

## Lantern™ 5G Outdoor FWA User Manual

Airgain, Inc

Updated: January 2024



Airgain, Inc. 2024. All Rights Reserved.

Airgain, Inc provides this documentation in support of its products for the internal use of its current and prospective customers. The publication of this document does not create any other right or license in any party to use and content in or referred to in this document and any modification or redistribution of this document is not permitted.

While efforts are made to ensure accuracy, typographical and other errors may exist in this document. Airgain, Inc reserves the right to modify or discontinue its products and to modify this and any other product documentation at any time.

All Airgain, Inc products are sold subject to its published Terms and Conditions, subject to any separate terms agreed with its customers. No warranty of any type is extended by publication of this documentation, including, but not limited to, implied warranties or merchantability, fitness for a particular purpose and non-infringement.

Airgain, Inc. is a registered trademark. Inc. All trademarks, service marks and similar designations referenced in this document are the property of their respective owners.

## Table of Contents

<b>Table of Contents</b>	<b>2</b>
<b>Web Interface</b>	<b>4</b>
<b>Function Icon</b>	<b>5</b>
<b>Status</b>	<b>6</b>
Device Status	6
Modem Status	7
Network Status	11
Client List	12
About	13
<b>Management</b>	<b>14</b>
Setup Wizard	14
Modem Setup	16
Internet Setup	18
LAN Setup	20
IPv6 Setup	23
Diagnostics	26
System Log	27
QoS	29
<b>Personalization</b>	<b>30</b>
PIN Management	30
Configuration	31
Device Setup	32
Software	33
SMS Management	34
LED Management	
<b>Basic</b>	<b>36</b>
Firewall	36
DMZ	37
UPnP	37
Dynamic DNS	38
VPN Passthrough	38

<b>Advanced</b>	<b>39</b>
MAC Filtering	39
IP Filtering	40
Port Forwarding	41
Port Triggering	42
Parental Control	43
Static Routing	44
<b>Wi-Fi</b>	<b>45</b>
Basic	45
Advanced	46
<b>Engineering</b>	<b>47</b>
Band Selection Settings	47
DM Settings	49
QXDM	51

## 1. Web Interface

Open Web browser and enter device's default IP address: <https://192.168.15.1/>  
 Enter login username and password to access Web management interface.

### Default Login Information

General Account

Username: admin.

Password: see device box label

Advanced Account

Username: operator

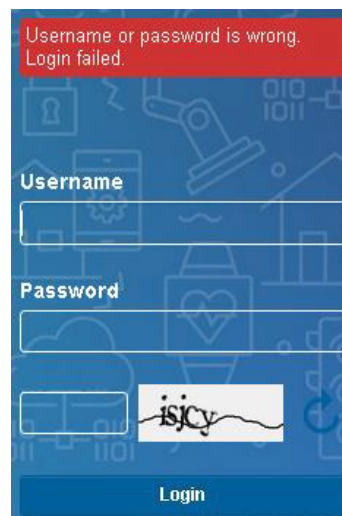
Password: see device box label



### Login Protection
















If you input wrong username and/or password more than three times, device will ask for additional identification.

You can press re-fresh button to re-generate identification if it is hard to recognize.



## 2. Function Icon

Below is an icon and definition list on Web UI.

Function Icon	Description
	Force device to reboot itself
	Logout device and it will be back to login page
	Force modem to reconnect to WAN
	Force modem to connect to WAN
	Force modem to disconnect from WAN
	No SIM card inserted into device
	Device is waiting for PIN / waiting for PUK
	Weak signal indication for 4G/5G
	Medium signal strength indication for 4G/5G
	Good signal strength indication for 4G/5G
	No signal indication for 4G/5G
	Traffic indication for up-stream direction
	Traffic indication for down-stream direction
	Traffic indication for both up-stream and down-stream directions
	No traffic indication for both up-stream and down-stream directions
	Indication for connected client(s)

NOTE: RECONNECT/CONNECT/DISCONNECT icons will be shown depending on the UI setting Management>Modem Setup.

If “Enable Auto Connection” is checked, RECONNECT icon is shown. Otherwise, CONNECT or DISCONNECT icon will be shown while modem is disconnected from WAN or connected to WAN.

### 3. Status

#### 3.1 Device Status

This page is information only, here displays the current status of the device such as WAN information. You can refer to below column for detail definitions.

Device Status	
Internet Mode	Dynamic IP
2.4GHz Host SSID	Spot_0005
Firewall	Medium (standard)
UPnP	Disable
DMZ	Disable
DDNS	Disable
Time Zone	(UTC) Coordinated Universal Time
Location (Latitude, Longitude)	Positioning

Below are the definitions for each item:

Item	Description
<b>Internet Mode</b>	<p>The mode to forward data packets between Internets</p> <ul style="list-style-type: none"> <li>• <b>Dynamic IP</b></li> <li>• <b>PPTP</b></li> <li>• <b>L2TP</b></li> <li>• <b>GRE</b></li> <li>• <b>IPsec</b></li> <li>• <b>IPv4 Passthrough</b></li> </ul> <p>Please go <b>Management &gt; Internet</b> Setup to configure it</p>
<b>2.4GHz Host SSID</b>	Show the current SSID of the 2.4G Wi-Fi. Please note, this item will only be seen when login in with the advanced account.
<b>Firewall</b>	Here displayed your current firewall level; there are three default configurations for you to select: Low/Medium/High. For more detail, please refer to Basic > Firewall section
<b>UPnP</b>	UPnP enabled or disabled
<b>DMZ</b>	DMZ enabled or disabled
<b>DDNS</b>	DDNS enabled or disabled
<b>Time Zone</b>	Time Zone
<b>Location (Latitude, Longitude)</b>	Show the location of the ODU by its coordinates



Below are the definitions for each item:

Common	
Item	Description
<b>Network</b>	Current active network mode.
<b>Connection Status</b>	The status of modem connection.
<b>Connection Time</b>	Time during which the unit is connected to the eNB or base station.
<b>Operator Name</b>	Current connected operator name.
<b>Uplink Current Speed</b>	Uplink data rate.
<b>Downlink Current Speed</b>	Downlink data rate.
<b>Data Uplink/ Downlink Traffic</b>	Displays the current accumulate Data Downlink/Uplink traffic. You can reset by press the "Clear Traffic" button in right.
<b>PIN Remain</b>	The remained PIN retry count.
<b>PUK Remain</b>	The remained PUK retry count.
<b>USIM Status</b>	SIM card status information.
<b>Roaming Status</b>	Informs current roaming status.
<b>PLMN</b>	Public Land Mobile Network identity.
<b>IMSI</b>	International mobile subscriber identity.
<b>ICCID</b>	Integrate circuit card identity.



LTE	
Item	Description
<b>Cell ID (DEC)</b>	Cell Identifier in hex decimal format.
<b>Connected Band</b>	Current connected Band(According to 3GPP defined).
<b>SINR</b>	Signal to Interference plus Noise Ratio.
<b>RSSI</b>	Received Signal Strength Indication.
<b>RSRQ</b>	Reference Signal Received Quality.
<b>RSRP</b>	Reference Signal Received Power.
<b>PCI</b>	Pre-coding Control Indication.

NR	
Item	Description
<b>Connected Band</b>	Current connected Band(According to 3GPP defined)
<b>Bandwidth</b>	Current connected Bandwidth.
<b>SINR</b>	Signal to Interference plus Noise Ratio.
<b>RSRQ</b>	Reference Signal Received Quality.
<b>RSRP</b>	Reference Signal Received Power.
<b>PCI</b>	Pre-coding Control Indication.
<b>SSB Arfcn</b>	Synchronization Signal Block Absolute Radio Frequency Channel Number.

### 3.2.2 Advanced

The Modem Status Advanced displays the information of each component carriers(CC). The information includes:

Advanced				
▼ LTE Cell Information				
PCC/SCC	Band	DL Earfcn	PCI	Bandwidth (MHz)
PCC	B7	3250	234	20
▼ NR Cell Information				
PCC/SCC	Band	SSB Arfcn	PCI	Bandwidth (MHz)
SCC	N78	625324	460	100

Below are the definitions for each item:

Item	Description
<b>LTE Cell Information</b>	<ul style="list-style-type: none"> <li>PCC/SCC               <ul style="list-style-type: none"> <li>PCC: Primary Component Carrier.</li> <li>SCC: Secondary Component Carrier.</li> </ul> </li> <li>Band: Current connected Band. (According to 3GPP defined.)</li> <li>DL Earfcn: Downlink Earfcn.</li> <li>PCI: Physical Cell Identifier.</li> <li>Bandwidth(MHz): Current connected Bandwidth</li> </ul>
<b>NR Cell Information</b>	<ul style="list-style-type: none"> <li>PCC/SCC               <ul style="list-style-type: none"> <li>PCC: Primary Component Carrier.</li> <li>SCC: Secondary Component Carrier.</li> </ul> </li> <li>Band: Current connected Band. (According to 3GPP defined.)</li> <li>SSB Arfcn: Synchronization Signal Block Absolute Radio Frequency Channel Number.</li> <li>PCI: Physical Cell Identifier.</li> <li>Bandwidth (MHz): Current connected Bandwidth</li> </ul>

### 3.3 Network Status

This page provides a summary of network status on WAN/LAN.

Network Status	
<b>IPv4</b>	
IP Address	10.83.74.253
Default Gateway	10.83.74.254
Primary DNS Server	210.241.208.1
Secondary DNS Server	139.175.1.2
<b>IPv6</b>	
WAN Global Address	2401:e180:8d53:237::94:a8:4eba:f2ca/64
Default Gateway	fe80::d87:28c4:a699:2418
Primary DNS Server	2401:e180:7863:218:241:208:1
Secondary DNS Server	2001:cd8:103::139:175:1:1
LAN Link-Local Address	fe80::4eba:7c8f:80e:ac8f/64
LAN Global Address	2401:e180:8d53:237::1800/64
Autoconfiguration Type	SLAAC DHCPv6





Below are the definitions for each item:

IPv4	
Item	Description
<b>IP Address</b>	IP address acquired on the WAN interface is displayed. Otherwise it is N/A.
<b>Default Gateway</b>	Device's WAN default gateway.
<b>Primary DNS Server</b>	The Primary Domain Name Server address is gotten from BS, if there is any.
<b>Secondary DNS Server</b>	The Secondary Domain Name Server address is gotten from BS, if there is any.

IPv6	
Item	Description
<b>WAN Global Address</b>	IPv6 address acquired on the WAN interface is displayed. Otherwise it is N/A.
<b>Default Gateway</b>	Device's WAN default gateway.
<b>Primary DNS Server</b>	The Primary IPv6 Domain Name Server address.
<b>Secondary DNS Server</b>	The Secondary IPv6 Domain Name Server address.
<b>LAN Link-Local Address</b>	IPv6 link-local address on the LAN interface is displayed.
<b>LAN Global Address</b>	IPv6 address acquired on the LAN interface is displayed. Otherwise it is N/A.
<b>Auto configuration Type</b>	The type to delegate IP address to PCs behind of the device.

### 3.4 Client List

This page displays all the end user information and contain two status information.

Client List					
▼ Connected Devices					
Icon	Host Name	IP Address	MAC Address	Connected via	Action
	20022921-N...	192.168.15.17	00:E0:84:2B:4A:21		<a href="#">Block</a>
▼ Blacklist					
Icon	Host Name	IP Address	MAC Address	Connected via	Action
	*	192.168.15.100	D4:5D:81:8A:7B:46		<a href="#">Unblock</a>

Below are the definitions for each item:

Item	Description								
<p><b>Connected Devices</b></p>	<p>The status displays currently connected end user information.</p> <ul style="list-style-type: none"> <li>Icon: The icon displays which device was connected</li> </ul> <table border="1" data-bbox="467 422 1031 554"> <tr> <td> Microsoft</td> <td> MacBook</td> <td> Android</td> <td> iPhone</td> </tr> <tr> <td> iPad</td> <td> TV</td> <td> Other</td> <td></td> </tr> </table> <ul style="list-style-type: none"> <li>Host Name: Display end user's name which connected the device.</li> <li>IP Address: Display end user's IP address which connected the device.</li> <li>MAC Address: Display end user's MAC address which connected the device.</li> <li>Connected via: Display access type.</li> <li>Action-Block: To Block the specific end user; After press the "Block" button the end user's record will be shown in Blacklist table.</li> </ul>	Microsoft	MacBook	Android	iPhone	iPad	TV	Other	
Microsoft	MacBook	Android	iPhone						
iPad	TV	Other							
<p><b>Blacklist</b></p>	<p>The status displays end user information was added in the blacklist table.</p> <ul style="list-style-type: none"> <li>Icon: The icon displays which device was blocked.</li> </ul> <table border="1" data-bbox="467 852 1031 984"> <tr> <td> Microsoft</td> <td> MacBook</td> <td> Android</td> <td> iPhone</td> </tr> <tr> <td> iPad</td> <td> TV</td> <td> Other</td> <td></td> </tr> </table> <ul style="list-style-type: none"> <li>Host Name: Display end user's name which blocked on the device..</li> <li>IP Address: Display end user's IP address which blocked on the device.</li> <li>MAC Address: Display end user's MAC address which blocked on the device.</li> <li>Connected via: Display access type.</li> <li>Action-Unblock: To Unblock the specific end user; After press the "Unblock" button the end user's record will be removed from Blacklist table.</li> </ul>	Microsoft	MacBook	Android	iPhone	iPad	TV	Other	
Microsoft	MacBook	Android	iPhone						
iPad	TV	Other							

### 3.5 About

This page displays the router default necessary information. Those values are set by the manufacturer as the factory defaults.

About	
Product Name	NR Outdoor CPE
Service Provider	Airgain
LAN MAC	4C:BA:7D:9E:4C:F8
Model Name	WNRQQ-110
2.4GHz Host Wi-Fi MAC	BA:4C:3F:9B:0B:05
Hardware Version	V00
Software Version	01.00.02.1070 (09/07/2023)
Modem Version	RG520NNADBRO3A01M8G_OCPU_GEMTEK_01.001.01.280
Serial Number	GMH2305_0000011
IMEI	863109100000000

Below are the definitions for each item:

Item	Description
<b>Product Name</b>	Router's product name.
<b>Service Provider</b>	Router's service provider
<b>LAN MAC</b>	Router's LAN MAC.
<b>Model Name</b>	Router's model name.
<b>2.4GHz Host Wi-Fi MAC</b>	The MAC address of 2.4G Wi-Fi interface. Please note, this item will only be seen when login in with the advanced account.
<b>Hardware Version</b>	Router's HW version.
<b>Software Version</b>	Router's SW/FW version.
<b>Modem Version</b>	Router's Modem version.
<b>Serial Number</b>	Router's serial number.
<b>IMEI</b>	International Mobile Equipment Identity number.

## 4. Management

### 4.1 Setup Wizard

1. By press the “Next” button to start Wizard, we will guide you to set up your Time Zone.

**Setup Wizard**

**Welcome to the Setup Wizard**

This wizard will guide you through the basic setup steps for your modem.

- Set your Time Zone
- Configure Security and Network Name
- Confirmation and Save

NOTE: The item “Configure Security and Network Name” will only be seen when login in with the advanced account.

- Set up your Time Zone, then press “Next”. (Not support Time Zone in Bridge Mode.)

**Setup Wizard**

**Set your Time Zone**

Update the fields below to change your time zone.

Time Zone	(UTC) Coordinated Universal Time
Primary NTP Server	clock.fmt.he.net
Secondary NTP Server	clock.nyc.he.net

- Set up your 2.4GHz Wi-Fi (advanced account only) parameters, such as SSID, Encryption, Password, etc.

**Setup Wizard**

**Configure Security and Network Name**

Update the fields below to change your Wi-Fi security settings.

▼ 2.4GHz Wi-Fi

Enable 2.4GHz Wi-Fi	<input checked="" type="checkbox"/>
Network Name(SSID)	Spot_0005
Hide SSID	<input type="checkbox"/>
Encryption	WPA2 PSK + AES
Password	•••••••• <input type="checkbox"/> display

- Check your settings again and then press “Save” button to apply the change. Please note, the Wi-Fi settings will only be seen when login in with the advanced account.

**Setup Wizard**

**Confirmation and Save**

Here is the summary of your settings. Confirm the settings and select 'Save'.

<b>Time</b>	
Time Zone	(UTC) Coordinated Universal Time
Primary NTP Server	clock.fmt.he.net
Secondary NTP Server	clock.nyc.he.net
<b>Wi-Fi</b>	
<b>2.4GHz Wi-Fi</b>	
Enable 2.4GHz Wi-Fi	Enable
Enable SSID	Enable
Network Name(SSID)	Spot_0005
Hide SSID	Disable
Encryption	WPA2 PSK + AES
Password	••••••••

## 4.2 Modem Setup

On this page, you can configure all the network related parameters.

### Modem Setup

Network Mode	5G/4G
Enable Auto Connection	<input checked="" type="checkbox"/>
Enable Roaming	<input type="checkbox"/>
Enable Data2 APN (Dedicated to second IP Passthrough)	<input type="checkbox"/>
Enable DM APN	<input type="checkbox"/>

#### ▼ Data APN

PDP Type	IPv4IPv6
APN Setting	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
APN	
Authentication	NONE
User Name	
Password	



Below are the definitions for each item:

Item	Description
<b>Network Mode</b>	Preference radio access technology.
<b>Enable Auto Connection</b>	<ul style="list-style-type: none"> <li>• Checked: Device will continuously try to connect network automatically.</li> <li>• Unchecked: You have to manually press the connect icon to re-connect to network every time if you failed to connect to network.</li> </ul>
<b>Enable Roaming</b>	Enable/Disable roaming to other network operator. <ul style="list-style-type: none"> <li>• Checked: Roaming to other network operator is enabled.</li> <li>• Unchecked: Roaming to other network operator is disabled.</li> </ul>
<b>Enable Data2 APN (Dedicated to second IP Passthrough)</b>	<ul style="list-style-type: none"> <li>• Checked: The second Data2 APN will be editable.</li> <li>• Unchecked: The second Data2 APN will be disappear and not editable.</li> </ul>
<b>Enable DM APN</b>	<ul style="list-style-type: none"> <li>• Checked: The second APN (DM APN) will be editable.</li> <li>• Unchecked: The second APN (DM APN) will be disappear and not editable.</li> </ul>
<b>PDP Type</b>	<ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> <li>• IPv4IPv6</li> </ul>
<b>APN Setting</b>	<ul style="list-style-type: none"> <li>• Auto: Device will automatically choose the default APN setting.</li> <li>• Manual: Manually enter the APN of your network, which your service provider gave you.</li> </ul>
<b>APN</b>	Enter the APN of your network, which your service provider gave you.
<b>Authentication</b>	<ul style="list-style-type: none"> <li>• None</li> <li>• PAP</li> <li>• CHAP</li> </ul>
<b>User Name</b>	Key-in the user name for the APN if there is any, this information should provide by your service provider.
<b>Password</b>	Key-in the password for the APN if there is any, this information should provide by your service provider.

### 4.3 Internet Setup

On this page, you can change the Web UI and device operation mode.

#### Internet Setup

Internet Mode	Dynamic IP
Set DNS Server Manually	<input type="checkbox"/>
MTU Size	1500 (576~1500)

Below are the definitions for each item:

Item	Description
<b>Internet Mode</b>	It displays the mode how to forward data packets between Internet and Intranet.
<b>Dynamic IP Mode</b>	<p>Device will get dynamic IP and related settings from ISP.</p> <ul style="list-style-type: none"> <li>Set DNS Server Manually: Use manually configured DNS server(s) for DNS query.</li> <li>Primary DNS Server: Primary DNS server for DNS query.</li> <li>Secondary DNS Server: Secondary DNS server for DNS query.</li> <li>MTU Size: Device's maximum transmission unit size of WAN interface (Range: 576-1500 bytes)</li> </ul>
<b>PPTP Mode</b>	<p>Device will establish tunnel in PPTP technique. Type.</p> <ul style="list-style-type: none"> <li>Default Gateway <ul style="list-style-type: none"> <li>VPN: VPN gateway of device.</li> <li>WAN: WAN gateway of device.</li> </ul> </li> <li>Connection Type <ul style="list-style-type: none"> <li>Dynamic IP <ul style="list-style-type: none"> <li>Set DNS Server Manually: Use manually configured DNS server(s) for DNS query.</li> <li>Primary DNS Server: Primary DNS server for DNS query.</li> <li>Secondary DNS Server: Secondary DNS server for DNS query.</li> </ul> </li> </ul> </li> <li>Server IP Address: PPTP server's IP address.</li> <li>Username: Username for tunnel authentication.</li> <li>Password: Password for tunnel authentication.</li> <li>MTU Size: Maximum transmission packet size on device's WAN interface (Unit: Byte).</li> </ul>

<p><b>L2TP Mode</b></p>	<p>Device will establish tunnel in L2TP tunnel mode technique.</p> <ul style="list-style-type: none"> <li>• NAT Support <ul style="list-style-type: none"> <li>• Enable: Enable to let the inner source IP to do the NAT.</li> <li>• Disable: Disable to let the inner source IP bypass the NAT.</li> </ul> </li> <li>• Default Gateway <ul style="list-style-type: none"> <li>• VPN: VPN gateway of device.</li> <li>• WAN: WAN gateway of device.</li> </ul> </li> <li>• Connection Type <ul style="list-style-type: none"> <li>• Dynamic IP <ul style="list-style-type: none"> <li>• Set DNS Server Manually: Use manually configured DNS server(s) for DNS query.</li> <li>• Primary DNS Server: Primary DNS server for DNS query.</li> <li>• Secondary DNS Server: Secondary DNS server for DNS query.</li> </ul> </li> </ul> </li> <li>• Server IP Address: PPTP server's IP address.</li> <li>• Username: Username for tunnel authentication.</li> <li>• Password: Password for tunnel authentication.</li> <li>• Host Name: If server requests the item, need to fill in.</li> <li>• Tunnel Password: VPN's tunnel password.</li> <li>• MTU Size: Enter the value for transmission unit size (Range: 576-1500).</li> </ul>
<p><b>GRE Mode</b></p>	<p>Device will establish tunnel in GRE tunnel mode technique.</p> <ul style="list-style-type: none"> <li>• GRE Type <ul style="list-style-type: none"> <li>• Layer2</li> <li>• Layer3 <ul style="list-style-type: none"> <li>• NAT Support <ul style="list-style-type: none"> <li>• Enable: Enable to let the inner source IP to do the NAT.</li> <li>• Disable: Disable to let the inner source IP bypass the NAT.</li> </ul> </li> <li>• Default Gateway <ul style="list-style-type: none"> <li>• VPN: VPN gateway of device.</li> <li>• WAN: WAN gateway of device.</li> </ul> </li> </ul> </li> </ul> </li> <li>• Connection Type <ul style="list-style-type: none"> <li>• Dynamic IP <ul style="list-style-type: none"> <li>• Set DNS Server Manually: Use manually configured DNS server(s) for DNS query.</li> <li>• Primary DNS Server: Primary DNS server for DNS query.</li> <li>• Secondary DNS Server: Secondary DNS server for DNS query.</li> </ul> </li> </ul> </li> <li>• Tunnel interface IP: Please input the VPN tunnel's IP address</li> <li>• Tunnel Interface Mask: Please input the VPN tunnel's IP subnet mask</li> <li>• Tunnel Destination IP: Please input VPN tunnel's Destination IP address.</li> <li>• MTU Size: Enter the value for transmission unit size (Range: 576-1500).</li> </ul>
<p><b>IPsec Mode</b></p>	<p>Device will establish tunnel in IPsec tunnel mode technique.</p> <ul style="list-style-type: none"> <li>• Connection Type <ul style="list-style-type: none"> <li>• Dynamic IP <ul style="list-style-type: none"> <li>• Set DNS Server Manually: Use manually configured DNS server(s) for DNS query.</li> <li>• Primary DNS Server: Primary DNS server for DNS query.</li> <li>• Secondary DNS Server: Secondary DNS server for DNS query.</li> </ul> </li> </ul> </li> <li>• Remote Tunnel IP: WAN IP address of remote IPsec tunnel end point.</li> <li>• Local Subnet: LAN host/subnet behind local IPsec end point.</li> <li>• Remote Subnet: LAN host/subnet behind local IPsec end point.</li> <li>• Pre-shared Key: This is used to authenticate remote IPsec end point.</li> <li>• MTU Size: Maximum transmission packet size on device's WAN interface (Unit: Byte).</li> </ul>
<p><b>IPv4 Passthrough</b></p>	<p>Device will forward WAN IP to the LAN host based on the selected IP Passthrough</p>

<b>Mode</b>	<p>Type.</p> <ul style="list-style-type: none"> <li>• IP Passthrough Type: You can select IP passthrough type of Auto/Manual             <ul style="list-style-type: none"> <li>• Auto: WAN IP will be assigned to the first IP-requesting host</li> <li>• Manual: WAN IP will be assigned to the host matching the specified MAC address.</li> </ul> </li> <li>• Enable second IP Passthrough: Check this item to enable the second IP Passthrough and call up the related setting item on the GUI.</li> <li>• IP Passthrough MAC Address: If the Second IP Passthrough function is disabled, set the MAC address that you want to get the WAN IP.</li> <li>• Data VLAN ID: The VLAN ID to map the Data APN. (When the Second IP Passthrough enabled.)</li> <li>• Data MAC Address: Define the MAC address you wish to obtain the WAN IP address from Data APN. (When the Second IP Passthrough function enabled.)</li> <li>• Data2 VLAN ID: The VLAN ID to map the Data2 APN. (When the Second IP Passthrough enabled.)</li> <li>• Data2 MAC Address: Define the MAC address you wish to obtain the WAN IP address from Data2 APN. (When the Second IP Passthrough enabled.)</li> <li>• MTU Size: Device's maximum transmission unit size of WAN interface (Range: 576-1500 bytes)</li> </ul>
-------------	---

## 4.4 LAN Setup

On this page, you can change the Web UI and device local IP address distribution range.

DHCP Service Type is Disabled

**LAN Setup**

LAN IP Address	192 . 168 . 15 . 1
Multicast Proxy	IGMPv2
DHCP Service Type	Disable

DHCP Service Type is Server

**LAN Setup**

LAN IP Address	192 . 168 . 15 . 1
Multicast Proxy	IGMPv2
DHCP Service Type	Server

**▼ DHCP Server**

DHCP Starting IP Address	192 . 168 . 15 . 2
DHCP Ending IP Address	192 . 168 . 15 . 254
DHCP Lease Time	1 hour(s) 0 minute(s) 0 second(s)
Enable DNS Proxy	<input checked="" type="checkbox"/>

**▼ DHCP Lease Reservation**  
The page did not have any data.

[Add](#)

**▼ DHCP Lease Status**

Icon	Host Name	MAC Address	IP Address	Remaining Lease Duration	Status
	20022921-NB01	00:ED:4A:30:80:01	192.168.15.17	3005 seconds	Active
	*	D4:5D:5E:6A:79:AE	192.168.15.100	929 seconds	Block

[Refresh](#)
[Auto](#)

## Add DHCP Reservation

**▼ DHCP Lease Reservation**

▼ Rule #1 ✕

<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>Host Name</b>	<input type="text"/>
<b>MAC Address</b>	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
<b>IP Address</b>	<input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 15 . <input type="text"/>

**Add**

**▼ DHCP Lease Status**

Icon	Host Name	MAC Address	IP Address	Remaining Lease Duration	Status
	20022921-NB01	00:E0:4A:3B:A9:31	192.168.15.17	3005 seconds	Active
	*	D4:5D:64:6A:79:AE	192.168.15.100	929 seconds	Block

**Refresh** **Auto**

Below are the definitions for each item:

Item	Description
<b>LAN IP Address</b>	Please input the LAN IP address here, the default value is 192.168.15.1
<b>Multicast Proxy</b>	<p>Multicast proxy is used to manage multicast group membership between device LAN and WAN.</p> <ul style="list-style-type: none"> <li>Disable</li> <li>IGMPv2</li> <li>IGMPv3</li> </ul>
<b>DHCP Service Type</b>	<p>Please select the DHCP service type, options are Disable, Server and Relay.</p> <ul style="list-style-type: none"> <li>Disable: The device will not assign LAN IP address to PC; you must manually set static IP address to the connected PC to access the UI.</li> <li>Server: The unit has a built-in DHCP server that can be used for managing the distribution of IP addresses for the devices connected to the local LAN port (Ethernet or Wi-Fi) and Web UI. In the DHCP Server page you set DHCP parameters for dynamic IP assignment.</li> </ul>

<p><b>DHCP Server</b></p>	<ul style="list-style-type: none"> <li>• DHCP Starting IP Address: Enter the first IP address assigned by the DHCP server.</li> <li>• DHCP Ending IP Address: Enter the last IP address assigned by the DHCP server.</li> <li>• DHCP Lease Time: Set the time, how long you want to renew the IP.</li> <li>• Enable DNS Proxy: Enable or disable DNS proxy. Default is enabled (check).             <ul style="list-style-type: none"> <li>• Check: DNS proxy is device's IP.</li> <li>• Uncheck: DNS proxy is from WAN's DNS information.                 <ul style="list-style-type: none"> <li>• From ISP                     <ul style="list-style-type: none"> <li>• Auto: DNS information is from ISP.</li> <li>• Manual: DNS information is manual.                         <ul style="list-style-type: none"> <li>• Primary DNS: Primary DNS information</li> <li>• Secondary DNS: Secondary DNS information</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>								
<p><b>DHCP Lease Reservation</b></p>	<p>The Lease Reservation page displays information on reserved IP addresses for leasing. In this page you assign the specific IP addresses to the specific client device connected to the Ethernet ports and Wi-Fi access point. You can also add, delete, or modify the reservation settings.</p> <ul style="list-style-type: none"> <li>• Add: Add the DHCP reservation item.</li> <li>• Enabled: Select if to enable or disable a specified IP setting.</li> <li>• Host Name: Enter a name to the host.</li> <li>• MAC Address: Add a device MAC address.</li> <li>• IP Address: Specify a reservation IP address for a specified MAC address.</li> </ul>								
<p><b>DHCP Lease Status</b></p>	<p>The Lease Status page displays information regarding the leased IP address(es):</p> <ul style="list-style-type: none"> <li>• Icon: The icon displays which device was connected.</li> </ul> <table border="1" data-bbox="467 989 1042 1134"> <tr> <td> Microsoft</td> <td> MacBook</td> <td> Android</td> <td> iPhone</td> </tr> <tr> <td> iPad</td> <td> TV</td> <td> Other</td> <td></td> </tr> </table> <ul style="list-style-type: none"> <li>• Host Name: This is display the connected PC name which connected to the device.</li> <li>• MAC Address: This is display the connected PC MAC address which connected to the device.</li> <li>• IP Address: This is display the IP address that assigned to this LAN device (Host PC).</li> <li>• Remaining Lease Duration: This display how many seconds remain for this assigned IP.</li> <li>• Status: This shows the current IP assignment availability.</li> </ul>	Microsoft	MacBook	Android	iPhone	iPad	TV	Other	
Microsoft	MacBook	Android	iPhone						
iPad	TV	Other							

## 4.5 IPv6 Setup

On this page, you can manage IPv6 settings on WAN/LAN

WAN Enabled, LAN Disabled

### IPv6 Setup

▼ WAN Setting

IPv6 Type	Autoconfiguration
DNS Server Source	<input checked="" type="radio"/> Auto <input type="radio"/> Manual

▼ LAN Setting

Autoconfiguration Type	Disable ▼
------------------------	-----------

WAN Enabled, LAN is SLAAC DHCPv6

### IPv6 Setup

▼ WAN Setting

IPv6 Type	Autoconfiguration
DNS Server Source	<input checked="" type="radio"/> Auto <input type="radio"/> Manual

▼ LAN Setting

Autoconfiguration Type	SLAAC DHCPv6 ▼
IPv6 SLAAC DHCPv6 RA Lifetime(seconds)	3600

WAN Enabled, LAN is SLACC RDNSS

### IPv6 Setup

▼ WAN Setting

IPv6 Type	Autoconfiguration
DNS Server Source	<input checked="" type="radio"/> Auto <input type="radio"/> Manual

▼ LAN Setting

Autoconfiguration Type	SLAAC RDNSS ▼
IPv6 SLAAC RDNSS RA Lifetime(seconds)	3600

WAN Enabled, LAN is Stateful DHCPv6

### IPv6 Setup

▼ WAN Setting

IPv6 Type	Autoconfiguration
DNS Server Source	<input checked="" type="radio"/> Auto <input type="radio"/> Manual

▼ LAN Setting

Autoconfiguration Type	Stateful DHCPv6 ▼
IPv6 Address Pool Start	2
IPv6 Address Pool End	200



Below are the definitions for each item:

WAN	
Item	Description
<b>IPv6 Type</b>	Auto configuration: The device will get IPv6 address automatically.
<b>DNS Server Source</b>	DNS Server Source: You can define the DNS as Auto or Manual. <ul style="list-style-type: none"> <li>• Primary DNS Server: Please input the IPv6 DNS server.</li> <li>• Secondary DNS Server: Please input the IPv6 DNS server if there is any.</li> </ul>
LAN Auto-configuration type: Disable, SLAAC DHCPv6, SLAAC RDNSS, Stateful DHCPv6	
Item	Description
<b>Disable</b>	Disable the IPv6 address assignment for LAN client.
<b>SLAAC DHCPv6</b>	(Stateless Address Auto-configuration DHCPv6), Router Advertisement (RA) will contain the IPv6 Prefix and default gateway information and DHCPv6 will provide DNS address and other network information. This method of LAN IP assignment will recommend to use at private area due to it is with lower security level. <ul style="list-style-type: none"> <li>• IPv6 SLAAC DHCPv6 RA Lifetime(seconds): The IP address will reset after X seconds, default is set as: 3600 sec</li> </ul>
<b>SLAAC RDNSS</b>	(Stateless Address Auto-configuration +Recursive DNS Server), Router Advertisement (RA) will regularly broadcast the multicast package and the Client will get Prefix, default gateway and DNS information, the Client will combine the Prefix and auto-generate the Host ID as the device's IPv6 address. <ul style="list-style-type: none"> <li>• IPv6 SLAAC RDNSS RA Lifetime(seconds): The IP address will reset after X seconds, default is set as: 3600 sec</li> </ul>
<b>Stateful DHCPv6</b>	RA only contain the default gateway information, the other information like IPv6 Prefix ,Host ID and DNS IP address is assigned by DHCPv6; DHCPv6 will record all the LAN IPv6 address, MAC list and regularly maintain the IPv6 address record. If you are in the public area, we will recommend using stateful DHCPv6. <ul style="list-style-type: none"> <li>• IPv6 Address Pool Start: Defined the IPv6 address start point, default is: 2</li> <li>• IPv6 Address Pool End: Defined the IPv6 address end point, default is: 200</li> </ul>

## 4.6 Diagnostics

This Diagnostics page will help you to perform a Ping or the Traceroute to troubleshoot the network connection.

### Ping

**Diagnostics**

<b>Diagnostic Tool</b>	<input checked="" type="radio"/> Ping <input type="radio"/> Traceroute
<b>IP Address/Domain Name</b>	<input type="text"/> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
<b>Ping Count</b>	<input type="text" value="4"/> (range: 1-50)
<b>Ping Packet Size</b>	<input type="text" value="64"/> (range: 4-1472 Bytes)

### Traceroute

**Diagnostics**

<b>Diagnostic Tool</b>	<input type="radio"/> Ping <input checked="" type="radio"/> Traceroute
<b>IP Address/Domain Name</b>	<input type="text"/> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
<b>TTL</b>	<input type="text" value="20"/> (range: 1-30)

Below are the definitions for each item:

Item	Description
<b>Diagnostic Tool (Ping)</b>	<ul style="list-style-type: none"> <li>IP Address/Domain Name: To issue a Test, please enter the destination IP address and Domain name here.</li> <li>IPv4: IPv4 format IP</li> <li>IPv6: IPv6 format IP</li> <li>Ping Count: Please fill how many times the test need to be performed (Range: 1-50).</li> <li>Ping Packet Size: Please fill how many buffer you want to add in a range of 4-1472 Bytes.</li> </ul>
<b>Diagnostic Tool (Traceroute)</b>	<ul style="list-style-type: none"> <li>IP Address/Domain Name: To issue a Test, please enter the destination IP address and Domain name here.</li> <li>IPv4: IPv4 format IP</li> <li>IPv6: IPv6 format IP</li> <li>TTL: Time To Live value; in the Traceroute test, please fill in a test value for the packet path time and check what is the path time that a packet takes to the specified host (Range: 1-30).</li> </ul>

Example	
Item	Description
<b>Diagnostic Tool (Ping)</b>	<p>If the CPE fails to access the Internet, run the ping command to preliminarily identify the problem. To do so:</p> <ol style="list-style-type: none"> <li>1. Choose Management &gt; Diagnostics. On the Diagnosis Tools, set to Ping. The Ping page is displayed.</li> <li>2. Enter the IP or domain name in the IP address/Domain Name field, for example, www.google.com.</li> <li>3. Set Ping Count and Ping Packet Size.</li> <li>4. Click Run</li> <li>5. Wait until the ping command is executed.</li> <li>6. The execution results are displayed in the box.</li> </ol>
<b>Diagnostic Tool (Traceroute)</b>	<p>If the CPE fails to access the Internet, run the traceroute command to preliminarily identify the problem. To do so:</p> <ol style="list-style-type: none"> <li>1. Choose Management &gt; Diagnostics. On the Diagnosis Tools, set to Traceroute. The Traceroute page is displayed.</li> <li>2. Enter the IP or domain name in the IP address/Domain Name field, for example, www.google.com.</li> <li>3. Set TTL</li> <li>4. Click Run</li> <li>5. Wait until the traceroute command is executed.</li> <li>6. The execution results are displayed in the box.</li> </ol>

## 4.7 System Log

The system log allows you can provide more detail information to your network provider. System log will not be recorded any individual privacy.

### System Log

Log Level Information
 Auto Scroll

```

Sep 7 07:35:33 CM HANDOVER: from <<ENDC,7,3250,46601,56365089,-95,-65,10,-11>> to <<ENDC,7,-1,46601,2147483647,-95,-65,-11,10>>
Sep 7 07:35:38 CM HANDOVER: from <<ENDC,7,-1,46601,2147483647,-95,-65,10,-11>> to <<ENDC,7,3250,46601,56365089,-94,-65,-10,10>>
Sep 7 07:39:06 CM HANDOVER: from <<ENDC,7,3250,46601,56365089,-96,-66,9,-10>> to <<ENDC,7,-1,46601,2147483647,-96,-66,-11,9>>
Sep 7 07:39:10 CM HANDOVER: from <<ENDC,7,-1,46601,2147483647,-96,-66,9,-11>> to <<ENDC,7,3250,46601,56365089,-93,-58,-10,9>>
Sep 7 07:40:21 CM HANDOVER: from <<ENDC,7,3250,46601,56365089,-93,-65,12,-10>> to <<ENDC,7,-1,46601,2147483647,-94,-63,-11,11>>
Sep 7 07:40:24 CM HANDOVER: from <<ENDC,7,-1,46601,2147483647,-94,-63,11,-11>> to <<ENDC,7,3250,46601,56365089,-92,-58,-11,11>>
Sep 7 07:47:00 dnsmasq-dhcp DHCPREQUEST(bridge0) 192.168.15.17 00:e0:4a:3b:a9:31
Sep 7 07:47:00 dnsmasq-dhcp Ignoring domain genteks.com for DHCP host name 20022921-NB01
Sep 7 07:47:00 dnsmasq-dhcp DHCPACK(bridge0) 192.168.15.17 00:e0:4a:3b:a9:31 20022921-NB01
Sep 7 08:02:39 CM HANDOVER: from <<ENDC,7,3250,46601,56365089,-94,-66,10,-10>> to <<ENDC,7,-1,46601,2147483647,-94,-66,-9,10>>
Sep 7 08:02:41 CM HANDOVER: from <<ENDC,7,-1,46601,2147483647,-94,-66,10,-9>> to <<ENDC,7,3250,46601,56365089,-92,-58,-11,11>>
Sep 7 08:14:47 dnsmasq-dhcp DHCPREQUEST(bridge0) 192.168.15.17 00:e0:4a:3b:a9:31
Sep 7 08:14:47 dnsmasq-dhcp Ignoring domain genteks.com for DHCP host name 20022921-NB01
Sep 7 08:14:47 dnsmasq-dhcp DHCPACK(bridge0) 192.168.15.17 00:e0:4a:3b:a9:31 20022921-NB01

```

Export

Below are the definitions for each item:

Item	Description
<b>Log level</b>	There are four levels pre-defined: Critical/Error/Warning/Information, Please see below table.
<b>Auto Scroll</b>	Automatic scrolling of the latest content.
<b>Export</b>	You can export your syslog out for the further analysis or issue tracking; the export format will be the .txt file with .tar compress.

System Log	
Item	Description
<b>Information</b>	<ul style="list-style-type: none"> <li>• System</li> <li>• Start/Reboot/Reset</li> <li>• Connection Manager</li> <li>• WAN Connection</li> <li>• WAN IP obtained</li> <li>• FOTA</li> <li>• Started/Stopped</li> <li>• Periodic Firmware check/upgrade result</li> <li>• Start download firmware</li> <li>• Start upgrade firmware</li> </ul>
<b>Warning</b>	<ul style="list-style-type: none"> <li>• Connection Manager</li> <li>• SIM card is not inserted</li> <li>• Verify PIN failed</li> <li>• FOTA</li> <li>• Failed to connect to server</li> <li>• Failed to download Packages or firmware</li> </ul>
<b>Error</b>	<ul style="list-style-type: none"> <li>• FOTA</li> <li>• Failed to upgrade firmware</li> <li>• Failed to verify firmware</li> </ul>
<b>Critical</b>	<ul style="list-style-type: none"> <li>• Critical Error</li> </ul>

NOTE: UNABLE to export System Log on IE8 browser

## 4.8 QoS

On this page, you can use QoS.

**QoS**

<b>Selection</b> <input type="text" value="20022921-NB01"/>	<b>MAC Address</b> <input type="text" value="00:EO:AA:30:AA:33"/>	<b>Limitation (Mbps)</b> Downlink <input type="text" value="10"/> Uplink <input type="text" value="10"/>
--	--	---

**Add**

▼ Rule #1 ✕

<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>MAC Address</b>	<input type="text" value="00:EO:AA:30:AA:33"/>
<b>Downlink (Mbps)</b>	<input type="text" value="10"/>
<b>Uplink (Mbps)</b>	<input type="text" value="10"/>

Below are the definitions for each item:

Item	Description
<b>QoS</b>	<ul style="list-style-type: none"> <li>Selection: Select to manually modify the MAC address or select the target end user.</li> <li>MAC Address: Enter the target MAC address to be bandwidth-limited.</li> <li>Limitation (Mbps)               <ul style="list-style-type: none"> <li>Downlink: Enter the downlink limit (Mbits per second) of the target MAC address.</li> <li>Uplink: Enter the uplink limit (Mbits per second) of the target MAC address.</li> </ul> </li> <li>Add: Add QoS items.</li> <li>Enabled: Select this checkbox to enable/disable downlink/uplink limit of the specific MAC address.</li> <li>MAC Address: Display the bandwidth-limited MAC address.</li> <li>Enter the MAC address to change the bandwidth-limited target.</li> <li>Downlink (Mbps): Enter the downlink limit (Mbits per second) of the end user.</li> <li>Uplink (Mbps): Enter the uplink limit (Mbits per second) of the end user.</li> </ul>

## 5 Personalization

### 5.1 PIN Management

On this page, you can secure a device with PIN (Personal Identification Number) and PUK (Personal Identification Number Unlock Key).

**PIN Management**

USIM Status USIM ready

▼ **USIM's PIN Management**

PIN Remain 3

PIN Protection  Enable  Disable

PIN Code (4~8 digits)

Below are the definitions for each item:

Item	Description
<b>USIM Status</b>	<p>This column will show current SIM card's status, detail definition as below:</p> <ul style="list-style-type: none"> <li>USIM not inserted: Your SIM card is not insert or SIM Card not able to be detected properly.</li> <li>USIM Ready: SIM card insert properly and is detected.</li> <li>Wait PIN /PUK code: SIM card is protected by PIN or PUK code, please go "USIM's PIN/PUK Verification" verify the code.</li> <li>Other Reason: Your SIM card can't use, please check your SIM card/Network provider.</li> </ul>
<b>USIM's PIN/PUK Verification</b>	<p>Only when your SIM card is locked by PIN/PUK code, the column wills become activate. Please fill your PIN code here then press "Verify" button. PIN code should be 4~8 digits number. If PIN retries error over 3 times, SIM card will be blocked and PUK code will be required to unblock the SIM card. Normally, PUK code should be 8 digits number. After PUK code is filled, press "Verify" to begin PUK verification.</p>
<b>USIM's PIN Management</b>	<p>If you select "Enable", device will activate SIM PIN Code Lock function which will request you to fill-in the PIN code while every time device boot up. Please enter your PIN code (4~8 digits number) then press "Apply" button to confirm the PIN code lock.</p> <p>If you select "Disable", device would disable the PIN code lock function, please press"Apply" button to confirm the change.</p>

NOTE: If you are in the first time use, please check Network Provider to get your PIN/PUK code details.

## 5.2 Configuration

On this page, you can restore a device to factory settings and export/import a device's configurations.

**Configuration**

▼ Restore Factory Settings [Restore Factory Settings](#)

▼ Export/Import Configuration File

Export/Import Password

[Export Configuration File](#)

[Browse](#) [Import Configuration File](#)

Below are the definitions for each item:

Item	Description
<b>Restore Factory Settings</b>	<p>You can use Reset Factory Settings function to set device to factory default settings. When returning to factory defaults, it will reset all the parameters/settings you had ever done. All the changes different from factory default settings will be lost; you will need to manually change the parameter again.</p> <ul style="list-style-type: none"> <li>Restore Factory Settings: To restore settings to factory defaults, click the Restore Factory Settings button. After applying factory defaults, device will reboot.</li> </ul>
<b>Export/Import Configuration File</b>	<ul style="list-style-type: none"> <li>Export/Import Password: Export/Import Password is used to protect the same configuration file for both Export and Import operations.</li> <li>Export Configuration File: You could export all of user settings in this device to a file.</li> <li>Import Configuration File: You could browse a configuration file and import it back.</li> </ul>

NOTE: UNABLE to export Configuration file on IE8 browser

### 5.3 Device Setup

On this page, you can manage a device's Web login password and system time.

#### Device Setup

Your password has not been changed. To protect your account, please change the default password as soon as possible. Click [here](#) if you no longer wish to receive these reminders.

**▼ Password**

Old Login Password	<input type="text"/>
New Login Password	<input type="text"/> (length: 1-128 characters)
New Login Password Confirm	<input type="text"/>

**▼ Device Time**

Enable NTP	<input checked="" type="checkbox"/>
Current Time	Sep 07 2023 08:32
Primary NTP Server	<input type="text" value="clock.fmt.he.net"/>
Secondary NTP Server	<input type="text" value="clock.nyc.he.net"/>
Time Zone	<input type="text" value="(UTC) Coordinated Universal Time"/>

Below are the definitions for each item:

Item	Description
<b>Password</b>	<p>You can change the default Graphical User Interface (GUI) access password here.</p> <ul style="list-style-type: none"> <li>Old Login Password: Input the original /current login password.</li> <li>New Login Password: Enter a new log-in password you want to change.</li> <li>New Login Password Confirm: Enter the new password again for verification.</li> </ul>
<b>Device Time</b>	<p>The modem uses the Simple Network Time Protocol (SNTP) to set its internal clock based on periodic updates from a time server. Maintaining an accurate time on the device will keep the system log to recording meaningful dates and times for event entries. The Device Time area displays the following information:</p> <ul style="list-style-type: none"> <li>Enable NTP: Allow device to synchronize system time with configured time server(s).</li> <li>Current Time: Displays the current time of the system clock.</li> <li>Primary NTP Server: The primary time server for device to synchronize system time.</li> <li>Secondary NTP Server: You can set the secondary NTP server in case of the Primary NTP server didn't work in some time.</li> <li>Time Zone: SNTP uses Greenwich Mean Time, or GMT (also known as Universal Time Coordinated, or UTC) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, select your time zone from the pull-down list.</li> </ul>

**NOTE:** We recommend you to change the default Login password while the first time log-in. If you don't fill any key in the Password field, it means that you don't modify



## 5.4 Software

Keep device update to latest firmware.

### Upgrade From File

**Software**

Device Software Source Upgrade From File v

Device Software Version : 01.00.02.1070 (09/07/2023)

Device Software Path  Browse Install Software

Software Name	Version	Action
---------------	---------	--------

Below are the definitions for each item:

Item	Description
<b>Upgrade From File</b>	<ul style="list-style-type: none"> <li>Step 1: Click Browse button to select the IPK file.</li> <li>Step 2: Click Install Software button to install the selected IPK file</li> </ul>
<b>Upgrade From FOTA</b>	<ul style="list-style-type: none"> <li>This option will appear only when the Engineering <span style="font-size: 0.8em;">□</span> DM Settings <span style="font-size: 0.8em;">□</span> FOTA is configured. Under this mode, the device will upgrade according to the instructions from the FOTA configuration. Please note, only the advanced account can access the Engineering Setting pages.</li> </ul>

NOTE: While firmware upgrade is in progress, please don't remove the power from device.

## 5.5 SMS Management

This feature is for SMS.

### SMS Management

**▼ Send Message**

**Phone Number**

**Message**

**▼ Inbox**

Newest ▼

	Date/Time	Phone Number	Message	Delete
	2023-09-07 16:42	09591100000	Test 002	<input style="background-color: #0070C0; color: white; padding: 2px 5px; border: none;" type="button" value="Del"/>

Below are the definitions for each item:

Item	Description
<b>Send Messages</b>	<p>You can send messages of up to 1000 alpha-numeric characters or 2000 non-Latin characters (The Chinese, Arabic, Thai, Cyrillic alphabets) to mobile handsets.</p> <ul style="list-style-type: none"> <li>Phone Number: Enter the phone number of the receiver.</li> <li>Message: Type a message of up to 1000 alpha-numeric characters or 2000 non-Latin characters in the message box and then click Send.</li> <li>Send: After writing message completely, please click Send bottom to send the message.</li> </ul>
<b>Inbox</b>	<p>The all received short messages are shown in the Inbox.</p> <ul style="list-style-type: none"> <li>Receive: You can click Receive button to check if new message is coming.</li> <li>Date/Time: The timestamp that message is sent.</li> <li>Phone Number: The sender's phone number.</li> <li>Message: The received message brief and you can click the button to check the whole message content.</li> <li>Newest: When working in an SMS message list, the default settings is to start at the newest SMS first.</li> <li>Oldest: You can do this by selecting 'Oldest' and then the messages are arranged in descending order from oldest to newest.</li> <li>Del: Click the delete button to delete the message.</li> </ul>

## 5.6 LED Management

This feature is for turning on/off the LEDs on the ODU.

### LED Management

Turn off all LEDs

Below are the definitions for each item:

Item	Description
<b>Turn off all LEDs</b>	<ul style="list-style-type: none"><li>• This feature is for turning on/off the LEDs on the ODU.</li><li>• Checked: To turn off all LEDs</li><li>• Unchecked: To turn on all LEDs.</li></ul>

## 6 Basic

### 6.1 Firewall

The modem provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks.

**Firewall**

<b>Current Firewall Level</b>	Medium (standard)
<b>Firewall Level</b>	Medium (standard) <span style="float: right;">▼</span>
	Stateful Packet Inspection (SPI) is enabled. Inbound (from Internet to LAN) policy: Dropped. Remote authorized access will override the inbound policy. Outbound (from LAN to Internet) policy: Accepted.
<b>Filtering Strategy</b>	The filtering rules you set will take precedence over the default inbound and outbound policies.
<b>MAC Filtering</b>	Disable/Blacklist/Whitelist
<b>IP Filtering</b>	Disable/Blacklist/Whitelist
<b>Prevent DoS Attack</b>	<input type="checkbox"/>
<b>Block Anonymous Internet Requests</b>	<input checked="" type="checkbox"/>
<b>Filter Multicast</b>	<input type="checkbox"/>
<b>Enable Remote Web Management</b>	<input type="checkbox"/> Port <input style="width: 50px;" type="text" value="8080"/>

Below are the definitions for each item:

Item	Description
<b>Current Firewall Level</b>	Shows the current device firewall level.
<b>Firewall Level</b>	Allows user to change the device firewall level here, there are four options pre-defined: <ul style="list-style-type: none"> <li>Low (filtering disabled)</li> <li>Medium (standard)</li> <li>High</li> </ul>
<b>Filtering Strategy</b>	The filtering rules you set will take precedence over the default inbound and outbound policies.
<b>MAC Filtering</b>	Block or allow the client device's internet access via MAC address, you can go Advanced > MAC Filtering to edit whitelist and blacklist.
<b>IP Filtering</b>	Block or allow the client device's internet access via IP address, you can go Advanced > IP Filtering to edit whitelist and blacklist.
<b>URL Filtering</b>	Advanced > IP Filtering to edit whitelist and blacklist.
<b>Prevent DoS Attack</b>	Block or allow the client device's internet access via URL (web address), you can go Advanced > URL Filtering to edit whitelist and blacklist.
<b>Block Anonymous Internet Requests</b>	Select this checkbox to reject anonymous Internet requests.

<b>Filter Multicast</b>	Select this checkbox to filter out multicast packets.
<b>Enable Remote Web Management</b>	Select this checkbox will accept to login from internet.

## 6.2 DMZ

For applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

**DMZ**

<b>Enable DMZ</b>	<input checked="" type="checkbox"/>
<b>DMZ IP Address</b>	192.168.15. <input style="width: 50px;" type="text"/>

Below are the definitions for each item:

Item	Description
<b>Enable DMZ</b>	Select this checkbox to enable or disable DMZ.
<b>DMZ IP Address</b>	Set client/server that acts as a "neutral zone" (DMZ stands for "Demilitarized Zone") and separates an internal network from a public one in order to prevent outside access to private data. The DMZ forwards the network traffic to specific hosts based on the protocol and port number.

## 6.3 UPnP

UPnP is a protocol that simplifies device connection and network implementation. When this option is enabled, certain Windows applications would setup the port forwarding rule dynamically.

**UPnP**

<b>Enable UPnP</b>	<input type="checkbox"/>
--------------------	--------------------------

Below are the definitions for each item:

Item	Description
<b>Enable UPnP</b>	Enable UPnP IGD - Select this checkbox to enable/disable Universal Plug and Play Internet Gateway Device.

## 6.4 Dynamic DNS

Dynamic Domain Name System (DNS) is a mechanism used for translating host names for network nodes into IP addresses in real-time. This page allows enabling the Dynamic DNS and selecting the service provider.

Service Provider is dyndns/noip/duckdns/Changelp

### Dynamic DNS

<b>Enable DDNS</b>	<input checked="" type="checkbox"/>
<b>Service Provider</b>	<div style="border: 1px solid #ccc; padding: 2px;">             dyndns ▾             <ul style="list-style-type: none"> <li>dyndns <input style="width: 100px;" type="text"/></li> <li>noip <input style="width: 100px;" type="text"/></li> <li>duckdns <input style="width: 100px;" type="text"/></li> <li>ChangeIp <input style="width: 100px;" type="text"/></li> </ul> </div>
<b>Username</b>	<input style="width: 100%;" type="text"/>
<b>Password</b>	<input style="width: 100%;" type="text"/>
<b>Domain Name</b>	<input style="width: 100%;" type="text"/>

Below are the definitions for each item:

Item	Description
<b>Enable DDNS</b>	Select this checkbox if the unit has a non-static IP address to keep the domain name associated with an ever-changing IP address. When DDNS is enabled, configure the following parameters: <ul style="list-style-type: none"> <li>Username</li> <li>Password</li> <li>Token</li> <li>Domain Name</li> </ul>
<b>Service Provider</b>	Select the DDNS service provider from the drop-down list.

## 6.5 VPN Passthrough

A VPN passthrough is a feature that allows any clients connected to the router to establish VPN connections.

### VPN Passthrough

<b>Enable IPSec Passthrough</b>	<input checked="" type="checkbox"/>
<b>Enable PPTP Passthrough</b>	<input checked="" type="checkbox"/>
<b>Enable L2TP Passthrough</b>	<input checked="" type="checkbox"/>

Below are the definitions for each item:

Item	Description
<b>Enable IPSec Passthrough</b>	Internet Protocol Security; IPSec provides encrypted security services at the IP layer, and enables to use encrypted tunnels/traffic between two hosts.
<b>Enable PPTP Passthrough</b>	Point to Point Tunneling Protocol; This protocol enables the transfer of data packets of TCP / IP through a foreign network that is not based on these protocols (by marking the packet with an address suited to the foreign network).
<b>Enable L2TP Passthrough</b>	Layer 2 Tunneling Protocol; An open standard with multivendor interoperability and acceptance.

## 7 Advanced

### 7.1 MAC Filtering

You can block access to the Internet from clients on the local network by MAC addresses. In the MAC Filter page you set MAC addresses to be filtered out by the security system.

#### MAC Filtering

**MAC Filtering Mode** 
 Disable
  Blacklist
  Whitelist

▼ Rule #1 ✕

**Enabled**

**MAC Address**

Add
Undo
Apply

Below are the definitions for each item:

Item	Description
<b>MAC Filtering Mode</b>	Select MAC filtering by Disable, Whitelist or Blacklist <ul style="list-style-type: none"> <li>• Disable: Disable filtering function.</li> <li>• Blacklist: Block internet access which listed on the blacklist.</li> <li>• Whitelist: Will only allow the units listed on the list to access the network.</li> </ul>
<b>Add</b>	Add MAC Filtering rule(s).
<b>Enabled</b>	Select this checkbox to enable/disable filter for the specific client device's MAC address.
<b>MAC Address</b>	Please key-in the client device which you want to do the MAC filtering MAC address.

## 7.2 IP Filtering

You can block access to the Internet from clients on the local network by specifying IP addresses. You can add addresses to the filtered group or delete/disable them.

**IP Filtering**

**IP Filtering Mode** 
 Disable
  Blacklist
  Whitelist

---

▼ Rule #1 ✕

**Enabled**

**IP Version** IPv4 ▼

**IP Address** 192.168.15.  ~

Add
Undo
Apply

Below are the definitions for each item:

Item	Description
<b>IP Filtering Mode</b>	Select IP filtering by Disable, Whitelist or Blacklist <ul style="list-style-type: none"> <li>• Disable: Disable filtering function.</li> <li>• Blacklist: Block internet access which listed on the blacklist.</li> <li>• Whitelist: Will only allow the units listed on the list to access the network.</li> </ul>
<b>Add</b>	Add IP Filtering rule(s).
<b>Enabled</b>	Select this checkbox to enable or disable filtering for the specific table entry.
<b>IP Version</b>	Select IP Version 4/6 address.
<b>IP Address</b>	Specify an IPv4 address range or an IPv6 address on the local network.



## 7.3 Port Forwarding

Port Forwarding instructs the router to which computer on the local area network to send data. According to the port forwarding rules or setup, the router sends the data from the external IP address: port number to an internal IP address: port number

### Port Forwarding

v Rule #1 ✕

<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>Application Name</b>	<input type="text"/>
<b>Protocol</b>	TCP ▾
<b>WAN Port</b>	<input type="text"/> ~ <input type="text"/>
<b>LAN Port</b>	<input type="text"/>
<b>LAN IP</b>	192.168.15. <input type="text"/>

Add

Undo

Apply

Below are the definitions for each item:

Item	Description
<b>Add</b>	Add Port Forwarding rule(s).
<b>Enabled</b>	Select this checkbox to enable/disable port forwarding for the specific IP.
<b>Application Name</b>	Enter a name for identifying this port forwarding protocol.
<b>Protocol</b>	Set the protocol for port forwarding: TCP, UDP or Both.
<b>WAN Port</b>	Enter the port number for WAN side.
<b>LAN Port</b>	Enter the port number for LAN side.
<b>LAN IP</b>	Enter the IP address that identifies the IP subnet of the remote network.

## 7.4 Port Triggering

Port triggering is a way to automate port forwarding: outbound traffic on predefined ports ('triggering ports') causes inbound traffic to specific incoming ports to be dynamically forwarded to the initiating host, while the outbound ports are in use.

### Port Triggering

▼ Rule #1
✕

<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>Application Name</b>	<input type="text"/>
<b>Protocol</b>	TCP ▼
<b>Triggered Range</b>	<input type="text"/> ~ <input type="text"/>
<b>Forwarded Range</b>	<input type="text"/> ~ <input type="text"/>

Add
Undo
Apply

Below are the definitions for each item:

Item	Description
<b>Add</b>	Add Port Triggering rule(s).
<b>Enabled</b>	Select this checkbox to enable/disable port triggering for the specific application.
<b>Application Name</b>	Enter a name for identifying this port triggering protocol.
<b>Protocol</b>	Set the protocol for port triggering: TCP, UDP or BOTH.
<b>Triggered Range</b>	Enter the trigger range (1024~65535).
<b>Forwarded Range</b>	Enter the forwarded range. Some forwarded port is reserved. Reserved port list: <ul style="list-style-type: none"> <li>• TCP: 80, 111, 443, 2049, 8080, 25001, 32777, 32778, 32780, 50003</li> <li>• UDP: 111, 1900, 2049, 32777, 32778, 32780</li> </ul>

## 7.5 Parental Control

On this page, you can manage internet access based on a scheduled plan.

### Parental Control

Name	Selection	MAC Address	Block Time	Block Traffic
<input type="text" value="Test01"/>	<input type="text" value="*"/>	<input type="text" value="00:EO:00:00:00:01"/>	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>

v Rule #1 - Test01 x

<b>Enabled</b>	<input checked="" type="checkbox"/>
<b>Name</b>	<input type="text" value="Test01"/>
<b>MAC Address</b>	<input type="text" value="00:EO:00:00:00:01"/>
<b>Block Time</b>	<input type="button" value="Edit"/>
<b>Block Traffic</b>	<input type="button" value="Edit"/>

Below are the definitions for each item:

Operation Area	
Item	Description
<b>Name</b>	Enter a name for identifying this parental control rule.
<b>Selection</b>	Choose the client device you would like to control from a drop-down list or key in the desired MAC address manually from the MAC Address column.
<b>Mac Address</b>	MAC address of the client device you would like to control.
<b>Block Time</b>	Choose time to control the out-going traffic.
<b>Block Traffic</b>	Choose the type to control all out-going traffic or url filter which user defined.
<b>Add</b>	Add Parental Control rule(s).

Below are the definitions for each item:

Rule List	
Item	Description
<b>Enabled</b>	Select this checkbox to enable/disable for parental control rule.
<b>Name</b>	The name for identifying this parental control rule.
<b>Mac Address</b>	MAC address of the client device you would like to control.
<b>Block Time</b>	Choose time to control the out-going traffic.
<b>Block Traffic</b>	Choose the type to control all out-going traffic or url filter which user defined.

## 7.6 Static Routing

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic.

### Static Routing

▼ Rule #1
⊗

<b>Destination IP Address</b>	<input style="width: 100%;" type="text"/>
<b>Subnet Mask</b>	<input style="width: 100%;" type="text"/>
<b>Gateway</b>	<input style="width: 100%;" type="text"/>
<b>Interface</b>	<input style="width: 100%;" type="text" value="WAN"/>

Add
Undo
Apply

Below are the definitions for each item:

Item	Description
<b>Add</b>	Add Static Route item(s).
<b>Destination IP Address</b>	Please fill-in the destination IP address for the route.
<b>Subnet Mask</b>	Please fill-in the subnet mask of the destination IP network.
<b>Gateway</b>	Please fill-in Gateway IP of the destination IP network. (Only for LAN)
<b>Interface</b>	The gateway may be a router or switch on the same network segment as the device's LAN/WAN interface. Please indicate the interface for setting the route rule.

## 8 Wi-Fi

NOTE: The Wi-Fi page will only appear when logging in to the Web GUI with the advanced account.

### 8.1 Basic

This page is for the advanced account user to set the basic Wi-Fi parameters.

**Basic**

▼ 2.4GHz Wi-Fi

Enable 2.4GHz Wi-Fi

Network Name(SSID)

Hide SSID

Encryption

Password   display

Below are the definitions for each item:

Item	Description
<b>Enable 2.4GHz Wi-Fi</b>	To enable or disable the Wi-Fi function.
<b>Network Name(SSID)</b>	To modify the desired SSID.
<b>Hide SSID</b>	Check to hide the SSID.
<b>Encryption</b>	To choose the encryption method, the options are <ul style="list-style-type: none"> <li>• None</li> <li>• WPA2 PSK + AES</li> <li>• WPA-WPA2-MIXED PSK + TKIP/AES</li> </ul>
<b>Password</b>	Set the Wi-Fi password.
<b>Password - Display</b>	Display the password in plain text.

## 8.2 Advanced

The advanced account user can configure the Wi-Fi radio property via this page.

**Advanced**

▼ 2.4GHz Wi-Fi

<b>Working Mode</b>	802.11b/g/n ▼
<b>Bandwidth</b>	20MHz/40MHz auto ▼
<b>Radio Channel</b>	Auto ▼
<b>Power Level</b>	High ▼

<b>Maximum Connection Number</b>	<input style="width: 100%;" type="text" value="4"/>
----------------------------------	---

Below are the definitions for each item:

Item	Description
<b>Working Mode</b>	To select the Wi-Fi radio mode, the options are <ul style="list-style-type: none"> <li>802.11b</li> <li>802.11b/g</li> <li>802.11b/g/n</li> </ul>
<b>Bandwidth</b>	To choose the Wi-Fi radio bandwidth, the options are <ul style="list-style-type: none"> <li>20MHz</li> <li>0MHz/40MHz auto</li> </ul>
<b>Radio Channel</b>	Choose the Wi-Fi radio channel, the options are <ul style="list-style-type: none"> <li>Auto</li> <li>1 ~11</li> </ul>
<b>Power Level</b>	Select the output power level of the Wi-Fi radio. This can be set as Low, Middle, or High.
<b>Maximum Connection Number</b>	Set the maximum Wi-Fi connection client.

## 9 Engineering

NOTE: Engineering page will only appear when logging in to the Web GUI with the advanced account.

### 9.1 Band Selection Settings

This page is for engineers to set the radio band that he wants the CPE to scanning in the 4G/5G searching mode. Moreover, he can also force the CPE to connect specified Cells on this page.

#### Band Selection Settings

Locking Mode
Manual ▼

LTE Band

2	4	5	12	13	14	25	26	41	46	48	66	71
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

NR Band

2	5	41	66	71	77
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

▼ Lock Cell for LTE PCC

▼ Rule #1 ✕

DL Earfcn

PCI

Add

▼ Lock Cell for NR PCC

Band

▼

SCS

▼

SSB Arfcn

PCI

Undo
Apply

Below are the definitions for each item:

Item	Description
<b>Locking Mode</b>	<ul style="list-style-type: none"> <li>• <b>Disable:</b> Disable the band locking and the CPE will try to connect to the 4G/5G radio automatically.</li> <li>• <b>Manual:</b> When set to manual, the user can choose the radio bands that he wants the CPE to scan when searching the 4G/5G radio. Or force the CPE to connect to specified 4G/5G Cells.</li> </ul>
<b>LTE Band</b>	<p>The list of the LTE (4G) bands supported by the CPE. When setting the locking mode to Manual, the user can select the radio bands that he wants the CPE to scan by the check box below the band ID.</p>
<b>NR Band</b>	<p>The list of the NR (5G) bands supported by the CPE. When setting the locking mode to Manual, the user can select the radio bands that he wants the CPE to scan by the check box below the band ID.</p>
<b>Lock Cell for LTE PCC</b>	<ul style="list-style-type: none"> <li>• <b>Add:</b> Add the items of the LTE lock cell.</li> <li>• <b>DL Earfcn:</b> Set the Downlink Earfcn of the desired Cell.</li> <li>• <b>PCI:</b> Set the Physical Cell Identifier of the desired Cell.</li> </ul>
<b>Lock Cell for NR PCC</b>	<ul style="list-style-type: none"> <li>• <b>Band:</b> Set the NR Band of the desired Cell.</li> <li>• <b>SCS:</b> The sub-carrier space.</li> <li>• <b>SSB Arfcn:</b> Set the Synchronization Signal Block Absolute Radio Frequency Channel Number.</li> <li>• <b>PCI:</b> Set the Physical Cell Identifier of the desired Cell.</li> </ul>



## 9.2 DM Settings

Engineers can set the parameters for TR-069, SNMP, and FOTA on this page.

### DM Settings

**▼ DM switch**

Supporting DM	<input checked="" type="checkbox"/> TR069 <input type="checkbox"/> SNMP <input type="checkbox"/> FOTA
DM WAN IP	N/A

**▼ TR069**

Connection Status	dis-connected
ACS URL	<input type="text"/>
ACS UserName	<input type="text"/>
ACS UserPassword	<input type="text"/>
Periodic Inform	Enable <input type="button" value="v"/>
Periodic Inform Interval	<input type="text" value="3600"/> seconds
Connection Request User Name	<input type="text"/>
Connection Request Password	<input type="text"/>

**▼ SNMP**

SNMP Version	SNMPv3 <input type="button" value="v"/>
USM User	<input type="text" value="gemtek"/>
Security Level	auth, priv <input type="button" value="v"/>
Auth Algorithm	SHA <input type="button" value="v"/>
Auth Password	<input type="text"/>
Privacy Algorithm	AES <input type="button" value="v"/>
Privacy Password	<input type="text"/>
SNMP Trap	Disable <input type="button" value="v"/>
Contact	<input type="text"/>
System Name	<input type="text"/>
Location	<input type="text"/>

**▼ FOTA**

Packages URL	<input type="text"/>
Server Username	<input type="text"/>
Server Password	<input type="text"/>
Upgrade Type	Periodic <input type="button" value="v"/>
Periodically Check Interval	<input type="text" value="86400"/> seconds

Item	Description
<b>DM Switch</b>	<ul style="list-style-type: none"> <li>Support DM: Check the checkboxes for enabling/disabling the device management protocols below.               <ul style="list-style-type: none"> <li>TR-069</li> <li>SNMP</li> <li>FOTA</li> </ul> </li> <li>DM WAN IP: The WAN IP of the CPE will show in this column.</li> </ul>
<b>TR-069</b>	<ul style="list-style-type: none"> <li>Connection Status: Shows the connection status to the ACS server.</li> <li>ACS URL: Set the URL of the ACS server.</li> <li>ACS Username: Set the ACS username for registering the ACS server.</li> <li>ACS UserPassword: Set the ACS user password for registering the ACS server.</li> <li>Periodic Inform: Choose to enable or disable the ACS periodic information.</li> <li>Periodic Inform Interval: Set the seconds of the time interval for the ACS periodic information.</li> <li>Connection Request User Name: Set the Connection Request User Name if needed.</li> <li>Connection Request Password: Set the password of the Connection Request User Name if needed.</li> </ul>
<b>SNMP</b>	<ul style="list-style-type: none"> <li>SNMP Version: Choose the SNMP version.</li> <li>SNMP Read-Only Community: Set the community string with read-only privilege for SNMPv1 and SNMPv2.</li> <li>SNMP Read-Write Community: Set the community string with read-write privilege for SNMPv1 and SNMPv2.</li> <li>USM User: Set the USM user name for SNMPv3.</li> <li>Security Level: Choose the security level for SNMPv3.               <ul style="list-style-type: none"> <li>No auth, no priv</li> <li>auth, no priv</li> <li>auth, priv</li> </ul> </li> <li>Auth Algorithm: Choose the authentication algorithm for SNMPv3               <ul style="list-style-type: none"> <li>SHA</li> <li>MD5</li> </ul> </li> <li>Auth Password: Set the password for the Authentication</li> <li>Privacy Algorithm: Select the encryption algorithm for Privacy.</li> <li>Privacy Password: Set the password for Privacy.</li> <li>SNMP Trap: Enable or disable the SNMP trap.</li> <li>SNMP Trap Community: Set the community string for the SNMP trap connection.</li> <li>SNMP Trap Server Address: Set the IP address of the SNMP trap server.</li> <li>SNMP Trap Server Port: Set the port used by the SNMP trap server.</li> <li>Contact: Set the contact person here.</li> <li>System Name: Set the system name.</li> <li>Location: Set the location of contact person.</li> </ul>
<b>FOTA</b>	<ul style="list-style-type: none"> <li>Packages URL: Set the packages URL of the package files.</li> <li>Server Username: Set the username if required by the server.</li> <li>Server Password: Set the password if required by the server.</li> <li>Upgrade Type: Choose whether you want the CPE to check for an upgrade by a time interval, daily schedule, or both methods.</li> <li>Periodically Check Interval: Set the time interval for the CPE to check for an upgrade.</li> <li>Daily Check Time (Hour): Set the scheduled hour for the CPE to check for an upgrade.</li> </ul>

### 9.3 QXDM

Engineers can gather the QXDM log via the function on this page.

**QXDM**

QXDM over FTP	<input checked="" type="checkbox"/>
FTP Server IP	192.168.15. <input type="text"/>

Item	Description
<b>QXDM over FTP</b>	Enable or disable the QXDM log capture function.
<b>FTP Server IP</b>	Specify the IP address of the LAN host that will receive the QXDM log via FTP service.

NOTE: Engineering page will only appear when logging in to the Web GUI with the advanced account.