CBRS DTU

User manual v1.0

4G Data Transmit Unit

Brand Name	Sirius Fly Pro
Product Description	CBRS DTU
Model Name	DTU-B048-101

Table of contents

FCC compliance statement

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.

changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

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.

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 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Introduction

1.1 Purpose

This document provides guidance on how to use and manage CBRS DTU.

1.2 References

[1] WINNF-TS-0016 Version V1.2.4, “Spectrum Access System (SAS) - Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification”.

[2] WINNF-TS-0112 Version V1.9.1, “Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band”.

[3] Electronic Code of Federal Regulations, Title 47, Chapter I, Subchapter D, Part 96.

[4] TR069 V1.4, “CPE WAN Management Protocol”.

Product overview

2.1 Panel layout

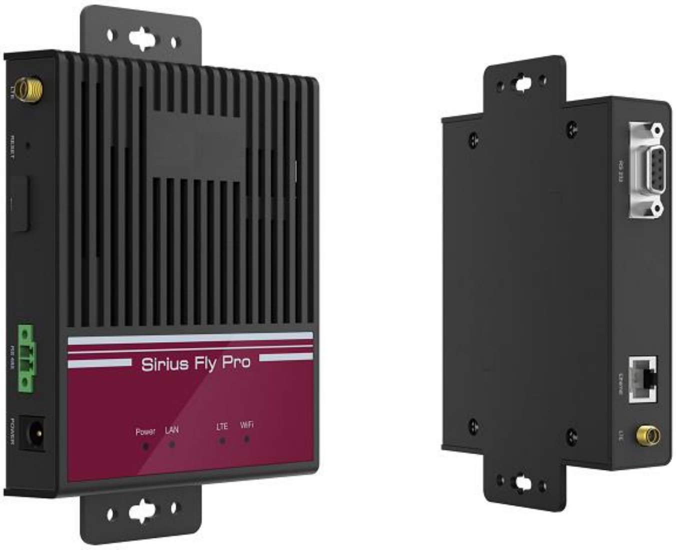
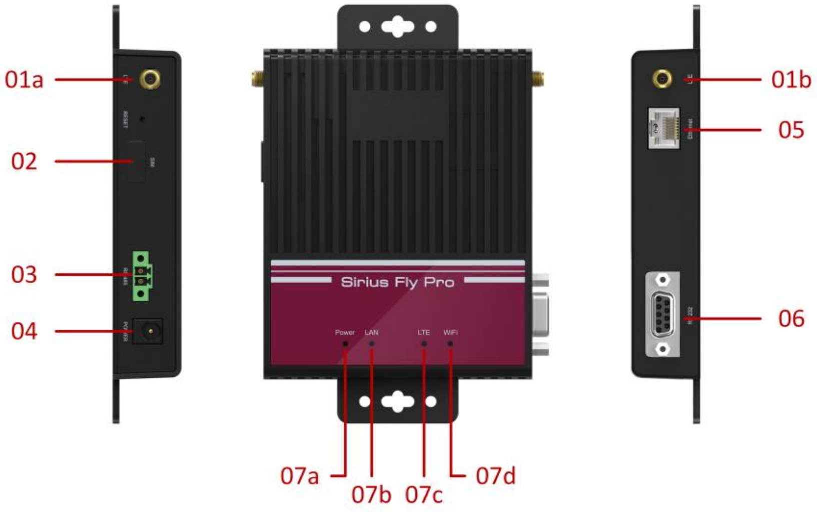


Figure 1:Front view and rear view of DTU

2.2 Interface definition



01a: LTE external antenna connector
01b: LTE external antenna connector
02: SIM card socket
03: RS485 port
04: Power socket
05: RJ45
06: RS232 port
07a: Power LED indicator
07b: Network LED indicator
07c: LTE LED indicator
07d: WIFI LED indicator

Figure 2: Interface panel

Quick installation

3.1 Position Your Sirius Fly

•The product should not be located where it will be exposed to moisture or excessive heat.

• Place Sirius Fly in a location where it can be connected to devices as well as to a power source.

• Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.

• The Sirius Fly can be placed on a Factory Field or Moveable device like AGV.

• Keep the Sirius Fly away from the strong electromagnetic radiation and the device of electromagnetic sensitive

3.2 Connect Your Sirius Fly

Follow the steps below to connect your Sirius Fly.

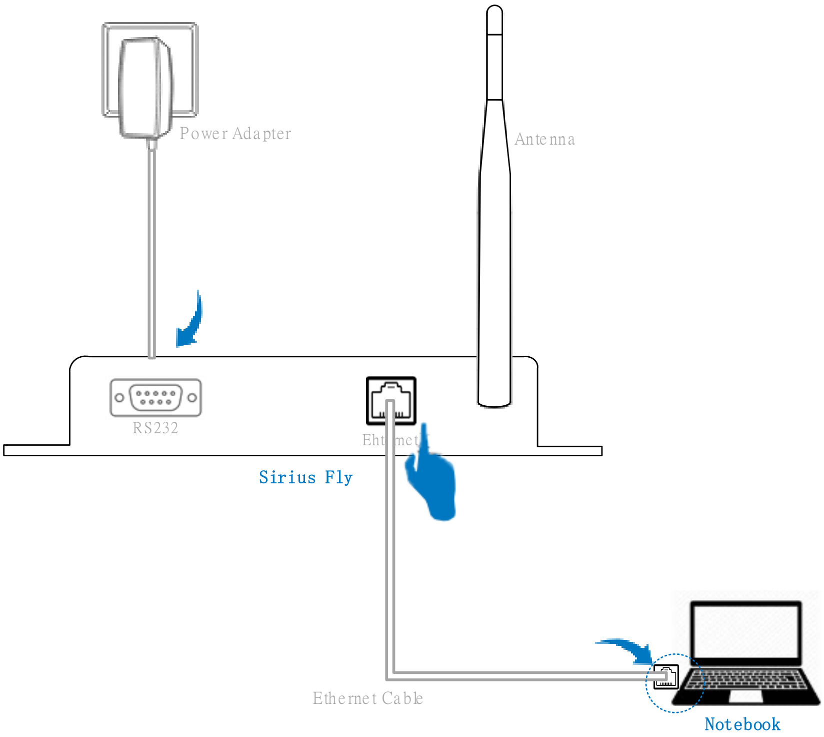


Figure 3: Connect to DTU

3.3 Access DTU

DTU offer two kinds of user account with different authorization. For more details refer to clause “User management”. To log on to DTU:

a) Launch a supported web browser.

> **Note:**DTU is optimized for the following browser:
>
> - Google Chrome (Version: **)
> - Mozilla Firefox (Version: **)
> - Microsoft Edge (Version: **)

b) In the web browser address bar, specify the gateway IP address (Default value should be 192.168.1.1) which automatically distributed via DHCP server.

c) Enter an user name and password (Refer to clause "User management").

d) Click Login to access DTU.

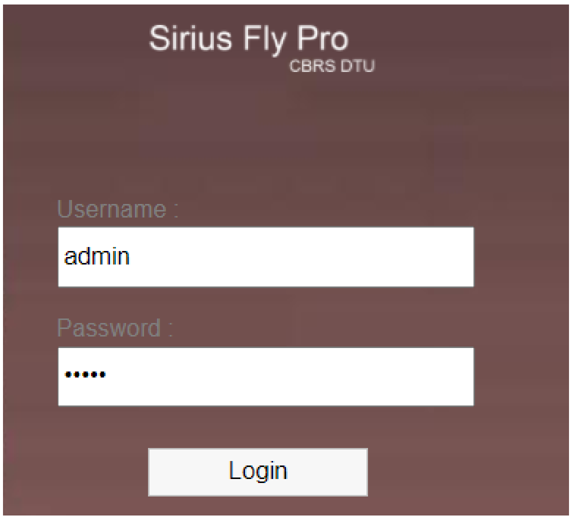


Figure 4: Login to DTU

User management

4.1 User authorization

To limit and control access to different features, DTU provides two kinds of user account (Normal user and Administrator) with different authorization. Following table shows corresponding authorization for each user.

Table 1: Authorization for each user

Features	Normal user	Administrator
Overview	√	√
Statistics	√	√
Settings->LTE	×	√
Settings->WIFI	×	√
Settings->LAN	×	√
Settings->Firewall	×	√
Settings->TR069	×	√
Settings->Ser2Net	×	√
Settings->Application Service	×	√
Settings->System	√ (Only support System->Diagnostics and System->System Reboot)	√

4.2 Default user account

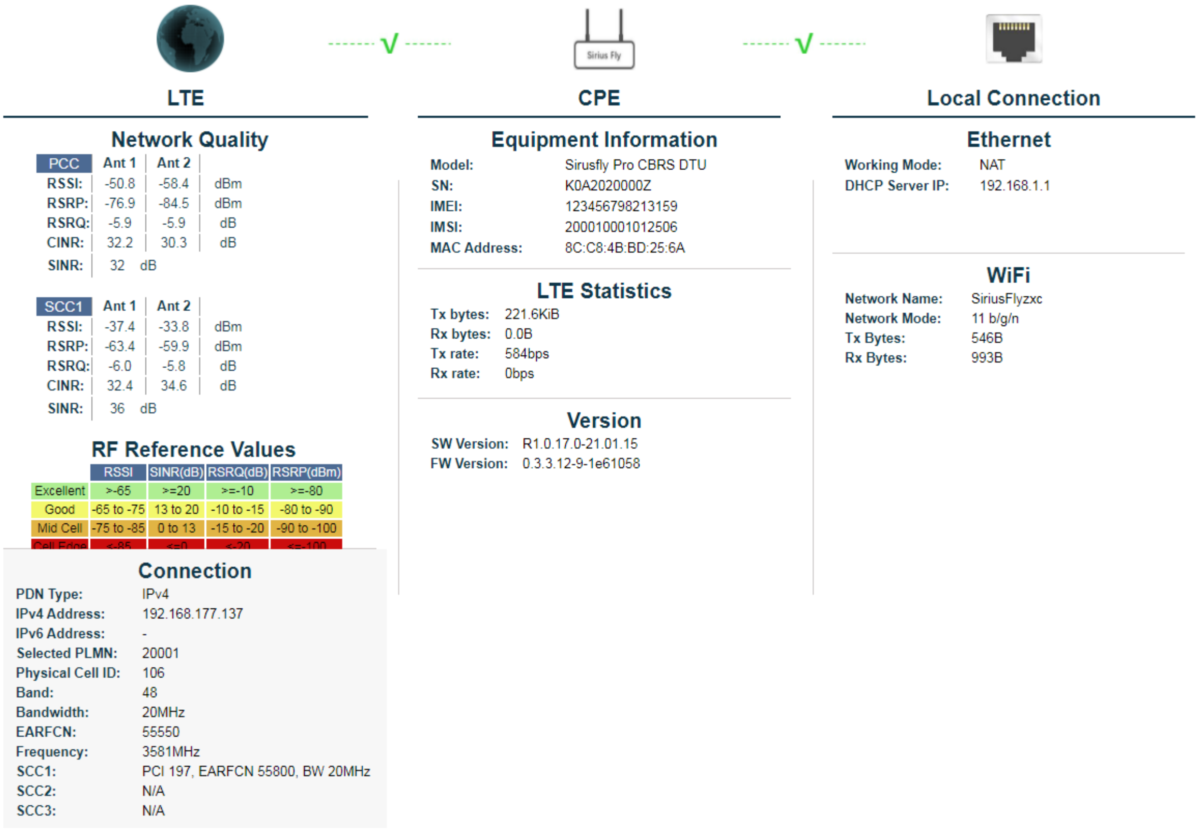
Table 2: Default user account

Role	Username	Password
Normal user	user	password
Administrator	admin	admin

Equipment status

5.1 Overview

In Overview page there are properties which would refresh automatically and allow you to determine the running status of DTU (As table “Overview page details” lists).



LTE

Network Quality

PCC	Ant 1	Ant 2	
RSSI:	-50.8	-58.4	dBm
RSRP:	-76.9	-84.5	dBm
RSRQ:	-5.9	-5.9	dB
CINR:	32.2	30.3	dB
SINR:	32 dB		

SCC1	Ant 1	Ant 2	
RSSI:	-37.4	-33.8	dBm
RSRP:	-63.4	-59.9	dBm
RSRQ:	-6.0	-5.8	dB
CINR:	32.4	34.6	dB
SINR:	36 dB		

RF Reference Values

	RSSI	SINR(dB)	RSRQ(dB)	RSRP(dBm)
Excellent	>-65	>=20	>=-10	>=-80
Good	-65 to -75	13 to 20	-10 to -15	-80 to -90
Mid Cell	-75 to -85	0 to 13	-15 to -20	-90 to -100
Cell Edge	<-85	<=0	<-20	<=-100

Connection

PDN Type:	IPv4
IPv4 Address:	192.168.177.137
IPv6 Address:	-
Selected PLMN:	20001
Physical Cell ID:	106
Band:	48
Bandwidth:	20MHz
EARFCN:	55550
Frequency:	3581MHz
SCC1:	PCI 197, EARFCN 55800, BW 20MHz
SCC2:	N/A
SCC3:	N/A

CPE

Equipment Information

Model:	Sirusfly Pro CBRS DTU
SN:	K0A2020000Z
IMEI:	123456798213159
IMSI:	200010001012506
MAC Address:	8C:C8:4B:BD:25:6A

LTE Statistics

Tx bytes:	221.6KiB
Rx bytes:	0.0B
Tx rate:	584bps
Rx rate:	0bps

Version

SW Version:	R1.0.17.0-21.01.15
FW Version:	0.3.3.12-9-1e61058

Local Connection

Ethernet

Working Mode:	NAT
DHCP Server IP:	192.168.1.1

WiFi

Network Name:	SiriusFlyzxc
Network Mode:	11 b/g/n
Tx Bytes:	546B
Rx Bytes:	993B

Figure 5: Properties on Overview page

Table 3: Overview page details

Property	Description
Network Quality	• **RSSI** – Received Signal Strength Indication per antennas. • **RSRP** – Reference Signal Receiving Power per antennas. • **RSRQ** – Reference Signal Receiving Quality per antennas. • **CINR** – Carrier to Interference plus Noise Ratio per antennas. • **SINR** – Signal to Interference plus Noise Ratio.
Connection	• **PDN Type** – PDN connection type (IPv4 / IPv6 / IPv4&IPv6) which assigned for Internet allocation.

	• **IPv4 Address** – IPv4 address of PDN connection which assigned for Internet allocation. • **IPv6 Address**– IPv6 address of PDN connection which assigned for Internet allocation. • **Selected PLMN** – PLMN Id of the eNB which DTU attached. • **Physical Cell Id** – Physical cell Id of the eNB. • **Band** – Operating band of the Enb (e.g. 48). • **BandWidth** –Channel bandwidth (e.g. 20MHz). • **EARFCN** – E-UTRA Absolute Radio Frequency Channel Number which eNB using for Tx/Rx. • **Frequency** – Radio Frequency which eNB using for Tx/Rx. • **SCC1** – Secondary component carrier #1 under CA scenario. • **SCC2** – Secondary component carrier #2 under CA scenario. • **SCC3** – Secondary component carrier #3 under CA scenario.
Equipment Information	• **SN** – Serial number. • **IMEI** – International Mobile Equipment Identity. • **IMSI** – International Mobile Subscriber Identity. • **MAC Address** – MAC address.
LTE Statistics	• **Tx bytes** – Total Tx bytes(Uplink) on LTE radio interface. • **Rx bytes** – Total Rx bytes(Downlink) on LTE radio interface. • **Tx rate** – Tx rate(Uplink) on LTE radio interface. • **Rx rate** – Rx rate(Downlink) on LTE radio interface.
Version	• **SW version** – Software version. • **FW version** – Modem FW version.
Ethernet	• **Working Mode** – Working mode of DTU applied to network packets transfer(NAT/Bridge). • **DHCP Server IP** – DHCP Server IP(Gateway IP) of DTU.

5.2 Statistics

In Statistics page you can observe performance statistics about system, radio network visually, and PDN connection status of all APNs.

- CPU usage and memory usage:

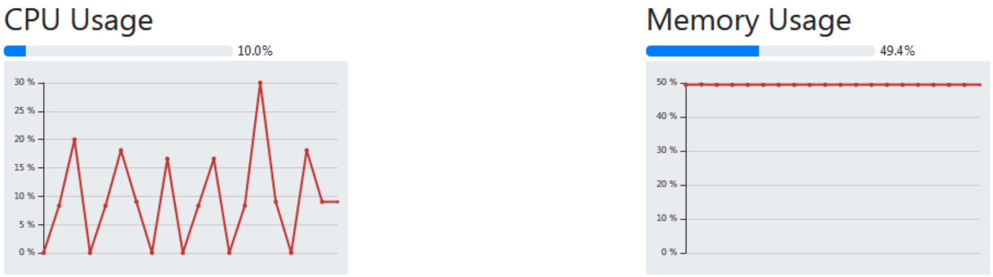
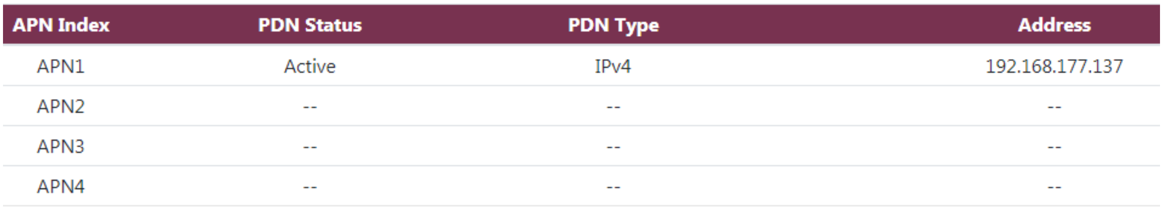


Figure 6: CPU Usage & Memory Usage

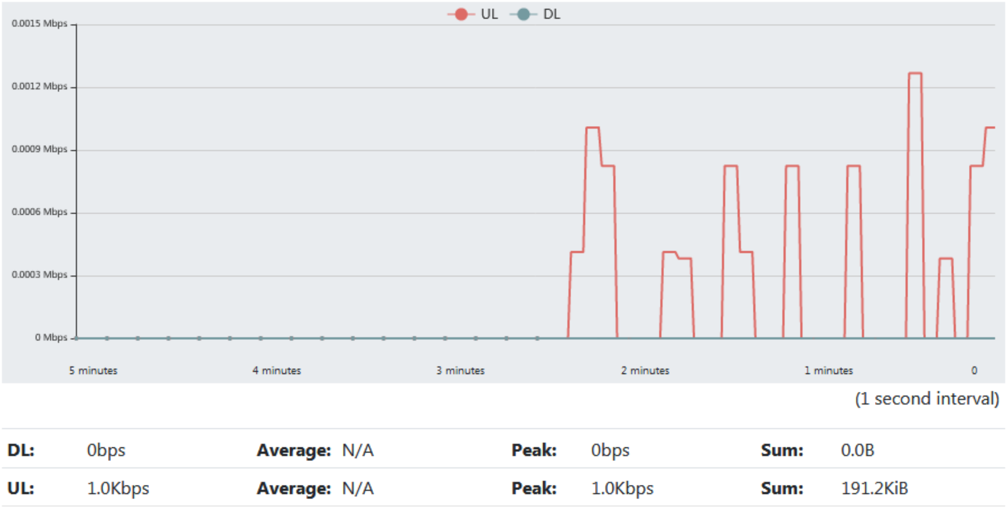
- APN list:



APN Index	PDN Status	PDN Type	Address
APN1	Active	IPv4	192.168.177.137
APN2	--	--	--
APN3	--	--	--
APN4	--	--	--

Figure 7: APNs status

- Bandwidth statistics:

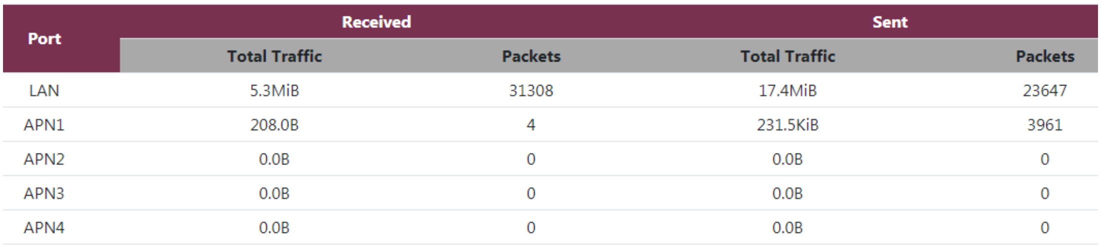


(1 second interval)

DL:	0bps	**Average:**	N/A	**Peak:**	0bps	**Sum:**	0.0B
UL:	1.0Kbps	**Average:**	N/A	**Peak:**	1.0Kbps	**Sum:**	191.2KiB

Figure 8: Bandwidth statistics

- Throughput statistics:



Port	Received		Sent	
	Total Traffic	Packets	Total Traffic	Packets
LAN	5.3MiB	31308	17.4MiB	23647
APN1	208.0B	4	231.5KiB	3961
APN2	0.0B	0	0.0B	0
APN3	0.0B	0	0.0B	0
APN4	0.0B	0	0.0B	0

Figure 9: Throughput statistics

Functional Configurations

6.1 LTE

6.1.1 APN Settings

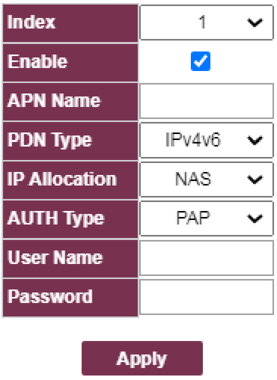
DTU provides up to 4 APNs. Each APN is assigned for specific purpose.

Table 4: APN assignment

APN Index	Assignment in NAT	Assignment in Bridge
1	Management	Internet (For LAN port access)
2	Internet (For LAN port access)	Open
3	TR069 service	Open
4	Open	Open

➢ To enable or disable the 4 APN, or edit the APN configurations:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to***Settings>LTE->APN settings*** page.



Index	1
Enable	☑
APN Name	
PDN Type	IPv4v6
IP Allocation	NAS
AUTH Type	PAP
User Name	
Password	

Figure 10: APN settings

- Selectspecified APN index and change APN parameters.

Table 5: APN parameters

Parameter	Description
Index	APN index (range: 1~4).

Enable	To enable or disable the selected APN.
APN Name	Access point name.
PDN Type	PDN connection type (IPv4 / IPv6 / IPv4&IPv6).
IP Allocation	IP Allocation method: - NAS, allocated via NAS protocol by EPC. - DHCP, allocated via DHCP protocol by DHCP server.
AUTH Type	Authentication type: - PAP - CHAP
User Name	User name for selected authentication type.
Password	Password for selected authentication type.

- Click the “Apply” button for modification take effect.

The APN List panel shows status of APN1 ~ APN4.

Table 6: APN properties

Property	Description
PDN Status	- Active, connection granted with IP allocation.
PDN Type	- IPv4 - IPv6 - IPv4&IPv6
Address	Assigned IP address.

The LTE Status panel shows status of LTE radio interface.

Table 7: LTE radio properties

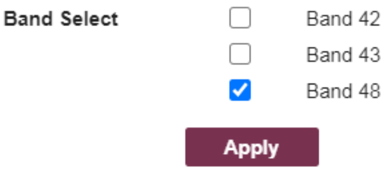
Property	Description
UICC State	- UICC Ready - NO UICC - Wait for PIN1
PLMN Search	- Success

	- Searching - Not Searching
PLMN Selected	PLMN Id of the eNB which DTU attached.
Physical CELL ID	Physical cell Id of the eNB.
ServCellState	- RCC IDLE - RRC CONNECTED
MCC	Mobile Country Code.
MNC	Mobile Network Code.
Cell ID	Cell Id of the eNB.

6.1.2 Scan Mode

DTU provides multiple scan mode applied to different cell selection scenarios, refer to ***Settings >LTE->Scan Mode*** page.

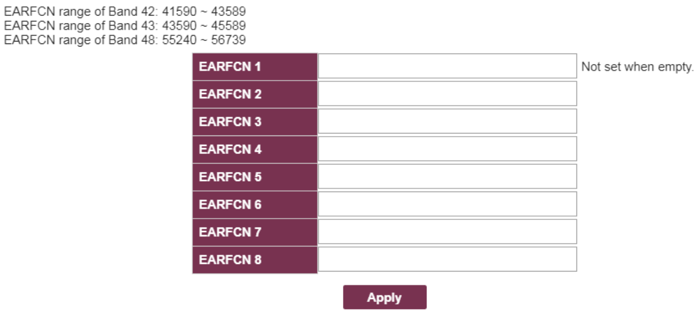
- CBRS DTU only support band 48.
- Full/Preferred band, DTU would execute Full band search including band 48.
- Band Lock, DTU would only search the selected bands.



Band Select
☐ Band 42
☐ Band 43
☑ Band 48

Figure 11: Band Lock settings

- EARFCN Lock, DTU would only search the specific EARFCNs which configured.

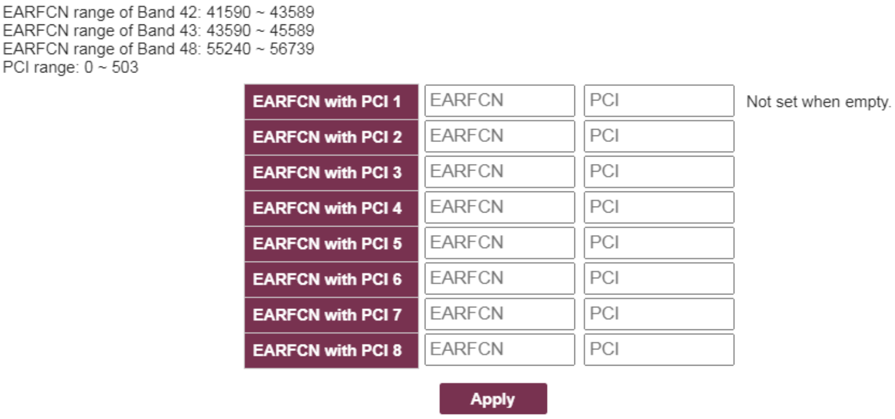


EARFCN range of Band 42: 41590 ~ 43589
EARFCN range of Band 43: 43590 ~ 45589
EARFCN range of Band 48: 55240 ~ 56739

EARFCN 1		Not set when empty.
EARFCN 2		
EARFCN 3		
EARFCN 4		
EARFCN 5		
EARFCN 6		
EARFCN 7		
EARFCN 8		

Figure 12: EARFCN Lock settings

- EARFCN with PCI, DTU would only search the specific EARFCNs with PCIs which configured.

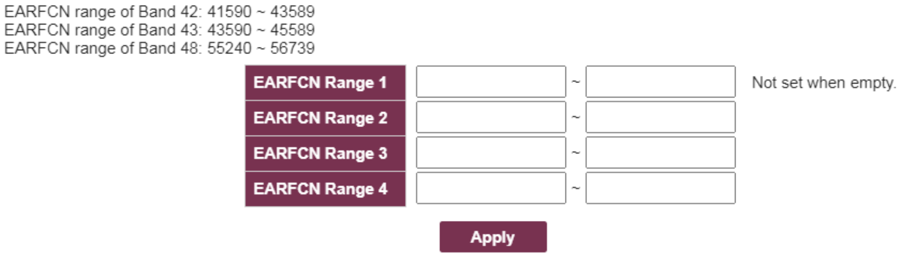


EARFCN range of Band 42: 41590 ~ 43589
EARFCN range of Band 43: 43590 ~ 45589
EARFCN range of Band 48: 55240 ~ 56739
PCI range: 0 ~ 503

EARFCN with PCI 1	EARFCN	PCI	Not set when empty.
EARFCN with PCI 2	EARFCN	PCI	
EARFCN with PCI 3	EARFCN	PCI	
EARFCN with PCI 4	EARFCN	PCI	
EARFCN with PCI 5	EARFCN	PCI	
EARFCN with PCI 6	EARFCN	PCI	
EARFCN with PCI 7	EARFCN	PCI	
EARFCN with PCI 8	EARFCN	PCI	

Figure 13: EARFCN with PCI Lock settings

- EARFCN Range Lock, DTU would only search the specific EARFCN ranges which configured.



EARFCN range of Band 42: 41590 ~ 43589
EARFCN range of Band 43: 43590 ~ 45589
EARFCN range of Band 48: 55240 ~ 56739

EARFCN Range 1		~		Not set when empty.
EARFCN Range 2		~		
EARFCN Range 3		~		
EARFCN Range 4		~		

Figure 14: EARFCN Range Lock settings

For "Full/Preferred band" scan, there are also particular parameters allow you to redefine the scan process.

Table 8: PLMN Search Configuration

Parameter	Description
Selection Mode	- Automatic network selection - Manual network selection - Manual to automatic fallback - Manual CSG selection
Operation Mode	- Normal searching - Emergency searching
PLMN ID	PLMN ID which DTU would only choose to attach(Applied to "Manual network selection").
Roaming Option	- Allowed, DTU is allowed to access network with PLMN different with HPLMN. - Not allowed

Power Scan	- First Detected Cell - Strongest Cell
Fast Scan	- Normal Scan - Fast Power Scan
ECI	E-UTRAN Cell Identifier.
Minimum RSRP	- Valid range: -150 ~ -100 dBm - Default value: 0, disable this filter option.

6.1.3 SIM PIN

DTU allows user to manage PIN code of SIM card, refer to ***Settings >LTE->SIM PIN*** page.

- PIN Information

Table 9: PIN information

Property	Description
PIN Status	- PIN NOT INITIALIZED - PIN ENABLED NOT VERIFIED - PIN ENABLED VERIFIED - PIN DISABLED - PIN BLOCKED - PIN PERMANENTLY BLOCKED
RETRIES PIN	The number of retries left of PIN.
RETRIES PUK	The number of retries left of PUK.

- PIN Management, enable or disable PIN.
- PIN Change
- PIN Unlock

6.2 LAN Network

6.2.1 Connection Mode

DTU is preconfigured to work in **NAT mode** and act as a DHCP server on the LAN side. Therefore, all the clients get IP addresses allocated from DTU with specific address range. The default LAN IP configuration is as follows:

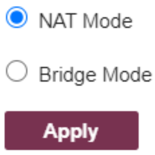
- LAN IP address/Gateway: 192.168.1.1
- Subnet mask: 255.255.255.0

To sets the LAN configuration parameters such as gateway IP, subnet mask and the enable DHCP flag, along with DHCP parameters, please refer to clause "6.2.2DHCP".

For **Bridge mode**, the Ethernet client device can get the WWAN interface IP directly via DHCP protocol.

➢ To change the connection mode:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to***Settings>LAN > Connection Mode***Page, choose the target mode.



● NAT Mode

○ Bridge Mode

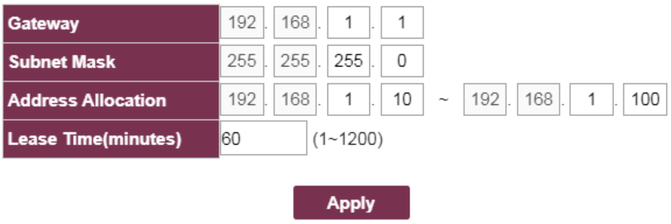
Figure 15: Connection Mode setting

- Click the "Apply" button for modification take effect.

6.2.2 DHCP

➢ To change the LAN DHCP settings:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to***Settings > LAN> DHCP***page, input new configurations.



Gateway	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
Address Allocation	192 . 168 . 1 . 10 ~ 192 . 168 . 1 . 100
Lease Time(minutes)	60 (1~1200)

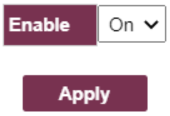
Figure 16: DHCP settings

- Click the “Apply” button for modification take effect.

6.2.3 IPv6

➢ To enable IPv6 function in LAN network:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to***Settings > LAN > IPv6***page, choose “On”.



Enable: On

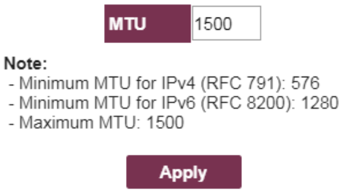
Figure 17: IPv6 setting

- Click the “Apply” button for modification take effect.

6.2.4 MTU

➢ To change MTU(Maximum Transmission Unit) size of Ethernet interface:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to***Settings > LAN> MTU***page, input the target MTU size (valid range: 68~1500).



MTU: 1500

Note:
- Minimum MTU for IPv4 (RFC 791): 576
- Minimum MTU for IPv6 (RFC 8200): 1280
- Maximum MTU: 1500

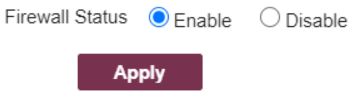
Figure 18: MTU setting

- Click the “Apply” button for modification take effect.

6.3 Firewall

6.3.1 Firewall Settings

Firewall settings include Port Filter and URL Filter. When disable Firewall, all rules in Port Filter and URL Filter would also be disabled.

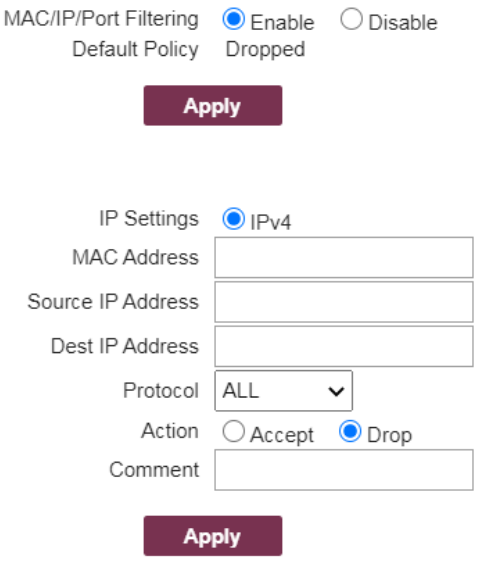


Firewall Status ● Enable ○ Disable

Figure 19: Firewall Settings

6.3.2 Port Filter

- To add new port filter rule:
  - Launch a web browser from a computer that is connected to DTU and access to web management system.
  - Go to***Settings > Firewall> Port Filter***page, input relevant filter parameters.



MAC/IP/Port Filtering ● Enable ○ Disable

Default Policy Dropped

IP Settings ● IPv4

MAC Address

Source IP Address

Dest IP Address

Protocol ALL

Action ○ Accept ● Drop

Comment

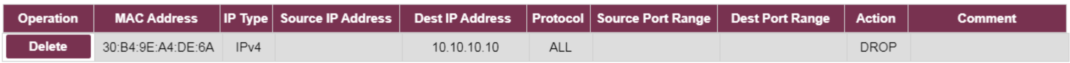
Figure 20: Port filter settings

Table 10: Rule parameters of port filter

Parameter	Description
IP Settings	- IPv4
MAC Address	MAC address of source network node.

Source IP Address	IP address of source network node.
Dest IP Address	IP address of destination network node.
Protocol	- ALL - TCP - UDP - ICMP
Action	- Accept - Drop
Comment	Extra description for rule.

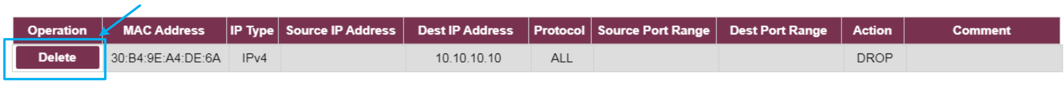
- Click the “Apply” button, and you can see new rule in active rules table.



Operation	MAC Address	IP Type	Source IP Address	Dest IP Address	Protocol	Source Port Range	Dest Port Range	Action	Comment
Delete	30:B4:9E:A4:DE:6A	IPv4		10.10.10.10	ALL			DROP	

Figure 21: Active port filter rules table

In active rules table, you can click “Delete” button to delete the rule directly.

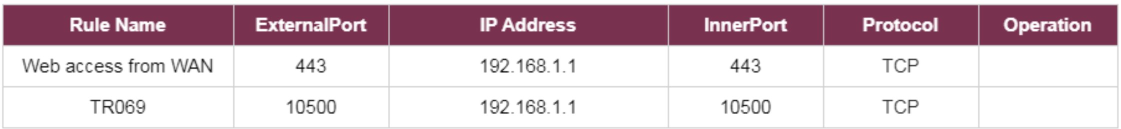


Operation	MAC Address	IP Type	Source IP Address	Dest IP Address	Protocol	Source Port Range	Dest Port Range	Action	Comment
Delete	30:B4:9E:A4:DE:6A	IPv4		10.10.10.10	ALL			DROP	

Figure 22: Delete port filter rule

6.3.3 Port Forward

To ensure web (https) and TR069 services working normally, two default port forward rules (Rule Name: Web access from WAN and TR069) were added when system boot up.

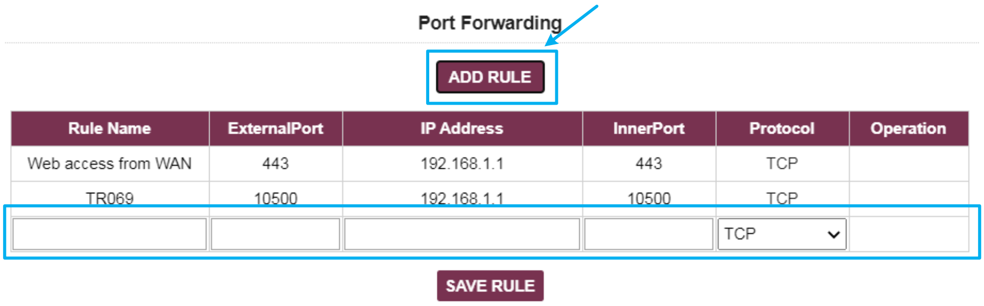


Rule Name	ExternalPort	IP Address	InnerPort	Protocol	Operation
Web access from WAN	443	192.168.1.1	443	TCP	
TR069	10500	192.168.1.1	10500	TCP	

Figure 23: Default port forward rules

➢ To add new port forward rule:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to ***Settings > Firewall > Port Forward***page, click “ADD RULE” button.



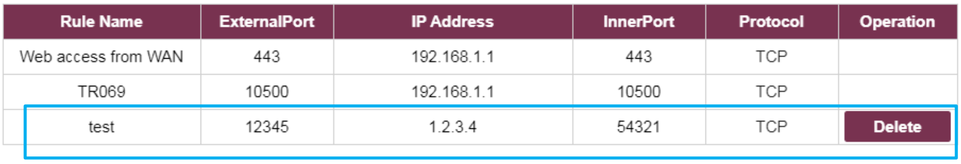
Rule Name	ExternalPort	IP Address	InnerPort	Protocol	Operation
Web access from WAN	443	192.168.1.1	443	TCP	
TR069	10500	192.168.1.1	10500	TCP	
				TCP	

Figure 24: Add new port forward rule

- Input relevant filter parameters.

Parameter	Description
Rule Name	Extra description.
ExternalPort	Original destination port of network packets.
IP Address	Forwarded destination IP address of network packets.
InnerPort	Forwarded destination port of network packets.
Protocol	- TCP - UDP

- Click the “SAVE RULE” button, and you can see new rule in active rules table.



Rule Name	ExternalPort	IP Address	InnerPort	Protocol	Operation
Web access from WAN	443	192.168.1.1	443	TCP	
TR069	10500	192.168.1.1	10500	TCP	
test	12345	1.2.3.4	54321	TCP	Delete

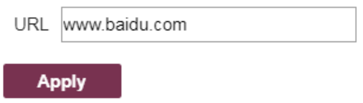
Figure 25: Active port forward rules table

In active rules table, you can also click “Delete” button to delete the rule directly.

6.3.4 URL Filter

➢ To add new URL filter rule:

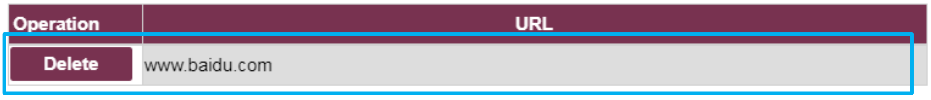
- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to ***Settings > Firewall > URL Filter***page, input target URL.



URL www.baidu.com

Figure 26: Add new URL filter rule

- Click the “Apply” button, and you can see new rule in active rules table.



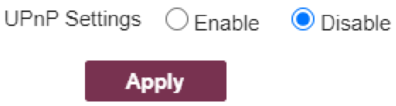
Operation	URL
Delete	www.baidu.com

Figure 27: Active URL filter rules table

In active rules table, you can also click “Delete” button to delete the rule directly.

6.3.5 UPnP

- To enable or disable UPnP service:
  - Launch a web browser from a computer that is connected to DTU and access to web management system.
  - Go to ***Settings > Firewall> UPnP***page,select target operation (Enable/Disable).



UPnP Settings ○ Enable ● Disable

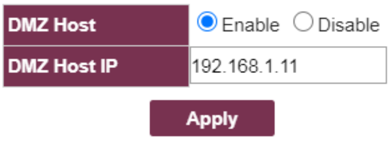
Figure 28: UPnP setting

  - Click the “Apply” buttonfor modification take effect.

6.3.6 DMZ Host

DMZ function is typically used in NAT mode. All network packets from WAN Internet interface would be forwarded to DMZ host IP directly.

- To enable or disable DMZ service:
  - Launch a web browser from a computer that is connected to DTU and access to web management system.
  - Go to ***Settings > Firewall > DMZ Host***page, select target operation (Enable/Disable) and input a valid DMZ host IP if enabled.



DMZ Host	● Enable ○ Disable
DMZ Host IP	192.168.1.11

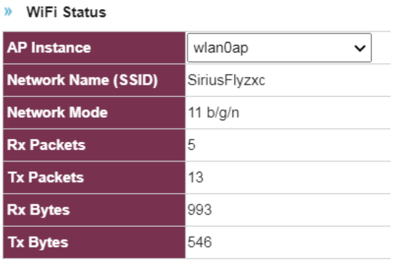
Figure 29: DMZ settings

- Click the “Apply” buttonfor modification take effect.

6.4 WIFI

6.4.1 AP Status

- Show WIFI AP statistics.



» WiFi Status

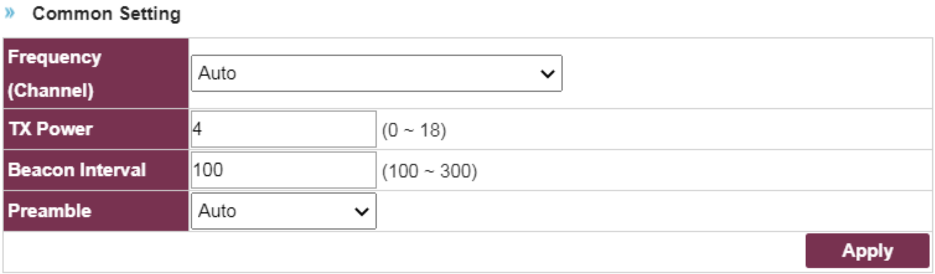
AP Instance	wlan0ap
Network Name (SSID)	SiriusFlyzxc
Network Mode	11 b/g/n
Rx Packets	5
Tx Packets	13
Rx Bytes	993
Tx Bytes	546

Figure 30: WIFI status

6.4.2 AP Sommon

➢ To set WIFI AP channel and RF parameters:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to ***<u>Settings > WIFI > AP Common</u>***page.



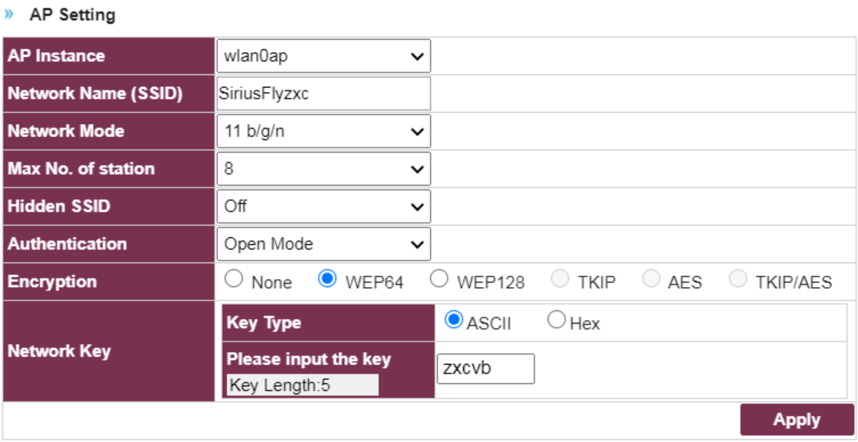
» Common Setting

Frequency (Channel)	Auto	
TX Power	4	(0 ~ 18)
Beacon Interval	100	(100 ~ 300)
Preamble	Auto	

Figure 31: Common Setting

6.4.3 AP Setting

- To set WIFI AP security:
  - Launch a web browser from a computer that is connected to DTU and access to web management system.
  - Go to ***Settings > WIFI > AP Setting***, Select encrypt type and set keys.



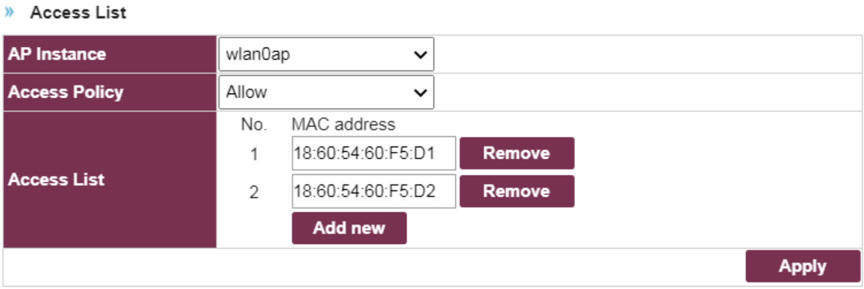
» AP Setting

AP Instance	wlan0ap
Network Name (SSID)	SiriusFlyzxc
Network Mode	11 b/g/n
Max No. of station	8
Hidden SSID	Off
Authentication	Open Mode
Encryption	○ None ● WEP64 ○ WEP128 ○ TKIP ○ AES ○ TKIP/AES
Network Key	Key Type: ● ASCII ○ Hex Please input the key (Key Length:5): zxcvb

Figure 32: AP Setting

6.4.4 AP Access

- To set WIFI AP security:
  - Launch a web browser from a computer that is connected to DTU and access to web management system.
  - Go to ***Settings > WIFI > AP Access***, Select access policy and set list.



» Access List

AP Instance	wlan0ap
Access Policy	Allow
Access List	No. MAC address 1 18:60:54:60:F5:D1 2 18:60:54:60:F5:D2

Figure 33: Access list

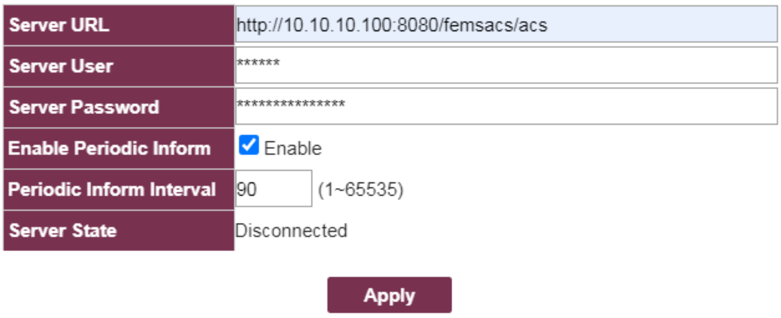
6.5 TR069

With the TR069 service (CPE WAN Management Protocol, Reference [4]. It is intended to support a variety of functionalities to manage a collection of CPE), you can manage DTU on ACS (Auto-Configuration Server, e.g. Friendly ACS), including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software/firmware image management
- Status and performance monitoring
- Diagnostics

➢ To initiate the TR069 service, you need to set correct parameters firstly:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to ***Settings > Firewall > TR069***page, input relevant parameter value.



Server URL	http://10.10.10.100:8080/femsacs/acs
Server User	******
Server Password	***************
Enable Periodic Inform	☑ Enable
Periodic Inform Interval	90 (1~65535)
Server State	Disconnected

Figure 34: Setting TR069 connection parameters

Table 11: TR069 parameters

Parameter	Description
Server URL	Connection address of ACS.
Server User	Username used to authenticate the DTU when making a connection to the ACS.
Server Password	Password used to authenticate the DTU when making a connection to the ACS.
Enable Periodic Inform	Whether or not the DTU MUST periodically send CPE information to the ACS using the Inform method call.
Periodic Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method if PeriodicInform is enabled.

Server state	- Connected, DTU has made successful connection to ACS. - Disconnected, DTU cannot connect to ACS.

- Click the “Apply” buttonfor modification take effect.

6.6 Ser2Net

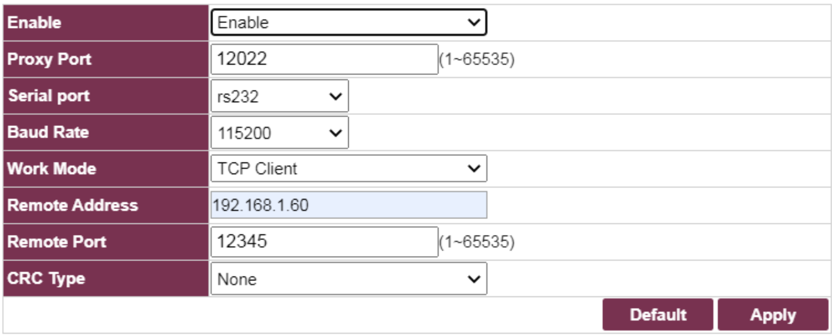
Ser2Net makes it possible of transmit data from serial lined devices through LTE network, including the following primary capabilities:

- RS232-to-net
- RS485-to-net

6.6.1 RS232toNet

➢ To enable RS232toNet:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to ***Settings > Ser2Net > RS232toNet***, input relevant parameter value.



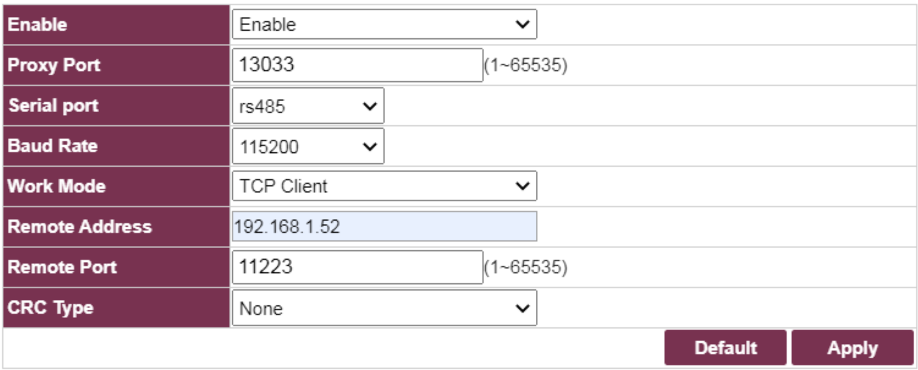
Enable	Enable
Proxy Port	12022 (1~65535)
Serial port	rs232
Baud Rate	115200
Work Mode	TCP Client
Remote Address	192.168.1.60
Remote Port	12345 (1~65535)
CRC Type	None

Figure 35: RS232toNet parameters

6.6.2 RS485toNet

➢ To enable RS485toNet:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to ***Settings > Ser2Net > RS485toNet***, input relevant parameter value.



Enable	Enable
Proxy Port	13033 (1~65535)
Serial port	rs485
Baud Rate	115200
Work Mode	TCP Client
Remote Address	192.168.1.52
Remote Port	11223 (1~65535)
CRC Type	None

Figure 36: RS485toNet parameters

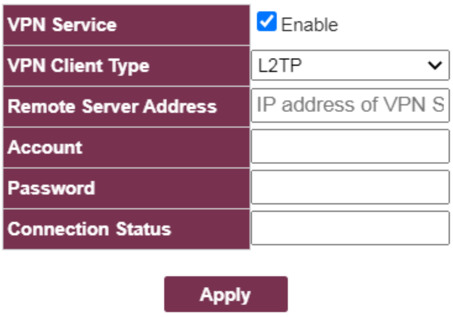
6.7 Application Service

6.7.1 VPN

DTU provides L2TP client solution for Ethernet port network service. With this function enabled, all network packages from Ethernet client PC would be routed to network of VPN server via an encrypted tunnel.

➢ To enable VPN service:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to***Settings>Application Service>VPN***.
- Click check box “Enable VPN Service”, Input relevant VPN parameters.



VPN Service	☑ Enable
VPN Client Type	L2TP
Remote Server Address	IP address of VPN S
Account	
Password	
Connection Status	

Figure 37: Setting VPN parameters

Table 12: VPN parameters

Parameter	Description
VPN Service	Enable or disable VPN service.

VPN Client Type	- L2TP
Remote Server Address	IP address of VPN server.
Account	Username used to authenticate the VPN client (DTU) when making a connection to the VPN server.
Password	Password used to authenticate the VPN client (DTU) when making a connection to the VPN server.
Connection Status	Status of connection between VPN client (DTU) and VPN server. Would also show failed cause if connect to VPN server failed.

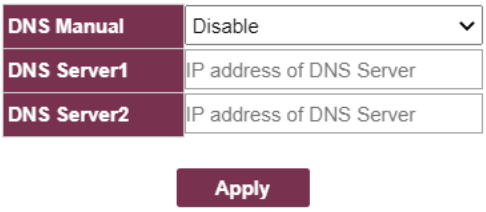
- Click the “Apply”button.

6.7.2 DNS

Except for DNS address assigned from EPC via LTE interface, you can also add additional DNS server.

➢ To add additional DNS server:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to ***Settings >Application Service > DNS***page, input relevant parameter value.



DNS Manual	Disable
DNS Server1	IP address of DNS Server
DNS Server2	IP address of DNS Server

Figure 38: Setting DNS servers

Table 13 DNS parameters

Parameter	Description
DNS Manual	- Enable - Disable
DNS Server1	Additional DNS server 1.
DNS Server2	Additional DNS server 2.

- Click the “Apply” buttonfor modification take effect.

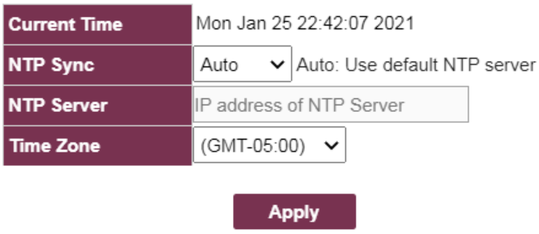
6.8 System

6.8.1 Time Settings

By default, the DTU uses the default NTP server (Automatically find best one from time.google.com, time1.google.com, time.windows.com and time.facebook.com) to sync the network time.You can also change the NTPserver to your preferred NTP server.

➢ To change the NTP server to your preferred NTP server:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to***Settings>System>Time Settings***.
- Select NTP Sync option “Manual”.
- Type your preferred NTP server.
- Click the “Apply”button.



Current Time	Mon Jan 25 22:42:07 2021
NTP Sync	Auto Auto: Use default NTP server
NTP Server	IP address of NTP Server
Time Zone	(GMT-05:00)

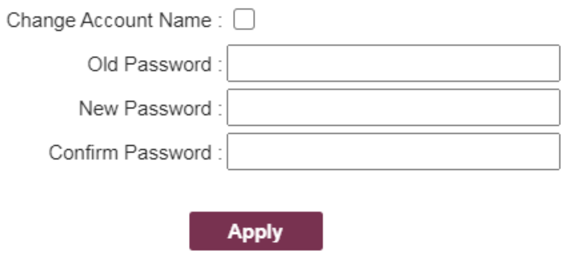
Figure 39: Time Settings

6.8.2 User Settings

In admin domain, you can change the default password (Refer to clause “4.2 Default user account")of “admin” account, and also Add/Delete/Edit the normal user account.

➢ To change the password of “admin”:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to***Settings>System>User Settings***.
- Type the old password in the Old Password field.
- Type the new password in the New Password and Confirm Password fields.



Change Account Name : ☐

Old Password :

New Password :

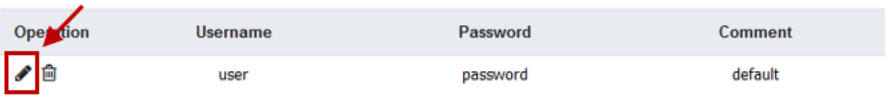
Confirm Password :

Figure 40: Password Setting

- Click the “Apply”button.

➢ Toedit the normal user account:

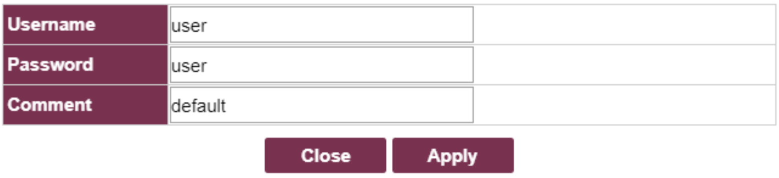
- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to***Settings>System>User Settings***.
- Click ✎ icon in “General User List” panel, “User Edit” panel would be showed.



Operation	Username	Password	Comment
✎ 🗑	user	password	default

Figure 41: Manage normal user account

- In “User Edit” panel, change the new “Username” and “Password” as you prefer.



Username	user
Password	user
Comment	default

Figure 42: Edit normal user account

- Click the “Apply”button.

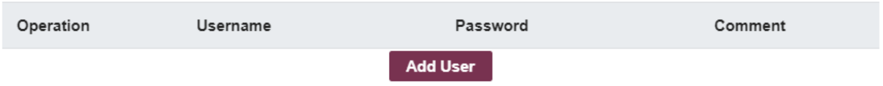
➢ Todelete the normal user account:

- Click 🗑 icon in “General User List” panel, normal user account would be deleted directly.

Currently DTU only support one normal user account. Only when there is no account existing, you are allowed to add a new normal user account.

➢ Toadd a normal user account:

- Click “Add User” button in “General User List” panel, “User Edit” panel would be showed.



Operation	Username	Password	Comment

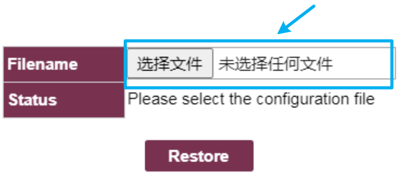
Figure 43: Add normal user account

- In “User Edit” panel, input a new “Username” and “Password” as you prefer.

- Click the “Apply”button.

6.8.3 Configuration Backup

- Tobackup configuration file:
  - Launch a web browser from a computer that is connected to DTU and access to web management system.
  - Go to ***Settings>System>Configuration Backup***.
  - Click “Backup” button.
- Torestore configuration file:
  - Select a valid configuration file.



Filename	选择文件 未选择任何文件
Status	Please select the configuration file

Figure 44: Restore configuration

- Click “Restore” button.

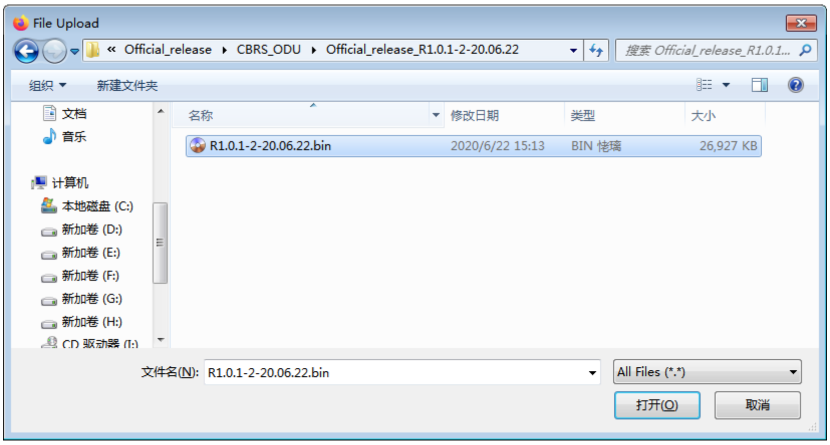
> - **Note:**The DTU reboots after the configuration is restored successfully.

6.8.4 Allow Ping

With the check box ☑ Allow Ping from WAN checked,ping request (ICMP request) from WAN interface is allowed. Otherwise, ping request is forbidden.

6.8.5 Firmware Update

- To update a specific firmware version:
  - Launch a web browser from a computer that is connected to DTU and access to web management system.
  - Select ***Settings>System>Firmware Update***.
  - In “Filename” option select the target firmware.



File Upload

« Official_release ▸ CBRS_ODU ▸ Official_release_R1.0.1-2-20.06.22

搜索 Official_release_R1.0.1...

组织 ▾ 新建文件夹

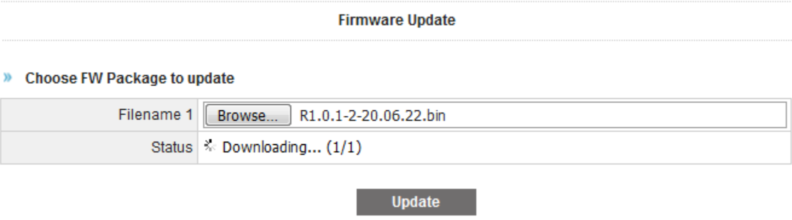
名称	修改日期	类型	大小
R1.0.1-2-20.06.22.bin	2020/6/22 15:13	BIN 怅璃	26,927 KB

文件名(N): R1.0.1-2-20.06.22.bin

All Files (*.*)

Figure 45: Select firmware package

- Click the “Update”button.



Firmware Update

» Choose FW Package to update

Filename 1	Browse... R1.0.1-2-20.06.22.bin
Status	Downloading... (1/1)

Figure 46: Update firmware

> **Note:**Do not interrupt the update process, which will not bring the target firmware into effect.The DTU reboots after the firmware is updated successfully.

6.8.6 Diagnostics

Following diagnostics items are provided for user to check the network performance.

- Ping

Table 14: Ping parameters

Parameter	Description
Target IP	Destination of ping request.
Packet Size	Payload size of the ping request message.
Time Out	Seconds to wait for the first response (default:10).

Count	Number of ping that sent.

- Iperf(v3.1.3)

Table 15: Iperf parameters

Parameter	Description
Target IP	Destination of ping request.
Direction	- Uplink - Downlink
Protocol	- TCP - UDP
BandWidth	Tested bandwidth.
Port	Working port number.
Window Size	Window size (socket buffer size).
Measure Time	Measure time.

- Traceroute

Table 16: Traceroute parameter

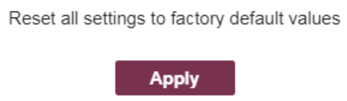
Parameter	Description
Host Name	Destination of traceroute.

6.8.7 Factory Reset

After execute factory reset, all settings would be reset to factory default values.

➢ To add additional DNS server:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to ***Settings >System > Factory Reset***page.
- Click the "Apply" button.



Reset all settings to factory default values

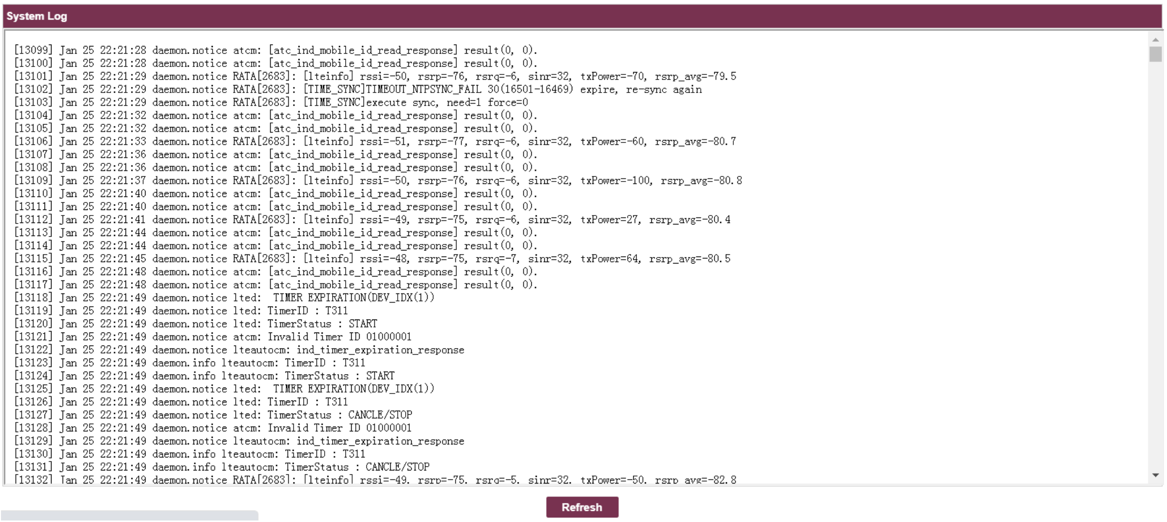
Figure 47: Execute factory reset

Note: The DTU reboots after factory reset is executed successfully.

6.8.8 System Log

6.8.8.1 Systemlog

In ***Settings > System > System Log*** page, you can check the system log in real time.



```
[13099] Jan 25 22:21:28 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13100] Jan 25 22:21:28 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13101] Jan 25 22:21:29 daemon.notice RATA[2683]: [lteinfo] rssi=-50, rsrp=-76, rsrq=-6, sinr=32, txPower=-70, rsrp_avg=-79.5
[13102] Jan 25 22:21:29 daemon.notice RATA[2683]: [TIME_SYNC]TIMEOUT_NTPSYNC_FAIL 30(16501-16469) expire, re-sync again
[13103] Jan 25 22:21:29 daemon.notice RATA[2683]: [TIME_SYNC]execute sync, need=1 force=0
[13104] Jan 25 22:21:32 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13105] Jan 25 22:21:32 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13106] Jan 25 22:21:33 daemon.notice RATA[2683]: [lteinfo] rssi=-51, rsrp=-77, rsrq=-6, sinr=32, txPower=-60, rsrp_avg=-80.7
[13107] Jan 25 22:21:36 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13108] Jan 25 22:21:36 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13109] Jan 25 22:21:37 daemon.notice RATA[2683]: [lteinfo] rssi=-50, rsrp=-76, rsrq=-6, sinr=32, txPower=-100, rsrp_avg=-80.8
[13110] Jan 25 22:21:40 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13111] Jan 25 22:21:40 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13112] Jan 25 22:21:41 daemon.notice RATA[2683]: [lteinfo] rssi=-49, rsrp=-75, rsrq=-6, sinr=32, txPower=27, rsrp_avg=-80.4
[13113] Jan 25 22:21:44 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13114] Jan 25 22:21:44 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13115] Jan 25 22:21:45 daemon.notice RATA[2683]: [lteinfo] rssi=-48, rsrp=-75, rsrq=-7, sinr=32, txPower=64, rsrp_avg=-80.5
[13116] Jan 25 22:21:48 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13117] Jan 25 22:21:48 daemon.notice atcm: [atc_ind_mobile_id_read_response] result(0, 0).
[13118] Jan 25 22:21:49 daemon.notice lted:  TIMER EXPIRATION(DEV_IDX(1))
[13119] Jan 25 22:21:49 daemon.notice lted: TimerID : T311
[13120] Jan 25 22:21:49 daemon.notice lted: TimerStatus : START
[13121] Jan 25 22:21:49 daemon.notice atcm: Invalid Timer ID 01000001
[13122] Jan 25 22:21:49 daemon.notice lteautocm: ind_timer_expiration_response
[13123] Jan 25 22:21:49 daemon.info lteautocm: TimerID : T311
[13124] Jan 25 22:21:49 daemon.info lteautocm: TimerStatus : START
[13125] Jan 25 22:21:49 daemon.notice lted:  TIMER EXPIRATION(DEV_IDX(1))
[13126] Jan 25 22:21:49 daemon.notice lted: TimerID : T311
[13127] Jan 25 22:21:49 daemon.notice lted: TimerStatus : CANCLE/STOP
[13128] Jan 25 22:21:49 daemon.notice atcm: Invalid Timer ID 01000001
[13129] Jan 25 22:21:49 daemon.notice lteautocm: ind_timer_expiration_response
[13130] Jan 25 22:21:49 daemon.info lteautocm: TimerID : T311
[13131] Jan 25 22:21:49 daemon.info lteautocm: TimerStatus : CANCLE/STOP
[13132] Jan 25 22:21:49 daemon.notice RATA[2683]: [lteinfo] rssi=-49, rsrp=-75, rsrq=-5, sinr=32, txPower=-50, rsrp_avg=-82.8
```

Figure 48: View system log

Click enableQLog button to record extra log of LTE modem.

Click Download button to download system log and kernel crash log if generated.

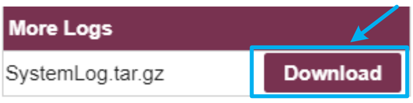


Figure 49: Download system log

6.8.8.2 Config

Switch to "Config" menu, you can also set log level and enable remote log function to transfer log to remote UDP server or FTP server.

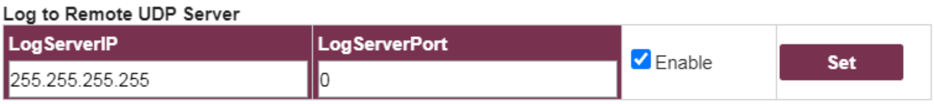
Log levels define as following:

- EMERGENCY
- ALERT
- CRITICAL
- ERROR
- WARNING
- NOTICE
- INFORMATION

- DEBUG

➢ To enable log to remote UDP server:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Go to ***Settings > System > System Log > Config***page.
- Ensure ☑ Enable box checked,input IP address and port of destination UDP server in “Log to Remote UDP Server”panel.



Log to Remote UDP Server

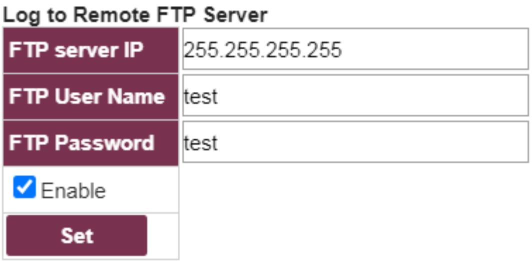
LogServerIP	LogServerPort		
255.255.255.255	0	☑ Enable	Set

Figure 50: Enable log to remote UDP server

- Click the “Set” button.

➢ To enable log to remote FTP server:

- Ensure ☑ Enable box checked,input IP address, username and password of destination FTP server in “Log to Remote FTP Server”panel.



Log to Remote FTP Server

FTP server IP	255.255.255.255
FTP User Name	test
FTP Password	test
☑ Enable	
Set	

Figure 51: Enable log to remote FTP server

- Click the “Set” button.

6.8.9 System Reboot

➢ To reboot the DTU:

- Launch a web browser from a computer that is connected to DTU and access to web management system.
- Select ***Settings>System>System Reboot***.
- Click the Rebootbutton.

Note: It would take about 90 seconds to reboot the system.

Revision History

Table 17: Revision history of this document

Version	Author	Date	Description