



TITAN4000

LTE Outdoor CPE
Quick User Guide V1.0

PLEASE READ THESE SAFETY PRECAUTIONS!

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 21cm between the radiator & your body.

FCC Warning

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

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

NOTE 1: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

NOTE 2: Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

1. Overview

The TITAN4000 is highly innovative and patented LTE outdoor CPE product designed to enable quick and easy LTE fixed data service deployment for residential and SOHO customers. It provides high speed LAN services to end users who need both bandwidth and multi-media data service in enterprise or home. It can also be used to support wireless fall back service.



1.1. User Interface Specification

Model	Description & User Interface
TITAN4000	- 1 RJ45 10/100/1000M LAN port - SYS, MOD, SIM, ETH, Wi-Fi, RF (5 Signal intensity LEDs) - PoE DC 48V, Power < 18 Watts (Average) - Dimensions: 300 mm (L) × 290 mm (W) × 97 mm (D) - Weight: <5Kg - Operating Temperature: -40°C to 55°C - Storage Temperature: -40°C to 85°C

2. Getting Started

2.1. Packing list and CPE Unit

Upon receiving the product, please unpack the product package carefully. Each product is shipped with the following items:

Table 2-1 Packing List

Products	Quantity
CPE Unit	1
Clamp	2
Mounting brackets	1
PoE Adapter	1
Power cord 1.5M	1
Quick user guide	1

If you find any of the items missed, please contact your local distributor immediately.

2.2. Installing the Equipment



Open the SIM card cover, insert the SIM card and connected the ETH cable.



The user should use SFTP CAT5E Ethernet cable and connect to the appropriate LAN port

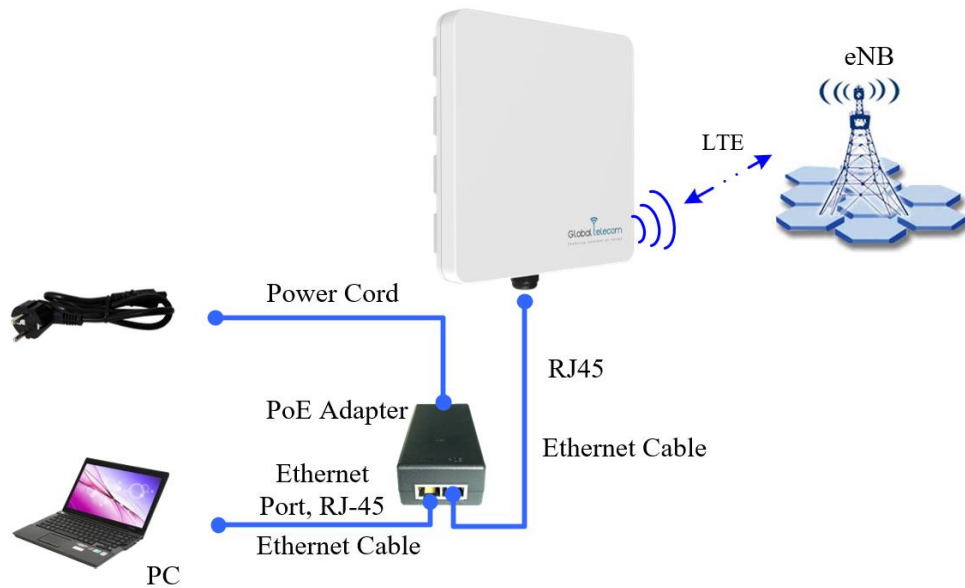
■ Mounting Bracket



■ Using clamps to fixed.



■ Device logic connection



■ LED Display

LED	Function	Description
SYS	System run indicator	Solid green – Device is in normal operation.
MOD	WAN port status	OFF – NO wireless network access. Solid Green – WAN data transmission in progress
SIM	SIM card indicator	Light is on – SIM card state is ready, Blinking Green – SIM card is error.
ETH	LAN port status	Solid Green – LAN port is up. Blinking Green –LAN port in working.
Wi-Fi	Wi-Fi indicator	Light is on –Wi-Fi is on.
RF (5LEDs)	RF Signal Strength	5 level signal strengths indication by 5 green LEDs. 1st Green LED: $-115\text{dBm} < \text{RSRP}$ 2nd Green LED: $-115\text{dBm} \leq \text{RSRP} < -105\text{dBm}$ 3rd Green LED: $-105\text{dBm} \leq \text{RSRP} < -95\text{dBm}$ 4th Green LED: $-95\text{dBm} \leq \text{RSRP} < -85\text{dBm}$ 5th Green LED: $-85 \leq \text{RSRP}$

3. Managing the CPE Device

3.1. WEB Login

User can access the dongle management GUI using a Web browser from a local PC connected to device LAN port. The user should ensure that the connected PC have acquired IP address via DHCP from the device. After IP connectivity is established between the PC and window CPE device, the user may launch a Web browser and specify Http://192.168.0.1 in the address bar, the default home page will appear. Note the default password is “admin”.

Log in to TITAN4000

Please enter your login password

Password:

Log in

Dashboard | Network | LAN | VPN | Security | Applications | UPnP | Maintenance | Logout | Reboot

Dashboard

LTE Information

Manufacturer	Global Telecom	UL/DL Bandwidth	- / - KHz
Model Name	TITAN4000	UL/DL Earfcn	- / -
Serial Number		UL/DL Throughput	0 bps / 0 bps
IMEI		Media State	Not Searching
RSRP	- dBm	Connection Time	0 sec
RSRQ	- dB	IPv4 Address	-
SINR	- dB	IPv6 Address	-

Networking

MAC Address	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Local DNS	

3.2. System configuration

■ DMZ

This menu allows user to configure the DMZ setting for CPE in router mode. Web server, Telnet/SSH and Ping Service port can be exempted from DMZ mapping if required. By enabling DMZ option will make the specified local LAN host (DMZ IP) exposed to Internet.

Demilitarized Zone (DMZ) | Help

DMZ

DMZ Enable Status ☐ Enable

DMZ Host IP Address 192.168.0.

Exclude Web Server Port ☒ Enable

Exclude Telnet/SSH Port ☒ Enable

Exclude Ping Service ☒ Enable

Save & Apply **Cancel**

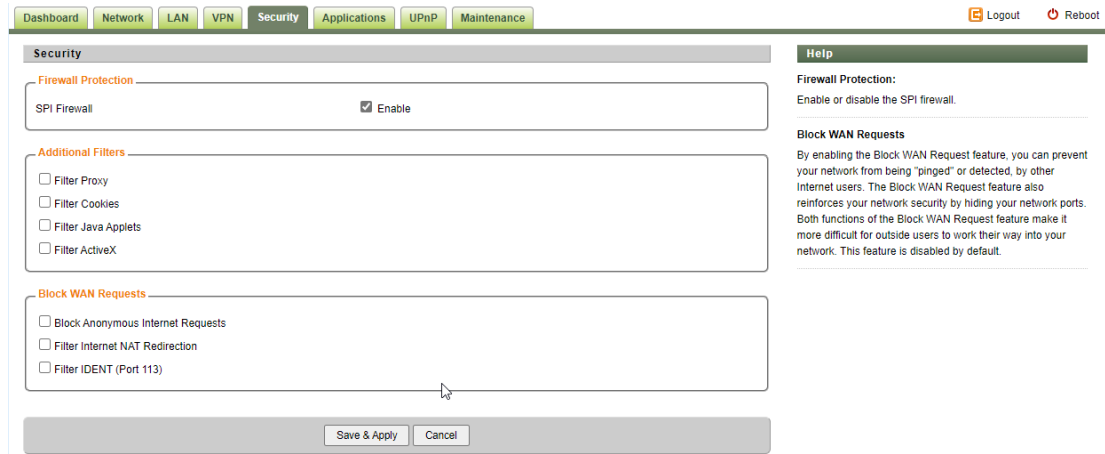
Help

DMZ:

Enabling this option will expose the specified host to the Internet. All ports will be accessible from the Internet.

■ Security

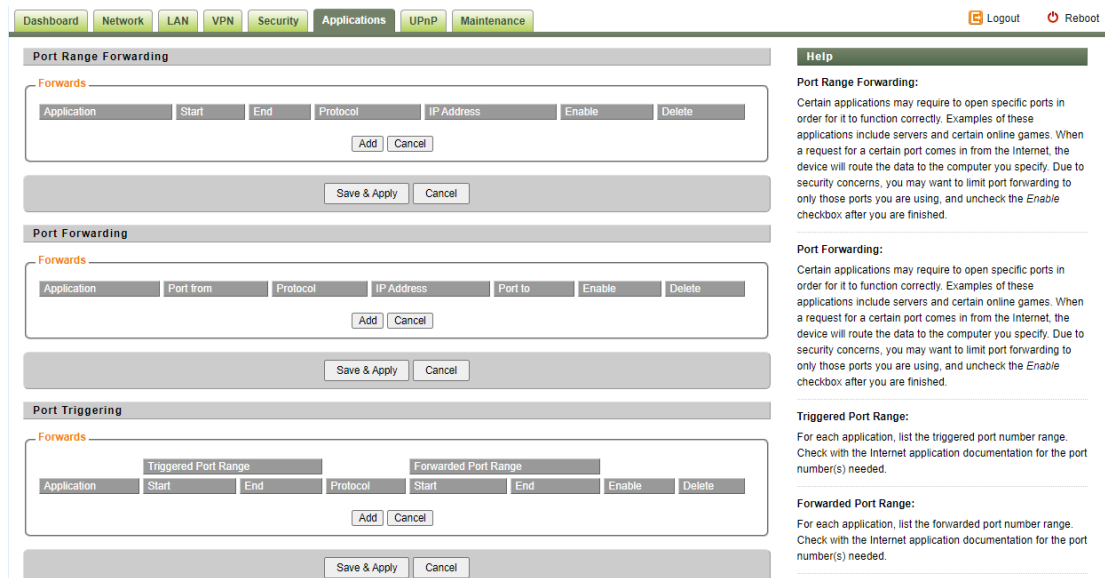
This page allows user to configure the security setting.



The screenshot shows the 'Security' configuration page. At the top, there is a navigation bar with tabs: Dashboard, Network, LAN, VPN, Security (selected), Applications, UPnP, and Maintenance. On the right, there are links for Logout and Reboot. The main content area is titled 'Security' and contains three sections: 'Firewall Protection', 'Additional Filters', and 'Block WAN Requests'. The 'Firewall Protection' section has a checkbox for 'SPI Firewall' which is checked and labeled 'Enable'. The 'Additional Filters' section has four checkboxes: 'Filter Proxy', 'Filter Cookies', 'Filter Java Applets', and 'Filter ActiveX', all of which are unchecked. The 'Block WAN Requests' section has three checkboxes: 'Block Anonymous Internet Requests', 'Filter Internet NAT Redirection', and 'Filter IDENT (Port 113)', all of which are unchecked. At the bottom of the main content area, there are 'Save & Apply' and 'Cancel' buttons. On the right side, there is a 'Help' section with two subsections: 'Firewall Protection' and 'Block WAN Requests'. The 'Firewall Protection' subsection explains that users can enable or disable the SPI firewall. The 'Block WAN Requests' subsection explains that enabling this feature can prevent the network from being pinged or detected by other Internet users and reinforces network security by hiding network ports.

■ Applications

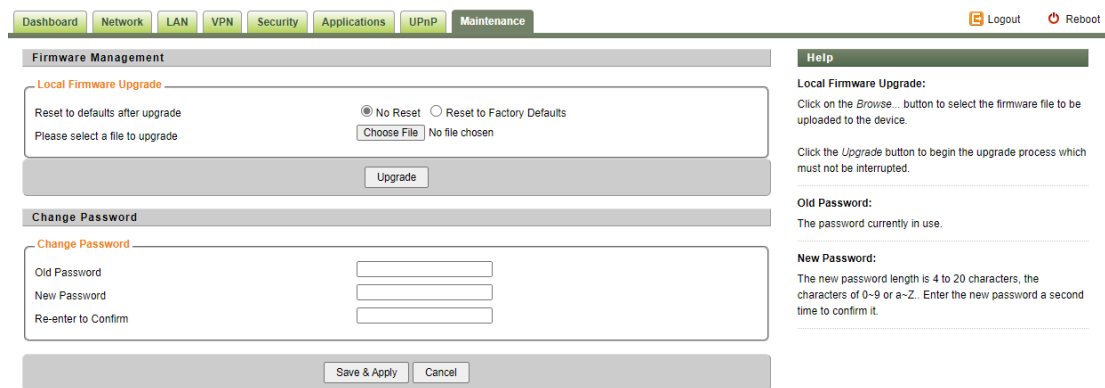
This menu allows user to configure the port forwarding rules for the CPE in router mode.



The screenshot shows the 'Applications' configuration page. At the top, there is a navigation bar with tabs: Dashboard, Network, LAN, VPN, Security, Applications (selected), UPnP, and Maintenance. On the right, there are links for Logout and Reboot. The main content area is titled 'Applications' and contains three sections: 'Port Range Forwarding', 'Port Forwarding', and 'Port Triggering'. Each section has a 'Forwards' table with columns for Application, Start, End, Protocol, IP Address, Port to, Enable, and Delete. The 'Port Range Forwarding' section has an 'Add' button and a 'Cancel' button. The 'Port Forwarding' section has an 'Add' button and a 'Cancel' button. The 'Port Triggering' section has an 'Add' button and a 'Cancel' button. At the bottom of each section, there are 'Save & Apply' and 'Cancel' buttons. On the right side, there is a 'Help' section with three subsections: 'Port Range Forwarding', 'Port Forwarding', and 'Triggered Port Range'. The 'Port Range Forwarding' subsection explains that certain applications may require open specific ports and that users should limit port forwarding to only those ports they are using. The 'Port Forwarding' subsection explains that certain applications may require open specific ports and that users should limit port forwarding to only those ports they are using. The 'Triggered Port Range' subsection explains that for each application, users should list the triggered port number range and check with the Internet application documentation for the port number(s) needed.

■ Maintenance

This page allows user to update the device firmware version, rest the device to factory setting and reboot the device.



Firmware Management

Local Firmware Upgrade

Reset to defaults after upgrade ☒ No Reset ☐ Reset to Factory Defaults

Please select a file to upgrade No file chosen

Change Password

Change Password

Old Password

New Password

Re-enter to Confirm

Help

Local Firmware Upgrade:

Click on the *Browse ...* button to select the firmware file to be uploaded to the device.

Click the *Upgrade* button to begin the upgrade process which must not be interrupted.

Old Password:

The password currently in use.

New Password:

The new password length is 4 to 20 characters, the characters of 0-9 or a-z. Enter the new password a second time to confirm it.

4. Troubleshooting

Q1: My PC cannot connect to the CPE.

- Check the PoE adapter LED is on and your PC LAN port is working.

Q2: My CPE networking is not working properly.

- Check and make sure you are within LTE coverage.

Q3: Unable to connect internet while the device is already connected to LTE network.

- Check and verify your computer has the ETH adapter installed and enabled. Unplug the PC Lan port and reconnect again if required.

Manufacturer : Global Telecom Corp

Address : 17901 Von Karman Ave, Suite 600, Irvine, California 92614

Website: www.GlobalTelecomUS.com