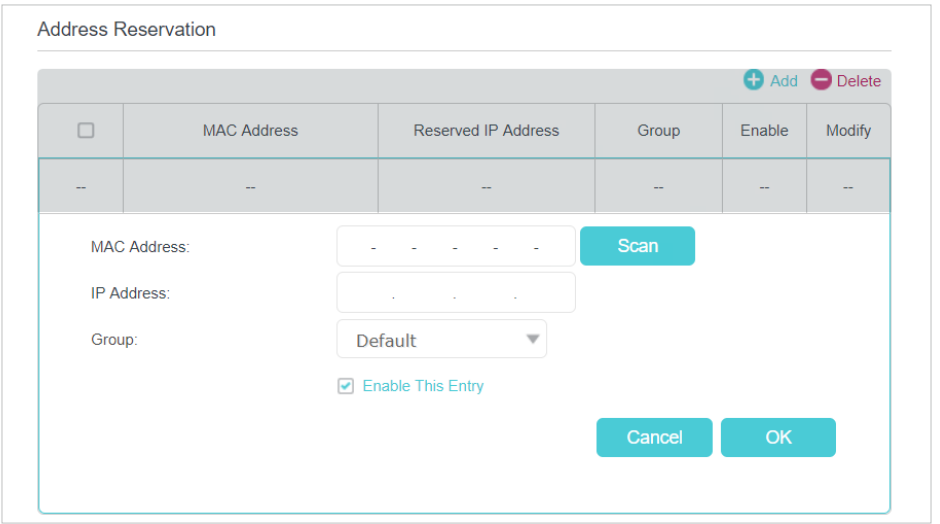
1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Network > LAN Settings page and select IPv4.
3. Scroll down to locate the Address Reservation section and click Add to add an address reservation entry for your device.



4. Enter the MAC Address of the device for which you want to reserve IP address.
5. Specify the IP address which will be reserved by the controller.
6. Keep the Enable This Entry check box selected and click OK to make the settings effective.

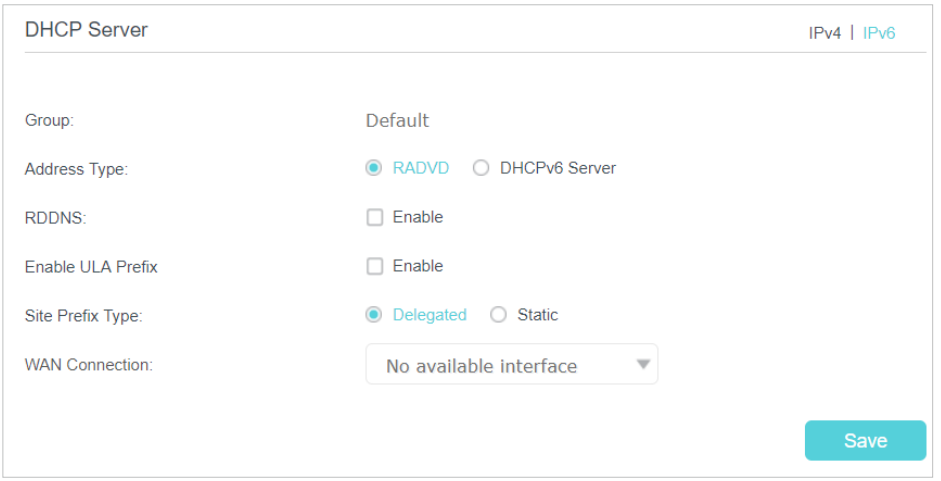
13. 2. Configure IPv6 LAN Settings

Based on the IPv6 protocol, the controller provides two ways to assign IPv6 LAN addresses:

- Configure the RADVD (Router Advertisement Daemon) address type
- Configure the DHCPv6 Server address type

13. 2. 1. Configure the RADVD Address Type

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Network > LAN Settings.
3. Select IPv6 to configure IPv6 LAN parameters.



1) Select the RADVD as the address type to make the controller assign IPv6 address prefixes to hosts.

Note:

Do not select the Enable check boxes to enable RDNSS and ULA Prefix unless required by your ISP. Otherwise you may not be able to access the IPv6 network. For more information about RDNSS and ULA Prefix, contact our technical support.

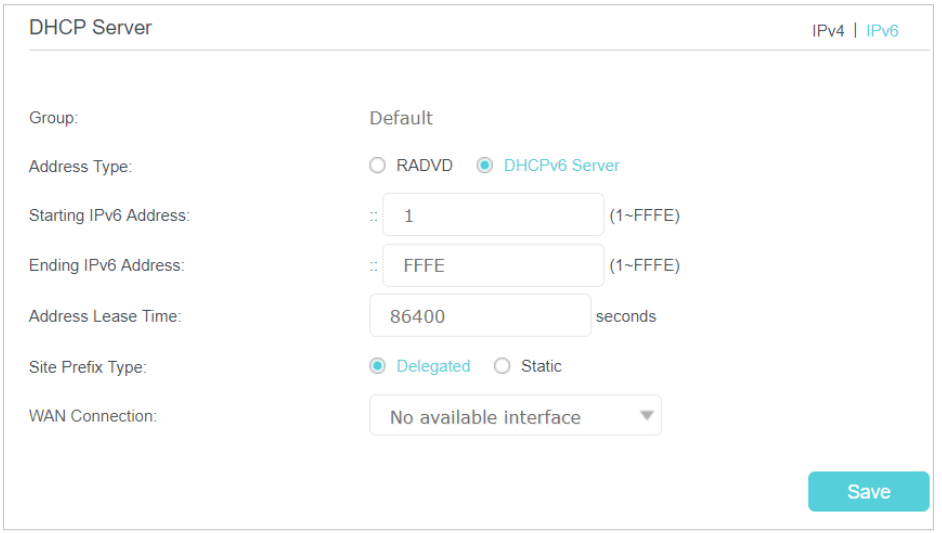
2) Keep Site Prefix Type as the default value Delegated. If your ISP has provided a specific IPv6 site prefix, select Static and enter the prefix.

3) Keep WAN Connection as the default setting.

4. Click Save to make the settings effective.

13. 2. 2. Configure the DHCPv6 Server Address Type

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Network > LAN Settings.
3. Select IPv6 to configure IPv6 LAN parameters.



1) Select the DHCPv6 Server as the address type to make the controller assign IPv6 addresses to hosts.

2) Specify the Starting/Ending IPv6 Address for the IPv6 suffixes. The controller will generate IPv6 addresses within the specified range.

3) Keep Address Lease Time as default.

4) Keep Site Prefix Type as the default value Delegated. If your ISP has provided a specific IPv6 site prefix, select Static and enter the prefix.

5) Keep WAN Connection as the default setting.

4. Click Save to make the settings effective.

13. 3. Set Up a Dynamic DNS Service Account

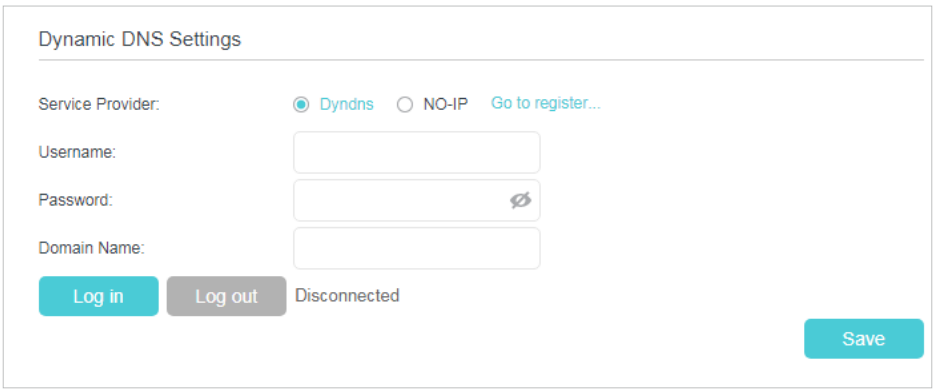
Most ISPs (Internet service providers) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on the router to allow you and your friends to access your router and local servers (FTP, HTTP, etc.) using domain name, in no need of checking and remembering the IP address.

Note: DDNS does not work if the ISP assigns a private WAN IP address (such as 192.168.1.x) to the router.

To set up DDNS, please follow the instructions below:

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Network > Dynamic DNS.
3. Select the Service Provider (Dyndns or NO-IP).

4. Log in with your DDNS account, select a service provider and click Go to register ... Enter the username, password and domain name of the account (such as lisa.ddns.net).



5. Click Log in and Save.

Tips: If you want to use a new DDNS account, please log out first, then log in with the new account.

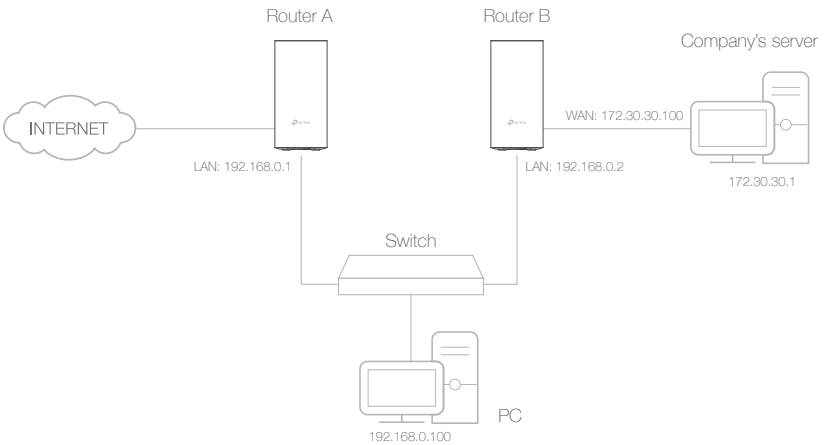
13. 4. Create Static Routes

A static route is a pre-determined path that network information must travel to reach a specific host or network. Data from one point to another will always follow the same path regardless of other considerations. Normal internet usage does not require this setting to be configured.

I want to:

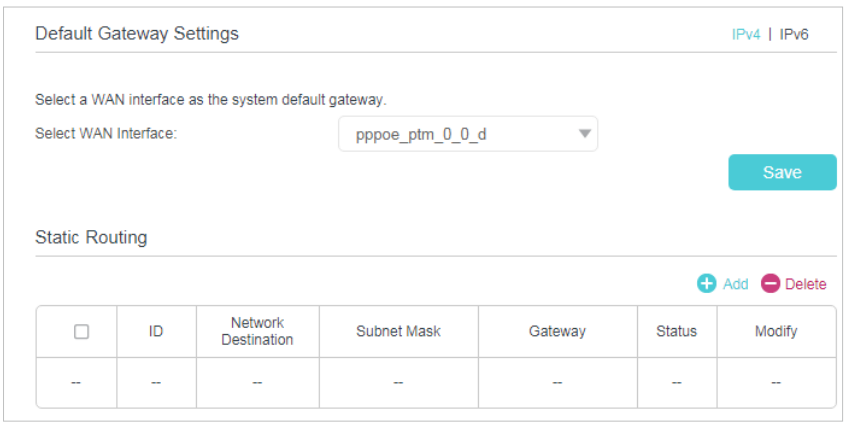
Visit multiple networks and multiple servers at the same time.

For example, in a small office, my PC can surf the internet through Router A, but I also want to visit my company's server. Now I have a switch and Router B. I connect the devices as shown in the following image so that the physical connection between my PC and my company's server is established. To surf the internet and visit my company's network at the same time, I need to configure the static routing.

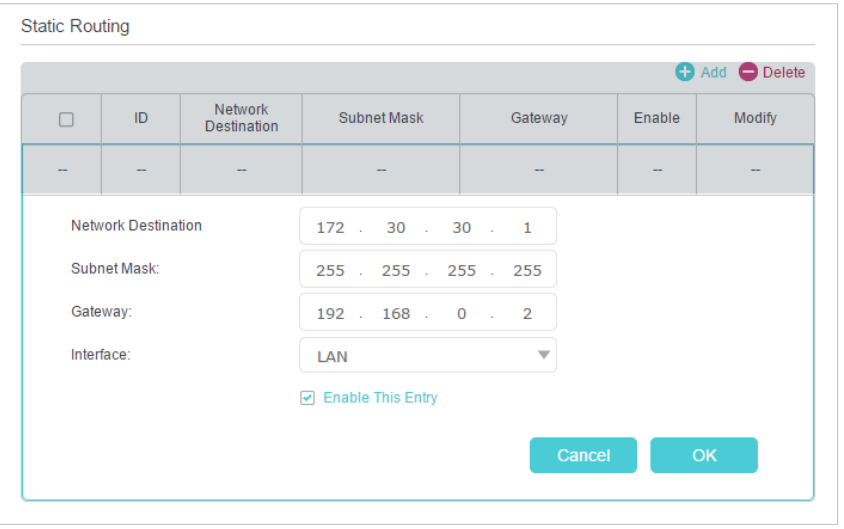


How can I do that?

1. Make sure the routers use different LAN IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit http://tplinkwifi.net, and log in with the password you set for Router A.
3. Go to Advanced > Network > Static Routing. Select your current WAN Interface and click Save.



4. Click Add to add a new static routing entry. Finish the settings according to the following explanations:



- Network Destination: The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of Router A. In the example, the IP address of the company network is the destination IP address, so here enter 172.30.30.1.
- Subnet Mask: Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enter 255.255.255.255.
- Gateway: The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the router's IP which sends out the data. In the example, the data packets will be sent to the LAN port of Router 2 and then to the Server, so the default gateway should be 192.168.0.2.
- Interface: Determined by the port (WAN/LAN) that sends out the data packets. In the example, the data is sent to the gateway through the LAN port of Router A, so LAN should be selected.

5. Select the Enable This Entry check box to enable this entry.
6. Click Save to save the settings.

Done!

Open a web browser on your PC. Enter the company server's IP address to visit the company network.

13. 5. Set Up the IPv6 Tunnel

The IPv6 Tunnel feature helps you obtain IPv6 resources based on an IPv4 WAN connection or vice versa.

IPv6 Tunnel is a transition mechanism that enables IPv6-only hosts to reach IPv4 services or vice versa and allows isolated IPv6 hosts and networks to reach each other over IPv4-only infrastructure before IPv6 completely supplants IPv4. It is a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

The controller provides four tunneling mechanisms: 6to4, 6rd, DS-Lite, and Map-T. The methods of setting up 6rd and DS-Lite tunnel are similar.

13. 5. 1. Use the Public IPv6 Tunnel Service-6to4

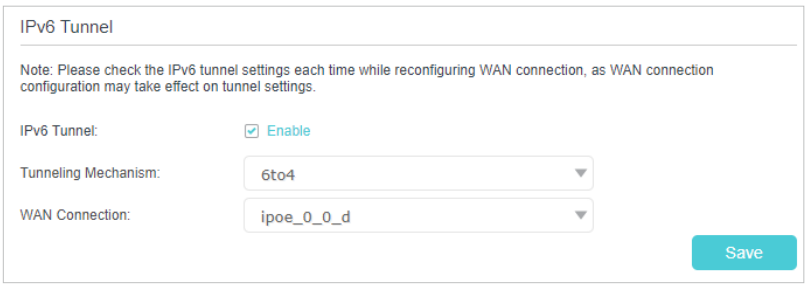
The 6to4 tunnel is a kind of public service. If there are any 6to4 servers on your network, you can use this mechanism to access IPv6 service. If your ISP provides you with an IPv4-only connection but you want to visit IPv6 websites, you can try to set up a 6to4 tunnel.

I want to:

Set up the IPv6 tunnel though my ISP doesn't provide me with the tunnel service.

How can I do that?

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Network > IPv6 Tunnel.
3. Enable IPv6 Tunnel, and select 6to4 as the tunneling mechanism and select a WAN connection from the drop-down list, then click Save.



Note:

If there is no available WAN connection to choose, make sure you have connected to the internet and the connection type is not Bridge.

Done!

Now you can visit the IPv6 websites with the 6to4 tunnel.

Note:

If you still can't access IPv6 resources, it may means that no 6to4 public server was found in your network. You can contact your ISP to sign up for IPv6 connection service.

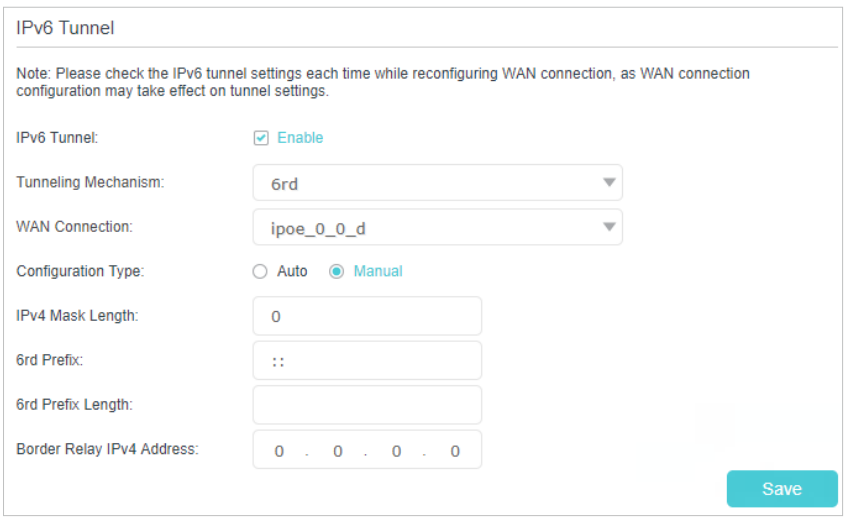
13. 5. 2. Specify the 6rd Tunnel with Parameters Provided by Your ISP

I want to:

Specify the 6rd tunnel with the parameters provided by my 6rd tunnel service provider.

How can I do that?

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Network > IPv6 Tunnel.
3. Enable IPv6 Tunnel, and select 6rd as the tunneling mechanism and select a WAN connection from the drop-down list.
4. According to the parameters provided by your ISP, choose Auto or Manual. More parameters are needed if you choose Manual.
5. Click Save.



Note:

If there is no available WAN connection to choose, make sure you have connected to the internet and the connection type is not Bridge.

Done!

Now you can visit the IPv6 websites with the 6rd tunnel.

Tips:

The ways to set up DS-Lite and Map-T tunnel are similar to that of 6rd tunnel. If you are provided with an IPv6-only WAN connection and have signed up for DS-Lite tunnel service, specify the DS-Lite tunnel by referring to the steps above.

13. 6. Specify Wireless Settings

13. 6. 1. Change Basic Wireless Settings

The router's wireless network name (SSID) and password, and security option are preset in the factory. The preset SSID and password can be found on the product label. You can customize the wireless settings according to your needs.

Visit http://tplinkwifi.net, and log in with the password you set for the controller.

➢ **To enable or disable the wireless function:**

1. Go to Basic > Wireless.
2. The wireless radio is enabled by default. If you want to disable the wireless function of the controller, just clear the Enable check box. In this case, all the wireless settings will be invalid.

➢ **To change the wireless network name (SSID) and wireless password:**

1. Go to Basic > Wireless.
2. Enter a new SSID (32 characters at most) in the Network Name (SSID) field and a new password in the Password field and click Save. The SSID and password are case-sensitive.

Note:
If you use a wireless device to change the wireless settings, you will be disconnected after the new settings are effective. Please write down the new SSID and password for future use.

➢ **To hide SSID:**

1. Go to Basic > Wireless.
2. Select Hide SSID, and your SSID will not be broadcast. Your SSID won't display on your wireless devices when you scan for local wireless networks and you need to manually join the network.

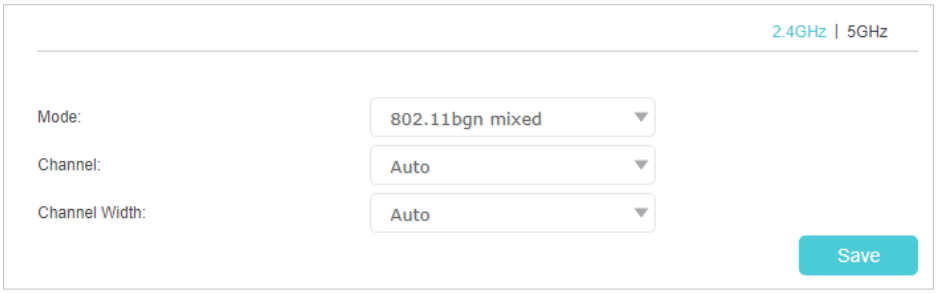
➢ **To enable or disable band steering:**

Band Steering allows each of the device's wireless bands to use the same wireless settings. The device can balance network demand and assign devices to the optimum band.

1. Go to Advanced > Wireless > Wireless Settings.
2. Turn on or off the Band Steering.

➢ **To change the mode or channel:**

1. Go to Advanced > Wireless > Wireless Settings, and select 2.4GHz or 5GHz you want to change.



2. Select the wireless network mode or channel and click Save to make the settings effective.

Mode: Select the desired transmission mode.

- 802.11n only: Select only if all of your wireless clients are 802.11n devices.
- 802.11gn mixed: Select if you are using both 802.11g and 802.11n wireless clients.
- 802.11bgn mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

Note: When 802.11n only mode is selected, only 802.11n wireless stations can connect to the controller. It is strongly recommended that you select 802.11b/g/n mixed, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the controller.

- 802.11ac only (5GHz): Select only if all of your wireless clients are 802.11ac devices.
- 802.11ac/n mixed (5GHz): Select if you are using a mix of 802.11n and 802.11ac wireless clients.
- 802.11a/n/ac/mixed (5GHz): Select if you are using a mix of 802.11a, 802.11n, and 802.11 ac wireless clients. It is strongly recommended that you select this option.

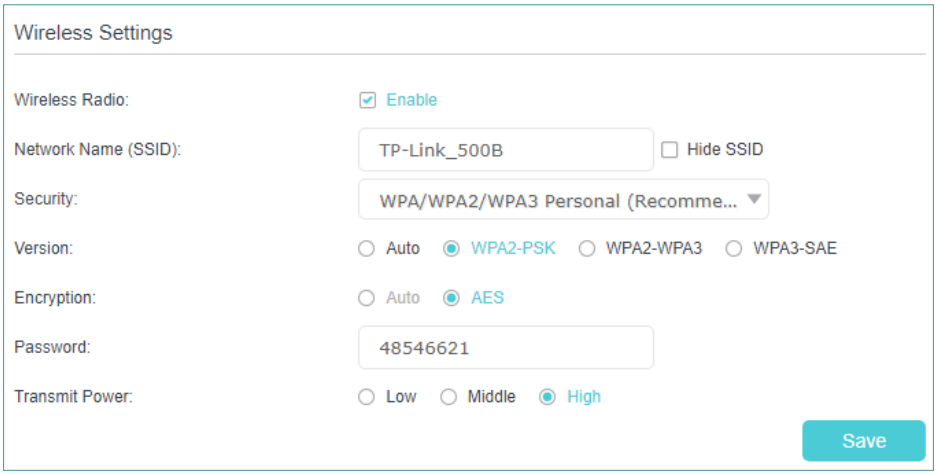
Channel: Select the channel you want to use from the drop-down list. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

Channel Width: Select the channel width from the drop-down list. The default setting is Auto, which can adjust the channel width for your clients automatically.

Note: These settings are available only when you turned off the Band Steering.

➢ **To change the security option:**

1. Go to Advanced > Wireless > Wireless Settings.

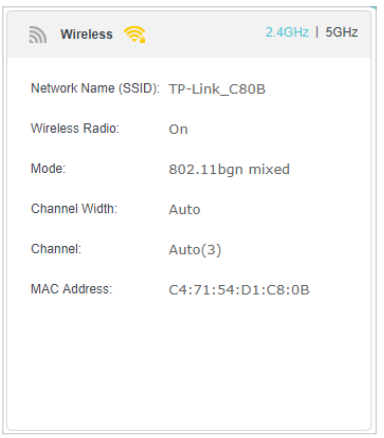


2. Select an option from the Security drop-down list and configure the related parameters. The router provides threr options, No Security, WPA/WPA2/WPA3 personal (Recommended), and WPA/WPA2 enterprise. WPA3 is the latest standard and the security level is the highest. We recommend you don't change the default settings unless necessary.
3. Click Save to make the settings effective.

13. 6. 2. View Wireless Information

➢ **To view the detailed wireless network settings:**

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Status page. You will find the Wireless panel.
3. Click 2.4GHz or 5GHz to view the wireless details.



Tips: You can also see the wireless details by clicking the Online Devices icon on Basic> Network Map.

➢ **To view the detailed information of the connected wireless clients:**

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.

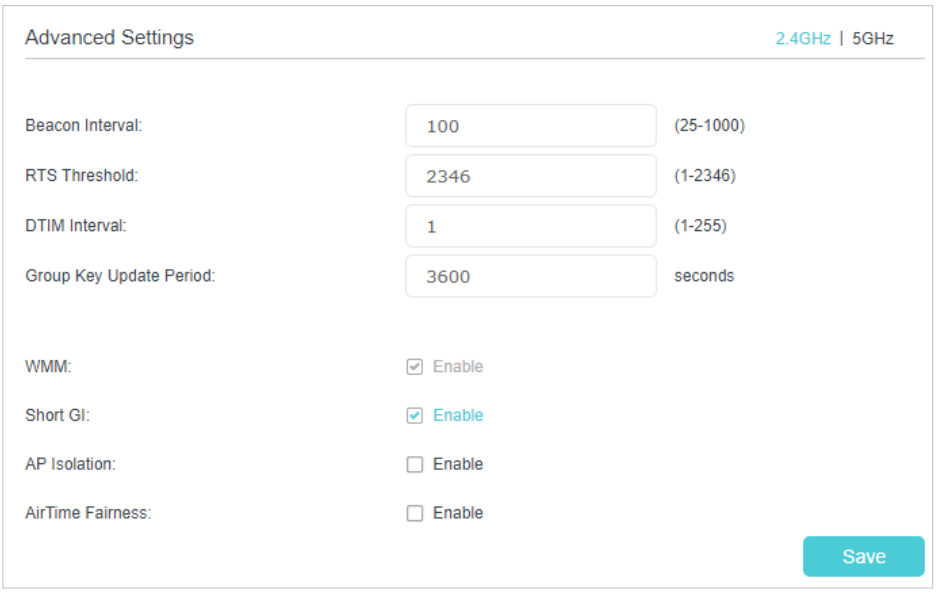
2. Go to Advanced > Wireless > Statistics page.
3. You can view the detailed information of the wireless clients, including its connection type and security option as well as the packets transmitted.

Tips: You can also see the wireless details by clicking the Online Devices icon on Basic> Network Map.

13. 6. 3. Advanced Wireless Settings

Advanced wireless settings are for those who want more network controls. If you are not familiar with the settings on this page, it's strongly recommended that you keep the provided default values; otherwise it may result in lower wireless network performance.

1. Visit http://tplinkwifi.net, and log in with the password you set for your router.
2. Go to Advanced > Wireless > Advanced Settings.



- Beacon Interval: Enter a value between 100 and 1000 in milliseconds to determine the duration between which beacon packets are broadcast by the router to synchronize the wireless network. The default is 100 milliseconds.
- RTS Threshold: Enter a value between 1 and 2346 to determine the packet size of data transmission through the router. By default, the RTS (Request to Send) Threshold size is 2346. If the packet size is greater than the preset threshold, the router sends Request to Send frames to a particular receiving station and negotiates the sending of a data frame, or else the packet will be sent immediately.
- DTIM Interval: Enter a value between 1 and 255 to determine the interval of the Delivery Traffic Indication Message (DTIM). 1 indicates the DTIM Interval is the same as Beacon Interval.
- Group Key Update Period: Enter the number of seconds to control the time interval for the encryption key automatic renewal. The default is 0, indicating no key renewal.

- WMM: This feature guarantees the packets with high-priority messages being transmitted preferentially. WMM is enabled compulsively under 802.11n or 802.11ac mode.
- Short GI: This feature is enabled by default and recommended to increase the data capacity by reducing the Guard Interval (GI) time.
- AP Isolation: Select this check box to enable the AP Isolation feature that allows you to confine and restrict all wireless devices on your network from interacting with each other, but still able to access the internet. AP isolation is disabled by default.
- AirTime Fairness: Enable this feature when you want to sacrifice some of the networking time from the slow devices, so that your faster devices can achieve better quality of service.
- Fast Roaming (802.11r): Select the Enable check box to enable the Fast Roaming(802.11r) feature that wireless clients reconnect fast in EasyMesh network. When EasyMesh disabled, this function will not take effect.

13. 7. Use WPS for Wireless Connection

You can use WPS (Wi-Fi Protected Setup) to add a new wireless device to your existing network quickly and easily.

Method 1: Use the WPS button

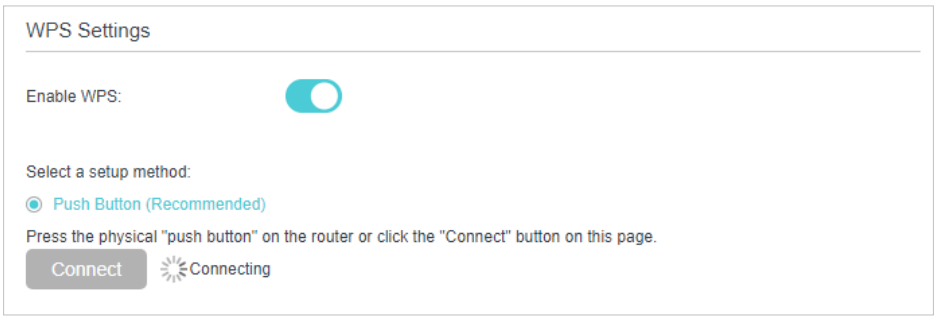
Use this method if your client device has a WPS button.

1. Press the WPS button of the controller.
2. Press the WPS button of the client device directly.
3. The status LED will flash blue fast for about 2 minutes during the WPS process.

Method 2: Use the WPS button on the web management page

Use this method if your client device has a WPS button.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Wireless > WPS, and locate the WPS Settings section.

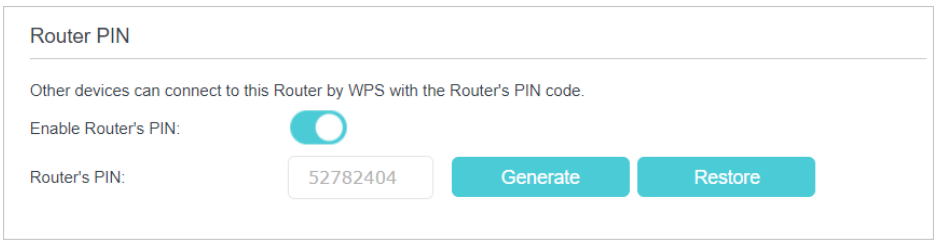


3. Make sure the Enable WPS is turned on, and then click Connect.
4. Press the WPS button of the client device directly.
5. The status LED may flash blue fast for about 2 minutes during the WPS process.
6. Connect successfully will appear after the Connect button, which means the client device has successfully connected to the controller.

Method 3: Enter the controller's PIN on your client device

Use this method if your client device asks for the controller's PIN.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Wireless > WPS, locate the Router PIN section and select 2.4GHz or 5GHz according to your needs.



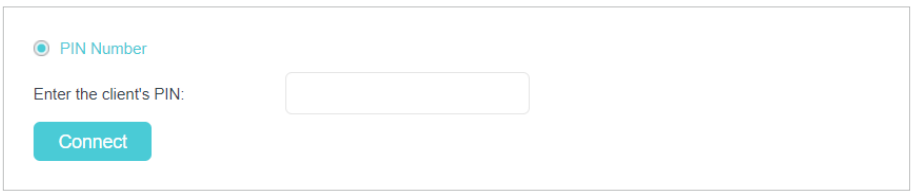
3. Make sure the Enable Router's PIN is turned on, and take a note of the current PIN of the controller. You can also click the Generate button to get a new PIN.
4. On the client device, enter the controller's PIN. (The default PIN is also printed on the label of the controller.)
5. The status LED may flash blue fast for about 2 minutes during the WPS process.

Note:

The WPS function cannot be configured if the wireless function of the controller is disabled. Please make sure the wireless function is enabled before configuring the WPS.

Method 4: Enter the client device's PIN on the controller

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Wireless > WPS, locate the WPS Settings section and select 2.4GHz or 5GHz according to your needs.
3. Make sure the Enable WPS is turned on, and then select PIN Number.



4. Enter the client device's PIN, and then click the Connect button.

5. Connect successfully will appear after the Connect button, which means the client device has successfully connected to the controller.

Chapter 14

Manage Your Controller

This chapter introduces how to change the system settings and administrate your controller's network.

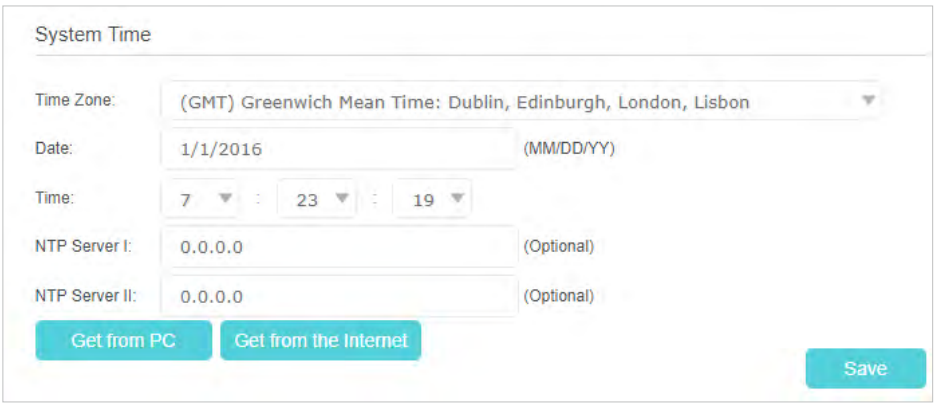
It contains the following sections:

14. 1. Set System Time

System time is the time displayed while the controller is running. The system time you configure here will be used for other time-based functions like Parental Controls and Wireless Schedule. You can manually set how to get the system time.

Follow the steps below to set your system time.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > Time Settings page.



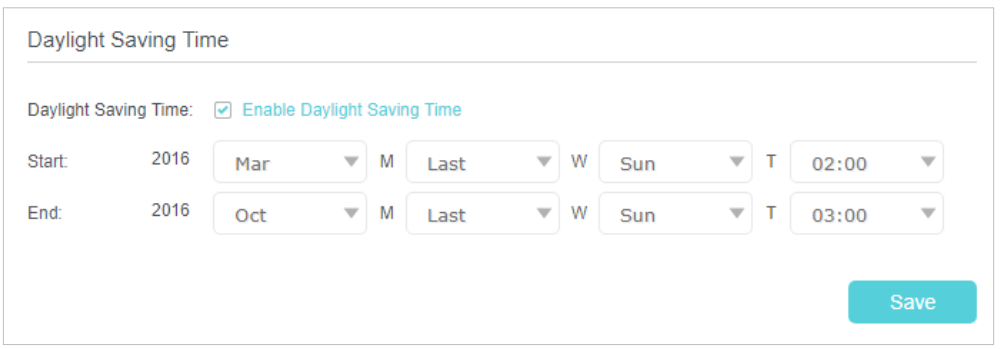
3. Configure the system time using the following methods:

   Manually: Select your time zone, enter the date and select the local time.

   Get from PC: Click this button if you want to use the current time of your PC.

   Get from the Internet: Click this button if you want to get time from the internet. Make sure your controller can access the internet before you select this way to get system time.

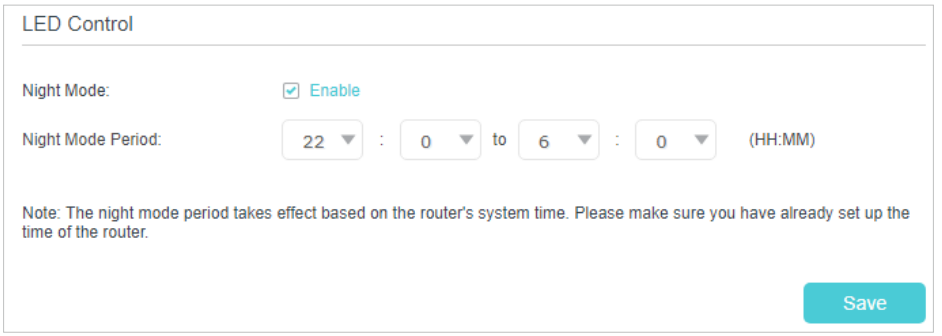
4. Click Save to make the settings effective.
5. After setting the system time, you can set Daylight Saving Time according to your needs. Select the Enable Daylight Saving Time check box to enable daylight saving, set the start and end time, and then click Save to make the settings effective.



14. 2. Control LED

The controller LED indicates controller activities and behaviors. You can turn on or turn off the controller from the management web-page.

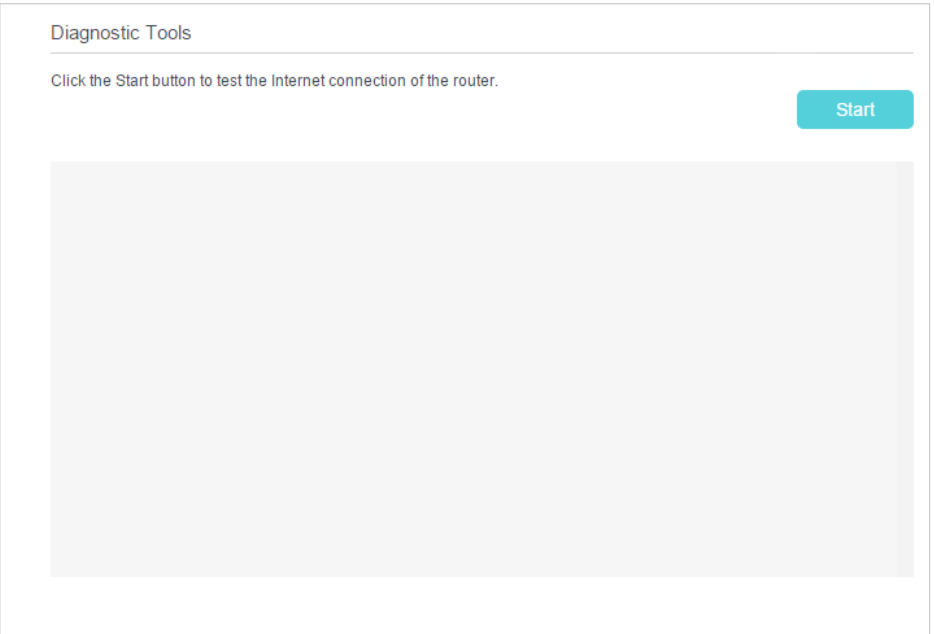
1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > LED Control, and enable Night Mode.
3. Specify the Night Mode Period according to your need, and the LEDs will be off during this period.
4. Click Save to make the settings effective.



14. 3. Test Internet Connectivity

Diagnostics is used to test the connectivity between the controller and the host or other network devices.

1. Visit http://tplinkwifi.net, and log in with the password you set for your controller.
2. Go to Advanced > System Tools > Diagnostics.



3. Click Start to test the internet connectivity and you will find the test results in the gray box.

14. 4. Update the Firmware

TP-Link is dedicated to improving product features, giving you a better network experience.

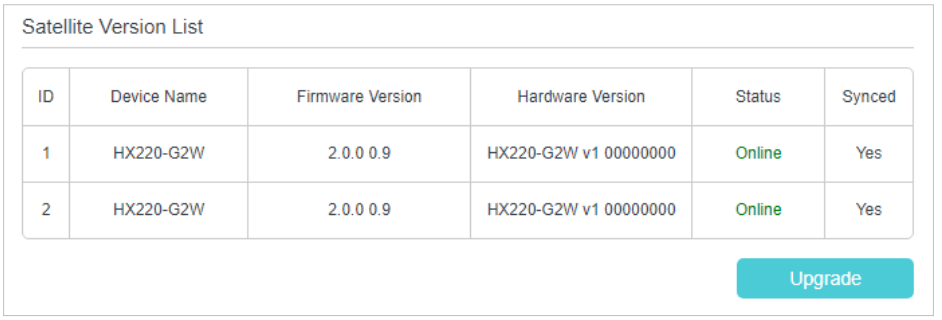
We will inform you through the web management page if there's any update firmware available for your controller. The latest firmware can also be downloaded from the Support page of our website www.tp-link.com for free.

Note:

1. Make sure that you have a stable connection between the controller and your computer. It is NOT recommended to upgrade the firmware wirelessly.
2. Back up your controller configuration before upgrading the firmware.
3. DO NOT turn off the controller during the firmware upgrade.

You can follow the steps below to manually update the firmware.

1. Download the latest firmware file for the controller from our website www.tp-link.com.
2. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
3. Go to Advanced > System Tools > Firmware Upgrade.
4. Focus on the Device Information section. Make sure the downloaded firmware file matches with the Hardware Version.
5. Focus on the Local Upgrade section. Click Browse to locate the downloaded new firmware file, and click Upgrade.



Note:

The upgrading will also take effect on the synced online satellites. We recommend that you keep the controller and its satellites in the same firmware version. Please do not turn off the controller and its satellites during the firmware upgrading process.

6. Wait a few minutes for the upgrading and rebooting.

14. 5. Back Up and Restore Configuration Settings

The configuration settings are stored as a configuration file in the controller. You can back up the configuration file to your computer for future use and restore the controller to a previous settings from the backup file when needed. Moreover, if needed you can erase the current settings and reset the controller to its default factory settings.

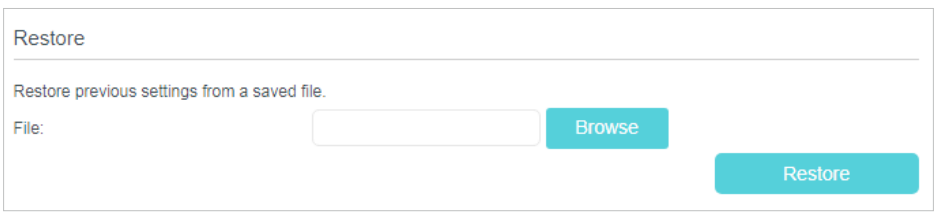
1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > Backup & Restore.

➢ **To back up configuration settings:**

Click Backup to save a copy of the current settings to your local computer. A conf.bin file will be stored to your computer.

➢ **To restore configuration settings:**

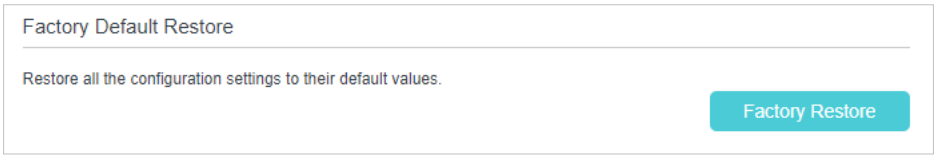
1. Click Browse to locate the backup configuration file stored on your computer, and click Restore



2. Wait a few minutes for the restoring and rebooting.

➢ **To reset the controller to factory default settings:**

1. Click Factory Restore to reset the controller.



2. Wait a few minutes for the restoring and rebooting.

Note:

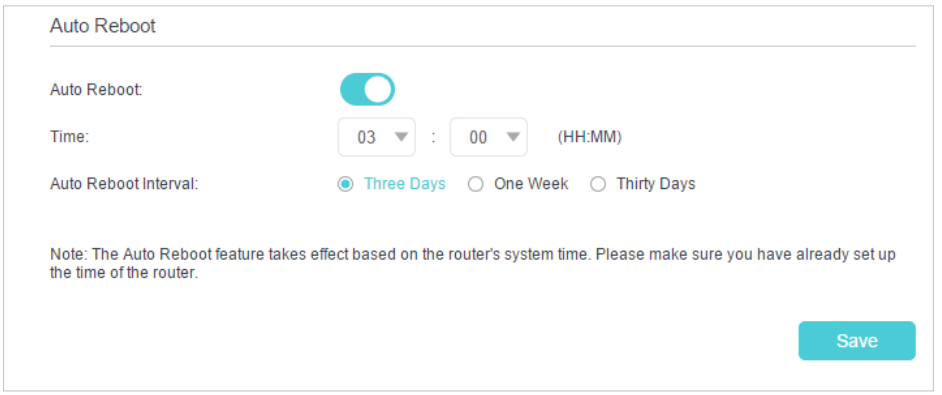
1. During the resetting process, do not turn off the controller.
2. We strongly recommend you back up the current configuration settings before resetting the controller.
3. If you want to reset the controller into its factory default settings, you need to add the agent again to create a mesh Wi-Fi system.

14. 6. Reboot the Controller

The reboot feature cleans the cache to enhance the running performance of the controller. You can schedule the controller to reboot regularly.

➢ **To schedule the controller to reboot at a specific time:**

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools> Reboot Schedule, and enable Auto Reboot.
3. Specify the Time when the controller reboots and the Auto Reboot Interval to decide how often it reboots.



4. Click Save to make the settings effective.

Some settings of the controller may take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Operation Mode.
- Change the Web Management Port.
- Upgrade the firmware of the controller (system will reboot automatically).
- Restore the controller to its factory defaults (system will reboot automatically).

- Update the configuration with the file (system will reboot automatically).

Note:

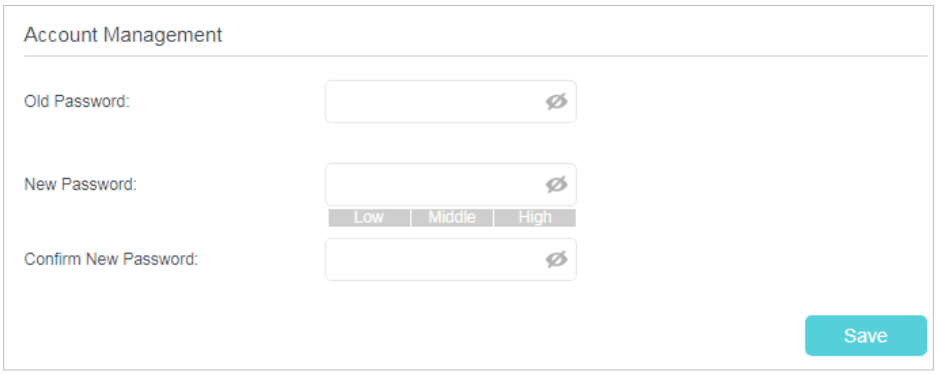
The Auto Reboot feature takes effect based on the controller's system time. Please make sure you have already set the time of the controller.

14. 7. Administration Management

14. 7. 1. Change the Login Password

The account management feature allows you to change your login password of the web management page.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > Administration page. Locate the Account Management section.



3. Enter the old password, then a new password twice (both case-sensitive).
4. Click Save to make the settings effective.
5. Use the new password for future logins.

14. 7. 2. Local Management

You can control the local devices' authority to manage the controller via Local Management feature. By default all local connected devices are allowed to manage the controller. You can also specify one device to manage the controller and enable local management over a more secure way, HTTPS.

Follow the steps below to allow only the specific device to manage the controller via the local management over HTTPS.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > Administration, and locate the Local Management section.

3. Enable Management over HTTPS and keep the Port for HTTP and Port for HTTPS as the default settings. Enter the IP address or MAC address of the local device to manage the controller.

4. Click Save.

Now, you can manage the controller over both HTTP (http://tplinkwifi.net) and HTTPS (https://tplinkwifi.net).

Note:

If you want all local devices can manage the controller, just leave the IP/MAC Address field blank.

14. 7. 3. Remote Management

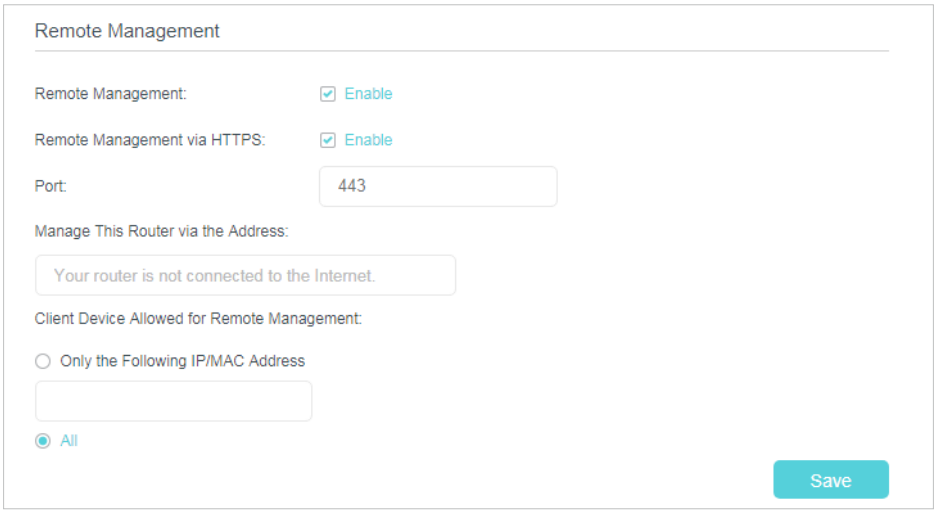
By default, the remote devices are not allowed to manage the controller from the internet. You can enable remote management over HTTP and/or HTTPS if needed. HTTPS is a more secure way to access the controller.

Note:

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), you cannot use the remote management feature because private addresses are not routed on the internet.

Follow the steps below to allow remote devices to manage the controller over HTTPS.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > Administration, and locate the Remote Management section.

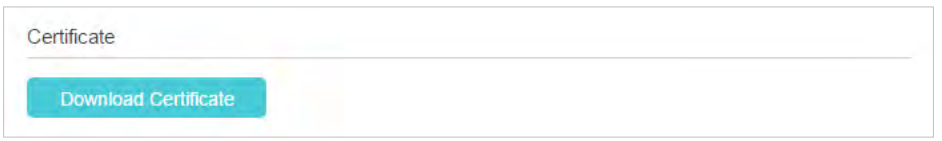


3. Enable Remote Management and Remote Management via HTTPS to allow for HTTPS connection. Keep the Port as the default setting.
4. Set the client device allowed for remote management. Select All to allow all remote devices to manage the controller. If you just want to allow a specific device to manage the controller, select Only the Following IP/MAC Address and enter the IP/MAC address of the remote device.
5. Click Save.

All devices or the specific device on the internet can log in to your controller using the address displayed on the Manage This Router via the Address field to manage the controller.

Tips:

1. If you were warned about the certificate when visiting the web management page remotely, click Trust (or a similar option) to continue. To avoid this warning, you can download and install the certificate on the controller's web management page at Advanced > System Tools > Administration.



2. The controller's WAN IP is usually a dynamic IP. Please refer to Set Up a Dynamic DNS Service Account if you want to log in to the controller through a domain name.

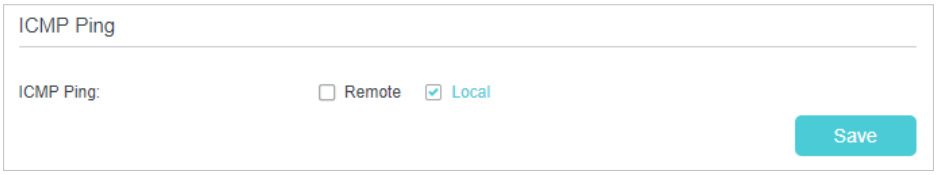
14. 7. 4. ICMP Ping

ICMP (Internet Control Message Protocol) Ping is used to diagnose the network by sending ICMP echo request packets to the target remote or local host and waiting for an ICMP response.

You can control the controller's replies to ICMP Ping requests.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.

2. Go to Advanced > System Tools > Administration, and locate the ICMP Ping section.

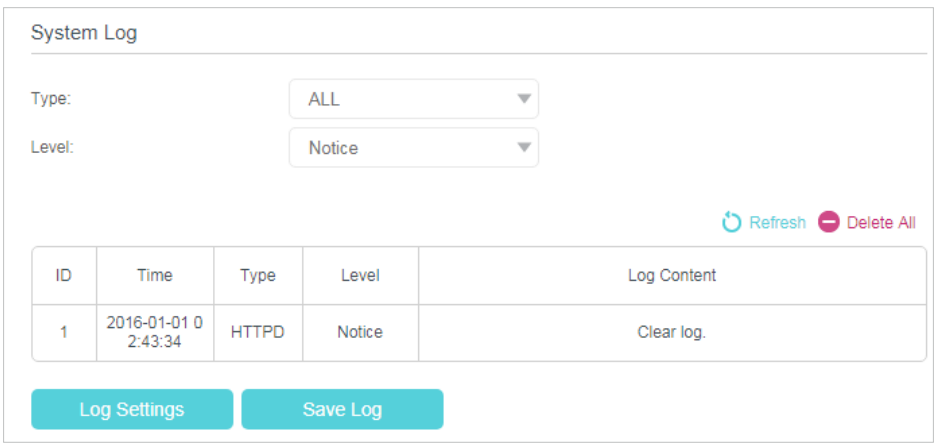


3. Specify the ICMP Ping reply options.
   - Remote: Select it if you want the computers on a public network to ping the controller's WAN IP address.
   - Local: Enabled by default, if enabled, the computers on a private network can ping the controller's LAN IP address.
4. Click Save to make the settings effective.

14. 8. System Log

System Log can help you know what happened to your controller, facilitating you to locate the malfunctions. For example when your controller does not work properly, you may need to save the system log and send it to the technical support for troubleshooting.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > System Log page.



➢ **To view the system logs:**

You can view specific system logs by selecting the log type and level.

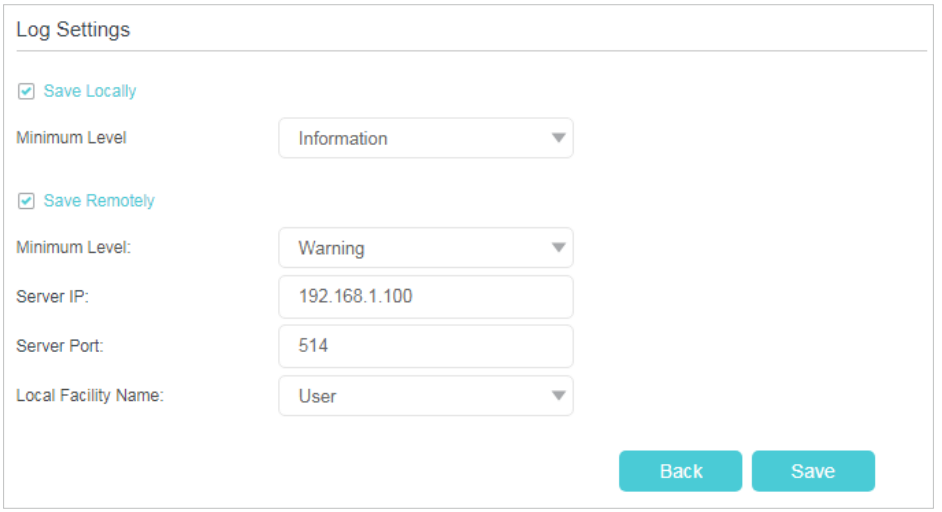
Click Refresh to refresh the log list.

➢ **To save the system logs:**

You can save the system logs to your local computer or a remote server.

Click Save Log to save the logs in a txt file to your computer.

Click Log Settings to set the storage path of logs.

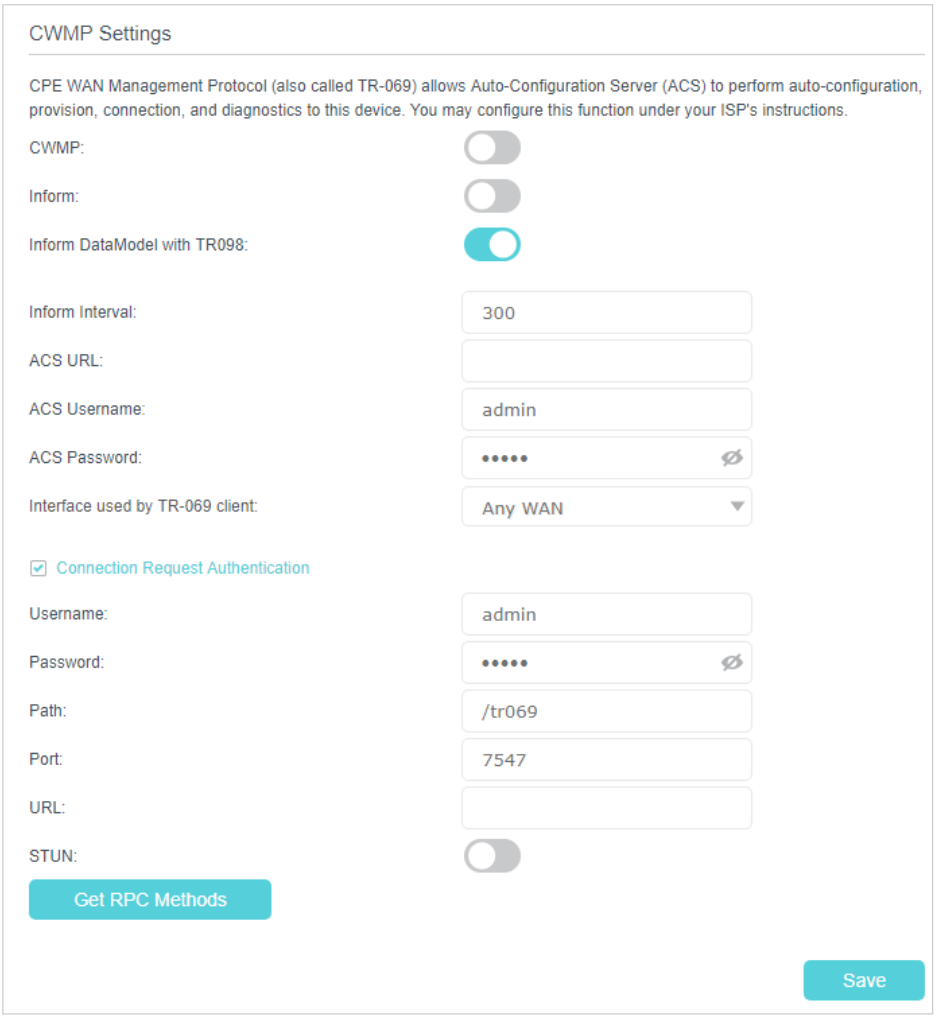


- Save Locally: Select this option to cache the system log to the controller's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- Save Remotely: Select this option to send the system log to a remote server, select the minimum level of system log to be saved from the drop-down list and enter the information of the remote server. If the remote server has a log viewer client or a sniffer tool implemented, you can view and analyze the system log remotely in real-time.

14. 9. CWMP Settings

The controller supports CWMP (CPE WAN Management Protocol), also called TR-069. This collects information, performs diagnostics and configures the devices automatically via ACS (Auto-Configuration Server).

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > CWMP Settings.



- CWMP: Enable or disable the CWMP (CPE WAN Management Protocol) function.
- Inform: Enable or disable the function of sending an inform message to the ACS (Auto Configuration Server) periodically.
- Inform DataModel with TR098: Enable or disable the function of sending inform complying with the data model defined in TR-098.
- Inform Interval: Set the time interval in seconds when the Inform message will be sent to the ACS.
- ACS URL: Enter the web address of the ACS which is provided by your ISP.
- ACS Username/Password: Enter the username/password to log in to the ACS server.
- Interface used by TR-069 client: Select which interface to be used by the TR-069 client.
- Connection Request Authentication: Select this check box to enable authentication for the connection request.
- Username/Password: Enter the username/password for the ACS server to log in to the controller.

- Path: Enter the path for the ACS server to log in to the controller.
- Port: Enter the port that connects to the ACS server.
- URL: Enter the URL that connects to the ACS server.
- STUN: Enable or disable the STUN(Simple Traversal of UDP through NAT) function.
- STUN Server Address/Port: Enter the STUN server address and port number provided by your ISP.
- STUN Username/Password: Enter the username/password to log in to the STUN server.
- Minimum/Maximum Keep Alive Period: Enter the minimum/maximum time for maintaining NAT binding.
- Get RPC Methods: Click to get the methods to support CWMP.

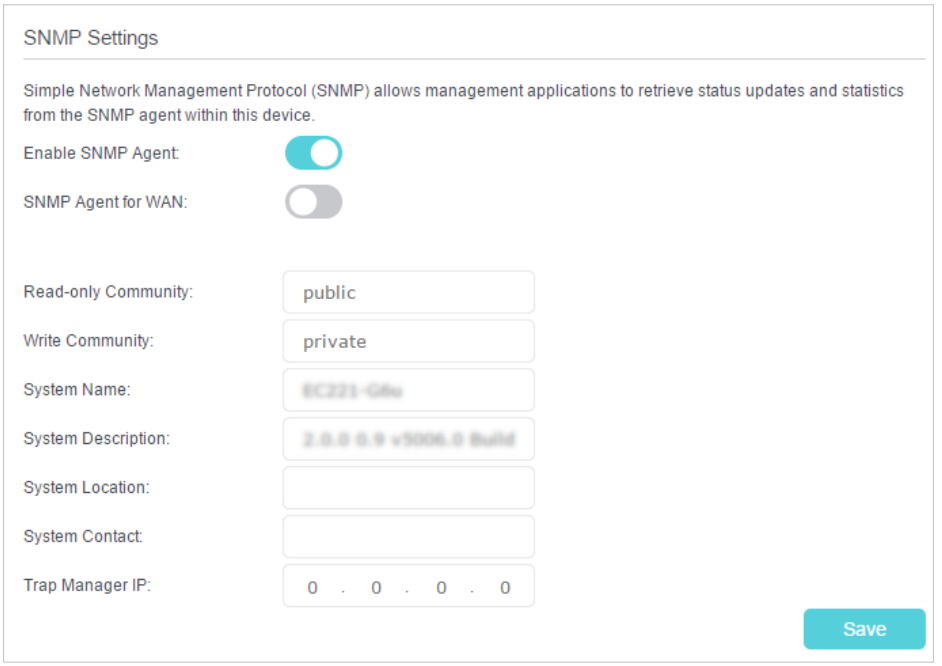
Click Save to make the settings effective.

14. 10. SNMP Settings

SNMP (Simple Network Management Protocol) is widely used in network management for network monitoring. It allows management applications to retrieve status updates and statistics from the SNMP agent within this device. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

The SNMP Agent is an application running on the router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a router contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > SNMP Settings.



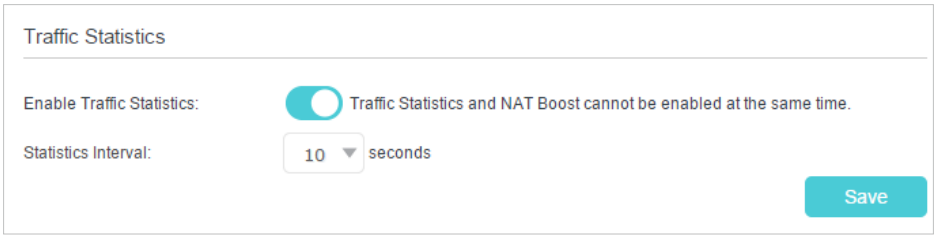
- Enable SNMP Agent/SNMP Agent for WAN: Turn on to enable the built-in SNMP agent that allows the controller to operate as the operational role in receiving and processing of SNMP messages, sending responses to the SNMP manager, and triggering SNMP traps when an event occurs.
- Read-only Community: Displays the default public community string that protects the controller from unauthorized access.
- Write Community: Displays the default write community string that protects the controller from unauthorized changes.
- System Name: Displays the administratively-assigned name for this managed device.
- System Description: Displays the textual description of the managed device. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.
- System Location: Displays the physical location of this device (for example, the telephone closet, 3rd floor).
- System Contact: Displays the textual identification of the contact person for this managed device, together with information on how to contact this person.
- Trap Manager IP: Displays the IP address of the host to receive the traps.

You are suggested to keep the default settings. Click Save to make the settings effective.

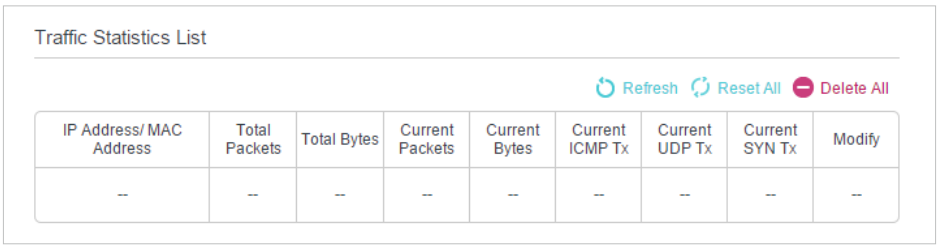
14. 11. Monitor the Internet Traffic Statistics

The Traffic Statistics page displays the network traffic of the LAN, WAN and WLAN sent and received packets, allowing you to monitor the volume of internet traffic statistics.

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > System Tools > Traffic Statistics.
3. Toggle on Enable Traffic Statistics to enable traffic statistics function, you can view the total number of packets and bytes received and transmitted by the controller within the selected Statistics Interval. This function is disabled by default.



4. You can refer to Traffic Statistics List for the detailed information about the traffic usage of all devices.



FAQ

Q1. What should I do if I forget my wireless password?

The default wireless password is printed on the label of the device. If the password has been changed:

1. Connect your computer to the controller using an Ethernet cable.
2. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
3. Go to Basic > Wireless to retrieve or reset your wireless password.

Q2. What should I do if I forget my web management password?

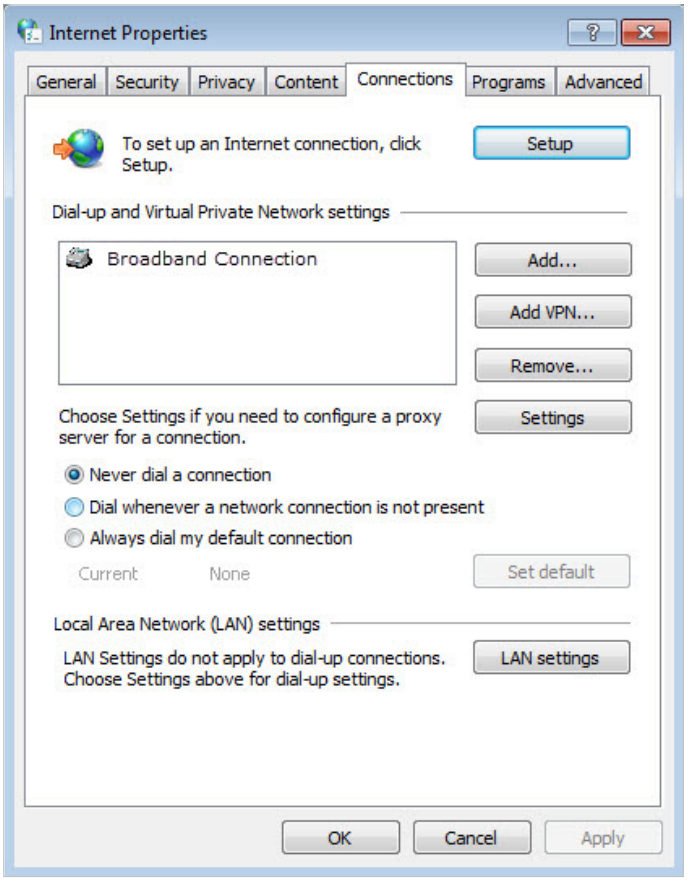
- Press and hold the RESET button on the bottom of the controller for about 5 seconds, and then visit http://tplinkwifi.net to create a new login password.

Note: You'll need to reconfigure the controller to surf the internet once the controller is reset, and please mark down your new password for future use.

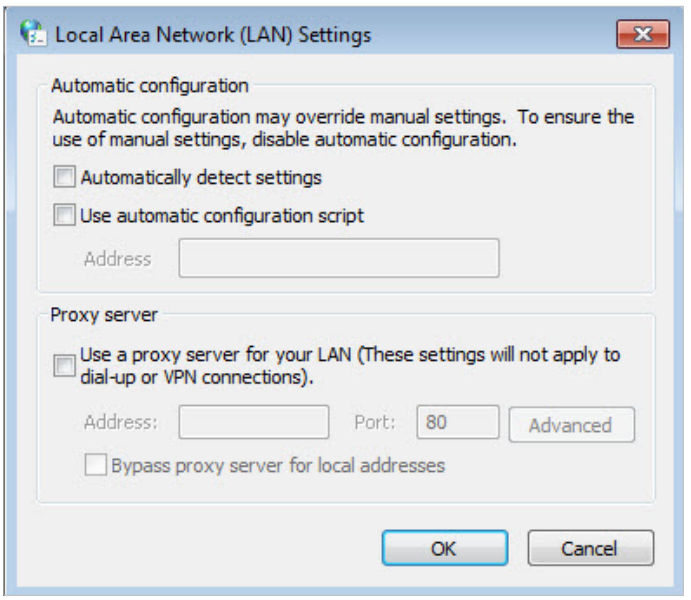
Q3. What should I do if I cannot log in to the controller's web management page?

This can happen for a variety of reasons. Please try the methods below to log in again.

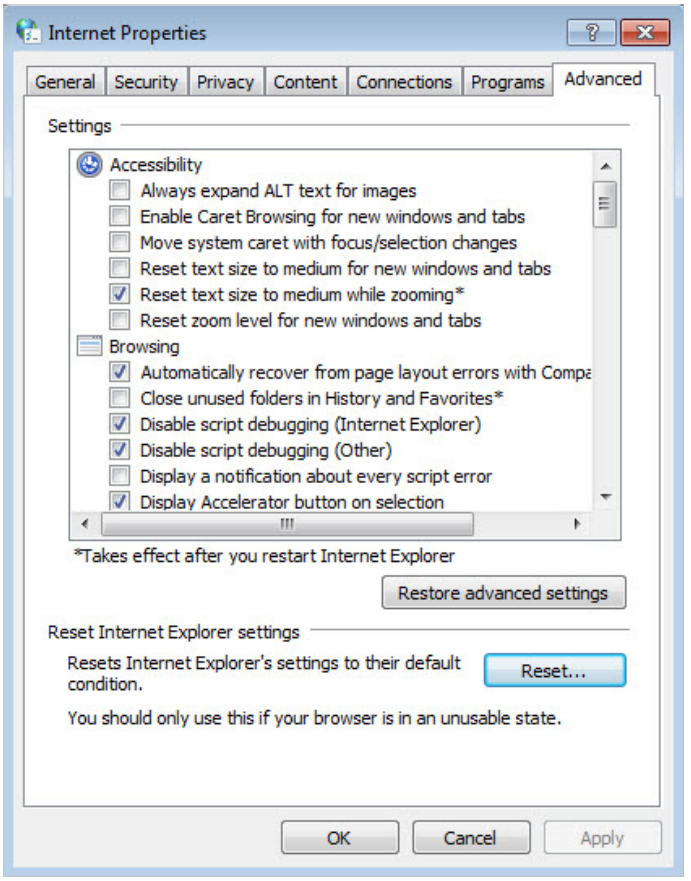
- Make sure your computer is connected to the controller correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as Obtain an IP address automatically and Obtain DNS server address automatically.
- Make sure http://tplinkwifi.net or http://192.168.0.1 is correctly entered.
- Check your computer's settings:
  1) Go to Start > Control Panel > Network and Internet, and click View network status and tasks.
  2) Click Internet Options on the bottom left.
  3) Click Connections and select Never dial a connection.



4) Click LAN settings and clear the following three options and click OK.



5) Go to Advanced > Restore advanced settings, click OK to save the settings.



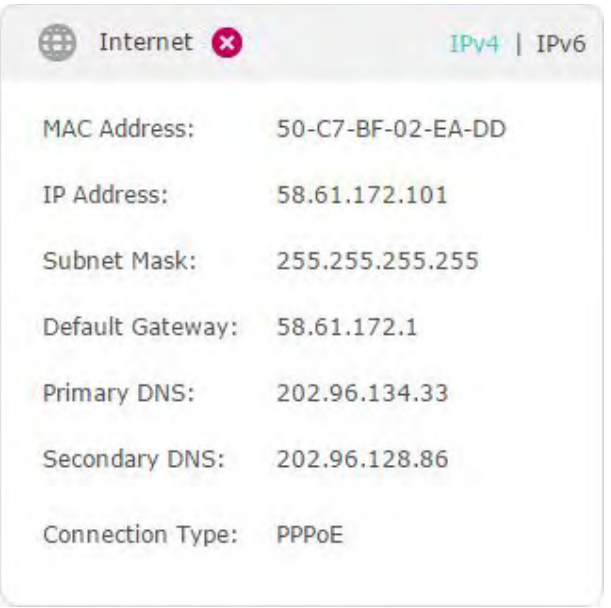
- Use another web browser or computer to log in again.
- Reset the controller to factory default settings and try again. If login still fails, please contact the technical support.

Note: You'll need to reconfigure the controller to access the internet once the controller is reset.

Q4. What should I do if I cannot access the internet even though the configuration is finished?

1. Visit http://tplinkwifi.net, and log in with the password you set for the controller.
2. Go to Advanced > Status to check internet status:

As the following image shows, if IP Address is a valid one, please try the methods below:

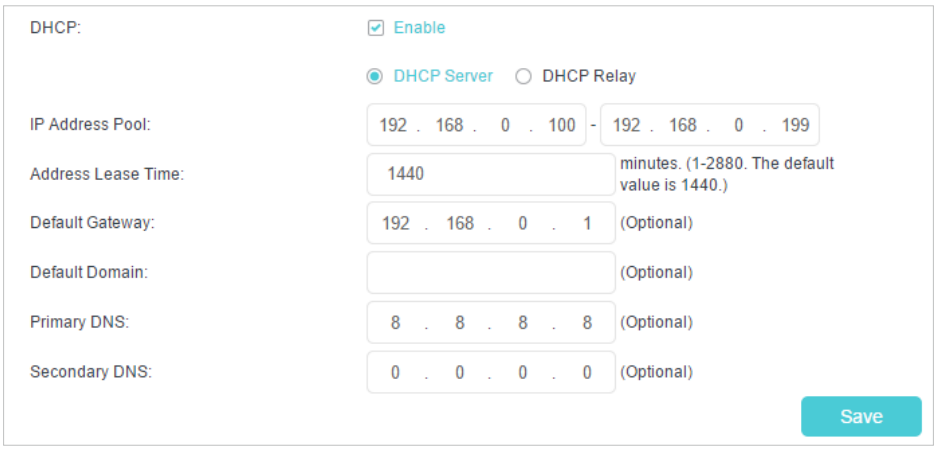


- Your computer might not recognize any DNS server addresses. Please manually configure the DNS server.

  1) Go to Advanced > Network > LAN Settings, and locate the DHCP section.

  2) Enter 8.8.8.8 as Primary DNS, click Save.

  Tips: 8.8.8.8 is a safe and public DNS server operated by Google.



- Restart the modem and the controller.

  1) Power off your modem and controller, and leave them off for 1 minute.

  2) Power on your modem first, and wait about 2 minutes until it gets a solid cable or Internet light.

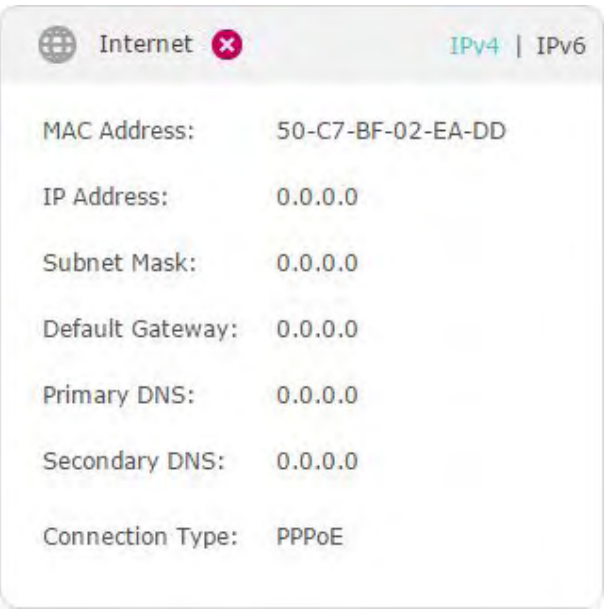
  3) Power on the controller.

  4) Wait another 1 or 2 minutes and check the internet access.

- Reset the controller to factory default settings and reconfigure the controller.
- Upgrade the firmware of the controller.

- Check the TCP/IP settings on the particular device if all other devices can get internet from the controller.

As the following image shows, if the IP Address is 0.0.0.0, please try the methods below:

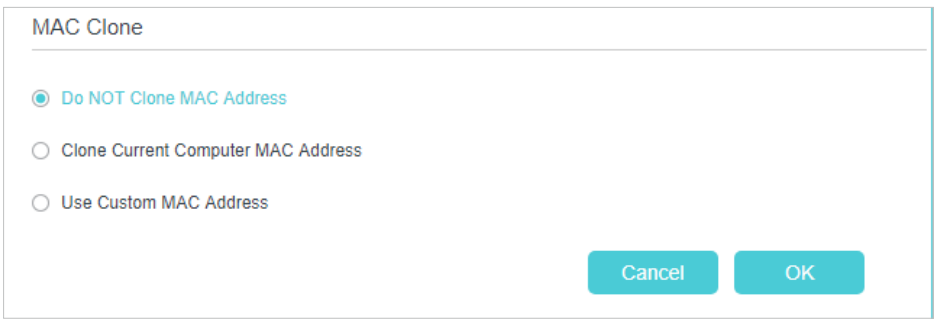


- Make sure the physical connection between the controller and the modem is proper.
- Clone the MAC address of your computer.

  1) Visit http://tplinkwifi.net, and log in with the password you set for the controller.

  2) Go to Advanced > Network > Internet and click the edit icon to find the MAC Clone section.

  3) Choose an option as needed (enter the MAC address if Use Custom MAC Address is selected), and click OK.



Tips:

- Some ISP will register the MAC address of your computer when you access the internet for the first time through their Cable modem, if you add a controller into your network to share your internet connection, the ISP will not accept it as the MAC address is changed, so you need to clone your computer's MAC address to the controller.

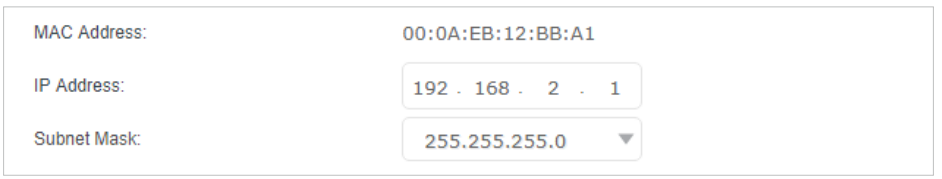
- The MAC addresses of a computer in wired connection and wireless connection are different.

- Modify the LAN IP address of the controller.

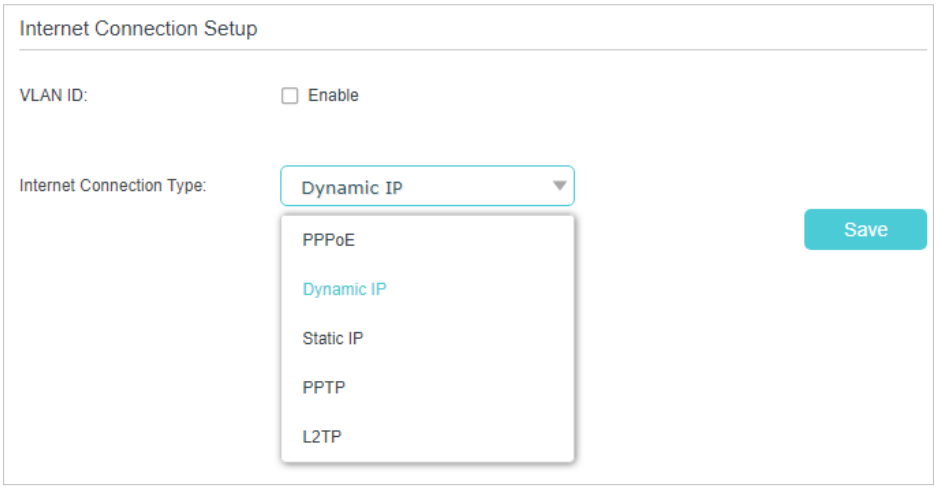
  Note:

  Most TP-Link routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, which may conflict with the IP range of your existing ADSL modem/router. If so, the router is not able to communicate with your modem and you can't access the internet. To resolve this problem, you need to change the LAN IP address of the router to avoid such conflict, for example, 192.168.2.1.

  1) Visit http://tplinkwifi.net, and log in with the password you set for the controller.
  2) Go to Advanced > Network > LAN Settings, and locate the DHCP section.
  3) Modify the LAN IP address as the following image shows. Here we take 192.168.2.1 as an example.
  4) Click Save to make the settings effective.



- Restart the modem and the controller.
  1) Power off your modem and controller, and leave them off for 1 minute.
  2) Power on your modem first, and wait about 2 minutes until it get a solid cable or Internet light.
  3) Power on the controller.
  4) Wait another 1 or 2 minutes and check the internet access.
- Double check the internet connection type.
  1) Confirm your internet connection type, which can be learned from the ISP.
  2) Visit http://tplinkwifi.net, and log in with the password you set for the controller.
  3) Go to Basic > Internet.
  4) Select your Internet Connection Type and enter other parameters if required.
  5) Click Save.



6) Restart the modem and the controller again.

- Please upgrade the firmware of the controller.

If you've tried every method above but still cannot access the internet, please contact the technical support.

Q5. What should I do if I cannot find my wireless network or I cannot connect the wireless network?

If you fail to find any wireless network, please follow the steps below:

- Make sure the wireless function of your device is enabled if you're using a laptop with built-in wireless adapter. You can refer to the relevant document or contact the laptop manufacturer.
- Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled.
  - **On Windows 7**

  1) If you see the message No connections are available, it is usually because the wireless function is disabled or blocked somehow.

  2) Click Troubleshoot and windows might be able to fix the problem by itself.
  - **On Windows XP**

  1) If you see the message Windows cannot configure this wireless connection, this is usually because windows configuration utility is disabled or you are running another wireless configuration tool to connect the wireless.

  2) Exit the wireless configuration tool (the TP-Link Utility, for example).

  3) Select and right click on My Computer on desktop, select Manage to open Computer Management window.

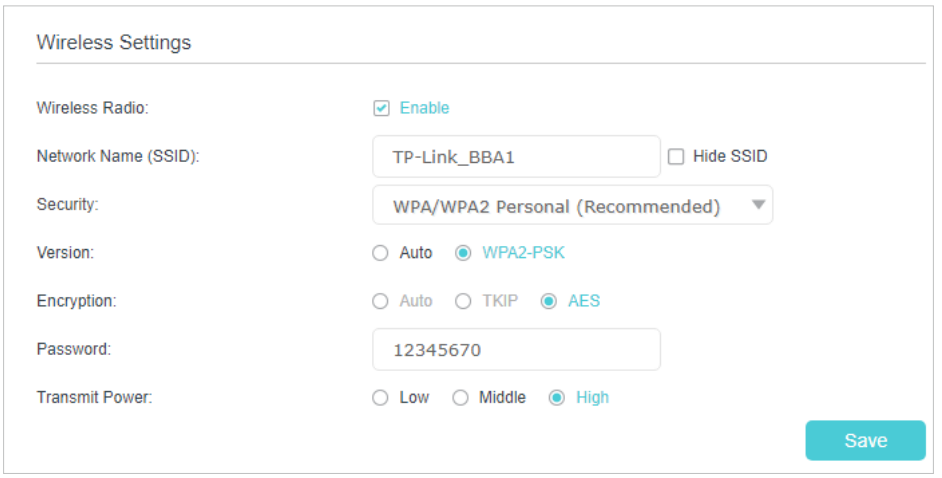
  4) Expand Services and Applications > Services, find and locate Wireless Zero Configuration in the Services list on the right side.

5) Right click Wireless Zero Configuration, and then select Properties.

6) Change Startup type to Automatic, click on Start button and make sure the Service status is Started. And then click OK.

If you can find other wireless network except your own, please follow the steps below:

- Check the WLAN LED indicator on your wireless controller/modem.
- Make sure your computer/device is still in the range of your controller/modem. Move it closer if it is currently too far away.
- Go to Advanced > Wireless > Wireless Settings, and check the wireless settings. Double check your Wireless Network Name and SSID is not hidden.



If you can find your wireless network but fail to connect, please follow the steps below:

- **Authenticating problem/password mismatch:**

1) Sometimes you will be asked to type in a PIN number when you connect to the wireless network for the first time. This PIN number is different from the Wireless Password/Network Security Key, usually you can only find it on the label of your router.

2) If you cannot find the PIN or PIN failed, you may choose Connecting using a security key instead, and then type in the Wireless Password/Network Security Key.

3) If it continues to show note of Network Security Key Mismatch, it is suggested to confirm the wireless password of your wireless controller.

Note: Wireless Password/Network Security Key is case sensitive.

- **Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:**
  - Check the wireless signal strength of your network. If it is weak (1~3 bars), please move the controller closer and try again.
  - Change the wireless Channel of the controller to 1, 6 or 11 to reduce interference from other networks.
  - Re-install or update the driver for your wireless adapter of the computer.

Q6. What should I do if the agent's status LED remains flashing red?

- Place the agent close to the controller until the status LED turns solid blue or white, then relocate the agent.
- Reset the agent and try to synchronize the agent with the mesh controller again.

FCC compliance information statement

Product Name: AC1200 Whole Home Mesh Wi-Fi AP

Model Number: HC220-G5

Component Name	Model
I.T.E. Power	T120100-2B1REV4.0.0

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: http://www.tp-link.com/us/

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

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 or more 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.

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.

2) This device must accept any interference received, including interference that may cause undesired operation.

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

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

FCC compliance information statement

Product Name: I.T.E. Power

Model Number: T120100-2B1REV4.0.0

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: http://www.tp-link.com/us/

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

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 or more 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.

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.

2) This device must accept any interference received, including interference that may cause undesired operation.

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

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2021.5.10

CE Mark Warning

CE

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 (the maximum transmitted power)

2400 MHz - 2483.5 MHz (20dBm)

5150 MHz - 5250 MHz (23dBm)

EU declaration of conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/53/EU, 2009/125/EC, 2011/65/EU and (EU)2015/863.

The original EU declaration of conformity may be found at https://www.tp-link.com/en/ce

RF Exposure Information

This device meets the EU requirements (2014/53/EU Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

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

Attention: This device may only be used indoors in all EU member states, EFTA countries and Northern Ireland.

Attention: This device may only be used indoors in Great Britain..

Canadian Compliance Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1) L'appareil ne doit pas produire de brouillage;

2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution:

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

Radiation Exposure Statement:

This equipment complies with IC 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.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Industry Canada Statement

CAN ICES-3 (B)/NMB-3(B)

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice:

注意！

依據 低功率電波輻射性電機管理辦法

LP0002低功率射頻器材技術規範_章節3.8.2

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前述合法通信，指依電信管理法規定作業之無線電通信。

低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

應避免影響附近雷達系統之操作。

BSMI Notice

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 不要私自拆開機殼或自行維修，如產品有故障請與原廠或代理商聯繫。

設備名稱： Equipment name				型號（型式）： Type designation (Type)		
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	–	○	○	○	○	○

電源線	◯	◯	◯	◯	◯	◯
網線	◯	◯	◯	◯	◯	◯
其他及其配件	–	◯	◯	◯	◯	◯

備考 1.〝超出 0.1 wt %〞及〝超出 0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值

Note 1：“Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考 2.〝◯〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2：“ ◯ ” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考 3.〝–〞係指該項限用物質為排除項目。

Note 3：The “–” indicates that the restricted substance corresponds to the exemption.

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

EAC

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended.
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Operating Temperature: 0℃~ 40℃ (32℉~ 104℉)

Storage Temperature: -40˚C~ 70˚C (-40˚F~ 158˚F)

Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

Explanations of the symbols on the product label

Symbol	Explanation
⎓	DC voltage
	Indoor use only
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.