

PW550+ 5G FWA Outdoor CPE User Manual



Table of Contents

1. About this Manual	3
2. Interfaces.....	3
3. Setting up your PW550+	5

1. Login	8
3.2 Dashboard.....	8
3.3 Status	9
3.3.1 WAN Status	9
3.3.2 WiFi LAN Status.....	10
3.3.2 Cellular Status	10
3.3.3 Network Status CA	11
3.3.4 Software.....	11
3.3.5 Statistics	12
3.4 Settings	12
3.4.1 Basic.....	12
3.4.3 VPN	16
3.4.4 Security	17
3.4.5 Advanced	24
3.4.6 Cellular Settings	27
3.5 SMS.....	32
4. ATRACS	33
5. FAQ.....	33
Regulatory Statements	34
Safety Hazards	35
Limited Warranty:	36

1. About this Manual

The contents of this User Manual have been made as accurate as possible. However, due to continual product improvements, specifications and other information are subject to change without notice. Please visit www.ATEL-USA.com or contact ATEL USA for additional information and the latest version of this User Manual.

2. Interfaces

- **LED**

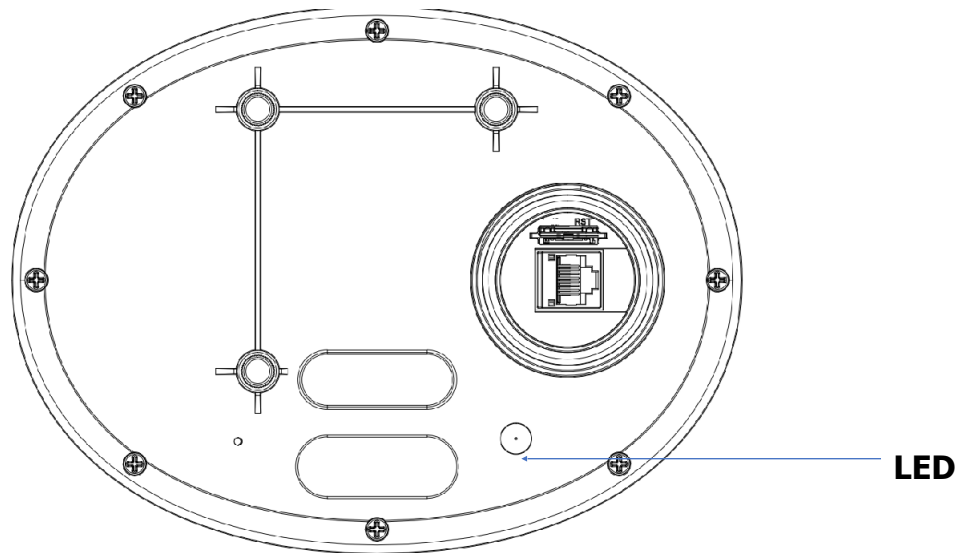


Figure 1 Bottom Panel

LED	Color	Status	Description
-----	-------	--------	-------------

Power/ Signal	Green	On	Good Signal, RSRP \geq -95dBm
	Blue	On	Normal Signal, -95dBm $>$ RSRP \geq -115dBm
	Red	On	Weak Signal, -115dBm $>$ RSRP \geq -125dBm
	Red	Blinking	No SIM or No Signal
	None	Off	No Signal/Power supply is not connected
Notes	<ol style="list-style-type: none"> LED blinks while software is updating. Lit up LED indicates power supply connected 		

Table 1 LED Definition

• Ports

- **RJ45** – This port allows the PW550+ to connect with your computer and provides power supply via PoE Injector.
- **SIM Slot** – Two 4FF SIM cards can be installed via this slot.
- **RST** – Press this keyhole for up to 10 seconds to reset the router to factory defaults.

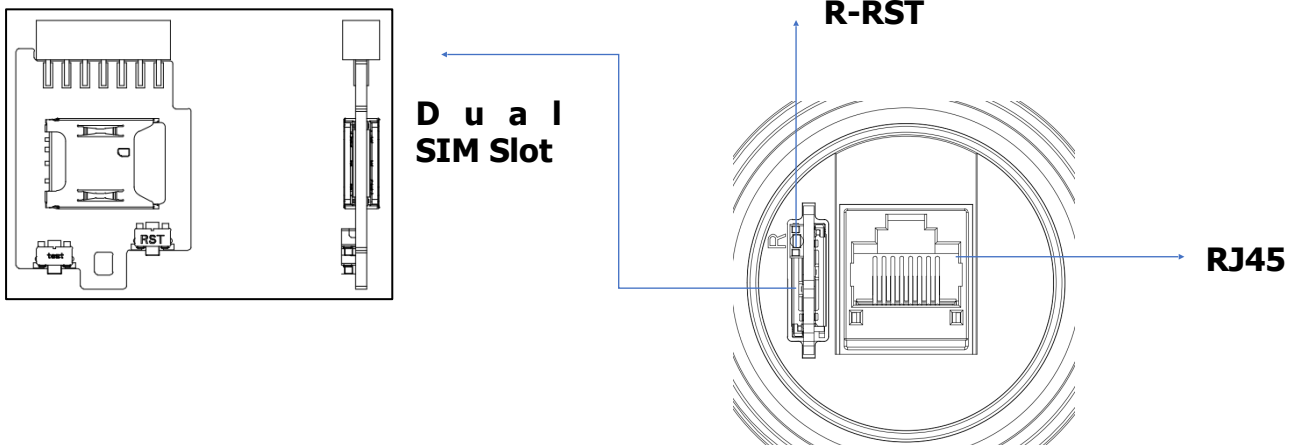


Figure 2 SIM Slot

3. Setting up your PW550+

Install the SIM Cards

1. Unscrew the Cap for Ethernet Port & SIM Slot access on the bottom panel.
2. Pull the strip to take out the SIM Slot.
3. Insert the SIM cards 4FF Size Properly as per the direction with image on the slot for SIM 1 & SIM2, as required.
4. Push back the SIM slot back to its place.

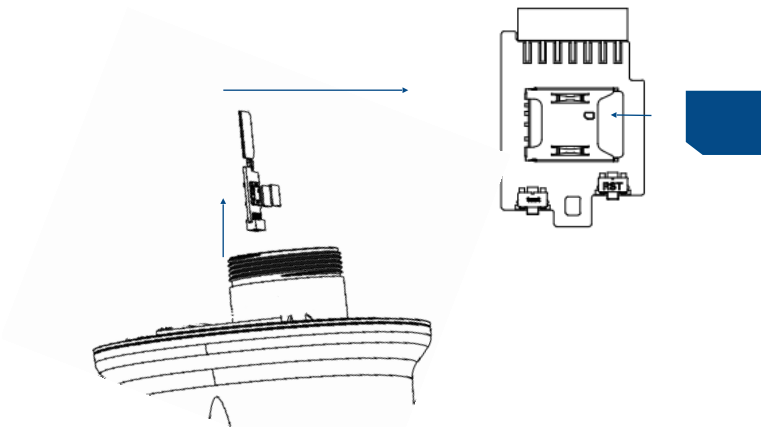


Figure 3 SIM Installation

Connect the Ethernet Cable

5. Connect an Ethernet cable to the LAN port on the bottom panel of your PW550+, threading it through the hole on the Ethernet cover.
6. Connect the other end to the PoE port available on the PoE Injector.
7. Tighten the cap on the bottom panel of your PW550+.

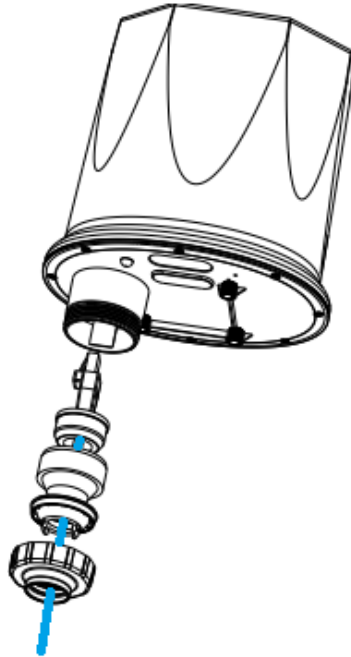


Figure 4 LAN/Power Supply via PoE

Turning ON your PW550+

8. To turn on your PW550+, you need to connect the Ethernet cable coming from the PW550+ to the PoE injector's PoE Port.
9. Now connect power adaptor output to PoE injector's DC Port Jack.
10. The Power LED on the PW550+ should now be on, this indicates that the PW550+ is successfully powered ON.

Note: Must use a 4 pair Ethernet cable between PW550+ & PoE Injector.

Using PoE to Connect PW Series PW550+ with PC

11. To connect your PW550+ to your PC, first turn the PW550+ on using the PoE injector.
12. Connect your computer/PC with the PoE LAN Port using the Ethernet cable.
13. Make sure your computer's Ethernet is configured to obtain an IP address automatically.

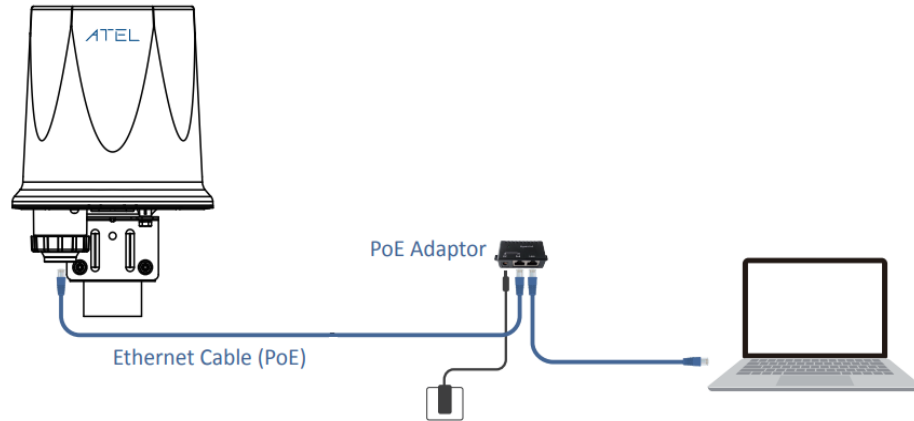


Figure 5 Connection Setup

Use Indoor Wi-Fi Routers with PW550+

Just follow the connection setup and instead of PC, you can connect any Wi-Fi Router available in market. However, make sure Wi-Fi router is designed to support WAN connection over ethernet port.

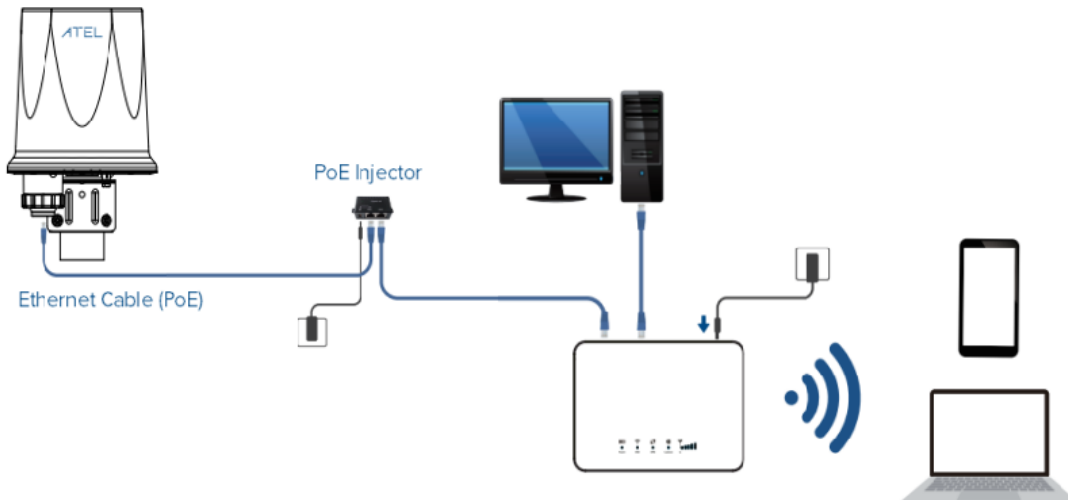


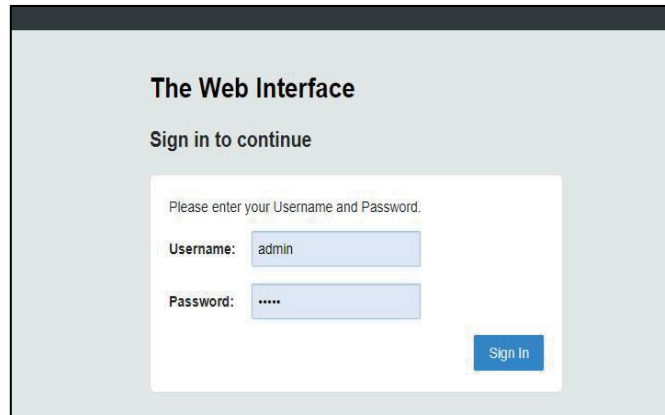
Figure 6 Connection Setup with indoor WiFi AP/Router

1. Login

Once your PC is connected to PW550+. Open your Web browser and enter 192.168.0.1 in the address bar. The login window will popup.

When prompted for the Username and password, enter the following:

- a. Username: admin
- b. Password: Unique to your device, check the device label for your password.



The screenshot shows a web browser window with a light blue background. At the top, it says "The Web Interface". Below that, it says "Sign in to continue". In the center, there is a white box with the text "Please enter your Username and Password." Below this text are two input fields: "Username:" with the value "admin" and "Password:" with masked characters ".....". To the right of the password field is a blue button labeled "Sign In".

Figure 7 Login Window

3.2 Dashboard

After successfully logging in, the screen below will appear and you will see four main menus on the top bar of the WebGUI.

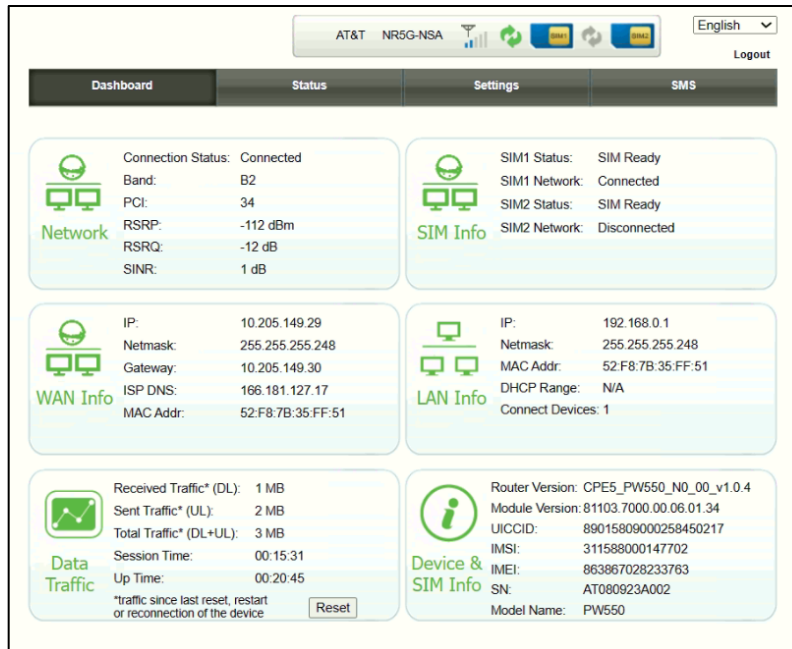


Figure 8 Dashboard

The bars in the middle indicate the signal level received and the USIM icon displays the status of the USIM. Click "Logout" and the WebGUI will log you out and return you to the login window.

From this dashboard page, you can also view Network status, SIM Connection Status, WAN Information, LAN Information, Data Traffic and Device & SIM Information.

3.3 Status

On this page, you can view WAN Status, Cellular Status, Network Status CA, Software and Statistics.

3.3.1 WAN Status

From the WAN Status page, you can view the WAN IP Address, WAN Primary DNS and WAN Secondary DNS information.

Dashboard	Status	Settings	SMS
WAN Status	WAN Status		
Cellular Status	WAN Mode	Cellular WAN	
Network Status CA	Cellular Information		
Software	Cellular IP Address	10.102.183.79	
Statistics	Cellular Primary DNS	112.65.184.255	
	Cellular Secondary DNS	210.22.84.3	
	IPv6 WAN Information		
	IPv6 WAN IP Address	2408:840d:9300:11c7:17b0:8ae0:c6a1:cc36	

Figure 9 WAN Status

3.3.2 WiFi LAN Status

From this page, you can view the WiFi LAN Status and information such as SSID, Channel, Security, Key, LAN IP and DHCP Server.

Dashboard	Status	Settings	SMS
WAN Status	2.4 GHz WiFi LAN Status		
WiFi LAN Status	WiFi Status	Enabled	
Cellular Status	Network Name (SSID)	ATEL 5G #1	
Network Status CA	Frequency (Channel)	Auto (Channel 1)	
Software	Security Mode	WPA2-PSK	
Device List	5 GHz WiFi LAN Status		
WLAN Device List	WiFi Status	Enabled	
Statistics	Network Name (SSID)	ATEL 5G #1	
	Frequency (Channel)	Auto (Channel 153)	
	Security Mode	WPA2-PSK	
	IP Settings		
	LAN IP	192.168.0.1	
	DHCP Server	192.168.0.2-192.168.0.254	

Connection
ell ID and

Dashboard	Status	Settings	SMS
WAN Status Cellular Status Network Status CA Software Statistics	Cellular Status Connection Status USIM Status IMEI IMSI RSRP RSRQ RSSI SINR PCI Band NCI NARFCN gNodeB ID	Connected No SIM Card or invalid SIM Card 862424050246536 460011162618016 -104 dBm -6 dB -73 dBm 3 dB 142 n78 5AE291002 627264 5AE291002	

Figure 10 Cellular Status

3.3.3 Network Status CA

On this page, you can view network status CA information, such as, Index, Band, PCI, EARFCN, Bandwidth, MIMO, Modulation and RSRP.

Dashboard	Status	Settings	SMS					
WAN Status	Network Status CA							
Cellular Status	Index	Band	PCI	EARFCN	Bandwidth	MIMO	Modulation	RSRP
Network Status CA	PCC	n78	226	633984	100MHz	1/1	16QAM	-112
Software								
Statistics								

Figure 11 Cellular Network Status CA

3.3.4 Software

From this page, you can view the software version and the Module software version for your PW550+.

Dashboard	Status	Settings	SMS
WAN Status	Software		
Cellular Status	Software Version	CPE5_PW550_N0_00_v1.0.6	
Network Status CA	Module Version	81103.7000.00.06.01.T16	
Software			
Statistics			

Figure 12 Software

3.3.5 Statistics

From the Statistics page, you can view the speed and data used traffic statistics. Click on “Clear” button to reset available traffic statistics.

Dashboard

Status

Settings

SMS

WAN Status

Cellular Status

Network Status CA

Software

Statistics

Statistics

	Download	Upload
Cellular Speed	29 Kb/s	16 Kb/s

Cellular	Duration	Downloaded	Uploaded	Total Used Data
Current Session	02:13:38	35 MB	6 MB	41 MB
Total	43:03:24	517 MB	105 MB	622 MB

The amounts of data is approximate. For more information please contact your network operator.

Clear

Figure 13 Statistics

Note: Statistics data might differ from the data consumed on the ISP side.

3.4 Settings

On this page, you will find some Basic & Advanced configuration useful options.

3.4.1 Basic

3.4.1.1 Management

On this page, you can modify the default password for the WebGUI login. You need to input the new password 2 times and click the “Apply” button for changes

to take effect. Next you would logout automatically and you should login to the system with the new password.

Dashboard	Status	Settings	SMS
Basic	Device Settings		
Management	Username admin		
LAN Settings	Current Password	<input type="password"/>	(32 characters max.)
Software Upgrade	New Password:	<input type="password"/>	(32 characters max.)
Automatic Reboot	Repeat Password	<input type="password"/>	(32 characters max.)
VPN	<input type="button" value="Apply"/> <input type="button" value="Clear"/>		
Security	Factory Reset		
Advanced	Click button to restore default settings <input type="button" value="Restore"/>		
Cellular Settings	Device Reboot		
	Click button to reboot the device <input type="button" value="Reboot"/>		

Figure 14 Basic > Management

On the same page, you can click the "Restore" button to load to the default factory settings and click the "Reboot" button to reboot the router.

Note: After factory reset, all the configuration or data on the router will be replaced with factory default settings.

3.4.1.2 LAN Settings

you can view the existing settings for the LAN (Local Area Network) and modify them as per your requirements.

This menu is visible when IP Passthrough feature is disabled.

Dashboard	Status	Settings	SMS
Basic	LAN Settings		
Management			
LAN Settings			
Software Upgrade			
Automatic Reboot			
VPN			
Security			
Advanced			
Cellular Settings			
	IP Address	<input type="text" value="192.168.0.1"/>	
	Subnet Mask	<input type="text" value="255.255.255.0"/>	
	DHCP	<input type="text" value="Enabled"/>	
	Start IP Address	<input type="text" value="192.168.0.2"/>	
	End IP Address	<input type="text" value="192.168.0.254"/>	
	Lease Time	<input type="text" value="86400"/>	
	Static IP 1	MAC: <input type="text"/>	IP: <input type="text"/>
	Static IP 2	MAC: <input type="text"/>	IP: <input type="text"/>
	Static IP 3	MAC: <input type="text"/>	IP: <input type="text"/>
	Static IP 4	MAC: <input type="text"/>	IP: <input type="text"/>
	Static IP 5	MAC: <input type="text"/>	IP: <input type="text"/>
	Static IP 6	MAC: <input type="text"/>	IP: <input type="text"/>
	<input type="button" value="Apply"/> <input type="button" value="Clear"/>		

Figure 15 Basic > LAN Settings

- **IP Address** - Displays the IP address of your router (default: 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Generally, use 255.255.255.0 as the subnet mask.
- **DHCP** - Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network, otherwise, you must configure the address of your PC manually.
- **Start IP Address** - Specify an IP address for the DHCP server to start with when assigning IP addresses. The default start address is 192.168.0.2.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. The default end address is 192.168.0.254.
- **Lease Time** - The Lease Time is the amount of time a user will be allowed connection to the router with their current assigned IP address. Enter the amount of time in minutes and the user will be "leased" the IP address for that time. After the time is up, the user will be assigned a new IP address automatically.
- **Static IP** - IP/MAC binding function, the router will assign a fixed IP address to a specific user using its MAC address according to the rules.

Note:

1. If you change the IP Address of LAN, you must use the new IP address to login to the router.
2. If the new LAN IP address you set is not in the same subnet, the IP address pool of the DHCP server will change at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

3.4.1.3 Software Upgrade

On this page, you can upgrade the SW version of the router manually from the connected PC. It will take several seconds (~120) to complete the whole upgrade process, and then the router will reboot automatically.

Dashboard	Status	Settings	SMS
Basic	Software Upgrade		
Management	Router Upgrade: <input type="button" value="Choose File"/> No file chosen		
LAN Settings	<input type="button" value="Apply"/>		
Software Upgrade			
Automatic Reboot			
VPN			
Security			
Advanced			
Cellular Settings			

Figure 16 Basic > Software Upgrade

3.4.1.5 Automatic Reboot

On this page, you can set up the Automatic Reboot feature. By default, it is Disabled.

Dashboard	Status	Settings	SMS
Basic	Automatic Reboot Settings		
Management	Automatic Reboot Enabled ▾		
LAN Settings	Date <input checked="" type="radio"/> every day <input type="radio"/> every week <input type="radio"/> every month		
Software Upgrade	Time At a defined time 00 ▾ h 00 ▾ min.		
Remote Upgrade	Apply		
Automatic Reboot			
WiFi			
VPN			
Security			
Advanced			
Cellular Settings			

Figure 17 Basic > Automatic Reboot

You can define the rule for this router to reboot itself automatically on a defined day and time. For the settings to take effect, make sure to click on the “Apply” button.

3.4.3 VPN

You can use the VPN feature if required. By default, this feature is disabled. You can find different VPN types (i.e., PPTP, IPsec, L2TP and GRE). You must know how to use them, otherwise check with your ISP or VPN provider. This menu is visible when IP Passthrough feature is disabled.

Dashboard	Status	Settings	SMS
Basic	PPTP VPN		
WiFi	Enable Disable ▾		
VPN	Apply		
PPTP VPN			
IPSec VPN			
L2TP VPN			
GRE VPN			
Security			
Advanced			
Cellular Settings			

Figure 18 VPN

3.4.4 Security

On this page, you can find basic security/firewall features supported by this router. You can define them as per your requirements. This menu is visible when IP Passthrough feature is disabled.

Figure 19 Security

3.4.4.1 MAC Filtering

This function is a powerful security feature that allows you to specify which user(s) are not allowed to ~~connect with this router and~~ surf the Internet.

Figure 20 MAC Filtering

The default MAC filtering setting is disabled, so you should enable it before you begin to configure the filter. Then click the "Add New" button and you can configure the rules you like.

Default Policy: The packets that don't match with any rules would be "Allow"

or “Deny”, as selected.

The new rules will be shown on the rule table, here you can delete the rules that you have selected and add new rules sequentially. The maximum rule count is 10.

MAC Address Rule Table			
ID	MAC Address	Action	
1	<input type="checkbox"/> 38:65:B2:43:31:1D	- - - - Drop	-
		Others would be accepted	
		-	
<input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/> (Note: maximum rule count is 10)			

Figure 21 MAC Filtering Rule Table

The MAC Filtering Schedule gives you the option to set up a schedule for the filtering policy.

Mac Filtering Schedule	
Schedule	Enabled <input type="button" value="v"/>
Date	<input checked="" type="checkbox"/> Every day <div> <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu </div> <div> <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun </div>
Time	<input checked="" type="radio"/> Every time <input type="radio"/> At a defined time From <input type="text" value="00"/> h <input type="text" value="00"/> min. To <input type="text" value="00"/> h <input type="text" value="00"/> min.
<input type="button" value="Apply"/>	

Figure 22 MAC Filtering Schedule

3.4.4.2 IP/Port Filtering

From this page, you can configure the IP/Port filter to forbid relevant users from accessing it via the router.

The default IP/Port filter setting is disabled, so you should enable it before you begin to configure the filter. Click the “Add New” button to configure settings, as needed.

Default Policy: The packets that don’t match with any rules would be “Dropped/Accepted”.

IP/Port Filtering Settings

IP/Port Filtering Disabled

Default policy - the IP/port that doesn't match any rule would be: Dropped

Apply

Rule Table

ID	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action
1 <input type="checkbox"/>	8.8.8.8	192.168.0.180	All	-	-	Drop
Others would be accepted						

Apply
Delete
Add New
(Note: maximum rule count is 10)

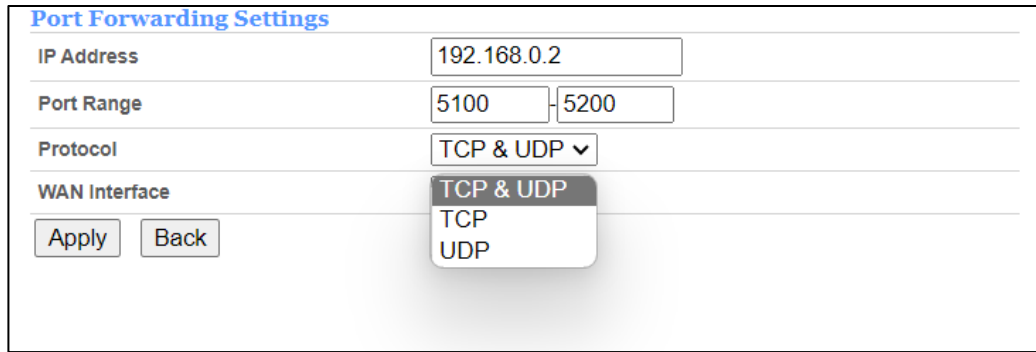
Figure 23 IP/Port Filtering Settings

- **Dest IP Address** – The IP address of a website that you want to filter (such as Google 74.125.128.106).
- **Source IP Address** - The IP address of a PC (such as 192.168.0.2).
- **Protocol** - TCP, UDP, ICMP
- **Dest Port Range** – Set a fixed value (such as 21-21) to restrict Internet access to a single user.
- **Source Port Range** - 1~65535
- **Action** - Accept, Drop

The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules. The maximum rule count is 10.

3.4.4.3 Port Forwarding

Clicking on the header of the “Port Forwarding” button will take you to the “Port Forwarding” page. By clicking on the “Add New” button, you can configure IP addresses and set a port range to achieve the port forwarding purpose.



Port Forwarding Settings

IP Address: 192.168.0.2

Port Range: 5100 - 5200

Protocol: TCP & UDP

WAN Interface: TCP & UDP (dropdown menu open showing TCP and UDP options)

Buttons: Apply, Back

Figure 24 Port Forwarding Settings

- **IP Address** - The IP address of the PC running the service application.
- **Port Range** - You can enter a range of the service port or set a fixed value.
- **Protocol** - UDP, TCP, TCP & UDP.
- **WAN Interface** – BOTH, LTE and ETH WAN. Choose on which interface to do the port forwarding.

The new rules will be shown on the Rule Table. You can delete the items that you have selected or add new rules by clicking the “Add New” button. The maximum rule count is 20.

Rule Table			
ID	IP Address	Port Range	Protocol
1 <input type="checkbox"/>	192.168.0.2	5100 - 5200	TCP + UDP
2 <input type="checkbox"/>	192.168.0.3	7777 - 8888	TCP
3 <input type="checkbox"/>	192.168.0.4	10010 - 10020	UDP
<input type="checkbox"/> Select All <input type="button" value="Delete"/> <input type="button" value="Add New"/>			
(Note: maximum rule count is 20)			

Figure 25 Port Forwarding Rule Table

3.4.4.4 Virtual Server

Clicking on the header of the “Virtual Server” button will take you to the “Virtual Server” page. It is a feature that is similar to port forwarding. Click on the “Add New” button to add a new rule. You can configure the IP Address, Public Port, Private Port and Protocol to achieve the virtual server function.

Rule Table

ID	IP Address	Public Port	Private Port	Protocol
<div> Delete Add New </div> <div>(Note: maximum rule count is 20)</div>				

Virtual Server Settings

IP Address	192.168.0.4
Public Port	5100
Private Port	5200
Protocol	TCP & UDP
WAN Interface	<div> TCP & UDP TCP UDP </div>
<div> Apply Back </div>	

Figure 26 Virtual Server Settings

- **IP Address** - The IP address of the PC running the service application.
- **Public Port** - The server-side port.
- **Private Port** - The client-side port. It can be same as the public port.
- **Protocol** - UDP, TCP, TCP & UDP.
- **WAN Interface** – BOTH LTE and ETH WAN. Choose on which interface to deliver the Virtual Server function.

The new rules will be shown on the Rule Table. You can delete the items that you have selected or add new rules by clicking the “Add New” button. The maximum rule count is 20.

Rule Table

ID	IP Address	Public Port	Private Port	Protocol
1	192.168.0.4	5100	5200	TCP + UDP
2	192.168.0.22	1111	2222	TCP
3	192.168.0.3	1220	1230	UDP

Delete
Add New

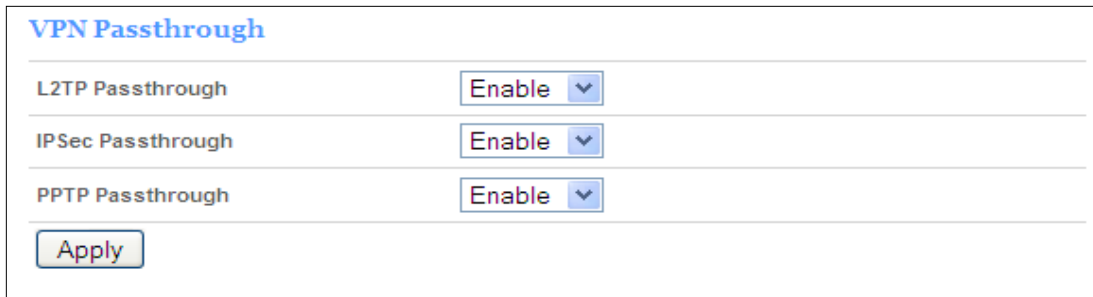
(Note: maximum rule count is 20)

Figure 27 Virtual Server Rule Table

3.4.4.5 VPN Passthrough

A virtual private network (VPN) is a point-to-point connection across a private or public network (Internet).

VPN Passthrough allows the VPN traffic to pass through the router. Thereby we can establish VPN connections to a remote network. For example, VPNs allow you to securely access your company's intranet at home. There are three main kinds of the VPN tunneling protocol: PPTP, L2TP and IPSec.



VPN Passthrough	
L2TP Passthrough	Enable ▼
IPSec Passthrough	Enable ▼
PPTP Passthrough	Enable ▼
<input type="button" value="Apply"/>	

Figure 28 VPN Passthrough

Note: VPN Passthrough does not mean the router can create a VPN endpoint. VPN Passthrough is a feature that allows VPN traffic created by other endpoints to "pass through" the router.

3.4.4.6 Demilitarized Zone(DMZ)

From this page, you can configure a Demilitarized Zone (DMZ) to separate the internal network and the Internet.

- **WAN Interface** - You can select LTE/ETH WAN port.
- **DMZ IP Address** - The IP address of your PC (such as 192.168.0.3).

Figure 29 DMZ Settings

3.4.4.7 Parental Control

By default, it is disabled. If you enable the Parental Control feature, the rules added to the Rule Table will determine when access to the Internet or website will be denied. Internet or website access will be automatically blocked in the defined time.

Figure 30 Parental Control

3.4.5 Advanced

3.4.5.1 Diagnostic

On this page, you will find "Ping" and "Traceroute" features.

Ping: allows you to check the reachability of an IP address/domain name.

Traceroute: allows you to check the host/route for an IP address/domain name.

The screenshot shows the 'Diagnostic Tool' interface. On the left is a sidebar menu with options: Basic, VPN, Security, Advanced, Diagnostic (highlighted), Dynamic DNS, Backup & Restore, Network Management, NTP, and Cellular Settings. The main content area is titled 'Diagnostic Tool' and contains a 'Choose Operation' section with radio buttons for 'Ping' (selected) and 'Traceroute'. Below this is a 'Host' input field and a 'Send' button. A large empty text area is provided for the results of the diagnostic operation.

Figure 31 Advanced > Diagnostic

3.4.5.2 Dynamic DNS

On this page, you can set up the DDNS service.

The screenshot shows the 'DDNS Settings' interface. The sidebar menu is identical to the previous figure, with 'Dynamic DNS' highlighted. The main content area is titled 'DDNS Settings' and contains the following fields: 'DDNS Status' (set to 'Disabled'), 'Dynamic DNS Provider' (a dropdown menu currently showing 'Disabled'), 'User Name' (input field), 'Password' (input field), and 'Domain Name' (input field). An 'Apply' button is located at the bottom of the settings section.

Figure 32 Advanced > Dynamic DNS

Figure 33 Advanced > Dynamic DNS Servers

3.4.5.3 Backup & Restore

On this page, you can back up the existing configuration and restore it (if required). When you click on Backup button, a Configuration file will be saved as a data file to the local PC. You can restore this router configuration from the files that you saved.

Figure 34 Advanced > Backup & Restore

3.4.5.4 Network Management

On this page, you can view and modify features related to the management of this router.

Network Management		
Remote management (http)	Disabled ▾	(e.g. http://ip_address:port)
Remote management (https)	Disabled ▾	(e.g. https://ip_address:port)
HTTP Login(WebUI Management)	Enabled ▾	
HTTPS Login(WebUI Management)	Enabled ▾	
Respond to PING on WAN	Disabled ▾	
Respond to PING on LAN	Enabled ▾	
<input type="button" value="Apply"/>		

Figure 35 Advanced > Network Management

➤ Remote Management (http)

You can access the router's WebGUI remotely using its WAN IP HTTP protocol when the remote management feature is enabled.

➤ Remote Management (https)

You can access the router's WebGUI remotely using its WAN IP HTTPS protocol when the remote management feature is enabled.

➤ Respond to PING on WAN

By default, ping on WAN is not allowed. You can Enable it here.

➤ Respond to PING on LAN

By default, ping on LAN is allowed. You can disable it here.

➤ HTTP Login (WebGUI Management)

This function allows users to login to the WebGUI via the http protocol method.

➤ HTTPS Login (WebGUI Management)

This function allows users to login to the WebGUI via the https protocol method.

3.4.5.5 NTP

From this page, you can set the Current Time, Time Zone, NTP Server and NTP synchronization. When this router obtains the WAN IP, the current time will synchronize with the NTP server automatically.

NTP Settings	
Current Time	<div>Mon, 31 Oct 2022, 23:22:13</div> <div>Sync with host</div>
Time Zone:	(GMT-08:00) Pacific Time ▼
NTP Server	<div>time.nist.gov</div> <div>e.g.:time.stdtime.gov.tw</div> <div>time.nist.gov</div> <div>ntp0.broad.mit.edu</div>
Interval synchronization (hours of range 1 - 300)	24
<div>Apply</div>	

Figure 36 NTP

3.4.6 Cellular Settings

3.4.6.1 Network

On this page, you can check and/or uncheck the network bands for 4G and 5G bands supported.

Auto: The router will automatically connect to the network with the best available signal/band.

4G Only: The router will use only 4G bands to connect with the network.

5G Only: The router will use only 5G bands to connect with the network.

Dashboard	Status	Settings	SMS
Basic	Network		
VPN	Band selection Auto ▼		
Security	4G Band		
Advanced	<input checked="" type="checkbox"/> B2	<input checked="" type="checkbox"/> B4	<input checked="" type="checkbox"/> B5
Cellular Settings	<input checked="" type="checkbox"/> B7	<input checked="" type="checkbox"/> B12	<input checked="" type="checkbox"/> B13
Network	<input checked="" type="checkbox"/> B14	<input checked="" type="checkbox"/> B17	<input checked="" type="checkbox"/> B25
SIM And APN Settings	<input checked="" type="checkbox"/> B26	<input checked="" type="checkbox"/> B29	<input checked="" type="checkbox"/> B30
Network Watchdog	<input checked="" type="checkbox"/> B41	<input checked="" type="checkbox"/> B46	<input checked="" type="checkbox"/> B48
IP Passthrough	<input checked="" type="checkbox"/> B66	<input checked="" type="checkbox"/> B71	
PCI LOCK	5G Band		
	<input checked="" type="checkbox"/> n2	<input checked="" type="checkbox"/> n5	<input checked="" type="checkbox"/> n7
	<input checked="" type="checkbox"/> n12	<input checked="" type="checkbox"/> n14	<input checked="" type="checkbox"/> n25
	<input checked="" type="checkbox"/> n30	<input checked="" type="checkbox"/> n41	<input checked="" type="checkbox"/> n48
	<input checked="" type="checkbox"/> n66	<input checked="" type="checkbox"/> n71	<input checked="" type="checkbox"/> n77
	<input checked="" type="checkbox"/> n78		
	<input type="checkbox"/> Select ALL		
	Apply		

Figure 37 Cellular Settings > Network

3.4.6.2 SIM And APN Settings

On this page, you can find the option to select the SIM & APN related settings which you want to use connect with network.

Dashboard	Status	Settings	SMS
Basic	Switch SIM Card		
VPN	Switch SIM Card SIM2 ▾		
Security	APN Settings		
Advanced	Current APN 3gnet		
Cellular Settings	Mode <input checked="" type="radio"/> Auto <input type="radio"/> Manual		
Network	Host Name ▾		
SIM And APN Settings	Profile Name Auto		
Network Watchdog	APN Auto		
IP Passthrough	Authentication None ▾		
PCI LOCK	User Name 		
	Password 		
	Set as default		

Figure 38 Cellular Settings > SIM and APN Settings

The default APN mode is set to "Auto", if you want to configure the APN, you should choose the manual mode, then you can define the required APN settings by clicking on the "Add New" button.

APN Settings	
Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Host Name	▾
Profile Name	Auto
APN	Auto
Authentication	None ▾
User Name	
Password	
Set as default	

Figure 39 Cellular Settings > APN

APN Settings

Mode: ☐ Auto ☒ Manual

Host Name:

Profile Name:

APN:

Authentication:

User Name:

Password:

Figure 40 APN > Manual APN

From the “Host Name” option, you can choose the APN that you had configured, then click “Set as default” to take effect.

3.4.6.3 Network Watchdog

On this page, you can view the network watchdog feature which is designed to support uninterrupted data services defined by the ISP.

Sometimes the router finds connected and acquired WAN IP addresses from the network but no data/internet services. In that scenario, this feature can reboot/re attach to network.

Dashboard	Status	Settings	SMS
Basic	Network Watchdog Settings		
WiFi	Network ping	<input type="text" value="Enabled"/>	
VPN	URL or IP adress to ping no.1:	<input type="text" value="Disabled"/>	
Security	URL or IP adress to ping no.2:	<input type="text" value="8.8.8.8"/>	
Advanced	URL or IP adress to ping no.3:	<input type="text" value="8.8.4.4"/>	
Cellular Settings	<input type="button" value="Apply"/>		
Network			
APN Settings			
Network Watchdog			
PCI LOCK			

Figure 41 Cellular Settings > Network Watchdog

You can define the URL/IP address that the router will use to check the internet/data accessibility in regular intervals.

3.4.6.4 IP Passthrough

On this page, you can enable or disable the IP Passthrough Mode. If this feature

is enabled, PW550+ assign the acquired WAN IP address to the device (PC/ Router) connected to it.
By default, this feature is enabled.

Dashboard	Status	Settings	SMS
Basic	IP Passthrough		
Cellular Settings	IP Passthrough Enabled ▼		
Network	<input type="button" value="Apply"/>		
SIM And APN Settings			
Network Watchdog			
IP Passthrough			
PCI LOCK			

Figure 42 Cellular Settings > IP Passthrough

3.4.6.5 PCI LOCK

On this page, you can lock the PW550+ on available cell ID.

Dashboard	Status	Settings	SMS
Basic	PCI Lock Status		
WiFi	Locked Status Disabled ▼		
VPN	<input type="button" value="Apply"/>		
Security	Enabled Disabled		
Advanced	PCI Lock		
Cellular Settings	Name	Cellular	EARFCN PCI
Network	Locked Value	5G ▼	<input type="text"/>
APN Settings	<input type="button" value="Lock"/>		
Network Watchdog	Serving Cell List		
PCI LOCK	No	Cellular	EARFCN PCI Band Bandwidth RSRP RSRQ SINR
	1	4G	5230 377 B13 10MHz -96 -15 - <input type="checkbox"/>
	2	5G	648672 147 n77 60MHz -110 -7 1 <input type="checkbox"/>
	Neighbour Cell List		
	No	Cellular	EARFCN PCI RSRP RSRQ SINR
	1	5G	648672 44 -31 - - <input type="checkbox"/>
	2	5G	648672 128 -31 - - <input type="checkbox"/>
	<input type="button" value="Lock"/> <input type="button" value="Refresh"/>		
	White List		
	No	Cellular	EARFCN PCI
	<input type="button" value="Unlock"/>		

Figure 43 Cellular Settings > PCI LOCK

4. ATRACS

Cloud Connect Remote Management

You can manage the device using the ATEL Remote Management Platform ATRACS, by visiting <http://aags.a-tracs.com> or <https://aags.a-tracs.com>. Please refer to the ATRACS User Manual for details.

5. FAQ

Common Problems, FAQ's and Solutions

1. **The LED indicator on PW550+ is not ON.**
 - a. Confirm the power adapter is plugged properly into the AC socket.
 - b. Confirm the PoE injector led it lit up.

Note: Use the same PoE injector & Power Adaptor which is provided and comes packaged with the device.
2. **Web Based Utility (WebGUI) cannot be accessed.**
 - a. Ensure that the PW550+ is powered on.
 - b. Ensure that your client device is connected and has acquired the IP address from the PW550+ in router or IP Passthrough mode.
 - c. Check with another web browser or try to reset the browser cache memory.
 - d. Try to Reboot or factory reset PW550+.
3. **PW550+ cannot access the network.**
 - a. Ensure your USIM card is valid and active.
 - b. Check the LED on PW550+, it should be On. Refer to LED definition for more details.
 - c. You can login to WebGUI and check the Network details available on the home page.
 - d. Network status should be showing Connected. If it is showing disconnected or connecting, check the network parameters RSRP, SINR values.
 - i. SINR value (dB) should be Positive.
 - ii. RSRP value must be greater than -115dBm. Preferred value should be around -90 dBm.
 - e. Try to Reboot or factory reset your PW550+.

4. How do I optimize the device to maximize throughput?

- a. You can log into the WebGUI to check the RSRP/RSRQ/SINR to verify the changes to signal quality.
- b. In the WebGUI, you can also go to "Settings" > "Cellular Settings" > "Network", to specify the band you want to use. Please check and confirm band information with your carrier before you adjust the band you prefer. Please note that we don't encourage customers to adjust these features by themselves if you are not familiar with mobile technology.

Regulatory Statements

FCC Equipment Authorization ID: **XYO-PW550+**

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

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

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.

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

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.

RF Exposure Warning Statements:

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons during the normal operations.

NOTE: The Radio Frequency (RF) emitter installed in your modem must not be located or operated in conjunction with any other antenna or transmitter, unless specifically authorized by ATEL.

Safety Hazards

Follow Safety Guidelines

Always follow the applicable rules and regulations in the area in which you are using your device. Turn your device off in areas where its use is not allowed or when its use may cause interference or other problems. Note that this type of device should be placed at least 10 ft from work area(s).

Electronic Devices

Most modern electronic equipment is shielded from radio frequency (RF) signals. However, inadequately shielded electronic equipment may be affected by the RF signals generated by your device.

Medical and Life Support Equipment

Do not use your device in healthcare facilities or where medical life support equipment is located as such equipment could be affected by your device's external RF signals.

Pacemakers

- It is recommended to maintain a minimum separation of six inches between a RF device and a pacemaker in order to avoid potential interference with the pacemaker.
- Persons with pacemakers should always follow these guidelines:
- Always keep the device at least six inches away from a pacemaker when the device is turned on.
- Place your device on the opposite side of your body where your pacemaker is implanted in order to add extra distance between the pacemaker and your device.
- Avoid placing a device that is on next to a pacemaker (e.g., do not carry your device in a shirt or jacket pocket that is located directly over the pacemaker).
- If you are concerned or suspect for any reason that interference is taking place with your pacemaker, turn your device OFF immediately.

Hearing Devices

When some wireless devices are used with certain hearing devices (including hearing aids and cochlear implants) users may detect a noise which may interfere with the effectiveness of the hearing device.

Use of Your Device while Operating a Vehicle

Please consult the manufacturer of any electronic equipment that has been installed in your

vehicle as RF signals may affect electronic systems in motor vehicles. Please do not operate your device while driving a vehicle. This may cause a severe distraction, and, in some areas, it is against the law.

Use of Your Device on an Aircraft

Don't use your device during flight, it may violate FAA regulations. Because your device may interfere with onboard electronic equipment, always follow the instructions of the airline personnel and turn your device OFF.

Blasting Areas

In order to avoid interfering with blasting operations, your device should be turned OFF when in a blasting area or in an area with posted signs indicating that people in the area must turn off two-way radios. Please obey all signs and instructions when you are in and around a blasting area.

Disclaimer:

Certain variations may be present between the device and user manual description depending on software release or specific network services. ATEL shall not be held legally responsible for such deviations, if any, nor for their potential consequences.

Limited Warranty:

The full ATEL USA Warranty Policy can be found at www.atel-usa.com/warranty. On this page you can "Start a Warranty Claim", "Check on an Existing Claim" and read the Warranty Policy by clicking on "ATEL's Warranty Policy". Please follow all warranty instructions available and if you have any questions contact us at support@atel-usa.com. Note that some actions such as, but not limited to, using sharp objects to open the device, may void the warranty.

Trademark. ATEL & Axis are trademarks owned and protected by Asiatelco Technologies, Inc.
© 2024 Asiatelco Technologies, Inc. All rights reserved.