

LTE CPE (J912) User Manual

Index

1.	About this Manual.....	3
2.	Product Overview.....	3
3.	Configuring the CPE	3
	3.1 Login	3
	3.2 Dashboard	4
	3.3 Status	4
	3.3.1 WAN Status.....	4
	3.3.2 Network Status	5
	3.3.3 Software.....	5
	3.3.4 Device List	5
	3.3.5 Statistics	6
	3.4 Settings.....	6
	3.4.1 Basic.....	7
	3.4.2 Advanced	9
	3.4.3 Security.....	13
	3.5 LTE	19
4.	Revision History	21

1. About this Manual

The content of this User Manual has been made as accurate as possible. However, due to continual product improvements, specifications and other information are subject to change without notice.

2. Product Overview

This CPE supports LTE Band (Subject to the configuration of LTE module) and it supports popular operating systems like Windows, Linux and Mac.

Please refer to the Quick Start Guide that is part of the CPE supply. Once you have identified the place for CPE, insert USIM card supplied by your service provider at the appropriate place, plug in the adapter in the AC socket and DC in the power port of CPE. Switch on the power Off/On switch and after few minutes the CPE should attach itself to the LTE network. It is as simple as that. It is advised to read this manual at leisure to make best use of the CPE.

3. Configuring the CPE

The basic settings in WebGUI consist of four main parts named Home, Diagnostics, Settings, LTE. You can login to WebGUI as follows, and configure the settings according to your requirements.

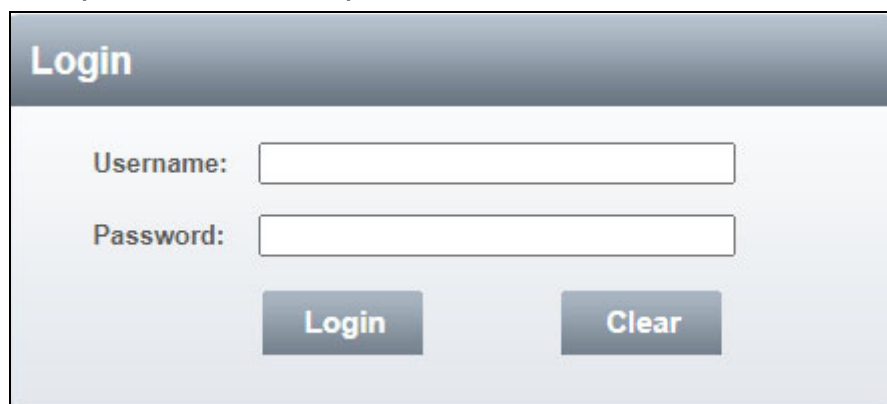
3.1 Login

Open your Web browser and enter 192.168.0.1 in the address bar;

Login window will popup;

When prompted for User name and password, enter the following username and password.

Username/Password: admin/admin



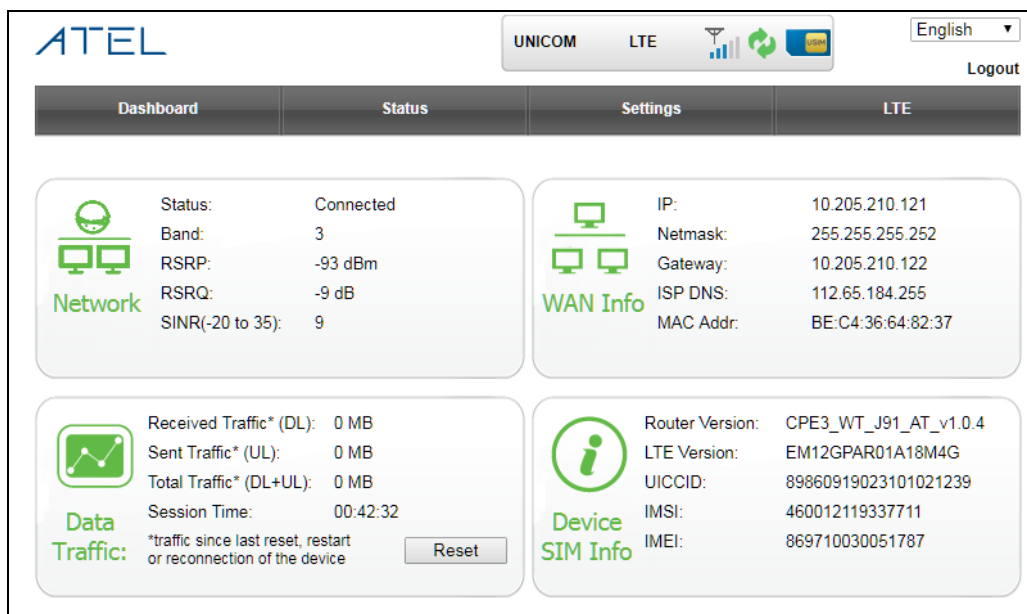
The screenshot shows a web browser window titled "Login". Inside the window, there are two text input fields. The first is labeled "Username:" and the second is labeled "Password:". Below these fields are two buttons: "Login" and "Clear". The background of the window is light blue with a subtle gradient.

3.2 Dashboard

After successful login, the following screen will appear and you will see four main menus on the top bar of the WebGUI.

The bars in the middle indicate the received signal level and USIM icon displays the status of USIM. Click "Logout", the screen will turn to login window.

From this page, you can also know the LTE network status and the LTE data transmission. Click "OK", it will take you to the device settings page, then you can modify the password as you like (32 characters max). Login the system by the new password, you can see the home page.



3.3 Status

On this page, you can see WAN Status, Network Status, Software, Device List and Statistics.

Dashboard	Status	Settings	LTE
WAN Status	WAN Status		
Network Status	WAN Mode	LTE/3G/2G	
Software	Bridge	Disabled	
Device List	IPv4 Address	10.205.210.121	
Statistics	IPv4 Primary DNS	112.65.184.255	
	IPv4 Secondary DNS	210.22.84.3	

3.3.1 WAN Status

From the WAN Status, you can see WAN Mode, Bridge, IPv4 Address, WAN

Primary DNS and DNS information.

WAN Status	WAN Status	
Network Status	WAN Mode	LTE/3G/2G
Software	Bridge	Disabled
Device List	IPv4 Address	10.205.210.121
Statistics	IPv4 Primary DNS	112.65.184.255
	IPv4 Secondary DNS	210.22.84.3

3.3.2 Network Status

Clicking on the “Network Status”, you can see the LTE information i.e. Connection Status, USIM Status, IMEI, IMSI, RSRP, RSRQ, RSSI, SINR, PLMN and Band.

WAN Status	LTE Status	
Network Status	Connection Status	Connected
Software	USIM Status	Ready
Device List	IMEI	869710030051787
Statistics	IMSI	460012119337711
	RSRP	-99 dBm
	RSRQ	-14 dB
	RSSI	67
	SINR	7
	PLMN	46001
	Band	3

3.3.3 Software

Clicking on the “Software”, you can see the Router Software version and Modem Software Version.

WAN Status	Software	
Network Status	Router Software Version	CPE3_WT_J91_AT_v1.0.4
Software	Modem Software Version	EM12GPAR01A18M4G
Device List		
Statistics		

3.3.4 Device List

From the device list, you can know the users’hostname, MAC address, IP address ,Type and expires time.

WAN Status	Device List				
Network Status	Hostname	MAC Address	IP Address	Type	Expires
Software	DMSHD3F8212	00:0E:C6:C3:9C:E2	192.168.0.189	Ethernet	23:38:51
Device List					
Statistics					

3.3.5 Statistics

From the device list, you can know the speed, Download, Upload and Total Used Data.

WAN Status	Statistics			
Network Status				
Software				
Device List				
Statistics				
		Download	Upload	
Speed		0 Kb/s	0 Kb/s	
		Duration	Downloaded	Uploaded
Current Session		17:25:00	0 MB	0 MB
Total		17:25:00	0 MB	0 MB
The amounts of data is approximate. For more information please contact your network operator.				
Clear				

3.4 Settings

The settings menu consists of three main menus named Basic advanced and Security settings.

Basic	UI Access Settings	
Management	Username	admin
LAN/DHCP	New Admin Access Password	(32 characters max.)
Manual Upgrade	Repeat Admin Access Password	(32 characters max.)
Automatic Upgrade	Apply	Clear
Advanced	Factory Reset	
Security	Click button to restore default settings	Restore
	Device Reboot	
	Click button to reboot the device	Reboot

3.4.1 Basic

3.4.1.1 Management

On this page, you can see UI Access Settings, Factory reset and device reboot.

Basic	UI Access Settings	
Management	Username	admin
LAN/DHCP	New Admin Access Password	(32 characters max.)
Manual Upgrade	Repeat Admin Access Password	(32 characters max.)
Automatic Upgrade	Apply Clear	
Advanced	Factory Reset	
Security	Click button to restore default settings	Restore
	Device Reboot	
	Click button to reboot the device	Reboot

- **UI Access Settings** –The default password is admin, you can enter 1~32 characters for 2 times as your new password. Then you would logout automatically and you should login to the system by the new password.
- **Factory Reset** –From this page, you can click the “Restore” button to load default to the factory setting.
- **Device Reboot**–From this page, you can click the “Reboot” button to restart the device.

3.4.1.2 LAN Settings

Clicking on the “LAN Settings” tab will take you to the “LAN Settings” header page. On this page, all settings for the internal LAN setup of the CPE router can be viewed and changed.

Basic	LAN Settings	
Management	IP Address	192.168.0.1
LAN/DHCP	Subnet Mask	255.255.255.0
Manual Upgrade	DHCP	Enabled ▼
Automatic Upgrade	Start IP Address	192.168.0.2
Advanced	End IP Address	192.168.0.254
Security	Lease Time	86400
	Apply Clear	

- **IP Address** - Enter the IP address of your router (factory default: 192.168.254.251).

- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **DHCP Type** - Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else 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 address. The default start address is 192.168.254.2.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP address. The default end address is 192.168.254.200.
- **Lease Time** - The Lease Time is the amount of time a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP address. After the time is up, the user will be assigned a new dynamic IP address automatically.

 Note:

1. If you change the IP Address of LAN, you must use the new IP address to login to the CPE 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 Device Software Upgrade

On this page, you can upgrade the current Router version from the local PC. 100s is needed to complete the whole upgrade process, and then the device will reboot automatically

Basic	Device Software Upgrade
Management	Router Upgrade: 选择文件 未选择任何文件
LAN/DHCP	Apply
Manual Upgrade	
Automatic Upgrade	
Advanced	
Security	

3.4.1.4 Automatic Upgrade

You should enable the Remote Upgrade before you use this function.

Basic	Device Remote Upgrade	
Management	Upgrade Status	The current firmware version is the latest one
LAN/DHCP	Remote Upgrade	Enabled ▼
Manual Upgrade	Upgrade Address (IP or URL)	http://ams.asiateelco.com:50001/www/upl
Automatic Upgrade	Upgrade Mode	No traffic ▼ (No traffic for ten minutes)
Advanced	Manual	Check Upgrade
Security	Apply	

Backup & Restore

Clicking the “Backup” button, the current settings will be saved as a data file to the local PC. You can restore the device configuration from the files that you saved.

Click the “Restore” button to load default to the factory setting.

Basic Settings	backup settings	
Management	Backup device configuration	Backup
LAN Settings	restore settings	
WiFi 2.4GHz Settings	Restore device configuration from file	选择文件 未选择任何文件 Restore
WPS Settings		
Backup & Restore		
Advanced Settings		

3.4.2 Advanced

3.4.2.1 Dynamic DNS

The dynamic DNS function is disabled in default, you can choose the dynamic DNS provider to configure the DDNS settings.

Basic	DDNS Settings	
Advanced	DDNS Status	Disabled
Dynamic DNS	Dynamic DNS Provider	Disabled ▼
Routing	User Name	
NTP	Password	
Diagnostic	Domain Name	
System Log	Apply	
Network Management		
Backup & Restore		
Security		

3.4.2.2 Routing

From the rule table, you can see the default route information. Clicking on the “Add New” button, you can configure the static routing setting. The new rules will be shown on the rule table, here you can delete the rules that you have selected or add new rules sequentially. The maximum rule count is 10.

Basic	Rule table								
Advanced	No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface
Dynamic DNS	1	0.0.0.0	0.0.0.0	10.239.184.108	3	1	0	0	wwan0(wwan0)
Routing	2	10.239.184.104	255.255.255.248	0.0.0.0	1	0	0	0	wwan0(wwan0)
	3	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)
NTP	Delete		Add New		(maximum alert10)				
Diagnostic									
System Log									
Network Management									
Backup & Restore									
Security									

Static Routing Settings

Destination

Range

Gateway

Interface

- **Destination:** The address of the network or host that assigned by the static route;
- **Range:** Host/Net;
- **Gateway :** This is the IP address of the gateway device that is used to contact between the router and the network or host;
- **Interface:** LAN/WAN/Custom;
- **RIP:** Enable the RIP, every 30 seconds, the system will update and learn the routing information nearby automatically.

3.4.2.3 NTP

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

Basic	Network Management	
Advanced	Remote management (http)	Disable ▼ (e.g. http://ip_address:port)
Dynamic DNS	Remote management (https)	Disable ▼ (e.g. https://ip_address:port)
Routing	HTTP Login(WebUI Management)	Enable ▼
NTP	HTTPS Login(WebUI Management)	Enable ▼
Diagnostic	Respond to PING on WAN	Disable ▼
System Log	Respond to PING on LAN	Enable ▼
Network Management	Apply	
Backup & Restore		
Security		

➤ **Remote management(http)**

You can access to the router via http IP address and achieve the remote control function when the remote management feature is enabled.

➤ **Remote management(https)**

You can access to the router via https IP address and achieve the remote control function when the remote management feature is enabled.

➤ **HTTP Web Login**

This function allows the users to login the system by the http protocol method.

➤ **HTTPS Web Login**

This function allows the users to login the system by the https protocol method.

➤ **Respond to PING on WAN**

It is allowed to ping on WAN in default, you can disable it here.

➤ **Respond to PING on LAN**

It is allowed to ping on LAN in default, you can disable it here.

3.4.2.7 Backup&Restore

Clicking the “Backup” button, the current settings will be saved as a data file to the local PC. You can restore the device configuration from the files that you saved.

Basic	Backup Settings	
Advanced	☐ Need password to backup	(32 characters max.)
Dynamic DNS	Backup device configuration	Backup
Routing	Restore Settings	
NTP	☐ Need password to restore	(32 characters max.)
Diagnostic	Restore device configuration from file	选择文件 未选择任何文件 Restore
System Log		
Network Management		
Backup & Restore		
Security		

3.4.3 Security

3.4.3.1 MAC Filtering

This function is a powerful security feature that allows you to specify which wireless client users are not allowed to surf the Internet.

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, you can configure the rules you like.

Mac Filtering Schedule: MAC devices that do not comply with the Schedule would be “Allow/Deny”.

3.4.3.2 IP/Port Filtering

From this page, you can configure the IP/Port filter to forbid relevant users to login the router device.

The default IP/Port filter setting is disabled, so you should enable it before you begin to configure the filter. Then clicking the “Add New” button, you can configure the settings you like (Figure 3-4-2-2-3).

Default Policy: The packets that don't match with any rules would be “Dropped/Accepted”. If you choose “Dropped” here, the action of the new rule

would be “Accept”. Otherwise, the action turns to be “Drop” and the packet that don’t match with any rules would be accepted.

The screenshot shows the 'IP/Port Filtering Settings' page. On the left is a sidebar menu with options: Basic, Advanced, Security, MAC Filtering, IP/Port Filtering (highlighted), Content Filtering, Port Forwarding, Virtual Server, DMZ, UPnP, and VPN Passthrough. The main content area has a title 'IP/Port Filtering Settings' and two dropdown menus: 'IP/Port Filtering' set to 'Disable' and 'Default policy - the device that don't match any rule would be:' set to 'Dropped'. There is an 'Apply' button below these settings.

The screenshot shows the 'IP/Port Filtering Settings' page with 'IP/Port Filtering' set to 'Enable'. Below the settings is a 'Rule Table' section. The table has columns: ID, Dest IP Address, Source IP Address, Protocol, Dest Port Range, Source Port Range, and Action. Below the table are buttons for 'Apply', 'Delete', and 'Add New', along with a note: '(Note: maximum rule count is 20)'. The text 'Others would be dropped' is also visible.

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 PC. (Such as 192.168.0.2).
- **Protocol**- TCP, UDP, ICMP
- **Dest Port Range**- To restrict Internet access to the single user, you can set a fixed value, such as 21-21.
- **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 sequentially . The maximum rule count is 10.

Basic	Add Rule
Advanced	Dest IP Address
Security	Source IP Address
MAC Filtering	Protocol All
IP/Port Filtering	Dest Port Range -
Content Filtering	Source Port Range -
Port Forwarding	Action Accept
Virtual Server	Apply Back
DMZ	
UPnP	
VPN Passthrough	

3.4.2.3 Content Filtering

From this page, you can configure the URL filter and the content filtering schedule.

Basic	Content Filtering Rule Table
Advanced	ID URL Address or Keyword Select
Security	Delete Add New Note: maximum rule count is 20
MAC Filtering	Content Filtering Schedule
IP/Port Filtering	Schedule Disabled
Content Filtering	Apply
Port Forwarding	
Virtual Server	
DMZ	
UPnP	
VPN Passthrough	

● Content Filtering

It is a function that forbids users to login the URL or keyword on the rule table. You can configure the settings you like by clicking the “Add New” button.

The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules sequentially. The maximum rule count is 8.

Basic Settings	Content Filtering Settings
Advanced Settings	Address URL or Keyword www.google.com
MAC Filtering	Add Back
IP/Port Filtering	

● Content Filtering Schedule

Here you can configure the schedule to define when the rules take effect. This feature is disabled in default, you should enable it first and then configure the date and time, such as working time. Click the “Apply” button, you can see the new rule on the content filtering page.

Content Filtering Schedule				
Schedule	Enabled ▼			
Date	☐ Everyday			
	☒ Mon	☒ Tue	☒ Wed	☒ Thu
	☒ Fri	☐ Sat	☐ Sun	
Time	☐ Everytime			
	☒ At a defined time From 09 h 00 min. To 18 h 00 min.			
Apply				

3.4.2.4 Port Forwarding

Clicking on the header of the “Port Forwarding” button will take you to the “Port Forwarding” header page. Clicking on the “Add New” button, you can configure IP address, port range to achieve the port forwarding purpose.

Basic	Advanced	Security	Port Forwarding Rule Table												
MAC Filtering	IP/Port Filtering	Content Filtering	<table border="1"> <thead> <tr> <th>ID</th> <th>IP Address</th> <th>Port Range</th> <th>Protocol</th> </tr> </thead> <tbody> <tr> <td colspan="4"> ☐ Select All </td> </tr> <tr> <td colspan="4"> Edit Delete Add New </td> </tr> </tbody> </table>	ID	IP Address	Port Range	Protocol	☐ Select All				Edit Delete Add New			
ID	IP Address	Port Range	Protocol												
☐ Select All															
Edit Delete Add New															
Port Forwarding	Virtual Server	DMZ	(Note: maximum rule count is 20)												
VPN Passthrough	UPnP														

Basic	Advanced	Security	Port Forwarding Settings								
MAC Filtering	IP/Port Filtering	Content Filtering	<table border="1"> <tr> <td>IP Address</td> <td> </td> </tr> <tr> <td>Port Range</td> <td> - </td> </tr> <tr> <td>Protocol</td> <td>TCP&UDP ▼</td> </tr> <tr> <td colspan="2"> Apply Back </td> </tr> </table>	IP Address		Port Range	-	Protocol	TCP&UDP ▼	Apply Back	
IP Address											
Port Range	-										
Protocol	TCP&UDP ▼										
Apply Back											
Port Forwarding	Virtual Server	DMZ									
VPN Passthrough	UPnP										

- **IP Address-** The IP address of the PC running the service application;
- **Port Range-** You can enter a range of service port or set a fixed value;
- **Protocol-** UDP, TCP, TCP&UDP.

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 here. The maximum rule count is 20.

3.4.2.5 Virtual Server

Clicking on the header of the “Virtual Server” button will take you to the “Virtual Server” header page. It is a feature that similar to port forwarding, clicking on the “Add New” button, you can configure IP address, public port, private port and protocol to achieve the virtual server function.

ID	IP Address	Public Port	Private Port	Protocol
☐ Select All (Note: maximum rule count is 20)				

IP Address	192.168.0.5
Public Port	5100
Private Port	5200
Protocol	TCP&UDP ▼

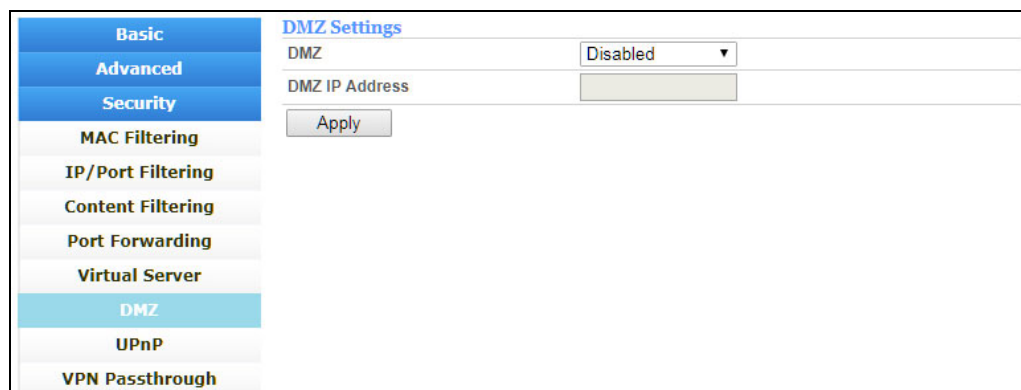
- **IP Address-** The IP address of the PC running the service application;
- **Public Port-** The port of server-side;
- **Private Port-** The port of client-side, it can be same with the public port;
- **Protocol-** UDP, TCP, TCP&UDP.

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 here. The

maximum rule count is 20.

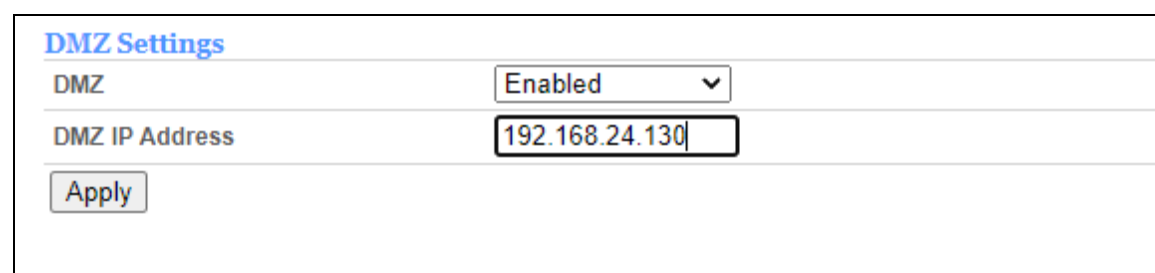
3.4.2.6 Demilitarized Zone

From this page, you can configure a De-militarized Zone (DMZ) to separate internal network and Internet.



DMZ Settings	
DMZ	Disabled ▼
DMZ IP Address	
Apply	

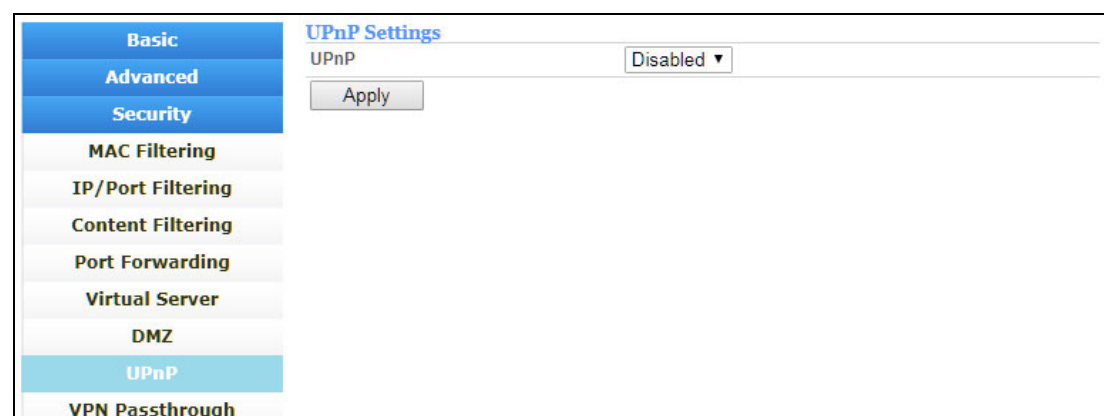
- **DMZ IP Address-** The IP address of your PC. (such as 192.168.254.130)



DMZ Settings	
DMZ	Enabled ▼
DMZ IP Address	192.168.24.130
Apply	

3.4.2.7 Upnp

The UPnP function is Enabled in default, you should enable it on the system security page. before using it. The new rules that you added will be shown on this page.



UPnP Settings	
UPnP	Disabled ▼
Apply	

3.4.2.8 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 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.

Basic	VPN Passthrough
Advanced	L2TP Passthrough Enabled
Security	IPSec Passthrough Enabled
MAC Filtering	PPTP Passthrough Enabled
IP/Port Filtering	Apply
Content Filtering	
Port Forwarding	
Virtual Server	
DMZ	
UPnP	
VPN Passthrough	

3.5 LTE

3.5.1 APN Settings

The default APN mode is automatic and APN is NULL, if you want to configure the LTE APN, you should choose the manual mode, then you can configure the APN settings by clicking on the “Add New” button.

Dashboard	Status	Settings	LTE
APN Settings	APN Settings		
PIN Management	Mode ☒ Auto ☐ Manual		
Network	Host Name		
	APN Type IPv4		
	Profile Name none		
	APN		
	Authentication None		
	User Name		
	Password		
	Set as default		

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

APN Settings	APN Settings	
PIN Management		
Network		
	Mode ☐ Auto ☒ Manual 	
	Host Name	Add New Cancel
	APN Type	IPv4
	Profile Name	1234
	APN	aaaa
	Authentication	CHAP
	User Name	1234
	Password	1234
	Save	

3.5.2 PIN Management

From this page, you can see the USIM card status and PIN status.

The default PIN status is disabled, you can input the correct PIN to enable the PIN function. The maximum PIN attempts are 3, otherwise you must enter PUK to reset the PIN code. The USIM will be invalid after the unsuccessful attempts for 10 times.

APN Settings	PIN Management	
PIN Management		
Network		
	USIM Card Status	USIM Ready
	PIN Status	Disabled
	Remaining PIN Attempts	3
	PIN Lock	 ☒ Enable ☐ Disable
	Delete PIN from device?	Delete
	Apply	

- **PIN Management:** Enter the correct PIN to enable or disable the PIN function, PIN code should be 4 to 8 digits;
- **Save PIN:** The system will remember the PIN code of the USIM and verify the USIM automatically if the save PIN function is enabled.
- **PIN change:** You can input the current PIN code 1 time and the new PIN code for 2 times to change the PIN code. PIN code should be 4 to 8 digits.
- **PUK Management:** Input the correct PUK code and the new PIN code for 2 times to reset the PIN code. The PIN code should be 4 to 8 digits.

PIN Management

PUK Management

Current PUK	
Remaining PUK attempts	10
New PIN	
Confirm New PIN	

Apply

4. Revision History

Author	Revision	Changes	Date
Jiawang	1.0	Create Draft	2021-12-08

FCC Regulations:

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.

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 manufacturer could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with FCC RF Exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for the transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.