

Welcome to the LTE CPE!

LTE CPE Online Help

Issue	01
Date	2012-09-22

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://www.huawei.com>

Email: mobile@huawei.com

Copyright © Huawei Technologies Co., Ltd. 2013. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Getting Started.....	6
1.1 Welcome to the CPE.....	6
1.2 Configuration Requirements for Your Computer	6
2 Home.....	7
2.1 Overview	7
2.1.1 Internet Status	7
2.1.2 Internet Usage	7
2.1.3 Wi-Fi Status	7
2.1.4 LAN Usage	7
2.2 Product Information	8
2.2.1 Product Information	8
2.2.2 Device List	8
2.3 Update	8
2.3.1 Local Update.....	8
2.3.2 HTTP Update	9
3 Internet.....	10
3.1 Network Connection	10
3.1.1 Selecting a Network Mode.....	10
3.1.2 Selecting a Connection Mode	10
3.1.3 Selecting a Network to Connect To.....	11
3.1.4 Turning Data Roaming On or Off.....	11
3.1.5 Selecting an APN Profile	12
3.2 APN Management	12
3.2.1 Creating an APN Profile	12
3.2.2 Modifying an APN Profile	12
3.2.3 Deleting an APN Profile	13
3.3 PIN Management	13
3.3.1 Viewing the USIM Card Status	13
3.3.2 Enabling PIN Verification	13
3.3.3 Disabling PIN Verification	14
3.3.4 Verifying the PIN	14
3.3.5 Changing the PIN.....	14




3.3.6 Setting Automatic Verification of the PIN	15
3.3.7 Verifying the PUK.....	15
3.4 Setting the MTU.....	15
3.5 Unlocking the USIM Card	16
4 LAN.....	17
4.1 DHCP Settings	17
4.1.1 LAN Host Settings	17
4.1.2 DHCP Settings	17
4.1.3 Bundled Address List	18
4.2 Static Routing.....	19
4.3 Dynamic Routing	19
5 Wi-Fi	21
5.1 Wi-Fi	21
5.1.1 General Settings	21
5.1.2 SSID Profile	21
5.2 Access Management	23
5.2.1 Settings.....	23
5.2.2 Wi-Fi Access List	24
5.3 WPS Settings.....	25
5.4 Wi-Fi Multi-SSID.....	26
5.5 Advanced Settings	27
5.6 WDS.....	28
6 Security.....	29
6.1 Firewall Level	29
6.2 MAC Filtering.....	29
6.2.1 MAC Address Whitelist	29
6.2.2 MAC Address Blacklist	31
6.3 URL Filtering	31
6.3.1 URL Whitelist	31
6.3.2 URL Blacklist	32
6.4 IP Filtering.....	32
6.4.1 IP Address Whitelist.....	32
6.4.2 IP Address Blacklist	33
6.5 Service Access Control.....	33
6.6 ALG.....	34
6.7 Port Forwarding	34
6.8 UPnP	36
6.8.1 UPnP	36
6.9 DMZ.....	36
7 Services.....	37

7.1 DDNS.....	37
7.2 SMS Messages	37
7.2.1 Viewing SMS Messages.....	37
7.2.2 Sending SMS Messages	38
7.2.3 Saving SMS Messages	38
7.2.4 Forwarding SMS Messages	38
7.2.5 Replying to SMS Messages	38
7.2.6 Deleting SMS Messages	39
7.3 SMS Settings.....	39
8 System	40
8.1 Maintenance	40
8.1.1 Restart	40
8.1.2 Reset.....	40
8.1.3 Download Configuration File	41
8.1.4 Upload Configuration File	41
8.2 Change Password	41
8.3 Date &Time.....	42
8.4 Diagnosis.....	42
8.4.1 Ping	43
8.4.2 Traceroute	43
8.4.3 System Check.....	43
8.4.4 Wireless Status Check	44
8.5 Logs.....	45
8.6 System Notification.....	45
9 FAQs	46
10 Acronyms and Abbreviations.....	47
11 Copyright Notice and Warranty Disclaimer.....	49

1 Getting Started

1.1 Welcome to the CPE

In this document, the LTE (Long Term Evolution) CPE (customer premises equipment) will be replaced by the CPE. Read the following safety symbols carefully to help you use your CPE safely and correctly:

-  Additional information about the topic
-  Optional methods or shortcuts for an action
-  Potential problems or conventions that need to be specified

1.2 Configuration Requirements for Your Computer

Your computer must meet the requirements of the CPE. Otherwise, performance deteriorates.

Item	Requirement
CPU	Pentium 500 MHz or higher
Memory	128 MB RAM or higher
Hard disk	50 MB available space
Operating system	<ul style="list-style-type: none">• Microsoft: Windows XP, Windows Vista, or Windows 7• Mac: Mac OS X
Display resolution	1024 x 768 pixels or higher
Browser	<ul style="list-style-type: none">• Internet Explorer 6.0 or a later version• Firefox 4.0 or a later version• Opera 11 or a later version• Safari 3 or a later version• Chrome of all versions

2 Home

2.1 Overview

2.1.1 Internet Status

To view the Internet connection status:

1. Choose **Home > Overview**.

The **Internet Status** page is displayed.

2. View the Internet status, including **USIM card status**, **Network mode**, **status**, and so on.

----End

2.1.2 Internet Usage

To view the network data usage:

1. Choose **Home > Overview**.

The **Internet Usage** page is displayed.

2. View the network data usage, including uplink and downlink rates, uplink and downlink traffic volumes, and time spent online.

----End

2.1.3 Wi-Fi Status

To view the Wi-Fi network connection status:

1. Choose **Home > Overview**.

The **Wi-Fi Status** page is displayed.

2. View the Wi-Fi network connection status, including the **SSID**, **IP Address**, **MAC Address**, broadcast mode, and wireless encryption mode.

3. View the statistics of the Wi-Fi network, including the number of bytes, packets, erroneous packets, and discarded packets transmitted and received over the Wi-Fi network.

----End

2.1.4 LAN Usage

To view the local area network (LAN) connection status, choose **Home > Overview**.

The **LAN Usage** page is displayed. You can then view the LAN status, including **IP address**, **MAC address**, **DHCP server**. You can also view the statistics of the LAN, including the number of bytes, packets, erroneous packets, and discarded packets transmitted and received over the LAN.

---End

2.2 Product Information

2.2.1 Product Information

To view basic product information, choose **Home > Product Information**.

The **Product Information** page is displayed. This page shows basic information about the CPE, for example, the model, serial number (SN), international mobile equipment identity (IMEI), firmware version, and hardware version.

2.2.2 Device List

The device list shows information about the active devices.

To view the device list, choose **Home > Product Information**.

The **Device List** page is displayed. You can then view information about the devices, including **Computer Name**, **MAC Address**, **IP Address**, and **Lease Time**. **Lease Time** indicates the remaining lease duration of the dynamic DHCP server. If a static IP address is bundled with the device, **Lease Time** and **Computer Name** are **N/A** and **Unknown**, respectively.

2.3 Update

This function enables you to upgrade the operating system to the latest version. It is recommended that you update your system because in the new version, certain bugs are fixed and the system stability is usually improved.

2.3.1 Local Update

Before performing an upgrade, save the target software version to your computer.

To perform a local upgrade:

1. Choose **Home > Update**.

The **Update** page is displayed.

2. Click **CHOOSE FILE** on the **Local Update** tab. In the displayed dialog box, select the target software version file.
3. Click **Open**. The dialog box closes. The save path and name of the target software version file are displayed in the **Update file** field.
4. Click **Update**. Then confirm your operation in the displayed dialog box.



During an update, do not power off the CPE or disconnect the CPE from the computer.

- Click **OK**. The software update starts. After the upgrade, the CPE is automatically restarted.

----End

2.3.2 HTTP Update

To perform an HTTP upgrade:

- Choose **Home > Update**.

The **HTTP Update** page is displayed.

- Click **Check** to check for updates.

If...	Then...
Updates are found.	Go to step 3.
No updates are found.	The procedure is complete.

- Click **Update** to download the updates.

A download progress bar is displayed.

- After the updates download, the update automatically begins.

An update progress bar is displayed.

- After the update is complete, the CPE automatically restarts.

A message is displayed, indicating that the update is complete.



During an upgrade, do not operate the CPE.

- If the update fails, the CPE may not power on. Try forcibly restoring the system to the previous version.



To forcibly restore the system, press the WPS button and WLAN button simultaneously, and then press the power button.

----End

3 Internet

3.1 Network Connection

3.1.1 Selecting a Network Mode

You can select a network mode for the CPE. **Network mode** can be set to **4G/3G Auto**, **4G/3G/2G Auto**, **4G**, **3G**, or **2G**.

To select a network mode:

1. Insert a valid USIM card into the CPE.
2. Power on the CPE, and then log in to the web UI as the admin user.
3. Choose **Internet > Network Connection**.

The **Network Connection** page is displayed.

4. Set **Network mode** to one of the following values:

Value	Description
4G/3G Auto	The CPE automatically selects its working mode, with an order of preference of 4G and 3G.
4G/3G/2G Auto	The CPE automatically selects its working mode, with an order of preference of 4G, 3G, and 2G.
4G	The CPE accesses 4G networks only.
3G	The CPE accesses 3G networks only.
2G	The CPE accesses 2G networks only.

5. Click **Submit**.

----End

3.1.2 Selecting a Connection Mode

You can select a network connection mode on the **Network Connection** page. **Always on** indicates that the connection is always on. If the CPE is set to **Always on** and a network connection is available, the CPE automatically connects to the Internet. **Manual** indicates that

you can manually connect or disconnect the CPE to or from the Internet. **On demand** indicates that the CPE connects to the Internet only when you make an Internet access request (for example, use a search engine) and disconnects from the Internet after a specified amount of idle time.

To select a network connection mode:

1. Choose **Internet > Network Connection**.

The **Network Connection** page is displayed.

2. Set **Connection mode** to **Always on**, **Manual**, or **On demand**.

- If you selected **Manual**, you can select **Restart option** to enable the CPE to retain the same connection status before and after it restarts.
- If you selected **On demand**, set **Maximum idle time**.

3. Click **Submit**.

----End

3.1.3 Selecting a Network to Connect To

When the CPE **Connection mode** is set to **Manual** and the CPE is not connected to a network, you can manually select a network to connect on the **Network Connection** page. To select a network:

1. Select **Manual** for **Network selection**.

By default, **Network selection** is set to **Auto**, allowing the CPE to automatically select a network.

2. Click **Search**.
3. From the list of networks found, select a network you wish to connect to and click **Register**.
4. Click **Submit**.

---End

3.1.4 Turning Data Roaming On or Off

To turn **Roaming** on or off:

1. Choose **Internet > Network Connection**.

The **Network Connection** page is displayed.

2. Select or clear **Roaming** to turn it on or off.
3. Click **Submit**.

----End

3.1.5 Selecting an APN Profile

An APN profile is a group of dial-up parameters related to an access point name (APN). You can select an APN profile for the CPE to access the Internet.

To set the dial-up parameters:

1. Choose **Internet > Network Connection**.

The **Network Connection** page is displayed.

2. Select a profile.
3. Click **Submit**.

---End

3.2 APN Management

3.2.1 Creating an APN Profile

To create an APN profile:

1. Choose **Internet > APN Management**.

The **APN Management** page is displayed.

2. Click **Add**.
3. On the displayed page, set **Profile name**, **APN**, **User name**, and **Password**.
4. Set **Authentication** to **None**, **PAP**, **CHAP**, or **Auto**.
5. Click **Submit**.

---End

3.2.2 Modifying an APN Profile

To modify an APN profile:

1. Choose **Internet > APN Management**.

The **APN Management** page is displayed.

2. Choose the **APN Profile** parameter to be changed, and click **Edit**.
3. On the displayed page, change **Profile Name**, **APN**, **User name**, or **Password**.
4. Set **Authentication** to **None**, **PAP**, **CHAP**, or **Auto**.
5. Click **Submit**.

---End

3.2.3 Deleting an APN Profile

To delete an APN profile:

1. Choose **Internet > APN Management**.

The **APN Management** page is displayed.

2. Choose the **APN Profile** parameter to be deleted, and click **Delete**.
3. From the displayed dialog box, click **OK**.

----End

3.3 PIN Management

From the **PIN Management** page, you can perform the following operations to manage the PIN:

- View the USIM card status.
- Enable or disable PIN verification.
- Verify the PIN.
- Change the PIN.
- Set automatic verification of the PIN.
- Verify the PIN unblocking key (PUK).

3.3.1 Viewing the USIM Card Status

To view the USIM card status:

1. Choose **Internet > PIN Management**.

The **PIN Management** page is displayed.

2. View the status of the USIM card in the **USIM card status** field.

----End

3.3.2 Enabling PIN Verification

To enable PIN verification:

1. Choose **Internet > PIN Management**.

The **PIN Management** page is displayed.

2. Select the **Enable** check box next to **PIN verification**.
3. Enter the PIN (four to eight digits) in the **Enter PIN** field.
4. Click **Submit**.

----End

3.3.3 Disabling PIN Verification

To disable PIN verification:

1. Choose **Internet > PIN Management**.
The **PIN Management** page is displayed.
2. Select the **Disable** check box next to **PIN verification**.
3. Enter the PIN (four to eight digits) in the **Enter PIN** field.
4. Click **Submit**.

---End

3.3.4 Verifying the PIN

If PIN verification is enabled but the PIN is not verified, verification is required.

To verify the PIN:

1. Choose **Internet > PIN Management**.
The **PIN Management** page is displayed.
2. Enter the PIN (four to eight digits) in the **PIN** field.
3. Click **Submit**.

---End

3.3.5 Changing the PIN

The PIN can be changed only when PIN verification is enabled and the PIN is verified.

To change the PIN:

1. Choose **Internet > PIN Management**.
The **PIN Management** page is displayed.
2. Select the **Enable** check box next to **PIN verification**.
3. Select the **Enable** check box next to **Change PIN**.
4. Enter the current PIN (four to eight digits) in the **PIN** field.
5. Enter a new PIN (four to eight digits) in the **New PIN** field.
6. Repeat the new PIN in the **Confirm PIN** field.
7. Click **Submit**.

---End

3.3.6 Setting Automatic Verification of the PIN

You can enable or disable automatic verification of the PIN. If automatic verification is enabled, the CPE automatically verifies the PIN after the CPE restarts. This function can be enabled only when PIN verification is enabled and the PIN is verified.

To enable automatic verification of the PIN:

1. Choose **Internet > PIN Management**.
2. The **PIN Management** page is displayed.
3. Select the **Enable** check box next to **PIN verification**.
4. Select the **Enable** check box next to **Remember my PIN**.
5. Click **Submit**.

---End

3.3.7 Verifying the PUK

If PIN verification is enabled and the PIN fails to be verified three consecutive times, the PIN will be locked. In this case, you need to verify the PUK and change the PIN to unlock the PIN.

To verify the PUK:

1. Choose **Internet > PIN Management**.
The **PIN Management** page is displayed.
2. Enter the PUK in the **PUK** field.
3. Enter a new PIN in the **New PIN** field.
4. Repeat the new PIN in the **Confirm PIN** field.
5. Click **Submit**.

---End

3.4 Setting the MTU

You can specify the maximum number of bytes per packet allowed to be transmitted through the network port.

Note: An excessive MTU value may result in network connection failure.

To change the MTU value:

1. Choose **Internet > Internet MTU**.
The **Internet MTU** page is displayed.
2. Enter an MTU value in the **Internet MTU** field.
3. Click **Submit**.

---End

3.5 Unlocking the USIM Card

Contact your service provider for the USIM unlock code. You can use the CPE after its USIM card is unlocked.

Note: If the number of unlock attempts exceeds the predefined limit, the USIM card is locked permanently.

To unlock a USIM card:

1. Choose **Internet** > **SIM Lock**.

The **SIM Lock** page is displayed.

2. Enter the unlock code in the **Unlock code** field.
3. Click **Submit**.

---End

4 LAN

4.1 DHCP Settings

4.1.1 LAN Host Settings

You can change the host IP address to another individual IP address that is easy to remember. Make sure the IP address is unique on your network. If you change the IP address of the CPE, access the web UI with the new IP address.

To change the IP address of the CPE:

1. Choose **LAN > DHCP Settings**.

The **DHCP Settings** page is displayed.

2. Set **IP address**.
3. Select the **Enable** check box next to **DHCP server**.
4. Click **Submit**.

----End

4.1.2 DHCP Settings

DHCP allows individual clients to automatically obtain TCP/IP configurations when a server starts up.

You can configure the CPE as a DHCP server or disable it when the CPE is working in routing mode.

When configured as a DHCP server, the CPE automatically provides TCP/IP configuration for the LAN clients that support DHCP client capabilities. If DHCP server services are disabled, you must have another DHCP server on your LAN, or each client must be manually configured.


To configure DHCP settings:

1. Choose **LAN > DHCP Settings**.


The **DHCP Settings** page is displayed.

2. Select the **Enable** check box next to **DHCP server**.

3. Set **Start IP address**.


 This IP address must be different from the IP address that is set on the **LAN Host Settings** page, but both addresses must be on the same network segment.

4. Set **End IP address**.

 This IP address must be different from the IP address that is set on the **LAN Host Settings** page, but both addresses must be on the same network segment.

The end IP address must be less than or equal to the start IP address.

5. Set **Lease time**.

 This parameter can be set to 1 to 10,080 minutes.

6. Click **Submit**.

----End

4.1.3 Bundled Address List

You can bundle an IP address with a device based on its MAC address. The device will always receive the same IP address each time it accesses the DHCP server. For example, you can bundle an IP address with an FTP server on the LAN.

 After you change the settings, click **Submit** for the changes to take effect. The DHCP server may need to restart.

To configure or view the bundled list page:

1. Choose **LAN > DHCP Settings**.
2. Click **Edit List**.

The **Bundled Address** page is displayed.

----End

To add a MAC/IP rule:

1. Click **Add**.
2. On the displayed page, set **MAC address** and **IP address**.
3. Click **Submit**.

----End

To modify a MAC/IP rule:

1. Choose the rule to be modified, and click **Edit**.
2. On the displayed page, set **MAC address** and **IP address**.
3. Click **Submit**.

----End

To delete a MAC/IP rule:

1. Choose the rule to be deleted, and click **Delete**.
2. From the displayed dialog box, click **OK**.

----End

To delete all MAC/IP rules:

1. Click **Delete All**.
2. From the displayed dialog box, click **OK**.

----End

To make the changes take effect, click Apply, or click Back and click Submit from the DHCP Settings screen.

4.2 Static Routing

If cascaded routers are used on the LAN, add static routing rules to ensure that the devices connected to the cascaded routers can be accessed. Static routing is similar to dynamic routing. However, manual configuration is required and the router must always be available.

- If the IP address of the cascaded router is fixed, static routing is recommended.
- If the IP address of the cascaded router is changeable, dynamic routing is recommended.

To configure static routing settings:

1. Choose **LAN > Static Routing**.

The **Static Routing** page is displayed.

2. Click **Add** in the upper right corner of the **Static Routing** page.
3. Set **Destination IP address**.
4. Set **Subnet mask**.
5. Set **Router IP address**. This IP address is obtained from the CPE and used for data transmission to the cascading devices. This IP address must be reachable.
6. Click **Submit**.

----End

4.3 Dynamic Routing

This function is enabled when cascaded routers are used on the LAN and the cascaded routers comply with the Routing Information Protocol (RIP). This page allows you to enable or disable RIP and set its version and operation mode.

To configure dynamic routing settings:

1. Choose **LAN > Dynamic Routing**.
The **Dynamic Routing** page is displayed.
2. Select the **Enable** check box next to **RIP**.
3. Set **Operation**. If it is set to **Active**, the CPE actively makes route changes and notifies surrounding routers of the changes. If it is set to **Passive**, the CPE does not make route changes until it is notified.
4. Set **Version** to **RIP v1**, **RIP v2**, or **RIP v1/RIP v2**.
5. Click **Submit**.
----End

5 Wi-Fi

5.1 Wi-Fi

5.1.1 General Settings

This function lets you configure the basic Wi-Fi parameters.

To configure the basic Wi-Fi settings:

1. Choose **Wi-Fi > Wi-Fi Settings**.

The **Wi-Fi Settings** page is displayed.

2. Select the **Enable** check box next to **Wi-Fi**.
3. Set **Mode** to one of the following values:

Value	Description
802.11b/g/n	The Wi-Fi client can connect to the CPE in 802.11b, 802.11g, or 802.11n mode. If the client connects to the CPE in 802.11n mode, the Advanced Encryption Standard (AES) encryption mode is required.
802.11b/g	The Wi-Fi client can connect to the CPE in 802.11b or 802.11g mode.
802.11b	The Wi-Fi client can connect to the CPE in 802.11b mode.
802.11g	The Wi-Fi client can connect to the CPE in 802.11g mode.
802.11n	The Wi-Fi client can connect to the CPE in 802.11n mode.

4. Click **Submit**.

---End

5.1.2 SSID Profile

Configuring the CPE on the **SSID Profile** page lets the Wi-Fi client connect to the CPE based on preset rules, improving access security.

To configure the CPE on the **SSID Profile** page:

1. Choose **Wi-Fi > Wi-Fi Settings**.

The **Wi-Fi Settings** page is displayed.

2. Set **SSID**.



SSID can contain 1 to 32 ASCII characters.

The Wi-Fi client connects to the CPE using the found SSID.

3. Set **Maximum number of devices**.



This parameter indicates the maximum number of Wi-Fi clients that connect to the CPE.

A maximum of 32 clients can connect to the CPE.

4. Select the **Enable** check box next to **Hide SSID broadcast**.

The SSID is hidden. In this case, the client cannot detect Wi-Fi information about the CPE.

5. Select the **Enable** check box next to **AP isolation**.

The clients can connect to the CPE but cannot communicate with each other.

6. Set **Security**.



If this parameter is set to **None (not recommended)**, the Wi-Fi client directly connects to the CPE. This causes security risks.

If this parameter is set to **WEP**, the Wi-Fi client connects to the CPE in web-based encryption mode.

If this parameter is set to **WPA-PSK**, the Wi-Fi client connects to the CPE in WPA-PSK encryption mode.

If this parameter is set to **WPA2-PSK (recommended)**, the Wi-Fi client connects to the CPE in WPA2-PSK encryption mode. This mode is recommended because it ensures a high level of security.

If this parameter is set to **WPA-PSK & WPA2-PSK**, the Wi-Fi client connects to the CPE in WPA-PSK or WPA2-PSK encryption mode.

7. Set **Authentication mode** to one of the following values, and configure the corresponding parameters.

Value	Settings	Description
WEP	Authentication mode	<ul style="list-style-type: none"> • Shared Authentication: The client connects to the CPE in shared authentication mode. • Open Authentication: The client connects to the CPE in open authentication mode. • Both: The client connects to the CPE in shared or open authentication mode.
	Password length	<ul style="list-style-type: none"> • 128-bit: Only 13 ASCII characters or 26 hex characters can be entered in the Password 1 to Password 4 fields. • 64-bit: Only 5 ASCII characters or 10 hex characters can be entered in the Password 1 to Password 4 fields.
	Current password index	It can be set to 1, 2, 3, or 4 . After a key index is selected, the corresponding key takes effect.
WPA-PSK	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA Encryption	It can be set to TKIP+AES, AES, or TKIP .
WPA2-PSK (recommended)	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA Encryption	It can be set to TKIP+AES, AES, or TKIP .
WPA-PSK & WPA2-PSK	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA Encryption	It can be set to TKIP+AES, AES, or TKIP .

8. Click **Submit**.

---End

5.2 Access Management

5.2.1 Settings

This function enables you to manage the access to the CPE. You can set access restriction policies for each SSID.

The MAC access of each SSID can be set to **Disable, Blacklist, or Whitelist**.

- If an SSID's MAC access is set to **Disable**, access restriction does not take effect.
- If an SSID's MAC access is set to **Blacklist**, only devices that are not in the blacklist can connect to the SSID.

- If an SSID's MAC access is set to **Whitelist**, only devices in the whitelist can connect to the SSID.

To configure Wi-Fi MAC control settings:

1. Choose **Wi-Fi > Access Management**.
The **Access Management** page is displayed.
 2. Set the SSID's MAC access.
 3. Click **Submit**.
- End

5.2.2 Wi-Fi Access List

This function allows you to set the SSID access policies based on MAC addresses. When you set a MAC address, you can set the SSID to which it corresponds.

To add an item to the Wi-Fi access list:

1. Choose **Wi-Fi > Access Management**.
The **Access Management** page is displayed.
 2. Click **Edit MAC List**.
The **Wi-Fi Access List** page is displayed.
 3. Click **Add**.
 4. Set **MAC address**.
 5. To make the MAC address take effect for **SSID-1**, select the **Enable** check box next to **SSID-1**.
The operations for other SSIDs are similar to those for **SSID-1**.
 6. Click **Submit**.
- End

To modify an item in the Wi-Fi access list:

1. Choose **Wi-Fi > Access Management**.
The **Access Management** page is displayed.
2. Click **Edit MAC List**.
The **Wi-Fi Access List** page is displayed.
3. Choose the item to be modified, and click **Edit**.
4. On the displayed page, set **MAC address**.
5. To make the MAC address take effect for **SSID-1**, select the **Enable** check box next to **SSID-1**.
The operations for other SSIDs are similar to those for **SSID-1**.

6. Click **Submit**.

----End

To delete an item from the Wi-Fi access list:

1. Choose **Wi-Fi > Access Management**.
The **Access Management** page is displayed.
2. Click **Edit MAC List**.
3. The **Wi-Fi Access List** page is displayed.
4. Choose the item to be deleted, and click **Delete**.
5. From the displayed dialog box, click **OK**.

----End

To delete all items from the Wi-Fi access list:

1. Choose **Wi-Fi > Access Management**.
The **Access Management** page is displayed.
2. Click **Edit MAC List**.
The **Wi-Fi Access List** page is displayed.
3. Click **Delete All**.
4. From the displayed dialog box, click **OK**.

----End

To make the changes take effect, click Apply. To return to the previous page, click Back.

5.3 WPS Settings

Wi-Fi Protected Setup (WPS) allows you to add a wireless client to the network easily without needing to specifically configure the wireless settings, such as the SSID, security mode, and passphrase. You can add a wireless client using either the WPS button or PIN.

To connect a client to the CPE's network:

- In PBC mode, press the CPE's and the client's WPS buttons.
- In router PIN mode, enter the router PIN on the client.
- In client PIN mode, enter the client PIN on the client.



When **Hide SSID broadcast** is enabled, WPS does not take effect. WPS supports only WPA2-PSK, WPA-PSK & WPA2-PSK, and open authentication.

To configure Wi-Fi WPS settings:

1. Choose **Wi-Fi > WPS Settings**.

The **WPS Settings** page is displayed.

2. Select the **Enable** check box next to **WPS**.
3. Set **WPS mode**.



If this parameter is set to **PBC**, after you click **Submit**, press the WPS button on the CPE and then on the client. The client can then connect to the CPE.

If this parameter is set to **Router PIN**, enter the router PIN on the client to connect it to the CPE.

If this parameter is set to **Client PIN**, enter the client PIN. After you correctly enter the PIN, click **Connect to Client** to connect the client to the CPE.

4. Click **Submit**.

---End

5.4 Wi-Fi Multi-SSID

The **SSID List** page shows information about the SSIDs to be configured. To configure an SSID:

1. Choose **Wi-Fi > Wi-Fi Multi-SSID**.

The **SSID List** page is displayed.

2. Choose an SSID to be configured, and click **Edit**.
3. Select the **Enable** check box next to **Status**.
4. Set **SSID**.



SSID can contain 1 to 32 ASCII characters.

SSID cannot contain any of the following characters: / ' = " \ &

5. Set **Maximum number of devices**.



The number of accessing devices must be an integer ranging from 1 to 32.

6. Select the **Enable** check box next to **Hide SSID broadcast**.

7. Set **AP isolation**.

If the **Enable** check box is selected, clients can connect to the CPE but cannot communicate with each other. If the **Enable** check box is not selected, clients can connect to the CPE and can communicate with each other.

8. Set **Security**.

If Security is set to WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK, you can set WPA-PSK and WPA encryption.



WPA-PSK can contain 8 to 63 ASCII characters or 64 hex characters.

If Security is set to **WEP**, set **Authentication mode**, **Password length**, and **Current password index**, and configure the corresponding keys.

If **Password length** is set to **128-bit**, **WPA-PSK** can contain 8 to 63 ASCII characters or 64 hex characters.

If **Password length** is set to **64-bit**, the 64-bit encryption key must contain 5 ASCII characters or 10 hex characters.

9. Click **Submit**.

----End

5.5 Advanced Settings

Advanced Settings affect Wi-Fi performance. These settings help you obtain the maximum access rate and optimal access performance.

To configure the advanced parameters:

1. Set **Channel**.

Auto indicates that the channel with the best signal quality is selected.

The values 1 to 13 indicate the selected channel.

2. Set **802.11n bandwidth**.

If this parameter is set to **20 MHz**, 802.11n supports only 20 MHz bandwidth.

If this parameter is set to **20/40 MHz**, 802.11n supports 20 MHz or 40 MHz bandwidth.

If **Mode** is set to **802.11b** or **802.11g**, this parameter does not need to be set.

3. Set **Rate**.

Rate varies with the selected mode.

If **Rate** is set to **Auto**, the Wi-Fi client connects to the CPE through the channel with the best signal quality.

If the rate is specified, the client connects to the CPE at the specified rate. If the channel conditions do not meet the requirements, the connection performance is affected.

4. Set **Transmit power**.

If this parameter is set to **100%**, the Wi-Fi client transmits signals at full power.

If this parameter is set to **80%**, **60%**, or **40%**, the Wi-Fi client transmits signals at low power. Wi-Fi clients located far from the CPE may fail to access the CPE.

5. Set **WMM**.

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories (AC) – voice, video, best effort, and background. However, WMM does not provide guaranteed throughput. WMM applies to simple applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones.

6. Click **Submit**.

----End

5.6 WDS

When the CPE works in repeater mode, the Wi-Fi module supports the wireless distribution system (WDS). The Wi-Fi clients must be configured to use the same radio channel, encryption mode, and encryption key. The WDS encryption mode can be set to **Open authentication** or **WPA-PSK & WPA2-PSK**. If the encryption mode is **Open authentication**, the Wi-Fi clients can use **NONE** or **WEP** encryption. If the encryption mode is **WPA-PSK & WPA2-PSK**, the Wi-Fi clients can use **WPA/WPA2-PSK** encryption. After you enable WDS, disable DHCP on CPEs that are not directly connected to the WAN port. Make sure that the CPEs are not using the same gateway IP address and all their gateway IP addresses are in the same network segment.

Note: If WDS is enabled, the WPS function will not take effect. If the channel is set to Auto, go to the **Advanced Settings** page to set the channel to a specific value.

To enable WDS:

1. Choose **Wi-Fi > WDS**.

The **WDS Settings** page is displayed.

2. Select the **Enable** check box next to **WDS**.
3. Click **Scan**.

From the search results, choose the SSID of the networking device.

4. Set **Security**.



WPA-PSK can contain 8 to 63 ASCII characters or 64 hex characters.

5. Click **Submit**.

----End

6 Security

6.1 Firewall Level

This page allows you to set the firewall level.

To set the firewall level:

1. Choose **Security > Firewall Level**.

The **Firewall Level** page is displayed.

2. Set **Firewall level**.
3. Click **Submit**.

----End

To configure the firewall filtering settings:

4. Choose **Security > Firewall Level**.

The **Firewall Level** page is displayed.

5. Set **Firewall level** to **Custom**.
6. Set **MAC filtering**.
7. Set **IP filtering**.
8. Set **URL filtering**.

9. Click **Submit**.

----End

6.2 MAC Filtering

This page allows you to configure the MAC address filtering rules.

6.2.1 MAC Address Whitelist

To add a MAC address whitelist rule:

1. Choose **Security > MAC Filtering**.
The **MAC Filtering** page is displayed.
2. Set **MAC filtering mode** to **Whitelist**.
3. Click **Add Item**.
4. On the displayed page, set **MAC**.
5. Click **Submit**.

----End

To change a MAC address whitelist rule:

1. Choose **Security > MAC Filtering**.
The **MAC Filtering** page is displayed.
2. Set **MAC filtering mode** to **Whitelist**.
3. Choose the entry you want to change and click **Edit**.
4. On the displayed page, set **MAC**.
5. Click **Submit**.

----End

To delete a MAC address whitelist rule:

1. Choose **Security > MAC Filtering**.
The **MAC Filtering** page is displayed.
2. Set **MAC filtering mode** to **Whitelist**.
3. In the entry of the rule to be deleted, click **Delete**.
4. From the displayed dialog box, click **OK**.

----End

To delete all MAC address whitelist rules:

1. Choose **Security > MAC Filtering**.
The **MAC Filtering** page is displayed.
2. Set **MAC filtering mode** to **Whitelist**.
3. Click **Delete All**.
4. From the displayed dialog box, click **OK**.

----End

6.2.2 MAC Address Blacklist

Choose **Security > MAC Filtering**. Set MAC filtering mode to **Blacklist**.

The other operations are the same as those of the MAC address whitelist.

6.3 URL Filtering

This page allows you to configure the URL filtering rules.

6.3.1 URL Whitelist

To add a URL whitelist rule:

1. Choose **Security > URL Filtering**.
The **URL Filtering** page is displayed.
2. Set **URL filtering mode** to **Whitelist**.
3. Click **Add Item**.
4. Set **URL**.
5. Click **Submit**.

----End

To change a URL whitelist rule:

1. Choose **Security > URL Filtering**.
The **URL Filtering** page is displayed.
2. Set **URL filtering mode** to **Whitelist**.
3. Choose the entry you want to change and click **Edit**.
4. On the displayed page, set **URL**.
5. Click **Submit**.

----End

To delete a URL whitelist rule:

1. Choose **Security > URL Filtering**.
The **URL Filtering** page is displayed.
2. Set **URL filtering mode** to **Whitelist**.
3. Choose the entry you want to delete and click **Delete**.
4. From the displayed dialog box, click **OK**.

----End

To delete all URL whitelist rules:

1. Choose **Security > URL Filtering**.
The **URL Filtering** page is displayed.
2. Set **URL filtering mode** to **Whitelist**.
3. Click **Delete All**.
4. From the displayed dialog box, click **OK**.

----End

6.3.2 URL Blacklist

Choose **Security > URL Filtering**. Set URL filtering mode to **Blacklist**.

The other operations are the same as those of the URL whitelist.

6.4 IP Filtering

This page allows you to configure the IP address filtering rules.

6.4.1 IP Address Whitelist

To add an IP address whitelist rule:

1. Choose **Security > IP Filtering**.
The **IP Filtering** page is displayed.
2. Set **IP filtering mode** to **Whitelist**.
3. Click **Add Item**.
4. Set **Service**.
5. Set **Protocol**.
6. Set **Source IP address range**, which is the IP address or IP address segment to be filtered.
7. Set **Source port range**, which is the port or port segment to be filtered.
8. Set **Destination IP address range**, which is the IP address or IP address segment to be filtered.
9. Set **Destination port range**, which is the port number or port number segment to be filtered.
10. Click **Submit**.

----End

To change an IP whitelist rule:

1. Choose **Security > IP Filtering**.
The **IP Filtering** page is displayed.

2. Set **IP filtering mode** to **Whitelist**.
3. Choose the entry you want to change and click **Edit**.
4. Make your changes.
5. Click **Submit**.

----End

To delete an IP address whitelist rule:

1. Choose **Security > IP Filtering**.
The **IP Filtering** page is displayed.
2. Set **IP filtering mode** to **Whitelist**.
3. Choose the entry you want to delete and click **Delete**.
4. From the displayed dialog box, click **OK**.

----End

To delete all IP address whitelist rules:

1. Choose **Security > IP Filtering**.
The **IP Filtering** page is displayed.
2. Set **IP filtering mode** to **Whitelist**.
3. Click **Delete All**.
4. From the displayed dialog box, click **OK**.

----End

6.4.2 IP Address Blacklist

Choose **Security > URL Filtering**. Set IP filtering mode to **Blacklist**.

The other operations are the same as those of the IP address whitelist.

6.5 Service Access Control

This function allows you to control the number of users connected to the CPE.

The access control list shows the types of services that are controlled by the CPE. By default, the access control rules are not in effect.

To set the access control list:

1. Choose **Security > Service Access Control**.
The **Service Access Control** page is displayed.
2. Choose the entry to be configured, and click **Edit**.

3. Set **IP address range**.



If **Access source** is **LAN**, the IP address must be on the same network segment as the IP address that is set on the **LAN Host Settings** page.

If **Access source** is **Internet**, the IP address must be on different network segments from the IP address that is set on the **LAN Host Settings** page.

4. Set **Status**.

5. Click **Submit**.

----End

6.6 ALG

On this page, you can enable or disable SIP ALG.

To enable SIP ALG:

1. Choose **Security > ALG**.

The **ALG Settings** page is displayed.

2. Select the **Enable** check box next to **SIP ALG**.

3. Set **SIP port**.



The default port numbered 5060 is recommended. If the default port is not used, VoIP software cannot be used.

4. Click **Submit**.

----End

6.7 Port Forwarding

When network address translation (NAT) is enabled on the CPE, only the IP address on the WAN side is open to the Internet. If a computer on the LAN is enabled to provide services for the Internet (for example, work as an FTP server), port forwarding is required so that all accesses to the external server port from the Internet are redirected to the server on the LAN.

To add a port forwarding rule:

1. Choose **Security > Port Forwarding**.

The **Port Forwarding** page is displayed.


2. Click **Add Item**.

3. Set **Type**.

4. Set **Protocol**.

5. Set **Remote host** (Optional).


6. Set **Remote port range**.

 The port number must range from 1 to 65535.

7. Set **Local host**.

 This IP address must be different from the CPE IP address, but it must be on the network segment set on the **LAN Host Settings** page.

8. Set **Local port**.

 The port number must range from 0 to 65535.

9. Set **Status** to **Enabled** or **Disabled**.

10. Click **Submit**.

---End

To change a port forwarding rule:

1. Choose **Security > Port Forwarding**.

The **Port Forwarding** page is displayed.

2. Choose the entry you want to change and click **Edit**.

3. Make your changes.

4. Click **Submit**.

---End

To delete a port forwarding rule:

1. Choose **Security > Port Forwarding**.

The **Port Forwarding** page is displayed.

2. Choose the entry you want to delete and click **Delete**.

3. From the displayed dialog box, click **OK**.

---End

To delete all port forwarding rules:

1. Choose **Security > Port Forwarding**.

The **Port Forwarding** page is displayed.

2. Click **Delete All**.

3. From the displayed dialog box, click **OK**.

---End

6.8 UPnP

On this page, you can enable or disable the UPnP function.

6.8.1 UPnP

To enable UPnP:

1. Choose **Security > UPnP**.
The **UPnP** page is displayed.
2. Select the **Enable** check box next to **UPnP**.
3. Click **Submit**.

---End

6.9 DMZ

If demilitarized zone (DMZ) is enabled, packets sent from the WAN are directly sent to a specified IP address on the LAN before they are discarded by the firewall.

To enable DMZ:

1. Choose **Security > DMZ**.
The **DMZ Settings** page is displayed.
2. Select the **Enable** check box next to **DMZ**.
3. Set **Host address**.



This IP address must be different from the IP address set on the **LAN Host Settings** page. However, both addresses must be on the same network segment.

4. Click **Submit**.

---End

7 Services

7.1 DDNS

Dynamic DNS (DDNS) is a real-time dynamic DNS updating service that provides a domain name for a resource that may change location on the network. To configure DDNS settings:

1. Choose **Services > DDNS**.
The **DDNS** page is displayed.
2. In **Service provider**, choose **DynDns.org**.
3. Select the **Enable** check box next to **DDNS**.
4. Enter **Domain name** and **Host name**. For example, if the domain name provided by your service provider is **test.customtest.dyndns.org**, enter **customtest.dyndns.org** as **Domain name**, and **test** as **Host name**.
5. Enter **User name** and **Password**.
6. Click **Submit**.
---End

7.2 SMS Messages

This page allows you to send, view, and delete SMS messages.

7.2.1 Viewing SMS Messages

You can check the messages in your inbox, drafts, and outbox folders.

To view a message:

1. Choose **Services > SMS Messages**.
The **SMS Messages** page is displayed.
2. Click **Inbox** to view received messages.
3. Click **Drafts** to view draft messages.
4. Click **Outbox** to view sent messages.

---End

7.2.2 Sending SMS Messages

To send a message:

1. Choose **Services > SMS Messages**.

The **SMS Messages** page is displayed.

2. In **Phone number**, enter the recipient's phone number. If you want to send a message to multiple recipients, use semicolons (;) to separate the phone numbers.
3. In **Content**, compose a message.
4. Click **Send**.

---End

7.2.3 Saving SMS Messages

To save a message:

1. Choose **Services > SMS Messages**.

The **SMS Messages** page is displayed.

2. In **Phone number**, enter the recipients' phone numbers.
3. In **Content**, compose a message.
4. Click **Save**.

---End

7.2.4 Forwarding SMS Messages

To forward a message:

1. Choose **Services > SMS Messages**.

The **SMS Messages** page is displayed.

2. Click **Forward** to the right of the message you want to forward.
3. In **Phone number**, enter the recipients' phone numbers.
4. Click **Send**.

---End

7.2.5 Replying to SMS Messages

To reply to a message:

1. Choose **Services > SMS Messages**.

The **SMS Messages** page is displayed.

2. Click **Reply** to the right of the message to which you want to reply.
3. In **Content**, compose a message.

4. Click **Send**.

----End

7.2.6 Deleting SMS Messages

To delete one or more SMS messages:

1. Choose **Services > SMS Messages**.

The **SMS Messages** page is displayed.

2. Click **Delete** to the right of the message you want to delete.
3. To delete all messages on a page, click **Delete Page**.

----End

7.3 SMS Settings

You can configure SMS settings, such as setting the SMS center number, enabling or disabling an SMS report, and setting whether to save sent messages.

1. Choose **Services > SMS Settings**.

The **SMS Settings** page is displayed.

2. In **Service center address**, enter the SMS center number.
3. Set whether to enable **SMS report**.
4. Set whether to enable **Save sent messages**.



A message sent to multiple recipients cannot be saved.

5. Click **Submit**.

----End

8 System

8.1 Maintenance

8.1.1 Restart

This function enables you to restart the CPE. Settings take effect only after the CPE restarts.

To restart the CPE:

1. Choose **System > Maintenance**.
The **Maintenance** page is displayed.
2. Click **Restart**.
3. From the displayed dialog box, click **OK**.

The CPE then restarts.

---End

8.1.2 Reset

This function enables you to restore the CPE to its default settings.

To restore the CPE:

1. Choose **System > Maintenance**.
The **Maintenance** page is displayed.
2. Click **Reset**.
3. From the displayed dialog box, click **OK**.

The CPE is then restored to its default settings.

---End

8.1.3 Download Configuration File

You can download the existing configuration file to back it up. To do so:

1. Choose **System > Maintenance**.

The **Maintenance** page is displayed.

2. Click **Download** on the **Maintenance** page.

In the displayed dialog box, select the save path and name of the configuration file to be backed up.

3. Click **Save**.

The procedure for file downloading may vary with the browser you are using.

---End

8.1.4 Upload Configuration File

You can upload a backed up configuration file to restore the CPE. To do so:

1. Choose **System > Maintenance**.

The **Maintenance** page is displayed.

2. Click **CHOOSE FILE** on the **Maintenance** page. In the displayed dialog box, select the backed up configuration file.

3. Click **Open**.

The dialog box closes. In the box to the right of **Configuration file**, the save path and name of the backed up configuration file are displayed.

4. Click **Upload**.

5. From the displayed dialog box, click **OK**.

The CPE uploads the backed up configuration file. The CPE then automatically restarts.

---End

8.2 Change Password

This function enables you to change the login password of the admin user. After the password changes, enter the new password the next time you log in.

To change the password:

1. Choose **System > Change Password**.

The **Change Password** page is displayed.

2. Enter the current password, set a new password, and confirm the new password.

New password and **Confirm password** must contain 6 to 15 ASCII characters.

3. Click **Submit**.

---End

8.3 Date & Time

You can set the system time or synchronize the system time with the network. If the **Sync from network** check box is selected, the CPE regularly synchronizes the time with the server. If daylight saving time (DST) is enabled, the CPE also adjusts the system time based on the DST time.

To set the date and time:

1. Choose **System > Date & Time**.
The **Settings** page is displayed.
2. Click **Set manually**.
3. Set **Local time** or click **Sync from PC**.
4. Click **Submit**.

---End

To synchronize the time with the network:

1. Choose **System > Date & Time**.
The **Settings** page is displayed.
2. Click **Sync from network**.
3. Set **Primary NTP server**, which is the primary server for time synchronization.
4. Set **Secondary NTP server**, which is the secondary server for time synchronization.
5. Set **Time zone**.

Different countries and regions have their own time zones. You can select a time zone from the drop-down list.

6. Select the **Daylight saving time** check box.
7. Click **Submit**.

---End

8.4 Diagnosis

If the CPE is not functioning correctly, you can use the diagnosis tools on the **Diagnosis** page to preliminarily identify the problem so that actions can be taken to solve it. The CPE supports SSH diagnostics. If this function is required, contact Huawei via mobile@huawei.com.

8.4.1 Ping

If the CPE fails to access the Internet, run the **ping** command to preliminarily identify the problem. To do so:

1. Choose **System > Diagnosis**. On the **Diagnosis** page, set **Method** to **Ping**.
The **Ping** page is displayed.
2. Enter the domain name in the **Target IP or domain** field, for example, www.google.com.
3. Set **Packet size** and **Timeout**, and select the **Enable** check box next to **Do not fragment**.
4. Click **Ping**.
5. Wait until the **ping** command is executed.

The execution results are displayed in the **Results** box.

---End

8.4.2 Traceroute

If the CPE fails to access the Internet, run the **traceroute** command to preliminarily identify the problem. To do so:

1. Choose **System > Diagnosis**. On the **Diagnosis** page, set **Method** to **Traceroute**. The **Traceroute** page is displayed.
2. Enter the domain name in the **Target IP or domain** field, for example, www.google.com.
3. Set **Maximum hops** and **Timeout**.
4. Click **Traceroute**.
5. Wait until the **traceroute** command is executed.

The execution results are displayed in the **Results** box.

---End

8.4.3 System Check

If the CPE is not functioning correctly, you can use the System Check tool to preliminarily identify the problem. To do so:

1. Choose **System > Diagnosis**. On the **Diagnosis** page, set **Method** to **System check**.
The **System Check** page is displayed.
2. Click **Check**.
3. Wait until the system check is performed.

The possible causes of the CPE problem are displayed on the page.

4. Click **Export** to export the detailed information to the computer. The follow table lists the exported files and their description.

File Name	Description
check_items.txt	Lists of the items on the web interface
operateLog_export.txt	Operation logs
traceLog_export.txt	System logs
router_ver.txt	Details of the router version
modem_ver.txt	Details of the modem version
sysmod.txt	System mode
boot.log	Boot log
curcfg.xml	Current configuration file
defaultcfg.xml	Default configuration file
arp.txt	ARP table
route.txt	Routing table
ps.txt	Process information
top.txt	System resource usage information
mount.txt	System mount information
wlctl_status.txt	Wi-Fi startup information
wlctl_isup.txt	Indicates whether Wi-Fi is on
wlctl_scanresults.txt	Access points within range
iptables.txt	Filter rules of iptables
iptables_nat.txt	NAT rules of iptables
eatables.txt	Filter rules of eatables
ifconfig.txt	Network adapter information
brctl.txt	Bridge information
plt.log	System kernel log
pltcheck.log	System self-check log

- If necessary, send the detailed information to maintenance personnel.

---End

8.4.4 Wireless Status Check

This page displays information about the wireless network status, such as the public land mobile network (PLMN), service status, RSSI, and roaming status.

To view the wireless status:

1. Choose **System > Diagnosis**.
2. On the Method page, set **Method** to **Wireless status check**.

The **RESULTS** page is displayed.

----End

8.5 Logs

Logs record user operations and key running events. To view logs:

1. Choose **System > Logs**.

The **Logs** page is displayed.

2. Select the corresponding log level from the **Log level** drop-down list.

The number of logs of this level is displayed to the right of the drop-down list, and the logs of this level are displayed below. You can view up to 500 of the latest logs.

3. Select the operation mode.

- **Clear**: Clear all logs in the CPE.
- **Export**: Export all logs in the CPE to a file in the computer.

----End

8.6 System Notification

This page allows you to configure the notification methods of key device status changes.

1. Choose **System > System Notification**.

The **System Notification** page is displayed.

2. Set **Frequency**, **Web popup receiving IP** (optional), **Send SMS notification to**, and **Forward SMS from** (optional).
3. When **Web popup receiving IP** is left blank, notifications are randomly sent to connected clients.
4. Message test, forwarding, and notification settings take effect only after the **Send SMS notification to** setting takes effect.
5. Configure the notification settings for each **Events**.
6. Click **Submit**.

----End

9

FAQs

The POWER indicator does not turn on.
<ul style="list-style-type: none">• Make sure the power cable is connected and the CPE is powered on.• Make sure the power adapter is compatible with the CPE.
Fails to log in to the web UI.
<ul style="list-style-type: none">• Make sure the CPE has started.• Check that the network cable is connected to the CPE and computer.• Check that the IP address of the computer is correctly set. <p>If the problem persists, contact an authorized local service provider.</p>
The CPE fails to search for wireless networks.
<ul style="list-style-type: none">• Check that the power adapter is connected.• Check that the CPE is placed in an open area that is far from obstructions, such as concrete or wooden walls.• Check that the CPE is placed far from electrical household appliances that generate strong electromagnetic fields, such as microwave ovens, refrigerators, and satellite dishes. <p>If the problem persists, contact an authorized local service provider.</p>
The power adapter of the CPE has overheated.
<ul style="list-style-type: none">• The CPE overheats after being used for a long period of time. Therefore, power off the CPE when you are not using it.• Check that the CPE is appropriately ventilated and shielded from direct sunlight.
The parameters are restored to their default values.
<ul style="list-style-type: none">• If the CPE unexpectedly powers off while being configured, the parameters may be restored to their default values.• After configuring the parameters, download the configuration file to quickly restore the CPE to the desired settings.

10 Acronyms and Abbreviations

AES	Advanced Encryption Standard
ALG	Application Layer Gateway
CPE	Customer-Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Server/Domain Name System
HTTP	Hypertext Transfer Protocol
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
NAT	Network Address Translation
DST	Daylight Saving Time
NTP	Network Time Protocol
PBC	Push Button Configuration
PIN	Personal Identification Number
USIM	Universal Subscriber Identity Module
SIP	Session Initiation Protocol
SN	Serial Number
SSID	Service Set Identifier
WAN	Wide Area Network
WEP	Wired Equivalent Privacy

WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA-PSK	Wi-Fi Protected Access-Pre-Shared Key
WPS	Wi-Fi Protected Setup

11 Copyright Notice and Warranty Disclaimer

This product incorporates open source software components covered by the terms of third party copyright notices and license agreements contained below.

1. Samba

Copyright© Andrew Tridgell 2004-2009

GNU General Public License V2.0

<http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html>

2. DJV Image and Movie Viewersg

Copyright© 2004-2009 Darby Johnston

<http://djh.sourceforge.net/legal.html>

BSD License/ Modified BSD License

<http://www.opensource.org/licenses/bsd-license>

3. EasySoap++

Copyright© 2001 David Crowley; SciTegic, Inc.

GNU Library or "Lesser" General Public License V2.0

<http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html>

4. Open BSD

Copyright©1996-2011 OpenBSD

BSD License/ Modified BSD License

<http://www.opensource.org/licenses/bsd-license>

5. m2sc

Copyright© 2009 Google

<http://code.google.com/p/m2sc/>

GNU General Public License 3.0

<http://www.gnu.org/licenses/gpl.html>

If you would like a copy of the GPL source code contained in this product shipped to you on CD for \$20, please contact us at mobile@huawei.com.