SUNGROW
Clean power for all

User Cybersecurity Operation Manual

Logger4000

Contents

All Rights Reserved

1 About This Manual

This manual provides a detailed description of the security-related features of Logger4000 and specific operation instructions. For more information, visit **www.sungrowpower.com** or the website of the equipment manufacturer.

Scope of Application

- Logger4000

Product Model

Model	Product Aliases	Description
Logger4000	Data logger, device, and product	-

Target Group

This manual is intended for:

- Field maintenance personnel
- System administrator
- Field technical engineers

Manual Description

This manual uses the standard Logger4000 interface as an example to briefly introduce its safety and security functions. For specific supported functions, refer to the content of the technical agreement or the contract.

Security Disclaimer

To learn more about the product cybersecurity vulnerability disclosure and handling process, visit https://en.sungrowpower.com/security-vulnerability-management.

Symbols in the Manual

To ensure the safety of life and property for users when using the product and to improve the efficiency of product use, the manual provides relevant information, which is highlighted by the following symbols.

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, may lead to 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, can lead to device malfunctions or financial losses.

Indicates additional information, emphasized contents, or tips that may be helpful, e.g. to help you solve problems or save time.

2 Basic Safety Instructions

⚠ WARNING

Life-threatening hazards caused by failure to follow safety instructions and risks from leftover components
Ignoring the safety instructions and the risks from leftover components in the attached hardware documentation may result in serious injury or death.

- **Follow the safety instructions in the hardware documentation.**
- **Consider the risks from leftover components during risk assessments.**

⚠ WARNING

Machine failures caused by incorrect parameter settings or modifications
Incorrect parameter settings may cause machine failures, resulting in serious injury or death.

- **Take protective measures to prevent unauthorized parameter settings.**
- **Take appropriate actions (such as stop or emergency stop) to handle potential faults.**

3 Industrial Cybersecurity

3.1 Industrial Cybersecurity Overview

Industrial cybersecurity integrates all measures used to protect industrial control system (ICS) and operational technology (OT) environments. It is primarily aimed at achieving the following key goals:

- **Availability:** Ensure that systems, networks, and data are accessible and usable by authorized users when needed, preventing business interruptions caused by destruction, failures, or denial-of-service (DoS) attacks.
- **Confidentiality:** Prevent unauthorized access, theft, or leakage of sensitive data, configuration information, and network resources.
- **Integrity:** Prevent unauthorized tampering, destruction, or malicious manipulation of data and applications, ensuring their accuracy and reliability.

3.2 Industrial Cybersecurity Protection Objectives

- Ensure the fault-free operation and availability of production equipment and processes.
- Prevent cyberattacks from posing risks to personnel safety and production safety.
- Prevent unauthorized access to, manipulation of, or data loss from industrial automation systems and their components.
- Prevent industrial communication data from being intercepted or tampered with.
- Prevent unauthorized access to confidential data.

Ensure that security measures do not hinder or compromise the operability of automation systems and their components during implementation.

3.3 Industrial Cybersecurity Reference Standards

Industrial cybersecurity reference standards include IEC 62443, etc.

IEC 62443

The IEC 62443 series of standards aims to support the secure operation of ICSs, covering aspects such as design, implementation, and management. To this end, the standards define the requirements for component manufacturers, system integrators, and operators. Component manufacturers must ensure the security of their products, while equipment and system manufacturers are responsible for ensuring secure product interactions. Operators bear the ultimate responsibility for the security of the entire operational process.

The ISO/IEC 27001 standard contains various IT security rules. These two standards offer comprehensive protection for enterprises against cybersecurity threats.

4 DiD Strategy

A layered network approach incorporating multiple security and defense controls can be adopted in IT and control systems to minimize gaps in data protection, reduce single points of failure, and establish a robust cybersecurity posture. The more security layers present in the network, the harder it becomes for malicious users to breach defenses, access digital assets, or cause disruptions. This section introduces the defense-in-depth (DiD) strategy of Logger4000, along with related issues and solutions.

4.1 Threat Model

The product has been securely designed to minimize the security exposure at different layers, including but not limited to the following:

- Environmental layer: Provide security recommendations for users and engineering personnel during installation, such as secure and stable hardware mounting, perimeter protection measures, as well as secure, reliable network environments and power supply. For details, refer to the DiD Strategy for Deployment Environment section.
- Physical layer: The product has a rugged, enclosed housing and tamper-evident labels to help users verify product integrity.
- Operating system (OS) layer: A hardened operating system is provided, which includes OS configuration based on best practices, OS vulnerability patches, firewall and network configuration recommendations, user group-based access control, system backup mechanisms, and a reliable logging system.
- System component layer: Implement secure development processes, comprehensive security testing, etc.
- Data storage layer: Data is protected based on an access control list (ACL) and data access policies designed based on the principle of least privilege.
- Data transmission layer: Secure transmission is ensured by using widely proven data encryption transmission protocols.

4.2 Security-Related Functions and Usage Instructions

This section provides descriptions and recommendations for the following security-related functions and usage procedures:

Security Function	Description	Security Recommendations
Secure login	Multi-factor authentication, login failure lockout to prevent	Change passwords regularly.

Security Function	Description	Security Recommendations
	brute-force attacks, and login logging.	
User and password management	User addition, deletion, and modification, as well as password security policy configuration.	Enable the minimum number of necessary users and configure password policies appropriately.
Protocol configuration	Configuration management of northbound protocols such as Modbus, IEC104, and GOOSE	Enable protocols only as needed based on the minimization principle.
Certificate management	HTTPS certificate management	Update HTTPS certificates regularly.
Factory reset	Reset to factory settings and delete device data	Use this function with caution.
Security traceback	Operation log recording	Analyze security logs regularly.
Security updates	Software and firmware updates	Pay attention to product-related security announcements and update to the latest version in a timely manner.

The above security functions, as a whole, provide multi-layered and multi-dimensional protection for Logger4000 and its adjacent smart power distribution systems, including the physical environment, OS, and system components. This ensures the confidentiality, availability, and integrity of communication and data storage, as well as the auditability of user operations and access. Malware protection functions may need to be verified to meet validation requirements.

⚠ WARNING

Possible damage to system availability, integrity, and confidentiality

- **Do not use real malware for malware protection testing.**
- **Do not download any antivirus test files from untrusted sources.**
- **Do not perform malware protection testing on production systems.**

Failure to follow these instructions may result in device damage, sensitive data leakage, or permanent data loss.

4.3 Protection Scope of DiD Strategy

The security functions of Logger4000 collectively form its DiD architecture. Within the security context defined for Logger4000, these functions provide fundamental protection against threats such as spoofing, tampering, repudiation, information disclosure, and DoS.

4.4 User Mitigation Measures

Device Security

When vulnerabilities exist in an enterprise's physical security, unauthorized personnel may gain access to the production environment, damage or modify production equipment, leading to the loss of confidential information. Therefore, appropriate measures must be taken to protect enterprise premises and critical production areas.

- Implement dedicated access control for critical production areas.
- Install important components in lockable control cabinets/rooms.
- Control cabinets/rooms must be equipped with proper locks and have monitoring and alarm systems. Do not use structurally simple locks such as universal keys, triangle locks, square locks, or double-bit locks.
- Protect power cables and data cables.
- Protect the current and data flow between the product and other drive components against malicious manipulation, such as cable cutting.
- Carefully plan and deploy the wireless local area network (WLAN), ensuring its coverage range does not exceed the specified boundaries.
- Provide instructions for mobile data storage media (e.g., USB drives and memory cards).
- Provide instructions for operator units such as programmers (PGs), PCs, or mobile terminals.

Cybersecurity

Cybersecurity covers all measures involved in its planning, implementation, and monitoring. It includes security reviews of all interfaces, such as those between the office network and the automation network, or for remote maintenance access.

- Network isolation needs to be implemented, through a firewall in the simplest case. This firewall can control and inspect communication between different networks.
- It is recommended to deploy anti-malware devices.

System Integrity

System integrity refers to both the intactness and accuracy of data and the proper functioning of the system. Measures to ensure system integrity help prevent unauthorized manipulation of data and system functions and allow monitoring of data/function manipulation attempts.

- Only enable necessary services and ports. Disable all unused ones.
- Use secure login passwords for user accounts. The passwords must be at least 8 characters long and contain at least three of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters.
- Minimize the number of user accounts to the minimum required. Disable or delete unused user accounts.
- Assign only the necessary permissions to user accounts.
- Regularly back up sensitive data. Ensure backups are properly secured to prevent unauthorized access, data loss, or manipulation.
- Keep informed about new product security announcements and follow the instructions accordingly.

5 DiD Strategy for Deployment Environment

This product is designed to operate within a local area network (LAN), with built-in safeguards to minimize risks from malicious devices on the network.

As with any security strategy, overall system protection depends on coordinated efforts. Users must take necessary steps to allow only trusted and verified devices to connect to the local network, and implement protective measures to ensure stable device operation. Such devices include, but are not limited to, switches, routers, power supplies, communication management units, communication cables, and power cables. Recommended protective measures include, but are not limited to, perimeter defenses, backup power systems, and redundant network configurations.

- Logger4000 is designed to be installed in a secured and enclosed physical area equipped with access control and surveillance measures, such as door locks and electronic access control systems. It should not be deployed in areas without access control.
- The Logger4000 is intended for environments with reliable power supply (e.g., UPS). Otherwise, issues such as information leakage, system malfunction, power distribution failures, or power outages may occur.
- Customers are responsible for ensuring proper access control to the installation area.
- Customers must follow the account management guidelines provided in this manual. For details, refer to the User Management section.
- For descriptions and recommendations regarding security-related tools and usage procedures, refer to the Security-Related Functions and Usage Instructions section.

5.1 Securing Deployment Environment

- **Cybersecurity Governance:** Ensure compliance with the latest guidelines on the use and management of company information and technical assets.
- **Perimeter Security:** Installed and inactive devices must be located in access-controlled or monitored areas.
- **Backup Power Supply:** Control systems must support seamless switching between primary and backup power sources without compromising security status or the recorded degraded operation modes.
- **Software and Firmware Updates:** Software and firmware must be updated to the latest version promptly.
- **Malware Control Measures:** Detection, prevention, and recovery mechanisms must be in place to defend against malware attacks and raise user awareness.
- **No Public Internet Access:** Internet access from control systems must be avoided. For remote connections, encrypted protocol transmissions must be used.

- **Resource Availability and Redundancy:** Systems must be capable of isolating different network segments or using redundant equipment to respond to incidents.
- **Control System Backup:** The system must maintain up-to-date backups for rapid recovery in the event of a control system failure.

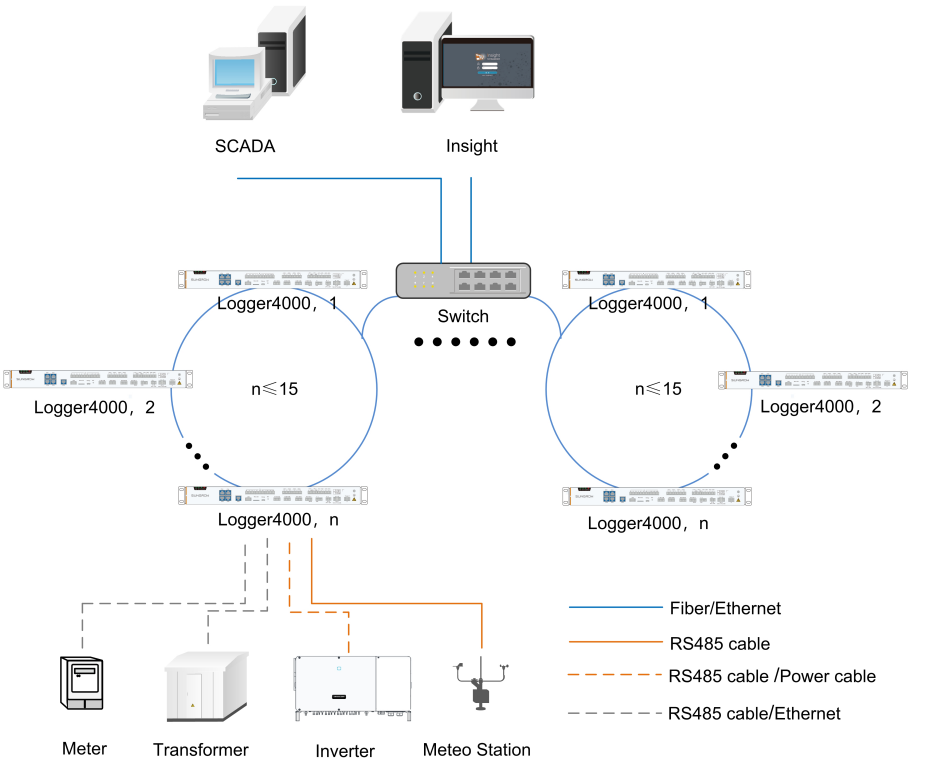
5.2 Potential Risks and Compensating Control Measures

Take the following compensating control measures to address potential risks:

Area	Issue	Risk	Compensating Control Measures
Security protocols	Insecure communication protocols are not allowed for transmitting encrypted data.	Malicious users may intercept communications if they gain network access.	For data transmission over internal networks, use physical or logical network segmentation. For data transmission over external networks, use virtual private networks (VPNs) or similar solutions to encrypt all protocol transmissions over external connections.

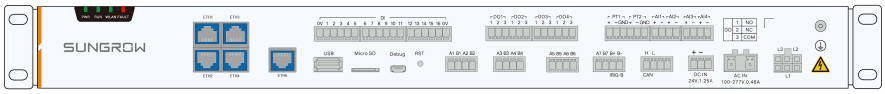
6 Product Functions and Deployment Overview

Logger4000 is a data logger that supports data collection, networking, and energy management for utility plants. It supports connections of southbound devices via the Modbus protocol and power line communication (PLC). It can collect data from southbound devices and forward data northbound to integrated automation systems, plant control systems, or iSolarCloud using communication protocols such as IEC 104, Modbus, MQTT, and GOOSE. It can also receive remote dispatch commands from northbound systems or execute local dispatch commands to regulate the active power and reactive power of connected inverters.



7 External Interface Description

The layout and identifiers of the data logger are shown below.



Identifier	Name	Recommended Cable	Description
ETH1–ETH2	Ethernet port	-	Used for data exchange. It can be connected to the background master via devices such as a router or switch
ETH3-ETH4	Fast dispatch port	-	Used for fast active and reactive power dispatch using the GOOSE protocol
ETH5	Ethernet port	-	Reserved for the master-standby feature
DI	Digital input	0.75 mm^2 outdoor anti-ultraviolet wire	Passive dry contact input
USB	USB port	-	Reserved
Micro SD	SD port	-	Used for software flashing (this port is only available for Sungrow technicians)
Debug	Serial port for debugging	-	Used for debugging the data logger
RST	Reset port	-	Press and hold (> 30s) to restart the data logger and restore factory settings Short press (< 3s). This function is reserved

Identifier	Name	Recommended Cable	Description
DO1–DO4	Digital output	0.75 mm^2 outdoor anti-ultraviolet wire	Relay output Relay specifications: 250 Vac / 1 A or 30 Vdc / 1 A
PT1, PT2 AI1–AI4	Analog input	0.75 mm^2 outdoor anti-ultraviolet wire	PT100/PT1000 detection range: -30°C to 120°C Two-wire or three-wire connection method AI1: 0–10 Vdc AI2–AI4: 4–20 mA
A1B1–A7B7	RS485 communication interface	2 × (0.75 to 1.5) mm^2 outdoor anti-ultraviolet twisted pair with a shielding layer	Provide 7 positions for RS485 wiring It can be connected to slave devices or background
IRIG-B	Used for IRIG-B time synchronization	-	Reserved
DC IN 24 V, 1.25 A	24 V DC power port	0.75-1.5 mm^2 outdoor anti-ultraviolet wire	Current ≤ 1.25 A. The switch mode power supply used by this port must be properly insulated.
AC IN 100–277 V, 0.48 A	AC power supply port	0.75-1.5 mm^2 outdoor anti-ultraviolet wire	Used for connecting 100-277 Vac (50/60 Hz), current ≤ 0.48 A
⏚	Grounding hole	1-1.5 mm^2 outdoor anti-ultraviolet wire	Used for connecting protective grounding cable
L1, L2, L3	MPLC communication port	0.5–0.75 mm^2, with a cable withstand voltage of ≥1000 V to ground	It can be connected to string inverters with MPLC communication functionality

AC Power Supply Port and MPLC Communication Port

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

DI/DO Ports

The digital input (DI) and digital output (DO1–DO4) ports are used to collect contact data and control contact communication.

RS485 Communication Port

The RS485 communication ports (A1B1–A7B7) support a maximum communication distance of 1000 m.

8 Port Matrix

Source Device	Source Port	Destination Device	Destination Port	Protocol	Authentication Method	Encryption Method	Description
PC	Any	Logger 4000	8080	HTTP	Username and password	None	Disabled by default. It can be enabled.
PC	Any	Logger 4000	8443	HTTPS	Username and password	TLS/SSL	Default access method.
PC	Any	Logger 4000	220	SSH	Username and password	TLS/SSL	Disabled by default.
Northbound device	Any	Logger 4000	2024–2048	IEC104	None	None	Disabled by default. A security warning will be displayed when it is enabled. It is

Source Device	Source Port	Destination Device	Destination Port	Protocol	Authentication Method	Encryption Method	Description
							accessible via network port or serial port.
Northbound device	Any	Logger 4000	502–516	Modbus	None	None	Disabled by default. A security warning will be displayed when it is enabled. It is accessible via network port or serial port.
PC	Any	Logger 4000	9998–9999	UDP	None	None	Disabled by default. It is used for internal debug

Source Device	Source Port	Destination Device	Destination Port	Protocol	Authentication Method	Encryption Method	Description
							ging and can be enabled in Linux shell.
PC	Debug port	Logger 4000	/	RS232	Username and password	TLS/SSL	Support access to Linux via serial port.
Logger 4000	Any	iSolar Cloud	19999	MQTT	Public key	None	Disabled by default. A security warning will be displayed when it is enabled. It is accessible via network port.
Logger 4000	Any	iSolar Cloud	16668	MQTT	Public key	TLS/SSL	Disabled by default. A

Source Device	Source Port	Destination Device	Destination Port	Protocol	Authentication Method	Encryption Method	Description
							security warning will be displayed when it is enabled. It is accessible via network port.
Logger 4000	Any	NTP server	123	NTP	None	None	Disabled by default. A security warning will be displayed when it is enabled.

9 User list

The administrator can assign different accounts and permissions to different users, which thus enhances the system security, improves operation efficiency for users, and lowers management costs. Three types of accounts are available in this system: administrator, O&M user, and developer. Their account names, default passwords, and permissions are as follows:

Table 9-1 Web User Accounts

User Type	Username	Default Password	Permissions
Administrator	administrator	pw1111	Add/delete a user, modify user information, empty users, login management, enable or disable R&D debugging.
O&M user	maintain	pw@111111	Operations mentioned in this manual.
Developer	develop	Obtain the SN based on customer authorization to generate dynamic passwords.	After being authorized by the administrator, complex device faults can be located and troubleshooted.

Table 9-2 System User Accounts

Username	Default Password
root	sungrow2016
sg	Sungrow@2023

10 User Management

The administrator can assign different accounts and permissions to different users, which thus enhances the system security, improves operation efficiency for users, and lowers management costs.

User Management

- In addition to the "maintain" account, the administrator can create up to 4 more O&M user accounts. Do not create a large number of users unless necessary to prevent issues such as multiple people competing for device operations or unauthorized operations due to password leaks.
- If suspicious user behavior is detected, log in as the Administrator to delete the user and immediately revoke their access permissions.
- If a user password is found to be leaked, you can log in as the Administrator to change the user password.
- The added username must be 4 to 16 characters long, start with a letter, and can contain uppercase letters, lowercase letters, numbers, and underscores.

The administrator can set the validity period of passwords based on the user type, in the range of 1–90 days. The validity period is calculated by rounding up. For example, if the validity period displayed is 3 days, the actual remaining time is between 2 and 3 days.

Password Usage Security

- All passwords must meet strong complexity requirements. The default password needs to be changed upon first login. The password must be 8 to 32 characters long and contain at least three of the following four character types: uppercase letters, lowercase letters, numbers, and special characters.
- Change passwords promptly upon expiration.
- If you find a password has been compromised, change it immediately. Do not reuse old passwords. The system only checks whether the new password is identical to the old one. Do not use the same password across accounts.

Session Management

Parameter	Default value	Range	Description
Number of illegal visits	6	3-6	Set the maximum number of allowed failed login attempts. If failed login attempts due to incorrect

Parameter	Default value	Range	Description
			passwords exceeds this number, the account will be locked out.
Session timeout	10	10-30	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.
User lock time	10	10-30	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.

11 Guidelines for Safely Removing Products

The guidelines for safely removing reference and configuration data stored in the environment and safely removing the product are as follows:

- Before safely removing the product, refer to 12 Security Configuration Guide.
- To dispose of the device, refer to 12.4 Factory Reset and destroy it through safe channels to ensure that the device is not redeployed to the user's operational system or misused.

12 Security Configuration Guide

12.1 Deployment Security

The product's northbound interfaces necessitate a strong security focus. Users need to deploy security devices, such as firewalls, anti-malware devices, and intrusion detection system (IDS), at the northbound data egress of their network environment to build a secure northbound network.

The southbound devices are typically deployed within the local network, which is relatively secure but not absolutely risk-free. The following recommendations are provided:

- Use independent switches for the northbound and southbound networks to achieve network isolation.
- Southbound devices are considered third-party devices to this product. Users are responsible for ensuring these devices do not pose network security risks.

12.2 Protocol Configuration

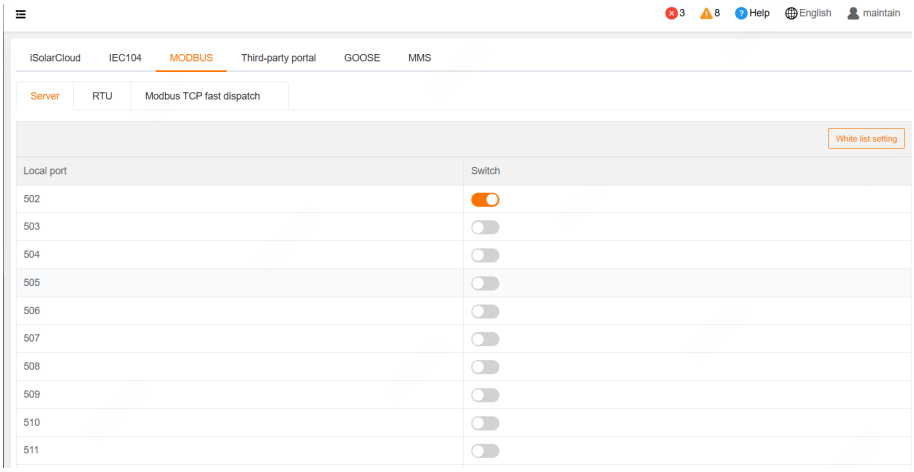
- Insecure protocols such as MODBUS, IEC104, and GOOSE are disabled by default.
- Northbound MODBUS, IEC104, and GOOSE protocols can be manually enabled. You can navigate to the **System > Forwarding configuration** page, and select the **IEC104**, **MODBUS**, or **GOOSE** tab to enable the corresponding port or function.

  MODBUS, IEC104, and GOOSE are insecure protocols. Please ensure the network environment is secure before using them.

- Disable unused protocol forwarding services promptly to prevent security incidents caused by insecure protocols.

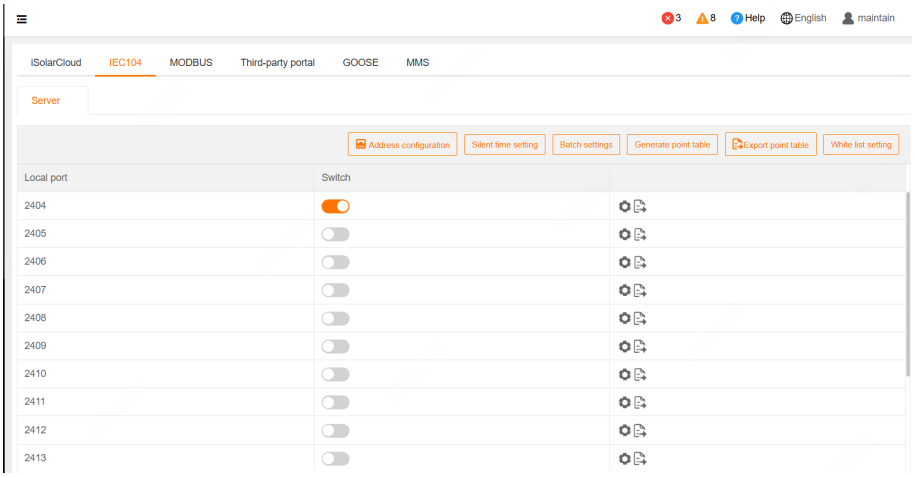
Modbus

Log in to the Logger4000 Web. Choose **System > Forwarding configuration**, click the **MODBUS** tab, and enable the corresponding local port.



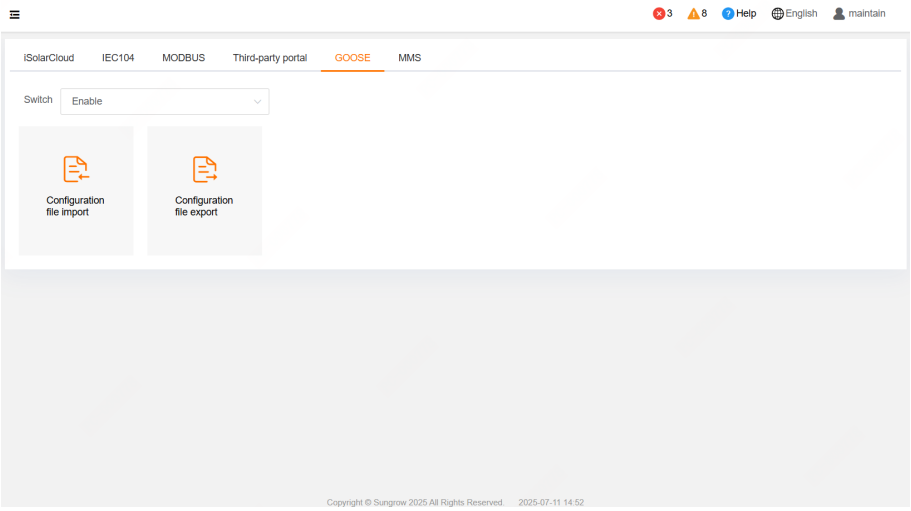
IEC104

Log in to the Logger4000 Web. Choose **System > Forwarding configuration**, click the **IEC104** tab, and enable the corresponding local port.



GOOSE

Log in to the Logger4000 Web. Choose **System > Forwarding configuration**, click the **GOOSE** tab, and enable the switch.



12.3 Certificate Management and Maintenance

12.3.1 Pre-Configured Certificate Risk Statement

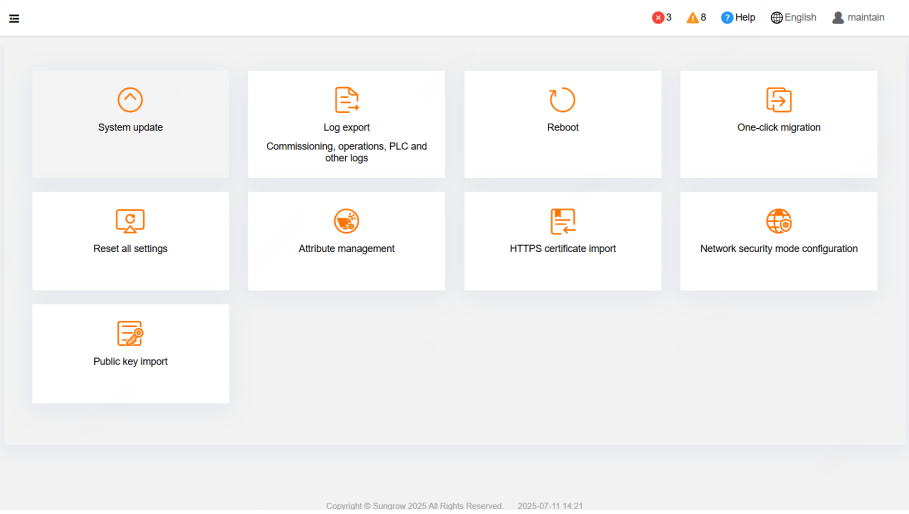
Certificates are pre-configured on Sungrow devices during the manufacturing process as their necessary identity credentials. Regarding the use of these pre-configured certificates, please note the following:

- Pre-configured certificates are only used to establish an initial secure channel for the device to access the customer network during the deployment process. Sungrow does not promise or guarantee the security of the pre-configured certificates.
- Sungrow does not promise or guarantee the security of the pre-configured certificates when used in services. It is recommended that users replace them with their own secure certificates.
- The validity period for HTTPS certificates pre-configured by Sungrow is 25 years.
- If users choose to use their own certificates, it is recommended that they properly manage the certificate lifecycle. Certificates with a short validity period are recommended to ensure security.

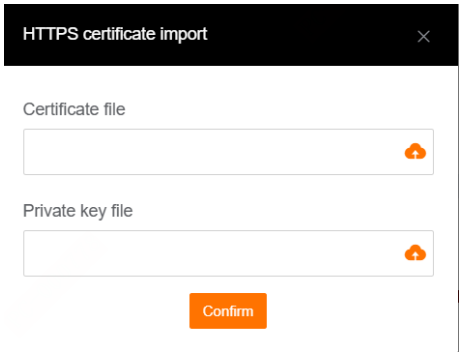
12.3.2 Secure Certificate Handling

Use the HTTPS protocol to connect to the device to ensure channel security.

1. Log in to the Logger4000 Web and choose **System > System maintenance**.



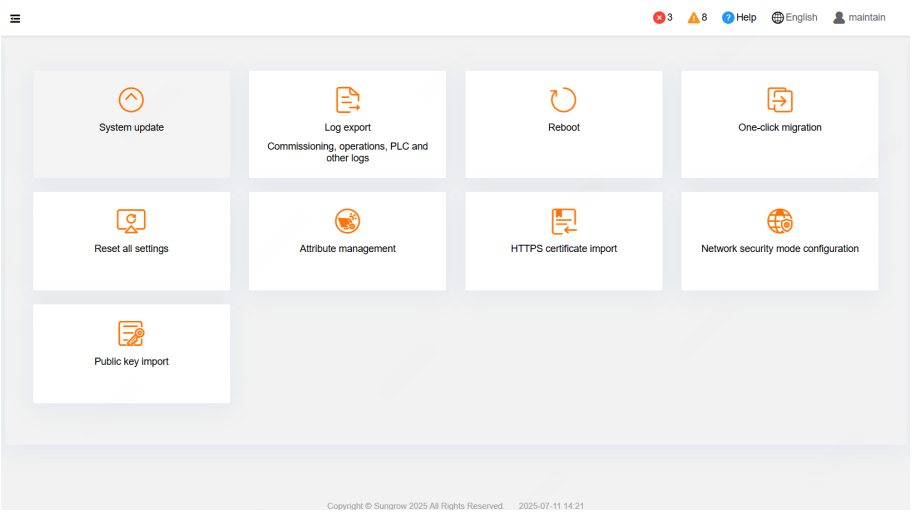
2. Click **HTTPS Certificate Import** to import certificate and private key files to the system.



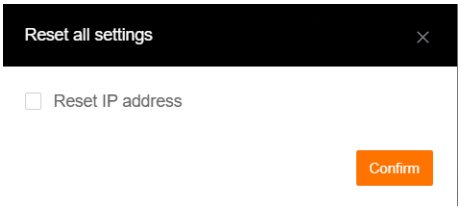
12.4 Factory Reset

If you find that the device is abnormal or its configuration has been maliciously tampered with, use the Reset all settings function to factory reset the device.

1. Log in to the Logger4000 Web and choose **System > System maintenance**.



2. Click **Reset all settings**, select **Reset IP address** in the pop-up dialog box, and then click **Confirm**.



12.5 System Restoration

If the device has been attacked and cannot function properly, contact Sungrow O&M personnel to re-flash the system through an SD card for restoration.

12.6 Security Traceback

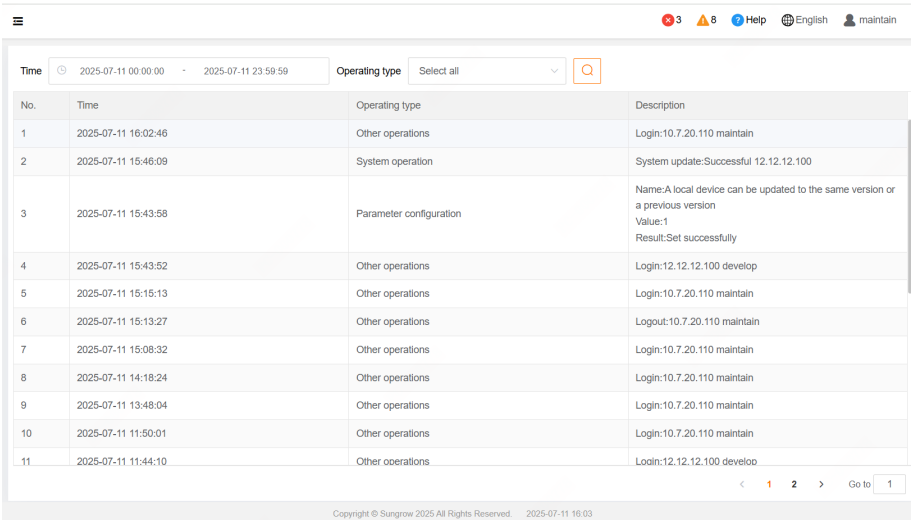
For security incidents that have already occurred, you can view the key operation records of each user on the Operation log page for traceback purposes. Alternatively, you can contact Sungrow O&M personnel to access the device backend, analyze the impact of the security incidents, assess risks, and formulate mitigation measures.

User Type	Operation	Information Recorded
All users	Login and logout	Username and user IP
System administrator	All operation logs, including but not limited to: add/delete an user, modify user information, empty users, login	Operating type, target object, settings made, and results

User Type	Operation	Information Recorded
	management, enable or disable R&D debugging.	
O&M user	Visits and key operations: • User login • System update • Import/export for one-click migration • Certificate import	Time, type, and details of operation

Search for Operation Logs

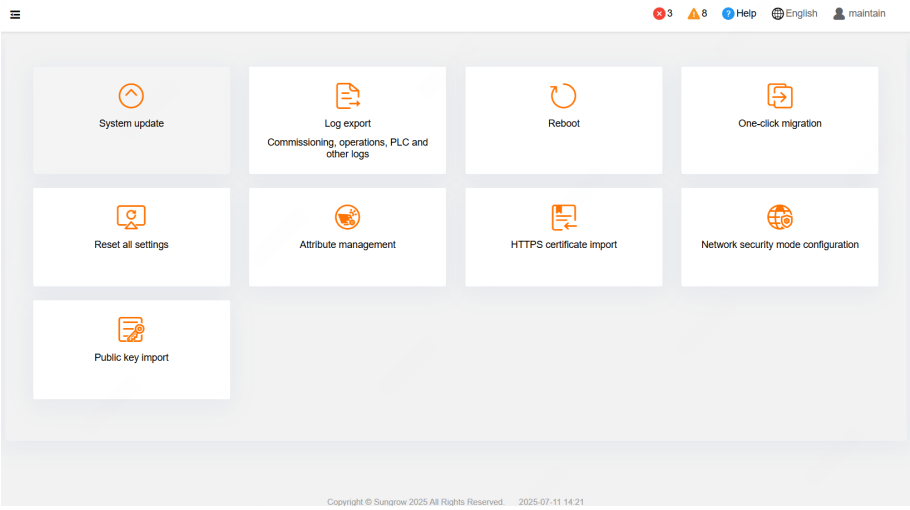
Log in to the Logger4000 Web. Choose **History data > Operation log** and view the operation logs. You can filter log records by the time range and operation type.



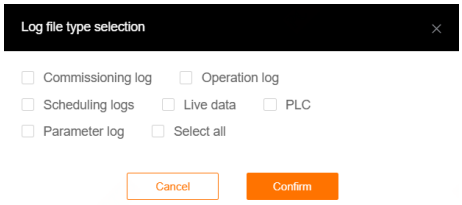
You can also contact Sungrow O&M personnel to log in to the device's backend to assess the impact of the security incident and provide appropriate solutions.

Export Operation Logs

1. Log in to the Logger4000 Web and choose **System > System maintenance**.



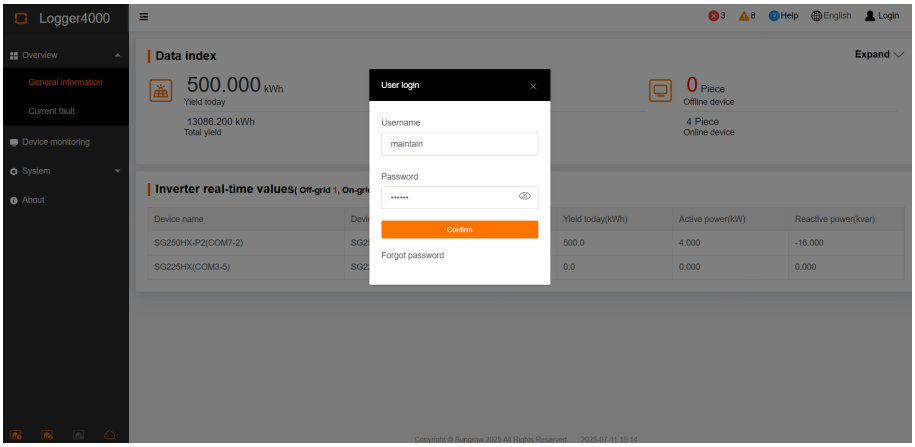
2. Click **Log export**, select **Operation log** in the **Log file type selection** window, and click **Confirm**.



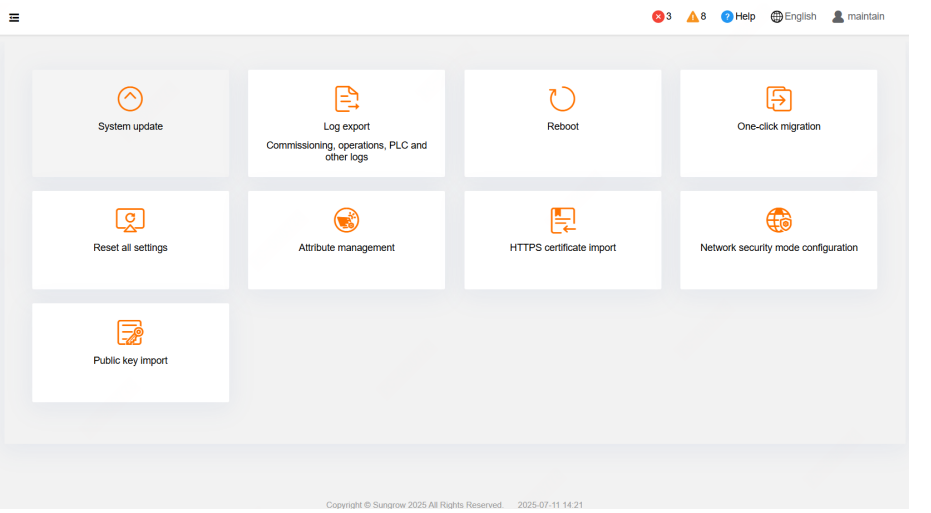
12.7 Security Updates

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.

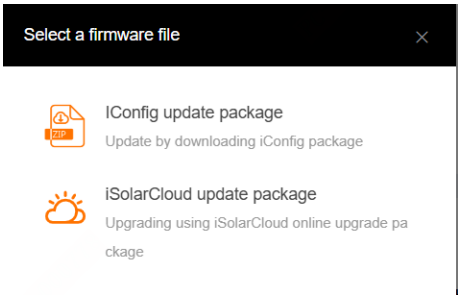
1. Log in to the Logger4000 Web, enter the username and password, and click **Confirm**.



2. After logging in to the homepage, choose **System > System maintenance**, and click **System update**.



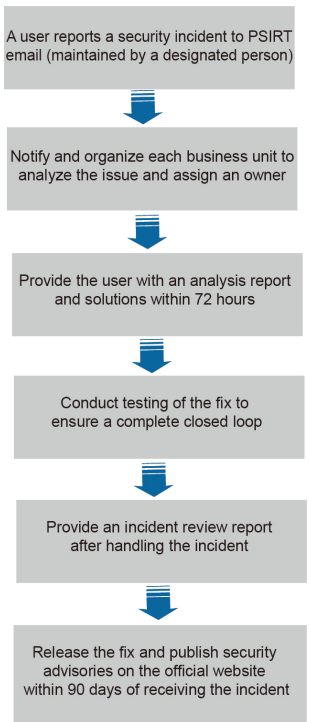
3. In the **Select a firmware file** pop-up dialog box, select an update method. The system will verify the device compatibility based on the update file.



4. On the **Firmware update** page, select the devices to be updated and click **Update**. After the update is completed, users can check the information such as the current version number, target version number, and update time.

13 Instructions for Reporting Product (Module) Security Incidents

The product security emergency response process is as follows:



If you discover a vulnerability in the product or a security risk in a module, click https://en.sungrowpower.com/security-vulnerability-management to visit the SUNGROW PSIRT page. On this page, you can click **More** to enter the details page, where you can view the list of security-related documents and vulnerability bulletins, or report security issues via email.

If the product security vulnerability has been fixed and a new version is available, you can update to the new version to fix the vulnerability on the **System > System Maintenance > System Update** page.

SUNGROW

Sungrow Power Supply Co., Ltd.

www.sungrowpower.com