Acer Connect Ovia T360
Dual Band Wi-Fi 7 Mesh Router
User Manual V1.0

Revision Jan, 2026

Contents

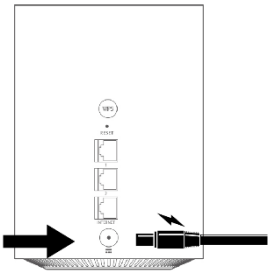
1. Overview

The Acer Connect Ovia T360 is a dual-band wireless router supporting the latest Wi-Fi 7 (IEEE 802.11be) standard, designed for home and small office use. It delivers improved efficiency and reduced latency to support high-definition streaming, online collaboration, cloud services, and multiple connected devices.

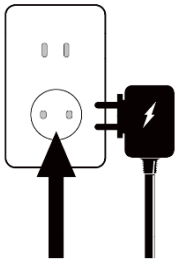
With a streamlined setup process and an intuitive management interface, the T360 allows users to quickly configure and manage their network. It also provides essential features such as device management, guest network support, and basic security settings to help maintain a stable and reliable wireless environment.

2. Installation and Setup

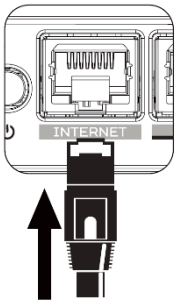
2.1. Plug in the AC adapter



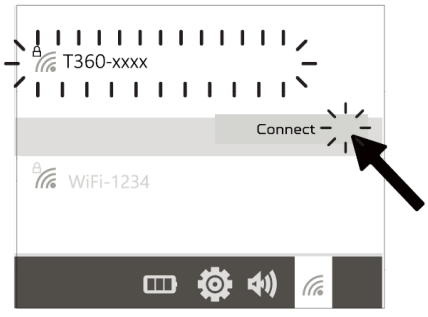
2.2. Plug into outlet.



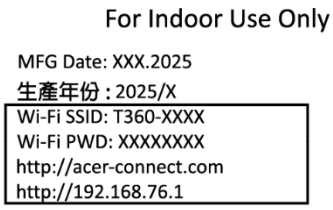
2.3. Plug in internet cable.



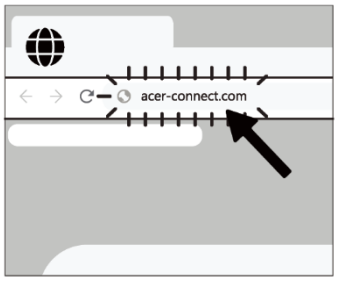
2.4. Connect to T360 Wi-Fi.



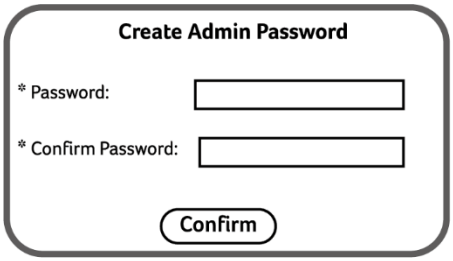
2.5. Important info at bottom of device.



2.6. Enter acer-connect.com to browser.



2.7. Set an admin password first to access the Internet or use the oruter.



2.8. The device can be either setup via acer Connect mobile App or the browser web admin.
How to setup the router via **Acer Connect Mobile App**:

- Use a mobile device camera to scan the QR code below.
  Download the acer Connect mobile App via Play Store or App Store.

Download APP

Available on the App Store

GET IT ON Google Play

- Open the acer Connect Mobile App and follow the steps for registering an account. Go to your email inbox, review the registration email, and input the 4-digit registration code onto the mobile App. When the whole process is completed, you will be automatically signed in.

- Launch the app and grant the required permissions when prompted.
  Ensure that your mobile device is connected to the T360 Wi-Fi network.
  After signing in, the app will automatically detect the router on the local network.
  Follow the on-screen instructions to complete the router setup.

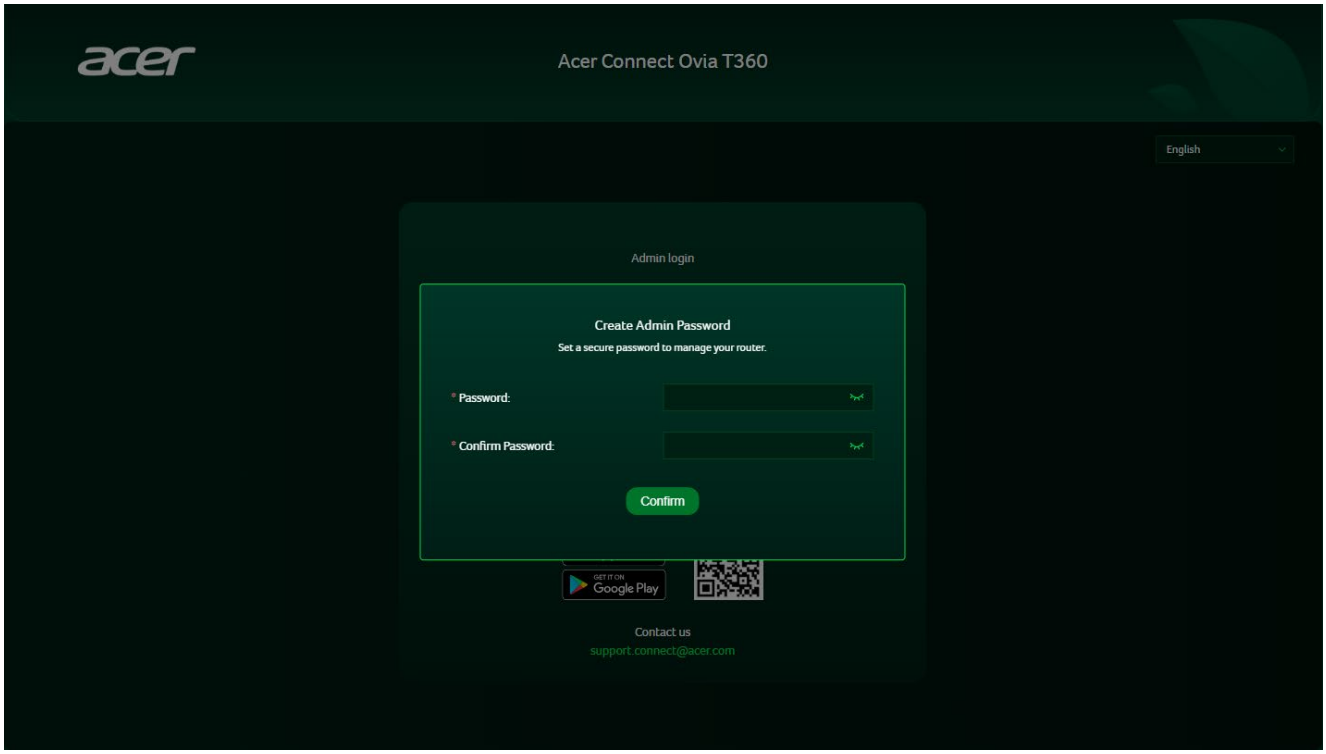
3.Initial Configuration

During first-time setup, you must create an Admin password before using the router.

For initial configuration, connect to the Acer Connect Ovia T360 Web Portal by opening a web browser and entering http://acer-connect.com or http://192.168.76.1 in the address bar.

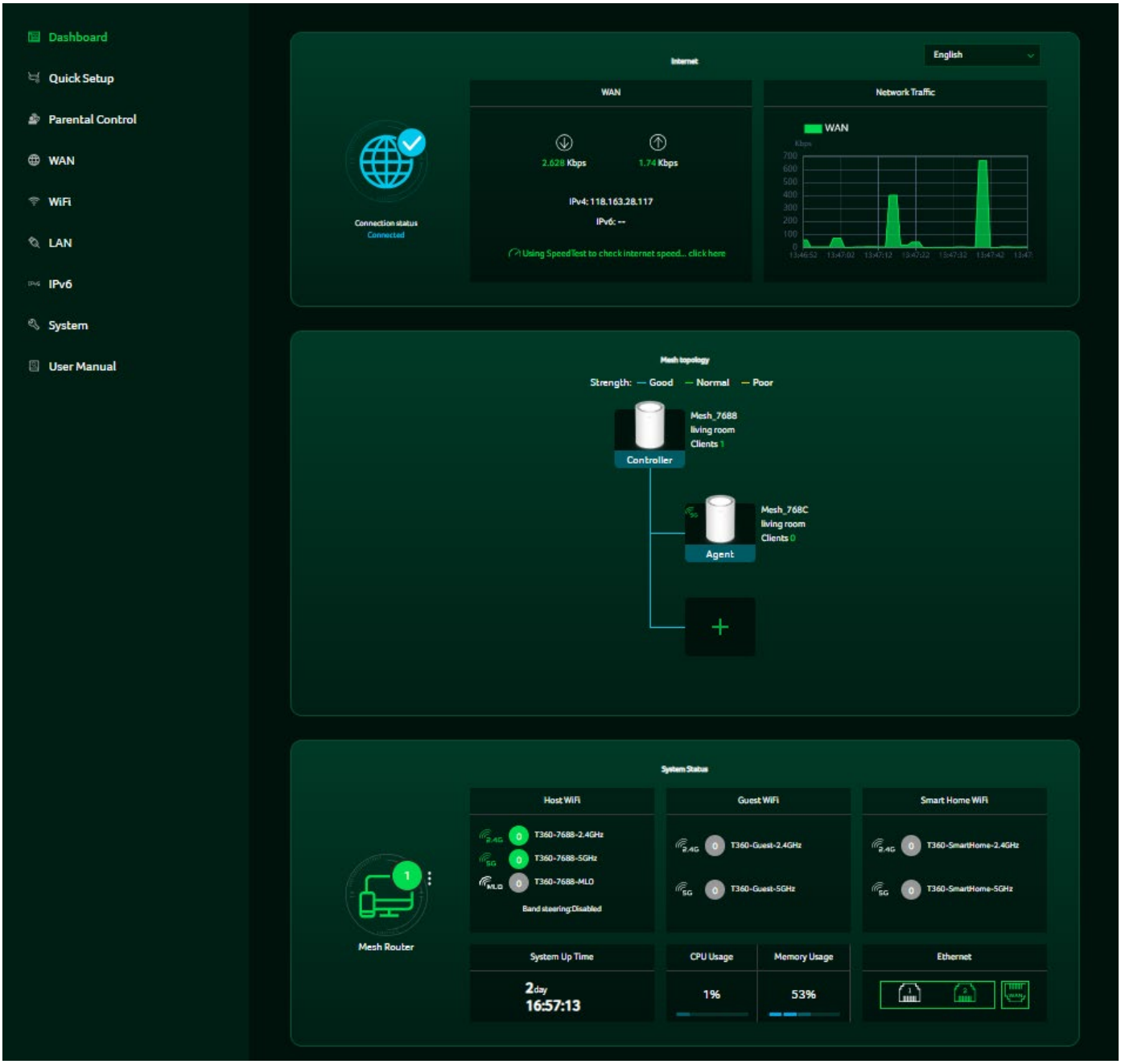
When prompted, create an Admin password to manage the router. After the password is set, you can continue with the router configuration.

The Web UI language is automatically determined based on your browser settings. To change to another language, click the drop-down arrow in the upper-right corner of the page, or select your preferred language from the language settings within the system.



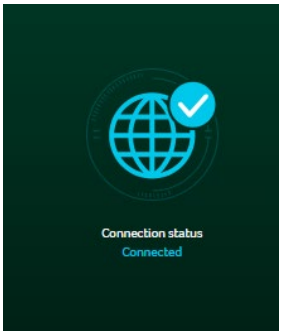
4. Dashboard

After logging in successfully, the dashboard of the Acer Connect Ovia T360 provides an overview of the router's status and key information.



4.1. Connection Status:

This section indicates the current Internet connection status of the router. When the connection is established successfully, the status shows **Connected**, confirming that the router is online and able to access the Internet.

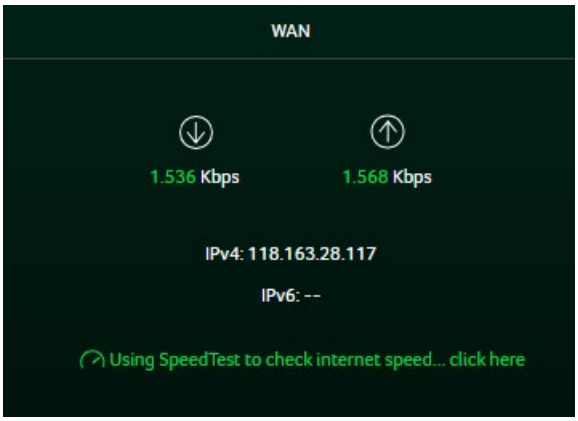


4.2. WAN:

The WAN section provides detailed information about the router's Internet connection. It displays the current download and upload traffic rate, allowing users to monitor network performance.

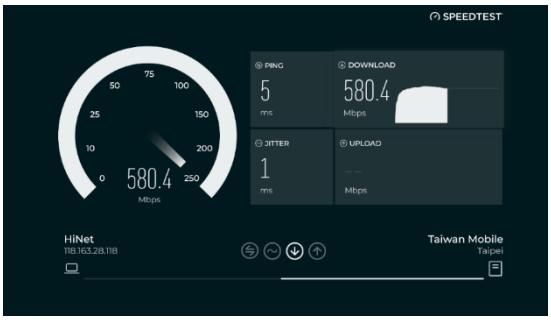
This section also shows the assigned IPv4 address and the status of IPv6 connectivity. If IPv6 service is not available or not enabled by the Internet Service Provider (ISP), the IPv6 field will appear unavailable.

In addition, users can click Speed Test to perform an Internet speed test directly from the Web UI. This feature measures the current Internet bandwidth and helps verify connection quality.



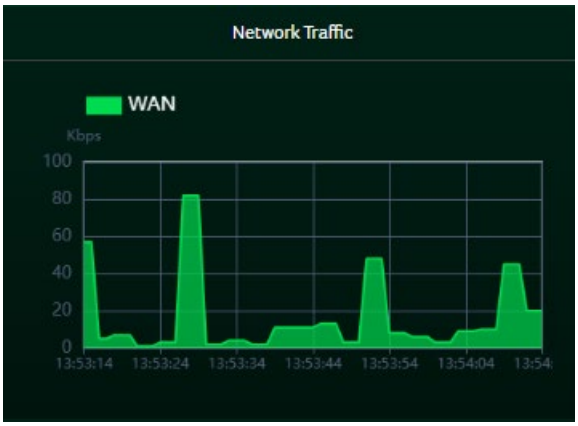
4.2.1. Network Speed Test

1. Powered by Ookla. Pressing the "GO" button tests the speed of the WAN connectivity.
2. You can manually select a server by clicking on the dropdown arrow to display available servers.
3. Clicking the "GO" button will test the network speed and display the results, as shown on the right.



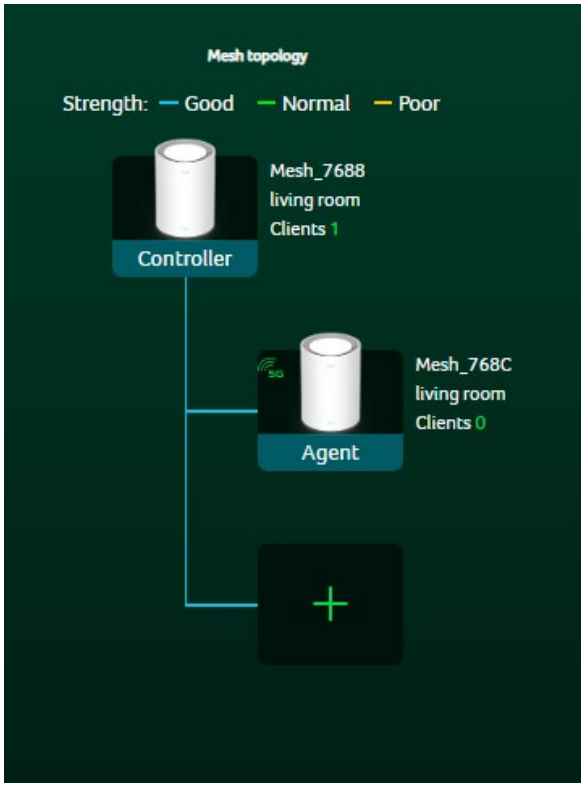
4.3. Network Traffic:

This section presents a graphical view of WAN network traffic over time. It allows users to monitor data transmission activity, helping to identify usage patterns and overall network load.



4.4. Mesh Topology:

The Mesh Topology section provides a visual representation of the current mesh network structure and connection status.
When using a multi-pack router bundle, the first router that is powered on, logged into, and configured with an admin password and Internet connection is automatically assigned as the Mesh Controller.



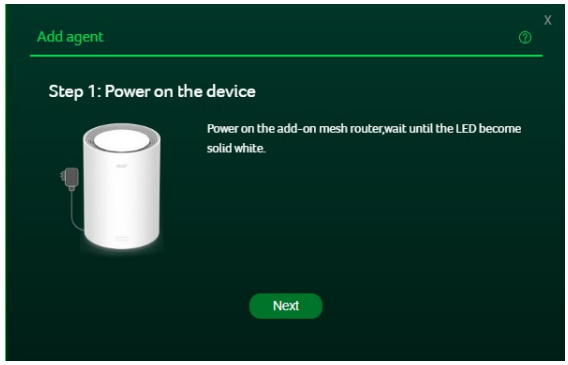
To add additional mesh Agent, click the "**+**" icon at the bottom of the topology view and follow the on-screen instructions to add an Agent.

This view also allows users to assess the backhaul signal quality between the Controller and each Agent, indicated by the signal strength status (Good / Normal / Poor). In addition, the number of connected client devices and the assigned location for each node are displayed, helping users evaluate mesh performance and placement.

4.4.1. Add Agent

Step 1: Power on the Device

Power on the additional router that you want to add as a Mesh Agent.



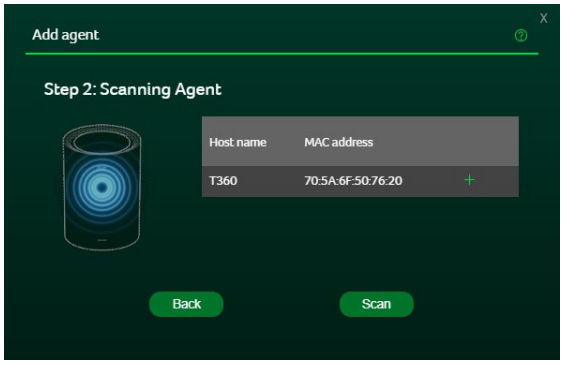
Wait until the LED indicator becomes solid white, indicating that the device is ready for pairing.

Click Next to continue.

4.4.2. Add Agent

Step 2: Scanning Agent

The system scans for available mesh devices nearby.



If no device appears automatically, click Scan search again.

When the router's MAC address is displayed in the list, click the **"+"** icon next to the device to proceed to the next step.

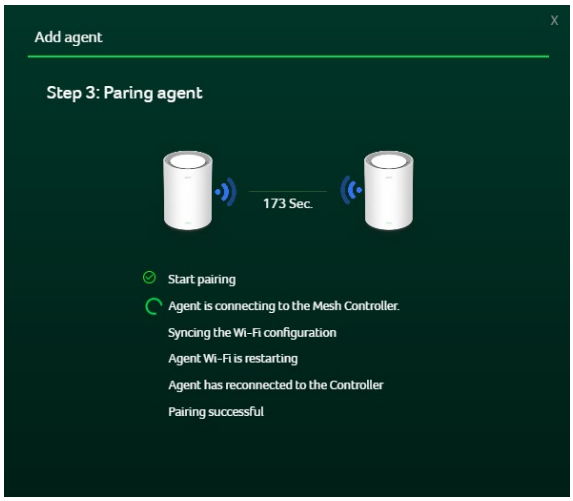
4.4.3. Add Agent

Step 3: Pairing Agent

During this step, the selected router attempts to connect to the Mesh Controller.

The pairing progress and connection status are displayed on the screen.

Please keep both devices powered on and within range during this process.



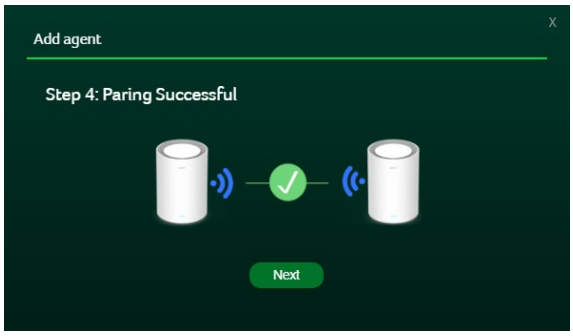
4.4.4. Add Agent

Step 4: Pairing Successful

Once pairing is complete, a confirmation message is displayed.

The newly added router is now successfully connected as a Mesh Agent.

Click Next to finish the setup.

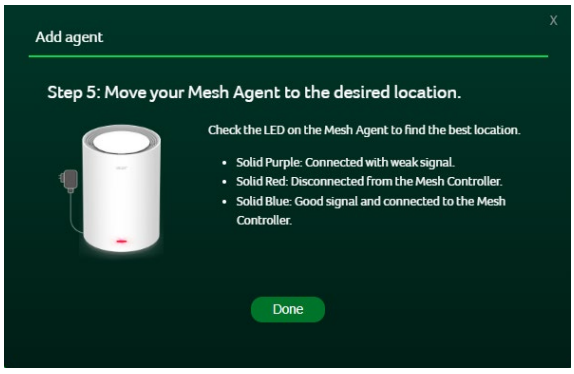


4.4.5. Add Agent

Step 5: Move the Mesh Agent to the Desired Location

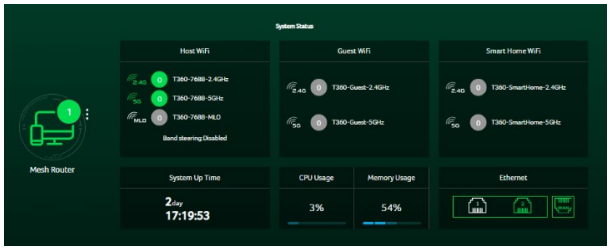
After the Mesh Agent has been added successfully, move it to the desired location. Check the LED indicator on the Mesh Agent to evaluate the connection status and signal quality.

When placement is complete, click Done to finish.



4.5. System Status

The System Status section provides an overview of the router's operational state, including Wi-Fi network status (Host Wi-Fi, Guest Wi-Fi, and Smart Home Wi-Fi), system uptime, CPU usage, memory usage, and Ethernet port status. It allows users to quickly assess overall system health and network availability.

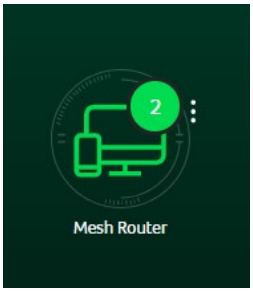


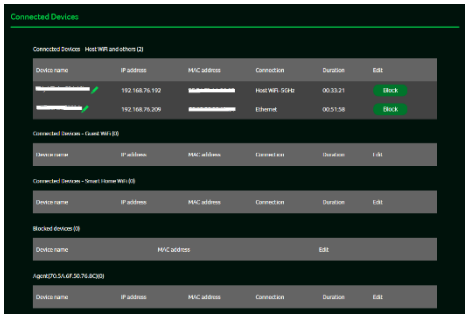
4.5.1. Role and Devices

This section indicates the current role of the router within the mesh network, such as whether the device is operating as a Mesh Router or a Mesh AP Mode.

It also displays the number of client devices currently connected to this router.

By clicking the three-dot (⋮) icon in the upper-right corner, users can view detailed information about the connected devices, including connection status and related details.



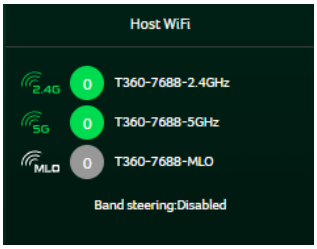


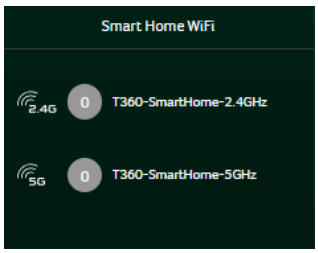
4.5.2. Host / Guest / Smart Home Wi-Fi

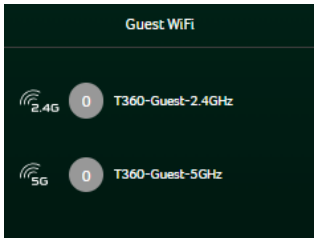
This section displays the status of the Host, Guest, and Smart Home wireless networks. By default, the Wi-Fi SSIDs are generated with the prefix T360-XXXX-XXX. Users can modify the SSID names at any time by going to the Wi-Fi settings page if customization is required.

The Guest Wi-Fi network provides Internet access for visitors while maintaining separation from the main network. The Smart Home Wi-Fi network is designed for smart home and IoT devices.

Note: Devices connected to the Host Wi-Fi and Smart Home Wi-Fi networks can communicate with each other, while the Guest Wi-Fi network is isolated for security purposes.

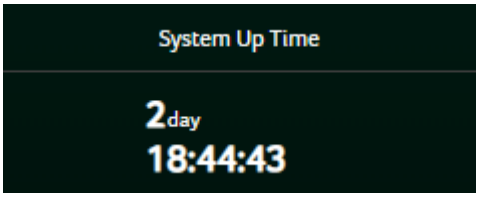






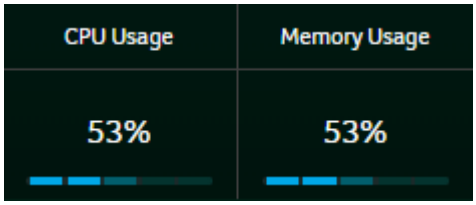
4.5.3. System Up Time

This section shows the amount of time the router has been operating since the last restart or power cycle. It helps users monitor system stability and determine how long the router has been running continuously.



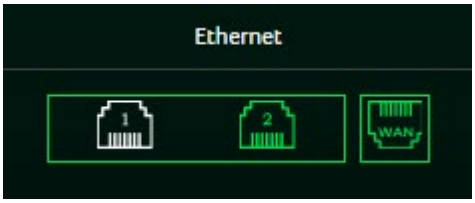
4.5.4. CPU Usage / Memory Usage

This section displays the current CPU usage and memory usage of the router in real time. These indicators reflect the system resource consumption and overall operating load. Higher usage levels may occur during periods of heavy network activity or advanced feature operation.



4.5.5. Ethernet

This section displays the connection status of the Ethernet ports on the router. Each icon represents a physical port and indicates whether a wired connection is connected or active. The status of the WAN port is also shown.



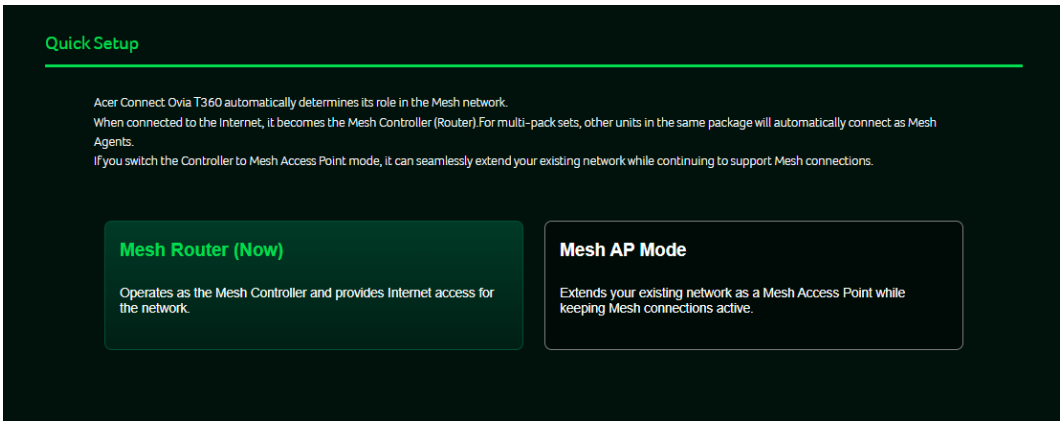
5. Quick Setup

During Quick Setup, the Acer Connect Ovia T360 automatically determines its role within the mesh network.
When connected to the Internet, it operates as the Mesh Controller. In multi-pack configurations, additional units are automatically added as Mesh Agents.

If Mesh AP Mode is selected, the device functions as a Mesh Access Point to extend an existing network.

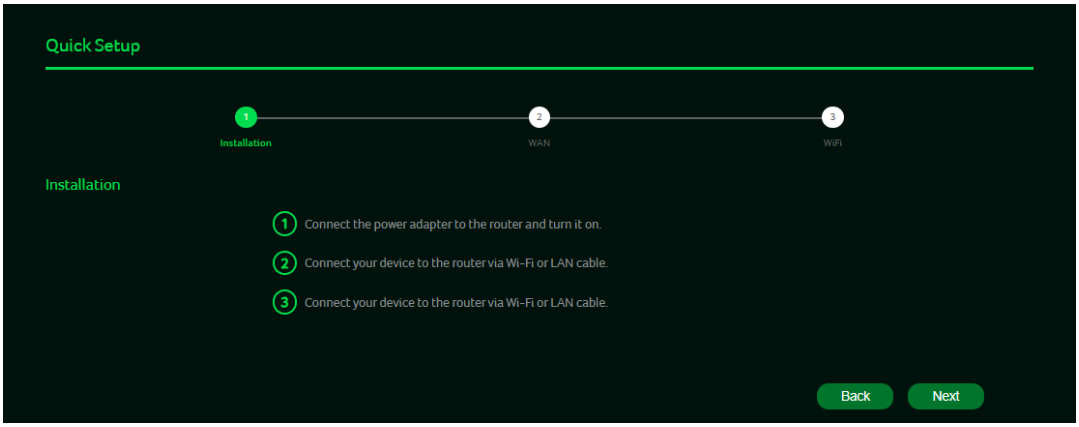
5.1 Mesh Router Setup

Mesh Router Mode allows the Acer Connect Ovia T360 to operate as the Mesh Controller of the network. In this mode, the device provides Internet access, manages network settings, and coordinates mesh connections between all mesh nodes.



Step 1: Installation
In this step, prepare the router and your device for configuration.

1. Connect the power adapter to the router and turn it on.
2. Connect your device (computer or mobile device) to the router using Wi-Fi or an Ethernet cable.
3. Click Next to continue.

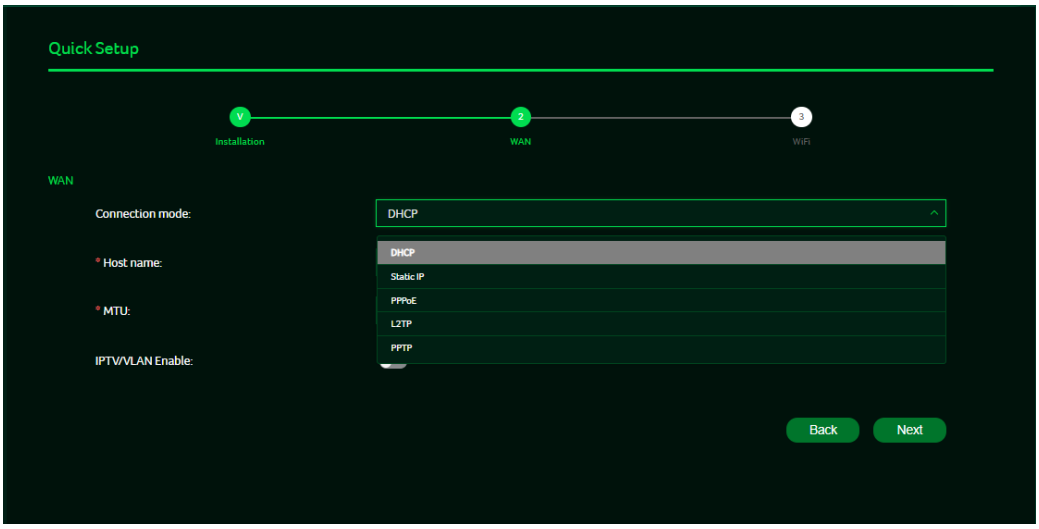


Step 2: WAN
Configure the Internet connection settings provided by your Internet Service Provider (ISP).

1. Select the Internet connection mode provided by your Internet Service Provider (ISP).
   In most cases, DHCP is selected by default and works for typical home networks.
   If your ISP requires a specific connection mode or additional settings, please follow the

information provided by your ISP.

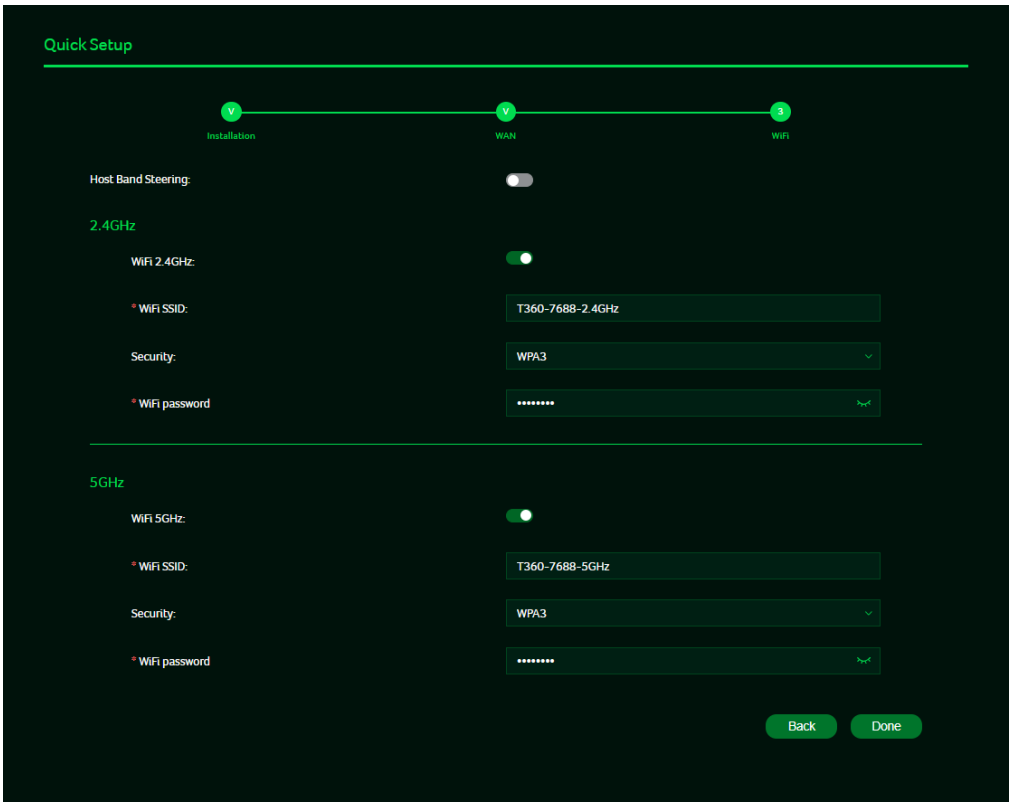
2. Enter any required information if prompted by your ISP.
3. Click Next to proceed.



Step 3: Wi-Fi

Set up your wireless network settings.

1. Enable or disable Host Band Steering as required.
2. Configure the 2.4 GHz and 5 GHz Wi-Fi settings, including:
   - Wi-Fi SSID
   - Security type
   - Wi-Fi password
3. Review the settings and click Done to complete the setup.

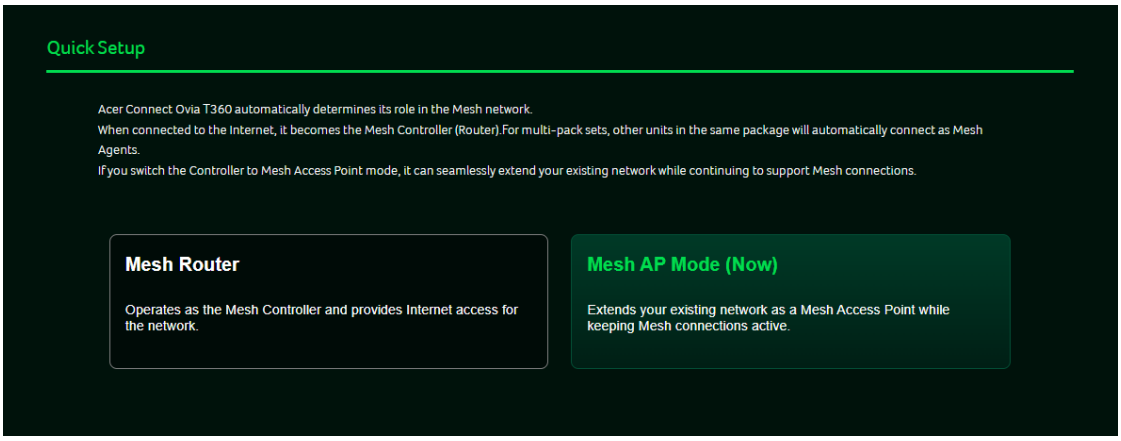


5.2 Mesh AP Mode Setup

Mesh AP Mode allows the Acer Connect Ovia T360 to extend an existing home network while continuing to support mesh connections between devices.

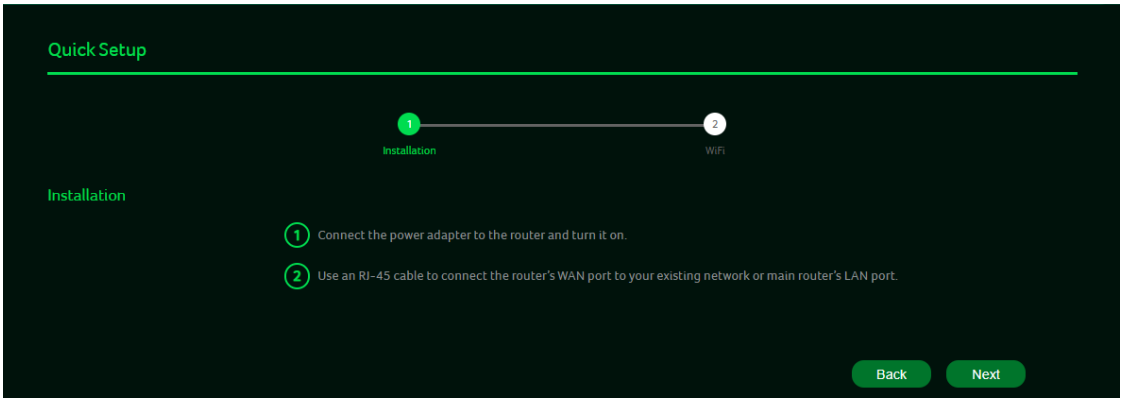
Step 1: Select Mesh AP Mode

During Quick Setup, select Mesh AP Mode to configure the device as a Mesh Access Point.



Step 2: Installation

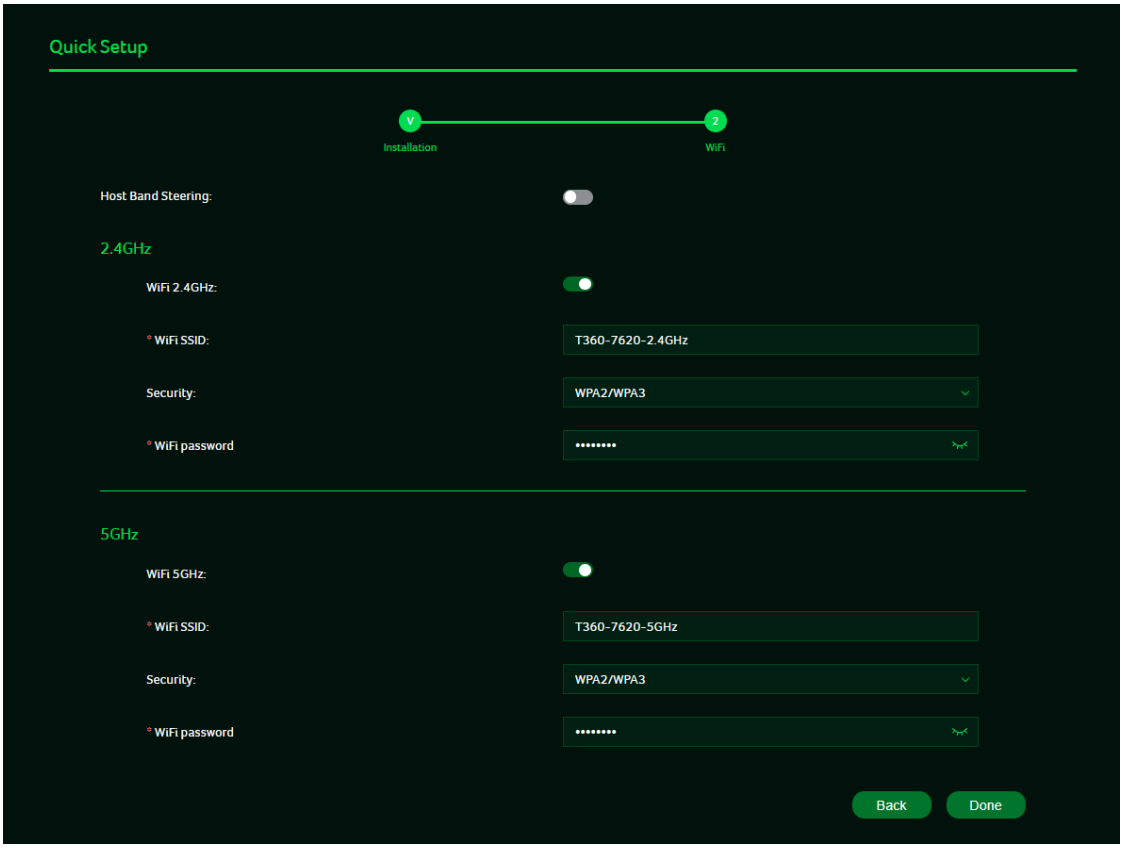
1. Connect the power adapter to the router and turn it on.
2. Use an Ethernet cable to connect the router's WAN or LAN port to the existing network provided by your main router or gateway.
3. Click Next to continue.



Step 3: Wi-Fi Settings

Configure the wireless settings for Mesh AP Mode.

1. Enable or disable Host Band Steering as required.
2. Configure the 2.4 GHz and 5 GHz Wi-Fi settings, including:
   - Wi-Fi SSID
   - Security type
   - Wi-Fi password
3. Click Done to apply the settings.



Completion

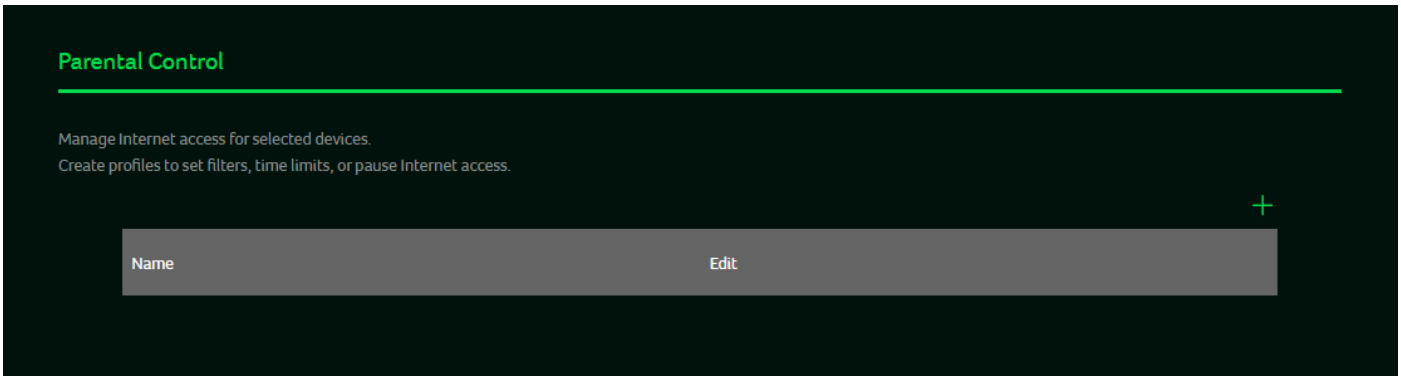
After setup is complete, the device operates as a Mesh Access Point, extending the existing network coverage while maintaining mesh connectivity.

Note

- In Mesh AP Mode, the router does not act as the main router and does not assign IP addresses.
- The device receives an IP address from the upstream router.
- To access the management page after setup, use the IP address assigned by the upstream router.

6. Parental Control

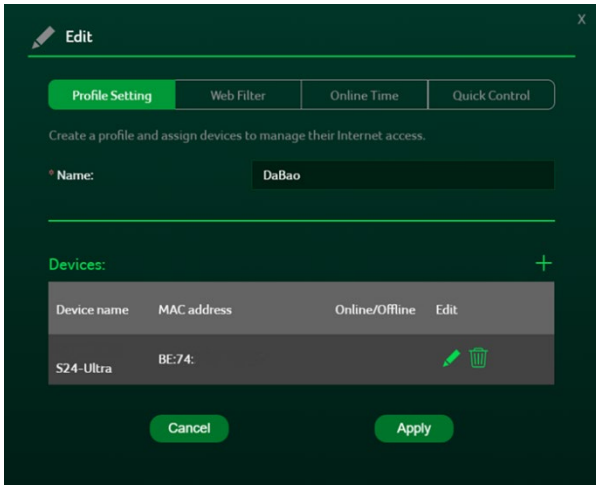
The Parental Control feature allows users to manage Internet access for selected devices. Users can create profiles to apply access rules, such as setting time limits, applying filters, or temporarily pausing Internet access for specific devices.



6.1. Profile Setting

To begin using Parental Control, create a profile to define access rules for specific devices.

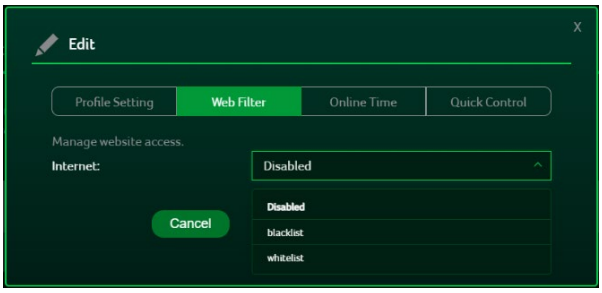
1. Enter a profile name to identify the group of devices you want to manage.
2. Click the “+” icon under Devices to add the devices that will be associated with this profile.
3. Select the desired devices from the list. Each device is identified by its device name and MAC address.
4. Click Apply to save the profile settings.



Once the profile is created, additional settings such as web filtering, online time limits, and quick controls can be configured for the selected devices.

6.2. Web Filter

The Web Filter feature allows users to control website access for devices associated with a profile.



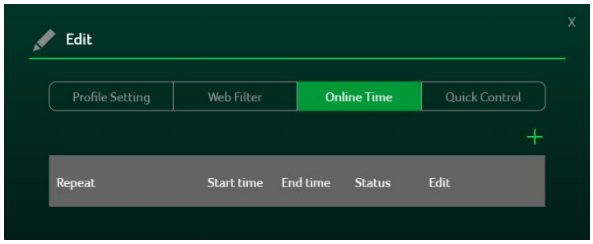
Users can select one of the following Internet access modes:

- Disabled – No web filtering is applied. Devices can access websites without restriction.
- Blacklist – Blocks access to specified websites. All other websites remain accessible.
- Whitelist – Allows access only to specified websites. All other websites are blocked.

Changes made in this section apply only to the devices assigned to the selected profile.

6.3. Online Time

The Online Time feature allows users to define when Internet access is permitted for devices associated with a profile.

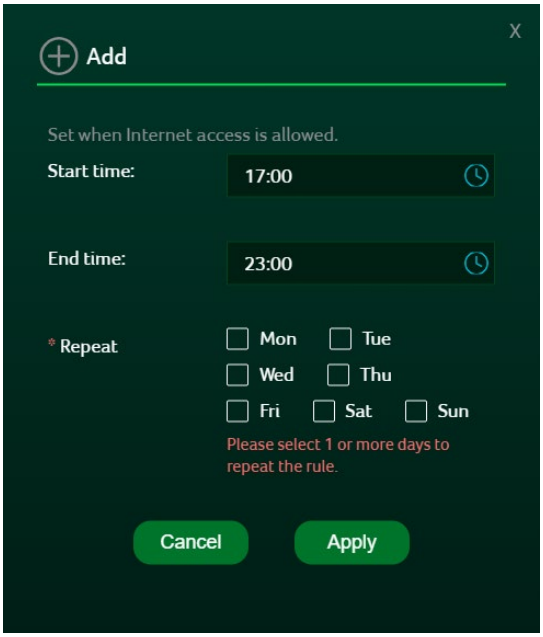


Users can create time rules by specifying the allowed start time and end time, and selecting one or more repeat days for the rule to apply.

To add a time rule:

1. Click the “+” icon to create a new rule.
2. Set the Start time and End time.
3. Select one or more days under Repeat.
4. Click Apply to save the rule.

Multiple time rules can be created and managed for each profile. The status of each rule is displayed in the list and can be edited as needed.

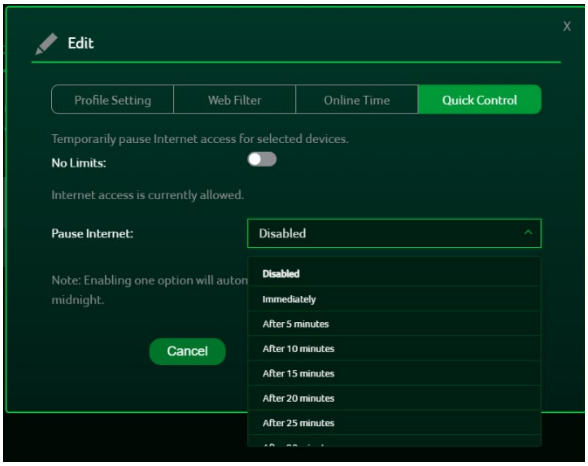


Note

- At least one repeat day must be selected for the rule to take effect.
- Internet access is restricted outside the defined time range.

6.4. Quick Control

The Quick Control feature allows users to temporarily pause Internet access for devices associated with a profile.



Users can enable Pause Internet and select when the pause takes effect, such as immediately or after a specified time interval. This provides a quick way to manage Internet access without changing detailed schedules or filter rules.

When Quick Control is enabled, Internet access for the selected devices will be paused according to the chosen setting.

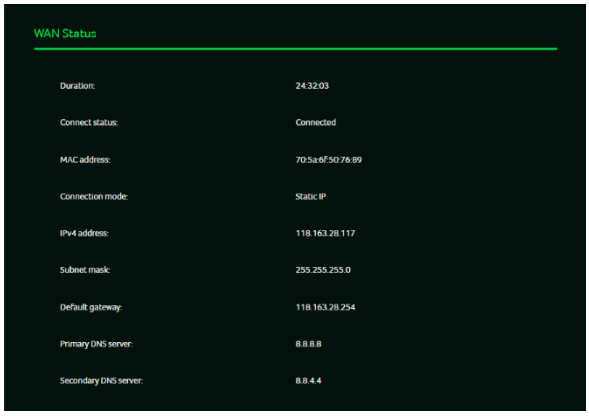
Note

- Quick Control settings apply only to the devices assigned to the selected profile.
- Internet access resumes automatically based on the selected option or after the pause period ends.

7. WAN

7.1. WAN Status

The WAN Status page displays detailed information about the current Internet connection.
It includes connection duration, connection status, MAC address, connection mode, IPv4 address, subnet mask, default gateway, and DNS server information. This page is intended for reference and troubleshooting purposes.



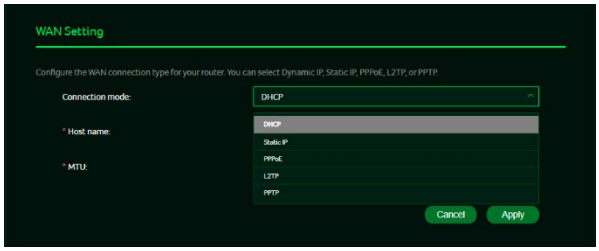
7.2. WAN Setting

The WAN Setting page allows users to configure the Internet connection parameters for the router.

Users can select the appropriate Connection Mode according to the information provided by their Internet Service Provider (ISP). Supported connection modes include DHCP, Static IP, PPPoE, L2TP, and PPTP.

Depending on the selected connection mode, additional settings such as Host Name and MTU may be available for configuration.

After completing the required settings, click Apply to save the configuration.



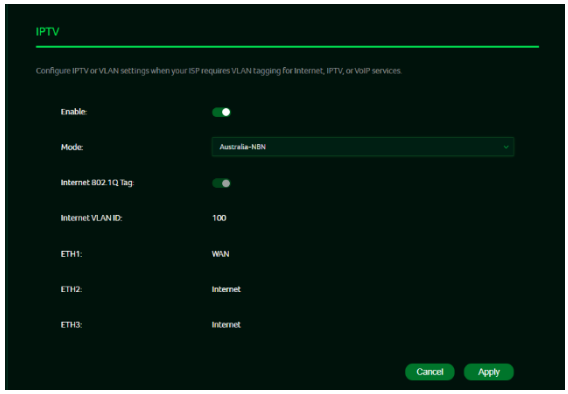
Note

- In most cases, DHCP is selected by default and works for typical home networks.
- If you are unsure which connection mode to use or what values to enter, contact your ISP for assistance.

7.3. IPTV

The IPTV page allows configuration settings related to IPTV services provided by the ISP.

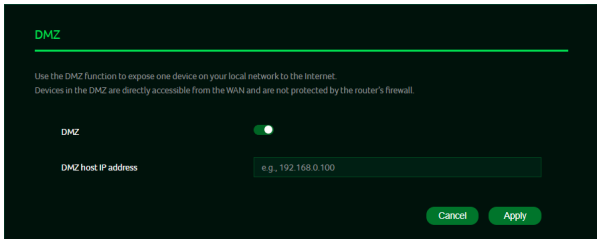
This feature is typically used when specific VLAN or network settings are required for IPTV services.



7.4. DMZ

The DMZ feature allows a specific device on the local network to be made accessible from the Internet.

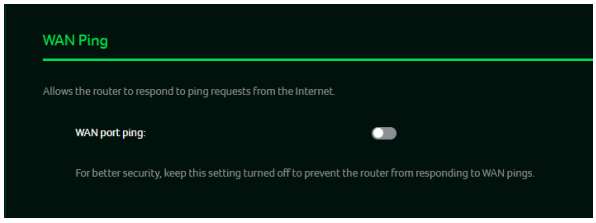
Devices placed in the DMZ are directly reachable from the WAN and are not protected by the router's firewall. This feature is intended for advanced users and should be used with caution.



7.5. WAN Ping

The WAN Ping feature allows the router to respond to ping requests from the Internet.

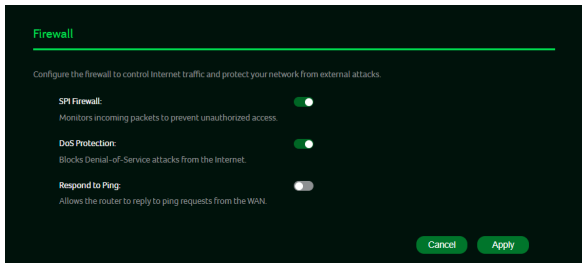
For better security, it is recommended to keep this setting disabled to prevent the router from responding to WAN ping requests.



7.6. Firewall

The Firewall feature allows users to control Internet traffic and protect the local network from external threats.

- SPI Firewall
  Enables stateful packet inspection to monitor incoming traffic and help prevent unauthorized access.
- DoS Protection
  Helps protect the network by blocking Denial-of-Service (DoS) attacks originating from the Internet.
- Respond to Ping
  Allows the router to respond to ping requests from the WAN.



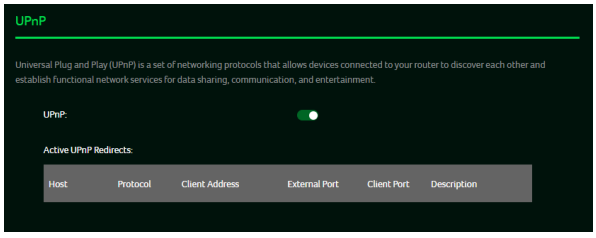
After configuring the firewall settings, click Apply to save the changes.

Note

- Disabling firewall features may reduce network protection.
- For improved security, it is recommended to keep firewall features enabled unless specific configuration is required.

7.7. UPnP

Universal Plug and Play (UPnP) allows compatible devices and applications on the local network to automatically discover the router and request port mappings as needed.



When UPnP is enabled, the router dynamically creates and manages port forwarding rules for supported applications.

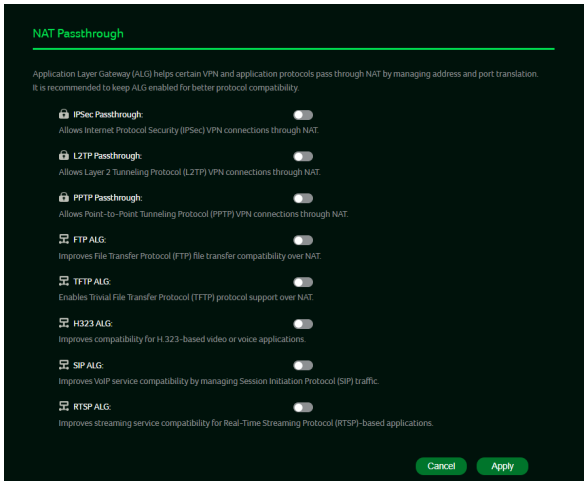
The Active UPnP Redirects list displays currently active UPnP port mappings, including the host, protocol, client address, external port, client port, and description.

Note

- Enabling UPnP may reduce network security, as ports can be opened automatically by applications.
- It is recommended to enable UPnP only when required by supported devices or applications.

7.8. NAT Passthrough

The NAT Passthrough page allows users to enable or disable ALG (Application Layer Gateway) features to improve compatibility for specific VPN and application protocols when operating behind NAT.



These settings are typically used in special network environments where certain protocols require additional handling to function correctly.

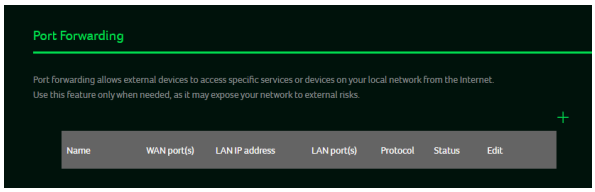
After adjusting the required options, click Apply to save the settings.

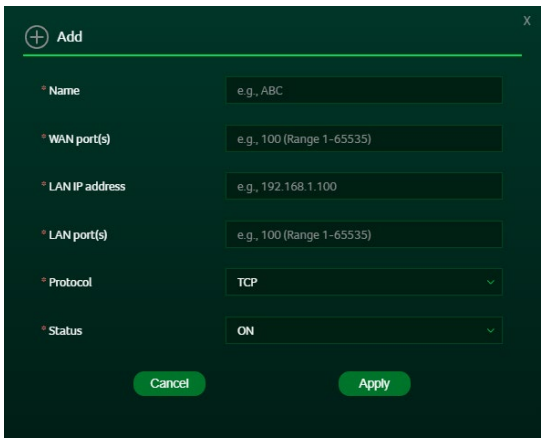
Note

- It is recommended to keep the default settings unless specific compatibility issues are encountered.
- Changing ALG settings may affect the behavior of VPN, voice, or streaming applications.

7.9. Port Forwarding

The Port Forwarding feature allows incoming Internet traffic to be redirected to specific devices or services on the local network.





This feature is typically used to allow external access to services hosted on internal devices, such as servers or network applications.

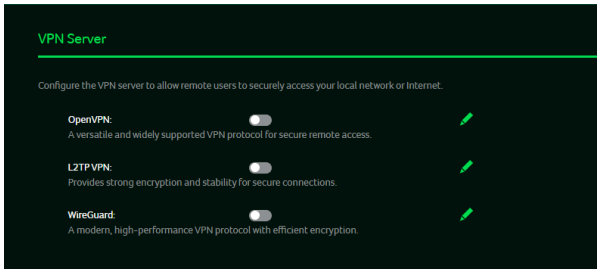
Use this feature only when necessary, as opening ports may increase exposure to external security risks.

Note

- Port forwarding rules apply only to the specified devices on the local network.
- It is recommended to enable port forwarding only for trusted services and disable unused rules.

7.10. VPN Server

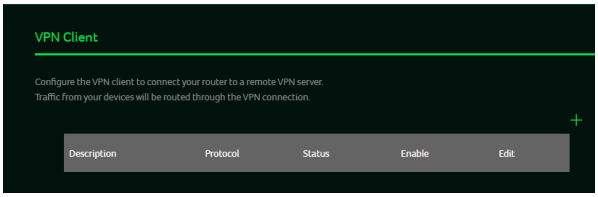
The VPN Server feature allows the router to operate as a VPN server, enabling remote users to securely access the local network or Internet through an encrypted connection.



Users can enable one or more supported VPN server protocols based on their requirements. Authorized remote devices can connect to the router using the selected VPN protocol after configuration.

7.11. VPN Client

The VPN Client feature allows the router to connect to a remote VPN server.

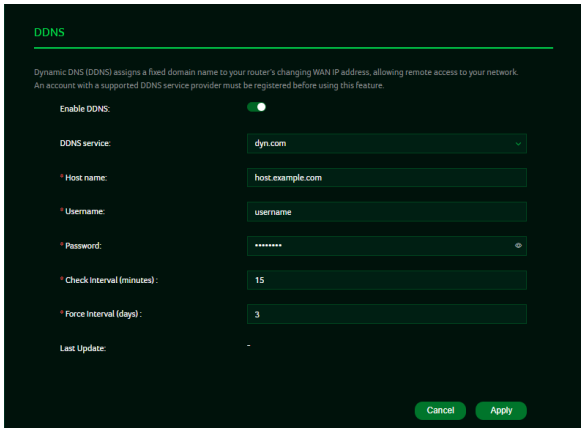


When the VPN Client is enabled, network traffic from devices connected to the router is routed through the VPN connection according to the configured settings. This allows devices on the local network to access the Internet through the remote VPN server.

Users can add, enable, or edit VPN client profiles as needed.

7.12. DDNS

Dynamic DNS (DDNS) allows a fixed domain name to be associated with the router's WAN IP address, even when the public IP address changes.



By using DDNS, users can access the network remotely through a consistent domain name instead of tracking the current IP address.

To use this feature, an account with a supported DDNS service provider is required.

8. Wi-Fi

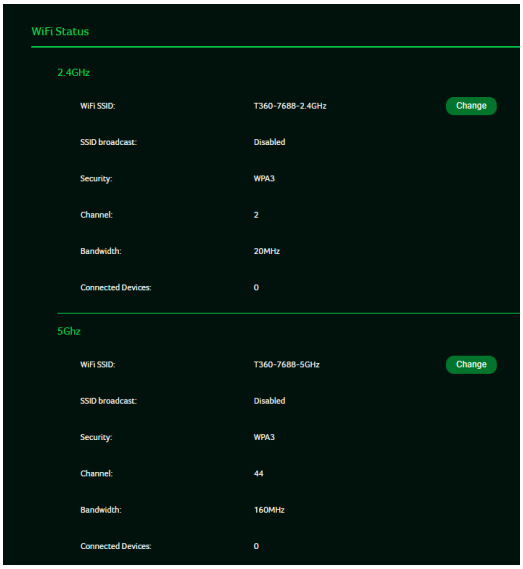
The Wi-Fi section is used to view and manage the router's wireless networking functions. It provides a general overview of the wireless network and allows you to adjust how the router delivers Wi-Fi connectivity to your devices.

Through this section, you can monitor the current wireless operation and manage how the router handles wireless connections, security, and device access. The router supports multiple wireless bands to accommodate different usage scenarios, such as broader coverage or higher wireless performance.

This section also includes options that help improve wireless stability, manage connected devices, and control how different types of devices access the network. By adjusting Wi-Fi-related options, you can tailor the wireless network to suit your environment and usage needs.

8.1. WiFi Status

The Wi-Fi Status page shows the current operating status of the router's wireless networks. It allows you to quickly check whether Wi-Fi is active and how many devices are currently connected.

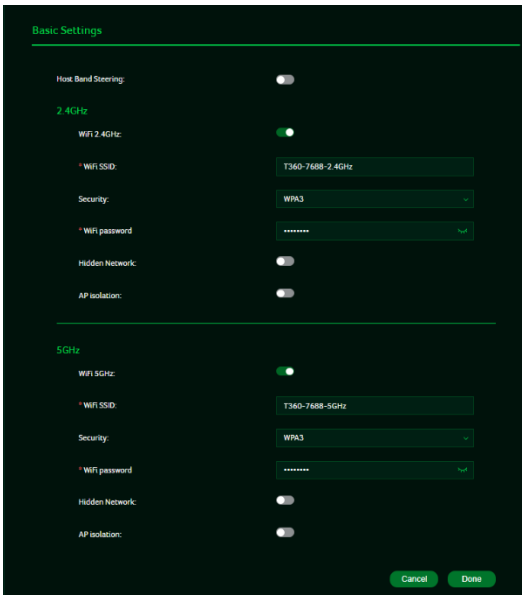


8.2. Basic Setting

The Wi-Fi Basic Settings page is used to control the availability and basic behavior of the router's wireless networks on each frequency band.

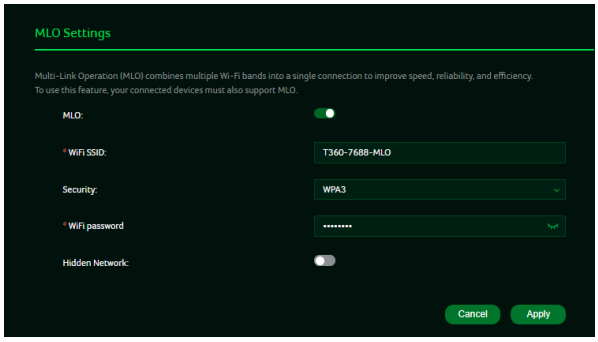
On this page, you can enable or disable Wi-Fi for each band, define the wireless network name and password, and manage basic access-related options. These settings determine how devices discover and connect to the router's Wi-Fi network.

This page is commonly used during initial setup or when making simple changes to wireless access.



8.3. MLO Setting

The MLO Settings page allows you to manage Multi-Link Operation (MLO) for the router's wireless network.

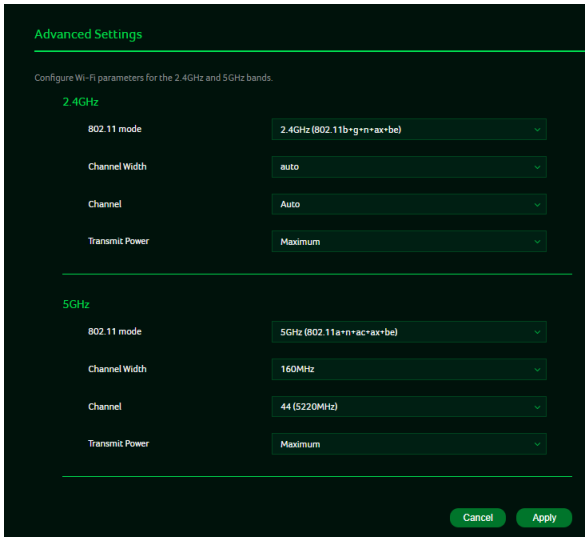


MLO combines multiple Wi-Fi bands into a single wireless connection to improve overall performance, reliability, and efficiency. When this feature is enabled, compatible devices can use multiple links simultaneously for a smoother wireless experience.

This page is intended for users whose devices support MLO. If connected devices do not support this feature, the router will continue to operate using standard Wi-Fi connections.

8.4. Advanced Setting

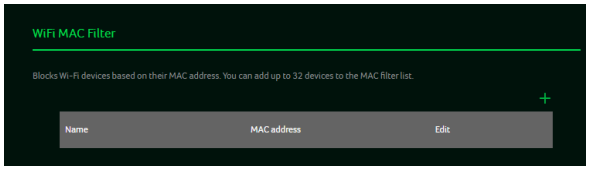
The Wi-Fi Advanced Settings page provides additional wireless configuration options for the router.



These options are designed for optimizing wireless behavior under specific conditions. For normal operation, the default settings are recommended, and no adjustment is required.

8.5. WiFi MAC Filter

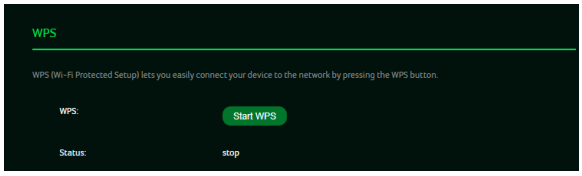
The Wi-Fi MAC Filter feature allows you to control which devices are permitted to connect to the router's Wi-Fi network.



By using this feature, you can restrict wireless access based on individual devices. This provides an additional layer of control for managing device access to the wireless network.

8.6. WPS

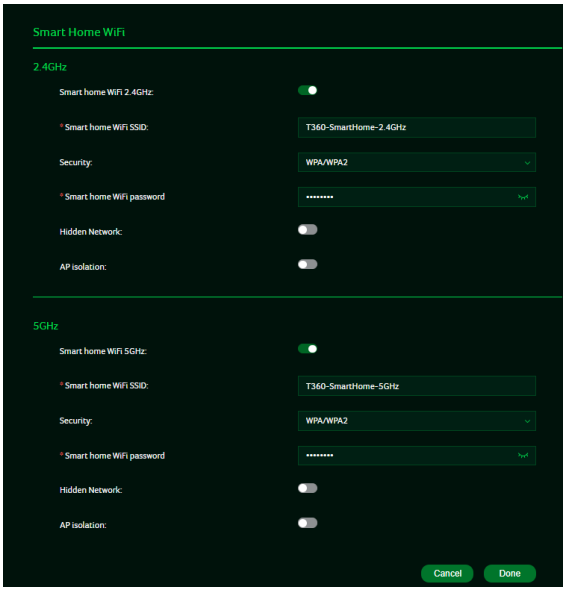
The WPS (Wi-Fi Protected Setup) feature provides a simplified way for compatible devices to connect to the router's Wi-Fi network.



This feature is designed to reduce the steps required when connecting certain devices. It may be useful in situations where entering a Wi-Fi password is inconvenient.

8.7. Smart Home WiFi

Smart Home Wi-Fi provides a separate wireless network designed for smart home and IoT devices.

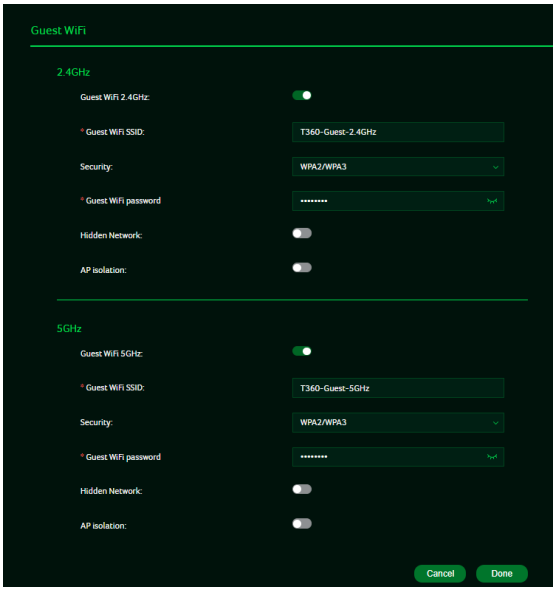


Many IoT devices use simpler or older security methods and may not be compatible with the main Wi-Fi network. Smart Home Wi-Fi helps improve connection compatibility for these devices while keeping them separated from your primary wireless network.

This feature is optional and only needs to be enabled when connecting smart home or IoT devices. It is not required for normal Internet usage.

8.8. Guest WiFi

Guest Wi-Fi allows you to create a separate wireless network for visitors or temporary users.



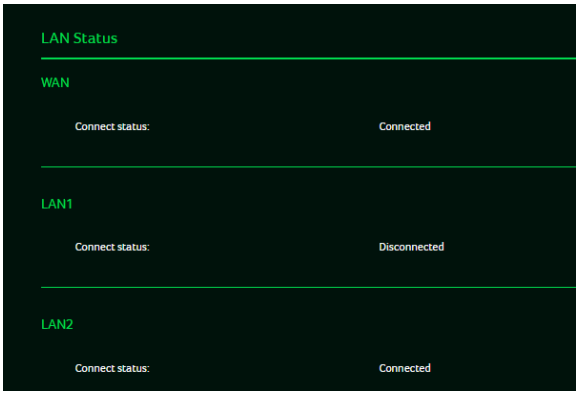
This network lets guests access the Internet without connecting to your main Wi-Fi network, helping protect your primary devices and personal data. Guest Wi-Fi is useful when sharing Internet access with friends, family, or visitors.

Guest Wi-Fi is optional and can be enabled when needed. It is not required for normal daily use of the router.

9. LAN

9.1. LAN Status

The LAN Status page shows the connection status of the router's WAN and LAN ports.

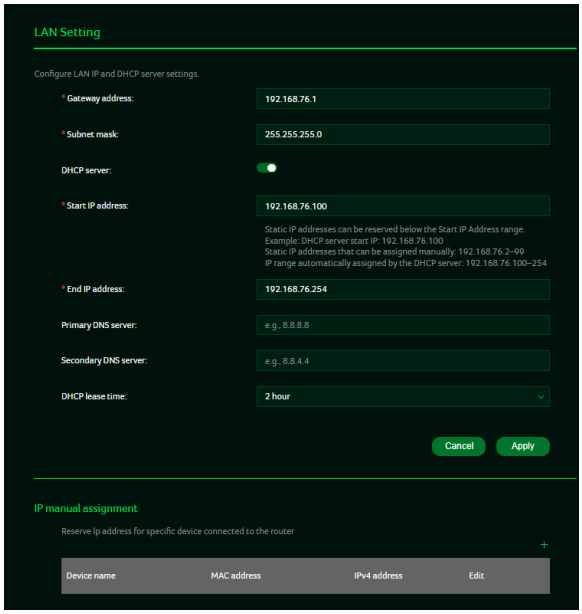


9.2. LAN Setting

The LAN Setting page is used to configure the router's local network settings, including how IP addresses are assigned to devices connected to the router.

In addition to automatic IP assignment, this page also provides an IP manual assignment function. It allows you to reserve a fixed IP address for a specific device so that the device can consistently use the same local IP address.

For most users, the default LAN settings are sufficient. IP manual assignment is typically used only when a device requires a consistent IP address for advanced features or network management.

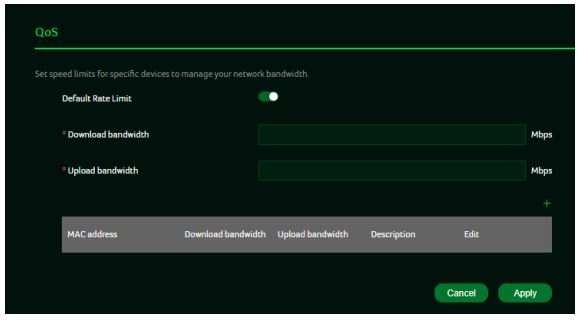


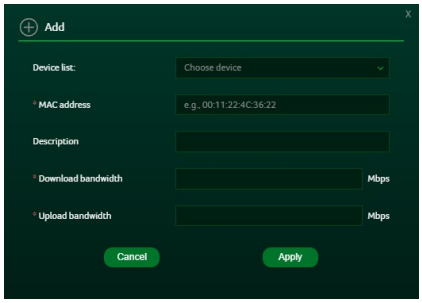
9.3. QoS

The QoS (Quality of Service) feature allows you to control how network bandwidth is shared among connected devices.

By setting upload and download speed limits for specific devices, you can prevent a single device from using too much bandwidth and affecting the performance of others. This is useful when activities such as video streaming, online gaming, or large file downloads are taking place at the same time.

QoS can be applied to individual devices when needed. For normal Internet usage, this feature does not need to be enabled.



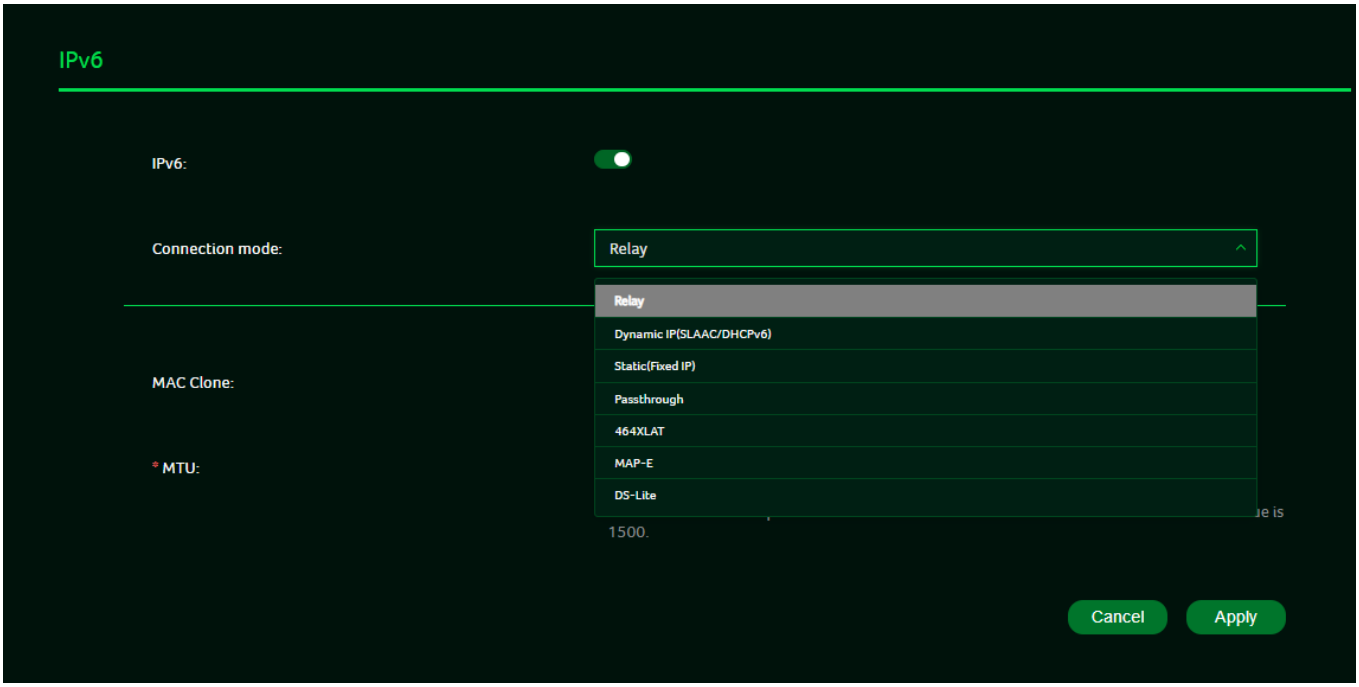


10. IPv6

The IPv6 section allows you to enable and configure IPv6 connectivity on the router.

The router supports multiple IPv6 connection modes to accommodate different Internet service provider (ISP) network environments. Available modes include Relay, Dynamic IP (SLAAC/DHCPv6), Static (Fixed IP), Passthrough, 464XLAT, MAP-E, and DS-Lite.

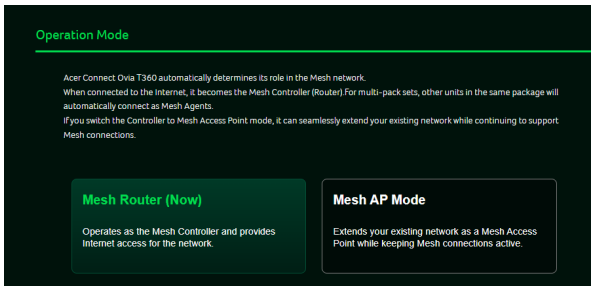
These IPv6 options are intended for use only when required by your ISP. By default, IPv6 settings do not need to be modified. Before enabling or changing IPv6 connection modes, please consult your Internet service provider for the correct configuration.



11. System

11.1. Operation Mode

The Operation Mode page displays the current operating role of the router within the Mesh network.

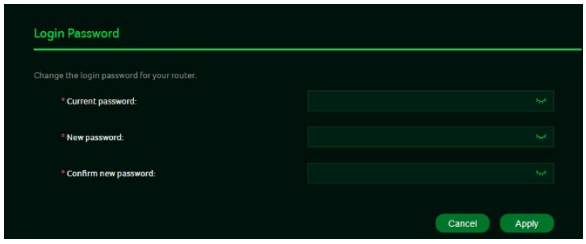


The router automatically determines its role based on the network environment. When connected to the Internet, it operates as a Mesh Router (Controller). In multi-pack setups, additional units automatically join the network as Mesh Agents.

This page is intended to provide an overview of the current Mesh operation mode. To change the operating mode or reconfigure the Mesh network, please use the Quick Setup process.

11.2. Login Password

The Login Password page allows you to change the administrator password used to access the router's management interface.

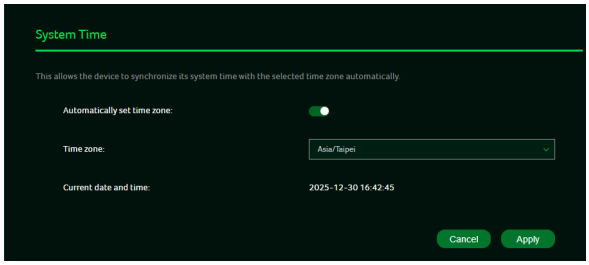


This password helps protect the router from unauthorized access and prevents others from modifying network settings. It is recommended to change the login password periodically or whenever you believe it may have been exposed.

For security reasons, always choose a strong password and keep it confidential. If the login password is forgotten, the router must be reset to factory settings before a new password can be set.

11.3. System Time

The System Time page allows the router to synchronize its internal clock based on the selected time zone.

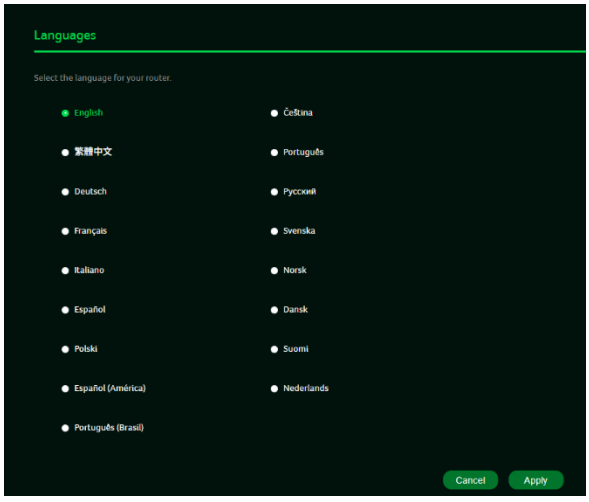


Accurate system time is important for functions such as system logs, scheduled features, and security-related operations. When automatic time synchronization is enabled, the router updates its time automatically according to the selected time zone.

For most users, the default time settings are sufficient and do not require modification.

11.4. Languages

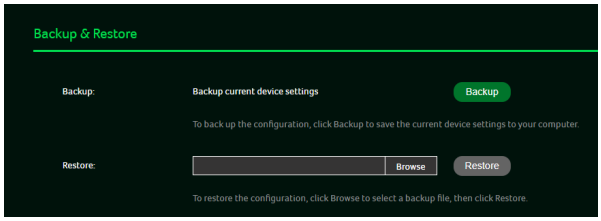
The router automatically selects the display language based on your browser's language settings.



If a different language is preferred, you can manually change the language from this page.

11.5. Backup & Restore

The Backup & Restore page allows you to save and restore the router's configuration settings.

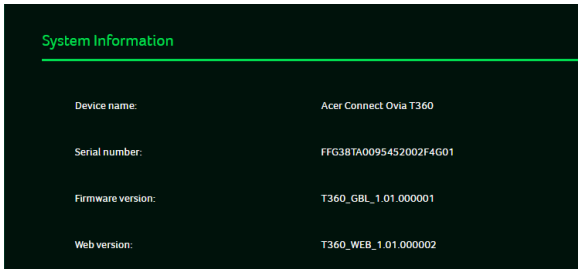


You can create a backup file of the current device settings for future use. This is useful before making major configuration changes or when preparing to reset the router. The saved backup file can later be used to restore the same settings on the router.

Restoring a configuration will replace the current settings with those from the selected backup file. It is recommended to restore settings only from a backup created on the same device.

11.6. System Information

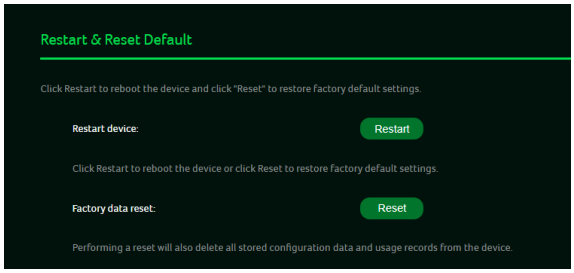
The System Information page displays key information about the router, including the device name, serial number, and software version details.



This information is useful when checking the current firmware version or when contacting technical support for assistance. All information on this page is for reference only and cannot be modified.

11.7. Restart & Reset Default

The Restart & Reset Default page allows you to restart the router or restore it to factory default settings.

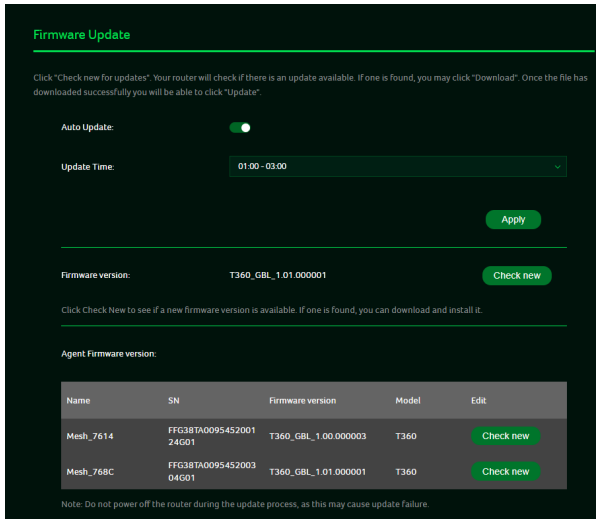


Restarting the device reboots the router without changing any existing settings. This option is typically used to refresh the system or apply certain configuration changes.

Resetting the router to factory default settings will erase all current configuration data and restore the device to its original state. After a factory reset, the router must be set up again before use.

11.8. Firmware Update

The Firmware Update page allows you to check for and install software updates for the router.



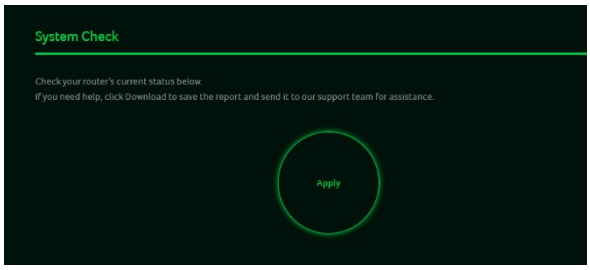
Firmware updates may include security enhancements, performance improvements, and stability fixes. To help ensure the router remains up to date, it is recommended to keep automatic updates enabled. Automatic updates are typically performed during the specified update time to minimize impact on normal usage.

You may also manually check for available updates when needed. For Mesh systems, firmware information for connected Mesh agents is displayed to help ensure version compatibility across all units.

During the firmware update process, do not power off the router or connected Mesh devices, as this may cause the update to fail.

11.9. System Check

The System Check feature allows you to quickly review the current operating status of the router.



By running a system check, the router evaluates key areas such as Internet connectivity, Mesh status, wireless services, connected devices, and system operation. The results help identify whether each function is operating normally.

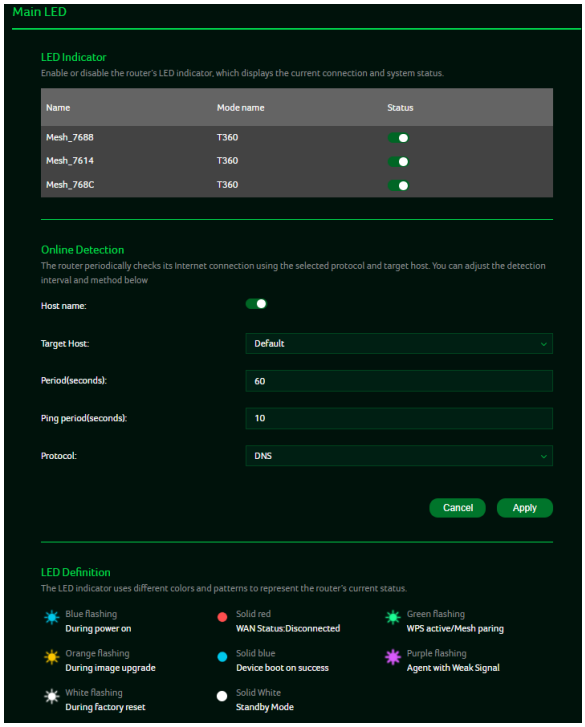
If an issue is detected, related services may be shown as unavailable or disabled. This information is provided for reference and basic troubleshooting.

You can download a system report and share it with acer Connect support team if further assistance is required.

11.10. Main LED

LED Indicator

The LED Indicator section allows you to enable or disable the LED indicators on the router.



When Mesh agents are connected, their LED indicators are also displayed on this page and can be controlled together. This allows you to manage the LED status of both the main router and connected Mesh units from a single location.

The LED indicators display the current system and connection status of each device. This option is typically used to reduce light output when LED visibility is not desired.

Online Detection

The Online Detection section monitors the router’s Internet connectivity by periodically checking network availability.

The router uses the selected detection method to determine whether the Internet connection is active. For most users, the default detection settings provide reliable results and do not require modification.

LED Definition

The LED Definition section explains the different LED colors and flashing patterns used by the router.

Each LED color or pattern represents a specific system or network condition, allowing you to quickly identify the router's operating status without accessing the management interface.

12. Troubleshooting

Frequently Asked Questions (FAQs)

12.1 What should I do if I forget my Wi-Fi password?

1. Connect a device to the T360 router using an Ethernet cable.
2. Open a web browser and visit http://acer-connect.com or http://192.168.76.1.
3. Log in to the Web UI using the admin password.
4. Go to Wi-Fi Settings to view or change the wireless network password.

12.2 I cannot access the router's Web UI. What should I check?

- Ensure your device is connected to the T360 router (wired or wireless).
- Verify that the device's IP address and DNS server are obtained automatically and are in the same subnet as the router.
- Try accessing the Web UI using a private/incognito browser window.
- Clear the browser cache or try a different web browser.

12.3 Internet connection issues with specific ISPs

In some regions, Internet access may require additional configuration depending on the Internet Service Provider (ISP).

If you are unable to access the Internet after completing the setup, please check with your ISP whether any of the following settings are required:

- PPPoE username and password
- VLAN ID configuration
- IPv6 connection settings

In some regions, certain ISPs may require additional WAN configuration before Internet access is available.

To verify or modify these settings:

1. Log in to the router's Web UI.
2. Go to **WAN Settings**.
3. Enter the information provided by your ISP and save the changes.
4. Reboot the router after applying the settings.

If you are unsure about the required parameters, please contact your ISP for assistance.

13. Router basic Specification

Processor	2.0 GHz Quad-Core ARM-Based Processor	
Memory	RAM	512MB
	Storage	128MB
Wireless LAN	IEEE standard	802.11 a/b/g/n/ac/ax/be
	MU-MIMO	2x2 MIMO
	Band	Dual band, 2.4+ 5GHz
	Throughput	BE3600
Ethernet	WAN	1 x1Gbps
	LAN	2 x 1Gbps
Button Key	WPS	Yes, WPS
	Reset	Yes, Factory reset
LED	LED	LED *1
Form factor	Dimension	Φ110×154.5 mm
	Weight	360g
DC Power Jack	Input Voltage	AC 100-240V, 50-60Hz,
	Power Adapter	12V/1A

14. Regulatory Information

14.1 Important Safety Precaution

Acer Connect Ovia T360 is manufactured to comply with European safety standards. This section outlines the safety precautions for using the device. Please read the safety and operation instructions before using your device and accessories and keep these instructions for future reference.

14.2 Condition of Use

- The device is not water-resistant. Please protect the device from water or moisture and do not touch the device with wet hands. Otherwise short-circuit and malfunction of the product or electric shock may occur.
- Keep the device and accessories in a cool, well- ventilated area and away from direct sunlight. Do not place the device in a container with poor heat dissipation. Do not enclose or cover your device with clothes, towels, or other objects.
- Put your device in places beyond the reach of children. Do not allow children to use the wireless device without guidance.
- Do not use your device at places for medical treatment (in an operating room, intensive care unit, or coronary care unit, etc.) where wireless device use is prohibited.
- To reduce the risk of accidents, do not use your device while driving.
- RF signals may affect the electronic systems of motor vehicles. For more information, consult the vehicle manufacturer.
- EE recommends using the charger supplied with your device. Use of another type of charger may result in malfunction and/or danger.

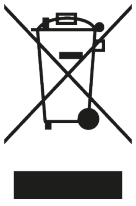
14.3 Cleaning and Maintenance

- Do not attempt to dry your device with an external heat source, such as a microwave oven or hair dryer.
- Use a clean, soft, and dry cloth to clean the device and accessories.

14.4 Disposal Instructions

Do not throw this electronic device into the trash when discarding. To minimize pollution and ensure utmost protection of the global environment, please recycle. For more information on the Waste from Electrical and

Electronics Equipment (WEEE) regulations, visit www.acer-group.com/public/Sustainability



14.5 Ethernet Cable Line Safety

- Disconnect all Ethernet cable lines from the equipment when not in use and/or before servicing.
- To avoid the remote risk of electric shock from lightning, do not connect the Ethernet cable line to this equipment during lightning or thunderstorms.

14.6 Medical Devices

The operation of radio transmitting equipment, including wireless phones, may interfere with inadequately protected medical devices. Consult a physician or the manufacturer of the medical device to determine if it is adequately shielded from external RF energy or if you have any questions. Turn off your device in health care facilities when regulations instruct you to do so, as hospitals or health care facilities may have equipment sensitive to external RF transmissions.

Pacemakers. Pacemaker manufacturers recommend that a minimum separation of 15.3 centimeters (6 inches) be maintained between wireless devices and a pacemaker to avoid potential interference with the pacemaker. These recommendations are consistent with the independent research by and recommendations of Wireless Technology Research. Persons with pacemakers should do the following:

- Always keep the device more than 15.3 centimeters (6 inches) from the pacemaker
- Not carry the device near you pacemaker when the device is switched on. If you suspect interference, switch off your device, and move it.

Hearing aids. Some digital wireless devices may interfere with some hearing aids. If interference occurs, consult your service provider.

14.7 Vehicles

RF signals can affect improperly installed or inadequately shielded electronic systems in motor vehicles, such as electronic fuel injection, anti-lock braking, electronic speed control, and airbag systems. For more information, consult the manufacturer or representative of your vehicle or any added equipment. Only qualified personnel should service or install the device in a vehicle. Faulty installation or service can be dangerous and may invalidate the device's warranty. Regularly check that all wireless equipment in your vehicle is properly mounted and functioning. Do not store or carry flammable liquids, gases, or explosive materials in the same compartment as the device, its parts, or accessories. For vehicles equipped with airbags, remember that airbags inflate with great force. Do not place objects, including installed or portable wireless equipment, over the airbag or in the airbag deployment area. Improper installation of in-vehicle wireless equipment can cause serious injury if the airbag inflates. Using your device while flying in an aircraft is prohibited. Turn off your device before boarding, as the use of wireless devices in an aircraft may be dangerous to its operation, disrupt the wireless network, and may be illegal.

14.8 Warning

- Do not attempt to open the device by yourself. Disassembling may result in damage to the device. Small parts may also present a choking hazard.
- When this device is switched on, it should be kept at least 15 cm from any medical device such as a pacemaker, a hearing aid or insulin pump, etc.
    - Switch this device off when you are near gas or flammable liquids. Strictly obey all signs and instructions posted in any potentially explosive atmosphere.

14.9 Explosive Device Proximity Warning

Turn off your device in any area with a potentially explosive atmosphere and follow all posted signs and instructions. These areas include places where you would normally be advised to turn off your vehicle engine, as sparks could cause an explosion or fire, leading to injury or death. Turn off the device at refueling points, such as near gas pumps at service stations, and adhere to restrictions on the use of radio equipment in fuel depots, storage and distribution areas, chemical plants, or areas with blasting operations. Potentially explosive atmospheres are often, but not always, clearly marked. They include locations such as below deck on boats, chemical transfer or storage facilities, vehicles using liquefied petroleum gas (e.g., propane or butane), and areas where the air contains chemicals or particles such as grain, dust, or metal powders. Do not use your device when wireless phone use is prohibited or when it may cause interference or danger.

- Warning: Do not operate a portable transmitter (including this wireless adapter device) near unshielded blasting caps or in an explosive environment unless the transmitter has been modified to be qualifies for such use.
- Warning: The wireless adapter is not designed for use with high-gain directional antennas

14.10 Wireless adapter regulatory information

- Warning: For safety reasons, turn off all wireless or radio transmitting devices when using your device under the following conditions.

Always follow any special regulations in force in any area, and switch off your device when its use is prohibited or when it may cause interference or danger. Use the device only in its normal operating positions. This device meets RF exposure guidelines when used as intended. To successfully transmit data files or messages, a good quality connection to the network is required. Sometimes, data transmission may be delayed until such a connection is available. Note that parts of the device are magnetic. Metallic materials may be attracted to it, and individuals with hearing aids should avoid holding the device close to their ear with the hearing aid. Keep credit cards or other magnetic storage media away from the device, as the information stored on them may be erased.

Aircraft

Warning: FCC and FAA regulations may prohibit the use of radio-frequency wireless devices (wireless adapters) during flight, as their signals could interfere with critical aircraft instruments. Always consult airport staff and cabin crew before activating your device's wireless adapter while on board.

The wireless adapter and your health

The wireless adapter, like other radio devices, emits radio frequency electromagnetic energy. However, the energy emitted by the wireless adapter is less than that emitted by other wireless devices, such as mobile phones. The wireless adapter operates within the guidelines established by radio frequency safety standards and recommendations. These standards are based on the consensus of the scientific community, formed through deliberations of panels and committees of scientists who continuously review and interpret extensive research literature. In certain situations or environments, the use of the wireless adapter may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:

- Using the wireless adapter on board airplanes, or
- Using the wireless adapter in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are unsure about the policy regarding the use of wireless adapters in a specific location or organization (such as an airport), it is recommended to seek authorization before activating the adapter.

14.11 Statement

[USA]

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

[Canada — Industry Canada (IC)]
This device complies with RSS247 of Industry Canada.

- This device contains licence-exempt transmitter(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 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.

- This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

- Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et un corps humain.

[NCC]

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。

高增益指向性天線只得應用於固定式點對點系統。

14.12 EU Regulatory Conformance

List of applicable countries

This product must be used in strict accordance with the regulations and constraints in the country of use. For further information, contact the local office in the country of use. Please see https://europa.eu/ european- union/about-eu/countries_en for the latest country list.

Specific absorption rate information

This device meets the EU requirements on the limitation of exposure of the general public to electromagnetic fields by way of health protection. The limits are part of extensive recommendations for the protection of the general public. These recommendations have been developed and checked by independent scientific organizations through regular and thorough evaluations of scientific studies. The unit of measurement for the European Council's recommended limit for mobile devices is the "Specific Absorption Rate" (SAR), and the SAR limit is 2.0 W/kg averaged over 10 grams of body tissue. It meets the requirements of the International Commission on Non-Ionizing Radiation Protection (ICNIRP).

For body worn operation, this device has been tested and meets the ICNIRP exposure guidelines and the European Standard, for use with dedicated accessories. Use of other accessories which contain metals may not ensure compliance with ICNIRP exposure guidelines.

Hereby, Acer Incorporated declares that the radio equipment T360 is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available: Please search for Acer Connect Ovia T360 at www.acer.com

14.13 Restrictions

Restriction or Requirement in the CE: 5150 to 5350 MHz indoor use only.

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

WLAN 5GHz Band: For indoor use only.

	UK

14.14 EU Regulatory Compliance -- Radio

e.i.r.p power limit											
2.4G		5G(U-NII-1)		5G(U-NII-2a)		5G(U-NII-2b)		5G(U-NII-3)		6E(U-NII-5)	
2400 MHz ~	2483.5 MHz	5150 MHz ~	5250 MHz	5250 MHz ~	5350 MHz	5470 MHz ~	5725 MHz	5725 MHz ~	5850 MHz	5945 MHz ~	6425 MHz
e.i.r.p 20dBm		e.i.r.p 23dBm		e.i.r.p 20dBm		e.i.r.p 27dBm		e.i.r.p 13.98dBm		e.i.r.p 23dBm	