SUNGROW
Clean power for all

User Manual

Data Logger

Logger4000



All Rights Reserved

All Rights Reserved

No part of this document can be reproduced in any form or by any means without the prior written permission of Sungrow Power Supply Co., Ltd (hereinafter "SUNGROW").

Trademarks

SUNGROW and other SUNGROW trademarks used in this manual are owned by SUNGROW.

Software Licenses

- It is prohibited to use data contained in firmware or software developed by SUNGROW, in part or in full, for commercial purposes by any means.
- It is prohibited to perform reverse engineering, cracking, or any other operations that compromise the original program design of the software developed by SUNGROW.

About This Manual

The manual mainly contains the product information, as well as guidelines for installation, operation and maintenance. Readers can get additional information at **www.sungrowpower.com** or on the webpage of the respective component manufacturer.

Validity

This manual is valid for the following models:

- Logger4000

Target Group

This manual is intended for qualified technicians who are responsible for installation, operation, and maintenance of the product, and users who need to check inverter parameters.

The product must only be installed by qualified technicians. The qualified technical technician must:

- Have electronic, electrical wiring, and mechanical expertise, and be familiar with electrical and mechanical schematics.
- Have received professional training related to the installation and commissioning of electrical equipment.
- Be able to respond quickly and effectively to dangers or emergencies that may occur during installation and commissioning.
- Be familiar with local standards and relevant safety regulations of electrical systems.
- Read this manual thoroughly and understand the safety instructions related to operations.

How to Use This Manual

Read through this manual carefully before using the product, and keep it properly in an easy-to-reach place.

The information in this manual is subject to ongoing updates and revisions. Although efforts have been made to ensure accuracy, there might be slight variations or errors compared to the actual product. Please refer to the actual product purchased, and the latest manual can be obtained from **support.sungrowpower.com** or sales channels.

Symbols

This manual contains important safety instructions, which are highlighted with the following symbols, to ensure personal and property safety during usage, or to help optimize the product performance in an efficient way.

Symbols used in this manual are listed below. Please review carefully for better use of this manual.

⚠ DANGER

Indicates high-risk potential hazards that, if not avoided, will result in death or serious injury.

⚠ WARNING

Indicates moderate-risk potential hazards that, if not avoided, may lead to death or serious injury.

⚠ CAUTION

Indicates low-risk potential hazards that, if not avoided, may lead to minor or moderate injury.

NOTICE

Indicates potential risks that, if not avoided, may lead to device malfunction or financial losses.

"NOTE" indicates additional information, important content, or helpful tips that may solve problems or save time.

Contents

All Rights Reserved.....I
About This Manual.....II
1 Safety Instructions.....1
2 Product Description.....3
2.1 Function Description.....3
2.2 Networking Application.....4
2.3 Product Introduction.....7
3 Unpacking and Storage.....9
3.1 Scope of Delivery.....9
3.2 Identifying the Data Logger.....10
3.3 Checking upon Receiving.....10
3.4 Storage.....10
4 Mechanical Installation.....12
4.1 Installation Location Selection.....12
4.2 Installation Tools.....12
4.3 Mounting the Data Logger.....14
4.3.1 Wall-Mounted Installation.....14
4.3.2 Rack-Mounted Installation.....15
5 Electrical Connection.....18
5.1 Safety Instructions.....18
5.2 Port Introduction.....18
5.3 Wiring Overview.....20
5.4 Connecting to the Inverter.....21
5.4.1 Connecting to the Device with RS485 Port.....21
5.4.2 Connecting to the Inverter with MPLC Port.....23
5.5 Connecting to the Meteo Station.....26
5.6 Connecting to the Meter.....27
5.6.1 RS485 Cable Connection.....27
5.6.2 Ethernet Cable Connection.....28
5.7 Wiring of DI Signal.....28
5.8 Wiring of DO Signal.....29
5.9 Wiring of AI Signal.....30
5.10 Wiring of PT Signal.....32
5.11 Connecting to the Remote Monitoring Device.....33

5.12 Connecting to the AC Power Supply..... 34
5.13 Connecting to the DC Power Supply..... 35
5.14 Earthing Connection..... 36
6 Commissioning..... 38
6.1 Inspection before Commissioning..... 38
6.2 Commissioning Steps..... 38
7 Web Interface..... 40
7.1 Log in to Web System..... 40
7.2 Modifying Password..... 43
7.3 Web UI Overview..... 43
7.3.1 Web Main Interface..... 43
7.3.2 Operating Environment Requirements..... 44
7.3.3 Operation Procedure..... 44
7.4 Overview..... 45
7.4.1 General Information..... 45
7.4.2 Current Fault..... 46
7.5 Device Monitoring..... 46
7.5.1 Real-Time Information..... 46
7.5.2 DC Info..... 46
7.5.3 Initial Parameters..... 46
7.5.4 Operation Parameters..... 47
7.5.5 System Parameters..... 47
7.5.6 Protection Parameters..... 47
7.5.7 Protection Parameters (Other)..... 47
7.5.8 Power Regulation Parameters..... 47
7.5.9 Fault Recording Parameters..... 48
7.5.10 General Parameters..... 48
7.5.11 Device Instructions..... 48
7.5.12 Device Information..... 49
7.5.13 Dispersion Rate Analysis..... 49
7.5.13.1 Enabling Dispersion Rate Diagnosis..... 50
7.5.13.2 Setting Array Parameters..... 50
7.5.13.3 Initiating Dispersion Rate Diagnosis..... 51
7.5.13.4 Viewing Diagnosis Results..... 51
7.5.14 Air Duct Health Detection..... 54
7.5.14.1 Enable Air Duct Health Detection..... 54
7.5.14.2 Setting Air Duct Health Detection Parameters..... 55
7.5.15 VSG Parameter Settings..... 55
7.6 Device Maintenance..... 58
7.6.1 Device List..... 58

7.6.1.1 Export..... 58
7.6.1.2 Import..... 58
7.6.1.3 Add Device..... 59
7.6.1.4 Edit Device..... 60
7.6.1.5 Delete Device..... 60
7.6.2 Inverter Log..... 60
7.6.3 AFCI Detection..... 61
7.6.4 Fault Recording..... 61
7.6.5 Configuring Bluetooth Pairing for Inverter..... 62
7.6.5.1 Enabling Bluetooth Pairing..... 62
7.6.5.2 Disabling Bluetooth Pairing..... 63
7.6.6 (Optional) Winding Temperature Detection..... 64
7.6.6.1 Viewing Real-time Data..... 64
7.7 History Data..... 67
7.7.1 Operation Log..... 67
7.7.2 Fault Records..... 68
7.7.3 History Curve..... 68
7.7.4 rsyslog..... 69
7.8 System..... 71
7.8.1 Operating Information..... 71
7.8.2 System Maintenance..... 71
7.8.2.1 Update System..... 71
7.8.2.2 Log Export..... 71
7.8.2.3 Restart..... 71
7.8.2.4 One-Click Migration..... 72
7.8.2.5 Backup and Restoration..... 72
7.8.2.6 Attribute Management..... 73
7.8.3 Remote Maintenance..... 73
7.8.4 Export Messages..... 74
7.8.5 System Time..... 75
7.8.6 Forwarding Configuration..... 77
7.8.6.1 Configure iSolarCloud Forwarding Service..... 77
7.8.6.2 Configure IEC 104 Forwarding Service..... 77
7.8.6.3 MODBUS..... 79
7.8.6.4 Configure Third-Party Cloud Forwarding Service..... 82
7.8.6.5 Configure GOOSE Forwarding Service..... 82
7.8.6.6 Setting MMS Forwarding Service..... 83
7.8.7 Port Parameter..... 83
7.8.7.1 RS485..... 83
7.8.7.2 Ethernet..... 84

7.8.7.3 Analog Input (AI)....84
7.8.7.4 Digital Input(DI)....85
7.8.7.5 Digital Output (DO)....85
7.8.8 MPLC (Broadband PLC)....85
7.8.8.1 MPLC Auto Frequency Hopping....86
7.8.8.2 One-Click MPLC Diagnosis....87
7.8.9 Certificate management....87
7.8.9.1 Collection....87
7.8.9.2 Forward....88
7.8.9.3 Import NTS Active Server Certificate....89
7.8.9.4 GOOSE Security Functions....90
7.8.9.5 System Update Certificate....90
7.8.9.6 rsyslog Certificate Management....90
7.8.9.7 View Certificate Information....91
7.8.9.8 Import Certificate Revocation List....91
7.8.9.9 View Certificate Revocation List....92
7.8.9.10 Certificate Expiration Management....93
7.8.10 More....93
7.8.11 Check Firmware Version....94
8 Firmware Upgrade....96
8.1 Updating SUNGROW Inverters or the Slave Node of PLC....96
8.2 Updating the Data Logger....97
8.3 Update PLC master node....97
9 Power Regulation....99
9.1 Options for Power Control Method....99
9.2 Selecting Power Control Mode....99
9.3 Active Power....100
9.3.1 Remote Power Control....101
9.3.2 Local Regulation....103
9.3.3 AI Control....106
9.3.4 Dry Contact....107
9.3.5 Country Mode....108
9.3.5.1 Korea....108
9.3.5.2 Japan Mode....109
9.3.5.3 Australia Mode....109
9.3.5.4 China....110
9.3.6 Disable Dispatch....110
9.3.7 Disable Derating....110
9.4 Reactive Power....110
9.4.1 Remote Power Control....111

9.4.2 Local Power Control..... 111
9.4.3 AI Control..... 112
9.4.4 Dry Contact..... 113
9.4.5 Country Mode..... 114
9.4.6 Disable Dispatch..... 114
9.4.7 Disable Output..... 115
9.5 Configure Emergency Shutdown..... 115
10 User management..... 116
10.1 Initial username and password..... 116
10.2 Password Management..... 117
10.3 Set up the administrator account..... 118
10.4 Create User Accounts..... 118
10.5 Delete User Accounts..... 119
10.6 Reset account passwords..... 119
10.6.1 Reset User Account Password..... 119
10.6.2 Reset Administrator Account Password..... 119
10.7 Enable Multi-factor authentication..... 120
10.8 Configure Account Protection and Session Security Parameters..... 121
10.9 Enable O&M Mode..... 122
10.10 LDAP Management..... 122
10.11 System Maintenance..... 123
10.11.1 Backup and Restore..... 123
10.11.2 Restore factory settings..... 124
10.12 Communication Settings..... 124
10.12.1 iSolarCloud..... 124
10.12.2 Third-Party Cloud..... 125
11 Routine Maintenance..... 126
11.1 Safety Instructions..... 126
11.2 Maintenance List..... 126
12 Troubleshooting..... 128
12.1 Safety Instructions..... 128
12.2 Common Fault Phenomena and Troubleshooting Methods..... 128
13 Frequently Asked Questions..... 134
14 Appendix A: Technical Data..... 136
15 Appendix B: Related Drawings..... 138
16 Appendix C: General Information..... 139
16.1 Quality Assurance..... 139
16.2 Software Security Update Information..... 139
16.3 Contact Information..... 139

1 Safety Instructions

When installing, commissioning, operating, and maintaining the product, strictly observe relevant safety instructions. Improper use or misoperation may result in:

- Injury or death to the operator or a third party.
- Damage to the product or the property of the operator or a third party.

- The safety instructions in this manual are only supplements and cannot cover all the precautions that should be followed. Perform operations considering actual on-site conditions.
- SUNGROW shall not be held liable for any damage caused by violation of general safety operation requirements, general safety standards, or any safety instruction in this manual.
- When installing, operating, and maintaining the device, comply with local laws and regulations. The safety precautions in this manual are only supplements to local laws and regulations.

⚠ WARNING

Only professional electricians or qualified personnel can operate and wire the product.

Warning Label

Warning label on enclosure of the Data Logger is as follows:



Symbol	Explanation
	High voltage inside. Risk of electrical shock hazard when it is touched.
	This symbol indicates a protective ground terminal which needs to be firmly grounded to ensure the safety of operators.
30s	Do not to touch energized components within 30 seconds after disconnecting the power.

Before Installation

NOTICE

After receiving the product, please check if there is damage caused during transport. Contact SUNGROW or the forwarding company once any problem is found.
The related operators must be familiar with the safety instructions in this manual and other safety regulations about the installation, operation and maintenance of the product.
Follow the instructions in the manual to perform handling, installation, and operation maintenance to ensure the safe and proper use of the product.

During Installation

NOTICE

This product can only be used for purposes specified in this manual. Unauthorized alternations or use of parts and components not sold or recommended by SUNGROW may result in fires, electric shocks, and other hazards.

NOTICE

Disconnect all electrical connection and the upstream input switch before installation, and ensure the device is voltage-free.

NOTICE

Disconnect all electrical connections and the upstream input switch and make sure the device is voltage-free.

Maintenance and Replacement

⚠ WARNING

Repair of the device can only be performed by the service department of SUNGROW or professionally qualified personnel.
Users are forbidden from performing repair and maintenance or replacing modules by themselves. Otherwise, it may cause severe personal injuries or property damages.

NOTICE

Never replace the internal components of the device without authorization. SUNGROW shall not be held liable for any possible damage caused by ignorance of this warning.

2 Product Description

2.1 Function Description

The Data Logger is equipped with the following functions:

Support of Device Connection

The Data Logger can be connected to devices in the PV system via an RS485 bus, and it can be also connected to SUNGROW string inverter equipped with the PLC communication function through the PLC cable. The Data Logger can store and process device information as well as convert data communication protocol.

Management of Communication Device

The Data Logger can centrally manage devices connected to it, including parameter setting, firmware upgrade, etc, which makes onsite maintenance more convenient.

Configuration through Web Interface

Users can set system time, network, serial port, etc., and maintain the protocol point table through the embedded Web interface of the Data Logger.

Network Port Configuration

There are five Ethernet ports (namely, ETH1 to ETH5) with the data exchange function on the Data Logger, three Ethernet ports, and two fast scheduling ports. It can be connected to SCADA or insight northward and to third-party devices southward.

Data Forwarding Function

The Data Logger can forward the collected data to iSolarInsight or iSolarCloud.

- The data forwarding function of the Data Logger is disabled by default. Prior to activation, the user must provide explicit consent with full awareness and establish a secure connection to the public network through encrypted authentication. Remote access is only valid after authorization, and all operations are logged for audit and traceability purposes.
- iSolarCloud is not applicable to North America.

Protocol Conversion Service

The Data Logger provides protocol conversion service, including converting Modbus RTU to IEC104, MQTT, ModbusTCP, etc.

The Data Logger provides protocol conversion service, including converting Modbus RTU to IEC104, ModbusTCP, etc.

Grid Dispatch

The Data Logger can receive and execute power dispatch instructions transmitted from the grid operator via the customer's local SCADA system

Local Power Control

The Data Logger can receive and perform local dispatching instructions, including delivering fixed value, energy meter closed-loop dispatching, etc.

Fast Dispatch

The Data Logger can accept and execute fast active and reactive dispatching instructions to achieve reactive power control within 30ms.

IV Curve Online Diagnosis

The Data Logger can perform I-V curve scanning on inverters developed by SUNGROW, and users can view scanning result via iSolarCloud, Insight or iSolarSuite. For detailed description of the I-V curve scanning, refer to the manual of iSolarCloud, Insight or iSolarSuite.

IV Curve Online Diagnosis

The Data Logger can perform I-V curve scanning on inverters developed by SUNGROW.

Built-in MPLC

The Data Logger has a built-in MPLC-H (Broadband Power Line Carrier Communication), which can be directly connected to the string inverter with MPLC function produced by SUNGROW.

2.2 Networking Application

The Data Logger can be applied to various networking scenarios. It can be connected to the inverter, transformer, Meteo Station, and energy meter in the PV system via RS485 bus, or connected to SUNGROW string inverter equipped with MPLC communication function through MPLC bus.

- The Data Logger can transmit the collected device data to the SCADA plant controller, such as Insight and SCADA, through the core switch.
- The Data Logger can also transmit the collected device data directly to iSolarCloud through the 4G router.

Connected to SCADA plant controller through a core switch

The following figures shows how the Data Logger is connected to the Insight or SCADA through a core switch.

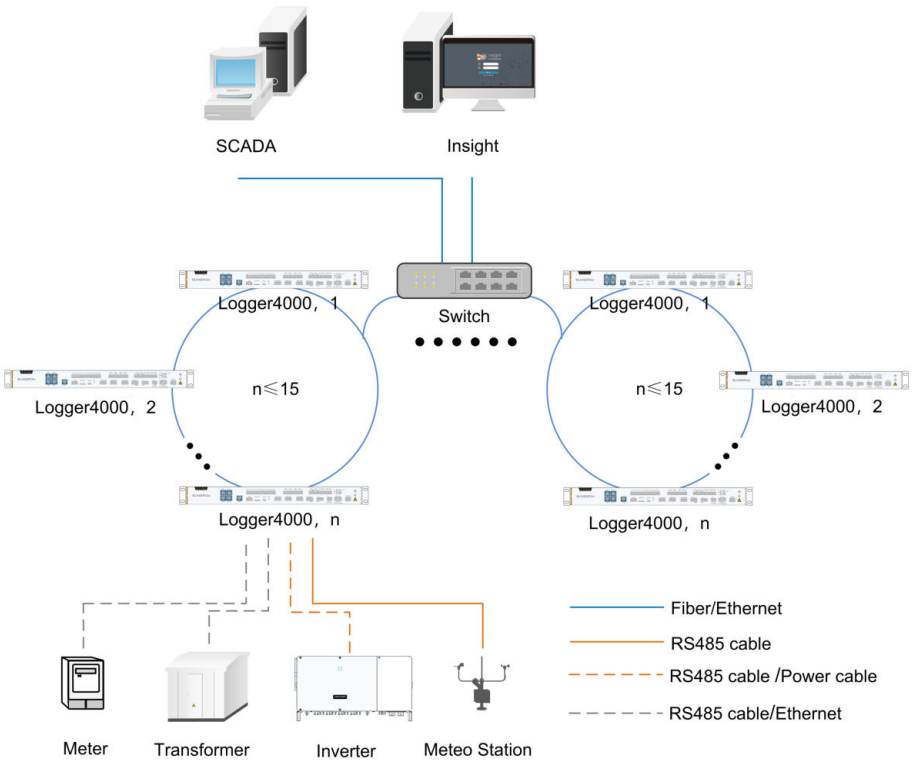


Figure 2-1 Ring networking

When the ring networking is used, a maximum of 15 Data Loggers can be connected to a ring network.

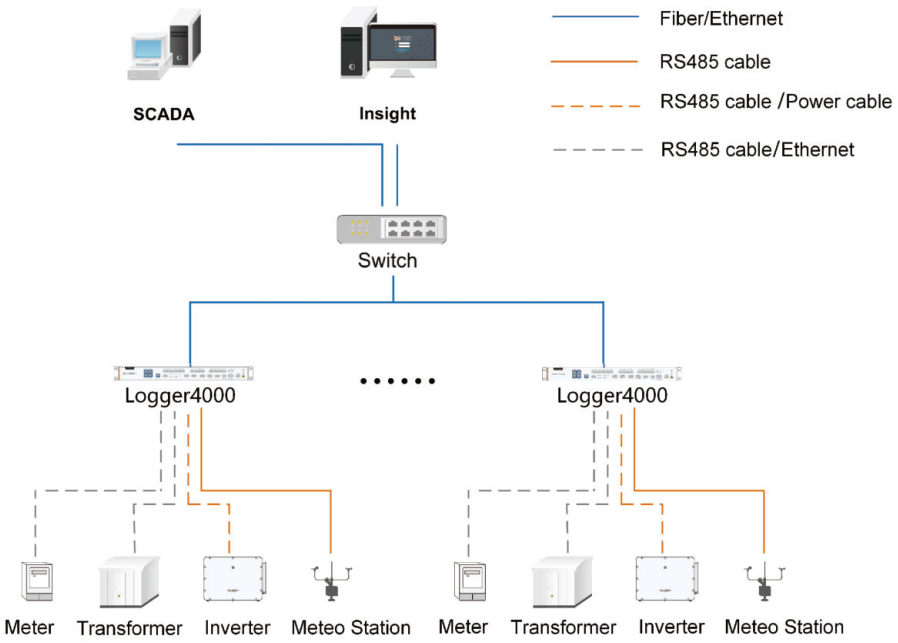
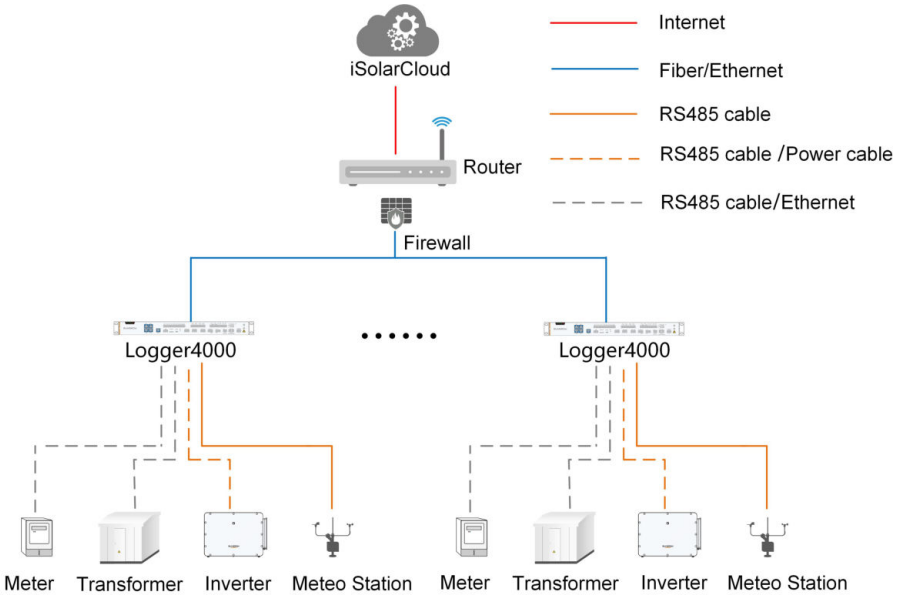


Figure 2-2 Star networking

Connected to iSolarCloud through a Router

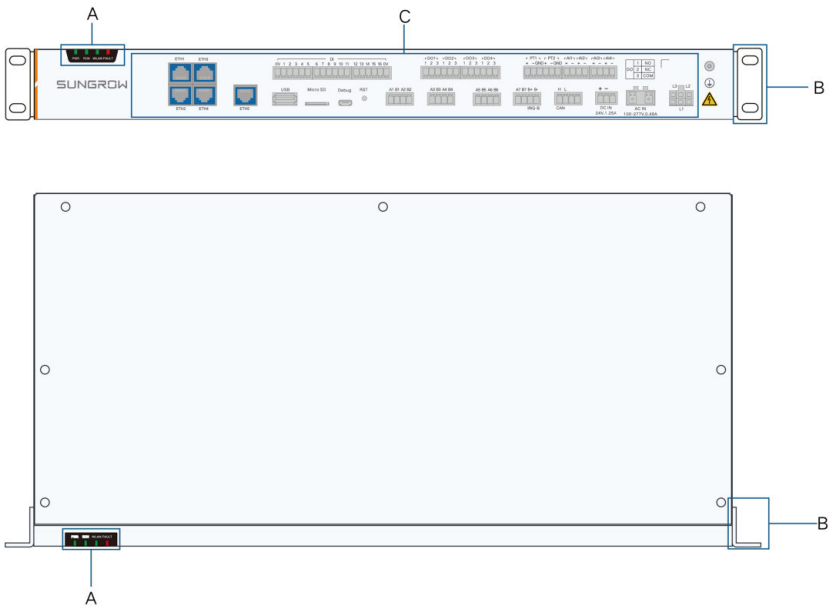
As shown in the figure below, the Data Logger can be directly connected to the iSolarCloud through a router.



The router and firewall are not included in the scope of delivery and need to be prepared by the customer.

2.3 Product Introduction

Appearance



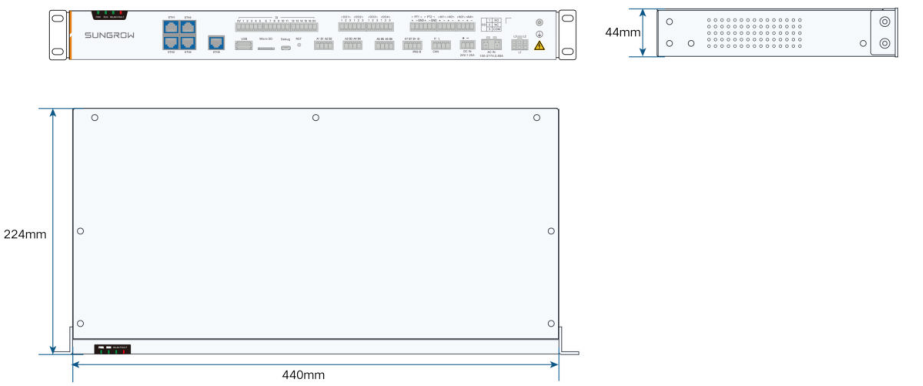
Item	Description
A	Indicators
B	Mounting ear
C	Wiring area

Indicators

Indicators	Name	Status	Status Description
PWR	Power indicators	Steady on (Red)	Normal power supply
		Off	Abnormal power supply
RUN	Running indicator	Blinking	Running normally
		Off/On	Abnormal operation
WLAN	WLAN indicator	Off	No WLAN function

Indicators	Name	Status	Status Description
FAULT	Fault indicator	Steady on (Red)	There is an alarm or fault in the connected inverter.
		Off	The connected inverter is free from faults.

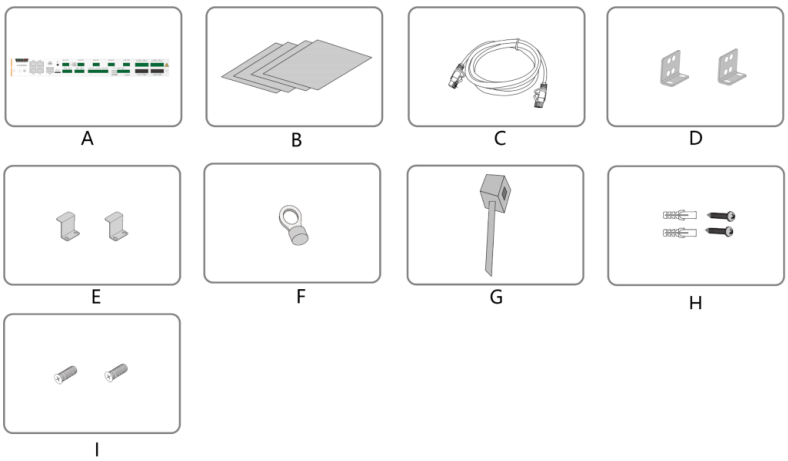
Dimensions



3 Unpacking and Storage

3.1 Scope of Delivery

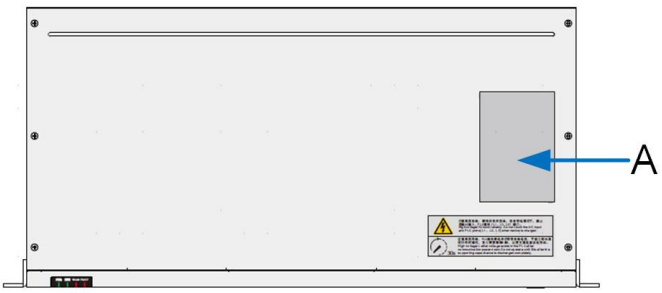
The items supplied with the data logger are listed below.



No.	Item	Description
A	Data logger	-
B	Documents supplied with the product	Quick installation guide, factory inspection record, packing list, warranty card, and certificate of conformity
C	Ethernet cable	1
D	Mounting ear	2
E	Mounting foot	2
F	OT terminal	2
G	Nylon cable tie	10
H	Self-tapping screw assembly	8 sets of ST4.8 × 19 expansion anchors and self-tapping screws for wall mounting.
I	Fastener assembly	6 sets of M4 × 8 cross-recessed countersunk-head screws, used to secure the mounting ears to the data logger

3.2 Identifying the Data Logger

The model and important technical parameters of the Data Logger can be found on the nameplate. The nameplate is attached to the back of the data logger, as shown in Figure A.



⚠ WARNING

The nameplate contains important parameters, which must be kept visible and free of stains and damage.

3.3 Checking upon Receiving

The product is thoroughly inspected and packed before delivery. However, it is possible for damage to occur during transport. Check the following items carefully once receiving the product:

- Check if the packing list matches the items included in the delivery. See 3.1 Scope of Delivery.
- Confirm that the received model is the same as the purchased one.
- Check the device thoroughly and ensure there are no visible damages.

If there are any problems, contact SUNGROW or the forwarding company.

⚠ WARNING

Proceed with installation and commissioning only if the product is intact without signs of damage! Before installation, ensure that:

- **The product is intact without any damages.**
- **Related documents, such as quick installation guide, are enclosed.**

3.4 Storage

If the Data Logger is not installed immediately after receiving, observe the following requirements to store it properly.

- Store the Data Logger in its original packing case in a well-ventilated, dry, and clean indoor environment.

- Ensure that the storage carrier can carry the weight of the Data Logger with the package.
- Ensure the device is kept in a well-ventilated and moisture-proof place, without accumulation of water.
- Ambient temperature: -40°C~+70°C. Relative humidity: 0~95%, no condensation.
- Take precautions to protect the device against damage due to harsh environment such as sudden temperature changes or collision.
- Conduct regular inspection, preferably at least once a week. Check whether the packaging is intact and prevent any damage that may be caused by pests and animals. Replace the packaging immediately if it is damaged.
- If the storage period exceeds six months, open the packaging to inspect the equipment and conduct power-on testing.

⚠ WARNING

- **Do not store the equipment without packaging!**
- **Do not store the equipment outdoors or under direct sunlight.**
- **No tilting or stacking!**

After long-time storage, thoroughly check the Data Logger and ensure it is undamaged before installation. If necessary, install the Data Logger only after it has been tested by qualified personnel.

4 Mechanical Installation

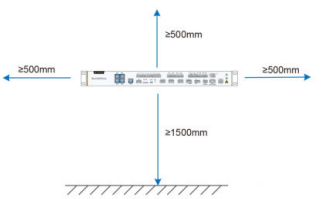
4.1 Installation Location Selection

Environment Requirements

- The Data Logger has an IP20 protection rating and should only be installed indoors.
- Ambient temperature: –30°C to +60°C. Ambient relative humidity: 0% to 95% (no condensation). Excessive humidity may cause damage to internal components.
- Pay attention to moisture prevention and ensure that the installation environment is free from flammable, explosive, and chemically corrosive substances.

Clearance Requirements

- Before installing the Data Logger, ensure that there is sufficient space around the installation location.
- Ensure that the Data Logger is oriented correctly, with the wiring terminals positioned at the bottom. This helps prevent dust, particles, and other airborne substances from entering the equipment over time, which could potentially impact its service life.
- Keep the Data Logger at least 1,500mm above the ground surface. Reserve a clearance of at least 500mm for convenient maintenance and servicing. The following figure shows the required minimum spacing.

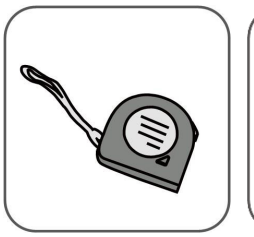
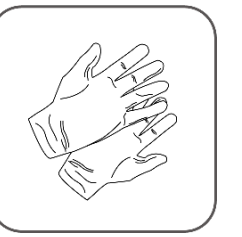
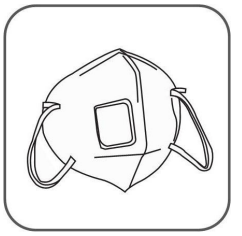
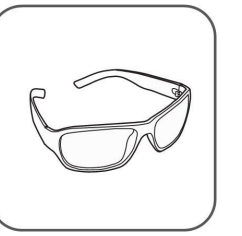
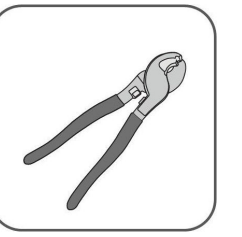
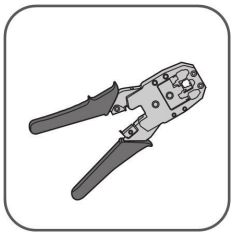
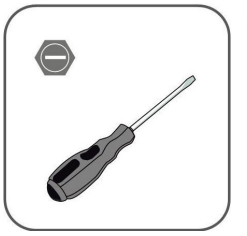
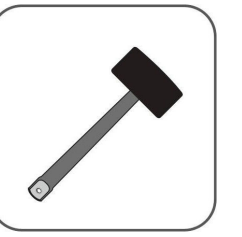


NOTICE

When connecting outdoor equipment, such as a Meteo Station, to the Data Logger, install a Surge Protection Device (SPD) to protect the communication system. Choose the right SPD based on the site conditions and requirements.

4.2 Installation Tools

Installation tools include, but are not limited to, the following recommended ones. If necessary, use other auxiliary tools on site.

			
Utility knife	Marker	Measuring tape	Protective gloves
			
Dust mask	Safety footwear	Vacuum cleaner	Goggles
			
Hammer drill	Electric screwdriver	Wire stripper	Wire cutter
			
Wire crimping tool	Slotted screwdriver	Phillips screwdriver	Rubber mallet

4.3 Mounting the Data Logger

As long as the installation environment requirements are met, the Data Logger can be installed at any suitable indoor location. The Data Logger can be rack-mounted or wall-mounted.

4.3.1 Wall-Mounted Installation

Prerequisite

DANGER

Avoid drilling holes in the utility pipes and/or cables attached to back of the wall!

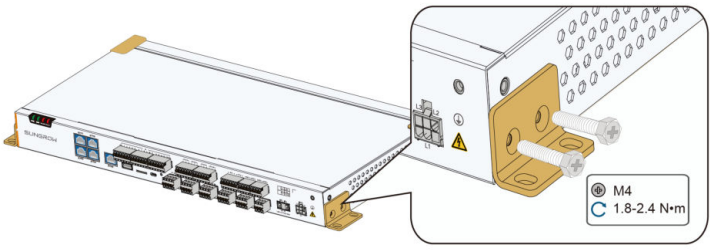
When holes are punched on the mounting surface, it is recommended to turn on a vacuuming device and wear goggles and a dust mask to prevent dust from entering the eyes or being inhaled into the body.

Installed parts

- Marker, not included in the scope of supply
- Hammer drill, not included in the scope of supply
- Bottom supporter, included in the scope of delivery
- Mounting ear, included in the scope of delivery
- Expansion bolt, included in the scope of delivery
- Tapping screw, included in the scope of delivery
- Screwdriver, not included in the scope of delivery

Install Mounting Ears and Bottom Supporters

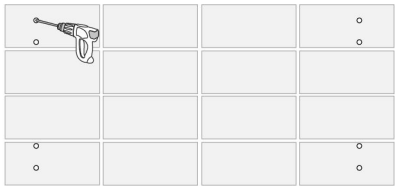
Anchor the mounting ears and bottom supporters to the Data Logger with supplied M4x8 cross recessed countersunk head screws. The fastening torque is 1.8-2.4N·m. The anchoring method is as follows:



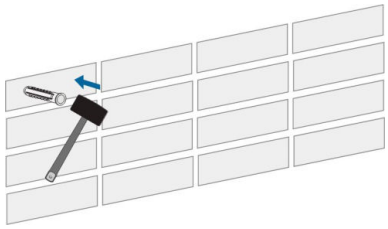
Mount the Data Logger to the Wall

Step 1 Mark positions for drilling holes on the installation wall. Drill the holes with a hammer drill of φ6mm. (Note: Ensure the required spacing between the Data Logger and surrounding objects.)

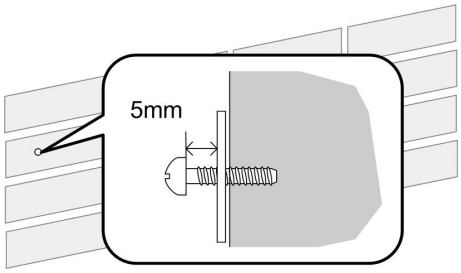




Step 2 Insert the expansion sleeve into the drilled hole, and make it completely embedded in the wall with a rubber hammer.



Step 3 Insert the tap screw and mounting ear successively into the expansion sleeve, to fix the Data Logger onto the wall.



Step 4 Fasten the tapping screw with a screwdriver by the torque of 0.3N·m.

--End

4.3.2 Rack-Mounted Installation

Use 1U standard rack in case of the rack-mounted installation.

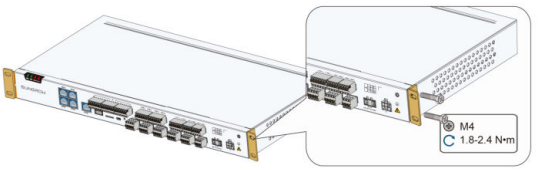
Prerequisite

The following lists the components, tools, and devices used during installation.

- 1U standard rack, not included in the scope of delivery
- Screwdriver, not included in the scope of delivery
- Screw, not included in the scope of delivery
- Nut, not included in the scope of delivery

Install mounting ears

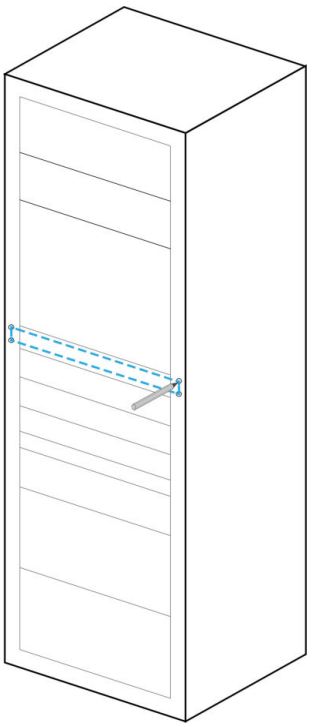
Anchor the mounting ears to the Data Logger with supplied M4x8 cross recessed countersunk head screws. The fastening torque is 1.8-2.4N·m. The anchoring method is as follows:



Step 1 Mark positions on the rack according to dimensions of the Data Logger.



Step 2 Drill holes on the rack with a hammer drill of φ6mm.



Step 3 Level the mounting ears with the drilled holes on the rack.



Step 4 Fix the Data Logger in the sequence of screws, mounting ears, rack, and nuts.

--End

5 Electrical Connection

5.1 Safety Instructions

⚠ DANGER

High voltage hazard!
The Data Logger should be reliably ground. Never touch the AC power supply port "AC IN 100–277V, 0.48A" and MPLC communication port "L1/L2/L3" when the device is powered on.

NOTICE

High Risk hazard! Danger will be caused by touching the MPLC communication port immediately after powering down. Wait at least 30s to have the capacitor discharge completely.

NOTICE

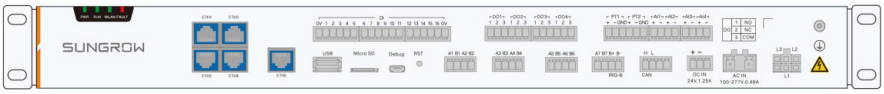
Incorrect wiring may result in damage to the Data Logger and potential harm to the operator.

NOTICE

All cables are intact, well-insulated, and appropriately dimensioned.

5.2 Port Introduction

The layout and identifiers of the Data Logger terminals are shown below.



Symbol	Name	Recommended cables	Description
ETH1~ETH2	Ethernet port	-	Data exchange Ethernet port. Can be connected to the SCADA using devices.
ETH3~ETH4	Fast dispatch port	-	Used for active and reactive fast scheduling using Goose.
ETH5	Ethernet port	-	Reserved for master/standby functions.

Symbol	Name	Recommended cables	Description
DI	Digital input	0.75mm^2 outdoor anti-ultraviolet wire	Passive dry contact input port
USB	USB port	-	Reserved
Micro SD	SD port	-	Used for software programming (this port is only available to SUNGROW technicians)
Debug	Debug port	-	Used for debugging of the Data Logger
RST	Reset	-	Press and hold it for > 30s to restore the default settings. Press and hold it for < 3 seconds, reserved
DO1~DO4	Digital output	0.75mm^2 outdoor anti-ultraviolet wire	Relay output interface Relay specification: 250Vac/1A or 30Vdc/1A
PT1 and PT2 AI1~AI4	Analog input	0.75mm^2 outdoor anti-ultraviolet wire	PT100/PT1000 detect range: -30°C ~120°C Two-wire or three-wire connection method AI1: 0~10Vdc AI2-AI4: 4~20mA
A1B1~A7B7	RS485 communication interface	2 x (0.75~1.5) mm^2 outdoor anti-ultraviolet twisted pair with a shielding layer	Support of 7 inputs of RS485 Can be connected to both slave device and SCADA
IRIG-B	Inter-Range Instrumentation Group-Time Code Format B	-	Reserved

Symbol	Name	Recommended cables	Description
CAN	CAN communication port	-	Reserved
DC IN 24V, 1.25A	DC24V power supply port	0.75~1.5mm^2 outdoor anti-ultraviolet wire	If the current is ≤1.25A, the switch mode power supply at this port requires reinforced insulation.
AC IN 100–277V, 0.48A	AC power supply port	0.75~1.5mm^2 outdoor anti-ultraviolet wire	Connecting 100~277Vac (50/60Hz), current≤0.48A
	Grounding hole	1~1.5mm^2 outdoor anti-ultraviolet wire	Connecting protective grounding cable
L1, L2, L3	MPLC communication interface	0.5~0.75mm^2, cable withstand voltage: cable grounding working voltage ≥ 1000 V	Can be connected to string inverters equipped with PLC communication function

AC power supply port and MPLC communication interface

High voltages may be present on the AC power supply port “AC IN 100–277V, 0.48A” and MPLC communication port “L1, L2, L3". Therefore, before cable connection, ensure that the ports are free of voltage and the grounding cable is reliably connected.

Digital input/output ports

Digital input/output ports (DI and DO1~DO4) are configured to collect node data and control node communication.

RS485 communication ports

For the RS485 communication ports (A1B1~A7B7), the communication distance should be no more than 1,000m.

5.3 Wiring Overview

The Data Logger:

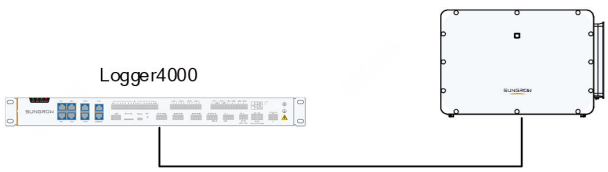
- can be connected to devices in the PV system such as the inverter, combiner box, Meteo Station, and energy meter through the RS485 port.
- can be connected to SCADA devices through the Ethernet port.
- can be connected to transformer or other devices through the MPLC port.

5.4 Connecting to the Inverter

5.4.1 Connecting to the Device with RS485 Port

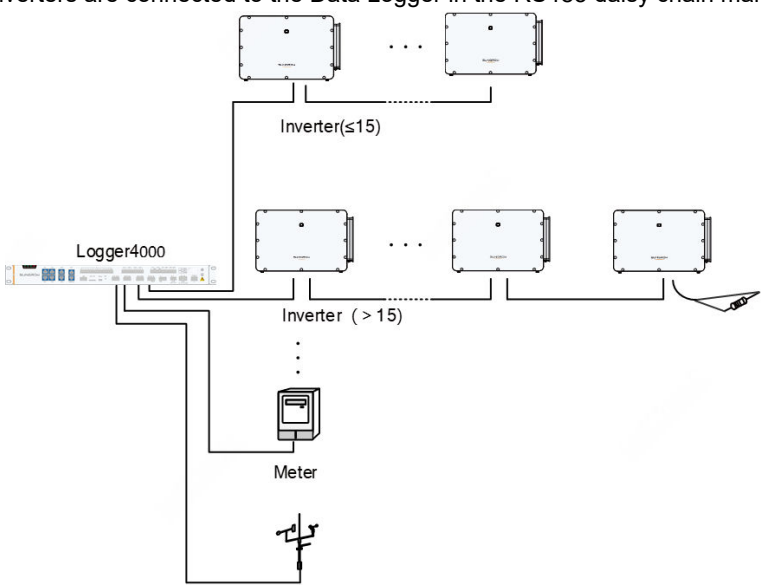
Use an RS485 shielded twisted pair (STP) to connect any RS485 port (A1B1–A7B7) of the Data Logger and the RS485 communication terminal of the inverter.

Connecting to a Single Inverter



Connecting to Multiple Inverters

Multiple inverters are connected to the Data Logger in the RS485 daisy chain manner.



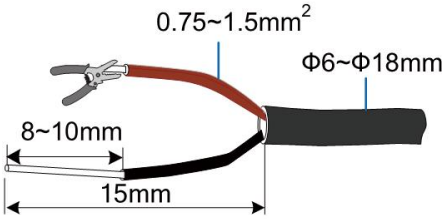
- The Data Logger supports 7 RS485 buses and 300 devices at most. Each RS485 bus supports 80 devices at most.
- Devices of different types must be connected to different RS485 communication ports of the Data Logger. For example, the transformer and the inverter should be connected to different RS485 communication ports of the Data Logger.

- The address of each device on the RS485 bus should be within the set address range (1 to 246) of the Data Logger, and duplicate addresses are not allowed. Otherwise, communication failure occurs.
- Serial port parameters of each device on the RS485 bus should be consistent with those of the Data Logger. The serial port parameters include baud rate, data bit, stop bit, and check bit.
- To ensure stable system communication and accurate data acquisition, make sure that all inverters connected to the same transformer winding access the data logger via the same RS485 channel.Inverters under different windings must not be daisy-chained to the data logger via RS485; otherwise, data acquisition may fail. Any issues arising from such improper connections are not covered by the warranty.

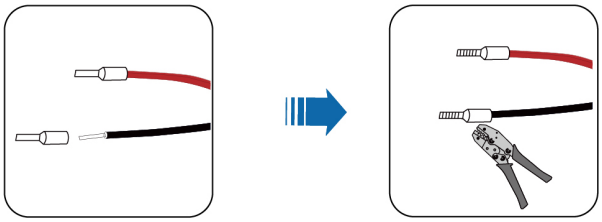
Connection Method

Step 1 Lead the RS485 communication cable from the inverter to the wiring area of the Data Logger.

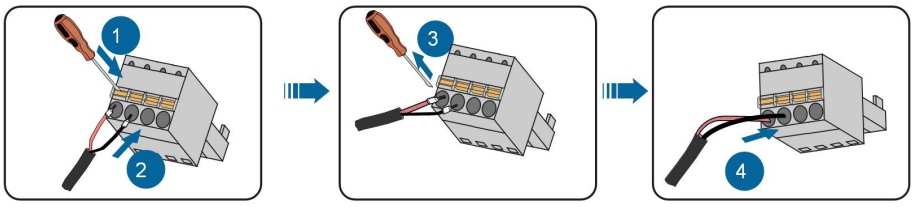
Step 2 Strip the protection layer of the communication cable with a wire stripper. Cable specification and stripped length are as follows.



Step 3 Install appropriate cord end terminals on the communication cables after removing the protective layer, and use a crimping tool to securely crimp them.



Step 4 Crimp the wiring terminals.

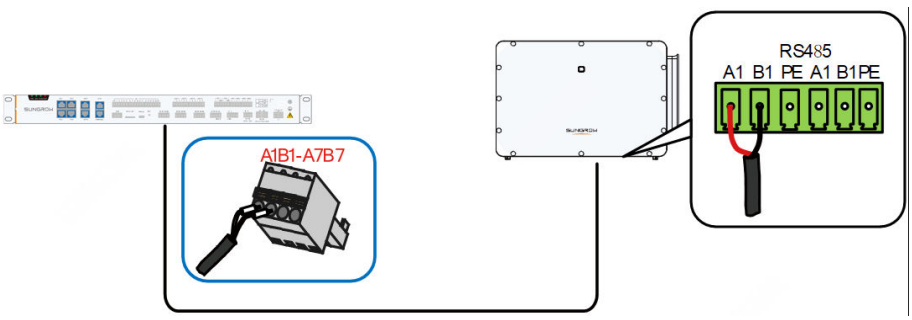


NOTICE

- **Connect RS485A to port A and RS485B to port B.**
- **The RS485 communication cable must be the shielded twisted pair with the shielding layer single-point grounded.**

When a multi-core and multi-strand copper core cable is used, the communications cable connected to an RS485 port on Logger must be crimped to cord end terminals of proper specification.

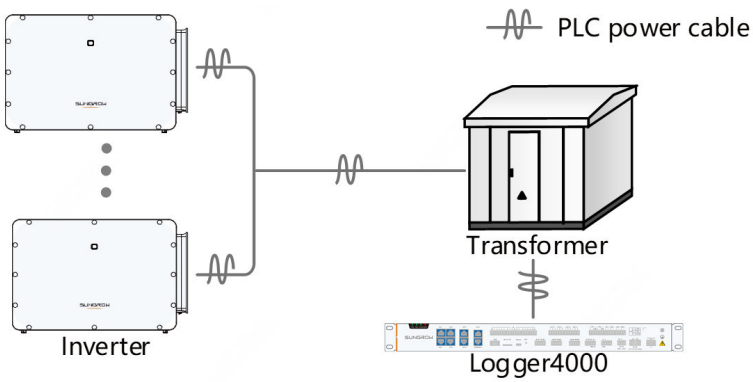
Step 5 Connect the wiring terminal to the terminal “A1B1~A7B7" of the Data Logger.



--End

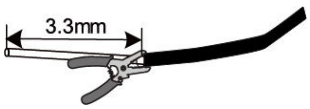
5.4.2 Connecting to the Inverter with MPLC Port

Integrated with MPLC master node, the Data Logger can be connected to the inverter integrated with MPLC slave node and achieve MPLC communication by using existing power cable.

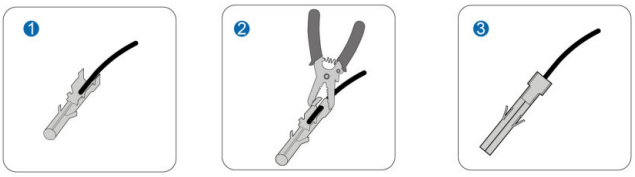


Preparation

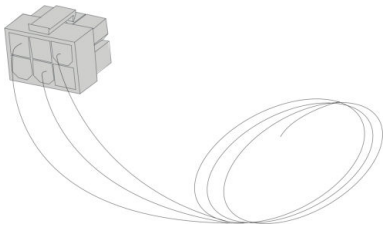
- Disconnect the transformer from the grid.
- Disconnect the DC side of the inverter and make sure the system is in safe state.
- If the MPLC cable in the scope of delivery is found short on site, prepare the MPLC cable referring to the following steps.
  1. Strip the protection layer of the MPLC cable with a wire stripper. Stripped length are as follows.



2. Install the pin on the MPLC cable after the protective layer has been removed, and crimp the MPLC cable using crimping tools. Prepare three MPLC cables with pins.



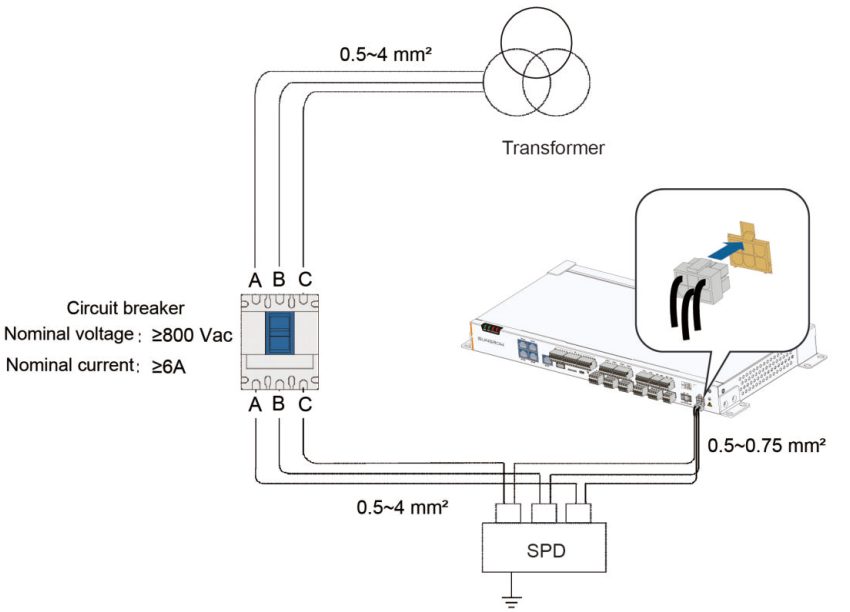
3. Connect the pins of the cables to the socket, as shown in the following figure.



Connection Method

Connect one end of the MPLC power cable in the scope of delivery to MPLC ports L1, L2, and L3 of the Data Logger, and the other end to the three-phase ports of the circuit breaker.

The L1 port of the Data Logger must be connected to phase A of the circuit breaker, the L2 port to phase B, and the L3 port to phase C. The details are as follows.



The external circuit breaker is not included in the scope of delivery, and users need to prepare it by themselves if necessary.
The external circuit breaker just needs to meet the above two parameters (nominal voltage and nominal current). Other parameters, such as breaking capacity, are not mandatory requirement.

NOTICE

Isolation voltage of the MPLC cable should be greater than 1,000V, recommended cable specification: 0.5~0.75mm^2.
The MPLC connection cable must be connected to a three-level surge protector, otherwise it may cause damage to the equipment.

NOTICE

The built-in MPLC module of the Data Logger supports AC voltage less than 1000V. When using the MPLC communication method, the communication distance between the Data Logger and the inverter should not exceed 1000 meters.

NOTICE

MPLC networking is intended for medium voltage grid-connection. If low voltage grid-connection is desired, observe the following two conditions:

- **Never connect a load between the Data Logger and the MPLC slave node.**
- **The distance between the Data Logger and the load should be greater than 20m, that is, the LV grid-connection point should be more than 20m away from the nearest load distribution line. The load includes air conditioners, machines, motors, etc.**

NOTICE

When using the MPLC communication method, consider the following:

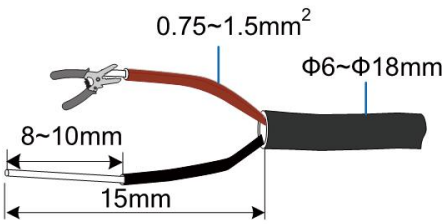
- **The electrical connection between the inverter and the downstream transformer has been successfully established and verified to be correct.**
- **Input and output circuit breakers of the Data Logger, inverter, and transformer are connected.**

5.5 Connecting to the Meteo Station

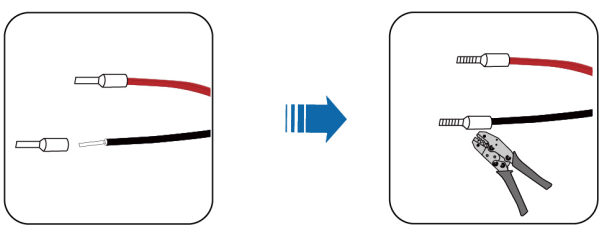
Meteo Station of the Modbus-RTU protocol can be connected to the Data Logger.

Step 1 Lead the RS485 communication cable from the Meteo Station to the wiring area of the Data Logger.

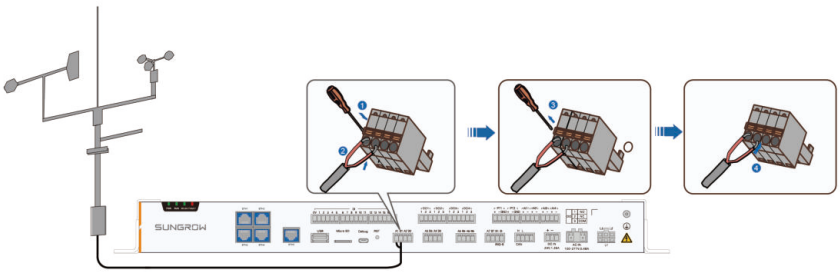
Step 2 Strip off the protective layer and insulation layer of the communication cable with wire strippers, as shown below.



Step 3 Install appropriate cord end terminals on the communication cables after removing the protective layer and insulation layers, and use a crimping tool to securely crimp them.



Step 4 Connect the cable to the RS485 port of the Data Logger, as shown in the figure below.



--End

5.6 Connecting to the Meter

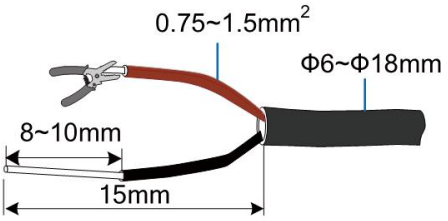
Connect the meter to the data logger through RS485 or Ethernet, as detailed in the following table.

Brand	Meter Communication Port	Port Definition	Protocol Type	Wiring Method
Wasion	24	RS485-A	Modbus RTU	5.6.1 RS485 Cable Connection
	25	RS485-B	Modbus RTU	
	26	Common ground	Modbus RTU	
	27	RS485-A	Modbus RTU	
	28	RS485-B	Modbus RTU	
Acrel	21	RS485-A	Modbus RTU	
	22	RS485-B	Modbus RTU	
Weidmüller EM610	17	RS485-A	Modbus RTU	
	16	RS485-B		
Janitza UMG604	22	RS485-B	Modbus RTU	
	23	RS485-A		
	Ethernet	Ethernet	Modbus TCP	5.6.2 Ethernet Cable Connection

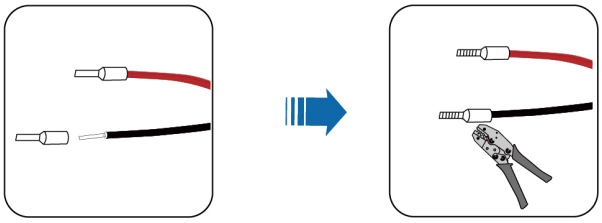
5.6.1 RS485 Cable Connection

Step 1 Lead the RS485 communication cable from the meter to the wiring area of the Data Logger.

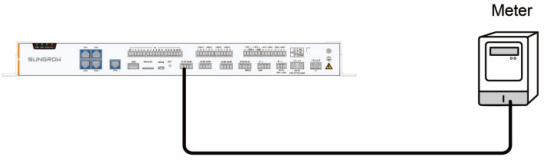
Step 2 Strip off the protective layer and insulation layer of the communication cable with wire strippers, as shown below.



Step 3 Install appropriate cord end terminals on the communication cables after removing the protective layer and insulation layers, and use a crimping tool to securely crimp them.



Step 4 Connect the cable to the RS485 port of the Data Logger, as shown in the figure below.



--End

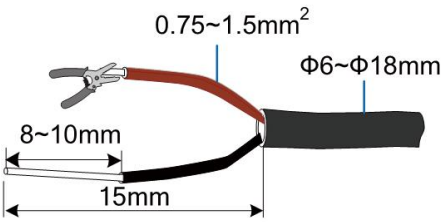
5.6.2 Ethernet Cable Connection

Connect the "Ethernet" port of the energy meter and the "ETH1, ETH2, ETH5" port of the Data Logger with a network cable.

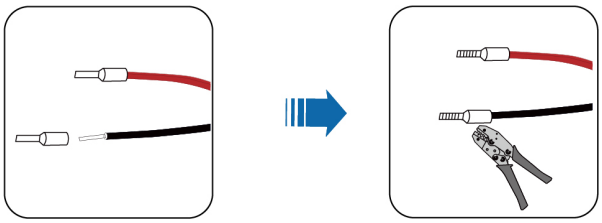
5.7 Wiring of DI Signal

The DI port is used to access DI signals, such as grid dispatching instructions and alarms. Only passive dry contact signals are supported. It is recommended that the signal transmission distance not exceed 10m.

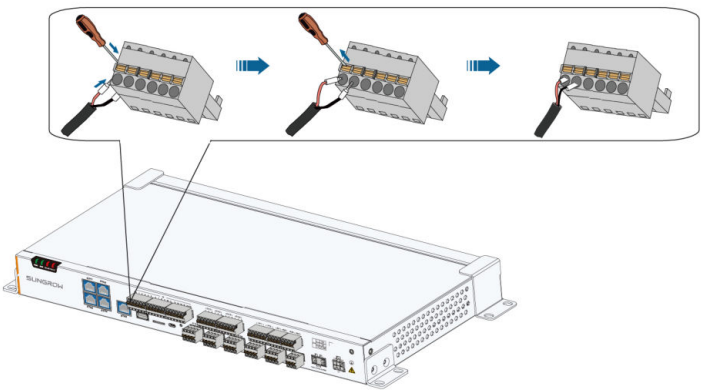
Step 1 Strip the protection layer and insulation layer of the dry contact input signal cable with a wire striper, as shown in the figure below.



Step 2 Install cord-end terminals and crimp them with crimping pliers.



Step 3 Connect the cord end terminals to the plug "DI" outside the Data Logger, as shown below. Port "OV" and Port "1" are taken as an example.

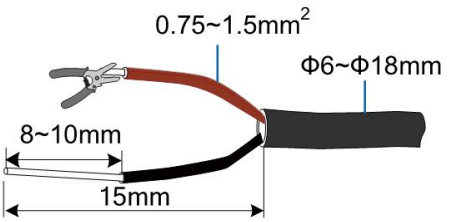


--End

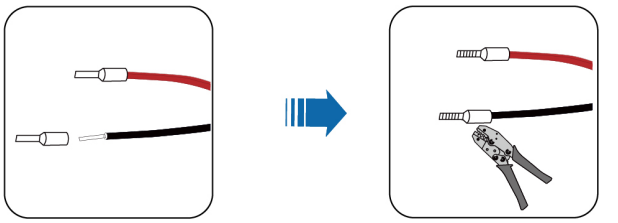
5.8 Wiring of DO Signal

Port 1 corresponds to NO, port 2 to NC, and port 3 to COM. NO/COM is the normally open contact, and NC/COM is the normally closed contact. It is recommended that the signal transmission distance not exceed 10m.

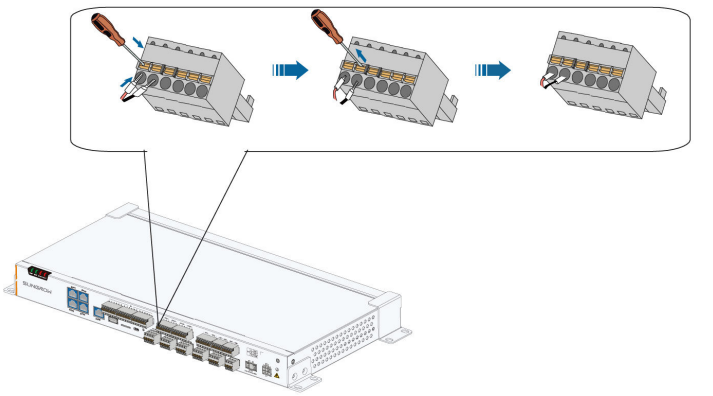
Step 1 Strip the protection layer and insulation layer of the dry contact output signal cable with a wire striper, as shown in the figure below.



Step 2 Install cord-end terminals and crimp them with crimping pliers.



Step 3 Connect the cord end terminals to plugs “DO1”~”DO4" outside the Data Logger, as shown below. Port “DO1" is taken as an example.

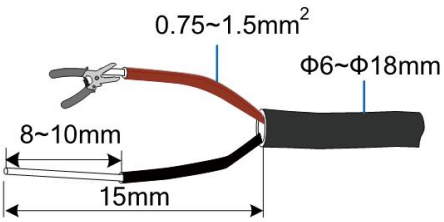


--End

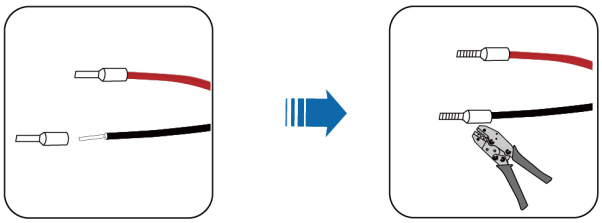
5.9 Wiring of AI Signal

The AI port is used to access AI signals of devices such as environmental monitoring sensors. It is recommended that the signal transmission distance not exceed 10m.

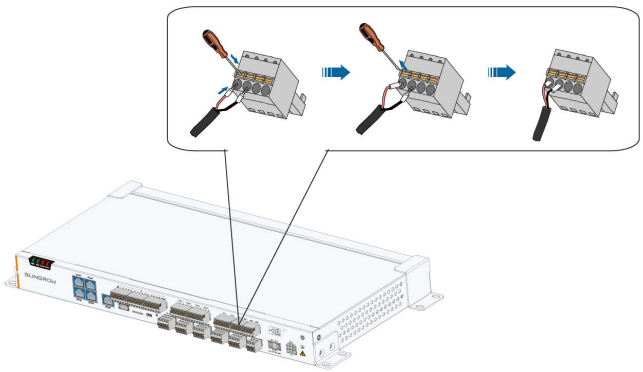
Step 1 Strip the protection layer and insulation layer of the analog input signal cable with a wire striper, as shown in the figure below.



Step 2 Install cord-end terminals and crimp them with crimping pliers.



Step 3 Connect the cord end terminals to plugs "AI1"~"AI4" outside the Data Logger, as shown below. Port "AI1" is taken as an example.



--End

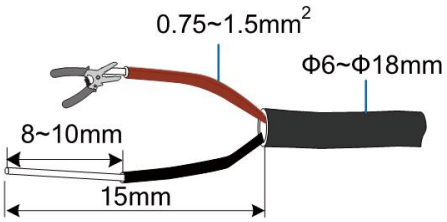
Port	Symbol	Description
AI	AI1	Supported voltage input range: 0V~10Vdc
	AI2	Supported current input range: 4mA~20mA
	AI3	
	AI4	

AI + is connected to AI signal +, AI - is connected AI signal -.

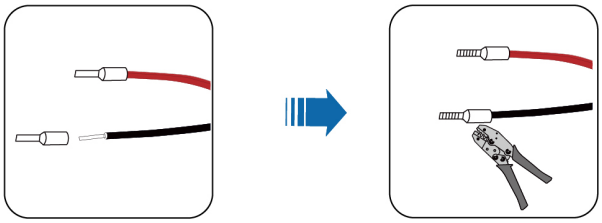
5.10 Wiring of PT Signal

The Data Logger is designed with two PT ports and supports 3-wire or 2-wire PT100/ PT1000 temperature sensor connection.

Step 1 Strip the protection layer and insulation layer of the signal cable for temperature detection with a wire striper, as shown in the figure below.



Step 2 Install cord-end terminals and crimp them with crimping pliers.



Step 3 Connect the cord end terminals to plugs “PT1”~”PT4" outside the Data Logger, as shown below. Port “PT1" is taken as an example.

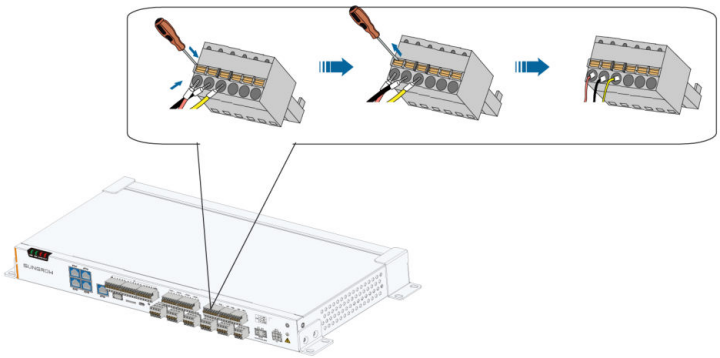


Figure 5-1 3–wire PT100/PT1000 connection

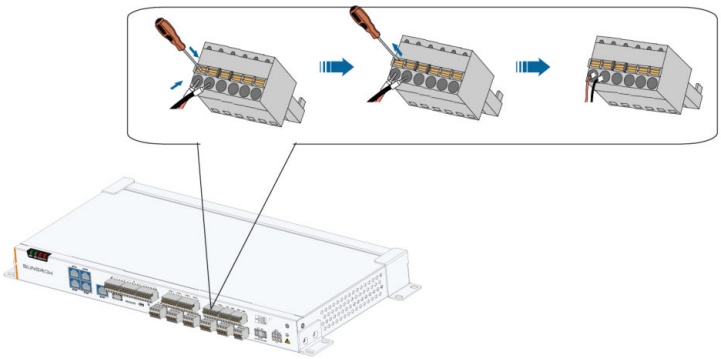


Figure 5-2 2–wire PT100/PT1000 connection

--End

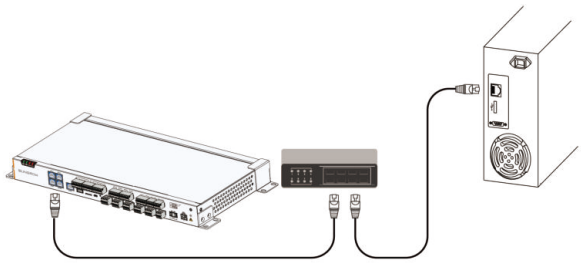
5.11 Connecting to the Remote Monitoring Device

The Data Logger can be connected to the SCADA with an Ethernet switch or a router.

The Data Logger is equipped with three Ethernet ports: ETH1, ETH2 and ETH5. Access the Ethernet switch and the router through either port. This section takes connecting to an Ethernet switch as an example to illustrate the wiring steps.

The ETH5 network port is only for debugging and cannot be connected to the SCADA communication system.

Step 1 Insert one plug of the supplied network cable into the network port of the Ethernet switch and the other plug into the ETH port of the Data Logger.



Step 2 Set network parameters.

--End

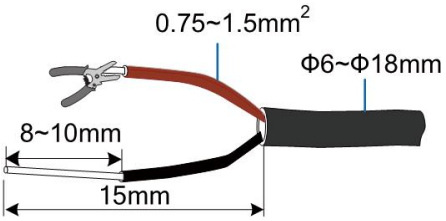
- For the default IP address of Ethernet ports (ETH1, ETH2, ETH5), see 6.2 Commissioning Steps.
- If the DHCP (Dynamic Host Configuration Protocol) feature is enabled for the Ethernet port (ETH1, ETH2, and ETH5), its IP address can be retrieved after it is connected to a router or other device.

5.12 Connecting to the AC Power Supply

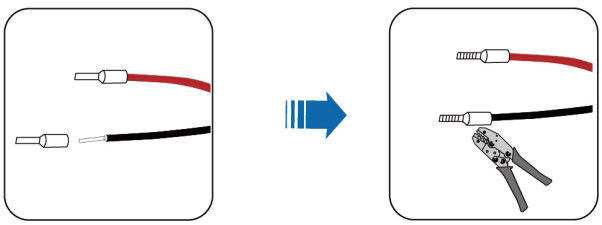
The Data Logger can be connected to a power source with voltage ranging from 100 to 277Vac.

Step 1 Lead the external power supply cable to the wiring area of the Data Logger.

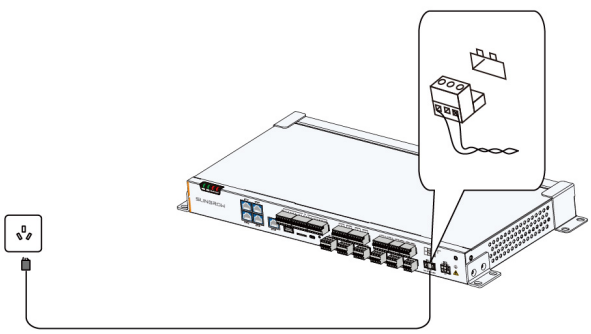
Step 2 Strip off the protective layer and insulation layer of the power cable with wire strippers, as shown below.



Step 3 Install appropriate cord end terminals on the power cables after removing the protective layer and insulation layers, and use a crimping tool to securely crimp them.



Step 4 Connect the cord end terminals to the plug "AC IN 100~277V, 0.48A" outside the Data Logger.



--End

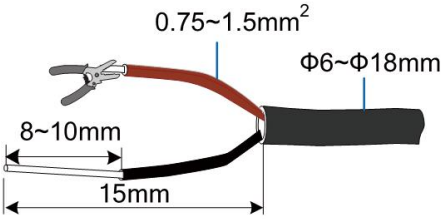
The Data Logger can be connected to both AC power supply and DC power supply. UPS can be used as a DC backup power source.

5.13 Connecting to the DC Power Supply

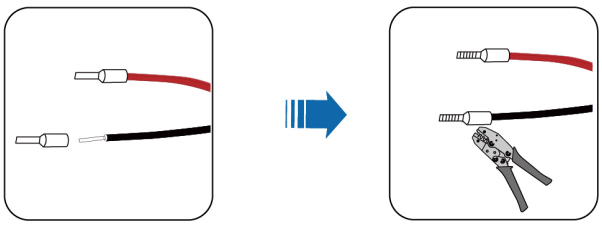
The Data Logger can be connected to 24Vdc external power supply. UPS can be used as a power source.

Step 1 Lead the external power supply cable to the wiring area of the Data Logger.

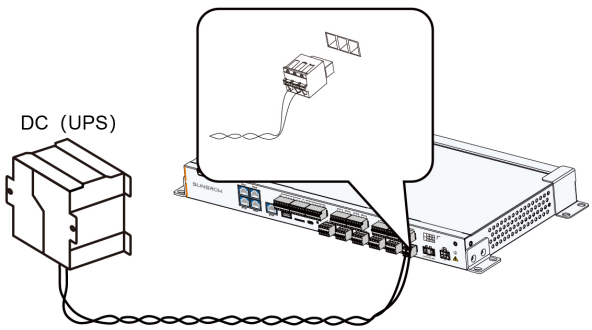
Step 2 Strip off the protective layer and insulation layer of the power cable with wire strippers, as shown below.



Step 3 Install appropriate cord end terminals on the power cables after removing the protective layer and insulation layers, and use a crimping tool to securely crimp them.



Step 4 Connect the cord end terminals to the plug "DC IN 24V, 1.25A" outside the Data Logger.



--End

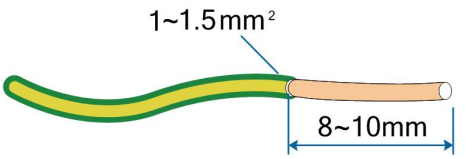
5.14 Earthing Connection

Prerequisite

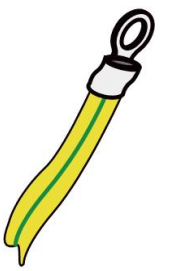
⚠ WARNING

The grounding cable should be grounded reliably. Otherwise, It may cause fatal electric shock to the operator in case of failure. The equipment may be damaged when struck by lightning.

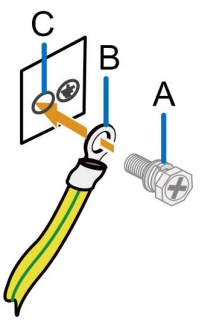
Step 1 Strip the protection layer and insulation layer of the grounding cable by specific length, as shown in the figure below.



Step 2 Select proper OT terminal and crimp them.



Step 3 Secure the grounding cable to the grounding hole of the Data Logger, as shown in the figure below.



Item	Definition	Remarks
A	Screw	M4
B	OT terminal	-
C	Grounding hole	-

Step 4 Fasten the screw with a wrench by the torque of 5±1N·m.

--End

6 Commissioning

6.1 Inspection before Commissioning

No.	Check Item	Result
1	All cables are intact, well-insulated, and appropriately dimensioned.	□
2	All cables are connected correctly and firmly.	□
3	The polarity of the power supply cable is correct. The grounding cable is reliably grounded.	□

6.2 Commissioning Steps

No.	Description
1	Connect the commissioning PC to one of ETH1, ETH2, ETH5 ports of the logger with a network cable. • ETH1, default IP: 12.12.12.12, virtual IP: 15.15. • ETH2, default IP: 13.13.13.13, virtual IP: 16.16.16.16 • ETH5, default IP: 14.14.14.14, virtual IP: 17.17.17
2	Power on the data logger by connecting an external power supply.
3	Check whether the RUN indicator light on the exterior of the data logger blinks normally.
4	Access the default IP address of the connected port using Internet Explorer, Safari, or Chrome.
5	In the web interface, configure the serial port parameters.
6	Add PV devices connected to the data logger to the Web interface by manually adding them.
7	Configure the IP address.
8	If inverter data needs to be uploaded to iSolarCloud, the address of the iSolarCloud cloud platform must be configured. The default iSolarCloud site for integration is “**Chinese Server**”. If used in the Chinese mainland, it must be set to “**Chinese Server**”.

No.	Description
	If used in the European region, set it to “**European Server**”. If used in the Australia region, it must be set to “**Australian Server**”. If used in the India region, it must be set to “**India**”. If used in other regions, it must be set to "**International Server**".
9	Log in to the data logger Web interface and check whether the operating data of the string inverters produced by Sungrow Power Supply is normal.
10	Create a plant using the iSolarCloud app and check whether the data on the iSolarCloud cloud platform is normal. The iSolarCloud platform has discontinued its services in the North America Region.

To create a new plant using the iSolarCloud App, you can either scan the QR code on the label on the front of the data logger or manually input its S/N number to add a communication device. For detailed instructions, refer to the "iSolarCloud App User Manual". Scan the QR Code to view or obtain the "iSolarCloud App User Manual".

7 Web Interface

7.1 Log in to Web System

Information Required for Login

Table 7-1 Default Accounts and Passwords

User Type	Username	Default Password	Permissions
General user	user	Username followed by the SN	Monitoring access and basic settings (e.g., overview, device monitoring, partial historical data).
O&M User	maintain	Username followed by the SN	All operations mentioned in this manual.
Auditor	auditor	Username followed by the SN	Audit the operation logs and rsyslog logs for all users.
Administrator	administrator	Username followed by the SN	Add or delete users, modify user information, empty users, manage sessions, enable or disable R&D debugging, and assign certificates.
Developer user	develop	Dynamic password generated based on the SN obtained after customer authorization.	Perform troubleshooting and fault diagnosis for complex device issues after being authorized by the administrator.

Table 7-2 Default Accounts and Passwords

User Type	Username	Password
Administrator	administrator	Please contact SUNGROW for the password; ensure you change the initial password.
O&M User	maintain	Please contact SUNGROW for the password; ensure you change the initial password.
Developer	develop	Dynamic password generated via S/N after customer authorization

Starting from firmware version P018 of Logger4000, the web interface adds a new user management feature. For details, see 10 User management.

Table 7-3 ETH Port Information

Port	IP address	Subnet mask
ETH1	Default IP address: 12.12.12.12 Virtual IP address: 15.15.15.15	255.255.255.0
ETH2	Default IP address: 13.13.13.13 Virtual IP address: 16.16.16.16	
ETH5	Default IP address: 14.14.14.14 Virtual IP address: 17.17.17.17	

Prerequisite

- The data logger has been connected to the PC via an Ethernet cable.

1. Taking connection via the ETH1 port as an example:

Step 1 Modify the PC network configuration to ensure it is on the same subnet as the data logger's IP address.

Item	Data Logger Default Setting	PC Setting Example
IP address	12.12.12.12	12.12.12.125

Item	Data Logger Default Setting	PC Setting Example
Subnet mask	255.255.255.0	255.255.255.0

Make sure the first three octets of the IP address are the same. The last octet must be within the range of 0 to 255 (excluding 12).

Step 2 Enter the IP address in the browser's address bar.https://12.12.12.12, press **[Enter]** to access the web interface.

Step 3 Log in to Web port.

a. Enter the username and password.

To enhance account security, starting from Logger4000 firmware version P018, the username must be entered when logging in as an O&M user. The default O&M username is “maintain”.

If upgrading the Logger4000 firmware from version P017 or earlier, note the following password changes:

- When upgrading to versions P018–P021: the initial login password for the O&M account is changed to “pw@111111”.
- When upgrading to version P022 or later: the initial login password for the O&M account remains “pw1111”.

If upgrading from versions P018–P021 to P022 or later, the initial login password for the O&M account is changed to “pw1111”.

Complete the required information. The actual display may vary.

If...	Then...
The login dialog box does not include a **Username** field	1. Enter the initial login password:pw1111. 2. Click **Login**.
The login dialog box includes a **Username** field	1. Enter the default O&M account:maintain. 2. Enter the initial login password:pw@111111or pw1111. 3. Click **Login**.

After logging in, the web interface will display the user operation screen.

Step 4 Check the Logger4000 firmware version and confirm whether an upgrade is required. See 7.8.11 Check Firmware Version for details.

For firmware update, see 8.2 Updating the Data Logger.

--End

7.2 Modifying Password

NOTICE

To keep your account secure, it is recommended to change the password regularly and always make sure you remember the new one. Not changing the default password can lead to unauthorized access, and continued use of the initial password increases the risk of theft and hacking. Additionally, loss of the password can prevent access to the device, potentially causing losses to the power station. In these cases, SUNGROW shall not be liable for any losses incurred due to non-compliance with the recommended security practices.

Step 1 Click > **Change password** to enter the corresponding page.

Step 2 In the pop-up **Change password** dialog box, enter the **Old password** and **New password**, and then **Confirm new password**.

Please change the initial password upon first login.
Passwords should be 8–32 character long and contain at least three of the following four character types: uppercase letters, lowercase letters, numbers, and special characters. The new password cannot be the same as the old one.

Step 3 Click **Confirm** and log into the system using the new password.

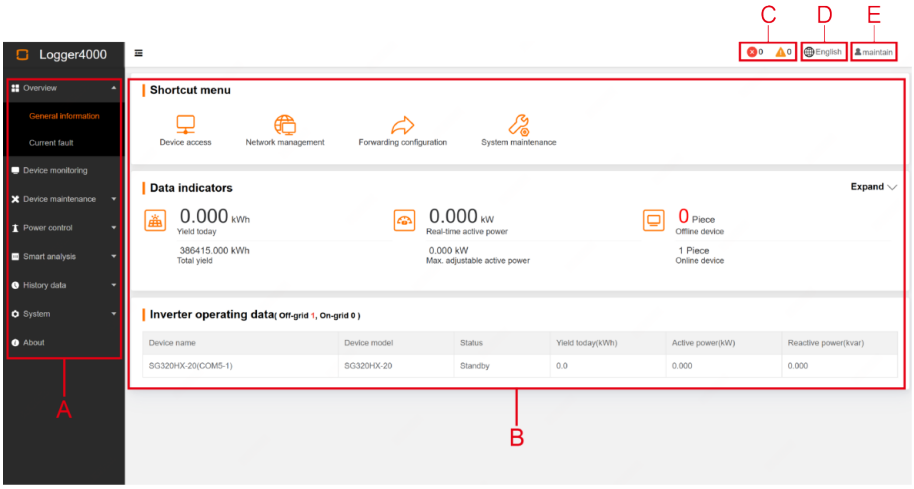
--End

If you forgot your password, contact system administrator or SUNGROW.

7.3 Web UI Overview

7.3.1 Web Main Interface

The main interface is as follows:



Item	Name	Description
A	Navigation menu	Display main function modules of the Web
B	Function display area	Display the current interface
C	Alarm icon	Display the current alarm level and alarm number. Users can click the icons to enter the corresponding alarm page.
D	Language menu	Click the button to select the desired language.
E	User	Display the current login user.

indicates the connection status of the Data Logger’s Ethernet port.

indicates the connection status of the Data Logger's cloud service.

7.3.2 Operating Environment Requirements

Item	Description
Browser	Chrome 65 or later; Safari 11 or later
Minimum resolution	1920 × 1080
Language	The Web interface supports eight languages: Simplified Chinese, English, German, Spanish, Brazilian Portuguese, French, Japanese, and Korean. The computer used to access the embedded Web interface must use one of these eight system languages. Otherwise, login is not supported.

7.3.3 Operation Procedure

Prerequisite

- Finished the electrical connection.
- Logged into the Web.

Step 1 Configure serial ports of the Data Logger.

After logging into the Web, first configure the serial ports to ensure that the Data Logger can normally communicate with downstream devices. See 7.8.7 Port Parameter.

Step 2 Calibrate the system time.

Check whether the current system time is correct, and perform manual time synchronization or automatic time synchronization when necessary. See 7.8.5 System Time.

Step 3 Add other devices. See 7.6.1 Device List.

Step 4 Configure forwarding service.

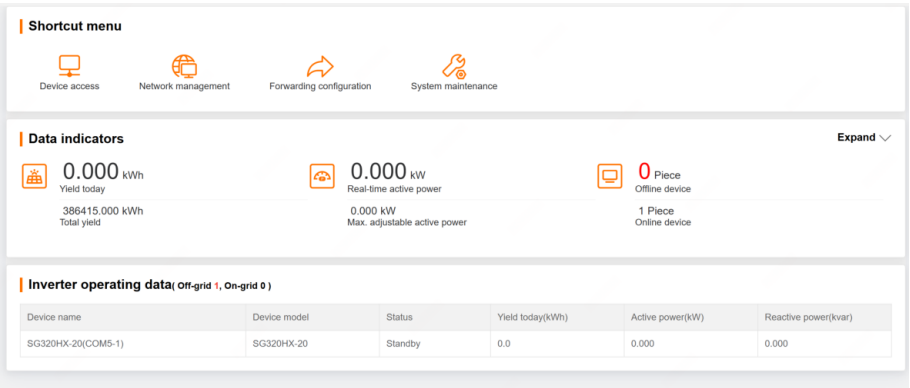
After all devices have been added, configure the forwarding service to ensure that the Data Logger can forward the data to upstream devices. See 7.8.6 Forwarding Configuration .

--End

7.4 Overview

7.4.1 General Information

Click **Overview** > **General information** to enter the corresponding page.



Shortcut menu

- **Device access**: Click the menu to add, delete, modify, and view the device. See 7.6.1 Device List。
- **Network management**: Set Ethernet parameters. See 7.8.7 Port Parameter.
- **Forwarding configuration**: Transfer the data connected by the system to the SCADA. See 7.8.6 Forwarding Configuration .
- **System maintenance**: Support of operations such as system upgrade, log export, and rebooting. See 7.8.2 System Maintenance.

Data indicators

Information such as today yield, total yield, real-time active power, number of offline devices, and real-time reactive power, reactive power range, active power set, and reactive power set can be viewed.

Click **Expand** to view more information.

Inverter operating data

Information on the inverter such as state, daily yield, active power, and reactive can be viewed.

7.4.2 Current Fault

Click **Overview** > **Current fault** to enter the corresponding page.

Information such as device name, alarm name, alarm type, alarm time, fault code, and fault ID can be viewed.

7.5 Device Monitoring

Click **Device Monitoring** to view device information.

View real-time information, DC information, initial parameters, operating parameters, system parameters, protection parameters, other protection parameters, power regulation parameters, fault recording parameters, general parameters, device instructions, and device information.

In the device list on the left, click ⌄ and select a device type from the drop-down list.

7.5.1 Real-Time Information

The Real-time information page shows device energy yield, status, active power, and other information.

Step 1 Choose **Device Monitoring**.

Step 2 Select a device from the list on the left, then choose **Realtime Values** to view its real-time information.

--End

7.5.2 DC Info

View the voltage and current of multiple maximum power point tracking (MPPT) channels and PV strings.

- Choose **Device Monitoring**. Select a device from the list on the left, then choose **DC Info** to view its DC information.

7.5.3 Initial Parameters

Select the inverter and configure the initial parameter settings. Both individual and batch settings are supported.

Step 1 Click **Device monitoring** > **Initial parameters** to enter the corresponding page.

Step 2 Click ⌄ in the device list on the left, select the device type in the drop-down list, and then select the device.

Step 3 Select **Country/region**.

Step 4 Click **Settings** to set initial parameters for an individual device.

Step 5 Set the initial parameters in batch.

a. Click **Configuration synchronization**.

b. Select the desired devices in the pop-up dialog, and click **Confirm** to apply the changes.

--End

7.5.4 Operation Parameters

- Click **Device monitoring** > **Operation parameters** to enter the corresponding page and set the operation parameters.

  Both individual and batch settings are supported. For configuration methods, see 7.5.3 Initial Parameters.

7.5.5 System Parameters

- Click **Device monitoring** > **System parameters** to enter the corresponding page and set the system time of the device.

  Both individual and batch settings are supported. For configuration methods, see 7.5.3 Initial Parameters.

7.5.6 Protection Parameters

- Click **Device monitoring** > **Protection parameters** to enter the corresponding page and set the protection parameters.

  Both individual and batch settings are supported. For configuration methods, see 7.5.3 Initial Parameters.

7.5.7 Protection Parameters (Other)

- Click **Device monitoring** > **Protection parameters (other)** to enter the corresponding page and set the protection parameters.

  Both individual and batch settings are supported. For configuration methods, see 7.5.3 Initial Parameters.

  Protection parameters (other)may vary by inverter model. Please refer to the actual page.

7.5.8 Power Regulation Parameters

- Click **Device monitoring** > **Power regulation parameters** to enter the corresponding page and set the power regulation parameters.

  Both individual and batch settings are supported. For configuration methods, see 7.5.3 Initial Parameters.

7.5.9 Fault Recording Parameters

Step 1 Choose **Device monitoring**.

Step 2 Select a device from the list on the left, then choose **Fault recording parameters** to view its fault recording parameters.

Step 3 For **Waveform recording standard**, select a recording standard from the drop-down list in the **Current value** column. The default parameter values for the selected mode appear.

Step 4 Change the fault recording parameters.

If an entered parameter value is outside the specified range, the system displays "Parameter check failed" when you save. Follow the message and enter a valid value.

a. To change a numeric parameter, enter the new value in the **Current value** column.

b. To change a status parameter, go to the **Current value** column, click ⌄, and select the required status from the drop-down list.

c. Click **Set**, then click **Confirm** in the dialog box to save.

Step 5 (Optional) Configure fault recording parameters for multiple devices.

a. Click **Configuration synchronization**.

b. In the dialog box, click **Confirm**. Then select the devices to apply the settings to and click **Confirm**.

--End

7.5.10 General Parameters

Step 1 Choose **Device monitoring**.

Step 2 Select a device from the list on the left, then choose **General Parameters** to view its general parameters.

Step 3 Select **Read-back**, then set **Register Address**, **Register Number**, and **Address Type**. Click **Read-back** to read the current values from the device.

Step 4 Select **Settings**, then set **Register Address**, **Data Type**, and **Set Value**. Click **Save** to apply the changes to the selected device.

Refer to the communication protocol for the relevant inverter for parameter details.

Step 5 (Optional) Configure general parameters for multiple devices.

a. Click **Configuration synchronization**.

b. In the device list that appears, select the devices to configure and click **Save**.

--End

7.5.11 Device Instructions

You can start up, shut down, and restore factory settings on SUNGROW inverters. Both individual and batch configuration are supported.

For example, to start up an inverter:

Step 1 Choose **Device monitoring**.

Step 2 Select a device from the list on the left, then choose **Device instruction** to view its commands.

Step 3 Click **Boot** to open the startup dialog box. Enter your password and click **Boot**.

Step 4 Click **Yes** to start up the selected inverter.

Step 5 (Optional) Start up multiple inverters.

a. In the startup dialog box, click **Configuration synchronization**.

b. In the device list that appears, select the devices to configure and click **Save**.

--End

7.5.12 Device Information

Choose **Device monitoring**. Select a device from the list on the left, then choose **Device information** to view its information.

View the device serial number (S/N), model, rated active power, and other parameters.

7.5.13 Dispersion Rate Analysis

The dispersion rate is a key indicator for assessing the health of a PV power plant. It is primarily used to monitor and evaluate the consistency of power generation performance across the PV strings. A low dispersion rate indicates good consistency in current curves among the strings and stable production performance, while a high dispersion rate signifies a significant performance deviation that requires further diagnostic analysis. The one-click dispersion rate diagnosis function allows the O&M team to view the dispersion rates of all strings, quickly locate the abnormal strings, and implement corrective actions promptly. This enhances the efficiency of O&M activities and improves overall production for the plant.

The Logger4000's dispersion rate analysis function utilizes a self-learning algorithm. When a new inverter is connected to the system, the algorithm automatically adjusts its analysis parameters and models based on the variations in time and light conditions and the user's PV array settings. It can identify potential causes of abnormal power generation data from PV modules, providing reference for the O&M team.

NOTICE

Typically, the system can deliver reliable preliminary diagnostic results after collecting data over at least two sunny days from the inverter. Ensure the Logger4000 is powered on at night, as the algorithm engages in self-learning during this time, to allow for effective data analysis and model optimization.

PV brackets equipped with a tracking feature will adjust their orientations and angles based on the sun's position, which may compromise the accuracy of dispersion rate analysis results. Therefore, it is recommended that dispersion rate analysis be conducted only for plants with fixed PV brackets.

The firmware version of Logger4000 should be P028 or later. See 7.8.11 Check Firmware Version for details.

7.5.13.1 Enabling Dispersion Rate Diagnosis

Enable dispersion rate diagnosis via the user interface to use this function.

Step 1 Choose **Smart analysis** > **Dispersion rate diagnosis** on the navigation bar.

Step 2 Enable dispersion rate diagnosis. This function is turned on by default for P010 (firmware version) or later. For earlier versions, it is off by default, and will remain off even after the firmware is updated to P010 or later.

--End

7.5.13.2 Setting Array Parameters

Differences in the orientation and tilt angle of strings in one PV array can directly affect the dispersion rate calculation results. It is essential to consider the installation environment of the PV array in practice to eliminate factors that may influence the dispersion rate data. This improves the accuracy of the analysis and reduces the need for on-site inspections. Therefore, ensure that all array settings are finalized before proceeding with the one-click diagnosis.

Step 1 Choose **Smart analysis** > **Dispersion rate diagnosis** on the navigation bar.

Step 2 Click **Settings** to open the window for parameter settings.

Step 3 Complete the array settings based on the actual conditions at the site.

a. Enter a name for the array in **Array name** for easy identification.

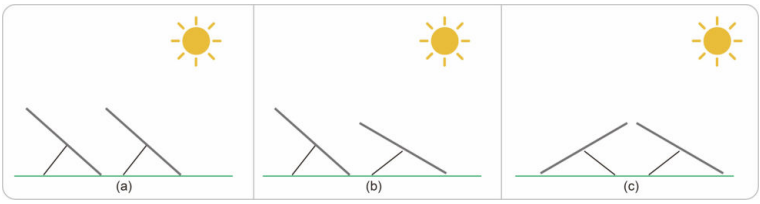
b. Specify the installation environment for the array in **Geographical environment**.

The following options are available:

- **Flat ground** (default)
- **Rooftop (distributed)**
- **Mountainous**
- **Water (pile-supported)**
- **Water (floating)**

c. Indicate whether the PV modules in the array are installed at a consistent angle in **Installation angle**.

- **Consistent (in both tilt angle and orientation)**: All PV modules have the same tilt and orientation, as shown in Figure (a).
- **Inconsistent**: The tilts or orientations of the PV modules vary, as shown in Figure (b) and (c).



Step 4 Click **Confirm**.

--End

7.5.13.3 Initiating Dispersion Rate Diagnosis

Users can initiate a dispersion rate diagnosis manually when light conditions are favorable.

Prerequisite

- The algorithm self-learning process for the currently connected inverter has been completed.
- Array parameters have been set. See 7.5.13.2 Setting Array Parameters for details.
- The inverter's communication is normal, and it has been online for at least 30 minutes.
- No dispersion rate diagnosis task is currently in progress.

Inverters in the array that are experiencing communication interruptions or have restored communication for less than 30 minutes will not be involved in the dispersion rate diagnosis.

Diagnosis of abnormal environmental conditions is not supported for an inverter that is newly connected in the array.

Step 1 Choose **Smart analysis** > **Dispersion rate diagnosis** on the navigation bar.

Step 2 Click **One-click diagnosis**.

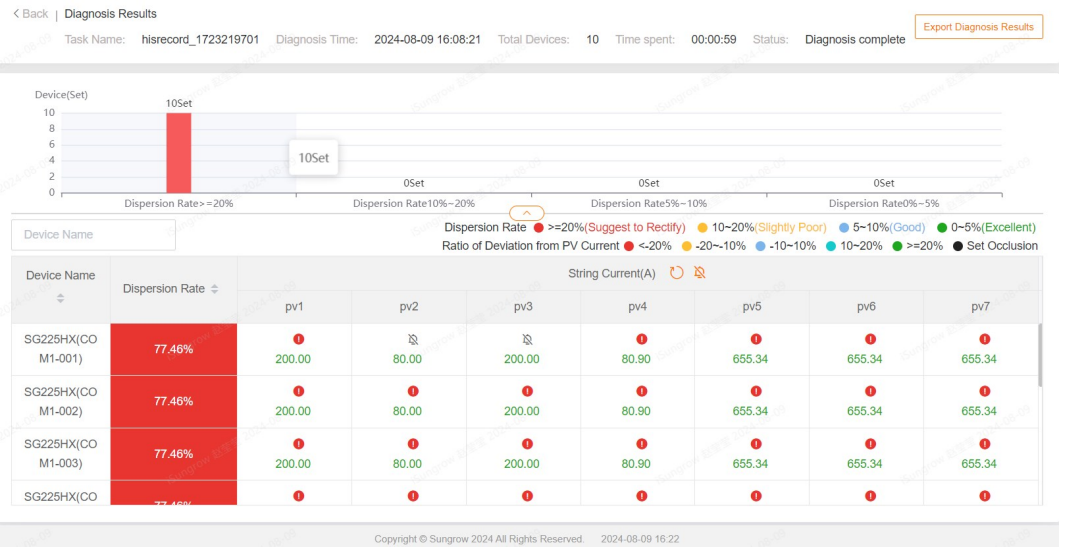
Task progress will be displayed in a pop-up window on the Web user interface.

Step 3 After the diagnosis is completed, click **View** to go to the **Diagnosis results** page and check the result. See 7.5.13.4 Viewing Diagnosis Results for details.

--End

7.5.13.4 Viewing Diagnosis Results

Users can view the dispersion rate grade, dispersion rate data, and alarms after the diagnosis is completed.



No.	Definition	Description
1	Dispersion rate grade	Inverters are graded based on their dispersion rate. The bar graph illustrates the distribution of inverters across various grades. • **Excellent** (0–5%): Branch currents are stable. • **Good** (5–10%): Branch currents are generally satisfactory, with a few branches experiencing relatively low current. • **Slightly Poor** (10–20%): Branch currents are generally not ideal, with a few noticeably lower than others. • **Suggest to Rectify** (over 20%): A few branches are experiencing open circuits, which compromises the plant's production. Corrective actions are necessary.
2	Details list	This list displays the dispersion rate of each inverter, the current of each string, and the alarms.

Only for a real-time diagnosis task, you can view the string alarms, configure occlusion time settings, and block the alarms as needed within the details list.

Step 1 Navigate to the **Diagnosis Results** page in the following ways.

- View the results of real-time diagnosis tasks: Choose **Smart analysis** > **Dispersion rate diagnosis** and initiate a diagnosis process. After the diagnosis is finished, click **View**. See 7.5.13.3 Initiating Dispersion Rate Diagnosis for details.

- View the results of history diagnosis tasks: Choose **Smart analysis** > **Dispersion rate diagnosis** . Find the **Diagnosis record** panel at the bottom, and click **View** in the "Action" column of the corresponding task to view its details.

Step 2 To view the diagnosis results for a specific inverter, type its name in the **Device Name** field at the top left of the list.
The **Diagnosis Results** page will then display the diagnosis results for that inverter.

Step 3 Click **Export Diagnosis Results** in the upper right corner of the page to download the diagnosis results to your local system (as an .xlsx file).

--End

7.5.13.4.1 Viewing String Alarms

PV strings with abnormal dispersion rates as well as the potential causes and analysis results of the alarms are shown on the **Diagnosis Results** page. Users can block the alarms not expected to be immediately addressed.

Prerequisite

- The dispersion rate diagnosis has been completed. See 7.5.13.4 Viewing Diagnosis Results for details.

Dispersion rate diagnosis can detect the following three abnormal symptoms.

Table 7-4 Abnormal Symptoms

Abnormal Symptom	Description
Logger abnormal	The string current shows abnormal because data cannot be collected properly due to incorrect logger configuration or device faults.
Inverter operation abnormal	The string current shows abnormal because the inverter cannot operate properly.
Environment abnormal	The string current shows abnormal because the modules are sheltered or due to other environmental factors.

Step 1 If a string sees an abnormal current issue, click  above the current data in the details list to open the **Alarm** window. You can then view the potential causes and analysis results of the alarm.

Step 2 If you do not plan to deal with the alarm in the short term, select the checkbox before the device name and click **Block Alarms**.

In future diagnosis tasks, the blocked alarm will not be shown for this string.

There might be more than one alarm in a string. You can select multiple alarms and block them all.

See 7.5.13.4.2 Unblocking String Alarms for how to unblock the alarms.

--End

7.5.13.4.2 Unblocking String Alarms

After a string alarm reported in a history diagnosis task has been addressed, users can unblock the alarm.

Prerequisite

- The dispersion rate diagnosis has been completed. See 7.5.13.4 Viewing Diagnosis Results for details.

Step 1 In the details list, click **String Current** to the right of to open the **Blocked Alarm History** window.
All the alarms that are blocked for the PV strings will be shown in "Blocked Alarm History".

Step 2 If an alarm has been addressed, select the checkbox before **Device Name**, and click **Delete** in the "Action" column to remove it from the blocked list.

Step 3 Click **Confirm**.

--End

7.5.14 Air Duct Health Detection

This function is jointly implemented by the Data Logger and SG320HX-20. The Data Logger monitors the inverter's operating status and performs diagnosis when the inverter operates at low power levels with minimal power fluctuations. Based on fan speed control and the temperatures of key inverter components, the system uses software algorithms to automatically detect cooling faults and assess the degree of blockage caused by inlet/heat sink blockage. It will also trigger active pre-alarms to assist O&M, thereby improving the air duct health of the inverter.

NOTICE

- **The Data Logger must be installed at an altitude no higher than 5300 meters.**
- **Diagnosis may be affected during cloudy, rainy, or overcast weather due to power fluctuations. It is recommended to perform diagnosis under clear weather conditions.**

This function is available on LOGGERSV400.001.00.P034 or later.

7.5.14.1 Enable Air Duct Health Detection

Prerequisite

An inverter has been added, and the array must include at least one SUNGROW inverter.

Before performing air duct health detection, make sure Air duct health detection is enabled.

Step 1 Choose **Smart analysis > Air duct health detection** from the navigation bar.

Step 2 By default, **Air duct health detection** is disabled. Select **Enable** from the drop-down list to enable it.

Step 3 Enter the data logger's actual altitude in the **Altitude** text box. The default range is 0–1500 m.

- If the altitude exceeds 1500 m, enter the actual value to ensure accurate detection. No change is needed at or below 1500 m.
- The altitude setting error must not exceed 200 m, or detection accuracy may be affected.

Step 4 Click **Save**.

--End

7.5.14.2 Setting Air Duct Health Detection Parameters

It is essential to consider the installation environment of PV arrays in practice to eliminate factors that may influence the data to be detected. This improves the accuracy of the air duct health detection and reduces the need for on-site inspections. Users can configure the sensitivity, diagnosis count, and diagnosis interval of the detection as needed.

Prerequisite

Air duct health detection is enabled.

Step 1 Choose **Smart analysis** > **Air duct health detection** .

Step 2 Click **Diagnosis settings**. In the pop-up dialog box, configure the parameters and click **Confirm**.

- **Max. daily diagnosis count (1–50)**: Set the maximum number of diagnoses per day. The default value is 3. Once the limit is reached, no further diagnoses will be performed on that day.
- **Diagnosis interval (0–365)**: Set the number of days between diagnoses. The default value is 7 days. The next diagnosis can only be performed after the set interval.

Step 3 Click **Sensitivity setting**. In the pop-up dialog box, set the parameter and click **Confirm**.

You can adjust the sensitivity level based on the severity of duct blockage. The default setting is Low.

- **High**: High sensitivity triggers alarms more frequently and allows earlier detection of air duct anomalies.
- **Low**: Low sensitivity triggers alarms less frequently and only when the blockage becomes more severe.

--End

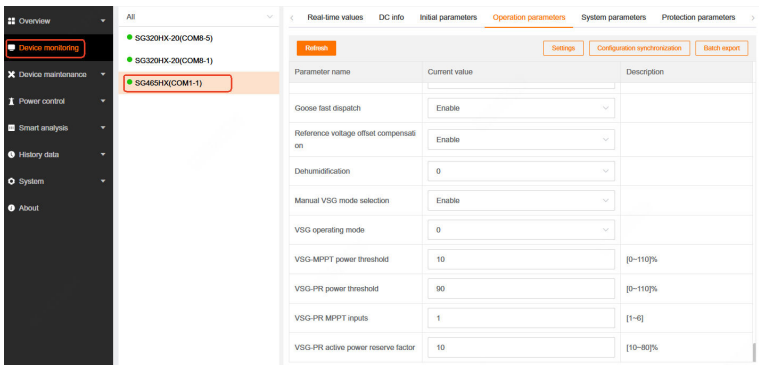
After adding a device for the first time, at least one sunny day is required to generate diagnosis results.

7.5.15 VSG Parameter Settings

Prerequisite

Grid-forming (VSG) mode affects grid stability and safety. Before enabling this mode, consult the local grid operator. Until then, you are advised to operate in grid-following mode.

Step 1 In the navigation bar, choose **Device monitoring**, select the target inverter, and click **Operation parameters** to open the corresponding page.



Step 2 Set **VSG operating mode** and adjust the corresponding parameters as required.

Parameter	Description
VSG operating mode	When "Manual VSG mode selection" is enabled, select the inverter operating mode. The available modes include PQ mode, VSG-MPPT mode, VSG-PR mode, and VSG-CV mode. This parameter is used to set the target VSG operating mode.
Manual VSG mode selection	When this function is disabled, the inverter operating mode automatically switches among PQ mode, VSG-PR mode, and VSG-MPPT mode. When this function is enabled, automatic switching among modes is not supported.
VSG-MPPT power threshold	When "Manual VSG mode selection" is disabled, set the power coefficient for automatic switching from PQ mode to VSG-MPPT mode. Mode switching is triggered when the actual power reaches this threshold.
VSG-PR power threshold	When "Manual VSG mode selection" is disabled, set the power coefficient for automatic switching from VSG-MPPT mode to VSG-PR mode. The mode is switched when the actual power reaches this threshold.
VSG-PR MPPT inputs	Specify the MPPT input to operate at the MPPT point in VSG-PR mode. For example, if this value is set to "1", DC input 1 operates at the MPPT point.

Parameter	Description
VSG-PR active power reserve factor	Set the active power reserve factor in VSG-PR mode. For example, if this value is set to "10%", the system reserves 10% active power in VSG-PR mode, and grid-forming control is performed at 90% of the forecast power.
VSG voltage ride-through	When this function is enabled, if a short-term grid voltage abnormality occurs, the device does not immediately disconnect from the grid and continues to support operation for a period of time.
VSG inertia time constant	Set the VSG inertia time constant. This parameter specifies the time required for the virtual synchronous generator rotor to accelerate from standstill to the rated speed under rated torque in grid-forming control.
VSG frequency damping coefficient	Set the VSG frequency damping coefficient. For example, when the rated frequency is 50 Hz and this value is set to "10", a 1 Hz frequency change corresponds to a 0.2Pn power change. This parameter specifies the power coefficient used by the virtual synchronous generator to oppose frequency changes in grid-forming control. It simulates the damping winding characteristics of a conventional synchronous generator, provides additional damping support, and suppresses system frequency oscillation.
VSG frequency droop coefficient	Set the VSG frequency droop coefficient. For example, when the rated frequency is 50 Hz and this value is set to "30", a 1 Hz frequency change corresponds to a 0.6Pn power change. This parameter indicates the primary frequency regulation droop characteristic that simulates a conventional synchronous generator in grid-forming control and automatically adjusts active power when the grid frequency changes.
VSG primary frequency regulation upper limit	Set the upper limit for VSG primary frequency regulation. For example, if this value is set to "10%", the upper limit of active power change is 10%Pn. This parameter limits the primary frequency regulation power range.
VSG primary frequency regulation lower limit	Set the lower limit for VSG primary frequency regulation. For example, if this value is set to "20%", the lower limit

Parameter	Description
	of active power change is 20%Pn. This parameter limits the primary frequency regulation power range.
VSG voltage droop slope	Set the VSG voltage droop slope. For example, if this value is set to "10.0", reactive power output is 1Pn when the voltage changes by 0.1Un. This parameter indicates the reactive power-voltage droop characteristic that simulates a conventional synchronous generator in grid-forming control and automatically adjusts reactive power when the grid voltage changes.
VSG voltage droop deadband	Set the VSG voltage droop deadband. When the grid voltage deviation is within the deadband, VSG does not regulate reactive power.
Parallel subarray No.	Set the Parallel subarray No. This parameter is used in multi-subarray black start scenarios. 1 indicates the primary subarray, and values ≥2 indicate secondary subarrays.

Step 3 After completing the adjustments, click **Settings**, then click **Confirm** in the confirmation dialog box to save the changes.

--End

7.6 Device Maintenance

7.6.1 Device List

The **Device list** function is used for managing devices connected to the Data Logger and configuring addresses for these devices.

7.6.1.1 Export

Step 1 Click **Device maintenance** > **Device list** to enter the corresponding page.

Step 2 Click  to export the device list.

--End

7.6.1.2 Import

Step 1 Click **Device maintenance** > **Device list** to enter the corresponding page.

Step 2 Click  to export the device list.

Step 3 After the device list is exported, user can modify device names in batch.

Step 4 After the modification is completed, save the device list file in the .csv format.

Step 5 Click  to import the .csv file into the Web interface.

--End

7.6.1.3 Add Device

Step 1 Choose **Device maintenance** > **Device list**.

Step 2 Click **Add device**. In the **Add device** window, select **Device type** and complete the required fields as prompted.

Step 3 Select the string inverter and the corresponding communication mode. Available **Communication method** include PLC and RS485.

> Inverter addresses must be unique within a single PV array.

- **PLC**: Whitelist-based addition is recommended.

  > Under PLC communication, the **Add sequentially** functions apply only when there is no PLC interference.

  - **Add via whitelist file**: Use the mobile app to scan the inverter barcode to generate a whitelist file. Transfer the file to the computer, and click the import icon to import it to the data logger. After whitelist networking is complete, the whitelist networking result is displayed. For adding devices to a new plant, whitelist addition is recommended first to ensure accuracy.

    > In the iSolarCloud app, tap More > Modbus whitelist configuration > specify the file name and PLC type. Then generate the whitelist file by scanning the inverter QR code or entering the information manually.

  - **Add sequentially** : Ensure that the array No. and band No. of the data logger primary and secondary nodes are consistent. In addition, obtain the inverter addresses in advance and ensure that the addresses are consecutive.
- **RS485**: **Add sequentially** is available.
  - **Add sequentially** : Add the inverter addresses in advance. When adding inverter addresses for the data logger array No., ensure that the addresses are consecutive.

- Only one communication mode can be selected for the same port. If the PLC function is enabled for the port, devices cannot be added through RS485 communication.
- After devices are added through whitelist addition, the **Replace device** button is added to the page, allowing you to update the device SN.

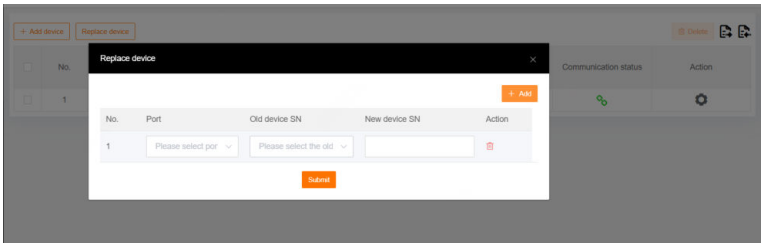


Figure 7-1 Replace Device

--End

7.6.1.4 Edit Device

Step 1 Click **Device maintenance** > **Device list** to enter the corresponding page.

Step 2 Click to open the **Edit device** pop-up window. The name of the device connected to the Logger and other parameters can be modified.

The "**Device name**" is named in the form device model (port number-communication address).
Take "SG36KTL-M (COM1-7)" as an example. "SG36KTL-M" is device type, "COM1" is the communication port, and "7" is the communication address.

Step 3 Click **Save** to apply the changes.

--End

7.6.1.5 Delete Device

After a device is deleted on site, the user can delete the device from the **Device list** page, to keep device consistency.

Step 1 Click **Device maintenance** > **Device list** to enter the corresponding page.

Step 2 Select the device to be deleted, click **Delete**.

Step 3 Click **Confirm** in the pop-up window, to delete the device.

--End

7.6.2 Inverter Log

Step 1 Click **Device maintenance** > **Inverter log** to enter the corresponding page.

Step 2 Select the device running information, and click to view the export progress.

Step 3 Click **Export** to store the exported log locally.

Step 4 Click **Cancel** and then **Confirm** on the pop-up window, to cancel the current operation.

--End

7.6.3 AFCI Detection

Step 1 Click **Device maintenance** > **AFCI detection** to enter the corresponding page.

Step 2 Check the devices that need to self-checking, click **Self-test** and then **Confirm** on the pop-up window.

> The status of the self-checking device must be **Enable**. If the self-checking status is **Disable**, you can click ⌄ to set the self-checking status to **Enable**.

Step 3 The result column shows the self-checking status as Self-Testing. After 7~8 seconds, the self-checking result will be displayed as Self-checking Failure or Self-test Pass.

Step 4 Click **Clear fault** to bring up a dialog box showing the status of fault clearing.

--End

7.6.4 Fault Recording

The fault recording module provides tools for capturing and analyzing electrical events. It covers fault recording, grid waveform recording, and RMS waveform recording for device troubleshooting, grid compliance, and event tracking on specific regional models.

Accessing the Module

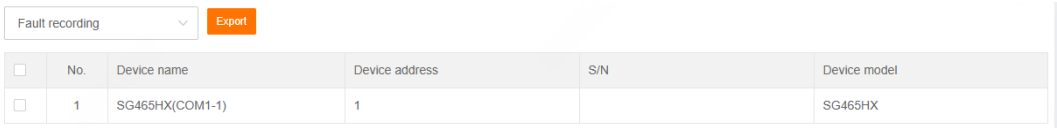
On the main screen or in the navigation bar on the left:

1. Choose **Device > Fault recording**.
2. A submenu appears in the upper-left area with three options:
   - **Fault recording**
   - **Grid waveform recording**
   - **RMS waveform recording**

Click the relevant submenu item to open the corresponding page, as described below.

Fault Recording

This page helps on-site personnel troubleshoot inverter faults.



Grid Waveform Recording

This page provides grid-compliant recording management and data exchange. Designed to meet State Grid, China Southern Power Grid, and international grid requirements for grid-connected equipment.

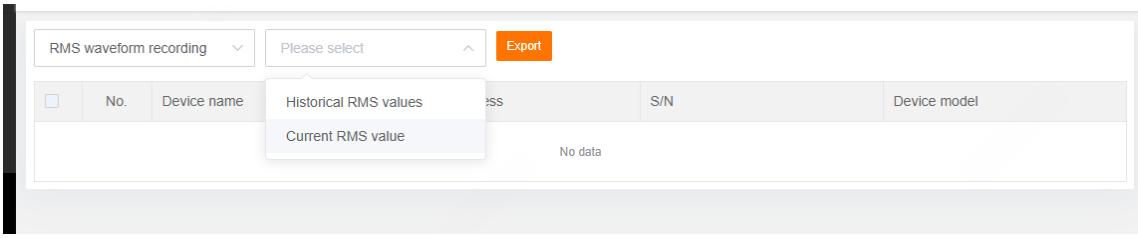
- **Submenu options**:

- **Full export**: Export complete recording files for detailed analysis.
- **Index export**: Export selected records by event index to streamline retrieval.
- **Export SER information**: Supports SER format for use by third-party systems.

RMS Waveform Recording

This page provides RMS event records for certain North American models.

- **Submenu options**:
  - **Historical RMS values**: Store long-term event records for trend analysis and review.
  - **Current RMS values**: Record the latest event data in real time for immediate monitoring and diagnostics.



7.6.5 Configuring Bluetooth Pairing for Inverter

The inverter's Bluetooth interface is provided solely for on-site commissioning and maintenance during installation.It is enabled by default for short-range local use and can be disabled for multiple inverters via the Data Logger before grid connection.In large utility plants where Bluetooth is not required, users are advised to disable the function to enhance.During inverter commissioning, a connection is established via Bluetooth to the offline SparkOps app, which is isolated from the public network. This Bluetooth feature is available for initial setup and debugging, typically during the power plant construction phase when LAN communication is unavailable. The Bluetooth function should be disabled immediately after the Logger establishes communication with the inverter. Any subsequent use requires manually re-enabling Bluetooth on the Logger.

Prerequisite

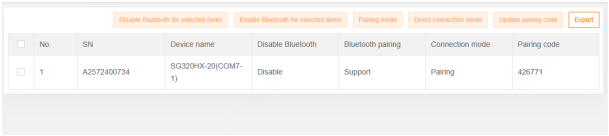
- The connected inverter supports local Bluetooth pairing and is now active within the short-range on-site network.Verify the connection details on the Bluetooth Pairing page.
- The firmware version of the Data Logger is P028 or later. See 7.8.11 Check Firmware Version for instructions on how to check the firmware version.
- Inverters produced after June 2024 are equipped with a dedicated Bluetooth pairing mode.

7.6.5.1 Enabling Bluetooth Pairing

The inverter supports the following two Bluetooth connection methods:

Bluetooth Mode	Description
Pairing Mode	The inverter can establish Bluetooth connections through the offline SparkOps APP only with devices authorized via a pairing code. This mode is suitable for scenarios that require additional protection and device authentication.
Direct Connection Mode	The inverter can establish direct Bluetooth connections with other devices without a pairing code; however, the connection must be established through the offline SparkOps APP. By default, the inverter operates in Direct Connection Mode.

Step 1 Navigate to **Device maintenance** > **Bluetooth pairing**.



The connected inverters will be displayed in a list on the screen, along with information on whether the inverter model supports Bluetooth pairing.

Step 2 Select the target inverters from the device list, and then click **Enable Bluetooth for selected items** in the upper right corner.

Step 3 Click **Pairing mode** in the upper right corner. Check that the selected inverters and the connection mode are correct and click **Confirm** in the pop-up dialog. The pairing code will then appear on the**Bluetooth pairing** page.

Step 4 Go to the Mobile App and complete Bluetooth pairing by following the onscreen instructions.

Step 5 (Optional) To manually update the pairing code, select the target inverter from the device list, and click **Update pairing code** in the upper right corner. Then, check that the inverter information is correct and click **Confirm** in the dialog.

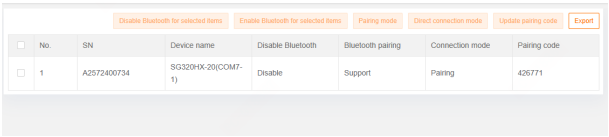
Pairing mode, **Direct connection mode**, and **Update pairing code** are available for use only if the inverter supports pairing code and its Bluetooth is enabled.

Step 6 (Optional) To export the inverters' Bluetooth pairing information, click **Export** in the upper right corner of the page.

--End

7.6.5.2 Disabling Bluetooth Pairing

Step 1 Navigate to **Device maintenance** > **Bluetooth pairing**..



The connected inverters will be displayed in a list on the screen, along with information on whether the inverter model supports Bluetooth pairing.

Step 2 Select the target inverters from the device list, and then click **Disable Bluetooth for selected items** in the upper right corner.

Step 3 Check that the information about the selected inverters is correct and click **Confirm** in the pop-up dialog. Then, the inverters' connection mode and pairing code will show "--" on the **Bluetooth pairing** page.

The connection mode and pairing code will show "--" if the inverter does not support Bluetooth pairing.

Step 4 (Optional) To export the inverters' Bluetooth pairing information, click **Export** in the upper right corner of the page.

--End

7.6.6 (Optional) Winding Temperature Detection

By collecting the apparent power of the inverter and the transformer oil temperature data in real time, the winding temperature detection function can calculate the transformer's winding temperature based on the rated transformer capacity and the winding and top oil temperature rise. It then uploads the real-time temperature data to the monitoring system, displays the alarm and trip information, and allows users to forward such information to the monitoring SCADA. Additionally, after setting the winding temperature alarm and trip parameters, O&M personnel can detect abnormal winding temperatures at an early stage, enhancing the efficiency of plant O&M.

Ensure the device is powered on and has a stable communication during detection. If the device loses power or if the detection time is less than 3 minutes, the data will be considered invalid.

The firmware version of Logger4000 should be P029 or later. See 7.8.11 Check Firmware Version for details. The function can be viewed only if **HV Side Winding Temperature Detection**, **LV Side Winding Temperature Detection**, or both are enabled on the Box-type Transformer Parameter Settings page.

7.6.6.1 Viewing Real-time Data

After completing the box-type transformer parameter and alarm parameter settings, users can check the real-time HV and LV winding temperatures and the alarm and trip information.

Real-time data can be viewed only if **HV Side Winding Temperature Detection**, **LV Side Winding Temperature Detection**, or both are enabled on the Box-type Transformer Parameter Settings page.

Table 7-5 Realtime Values

Parameter	Range	Description
HV Side Winding Temperature	Floating-point format, with an accuracy of 0.1. Unit: ℃.	A value will be shown only if **HV Side Winding Temperature Detection** is enabled. If the detection is disabled or if the detection duration is shorter than 3 minutes, the value shown will be "--".
HV Side Winding Temperature Alarm	Value: 0 or 1. "0" indicates no alarm, while "1" indicates an alarm due to the temperature exceeding the preset alarm threshold.	
HV Side Winding Temperature Trip	Value: 0 or 1. "0" indicates no tripping, while "1" indicates tripping due to the temperature exceeding the preset trip threshold.	
LV Side Winding Temperature	Floating-point format, with an accuracy of 0.1. Unit: ℃.	A value will be shown only if **LV Side Winding Temperature Detection** is enabled. If the detection is disabled or if the detection duration is shorter than 3 minutes, the value shown will be "--". This parameter is available only for the double-winding transformer.
LV Side Winding Temperature Alarm	Value: 0 or 1. "0" indicates no alarm, while "1" indicates an alarm due to the temperature exceeding the preset alarm threshold.	
LV Side Winding Temperature Trip	Value: 0 or 1. "0" indicates no tripping, while "1" indicates tripping due to the temperature exceeding the preset trip threshold.	
1# LV Side Winding Temperature	Floating-point format, with an accuracy of 0.1. Unit: ℃.	A value will be shown only if **1# LV Side Winding Temperature Detection** and **2# LV Side Winding Temperature Detection** are enabled. If the detections are disabled or if the detection duration is shorter than
1# LV Side Winding Temperature Alarm	Value: 0 or 1. "0" indicates no alarm, while "1" indicates an alarm due to the temperature	

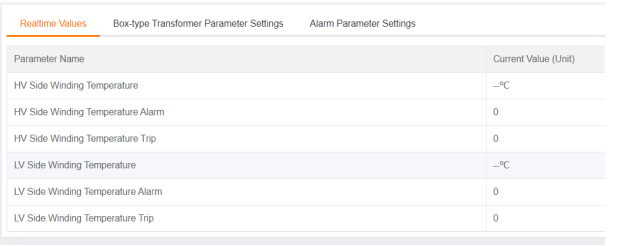
Parameter	Range	Description
	exceeding the preset alarm threshold.	
1# LV Side Winding Temperature Trip	Value: 0 or 1. "0" indicates no tripping, while "1" indicates tripping due to the temperature exceeding the preset trip threshold.	
2# LV Side Winding Temperature	Floating-point format, with an accuracy of 0.1. Unit: ℃.	3 minutes, the value shown will be "--". This parameter is available only for the double-split transformer.
2# LV Side Winding Temperature Alarm	Value: 0 or 1. "0" indicates no alarm, while "1" indicates an alarm due to the temperature exceeding the preset alarm threshold.	
2# LV Side Winding Temperature Trip	Value: 0 or 1. "0" indicates no tripping, while "1" indicates tripping due to the temperature exceeding the preset trip threshold.	

If the temperature reaches the alarm or trip threshold and the detection duration exceeds 3 minutes, the value of winding alarm or trip status in the "Real-time Values" will be "1".

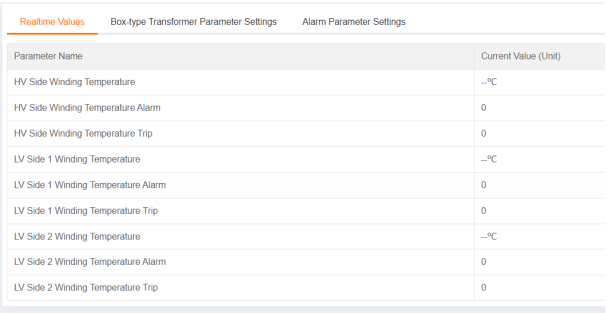
Step 1 Navigate to **Other Functions > Winding Temperature Detection**.

Step 2 Choose the **Real-time Values** tab to view the real-time data.

- **Double-winding Transformer**



- **Double-split Transformer**



Step 3 View the history winding temperature data. Navigate to **History Data > History Curve**. Then, click in the upper right corner to view the history winding temperature data.

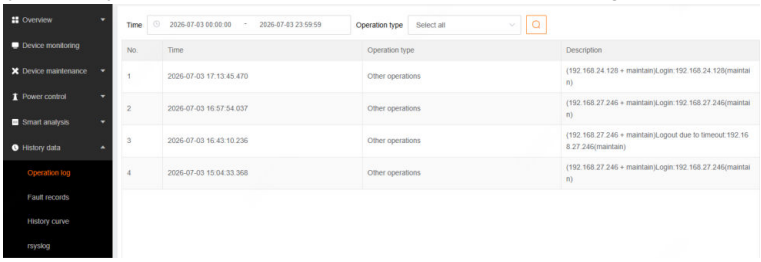
--End

7.7 History Data

7.7.1 Operation Log

Query Operation Log

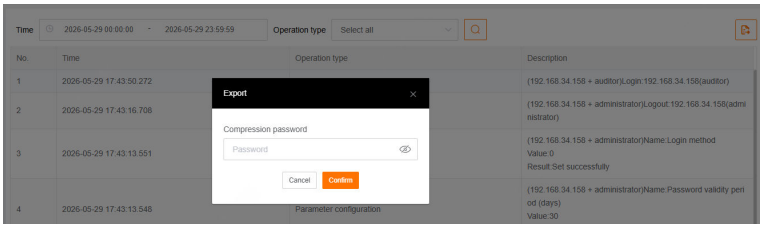
On the **History data** interface, click **Operation log**, select the desired time period and operation type, and you can view the user's operation records during that time.



- The system can store up to 10,000 operation log entries. When the storage space is full, the system automatically overwrites the oldest entries. Export the logs promptly if you need to retain them long term.
- Operation log timestamps are recorded in local time (with time zone information), with millisecond-level precision. The standard format is YYYY-MM-DD HH:MM:SS.sss (e.g., 2026-03-18 09:55:25.219).

Export Operation Log

Log in to the audit user account, and on the **History data** interface, click the **Operation log** icon, set the compression password, and then you can export the operation log.



The compression password should be 8 to 32 characters in length and contain at least three of the following four character types: uppercase letters, lowercase letters, numbers, and special characters.

7.7.2 Fault Records

You can check the device's fault information within a certain period of time by setting the search criteria.

Step 1 Click **History data** > **Fault records** to enter the corresponding page.

Step 2 Set the start and end time, and click to select the device name and fault type.

Step 3 Click to view the fault records in the set time period. The fault records mainly include the following information.

Table 7-6 Description of Parameters

Parameters	Description
Time	Time of fault.
Device Name	The faulty device.
Name	Detailed description of the fault.
Type	The corresponding type of this fault.
Status	Current status of the fault.

Step 4 Click to export the queried information to local for viewing.

--End

7.7.3 History Curve

On this interface users can view the data records of parameters of every device in the plant by selecting the device and the parameter.

Step 1 Click **History data** > **History curve** to enter the corresponding page.

Step 2 Click , select the device and parameter to be viewed, and set the start and end time.

Step 3 Click to view the history curve within the specified time period.

Users can select to view data records in a table or a chart. Click the icons in the following table to switch between display methods.

Table 7-7 Icon explanation

Icon	Description
	Switch to table form.
	Switch to curve form.

Step 4 Click to export the queried information to local for viewing.

--End

7.7.4 rsyslog

The system uses rsyslog to record security events such as abnormal network traffic. It also records expiration reminders for login and digital certificates, memory usage alarms, and log storage alarms. These records help you quickly identify abnormal activity during log audits and take steps to protect the device.

View rsyslog Log

Choose **History data** > **rsyslog**, and then click the **Log record** tab. Select a time range and filter by log level to view the rsyslog entries for that period.



- The system can store up to 11 rsyslog log files, with limits of 1 MB per file and 11 MB in total. When all log files are full and the file count reaches the limit, the system automatically overwrites the oldest log file. Export the logs promptly if you need to retain them for an extended period.
- The rsyslog timestamps are recorded in local time (including the time zone) with millisecond precision. The date and time are formatted as YYYY-MM-DD HH:MM:SS.sss (e.g., 2026-03-18 09:55:25.220).

Export rsyslog Log

Log in to the Web interface as an audit user. Choose **History data** > **rsyslog**, and then click . Set a compression password to export the rsyslog logs.



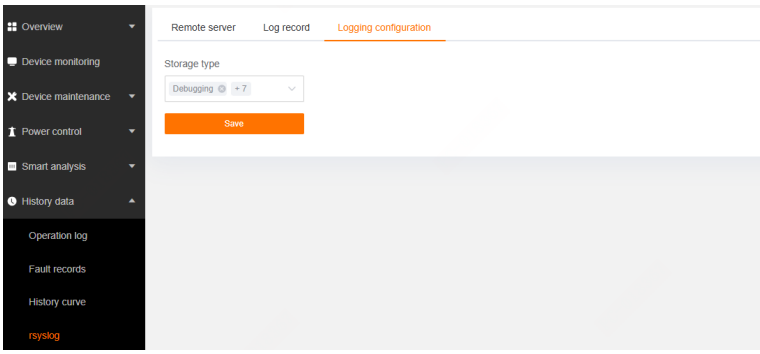
The compression password must contain 8–32 characters and include at least three of the following four character types: uppercase letters, lowercase letters, digits, and special characters.

Configure rsyslog Logging

Log in to the Web interface as an O&M user. Choose **History data** > **rsyslog,** and then select the **Log record settings** tab. In the **Storage type** drop-down list, select the levels of the logs you want to store. Click **Save**.

By default, the system records log entries at all severity levels. You can select specific severity levels from the following list:

- **Emergency**
- **Warning**
- **Critical**
- **Error**
- **Alarm**
- **Caution**
- **Notice**
- **Debugging**



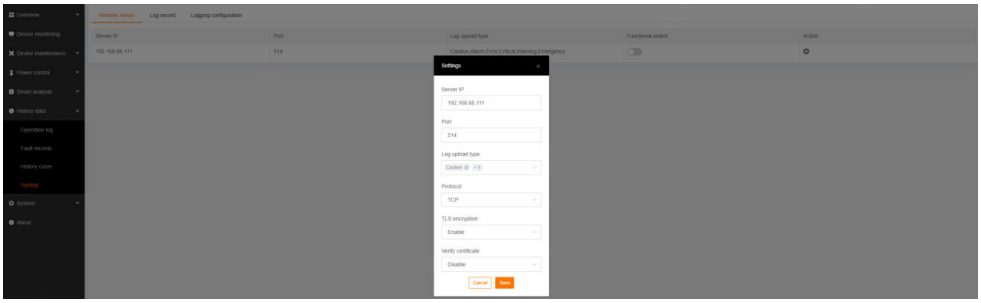
Configure Remote rsyslog Forwarding

Log in to the Web interface as an O&M user. Choose **History data** > **rsyslog**, and then select the **Remote server** tab. Click

, and then configure remote forwarding in the dialog box as follows:

- **Server IP**: Enter the remote server's IP address.
- **Port**: Enter the remote server's port number.
- **Log upload type**: All log severity levels are selected by default.
- **Protocol**: UDP and TCP are supported.
- **TLS encryption**: TLS encryption can be enabled when TCP is selected.
- **Verify certificate**: Certificate verification can be enabled when TCP is selected and TLS encryption is enabled.

Click **Save**.



On the **Remote server** tab, turn on the **Functional switch** to enable remote log forwarding.

7.8 System

7.8.1 Operating Information

- Click **System** > **Operating information** to enter the corresponding page.

  The following information can be viewed:

  - **General information**Check information like system time, IP address, MAC address, and mobile network.
  - **I/O information**
    Check information like AI voltage and current values, and DI status.
  - **Forwarding information**
    Check the current value of MODBUS-TCP and IEC104 parameters.

7.8.2 System Maintenance

7.8.2.1 Update System

Step 1 Choose **System** > **System maintenance** to open the page.

Step 2 Click **System update** and select an update package to perform the update.

- **iConfig update package**: Uses an update package downloaded through iConfig.
- **iSolarCloud update package**: Uses an update package available online in iSolarCloud.

--End

7.8.2.2 Log Export

Step 1 Click **System** > **System maintenance** to enter the corresponding page.

Step 2 Click **Log export** to enter the **Log export** page.

Step 3 Select the type of logs to be exported, and click **Confirm**.

--End

7.8.2.3 Restart

Step 1 Choose **System > System Maintenance**.

Step 2 Click **Rebooting**. In the warning dialog box, enter your current password to verify your identity again before restarting the system.

--End

7.8.2.4 One-Click Migration

Back up and export selected critical configuration files to your computer. You can also import local configuration files to restore the corresponding operating settings.

One-click migration supports importing and exporting data only between devices running the same version.

Step 1 Choose **System > System Maintenance**.

Step 2 Click **One-click Migration**. In the **One-click Migration** dialog box, select **Import** or **Export** as needed.

Table 7-8 Parameter Description

Parameter	Description
Export	Back up the system configuration files and save them locally. When exporting, set a password for the compressed file that meets the password requirements.
Import	Import local configuration files to the system. When importing, enter the same password used when the file was exported.

--End

7.8.2.5 Backup and Restoration

Click **System** > **System maintenance** > **Backup and restore**.

Backup

1. Click **Backup and restore** > **Back up**, and click the **Confirm** button to proceed.
2. Set a compression password and click **Confirm**. An encrypted archive will be generated locally.

The password should be 8–32 character long and contain at least three of the following four character types: uppercase letters, lowercase letters, numbers, and special characters.

Restoration

1. Click **Backup and restore** > **Restore**, and click the **Confirm** button to proceed.

2. Entering the compression password and click **Confirm**.
3. Select the encrypted backup archive to trigger a system restart and complete the restoration.

7.8.2.6 Attribute Management

Step 1 Click **System** > **System maintenance** to enter the corresponding page.

Step 2 Click **Attribute management**.

Step 3 In the pop-up dialog, select **Array mode**.

Table 7-9 Parameter description

Array Mode	Description
Conventional mode	The array is involved in dispatching.
Sample machine mode	The array is not involved in dispatching.

Step 4 Click Confirm.

--End

7.8.3 Remote Maintenance

Only the administrator account can configure the remote maintenance function.

Remote maintenance is disabled by default to ensure cybersecurity. Before enabling this function, the customer must be fully informed and manually authorize it using the administrator account. Access to the public network must use secure authentication and encryption. Remote access becomes available only after authorization using the administrator account. The system's access control policies govern remote access operations.

Step 1 Log in to the Web interface as an administrator. Click **Communication settings**, then click **iSolarCloud**.

Step 2 Turn on **Communication master switch** to enable communication with iSolarCloud.

Step 3 Turn on **Cloud-to-device**.

Step 4 Click **Remote maintenance** and enter the password of the currently logged-in account to reauthenticate. The **Remote maintenance** switch can be turned on only after successful reauthentication.

Step 5 Log in to the Web interface as an O&M user, then choose **System** > **Remote maintenance**.

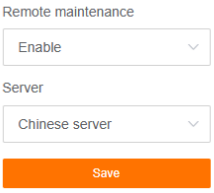


Table 7-10 Parameter Description

Remote Maintenance Switch Status	Description
Disable	Remote maintenance of the data logger is unavailable.
Enable	Remote maintenance of the data logger is available.

Step 6 If the iSolarCloud forwarding service is enabled, **Server** is bound to the iSolarCloud forwarding address. To update this value, please change the iSolarCloud site.

Step 7 Click **Save** to open the **Remote access** page.

Step 8 Enter the login password and click **Confirm**.

Step 9 Save the remote access information using either of the following methods:

- Click **Copy Remote Access Information** and then save the copied information locally.
- Enter an email address and click **Send** to send the remote access information to that address.

The system uses the email address solely to send the remote access information. You must sign in to the corresponding account to view the information. The email address is not stored on the device or the server, so there is no risk of disclosure of users' personal information.

Step 10 Enter the access link in the browser's address bar to open the **Remote maintenance** page. Enter the device's S/N and password, then click **Login** to perform remote maintenance.

--End

7.8.4 Export Messages

Step 1 Choose **System > Message Export**.

Parameter	Description
Type	-
Work Mode	• Master mode • Monitoring mode

Parameter	Description
	For example: When the device is connected to COM1, select COM1 in Master mode to capture messages directly from COM1. In Monitoring mode, select COM2 to capture messages from the COM1 bus through COM2, with the device connected to the RS485 port of COM1.
Port	-
Duration	Export message records for the configured duration

Step 2 After configuring the parameters, click **Start** to start recording messages. Recording stops automatically when the set duration expires, or click **Stop** to stop it manually.

Step 3 Click **Export** to export the messages.

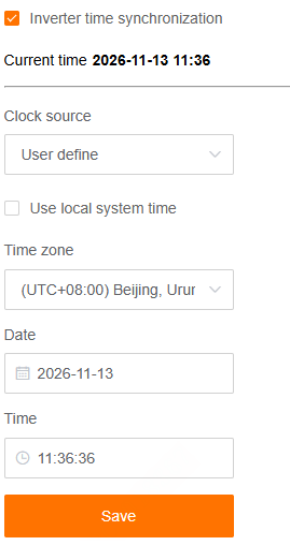
--End

7.8.5 System Time

Use this function to check and correct the system time and configure scheduled time synchronization with the inverters.

- Before enabling NTP, make sure the device is connected to a secure network.
- For time synchronization, **IEC104** is recommended first, followed by **iSolarCloud**. Other methods may be selected as needed.
- Only one clock source can be active at a time.

Step 1 Choose **System > System Time**.



Step 2 Select **Inverter Timing** to synchronize the data logger time to connected devices.

Step 3 Select the appropriate time source from the drop-down list.

Clock Source	Description
User Define	The current system time and time zone can be set in the following two ways: • Select **Use PC Time** to synchronize the data logger's clock with the local computer. • Select the local **Time Zone**, **Date**, and **Time**, then click **Save** to set the data logger's time manually. **User Define** is recommended during commissioning.
NTP/NTS	Synchronizes the clocks of devices on the network. Select the local **Time Zone**. Enter **Server**, configure **Time Interval**, and click **Save**. The data logger synchronizes its clock with the server.
IEC104	This method works only if the data logger communicates with the backend system using IEC 104; otherwise, time synchronization with the clock source set to "**IEC104**" will not work.
iSolarCloud	This method works only if the data logger is connected to iSolarCloud; otherwise, time synchronization with the clock source set to "**iSolarCloud**" will not work.
Modbus-TCP	This method works only if the data logger communicates with the backend system using Modbus TCP; otherwise, time synchronization with the clock source set to "**Modbus-TCP**" will not work.

Clock Source	Description
B Code	Synchronizes time using the IRIG-B time-code protocol.
PTP	Synchronize the clocks of multiple data loggers in the plant through a backend time server.

--End

NOTICE

Set the system time before using the data logger for the first time.

7.8.6 Forwarding Configuration

7.8.6.1 Configure iSolarCloud Forwarding Service

- Data forwarding is disabled by default on the data logger. Before enabling this function, customers must provide informed authorization and use secure, encrypted authentication when connecting to public networks. Remote access requires customer authorization and is subject to the system access control policies.
- iSolarCloud services have been discontinued in North America.

Cloud services exchange data over the public network. Ensure the device network environment is secure before enabling the function.

Step 1 Choose **System > Transfer Configuration**.

Step 2 Enable the site connection switch, then click in the Action column to edit iSolarCloud forwarding settings.

The default iSolarCloud site is "**Chinese Server**". Connect to **Chinese Server** in mainland China, **European Server** in Europe, **Australian Server** in Australia, **India site** in India, and **International Server** in other regions.
Configure the router whitelist to ensure proper operation of the data logger. For the settings, refer to Router whitelist settings.

--End

7.8.6.2 Configure IEC 104 Forwarding Service

Use this function to configure IEC 104 forwarding on the data logger.

- This protocol is not secure and may pose risks. Make sure the device is on a secure network before enabling it.
- Enable TLS encryption as needed to enhance information security.

Server mode

In Server mode, the data logger acts as a server, and the host computer connects to it to exchange data and commands.

Set the local port number to 2418 when configuring IEC 104 forwarding.

7.8.6.2.1 Whitelist Settings

Choose **System > Transfer Configuration > IEC104** to open the **Server** page, then click **Whitelist settings**.

- If **Enable White List** is not selected and the IP address remains at its default value of 0.0.0.0, any backend device with a valid IP address can access the data logger.
- Select **Enable White List** and enter an IP address to allow access only from the specified device.

7.8.6.2.2 Generate Point List

Step 1 Turn on the switch of local port 2404.

Step 2 Click **Generate point list**, and the default IEC104 point table will be automatically imported to the configuration file.

--End

7.8.6.2.3 Import IEC104 Forwarding Point Table

Step 1 Click to open the **Advanced settings** pop-up window.

Step 2 Click to import the .zip file.

Step 3 Click **Save**.

--End

7.8.6.2.4 Export IEC 104 Forwarding Point Table

Step 1 Choose **System > Transfer Configuration > IEC104**. The **Server** page appears by default.

Step 2 Click **Export point table** to export the forwarding point table as a CSV file to your computer.

--End

7.8.6.2.5 Set IEC 104 Dispatch Mode

Step 1 Choose **Device monitoring**.

Step 2 Select an inverter from the list on the left, then choose **Power regulation parameters** to configure its power regulation settings.

Step 3 In the **Fast grid dispatch mode** drop-down list, do one of the following:

- Select **Enable** to enable IEC 104 fast dispatch.
- Select **Disable** to disable IEC 104 fast dispatch.

Step 4 In the **Ultra-fast grid dispatch mode** drop-down list, do one of the following:

- Select **Enable** to enable IEC 104 ultra-fast dispatch.
- Select **Disable** to disable IEC 104 ultra-fast dispatch.

If **Fast grid dispatch mode** and **Ultra-fast grid dispatch mode** are both enabled, **Ultra-fast grid dispatch mode** takes priority for active and reactive power regulation.

Step 5 Click **Set** to save the settings.

Step 6 Click the **General parameters** tab to configure device parameters.

Step 7 Select **Set** and configure **Register address**, **Data type**, and **Set value**. Click **Set** to apply the changes to the selected inverter.

Step 8 (Optional) Click **Configuration synchronization**, select the devices in the pop-up list, and click **Save** to apply the settings in a batch.

--End

7.8.6.3 MODBUS

Configure the MODBUS forwarding service for the Data Logger on this page.

- Before enabling this switch, ensure the device is connected to a trusted management network.
- Enable TLS encryption as needed to enhance information security.

7.8.6.3.1 Server Mode

In Sever mode, Logger4000 functions as a sever. Through Modbus TCP protocol, the host computer server is connected to Logger4000 for data and instruction transmission.

Step 1 Click **System** > **Forwarding configuration** > **MODBUS** to enter the "**Sever**" interface by default.

Step 2 Set white list referring to 7.8.6.2 Configure IEC 104 Forwarding Service.

--End

7.8.6.3.2 RTU Mode

n the RTU mode, Logger4000 is connected to PC server through Modbus RTU protocol to implement data transmission and instruction delivery.

Step 1 Click **System** > **Forwarding configuration** > **MODBUS** to enter the "**Sever**" interface by default.

Step 2 Click "**RTU**" to enter the corresponding tab.

Step 3 Select serial port and enter delay time.

Step 4 Click  .

--End

7.8.6.3.3 Modbus TCP Fast Dispatch

Enabling Modbus TCP Fast Dispatch can enhance the responsiveness of power control.

Prerequisite

- When employing Modbus-TCP fast dispatch, an Ethernet switch is set up between the SCADA and the Logger4000's ETH3 or ETH4 rapid control ports, connected using standard Ethernet cables. A standard CAT5E/75cm Ethernet cable will suffice.
- Only configure the IP address for one of the fast dispatch ports (either ETH3 or ETH4), ensuring it is within the same subnet as the SCADA IP wherever possible.

- Firmware version of Logger4000: P019 or above. See 7.8.11 Check Firmware Version.
- Modbus TCP Fast Dispatch and GOOSE forwarding service cannot be enabled at the same time.
- Modbus TCP only supports open-loop control.

After enabling the Modbus TCP fast dispatch, ensure the interval between two consecutive dispatch commands meets the following requirements. Otherwise, the inverter might not fully respond to the target values.

- Active power control: The interval should be at least 60 milliseconds.
- Reactive power control: The interval should be at least 30 milliseconds.

Step 1 Click **System** > **Forwarding configuration** > **MODBUS** to enter the "**Sever**" interface by default.

Step 2 Click **Modbus TCP fast dispatch**.

Step 3 In the drop-down list **Switch**, select **Enable**.

Step 4 In the drop-down list **Port**, select the port number of the SCADA.

Step 5 Based on the actual situation of the power station, configure the network parameters for the fast dispatch ports ETH3 and ETH4.

Step 6 To enable **Northbound communication anomaly protection**, under the field **Protection switch**, select **Enable**.

a. In the field **Peer IP address**, enter the IP address of the control device.

b. In the field **Communication anomaly trigger delay**, specify the time to pause before the Data Logger performs protection operations on the inverter.
For example, setting the **Communication anomaly trigger delay** to "30" means the Data Logger will wait 30 seconds before limiting the inverter's output power.

c. In the field **Communication anomaly output**, specify the inverter's output power as a percentage when a communication fault is detected.

For example, setting the **Communication anomaly output** to "80" means the Data Logger of will limit the inverter's output power to 80% of its rated power during a communication fault.

d. In the field **Communication anomaly auto recovery time**, specify the waiting time of the Data Logger after the communication resumes.

After this time period, the Data Logger will adjust the inverter's output power or restart the inverter based on the **Output after communication recovery** settings.

e. In the drop-down list **Output after communication recovery**, specify the action the Data Logger should take when the communication resumes.

- **No action**: The Data Logger adjusts the inverter's output power based on the last target value issued by the SCADA.
- **Start up**: The Data Logger first issues a power-on command to the inverter, then adjusts the output power based on the last target value issued by the SCADA. This is suitable when the inverter was shut down due to a communication fault.

For example, setting the **Communication anomaly auto recovery time** to "30" and the **Output after communication recovery** to **No action** means the Data Logger will wait 30 seconds after communication is restored before resuming output power.

Step 7 Click **Save**.

The Web UI will prompt you that the changes will take effect after a restart.

--End

7.8.6.3.4 Modbus TCP Normal Dispatch Mode

Step 1 Choose **Device monitoring**.

Step 2 Select an inverter on the left and click **Power regulation parameters** to configure its power regulation settings.

Step 3 In the **Fast grid dispatch mode** drop-down list, do one of the following:

- Select **Enable** to enable Modbus TCP fast dispatch.
- Select **Disable** to disable Modbus TCP fast dispatch.

Step 4 In the **Ultra-fast grid dispatch mode** drop-down list, do one of the following:

- Select **Enable** to enable Modbus TCP ultra-fast dispatch.
- Select **Disable** to disable Modbus TCP ultra-fast dispatch.

If **Fast grid dispatch mode** and **Ultra-fast grid dispatch mode** are both enabled, **Ultra-fast grid dispatch mode** takes priority for active and reactive power regulation.

Step 5 Click **Set**.

Step 6 Click the **General parameters** tab to configure device parameters.

Step 7 Select **Set** and configure **Register address**, **Data type**, and **Set value**. Click **Set** to apply the changes to the selected inverter.

Step 8 (Optional) Click **Configuration synchronization**, select the devices in the pop-up list, and click **Save** to apply the settings in a batch.

--End

7.8.6.4 Configure Third-Party Cloud Forwarding Service

The Forwarding Third-Party Cloud Service Configuration function configures the data logger to forward data to third-party cloud services.

1. Cloud services exchange data over the public network. Ensure the device network environment is secure before enabling this function.
2. Third-party cloud forwarding is disabled by default. Before enabling this function, the customer must knowingly authorize it manually using an administrator account and connect to the public network through secure encrypted authentication. This function takes effect only after administrator authorization, and all related operations are subject to system access controls.

Step 1 Log in with an O&M account and choose **System > Transfer Configuration > Third-party Portal** to open the **Third-party Portal** page.

Step 2 Turn on the switch.

Step 3 Click ⚙ to open the **Advanced Settings** window.

Step 4 Edit the settings and click **Save**.

Use the format /FTP server directory for the FTP path.
For example, in /SUNGROW, / denotes the root directory and SUNGROW is the directory used to store data on the FTP server.

--End

7.8.6.5 Configure GOOSE Forwarding Service

Configure GOOSE forwarding on the data logger.

Prerequisite

- When using GOOSE fast dispatch, connect a switch between the backend system and the data logger's ETH3 or ETH4 fast dispatch port using Ethernet cables. Use a standard Ethernet cable, such as a 75 cm Cat 5e cable.
- Configure the IP address of either ETH3 or ETH4; preferably use the same subnet as the backend system.

This protocol is not secure and may pose risks. Make sure the device is on a secure network before enabling it.

After GOOSE forwarding is enabled, ensure that backend dispatch commands meet the following minimum intervals. Otherwise, the inverters may not fully respond to the setpoints.

- Active power regulation: Dispatch interval: at least 60 ms.
- Reactive power regulation: Dispatch interval: at least 30 ms.

Step 1 Choose **System > Transfer Configuration > GOOSE** to open the **GOOSE** page.

Step 2 Set **Switch** to **Enable**.

Step 3 Click **Configuration File Export** to export the GOOSE configuration file locally.

Step 4 Extract the exported archive, then open the .cfg file in Excel to review or edit the GOOSE configuration.

Step 5 Save the updated GOOSE data configuration file.

Step 6 Click **Configuration File Import**, select the saved GOOSE configuration file, then click Open to import it.

--End

Enable **Anti-replay** as needed to reduce the risk of replay attacks and configure the detection interval.

7.8.6.6 Setting MMS Forwarding Service

Configure MMS forwarding service for the data logger.

- This function is available on LOGGERSV400.001.00.P031 or later.

Step 1 Choose **System** > **Forwarding configuration** > **MMS**.

Step 2 Select **Enable** from the **Switch** drop-down list. The switch is disabled by default.

Step 3 Click **Configuration file import** to import a .zip configuration file.

Step 4 The import will take effect after a restart. Click **Confirm**.

Click **Configuration file**.

Step 5 (Optional) Click **Configuration file export** to export the imported and effective configuration file to your local system.

--End

7.8.7 Port Parameter

Configure serial ports of the Data Logger.

7.8.7.1 RS485

Step 1 Click **System** > **Port parameter** > **RS485** to enter the **RS485** page.

Step 2 Click ⚙ to modify **Baud rate**, **Parity bit**, **Stop bit**, and **PLC access**. The default value of each parameter are as follows.

Parameter	Default value
Port function	**Collection**
Baud rate	9600

Parameter	Default value
Parity bit	None
Stop bit	1
PLC access	**Disable**
Fast dispatch switch	**Disable**

When the Data Logger is connected to a device via the serial port, the settings of **Baud rate**, **Parity bit**, and **Stop bit** of the serial port should match those set for the connected device, to ensure normal communication.

Only when COM1 to COM7 ports are connected to the device can the **PLC access** status corresponding to COM1 to COM7 ports be set to **Enable**. After setting the enable, the baud rate for COM1 to COM7 ports will be automatically modified to 115200. At this time, you can configure the PLC node parameters. For details, see 7.8.8 MPLC (Broadband PLC).

--End

7.8.7.2 Ethernet

Step 1 Click **System** > **Port parameter** > **Ethernet** to enter the **Ethernet** page.

Step 2 If **Auto IP assignment** is set to **On**, the IP address corresponding to the port is invalid. Log in the device through the virtual IP address.

Port	Default IP address	Subnet mask	Gateway	DNS1	DNS2
ETH1	12.12.12.12	255.255.255.0	12.12.12.1	1.2.4.8	8.8.8.8
ETH2	13.13.13.13	255.255.255.0	13.13.13.1	1.2.4.8	8.8.8.8
ETH5	14.14.14.14	255.255.255.0	14.14.14.1	1.2.4.8	8.8.8.8

Step 3 If the parameter **Auto IP assignment** is set to **Off**, fill in the information such as the **IP address**, **Subnet mask**, and **Gateway address**, and click to save the operation.

--End

7.8.7.3 Analog Input (AI)

Step 1 Click **System** > **Port parameter** > **Analog input** to enter the **Analog input** page.

Step 2 Select **Input type**, set **Lower limit** and **Upper limit**, and click to save the operation.

AI Port	Input type	Lower limit	Upper limit
Analog input 1	**Voltage**(V)	0	10
Analog input 2	**Current**(mA)	4	20
Analog input 3	**Current**(mA)	4	20
Analog input 4	**Current**(mA)	4	20
PT1	-	-30	160
PT2	-	-30	160

For Logger4000 with firmware version higher than P028, the upper limit temperature for PT100 is increased from 120°C to 160°C.

Step 3 If there is an external IO device connected to the Data Logger, click **External** to set the AI parameters of this device.

--End

7.8.7.4 Digital Input(DI)

Step 1 Click **System** > **Port parameter** > **Digital input** to enter the **Built-in** page.

Step 2 Set **Initial status** to **NO** or **NC**. Click to apply the changes.

Step 3 If there is an external IO device connected to the Data Logger, click **External** to set the DI parameters of this device.

--End

7.8.7.5 Digital Output (DO)

Step 1 Click **System** > **Port parameter** > **Digital output** to enter the **Built-in** page.

Step 2 Set **Initial status** to **NO** or **NC**, and click to set **Function**, **Action mode**, and **Pulse duration**. Click to save the settings.

Selecting **Communication control** under **Function** enables the SCADA and the Data Logger to send commands to the port, while selecting **Manual control** allows commands to be sent to the port manually.

Step 3 If there is an external IO device connected to the Data Logger, click **External** to set the DO parameters of this device.

--End

7.8.8 MPLC (Broadband PLC)

Step 1 In the navigation bar, choose **System > MPLC**.

The **MPLC** tab appears by default on the Web interface.

Step 2 Locate the PLC to configure and click in the Action column to open the **PLC settings** dialog box.

Step 3 Configure the master node.

a. Select a communication frequency band from the **Band Num** drop-down list. By default, the communication frequency band is **Band1**.

If communication on Band1 is poor, switch to **Band2** or **Band3**.

b. In **Array ID**, set the current array ID.

The ID of each array on site must be different.

For a split-winding system, assign different array IDs to the two PLC modules connected to the same data logger.

Keep the default values of the parameters in **Advanced Settings** unless a change is necessary.

Step 4 Click **Next**.

Step 5 Configure the PLC slave node.

a. Select the device.

b. Click **Synchronization** to synchronize master node parameters to the slave node.

Step 6 After synchronization is complete, click **Logout** to finish configuring the parameters of the master and slave nodes.

The PLC master and slave nodes will automatically restart to apply the changes.

Step 7 Click the **Action** tab to either upgrade the PLC master node or export the PLC operation logs.

--End

7.8.8.1 MPLC Auto Frequency Hopping

If communication between the Data Logger and inverter fails (e.g., the port enabled PLC has a packet loss rate exceeding 0.5% or some inverters frequently go offline), you can enable the automatic frequency hopping feature to improve reliability.

Prerequisite

- Firmware version of the Data Logger: P025 or above. See 7.8.11 Check Firmware Version.

To check the packet loss rate, navigate to the page **System** > **Operating information**.

Step 1 Click **System > MPLC > Action** to navigate to the corresponding page.

Step 2 Click **MPLC auto frequency hopping**.

Step 3 In the pop-up dialog, select the MPLC link that requires automatic frequency hopping.

Step 4 Click **Confirm**.
In the dialog box that appears, select the MPLC links that require auto-frequency hopping. Progress will be shown, and completion is indicated by the progress bar reaching 100%.

--End

7.8.8.2 One-Click MPLC Diagnosis

When there is a communication abnormality between the data collector and the inverter, you can use the one-click diagnosis feature to view possible fault causes and repair suggestions.

Prerequisite

- Firmware version of the Data Logger: P025 or above. See 7.8.11 Check Firmware Version.

Step 1 Click **System > MPLC > Action** to navigate to the corresponding page.

Step 2 Click **One-click MPLC diagnosis**.
Progress and results of diagnostics will be displayed in the dialog box.

Step 3 Follow on-screen instructions to address any identified faults.

Step 4 Click **Export** to save the diagnostic results locally.

--End

7.8.9 Certificate management

Navigate to the **System > Certificate management** tab to import a certificate.

- The default PKI-issued certificate is factory-installed. It is recommended to import the customer's signing certificate.
- If the NTS function is used, customers must import the NTS server certificate. This certificate can be obtained from the NTS server and supports X.509 certificate import in PEM format.
- In the absence of imported third-party certificates, the server-side HTTPS, IEC104, and MODBUS certificates use the default forwarding certificate.
- Updating or deleting an HTTPS certificate requires re-establishing the connection. If the webpage cannot be opened normally, please restart the browser.

7.8.9.1 Collection

On the **Certificate management** page, select **Collection** and click **Add**. Enter the certificate name and click **Confirm**.

The certificate name must be 2–16 characters long, contain only letters and digits, and start with a letter.

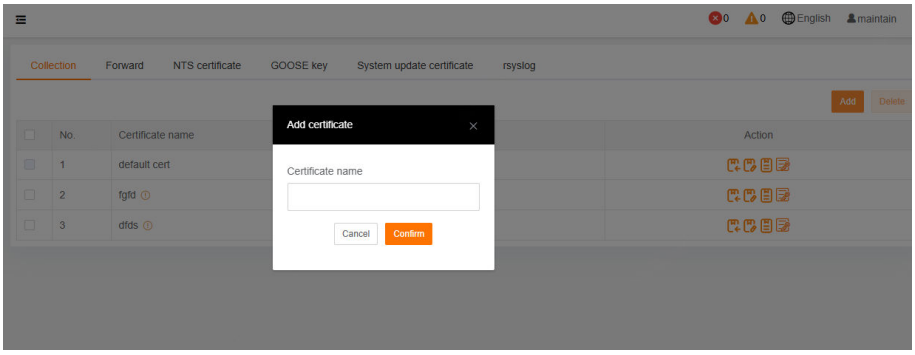


Figure 7-2 Add Certificate

In the row for the newly added certificate, click in the Action column. Set the **File type** to **Certificate**. Specify the certificate type and format, upload the certificate file, and click **Save**.

- Certificate type: Certificate chain, intermediate certificate and root certificate are supported.
- Certificate format: If **Certificate type** is set to **Certificate chain**, .pem and .p12 files are supported. If it is set to **Intermediate certificate** or **Root certificate**, only .pem files are supported.
- A decryption password is required when **Certificate type** is set to **Certificate chain** and **Certificate format** is set to **p12 format**.

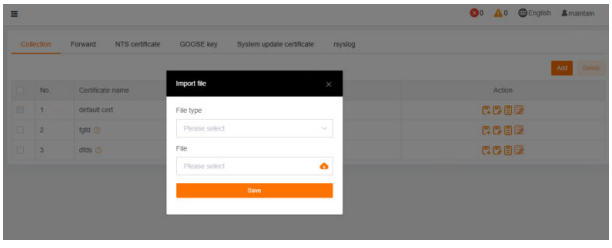


Figure 7-3 Import Certificate

7.8.9.2 Forward

Import HTTPS certificates on this page.

On the **Certificate management** page, select **Forward** and click **Add**. Enter the certificate name, specify the protocol and port, and click **Confirm**.

The certificate name must be 2–16 characters long, contain only letters and digits, and start with a letter.

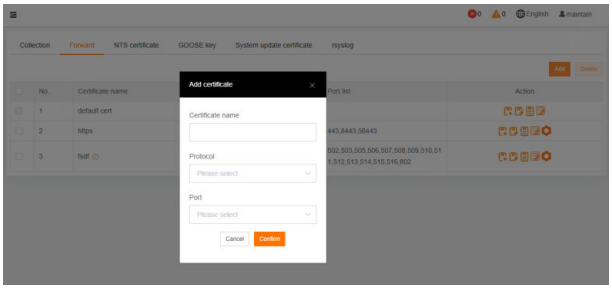


Figure 7-4 Add Certificate

In the row for the newly added certificate, click in the Action column. Set the **File type** to **Certificate**. Specify the certificate type and format, upload the certificate file, and click **Save**.

- Certificate type: Certificate chain, intermediate certificate and root certificate are supported.
- Certificate format: If **Certificate type** is set to **Certificate chain**, .pem and .p12 files are supported. If it is set to **Intermediate certificate** or **Root certificate**, only .pem files are supported.
- A decryption password is required when **Certificate type** is set to **Certificate chain** and **Certificate format** is set to **p12 format**.

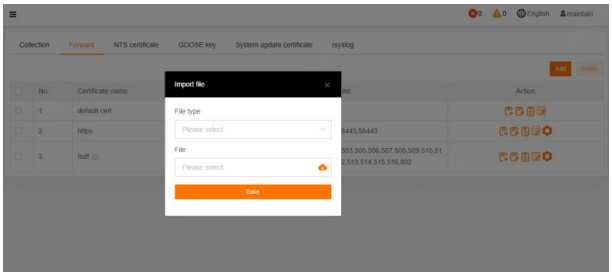
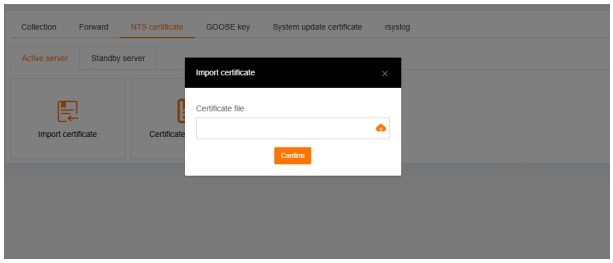


Figure 7-5 Import Certificate

7.8.9.3 Import NTS Active Server Certificate

On the **Certificate management** page, click **NTS certificate**.

On the active or standby server page, click **Import certificate** to import the NTS server certificate.



7.8.9.4 GOOSE Security Functions

GOOSE supports functions such as anti-replay and key update.

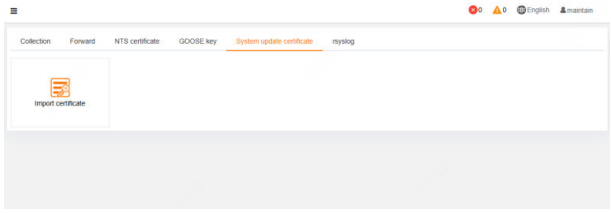
Anti-replay: Navigate to the **System > Forwarding configuration** page, choose the **GOOSE** tab, then enable the anti-replay switch. Users can set anti-replay detection time as needed.

Key update: Navigate to the **System > Certificate management** page, choose the **GOOSE key** tab, click Import key, and upload the key file.

7.8.9.5 System Update Certificate

To ensure secure system updates, digital signatures are used to verify the authenticity and integrity of update packages. When updating the data logger, you may need to import the certificate associated with the update package to complete digital signature verification.

On the **Certificate management** page, select **System update certificate** and click **Import certificate** to import the system update certificate.



7.8.9.6 rsyslog Certificate Management

On the **Certificate management** page, select **rsyslog** and click **Add**. Enter the certificate name and click **Confirm**.

Up to 2 rsyslog certificates can be configured: 1 system default certificate and 1 additional third-party certificate.

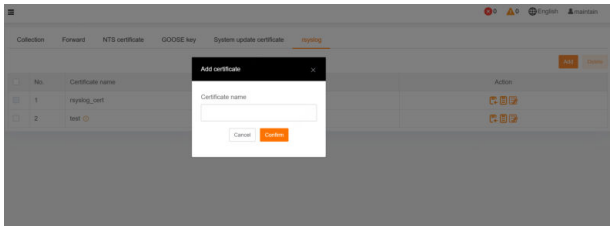


Figure 7-6 Add Certificate

In the row for the newly added certificate, click in the Action column. Set the file type to certificate. Specify the certificate type and format, upload the certificate file, and click **Save**.

- **File type**: Certificate and certificate revocation lists are supported.
- **Certificate type**: Intermediate and root certificates are supported.
- **Certificate format**: Only pem is supported.

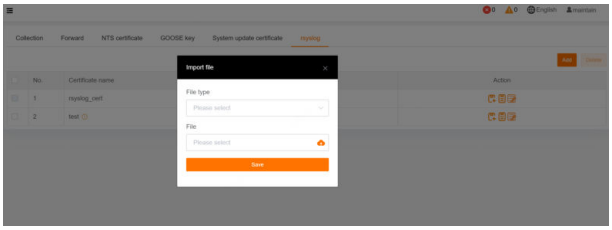


Figure 7-7 Import Certificate

7.8.9.7 View Certificate Information

Prerequisite

Log in to the Web interface as an O&M user.

Step 1 In the navigation bar, click **Certificate management**. On the page that opens, look under **Collection**, **Forward**, or **rsyslog** for the certificate you want to view.

Step 2 In the Action column for the certificate, click to open the certificate information dialog box.

- For certificates under **Collection** or **Forward**, the certificate information dialog box displays the following details: serial number, common name, encryption algorithm, signature algorithm, revocation status, and validity period.
- For intermediate and root certificates under **Collection**, **Forward**, or **rsyslog**, the certificate information dialog box displays the serial number, common name, encryption algorithm, signature algorithm, revocation status, and validity period.
- For certificates under **Collection** or **Forward**, choose **More** in the Action column of the certificate information dialog box. You can view details about the selected certificate or download it.
- For intermediate and root certificates under **Collection**, **Forward**, or **rsyslog**, choose **More** in the Action column of the certificate information dialog box. You can view details about the selected certificate, or disable, delete, or download the certificate.

--End

7.8.9.8 Import Certificate Revocation List

A certificate revocation list (CRL) is a digital file periodically issued by a certification authority (CA). It lists the serial numbers and revocation information of digital certificates revoked before

they expire for reasons such as private key compromise, changes to identity information, or certificate misissuance.

Prerequisite

Log in to the Web interface as an O&M user.

Step 1 In the navigation bar, click **Certificate management**. On the page that opens, look under **Collection**, **Forward**, or **rsyslog** for the certificate for which you want to import a revocation list.

Step 2 In the Action column for the selected certificate, click to open the **Import file** dialog box.

a. In the **File type** drop-down list, select Certificate revocation list.

b. In the **Revocation list type** drop-down list, select Leaf certificate revocation list or Intermediate certificate revocation list.

c. In the **Revocation list format** drop-down list, select crl format.

d. Click the File field and select the certificate revocation list file to upload.

- The uploaded file must be in CRL format.
- The file name can contain only digits, letters, half-width underscores (_), and half-width hyphens (-).

e. Click **Save** to complete the import.

--End

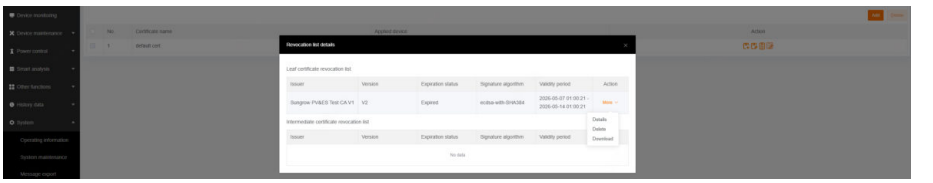
7.8.9.9 View Certificate Revocation List

Prerequisite

Log in to the Web interface as an O&M user.

Step 1 In the navigation bar, click **Certificate management**. On the page that opens, look under **Collection**, **Forward**, or **rsyslog** for the certificate for which you want to view a revocation list.

Step 2 In the Action column for the certificate, click to open the **Revocation list details** dialog box. You can view the issuer, version, expiration status, signature algorithm, and validity period for the **Leaf certificate revocation list** and **Intermediate certificate revocation list**.



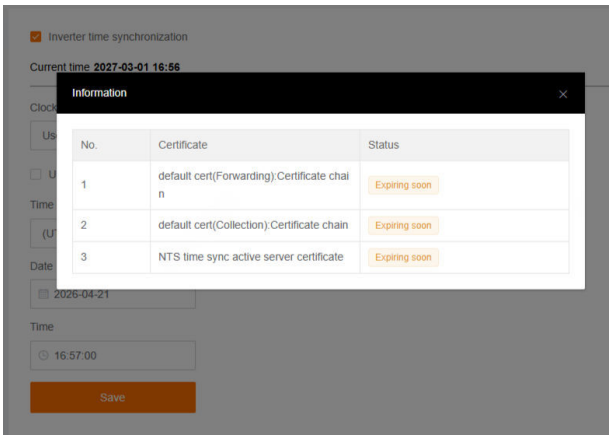
Step 3 In the **Action** column for the selected certificate revocation list, click **More** . You can then view its details or delete or download the list.

--End

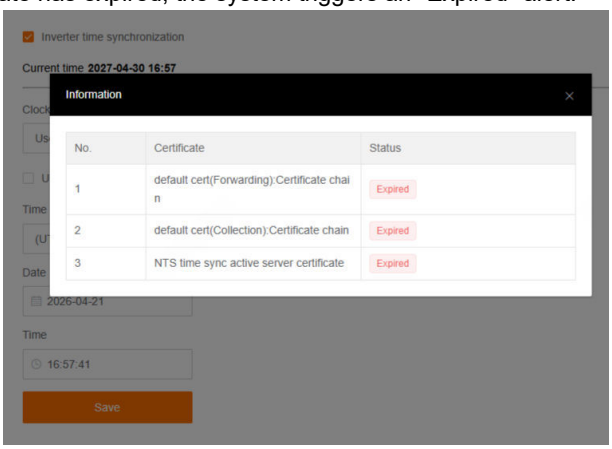
7.8.9.10 Certificate Expiration Management

After successful user login, if the certificate is about to expire or has expired, the system will display a prompt and log the result to the rsyslog log.

When the certificate is less than 90 days from expiration, the system triggers an "Expiring soon" alarm.



When the certificate has expired, the system triggers an "Expired" alert.



7.8.10 More

Step 1 Choose **System** > **More**, and then select the **Basic functions** tab.

Step 2 In the **Set islanded inverter to offline** drop-down list, select **Enable** or **Disable**.

- **Enable**: If Logger4000 communicates with an inverter via power line communication (PLC) and the inverter is islanded, Logger4000 sets the inverter's communication status to offline.
- **Disable**: Logger4000 does not set the inverter's communication status to offline based on its islanding status.

Logger4000 must run firmware version P028 or later. Refer to7.8.11 Check Firmware Version for details.

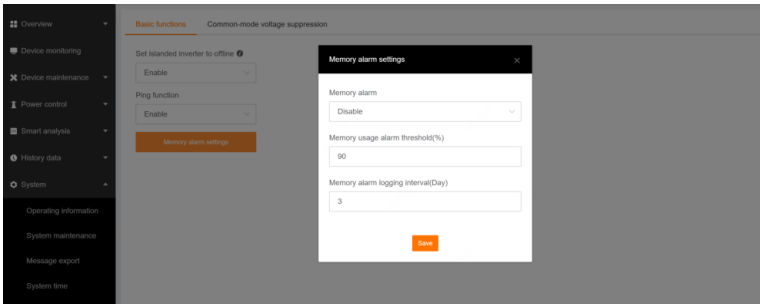
Step 3 In the **Ping function** drop-down list, select **Enable** or **Disable** as needed.

- By default, the **Ping function** is disabled to block probes from external devices and reduce attack risk. Depending on your network environment, you can enable this function manually.
- **Enable**: The device responds to ping requests. You can ping the device's IP address to check network connectivity.
- **Disable**: The device does not respond to ping requests.

This function uses an insecure protocol, which poses security risks. Ensure that the device's network environment is secure before enabling the function.

Step 4 Configure the memory alarm parameters as needed:

a. Click **Memory alarm settings**. The **Memory alarm settings** dialog box opens.



b. In the **Memory alarm** drop-down list, select **Enable** or **Disable**.

c. In the **Memory usage alarm threshold** input box, enter the memory usage alert threshold.

The default memory usage alarm threshold is 90%, with an allowed range of 85%–95%.

d. In the **Memory alarm logging interval** field, enter the interval for recording memory alarms via rsyslog.

- When memory usage exceeds the configured alarm threshold, the system records a memory alarm via rsyslog once per configured logging interval.
- The default memory alarm logging interval is 3 days, with an allowed range of 1–7 days.

e. Click **Save**.

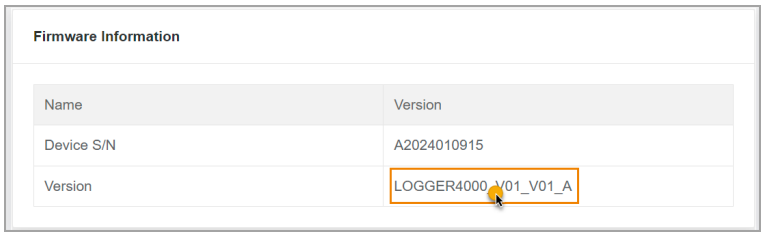
--End

7.8.11 Check Firmware Version

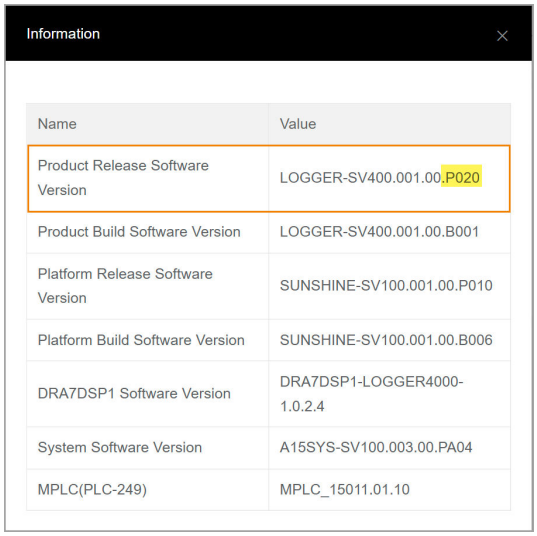
View the data logger's firmware information.

Step 1 Choose **About** from the navigation bar.

Step 2 Click the field corresponding to **Version** five times to view the data logger version information.



The data logger firmware version is indicated by Product Release Software Version, in the following format: "LOGGER-SV400.001.00.P[XXX]". The P[XXX] portion identifies the specific firmware version.



--End

8 Firmware Upgrade

Firmware updates provide critical security enhancements and performance optimizations, serving as essential measures to ensure stable, secure, and efficient device operation. Timely firmware updates can fix security vulnerabilities and performance issues, thereby reducing system faults and lowering maintenance costs. You can upgrade SUNGROW inverters, data loggers, and PLC nodes through the Web interface.

Upgrade Method	Description
Upgrade using the iConfig configuration tool*	The Web interface checks whether iConfig is installed on a computer in the same local area network as the data logger. If iConfig is installed and a compatible upgrade package has been downloaded, the Web interface displays the package.
Update via iSolarCloud	The Web interface displays available online upgrade packages for the current device from iSolarCloud.

*Upgrading through iConfig is not supported when accessing the data logger through Remote maintenance.

For the iConfig installation package and instructions, contact SUNGROW Customer Service.

8.1 Updating SUNGROW Inverters or the Slave Node of PLC

Prerequisite

Prepare the necessary files or configurations based on your chosen update method:

- Update via iConfig: The iConfig tool is installed, and the relevant update package is downloaded.
- Update via iSolarCloud: The connection between the Data Logger and iSolarCloud is established, and there is available update package. See 7.8.6.1 Configure iSolarCloud Forwarding Service.

The update process cannot be interrupted once it has begun.

Step 1 Click **Device maintenance** > **Firmware update** to navigate to the corresponding page.

Step 2 Click **Select update package**, select the appropriate update method from the dialog.

The Web UI will verify which devices are compatible with the uploaded update package.

Step 3 On the page **Firmware update**, select the devices to be updated, and click **Start updating**.

--End

After updating, you can view details such as the current firmware version, target version number, and the time of the update.

8.2 Updating the Data Logger

Prerequisite

Prepare the necessary files or configurations based on your chosen update method:

- Update via iConfig: The iConfig tool is installed, and the relevant update package is downloaded.
- Update via iSolarCloud: The connection between the Data Logger and iSolarCloud is established, and there is available update package. See 7.8.6.1 Configure iSolarCloud Forwarding Service.

Step 1 Click **System** > **System maintenance** to navigate to the corresponding page.

Step 2 Click **System update**, select the appropriate update method from the dialog.

Step 3 Follow the on-screen instructions to complete the update process.

If a pop-up window indicates that the public key file is missing, you need to import the corresponding public key file for the update package before proceeding with the update. Click **System** > **Certificate management** > **System update certificate** to import the required certificates.

A confirmation dialog box appears. Upon confirmation, the Data Logger will automatically restart to apply the firmware update. The new firmware will take effect after a reboot.

--End

8.3 Update PLC master node

Prerequisite

- Data logger firmware version: P013 and above.

Prepare the corresponding resource file or configuration according to the update method:

- Update via the configuration tool iConfig: The iConfig tool has been installed and the relevant update package downloaded.
- Update via iSolarCloud: Connected to cloud service and there is an available update package currently. See7.8.6.1 Configure iSolarCloud Forwarding Service.

If the current data logger version is P012 or lower, use the **System** > **System maintenance** > **System update** method to update the PLC main node.

Step 1 Click **System > MPLC > Action** in the navigation bar to jump to the corresponding page.

Step 2 Click **PLC module update**, in the pop-up dialog box, select the update method according to the actual situation.

Step 3 According to the update method, follow the on-screen prompts to complete the update.

--End

9 Power Regulation

The data logger has a power regulation module that controls the active and reactive power of connected inverters. Users can send control commands to the inverters through a local or third-party control system to adjust grid feed-in power in response to grid requirements, helping maintain grid stability and efficient power use.

NOTICE

Power regulation parameters must be configured by qualified personnel. Incorrect settings may prevent the plant from meeting grid connection requirements and reduce energy yield.

9.1 Options for Power Control Method

When adjusting active or reactive power, you can select between two control method: open-loop or closed-loop.

Open-Loop Control

Open-loop control does not rely on feedback from the inverter's actual output. Once the Data Logger sends the initial power control command, no further adjustments are made based on the inverter's output. This control method is suitable for scenarios that require quick adjustments.

Closed-loop control

Closed-loop control depends on feedback from the inverter's actual output. The Data Logger continuously monitors the inverter's output power and compares it to the target power. If any deviation is detected, the Data Logger automatically adjusts the control commands to ensure accuracy and stability in output power. This control method is ideal for scenarios that require precise power adjustments.

To ensure accurate data feedback, closed-loop control requires connecting an smart energy meter or a box transformer with a control device to the Data Logger.

9.2 Selecting Power Control Mode

Both active power limitation and reactive power adjustment support various control methods. You can select based on the scale and needs of your power station.

Mode	Description
Remote Power Control	According to the instructions control the equipment power generation. Recommended for scenarios requiring power

Mode	Description
	adjustment through PPC (Power Plant Controller) or AGC (Automatic Generation Controller).
Local Power Control	Directly control the inverter's photovoltaic power via the Data Logger. This method is suitable for distributed power stations and zero-feed-in scenarios. Recommended when the power station is in a commissioning phase.
Analog Input	Use digital signals from the Data Logger's AI port (e.g., current or voltage) to adjust inverter power.
Digital Input	Use digital signals from the Data Logger's DI port, typically for responding to dry contact signals.
Country Mode	Suitable for meeting specific national or regional grid requirements.
Disable Dispatching	Select this option when the power adjustment has started and the inverter needs to maintain its current state.
Disable Derating	Recommended for scenarios where the inverter needs to maintain maximum power output. For example, during peak energy demand periods, this option ensures active power output is not reduced due to power adjustment. Only supports active power control.
Disable Output	Recommended for scenarios where the inverter needs to stop reactive power output. Only supports reactive power control.

Step 1 Click **Power control** in the navigation bar, from the expanded menu options, select **Active power** or **Reactive power**.

Step 2 On the page **Active power** or **Reactive power**, in the drop-down list **Active power control mode** or **Reactive control mode**, select the desired power control method.

--End

9.3 Active Power

Active power regulation controls power fed from the plant to the grid to help balance loads across the power system. When active power regulation is requested, O&M personnel should select an appropriate active power control method and configure the relevant parameters on the Web interface. These settings allow the inverter to respond promptly to regulation commands from the data logger or other control devices.

9.3.1 Remote Power Control

Open-Loop Control

Prerequisite

- The **Active power control mode** is currently set to **Remote power control**. Refer to 9.2 Selecting Power Control Mode.

Step 1 In the drop-down list **Control Method**, select **Open-loop Control**.

Step 2 In the field **Query recovery time**, specify the time to pause data interaction between the Data Logger and the inverter.

When power adjustment starts, the Data Logger temporarily stops regular data reading to prioritize adjusting the inverter's power output for quick and accurate control.

For example, if **Query recovery time** is set to "60," the Data Logger will not collect data from the inverter for 60 seconds after the power adjustment command is received. This might cause a delay in viewing device data via the Web UI or cloud platform during this period.

Step 3 In the field **Frame Delay**, specify the frame interval for the Data Logger to read inverter data.

Step 4 In the drop-down list **Target value filtering**, select the desired target value filtering method.

When the target value for power adjustment changes dramatically or suddenly, the inverter may need to rapidly adjust its output, which could impact grid stability. By implementing a filtering method, you can ensure a smoother inverter output and minimize negative effects on the grid.

- **Identical values**: The inverter only responds to the first power adjustment command's target value.
- **Change rate ≤ 0.5%Pn**: Allows the target value to vary within a certain percentage. If the change rate of the target value tween the two consecutive commands is within 0.5% of the inverter's rated power (Pn), the inverter does not need to adjust its output.
- **No filtering**: The inverter responds to any target value for power adjustment.

Step 5 In the field **Filter Time**, enter the time to filter dispatch commands.

During this period, the Data Logger decides whether to respond to the commands based on the target value filtering method.

Step 6 In the drop-down list **Maximum inverter output trigger switch**, select **Enable** or **Disable**.

- If you select **Enable**, you can set the **Maximum output trigger threshold**. When the remote dispatch target value is greater than or equal to **Maximum output trigger threshold**, the Logger sends an active power limit ratio of 100% to the inverter.
- If you select **Disable**, the above operations are not supported.

The firmware version of Logger4000 is P028 or later. See 7.8.11 Check Firmware Version for instructions on how to check the firmware version.

Step 7 Click **Save**.

--End
Once the configuration is complete, you can send further dispatch commands through the SCADA.

Closed-Loop control

Prerequisite

- **Active power control mode** is currently set to **Remote power control**.
  Refer to 9.2 Selecting Power Control Mode.
- A gateway meter or a box transformer with monitoring and control devices is connected.

Step 1 In the drop-down list **Control Method**, select **Closed-loop Control**.

Step 2 In the drop-down list **Select Energy Meter or Transformer**, select the meter or transformer for power regulation.

Step 3 In the drop-down list **Control Cycle**, specify the interval at which the Data Logger sends dispatch commands to the inverter.

Step 4 In the field **Error Limit**, specify the allowable error range for the ratio between the difference in actual active power and the target value, relative to the rated power.

If the ratio is within the error range, the power adjustment is considered to have reached the target value. You should adjust this parameter in real-time based on the inverter's output power.

Step 5 In the field **Adjustment Ratio**, set the ratio between the inverter's output power and the target value.

If If the adjustment result does not reach the set target value, the Data Logger will adjust according to the set adjustment ratio to achieve the target value. You should adjust this parameter in real-time based on the inverter's output power.

Step 6 Click **Save**.

--End
Once the configuration is complete, you can send further dispatch commands through the SCADA.

Configure Northbound Communication Anomaly Protection

If communication between the data logger and the backend system fails, active power regulation commands may not reach the inverters. This could leave inverter output uncontrolled and disturb the grid. To prevent this, configure power limits for the inverters on the data logger.

If you do not need additional communication protection, use the **Northbound Communication Abnormal Protection** drop-down list to select **Close** (default).

Step 1 From the **Northbound Communication Abnormal Protection** drop-down list, select the communication protocol used between the backend system and the data logger.

- **Modbus-TCP/IEC104**: The data logger communicates with the backend system using Modbus TCP or IEC 104.
- **Modbus-RTU**: The data logger communicates with the backend system using Modbus RTU.

The communication failure protection configuration table appears below.

Step 2 Configure the communication failure protection parameters.

O&M personnel can configure up to three backup inverter power output values.

a. Under the **Protection Switch** field, select **Enable** to enable communication failure protection settings.

b. Enter the backend system's IP address and port number in the **Peer IP Address** and **Port** text boxes, respectively.

c. In the **Communication Error Tripping Time** text box, enter the delay before the data logger initiates inverter protection.
For example, setting **Communication Error Tripping Time** to 30 means the data logger waits 30 seconds before limiting inverter output.

d. In the **Communication Abnormality Output** text box, enter the inverter output power as a percentage when a communication failure is detected.
For example, setting **Communication Abnormality Output** to 80 limits inverter output to 80% of rated power after communication is lost.

e. In the **Communication Error Auto Recovery Time** text box, enter how long the data logger waits after communication is restored.

After this period, the data logger adjusts inverter output or starts the inverter according to the **Communication Output Recovered** setting.

f. From the **Communication Output Recovered** drop-down list, select the action to take after communication is restored.

- **No Action**: When communication is restored, the data logger maintains the configured fallback output level until the backend system sends a new dispatch command to adjust the inverter's output power.
- **Boot**: The data logger first sends a startup command to the inverter, then adjusts its output according to the most recent setpoint from the backend system. This option applies if the inverter shuts down due to a communication failure.

Step 3 Click **Save**.

--End

9.3.2 Local Regulation

Open-Loop Control

Prerequisite

- **Active Control Mode** is currently set to **Local Power Control**. Refer to 9.2 Selecting Power Control Mode.

Step 1 In the drop-down list **Control Method**, select **Open-loop Control**.

Step 2 In the drop-down list **Control Cycle**, specify the interval at which the Data Logger sends dispatch commands to the inverter.

Step 3 In the drop-down list **Instruction Type**, select the designated unit for power regulation.

- **kW**: Adjusts the power by setting the total rated power of the inverter array. Recommended for scenarios where precise control of the inverter's output power is required, such as when a power station needs to comply with grid capacity limits.
- **%**: Adjusts power based on a percentage of the inverter's maximum rated power. Recommended for scenarios where the output needs to be adjusted according to the inverter's capacity.

Step 4 Click **Save**.

--End

After configuration, set the time and target value for power regulation commands issued locally by the data logger. Refer to Configuring Adjustment Time and Target Values.

Closed-Loop control

Prerequisite

- The current **Active Control Mode** is set to **Local Power Control**. Refer to 9.2 Selecting Power Control Mode.
- For closed-loop control, a gateway meter for power control must be connected.

Step 1 In the drop-down list **Control Method**, select **Closed-loop Control**.

Step 2 In the drop-down list **Control Cycle**, specify the interval at which the Data Logger sends dispatch commands to the inverter.

Step 3 In the drop-down list **Instruction Type**, select the designated unit for power regulation.

- **kW**: Adjusts the power by setting the total rated power of the inverter array. Recommended for scenarios where precise control of the inverter's output power is required, such as when a power station needs to comply with grid capacity limits.
- **%**: Adjusts power based on a percentage of the inverter's maximum rated power. Recommended for scenarios where the output needs to be adjusted according to the inverter's capacity.

Step 4 In the drop-down list **Select Meter**, select the designated meter for power regulation.

Step 5 Based on the configuration of inverter's parameter **Shutdown When Active Power Limit to 0%**, you can set related parameters of Data Logger in case of a meter communication failure.

> On the page **Device Monitoring > Power Regulation Parameters**, you can set **Shutdown When Active Power Limit to 0%** to **Enable** or **Disable**.

a. In the field **Communication Abnormality Output**, specify the target value as a percentage to be issued by the Data Logger when there is a communication failure with the meter.

If **Shutdown When Active Power Limit to 0%** is enabled, and **Communication Abnormality Output** is set to 0%, the the Data Logger sends a shutdown command to the inverters.

b. When the inverters are shut down due to **Shutdown When Active Power Limit to 0%**, in the drop-down list **Start After Communication Recovery**, select whether the Data

Logger should send a power-on command to the inverters when communication with the meter resumes.

- **Enable**: When the communication resumes, the Data Logger sends a power-on command to the inverter.
- **Disable**: When the communication resumes, the inverter will remain shut down.

c. In the field **Start Delay After Communication Recovery**, specify the waiting time for the Data Logger to send a power-on command specify to the inverter after communication is restored.

Step 6 If zero power feed-in is required, in the drop-down list **Wiring Mode**, select the connection mode of the Data Logger based on the actual situation.

- **Direct Connection**: One Data Logger is connected to all inverters, where all the inverters must be string inverters or central inverters.
- **Cascading**: Multiple Data Loggers are cascaded, and this Data Logger is used as the host.

Step 7 In the drop-down list **Feed-in Stop**, select whether the Data Logger should send a shutdown command to the inverter when feed-in power is detected.

- **Enable**: The inverter will shut down when feed-in power is detected by the meter. Select this option when zero power feed-in is required.
- **Disable**: The inverter will remain on even when feed-in power is detected by the meter.

Step 8 Select an option in the drop-down list of **Feed-in Control Mode** based on the type of data collected by the meter.

- **Total Active Power Control**: The meter collects data of three phases on the grid side as feedback values for power regulation.
- **Split-phase Active Power Control**: The meter collects data of a single phase as feedback values for power regulation.

The firmware version of the Data Logger P028 or later supports this step. See 7.8.11 Check Firmware Version for instructions on how to check the firmware version.

Step 9 Click **Save**.

--End

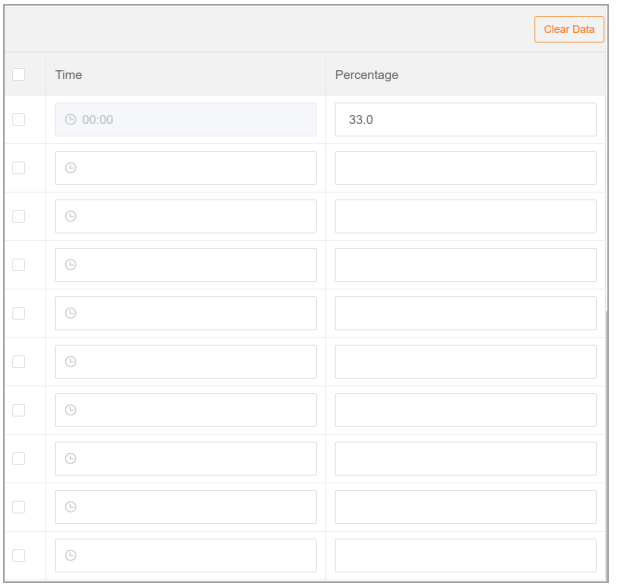
After configuration, specify the time and target values for local power control. Refer to Configuring Adjustment Time and Target Values.

Configuring Adjustment Time and Target Values

Prerequisite

- The selected power control strategy and related configurations are complete.

The specific time and target values for local power control is presented in a table.



If no additional combinations of time and target values are set, the Data Logger will adjust power according to default values throughout the day.

Step 1 Position the cursor in the column**Time**, and in the time picker, select the time to deliver the power control command.

Time is precise to the minute. The default power adjustment starts at "00:00" and cannot be changed.

Step 2 Depending on the selected **Instruction Type**, enter the target value for active power in the corresponding column **Fixed Value of Active Power** or **Percentage**.

To meet zero power feed-in or anti-backflow requirements, set the target value to "0", indicating that the inverter will not output any active power to the grid. However, to strictly control feed-in power and handle load fluctuations, it is recommended to set the target value to a negative number. After configuration, the load will draw power from the grid instead, ensuring the inverter does not active power is fed into the grid.

Step 3 To delete a specific adjustment time and target value, check the corresponding box in the first column, and click **Clear Data**.

Step 4 Click **Save**.

--End

9.3.3 AI Control

Prerequisite

- **Active Control Mode** is currently set to **Analog Input**. Refer to 9.2 Selecting Power Control Mode.
- For closed-loop control, a gateway meter for power control must be connected.

Step 1 In the drop-down list **Control Method**, select **Open-loop Control** or **Closed-loop Control**.

Step 2 For **Closed-loop Control**, in the drop-down list **Select Meter**, select the meter for power control.

Step 3 In the drop-down list **Control Cycle**, specify the interval at which the Data Logger sends dispatch commands to the inverter.

Step 4 From the **AI Port** drop-down list, select the AI port receiving analog input signals.

Click **AI Configuration** to open the **System > Port Parameter > AI** page. Modify the AI port parameters as needed. Refer to 7.8.7.3 Analog Input (AI).

Step 5 In the drop-down list **Instruction Type**, select the designated unit for power regulation.

- **kW**: Adjusts the power by setting the total rated power of the inverter array. Recommended for scenarios where precise control of the inverter's output power is required, such as when a power station needs to comply with grid capacity limits.
- **%**: Adjusts power based on a percentage of the inverter's maximum rated power. Recommended for scenarios where the output needs to be adjusted according to the inverter's capacity.

Step 6 Based on **Instruction Type**, set the power regulation setpoint range corresponding to the analog inputs in the **Min** and **Max** text boxes.

- **kW**: The values of **Min** and **Max** must both be in the range of 0.0–999999.9 kW.
- **%**: The values of **Min** and **Max** must both be between 0% and 100%.

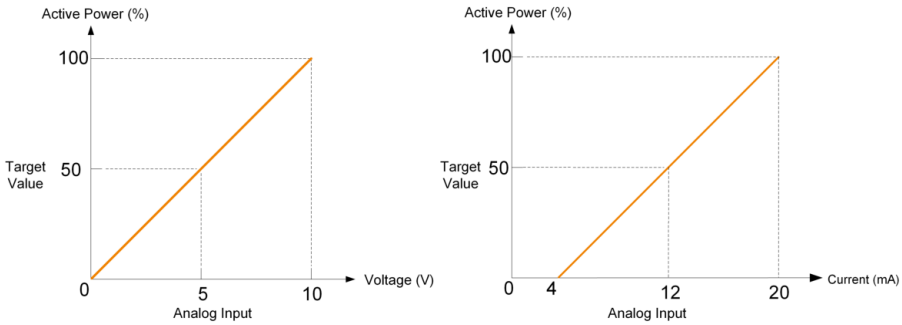


Figure 9-1 Example Mapping Between Analog Input Values and Target Values

Step 7 Based on **Instruction Type**, enter the difference between consecutive power dispatch commands in the **Step** text box.

Step 8 Click **Save**.

--End

9.3.4 Dry Contact

Prerequisite

- **Active Control Mode** is currently set to **Digital Input**. Refer to 9.2 Selecting Power Control Mode.
- For closed-loop control, a gateway meter for power control must be connected.

Step 1 In the drop-down list **Control Method**, select **Open-loop Control** or **Closed-loop Control**.

Step 2 For **Closed-loop Control**, in the drop-down list **Select Meter**, select the meter for power control.

Step 3 In the drop-down list **Control Cycle**, specify the interval at which the Data Logger sends dispatch commands to the inverter.

Step 4 In the drop-down list **Instruction Type**, select the designated unit for power regulation.

- **kW**: Adjusts the power by setting the total rated power of the inverter array. Recommended for scenarios where precise control of the inverter's output power is required, such as when a power station needs to comply with grid capacity limits.
- **%**: Adjusts power based on a percentage of the inverter's maximum rated power. Recommended for scenarios where the output needs to be adjusted according to the inverter's capacity.

Step 5 In the table at the bottom of the page, configure the power regulation setpoints corresponding to the digital input signals.

a. Select the corresponding DI ports based on the dry-contact signals received by the DI ports.

b. Based on **Instruction Type**, enter a fixed active power value or an active power percentage.

To delete a DI signal combination, select the checkbox in the first column of its row and click **Clear Data**.

Step 6 Click **Save**.

--End

9.3.5 Country Mode

Prerequisite

- **Active Control Mode** is currently set to **Country Mode**. Refer to 9.2 Selecting Power Control Mode.

Currently supported countries

- Korea
- Japan
- Australia
- China

9.3.5.1 Korea

Step 1 In the drop-down list **Country**, select **Korea**.

Step 2 In the drop-down list **PPC Type**, select the power plant controller DER-AVM.

Step 3 In the field **Forwarding Modbus ID**, enter the Modbus forwarding address (Range: 1~10).

Step 4 Click **Save**.

Step 5 During the installation and commissioning phase of the power station, if the inverter is not yet connected, you can use the data simulation feature to test whether the Data Logger forwards data correctly.

By default, the data simulation switch is disabled.

a. In the drop-down list **Enable**, select **Enable** to turn on the data simulation switch.

The Web UI will display multiple parameters for configuring simulated data.

b. Enter the required simulated data based on your testing needs.

c. Click **Save**.

d. On the AVM device, check whether it correctly receives the data forwarded by the Data Logger.

--End

9.3.5.2 Japan Mode

Step 1 From the **Country** drop-down list, select **Japan**.

Step 2 From the **Scheduling Mode** drop-down list, select the power company to which the plant is connected.

The data logger then connects to the power company's dispatch server.

Step 3 From the **Obtaining Schedule** drop-down list, select how the schedule is obtained.

- **Remote Download**: Download the schedule from the connected power company's server. Enter the plant ID, verification information, time range, and server URL, and upload the certificate.
- **Local Import**: Upload a schedule file.

Step 4 From the **Parameter Type** drop-down list, select the parameter settings to complete.

- **Plant Parameter**: Set **Plant Information** and **PV Module Capacity**.
- **Device Parameter**: Click **Detailed Device Parameter** to view and configure device details.

Step 5 From the **Time Calibration** drop-down list, select the number of minutes to adjust the time by.

A positive value advances the time; a negative value moves it back.

The **Time Validity** field displays the time correction result.

If **Invalid** is displayed, the data logger sends shutdown commands to the inverters until time correction or synchronization succeeds.

Time correction may fail for the following reasons:

- Data logger system time < corrected time
- Data logger system time < NTP synchronization time

Step 6 Click **Save**.

--End

9.3.5.3 Australia Mode

Step 1 From the **Country** drop-down list, select **Australia**.

Step 2 In the **Scheduling Mode** drop-down list, select a dispatch method.

Step 3 In the **DO Control** drop-down list, select whether dispatch is controlled by digital output signals.

Step 4 In the **Limited Power** text box, enter the percentage by which inverter power is to be limited.

Step 5 In the **Server URL** text box, enter the server URL. In the **Token** text box, enter the token for the server.

Step 6 In the **Power Threshold for Negative Power Prices** input field, set the percentage limit on inverter output when electricity prices are negative.

Step 7 Click **Save**.

--End

9.3.5.4 China

Step 1 In the drop-down list **Country**, select **China**.

Step 2 In the drop-down list **Scheduling Mode**, select **DC Energy Storage**.

Step 3 Click **Save**.

--End

9.3.6 Disable Dispatch

If the data logger is already limiting the inverter's active power and the inverter needs to maintain its current operating state, you can disable active power regulation.

Step 1 On the **Active Power** page, set **Active Control Mode** to **Disable Dispatching**.

Step 2 Click **Save**.

--End

The inverter continues operating under the current active power limit.

9.3.7 Disable Derating

Disable derating prevents reductions in inverter power output.

Step 1 On the **Active power** page, set **Active Control Mode** to **Disable Derating**.

Step 2 Click **Save**.

--End

The data logger stops limiting active power, and the inverter operates at full load with its power output maintained at 100%.

9.4 Reactive Power

Reactive power regulation adjusts reactive power generation or consumption to help maintain grid voltage and stability. When the grid requires reactive power compensation or injection, O&M personnel must select an appropriate reactive power control method and configure the relevant parameters on the Web interface. This allows the inverter to respond accurately to commands from the data logger or third parties.

9.4.1 Remote Power Control

Prerequisite

- **Reactive Control Mode** is currently set to **Remote Power Control**. Refer to 9.2 Selecting Power Control Mode.
- For closed-loop control, a gateway meter or a box transformer with monitoring and control devices must be connected.

Step 1 In the drop-down list **Control Method**, select **Open-loop Control** or **Closed-loop Control**.

Step 2 When **Open-loop Control** is selected, refer to remote active power regulation and configure the relevant parameters. Refer to Open-Loop Control.

Intelligent reactive power distribution is disabled by default and can be enabled as needed.

Step 3 When **Closed-loop Control** is selected, refer to remote active power regulation and configure the relevant parameters. Refer to Closed-Loop control.

For closed-loop control, the error tolerance percentage must be greater than the adjustment ratio percentage.

Step 4 When **Closed-loop Control** is selected, use the **Reactive Power Direction** drop-down list to specify whether the reactive power direction reported by the meter or MVS matches that of the inverter.

By default, SUNGROW inverters output positive inductive reactive power when grid voltage must be increased and negative capacitive reactive power when it must be decreased.

- **Forward Direction**: The reactive power direction recorded at the point of grid connection matches that of the inverter.
- **Direction Reverse**: The reactive power direction recorded at the point of grid connection is opposite to that of the inverter.

Step 5 Click **Save**.

--End

After configuration, O&M personnel can send power regulation setpoints from the backend system.

9.4.2 Local Power Control

Configure reactive power regulation parameters locally.

Prerequisite

- **Reactive Control Mode** is currently set to **Local Power Control**. Refer to 9.2 Selecting Power Control Mode.
- For closed-loop control, a gateway meter for power control must be connected.

Step 1 In the drop-down list **Control Method**, select **Open-loop Control** or **Closed-loop Control**.

Step 2 In the drop-down list **Instruction Type**, select the designated unit for power regulation.

- **PF**: Adjusts power based on the power factor. Recommended for scenarios where the inverter needs to maintain a specific power factor level.
- **%**: Adjusts power based on a percentage of the inverter's maximum rated power. Recommended for scenarios where the output needs to be adjusted according to the inverter's capacity.

Step 3 When **Closed-loop Control** is selected, configure the relevant parameters.

a. From the **Select meter** drop-down list, select the meter used for power regulation.

b. From the **Wiring scheme** drop-down list, select the inverter connection method.

c. In the **Line Reactive Power Compensation** text box, enter an estimate of reactive power losses in the line.

d. In the **Control cycle** text box, enter the interval at which the data logger sends power regulation commands to the inverter.

e. From the Instruction type drop-down list, select the unit for the power regulation setpoint.

Step 4 Refer to local active power regulation and add the dispatch times and setpoints. Refer to Configuring Adjustment Time and Target Values.

--End

9.4.3 AI Control

Prerequisite

- **Reactive Control Mode** is currently set to **Analog Input**. Refer to 9.2 Selecting Power Control Mode.
- For closed-loop control, a gateway meter for power control must be connected.

Step 1 In the drop-down list **Control Method**, select **Open-loop Control** or **Closed-loop Control**.

Step 2 In the drop-down list **Control Method**, select **Open-loop Control** or **Closed-loop Control**.

Step 3 Based on **Instruction Type**, set the power regulation setpoint range corresponding to the analog inputs in the **Min** and **Max** text boxes.

- **PF** (open-loop control): The values of **Min** and **Max** must be between 0.8 and 1.
- **%**: The values of **Min** and **Max** must both be between 0% and 100%.

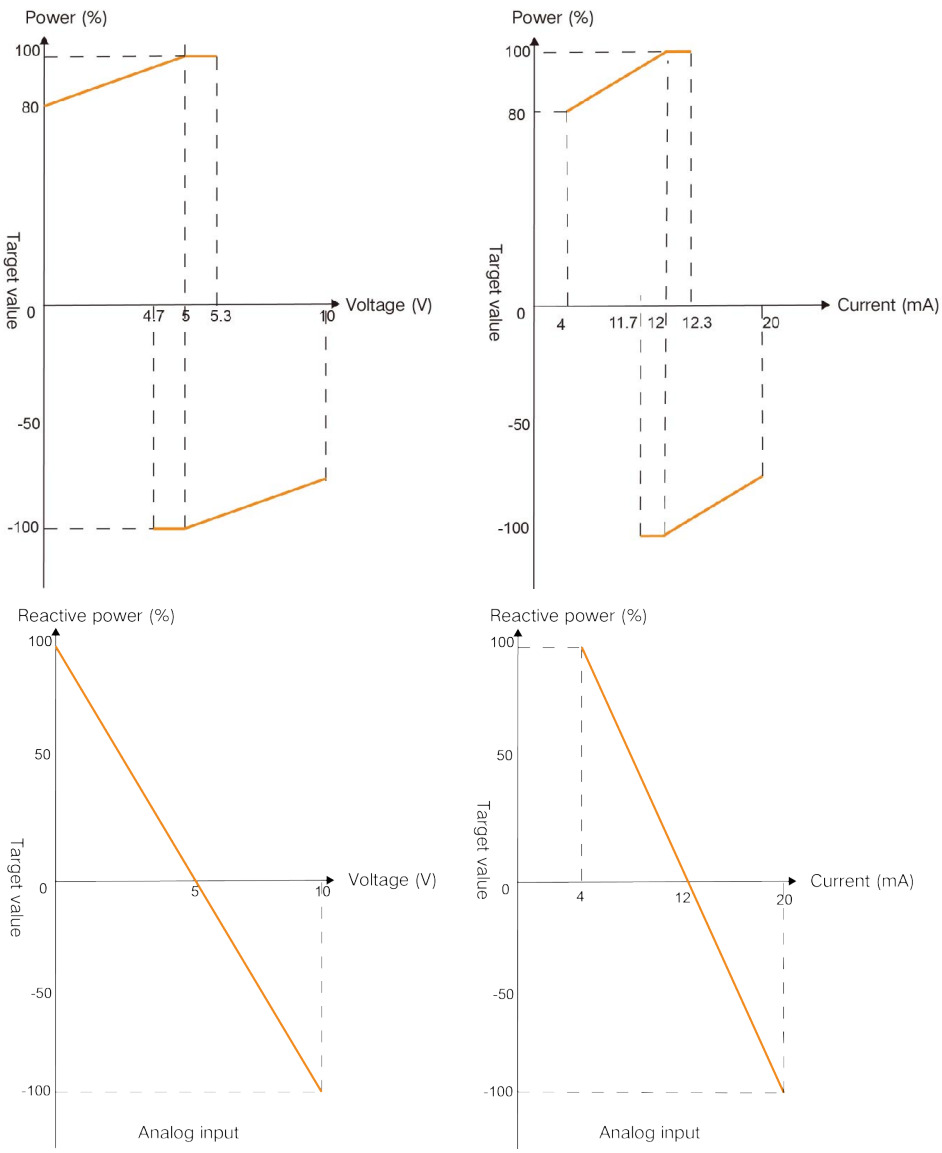


Figure 9-2 Example Mapping Between Analog Input Values and Target Values

Step 4 Based on **Instruction Type**, enter the difference between consecutive power dispatch commands in the **Step** text box. This specifies the minimum change required to issue a new command. If the change is smaller than the step size, no command is sent and the previous setpoint is retained. Otherwise, a new command can be sent.

Step 5 Click **Save**.

--End

9.4.4 Dry Contact

Prerequisite

- **Reactive Control Mode** is currently set to **Digital Input**. Refer to 9.2 Selecting Power Control Mode.
- For closed-loop control, a gateway meter for power control must be connected.

Step 1 In the drop-down list **Control Method**, select **Open-loop Control** or **Closed-loop Control**.

Step 2 When **Closed-loop Control** is selected, configure the following parameters.

a. From the **Select Meter** drop-down list, select the meter used for power regulation.

b. In the **Control Cycle** text box, enter the interval at which the data logger sends power regulation commands to the inverter.

Step 3 In the drop-down list **Instruction Type**, select the designated unit for power regulation.

- **PF**: Adjusts power based on the power factor. Recommended for scenarios where the inverter needs to maintain a specific power factor level.
- **%**: Adjusts power based on a percentage of the inverter's maximum rated power. Recommended for scenarios where the output needs to be adjusted according to the inverter's capacity.

Step 4 In the table at the bottom of the page, configure the power regulation setpoints corresponding to the digital input signals.

a. Select the corresponding DI ports based on the dry-contact signals received by the DI ports.

b. Based on **Instruction Type**, enter the reactive power percentage or power factor.

To delete a DI signal combination, select the checkbox in the first column of its row and click **Clear Data**.

Step 5 Click **Save**.

--End

9.4.5 Country Mode

Select national grid dispatch commands as the source of dispatch instructions.

Prerequisite

- **Reactive Control Mode** is currently set to **Country Mode**. Refer to 9.2 Selecting Power Control Mode.

Step 1 From the **Country** drop-down list, select the country where the device is installed.

Step 2 When the country is set to **Korea**, configure the following parameters.

a. From the **PPC Type** drop-down list, select a PPC device of the DER-AVM type.

b. In the **Forwarding Modbus ID** text box, enter the Modbus forwarding address (1–10).

Step 3 Click **Save**.

--End

9.4.6 Disable Dispatch

Disable reactive power dispatch from the data logger to the inverter.

Step 1 On the **Reactive Power** page, set **Reactive Control Mode** to **Disable Dispatching**.

Step 2 Click **Save**.

--End

The inverter continues operating at its current reactive power setting.

9.4.7 Disable Output

In certain circumstances, such as when the grid operator does not require the plant to regulate the voltage at the point of grid connection and the grid does not require reactive power compensation, the inverter can be configured to stop supplying reactive power. This helps maintain grid stability and prevents voltage fluctuations caused by reactive power regulation.

Step 1 On the **Reactive Power** page, set **Reactive Control Mode** to **Disable Output**.

Step 2 Click **Save**.

--End

After configuration, the inverter's reactive power output returns to 0%.

9.5 Configure Emergency Shutdown

If a short circuit, overload, or equipment fault occurs on the grid, emergency shutdown quickly shuts down multiple inverters to maintain grid stability and operational safety.

Prerequisite

- The data logger is connected to an emergency stop device.

The DI emergency shutdown message channel can be enabled or disabled through the Modbus TCP or GOOSE fast dispatch switch without restarting the data logger.

Step 1 In the navigation bar, choose **Power Control > Emergency Button**.

Step 2 Set **Emergency Button** to **Enable**.

Step 3 From the **DI Port** drop-down list, select the DI port connected to the emergency stop device.

Step 4 From the **Inverter Status During Emergency Stop Recovery** drop-down list, select the inverter state after emergency shutdown is released.

- **Boot**: When emergency shutdown is released, the data logger sends startup commands to multiple inverters.
- **Shutdown**: When emergency shutdown is released, the inverters remain in standby mode.

Step 5 Click **Save** to apply the changes.

--End

If the inverter remains in standby after the emergency stop switch is reset, start it manually through **Device Monitoring > Device Instruction**. If you have any questions, contact SUNGROW.

10 User management

The administrator account can create O&M user accounts, reset account passwords, configure account protection and session security parameters, and enable the R&D debugging switch.

Prerequisite

- The firmware version of Logger4000 is P018 or later. See 7.8.11 Check Firmware Version.
- The operator has administrator permissions.

10.1 Initial username and password

User Type	Username	Default Password	Permissions
General user	user	Username + S/N	Monitoring permissions and basic setting permissions only, such as viewing Overview, device monitoring, and some historical data.
O&M User	maintain	Username + S/N	All operations described in this manual by default.
Auditor	auditor	Username + S/N	Audit the operation logs, parameter logs, and rsyslog logs of all users.
Administrator	administrator	Username + S/N	Add, delete, modify, and clear users; manage sessions; enable or disable developer debugging; assign certificates.

User Type	Username	Default Password	Permissions
Developer user	develop	Generate a dynamic password based on the S/N obtained through customer authorization.	After authorization by the administrator, diagnose and clear complex device faults.

For firmware version LOGGER-SV400.001.00.P036B001 and later, the system requires the default password to be changed. Earlier versions do not enforce this requirement. Customers can decide whether to change the default password, but changing the password is still recommended to improve security.
On the User management page, the Clear users function is available. Click it to clear the accounts managed under administrator. This function applies only to the maintain, auditor, and user accounts. It is not supported for the administrator or develop account.

10.2 Password Management

1. All passwords have been encrypted and stored.
2. All passwords require strong complexity. The default password must be changed after the first login.
3. If there is a suspicion of password leakage, please change the password immediately. The new password must not be the same as the old one.

Log in as an administrator user and go to the **Password management** page to dynamically set the following parameters:
- Minimum password length
- Password Complexity
- Number of repeated old and new passwords

After the settings are completed, click Save to take effect.

4. All user passwords have an expiration period. The password validity period can be set by the administrator account, with the configurable range for password validity being 1 to 90 days. Please update your password promptly when it expires.

- By setting different privilege accounts for different users, administrators can enhance system security, improve operational efficiency for different users, and reduce management costs.
- When a regular user logs in and the prompt **Other user login** appears, it is necessary to log out of the other user session first.

10.3 Set up the administrator account

The administrator account must be bound to an email address or mobile number so that the password can be reset through email or mobile verification if the password is forgotten.

Prerequisite

- Log in to the Web UI with the administrator account. See 10.1 Initial username and password.

Step 1 In the navigation bar, click **Link Account** to go to the corresponding page.

Step 2 Set the binding information for the administrator account.

Depending on the UI language, the following information can be bound:

- Email address
- Mobile number

If both an email address and a mobile number are bound, mobile verification is used first.

Step 3 Click **Save**.

Step 4 To delete the account binding information, click **Unlink**.

--End

10.4 Create User Accounts

An administrator can create general user, O&M, and audit accounts to support team operations and maintenance.

The system includes a default O&M account named "maintain".

An administrator can create accounts, with a maximum of seven Web interface user accounts.

Username requirements

- Usernames must be 2–16 characters long, contain only letters and numbers, and start with a letter.

Password requirements

User passwords must meet the complexity requirements set by the administrator. Refer to 10.2 Password Management.

Prerequisite

- Log in to the Web interface using an administrator account. Refer to 10.1 Initial username and password.

Step 1 Choose **User Management** from the navigation bar.

Step 2 Click **Add** to open the **Add User** dialog box.

Step 3 Set the username and password.

Step 4 From the **Permission** drop-down list, select **O&M User**.

Step 5 Click **Confirm**.

--End

10.5 Delete User Accounts

Prerequisite

- Log in to the Web interface using an administrator account. Refer to 10.1 Initial username and password.

Step 1 Choose **User Management** from the navigation bar.

Step 2 In the **Action column for the selected user account, click** .

Step 3 In the pop-up window, click **Confirm** to delete the user account.

Step 4 Click **Clear Users** to delete all user accounts.

--End

10.6 Reset account passwords

10.6.1 Reset User Account Password

Reset passwords for super administrator, O&M user, audit user, and general user accounts.

Prerequisite

- Log in to the Web interface as an administrator. Refer to 10.1 Initial username and password for details.

Step 1 In the navigation bar, click **User Management**.

Step 2 In the Action column for the user account, click to open the **Modify User** dialog box.

Step 3 Enter the new password.

Step 4 Click **Confirm** and enter the password of the currently logged-in account to reauthenticate. You can change the selected account's password after successful reauthentication.

--End

10.6.2 Reset Administrator Account Password

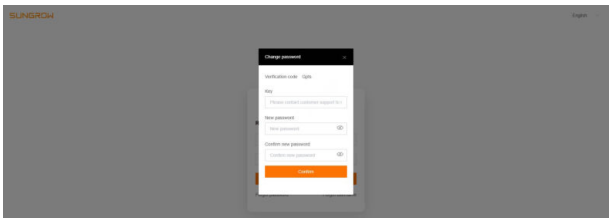
- If you are already logged in to the Web interface as an administrator, you can reset the password on the **User management** page. Refer to 10.6.1 Reset User Account Password for details.
- If you forget the administrator account password, use **Forgot password** on the login page to reset it. Follow these steps:

Step 1 Open the Logger4000 Web interface.

Step 2 Enter the username: administrator.

Step 3 Click **Forgot Password** to open the **Modify Password** dialog box.

Step 4 Send the verification code and the device serial number to SUNGROW O&M personnel. When you receive the key, enter it to reset the password.



Step 5 Enter and confirm the new password.

Step 6 Click **Confirm**.

--End

10.7 Enable Multi-factor authentication

Multi-factor authentication (MFA) is a security mechanism that requires users to verify their identity using two or more different types of authentication factors to enhance account or system security. This function is disabled by default. Enable it as needed.

Prerequisite

- Log in to the Web interface as an administrator.
- The browser you use to log in must have an HTTPS client certificate installed. The certificate must be bound to the account's username.

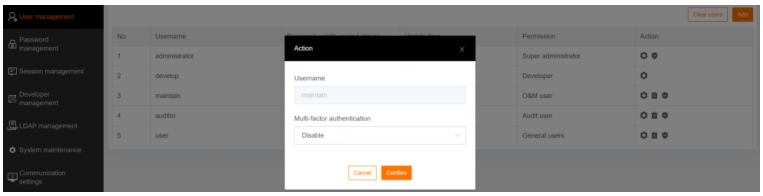
  - An HTTPS client certificate can be generated using the iConfig configuration tool. Please contact Sungrow Customer Service for the iConfig installation package and instructions for using the tool. If you use your own certificate, ensure that its common name (CN) field matches the username used to log in with MFA.
  - An HTTPS client certificate in PKCS #12 (.p12) format is recommended. This format combines the device certificate, private key, and certificate chain in a single file. Exporting the file requires verification with an access password, helping protect the private key.

- Import the root certificate used to verify the HTTPS client certificate into the device.

- You can export this root certificate from the browser in which the HTTPS client certificate is installed.
- Choose **Certificate management > Forward**. In the Action column for the HTTPS certificate, click . Select the certificate type and format, upload the root certificate file, and click **Save**.
- The root certificate must be in PEM format.

Step 1 In the navigation bar, click **User management**.

Step 2 In the Action column for the user account, click to open the **Action** dialog box.



Step 3 In the **Multi-factor authentication** drop-down list, select **Enable** and click Confirm.

Step 4 After reviewing and confirming all items in the warning dialog box, click **Confirm** to enable MFA.

- After MFA is enabled, you must access the device at https://<device IP>:58443.
- Ensure that proxies, firewalls, and other tools running on the computer used to log in to this account do not block mutual TLS authentication for the HTTPS connection.

--End

10.8 Configure Account Protection and Session Security Parameters

To enhance account security, you can configure the relevant parameters to control login behavior and session validity.

Prerequisite

- Log in to the Web as an administrator.

Step 1 In the navigation bar, click**Session management** to go to the corresponding page.

Step 2 Change the account and session security settings.

The following settings are available:

- **Number of illegal visits**: Set the maximum number of allowed failed login attempts. If the number of incorrect password attempts exceeds the specified limit, the account is locked automatically. (Range: 5–20; default: 5)

- **Unauthorized access time window**: Sets the time window for counting unauthorized access attempts. If the number of unauthorized access attempts exceeds the limit within the specified period (range: 1–24 h; default: 24 h), the account is locked automatically.
- **Session timeout**: Define the period of inactivity after which the login session will time out. Once timed out, the user will be required to log in again. (Range: 1–60 min; default: 10 min)
- **User lock duration**: Specify the duration for which the user account remains locked after exceeding the failed login attempts limit. The user must wait until this period expires for the account to be unlocked. (Range: 1–60 min; default: 10 min)

Step 3 Click **Save**.

--End

10.9 Enable O&M Mode

To allow Developer users to log in to the Web interface for debugging, the administrator must enable **R&D Debugging**.

- **R&D Debugging** is disabled by default.

Prerequisite

- Log in to the Web interface using an administrator account. Refer to 10.1 Initial username and password.

Step 1 Choose **R&D Management** from the navigation bar.

Step 2 Turn on the switch.

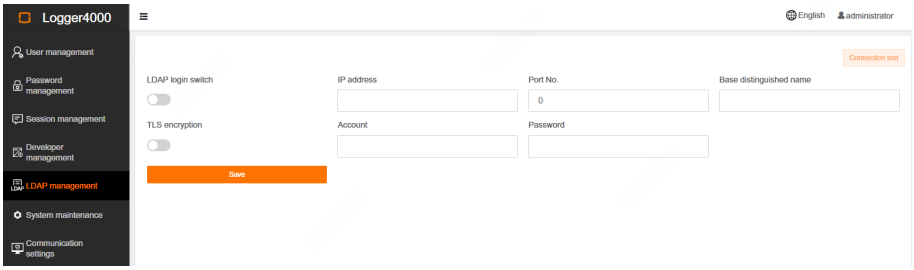
The switch automatically turns off after being enabled for 24 hours.

--End

10.10 LDAP Management

Supports login via LDAP, suitable for power stations that provide LDAP services on-site, enabling centralized account management.

Log in with the administrator account, click **LDAP management**, and enter the LDAP management operation interface.



- When the LDAP login switch is enabled, the system will synchronize the TLS encryption. If the user manually disables TLS encryption, the system will issue a security warning: "Disabling this will stop data encryption. Are you sure you want to proceed?"
- The LDAP server must support TLS 1.2 or higher encryption algorithms to enable communication.

Parameter Name	Explanation
IP address	The IP address of the LDAP server
Port Number	The port of the LDAP server
Base Identifier Name	LDAP Base Distinguished Name
Account	LDAP Server Account
Password	LDAP Server Password

After enabling the LDAP login switch, you need to fill in the configuration parameters and click**Save**. After successfully saving, the interface displays "Operation successful".

After enabling LDAP login, users will no longer see the prompt "Please contact the administrator to enable <LDAP login> and try again" during LDAP login. They can input their username and password to log in.

- LDAP login does not support forgetting the password.
- User authentication information related to LDAP login is stored in the customer's own LDAP server.

10.11 System Maintenance

10.11.1 Backup and Restore

Log in with the administrator account, then choose **System Maintenance > Backup and Restore**.

Back Up

1. Choose **Backup and Restore > Back Up**, then click **OK** to perform the backup.
2. Set the archive password and click **OK**. The system generates an encrypted archive locally.

> The archive password must be 8–32 characters long and include at least three of the following: uppercase letters, lowercase letters, digits, and special characters.

Restore

1. Choose **Backup and Restore > Restore**, then click **OK** to perform the restore.
2. Enter the password for the backup archive and click **OK**.
3. Select the encrypted backup archive. The system restarts and completes the restore.

10.11.2 Restore factory settings

> After restoring the factory settings, log in to the Web UI again. The page prompts you to choose whether to enable network security mode.

Step 1 Choose **System maintenance > Restore factory settings**.

Step 2 In the warning dialog box, click **Confirm**.

--End

> Restoring the factory settings only resets all modified settings to the factory defaults. It does not clear data.

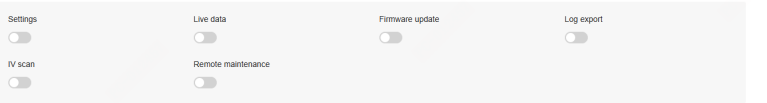
10.12 Communication Settings

10.12.1 iSolarCloud

1. Log in as administrator and click the **Communication settings** module to go to the **iSolarCloud** submodule.
2. Enable **Communication master switch** to connect to iSolarCloud. This function enables the iSolarCloud communication channel and allows authorized O&M personnel to configure remote maintenance and iSolarCloud access.
3. Click **Cloud-to-device**. Set the authorization validity period as needed, and then click **Confirm** to authorize.

   > To update the authorization validity period, click **Validity update** to reset the permission period. The extended permission period is calculated from the currently set time.

4. Configure the view and control permissions for authorized O&M personnel. Enable the corresponding function switches as needed.



10.12.2 Third-Party Cloud

1. Log in as administrator and choose **Communication settings > Third-party cloud** to enter the **Third-party cloud** subpage.
2. Enable **Third-party cloud** and confirm the authorization prompt. Authorized O&M personnel can configure Third-party cloud. Enabling this function allows device data to be uploaded to the configured server.

11 Routine Maintenance

Due to ambient temperature, humidity, dust, and vibration, the internal components of the Data Logger may age and wear, which may lead to potential failures inside the device. Therefore, it is necessary to perform daily and regular maintenance on the Data Logger to ensure its normal operation and service life.

All measures, which can help the Data Logger to keep good working conditions, are within the maintenance scope.

11.1 Safety Instructions

⚠ WARNING

Only qualified and authorized personnel may perform maintenance and other operations on the Data Logger.
Do not leave screws, washers or other metal parts in the Data Logger during maintenance. Otherwise, damage may be caused to the device!

⚠ WARNING

After the Data Logger stops running, wait at least 5 minutes before performing any operation on it.

Five Safety Rules

The following five safety rules shall be observed during maintenance or troubleshooting of the Data Logger to ensure operators' safety:

- Disconnect the Data Logger from all external connections and internal power supplies.
- Ensure that the Data Logger will not be inadvertently connected.
- Ensure that the Data Logger is voltage-free using a multimeter.
- Connect necessary grounding cables.
- If there are parts in the operation area that may carry voltage, cover them with insulated cloth for insulation shielding.

11.2 Maintenance List

Item	Method
Working environment	• Ensure that there are no devices emitting strong electromagnetic interference near the Data Logger. • Ensure that there are no heat sources near the Data Logger.

Item	Method
	• Ensure that there are no corrosive materials present near the Data Logger.
Hardware	• Ensure that the power supply voltage is within the normal range. • Ensure that the wiring connections are secure and reliable. • Ensure that the device is properly grounded.
System cleaning	• Ensure that the enclosure, circuit board and other components are clean. • Check for dust or obstructions in the ventilation holes.
Terminal and cable connection	• Check whether the screws of control terminals are loose. Tighten them with a screwdriver if necessary. • Check whether the copper bars or screws are oxidized and discolored. • Visually inspect the connections and distribution of terminals and cables.
Software	• Log in to the web interface to check the device's communication status. • Log in to the web interface to review and adjust the parameters of the Data Logger. • Log in to the web interface to check the software version of the Data Logger.

12 Troubleshooting

12.1 Safety Instructions

⚠ DANGER

Before proceeding with any troubleshooting, ensure that the grounding cable is properly grounded. Failure to do so may result in a severe electric shock hazard for the operators.

12.2 Common Fault Phenomena and Troubleshooting Methods

The common faults of the data logger and their corresponding solutions are listed in the table below. If you still cannot resolve the issue or have further questions even after referring to this manual, please contact Sungrow Power Supply Co., Ltd. To resolve the issue more efficiently, the following information needs to be provided simultaneously:

- Data logger serial number, production date, and software version information
- Brand, model, configuration, and other information of the device connected to the data logger
- Fault information and a brief description of the fault;
- Pictures of the fault occurrence site (if on-site conditions permit)

Fault Details	Possible Cause	Suggestions
Cannot log in to the data logger Web interface	The network connection between the PC and the data logger is incorrect.	Check whether the network port connection between the PC and the data logger is normal.
	PC network signal abnormal.	Check if the PC network signal icon is normal.
	The IP address settings on the PC are incorrect.	Manually configure the IP address of the PC's network port to ensure it is in the same subnet as the data logger's IP address.
	The PC cannot receive data normally.	Manually enable the Ping function by using the shortcut key **Win+R** Bring up the Run command box, inputping

Fault Details	Possible Cause	Suggestions
		12.12.12.12(The IP address of the data logger), check whether it can receive data packets.
	Conflicts with network cards, antivirus software, etc.	If you cannot receive the data packet, please disable other network cards, antivirus software, or firewalls, and retry.
The data logger is unable to communicate with the device.	The RS485 communication cable between the device and the data logger is abnormal.	Check if the RS485 communication cable between the device and the data logger has any short circuit, open circuit, or reverse connection issues between RS485–A and RS485–B.
	The serial port configuration is inconsistent with the RS485 parameters of the device.	Log in to the Web page of the data logger, and on the **System > Port Parameter > RS485** page, check whether the serial port configuration matches the RS485 parameters of the device.
	Abnormal communication connection status between the data logger and the device.	Log in to the data logger's web page and observe**Device Monitoring**On the page, does the communication status icon display normally? If an exception occurs, check whether there is an address duplication under the same port. If the issue persists, please contact Sungrow's customer service center.

Fault Details	Possible Cause	Suggestions
The data logger forwards ModbusRTU with no background data.	The RS485 communication cable between the device and the data logger is abnormal.	Check if the RS485 communication cable between the equipment and the data logger has a short circuit, open circuit, or reverse connection of RS485–A and RS485–B.
	The Web interface has incorrect COM port parameter settings.	Log in to the web page of the data logger, and on the **System > Port Parameter > MODBUS > RTU** page, check whether the serial port forwarded to the backend is configured as **Forwarding is Prohibited** . Check if the serial port parameters are correct.
	The "collection address" and "backend address" of the device do not match.	On the **Device > Device List** page, verify whether it corresponds to **Forwarding Modbus ID**.
	The backend protocol configuration is inconsistent with the device.	Check whether the backend protocol configuration is consistent with the device.
The data logger forwards Modbus TCP and there is no data in the background.	There is a network connection error between the data logger and the backend.	Check if the network connection between the data logger and the backend is correct.
	The ETH port configuration of the data logger is incorrect.	The ETH port configuration of the data logger is set to the IP address that needs to be connected in the background.
	The device's collection address does not correspond to the forwarding address.	On the **Device > Device List** page, verify whether it corresponds to **Forwarding Modbus ID**.

Fault Details	Possible Cause	Suggestions
	The backend protocol configuration is inconsistent with the device.	Confirm whether the backend protocol configuration matches the device.
The data logger forwards IEC104 background no data.	There is an error in the network connection between the data logger and the backend.	Check whether the network connection between the data logger and the backend is correct.
	The IP address of the forwarding device is incorrect, or the backend IP address is incorrect.	Log in to the Web page of the **data logger**, click on the **System > Port Parameter > IEC104** page, click **White List Setting**, and check whether the whitelist is enabled. If enabled, only IP addresses in the whitelist are allowed to connect to the data logger.
	Device communication abnormal.	Check if the device communication is abnormal.
	There is an error in the backend parameter configuration.	Confirm that the backend parameter configuration is correct.
The data logger forwards no data from the iSolarCloud platform.	The system time of the data logger is incorrect.	Log in to the data logger web interface, and click **System > System Time**to check whether the time settings are correct.
	ETH network port abnormal.	The Internet network can be accessed through the Ethernet port of the data logger.
	Communication anomaly between the data logger and equipment such as the inverter and combiner box.	Confirm whether the data logger can communicate normally with devices such as the inverter and combiner box.

Fault Details	Possible Cause	Suggestions
Failed to update the inverter via the WEB interface.	The inverter of the current version does not support the remote update function, or the update file is inconsistent with the actual device version.	Confirm that the inverter's current version supports the remote update function, and that the version of the sgu file for updating is consistent with the existing version on the actual device.
	The upgrade file is incorrect.	The upgrade file is invalid, including cases where the upgrade file is encrypted or incorrectly named.
	The inverter model to be updated does not match the update file.	Check whether the inverter model to be updated matches the model of the update file.
	Communication connection exception.	After verifying the communication cable, retry. If the issue persists, contact Sungrow's customer service center.
Failed to set parameters through the WEB interface.	Communication connection exception.	Through the data logger's web interface, observe**Device Monitoring**Check whether the displayed communication status icon is normal.
	The current inverter operating state does not allow this parameter setting.	Confirm the operating status of the inverter. For example, when the inverter speed control switch is enabled, it is possible to set the active power rise speed and fall speed.
The fast dispatch instruction in Goose messages is not issued to the inverter when an external	Port parameters for rapid dispatch**Fast Scheduling Switch** not enabled	• Log on to the data logger web page. • Click **System > Port Parameter > RS485**, click ⚙, and set the

Fault Details	Possible Cause	Suggestions
		port's **Fast Scheduling Switch** to **Enable**.
communication module is connected.	The inverter device has not been added to the MPLC port.	• Log on to the data logger web page. • Click **Device > Device List > Add Device**. • When adding a device, click the corresponding DO function column and select **Communication Control**.
104 background cannot remotely control DO	The DO control type is not configured as "**Communication Control**".	• Log in to the data logger web page. • Click **System > Port Parameter > DO**, click the function column corresponding to DO, and select **Communication Control**.

13 Frequently Asked Questions

What types of external communication ports does the data logger have, what are their names, and how are they configured?

Communication Type	Port Name	Default Settings
Ethernet	ETH1, ETH2, ETH5	Refer to 7.8.7.2 Ethernet for default settings.
RS485	A1B1– A9B9	Baud rate: 9600, Parity: None, Data bits: 8, Stop bits: 1.
MPLC	L1, L2, L3	Baud rate: 115200, Parity: None, Data bits: 8, Stop bits: 1.

Which forwarding protocols does the data logger support?

Protocol Type	Description
Modbus RTU/Modbus TCP protocols	The data logger forwards data collected from connected devices, such as inverters, combiner boxes, and meteo stations, to the backend system. The backend system assigns forwarding addresses to these devices and uses those addresses to query and retrieve their data.
IEC 104 protocol	1. Add devices, such as inverters, combiner boxes, and meteo stations, through the Web interface. 2. Export the IEC 104 point table on the **System > Transfer Configuration > IEC104** page. The point table contains the devices' measurement point information.
FTP protocol	The data logger uses FTP to transfer data files collected from devices such as inverters, combiner boxes, and meteo stations to the backend system.

Protocol Type	Description
MQTT protocol	The data logger uses MQTT to send data from connected devices, such as inverters, combiner boxes, and meteo stations, to iSolarCloud.

How Do I Log In with a Developer Account and Obtain the Password?

An O&M account meets most on-site configuration needs. If special on-site requirements call for Developer access, contact Sungrow Customer Service to obtain a temporary login password. The temporary password is valid only on the day it is issued.

How do I connect multiple data loggers to the backend system over a network?

1. Connect nearby data loggers (less than 100 m away) to a fiber-optic switch using Ethernet cables.
2. For data loggers more than 100 m away, install optical fiber cables to connect them to the fiber-optic switch.
3. After connecting them, assign IP addresses in the same subnet to all data loggers. Each address must be unique.

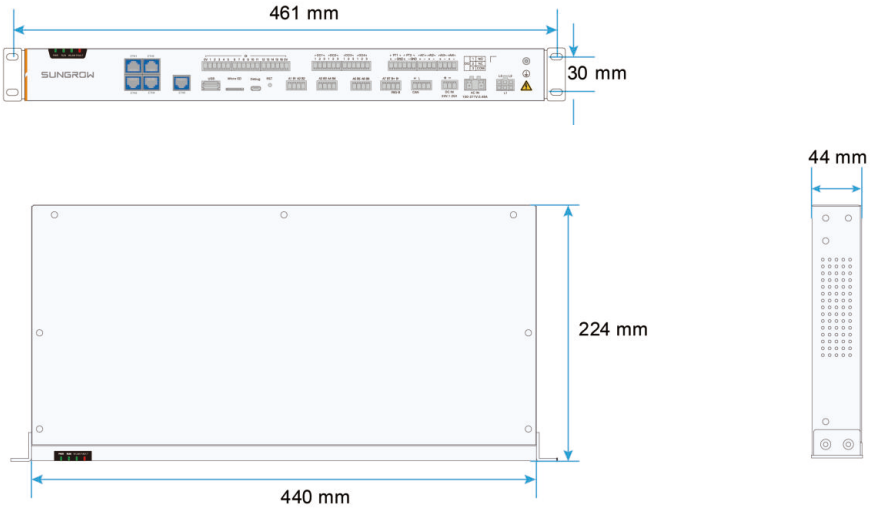
14 Appendix A: Technical Data

Communication	
Inverter communication	RS485, MPLC
PC communication	10 / 100 Mbps Ethernet / RS485
Max. Communication Range	
RS485	1000m
Ethernet	100m
MPLC*	1000m
Communication Ports	
RS485	7
Ethernet	5 × 10/100Mbps ETH1/2: Ethernet port ETH3/4: Fast dispatch port ETH5: Reserved port
Digital input	16
Digital output	4
Built-in MPLC	1
PT100/PT1000	2
Analog input	4 (AI1□0~10 Vdc□AI2~AI4□4~20 mA)
Power Supply	
AC input	100V~277Vac, 50 / 60Hz
DC input	24Vdc, 1.25A
Power consumption	• Typ. 18W • Max. 30W
Environment	
Operating temperature	- 30°C~+60°C
Storage temperature	-40°C~+70°C

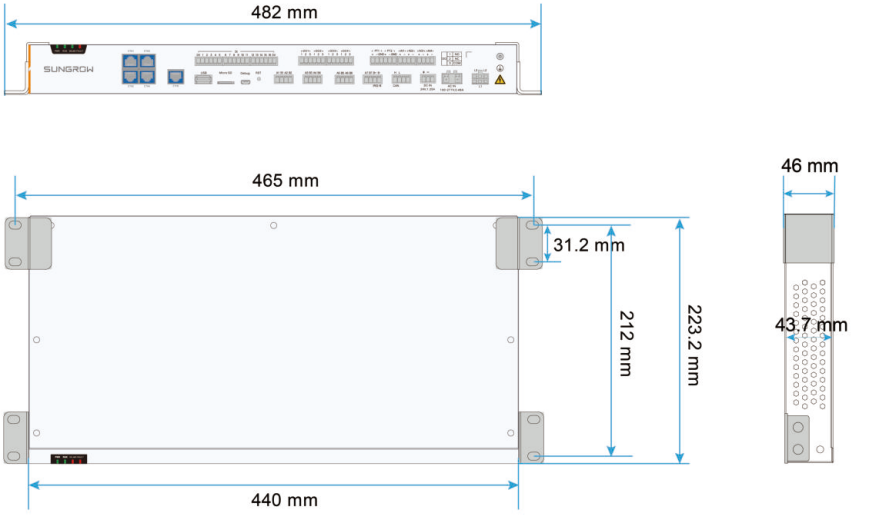
Operating humidity	≤ 95%, no condensation
Elevation	≤4000m
IP rating	IP20
Mechanical Parameters	
Dimensions (W x H x D)	440×44×224 mm
Weight	3 kg
Installation	Rack-mounting, wall-mounting

15 Appendix B: Related Drawings

Rack-Mounted Drawings



Wall-Mounted Drawings



16 Appendix C: General Information

16.1 Quality Assurance

Evidence

During the warranty period, the customer shall provide the product purchase invoice and date. In addition, the trademark on the product shall be undamaged and legible. Otherwise, SUNGROW has the right to refuse to honor the quality guarantee.

Conditions

- When product faults occur during the warranty period, SUNGROW will provide free repairs or replace the product with a new one.
- After replacement, unqualified products shall be processed by SUNGROW.
- The customer shall give SUNGROW a reasonable period to repair the faulty device.

In the following circumstances, SUNGROW has the right to refuse to honor the quality guarantee:

- The equipment is damaged during transport.
- The equipment is improperly installed.
- The equipment is improperly modified.
- The equipment is improperly used.
- The equipment operates under harsh conditions beyond those described in this document.
- The equipment is damaged by an abnormal natural environment.

16.2 Software Security Update Information

The software security update period is the same as the product warranty period. During the warranty period, software patches or security updates will be provided if security vulnerabilities or compatibility issues are identified.

After the software is officially released, upgrade plans will be tailored to each site's operating environment and business requirements and implemented as scheduled.

16.3 Contact Information

If you have any questions about this product, please reach out to us. In order to be more responsive and provide you with better service, please offer the following information:

- Model of the device
- Serial number of the device

- Fault code/name
- Brief description of the problem

HQ Tel: 0551 - 6532 7878 / 0551 - 6532 7877

For detailed information, see **https://www.sungrowpower.com/headquarter.html**.

SUNGROW

Sungrow Power Supply Co., Ltd.

www.sungrowpower.com

M-D-000287