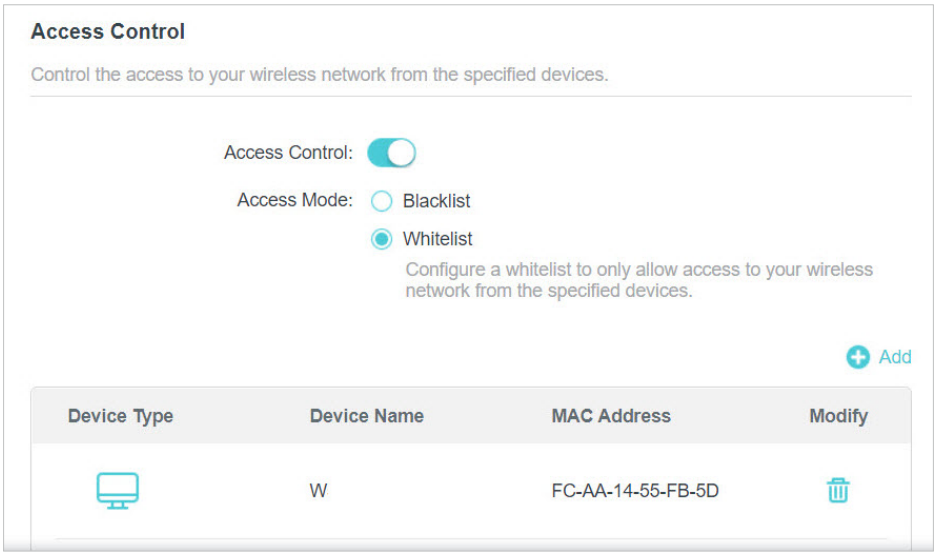
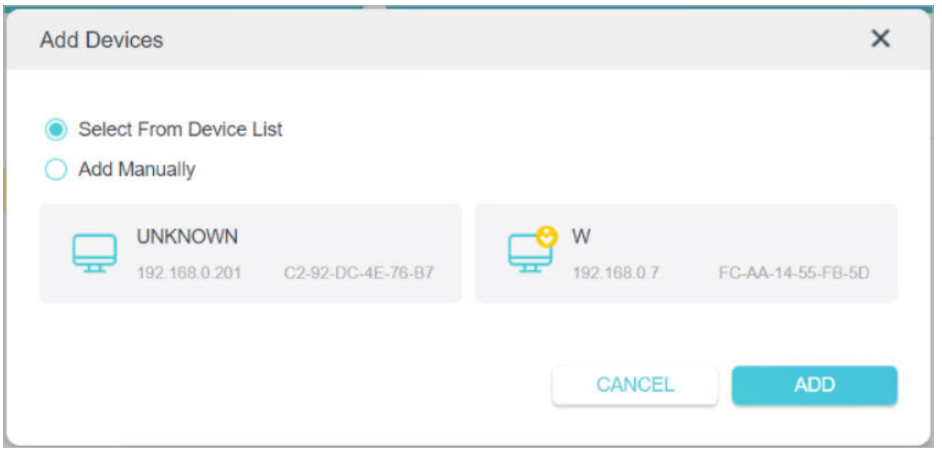
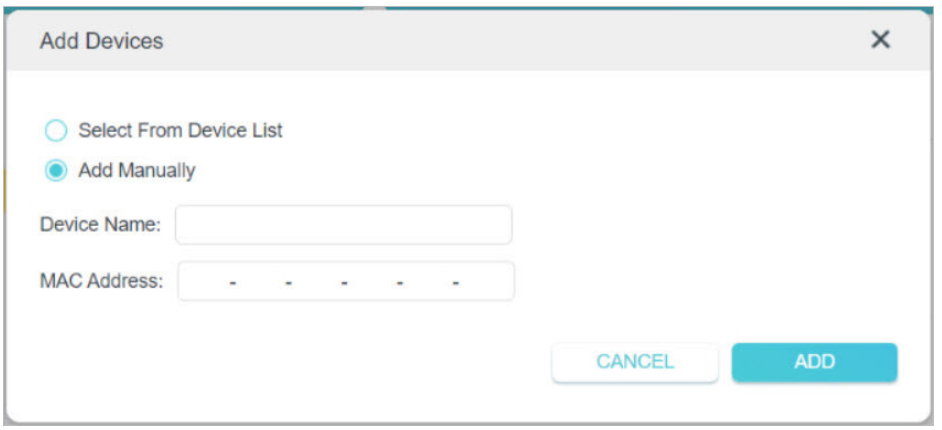


2) Click Add to add other devices you want to allow.

3) Click Select From Device List, choose devices, then click ADD.



Alternatively, click Add Manually, enter the device name and MAC address, then click ADD.



Done!

Now you can block or allow specific client devices to access your network using the Blacklist or Whitelist.

Chapter 7

Customize Network Settings

This chapter introduces how to customize your network settings.

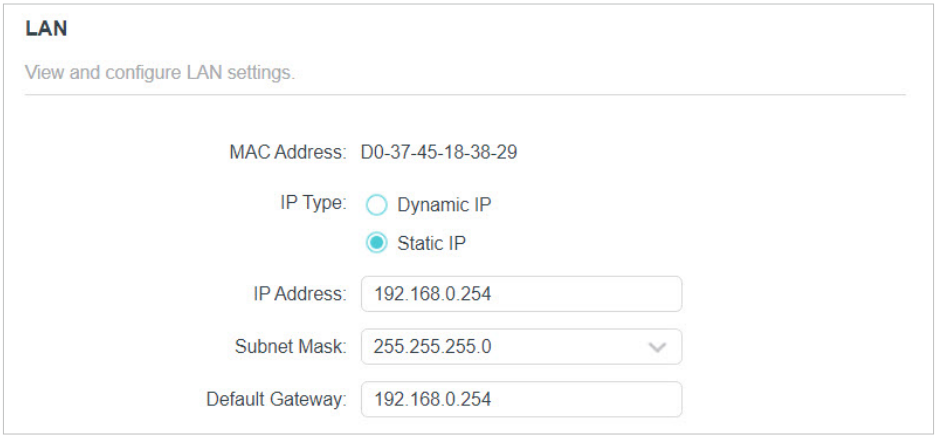
It contains the following sections:

7. 1. Change the LAN Settings

The access point is preset with Dynamic IP, which allows it to dynamically obtain an IP address and gateway from the main router/AP. It is recommended that you keep the default LAN settings to avoid IP conflict with the main router/AP or other devices on your local network.

If you want to set a static IP address for the access point, follow the steps below:

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Internet > LAN.
3. Choose Static IP.
4. Set an IP address, which should be in the same subnet as the main router/AP.



5. Leave other parameters as the default settings.
6. Click SAVE.

Tip:
After setting a static IP address, you can use the new IP address to log into the web management page besides http://tplinkap.net.

7. 2. Specify DHCP Server Settings

By default, the DHCP (Dynamic Host Configuration Protocol) server works in Auto mode to avoid IP conflict. It will automatically assign IP addresses to clients from its IP address pool only when the DHCP server of the main router/AP is disabled.

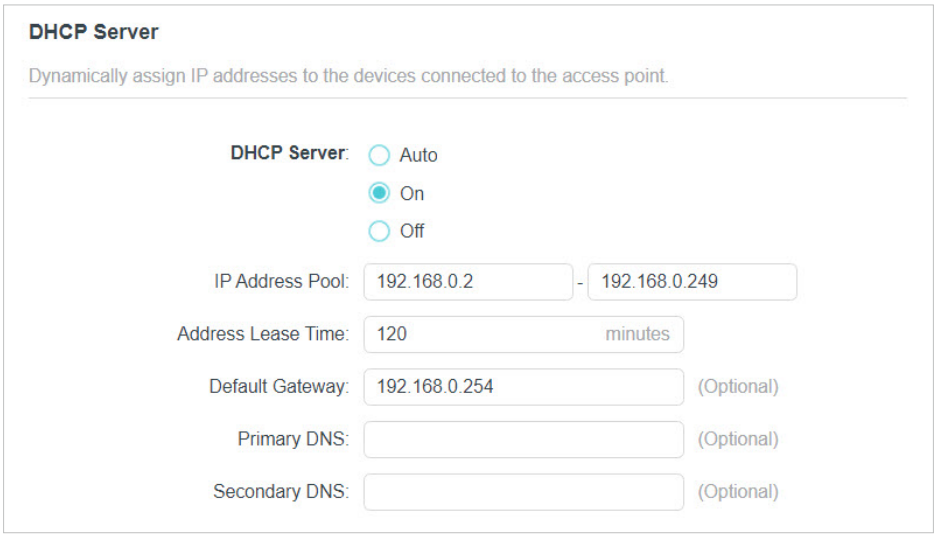
You can change the DHCP server settings if necessary, and you can reserve LAN IP addresses for specified client devices.

Note:
If you disable the DHCP server and there is no other DHCP server within your LAN, you have to configure the IP address for each client manually.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Internet > DHCP Server.

- **To specify the IP address range that the access point assigns:**

1. Turn on DHCP Server.

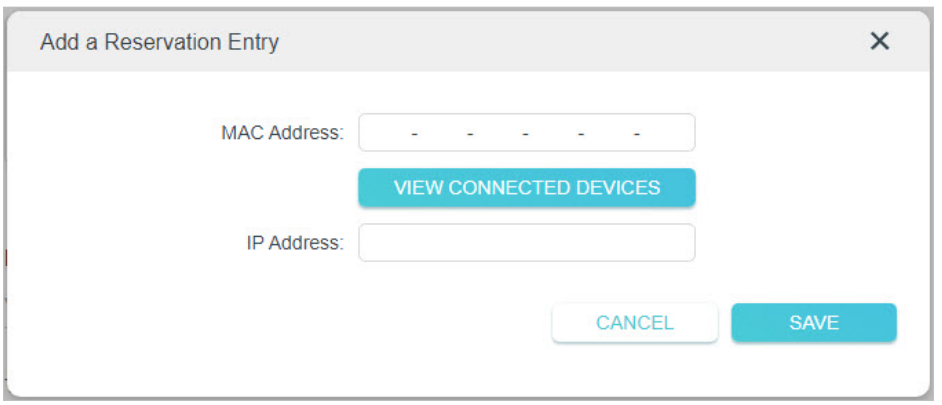


2. Enter the starting and ending IP addresses of the IP Address Pool.
3. Leave other parameters as the default settings.
4. Click SAVE.

- **To reserve an IP address for a specified client device:**

The DHCP server of the access point works when it is turned on, or when it is in Auto mode with the DHCP server of the main router/AP disabled. When it is working, you can view the DHCP clients and reserve IP addresses for them.

1. In the Address Reservation section, click Add.



2. Click VIEW CONNECTED DEVICES and select the device you want to reserve an IP for. The MAC Address will be automatically filled in. You can also enter the MAC address of the client device manually.
3. Enter the IP address to reserve for the client device.
4. Click SAVE.

Chapter 8

Manage Your Access Point

This chapter will show you how to configure and manage your access point.

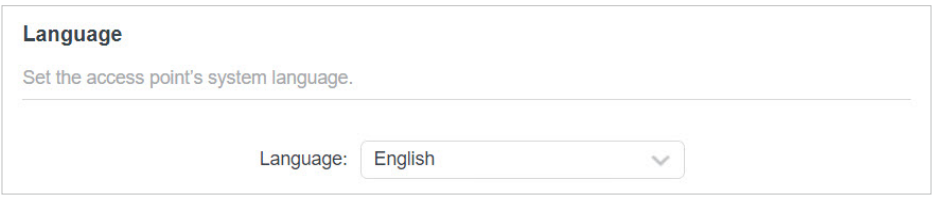
It contains the following sections:

8. 1. Set the System Time and Language

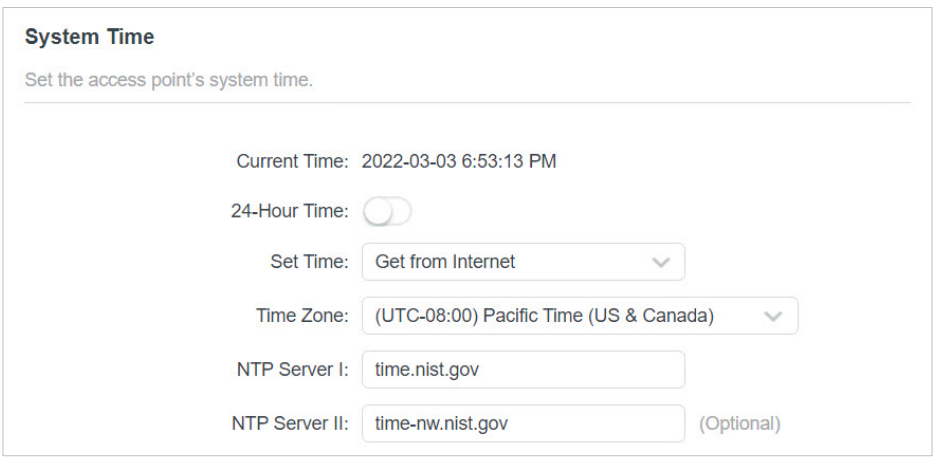
System time is the time displayed while the access point is running. The system time you configure here will be used for other time-based functions like Reboot Schedule. You can choose the way to obtain the system time as needed.

System language is the language displayed when you log into the access point. You can change the system language as needed.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Time & Language.
3. (Optional) Enable 24-Hour Time if you want to display the time in 24-hour format.
4. Set the system time and languange according to your needs.
   - **To set system language:**
     1) Select the language from the dropdown list.



     2) Click SAVE.
   - **To get the system time from the internet:**
     1) In the Set Time field, select Get from Internet.



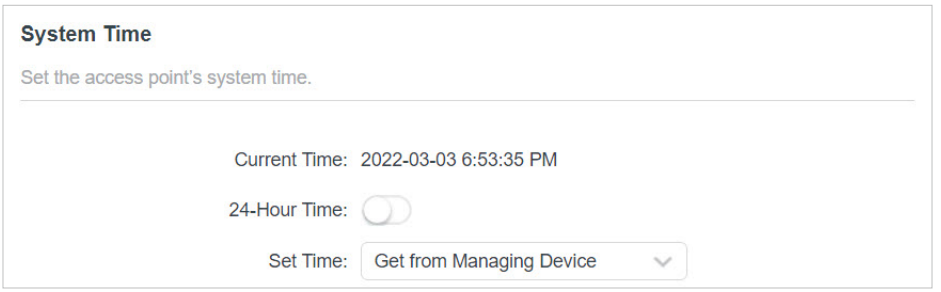
     2) Select your local Time Zone from the drop-down list.
     3) In the NTP Server I field, enter the IP address or domain name of your desired NTP Server.

4) (Optional) In the NTP Server II field, enter the IP address or domain name of the second NTP Server.

5) Click SAVE.

- **To get the system time from the managing device:**

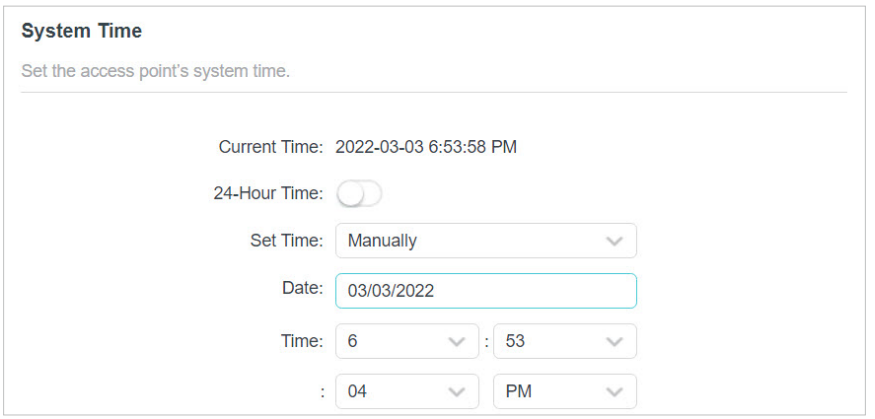
1) In the Set Time field, select Get from Managing Device.



2) Click SAVE.

- **To manually set the system time:**

1) In the Set Time field, select Manually.



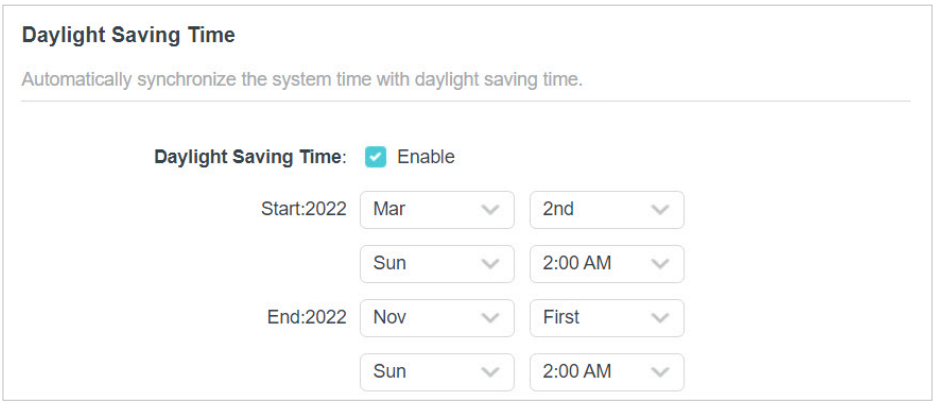
2) Set the current Date (In MM/DD/YYYY format).

3) Set the current Time (In HH/MM/SS format).

4) Click SAVE.

- **To set up Daylight Saving Time:**

1) Enable Daylight Saving Time.



2) Select the correct Start date and time when daylight saving time starts at your local time zone.

3) Select the correct End date and time when daylight saving time ends at your local time zone.

4) Click SAVE.

8. 2. Control LEDs

The LEDs of access point indicate its activities and status. You can turn off the LEDs when you don't need them.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.

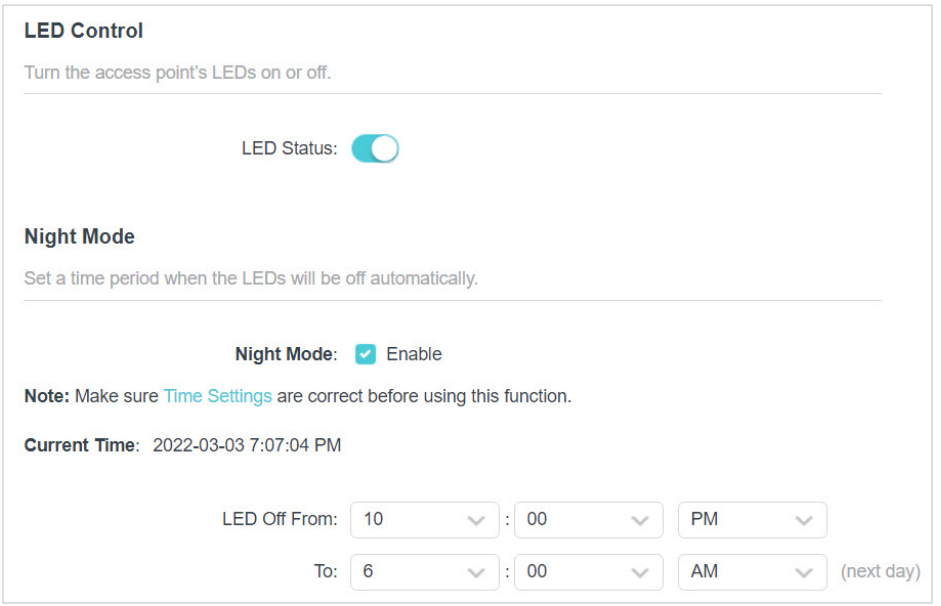
2. Go to System > LED Control.

3. Turn off the LEDs when you don't need them.

- If you want to turn off LEDs immediately, turn off LED Status.

- If you want to turn off LEDs during a specific time period, follow the steps below:

  1) Enable LED Status and Night Mode.



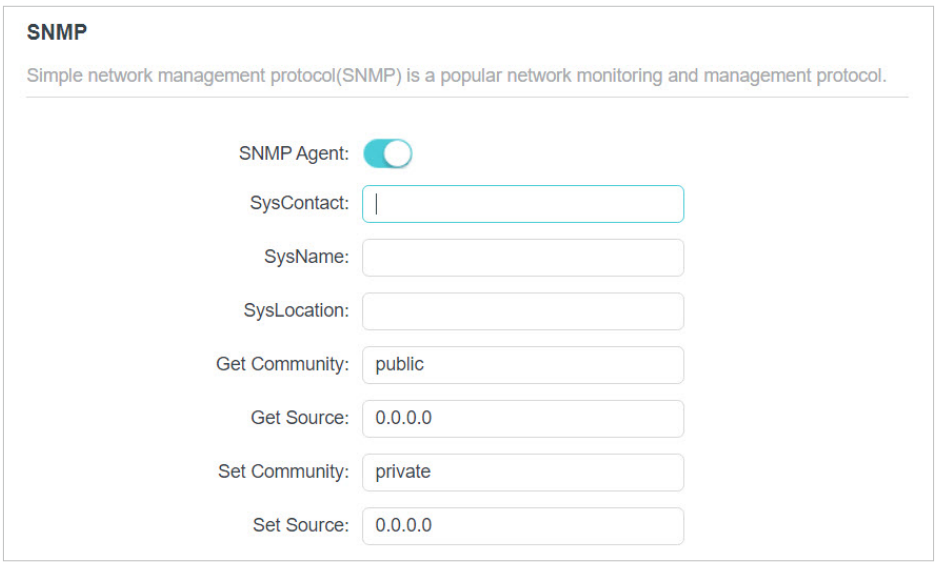
2) Specify the LED Off Time as needed, and the LEDs will be off during the period.

4. Click SAVE.

8. 3. Configure the SNMP Agent

SNMP (Simple Network Management Protocol) is a popular network monitoring and management protocol. You can configure the SNMP agent to communicate with your network monitoring tool or network management system.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > SNMP.
3. Enable SNMP Agent.



4. Configure the SNMP agent according to your actual network requirement.

- SysContact – Enter the contact email address of the node to be managed.
- SysName – Set a user-defined name for the node to be managed.
- SysLocation – Enter the physical location of the node to be managed.
- Get Community – Enter the community name that allows read-only access to the device's SNMP information. The community name is considered as a group password. The default setting is public.
- Get Source – Enter the IP address or subnet that management systems can read information from this 'get' community.

  Note: A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If 0.0.0.0 is specified as the IP address, the agent will accept all requests under the corresponding community name.

- Set Community – Enter the community name that allows read/write access to the device's SNMP information. The community name can be considered as a group password. The default setting is private.
- Set Source – Enter the IP address or subnet that management systems can read and write to this 'set' community.

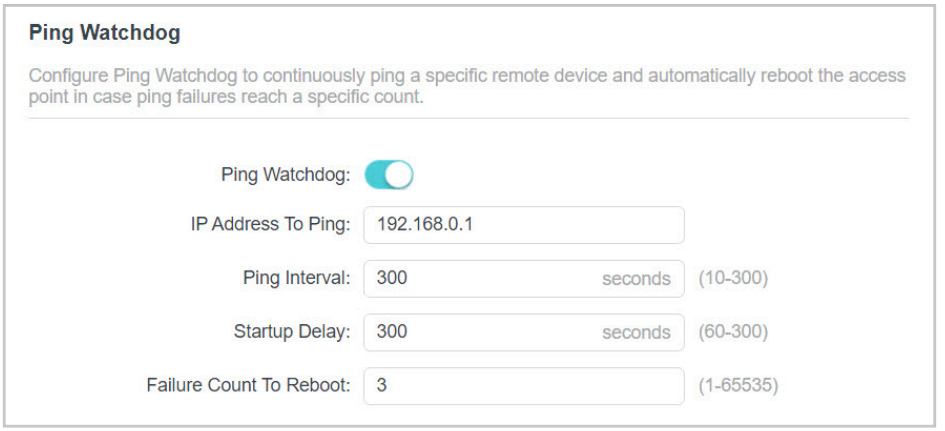
  Note: A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If 0.0.0.0 is specified as the IP address, the agent will accept all requests under the corresponding community name.

5. Click SAVE.

8. 4. Configure the Ping Watchdog

Ping Watchdog allows the access point to continuously ping a specific remote host for connection status using a user-defined IP address (or an internet gateway). If it is unable to ping the target IP address under the user-defined constraints, the device will automatically reboot.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Ping Watchdog.
3. Enable Ping Watchdog.



4. In IP Address To Ping field, enter the IP address of the target host that you want to send ping packets to.
5. In Ping Interval field, enter the time interval between two continuous ping packets.
6. In Startup Delay field, enter the time delay before the first ping packet is sent out when the device is restarted.
7. In Fail Count To Reboot field, enter a number of ping count(s) that the device can send continuously. If ping failures reaches the value, the device will restart automatically.
8. Click SAVE.

8. 5. Update the Firmware

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

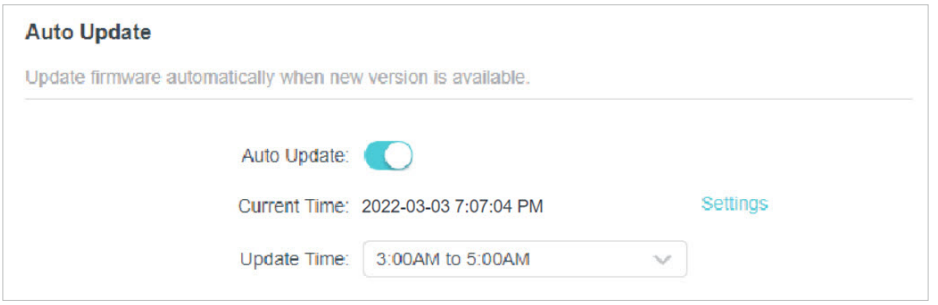
We will inform you through the web management page if there's any new firmware available for your access point. Also, the latest firmware will be released at the TP-Link official website www.tp-link.com, and you can download it from the Support page for free.

Note:

- Make sure the latest firmware file matches the hardware version (as shown in the download section of the Support page).
- Make sure that you have a stable connection between the access point and your computer. Wired connection is recommended.
- Back up your access point's configurations before firmware update.
- Do NOT turn off the access point during the firmware update.

8. 5. 1. Auto Update

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Firmware Update.
3. Enable Auto Update.



4. Specify the Update Time and save the settings.

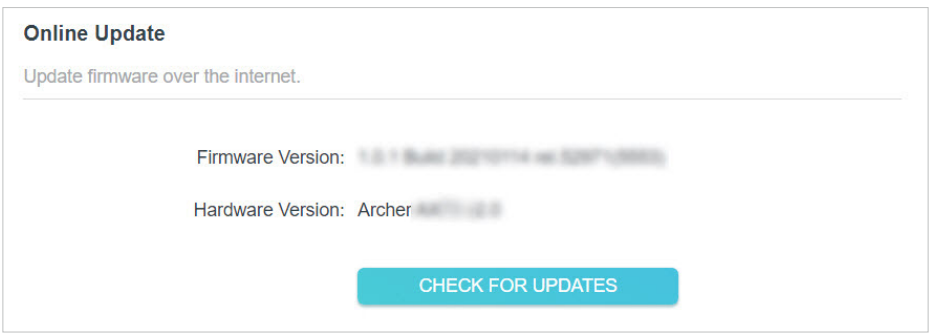
When a new version is available, the access point will update the firmware automatically at the specified time.

8. 5. 2. Online Update

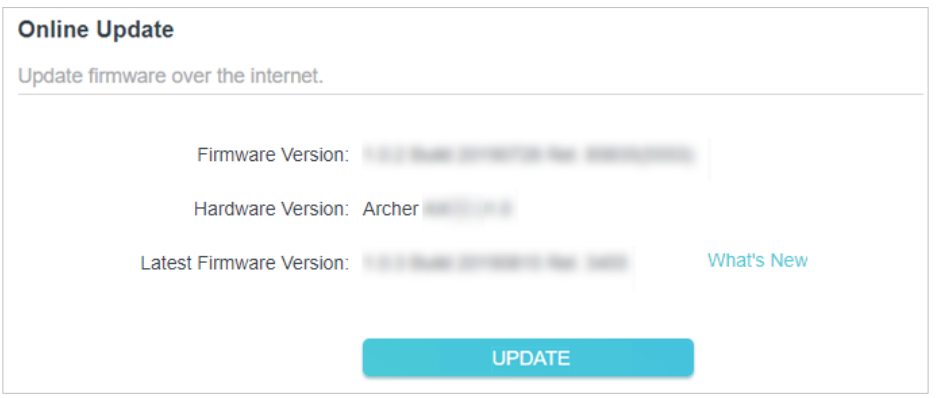
1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Firmware Update.

Tip: When new firmware is available for your access point, the update icon will display in the top-right corner of the web page. You can click the icon to go to the Firmware Update page.

3. Focus on the Online Update section, click CHECK FOR UPDATES to see whether new firmware is available.



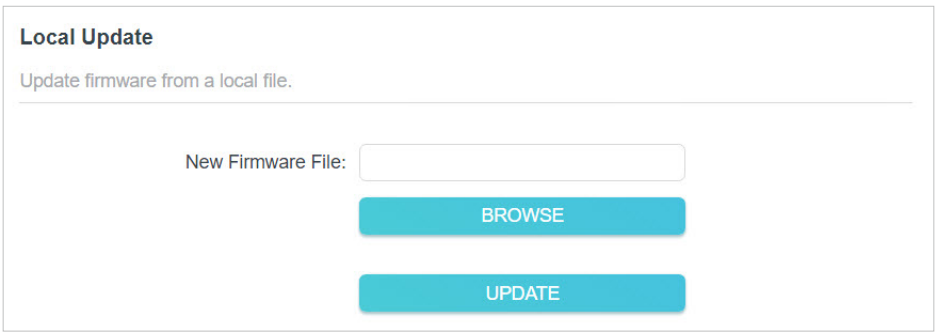
4. Click UPDATE if there is new firmware.



5. Wait a few minutes for the update and reboot to complete.

8. 5. 3. Local Update

1. Download the latest firmware file for the access point from www.tp-link.com.
2. Visit http://tplinkap.net, and log in with the password you set for the access point.
3. Go to System > Firmware Update.
4. Focus on the Local Update section, click BROWSE to locate the downloaded new firmware file, and click UPDATE.



5. Wait a few minutes for the update and reboot to complete.

Note: If you fail to update the firmware for the access point, please contact our Technical Support.

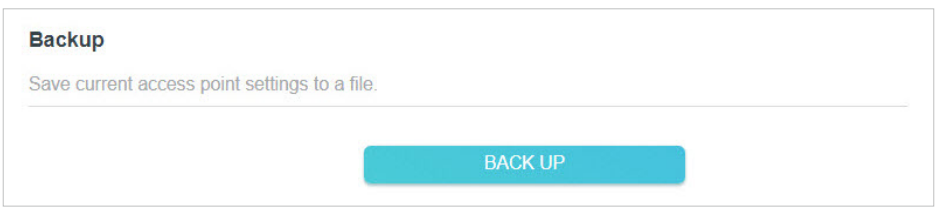
8. 6. Backup and Restore Configuration Settings

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

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Backup & Restore.

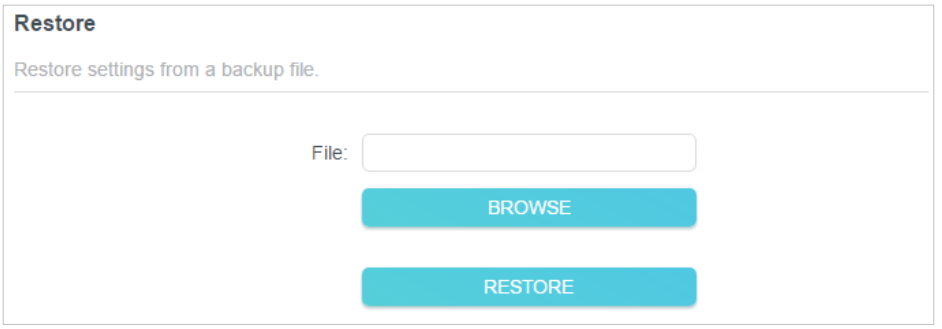
- **To back up configuration settings**

  Click BACK UP to save a copy of the current settings to your local computer. A '.bin' file of the current settings will be stored on your computer.



- **To restore configuration settings**

  1) Click BROWSE to locate the backup configuration file stored on your computer, and click RESTORE.

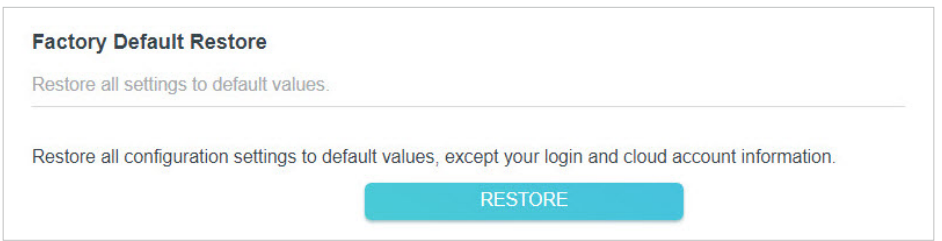


2) Wait a few minutes for the restore and reboot.

Note: During the restore process, do not power off or reset the access point.

- **To reset the access point except your login password and cloud account information:**

1) In the Factory Default Restore section, click RESTORE.



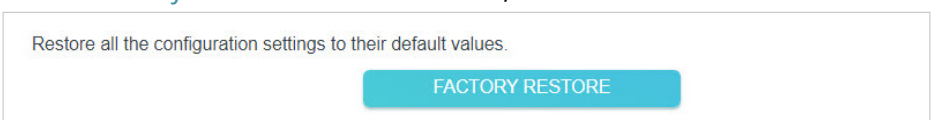
2) Wait a few minutes for the resetting and rebooting.

Note:

- During the resetting process, do not turn off the access point.
- After reset, you can still use the current login password or the TP-Link ID to log in to the web management page.

- **To reset the access point to its factory settings:**

1) In the Factory Default Restore section, click FACTORY RESTORE.



2) Wait a few minutes for the resetting and rebooting.

Note:

- During the resetting process, do not turn off or reset the access point.
- We strongly recommend you back up the current configuration settings before resetting the access point.

8. 7. Reboot the Access Point

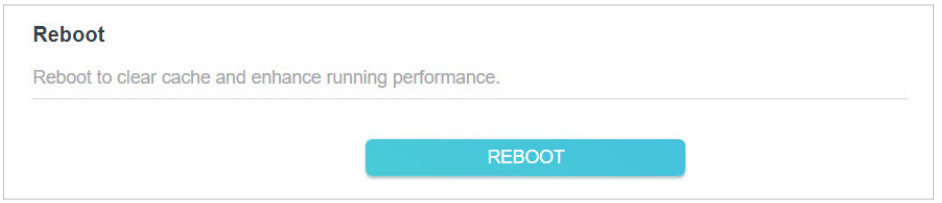
Rebooting help clean cache and enhance running performance of the access point. You can reboot the access point immediately or schedule it to reboot periodically.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.

2. Go to System > Reboot.

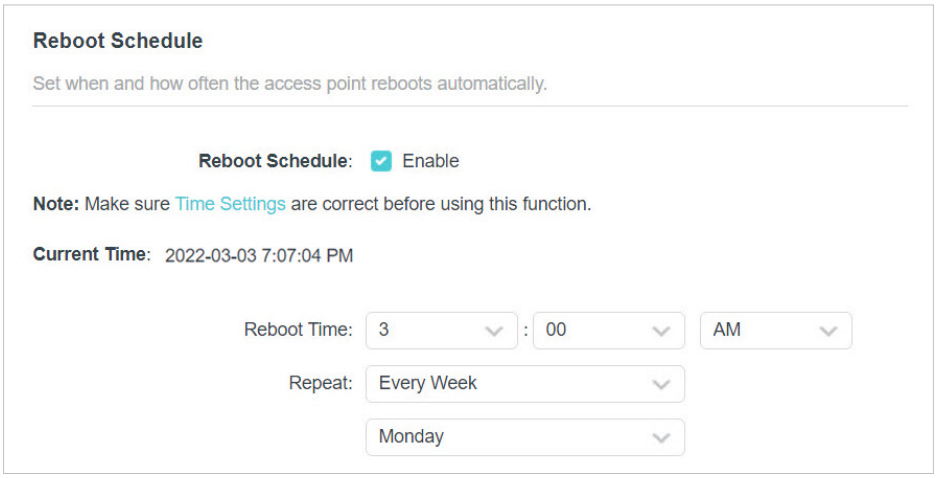
- **To reboot the access point immediately:**

  Click REBOOT.



- **To schedule the access point to reboot periodically:**

  1) Enable Reboot Schedule.



  2) Set the Reboot Time and Repeat time.

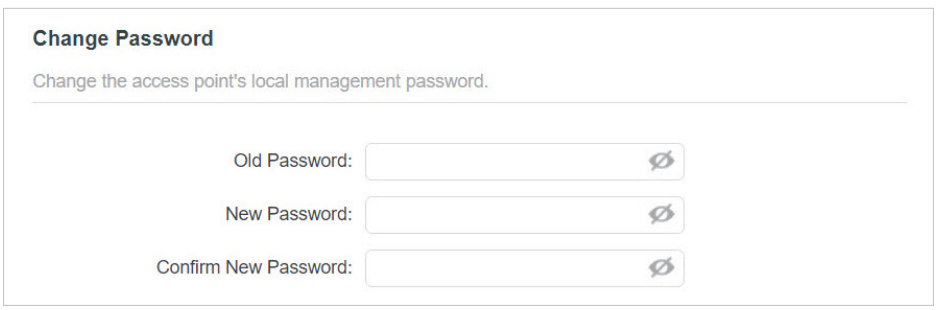
  3) Click SAVE. The access point will reboot periodically as scheduled.

8. 8. Change the Login Password

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

1. Visit http://tplinkap.net, and log in with the password you set for the access point.

2. Go to System > Administration.



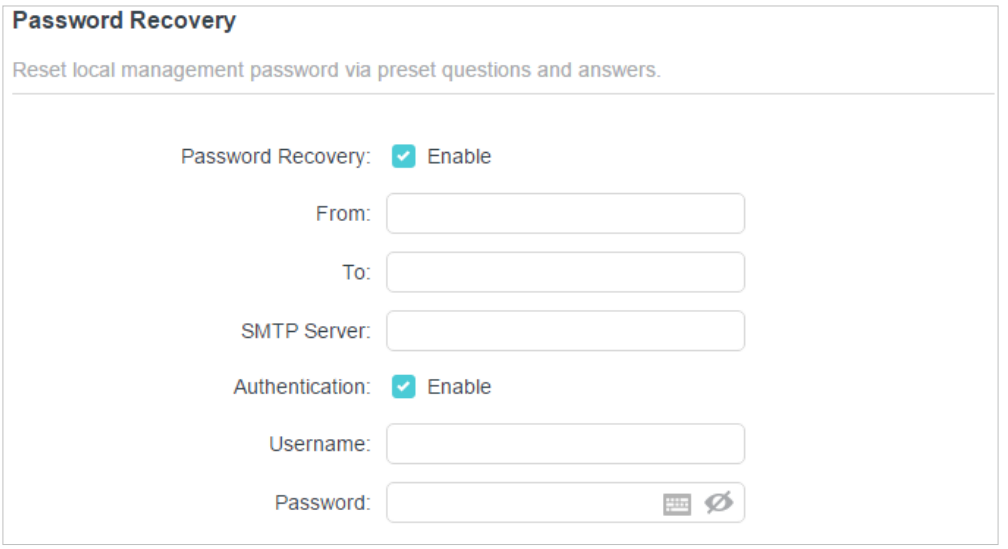
3. Enter the old password, and then enter a new password twice (both case-sensitive).

4. Click SAVE and use the new password for future logins.

8. 9. Password Recovery

This feature allows you to recover the login password you set for you access point in case you forget it.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Administration and focus on the Password Recovery section.
3. Enable Password Recovery.



4. Specify a mailbox (From) for sending the recovery letter and enter its SMTP Server address.
5. Specify a mailbox (To) for receiving the recovery letter.
6. If the mailbox (From) to send the recovery letter requires encryption, tick the Enable box of Authentication and enter its username and password.

   Tips:

   - SMTP server is available for users in most webmail systems. For example, the SMTP server address of Gmail is smtp.gmail.com.
   - Generally, Authentication should be enabled if the login of the mailbox requires username and password.

7. Click SAVE.

To recover the login password, visit http://tplinkap.net, click Forgot Password? on the login page and follow the instructions to set a new password.

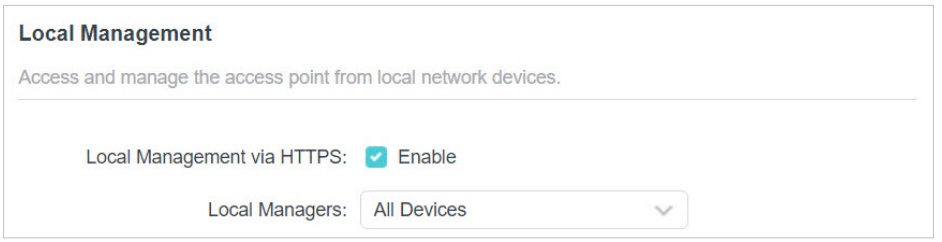
8. 10. Local Management

This feature allows you to limit the number of client devices on your LAN from accessing the access point by using the MAC address-based authentication.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Administration and focus on the Local Management section.

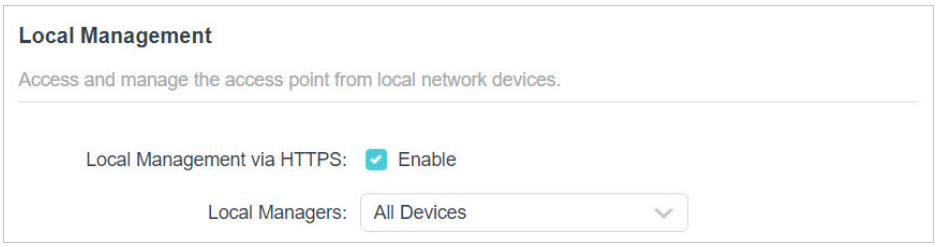
- **Access the access point via HTTPS and HTTP:**

Tick the Enable box of Local Management via HTTPS to access the access point via HTTPS and HTTP, or keep it disabled to access the access point only via HTTP.



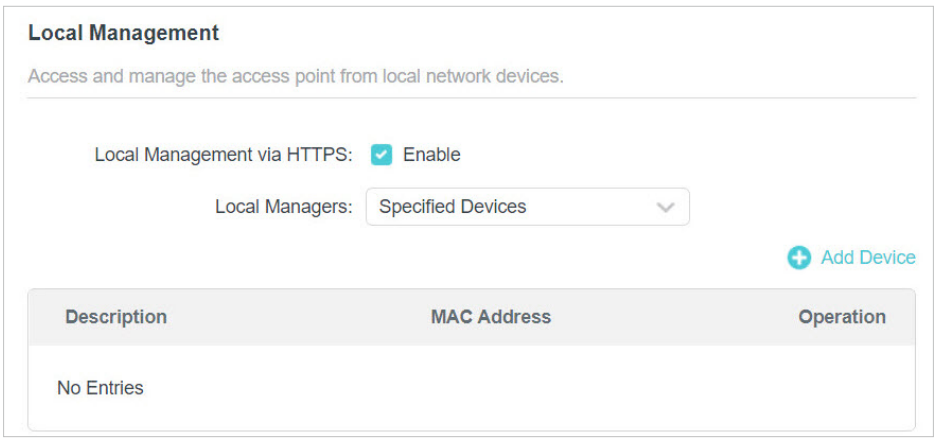
- **Allow all LAN connected devices to manage the access point:**

Select All Devices for Local Managers.

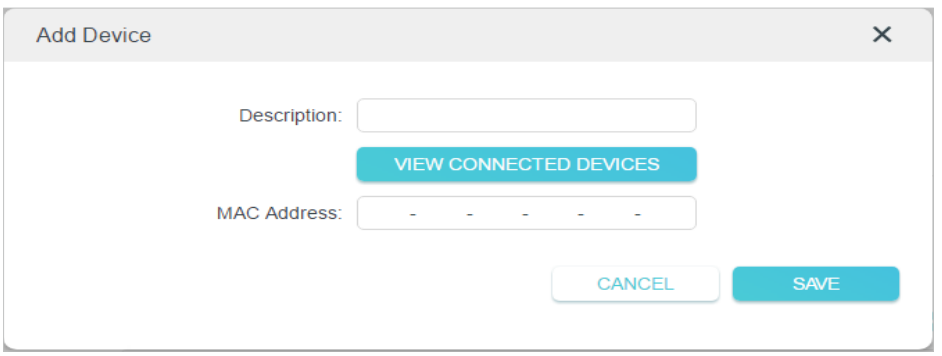


- **Allow specific devices to manage the access point:**

1. Select Specified Devices for Local Managers and click SAVE.



2. Click Add Device.



3. Click VIEW CONNECTED DEVICES and select the device to manage the access point from the devices list, or enter the MAC address of the device manually.
4. Specify a Description for this entry.
5. Click SAVE.

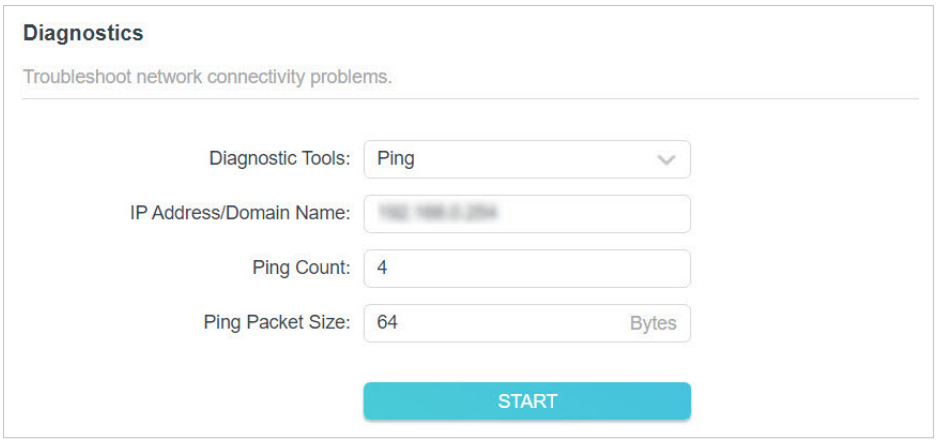
8. 11. Test the Network Connectivity

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

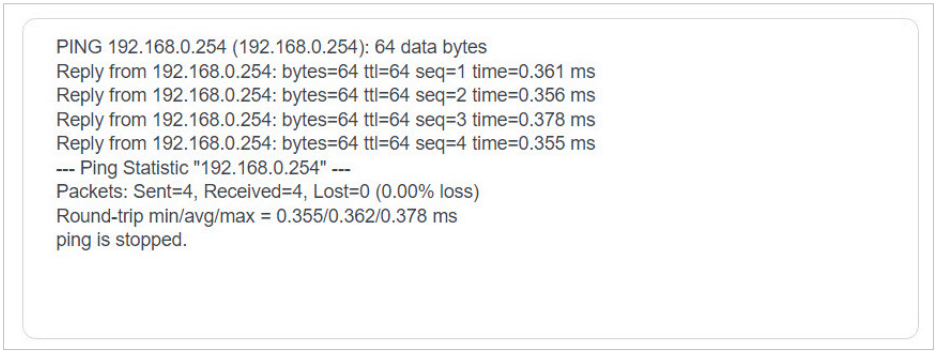
Ping is used to test the connectivity between the access point and the tested host, and measure the round-trip time.

Traceroute is used to display the route (path) your access point has passed to reach the tested host, and measure transit delays of packets across an Internet Protocol network

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Diagnostics.
   - **To test the connectivity via Ping:**
     1) Choose Ping as the diagnostic tool.

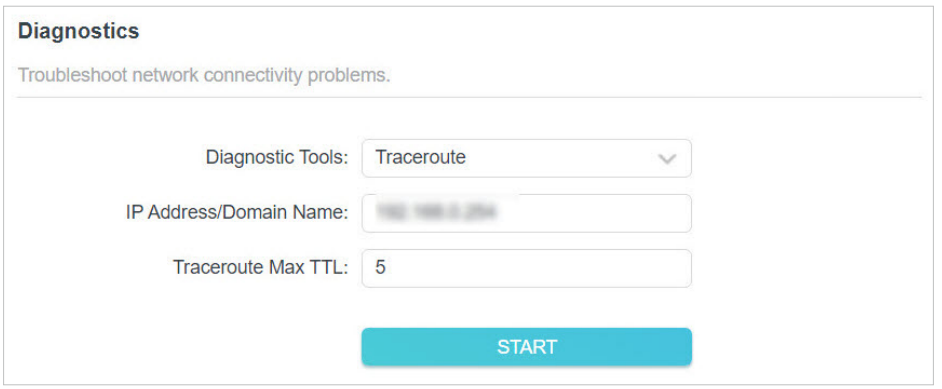


     2) Enter the IP Address or Domain Name of the tested host.
     3) Keep the default Ping Count and Ping Packet Size.
     4) Click START to begin the diagnostics. The diagnostics result will be displayed.



- **To test the connectivity via Traceroute:**

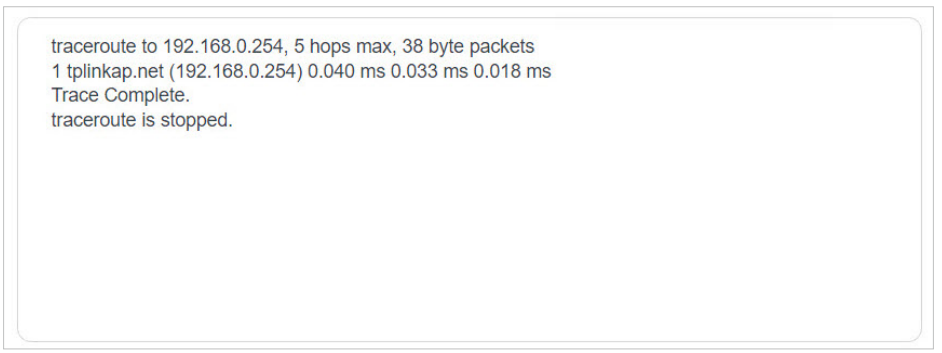
1) Choose Traceroute as the diagnostic tool.



2) Enter the IP Address or Domain Name of the tested host.

3) Keep the default Traceroute Max TTL.

4) Click START to begin the diagnostics. The diagnostics result will be displayed.



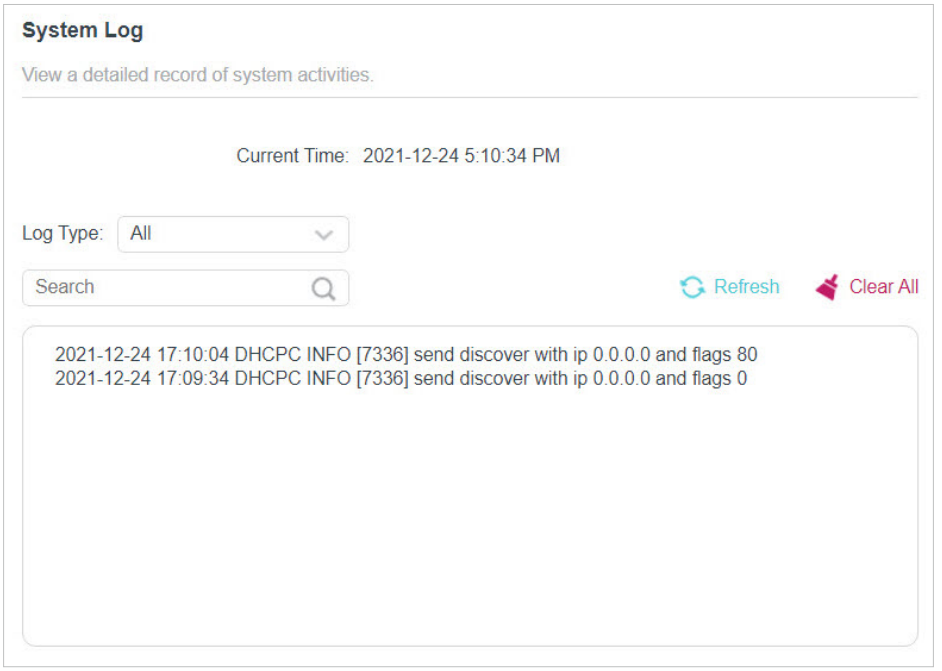
8. 12. System Log

When the access point does not work normally, you can save the system log and send it to the technical support for troubleshooting.

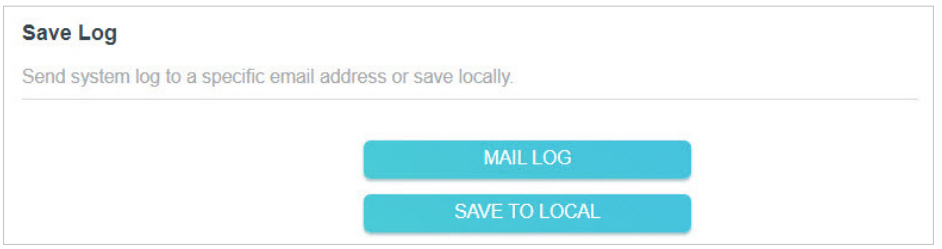
- **To save the system log locally:**

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > System Log.

3. Choose the type and level of the system logs as needed.



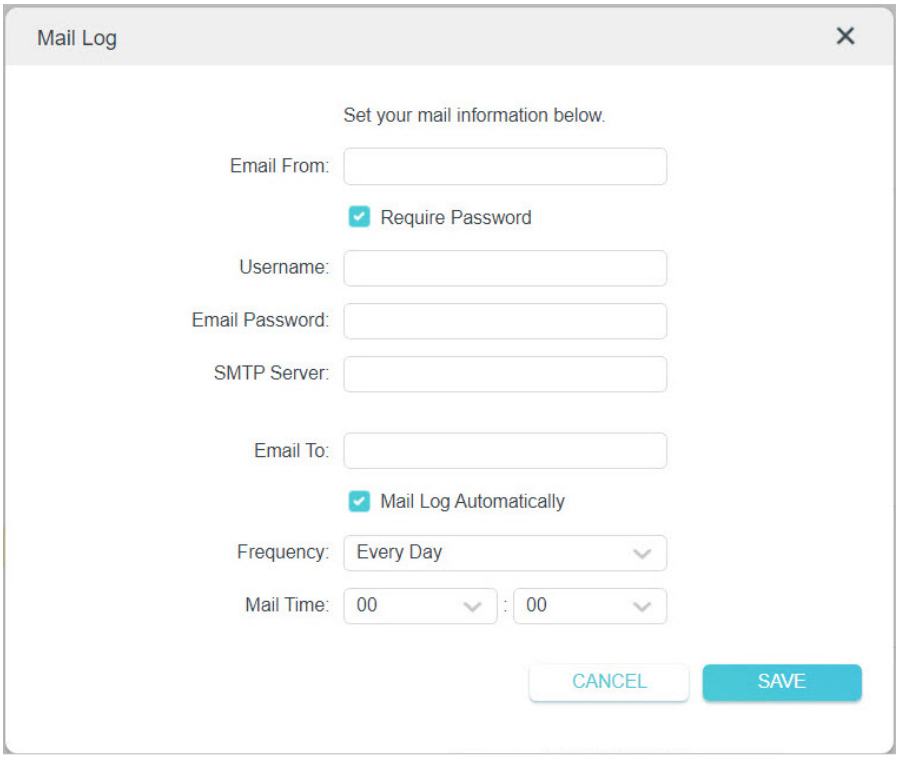
4. In the Save Log section, click SAVE TO LOCAL to save the system logs to a local disk.



- **To send the system log to a mailbox at a fixed time:**

For example, I want to check my access point's working status at a fixed time every day, however, it's too troublesome to log in to the web management page every time I want to go checking. It would be great if the system logs could be sent to my mailbox at 8 a.m. every day.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > System Log.
3. In the Save Log section, click MAIL LOG.
4. Enter the information required:



1) Email From: Enter the email address used for sending the system log.

2) Select Require Password.

Tips: Generally, Require Password should be selected if the login of the mailbox requires username and password.

3) Username: Enter the user name to log in to the sender's email address.

4) Email Password: Enter the password to log in to the sender's email address.

5) SMTP Server: Enter the SMTP server address.

Tips: SMTP server is available for users in most webmail systems. For example, the SMTP server address of Hotmail is smtp-mail.outlook.com.

6) Email To: Enter the recipient's email address, which can be the same as or different from the sender's email address.

7) Select Mail Log Automatically.

Tips: The access point will send the system log to the designated email address if this option is enabled.

8) Frequency: This determines how often the recipient will receive the system log.

9) Mail Time: Set the time when the recipient will receive the system log.

5. Click SAVE.

FAQ

Q1. How do I restore the access point to its factory default settings?

With the access point powered on, use a pin to press and hold the Reset button until the Power LED blinks, then release the button.

Note: Resetting the access point will clear all previous configurations, and the access point will reset to the default Access Point mode.

Q2. What should I do if I cannot access the web management page?

- If the computer has a static IP address, change its settings to obtain an IP address automatically.
- Verify that http://tplinkap.net or http://192.168.0.254 is correctly entered in the web browser.
- Use another web browser and try again.
- Reboot your access point and try again.
- Power off your host AP and enter http://tplinkap.net in the web browser to try again.

Q3. What should I do if I forget my wireless password?

The default wireless password is printed on the label of the access point. If the password has been altered, please connect your computer to the access point using an Ethernet cable and follow the steps below:

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Wireless Settings to retrieve or reset your wireless password.

Q4. What should I do if I forget my login password of the web management page?

1. Refer to Q1 to reset the access point to its factory default settings.
2. Visit http://tplinkap.net, and create a new login password.

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

Q5. What should I do if my wireless is not stable?

This could be caused by interference. You can try the following methods:

- Log in to the web management page. Go to Wireless > Wireless Settings and change your wireless channel to a different one.
- Move the access point to a new location away from Bluetooth devices and other household electronics, such as cordless phones, microwaves, and baby monitors, to minimize signal interference.

Q6. What should I do to maximize my signal strength in Range Extender mode?

When choosing an ideal location to optimize wireless signal in Range Extender mode, please refer to the following recommendations.

- Halfway is the best way.

  Generally, the ideal location for an access point is about halfway between your wireless router and your wireless clients and make sure that the location you choose is within the range of the host router. If that is not possible, place it closer to your wireless router to ensure stable performance.

- Fewer obstacles ensure better performance.

  Choose a location with less obstacles around that may block the signal between the access point and the host network. An open corridor or a spacious location is ideal.

- Less interference provides more stability.

  Choose a location away from Bluetooth devices and other household electronics, such as cordless phones, microwaves, and baby monitors to minimize signal interference.

FCC compliance information statement

Product Name: AX1800 Gigabit Wi-Fi 6 Access Point

Model Number: TL-WA1801

Component Name	Model
I.T.E. Power Supply	T480038-2B1

Responsible party:

TP-Link USA Corporation

Address: 10 Mauchly, Irvine, CA 92618

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

Tel: +1 626 333 0234

Fax: +1 909 527 6804

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.

FCC compliance information statement

Product Name: I.T.E. Power Supply
Model Number: T480038-2B1
Responsible party:
TP-Link USA Corporation
Address: 10 Mauchly, Irvine, CA 92618
Website: http://www.tp-link.com/us/
Tel: +1 626 333 0234
Fax: +1 909 527 6804
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: 2023-06-13

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 (19dB)

5150 MHz -5250 MHz (22dB)

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/support/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.

National Restrictions

Frequency band: 5150 - 5250 MHz:

Indoor use: Inside buildings only. Installations and use inside road vehicles and train carriages are not permitted. Limited outdoor use: If used outdoors, equipment shall not be attached to a fixed installation or to the external body of road vehicles, a fixed infrastructure or a fixed outdoor antenna. Use by unmanned aircraft systems (UAS) is limited to within the 5170 - 5250 MHz band.

	AT	BE	BG	CH	CY	CZ	DE	DK
	EE	EL	ES	FI	FR	HR	HU	IE
	IS	IT	LI	LT	LU	LV	MT	NL
	NO	PL	PT	RO	SE	SI	SK	UK(NI)

UKCA Mark

UK
CA

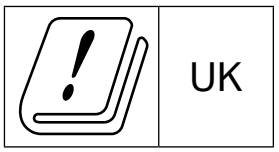
UK Declaration of Conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.

The original UK Declaration of Conformity may be found at
https://www.tp-link.com/support/ukca

National Restrictions

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 & BSMI Notice:

注意!

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。

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。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

限用物質含有情況標示聲明書

設備名稱：AX1800 Gigabit Wi-Fi 6 Access Point Equipment name	型號（型式）：TL-WA1801 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	—	○	○	○	○	○
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.

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°C ~ 40°C (32°F ~ 104°F)
- This product uses radios and other components that emit electromagnetic fields. Electromagnetic fields and magnets may interfere with pacemakers and other

implanted medical devices. Always keep the product and its power adapter more than 15 cm (6 inches) away from any pacemakers or other implanted medical devices. If you suspect your product is interfering with your pacemaker or any other implanted medical device, turn off your product and consult your physician for information specific to your medical device.

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
	AC voltage
	Class II equipment
	Polarity of output terminals
	Energy efficiency Marking
	Indoor use only
	Caution
	Operator's manual
	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.