SDongle V200R022C10

Security Maintenance Guide

Issue 01

Date 2024-07-10

HUAWEI DIGITAL POWER TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Preface

Purpose

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.

Intended Audience

This document is intended for maintenance personnel. Upgrade personnel must:

- Be familiar with the product networking and related NEs' versions.
- Have device maintenance experience and be familiar with device operation and maintenance.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.

Symbol	Description
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Issue	Date	Description
01	2022-06-25	This issue is the first official release.
02	2023-11-1	Add the description of public IP addresses and websites.
03	2024-07-10	Add Chapter 1.2.5 Enabling and disabling on a Third-Party NTP server. Add Chapter 1.4 Charger Maintenance. Modify Chapter 1.5 Modify WLAN Password and Chapter Modify APP Password.

Contents

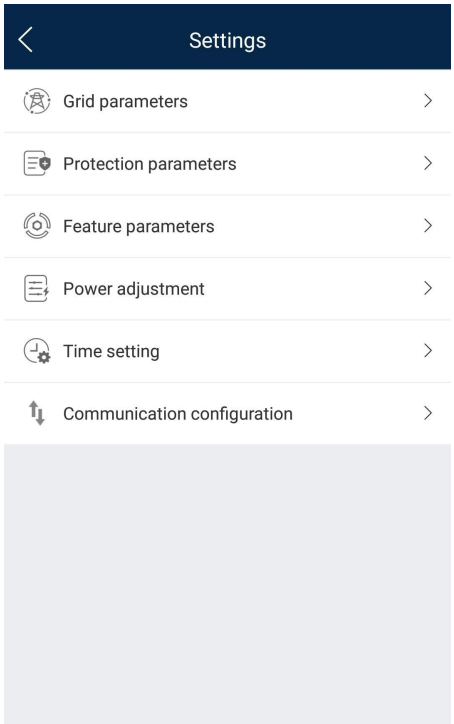
1 Device Layer Security

1.1 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:

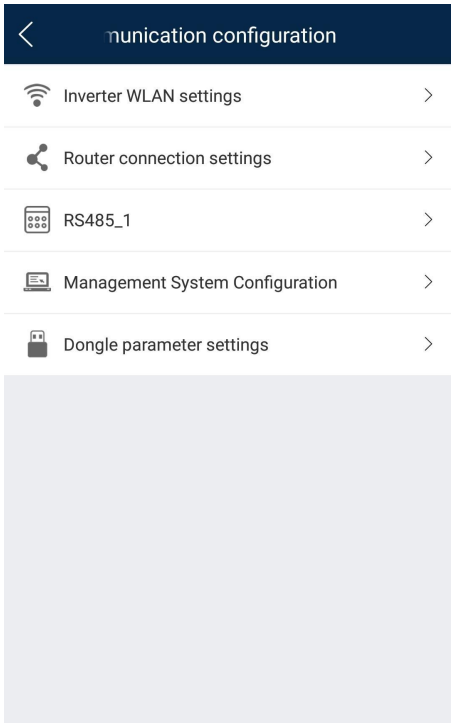
Step 1 On the Operation Console screen, tap **Settings** to access the Settings screen.

Figure 1-1 Settings



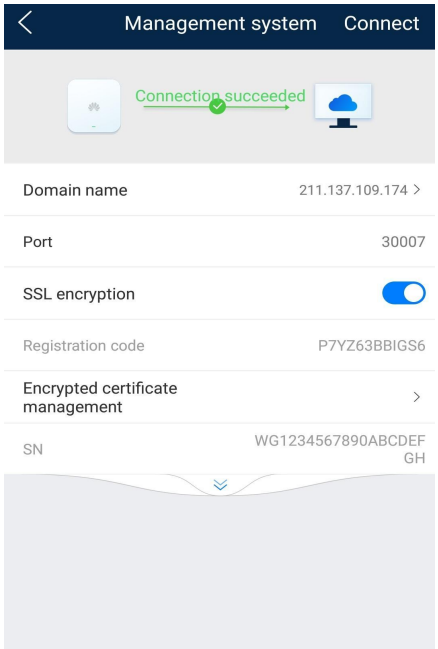
Step 2 On the Settings screen, tap **Communication configuration** to access the Communication configuration screen.

Figure 1-2 Communication configuration



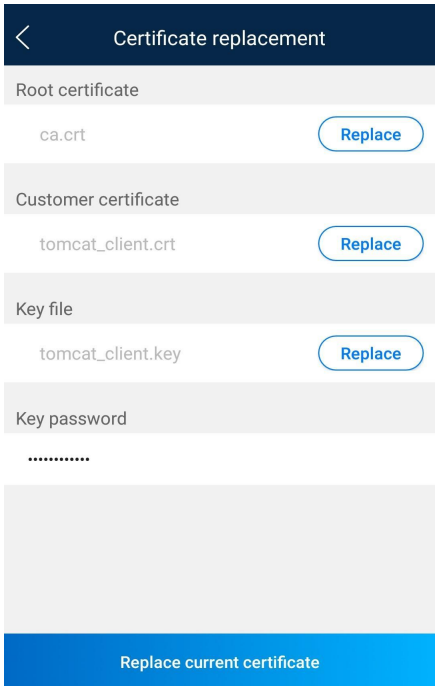
Step 3 On the Communication configuration screen, tap **Management System Configuration** to access the Management system screen.

Figure 1-3 Management system



Step 4 On the Management system screen, tap **Encrypted certificate management** access the Certificate replacement screen.

Figure 1-4 Certificate replacement



Step 5 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**.

Figure 1-5 Select certificate file

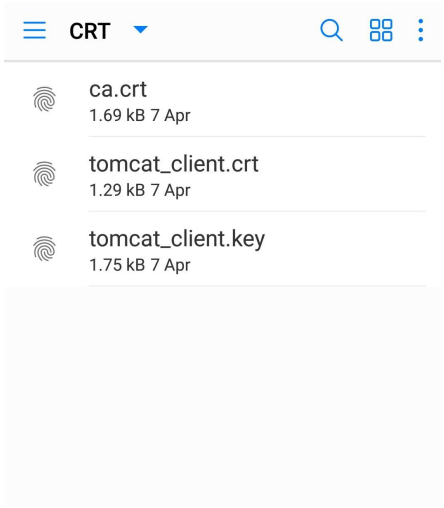
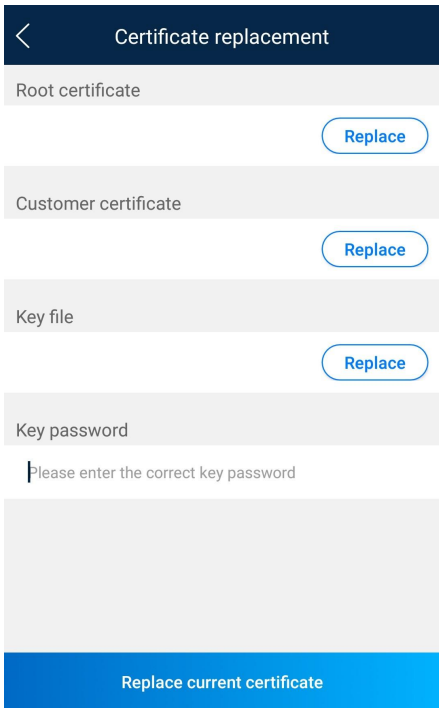
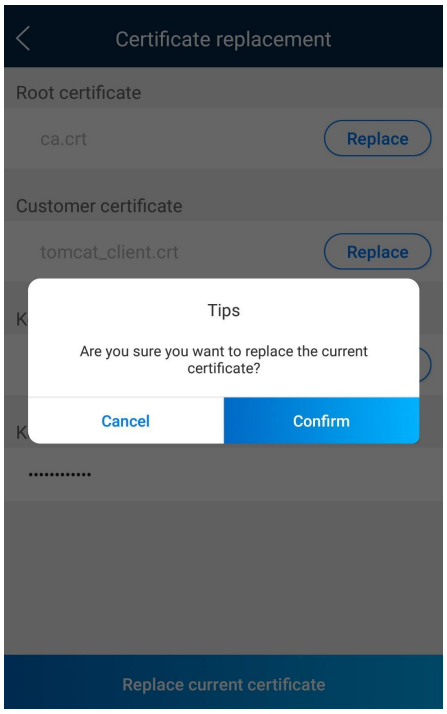


Figure 1-6 Certificate replacement



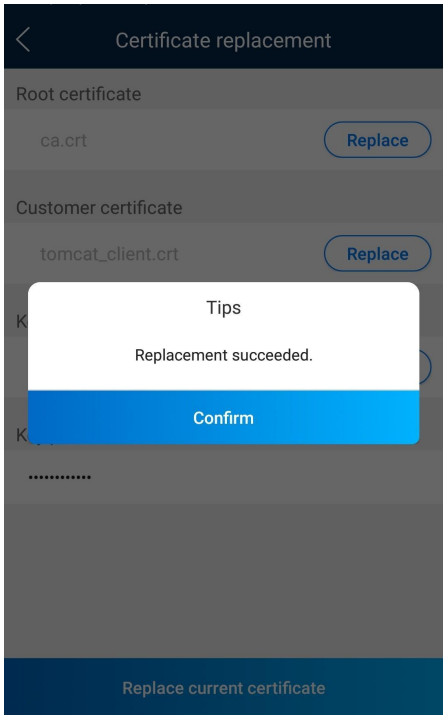
Step 6 Tap **Confirm** to replace the certificate. If you want to exit the certificate replacement operations, tap **Cancel**.

Figure 1-7 Replace



Step 7 After the certificate is replaced successfully, the "Replacement succeeded" message is displayed. Then connect the SDongle to the management system and check the correctness of the certificate.

Figure 1-8 Replacement successed



----End

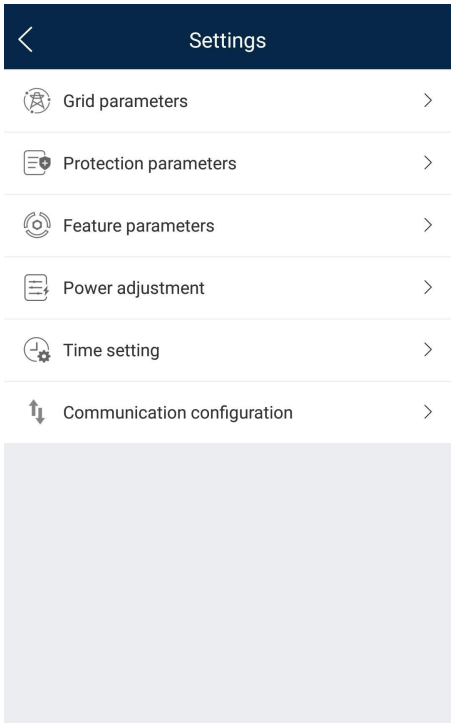
1.2 Management System Maintenance

1.2.1 Maintenance Suggestion

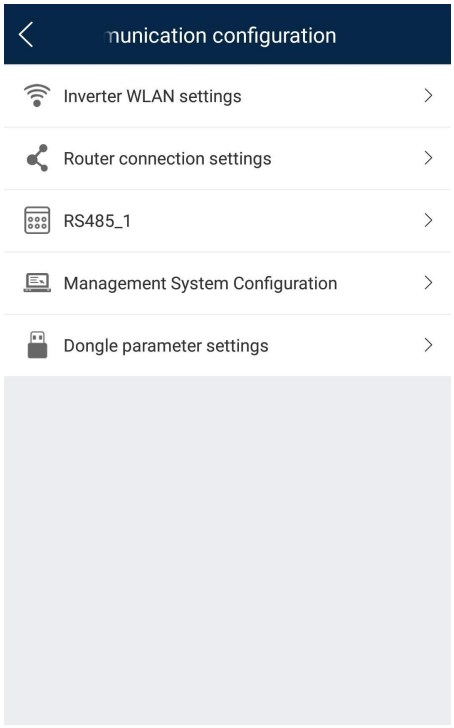
- A security certificate is preset in the SDongle. The certificate ensures that data is encrypted and transmitted in SSL mode when the SDongle connects to the management system. The SDongle management system certificate can be replaced. If the certificate needs to be replaced, update it in the management system and SDongle at the same time.
- The user name of the management system is emscomm, and the initial password is /EzFp+2%r6@IxSCv. To ensure system security, change the password immediately after the first login.
- Configure the SSL protocol to improve product security. You are not advised to disable SSL for connection with a network management system (NMS), as this will pose safety risks.
- Remaining a password unchanged for a long time increases the risk of password compromise or cracking. Change the password at least once every six months.

1.2.2 Enabling and Disabling SSL on a Huawei NMS

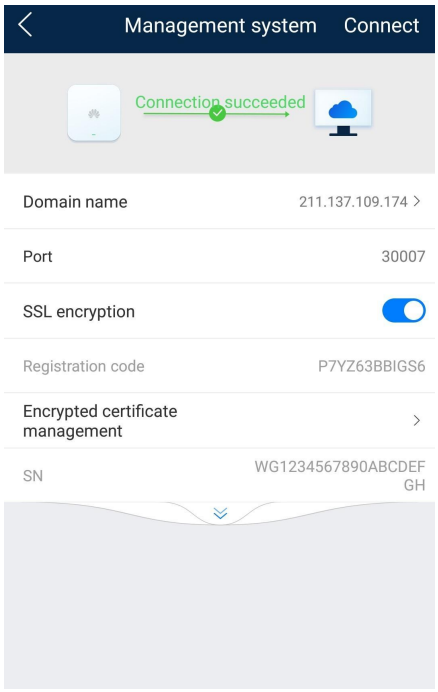
Step 1 On the home screen, tap **Settings**. The **Settings** screen is displayed.



Step 2 On the **Settings** screen, tap **Communication configuration**. The **Communication configuration** screen is displayed.



Step 3 On the **Communication configuration** screen, tap **Management system**. On the **Management system** screen, disable or enable **SSL encryption**.

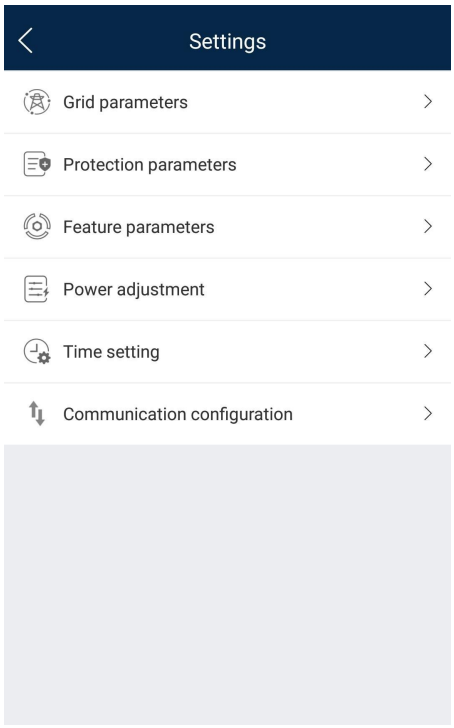


----End

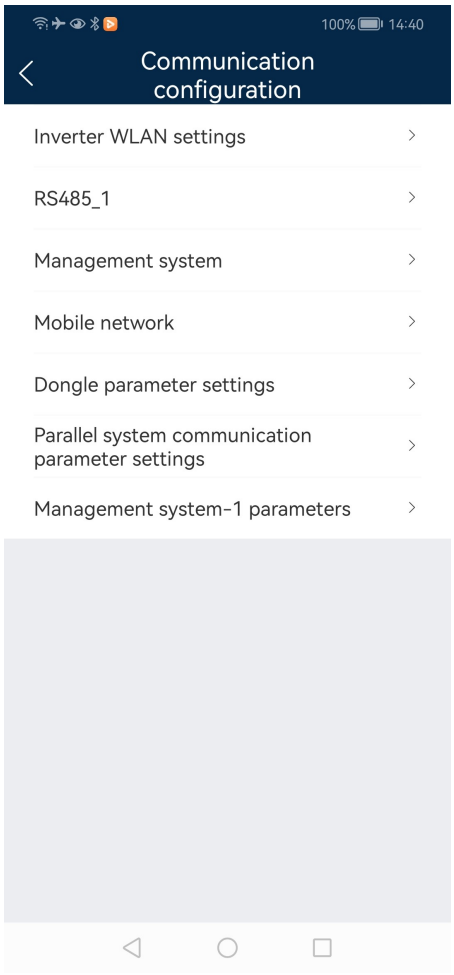
1.2.3 Enabling and Disabling SSL on a Third-Party NMS

- The Smart Dongle can connect to a third-party NMS that uses the Modbus-TCP or Trina protocol. If you need to connect to a third-party NMS, you have to enable this function manually and pay attention to the network security of the plant.
- Configure the SSL protocol to improve product security. You are not advised to disable SSL for connection with a network management system (NMS), as this will pose safety risks.

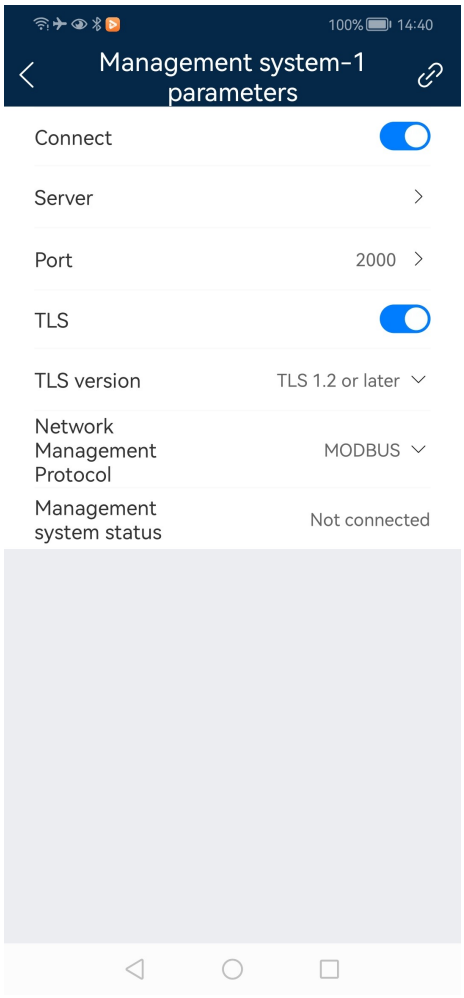
Step 1 On the home screen, tap **Settings**. The **Settings** screen is displayed.



Step 2 On the **Settings** screen, choose **Communication configuration** > **Management system-1**.



Step 3 On the **Management system-1** screen, enable **Connection**. On the **Management system settings** screen, disable or enable SSL.

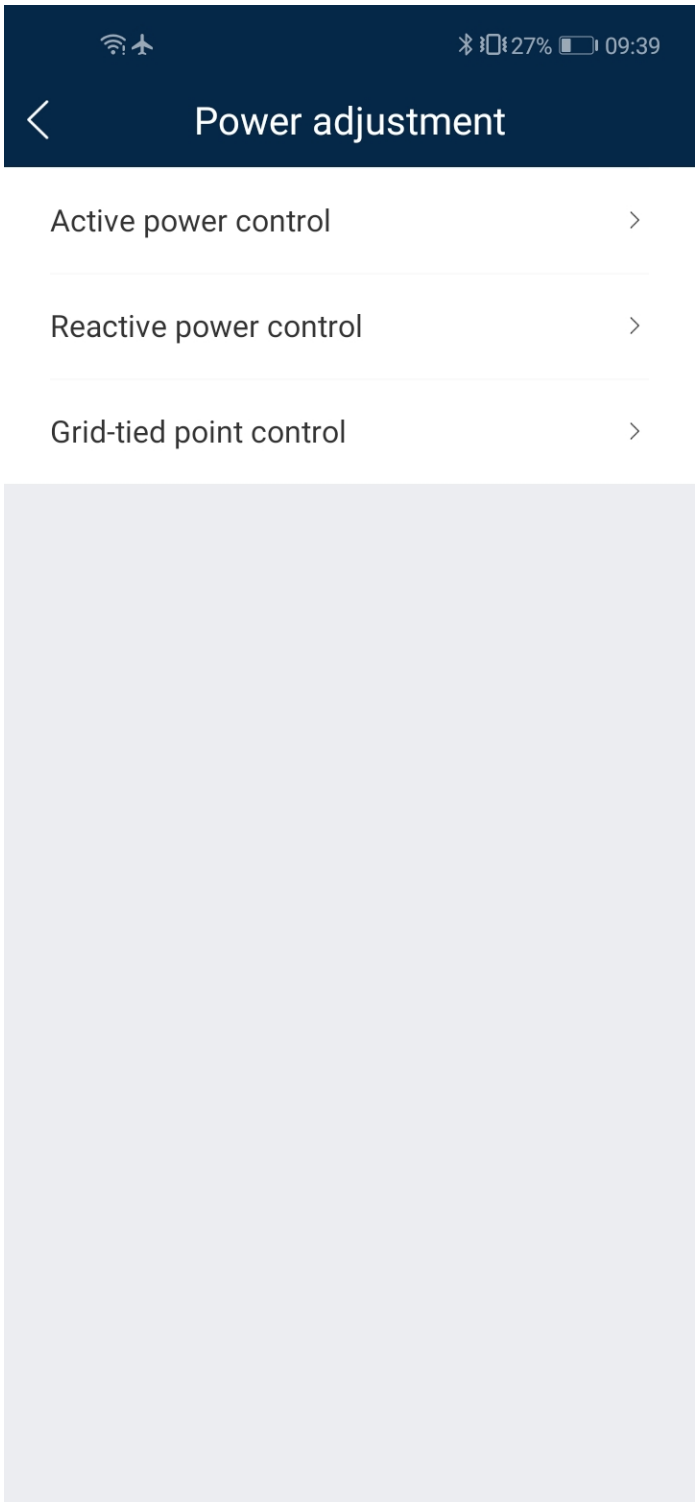


----End

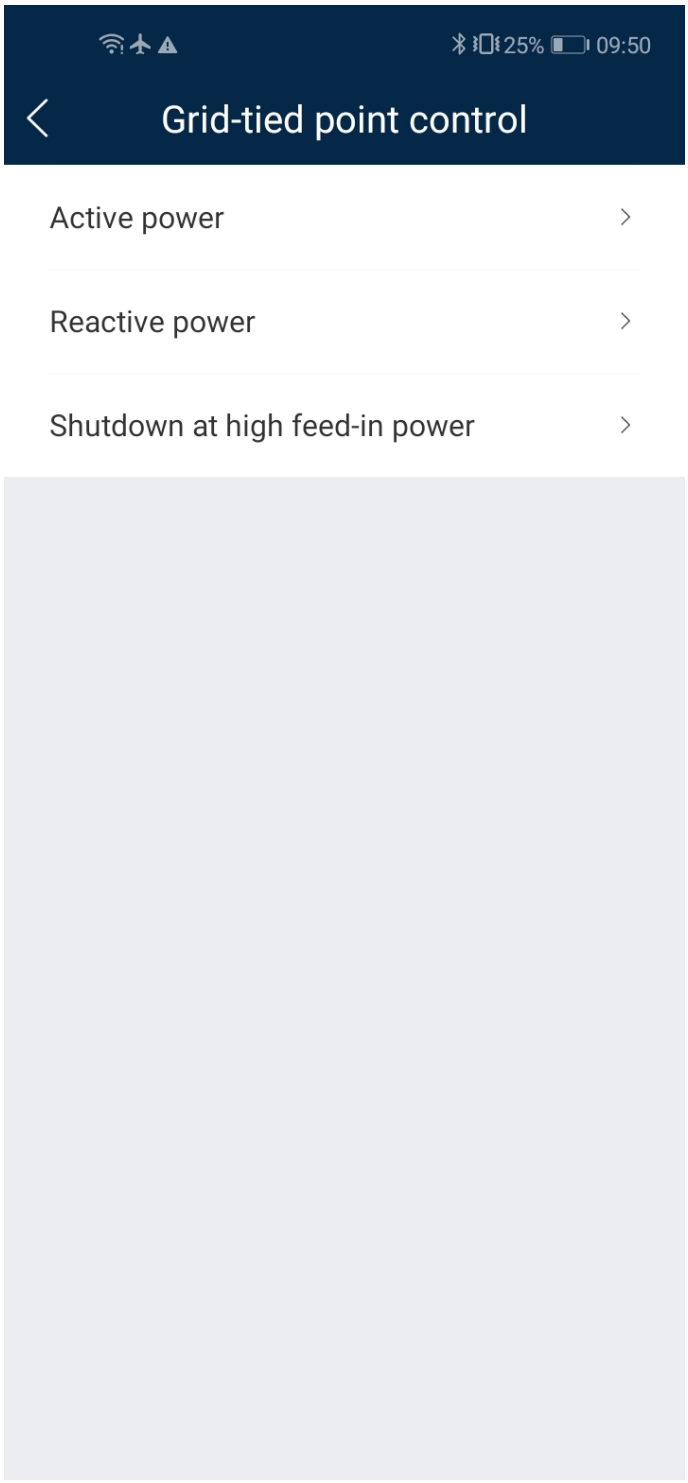
1.2.4 Enabling and Disabling SSL on a Remote Output Control NMS

- Smart Dongle can connect to a remote output control NMS through HTTPS. If you need to connect to a remote output control NMS, you have to enable this function manually and pay attention to the network security of the plant.
- Configure the SSL protocol to improve product security. You are not advised to disable SSL for connection with a network management system (NMS), as this will pose safety risks.

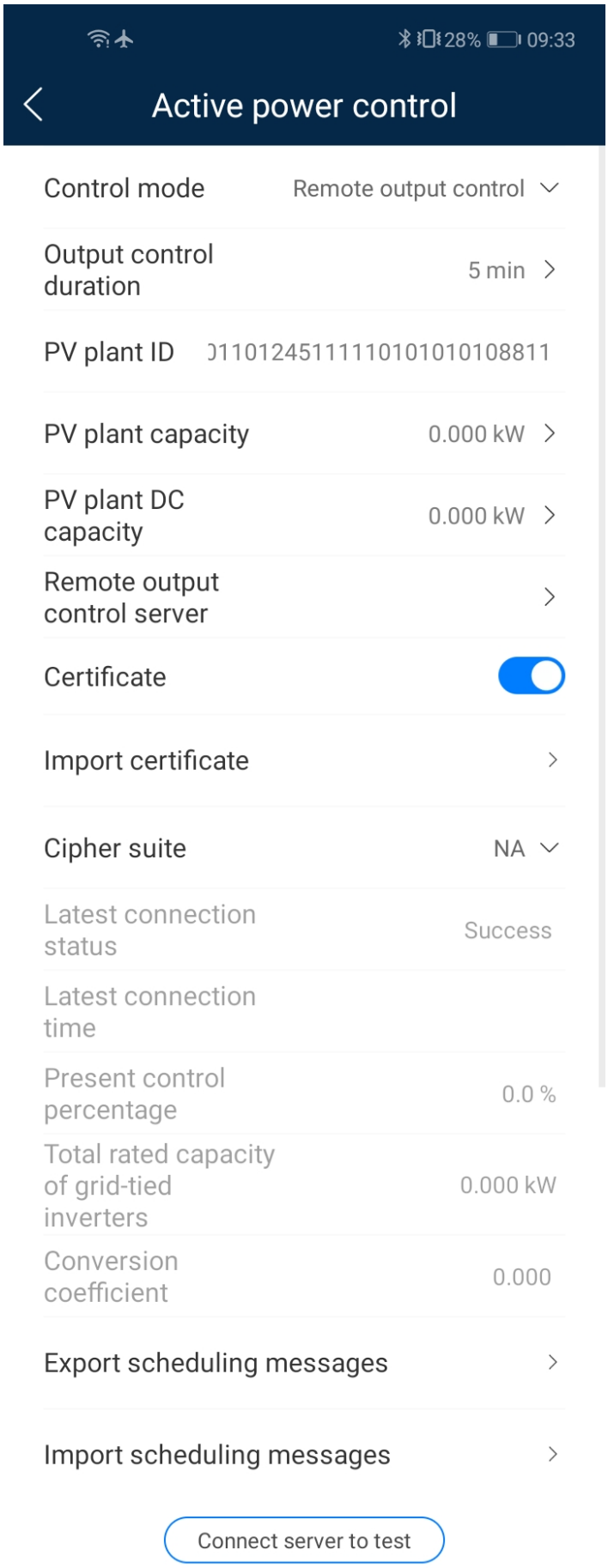
Step 1 On the home screen, tap **Power adjustment**. The **Power adjustment** screen is displayed.



Step 2 On the **Power adjustment** screen, tap **Grid-tied point control**. The following screen is displayed.



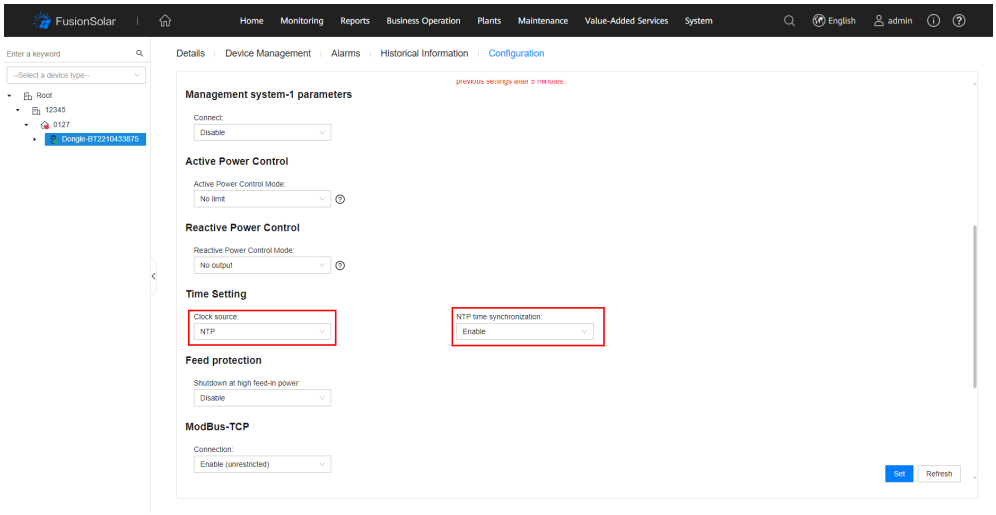
Step 3 On the **Communication configuration** screen, tap **Management system**. On the **Management system** screen, disable or enable **SSL encryption**.



----End

1.2.5 Enabling and disabling on a Third-Party NTP server

SDongle can synchronize time with a Third-Party NTP server. This function is disabled by default and can be manually enabled as required.



1.2.6 Environment Setup

[Required components] A PC, a Dongle, a power cable, and a network cable

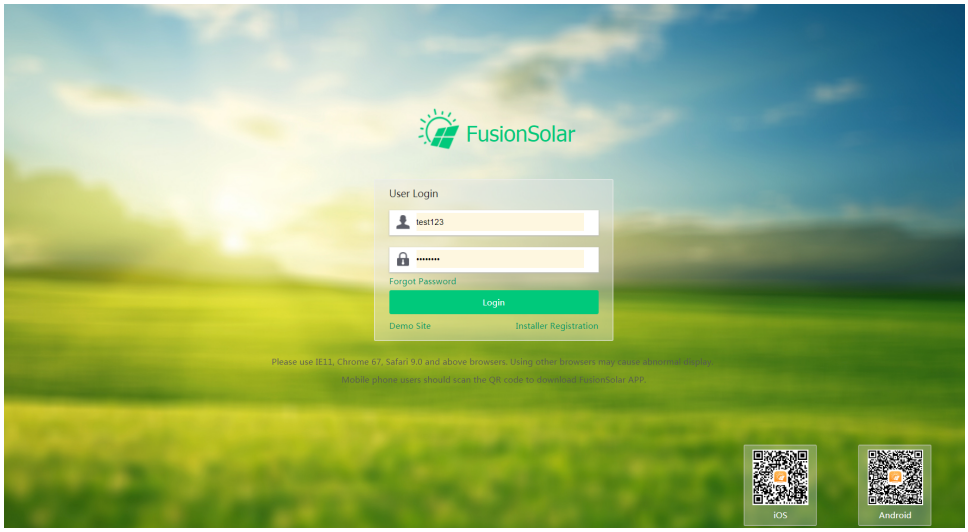
[Device requirement] The Dongle is properly powered on and communicating properly. The computer is connected to the network.

1.2.7 Procedure

To change the password of the SDongle user, perform the following steps:

Step 1 Open the browser, enter the management system address **https://intl.fusionsolar.huawei.com** to enter the management system. Enter the user name and password to log in.

Figure 1-9 Logging in to the management system



NOTE

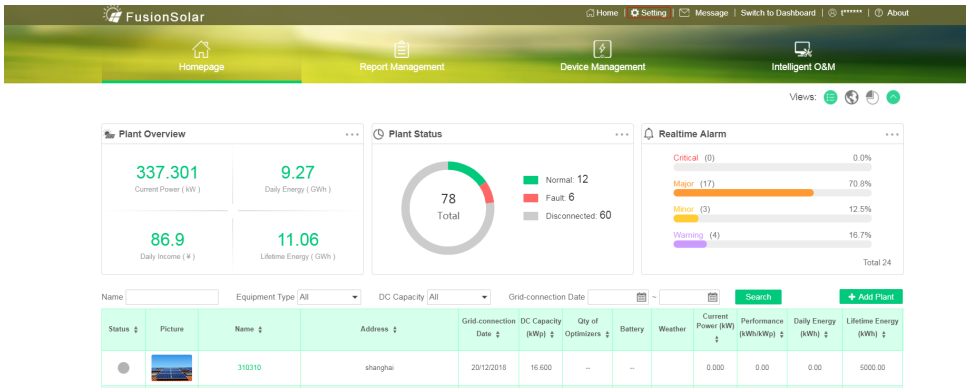
This document uses the management system https://intl.fusionsolar.huawei.com/ as an example to describe related operations. The operation is subject to the management system to which the Dongle connects.

If you do not have an account, you need to register an installer account before logging in to the system.

Use Internet Explorer 11, Chrome 67, Safari 9.0, or a later version. Otherwise, exceptions may occur.

Step 2 On the home page of the management system, click **Setting** at the upper right corner.

Figure 1-10 Home page of the management system

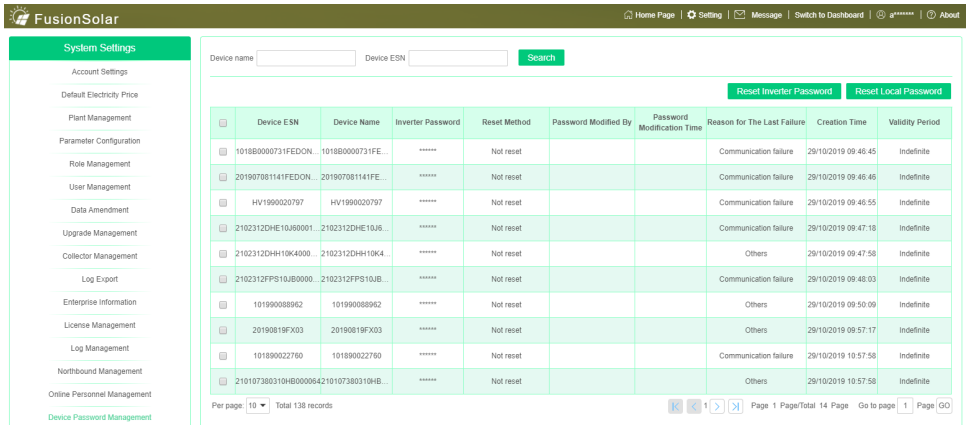


NOTE

Before the operation, ensure that the PV plant is created successfully and you can find the corresponding device on the **Device Management** tab page.

Step 3 Go to the **Setting** page and select **Device Password Management**. The password management subpage is displayed.

Figure 1-11 Device Password Management

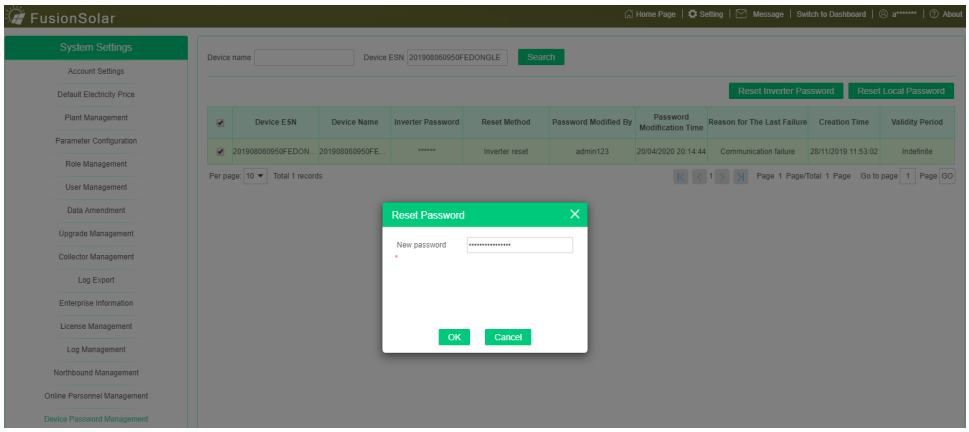


NOTE

If the current account does not have the permission to **Device Password Management** (**Device Password Management** is not displayed on the page), contact the system administrator.

Step 4 Select the device to be modified, click **Reset Inverter Password** in the upper right corner, enter the new password on the page that is displayed, and click **OK.**

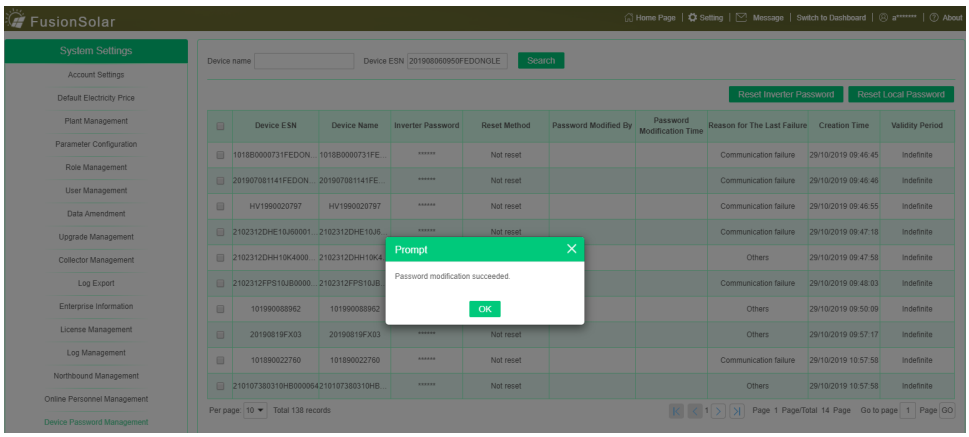
Figure 1-12 Changing the Login Password



You can search the Dongle whose you want to modify password through the plant name or SN.

Step 5 After the password is changed successfully, the new password takes effect upon the next connection.

Figure 1-13 Modification successed



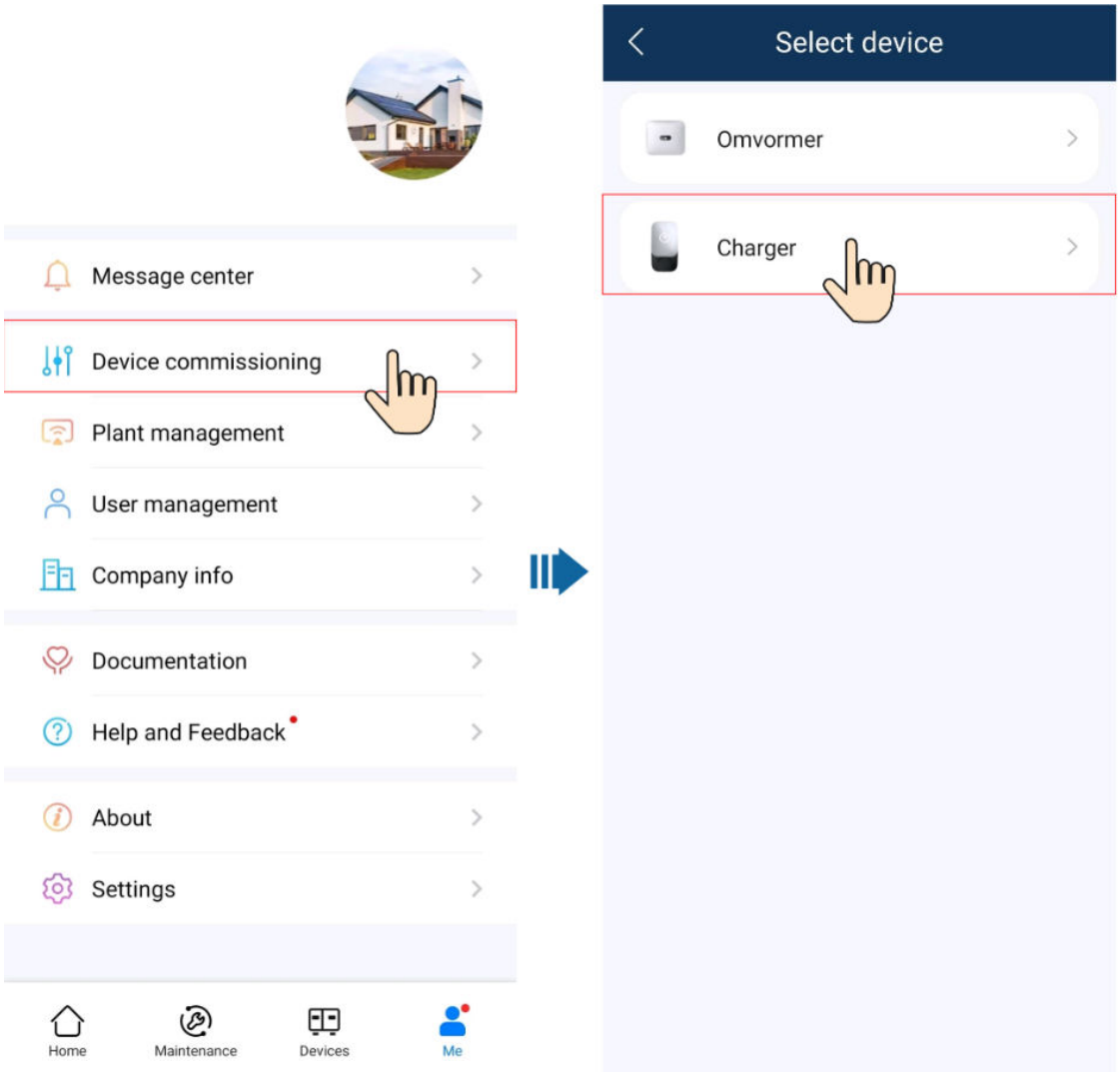
----End

1.3 Serial Port Maintenance

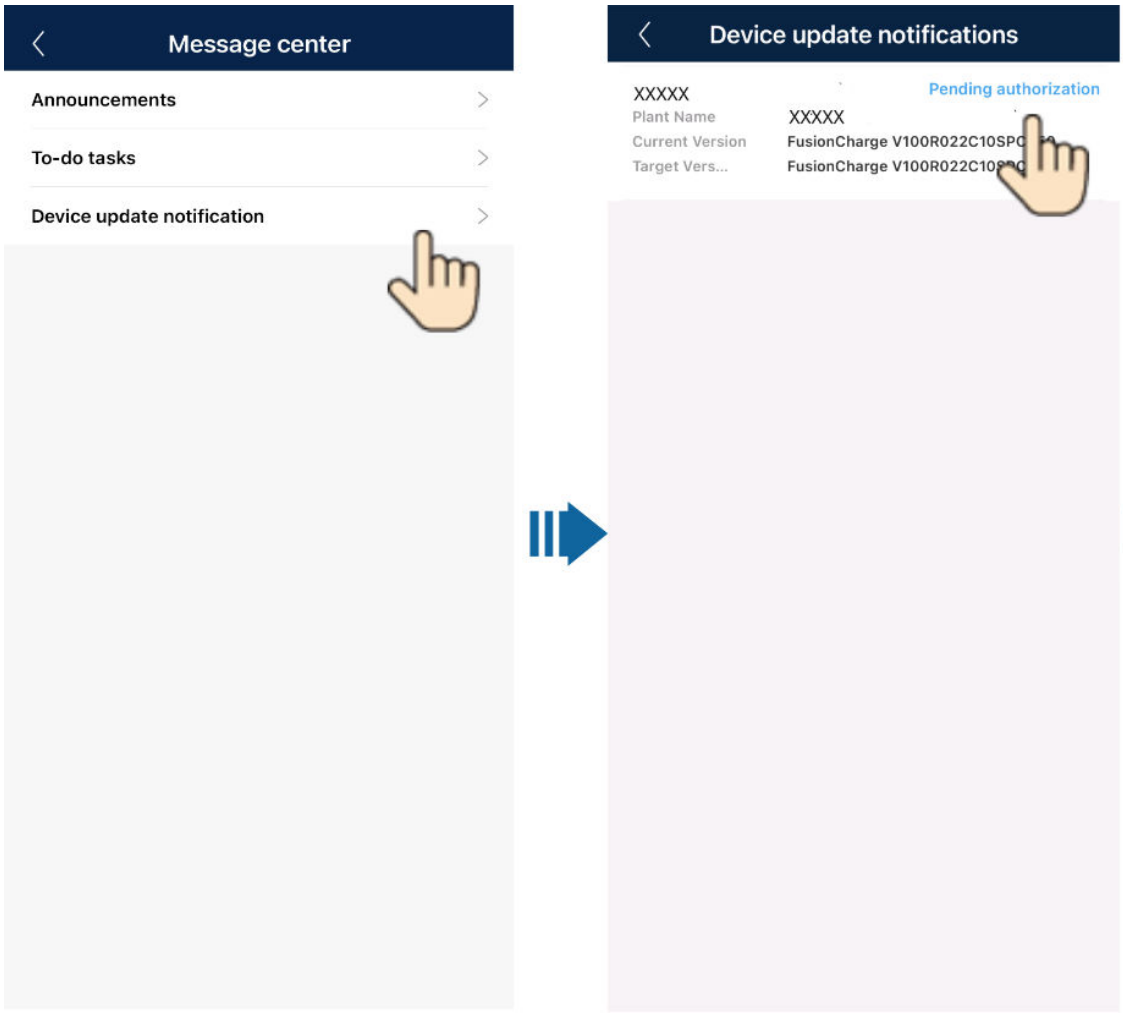
The commissioning serial port has been removed.

1.4 Charger Maintenance

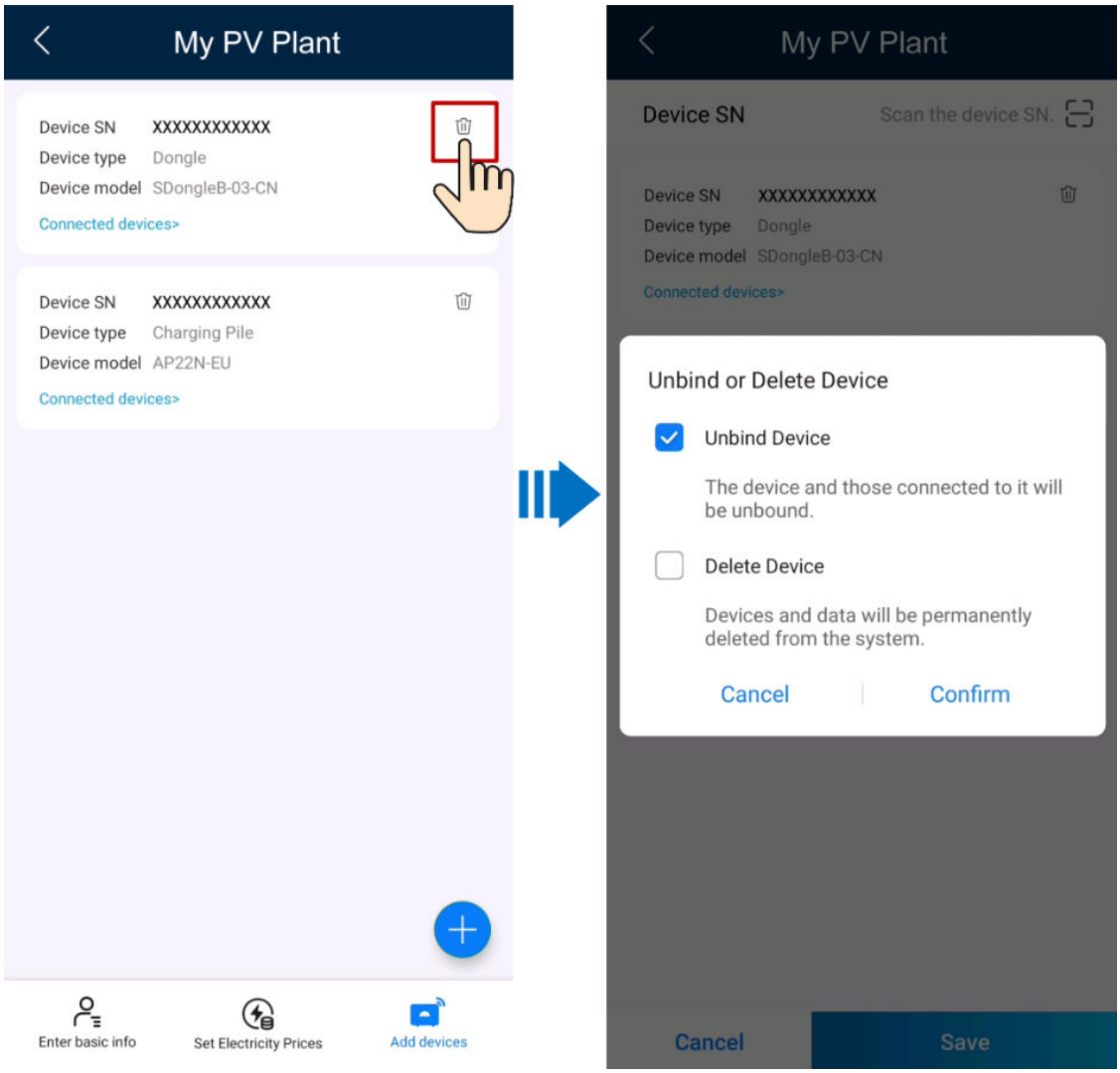
1. The SDongle supports the scenario with "PV+ESS+Charger" and the access of a charger.
2. Connecting to a Charger: Me -> Device commissioning -> Charger -> connect to the WLAN of the charger as prompted.



3. On the home screen of the app, tap Maintenance to set charger running parameters, export logs, Restoring Factory Settings, and change passwords.
4. When receiving an update notification in the message center, you can authorize the device update.



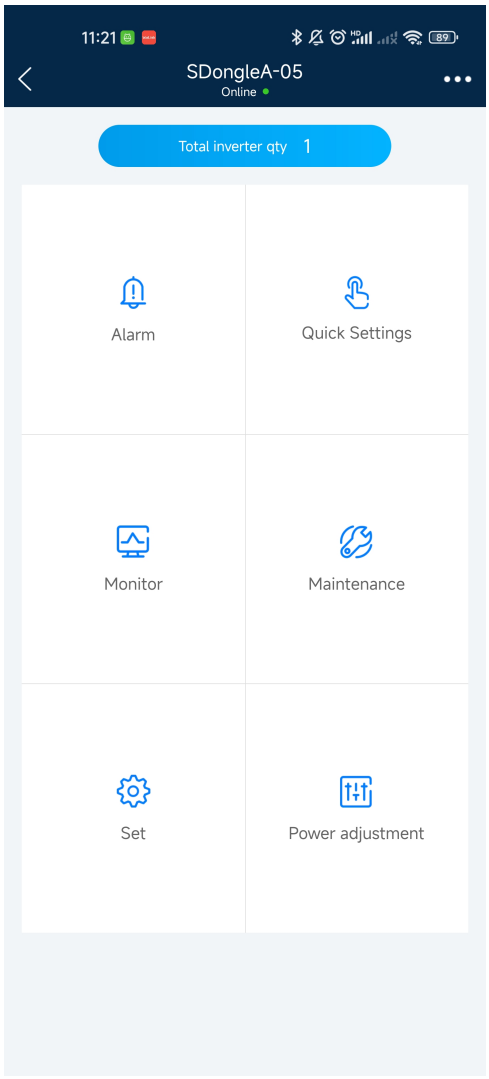
5. Unbind the old charger on the FusionSolar app: Me -> Plant management -> Target plan -> Add devices -> Unbind Device or Delete Device.



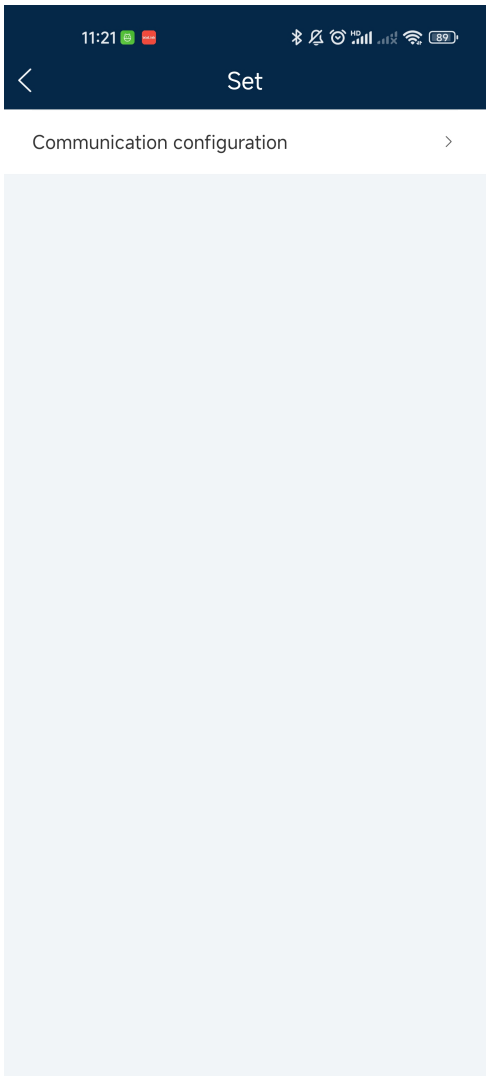
1.5 Modify WLAN Password

The app version can be 3.2.00.005 or later. If the app version does not support the modification, upgrade the app version.

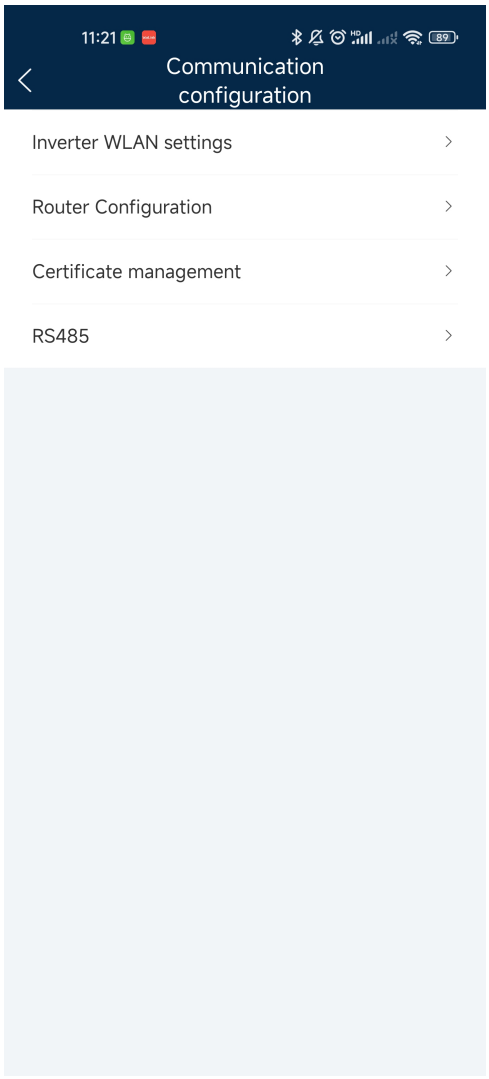
Step 1 Log in to the home page, tap Set.



Step 2 Tap Communication configuration.



Step 3 Tap Inventer WLAN settings.



Step 4 Tap New password -> Confirm new password -> Finish.

----End

1.6 Modify APP Password

The app login password cannot be changed.

1.7 Restoring the preset password

The following steps can be used to restore the WLAN password and APP login password.

Step 1 Remove and insert the SDongle for three consecutive times. There is no requirement on the time interval, but the power-on time for each time must be no less than 1 minute and no more than 2 minutes.

Step 2 Insert the SDongle for the fourth time. You can see that the SDongle automatically resets (all indicators are off) after a period of time.

Step 3 Within 10 minutes after the automatic reset, use the default password to connect to the hotspot of the SDongle and log in to the app. The password is successfully restored.

Step 4 If you do not log in to the mobile app within 10 minutes, the system will restore the WLAN password and app login password.

----End

1.8 Log Maintenance

1.8.1 Maintenance Suggestions

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

1.8.2 Environment Setup

[Required components] A PC,a Phone, a Dongle, a power cable, and a network cable

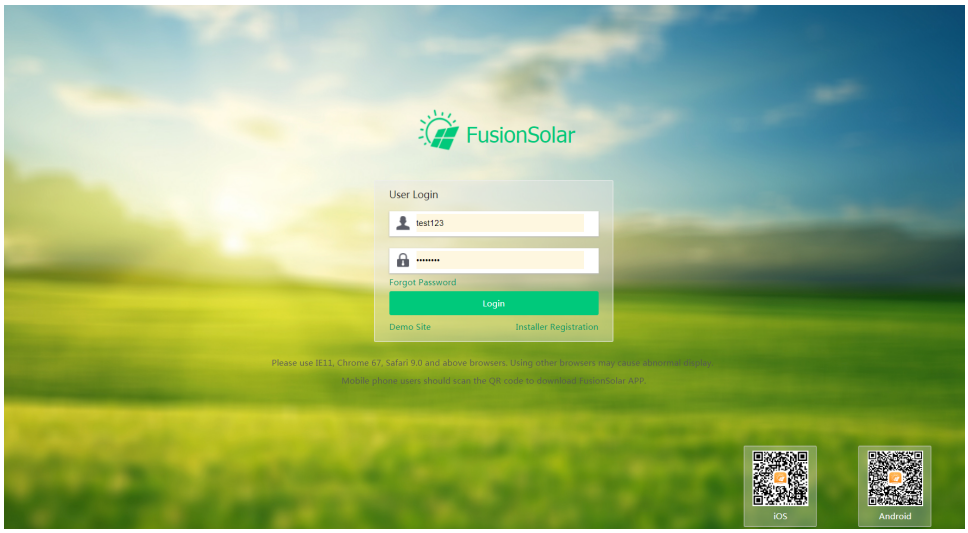
[Device requirement] The Dongle is properly powered on and communicating properly. The computer is connected to the network.

1.8.3 Remote log export

To export SDongleA logs from FusionSolar, perform the following steps:

Step 1 Open the browser, enter the management system address **https://intl.fusionsolar.huawei.com** to enter the management system. Enter the user name and password to log in.

Figure 1-14 Logging in to the management system

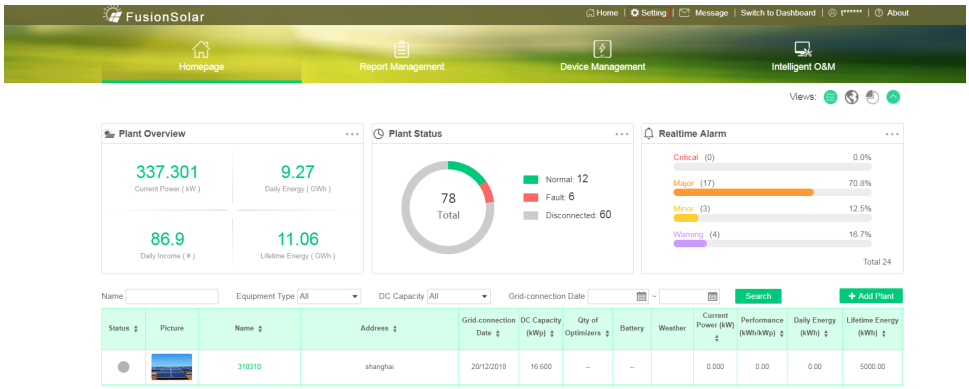


If you do not have an account, you need to register an installer account before logging in to the system.

Use Internet Explorer 11, Chrome 67, Safari 9.0, or a later version. Otherwise, exceptions may occur.

Step 2 On the home page of the management system, click **Setting** at the upper right corner.

Figure 1-15 Home page of the management system

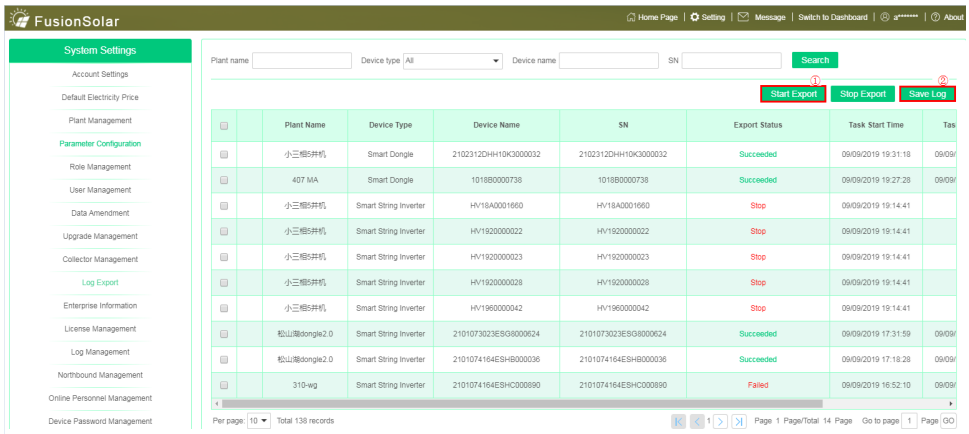


NOTE

Before exporting log, ensure that the PV plant is created successfully and you can find the corresponding device on the **Device Management** tab page.

Step 3 Go to the **Setting** page and select **Log Export**. The log export subpage is displayed.

Figure 1-16 Log Export



You can search the Dongle whose logs you want to export through the plant name or SN, select the Dongle, and click **Start Export** to export logs. After the export is complete, click **Save Log** to save the logs to the local PC.

----End

1.8.4 Local log export

App logs cannot be exported because the Smart Dongle WiFi hotspot is disabled.

1.9 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/enterprise/en/tool/software-digital-signature-validation-tool--pgp-verify--TL1000000054

1.10 Preconfigured Certificate Disclaimer

The Huawei-issued certificates preconfigured on Huawei devices during manufacturing are mandatory identity credentials for Huawei devices. The disclaimer statements for using the certificates are as follows:

1. Preconfigured Huawei-issued certificates are used only in the deployment phase, for establishing initial security channels between devices and the customer's network. Huawei does not promise or guarantee the security of preconfigured certificates.

2. The customer shall bear consequences of all security risks and incidents arising from using preconfigured Huawei-issued certificates as service certificates.

3. A preconfigured Huawei-issued certificate is valid for 20 years (for devices delivered before January 2021) or 19 years (for devices delivered during or after January 2021) starting from the manufacturing date.

4. Services using a preconfigured Huawei-issued certificate will be interrupted when the certificate expires.

5. It is recommended that customers deploy a PKI system to issue certificates for devices and software on the live network and manage the lifecycle of the certificates. To ensure security, certificates with short validity periods are recommended.

Note: You can view the validity period of a preconfigured certificate on the NMS.

1.11 Privacy Statement

Personal data used in the Smart Dongle+inverter networking scenario is collected for different functions based on service requirements. The data processing methods may vary. For details, see the product privacy statement.