Smarter. Greener. Together.

Industrial Automation Headquarters

Delta Electronics, Inc.
Taoyuan Technology Center
No.18, Xinglong Rd., Taoyuan City,
Taoyuan County 33068, Taiwan
TEL: 886-3-362-6301 / FAX: 886-3-371-6301

Asia

Delta Electronics (Jiangsu) Ltd.
Wujiang Plant 3
1688 Jiangxing East Road,
Wujiang Economic Development Zone
Wujiang City, Jiang Su Province, P.R.C. 215200
TEL: 86-512-6340-3008 / FAX: 86-769-6340-7290

Delta Greentech (China) Co., Ltd.
238 Min-Xia Road, Pudong District,
ShangHai, P.R.C. 201209
TEL: 86-21-58635678 / FAX: 86-21-58630003

Delta Electronics (Japan), Inc.
Tokyo Office
2-1-14 Minato-ku Shibadaimon,
Tokyo 105-0012, Japan
TEL: 81-3-5733-1111 / FAX: 81-3-5733-1211

Delta Electronics (Korea), Inc.
1511, Byucksan Digital Valley 6-cha, Gasan-dong,
Geumcheon-gu, Seoul, Korea, 153-704
TEL: 82-2-515-5303 / FAX: 82-2-515-5302

Delta Electronics Int'l (S) Pte Ltd.
4 Kaki Bukit Ave 1, #05-05, Singapore 417939
TEL: 65-6747-5155 / FAX: 65-6744-9228

Delta Electronics (India) Pvt. Ltd.
Plot No 43 Sector 35, HSIIDC
Gurgaon, PIN 122001, Haryana, India
TEL : 91-124-4874900 / FAX : 91-124-4874945

Americas

Delta Products Corporation (USA)
Raleigh Office
P.O. Box 12173,5101 Davis Drive,
Research Triangle Park, NC 27709, U.S.A.
TEL: 1-919-767-3800 / FAX: 1-919-767-8080

Delta Greentech (Brasil) S.A.
Sao Paulo Office
Rua Itapeva, 26 - 3° andar Edificio Itapeva One-Bela Vista
01332-000-São Paulo-SP-Brazil
TEL: 55 11 3568-3855 / FAX: 55 11 3568-3865

Europe

Delta Electronics (Netherlands) B.V.
Eindhoven Office
De Witbogt 20, 5652 AG Eindhoven, The Netherlands
TEL : +31 (0)40-8003800 / FAX : +31 (0)40-8003898

DX-020BB20-02

2020-05-14

*We reserve the right to change the information in this manual without prior notice.

DX-2100 **Series Industrial 3G Cloud Router User Manual**

DIACloud Cloud Platform

www.deltaww.com

Smarter. Greener. Together.

DX-2100 Series
Industrial 3G Cloud Router
User Manual

Revision History

Version	Revision	Date
1st	The first version was published.	2016/3/21
2nd	1. Add new function of Cloud Service for Auto Detect in section 3.2.1. 2. Chapter 3: Add new function of PIN Management in Section 3.2.2. 3. Chapter 3: Add new function of PHY Auto Reset in Section 3.2.3. 4. Chapter 3: Add new function of Set Local PC Time in Section3.4.2. 5. Chapter 3: Update information concerning Transparent mode/ Slave mode/ Master mode/ Serial Server-TCP Server/ Serial Server-TCP Client/ Serial Server-UDP Client/ RS485 mode in Section3.4.3. 6. Chapter 3: Add new function of MC master mode in section 3.4.3. 7. Chapter 3: Add new function of Siemens TCP in section 3.4.6. 8. Chapter 3: Update information concerning functions of Diagnosing Method/ Host Name/IP Address in section 3.4.14. 9. Chapter 3: Add new function of Trouble shooting in section3.4.15. 10. Chapter 3: Add new function of Add/ Export Configure List/ Import Configure List/ Register Type/ Register Start Address in section 3.4.19. 11. Chapter 4: Update information concerning functions of PPI and add new function of Auto Baudrate.	2020/5/14

DX-2100 Series Industrial 3G Cloud Router User Manual

Table of Contents

Chapter 1 Introduction

1.1 Product Overview 1-3
1.1.1 Network Design 1-4
1.1.2 Features 1-4
1.1.3 Front Panel Ports and LEDs 1-5
1.1.4 Top Panel 1-5
1.1.5 Bottom Panel 1-6
1.1.6 Dimension 1-7
1.2 Package Checklist 1-7

Chapter 2 User Interface

2.1 Web-based GUI Configuration 2-2
2.1.1 System Connection 2-2
2.1.2 Default IP Address/Account/Password 2-2
2.1.3 Local Network Setups 2-2
2.1.4 Logging in 2-4
2.2 DIADevice 2-5
2.2.1 Device Connection and Detection 2-5
2.2.2 Network Setting 2-7
2.2.3 Bind Device 2-9
2.2.4 Open Device Webpage 2-11
2.3 Typical Application Configuration 2-12
2.3.1 Data collection 2-12
2.3.2 Remote debugging 2-16

Chapter 3 Functions

3.1 Status 3-3
3.1.1 Device Information 3-3
3.1.2 Network Status 3-5
3.1.3 Routing Table 3-6
3.1.4 Local Log 3-6
3.1.5 Traffic Statistics 3-7
3.1.6 Cloud Status 3-7
3.1.7 Connected Device 3-8
3.2 Network 3-8

3.2.1 Cellular Network Configurations 3-8
3.2.2 PIN Management 3-11
3.2.3 LAN Configurations 3-14
3.2.4 Static Routing Rules 3-16
3.2.5 Dynamic DNS 3-18
3.3 Firewall 3-19
3.3.1 Firewall Settings 3-19
3.3.2 DMZ Settings 3-19
3.3.3 Port Forward 3-20
3.3.4 Port Trigger 3-22
3.3.5 URL Filter 3-24
3.3.6 MAC Filter 3-24
3.3.7 IP Filter 3-25
3.4 System 3-26
3.4.1 User Management 3-26
3.4.2 Time Zone Configurations 3-27
3.4.3 RS232 3-28
3.4.4 RS485 3-38
3.4.5 Modbus TCP 3-46
3.4.6 Siemens TCP 3-49
3.4.7 Log Settings 3-52
3.4.8 Firmware Upgrade 3-53
3.4.9 Backup & Restore 3-53
3.4.10 Scheduled Jobs 3-54
3.4.11 Add A New Job 3-54
3.4.12 Export Job List 3-55
3.4.13 Import Job List 3-55
3.4.14 Network Diagnosis 3-55
3.4.15 Trouble shooting 3-56
3.4.16 System Reboot 3-57
3.4.17 Privilege Management 3-57
3.4.18 Event Management 3-60
3.4.19 Register Management 3-63
3.5 Cloud Service 3-65
3.5.1 Cloud Configuration 3-65
3.5.2 Secure Tunnel Firewall 3-68
3.5.3 Cloud Log 3-69
3.6 SD Card Quick Configuration 3-70

Chapter 4 DIACom

4.1 Introduction to DIACom 4-2

4.1.1 Select a Suitable Firmware Version 4-2

4.1.2 DIACom Installation 4-3

4.1.3 DIACloud Account Registration 4-3

4.1.4 Bind DIACloud Account 4-5

4.2 DIACom Operation 4-6

4.2.1 Setup a Secure Tunnel 4-6

4.2.2 Create a Virtual Serial-Port 4-10

4.2.3 Remote Control and Monitoring via DIACom 4-12

4.2.4 Automation Startup 4-14

Chapter 5 DIACloud

5.1 Introduction to DIACloud 5-2

5.1.1 Select a Suitable Firmware Version 5-2

5.2 Instructions for DIACloud 5-2

5.2.1 Register and Login 5-2

5.2.2 Home 5-4

5.2.3 Devices 5-6

5.2.4 Alarm 5-16

5.2.5 Secure Tunnels 5-16

5.2.6 Sub Users 5-18

5.2.7 Logs 5-21

5.2.8 Orders 5-22

5.2.9 Profile 5-23

Chapter 6 DIACloud APP

6.1 Introduction to DIACloud APP 6-2

6.1.1 Select a Suitable Firmware Version 6-2

6.1.2 DIACloud APP Installation 6-2

6.2 DIACloud APP Function 6-3

6.2.1 DIACloud APP Login 6-3

6.2.2 Device List 6-4

6.2.3 Device Details 6-5

6.2.4 Registers View 6-6
6.2.5 Alarm List 6-7

Chapter 1 Product Introduction

Table of Contents

1.1 Product Overview 1-3

1.1.1 Network Design 1-4

1.1.2 Features 1-4

1.1.3 Front Panel Ports and LEDs 1-5

1.1.4 Top Panel 1-5

1.1.5 Bottom Panel 1-6

1.1.6 Dimension 1-7

1.2 Package Checklist 1-7

About This Manual

The user manual is suitable for **DX-2100RW-WW**. If you need to use the Delta DX-2100 series products in China areas, please refer to the model name **DX-2100RW-CN** on the Delta website, or contact our branch offices or distributors.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a class A 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 radio frequency signal 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.

CE Declaration of Conformity

In accordance with the Directives 2004/108/EC*, 2014/30/EU, 2006/95/EC*, 2014/35/EU and 1999/5/EC. The test record, data evaluation and DX-2100RW-WW configurations represented herein are true and accurate under the standards herein specified.

EN 301 511 V9.0.2 (2003-3)
Test Items:
Radiated spurious emissions – MS allocated channel (Clause 4.2.16)
Radiated spurious emissions – MS in idle mode (Clause 4.2.17)
EN 301 908-1 V7.1.1 (2015-03)
EN 301 489-1 V1.9.2 (2011-09)
EN 301 489-7 V1.3.1 (2005-11)
EN 301 489-24 V1.5.1 (2010-10)

Disclaimers and Limitation of Liabilities

To the maximum extent permitted by law and regardless DELTA be aware or has been advised of the possibility of these damages, DELTA is not liable to any user or anyone else for: (a) any loss of use, data, reputation, goodwill, credit, opportunity, economy or profits, whether or not foreseeable; (b) any special, incidental, indirect, consequential, or punitive damages whatsoever; (c) any losses or damages based on any theory of liability, including breach of contract or warranty, negligence or other tortious action; (d) any losses or damages resulting from use or unable to use the systems or devices to which the Software or Services are incorporated or co-operated; and (e) any losses or damages arising from any other claim or in connection with the use of or access to the Software or Services.

ประกาศเรื่องระบบไร้สายของไทย

“เครื่องวิทยุคมนาคมนี้มีระดับการแผ่คลื่นแม่เหล็กไฟฟ้าสอดคล้องตามมาตรฐานความปลอดภัยต่อสุขภาพของมนุษย์จากการใช้เครื่องวิทยุคมนาคมที่คณะกรรมการกิจการโทรคมนาคมแห่งชาติประกาศกำหนด”

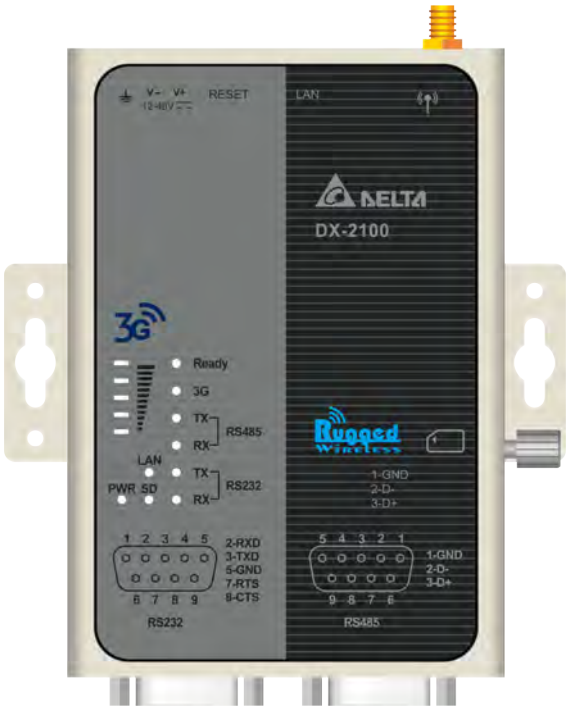
(This radiocommunication equipment has the electromagnetic field strength in compliance with the Safety Standard for the Use of Radiocommunication Equipment on Human Health announced by the National Telecommunications Commission.)

1.1 Product Overview

The DX-2100RW-WW is a single-port 3G industrial router, an Internet of Things wireless communication product of industrial grade. Apart from supporting HSPA+/HSUPA/HSDPA/UMTS, the product is also downward compatible with GSM/GPRS/EDGE mobile network. Moreover, the product is equipped with multiple application interfaces, including Ethernet interface, RS232 serial interface and RS485 serial interface, and thus can satisfy the user’s various different application demands.

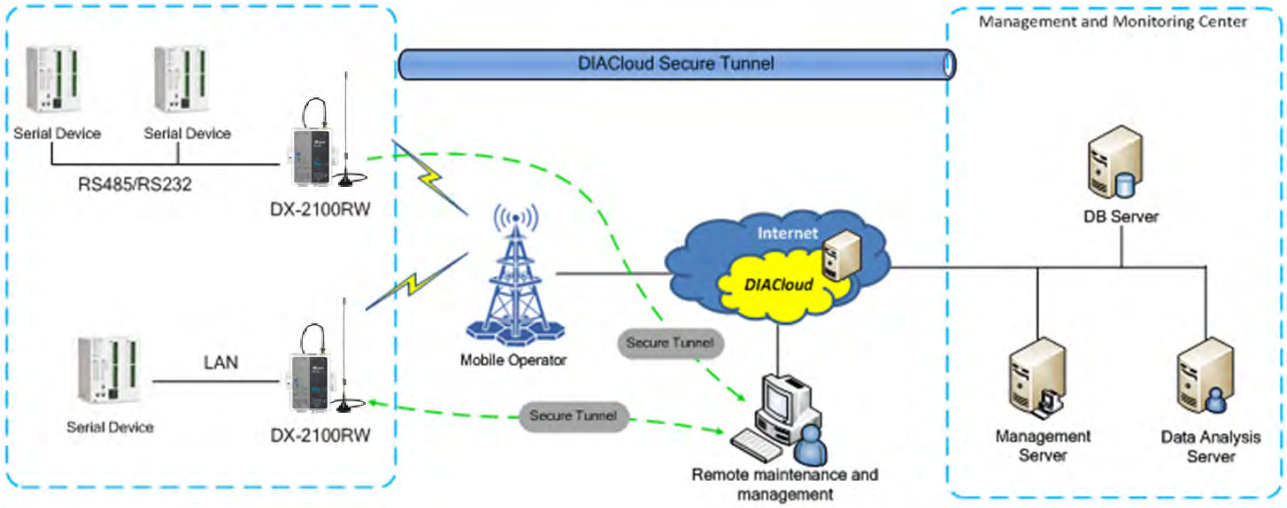
The product supports DIACloud platform services, and by this platform, convenient and efficient point-to-point connection with the router, safe and reliable data transmission, remote device management and configuration, remote firmware upgrading, remote maintenance and other functions can be realized, so as to save the cost of device operation and maintenance for users.

The product can be widely used in the fields requiring mobile network interconnection, such as industrial automation, smart home, intelligent building, smart power grids, mobile video surveillance, intelligent self-service and intelligent transportation.



1.1.1 Network Design

DIACloud platform services supported, users can connect intelligent devices from different locations to the internet with DX-2100RW-WW and use point-to-point connection with the router for a safe and reliable data transmission and additionally save the costs of VPN device operation as well as maintenance. By browsing the web or apps on the handheld computers, managers can check the data and monitor the devices remotely in real-time

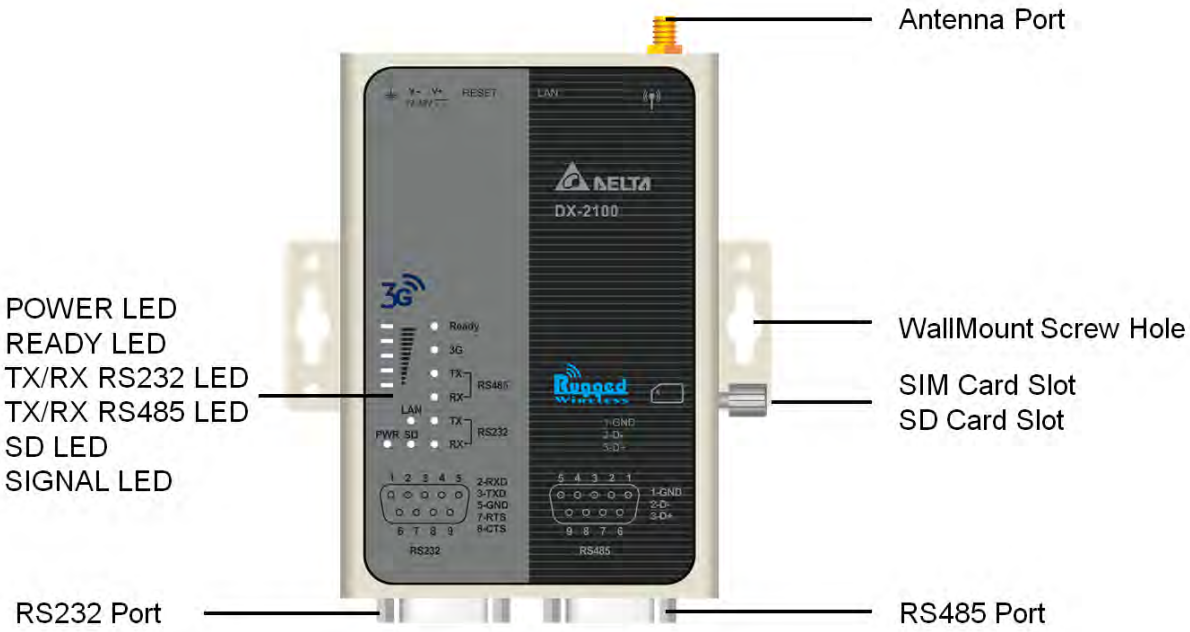


1.1.2 Features

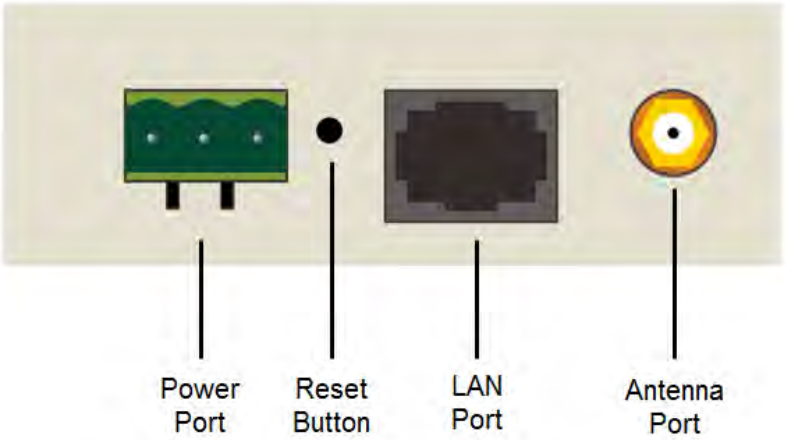
- HSPA+/HSUPA/HSDPA/UMTS: 800/850/900/1700(AWS)/1900/2100 MHz
- GSM/GPRS/EDGE: 850/900/1800/1900 MHz
- Authentication Protocols, CHAP and PAP
- Access Point Name (APN) gateway
- Auto Dial-up Connection
- Provide Dual Port RS232 & RS485 and LAN Port Interfaces for Different Application Demands
- Built-in a Watchdog Timer to Ensure System Stability
- Built-in RTC and Support NTP Server
- Firmware Upgrade Locally and Remotely
- Support Firewall: Stateful Packet Inspection (SPI), Prevent Denial of Service (DoS) Attacks, NAT (Network Address Translation), Port Trigging, Port Mapping, IP Address Filtering, MAC Address Filtering, URL Filtering, DHCP Server, Dynamic DNS, Static Routes, Demilitarized Zone (DMZ)
- Various Protocols, TCP/IP, UDP, ICMP, DHCP, HTTP, DNS, SSH and More
- Modbus TCP, Modbus ASCII and Modbus RTU protocol
- Mitsubishi MC and Siemens ISO TCP protocol
- Scheduled Task Management
- Servers for Local Log and Remote Log
- Configurations Backup, Export and Import

- Network Flow Monitoring
- Network Fault Detection and Diagnosis
- DIACloud Service to Secure Point-to-point Data Transmission, to Manage Device Configurations Piece by Piece or in Batch and to Upgrade Firmware Remotely

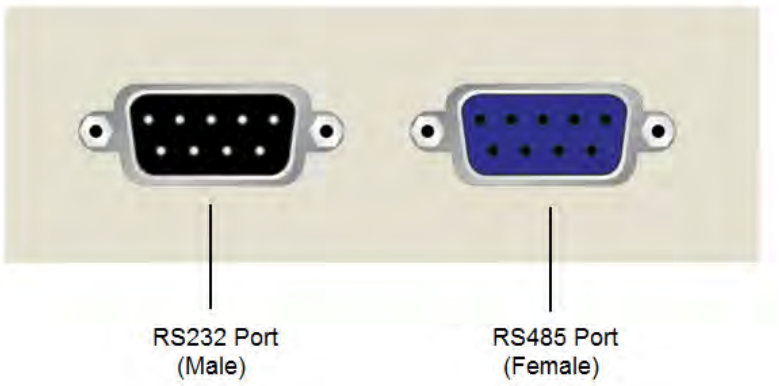
1.1.3 Front Panel Ports and LEDs



1.1.4 Top Panel



1.1.5 Bottom Panel



Notice

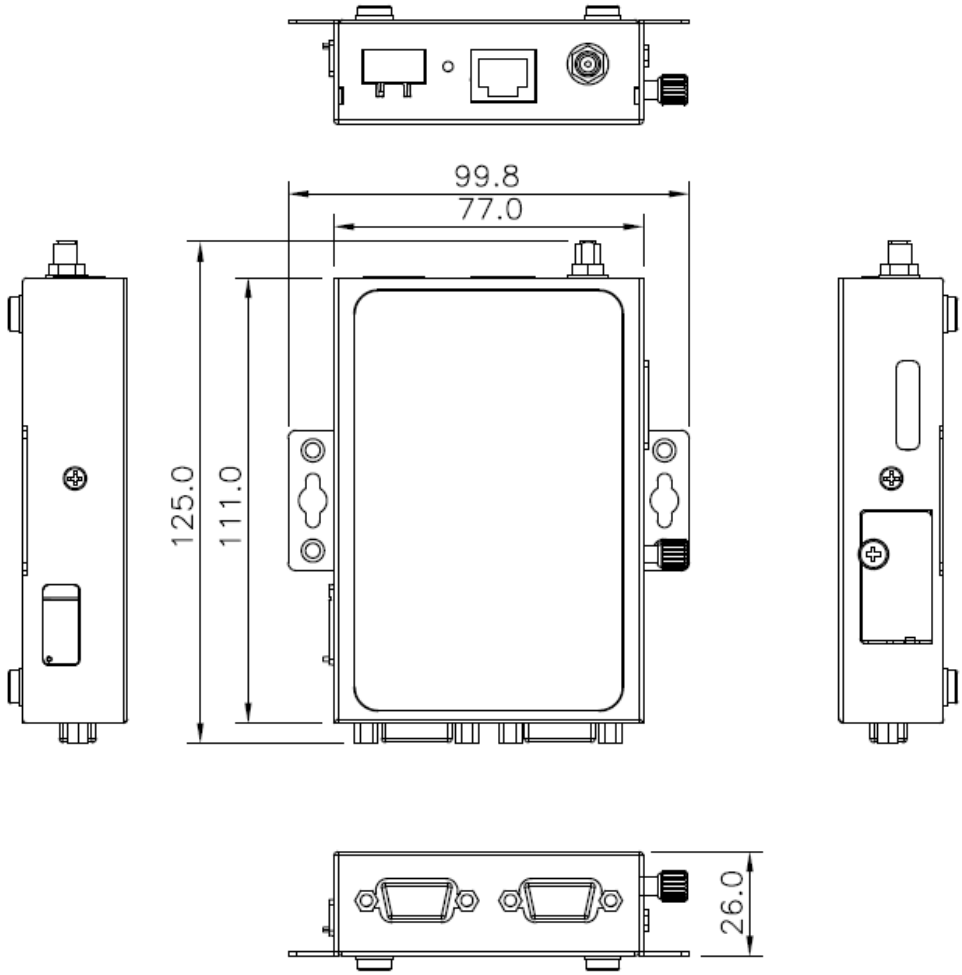
This router's reset button is on the front panel. By pressing the Reset button, users can reset the router or reset the router to factory default settings. See the instruction below:

- Reset the Router: With the router powered on, press the Reset button and release the button right away.
- Reset to Factory Defaults: With the router powered on, press and hold the Reset button for 3~6 seconds and then release the button.
  - Reset can only be done when the device is running properly.

With the router powered on, press and hold the Reset button until all the LEDs go out (except the Power LED). Then release the button and wait the router to reboot to its factory default settings.

1.1.6 Dimension

Unit = mm



1.2 Package Checklist

Unpack the package carefully and check the package contents. The package should contain the following items:

- DX-501L1-CN Industrial 4G Cloud Router x 1
- Quick Installation Guide x 1
- 10/100Mbps Ethernet Cable (100cm) x1
- SMA Antenna (300cm) x 1

Notice

Verify that nothing is missing from the DX-2100RW-WW package by using the check list above. If any item is found missing or damaged, please contact your local sales representative for support.

Memo

2

Chapter 2 User Interface

Table of Contents

2.1 Web-based GUI Configuration 2-2

2.1.1 System Connection 2-2

2.1.2 Default IP Address/Account/Password 2-2

2.1.3 Local Network Setups 2-2

2.1.4 Logging in 2-4

2.2 DIADevice 2-5

2.2.1 Device Connection and Detection 2-5

2.2.2 Network Setting 2-7

2.2.3 Bind Device 2-9

2.2.4 Open Device Webpage 2-11

2.3 Typical Application Configuration 2-12

2.3.1 Data collection 2-12

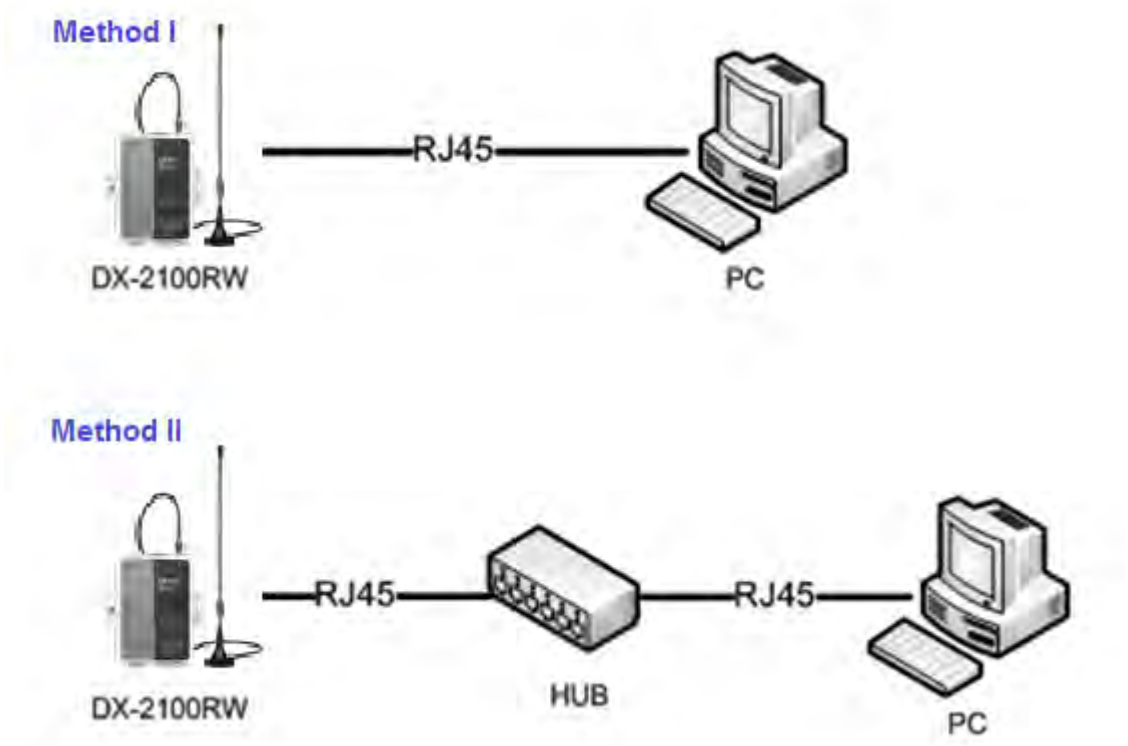
2.3.2 Remote debugging 2-16

2.1 Web-based GUI Configuration

The DX-2100RW-WW Industrial 3G Cloud Router provides a friendly Web Browser Configuration for users to set up and operate more intruitivly.

2.1.1 System Connection

Connect the DX-2100RW-WW with a computer directly or via a switch/hub.



2.1.2 Default IP Address / Account / Password

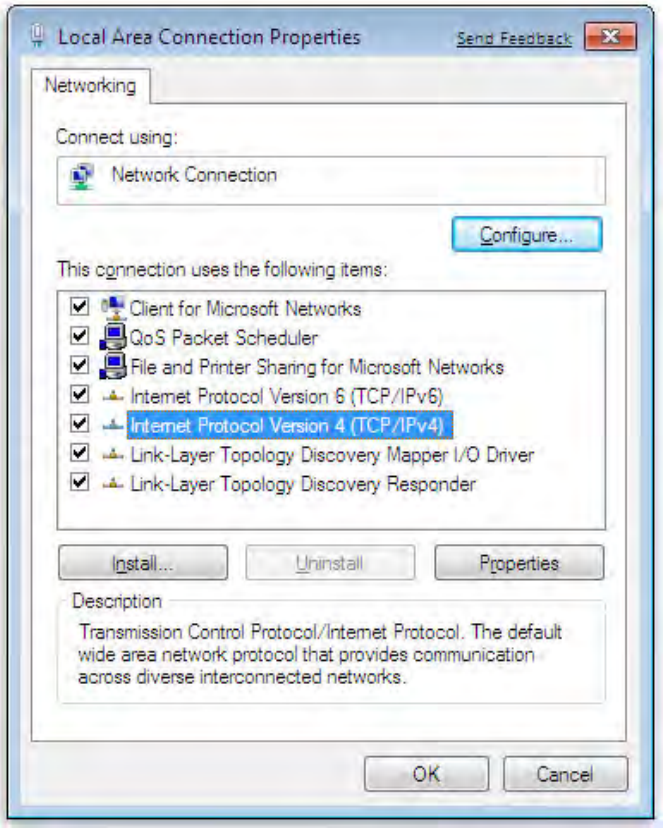
The default IP address of router is 192.168.5.5. The default account and password is admin/admin.

2.1.3 Local Network Setups

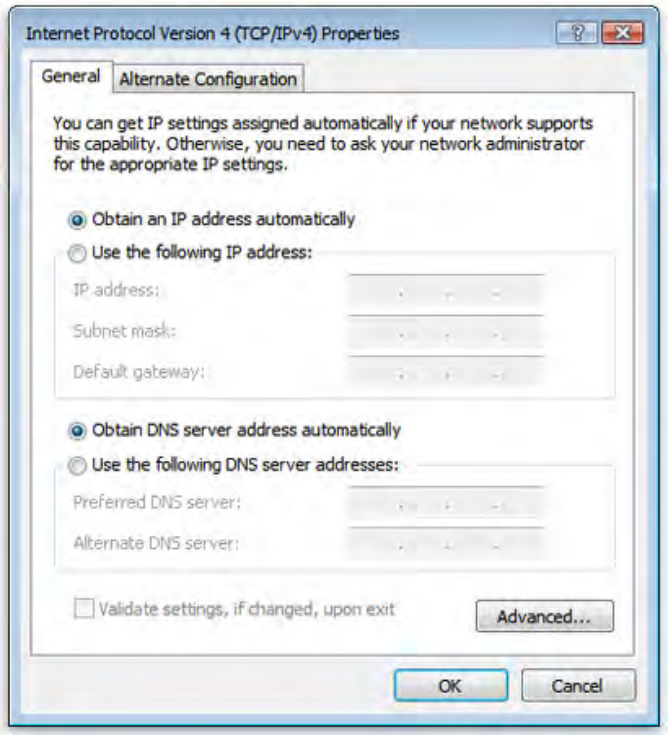
After the connection of the local computer and the router is established, users will need to set the network configruration for the PC. There are 2 methods to configure the setting, we recommand using the first one:

- **Obtain an IP address automatically by using the router as a DHCP server.**

  1. Open Network Connections by clicking the Start button, and then clicking Control Panel.
  2. Under Network and Sharing Center, click View network connections.
  3. Right-click the connection that you intend to change, and then click Properties. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
  4. Click the Networking tab. Click either Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6), then click Properties.



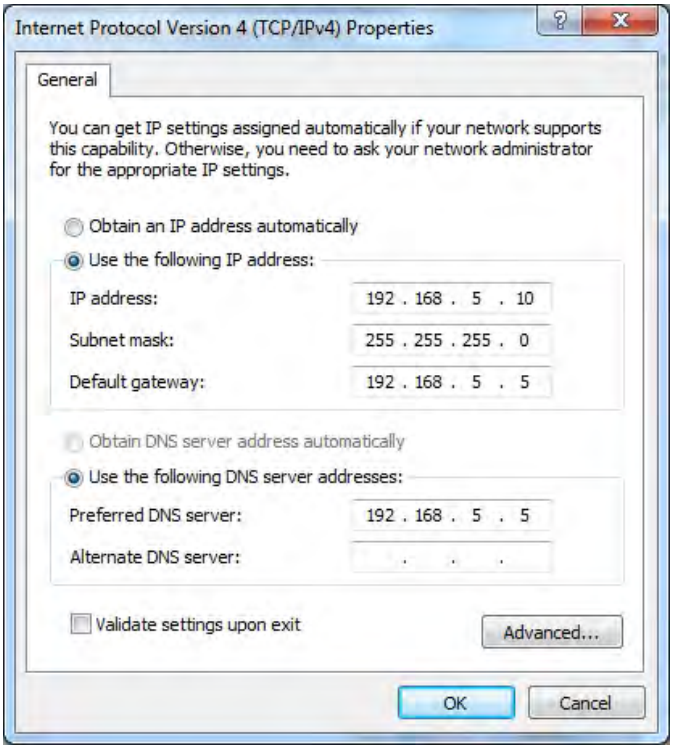
5. Click Obtain DNS server address automatically and then click OK to get a DNS server address automatically using DHCP.



- **Set up the IP address manually.**
  (The IP address of the computer should be in the same subnet as the router's.)

  Since the router's default IP address is 192.168.5.5 and the subnet mask is 255.255.255.0, the computer's IP address can be set between 192.168.5.1 to 192.168.5.254 except 192.168.5.5. In addition, IP conflicts shouldn't exist.

  Here, we set the IP address to 192.168.5.10 and the default gateway to 192.168.5.5. For DNS, the usable DNS address can be selected or the address can also be set to 192.168.5.5.

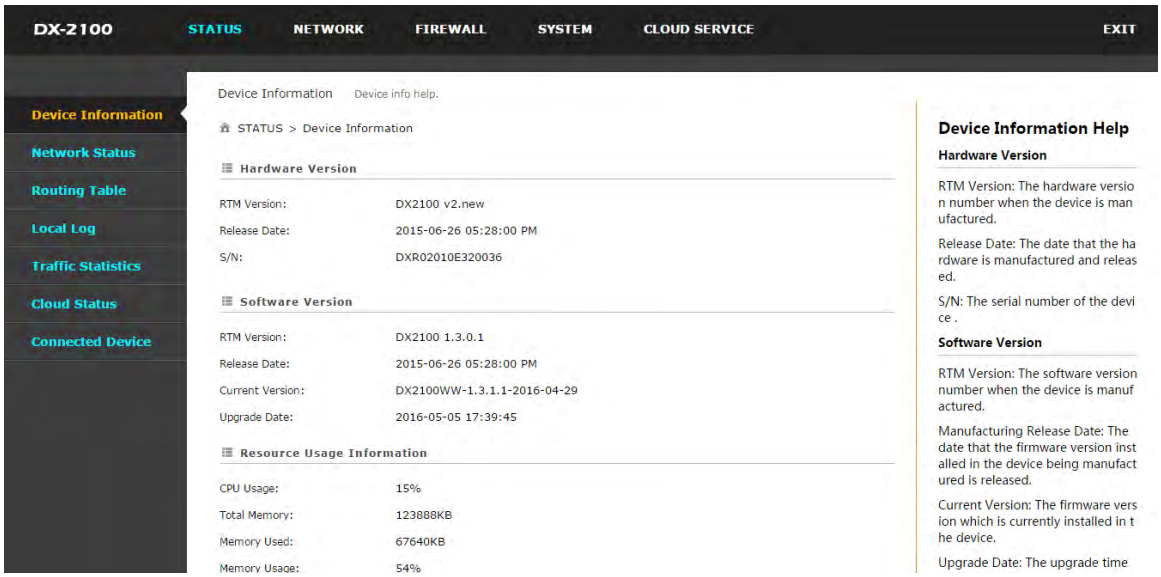


2.1.4 Logging in

1. Open your Internet Explorer browser and input LAN IP address (Default is 192.168.5.5) in the search bar and then press Enter.

2. You'll be prompted with the log-in page. Input the user name and the password (Default is admin/admin) and then press Enter to log in to the setup page.

3. After login, you can see the main selection area on the left hand side and the upper area of the page. The detailed settings can be seen on the right side of the page.



2.2 DIADevice

DIADevice is a tool for quickly configuring network devices. Users simply connect the DX device to the PC through the network cable. This tool can be used to quickly and easily configure the network setting of the device and complete the device binding DIACloud cloud account.

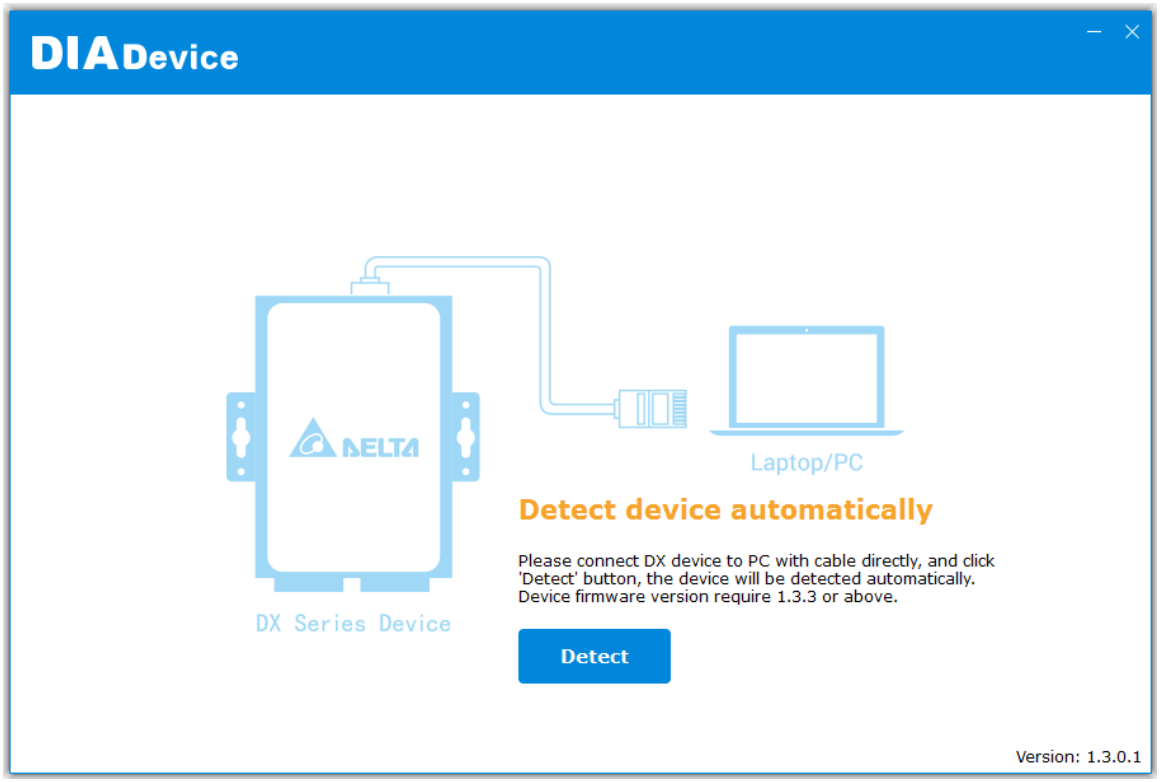
The DIADevice software is included in the latest DIACom software package. From the official website or sales staff to obtain DIACom package. DX-2100 below as an example on how to configure the device through DIADevice.

The following example uses DX-2100 to explain how to configure your device with DIADevice.

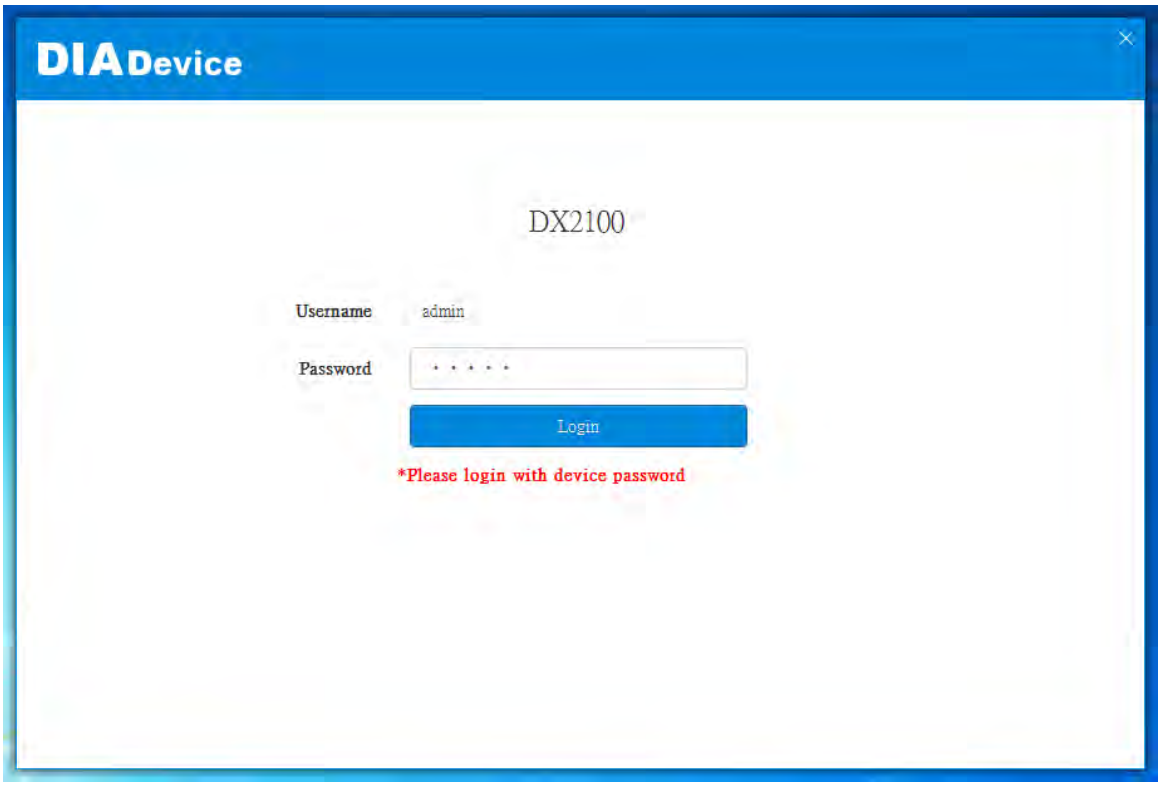
2.2.1 Device Connection and Detection

1. Connect the device to the power supply, and connect the device to the PC using a network cable. Plug the network cable connected to the Internet into the WAN port of the device

2. Run DIADevice software, click "Detect" button.



3. After DIACom detects the device, it will automatically go to the login page, and the user needs to enter login password on the login page.



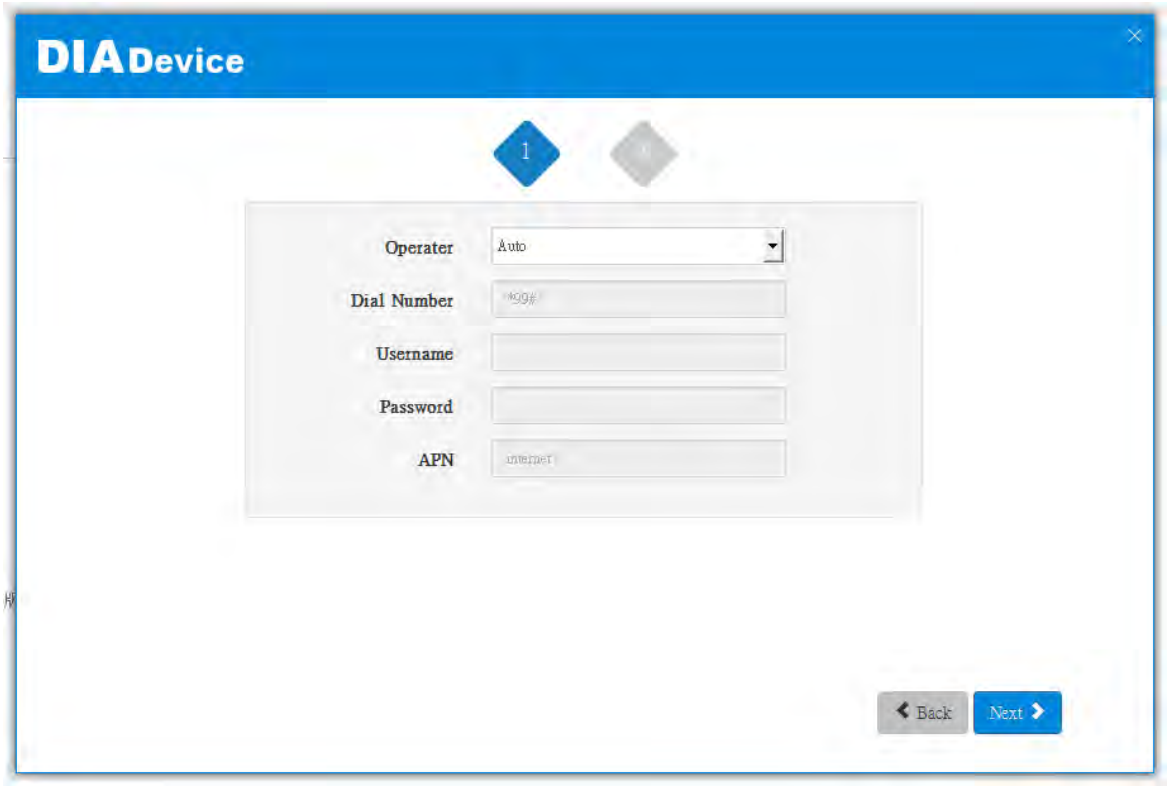
4. After passing the authentication, the device information page is displayed, including the basic device information (Device Name, S / N, firmware, LAN IP address), network status, WAN information, and cloud service information

2.2.2 Network Setting

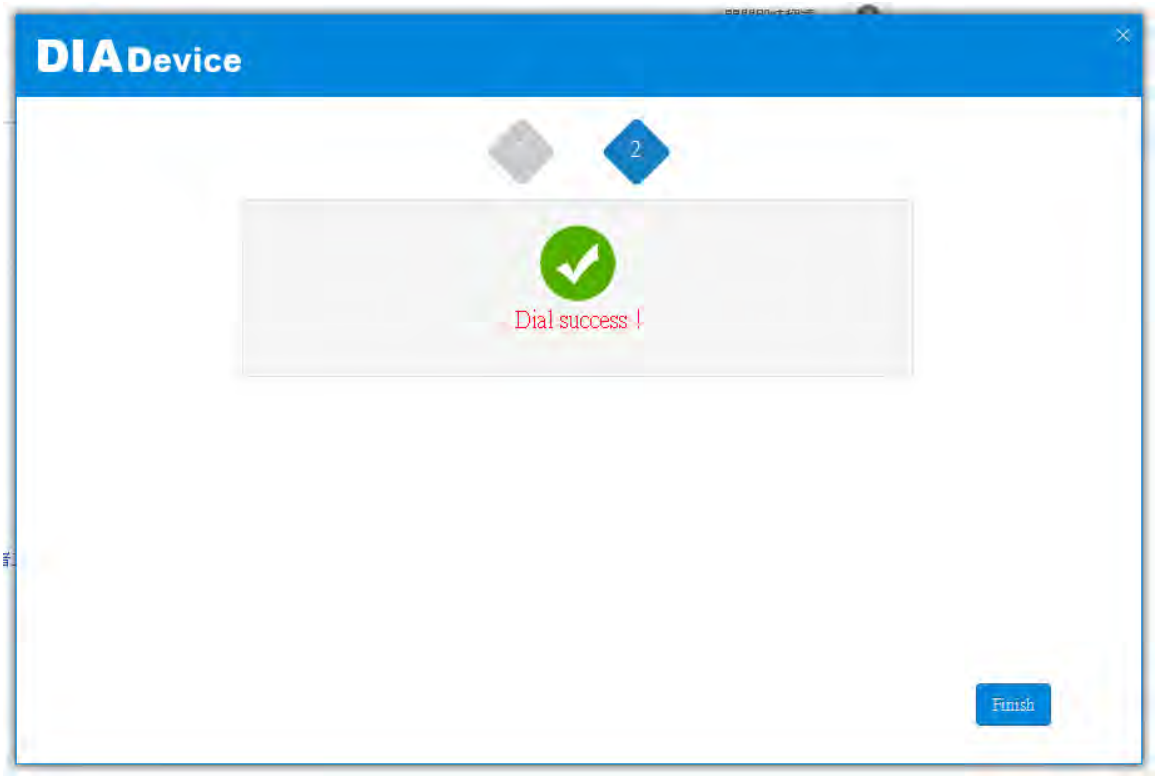
This feature allows users to quickly configure network in two steps.

1. Click “Network Setting”

2. The default is automatic. If you can not connect to the Internet using auto-setup, please use manual settings.



3. After the device successfully connected to the Internet, the connection was successful.

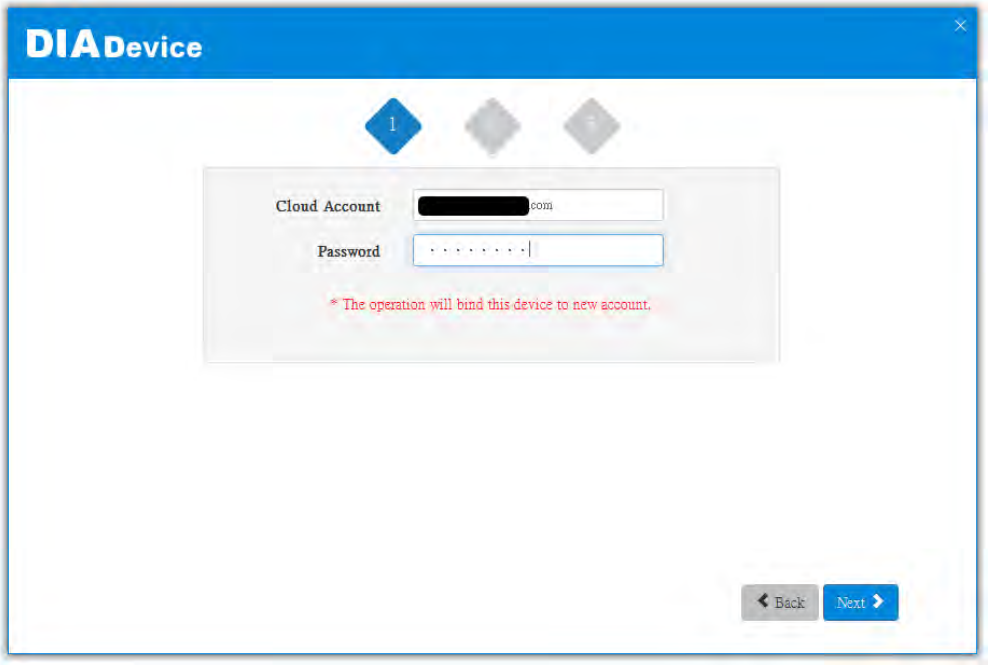


2.2.3 Bind Device

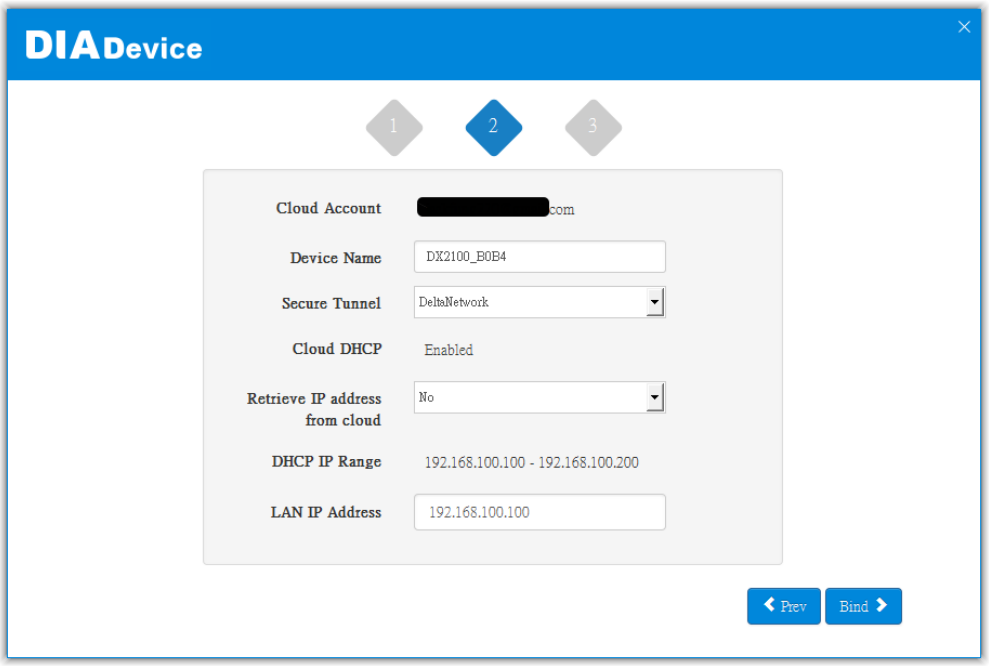
This feature allows users to quickly bind devices to the DIAcloud in three steps.

1. Click “Bind Device”

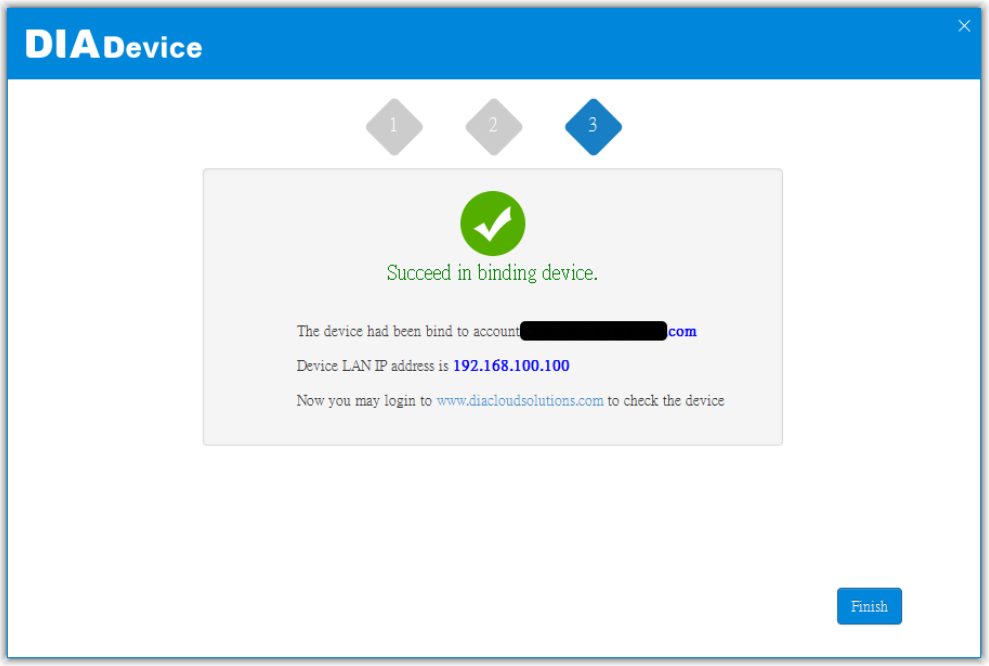
2. Enter the DIAcloud account number and password, and click Next.



3. After binding configuration is configured, click “Bind” to bind.



4. If your device is successfully bound to the cloud, the following screen will appear

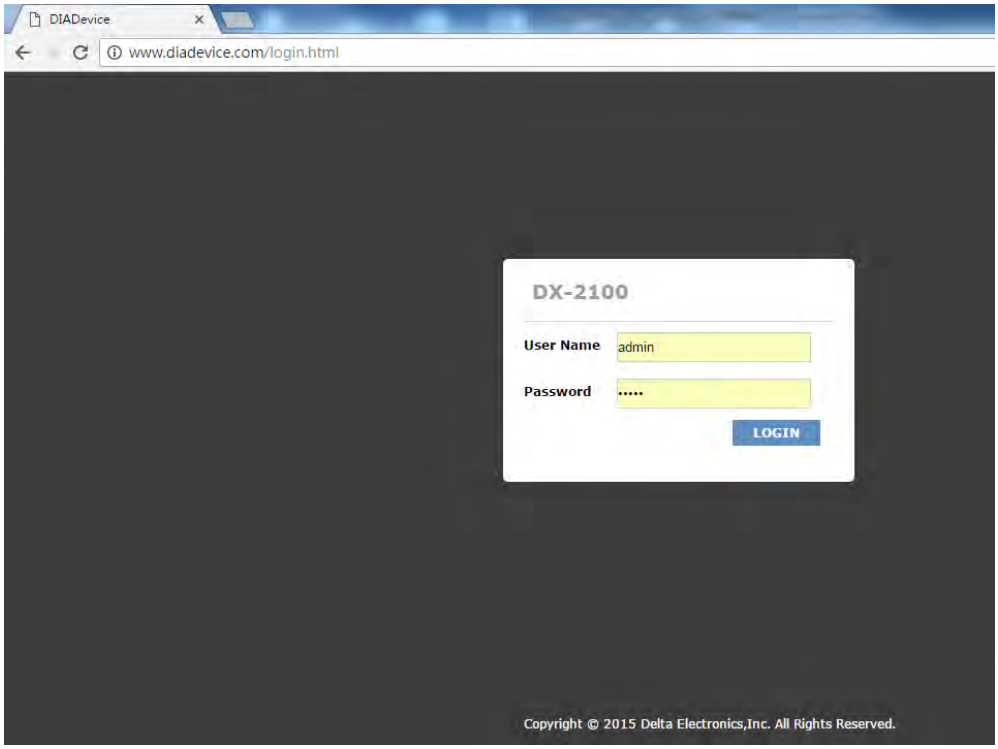


Notice

If the device has been bound to the cloud account, you need to switch to another cloud account binding, repeat 1-3 steps only and then enter the new cloud account you intend to bind.

2.2.4 Open Device Webpage

Click open device webpage button, the browser will open the device settings page, users can set the parameters of RS232 / 485 configuration.



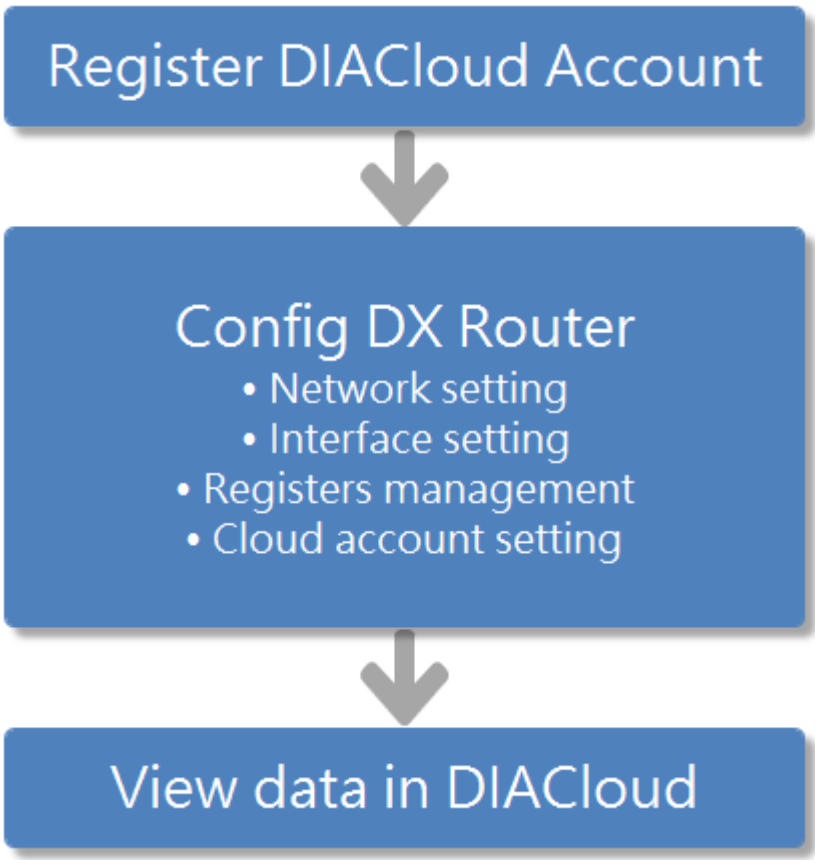
2.3 Typical application configuration

DX-2100 is an industrial-grade cloud router, providing users an easiler and faster experience of remote data collection and remote device debugging.

2.3.1 Data collection

DX router can connect to the Slave via serial port or Ethernet port, router with more than 2000 built-in registers, supporting standard Modbus RTU ASCII and Modbus/TCP protocol, and Mitsubishi MC and Siemens TCP protocol, to collect, receive and upload data to the cloud in the master-slave mode.

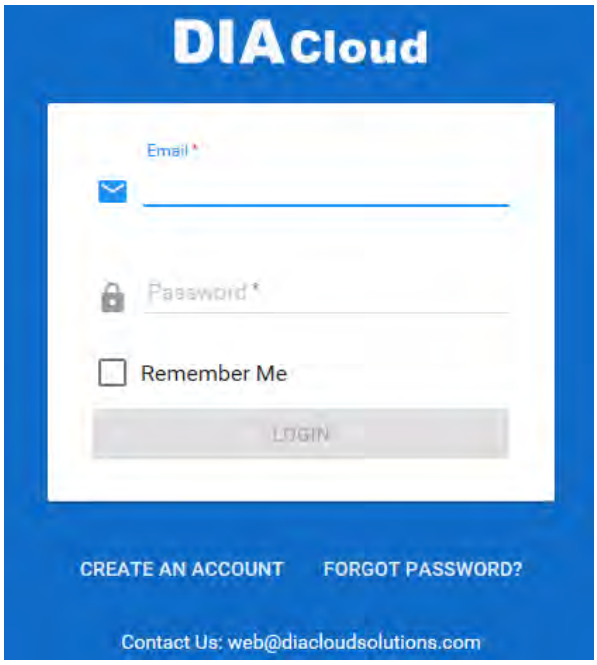
The basic steps of data collection are as follows:



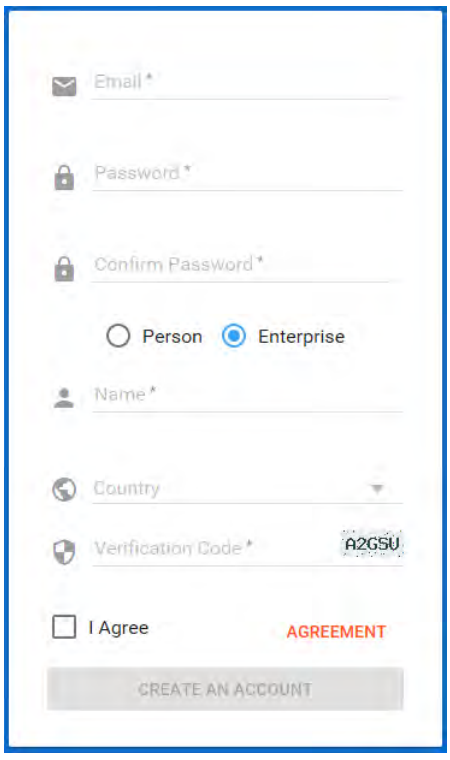
1. Register DIACloud Account

Cloud account is an important credential of DX router ownership. When the router is bound with a DIACloud account, only the account or the sub-account authorized by the account can access the device remotely. All data uploaded by the router belongs to this account, which can only be accessed by this account or sub-accounts authorized by this account. If you haven't had a cloud account, follow these steps to register:

- Browsing DIACloud website (http://www.DIACloudSolutions.com), click "CREATE AN ACCOUNT".



- Fill in account info and select “I Agree”, then click “CREATE AN ACCOUNT” button.



- Login your mailbox. Open the activation email sent from no-reply@DIACloudSolutions.com and complete DIACloud account activation operation.

2. Config DX Router

Please find below the guide to configuring the DX router for the purpose of making it as the modbus master to collect the data from Delta PLC via RS-485.

- Connect DX router to local PC via cable and login the config GUI. See section 2.1 for more details

- Normally the router has already been connected to internet with preset parameters of mobile network. Users can go to “Status”-“network status” in the menu to confirm the connection is ready.

Cellular Network Status

Connect | Disconnect

Operator	China Unicom 3G	Signal Strength	3
Connection Status	Online	Online Duration	5day 22:49:04
Authorization Mode	Auto	APN	3gnet
Telephone Number	+8618559634093	IP Address	10.141.239.9
Network Mask	255.255.255.255	Gateway Address	10.141.239.9
Primary DNS	218.104.128.106	Secondary DNS	58.22.96.66
SIM Card Status	SIM card normal		

- Go to "System”-“RS485” and set the mode as “Master mode”. Please find below for the detailed configuration:

RS485

Working Mode	Master mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Slave ID	1
Mode	Modbus RTU
Timeout	200 (ms)

Read/Write Configuration

Scan Interval: 30000 (ms)

When communicate with PLC of Delta, the starting address can be set as the internal register number. For example, input 0 for register D0.

The acceptable address range of this device is: $0-$1535 or $2048-$4095 or M0-M511.

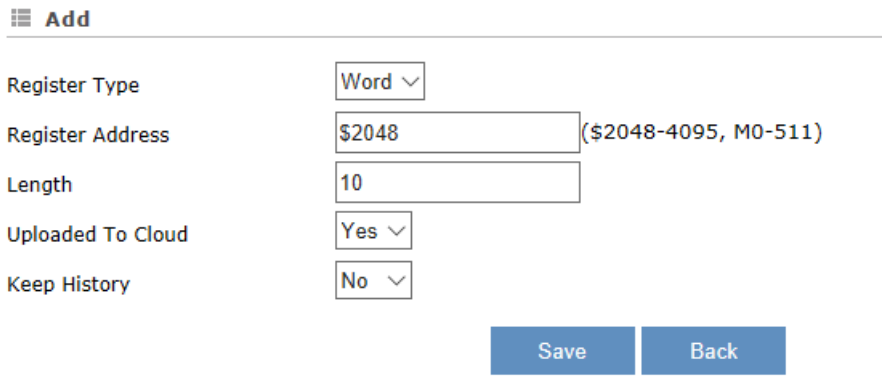
Add Mappings | Delete All Mappings | Export Configure List | Import Configure List

浏览...

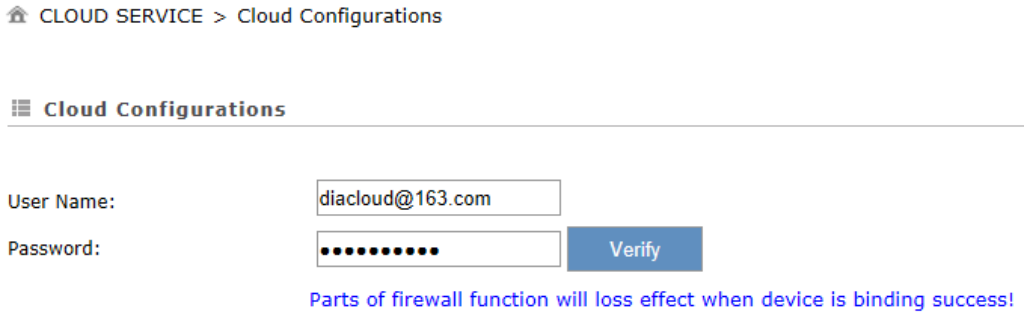
Row Number	Read/Write	Slave ID	Controller	Address Type	Slave Starting Address	Bit	Device Starting Address	Length (1-123)	Operation
1	Read/Write	1	Delta DVP PLC	D	100	0	$2048	10	+ -

Save | Cancel

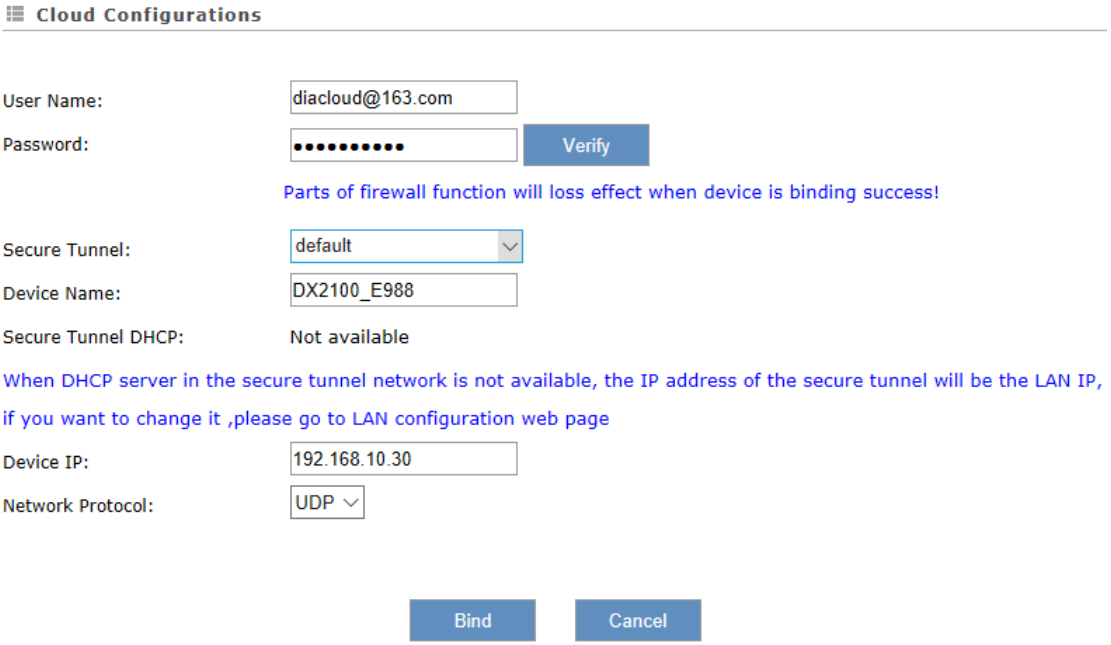
- Go to “System”-“Register Management” and set up the data upload rules. Please find below for the detailed configuration:



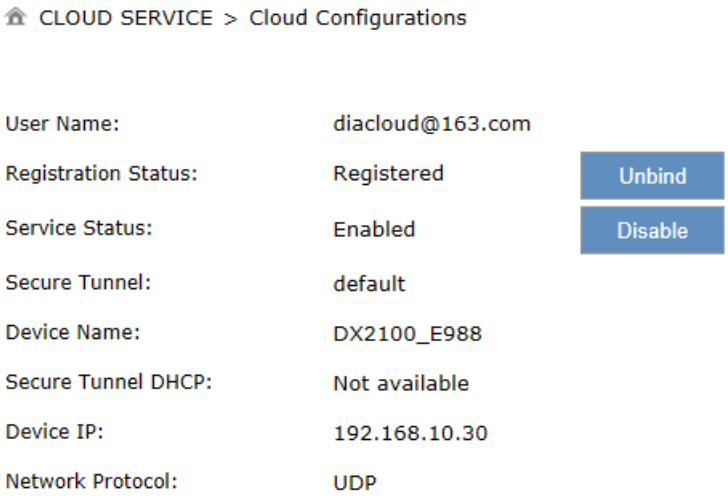
- Go to “Cloud Service”-“Cloud configurations” and bind the device with DIACloud account Please find below for the detailed configuration:



- Click the "verify" button to verify the user name/password, the below messages will be displayed after verification passes. Users can use the default parameters and click the "bind" button to bind the device to this account.

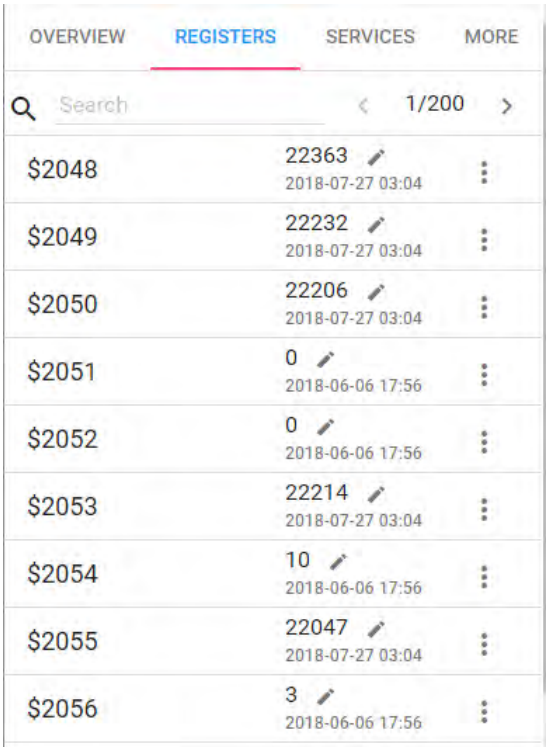


After binding completed, users can enter the device configuration page again and check the binding information.



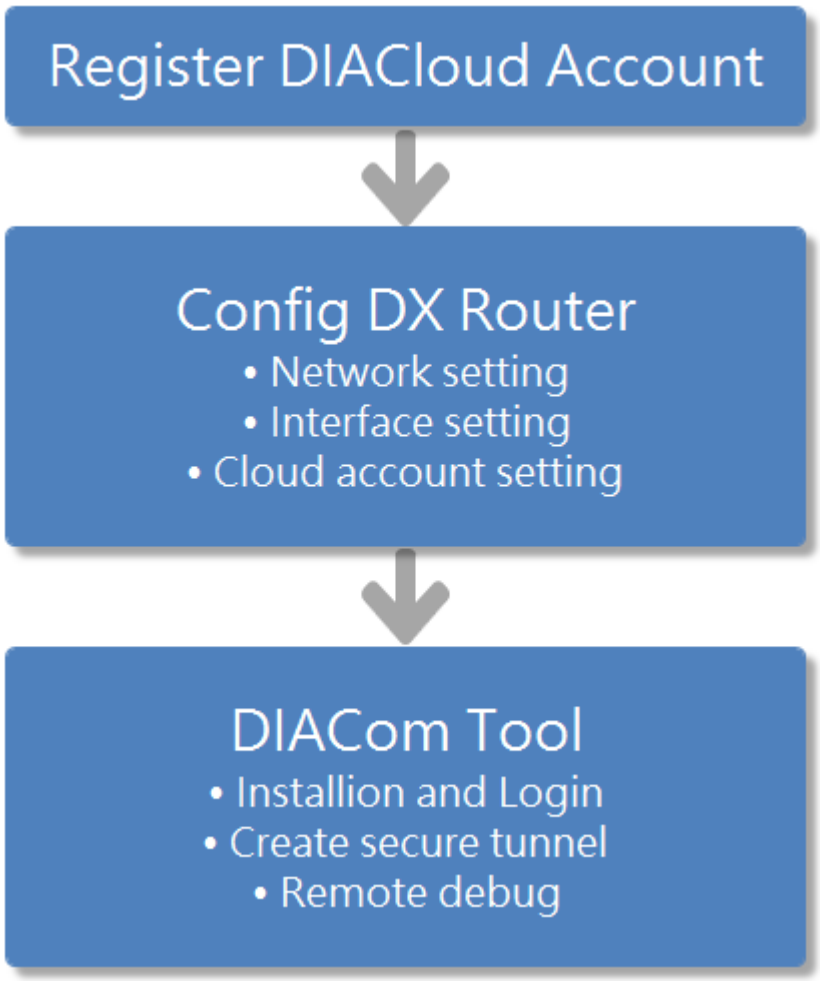
3. View data in DIACloud

- Browsing DIACloud website, login with your account.
- Click “Devices” in the menu, find the target device and click the *** to view the detail.
- Select “Registers” to display the register list, values behind registers’ addresses are the collection data.



2.3.2 Remote debugging

DX router features a built-in DIACloud cloud service, so when the router is bound to the DIACloud account and connected to the DIACloud cloud platform, the router and the cloud platform will create a secure tunnel, and all the devices in the same secure tunnel group under the account will be in the same secure virtual LAN. With our DIACom PC tool, users can also add their local computers to the virtual LAN, allowing them to download and debug remote devices as if they were operating locally, either through the network port or by creating a virtual serial port.



1. Register DIACloud Account

If your DIACloud account already exists, skip to step 2. To register a new account, please refer to section 2.3.1

2. Config DX Router

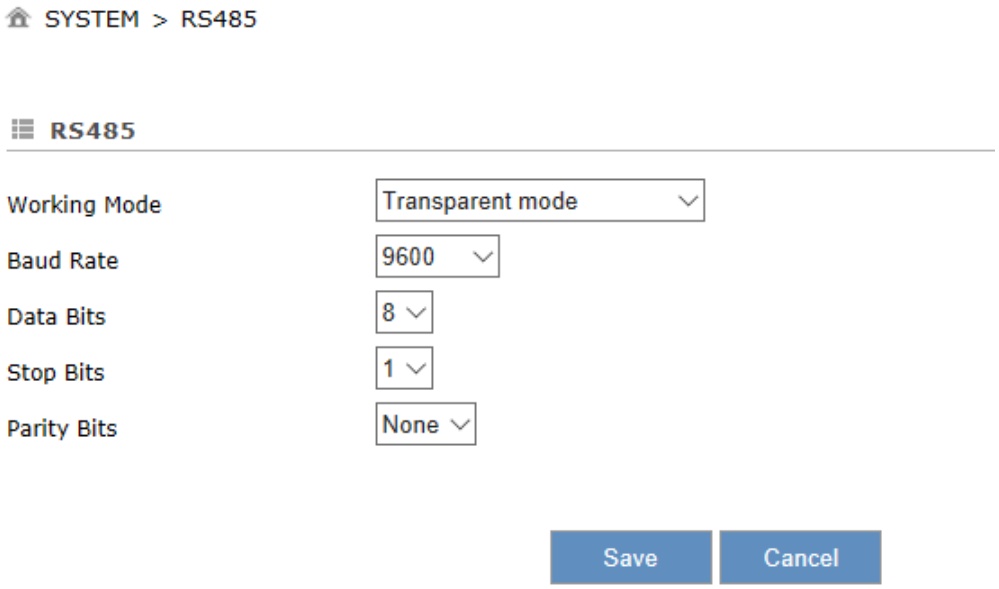
Please find the below steps to perform remote debug with Delta PLC via RS-485 by configuring the DX router.

- Connect DX router to local PC via cable, login the config GUI. See section 2.1 for more details
- Normally the router has already been connected to internet with preset parameters of mobile network. Users can go to “Status”-“network status” in the menu to confirm the connection is ready.

Cellular Network Status Connect Disconnect

Operator	China Unicom 3G	Signal Strength	3
Connection Status	Online	Online Duration	5day 22:49:04
Authorization Mode	Auto	APN	3gnet
Telephone Number	+8618559634093	IP Address	10.141.239.9
Network Mask	255.255.255.255	Gateway Address	10.141.239.9
Primary DNS	218.104.128.106	Secondary DNS	58.22.96.66
SIM Card Status	SIM card normal		

- Go to ”System”-“RS485” in the menu and set the working mode as “Transparent mode”, configuration as follows:

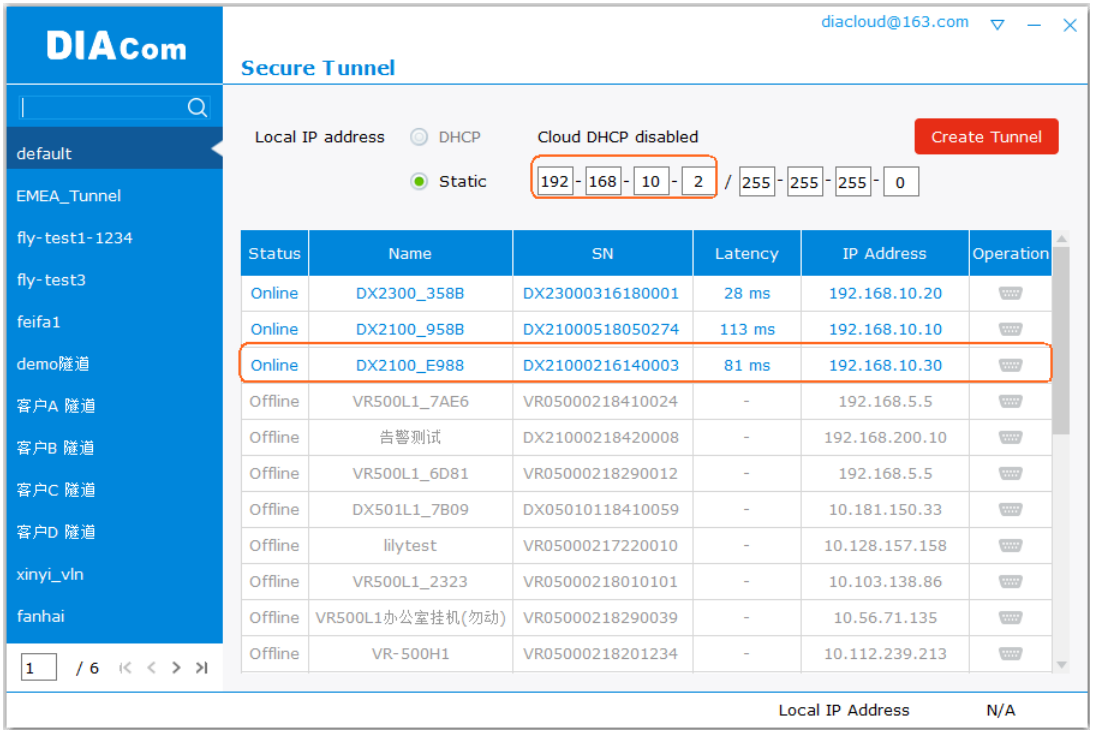


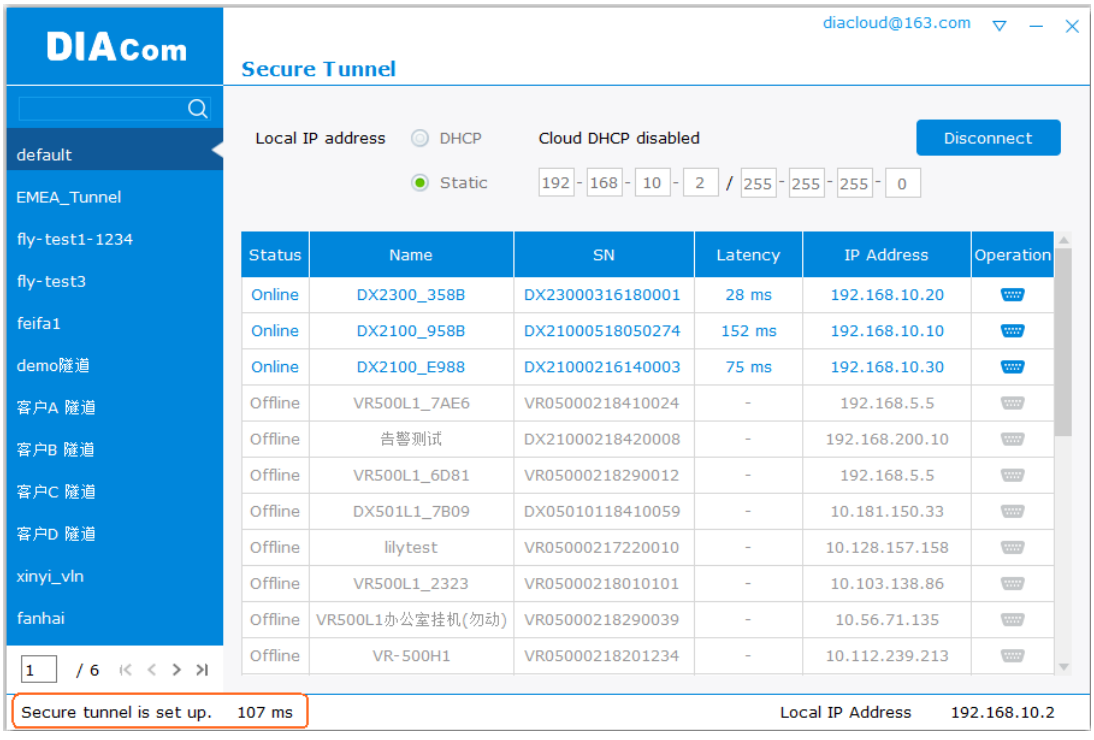
- Go to ”Cloud Service”-“Cloud configurations” and bind the device with DIACloud account, please refert to section 2.3.1 for more details.

3. DIACom Tool

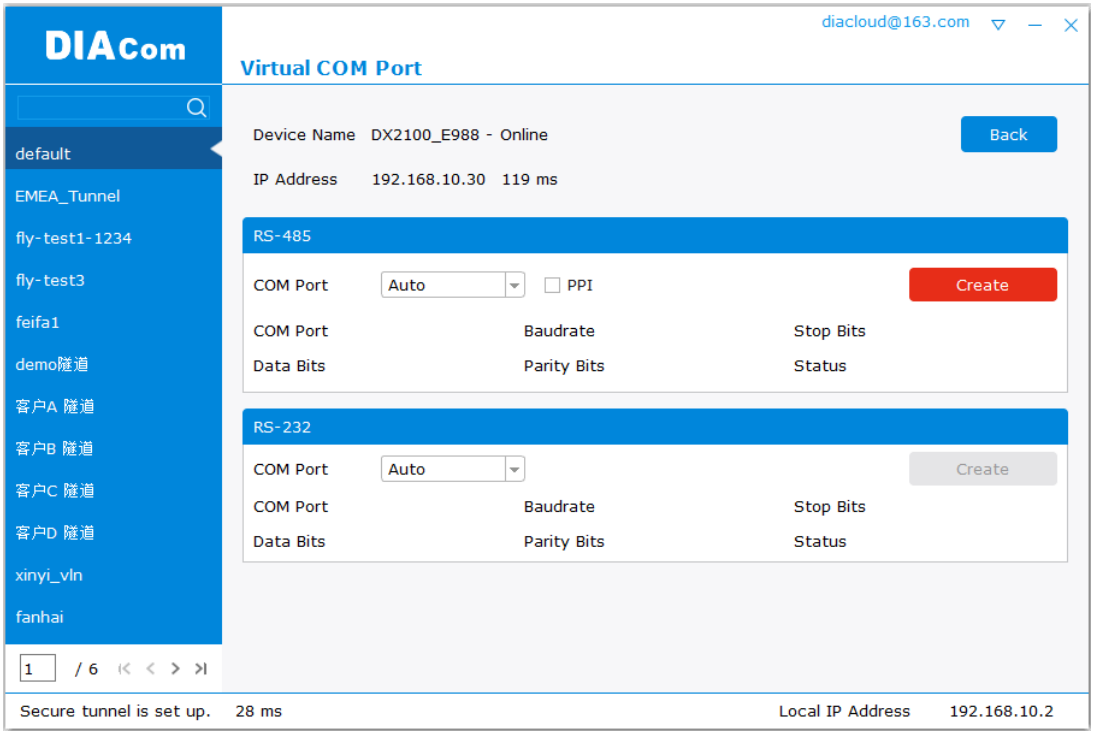
- Obtain the DIACom firmware package from the official website or from our sales representative. Administrator privileges are required to run and install the package. After install successfully, run this programe and login with DIACloud account.

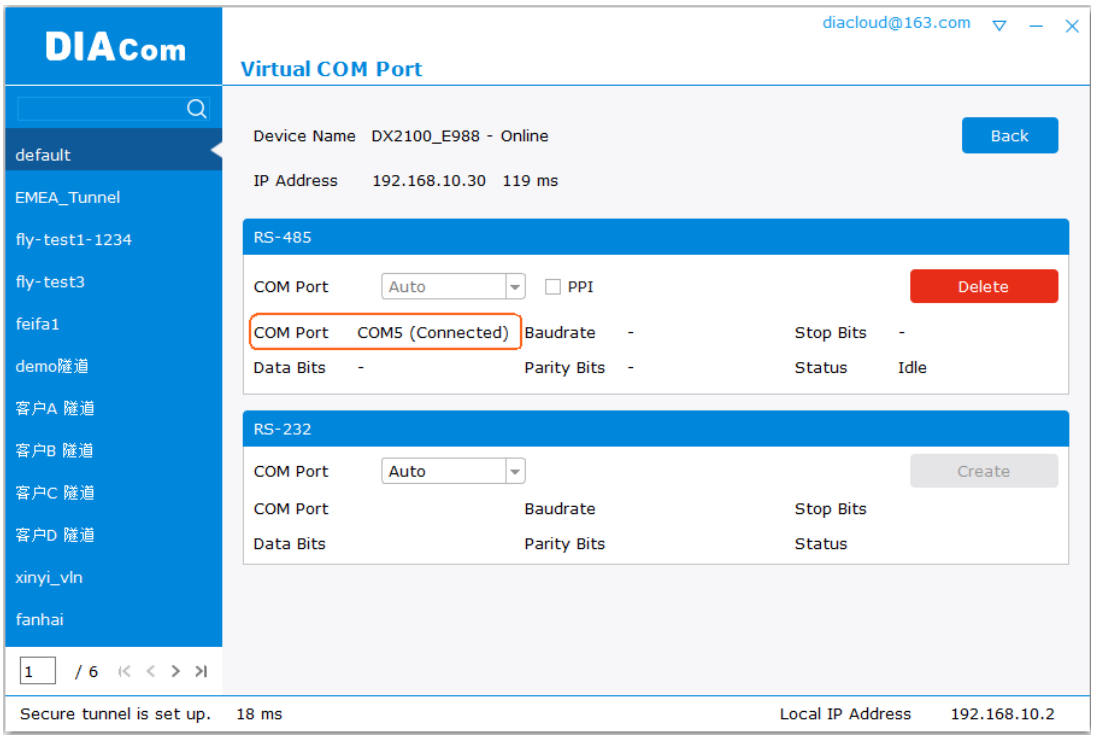
- Select the tunnel group which the target DX device belongs to. Set up local IP address same segment with DX route and click “Create Tunnel” button. Messages will be shown on the lower-left corner of the status bar after the tunnel is created.



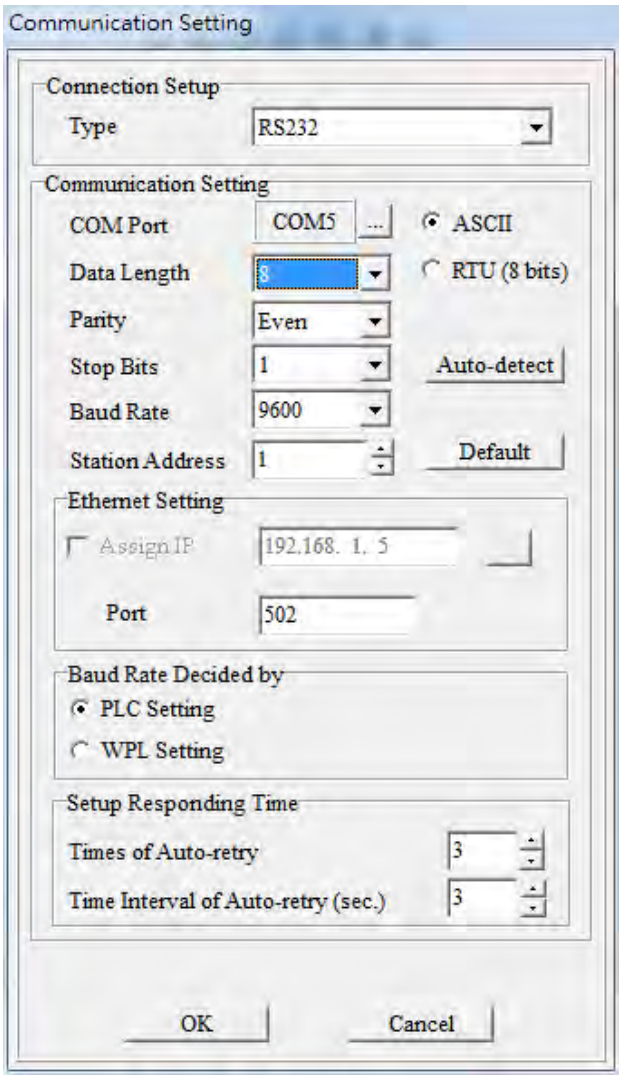


- After the tunnel has been created, click button of the DX router, goto create virtual com page. If “Create” button is not available, please check the RS-485 wrok mode in DX router config page.





- After the virtual serial port is created, open the corresponding debugging tool WPLSoft, you can upload and download the program to the PLC remotely with the connection to DX router through RS-485.


Communication Setting
Connection Setup
Type
RS232
Communication Setting
COM Port
COM5
...
ASCII
Data Length
8
RTU (8 bits)
Parity
Even
Stop Bits
1
Auto-detect
Baud Rate
9600
Station Address
1
Default
Ethernet Setting
Assign IP
192.168. 1. 5
Port
502
Baud Rate Decided by
PLC Setting
WPL Setting
Setup Responding Time
Times of Auto-retry
3
Time Interval of Auto-retry (sec.)
3
OK
Cancel

3

Chapter 3 Functions

Table of Contents

3.1 Status 3-3
3.1.1 Device Information 3-3
3.1.2 Network Status 3-5
3.1.3 Routing Table 3-6
3.1.4 Local Log 3-6
3.1.5 Traffic Statistics 3-7
3.1.6 Cloud Status 3-7
3.1.7 Connected Device 3-8
3.2 Network 3-8
3.2.1 Cellular Network Configurations 3-8
3.2.2 PIN Management 3-11
3.2.3 LAN Configurations 3-14
3.2.4 Static Routing Rules 3-16
3.2.5 Dynamic DNS 3-18
3.3 Firewall 3-19
3.3.1 Firewall Settings 3-19
3.3.2 DMZ Settings 3-19
3.3.3 Port Forward 3-20
3.3.4 Port Trigger 3-22
3.3.5 URL Filter 3-24
3.3.6 MAC Filter 3-24
3.3.7 IP Filter 3-25
3.4 System 3-26
3.4.1 User Management 3-26
3.4.2 Time Zone Configurations 3-27
3.4.3 RS232 3-28
3.4.4 RS485 3-38
3.4.5 Modbus TCP 3-46
3.4.6 Siemens TCP 3-49
3.4.7 Log Settings 3-52
3.4.8 Firmware Upgrade 3-53
3.4.9 Backup & Restore 3-53
3.4.10 Scheduled Jobs 3-54
3.4.11 Add A New Job 3-54
3.4.12 Export Job List 3-55

3.4.13 Import Job List 3-55
3.4.14 Network Diagnosis 3-55
3.4.15 Trouble shooting 3-56
3.4.16 System Reboot 3-57
3.4.17 Privilege Management 3-57
3.4.18 Event Management 3-60
3.4.19 Register Management 3-63
3.5 Cloud Service 3-65
3.5.1 Cloud Configuration 3-65
3.5.2 Secure Tunnel Firewall 3-68
3.5.3 Cloud Log 3-69
3.6 SD Card Quick Configuration 3-70

3.1 Status

You can view summary or detailed information of Device Information, Network Status, Routing Table, Local Log, Traffic Statistics, Cloud Status, and Connected Device.

3.1.1 Device Information

This page shows basic information on the Hardware/Software version and Resource Usage Information.

STATUS > Device Information

Hardware Version

RTM Version:	DX2100 v2.new
Release Date:	2015-06-26 05:28:00 PM
S/N:	DXR02010E320036

Software Version

RTM Version:	DX2100 1.3.0.1
Release Date:	2015-06-26 05:28:00 PM
Current Version:	DX2100WW-1.3.1.1-2016-04-29
Upgrade Date:	2016-05-05 17:39:45

Resource Usage Information

CPU Usage:	15%
Total Memory:	123888KB
Memory Used:	69812KB
Memory Usage:	56%

- Hardware Version

Item	Description
RTM Version	Release to manufacturing version of the router
Release Date	Hardware release date
S/N	Serial number of the router

- Software Version

Item	Description
RTM Version	Release to manufacturing version of the software
Release Date	Software release date
Current Version	Version number of the software currently used on the router
Upgrade Date	Upgrade time of the software currently used on the router

- Resource Usage Information

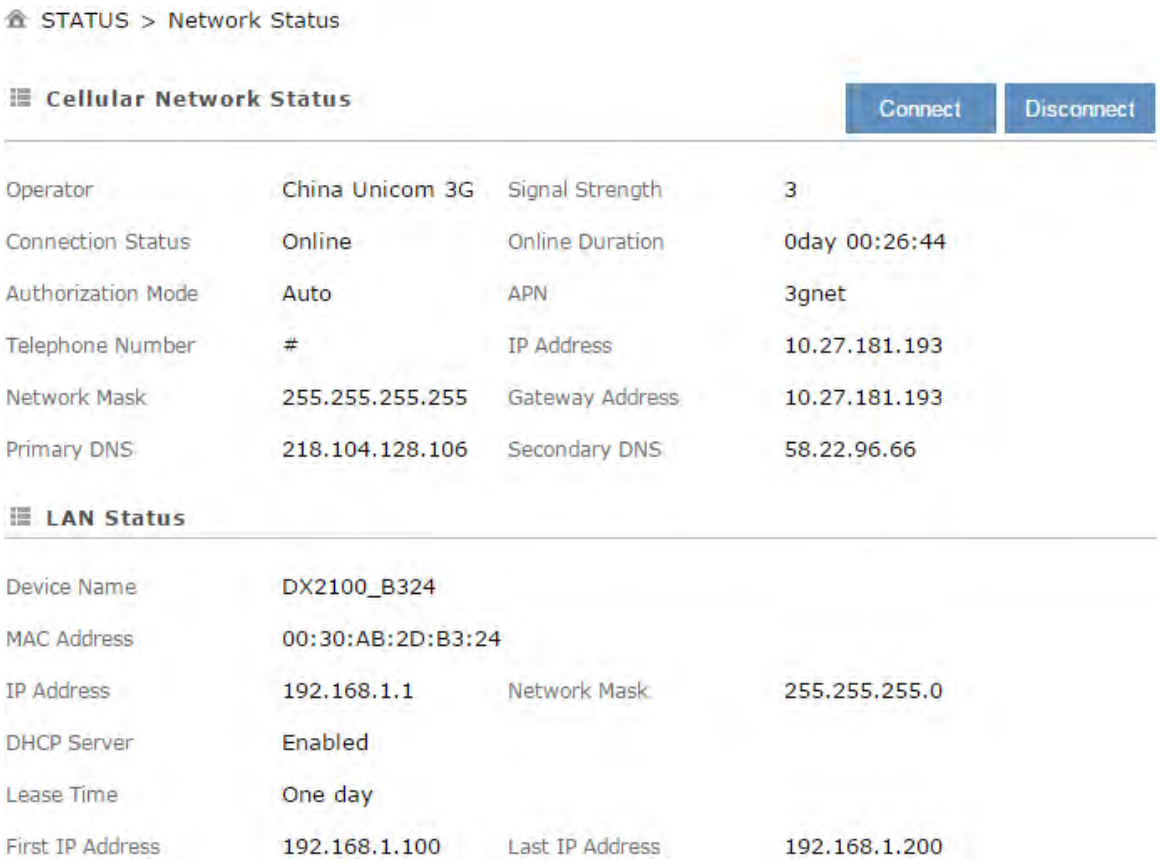
Item	Description
CPU Usage	The CPU usage of current router
Total Memory	The total memory on the router
Memory Used	The memory currently used on the router.
Memory Usage	The current ratio of the router usage

3.1.2 Network Status

This page shows basic information on Cellular Network Status and LAN Status.

Cellular Network Status includes the Operator, Signal Strength, Connection Status, Online Duration, Authorization Mode, APN, Telephone Number, IP Address Network Mask, Gateway Address, primary DNS, and Secondary DNS.

LAN Status includes the Device Name, MAC Address, IP Address, DHCP Server, Lease Time and First IP Address.



3.1.3 Routing Table

This page shows basic information on the routing table, including the Destination, Gateway, Network Mask, HOPS and Network Interface.

STATUS > Routing Table

Destination	Gateway	Network Mask	HOPS	Network Interface
10.64.64.64	0.0.0.0	255.255.255.255	0	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	0	br0
0.0.0.0	0.0.0.0	0.0.0.0	0	ppp0

3.1.4 Local Log

This page shows logs of the router, including the System log, Warning lot and the Debug log. You can use the buttons on the right side to refresh, clear or download the displayed logs.

STATUS > Local Log

Log Type

Informative log Warning log Debug log

Log Content

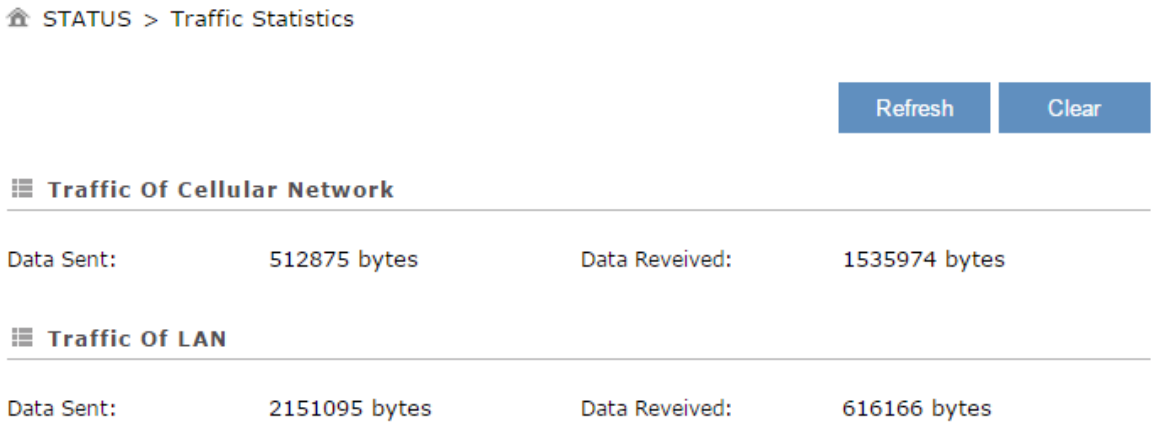
Refresh Clear Download

Timestamp	Content
May 6 10:09:08	syslog.info syslogd started: BusyBox v1.15.0
May 6 10:09:15	user.info kernel: ip_tables: (C) 2000-2006 Netfilter Core Team
May 6 10:09:17	user.info kernel: ipt_CLUSTERIP: ClusterIP Version 0.8 loaded successfully
May 6 10:09:19	user.info kernel: arp_tables: (C) 2002 David S. Miller
May 6 10:09:22	user.info kernel: usbcore: registered new interface driver usbserial
May 6 10:09:22	user.info kernel: USB Serial support registered for generic
May 6 10:09:22	user.info kernel: usbcore: registered new interface driver usbserial_generic
May 6 10:09:22	user.info kernel: usbserial: USB Serial Driver core
May 6 10:09:22	user.err kernel: cdc_acm 1-1:1.0: This device cannot do calls on its own. It is not a modem.
May 6 10:09:22	user.info kernel: cdc_acm 1-1:1.0: ttyACM0: USB ACM device
May 6 10:09:22	user.err kernel: cdc_acm 1-1:1.2: This device cannot do calls on its own. It is not a modem.
May 6 10:09:22	user.info kernel: cdc_acm 1-1:1.2: ttyACM1: USB ACM device

PREV 1 2 3 ... 13 14 15 NEXT

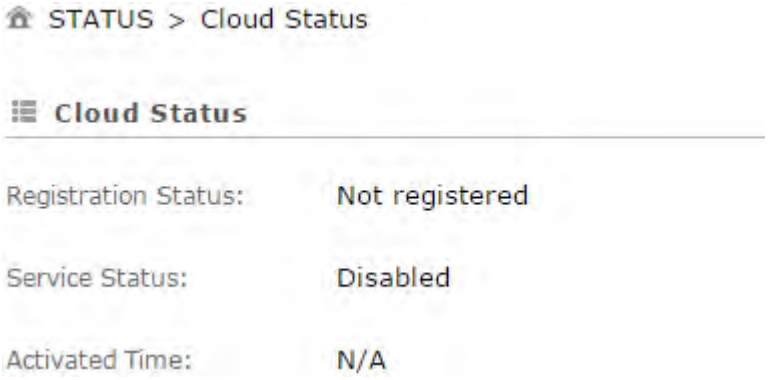
3.1.5 Traffic Statistics

This page shows network traffic information of the router, including the data sent and received over Cellular and LAN. You can use the buttons on the right side to refresh or clear the traffic information.



3.1.6 Cloud Status

This page shows cloud server information of the router, including the Registration Status, Service Status, and Activated Time.



3.1.7 Connected Device

This page shows information of the devices connected to the router, including the IP Address, Host Name, MAC Address.

STATUS > Connected Device

Refresh

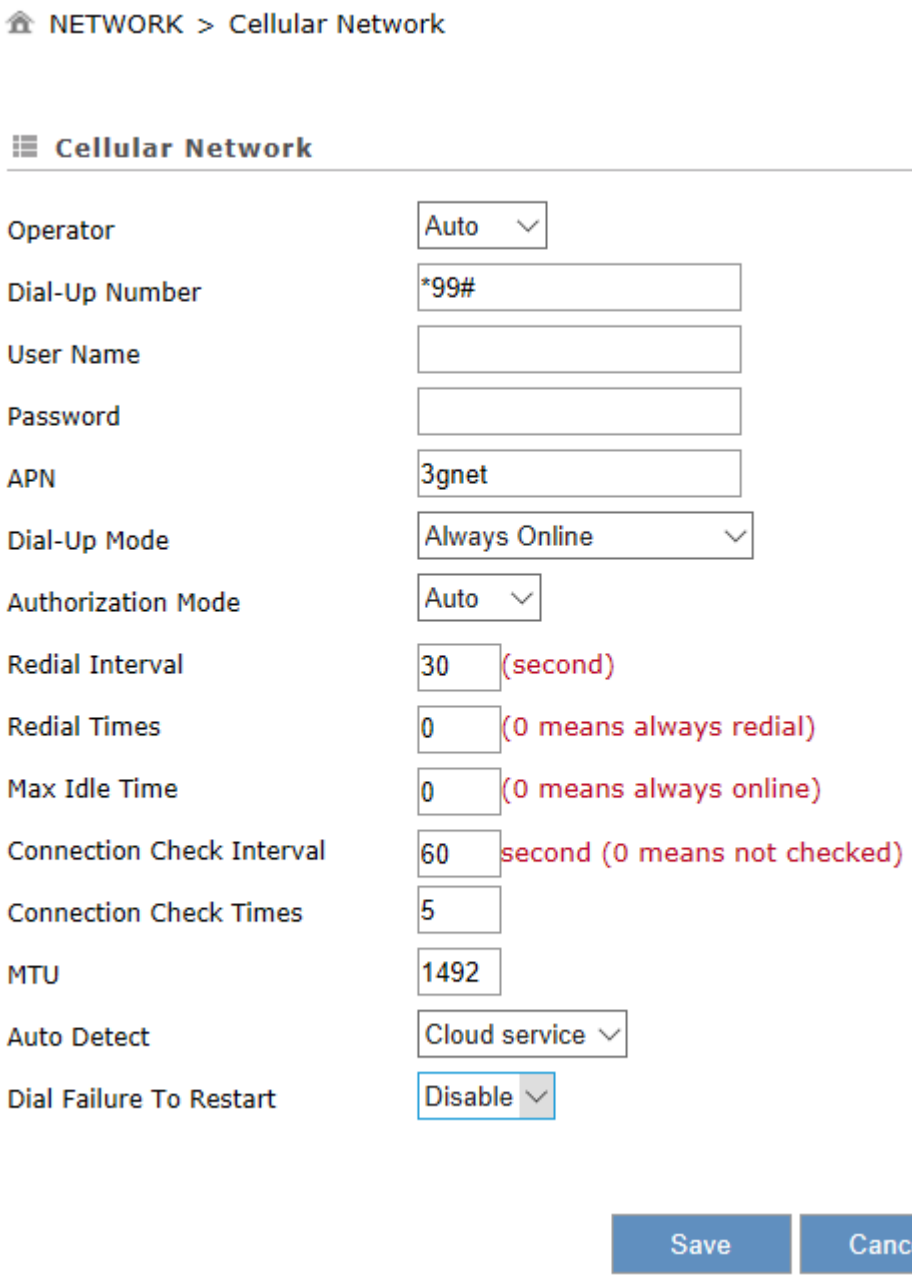
ID	IP Address	Host Name	MAC Address
1	192.168.1.100	CNXMDNIPC062	3C:97:0E:DE:7B:25

3.2 Network

You can set up networks, including the WAN Configurations, LAN Configurations, Static Routing Rules and Dynamic DNS.

3.2.1 Cellular Network Configurations

This page is used for setting up the Cellular Network, including the Operator, Dial-Up Number, User Name, Password, APN, Dial-Up Mode, Authorization Mode, Redial Interval, Redial Times, Max Idle Time, Connection Check Interval, Connection Check Times, and MTU.



Description	Default
Operator	
Select Auto or Others for the Operator from the dropdown list. • **Auto:** the system will detect the operator from the inserted SIM card and set up accordingly. • **Others**: users can set up the operator manually.	AUTO
Dial-Up Number	
This number is provided by the operator. When “Auto” is selected, the system will set the number up automatically and users cannot change the setting.	*99#

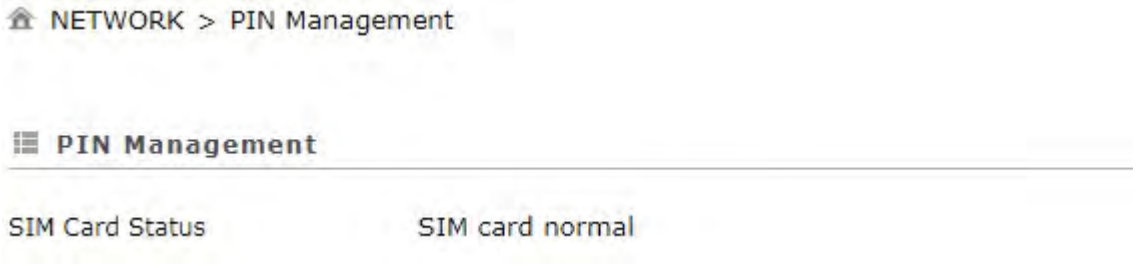
Description	Default
User Name	
This name is provided by the operator. When “Auto” is selected, the system will set the name up automatically and users cannot change the setting.	N/A
Password	
This password is provided by the operator. When “Auto” is selected, the system will set the password up automatically and users cannot change the setting.	N/A
APN (Access Point Name)	
This APN is provided by the operator. When “Auto” is selected, the system will set the APN up automatically and users cannot change the setting.	3gnet
Dial-Up Mode	
Options are : • **Always online**: stay connected and once a disconnection is detected, the router will redial to connect automatically. • **On-demand connection**: redial when connection to the internet is on demand. • **Manual connection**: users dial to connect and when it fails to connect, it will not redial.	Always online
Authorization Mod	
Options are “Auto”, “PAP” and “CHAP”.	Auto
Redial Interval	
Set the time to redial when the system fails to connect. This will only be executed when the option “Always online” or “On-demand connection” is selected.	30
Redial Times	
Set the maximum redial time, 0 indicating infinity. This will only be executed when the option “Always online” or “On-demand connection” is selected.	5
Max Idle Time	
Set the maximum idle time. When the idle time exceeds the set value, the router will disconnect and then redial, 0 indicating not to disconnect.	180
Connection Check Interval	
Set the connection check interval. Check the connectivity, if the connection is lost, it will redial automatically, 0 indicating not to check the connectivity.	60
Connection Check Times	
Set the connection check times, 0 indicating infinity. Once a disconnection is detected, and the option “Always online” or “On-demand connection” is selected, the router will redial according to the set value in the Redial Times.	5

Description	Default
MTU	
Maximum Transmission Unit is the largest packet that can be transmitted over packet based networks.	1492
Auto Detect	
With two ways to detect the network connection automatically, users can choose between “PING” and “Cloud Service” or choose “Disable” to shut down this function.	Cloud Service
Target Address	
Set the IP/domain of the server that program will do a ping testing.	www.DIACloudSolutions.com
Dial Failure To Restart	
Enable or disable the function if the dial failure will be in the default time to restart device.	Disable

3.2.2 PIN Management

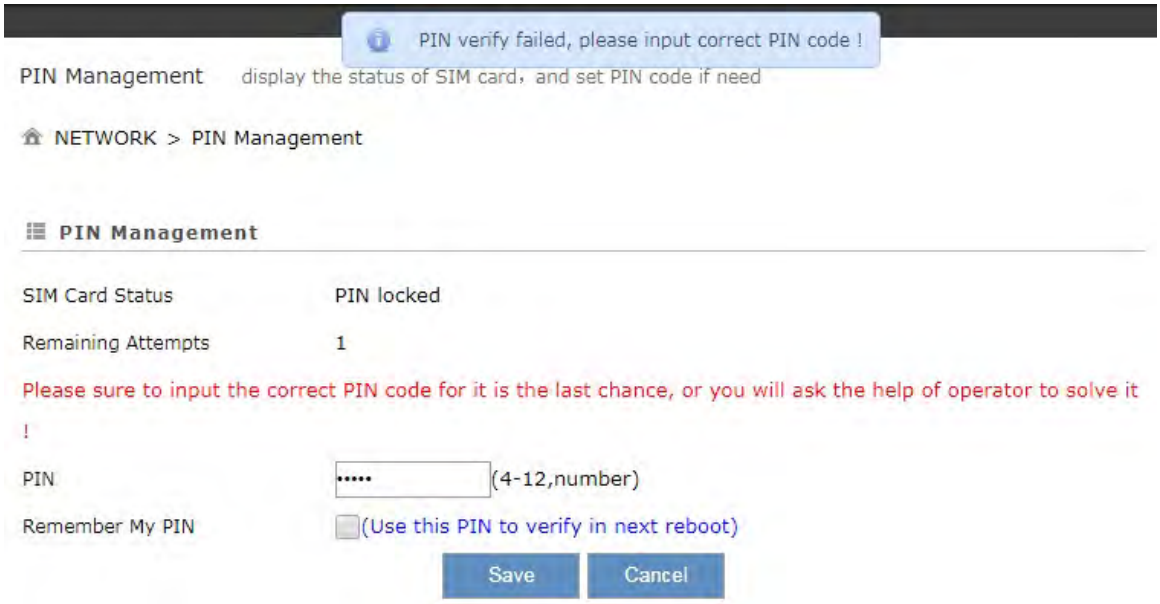
Operators can use this feature to view or unlock PIN LOCK.

- The SIM card is inserted correctly and functions normally, which the status would be shown as below

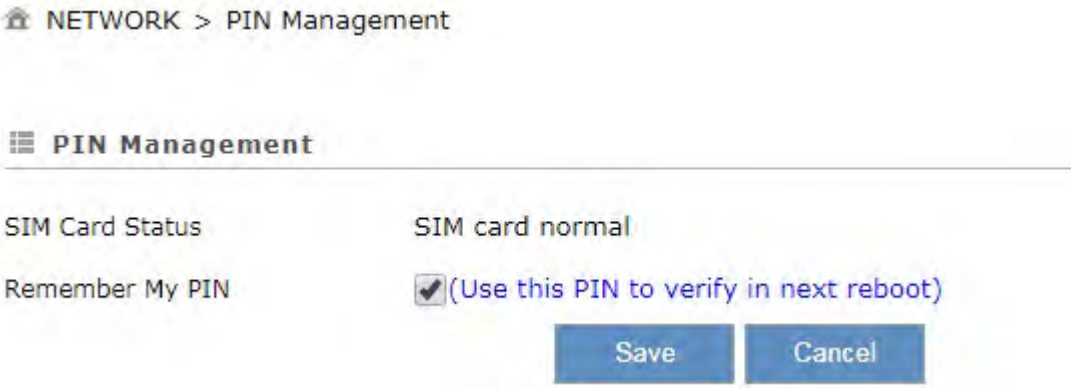


- The SIM card is inserted correctly and need correct PIN code input to operate normally, which the status would be shown as below.

- A pop-up dialogue box would be displayed as below if the verification fails.



- If the verification passes, it will display as below.

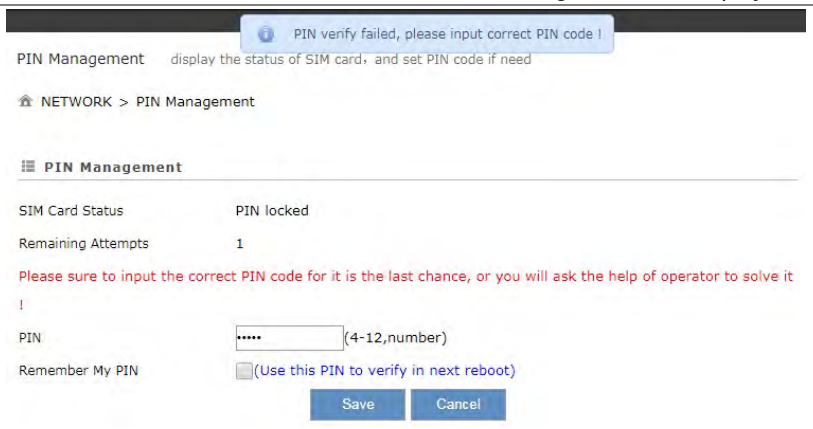


Description	Default
SIM card status	
● No SIM： No SIM cards detected in the slot. ● SIM card normal：The SIM card is in the slot and functions normally. ● PIN locked：Need the correct PIN code input to enable the SIM card. ● PUK locked：Exceed the maximum PIN code input tries. Need the correct PUK (Personal Unlocking Key) to unlock and resume normal operation.	N/A
Remaining attempts	
The allowable entry attempts is normally 3 times. When the remaining attempts is zero and the SIM card is locked, users must ask for help from operators or unlock it with PUK code.	N/A

Description	Default
PIN	
A personal identification number used in SIM card is a security measure to protect SIM card from being stolen.	N/A
Remember my PIN	
Enable this function to remember the PIN code in the system and the code would be input automatically every time after booting.	Uncheck

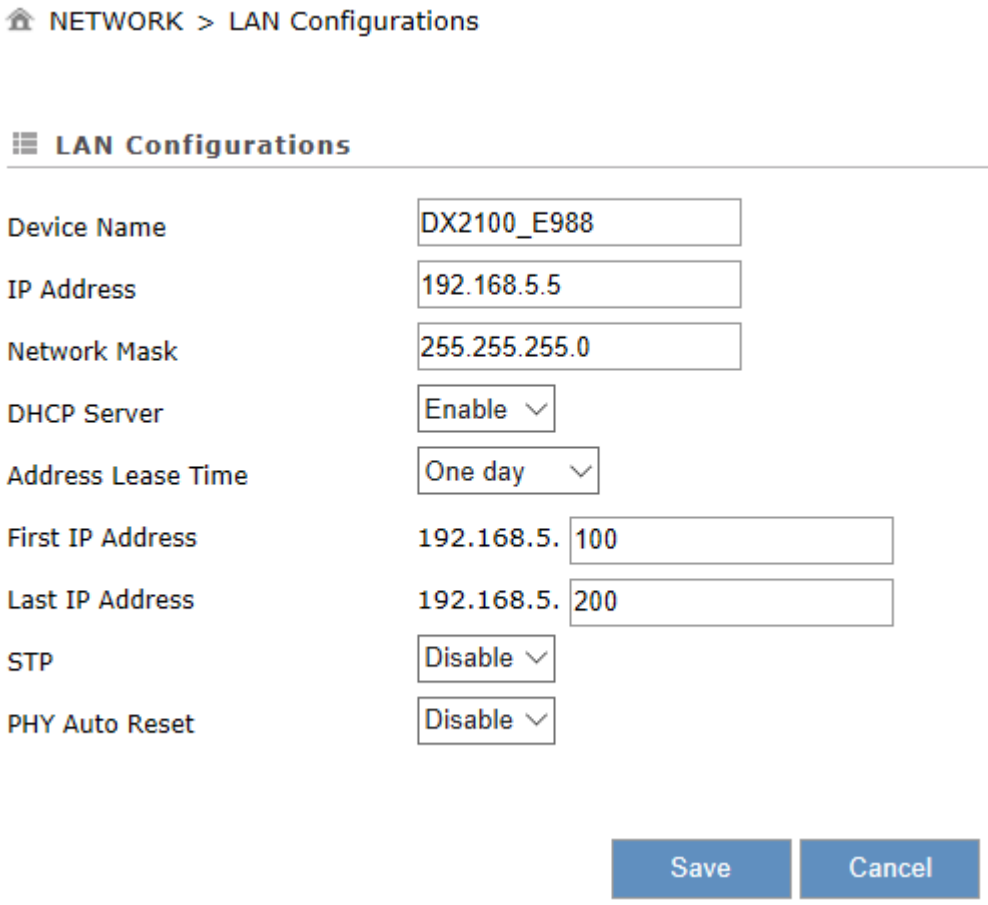
Notice

- If you enter the wrong PIN three times, your SIM card will become locked.
- Once SIM card is blocked, you need PUK code to unlock it or find operator's help.

Instruction	**Example: Insert and unlock a PIN-locked SIM card** 1. Insert a SIM card locked by PIN codes into the SIM1 slot of the DX Shell. 2. Login to DX system. 3. Follow the path: Network -> PIN Management to access "SIM1 PIN Management". 4. Enter the correct PIN code. 5. Click "Save" and a "unlock successful" message would be displayed.
Figure	

3.2.3 LAN Configurations

This page is used for setting up the LAN, including the Device Name, IP Address, Network Mask, and DHCP Server.



Description	Default
Device Name	
Set up a device name for your router. The name shall be composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	DX2100 + "_" + "the last four digits of Mac address"
IP Address	
Set up an IP address for your device.	192.168.5.5
Network Mask	
Set up the LAN network mask.	255.255.255.0
DHCP Server	
If DX router uses DHCP to assign IP addresses automatically on your network, you can specify the IP address range and lease time for the clients on your network. Once the DX router have bound the DIACloud and enabled the DIACloud DHCP, the DHCP in DX router will be disabled automatically.	Enable
Address Lease Time	
To set up the address lease time so that a client doesn't hold an IP address indefinitely. It allows for a mechanism to gracefully reuse DHCP addresses.	One day

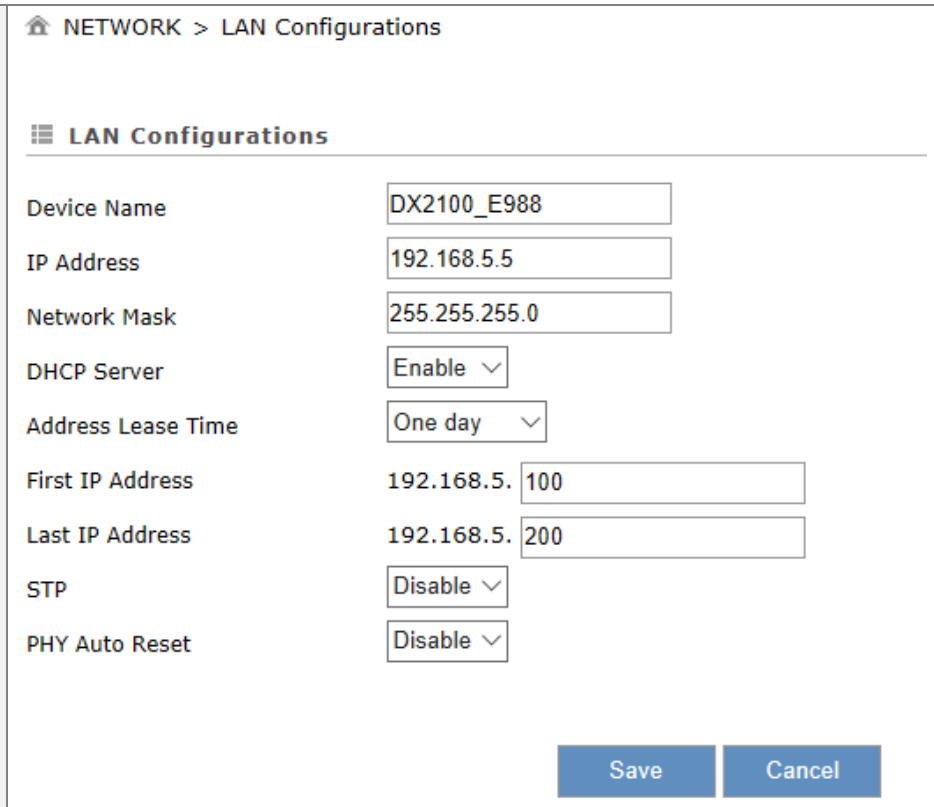
Description	Default
Options here are 1 to 3 days.	
First IP Address	
To increase the number of addresses available to clients, you can change the Start Address.	192.168.1.100
Last IP Address	
To increase the number of addresses available to clients, you can change the End Address.	192.168.1.200
STP	
STP is a network protocol that builds a logical loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. If this STP is enabled, the traffic usage will increase about 15Mbit in 24 hours.	Disable
PHY Auto Reset	
Activate DIACloud DHCP after the account is bound. To determine whether LAN needs to be reset if DIACloud is manually reboot or reconnected due to unstable network. ● Disable: Not allow LAN reset automatically. ● Enable: Allow LAN to be reset which would cause a short period of disconnection between devices and DX LAN ports **Notice:** It is suggested to disable DIACloud DHCP function and assign IP addresses in manual mode.	Disable

An example of operation:

1. Confirm "PHY Auto Reset" is set as Disable.

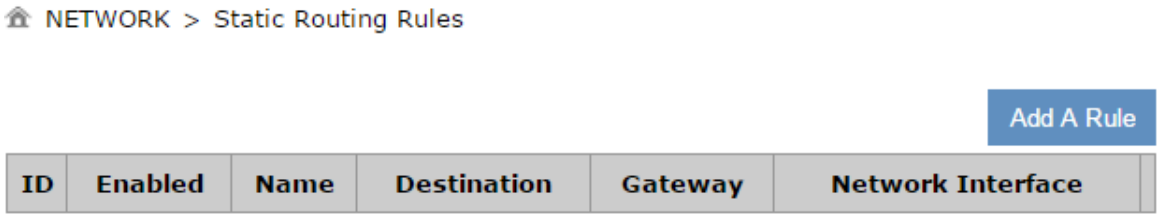
Instruction	1. Logged into www.diacloudsolutions.com 2. Click the secure tunnel and create a new network. 3. Enable the function to assign IP address 4. Log into DX webpage and bind your account to the DIACloud. Make sure if the LAN port is receiving the DHCP IP address from DIACloud. 5. Go to NETWORK -> LAN Configurations -> PHY Auto Reset and select Disable. 6. Connect the device to the LAN1 port. 7. Restart the Cloud service to see if the LAN1 is not trying to reconnect. (LAN1 should not be restarted.) 8. Connect your PC to LAN2 to ping LAN1 to see if the IP address of the LAN1 cannot communicate for a short time.

Figure

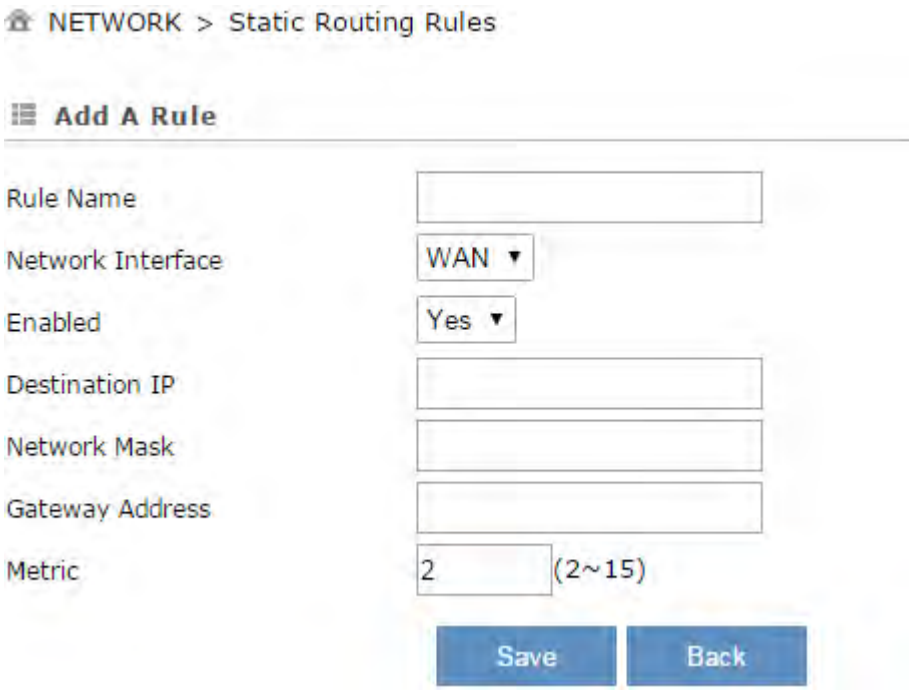


3.2.4 Static Routing Rules

This page is used for setting up the Static Routing, including the Rule Name, Network Interface, Enabled, Destination IP, Network Mask, Gateway Address and Metric. Click the "Add A Rule" to add static routing rules.



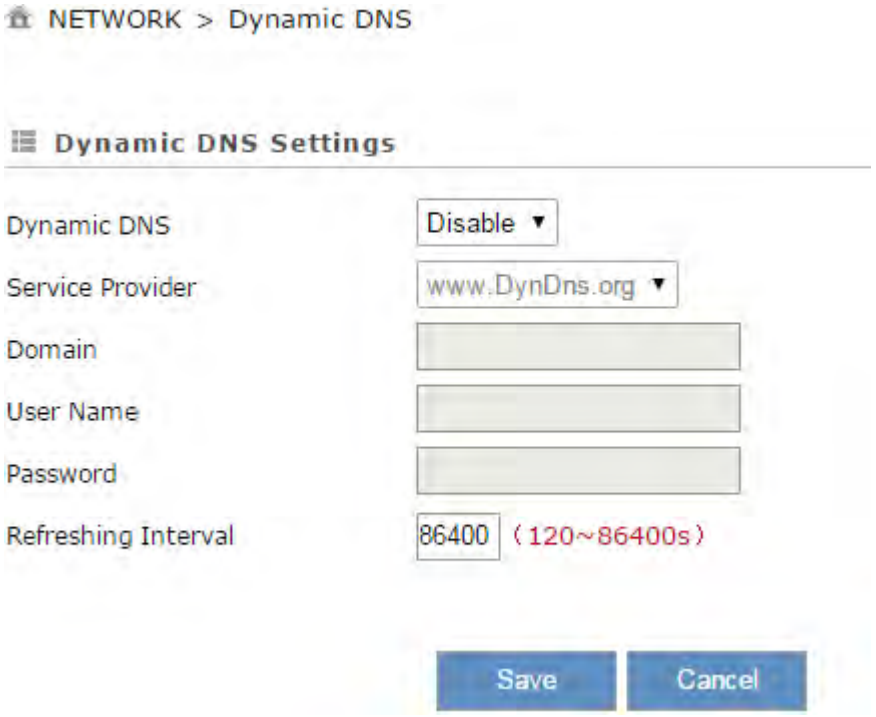
After clicking the "Add A Rule", you will see the following page.



Description	Default
Rule Name	
Set up a name for your rule. The name shall be composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Network Interface	
For a specific network destination address, select the network interface of the router for sending data package. Options are LAN and WAN.	WAN
Enabled	
Activate the static routing functionality.	Yes
Destination IP	
Set up a Destination IP address for your device.	N/A
Network Mask	
Set up the subnet mask corresponding to the destination network segment. If the final destination of the routing is a single host, please type in 255.255.255.255.	N/A
Gateway Address	
Set up the next-hop routing address.	N/A
Metric	
Set up the hops. The number of hops that are passed for reaching the destination address. One hop indicates passing one router passed. The range is 2~15.	2

3.2.5 Dynamic DNS

This page is used for setting up the Dynamic DNS Settings, including the Dynamic DNS, Service Provider, Domain User Name, Password, and the Refreshing Interval.



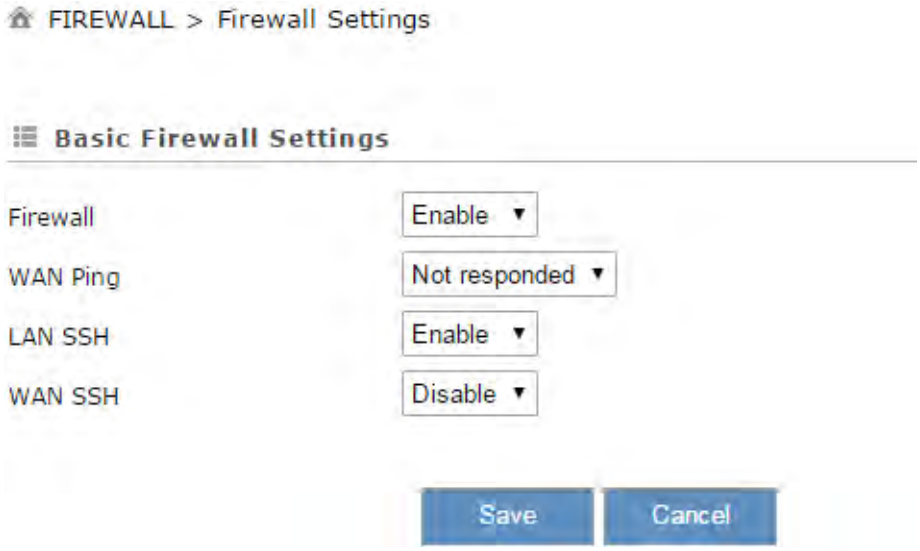
Description	Default
Dynamic DNS	
Dynamic Host Configuration Protocol allows you to obtain an IP address automatically from your router. You can enable or disable this functionality.	Disable
Service Provider	
Select the dynamic domain service provider. Options are www.DynDNS.org and www.NOIP.com	www.DynDns.org
Domain	
The domain applied for to the corresponding dynamic domain service provider.	N/A
User Name	
The name of the user registered at the corresponding dynamic domain service provider.	N/A
Password	
The corresponding password to the registered user.	N/A
Refreshing Interval	
Set the time interval for routers to update its public network IP from the dynamic domain service provider. The value range is 120~86400 sec.	86400

3.3 Firewall

You can set up firewall configurations, including the Firewall Settings, DMZ Settings, Port Forward, Port Trigger, URL Filter, MAC Filter, and IP Filter.

3.3.1 Firewall Settings

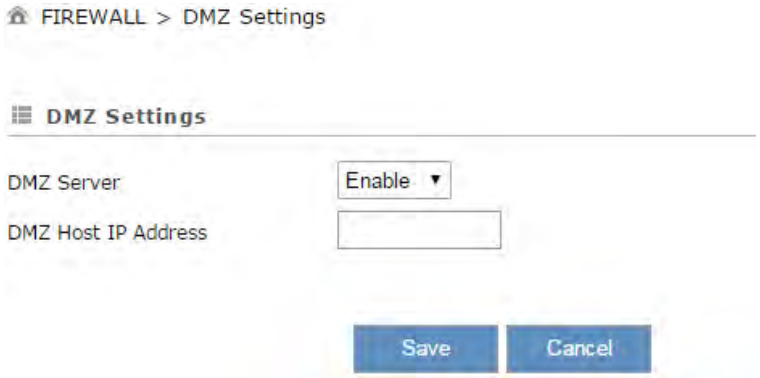
This page is used for setting up the basic firewall settings, including the SPI firewall switch, WAN Ping response, LAN SSH function and WAN SSH.



Description	Default
Firewall	
The SPI Firewall keeps track of the state of network connections travelling across it, protecting your Internet connection against Internet threats and Denial of Service (DoS).	Enable
WAN Ping	
It creates a filter that your router not to respond to Ping command and prevents other users on the internet from pinging your pc and gaining your IP address.	Not responded
LAN SSH	
Choose whether to allow LAN end to connect with the router via SSH.	Enable
WAN SSH	
Choose whether to allow WAN end to connect with the router via SSH.	Disable

3.3.2 DMZ Settings

This page is used for setting up the DMZ server.

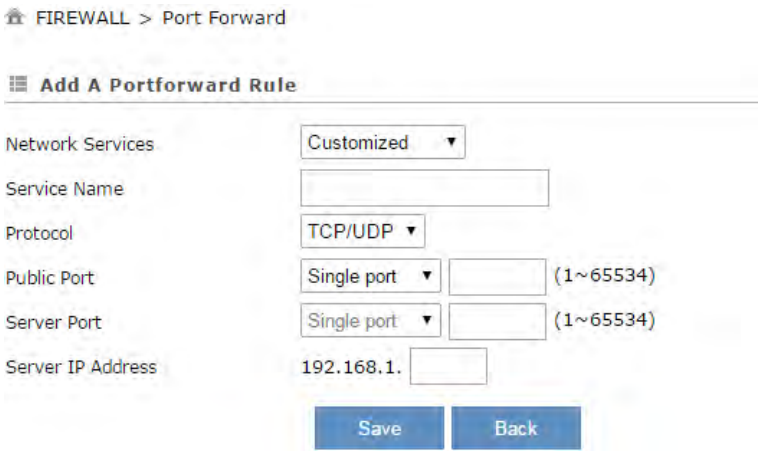


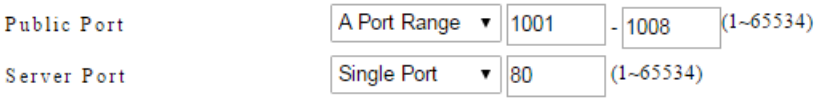
Description	Default
DMZ Server	
Demilitarized zone (DMZ) is a special segment of the local network reserved for servers accessible from the Internet, adding an additional layer of security.	Disable
DMZ Host IP Address	
Enter the IP address for the DMZ host.	N/A

3.3.3 Port Forward

This page is for setting up the port forward, including configuring the Network Services, Service Name, Protocol, Public Port, Server Port, and Server IP Address. Click "Add A Portforward Rule" to add port forwarding entries to the router.

After clicking the "Add A Portforward Rule", you will see the following page.



Description	Default
Network Services	
Select the common network services. Refer to the following common service list for optional values.	Customized
Service Name	
Set up the service name for port forwarding. The name is composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Protocol	
Set the protocol type for port forwarding.	TCP/UDP
Public Port	
Set the public port for port forwarding. The port range is 1~65534. A Public port should be less than or equal to the server port.	Single Port
Server Port	
Set up the server port for port forwarding. The port range is 1~65534. A server port should be greater than or equal to the public port. When the public port is set to a Single Port, the server port can only be set to a Single Port. When the public port is set to a Port Range, the server port can be set to a Single Port or a Port Range. And when the public port is set to a single port, all the port will be forwarded to ONE single port. Examples of different port forwarding settings: 1:1 N:1  N:N 	Single Port
Server IP Address	
Set up the server IP address that applies to the port mapping rule.	192.168.1.*

Common Service List for Port Forwarding			
Service name	**Protocol**	**Starting Port**	**Ending Port**
Customized	TCP, UDP, TCP/UDP	1~65534	1~65534
FTP	TCP	20	21

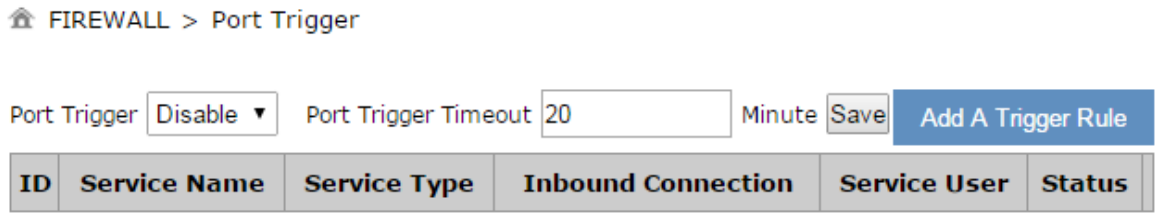
Service name	Protocol	Starting Port	Ending Port
HTTP	TCP	80	80
ICUII	TCP	23566	23566
IP_PHONE	TCP	6670	6670
NetMeeting	TCP	1720	1720
News	TCP	119	119
PPTP	TCP/UDP	1723	1723
Telnet	TCP	23	23
QuakeII/III	TCP/UDP	27960	27960
Real-Audio	TCP	6970	7170

3.3.4 Port Trigger

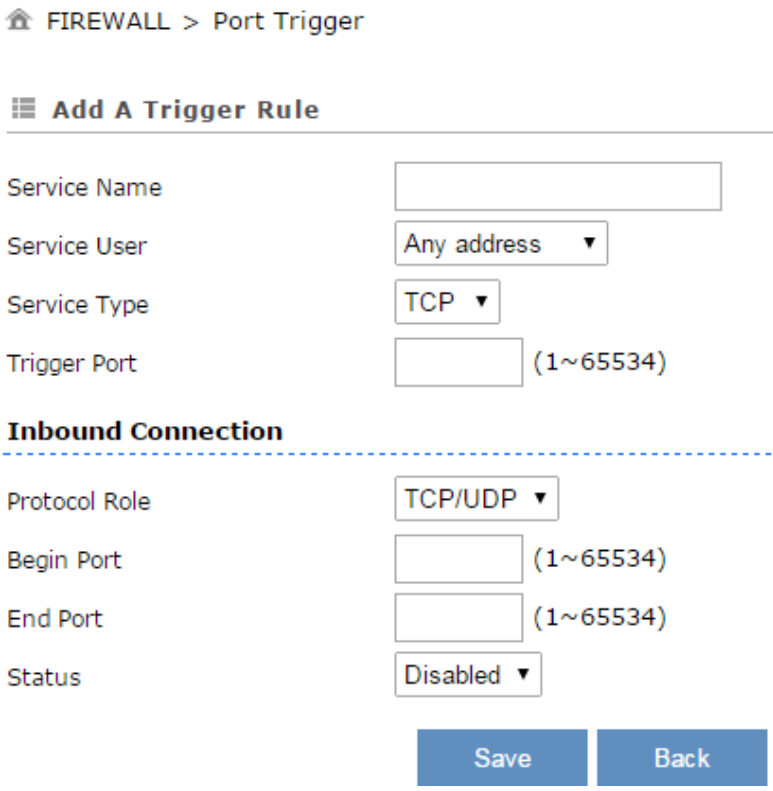
This page is used for setting up the port trigger, including configuring the Service Name, Service User, Service Type, Trigger Port, Protocol Role, Begin Port, End Port, and Status.

Port triggering is port forwarding with an on/off switch for the ports that have been forwarded. Have data flown out of a trigger port or not by enabling or disabling this functionality. Set up the time for the Port Trigger Timeout and click "Save" to save the setting.

Click the "Add ATrigger Rule" to add port trigger entries to the router.



After clicking the "Add A Trigger Rule", you will see the following page.



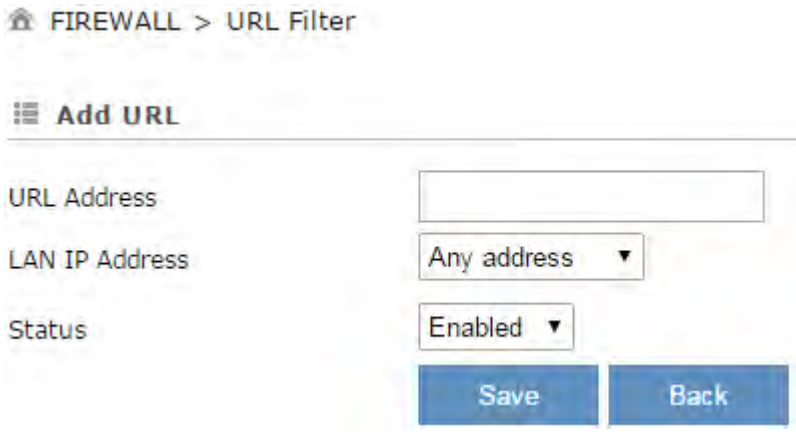
Description	Default
Service Name	
Set the service name for port triggering. The name is composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Service User	
Select the service user to apply the port triggering rule.	Any Address
Service Type	
Set the protocol type for port triggering.	TCP
Triggering Port	
Set the triggering port. The port range is 1~65534.	N/A
Protocol Role	
Set the protocol type for the inbound connection.	TCP/UDP
Begin port	
Set the starting port for the inbound connection. The port range is 1~65534.	N/A
End Port	
Set the ending port for the inbound connection. The port range is 1~65534.	N/A
Status	
Enable/disable the port triggering functionality.	Disabled

3.3.5 URL Filter

This page is used for setting up the URL Filter, including configuring the URL Address, LAN IP Address and Status.

URL Filter is used to block particular website from the local network. Select Enable/Disable to activate/deactivate this functionality. Click the "Add An URL Address" to block the URL.

After clicking the "Add An URL Address", you will see the following page.



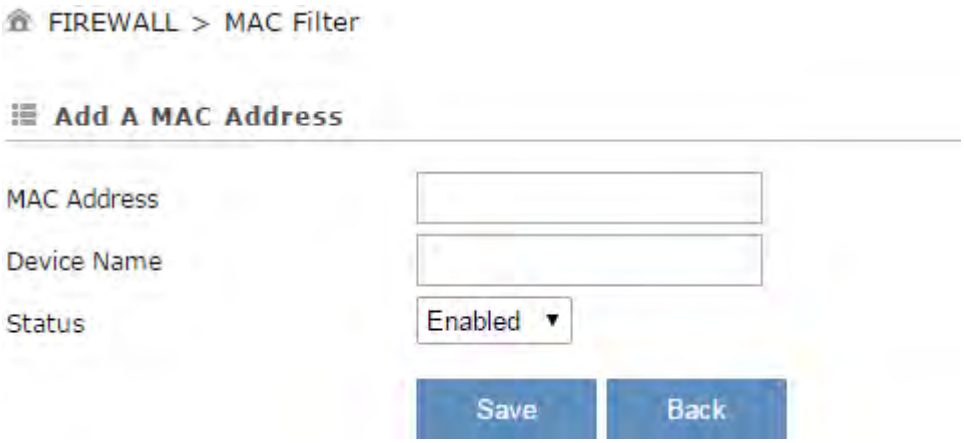
Description	Default
URL Address	
Manually input the URL address that you'd like to block, for example www.baidu.com.	N/A
LAN IP Address	
Enter the LAN IP address that you'd like to block. Options are "Any Address", "Single Address" and "Address Range".	Any Address
Status	
Enable/disable the URL Filter functionality.	Enabled

3.3.6 MAC Filter

This page is used for setting up the MAC Filter, including configuring the MAC Address, Device Name and Status.

MAC Filter is used to block particular MAC address from the local network. Select Enable/Disable to activate/deactivate this functionality. Click the "Add A MAC Address" to block the MAC Address.

After clicking the "Add A MAC Address", you will see the following page.

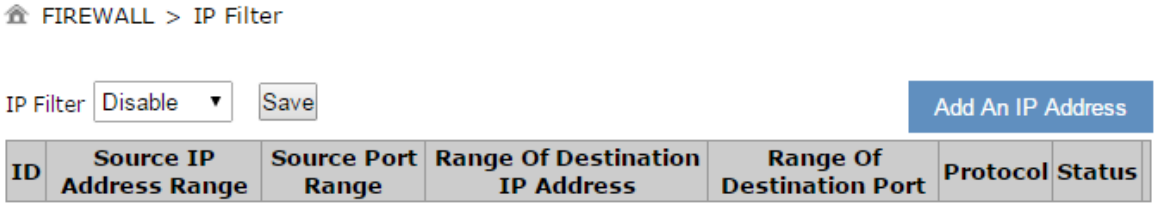


Description	Default
MAC Address	
Manually input the MAC address that you'd like to block.	N/A
Device Name	
Enter the device name corresponding to the set MAC address.	N/A
Status	
Enable/disable the MAC Filter functionality.	Enabled

3.3.7 IP Filter

This page is used for setting up the IP Filter, including configuring the Source IP, Source Port, Destination IP, Destination Port, Protocol and Status.

IP Filter is used to block particular IP address from the local network. Select Enable/Disable to activate/deactivate this functionality. Click the "Add An IP Address" to block the IP Address.



After clicking the "Add An IP Address", you will see the following page.

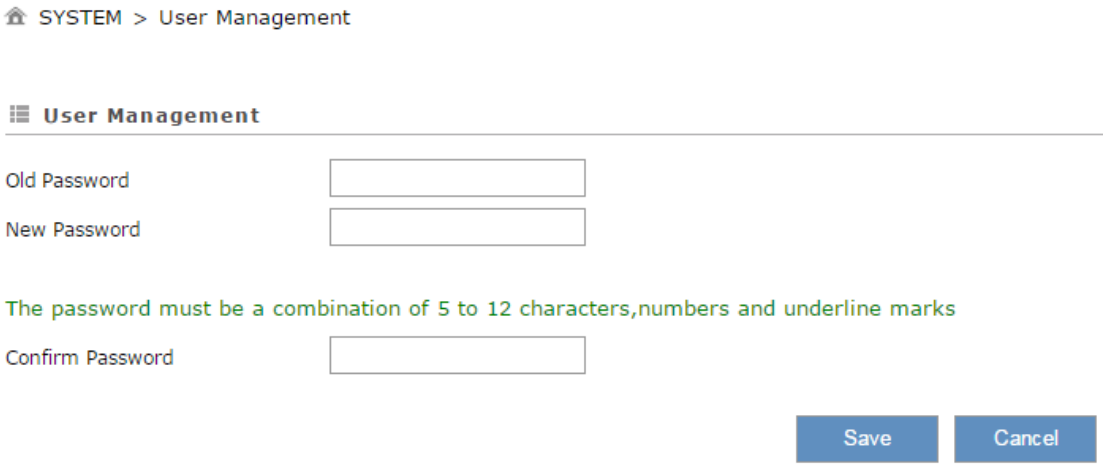
Description	Default
Source IP	
Set the source IP.	Any Address
Source Port	
Set the source port where the datagram came from.	Any port
Destination IP	
Set the destination IP.	Any Address
Destination Port	
Set the destination port where the datagram is going to.	Any port
Protocol	
Set the protocol type for the IP Filter.	TCP/UDP
Status	
Enable/disable the URL Filter functionality.	Enabled

3.4 System

You can set up the system configurations, including the User Management, Time Zone Configurations, RS232, RS485, Modbus TCP, Log Setting, Firmware Upgrade, Backup & Restore, Scheduled Jobs, Network Diagnosis, System Reboot, Event Management, and Register Management.

3.4.1 User Management

You can change the administrator password and set session timeout here. The password must be a combination of 5 to 12 characters, numbers and/or underline symbols.



Description	Default
Old Password	
Input the original password.	admin
New Password	
Input the new password you'd like to use. The password length should be 5-12 digits and is composed of lowercase letters, uppercase letters (case sensitive), numerals 0-9 and underline.	N/A
Confirm Password	
Again input the password you'd like to use to double confirm there is no typo.	N/A
Session Timeout	
Session timeout is an expired time limit for a logged in user which as been inactive for a period of time. Setting range is from 10 to 1440 minutes	30

3.4.2 Time Zone Configurations

You can change the current time of the device. Use the dropdown list to select the correct time zone for your device.

Description	Default
The current time of device	
Here shows the current time of your device.	N/A
Set Local PC Time	
Configure time and date settings of the router to be synchronized with the connected PC.	N/A
Time Zone Setting	
Select the operating time zone of your device: GMT-12:00 - GMT+13:00.	N/A

Instruction	Example: Sync time between routers and the connected PC. 1. Enter DX webpage. 2. Go to “SYSTEM -> Time Zone Settings” 3. Click “Set Local PC Time” 4. After a confirmation message prompted, click yes and reboot the device to complete synchronization.
Figure	

3.4.3 RS232

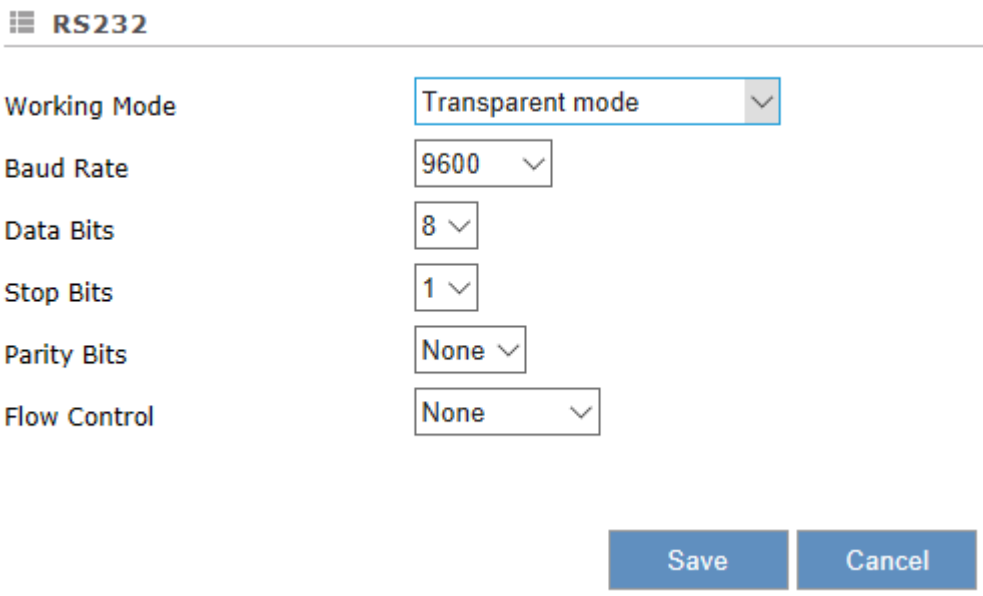
RS-232 supports 7 working modes: Transparent mode, Slave mode, Master mode, Serial Server-TCP Server, Serial Server-TCP Client, Serial Server-UDP Client and MC master mode. This section provides information of specific RS232 port parameters under different working modes. The basic parameters are presented in the table below.

Description	Default
Working Mode	
Select the working mode for the current active serial port.	Close
Baud Rate	
Set the baud rate for the serial port. Options are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.	9600
Data Bits	
Set port data bits as 7 or 8. When operating in Modbus RTU mode, the value can only be set as 8.	8
Stop Bits	
Set the stop bits for the serial port. Options are 1 and 2.	1
Parity Bits	
Set the parity bits for the serial port. Options are None, Odd and Even.	None

Description	Default
Flow Control	
Set the flow control. Options are None, XON, XOFF, RTS, and CTS.	None

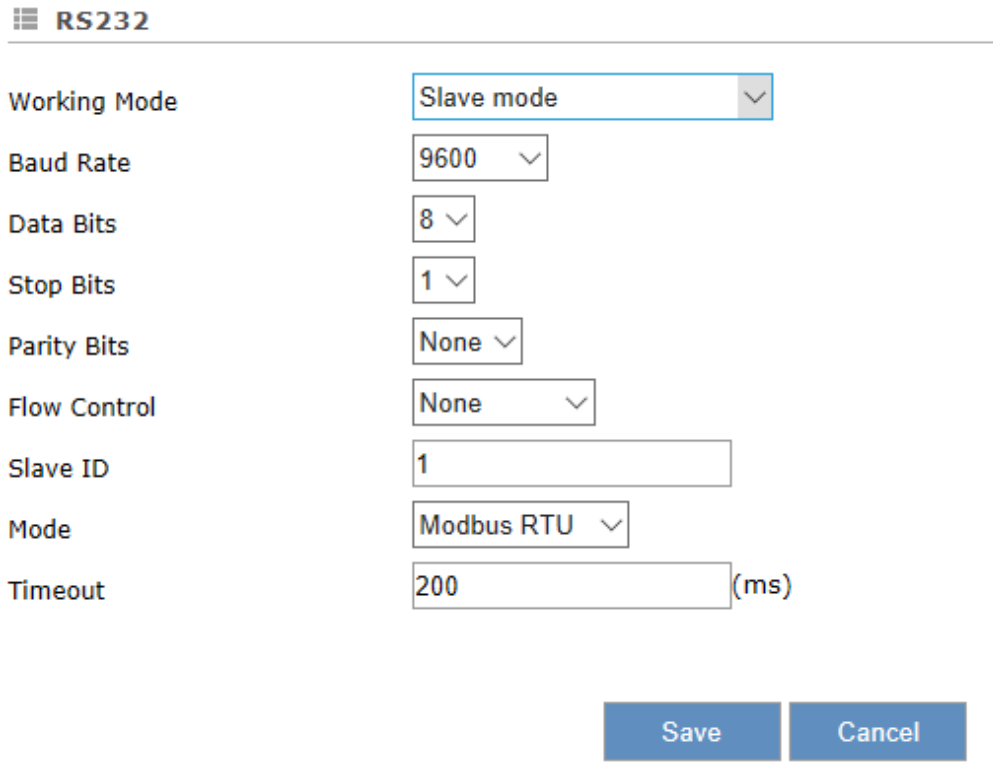
- **Transparent mode**

When RS-232 is under transparent mode, users can debug devices and upload/ download data remotely by creating virtual serial ports via DIACom.



- **Slave mode**

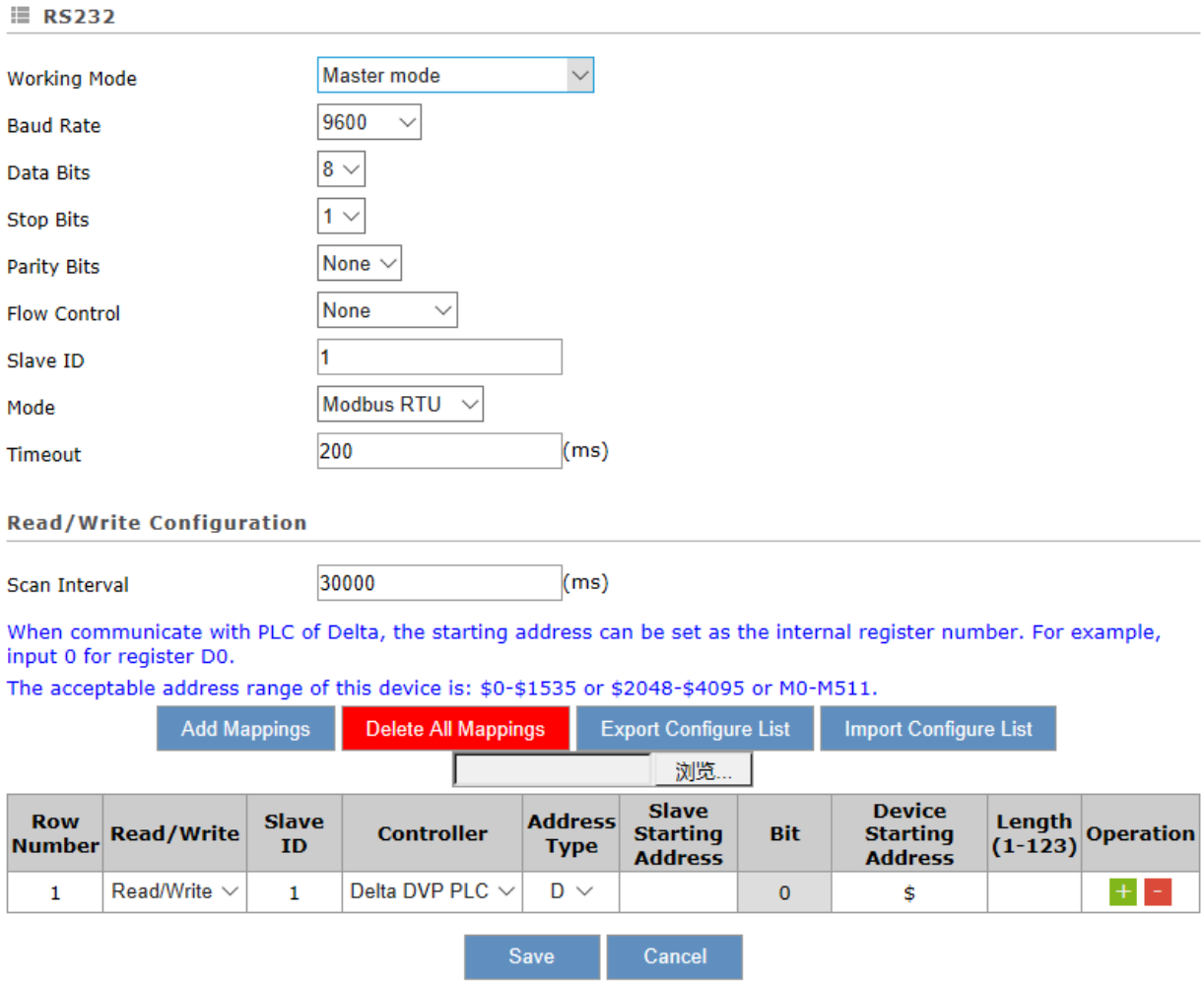
This mode is for the master device to perform the read/ write tasks on the open register of DX-2100RW-WW to achieve bidirectional data transmission.



Description	Default
Slave ID	
Enter the MODBUS ID. The value is between 1 and 247.	1
Mode	
Set the communication mode for the device. Device support Modbus RTU and Modbus ASCII	Modbus RTU
Timeout	
Set the timeout timer from 200ms to 5000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	200ms

- **Master mode**

In this mode, it is allowable for DX router to perform the read/ write tasks on the open register of the slave device to achieve bidirectional data transmission.

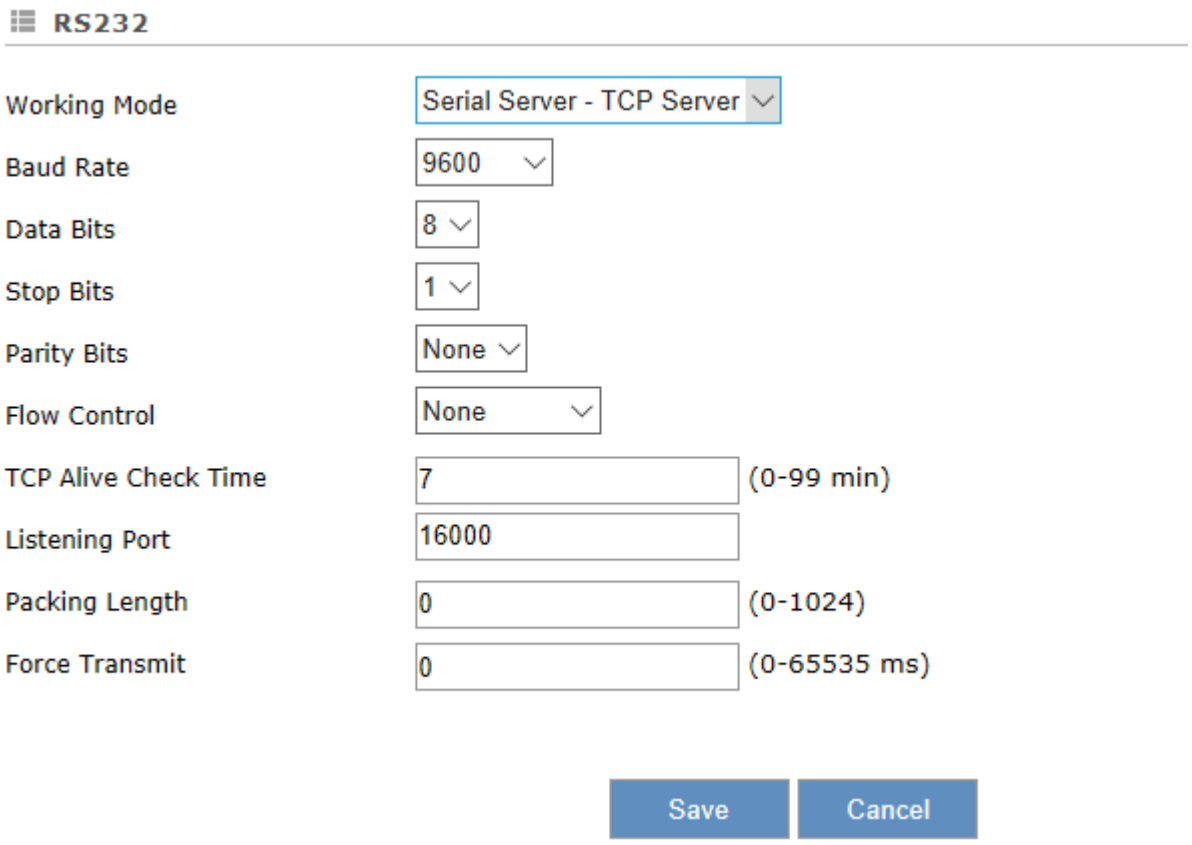


Description	Default
Slave ID	
Set the MODBUS ID for DX router. Invalid in Master mode.	1
Mode	
Set the communication mode for the device. Device support Modbus RTU and Modbus ASCII.	Modbus RTU
Timeout	
Set the timeout timer from 200ms to 5000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	200ms
Scan Interval	
Set the time for scan interval, ranging from 50ms to 60000ms.	30000ms
Add Mappings	
Click the button to add mappings. After creating a mapping between IP addresses of slave device and DX router under the user's configuration, the system will collect data from the slave device.	N/A
Delete All Mappings	
Delete all the existing mapping under the master mode of RS-232.	N/A
Export Configure List	
Export all the mapping and save as a file in the local PC.	N/A
Import Configure List	
This function supports communication interfaces including RS232/RS485/MODBUS TC/MC/SIEMEN TCP, which share a total of 600 mapping web addresses. **Notice:** • Each communication interface can import up to 600 mapping addresses. However, if RS232 has been mapped to 10 addresses and another 600 mapping addresses are imported, the 10 mapping address imported previously will be covered. • If 10 addresses has been mapping to RS232, there would be only 590 addresses left for other communication interfaces to import. A warning message will be displayed if exceeds the limit.	N/A
Read/Write	
Set the access permissions for the mapped register address; • **Read-only:** The device regularly reads data from appointed registers in the slave, but will not update the data to the slave • **Write-only:** The device updates the data to the slave when the registers values were changed, but will not read the data from the slave • **Read/write:** The device regularly reads data from appointed registers in the slave, will update the data to the slave when the registers values are changed.	Read/Write
Slave ID	
Set the corresponding slave communication port. The value is between 1 and 247.	1

Description	Default
Controller	
In master mode, device types options are: • **Delta PLC:** Use this option for Delta DVP / AH / AS series PLCs • **Other:** Use this option for non-Delta PLCs. HEX means hexadecimal address; DEC means decimal address.	Delta DVP PLC
Address Type	
In master mode, the address type would changes with different options of controller type: • **Delta PLC:** address types would be D/M/S/X/Y, which D is a word type and M/S/X/Y are of bit type. • **Other: Address type is** 0x/1x/3x/4x/Swap a) 0x: Coils(Modbus function code: 01/05), read-write. b) 1x: Discrete Inputs(Modbus function code: 02), read only. c) 3x: Input Registers (Modbus function code: 04) , read only. d) 4x: Holding Registers (Modbus function code: 03/16), read-write. e) Swap: If using “double words” to read/write “holding registers”, before reading or writing, the values in Hi Word and Low Word will be swapped first.	D
Slave Starting Address (decimal)	
Set the slave starting address for read/write the registers in a PLC. • **Delta PLC:** Enter the internal D register number. If you need to read / write D0, please enter 0 here. • **Other:** Enter the Hexadecimal or Decimal actual address. For example: Holding Register: 400100, take 0100 (decimal) that is 64 (hex).	N/A
Bit	
For the X/Y type of Delta AH/AS series, the address input format is 0.0~X.15. Enter the values before decimal point in the input field of Slave Starting Address, while values after decimal point should be entered in the input field of Bit.	N/A
Device Starting Address (decimal)	
Set up the device starting address (decimal, input range is from $2048 to $4095). Must start at the beginning of a Device Starting Address with a “$” or “M”.	N/A
Length (1-123)	
Set the number of continuous addresses followed by the starting address which will be read or write, ranging from 1 to 123.	N/A
Operation	
Click the +/- button to add mapping or delete mapping.	N/A
Edit	
Click an item of register mapping forms that can be edited.	N/A

- **Serial Server-TCP Server**

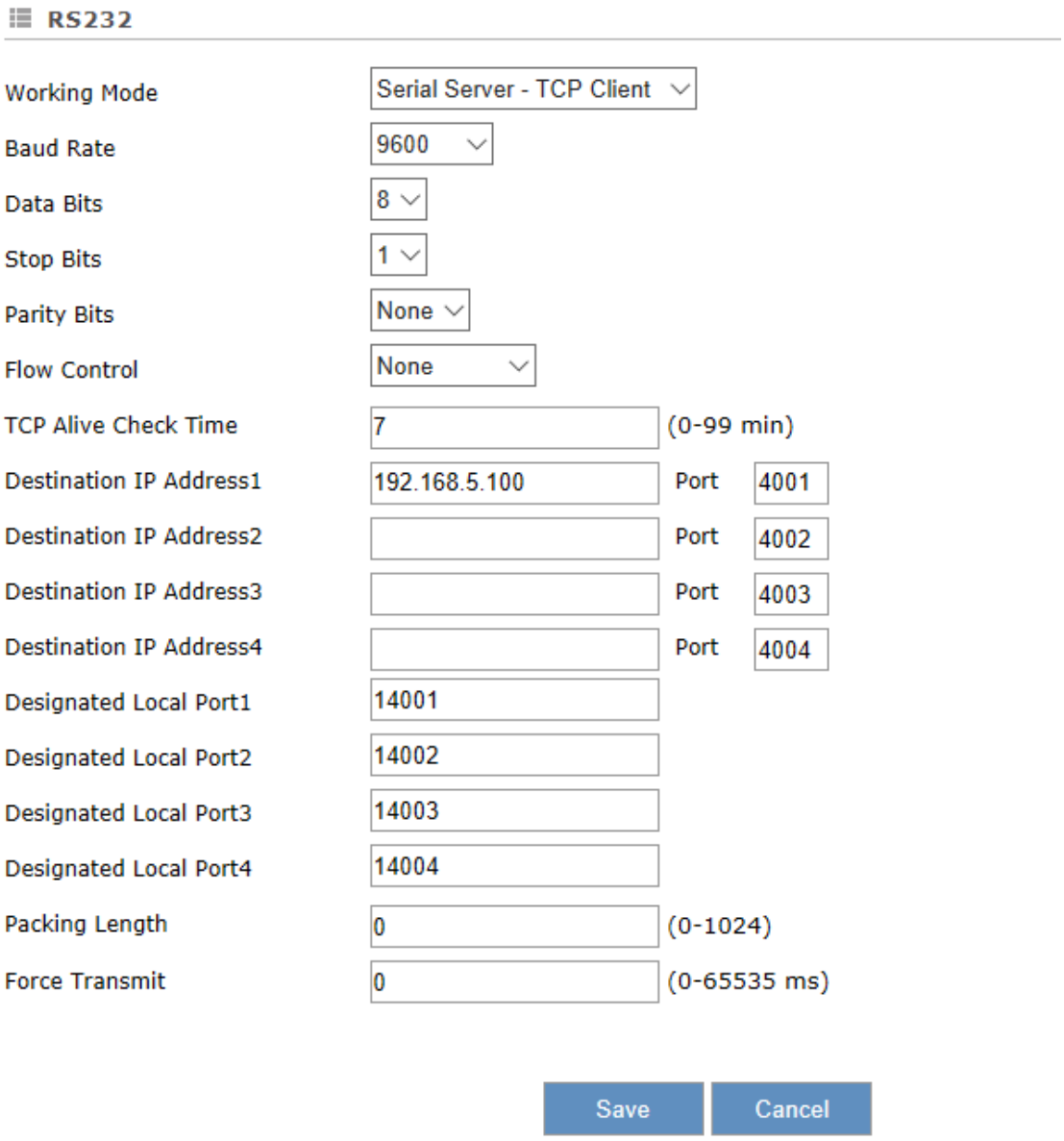
In this working mode, DX series routers working as TCP servers receive data packets from clients, then send to RS-232 after parsing.



Description	Default
TCP Alive Check Time	
Configure the duration of the idle state before disconnect TCP automatically. Selectable values: 0~99 -0：Never shut off TCP connection due to idle state. -1~99：Shut off when reaches the setting value.	7
Listening Port	
Configure the listening port of the server.	16000
Packing Length	
Configure the length of the accumulated data for packets sending, ranging 0~1024 bytes. Set as 0 for real-time data transmission.	0
Force Transmit	
Configure the length of time awaiting to transmit a data packet, ranging 1~65535. When reaches the setting of time duration or the length of accumulated data, the data would be transmitted immediately. If set as 0, no data packet would be sent.	0

- **Serial Server-TCP Client**

Under this mode, DX routers will be clients of device servers to send data with a TCP connection.

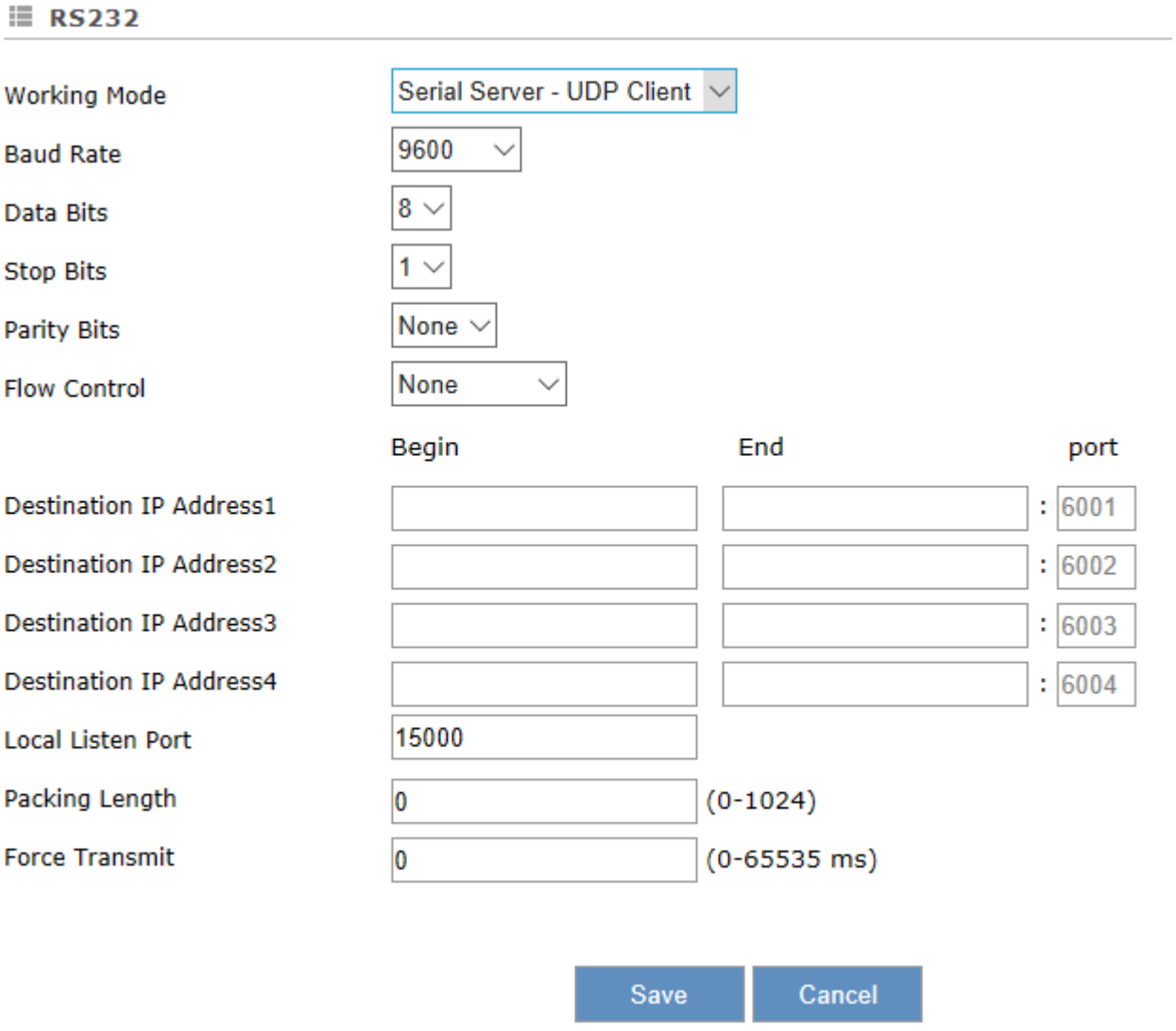


Description	Default
TCP Alive Check Time	
Configure the duration of the idle state before disconnect TCP automatically. Selectable values: 0~99 -0：Never shut off TCP connection due to idle state. -1~99：Shut off when reaches the setting value.	7
Destination IP address and Port	
Set up destination IP addresses and ports. (Default:4001~4004, configurable) IP addresses and ports cannot be duplicated with a maximum of 4 servers allowed to be connected at the same time.	N/A

Description	Default
Designated local port	
Set local ports for your device.	14001~14004
Packing Length	
Configure the length of the accumulated data for packets sending, ranging 0~1024 bytes. Set as 0 for real-time data transmission.	0
Force Transmit	
Configure the length of time awaiting to transmit a data packet forcibly, ranging 0~65535ms. When reaches the setting of time duration or the length of accumulated data, the data would be transmitted immediately. If set as 0, no data packet would be sent.	0

- **Serial Server-UDP Client**

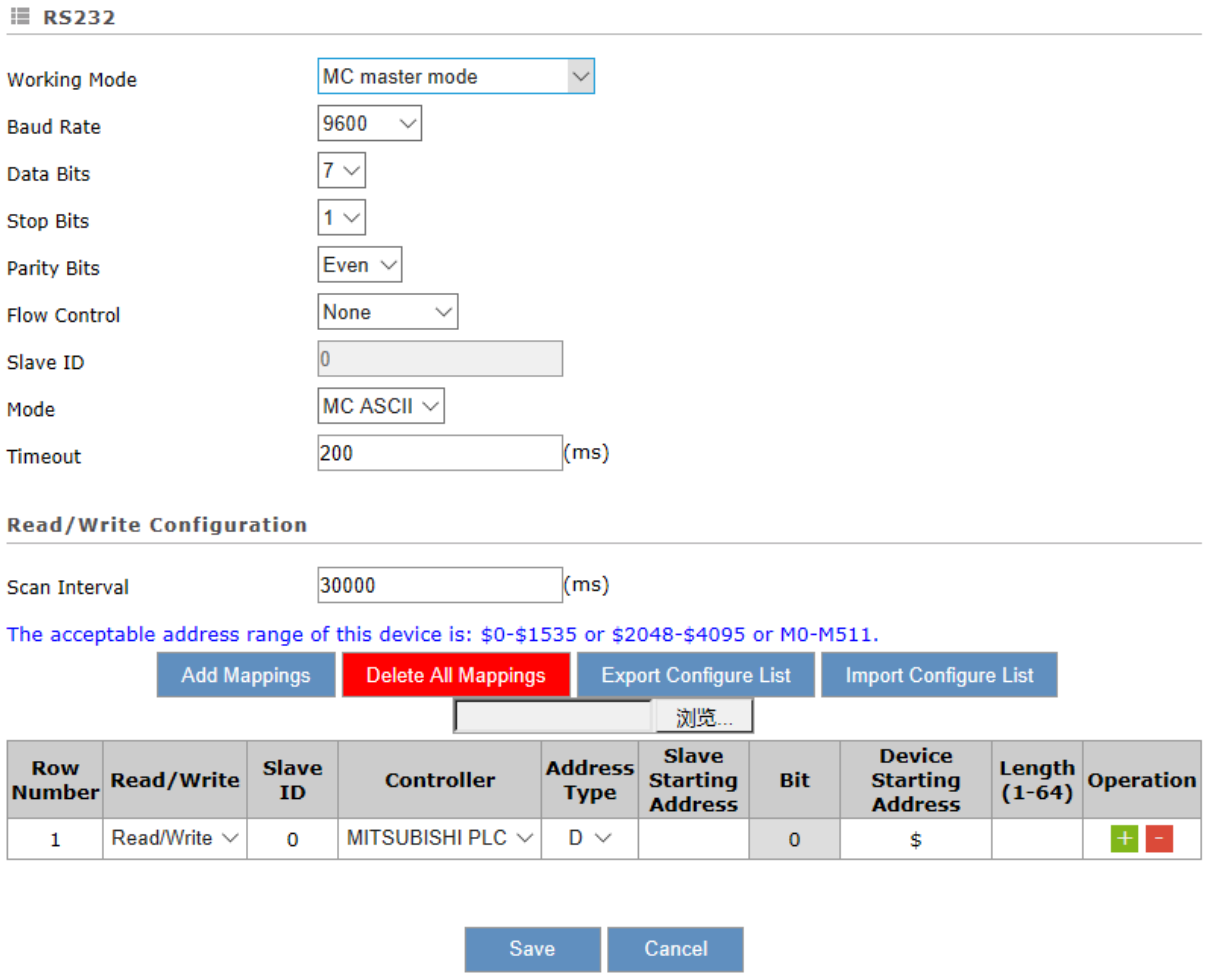
Under this mode, DX routers will be clients of device servers to send data with a UDP connection.



Description	Default
Destination IP address and Port	
Set the destination IP addresses and ports. (Default:6001~6004, configurable) IP addresses and ports cannot be duplicated with a maximum of 4 servers allowed to be connected at the same time. Each server can support up to 99 addresses, counting from the starting address.	Default port 6001~6004
Local listen port	
Set the local listen port for your device.	15000
Packing Length	
Set the length of the accumulated data for packets sending, ranging 0~1024 bytes. Set as 0 for real-time data transmission.	0
Force Transmit	
Set the length of time awaiting to transmit a data packet forcibly, ranging 0~65535ms. When reaches the setting of time duration or the length of accumulated data, the data would be transmitted immediately. If set as 0, no data packet would be sent.	0

- **MC master mode**

When RS232 is in MC master mode, DX series routers can perform the read/ write tasks on the slave device of Mitsubishi PLC FX series via RS232 to achieve bidirectional data transmission.



Description	Default
Slave ID	
Set the MODBUS ID for DX router. Invalid in MC Master mode.	0
Mode	
It's fixed to "MC ASCII" in MC master mode.	MC ASCII
Timeout	
Set the timeout timer from 200ms to 5000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	200ms
Scan Interval	
Set the time for scan interval, ranging from 50ms to 60000ms.	30000ms
Add Mappings	
Click the button to add mappings. After creating a mapping between IP addresses of slave device and DX router under the user's configuration, the system will collect data from the slave device.	N/A
Delete All Mappings	
Delete all the existing mapping under the master mode of RS-232.	N/A
Export Configure List	
Export all the mapping and save as a file in the local PC.	N/A
Import Configure List	
This function supports communication interfaces including RS232/RS485/MODBUS TC/MC/SIEMEN TCP, which share a total of 600 mapping web addresses. **Notice:** • Each communication interface can import up to 600 mapping addresses. However, if RS232 has been mapped to 10 addresses and another 600 mapping addresses are imported, the 10 mapping address imported previously will be covered. • If 10 addresses has been mapping to RS232, there would be only 590 addresses left for other communication interfaces to import. A warning message will be displayed if exceeds the limit.	N/A
Read/Write	
Set the access permissions for the mapped register address; • **Read-only:** The device regularly reads data from appointed registers in the slave, but will not update the data to the slave • **Write-only:** The device updates the data to the slave when the registers values were changed, but will not read the data from the slave • **Read/write:** The device regularly reads data from appointed registers in the slave, will update the data to the slave when the registers values are changed.	Read/Write
Slave ID	
It's fixed to 0 in MC master mode.	0

Description	Default
Controller	
It's fixed to "MITSUBISHI PLC" in MC master mode.	MITSUBISHI PLC
Address Type	
Address types would be D/M/S/X/Y, which D is a word type and M/S/X/Y are bit types.	D
Slave Starting Address (decimal)	
Set the slave starting address for read/write the registers in MITSUBISHI PLC.	N/A
Bit	
Invalid under MC master mode.	
Device Starting Address (decimal)	
Set up the device starting address (decimal, input range is from $2048 to $4095). Must start at the beginning of a Device Starting Address with a "$" or "M".	N/A
Length	
Set the length, which is the number of the continuous address followed by the starting address, ranging from 1 to 64.	N/A
Operation	
Click the +/- button to add mapping or delete mapping.	N/A
Edit	
Click an item of register mapping forms that can be edited.	N/A

3.4.4 RS485

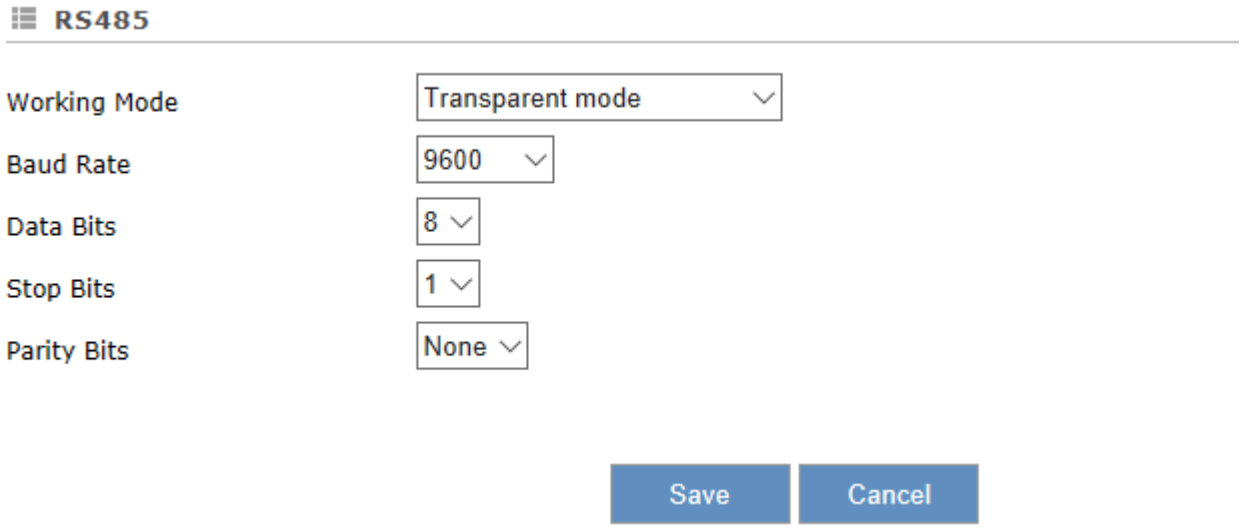
RS-485 supports 6 working modes: Transparent mode, Slave mode, Master mode, Serial Server-TCP Server, Serial Server-TCP Client and Serial Server-UDP Client. This section provides information of specific RS-485 port parameters under different working modes. The basic parameters are presented in the table below.

Description	Default
Working Mode	
Select the working mode for the current active serial port.	Close
Baud Rate	
Set the baud rate for the serial port. Options are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.	9600
Data Bits	
Set port data bits as 7 or 8. When operating in Modbus RTU mode, the value can only be set as 8.	8
Stop Bits	
Set up the stop bits for the serial port. Options are 1 and 2.	1
Parity Bits	

Description	Default
Set the parity bits for the serial port. Options are None, Odd and Even.	None

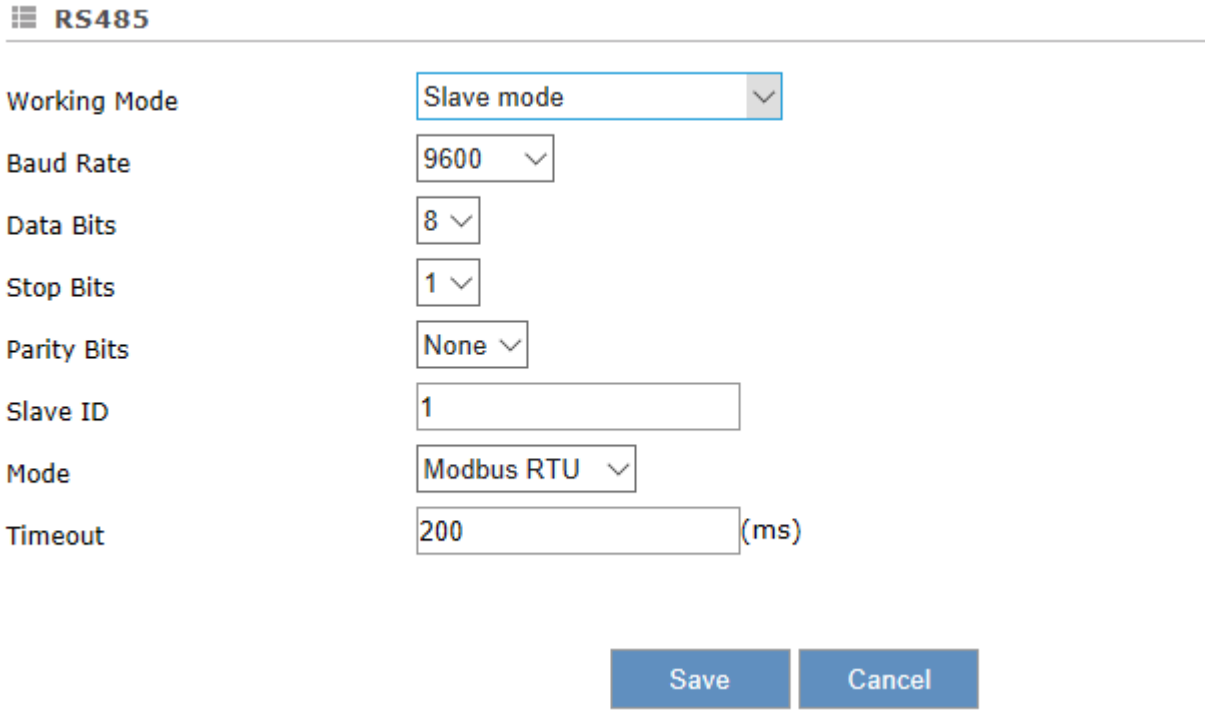
- **Transparent mode**

When RS-485 is under transparent mode, users can debug devices and upload/ download data remotely by creating virtual serial ports via DIACom.



- **Slave mode**

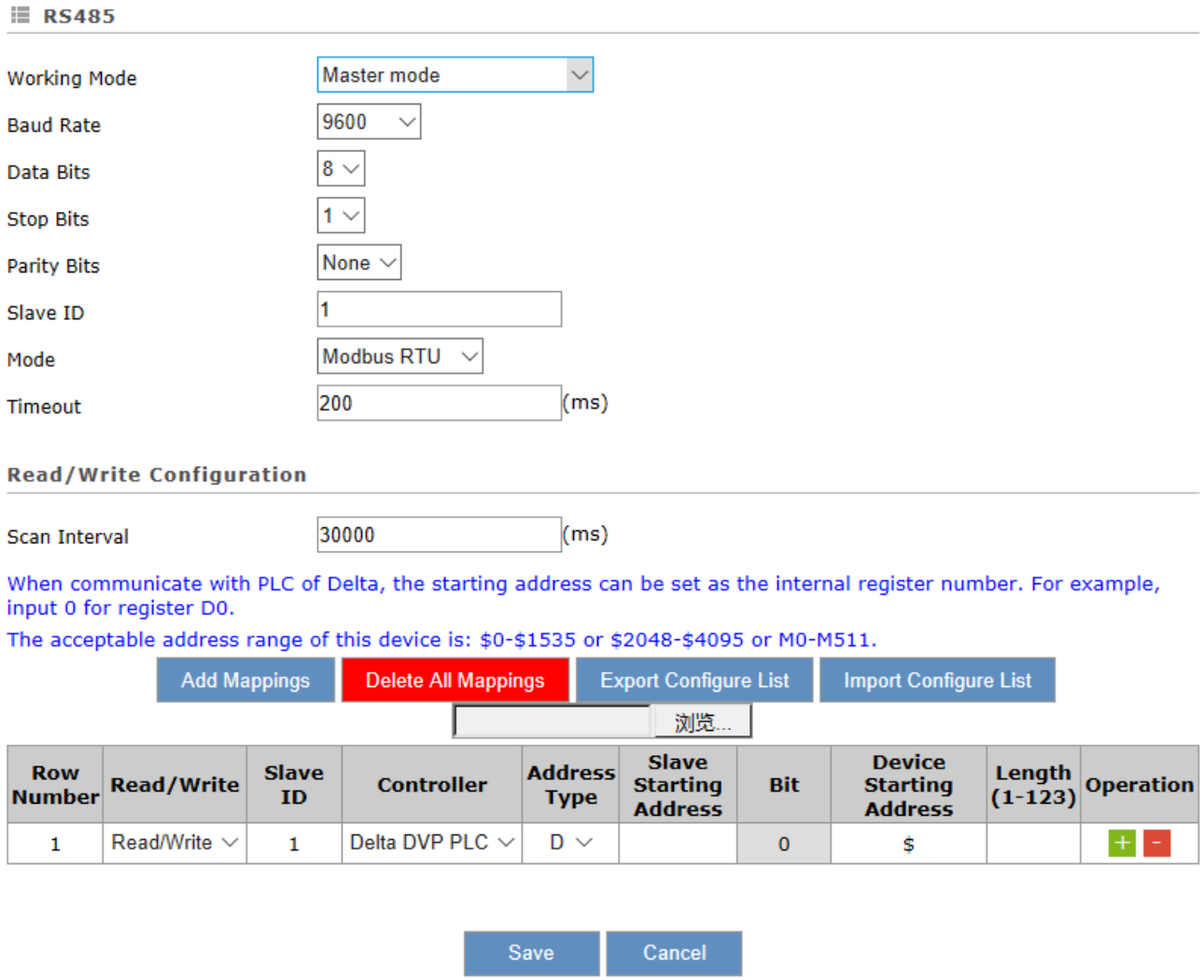
This mode is for the master device to perform the read/ write tasks on the open register of DX routers to achieve bidirectional data transmission.



Description	Default
Slave ID	
Set the MODBUS ID. The value is between 1 and 247.	1
Mode	
Set the communication mode for the device. Device support Modbus RTU and Modbus ASCII	Modbus RTU
Timeout	
Set the timeout timer from 200ms to 5000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	200ms

- **Master mode**

In this mode, it is allowable for DX router to perform the read/ write tasks on the slave device via an RS-485 connection to achieve bidirectional data transmission.

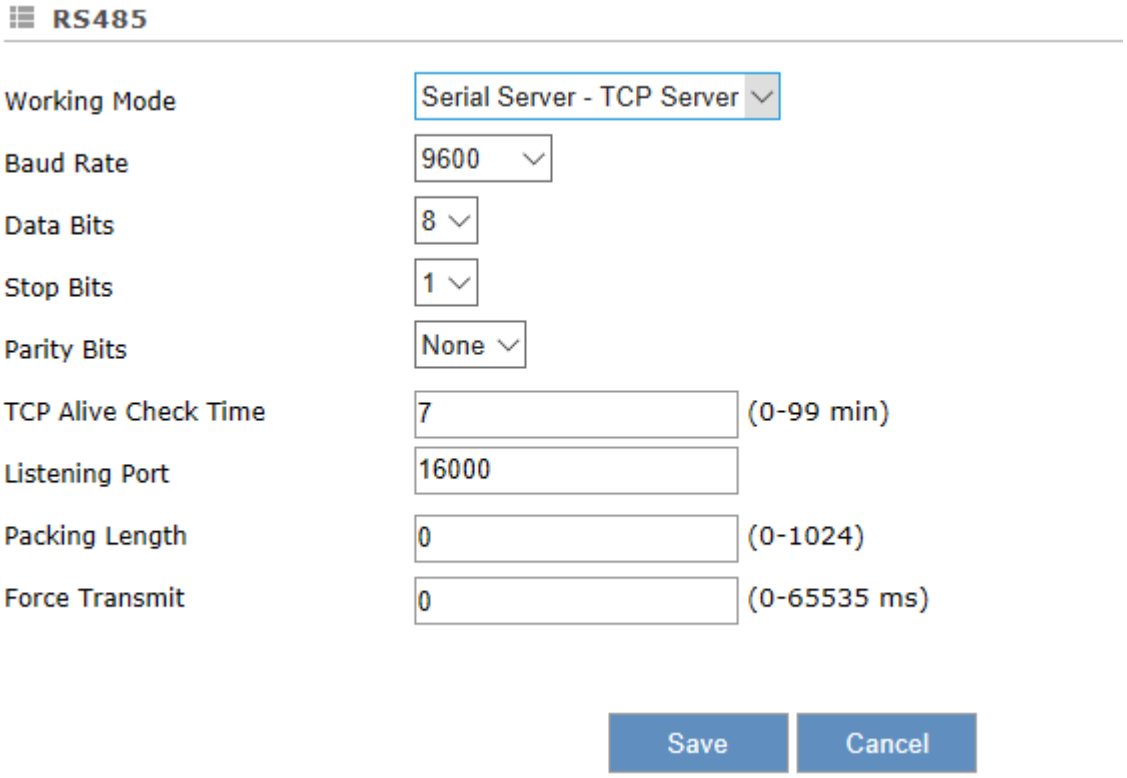


Description	Default
Slave ID	
Set the MODBUS ID for DX router. Invalid in Master mode.	1
Mode	
Set the communication mode for the device. Device support Modbus RTU and Modbus ASCII.	Modbus RTU
Timeout	
Set the timeout timer from 200ms to 5000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	200ms
Scan Interval	
Set the time for scan interval, ranging from 50ms to 60000ms.	30000ms
Add Mappings	
Click the button to add mappings. After creating a mapping between IP addresses of slave device and DX router under the user's configuration, the system will collect data from the slave device.	N/A
Delete All Mappings	
Delete all the existing mapping under the master mode of RS-485.	N/A
Export Configure List	
Export all the mapping and save as a file in the local PC.	N/A
Import Configure List	
This function supports communication interfaces including RS232/RS485/MODBUS TC/MC/SIEMEN TCP, which share a total of 600 mapping web addresses. **Notice:** • Each communication interface can import up to 600 mapping addresses. However, if RS485 has been mapped to 10 addresses and another 600 mapping addresses are imported, the 10 mapping address imported previously will be covered. If 10 addresses has been mapping to RS485, there would be only 590 addresses left for other communication interfaces to import. A warning message will be displayed if exceeds the limit.	N/A
Read/Write	
Set the access permissions for the mapped register address; • **Read-only:** The device regularly reads data from appointed registers in the slave, but will not update the data to the slave • **Write-only:** The device updates the data to the slave when the registers values were changed, but will not read the data from the slave • **Read/write:** The device regularly reads data from appointed registers in the slave, will update the data to the slave when the registers values are changed.	Read/Write
Slave ID	
Set the corresponding slave communication port. The value is between 1 and 247.	1

Description	Default
Controller	
In master mode, device types options are: • **Delta PLC:** Use this option for Delta DVP / AH / AS series PLCs • **Other:** Use this option for non-Delta PLCs. HEX means hexadecimal address; DEC means decimal address.	Delta DVP PLC
Address Type	
In master mode, the address type would changes with different options of controller type.: • **Delta PLC:** address types would be D/M/S/X/Y, which D is a word type and M/S/X/Y are of bit type. • **Other: Address type is** 0x/1x/3x/4x/Swap a) 0x: Coils(Modbus function code: 01/05), read-write. b) 1x: Discrete Inputs(Modbus function code: 02), read only. c) 3x: Input Registers (Modbus function code: 04) , read only. d) 4x: Holding Registers (Modbus function code: 03/16), read-write. Swap: If using “double words” to read/write “holding registers”, before reading or writing, the values in Hi Word and Low Word will be swapped first.	D
Slave Starting Address (decimal)	
Set the slave starting address for read/write the registers in a PLC. • **Delta PLC:** Enter the internal D register number. If you need to read / write D0, please enter 0 here. • **Other:** Enter the Hexadecimal or Decimal actual address. For example: Holding Register: 400100, take 0100 (decimal) that is 64 (hex).	N/A
Bit	
For the X/Y type of Delta AH/AS series, the address input format is 0.0~X.15. Enter the values before decimal point in the input field of Slave Starting Address, while values after decimal point should be entered in the input field of Bit.	
Device Starting Address (decimal)	
Set up the device starting address (decimal, input range is from $2048 to $4095). Bit type range is M0~M511. The beginning of a Device Starting Address must starts with a “$” or “M”.	N/A
Length (1-123)	
Set the number of the continuous address followed by the starting address which will be read or write, ranging from 1 to 123.	N/A
Operation	
Click the +/- button to add mapping or delete mapping.	N/A
Edit	
Click an item of register mapping forms that can be edited.	N/A

- **Serial Server-TCP Server**

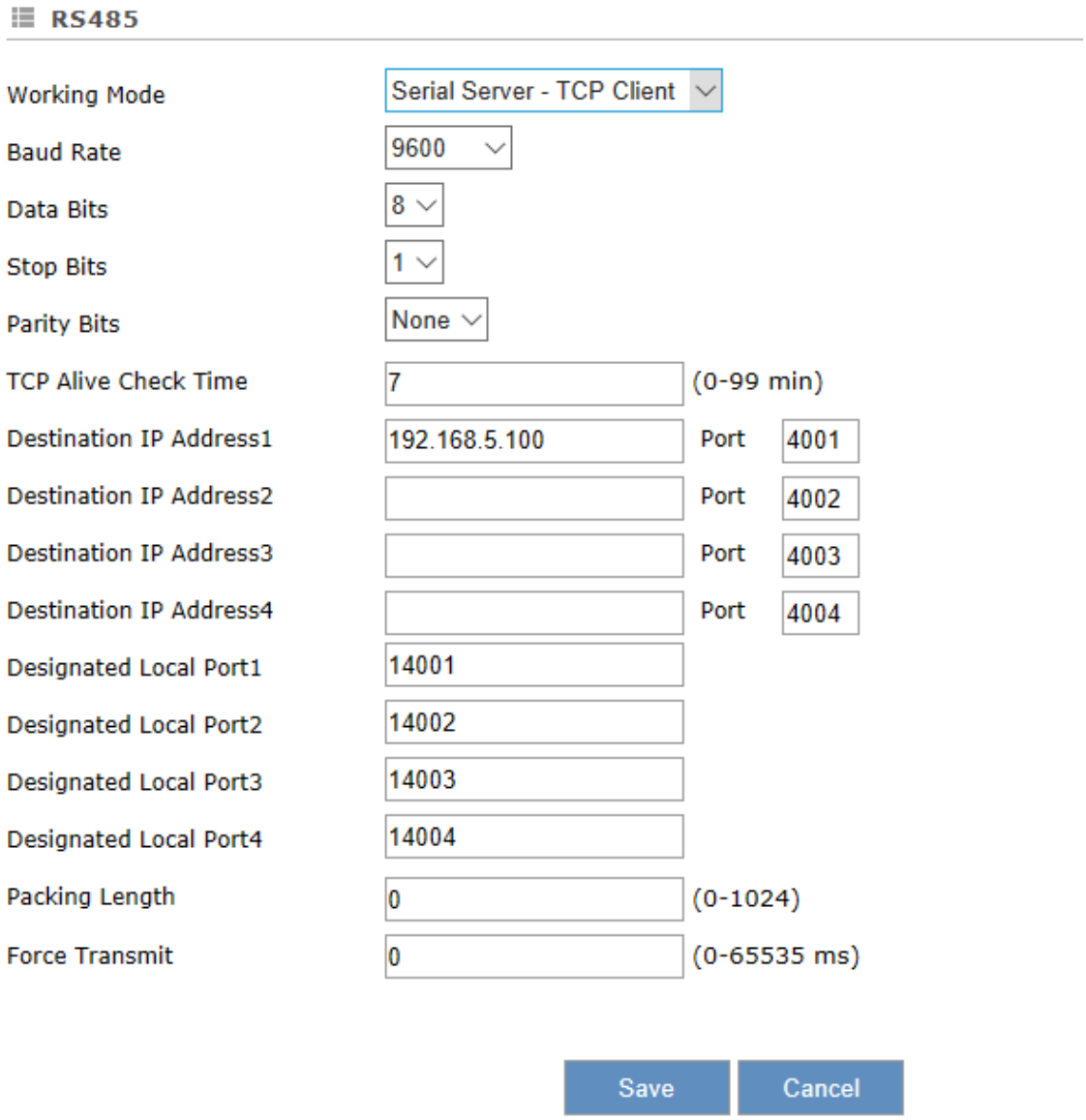
In this working mode, DX series routers working as TCP servers receive data packets from clients, then send to RS-485 after parsing.



Description	Default
TCP Alive Check Time	
Configure the duration of the idle state before disconnect TCP automatically. Selectable values: 0~99 -0：Never shut off TCP connection due to idle state. -1~99：Disconnect TCP once the duration reaches the setting value.	7
Listening Port	
Set the listening port of the server.	16000
Packing Length	
Set the length of the accumulated data for packets sending, ranging 0~1024 bytes. Set as 0 for real-time data transmission.	0
Force Transmit	
Set the length of time awaiting to transmit a data packet, ranging 0~65535 ms. When reaches the setting of time duration or the length of accumulated data, the data would be transmitted immediately. If set as 0, no data packet would be sent.	0

- **Serial Server-TCP Client**

Under this mode, DX routers will be clients of device servers to send data with a TCP connection.

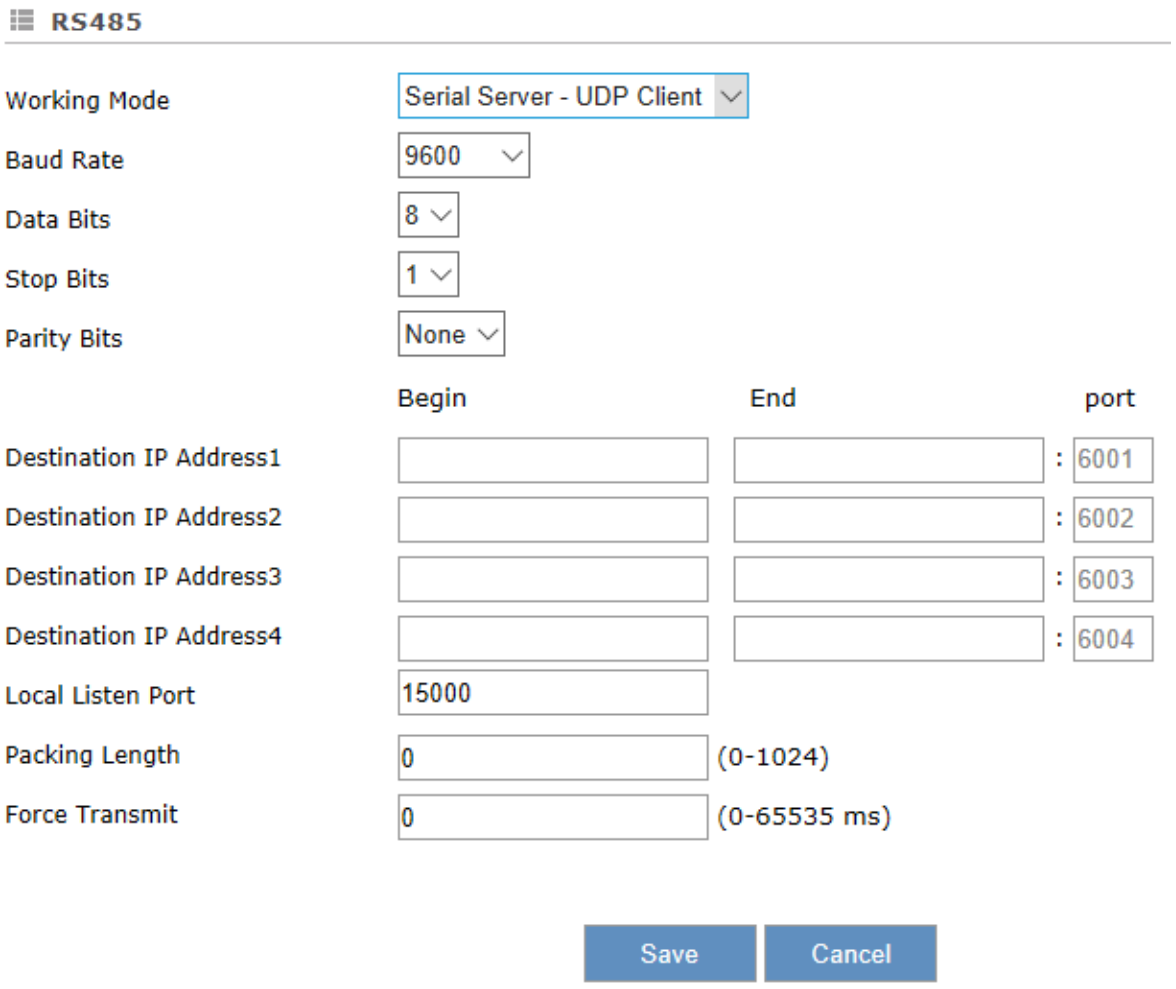


Description	Default
TCP Alive Check Time	
Configure the duration of the idle state before disconnect TCP automatically. Selectable values: 0~99 -0：Never shut off TCP connection due to idle state. -1~99：Disconnect TCP once the duration reaches the setting value.	7
Destination IP address and Port	
Set the destination IP addresses and ports. (Default:4001~4004, configurable) IP addresses and ports cannot be duplicated with a maximum of 4 servers allowed to be connected at the same time.	4001~4004

Description	Default
Designated local port	
Set local ports for your device.	14001~14004
Packing Length	
Set the length of the accumulated data for packets sending, ranging 0~1024 bytes. Set as 0 for real-time data transmission.	0
Force Transmit	
Set the length of time awaiting to transmit a data packet, ranging 0~65535 ms. When reaches the setting of time duration or the length of accumulated data, the data would be transmitted immediately. If set as 0, no data packet would be sent.	0

- **Serial Server-UDP Client**

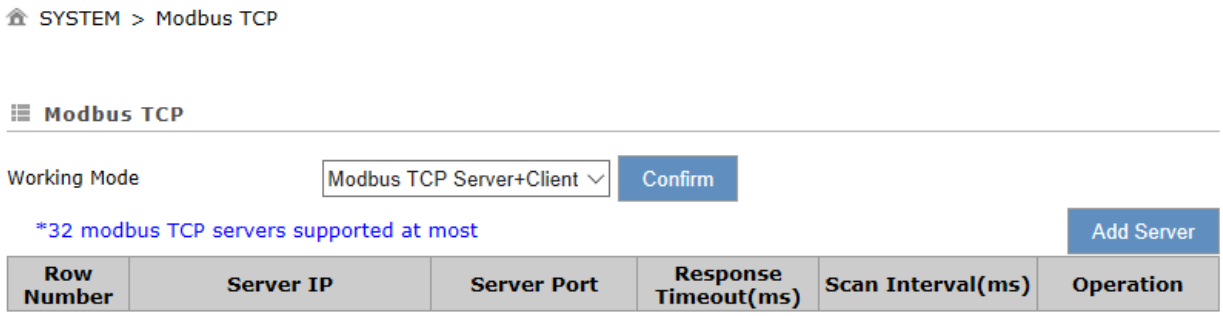
Under this mode, DX routers will be clients of device servers to send data with a UDP connection.



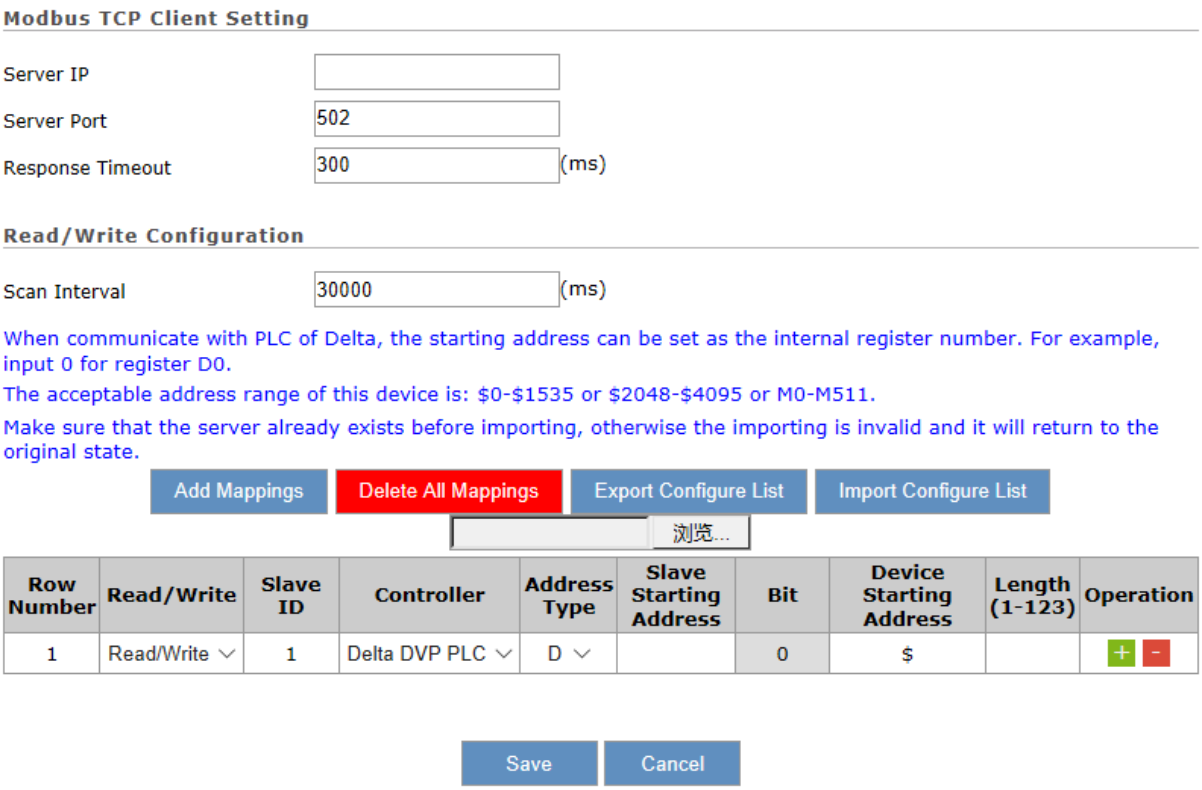
Description	Default
Destination IP address and Port	
Set the destination IP addresses and ports. (Default:6001~6004, configurable) IP addresses and ports cannot be duplicated with a maximum of 4 servers allowed to be connected at the same time. Each server can support up to 99 addresses, counting from the starting address.	6001~6004
Local listen port	
Set the local listen port for your device.	15000
Packing Length	
Set the length of the accumulated data for packets sending, ranging 0~1024 bytes. Set as 0 for real-time data transmission.	0
Force Transmit	
Set the length of time awaiting to transmit a data packet, ranging 0~65535 ms. When reaches the setting of time duration or the length of accumulated data, the data would be transmitted immediately. If set as 0, no data packet would be sent.	0

3.4.5 Modbus TCP

This page allows users to set whether to enable Modbus TCP client mode and set relevant parameters.



Click "Add Server", the below page will be displayed.



Description	Default
Working Mode	
• **Modbus TCP Server:** Only Modbus TCP server works. And supports up to 32 Client to connect. • **Modbus TCP Server+Client:** Modbus TCP server + Modbus TCP client work at the same time. MODBUS TCP Client supports to connect to 32 different servers at most.	Modbus TCP Server
Server IP	
Set up the IP address of a PLC in the Modbus TCP Client mode	N/A
Server Port	
Set up the server port of a PLC in the Modbus TCP Client mode	502
Response Timeout	
Set up the timeout timer from 50ms to 10000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value. The default is 300ms.	300
Scan Interval	
Set up the time for scan interval, ranging from 50ms to 60000ms; the default is 3000ms.	30000
Add Mappings	
Click the button to add mappings. After creating a mapping between IP addresses of slave device and DX router under the user's configuration, the system will collect data from the slave device.	N/A
Delete All Mappings	
Delete all the existing mapping under the Modbus TCP mode.	N/A

Description	Default
Export Configure List	
Export all the mapping and save as a file in the local PC.	N/A
Import Configure List	
This function supports communication interfaces including RS232/RS485/MODBUS TC/MC/SIEMEN TCP, which share a total of 600 mapping web addresses. **Notice:** • Each communication interface can import up to 600 mapping addresses. However, if RS232 has been mapped to 10 addresses and another 600 mapping addresses are imported, the 10 mapping address imported previously will be covered. • If 10 addresses has been mapping to RS232, there would be only 590 addresses left for other communication interfaces to import. A warning message will be displayed if exceeds the limit.	N/A
Read/Write	
Set up the access permissions for the mapped register address; • **Read-only:** The device regularly reads data from appointed registers in the slave, but will not update the data to the slave • **Write-only:** The device updates the data to the slave when the registers values were changed, but will not read the data from the slave • **Read/write:** The device regularly reads data from appointed registers in the slave, will update the data to the slave when the registers values are changed.	Read/Write
Slave ID	
Set up the corresponding slave communication port. The value is between 1 and 247.	1
Controller	
In master mode, device types options are: • **Delta PLC:** Use this option for Delta DVP / AH / AS series PLCs • **Other:** Use this option for non-Delta PLCs. HEX means hexadecimal address; DEC means decimal address.	Delta DVP PLC
Address Type	
In master mode, the address type would changes with different options of controller type.: • **Delta PLC:** address types would be D/M/S/X/Y, which D is a word type and M/S/X/Y are of bit type. • **Other: Address type is** 0x/1x/3x/4x/Swap a) 0x: Coils(Modbus function code: 01/05), read-write. b) 1x: Discrete Inputs(Modbus function code: 02), read only. c) 3x: Input Registers (Modbus function code: 04) , read only. d) 4x: Holding Registers (Modbus function code: 03/16), read-write. e) Swap: If using “double words” to read/write “holding registers”, before reading or writing, the values in Hi Word and Low Word will be swapped first.	D

Description	Default
Slave Starting Address (decimal)	
Set up the slave starting address for read/write the registers in a PLC. • **Delta PLC:** Enter the internal D register number. If you need to read / write D0, please enter 0 here. • **Other:** Enter the Hexadecimal or Decimal actual address. For example: Holding Register: 400100, take 0100 (decimal) that is 64 (hex).	N/A
Bit	
For the X/Y type of Delta AH/AS series, the address input format is 0.0~X.15. Enter the values before decimal point in the input field of Slave Starting Address, while values after decimal point should be entered in the input field of Bit.	
Device Starting Address (decimal)	
Set up the device starting address (decimal, input range is from $2048 to $4095 for word type data, input range is from M0 to M511 for bit type data). $ or M specifies that the match must start at the beginning of a Device Starting Address.	N/A
Length (1-123)	
Set the number of the continuous address followed by the starting address which will be read or write. Input range is from 1 to 123.	N/A
Operation	
Click the +/- button to add mapping or delete mapping.	N/A
Edit	
Click an item of register mapping forms that can be edited.	N/A

3.4.6 Siemens TCP

Support Siemens TCP Client mode to perform data exchange with Siemens S7-300/S7-1200/S7-1500 through Ethernet.

SYSTEM > Siemens TCP

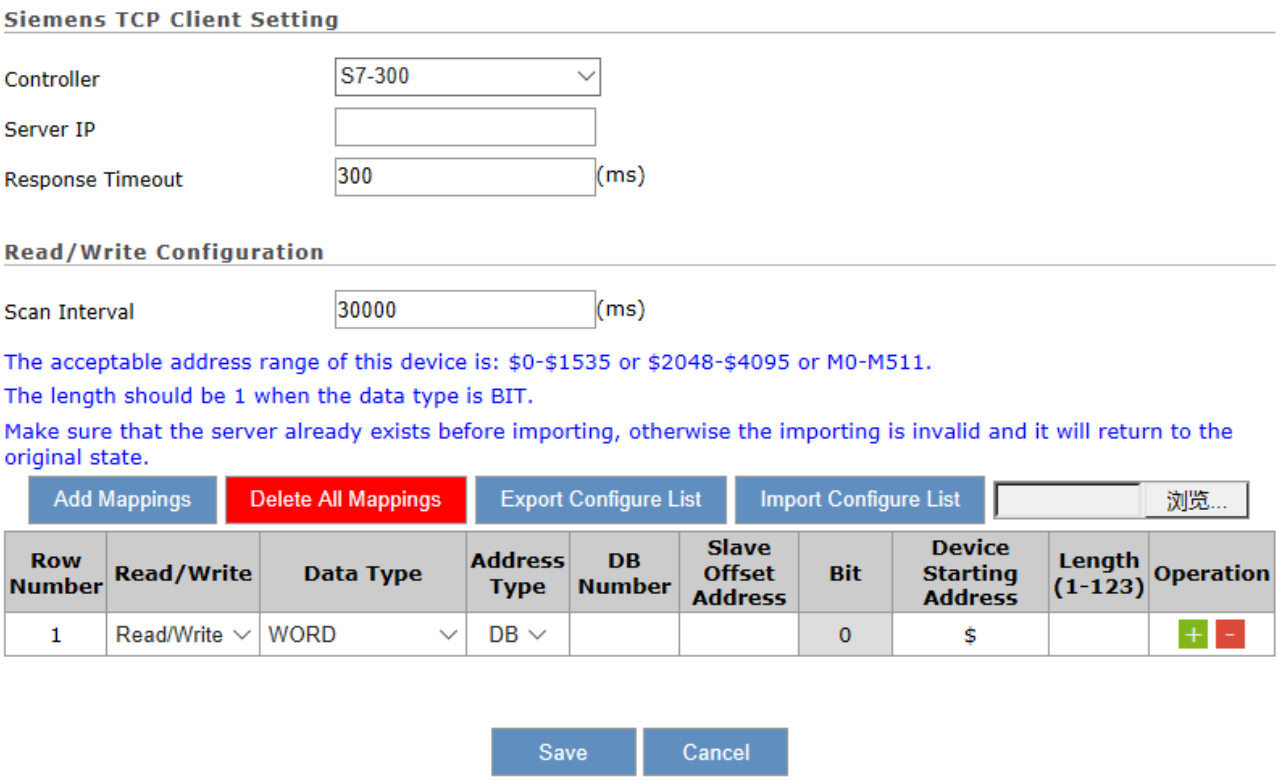
Siemens TCP Client

*32 Siemens TCP servers supported at most

Add Server

Row Number	Server IP	Controller	Response Timeout(ms)	Scan Interval(ms)	Operation

Click Add Server to enter the setting page.



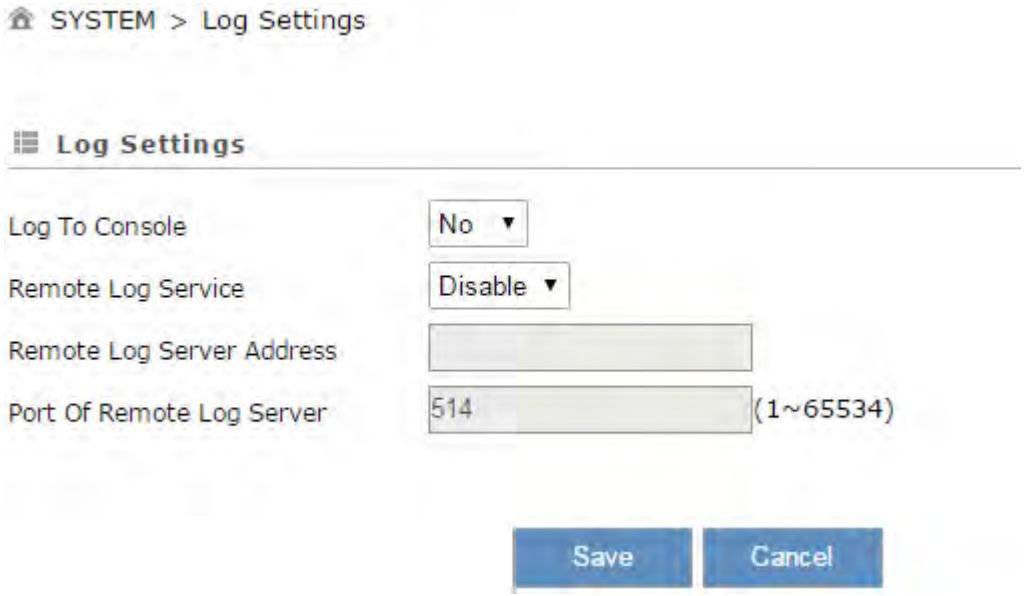
Description	Defualt
Add Server	
Choose the target Siemens TCP server for connection to the routers with 32 servers supported at most.	N/A
Controller	
Set the model type of the Siemens devices for communication.	S7-300
Server IP	
Set the IP address of the Siemens devices for communication.	1
Local TSAP	
Set up the address of local TSAP with Siemens ISO-on-TCP only when controller's model "S7-200 ISO TCP" or "S7-1200/1500 ISO TCP" is used.	N/A
Remote TSAP	
Set up the address of remote TSAP with Siemens ISO-on-TCP only when controller's model "S7-200 ISO TCP" or "S7-1200/1500 ISO TCP" is used.	N/A
Response Timeout	
Users can change the time-out value according to the actual situation with the acceptable time range from 50ms to 10000ms. If specified but the input value is out of the range, it will be set to the value of the min or max attribute.	300
Scan Interval	
Specifies the interval between cyclic scan operations to read the slave devices.	30000
Add Mappings	
Click the button to add mappings. After creating a mapping between IP addresses of slave device and DX router under the user's configuration, the system will collect data from the slave device.	N/A
Delete All Mappings	
Delete all the existing mappings under the server.	N/A

Description	Defualt
Export Configure List	
Export all the mapping and save as a file in the local PC.	N/A
Import Configure List	
Import mappings from the local PC. Click “浏览” to select the target file first.	N/A
Read/ Write	
Set the access permissions for the mapped register address: • **Read-only:** Regularly read data from the appointed slave devices and update to the corresponding register. • **Write-only:** Automatically updates the data to the slave once the registers values changed. • **Read/write:** Regularly read data from the appointed slave devices and update to the corresponding register as well as updating data to the slave once the registers values changed.	Read/ Write
Data Type	
Set the type for collected data: • **BIT:** Bit type • **WORD:** Word type • **WORD(SWAP) :** Double words type.	WORD
Address Type	
• If controller’s model type is “S7-200 ISO TCP”, address type can be set as V/M/Q/I; combined with data types: -Bit type：VB/MB/QB/IB -Word type：VW/MW/QW/IW -DWord type：VD/MD/QD/ID • If controller’s model type is “S7-300” or “S7-1200/1500 ISO TCP”, address type can be set as DB/M/Q/I; combined with data types: -Bit type: DBn_DBX/MB/QB/IB -Word type: DBn_DBW/MW/QW/IW -DWord type: DBn_DBD/MD/QD/ID	DB
DB Number	
Set the DB number for the starting address of Siemens slave’s register operated in read/ write tasks. Not configurable when controller’s model type is “S7-200 ISO TCP”.	N/A
Slave Offset Address	
Set the starting address of Siemens slave’s register operated in read/ write tasks. If the address is VD100, the input value would be 100.	N/A
Bit	
The address input format is 0.0~X.7. Enter the values before decimal point in the input field of Slave Offset Address, while values after decimal point should be entered in the input field of Bit.	N/A
Device Starting Address	
Set the starting address of the corresponding register. Word-type input range is from $2048 to $4095. Bit type range is M0~M511. The beginning of a Device Starting Address must starts with a “$” or “M”.	N/A
Length	
Set the number of the continuous address followed by the starting address which will be read or write. Input range is from 1 to 123.	N/A
Operation	
Click on +/- buttons to add or delete mappings.	N/A

Description	Defualt
Edit	
To edit the parameters or change the setting by clicking on the target field.	N/A

3.4.7 Log Settings

This page is used for configuring the log settings, including Log to Console, Remote Log Service, Remote Log Server Address, and Port of Remote Log Server.



Description	Default
Log to Console	
Set up the log to the console port.	No
Remote Log Service	
Enable/disable the remote log service.	Disable
Remote Log Server Address	
Set up the remote log server address	N/A
Port of Remote Log Server	
Set up the remote log server port, ranging from 1 to 65534.	514

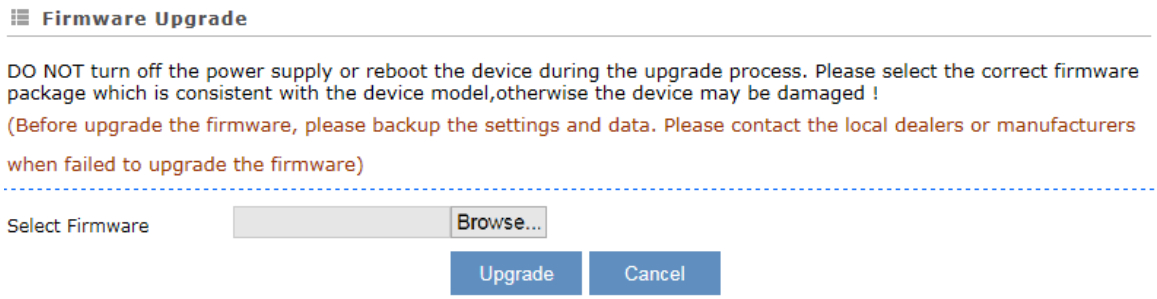
Notice

- Remote log service is used for qualified engineers to check the device remotely when errors occurred. With this service, there is no need to log in to the device, device logs can be exported to the remote log server. The server should support the syslog protocol. When this functionality is enabled, it will take up some resources. Do not enable this functionality disabled, unless it' s necessary.

3.4.8 Firmware Upgrade

This page is used for upgrading the system.

SYSTEM > Firmware Upgrade

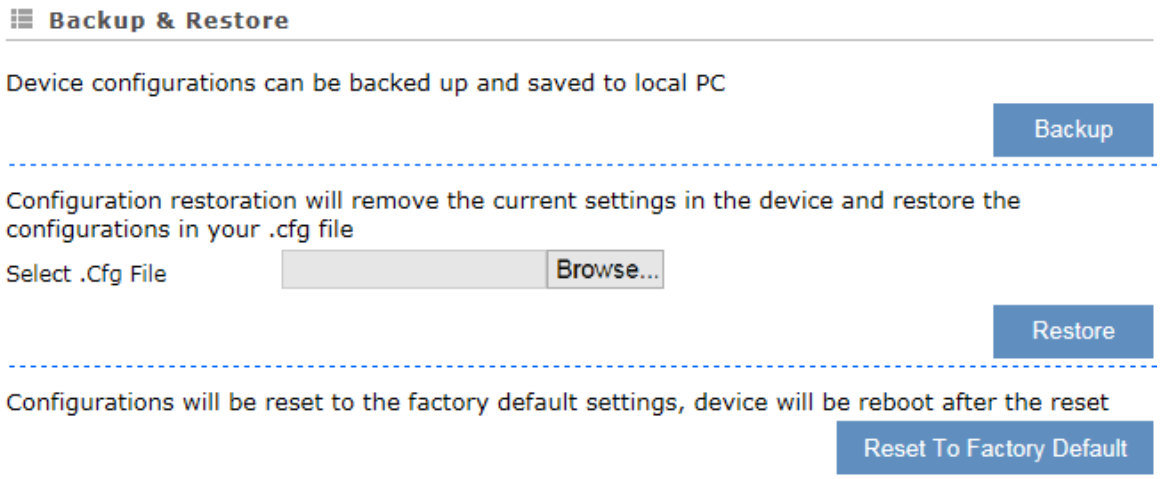


Description	Default
Select Firmware	
Click “Browse” to select the new firmware file.	N/A
Upgrade	
Click “Upgrade” to upgrade firmware. The device will reboot after the upgrade is done.	N/A

3.4.9 Backup & Restore

This page is used for backing up and restoring the configurations.

SYSTEM > Backup & Restore



Description	Default
Backup	
Click “Backup” to save the device configurations on your computer.	N/A
Restore	
Click “Browse” to select the backup file and then click “Restore” to restore the configurations. The device configuration will be restored to the previous version and the device will reboot after the restoring is done.	N/A
Restore To Factory Default	

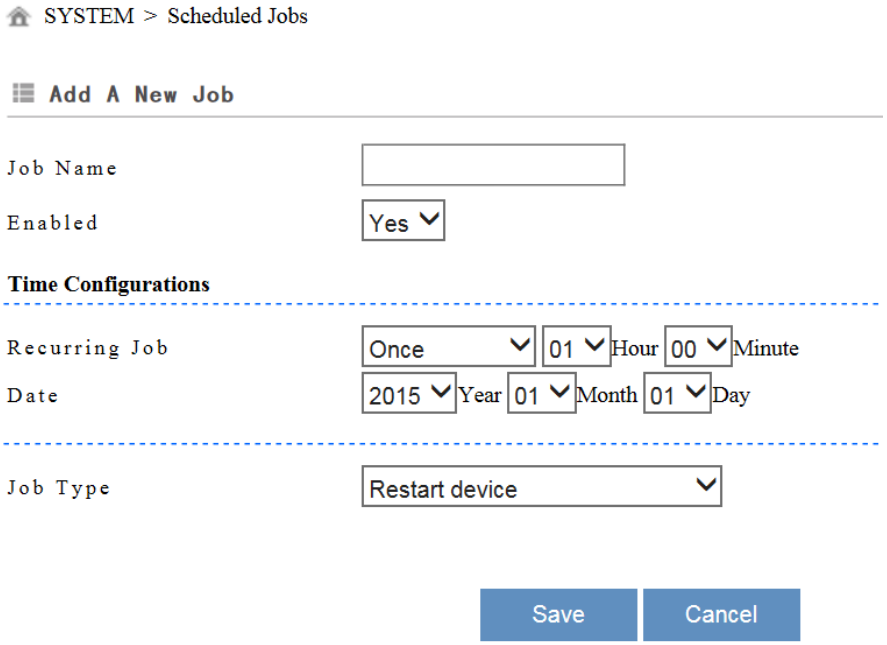
Description	Default
Click “Restore To Factory Default” to reset the configurations to the factory defaults. The device will reboot after the reset is done.	N/A

3.4.10 Scheduled Jobs

This page is used for scheduling job configurations, including ADD A New Job, Export Job List, and Import Job List.

3.4.11 Add A New Job

Click “Add A New Job”, and then you will see the following page. Follow the instruction to add a new scheduled job.

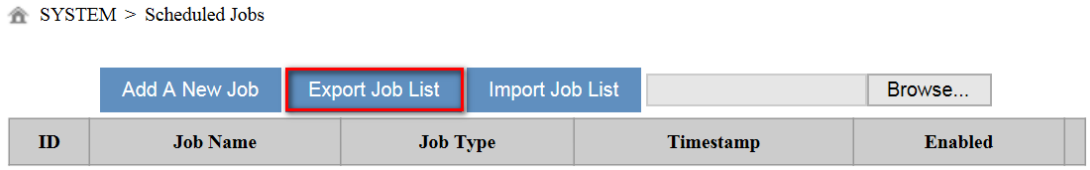


Description	Default
Job Name	
Set up a name for your scheduled job. The name shall be composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Enable	
Select “Enable” to activate this functionality.	Enable
Recurring Job	
The scheduled job can be done Once, Every day, Every week, or Every month. And the specific time can be further defined.	Once 01:00

Description	Default
Date	
Select a specific date to perform the scheduled job.	2015.01.01
Job Type	
Select one of the job type for the scheduled job. • **Restart device** • **Enable DIACloud Service** • **Disable DIACloud Service**	Restart device

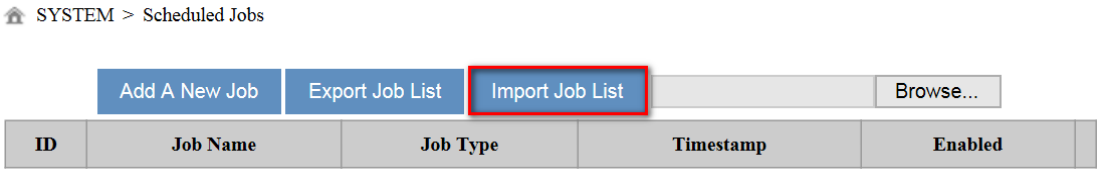
3.4.12 Export Job List

Click "Export Job List" to export the scheduled jobs for future usage.



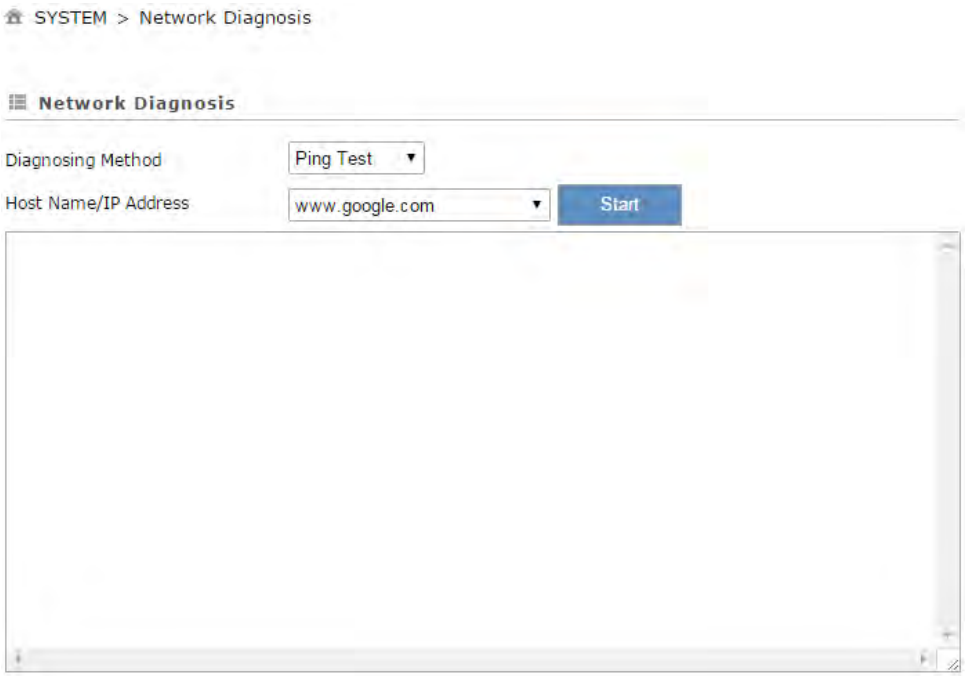
3.4.13 Import Job List

Click "Chose file" to select the scheduled jobs file you have saved and then click "Import Job List" to import the scheduled jobs you have set before.



3.4.14 Network Diagnosis

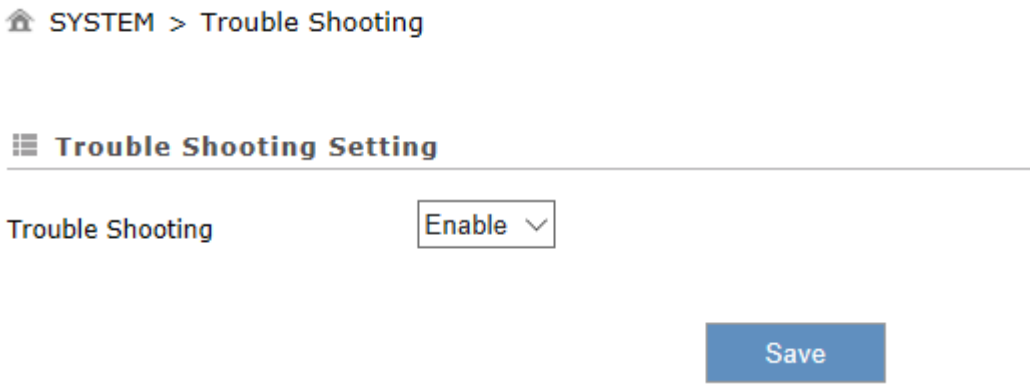
This page is used for diagnosing the network status; methods are Ping Test and Route Trace.



Description	Default
Diagnosing Method	
Selections are “Ping Test”, “Route Trace” and “Cloud Service Diagnose”.	Ping Test
Host Name/IP Address	
Select the domain name or IP address of the server that you want to test. The default options are www.google.com, www.yahoo.com, www.MSN.com, www.amazon.com, www.wikipedia.org, www.facebook.com, www.diacloudsolutions.com and others. When users choose others, users can input the domain/IP manual. **Notice** This function would be disabled when the setting of diagnosing method is “Cloud Service Diagnose”.	www.diacloudsolutions.com
Start	
Click “Start” to start the network diagnosing. While running the network diagnosing, the settings cannot be changed.	N/A

3.4.15 Trouble shooting

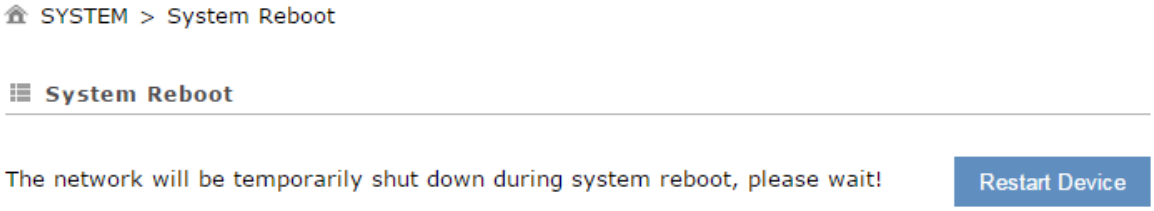
Under normal conditions of network, if the connection with DIACloud has been failing over 30 mins after enabling the Trouble Shooting function, the device will begin to upload all device logs to the specific server directly.



Description	Default
Trouble Shooting	
● Enable: 1. Upload all device logs to the specified server directory for engineers to troubleshoot remotely. If the problem persists, the time interval for the device to upload the logs is 1, 2, 4, 5, 16, and 24 and then the time interval is fixed to every 24 hours. ● Disable: No operation. **Notice** It is suggested to disable this function. However you should enable this function, if the engineer analyzed and advised you to, when some issues occur.	Disable

3.4.16 System Reboot

This page is used for manually rebooting the system. Click "Restart Device" and the system will reboot.



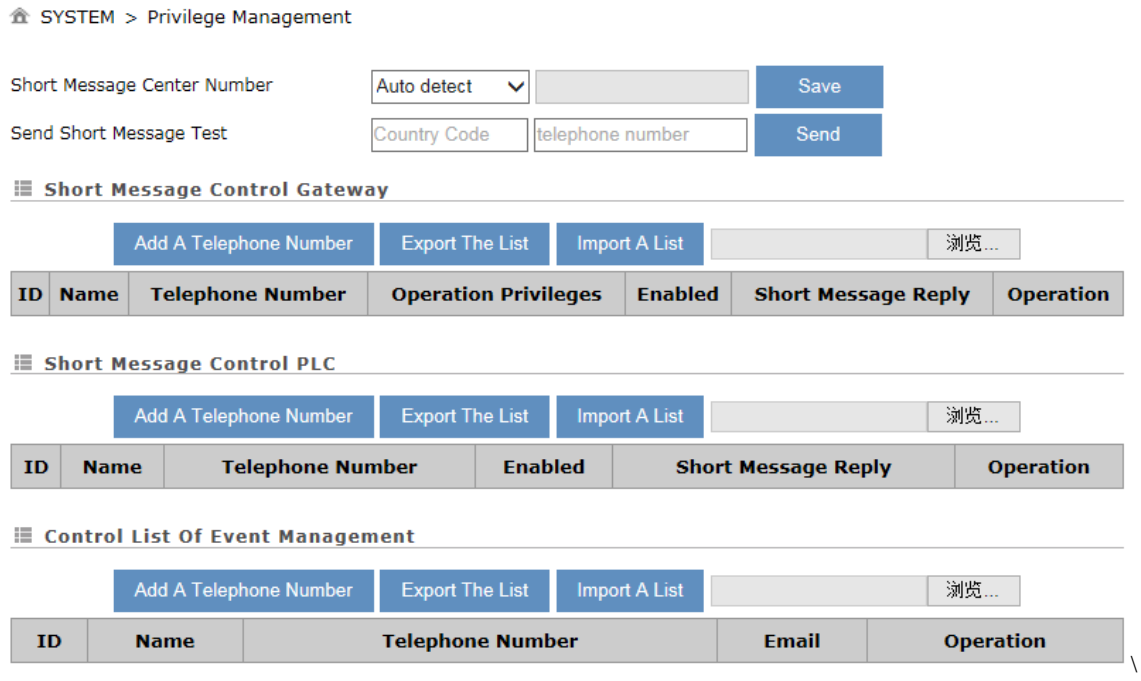
3.4.17 Privilege Management

Privilege management use in order to set the white list of phone numbers and the device operation can be triggered via the specific SMS text from the white list of phone numbers.

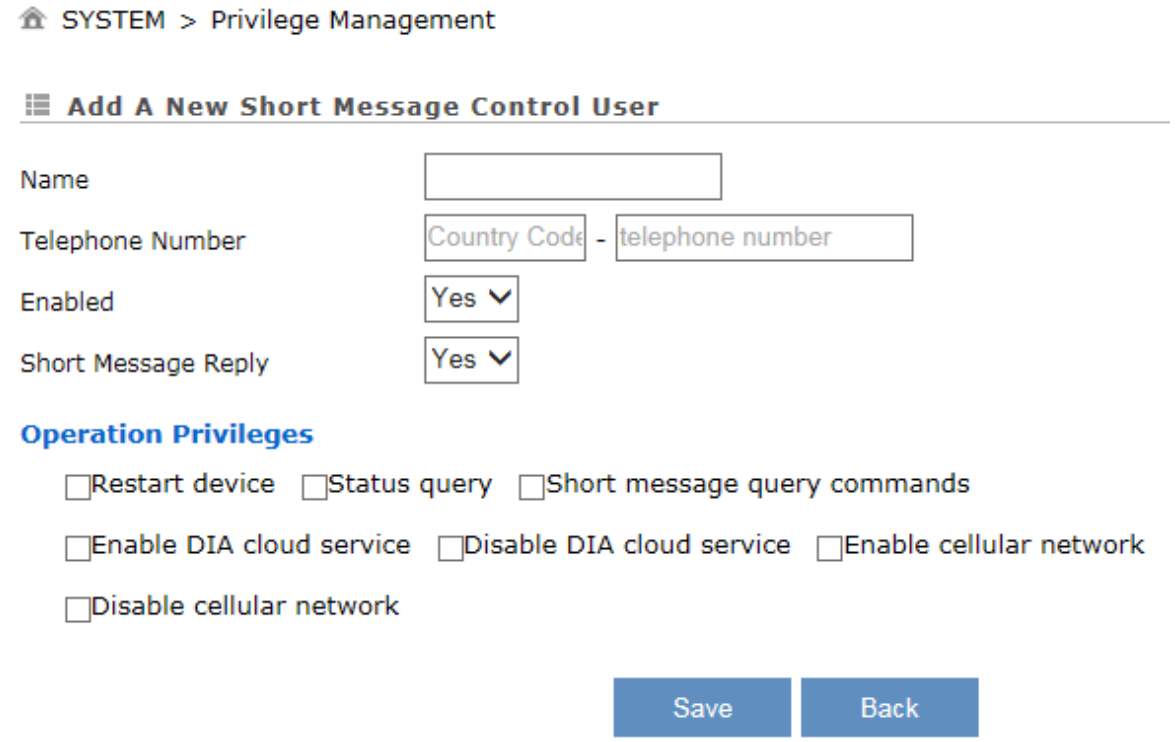
You can fill in the target mobile phone number and press 'Send' button to test the Short Message function of the device.

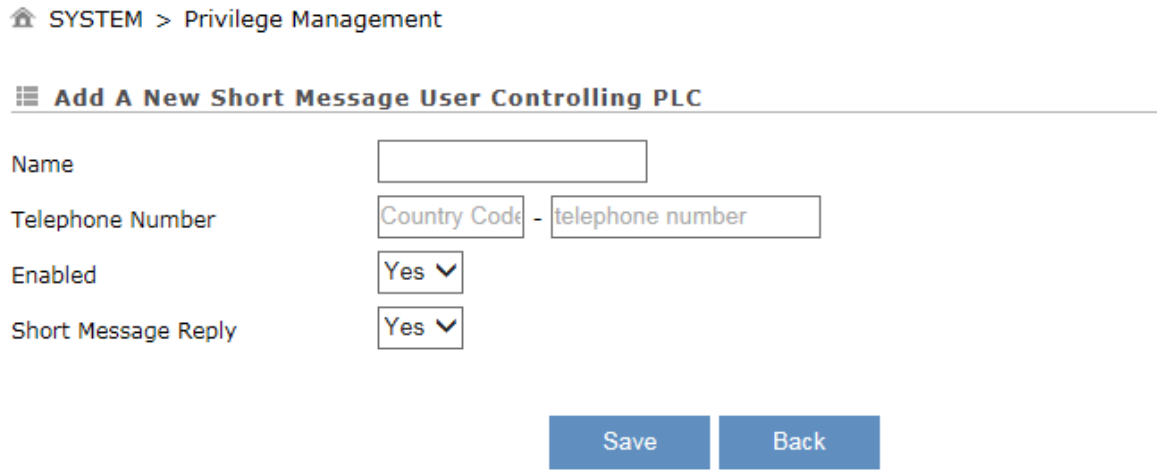
The SMS commands listed below:

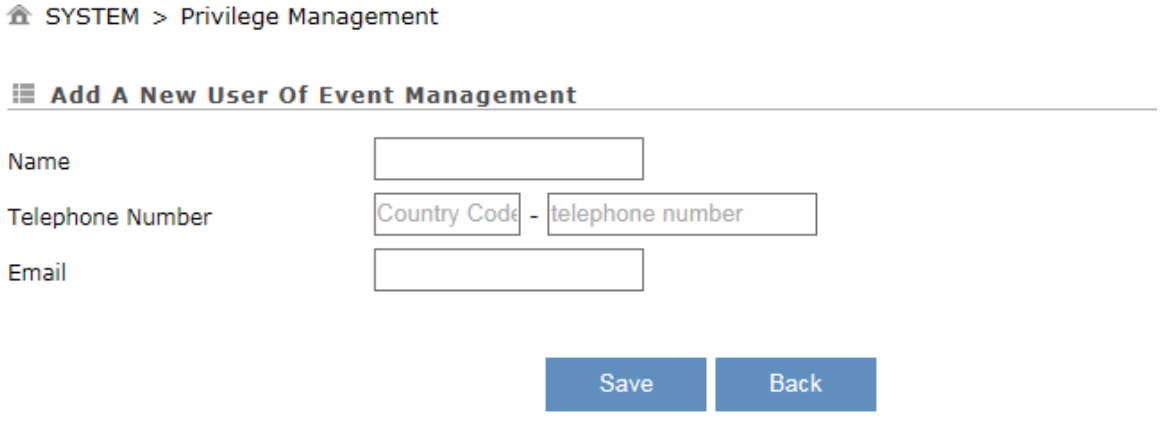
Function	SMS Command	Description
SMS Query commands	"ZLCX" or "zlcx"	List all SMS commands and explanations.
Status Query	"ZTCX" or "ztcx"	Discover the router's current status information, including the following: 1. Cellular network state 2. Firewall state 3. DIACloud state
Restart Device	"CQLY" or "cqly"	Restart the router
Enable cellular network	"KQBH" or "kqbh"	Dial-up the router to internet
Disable cellular network	"DKBH" or "dkbh"	The router disconnects from the internet
Enable DIA cloud service	"KQVD" or "kqvd"	DIA cloud service enables on the router
Disable DIA cloud service	"GBVD" or "gbvd"	DIA cloud service disables on the router



Currently, there are three the main SMS settings: 1. Short Message Control Gateway. 2. Short Message Controlling PLC. 3. Control List of Event Management. Setting interface as follows:





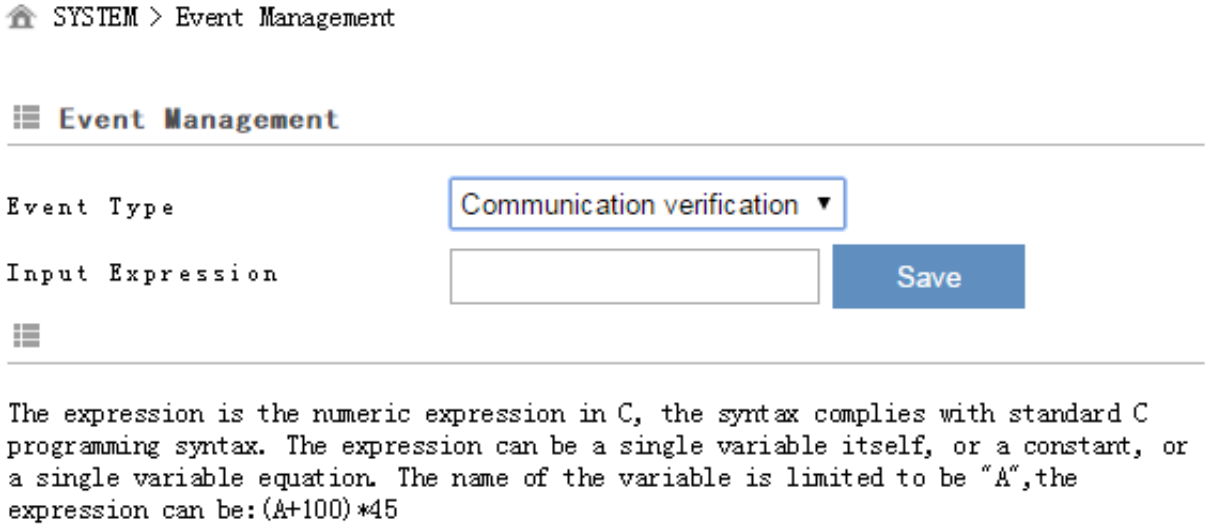


Description		Default
Short Message Center Number		
Input the short message center number supported by this SIM card, the input format is: **"+" "country code" "short message center number"**. **Example: +8613800100500**		**N/A**
Send Short Message Test		
Confirm SMS module related functions are executed correctly, you can send a function test message to the specified number to send a test message to verify the relevant settings are correct. The input format is as follows: • Country Code: **"+" "Country Code".** • Cell phone number: **13800100500.** **Example: +8613800100500**		**N/A**
Add A Telephone Number	**ID**	
	The maximum allow the 10 phone numbers	**N/A**
	Name	
	Set up a name for phone number, The name shall be composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	**N/A**
	Telephone Number	
	Set up a telephone number and country code which can receive the alarm message. The input format is as follows: • Country Code: **"+" "Country Code".** • Cell phone number: **13800100500.** **Example: +8613800100500**	**N/A**
	Enabled	
	Set up the permission to enable or disable	**Yes**
	Short Message Reply	
	When the router receives the SMS commands, the router will response a confirmed message.	**Yes**
	Email	
	Set up an Email address to receive the alarm message. This setting work with The Event management.	**N/A**
Edit		
Edit the existing event		**N/A**
Delete		
Delete the existing event		**N/A**
Export The List		
Export the event of SMS		**Fixed_sms_control_list.cfg**
Import A List		
Import the event of SMS to the router		**N/A**

3.4.18 Event Management

This page is used for setting up 3 types of events, Communication Verification, Alarm Event and SMS Queries Event.

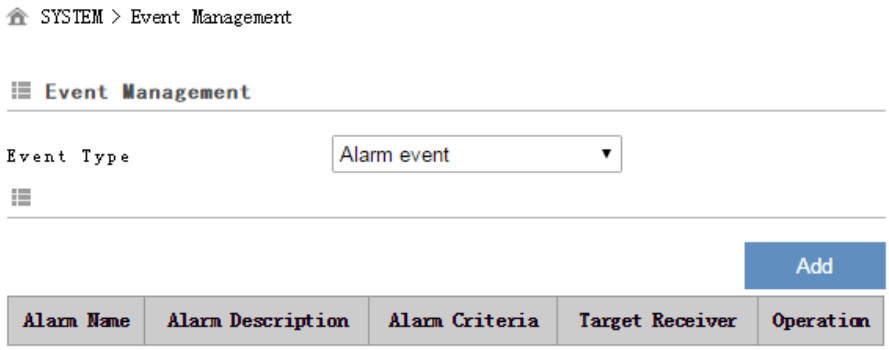
- **Communication Verification:** When this option is selected, the router will monitor and check if this channel is trustable to ensure a safe communication between a router and a PLC via MODBUS TCP, MODBUS ASCII or MODBUS RTU.



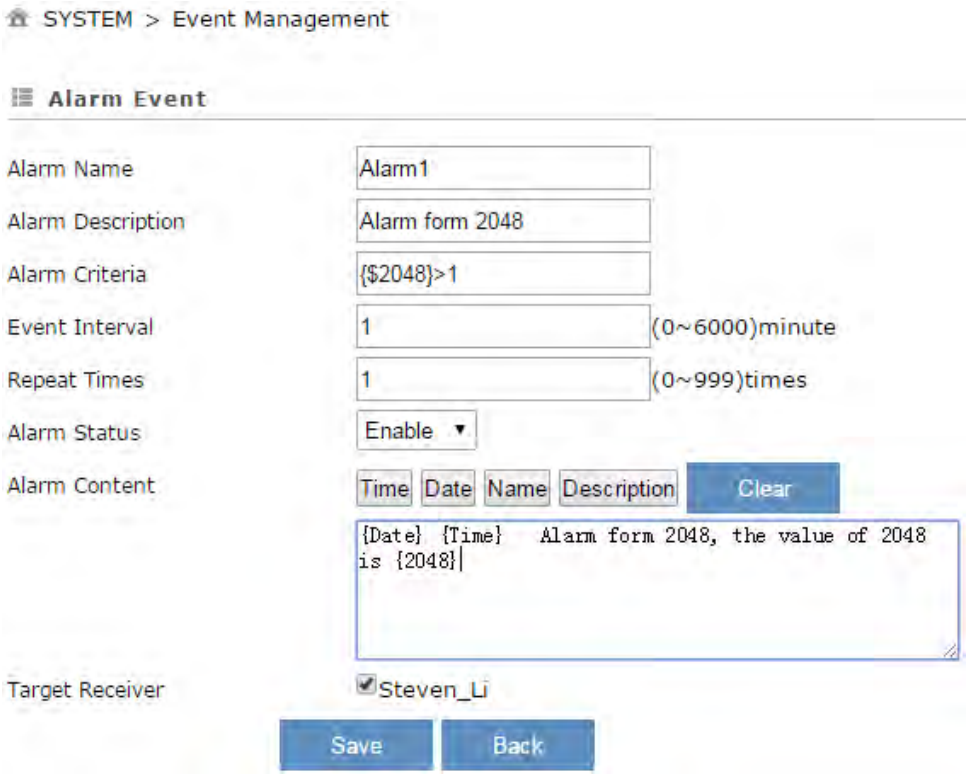
The operators that the expression supports are as below:

Operators	Types	Examples	Description
+	Arithmetic operator	A+100	Addition
-	Arithmetic operator	A-100	Subtraction
*	Arithmetic operator	A*100	Multiplication
/	Arithmetic operator	A/100	Division
&	Logic operator	A&A+100	Logic AND
|	Logic operator	A|A+100	Logic OR
()	Bracket operator	(A+100)*45	Change operation order
^	XOR operation	A^100	XOR operation

- **Alarm Event:** Users can set up the Alarm Name, Alarm Description, Alarm Criteria, Target Receiver and Operation.



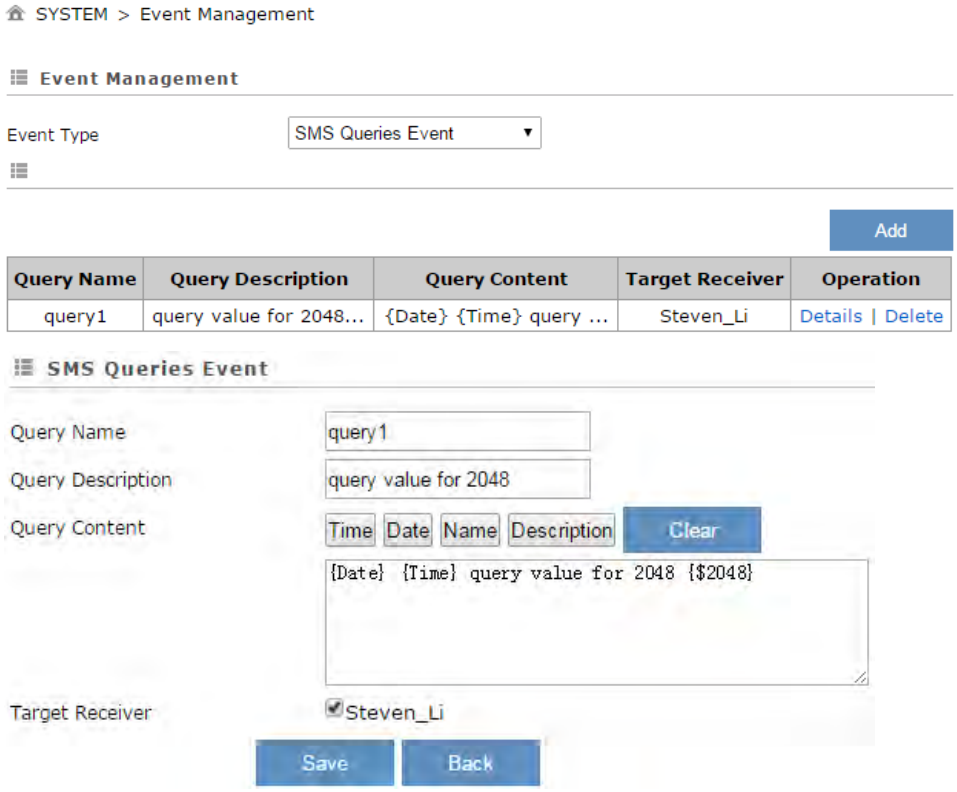
Click “Add” button to create new alarm event and click “Details” to edit the existing event and use ”Delete” button to delete the selected event. Click “Copy” to duplicate the event.



Description	Default
Alarm Name	
Input an alarm name. The name shall be composed of numbers, English letters, uppercase and lowercase. The maximum string length is 32 bytes.	N/A
Alarm Description	
The alarm description shall be composed of numbers, English letters, uppercase and lowercase. The maximum string length is 50 bytes.	N/A
Alarm Criteria	
Setup the alarm trigger condition. The format of alarm variable is {$number 0-4095}, the alarm criteria can be a single alarm variable, or a formula of one or several alarm criteria. For example, the formula can be: {$2048}>100	N/A
Event Interval	
The time interval of alarm sending	0
Repeat Times	
The repeated times of alarm sending	0
Alarm Status	
Enable or disable this alarm setting	Enable
Alarm Content	
Set up the information shown on the alarm contents. The content of the alarm will be sent to the target when alarm criteria are met. The information order can be self-defined. • **Time:** the time when the alarm occurred • **Date:** the date when the alarm occurred • **Name:** the name of the occurred alarm	N/A

Description	Default
• **Description:** the description of the occurred alarm **For example:** Register $2048 represents electrical voltage, the value of register $2048 is 10, and the alarm content is set as: {Date} {Time} Voltage = {$2048}, then the alarm content received by users will be: 2016/06/01 10:00:00(currently time) Voltage = 10. The maximum content length is 160 characters.	
Target Receiver	
Set up the recipient. User can maintain the list by “Control List Of Event Management” in Privilege Management function.	N/A

- **SMS Queries Event**: UserS can declar a query event, when the mobile number in the Control List of event send a query message, system will reply the special content to the mobile number.



Description	Default
Query Name	
Input an query name. The name shall be composed of numbers, English letters, and underline. The maximum string length is 9 characters. For example, after you create a query event name query1, you can send a message with content #MSG#query1 to device SIM card number, then it will reply you the content you setup in the event.	N/A
Query Description	
The query description shall be composed of numbers, English letters, uppercase and lowercase. The maximum string length is 50 bytes.	N/A
Query Content	
Set up the information shown on the alarm contents. The content of the alarm will be sent to the target when alarm criteria are met. The information order can	N/A

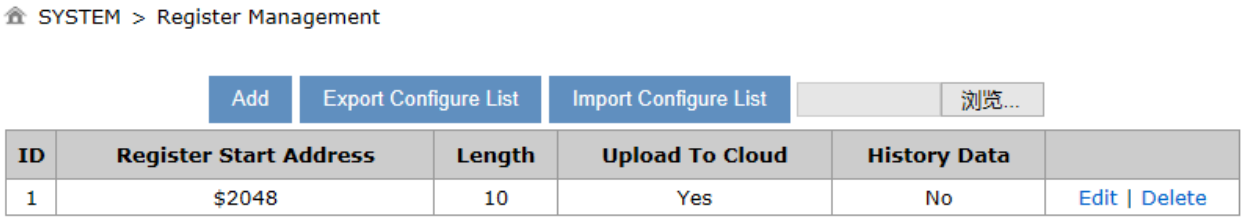
Description	Default
be self-defined. • **Time:** the time when the alarm occurred • **Date:** the date when the alarm occurred • **Name:** the name of the occurred alarm • **Description:** the description of the occurred alarm **For example:** Register $2048 represents electrical voltage, the value of register $2048 is 10, and the alarm content is set as: {Date} {Time} Voltage = {$2048}, then the query content received by users will be: 2016/06/01 10:00:00(currently time) Voltage = 10. The maximum content length is 95 characters.	
Target Receiver	
Set up the recipient. User can maintain the list by 【Control List Of Event Management】in Privilege Management function. System only response the query from receiver list.	N/A

Notice

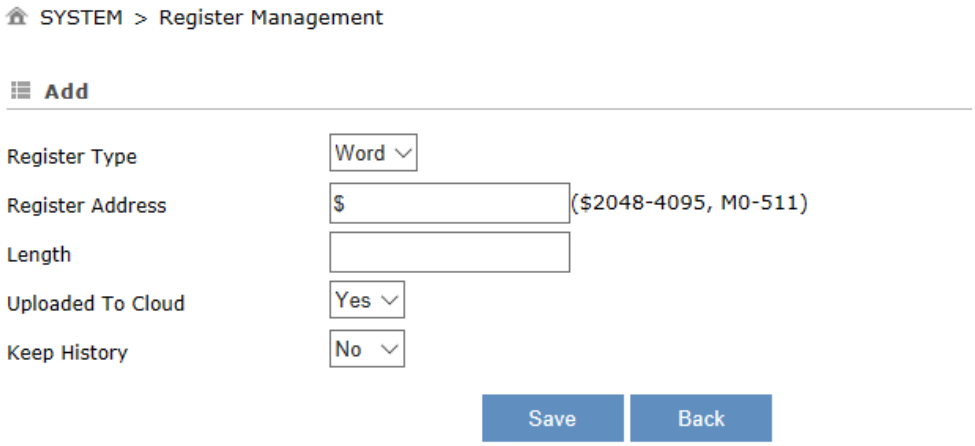
- {} is a special system symbol, which is used to reference system variables or system registers, like ${Time}, ${Date} or ${Number 0 - 4095}. Please use it with caution.

3.4.19 Register Management

This page is used for setting up the rules of register data upload to Cloud. Click “Add” to set a new rule. Click “Edit” to modify the existing rule. Click “Delete” to delete the existing rule.



The address segment M0~M511 and $2048~$4095 can be self-defined. The Start address, Length, Uploaded to Cloud or not and keep history or not can be set up. After clicking “Add”, the following page will show up.



Description	Default
Add	
Click ADD to upload register addresses to the cloud. Up to 20 addresses can be added.	**N/A**
Export Configure List	
Export all the existing rules and save as a file named “fixed_register_list.cfg” in the local PC	N/A
Import Configure List	
Import configure list from the local PC. **Notice: Up to 20 mappings can be imported.** If a total of 10 addresses have been mapped and another 20 mapping addresses are imported, the 10 mapping address imported previously will be covered.	N/A
Register Type	
Choose register type between “Word” and “Bit”.	Word
Register Start Address	
Set Register Start Address applicable for rules. Word-type addresses start with “$”, configurable from $2048~$4095. Bit-type addresses start with “M”, configurable from M0~M511.	N/A
Length	
Set the number of the effective register address followed by the start address. Input value as 1 indicates one register. Word-type effective range:1-2048. Bit-type effective range: 1-512.	N/A
Uploaded To Cloud	
Whether to upload the variable information to Cloud.	Yes
Keep History Data	
This function will keep or overwrite the history data when the register values are uploaded to Cloud. • **Yes:** The existed register values in the cloud **WON’T** be overwritten by the new uploaded register values. • **No:** The existed register values in the cloud **CAN** be overwritten by the new uploaded register values.	No

Notice

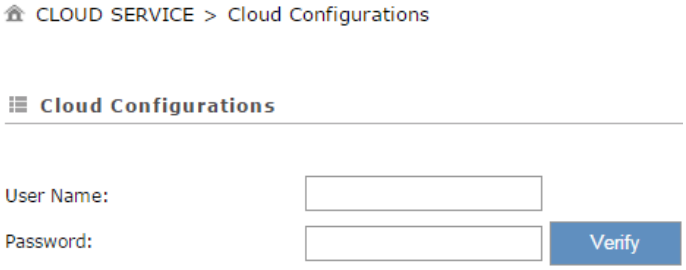
- When the values in the register changes, the results will be uploaded to cloud.

3.5 Cloud Service

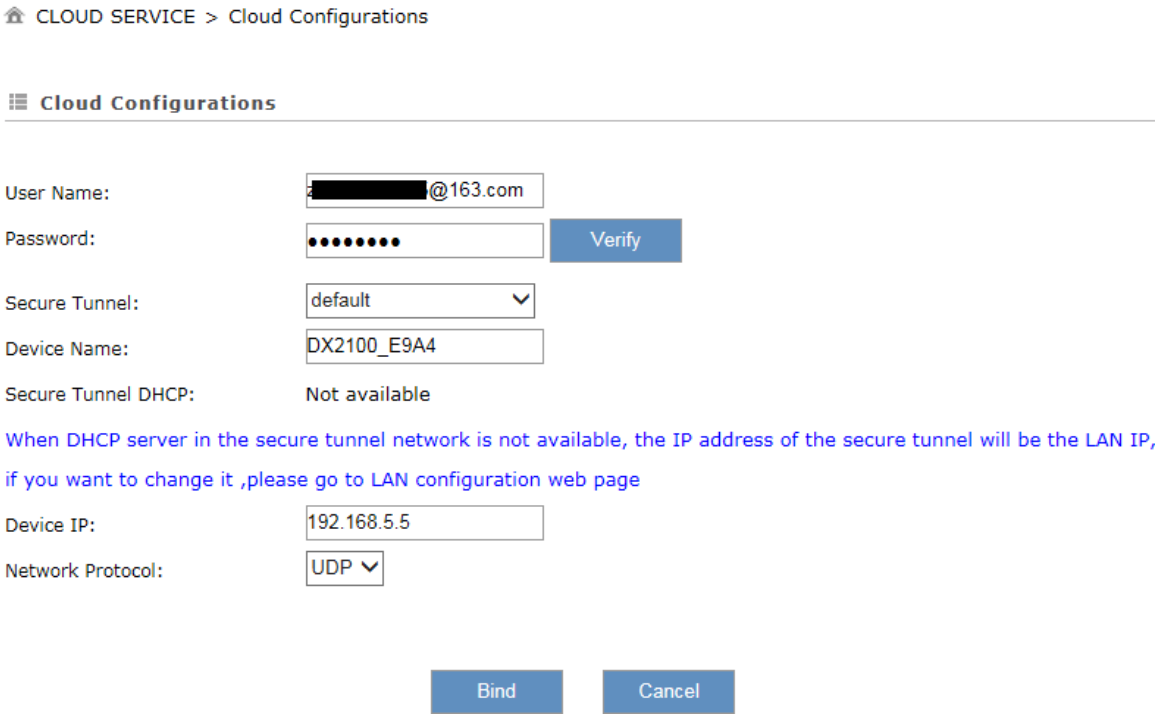
3.5.1 Cloud Configuration

In this page, user can assign the cloud account which will be used to connect to DIACloud by device. Input the user name, the password and click “Verify”. Refer to Chapter 4 for DIACloud account registration.

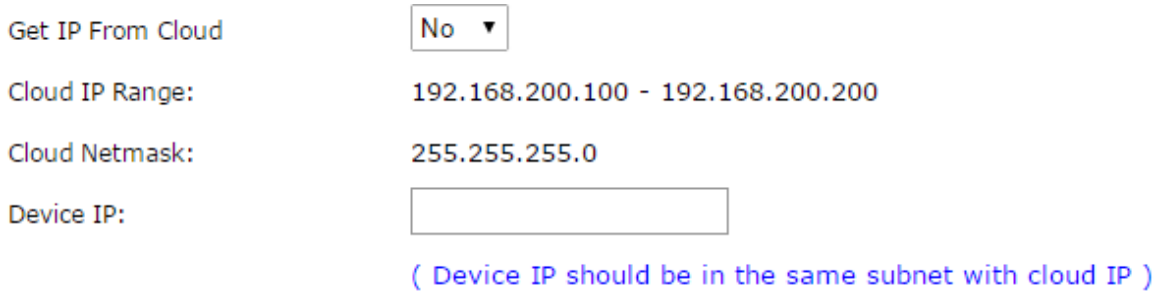
1. Login with your DIACloud account then click the “Verify” button to authenticate with DIACloud server.



2. After authentication successfully, the cloud configurations will show up then the user can modify the secure tunnel and device name.

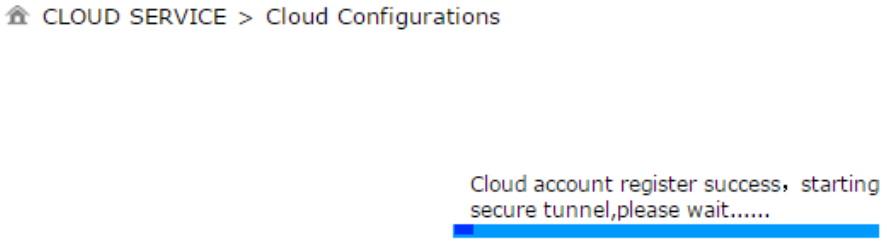


3. Users can also set IP address manually.

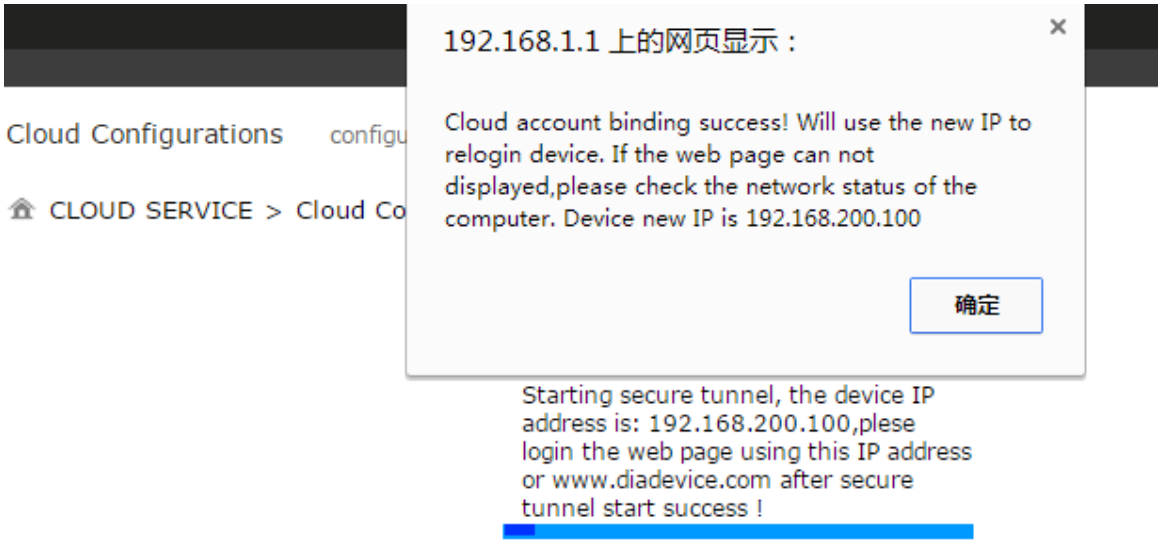


4. Click the "Bind" button, the DX router will bind with DIACloud server and established a secure tunnel between DIACloud server and the DX router. Meanwhile a new IP will assigns to DX router from DIACloud server (assign from

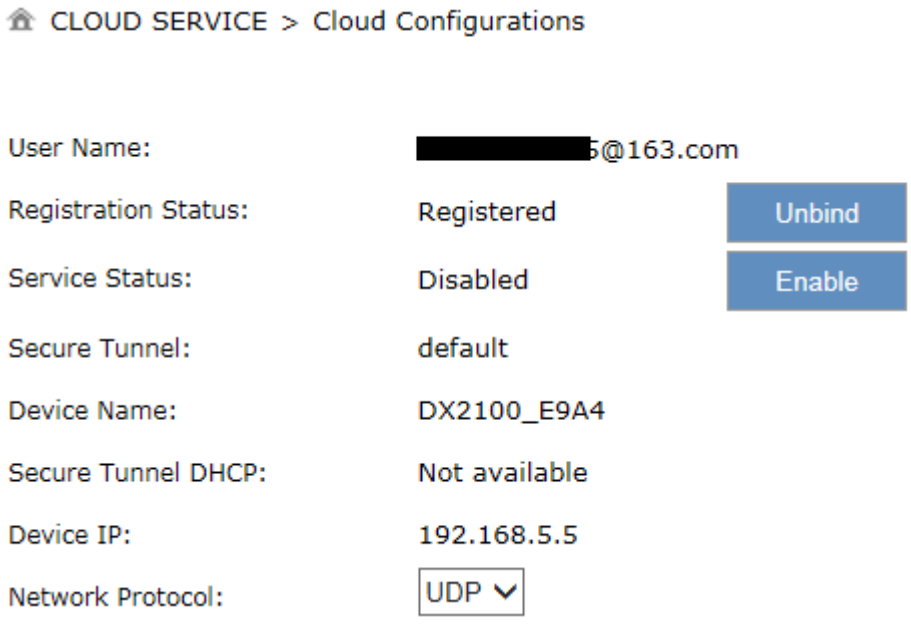
the cloud HDCP server or a user specified).



5. Your browser will access to the DX router with new IP address automatically if DIACloud account binds with DIACloud server successfully. Please make sure a PC and DX router are in the same subnet; otherwise PC will not be able to access to the DX router.

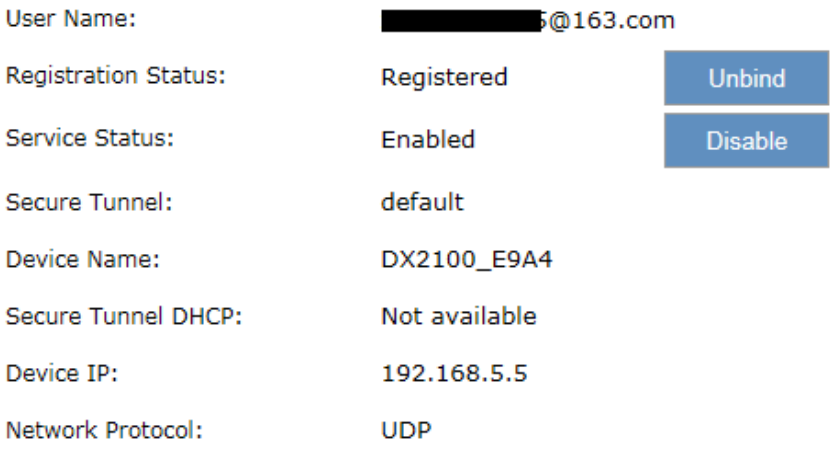


6. If the network is in the poor condition, The binding proccess could be successfully but the Service Status is shown “Disable”.



7. In this situation, the browser will access with 192.168.1.1 and the service status will be “Disable”. You can re-enable the service status to rebuild the secure tunnel again in cloud configurations.

8. When the service status is shown “Enable”, that means the DIACloud service is actived on DX-2100RW-WW. The user also can get the related information in cloud platform.
CLOUD SERVICE > Cloud Configurations



9. Click the “Unbind” button, DX-2100RW-WW will remove the registered account in DIACloud.

Description	Default
User Name	
Set up the name for the DIACloud account.	N/A
Password	
Set up the password for the account.	N/A
Verify	
Check if the username and the password are matched.	N/A
Secure Tunnel	
Select the device under the account to join in a certain secure tunnel network group. For secure tunnel related settings, go to http://www.DIACloudsolutions.com/	Default
Device Name	
Set up the name for the device	N/A
Secure Tunnel DHCP	
When secure tunnel DHCP server is available, and the IP address is allocated by the DHCP server in secure tunnel network, the IP address of this device can be found in the cloud portal.	N/A
Get IP From Cloud	
When selecting “Yes”, IP address can be obtained by the cloud. When selecting “No”, the IP address can be manually set.	Yes
Network protocol	
Set the network protocol of the security tunnel with TCP and UDP. • **UDP:** UDP has a faster data transfer speed. If the network is not lost packet, please use this option	UDP

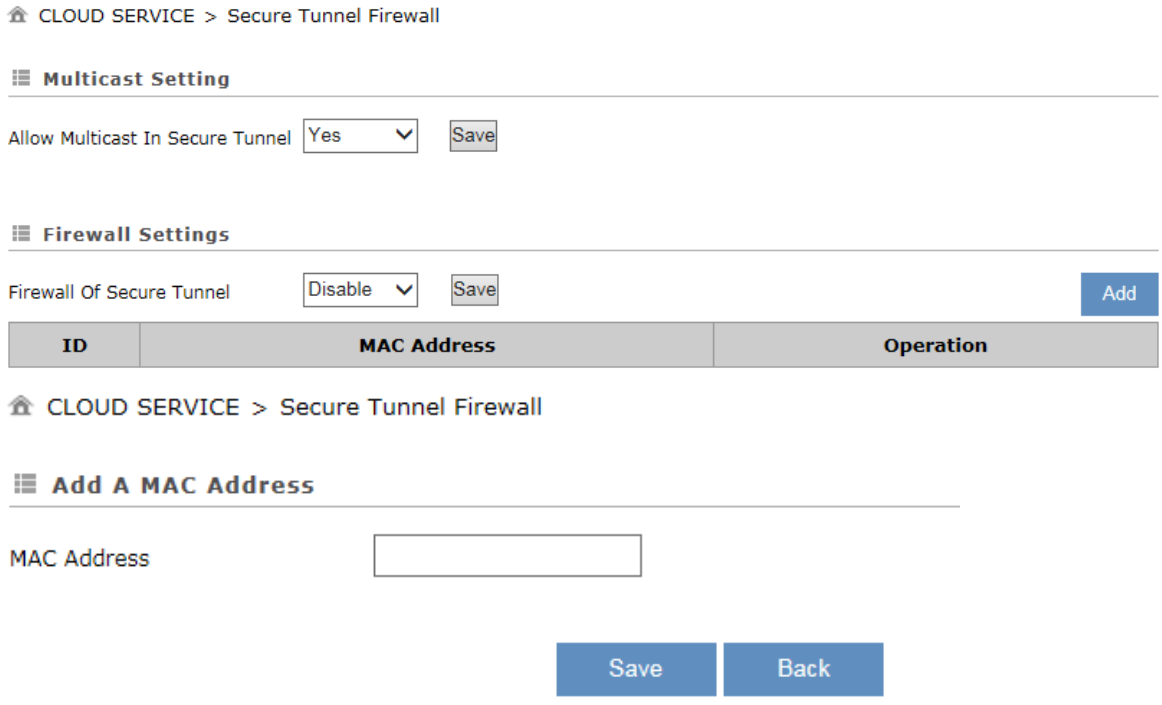
Description	Default
• **TCP:** When the network packet loss is serious, it is recommended to select TCP. After binding the cloud account, you can still change this option, but you must disable the cloud service before changing. When the agent is turned on, the user can only select TCP.	
Cloud IP Range	
Display the Cloud IP Range. The Cloud IP Range is depended on the secure tunnel setting. For the secure tunnel setting, please refer to 5.2.5 Tunnel Network.	N/A
Cloud Netmask	
Display the Cloud Netmask. The Cloud Netmask is depended on the secure tunnel setting. For the secure tunnel setting, please refer to 5.2.5 Tunnel Network.	N/A
Device IP	
User can assign an IP address manually; remember that IP address should be the same subnet as the secure tunnel setting. For the secure tunnel setting, please refer to 5.2.5 Tunnel Network.	N/A

Notice

- Users can log-in to **http://www.DIACloudSolutions.com/** and register for a DIACloud account.
- In rare case, you can't access the web because the computer did not refresh the IP and DNS after the activation, please re-plug the cable to resolve the issue.

3.5.2 Secure Tunnel Firewall

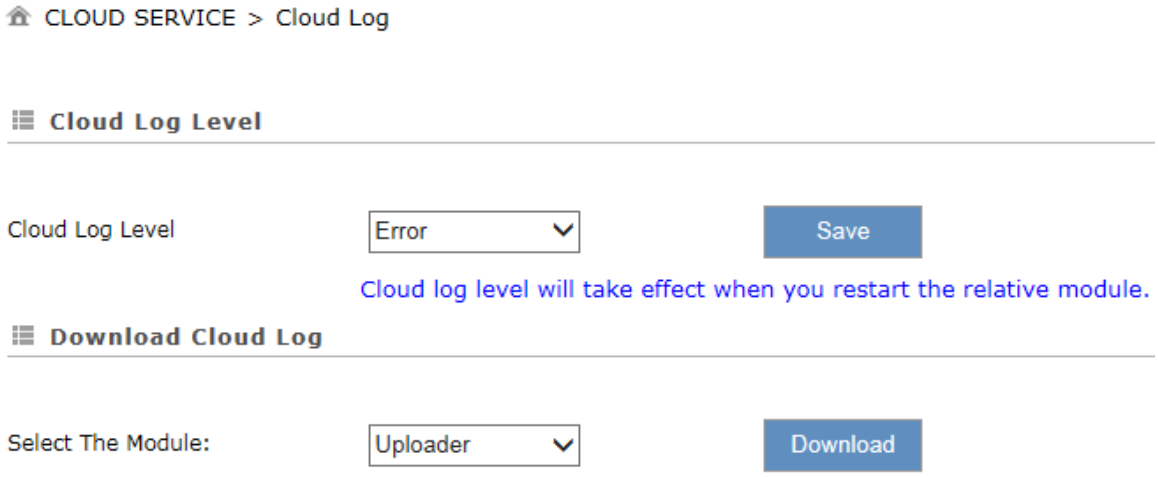
In this page, user can set up the firewall for the secure tunnel.



Description	Default
Allow multicast in secure tunnel	
Set the security tunnel, whether to allow multicast transmission of the nature of the packet. **Options:** Allowed, not allowed	Yes
Firewall of secure tunnel	
Set up the specified MAC device will be allow or forbid to transmit the data in the secure tunnel. Options as below: • **Disable:** Disable this function. • **Black List:** If the network device's MAC address is blacklisted, these devices will **NOT** be able to transmit packets to the secure tunnel • **White List**: If the network device's MAC address is blacklisted, these devices will be able to transmit packets to the secure tunnel.	Disable
Add	
Add a new MAC address into the list.	N/A

3.5.3 Cloud Log

Any information about cloud event can be exported from this function



Description	Default
Cloud Log Level	
You can set different levels of log messages and saved to export to the engineering staff to view. Options as below (Level from low to high): • **Trace:** The TRACE Level designates finer-grained informational events than the DEBUG • **Debug:** Fine-grained informational events that are most useful to debug an application • **Info:** The INFO level designates informational messages that highlight the progress of the application at coarse-grained level. • **Warm:** The WARN level designates potentially harmful situations. • **Error:** The ERROR level designates error events that might still allow the application to continue running. • **Fatal:** The FATAL level designates very severe error events that will presumably lead the application to abort.	Error

Description	Default
Select Log Level	
Specify to download the cloud service module log. Options as below: • Uploader: Data upload module • Secure Tunnel: Secure Tunnel module • Binding: Account binding module	Uploader

3.6 SD Card Quick Configuration

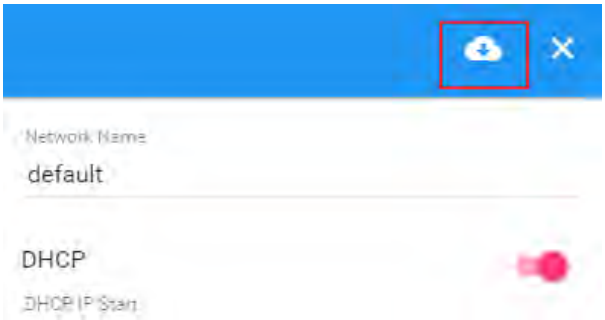
DX-2100RW provides the multiple quick configurations via SD Card.

- Upgrade the device firmware
- Import the device configuration
- Active the device with the DIACloud account.

The SD Card quick configurations will triggers by the following file is created in the SD card after the DX-2100RW reboots:

- The upgrade-package file 'DX2100_UpgradeImage_NorFlash_xxxx_xxxx.bin'
- The device configuration files 'backup.cfg'. (Please refer 3.4.8 Backup & Restore)
- The cloud configuration file 'Provision.bin' (Please refer to the following steps).

1. Go to the DIACloud platform (DIACloudSolutions.com).
2. Log in the DIACloud webpage and click "SECURE TUNNELS"
3. Click to select the Network which you'd like to use and then click the ••• to see and check the details.
4. Click the to download the generated Provision.bin to the local computer.



5. Copy Provision.bin file to SD card.

Power off the device and then insert the SD card into the device (SD card slot below the SIM card slot, on the right side of the device). Turn on the device and it will automatically bind. Check the SD card status indicator to see if the binding is successful.

The following beep codes are for SD Card Quick Configurations, its definition that the various combinations of the configuration file exist on SD card. (× – fail, √ - success or not this operation)

Beep Code	Upgrade.bin	backup.cfg	Provision.bin
1 long	×	√	√
1 long, 1 short	√	×	√
1 long, 2 short	×	×	√
1 long, 3 short	√	√	×
1 long, 4 short	×	√	×
1 long, 5 short	√	×	×
1 long, 6 short	×	×	×
None	√	√	√

Notice

- Name rule for BIN file: Provision.bin
- Please do not change the file name of firmware upgrade-package.
- Please do not create the two different upgrade-package file in SD Card. In order to avoid the upgrading process fails.
- At least a 10-minute interval of separation between the two SD Card Quick Configuration

MEMO

4

Chapter 4 DIACom

Table of Contents

4.1 Introduction to DIACom 4-2

4.1.1 Select a Suitable Firmware Version 4-2

4.1.2 DIACom Installation 4-3

4.1.3 DIACloud Account Registration 4-3

4.1.4 Bind DIACloud Account 4-5

4.2 DIACom Operation 4-6

4.2.1 Setup a Secure Tunnel 4-6

4.2.2 Create a Virtual Serial-Port 4-10

4.2.3 Remote Control and Monitoring via DIACom 4-12

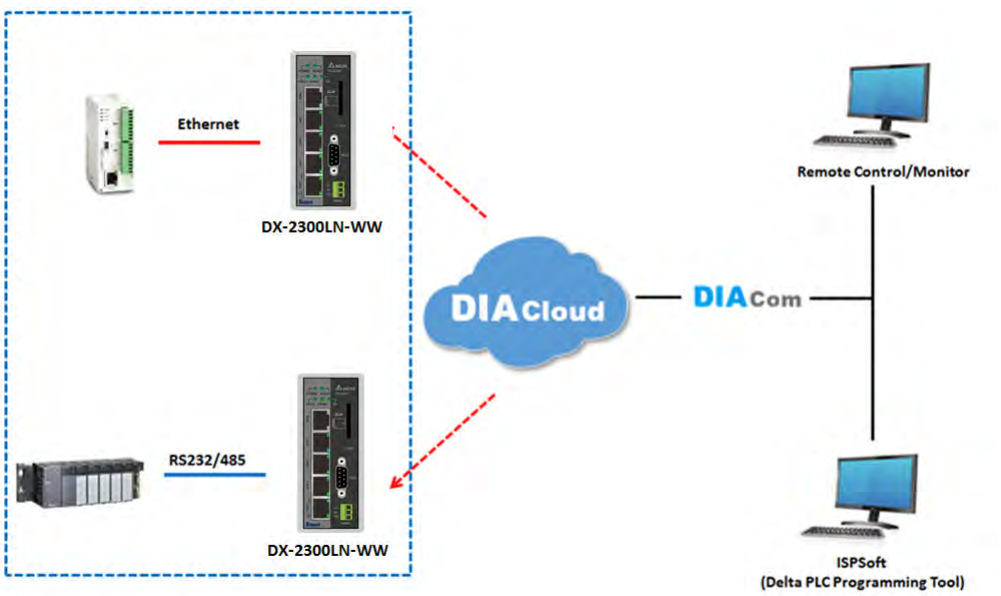
4.2.3.1 Via a LAN Port 4-12

4.2.3.2 Via a RS232/RS485 Port 4-12

4.2.4 Automation Startup 4-14

4.1 Introduction to DIACom

DIACom allows you to create a secure tunnel between your PC and router, making it possible for your PC to communicate remotely with the devices connected to the router. Thus, engineers can control, monitor, operate, program and diagnose the device remotely whenever there is internet connectivity.



Notice

- DIACloud provides you with cloud services, including the connected device management, secure tunnel network creation, data upload/download, and directional transmission.
- If you need to configure or monitor your controller, you will need to install programmable logic controller software, for example WPLSoft/ISPSoft for Delta PLC.

4.1.1 Select a Suitable Firmware Version

Find a suitable DIACom firmware version according to the following table below for your router.

Corresponding Table:

Device Model	Firmware Version
DX-2100	V1.3.3.0 or above
DX-2300	V1.3.3.0 or above

Notice

If the device firmware is lower than 1.3.3.0, please use DIACom 1.2.8.0 or lower.

4.1.2 DIACom Installation

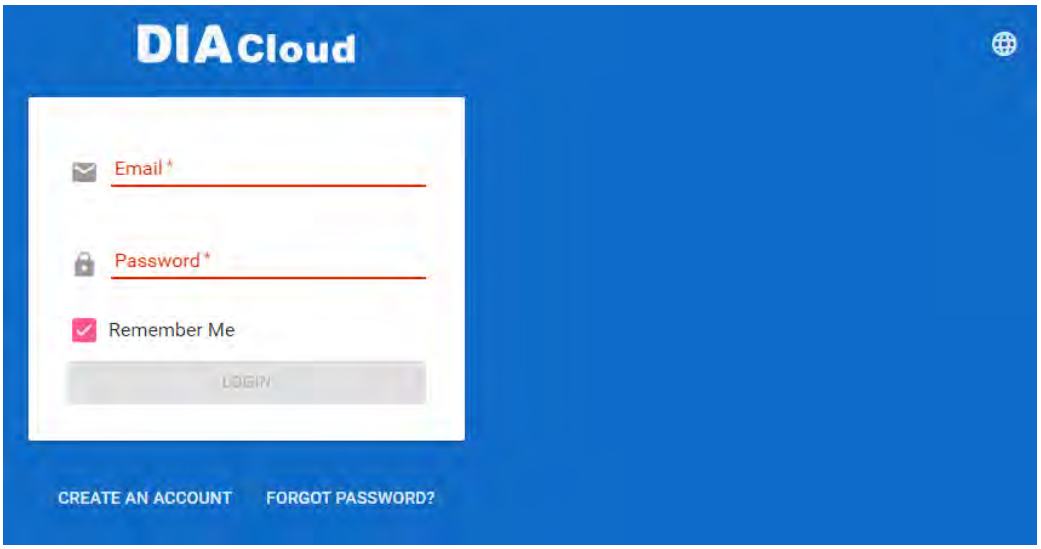
Obtain the DIACom firmware package from the official website or from our sales representative. Administrator privileges are required to run and install the package. Uninstall older versions of DIACom before downloading new DIACom firmware package.

Notice

DIACom supports Windows XP, Windows 7 (32-bit and 64-bit) and Windows 8 (32-bit and 64-bit).

4.1.3 DIACloud Account Registration

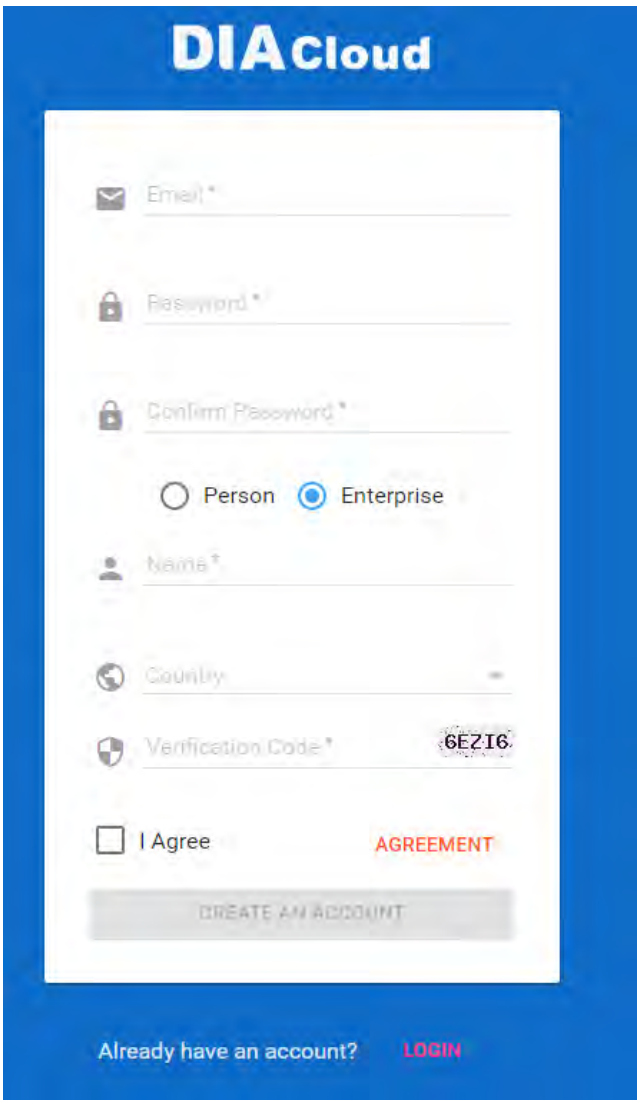
1. Before registration, you should have a valid email account. (DIACloud uses your email address as your account.)
2. Open the DIACloud web page (http://www.DIACloudSolutions.com). The system will redirect you to the registration page:



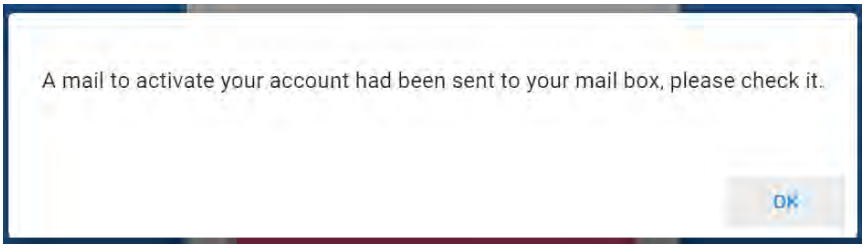
Notice

Click at the upper right corner to change the interface language to English.

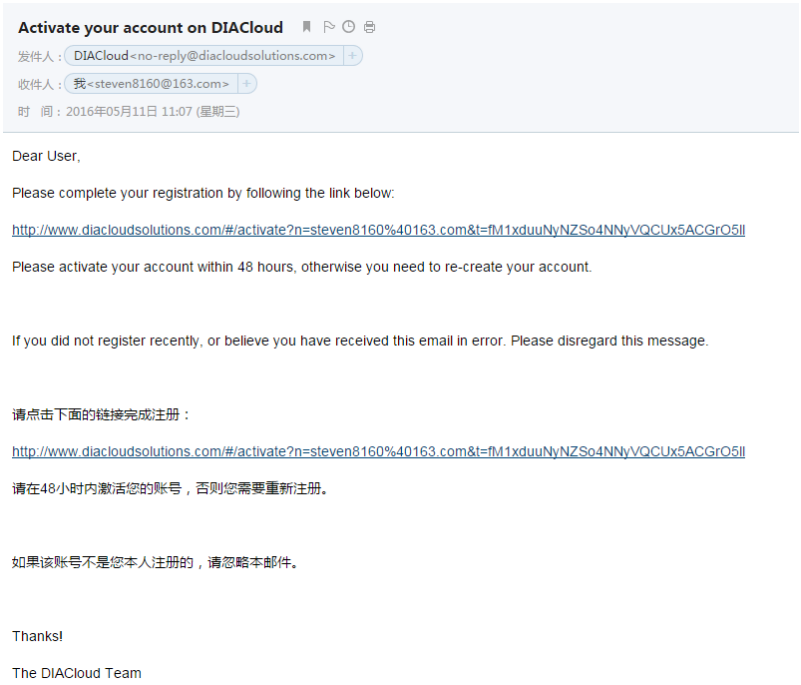
3. Input your email address, password and other relevant information on the registration page. Select “I Agree” and click “CREATE AN ACCOUNT”.



4. After clicking “CREATE AN ACCOUNT”, a congratulation page will be prompted and an activation email will be sent to the email address you have used as your DIACloud account.



5. You will find an activation email sent from no-reply@diacloudsolutions.com in your email box. Open the email, click “here” link in the email and complete DIACloud account activation operation. And you will be redirected to the DIACloud login page. Input your account and password to log in to the DIACloud.



Activate your account on DIACloud

发件人：DIACloud<no-reply@diacloudsolutions.com>

收件人：我<steven8160@163.com>

时　间：2016年05月11日 11:07 (星期三)

Dear User,

Please complete your registration by following the link below:

http://www.diacloudsolutions.com/#/activate?n=steven8160%40163.com&t=fM1xduuNyNZSo4NNyVQCUx5ACGrO5ll

Please activate your account within 48 hours, otherwise you need to re-create your account.

If you did not register recently, or believe you have received this email in error. Please disregard this message.

请点击下面的链接完成注册：

http://www.diacloudsolutions.com/#/activate?n=steven8160%40163.com&t=fM1xduuNyNZSo4NNyVQCUx5ACGrO5ll

请在48小时内激活您的账号，否则您需要重新注册。

如果该账号不是您本人注册的，请忽略本邮件。

Thanks!

The DIACloud Team

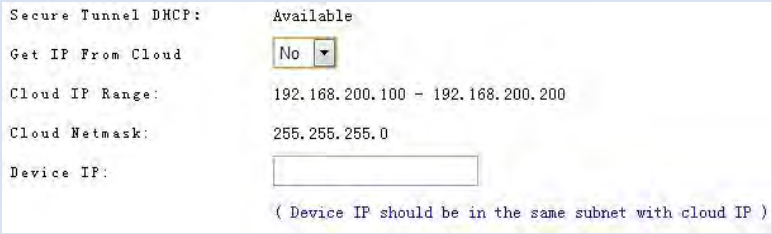
4.1.4 Bind DIACloud Account

Follow the steps blow to bind your DIACloud Account.

1. Local Network Setups: Please refer to Chapter 2.1 to 2.1.3 Web-based GUI Configuration for more information.
2. Bind DIACloud Account: Please refer to Chapter 3.5 Cloud Service for more information.

Notice

- **Secure Tunnel:** Secure tunnel is a virtual network. Users can set up several groups of secure tunnel for easier device management.
- **Device Name:** the serial number + "_" + "Mac address" of the device is the device name by default.
- **Get IP From Cloud:**
  - When selecting "Yes": The system will assign an IP address for the device according to the Secure Tunnel settings and the availability of the IP addresses. Take note of the assigned IP address, it will be used when logging to the DIACloud.
  - When selecting "No": The IP address can be manually set.



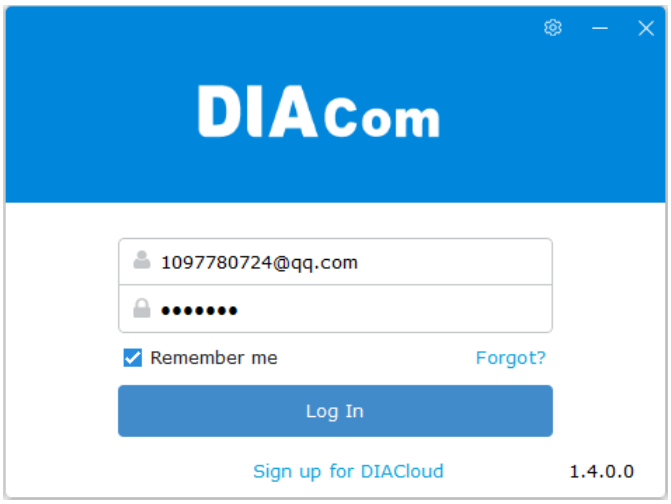
The IP address of the DX-2100 Series and the WAN of your connected PC should be in different network segments.

4.2 DIACom Operation

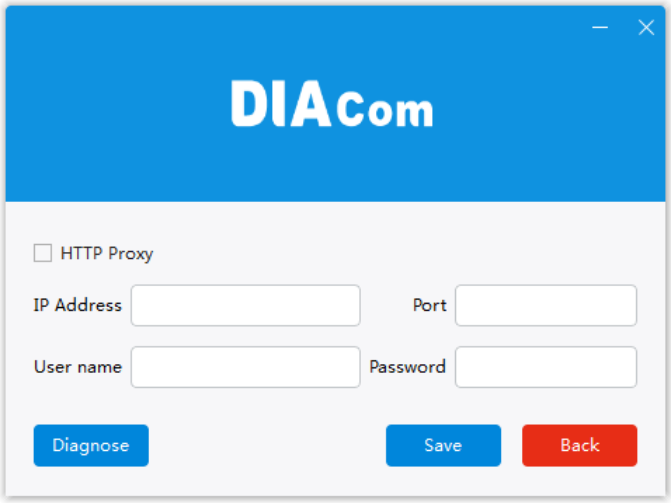
4.2.1 Setup a Secure Tunnel

Make sure there is internet connectivity, before creating a secure tunnel between your local PC and router via the DIACom. Http Proxy and Port Agent are configurable in DIACom network setting function, you can set it to avoid the possible limitation.

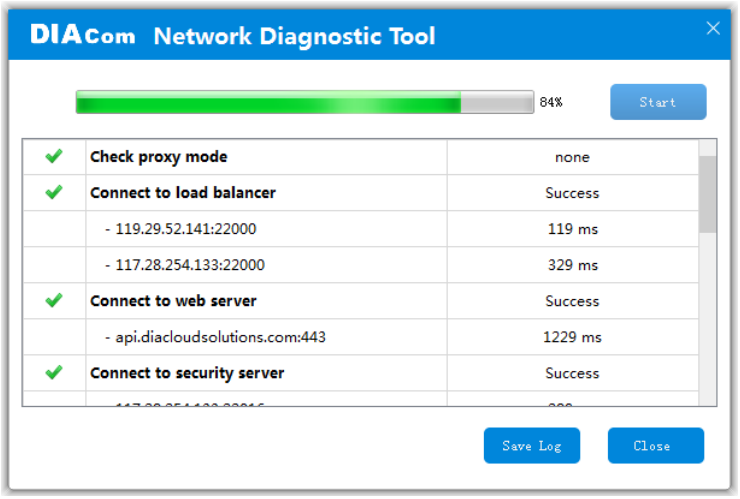
1. Run DIACom and log in with your router's cloud account.



2. Click to go into network setting page if need be.



- **Http proxy:** Please fill in the proxy server address, port, username and password if the LAN needs to set the proxy to access the Internet. Click "Save" button to enable the config.
- **Diagnose:** The user can click the Diagnostic button to test the current internet settings, whether to connect to the DIACloud server

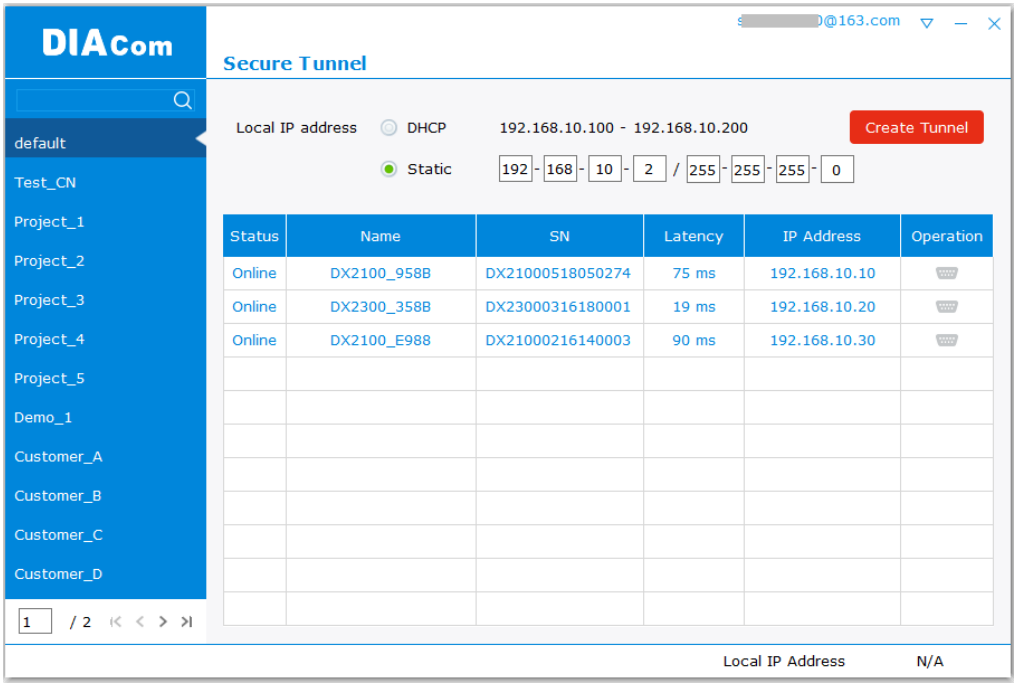


Notice

- DIACom will automatically determine whether the port agent needs to enable.
- Make sure that the external network port 80 and port 443 are opened and can access any network domains and IP addresses

3. After the login is successful, the software displays the security tunnel page. The security tunnel list is displayed on the left side of the page, and the network information of the security tunnel and the device list are displayed on the right. Users can choose to use DHCP or manually set the cloud IP address

   - **DHCP:** Obtain an IP address from Cloud automatically when Cloud DHCP function is available.
   - **Static:** Manually set the IP address, the IP should be in the same subnet with DX device

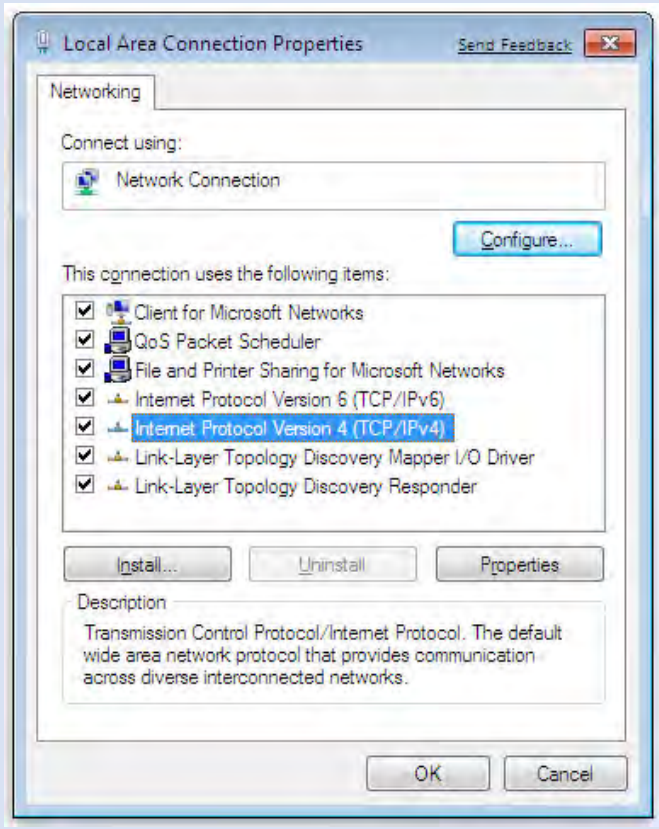


Notice

If it is found that the static IP address is configured from DIACom, the IP address of the local IP address in the bottom right corner will be different from the original setting. Please change according to the following settings.

1. Go to Network and Sharing Center and click on the DIACom Ethernet Adapter for your network connection.

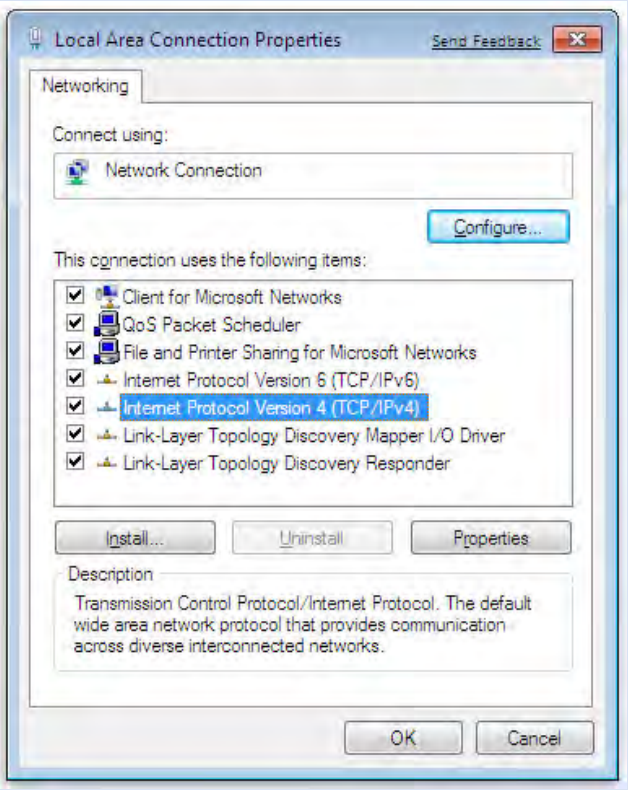
2. Right-click, then click Properties.
3. Click the Networking tab. Under This connection uses the following items, click either Internet Protocol Version 4 (TCP/IPv4)。



4. Go to Network and Sharing Center and click on the DIACom Ethernet Adapter for your network connection.

5. Right-click, then click Properties.

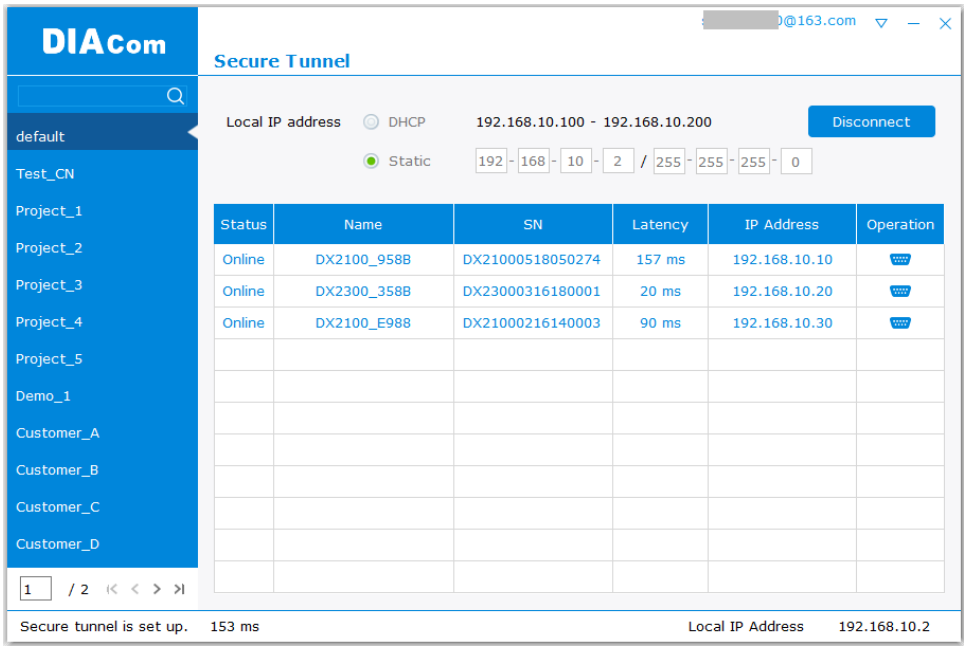
6. Click the Networking tab. Under This connection uses the following items, click either Internet Protocol Version 4 (TCP/IPv4)



7. Set the IP address of the local computer manually. However, you'll need to make sure there are no IP conflicts.

4. After the configuration is complete, click the Create Tunnel button to establish a connection with the specified tunnel.

5. The following information is displayed: tunnel connection status, local delay to the DIACloud cloud server, and the IP address used by the local virtual network adapter.



6. After successful connection with the cloud, the local computer will be able to use debugging tools or monitoring software to debug, monitor, and program the remote network interface devices. In addition, you can remotely configure the router's router page (click the device in the device list Of the IP address) of the router for remote configuration.

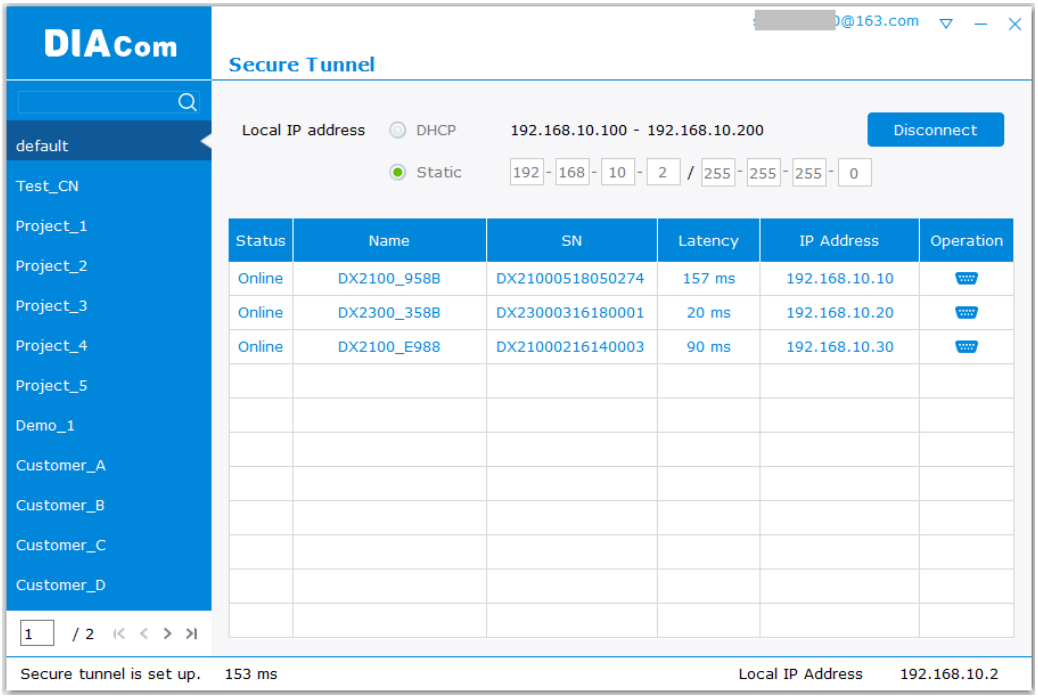
Notice

- You can create different groups of secure tunnels, divide different devices into groups according to their needs, and implement group management devices
- To avoid the virtual network card IP network segment and the local computer network card of the actual network to avoid the same network conflict
- After the secure tunnel is successfully connected, you must first disconnect the current connection to select another security tunnel,

4.2.2 Create a Virtual Serial-Port

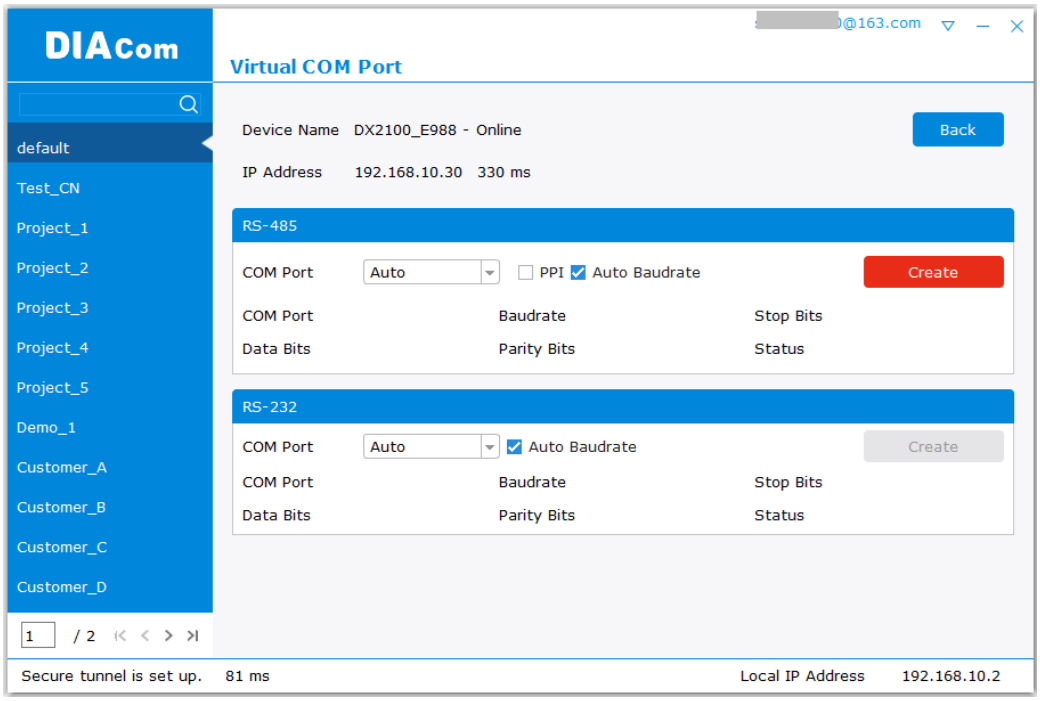
To debug a remote serial device,

1. Click the icon at the back of the corresponding remote device to enter the Create Virtual Serial Interface



2. Click on the “Create” button to create a virtual COM port on the local PC, related to the RS-232 or RS-485 port on the remote devices. If the RS-232 or RS-485 port is not working with transparent mode, the corresponding “Create” button would be unavailable.

> **Notice**
>
> Support RS-232 and RS-485 working with transparent mode at the same time.

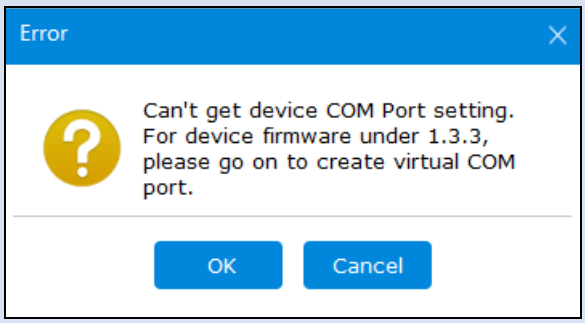


3. After create successfully, the local PC can perform commissioning, programming and monitoring to the remote devices with debugging tools or monitoring software.

Description	Default
PPI	
Specially optimize uploading and downloading action PPI for Siemens S7-200 series. **Notice** Please leave unchecked for devices not included in Siemens S7-200 series to avoid failed upload/ download error.	Unchecked
Auto Baudrate	
Enable or disable Auto Baudrate function. ● Checked: Perform Auto Baudrate detection. ● Unchecked: Close Auto Baudrate detection. **Notice** We suggest to turn off this function if you’re using Gitzo’s or Mitsubishi’s PLC devices.	Checked

Notice

- If the device's RS-232 / RS-485 is not operating in Transparent mode, the corresponding button is grayed out.
- DIACom will prompt an error message if the FW version of DX is under V1.3.3.



4.2.3 Remote Control and Monitoring via DIACom

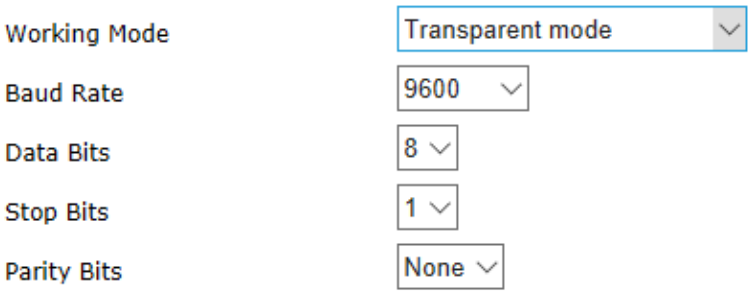
4.2.3.1 Via a LAN Port

If your router is connected to remote devices via a LAN port, you can use the configuring/monitoring software on your local computer to configure and monitor after opening a virtual tunnel. Some program would require the IP addresses of your remote device. Simply input the required information in the configuring/monitoring software and then you can configure and monitor the connected device remotely.

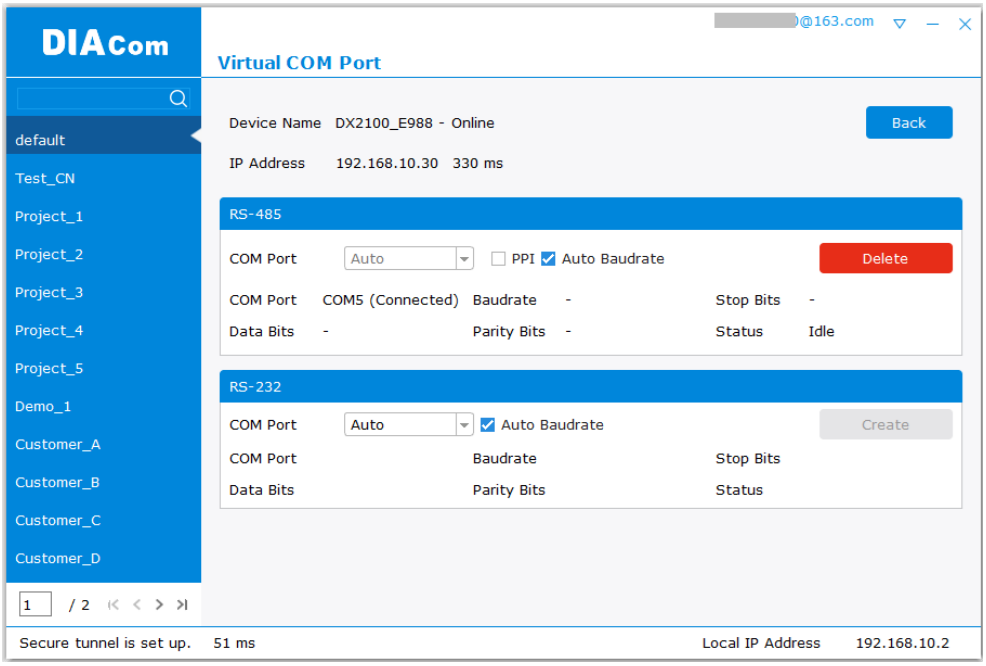
4.2.3.2 Via a RS232/RS485 Port

After opening a virtual tunnel, you will need to follow the setups below before using WPLSoft or other configuring/monitoring software on your local computer to configure and monitor the connected device remotely.

1. Click IP address in the DIACom device list or open a browser and input the IP address of the router which is connected to your remote device on the search bar and then log in.
2. Go to the System setup page, select the setup option RS232 or RS485 and input the required information to set up. Make sure the parameters are consistent with your remote device.
   - Working Mode：Transparent mode
   - Parameters of COM (Baud Rate, Data Bits, Stop Bits, Parity Bits, Flow Control)



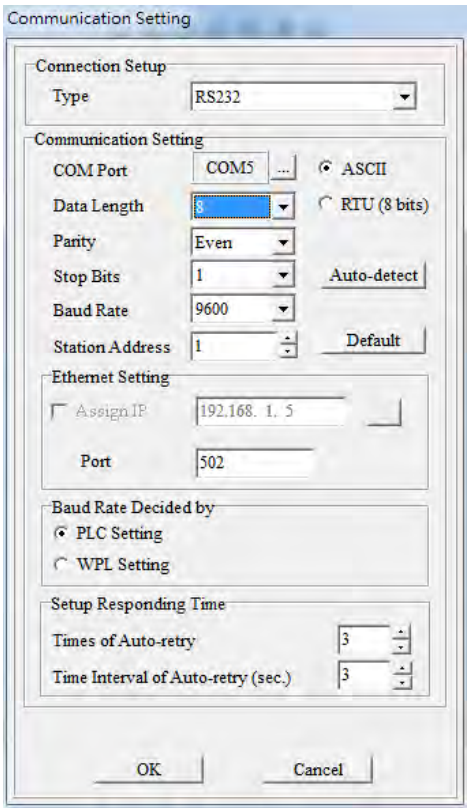
3. Go back to the DIACom and click to create a virtual tunnel. Once the creation is done, the virtual serial-port number will show up on the same page. Users can use it to configure and monitor the connected device remotely. Click “Delete” to delete the virtual serial-port.



Notice

If the PLC is Siemens S7-200, you can select the “PPI” in the DIACom to support PPI protocol.

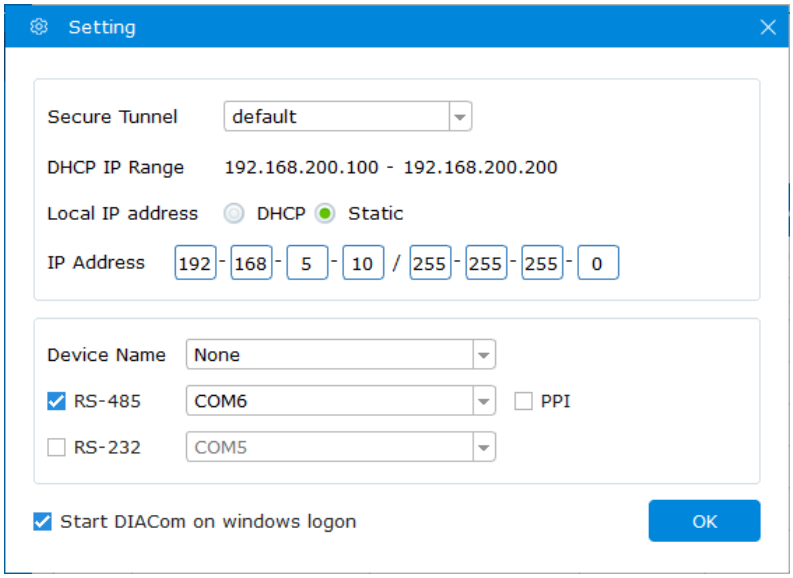
4. Open the WPLSoft to check if the COM parameters are consistent with the settings on your router. When these parameters are consistent, you can use the WPLSoft to configure/monitor your device remotely.



4.2.4 Automation Startup

Users can set Automation Startup for DIACOM, The setting steps see blow.

1. Login to DIACom.
2. Click on the icon button ▽ in the upper right corner of the windows, and select "Settings".
3. Boot automatically log in the required configuration is as follows. Users can set according to your needs. If you only need DIACom to connect the security tunnel automatically, the device list, RS-485 and RS-232 do not need to be set.



4. Check " Start DIACom on windows logon ", and click "OK" button to save the settings.

Notice

- Login must be checked "remember password", otherwise DIACom can not be activated automatically
- Confirm that the IP / Serial Port settings do not cause conflicts

5

Chapter 5 DIACloud

Table of Contents

5.1 Introduction to DIACloud 5-2

5.1.1 Select a Suitable Firmware Version 5-2

5.2 Instructions for DIACloud 5-2

5.2.1 Register and Login 5-2
5.2.2 Home 5-4
5.2.3 Devices 5-6
5.2.4 Alarm 5-16
5.2.5 Secure Tunnels 5-16
5.2.6 Sub Users 5-18
5.2.7 Logs 5-21
5.2.8 Orders 5-22
5.2.9 Profile 5-23

5.1 Introduction to DIACloud

DIACloud Web is a web portal of DIACloud cloud platform. Users can check the status of connected industrial device through DIACloud Web, browse data that has been collected, receive warnings, notices and other messages that are sent by cloud platform, create and manage sub-account and virtual safety network and check login and interface logging, to improve the manageability of devices, optimize the device performance and efficiency, save the operation cost and enhance the service quality.

5.1.1 Select a Suitable Firmware Version

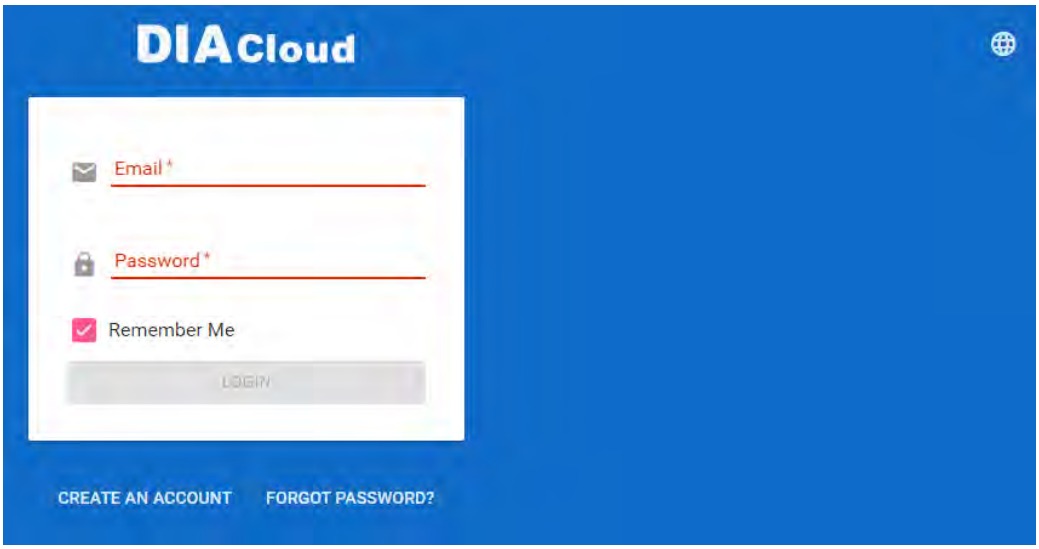
Please confirm that your Firmware version of router meets the requirements in the following table before use:

Device Model	Firmware Version
DX-2100	V1.3.0.1 or above
DX-2300	V1.0.0.1 or above

5.2 Instructions for DIACloud

5.2.1 Register and Login

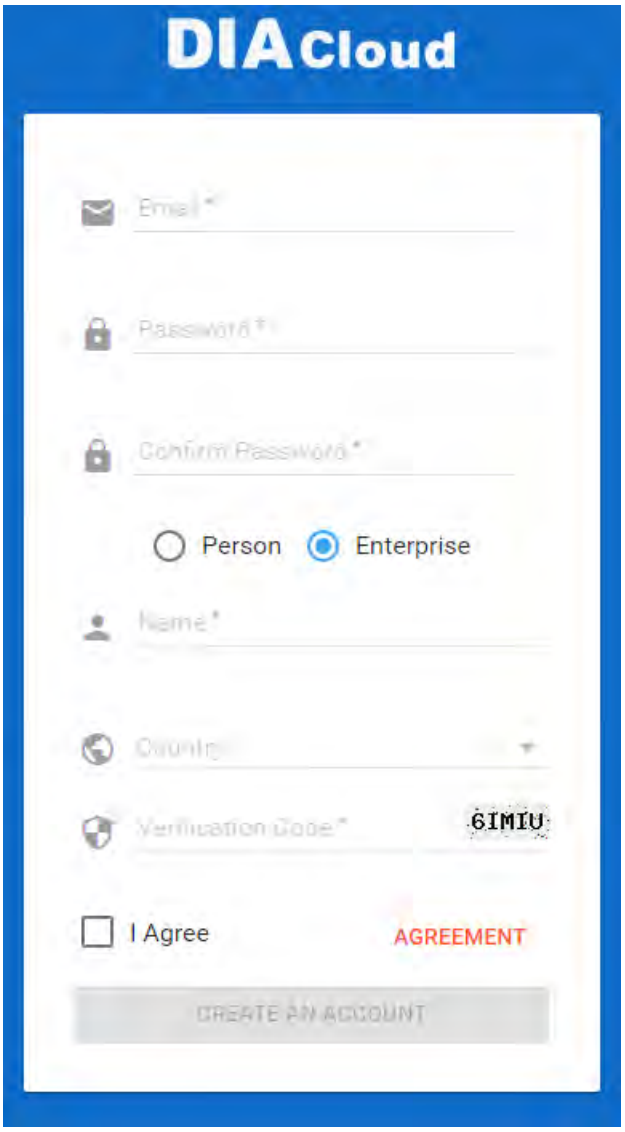
1. Open the DIACloud web page (http://www.DIACloudSolutions.com). If you have got an account, input your account and password in the following page to log in; if you have not got an account, click “CREAT AN COUNT” to register. Then the system will redirect you to the registration page:



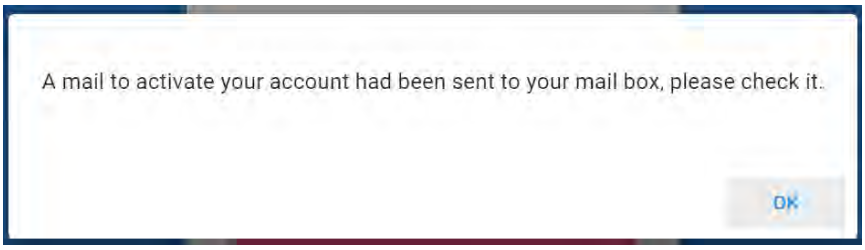
2. Input your email address, password and other relevant information on the registration page. Select “I Agree” and click “CREATE AN ACCOUNT”. Please insure your region information is correct, otherwise it may cause problems in payment when you extend your service.

Notice

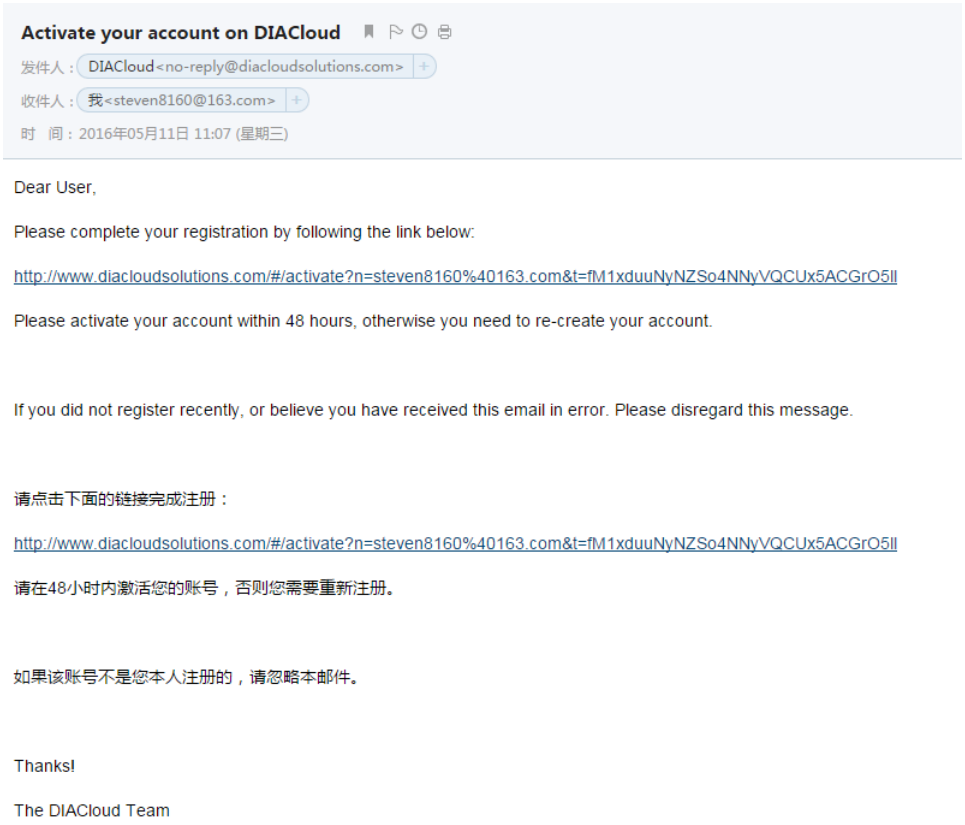
Click at the upper right corner to change the interface language to English or Chinese.



3. After clicking “CREATE AN ACCOUNT”, a congratulation page will be prompted and an activation email will be sent to the email address you have used as your DIACloud account.



4. You will find an activation email sent from no-reply@DIACloudSolutions.com in your email box. Open the email, click the link in the email and complete DIACloud account activation operation. And you will be redirected to the DIACloud login page. Input your account and password to log in to the DIACloud.



Activate your account on DIACloud

发件人：DIACloud<no-reply@diacloudsolutions.com>

收件人：我<steven8160@163.com>

时　间：2016年05月11日 11:07 (星期三)

Dear User,

Please complete your registration by following the link below:

http://www.diacloudsolutions.com/#/activate?n=steven8160%40163.com&t=fM1xduuNyNZSo4NNyVQCUx5ACGrO5ll

Please activate your account within 48 hours, otherwise you need to re-create your account.

If you did not register recently, or believe you have received this email in error. Please disregard this message.

请点击下面的链接完成注册：

http://www.diacloudsolutions.com/#/activate?n=steven8160%40163.com&t=fM1xduuNyNZSo4NNyVQCUx5ACGrO5ll

请在48小时内激活您的账号，否则您需要重新注册。

如果该账号不是您本人注册的，请忽略本邮件。

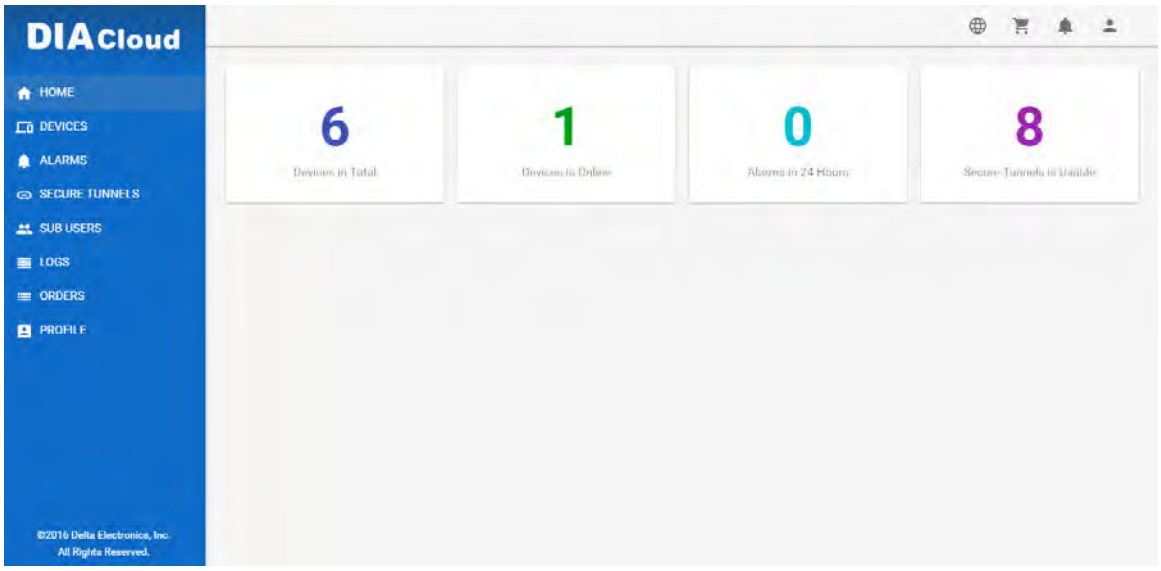
Thanks!

The DIACloud Team

5. Open the DIACloud web page (http://www.DIACloudSolutions.com). Log in using your account that you have registered.

5.2.2 Home

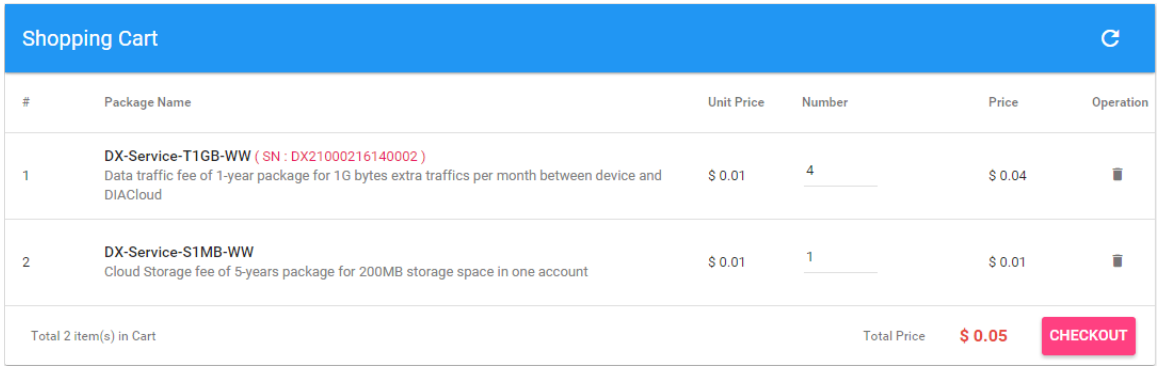
The Home Page will show up after login.



Item	Description
Menu	User can switch to corresponding function through menu on the left.
Devices Total	The number of total devices.
Devices is Online	The number of total online devices.
Alarms in 24 Hours	The number of alarms in Recently 24 hours.
Secure Tunnel is Usable	It will show the number of Secure Tunnel groups under the account.
	Switch between Chinese and English
	Show the service package you selected, users can add package to shopping cart through Devices function and Profile function.
	Show the alarm message(s) in latest 7 days
	Show the profile or logout

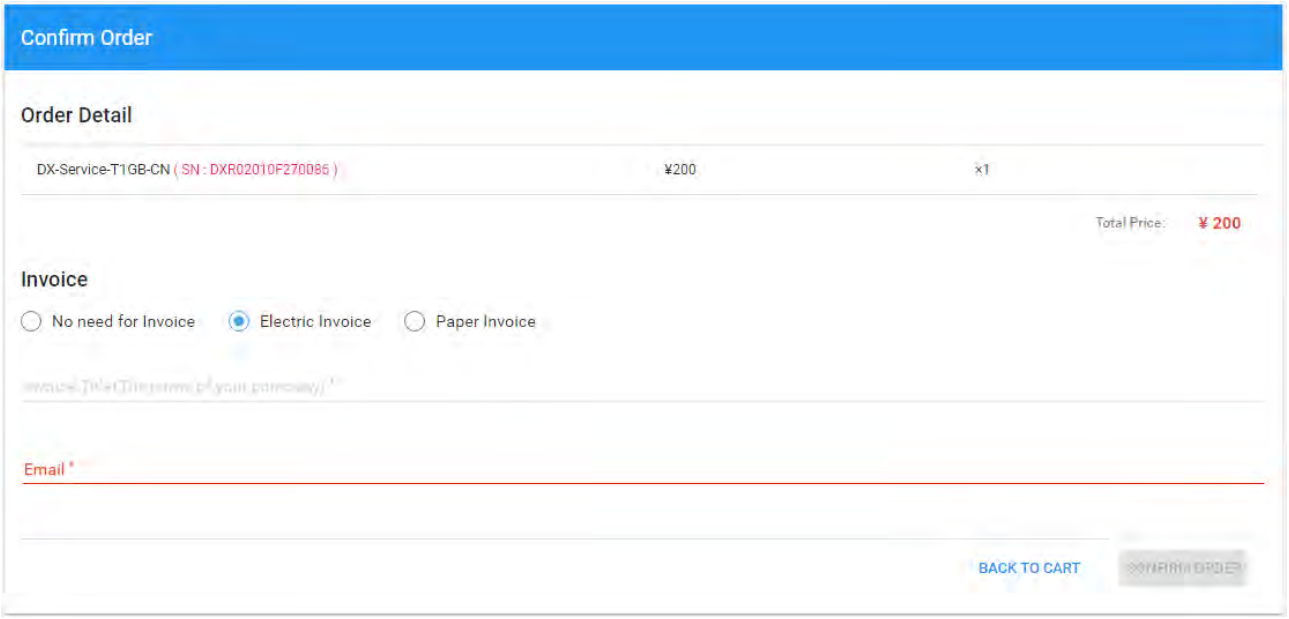
Online payment process as below:

1. After click , it will show the detail information in shopping cart.

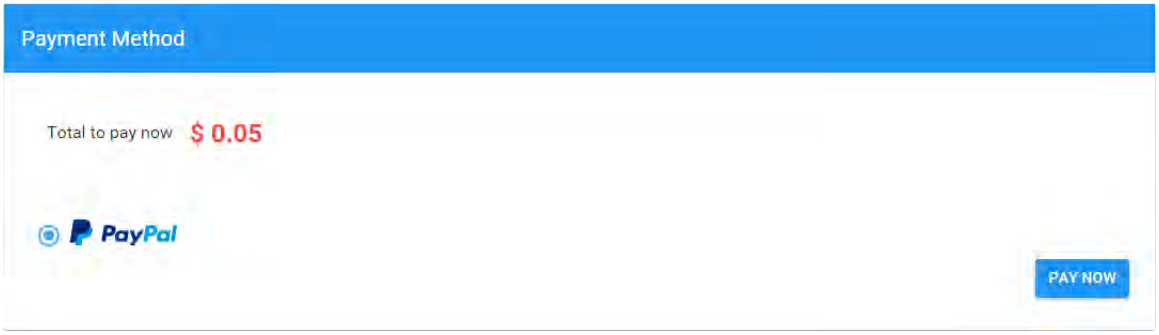


2. Click to generate an order. DIACloud provides the follow types of invoices.

- No need For Invoice
- Electric Invoice
- Paper Invoice



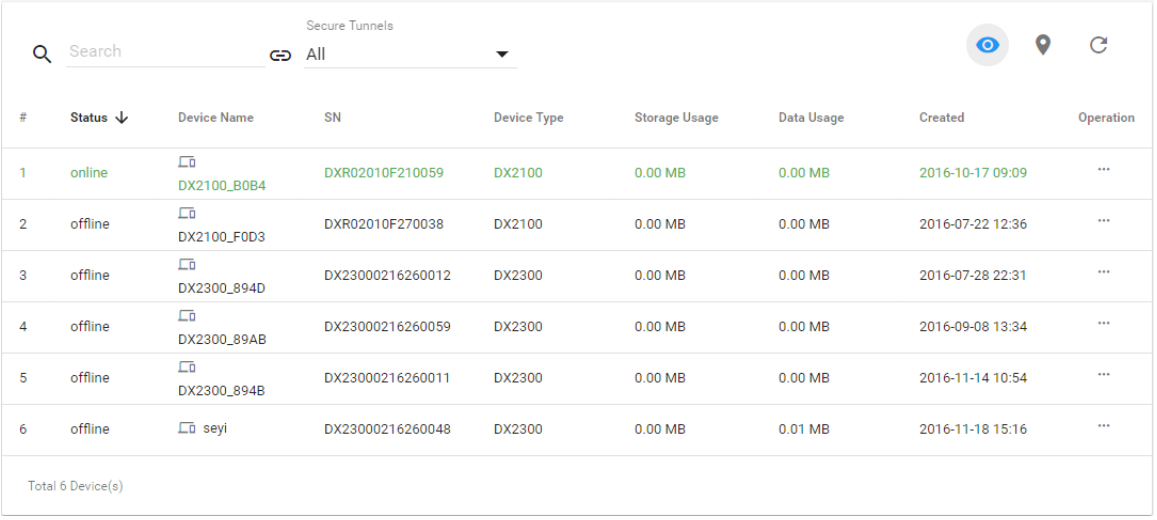
3. Click CONFIRM ORDER, we accept PayPal payments and process credit cards on your order forms.



5

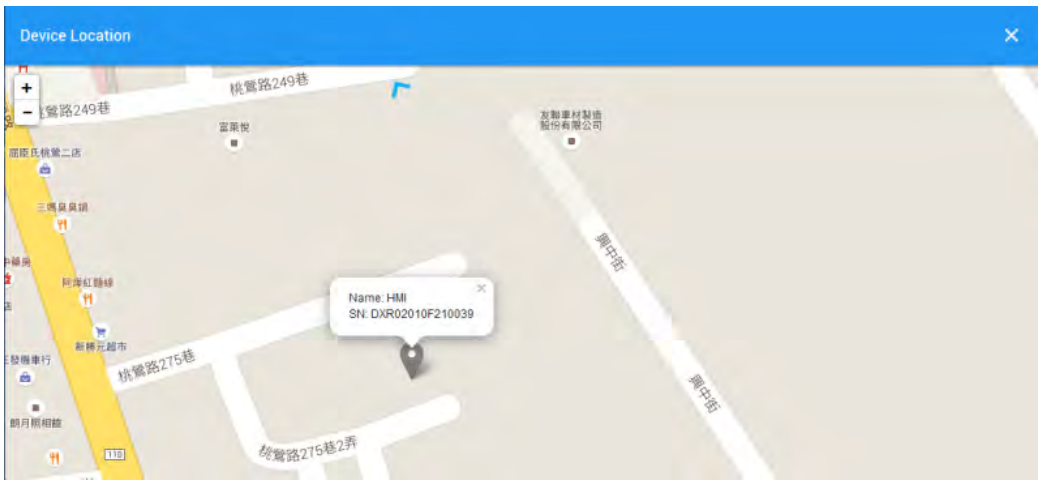
5.2.3 Devices

It will switch to page of device list after clicking “Devices” in navigation bar.



Item	Description
Search	You can filter the device base on you input the key word of the device name.
All	Filter base on tunnel group, show all devices or only show the devices under user specified tunnel group.
Devices List	Show the list of device.The information includes device's name, device's SN, device's type, storage usage, data usage and the time of binding device. • Green represents that the device is online • Gray represents the device is offline.
	• : Represents that all device is displayed currently, and you can switch to on-line device list after clicking this icon. • : Represents that on-line device is displayed currently, and you can switch to list of on-line device after clicking this icon.
	Show relevant position information of the device.
	Refresh pages
...	Show detail information of the device

- : It will show relevant position information of the device after you click " " , which is shown as follows:



It will show the device name and SN of the device after clicking position icon in the map. When a large number of devices bound to the user's account, it will switch to other corresponding devices when user clicks blue arrows at the edge of the map.

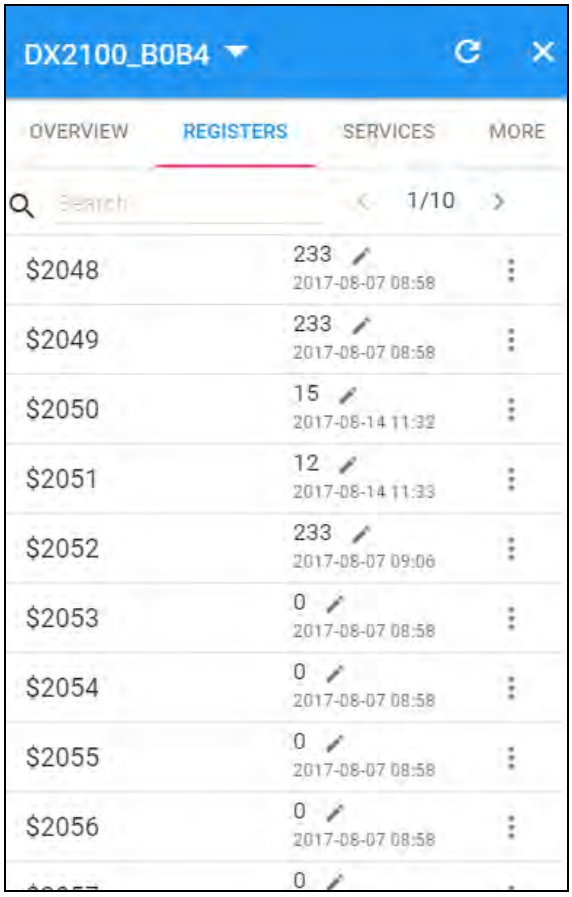
- ... : More detail information about the device will be shown after clicking ... under the "Operation" on the right side of the device list:

1. **OVERVIEW:** The page will show the basic information of the device and the latest alarm message.

Item	Description
Operation zone of device	It represents that device is online if background color is blue, and device is offline if shows gray. • DX2100_B0B4 : Show device names; it can switch device after clicking the drop down arrow. • : Realize refresh of device data on operation page. • : Close the operation page.
Page switching	Operation is divided into 4 pages: • Overview • Registers • Package • More Different buttons are used to switch different pagers.
Basic information zone	Basic information is shown in Overview page. • **IP Address:** IP address of a device; • **Tunnel Network:** it means virtual network that has been bound to device; • **Boot Time:** it means the boot time of device; • **RS232 Mode:** work modes of RS232, including transparent transmission mode and slave station mode; • **RS485** Mode: work modes of RS 485, including transparent transmission mode, slave station mode and master station mode;

	• **Modbus TCP:** work modes of Modbus TCP, including Modbus TCP Server，Modbus TCP Client and Closed • **RSSI:** it means signal strength of device which contains 5 bars; the larger the number of green bars is, the stronger the signal strength is;
Latest Alarms	The latest five Alarm of the current device. “ ” represents the state that the email has been sent; • **Green** represents that the email has been sent successfully • **Red** represents failure of sending.

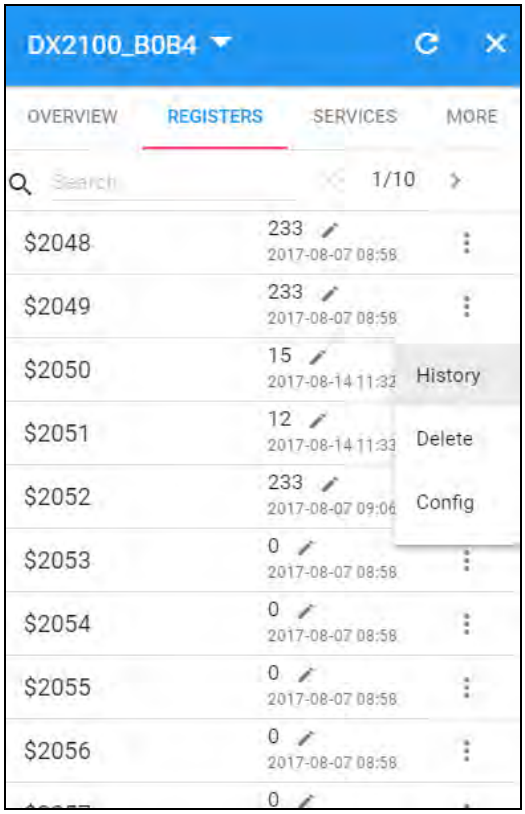
2. **REGISTER:** The page will show and manage register value that uploaded from DX devices.



Item	Description
Search	The filtering function displays a list of keywords that match specific registers.
	Click and add the corresponding register and register value, then click “SAVE” button. DIACloud server will send the corresponding data to the device.
1/205	“<” Pervious page · “>” Next page · “1/205” show the current page of register table and the total amount of register table page.

Register Table	Show the register table, displaying a maximum of 10 registers per page.
Register Name	Show the register name, when you do not configure an alias in the register, the register number is displayed.
Register Value	Show the current register value and data transfer time.
⋮	You can view the current register of historical data or delete the current register; it can also be configuring registers. P.S. If this register is not set to remeber history (device configuration page), the menu does not appear [History] after clicking ⋮ icon.

The History and Config options will be shown after clicking ⋮

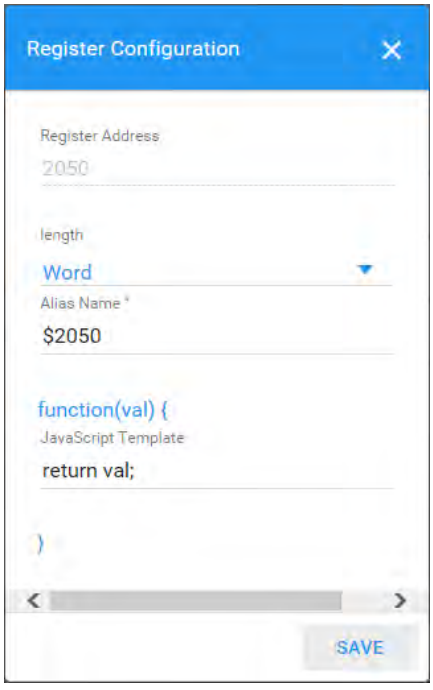


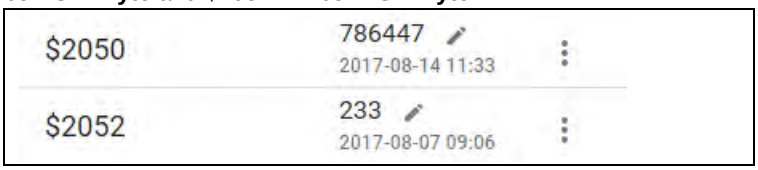
Item	Description
History	It represents trend chart of historical data
Delete	User can delete all the data of a target register.
Config	User can customize name of register and content returned.

- **History :** The following figure will be shown after clicking “History”:

Item	Description
Date Start	Set the Start Date and query the historical data for a specific time.
Date End	Set the End Date and query the historical data for a specific time.
Register Value History Diagram	The latest trend chart of value of register;
Time Axis	Users can change time scope of historical data by sliding "".
	Export the data to XLS.file.

- **Config :** The following information will be shown after clicking "Config"

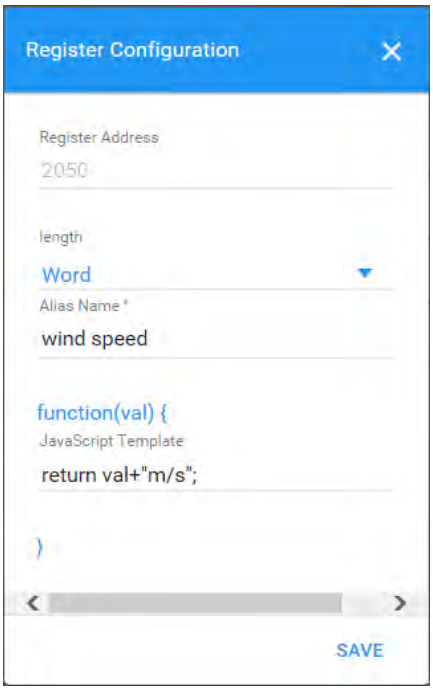


Item	Description
Length	Length can be set to Word, DWord and Float. • **DWord:** DWord needs to use two DX internal registers. For example: $2050 and $2051 are set to DWord and combined as one. $2050 will be **LOW Byte** and $2051 will be **HIGH Byte.**  • **Float:** Float needs to use two DX internal registers. For example: $2050 and $2051 are set to DWord and combined as one. $2050 will be **LOW Byte** and $2051 will be **HIGH Byte.**
Alias Name	Users can set the display name of the register in "Alias Name"
function(val)	function(val) is used for converting register values and similar to the grammar of function-supported JavaScript.

There are two examples for “function (val)”.

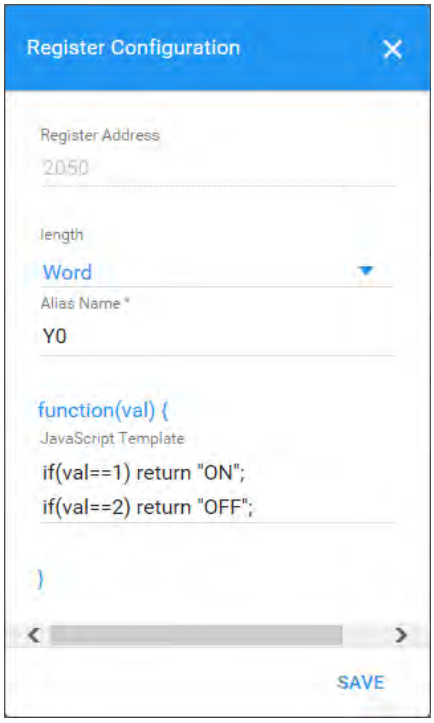
- **Example 1** : If you want to show the wind speed as 10m/s. (Data +unit, such as: speed 10m/s).

  Input the code: **return val+“m/s”** in function (val){…} as the following picture and save the configuration.

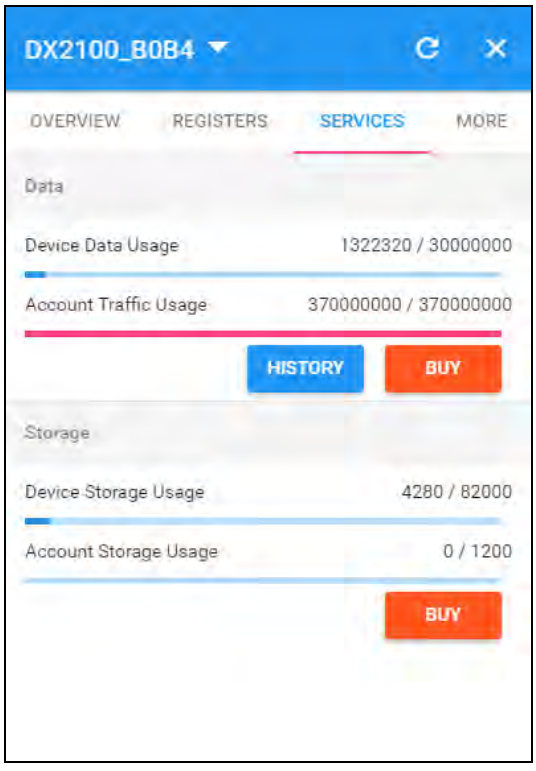


- **Example 2**: If you want to convert the register value to the text such as the register value of 1 showing the text as 'NO'; register value of 2 showing the text as 'OFF'

  Input the code in function (val) {…} as the following picture and Click "Save" botton.



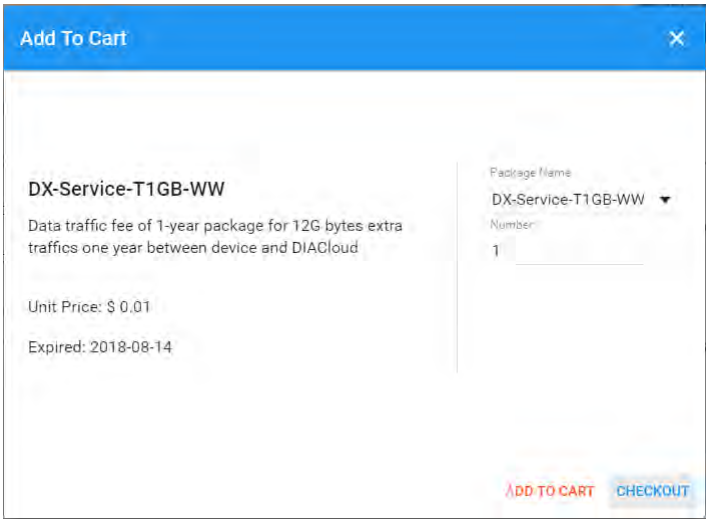
3. **SERVICES:** This page shows the Device Data Usage, Device Storage Usage and Account Storage Usage for users.



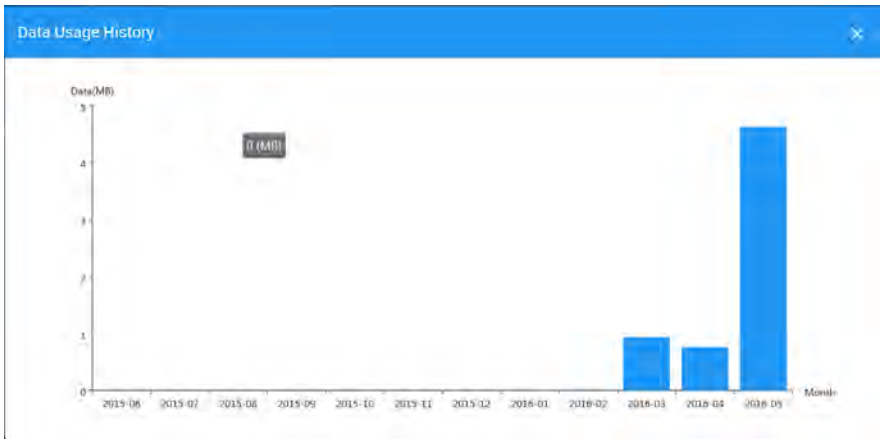
Item	Description
Data	• **Device Data Usage:** Show device traffic usage till now and total capacity. • **Account Traffic Usage:** 1. Account traffic is the total amount of traffic showing additional purchases. 2. Account traffic can be shared with all devices under your account. 3. Before the device traffic is exhausted clould traffic, the account traffic will not be used. • BUY: User can purchase more traffic package for this accoount if need. After successful payment, the moment is ready for use. • HISTORY: Show the Data Usage History in past 12 months.
Storage	• **Device Storage Usage:** Show device storage usage till now and total capacity. • **Account Storage Usage:** 1. Account storage is the total amount of traffic showing additional purchases. 2. Account storage can be shared with all devices under your account. 3. Before the device storage is exhausted strorage space, the account storage will not be used. • BUY: User can purchase more traffic package for this accoount if need. After successful payment, the moment is ready for use.

5

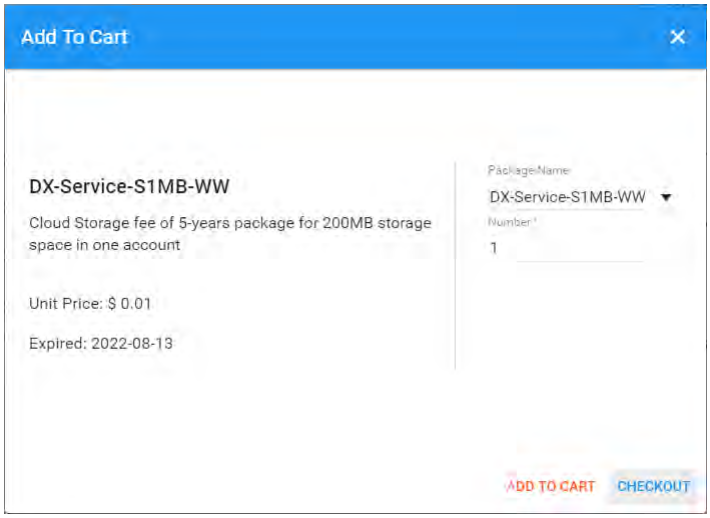
- After Click the BUY in Data field, it will show the traffic package select page. User can add a package to cart or checkout directly.



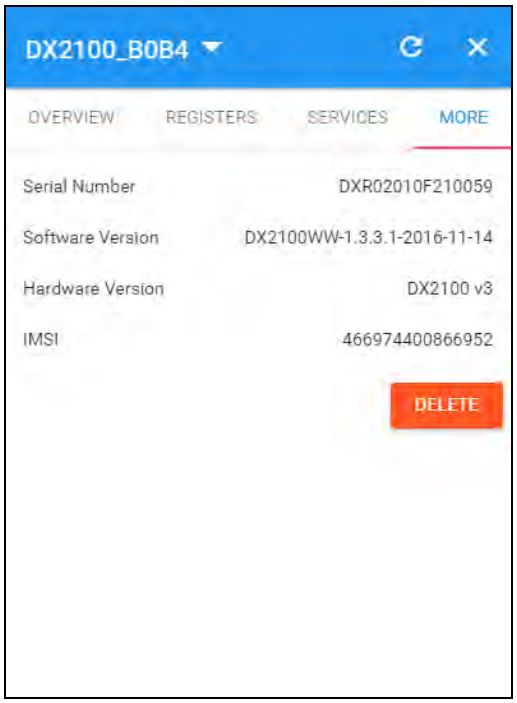
- After Click the HISTORY, it will show the Data Usage History in past 12 months.



- After Click the BUY in Storage field, it will show the storage package select page. User can add a package to cart or checkout directly.



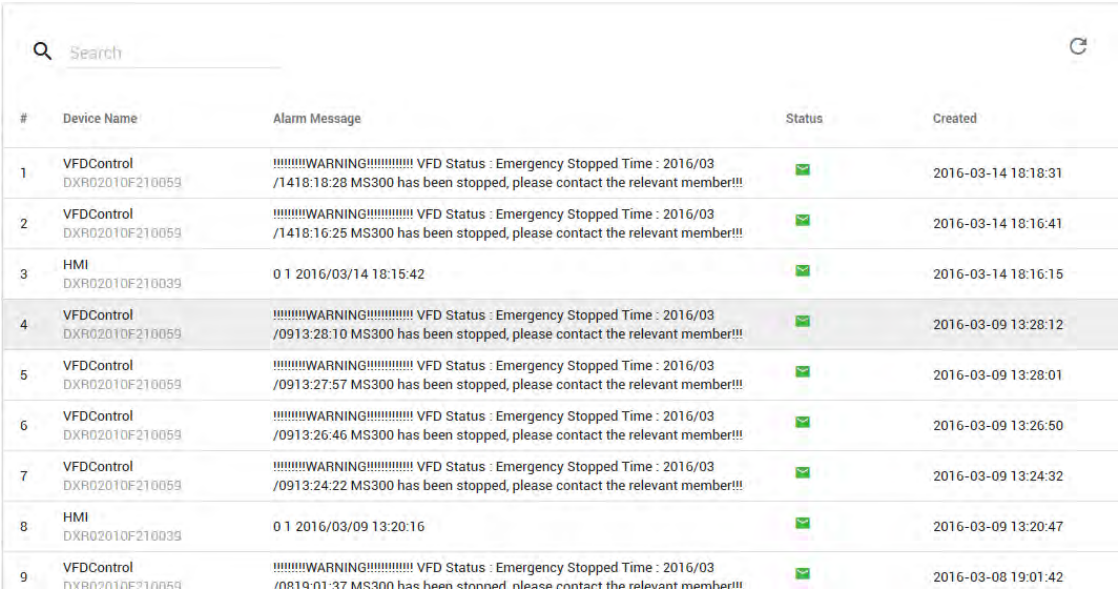
4. **MORE:** This page will show the Serial Number, Software Version, Hardware Version, and IMEI for users.



Item	Description
Serial Number	Serial number of device
Software Version	Version information of software
Hardware Version	Version information of hardware
IMSI	International Mobile Subscriber Identification Number.
DELETE	Delete binding relationship between devices and the account. Devices need to be un-bund after clicking this button, and users can recover the device by rebinding.

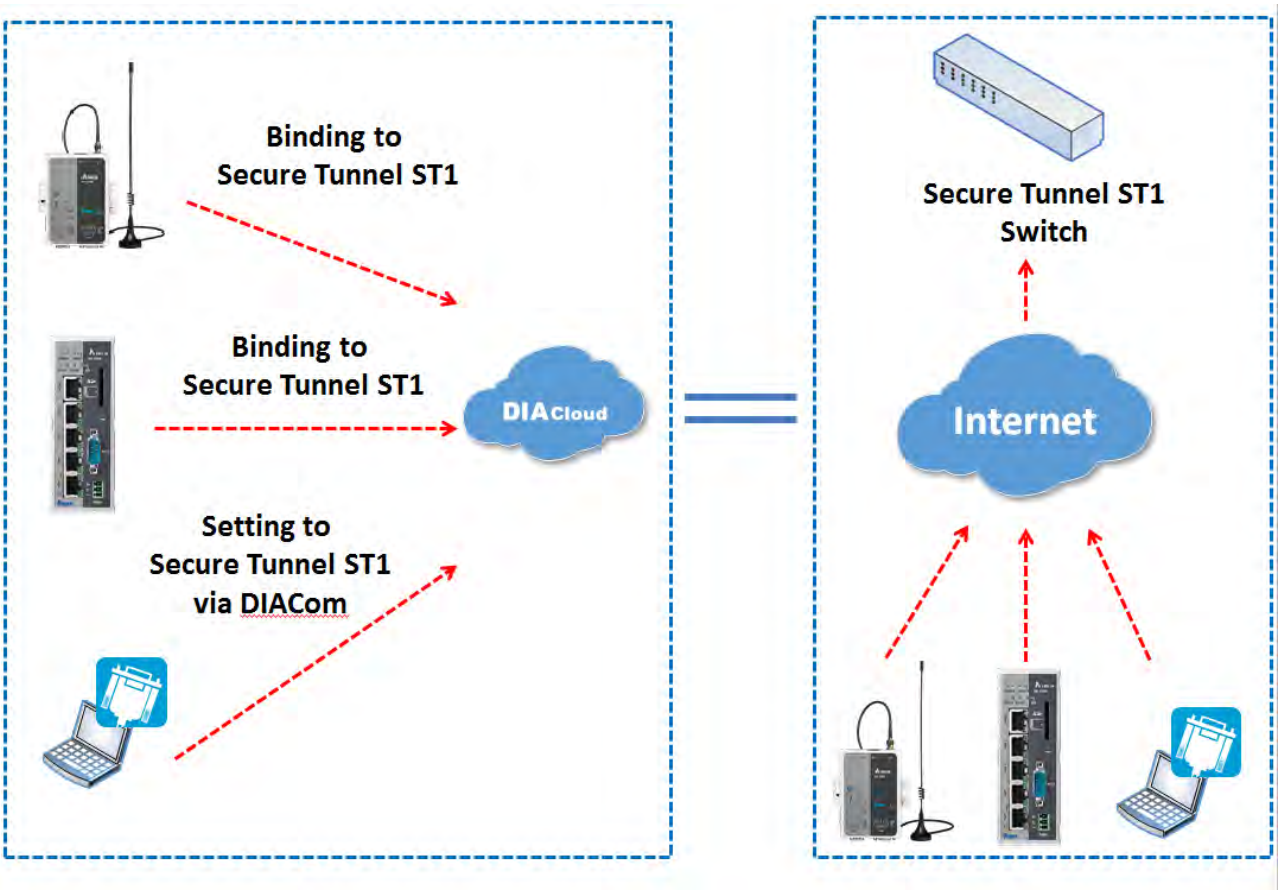
5.2.4 Alarm

Click the Alarm in the left menu. The warning information in the latest 7 days will be shown in this page. The warning information includes name and serial number of device, content of warning, status of email that is being sent (green“ ” represents that the email has been sent successfully, and red represents fail.), time of warning and content record of warning.

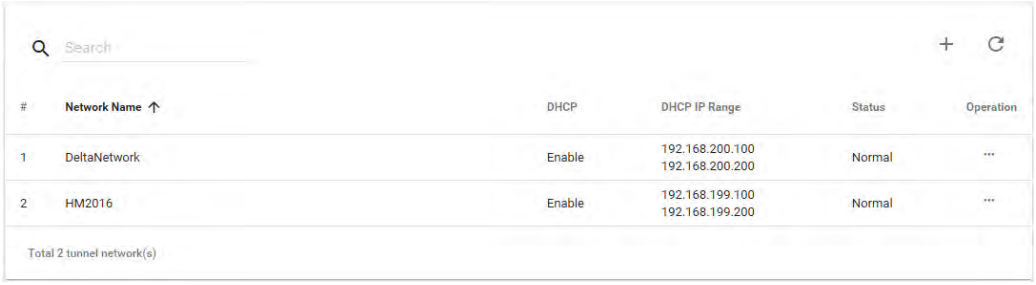


5.2.5 Secure Tunnels

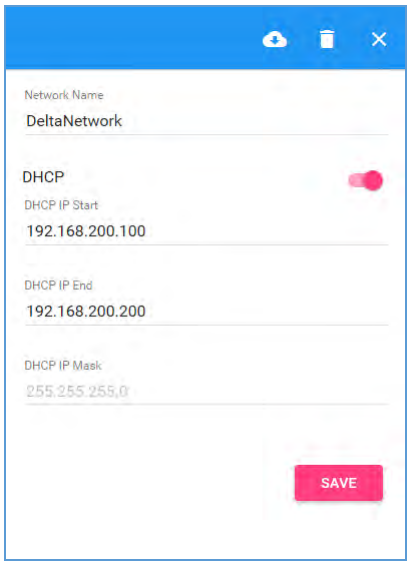
Secure Tunnel is an important concept in DIACloud. Its objective is to realize virtual Switch across Internet; when device is bound to this network, it will be equivalent to add devices with one LAN port; when PC operates DIACom and creates a virtual network, PC and the device will be under the same switch at this time. It is shown as follows



Users can manager the tunnel network in this page. Interface is shown as follows:



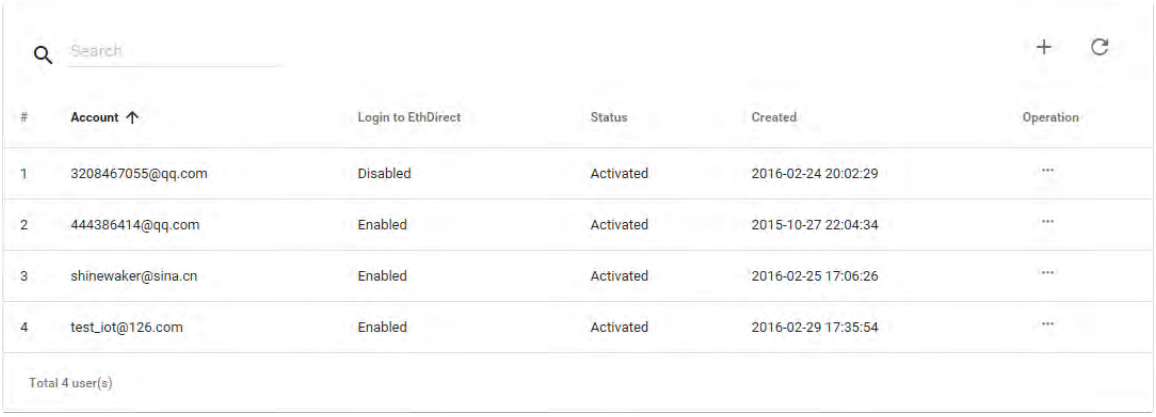
tem	Description
Search	Search the existed tunnel network.
Tunnel network List	List all tunnel network under this account.
+	Add a new tunnel network.
↻	Refresh the tunnel network list.
···	Edit the tunnel network.



Item	Description
Tunnel Network Information	The detail information of tunnel network: • **Network Name:** User can enter a name of tunnel network. • **DHCP Option:** Automatic IP Address Assignment by DIACloud. • **DHCP IP Start:** it represents the beginning IP in automatic IP distribution address pool of DIACloud • **DHCP IP End:** it represents the ending IP in automatic IP distribution address pool of DIACloud.
	If the DHCP of thes tunnel network is enabled, click will export configurations include DIACloud Servier /account /Tunnel networks info to a file (default file name Provision_vlnname_date_time.bin). Note: Detail configuration, please refer to **3.2 SD Card Quick Installation.**
	Delete the current tunnel network
	Close the current operation window.
	Save the configuration of tunnel network

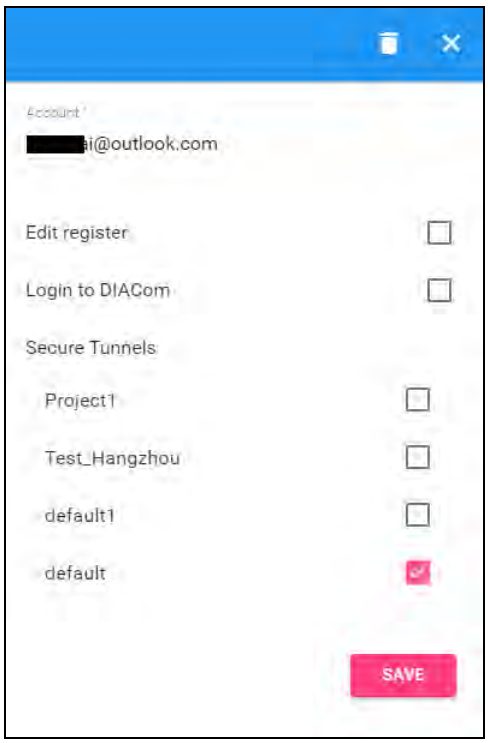
5.2.6 Sub Users

All accounts that are registered through register page of DIACloud (http://www.DIACloudSolutionscom/#/signup) are main accounts. Every main account can create sub-accounts, and users can realize power separation and grouping management of device by conducting authorization for virtual network and DIACom by sub-account. Use can conduct addition and operation for sub-account through the “Sub Users” page.



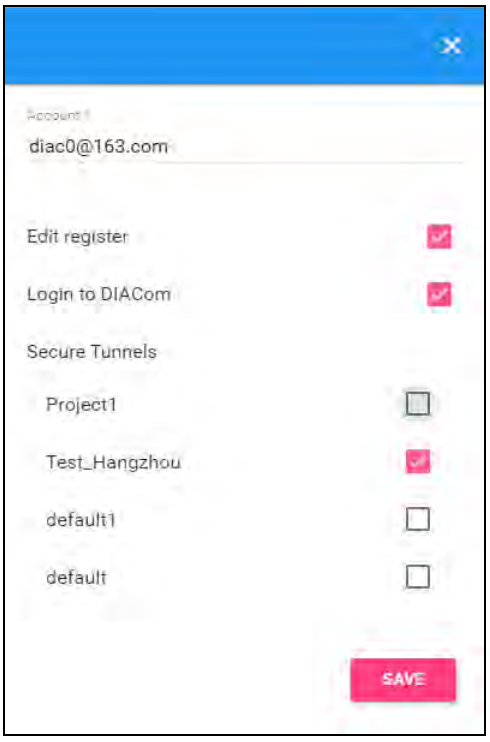
Item	Description
Search	Search the sub users.
Sub Users List	Show the list of all sub users in main account.
+	Add a sub user.
↻	Refresh the list of sub users.
···	Modify the access control of the tunnel network.

- ··· : User can modify the access control of the tunnel network.

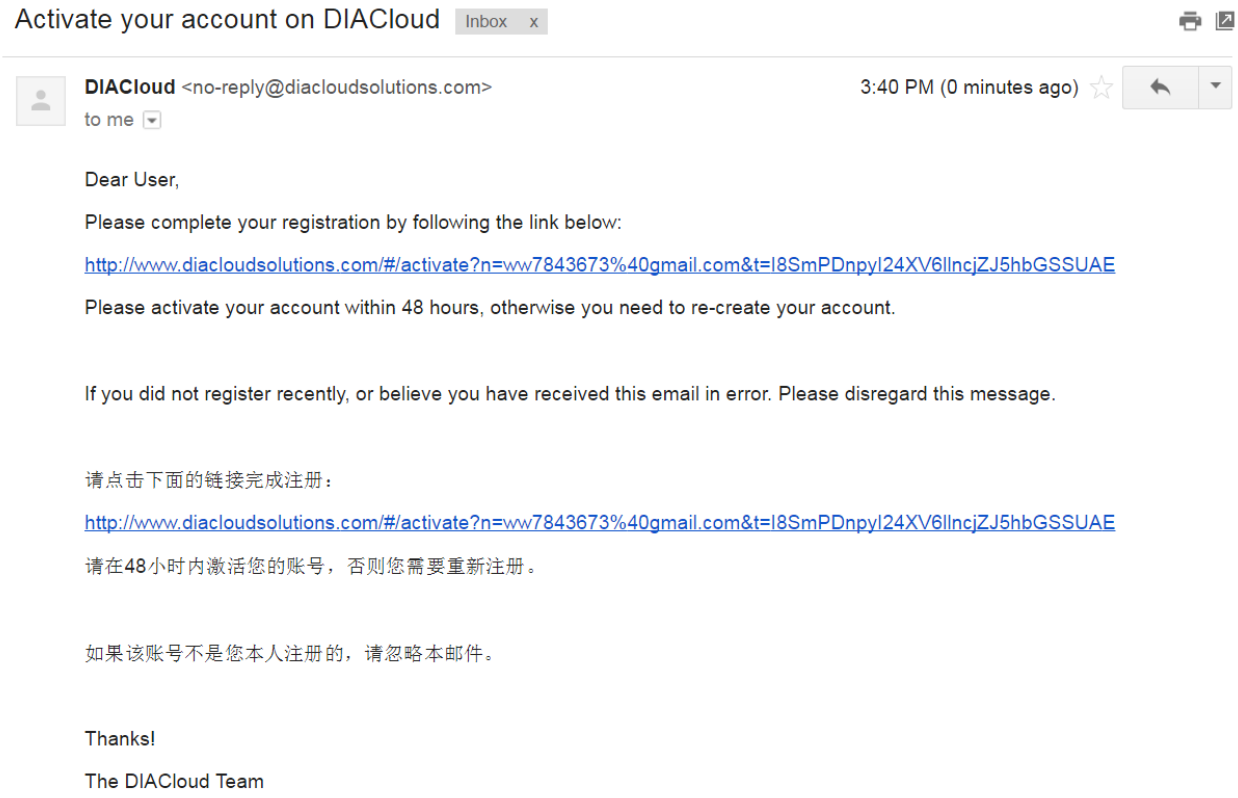


Item	Description
Sub Users Information	• **Edit register:** Allow the Sub User to modify register • **Login to DIACom:** Allow the sub user to access the DIACom if the option is enabled. • **Tunnel Network:** Allow the sub user to access the Tunnel Network if the option of Tunnel Network is checked.
	Delete a sub user.
	Close the current operation window.

- ＋ : User can add sub users after clicking the “+” on the page, and.the following interface will be shown after clicking the “+” in the page:



1. Fill in corresponding account information and conduct authorization for it.
2. The system will send an activation email which is attached with random login password to email box of sub user. The account status is “Un-activated” now.
3. Go to the mailbox, click the hyperlink to complete account activation operation, then sub user can login DIACloud with new account.
4. The page will link to the following page after clicking the activation link in the email:



Activate your account on DIACloud Inbox x

DIACloud <no-reply@diacloudsolutions.com> 3:40 PM (0 minutes ago)

to me

Dear User,

Please complete your registration by following the link below:

http://www.diacloudsolutions.com/#/activate?n=ww7843673%40gmail.com&t=I8SmPDnpyI24XV6lIncjZJ5hbGSSUAE

Please activate your account within 48 hours, otherwise you need to re-create your account.

If you did not register recently, or believe you have received this email in error. Please disregard this message.

请点击下面的链接完成注册：

http://www.diacloudsolutions.com/#/activate?n=ww7843673%40gmail.com&t=I8SmPDnpyI24XV6lIncjZJ5hbGSSUAE

请在48小时内激活您的账号，否则您需要重新注册。

如果该账号不是您本人注册的，请忽略本邮件。

Thanks!

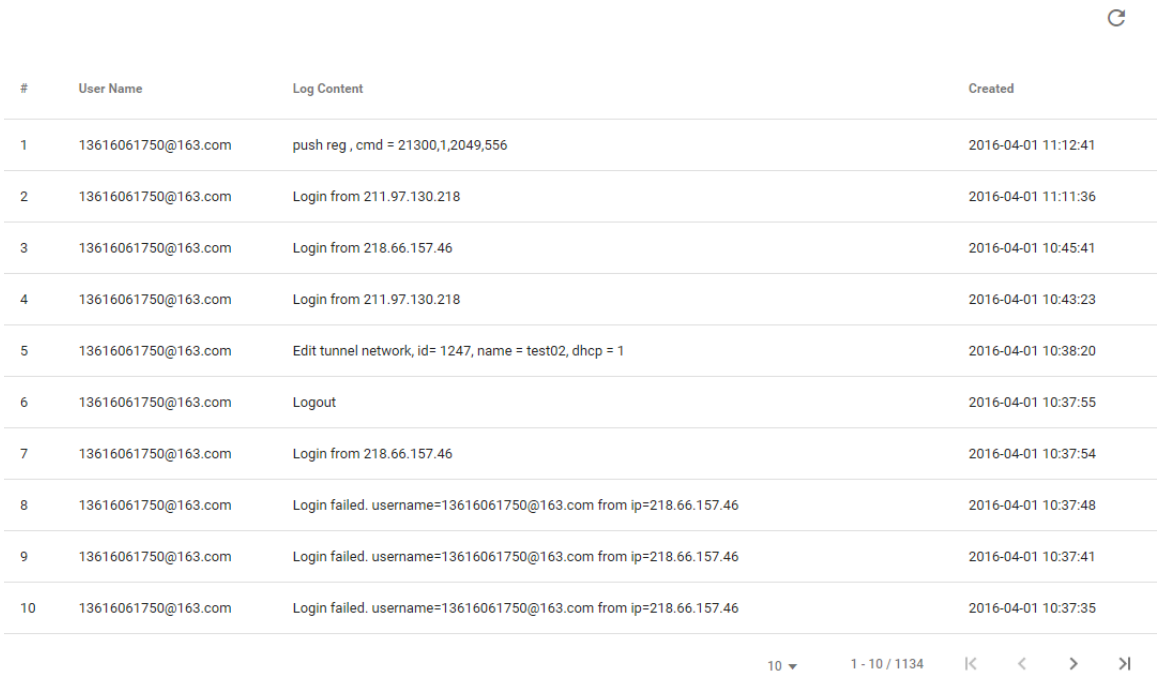
The DIACloud Team

5

5. When user login to DIACloud with main account and the sub user that we created has been activated.

5.2.7 Logs

This page will show the web operation information of some users. It includes: login IP, setup of register, API interface call of DIACloud and other information.

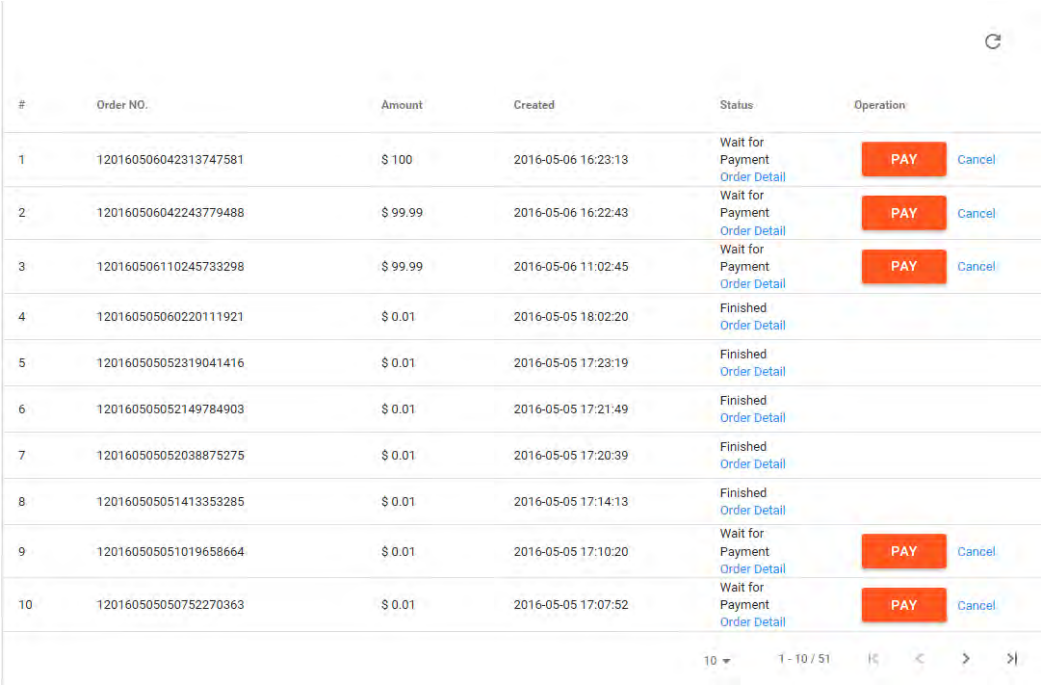


#	User Name	Log Content	Created
1	13616061750@163.com	push reg , cmd = 21300,1,2049,556	2016-04-01 11:12:41
2	13616061750@163.com	Login from 211.97.130.218	2016-04-01 11:11:36
3	13616061750@163.com	Login from 218.66.157.46	2016-04-01 10:45:41
4	13616061750@163.com	Login from 211.97.130.218	2016-04-01 10:43:23
5	13616061750@163.com	Edit tunnel network, id= 1247, name = test02, dhcp = 1	2016-04-01 10:38:20
6	13616061750@163.com	Logout	2016-04-01 10:37:55
7	13616061750@163.com	Login from 218.66.157.46	2016-04-01 10:37:54
8	13616061750@163.com	Login failed. username=13616061750@163.com from ip=218.66.157.46	2016-04-01 10:37:48
9	13616061750@163.com	Login failed. username=13616061750@163.com from ip=218.66.157.46	2016-04-01 10:37:41
10	13616061750@163.com	Login failed. username=13616061750@163.com from ip=218.66.157.46	2016-04-01 10:37:35

10 1 - 10 / 1134

5.2.8 Orders

In this page, users can check all orders. Continue to pay for the unpaid orders or cancel the unpaid orders.



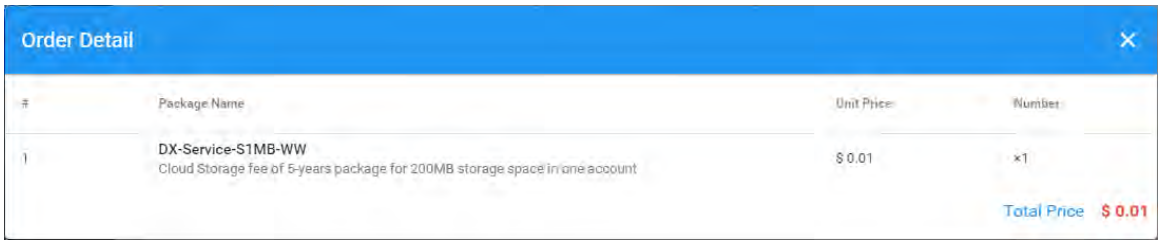
#	Order NO.	Amount	Created	Status	Operation
1	120160506042313747581	$ 100	2016-05-06 16:23:13	Wait for Payment Order Detail	PAY Cancel
2	120160506042243779488	$ 99.99	2016-05-06 16:22:43	Wait for Payment Order Detail	PAY Cancel
3	120160506110245733298	$ 99.99	2016-05-06 11:02:45	Wait for Payment Order Detail	PAY Cancel
4	120160505060220111921	$ 0.01	2016-05-05 18:02:20	Finished Order Detail	
5	120160505052319041416	$ 0.01	2016-05-05 17:23:19	Finished Order Detail	
6	120160505052149784903	$ 0.01	2016-05-05 17:21:49	Finished Order Detail	
7	120160505052038875275	$ 0.01	2016-05-05 17:20:39	Finished Order Detail	
8	120160505051413353285	$ 0.01	2016-05-05 17:14:13	Finished Order Detail	
9	120160505051019658664	$ 0.01	2016-05-05 17:10:20	Wait for Payment Order Detail	PAY Cancel
10	120160505050752270363	$ 0.01	2016-05-05 17:07:52	Wait for Payment Order Detail	PAY Cancel

10 1 - 10 / 51

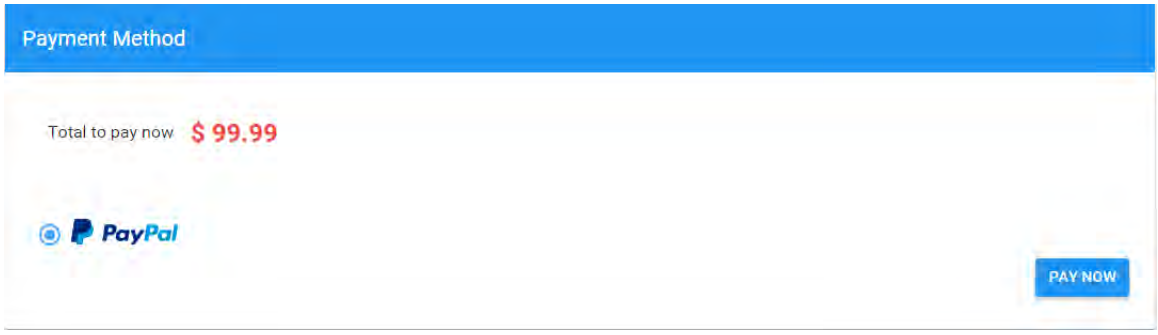
5

Item	Description
Order Detail	View the order detail information
PAY	Pay for the unpaid order
Cancel	Cancel the order, order will remove from the list.

- Order detail

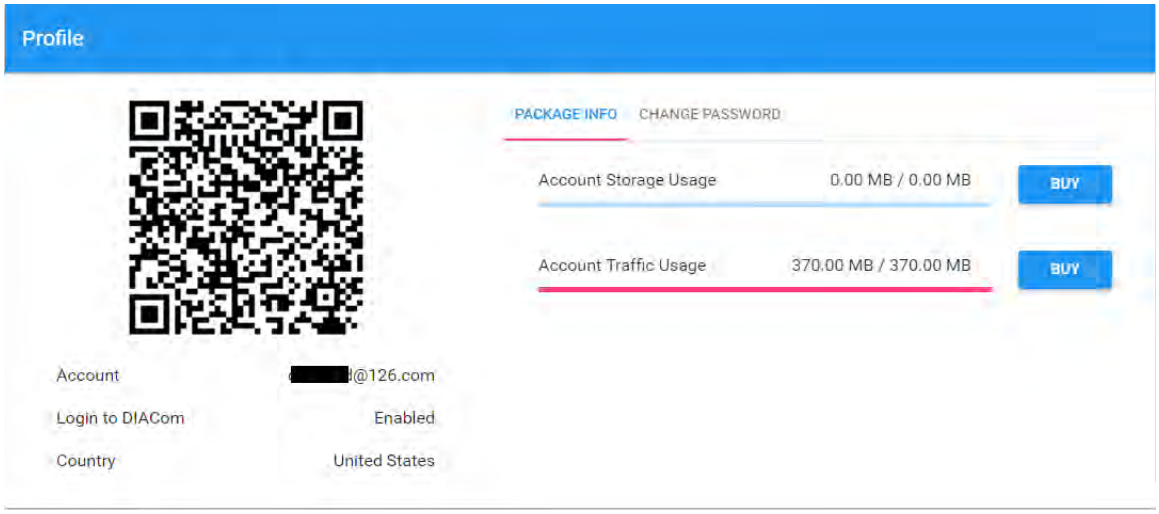


- Payment Method: Currently, we only support PayPal payment for the world wide user.



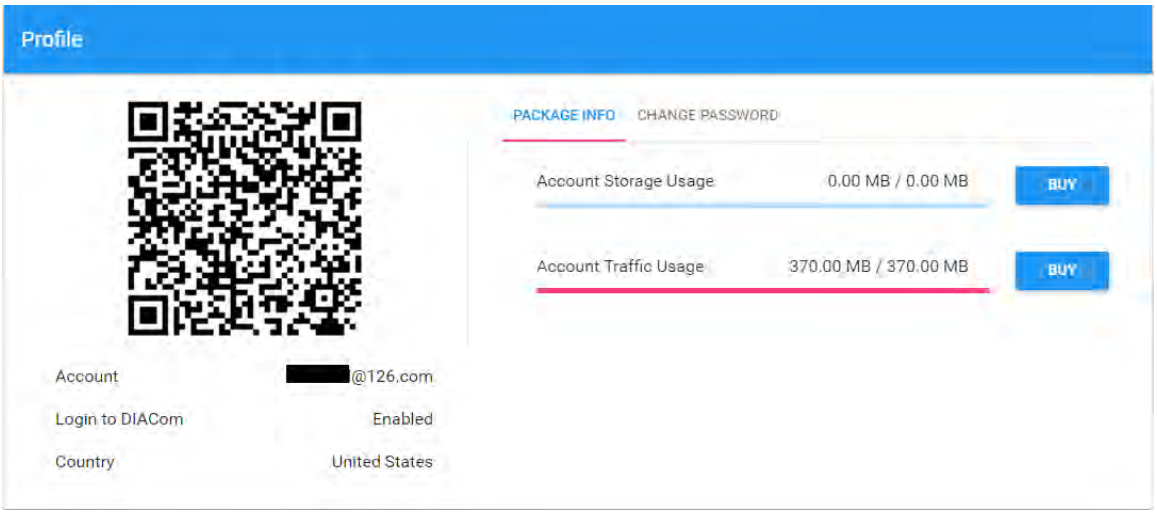
5.2.9 Profile

In this page, QR Code of user, Package info, password management and other information will be shown.



Item	Description
QR Code	You can get the part information of user by using DIACloud APP and scanning QR Code.
Account	The current account information.
Packeage info	• Show account traffic/storage usage till now • BUY Users can purchase more traffic/storage package for this account if need ⚠ Account traffic/storage will be shared to all devices under this account.
Change Password	Change the password of DIACloud user account. **Note:** parts of old users use password in 6 digits; the new password has been increased to 8 digits to improve safety of their accounts.

Change Password page as below



MEMO

6

Chapter 6 DIACloud APP

Table of Contents

6.1 Introduction to DIACloud APP 6-2

6.1.1 Select a Suitable Firmware Version 6-2

6.1.2 DIACloud APP Installation 6-2

6.2 DIACloud APP Function 6-2

6.2.1 DIACloud APP Login 6-2

6.2.2 Device List 6-4

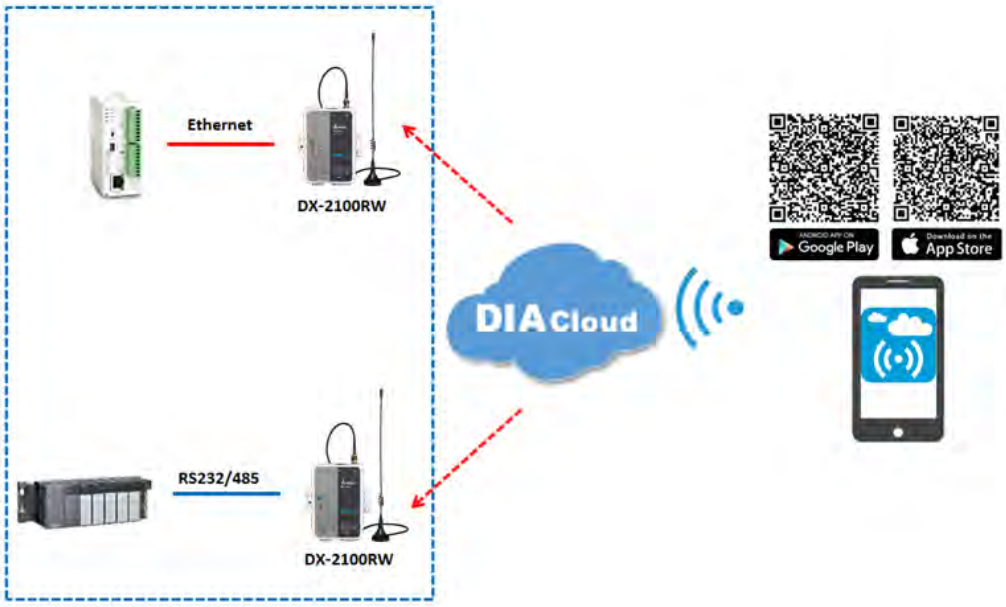
6.2.3 Device Details 6-5

6.2.4 Registers View 6-6

6.2.5 Alarm List 6-7

6.1 Introduction to DIACloud APP

DIACloud APP is the client software of DIACloud cloud platform running on mobile devices. The APP supports both iOS and Android mobile system, it enables users to view the collected field data, the locations of the field devices, and the alarms/notifications pushed by the industrial IOT cloud platform, so that keep users posted anytime and anywhere, and therefore improve the manageability of devices, optimize the device performance and efficiency, save the operation cost and enhance the service quality.



6.1.1 Select a Suitable Firmware Version

The APP can support the devices below:

Device Model	Firmware Version
DX-2100	V1.3.0.1 or above
DX-2300	V1.0.0.1 or above

6.1.2 DIACloud APP Installation

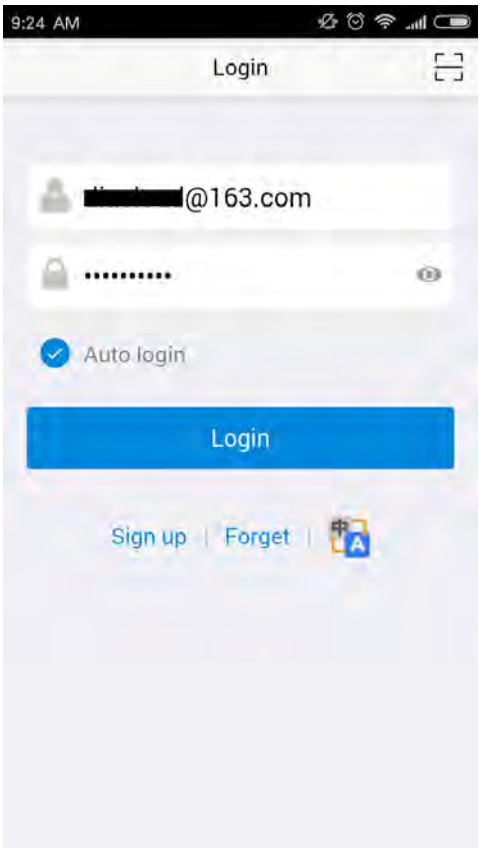
The DIACloud APP is available on Google Play and Apple APP Store.

Mobile Device	OS Version
Android	4.4.0 or above
iPhone	6.2.0 or above

6.2 DIACloud APP Function

6.2.1 DIACloud APP Login

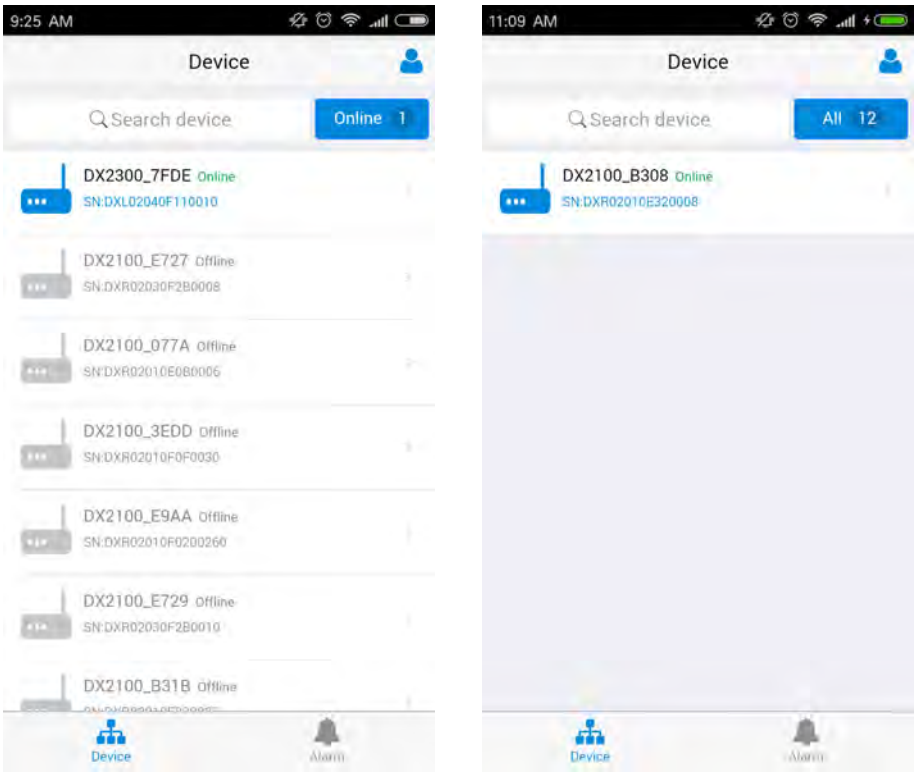
Enter the DIACloud account and password, then click the “Sign in” button to login the APP. Click the “Sign up” to register an account if you don’t have one.



Item	Description
	Scan QR code, the QR code is generated by DIACloud Web portal, which carries the user name and password information. By scanning the QR code, user won't need to input user name. By default, the APP will connect the default DIACloud server in the cloud, if the APP is to connect other servers, QR code should be scanned to provision the APP.
	DIACloud account, Email format
	The password of DIACloud account, click to see what are you input
Auto Login	Save the password and login the APP automatically
Login	Login to App
Sign up	Create a new DIACloud account
Forget	Reset the password if you forget it.
	Switch the language.

6.2.2 Device List

Device list will be shown after logging in the APP.

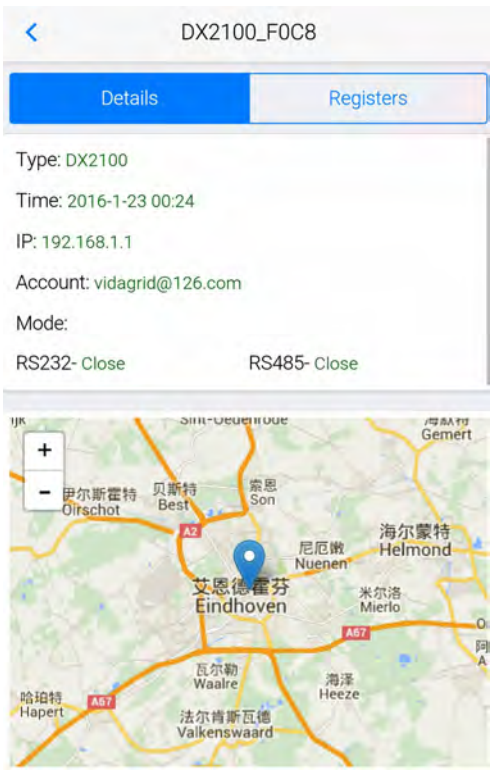


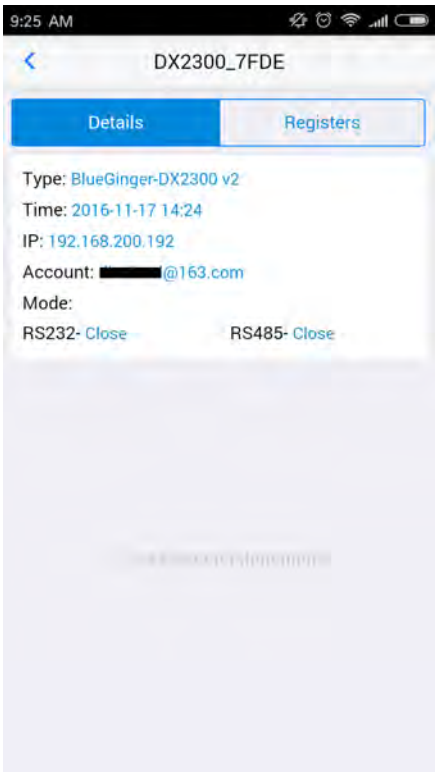
Device tab and alarm tab will be shown in the APP. In the device tab, the device information will be shown, including the value of registers of the remote device. And the value of the register can be changed in the APP as well. In the alarm tab, users can read the alarm messages.

Item	Description
	Logoff or exit App
Search	Search device base on key word
All/Online	• Click “ALL” to show all device • Click “Online” only show online device. Digit at the back is the all/online device count.
Device list	Display device online/offline status, device name, device serial number. Click it will go into device detail page
	Switch to device list page
	Switch to alarm list page.

6.2.3 Device Details

Device details will be shown by selecting a device in the device list.





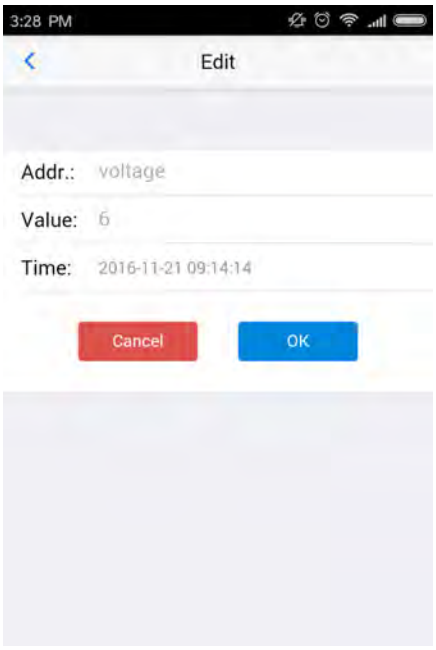
Item	Description
Type	Type of the device
Time	The time when the device is online.
IP	IP Address of the device
Account	The DIACloud account which activates the device.
Mode	The working mode of RS485 and RS232. • **RS232:** Transparent transmission mode or Slave mode • **RS485:** Transparent transmission mode /Slave mode /Master mode
Map	Showing the location of the device on the map P.S. DX-2300 Series doesn't support this function.

6.2.4 Registers View

Click [Register] on the device details page to switch to the register page

In the register page, the user can browse the collected data. The register data can be refreshed by the pull-down screen. When the number of registers is large, you can pull up the screen to display more data.

Item	Description
	Refresh the register data.
	Edit the register value.

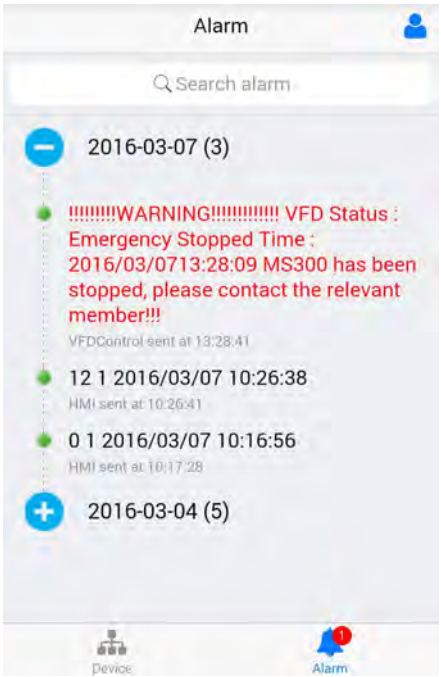


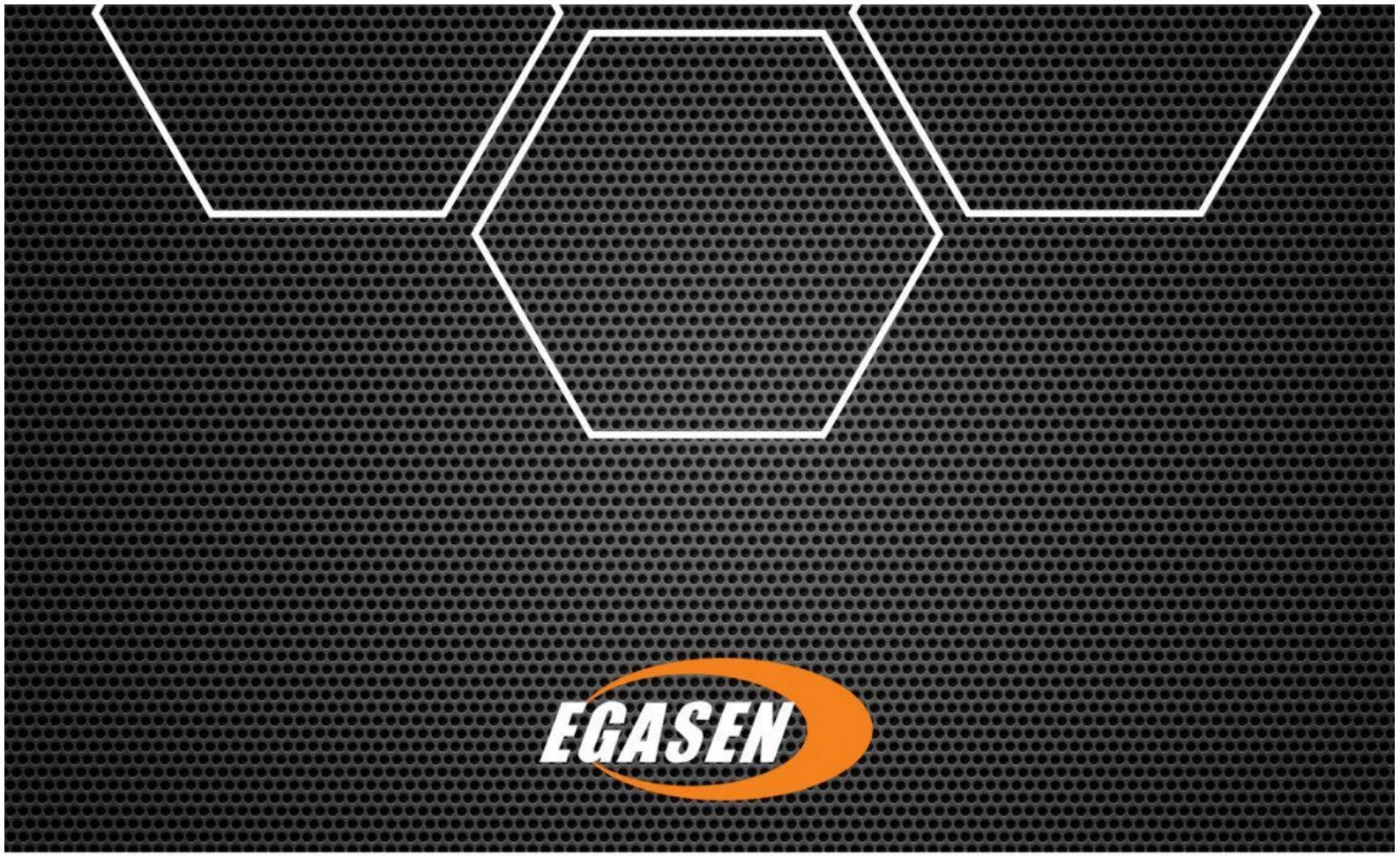
Click “ok” button, the register value will be pushed to the device.

6.2.5 Alarm List

Alarm criteria can be set on the device configuration web page. When the alarm criteria are met, the device will send out alarm messages. User can click the “Alarm” tab to read the alarm messages. When there are new alarm messages, the number of the unread messages will be shown on the icon Alarm.

- Alarm tab will be shown by clicking icon Alarm, the alarm messages in Red are unread messages. Digit in parentheses is the number of alarm messages.
- Pull down the APP to refresh the alarm list.



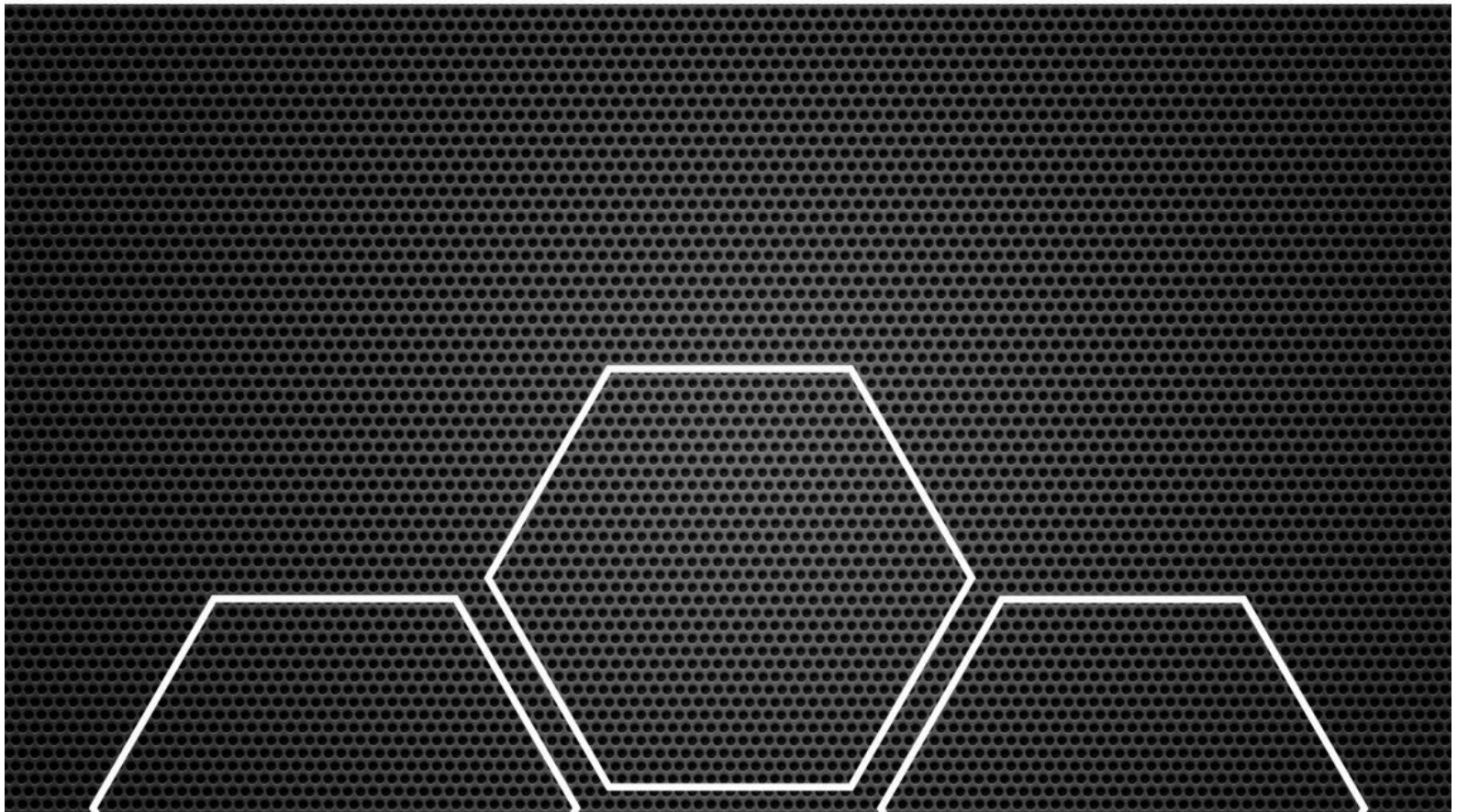


Polígono Industrial A Reigosa Parcela B-33

36828 Ponte Caldelas

Pontevedra - España

Telf. (+34) 986 872 010

E-mail: egasen@egasen.com

Web: www.egasen.com