FunsionSolarDG
V100R002C00SPC127

Security Maintenance Guide

Issue	04
Date	2024-01-12

HUAWEI DIGITAL POWER TECHNOLOGIES CO., LTD.

Copyright © Huawei Digital Power Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Digital Power Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Digital Power Technologies Co., Ltd. and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied. The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Digital Power Technologies Co., Ltd.

Address: Huawei Digital Power Antuoshan Headquarters

Futian, Shenzhen 518043

People's Republic of China

Website: https://digitalpower.huawei.com

Change History

Issue	Date	Description
04	2024-01-12	This issue is the fourth official release.
03	2023-10-10	This issue is the third official release.
02	2023-05-05	This issue is the second official release.
01	2021-02-08	This issue is the first official release.

 Copyright © Huawei Digital Power Technologies Co., Ltd.

Contents

Change History ii

1 Security Assurance Overview 1

2 Device Layer Security 2

2.1 Mobile Phone App Maintenance 2
2.1.1 Maintenance Suggestions 2
2.1.2 Procedure 2
2.1.3 Troubleshooting 4
2.2 Inverter WiFi Maintenance 4
2.2.1 Maintenance Suggestions 4
2.2.2 Procedure 5
2.3 Certificate Replacement 6
2.4 Management System Maintenance 10
2.4.1 Maintenance Suggestions 10
2.4.2 Procedure 10
2.5 Serial Port Maintenance 11
2.6 Restoring the Default Password 11
2.7 Log Maintenance 12
2.7.1 Maintenance Suggestions 12
2.7.2 Procedure 12
2.8 Outer Integrity Check 16

1 Security Assurance Overview

Photovoltaic (PV) operators need to establish a security assurance mechanism to ensure that their application systems operate properly in a secure environment.

Application systems are now exposed to increasingly severe security threats, which may result in power production interruption, revenue loss, or system breakdown. Therefore, PV operators need to build and maintain security mechanisms for application systems at several layers to early detect and handle any possible security issues.

These threats cannot be all prevented by technology. To address these issues, PV operators need to establish a security management system based on security assurance suggestions and security issues found in routine maintenance, thereby ensuring that application systems operate securely and properly.

 Copyright © Huawei Digital Power Technologies Co., Ltd.

2 Device Layer Security

2.1 Mobile Phone App Maintenance

2.1.1 Maintenance Suggestions

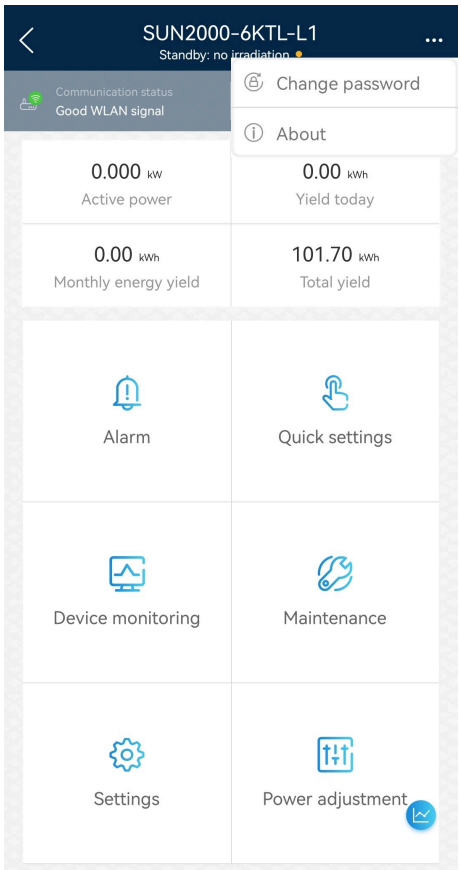
- Avoid using the preset password or low-complexity passwords that are prone to attacks and cracking by unauthorized users, which will affect the device security. To ensure system security, maintenance engineers need to confirm that the password length and complexity meet requirements when changing passwords. A password must meet the following requirements:
  - The password must contain at least 8 characters.
  - Can contain digits, uppercase letters, and lowercase letters.
- Change the password immediately after logging in to the mobile phone app for the first time. The preset passwords for **user** and **installer** are both **00000a**.
- A password that has been used for a long time is likely to be stolen or cracked, and the risk increases along with the time of use. Change the password at least once every six months.
- For security, you are advised to disable data connection when using the mobile phone app to connect to a SUN2000MA.
- You are advised to use a mobile phone that has not been rooted to reduce the risk of information leakage.
- Mobile phone logs are saved in the app directory. Export and back up mobile phone logs when you need to use them.

2.1.2 Procedure

To change the user password on the mobile phone app screen, perform the following steps:

Step 1 On the Operation Console screen, tap Change password to access the Change password screen.

Figure 2-1 Operation Console

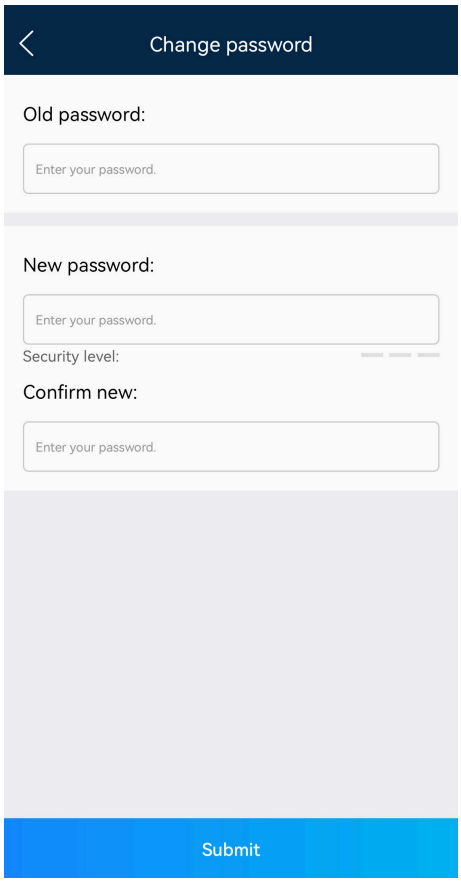


NOTE

The login user for all the screenshots in this document is **installer**.

The Change password screen is displayed.

Figure 2-2 Change password



Step 2 Specify Old password, New password, and Confirm new, and then tap COMMIT.

NOTE

Ensure that the confirm password is the same as the new password. Otherwise, an error message will be displayed.

----End

2.1.3 Troubleshooting

Keep the password properly. The system cannot be logged in without the correct password.

2.2 Inverter WiFi Maintenance

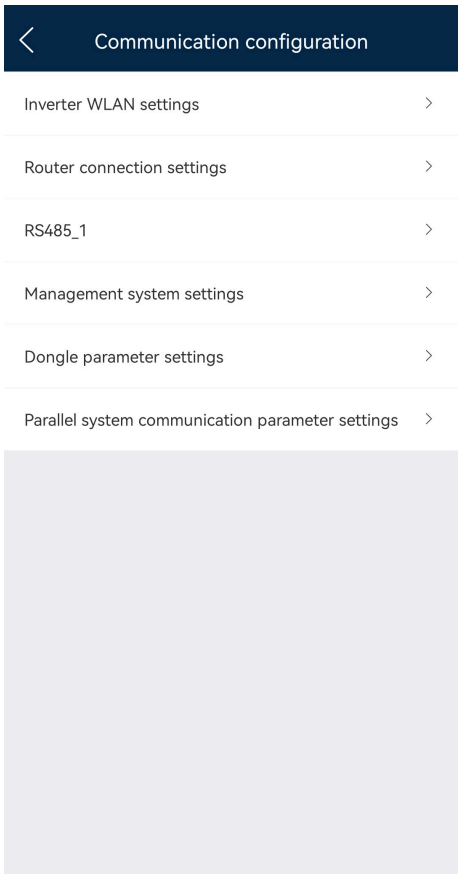
2.2.1 Maintenance Suggestions

- Avoid using the preset password or low-complexity passwords that are prone to attacks and cracking by unauthorized users, which will affect the device security. To ensure system security, maintenance engineers need to confirm that the password length and complexity meet requirements when changing passwords. The password must contain 8–64 characters.

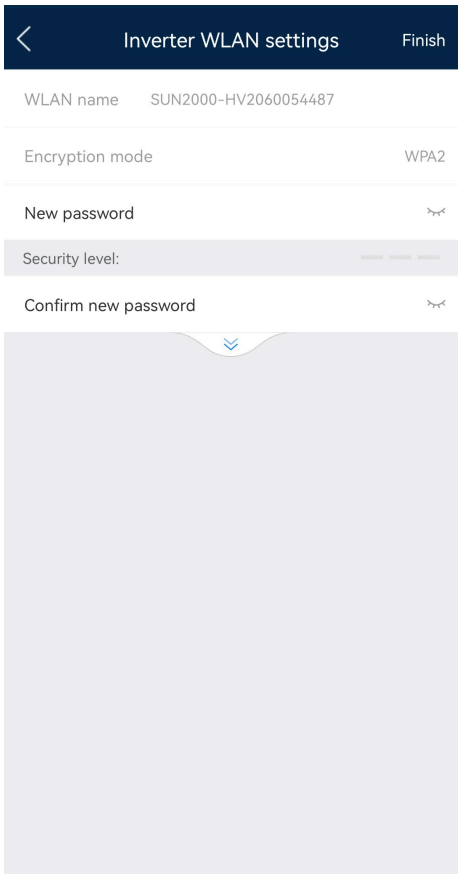
- Use the initial password **Changeme** to connect to WiFi for the first time. To ensure account security, change the password immediately after login.
- The encryption and authentication modes for the inverter WiFi are WPA2 (which is of high security level) by default and cannot be modified.
- A password that has been used for a long time is likely to be stolen or cracked, and the risk increases along with the time of use. Change the inverter WiFi password at least once every six months.

2.2.2 Procedure

Step 1 On the Operation Console screen, tap Comm config to access the Comm config screen.



Step 2 On the Comm config screen, tap Inverter WiFi settings to access the Inverter WiFi settings screen.



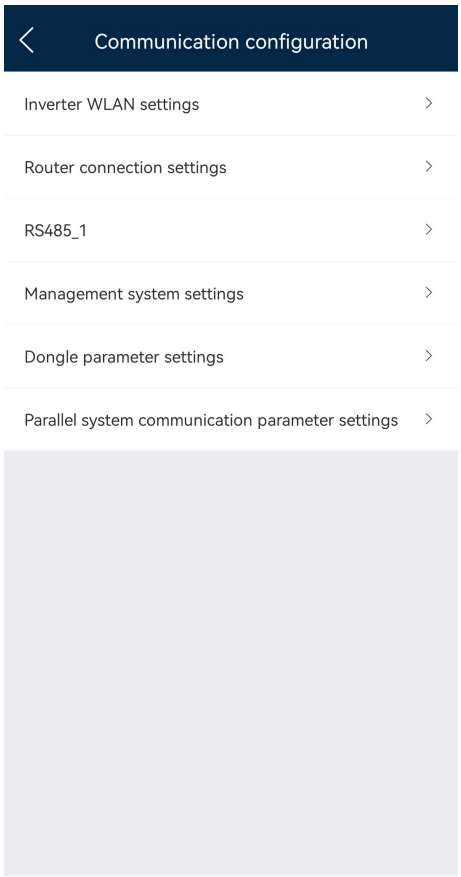
Step 3 Set the inverter WiFi password and tap Finish.

----End

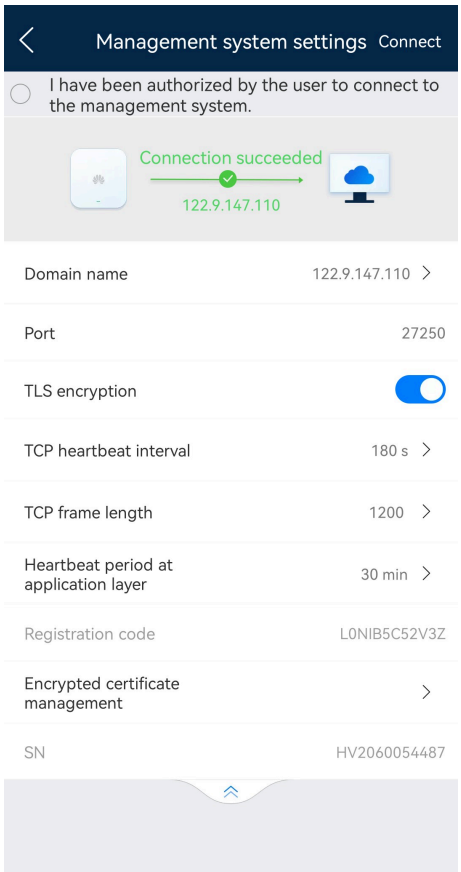
2.3 Certificate Replacement

To replace the certificate file used for connecting to the remote network management system (NMS) over the mobile phone app, perform the following steps:

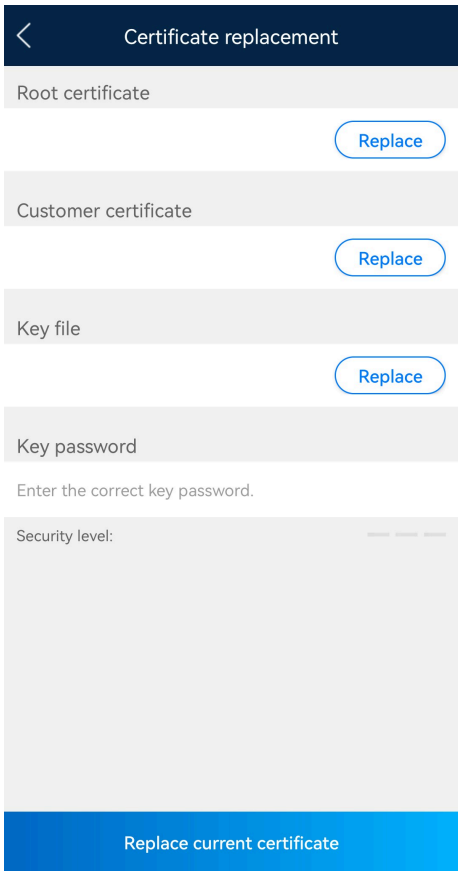
Step 1 On the Operation Console screen, tap Comm config to access the Comm config screen.



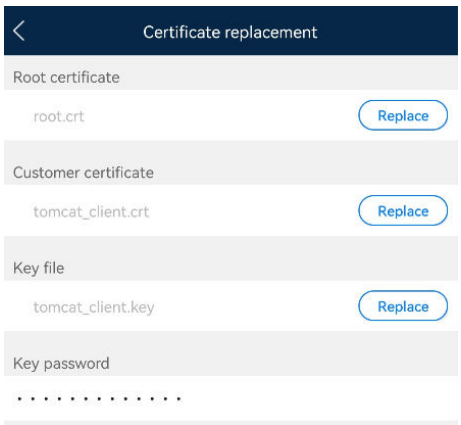
Step 2 On the Comm config screen, tap Management system setting to access the Connect to mgmt syst screen.



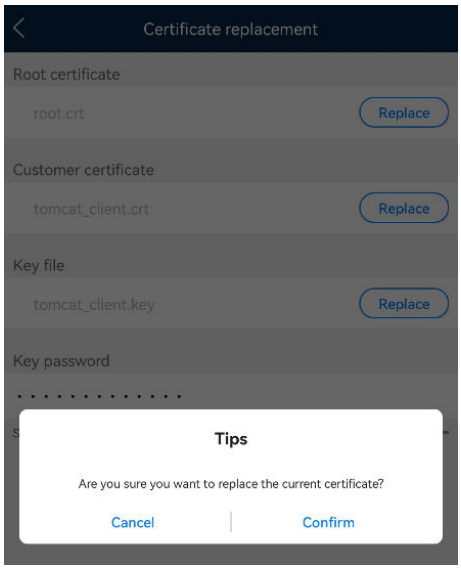
Step 3 On the Connect to mgmt syst screen, tap Encrypted certificate mgmtto access the Certificate replacement screen.



Step 4 Tap Replace after Root certificate, and select the appropriate root certificate file. Perform the same operations to select the appropriate customer certificate and private key certificate files, specify Key password, and then tap Replace current certificate.



Step 5 Tap Confirm to replace the certificate. If you want to exit the certificate replacement operations, tap Cancel.



Step 6 After the certificate is replaced successfully, the "Replacement succeeded" message is displayed. Then connect the SUN2000MA to the management system and check the correctness of the certificate.

NOTE

For security purposes, do not use secure hash algorithm 1 (SHA1) or Hash algorithm which is of low strength as the certificate signature algorithm, and ensure that the Rivest-Shamir-Adleman (RSA) key is greater than 1024 and the elliptic curve cryptography (ECC) key is greater than 256.

----End

2.4 Management System Maintenance

2.4.1 Maintenance Suggestions

- A security certificate is preset for the **Inverter** to ensure that the data exchanged with the management system is encrypted using SSL. The **Inverter** supports replacement of the management system certificate. If the certificate needs to be replaced, update it on both the management system and the **Inverter**.
- The user name of the management system is **emscomm**, and the initial password is **/EzFp+2%r6@IxSCv**. Change the password upon the first login to ensure system security.

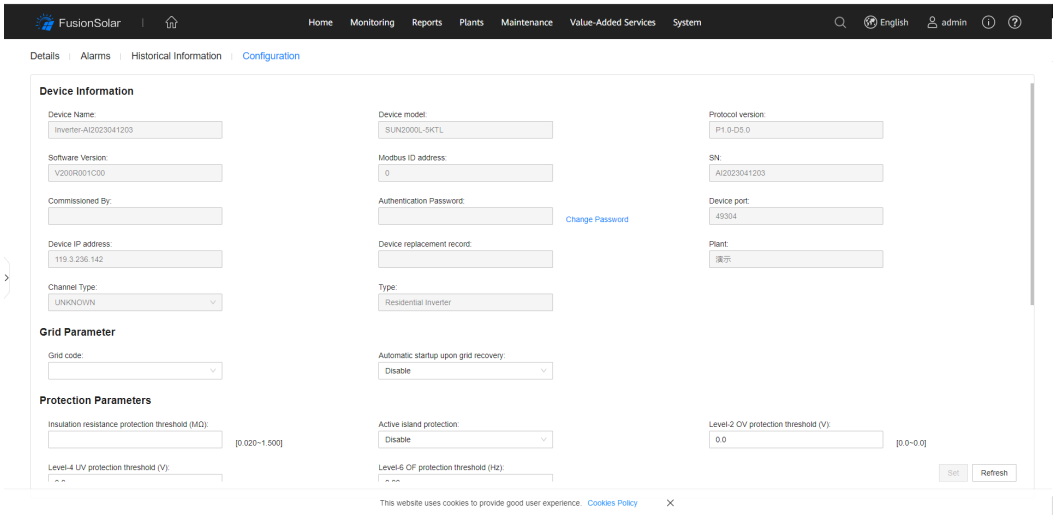
2.4.2 Procedure

To change the inverter password, perform the following steps:

Step 1 Log in to the NMS.

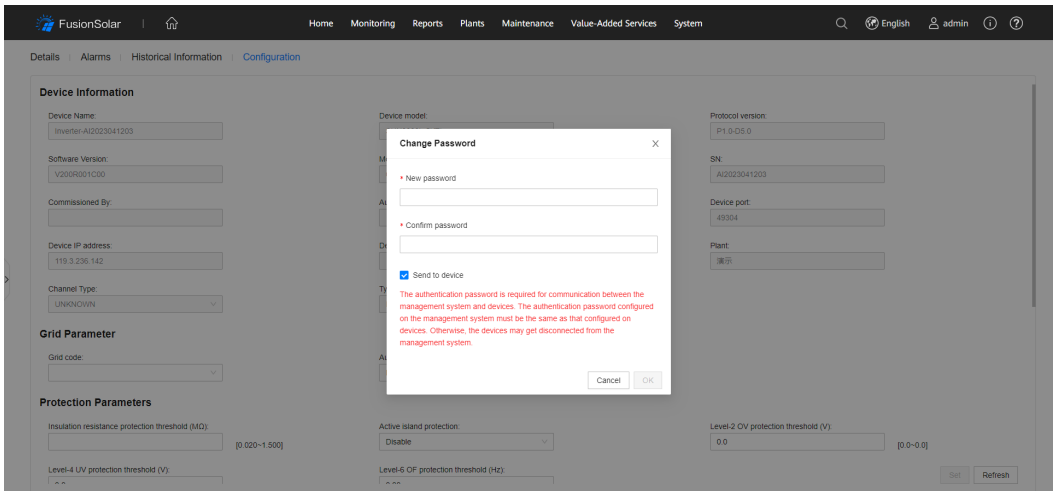
Step 2 Open the home page of the NMS, select the ESN of the inverter to be operated, and click Configure.

Figure 2-3 Home page of the NMS



Step 3 Set a new password and confirm the setting.

Figure 2-4 NMS password resetting page



----End

2.5 Serial Port Maintenance

The commissioning serial port has been removed.

2.6 Restoring the Default Password

Step 1 Ensure that the SUN2000 connects to the AC and DC power supplies at the same time. Indicators **=[** and **]~** are steady green or blink at long intervals for more than 3 minutes.

Step 2 Perform the following operations within 4 minutes:

- Turn off the AC switch and set the DC switch at the bottom of the SUN2000 to OFF. If the SUN2000 connects to batteries, turn off the battery switch. Wait until all the LED indicators on the SUN2000 panel turn off.
- Turn on the AC switch, set the DC switch to ON, and wait for about 90s. Ensure that the indicator **]~** is blinking green slowly.
- Turn off the AC switch and set the DC switch to OFF. Wait until all LED indicators on the SUN2000 panel are off.
- Turn on the AC switch and set the DC switch to ON. Wait until all indicators on the solar inverter panel blink and turn off 30 seconds later.

Step 3 Reset the password within 10 minutes. (If no operation is performed within 10 minutes, all inverter parameters remain unchanged.)

- Wait until the indicator **]~** blinks green at long intervals.
- Obtain the initial WLAN hotspot name (SSID) and initial password (PSW) from the label on the side of the SUN2000 and connect to the App.
- On the login screen, set a new login password and log in to the App.

----End

2.7 Log Maintenance

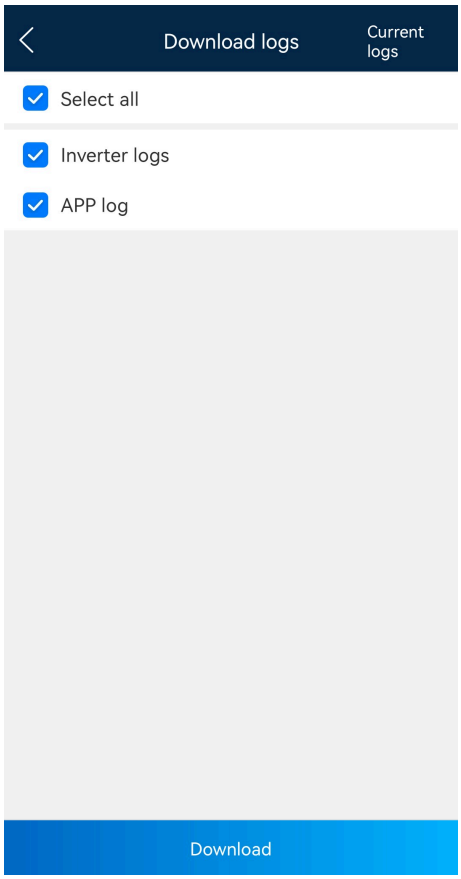
2.7.1 Maintenance Suggestions

Periodically audit the device security logs and data logs for knowledge of device security.

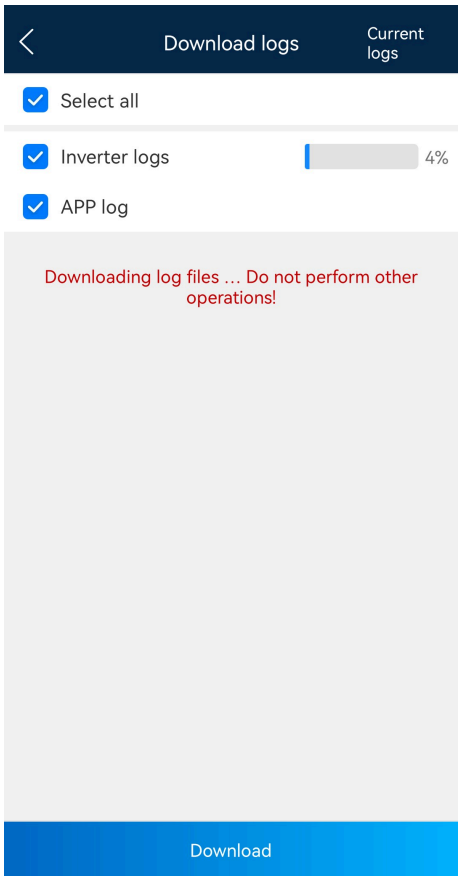
2.7.2 Procedure

To export SUN2000MA logs over the mobile phone app, perform the following steps:

Step 1 On the Operation console screen, tap Log mgmt to access the Download logs screen.



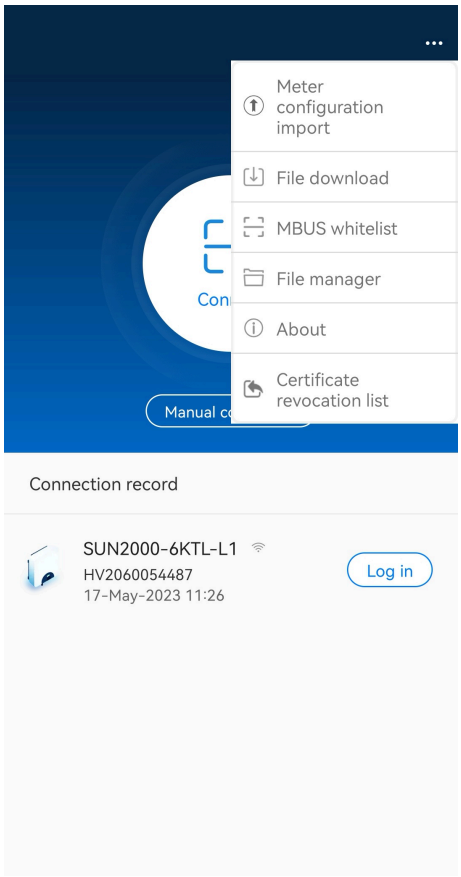
Step 2 On the Download logs screen, tap Download, then log export starts.



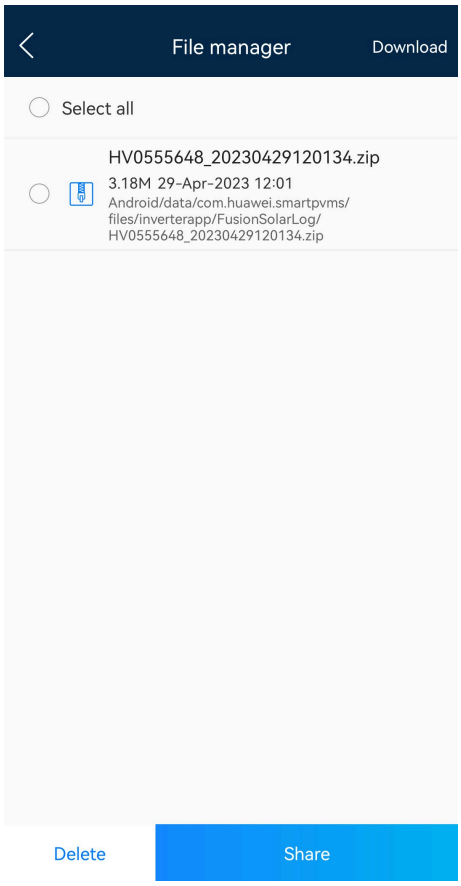
----End

To export inverter logs using the mobile app, perform the following steps:

Step 1 Switch to the network on your phone, access the FusionSloar software, touch the icon in the upper right corner, and select File Management.



Step 2 On the Existing Logs page, select a log, click Share, and select a sharing mode to export the log.



----End

2.8 Outer Integrity Check

This section describes how to verify the integrity of an obtained software package, thereby preventing PV system network risks that may be caused by malicious alteration or damage during the transmission of the software package. A software package can be installed only after it passes the verification.

For details about the check procedure and check document, access the following link:

https://support.huawei.com/carrier/digitalSignatureAction