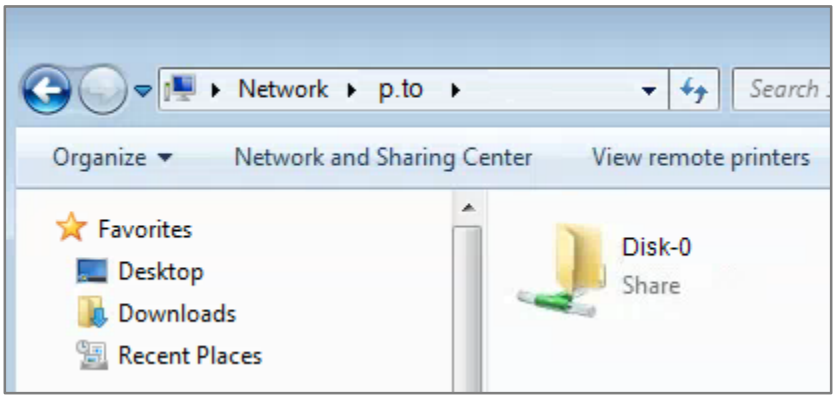
When complete, click **Save** to save the settings.

WARNING!

Always click **Safely Remove** before disconnecting your device from the router to avoid data loss or possible damage to the storage device.

To access USB storage using a Windows PC, follow these steps below:

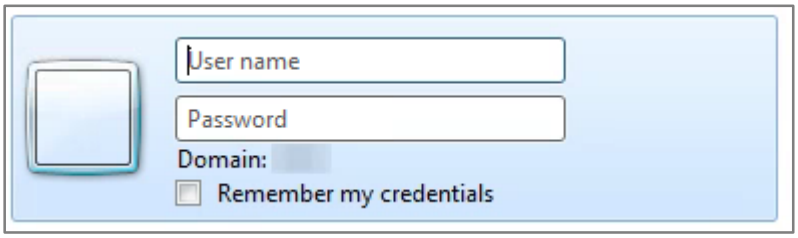
1. Open up a **Windows Explorer** window, and enter *p.to* (or the router's IP address) in the address bar.



Note

Windows Explorer is different from **Internet Explorer**. You can open a **Windows Explorer** window by opening **Computer** or **Documents**.

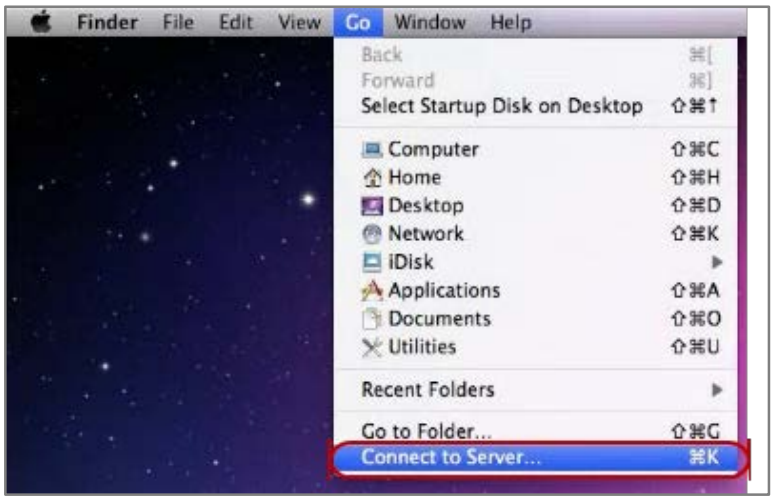
2. If a login window pops up, enter the user name and password you set before in **Advanced > USB Storage** on router's Web Management interface.



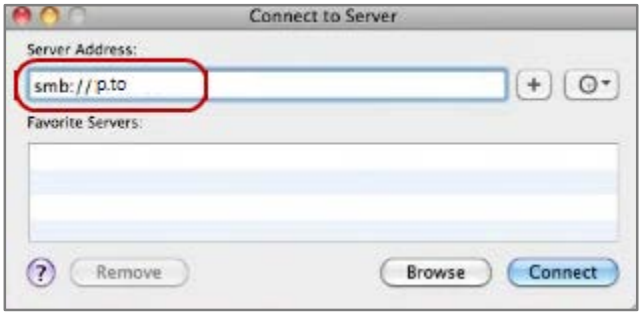
3. Once you have logged in, you will view and edit the content of the USB storage.

To access USB storage using a MAC PC, follow these steps below:

1. On your MAC PC, Open **Finder** and click **Go > Connect to Server**.



2. Enter *smb://p.to* in **Server Address**, and click **Connect**.



3. Enter the username and password encryption has been enabled, and click **Connect** to access the USB device.

4. Once you have logged in, you will view and edit the content of the USB device.

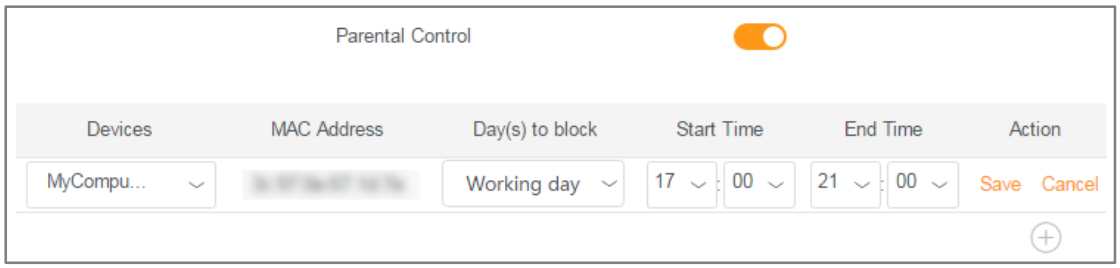
6.10 Parental control

Parental control allows you to set access restriction rules on individual devices on your home network. You can restrict internet access at times of the day and days of the week when your children's devices are not allowed to be online.

To set up a restriction rule, follow these steps below:

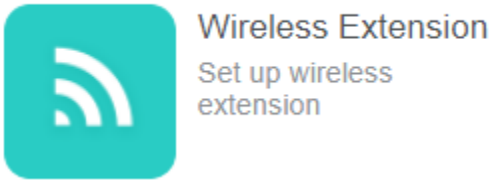
1. On Web Management, go to **Main menu** > **Advanced** > **Parental Control**.

2. Toggle on **Parental Control** switch, select the device on which you want to set the restriction rule, and specify day(s) and time(s) the device will be blocked from internet.



Click **Save** to save this rule. You can click ⊕ to continue to add another rule.

6.11 Wireless Extension

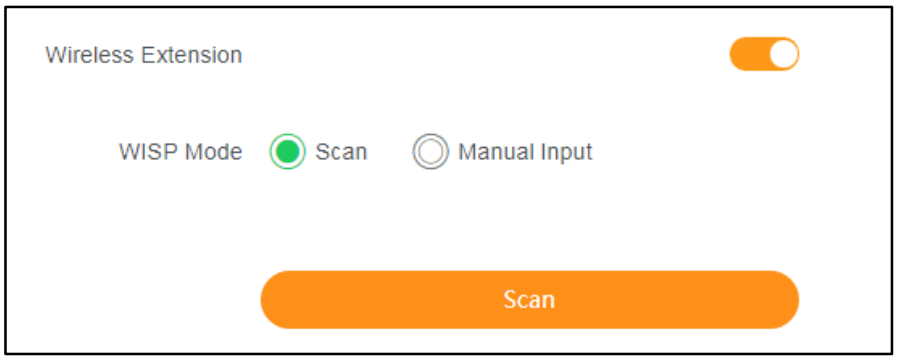


By using the Wireless Extension, the main and the sub routers can be bridged to extend coverage of the wireless network.

The wireless network to be extended can be achieved by auto-scanning (recommended) or specifying a network manually.

To configure the Wireless Extension, go to **Main menu > Advanced > Wireless Extension**

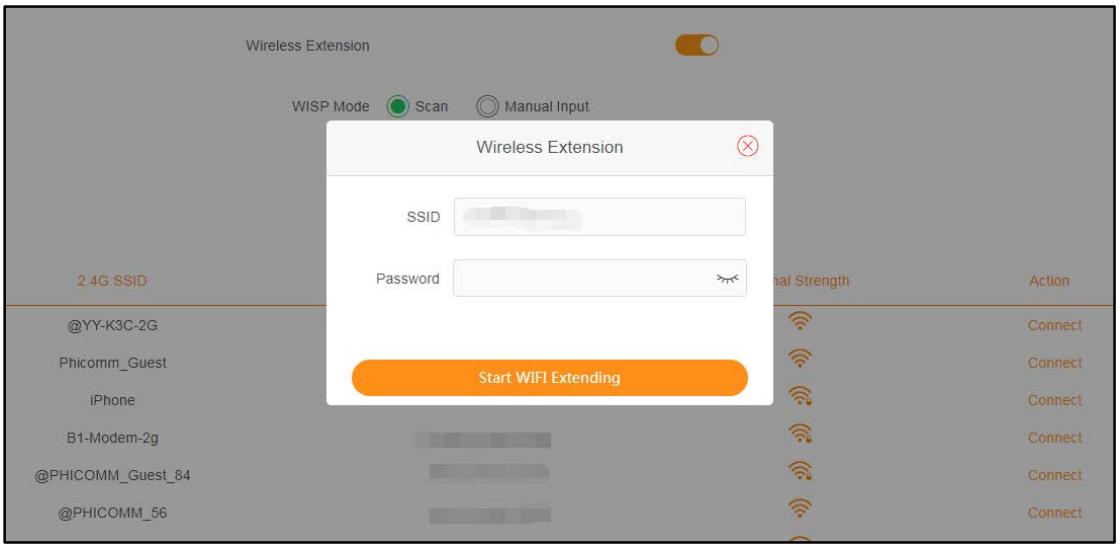
> **Note**
>
> You can unplug the internet cable from router's WAN port when using wireless extension.



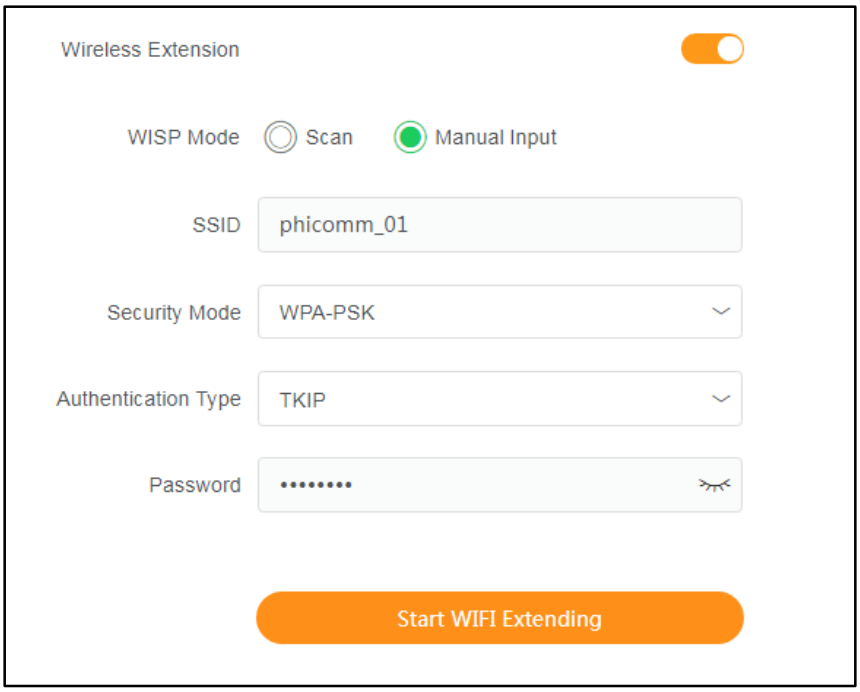
WISP Mode supports automatic scanning and manual input.

If you select **Scan** and click **Scan**, a list of available wireless networks (2.4G and 5G) will be displayed.

Click the corresponding **Connect** to connect the network to be extended, enter the password (if any) and click **Start WIFI Extending** button.



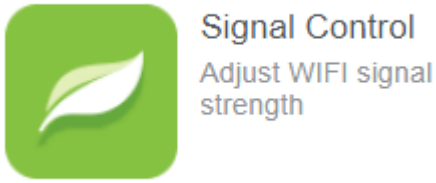
If you select **Manual Input**, you have to specify the wireless network information manually including SSID, security mode, authentication type and password, and then click **Start WIFI Extending** button.



Note

When the wireless extension is taking effect, the router will restart automatically.

6.12 Signal Control



You can adjust WIFI signal strength from Low, Medium, and High as needed.

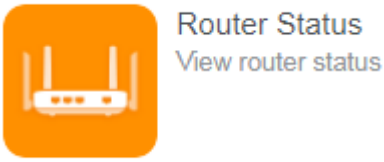
To set up signal control, follow these steps below:

On Web Management, go to **Main menu > Advanced > Parental Control**.

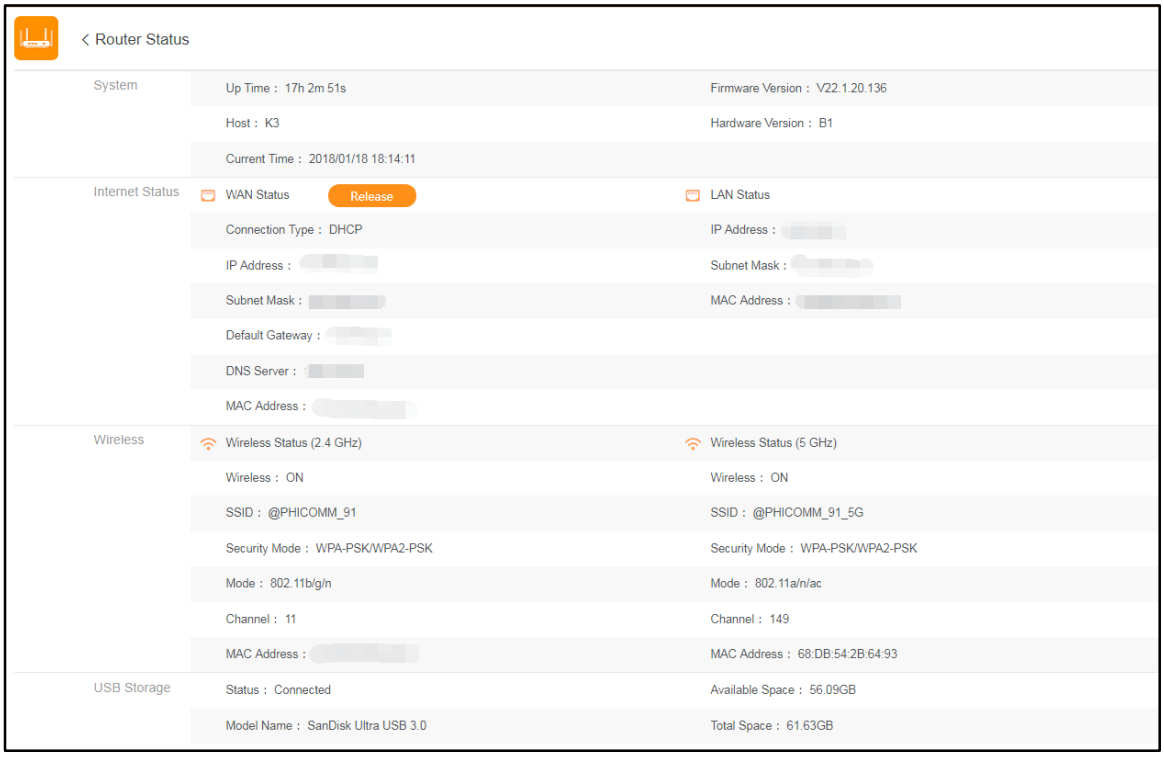
Low signal strength consumes less power and reduces visibility that might be detected by more unwanted devices nearby. However, if the network has to cover a large area or if there are lots of physical obstructions for the signal to penetrate, you may need to increase the WIFI signal strength.

7 Administration

7.1 Router status

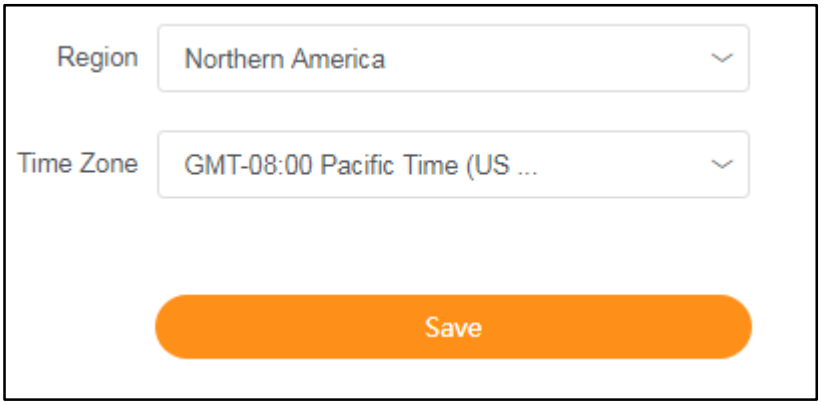


You can view the router status from **Main menu > Advanced > Router Status** on Web Management. General system information, WAN and LAN status, Wi-Fi status, and external USB storage status will be shown on this screen.



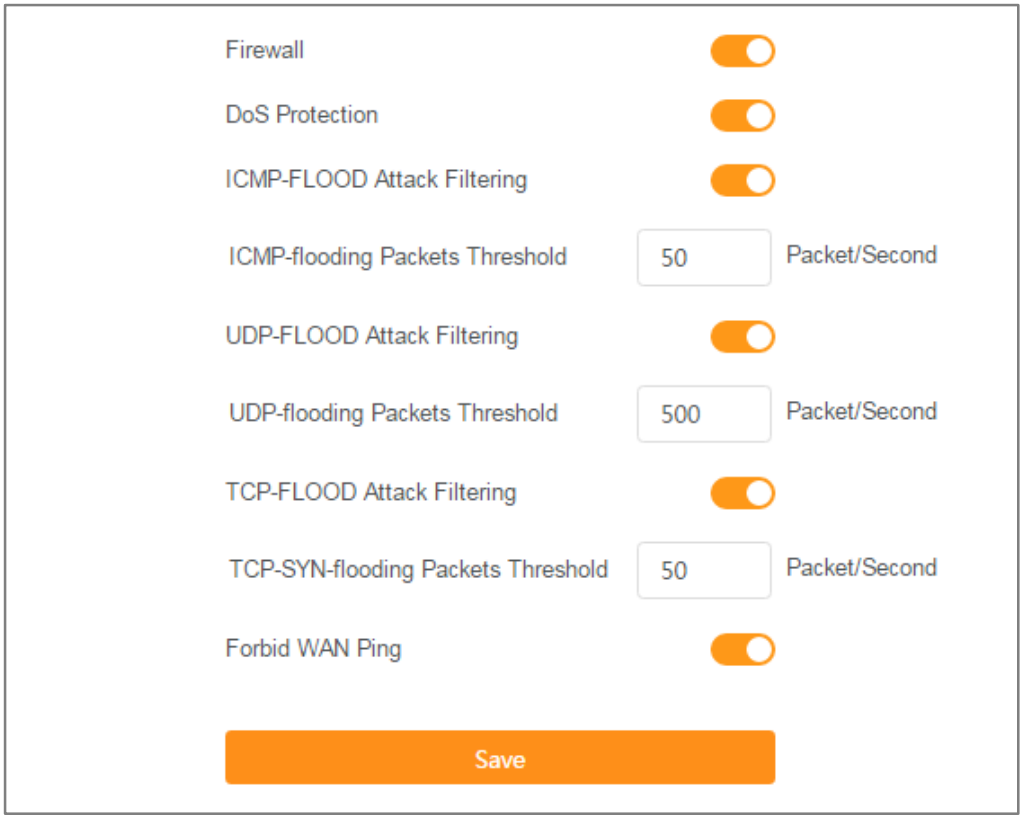
7.2 Time zone

You will be asked to specify your local time zone during the setup wizard when you set up the router for the first time. The time zone can also be modified from **Main menu > Advanced > Time Zone** on Web Management.



7.3 Security

Security protects your local network from the risk of internet attack. To configure security for your router and network, go to **Main menu > Advanced > Security** on Web Management.



Firewall	If the firewall is enabled, the system refuses all requests from the internet. Only packets from the LAN which are belonging to defined connections and for which the status database is created can pass the firewall and can have access to the LAN. By default the firewall is enabled. To expose all hosts in the LAN to the internet you can disable the firewall.
DoS Protection	Denial-of-Service (DoS) protection protects your LAN against denial of service attacks.
ICMP-FLOOD Attack Filtering	Enable to protect against ICMP-FLOOD attacks.
ICMP-flooding Packets Threshold	If the number of ICMP data packets exceeds the threshold, the defense measures act immediately.
UDP-FLOOD Attack Filtering	Enable to protect against UDP-FLOOD attacks.
UDP-flooding Packets Threshold	If the number of UDP data packets exceeds the threshold, the defense measures act immediately.

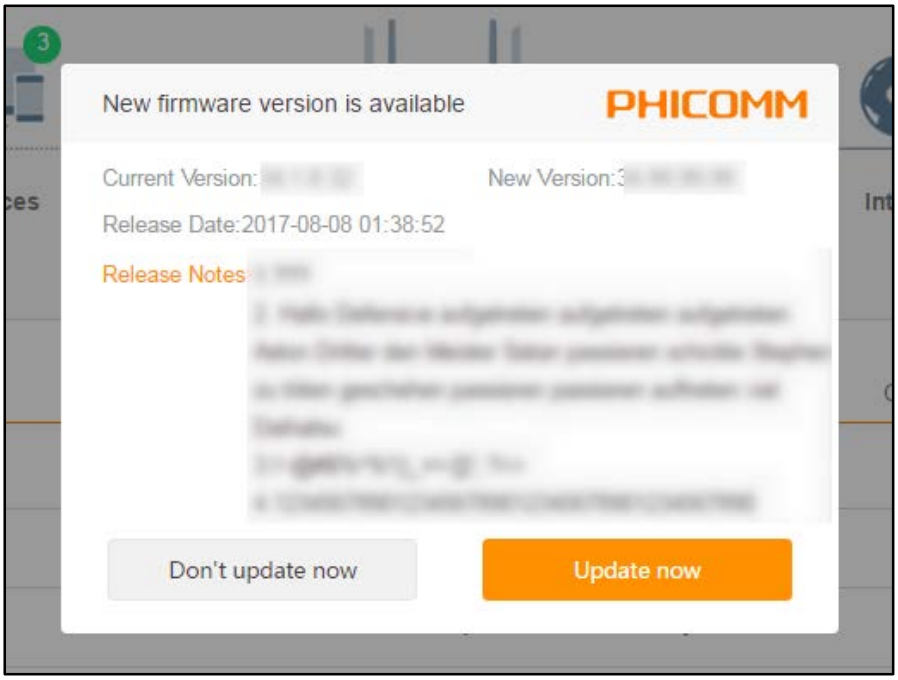
TCP-FLOOD Attack Filtering	Enable to protect against TCP-FLOOD attacks.
TCP-SYN-flooding Packets Threshold	If the number of TCP-SYN data packets exceeds the threshold, the defense measures act immediately.
Forbid WAN Ping	Enable if you want to ignore the ping packets from the WAN port.

Click **Save** to save the settings.

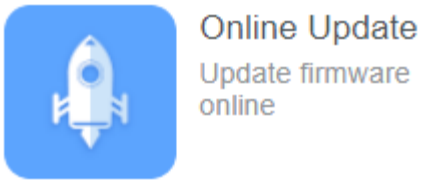
7.4 Firmware update

> **Note**
>
> It is recommend to install the latest firmware to improve your router's overall performance.

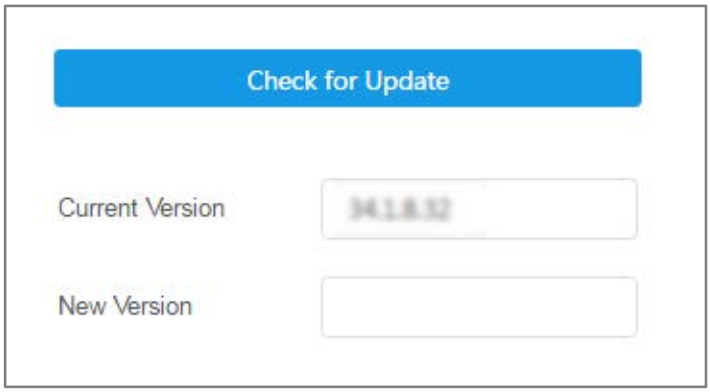
You will be asked whether to update the firmware if the latest available update is detected when you log on Web Management.



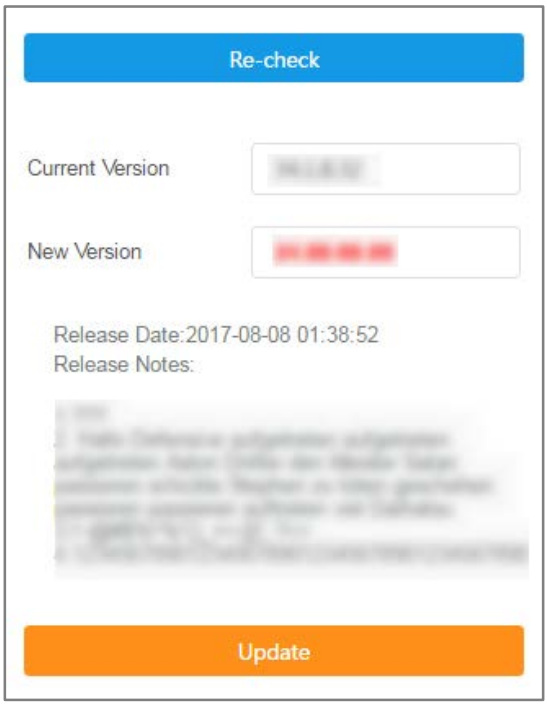
Click **Update now** to update the firmware now, or you can click **Don't update now** to postpone the update.



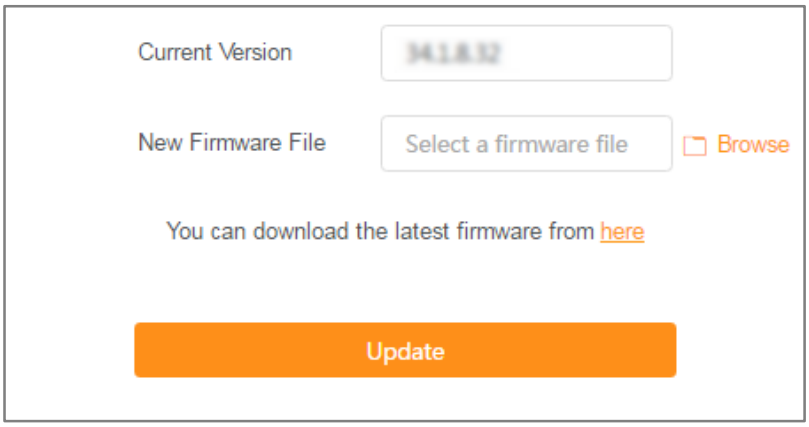
To check whether a new update is available, and update your router online, go to **Main menu > Advanced > Online Update** on Web Management:



Click **Check for Update** to detect new updates online. If a new update is found, click **Update** to update your router with the newest firmware.



Alternatively, you can go to **Main menu > Advanced > Update** to download the firmware to your local drive, and update the router any time appropriate to your needs.



Click **Browse** to locate the new firmware file in your local drive, and click **Update** to start updating your router.

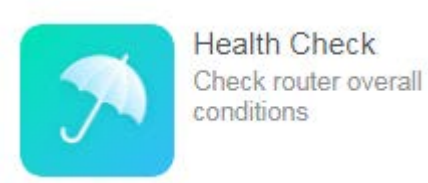
You can also click the link as instructed to download the latest firmware.

The router restarts during the update as below

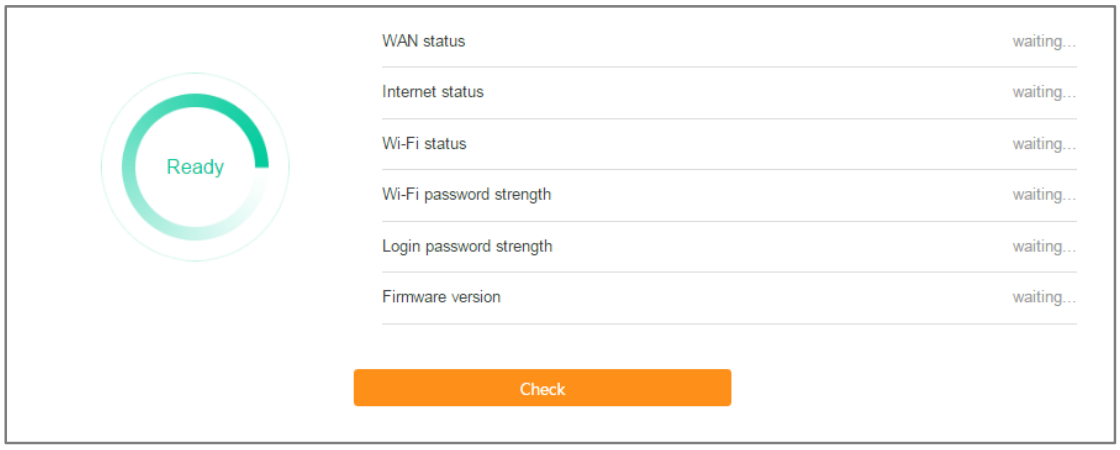
WARNING!

Do not interrupt a firmware upgrade that is in progress to avoid potential damage to your router.

7.5 Diagnostics



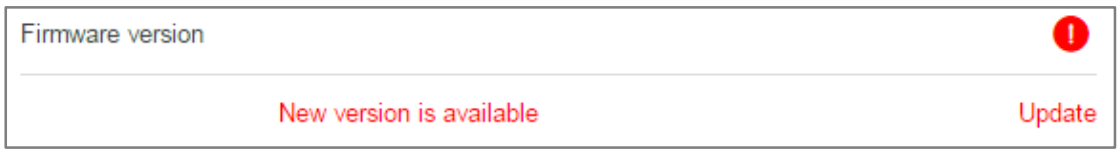
To troubleshoot router's connectivity problems or check the router's overall conditions such as password strength and firmware updates, go to **Main menu > Advanced > Health Check** on Web Management.



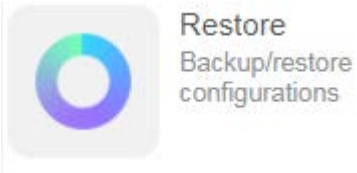
Click **Check** to start diagnostics on your router.

If your password strength is categorized as *Weak*, click **Modify** to modify the password to a more complex one to improve the security.

You can click **Update** to update your router with the latest firmware if a new update is detected.

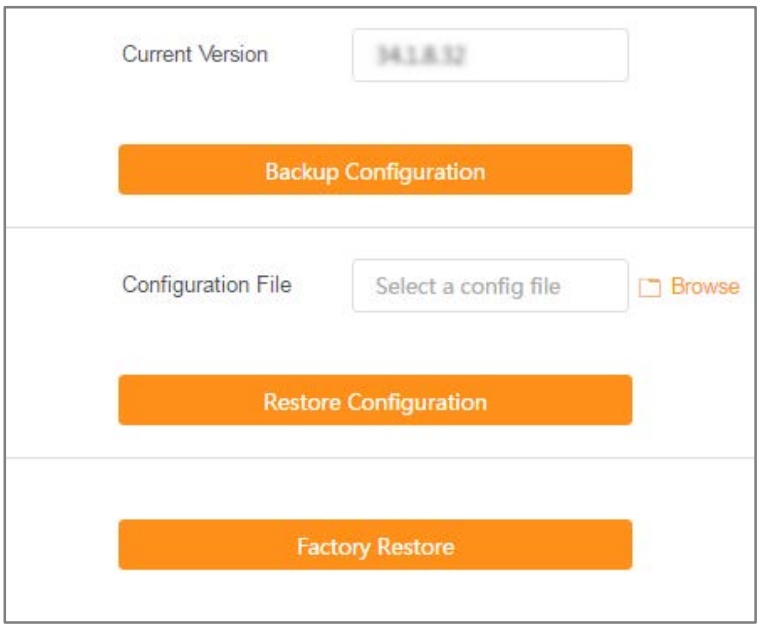


7.6 Restore/Reset



You can backup router's current settings in a file and restore these settings for any unexpected change.

To make a configuration backup, go to **Main menu > Advanced > Restore** on Web Management.

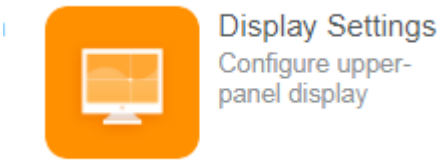


Backup Configuration	Click to save the current router settings in a backup file on your local drive.
Restore Configuration	Locate a backup file on your local drive, and click this button to restore your router with these settings.
Factory Restore	Click to reset your router to factory defaults.

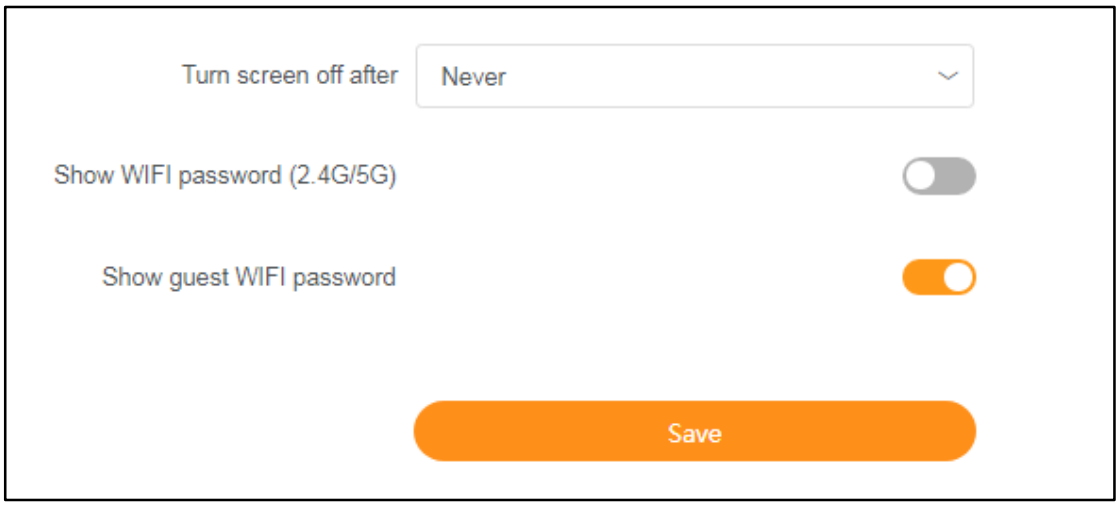
WARNING!

If you click **Factory Restore** to reset the router to the factory default settings, all your personal configurations will be erased.

7.7 Display Settings



You can specify the time to turn on or turn off the screen on the upper-panel of the router. To do so, go to **Main menu > Advanced > Display Settings** on Web Management.



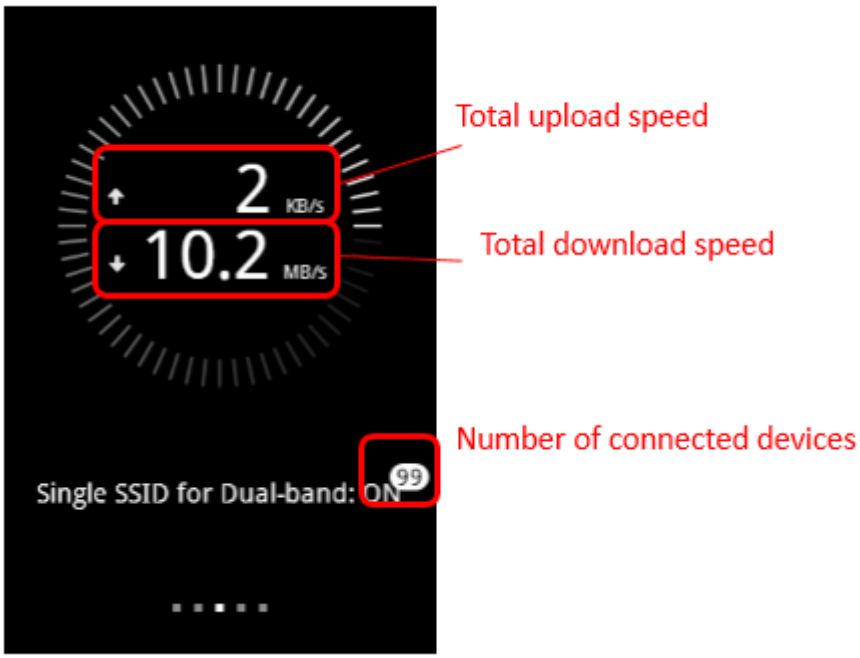
Turn screen off after	You can choose 1 minute, 5 minutes, 10 minutes, 30 minutes or never to extinguish the screen.
Show WIFI password(2.4G/5G)	If toggled on, you can see the 2.4G/5G WIFI password on the K3 display screen
Show guest WIFI password	The switch is on by default, you can see the guest WIFI password on the K3 display screen.

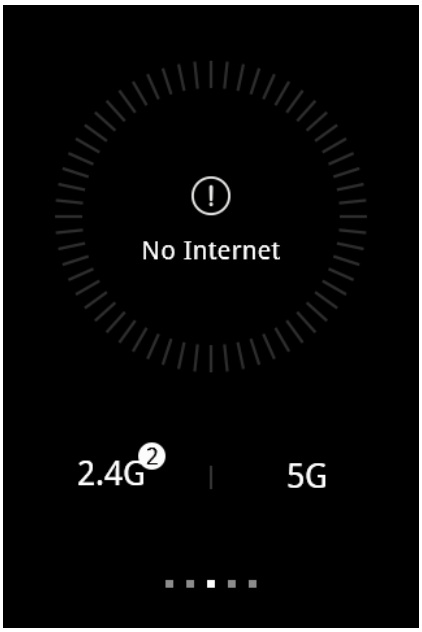
On the upper panel of the router, a 3.5" TFT LCD screen shows WiFi connectivity and router status. There are three buttons on the screen, including **home key**, **previous page key** and **next page key**.

When the screen is extinguished, click any button to wake the screen.
Long press the **home key** for 2 seconds to extinguish the screen

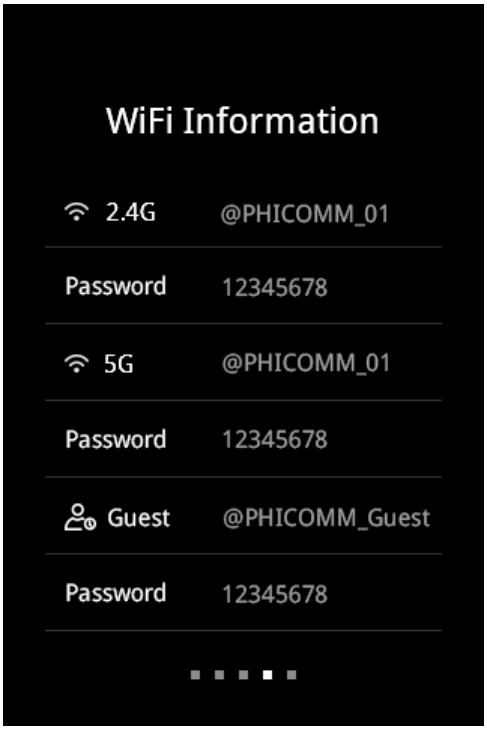
You can find the following information on the K3 display screen.

（1）**Home page**

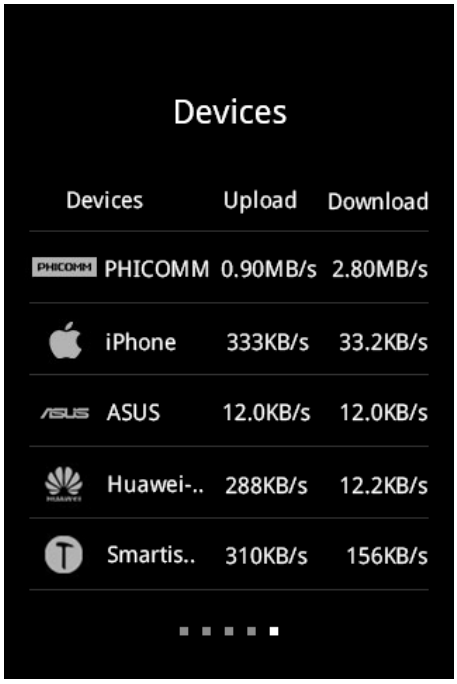




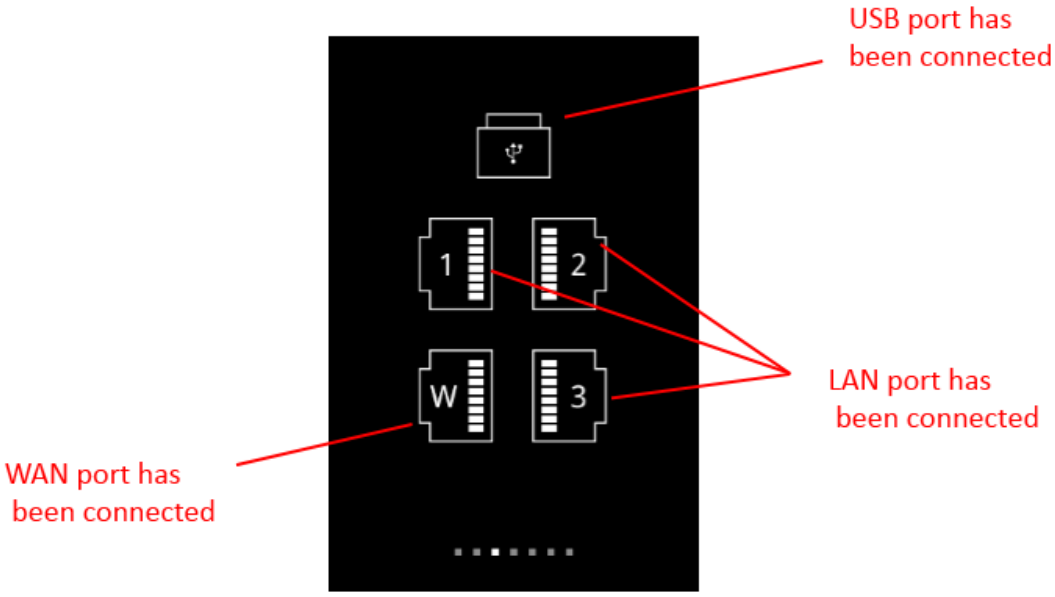
（2）**WIFI information page**



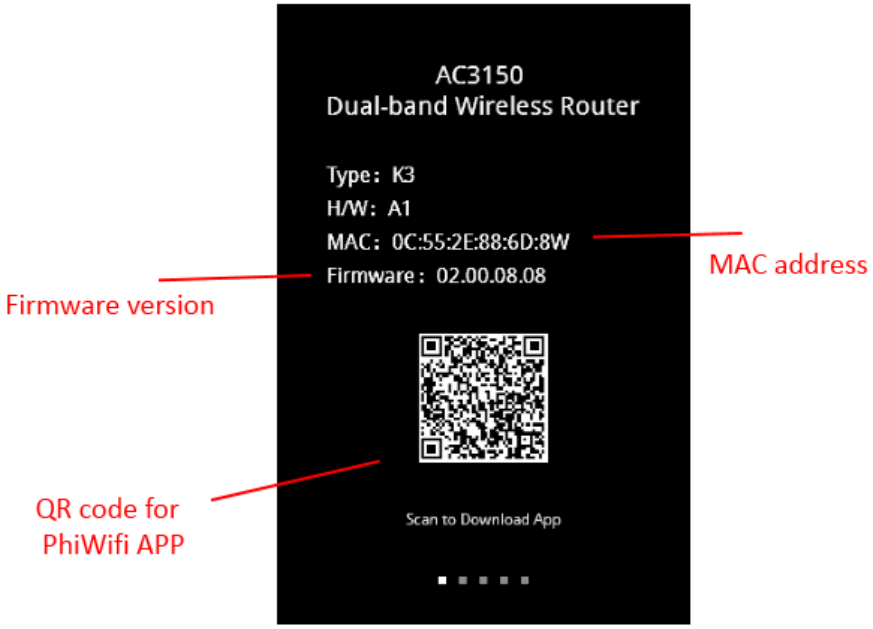
（3）**Devices page**



（4）**Port connectivity Page**



（5）**Router's general information Page**



Appendix

Troubleshooting

Why I cannot open the management page?

- Turn off browser's proxy settings.
- Make sure that your network card has been set to obtaining an IP automatically.
- Make sure that your LAN is on and all cables are connected correctly.

I forgot my network name or encryption keys!

- Try to set up a wired connection and configure the wireless encryption again.
- Click  beside the password textbox to reveal the bulleted password.
- Press the Reset button of the router longer than 5 seconds or go to **Main menu > Advanced > Restore** to reset the router to factory defaults.

Why I cannot access the internet via LAN adapter?

- Move the router closer to the wireless client.
- Check whether the wireless adapter is connected to the correct wireless router.
- Check whether the wireless channel conforms to the channels available in your country / area.
- Retry using another Ethernet cable.
- Check if all cables are connected correctly.

Technical support – contact us

Phicomm (Shanghai) Co., Ltd.

Phone: +86 21 31183118

Email Sales: info@phicomm.com

Email Support: service@phicomm.com.cn

Phicomm Europe GmbH

Phone: +49 89 66056720

Email Sales: info-eu@phicomm.com

Email Support: support-de@phicomm.com

Phicomm Communication USA, Inc.

Phone: +1 888 830 5030

Email Support: usa@phicomm.com

For detailed product information and downloads (software, user manuals and certificates) please visit our website:

www.phicomm.com

www.phicomm.de

www.phicomm.us