Digitized Automation for a Changing World

Industrial LTE / WAN DIACloud Router DX-2400L9 Series User Manual

www.deltaww.com

Industrial LTE/WAN DIACloud Router DX-2400L9 Series User Manual

Revision History

Version	Revision	Date
1st	The first version was published.	2023/11/14

Industrial LTE/WAN DIACloud Router DX-2400L9 Series User Manual

Table of Contents

Chapter 1 Product Introduction

Chapter 2 Basic Application

Chapter 3 Functions

Chapter 1 Product Introduction

Table of Contents

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.

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 RED 2014/53/EU. The test record, data evaluation and DX-2400L9 configurations represented herein are true and accurate under the standards herein specified.

Test Items:

EN 301511 V12.5.1(2017-03)
EN 50385:2017
EN 301 908-2 V13.1.1
EN 301 908-13 V13.1.1
EN 301 908-1 V13.1.1
EN 301 489-1 V2.2.3 (2019-11)
EN 301 489-52 V1.2.1 (2021-11)
EN 55032: 2015+A11:2020,Class A
EN 55035: 2017+A11:2020
EN 61000-6-4: 2007+A1:2011
EN IEC 61000-6-4: 2019 /IEC 61000-6-4: 2018 ED.3.0
EN 61000-6-2: 2005+AC:2005
EN IEC 61000-6-2: 2019 /IEC 61000-6-2: 2016 ED.3.0
EN 61131-2:2007 (Zone A & B)
EN IEC 62368-1:2020+A11:2020

Frequency Information for Europe area

Radio	Description	Frequency	Max Output Power E.I.R.P
GSM	GSM 900	880.2~914.8MHz	31.18dBm
	DCS 1800	1710.2~1784.8MHz	29.25dBm
WCDMA	Band I	1920-1980 MHz	22.19dBm
	Band VIII	880-915 MHz	23.26dBm
LTE	Band1	1920-1980 MHz	21.63dBm
	Band 3	1710-1785 MHz	21.60dBm
	Band 7	2500-2570 MHz	22.18dBm
	Band 8	880-915 MHz	23.09dBm
	Band 20	832-862 MHz	22.93dBm
	Band 28	703-748 MHz	22.56dBm
	Band 38	2570-2620 MHz	22.58dBm
	Band 40	2300-2400 MHz	21.85dBm

設備天線輸出增益(NCC)

廠牌/製造商	型號	天線型式	接頭型式	增益(dBi)	
Master Wave Technology C0.,Ltd	98122ZSAF000	Monopole	SMA Plug	WCDMA I	-1.0
				WCDMA VIII	0.0
				LTE B1	-1.0
				LTE B3	-1.0
				LTE B7	-1.0
				LTE B8	0.0
				LTE B28	0.0
				LTE B38	-1.0
				LTE B41	-1.0

限用物質含有情況標示(BSMI)

設備名稱：工業級 LTE/WAN 雲端路由器，型號（型式）：DX-2400L9 Equipment name Type designation (Type)						
單元Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
金屬部件 (Metal Parts)	—	○	○	○	○	○
電路模組 (Circuit Modules)	—	○	○	○	○	○
塑膠和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	○	○
電源元件 (Power Assemblies)	—	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

備考 3. 〝—〞係指該項限用物質為排除項目。

Warning

⚠	減少電磁波影響，請妥適使用。
⚠	電波功率密度MPE 標準值：0.045 mW/cm^2，送測產品實測值：0.045 mW/cm^2，建議使用時設備天線至少距離人體 20 公分。
⚠	為避免電磁干擾，本產品不應安裝或使用於住宅環境。
⚠	This equipment should be installed in a place where access is restricted. Restricted places are places that can only be accessed through special tools, locks, and keys or other security means.
⚠	The product is open-type, indoor use at PD 2, ambient up to 75°C and 2000m in altitude. Clean with a dry cloth for the device and label. If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.
⚠	There will be a warning sign in an obvious position near the heat source part.
⚡	Powered only by SELV (Safety Extra Low Voltage) or by a power source assessed according to UL 61010-1, 61010-2-201, or UL 62368-1 for LE (Limited Energy) or LPS (Limited Power Source) double-insulated power supply.

1.1 Product Overview

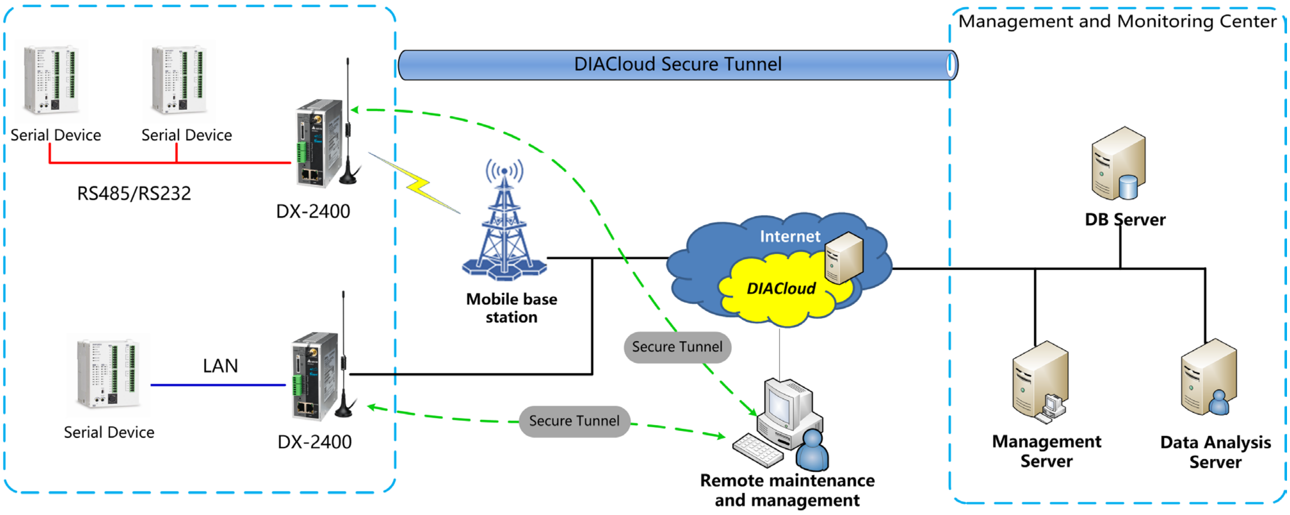
The DX-2400L9 is an industrial router that supports multiple mobile networks, including LTE, DC-HSPA+, UMTS, EDGE, GPRS, and GSM. It can connect to the Internet and DIACloud services via both Wide Area Network (WAN) and cellular network connections, with configurable network usage priority. Additionally, this product is equipped with various application interfaces, including Ethernet interfaces, RS232 serial interfaces, and RS485 serial interfaces, to meet a wide range of user application needs.

The product supports DIACloud platform services, which enable convenient and efficient point-to-point connections with the router, secure and reliable data transmission, remote device management and configuration, remote firmware upgrades, remote maintenance, and more. This helps users save on equipment maintenance costs.

The product finds wide applications in areas that require mobile network connectivity, including industrial automation, smart homes, intelligent buildings, smart grids, mobile video surveillance, smart self-service solutions, intelligent transportation, and other fields.

1.1.1 Network Design

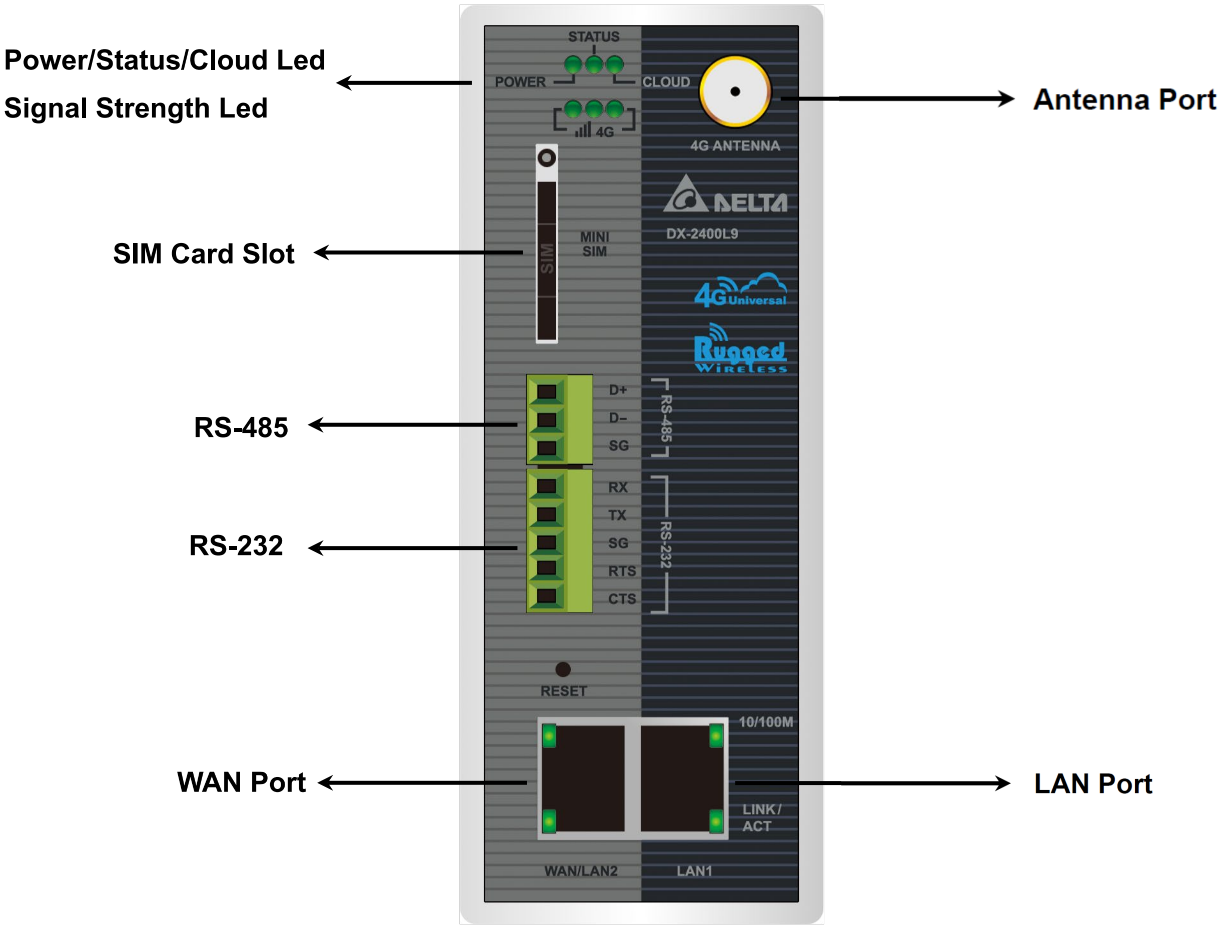
Users can connect smart devices from different locations to the internet through the DX-2400L9 cloud router, establishing secure and reliable data transmission through point-to-point connections. This approach saves on the operational and maintenance costs of VPN devices. Administrators can remotely and in real-time check data and monitor devices through web browsing or a mobile app.



1.1.2 Features

- Supports various LTE FDD and LTE TDD frequency bands, including LTE TDD bands B38/B39/B40/B41 and LTE FDD bands B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28.
- It is downward compatible with WCDMA (B1/B2/B4/B5/B6/B8/B19) and GSM (850/900/1800/1900MHz) networks.
- It can automatically redial when the connection is lost.
- It can be configured to prioritize internet connections using WAN and mobile networks.
- It offers dual RS232 and RS485 ports as well as LAN port interfaces to meet various application needs.
- It includes a built-in watchdog timer to ensure system stability.
- Built-in RTC(Real-time clock) with the ability to automatically connect to a specific NTP server for time synchronization. (Users are unable to set the NTP server manually.)
- Firmware upgrades can be performed locally and remotely.
- Supports firewall features such as Stateful Packet Inspection (SPI), Denial of Service (DoS) prevention, Network Address Translation (NAT), port triggering, port mapping, IP address filtering, MAC address filtering, URL filtering, DHCP server, Dynamic DNS, static routing, and Demilitarized Zone (DMZ).
- Supports various protocols, including TCP/IP, UDP, ICMP, DHCP, HTTP, DNS, SSH, and more.
- Supports Modbus TCP, Modbus ASCII, and Modbus RTU protocols.
- Supports Mitsubishi MC and Siemens ISO TCP protocols.
- It can manage scheduled tasks.
- It provides both local and remote log server services.
- Supports configuration backup, export, and import.
- Supports network traffic monitoring.
- Supports network fault detection and diagnosis.
- It can support local data caching.
- Provides DIACloud services for secure point-to-point data transmission, individual or batch device configuration management, and remote upgrades.
- Supports the standard MQTT protocol, allowing seamless integration with AWS IoT.

1.1.3 Front Panel Ports and LEDs



- **LED Description**

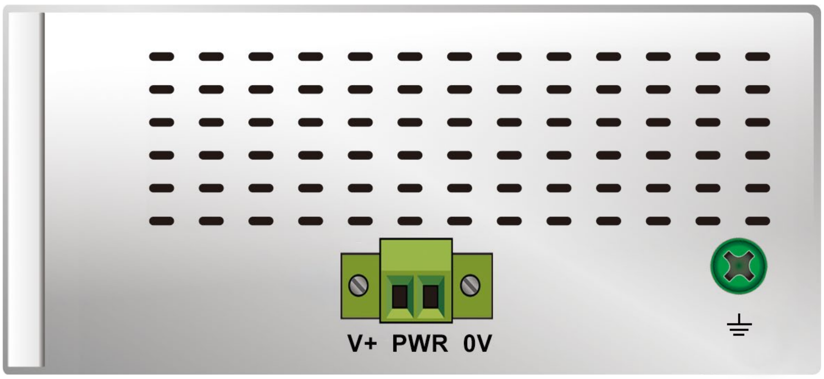
Items	Color	Status	Description
POWER	Green	ON	Power on.
		OFF	Power off.
STATUS	Green	ON	The router is on and ready for use, internet connection is active.
		OFF	The router is off or not receiving any power.
		blinking	The router is on but no active internet connection.
CLOUD	Green	ON	Cloud service is normal.
		blinking (once/s)	Security tunnel connection is normal, but Data Channel service is abnormal or disabled.

		blinking (twice/s)	Secure Tunnel service is abnormal or disabled, but Data Channel service is normal.
		OFF	Unbound cloud account; or Secure Tunnel and Data Channel services are abnormal or disabled.
4G	Green	ON	Operating on a 4G network mode, with 1-3 lights based on signal strength. It is recommended to have at least 2 lights for optimal performance.
		blinking (once/s)	Operating on a non-4G network mode, with 1-3 lights based on signal strength. It is recommended to have at least 2 lights for optimal performance.
		OFF	No network signal available.
WAN/LAN	Green	ON	Operating at a speed of 100 Mbps.
		OFF	Operating at a speed of 10 Mbps.
	Yellow	ON	Ethernet connection is active.
		blinking	Data transmission in progress.
		OFF	No Ethernet connection or not receiving any power.

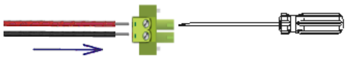
- ## Terminal Description

Item	Terminal	Description
Reset Button	○ **RST**	• **Reboot**: Press and hold the 'Ready' button until it starts flashing within 5 seconds. After releasing, the 'Ready' light will turn off, and the restart process will begin. Wait for approximately 80-90 seconds for the device to complete the reboot. When the restart is complete, a beep sound will be emitted. • **Reset to Factory Default**: Press and hold the button for more than 5 seconds, the 'Ready' light will start to stay continuously lit. After releasing the button, when the 'Ready' light turns off, the device will reset to factory default settings. When the reset is complete, a beep sound will be emitted.

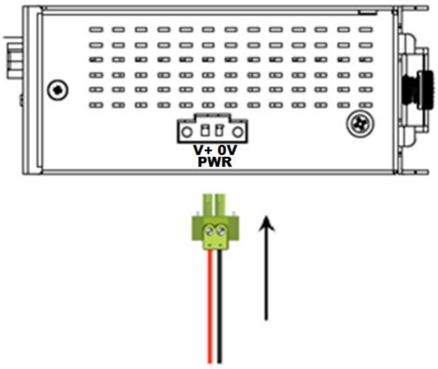
1.1.4 Button Panel



1. Insert the +12 ~ +48VDC direct current (DC) power cable into the terminal socket, ensure that the positive terminal (+) is connected to V+ while the negative terminal (-) is connected to V-.



2. After securely fastening the power cable with a flathead screwdriver, reattach the male plug of the terminal block onto the female socket.

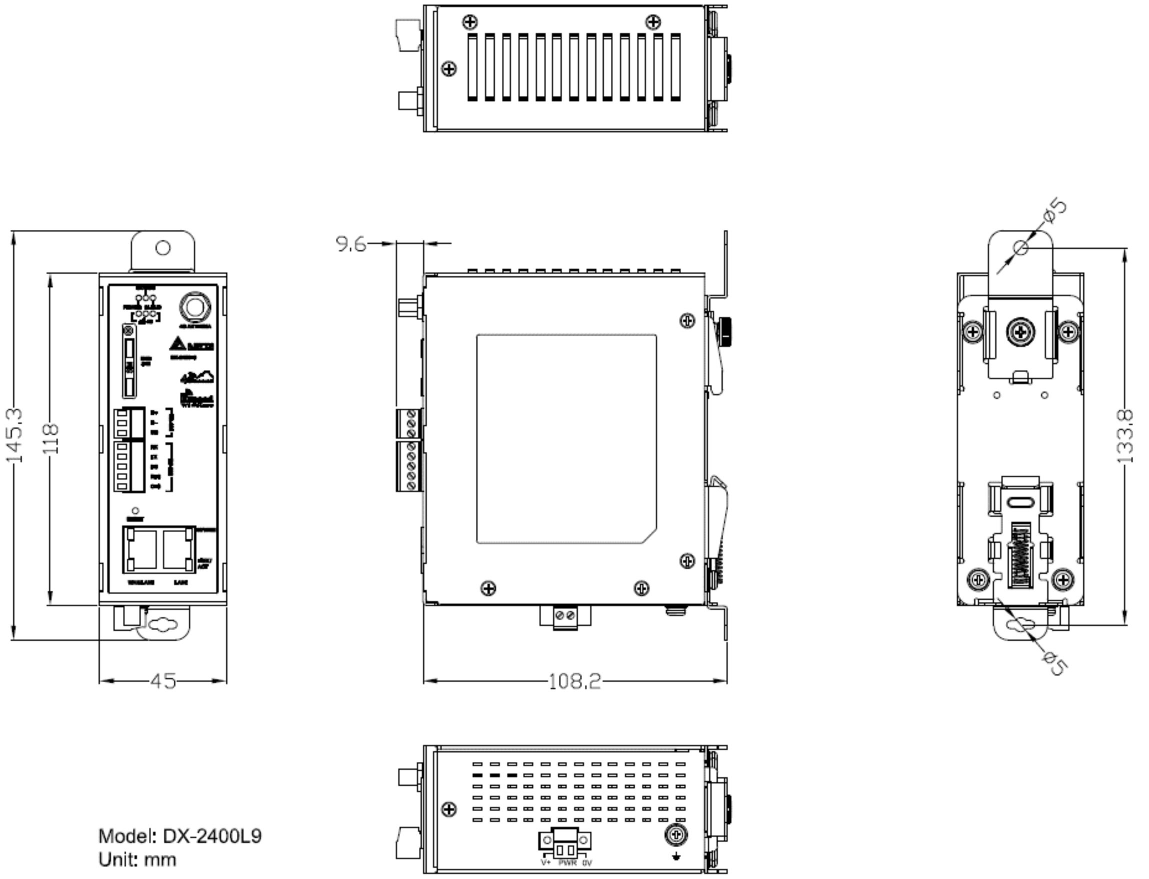


The power input need to use copper wire Min. 85°C, AWG(American Wire Gauge) 16-24, screw torque is 2.5 kgf-cm (2.17 in-lbs).

- **Terminal Description**

Item	Terminal	Description
Power Supply	⏚	Power grounding, the two power grounds are interconnected
	V- V+	• PWR: +12V ~ +48VDC, MAX 0.83A Redundant input. • Power consumption: 3.6 W • Support reverse polarity protection.

1.1.5 Dimension



Model: DX-2400L9
Unit: mm

Shell	IP40 Metal Case (chassis only, excluding all connectors) (Not certified by UL)
Dimension(mm)	145.3H x 45W x 117.8D
Weight(g)	355g

1.2 Installation

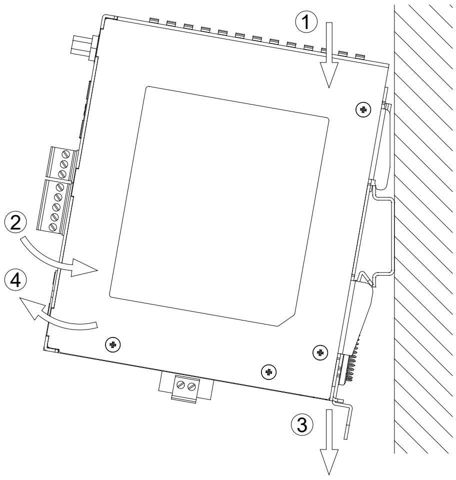
1.2.1 Din Rail Mounting

Din-rail mounting:

Attach the machine's rear hooks into the aluminum rails in the direction indicated by arrow ①, and then press towards the aluminum rails in the direction indicated by arrow ②.

Din-rail removal:

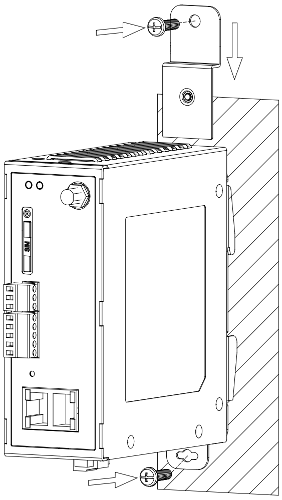
To remove the machine, pull downwards in the direction indicated by arrow ③ and then pull it out in the direction indicated by arrow ④.



1.2.2 Wall Mount Installation

Installation/Removal:

Prepare M4 screws and secure them in the upper and lower hanging bracket screw holes to complete the installation. For removal, simply unscrew the screws.



1.2.3 SIM Card Installation

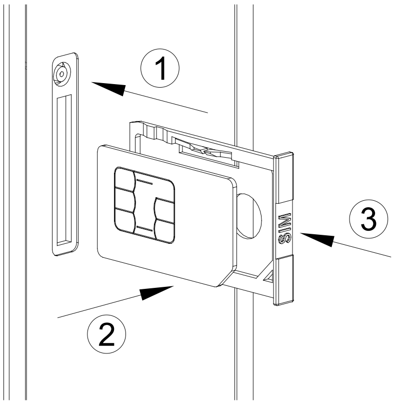
The DX cloud router requires a Mini SIM card (25mm x 15mm) to be inserted into the card tray. If you only have a Micro or Nano SIM, you can use an adapter to convert it into a Mini SIM.

SIM Card Installation:

Step1: Please use a paperclip or a SIM card ejection tool to insert it into the yellow button located next to the tray, push it towards the cloud router, and the SIM card tray will pop out.

Step2: Use a Mini SIM card and place it in the SIM card tray.

Step3: Place the SIM card tray into the SIM card slot.



SIM Card Removal:

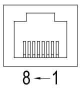
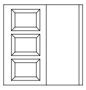
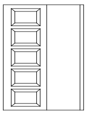
Step1: Turn off the power.

Step2: Insert a paperclip or SIM card ejection tool into the yellow button next to the tray. Push it towards the DX cloud router.

Step3: The tray will pop out, allowing user to remove the SIM card.

⚠Does not support automatic SIM card hot swapping; user must power off the device for SIM card to be recognized.

1.3 Pin Assignment

Pin no.	Ethernet		Pin no.	RS-485		Pin no.	RS-232	
1	TX+		1	D+		1	RX	
2	TX-		2	D-		2	TX	
3	RX+		3	GND		3	SG	
4	-		4	-		4	RTS	
5	-		5	-		5	CTS	
6	RX-		6	-		6	-	
7	-		7	-		7	-	
8	-		8	-		8	-	
9	-		9	-		9	-	

1.4 Package Checklist

The packaging should include the following items. Please check the DX-2400L9 packaging upon opening to ensure that nothing is missing. If you find any items missing or damaged, please contact your local sales representative for support.

1. DX-2400L9 Industrial 4G Cloud Router x 1

2. Quick Installation Guide x 1

3. SMA Antenna (300cm) x 1

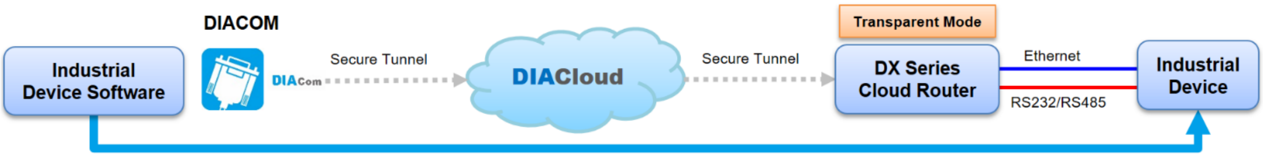
Chapter 2 Basic Application

Table of Contents

2.1 Application

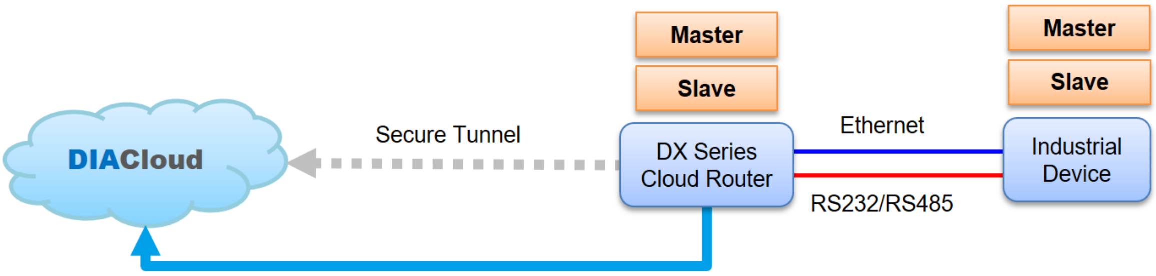
This chapter is an introduction to the basic application process which is divided into cloud storage upload and device remote connection.

- **Device remote connection:** Perform connections in a short period of time via RS485 or Ethernet, such as remote data monitoring, uploading and downloading program remotely. In addition, we would suggest you use DIACloud Restful API to perform long-term or even 24-hour monitoring if required.



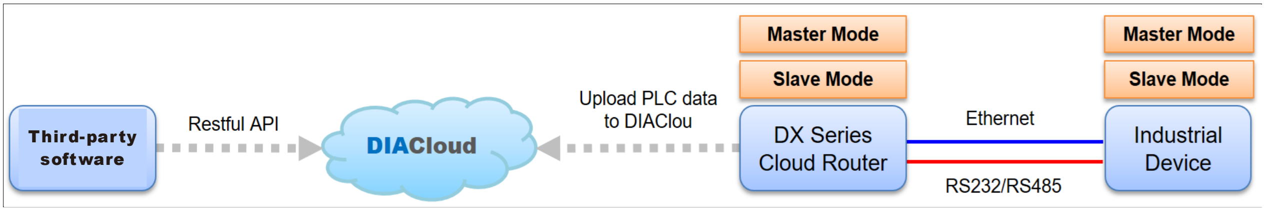
Remote connection function

- **Coud storage upload:** DIACloud Upload device data to the cloud via RS485 or Ethernet so as to monitor device data on DIACloud webpage or APP (Supporting protocols: MODBUS/ MODBUS TCP/ Mitsubishi MC/ Siemens ISO TCP/ OMRON FINS).

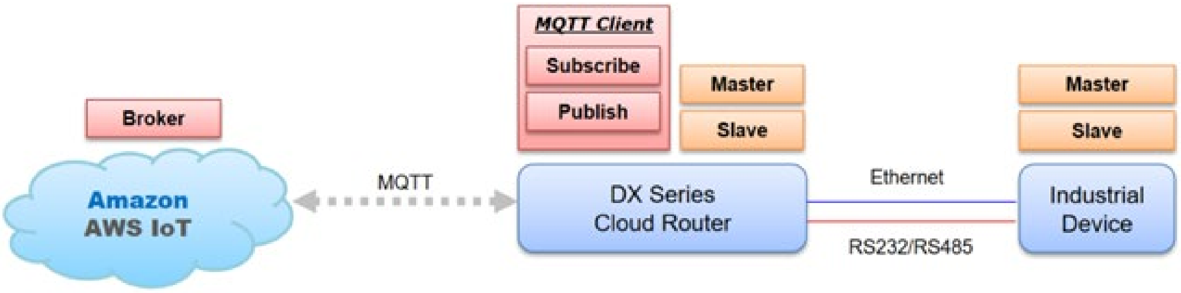


Upload PLC data to DIACloud

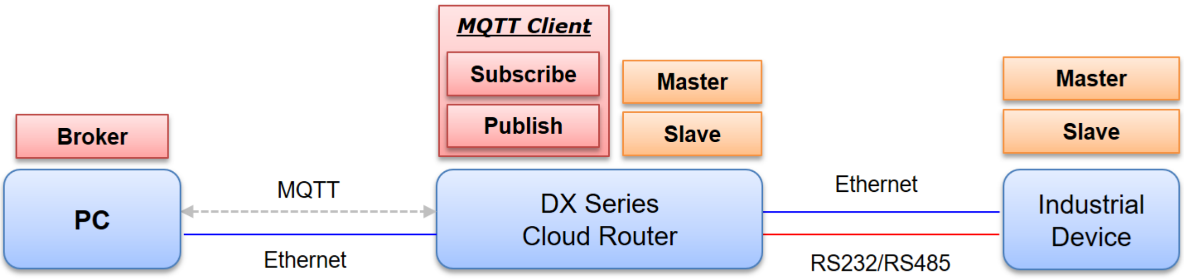
- **Device remote connection (Restful API):** Monitor device data remotely with a custom software, which need to support read-write Restful API.



- **Cloud Router MQTT Connection to AWS IoT Application:** Establishes a connection with the AWS IoT Broker, where the DX Cloud Router retrieves industrial equipment data and use MQTT for data exchange with the AWS IoT Broker.



- **Local MQTT Connection Application:** Establishes a connection with a local broker, where the DX Cloud Router retrieves industrial equipment data and uses MQTT for data exchange with the broker.



2.2 Basic Configuration

2.2.1 Operating Environment

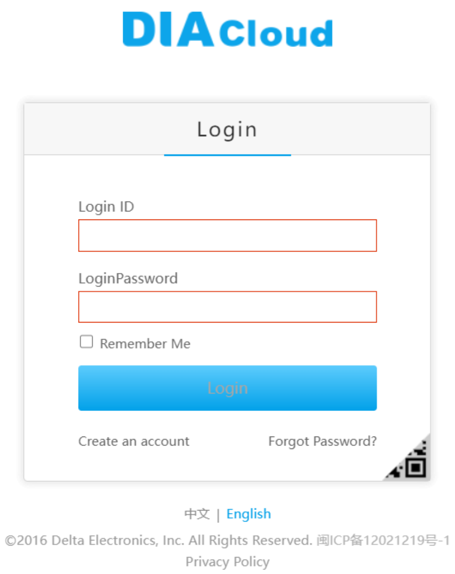
The following browsers are suggested to use when open DIAcloud(https://diacloudsolutions.com) or DX router webpage.

- Google Chrome
- Microsoft Edge

2.2.2 Register an Account

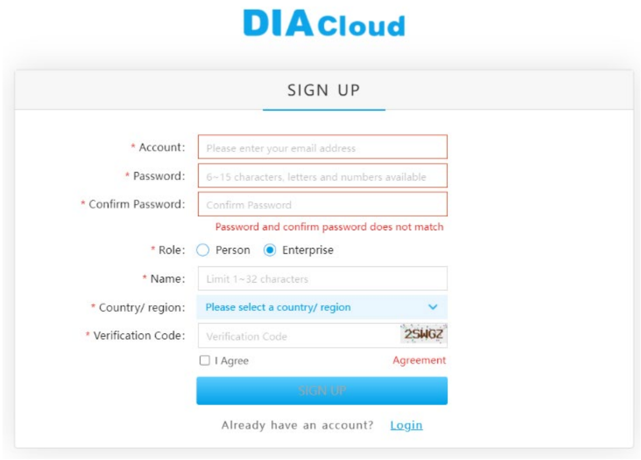
Bonding between DIACloud accounts and devices determine who would be privileged to access device data. Once the device is bonded to the account, only persons who have the account and its sub-account are allowed to remotely access the device and all the uploaded device data. If you haven't had a DIACloud account, please register by the following steps:

1. Open DIACloud website(http://www.DIACloudSolutions.com) and click "Create an account", then the register page would be displayed.



©2016 Delta Electronics, Inc. All Rights Reserved. 闽ICP备12021219号-1

2. Enter your Email address, password, and other information. Continue to agree the policies by checking the checkbox, then click "Create an Account."



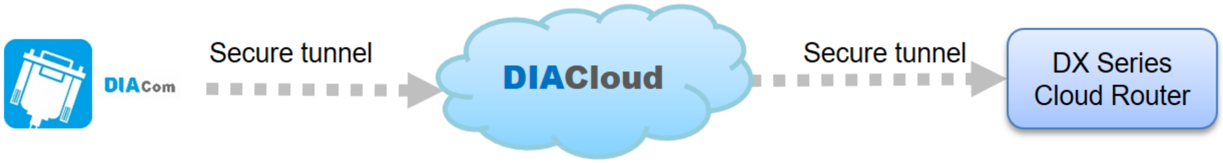
Password and confirm password does not match

* Role: ○ Person ● Enterprise

3. You will receive an activation email(no-reply@DIACloudSolutions.com) and open it to complete the account activation procedure.

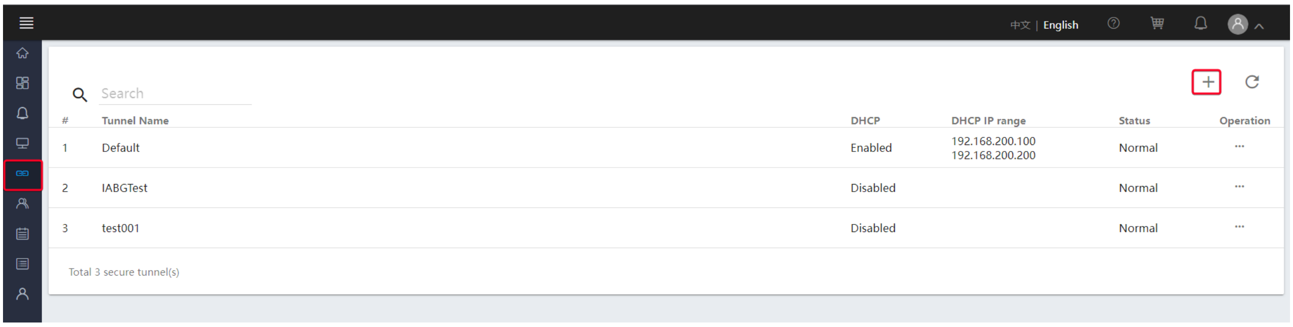
2.2.3 Security Tunnel Setting

Set a security tunnel between DX routers and DIACOM, establishing communication between industrial devices under cloud router devices and computers with DIACOM remotely installed. You are allowed to create different security tunnels for different device groups and devices in each tunnel would not be able to communicate with each other.



1. Open the browser and enter https://diacloudsolutions.com/. Then use DIACloud account and password to login.

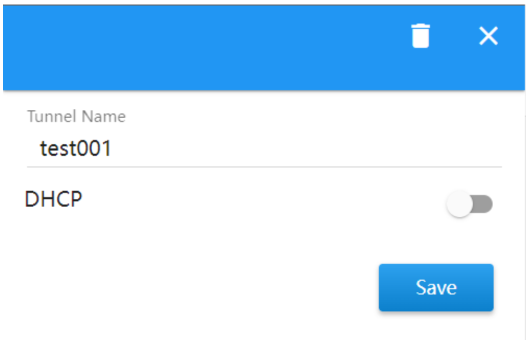
2. Click Secure Tunnel from the left side munu and click + to create security tunnels.



#	Tunnel Name	DHCP	DHCP IP range	Status	Operation
1	Default	Enabled	192.168.200.100 192.168.200.200	Normal	···
2	IABGTest	Disabled		Normal	···
3	test001	Disabled		Normal	···

Total 3 secure tunnel(s)

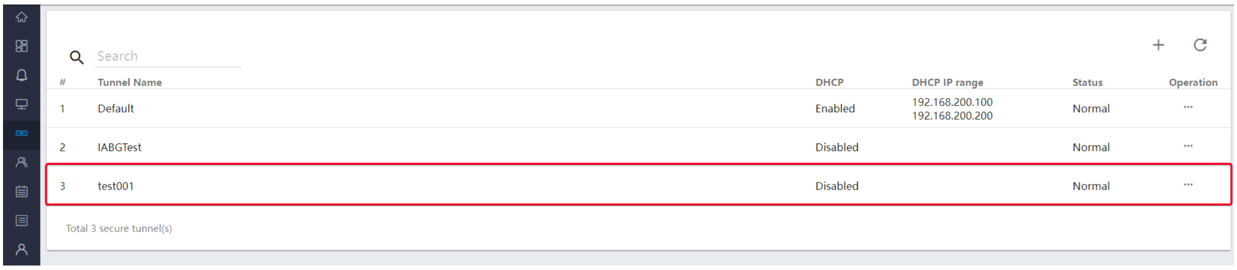
3. Specify a Tunnel Name (At least six characters long) and we suggest not to enable DHCP.



Tunnel Name: test001

DHCP: ○

4. The tunnel you've just created would be displayed in the list.



#	Tunnel Name	DHCP	DHCP IP range	Status	Operation
1	Default	Enabled	192.168.200.100 192.168.200.200	Normal	···
2	IABGTest	Disabled		Normal	···
3	test001	Disabled		Normal	···

Total 3 secure tunnel(s)

2.2.4 Install DIADEVICE

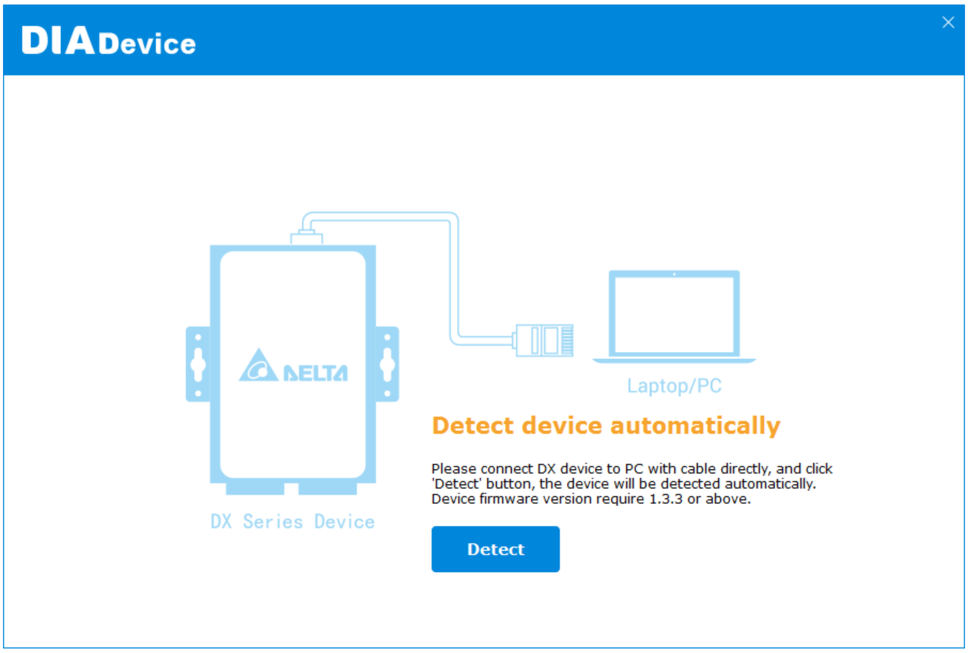
Bind Accounts to DIADevice

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

The DIADevice software is included in the latest DIACom software package. From the official website or sales staff to obtdain DIACom package. The following example uses DX series routers to show you how to configure your device with DIADevice.

Download link: https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&CID=06&itemID=060308&downloadID=DX&sortexpr=cdate&sortdir=DESC

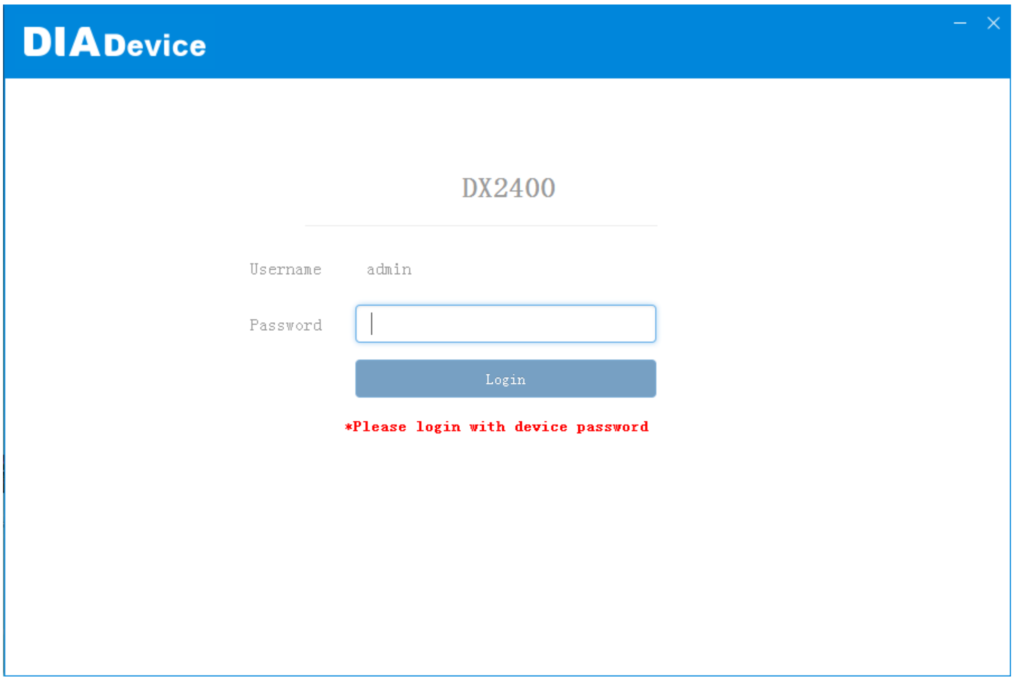
1. Download the software on the official site and install it on your PC web.
2. If the digital signature window pop up while installing, please click on agree. A reboot is required when finish installation.
3. Connect the device to the power supply, and connect the device to the PC using a network cable. Plug the network cable connected to the Internet into the WAN port of the device.
4. Run DIADevice and click ‘Detect’ button.



Detect device automatically

Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

5. After DIACom detects the device, it will automatically jump to the login page, and you need to enter login password on the login page (Default username/ password = admin/admin).



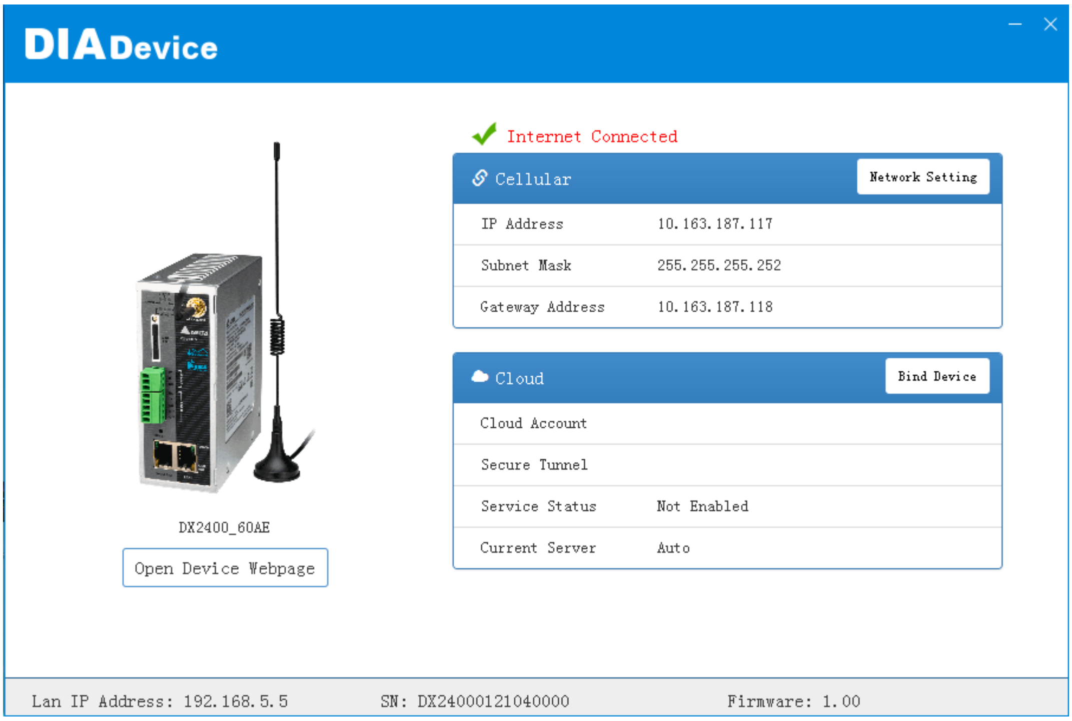
DX2400

Username admin

Password

*Please login with device password

6. Click on Open Device Webpage to open DX router configuration page to configure internet settings, register mappings and so on.



✓ Internet Connected

Cellular

IP Address	10.163.187.117
Subnet Mask	255.255.255.252
Gateway Address	10.163.187.118

Cloud

Cloud Account	
Secure Tunnel	
Service Status	Not Enabled
Current Server	Auto

DX2400_60AE

Lan IP Address: 192.168.5.5 SN: DX24000121040000 Firmware: 1.00

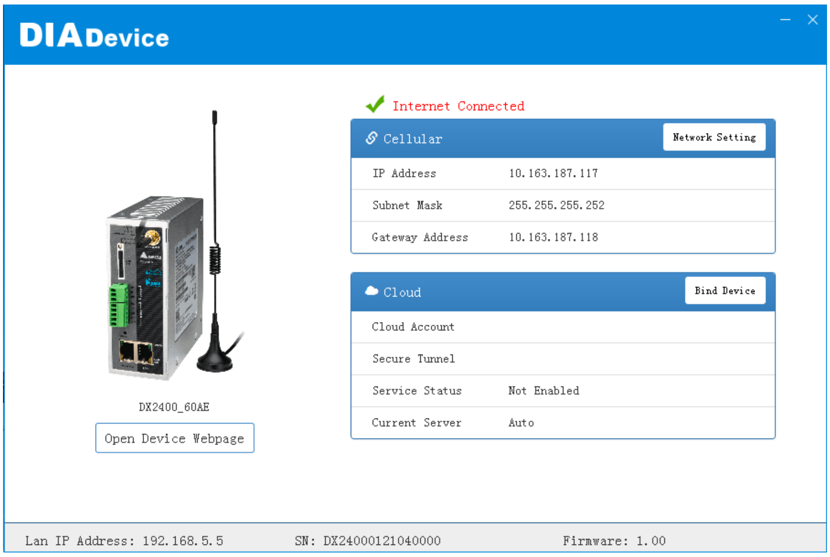
2.2.5 Network Setting

Use Wide-Area Network (WAN)

1. Connect the WAN port of the DX to the internet using an Ethernet cable.

2. Connect the PC to the LAN port of the DX using an Ethernet cable.

3. Click Open Device Webpage on DIADevice interface.



DIADevice

✓ Internet Connected

Cellular	Network Setting
IP Address	10.163.187.117
Subnet Mask	255.255.255.252
Gateway Address	10.163.187.118

Cloud	Bind Device
Cloud Account	
Secure Tunnel	
Service Status	Not Enabled
Current Server	Auto

DX2400_60AE

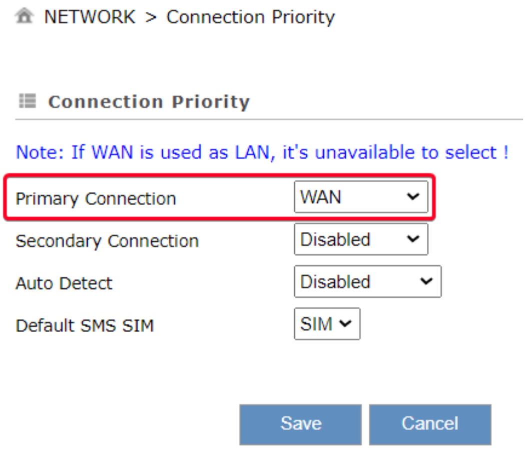
Open Device Webpage

Lan IP Address: 192.168.5.5 SN: DX24000121040000 Firmware: 1.00

4. Enter admin/admin(default) on the login page.

5. Verify that the public network is connected to the WAN port of the cloud router.

6. Go to **NETWORK** → **Connection Priority**, choose WAN for the Primary Connection, then click Save. Please be noted with the following matters:



NETWORK > Connection Priority

Connection Priority

Note: If WAN is used as LAN, it's unavailable to select !

Primary Connection	WAN
Secondary Connection	Disabled
Auto Detect	Disabled
Default SMS SIM	SIM

Save Cancel

a. Check whether the light of LINK/Ack on WAN port is on or not. If not, check the network cable is connected and functioning properly.

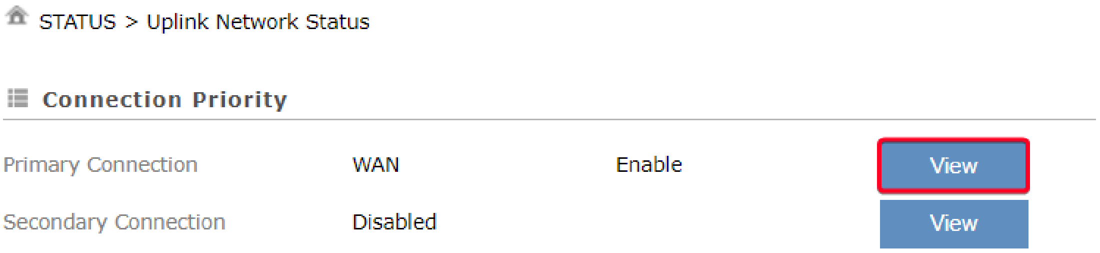
b. Check whether WAN IP address setting differs from LAN IP address.

c. Check if there’s a firewall setup for your corporate network. In case external ports or IP addresses are restricted, login to https://diacloudsolutions.com/ and click ? from the menu on the upper right corner, then set the required port for DIACloud to the white list in Firewall Rule.

Notice

If required, MAC address of DX router can be found via the following page.

1. Go to **STATUS** → **Uplink Networks Status** → **Primary Connection** and click **View**.

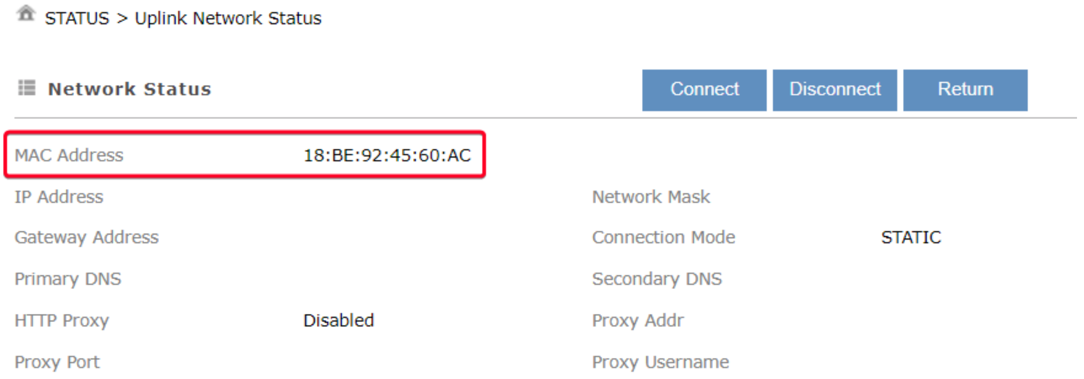


STATUS > Uplink Network Status

Connection Priority

Primary Connection	WAN	Enable	View
Secondary Connection	Disabled		View

2. Find MAC address in Network Status.



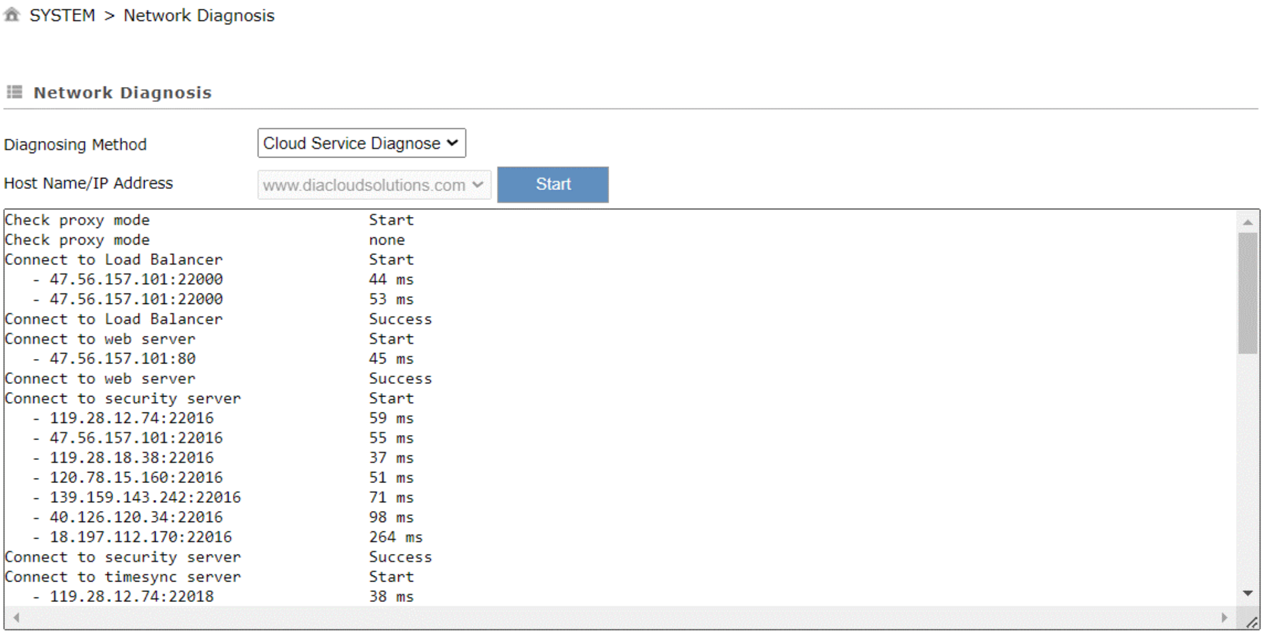
STATUS > Uplink Network Status

Network Status

MAC Address	18:BE:92:45:60:AC		
IP Address		Network Mask	
Gateway Address		Connection Mode	STATIC
Primary DNS		Secondary DNS	
HTTP Proxy	Disabled	Proxy Addr	
Proxy Port		Proxy Username	

d. Go to **STATUS** → **Uplink Network Status** → **Primary connection** and click **View**, check if there's an IP Address on the Network Status page.

e. Go to **SYSTEM** → **Network Diagnosis** → **Cloud Service Diagnose** and check if there's any error. If there's any error, please go back to step three to verify.



SYSTEM > Network Diagnosis

Network Diagnosis

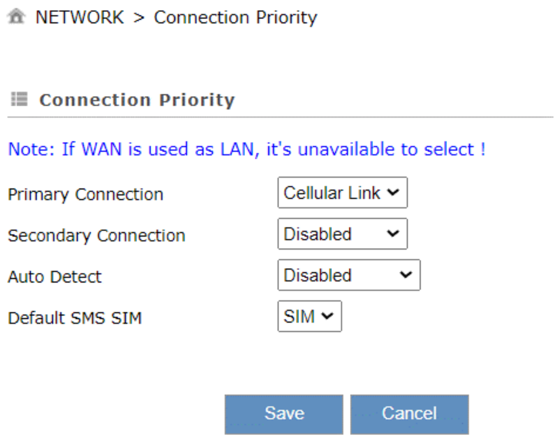
Diagnosing Method: Cloud Service Diagnose

Host Name/IP Address: www.diacloudsolutions.com

```
Check proxy mode                        Start
Check proxy mode                        none
Connect to Load Balancer                Start
   - 47.56.157.101:22000                44 ms
   - 47.56.157.101:22000                53 ms
Connect to Load Balancer                Success
Connect to web server                   Start
   - 47.56.157.101:80                   45 ms
Connect to web server                   Success
Connect to security server              Start
   - 119.28.12.74:22016                 59 ms
   - 47.56.157.101:22016                55 ms
   - 119.28.18.38:22016                 37 ms
   - 120.78.15.160:22016                51 ms
   - 139.159.143.242:22016              71 ms
   - 40.126.120.34:22016                98 ms
   - 18.197.112.170:22016               264 ms
Connect to security server              Success
Connect to timesync server              Start
   - 119.28.12.74:22018                 38 ms
```

Use 4G Internet

1. Place the SIM card on the card tray and insert the tray to SIM1 slot.
2. Go to **NETWORK** → **Connection Priority**, then select **Cellular Link** for **Primary Connection.**



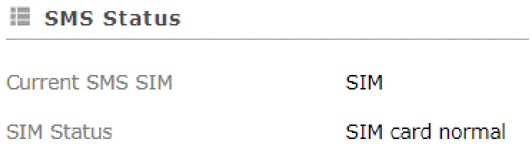
NETWORK > Connection Priority

Connection Priority

Note: If WAN is used as LAN, it's unavailable to select !

Primary Connection	Cellular Link
Secondary Connection	Disabled
Auto Detect	Disabled
Default SMS SIM	SIM

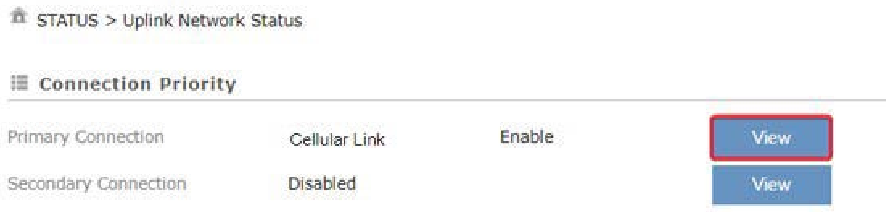
3. Go to **STATUS** → **Uplink Network Status** and check if SIM Status is shown to be **SIM Card normal**. If showing No SIM Card or SIM Card has no response, please reinsert SIM Card and check whether the card has been damaged.



SMS Status

Current SMS SIM	SIM
SIM Status	SIM card normal

4. After confirming that there are no issues in step three, click **"View".**

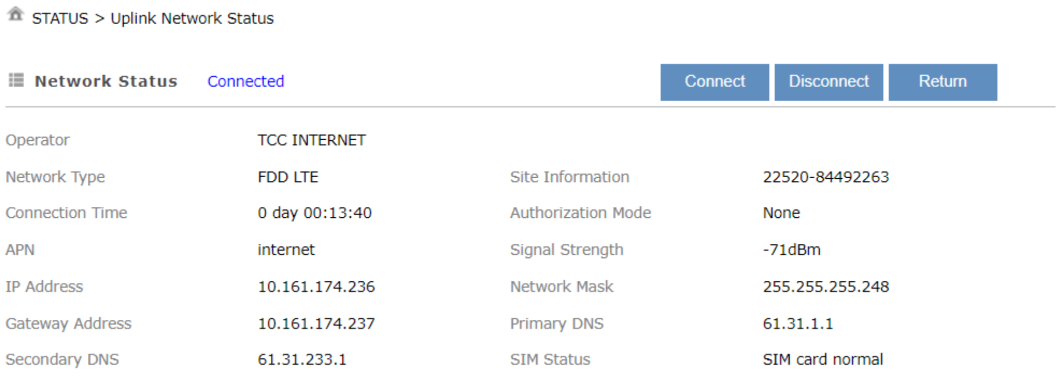


STATUS > Uplink Network Status

Connection Priority

Primary Connection	Cellular Link	Enable
Secondary Connection	Disabled	

5. In the Uplink Network Status page, SIM Card network information and signal strength will be displayed. Please verify that you have obtained an IP address.

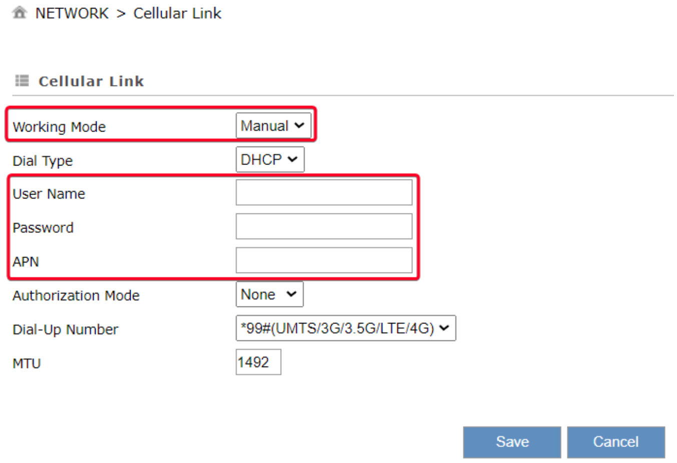


STATUS > Uplink Network Status

Network Status Connected

Operator	TCC INTERNET		
Network Type	FDD LTE	Site Information	22520-84492263
Connection Time	0 day 00:13:40	Authorization Mode	None
APN	internet	Signal Strength	-71dBm
IP Address	10.161.174.236	Network Mask	255.255.255.248
Gateway Address	10.161.174.237	Primary DNS	61.31.1.1
Secondary DNS	61.31.233.1	SIM Status	SIM card normal

6. If Network Status still shows Disconnected, it's probably because the SIM card cannot match with a proper APN. You would need to go to **NETWORK → Cellular LINK** to perform manual configuration which infromation of **User Name/Password/APN** should be inquired with your network operator.

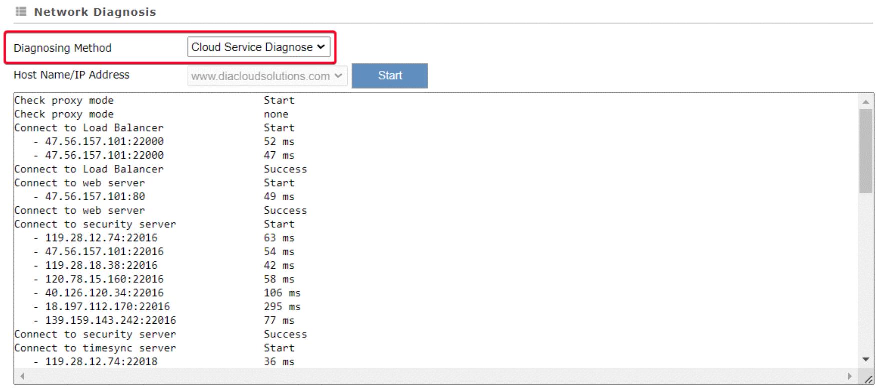


NETWORK > Cellular Link

Cellular Link

Working Mode	Manual
Dial Type	DHCP
User Name	
Password	
APN	
Authorization Mode	None
Dial-Up Number	*99#(UMTS/3G/3.5G/LTE/4G)
MTU	1492

7. After the SIM Card is connected successfully, go to **SYSTEM → Network Diagnosis** and select **Cloud Service Diagnose** for Diagnosis Mthod so as to check if the network is functioning properly. If there's an existing Fail, confirm with IT staffs that both DIACloud IP address and port are set to be on the white list of firewall in your corporation network.



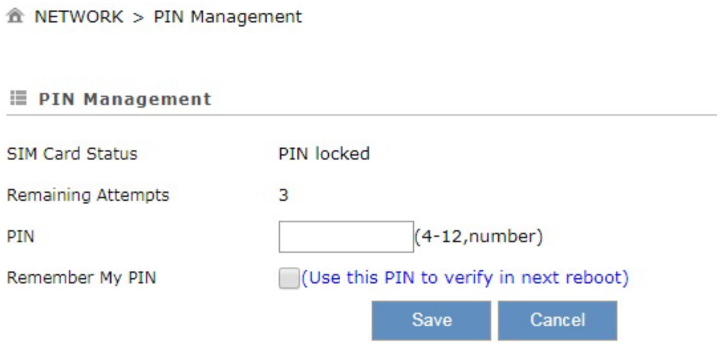
Network Diagnosis

Diagnosing Method: Cloud Service Diagnose

Host Name/IP Address: www.diacloudsolutions.com

```
Check proxy mode                Start
Check proxy mode                none
Connect to Load Balancer        Start
   - 47.56.157.101:22000        52 ms
   - 47.56.157.101:22000        47 ms
Connect to Load Balancer        Success
Connect to web server           Start
   - 47.56.157.101:80           49 ms
Connect to web server           Success
Connect to security server      Start
   - 119.28.12.74:22016         63 ms
   - 47.56.157.101:22016        54 ms
   - 119.28.18.38:22016         42 ms
   - 120.78.15.160:22016        58 ms
   - 40.126.120.34:22016        106 ms
   - 18.197.112.170:22016       295 ms
   - 139.159.143.242:22016      77 ms
Connect to security server      Success
Connect to timesync server      Start
   - 119.28.12.74:22018         36 ms
```

8. If SIM card is locked by PIN code, please go to **NETWORK → PIN Management** and insert the correct SIM PIN. We suggest to remove the PIN code before inserting SIM card to your DX routers which you can contact your network operator for more detailed information.



NETWORK > PIN Management

PIN Management

SIM Card Status	PIN locked
Remaining Attempts	3
PIN	(4-12,number)
Remember My PIN	□ (Use this PIN to verify in next reboot)

9. Check if there's a firewall setup for your corporate network. In case external ports or IP addresses are restricted, login to https://diacloudsolutions.com/ and click ? from the menu on the upper right corner, then set the required port for DIACloud to the white list in Firewall Rule.

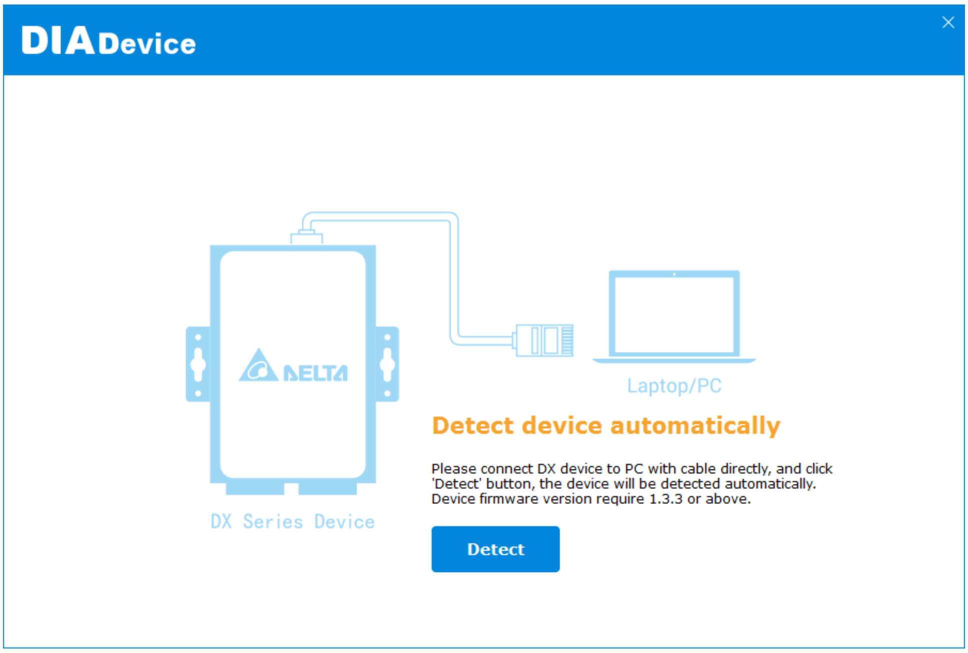
2.2.6 Bind Account

There's two ways to bind DIACloud accounts supported by DX routers.

- **Bind accounts via DIADevice(Suggested).**
- **Bind accounts on DX routers webpage.**

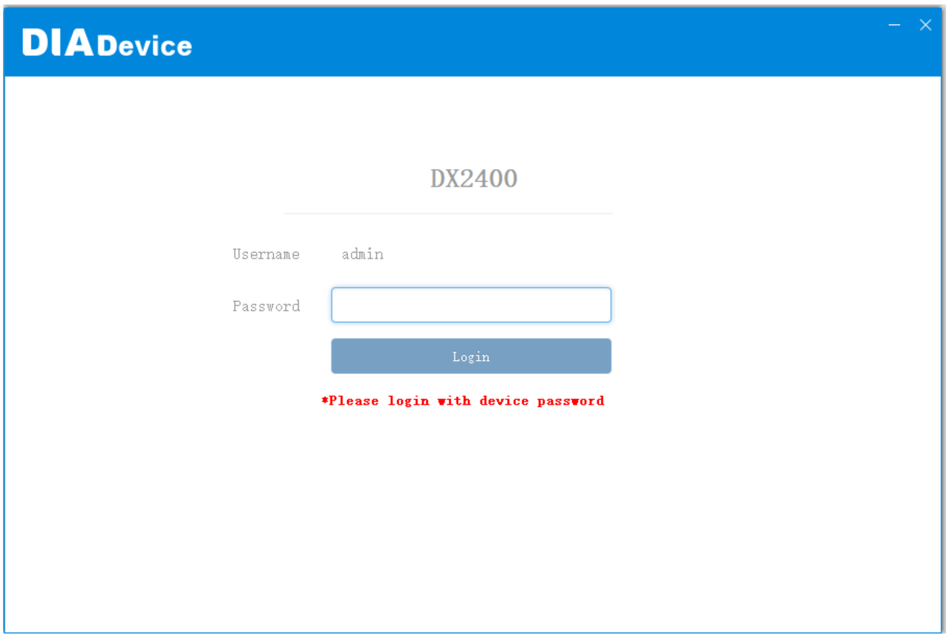
<u>Bind accounts via DIADevice.</u>

1. Power on the DX device and use a network cable to connect the LAN port of your computer and DX device. Also, plug the network cable connected to the external network into the WAN port of the device.
2. Run DIADevice and click "**Detect**".



Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

3. When the device is detected, the page would jump directly to the login page for you to enter login password. (Default username/ password = admin/admin)



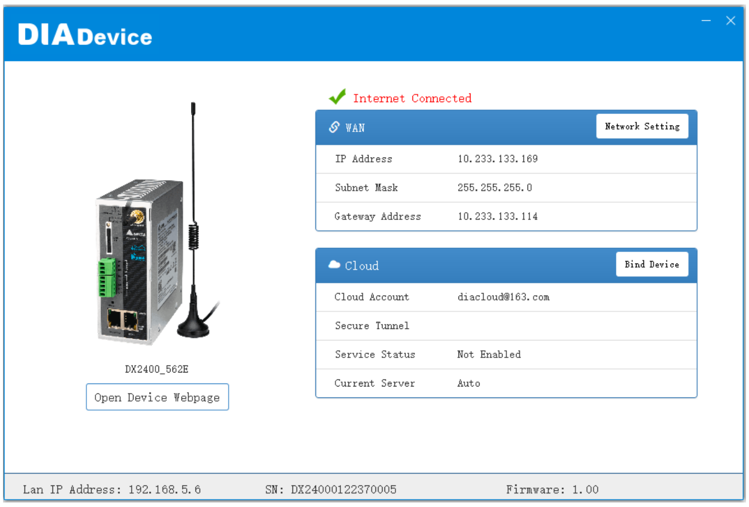
Username admin

Password

*Please login with device password

4. After the authentication is passed, the device information would be displayed which include basic information(Device name, S/N, firmware, LAN IP address), internet connection status, WAN, and cloud service information.

5. Click “**Bind Device**” to bind the device to the account. If the device has been previously bound to a cloud account, this former setting would be remoed by DIADevice so as to bind it to the new account.



✓ Internet Connected

WAN

IP Address	10.233.133.169
Subnet Mask	255.255.255.0
Gateway Address	10.233.133.114

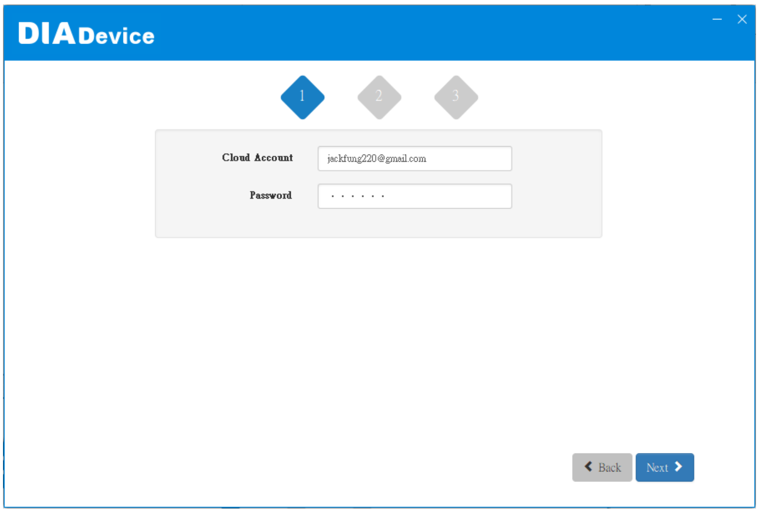
Cloud

Cloud Account	diacloud@163.com
Secure Tunnel	
Service Status	Not Enabled
Current Server	Auto

DX2400_562E

Lan IP Address: 192.168.5.6 SN: DX24000122370005 Firmware: 1.00

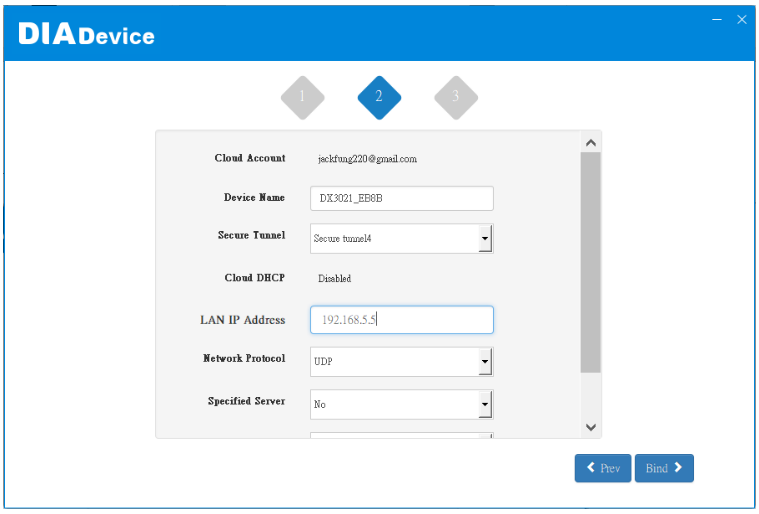
6. Enter the target cloud account and password, then click”**Next**”.



Cloud Account jackfung220@gmail.com

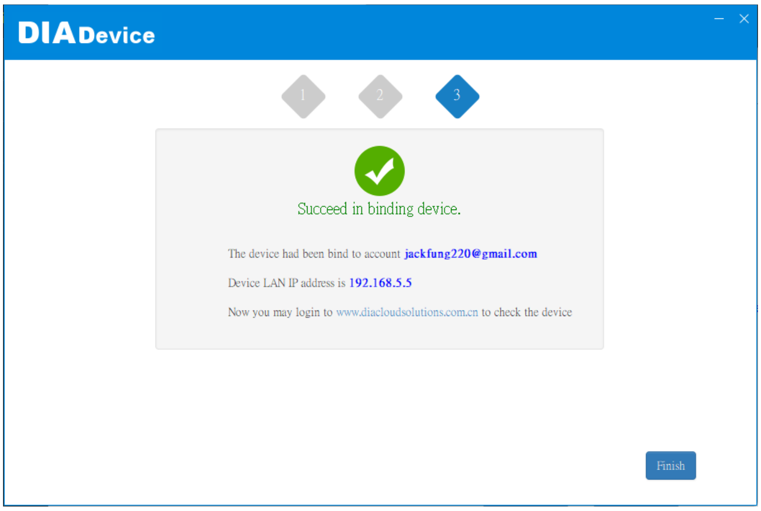
Password ······

7. Configure the relevant settings and click “**Bind**” to complete.



Cloud Account	jackfung220@gmail.com
Device Name	DX3021_EB8B
Secure Tunnel	Secure tunnel4
Cloud DHCP	Disabled
LAN IP Address	192.168.5.5
Network Protocol	UDP
Specified Server	No

8. After successfully binding the device to the account, a notification message would be displayed as the following shown.



Succeed in binding device.

The device had been bind to account jackfung220@gmail.com

Device LAN IP address is 192.168.5.5

Now you may login to www.diacloudsolutions.com.cn to check the device

Webpage Account Binding

1. Obtain an IP address automatically by using the routers as a DHCP server.

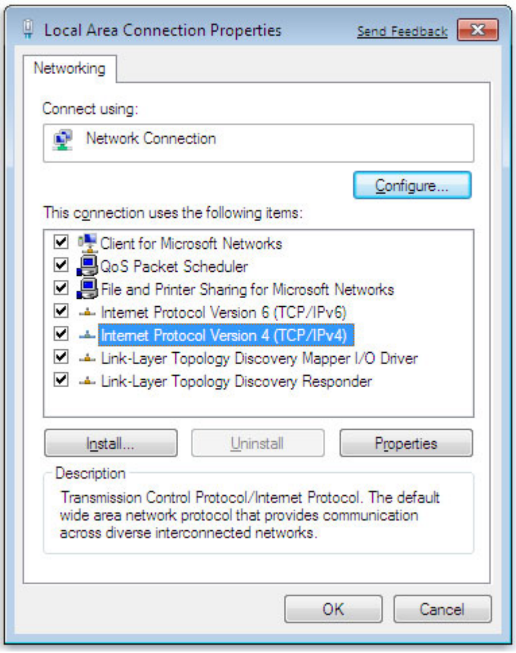
   1) Ensure that the PC is connected to a network with a DHCP server.

   2) Click the start icon ⊞ and select control panel.

   3) Check network connection in Network and Sharing Center.

   4) Right click on the connection to modify and click properties 🛡. Please enter administrative password for confirmation if required by the system.

   5) Networking: Select Internet Protocol Version 4 (TCP / IPv4) or Internet Protocol Version 6 (TCP/ IPv6) for “This connection uses the following items” Section, then click **Properties**.



Connect using:

Network Connection

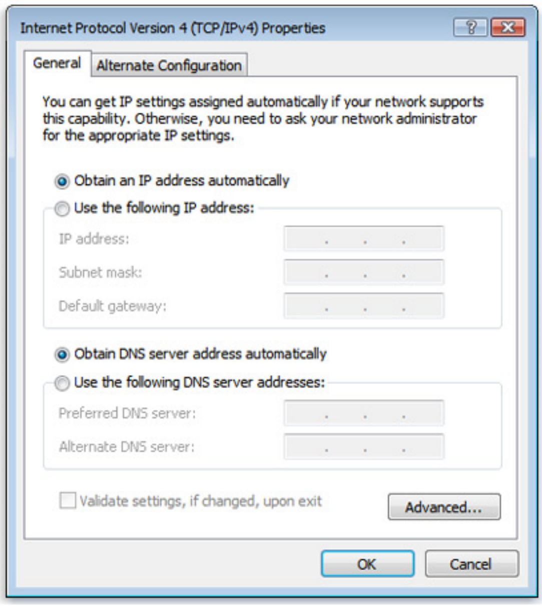
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6) Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings, if changed, upon exit

7) Confirm that the IP address has been obtained from DHCP server.

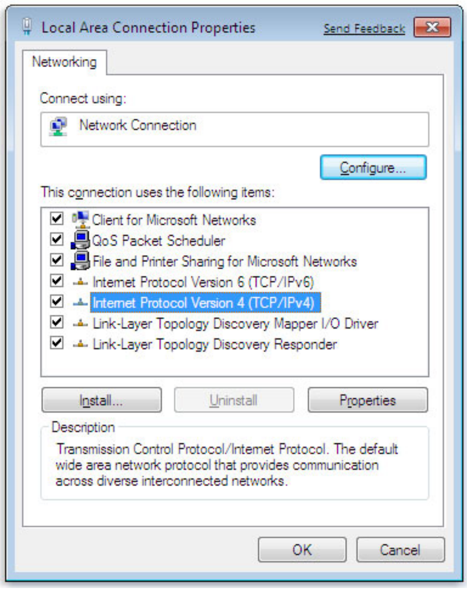
2. Manually set the local IP address of your PC (The local IP address of your PC and the router must share the same network segment) For example: The default IP address of router is 192.168.5.5 and subnet mask is 255.255.255.0, the IP address of your PC can be set from 192.168.5.1 to 192.168.5.254 (except for 192.168.5.5) and make sure there’s no IP address conflict.

1) Click the start icon and select control panel.

2) Check network connection in Network and Sharing Center.

3) Right click on the connection to modify and click properties. Please enter administrative password for confirmation if required by the system.

4) Networking: Select Internet Protocol Version 4 (TCP / IPv4) or Internet Protocol Version 6 (TCP/ IPv6) for “This connection uses the following items” Section, then click **Properties.**



Local Area Connection Properties

Connect using:

Network Connection

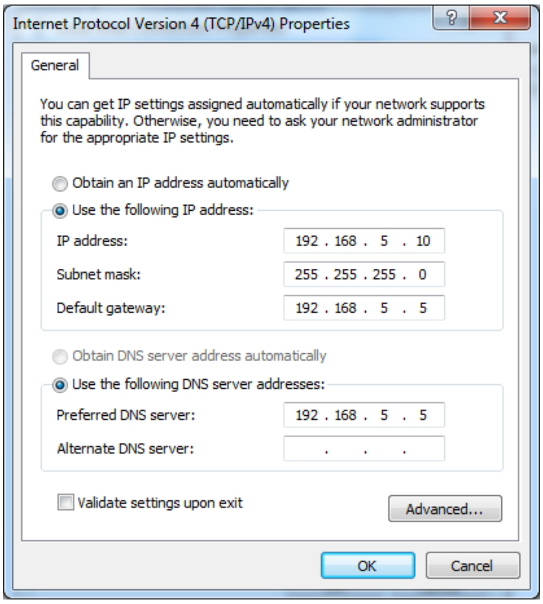
This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5) Enter 192.168.5.10 for IP address, 255.255.255.0 for subnet mask, then click “**OK**”.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 5 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 5 . 5

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 5 . 5

Alternate DNS server: . . .

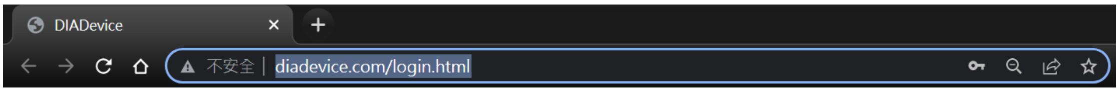
□ Validate settings upon exit

3. Connect the PC directly to the LAN port of the DX cloud router using network cable.

4. The default device IP address is 192.168.5.5, and enter the default username and password: admin/admin.

5. After connecting the PC and the DX router, the next step is to configure the IP address for the PC. There are two ways to configure the IP address for the PC, we recommend using the first method.

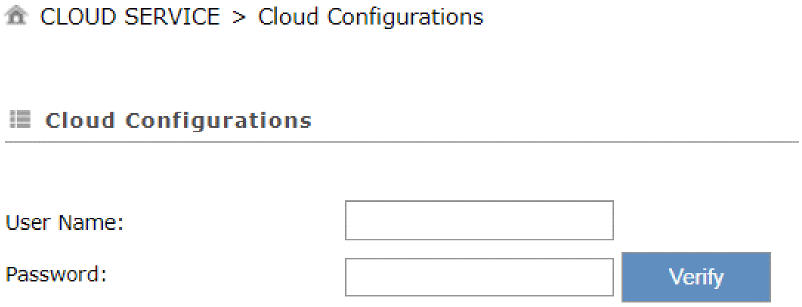
6. Open the browser (such as Chrome or Edge) and enter the default device IP address 192.168.5.5 or www.diadevice.com.



diadevice.com/login.html

7. Login page would pop up as the following shown. Login with the username and password of DX router (Default: admin/admin) to enter the configuration page.

8. Go to **Cloud Service** → **Cloud Configuration**, enter the username and password of DIACloud, then click “**Verify**”.



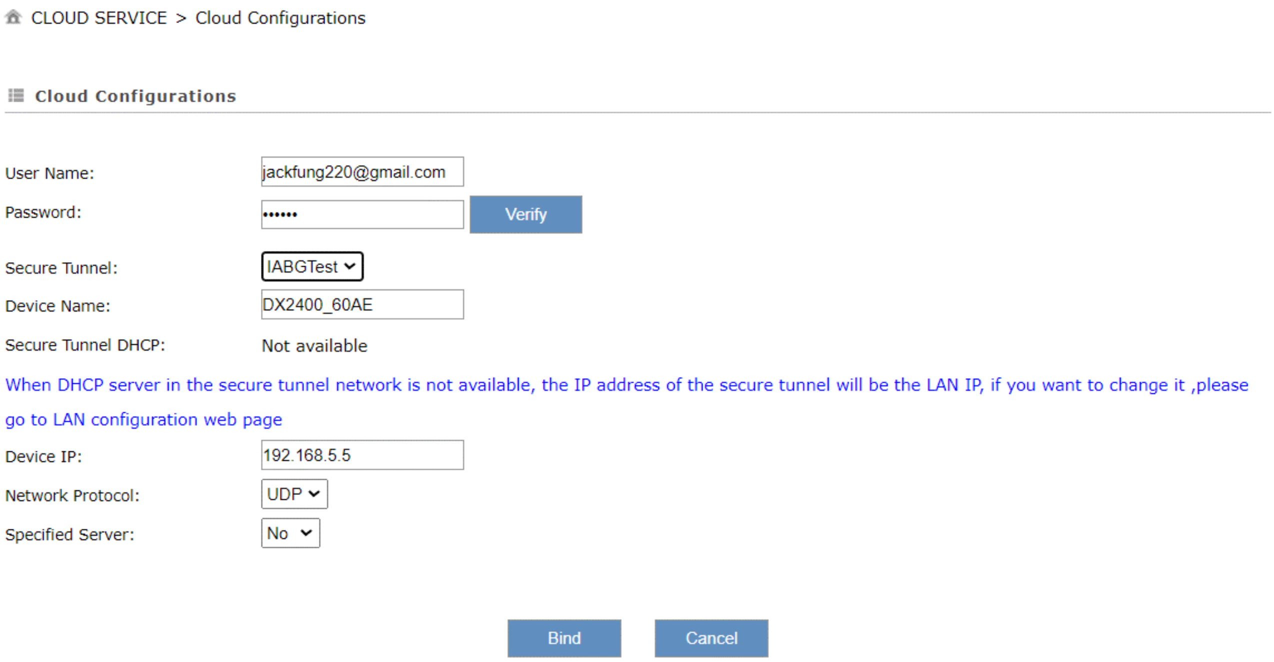
CLOUD SERVICE > Cloud Configurations

Cloud Configurations

User Name:

Password:

9. Click “**Verify**”. After the account and password being successfully verified, the following page would be displayed. You can bind devices to the account by clicking “**Bind**” with default parameter settings.



CLOUD SERVICE > Cloud Configurations

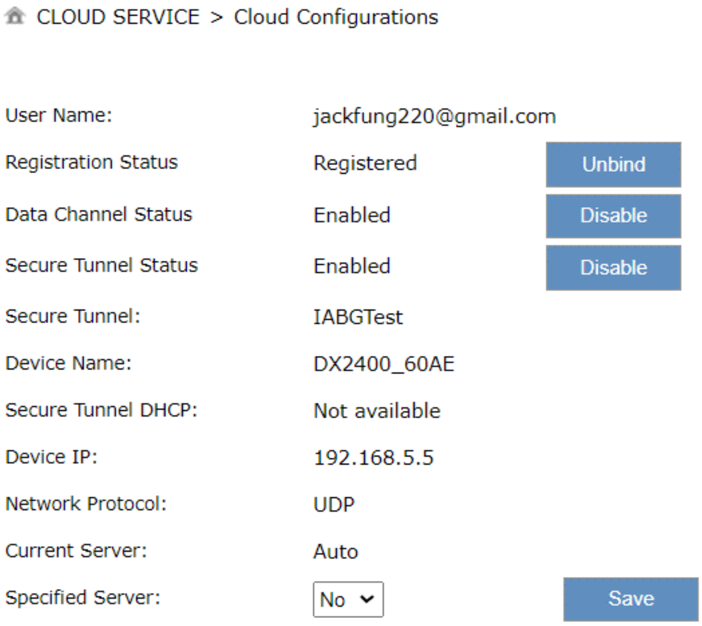
Cloud Configurations

User Name:	jackfung220@gmail.com
Password:	••••••
Secure Tunnel:	IABGTest
Device Name:	DX2400_60AE
Secure Tunnel DHCP:	Not available

When DHCP server in the secure tunnel network is not available, the IP address of the secure tunnel will be the LAN IP, if you want to change it ,please go to LAN configuration web page

Device IP:	192.168.5.5
Network Protocol:	UDP
Specified Server:	No

10. After binding successfully, you are allowed to login to the configuration page again to view the device information.



CLOUD SERVICE > Cloud Configurations

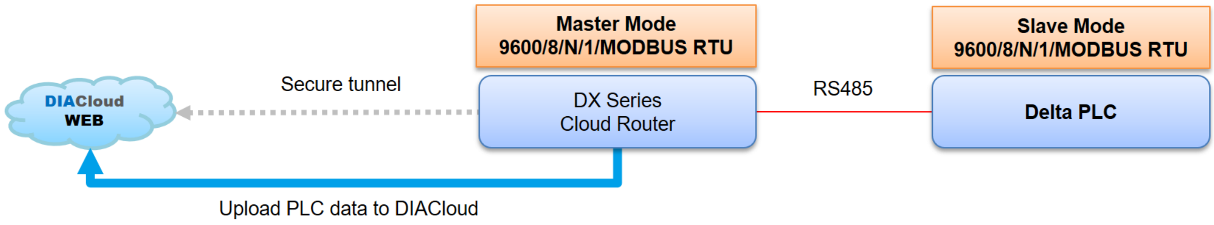
User Name:	jackfung220@gmail.com
Registration Status	Registered
Data Channel Status	Enabled
Secure Tunnel Status	Enabled
Secure Tunnel:	IABGTest
Device Name:	DX2400_60AE
Secure Tunnel DHCP:	Not available
Device IP:	192.168.5.5
Network Protocol:	UDP
Current Server:	Auto
Specified Server:	No

2.3 Application

2.3.1 RS485 Master Data Collection and Application

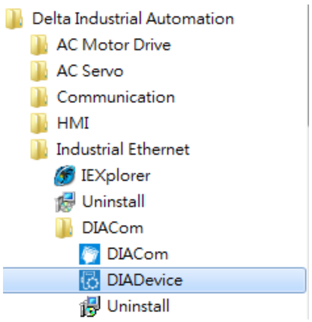
Use DX router to upload MODBUS data to DIACloud via RS485.

Please refer to Chapter 3.4.1 RS-232/RS-485 for detailed configuration parameter explanations.

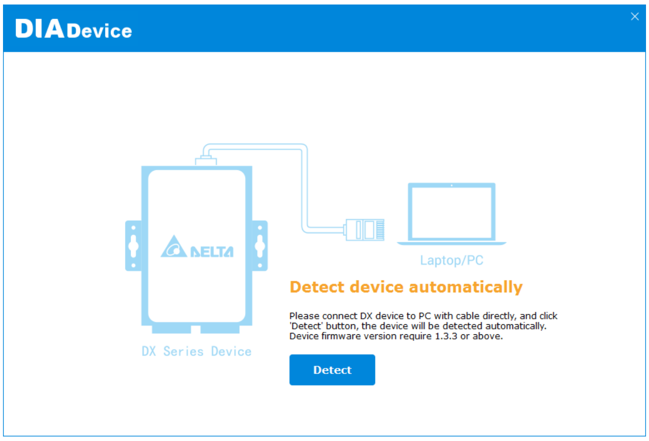


Setup Steps

1. Make sure that all the basic configuration detailed in chapter 2 has been completed and functions properly.
2. Connect the industrial device to the DX cloud router via RS485, then change the industrial device's transfer format to **9600/8/N/1/RTU**.
3. Use a network cable to connect LAN ports on your PC and the DX router.
4. Open DIADevice: Click Start icon on Window and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice.**



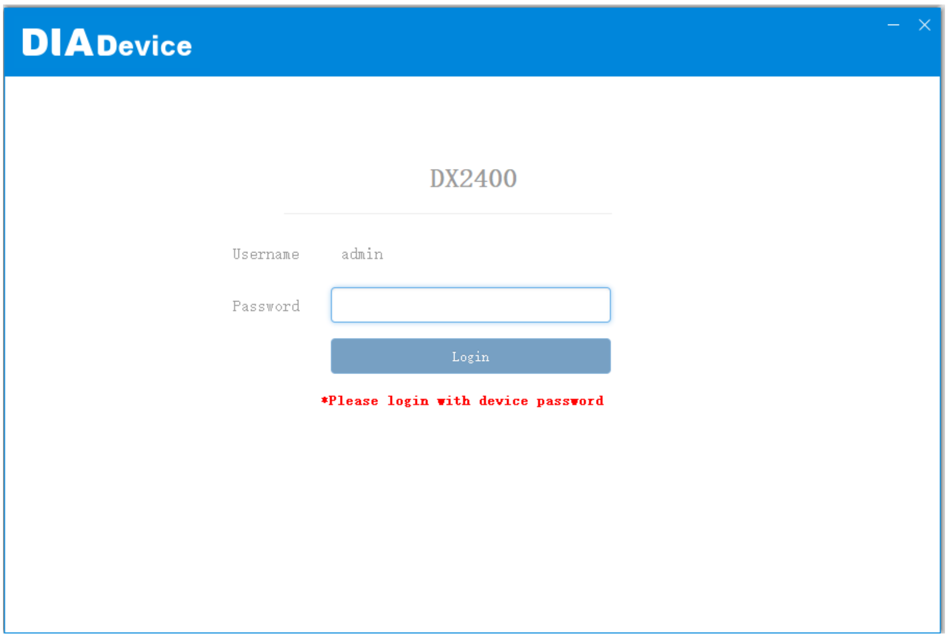
5. Connect the device to the power supply and connect the device to the PC using a network cable. Plug the network cable connected to the Internet into the WAN port of the device.
6. Click **Detect** and the page would jump to the login page of DX router.



Detect device automatically

Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

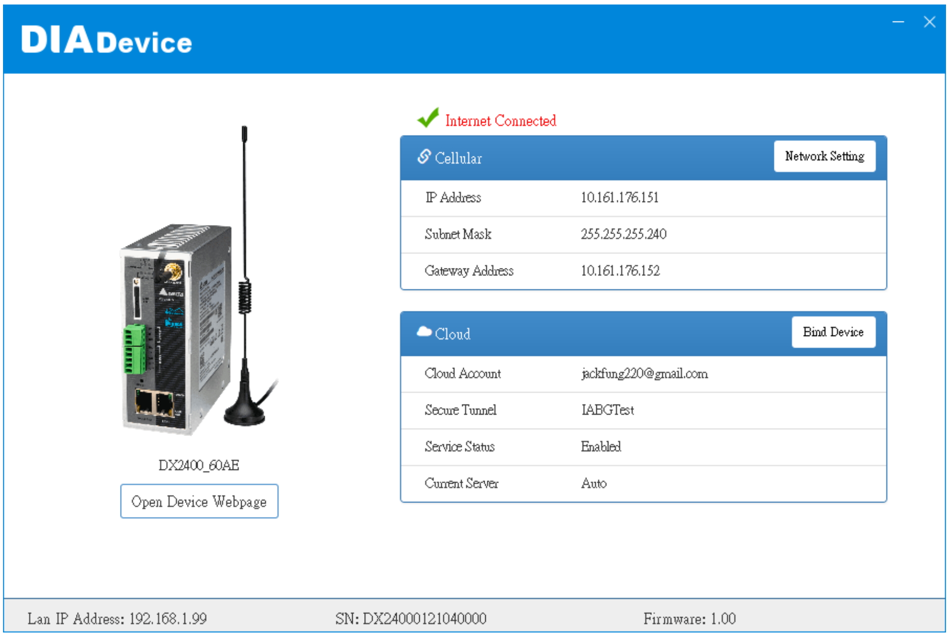
7. It will automatically redirect to the login page upon detecting the device. Enter the account and password on the login page.(Default: admin/admin)



Username admin

*Please login with device password

8. Click “Open Device Webpage”.



Internet Connected

Cellular

IP Address	10.161.176.151
Subnet Mask	255.255.255.240
Gateway Address	10.161.176.152

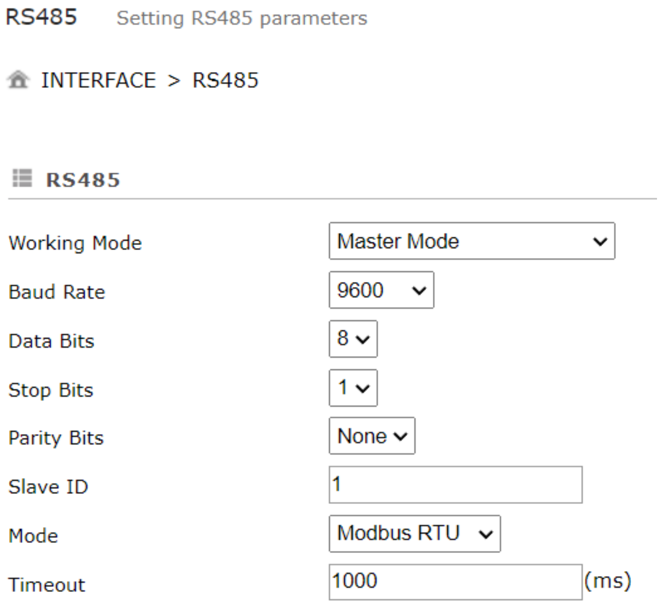
Cloud

Cloud Account	jackfung220@gmail.com
Secure Tunnel	IABGTest
Service Status	Enabled
Current Server	Auto

Lan IP Address: 192.168.1.99 SN: DX24000121040000 Firmware: 1.00

9. After entering DX router login page, input your account and password (Default: admin / admin), then click login.

10. Go to **INTERFACE** → **RS485** and select **Master Mode** as Working mode. DX router and PLC device must share the same communication parameters for RS485.



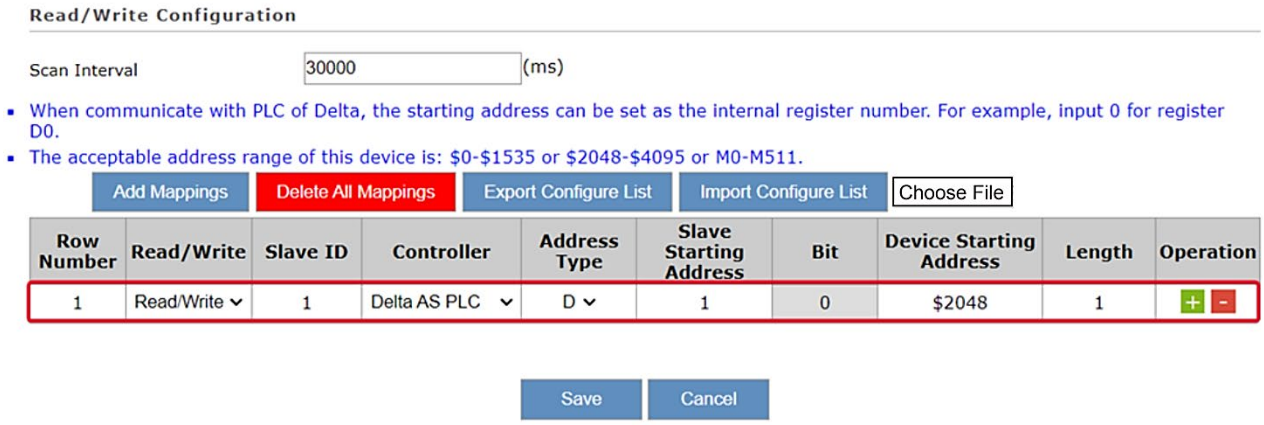
RS485 Setting RS485 parameters

INTERFACE > RS485

RS485

Working Mode	Master Mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Slave ID	1
Mode	Modbus RTU
Timeout	1000 (ms)

11. The Scan Interval in the Read/Write Configuration can be changed manually. Click "**Add Mappings**" and set the mapping register address**(D1→$2048)**, as shown below**.** The following example is the mapping address of **Delta PLC AS300**. **Please choose "Others" if the product is not Delta series** and check the mapping address in its own product manual. Then click **save** to complete.



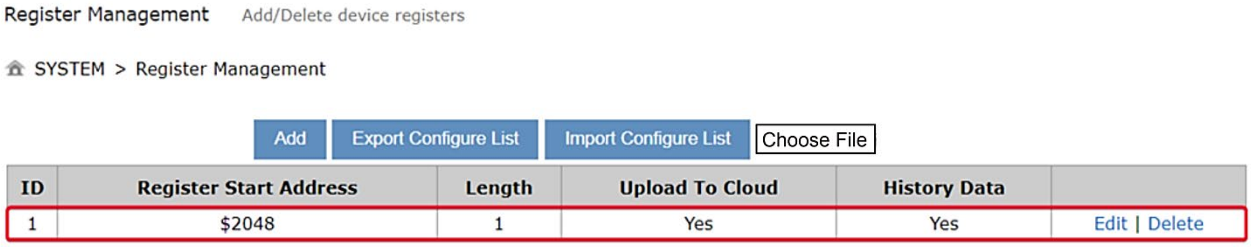
Read/Write Configuration

Scan Interval 30000 (ms)

- When communicate with PLC of Delta, the starting address can be set as the internal register number. For example, input 0 for register D0.
- The acceptable address range of this device is: $0-$1535 or $2048-$4095 or M0-M511.

Row Number	Read/Write	Slave ID	Controller	Address Type	Slave Starting Address	Bit	Device Starting Address	Length	Operation
1	Read/Write	1	Delta AS PLC	D	1	0	$2048	1	+ -

12. Go to **SYSTEM** → **Register Management** to set the Register Start Address for uploading to DIACloud on the DX router. Click **ADD** and key in the following items: Register Start Address: $2048, Length: 1, Upload to Cloud: Yes, History Data: Yes. Then click Save.



Register Management Add/Delete device registers

SYSTEM > Register Management

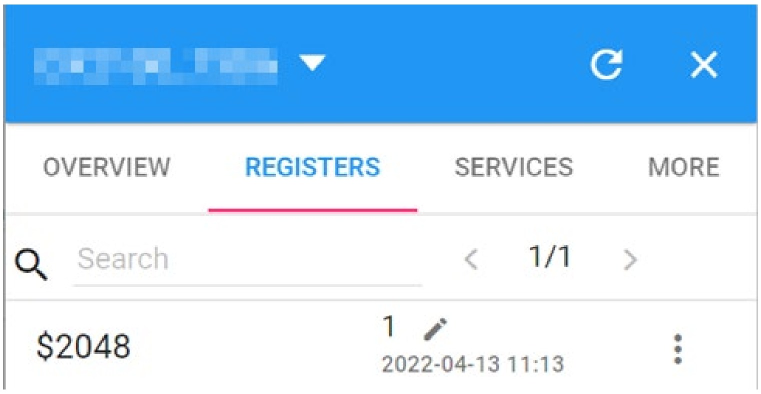
ID	Register Start Address	Length	Upload To Cloud	History Data	
1	$2048	1	Yes	Yes	Edit | Delete

13. After connecting Delta AS PLC to DX router via RS485 cable, change the AS PLC data transfer format to 9600/8/N/1/Modbus ASCII, with Slave ID:1.

14. Configure the PLC to write D1 to the cloud router's register address $2048 and write the value 1 to the register.

15. Change the data of Delta AS PLC register D1 to 1.

16. Login to diacloudsolutions.com, select **Devices** → More → **Registers**. You'll see the value of $2048 is displayed as 1.

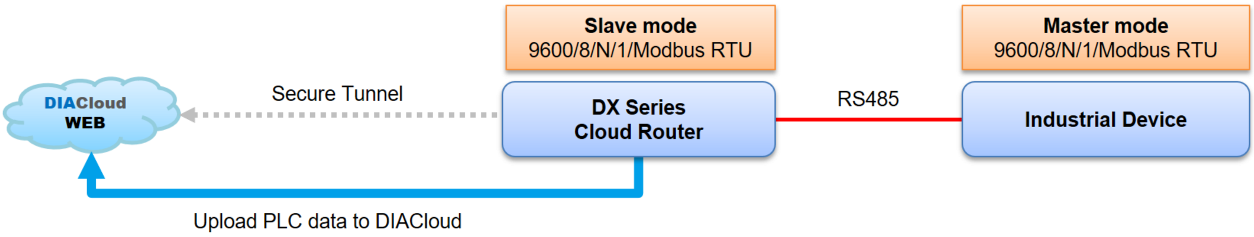


$2048 1
2022-04-13 11:13

2.3.2 RS485 Slave Data Collection and Application

DX router operates in Slave mode, with PLC writing data to the DX router's registers and uploading the data in registers to DIACloud.

Please refer to Chapter 3.4.1 RS-232/RS-485 for detailed configuration parameter explanations.



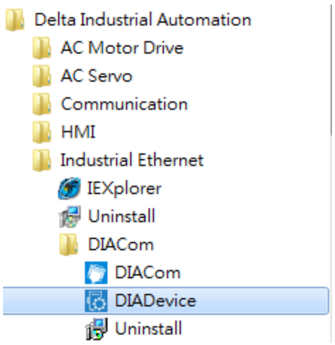
Setup Steps

1. Make sure that all the basic configuration in chapter2 has been completed and functions properly.

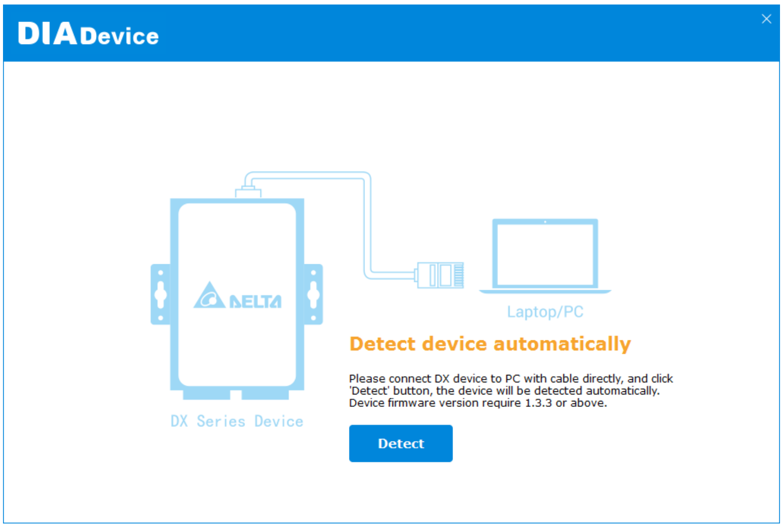
2. Connect RS485 to DX router, change the transfer format of the industrial device to **9600/8/N/1/RTU.**

3. Use a network cable to connect LAN ports on your PC and the DX router.

4. Install DIACom software, open DIADevice: Click start icon on Windows → **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice**.

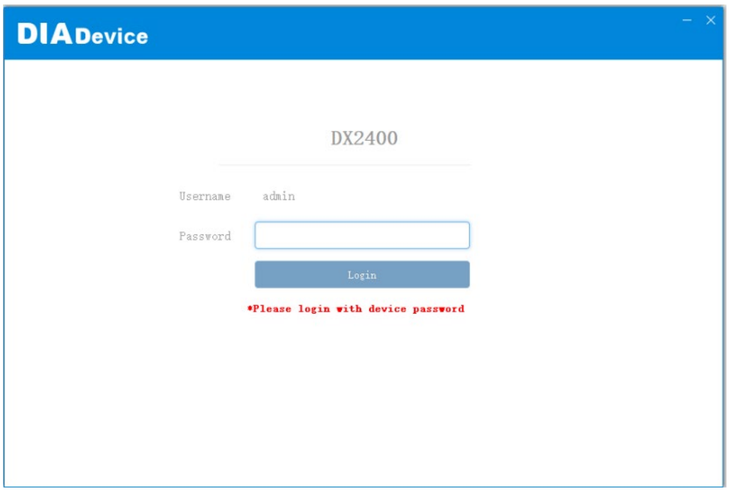


5. Click **Detect**, and it will redirect to DX router login page.



Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

6. Enter username / password. (Default: admin/admin)



DIADevice

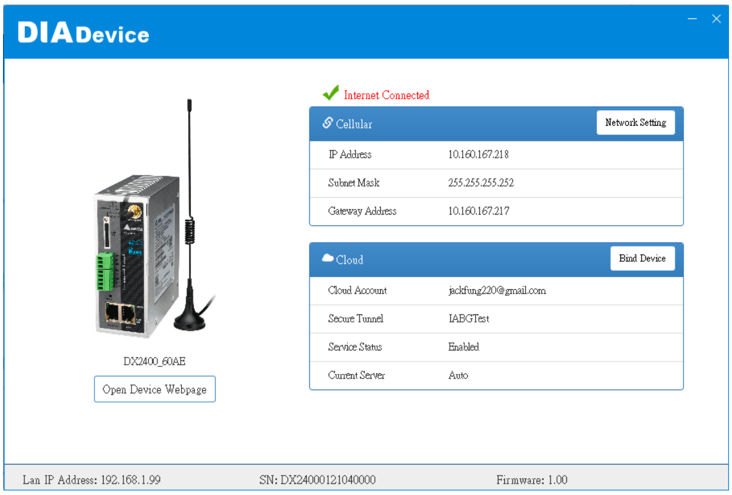
DX2400

Username	admin
Password	

Login

*Please login with device password

7. Click Open Device Webpage and verify that the bound IP address is 192.168.1.99.



DIADevice

DX2400_60AE

Open Device Webpage

✓ Internet Connected

Cellular — Network Setting

IP Address	10.160.167.218
Subnet Mask	255.255.255.252
Gateway Address	10.160.167.217

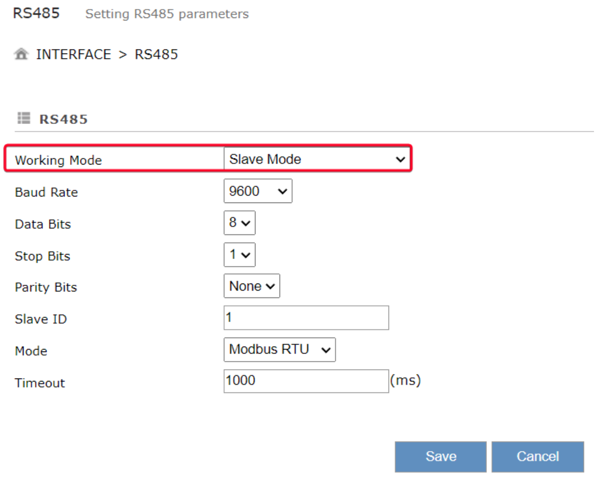
Cloud — Bind Device

Cloud Account	jackfung220@gmail.com
Secure Tunnel	IABGTest
Service Status	Enabled
Current Server	Auto

Lan IP Address: 192.168.1.99   SN: DX24000121040000   Firmware: 1.00

8. After entering DX router login page, input your account and password (Default: admin / admin), click **Login**.

9. Go to **INTERFACE** → **RS485**, select **Slave Mode** as working mode. Set the communication parameters as 9600/8/N/1, Slave ID:1, Mode: Modbus RTU, then click on **Save**.



RS485   Setting RS485 parameters

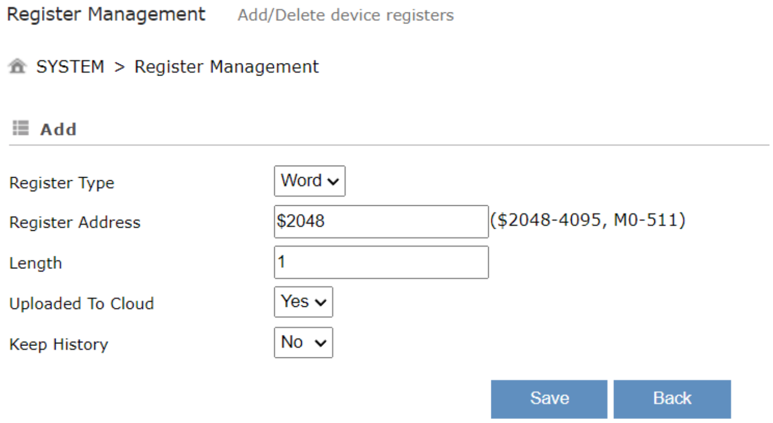
INTERFACE > RS485

RS485

Working Mode	Slave Mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Slave ID	1
Mode	Modbus RTU
Timeout	1000 (ms)

Save   Cancel

10. Go to **SYSTEM** → **Register Management** to set the Register Address for uploading to DIACloud on the DX router. Click on “**Add**” and key in the following items: Register Address: $2048, Length: 1. Then click **Save**.



Register Management Add/Delete device registers

SYSTEM > Register Management

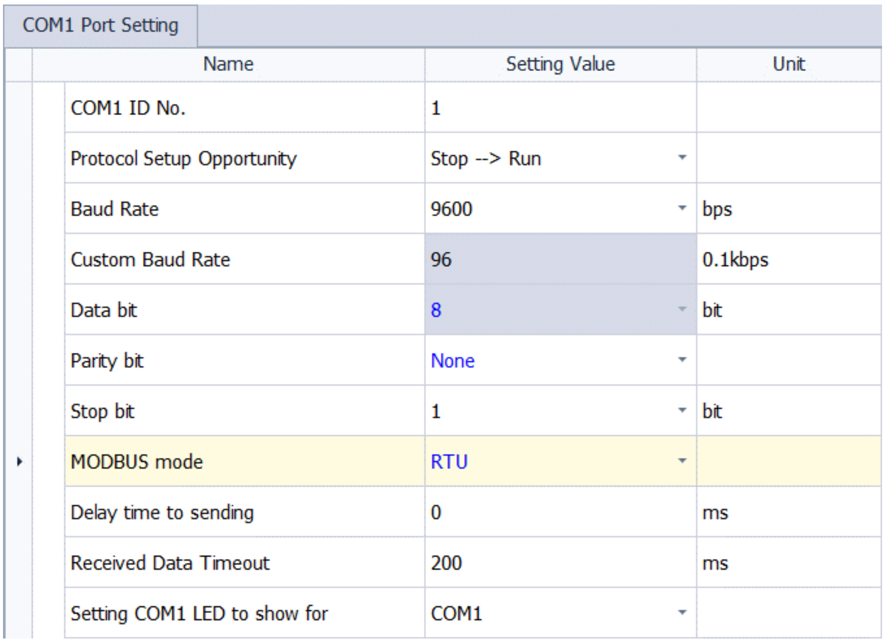
Add

Register Type	Word
Register Address	$2048 ($2048-4095, M0-511)
Length	1
Uploaded To Cloud	Yes
Keep History	No

11. **PLC Setting**: Use ISP Soft to log in Delta PLC data exchange setting.

a. Connect PLC to DX router via RS485 and change the following setting:

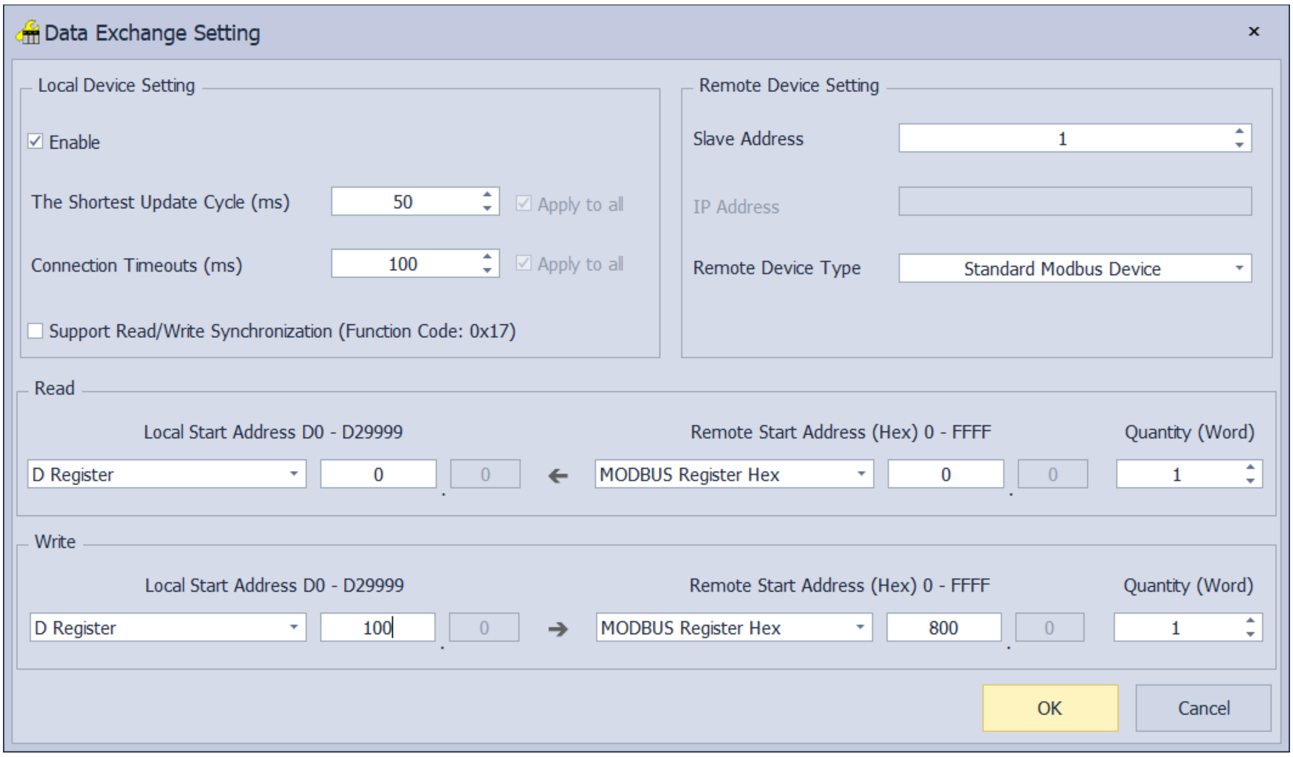
- Transfer Format: 9600/8/N/1/RTU



COM1 Port Setting

Name	Setting Value	Unit
COM1 ID No.	1	
Protocol Setup Opportunity	Stop --> Run	
Baud Rate	9600	bps
Custom Baud Rate	96	0.1kbps
Data bit	8	bit
Parity bit	None	
Stop bit	1	bit
MODBUS mode	RTU	
Delay time to sending	0	ms
Received Data Timeout	200	ms
Setting COM1 LED to show for	COM1	

- Slave Address: **1**
- Remote Device Type: **Standard Modbus Device**
- Data Exchange: Register PLC D100 > Write > DX router $2048 Register (MODBUS Register Hex: 800)



Data Exchange Setting

Local Device Setting

☑ Enable

The Shortest Update Cycle (ms): 50 ☑ Apply to all

Connection Timeouts (ms): 100 ☑ Apply to all

□ Support Read/Write Synchronization (Function Code: 0x17)

Remote Device Setting

Slave Address: 1

IP Address:

Remote Device Type: Standard Modbus Device

Read

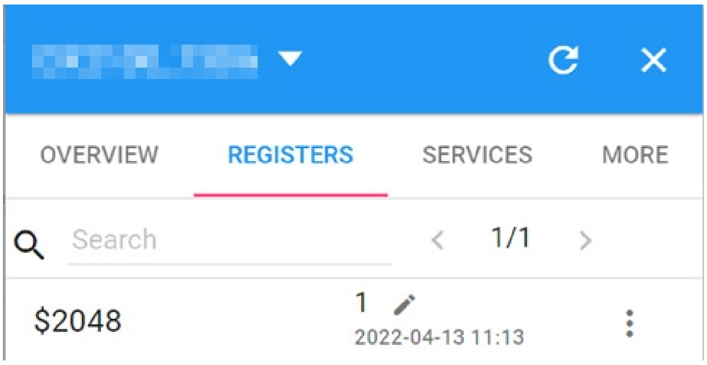
Local Start Address D0 - D29999				Remote Start Address (Hex) 0 - FFFF			Quantity (Word)
D Register	0	0	←	MODBUS Register Hex	0	0	1

Write

Local Start Address D0 - D29999				Remote Start Address (Hex) 0 - FFFF			Quantity (Word)
D Register	100	0	→	MODBUS Register Hex	800	0	1

b. Change the register PLC D100 to 1.

c. Login to diacloudsolutions.com and select **Devices** → More → **Registers**. The value of $2048 is displayed as 1.



[redacted]

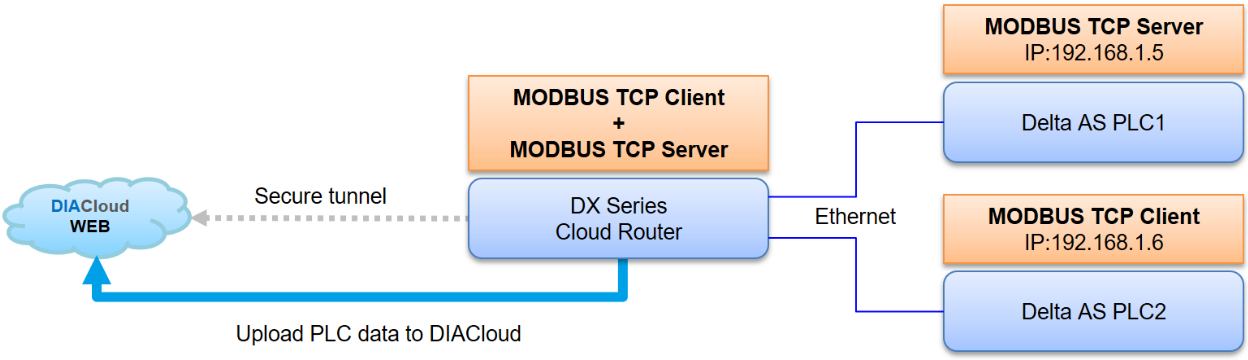
$2048 1
2022-04-13 11:13

2.3.3 Ethernet Master and Slave Mode Data Collection Application

Application

DX Router can function simultaneously as a MODBUS TCP Client + Server, allowing data exchange with two PLCs while uploading the data to DIACloud.

Please refer to Chapter 3.4.2 MODBUS TCP for a detailed explanation of the configuration parameters.

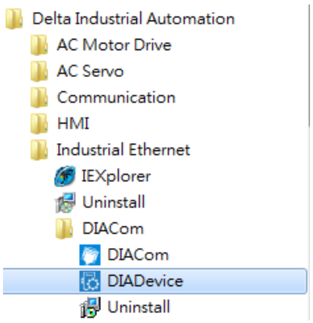


Setup Steps

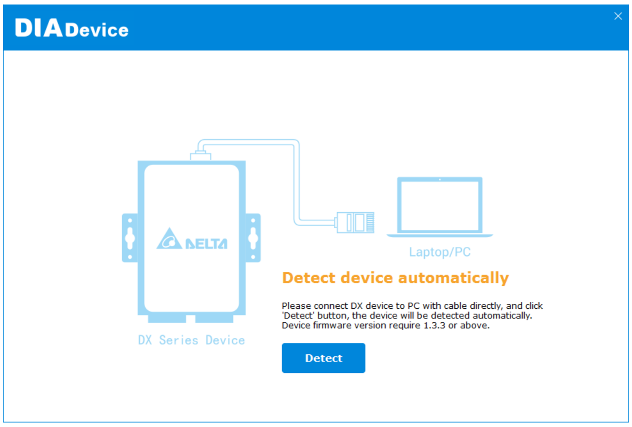
1. Make sure that all the basic configuration detailed in chapter 2 has been completed and functions properly.

2. Use a network cable to connect LAN ports on your PC and the DX router.

3. Install DIACom software, open DIADevice: Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice**.

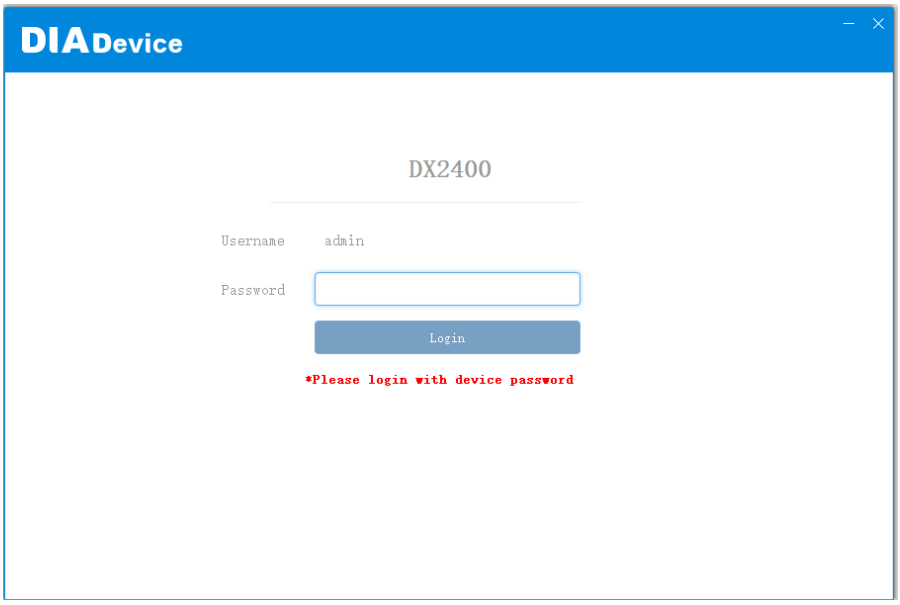


4. Click **Detect**, and it will redirect to the login page of DX router.



Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

5. Enter your account and password. (Default: admin/admin)



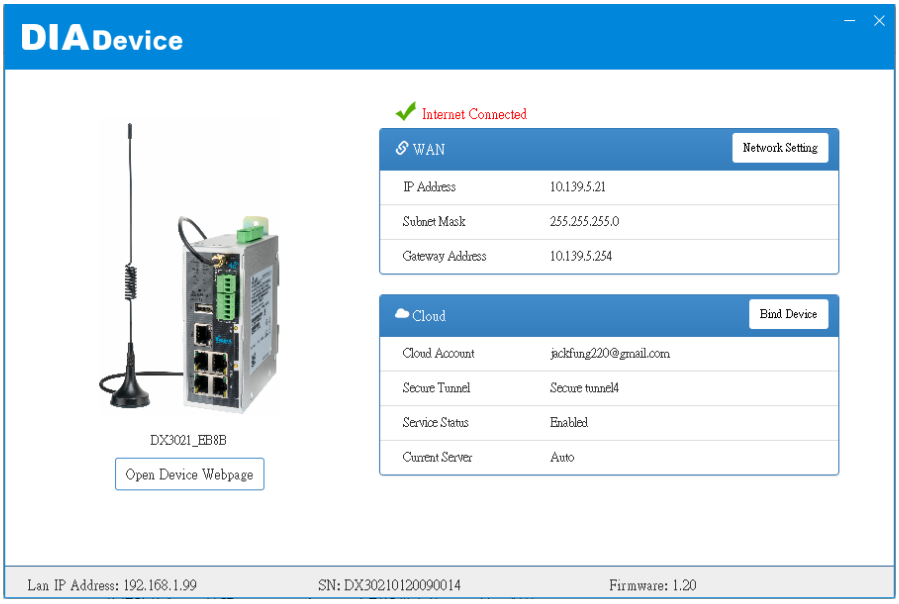
DX2400

Username admin

Password

*Please login with device password

6. Click Open Device Webpage and verify that the bound IP address is 192.168.1.99.



Internet Connected

WAN

IP Address	10.139.5.21
Subnet Mask	255.255.255.0
Gateway Address	10.139.5.254

Cloud

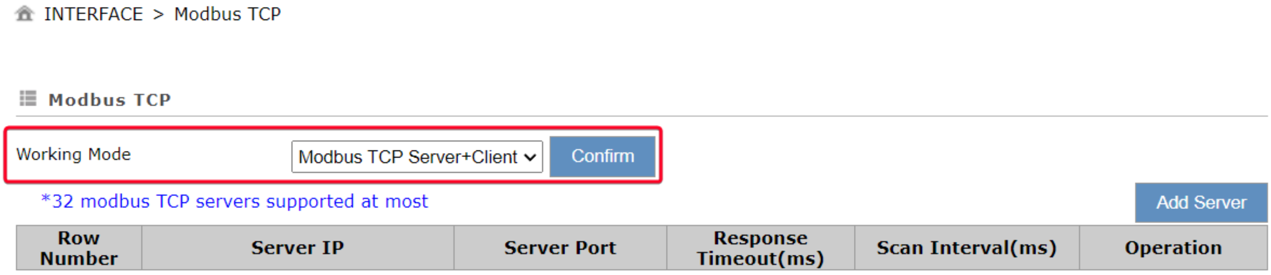
Cloud Account	jackfung220@gmail.com
Secure Tunnel	Secure tunnel4
Service Status	Enabled
Current Server	Auto

DX3021_EB8B

Lan IP Address: 192.168.1.99 SN: DX30210120090014 Firmware: 1.20

7. After entering DX router login page, input your account and password. (Default: admin/admin) and click **login**.

8. Go to **INTERFACE** → **MODBUS TCP** and select **Modbus TCP Server+Client** as working mode, then click **Confirm**.



INTERFACE > Modbus TCP

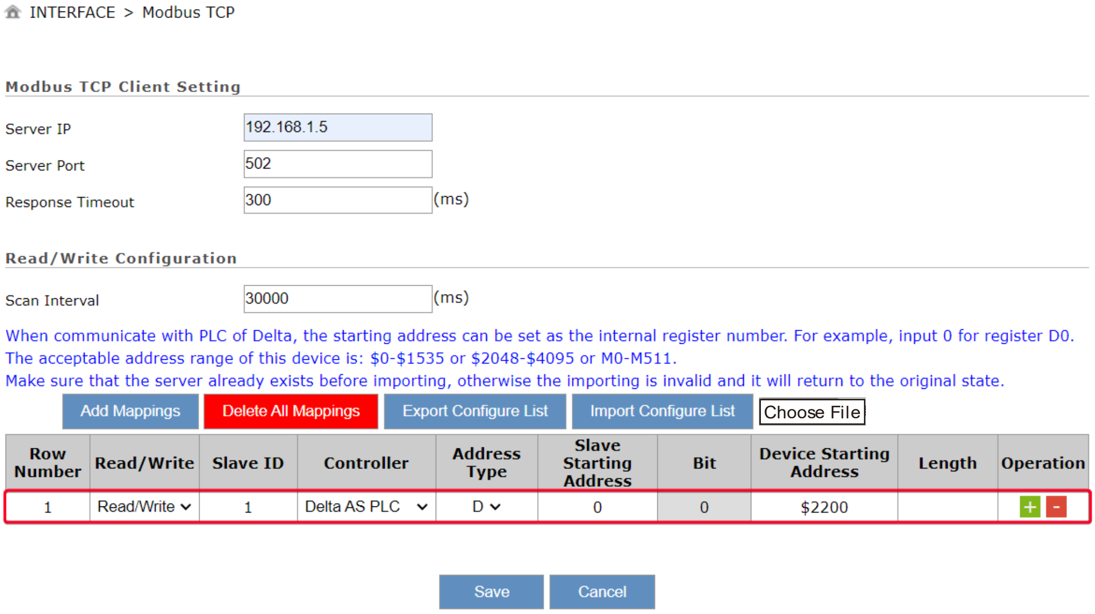
Modbus TCP

Working Mode Modbus TCP Server+Client

*32 modbus TCP servers supported at most

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

9. Click on **Add Server** and configure **PLC1 (MODBUS TCP server)** as shown in the figure below. Set the controller register to **Delta AS PLC D0**, and map the register to DX router register **$2200**, then click on **Save**.



INTERFACE > Modbus TCP

Modbus TCP Client Setting

Server IP: 192.168.1.5

Server Port: 502

Response Timeout: 300 (ms)

Read/Write Configuration

Scan Interval: 30000 (ms)

- When communicate with PLC of Delta, the starting address can be set as the internal register number. For example, input 0 for register D0.
- The acceptable address range of this device is: $0-$1535 or $2048-$4095 or M0-M511.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Read/Write	Slave ID	Controller	Address Type	Slave Starting Address	Bit	Device Starting Address	Length	Operation
1	Read/Write	1	Delta AS PLC	D	0	0	$2200		+ -

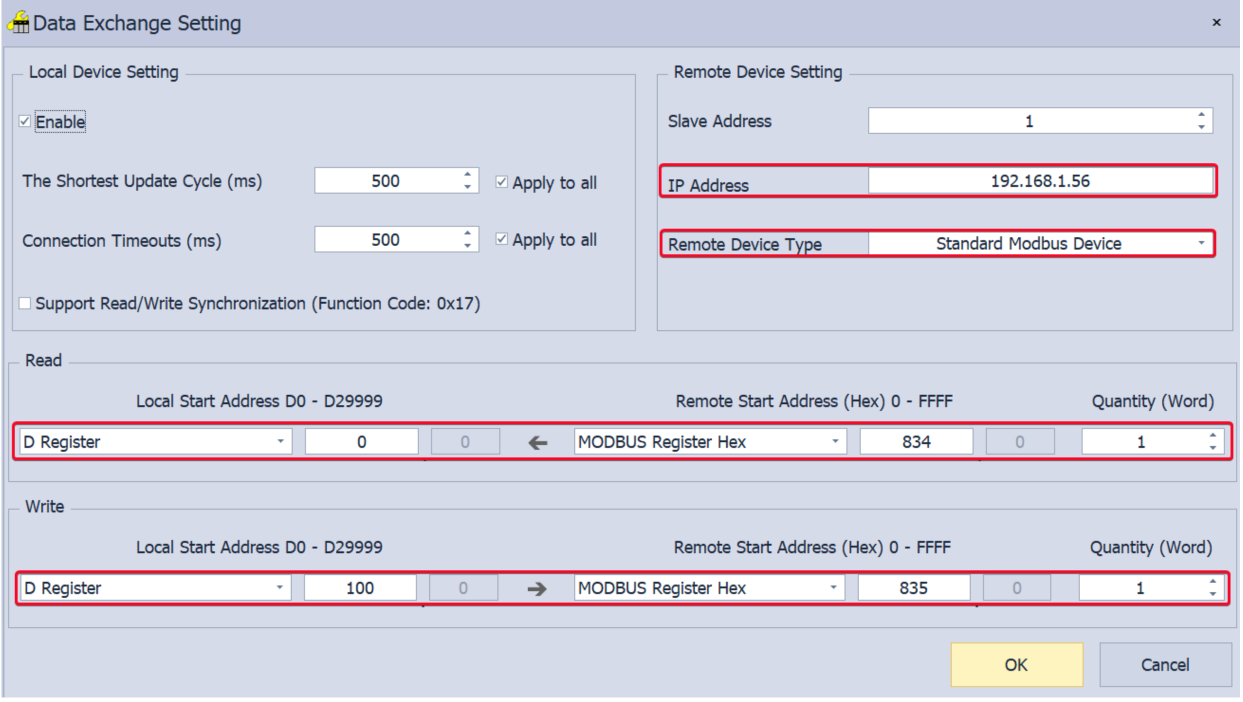
10. Click on "**Add Mappings**" and configure **PLC2 (MODBUS TCP client).**

11. Use ISP Soft to log in to the PLC2 configuration page.

12. The data exchange settings as shown in the figure below:

   a) Read the DX Router register $2101 and store it in PLC2 D0 register.

   b) Write PLC2 D100 register to the DX Cloud Router register $2101.



Data Exchange Setting

Local Device Setting

☑ Enable

The Shortest Update Cycle (ms): 500 ☑ Apply to all

Connection Timeouts (ms): 500 ☑ Apply to all

□ Support Read/Write Synchronization (Function Code: 0x17)

Remote Device Setting

Slave Address: 1

IP Address: 192.168.1.56

Remote Device Type: Standard Modbus Device

Read

Local Start Address D0 - D29999				Remote Start Address (Hex) 0 - FFFF			Quantity (Word)
D Register	0	0	←	MODBUS Register Hex	834	0	1

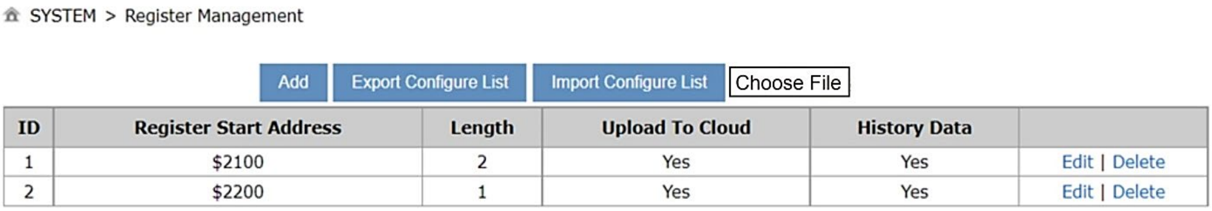
Write

Local Start Address D0 - D29999				Remote Start Address (Hex) 0 - FFFF			Quantity (Word)
D Register	100	0	→	MODBUS Register Hex	835	0	1

DX Router register addresses

Internal Registers	DEC	HEX	Description	Notes
$2048~$4095	2048~4095	800~FFF	Holding register address	
M0~M511	1536~2047	600~7FF	Coil register address	

13. Go to **SYSTEM** → **Register Management**, add registers $2100, $2200 for uploading to DIACloud, as shown in the figure below, then click on Save.

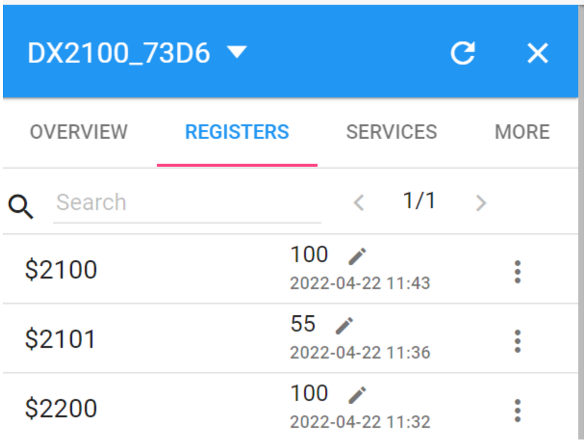


SYSTEM > Register Management

ID	Register Start Address	Length	Upload To Cloud	History Data	
1	$2100	2	Yes	Yes	Edit | Delete
2	$2200	1	Yes	Yes	Edit | Delete

14. Modify the value of PLC1 D0 register to 100, and modify the value of PLC1 D100 to 55.

15. Login to diacloudsolutions.com, select **DEVICES** → ··· More → **REGISTERS**, The registers $2100, $2101, and $2200 will display the data from Delta PLC1 and PLC2.

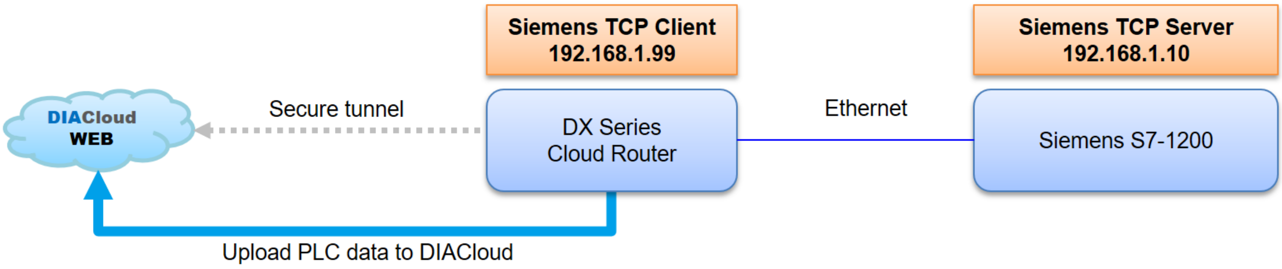


$2100	100 2022-04-22 11:43	
$2101	55 2022-04-22 11:36	
$2200	100 2022-04-22 11:32	

2.3.4 Siemens Data Collection Application

The Cloud Router can be configured to exchange data with Siemens S7-1200 PLC using Siemens TCP and upload the data to DIACloud.

Please refer to Chapter 3.4.3 Siemens TCP for a detailed explanation of the configuration parameters.



Setup Steps

1. Make sure that all the basic configuration detailed in Chapter 2 has been completed and functions properly.

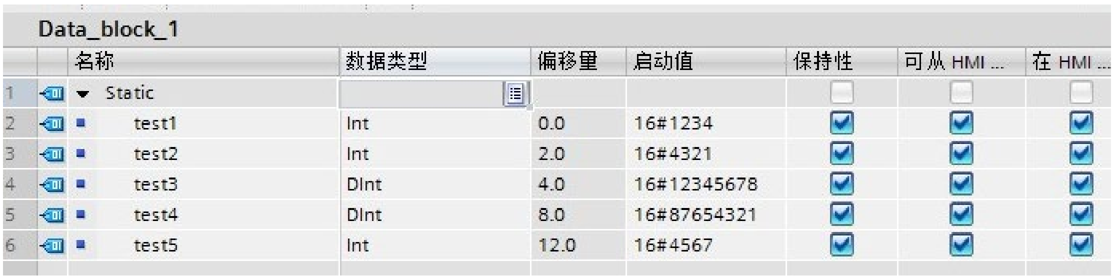
2. Use a network cable to connect LAN ports on your PC and the DX router.

3. Configure the Siemens PLC S7-1200 IP address and data blocks as follows.

Siemens S7-1200 PLC Parameters

IP Address	192.168.1.10
Local TSAP	102
Remote TSAP	100
Response Timeout	300ms

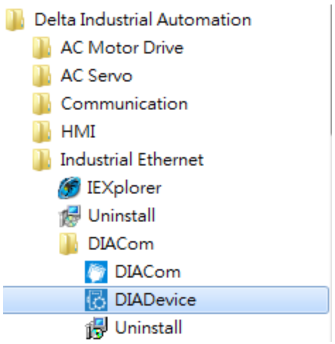
Siemens S7-1200 PLC Data Block Settings



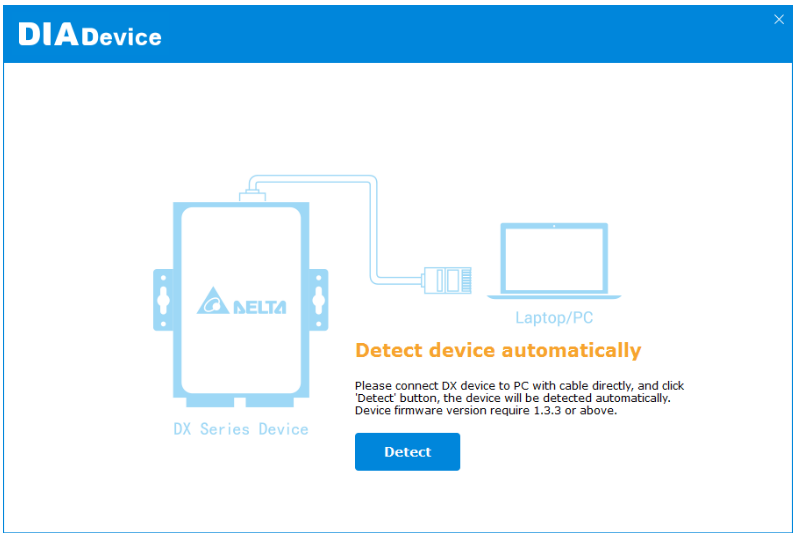
Data_block_1

	名称	数据类型	偏移量	启动值	保持性	可从 HMI ...	在 HMI ...
1	Static				□	□	□
2	test1	Int	0.0	16#1234	☑	☑	☑
3	test2	Int	2.0	16#4321	☑	☑	☑
4	test3	DInt	4.0	16#12345678	☑	☑	☑
5	test4	DInt	8.0	16#87654321	☑	☑	☑
6	test5	Int	12.0	16#4567	☑	☑	☑

4. Install DIACom software, open DIADevice: Click Windows Start icon → **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice.**



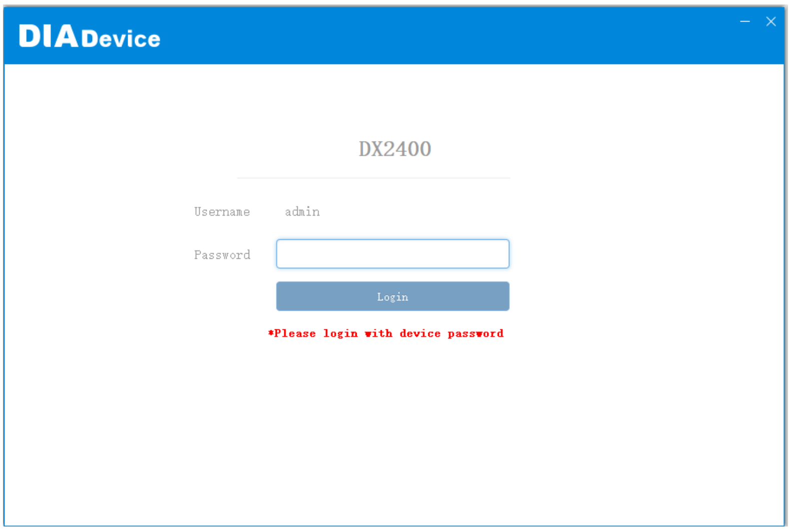
5. Click on **Detect**, and it will redirect to the login page of DX router.



Detect device automatically

Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically.
Device firmware version require 1.3.3 or above.

6. Enter your account and password. (Default: admin/admin)

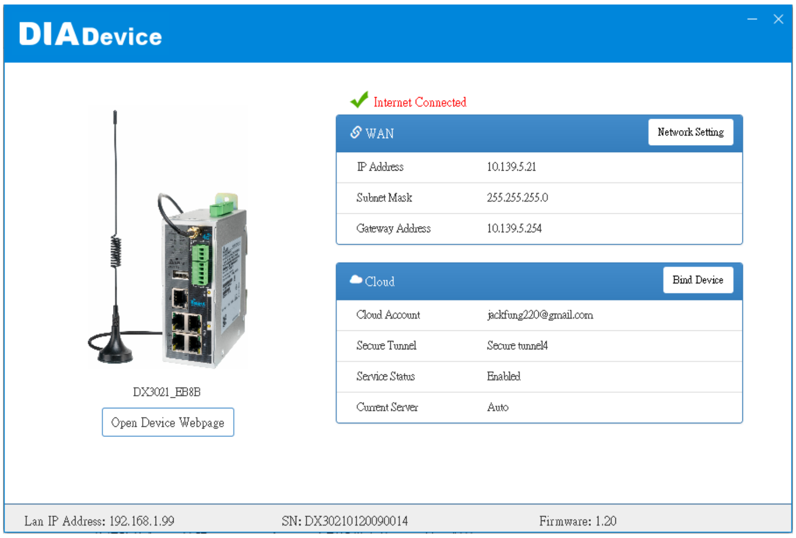


Username admin

Password

*Please login with device password

7. Click on **Open Device Webpage** and verify that the bound IP address is 192.168.1.99.



DX3021_EB8B

Internet Connected

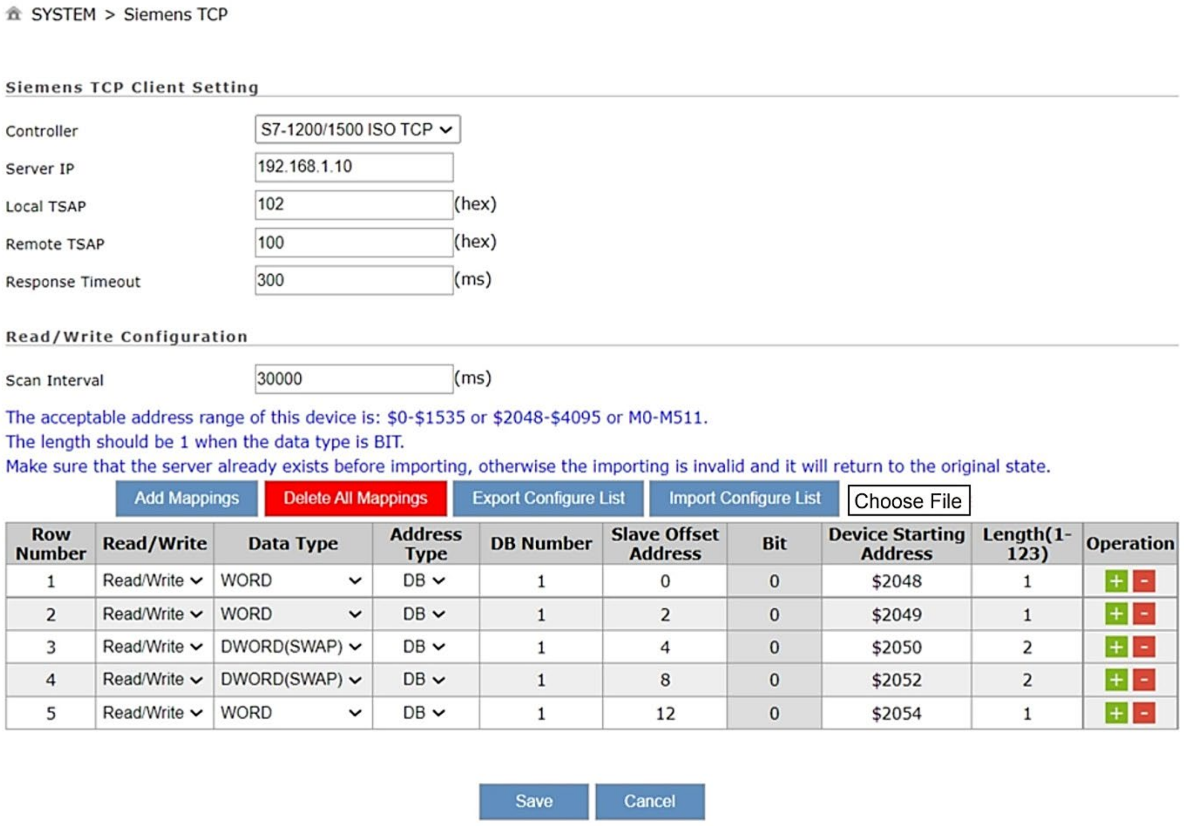
IP Address	10.139.5.21
Subnet Mask	255.255.255.0
Gateway Address	10.139.5.254

Cloud Account	jackfung220@gmail.com
Secure Tunnel	Secure tunnel4
Service Status	Enabled
Current Server	Auto

Lan IP Address: 192.168.1.99 SN: DX30210120090014 Firmware: 1.20

8. After entering DX router login page, input your account and password. (Default: admin/admin) and click on **login**.

9. Go to **SYSTEM** → **Sienmens TCP**, click on **Add Server**. Configure Siemens S7-1200 as shown in the following image.



SYSTEM > Siemens TCP

Siemens TCP Client Setting

Controller	S7-1200/1500 ISO TCP
Server IP	192.168.1.10
Local TSAP	102 (hex)
Remote TSAP	100 (hex)
Response Timeout	300 (ms)

Read/Write Configuration

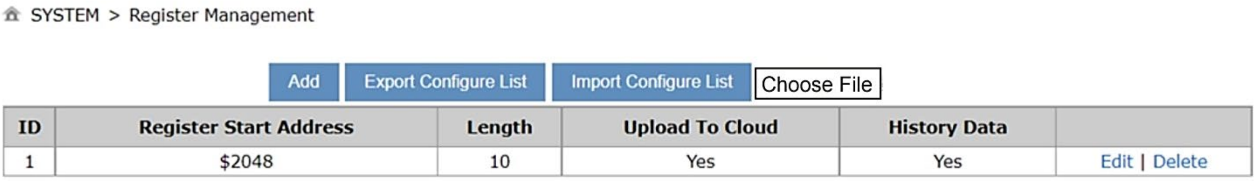
Scan Interval	30000 (ms)

- The acceptable address range of this device is: $0-$1535 or $2048-$4095 or M0-M511.
- The length should be 1 when the data type is BIT.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Read/Write	Data Type	Address Type	DB Number	Slave Offset Address	Bit	Device Starting Address	Length(1-123)	Operation
1	Read/Write	WORD	DB	1	0	0	$2048	1	+ -
2	Read/Write	WORD	DB	1	2	0	$2049	1	+ -
3	Read/Write	DWORD(SWAP)	DB	1	4	0	$2050	2	+ -
4	Read/Write	DWORD(SWAP)	DB	1	8	0	$2052	2	+ -
5	Read/Write	WORD	DB	1	12	0	$2054	1	+ -

Siemens S7-1200 PLC Data Block				Register mapping relationship	Register	
Name	Data Types	Offset	Space		Address	Data Types
test1	int	0.0	0.0~1.7	↔	**$2048**	DB
test2	int	2.0	2.1~3.7	↔	**$2049**	DB
test3	Dint	4.0	3.0~4.7	⤨	**$2050**	DB(SWAP)
			5.0~6.7		**$2051**	
test4	Dint	8.0	8.0~9.7	⤨	**$2052**	DB(SWAP)
			10.0~11.7		**$2053**	
test5	int	12.0	12.0~13.7	↔	**$2054**	DB

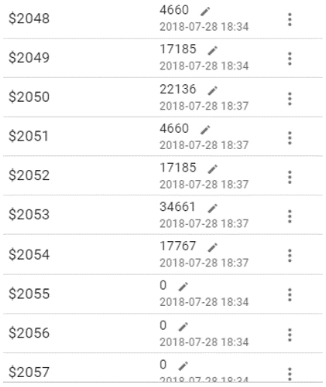
10. Go to **SYSTEM** → **Register Management** to set the Register Address for data uploads to DIACloud. Click on “Add”, add the register address as follows.



SYSTEM > Register Management

ID	Register Start Address	Length	Upload To Cloud	History Data	
1	$2048	10	Yes	Yes	Edit | Delete

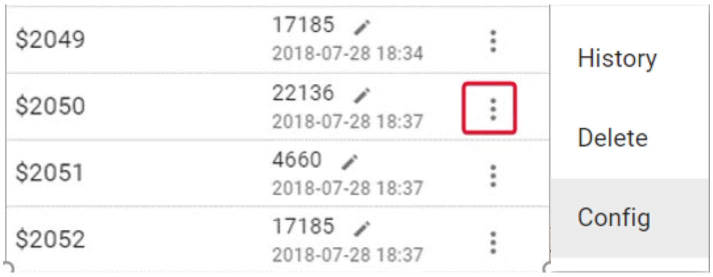
11. Login to diacloudsolutions.com, select **DEVICES** → ⋮ More → **REGISTERS**, The registers $2048 ~ $2057 will display the data from Siemens S7-1200 PLC.



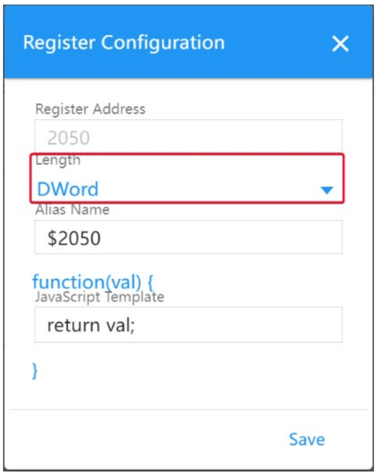
$2048	4660 2018-07-28 18:34	⋮
$2049	17185 2018-07-28 18:34	⋮
$2050	22136 2018-07-28 18:37	⋮
$2051	4660 2018-07-28 18:37	⋮
$2052	17185 2018-07-28 18:37	⋮
$2053	34661 2018-07-28 18:37	⋮
$2054	17767 2018-07-28 18:37	⋮
$2055	0 2018-07-28 18:34	⋮
$2056	0 2018-07-28 18:34	⋮
$2057	0 2018-07-28 18:34	⋮

12. Due to ($2050, $2051) and ($2052, $2053) being Din data, which is 32 bits in length, the data needs to be displayed as DWord data type.

13. For $2050 and $2052, click ⋮ More and click **Config** so as to set Length to DWord.



$2049	17185 2018-07-28 18:34	⋮
$2050	22136 2018-07-28 18:37	⋮
$2051	4660 2018-07-28 18:37	⋮
$2052	17185 2018-07-28 18:37	⋮



Register Configuration ✕

Register Address: 2050

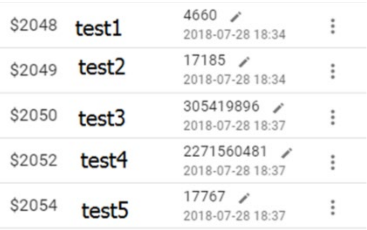
Length: DWord

Alias Name: $2050

JavaScript Template:

```
function(val) {
return val;
}
```

14. The data value would be displayed as shown in the following figure.

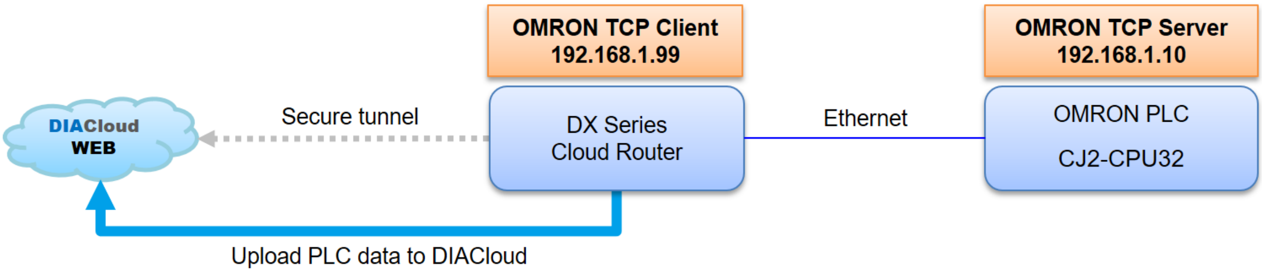


$2048	test1	4660 2018-07-28 18:34	⋮
$2049	test2	17185 2018-07-28 18:34	⋮
$2050	test3	305419896 2018-07-28 18:37	⋮
$2052	test4	2271560481 2018-07-28 18:37	⋮
$2054	test5	17767 2018-07-28 18:37	⋮

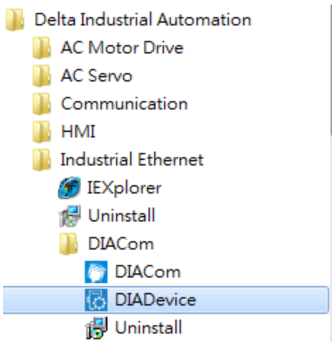
2.3.5 OMRON Data Collection Application

Supports FINS TCP Client to exchange data with Omron CJ2-CPU32 PLC and upload the data to DIACloud.

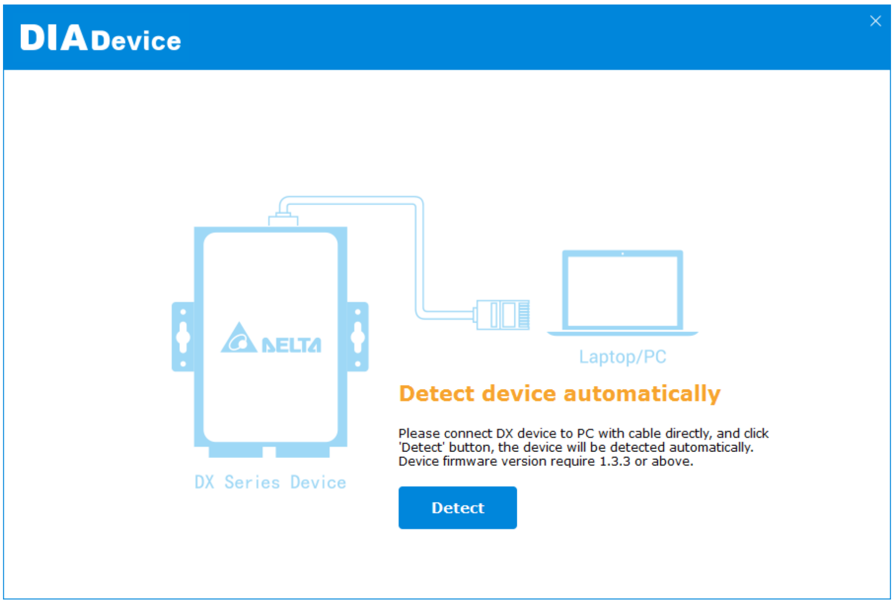
Please refer to Chapter 3.4.4 OMRON Fins for a detailed explanation of the configuration parameters.



1. Make sure that all the basic configuration detailed in chapter 2 has been completed and functions properly.
2. Change the Omron PLC IP address to 192.168.1.10.
3. Use a network cable to connect LAN ports on your PC and the DX router.
4. Install DIACom software, open DIADevice: Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice**.

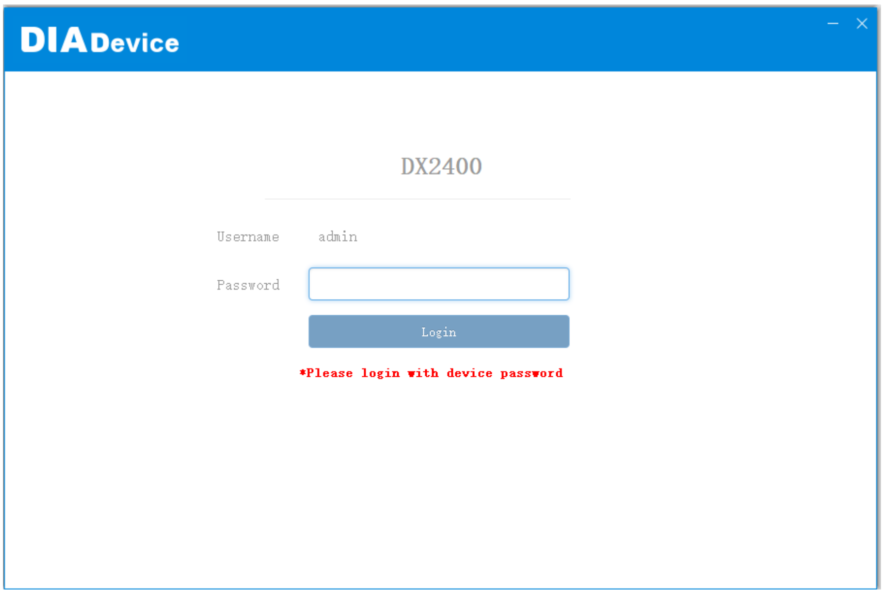


5. Click **Detect**, and it will redirect to the login page of DX router.



Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically.
Device firmware version require 1.3.3 or above.

6. Enter your account and password. (Default: admin/admin)



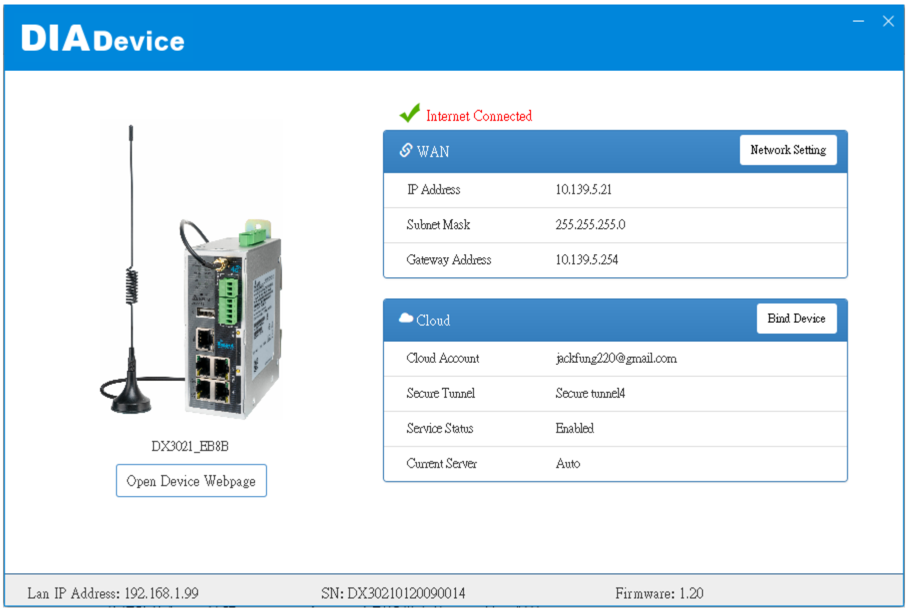
DX2400

Username admin

Password

*Please login with device password

7. Click on **Open Device Webpage** and verify that the bound IP address is 192.168.1.99.



✓ Internet Connected

WAN	
IP Address	10.139.5.21
Subnet Mask	255.255.255.0
Gateway Address	10.139.5.254

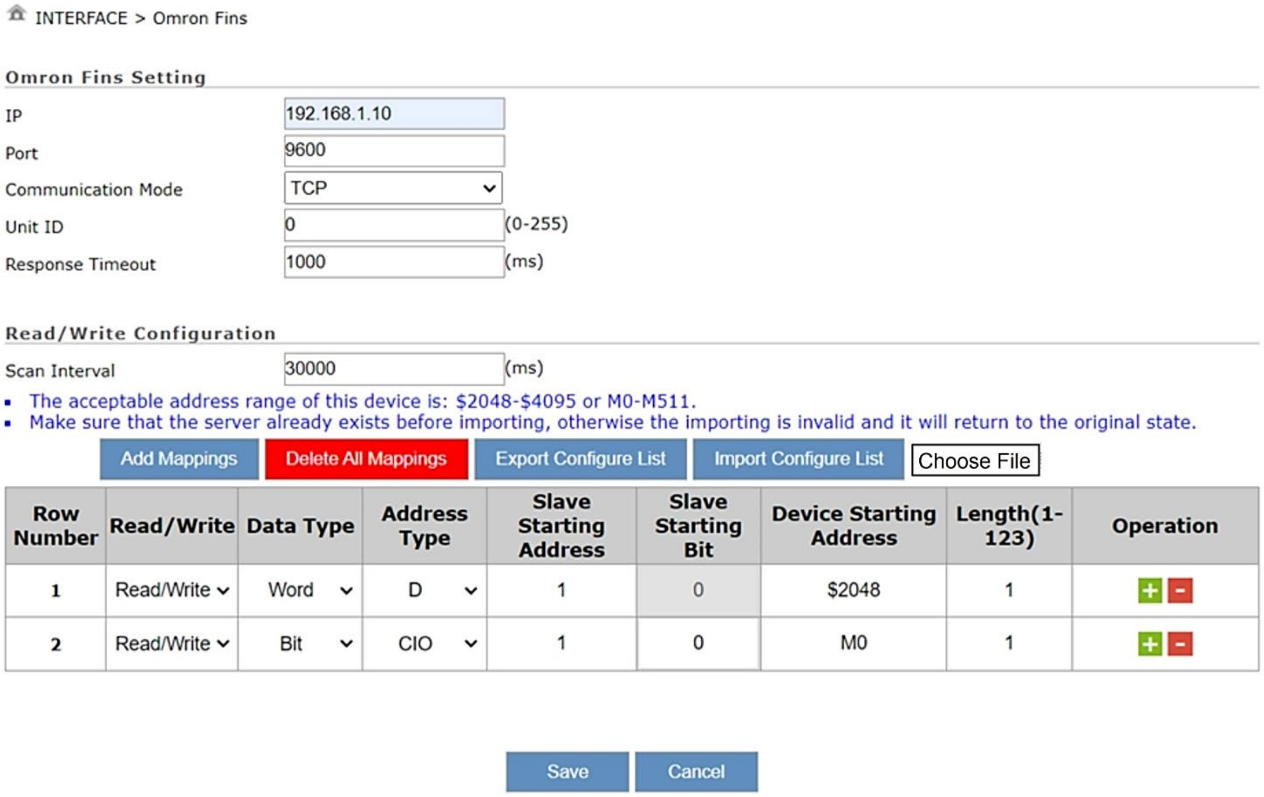
Cloud	
Cloud Account	jackfung220@gmail.com
Secure Tunnel	Secure tunnel4
Service Status	Enabled
Current Server	Auto

DX3021_EB8B

Lan IP Address: 192.168.1.99 SN: DX30210120090014 Firmware: 1.20

8. After entering DX router login page, input your account and password. (Default: admin/admin) and click login.

9. Go to **INTERFACE** → **Omron Fins**, click on **Add PLC**, configure the Omron CJ2-CPU32 PLC as shown in the following image.



INTERFACE > Omron Fins

Omron Fins Setting

IP	192.168.1.10
Port	9600
Communication Mode	TCP
Unit ID	0 (0-255)
Response Timeout	1000 (ms)

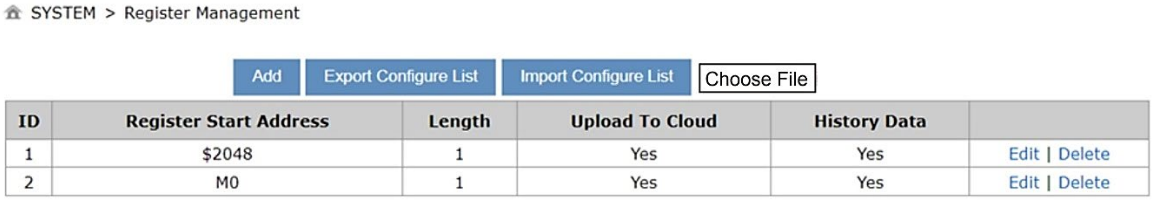
Read/Write Configuration

Scan Interval 30000 (ms)

- The acceptable address range of this device is: $2048-$4095 or M0-M511.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Read/Write	Data Type	Address Type	Slave Starting Address	Slave Starting Bit	Device Starting Address	Length(1-123)	Operation
1	Read/Write	Word	D	1	0	$2048	1	+ -
2	Read/Write	Bit	CIO	1	0	M0	1	+ -

10. Go to **SYSTEM** → **Register Management**, add $2048 and M0 registers for data uploads to DIACloud, as shown in the following image. Then, click on Save.



SYSTEM > Register Management

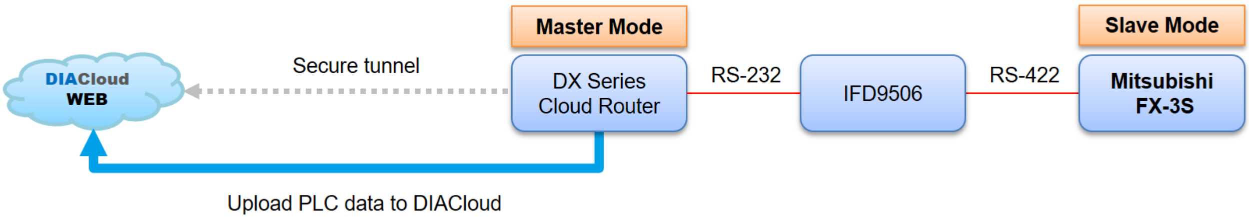
ID	Register Start Address	Length	Upload To Cloud	History Data	
1	$2048	1	Yes	Yes	Edit | Delete
2	M0	1	Yes	Yes	Edit | Delete

11. Login to diacloudsolutions.com, select **DEVICES** → **REGISTERS**, The registers $2048, M0 will display the data from Omron CJ2-CPU32 PLC.

2.3.6 Mitsubishi Data Collection Application

As the Master, DX Router reads data from Mitsubishi FX-3S and uploads the data to DIACloud.

Please refer to Chapter 3.4.1.8 MC Master Mode for a detailed explanation of the configuration parameters.



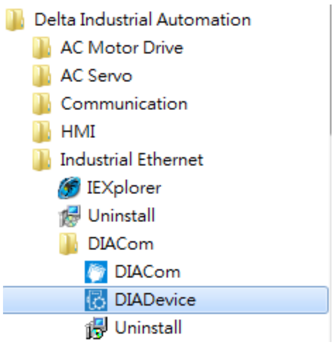
Setup Steps

1. Make sure that all the basic configuration detailed in chapter 2 has been completed and functions properly.

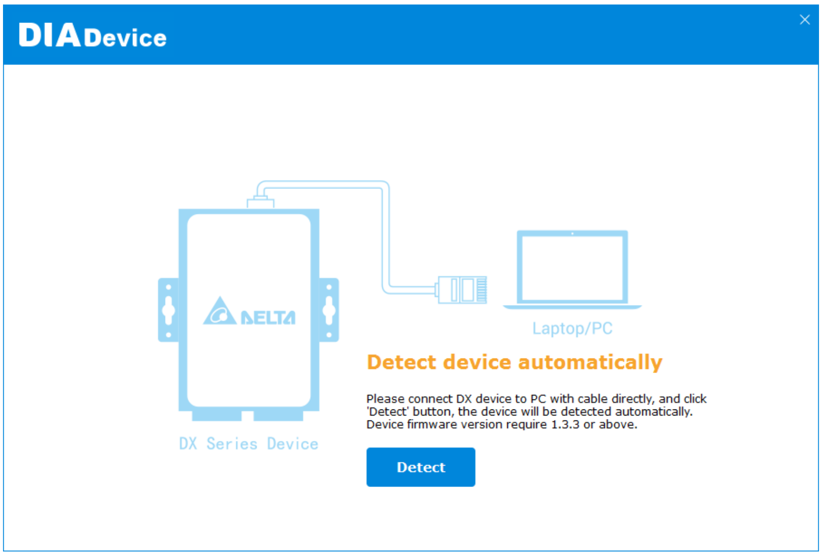
2. Connect the industrial device to the DX cloud router via RS232, then change the industrial device's transfer format to 9600/8/N/1/RTU.

3. Use a network cable to connect LAN ports on your PC and the DX router.

4. Install DIACom software, open DIADevice: Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice**.

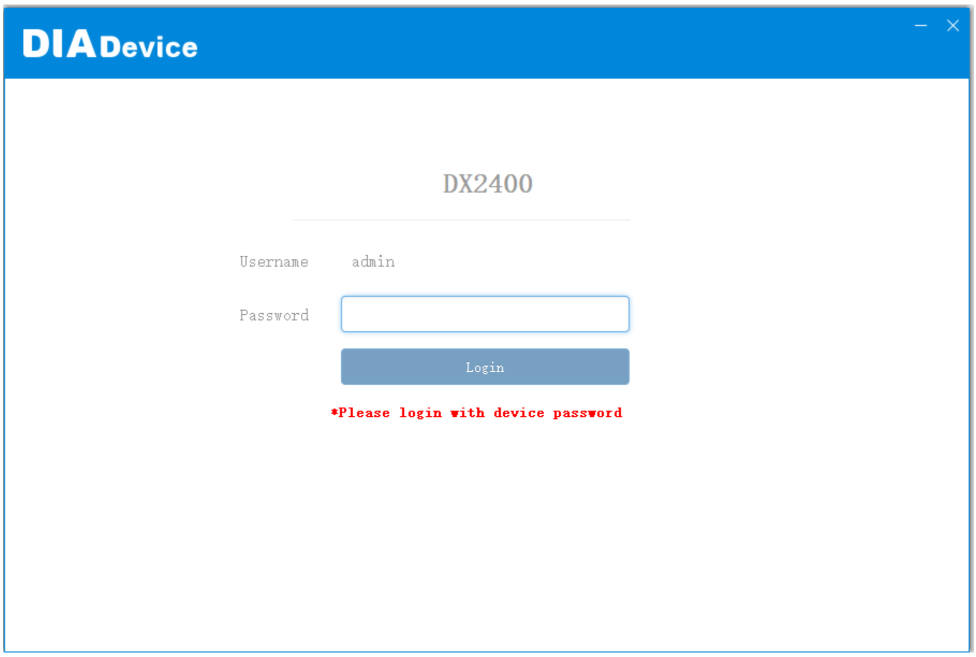


5. Click on **Detect**, and it will redirect to the login page of DX router.



Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

6. Enter your account and password. (Default: admin/admin)



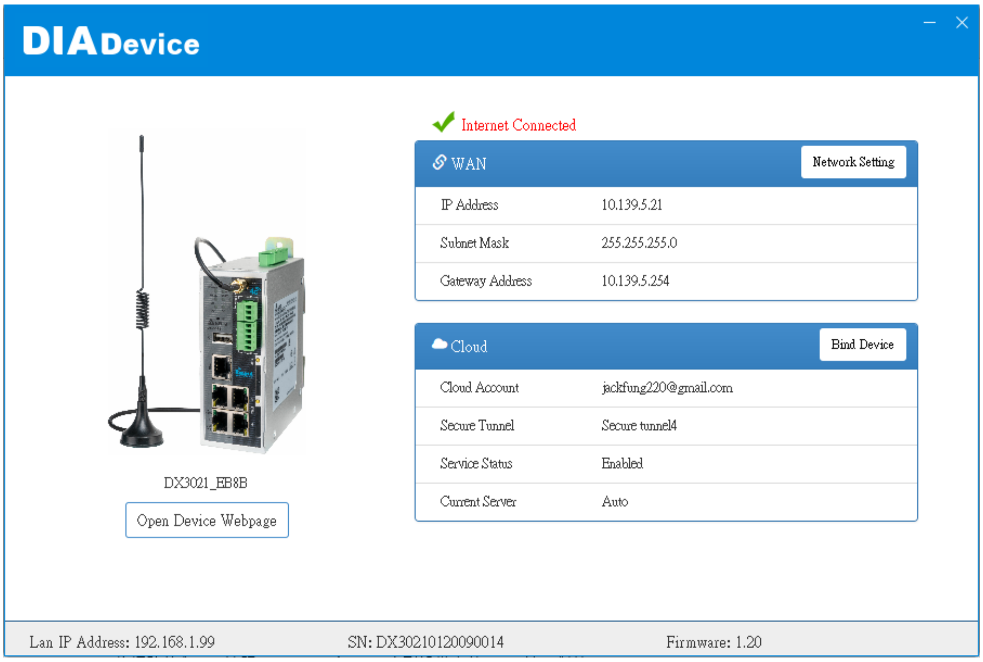
DX2400

Username admin

Password

*Please login with device password

7. Click on **Open Device Webpage** and verify that the bound IP address is 192.168.1.99.



✓ Internet Connected

WAN	
IP Address	10.139.5.21
Subnet Mask	255.255.255.0
Gateway Address	10.139.5.254

Cloud	
Cloud Account	jackfung220@gmail.com
Secure Tunnel	Secure tunnel4
Service Status	Enabled
Current Server	Auto

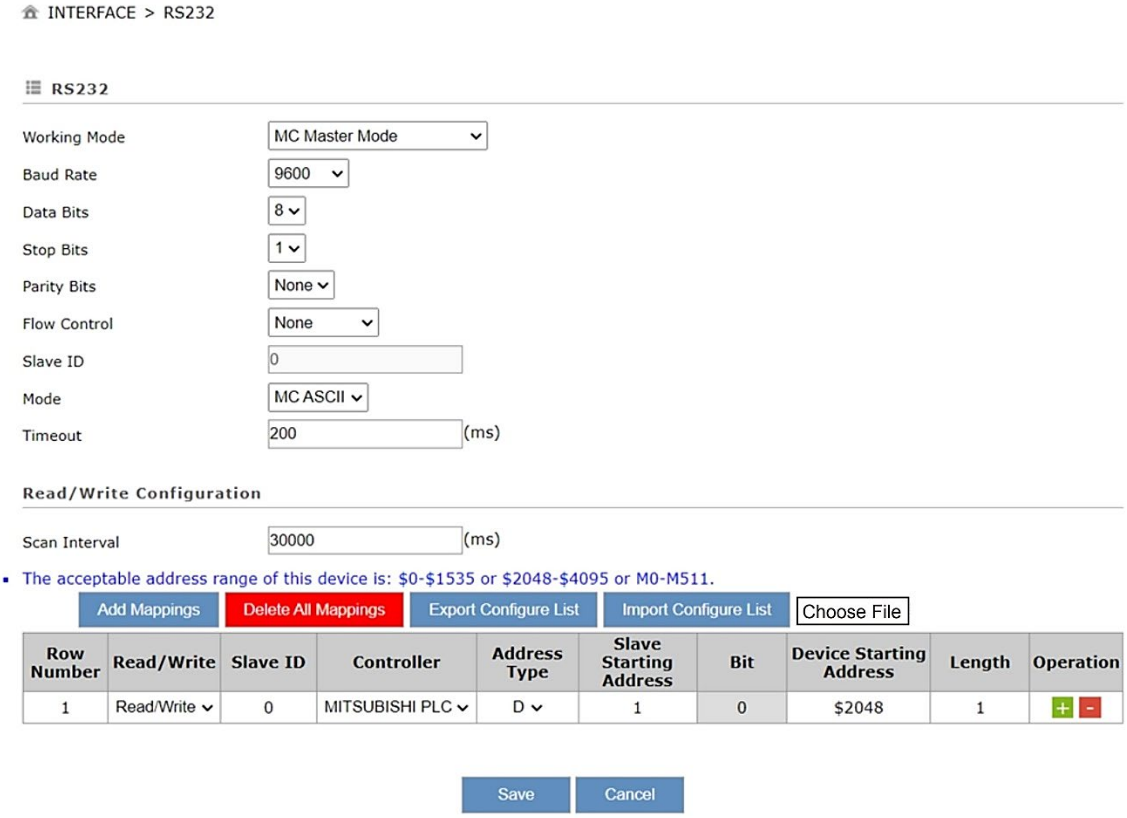
DX3021_EB8B

Lan IP Address: 192.168.1.99 SN: DX30210120090014 Firmware: 1.20

8. After entering DX router login page, input your account and password. (Default: admin/admin) and click on **login**.

9. Go to **INTERFACE** → **RS232**, select **MC Master Mode** as working mode. Set the communication parameters as 9600/8/N/1, Mode: MC ASCII, then click on **Save**.

10. Connect DX router to IFD8500 using RS-232, and then connect IFD8500 to Mitsubishi FX-3S using RS-422.



INTERFACE > RS232

RS232

Working Mode	MC Master Mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Flow Control	None
Slave ID	0
Mode	MC ASCII
Timeout	200 (ms)

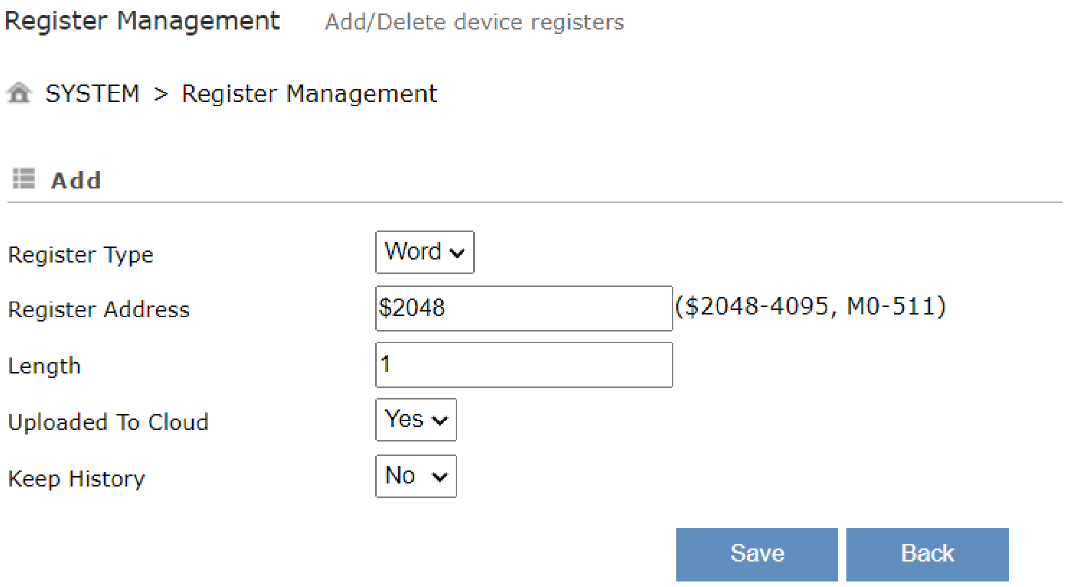
Read/Write Configuration

Scan Interval 30000 (ms)

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

Row Number	Read/Write	Slave ID	Controller	Address Type	Slave Starting Address	Bit	Device Starting Address	Length	Operation
1	Read/Write	0	MITSUBISHI PLC	D	1	0	$2048	1	+ -

12. Go to **SYSTEM** → **Register Management** to set the Register Address for data uploads to DIACloud. Click on "Add" and key in the following items: Register Address: $2048, Length: 1. Then click on Save.



Register Management Add/Delete device registers

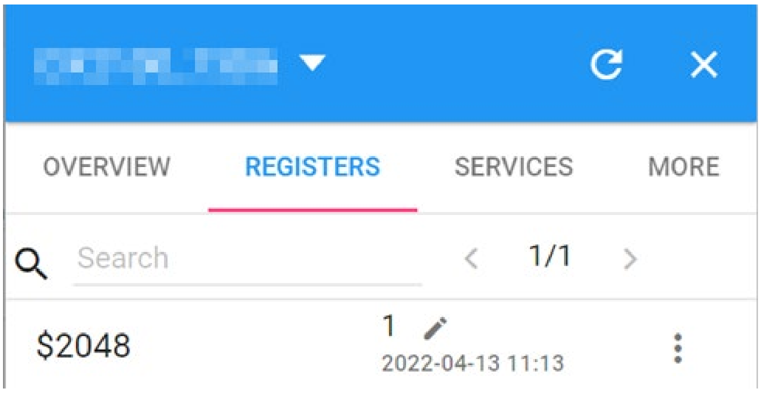
SYSTEM > Register Management

Add

Register Type	Word
Register Address	$2048 ($2048-4095, M0-511)
Length	1
Uploaded To Cloud	Yes
Keep History	No

13. Change the data of PLC Mitsubishi FX-3S register D0 to 1.

14. Login to diacloudsolutions.com, and go to **DEVICES** → ⋮ More → **REGISTERS**, you will see $2048 displayed as 1.



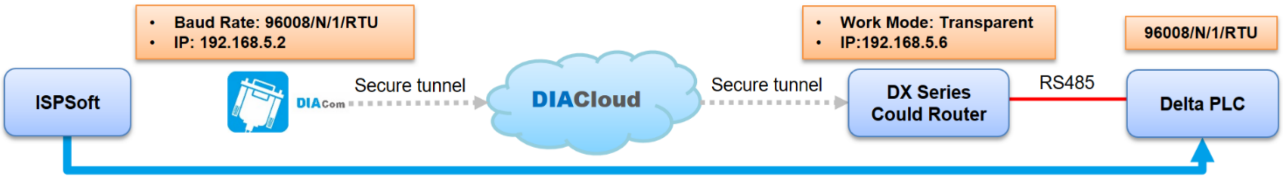
$2048 1 2022-04-13 11:13

2.3.7 RS485 Application for Remote Connection

Performing remote data upload and download to the PLC program using RS485 connection.

****Not recommended for continuous 24-hour monitoring. If required, please use DIACloud Restful API to achieve the goal.**

Please refer to Chapter 3.4.1 RS-232/RS485 for a detailed explanation of the configuration parameters.



Remote access via DIACloud

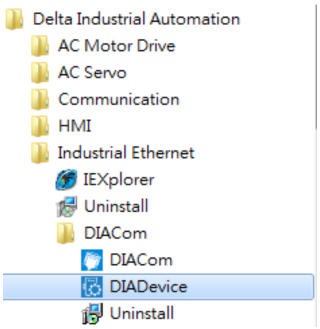
Setup Steps

1. Make sure that all the basic configuration detailed in chapter 2 has been completed and functions properly.

2. Connect the industrial device to the DX cloud router via RS485, then change the industrial device's transfer format to **9600/8/N/1/RTU**.

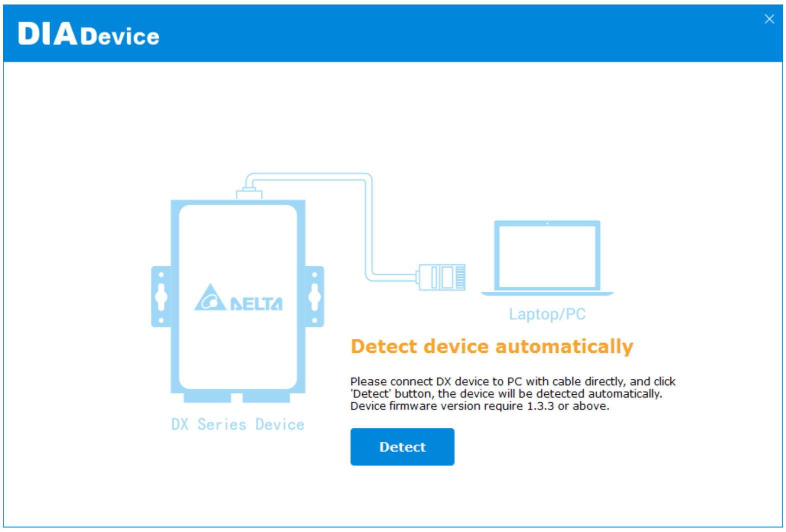
3. Use a network cable to connect LAN ports on your PC and the DX router.

4. Open DIADevice**:** Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice.**



5. Connect the device to the power supply, and connect the device to the PC using a network cable.

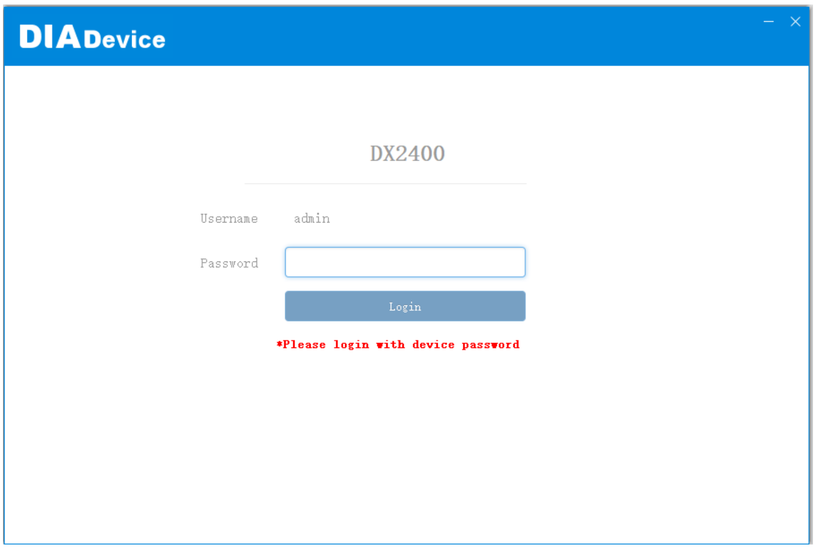
6. Click on **Detect.**



Detect device automatically

Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

7. After detected the device, it will automatically redirect to the login page. Enter your account and password.(Default: admin/admin)



DIADevice

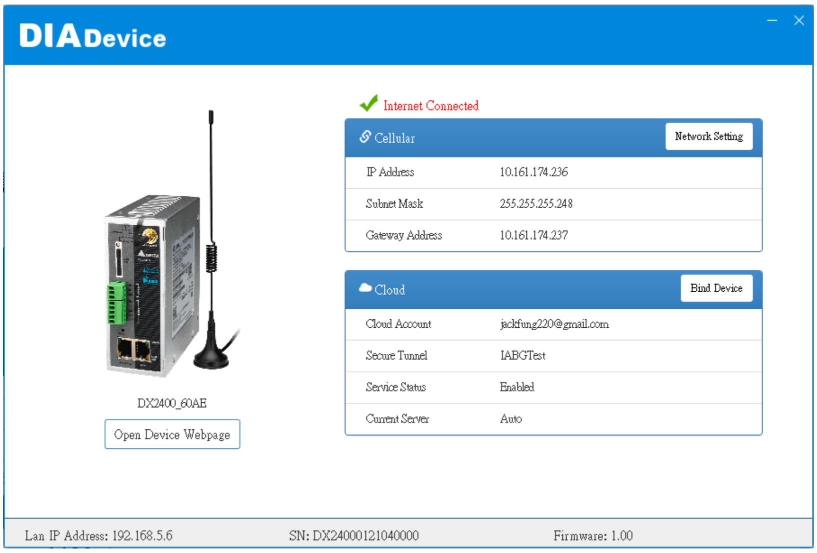
DX2400

Username admin

Password

*Please login with device password

8. Click on **Open Device Webpage**.



DIADevice

✓ Internet Connected

Cellular

IP Address	10.161.174.236
Subnet Mask	255.255.255.248
Gateway Address	10.161.174.237

Cloud

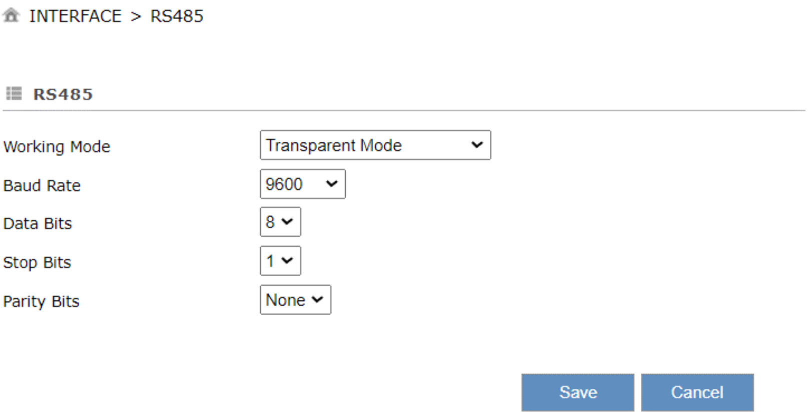
Cloud Account	jackfung220@gmail.com
Secure Tunnel	IABGTest
Service Status	Enabled
Current Server	Auto

DX2400_60AE

Lan IP Address: 192.168.5.6 SN: DX24000121040000 Firmware: 1.00

9. After entering DX router login page, input your account and password. (Default: admin/admin) and click login.

10. Go to **INTERFACE** → **RS485** and select **Transparent Mode** as working mode.

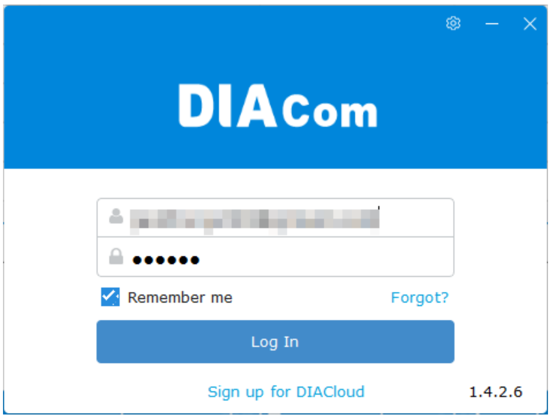


INTERFACE > RS485

RS485

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

11. Download the DIACom software from Delta's official website and install it, run the software, enter the registered DIACloud cloud account, and click on "**Login**."



DIACom

[redacted]

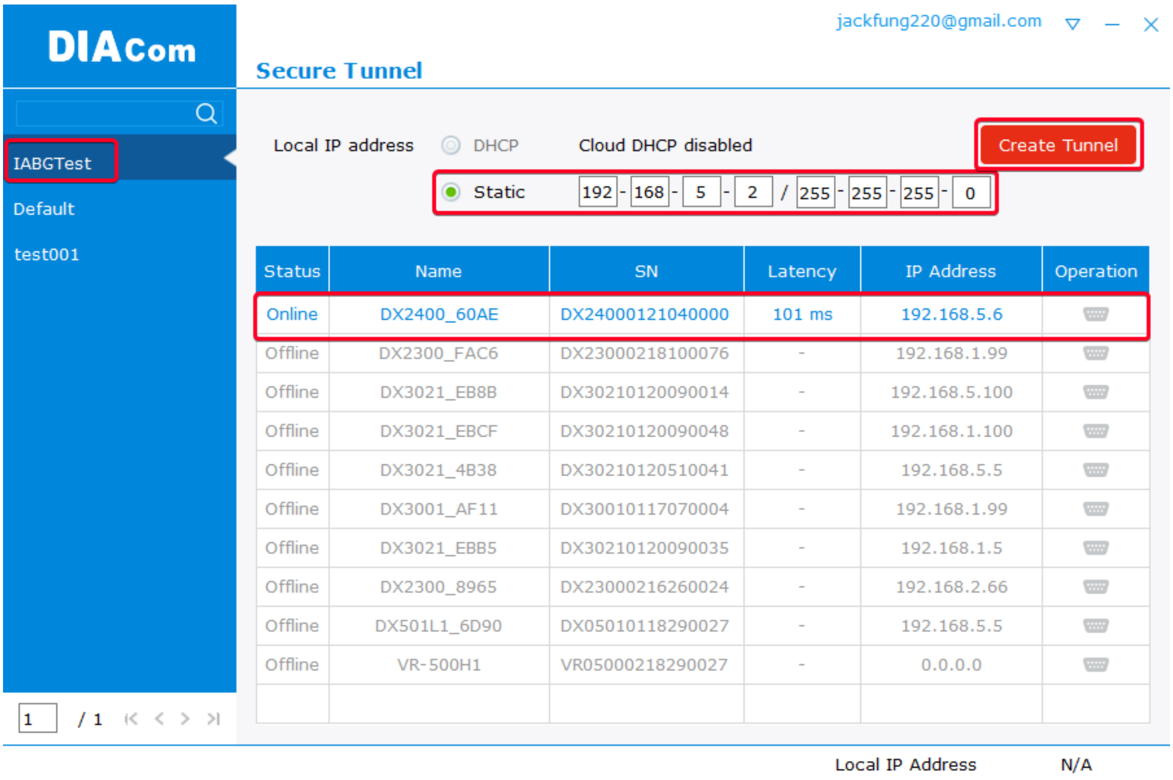
••••••

☑ Remember me Forgot?

Log In

Sign up for DIACloud 1.4.2.6

12. Select the secure tunnel which has been bound to the DX router, this example is set as default. Enter the IP address **192.168.5.2,** which belongs to the same network segment as the DX Router, in the Static blank space, then click on “**Create Tunnel**”.



DIACom

jackfung220@gmail.com

Secure Tunnel

IABGTest
Default
test001

Local IP address ○ DHCP Cloud DHCP disabled

● Static 192 - 168 - 5 - 2 / 255 - 255 - 255 - 0

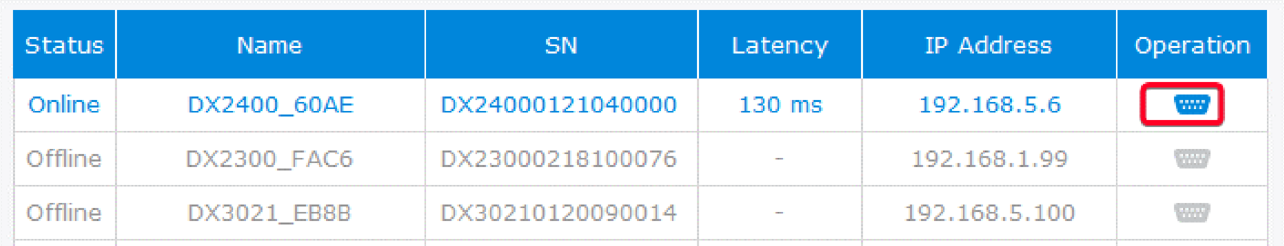
Create Tunnel

Status	Name	SN	Latency	IP Address	Operation
Online	DX2400_60AE	DX24000121040000	101 ms	192.168.5.6	⌨
Offline	DX2300_FAC6	DX23000218100076	-	192.168.1.99	⌨
Offline	DX3021_EB8B	DX30210120090014	-	192.168.5.100	⌨
Offline	DX3021_EBCF	DX30210120090048	-	192.168.1.100	⌨
Offline	DX3021_4B38	DX30210120510041	-	192.168.5.5	⌨
Offline	DX3001_AF11	DX30010117070004	-	192.168.1.99	⌨
Offline	DX3021_EBB5	DX30210120090035	-	192.168.1.5	⌨
Offline	DX2300_8965	DX23000216260024	-	192.168.2.66	⌨
Offline	DX501L1_6D90	DX05010118290027	-	192.168.5.5	⌨
Offline	VR-500H1	VR05000218290027	-	0.0.0.0	⌨

1 / 1

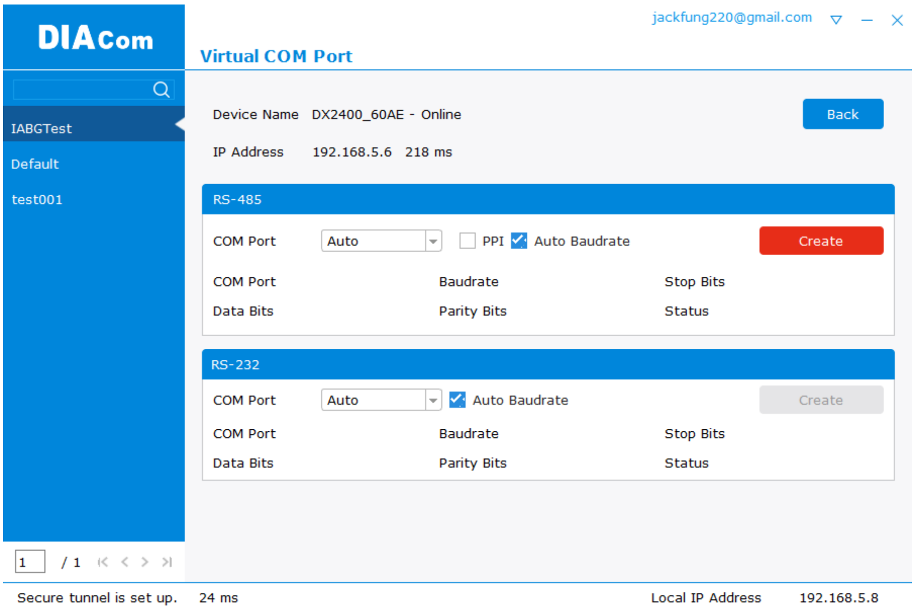
Local IP Address N/A

13. After the secure tunnel is created successfully, click ⌨ icon from the device list.



Status	Name	SN	Latency	IP Address	Operation
Online	DX2400_60AE	DX24000121040000	130 ms	192.168.5.6	⌨
Offline	DX2300_FAC6	DX23000218100076	-	192.168.1.99	⌨
Offline	DX3021_EB8B	DX30210120090014	-	192.168.5.100	⌨

14. Enter Virtual COM Port page, click **Create** in RS485 section.



Virtual COM Port

Device Name DX2400_60AE - Online

IP Address 192.168.5.6 218 ms

RS-485

COM Port: Auto □ PPI ☑ Auto Baudrate

COM Port		Baudrate		Stop Bits	
Data Bits		Parity Bits		Status	

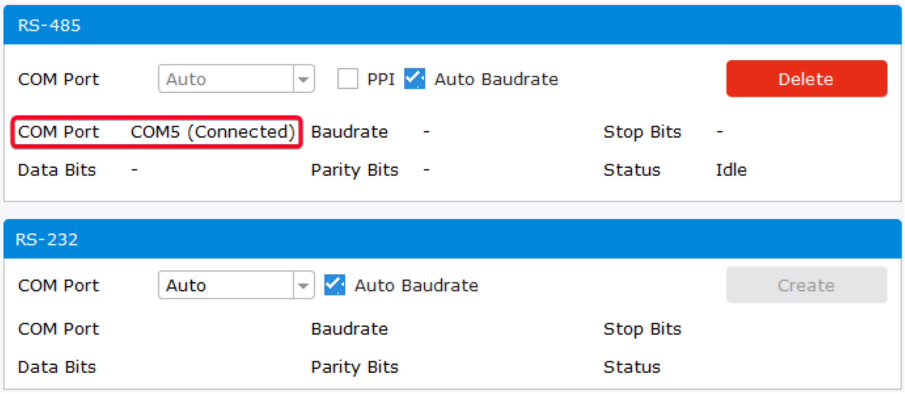
RS-232

COM Port: Auto ☑ Auto Baudrate

COM Port		Baudrate		Stop Bits	
Data Bits		Parity Bits		Status	

Secure tunnel is set up. 24 ms Local IP Address 192.168.5.8

15. When it shows **COM5 (Connected)**, it indicates that the virtual serial port COM5 has been established.



RS-485

COM Port: Auto □ PPI ☑ Auto Baudrate

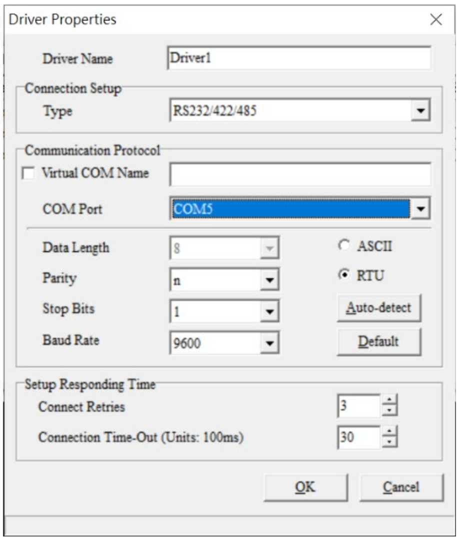
COM Port	COM5 (Connected)	Baudrate	-	Stop Bits	-
Data Bits	-	Parity Bits	-	Status	Idle

RS-232

COM Port: Auto ☑ Auto Baudrate

COM Port		Baudrate		Stop Bits	
Data Bits		Parity Bits		Status	

16. At this point, you can use the corresponding software tools, such as the following Delta/ISPSoft. By selecting COM5 as the COM Port, you can perform remote program upload and download on the PLC connected to the RS-485 port of the DX device.



Driver Properties

Driver Name: Driver1

Connection Setup
Type: RS232/422/485

Communication Protocol
□ Virtual COM Name:
COM Port: COM5

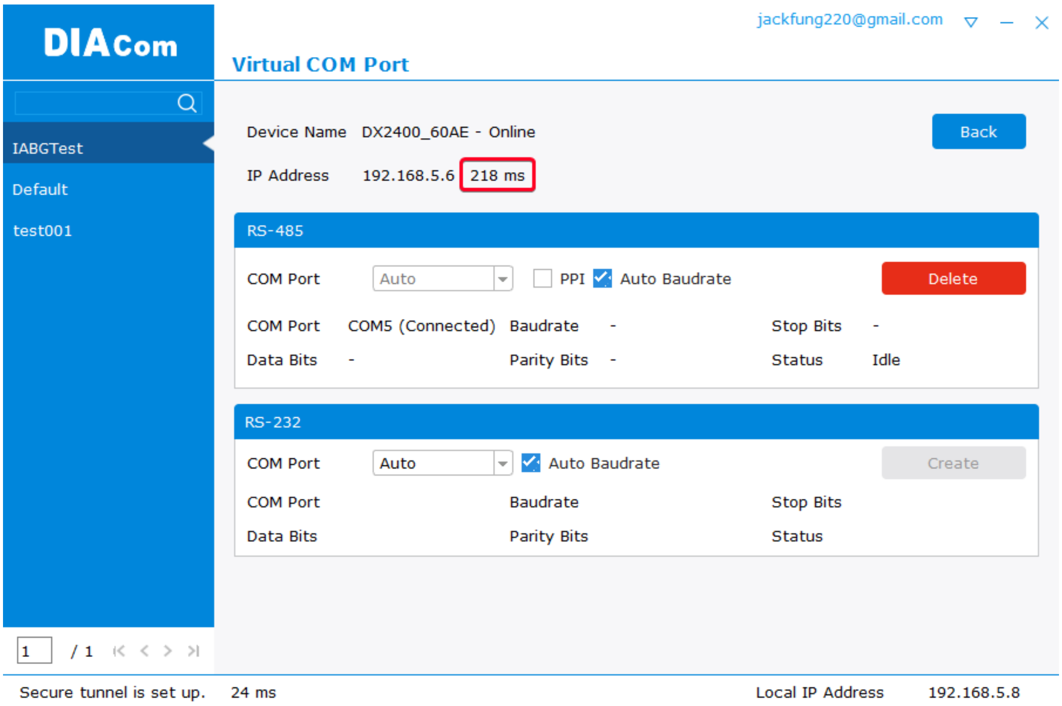
Data Length: 8
Parity: n
Stop Bits: 1
Baud Rate: 9600
○ ASCII
● RTU

Setup Responding Time
Connect Retries: 3
Connection Time-Out (Units: 100ms): 30

Troubleshooting

1. Connection failure may occur when the **"waiting for response time" setting in the device software is too short.** Please modify the the setting for a longer period of time.

2. If errors occur while uploading/downloading data, it may be caused by an unstable network. Please check if the signal strength of 4G network is too weak (all indicater lights must be lit) or check if there is a significant delay in communication between the PC and the device. If the latency is too high, consider using Ethernet connection or try using another 4G network provider.



Device Name DX2400_60AE - Online

IP Address 192.168.5.6 218 ms

RS-485

COM Port Auto □ PPI ☑ Auto Baudrate

COM Port COM5 (Connected) Baudrate - Stop Bits -

Data Bits - Parity Bits - Status Idle

RS-232

COM Port Auto ☑ Auto Baudrate

COM Port Baudrate Stop Bits

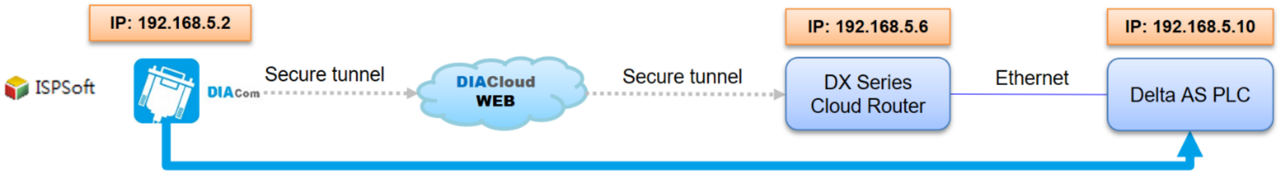
Data Bits Parity Bits Status

Secure tunnel is set up. 24 ms Local IP Address 192.168.5.8

2.3.8 Ethernet Application for Remote Connection

Remotely control PLC program and data uploads/downloads via Ethernet.

Please refer to Chapter 3.4.2 MODBUS TCP for a detailed explanation of the configuration parameters.



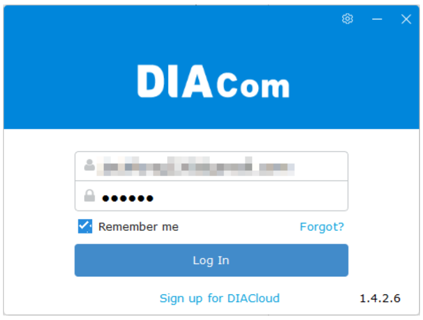
Remote connection function

Setup Steps

1. Make sure that all the basic configuration detailed in Chapter 2.2 has been completed and functions properly, which includes **the registration of cloud account, internet settings, and account binding**.

2. After connecting the industrial equipment to the LAN port of the DX router using an Ethernet cable, change the IP address of the PLC to be in the same network segment as the DX router's IP address.

3. Download the DIACom software from Delta's official website and install it, run the software, enter the registered DIACloud cloud account , then click on "**Login**".



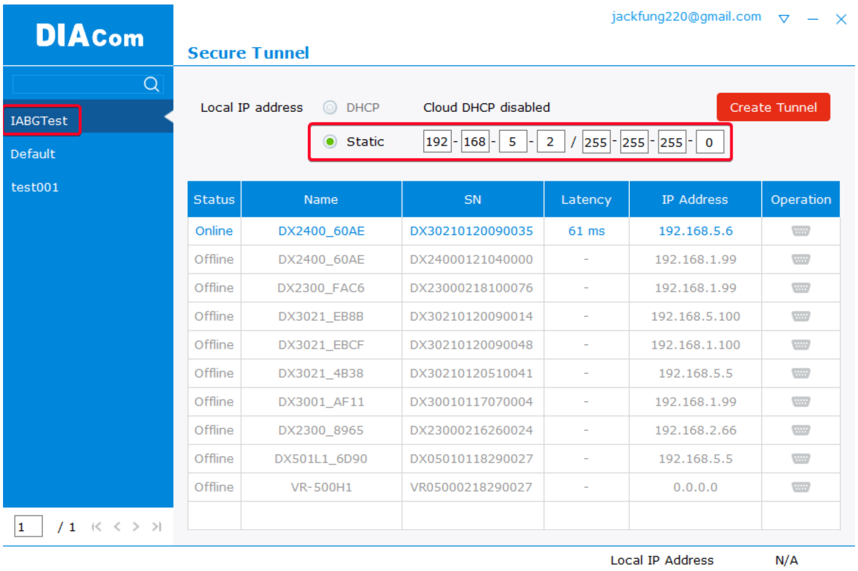
DIACom

[redacted]

••••••

☑ Remember me　Forgot?

4. Select the secure tunnel which has been bound to the DX router, this example is IABGTest. Enter the IP address **192.168.5.2**, which belongs to the same network segment as the DX Router, in the Static blank space, then click on "**Create Tunnel**".



DIACom　jackfung220@gmail.com

Secure Tunnel

Local IP address ○ DHCP　Cloud DHCP disabled

● Static 192 - 168 - 5 - 2 / 255 - 255 - 255 - 0

Status	Name	SN	Latency	IP Address	Operation
Online	DX2400_60AE	DX30210120090035	61 ms	192.168.5.6	⌨
Offline	DX2400_60AE	DX24000121040000	-	192.168.1.99	⌨
Offline	DX2300_FAC6	DX23000218100076	-	192.168.1.99	⌨
Offline	DX3021_EB8B	DX30210120090014	-	192.168.5.100	⌨
Offline	DX3021_EBCF	DX30210120090048	-	192.168.1.100	⌨
Offline	DX3021_4B38	DX30210120510041	-	192.168.5.5	⌨
Offline	DX3001_AF11	DX30010117070004	-	192.168.1.99	⌨
Offline	DX2300_8965	DX23000216260024	-	192.168.2.66	⌨
Offline	DX501L1_6D90	DX05010118290027	-	192.168.5.5	⌨
Offline	VR-500H1	VR05000218290027	-	0.0.0.0	⌨

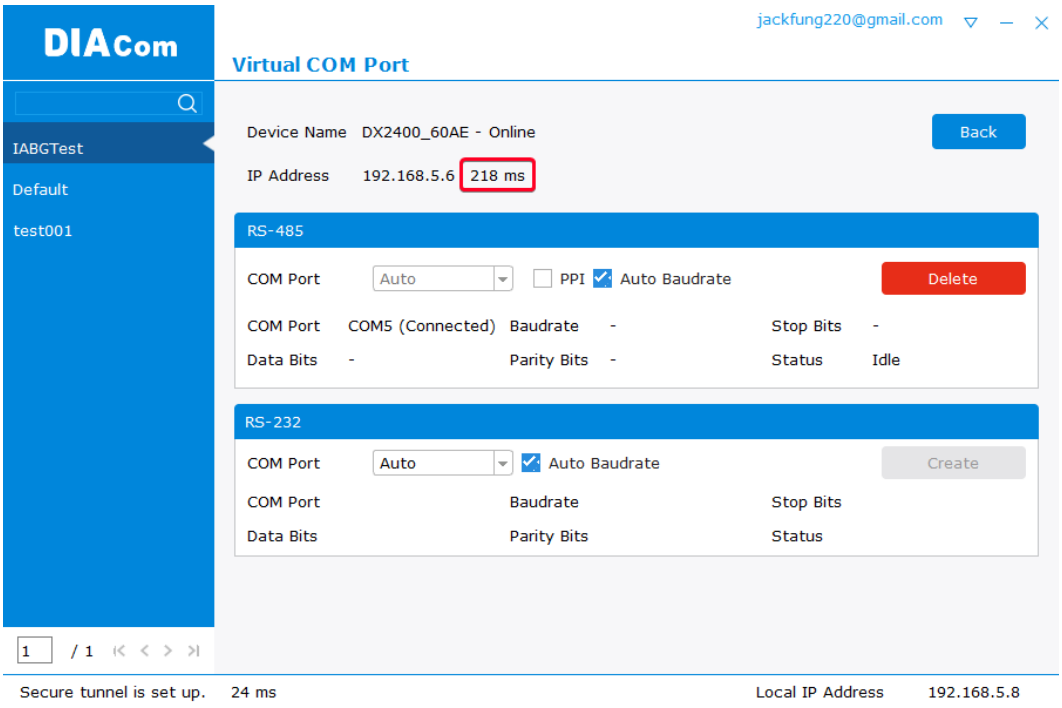
Local IP Address　N/A

5. At this point, you can use the corresponding editing software ISPSoft for Delta PLC. Select the communication type as Ethernet and configure the remote PLC IP address to establish the connection.

Troubleshooting

1. Connection failure may occur when the **"waiting for response time" setting in the device software is too short.** Please modify the the setting for a longer period of time.

2. If errors occur while uploading/downloading data, it may be caused by an unstable network. Please check if the signal strength of 4G network is too weak (all indicater lights must be lit) or check if there is a significant delay in communication between the PC and the device. If the latency is too high, consider using Ethernet connection or try using another 4G network provider.



Virtual COM Port

Device Name DX2400_60AE - Online

IP Address 192.168.5.6 218 ms

RS-485

COM Port Auto □ PPI ☑ Auto Baudrate

COM Port	COM5 (Connected)	Baudrate	-	Stop Bits	-
Data Bits	-	Parity Bits	-	Status	Idle

RS-232

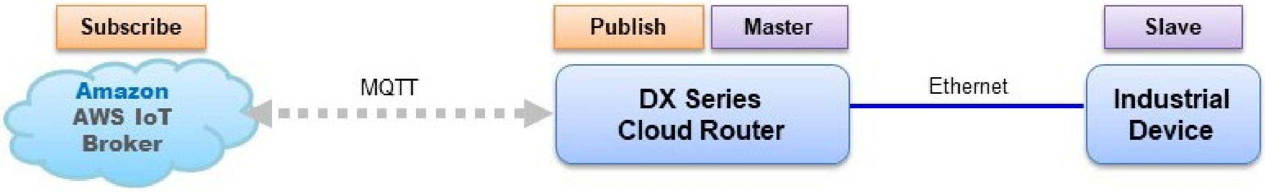
COM Port Auto ☑ Auto Baudrate

COM Port		Baudrate		Stop Bits	
Data Bits		Parity Bits		Status	

Secure tunnel is set up. 24 ms Local IP Address 192.168.5.8

2.3.9 Application for Publishing MQTT Data to AWS Broker

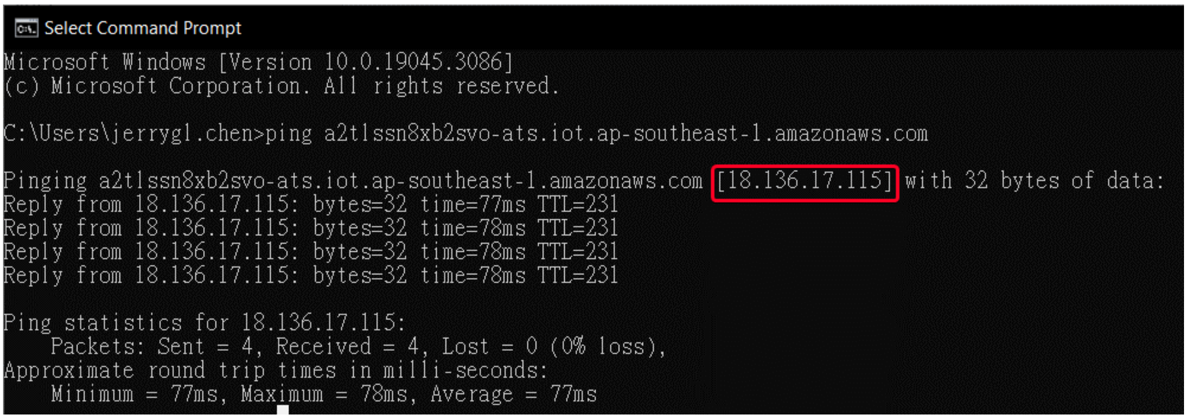
The DX-2400L9 cloud router can utilize the MQTT protocol to publish data from its registers to the topics configured on the AWS IoT platform.



Setup Steps

- **AWS IoT Core Setup**

1. Open the URL aws.amazon.com and click on **Sign In.**
2. Sign in to AWS. If you don't have an account, please apply for a free trial account first.
3. Click on **Services,** then click on **IoT Core.**
4. On the left-hand menu, click on **Connect one device**.
5. On the page, copy the following command to complete the following test, then click on "**Next**".
6. Execute this command in the CMD (Command Prompt) interface on Windows system. Please follow the steps below:First, copy and paste the command from the example to the CMD interface, and then press Enter. Next, copy the AWS IoT server IP address (18.136.17.115)



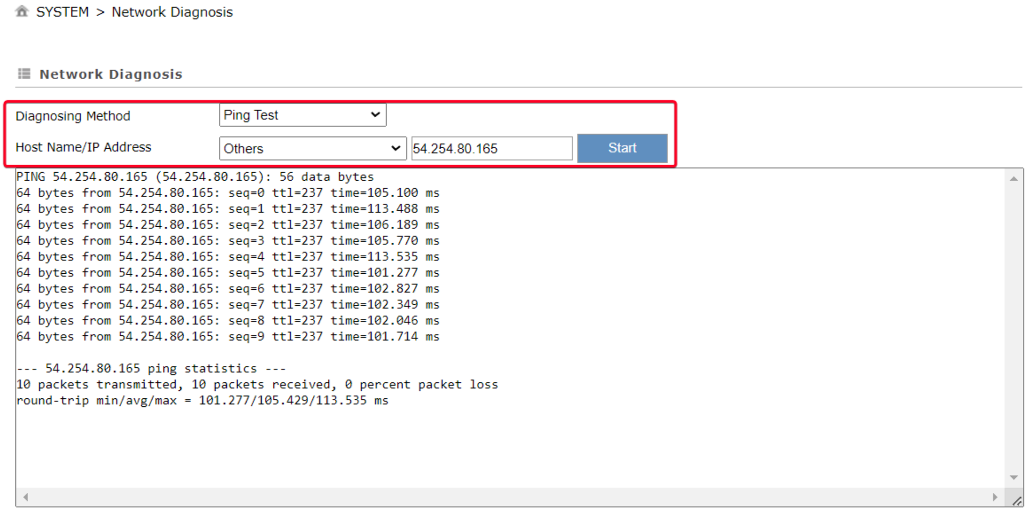
```
Microsoft Windows [Version 10.0.19045.3086]
(c) Microsoft Corporation. All rights reserved.

C:\Users\jerrygl.chen>ping a2tlssn8xb2svo-ats.iot.ap-southeast-1.amazonaws.com

Pinging a2tlssn8xb2svo-ats.iot.ap-southeast-1.amazonaws.com [18.136.17.115] with 32 bytes of data:
Reply from 18.136.17.115: bytes=32 time=77ms TTL=231
Reply from 18.136.17.115: bytes=32 time=78ms TTL=231
Reply from 18.136.17.115: bytes=32 time=78ms TTL=231
Reply from 18.136.17.115: bytes=32 time=78ms TTL=231

Ping statistics for 18.136.17.115:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 77ms, Maximum = 78ms, Average = 77ms
```

7. To confirm that the cloud router can correctly ping the AWS IoT server, please log in to the cloud router's web interface, then go to **SYSTEM→Network Diagnostics**.Please input **"Ping Test" for Diagnostic Method** and **"Others" for the Host Name/IP address.** Enter the IP address displayed in CMD, as shown in the image, and then click on "Start".If you are unable to ping the AWS IoT server, please refer to Step c. Internet Configuration, to ensure that the cloud router can connect to the public network.



Diagnosing Method: Ping Test

Host Name/IP Address: Others 54.254.80.165

```
PING 54.254.80.165 (54.254.80.165): 56 data bytes
64 bytes from 54.254.80.165: seq=0 ttl=237 time=105.100 ms
64 bytes from 54.254.80.165: seq=1 ttl=237 time=113.488 ms
64 bytes from 54.254.80.165: seq=2 ttl=237 time=106.189 ms
64 bytes from 54.254.80.165: seq=3 ttl=237 time=105.770 ms
64 bytes from 54.254.80.165: seq=4 ttl=237 time=113.535 ms
64 bytes from 54.254.80.165: seq=5 ttl=237 time=101.277 ms
64 bytes from 54.254.80.165: seq=6 ttl=237 time=102.827 ms
64 bytes from 54.254.80.165: seq=7 ttl=237 time=102.349 ms
64 bytes from 54.254.80.165: seq=8 ttl=237 time=102.046 ms
64 bytes from 54.254.80.165: seq=9 ttl=237 time=101.714 ms

--- 54.254.80.165 ping statistics ---
10 packets transmitted, 10 packets received, 0 percent packet loss
round-trip min/avg/max = 101.277/105.429/113.535 ms
```

8. In the Thing Properties page, choose **Create a new thing**. Enter the name in the "Thing name", for example, **"DX-2400L9_MQTT_Test,"** and finally, click on "**Next**."

9. On the Platform and SDK page, choose **Windows** and **Python**, then click on **Next**.

10. On the Connection kit page, click on **Download connection kit** to begin downloading the **"connect_device_package.zip"** file, Finally, click on "**Next**."

11. In the Connection Kit page, click on **"Continue.**

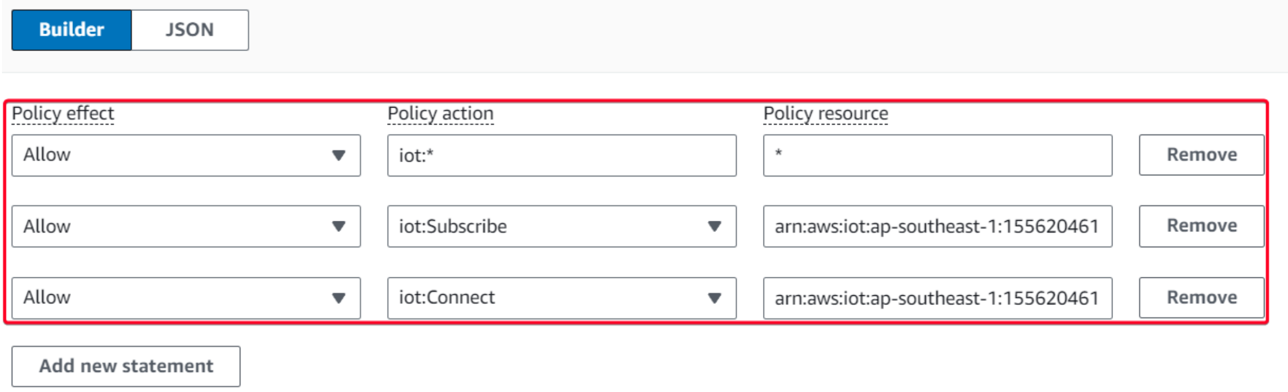
12. Click on **View thing**, the page will link to the newly created Thing and display detailed information.

- **Create Certificate**

1. Go to **Manage** → **Things** → **DX-2400L9_MQTT_Test** → **Certificates,** then click on **Create Certificate.**
2. Activate the device certificate, and download **the device certificate**, **public key file**, **private key file**, and **root CA certificate (Amazon Root CA1 and Amazon Root CA3)** to your computer for safekeeping. Finally, click on "Completed."
3. On the certificate page, you will see a message indicating that the certificate has been successfully created, and the newly created certificate needs to be set as **active. If there are multiple certificates, please make sure to take note of the certificate number.**

- **Create Policy**

1. Go to **Management** → **Security** → **Policies,** In the AWS IoT policies list, click on **"DX-2400L9_MQTT_Test-Policy"**
2. Click on **Edit active version.**
3. Go to **Policy statements** → **Policy document**, **and choose Builder**, modify the policy statement within the red box. Modify the policy statement as follows to allow external devices (non-AWS devices). Check the option **"Set the edited version as the active version for this policy"**. Finally, **"save as new version"**.

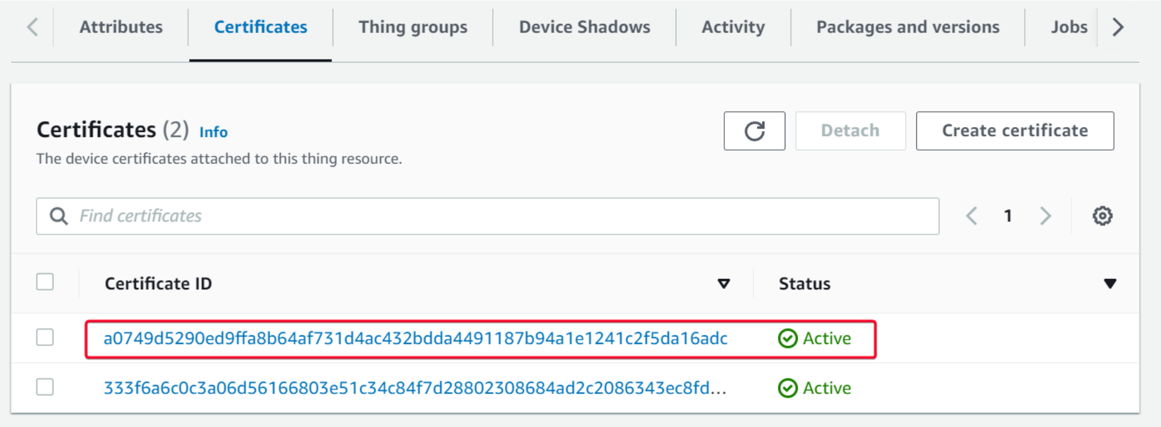


Policy effect	Policy action	Policy resource
Allow	iot:*	*
Allow	iot:Subscribe	arn:aws:iot:ap-southeast-1:155620461
Allow	iot:Connect	arn:aws:iot:ap-southeast-1:155620461

4. Modify the policy statement as follows to allow external devices (non-AWS devices). Check the option **"Set the edited version as the active version for this policy"**. Finally, **"save as new version"**.
5. The 2nd version of the policy will become the active state.

- **Associate Policies and Things with Certificates.**

1. Go to **Manage** → **Security** → **Certificates**, Click on the newly created certificate created in the certificates list.
2. Click on **Action** and select **Activate**, and activate this certificate.
3. On the certificate page, in the Policy field, click on **Attach Policies**, and add the **DX-2400L9_MQTT_Test-Policy**. If successful, it will appear in the list of policies.
4. On the certificate page, in the Things field, click on **Attach Policies**, and add the **DX-2400L9_MQTT_Test** certificate. If successful, it will appear in the list of things. Finally, click on **DX-2400L9_MQTT_Test**.
5. Click on **Certificates**, ensure that the status of 'a0749d5290ed9ffa8b64af731d4ac432bdda4491187b94a1e1241c2f5da16a...' is **Active**.



Certificates (2) Info

The device certificates attached to this thing resource.

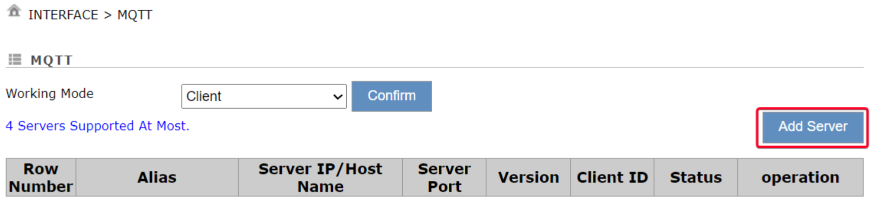
□	Certificate ID	Status
□	a0749d5290ed9ffa8b64af731d4ac432bdda4491187b94a1e1241c2f5da16adc	✓ Active
□	333f6a6c0c3a06d56166803e51c34c84f7d28802308684ad2c2086343ec8fd...	✓ Active

- **BrokerAddress**

1. Select **Settings** from the menu, and the Device data endpoint is the Broker address. **a2tlssn8xb2svo-ats.iot.ap-southeast-1.amazonaws.com**
2. In the menu, select **MQTT test client**, then click **Subscribe to a topic**, and subscribe to the topic '**DX2400/topic01**' in the **Topic filter**.

- **DX-2400L9 Publish Function Setting**

1. Log in to the DX-2400L9 cloud router, click on **INTERFACE** → **MQTT**, set **Client** as the working mode and add a server.



INTERFACE > MQTT

MQTT

Working Mode: Client

4 Servers Supported At Most.

Row Number	Alias	Server IP/Host Name	Server Port	Version	Client ID	Status	operation

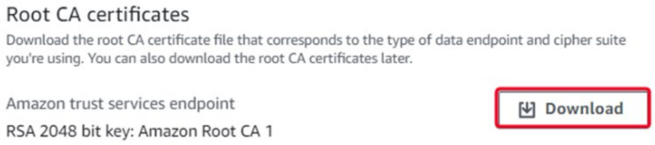
2. Please refer to the following description for MQTT client configuration, but pay attention to the related settings:

   a. Server IP/Host Name: AWS Broker server connection address.

   b. Server Port: AWS Broker server port, default is 8883.

   c. QoS: It is recommended to set it to 'At least Once.'

   d. CA Certificate: Import the RootCA for the AWS Broker server, found in the certificate downloaded in the second step of the Create Certificate process, look for 'Amazon Root CA1' and import it."



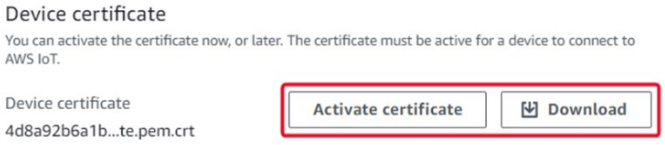
Root CA certificates

Download the root CA certificate file that corresponds to the type of data endpoint and cipher suite you're using. You can also download the root CA certificates later.

Amazon trust services endpoint

RSA 2048 bit key: Amazon Root CA 1

   e. Client Certificate: To import the client certificate, find the 'Device certificate' in the certificate downloaded in the second step of the Create Certificate process, and import it. If the file name is too long and cannot be imported, please shorten the file name.



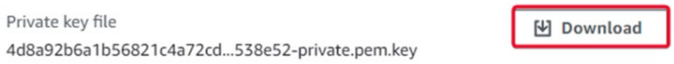
Device certificate

You can activate the certificate now, or later. The certificate must be active for a device to connect to AWS IoT.

Device certificate

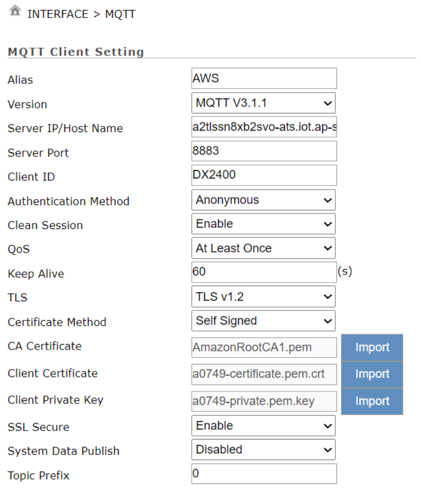
4d8a92b6a1b...te.pem.crt

   f. Client Private key: To import the client private key, find the 'Private Key file' in the certificate downloaded in the second step of the Create Certificate process, and import it. If the file name is too long and cannot be imported, please shorten the file name.



Private key file

4d8a92b6a1b56821c4a72cd...538e52-private.pem.key

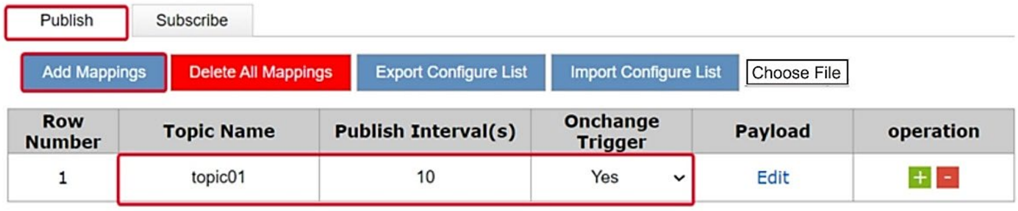


INTERFACE > MQTT

MQTT Client Setting

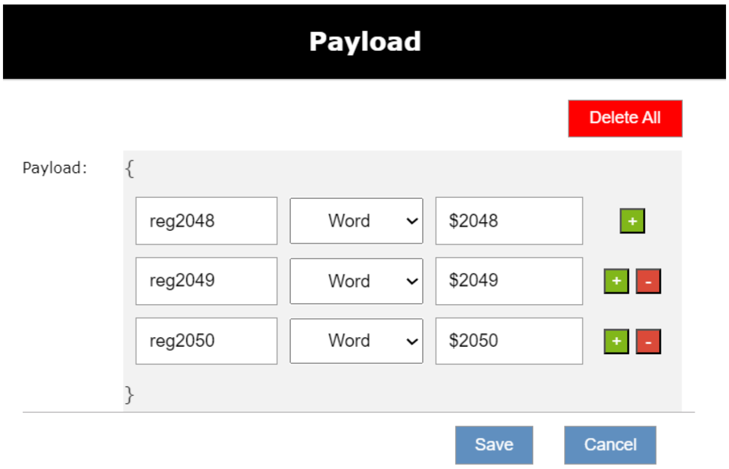
Alias	AWS
Version	MQTT V3.1.1
Server IP/Host Name	a2tlssn8xb2svo-ats.iot.ap-s
Server Port	8883
Client ID	DX2400
Authentication Method	Anonymous
Clean Session	Enable
QoS	At Least Once
Keep Alive	60 (s)
TLS	TLS v1.2
Certificate Method	Self Signed
CA Certificate	AmazonRootCA1.pem Import
Client Certificate	a0749-certificate.pem.crt Import
Client Private Key	a0749-private.pem.key Import
SSL Secure	Enable
System Data Publish	Disabled
Topic Prefix	0

3. Click on 'Publish,' then click on 'Add Mappings' to add a topic as follows:



Row Number	Topic Name	Publish Interval(s)	Onchange Trigger	Payload	operation
1	topic01	10	Yes	Edit	+ -

4. Click on 'Edit' and enter the following content into the Payload.

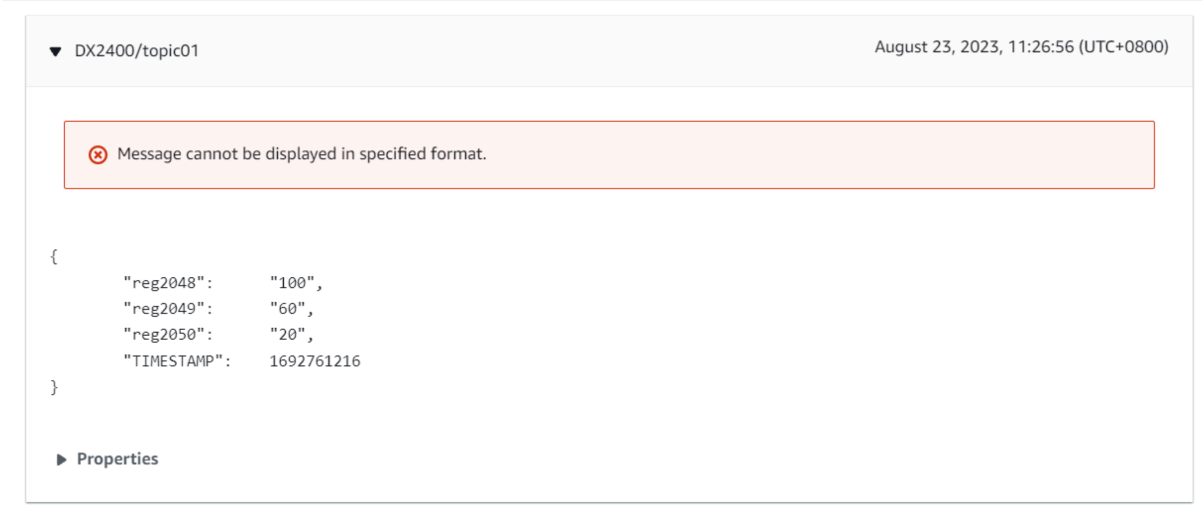


Payload: {

reg2048	Word	$2048	+
reg2049	Word	$2049	+ -
reg2050	Word	$2050	+ -

}

5. Modify the data in the internal registers $2048/$2049 of the DX cloud router. Return to the AWS Test Home, click on the 'MQTT test client' in the menu, and you will see that this data has been uploaded to the AWS MQTT Broker.



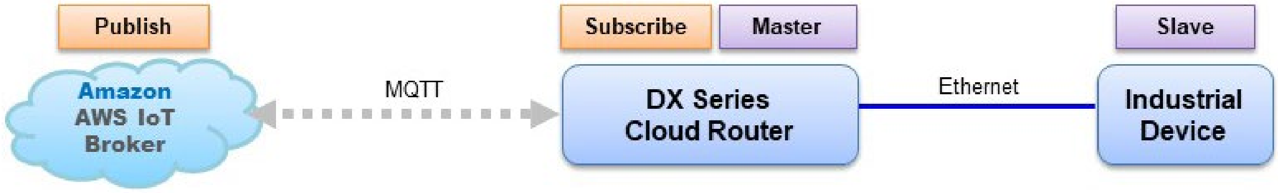
DX2400/topic01 August 23, 2023, 11:26:56 (UTC+0800)

Message cannot be displayed in specified format.

```
{
        "reg2048":      "100",
        "reg2049":      "60",
        "reg2050":      "20",
        "TIMESTAMP":    1692761216
}
```

2.3.10 Application for Subscribing to AWS Broker Topics with MQTT

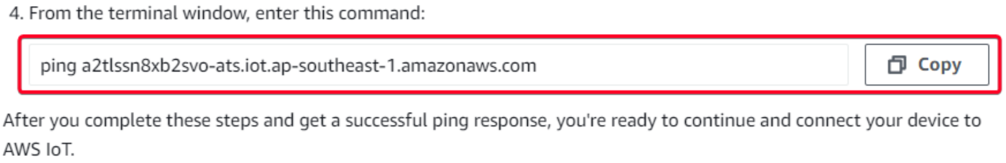
The DX-2400L9 cloud router can subscribe to topics in the AWS Broker using the MQTT protocol and store the data in registers.



Setup Steps

- **AWS IoT Core Setup**

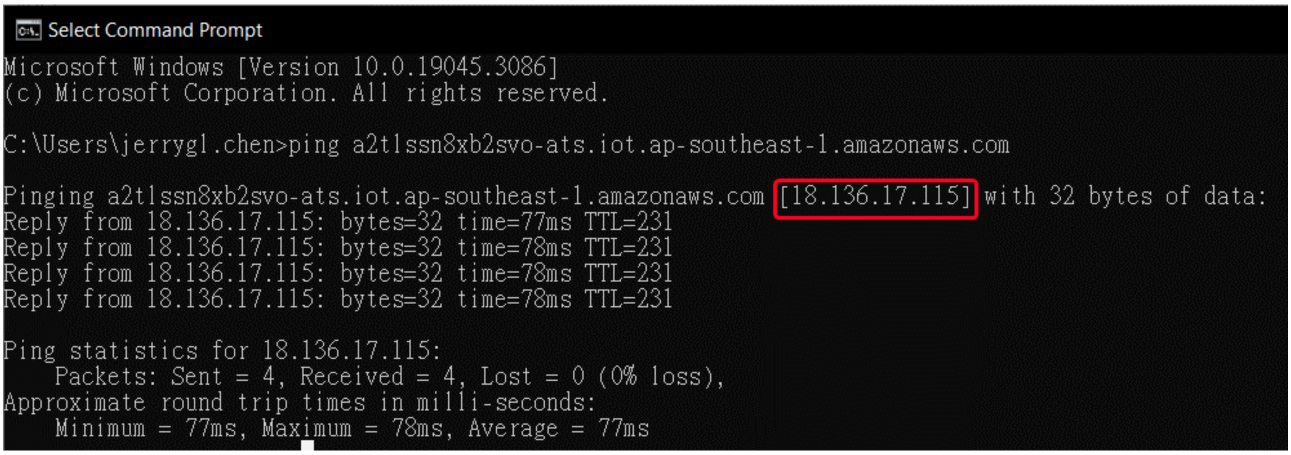
1. Open the URL aws.amazon.com and click on **Sign In.**
2. Sign in to AWS. If you don't have an account, please apply for a free trial account first.
3. Click on **Services,** then click on **IoT Core.**
4. On the left-hand menu, click on **Connect one device**.
5. On the page, copy the following command to complete the following test, then click on "**Next".**


4. From the terminal window, enter this command:

```
ping a2tlssn8xb2svo-ats.iot.ap-southeast-1.amazonaws.com
```

After you complete these steps and get a successful ping response, you're ready to continue and connect your device to AWS IoT.

6. Execute this command in the CMD (Command Prompt) interface on Windows system. Please follow the steps below:First, copy and paste the command from the example to the CMD interface, and then press Enter. Next, copy the AWS IoT server IP address (18.136.17.115)



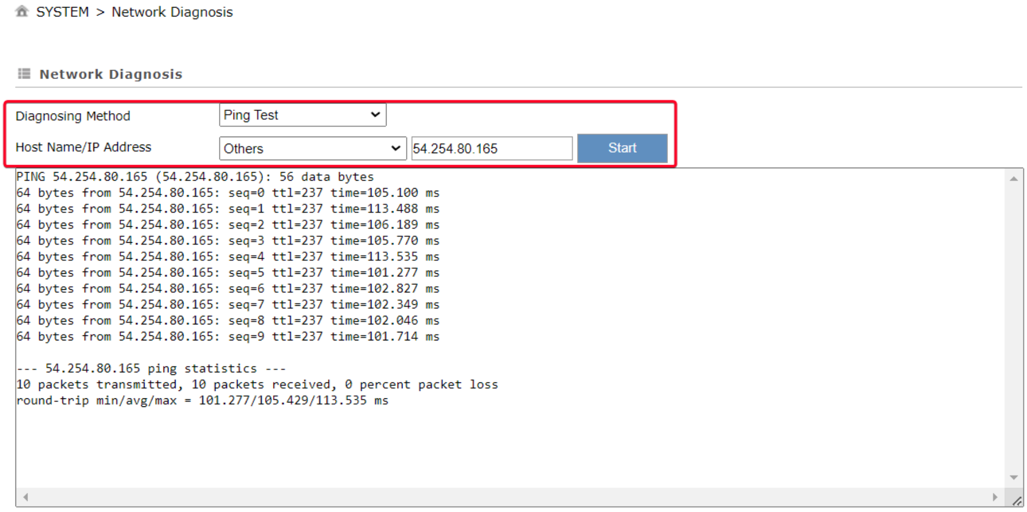
```
Microsoft Windows [Version 10.0.19045.3086]
(c) Microsoft Corporation. All rights reserved.

C:\Users\jerrygl.chen>ping a2tlssn8xb2svo-ats.iot.ap-southeast-1.amazonaws.com

Pinging a2tlssn8xb2svo-ats.iot.ap-southeast-1.amazonaws.com [18.136.17.115] with 32 bytes of data:
Reply from 18.136.17.115: bytes=32 time=77ms TTL=231
Reply from 18.136.17.115: bytes=32 time=78ms TTL=231
Reply from 18.136.17.115: bytes=32 time=78ms TTL=231
Reply from 18.136.17.115: bytes=32 time=78ms TTL=231

Ping statistics for 18.136.17.115:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 77ms, Maximum = 78ms, Average = 77ms
```

7. To confirm that the cloud router can correctly ping the AWS IoT server, please log in to the cloud router's web interface, then go to **SYSTEM→Network Diagnostics**.Please input **"Ping Test" for Diagnostic Method** and **"Others" for the Host Name/IP address.** Enter the IP address displayed in CMD, as shown in the image, and then click on "Start". If you are unable to ping the AWS IoT server, please refer to Chapter 2.2.5 Network Setting, to ensure that the cloud router can connect to the public network.



Diagnosing Method: Ping Test

Host Name/IP Address: Others 54.254.80.165

```
PING 54.254.80.165 (54.254.80.165): 56 data bytes
64 bytes from 54.254.80.165: seq=0 ttl=237 time=105.100 ms
64 bytes from 54.254.80.165: seq=1 ttl=237 time=113.488 ms
64 bytes from 54.254.80.165: seq=2 ttl=237 time=106.189 ms
64 bytes from 54.254.80.165: seq=3 ttl=237 time=105.770 ms
64 bytes from 54.254.80.165: seq=4 ttl=237 time=113.535 ms
64 bytes from 54.254.80.165: seq=5 ttl=237 time=101.277 ms
64 bytes from 54.254.80.165: seq=6 ttl=237 time=102.827 ms
64 bytes from 54.254.80.165: seq=7 ttl=237 time=102.349 ms
64 bytes from 54.254.80.165: seq=8 ttl=237 time=102.046 ms
64 bytes from 54.254.80.165: seq=9 ttl=237 time=101.714 ms

--- 54.254.80.165 ping statistics ---
10 packets transmitted, 10 packets received, 0 percent packet loss
round-trip min/avg/max = 101.277/105.429/113.535 ms
```

8. In the Thing Properties page, choose **Create a new thing**. Enter the name in the "Thing name", for example, **"DX-2400L9_MQTT_Test,"** and finally, click on "**Next**."

9. On the Platform and SDK page, choose **Windows** and **Python**, then click on **Next**.

10. On the Connection kit page, click on **Download connection kit** to begin downloading the **"connect_device_package.zip"** file, Finally, click on "**Next**."

11. In the Connection Kit page, click on **"Continue.**

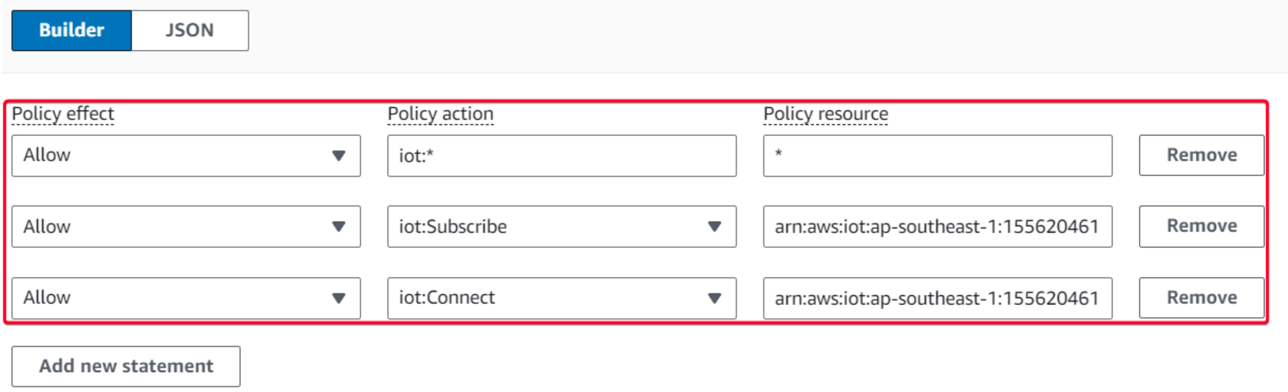
12. Click on **View thing**, the page will link to the newly created Thing and display detailed information.

- **Create Certificate**

1. Go to **Manage** → **Things** → **DX-2400L9_MQTT_Test** → **Certificates,** then click on **Create Certificate.**
2. Activate the device certificate, and download **the device certificate**, **public key file**, **private key file**, and **root CA certificate (Amazon Root CA1 and Amazon Root CA3)** to your computer for safekeeping. Finally, click on "Completed."
3. On the certificate page, you will see a message indicating that the certificate has been successfully created, and the newly created certificate needs to be set as **active. If there are multiple certificates, please make sure to take note of the certificate number.**

- **Create Policy**

1. Go to **Management** → **Security** → **Policies,** In the AWS IoT policies list, click on **"DX-2400L9_MQTT_Test-Policy"**
2. Click on **Edit active version.**
3. Go to **Policy statements** → **Policy document**, **and choose JSON**, modify the policy statement within the red box.
4. Modify the policy statement as follows to allow external devices (non-AWS devices). Check the option **"Set the edited version as the active version for this policy"**. Finally, **"save as new version"**.



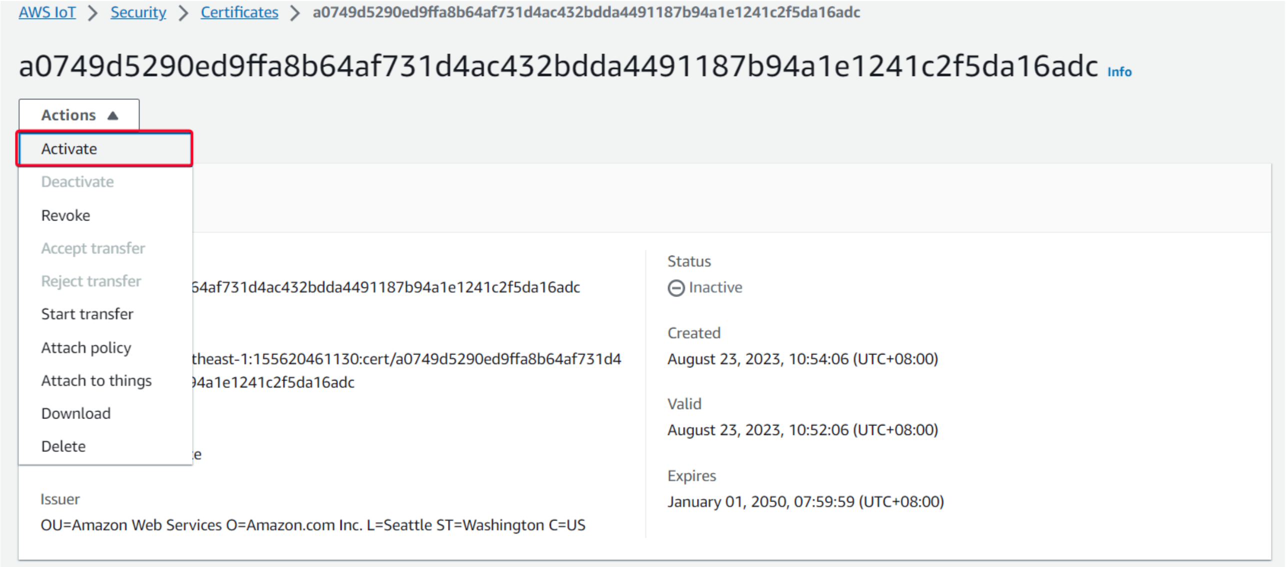
Policy effect	Policy action	Policy resource	
Allow	iot:*	*	Remove
Allow	iot:Subscribe	arn:aws:iot:ap-southeast-1:155620461	Remove
Allow	iot:Connect	arn:aws:iot:ap-southeast-1:155620461	Remove

5. The 2nd version of the policy will become the active state

- **Associate Policies and Things with Certificates.**

1. Go to **Manage** → **Security** → **Certificates**, Click on the newly created certificate created in the certificates list.

2. Click on 'Action,' select 'Activate,' and activate this certificate.


AWS IoT > Security > Certificates > a0749d5290ed9ffa8b64af731d4ac432bdda4491187b94a1e1241c2f5da16adc
a0749d5290ed9ffa8b64af731d4ac432bdda4491187b94a1e1241c2f5da16adc Info
Actions ▲
Activate
Deactivate
Revoke
Accept transfer
Reject transfer
Start transfer
Attach policy
Attach to things
Download
Delete

54af731d4ac432bdda4491187b94a1e1241c2f5da16adc

theast-1:155620461130:cert/a0749d5290ed9ffa8b64af731d4
94a1e1241c2f5da16adc

e

Issuer
OU=Amazon Web Services O=Amazon.com Inc. L=Seattle ST=Washington C=US

Status
⊖ Inactive

Created
August 23, 2023, 10:54:06 (UTC+08:00)

Valid
August 23, 2023, 10:52:06 (UTC+08:00)

Expires
January 01, 2050, 07:59:59 (UTC+08:00)

3. On the certificate page, in the Policy field, click on **Attach Policies**, and add the **DX-2400L9_MQTT_Test-Policy**. If successful, it will appear in the list of policies.

4. On the certificate page, in the Things field, click on **Attach Policies**, and add the **DX-2400L9_MQTT_Test** certificate. If successful, it will appear in the list of things. Then click **DX-2400L9_MQTT_Test.**

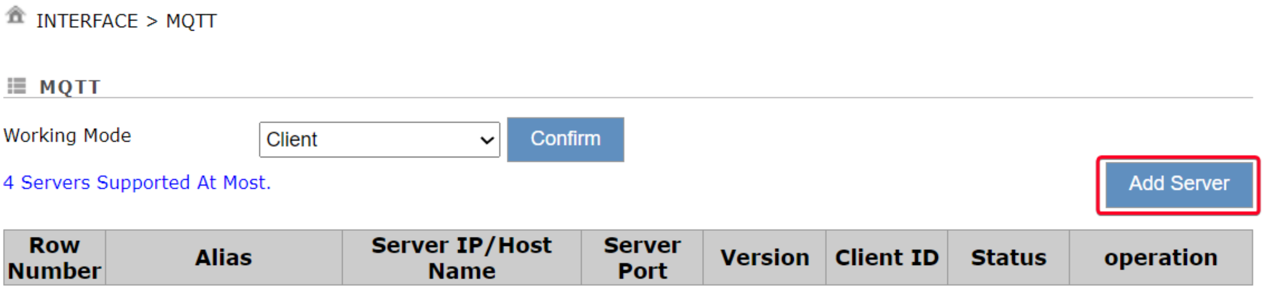
5. Click on 'Certificates,' and ensure that the status of 'a0749d5290ed9ffa8b64af731d4ac432bdda4491187b94a1e1241c2f5da16a...' is 'Active'.

- **BrokerAddress**

  Select **Settings** from the menu, and the Device data endpoint is the Broker address.

- **DX-2400L9 Subscribe Function Setting**

1. Log in to the DX-2400L9 cloud router, click on **INTERFACE** → **MQTT**, set **Client** as the working mode and add a server.



INTERFACE > MQTT

MQTT

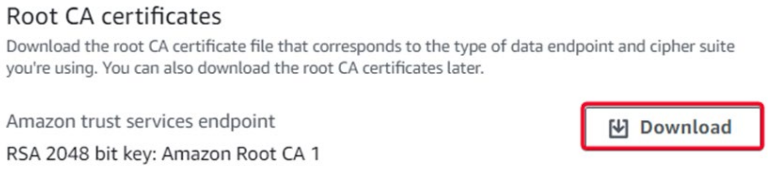
Working Mode: Client

4 Servers Supported At Most.

Row Number	Alias	Server IP/Host Name	Server Port	Version	Client ID	Status	operation

2. Please refer to the following for MQTT client configuration, but pay attention to the related settings:
   a. Server IP/Host Name: AWS Broker server connection address.
   b. Server Port: AWS Broker server port, default is 8883.
   c. QoS: It is recommended to set it to 'At least Once.'

d. CA Certificate: Import the RootCA for the AWS Broker server, found in the certificate downloaded in the second step of the Create Certificate process, look for 'Amazon Root CA1' and import it."



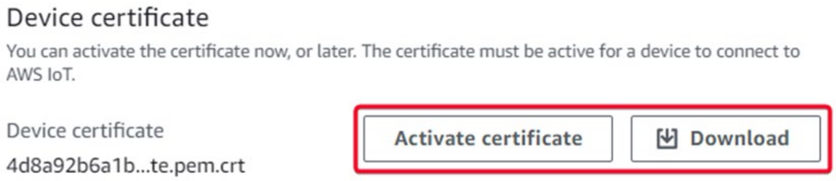
Root CA certificates

Download the root CA certificate file that corresponds to the type of data endpoint and cipher suite you're using. You can also download the root CA certificates later.

Amazon trust services endpoint

RSA 2048 bit key: Amazon Root CA 1

e. Client Certificate: To import the client device certificate, find the 'Device certificate' in the certificate downloaded in the second step of the Create Certificate process, and import it. If the file name is too long and cannot be imported, please shorten the file name.



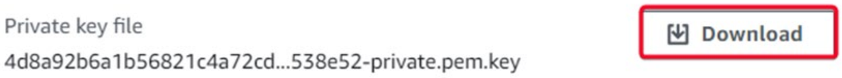
Device certificate

You can activate the certificate now, or later. The certificate must be active for a device to connect to AWS IoT.

Device certificate

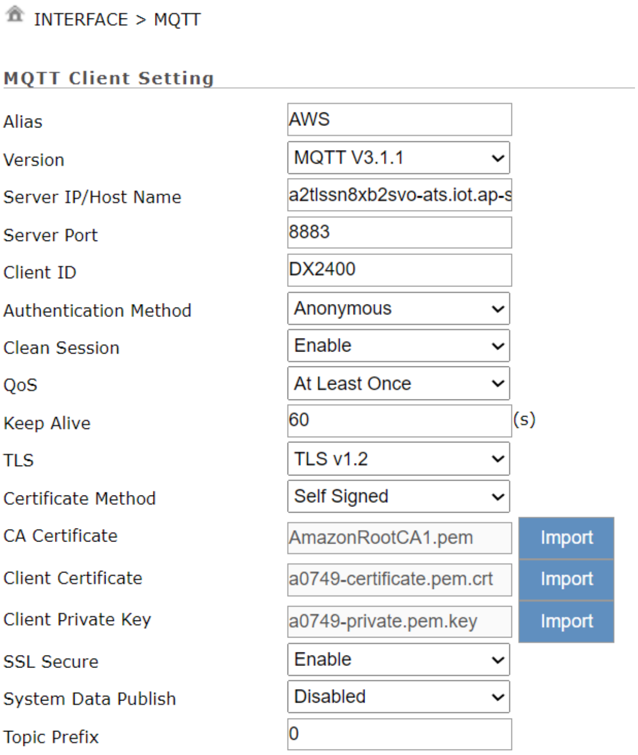
4d8a92b6a1b...te.pem.crt

f. Client Private key:To import the client private key, find the 'Private Key file' in the certificate downloaded in the second step of the Create Certificate process, and import it. If the file name is too long and cannot be imported, please shorten the file name.



Private key file

4d8a92b6a1b56821c4a72cd...538e52-private.pem.key

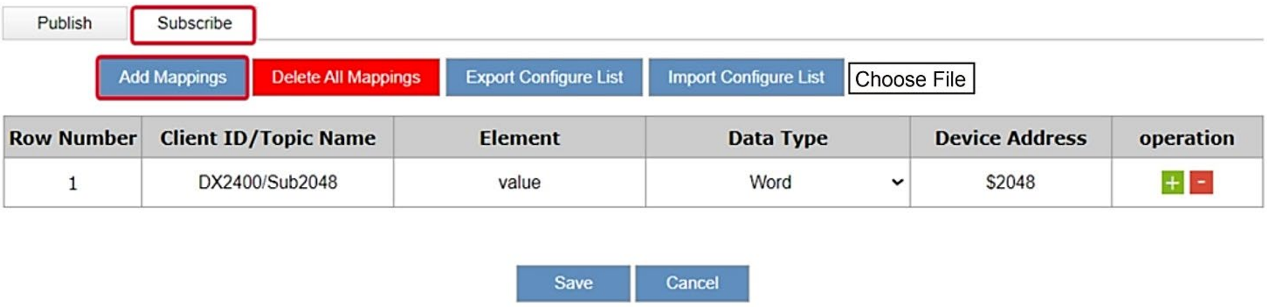


INTERFACE > MQTT

MQTT Client Setting

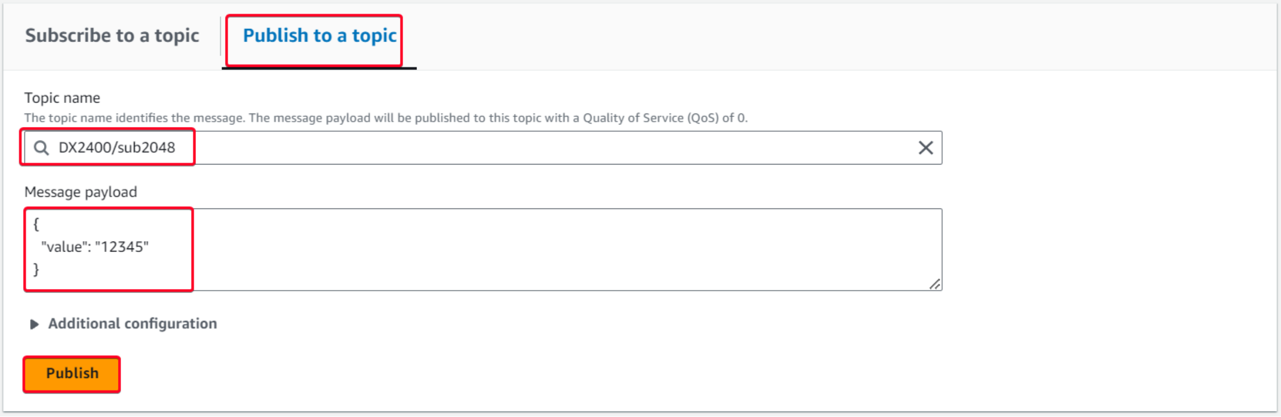
Alias	AWS
Version	MQTT V3.1.1
Server IP/Host Name	a2tlssn8xb2svo-ats.iot.ap-s
Server Port	8883
Client ID	DX2400
Authentication Method	Anonymous
Clean Session	Enable
QoS	At Least Once
Keep Alive	60 (s)
TLS	TLS v1.2
Certificate Method	Self Signed
CA Certificate	AmazonRootCA1.pem Import
Client Certificate	a0749-certificate.pem.crt Import
Client Private Key	a0749-private.pem.key Import
SSL Secure	Enable
System Data Publish	Disabled
Topic Prefix	0

3. Click on 'Subscribe,' then click on 'Add Mappings' to add a topic as follows, and then click 'Save'.



Row Number	Client ID/Topic Name	Element	Data Type	Device Address	operation
1	DX2400/Sub2048	value	Word	$2048	+ -

4. Go back to the AWS Test Home, click on the 'MQTT test client' menu, then select 'Publish to a topic.' Fill in the 'Topic name' and 'Message payload' as follows.



Topic name

The topic name identifies the message. The message payload will be published to this topic with a Quality of Service (QoS) of 0.

DX2400/sub2048

Message payload

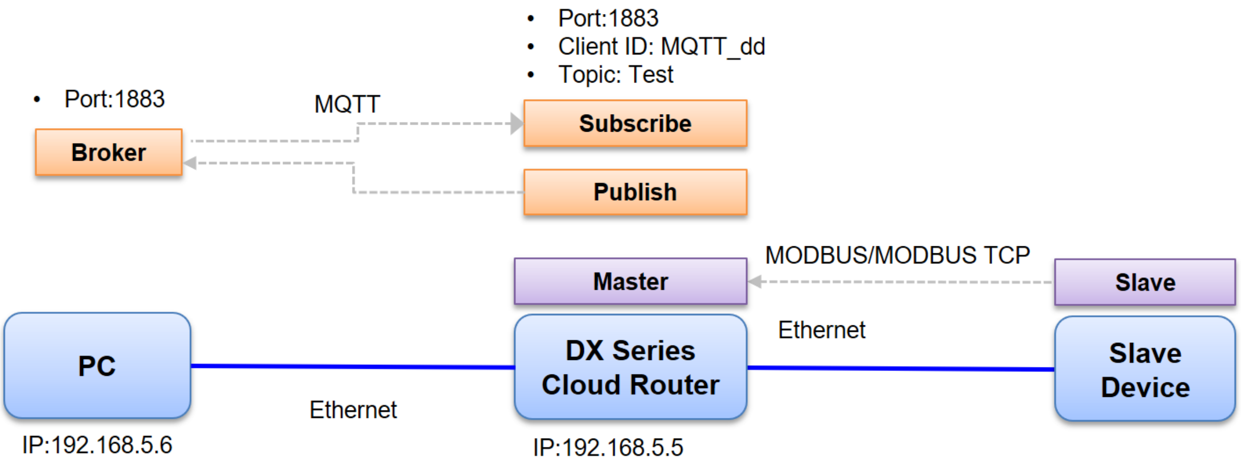
```
{
  "value": "12345"
}
```

5. Verify that the DX $2048 register has been updated to 12345.

2.3.11 Cloud Router MQTT Application for Connecting to a Local Broker Server

After successfully connecting the DX-2400L9 router to the local MQTT Broker server, the DX-2400L9 router can publish data from its registers to the MQTT Broker server platform's configured topics using the MQTT protocol. Simultaneously, the DX-2400L9 cloud router is capable of subscribing to specific topics on the MQTT Broker server platform, storing the data in the DX cloud router's registers, and then forwarding it to the slave devices.

Please refer to Chapter 3.4.5 MQTT for a detailed explanation of the configuration parameters.



- **BrokerSetup Steps**

1. Click on **Windows Defender Firewall** on the PC → **Input Rules** → **Add Rule** → **Protocol and Port**, and configure the following parameters.

   a. Protocol type(P): TCP

   b. Local port(U): Set the port number/1833.

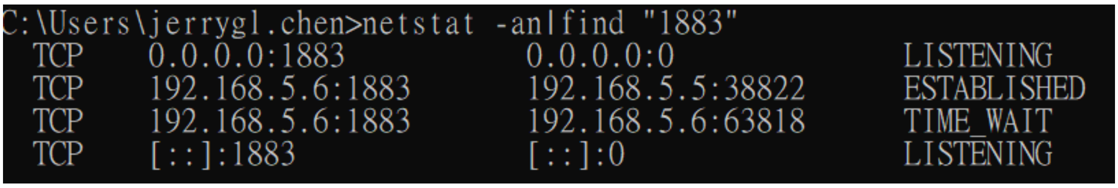
2. PC IP address configuration: 192.168.5.6

3. Install MQTT Broker server on the PC and configure the Broker with the following parameters.

   a. Listen Port: 1883 Port

   b. Allow anonymmous: Allow

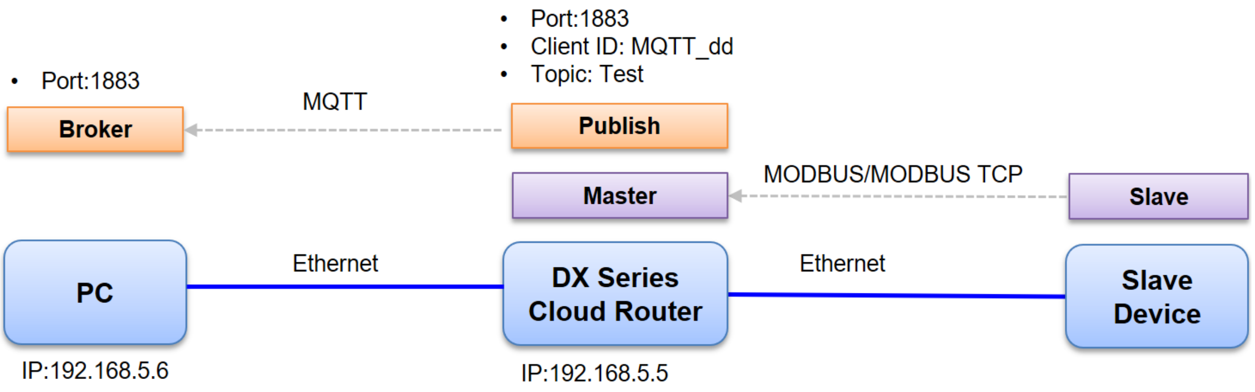
4. To confirm if the MQTT Broker server is already running on the PC, enter **netstat -an|find "1883"** in the CMD command prompt. If you see "**TCP 0.0.0.0:1883**" in the output, it means the MQTT Broker server is already started.



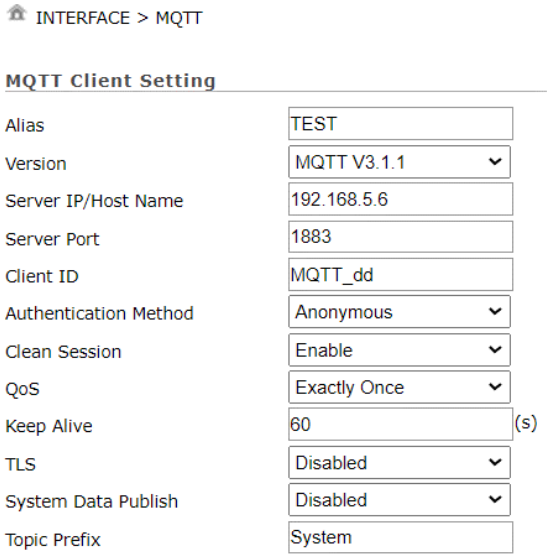
```
C:\Users\jerrygl.chen>netstat -an|find "1883"
  TCP    0.0.0.0:1883           0.0.0.0:0              LISTENING
  TCP    192.168.5.6:1883       192.168.5.5:38822      ESTABLISHED
  TCP    192.168.5.6:1883       192.168.5.6:63818      TIME_WAIT
  TCP    [::]:1883              [::]:0                 LISTENING
```

5. Use a network cable to connect LAN ports on your PC and the DX router.

- **PublishSetup Steps**



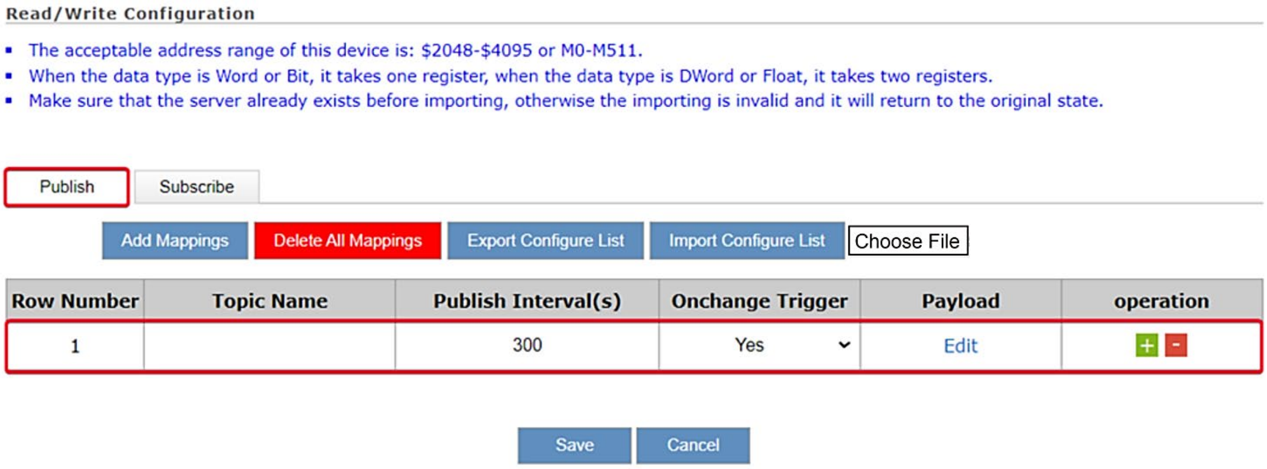
1. Login to the DX cloud router. (Default: admin/admin).
2. Set the IP address of the DX cloud router to 192.168.5.5.
3. Go to **INTERFACE** → **MQTT** and select **Client** as **working mode**, then click Confirm.
4. Click on **Add Server**, configure the client settings as follows.



MQTT Client Setting

Alias	TEST
Version	MQTT V3.1.1
Server IP/Host Name	192.168.5.6
Server Port	1883
Client ID	MQTT_dd
Authentication Method	Anonymous
Clean Session	Enable
QoS	Exactly Once
Keep Alive	60 (s)
TLS	Disabled
System Data Publish	Disabled
Topic Prefix	System

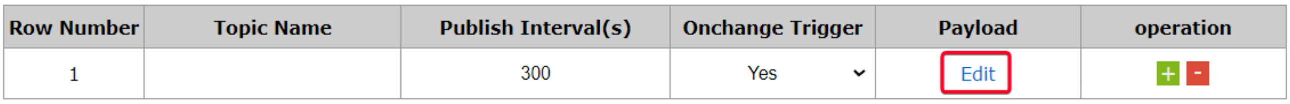
5. In the Read/Write Configuration section, click on **Publish**, and then click **Add Mappings**.


Read/Write Configuration

- The acceptable address range of this device is: $2048-$4095 or M0-M511.
- When the data type is Word or Bit, it takes one register, when the data type is DWord or Float, it takes two registers.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Topic Name	Publish Interval(s)	Onchange Trigger	Payload	operation
1		300	Yes	Edit	+ -

6. Click on “Edit” and fill in the content of the Payload packet.



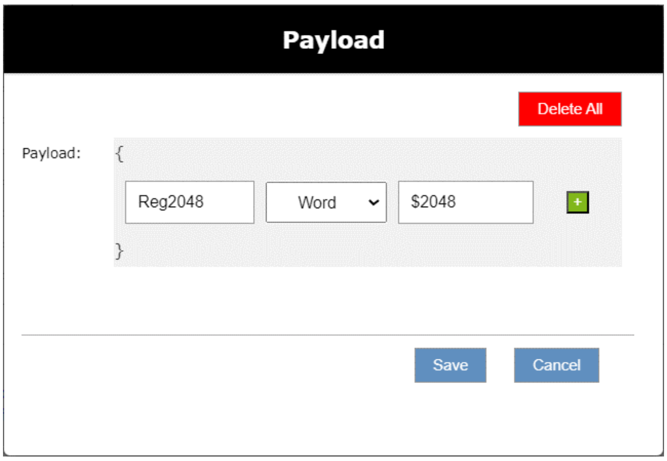
Row Number	Topic Name	Publish Interval(s)	Onchange Trigger	Payload	operation
1		300	Yes	Edit	+ -

7. The explanation of the Payload content is as follows. After entering the information, click on “Save”.

   a. First field: Reg2048, Data Name, with a maximum length of 64 bits as a string.

   b. Second field: Word, Data Type, for example, string or integer, etc.

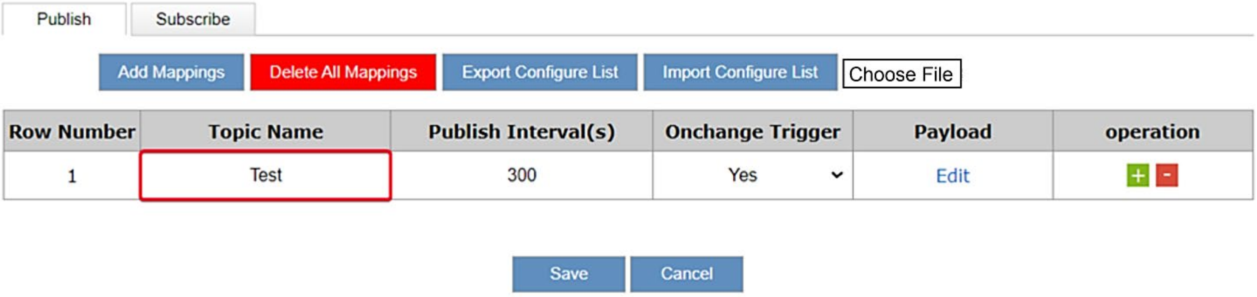
   c. Third field: $2048, indicates the data source from which DX register.



Payload

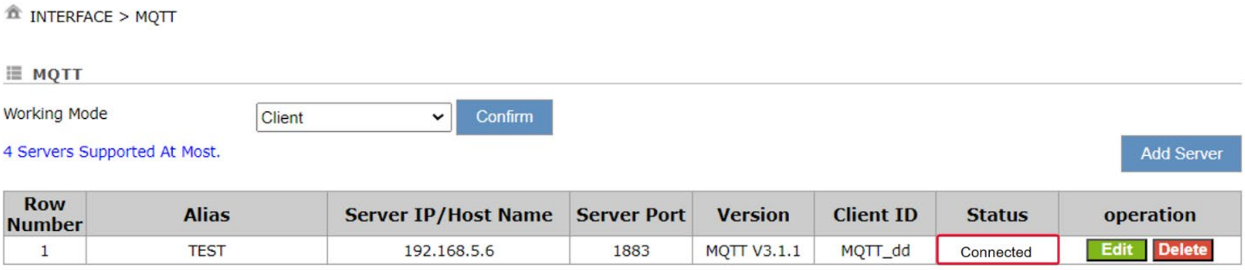
Payload: {
Reg2048 Word $2048
}

8. Finally, fill in the topic name as "Test" and click on "Save."



Row Number	Topic Name	Publish Interval(s)	Onchange Trigger	Payload	operation
1	Test	300	Yes	Edit	+ -

9. After returning to the settings homepage, check the Status, and it will show as "Connected." At this point, the DX cloud router has started publishing the data from the $2048 register to the Broker.



INTERFACE > MQTT

MQTT

Working Mode: Client

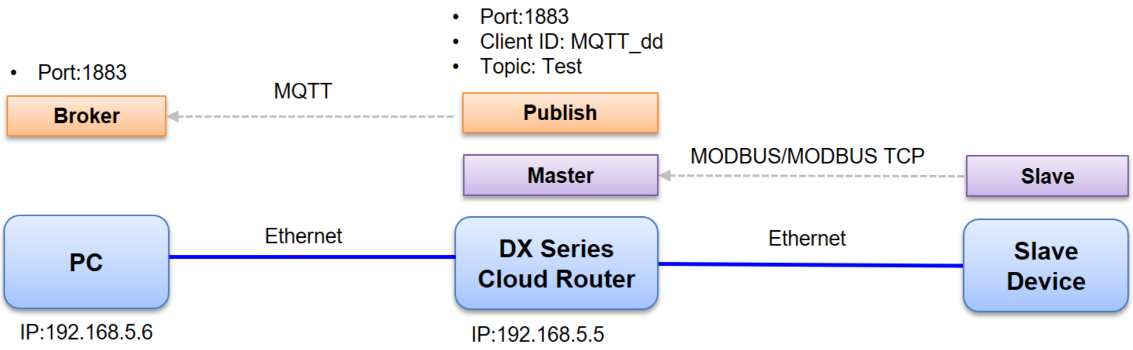
4 Servers Supported At Most.

Row Number	Alias	Server IP/Host Name	Server Port	Version	Client ID	Status	operation
1	TEST	192.168.5.6	1883	MQTT V3.1.1	MQTT_dd	Connected	Edit Delete

10. To view the messages published by the DX cloud router, you need to install an MQTT Subscribe software and enter the following information: **Broker IP address: 192.168.5.6**, **Client ID from Publish field,** and **Topic Name: MQTT_dd/Test.** The displayed JSON content is as follows.

```
{
        “Reg2048”:      “0”,
        “TIMESTAMP”:        16781093236
}
```

- **SubscribeSetup Steps**

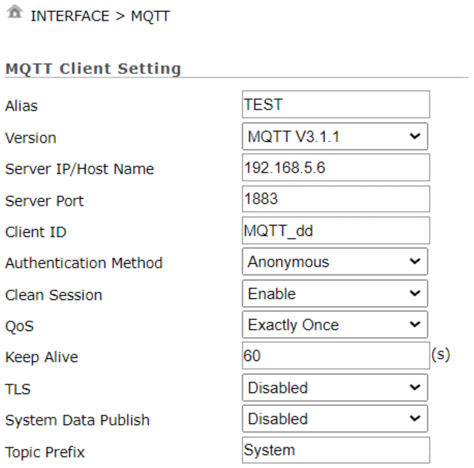


1. Login to the DX cloud router. (Default: admin/admin).

2. Set the IP address of the DX cloud router to 192.168.5.5.

3. Go to **INTERFACE** → **MQTT** and select **Client** as **working mode**, then click “Confirm”.

4. Click on **Add Server**, configure the client settings as follows.



MQTT Client Setting

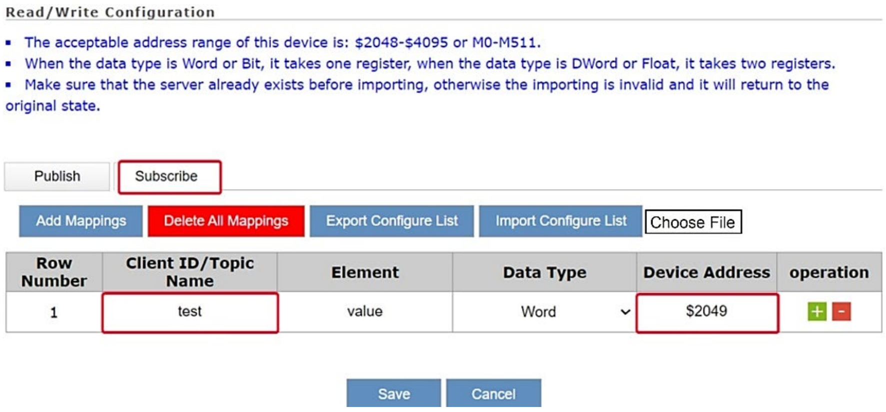
Alias	TEST
Version	MQTT V3.1.1
Server IP/Host Name	192.168.5.6
Server Port	1883
Client ID	MQTT_dd
Authentication Method	Anonymous
Clean Session	Enable
QoS	Exactly Once
Keep Alive	60 (s)
TLS	Disabled
System Data Publish	Disabled
Topic Prefix	System

5. In the Read/Write Configuration section, click on **Subscribe**, and then click on **Add Mappings.** Then click on “Save”.

   a. Topic Name: Test. You can only subscribe to the topic of the client ID: MQTT_dd, which is a string with a maximum length of 64 bits.

   b. Data Type: Word

   c. Device Address: $2049, storing DX register addresses.


Read/Write Configuration

- The acceptable address range of this device is: $2048-$4095 or M0-M511.
- When the data type is Word or Bit, it takes one register, when the data type is DWord or Float, it takes two registers.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

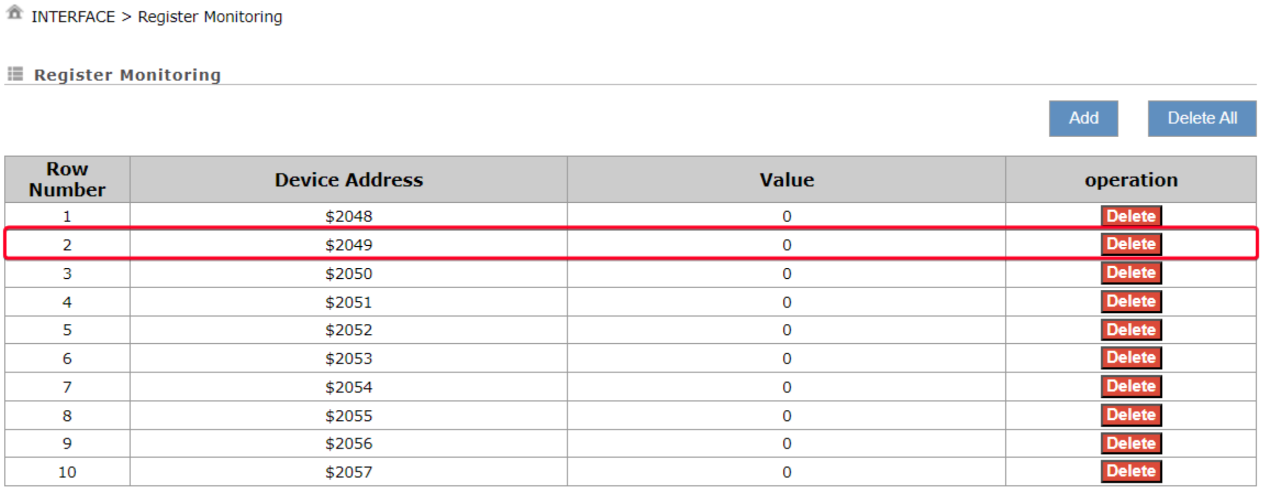
Row Number	Client ID/Topic Name	Element	Data Type	Device Address	operation
1	test	value	Word	$2049	+ -

6. At this moment, publish a data record to the topic "Test" under the client ID "MQTT_dd". The Payload content for publishing should follow the following JSON format:

```
{
        “value”:     “66”,
}
```

7. After the data is received, it will be stored in the DX cloud router's register $2049.

8. Click on the DX cloud router menu **SYSTEM INTERFACE → Register Monitoring** , "Add New Monitor" to create a new register monitoring to check whether the value of register $2049 has changed to 66. If not, it's possible that the Payload format is incorrect or the data has not been successfully published to the Broker.

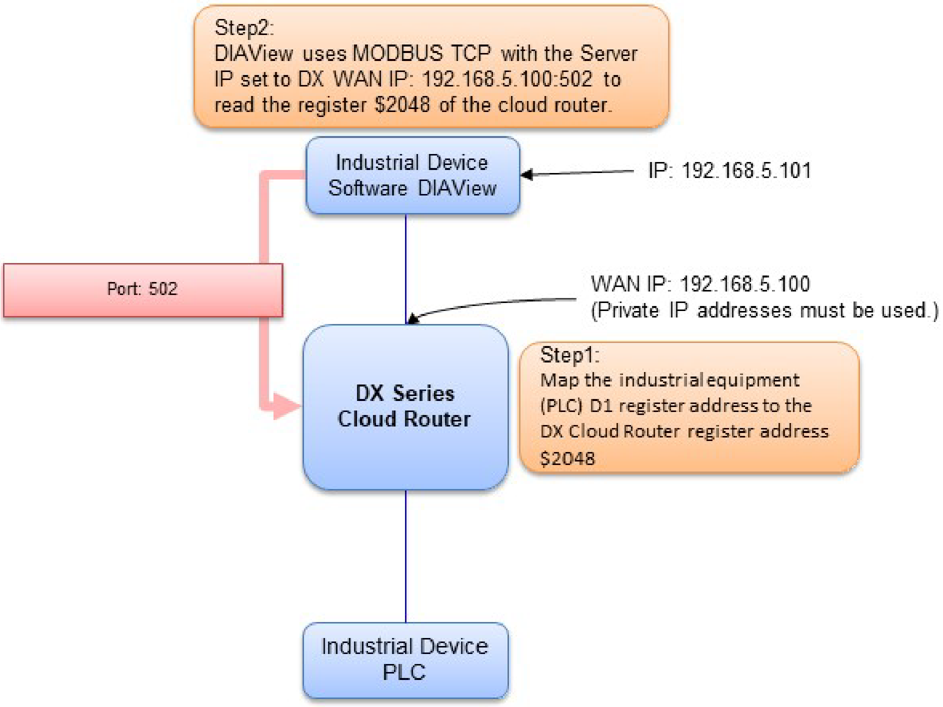


Row Number	Device Address	Value	operation
1	$2048	0	Delete
2	$2049	0	Delete
3	$2050	0	Delete
4	$2051	0	Delete
5	$2052	0	Delete
6	$2053	0	Delete
7	$2054	0	Delete
8	$2055	0	Delete
9	$2056	0	Delete
10	$2057	0	Delete

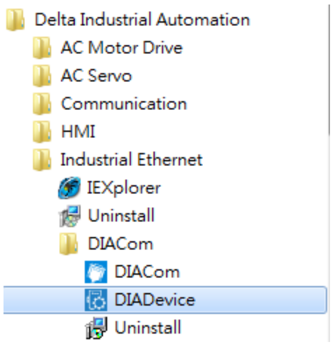
2.3.12 WAN Port Access (Port 502) for Private Network Applications.

Obtain a Private IP address from WAN port of the cloud router, so external devices can access register data of cloud router through port 502 over MODBUS TCP protocol. (This application will open port 502 on the Internet. Please do not use this feature if there's any security concerns.)

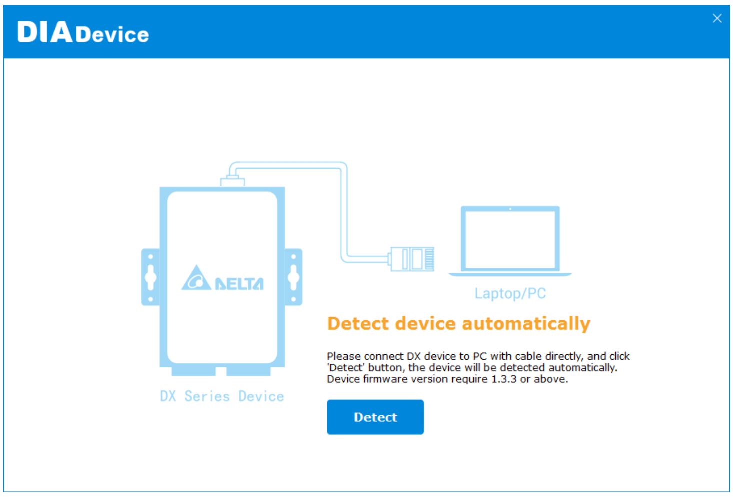
Please refer to Chapter 3.3.1 Firewall Settings for a detailed explanation of the configuration parameters.


Step2:
DIAView uses MODBUS TCP with the Server IP set to DX WAN IP: 192.168.5.100:502 to read the register $2048 of the cloud router.
Industrial Device Software DIAView
IP: 192.168.5.101
Port: 502
WAN IP: 192.168.5.100
(Private IP addresses must be used.)
DX Series Cloud Router
Step1:
Map the industrial equipment (PLC) D1 register address to the DX Cloud Router register address $2048
Industrial Device PLC

1. This application can be used on the local network. The cloud router does not need to be bound to DIACloud.
2. Use a network cable to connect LAN ports on your PC and the DX router.
3. Install DIACom software.
4. Open DIADevice: Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice**.



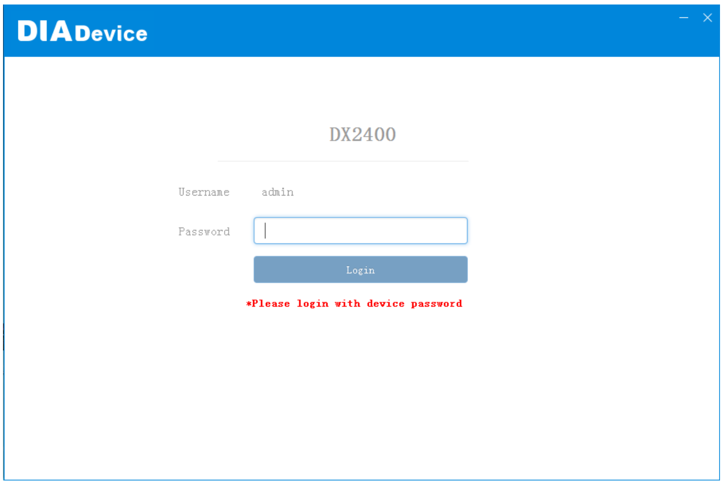
5. Click on “Detect”, and it will redirect to the login page of DX router.



Detect device automatically

Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

6. It will automatically redirect to the login page upon detecting the device. Enter the account and password on the login page.(Default: admin/admin)

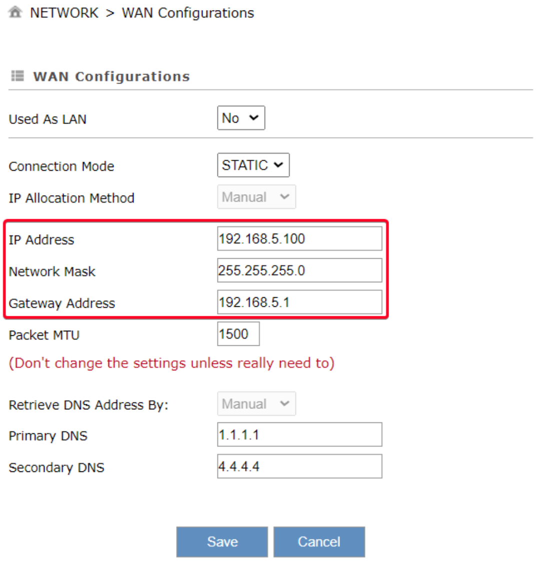


Username admin

Password

*Please login with device password

7. Since this application uses a Private IP, the cloud router's WAN port obtains a DHCP IP address from the upstream router.Or go to **NETWORK** → **WAN Configurations**, manually configure the IP address to 192.168.5.100.



NETWORK > WAN Configurations

WAN Configurations

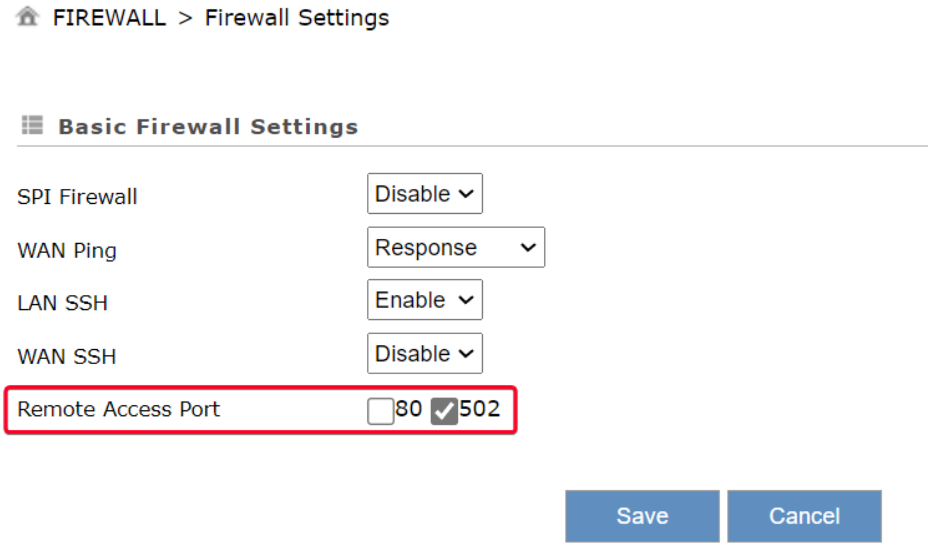
Used As LAN	No
Connection Mode	STATIC
IP Allocation Method	Manual
IP Address	192.168.5.100
Network Mask	255.255.255.0
Gateway Address	192.168.5.1
Packet MTU	1500

(Don't change the settings unless really need to)

Retrieve DNS Address By:	Manual
Primary DNS	1.1.1.1
Secondary DNS	4.4.4.4

8. After entering DX router login page, input your account and password. (Default: admin/admin) and click on “login”.

9. Go to **FIREWALL** → **FIREWALL Settings** and check the checkbox of **Remote Access Port: 502,** then click on “Save”.

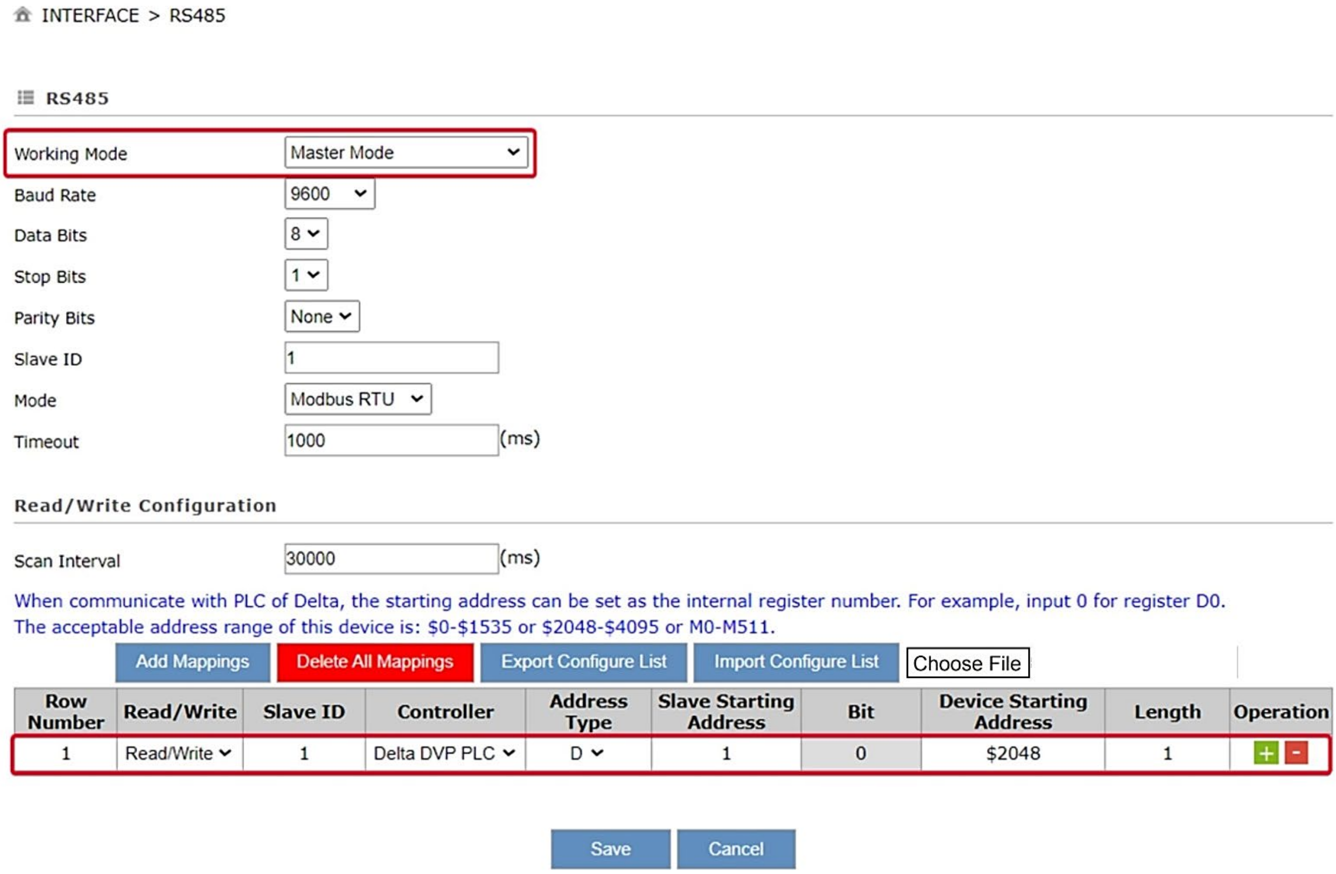


FIREWALL > Firewall Settings

Basic Firewall Settings

SPI Firewall	Disable
WAN Ping	Response
LAN SSH	Enable
WAN SSH	Disable
Remote Access Port	□80 ☑502

10. Go to **INTERFACE** → **RS485**, select **Master Mode** as **Working Mode**, select Delta AS PLC as the controller (This example uses Delta PLC) with the address of mapped register set to D1→$2048, then click on "Save”.



INTERFACE > RS485

RS485

Working Mode	Master Mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Slave ID	1
Mode	Modbus RTU
Timeout	1000 (ms)

Read/Write Configuration

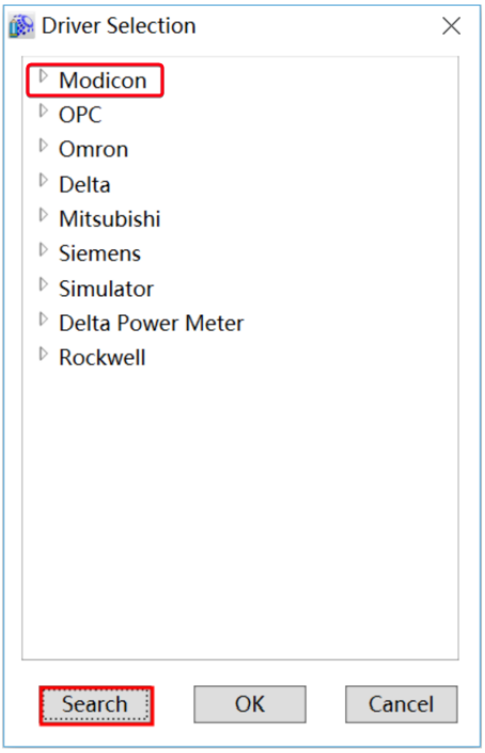
Scan Interval 30000 (ms)

When communicate with PLC of Delta, the starting address can be set as the internal register number. For example, input 0 for register D0.
The acceptable address range of this device is: $0-$1535 or $2048-$4095 or M0-M511.

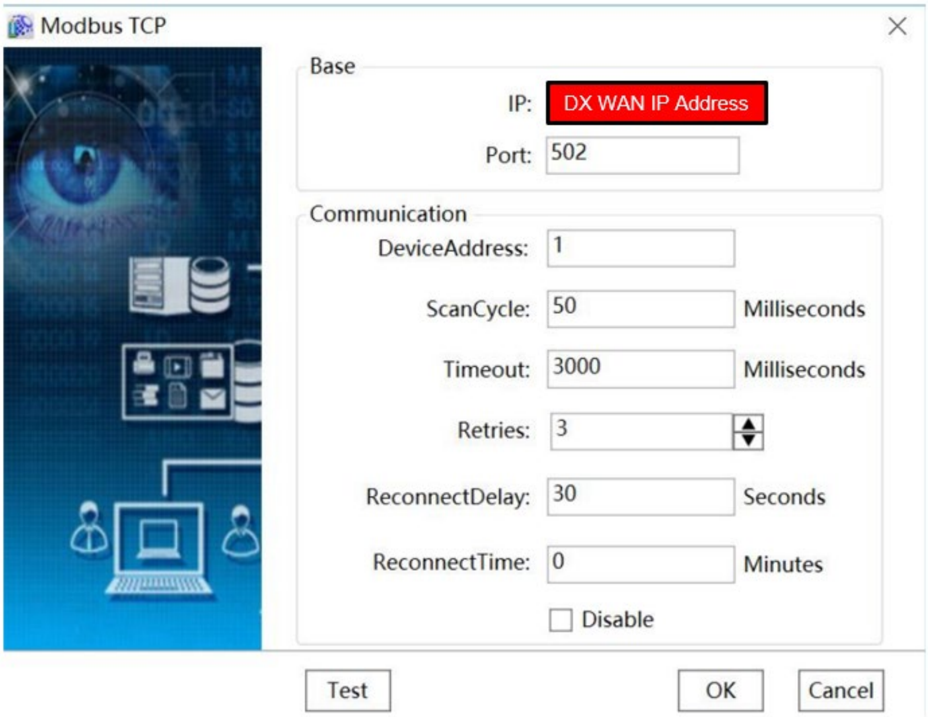
Row Number	Read/Write	Slave ID	Controller	Address Type	Slave Starting Address	Bit	Device Starting Address	Length	Operation
1	Read/Write	1	Delta DVP PLC	D	1	0	$2048	1	+ -

11. Connect the PC, which has been installed DIAView, to the WAN port of the cloud router using Ethernet cable.

12. Open DIAView and go to **I/O** → **Driver** → **Modicon** → **MODBUS TCP.**



13. Enter the IP address of the cloud router's WAN port: **192.168.5.100:502**, then click on “Test” to check if communication is successful.


Modbus TCP

Base

IP: DX WAN IP Address

Port: 502

Communication

DeviceAddress: 1

ScanCycle: 50 Milliseconds

Timeout: 3000 Milliseconds

Retries: 3

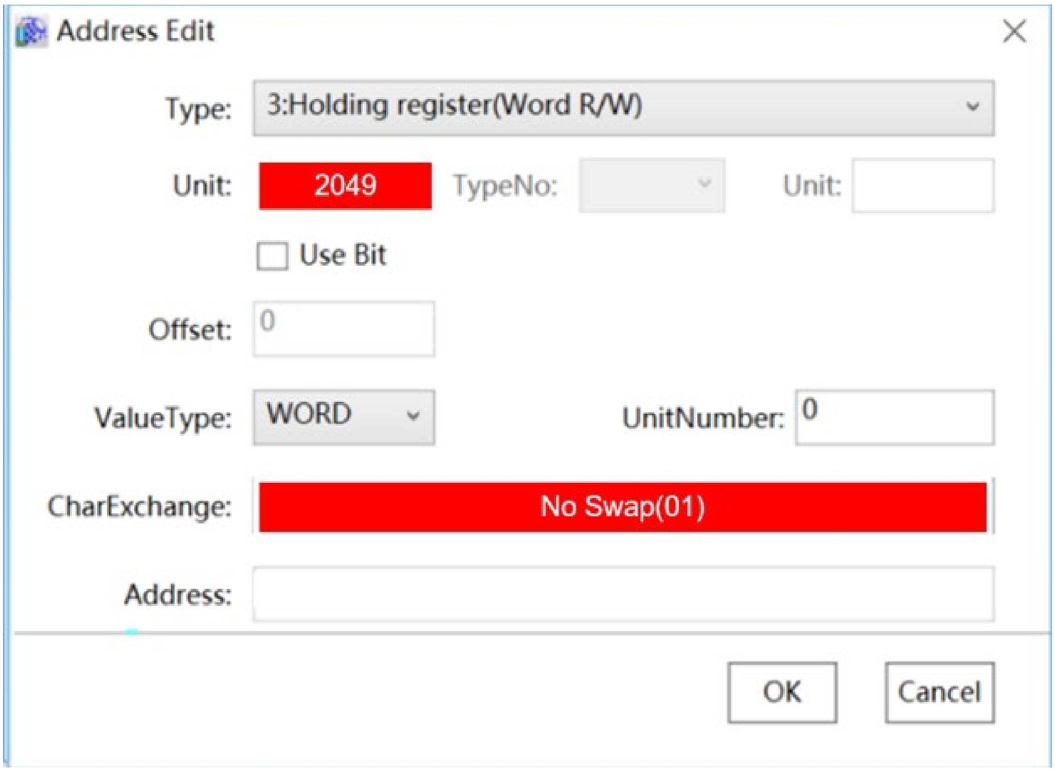
ReconnectDelay: 30 Seconds

ReconnectTime: 0 Minutes

□ Disable

14. Select Driver and click ⊕Add , then double click on ... .

15. Select: **Type: 3:Holding register(Word R/W), Unit: 2049**, to read the data in the cloud router's register $2048."



Address Edit

Type: 3:Holding register(Word R/W)

Unit: 2049 TypeNo: Unit:

□ Use Bit

Offset: 0

ValueType: WORD UnitNumber: 0

CharExchange: No Swap(01)

Address:

Notice

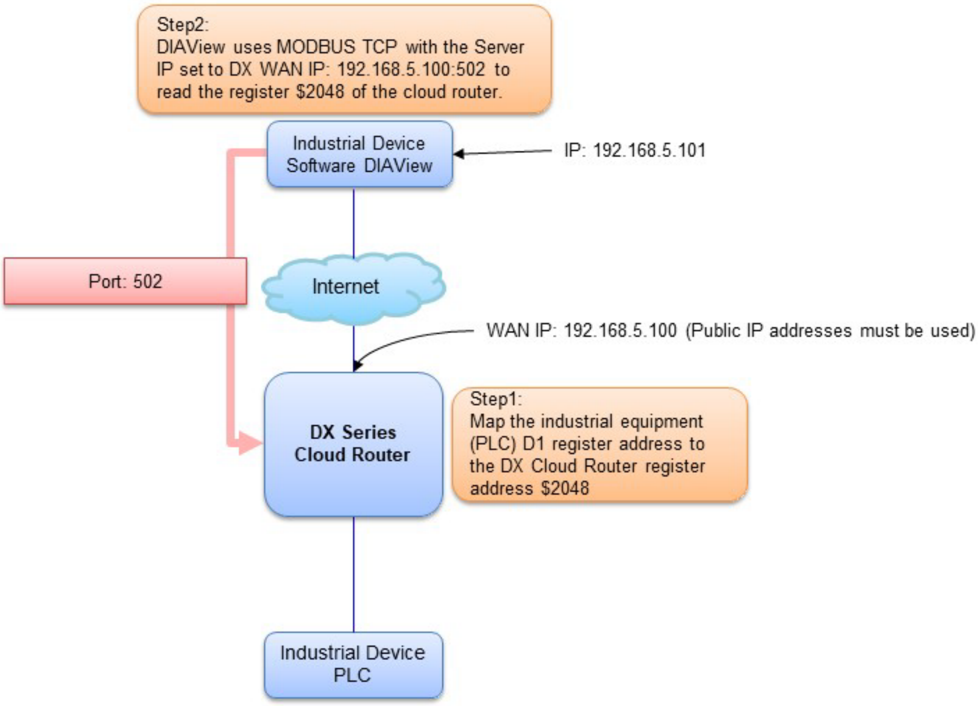
- The cloud router only supports Function code 3/16.
- To read the data in the cloud router's internal register $2048 in DIAView, you need to add 1 to the number, i.e., use 2049 to access that location.

2.3.13 WAN Port Access (Port 502) for Public Network Applications

With the WAN public IP address, DIAView can communicate with cloud routers from the Internet, and read/write DX register data through port 502 and MODBUSTCP protocol.

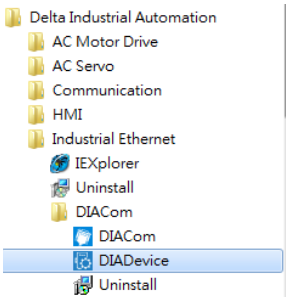
Notice:

1. This application will open port 502 on the Internet. Please do not use this feature if there's any security concerns.
2. If the cloud router's WAN cannot obtain a public IP address, this application cannot be used. Please contact the company's IT department or network service provider to inquire about obtaining a public IP address.
3. Please refer to Chapter 3.3.1 Firewall Settings for a detailed explanation of the configuration parameters.

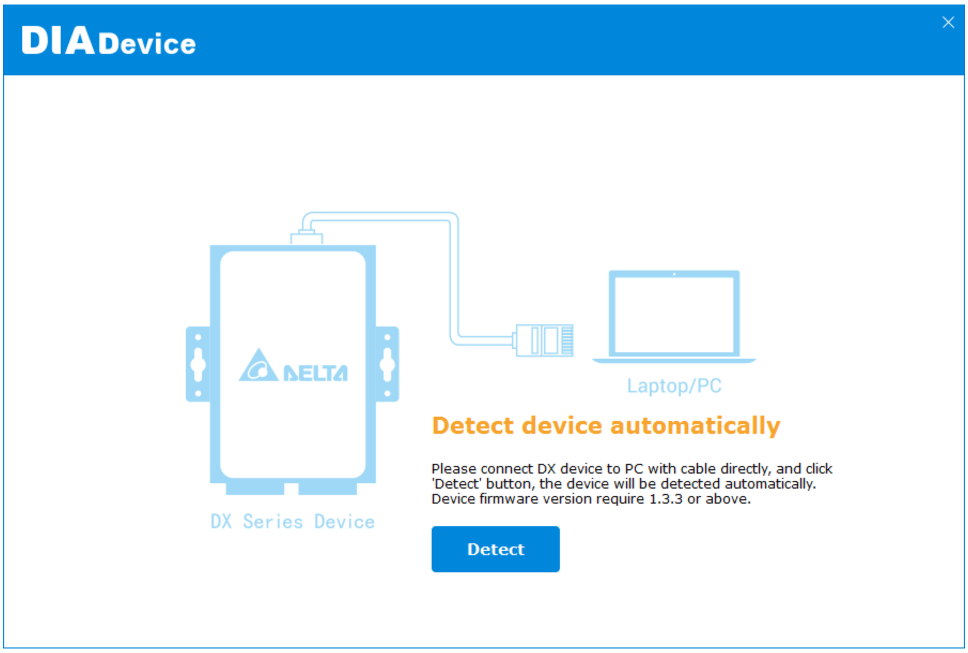

Step2:
DIAView uses MODBUS TCP with the Server IP set to DX WAN IP: 192.168.5.100:502 to read the register $2048 of the cloud router.
Industrial Device Software DIAView
IP: 192.168.5.101
Port: 502
Internet
WAN IP: 192.168.5.100 (Public IP addresses must be used)
DX Series Cloud Router
Step1:
Map the industrial equipment (PLC) D1 register address to the DX Cloud Router register address $2048
Industrial Device PLC

Setup Steps

1. This application can be used on the local network. The cloud router does not need to be bound to DIACloud.
2. Make sure that all the basic configuration detailed in Chapter 2.2 has been completed and functions properly. Please verify with your IT department or network service provider if the IP address is indeed a Public one.
3. Use a network cable to connect LAN ports on your PC and the DX router.
4. Install DIACom software.
5. Open DIADevice: Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice.**



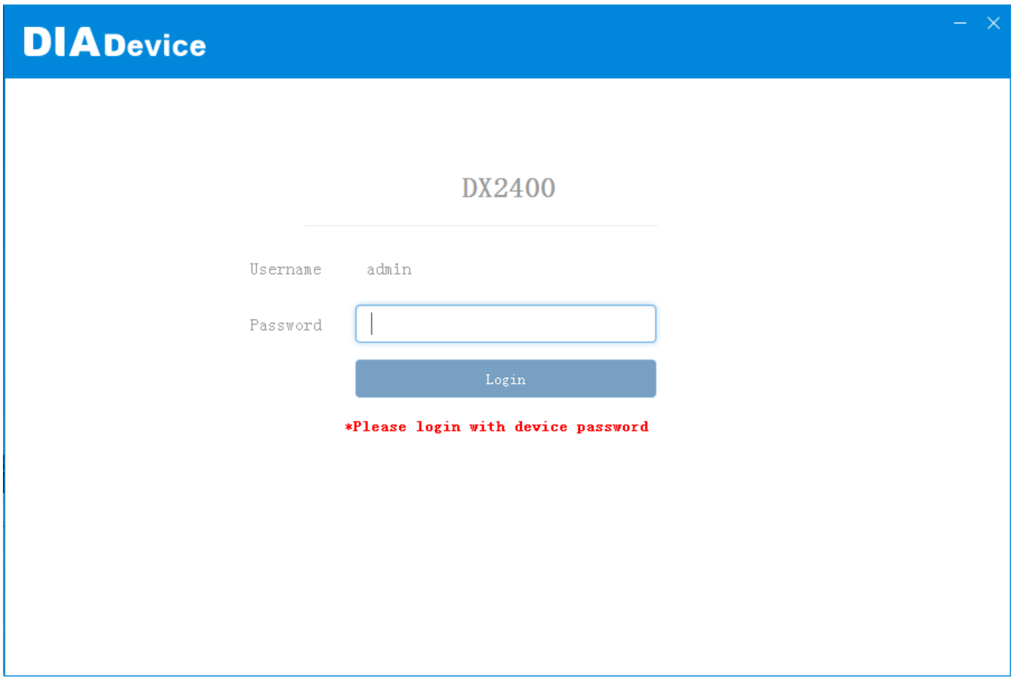
6. Click on “Detect”, and it will redirect to the login page of DX router.



Detect device automatically

Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

7. It will automatically redirect to the login page upon detecting the device. Enter the account and password on the login page.(Default: admin/admin)



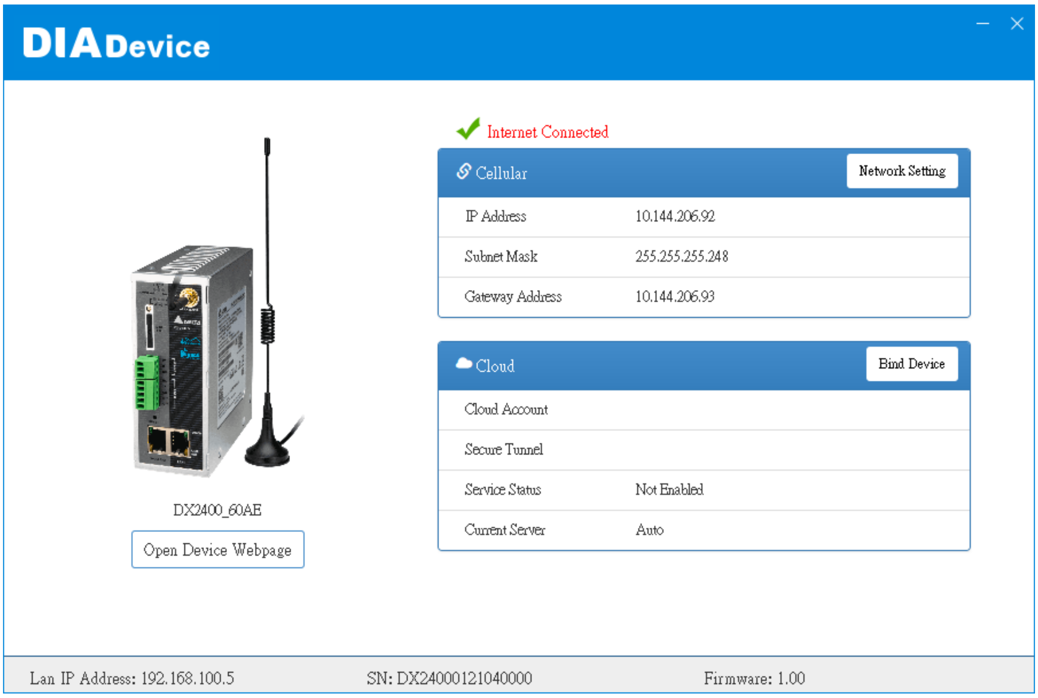
DX2400

Username admin

Password

*Please login with device password

8. Confirm if the network displays ✓ Internet Connected and the WAN port's IP Address is 10.144.206.92. (This is an example using a Private IP) Please verify with your IT department or network service provider if the IP address is indeed a Public one.



✓ Internet Connected

Cellular	Network Setting
IP Address	10.144.206.92
Subnet Mask	255.255.255.248
Gateway Address	10.144.206.93

Cloud	Bind Device
Cloud Account	
Secure Tunnel	
Service Status	Not Enabled
Current Server	Auto

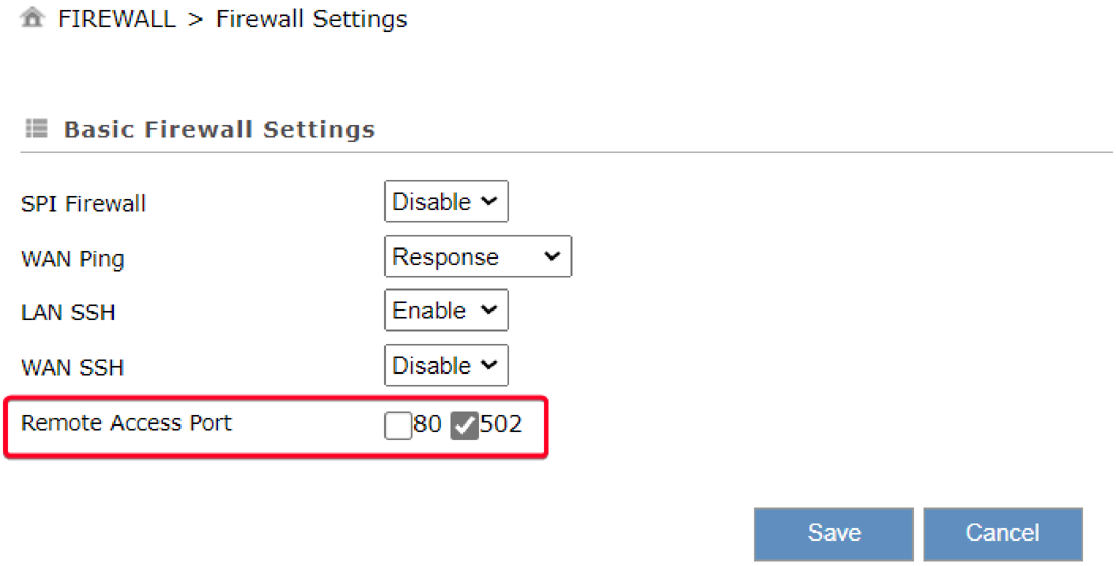
Lan IP Address: 192.168.100.5 SN: DX24000121040000 Firmware: 1.00

Notice

This application does not require binding with a DIACloud account, but if needed, data can also be uploaded to the DIACloud cloud platform for synchronization.

9. After entering DX router login page, input your account and password. (Default: admin/admin) and click on “login”.

10. Go to **FIREWALL** → **Firewall Settings**, check the checkbox of **Remote Access Port: 502**, then click on “Save”.



SPI Firewall: Disable

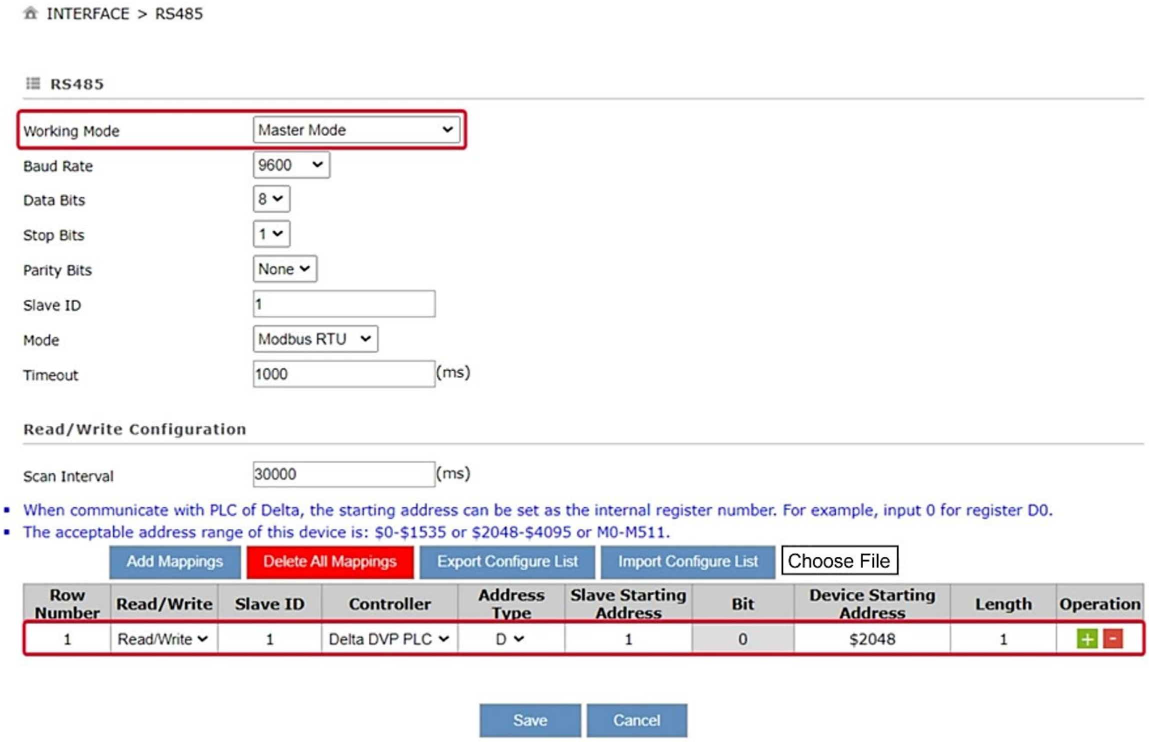
WAN Ping: Response

LAN SSH: Enable

WAN SSH: Disable

Remote Access Port: □80 ☑502

11. Go to **INTERFACE** → **RS485**, select **Master Mode** as **Working Mode** with the address of mapped register set to D1 →$2048, then click on "Save".



INTERFACE > RS485

RS485

Working Mode	Master Mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Slave ID	1
Mode	Modbus RTU
Timeout	1000 (ms)

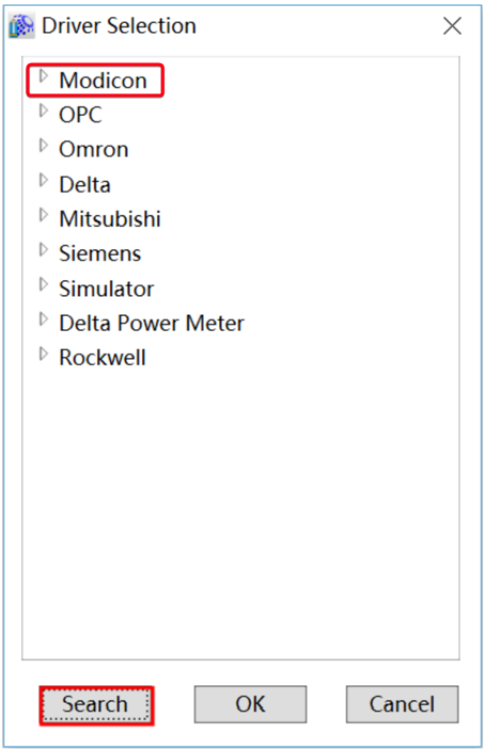
Read/Write Configuration

Scan Interval 30000 (ms)

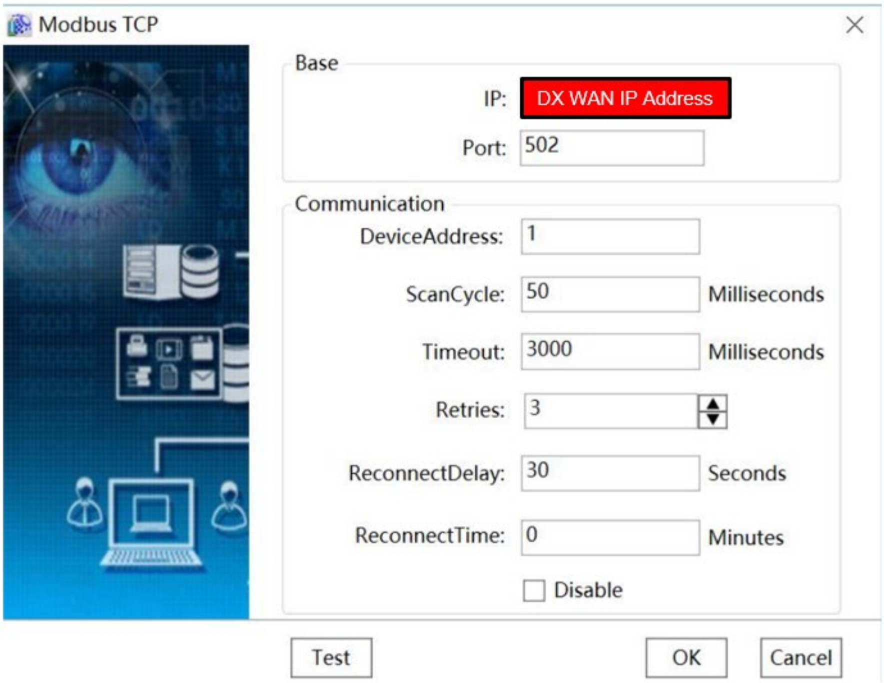
- When communicate with PLC of Delta, the starting address can be set as the internal register number. For example, input 0 for register D0.
- The acceptable address range of this device is: $0-$1535 or $2048-$4095 or M0-M511.

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

12. On another PC with network connected, open DIAView and go to **I/O** → **Driver** → **Modicon** → **MODBUS TCP.**



13. Enter the IP address of the cloud router's WAN port: 192.168.5.100:502, then click on “Test” to check if communication is successful.



Modbus TCP

Base

IP: DX WAN IP Address

Port: 502

Communication

DeviceAddress: 1

ScanCycle: 50 Milliseconds

Timeout: 3000 Milliseconds

Retries: 3

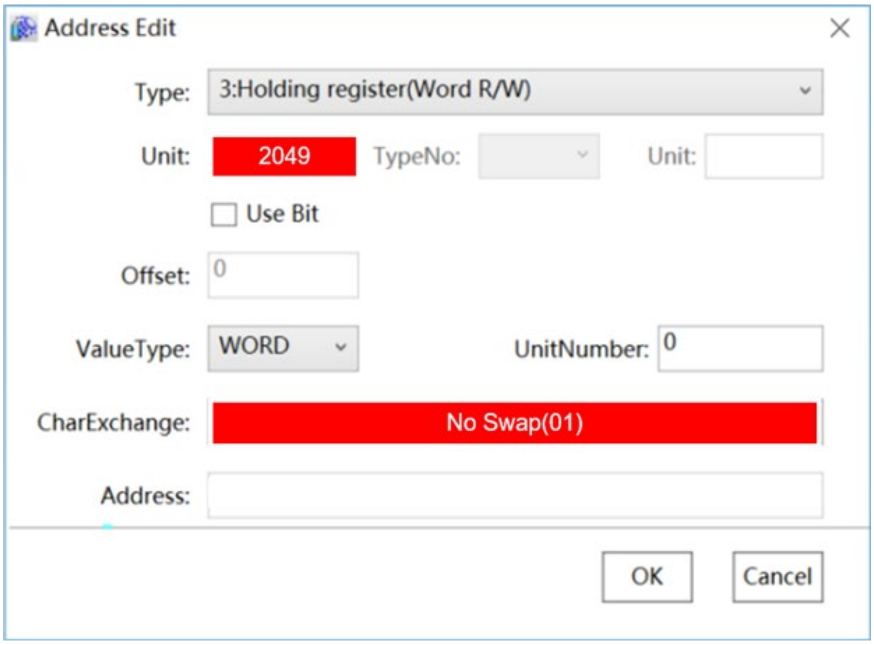
ReconnectDelay: 30 Seconds

ReconnectTime: 0 Minutes

☐ Disable

14. Select Driver and click +Add, then double click on ....

15. Select: **Type: 3:Holding register(Word R/W), Unit: 2049**, to read the data in the cloud router's register $2048."



Address Edit

Type: 3:Holding register(Word R/W)

Unit: 2049 TypeNo: Unit:

☐ Use Bit

Offset: 0

ValueType: WORD UnitNumber: 0

CharExchange: No Swap(01)

Address:

Notice

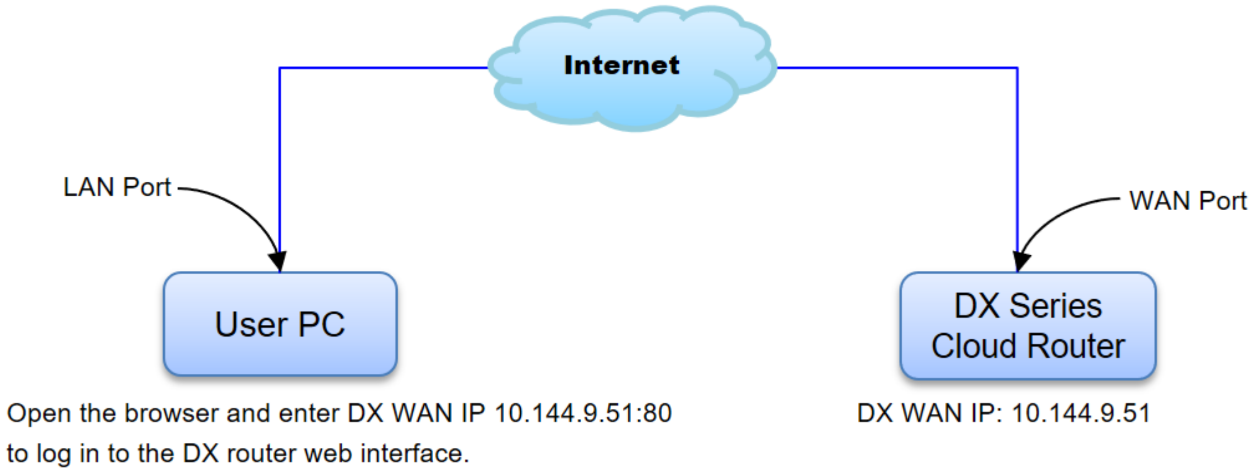
- The cloud router only supports Function code 3/16.
- To read the data in the cloud router's internal register $2048 in DIAView, you need to add 1 to the number, i.e., use 2049 to access that location.

2.3.14 WAN Port Access (Port 80) for Public Network Applications

With WAN Public IP address obtained from cloud router, you can login to the configuration page of cloud routers and configure parameters on your PC through port 80 from WAN of the cloud router in the external network.

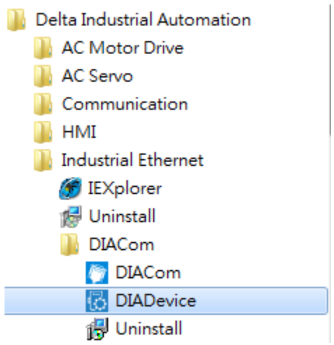
Notice:

1. This application would have port 80 open. Please do not use this feature if there's any security concern.
2. If the cloud router's WAN cannot obtain a public IP address, this application cannot be used. Please contact the company's IT department or network service provider to inquire about obtaining a public IP address.
3. Please refer to Chapter 3.3.1 Firewall Settings for a detailed explanation of the configuration parameters.


Internet
LAN Port
WAN Port
User PC
DX Series Cloud Router
Open the browser and enter DX WAN IP 10.144.9.51:80 to log in to the DX router web interface.
DX WAN IP: 10.144.9.51

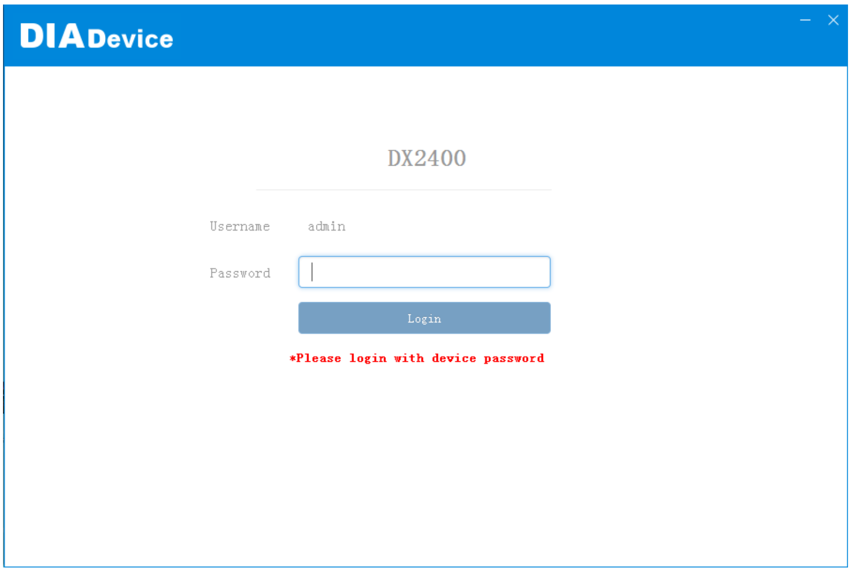
Setup Steps

1. Make sure that all the basic configuration detailed in Chapter 2.2 has been completed and functions properly. Please verify with your IT department or network service provider if the IP address is indeed a Public one.
2. Use a network cable to connect LAN ports on your PC and the DX router.
3. Install DIACom software.
4. Open DIADevice: Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice**.



5. Click on “Detect”, and it will redirect to the login page of DX router.

6. After DIACom detects the device, it will automatically jump to the login page, and you need to enter login password on the login page (Default username/ password = admin/admin)



DIADevice

DX2400

Username admin

Password |

Login

*Please login with device password

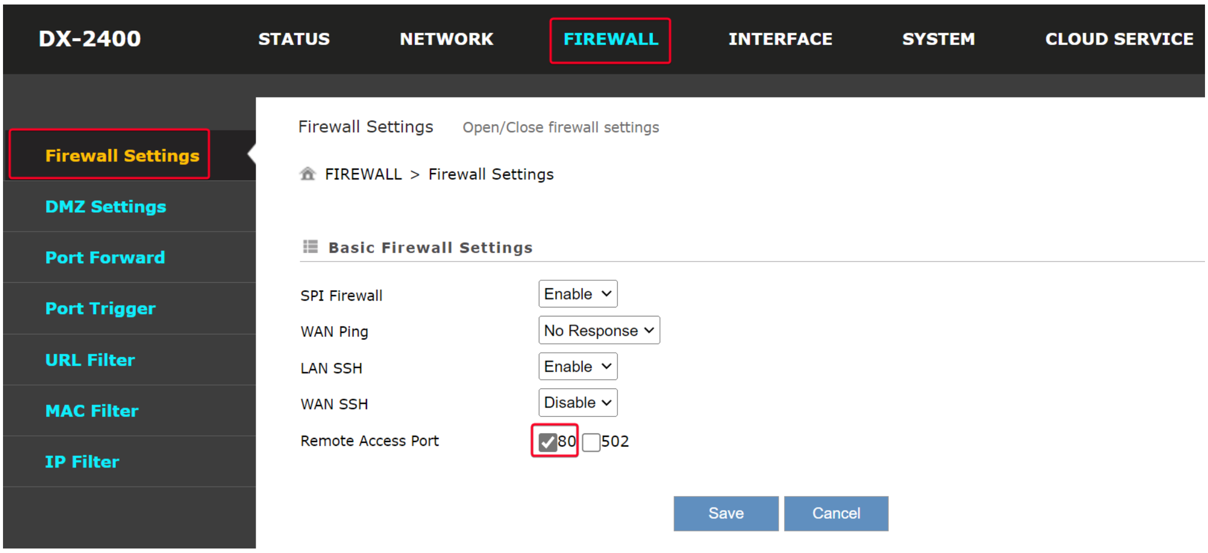
7. Confirm if the network displays ✓ Internet Connected and the WAN port's IP Address is 10.144.9.51. (This is an example using Class B Private network, the Internet cannot connect to the cloud router.) Please verify with your IT department or network service provider if the IP address is indeed a Public one.

Notice

- If a private IP address is obtained = 192.168.x.x(Class A)、172.16.x.x(Class B)、10.x.x.x(Class C)， it will not be possible to establish a connection from the public network.
- This application does not require binding with a DIACloud account, but if needed, data can also be uploaded to the DIACloud cloud platform for synchronization.
- This application can be used within a local network, so it may display messages indicating internet disconnection. The network status will depend on the user's context.

8. After entering DX router login page, input your account and password. (Default: admin/admin) and click on “login”.

9. Go to **FIREWALL** → **Firewall Settings**, check the checkbox of **Remote Access Port: 80**, then click on “Save”.



Firewall Settings Open/Close firewall settings

FIREWALL > Firewall Settings

Basic Firewall Settings

SPI Firewall: Enable
WAN Ping: No Response
LAN SSH: Enable
WAN SSH: Disable
Remote Access Port: ☑80 □502

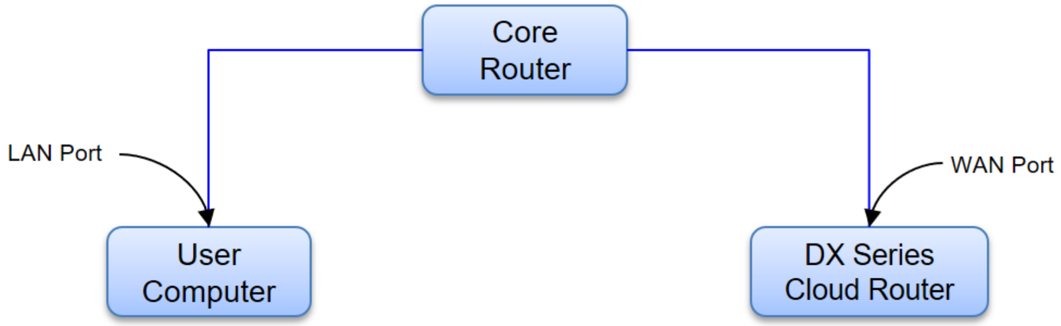
10. After connecting the Ethernet cable from your PC to the WAN port of the cloud router, enter http://10.144.9.51:80 on your browser and you can login to the cloud router’s configuration page.

2.3.15 WAN Port Access (Port 80) for Private Network Applications

With the Private IP address obtained from the cloud router, you can login to the configuration page of cloud routers and configure parameters on your PC through port 80 from WAN of the cloud router in the internal network.

Notice:

1. This application would have port 80 open. Please do not use this feature if there’s any security concern.
2. Please refer to Chapter 3.3.1 Firewall Settings for a detailed explanation of the configuration parameters.

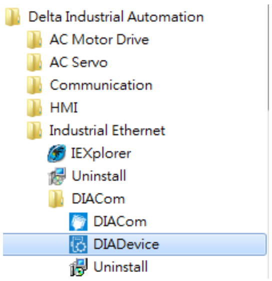


Launch the browser and enter DX WAN IP 192.168.5.100:80
You can log in to the DX router web interface

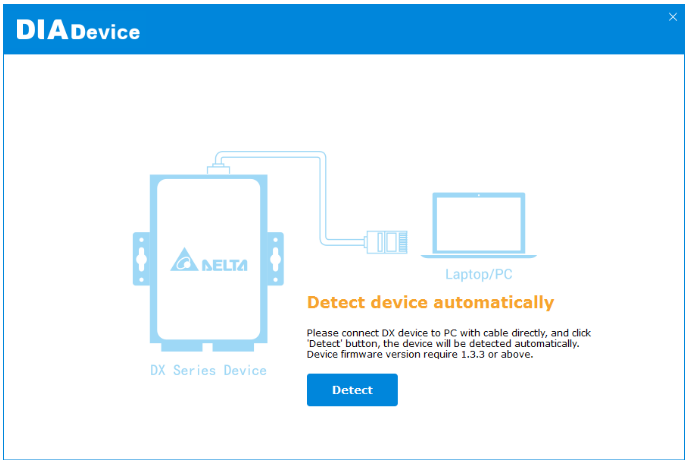
DX WAN IP: 192.168.5.100:80

Setup Steps

1. Use a network cable to connect LAN ports on your PC and the DX router.
2. Install DIACom software.
3. Open DIADevice: Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice**.



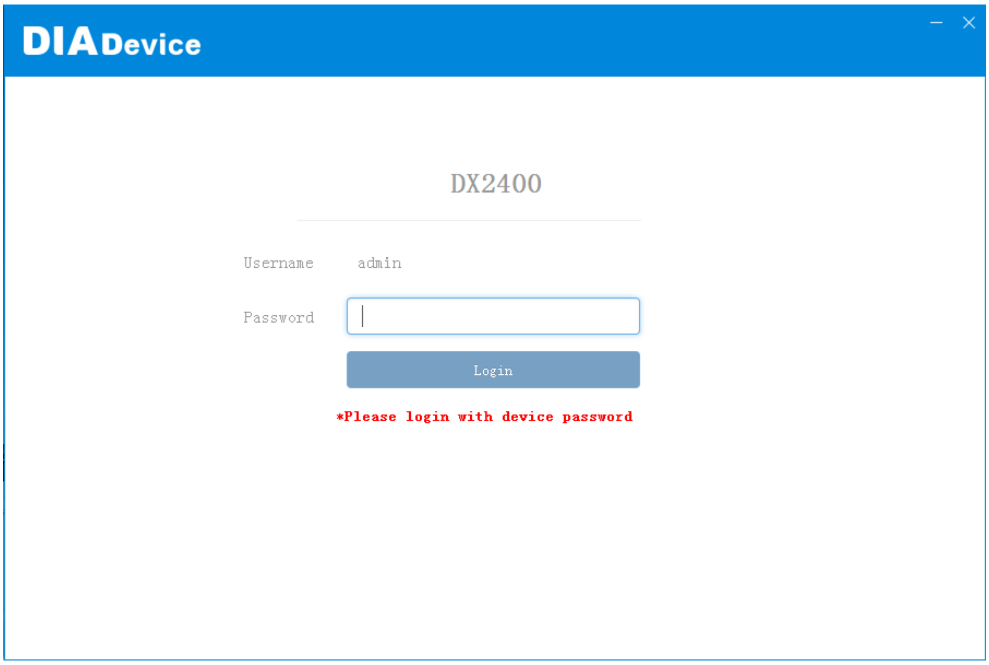
4. Click on “Detect”, and it will redirect to the login page of DX router.



Detect device automatically

Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

5. It will automatically redirect to the login page upon detecting the device. Enter the account and password on the login page.(Default: admin/admin)



DIADevice

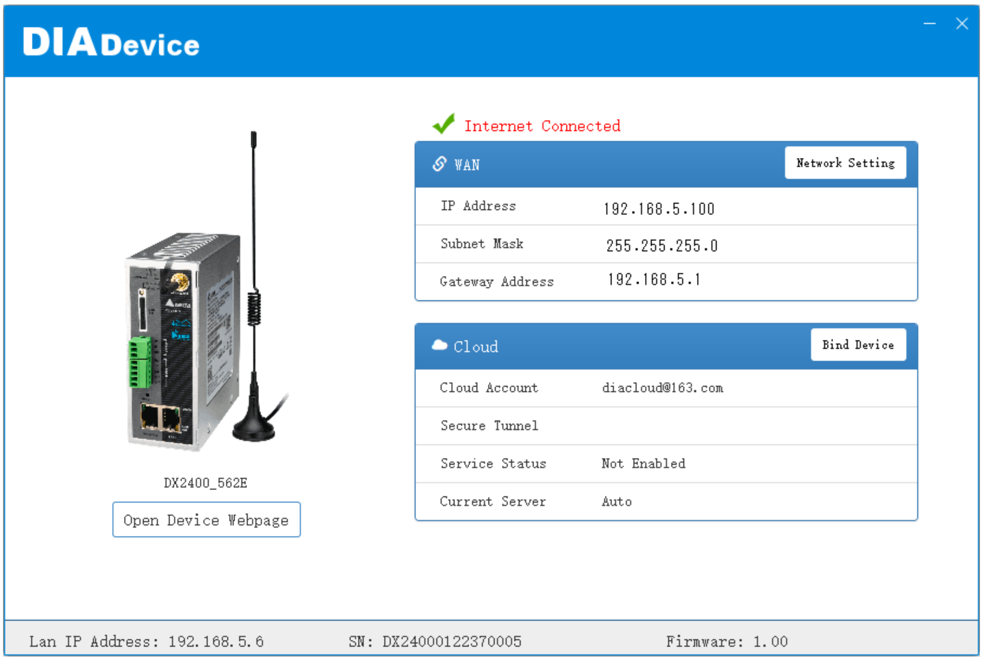
DX2400

Username admin

Password

*Please login with device password

6. The cloud router's WAN port obtains a DHCP IP address from the upstream router, or manually configure the IP address to 192.168.5.100. Because this application uses a Private IP, so it may display messages indicating internet disconnection. The network status will depend on the user's context.



DIADevice

✓ Internet Connected

WAN	Network Setting
IP Address	192.168.5.100
Subnet Mask	255.255.255.0
Gateway Address	192.168.5.1

Cloud	Bind Device
Cloud Account	diacloud@163.com
Secure Tunnel	
Service Status	Not Enabled
Current Server	Auto

DX2400_562E

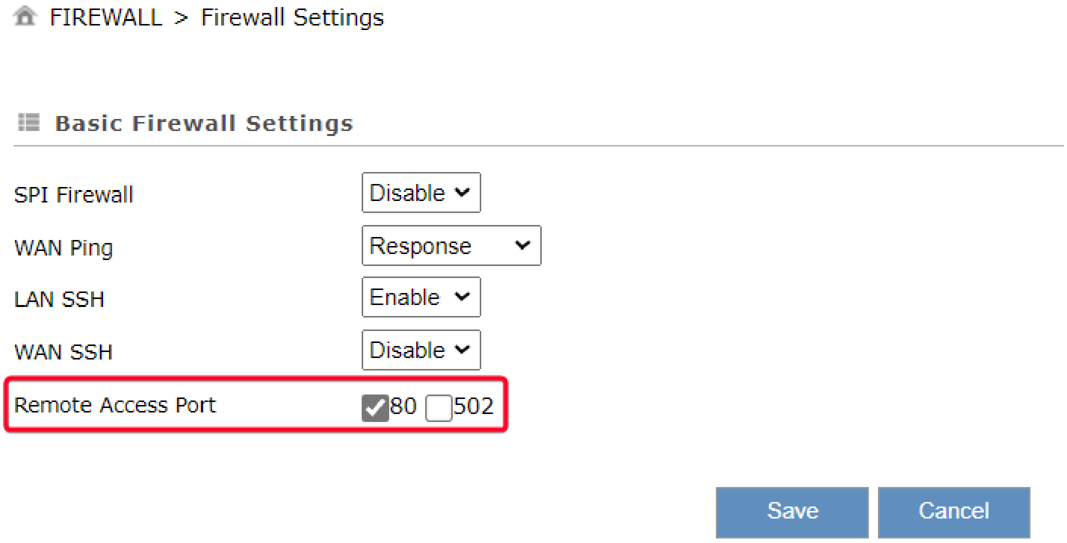
Lan IP Address: 192.168.5.6 SN: DX24000122370005 Firmware: 1.00

Notice

- This application does not require binding with a DIACloud account, but if needed, data can also be uploaded to the DIACloud cloud platform for synchronization.
- This application can be used within a local network, so it may display messages indicating internet disconnection. The network status will depend on the user's context.

7. After entering DX router login page, input your account and password. (Default: admin/admin) and click on “login”.

8. Go to **FIREWALL → Firewall Settings**, check the checkbox of **Remote Access Port: 80**, then click on “Save”.


FIREWALL > Firewall Settings

Basic Firewall Settings

SPI Firewall: Disable

WAN Ping: Response

LAN SSH: Enable

WAN SSH: Disable

Remote Access Port: ☑80 □502

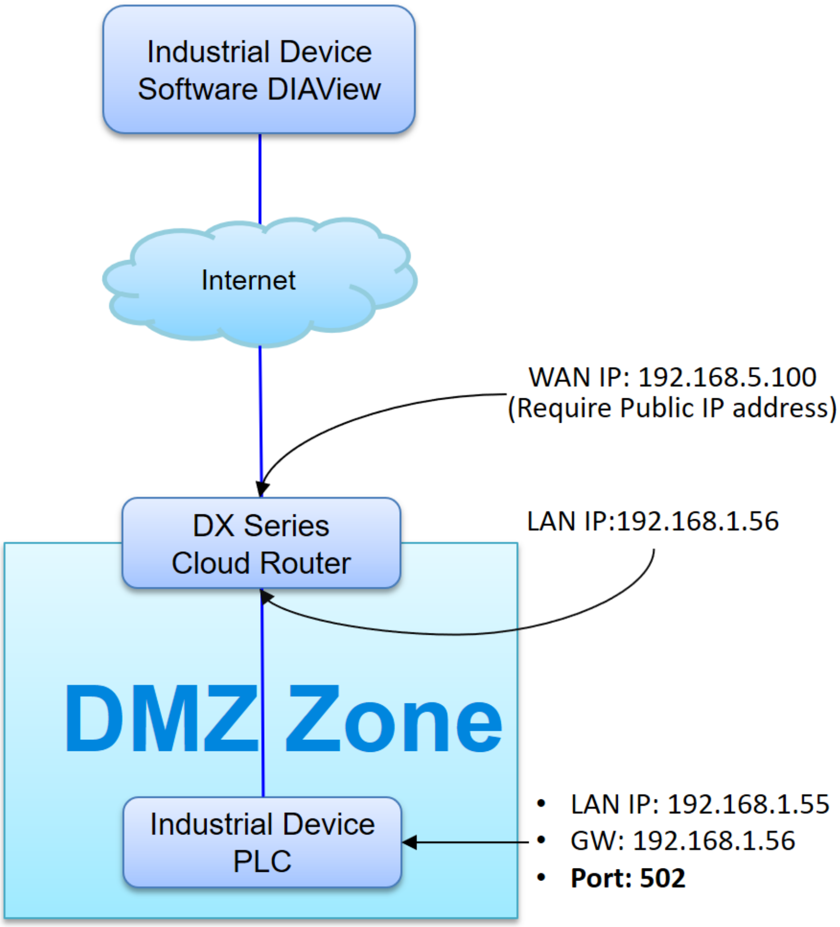
9. After connecting the Ethernet cable from your PC to the WAN port of the cloud router, enter http://192.168.5.100:80 on your browser and you can login to the cloud router’s configuration page.

2.3.16 DMZ Public Network Application

DIAView sends data to the Cloud Router WAN port via the Internet, and then transmits the data to the PLC through the LAN port. DIAView can communicate directly with the PLC.

If the cloud router's WAN cannot obtain a public IP address, this application cannot be used. Please contact the company's IT department or network service provider to inquire about obtaining a public IP address.

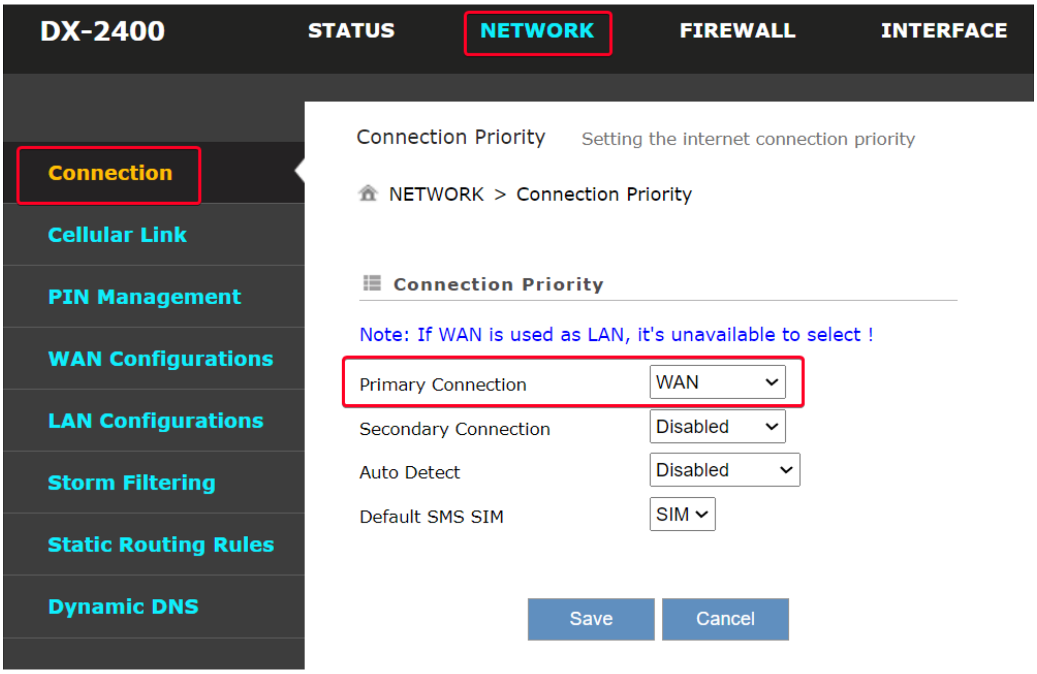
Please refer to Chapter 3.3.2 DMZ Settings for a detailed explanation of the configuration parameters.



Cloud Router Configuration

1. Login to the cloud router config page with ID: admin/ PW: admin.
2. Connect the WAN port of cloud router to a public network.
3. Use a network cable to connect LAN ports on your PC and the DX router.
4. Login to DX cloud router. Account: admin / Password: admin.

5. Go to **Network** → **Connection,** choose **WAN** as **Primary Connection**, then click on **"Save".**



Connection Priority Setting the internet connection priority

NETWORK > Connection Priority

Connection Priority

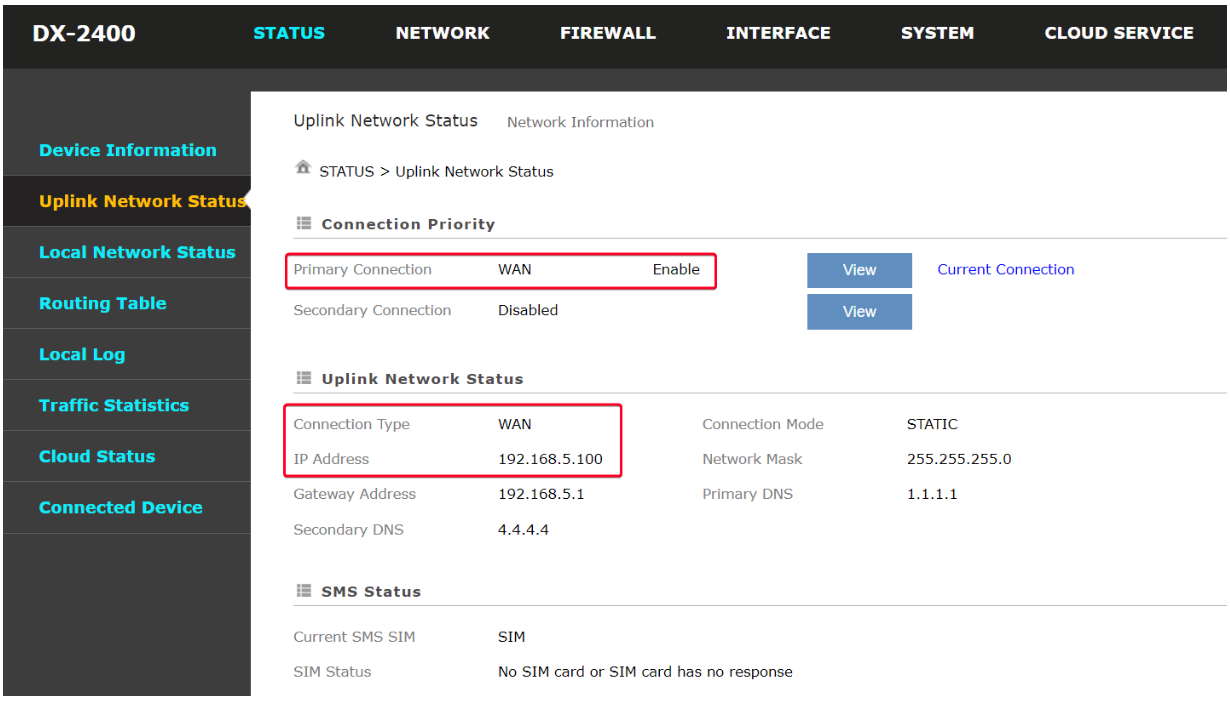
Note: If WAN is used as LAN, it's unavailable to select !

Primary Connection	WAN
Secondary Connection	Disabled
Auto Detect	Disabled
Default SMS SIM	SIM

6. Go to **STATUS** → **Uplink Network Status**, check the IP address and confirm with the internal IT or network service provider whether a fixed public IP address is available. **(This is an example using Class A Private network, the Internet cannot connect to the cloud router).**

Notice

If a private IP address is obtained = 192.168.x.x(Class A)、172.16.x.x(Class B)、10.x.x.x(Class C), it will not be possible to establish a connection from the public network.



Uplink Network Status Network Information

STATUS > Uplink Network Status

Connection Priority

Primary Connection	WAN	Enable
Secondary Connection	Disabled	

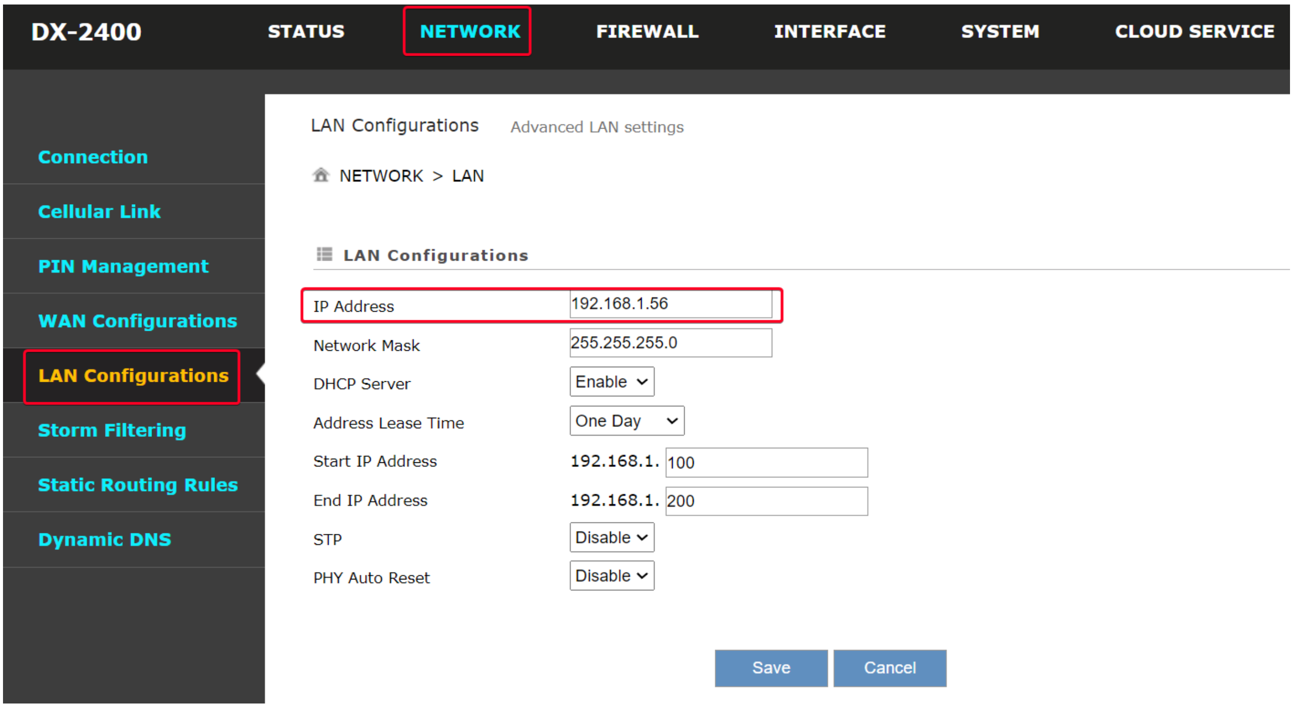
Uplink Network Status

Connection Type	WAN	Connection Mode	STATIC
IP Address	192.168.5.100	Network Mask	255.255.255.0
Gateway Address	192.168.5.1	Primary DNS	1.1.1.1
Secondary DNS	4.4.4.4		

SMS Status

Current SMS SIM	SIM
SIM Status	No SIM card or SIM card has no response

7. Go to **NETWORK** → **LAN Configuration**, the information of IP configuration is shown below. Please note that the LAN port IP segment should not be the same as the WAN port segment.



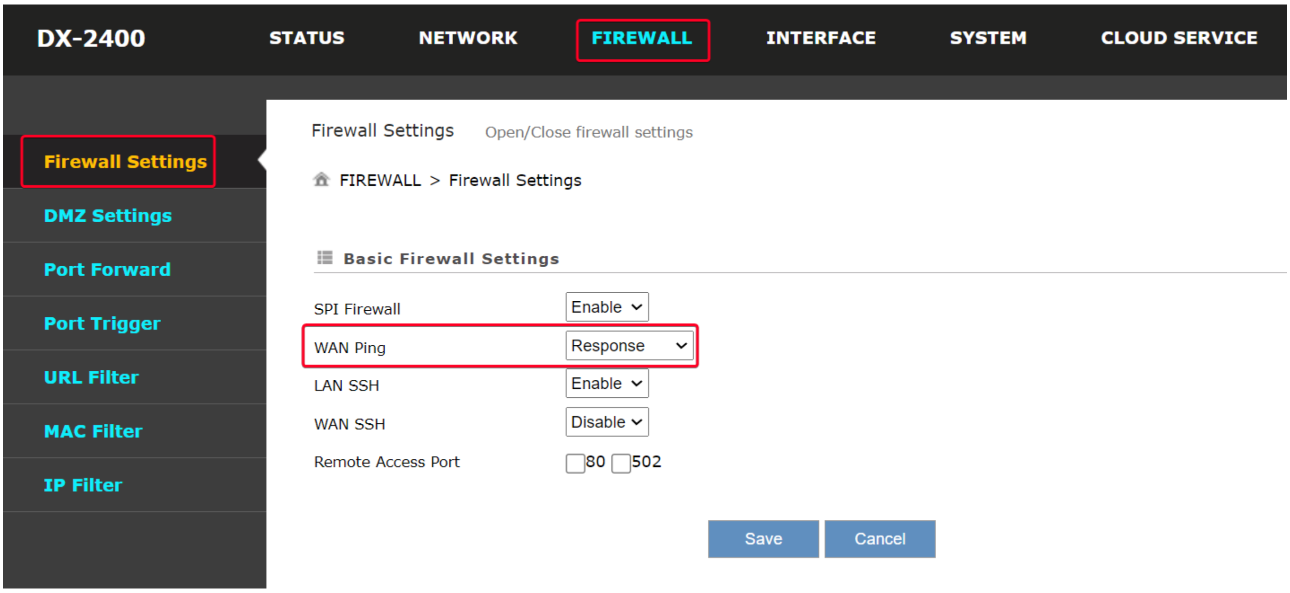
LAN Configurations Advanced LAN settings

NETWORK > LAN

LAN Configurations

IP Address	192.168.1.56
Network Mask	255.255.255.0
DHCP Server	Enable
Address Lease Time	One Day
Start IP Address	192.168.1. 100
End IP Address	192.168.1. 200
STP	Disable
PHY Auto Reset	Disable

8. Go to **FIREWALL** → **Firewall Settings** and set **WAN Ping** to **Response**.



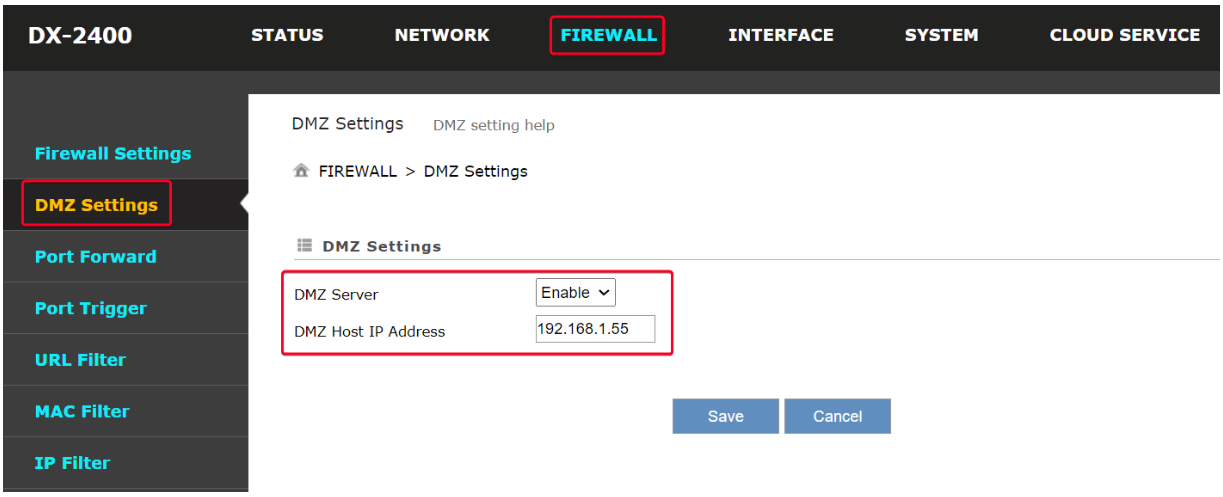
Firewall Settings Open/Close firewall settings

FIREWALL > Firewall Settings

Basic Firewall Settings

SPI Firewall	Enable
WAN Ping	Response
LAN SSH	Enable
WAN SSH	Disable
Remote Access Port	□80 □502

9. Go to **FIREWALL** → **DMZ Settings**, set **DMZ server** to **Enable** and set **DMZ Host IP Address** to the IP address of the downstream device:**192.168.1.55**. Please note that only one downstream device can be set as the DMZ host.



DMZ Settings

FIREWALL > DMZ Settings

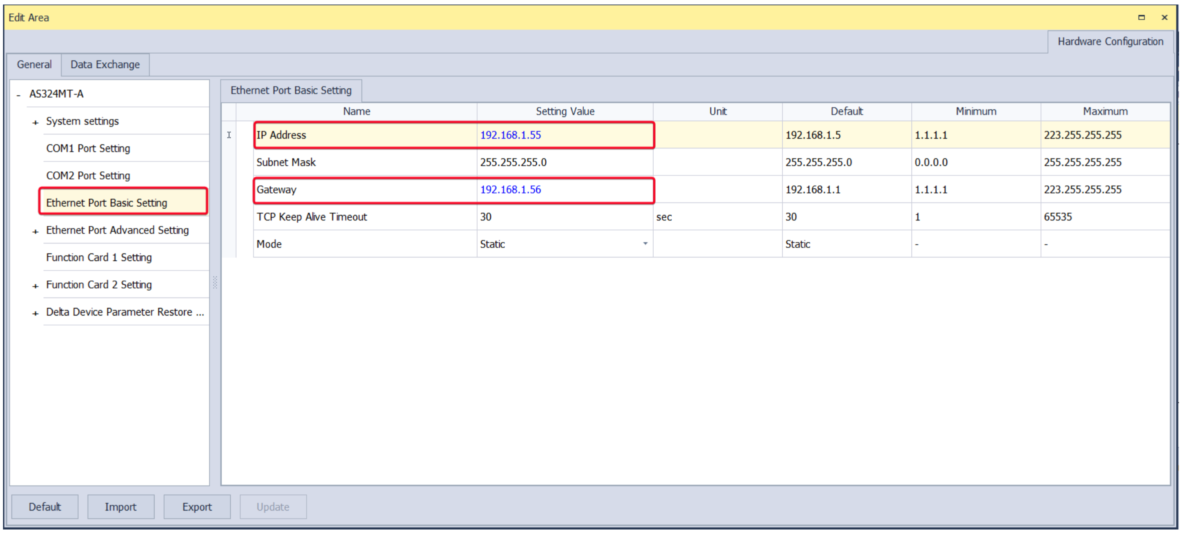
DMZ Settings

DMZ Server: Enable

DMZ Host IP Address: 192.168.1.55

PLC Configuration

1. To change the Delta PLC IP address to 192.168.1.55 using ISPSoft, the IP address should be in the same network segment as the Cloud Router LAN IP. Additionally, set the gateway address to the Cloud Router LAN IP address, which is 192.168.1.56.

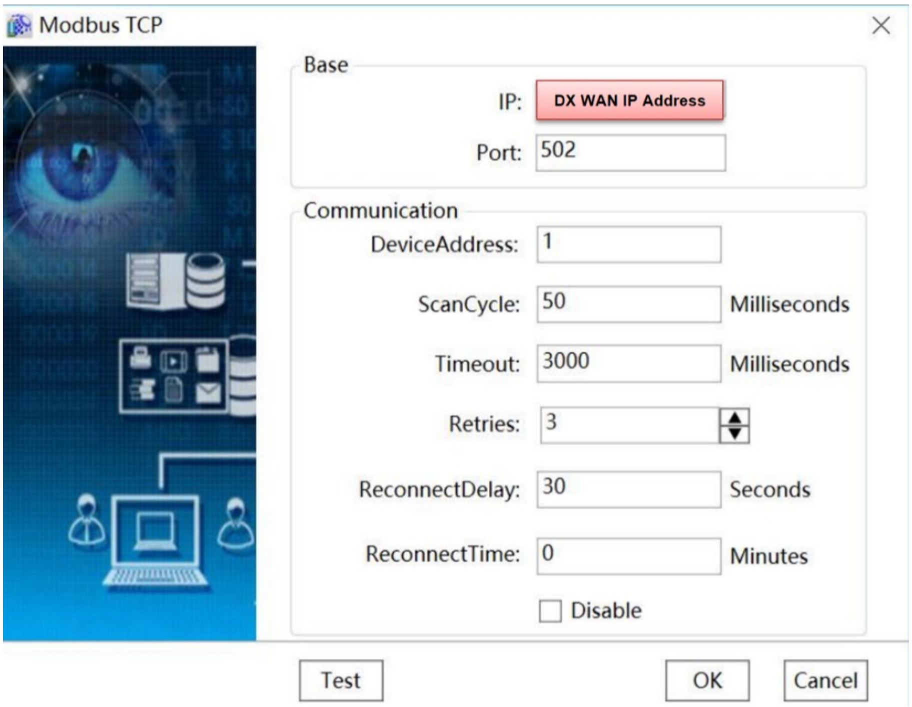


Ethernet Port Basic Setting

Name	Setting Value	Unit	Default	Minimum	Maximum
IP Address	192.168.1.55		192.168.1.5	1.1.1.1	223.255.255.255
Subnet Mask	255.255.255.0		255.255.255.0	0.0.0.0	255.255.255.255
Gateway	192.168.1.56		192.168.1.1	1.1.1.1	223.255.255.255
TCP Keep Alive Timeout	30	sec	30	1	65535
Mode	Static		Static	-	-

PC&DIAView Configuration

1. Check whether the PC can connect to the internet.
2. Open DIAView, set the connection IP to the **Cloud Router's WAN IP address: 192.168.5.100**, set **the port number to 502.** With the function enabled, DMZ will forward packets to the destination device on LAN port with the IP address 192.168.1.55. Thus, the communication would be completed.



Modbus TCP

Base

IP: DX WAN IP Address

Port: 502

Communication

DeviceAddress: 1

ScanCycle: 50 Milliseconds

Timeout: 3000 Milliseconds

Retries: 3

ReconnectDelay: 30 Seconds

ReconnectTime: 0 Minutes

□ Disable

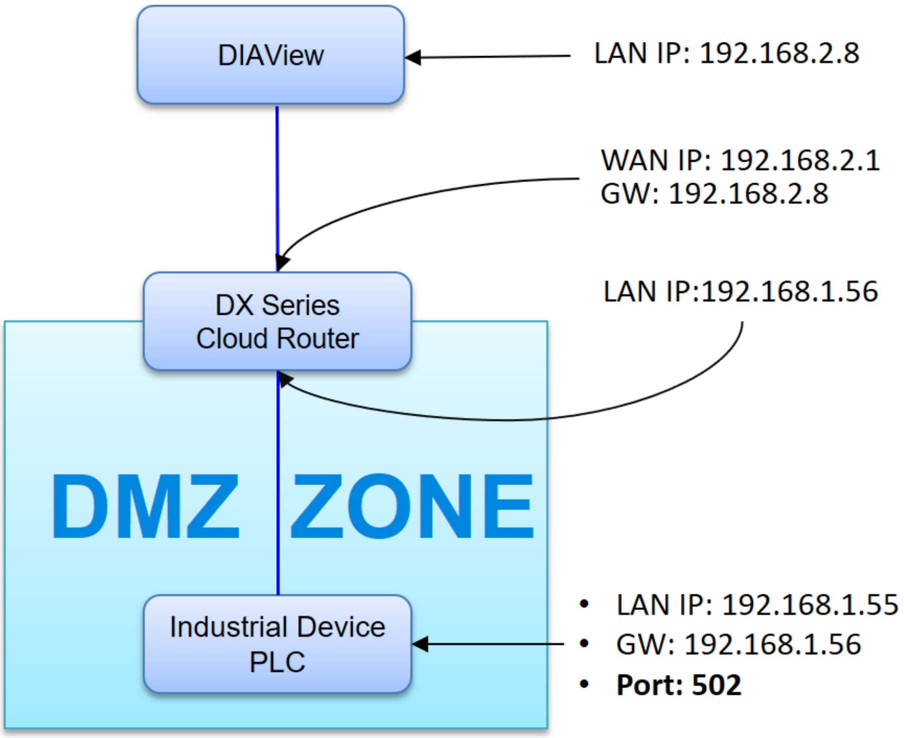
Notice:

In case that the connection between DIAview and the PLC failed, please check whether the PC is connected to multiple networks at the same time. For example, both WiFi and LAN network are currently being used. Please turn off WiFi network and remain the LAN network connected to the cloud routers.

2.3.17 DMZ Private Network Application

DIAView sends data to the Cloud Router WAN port through a private network, and then transmits the data to the PLC through the LAN port. DIAView can communicate directly with the PLC.

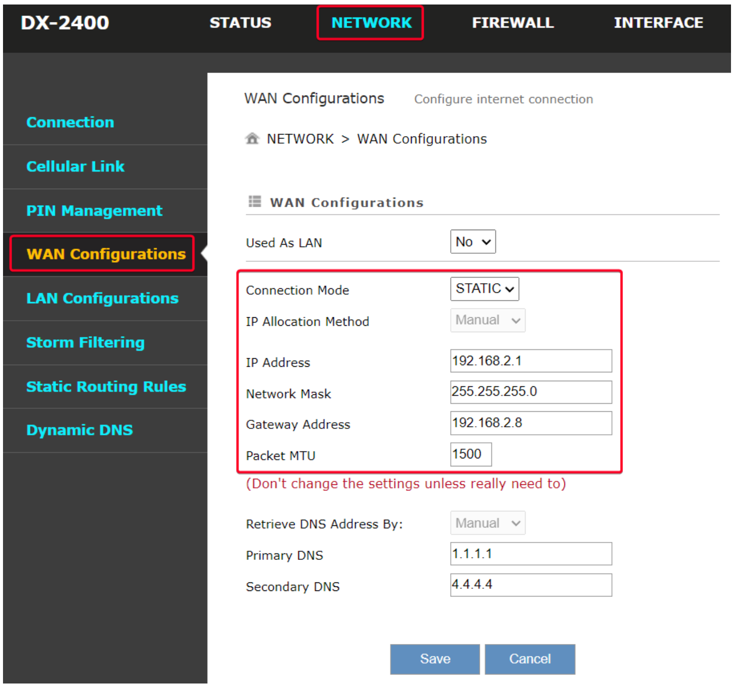
Please refer to Chapter 3.3.2 DMZ Settings for a detailed explanation of the configuration parameters.



Cloud Router Configuration

1. Login to the cloud router config page with ID: admin/ PW: admin
2. Connect the PC, which has been installed DIAView, to the WAN port of the cloud router using Ethernet cable.
3. Use a network cable to connect LAN ports on your PC and the DX router.
4. Login to DX cloud router. Account: admin / Password: admin.

5. Go to **NETWORK** → **WAN Configurations**, select **STATIC** as **Connection Mode**, enter the other IP address information as shown below.



WAN Configurations Configure internet connection

NETWORK > WAN Configurations

WAN Configurations

Used As LAN: No

Connection Mode: STATIC

IP Allocation Method: Manual

IP Address: 192.168.2.1

Network Mask: 255.255.255.0

Gateway Address: 192.168.2.8

Packet MTU: 1500

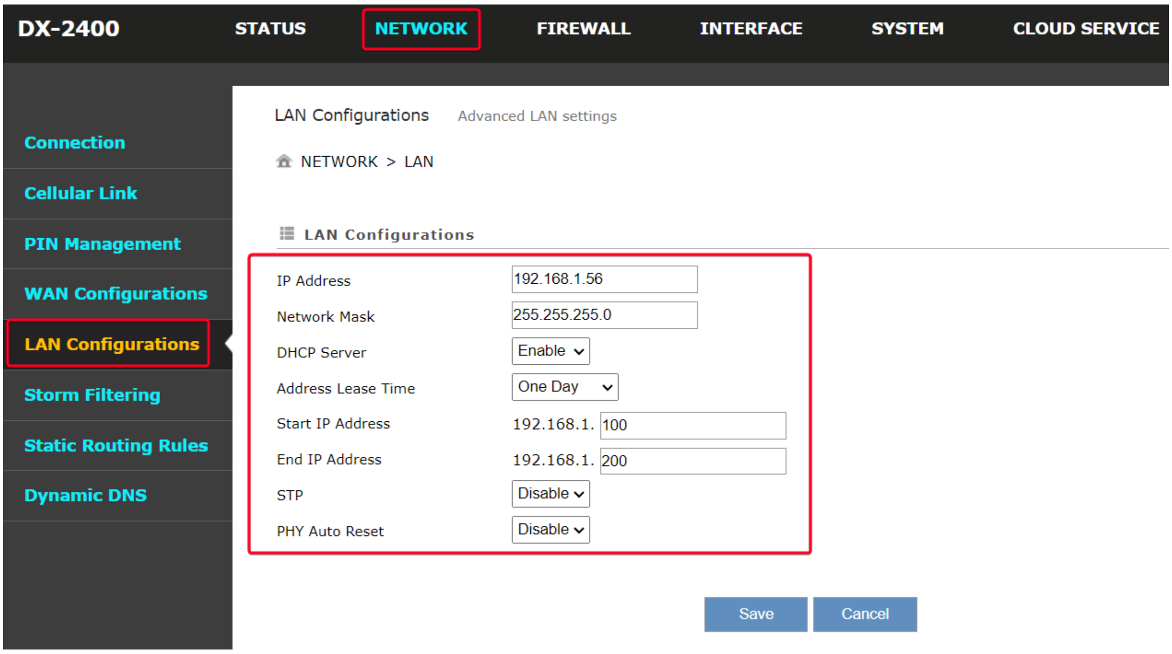
(Don't change the settings unless really need to)

Retrieve DNS Address By: Manual

Primary DNS: 1.1.1.1

Secondary DNS: 4.4.4.4

6. Go to **NETWORK** → **LAN Configuration**, for setting the following IP-related information. Please note that the LAN port IP segment must not be the same as the WAN port segment.



LAN Configurations Advanced LAN settings

NETWORK > LAN

LAN Configurations

IP Address: 192.168.1.56

Network Mask: 255.255.255.0

DHCP Server: Enable

Address Lease Time: One Day

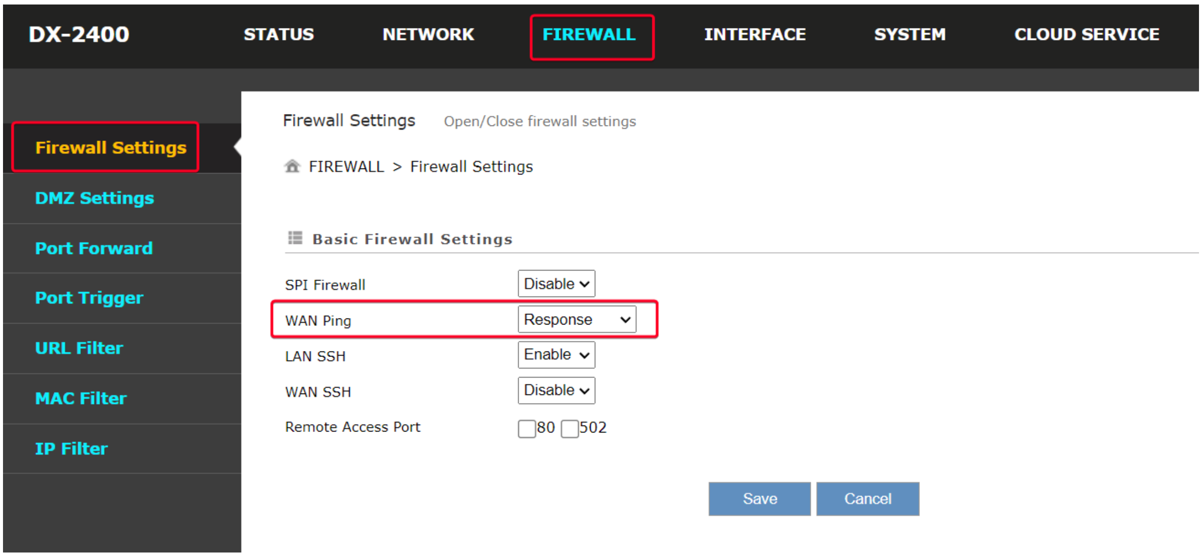
Start IP Address: 192.168.1. 100

End IP Address: 192.168.1. 200

STP: Disable

PHY Auto Reset: Disable

7. Go to **FIREWALL** → **Firewall Settings** and set **WAN Ping** to **Response.**



Firewall Settings Open/Close firewall settings

FIREWALL > Firewall Settings

Basic Firewall Settings

SPI Firewall: Disable

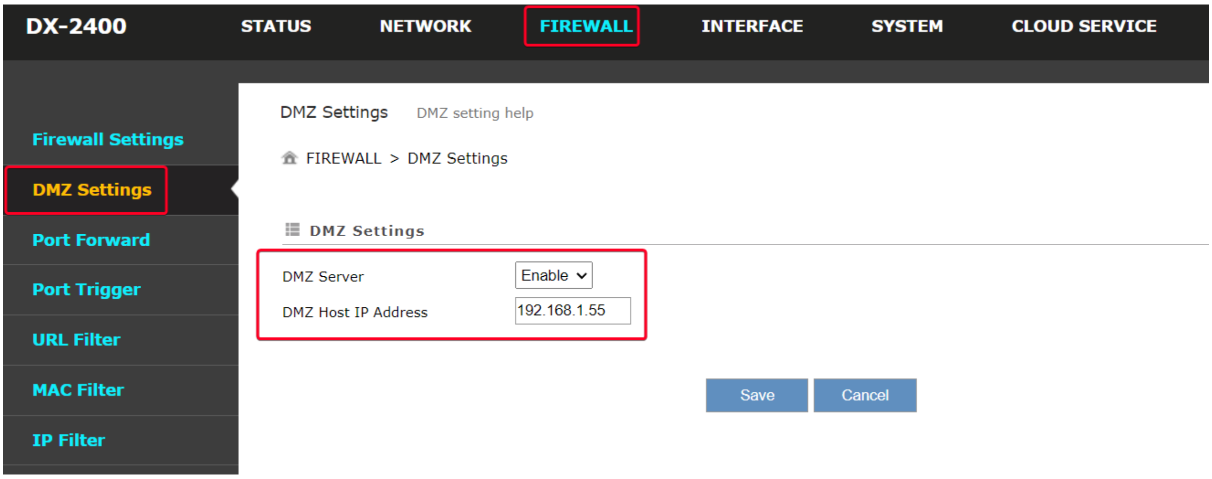
WAN Ping: Response

LAN SSH: Enable

WAN SSH: Disable

Remote Access Port: □80 □502

8. Go to **FIREWALL** → **DMZ Settings**, set **DMZ server** to **Enable** and set **DMZ Host IP Address** to the IP address of the downstream device:**192.168.1.55.** Please note that only one downstream device can be set as the DMZ host.



DMZ Settings DMZ setting help

FIREWALL > DMZ Settings

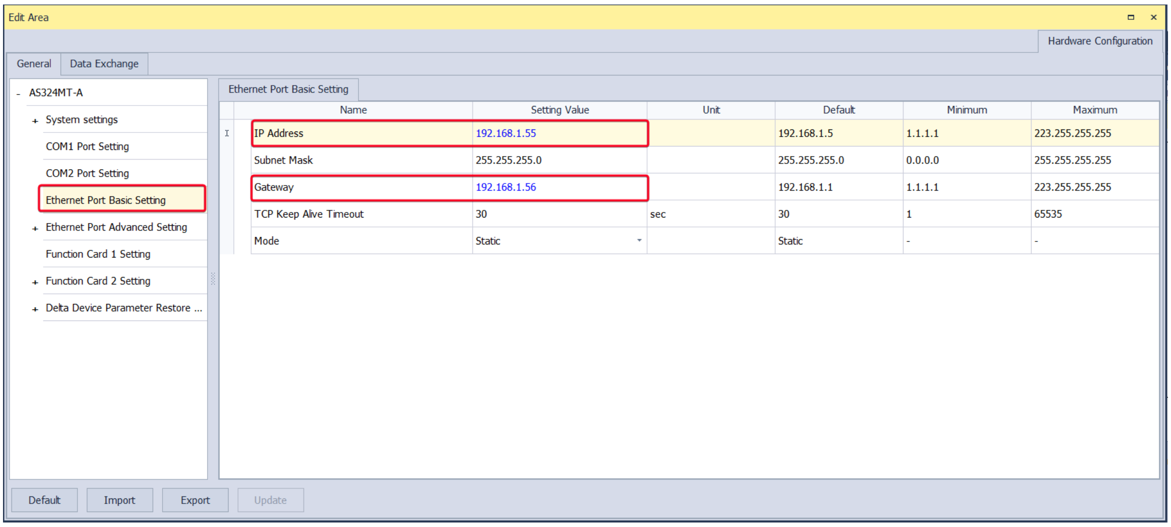
DMZ Settings

DMZ Server: Enable

DMZ Host IP Address: 192.168.1.55

PLC Configuration

1. To change the Delta PLC IP address to 192.168.1.55 using ISPSoft, the IP address should be in the same network segment as the Cloud Router LAN IP. Additionally, set the gateway address to the Cloud Router LAN IP address, which is 192.168.1.56



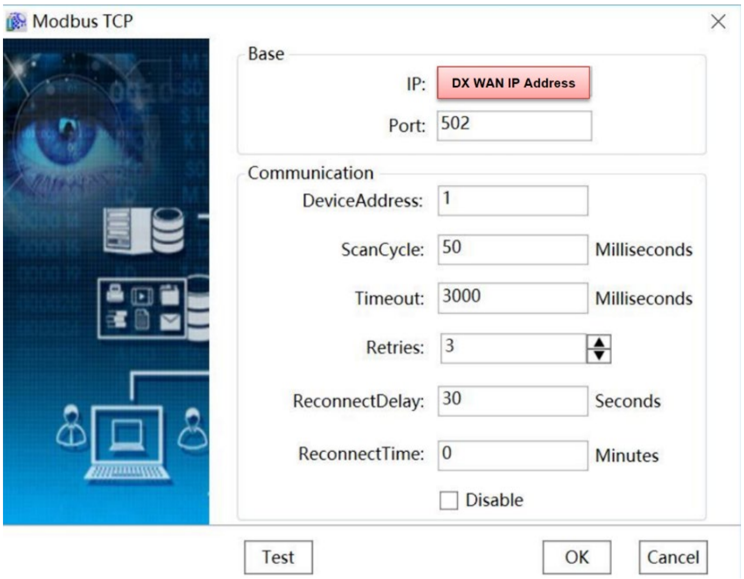
- AS324MT-A
  - System settings
  - COM1 Port Setting
  - COM2 Port Setting
  - Ethernet Port Basic Setting
  - Ethernet Port Advanced Setting
  - Function Card 1 Setting
  - Function Card 2 Setting
  - Delta Device Parameter Restore ...

Name	Setting Value	Unit	Default	Minimum	Maximum
IP Address	192.168.1.55		192.168.1.5	1.1.1.1	223.255.255.255
Subnet Mask	255.255.255.0		255.255.255.0	0.0.0.0	255.255.255.255
Gateway	192.168.1.56		192.168.1.1	1.1.1.1	223.255.255.255
TCP Keep Alve Timeout	30	sec	30	1	65535
Mode	Static		Static	-	-

DIAView Configuration

1. Check whether the PC can connect to the internet.

2. Open DIAView, set the connection IP to the **Cloud Router's WAN IP address: 192.168.5.100, set the port number to 502**. With the function enabled, DMZ will forward packets to the destination device on LAN port with the IP address 192.168.1.55. Thus, the communication would be completed.



Base

IP: DX WAN IP Address

Port: 502

Communication

DeviceAddress: 1

ScanCycle: 50 Milliseconds

Timeout: 3000 Milliseconds

Retries: 3

ReconnectDelay: 30 Seconds

ReconnectTime: 0 Minutes

☐ Disable

Notice:

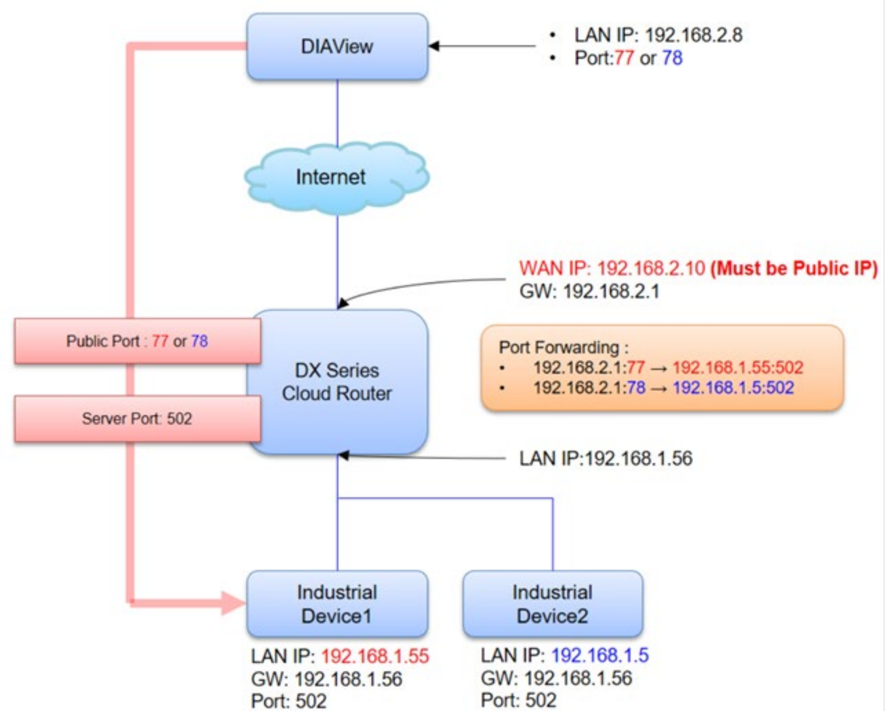
In case that the connection between DIAview and the PLC failed, please check whether the PC is connected to multiple networks at the same time. For example, both WiFi and LAN network are currently being used. Please turn off WiFi network and remain the LAN network connected to the cloud routers.

2.3.18 Port Forward Public Network Application

DIAView uses Port 77 or 78 over the public network (Internet) to transmit data from the WAN port of the cloud router to the specified 502 Port and IP address under the LAN port, either to the PLC device at 192.168.1.5:502 or 192.168.1.55:502.

If the cloud router's WAN cannot obtain a public IP address, this application cannot be used. Please contact the company's IT department or network service provider to inquire about obtaining a public IP address.

Please refer to Chapter 3.3.4 Port Forward for a detailed explanation of the configuration parameters.



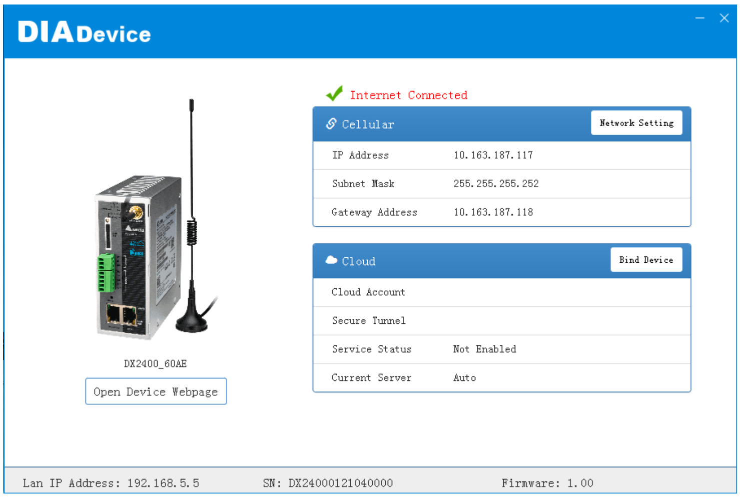
Cloud Router Configuration

1. Connect the WAN port of cloud router to a public network

2. Use a network cable to connect LAN ports on your PC and the DX router.

3. Login to DX cloud router. Account: admin / Password: admin.

4. Click on Open Device Webpage.



✓ Internet Connected

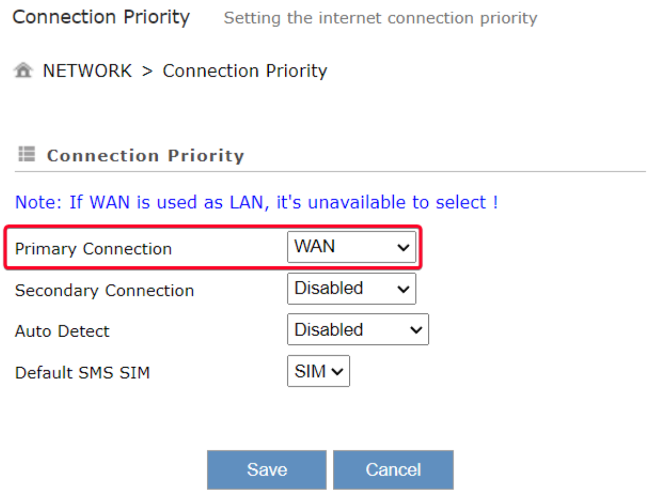
Cellular	
IP Address	10.163.187.117
Subnet Mask	255.255.255.252
Gateway Address	10.163.187.118

Cloud	
Cloud Account	
Secure Tunnel	
Service Status	Not Enabled
Current Server	Auto

Lan IP Address: 192.168.5.5 SN: DX24000121040000 Firmware: 1.00

5. After entering DX router login page, input your account and password. (Default: admin/admin) and click login.

6. Go to **Network** → **Connection**, choose **WAN** as **Primary Connection**, then click on “Save” and confirm the following items.



Connection Priority Setting the internet connection priority

NETWORK > Connection Priority

Connection Priority

Note: If WAN is used as LAN, it's unavailable to select !

Primary Connection	WAN
Secondary Connection	Disabled
Auto Detect	Disabled
Default SMS SIM	SIM

a. Check whether the light of LINK/Ack on WAN port is on or not. If not, check the network cable is connected and functioning properly.

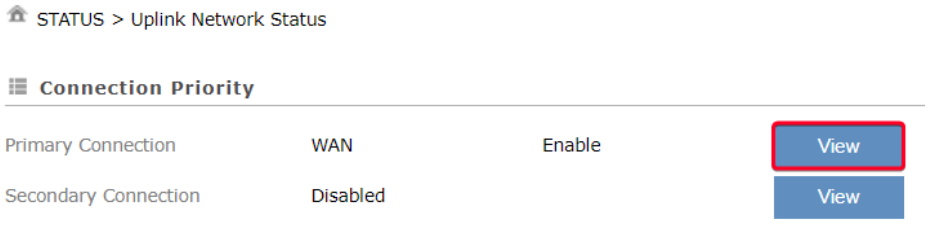
b. Check whether WAN IP address setting differs from LAN IP address.

c. Check if there’s a firewall setup for your corporate network. In case external ports or IP addresses are restricted, login to https://diacloudsolutions.com/and click ? from the menu on the upper right corner, then set the required port for DIACloud to the whitelist in Firewall Rule.

Notice

If required, MAC address of DX router can be found via the following page.

1. Go to **STATUS** → **Uplink Networks Status** → **Primary Connection** and click **View**.

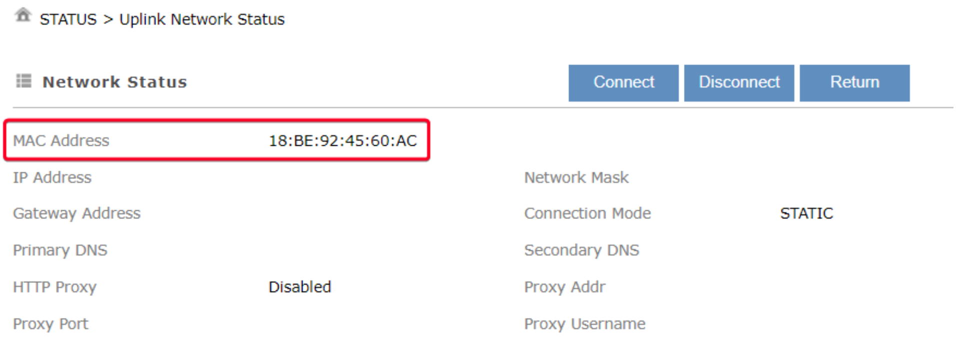


STATUS > Uplink Network Status

Connection Priority

Primary Connection	WAN	Enable	View
Secondary Connection	Disabled		View

2. Find MAC address in Network Status.



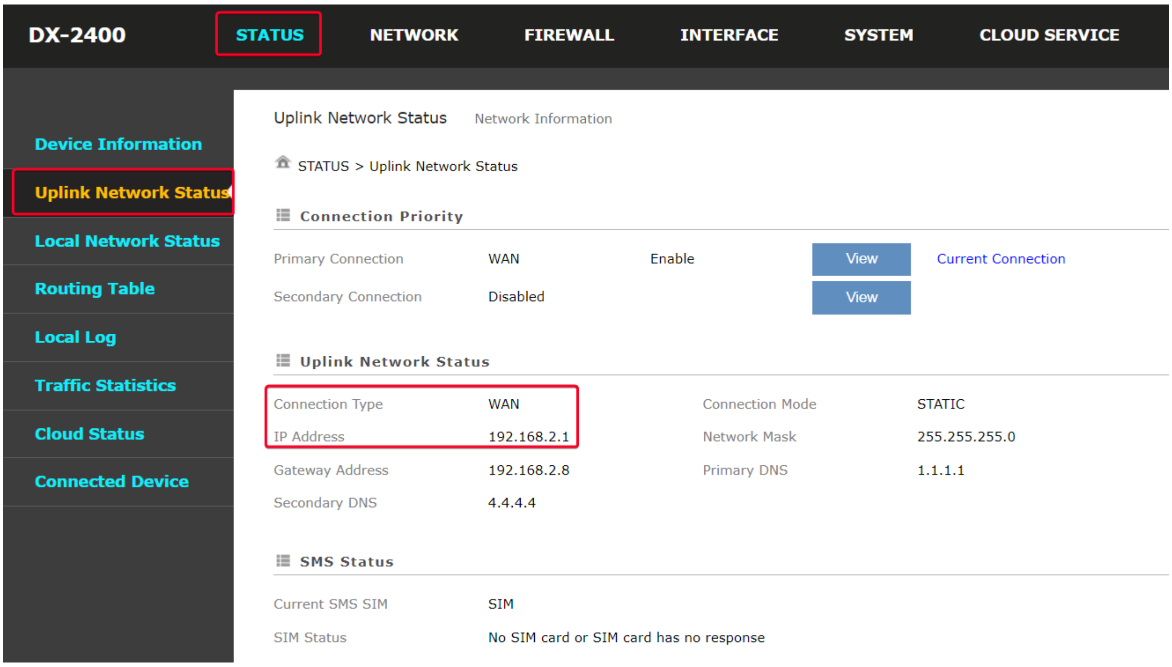
STATUS > Uplink Network Status

Network Status

MAC Address	18:BE:92:45:60:AC		
IP Address		Network Mask	
Gateway Address		Connection Mode	STATIC
Primary DNS		Secondary DNS	
HTTP Proxy	Disabled	Proxy Addr	
Proxy Port		Proxy Username	

7. Go to **STATUS** → **Uplink Network Status** → **Primary connection** and click **View**. Check if there's an IP Address on the Network Status page and verify with your internal IT department or network service provider whether a fixed public IP address is available. (Example shown below is private network).

> **Notice**
>
> ⚠ If a private IP address is obtained = 192.168.x.x(Class A) 、172.16.x.x(Class B) 、10.x.x.x(Class C), it will not be possible to establish a connection from the public network.



Connection Priority

Primary Connection	WAN	Enable	View
Secondary Connection	Disabled		View

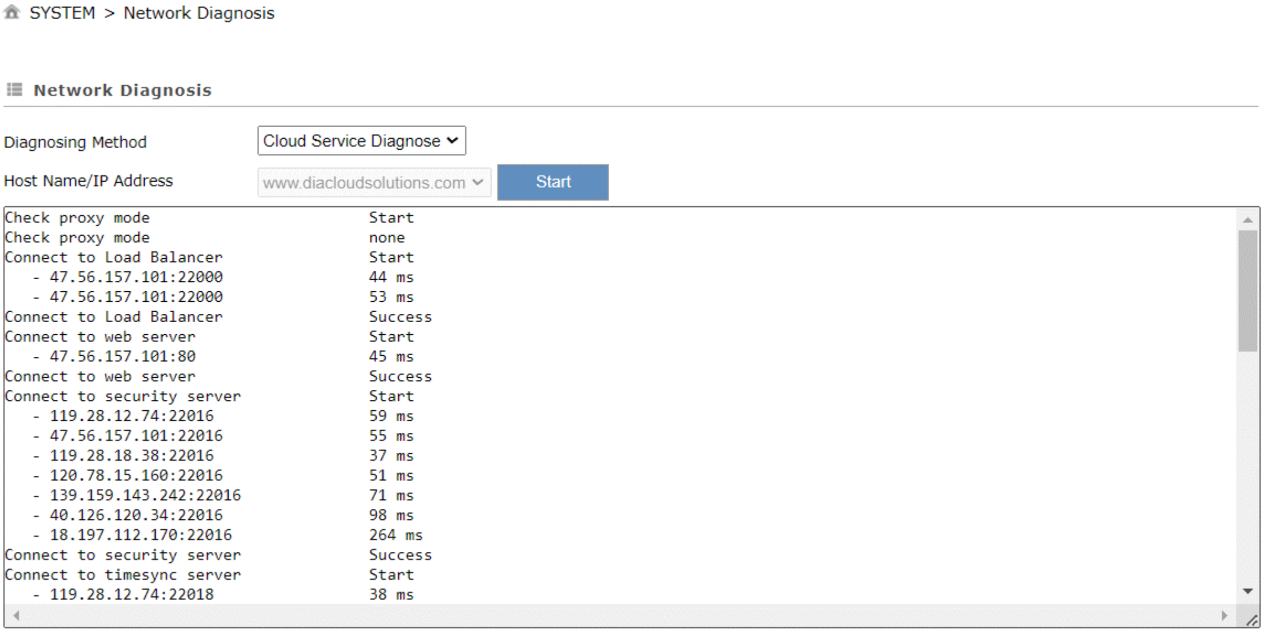
Uplink Network Status

Connection Type	WAN	Connection Mode	STATIC
IP Address	192.168.2.1	Network Mask	255.255.255.0
Gateway Address	192.168.2.8	Primary DNS	1.1.1.1
Secondary DNS	4.4.4.4		

SMS Status

Current SMS SIM	SIM
SIM Status	No SIM card or SIM card has no response

8. Go to **SYSTEM** → **Network Diagnosis** → **Cloud Service Diagnose** and check if there's any error. If there's any error, please go back to step three to verify.

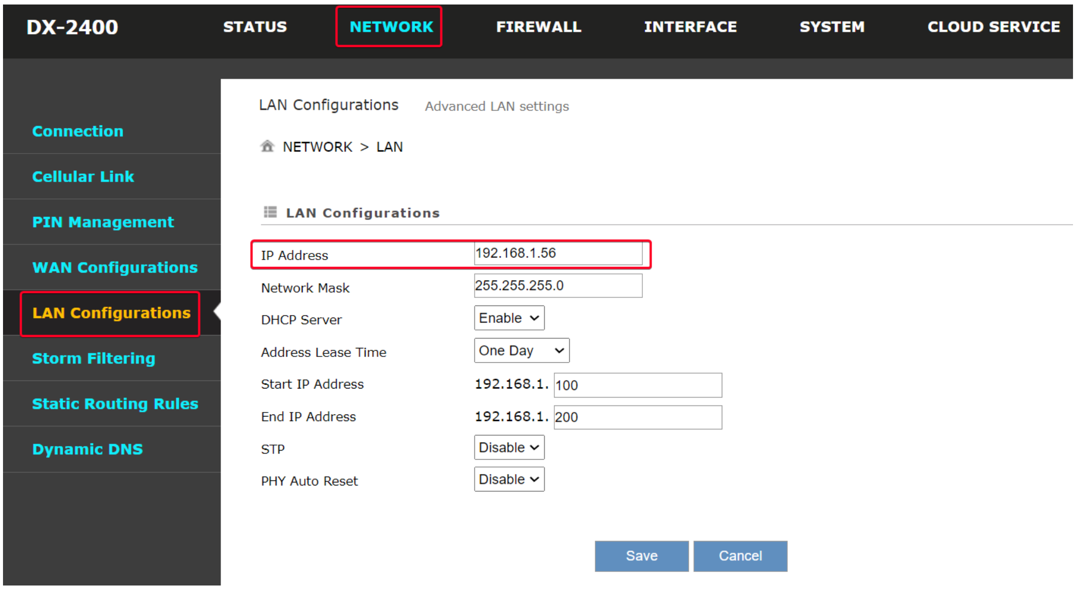


Diagnosing Method: Cloud Service Diagnose

Host Name/IP Address: www.diacloudsolutions.com

```
Check proxy mode                        Start
Check proxy mode                        none
Connect to Load Balancer                Start
   - 47.56.157.101:22000                44 ms
   - 47.56.157.101:22000                53 ms
Connect to Load Balancer                Success
Connect to web server                   Start
   - 47.56.157.101:80                   45 ms
Connect to web server                   Success
Connect to security server              Start
   - 119.28.12.74:22016                 59 ms
   - 47.56.157.101:22016                55 ms
   - 119.28.18.38:22016                 37 ms
   - 120.78.15.160:22016                51 ms
   - 139.159.143.242:22016              71 ms
   - 40.126.120.34:22016                98 ms
   - 18.197.112.170:22016               264 ms
Connect to security server              Success
Connect to timesync server              Start
   - 119.28.12.74:22018                 38 ms
```

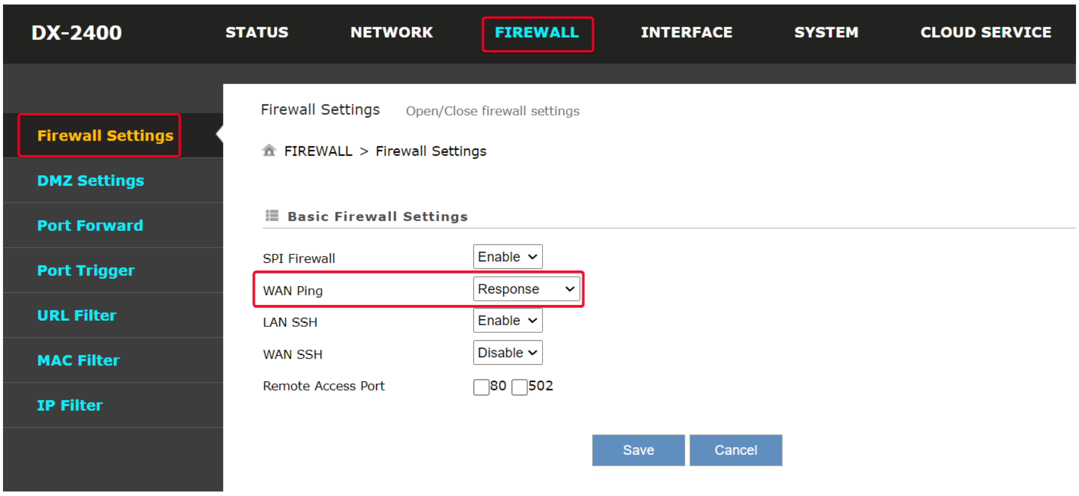
9. Go to **NETWORK** → **LAN Configuration**, the information of IP configuration is shown below. Please note that the LAN port IP segment should not be the same as the WAN port segment.



LAN Configurations

IP Address	192.168.1.56
Network Mask	255.255.255.0
DHCP Server	Enable
Address Lease Time	One Day
Start IP Address	192.168.1. 100
End IP Address	192.168.1. 200
STP	Disable
PHY Auto Reset	Disable

10. Go to **FIREWALL** → **Firewall Settings** and set **WAN Ping** to **Response**.



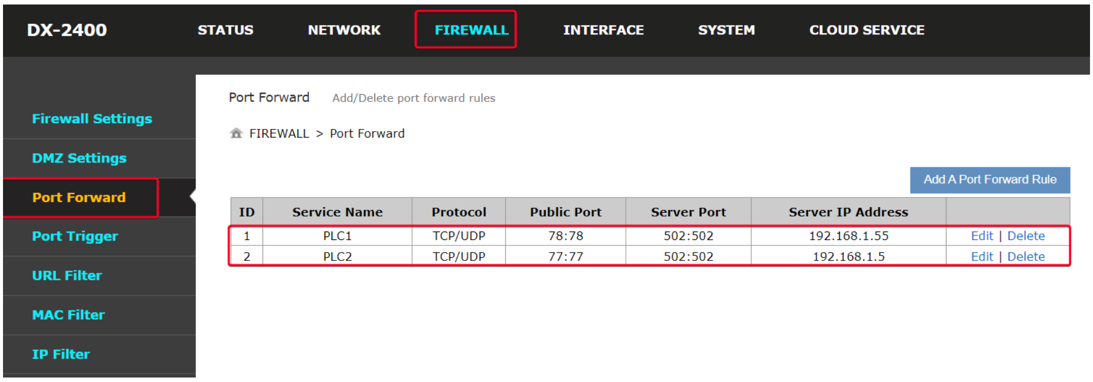
Basic Firewall Settings

SPI Firewall	Enable
WAN Ping	Response
LAN SSH	Enable
WAN SSH	Disable
Remote Access Port	□80 □502

11. Go to **FIREWALL** → **Port Forward,** and click on **Add a Port Forward Rule**

ID1: Triggers port 78 from external network to forward data to internal IP: 192.168.1.55:502.

ID2: Triggers port 77 from external network to forward data to internal IP: 192.168.1.5:502.

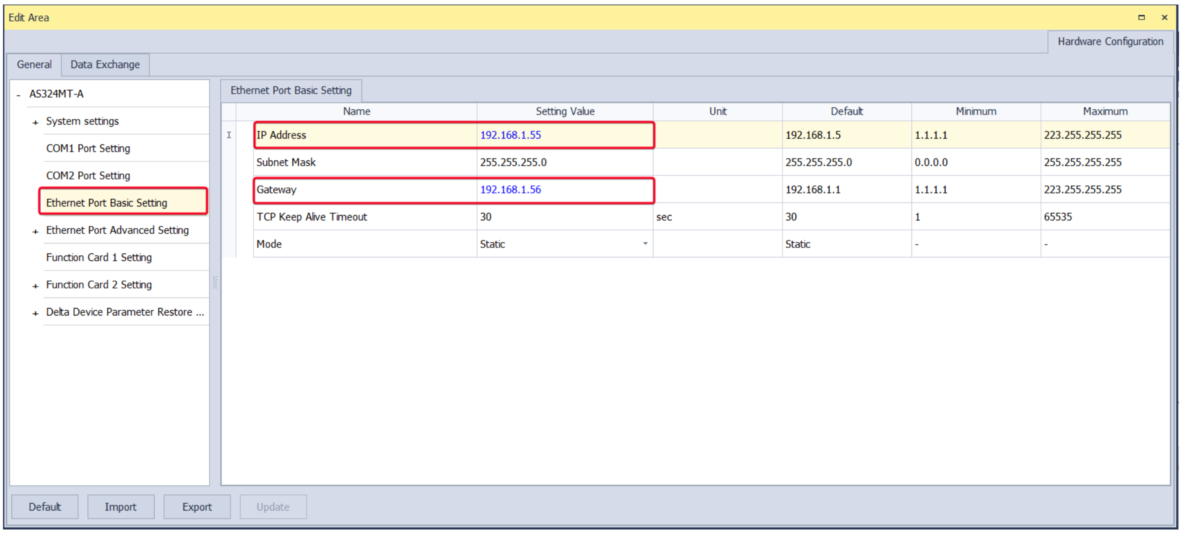


ID	Service Name	Protocol	Public Port	Server Port	Server IP Address	
1	PLC1	TCP/UDP	78:78	502:502	192.168.1.55	Edit | Delete
2	PLC2	TCP/UDP	77:77	502:502	192.168.1.5	Edit | Delete

PLC Configuration

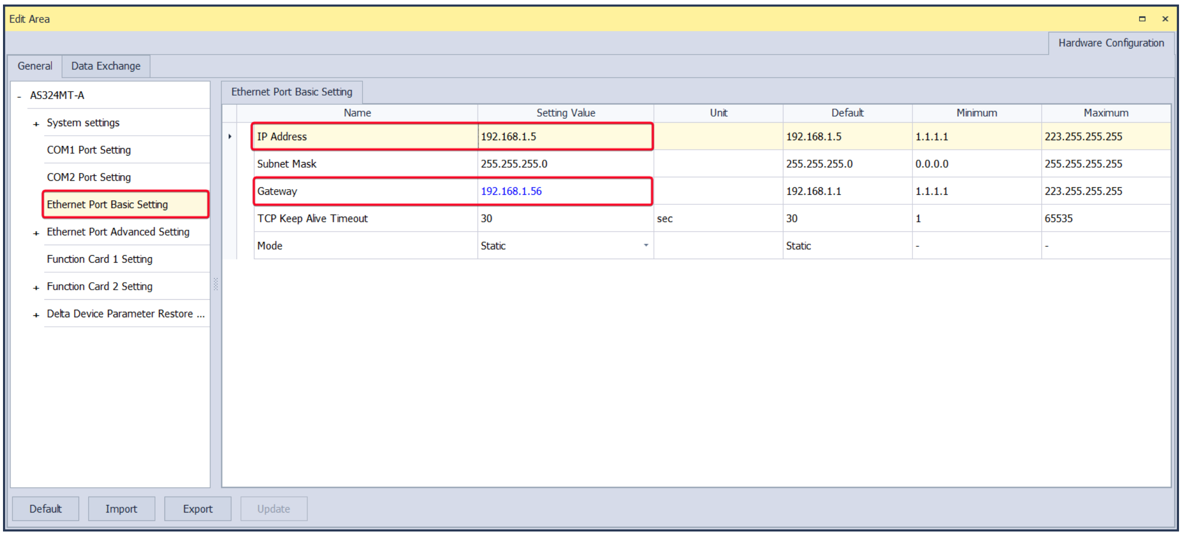
Use ISPSoft to change the IP addresses of Delta PLC1/2 to 192.168.1.55 and 192.168.1.56, with a gateway address of 192.168.1.56.

PLC1:



Name	Setting Value	Unit	Default	Minimum	Maximum
IP Address	192.168.1.55		192.168.1.5	1.1.1.1	223.255.255.255
Subnet Mask	255.255.255.0		255.255.255.0	0.0.0.0	255.255.255.255
Gateway	192.168.1.56		192.168.1.1	1.1.1.1	223.255.255.255
TCP Keep Alive Timeout	30	sec	30	1	65535
Mode	Static		Static	-	-

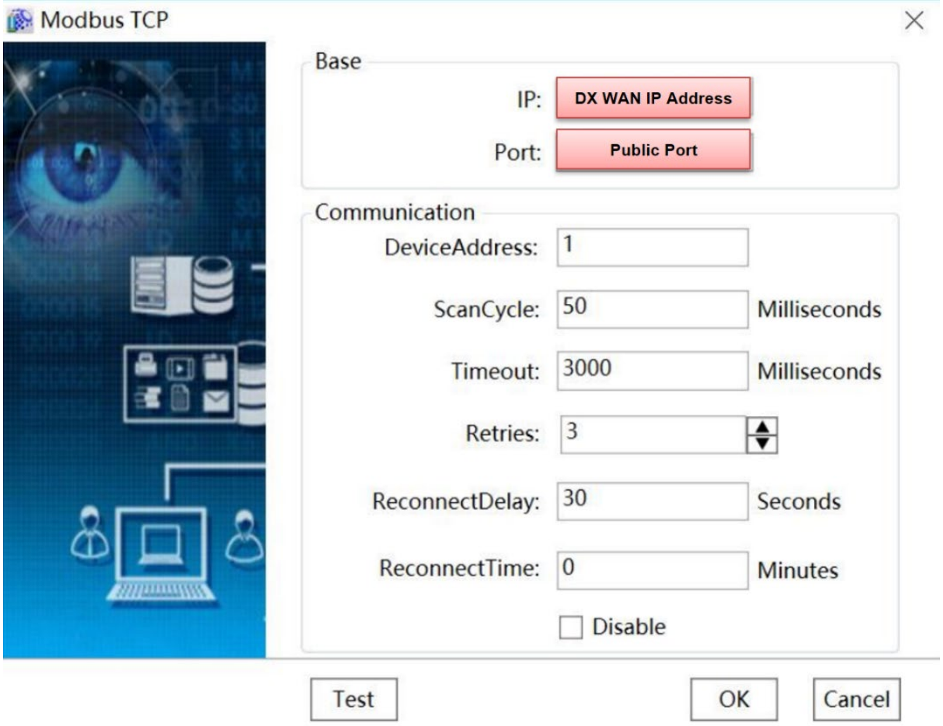
PLC2:



Name	Setting Value	Unit	Default	Minimum	Maximum
IP Address	192.168.1.5		192.168.1.5	1.1.1.1	223.255.255.255
Subnet Mask	255.255.255.0		255.255.255.0	0.0.0.0	255.255.255.255
Gateway	192.168.1.56		192.168.1.1	1.1.1.1	223.255.255.255
TCP Keep Alive Timeout	30	sec	30	1	65535
Mode	Static		Static	-	-

DIAView Configuration

1. Check whether the PC can connect to the internet.
2. Open DIAView, set the connection IP to the **DX WAN IP address: 192.168.2.1, set the port number to 77.** With the function enabled, the port forwarding function will forward packets to the destination device on LAN port with the IP address 192.168.1.5. Thus, the communication would be completed. To establish a connection with the device at 192.168.1.55, simply change the port to 78.



Modbus TCP

Base

IP: DX WAN IP Address

Port: Public Port

Communication

DeviceAddress: 1

ScanCycle: 50 Milliseconds

Timeout: 3000 Milliseconds

Retries: 3

ReconnectDelay: 30 Seconds

ReconnectTime: 0 Minutes

□ Disable

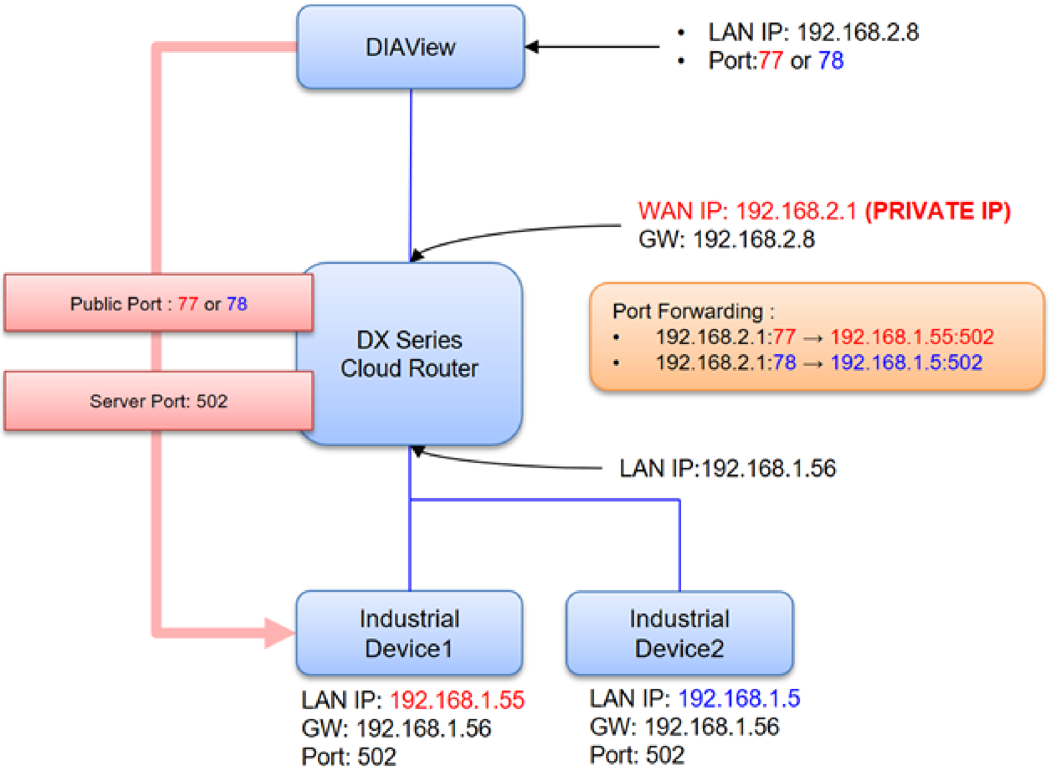
Notice

In case that the connection between DIAview and the PLC failed, please check whether the PC is connected to multiple networks at the same time. For example, both WiFi and LAN network are currently being used. Please turn off WiFi network and remain the LAN network connected to the cloud routers.

2.3.19 Port Trigger Private Network Application

DIAView utilizes private network to transmit data from the WAN port of the cloud router through Port 77 or 78, forwarding the data to the specified 502 Port and IP address under the LAN port, either to the PLC device at 192.168.1.5:502 or 192.168.1.55:502.

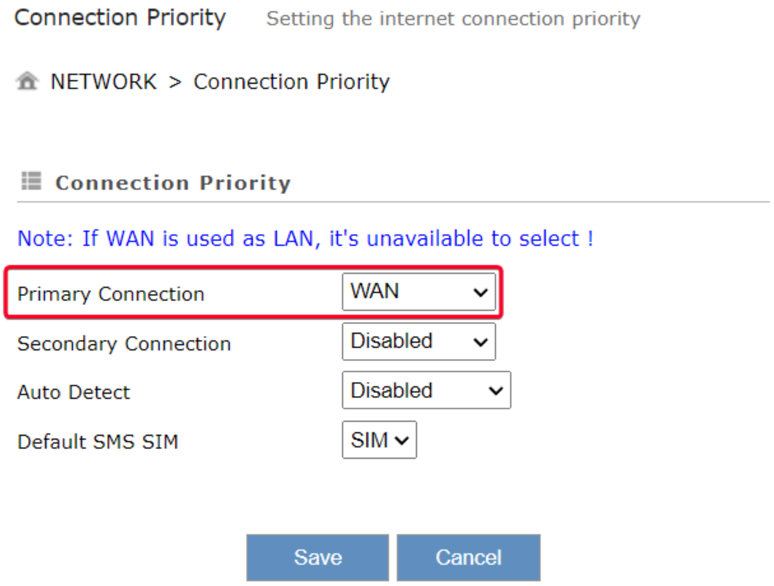
Please refer to Chapter 3.3.4 Port Trigger for a detailed explanation of the configuration parameters.



Cloud Router Configuration

1. Use a network cable to connect LAN ports on your PC and the DX router.
2. Login to DX cloud router using DIADevice. Account: admin / Password: admin.

3. Go to **Network** → **Connection**, choose **WAN** as **Primary Connection**, then click on “Save” and confirm the following items.


Connection Priority
Setting the internet connection priority
NETWORK > Connection Priority
Save
Cancel

Connection Priority

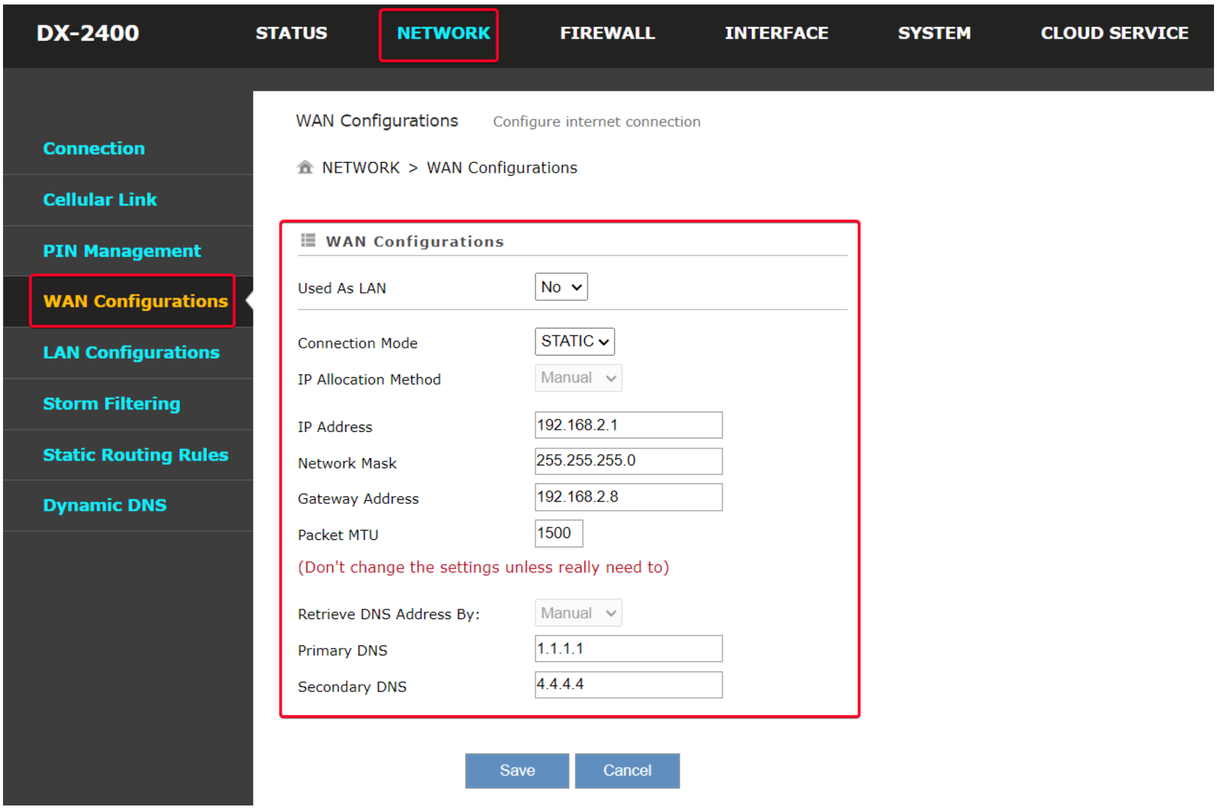
Note: If WAN is used as LAN, it's unavailable to select !

Primary Connection	WAN
Secondary Connection	Disabled
Auto Detect	Disabled
Default SMS SIM	SIM

a. Check whether the light of LINK/ACK on WAN port is on or not. If not, check the network cable is connected and functioning properly.

b. Check whether WAN IP address setting differs from LAN IP address.

4. Go to **NETWORK** → **WAN Configurations**, select **STATIC** as **Connection Mode**, enter the IP address information as shown below.



WAN Configurations

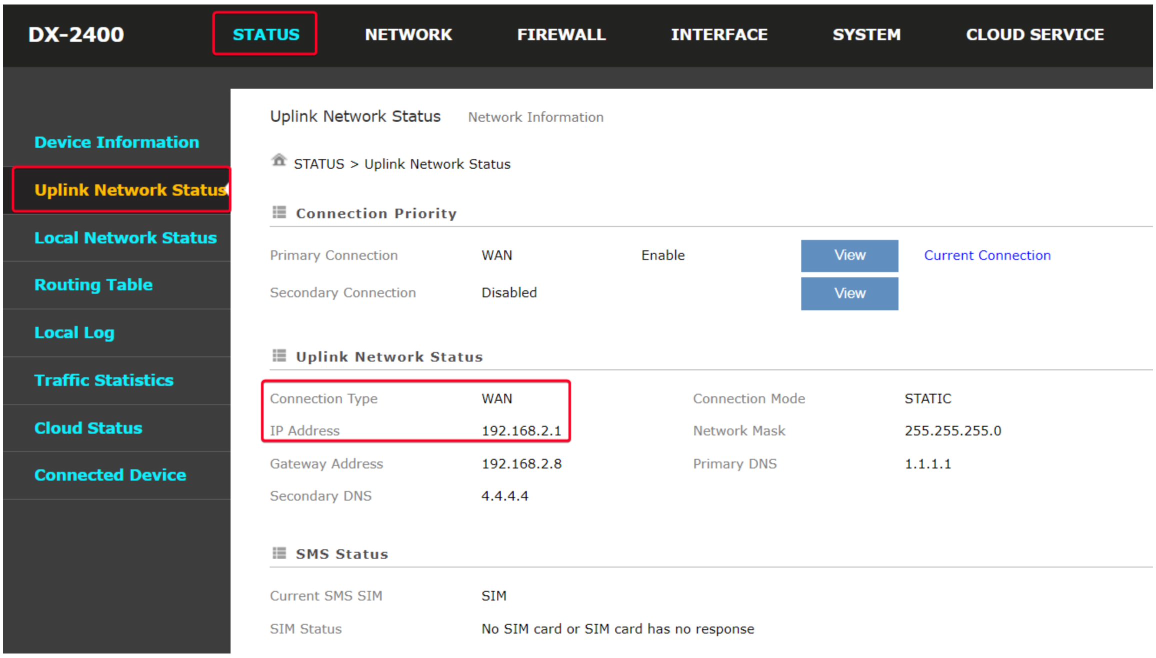
Used As LAN	No
Connection Mode	STATIC
IP Allocation Method	Manual
IP Address	192.168.2.1
Network Mask	255.255.255.0
Gateway Address	192.168.2.8
Packet MTU	1500

(Don't change the settings unless really need to)

Retrieve DNS Address By:	Manual
Primary DNS	1.1.1.1
Secondary DNS	4.4.4.4

5. Go to **STATUS** → **Uplink Networks Status** → **Primary Connection** and click on **View.**

> **Notice**
>
> ⚠ If a private IP address is obtained = 192.168.x.x(Class A)、172.16.x.x(Class B)、10.x.x.x(Class C), it will not be possible to establish a connection from the public network.



Connection Priority

Primary Connection	WAN	Enable	View
Secondary Connection	Disabled		View

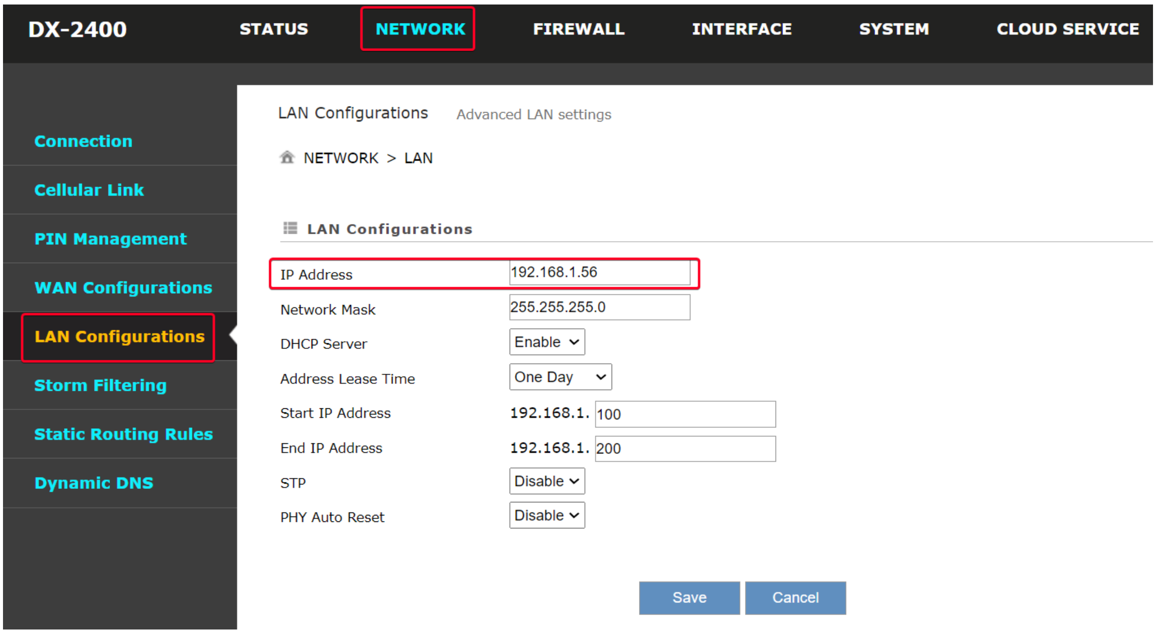
Uplink Network Status

Connection Type	WAN	Connection Mode	STATIC
IP Address	192.168.2.1	Network Mask	255.255.255.0
Gateway Address	192.168.2.8	Primary DNS	1.1.1.1
Secondary DNS	4.4.4.4		

SMS Status

Current SMS SIM	SIM
SIM Status	No SIM card or SIM card has no response

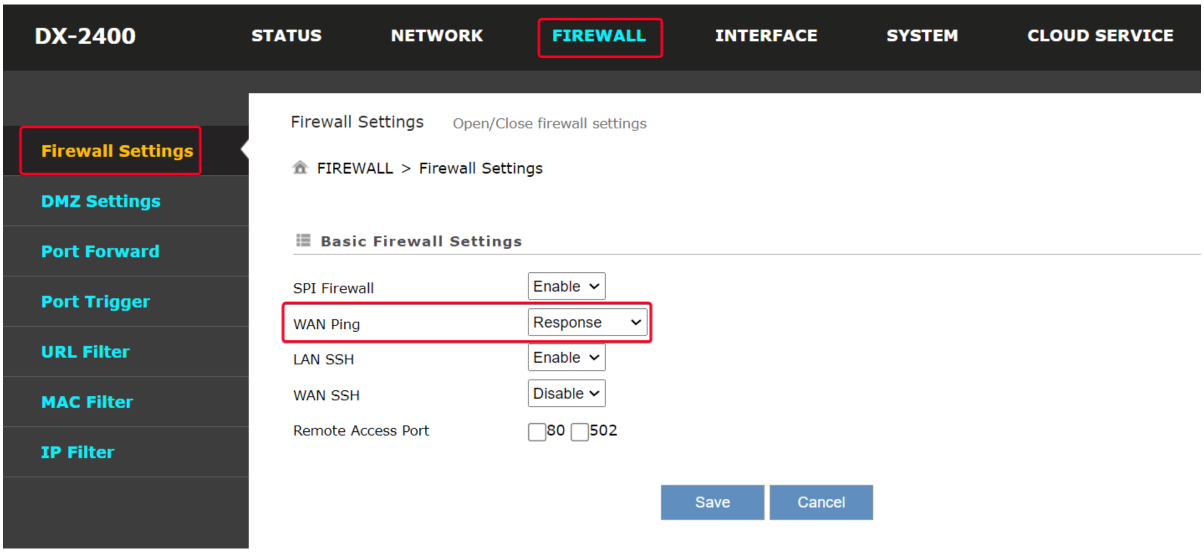
6. Go to **NETWORK** → **LAN Configuration**, the information of IP configuration is shown below. Please note that the LAN port IP segment should not be the same as the WAN port segment.



LAN Configurations

IP Address	192.168.1.56
Network Mask	255.255.255.0
DHCP Server	Enable
Address Lease Time	One Day
Start IP Address	192.168.1. 100
End IP Address	192.168.1. 200
STP	Disable
PHY Auto Reset	Disable

7. Go to **FIREWALL** → **Firewall Settings** and set **WAN Ping** to **Response**.



Firewall Settings Open/Close firewall settings

FIREWALL > Firewall Settings

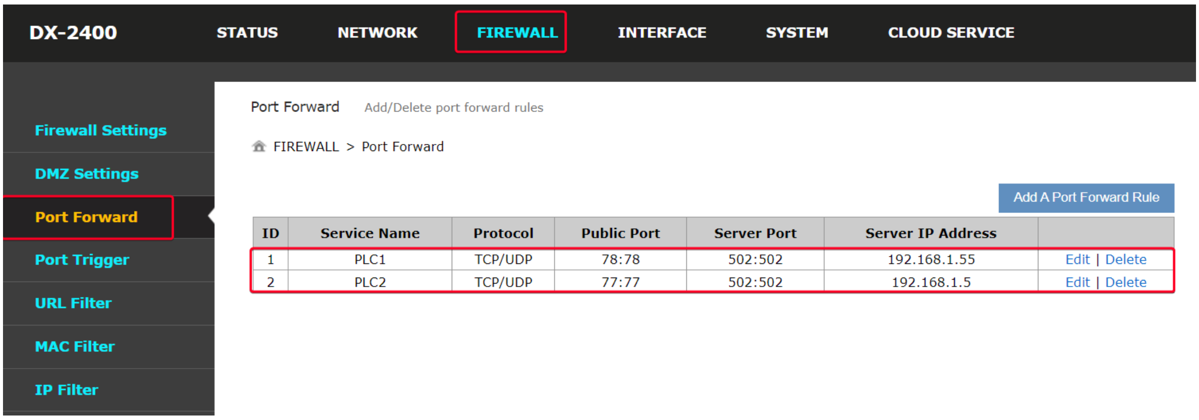
Basic Firewall Settings

SPI Firewall	Enable
WAN Ping	Response
LAN SSH	Enable
WAN SSH	Disable
Remote Access Port	□80 □502

8. Go to **FIREWALL** → **Port Forward,** click on **Add a Port Forward Rule.**

ID1: Triggers port 78 from external network to forward data to internal IP: 192.168.1.55:502.

ID2: Triggers port 77 from external network to forward data to internal IP: 192.168.1.5:502.



Port Forward Add/Delete port forward rules

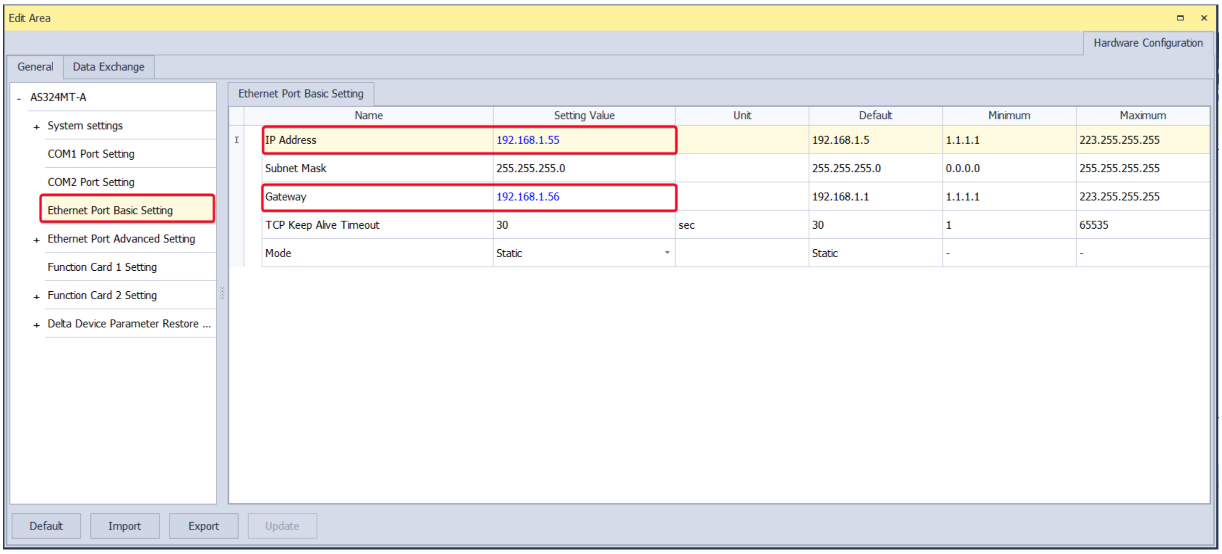
FIREWALL > Port Forward

ID	Service Name	Protocol	Public Port	Server Port	Server IP Address	
1	PLC1	TCP/UDP	78:78	502:502	192.168.1.55	Edit | Delete
2	PLC2	TCP/UDP	77:77	502:502	192.168.1.5	Edit | Delete

PLC Configuration

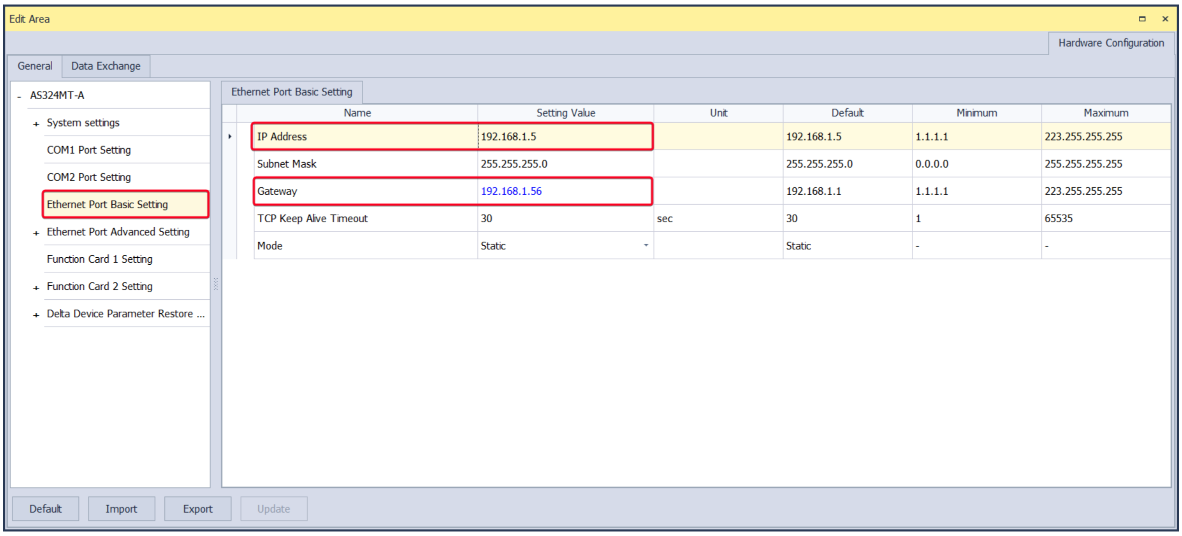
Use ISPSoft to change the IP addresses of Delta PLC1/2 to 192.168.1.55 and 192.168.1.56, with a gateway address of 192.168.1.56.

PLC1:



Name	Setting Value	Unit	Default	Minimum	Maximum
IP Address	192.168.1.55		192.168.1.5	1.1.1.1	223.255.255.255
Subnet Mask	255.255.255.0		255.255.255.0	0.0.0.0	255.255.255.255
Gateway	192.168.1.56		192.168.1.1	1.1.1.1	223.255.255.255
TCP Keep Alive Timeout	30	sec	30	1	65535
Mode	Static		Static	-	-

PLC2:

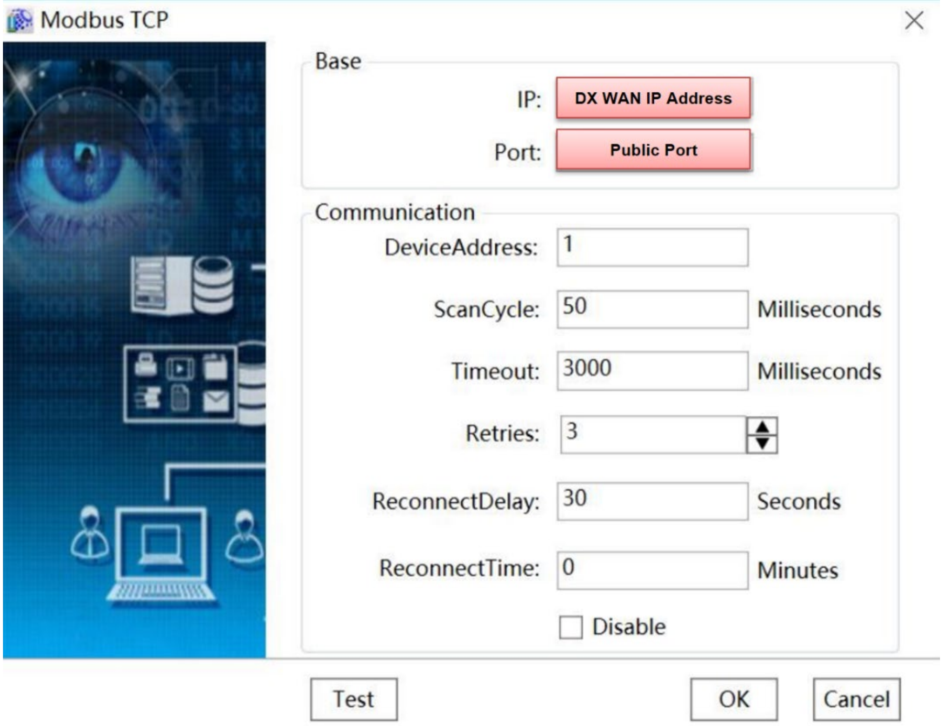


Name	Setting Value	Unit	Default	Minimum	Maximum
IP Address	192.168.1.5		192.168.1.5	1.1.1.1	223.255.255.255
Subnet Mask	255.255.255.0		255.255.255.0	0.0.0.0	255.255.255.255
Gateway	192.168.1.56		192.168.1.1	1.1.1.1	223.255.255.255
TCP Keep Alive Timeout	30	sec	30	1	65535
Mode	Static		Static	-	-

DIAView Configuration

1. Check whether the PC can connect to the internet.

2. Open DIAView, set the connection IP to the **DX WAN IP address: 192.168.2.1, set the port number to 77**. With the function enabled, the port forwarding function will forward packets to the destination device on LAN port with the IP address 192.168.1.5. Thus, the communication would be completed. To establish a connection with the device at 192.168.1.55, simply change the port to 78.



Modbus TCP

Base

IP: DX WAN IP Address

Port: Public Port

Communication

DeviceAddress: 1

ScanCycle: 50 Milliseconds

Timeout: 3000 Milliseconds

Retries: 3

ReconnectDelay: 30 Seconds

ReconnectTime: 0 Minutes

☐ Disable

Notice

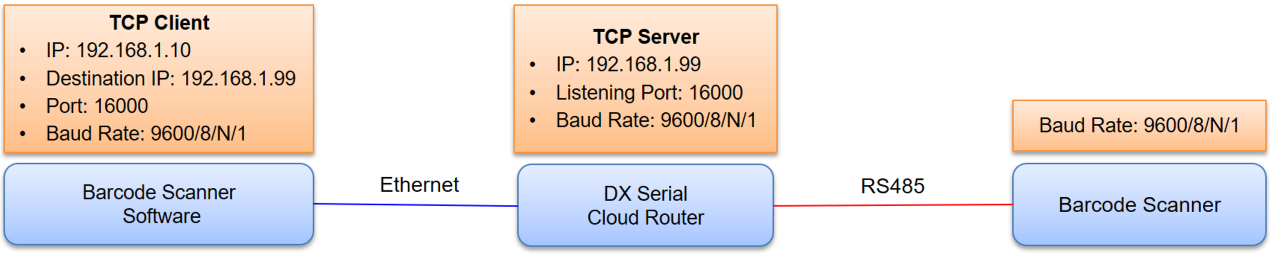
In case that the connection between DIAview and the PLC failed, please check whether the PC is connected to multiple networks at the same time. For example, both WiFi and LAN network are currently being used. Please turn off WiFi network and remain the LAN network connected to the cloud routers.

2.3.20 Serial Server TCP Server Application

Example

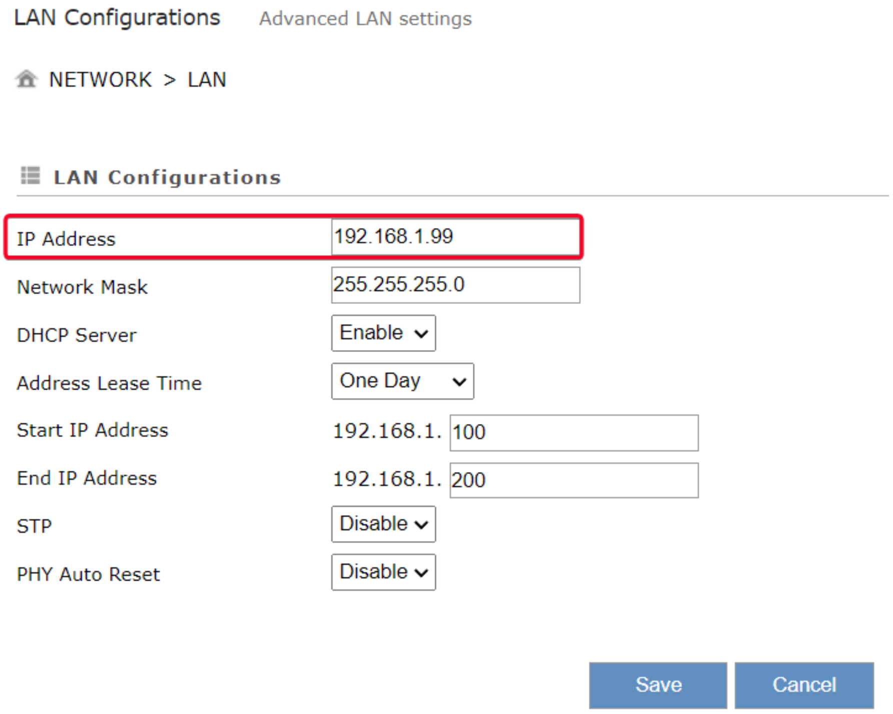
By utilizing the cloud router's TCP Server mode, the Barcode Scanner Software (acting as the TCP client) is enabled to perform bi-directional data exchange with Barcode Scanner devices.

Please refer to Chapter 3.4.1.5 Serial Server-TCP Server for a detailed explanation of the configuration parameters.



Setup Steps

1. Login to the cloud router, go to **NETWORK → LAN Configuration**, set the **IP Address: 192.168.1.99**.



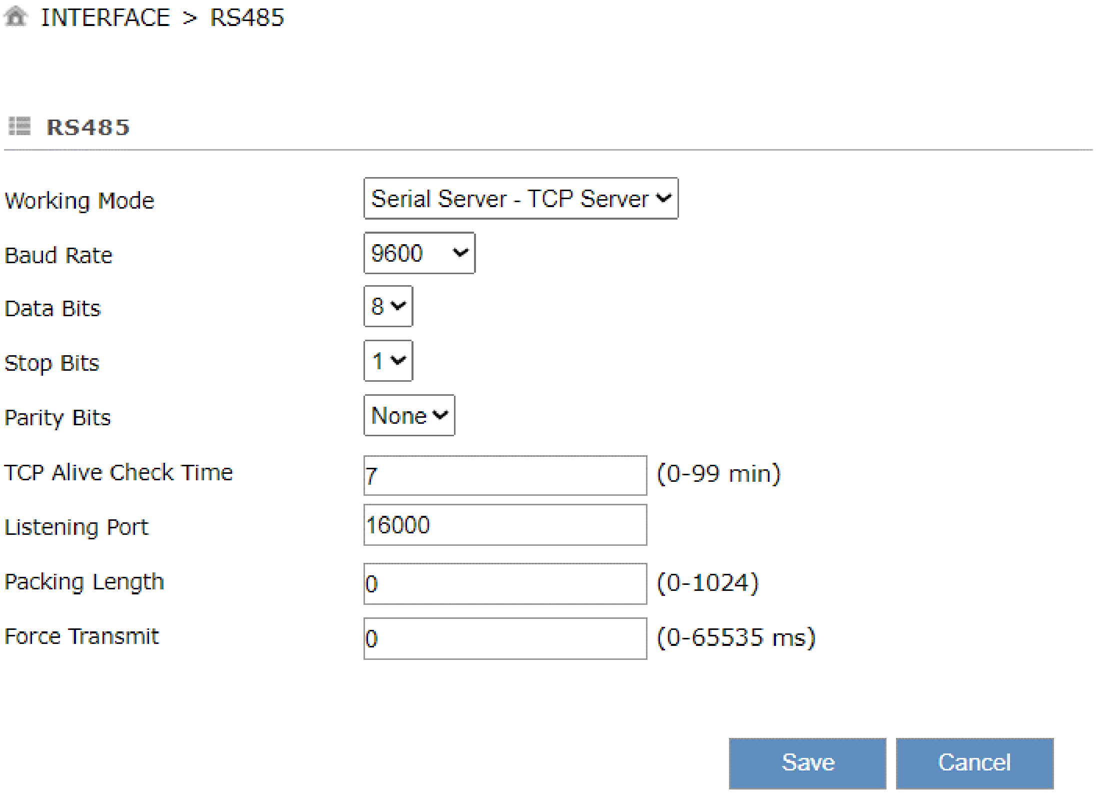
IP Address	192.168.1.99
Network Mask	255.255.255.0
DHCP Server	Enable
Address Lease Time	One Day
Start IP Address	192.168.1. 100
End IP Address	192.168.1. 200
STP	Disable
PHY Auto Reset	Disable

2. Go to **SYSTEM→ RS485**, configuration as follows:

   a) **Working Mode:** Serial Server-TCP Server

   b) **Baud Rate:** Configure to9600/8/N/1; same as setting for Barcode Scanner.

   c) **Listening Port:** 16000



INTERFACE > RS485

RS485

Working Mode	Serial Server - TCP Server	
Baud Rate	9600	
Data Bits	8	
Stop Bits	1	
Parity Bits	None	
TCP Alive Check Time	7	(0-99 min)
Listening Port	16000	
Packing Length	0	(0-1024)
Force Transmit	0	(0-65535 ms)

3. The TCP client device connects to the cloud router with IP: 192.168.1.99 / Port: 16000, to initiate data transmission.

4. If the Serial Device applied self-defined protocol, the TCP client will either need the manufacturer to provide a corresponding barcode scanner connection software tool, or it will require independent development.

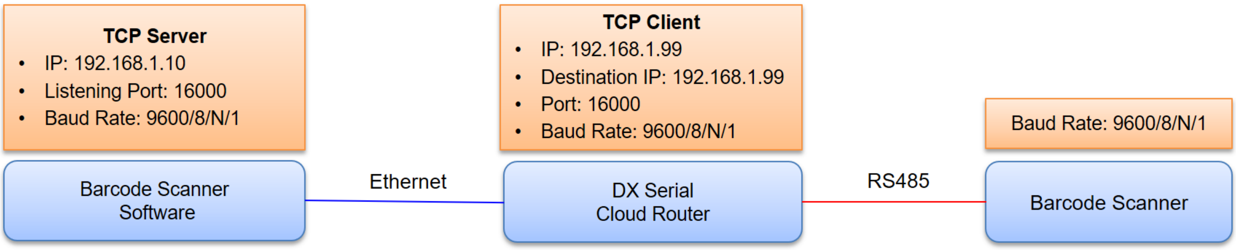
5. If data transmission failed, you can adjust the **Force Transmit** to 1000ms so as to slow down the speed of data transmission, then test again.

2.3.21 Serial Server-TCP Client Application

Example

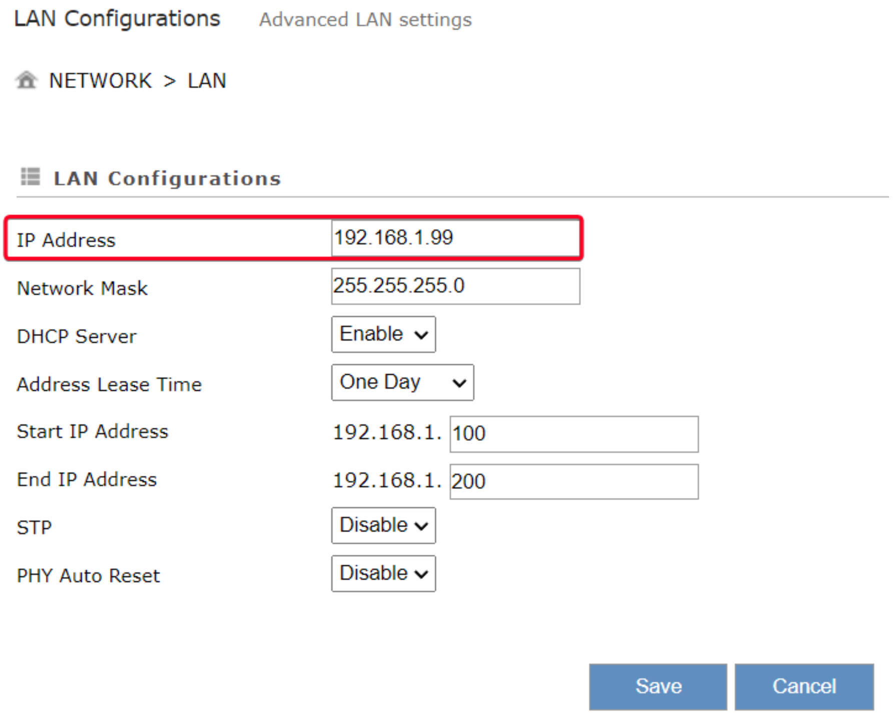
By utilizing the cloud router's TCP Client mode, allowing the Third-party software for Barcode Scanner (acting as the TCP Server) to perform bi-directional data exchange with Barcode Scanner devices.

Please refer to Chapter 3.4.1.6 Serial Server-TCP Client for a detailed explanation of the configuration parameters.



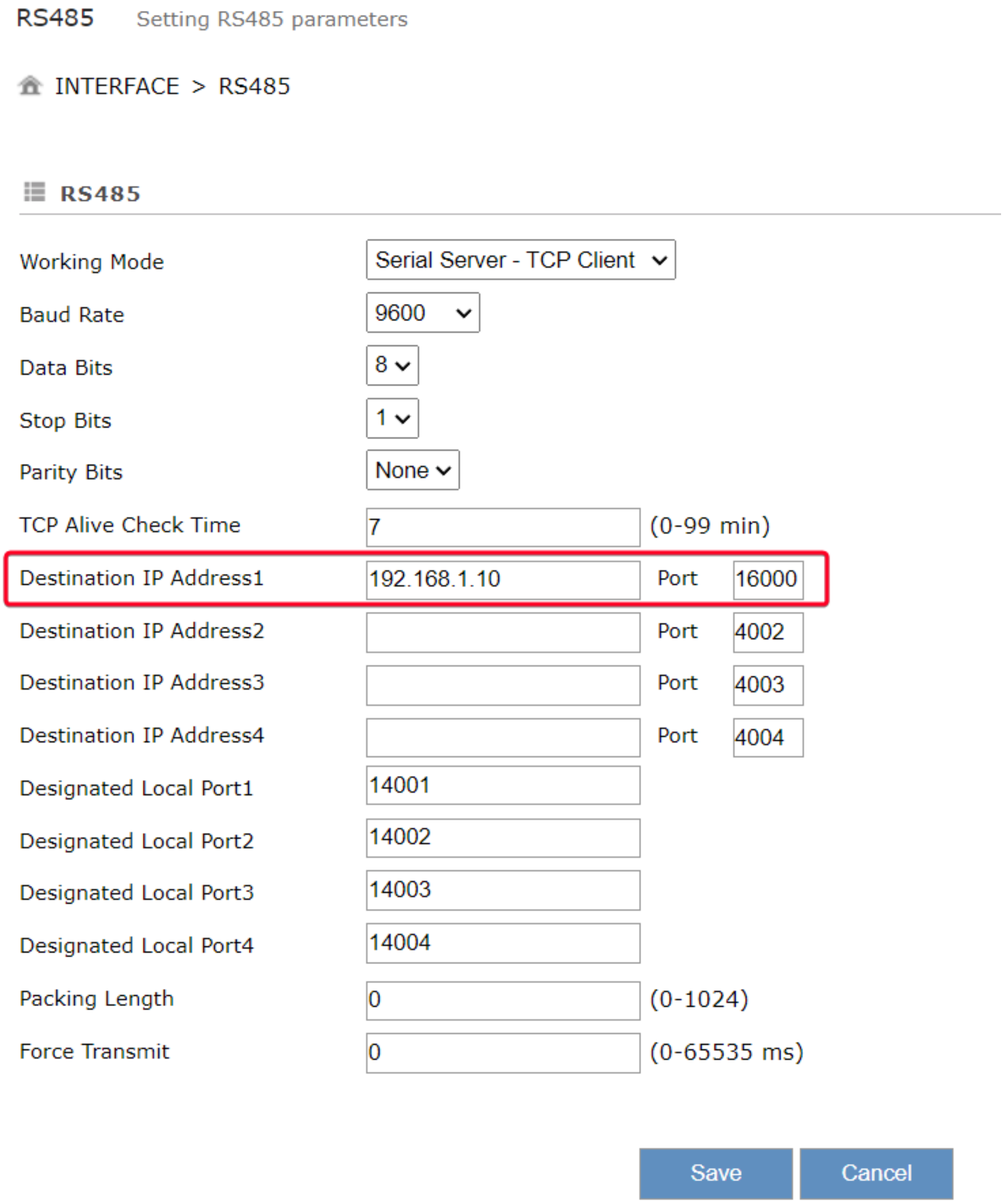
Setup Steps

1. Login to the cloud router, go to **NETWORK** → **LAN Configuration,** set the **IP Address: 192.168.1.99.**



IP Address	192.168.1.99
Network Mask	255.255.255.0
DHCP Server	Enable
Address Lease Time	One Day
Start IP Address	192.168.1. 100
End IP Address	192.168.1. 200
STP	Disable
PHY Auto Reset	Disable

2. Go to **SYSTEM→ RS485**, configuration as follows:
   a) **Working Mode:** Serial Server-TCP Client
   b) **Baud Rate:** Configure to 9600/8/N/1; same as setting for Barcode Scanner.
   c) **Listening Port:** 16000



RS485 Setting RS485 parameters

INTERFACE > RS485

RS485

Working Mode	Serial Server - TCP Client		
Baud Rate	9600		
Data Bits	8		
Stop Bits	1		
Parity Bits	None		
TCP Alive Check Time	7	(0-99 min)	
Destination IP Address1	192.168.1.10	Port	16000
Destination IP Address2		Port	4002
Destination IP Address3		Port	4003
Destination IP Address4		Port	4004
Designated Local Port1	14001		
Designated Local Port2	14002		
Designated Local Port3	14003		
Designated Local Port4	14004		
Packing Length	0	(0-1024)	
Force Transmit	0	(0-65535 ms)	

3. The TCP client device connects to the cloud router (TCP Server) with IP: 192.168.1.99 / Port: 16000, to initiate data transmission.

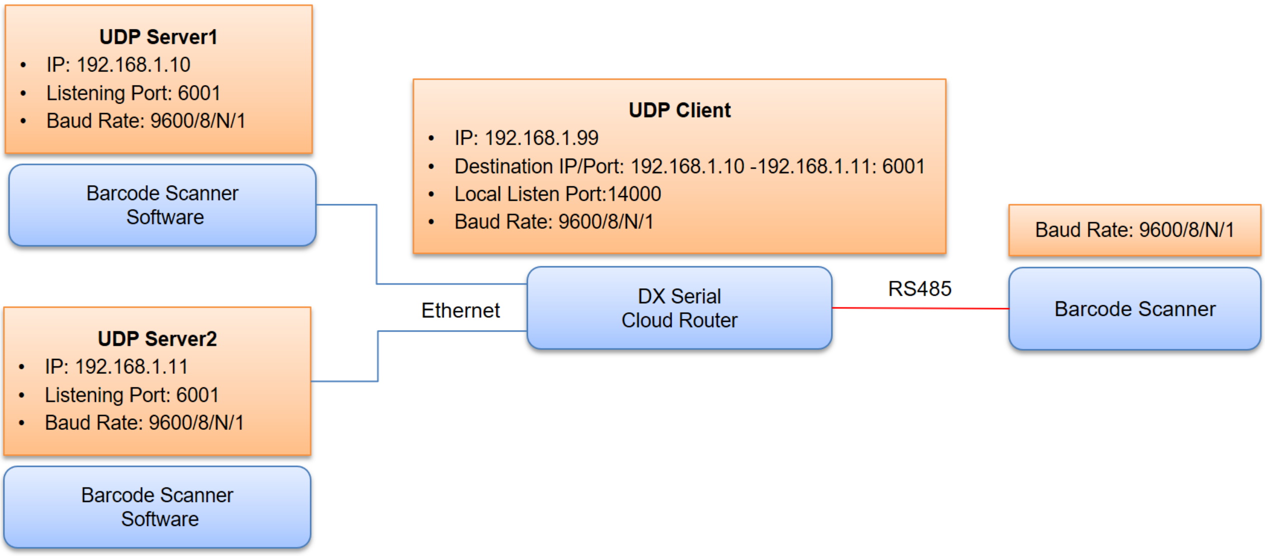
4. If the Serial Device applied self-defined protocol, the TCP server will either need the manufacturer to provide a corresponding barcode scanner connection software tool, or it will require independent development.

5. If data transmission failed, you can adjust the **Force Transmit** to 1000ms so as to slow down the speed of data transmission, then test again.

2.3.22 Serial Server-UDP Client Application

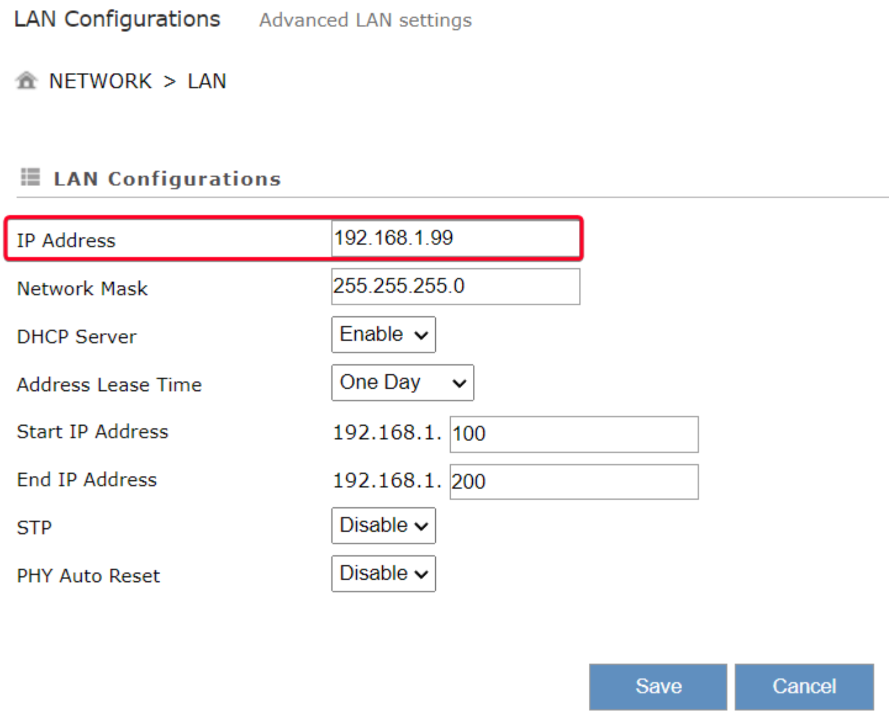
By utilizing the cloud router's UDP Client mode, allowing the Third-party software for Barcode Scanner (acting as the UDP Server) to perform bi-directional data exchange with Barcode Scanner devices.

Please refer to Chapter 3.4.1.7 Serial Server-UDP Client for a detailed explanation of the configuration parameters.



Setup Steps

1. Login to the cloud router, go to **NETWORK → LAN Configuration,** set the **IP Address: 192.168.1.99.**



LAN Configurations

IP Address	192.168.1.99
Network Mask	255.255.255.0
DHCP Server	Enable
Address Lease Time	One Day
Start IP Address	192.168.1. 100
End IP Address	192.168.1. 200
STP	Disable
PHY Auto Reset	Disable

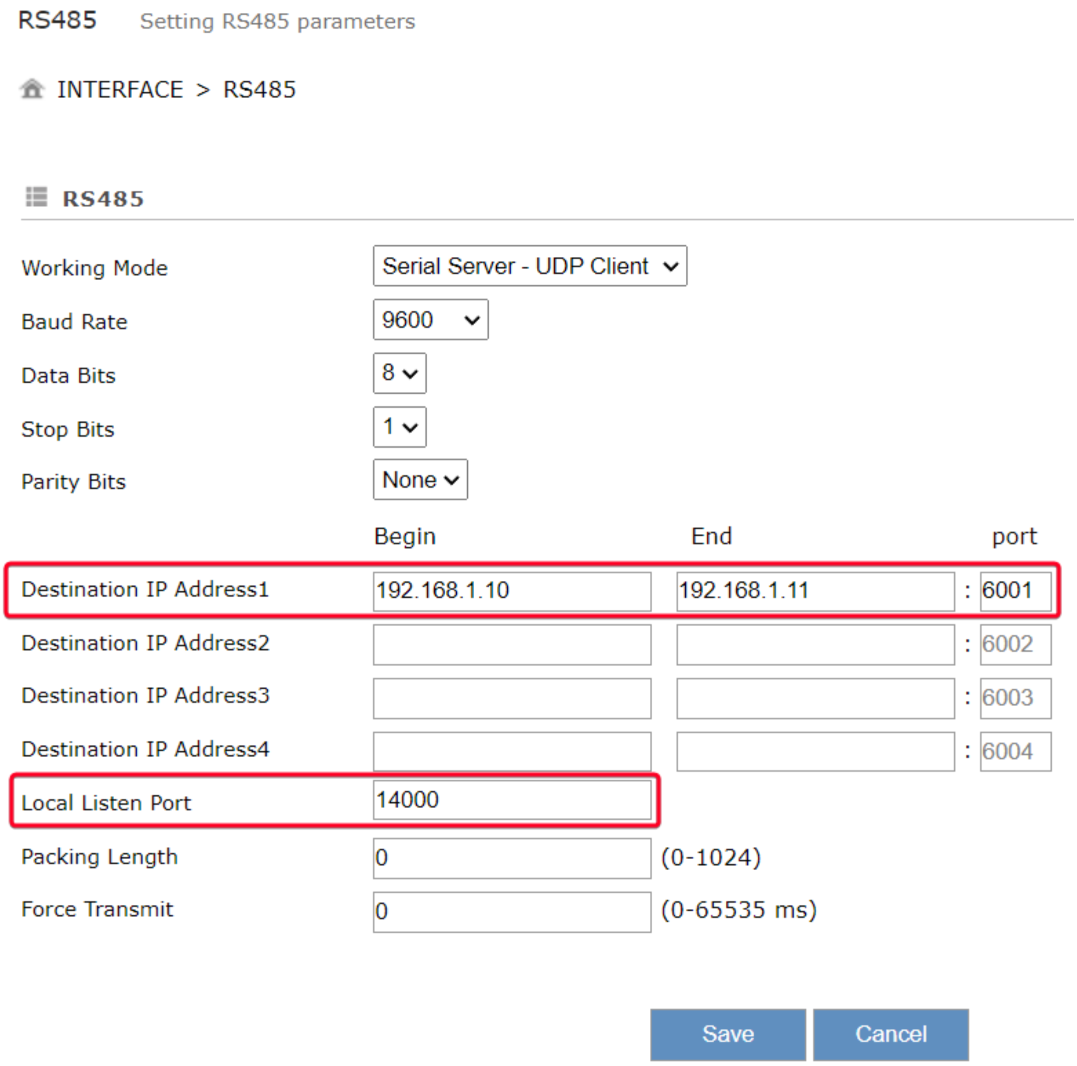
2. Go to **SYSTEM**→ **RS485**, configuration as follows:

    a) **Working Mode:** Serial Server-UDP Client

    b) **Baud Rate:** Configure to 9600/8/N/1, same as setting for Barcode Scanner

    c) **Port:** 6001

    d) **Local Listen Port:** 14000



RS485 Setting RS485 parameters

INTERFACE > RS485

RS485

Working Mode	Serial Server - UDP Client		
Baud Rate	9600		
Data Bits	8		
Stop Bits	1		
Parity Bits	None		
	Begin	End	port
Destination IP Address1	192.168.1.10	192.168.1.11	: 6001
Destination IP Address2			: 6002
Destination IP Address3			: 6003
Destination IP Address4			: 6004
Local Listen Port	14000		
Packing Length	0	(0-1024)	
Force Transmit	0	(0-65535 ms)	

3. Configure UDP Server 1 and UDP Server 2 to use port 6001 for connection, and you can start transmitting with the UDP client.

4. If the Serial Device applied self-defined protocol, the UDP server will either need the manufacturer to provide a corresponding TCP/UDP connection software tool, or it will require independent development.

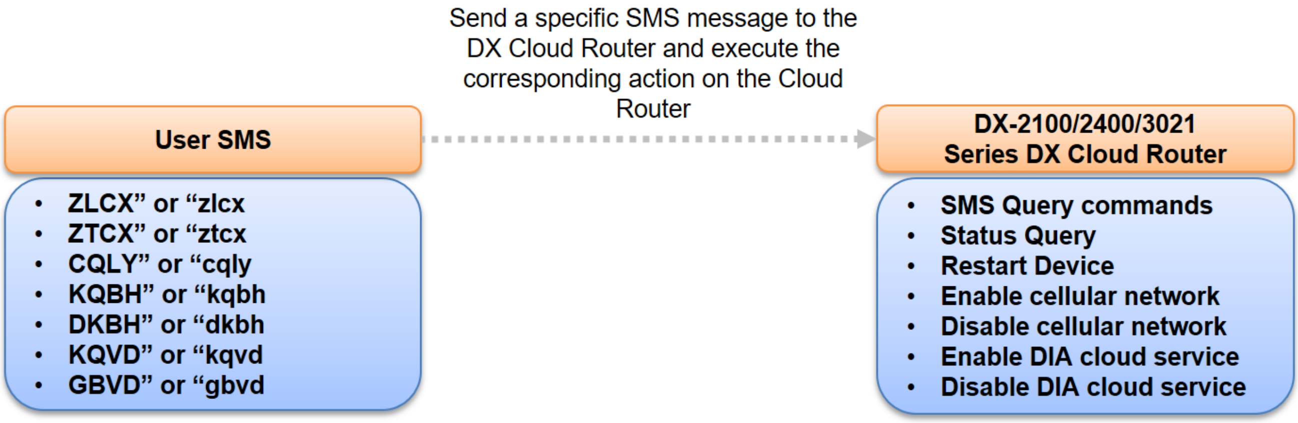
5. If data transmission failed, you can adjust the **Force Transmit** to 1000ms so as to slow down the speed of data transmission, then test again.

6. If the UDP server needs to establish a reverse connection with the UDP client, the port should be set to **Local Listen Port: 14000** for the connection to be established.

2.3.23 Short Message Control Router Application

Send short messages of commands from your mobile to the DX router for it to perform specific actions.

Please refer to Chapter 3.5.10 Privilege Management for a detailed explanation of the configuration parameters.



Send a specific SMS message to the DX Cloud Router and execute the corresponding action on the Cloud Router

User SMS

- **ZLCX" or "zlcx**
- **ZTCX" or "ztcx**
- **CQLY" or "cqly**
- **KQBH" or "kqbh**
- **DKBH" or "dkbh**
- **KQVD" or "kqvd**
- **GBVD" or "gbvd**

DX-2100/2400/3021 Series DX Cloud Router

- **SMS Query commands**
- **Status Query**
- **Restart Device**
- **Enable cellular network**
- **Disable cellular network**
- **Enable DIA cloud service**
- **Disable DIA cloud service**

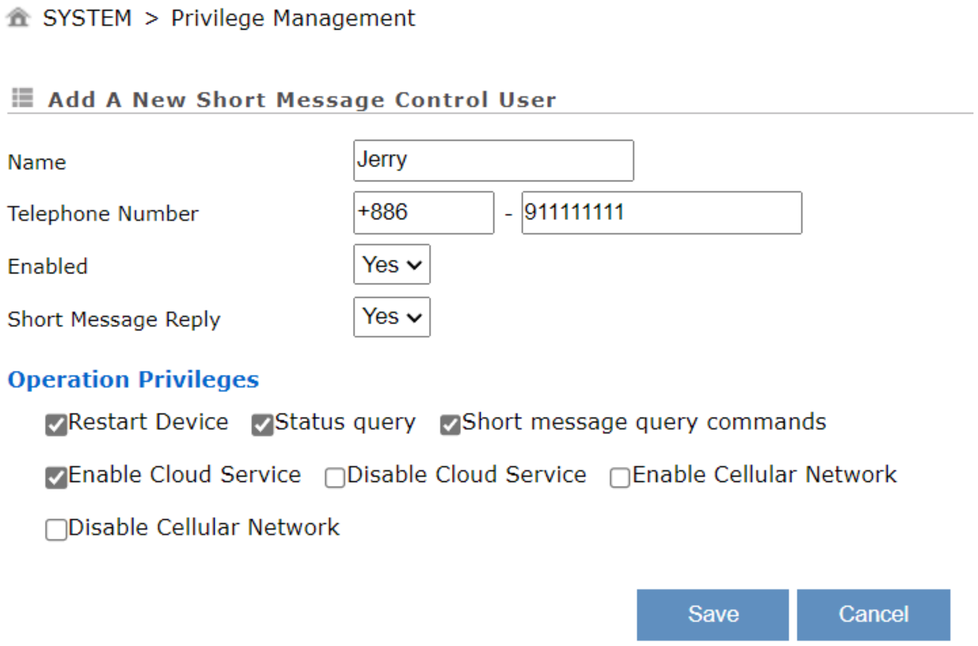
Setup Steps

1. Check the SIM card in the cloud router is capable of using the SMS function. Please refer to section **3.5.10.1 Send Short Message Test.**

2. Use your mobile to confirm that the SIM card number of the cloud router is +886922222222 and memorize this number.

3. Login to the cloud router device and go to **SYSTEM** → **Privilege Management**, then click on **Add A Telephone Number** under **Short Message Control Gateway**.

4. Configure telephone number and operation privileges, then click on **Save**.



SYSTEM > Privilege Management

Add A New Short Message Control User

Name	Jerry
Telephone Number	+886 - 911111111
Enabled	Yes
Short Message Reply	Yes

Operation Privileges

☑Restart Device ☑Status query ☑Short message query commands

☑Enable Cloud Service ☐Disable Cloud Service ☐Enable Cellular Network

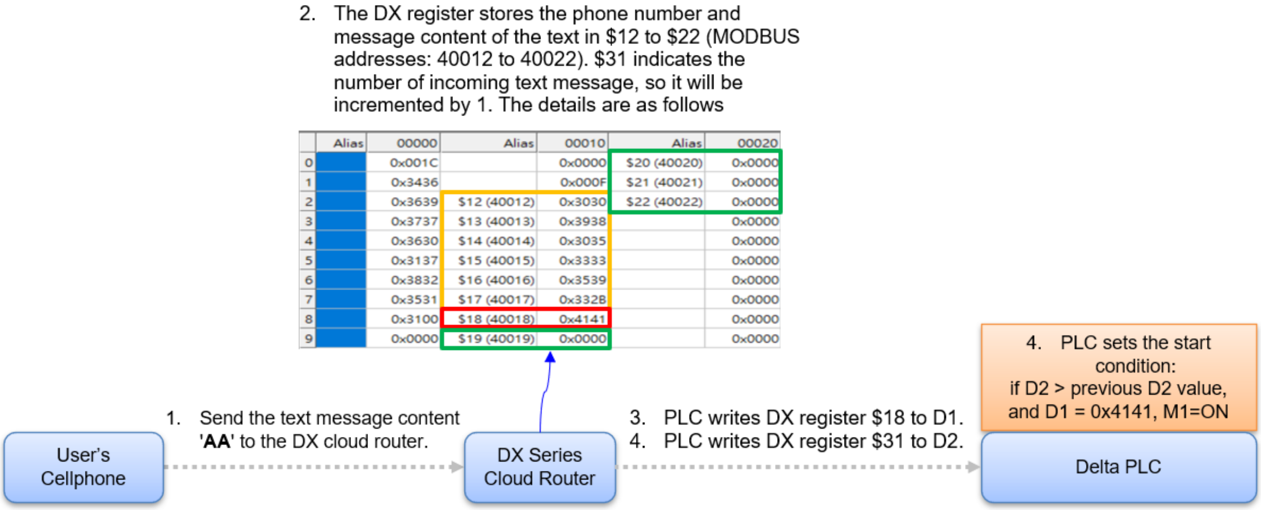
☐Disable Cellular Network

5. Based on the privilege settings, use the mobile phone(phone number: +886911111111) to send CQLY、KQVD、KQBH commands to the SIM card in the cloud router which the number is +88692222222, so as to control the cloud router's devices.

2.3.24 Short Message Control PLC Application

Send a text message with the content 'AA' from mobile phone to the DX Cloud Router to turn on PLC's M1. The process is as follows:

Please refer to Chapter 3.5.10 Privilege Management for a detailed explanation of the configuration parameters



2. The DX register stores the phone number and message content of the text in $12 to $22 (MODBUS addresses: 40012 to 40022). $31 indicates the number of incoming text message, so it will be incremented by 1. The details are as follows

	Alias	00000	Alias	00010	Alias	00020
0		0x001C		0x0000	$20 (40020)	0x0000
1		0x3436		0x000F	$21 (40021)	0x0000
2		0x3639	$12 (40012)	0x3030	$22 (40022)	0x0000
3		0x3737	$13 (40013)	0x3938		0x0000
4		0x3630	$14 (40014)	0x3035		0x0000
5		0x3137	$15 (40015)	0x3333		0x0000
6		0x3832	$16 (40016)	0x3539		0x0000
7		0x3531	$17 (40017)	0x332B		0x0000
8		0x3100	$18 (40018)	0x4141		0x0000
9		0x0000	$19 (40019)	0x0000		0x0000

1. Send the text message content **'AA'** to the DX cloud router.

3. PLC writes DX register $18 to D1.
4. PLC writes DX register $31 to D2.

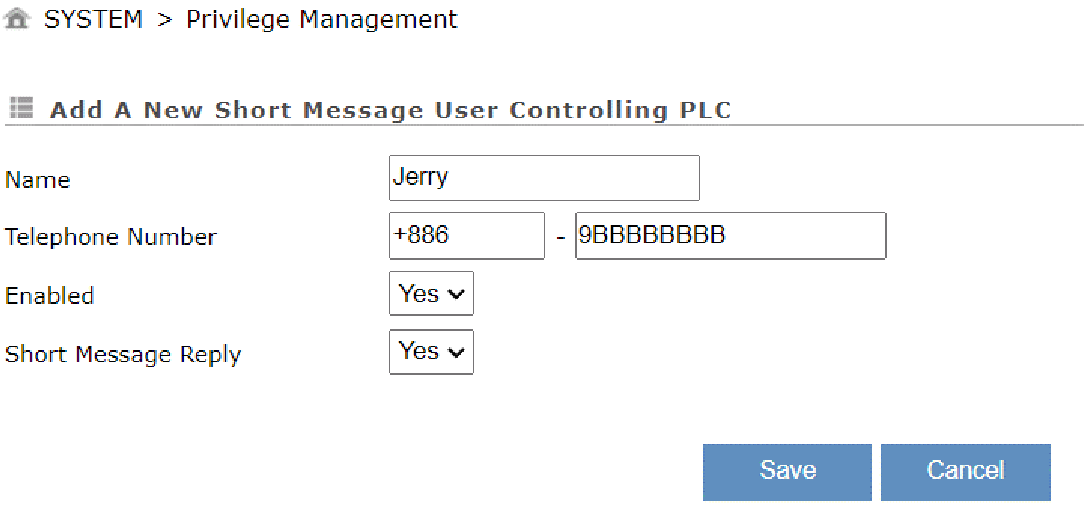
4. PLC sets the start condition: if D2 > previous D2 value, and D1 = 0x4141, M1=ON

1. Check the SIM card in the cloud router can use the SMS function. Please refer to section **3.5.10.1 Send Short Message Test.**

2. Use your mobile to confirm that the SIM card number of the cloud router is +8869AAAAAAAA and memorize this number.

3. Login to the cloud router device and go to **SYSTEM** → **Privilege Management**, then click on **Add A Telephone Number** under **Short Message Control PLC**

4. Add telephone numbers to control PLCs as shown below:



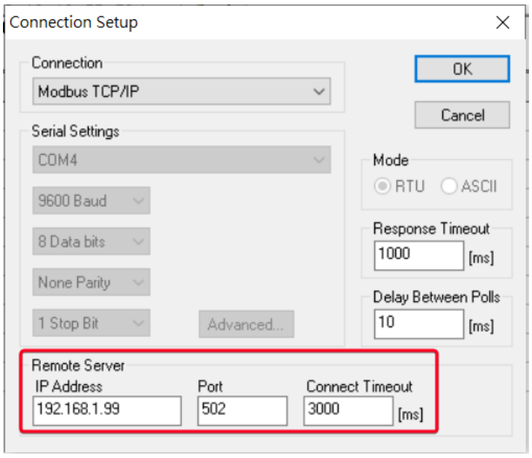
SYSTEM > Privilege Management

Add A New Short Message User Controlling PLC

Name	Jerry
Telephone Number	+886 - 9BBBBBBBB
Enabled	Yes
Short Message Reply	Yes

5. Use the mobile phone with the number +8869BBBBBBBB to send an SMS with the content "M1on" to the SIM card number of the cloud router, +8869AAAAAAAA.

6. Download the **Modbus Poll testing tool** and connect to the cloud router's IP address, 192.168.1.99, using MODBUS TCP/IP.



Connection Setup

Connection: Modbus TCP/IP

Serial Settings: COM4, 9600 Baud, 8 Data bits, None Parity, 1 Stop Bit, Advanced...

Mode: ● RTU ○ ASCII

Response Timeout: 1000 [ms]

Delay Between Polls: 10 [ms]

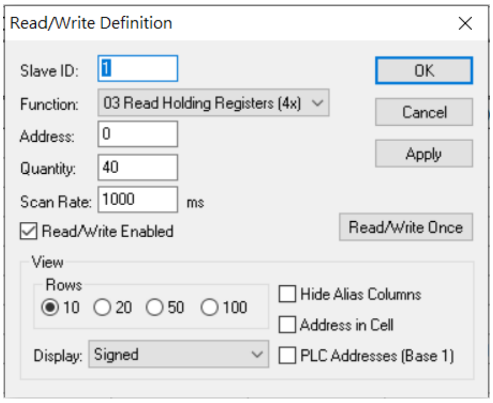
Remote Server

IP Address: 192.168.1.99

Port: 502

Connect Timeout: 3000 [ms]

7. When successfully connected, go to **Setup** → **Read/Write Definition**. Configure the settings as shown in the following figure, then click OK to start reading registers $0 - $30 in the cloud router.



Read/Write Definition

Slave ID: 1

Function: 03 Read Holding Registers (4x)

Address: 0

Quantity: 40

Scan Rate: 1000 ms

☑ Read/Write Enabled

View

Rows: ● 10 ○ 20 ○ 50 ○ 100

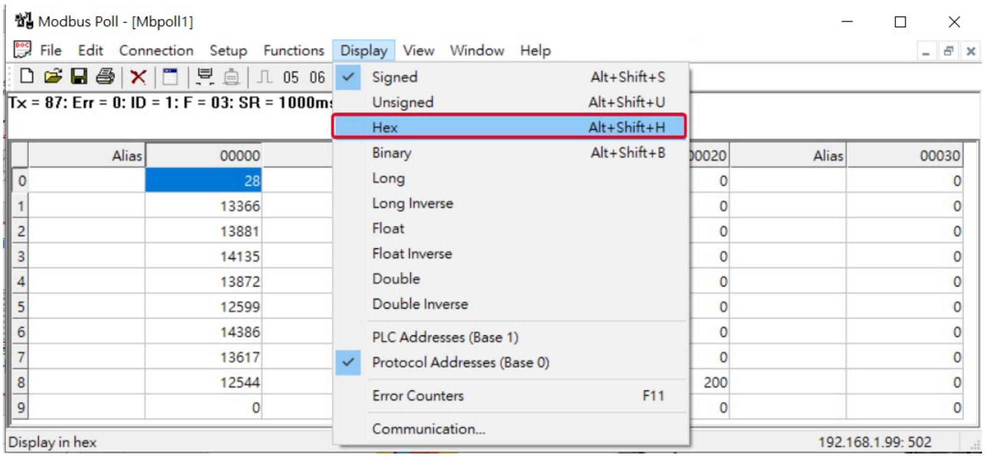
☐ Hide Alias Columns

☐ Address in Cell

☐ PLC Addresses (Base 1)

Display: Signed

8. Click Display and select HEX.



Modbus Poll - [Mbpoll1]

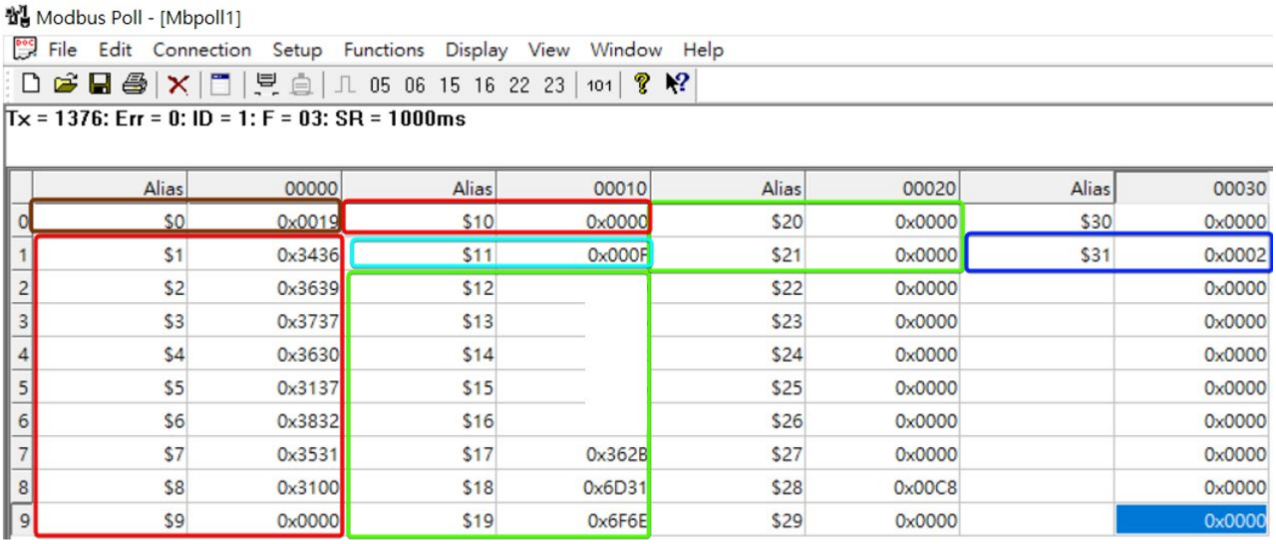
Tx = 87: Err = 0: ID = 1: F = 03: SR = 1000m:

	Alias	00000	00020	Alias	00030
0		28	0		0
1		13366	0		0
2		13881	0		0
3		14135	0		0
4		13872	0		0
5		12599	0		0
6		14386	0		0
7		13617	0		0
8		12544	200		0
9		0	0		0

Display in hex

192.168.1.99: 502

9. Send an SMS with the content "M1on" from the mobile phone number +8869BBBBBBBB and check the status displayed in Modbus Poll.


Modbus Poll - [Mbpoll1]
File Edit Connection Setup Functions Display View Window Help
05 06 15 16 22 23 101

Tx = 1376: Err = 0: ID = 1: F = 03: SR = 1000ms

	Alias	00000	Alias	00010	Alias	00020	Alias	00030
0	$0	0x0019	$10	0x0000	$20	0x0000	$30	0x0000
1	$1	0x3436	$11	0x000F	$21	0x0000	$31	0x0002
2	$2	0x3639	$12		$22	0x0000		0x0000
3	$3	0x3737	$13		$23	0x0000		0x0000
4	$4	0x3630	$14		$24	0x0000		0x0000
5	$5	0x3137	$15		$25	0x0000		0x0000
6	$6	0x3832	$16		$26	0x0000		0x0000
7	$7	0x3531	$17	0x362B	$27	0x0000		0x0000
8	$8	0x3100	$18	0x6D31	$28	0x00C8		0x0000
9	$9	0x0000	$19	0x6F6E	$29	0x0000		0x0000

10. Set the register data to be displayed in DEC or ASCII format as shown below, the red words below are the converted parameters.

a. 3/4GSignal Strength→25

Function	**3/4GSignal Strength**	
Register	**$0**	
	High	Low
HEX	00	19
DEC	00	**25**

b. Network Status→15

Function	**Network Status**	
Register	**$11**	
	High	Low
HEX	00	0F
DEC	00	**15**

c. Receiver's phone number+SMS messages: 09BBBBBBBB + M1on

Function	**Receiver's phone number+SMS messages**																			
Register	**$12**		**$13**		**$14**		**$15**		**$16**		**$17**		**$18**		**$19**		$20		$21	
	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low
HEX	30	30	39	XX	XX	XX	X	XX	X	XX	XX	2B	6D	31	6F	6E	00	00	00	00
ASCII	**0**	**0**	**9**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**+**	**m**	**1**	**o**	**n**	null	null	null	null

d. The number of received SMS messages: 2

Function	SMS message number	
Register	$31	
	High	Low
HEX	00	02
DEC	0	2

11. Check the messages: $18=6D、31，$19 =6F、6E(HEX)=M1on(ASCII)

12. Read the cloud router's registers $12~$19 and $31 into Delta PLC's D12~D19 and D31 in advance, as shown below.

Function	Receiver’s phone number+SMS messages															
Delta PLC Register	D12		D13		D14		D15		D16		D17		D18		D19	
Cloud router Register	$12		$13		$14		$15		$16		$17		$18		$19	
	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low
HEX	30	30	39	36	33	32	32	36	38	31	36	2B	6D	31	6F	6E
ASCII	0	0	9	6	3	2	2	6	8	1	6	+	m	1	o	n

Function	SMS message number	
Delta Register	D31	
Cloud router Register	$31	
	High	Low
HEX	00	02
DEC	0	2

13. The PLC program is designed as follows:

    a. The preset SMS message would be sent to execute certain actions, such asD18, D19=m1on=6D31, 6F6E (HEX).The PLC command should be set first that M1 would change to ON whenD18=6D31(HEX), D19=6F6E(HEX).The SMS content can be customized, as long as the PLC can interpret the value and execute the corresponding action.

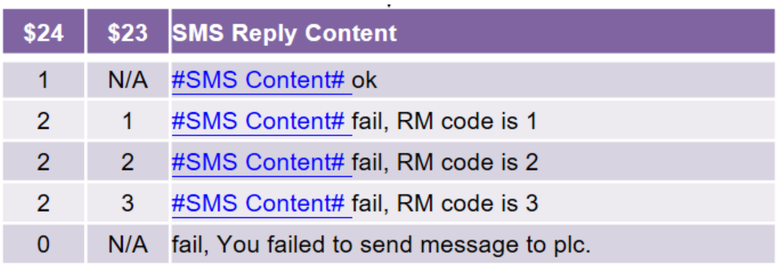
    b. When SMS is received, if $31 > D31, it can be determined that a new SMS has arrived. Begin reading the SMS content from D12 to D19 and execute the corresponding action. After execution, increment D31 by 1 and ensure that it is equal to $31.

    c. After executing the actions, the execution status should be reported back and written to the cloud router registers $23 and $24. Register $24 needs to be reset to 0 before the arrival of the next control SMS.

⚠ **Notice:**

Once the PLC completes the action and writes the result to $24, it needs to ensure that $24 is written to 0 before the arrival of the next control SMS (the simplest way is to compulsorily write 0 to $24 after two seconds). Failing to implement this action could result in incorrect SMS status in the subsequent cloud router reply.

14. The cloud router replies to the user with SMS content based on the contents of $23 and $24 as follows:

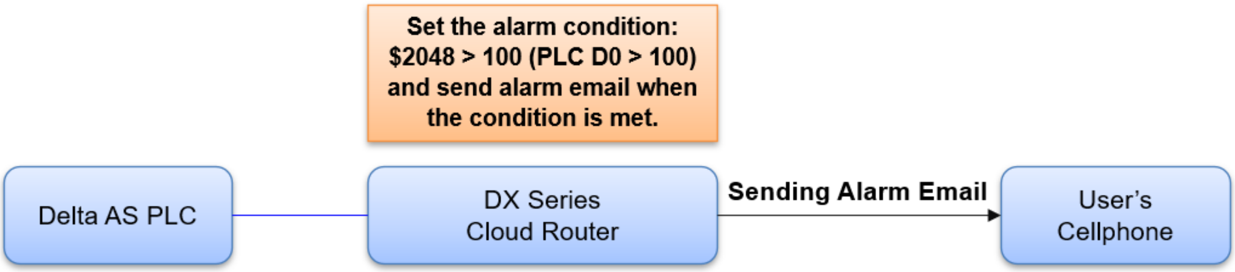


$24	$23	SMS Reply Content
1	N/A	#SMS Content# ok
2	1	#SMS Content# fail, RM code is 1
2	2	#SMS Content# fail, RM code is 2
2	3	#SMS Content# fail, RM code is 3
0	N/A	fail, You failed to send message to plc.

2.3.25 Alarm E-mail Sending Application

When the register D0 in the PLC is greater than 100, the alarm would be triggered and emails would be sent to users.

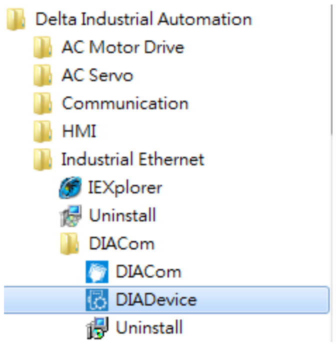
Please refer to Chapter 3.5.11 Event Management for a detailed explanation of the configuration parameters.



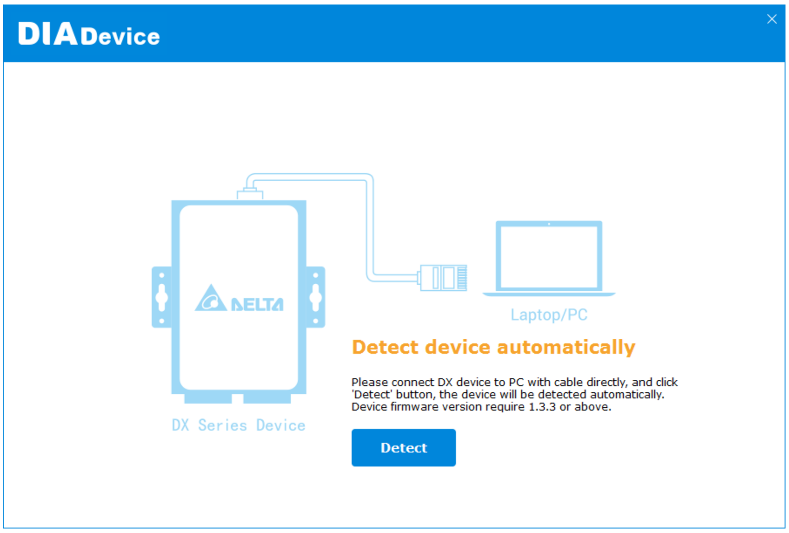
Set the alarm condition: $2048 > 100 (PLC D0 > 100) and send alarm email when the condition is met.

Setup Steps

1. Make sure that all **the basic configuration** detailed in Chapter 2 has been completed and functions properly.
2. Use a network cable to connect LAN ports on your PC and the DX router.
3. Install DIACom software, open DIADevice: Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice**.



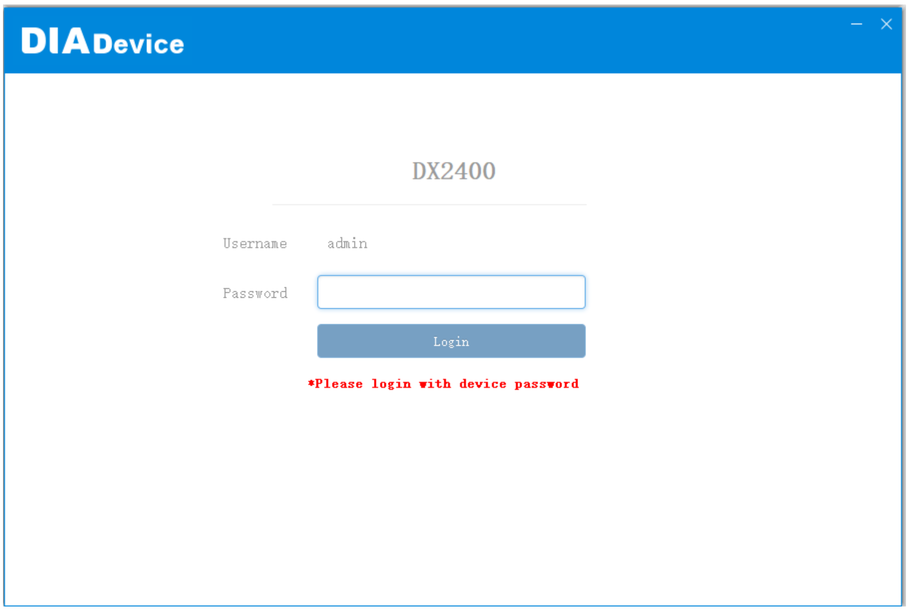
4. Click on **Detect**, and it will redirect to the login page of DX router.



Detect device automatically

Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically. Device firmware version require 1.3.3 or above.

5. Enter your account and password. (Default: admin/admin)



DIADevice

DX2400

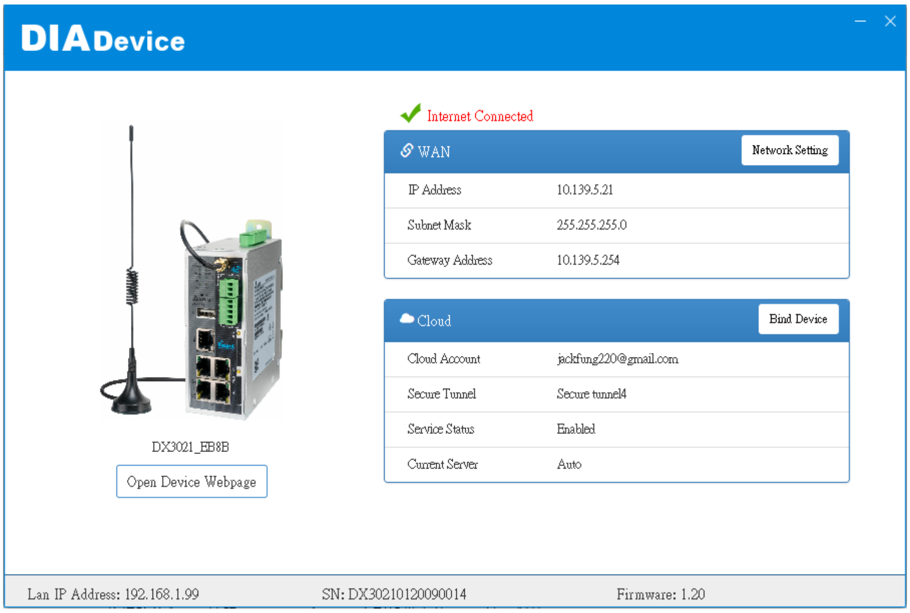
Username admin

Password

Login

*Please login with device password

6. Click on **Open Device Webpage** and verify that the bound IP address is 192.168.1.99.



DIADevice

Internet Connected

WAN — Network Setting

IP Address	10.139.5.21
Subnet Mask	255.255.255.0
Gateway Address	10.139.5.254

Cloud — Bind Device

Cloud Account	jackfung220@gmail.com
Secure Tunnel	Secure tunnel4
Service Status	Enabled
Current Server	Auto

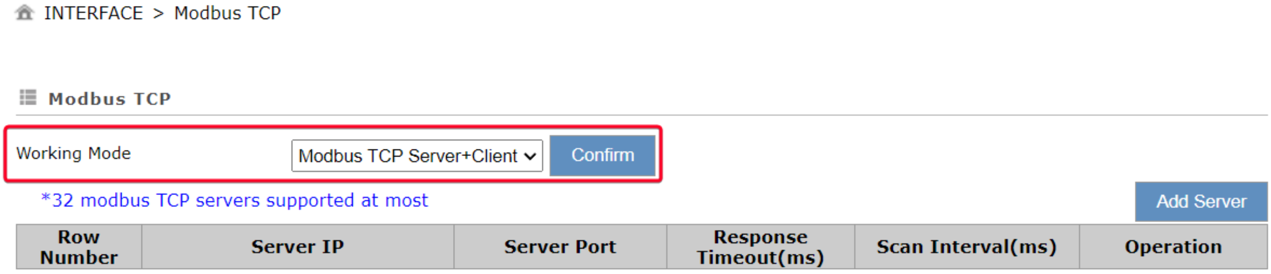
DX3021_EB8B

Open Device Webpage

Lan IP Address: 192.168.1.99 SN: DX30210120090014 Firmware: 1.20

7. After entering DX router login page, input your account and password. (Default: admin/admin) and click on **login**.

8. Go to **INTERFACE** → **MODBUS TCP** and select **Modbus TCP Server+Client** as **working mode**, then click on **Confirm**.



INTERFACE > Modbus TCP

Modbus TCP

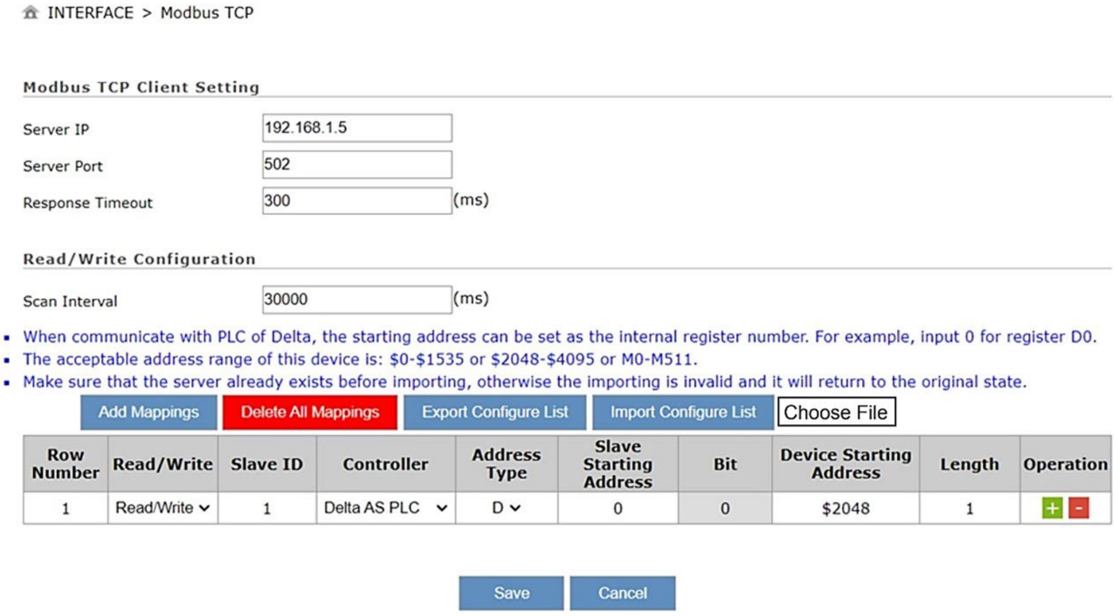
Working Mode: Modbus TCP Server+Client — Confirm

*32 modbus TCP servers supported at most

Add Server

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

9. Click on **Add Server** and configure PLC as shown in the figure below. Set the controller register to Delta AS PLC D0, and map the register to DX router register $2048, then click on **Save**.



INTERFACE > Modbus TCP

Modbus TCP Client Setting

Server IP: 192.168.1.5

Server Port: 502

Response Timeout: 300 (ms)

Read/Write Configuration

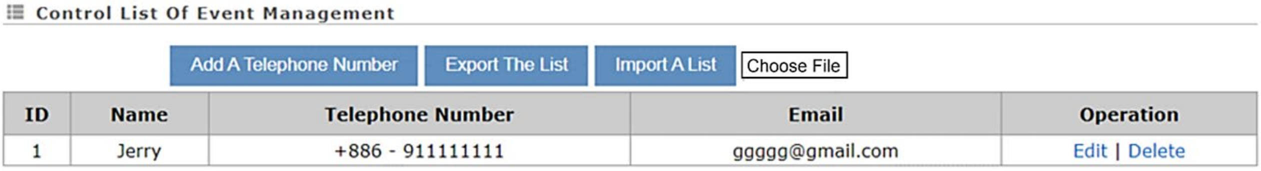
Scan Interval: 30000 (ms)

- When communicate with PLC of Delta, the starting address can be set as the internal register number. For example, input 0 for register D0.
- The acceptable address range of this device is: $0-$1535 or $2048-$4095 or M0-M511.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Read/Write	Slave ID	Controller	Address Type	Slave Starting Address	Bit	Device Starting Address	Length	Operation
1	Read/Write	1	Delta AS PLC	D	0	0	$2048	1	+ -

10. Go to **SYSTEM** → **Privilege Management**, refer to section 3.5.10.1 to check for the SMS function of the SIM card.

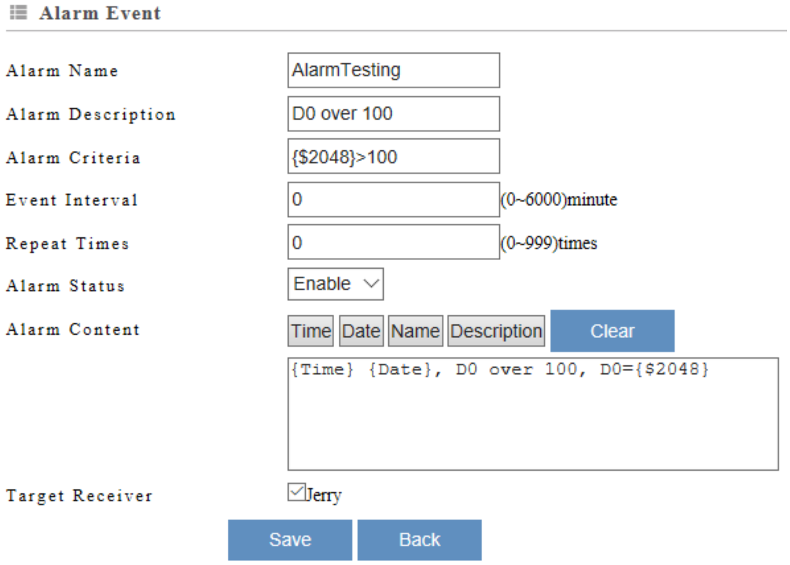
11. In **Control List of Event Management**, click on **Add A Telephone Number**, to create a new entry for a user who needs to receive alerts.



Control List Of Event Management

ID	Name	Telephone Number	Email	Operation
1	Jerry	+886 - 911111111	ggggg@gmail.com	Edit | Delete

12. Go to **SYSTEM** → **Event Management**, click on **ADD** to configure the setting for **Alarm Event,** click on **Save** to complete. Set it up as follows:



Alarm Event

Alarm Name: AlarmTesting

Alarm Description: D0 over 100

Alarm Criteria: {$2048}>100

Event Interval: 0 (0~6000)minute

Repeat Times: 0 (0~999)times

Alarm Status: Enable

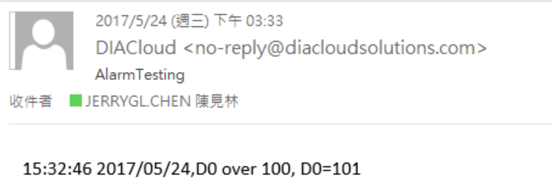
Alarm Content: {Time} {Date}, D0 over 100, D0={$2048}

Target Receiver: ☑Jerry

13. Connect the PLC to the network port of the DX Cloud Router using an Ethernet cable.

14. After triggering **PLC D0 > 100**, you can receive warning messages via SMS, email, DIACloud cloud platform, and DIACloud app.

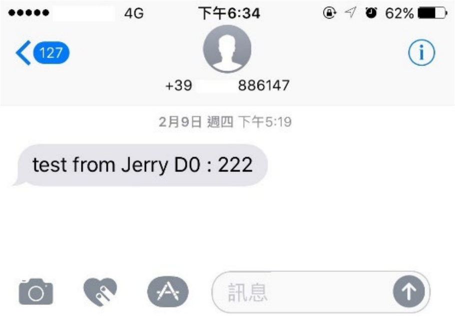
- Emails



2017/5/24 (週三) 下午 03:33
DIACloud <no-reply@diacloudsolutions.com>
AlarmTesting
收件者 JERRYGL.CHEN 陳見林

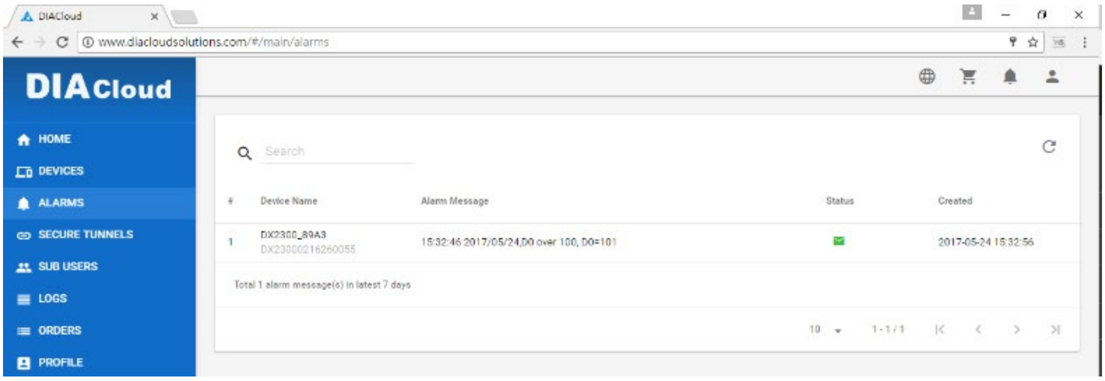
15:32:46 2017/05/24,D0 over 100, D0=101

- SMS messages



test from Jerry D0 : 222

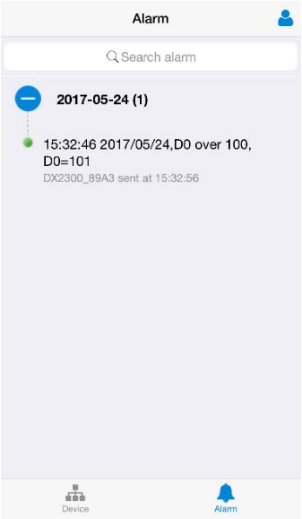
- DIACloud platform



#	Device Name	Alarm Message	Status	Created
1	DX2300_89A3 DX23000216260055	15:32:46 2017/05/24,D0 over 100, D0=101	✉	2017-05-24 15:32:56

Total 1 alarm message(s) in latest 7 days

- DIACloud APP



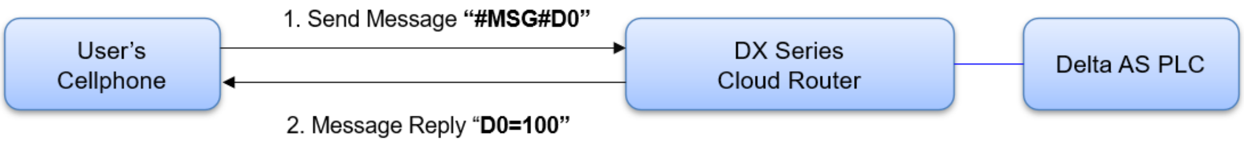
2017-05-24 (1)

15:32:46 2017/05/24,D0 over 100, D0=101
DX2300_89A3 sent at 15:32:56

2.3.26 SMS Querying Cloud Router Data Application

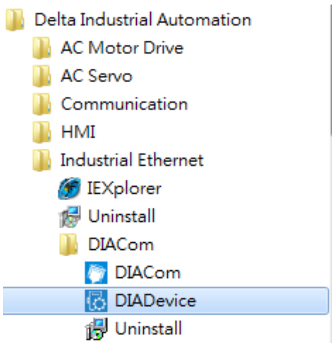
Send SMS messages to check the register D0 in the PLC, and the cloud router will respond via SMS with the current value of D0.

Please refer to Chapter 3.5.11 Event Management for a detailed explanation of the configuration parameters.

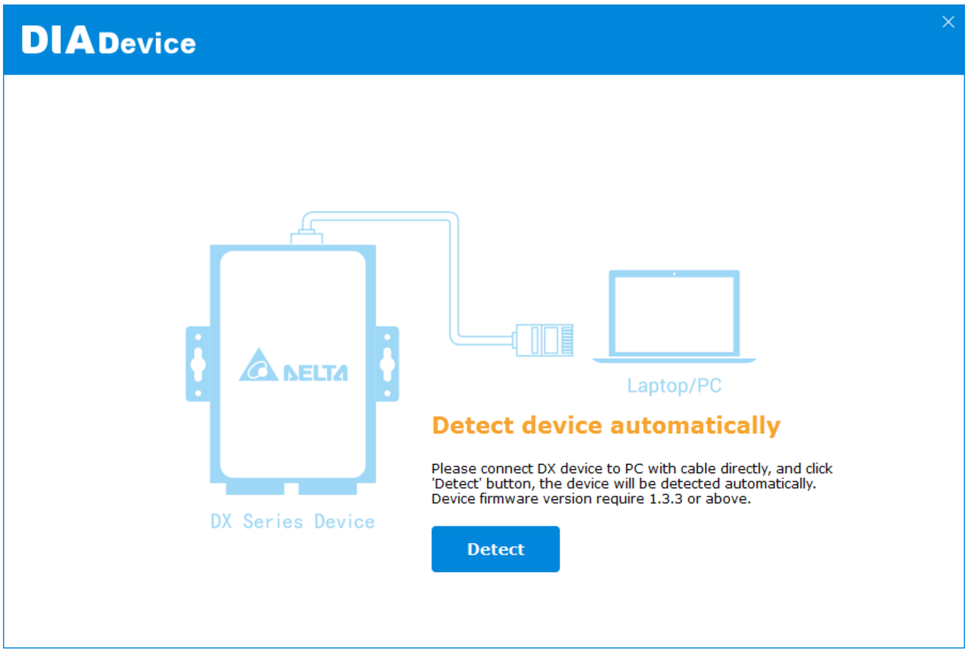


Setup Steps

1. Make sure that all **the basic configuration** detailed in Chapter 2 has been completed and functions properly.
2. Use a network cable to connect LAN ports on your PC and the DX router.
3. Install DIACom software, open DIADevice: Click Start icon on Windows and go to **All APPs** → **Delta Industrial Automation** → **Industrial Ethernet** → **DIACom** → **DIADevice**.

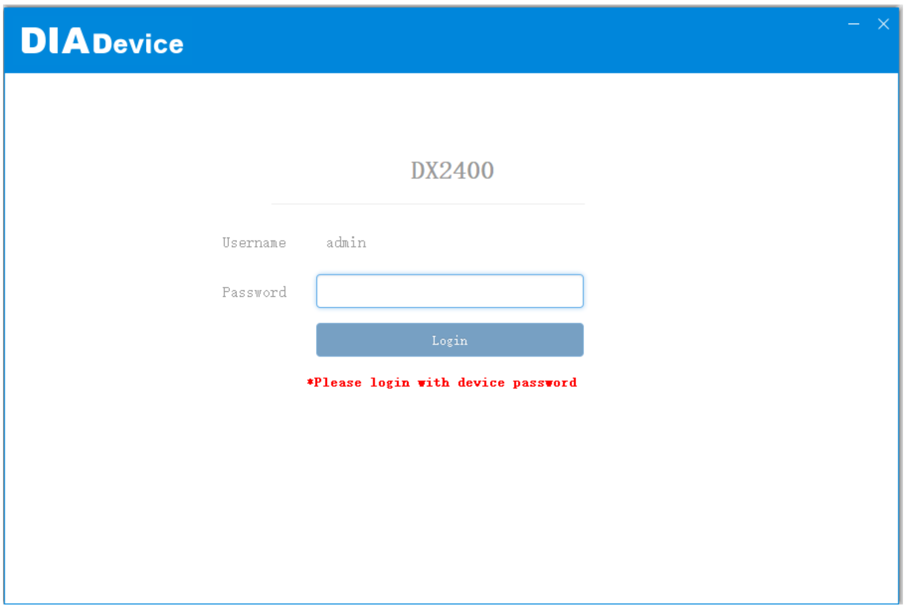


4. Click on **Detect**, and it will redirect to the login page of DX router.



Please connect DX device to PC with cable directly, and click 'Detect' button, the device will be detected automatically.
Device firmware version require 1.3.3 or above.

5. Enter your account and password. (Default: admin/admin)



DIADevice

DX2400

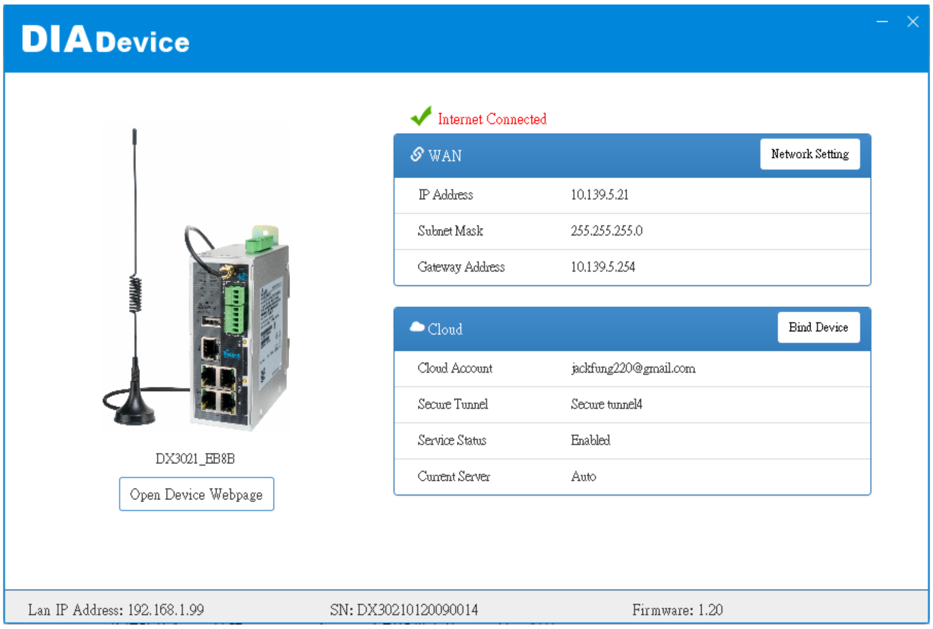
Username admin

Password

Login

*Please login with device password

6. Click on **Open Device Webpage** and verify that the bound IP address is 192.168.1.99.



DIADevice

✓ Internet Connected

WAN — Network Setting

IP Address	10.139.5.21
Subnet Mask	255.255.255.0
Gateway Address	10.139.5.254

Cloud — Bind Device

Cloud Account	jackfung220@gmail.com
Secure Tunnel	Secure tunnel4
Service Status	Enabled
Current Server	Auto

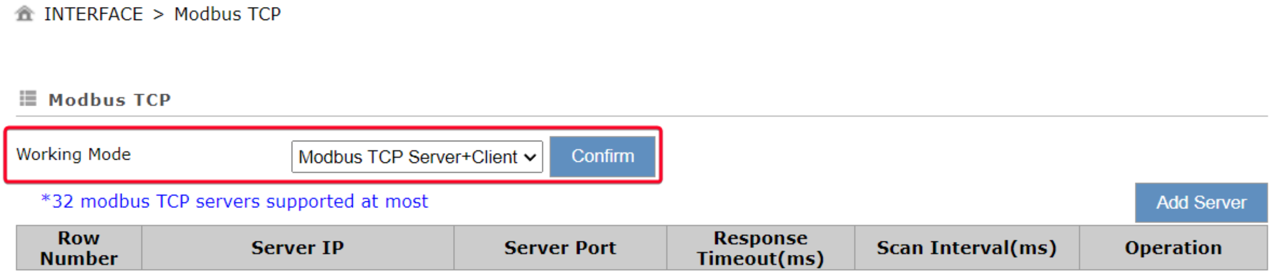
DX3021_EB8B

Open Device Webpage

Lan IP Address: 192.168.1.99 SN: DX30210120090014 Firmware: 1.20

7. After entering DX router login page, input your account and password. (Default: admin/admin) and click on **login**.

8. Go to **INTERFACE** → **MODBUS TCP** and select **Modbus TCP Server+Client** as **working mode**, then click on **Confirm**.



INTERFACE > Modbus TCP

Modbus TCP

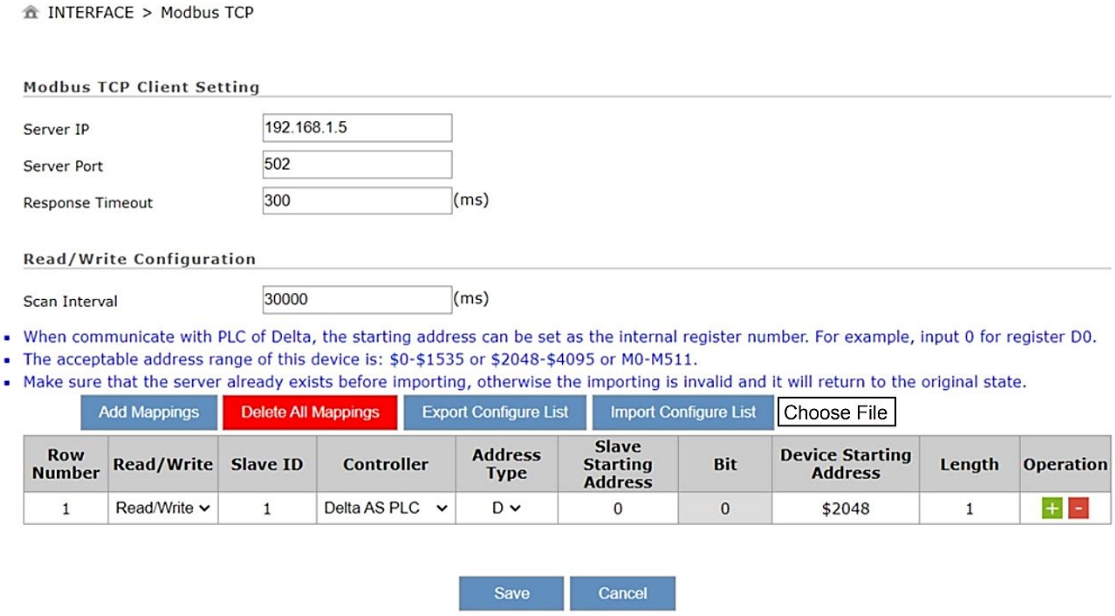
Working Mode: Modbus TCP Server+Client — Confirm

*32 modbus TCP servers supported at most

Add Server

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

9. Click on **Add Server** and configure PLC as shown in the figure below. Set the controller register to Delta AS PLC D0, and map the register to DX router register $2048, then click on **Save**.



Modbus TCP Client Setting

Server IP: 192.168.1.5

Server Port: 502

Response Timeout: 300 (ms)

Read/Write Configuration

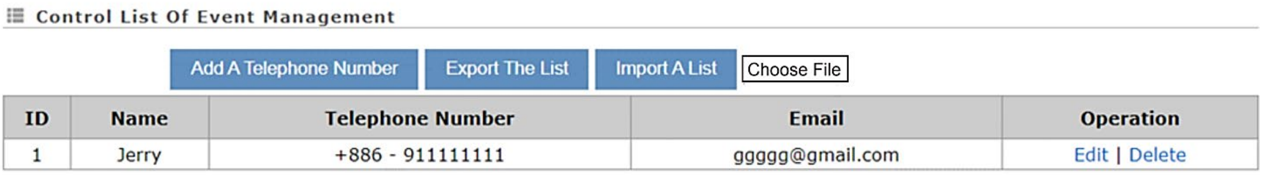
Scan Interval: 30000 (ms)

- When communicate with PLC of Delta, the starting address can be set as the internal register number. For example, input 0 for register D0.
- The acceptable address range of this device is: $0-$1535 or $2048-$4095 or M0-M511.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Read/Write	Slave ID	Controller	Address Type	Slave Starting Address	Bit	Device Starting Address	Length	Operation
1	Read/Write	1	Delta AS PLC	D	0	0	$2048	1	+ -

10. Go to **SYSTEM** → **Privilege Management**, refer to section 3.5.10.1 to check for the SMS function of the SIM card.

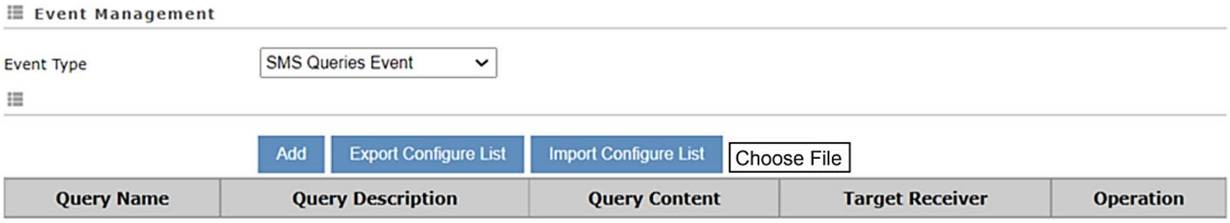
11. In **Control List of Event Management**, click on **Add A Telephone Number**, to create a new entry for a user who needs to receive alerts.



Control List Of Event Management

ID	Name	Telephone Number	Email	Operation
1	Jerry	+886 - 911111111	ggggg@gmail.com	Edit | Delete

12. Go to **SYSTEM** → **Event Management,** select **SMS Queries** as **Event Type.**

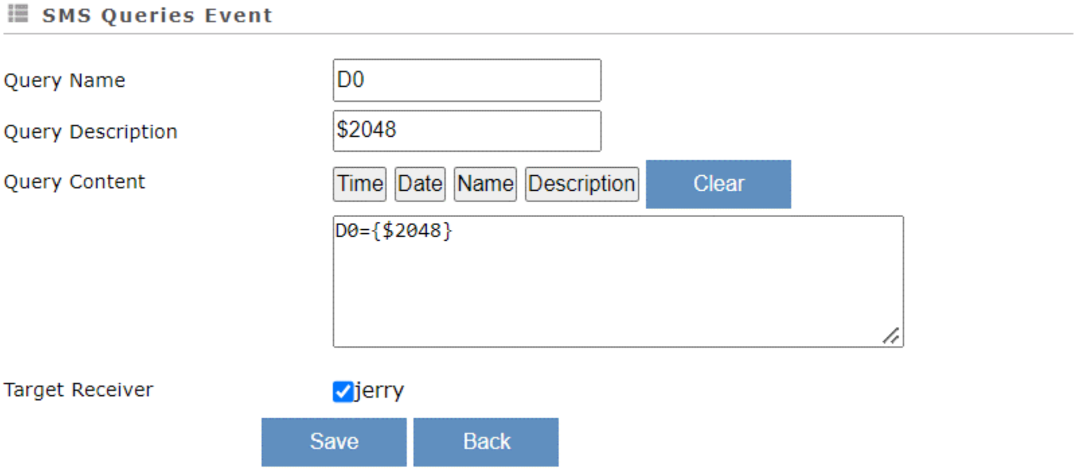


Event Management

Event Type: SMS Queries Event

Query Name	Query Description	Query Content	Target Receiver	Operation

13. Click on **Add** to configure **SMS Queries Event** as follows. When the DX Cloud Router receives an SMS with the content '#MGS#D0', it will respond with 'D0=XX'. Click on 'Save' to complete.



SMS Queries Event

Query Name: D0

Query Description: $2048

Query Content: D0={$2048}

Target Receiver: ☑jerry

14. Send the SMS content **#MSG#D0** to the SIM card number of the cloud router. The cloud router will respond via SMS with **'D0=XXX'**.

Notice

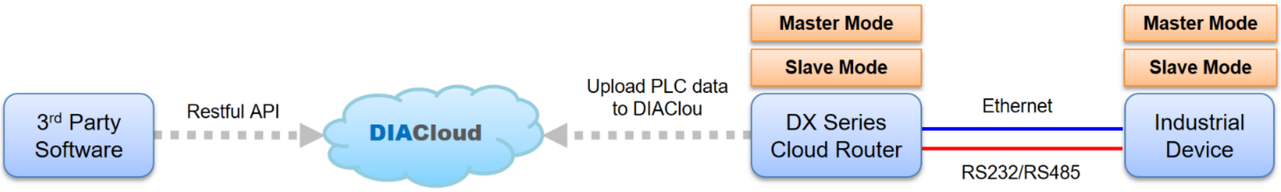
SMS query message format = #MSG#Query Name

2.3.27 Device Remote Connection Application (Restful API)

DIACloud supports Restful API, allowing third-party software to access DIACloud data. For more information on DIACloud Restful API, please refer to the DIACloud Restful API Manual.

Example

After PLC uploads data to DIACloud, the third-party software retrieves register data from DIACloud WEB using the RESTful API.

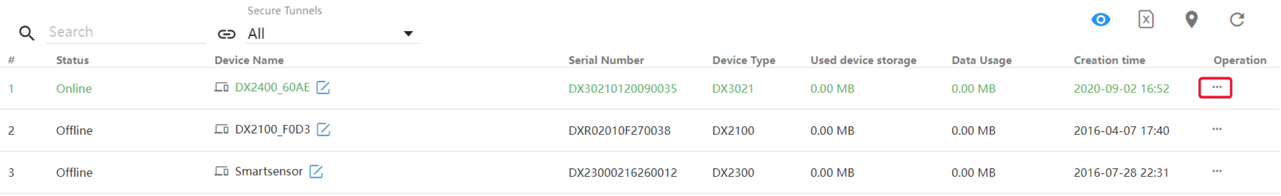


Setup Steps

1. Refer to **Section 2.3.1 Data Collection** configuration and upload the data to DIACloud.

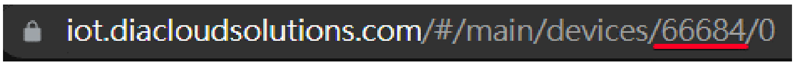
2. Login to https://iot.diacloudsolutions.com

3. Click on the device menu and select the DX Cloud Router that needs to retrieve data, click ··· .



#	Status	Device Name	Serial Number	Device Type	Used device storage	Data Usage	Creation time	Operation
1	Online	DX2400_60AE	DX30210120090035	DX3021	0.00 MB	0.00 MB	2020-09-02 16:52	···
2	Offline	DX2100_F0D3	DXR02010F270038	DX2100	0.00 MB	0.00 MB	2016-04-07 17:40	···
3	Offline	Smartsensor	DX23000216260012	DX2300	0.00 MB	0.00 MB	2016-07-28 22:31	···

4. Record the **Device ID = 66684** in the browser URL.

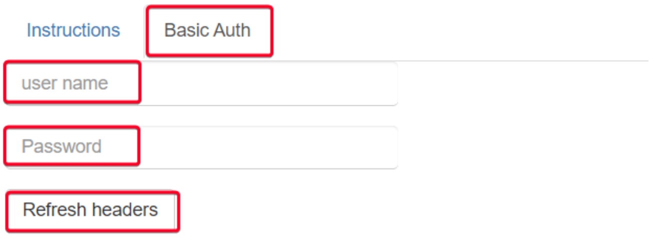


iot.diacloudsolutions.com/#/main/devices/66684/0

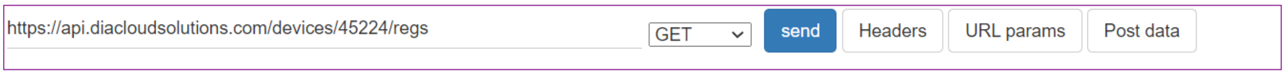
5. Log in to the DIACloud API webpage https://api.diacloudsolutions.com.cn/

6. Click on the left menu GET /devices/**{device_id}**/regs , to retrieve data from the registers of the DX device.

7. Click **Basic Auth** on the right-hand side page, enter **DIACloud account/password,** then click on **Refresh headers.**

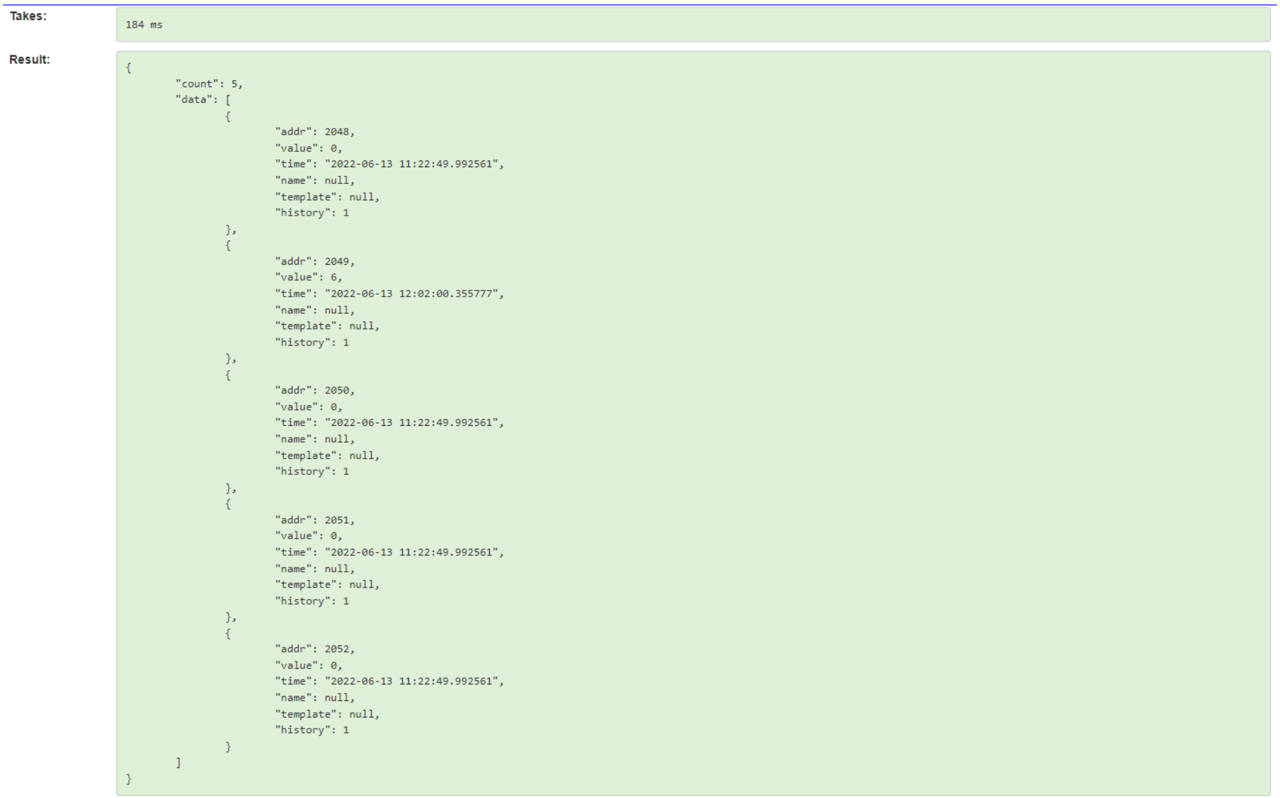


8. Replace {device_id} in the API address with the **Device ID=66684**. The modified address should be as follows:



https://api.diacloudsolutions.com/devices/45224/regs

9. Click on send to display the JSON data content.



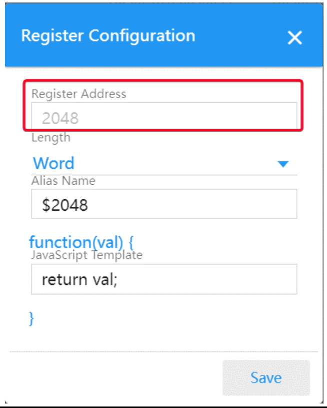
Takes: 184 ms

Result:

```
{
        "count": 5,
        "data": [
                {
                        "addr": 2048,
                        "value": 0,
                        "time": "2022-06-13 11:22:49.992561",
                        "name": null,
                        "template": null,
                        "history": 1
                },
                {
                        "addr": 2049,
                        "value": 6,
                        "time": "2022-06-13 12:02:00.355777",
                        "name": null,
                        "template": null,
                        "history": 1
                },
                {
                        "addr": 2050,
                        "value": 0,
                        "time": "2022-06-13 11:22:49.992561",
                        "name": null,
                        "template": null,
                        "history": 1
                },
                {
                        "addr": 2051,
                        "value": 0,
                        "time": "2022-06-13 11:22:49.992561",
                        "name": null,
                        "template": null,
                        "history": 1
                },
                {
                        "addr": 2052,
                        "value": 0,
                        "time": "2022-06-13 11:22:49.992561",
                        "name": null,
                        "template": null,
                        "history": 1
                }
        ]
}
```

Parameter Explanation

Parameters	Name	Description

addr	Register Address	Register Address ($2048~$4096), the corresponding register addresses can be queried from Register Configuration of this URL:iot.diacloudsolutions.com
		
		Register Configuration
		Register Address: 2048
		Length: Word
		Alias Name: $2048
		function(val) {
		JavaScript Template: return val;
		}
		Save

value	Register Value	Register value (Unsigned Decimal Integer, other types need to be converted manually)
time	Time	Time of Register Value Upload. The time format is UTC/GMT+08:00 (China Standard Time).
template	Java Script	If need to perform operations such as addition, subtraction, multiplication, division, or manipulate text descriptions on the registers' values, users can achieve this using JavaScript syntax in this field.
history	Save History?	1: Save History 0: Do Not Save History

10. Developers can now begin to retrieve the required data from DIACloud.

Chapter 3 Functions

Table of Contents

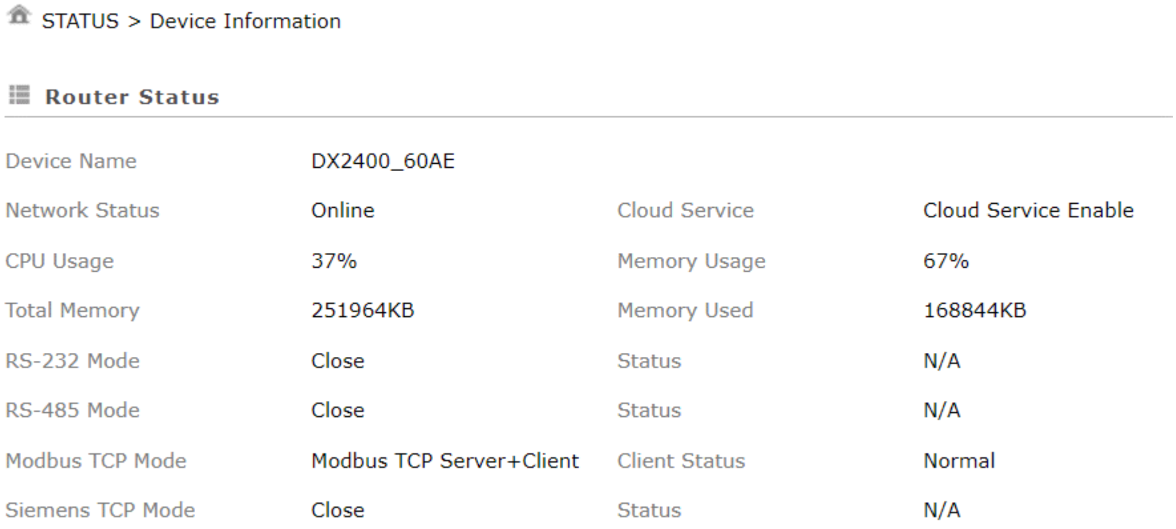
3.1 STATUS

You can view summary and detailed information on the Device Information. Which includes seven categories: Device Information, Network Status, Routing Table, Local Log, Traffic Statistics, Cloud Status, and Connected Devices.

3.1.1 Device Information

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

- **Router Status**



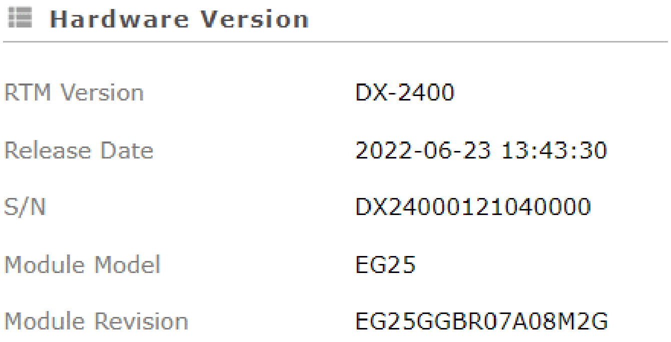
STATUS > Device Information

Router Status

Device Name	DX2400_60AE		
Network Status	Online	Cloud Service	Cloud Service Enable
CPU Usage	37%	Memory Usage	67%
Total Memory	251964KB	Memory Used	168844KB
RS-232 Mode	Close	Status	N/A
RS-485 Mode	Close	Status	N/A
Modbus TCP Mode	Modbus TCP Server+Client	Client Status	Normal
Siemens TCP Mode	Close	Status	N/A

Item	Description
Device name	Router device name.
Network Status	Network status.
Cloud Service	Cloud service status.
CPU Usage	Router’s CPU usage.
Memory Usage	Router’s memory usage.
Memory Used	Router’s memory usage.
Total Memory	Router’s total memory.

- **Hardware Version**

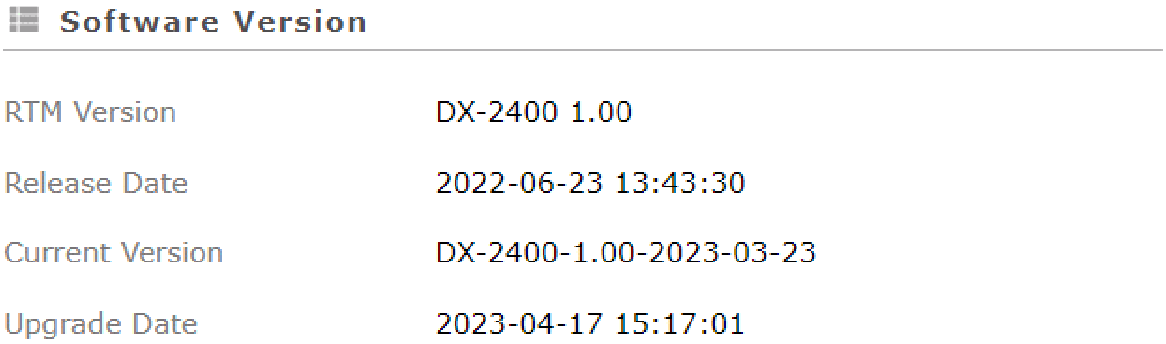


Hardware Version

RTM Version	DX-2400
Release Date	2022-06-23 13:43:30
S/N	DX24000121040000
Module Model	EG25
Module Revision	EG25GGBR07A08M2G

Item	Description
RTM Version	Release to manufacturing version of the router.
Release Date	Hardware release date.
S/N	Serial number of the router.
Module Model	Cellular module model name.
Module Revision	Cellular module Firmware version.

- **Software Version**



Software Version

RTM Version	DX-2400 1.00
Release Date	2022-06-23 13:43:30
Current Version	DX-2400-1.00-2023-03-23
Upgrade Date	2023-04-17 15:17:01

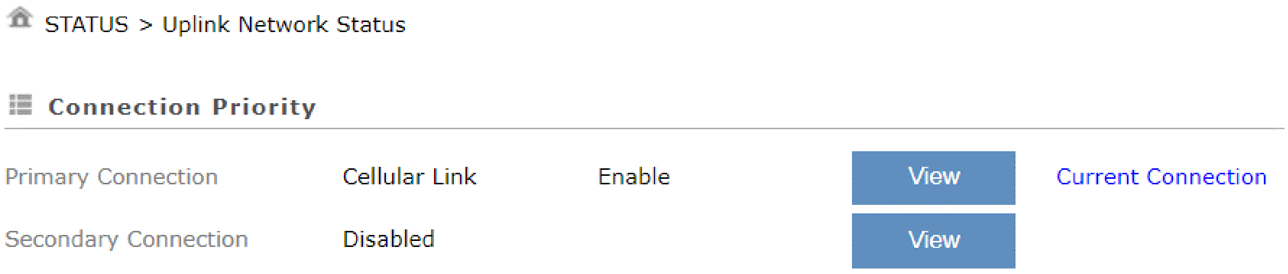
Item	Desription
RTM Version	The software version number at the time of factory release for the cloud router.
Release Date	Software release date.
Current Version	Version number of the software currently used on the router.
Upgrade Date	Upgrade time of the software currently used on the router.

3.1.2 Uplink Network Status

Displaying the network status information of the cloud router. Which includes Connection Priority, Uplink Network Status, SMS Status.

- **Connection Priority**

Display the network status, network signal, and network log information for the primary and secondary connection.

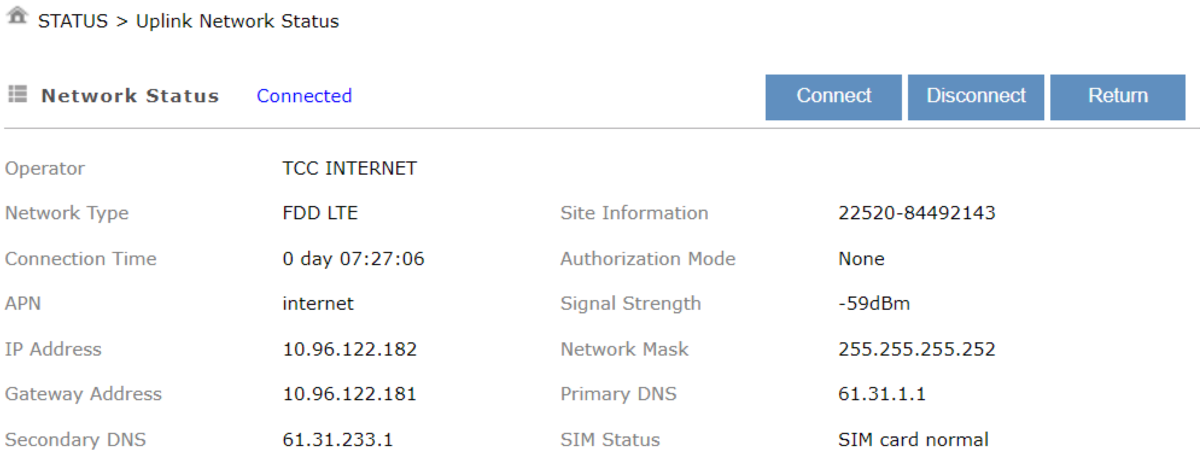


STATUS > Uplink Network Status

Connection Priority

Primary Connection	Cellular Link	Enable	View	Current Connection
Secondary Connection	Disabled		View	

Description	Default
View	
Display Network Status / Signal Strength / Network Logs.	N/A



STATUS > Uplink Network Status

Network Status Connected

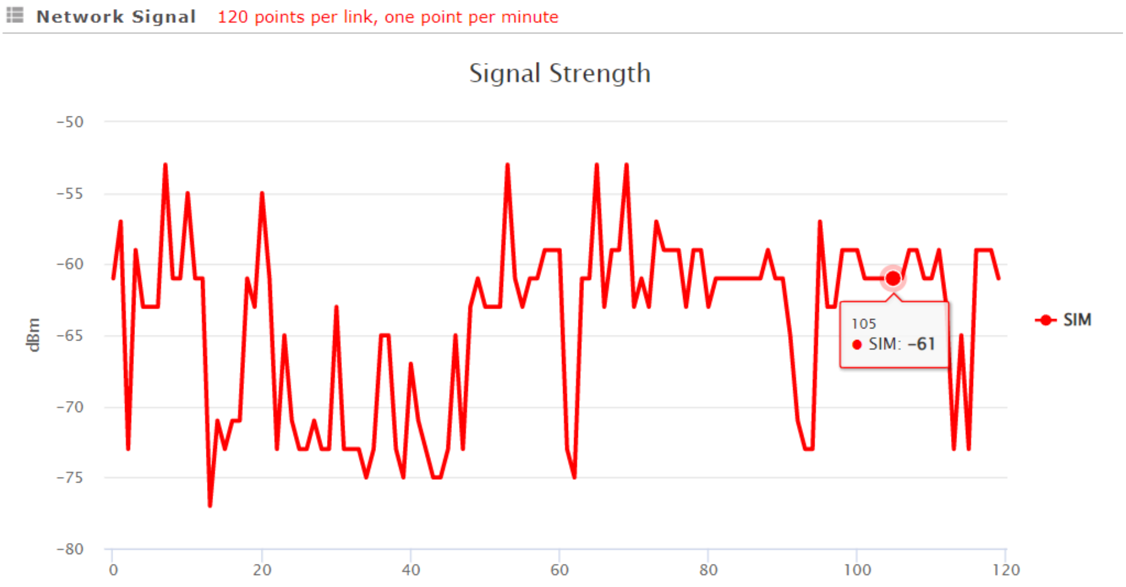
Operator	TCC INTERNET		
Network Type	FDD LTE	Site Information	22520-84492143
Connection Time	0 day 07:27:06	Authorization Mode	None
APN	internet	Signal Strength	-59dBm
IP Address	10.96.122.182	Network Mask	255.255.255.252
Gateway Address	10.96.122.181	Primary DNS	61.31.1.1
Secondary DNS	61.31.233.1	SIM Status	SIM card normal

Description	Default
Connect	
Connect to the internet	N/A
Disconnect	
Disconnect from the internet.	N/A
Return	
Return to the previous page.	N/A

Description	Default
Operator	
Display SIM card operator.	N/A
Network Type	
Display the network type applied to your SIM card.	N/A
Site Information	
Display LAC and Cellid information of 3G/4G base station.	N/A
Connection Time	
Display the time spent attempting to connect to a network.	N/A
Authorization Mode	
Display the authorization mode applied to your SIM card.	N/A
APN	
Display APN(Access Point Network) name of your SIM card.	N/A
Signal Strength	
Display the signal strength of your SIM card.	N/A
IP Address	
Display the IP address assigned to your SIM card.	N/A
Network Mask	
Display the subnet mask of your SIM card.	N/A
Gateway Address	
Display the gateway address of your SIM card.	N/A
Primary DNS	
Display primary DNS server address of your SIM card.	N/A
Secondary DNS	
Display secondary DNS server address of your SIM card.	N/A
SIM Status	
Display the operating status of your SIM card.	N/A

1. Network Signal

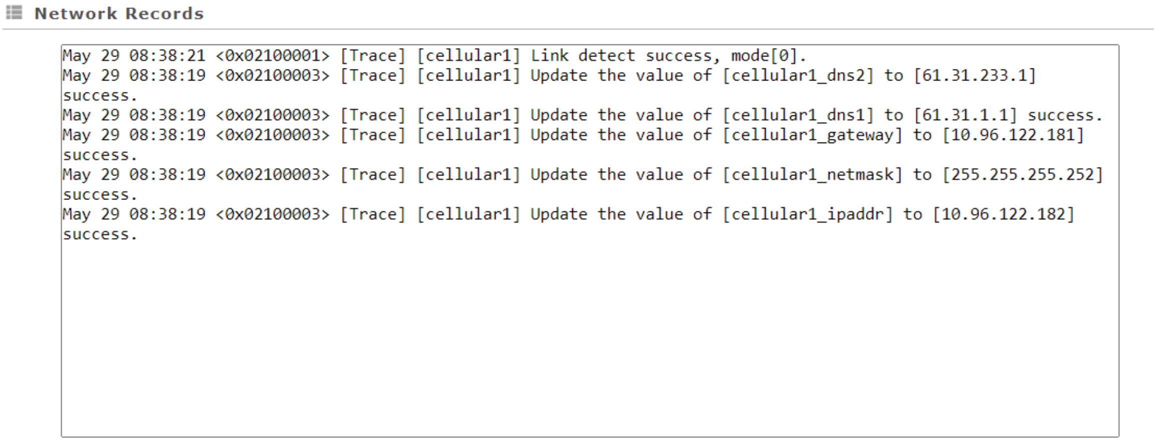
Show the information of operator, base station ID, network type, signal strength records for the past 2 hours and other network information.



Description	Default
Network Signal	
Display the current SIM card signal strength, with a maximum of 120 dBm.	N/A

2. Network Records

Display the current network records.

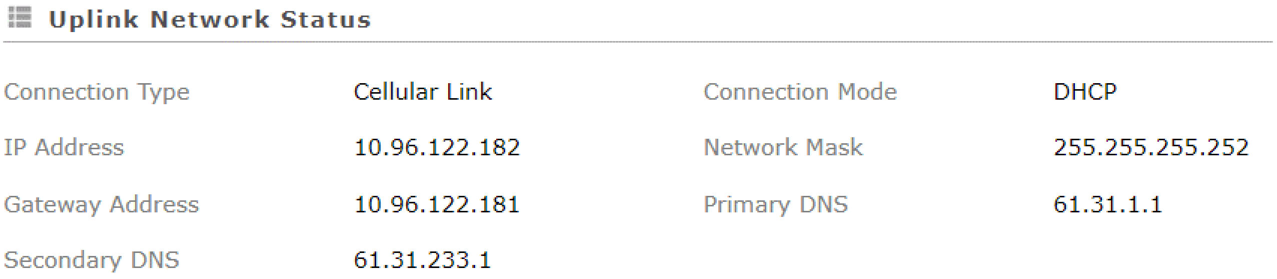


```
May 29 08:38:21 <0x02100001> [Trace] [cellular1] Link detect success, mode[0].
May 29 08:38:19 <0x02100003> [Trace] [cellular1] Update the value of [cellular1_dns2] to [61.31.233.1]
success.
May 29 08:38:19 <0x02100003> [Trace] [cellular1] Update the value of [cellular1_dns1] to [61.31.1.1] success.
May 29 08:38:19 <0x02100003> [Trace] [cellular1] Update the value of [cellular1_gateway] to [10.96.122.181]
success.
May 29 08:38:19 <0x02100003> [Trace] [cellular1] Update the value of [cellular1_netmask] to [255.255.255.252]
success.
May 29 08:38:19 <0x02100003> [Trace] [cellular1] Update the value of [cellular1_ipaddr] to [10.96.122.182]
success.
```

Description	Default
Network Records	
Capture and display the current network records.	N/A

3. Uplink Network Status

Display Uplink Network connection information.



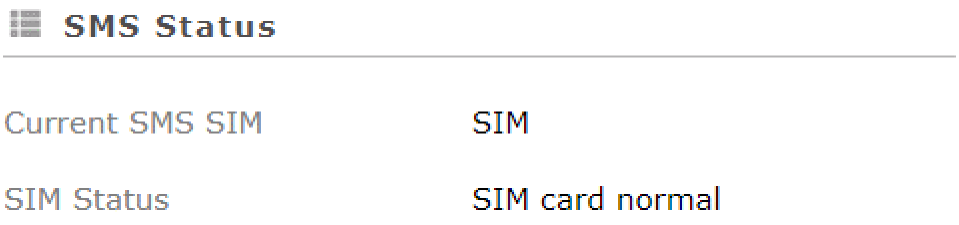
Uplink Network Status

Connection Type	Cellular Link	Connection Mode	DHCP
IP Address	10.96.122.182	Network Mask	255.255.255.252
Gateway Address	10.96.122.181	Primary DNS	61.31.1.1
Secondary DNS	61.31.233.1		

Description	Default
Connection Type	
Display the current network connection type.	N/A
Connection Mode	
Display the network access mode.	N/A
IP Address	
Display the network IP address.	N/A
Gateway Address	
Display the gateway address.	N/A
Netwoek Mask	
Display network subnet mask.	N/A
Primary DNS	
Display primary DNS server address.	N/A
Secondary DNS	
Display secondary DNS server address.	N/A

- **SMS Network Status**

Display SMS network status.



SMS Status

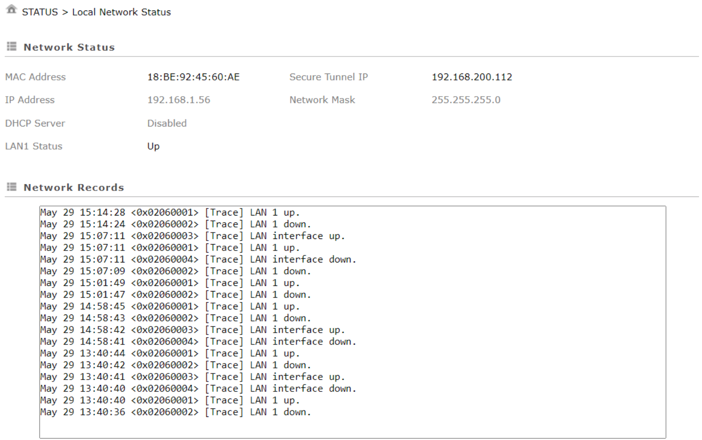
Current SMS SIM SIM

SIM Status SIM card normal

Description	Default
Currenet SMS SIM	
Display the SIM card slot currently being used.	N/A
SIM Status	
Display the status of SIM card. ● **Inactive:** SIM card is functioning normally but have not been activated. ● **No SIM card or SIM card has no response:** 1. SIM card has not been placed in the card slot. 2. SIM card has been placed in the card slot but can't be detected. Please remove and re-insert the SIM card to the slot. ● **SIM card normal:** The SIM card is in normal use. ● **PIN locked:** Entered incorrect PIN code too many times. ● **PUK locked:** PUK is an 8-digit code unique to your SIM card to prevent unauthorized use of your data, usually applied with PIN code as the second level of security on your SIM card. PUK locked would be displayed and you'll be requested to enter PUK code when you've incorrectly entered the PIN for three times and more.	N/A

3.1.3 Local Network Status

Display local network information and local network logs.



STATUS > Local Network Status

Network Status

MAC Address	18:BE:92:45:60:AE	Secure Tunnel IP	192.168.200.112
IP Address	192.168.1.56	Network Mask	255.255.255.0
DHCP Server	Disabled		
LAN1 Status	Up		

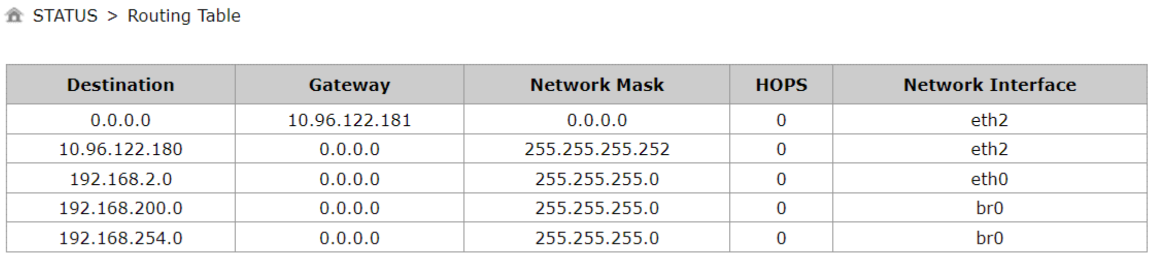
Network Records

```
May 29 15:14:28 <0x02060001> [Trace] LAN 1 up.
May 29 15:14:24 <0x02060002> [Trace] LAN 1 down.
May 29 15:07:11 <0x02060003> [Trace] LAN interface up.
May 29 15:07:11 <0x02060001> [Trace] LAN 1 up.
May 29 15:07:11 <0x02060004> [Trace] LAN interface down.
May 29 15:07:09 <0x02060002> [Trace] LAN 1 down.
May 29 15:01:49 <0x02060001> [Trace] LAN 1 up.
May 29 15:01:47 <0x02060002> [Trace] LAN 1 down.
May 29 14:58:45 <0x02060001> [Trace] LAN 1 up.
May 29 14:58:43 <0x02060002> [Trace] LAN 1 down.
May 29 14:58:42 <0x02060003> [Trace] LAN interface up.
May 29 14:58:41 <0x02060004> [Trace] LAN interface down.
May 29 13:40:44 <0x02060001> [Trace] LAN 1 up.
May 29 13:40:42 <0x02060002> [Trace] LAN 1 down.
May 29 13:40:41 <0x02060003> [Trace] LAN interface up.
May 29 13:40:40 <0x02060004> [Trace] LAN interface down.
May 29 13:40:40 <0x02060001> [Trace] LAN 1 up.
May 29 13:40:36 <0x02060002> [Trace] LAN 1 down.
```

Description	Default
MAC Address	
Display local MAC address.	N/A
IP Address	
Display local IP address.	N/A
Secure Tunnel IP	
Display the IP address bound with the cloud.	N/A
Network Mask	
Display local subnet mask.	N/A
DHCP Server	
Display whether the local DHCP Server is enabled.	N/A
Start IP Address	
Display the starting IP address of the local DHCP Server's IP address pool.	N/A
End IP Address	
Display the ending IP address of the local DHCP Server's IP address pool.	N/A
Address Lease Time	
Display the valid duration for IP address assignments by the local DHCP server.	N/A
LAN1 Status	
Display LAN operating status: ● **Connected:** Already connected to a network cable. ● **Not Connected:** No network cable connected.	N/A
Network Records	
Capture and display the current local network records.	N/A

3.1.4 Routing Table

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



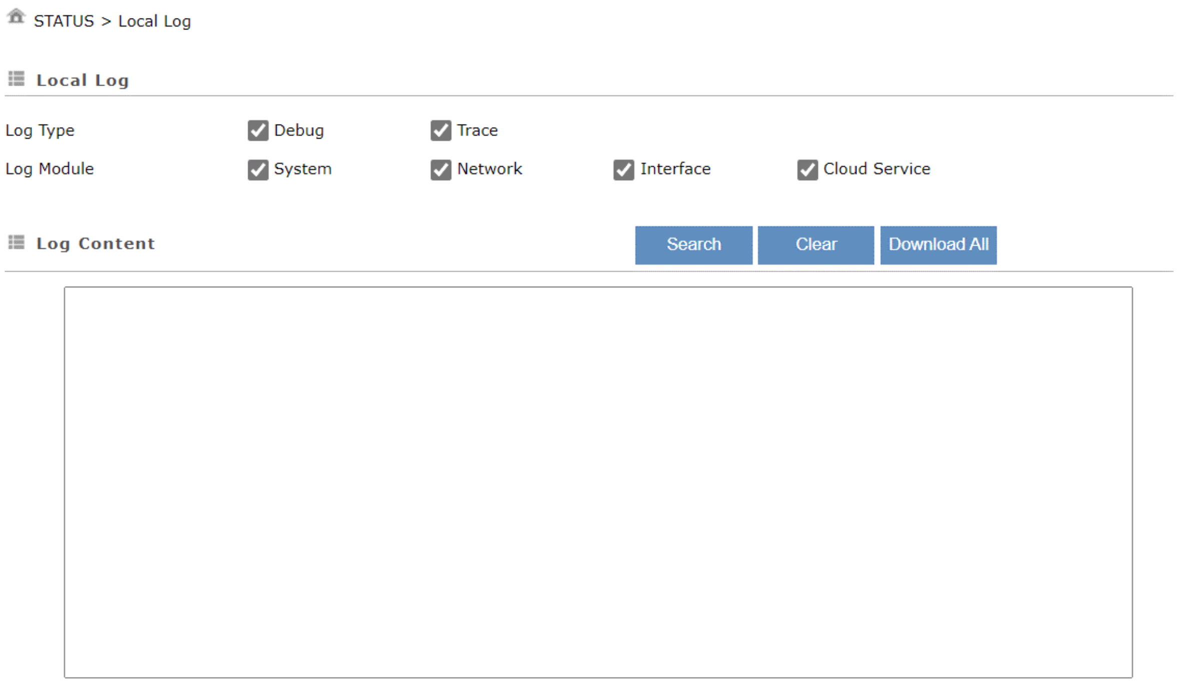
STATUS > Routing Table

Destination	Gateway	Network Mask	HOPS	Network Interface
0.0.0.0	10.96.122.181	0.0.0.0	0	eth2
10.96.122.180	0.0.0.0	255.255.255.252	0	eth2
192.168.2.0	0.0.0.0	255.255.255.0	0	eth0
192.168.200.0	0.0.0.0	255.255.255.0	0	br0
192.168.254.0	0.0.0.0	255.255.255.0	0	br0

Description	Default
Destination	
Display IP address of the network destination.	N/A
Gateway	
Display gateway address of the network destination.	N/A
Network Mask	
Display the network subnet mask.	N/A
HOPS	
"HOPS" refers to the number of routers passed through during network transmission, used to measure the length of the path for data transfer. A lower hop count indicates a shorter transmission path and faster speed.	N/A
Network Interface	
The network interface that is currently being used.	N/A

3.1.5 Local Log

Display the operation logs of cloud router, including system, network, interface, cloud service and so on.



STATUS > Local Log

Local Log

Log Type ☑ Debug ☑ Trace

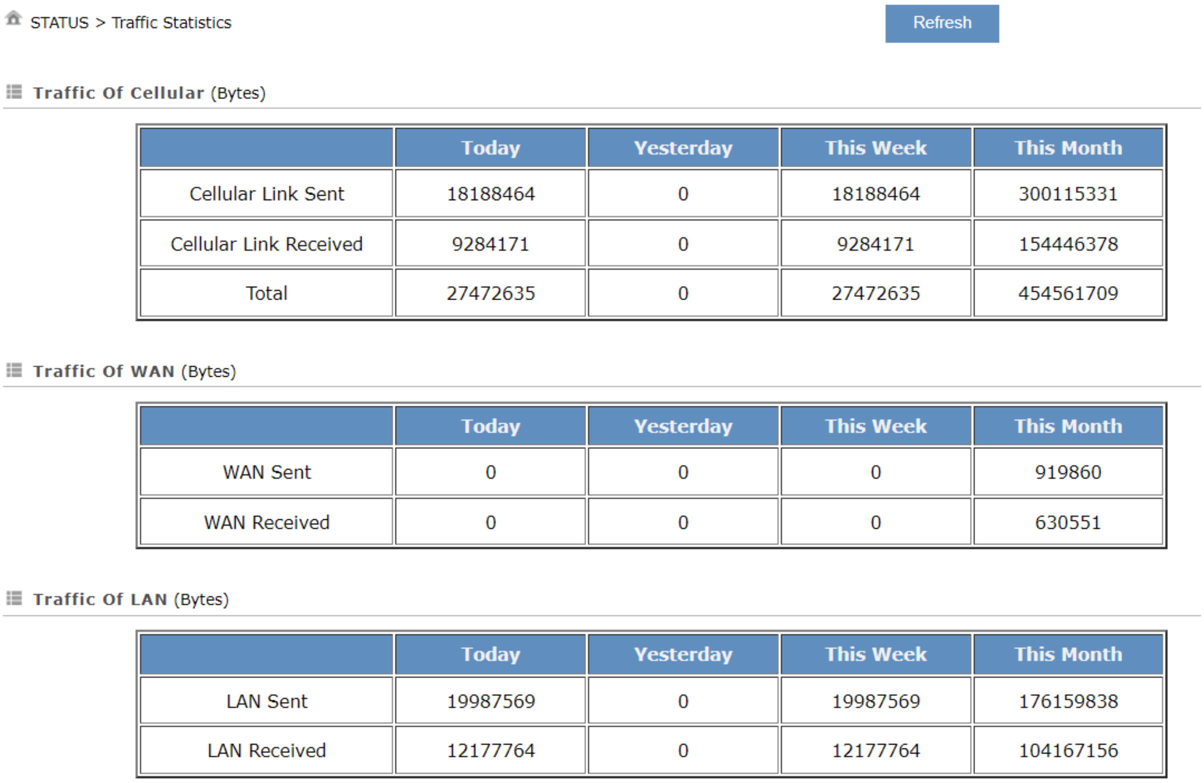
Log Module ☑ System ☑ Network ☑ Interface ☑ Cloud Service

Log Content

Description	Default
Local Log	
● Log Type: Choose to record Debug logs or use Trace-level logging. ● Log Module: Select the target features to record with options of System, Network, Interface, Cloud Service Log.	Select all
Log Content	
Record and display the current information of system, network, interface and cloud services.	N/A

3.1.6 Traffic Statistics

This page displays router network traffic statistics, including data on sending and receiving traffic for mobile, wide area network (WAN), and local area network (LAN). Users can select the refresh button to display the latest statistical results or the clear button to reset the traffic information.



Traffic Of Cellular (Bytes)

	Today	Yesterday	This Week	This Month
Cellular Link Sent	18188464	0	18188464	300115331
Cellular Link Received	9284171	0	9284171	154446378
Total	27472635	0	27472635	454561709

Traffic Of WAN (Bytes)

	Today	Yesterday	This Week	This Month
WAN Sent	0	0	0	919860
WAN Received	0	0	0	630551

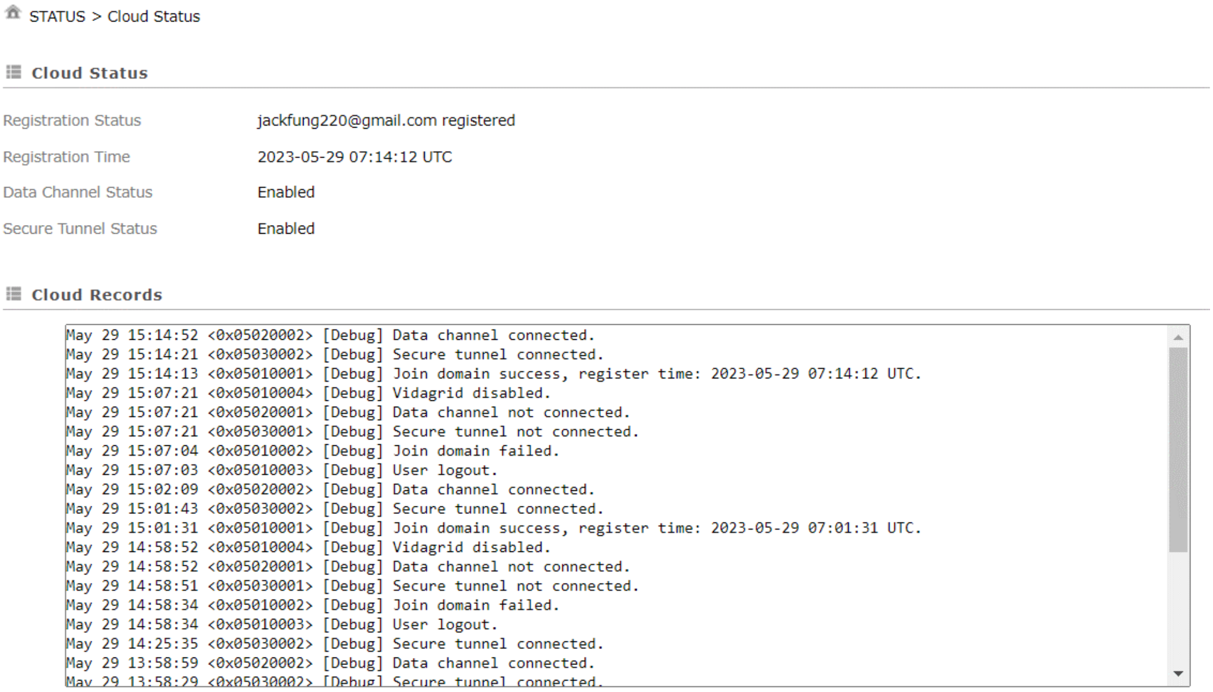
Traffic Of LAN (Bytes)

	Today	Yesterday	This Week	This Month
LAN Sent	19987569	0	19987569	176159838
LAN Received	12177764	0	12177764	104167156

Description	Default
Refresh	
Update send / receive data immediately.	N/A
Traffic of Cellular	
Statistics for mobile network: sent data / received data.	N/A
Traffic of WAN	
Statistics for WAN network: sent data / received data	N/A
Traffic of LAN	
Statistics for LAN network: sent data / received data	N/A

3.1.7 Cloud Status

This page displays cloud service status information, including registration status, registered account (if already registered), service status, and device registration time.



STATUS > Cloud Status

Cloud Status

Registration Status	jackfung220@gmail.com registered
Registration Time	2023-05-29 07:14:12 UTC
Data Channel Status	Enabled
Secure Tunnel Status	Enabled

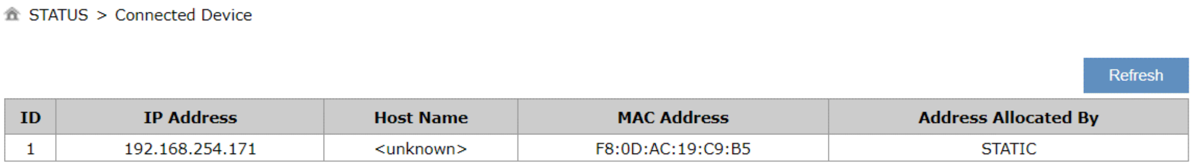
Cloud Records

```
May 29 15:14:52 <0x05020002> [Debug] Data channel connected.
May 29 15:14:21 <0x05030002> [Debug] Secure tunnel connected.
May 29 15:14:13 <0x05010001> [Debug] Join domain success, register time: 2023-05-29 07:14:12 UTC.
May 29 15:07:21 <0x05010004> [Debug] Vidagrid disabled.
May 29 15:07:21 <0x05020001> [Debug] Data channel not connected.
May 29 15:07:21 <0x05030001> [Debug] Secure tunnel not connected.
May 29 15:07:04 <0x05010002> [Debug] Join domain failed.
May 29 15:07:03 <0x05010003> [Debug] User logout.
May 29 15:02:09 <0x05020002> [Debug] Data channel connected.
May 29 15:01:43 <0x05030002> [Debug] Secure tunnel connected.
May 29 15:01:31 <0x05010001> [Debug] Join domain success, register time: 2023-05-29 07:01:31 UTC.
May 29 14:58:52 <0x05010004> [Debug] Vidagrid disabled.
May 29 14:58:52 <0x05020001> [Debug] Data channel not connected.
May 29 14:58:51 <0x05030001> [Debug] Secure tunnel not connected.
May 29 14:58:34 <0x05010002> [Debug] Join domain failed.
May 29 14:58:34 <0x05010003> [Debug] User logout.
May 29 14:25:35 <0x05030002> [Debug] Secure tunnel connected.
May 29 13:58:59 <0x05020002> [Debug] Data channel connected.
May 29 13:58:29 <0x05030002> [Debug] Secure tunnel connected.
```

Description	Default
Cloud Status	
● **Registration Status:** Show the information of bound account. ● **Registration Time:** Show the account binding time. ● **Data Channel Status:** Display the status of cloud data upload. If showing "Disable", it's possibly because the network is disconnected. Please refer to section 2.2.5. ● **Secure Tunnel Status:** Display the connection status of DIACloud and the secure tunnel. If showing "Disable", it's possibly because the network is disconnected. Please refer to section 2.2.5.	N/A
Cloud Records	
Display cloud service records.	N/A

3.1.8 Connected Device

This page shows information of the devices connected to the router, including the IP Address, Host Name, MAC Address. Users can click the refresh button to display the latest network devices.



STATUS > Connected Device

Refresh

ID	IP Address	Host Name	MAC Address	Address Allocated By
1	192.168.254.171	<unknown>	F8:0D:AC:19:C9:B5	STATIC

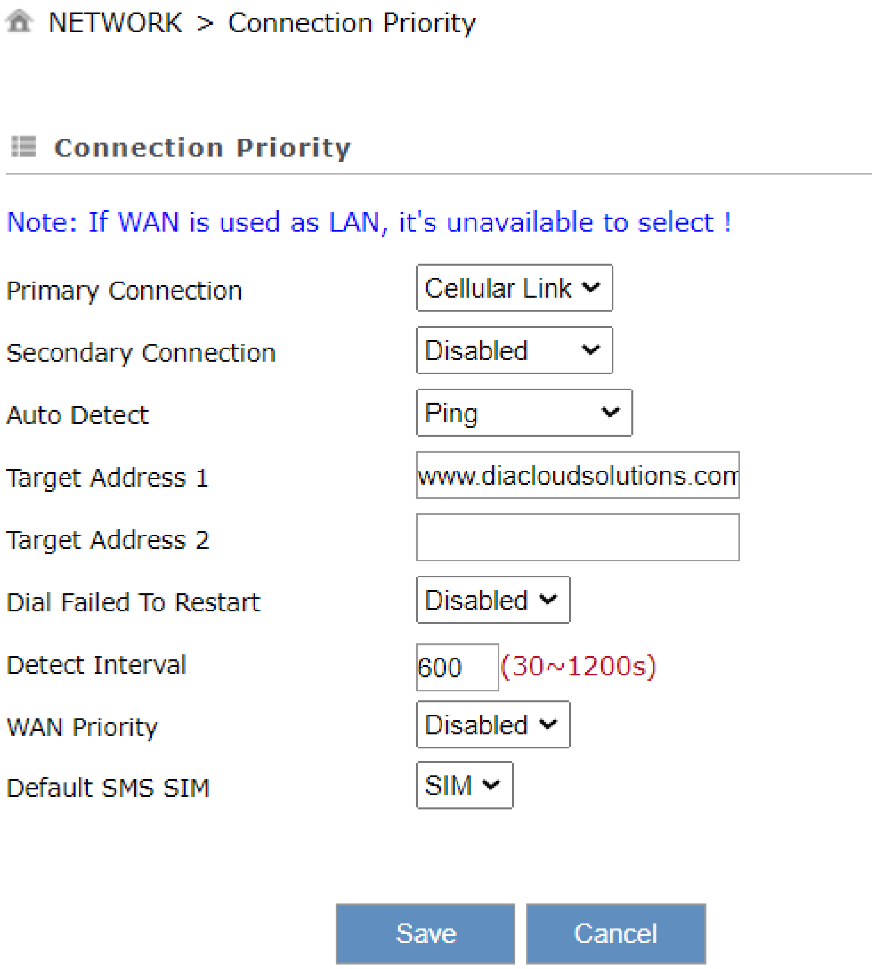
Description	Default
Connected Device	
● **Refresh:** Rescan LAN devices list. If you still don't see the device after refreshing, please try clicking the refresh button multiple times as the device might not be responding. ● **IP Address:** IP address of LAN devices. ● **Host Name:** Host Name of LAN devices. ● **MAC Address:** MAC Address of LAN devices ● **Address Allocated By:** IP address allocated by STATIC or DHCP.	N/A

3.2 NETWORK

Network configuration also includes four sub-configuration pages: WAN Settings, LAN Settings, Static Routing, and Dynamic DNS.

3.2.1 Connection

This page is used for setting up the connection priority, including settings for access methods, IP address acquisition methods, IP address, subnet mask, gateway, and other information.



NETWORK > Connection Priority

Connection Priority

Note: If WAN is used as LAN, it's unavailable to select !

Primary Connection: Cellular Link

Secondary Connection: Disabled

Auto Detect: Ping

Target Address 1: www.diacloudsolutions.com

Target Address 2:

Dial Failed To Restart: Disabled

Detect Interval: 600 (30~1200s)

WAN Priority: Disabled

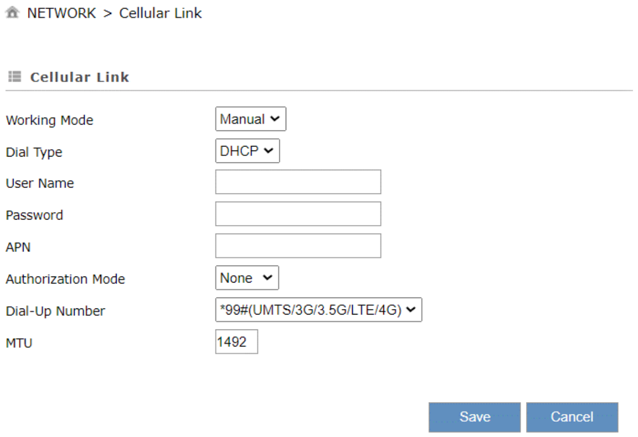
Default SMS SIM: SIM

Description	Default
Primary Connection	
Set the primary uplink network interface.	WAN
Secondary Connection	
Set the secondary uplink network interface.	Disabled
Auto Detect	
Check that the cloud router can establish a proper connection to the internet.	Cloud Service

Description	Default
● **Disabled:** Do not enable this feature. ● **Ping:** Enter the specific function variable name / IP address in the monitoring field to test whether the cloud router can communicate with the specified function variable name / IP address. ● **Cloud Service:** Test if the cloud router can communicate with the cloud server.	
Target Address 1/2	
Auto Detect, such as setting up PING. It will sequentially test communication with the cloud router based on the function variable name / IP address entered in fields 1 and 2.	N/A
Dial Failed to Restart	
Enable or disable the function that restart the router when the SIM card fails to dial the base station and cannot establish connection.	Disabled
Detect Interval	
Test the cloud router's internet connection status with a detection interval. Set the range between 30 ~ 1200 seconds.	600
WAN Priority	
When the WAN Priority feature is enabled and the first link is WAN, if a failure occurs (such as the WAN cable being unplugged), the system will monitor the WAN link's recovery. Once the WAN link is restored, the system will automatically switch back to the WAN link. If this feature is disabled, the switching will occur in the default order.	Disabled
Default SMS SIM	
Configure the default SIM card for sending text messages.	SIM

3.2.2 Cellular Link

Configure parameters related to the mobile network.



NETWORK > Cellular Link

Cellular Link

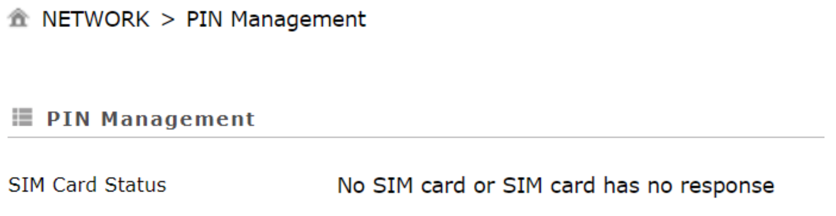
Working Mode	Manual
Dial Type	DHCP
User Name	
Password	
APN	
Authorization Mode	None
Dial-Up Number	*99#(UMTS/3G/3.5G/LTE/4G)
MTU	1492

Description	Default
Working Mode	
● **Auto:** The system will detect the operator from the inserted SIM card and set up the parameters accordingly. If the network is still disconnected, change Auto to Other mode. In this case, users need to manually input APN information obtained from the SIM card supplier. ● **Manual**: Users can set up the parameter manually, relevant parameters need to be obtained directly from the service supplier.	AUTO
Dial Type	
Only DHCP dialing type is supported currently.	DHCP
Username	
This username is provided by the operator. When selecting the "Auto" mode for the working mode, the system will automatically set up the name.	N/A
Password	
This password is provided by the operator. When selecting the "Auto" mode for the working mode, the system will automatically set up the password.	N/A
APN	
This Access Point Name is provided by the operator.	N/A
Authorization Mode	
You can choose "Auto”, “PAP" or "CHAP".	Auto
Dial-Up Number	
This number is provided by the operator.	*99#
MTU	
Set the maximum data packet size for network transmission.	1492

3.2.3 PIN Management

Users can view the status of the SIM card on the PIN Management page.

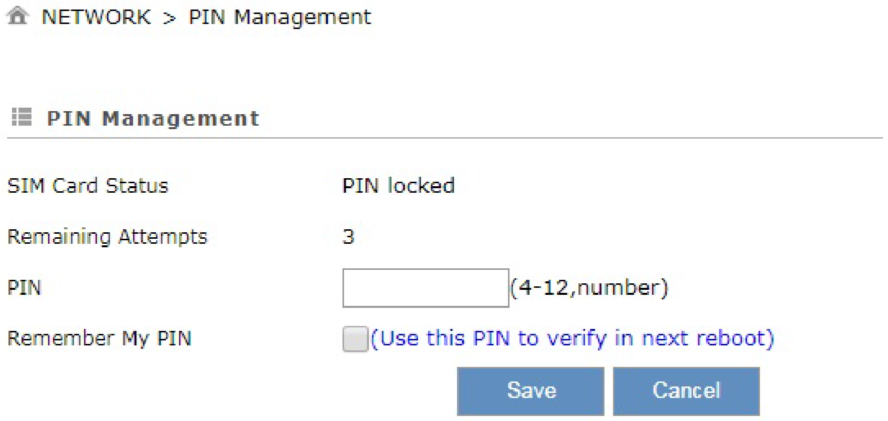
No SIM card or SIM card has no response


NETWORK > PIN Management

PIN Management

SIM Card Status No SIM card or SIM card has no response

Enter PIN code to unlock


NETWORK > PIN Management

PIN Management

SIM Card Status PIN locked

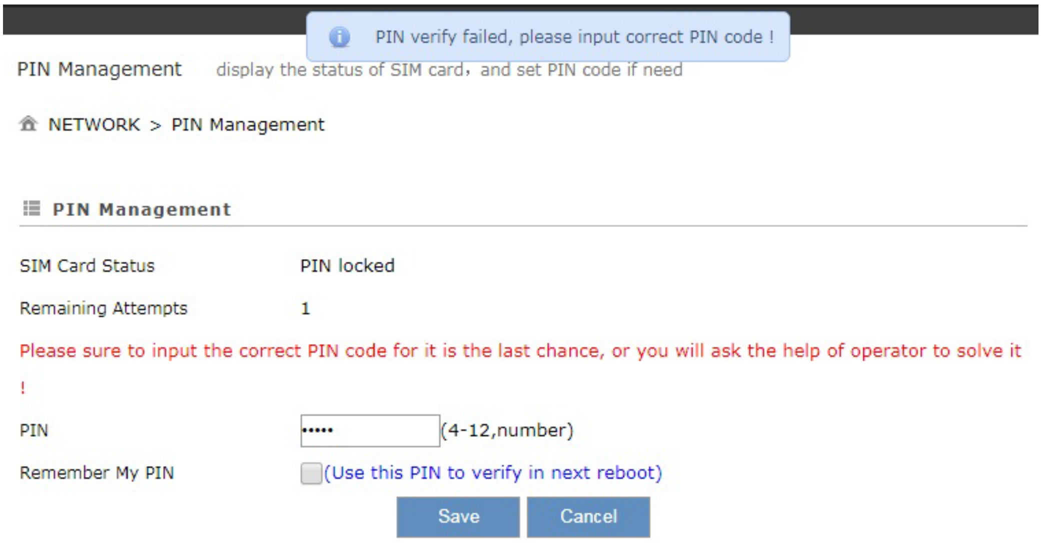
Remaining Attempts 3

PIN (4-12,number)

Remember My PIN □(Use this PIN to verify in next reboot)

⚠If the PIN is entered incorrectly three times, your SIM card will be locked. Once the SIM card is locked, you will need the PUK code to unlock it or seek assistance from the operator.

PIN verification failed


PIN verify failed, please input correct PIN code !

PIN Management display the status of SIM card, and set PIN code if need

NETWORK > PIN Management

PIN Management

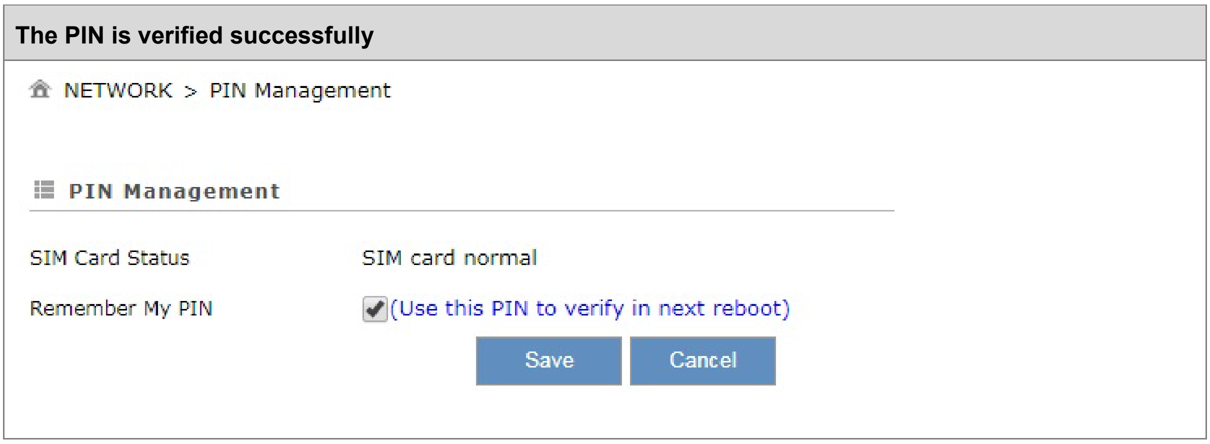
SIM Card Status PIN locked

Remaining Attempts 1

Please sure to input the correct PIN code for it is the last chance, or you will ask the help of operator to solve it !

PIN ••••• (4-12,number)

Remember My PIN □(Use this PIN to verify in next reboot)



The PIN is verified successfully

NETWORK > PIN Management

PIN Management

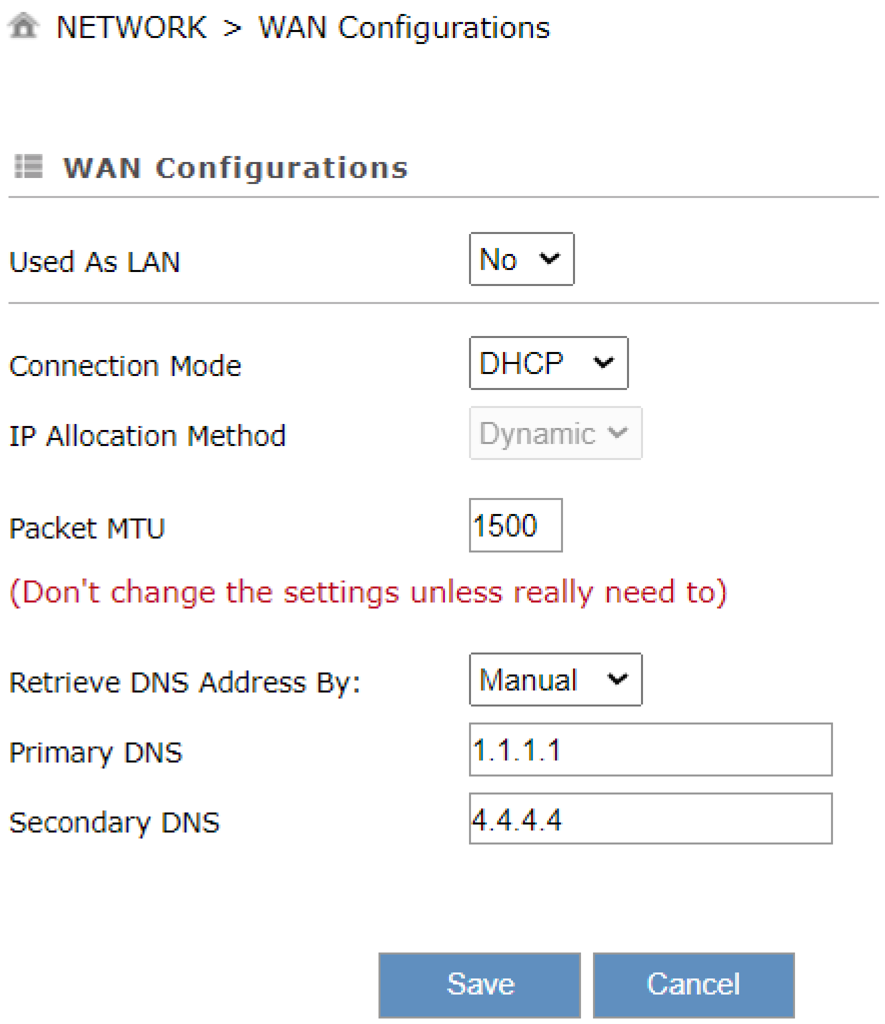
SIM Card Status SIM card normal

Remember My PIN ☑(Use this PIN to verify in next reboot)

Description	Default
SIM card status	
- **No SIM**：No SIM cards detected in the slot. - **SIM card normal**：The SIM card is in the slot and functions normally. - **PIN locked**：Need the correct PIN code input to enable the SIM card. - **PUK locked**：Exceed the maximum PIN code input tries. Need the correct PUK (Personal Unlocking Key) to unlock and resume normal operation.	N/A
Remaining attempts	
The allowable entry attempts are normally 3 times. When the remaining attempts is zero and the SIM card is locked, users must ask for help from operators or unlock it with PUK code.	N/A
PIN	
Enter the PIN code for this SIM card. You need to obtain the SIM card password from the operator.	N/A
Remember my PIN	
Enable this function to remember the PIN code in the system and the code would be input automatically every time after booting.	Uncheck

3.2.4 WAN Configurations

Users can configure WAN settings in this page, including configuring the access method, obtaining IP address method, IP address, subnet mask, gateway, and other information.



NETWORK > WAN Configurations

WAN Configurations

Used As LAN	No
Connection Mode	DHCP
IP Allocation Method	Dynamic
Packet MTU	1500

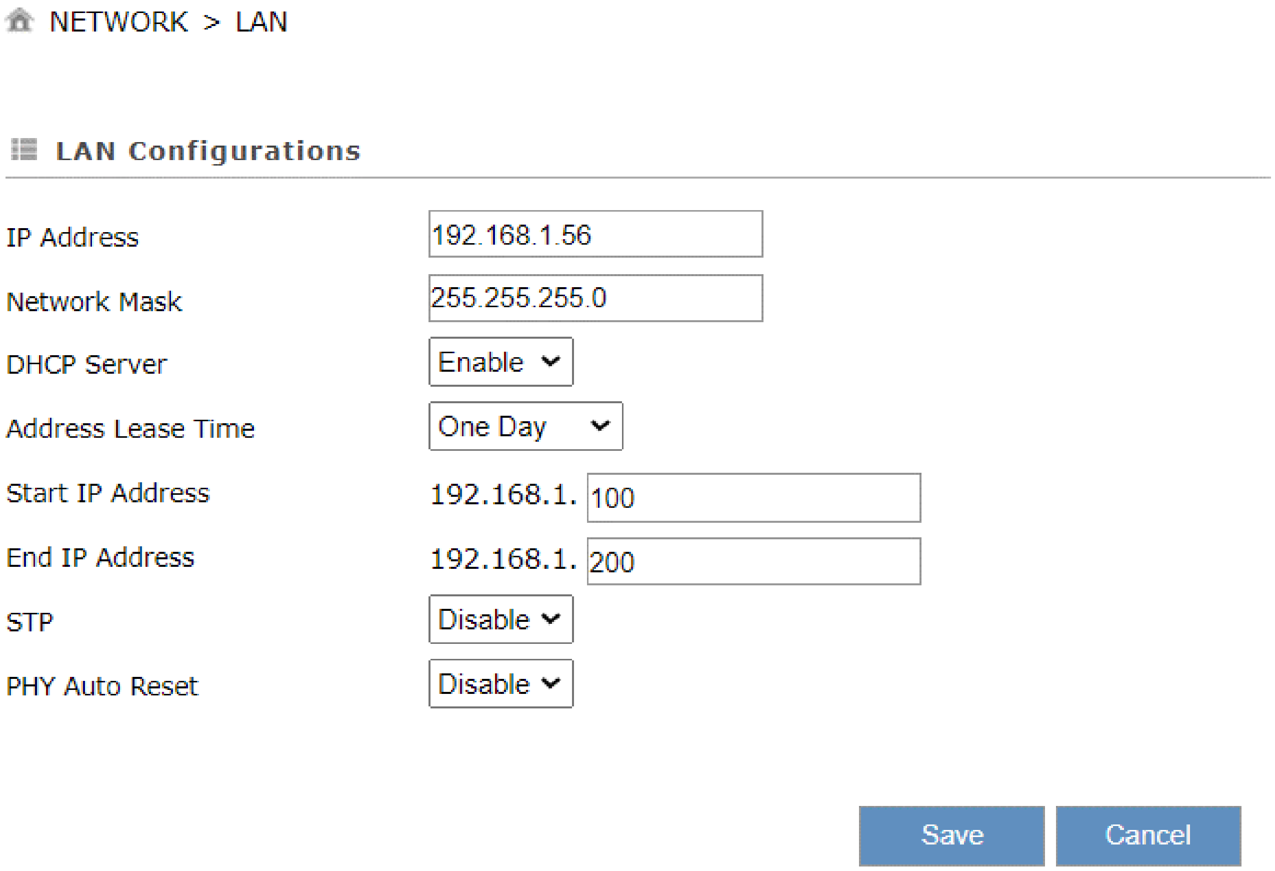
(Don't change the settings unless really need to)

Retrieve DNS Address By:	Manual
Primary DNS	1.1.1.1
Secondary DNS	4.4.4.4

Description	Default
Used As LAN	
Switch WAN port mode. ● **YES:** Switch the WAN port to a LAN port. ● **NO:** Keep LAN port.	NO
Connection Mode	
Set the WAN access method. Options are "**Dynamic IP Address**" and "**Static IP Address**". ● **Static IP Address:** Manually set up the IP address for Cloud router. ● **Dynamic IP Address:** Cloud router obtain an IP address automatically from DHCP Server.	Dynamic IP Address
IP Allocation Method	
Automatically match based on the connection mode: ● **DHCP**: Dynamically obtain IP address, subnet mask, gateway, and related information from the DHCP server. ● **Dynamic**: Manually set up IP address, subnet mask, gateway, and related information	DHCP
IP Address	
Set up the router's IP address for WAN access.	0.0.0.0
Network Mask	
Set the subnet mask for the router's LAN port.	0.0.0.0
Gateway Address	
Set up the router's gateway address for WAN access.	0.0.0.0
Packet MTU	
Set the Maximum Transmission Unit (MTU) for data packets.	1500
Retrieve DNS Address By	
When selecting the "Dynamic IP Address" access method, the DNS retrieval method can be either "Dynamic" or "Manually Specified." When selecting the "Static IP Address" access method, the DNS retrieval method can only be "Manually Specified."	DHCP
Primary DNS	
Set the IP address of Primary DNS for the router's WAN access.	0.0.0.0
Secondary DNS	
Set the IP address of Secondary DNS for the router's WAN access.	0.0.0.0

3.2.5 LAN Configurations

Users can configure LAN (Local Area Network) settings in this page, including configuring device names, IP address, subnet masks, DHCP servers, and other information.



NETWORK > LAN

LAN Configurations

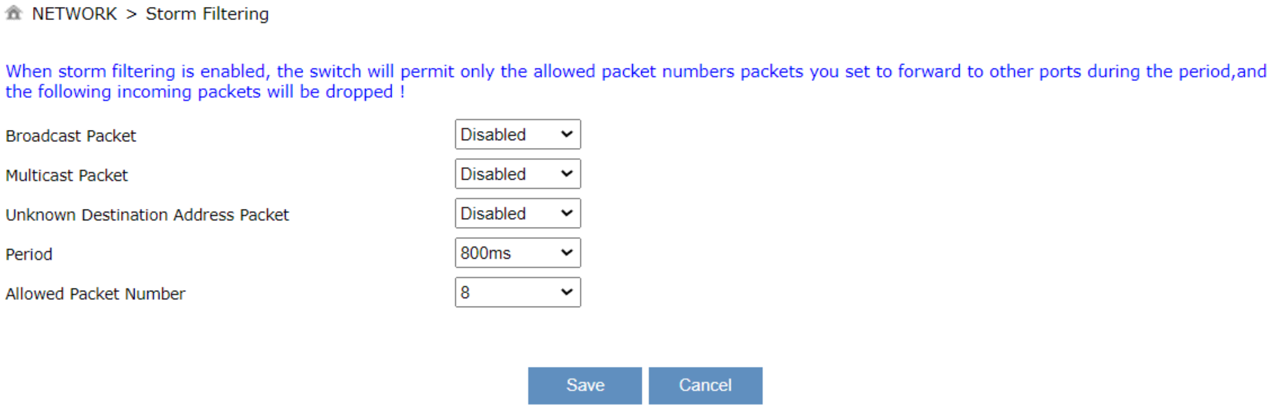
IP Address	192.168.1.56
Network Mask	255.255.255.0
DHCP Server	Enable
Address Lease Time	One Day
Start IP Address	192.168.1. 100
End IP Address	192.168.1. 200
STP	Disable
PHY Auto Reset	Disable

Description	Default
IP Address	
Set up the router's IP address for LAN access.	192.168.5.5
Network Mask	
Set the subnet mask for the router's LAN port.	255.255.255.0
DHCP Server	
DHCP server function switch, with options for "Enable" and "Disable".	Enable
Address Lease Time	
Configure the lease time for IP addresses assigned by the DHCP server, with options for "One day", "Two days" and "Three days."	One Day
Start IP Address	
Set the starting address of the IP range allocated by the DHCP server to the local network.	192.168.5.100
End IP Address	
Set the ending address of the IP range allocated by the DHCP server to the local network.	192.168.5.200
STP	
The purpose of Spanning Tree Protocol (STP) is to prevent the occurrence of network storms and subsequent network collapses in bridged networks. In the presence of a looped network topology, STP will select and disconnect one of the loops, establishing a loop-free tree-like topology structure for the network, thereby ensuring its stability. This prevents the continuous forwarding of packets in looped networks, which can lead to network storms, and ensures the normal operation of the network.	Disable
PHY Auto Reset	
After binding your DIACloud account, enable DIACloud DHCP. In the event of a manual reboot of cloud services or if cloud services reconnect due to unstable network conditions, determine whether automatic LAN port restart is required. ● **Disable**: Disable auto reboot on LAN port. ● **Enable**: Allow the LAN ports to automatically restart because of manual reboot of cloud services or when cloud services reconnect due to unstable network conditions, forcing the port devices to request DHCP from DIACloud. However, please note that this may result in temporary interruption of communication between the cloud router and LAN port devices. ⚠ It is recommended to disable the DIACloud DHCP functionality and use manual configuration for device IP address.	Disable

3.2.6 Storm Filtering

This page primarily focuses on configuring LAN storm control. Enabling this feature allows the system to restrict the flow of specific types of packets. When the broadcast (unknown unicast or multicast) storm control function is activated, within the user-defined timeframe, each port will only permit a user-defined quantity of consecutive data packets to be forwarded to other ports.

As shown in the following figure, within a period of 800 ms, each port will allow a maximum of 8 consecutive broadcast packets / unknown unicast / multicast packets (depending on user settings) to be forwarded to other ports. The excess would not be forwarded until there’s another packet being sent, or the current period is ended.



NETWORK > Storm Filtering

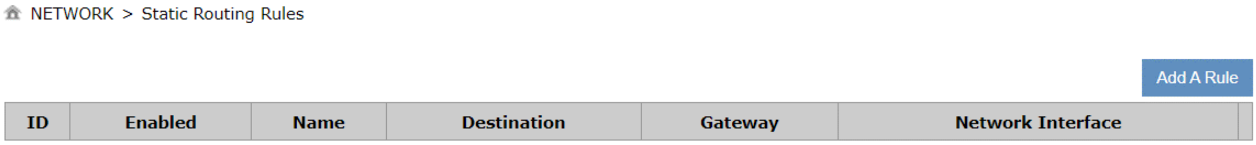
When storm filtering is enabled, the switch will permit only the allowed packet numbers packets you set to forward to other ports during the period,and the following incoming packets will be dropped !

Broadcast Packet	Disabled
Multicast Packet	Disabled
Unknown Destination Address Packet	Disabled
Period	800ms
Allowed Packet Number	8

Description	Default
Broadcast Packet	
Decide whether to enable storm control of broadcast packets.	Disable
Multicast Packet	
Decide whether to enable storm control of multicast packets.	Disable
Unknown Destination Address Packet	
Decide whether to enable storm control of unknown destination address packets.	Disable
Period	
Set the period of storm control with options of 800ms, 400ms, 200ms, and 100ms.	800ms
Allowed Packet Number	
Set the maximum number of packets permitted to be forwarded within a period. Options are 8, 16, 32, 64, and 256.	8

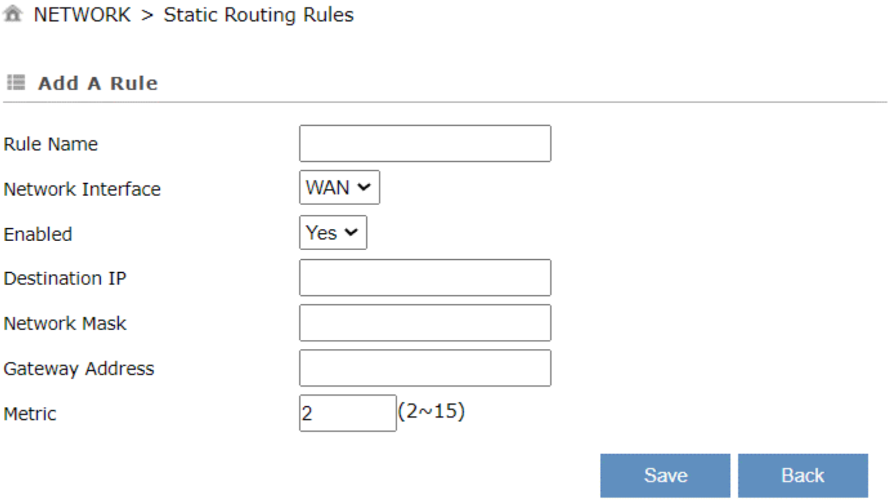
3.2.7 Static Routing Rules

Static routing is manually configured rather than determined dynamically. Unlike dynamic routing, static routes are fixed and do not change even if the network conditions have altered or have been reconfigured.



NETWORK > Static Routing Rules

ID	Enabled	Name	Destination	Gateway	Network Interface



NETWORK > Static Routing Rules

Add A Rule

Rule Name	
Network Interface	WAN
Enabled	Yes
Destination IP	
Network Mask	
Gateway Address	
Metric	2 (2~15)

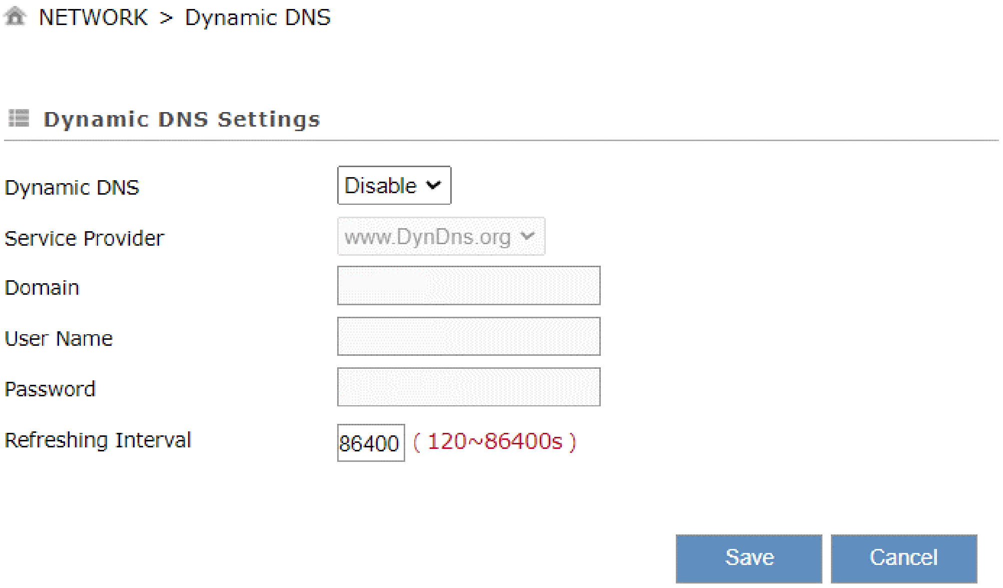
Description	Default
Add A Rule	
Add static routing rules, with a maximum limit of 10 entries.	N/A
Rule Name	
Set a name for your rule. The name shall be composed of letters, numbers, and underlines, starting with a letter or number, and the maximum length of the string is 32 bytes.	N/A
Network Interface	
For a specific network destination address, select the network interface of the router for sending data package. Options are LAN and WAN.	WAN
Enabled	
Active this static routing or not. Options are YES and NO.	YES
Destination IP	
Set up a Destination IP address for your device.	N/A

Description	Default
Network Mask	
Set the subnet mask corresponding to the destination network segment. If the destination of the routing is a single host, enter 255.255.255.255.	N/A
Gateway Address	
The address of another network connected by a router. It serves as an exit point to other networks, allowing data to be forwarded from one network to another. In simple terms, the Gateway Address is like a relay station for data transmission, used by the router.	N/A
Metric	
Metric is a value used to measure the priority or cost between different paths. It serves as a reference for routers to determine the best path. A lower metric value indicates a better or more preferred path. When a router needs to choose the best path, it compares the metric values of different paths and selects the path with the lowest metric value as the preferred route for data forwarding. The range is from 2~15.	2

3.2.8 Dynamic DNS

If the cloud router dose not have a static public IP address, Dynamic DNS service can be used. This service enables the cloud router to use the same domain name regarding to changeds in IP address in order to create connections with your router. Supported Dynamic DNS providers and related settings are as follows:

1. **www.dyndns.org**: https://help.dyn.com/remote-access/getting-started-with-remote-access/
2. **www.noip.com:** https://www.noip.com/support/knowledgebase/getting-started-with-no-ip-com/


NETWORK > Dynamic DNS

Dynamic DNS Settings

Dynamic DNS: Disable

Service Provider: www.DynDns.org

Domain:

User Name:

Password:

Refreshing Interval: 86400 (120~86400s)

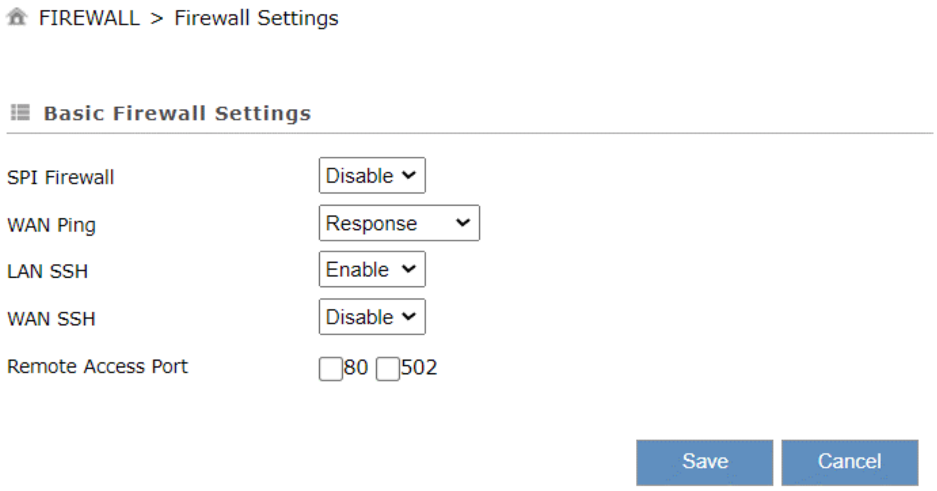
Description	Default
Dynamic DNS	
Dynamic DNS service function switch, options are “Enable” and “Disable”.	Disable
Service Provider	
Select the Dynamic DNS service provider, Options are www.DynDNS.org and “http://www.NOIP.com”	www.DynDns.org
Domain	
The domain applied for to the corresponding dynamic domain service provider.	N/A
Username	
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

3.3 FIREWALL

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

3.3.1 Firewall Settings

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


FIREWALL > Firewall Settings

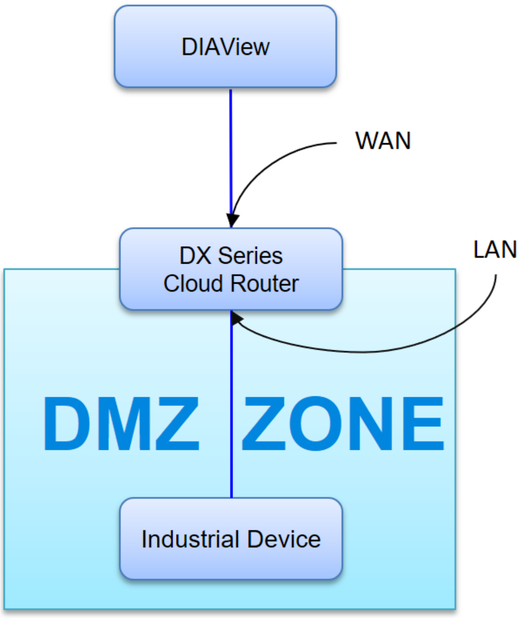
Basic Firewall Settings

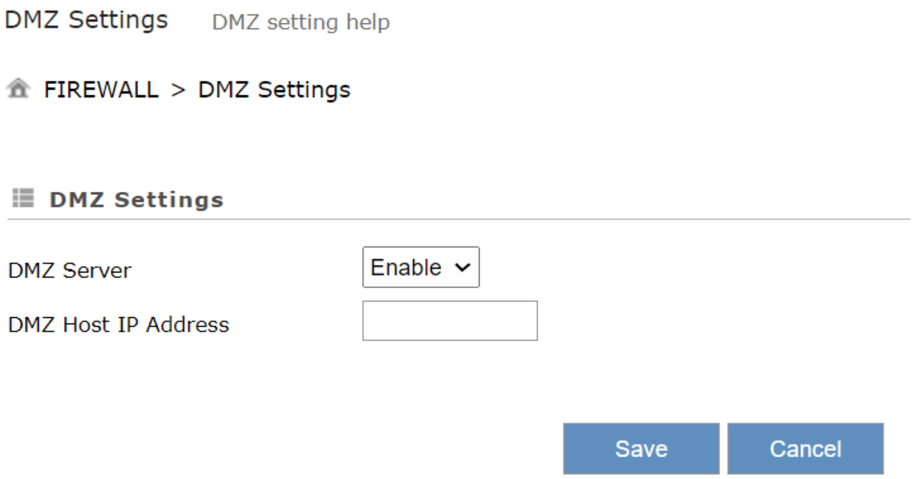
SPI Firewall: Disable
WAN Ping: Response
LAN SSH: Enable
WAN SSH: Disable
Remote Access Port: □80 □502

Description	Default
SPI Firewall	
Firewall function switch, options are “Enable” and “Disable”.	Enable
WAN Ping	
Whether to respond to external network with the IP obtained from the WAN IP. By default, it is set not to respond in order to conceal the device's identity on the Internet. However, there are situations where it may be necessary to test if the IP is reachable. In such cases, user can enable it.	Not responded
LAN SSH	
Set up whether to allow LAN end to connect with the router via SSH, options are “Enable” and “Disable”.	Enable
WAN SSH	
Set up whether to allow WAN end to connect with the router via SSH, options are “Enable” and “Disable”.	Disable
Remote Access Port	
Users can use the public WAN IP address obtained, along with port 80 or 502, to perform configuration from external networks. ● **Port 80**: Access the configuration page of this DX router. ● **Port 502**: External devices use MODBUS Client to connect to this device's MODBUS TCP Server, enabling them to read data from MODBUS slave devices.	Uncheck

3.3.2 DMZ Settings

All data sent through WAN IP address or WAN port will be forwarded to another IP address specified by DMZ.




DMZ Settings DMZ setting help

FIREWALL > DMZ Settings

DMZ Settings

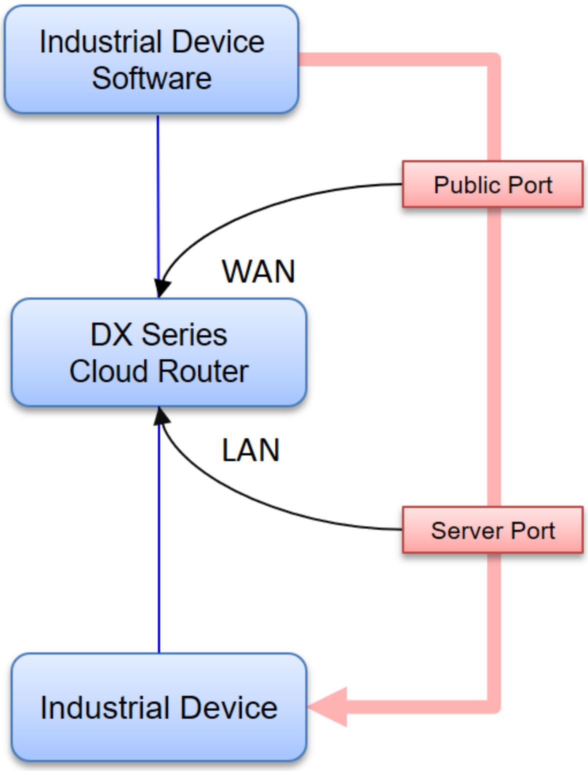
DMZ Server: Enable

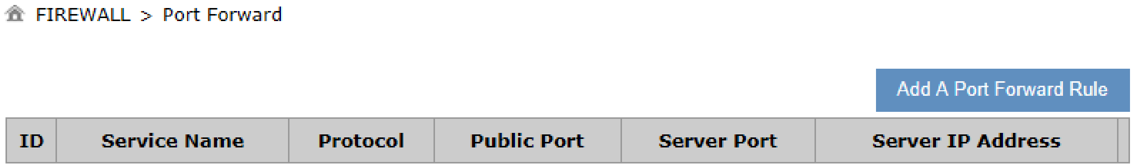
DMZ Host IP Address:

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

3.3.3 Port Forward

Data sent through the specified WAN network port is forwarded to the designated network port and IP location. This is for scenarios where external devices need to establish connections with local LAN devices of the cloud router.



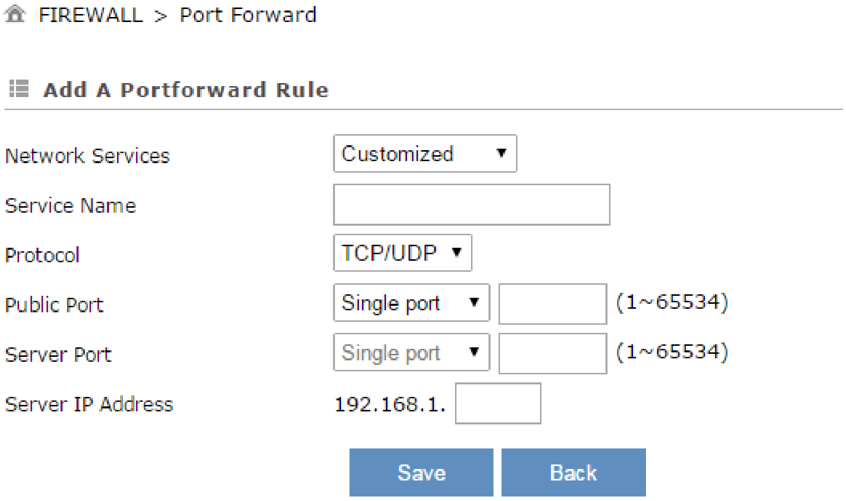


FIREWALL > Port Forward

Add A Port Forward Rule

ID	Service Name	Protocol	Public Port	Server Port	Server IP Address

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

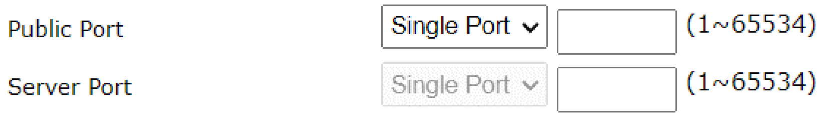
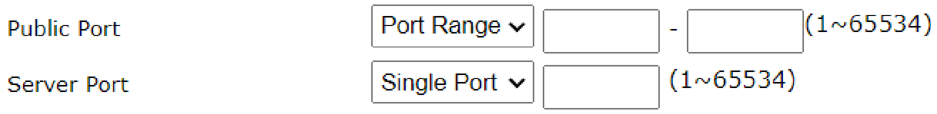
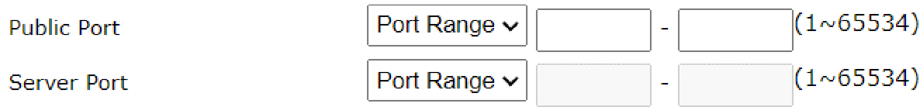


FIREWALL > Port Forward

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.

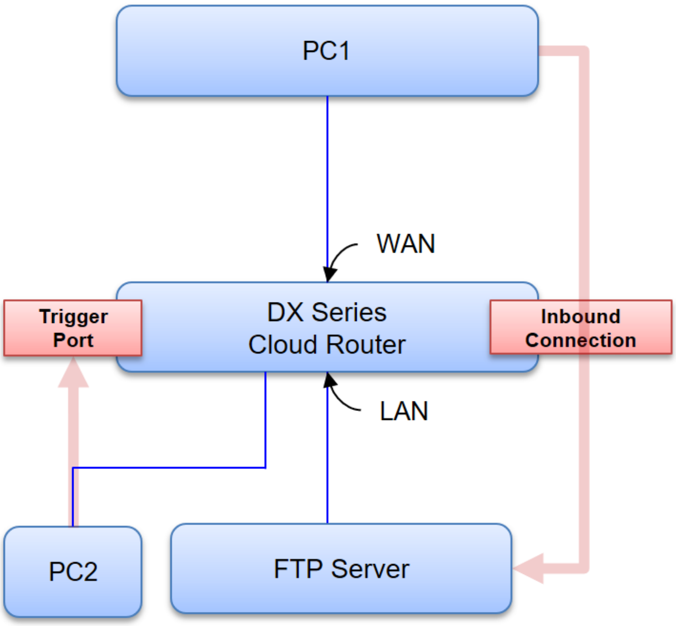
Save Back

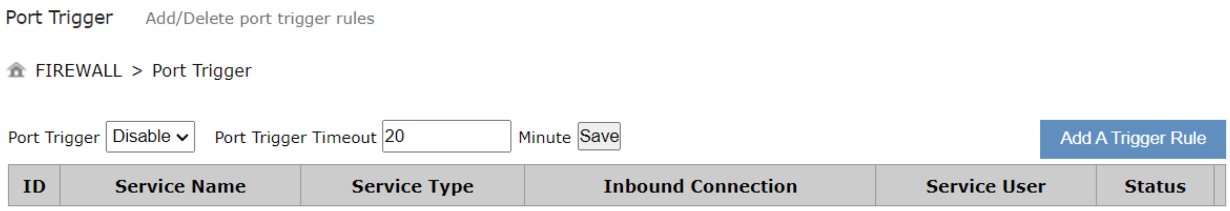
Description	Default
Add A Port Forward Rule	
Add a new Port Forward rule, with a maximum of 10 rules available.	N/A
Network Services	
Select commonly used network services; available options are listed in the following common services list.	Customized
Service Name	
Set up the service name for port forwarding. 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, options are “TCP/UDP”, “TCP”, “UDP”.	TCP/UDP
Public Port	
Configure the external host (i.e., router) ports, which can be specified as either a 'single port' or a 'port range'; when selecting a port range, the range is from 1 to 65534, and the starting port must be less than or equal to the ending port	Single Port / N/A
Server Port	
Set up the internal server ports: 1. When the public port is set to "Single Port" mode, the server port can only be selected as a "Single Port. 2. When the public port is set to "Port Range" mode, the server port can be selected as either a "Single Port" or a "Port Range." 3. If "Single Port" is chosen, all public port ranges will be forwarded to a single port. 4. If "Port Range" is chosen, the port range will match the public port range, and a one-to-one forwarding will be established. Example of different port forwarding settings: ● 1:1 mode  Public Port Single Port ▾ (1~65534) Server Port Single Port ▾ (1~65534) ● N:1 mode  Public Port Port Range ▾ - (1~65534) Server Port Single Port ▾ (1~65534) ● N:Nmode  Public Port Port Range ▾ - (1~65534) Server Port Port Range ▾ - (1~65534)	Single Port
Server IP Address	
Set up the server IP address that applies to the port mapping rule.	192.168.1.*

Common Service List for Port Forwarding			
Service name	**Protocol**	**Starting Port**	**Ending Port**
Customized	TCP, UDP, TCP/UDP	1~65534	1~65534
FTP	TCP	20	21
HTTP	TCP	80	80
ICUII	TCP	23566	23566
IP_PHONE	TCP	6670	6670
NetMeeting	TCP	1720	1720
News	TCP	119	119
PPTP	TCP/UDP	1723	1723
Telnet	TCP	23	23
QuakeII/III	TCP/UDP	27960	27960
Real-Audio	TCP	6970	7170

3.3.4 Port Trigger

After PC2 triggers a specific port, PC1 can establish a connection with devices under the cloud router within a limited time frame.

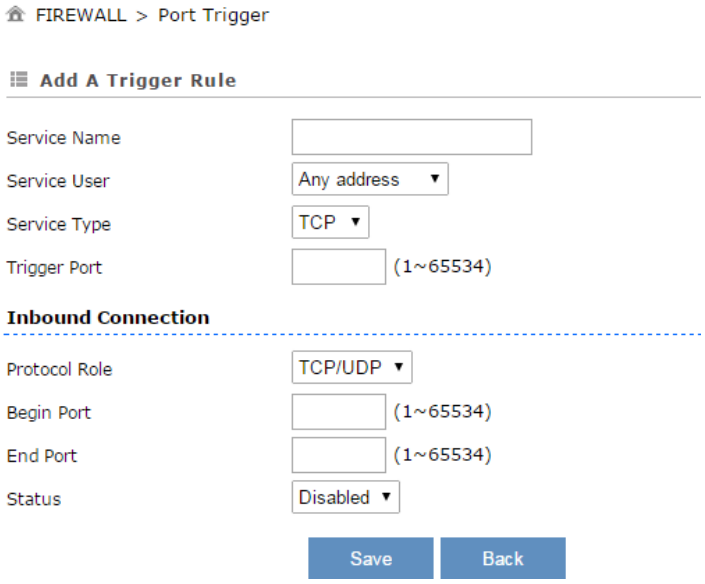



Port Trigger Add/Delete port trigger rules

FIREWALL > Port Trigger

Port Trigger Disable Port Trigger Timeout 20 Minute Save

ID	Service Name	Service Type	Inbound Connection	Service User	Status


FIREWALL > Port Trigger

Add A Trigger Rule

Service Name	
Service User	Any address
Service Type	TCP
Trigger Port	(1~65534)

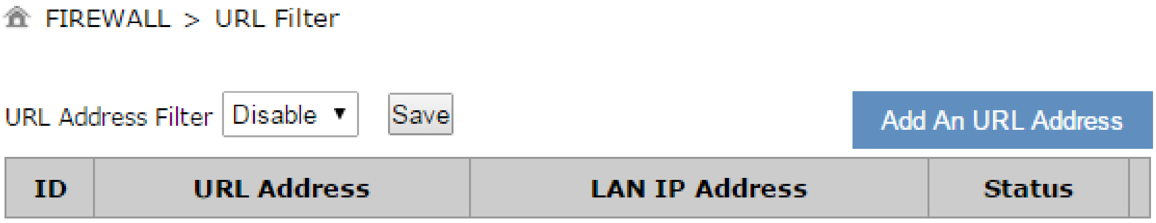
Inbound Connection

Protocol Role	TCP/UDP
Begin Port	(1~65534)
End Port	(1~65534)
Status	Disabled

Description	Default
Add A Trigger Rule	
Add a new Port Trigger rule, with a maximum of 10 rules available.	N/A
Port Trigger	
Port Trigger function switch, options are “Enable” and “Disable”.	Disable
Port Trigger Timeout	
Setting up the connection time after triggering the port.	20
Service Name	
Set up the service name for port trigger. 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 Port Trigger Rule Service User, options are “Single Address” or “Any Address”.	Any Address
Service Type	
Select the protocol type for port triggering, options are “TCP”, “UDP”.	TCP
Trigger 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, options are “TCP”, “UDP”.	TCP/UDP
Begin Port	
Set up the starting port for the inbound connection, the port range is 1~65534.	N/A
End Port	
Set up the ending port for the inbound connection, the port range is 1~65534.	N/A
Status	
Enable/Disable the status of port triggering.	Disable

3.3.5 URL Filter

This page is used for setting up the URL Filter, including URL Address, LAN IP Address and Status. Users can add URL filtering entries to the router by clicking on "Add an URL Address".

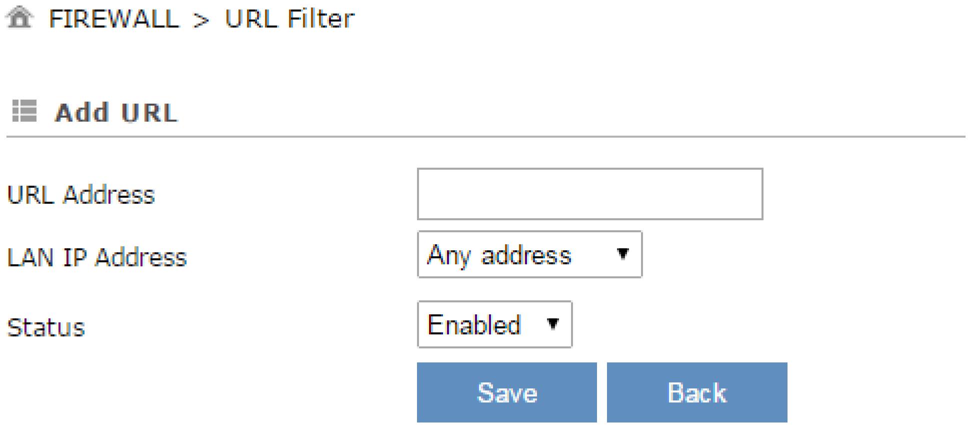


FIREWALL > URL Filter

URL Address Filter: Disable

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:

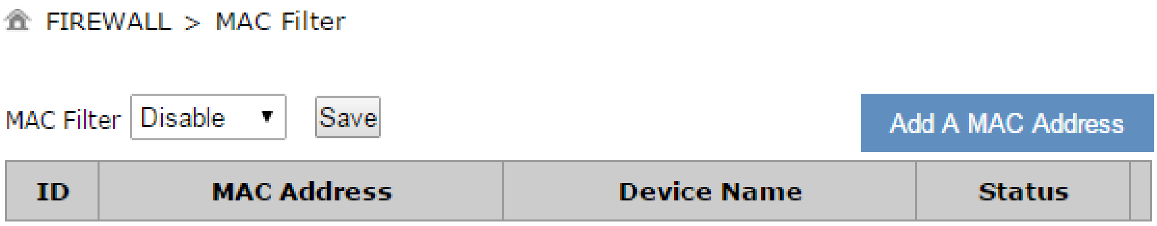
LAN IP Address: Any address

Status: Enabled

Description	Default
Add an URL Address	
Add URL Address Rule, with a maximum of 10 rules available.	N/A
URL Address Filter	
URL Address Filter function switch, options are “Enable”and “Disable”.	Disable
URL Address	
Configure the URL address to be filtered, such as www.baidu.com.	N/A
LAN IP Address	
Set the local LAN IP address range for URL filtering, options are "Any Address", "Single Address", "Address Range".	Any Address
Status	
Set the current status of this filtering rule, options are “Enable” and “Disable”.	Enable

3.3.6 MAC Filter

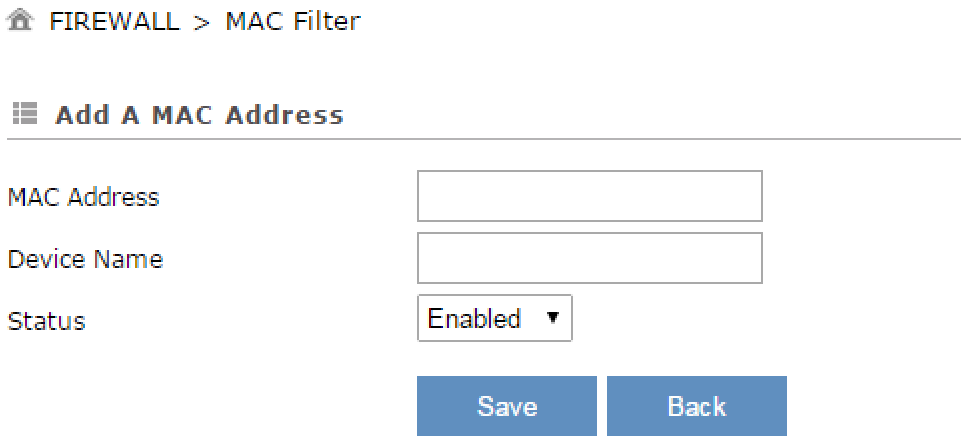
This page is used for setting up the MAC Filter, including the MAC Address, Device Name and Status. Users can add MAC filtering entries to the router by clicking on "Add a MAC Address".



FIREWALL > MAC Filter

MAC Filter: Disable

ID	MAC Address	Device Name	Status



FIREWALL > MAC Filter

Add A MAC Address

MAC Address:

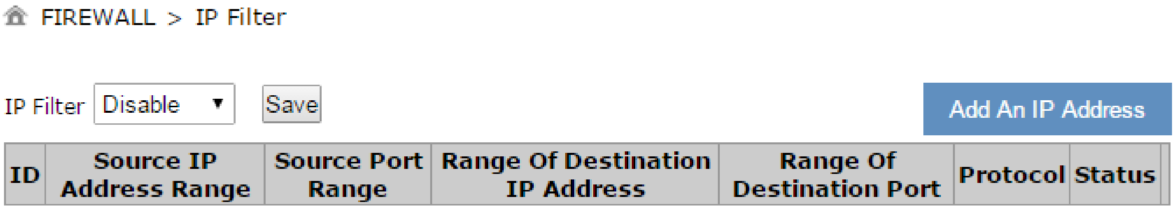
Device Name:

Status: Enabled

Description	Default
Add A MAC Address	
Add MAC Address, with a maximum of 10 addresses available.	N/A
MAC Filter	
MAC Filter function switch, options are "Disable Function" and "Forbidden List".	Disable Function
MAC Address	
Configure MAC address to be filtered.	N/A
Device Name	
Set the corresponding device name for this MAC address.	N/A
Status	
Set the current status of this filtering rule, options are “Enable” and “Disable”.	Enable

3.3.7 IP Filter

This page is used for setting up the IP Filter, including the Source IP Address, Source Port, Destination IP, Desination Port, Protocol and Status. Users can add IP filtering entries to the router by clicking on "Add an IP Address".



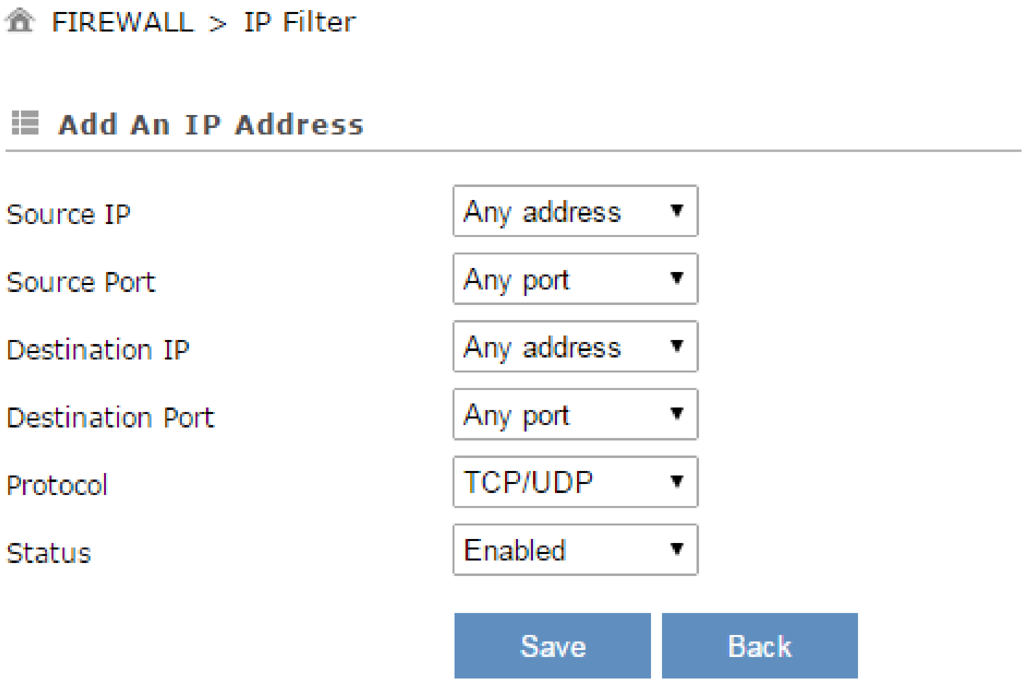
FIREWALL > IP Filter

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 ▼

Description	Default
Add an IP Address	
Add IP Address Filter Rule, with a maximum of 10 rules available.	N/A
IP Address Filter	
IP Address Filter function switch, options are "Disable Function" and "Forbidden List".	Disable Function
Source IP	
Set up the source IP, options are "Any Address", "Single Address", "Address Range".	Any Address

Description	Default
Source Port	
Set up the source port, options are "Any Port", "Single Port", "Port Range".	Any Port
Destination IP	
Set up the destination IP, options are "Any Address", "Single Address", "Address Range".	Any Address
Destination Port	
Set up the destination port, options are "Any Port", "Single Port", "Port Range".	Any Port
Protocol	
Select the protocol type for the IP Filter, options are “TCP/UDP”, “TCP”, “UDP”.	TCP/UDP
Status	
Set the current status of this filtering rule, options are “Enable” and “Disable”.	Enable

3.4 INTERFACE

You can set up the interface configurations, including the RS-232, RS-485, Modbus TCP, DI/DO and USB interface.

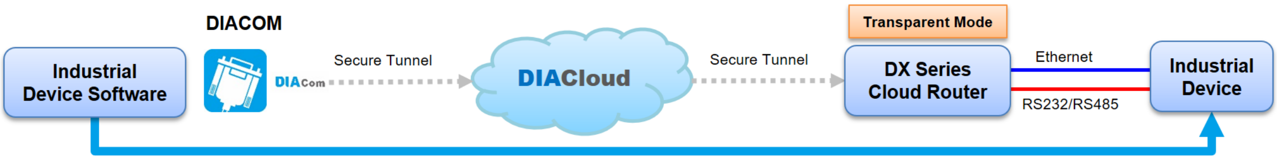
3.4.1 RS-232 /RS-485

RS-232/RS-485 (Recommended Standard – 232/485) is a telecommunication standard for binary serial communications between devices. It supports seven work modes, include: Transparent mode, Slave mode, Master mode, Serial Server-TCP Server, Serial Server-TCP Client, Serial Server-UDP Client and MC Master mode.

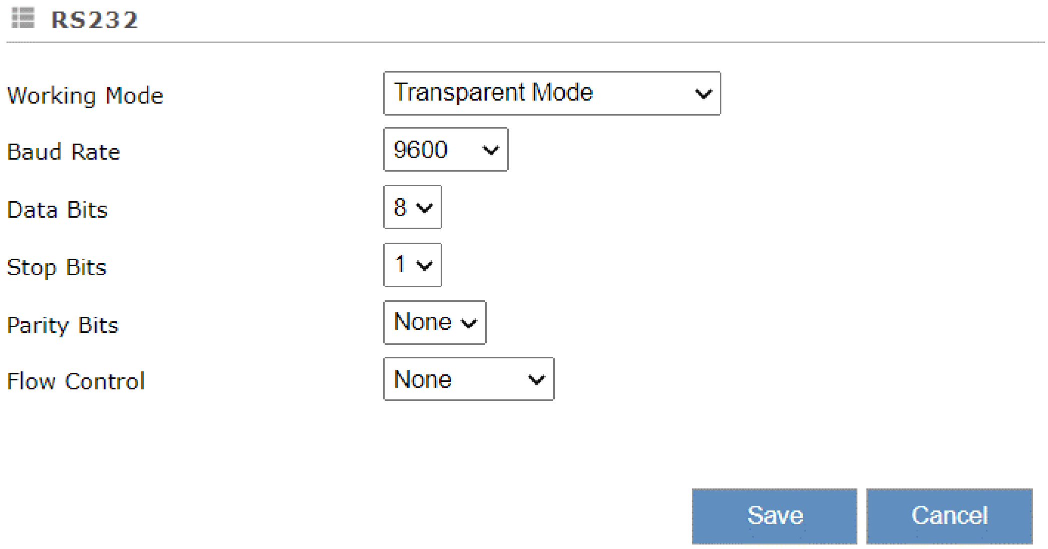
You can set up the configurations for RS-232/RS-485, including Baud Rate, Data Bits, Stop Bits, Parity Bits and Flow Control.

3.4.1.1 Transparent Mode

With DIACom Software, transparent mode allows users to perform remotely uploads, downloads, and other operations on devices connected to the cloud router via the RS-232/RS-485 serial port using a remote virtual serial port.

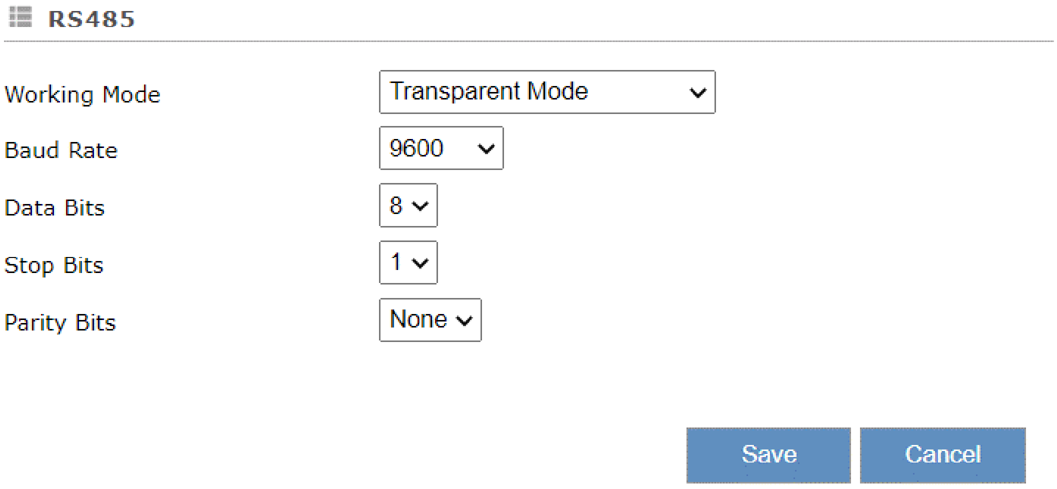


Remote connection function



RS232

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



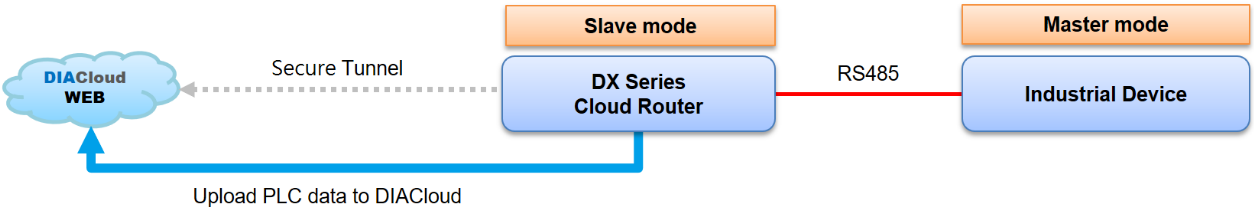
RS485

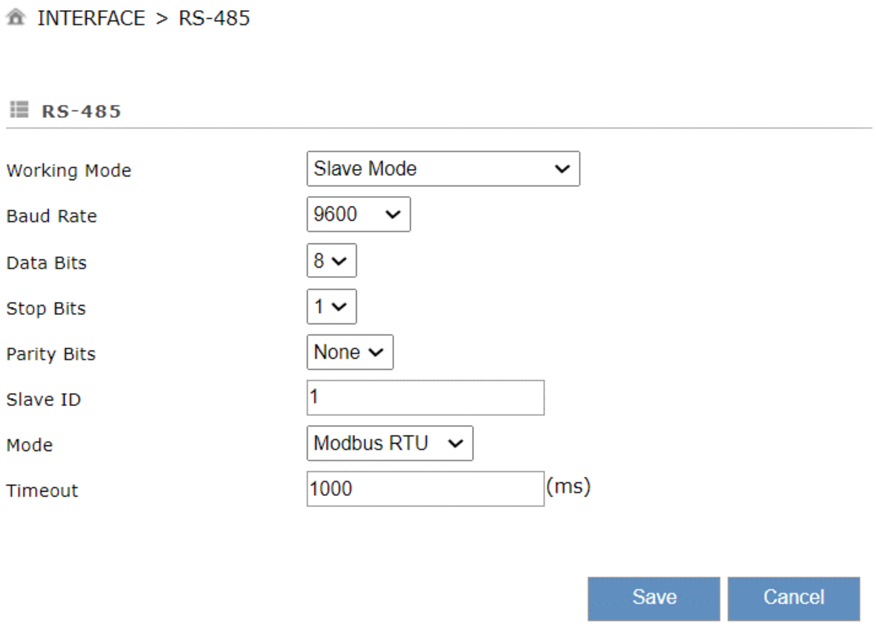
Working Mode	Transparent Mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None

Description	Default
Working Mode	
● RS-232 Mode 1. Close 2. **Transparent Mode** 3. Slave Mode 4. Master Mode 5. Serial Server –TCP Server 6. Serial Server –TCP Client 7. Serial Server –UDP Client 8. MC Master Mode ● RS-485 Mode: 1. Close 2. **Transparent Mode** 3. Slave Mode 4. Master Mode 5. Serial Server –TCP Server 6. Serial Server –TCP Client 7. Serial Server –UDP Client	Close
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. Options are 7 and 8. It must be set to 8 when communication mode is 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
Flow Control	
Set up the flow control. Options are None, “XON/XOFF”, “RTS/CTS”.	None

3.4.1.2 Slave Mode

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

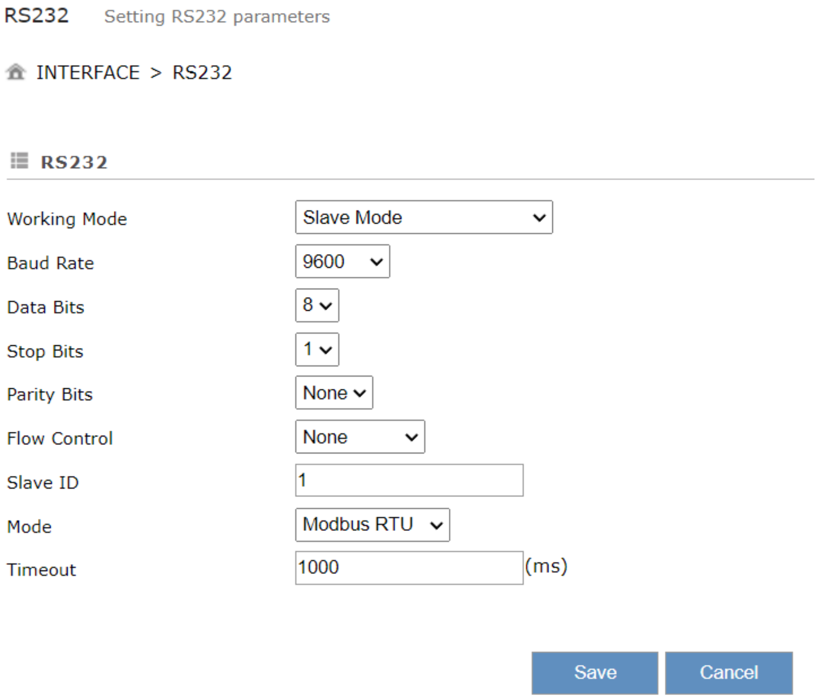




INTERFACE > RS-485

RS-485

Working Mode	Slave Mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Slave ID	1
Mode	Modbus RTU
Timeout	1000 (ms)



RS232 Setting RS232 parameters

INTERFACE > RS232

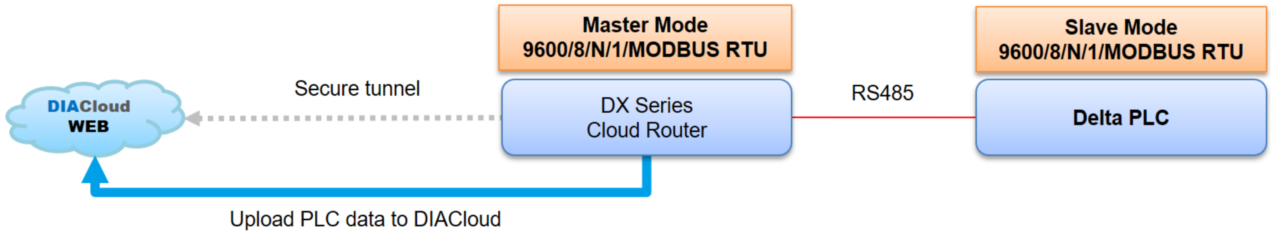
RS232

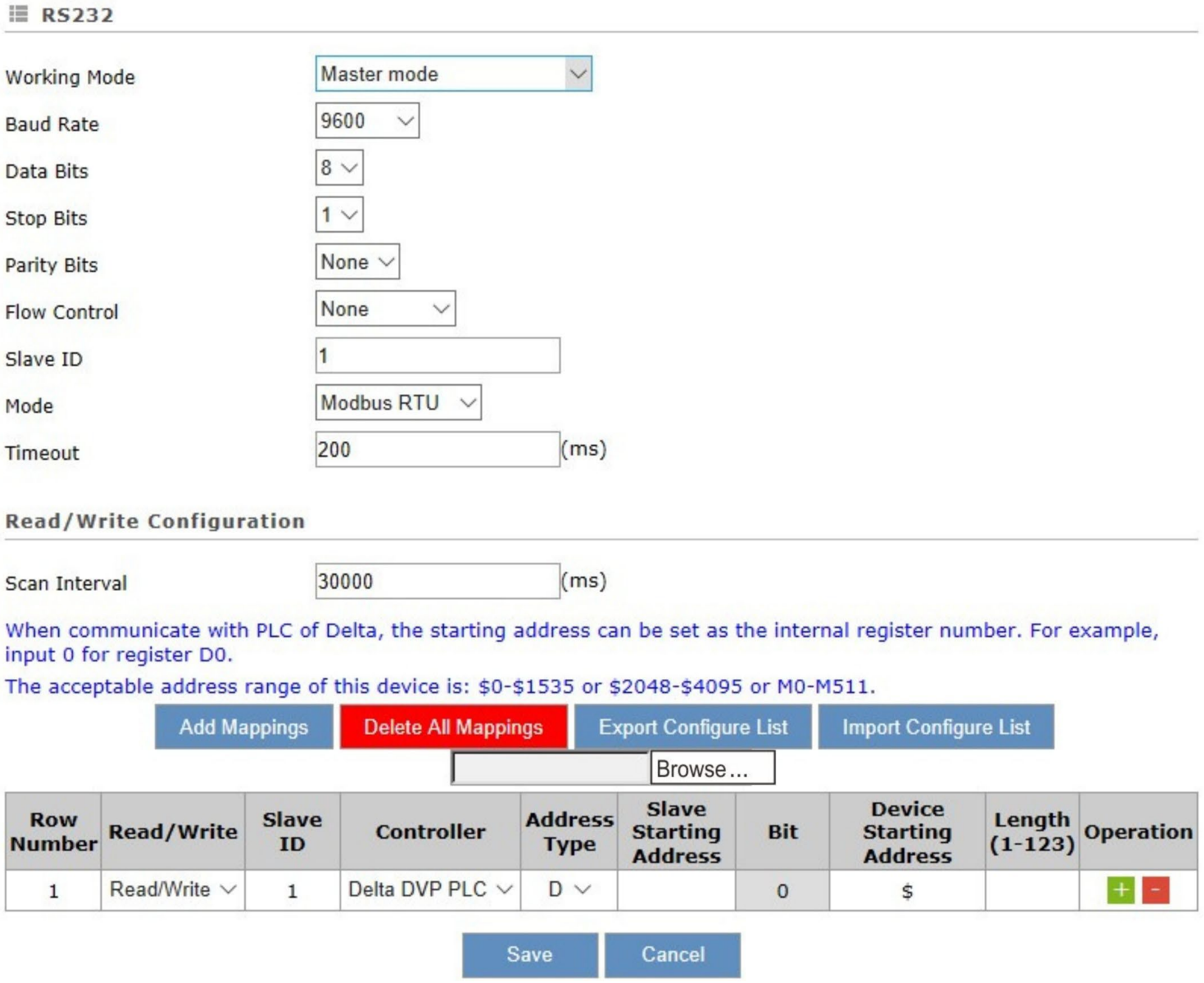
Working Mode	Slave Mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Flow Control	None
Slave ID	1
Mode	Modbus RTU
Timeout	1000 (ms)

Description	Default
Working Mode	
● RS-232 Mode **1.** Close **2.** Transparent Mode **3.** **Slave Mode** **4.** Master Mode **5.** Serial Server –TCP Server **6.** Serial Server –TCP Client **7.** Serial Server –UDP Client **8.** MC Master Mode ● RS-485 Mode: **1.** Close **2.** Transparent Mode **3.** **Slave Mode** **4.** Master Mode **5.** Serial Server –TCP Server **6.** Serial Server –TCP Client **7.** Serial Server –UDP Client	Close
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. Options are 7 and 8. It must be set to 8 when communication mode is 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
Flow Control	
Set up the flow control. Options are None, “XON/XOFF”, “RTS/CTS”.	None
Slave ID	
Set up the MODBUS ID. The value is between 1 and 247.	1
Mode	
Set up the communication mode for the device. Device support Modbus RTU and Modbus ASCII	Modbus RTU
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.	200

3.4.1.3 Master Mode

In this mode, it is allowable for Cloud router to perform the read/ write tasks on the open register of the slave device via RS-232/RS-485 to achieve bidirectional data transmission.





RS232

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

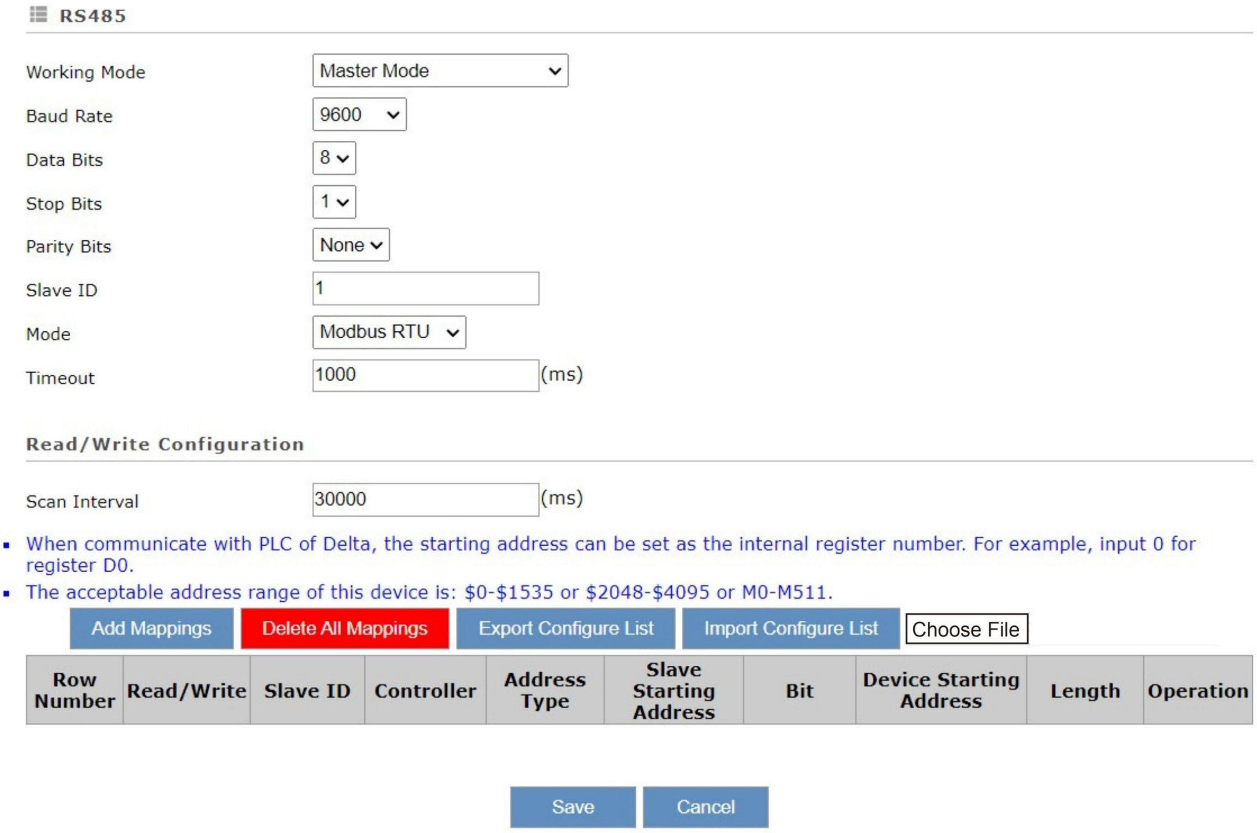
Read/Write Configuration

Scan Interval	30000 (ms)

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

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

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



RS485

Working Mode	Master Mode
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Slave ID	1
Mode	Modbus RTU
Timeout	1000 (ms)

Read/Write Configuration

Scan Interval: 30000 (ms)

- When communicate with PLC of Delta, the starting address can be set as the internal register number. For example, input 0 for register D0.
- The acceptable address range of this device is: $0-$1535 or $2048-$4095 or M0-M511.

Row Number	Read/Write	Slave ID	Controller	Address Type	Slave Starting Address	Bit	Device Starting Address	Length	Operation

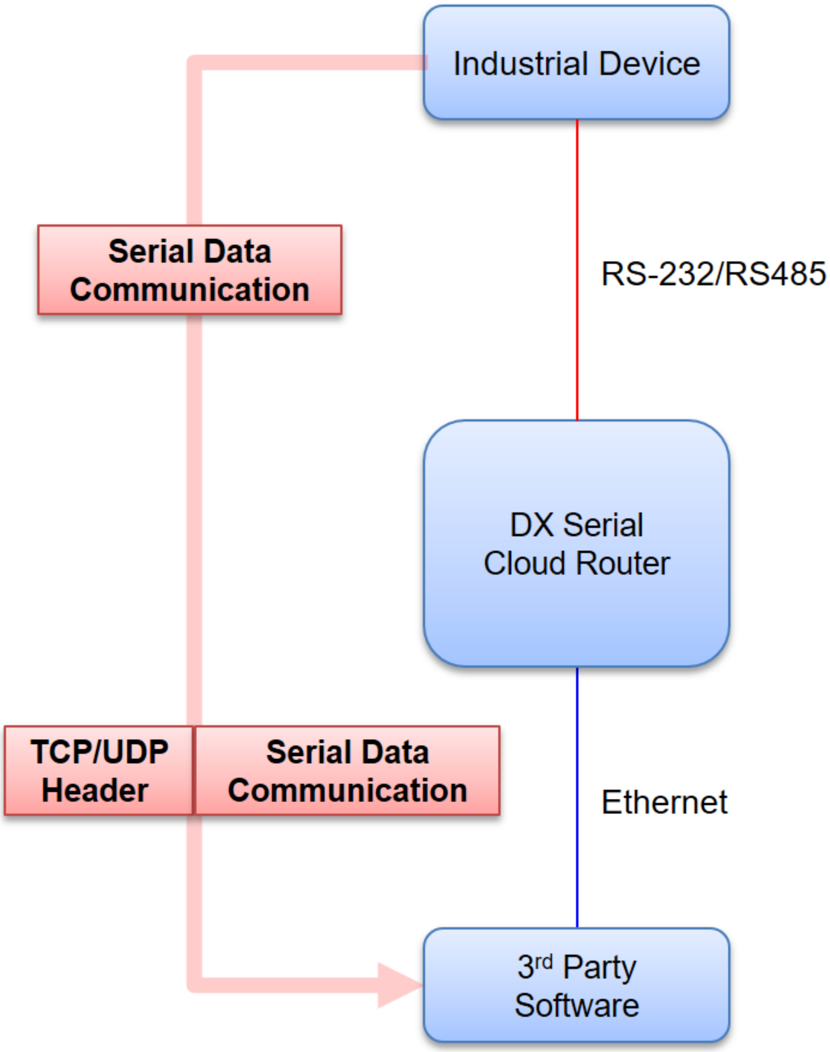
Description	Default
Slave ID	
Set up the MODBUS ID, for Cloud router with value between 1 and 247. No need to set in master station mode.	1
Communication Mode	
Select the communication mode for the device. Options are "Modbus RTU" and "Modbus ASCII."	Modbus RTU
Timeout	
Set up the timeout timer from 200ms to 5000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	200ms
Scan Interval	
Set up the time for scan interval, the interval refers to the time span between the conclusion of the previous polling cycle and the commencement of a new polling cycle.	30000ms
Add Mappings	
Once the user configures the mapping relationship between the device address and the cloud router register, the system will gather data from the connected device based on the established mapping relationship.	N/A
Delete All Mappings	
Clear all existing mapping relationships in RS-232 master mode.	N/A

Description	Default
Export Configure List	
Export the existing mapping relationships and save the file to the local computer.	N/A
Import Configure List	
The mapping list can be imported for RS-232/RS-485/MODBUS TC/MC/SIEMEN TCP communication interfaces. A total of 600 mapping addresses are shared among all communication interfaces. ⚠**Notcie:** ● Each communication interface can import a maximum of 600 mapping addresses. If RS-232 already has 10 configured mapping addresses and an import of 600 mapping addresses is performed from RS-232, the previously set 10 mapping addresses will be overwritten. ● If RS-232 has 10 mapping addresses, then the maximum import of mapping addresses from RS-485/MODBUS TCP is limited to 590. If the number exceeds 590, a warning message will be displayed.	N/A
Read/Write	
Set up the mapping relationship is for "Read/Write", "Read-only" or "Write-only". ● Read-only: Automatically read data from the mapped slave device address according to the scanning cycle and update it to the corresponding register in the cloud router. ● Write-only: When the value of the cloud router's register is changed, the latest value will be automatically written to the corresponding slave device address. ● Read/Write: Periodically read data from the slave device, then update it to the corresponding register in the cloud router. When the value of the register is changed, the latest value will also be automatically written to the corresponding slave device address.	Read/Write
Slave ID	
Set up the corresponding slave communication station number. The value is between 1 to 247.	1
Controller	
In master mode, device types' of options: ● **Delta PLC:** Please use this option for Delta DVP/AH/AS series PLC. ● **Other:** For non-Delta DVP/AH/AS series PLCs, please use this option. "HEX" represents inputting hexadecimal addresses, while "DEC" represents inputting decimal addresses.	Delta DVP PLC
Address Type	
In master mode, the options vary based on the selected controller type.: ● **Delta PLC:** The URL classification types are D/M/S/X/Y, where D represents word type and M/S/X/Y represent bit type. ● **Other:** The URL classification types are 0x/1x/3x/4x/Swap a) 0x: Read or write coils data (Modbus function code: 01/05) b) 1x: ReadDiscrete Inputs (Modbus function code: 02)	D

Description	Default
c) 3x: Read or writeInput Registers (Modbus function code: 04) d) 4x: Read or writeHolding Registers (Modbus function code: 03/16) e) Swap: Read or writeHolding Registers, during processing, start from the first register, grouping them in pairs. The previous Word and the subsequent Word are swapped with each other.	
Slave Starting Address	
Set the starting address of the slave device registers for read/write operations. Master Mode： ● **Delta PLC:** Enter the internal D register number, for example, enter 0 for D0 or enter 12 for M12. ● **Other:** Enter the actual address in hexadecimal or decimal format. To retrieve the holding register 400100, take the last four digits: 0100 (decimal) or 64 (hexadecimal).	N/A
Bit	
For the Delta AH/AS series X/Y types, the address input format is 0.0 ~ X.15. The part before the decimal point should be entered in the slave device's starting address field, while the part after the decimal point should be entered in this field.	N/A
Device Starting Address	
Set the starting register address for the device mapping. For word type, the range is $2048 to $4095; for bit type, the range is M0 to M511. When entering the register address, it must start with "$" or "M" and use the decimal addressing format.	N/A
Length	
Set the length, which specifies how many consecutive registers' data to read/write from the starting address. The range is from 1 to 123.	N/A
Operation	
Click the +/- button to add mapping or delete mapping.	N/A
Edit	
You can directly click on a specific column to edit its content.	N/A

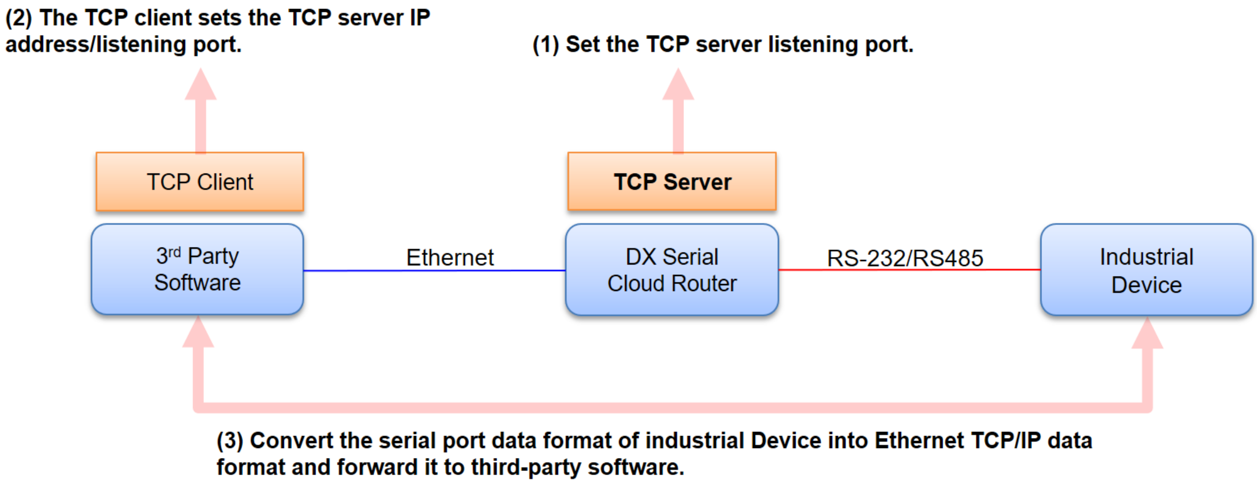
3.4.1.4 Introduction to Serial Server

A serial server is a device that converts data from a serial port (such as RS-232 or RS-485) into the TCP/IP protocol for transmission over an Ethernet network. The purpose of this is to achieve bidirectional data transfer between serial and TCP/IP protocols, enabling serial devices to immediately possess TCP/IP networking capabilities and communicate data over a network connection, while also extending the communication distance of serial devices. The primary function of a serial server is to transform serial messages into TCP/UDP format and forward the data to the respective destination. In other words, it acts as an intermediary transmitter, encapsulating serial data into a network-recognizable format and forwarding it to the appropriate destination.



3.4.1.5 Serial Server – TCP Server

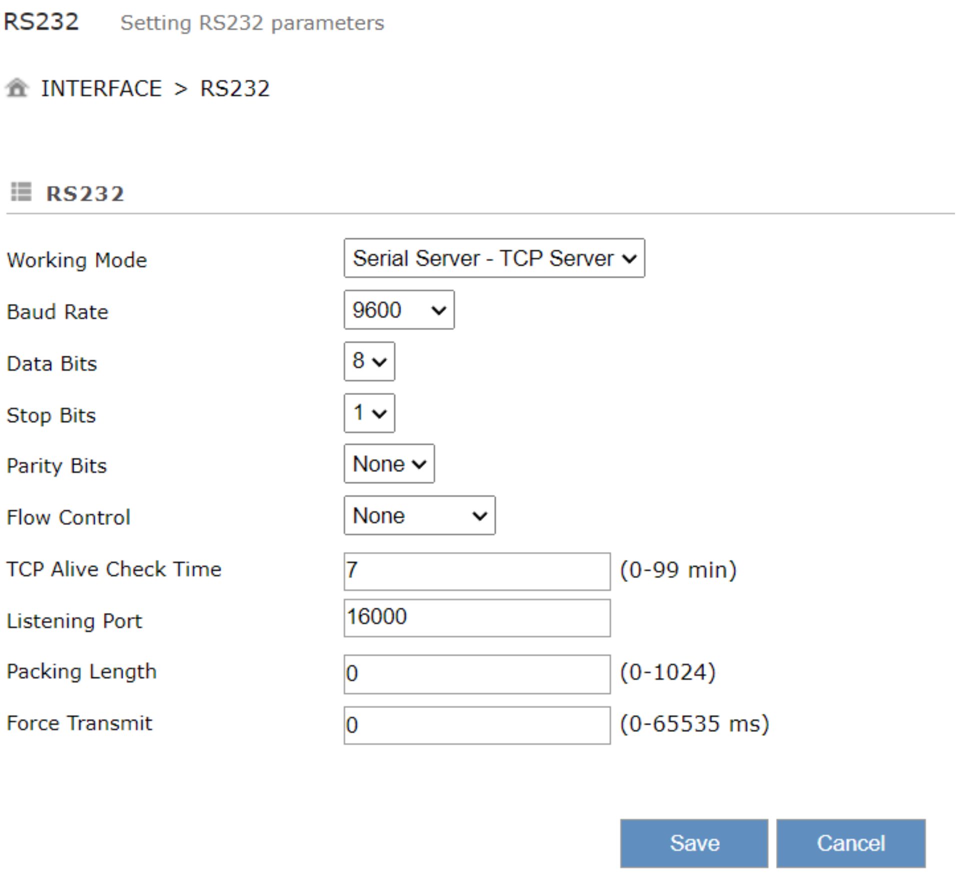
This mode is suitable for custom protocol transmission, where the cloud router is configured as a TCP server and requires the setup of a listening port. Serial data is encapsulated into a network-recognizable format and forwarded to the appropriate destination. The maximum number of TCP client connections is 32. **If the serial device employs a customized protocol, the TCP client needs to have corresponding TCP/UDP connection software tools provided by the manufacturer or developed independently.**



(2) The TCP client sets the TCP server IP address/listening port.

(1) Set the TCP server listening port.

(3) Convert the serial port data format of industrial Device into Ethernet TCP/IP data format and forward it to third-party software.

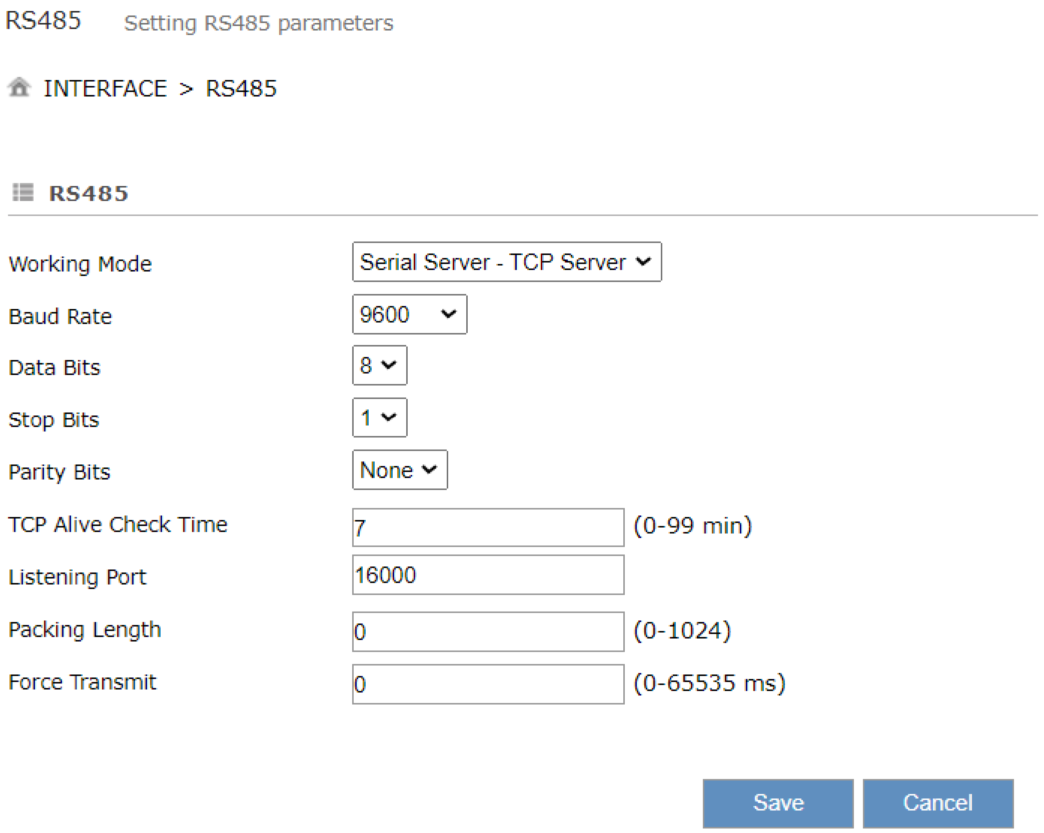


RS232 Setting RS232 parameters

INTERFACE > RS232

RS232

Working Mode	Serial Server - TCP Server
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity Bits	None
Flow Control	None
TCP Alive Check Time	7 (0-99 min)
Listening Port	16000
Packing Length	0 (0-1024)
Force Transmit	0 (0-65535 ms)



RS485 Setting RS485 parameters

INTERFACE > RS485

RS485

Working Mode: Serial Server - TCP Server

Baud Rate: 9600

Data Bits: 8

Stop Bits: 1

Parity Bits: None

TCP Alive Check Time: 7 (0-99 min)

Listening Port: 16000

Packing Length: 0 (0-1024)

Force Transmit: 0 (0-65535 ms)

Description	Default
Working Mode	
● RS-232Mode 1. Close 2. Transparent Mode 3. Slave Mode 4. Master Mode 5. **Serial Server – TCP Server** 6. Serial Server – TCP Client 7. Serial Server – UDP Client 8. MC Master Mode ● RS-485 Mode: 1. Close 2. Transparent Mode 3. Slave Mode 4. Master Mode 5. **Serial Server – TCP Server** 6. Serial Server – TCP Client 7. Serial Server – UDP Client	Close
Baud Rate	
Set up the baud rate for the serial port. Options are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.	9600

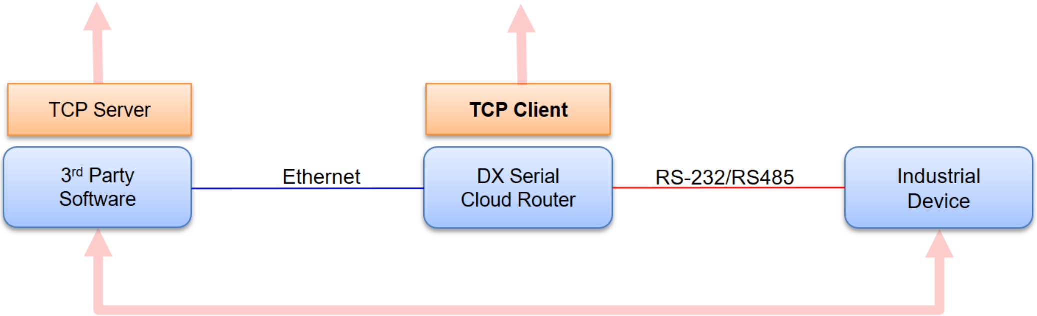
Description	Default
Data Bits	
Set up the data bits for the serial port. Options are 7 and 8. It must be set to 8 when communication mode is Modbus RTU.	8
Stop Bits	
Set up the stop bits for the serial port. Options are 1 and 2.	1
Parity Bits	
Set up the parity bits for the serial port. Options are None, Odd and Even.	None
Flow Control	
Set up the flow control. Options are None, “XON/XOFF”, “RTS/CTS”.	None
TCP Keep-Alive Time	
Set how long the TCP connection remains active without activity before it automatically closes. Available values are 0 to 99 minutes. ● 0: TCP connection will not close due to inactivity (never close). ● 1~99: If the idle time reaches the set value, the TCP connection will close.	7
Listening Port	
Set up the listening port in server.	16000
Packing Length	
Setting the length of packet, packet will be transmitted when the size reaches the values. Input range is from 0 to 1024 byte. Setting it to 0 means that data will be sent immediately when received it.	0
Force Transmit	
Set how long to wait before forcing data packet transmission. The range is from 0~65535 ms. Setting it to 0 means never forcing transmission. Setting it to 1~65535 will trigger data transmission either when the time reaches the set value or when the data accumulation length reaches the set length.	0
TCP Client Connection	
It is recommended to have a maximum of 32 TCP client connections.	32

3.4.1.6 Serial Server–TCP Client

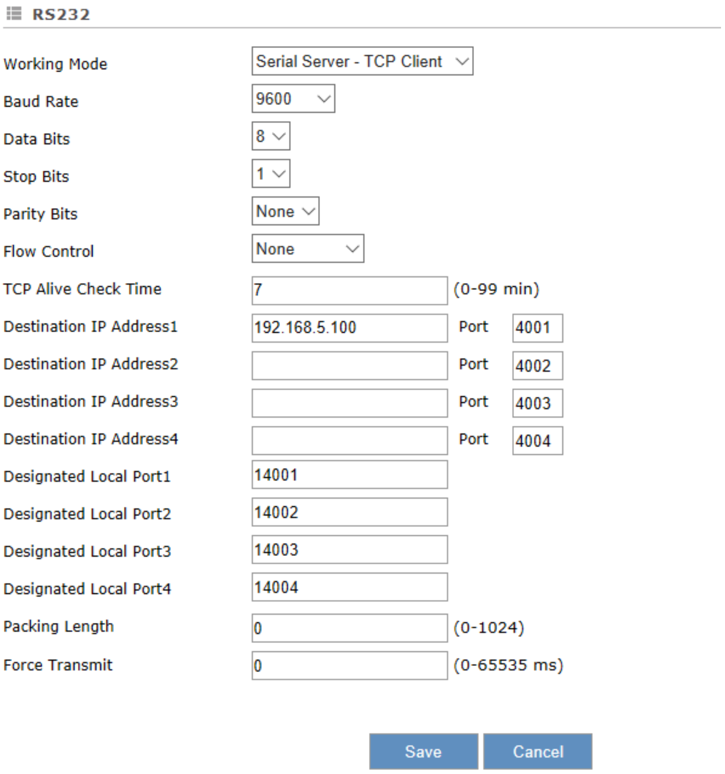
This mode is suitable for custom protocol transmission, where the cloud router is configured as TCP client and requires the setup of destination IP address and port number. Serial data is encapsulated into a network-recognizable format and forwarded to the appropriate destination. The maximum number of connections to the destination IP address is 4. **If the serial device employs a customized protocol, the TCP client needs to have corresponding TCP/UDP connection software tools provided by the manufacturer or developed independently.**

(2) TCP Server sets the listening port.

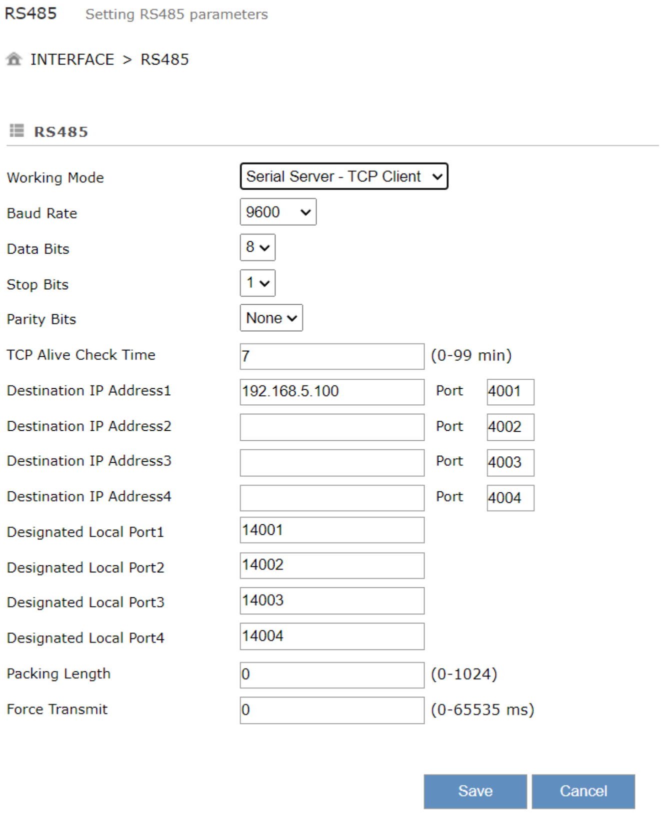
(1) Set the TCP server IP address and port.



(3) Convert the serial port data format of industrial Device into Ethernet TCP/IP data format and forward it to third-party software.



Working Mode	Serial Server - TCP Client		
Baud Rate	9600		
Data Bits	8		
Stop Bits	1		
Parity Bits	None		
Flow Control	None		
TCP Alive Check Time	7	(0-99 min)	
Destination IP Address1	192.168.5.100	Port	4001
Destination IP Address2		Port	4002
Destination IP Address3		Port	4003
Destination IP Address4		Port	4004
Designated Local Port1	14001		
Designated Local Port2	14002		
Designated Local Port3	14003		
Designated Local Port4	14004		
Packing Length	0	(0-1024)	
Force Transmit	0	(0-65535 ms)	



RS485 Setting RS485 parameters

INTERFACE > RS485

RS485

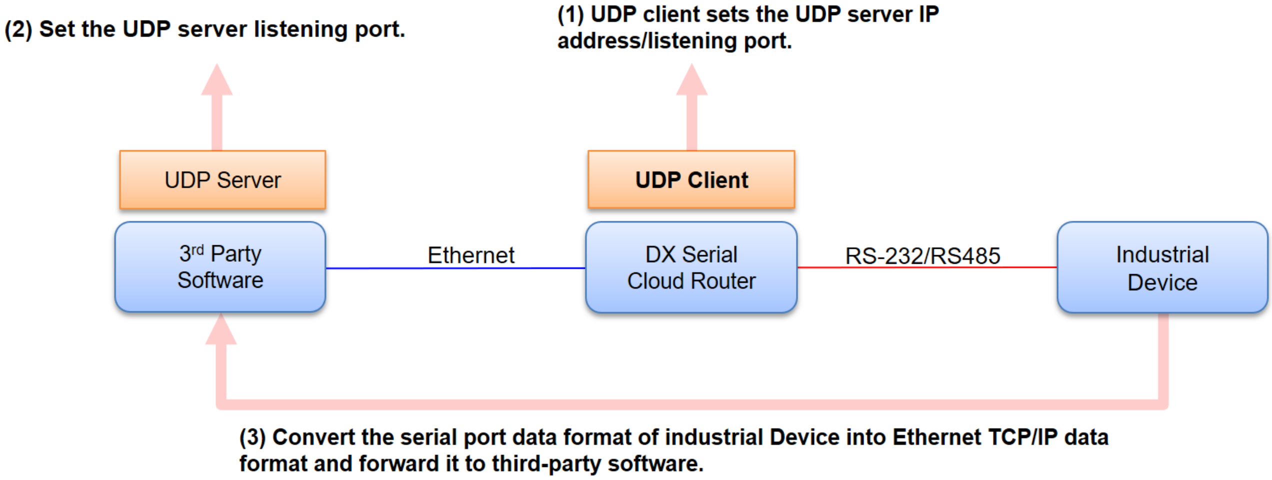
Working Mode	Serial Server - TCP Client		
Baud Rate	9600		
Data Bits	8		
Stop Bits	1		
Parity Bits	None		
TCP Alive Check Time	7	(0-99 min)	
Destination IP Address1	192.168.5.100	Port	4001
Destination IP Address2		Port	4002
Destination IP Address3		Port	4003
Destination IP Address4		Port	4004
Designated Local Port1	14001		
Designated Local Port2	14002		
Designated Local Port3	14003		
Designated Local Port4	14004		
Packing Length	0	(0-1024)	
Force Transmit	0	(0-65535 ms)	

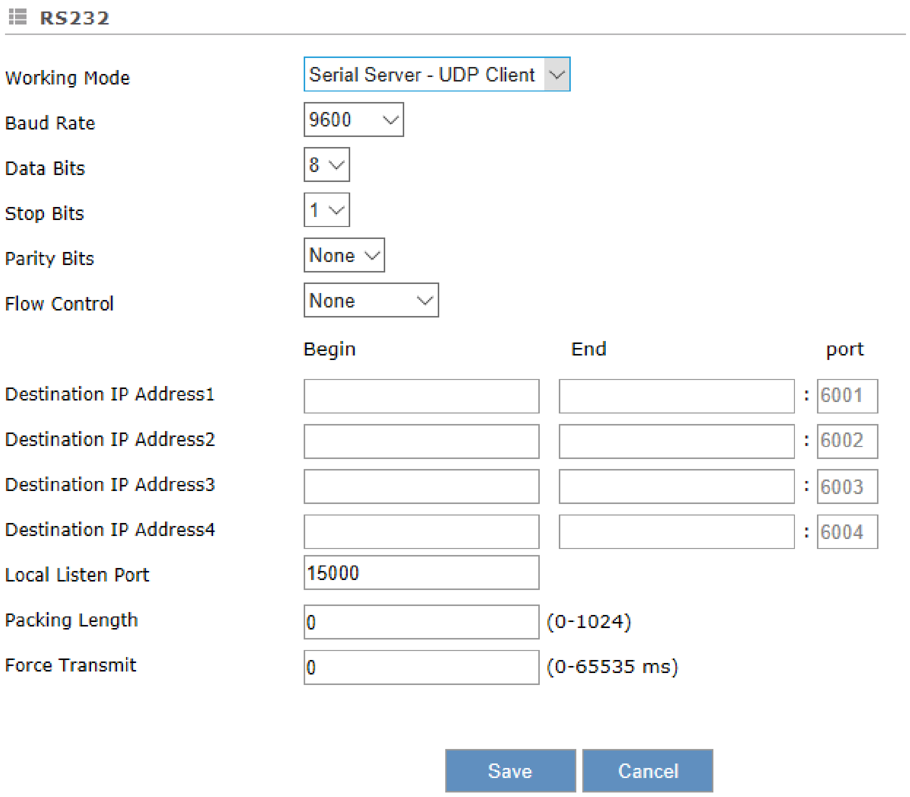
Description	Default
Working Mode	
● RS-232 Mode 1. Close 2. Transparent Mode 3. Slave Mode 4. Master Mode 5. Serial Server – TCP Server 6. **Serial Server – TCP Client** 7. Serial Server – UDP Client 8. MC Master Mode ● RS-485 Mode: 1. Close 2. Transparent Mode 3. Slave Mode 4. Master Mode 5. Serial Server – TCP Server 6. **Serial Server – TCP Client** 7. Serial Server – UDP Client	Close
Baud Rate	
Set up the baud rate for the serial port. Options are 2400, 4800, 9600, 19200, 38400, 57600 and 115200.	9600

Description	Default
Data Bits	
Set up the data bits for the serial port. Options are 7 and 8. It must be set to 8 when communication mode is 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
Flow Control	
Set up the flow control. Options are None, “XON/XOFF”, “RTS/CTS”.	None
TCP Keep-Alive Time	
Set how long the TCP connection remains active without activity before it automatically closes. Available values are 0 to 99 minutes. ● 0：TCP connection will not close due to inactivity (never close). ● 1~99：If the idle time reaches the set value, the TCP connection will close.	7
Destination IP address and Port	
Set the server IP address range and ports for connecting to serial port servers (default ports 4001 to 4004, configurable). IP addresses and ports cannot be configured with duplicates. Up to a maximum of 4 serial port servers can be connected simultaneously.	N/A
Local Port	
Configure the TCP port for local data transmission.	14001~14004
Packing Length	
Setting the length of packet, packet will be transmitted when the size reaches the values. Input range is from 0 to 1024 byte. Setting it to 0 means that data will be sent immediately when received it.	0
Force Transmit	
Set how long to wait before forcing data packet transmission. The range is from 0~65535 ms. Setting it to 0 means never forcing transmission. Setting it to 1~65535 will trigger data transmission either when the time reaches the set value or when the data accumulation length reaches the set length.	0

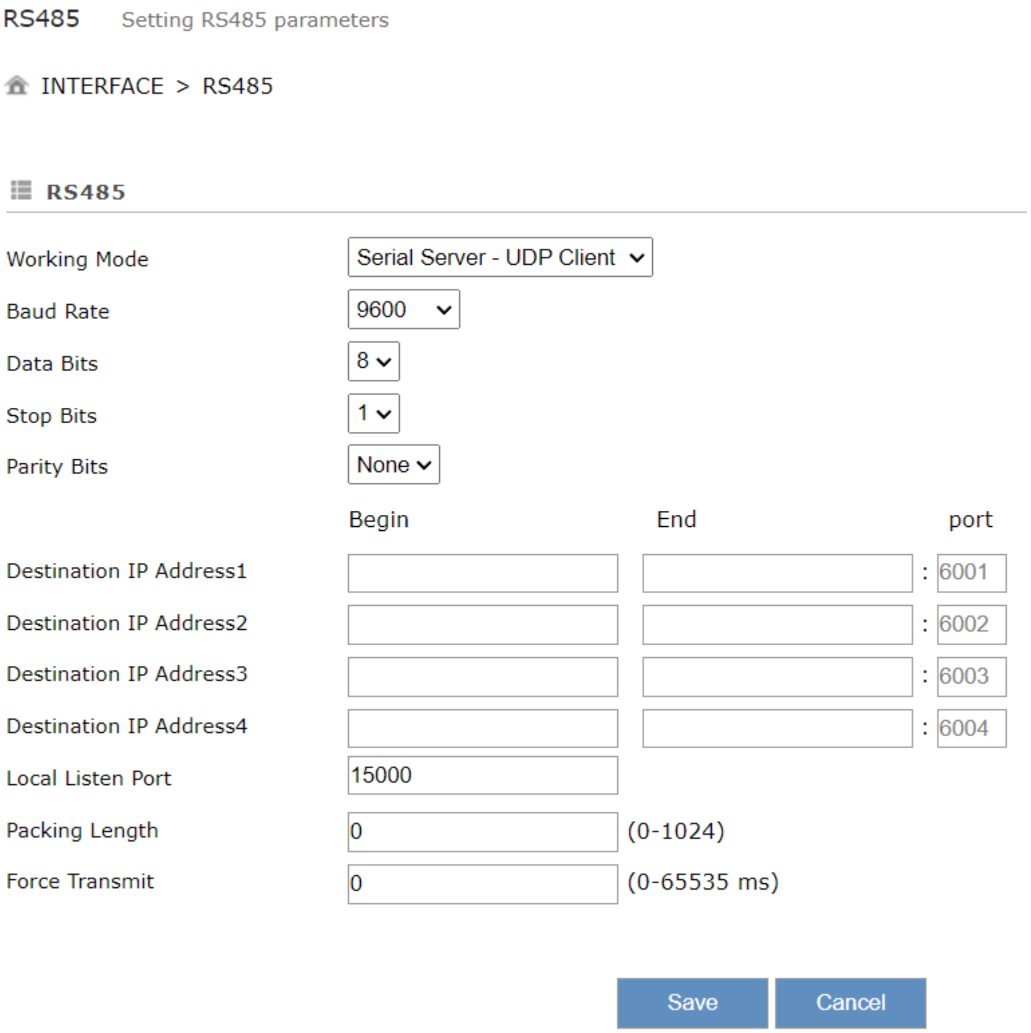
3.4.1.7 Serial Server–UDP Client

This mode is suitable for custom protocol transmission, where the cloud router is configured as UDP client and requires the setup of destination IP address and port number. Serial data is encapsulated into a network-recognizable format and forwarded to the appropriate destination. The maximum number of connections to the destination IP address is 4. **If the serial device employs a customized protocol, the UDP server needs to have corresponding TCP/UDP connection software tools provided by the manufacturer or developed independently.**


(2) Set the UDP server listening port.
(1) UDP client sets the UDP server IP address/listening port.
UDP Server
UDP Client
3rd Party Software
Ethernet
DX Serial Cloud Router
RS-232/RS485
Industrial Device
(3) Convert the serial port data format of industrial Device into Ethernet TCP/IP data format and forward it to third-party software.


RS232

Working Mode	Serial Server - UDP Client		
Baud Rate	9600		
Data Bits	8		
Stop Bits	1		
Parity Bits	None		
Flow Control	None		
	Begin	End	port
Destination IP Address1			: 6001
Destination IP Address2			: 6002
Destination IP Address3			: 6003
Destination IP Address4			: 6004
Local Listen Port	15000		
Packing Length	0	(0-1024)	
Force Transmit	0	(0-65535 ms)	



RS485 Setting RS485 parameters

INTERFACE > RS485

RS485

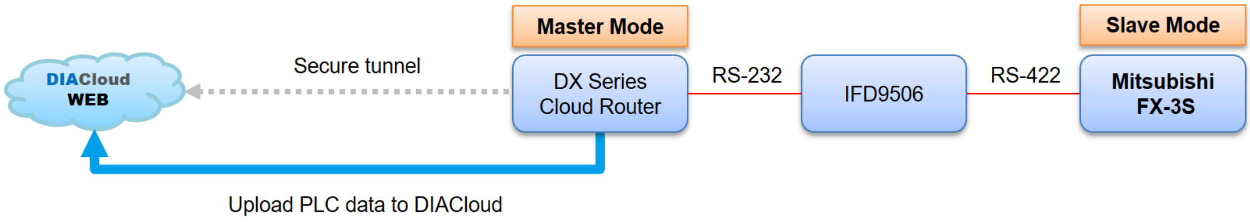
Working Mode	Serial Server - UDP Client		
Baud Rate	9600		
Data Bits	8		
Stop Bits	1		
Parity Bits	None		
	Begin	End	port
Destination IP Address1			6001
Destination IP Address2			6002
Destination IP Address3			6003
Destination IP Address4			6004
Local Listen Port	15000		
Packing Length	0 (0-1024)		
Force Transmit	0 (0-65535 ms)		

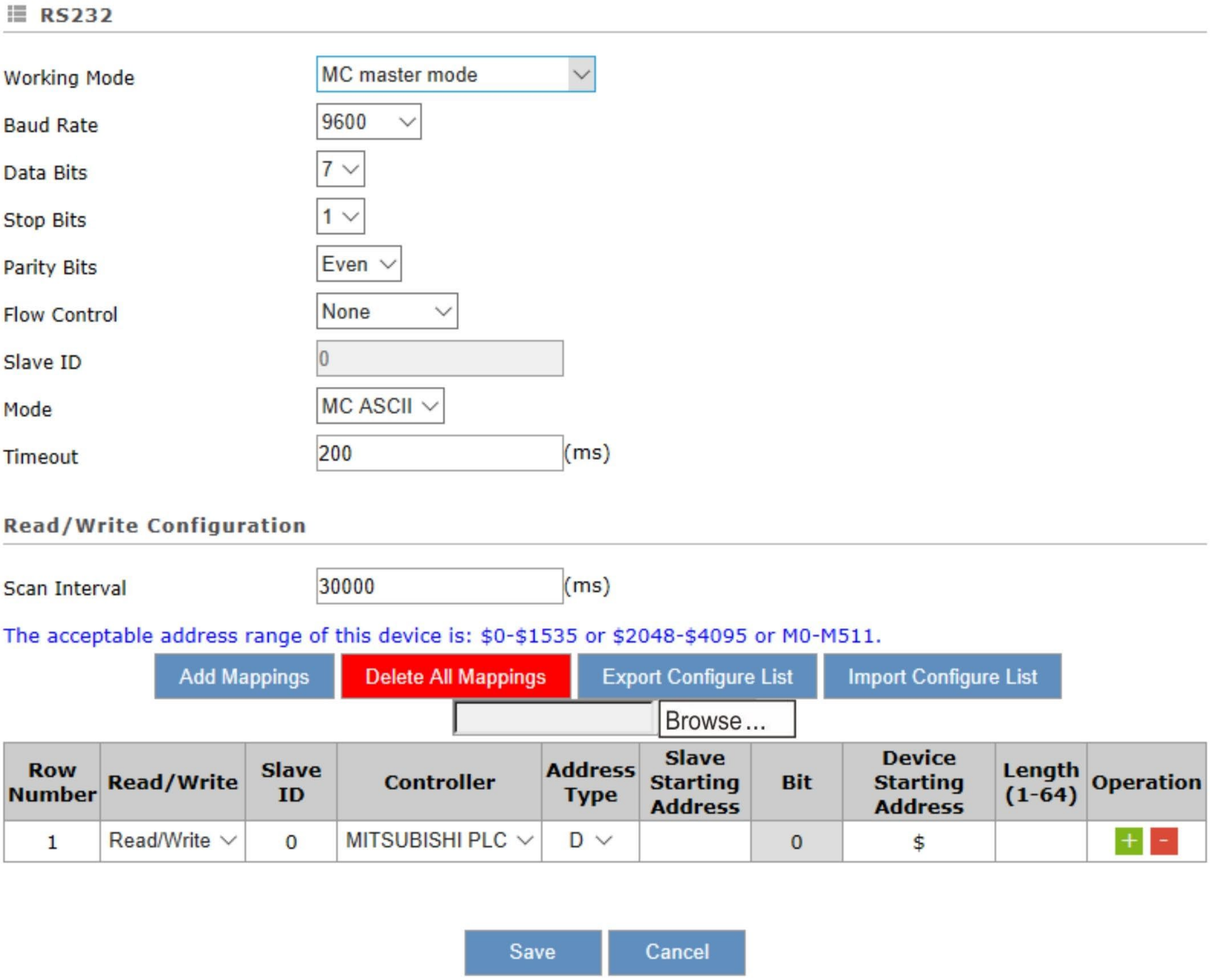
Description	Default
Working Mode	
● RS-232 Mode 1. Close 2. Transparent Mode 3. Slave Mode 4. Master Mode 5. Serial Server – TCP Server 6. Serial Server – TCP Client 7. **Serial Server – UDP Client** 8. MC Master Mode ● RS-485 Mode: 1. Close 2. Transparent Mode 3. Slave Mode 4. Master Mode 5. Serial Server – TCP Server 6. Serial Server – TCP Client 7. **Serial Server – UDP Client**	Close

Description	Default
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. Options are 7 and 8. It must be set to 8 when communication mode is 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
Flow Control	
Set up the flow control. Options are None, “XON/XOFF”, “RTS/CTS”.	None
Destination IP address and Port	
Set the server IP address range and ports for connecting to serial port servers (default ports 6001 to 6004, configurable). IP addresses and ports cannot be configured with duplicates. Up to a maximum of 4 serial port servers can be connected simultaneously. Each set can support up to 99 server addresses, meaning the maximum range for the starting and ending IP address segments is 99.	Default Ports6001~6004
Local Listening Port	
Set the local listening port, which is required when establishing a connection under UDP server mode	15000
Packing Length	
Setting the length of packet, packet will be transmitted when the size reaches the values. Input range is from 0 to 1024 byte. Setting it to 0 means that data will be sent immediately when received it.	0
Force Transmit	
Set how long to wait before forcing data packet transmission. The range is from 0~65535 ms. Setting it to 0 means never forcing transmission. Setting it to 1~65535 will trigger data transmission either when the time reaches the set value or when the data accumulation length reaches the set length.	0

3.4.1.8 MC Master Mode

When RS-232 operates in this mode, it allows the DX Cloud Router to perform data read and write operations on Mitsubishi slave devices connected via the RS-232 serial port, enabling bidirectional data transmission between the devices and the cloud platform.





Working Mode: MC master mode

Baud Rate: 9600

Data Bits: 7

Stop Bits: 1

Parity Bits: Even

Flow Control: None

Slave ID: 0

Mode: MC ASCII

Timeout: 200 (ms)

Read/Write Configuration

Scan Interval: 30000 (ms)

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

Row Number	Read/Write	Slave ID	Controller	Address Type	Slave Starting Address	Bit	Device Starting Address	Length (1-64)	Operation
1	Read/Write	0	MITSUBISHI PLC	D		0	$		+ -

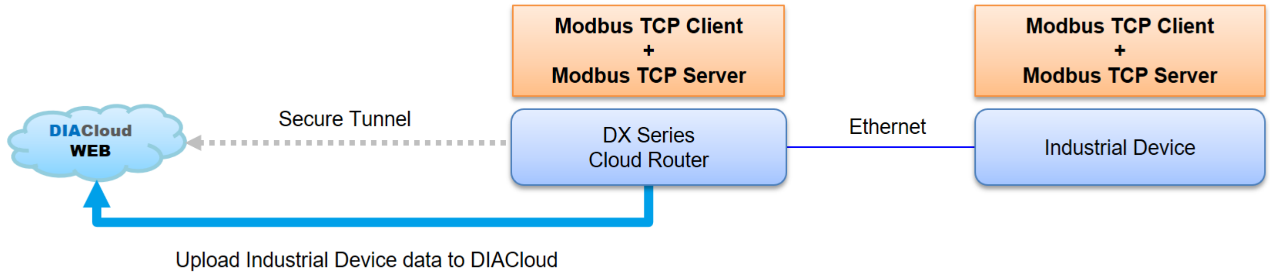
Description	Default
Working Mode	
● RS-232 Mode 1. Close 2. Transparent Mode 3. Slave Mode 4. Master Mode 5. Serial Server – TCP Server 6. Serial Server – TCP Client 7. Serial Server – UDP Client 8. **MC Master Mode** ● RS-485 Mode: 1. Close 2. Transparent Mode 3. Slave Mode 4. Master Mode 5. Serial Server – TCP Server 6. Serial Server – TCP Client 7. Serial Server – UDP Client	Close
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. Options are 7 and 8. It must be set to 8 when communication mode is 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
Flow Control	
Set up the flow control. Options are None, “XON/XOFF”, “RTS/CTS”.	None
Slave ID	
Cannot be configured in MC master mode.	0
Communication Mode	
It’s fixed to “MC ASCII” in MC master mode.	MC ASCII
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.	200

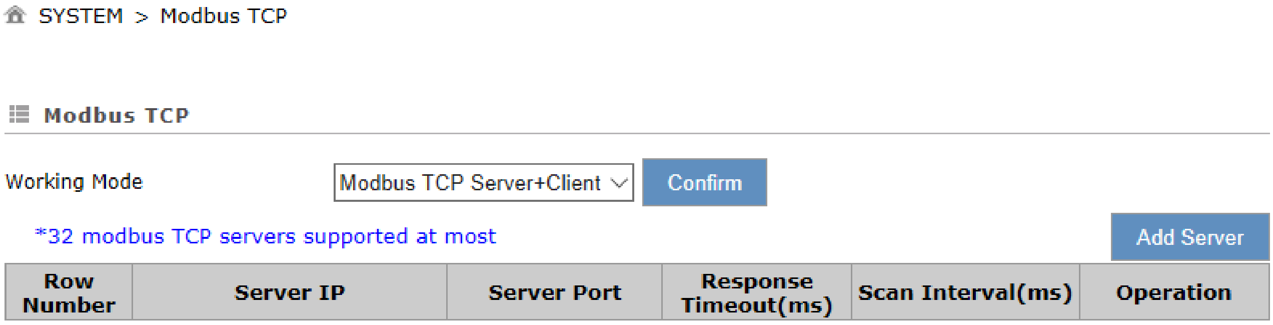
Description	Default
Scan Interval	
Set up the time for scan interval, the interval refers to the time span between the conclusion of the previous polling cycle and the commencement of a new polling cycle.	30000
Add Mappings	
Once the user configures the mapping relationship between the device address and the cloud router register, the system will gather data from the connected device based on the established mapping relationship.	N/A
Delete All Mappings	
Clear all existing mapping relationships in RS-232 MC master mode.	N/A
Export Configure List	
Export the existing mapping relationships and save the file to the local computer.	N/A
Import Configure List	
The mapping list can be imported for RS-232/RS-485/MODBUS TC/MC/SIEMEN TCP communication interfaces. A total of 600 mapping addresses are shared among all communication interfaces. ⚠**Notice:** ● Each communication interface can import a maximum of 600 mapping addresses. If RS-232 already has 10 configured mapping addresses, then an import of new 600 mapping addresses is performed from RS-232, the previously set 10 mapping addresses will be overwritten. ● If RS-232 has 10 mapping addresses, then the maximum import of mapping addresses from RS-485/MODBUS TCP is limited to 590. If the number exceeds 590, a warning message will be displayed.	N/A
Read/Write	
Set up the mapping relationship is for "Read/Write", "Read-only" or "Write-only". ● Read-only: Automatically read data from the mapped slave device address according to the scanning cycle and update it to the corresponding register in the cloud router. ● Write-only: When the value of the cloud router's register is changed, the latest value will be automatically written to the corresponding slave device address. ● Read/Write: Periodically read data from the slave device, then update it to the corresponding register in the cloud router. When the value of the register is changed, the latest value will also be automatically written to the corresponding slave device address.	Read/Write
Slave ID	
Cannot be configured in MC master mode.	0
Controller	
The slave device's type is fixed as MITSUBISHI PLC.	MITSUBISHI PLC

Description	Default
Address Type	
The URL classification types are D/M/X/Y, where D represents word type and M/X/Y represent bit type.	D
Slave Starting Address	
Set the starting address of the slave device registers for read/write operations. Enter the internal D register number, for example, enter 0 for D0.	N/A
Bit	
Cannot be configured in MC master mode.	
Device Starting Address	
Set the starting register address for the device mapping. For word type, the range is $2048 to $4095; for bit type, the range is M0 to M511. When entering the register address, it must start with "$" or "M" and use the decimal addressing format.	N/A
Length	
Set the length, which specifies how many consecutive registers' data to read/write from the starting address. The range is from 1 to 64.	N/A
Operation	
Click the +/- button to add mapping or delete mapping.	N/A
Edit	
You can directly click on a specific column to edit its content.	N/A

3.4.2 Modbus TCP

The cloud router can be used as both **MODBUS TCP client and server** or as **MODBUS TCP server** to communicate with slave devices and upload data to the cloud. It also supports remotely uploading and downloading.


Modbus TCP Client + Modbus TCP Server
Modbus TCP Client + Modbus TCP Server
DIACloud WEB
Secure Tunnel
DX Series Cloud Router
Ethernet
Industrial Device
Upload Industrial Device data to DIACloud



SYSTEM > Modbus TCP

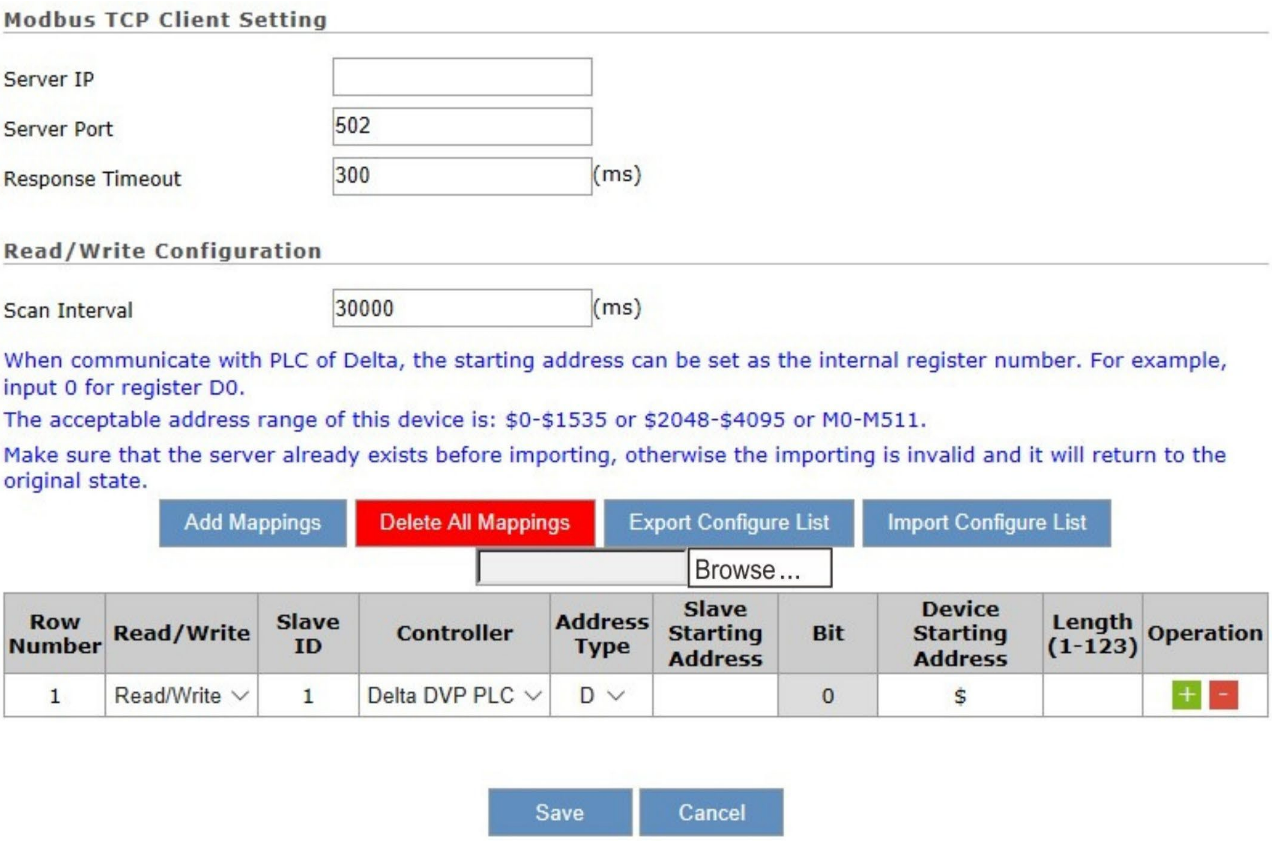
Modbus TCP

Working Mode: Modbus TCP Server+Client [Confirm]

*32 modbus TCP servers supported at most [Add Server]

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

Click “Add Server”, it will show the following page.



Modbus TCP Client Setting

Server IP	
Server Port	502
Response Timeout	300 (ms)

Read/Write Configuration

Scan Interval: 30000 (ms)

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

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

Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

[Add Mappings] [Delete All Mappings] [Export Configure List] [Import Configure List]

Browse...

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

[Save] [Cancel]

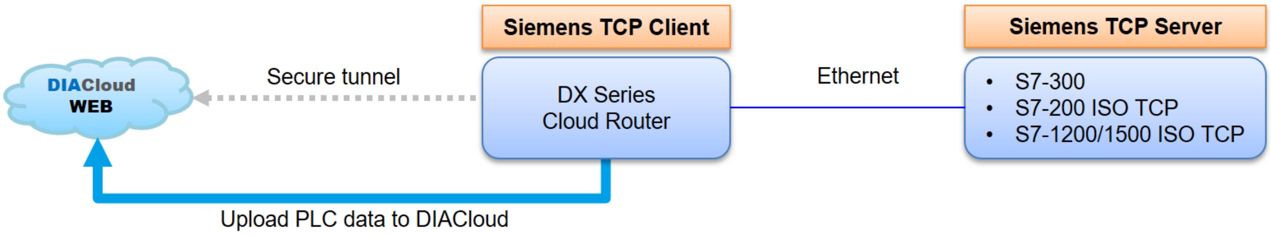
Description	Default
Working Mode	
● **Modbus TCP Server:** Only the Modbus TCP server is activated, and it supports a maximum of 32 slave devices as clients. ● **Modbus TCP Server+Client:** Simultaneously enable both Modbus TCP server and Modbus client. Users can configure up to 32 different servers at most.	Modbus TCP Server
Server IP	
In Modbus TCP client mode, configure the IP address of the server (slave device).	N/A
Server Port	
In Modbus TCP client mode, configure the port of the server (slave device).	502
Response Timeout	
Set up the timeout timer from 50ms to 10000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	300
Scan Interval	
Set up the time for scan interval, the interval refers to the time span between the conclusion of the previous polling cycle and the commencement of a new polling cycle.	30000
Add Mappings	
Once the user configures the mapping relationship between the device address and the cloud router register, the system will gather data from the connected device based on the established mapping relationship.	N/A
Delete All Mappings	
Clear all existing mapping relationships on the server.	N/A
Export Configure List	
Export the existing mapping relationships and save the file to the local computer.	N/A
Import Configure List	
The mapping list can be imported for RS-232/RS-485/MODBUS TC/MC/SIEMEN TCP communication interfaces. A total of 600 mapping addresses are shared among all communication interfaces. ⚠**Notice:** ● Each communication interface can import a maximum of 600 mapping addresses. If RS-232 already has 10 configured mapping addresses, then an import of new 600 mapping addresses is performed from RS-232, the previously set 10 mapping addresses will be overwritten. ● If RS-232 has 10 mapping addresses, then the maximum import of mapping addresses from RS-485/MODBUS TCP is limited to 590. If the number exceeds 590, a warning message will be displayed.	N/A

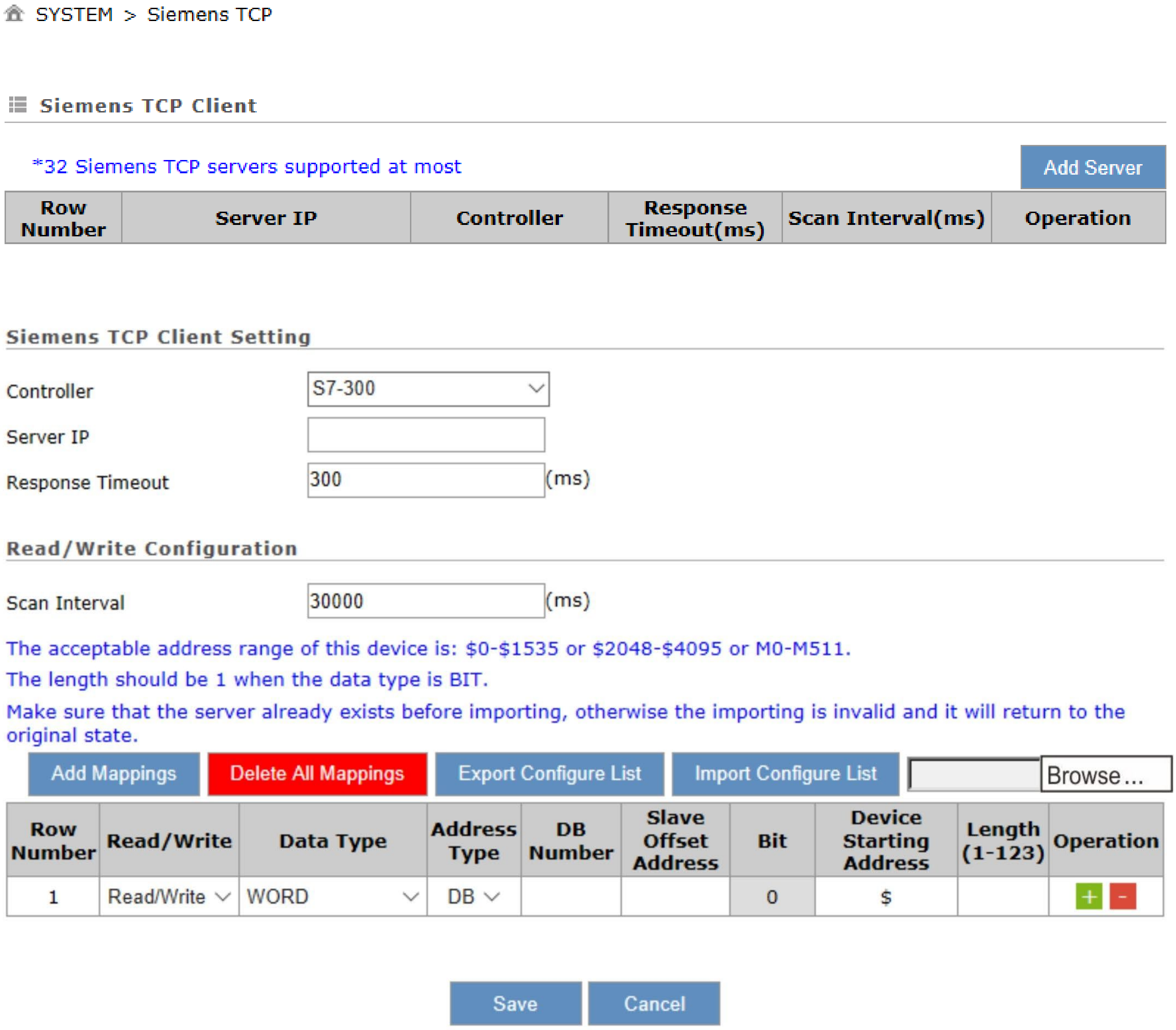
Description	Default
Read/Write	
Set up the mapping relationship is for “Read/Write”, “Read-only” or “Write-only”. ● **Read-only**: Automatically read data from the mapped slave device address according to the scanning cycle and update it to the corresponding register in the cloud router. ● **Write-only**: When the value of the cloud router's register is changed, the latest value will be automatically written to the corresponding slave device address. ● **Read/Write**: Periodically read data from the slave device, then update it to the corresponding register in the cloud router. When the value of the register is changed, the latest value will also be automatically written to the corresponding slave device address.	**Read/Write**
Slave ID	
Set up the corresponding slave communication station number. The value is between 1 to 247.	1
Controller	
In master mode, device types’ of options: ● **Delta PLC:** Please choose this option for Delta DVP/AH/AS series PLC. ● **Other:** For non-Delta DVP/AH/AS series PLCs, please choose this option. "HEX" represents inputting hexadecimal addresses, while "DEC" represents inputting decimal addresses.	Delta DVP PLC
Address Type	
In master mode, the options vary based on the selected controller type: ● **Delta PLC:** The URL classification types are D/M/S/X/Y, where D represents word type and M/S/X/Y represent bit type. ● **Other:** The URL classification types are0x/1x/3x/4x/Swap a) 0x: Read or write coils data(Modbus function code: 01/05) b) 1x: ReadDiscrete Inputs(Modbus function code: 02), read-only c) 3x: Read or writeInput Registers (Modbus function code: 04) d) 4x: Read or writeHolding Registers (Modbus function code: 03/16) e) Swap: Read or writeHolding Registers, during processing, start from the first register, grouping them in pairs. The previous Word and the subsequent Word are swapped with each other.	D
Slave Starting Address	
Set the starting address of the slave device registers for read/write operations. Master Mode： ● **Delta PLC:** Enter the internal D register number, for example, enter 0 for D0 or enter 12 for M12. ● **Other:** Enter the actual address in hexadecimal or decimal format. To retrieve the holding register 400100, take the last four digits: 0100 (decimal) or 64 (hexadecimal).	N/A

Description	Default
Bit	
For the Delta AH/AS series X/Y types, the address input format is 0.0 ~ X.15. The part before the decimal point should be entered in the slave device's starting address field, while the part after the decimal point should be entered in this field.	
Device Starting Address	
Set the starting register address for the device mapping. For word type, the range is $2048 to $4095; for bit type, the range is M0 to M511. When entering the register address, it must start with "$" or "M" and use the decimal addressing format.	N/A
Length	
Set the length, which specifies how many consecutive registers' data to read/write from the starting address. The range is from 1 to 123.	N/A
Operation	
Click the +/- button to add mapping or delete mapping.	N/A

3.4.3 Siemens TCP

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





SYSTEM > Siemens TCP

Siemens TCP Client

*32 Siemens TCP servers supported at most

Add Server

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

Siemens TCP Client Setting

Controller	S7-300
Server IP	
Response Timeout	300 (ms)

Read/Write Configuration

Scan Interval	30000 (ms)

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

The length should be 1 when the data type is BIT.

Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

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

Row Number	Read/Write	Data Type	Address Type	DB Number	Slave Offset Address	Bit	Device Starting Address	Length (1-123)	Operation
1	Read/Write	WORD	DB			0	$		+ -

Save | Cancel

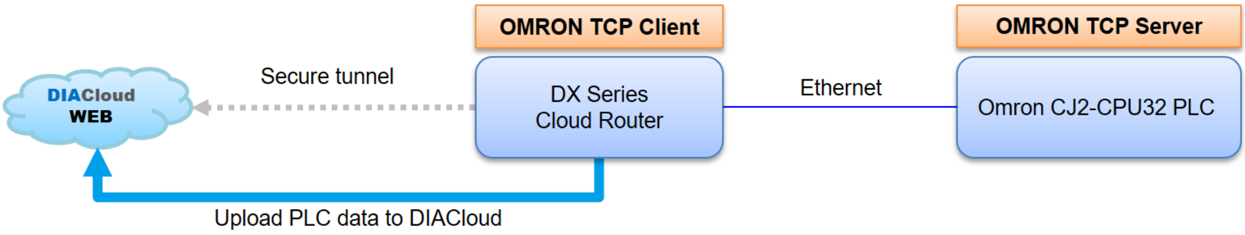
Description	Default
Add Server	
Click to configure the Siemens TCP server that the router should connect to. User can create up to 32 different servers	N/A
Controller	
Set up the model of Siemens device you want to communicate with.	S7-300
Server IP Address	
Set up the IP address of Siemens device you want to communicate with.	1
Local TSAP	
Set the local TSAP in Siemens ISO-on-TCP; configuration is required only when the controller model is 'S7-200 ISO TCP' or 'S7-1200/1500 ISO TCP'.	N/A
Remote TSAP	
Set the remote TSAP in Siemens ISO-on-TCP; configuration is required only when the controller model is 'S7-200 ISO TCP' or 'S7-1200/1500 ISO TCP'.	200
Response Timeout	
Set up the timeout timer from 50ms to 10000ms. If the set value is out of range, it will be automatically changed to its maximum or minimum value.	300
Scan Interval	
Set up the time for scan interval, the interval refers to the time span between the conclusion of the previous polling cycle and the commencement of a new polling cycle.	30000
Add Mappings	
Once the user configures the mapping relationship between the device address and the cloud router register, the system will gather data from the connected device based on the established mapping relationship.	N/A
Delete All Mappings	
Clear all existing mapping relationships on the server.	N/A
Export Configure List	
Export the existing mapping relationships and save the file to the local computer.	N/A
Import Configure List	
The mapping list can be imported for RS-232/RS-485/MODBUS TC/MC/SIEMEN TCP communication interfaces. A total of 600 mapping addresses are shared among all communication interfaces. ⚠ **Notice:** ● Each communication interface can import a maximum of 600 mapping addresses. If RS-232 already has 10 configured mapping addresses, then an import of new 600 mapping addresses is performed from RS-232, the previously set 10 mapping addresses will be overwritten.	N/A

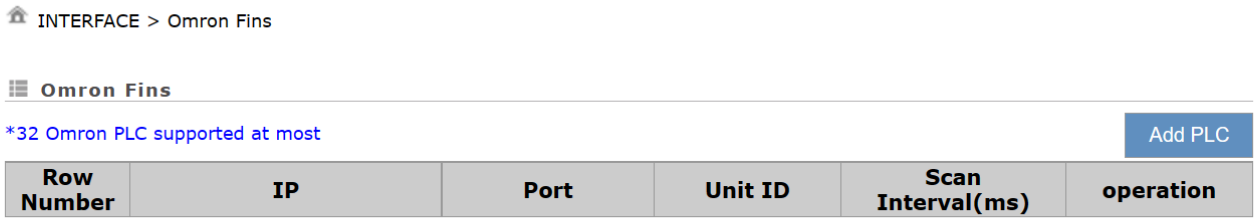
Description	Default
● If RS-232 has 10 mapping addresses, then the maximum import of mapping addresses from RS-485/MODBUS TCP is limited to 590. If the number exceeds 590, a warning message will be displayed.	
Read/Write	
Set up the mapping relationship is for “Read/Write”, “Read-only” or “Write-only”. ● Read-only: Automatically read data from the mapped slave device address according to the scanning cycle and update it to the corresponding register in the cloud router. ● Write-only: When the value of the cloud router's register is changed, the latest value will be automatically written to the corresponding slave device address. ● Read/Write: Periodically read data from the slave device, then update it to the corresponding register in the cloud router. When the value of the register is changed, the latest value will also be automatically written to the corresponding slave device address.	Read/Write
Data Type	
Set up the data type to be collected: ● **BIT:** bit type ● **WORD:** word type ● **WORD(SWAP):** double-word type; start from the first register, grouping them in pairs. The previous Word and the subsequent Word are swapped with each other.	WORD
Address Type	
● The controller is "S7-200 ISO TCP," and the options for address type can be V/M/Q/I, combined with data types as follows: -Bit type：VB/MB/QB/IB -Word type：VW/MW/QW/IW -DWord type：VD/MD/QD/ID ● The controller is “S7-300” or “S7-1200/1500 ISO TCP” and the options for address type can be DB/M/Q/I, combined with data types as follows: -Bit type：DBn_DBX/MB/QB/IB -Word type：DBn_DBW/MW/QW/IW ● -DWord type：DBn_DBD/MD/QD/ID	DB
DB Number	
Enter the number of the DB (Data Block). This parameter will appear in the project menu, and after creating the DB, the DB name [DB1] will be displayed on the menu. Then, simply enter '1' in the DB Number field in DX. It cannot be configured when the controller is "S7-200 ISO TCP."	N/A
Slave Offset Address	
Enter the Data Block (DB) offset address. This parameter will be automatically generated after creating and compiling the PLC program with the DB (Data Block).	N/A
Bit	
For the bit type data, the address input format is 0.0 ~ X.7. The part before the decimal point should be entered in the subunit offset address field, while the part after the decimal point should be entered in this field.	N/A

Description	Default
Device Starting Address	
Set the starting register address for the device mapping. For word type, the range is $2048 to $4095; for bit type, the range is M0 to M511. When entering the register address, it must start with "$" or "M" and use the decimal addressing format.	N/A
Length	
Set the length, which specifies how many consecutive registers' data to read/write from the starting address. The range is from 1 to 123.	N/A
Operation	
Click the +/- button to add mapping or delete mapping.	N/A
Edit	
You can directly click on a specific column to edit its content.	N/A

3.4.4 Omron Fins

Omron's CP/CJ/NJ/NX series PLCs all support the FINS TCP protocol, and the DX-2400 Ethernet port allows data retrieval from Omron PLC via the FINS TCP protocol.





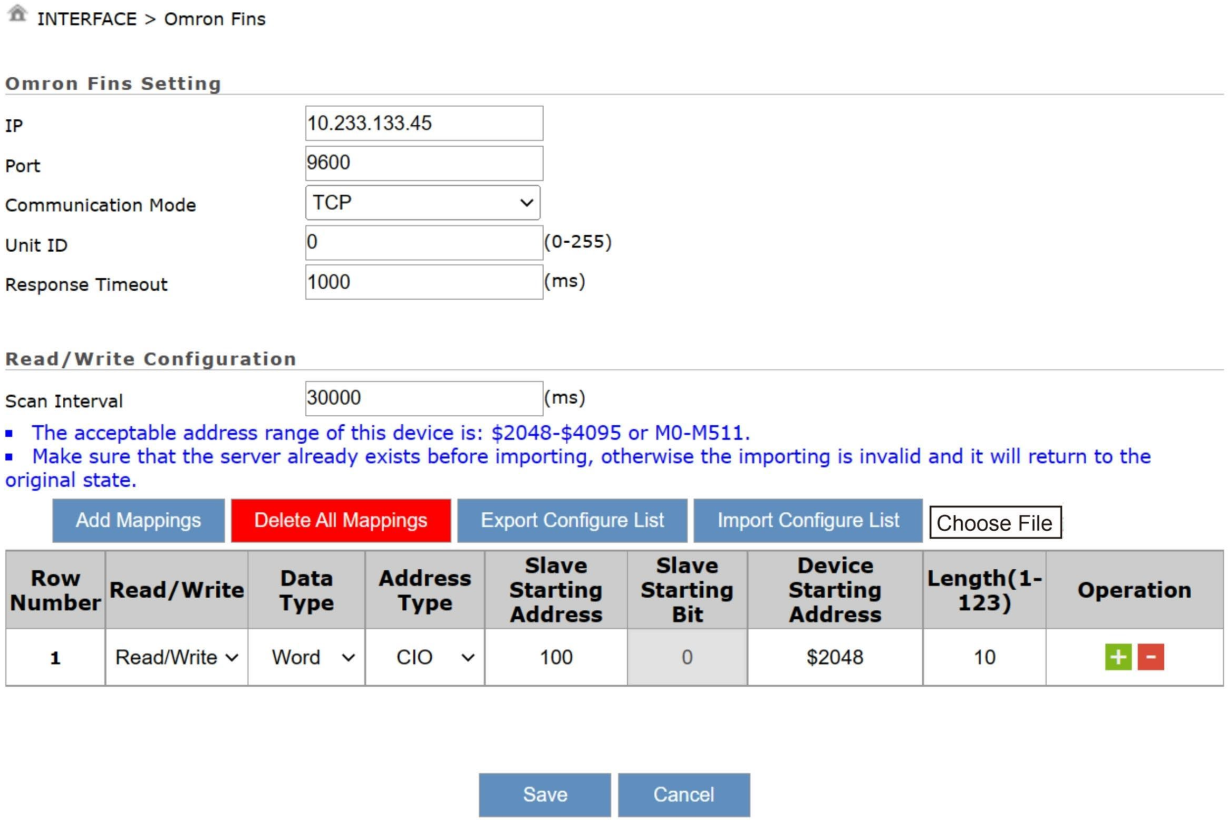
INTERFACE > Omron Fins

Omron Fins

*32 Omron PLC supported at most

Add PLC

Row Number	IP	Port	Unit ID	Scan Interval(ms)	operation



INTERFACE > Omron Fins

Omron Fins Setting

IP	10.233.133.45
Port	9600
Communication Mode	TCP
Unit ID	0 (0-255)
Response Timeout	1000 (ms)

Read/Write Configuration

Scan Interval 30000 (ms)

- The acceptable address range of this device is: $2048-$4095 or M0-M511.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Read/Write	Data Type	Address Type	Slave Starting Address	Slave Starting Bit	Device Starting Address	Length(1-123)	Operation
1	Read/Write	Word	CIO	100	0	$2048	10	+ -

Description	Default
IP Address	
Set up the Omron PLC IP address. Supports connecting to 32 Omron PLCs at most.	N/A
Port	
Set up the communication port with the Omron PLC.	9600
Communication Mode	
Set up the communication protocol with the Omron PLC. Currently support TCP only.	TCP
Unit Number	
Set the unit ID for the Omron PLC.	0
Response Timeout	
Set the communication timeout, which ranges from 100ms to 10000ms.	1000
Scan Interval	
Set up the time for scan interval, the interval refers to the time span between the conclusion of the previous polling cycle and the commencement of a new polling cycle.	30000
Add Mappings	
Once the user configures the mapping relationship between the device address and the cloud router register, the system will gather data from the connected device based on the established mapping relationship.	N/A
Delete All Mappings	
Clear all existing mapping relationships in the server.	N/A
Export Configure List	
Export the existing mapping relationships and save the file to the local computer.	N/A
Import Configure List	
The mapping list can be imported for RS-232/RS-485/MODBUS TC/MC/SIEMEN TCP communication interfaces. A total of 600 mapping addresses are shared among all communication interfaces. ⚠**Notice:** ● Each communication interface can import a maximum of 600 mapping addresses. If RS-232 already has 10 configured mapping addresses, then an import of new 600 mapping addresses is performed from RS-232, the previously set 10 mapping addresses will be overwritten. ● If RS-232 has 10 mapping addresses, then the maximum import of mapping addresses from RS-485/MODBUS TCP is limited to 590. If the number exceeds 590, a warning message will be displayed.	N/A
Read/Write	
Set up the mapping relationship is for “Read/Write”, “Read-only” or “Write-only”.	Read/Write

Description	Default
● **Read-only:** Automatically read data from the mapped slave device address according to the scanning cycle and update it to the corresponding register in the cloud router. ● **Write-only:** When the value of the cloud router's register is changed, the latest value will be automatically written to the corresponding slave device address. ● **Read/Write:** Periodically read data from the slave device, then update it to the corresponding register in the cloud router. When the value of the register is changed, the latest value will also be automatically written to the corresponding slave device address.	
Slave ID	
Set up the corresponding slave communication station number. The value is between 1 to 247.	1
Data Type	
Supported data types are as follows: ● Word ● Bit	WORD
Address Type	
Supports reading and writing data to the following address areas of Omron PLC: a) D：DM area data b) CIO：CIO area data c) W：Work area data d) H：Holdingarea data e) A：Auxiliary Bitarea data f) E0：EMarea data	D
Slave Starting Address	
Set the starting address for reading/writing Omron PLC registers. For example, for D100 register, enter 100.	N/A
Bit	
Bit-type data; enter the number of bits in this field. Enter the value between 0 and 15.	0
Device Starting Address	
Set the starting register address for the device mapping. For word type, the range is $2048 to $4095; for bit type, the range is M0 to M511. When entering the register address, it must start with "$" or "M" and use the decimal addressing format.	N/A
Length	
Set the length, which specifies how many consecutive registers' data to read/write from the starting address. The range is from 1 to 123.	N/A
Operation	
Click the +/- button to add mapping or delete mapping.	N/A
Edit	
You can directly click on a specific column to edit its content.	N/A

3.4.5 MQTT

DX-2400L9 supports MQTT Client (Publish/Subscribe) and is compatible with self-hosted MQTT Brokers as well as the Amazon MQTT Broker. It also supports the following features:

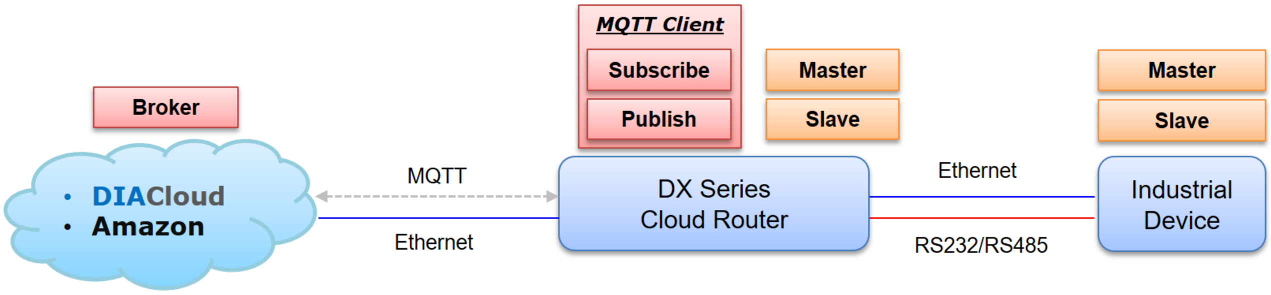
- **QoS (Quality of Service):** Sets the quality of sending and receiving messages, with the option to configure three different conditions.
  1. At most once (0): After MQTT Client sent data, there's no need to confirm whether the Broker has received it.
  2. At least once (1): After MQTT Client sent data, the Broker will send PUBACK packet to confirm the receipt of data.
  3. Exactly once (2): Every time MQTT Client sent data, it undergoes three-way handshake confirmation to verify whether the Broker has received it, ensuring receipt only once.
- **Persistent Session:** To prevent frequent reestablishment of sessions between the client and the server due to network fluctuations, the client can choose to establish a persistent session with the broker. In this case, the broker and the client will retain the following information.

  Client:

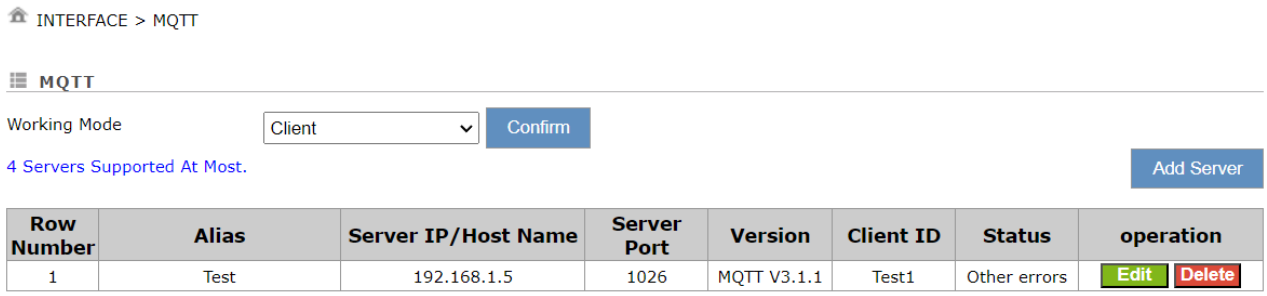
  1. QoS 1 and QoS 2 messages that have been sent to the server but have not yet completed confirmation.
  2. QoS 2 messages received from the server but have not yet completed confirmation.

  Broker:

  1. Session
  2. QoS 1 and QoS 2 messages sent to clients but not yet confirmed.
  3. Awaiting transmission to clients: QoS 0 messages (optional), QoS 1, and QoS 2 messages.
  4. QoS 2 messages received from clients but not yet confirmed, last will messages, and last will delay intervals.
- **Last Will and Testament:** When the MQTT Client comes online, it sends a message that is saved by the Broker. When the Broker detects that the Client has disconnected, it pushes this information to the subscribers.



- **MQTT Setting**



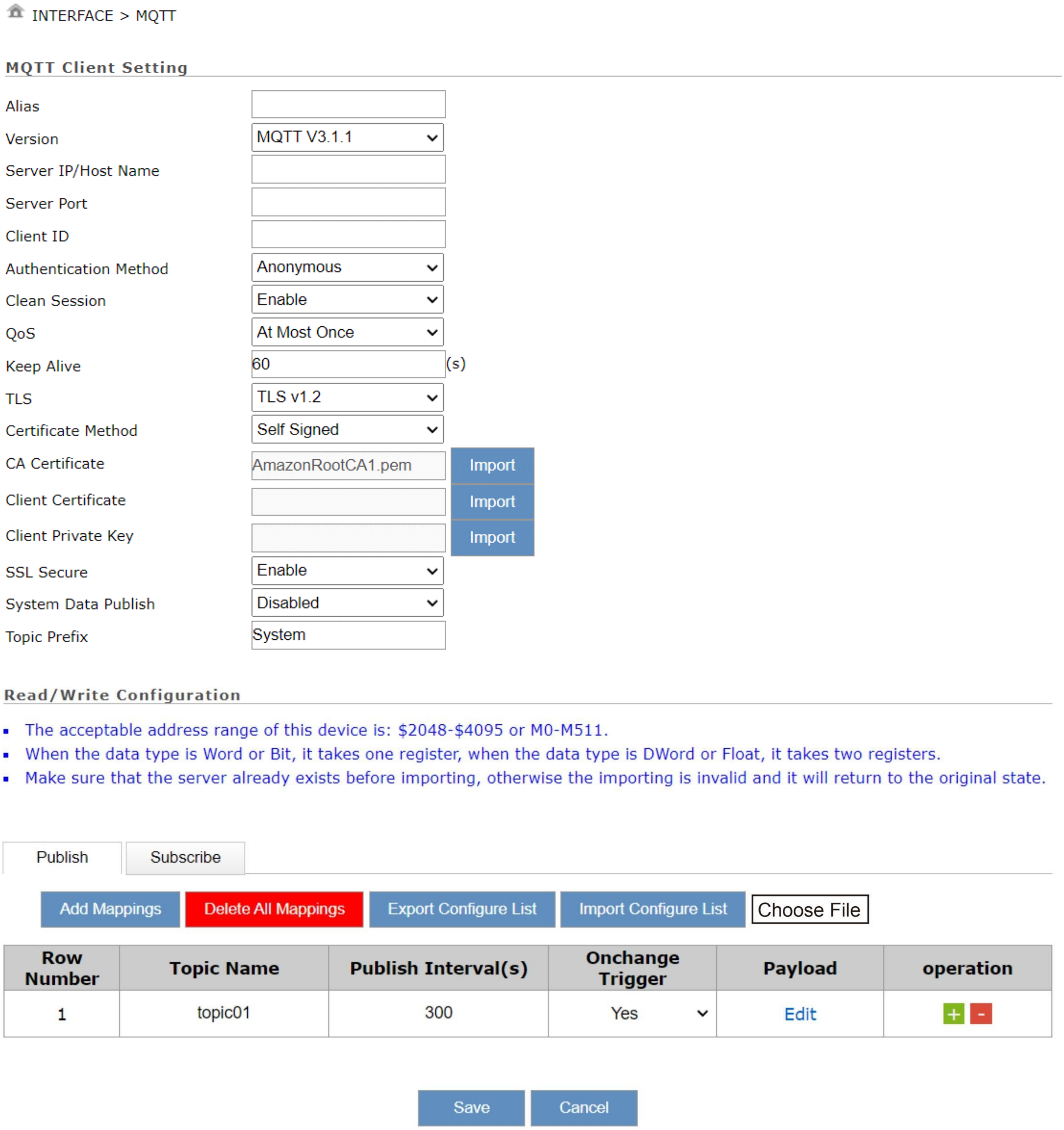
INTERFACE > MQTT

MQTT

Working Mode: Client

4 Servers Supported At Most.

Row Number	Alias	Server IP/Host Name	Server Port	Version	Client ID	Status	operation
1	Test	192.168.1.5	1026	MQTT V3.1.1	Test1	Other errors	Edit Delete



INTERFACE > MQTT

MQTT Client Setting

Alias	
Version	MQTT V3.1.1
Server IP/Host Name	
Server Port	
Client ID	
Authentication Method	Anonymous
Clean Session	Enable
QoS	At Most Once
Keep Alive	60 (s)
TLS	TLS v1.2
Certificate Method	Self Signed
CA Certificate	AmazonRootCA1.pem Import
Client Certificate	Import
Client Private Key	Import
SSL Secure	Enable
System Data Publish	Disabled
Topic Prefix	System

Read/Write Configuration

- The acceptable address range of this device is: $2048-$4095 or M0-M511.
- When the data type is Word or Bit, it takes one register, when the data type is DWord or Float, it takes two registers.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Topic Name	Publish Interval(s)	Onchange Trigger	Payload	operation
1	topic01	300	Yes	Edit	+ -

Description	Default
Add Server	
Add MQTT Broker connections and configure various parameters. User can configure up to four different connection addresses	N/A
Alias	
Set the name. Maximum length is 64 characters	N/A
Server IP Address/Function Variable Name	
Configure the IP address or hostname of the MQTT Broker.	N/A
Server Port	
Configure the port of the MQTT Broker.	N/A
Version	
Set the MQTT protocol version, which must match the Broker's configuration. Options are: ● MQTT V3.1 ● MQTT V3.1.1	MQTT V3.1.1
Client ID	
Set the MQTT Client ID, which is used to identify the device to the Broker.	N/A
Authentication Mode	
Set the MQTT Client authentication method. Options are: ● **Username:** Authenticate using a username/password method. ● **Anonymous:** Authenticate anonymously	Anonymous
Clear Session	
When the Broker and MQTT Client connection is interrupted, whether to continue storing/retaining the client's subscription status, options: ● **Enable:** The Broker does not continue to store/retain the Session, and the MQTT Client will request a new Session each time it reconnects. ● **Disable:** The Broker continues to store/retain the Session, so when the MQTT Client reconnects, it will receive any offline messages if available.	Enable
QoS	
Setting communication quality of service, options: ● **At most once:** The MQTT client send messages without the need to confirm whether the Broker has received them. ● **At least once:** After sending message, the MQTT client will wait for a PUBACK packet to confirm that the Broker has received it. ● **Exactly once:** After each message sent by the MQTT Client, a three-way handshake is performed to confirm whether the Broker has received it, ensuring that it is received only once.	Exactly once

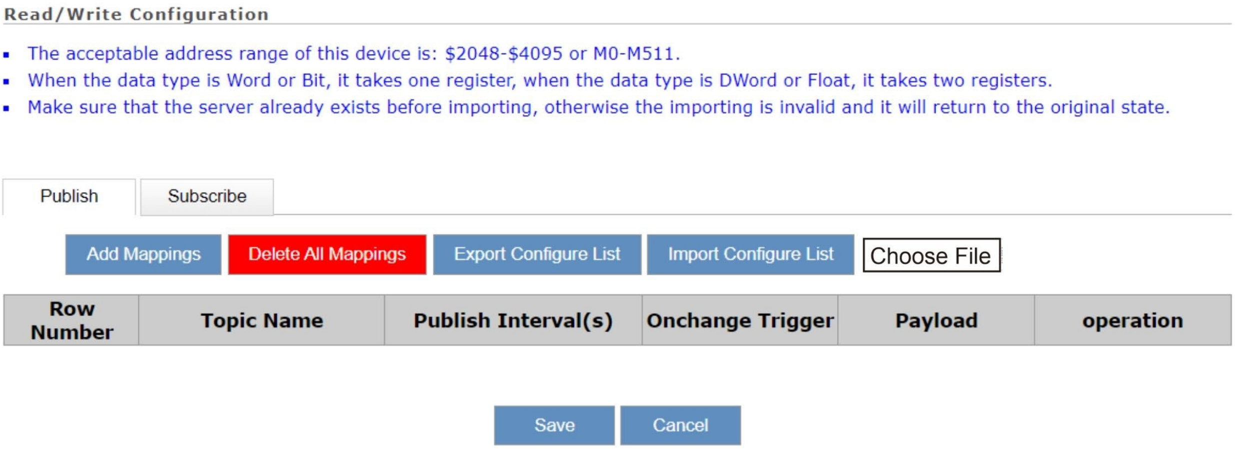
Description	Default
Keep-Alive	
Set the connection's keep-alive time in seconds. As per the MQTT protocol specification, if within an interval of 1.5 * Keep Alive duration, the Broker doesn't receive any data packets from the MQTT Client, it considers the connection between them to be disconnected. Similarly, if the MQTT Client doesn't receive any data packets from the Broker within this interval, it considers the connection to the Broker as disconnected.	60
TLS	
Setting the TLS encryption version used by the MQTT Client, options are: ● TLS v1.1 ● TLS v1.2 ● Disable	Disable
Authentication Mode	
After enabling TLS, users can configure the client's certificate method, with the following options: ● **Self-Signed:** Users import their own certificates, including CA certificate, Client certificate, and Client key. ● **CA-Signed Server:** Utilizes the CA server's certificate.	CA-Signed Server
Automatic Retrieval	
When selecting 'CA-Signed Server,' users can choose whether to automatically retrieve certificates here: ● **YES:** Retrieve certificates from the MQTT Broker server. ● **NO:** Manually import the CA root certificate, client certificate, and client certificate private key.	YES
SSL Safety	
Configure whether to validate the hostname in the server certificate, options are: ● Enable ● Disable	Enable
System Data Upload	
The default system Topic inside the DX Cloud Router is used to publish basic device information, status, and other data. Users can configure whether to publish this system data on the configuration page. **Disable:** Disable System Data Upload **Enable:** The following data will be published to the Broker: ● Device Information: Includes device SN, device name, firmware version information. Any change triggers an upload. Topic name: sys_dev_info. ● Network Status: Includes operator and signal strength information, uploaded every 10 minutes regularly. Topic name: sys_cellular_info. ● Slave Device Communication Status: Includes RS-232, RS-485, and Ethernet status information. Any change triggers an upload. Topic name: sys_slave_status.	Disable

Description	Default

In addition, regardless of whether the user chooses to upload historical data, the following two topics will be published by default:
● When the device comes online, it automatically publishes a topic in JSON format as follows:
<Client ID>/<topic prefix>/sys_status
< Payload> {
“online”: true
}
● Supports the Last Will and Testament mechanism topic in JSON format as follows:
<Client ID>/<topic prefix >/sys_status
<payload> {
“online”: false
}	

Topic Prefix	
Set the prefix for publishing system data topics, which only applies to system topics. For example, if the user enters 'system' here, the final complete topic for device information publishing will be: client_ID/system/sys_dev_info.	N/A

- **Publish Setting**

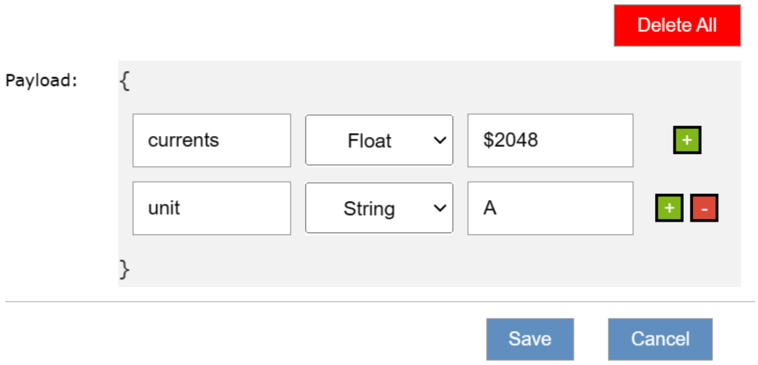

Read/Write Configuration

- The acceptable address range of this device is: $2048-$4095 or M0-M511.
- When the data type is Word or Bit, it takes one register, when the data type is DWord or Float, it takes two registers.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Topic Name	Publish Interval(s)	Onchange Trigger	Payload	operation

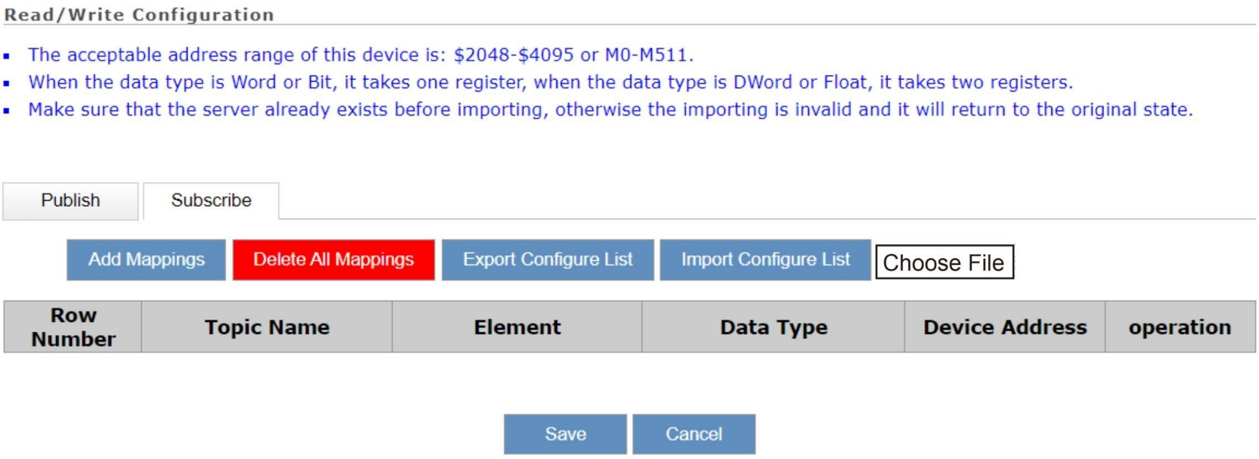
Description	Default
Add Mappings	
Add Publish Topic, users can add up to a maximum of 100 topics for publishing.	N/A
Delete All Mappings	
Delete all Publish Topic settings.	N/A
Export Configure List	
Export Publish Topic settings. The default filename for export is mqtt_publish_mapping_time.cfg	mqtt_publish_mapping_time.cfg
Import Configure List	
Import Publish Topic settings. The file extension must be *.cfg.	**.cfg
Topic Name	
Set the topic name for Publish Topic, allowing users to configure multiple levels with a maximum length of 64 characters. For example, 'Box1/Currents,' and the final complete topic for device information publishing will be: Client_ID/Box1/Currents.	N/A
Publish Interval	
Set the message publish interval in seconds, with a configurable range of 10 to 3600 seconds.	300s
Change Trigger	
Whether to check if the data has changed before publishing the message, options are: ● Yes: Publish data only if it has changed since the last publication. ● No: Publish data regardless of whether it has changed since the last publication.	Yes

Description	Default
Payload	

Configure the content to be uploaded on this topic.

 	
Payload: {
currents Float $2048
unit String A
}
Topic messages are transmitted in JSON format. The payload serves as the message carrier and is composed of key-value pairs. In the figure above, the first item on each line is the key's name, with a maximum length of 64 characters. The second item indicates the data type for that key, and the third item specifies the source register for the key's value. Supported data types include:
● **Word：** Takes a single Word from the specified register as the key's value. Valid register addresses are from $2048 ~ $4095.
● **DWord：** Takes two Words from the specified register and combines them as the key's value. Valid register addresses are from $2048 ~ $4095.
● **Float：**Takes two Words from the specified register and converts the data to a Float type using the IEEE754 standard, serving as the key's value. Valid register addresses are from $2048 ~ $4095.
● **Bit:** Represents boolean data with values of 0 or 1. Valid register addresses are from M0 to M511.
● **String:** Non-variable, publishes whatever the user inputs, supports special symbols such as '℃' and '%'. With a maximum length of 64 characters.
Users can create a maximum of 30 keys in the payload, and the total number of keys across all MQTT clients cannot exceed 3000.
	N/A

Operation	
Click the +/- button to add topic or delete topic.	N/A

• Subscribe Setting



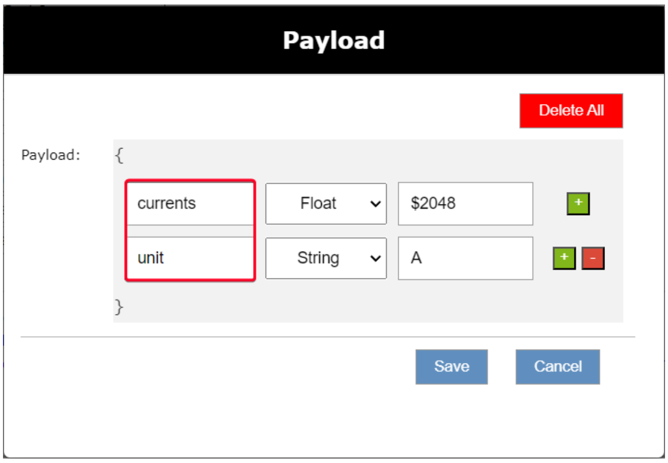
Read/Write Configuration

- The acceptable address range of this device is: $2048-$4095 or M0-M511.
- When the data type is Word or Bit, it takes one register, when the data type is DWord or Float, it takes two registers.
- Make sure that the server already exists before importing, otherwise the importing is invalid and it will return to the original state.

Row Number	Topic Name	Element	Data Type	Device Address	operation

Description	Default
Add Mappings	
Add Subscribe Topic. Users can add 200 topics at most.	N/A
Delete All Mappings	
Delete all Subscribe Topic settings.	N/A
Export Configure List	
Export the Subscribe Topic settings. The default file name for the export is \`mqtt_subscribe_mapping_time.cfg\`.	mqtt_ subscribe _mapping_time.cfg
Import Configure List	
Import the Subscribe Topic settings with a file extension of *.cfg.	****.cfg**
Topic Name	
Set the topic names that needed to be retrieve data. ● If no component identifier (Element) is provided and only the topic name (Topic Name) is filled, then all data within the topic name will be retrieved. ● If both the component identifier (Element) and topic name (Topic Name) are provided, then only data matching the component identifier will be retrieved.	N/A

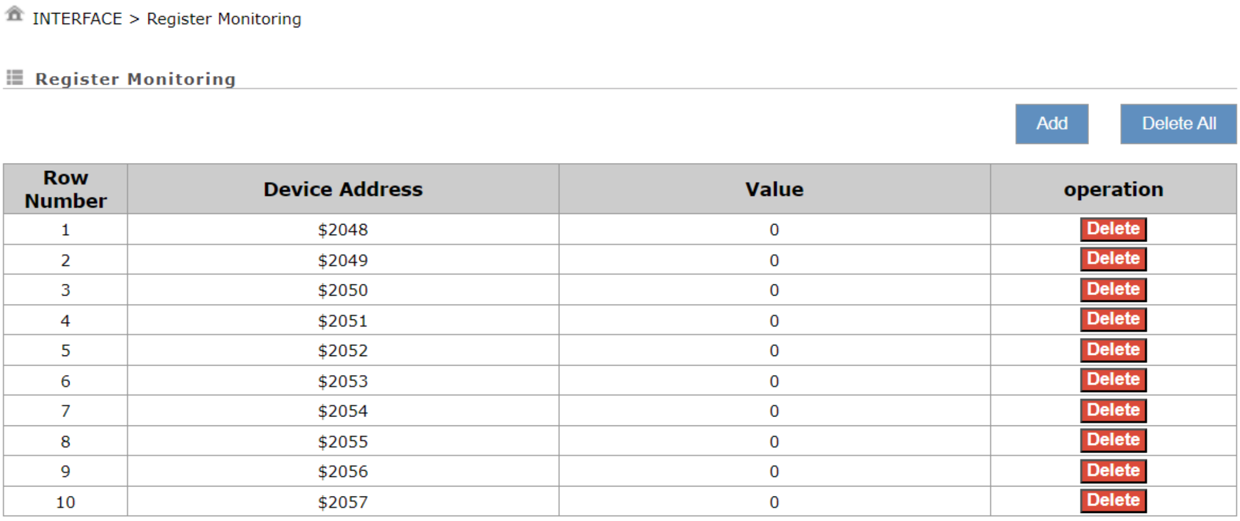
Description	Default
Component Identifier	

This represents the field in the Payload where the data name is located (highlighted in red). The purpose is to specify a particular data name and capture only that data record.

Payload
Delete All
Payload: {
currents Float $2048 +
unit String A + -
}
Save Cancel	

Data Type	
Set the data type of the message: ● Word：Write the parsed value to the specified address in the register. ● DWord：Write the parsed value to the specified address and the address + 1 of the two registers. ● Float：Reversely convert the Float data using the IEEE 754 standard, and then write the parsed value to the specified address and the address + 1 of the two registers. ● Bit: Write the parsed value to the specified address in the register. The data must be of boolean type with values of 0 or 1.	300
Device Address	
Configure the parsed values from the Subscribe Topic to be written to the DX Cloud Router registers as follows: ● Word/DWord/Float： Register addresses range from $2048 to $4095. ● Bit： Register addresses range from M0 to M511.	N/A
Operation	
Click the +/- button to add topic or delete topic.	N/A

3.4.6 Register Monitoring

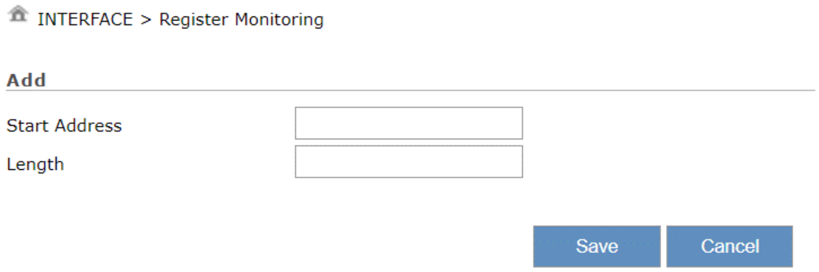
Users can use this feature to monitor the real-time values of registers M0-M511 and $2048-$4095 on the device. This is valuable for data acquisition applications, allowing users to verify whether various settings are correctly applied and whether communication with the lower computer is functioning correctly.



INTERFACE > Register Monitoring

Register Monitoring

Row Number	Device Address	Value	operation
1	$2048	0	Delete
2	$2049	0	Delete
3	$2050	0	Delete
4	$2051	0	Delete
5	$2052	0	Delete
6	$2053	0	Delete
7	$2054	0	Delete
8	$2055	0	Delete
9	$2056	0	Delete
10	$2057	0	Delete



INTERFACE > Register Monitoring

Add

Start Address

Length

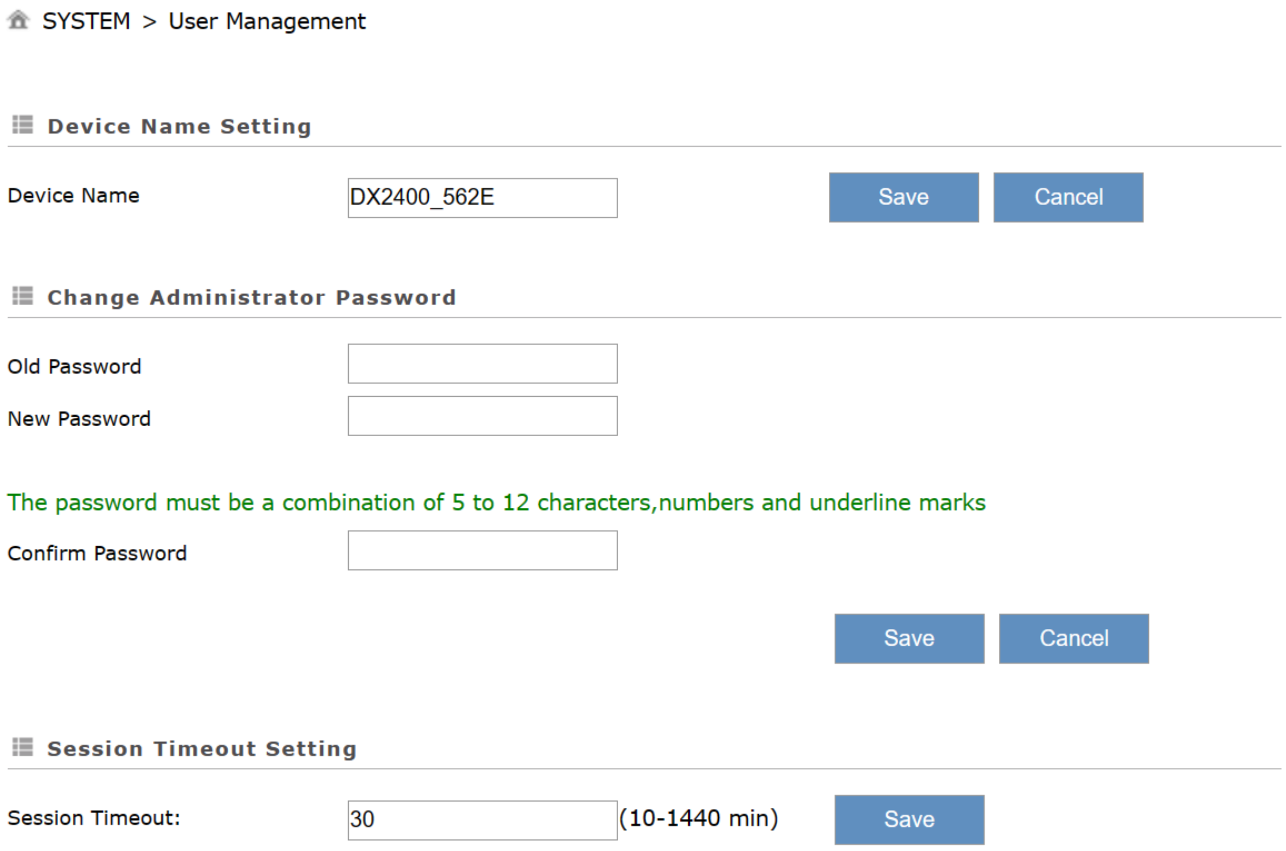
Description	Default
Add	
Add the register address that need to be monitored. User can add up to 100 register locations.	N/A
Delete All	
Delete all monitored register addresses.	N/A
Device Starting Address	
Input the internal register addresses of the DX Cloud Router that need to be monitored, including addresses from $2048 to $4096 and M0 to M511.	N/A
Value	
Display the values of the register address, updating every second.	N/A
Operation	
Delete the register monitoring settings.	N/A

3.5 SYSTEM

You can set up the system configurations, including the User Management, Time Zone Configurations, Log Setting, Firmware Upgrade, Backup & Restore, System Reboot, Network Diagnosis, Trouble Shooting, Scheduled Jobs, Privilege Management, Event Management, Register Management and Data Local Storage.

3.5.1 User Management

This page is to set the web administrator password and the web timeout duration.



SYSTEM > User Management

Device Name Setting

Device Name: DX2400_562E

Change Administrator Password

Old Password

New Password

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

Confirm Password

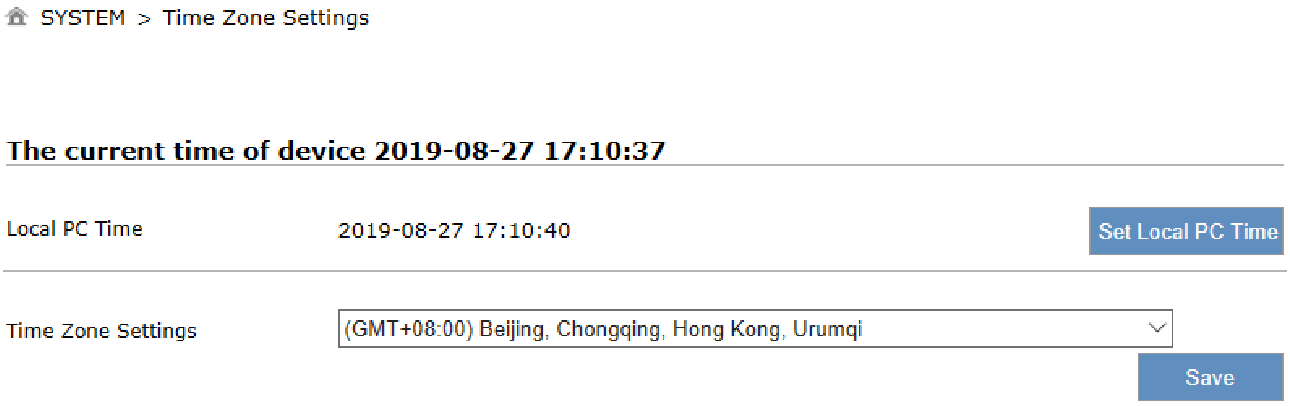
Session Timeout Setting

Session Timeout: 30 (10-1440 min)

Description	Default
Device Name	
Set a device name for the DX cloud router. The name should consist of letters, numbers, and underline, and must start with a letter or number. The maximum string length is 32 bytes.	DX2400 + "_" + "The last four digits of the MAC address."
Old Password	
The old password for the web administrator. The default username and password for the router are "admin/admin".	admin
New Password	
Set a new password for the web administrator. The password should be between 5 to 12 characters in length and can consist of uppercase and lowercase letters (case sensitive), numbers (0-9), and underlines.	N/A
Comfirm Password	
The new password for the web administrator.	N/A
Session Timeout	
This function is used to configure the session timeout duration after user logs into the configuration web page. The session will timeout if there is no activity for a specified duration, and the user will need to log in again to continue. You can set the timeout duration within the range of 10 to 1440 minutes.	30

3.5.2 Time Zone Configurations

This page is used to configure the router's time zone. Users can choose a time zone, and after making changes, the system will automatically restart and, in a networked environment, synchronize to the accurate time of that selected time zone.


SYSTEM > Time Zone Settings

The current time of device 2019-08-27 17:10:37

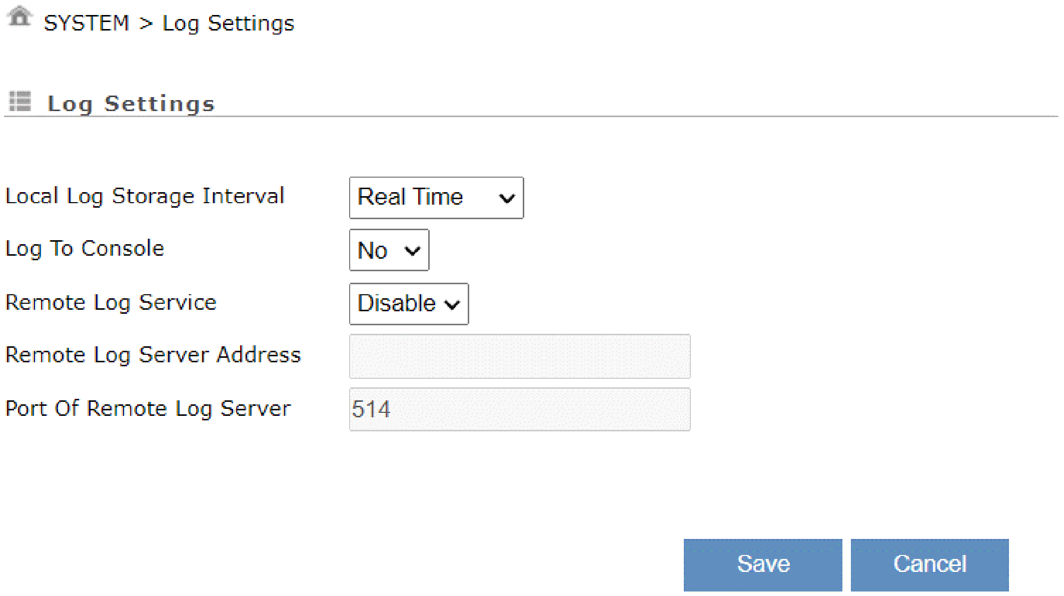
Local PC Time 2019-08-27 17:10:40

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

Description	Default
The current time of the router.	
Display the current router time.	N/A
Set to local PC time	
Clicking this option will synchronize with the time on your PC.	N/A
Time Zone Setting	
Select the time zone for the router: GMT-12:00 to GMT+13:00.	GMT+08:00

3.5.3 Log Settings

This page is for configuring the router's log settings, including logging output to the debugging port and setting up remote log services.



SYSTEM > Log Settings

Log Settings

Local Log Storage Interval: Real Time

Log To Console: No

Remote Log Service: Disable

Remote Log Server Address:

Port Of Remote Log Server: 514

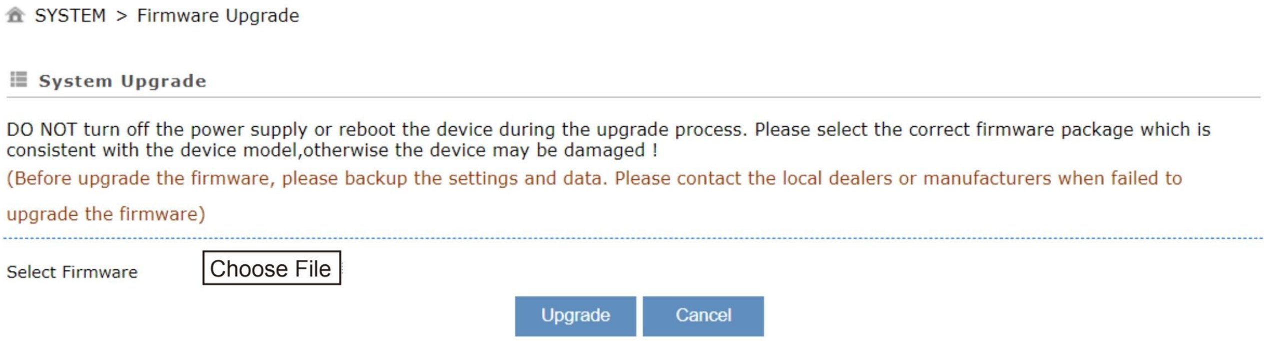
Description	Default
Log Local Save Interval	
Set the interval for saving log files. Options include real-time, 1 minute, 5 minutes, 10 minutes, 30 minutes, 120 minutes, or disabled.	Real-Time
Log Output to Debugging Port	
This option allows local logs to be output to the router's debugging port.	Disable
Remote Log Service	
Enable/disable the remote log service feature.	Disable
Remote Log Server Address	
Configure the remote log server address.	N/A
Log Server Port	
Set the port number for the remote log server address, with range from 1 to 65534.	514

⚠ **Notice**

Remote log service is used for 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 consume network traffic. It is advisable to keep it disabled unless necessary.

3.5.4 Firmware Upgrade

This page is used for upgrading the system.



SYSTEM > Firmware Upgrade

System 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 !

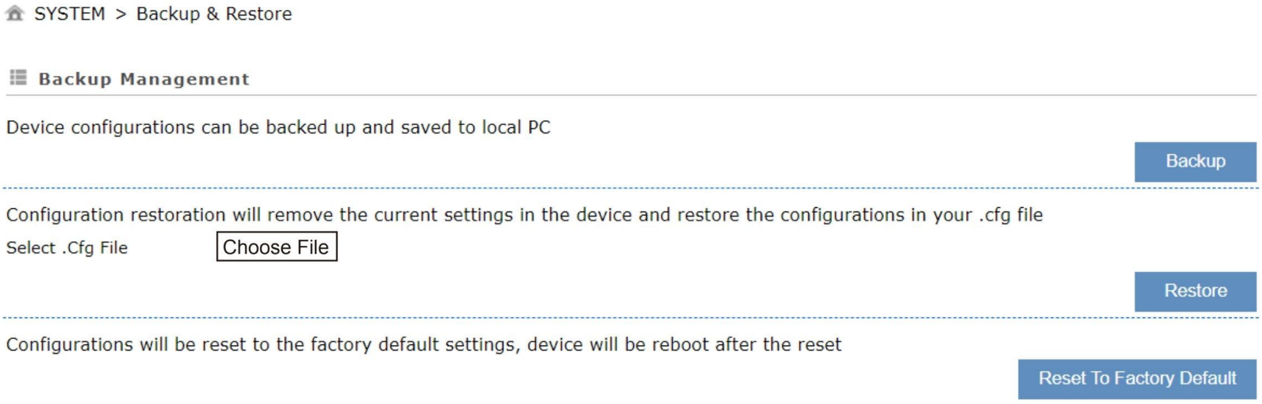
(Before upgrade the firmware, please backup the settings and data. Please contact the local dealers or manufacturers when failed to upgrade the firmware)

Select Firmware

Description	Default
Select Firmware	
Click the "Choose File" button to select the upgrade file **.bin from your local device and upload it to the device.	N/A
Upgrade	
Clicking this button will upgrade the device's firmware.	N/A

3.5.5 Backup & Restore

This page is used for router configuration management, including data backup, data restoration, and restoring default settings, among other functions.



SYSTEM > Backup & Restore

Backup Management

Device configurations can be backed up and saved to local PC

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

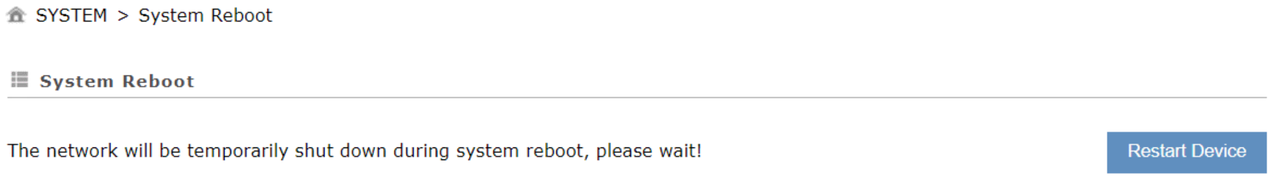
Select .Cfg File

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

Description	Default
Backup	
Backup the current router configuration information.	backup.cfg
Restore	
Restore the router configuration information using the previously backed-up settings file.	N/A
Restore Factory Settings	
Restore the router to its factory default settings.	N/A

3.5.6 System Reboot

Users can manually restart the cloud router.



SYSTEM > System Reboot

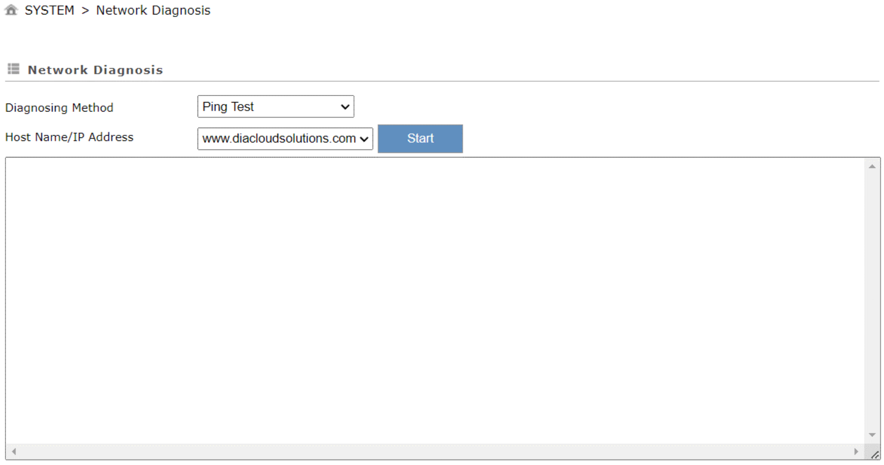
System Reboot

The network will be temporarily shut down during system reboot, please wait!

Description	Default
Restart the gateway	
The cloud router will be restarted.	N/A

3.5.7 Network Diagnosis

This feature provides a simple diagnostic tool to check the communication status between the cloud router and the Internet and DIACloud network. Users can use it to assess the status and troubleshoot any issues.



SYSTEM > Network Diagnosis

Network Diagnosis

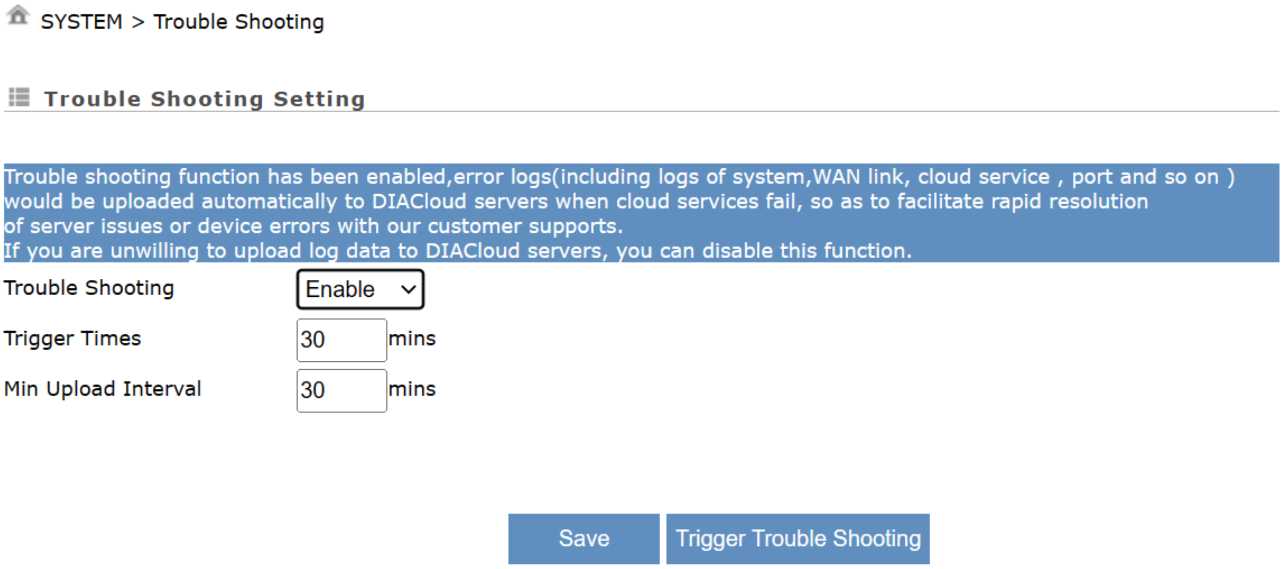
Diagnosing Method: Ping Test

Host Name/IP Address: www.diacloudsolutions.com

Description	Default
Diagnosis Type	
Choose the diagnosis type, with options "Ping Test," "Route Tracing," and "Cloud Service Diagnosis." ● **Ping Test:** Perform a Ping test between the cloud router and a specific Host name/IP Address. ● **Route Tracing:** Trace the path between the cloud router and a specific Host name/IP Address. ● **Cloud Service Diagnosis:** Check the status of the cloud router's connection to the DIACloud network.	Ping Test
Hostname/IP Address	
Set the target's functional variable name or IP address. Options are:www.baidu.com, www.sohu.com, www.sina.com.cn, www.163.com, www.taobao.com, www.qq.com, www.diacloudsolutions.com and "Other." When selecting "Other," users can manually enter the functional variable name name or IP address. ⚠**Notice**: When selecting "Cloud Service Diagnosis," this item cannot be configured.	www.diacloudsolutions.com
Start	
Quick button used to initiate the diagnostic testing process. When you click this button, both the "Diagnosis Type" and "Hostname/IP Address" fields will become unselectable or non-inputtable.	N/A
Stop	
Quick button used to stop the diagnostic testing process. When you click this button, both the "Diagnosis Type" and "Hostname/IP Address" fields will become selectable or inputtable.	N/A

3.5.8 Trouble shooting

This feature is typically not needed to be activated, but it should only be used when recommended by the manufacturer's personnel for troubleshooting purposes requiring extended log retrieval.



SYSTEM > Trouble Shooting

Trouble Shooting Setting

Trouble shooting function has been enabled,error logs(including logs of system,WAN link, cloud service , port and so on) would be uploaded automatically to DIACloud servers when cloud services fail, so as to facilitate rapid resolution of server issues or device errors with our customer supports.
If you are unwilling to upload log data to DIACloud servers, you can disable this function.

Trouble Shooting: Enable

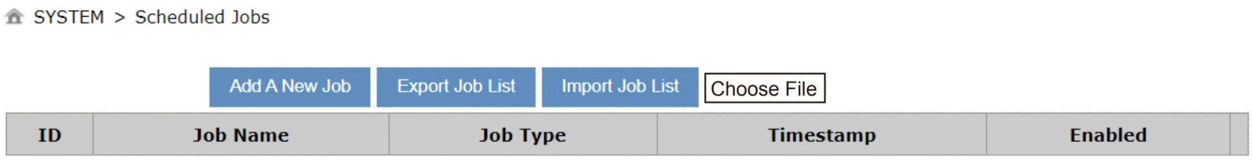
Trigger Times: 30 mins

Min Upload Interval: 30 mins

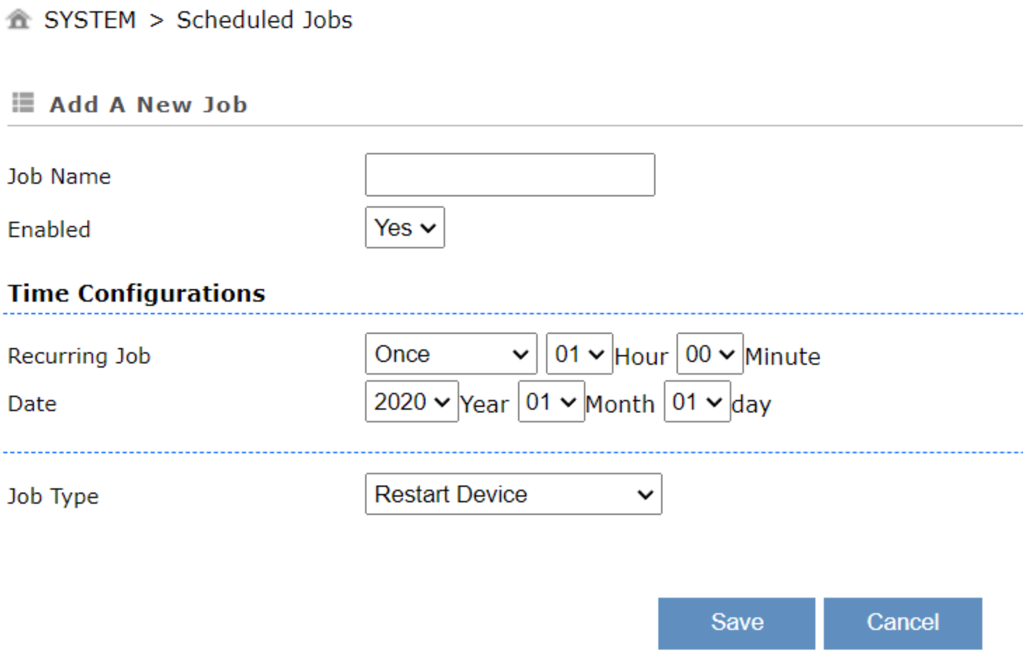
Description	Default
Trouble Shooting	
- **Enable:** When the device fails to connect to DIACloud for more than 30 minutes, it will perform the following actions: automatically upload all device logs to a specified server directory for remote analysis by engineers to locate device faults. If the issue persists, the log upload interval will gradually increase to 1/2/4/8/16/24 hours, and then remain fixed at 24 hours. - **Disable:** Turn off this function.	Disable
Trigger Times	
Set how long the continuous cloud service disruption after which automatic log upload will begin.	30
Min Upload Interval	
If the cloud service remains abnormal, automatic log uploads will occur at regular intervals. These intervals start at the minimum time, then double (minimum time * 2), quadruple (minimum time * 4), and so on, up to 24 hours. After reaching the 24-hour interval, the log uploads will continue at that frequency.	30
Trigger Trouble Shooting	
Immediate log upload.	N/A

3.5.9 Scheduled Jobs

This feature allows users to create task to execute specific functions on the cloud router at scheduled intervals. For example, tasks could include restarting the router, enabling cloud services, disabling cloud services, enabling Cellular Network, or disabling Cellular Network.



ID	Job Name	Job Type	Timestamp	Enabled



Job Name

Enabled: Yes

Time Configurations

Recurring Job: Once 01 Hour 00 Minute

Date: 2020 Year 01 Month 01 day

Job Type: Restart Device

Description	Default
Add A New Job	
Add a new scheduled job with a maximum of 10 new jobs.	N/A
Export Job List	
Export scheduled job list with the default file name “Schedule_task.cfg”	Schedule_task.cfg
Import Job List	
Import scheduled job list with the default file exention “*.cfg”	N/A
Job Name	
Set up name for the 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

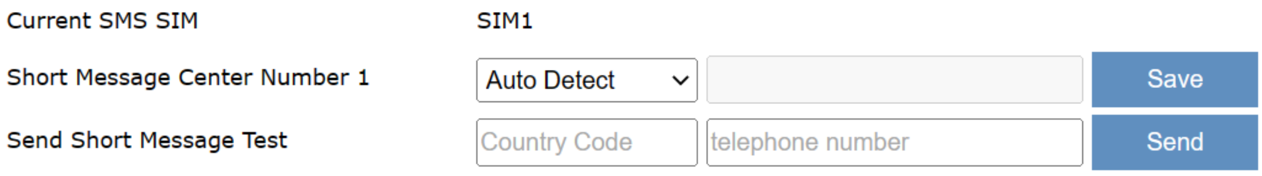
Description	Default
Enable	
Choose whether this scheduled job is effective or not, with the options "Enable" or "Disable."	Enable
Frequency	
Choose the task execution frequency, with the options "Once," "Daily," "Weekly," "Monthly," and the default being "Once." Frequency details are as follows: ● **Once**: You can specify a specific date and time for job execution. ● **Daily**: You can specify a specific time for job execution every day. ● **Weekly**: You can set the job to run at a specific time on specific days of the week. ● **Monthly**: You can set the task to run at a specific time on a particular day of the month.	Once/01/00(hour/min); 2015/01/01(year/month /day)
Job Type	
Select the type of job you want to execute, with the options “Restart Device”, “Enable DIACloud”, “Disable DIACloud”, “Enable Cellular Network”, “Disable Cellular Network”.	Restart Device

3.5.10 Privilege Management

This feature utilizes a SIM card with activated SMS functionality to enable DX Cloud Router to send SMS commands to control PLC, send SMS queries to check PLC register status, and send SMS alert messages.

3.5.10.1 Send Short Message Test

This feature checks whether the SIM card has activated SMS functionality.



Current SMS SIM SIM1

Short Message Center Number 1 Auto Detect

Send Short Message Test Country Code telephone number

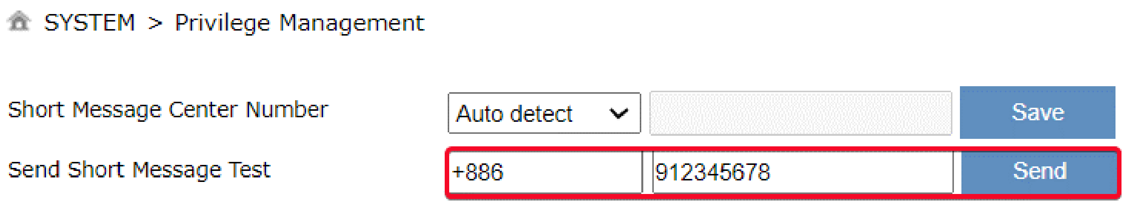
Description	Default
Current SMS SIM	
Display the currently used SIM card.	N/A
Short Message Center Number 1	
Configure the short message service center (smsc) number on the SIM card. 1. **Auto Detect:** Automatically detect the smsc number. 2. **Manual Setting:**，If you are unable to send text messages even after using the "Auto Detect" feature, it may be due to an incorrect Short Message Service Center (SMSC) Number. In this case, users should contact their SIM card provider to obtain the correct SMSC number and enter it manually. **The format should be: "+" "country code" "SMSC number." For example: +8613800100500.**	Auto Detect
Send Short Message Test	
When using the SMS functionality, it's important to test whether the SIM card's SMS feature is activated and ensure that both the SMS center number and recipient's number are correct. ● Input format is as follows: Country Code**: "+" "Country Code".** ● Phone Number: **13800100500.** ● Example: **+8613800100500.**	N/A

Setup Steps

1. Start by placing the SIM card into your own mobile phone. Choose any contact and send a text message to confirm whether it can be sent successfully. If successful, proceed to step 2.

2. Turn off the cloud router, insert the SIM card into the router, and then power it on. Wait until the cloud router's "Ready" indicator light is on and the 3G/4G LED displays a signal strength of at least two bars.

3. Log in to the cloud router, go to **SYSTEM** > **Privilege Management**. In the "**Send Short Message Test**" section, enter the phone number where you want to receive the text message.



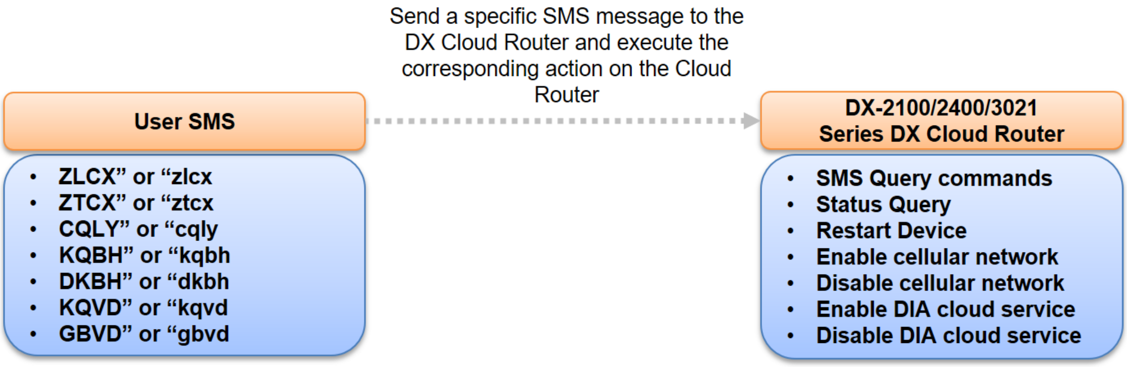
SYSTEM > Privilege Management

Short Message Center Number	Auto detect		Save
Send Short Message Test	+886	912345678	Send

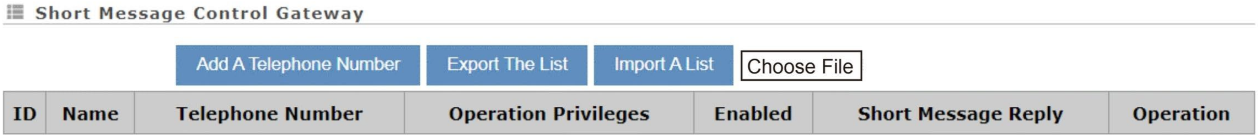
4. Verify whether +886912345678 has received the text message "Test message from DX3021__XXXX." If the message is received, then the SMS functionality of this SIM card is working correctly.

3.5.10.2 Short Message Control Gateway

By sending specific text messages to the DX Cloud Router, user can trigger corresponding actions or functions to be executed by the router.

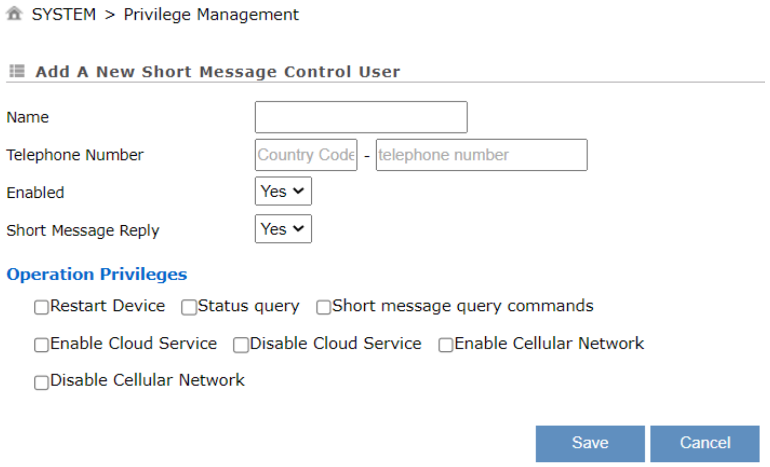


Function	SMSCommand	Description
SMS Query commands	"ZLCX" or "zlcx"	List all SMS commands and explanations.
Status Query	"ZTCX" or "ztcx"	Query the router's status information, including the following: 1. 4G/3GCellular network state 2. Firewall state 3. DIA Cloud state
Restart Device	"CQLY" or "cqly"	Restart the router
Enable cellular network	"KQBH" or "kqbh"	Enable mobile network service on the cloud router.
Disable cellular network	"DKBH" or "dkbh"	Disable mobile network service on the cloud router.
Enable DIA cloud service	"KQVD" or "kqvd"	Enable DIA cloud service on the router.
Disable DIA cloud service	"GBVD" or "gbvd"	Disable DIA cloud service on the router.



ID	Name	Telephone Number	Operation Privileges	Enabled	Short Message Reply	Operation

Description	Default
Add A Telephone Number	
Add up to 10 allowed phone numbers for controlling the cloud router.	N/A
Expore The List	
Export the control settings list.	**Fixed_sms_control_list.cfg**
Import A List	
Import the control settings list.	N/A



SYSTEM > Privilege Management

Add A New Short Message Control User

Name	
Telephone Number	Country Code - telephone number
Enabled	Yes
Short Message Reply	Yes

Operation Privileges

□Restart Device □Status query □Short message query commands

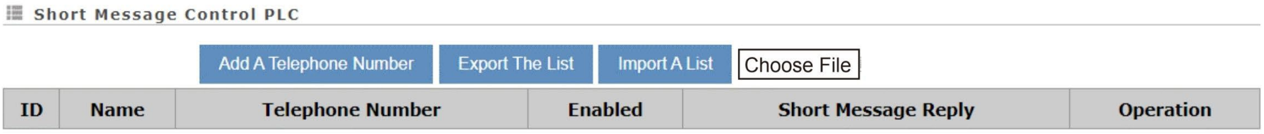
□Enable Cloud Service □Disable Cloud Service □Enable Cellular Network

□Disable Cellular Network

Description	Default
Name	
Set up a name for phone number, The name shall be composed of letters, numbers, and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Telephone Number	
Set up a telephone number and country code which can receive the message. The input format is as follows: ● Country Code: **"+" "Country Code".** ● Cell phone number: **13800100500.** ● **Example: +8613800100500**	N/A
Enable	
Set the effectiveness of this feature field, with options "Enable" or "Disable."	Enable
Short Message Reply	
Set whether the router should respond a confirmed message when receiving the SMS commands. Options are "Yes" or "No."	Yes
Operation Privileges	
Configure the operational permissions associated with the phone number, applicable only on the SMS control router module. ● Restart device: Reboot the cloud router device. ● Status query: Check the router's internet status (status of signal strength, internet connection, firewall, DIACloud connection, SMS.) ● Short message query commands: List all SMS commands and explanations. ● Enable cloud service: Enable cloud service on the router. ● Disable cloud service: Disable cloud service on the router. ● Enable cellular network: Enable mobile network service on the cloud router. ● Disable cellular network: Disable mobile network service on the cloud router.	N/A

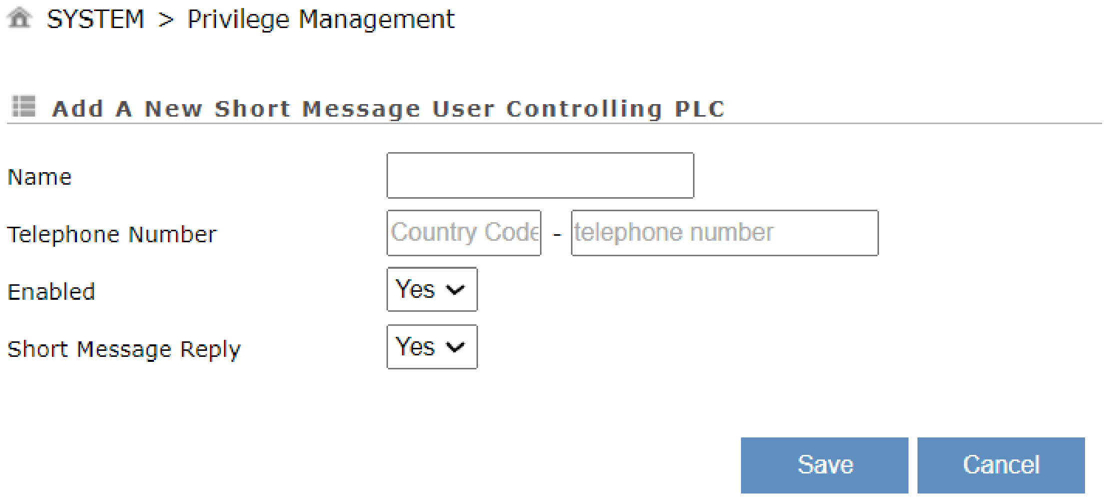
3.5.10.3 PLC Short Message Control PLC

Users can send specific text messages to trigger specific actions on PLC. This functionality is supported by the cloud router only in slave mode.



Short Message Control PLC

ID	Name	Telephone Number	Enabled	Short Message Reply	Operation



SYSTEM > Privilege Management

Add A New Short Message User Controlling PLC

Name	
Telephone Number	Country Code - telephone number
Enabled	Yes
Short Message Reply	Yes

- **Operating Principle:**

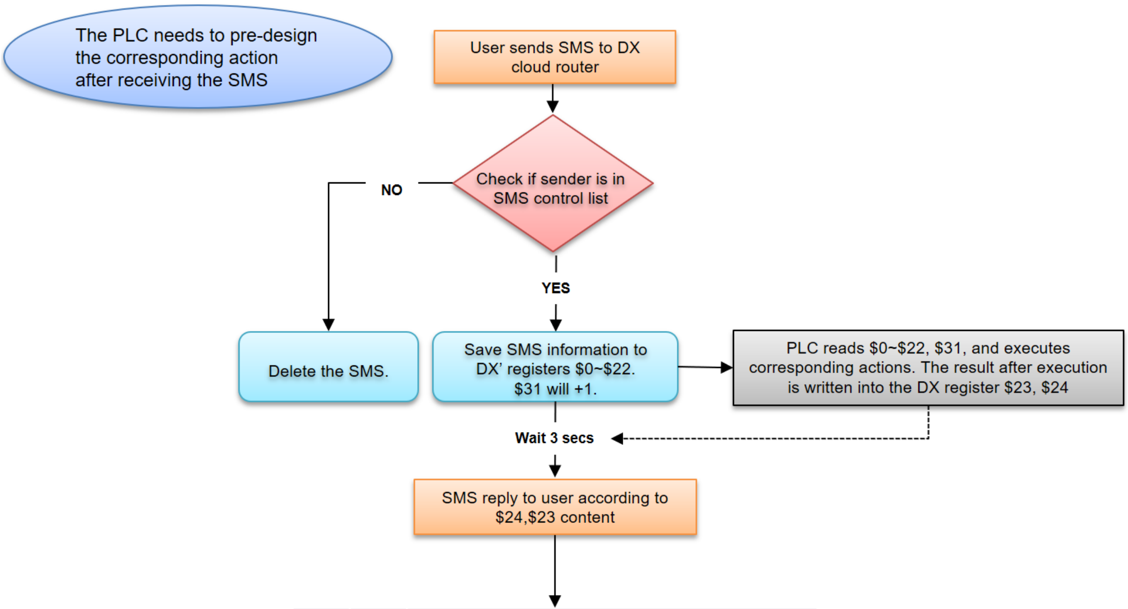
When the cloud router receives a text message, it stores the phone number and message content in the cloud router's registers $12-$22, with $31 representing the number of received text messages. The PLC uses the content of these registers received through the cloud router to determine the corresponding action to execute. Finally, the PLC writes the execution result to the cloud router's registers $23-$24. Based on the values in $23-$24, the cloud router sends a text message response to the user indicating the PLC's execution status.

- **Cloud Router Register List**

DX Register Address	MODBUSAddress		Description	
	DEC	HEX		
$0	0	0	3G/4G mobile network signal strength: (0~31) ● **DX-2400 Series** a. No LED on: 0, No signal. b. One LED on: 1-10. c. Two LED on: 11-20. d. Three LED on: 21-31. ● **DX-30X1 Series** a. No LED on: 0, No signal. b. One LED on: 1-10. c. Two LED on: 11-20. d. Three LED on: 21-31. ● **DX-2100 Series** a. No LED on: 0, No signal. b. One LED on: 1-7. c. Two LED on: 8-13. d. Three LED on: 14-19. e. Four LED on: 20-25. f. Five LED on: 26-31.	
$1-$10	1~10	1~A	The IMSI (International Mobile Subscriber Identity) number of the SIM card.	
$11	11	B	Corresponding status for each bit. 1: Normal 0: Abnormal	bit0：SIM Card
				bit1：GPRS/3G/LTE
				bit2：DIACloud Service
$12-$22	12-22	C-16	Phone number+SMS content.	
$23	23	17	PLC needs to customize error codes in $23, as shown below: ● $23=1: Incorrect IMSI comparison. ● $23=2: AAAA execution failed. ● $23=3: BBBB execution failed. ● $23=4: CCCC execution failed.	
$24	24	18	PLC needs to write the execution result code to $24 as follows: ● 0: PLC task execution failed. ● 1: PLC task execution succeeded.	
$31	31	1F	The number of received SMS messages.	

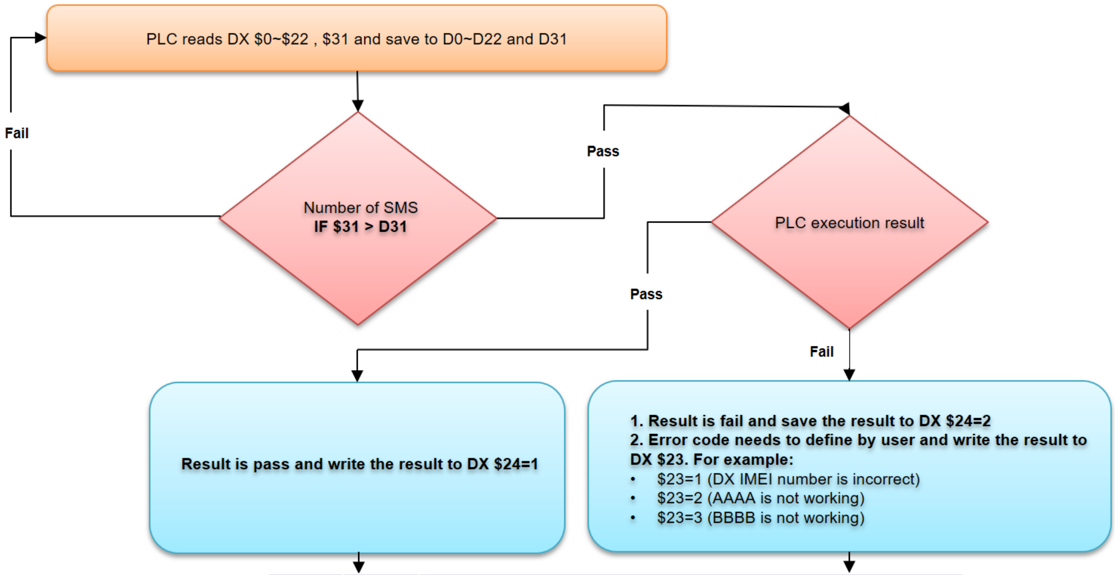
Flowchart and Application

1. Cloud Router Processing Flow


The PLC needs to pre-design the corresponding action after receiving the SMS
User sends SMS to DX cloud router
Check if sender is in SMS control list
NO
YES
Delete the SMS.
Save SMS information to DX' registers $0~$22. $31 will +1.
PLC reads $0~$22, $31, and executes corresponding actions. The result after execution is written into the DX register $23, $24
Wait 3 secs
SMS reply to user according to $24,$23 content

$24	$23	SMS Reply Content
1	N/A	#SMS Content# ok
2	1	#SMS Content# fail, RM code is 1
2	2	#SMS Content# fail, RM code is 2
2	3	#SMS Content# fail, RM code is 3
0	N/A	fail, You failed to send message to plc.

2. PLC Processing Flow

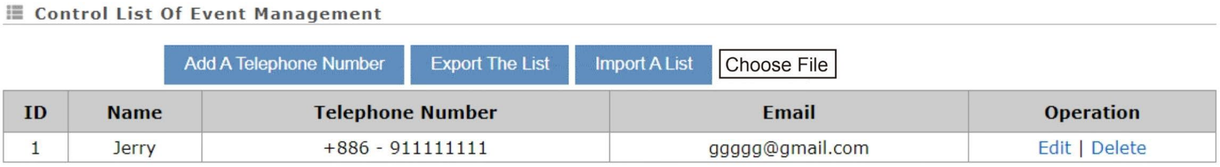

PLC reads DX $0~$22 , $31 and save to D0~D22 and D31
Fail
Number of SMS
IF $31 > D31
Pass
PLC execution result
Pass
Fail
Result is pass and write the result to DX $24=1
1. Result is fail and save the result to DX $24=2
2. Error code needs to define by user and write the result to DX $23. For example:
• $23=1 (DX IMEI number is incorrect)
• $23=2 (AAAA is not working)
• $23=3 (BBBB is not working)

$24	$23	SMS Reply Content
1	N/A	#SMS Content# ok
2	1	#SMS Content# fail, RM code is 1
2	2	#SMS Content# fail, RM code is 2
2	3	#SMS Content# fail, RM code is 3
0	N/A	fail, You failed to send message to plc.

Description	Default
Add A Telephone Number	
Add up to a maximum of 10 allowed phone numbers to control the cloud router.	N/A
Export The List	
Export the control setting list.	fixed_sms_plc_list.cfg
Import A List	
Import the control setting list.	N/A
Name	
Set up a name for phone number, The name shall be composed of letters, numbers, and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Telephone Number	
Set up a telephone number and country code which can receive the alarm message. The input format is as follows: ● Country Code: **"+" "Country Code".** ● Cell phone number: **13800100500.** **Example: +8613800100500**	N/A
Enabled	
Set up the permission to enable or disable.	Yes
Short Message Reply	
When the router receives the SMS commands, the router will response a confirmed message.	Yes
Email	
Set up an Email address to receive the alarm message. This setting work with The Event management.	N/A
Operation	
Edit or delete the users’ data.	N/A

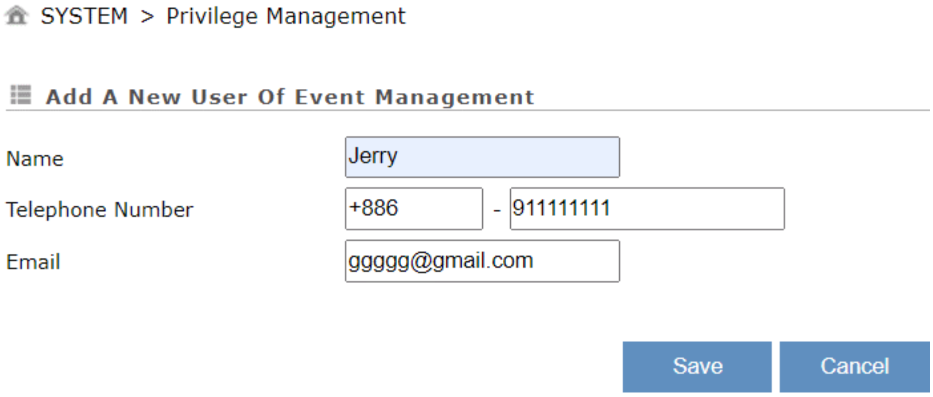
3.5.10.4 Control List of Event Managemnt

Setting up user previlege list. This list primarily manages the functionality where DX Cloud Router can send email alerts to other users or allow users to query real-time register data within DX Cloud Router through text messages.



Control List Of Event Management

ID	Name	Telephone Number	Email	Operation
1	Jerry	+886 - 911111111	ggggg@gmail.com	Edit | Delete



SYSTEM > Privilege Management

Add A New User Of Event Management

Name	Jerry
Telephone Number	+886 - 911111111
Email	ggggg@gmail.com

Description	Default
Add A Telephone Number	
Add up to a maximum of 10 allowed phone numbers to control the cloud router.	N/A
Expore The List	
Export the control setting list.	**Fixed_sms_event_list.cfg**
Import A List	
Import the control setting list.	N/A
Name	
Set up a name for phone number, The name shall be composed of letters, numbers, and underline, starting with a letter or number. The maximum string length is 32 bytes.	N/A
Telephone Number	
Set up a telephone number which can receive the alarm message. Please enter the country code and phone number separately in the respective fields. The input format is as follows: ● Country Code: **"+" "Country Code".** ● Cell phone number: **13800100500.** **Example: +8613800100500**	N/A

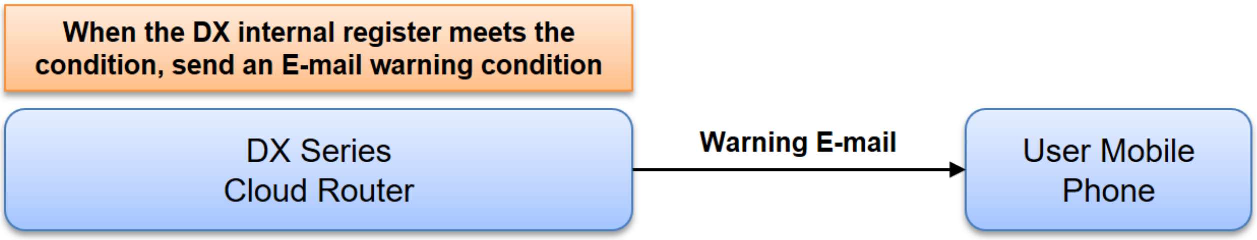
Description	Default
Email	
Enter the email address to which you want to send the alarm.	N/A
Operation	
Edit or delete the users' data.	N/A

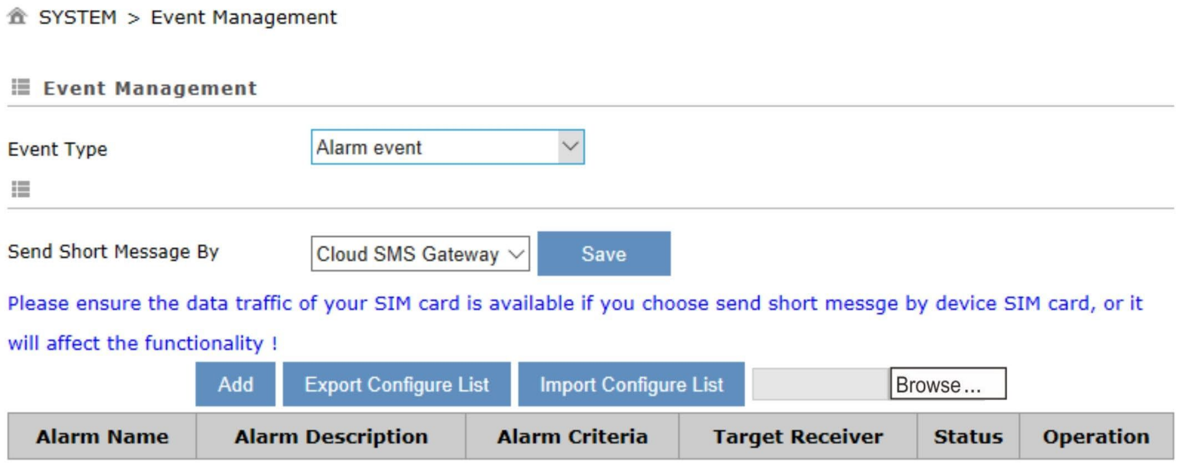
3.5.11 Event Management

Event management primarily consists of two main functions: alarm event and SMS queries event.

- **Alarm Event:**

DX Cloud Router can be configured to send email alerts to other users after triggering conditions are met for specific registers.


When the DX internal register meets the condition, send an E-mail warning condition
DX Series Cloud Router
Warning E-mail
User Mobile Phone



SYSTEM > Event Management

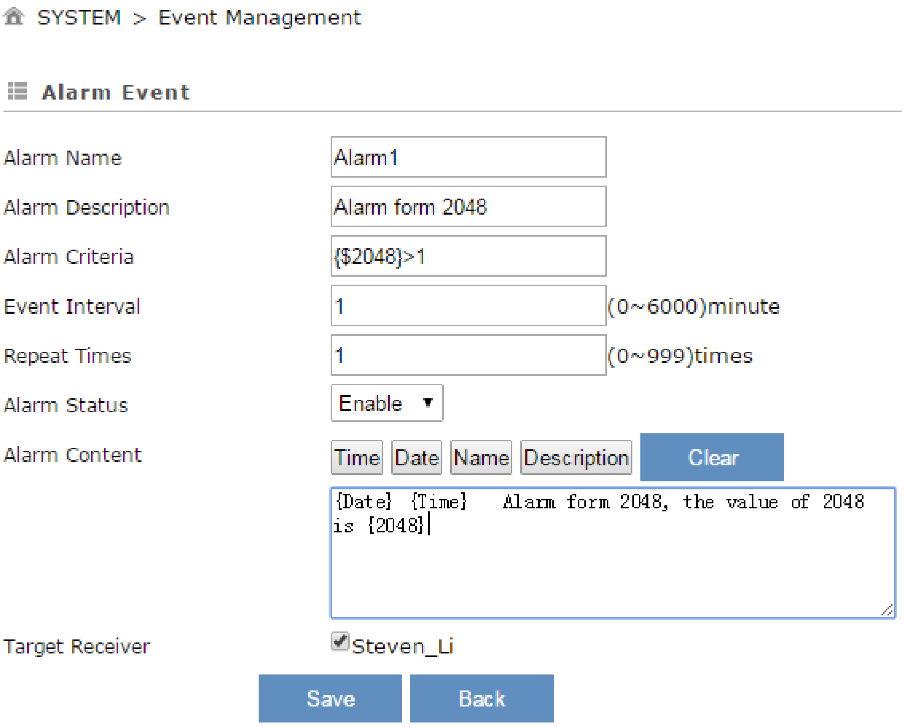
Event Management

Event Type: Alarm event

Send Short Message By: Cloud SMS Gateway

Please ensure the data traffic of your SIM card is available if you choose send short messge by device SIM card, or it will affect the functionality !

Alarm Name	Alarm Description	Alarm Criteria	Target Receiver	Status	Operation



SYSTEM > Event Management

Alarm Event

Alarm Name: Alarm1

Alarm Description: Alarm form 2048

Alarm Criteria: {$2048}>1

Event Interval: 1 (0~6000)minute

Repeat Times: 1 (0~999)times

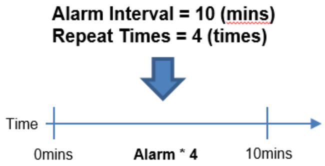
Alarm Status: Enable

Alarm Content:

```
{Date} {Time}  Alarm form 2048, the value of 2048
is {2048}
```

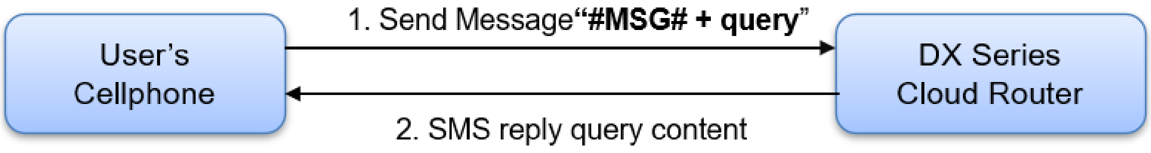
Target Receiver: ☑Steven_Li

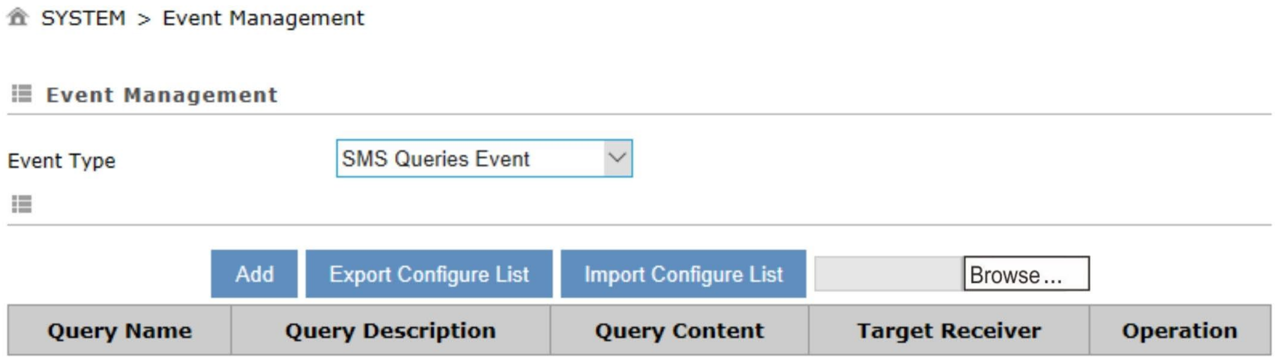
Description	Default
Event Type	
Alarm Event: DX Cloud Router can be configured to send email alerts to other users after triggering conditions are met for specific registers. **SMS Queries:** Users can send text messages to inquire about real-time register data within the DX Cloud Router.	Alarm Event
Add	
User can add up to a maximum of 64 warning conditions.	**N/A**
Export Configure List	
Export the warning settings with the default file name “ fixed_alarm_list.cfg”	**fixed_alarm_list.cfg**
Import Configure List	
Import the warning settings, and the file extension should be “*.cfg”	****.cfg**
Alarm Name	
Input the alarm name in fewer than 50 characters and avoid using Chinese characters and symbols.	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 input format for registers should be like {$2050}, indicating the value of the variable stored in register 2050. Alarm conditions can be for a single variable or a logical expression. The length can be up to 100 characters. You can use register locations. Word: $2048~$4095、Bit: M0~M511 ● $2048~$4096Alarm condition examples {$2048}>0, {$2048}==0, {$2048}<0, {$2003}+{$2004}*100/2-1 ● M0~M511Alarm condition examples M0>0, M1==0,	N/A
Event Interval	
The alarm sending interval is configurable, with a default value of 0, meaning that it will send the alarm once the condition is met. For example, set the condition as if $2048 > 100 then trigger an	0

Description	Default
alarm, the next trigger for the alarm must first satisfy $2048 < 100, and then $2048 > 100 again to trigger the alarm once more. If the data in $2048 remains consistently greater than 100, the alarm won't be triggered again.	
Repeat Times	
Maximum number of warning notifications to be sent within the trigger interval after triggering an alert (repetition count); default value is 0, indicating unlimited repetitions. Example: Trigger interval = 10, repetition count = 4. Within 10 minutes after triggering an alert, only 4 warning messages will be sent. The next trigger must wait for 10 minutes.  Alarm Interval = 10 (mins) Repeat Times = 4 (times) Time 0mins Alarm * 4 10mins	0
Alarm Status	
Enable or disable this alarm setting	Enable
Alarm Content	
Configure the information displayed on the alert content. When the alarm conditions are met, the content of the alarm will be sent to the target. The order of information can be customized. ● **Time:** The time at which the alarm occurred. ● **Date:** The date on which the alarm occurred. ● **Alarm Name:** The name of the alarm that occurred. ● **Alarm Description:** A description of the alarm that occurred, with a maximum content length of 160 characters. Double-word registers are not supported, and Chinese characters are not supported. Example: if register $2048 represents voltage and its value is 10, and the alarm content is configured as: "{Date}{Time} Voltage={$2048}", then the user will receive the following alarm content: "2016/06/01 (Date) 10:00:00 (Time) Voltage = 10.	N/A
Target Receiver	
After enabling alarm settings, when an alarm is triggered, the target which the alarm information will be sent to. Please go to **System→ Privilege Management →Control List of Event Management** to set the target object.	N/A

- **SMS Queries Event**

Users can send text messages to inquire about real-time register data within the DX Cloud Router.



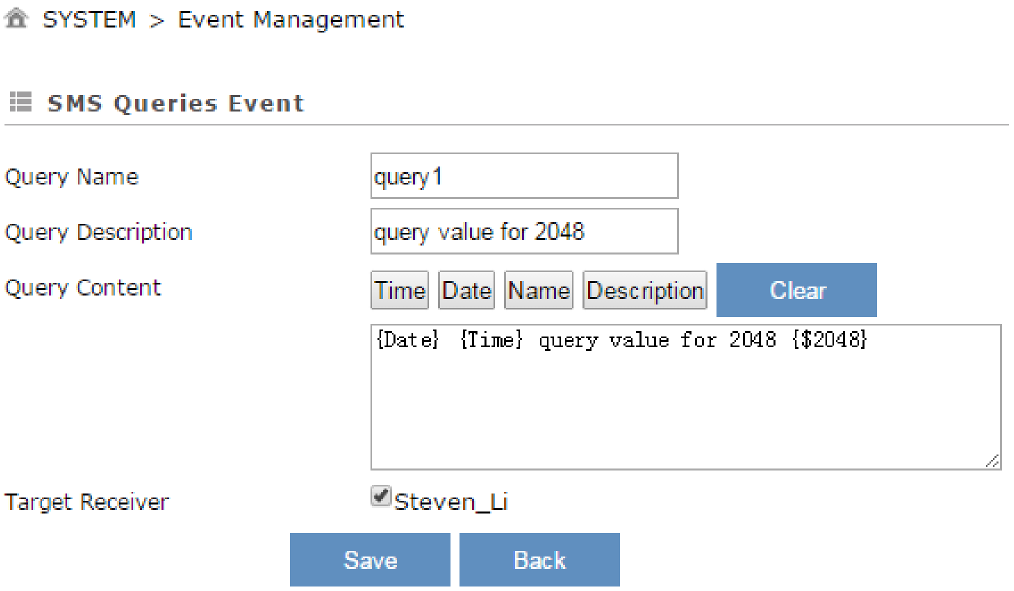


SYSTEM > Event Management

Event Management

Event Type: SMS Queries Event

Query Name	Query Description	Query Content	Target Receiver	Operation



SYSTEM > Event Management

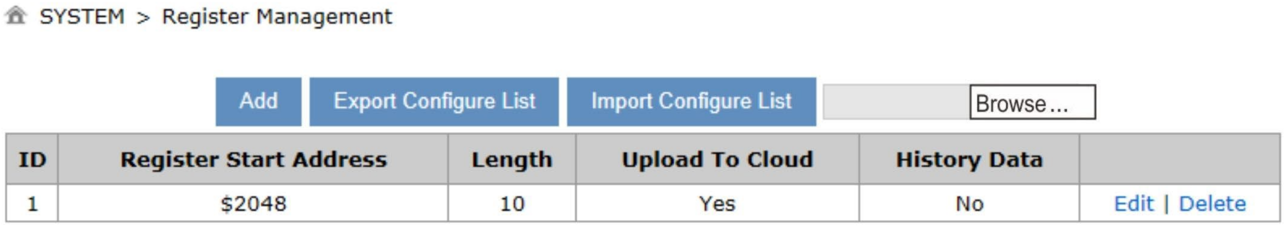
SMS Queries Event

Query Name	query1
Query Description	query value for 2048
Query Content	{Date} {Time} query value for 2048 {$2048}
Target Receiver	☑ Steven_Li

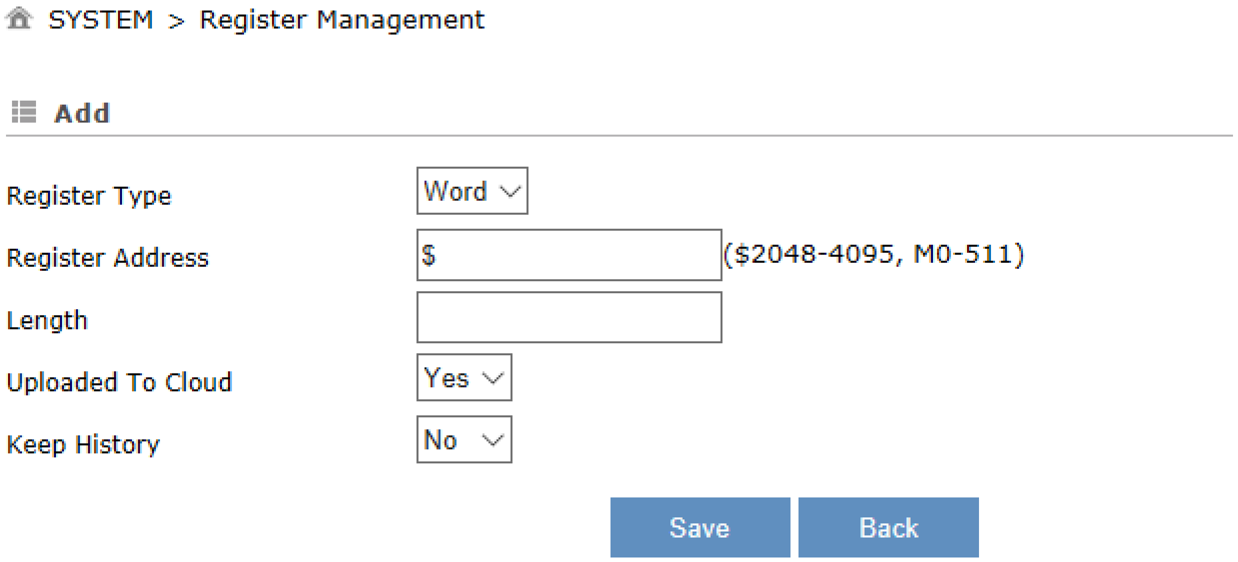
Description	Default
Add	
User can add up to 20 SMS query conditions.	**N/A**
Export Configure List	
Export the SMS query settings, with the default file name set as “fixed_alarm_list.cfg”	**fixed_query_list.cfg**
Import Configure List	
Import the SMS query settings, and the file extension should be “*.cfg”.	****.cfg**
Query Name	
Input a query name. The name shall be composed of numbers, English letters, and underline. The maximum string length is 9 characters. For example, after you create a query event named “query1,” you can send a message with content “#MSG#query1” to device SIM card number, then it will reply with the content you have set in the event.	N/A
Query Description	
The query description shall be composed of numbers, English letters, uppercase and lowercase. The maximum string length is 50 bytes.	N/A
Query Content	
Configure the information displayed on the query content. When the event conditions are met, the content of the event will be sent to the target. The order of information can be customized. ● **Time:** The time at which the event occurred. ● **Date:** The date on which the event occurred. ● **Name:** The name of the event that occurred. ● **Description:** A description of the event that occurred, with a maximum content length of 160 characters. Double-word registers are not supported, and Chinese characters are not supported. Example: if register $2048 represents voltage and its value is 10, and the event content is configured as: "{Date}{Time} Voltage={$2048}", then the user will receive the following alarm content: "2016/06/01 (Date) 10:00:00 (Time) Voltage = 10.	N/A
Target Receiver	
After enabling SMS Queries Event, when an event is triggered, the target which the event information will be sent to. Please go to **System→ Privilege Management →Control List of Event Management** to set the target object.	N/A

3.5.12 Register Management

Setting the register address of DX Cloud Router that need to upload data to DIACloud. The available register address for upload includes Bits: M0~M511 and Words: $2048~$4095.


SYSTEM > Register Management

ID	Register Start Address	Length	Upload To Cloud	History Data	
1	$2048	10	Yes	No	Edit | Delete


SYSTEM > Register Management

Add

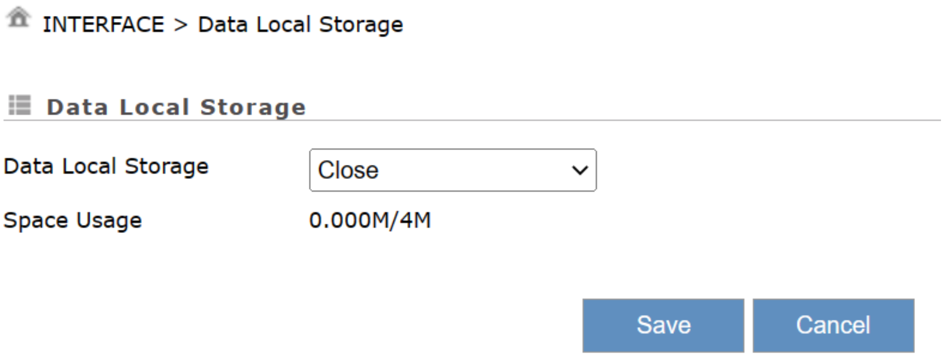
Register Type	Word
Register Address	$ ($2048-4095, M0-511)
Length	
Uploaded To Cloud	Yes
Keep History	No

Description	Default
Add	
Add a register upload rule. User can configure up to 20 rules.	N/A
Export Configure List	
Export the existing rules to a file and save it on your local computer. The exported file will be named “fixed_register_list.cfg”	N/A
Import Configure List	
User can import rules from the local computer. A maximum of 20 rules can be imported. ⚠**Notice:** A maximum of 20 mapping addresses can be imported. If there were already 10 mapping addresses configured previously, importing 20 new mapping addresses from this interface will override the previous 10 mapping addresses.	N/A

Description	Default
Register Type	
Set up the register data type, options are “Word” and “Bit”.	Word
Register Start Address	
Set the starting address for the registers to which the rules apply. For Word type, it should start with "$" and the configuration range is $2048~$4095. For Bit type, it should start with "M" and the configuration range is M0~M511."	N/A
Length	
The number of registers. Enter '1' for one register. The valid range for Word is 1-2048, and for Bit, it's 1-512.	N/A
Uploaded To Cloud	
Whether to upload the registers’ data to Cloud. ⚠**Notice** When the value of register changes, it will trigger the action to upload to the cloud.	Yes
Keep History Data	
User can choose to keep or overwrite the history data when the latest registers’ values are uploaded to Cloud. ● **Yes:** When new data is uploaded to the cloud, the cloud will create a new record. The existed register values in the cloud **WON’T** be overwritten. ● **No:** When uploading new data, it will directly **OVERWRITE** the old data. The cloud will always retain only the latest record for that variable.	No

3.5.13 Data Local Storage

DX-2400L9 allows users to temporarily store data in local storage. This is primarily to prevent data loss on the downstream device during internet disconnection periods.



INTERFACE > Data Local Storage

Data Local Storage

Data Local Storage: Close

Space Usage: 0.000M/4M

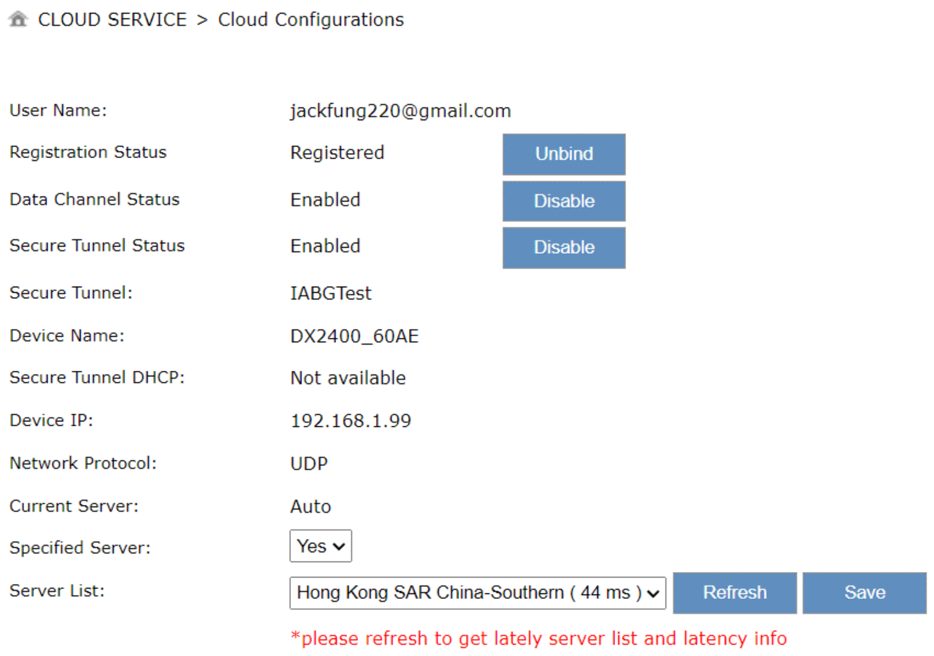
Description	Default
Data Local Storage	
When the internet disconnect, DX Cloud Router will continue to retrieve data from downstream devices and store it in memory. Once the network is restored, it will upload the stored data to DIACloud. Here is the explanation: ● Close: Do not activate this feature ● DC (Data Channel) Data: a. When the internet disconnects or when the DC service is turned off, DX Cloud Router will continue to retrieve and store data from the downstream device's registers in memory. It will then upload this data to DIACloud once the internet or DC service is restored. b. When unbinding a cloud account, if there is still pending data in the database that has not been uploaded, a reminder will appear. Unbinding will result in the loss of stored data. c. If the storage space is full, the oldest data entry will be overwritten by the most recent one. ● MQTT Data: a. When the internet disconnects, DX Cloud Router will continue to retrieve MQTT data from the downstream device and store it in memory. It will then upload this data to the MQTT server once the internet connection is restored. b. If there are multiple MQTT servers fetching data, the storage space will be evenly divided among them. However, when a new MQTT server is added, the storage space will be redistributed evenly among all clients, and any previously cached MQTT data will be cleared. c. Unbinding cloud account operation will not affect the saved MQTT data. d. If the storage space is full, the oldest data entry will be overwritten by the most recent one.	Close
Space Usag	
Provide 4MB of space for data caching with a storage interval of 1 minute.	0.000M

3.6 Cloud Service

User can configure Cloud Account, Proxy Setting, Tunnel Firewall, and Cloud Log.

3.6.1 Cloud Configuration

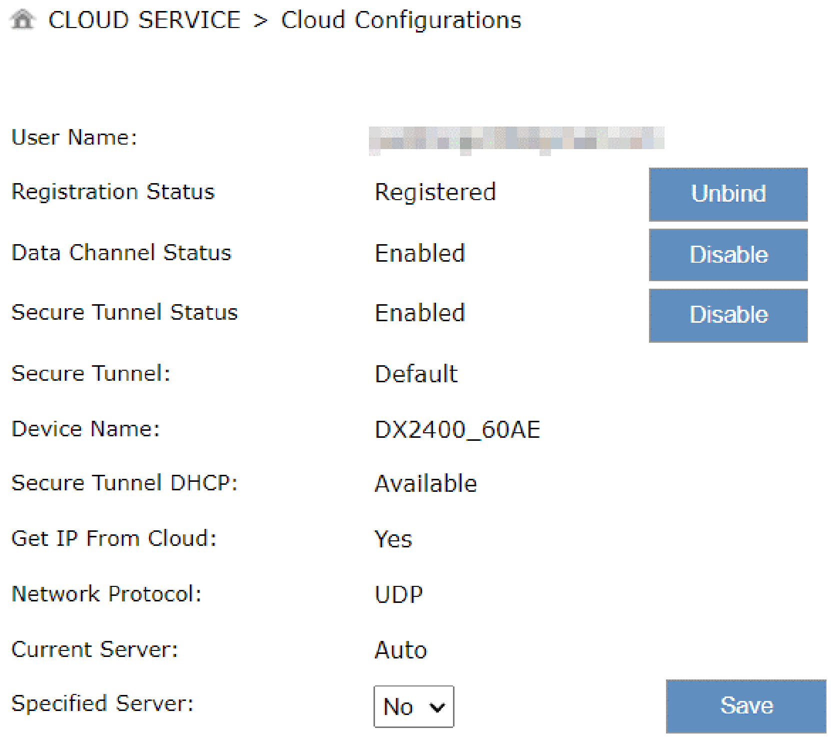
Configure DX Cloud Router to bind with DIACloud through the DX web interface and display the binding information, as well as the status of the Data Channel (DC) and the security tunnel.



CLOUD SERVICE > Cloud Configurations

User Name:	jackfung220@gmail.com
Registration Status	Registered
Data Channel Status	Enabled
Secure Tunnel Status	Enabled
Secure Tunnel:	IABGTest
Device Name:	DX2400_60AE
Secure Tunnel DHCP:	Not available
Device IP:	192.168.1.99
Network Protocol:	UDP
Current Server:	Auto
Specified Server:	Yes
Server List:	Hong Kong SAR China-Southern (44 ms)

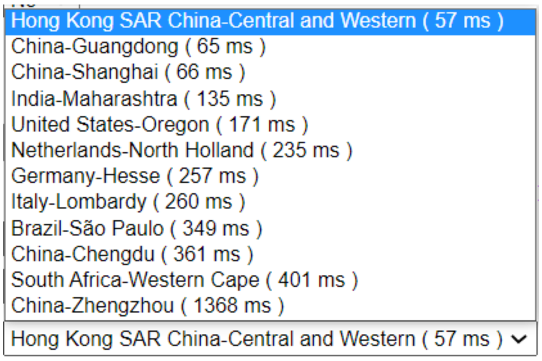
*please refresh to get lately server list and latency info



CLOUD SERVICE > Cloud Configurations

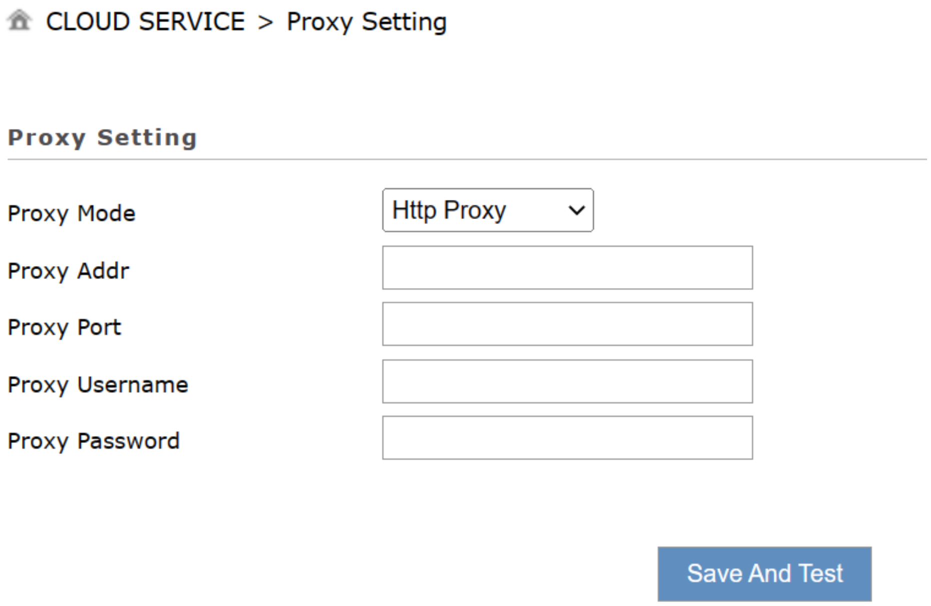
User Name:	[redacted]
Registration Status	Registered
Data Channel Status	Enabled
Secure Tunnel Status	Enabled
Secure Tunnel:	Default
Device Name:	DX2400_60AE
Secure Tunnel DHCP:	Available
Get IP From Cloud:	Yes
Network Protocol:	UDP
Current Server:	Auto
Specified Server:	No

Description	Default
Username	
Set up the name for the DIACloud account.	N/A
Password	
Set up the password for the DIACloud account.	N/A
Registration Status	
Display account binding information.	N/A
Data Channel Status	
Display the status of cloud data uploading. If it shows 'Disable,' it may indicate the Internet is unavailable. Please refer to Section 2.2.3	N/A
Secure Tunnel Status	
Display the status of secure tunnel uploading. If it shows 'Disable,' it may indicate the Internet is unavailable. Please refer to Section 2.2.3	N/A
Verify	
Check if the username and the password are matched.	N/A
Secure Tunnel	
Select the device under the account to join a specific security tunnel network group. For more related settings, please go to http://www.DIACloudsolutions.com/	Default
Device Name	
Set up the name for the device on the cloud.	N/A
Secure Tunnel DHCP	
When the security tunnel's DHCP server is set to 'enabled,' the option for obtaining IP addresses from the cloud will appear on the menu. Users can decide whether to use the cloud's DHCP server to obtain an IP address. For security tunnel settings, please refer to the Delta DIACloud Digital Dashboard Web User Manual → Tunnel Networks.	N/A
Get IP From Cloud	
● **Yes:** IP address can be obtained by the cloud. ● **No:** IP address can be manually set.	Yes
Cloud IP Range	
Display the Cloud IP Range. The Cloud IP Range depends on the secure tunnel setting. For the secure tunnel setting, please refer to Delta DIACloud Digital Dashboard Web User Manual → Tunnel Network.	N/A

Description	Default
Cloud Netmask	
Display the Cloud Netmask. The Cloud Netmask depended on the secure tunnel setting. For the secure tunnel setting, please refer to **Delta DIACloud Digital Dashboard Web User Manual → Tunnel Network.**	N/A
Device IP	
User can assign an IP address manually; please notice that IP address should be within the same subnet as the secure tunnel setting. For the secure tunnel setting,	N/A
Network protocol	
Set the network protocol of the security tunnel. Options are TCP and UDP. ● **UDP:** UDP offers faster data transmission speed. Please use this option if the network is stable. ● **TCP:** When the network is unstable, it is recommended to select TCP. After binding the cloud account, you can still change this option, but you must disable the cloud service to make changes. Once the proxy is enabled, the user can only select TCP.	UDP
Specified Server	
Setting whether to connect to a specific DIACloud server. ● **Yes:** Connect to a specific DIACloud server. ● **No:** Automatically select the DIACloud server with the lowest latency.	No
Server List	
Display a list of available DIACloud servers along with their latency times, allowing users to choose specific server for the connection. It is recommended to select a server with the lowest latency for better connection quality.  Hong Kong SAR China-Central and Western (57 ms) China-Guangdong (65 ms) China-Shanghai (66 ms) India-Maharashtra (135 ms) United States-Oregon (171 ms) Netherlands-North Holland (235 ms) Germany-Hesse (257 ms) Italy-Lombardy (260 ms) Brazil-São Paulo (349 ms) China-Chengdu (361 ms) South Africa-Western Cape (401 ms) China-Zhengzhou (1368 ms) Hong Kong SAR China-Central and Western (57 ms)	N/A

3.6.2 Proxy Setting

If the user’s networking environment requires outbound network connections to go through a HTTP or HTTPS proxy, user can setup it here.



CLOUD SERVICE > Proxy Setting

Proxy Setting

Proxy Mode: Http Proxy

Proxy Addr:

Proxy Port:

Proxy Username:

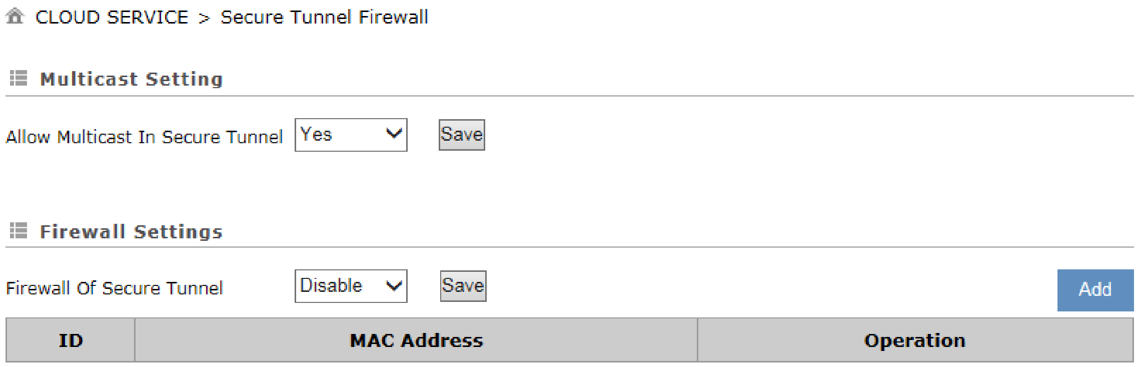
Proxy Password:

Description	Default
Proxy Mode	
Primarily used for accessing web pages, it can filter web content and cache web pages. If you configure an HTTP proxy server in your browser, all traffic in the browser will be routed through this proxy server. ● **Disable:** Disable the proxy function. ● **Http Proxy:** The LAN firewall only allows devices within the network to access the internet through a proxy server, and the proxy server's port is not restricted. ● **Port Proxy**: The LAN firewall only allows specific 443 port connections to the external network. In this mode, we will set up a 443 server, and then forward the data packets received from the 443 port to their respective actual ports. ● **Http+Port / Combine Proxy:** When the LAN firewall only allows internal devices to access the external network through a proxy server, and the proxy server's port is restricted to allowing only port 443 connections to the external network. In this mode, we will set up a 443 server. Then, data packets received on the 443 port will be forwarded to their respective actual ports.	Disable
Proxy Addr	
Set up the domain/IP of the proxy server.	N/A

Description	Default
Proxy Port	
Set up the port of the proxy server.	N/A
Proxy Username	
Set the username for connecting to the proxy server.	N/A
Proxy Password	
Set the password for connecting to the proxy server.	N/A
Save and Test	
Save the user-configured parameters, enable the proxy service, and test the connection to the DIACloud through the proxy.	N/A

3.6.3 Tunnel Firewall

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



CLOUD SERVICE > Secure Tunnel Firewall

Multicast Setting

Allow Multicast In Secure Tunnel: Yes

Firewall Settings

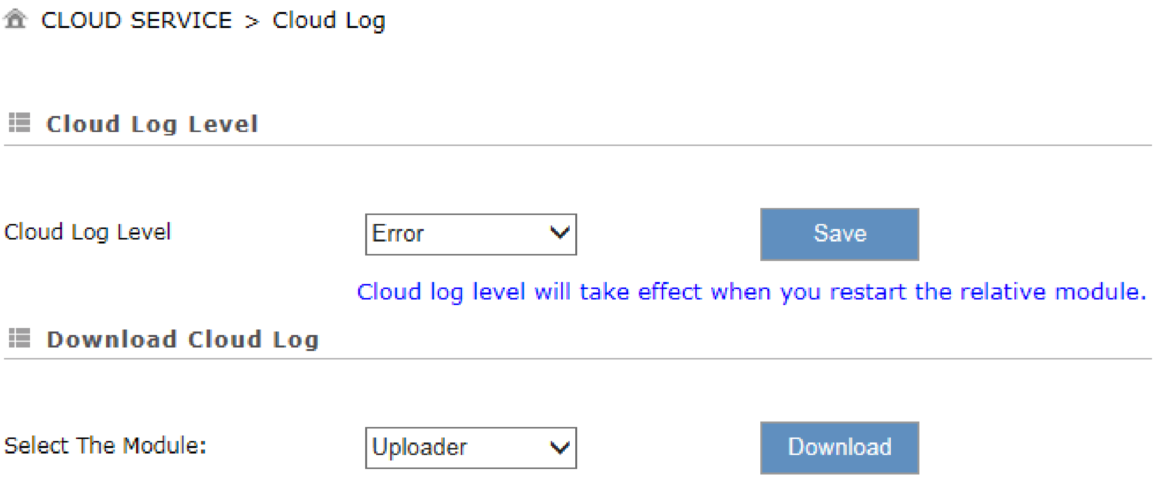
Firewall Of Secure Tunnel: Disable

ID	MAC Address	Operation

Description	Default
Allow multicast in secure tunnel	
In the configuration of a secure tunnel network, whether to allow the transmission of multicast data packets. **Options:** Allowed, not allowed	Yes
Firewall of secure tunnel	
Setting to allow or prohibit packets from specific devices with certain MAC addresses to be transmitted within a secure tunnel network. Options include: ● **Disable:** Disable this function. ● **Blacklist:** Only packets from devices listed in the MAC address blacklist are prohibited from being transmitted within the secure tunnel. ● **Whitelist:** Only packets from devices listed in the MAC address whitelist are allowed to be transmitted within the secure tunnel.	Disable
Add	
Add a new MAC address into the list.	N/A

3.6.4 Cloud Log

Users can download logs related to device and cloud platform interactions on this page.



CLOUD SERVICE > Cloud Log

Cloud Log Level

Cloud Log Level: Error

Cloud log level will take effect when you restart the relative module.

Download Cloud Log

Select The Module: Uploader

Description	Default
Cloud Log Level	
Specify which levels of logs should be saved to the log file for future export. Options (from lowest to highest level) include: ● **Trace:** Records event messages. ● **Debug:** Contains information helpful for debugging tools. ● **Info:** Emphasizes the operational status of the program. ● **Warn:** Indicates potential error situations. ● **Error:** Logs errors that do not disrupt the system's operation. ● **Fatal:** Logs critical errors that can lead to program termination or exit.	Error
Select Log Level	
Specify which cloud service module's logs to download. Options include: ● **Uploader:** Logs related to the data uploading module. ● **Secure Tunnel:** Logs for the secure tunnel module. ● **Binding:** Logs from the account binding module. ● **Agent:** Logs from the HTTP proxy module.	Uploader

Appendix A Internal Register

Table of Content

A.1 Register Value Description

Internal Register Address	MODBUS Address		Description	Supported Models
	DEC	HEX		

$0	0	0	RF Signal strength: (0~31)
			For DX-3021L9
			None LED：0, There is no wireless signal.
			One LED：1-10;
			Two LEDs：11-20;
			Three LEDs：21-31;
			For DX-3001H9
			None LED：0, There is no wireless signal.
			One LED：1-10;
			Two LEDs：11-20;
			Three LEDs：21-31;
			For DX-2100
			None LED：0, There is no wireless signal.
			One LED：1-7;
			Two LEDs：8-13;
			Three LEDs：14-19;
			Four LEDs：20-25;
			Five LEDs：26-31;
			For DX-2400
			None LED：0, There is no wireless signal.
			One LED：1-10;
			Two LEDs：11-20;
			Three LEDs：21-31;
				DX-2100RW
				DX-2400L9
				DX-3001H9
				DX-3021L9

$1-$10	1~10	1~A	IMSI number	DX-2100RW DX-2400L9 DX-3001H9 DX-3021L9

$11	11	B	SIM card error code: ● 1: normal ● 0: abnormal	bit0：SIM Card	DX-2100RW DX-2400L9 DX-3001H9 DX-3021L9
				bit1：GPRS/3G/LTE	DX-2100RW DX-2400L9 DX-3001H9 DX-3021L9
				bit2：DIACloud Service	DX-2100RW DX-3001H9 DX-2300LN
			Error code: ● 1: normal ● 0: abnormal	bit2：VLN status bit3：DC status	DX-2400L9 DX-3021L9
$12-$22	12-22	C-16	SMS: Mobile phone number + SMS Content		DX-2100RW DX-2400L9 DX-3001H9 DX-3021L9
$23	23	17	Error code $23 needs to be defined by PLC itself. The example is shown below. For more details, please refer to section Short Message Control PLC. ● $23=1: Incorrect IMSI comparison ● $23=2: AAAA execution failed ● $23=3: BBBB execution failed ● $23=4: CCCC execution failed		DX-2100RW DX-2400L9 DX-3001H9 DX-3021L9
$24	24	18	The PLC needs to write the execution result code to $24. ● 0: PLC task execution failed. ● 1: PLC task execution success.		DX-2100RW DX-2400L9 DX-3001H9 DX-3021L9

$29-$30	29-30	1D-1E	Reserved	DX-2100RW DX-2300LN DX-2400L9 DX-3001H9 DX-3021L9
$31	31	1F	The number of received SMS messages	DX-2100RW DX-2400L9 DX-3001H9 DX-3021L9
$89	89	59	● 0: The network status is normal ● non-zero: The network status is abnormal.	DX-2100RW DX-2400L9 DX-3001H9 DX-3021L9
$99	99	63	System time: years	DX-2100RW DX-2300LN DX-2400L9 DX-3001H9 DX-3021L9
$100	100	64	System time: months	DX-2100RW DX-2300LN DX-2400L9 DX-3001H9 DX-3021L9
$101	101	65	System time: days	DX-2100RW DX-2300LN DX-2400L9 DX-3001H9 DX-3021L9
$102	102	66	System time: hours	DX-2100RW DX-2300LN DX-2400L9 DX-3001H9 DX-3021L9

$103	103	67	System time: minutes	DX-2100RW DX-2300LN DX-2400L9 DX-3001H9 DX-3021L9
$104	104	68	System time: seconds	DX-2100RW DX-2300LN DX-2400L9 DX-3001H9 DX-3021L9
$900	900	384	**Explanation:** When an error occurs in the **RS-232 master station**, it will display the total number of data exchange errors between the master station and the slave. **Example:** If 100 mapping tables are configured, and 10 of them have errors, then $900 is 10.	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9
$901	901	385	**Explanation:** When an error occurs in the **RS-232 master station**, as configured in the mapping table, it displays the row number of the first data exchange error. **Example:** If there are errors in rows 2 to 10 of the mapping table, then $901 will display the first error row number as 2 in numerical order. In this example, $901 will display 1 **(starting from 0, so the error is at 2, but $901 will display it as 1).**	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9

$902	902	386	**Explanation** When an error occurs in the **RS-232 master station**, it displays the MODBUS error code for the first data exchange error row number in the mapping table. **Example:** If there is an error in data exchange row number 10, indicating an unauthorized command, then $902 will display the corresponding Modbus error code. For error code details, please refer to Chapter 3 Router Information.	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9
$903	903	387	**Explanation:** When an error occurs in the **RS-485 master station**, it displays the total number of rows in the mapping table that have experienced data exchange errors along with their respective quantities. **Example:** If 100 mapping tables are configured, and 10 of them have errors, then $900 is 10.	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9
$904	904	388	**Explanation:** When an error occurs in the **RS-485 master station**, as configured in the mapping table, it displays the row number of the first data exchange error. **Example:** If there are errors in rows 2 to 10 of the mapping table, then $901 will display the first error row number as 2 in numerical order. In this example, $901 will display 1 **(starting from 0, so the error is at 2, but $901 will display it as 1).**	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9

$905	905	389	**Explanation:** When an error occurs in the **RS-232 master station**, it displays the MODBUS error code for the first data exchange error row number in the mapping table. **Example:** If there is an error in data exchange row number 10, indicating an unauthorized command, then $905 will display the corresponding Modbus error code. For error code details, please refer to Chapter 3 Router.	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9
$906	906	38A	**Explanation:** When an error occurs in the **Modbus TCP Client**, it displays the total number of rows in the mapping table that have experienced data exchange errors along with their respective quantities. **Example:** If 100 mapping tables are configured, and 10 of them have errors, then $900 is 10.	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9
$907	907	38B	**Explanation:** When a connection error occurs for one of the 4 **Modbus TCP Clients**, $907 will display its corresponding number. **Example:** If you have configured 4 Modbus TCP Client connections and the second group encounters a connection error or any issues, then $907 will display 1. **(Starting from 0, so the error is at 2, but $907 will display it as 1).**	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9

$908	908	38C	**Explanation:** Display the data exchange ROW number position of the error in a specific group of **Modbus TCP Client.** **Example:** If you have configured 4 Modbus TCP Client connections and the second group encounters a connection error, and within the second group, ROW number 10 encounters an error, then: ● $907 will display 1, indicating the second group of Modbus TCP connection. **(Starting from 0, so the error is in the second group but $907 will display it as 1).** ● $908 will display 9, indicating that ROW number 10 has encountered an error within the second group. **(Starting from 0, so the error is in ROW number 10, but $908 will display it as 9).**	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9
$909	909	38D	**Explanation:** When an error occurs in the **Modbus TCP Client**, it displays the MODBUS error code for the first data exchange error row number in the mapping table. **Example:** If there is an error in data exchange ROW number 10, indicating an unauthorized command, then $909 will display the corresponding Modbus error code. For error code details, please refer to Chapter 3 Router Information.	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9
$910	910	38E	**0:** Both Modbus TCP and Siemens TCP communication status are normal. **1:** One of Modbus TCP and Siemens TCP communication status is wrong.	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9

$911	911	38F	**Explanation:** When an error occurs in **Siemens TCP**, it displays the total number of rows in the mapping table that have experienced data exchange errors along with their respective quantities. **Example:** If you have configured 100 mapping table entries and 10 of them have errors, then $911 will display 10.	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9
$912	912	390	**Explanation:** **Siemens TCP** allows you to set up 32 connections, and when an error occurs in a particular connection, $912 can display its number. **Example:** If you have configured 32 Siemens TCP connections and the second connection encounters a connection error or other issues, then $912 will display 1. **(The counting starts from 0, so even though the error is in the second connection, $912 will display it as 1).**	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9
$913	913	391	**Explanation:** Display the data exchange ROW number position of the error in a specific group of **Siemens TCP**. **Example:** If you have configured 4 groups of Siemens TCP connections and the second group encounters a connection error, and within the second group, ROW number 10 encounters an error, then: ● $912 will display 1, indicating the second group of Siemens TCP connection. **(Starting from 0, so the error is in the second group but $912 will display it as 1).** ● $913 will display 9, indicating that data exchange ROW number 10 has encountered an error within the second group. **(Starting from 0, so the error is in ROW number 10, but $913 will display it as 9).**	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9

$914	914	392	When **Siemens TCP** connection encounters an error, it displays the Siemens TCP error code for the first data exchange error row number. **<u>Explanation:</u>** When a Siemens TCP connection experiences an error, it shows the MODBUS error code for the first data exchange error row number. **<u>Example:</u>** If there is an error in data exchange ROW number 10, indicating an unauthorized command, then $914 will display the corresponding Siemens TCP error code.	DX-2100RW DX-2300LN DX-2400L9 DX-3021L9

Smarter. Greener. Together.

Industrial Automation Headquarters

Delta Electronics, Inc.
Taoyuan Technology Center
No.18, Xinglong Rd., Taoyuan District,
Taoyuan City 330477, Taiwan
TEL: +886-3-362-6301 / FAX: +886-3-371-6301

Asia

Delta Electronics (Shanghai) Co., Ltd.
No.182 Minyu Rd., Pudong Shanghai, P.R.C.
Post code : 201209
TEL: +86-21-6872-3988 / FAX: +86-21-6872-3996
Customer Service: 400-820-9595

Delta Electronics (Japan), Inc.
Industrial Automation Sales Department
2-1-14 Shibadaimon, Minato-ku
Tokyo, Japan 105-0012
TEL: +81-3-5733-1155 / FAX: +81-3-5733-1255

Delta Electronics (Korea), Inc.
1511, 219, Gasan Digital 1-Ro., Geumcheon-gu,
Seoul, 08501 South Korea
TEL: +82-2-515-5305 / FAX: +82-2-515-5302

Delta Energy Systems (Singapore) Pte Ltd.
4 Kaki Bukit Avenue 1, #05-04, 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

Delta Electronics (Thailand) PCL.
909 Soi 9, Moo 4, Bangpoo Industrial Estate (E.P.Z),
Pattana 1 Rd., T.Phraksa, A.Muang,
Samutprakarn 10280, Thailand
TEL: +66-2709-2800 / FAX: +66-2709-2827

Delta Electronics (Australia) Pty Ltd.
Unit 2, Building A, 18-24 Ricketts Road,
Mount Waverley, Victoria 3149 Australia
Mail: IA.au@deltaww.com
TEL: +61-1300-335-823 / +61-3-9543-3720

Americas

Delta Electronics (Americas) Ltd.
5101 Davis Drive, Research Triangle Park, NC 27709, U.S.A.
TEL: +1-919-767-3813 / FAX: +1-919-767-3969

Delta Electronics Brazil Ltd.
Estrada Velha Rio-São Paulo, 5300 Eugênio de
Melo - São José dos Campos CEP: 12247-004 - SP - Brazil
TEL: +55-12-3932-2300 / FAX: +55-12-3932-237

Delta Electronics International Mexico S.A. de C.V.
Gustavo Baz No. 309 Edificio E PB 103
Colonia La Loma, CP 54060
Tlalnepantla, Estado de México
TEL: +52-55-3603-9200

EMEA

Delta Electronics (Netherlands) B.V.
Sales: Sales.IA.EMEA@deltaww.com
Marketing: Marketing.IA.EMEA@deltaww.com
Technical Support: iatechnicalsupport@deltaww.com
Customer Support: Customer-Support@deltaww.com
Service: Service.IA.emea@deltaww.com
TEL: +31(0)40 800 3900

Delta Electronics (Netherlands) B.V.
Automotive Campus 260, 5708 JZ Helmond, The Netherlands
Mail: Sales.IA.Benelux@deltaww.com
TEL: +31(0)40 800 3900

Delta Electronics (Netherlands) B.V.
Coesterweg 45, D-59494 Soest, Germany
Mail: Sales.IA.DACH@deltaww.com
TEL: +49 2921 987 238

Delta Electronics (France) S.A.
ZI du bois Challand 2, 15 rue des Pyrénées,
Lisses, 91090 Evry Cedex, France
Mail: Sales.IA.FR@deltaww.com
TEL: +33(0)1 69 77 82 60

Delta Electronics Solutions (Spain) S.L.U
Ctra. De Villaverde a Vallecas, 265 1º Dcha Ed.
Hormigueras – P.I. de Vallecas 28031 Madrid
TEL: +34(0)91 223 74 20

Carrer Llacuna 166, 08018 Barcelona, Spain
Mail: Sales.IA.Iberia@deltaww.com

Delta Electronics (Italy) S.r.l.
Via Meda 2–22060 Novedrate(CO)
Piazza Grazioli 18 00186 Roma Italy
Mail: Sales.IA.Italy@deltaww.com
TEL: +39 039 8900365

Delta Energy System LLC
Vereyskaya Plaza II, office 112 Vereyskaya str.
17 121357 Moscow Russia
Mail: Sales.IA.RU@deltaww.com
TEL: +7 495 644 3240

Delta Greentech Elektronik San. Ltd. Sti. (Turkey)
Şerifali Mah. Hendem Cad. Kule Sok. No:16-A
34775 Ümraniye – İstanbul
Mail: Sales.IA.Turkey@deltaww.com
TEL: + 90 216 499 9910

Eltek Dubai (Eltek MEA DMCC)
OFFICE 2504, 25th Floor, Saba Tower 1,
Jumeirah Lakes Towers, Dubai, UAE
Mail: Sales.IA.MEA@deltaww.com
TEL: +971(0)4 2690148

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