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

Deltronics (The Netherlands) B.V.
Eindhoven Office
De Witbogt 20, 5652 AG Eindhoven, The Netherlands
TEL : +31-40-2592850 / FAX : +31-40-2592851

2016-02-03

DX-2100 Series Industrial 3G Cloud Router User Manual

www.deltaww.com

Smarter. Greener. Together.

DX-2100 Series Industrial 3G Cloud Router

User Manual

Table of Contents

Chapter 5 DIACloud

Chapter 6 DIACloud APP

1

Chapter 1 Product Introduction

Table of Contents

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

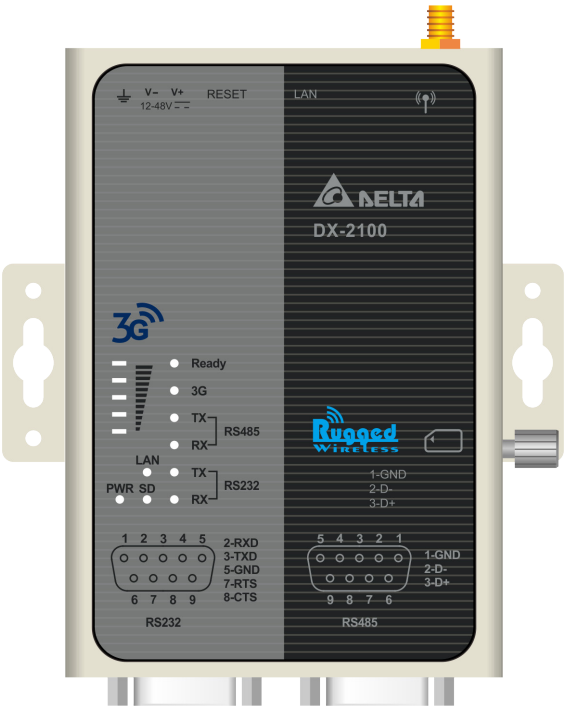
To the maximum extent permitted by law and regardless DELTA be aware or has been advised of the possibility of these damages, DELTA is not liable to any user or anyone else for: (a) any loss of use, data, reputation, goodwill, credit, opportunity, economy or profits, whether or not foreseeable; (b) any 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.

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.

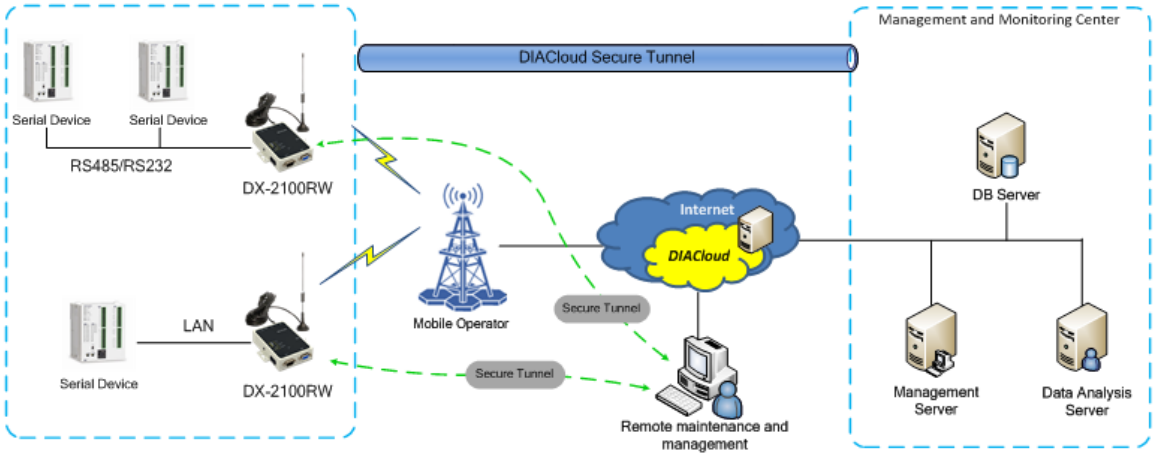
The product supports DIACloud platform services, and by this platform, convenient and efficient point-to-point connection with the router, safe and reliable data transmission, remote device management and configuration, remote firmware upgrading, remote maintenance and other functions can be realized, 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

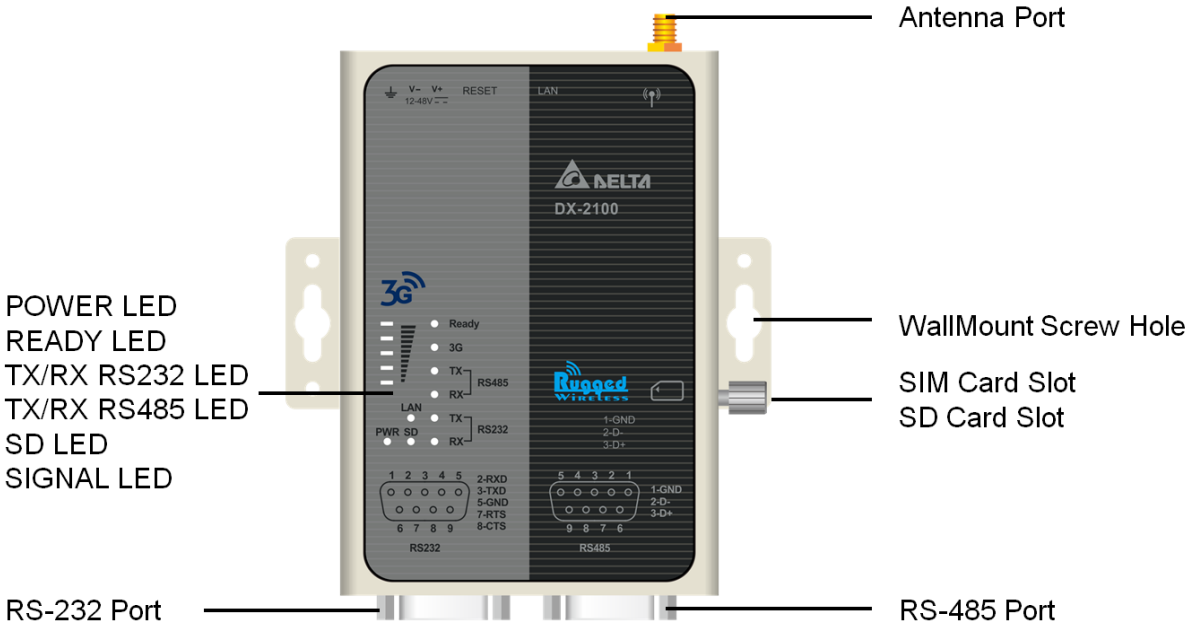
DIACloud platform services supported, users can connect intelligent devices from different locations to the internet with DX-2100RW-WW and use point-to-point connection with the router for a safe and reliable data transmission and additionally save the costs of VPN device operation as well as maintenance.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



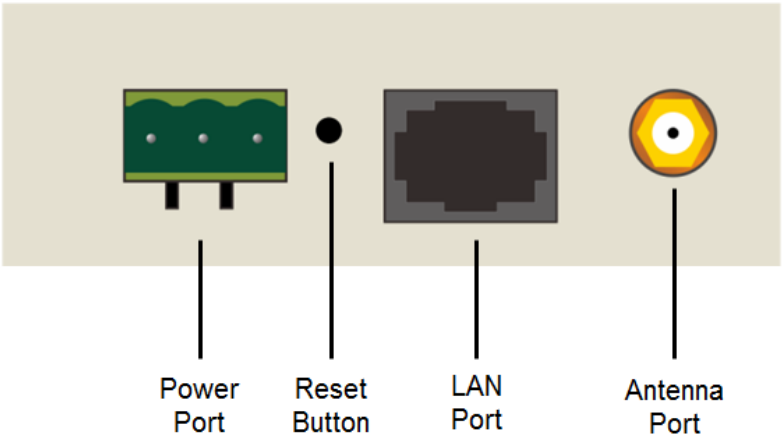
1.1.2 Features

- 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 RS-232 & RS-485 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
- 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

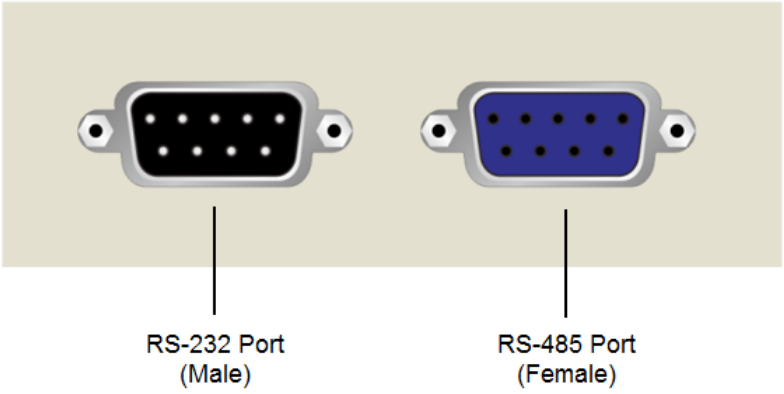
1.1.3 Front Panel Ports and LEDs



1.1.4 Top Panel



1.1.5 Bottom Panel



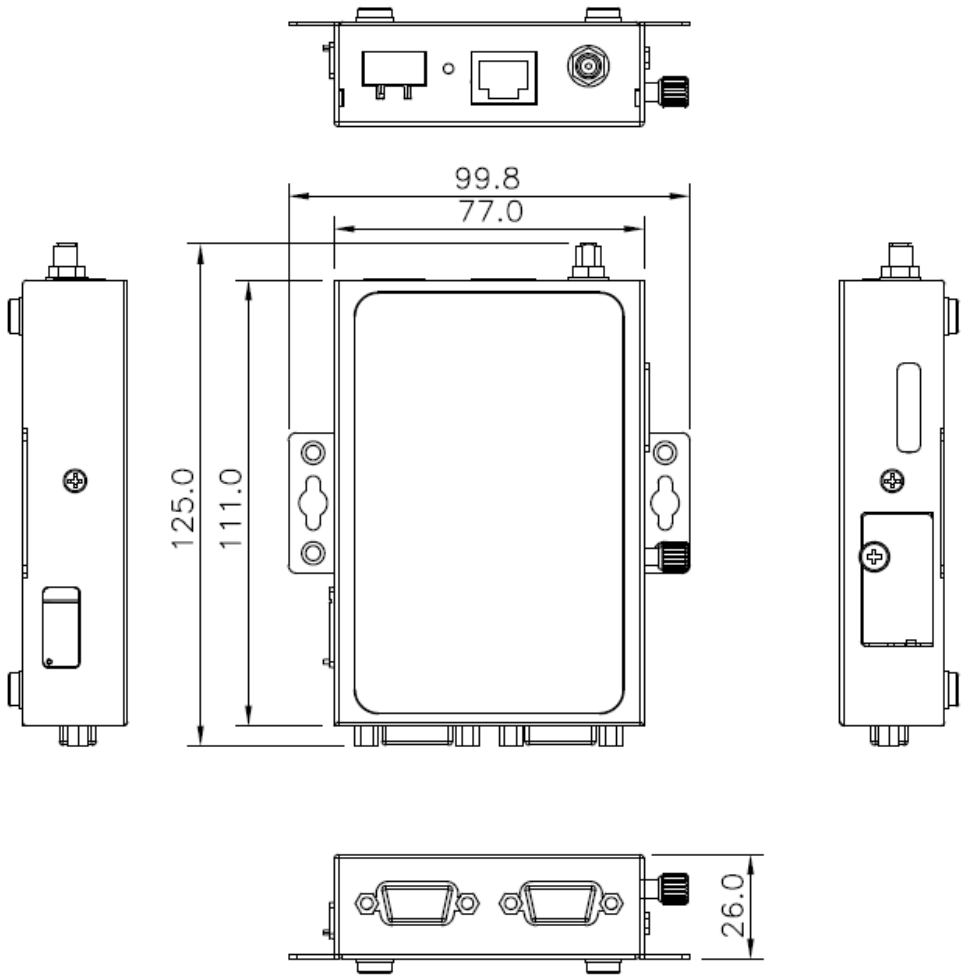
Notice

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-2100RW-WW Industrial 3G 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.

2

Chapter 2 User Interface

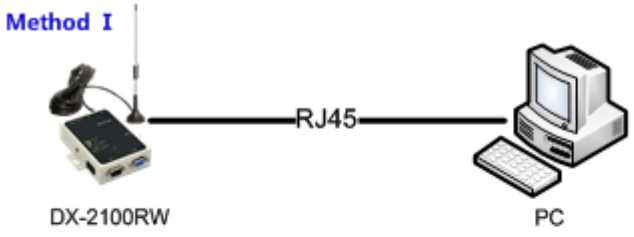
Table of Contents

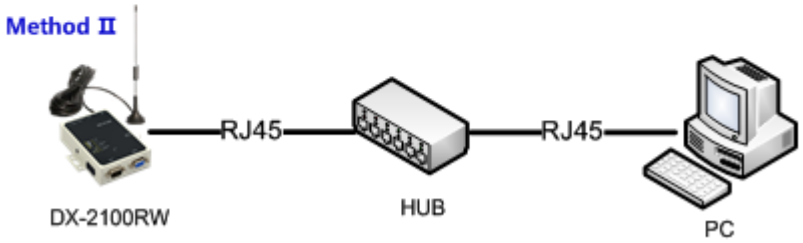
2.1 Web-based GUI Configuration

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

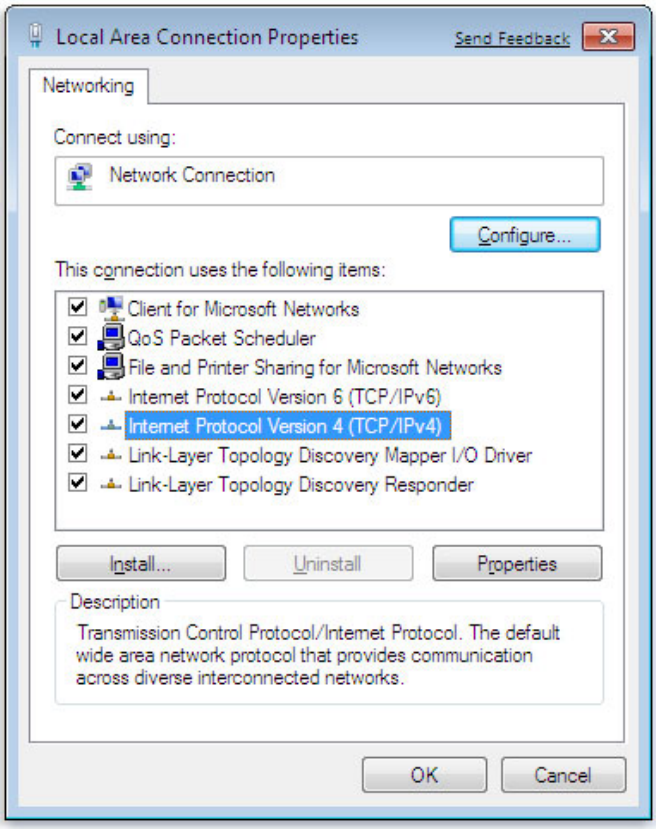
The default domain name of router is **www.diadevice.com**, default IP address is **192.168.1.1.** The initial account and password is **admin/admin**

2.1.3 Local Network Setups

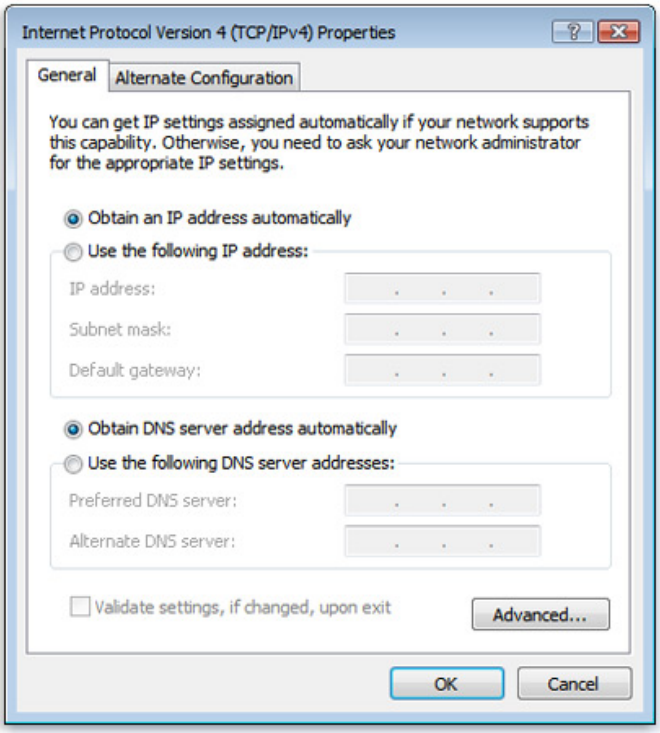
After the connection of the local computer and the router is done, you will need to set the network configruration for your computer. There are 2 methods for the setting, we prefer you use the first one:

- **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 want 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. Under This connection uses the following items, click either Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6), and then click Properties.



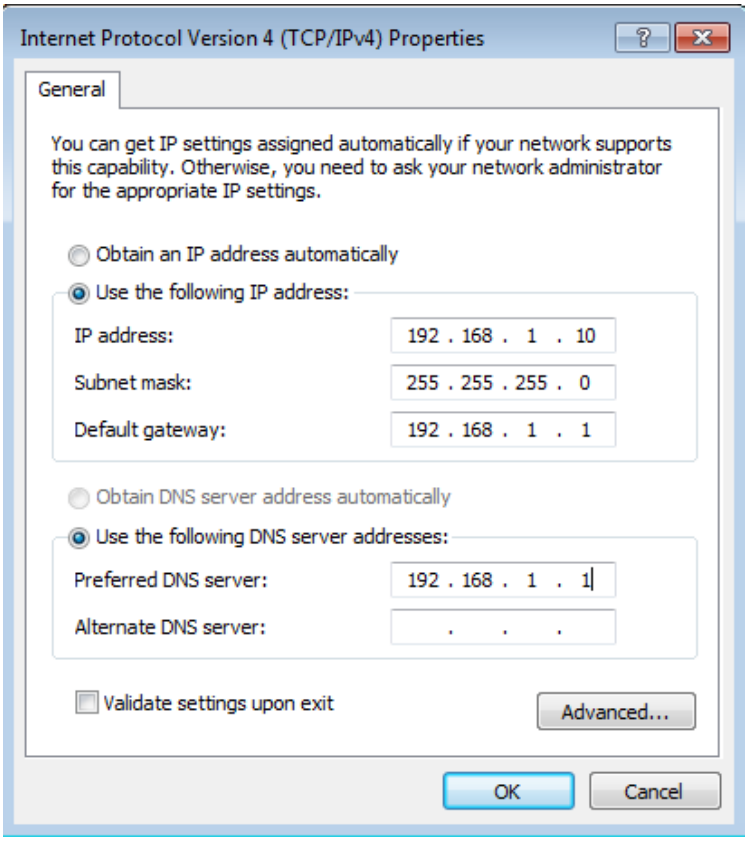
5. Click Obtain DNS server address automatically and then click OK to get a DNS server address automatically using DHCP.



- **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 192.168.1.1 and the subnet mask is 255.255.255.0, the computer's IP address can be set between 192.168.1.2 to 192.168.1.254. However, you'll need to make sure there are no IP conflicts.

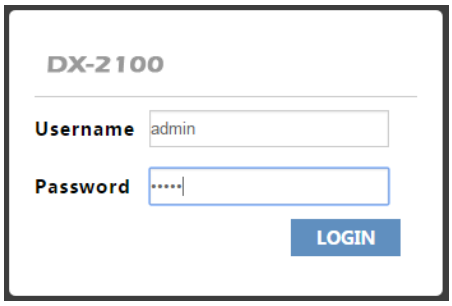
  Here, we set the address to 192.168.1.10 and the default gateway to 192.168.1.1. For DNS, the usable DNS address can be selected or the address can also be set to 192.168.1.1.



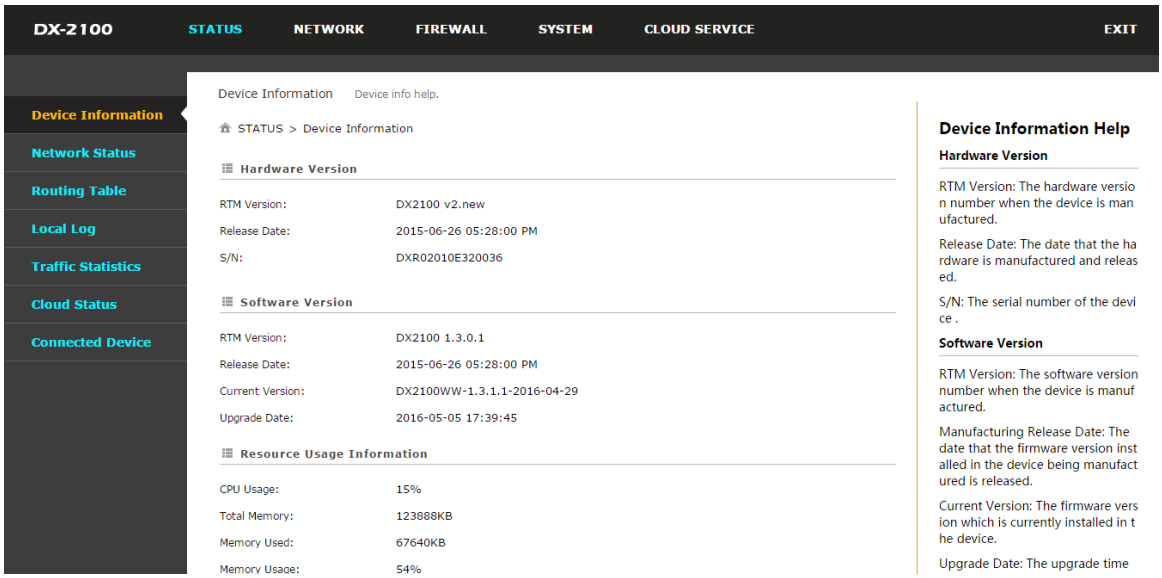
2.1.4 Logging in

1. Open your Internet Explorer browser and input the router's domain name (**www.diadevice.com**) or LAN IP address (Default is 192.168.1.1) 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 hand side of the page.



Notice

Considerations of the router LAN port IP will be change after the device is bind with DIACloud account, we prefer you use www.diadevice.com and use the automatically obtained IP address and DNS server for the computer

3

Chapter 3 Functions

Table of Contents

3.1 Configuration Page

After logging in to the DX-2100RW-WW, you will see 5 setting categories on the top of the configuration page, Status, Network, Firewall, System and Cloud Service. Each category will be covered in the following sections respectively.

3.1.1 Status

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

3.1.1.1 Device Information

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

STATUS > Device Information

Hardware Version

RTM Version:	DX2100v2.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-1.3.1-2016-03-09
Upgrade Date:	2016-03-09 20:05:33

Resource Usage Information

CPU Usage:	15%
Total Memory:	123888KB
Memory Used:	67684KB
Memory Usage:	54%

- 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

3.1.1.2 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.

STATUS > Network Status

Cellular Network Status Connect Disconnect

Operator	China Unicom 3G	Signal Strength	3
Connection Status	Online	Online Duration	
0day 00:04:49			
Authorization Mode	Auto	APN	3gnet
Telephone Number	#	IP Address	10.22.114.35
Network Mask	255.255.255.255	Gateway Address	10.64.64.64
Primary DNS	218.104.128.106	Secondary DNS	58.22.96.66

LAN Status

Device Name	DX2100_4455		
MAC Address	00:11:22:33:44:55		
IP Address	192.168.1.1	Network Mask	255.255.255.0
DHCP Server	Enabled		
Lease Time	One day		
First IP Address	192.168.1.100	Last IP Address	192.168.1.200

3.1.1.3 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

3.1.1.4 Local Log

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

STATUS > Device Logs

Log Type

◉Informative log ○Warning log ○Debug log

Log Content

Refresh Clear Download

Timestamp	Content
Apr 1 09:49:08	syslog.info syslogd started: BusyBox v1.15.0
Apr 1 09:49:15	user.info kernel: ip_tables: (C) 2000-2006 Netfilter Core Team
Apr 1 09:49:17	user.info kernel: ipt_CLUSTERIP: ClusterIP Version 0.8 loaded successfully
Apr 1 09:49:19	user.info kernel: arp_tables: (C) 2002 David S. Miller
Apr 1 09:49:22	user.info kernel: usbcore: registered new interface driver usbserial
Apr 1 09:49:22	user.info kernel: USB Serial support registered for generic
Apr 1 09:49:22	user.info kernel: usbcore: registered new interface driver usbserial_generic
Apr 1 09:49:22	user.info kernel: usbserial: USB Serial Driver core
Apr 1 09:49:22	user.err kernel: cdc_acm 1-1:1.0: This device cannot do calls on its own. It is not a modem.
Apr 1 09:49:22	user.info kernel: cdc_acm 1-1:1.0: ttyACM0: USB ACM device
Apr 1 09:49:22	user.err kernel: cdc_acm 1-1:1.2: This device cannot do calls on its own. It is not a modem.
Apr 1 09:49:22	user.info kernel: cdc_acm 1-1:1.2: ttyACM1: USB ACM device

PREV 1 2 3 ... 13 14 15 NEXT

3.1.1.5 Traffic Information

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 hand side to refresh or clear the traffic information.

STATUS > Traffic Statistics

Refresh Clear

Cellular

Data Sent: 248039 bytes Data Reveived: 280291 bytes

LAN

Data Sent: 860865 bytes Data Reveived: 301113 bytes

3.1.1.6 Cloud Service

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

STATUS > Cloud Status

Cloud Status

Registration Status: Not registered

Service Status: Disabled

Activated Time: N/A

3.1.1.7 Connected Device

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

STATUS > Connected Device

Refresh

ID	IP Address	Host Name	MAC Address	Address Allocated By
1	192.168.1.28	CNXMDNIPC062	3C:97:0E:DE:7B:25	STATIC

3.1.2 Network

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

3.1.2.1 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.

NETWORK > Cellular Network

Cellular Network

Operator	Auto
Dial-Up Number	*99#
User Name	
Password	
APN	3gnet
Dial-Up Mode	Always Online
Authorization Mode	Auto
Redial Interval	30 (second)
Redial Times	0 (0 means always redial)
Max Idle Time	0 (0 means always online)
Connection Check Interval	60 second (0 means not checked)
Connection Check Times	5
MTU	1492
Auto Detect	Ping
Target Address	www.DIACloudSolutions.co
Dial Failure To Restart	Enable

Save Cancel

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	*99#

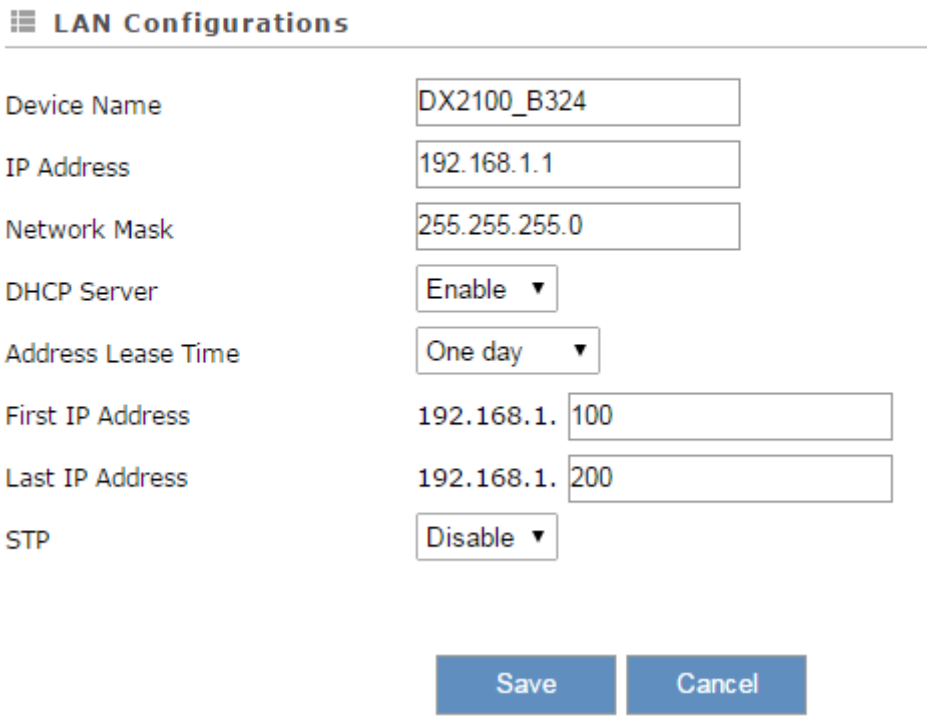
Description	Default
system will set the number up automatically and users cannot change the setting.	
User Name	
This name is provided by the operator. When “Auto” is selected, the system will set the name up automatically and users cannot change the setting.	N/A
Password	
This password is provided by 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 up 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 up 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 up 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 up 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	

Description	Default
Set up 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
MTU	
Maximum Transmission Unit is the largest packet that can be transmitted over packet based networks.	1492
Auto Detect	
If the connection is dropped, a ping test will launch automatically.	Enable
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.	Enable

3.1.2.2 LAN Configurations

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

NETWORK > LAN Configurations



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.	192.168.1.1
Network Mask	
Set up the LAN network mask.	255.255.255.0
DHCP Server	
Dynamic Host Configuration Protocol allows you to obtain an IP address automatically from your router. You can enable or disable this functionality.	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. Options here are 1 to 3 days.	One day
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

3.1.2.3 Static Routing Rules

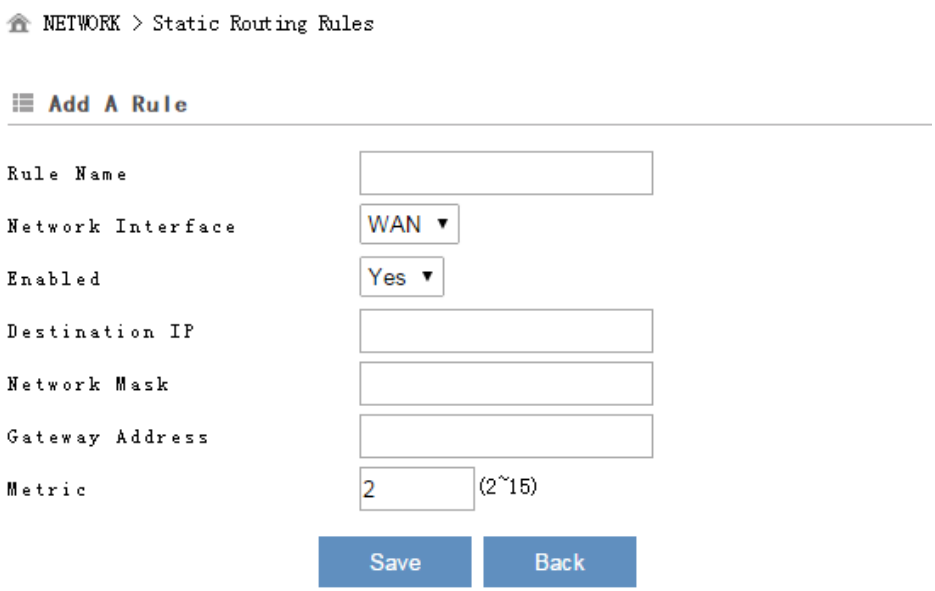
This page is used for setting up the Static Routing, including the Rule Name, Network Interface, Enabled, Destination IP, Network Mask, Gateway Address and Metric. Click the "Add A Rule" to add static routing rules.

NETWORK > Static Routing Rules

Add A Rule

ID	Enabled	Name	Destination	Gateway	Network Interface

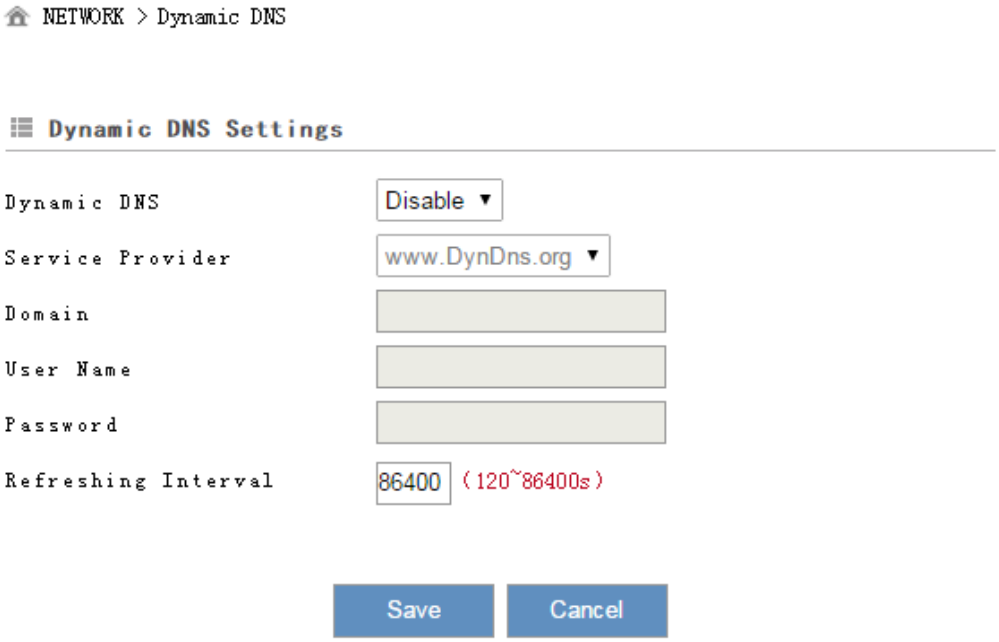
After clicking the "Add A Rule", you will see the following page.



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

3.1.2.4 Dynamic DNS Settings

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.	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 up the time for the router to update its public network IP from the dynamic domain service provider. The value range is 120~86400 sec.	86400

3.1.3 Firewall

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

3.1.3.1 Basic Configurations

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.

FIREWALL > Firewall Settings

Basic Firewall Settings

Firewall	Enable
WAN Ping	Not responded
LAN SSH	Enable
WAN SSH	Disable

Save Cancel

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	
Set up whether to allow LAN end to connect with the router via SSH.	Enable
WAN SSH	
Set up whether to allow WAN end to connect with the router via SSH.	Disable

3.1.3.2 DMZ Configurations

This page is used for setting up the DMZ server.

FIREWALL > DMZ Settings

DMZ Settings

DMZ Server Enable

DMZ Host IP Address

Save Cancel

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	
Set up the IP address for the DMZ host.	N/A

3.1.3.3 Port Forward

This page is used for setting up the port forward, including configuring the Network Services, Service Name, Protocol, Public Port, Server Port, and Server IP Address.

Click the "Add A Portforward Rule" to add port forwarding entries to the router.

FIREWALL > Port Forward

Add A Portforward Rule

ID	Service Name	Protocol	Public Port	Server Port	Server IP Address

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

FIREWALL > Port Forward

Add A Portforward Rule

Network Services	Customized
Service Name	
Protocol	TCP/UDP
Public Port	Single port (1~65534)
Server Port	Single port (1~65534)
Server IP Address	192.168.1.

Save Back

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 up the protocol type for port forwarding.	TCP/UDP
Public Port	
Set up 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 Public Port: Single Port 1001 (1~65534) Server Port: Single Port 80 (1~65534)	Single Port

Description	Default
N:1 Public Port: A Port Range ▼ 1001 - 1008 (1~65534) Server Port: Single Port ▼ 80 (1~65534) N:N Public Port: A Port Range ▼ 1001 - 1008 (1~65534) Server Port: A Port Range ▼ 1001 - 1008 (1~65534)	
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
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
Quakell/III	TCP/UDP	27960	27960
Real-Audio	TCP	6970	7170

3.1.3.4 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.

FIREWALL > Port Trigger

Port Trigger Disable ▼ Port Trigger Timeout 20 Minute Save Add A Trigger Rule

ID	Service Name	Service Type	Inbound Connection	Service User	Status

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

FIREWALL > Port Trigger

Add A Trigger Rule

Service Name

Service User Any address ▼

Service Type TCP ▼

Trigger Port (1~65534)

Inbound Connection

Protocol Role TCP/UDP ▼

Begin Port (1~65534)

End Port (1~65534)

Status Disabled ▼

Save Back

Description	Default
Service Name	
Set up 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 up the protocol type for port triggering.	TCP
Triggering Port	
Set up the triggering port. The port range is 1~65534.	N/A
Protocol Role	
Set up the protocol type for the inbound connection.	TCP/UDP
Begin port	
Set up the starting port for the inbound connection. The port range is 1~65534.	N/A

Description	Default
End Port	
Set up the ending port for the inbound connection. The port range is 1~65534.	N/A
Status	
Enable/disable the port triggering functionality.	Disable

3.1.3.5 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.

FIREWALL > URL Filter

URL Address Filter Disable Save Add An URL Address

ID	URL Address	LAN IP Address	Status

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

FIREWALL > URL Filter

Add URL

URL Address

LAN IP Address Any address

Status Enabled

Save Back

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	
Set up 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.	Enable

3.1.3.6 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.

FIREWALL > MAC Filter

MAC Filter Disable Save Add A MAC Address

ID	MAC Address	Device Name	Status

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

FIREWALL > MAC Address Filter

Add A MAC Address

MAC Address

Device Name

Status Enabled

Save Back

Description	Default
MAC Address	
Manually input the MAC address that you'd like to block.	Disable
Device Name	
Set up the device name corresponding to the set MAC address.	Any Address
Status	
Enable/disable the MAC Filter functionality.	Enable

3.1.3.7 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.

FIREWALL > IP Filter

IP Filter Disable Save Add An IP Address

ID	Source IP Address Range	Source Port Range	Range Of Destination IP Address	Range Of Destination Port	Protocol	Status

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

FIREWALL > IP Filter

Add An IP Address

Source IP	Any address
Source Port	Any port
Destination IP	Any address
Destination Port	Any port
Protocol	TCP/UDP
Status	Enabled

Save Back

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

3.1.4 System

You can set up the system configurations, including the User Management, Time Configurations, RS-232, RS-485, Modbus TCP, Log Setting, System Upgrade, Backup & Restore, Scheduled Jobs, Network Diagnosis, System Reboot, Event Management, and Variable Management.

3.1.4.1 User Management

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

SYSTEM > User Management

User Management

Old Password

New Password

The password must be a combination of 5 to 12 characters,numbers and underline marks

Confirm Password

Save Cancel

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.	A/A

3.1.4.2 Time Configuration

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

SYSTEM > Time Configurations

The current time of device 2016-05-06 16:02:55

Time Zone Setting (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

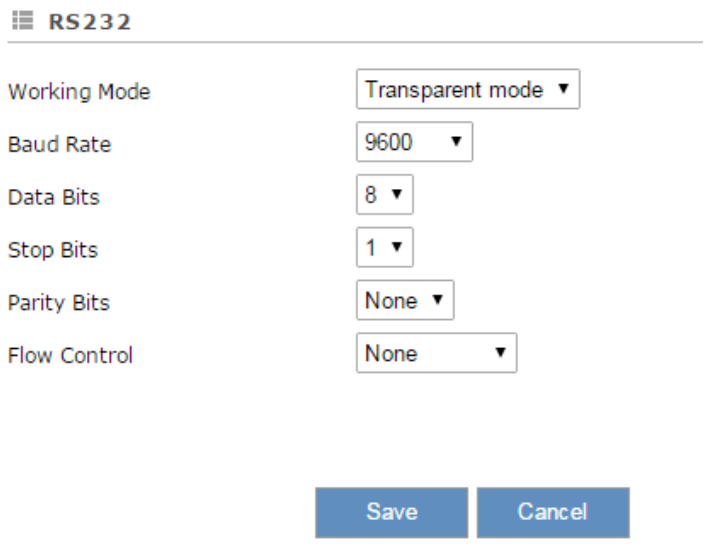
Save

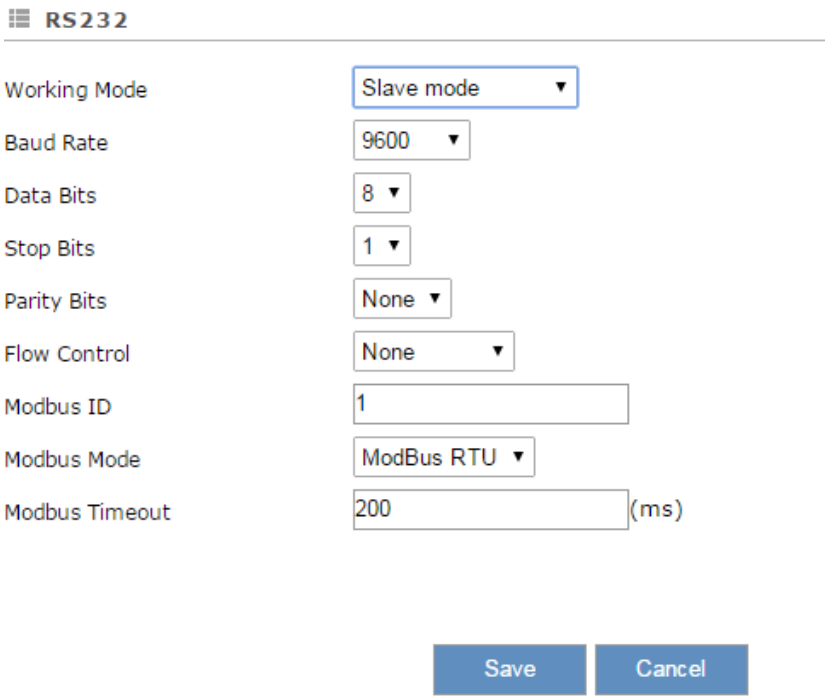
Description	Default
The current time of device	
Here shows the current time of your device.	N/A
Time Zone Setting	
Select the operating time zone of your device: GMT-12:00 - GMT+13:00.	N/A

3.1.4.3 RS-232

RS-232 (Recommended Standard - 232) is a telecommunication standard for binary serial communications between devices. You can set up the configurations for RS-232, including Baud Rate, Data Bits, Stop Bits, Parity Bits and Flow Control.

SYSTEM > RS232





Description	Default
Working Mode	
Select the working mode for the current active serial port. ● **Transparent mode:** This mode is suitable for uploading and downloading data remotely via the serial port.	Close

Description		Default
● **Slave mode:** This mode is suitable for the PLC to perform the read/ write tasks on the open register of the DX-2100RW-WW. ● **Close:** Disable this functionality.		
Parameters of COM	**Baud Rate**	
	Set up the baud rate for the serial port. Options are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.	9600
	Data Bits	
	Set up the data bits for the serial port. ● **Transparent mode:** 7, 8 ● **Slave mode:** 8	8
	Stop Bits	
	Set up the stop bits for the serial port. Options are 1 and 2.	1
	Parity Bits	
	Set up the parity bits for the serial port. Options are None, Odd and Even.	None
	Flow Control	
	Set up the flow control. Options are None, XON, XOFF, RTS, and CTS.	None
Slave Mode	**MODBUS ID**	
	Set up the MODBUS ID. The value is between 1 and 255.	1
	MODBUS Mode	
	Set up the communication mode for the device.	MODBUS RTU
	MODBUS Timeout	
	Set up the timeout timer from 200ms to 3000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	200ms

3.1.4.4 RS-485

RS-485 (Recommended Standard - 485) is a telecommunication standard for binary serial communications between devices. You can set up the configurations for RS-485, including Baud Rate, Data Bits, Stop Bits, Parity Bits, and many more.

SYSTEM > RS485

RS485

Working Mode	Transparent mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None

Save Cancel

SYSTEM > RS485

RS485

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

Save Cancel

SYSTEM > RS485

RS485

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

Read/Write Configuration

Scan Interval 30000 (ms)

Setting Address: address is decimal, taking care to avoid conflicts with address set in other feature!

Add Mappings

Read/Write	Slave ID	Slave Starting Address	Device Starting Address(2048-4095)	Length(1-123)	Operation
Read					Delete

Save Cancel

Description		Default
Working Mode		
Select the working mode for the current active serial port. ● **Transparent mode:** This mode is suitable for uploading and downloading data remotely via the serial port. ● **Slave mode:** This mode is suitable for the PLC to perform the read/ write tasks on the open register of the DX-2100RW-WW. ● **Master mode:** This mode is suitable for the DX-2100RW-WW to perform the read/write tasks on the open register of the PLC. ● **Close:** Disable this functionality.		Close
Parameters of COM	**Baud Rate**	
	Set up the baud rate for the serial port. Options are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.	9600
	Data Bits	
	Set up the data bits for the serial port.	8

Description		Default
	● **Transparent mode:** 7, 8 ● **Modbus RTU:** 8	
	Stop Bits	
	Set up the stop bits for the serial port. Options are 1 and 2.	1
	Parity Bits	
	Set up the parity bits for the serial port. Options are None, Odd and Even.	None
MODBUS ID		
Set up the MODBUS ID. The value is between 1 and 255.		1
MODBUS Mode		
Set up the communication mode for the device.		MODBUS RTU
MODBUS Timeout		
Set up 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	**Scan Interval**	
	Set up the time for scan interval, ranging from 20ms to 60000ms.	30000ms
	Read/Write	
	Set up the access permissions for the mapped register address; the default is read-only.	Read
	Slave ID	
	Set up the corresponding slave communication port. The value is between 1 and 255.	N/A
	Slave Starting Address (decimal)	
	Set up the slave starting address (decimal) for read/write the registers in a PLC.	N/A
	Device Starting Address (decimal)	
	Set up the device starting address (decimal, starting from 2048). If the mapped address is with “Read” permission, data read from appointed registers in the PLC will be stored in this device starting address. If the mapped register address is with “Write” permission, data from the device starting address will be stored in the appointed registers in the PLC.	N/A
	Length (1-123)	
	Here displays the number of the continuous	N/A

Description		Default
	address followed by the default mapped address.	
	Add Mappings	
	Click the button to add mappings; up to 100 addresses can be set up.	N/A
	Edit	
	Click an item of register mapping forms that can be edited.	N/A
	Operation	
	The added mappings can be deleted here.	N/A

3.1.4.5 Modbus TCP

This page is used for configuring the Modbus TCP, including Working Mode, Server IP, Server Port, and Response Timeout.

SYSTEM > Modbus TCP

Modbus TCP

Working Mode: Modbus TCP Client

Server IP:

Server Port: 502

Response Timeout: 300 (ms)

Read/Write Configuration

Scan Interval: 30000 (ms)

Setting Address: address is decimal, taking care to avoid conflicts with address set in other feature!

Add Mappings

Read/Write	Slave ID	Slave Starting Address	Device Starting Address(2048-4095)	Length(1-123)	Operation
Read					Delete

Save Cancel

Description	Default
Working Mode	
The default is OFF. Other options are: • **Modbus TCP Server (Slave)**: for applications of a PLC to read/write the open registers in DX-2100RW-WW • **Modbus TCP Client (Master):** for DX-2100RW-WW to read/write the open registers in a PLC	OFF

Description		Default
Modbus TCP Client	**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 100000ms. 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 20ms to 60000ms; the default is 3000ms.	30000
Add Mappings	**Read/Write**	
	Set up the access permissions for the mapped register address; the default is read-only.	Read
	Slave ID	
	Set up the corresponding slave communication port. The value is between 1 and 255.	N/A
	Slave Starting Address	
	Set up the slave starting address (decimal) for read/write the registers in a PLC.	N/A
	Device Starting Address	
	Set up the device starting address (decimal, starting from 2048). If the mapped address is with “Read” permission, data read from appointed registers in the PLC will be stored in this device starting address. If the mapped register address is with “Write” permission, data from the device starting address will be stored in the appointed registers in the PLC.	N/A
	Length (1-123)	
	Here displays the number of the continuous address followed by the default mapped address.	N/A
	Operation	
	Delete the selected mapped address.	N/A
	Add Mappings	
	Click the button to add mappings; up to 100 addresses can be set up.	N/A

Description		Default
	Edit	
	Click to select the records from the mapped address to edit.	N/A
	Operation	
	The added mappings can be deleted here.	N/A

3.1.4.6 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.

SYSTEM > Log Settings

Log Settings

Log To Console: No

Remote Log Service: Disable

Remote Log Server Address:

Port Of Remote Log Server: 514 (1~65534)

Save Cancel

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.

3.1.4.7 Firmware Upgrade

This page is used for upgrading the system.

SYSTEM > Firmware Upgrade

Firmware Upgrade

DO NOT turn off the power supply or reboot the device during the upgrade process. Please select the correct firmware package which is consistent with the device model,otherwise the device may be damaged !

(Before upgrade the firmware, please backup the settings and data. Please contact the local dealers or manufacturers when failed to upgrade the firmware)

Select Firmware Browse...

Upgrade Cancel

Description	Default
Chose file	
Click “Choose file” 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

3.1.4.8 Backup & Restore

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

SYSTEM > Backup & Restore

Backup & Restore

Device configurations can be backed up and saved to local PC

Backup

Configuration restoration will remove the current settings in the device and restore the configurations in your .cfg file

Select .Cfg File Browse...

Restore

Configurations will be reset to the factory default settings, device will be reboot after the reset

Reset To Factory Default

Description	Default
Backup	
Click “Backup” to save the device configurations on your computer.	N/A
Restore	
Click “Chose file” to select the backup file and then click “Restore” to restore the configurations. The device configuration will be restored to the previous	N/A

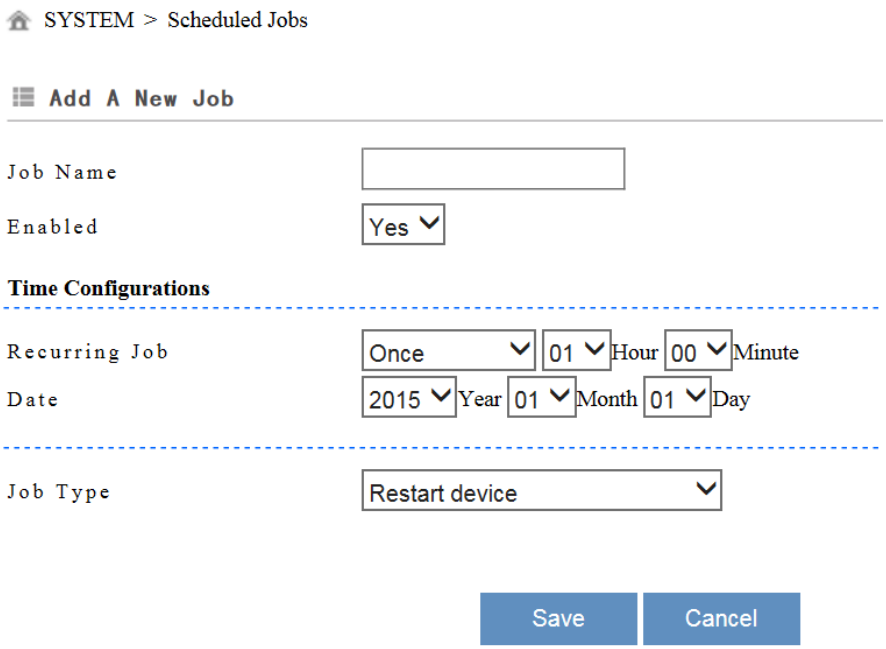
Description	Default
version and the device will reboot after the restoring is done.	
Restore To Factory Default	
Click “Restore To Factory Default” to reset the configurations to the factory defaults. The device will reboot after the reset is done.	N/A

3.1.4.9 Scheduled Jobs

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

3.1.4.9.1 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.

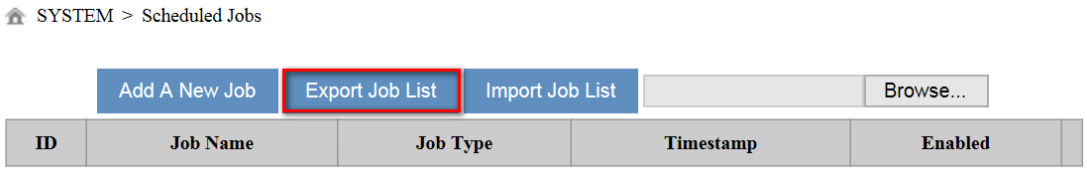


Description	Default
Job Name	
Set up a name for your scheduled job. The name shall be composed of letters, numbers and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Enable	
Select “Enable” to activate this functionality.	Enable
Recurring Job	

Description	Default
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
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

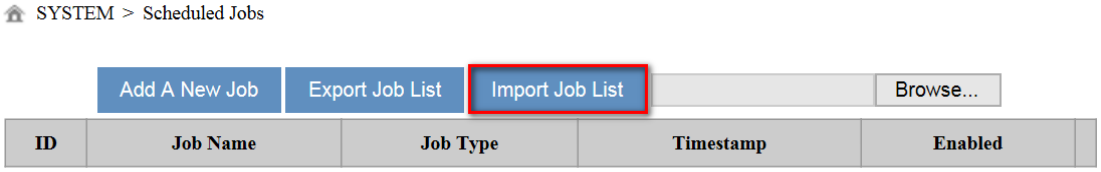
3.1.4.9.2 Export Job List

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



3.1.4.9.3 Import Job List

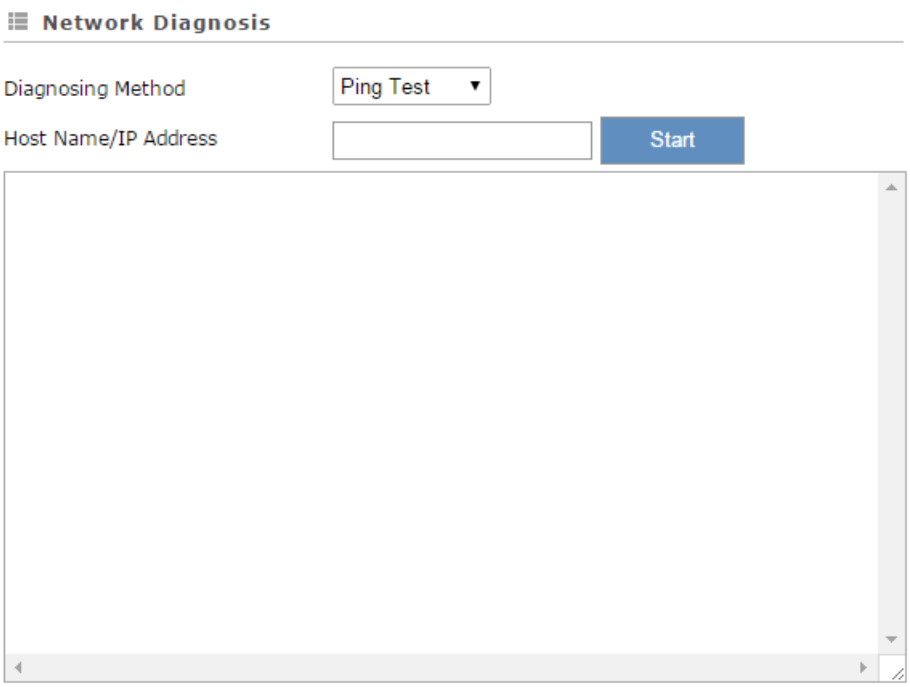
Click "Chose file" to select the scheduled jobs file you have saved and then click "Import Job List" to import the scheduled jobs you have set before.



3.1.4.10 Network Diagnosis

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

SYSTEM > Network Diagnosis

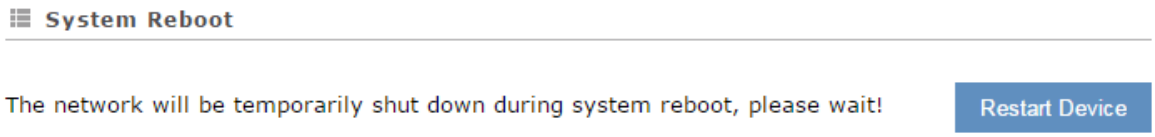


Description	Default
Diagnosing Method	
Select the Diagnosing Method; options are Ping Test and Route Trace.	Ping Test
Host Name/IP Address	
Input the Host Name or the IP Address.	N/A
Start	
Click “Start” to start the network diagnosing. While running the network diagnosing, the settings cannot be changed.	N/A

3.1.4.11 System Reboot

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

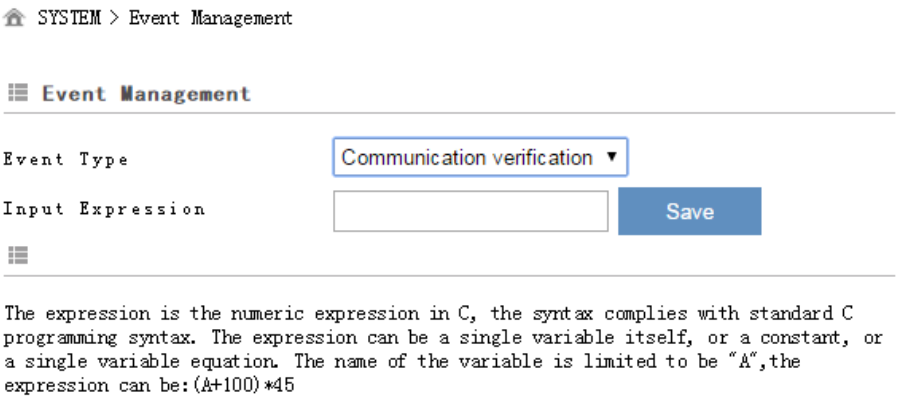
SYSTEM > System Reboot



3.1.4.12 Event Management

This page is used for setting up 2 types of events, Communication Verification and Alarm Event.

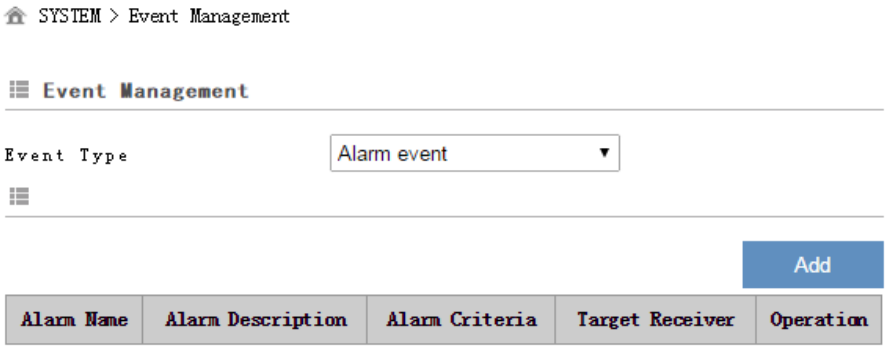
- Communication Verification: when this option is selected, the router will monitor and check if this channel is trustable to ensure a safe communication between a router and a PLC via Modbus TCP or Modbus RTU.



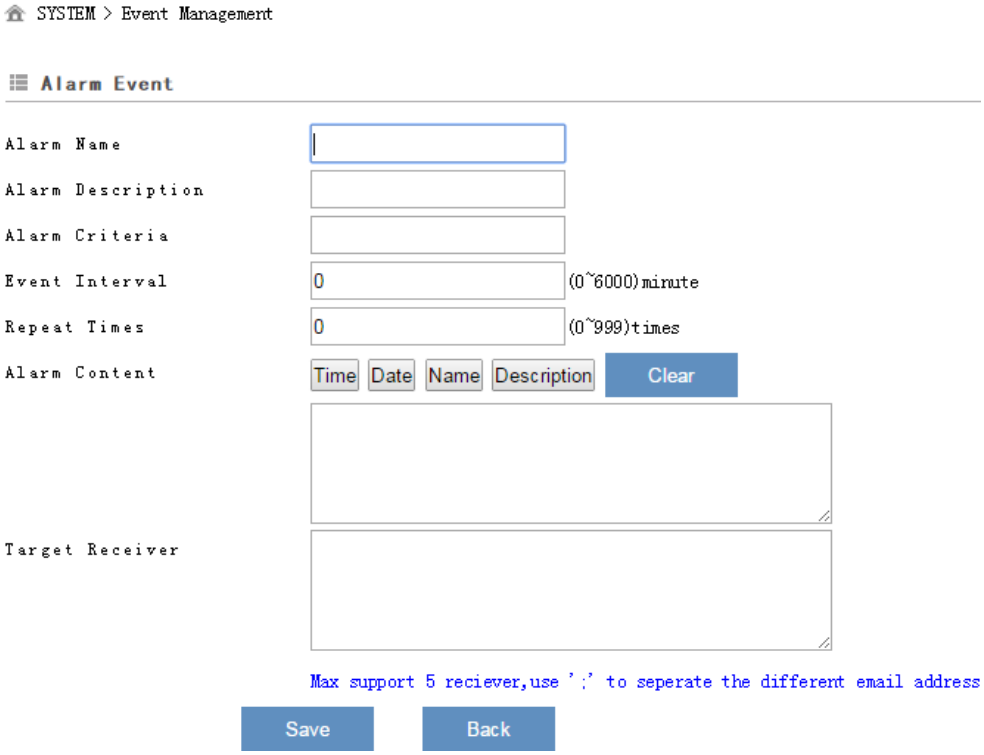
The operators that the expression supports are as below:

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: uses 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.



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	
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: {$2003}+{$2004}*100/2-1.	N/A
Event Interval	
The time interval of alarm sending	0
Repeat Times	
The repeated times of alarm sending	0
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	N/A

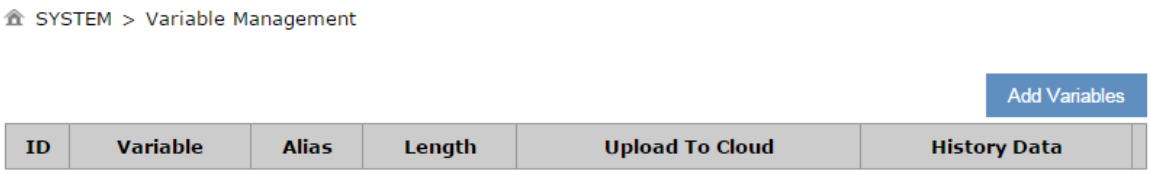
Description	Default
● **Date:** the date when the alarm occurred ● **Name:** the name of the occurred alarm ● **Description:** the description of the occurred alarm **For example:** Register $2003 represents electrical voltage, the value of register $2003 is 10, and the alarm content is set as: {Date} {Time} Voltage = {$2003}, then the alarm content received by users will be: 2015/06/01 10:00:00 Voltage = 10. The maximum content length is 160 characters.	
Target Receiver	
Set up the recipient. The alarm notification will be sent via email, up to 5 email addresses can be used and separate each recipient with a semicolon.	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.

3.1.4.13 Variable Management

This page is used for setting up the variables. Click “Add” to set a new variable. Click ”Edit” to modify the existing variable. Click “Delete” to delete the existing variable.



The address segment 2048~4095 can be self-defined. The Variable Name, Alias, Length, and Uploaded To Cloud can be set up. After clicking “Add”, the following page will show up.

Description	Default
Variable Name	
Register address. The allowable range is 2048~4095. Start with $.	N/A

Description	Default
Alias	
Input a variable name. The name shall be composed of numbers, English letters, uppercase and lowercase. The maximum string length is 30 bytes.	N/A
Length	
To register as a unit. If you input 1 in length field, it is meaning one register (16bit) will be created. Effective range: 1-2048.	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.

3.1.5 Cloud Service

You can log in to the DIACloud Service. Input the user name, the password and click "Verify". Refer to Chapter 4 for DIACloud account registration.

CLOUD SERVICE > Cloud Configurations

Cloud Configurations

User Name:

Password: Verify

After clicking "Verify", the following page will show up. The contents here can be further defined. Clicking "Bind" to have the device connected to the Cloud, and then you can open the web management page to configure and manage the device remotely via the DIACloud platform.

CLOUD SERVICE > Cloud Configurations

Cloud Configurations

User Name: 1[redacted]0@163.com

Password: ••••••••••• Verify

Secure Tunnel: default

Device Name: DX2100_B324

Secure Tunnel DHCP: Available

When secure tunneling 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

Get IP From Cloud Yes

Bind Cancel

If don't obtain IP from Cloud, will request you manual setup the IP for device.

Secure Tunnel DHCP: Available

Get IP From Cloud No

Cloud IP Range: 192.168.20.100 - 192.168.20.200

Cloud Netmask: 255.255.255.0

Device IP:

(Device IP should be in the same subnet with cloud IP)

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	N/A

Description	Default
by the DHCP server in secure tunnel network, the IP address of this device can be found in the cloud portal.	
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
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

The following page will show up after bind successfully. You can also select “Unbind” to free the device from the Cloud.

CLOUD SERVICE > Cloud Configurations

User Name:	1[redacted]0@163.com	
Registration Status:	Registered	Unbind
Service Status:	Enabled	Disable
Secure Tunnel:	default	
Device Name:	DX2100_B324	
Secure Tunnel DHCP:	Available	
Get IP From Cloud	Yes	

Notice

- Users can log in to **http://www.DIACloudSolutions.com/** and register for a DIACloud account.
- If the IP is obtained from the Cloud, users can log in to the DIACloud and check for the device IP address after configuration.
- Device IP will change after activation. Please use new IP to access the device and insure your computer’s IP is in the same subnet with new device’s IP, or use

domain **www.diadevice.com** to access the device and insure you use the automatically obtained IP address and DNS server for the computer.

- 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.

3.2 SD Card Quick Installation

User can perform below operation via SD Card function.

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

Trigger process as below:

- When device reboot and detect SD card
- If SD card exists upgrade-package file, then trigger to upgrade device firmware base on this file
- If SD card exist file 'backup.cfg', then trigger to import device configuration base on this file
- If SD card exist file 'Provision.bin' , then trigger to activate device with the account provide by this file, even device has been activated before.

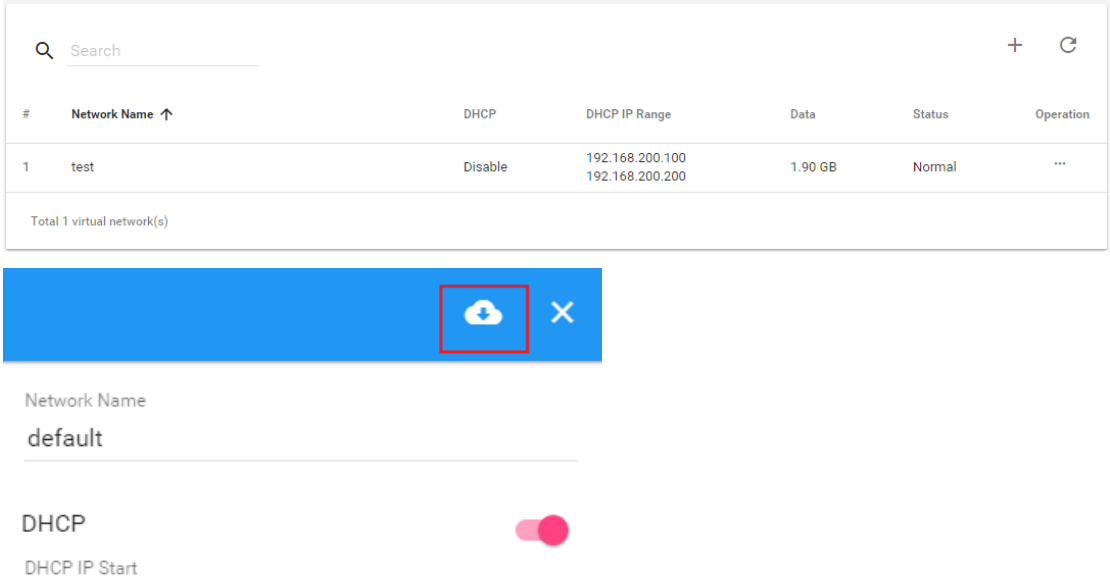
The operate result will cause in buzzer beep as below. (× – fail, √ - success or not this operation)

Buzzer action	upgrade	backup.cfg	Provision.bin
1 long beep	×	√	√
1 long beep and 1 short beep	√	×	√
1 long beep and 2 short beep	×	×	√
1 long beep and 3 short beep	√	√	×
1 long beep and 4 short beep	×	√	×
1 long beep and 5 short beep	√	×	×
1 long beep and 6 short beep	×	×	×
None	√	√	√

User can generate file 'backup.cfg' by function 3.1.4.8.

How to create and bind the DX-Series with SD Card.

1. Go to the DIACloud platform iot.DIACloud.com.
2. Log in the DIACloud webpage, and click [TUNNEL NETWORKS]
3. Click to select the Network 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.

6. 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.

Notice

- Name rule for BIN file: Provision.bin
- Please do not change the file name of firmware upgrade-package.
- Please do not copy more than 1 firmware upgrade-package file to SD Card, to avoid the device be upgrade base on random upgrading file.
- Import the second profile has to wait for 10 minutes if the first profile already imported.

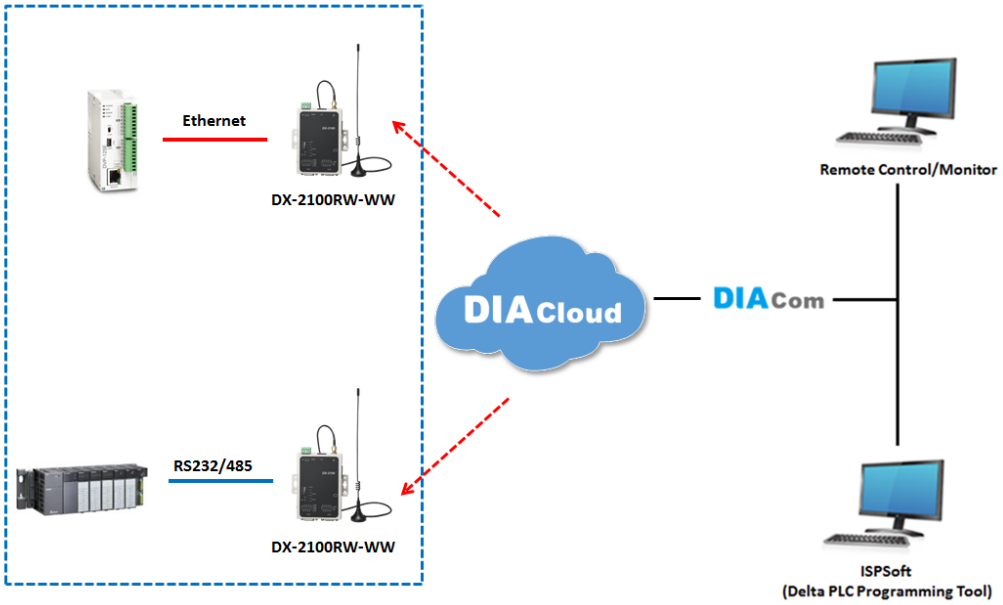
4

Chapter 4 DIACom

Table of Contents

4.1 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	V1.3.0.1 or above
DX-2300	V1.0.0.1 or above

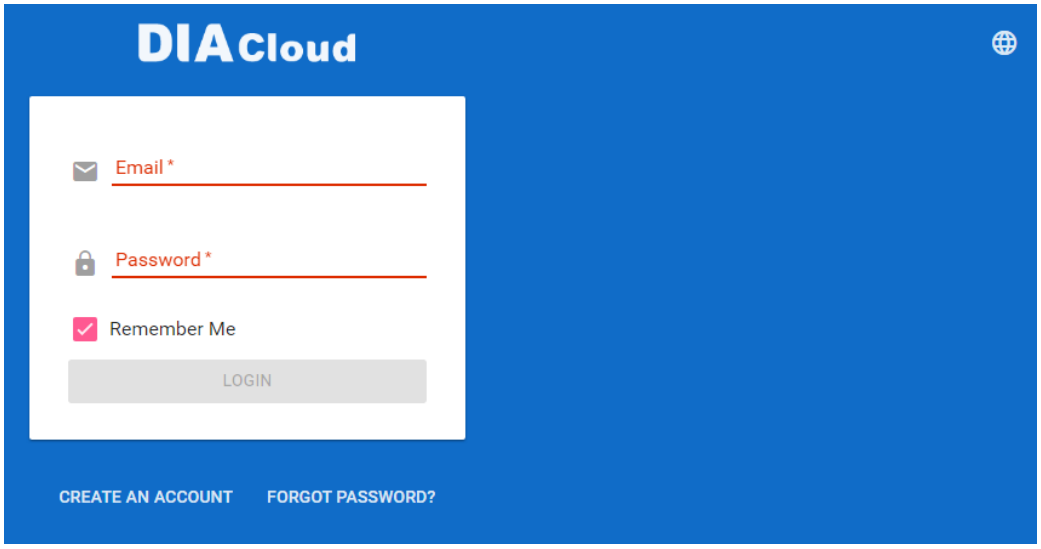
4.1.2 DIACom Installation

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).

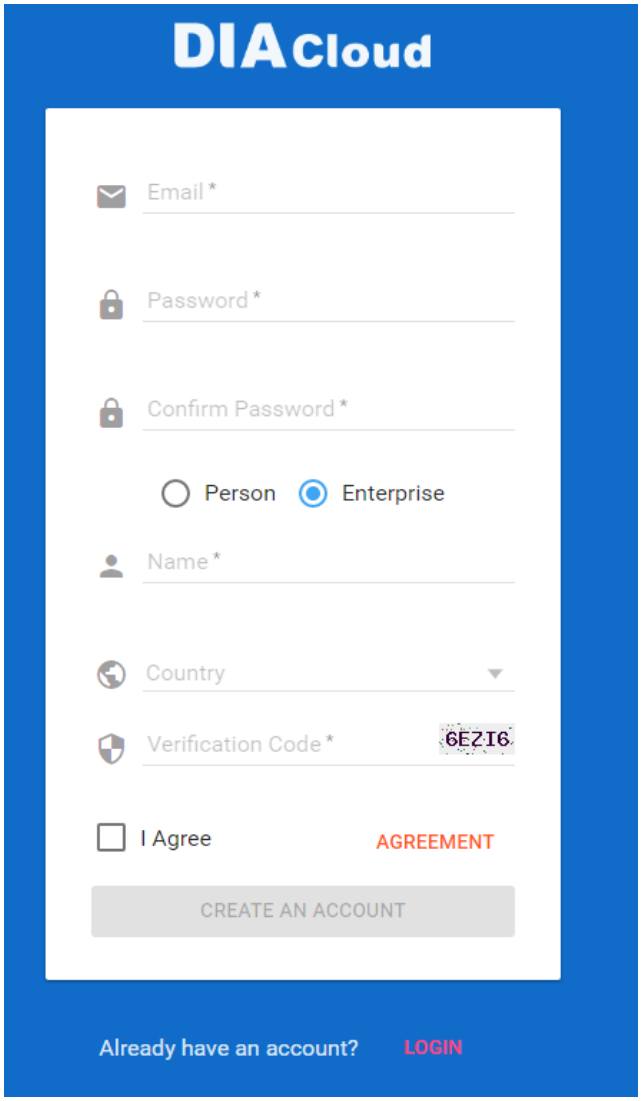
4.1.3 DIACloud Account Registration

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:

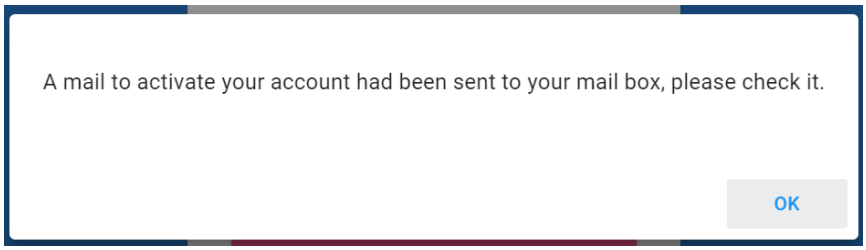


Notice
*Click at the upper right corner to change the interface language to English.

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=fM1xduuNyNZSo4NNyVQCUx5ACGrO5II

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=fM1xduuNyNZSo4NNyVQCUx5ACGrO5II

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 3.1.5 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.

Secure Tunnel DHCP:	Available
Get IP From Cloud	No
Cloud IP Range:	192.168.200.100 - 192.168.200.200
Cloud Netmask:	255.255.255.0
Device IP:	

(Device IP should be in the same subnet with cloud IP)

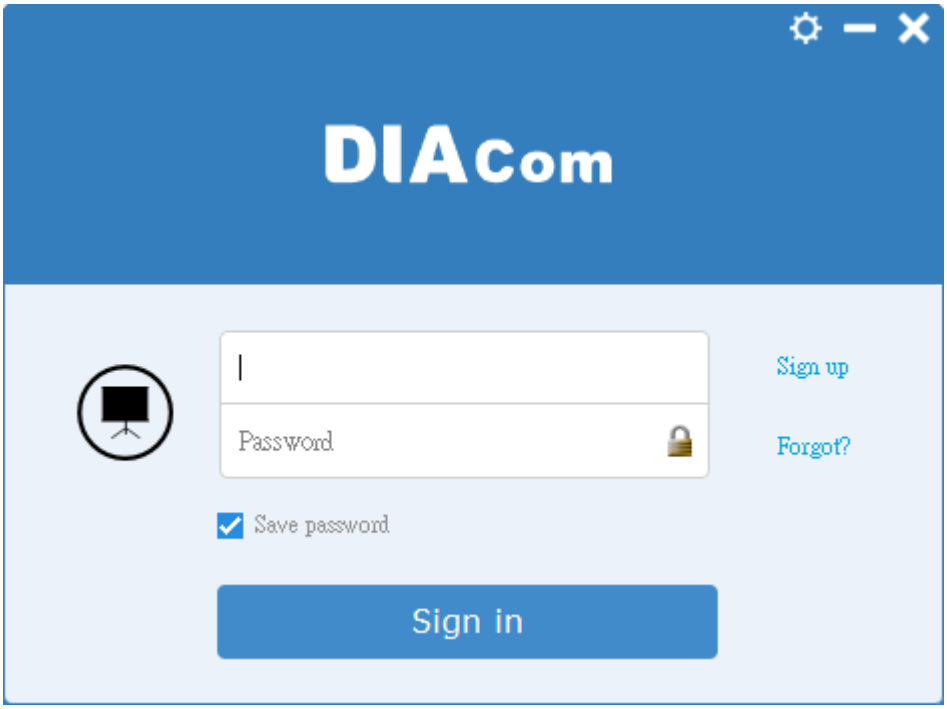
The IP address of the DX-2100 Series and the WAN of your connected PC should be in

different network segments.

4.1.5 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.

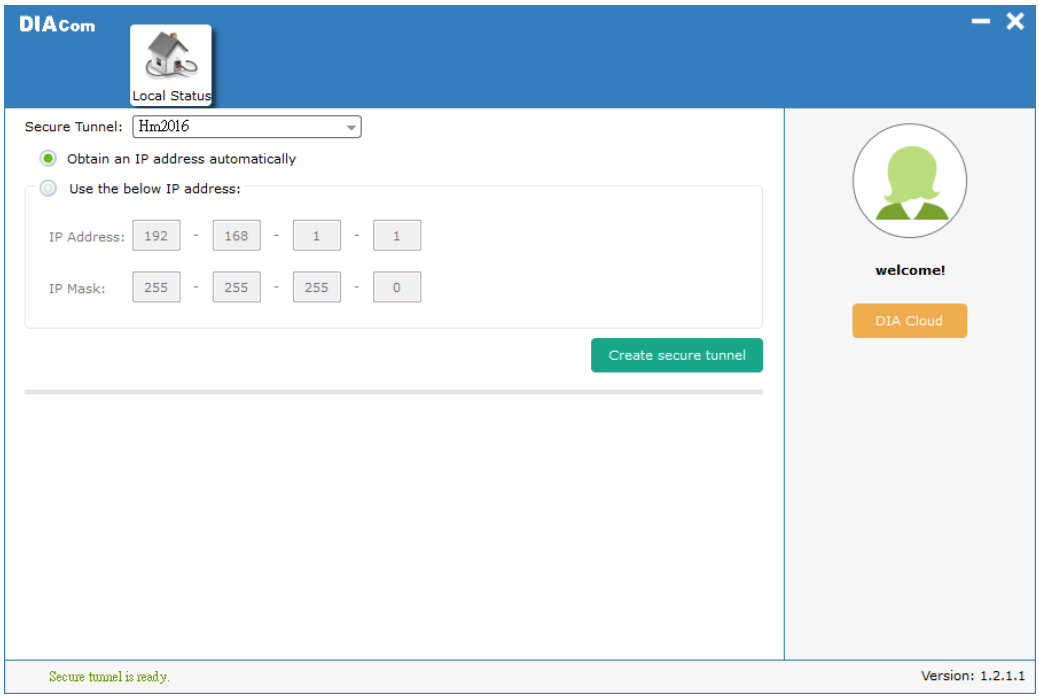
1. Run DIACom and log in with your router's cloud account.



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

- **Http proxy:** Please fills in the proxy server address, port, username and password if the LAN needs to set the proxy to access the Internet.
- **Port Agent:** When the firewall of LAN prohibit some ports which DIACom will use, such as 22013, select this option, DIACom will use the port 443 to send and receive data to the original port, to avoid the restrictions of the firewall.
- These two options can be select simultaneously. The list of port which used by DIACom is in appendix.

3. Add a virtual IP address and subnet mask for your computer. You can use DHCP to obtain an IP address automatically or manually set the IP address. Be sure to set the IP address in the same network segment as your router's, for example, your router IP is 192.168.200.6, and the computer's virtual IP should be set to 192.168.200.xxx.



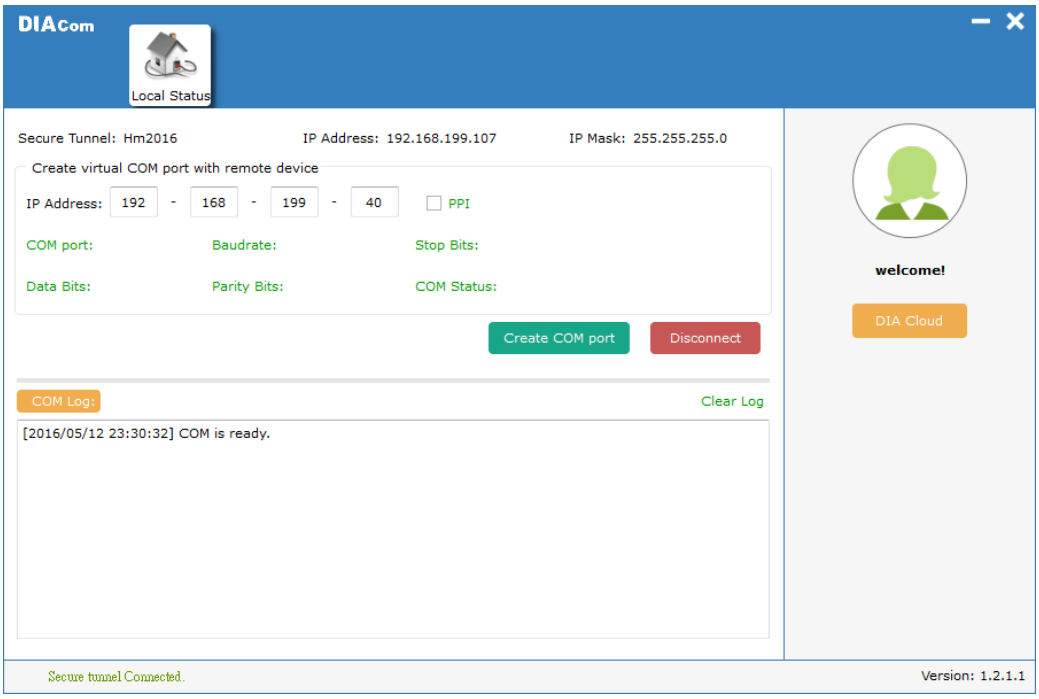
4. Select the same group of VLN, same as your router's group (refer to 3.1.5 Cloud Service for details) and specify an IP address with the same network segment of your router IP and the virtual IP of the computer (); or select "Obtain an IP address automatically".

Notice

Secure Tunnel is a virtual network. Users can create various secure tunnel groups and design different devices to the appointed groups for easier group management. When your DIACloud account is successfully registered, the system will assign a new secure tunnel group named default for your router.

5. Click "Create secure tunnel" and the following image will show up, indicating the creation is successful. Whenever there is internet connectivity, you can use programmable logic controller software to control, monitor, operate, and program your PLC and open your router's webpage (simply input your router's IP in the search bar of a browser) to configure your router remotely.

6. Click "Disconnect" or exit from the DIACom to close the secure tunnel.



4.1.6 Remote Control and Monitoring via DIACom

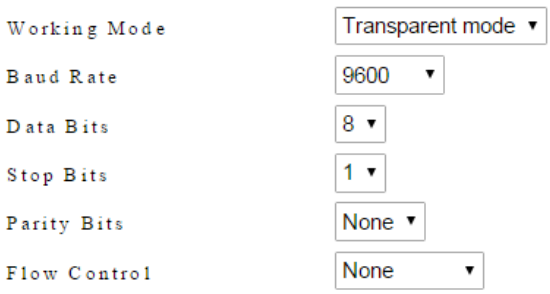
4.1.6.1 Via a LAN Port

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.

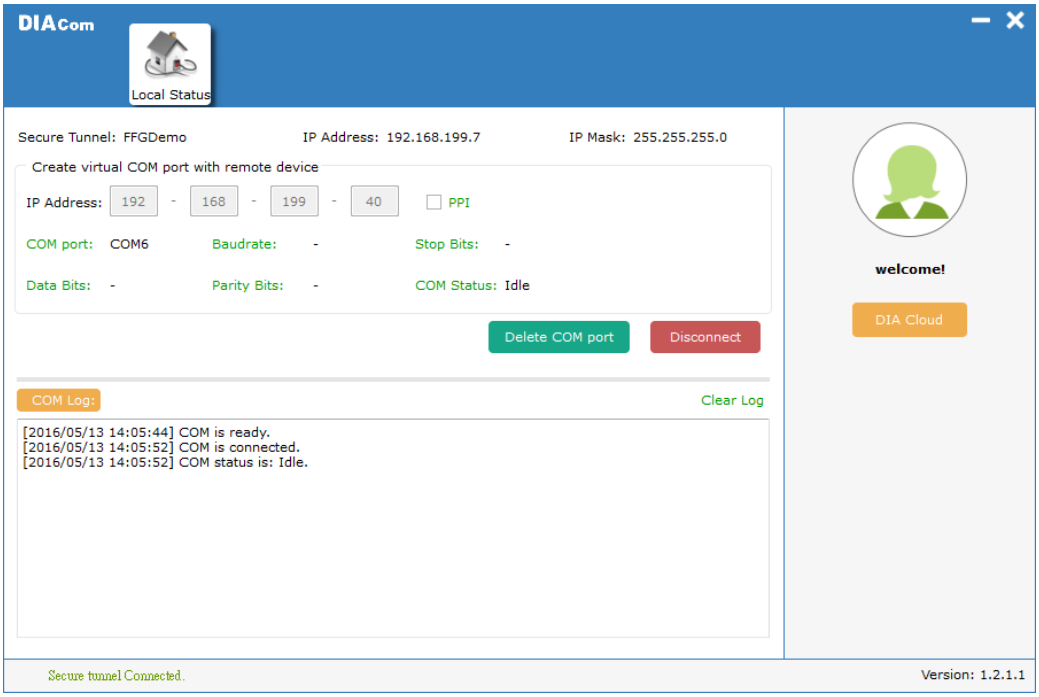
4.1.6.2 Via a RS232/RS485 Port

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. 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)



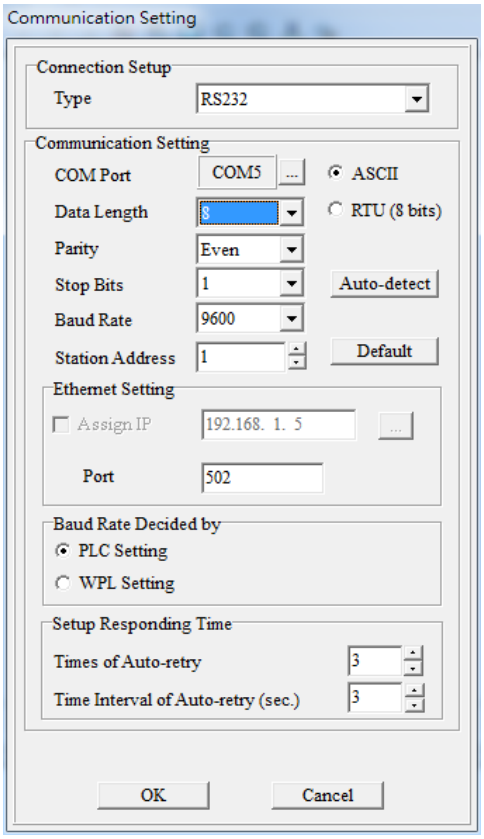
3. Go back to the DIACom and input the IP address of the router which is connected to your remote device. Click “Create COM port” to create a virtual tunnel. Once the creation is done, the virtual IP address will show up on the same page. Users can use this IP address to connect to your local computer and then you can use the configuring/monitoring software to configure and monitor the connected device remotely. Click “Delete COM port” to close the virtual tunnel.



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.


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

5

Chapter 5 DIACloud

Table of Contents

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

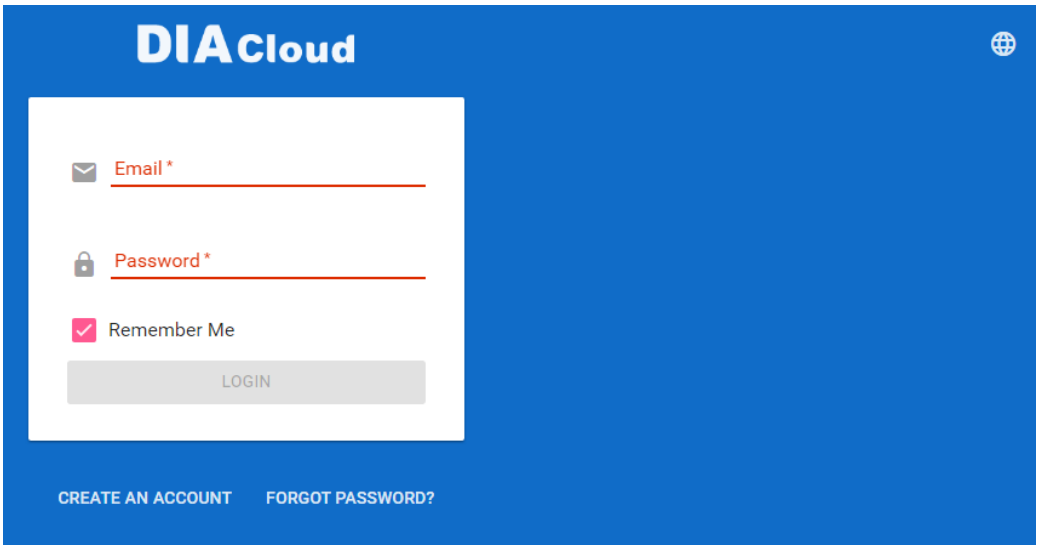
Please confirm that your Firmware version of router meets the requirements in the following table before use:

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

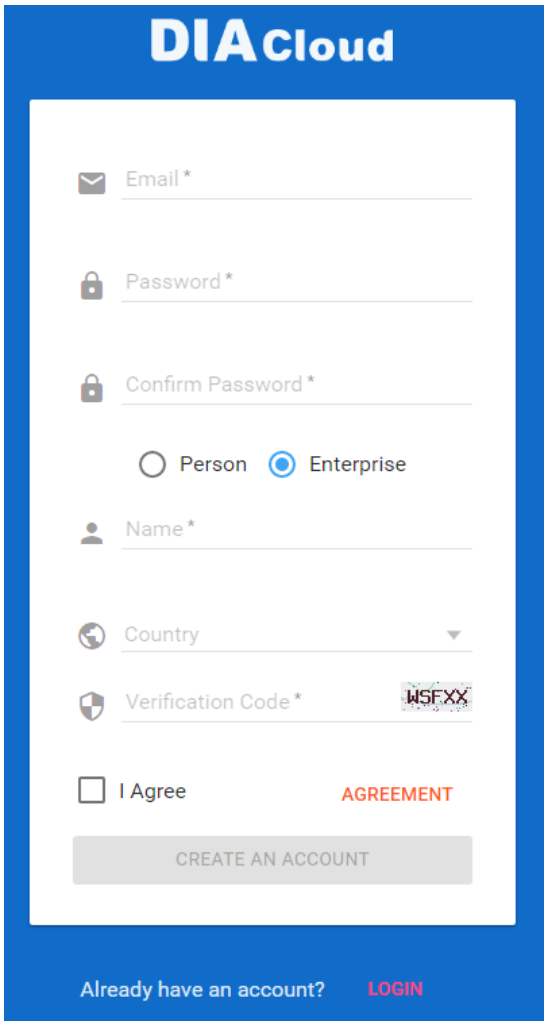
1. Open the DIACloud web page (http://www.DIACloudSolutions.com). If you have got an account, input your account and password in the following page to log in; if you have not got an account, click “CREAT AN COUNT” to register. Then the system will redirect you to the registration page:



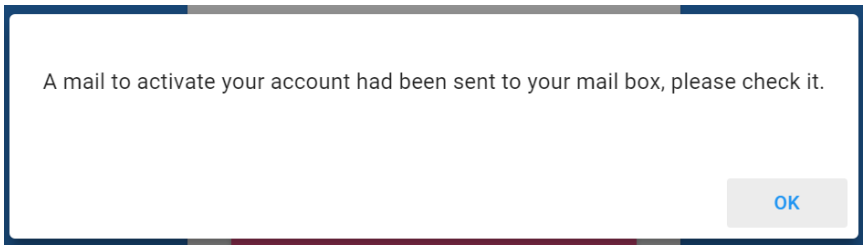
Notice

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

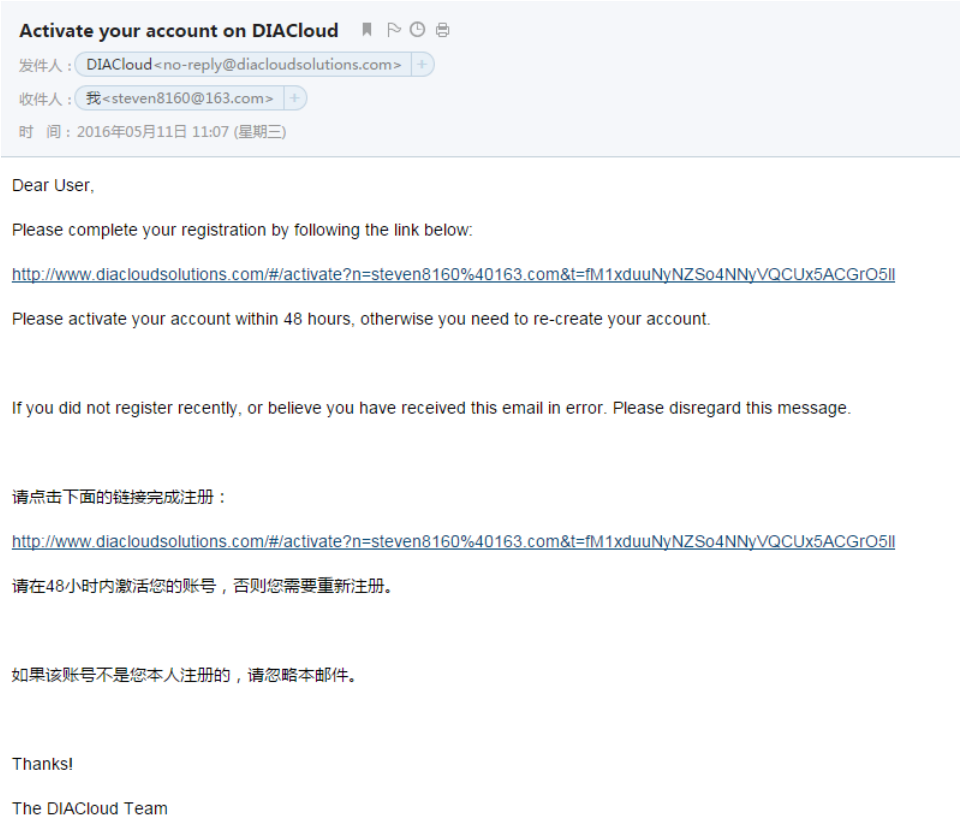
2. Input your email address, password and other relevant information on the registration page. Select “I Agree” and click “CREATE AN ACCOUNT”. PIs insure your region information is correct, otherwise it maybe cause problem in payment when you extend your service.



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 web@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=fM1xduuNyNZSo4NNyVQCUx5ACGrO5II

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=fM1xduuNyNZSo4NNyVQCUx5ACGrO5II

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。

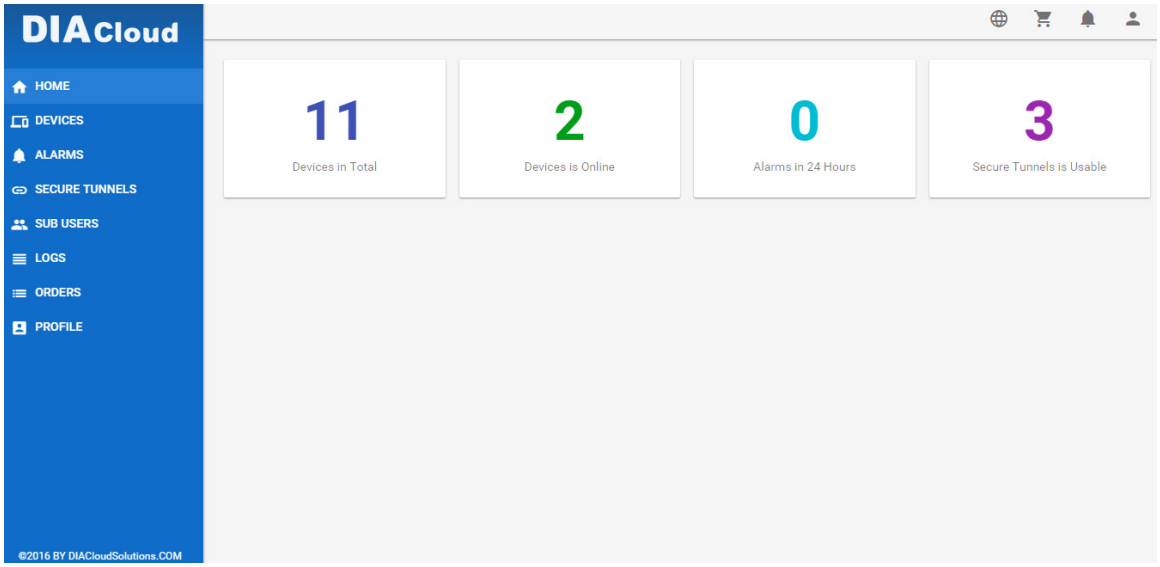
Thanks!

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.

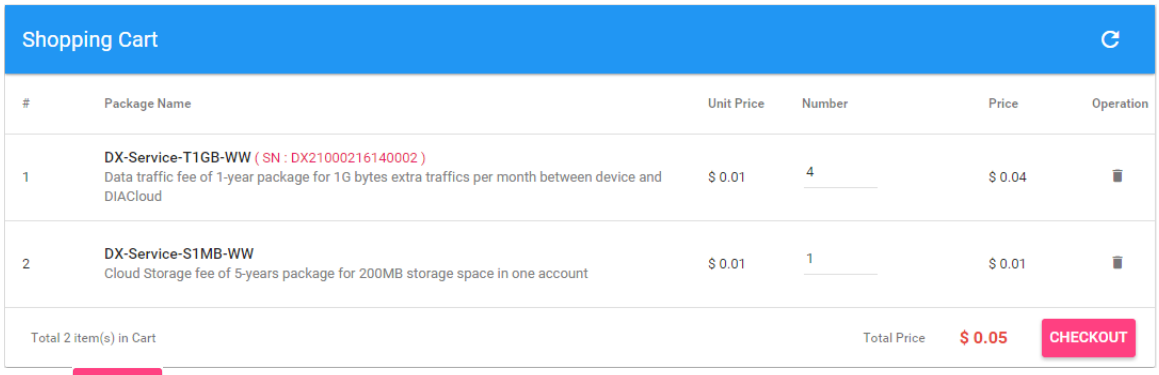


Item	Description
Menu	User can switch to corresponding function through menu on the left.

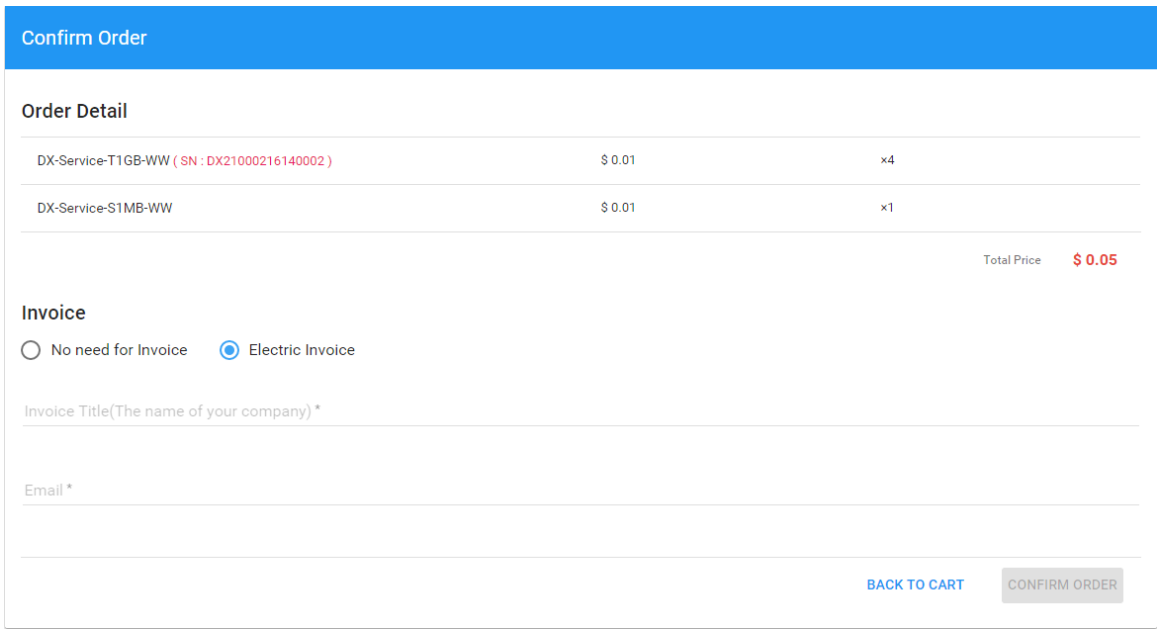
Devices Total	The number of total devices
Devices is Online	The number of total online devices
Alarms in 24 Hours	The number of alarms in Recently 24 hours
Virtual Networks is Usable	It will show the number of Secure Tunnel groups under the account.
	Switching among the Chinese and English
	Show the service package you selected, user can add packeage 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:

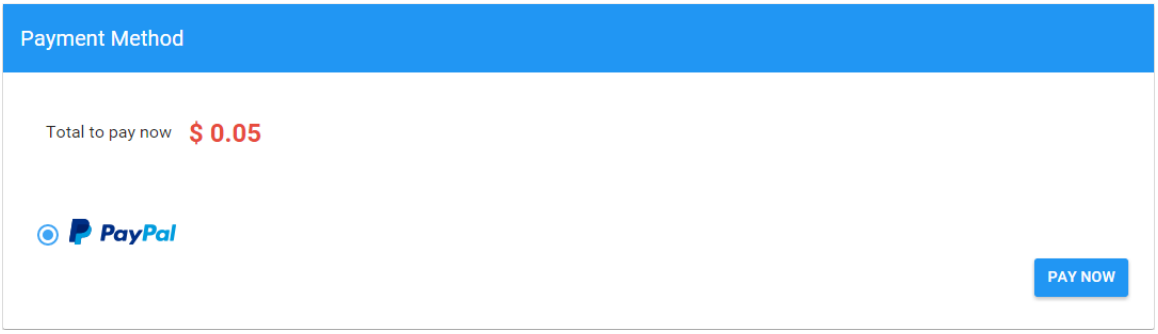
After click , it will show the detail in shopping cart.



Click CHECKOUT to generate an order.

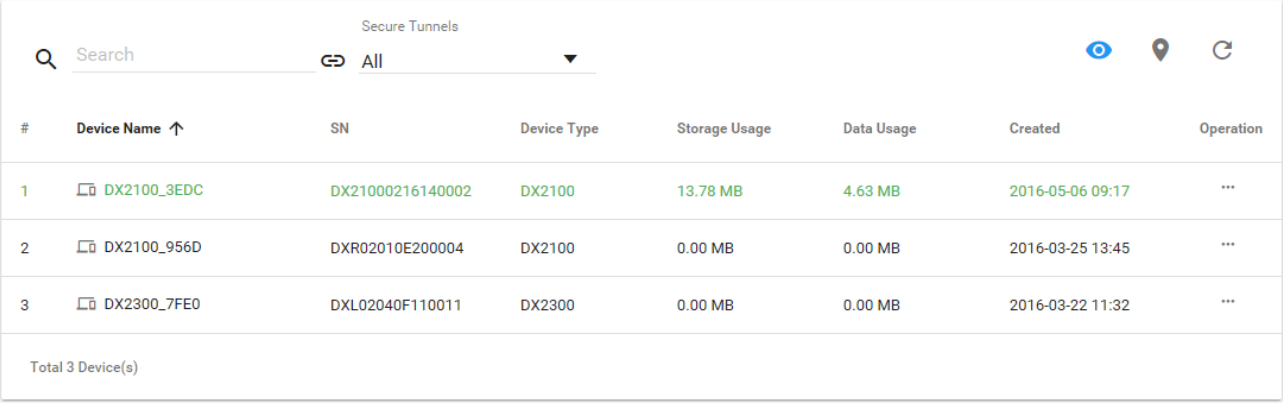


Click CONFIRM ORDER to pay this order.



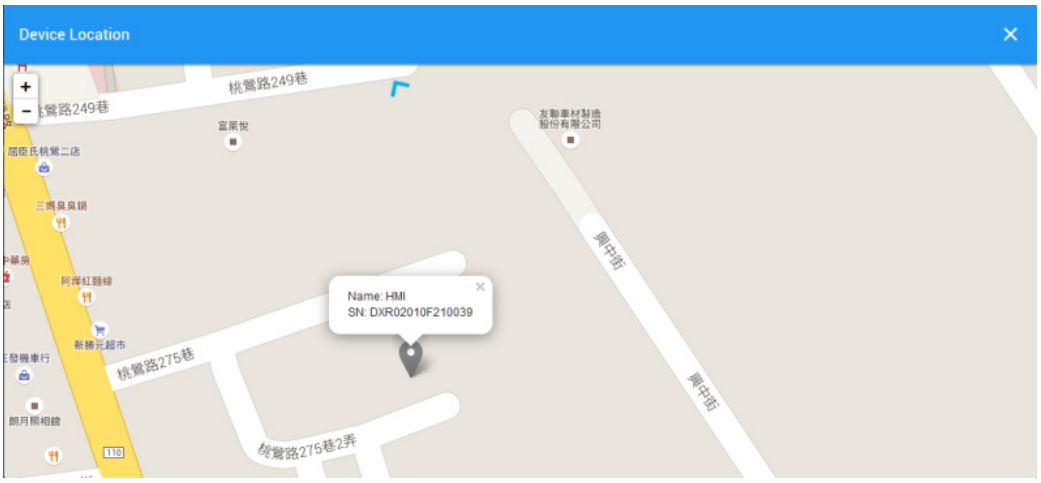
5.2.3 Devices

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 include device’s name, device’s SN, device’s type, storage usage, data usage, the time of binding device. ● Green represents that the device is on-line ● Gray represents the device is off-line.
	● : 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 device.
	Refresh pages
...	Show detail information of the device

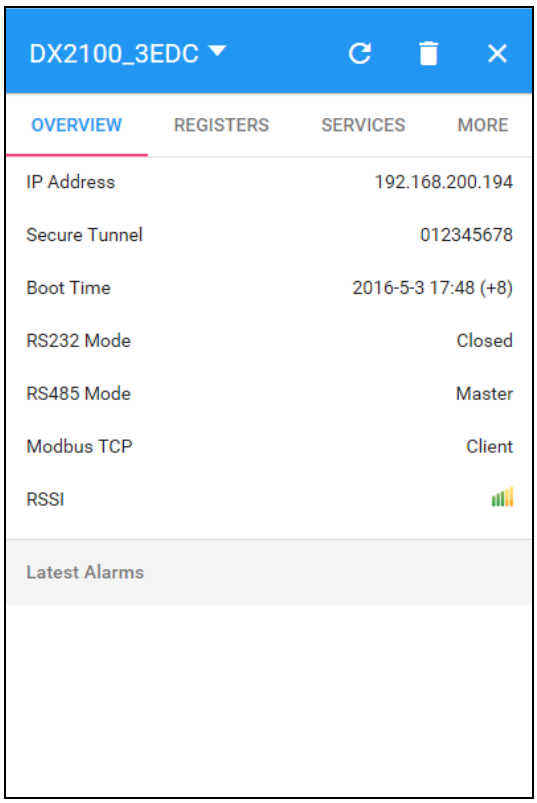
- : It will show relevant position information of device after you click “ ” , which is shown as follows:



It will show the device name and SN of the device after clicking position icon in the map. When there is large number of device of user, it will switch to corresponding device when user clicks blue arrows at the edge of the map.

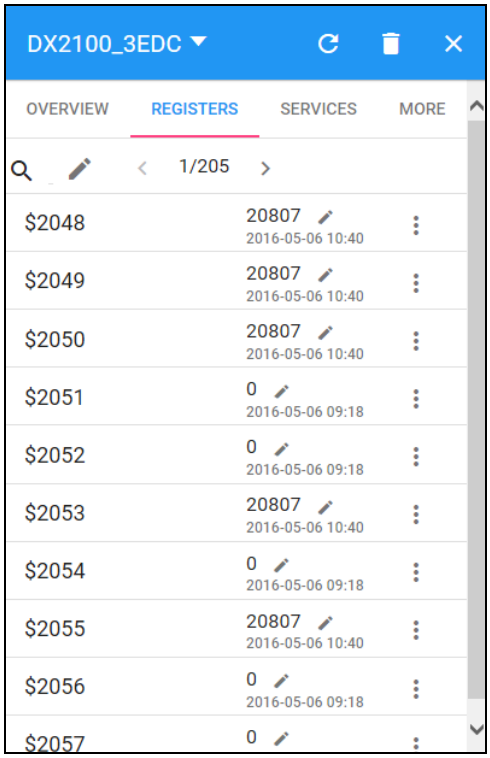
- ··· : More detail information about device will be shown after clicking ··· under the “Operation” at the most right side of device list:

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

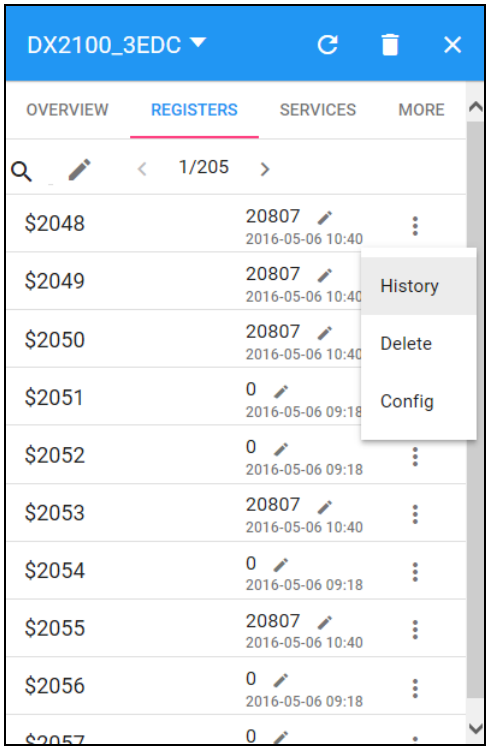


Item	Description
Operation zone of device	It represents that device is on-line if background color is blue, and device is off-line if it is gray. • DX2100_3EDC ▼: Show device names; it can switch device after clicking the drop down arrow. • : Realize refresh of device data on operation page. • : Delete binding relationship between device and the account. Device needs to be un-bund after clicking this button, and user can recover the device by rebinding. • : 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:** it means the IP that has been bound for 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 is being 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 production.

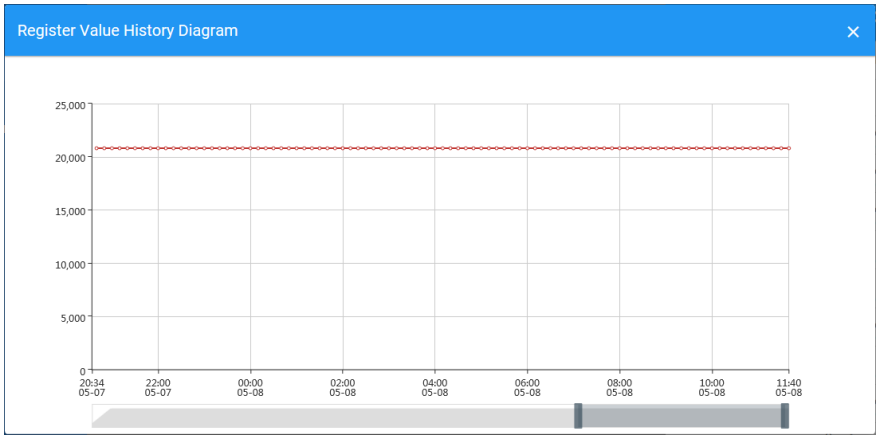


The History and Config options will be shown after clicking ⋮



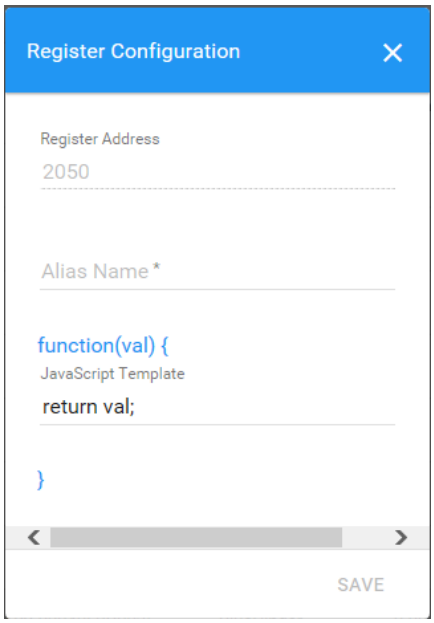
Item	Description
History	It represents trend chart of historical data
Delete	User can delete the all data of this register
Config	User can customize name of register and content returned.

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



Item	Description
Register Value History Diagram	The latest trend chart of value of register;
Time Axis	User can change time scope of historical data by sliding “ ”.

Config : The following information will be shown after clicking “Config”

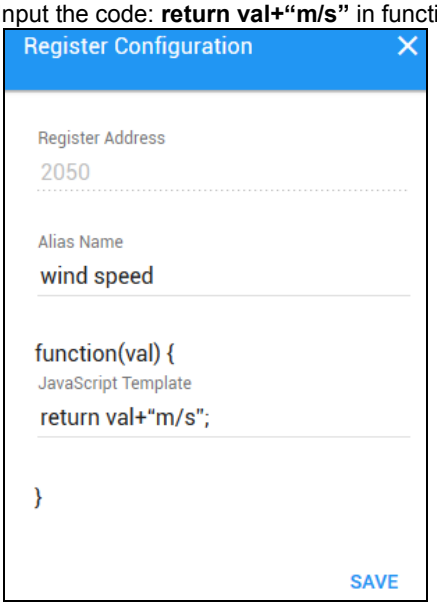


Item	Description
Alias Name	The user can set the name of the register to be displayed in the "Alias Name"
function(val)	function(val) is used for convert the register value, and the grammar of function-supported JavaScript is similar.

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).

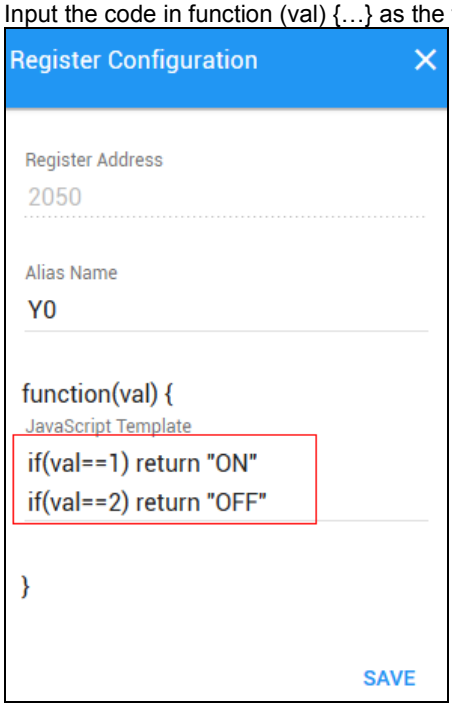
1. Input the code: **return val+“m/s”** in function (val){…} as the following picture.



2. Save the configuration.

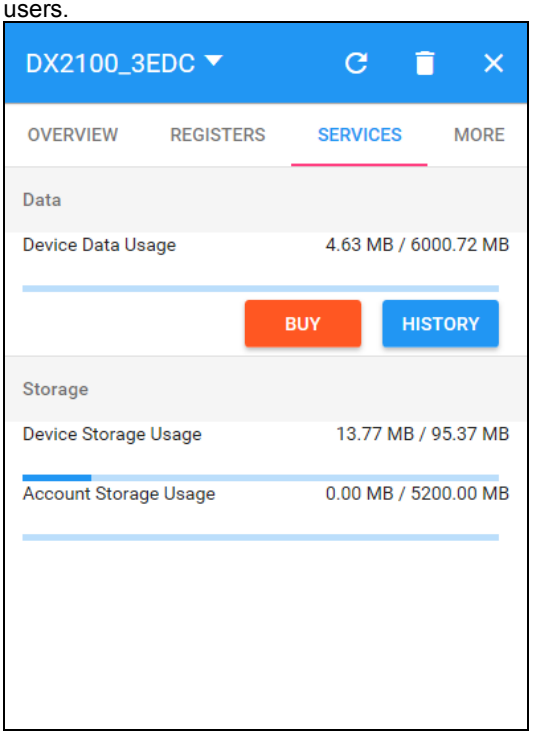
- **Example 2** : If you want to convert the register value to the text such as the register value of 1 shows the text as ‘NO’; register value of 2 shows the text as ‘OFF’

1. Input the code in function (val) {…} as the following picture.



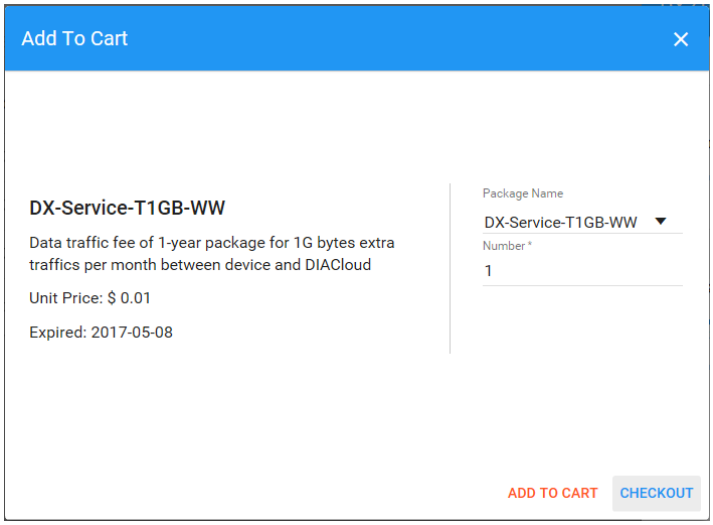
2. Save the configuration.

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

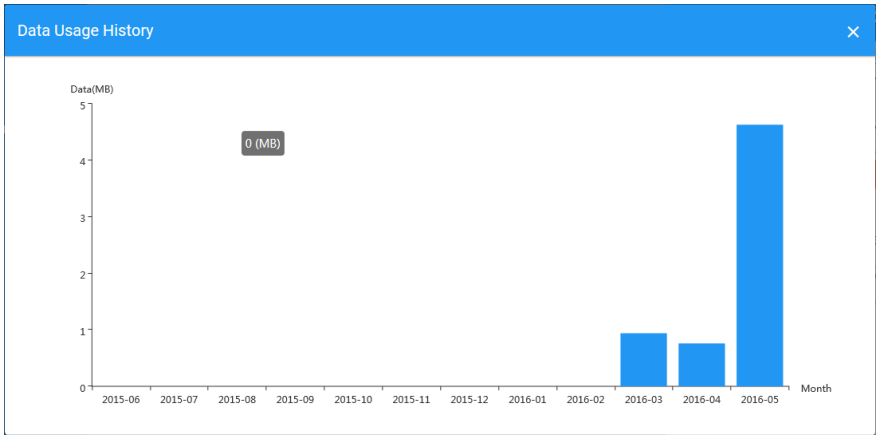


Item	Description
Data	● **Device Data Usage:** Show device traffic usage this month and monthly capacity. ● BUY: User can purchase more traffic package for this device if need. ● HISTORY: Show the Data Usage History in past 12 months.
Storage	● **Device Storage Usage:** Show device storage usage till now and total capacity ● **Account Storage Usage:** Show account and device storage usage till now and total capacity，account storage will share to all device under this account, device storage only use for itself.

1. After Click the BUY, it will show the traffic package select page. User can add a package to cart or pay it direct.



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

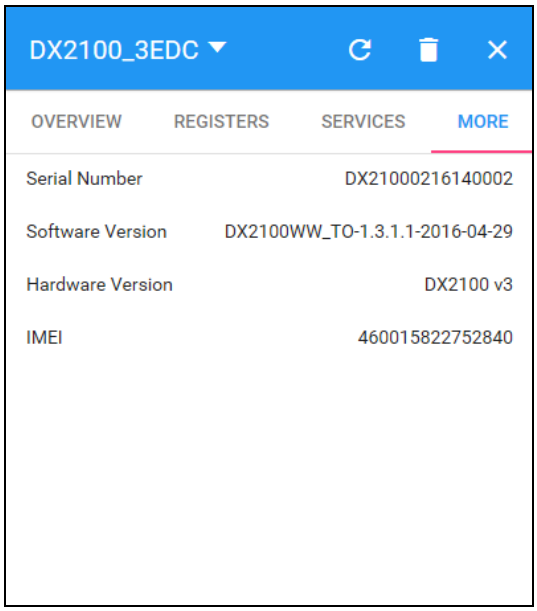


Notice

Traffic package is tie to device and computed separately for each device, user can purchase more for each device

Initial storage package is tie to device, after the device's storage is spent all, it wil charge to account storage. User can purchase more for account only, this means the account storage will share to all devices under this account.

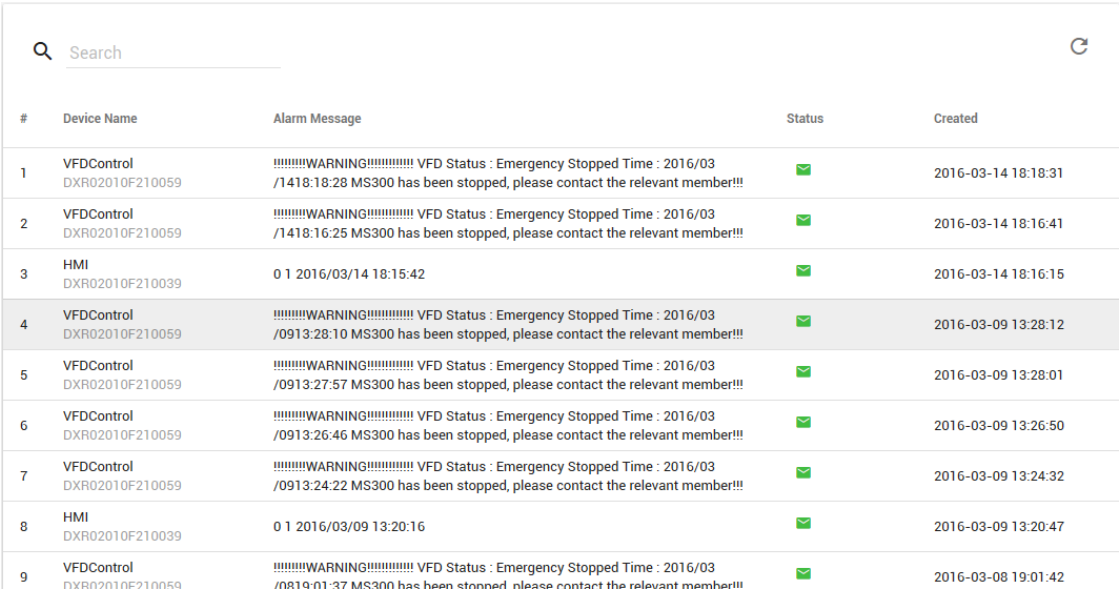
4. **MORE:** This page will show the Serial Number, Software Version, Hardware Version, and IMEI for users.



Item	Description
Serial Number	Serial number of device
Software Version	Version information of software
Hardware Version	Version information of hardware
IMEI	Device Identity which is the only identification number of telephone.

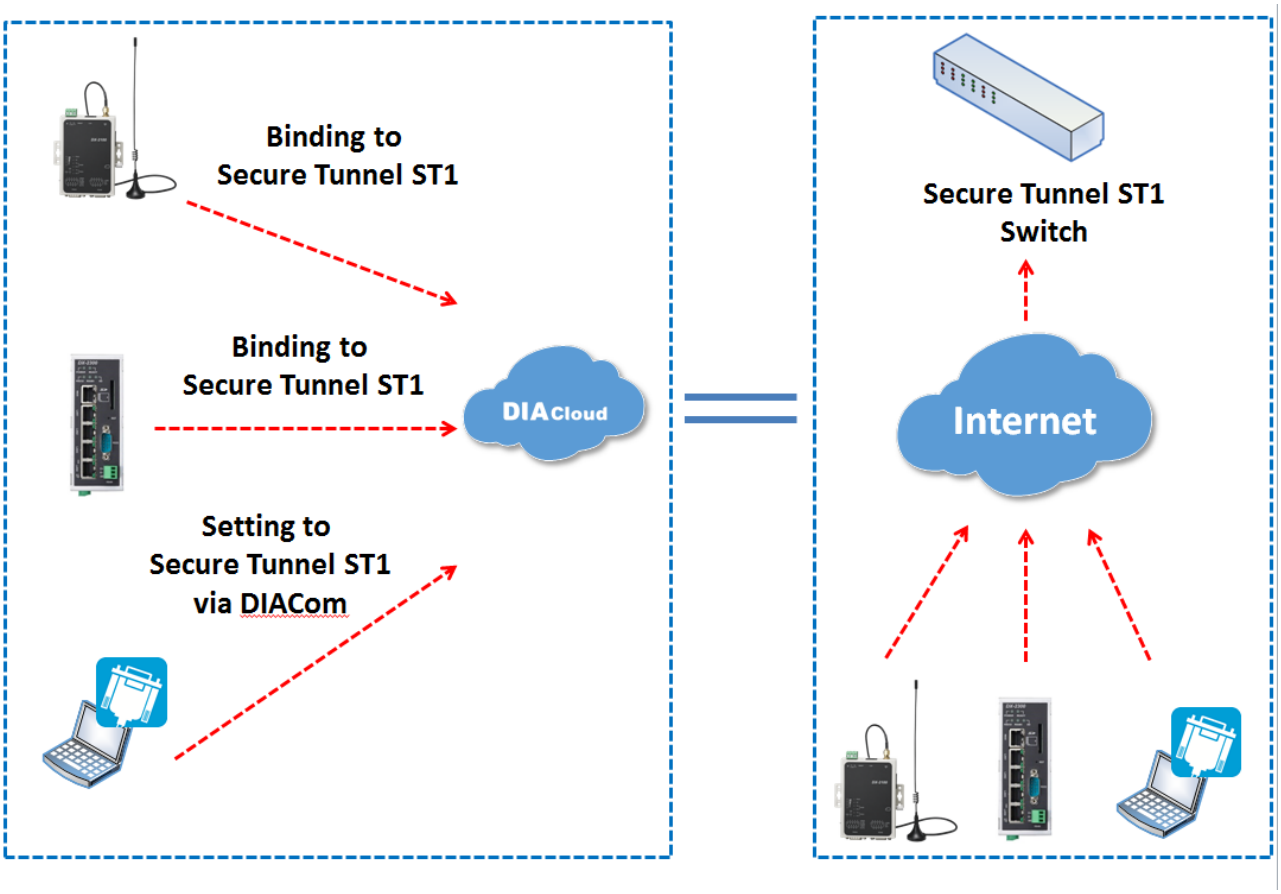
5.2.4 Alarm

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.

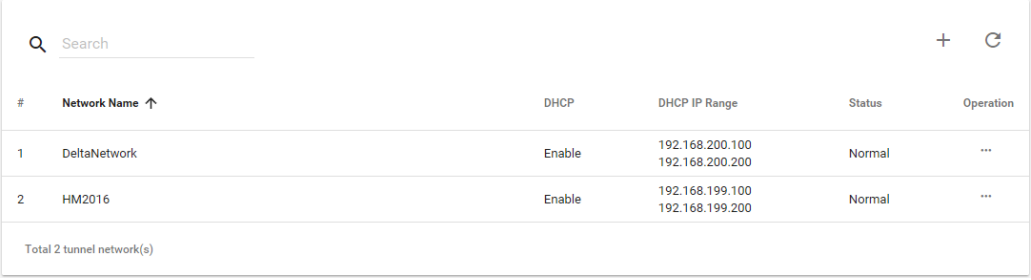


5.2.5 Secure Tunnels

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 adding device 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:

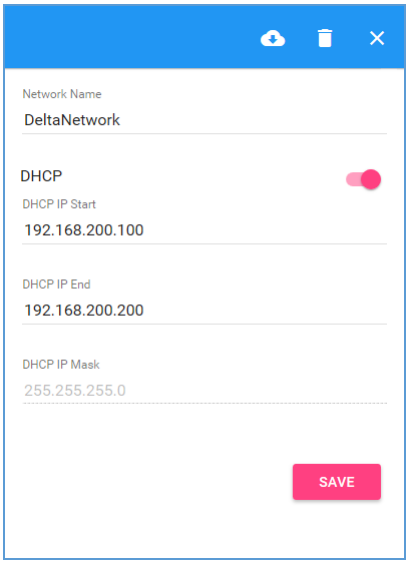


Users can manager the tunnel network in this page. Interface is shown as follows:



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

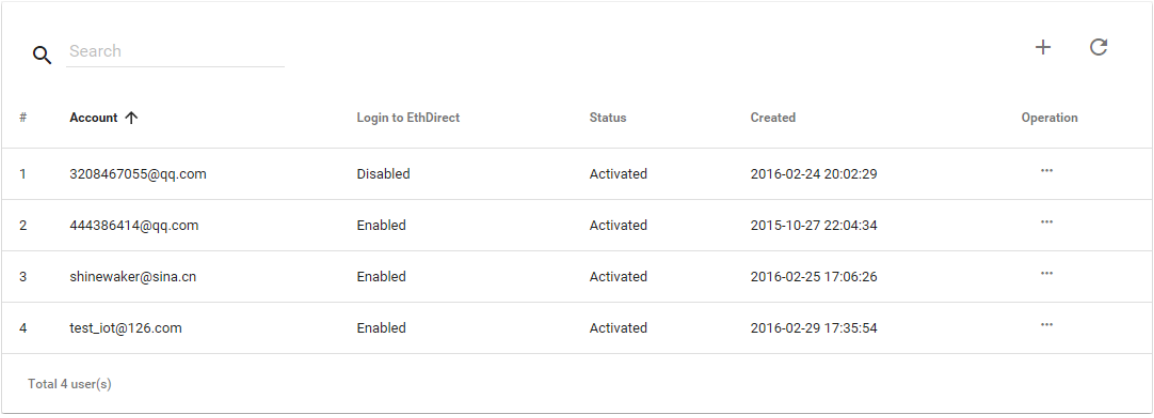
•••	Edit the tunnel network



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	Save the configuration of tunnel network

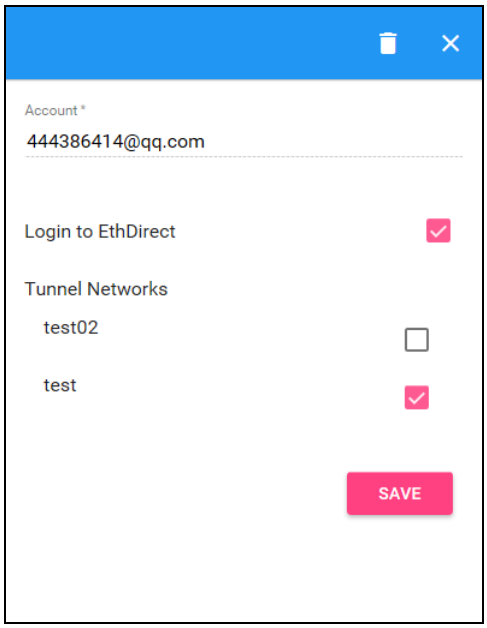
5.2.6 Sub Users

All accounts that are registered through register page of DIACloud (http://www.DIACloudSolutionscom/#/signup) are main accounts. Every main account can create sub-account, 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.

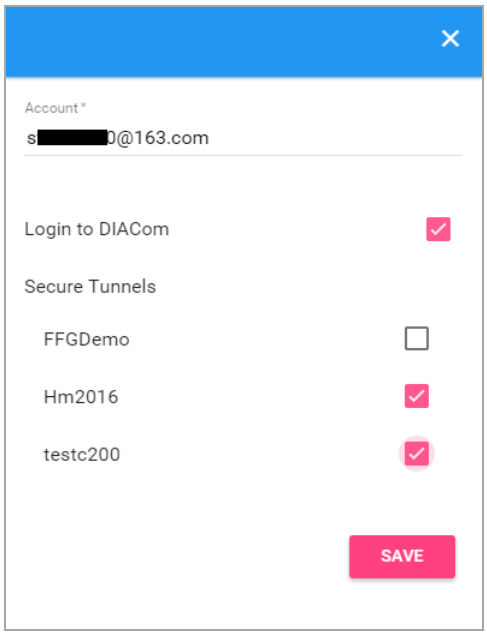
- ··· : User can modify the access control of the tunnel network.



Item	Description
Sub Users Information	● **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 “+” in 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. Goto 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. When user login to DIACloud with main account and the sub user that we created has been activated.

5.2.7 Logs

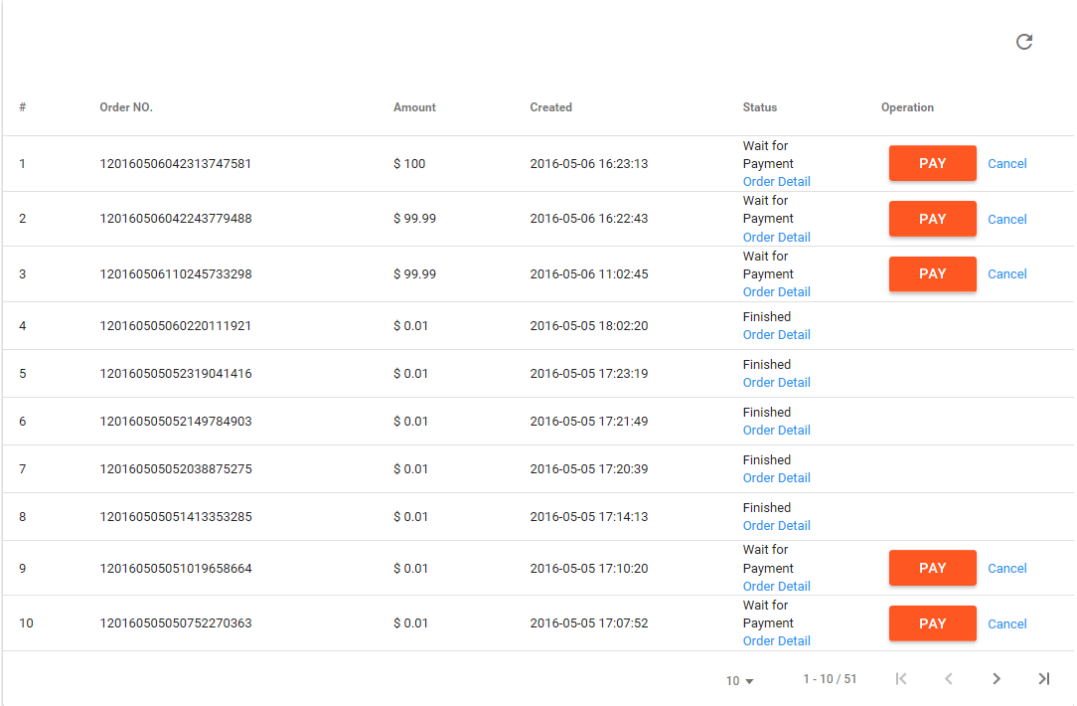
This page will show the web operation information of some users. It includes: login IP, setup of register, API interface call of DIACloud and other information.

#	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, user can check his all orders. Continue to pay for the unpaid orders or cancel the unpaid orders.

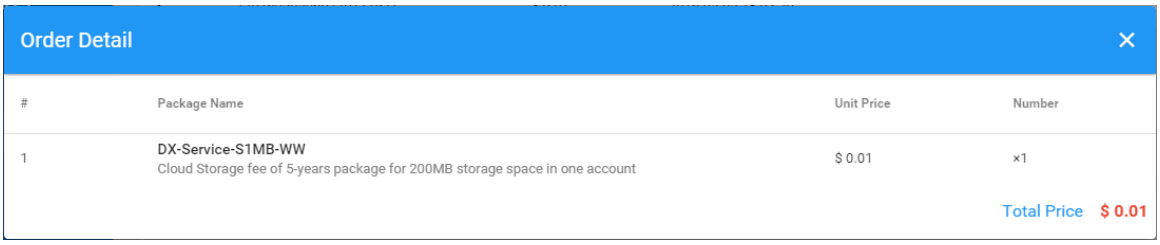


#	Order NO.	Amount	Created	Status	Operation
1	12016050604231374758 1	$ 100	2016-05-06 16:23:13	Wait for Payment Order Detail	PAY Cancel
2	12016050604224377948 8	$ 99.99	2016-05-06 16:22:43	Wait for Payment Order Detail	PAY Cancel
3	12016050611024573329 8	$ 99.99	2016-05-06 11:02:45	Wait for Payment Order Detail	PAY Cancel
4	12016050506022011192 1	$ 0.01	2016-05-05 18:02:20	Finished Order Detail	
5	12016050505231904141 6	$ 0.01	2016-05-05 17:23:19	Finished Order Detail	
6	12016050505214978490 3	$ 0.01	2016-05-05 17:21:49	Finished Order Detail	
7	12016050505203887527 5	$ 0.01	2016-05-05 17:20:39	Finished Order Detail	
8	12016050505141335328 5	$ 0.01	2016-05-05 17:14:13	Finished Order Detail	
9	12016050505101965866 4	$ 0.01	2016-05-05 17:10:20	Wait for Payment Order Detail	PAY Cancel
10	12016050505075227036 3	$ 0.01	2016-05-05 17:07:52	Wait for Payment Order Detail	PAY Cancel

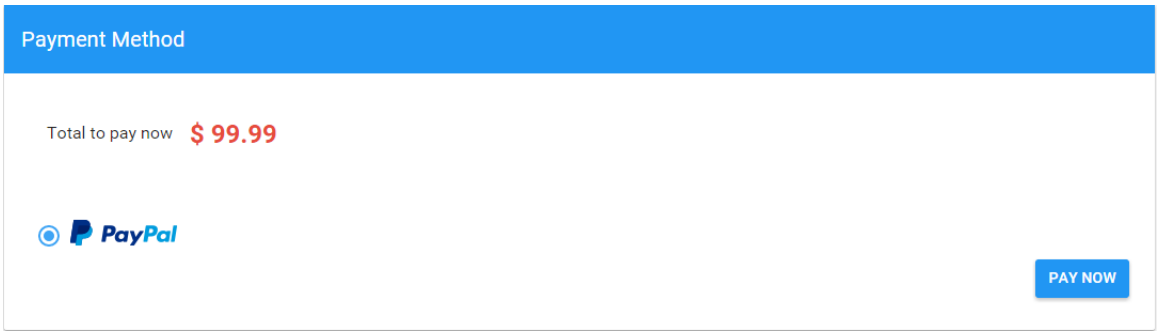
10 1 - 10 / 51

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

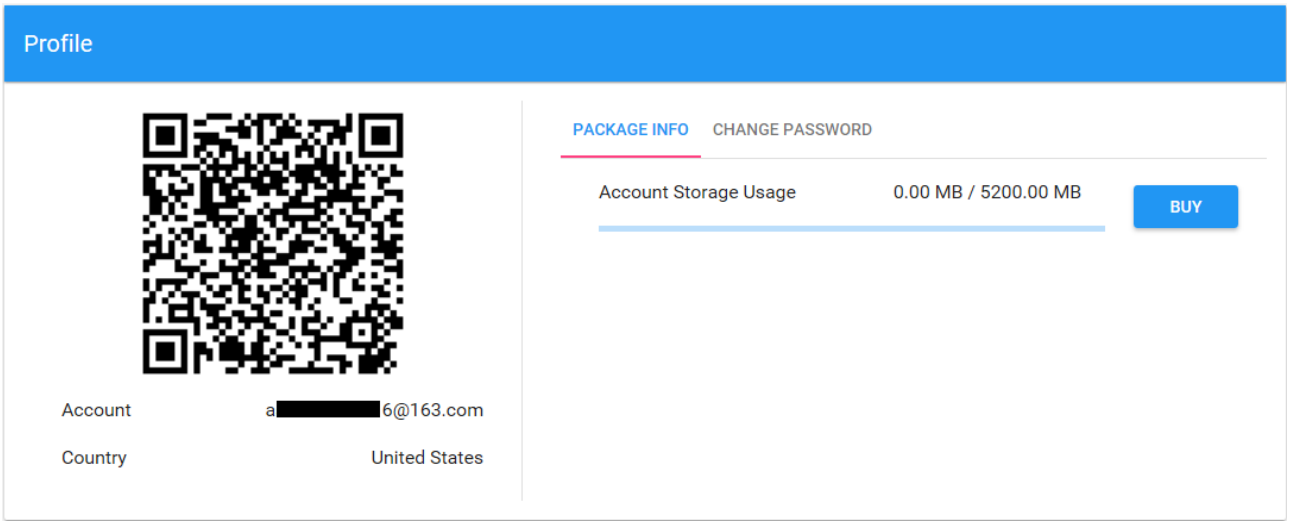


- Pay: Currently, we only support payments through PayPal for Non-Chinese user.



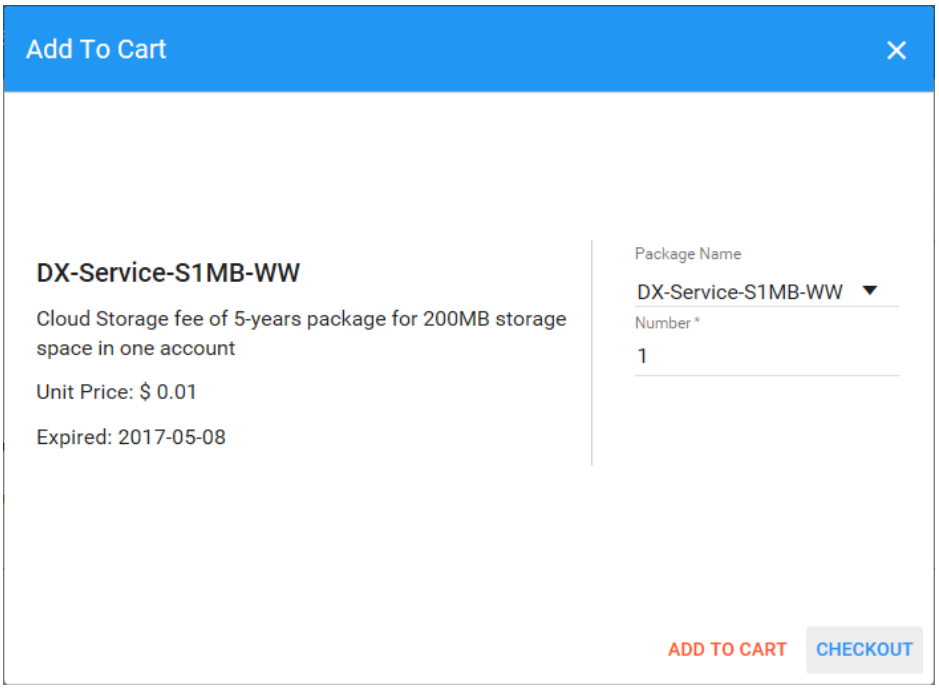
5.2.9 Profile

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

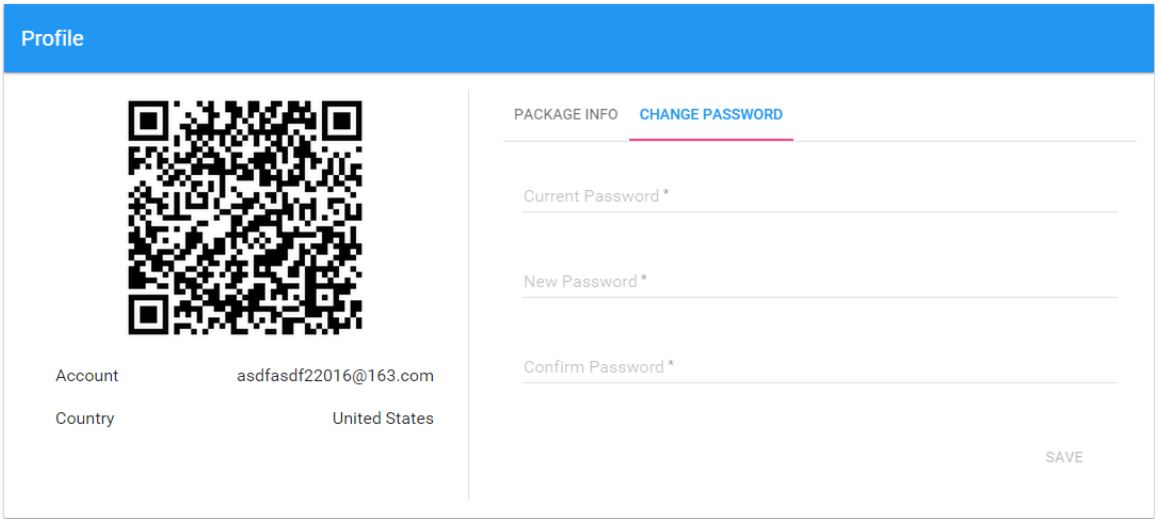


Item	Description
QR Code	You can get the part information of user by using DIACloud APP and scanning QR Code.
Account	The current account information.
Packeage info	• Show account storage usage till now • BUY user can purchase more storage package for this account if need Notice: account storage will share to all device 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.

After Click the BUY, it will show the storage package select page.



Change Password page as below



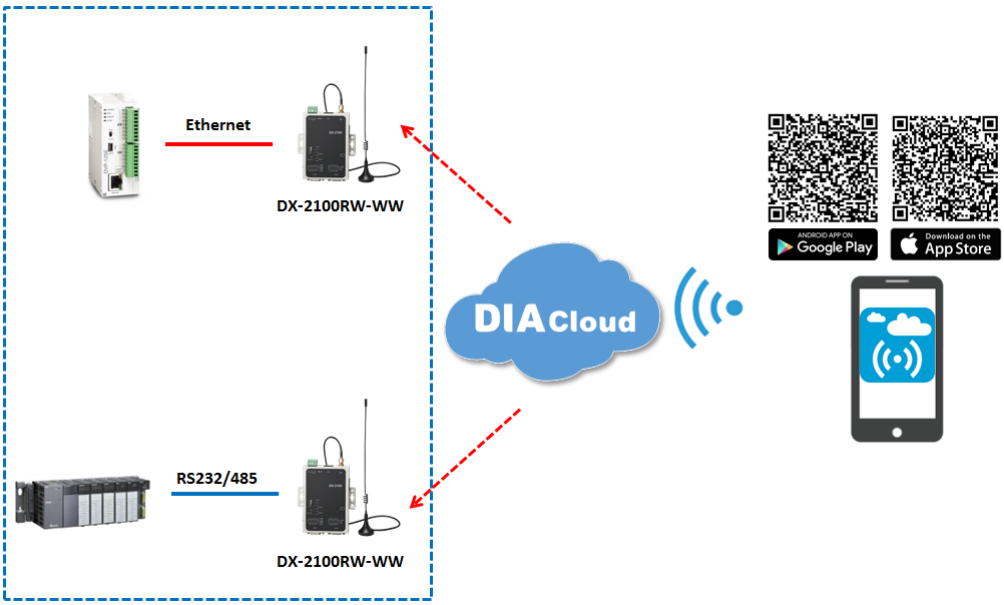
6

Chapter 6 DIACloud APP

Table of Contents

6.1 DIACloud APP Introduction

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 field data collected, 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 Devices Supported

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

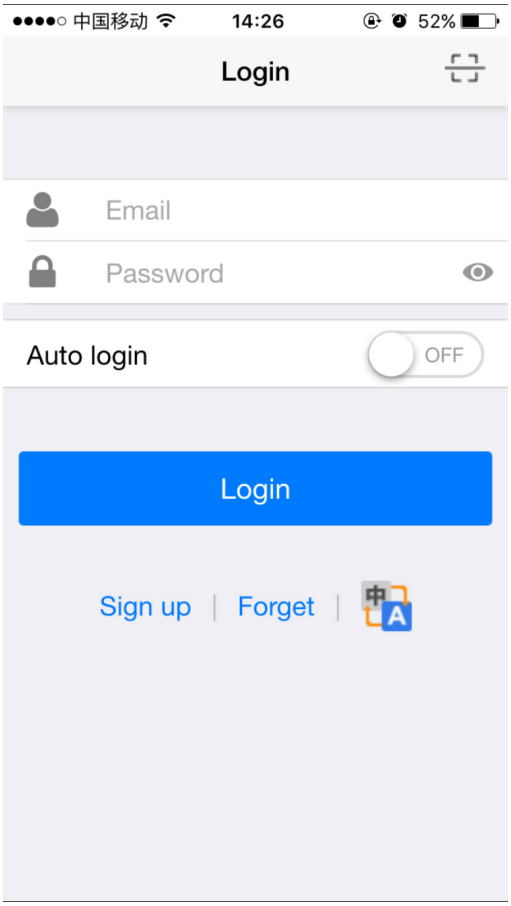
The DIACloud APP is available on Google Play and Apple APP Store.

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

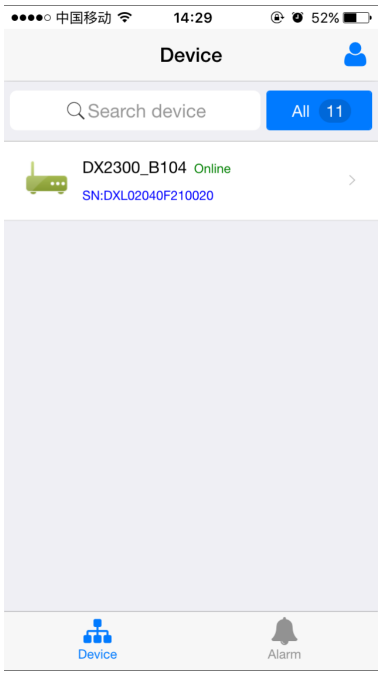
Enter the DIACloud account and password, then click the “Sign in” button to login the APP. Click the “Sign up” to register an account if you don’t have one.



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 user login the APP.

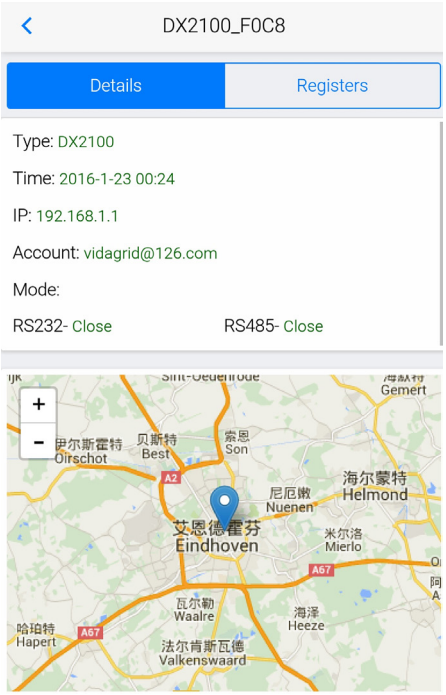


Device tab and alarm tab will be shown in the APP. In the device tab, the device information will be shown, include the value of registers of the remote device. And the value of the register can be changed in the APP as well. In the alarm tab, users can read the alarm messages.

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
Device	Switch to device list page
Alarm	Switch to alarm list page.

6.2.3 Device Details

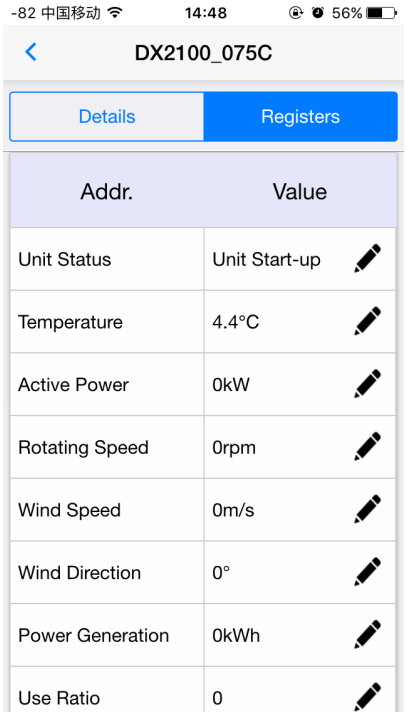
Device details will be shown by selecting a device in the device list.



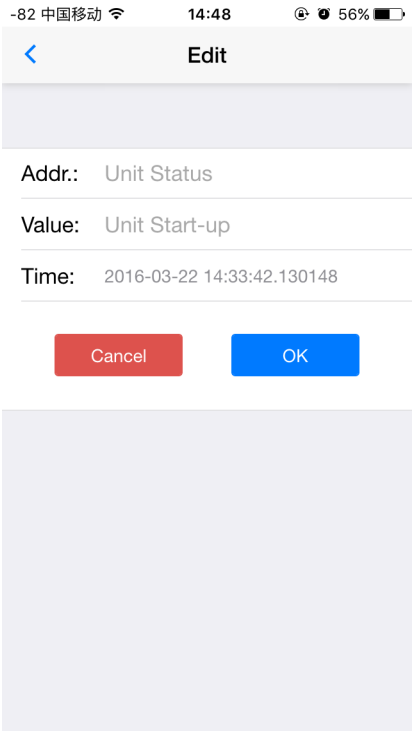
Item	Description
Type	Type of the device
Time	The time when the device is online.
IP	IP Address of the device
Account	DIACloud account activating the device.
Mode	The working mode of RS485 and RS232. ● **RS232:** Transparent transmission mode or Slave mode ● **RS485:** Transparent transmission mode / Slave mode / Master mode
Map	Showing the location of the device on the map

6.2.4 Registers View

By selecting the “Registers” table, the name, value and last change time of the register will be shown. The information can be refreshed by pulling down the APP. When there are a lot of registers, more registers can be shown by pulling up the App.



Click icon to 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.