SmartPVMS
V500R007C00

User Manual

Issue 01

Date 2021-10-09

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://solar.huawei.com

Contents

1 User Manual

This document describes how to log in to the SmartPVMS server by using the Webbased SmartPVMS client to operate and maintain the SmartPVMS system.

Product Version

The following table lists the product versions related to this document.

Product Name	Product Version
SmartPVMS	V500R007C00

Intended Audience

This document is intended for network management engineers.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in previous issues.

01 (2021-10-09)

This issue is the first official release of SmartPVMS V500R007C00.

Draft C (2021-07-30)

This issue is used for the third office application (FOA) of SmartPVMS V500R007C00 and is the third release.

Draft B (2021-02-03)

This issue is used for the second office application (FOA) of SmartPVMS V500R007C00 and is the second release.

Draft A (2020-08-14)

This issue is used for the first office application (FOA) of SmartPVMS V500R007C00and is the first release.

1.1 Getting Started

This topic describes how to register an installer, log in to and log out of the system, retrieve the password, and experience the plant functions.

1.1.1 Overview

The SmartPVMS is a software system for monitoring and O&M of PV power systems. It aims to display the current and historical running status of PV plants in a more real-time and comprehensive manner. In addition, the SmartPVMS provides functions such as intelligent alarming, analysis, diagnosis, and O&M to help customers improve the power generation efficiency and lower the O&M cost, achieving refined management and improved profitability.

Full-lifetime Management Allows You to Learn the Plant Operating Status

- PV plant information on one screen, facilitating management.
- Real-time monitoring of plant-level, device-level, and module-level running data.
- Traceable and presentable plant-level and device-level historical data of multiple types.
- Real-time display of fault alarms, facilitating quick response and troubleshooting.
- Report and alarm push and subscription for learning the plant running status.

Intelligent and Efficient O&M

- Simple and efficient centralized O&M and monitoring.
- Real-time alarm push and troubleshooting suggestions, enabling quick response.
- Accurate locating of arc faults, reducing the onsite troubleshooting time (full optimizer configuration required).
- Intelligent diagnosis and warning, detecting device exceptions in advance.
- Mobile O&M/Electronic tickets, delivering simple and efficient O&M.
- Remote health check and proactive optimization, ensuring the healthy and stable operation of PV plants.

Networking Mode

Figure 1-1 shows the system networking.

Figure 1-1 System networking

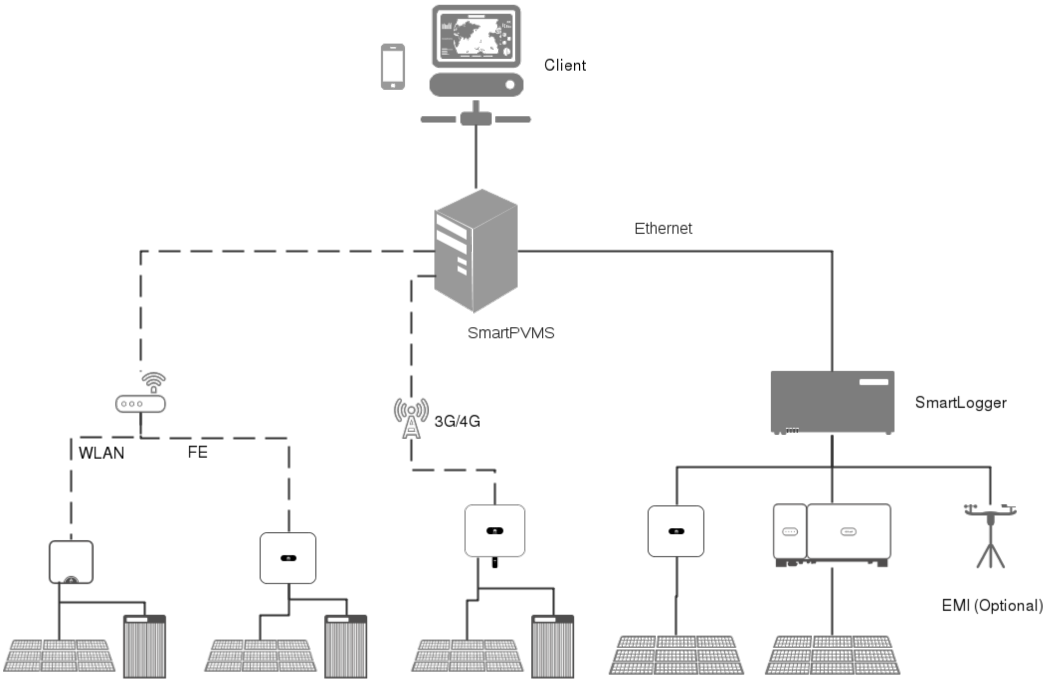


Table 1-1 lists the device types that can be managed by the system.

Table 1-1 Types of supported devices

Device Type	Description
Inverter	Only Huawei inverters can be managed.
SmartLogger	Can be connected to, managed and remotely upgraded on the system, covering performance indicator monitoring, configuration information, alarm information, and log information.
SDongle	
Residential battery	
LG battery	Can be connected to and managed on the system, covering performance indicator monitoring, configuration information, alarm information, and log information. Remote upgrade is not supported.
Electricity meter	Can be connected to and managed on the system, covering performance indicator monitoring, configuration information, and alarm information.
Environmental monitoring instrument	Can be connected to and managed on the system, covering performance indicator monitoring and configuration information.

1.1.2 Installer Registration

This topic describes how to register an account before the first login.

Procedure

Step 1 Open a web browser, enter **https://intl.fusionsolar.huawei.com** in the address box, and press **Enter**. The login page is displayed.

Step 2 **Optional:** Select a language from the drop-down list box in the upper-right corner of the page.

Step 3 Click **Installer Registration**. The **Installer Registration** page is displayed.

Step 4 Enter the installer registration information as required.

Step 5 Click **Send**.

Step 6 Enter the obtained verification code.

Step 7 Select **I have read and agreed to the Terms of Use and Privacy Policy** and click **Submit**.

NOTE

- The email address and user name entered during registration can be logging in to the SmartPVMS system.
- The system automatically checks whether the company name exists.If so, the system displays a message indicating that the company name already exists. This indicates that your company has registered an account in the system. In this case, you do not need to register an account. Ask your company administrator to add you to the user list.

----End

1.1.3 Login and Logout

This topic describes how to log in to and log out of the SmartPVMS system.

Prerequisites

You have obtained the username or email address and password for logging in to the system.

Context

To ensure account security, change the password periodically and keep the new password in mind. Not changing the initial password may cause password disclosure. A password left unchanged for a long period of time may be stolen or cracked. If a password is lost, the user cannot access the system. In these cases, the user is liable for any loss caused to the PV plant.

Procedure

Step 1 Open a web browser, enter **https://intl.fusionsolar.huawei.com** in the address box, and press **Enter**. The login page is displayed.

Step 2 **Optional:** Select a server and a language from the drop-down list boxes in the upper-right corner of the page.

NOTE

When you select a site, the system automatically switches to the site web page.

Step 3 Enter the username or email address and password, and click **Log In**.

If you log in to the system for the first time or for the first time after the privacy policy is updated, select the item for agreeing to the terms of use and privacy policy. In addition, change the password immediately after the login if you are not a self-registered user.

----End

Follow-up Procedure

To log out, move the pointer to the user icon on the home page and choose **Log Out** from the drop-down list box.

1.1.4 Associate Email Address

After an email is associated, you can use the associated email to reset the password if you forgets the login password.

Prerequisites

You have logged in to the SmartPVMS.

Procedure

Step 1 Choose **System** > **System Settings** > **Personal Settings** from the main menu.

Step 2 In the navigation pane, choose **Modify Personal Info**.

Step 3 On **Associate Email Address** area, click **Verify**.

Step 4 Click **Send Code** and enter the obtained verification code to verify that the email address is valid.

Step 5 Click **OK**.

----End

1.1.5 Password Retrieval

If a user forgets the password, the user can retrieve the password by email or contact the company administrator to reset the password.

Prerequisites

You account is associated with a personal email address that has been verified. For details, see **1.1.4 Associate Email Address**.

Context

To ensure account security, change the password periodically and keep the new password in mind.

Procedure

Step 1 Open a web browser, enter **https://intl.fusionsolar.huawei.com** in the address box, and press **Enter**. The login page is displayed.

Step 2 Click . The **Forgot password** page is displayed.

Step 3 Set **Email** and **Verification code**, and click **Next**. The email address verification page is displayed.

Step 4 Click **Send Verification Code** and enter the obtained email verification code.

Step 5 Click **Next**. The page for resetting the password is displayed.

Step 6 Enter the new password and confirm the password, and click **Submit**. In the displayed dialog box, click **OK**.

----End

1.1.6 Demo Site

This section describes how to log in to the system using the guest status to promote the value of the management system to installation providers and proprietors, and browse plant information to help users understand the functions of the management system.

Prerequisites

The demo account function has been enabled. For details, see **1.6.7.4 Configuring Demo Account**.

Procedure

Step 1 Open a web browser, enter **https://intl.fusionsolar.huawei.com** in the address box, and press **Enter**. The login page is displayed.

Step 2 Click **Demo Site** to experience the system.

----End

1.1.7 User Operation Permissions (Owner)

Level 1 Menu	Level 2 Menu	Level 3 Menu	Sub Menu
Home	Home	List View	Kiosk
		Map View	-
		KPI View	-
Plants	Plant	Plant Management	Viewing the PV plant list
			Modify
			Export

Level 1 Menu	Level 2 Menu	Level 3 Menu	Sub Menu
	Device	Device Management	Viewing the Device List
Settings	Message Management	Announcements	-
	System Settings	Personal Settings	Change Password
			Modify Personal Info
	About	Privacy Policy	-
		Terms of Use	-
		Version Information	-

1.1.8 User Operation Permissions (Installer)

Level 1 Menu	Level 2 Menu	Level 3 Menu	Sub Menu
Home	Home	List View	Add Plant
		Map View	-
		KPI View	-
		Dashboard	-
Reports	Reports	Plant Report	-
		Inverter Report	-
		Battery Report	-
Plants	Plant	Plant Management	Viewing the PV plant list
			Add Plant
			Modify
			Delete
	Device	Device Management	Viewing the Device List
			Set Parameters
			Replace Device
			Delete

Level 1 Menu	Level 2 Menu	Level 3 Menu	Sub Menu
			Export Basic Info
			Export Performance Data
			Modify
		Upgrade Management	Device Upgrade
		Device Log Export	Device Log Export
			Optimizer Log Export
			Battery Log Export
Maintenance	Maintenance	Real-Time Status	-
		Alarm Management	Device Alarm
		Task Management	Inspection
			Defect Elimination
		Smart Diagnosis	I-V Curve
			Module Library Management
		Smart Tracking	-
Settings	System	Company Management	User Management
			User Management
			Mailbox
			Default Electricity Prices
	Message Management	Announcements	-
		Send Announcement	-
	Business Configuration	Alarm Configuration	Push Settings
			Redefine Alarm
	System Settings	License Management	License Overview

Level 1 Menu	Level 2 Menu	Level 3 Menu	Sub Menu
			License Information
			License File
			Device License Management
		Personal Settings	Change Password
			Modify Personal Info
	About	Privacy Policy	-
		Terms of Use	-
		Version Information	-

1.2 Home

On the home page, you can learn about the running status of all plants in the SmartPVMS. In the list view, you can view the global information about multiple plants and important information about a single plant. In the map view, you can view the location and distribution of plants. In the KPI view, you can view the key energy yield indicators of the plants managed by your company. In addition, you can view the overall O&M and operational status of plants in a dashboard.

1.2.1 List View

In the list view, you can gain an overview of plants and important plant information, and navigate to individual plants for details.

Context

If the real-time device data cannot be obtained and the running information is displayed as **-**, check whether the device is offline or faulty.

Procedure

- Multi-plant view
  a. Choose **Home** > **Home** > **List View** or click  in the upper right corner of the home page.
  b. In the multi-plant view, you can view the KPIs, running status, and alarm status of all managed plants.

     On the multi-plant view page, you can perform the following operations.

Operation Type	Procedure
Viewing energy yield and revenue	Click in the **Plant KPIs** area to access the **Plant Report** tab page to query the energy yield revenue of the plant.
Viewing current plant status	Click in the **Plant Status** area to access the **Real-Time Status** page to view the plant running status, key information, device alarm information, plant location, and O&M personnel information.
Viewing device alarms	Click in the **Real-Time Alarms** area to access the **Alarm Management** page. On the page, choose **Device Alarm** > **Current Alarms** to view detailed device alarm information.
Viewing the running status of a plant	In the plant list area, click the plant image or name to access the plant **Overview** page and view the real-time running status of the plant.
Creating a plant	1. Click **Add Plant**. 2. In the displayed **Add Plant** dialog box, complete the configuration wizard. 3. Click **Save**.

- Single-plant view
  a. In the plant list, click a plant image or name to access the single-plant page and check the plant running status. For details, see **Table 1-2**.

Table 1-2 Plant details

Menu Name	Description	Procedure
Overview	Displays general information about the plant, such as energy yields, environmental benefits, current alarms, energy flow, basic plant information, energy management, weather, and revenue statistics.	• In the **Energy Flow** area, you can perform the following operations: – Click > to access the **Devices** page. – If there is only one inverter in the plant, click the inverter icon to access the **Real-Time Info** page. If there are multiple inverters in the plant, click the inverter icon to access the **Devices** page. – Move the mouse cursor to device icons, such as inverter, battery, and power sensor icons to view the brief metrics. • In the **Energy Management** area, you can view energy yield by day, month, or year. • In the **Revenue Statistics** area, you can view revenue by day, month, year, or lifetime. • In the **Real-Time Alarms** area, click > to access the **Alarm Management** page.
Kiosk view	Owners can share the plant running information in the Kiosk view. Other users can view the Kiosk view and check the plant information without logging in to the system. **NOTE** Only a user who has the Kiosk view permission and logs in as the owner can create a Kiosk view.	1. On the **Overview** page, click **Kiosk** in the upper right corner. 2. In the dialog box that is displayed, set the Kiosk view as prompted. Click **Copy** to copy the URL and save it to the local PC. 3. Click **OK**. After the setting is complete, you can share the URL with others who need to know the plant information. **NOTE** • The validity period of the URL of the Kiosk view is one year. • After the Kiosk view is generated, the plant running data is refreshed every 30 minutes. You can refresh the browser to obtain the latest data.

Menu Name	Description	Procedure
Layout	Displays the logical view and physical layout of PV modules in a plant to monitor energy yield at PV module level (each module requires an optimizer).	● Automatic generation of physical layout diagram 1. In the **Layout** tab page of a plant, click **Click to Upload** to upload a layout diagram. **NOTE** ● Click an image thumbnail to zoom in. ● Click the button in the upper-right corner of the thumbnail to delete the layout diagram. ● Click **Move Drawing** to adjust the position of the layout diagram. 2. Click **Generate Layout** to generate a physical layout diagram. 3. In the **Result** preview dialog box, click **Save** to save the generated physical layout diagram. 4. (Optional) If some QR codes are not recognized, manually bind the optimizers. a. In the **Physical Layout** area, click the saved layout diagram. b. On the **Layout Configuration** page, drag the optimizers in the **Device List** area on the left to the PV modules that are not successfully bound. c. Click .

<table>
<tr><th>Menu Name</th><th>Description</th><th>Procedure</th></tr>
<tr><td></td><td></td><td>NOTE
On the Layout Configuration page, you can perform the following operations to adjust the layout:
Adding a diagram element: Drag a component diagram element to the layout design area and adjust the diagram element position based on the site requirements.
Selecting a diagram element: Click a diagram element to select it, and press Ctrl+A to select all diagram elements. Hold down Ctrl and click diagram elements to select multiple diagram elements.
Moving a diagram element: After selecting a diagram element, drag it to adjust its position. Drag the mouse cursor in the blank area to move the drawing canvas.
Copying and pasting a diagram element: Right-click a diagram element to copy or delete it. After copying a diagram element, right-click in the view area to paste it.
Right-click a diagram element that has been bound to unbind it.</td></tr>
</table>

Menu Name	Description	Procedure
		● Manual configuration of physical layout diagram 1. In the **Physical Layout** area, click **Click to Create**. 2. On the **Layout Configuration** page, drag the diagram elements on the left to the design area based on the plant drawing. 3. Set the parameters based on actual conditions. 4. Click **Save**. The created device diagram element is displayed in the view area. 5. Click a device diagram element and set device attribute values in the **Device Attribute** area. 6. After the diagram element is created, drag the optimizer in the **Device List** area to the corresponding diagram element position for binding. 7. Click . The physical layout diagram is created successfully.
Devices	Allows you to monitor the devices bound to a plant in real time to handle exceptions promptly and ensure the safety of devices.	For details, see **1.4.2.1 Device Management**.
Alarms	Allows you to check alarms in real time and handle them promptly.	For details, see **1.5.2 Alarm Management**.
Reports	Displays plant, inverter, and battery reports in different dimensions and allows you to subscribe to and export reports.	For details, see **1.3 Report Management**.

----End

1.2.2 Map View

You can intuitively view the location and distribution of a plant in this mode.

Prerequisites

The SmartPVMS is connected to the network.

Procedure

1. Choose **Home** > **Home** > **Map View**. Or in the upper-right corner of the home page, click .
2. Click . In the displayed dialog box, set Default Map, and API Key.
3. **Optional:** Select the PV plant status, enter the PV plant name, and click . The location of the PV plant is displayed in the map view.
4. Move the pointer to the location of the target PV plant. The PV plant information of the Location, energy yield, and weather window is displayed.
5. Click the PV plant icon to view details. For details, see **Table 1-2**.

1.2.3 KPI View

Displays key energy yield indicators of the plants managed by the company, facilitating monitoring and management.

Procedure

1. Choose **Home** > **Home** > **KPI View**. Or in the upper-right corner of the home page, click .

   On the KPI View page, you can view the KPIs of the plants managed by the company.

1.2.4 Dashboard

You can view the company- or plant-level dashboard data of the entire intelligent O&M center.

Prerequisites

You have the permission for **Dashboard Display**.

Procedure

Step 1 Choose **Home** > **Home** > **Dashboard**.

NOTE

- By default, the company-level dashboard is displayed. Only six function modules can be displayed on the company-level dashboard and plant-level dashboard.
- Method for accessing the plant-level dashboard:
  - On the company-level dashboard, select a company and then a plant on the plant map to access the plant-level dashboard.
  - In the search box on the plant map, enter the plant name to enter the plant-level dashboard.

Step 2 In the upper-right corner of the company-level dashboard, click .

Step 3 In the displayed **Dashboard Configuration** dialog box, click the **Company Level** or **Plant Level** tab, Select a function block and drag it to set the layout. For details, see **Table 1-3** and **Table 1-4**.

Table 1-3 Description about the company-level dashboard

Section	Description
Plant map	Displays the locations of all plants under the current company.
Real-time Power	Displays the real-time power and current power. You can move the pointer on the time axis to view the data in the corresponding time period.
Energy Yield Ranking	Displays the top 10 plants of the current company by energy yield and their energy yields.
Yield	Displays the energy yield of the current month and the energy yield of the current day. You can drag the time axis to display data in the corresponding time period.
Real-time Alarm	Displays the total number of alarms of all plants under the current company and the number of alarms of each severity.
Environmental Benefits	Displays the environmental benefits of all plants under the current company, including carbon dioxide emission reduced, standard coal saved, and equivalent trees planted.
O&M Statistics	Displays the defect tasks of all plants under the current company.

Table 1-4 Description about the plant-level dashboard

Section	Description
Revenue This Month	Displays the monthly and daily revenues of the plant.

Section	Description
Real-time Power	Displays the real-time and current power of the plant. You can move the pointer on the time axis to view the data in the corresponding time period.
Real-time Alarm	Displays the total number of alarms of the plant and the number of alarms of each severity.
O&M Statistics	Displays the defect tasks of the plant.
Environmental Benefits	Displays the environmental benefits of the plant, including carbon dioxide emission reduced, standard coal saved, and equivalent trees planted.
Performance Ratio	Theoretical energy yield = Total irradiance in the daily KPI of the EMI x total string capacity of the plant System efficiency = Energy yield/Theoretical energy yield
Real-time Power and Irradiance	The EMI collects the irradiation strength and reports it to the SmartPVMS.
Yield This Month	Displays the monthly and daily energy yields of the plant. You can move the pointer on the time axis to view the data in the corresponding time period.

Step 4 Click **OK**.

----End

Follow-up Procedure

Exit the dashboard display: You can click the logo or title to return to the multi-plant home page.

1.3 Report Management

Report management includes **Plant Report**, **Inverter Report**, and **Battery Report** to display report data in different dimensions and allow you to subscribe to and export reports.

Prerequisites

- You have gained access to **Report Management**.
- The email server of the company has been configured. For details, see **1.6.1.4 Configuring an Email Server**.

Context

The revenue unit displayed for PV plants is the currency selected by the company to which the plant belongs. If the price unit is inconsistent with the local type, contact the company administrator to change the currency. For details, see **1.6.1.3 Company Information Configuration**.

Procedure

Step 1 Open the desired log pages as follows:

- Plant report: Choose **Reports** > **Reports** > **Plant Report**.
- Inverter report: Choose **Reports** > **Reports** > **Inverter Report**.
- Battery report: Choose **Reports** > **Reports** > **Battery Report**.

NOTE

- **Plant Report**: Collects the energy yield, power consumption, and income of the PV plant by time or plant.
- **Inverter Report**: Collects the energy yield and running status of solar inverters by day, month, and year.
- **Battery Report**: Collects the charging and discharging status of batteries by day, month, and year.

Step 2 Select a report function as required. For details, see **Table 1-5**.

Table 1-5 Report task

Task	Description	Procedure
Querying a report	Used to view the running data of a plant or device in a specified period.	Select a PV plant or device, set time, and click **Search**. NOTE In the plant report, if **Time dimension** is set to **By day**, the report displays only the energy yield and income.
Exporting a report	Used to save the query result to the local client.	Click **Export**.
Subscribing to a report	Used to send the report data of the plant or device to a user's mailbox.	Click **Subscribe**. On the displayed page, click **Add**. NOTE The system sends the statistical report of the previous day to the user's mailbox at 04:30 in the time zone of the selected plant or device.

----End

1.4 Plant

You can manage multiple PV plants in a centralized manner and manage the device adaptation packages, device upgrade, and device log export.

1.4.1 Plant

Manage the PV plant and plan the annual energy yield of the power station.

1.4.1.1 Plant Management

You can centrally manage multiple plants and view important information about a single plant. This meets different management requirements.

1.4.1.1.1 Creating a Plant

After a device is connected to the management system, you can create a plant in the management system.

Prerequisites

- You have commissioned devices and set management system parameters. For details, see the *FusionSolar App Quick Guide*.
- You have obtained the SN of the access device.

NOTE

If the devices are cascaded, record the SN of only one device so that the system automatically identifies the cascaded device when a PV plant is created.

Procedure

Step 1 Choose **Plants** > **Plants** > **Plant Management**.

Step 2 On the **Plant Management** page, click **Add Plant**.

Step 3 In the displayed dialog box, enter the basic information about the plant and click **Next**.

Step 4 Enter the SN of the device and click **Next**.

NOTE

- If multiple devices need to be connected, click **Add**.
- If the connected devices are cascaded, you only need to enter the SN of one device. The system automatically identifies the SNs of cascaded devices.

Step 5 Set the string capacity.

1. Select the inverter and click **Set String Capacity**.

   NOTE

   - For inverters with the same string capacity configuration scheme, the string capacity can be configured at the same time.
   - For inverters with different string capacity configuration schemes, the string capacity needs to be configured separately.

2. In the displayed dialog box, enter the PV capacity values and click **OK**.
3. Confirm the configured string capacity and click **Next**.

Step 6 On the **Set Electricity Prices** page, set **Feed-in Tariff** and **Purchase Price**, and click **Next**.

NOTICE

- The selected date range must cover a calendar year, and the start time and end time must cover a calendar day.
- If the price unit is inconsistent with the local type, contact the company administrator to change the currency. For details, see **1.6.1.3 Company Information Configuration**.

Step 7 On the **Set Other Info** page, configure the address, location, and time zone of the plant.

NOTE

When setting the plant time zone, ensure that the plant time zone is the same as the device time zone. Otherwise, the management system delivers the plant time zone to the devices to overwrite the time zone configured on devices after the plant is created.

Step 8 Click **Save**.

----End

Follow-up Procedure

For details about other operations, see **1.4.1.1.2 Managing Plants**.

1.4.1.1.2 Managing Plants

On the **Plant Management** page, you can manage multiple plants in a centralized manner, such as sharing EMI (Environmental Monitoring Instrument), sharing plants, and modifying plant information.

Prerequisites

You have logged in to the management system as an installer.

Procedure

Step 1 Choose **Plants** > **Plants** > **Plant Management**.

Step 2 On the **Plant Management** page, you can perform the operations listed in **Table 1** as required.

Table 1-6 Plant management operations

Operation	Procedure
Sharing EMI	1. In the plant list, select one or more plants that require EMI sharing and click **Shared EMI**. 2. In the displayed dialog box, select the EMI to be shared, and click **Save**. **NOTE** Each plant can receive a maximum of one EMI.

Operation	Procedure
Canceling EMI sharing	1. Select a plant that has received a shared EMI and click **Shared EMI**. 2. In the displayed dialog box, click **Reset**, and then click **Save**. 3. In the displayed dialog box, click **Confirm**.
Sharing a plant	1. Select a plant in the plant list and click **Share**. 2. In the displayed dialog box, enter the recipient contact information and click **OK**. **NOTE** A shared plant cannot be shared again.
Viewing sharing details	● For those who offered shared plants 1. In the plant list, click **Shared** in the **Shared Plant** column to view the sharing details. ● For those who received shared plants 1. Click **Shared Plants** in the company list on the left. 2. In the plant list, click **Received** in the **Share Plant** column to view the sharing details.
Canceling plant sharing	1. Select a shared plant in the plant list and click **Cancel Sharing**. 2. In the displayed dialog box, select the plant the sharing of which is to be canceled and click **Cancel Sharing**. **NOTE** Only those who have offered shared plants can cancel the plant sharing.
Modifying plant information	1. Click in the **Operation** column. 2. In the displayed dialog box, enter the basic information about the plant and click **Apply**. 3. Click **Save**.
Deleting a plant	Select a plant in the plant list and click **Delete** or in the **Operation** column.

----End

1.4.1.2 Plan Management

You can plan the annual energy yield of a plant for power scheduling decision-making, for example, on whether to feed power to the grid or whether to purchase electricity.

Prerequisites

You have permission to **manage plans**.

Procedure

Step 1 Choose **Plants** > **Plants** > **Plan Management**.

Step 2 On the **Plan Management** page, manage energy yield plans. For details, see **Table 1-7**.

Table 1-7 Plan management operations

Operation	Procedure
Adding an energy yield plan	1. Click **Add**. The **Add Plan** dialog box is displayed. 2. Set the energy yield plan information as prompted and click **OK**.
Deleting an energy yield plan	● Select one or more PV plants and click **Delete**. In the displayed dialog box, click **OK**. ● Click for a PV plant. In the displayed dialog box, click **OK**.
Modifying an energy yield plan	Click for a PV plant. In the displayed **Modify** dialog box, modify parameters as required and click **Save**.
Exporting energy yield plans	Select one or more PV plants and click **Export**.
Importing energy yield plans	Click **Import**. In the displayed dialog box, select the updated energy yield plan template and click **Open**.

----End

1.4.2 Device

Manage mediation packages on devices, upgrade devices, export device logs, and manage device licenses.

1.4.2.1 Device Management

You can manage all devices in a unified manner.

Procedure

Step 1 Choose **Plants** > **Device** > **Device Management**.

Step 2 On the **Device Management** page, perform operations based on the application scenario. For details, see **Table 1-8**.

Table 1-8 Device management operations

Operation	Procedure
Searching for a device	Set the search criteria and click **Search**. **NOTE** The communication status is described as follows: : The device is normal. : The device is faulty. : The device is disconnected.
Setting device parameters	1. In the device list, select the device to be configured, and click **Set Parameters**. 2. In the displayed dialog box, set parameters as required. Click **Set** for the settings to take effect. **NOTE** This function is supported only by Inverter, Battery, SmartLogger, and Smart Dongle.
Deleting a device	Select one or more devices and click **Delete**. In the displayed dialog box, click **OK**.
Exporting basic device information	Select one or more devices and click **Export Basic Info**.
Exporting device performance data	1. Select one or more devices and click **Export Performance Data**. 2. Select signal point, and click **OK**. 3. In the displayed **Export** dialog box, set **Task Name**, **Start Time**, and **End Time**, and click **OK**. 4. In the displayed **Export Performance Data** dialog box that is displayed, click . **NOTE** The naming convention of the exported file is as follows: Historical data_*Start time*_*End time*_*Export time*.
Changing a device name	1. Click for a device. 2. Change the name of the selected device and click **OK**.
Viewing device details	You can click a device name to view the device details.

Operation	Procedure
Replace device **NOTE** The following conditions must be met for device replacement: ● The current device is disconnected from the management system. ● Device replacement and commissioning have been completed on the device. For details, see *FusionSolar Smart PV Solution-Device Replacement Commissioning Guide*. ● The following types of devices can be replaced: inverter, Smart Dongle and communications module. ● Inverters of the same type can be replaced with each other. ● Inverters connected to the same SmartLogger or Smart Dongle can be replaced with each other.	1. Select a devices and click **Replace Device**. 2. In the displayed dialog box, enter the SN of the target device and click **View**. 3. Click **Replace**. **NOTE** When an inverter is replaced, the total energy yield and total power supply from grid data of the old device can be synchronized to the new device. After the device is replaced, the data is automatically calibrated on the new device.

----End

Follow-up Procedure

If automatic calibration fails due to device disconnection or poor network quality, manually calibrate the device after the fault is rectified.

1. Export the device performance data.
   a. Select the target inverter and click **Export Performance Data**.
   b. Select the total energy yield and total power supply from grid, and click **OK**.
   c. In the **Export** dialog box that is displayed, enter **Task name**, set **Start date** and **End date**, and click **OK**.

      NOTE

      Start date: You are advised to set this parameter to 30 days before the old device is disconnected. For example, if the old device is disconnected on September 30, set this parameter to August 30.

      End date: You are advised to set this parameter to any date after the device is disconnected.
   d. In the **Export Performance Data** dialog box that is displayed, click .
   e. Open the downloaded performance data file and record the latest valid values.
2. Calibrate the energy parameters.
   a. Select the target inverter and click **Set Parameters**.
   b. In the displayed dialog box, click **Feature Parameter**.

c. Enter the values of the total energy yield and total power supply from grid obtained in step **1.e**.

d. Click **Set**.

1.4.2.2 Adapter Management

The adapter packages is managed to reduce the dependency on the interface between the device and the SmartPVMS.

Prerequisites

- You have permission to **manage adapters**.
- You have obtained the NE mediation software package.

Procedure

Step 1 Choose **Plants** > **Device** > **Adapter Management**.

Step 2 On the **Adapter Management** page, manage adapter packages. For details, see **Table 1-9**.

Table 1-9 Adapter package management operations

Operation	Procedure
Uploading an adapter package	1. Click **Upload**. In the **Upload Adapter Package** dialog box, click , select an adapter package, and click **Open**. 2. Click **Upload**.
Installing an adapter package	Select an uploaded adapter package, click **Install** or , and complete the installation as prompted.
Uninstalling an adapter package	Select an installed adapter package and click **Uninstall** or . Then, click **OK** as prompted.
Deleting an adapter package	Select an adapter package, click **Delete** or , and click **OK**.
Reinstall an adapter package	Select the adapter package to be reinstall and click .

----End

1.4.2.3 Device Access

You can bind devices or unbind users connected to the system to quickly connect to or disconnect from a plant.

Prerequisites

- You have permission to manage device access.
- The new device has been connected to the SmartPVMS.

Procedure

Step 1 Choose **Plants** > **Device** > **Device Access**.

Step 2 On the displayed page, manage device access. For details, see **Table 1-10**.

Table 1-10 Operations related to new device management

Operation	Procedure
Binding to an existing PV plant	1. Select one or more devices and click **Bind to Existing Plant**. In the displayed dialog box, select a PV plant and click **OK**. 2. On the **Add Devices** tab page, click **Apply** and click **Confirm** to complete the device binding. 3. On the **Set String Capacity** tab page, select the bound devices and click **Set String Capacity**, In the displayed dialog box, set the string capacity and click **OK**. 4. Click **Save**, and then click **Confirm**.
Binding to a new PV plant	1. Select one or more devices and click **Bind to New Plant**. 2. In the displayed **Add Plant** dialog box, enter related information as prompted and click **Save** to complete the creation and device binding of the new plant.
Unbinding a user	Select a device whose **Bound User** is not empty, and click **Unbind User**.

----End

1.4.2.4 Upgrade Management

This function allows you to manage and upgrade app and device software versions..

Prerequisites

- You have permission to manage device upgrade.
- You have obtained the software packages required for device upgrade.
  - For details about how to obtain the device software package, see the upgrade guide of the corresponding device.
  - To obtain the app software package, perform the following steps:
    i. Log in to Huawei enterprise technical support website **http://support.huawei.com/enterprise**.
    ii. Browse or search for **SmartPVMS**.

iii. On the **Software** tab page, download the app software and digital signature file.

– After the downloading is complete, use the digital certificate and verification tool available at Huawei technical support website to verify the digital signature of the software package.

i. Log in to Huawei enterprise technical support website **http://support.huawei.com/enterprise**.

ii. Browse or search for **PGP Verify**.

Procedure

- Device Upgrade.

a. Choose **Plants** > **Device** > **Upgrade Management**. The **Software Packages** tab page is displayed.

b. On the **Software Packages** tab page, upload the device software package for upgrade. For details about the operations allowed, see **Table 1-11**.

Table 1-11 Version management operations

Operation	Procedure
Adding a software version	1. Click **Add**. 2. In the displayed **Add** dialog box, set **Device Type**, select the file to be uploaded and the verification file, set **Version Description**. 3. Click **OK**.
Deleting a software version	Select the target software version and click **Delete**.
Editing a software version	Select the target software version, click **Edit**, set related information, and click **OK**.

c. Click the **Device upgrade** tab. On the tab page, click **Add**.

d. In the displayed **Add** dialog box, set the upgrade mode, device type, target version, and devices. Select **Your operation will affect customer equipment**. **Obtain authorization in advance**, and click **OK**.

NOTICE

- **Upgrade now**: You do not need to confirm whether to upgrade the device. After a device upgrade task is added successfully, the task is executed immediately.
- **Upgrade after user authorization**: After upgrade tasks are added successfully, the system pushes all upgrade messages to all residential plant users. After a residential plant user logs in to the system through the app, the user can confirm the upgrade messages one by one. Once a residential plant user confirms an upgrade message, the corresponding device can be upgraded. If the user does not confirm the device upgrade message within 48 hours after the upgrade task is added, the upgrade result of the device is marked as timeout.

e. In the displayed dialog box, click **I Know**.

f. In the upgrade task list, click + to view the upgrade details.

- App Versions.
  - If the FusionSolar app version is 2.6.2 or earlier, upgrade the app version. Otherwise, the FusionSolar app functions cannot be used.
  - After a new version of the SmartPVMS app is released, upload the app software package on the SmartPVMS client to remind app users to upgrade the app.

a. Choose **Plants** > **Device** > **Upgrade Management**.

b. Click **App Versions**.

- Upload the app software package.

1) Click **Add**.

2) In the displayed dialog box, select an app type and upload the software package and verification file.

3) Click **Upload**.

NOTE

- If the software package is uploaded for the first time, you need to manually release it. On the **App Versions** tab page, click **Publish** in the **Operation** column of the corresponding software version.
- If a released version exists on the SmartPVMS client and a new version is uploaded, the system automatically releases the new version and suspends the historical version. Click **Republish** in the **Operation** column of the corresponding software version to change the version.

- Manage historical software packages.

Modifying the app type and remarks of a software package: Select the app version to be modified and click **Modify**.

Deleting a software package: After the app software package of the new version is uploaded, click **Delete** to delete the historical version to ensure that users can upgrade the app to the latest version.

NOTE

The SmartPVMS server scans the uploaded app software packages at 00:00 on the first day of each month and retains the released version and the latest suspended version. Other suspended versions are deleted by the system.

----End

1.4.2.5 Device Log Export

Allows users to export and view device logs, optimizer logs, and battery storage logs.

Procedure

Step 1 Choose **Plants** > **Device** > **Device Log Export**.

Step 2 In the log list, select one or more devices whose logs need to be exported and click **Start export** to create an export task.

Step 3 Select one or more ongoing export tasks and click **Stop export** to stop the selected tasks.

Step 4 After the logs are exported, select the devices whose logs need to be saved and click **Save logs** to download the logs to the local PC.

NOTE

- After the logs are exported successfully, the logs will be automatically cleared after 24 hours if the logs are not saved to the local PC.
- After the logs are saved successfully, the logs will be automatically cleared after 2 hours.

----End

1.4.2.6 Device License Management

This section describes how to check device license status on the **Device License Management** page. When the license files are about to expire or have expired, or the I-V curve function needs to be enabled for devices, you can apply for and update the licenses in a timely manner to ensure that the I-V curve function can be used properly.

Context

Before starting the I-V curve scanning, you need to load the corresponding device licenses.

Procedure

1. Choose **Plants** > **Device** > **Device License Management** from the main menu.
2. **Table 1-12** describes the operations related to device license management.

Table 1-12 Operations related to device license management

Task Name	Procedure
Checking license information	On the **License Information** tab page, enter the **Device name**, **Plant name**, and **Device SN**, or select **License status**, and click **Search**.
Applying for device licenses	1. On the **License Application** tab page, click **Export All** or select the devices for which you want to apply for licenses, and click **Export Selected**. 2. After exporting the application form, send it to system administratortechnical support engineers to apply for a license file.
Loading device licenses	1. Click **Upload License** to upload license files. 2. After the license files are uploaded successfully, click **Load All** to load the licenses for all devices. Alternatively, select the devices for which licenses need to be loaded and click **Load Selected** to load the licenses for the selected devices. During the loading, click **Stop Loading** to stop all loading tasks. If you select the loading tasks to be stopped and then click **Stop Loading**, the selected tasks will be stopped.
Revoking device licenses	● Select one or more devices whose licenses are to be revoked and click **Revoke License**. ● For devices whose licenses have been revoked, click **Export All Revocation Codes** or **Export Selected Revocation Codes** to export the license revocation codes of all or selected devices. After obtaining the revocation codes, contact system administratortechnical support engineers to apply for new license files using the ESNs and revocation codes of the current licenses.

1.5 Maintenance

You can learn the real-time status, location distribution, and alarm information of PV plants through O&M, and quickly trace and handle PV plant faults.

1.5.1 Real-time Status

The real-time status of plants allows you to learn about the plant status, location, and alarm information, facilitating quick tracking and handling of plant faults.

Procedure

Step 1 Choose **Maintenance** > **Maintenance** > **Real-Time Status** from the main menu.

- View the plant status and evaluate the plant advantages by comparing the plants in the same environment.
  a. In the Plant Status Center area, select a maximum of five plants to be compared and click the in the upper-left corner.In the displayed Comparison of plants dialog box, view the plant comparison charts about power per MW and specific energy (kWh/kWp).
  b. Drag below a comparison chart to display the plant comparison chart in the specified period.

  NOTE

  - Click to remove a plant that participates in the comparison.
  - Click to add a plant for comparison.
- View the plant map to learn about the geographical distribution of the plant.
  - In the list in the **Plant Status Center** area, select a plant and click . The location details of the plant are displayed under the SmartPVMS, and the alarms of the plant are displayed in the **Plant Alarm Center** area.
  - Under the SmartPVMS, enter a plant name to search for the plant, or select **All** as the plant status. The plants that meet the search criteria are displayed on the map.

  NOTE

  Move the pointer over a plant icon to display the plant details.

  Click in the lower-left corner of the map to switch between maps.

  Click in the lower-left corner of the map. In the **Map Settings** dialog box, set the default map and API key.
- View the real-time alarms of the PV plant, and acknowledge and trace the alarms.
  a. In the **Plant Alarm Center** area that displays active and acknowledged alarms, click to expand the alarm cause and handling suggestions.
  b. Analyze and handle the alarm based on the alarm cause.
     - Click **Clear**. In the displayed dialog box, click **OK**. The alarm is deleted from the list.
     - Click **Confirm**. In the displayed dialog box, click **OK**. The alarm status changes to **Acknowledged**.
     - Click **Recovery**. In the displayed **New Defect Elimination** dialog box, set related information and submit the defect elimination process. The handler will receive the defect elimination task.
     - Click **Device details** to view the device details.

----End

1.5.2 Alarm Management

This section describes how to view and manage current and historical alarms of devices, the system alarms. Device alarms are used to trace real-time and historical alarms of devices. System alarms are used to trace alarms generated during system operations.

1.5.2.1 Monitoring and Viewing Current Alarms

On the **Current Alarms** page, O&M personnel can view current alarms that are updated in real time to better understand the latest alarm information.

Context

- The maximum number of alarms displayed on the **Current Alarms** page is 300,000 when the physical memory is 3.5 GB. If a new alarm is reported and the number of current alarms exceeds the upper limit, alarm management enables the function of processing full current alarm cache and moves some alarms to the historical-alarm list.
- When you go to the **Current Alarms** page for the first time, alarms in the alarm list are sorted in descending order of **Arrived On** by default.
- The newly reported alarms are displayed in bold on the page.
- The background color of cleared alarms is green by default.
- You can only monitor and view alarms of authorized MOs.
- Alarm synchronization period.
  – SmartLogger3000, Distributed SmartLogger, Dongle2.0: 1 minute.
  – SmartLogger1000, SmartLogger2000, Inverter, Dongle1.0: 5 minutes.

  NOTE

  - A maximum of 50 to 100 alarms can be synchronized every minute. Synchronizing more alarms will take longer time.
  - If a device upgrade, historical data recovery, or log export task is being executed, start alarm synchronization after the task is complete.

Procedure

- Monitoring alarms
  a. Choose **Maintenance** > **Maintenance** > **Alarm Management** from the main menu.
  b. **Table 1-13** describes alarm monitoring methods.

Table 1-13 Alarm monitoring methods

Task	Task Description
Monitoring alarms using the alarm list	O&M personnel can monitor alarms reported by all NEs and systems on the **Current Alarms** page in real time. A maximum of 300,000 alarms can be displayed on the page when the physical memory is 3.5 GB.

Task	Task Description
Monitoring alarms using alarm indicators	The alarm indicators in the upper right corner of the **Current Alarms** page show the number of critical alarms, number of major alarms, number of minor alarms, and number of warning alarms.
Monitoring alarms using the statistics panel	Click in the upper right corner of the **Current Alarms** page to view the alarm statistics charts. The statistical result is obtained based on the filtered alarms. The **Top 10 Alarms**, **Duration**, **Top 10 Alarm Sources**, **Severity**, and **Status** statistical charts can be displayed on the statistics panel. Four statistical charts can be displayed at the same time. You can click in the upper right corner of the statistics panel and then select the chart to be displayed from the drop-down menu in the upper right corner of each chart. On the statistics panel, you can click any statistical result to quickly display the alarms that meet the condition. If you close the statistics panel, the filter criteria selected on the panel are automatically deselected. **NOTE** ● Alarm management allows a maximum of 10 statistics panels to be opened by online users concurrently. ● You can click in the upper right corner of the statistics panel to manually refresh the statistical data. Within 10 minutes after you open the statistics panel or manually refresh the statistical data, the system automatically refreshes the data every minute.

- Querying alarms
  a. Choose **Maintenance** > **Maintenance** > **Alarm Management** from the main menu.
  b. You can click **Template Management** in the upper left corner of the page to view all filter templates and select a filter template from the **Quick Filter** panel. Users with the **Administrators** role can manage templates saved by all users.

     The following types of templates are provided:

     - **Favorite**: You can add the templates that you often use to your favorites.
     - **Custom**: Filter templates customized by the current user, which can be shared to other users.

- **Shared**: Available filter templates shared by other users.
- **Default**: Default filter template.
- **Other**: Filter templates that are not shared by other users. These templates are visible only to users with the **Administrators** role.

NOTE

The filter templates on the **Current Alarms**, and **Historical Alarms** pages are independent from each other and cannot be shared.

c. If the filter templates on the **Template Management** panel do not meet your requirements, click **Filter** in the upper left corner of the **Current Alarms** page. Set filter criteria and click OK to search for the alarms to be concerned about and handled.

d. Click **Save** or **Save As** to save the current filter criteria as a filter template.

e. Export current alarms. Alarms can be exported to an .xlsx or .csv file. When the export file format is set to .xlsx and the number of alarms exceeds 100,000, the file is exported as a .zip package. When the exported file format is set to .csv and the number of alarms exceeds 10,000, the file is exported as a .zip package.

- Export some alarms: Select the alarms to be exported, click **Export**, and choose **Selected**.
- Export all alarms: Click **Export** and choose **All**.

NOTE

Only the information about the alarm columns displayed on the page can be exported. You can click  in the upper right corner of the alarm list to set the alarm columns to be displayed.

- Alarm sound

  Alarm Management provides the alarm sound notification function. By default, the function is mute. If you do need the function, click  in the upper-right corner of the **Current Alarms** page to enabled the alarm sound.

  – : Sound is enabled. When an alarm is reported, the sound box on the user's PC plays a sound.

  – : Indicates the mute mode. No sound is played when an alarm is reported.

Parameter Description

For details about parameters on the alarm filter panel, see **Table 1-14**.

Table 1-14 Description of parameters on the alarm filter panel

Parameter	Description
Alarm name	Name of the alarms to be queried.
Alarm source	Device where an alarm is generated. If multiple alarm source conditions are set, the filtering result is the union of all the conditions. That is, all the alarms that meet any of the conditions are displayed on the page.
Severity	Alarm severities, including critical, major, minor, and warning. By default, all severities are selected. You need to select at least one alarm severity.
Alarm status	Alarm status, including the acknowledged and cleared, acknowledged and uncleared, unacknowledged and cleared, unacknowledged and uncleared.
Last occurred	Time when the alarm last occurred. This parameter is displayed as **Occurred** in **Historical Alarms**, indicating the last occurrence time of an alarm.
Cleared	Time when an alarm is cleared.

Parameter	Description
Advanced settings	You can set filter criteria to filter desired alarms. If multiple advanced setting conditions are set, the filtering result is the intersection of all the conditions. That is, the alarms that meet all the advanced setting conditions are displayed on the page. Operators (case-sensitive): ● **contains**: Filters the alarms that contain the specified character string. ● **does not contain**: Filters alarms that do not contain the specified character string. ● **begins with**: Filters alarms that begin with the specified character string. ● **ends with**: Filters alarms that end with the specified character string. ● **is in**: Filters the alarms that are the same as the specified character string. For example, in the **Location Info** area, set **Operator** to **is in** and set **Value** to *XXX*. In this case, the location information of the filtered alarms contains *XXX*, and the alarms whose location information contains *XXX***123** are not displayed. ● **is not in**: Filters alarms that are different from the specified character string. For example, in the **Location Info** area, set **Operator** to **is not in** and set **Value** to *XXX*. In this case, the location information of the filtered alarms does not contain *XXX*, and the alarms whose location information contains *XXX***123** are displayed. ● **Blank**: Filters the alarms if their values of this parameter are empty. ● **Non-blank**: Filters the alarms if their values of this parameter are not empty.

For details about parameters in the alarm list, see **Table 1-15**.

Table 1-15 Description of parameters in the alarm list

Name	Description
Plant Name	Plant of an alarm source.
Device Type	Type of the Device where an alarm is generated.
Device Name	Device where an alarm is generated.
Type	Type of an alarm, indicating the type of the cause which triggers the alarm.

Name	Description
Name	Name of an alarm. An alarm name tells what faults occur on an alarm source. For example, the high CPU usage alarm can be known by its name that the alarm is sent from the CPU.
Alarm ID	ID of an alarm, which corresponds to the alarm name.
Possible ID	ID of the specific cause of the alarm.
Severity	Four alarm severities, which include acknowledge, clear, comment, and copy.
Clearance Status	Clearance status of an alarm. Available options are: ● **Cleared** ● **Uncleared**

Name	Description
Clearance Type	Alarm clearance type: ● **(Blank)**: uncleared. ● **normal clear**: A device fault is rectified and alarm management receives a clear alarm. Then the alarm is automatically cleared. ● **restore clear**: After a device restarts, alarm management detects whether a fault exists. The original fault alarm is automatically cleared. ● **manual clear**: An alarm is manually cleared. ● **configure clear**: A resource object is deleted, and the alarms generated by the resource object are automatically cleared. ● **correlation clear**: When receiving a root alarm of uncleared correlative alarms, alarm management handles the alarms using a correlation rule, reports the root alarm, and automatically clears the correlative alarms. The clearance type of the correlative alarms is correlation clearance. ● **clear from system**: The system clears earlier alarms according to the full-cache processing rule because the storage space is limited. ● **status switch clear**: Because the device status switches, the active alarm in the previous status is automatically cleared and is reported again in the device status after the switch. The clearance type of the active alarm in the previous status is status switch clearance. ● **alarm synchronization-based clear**: During alarm synchronization, if some uncleared alarms exist in alarm management but cannot be found in the alarms synchronized from NEs, these uncleared alarms are automatically cleared. This parameter is not displayed on the **Masked Alarms** page.
Acknowledgement Status	Acknowledgement status of the alarm. Available options are: ● **Acknowledged** ● **Unacknowledged**
Acknowledged On	Time when an alarm is acknowledged.

Name	Description
Defect Status	If a defect ticket has been created for the alarm, the defect status can be either of the following: ● **In Elimination** ● **Processed** If no defect ticket is created for the alarm, this field is left blank.

For details about the parameters on the Alarm Information tab page, see **Table 1-16**.

Table 1-16 Description of the Alarm Information tab page

Tab Page	Description	Operation Method
Details	For details about alarm parameters, see **Table 1-15**.	To set the parameters to be displayed on the **Details** tab page, click in the upper right corner of the **Details** tab page.
Handling and Experience	● On the **Handling** tab page, you can view alarm handling recommendations pre-configured in alarm management. ● On the **Experience** tab page, you can view or modify alarm handling experience.	To modify the experience records, click **Experience**. On the tab page that is displayed, click **Modify**, record the experience, and then click **Save**.
Comments	On the **Comments** tab page, you can add comments for the alarm.	To modify comments, click **Modify** in the upper right corner of the tab page, enter comments, and then click **Save**.
Handling Records in Last 2 Months	You can view all manual operations performed on the alarm in the last two months for O&M personnel to handle alarms.	-

Description of the Buttons in the alarm operation bar, see **Table 1-17**.

Table 1-17 Buttons in the alarm operation bar

Button	Description
Combo Sorting	Sorts alarms by multiple alarm fields. A maximum of four alarm fields can be set.
Clear	When the fault that triggers an alarm is rectified but the alarm is not cleared automatically, click **Clear** to manually clear the alarm. After the alarm is cleared, its status is changed to **Cleared**.
Acknowledge/ Unacknowledge	After an alarm is acknowledged, the alarm will be or has been handled. When the alarm is acknowledged, the alarm status is changed from unacknowledged to acknowledged. If you want another engineer to handle the alarm, you can unacknowledge the alarm. When the alarm is unacknowledged, the alarm status is changed from acknowledged to unacknowledged.
Comment	Edits the comments of an alarm.
Export	Alarms can be exported to an .xlsx or .csv file. When the export file format is set to .xlsx and the number of alarms exceeds 100,000, the file is exported as a .zip package. When the exported file format is set to .csv and the number of alarms exceeds 10,000, the file is exported as a .zip package. A maximum of five users can export some alarms at a time, and a maximum of two users can export all alarms at a time.
Recovery	Recording, tracking, and monitoring of faults or defects.

For details about the parameters on the **Template Management** panel, see **Table 1-18**.

Table 1-18 Buttons on the Template Management panel

Button	Description	Operation Method
Search Template	You can search for a filter template based on the template name, name of the user who created the template, or comments.	1. On the **Quick Filter** panel, enter a template name, username, or comment in the search box. 2. Click to search the template.

Button	Description	Operation Method
Share/ Unshare	You can share or cancel the sharing of custom templates. You can also select a template shared by other users from the **Shared** area. The administrator can share or cancel the sharing of all templates except the default templates. Other users can only share or cancel the sharing of custom templates. ● : The template is not shared. ● : The template is shared.	1. On the **Quick Filter** panel, select the desired template. 2. Click the icon next to the template name.
Add to Favorites/ Remove from Favorites	You can add a template to or remove a template from your favorites. The favorite template will be displayed in the **Favorite** area. You can only perform the following operations on the preset templates: **Add to Favorites**, **Remove from Favorites**, **Set as Default Template**, or **Cancel Default Template**. ● : The template is not added to favorites. ● : The template is added to favorites.	
Set as Default Template/ Cancel Default Template	You can set or cancel the default template for the current page. Filtered alarms will be displayed based on the default template when you enter this page. If is displayed on the right of a template, it is a default template.	1. On the **Quick Filter** panel, select the desired template. 2. Click on the right of the template. 3. In the displayed menu, select **Set as Default Template** or **Cancel Default Template**.

Button	Description	Operation Method
Rename	Renames a filter template. The administrator can rename all the templates except the templates in the **Default** area. Other users can rename only custom templates.	1. On the **Quick Filter** panel, select the desired template. 2. Click on the right of the template. 3. Choose **Rename** from the displayed menu. 4. In the dialog box that is displayed, enter the new template name.
Modify Comments	Modifies the comments of a filter template. The administrator can modify the comments of all templates except the templates in the **Default** area. Other users can modify only the comments of the custom templates.	1. On the **Quick Filter** panel, select the desired template. 2. Click on the right of the template. 3. Choose **Modify Comments** from the displayed menu. 4. In the dialog box that is displayed, modify the comments.
Delete	Deletes a filter template. The administrator can delete all the templates except the templates in the **Default** area. Other users can delete only custom templates.	1. On the **Quick Filter** panel, select the desired template. 2. Click on the right of the template. 3. Choose **Delete** from the displayed menu.
Open Template on New Tab	A new tab page is opened and the list of the alarms or events that are filtered using the filter template is displayed on the new tab page.	1. On the **Quick Filter** panel, select the desired template. 2. Click on the right of the template, or click and choose **Open Template on New Tab**.

1.5.2.2 Viewing Historical Alarms

By analyzing historical alarms, users can understand device running statuses and determine whether rules are properly configured.

Context

- By default, 20,000 historical alarms can be displayed. When the number of alarms exceeds the upper limit, the first 20,000 alarms are displayed based on the filter criteria and sorting. If you want to query other alarms, you can modify the filter criteria and sort the alarms.
- You can only monitor and view alarms of authorized MOs.
- A total number of 30 **Historical Alarms** pages can be opened concurrently by online users.

Procedure

Step 1 Choose **Maintenance** > **Maintenance** > **Alarm Management** from the main menu.

Step 2 On the **Historical Alarms** page, click **Filter** to expand the panel and set filter criteria to find desired historical alarms.

Step 3 Click **Save** or **Save As** to save the current filter criteria as a filter template.

You can click **Template Management** in the upper left corner of the page to view all filter templates and select a filter template from the **Quick Filter** panel. Users with the **Administrators** role can manage templates saved by all users.

The following types of templates are provided:

- **Favorite**: You can add the templates that you often use to your favorites.
- **Custom**: Filter templates customized by the current user, which can be shared to other users.
- **Shared**: Available filter templates shared by other users.
- **Other**: Filter templates that are not shared by other users. These templates are visible only to users with the **Administrators** role.

NOTE

The filter templates on the **Current Alarms**, and **Historical Alarms** pages are independent from each other and cannot be shared.

Step 4 Export historical alarms. Alarms can be exported to an .xlsx or .csv file. When the export file format is set to .xlsx and the number of alarms exceeds 100,000, the file is exported as a .zip package. When the exported file format is set to .csv and the number of alarms exceeds 10,000, the file is exported as a .zip package.

- Export some alarms: Select the alarms to be exported, click **Export**, and choose **Selected**.
- Export all alarms: Click **Export** and choose **All**.

NOTE

Only the information about the alarm columns displayed on the page can be exported. You can click in the upper right corner of the alarm list to set the alarm columns to be displayed.

----End

1.5.3 Task Management

This topic describes how to manage inspection tasks and defect elimination tasks to ensure the normal running of plant devices. Inspection is performed in the form of tasks and inspection tasks are specified for each plant. Defect elimination enables recording, tracking, and monitoring of faults or defects as well as archiving after elimination or elimination acceptance.

Procedure

Step 1 Choose **Maintenance** > **Maintenance** > **Task Management** from the main menu.

Step 2 On the **Task Management** tab page, choose **Inspection Management** or choose **Defect Elimination Management** to manage and trace tasks. .

- The task list is a dimension of tasks. You can view the execution information about inspection tasks. The Plant List displays the information about the last inspection result of a plant by plant. The procedure for creating a task is the same as that for executing a task. For details, see **Table 1-19**.

Table 1-19 Inspection task operations

List Type	Operation	Procedure
Task List	Searching for a task	Set the task name, start time, and task status, and click **Search**.

List Type	Operation	Procedure
	Adding an inspection task	1. Configuring inspection items a. Click **Set Inspection Items**. The **Set Inspection Items** dialog box is displayed. b. Select a plant and click **Add**. Set the inspection item name and description, and click **OK** to create an inspection item. c. Select an inspection item, and click **Modify** to modify the inspection item, or click **Delete** to delete the inspection item. **NOTE** The preset inspection items in the system cannot be modified or deleted. d. **Optional:** Select a plant and click **Export** to export inspection items. e. **Optional:** Click **Download Template**, edit the inspection item name and description in the template, and click **Import** to create an inspection item. 2. Setting node personnel a. Click **Set Handlers**. The **Set Handlers** dialog box is displayed. b. Select a node and set the handler of the node. 3. Click **Add**, set the task name and description, select plants, and click **OK**. 4. Click **Execute** in the **Operation** column, select the handler for the next node, enter the transfer opinion, and click **Submit**.
	Viewing task details	Click + for an inspection task.
Plant List	Searching for a Plant task	Set the last inspection time and click **Search**.

- Defect elimination management is to track and manage the tasks of defect elimination. For details, see **Table 1-20**.

Table 1-20 Defect elimination tasks

Operation	Procedure
Creating a Defect Elimination Task	1. Setting node personnel a. Click **Set Node Personnel**. The **Set Node Personnel** dialog box is displayed. b. Select a node and set the handler of the node. If no personnel is set for a node, **All** is displayed. 2. Click **Add**, set information as required, and click **Submit**. After a defect elimination ticket is created, the defect elimination process starts. The principle owner starts to execute the next node. **NOTE** The principal owner to be selected must meet the following requirements: ■ The user has the permission of defect elimination management. ■ The user is in the node personnel list. 3. In the Operation column, click **Execute**. The **Execution Flow** dialog box is displayed. Execute the defect elimination process based on the actual defect elimination status.
View Task Details	In the Operation column, click Details.

----End

1.5.4 Smart Diagnosis

Supports I-V curve scanning and health diagnosis for PV strings to detect potential PV string faults in a timely manner and improve PV plant quality.

1.5.4.1 I-V Curve

Device voltage and current data can be obtained through I-V curve scan to analyze and evaluate the health status of PV strings and automatically generate a diagnosis report to facilitate O&M.

Prerequisites

- You have the **Smart Diagnosis** permission.
- You need to load the corresponding device licenses. For details, see **1.4.2.6 Device License Management**.

Procedure

Step 1 Choose **Maintenance** > **Maintenance** > **Smart Diagnosis** from the main menu.

Step 2 Click **Configure Strings** on the **IV curve** page to configure parameters.

Step 3 In the displayed **Configure Strings** dialog box, select one or more devices, and click **Configure Strings**.

Step 4 In the displayed **Configure String Details** dialog box, set parameters and Click **Save**.

NOTE

- If the PV strings are connected in **2-in-1** mode, select **2-in-1 string** when configuring the string details.
- For the Japanese model SUN2000-4.95KTL-JP1, if two PV strings are connected to the same MPPT circuit, **2-in-1** string must be selected.

Step 5 Manage diagnosis tasks on the **IV curve** page. For details, see **Table 1-21**.

Table 1-21 Diagnosis task operations

Operation	Procedure
Creating a diagnosis task	1. Click **Add Diagnosis Task**. 2. Set information as required. 3. Click **Start Scanning** to add an I-V curve scanning task.
Viewing scanning details	In the task list, click **View Details** to view the details about the scanned object.
Viewing and exporting scanning results	1. Click + in the task list to expand **Fault List**. 2. Click **Export** to export the scanning result list. Click **View** in the list to view exception handling suggestions.

----End

1.5.4.2 Module Library

If the preset PV module information templates cannot meet requirements, you can customize a PV module information template to improve the accuracy of I-V diagnosis.

Prerequisites

You have the **Smart Diagnosis** permission.

Context

- The PV module information template added by the system administrator is preset in the system and can be viewed and used by all users. The PV module information template added by a company administrator can be viewed and used by all users in the company. The PV module information template added by an installer can be viewed and used only by the installer.
- A company administrator can add a maximum of 100 PV module information templates. An installer can add a maximum of 20 PV module information

templates (if an installer needs to add more templates, the installer needs to contact the system administrator).

- If a PV module information template is in use, modifying or deleting the template does not affect the use by configured PV modules.

Procedure

Step 1 Choose **Maintenance** > **Maintenance** > **Smart Diagnosis** from the main menu.

Step 2 In the navigation pane, choose **Module Library**.

Step 3 On the **Module Library** page, you can perform the following operations as required.

Table 1-22 Module library operations

Operation	Procedure
Querying a module information template	Set the search criteria and click **Search**.
Adding a module information template	1. Click **Add**. 2. Set module information and click **Save**.
Downloading a template	Click **Download Template** to download the template file for importing module information.
Importing a module information template	Click **Import** and select the template file that has been filled in. **NOTE** The file containing a maximum of 100 module information records can be imported at a time. The file size cannot exceed 1 MB.
Modifying a module information template	In the module information list, click **Modify** in the **Operation** column for the module information template to be modified.
Viewing details	In the module information list, click **View Details** in the **Operation** column for the module information template to be viewed.
Exporting a module information template	1. In the list, select the modules whose information you want to export. 2. Click **Export** to save the exported module information as a file to the local PC.
Deleting a module information template	In the module information list, select the module information templates to be deleted and click **Delete**.

----End

1.5.5 Smart Tracking

Inverters adjust tracker angle based on tracker status and weather conditions so that the plant can obtain the maximum energy yield and effectively avoid damage to PV modules caused by bad weather, thereby increasing revenue.

Prerequisites

You have the **Smart Tracking** permission.

Context

- When the tracker type is tilted single axis, the azimuth and tilt angle can be set.
- When the tracker type is horizontal single axis or vertical single axis, only the azimuth can be set.

Procedure

Step 1 Choose **Maintenance** > **Maintenance** > **Smart Tracking** from the main menu.

Step 2 On the **Smart Tracking** tab page, set **Plant selection**, **SmartLogger name**, and **Inverter name**, and click **Search** to query the inverters that support smart tracking.

Step 3 In the inverter list, click  to expand the tracker list of the inverter.

- To set a single tracker, perform the following steps:
  a. Click **Set** in the **Operation** column of the tracker to be adjusted.
  b. In the dialog box that is displayed, select **Control Mode**, set **Azimuth** and **Tilt Angle**, and click **OK**.
- For details about how to set trackers in batches, see **Table 1-23**.

Table 1-23 Batch settings

Mode	Description	Procedure
Automatic mode	An inverter in automatic mode can automatically adjust the tracker angle based on sunlight conditions to obtain the maximum energy yield.	1. Click **Set Automatic Mode**. 2. In the displayed dialog box, select plants and SmartLoggers in the navigation tree on the left to query the inverters that support smart tracking. 3. Select the inverters to be set and click **Set to Automatic Mode**. 4. In the displayed dialog box, click **OK**.

Mode	Description	Procedure
Manual mode	Manually adjust the tracker angle based on the tracker status and weather conditions.	1. Click **Set Manual Mode**. 2. In the displayed dialog box, select plants and SmartLoggers in the navigation tree on the left to query the inverters that support smart tracking. 3. Select the inverters to be set and click **Set to Manual Mode**. 4. In the displayed dialog box, click **OK**. 5. Select the inverters that have been set to manual mode, set **Azimuth** and **Tilt Angle**, and click **Apply**.
Weather mode	Set inverters to the wind, rain, overcast, or snow mode based on the weather conditions to protect PV modules.	Click **Wind**, **Rain**, **Overcast**, or **Snow**. In the displayed dialog box, click **Yes**.
Fault rectificati on	Reset inverters to rectify tracker faults.	1. Click **Fault Rectification**. 2. In the displayed dialog box, select plants and SmartLoggers in the navigation tree on the left to query the inverters that support smart tracking. 3. Select the inverters whose faults need to be rectified and click **OK**. 4. In the displayed dialog box, click **OK**.

----End

1.6 System

1.6.1 Company Management

A company administrator can create and manage companies and organizational structures, and maintain company information based on business requirements.

1.6.1.1 Creating a company

Create a company under the root node or create a subsidiary under a company node based on service requirements.

Prerequisites

You have permission to perform operations on **Company Management**.

Context

- The system administrator or a user who has the rights of the system administrator can select the root node to create a company, or select a company from the navigation tree on the left to create a subsidiary for the company.
- An installer user can create a subsidiary for the company to which the installer belongs, or select a target subsidiary and create a lower-level subsidiary for the selected subsidiary.

Procedure

1. Choose **System** > **System** > **Company Management** from the main menu.
2. Click **Add Company**.
3. In the dialog box that is displayed, enter the basic information about the company.

   NOTE

   - When a company is created under the root node, a company administrator account of the installer role is also created.
     - **Username**: Indicates the username used by the company administrator to log in to the SmartPVMS.
     - **Mobile number**: Indicates the mobile number used by the company administrator to log in to the SmartPVMS.
     - **Email**: Indicates the personal email address of the company administrator. The email address can be used to receive subscribed reports, alarm push messages, and verification codes for password retrieval.
   - **Start date of safe running**: Indicates the day when the plant starts to generate energy normally. It is mainly used to calculate the safe running days of the plant.
   - **Longitude and latitude**: Indicates the location and scope of a company. Click . On the displayed map, drag the circle to set the longitude and latitude, and drag the hollow area of the arc to set the radius.
4. Click **OK**.

Follow-up Procedure

After a company is created, you can click the **Company Info** tab page to supplement or modify the basic information about the company.

Related Operations

- Modifying company information: Select the target company, click the **Company Info** tab page, and modify or supplement the basic information about the company.
- Deleting a company:
  a. Select the target company and click **Delete Company**.

NOTE

- Before deleting a company, you need to delete the users and PV plants managed by the company.
- If a subsidiary already exists under the company, delete the subsidiary first.

b. Click **OK**.

1.6.1.2 Creating a User in the Company and Associating the User with the Plant

After an administrator or installer creates a user and adds the user to a role, the user has the rights of the role. User authorization is complete.

Prerequisites

You have permission to perform operations on **Company Management**.

Procedure

1. Choose **System** > **System** > **Company Management** from the main menu.
2. Choose a company or subsidiary from the navigation tree on the left and click **Add user**.
3. In the displayed dialog box, enter the basic information about the user and click **Next**.

   NOTE

   The mobile number entered can be used as the mobile number used to log in to the SmartPVMS.
4. Select a role to which the user belongs and click **Next**.
5. Select the plant associated with the user and click ».

   NOTE

   Associate an installer with a company. The installer can manage all PV plants of the company within its role permissions.
6. click **Confirm**.

Related Operations

- Modifying user information: Select the target user and click .
- Resetting user password: Select the target user and click .
- Deleting a user: Select the target user and click .

  NOTE

  - The current user cannot be deleted.
  - Deleting a logged-in user will force a logout of the user. Therefore, exercise caution when performing this operation.
- Disabling a user: Select the target user and click .

- Enabling a user: Select the target user and click .
- Export personal information: Only the system administrator with the user management permission can modify or export user information. If you need to export personal information, contact and authorize the system administrator to export the information.

1.6.1.3 Company Information Configuration

After a company is created, a system administrator or user who has the system management permission can add or modify the basic information about the company.

Prerequisites

You have permission to perform operations on **Company Management**.

Procedure

Step 1 Choose **System** > **System** > **Company Management** from the main menu.

Step 2 In the navigation tree on the left, choose the target company and click **Company Info**.

Step 3 On the **Company Info** page, add or modify basic company information.

- **Currency**: Multiple currencies are supported. You can select a currency based on the site requirements.

  NOTE

  The revenue unit displayed for PV plants is the currency selected by the company to which the plant belongs. You cannot switch the currency unit by switching the system language.

- **Support for poverty alleviation PV plant**: When the status is , the poverty alleviation PV plant can be connected.
- **Title/Logo on the home page**: You can customize the title and company logo on the home page as needed.
- **Title/Logo on the dashboard**: You can customize the title and company logo on the dashboard as needed.

Step 4 Click **Save**.

----End

1.6.1.4 Configuring an Email Server

Configure an email server for the company to send subscription emails to users for service functions such as report subscription and alarm push. For data security during communication, you are advised to configure the email server certificate. To prevent certificate expiration or private key leakage, you need to periodically update the certificate (once every three months is recommended). If the certificate is about to expire, update them in a timely manner.

Prerequisites

- You have permission to perform operations on **Company Management**.
- The interconnected email server must support the Simple Mail Transfer Protocol (SMTP).
- You have obtained the server information from the SMTP server administrator, such as the domain name or IP address, port number, whether identity authentication is required, user name, and user password.
- The SMTP port is available.
  - In common connection mode, port 25 is used.
  - In TLS connection mode, port 587 is used.
  - In SSL connection mode, port 465 is used.

Context

- If a company has multiple levels of subsidiaries, the email server must be configured based on the following rules:
  - If a company has configured an email server but no subsidiary has, all subsidiaries use the email server to send subscription emails.
  - If no email server is configured for a subsidiary, the email server configured for the upper-level subsidiary is used by default to send subscription emails. The email server configured for the lower-level subsidiary cannot be used.

Company Level						**Email Server**	**Subscribing to Emails**	**Sender Email**
Company						Unconfigured	Subscription is not allowed.	An email server needs to be configured.
	Level-1 subsidiary					Configured	Subscription is allowed.	Use the email server configured for the level-1 subsidiary to send subscription emails.
		Level-2 subsidiary				Unconfigured	Subscription is allowed.	

Company Level						Email Server	Subscribing to Emails	Sender Email
			Level-3 subsidiary			Configured	Subscription is allowed.	Use the email server configured for the level-3 subsidiary to send subscription emails.
				Level-4 subsidiary		Unconfigured	Subscription is allowed.	
					......	Unconfigured	Subscription is allowed.	

- To ensure data security and improve the security of sending notifications, the TLSv1.2 protocol is recommended on the email server.
- To send notifications, you need to enter personal data such as email addresses. You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that users' personal data is fully protected.
- For personal data security, the personal data, such as email addresses, are anonymized on the user interface and encrypted during transmission.
- Google Mailbox Service limits the number of emails that a user can send every day and the number of recipients of each email. If they exceed the limit, you are advised to switch to an unlimited mailbox service.

Restriction Type	Description	Quantity Limit
Number of emails per day (For internal and external recipients)	Maximum number of emails that can be sent per day	2000 (500 for trial accounts)
Number of automatically forwarded emails	The number of emails that are automatically forwarded to other accounts is not counted in the maximum number of emails that can be sent per day.	10,000

Restriction Type	Description	Quantity Limit
Auto-forward email filter	Account filter for automatically forwarding emails	20
Number of recipients of each email (For internal and external recipients)	Addresses in the **To**, **Cc**, and **Bcc** fields of a single email	2000 (500 for external recipients)
Number of recipients of each email sent through **SMTP** (**POP** or **IMAP** users) or **Gmail API** (For internal and external recipients)	Addresses in the **To**, **Cc**, and **Bcc** fields of a single email This includes emails sent via smtp-relay.gmail.com or smtp.gmail.com.	100
Total number of recipients per day (For internal and external recipients)	The system counts the number of email addresses (recipients) each time an email is sent. Five emails to each of the 10 addresses are counted as 50 recipients.	10000
Number of external recipients per day	Email addresses other than your primary domain name, including the domain alias and alternate domain name	3000
Number of unique identity recipients per day (For internal and external recipients)	Each email address (each unique identity recipient) is counted only once a day: • Five emails to each of the 10 addresses are counted as 10 unique identity recipients. • Five emails sent to a single address are counted as one unique identity recipient.	3000 (2000 for external recipients, and 500 for external recipients of the trial account)

NOTE

The preceding description is for reference only. Google Mail may change the maximum number of emails that can be sent. Visit https://support.google.com and search for **Gmail sending limit** to view the latest description.

Procedure

1. Choose **System** > **System** > **Company Management** from the main menu.
2. In the navigation tree on the left, choose the target company and click **Mailbox**.
3. Set the domain name or IP address of the SMTP server, sender email address, and server port.

   NOTE

   - The sender email address must be registered on the interconnected SMTP server and must be complete. Otherwise, the email fails to be sent. Recipients can view the email address when receiving the email. You are not advised to use a personal email address to send notifications.
   - If the SMTP server requires secure connections, you are advised to enable the default TLS secure connection. When the SMTP server does not require secure connections, the default port number of SMTP is 25. To ensure that emails are sent successfully, check that the email server port is available and the configuration certificate is valid.
   - If the SMTP server requires user identity verification, obtain the username and user password from the SMTP server administrator.
     - The username must be the same as that contained in the value of **Sender email address**. You are not advised to use a personal username.
     - If no authorization code is available for logging in to the SMTP email server, set the password to the password of **Sender email address**. Otherwise, set the password to the authorization code for logging in to the SMTP email server.
4. (Optional) If **Enable secure connection over SMTP (Applies when an email server certificate for SMTP server is already installed. TLS is recommended.)** is selected, choose TLS or SSL, import a certificate and CRL. For data security purpose, TLS is recommended.

   a. Obtain an email server SSL/TLS certificate and save it to your local PC.

      NOTE

      - For details about how to obtain the mail server certificate, see FAQs.
      - The certificate is used for two-way authentication between the system and the email server. The system and the email server can communicate with each other only after both of them trust the certificate.
      - For data security, the notification function supports only the email server certificate generated using the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 signature algorithm.

   b. Press win+R to open the **Run** dialog box, enter **CMD**, and click **OK**.

   c. Run the following command to switch to the keytool directory:

      cd /d <*Directory storing keytool*>

      NOTE

      - In most cases, *Directory storing keytool* is *JDK installation path***bin**.
      - Keytool is a Java runtime environment (JRE) command. Ensure that the JRE has been installed on the local PC.

   d. In the **cmd** window, run the following command to convert the certificate format and encrypt the keystore:

keytool -import -file *<Path for saving the original certificate>|<Name of the original certificate>* **-keystore** *<Path for saving the certificate after conversion>|<Name of the certificate after conversion>*

```
Enter keystore Password:
Reenter New Password:
```

The file name extension of the converted certificate is .keystore. Remember the password set here. You need to enter the password when importing the certificate.

NOTE

The keystore password is user-defined and must contain 6 to 32 characters. For security purposes, it is recommended that the keystore password meet the following requirements:

- Cannot contain the user name or its reverse.
- Contain at least one uppercase letter (A to Z), one lowercase letter (a to z), and one digit (0 to 9).
- Contain at least one of the following special characters: !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces.

e. Click **Configure Certificate**.

f. In the **Configure Certificate** dialog box, click ··· next to **Certificate file** and select the certificate after format conversion.

g. In the **Certificate password** text box, enter the keystore password set in **4.d**.

h. Click **Save**.

5. Click **Test** to check whether the system is connected to the email server properly.
   - If the test successfully, **Test email sent successfully. The email server is available.** is displayed on the user interface.
   - If the test fails, check whether the email settings are correct. If the email server still cannot be connected after the parameter are correctly set, contact the system administrator.
6. Click **Apply**. In the displayed **Warning** dialog box, click **OK**.

   NOTE

   If you click **Test** but do not click **Apply**, only the connectivity between the system and the email server is tested, and the entered parameter values are not saved to the database. The entered parameter values are saved to the database only after you click **Apply**.

Follow-up Procedure

After interconnecting with an SMTP server, the system sends notifications to specified personnel by email through the SMTP server.

1.6.1.5 Default Electricity Prices

You can set an electricity price for each time period to accurately calculate the revenue.

Prerequisites

You have permission to manage **Default Electricity Price**.

Procedure

Step 1 Choose **System** > **System** > **Company Management** from the main menu.

Step 2 In the navigation pane, select the target company, click **Default Electricity Prices**.

Step 3 On the default electricity price page, manage the electricity price for power supply and purchase. For details about other operations, see **Table 1-24**.

Table 1-24 Operations allowed on the Default Electricity Price tab page

Operation	Procedure
Adding electricity price	1. Click **Add**. 2. Set **Date Range**, **Start Time**, **End Time**, and **Electric price**, and click **Save**.
Adding a time range	Click , set parameters as required, and click **Save**.
Deleting a date range	Click .
Deleting a time range	Click **Delete**.
Modifying a time range and electric price	Modify parameters as required and click **Save**.

NOTE

If the price unit is inconsistent with the local type, contact the company administrator to change the currency. For details, see **1.6.1.3 Company Information Configuration**.

----End

1.6.1.6 Online users monitoring

Online users can be monitored so that security administrators can know the online users in the system, access addresses of these users, access time, and type of the users. When detecting an unauthorized user operation, the system forcibly log out the user.

Prerequisites

You have logged in to SmartPVMS as a **Security Administrator** or **System Administrator**.

Procedure

Step 1 Choose **System** > **System** > **Company Management** from the main menu.

Step 2 In the navigation pane, select the target company, click **Online Users**.

The information about all online users is displayed in the list.

Step 3 When detecting that a user is performing risky operations, click **Log Out** in the **Operation** column of the user to forcibly log out the user. Alternatively, select multiple users and click **Log Out** in the upper right of the user list to force a logout of these users in batches.

NOTICE

This operation involves user login status and may force a logout of logged-in users. Therefore, exercise caution when performing this operation.

----End

1.6.1.7 Creating a System Administrator

After the SmartPVMS system is installed, an **admin** account is provided by default to manage the SmartPVMS system. If the admin user cannot meet service management requirements, you can create a **System Administrator** or **Security Administrator** under the root node based on the service plan.

Prerequisites

You have logged in to SmartPVMS as system administrator.

Procedure

Step 1 Choose **System** > **System** > **Company Management** from the main menu.

Step 2 Choose **Root** from the navigation tree on the left and click **Add user**.

Step 3 In the displayed dialog box, enter the basic information about the user and click **Next**.

Step 4 Select **System Administrator** or **Security Administrator**, click **Next**.

Step 5 Select **Root**, click .

Step 6 click **Confirm**.

----End

1.6.2 User Policy Management

User policies allow you to set access control rules for users. This function improves O&M efficiency and prevents unauthorized users from accessing the system to ensure system security.

1.6.2.1 Setting the Account Policy

Security administrators set login or lockout policies for user accounts as needed to improve system access security. The account policy takes effect for all users.

Prerequisites

You have logged in to the SmartPVMS as a security administrator.

Procedure

Step 1 Choose **System** > **System** > **Security Policies** from the main menu.

Step 2 In the navigation pane, choose **Account Policy**.

Step 3 On the **Account Policy** page, set the account policy.

NOTE

- If **Enable the user policy if no login within a period** is selected, the system will automatically delete the users who meet the policy. Perform this operation with caution.
- **Auto-logout if no activity within**: If a user does not perform any operation within the period specified by this parameter, the user will be logged out. The setting takes effect only for local and remote users and does not take effect for third-party users. If this parameter is set to **Unlimited**, user sessions will not be automatically logged out.
- If **Show warning upon successful login** is selected, a login warning message is displayed to notify users of rules that should be obeyed after users log in to the system. The warning message provides legal declaration. Security administrators can customize this warning message based on user management regulation.
- To improve account security, you are advised to enable all the items in the account policy.

Step 4 Click **Apply**.

----End

1.6.2.2 Setting the Password Policy

Security administrators set password complexity, change interval, and character limitation as needed to prevent users from setting weak passwords or using a password for a long period of time, improving system access security. The password policy takes effect for all users.

Prerequisites

You have logged in to the SmartPVMS as a security administrator.

Context

- If you disable the password complexity policy items and the item of forcibly changing passwords after they expire, user security reduces. You are advised to enable all password policies provided by the system.
- If the settings of the same policies in the personal policy of a user and the password policy are different, the settings in the personal policy take effect for the user.

- Periodically changing passwords can improve user information security and prevent accounts from being stolen. Exercise caution when disabling the function of periodically changing passwords and modifying a password change period.
- A new password policy does not affect the existing passwords.

Procedure

Step 1 Choose **System** > **System** > **Security Policies** from the main menu.

Step 2 In the navigation pane, choose **Password Policy**.

Step 3 On the **Password Policy** page, set the password policy. Some of the policy parameters are described in **Table 1-25**.

Table 1-25 Parameter description

Parameter	Description
Force logout upon password reset	When a user password is reset, all online sessions generated by the user will be logged out.
Password cannot be an increasing, decreasing, or interval sequence of digits or letters	When setting a user password, the password must meet the following requirements: ● The password cannot be digits or letters in ascending or descending sequence. For example, the password cannot be **abcdef**, **fedcba**, **123456**, or **654321**. ● The password cannot contain an ascending or descending arithmetic sequence in consecutive odd digits or even digits. For example, the password cannot be **1a2a3a**, **5a3a1a**, **a2b2c2**, or **2e2c2a**.
Password cannot contain words in password dictionary	When you create a user and set the password, the password cannot contain words in the password dictionary. ● No default password dictionary is provided. You can customize a password dictionary. For example, **abcd1234** is a weak password and if it is added to the password dictionary, **abcd1234** cannot be used as a user password. ● In a password dictionary file, passwords are separated by line feeds. In the dictionary, a password that contains more than 128 characters is invalid. **NOTE** To update the password dictionary, perform the following steps: 1. Click **Download Password Dictionary** to download the existing password dictionary and modify it as required. 2. Click and select the modified password dictionary. 3. Click **Upload** to update the password dictionary.

Parameter	Description
Convert strings in password based on conversion rules (refer to help documentation to configure the rules) **NOTE** This parameter is displayed only when **Password cannot contain words in password dictionary** is selected.	If a password contains a character string defined in the string conversion rules, the character string is converted into other characters based on certain rules. The converted password must meet complexity requirements. The string conversion rules define the rules for converting a character or string into an uppercase or lowercase letter. For example, if a rule for converting the string **|-|1234 a** into **x** exists in the string conversion rules, and **xbcd!123** is contained in the password dictionary, and when the policy is enabled, **|-|1234 abcd!123** cannot be used as a user password. **NOTE** ● For details about how to configure the string conversion rules, see "Configuring the String Conversion Rules of User Management" in *Administrator Guide*. ● Strings refer to strings consisting of dangerous characters, invisible characters, and characters incurring SQL injection.

Step 4 Click **Apply**.

----End

1.6.2.3 Setting a Client IP Address Policy

A client IP address policy provides a control mechanism for checking the accessibility of the IP address used by an external access request. Security administrators can set client IP address policies as required and bind the policies to specified users. The policies take effect only for the bound users. In this way, users can log in to the SmartPVMS only from specified IP address segments, which improves system security.

Prerequisites

You have logged in to the SmartPVMS as a security administrator.

Procedure

Step 1 Choose **System** > **System** > **Security Policies** from the main menu.

Step 2 In the navigation pane, choose **Client IP Address Policies**.

Step 3 On the **Client IP Address Policies** page, click **Create**.

Step 4 Set a client IP address policy and click **OK**.

----End

1.6.2.4 Setting a Login Time Policy

A login time policy provides a control mechanism for checking the validity time of an external access request during system operation. Security administrators can set login time policies as required and bind the policies to specified users. The policies take effect only for the bound users. In this way, users can log in to the SmartPVMS only within the specified time segments, which improves system security.

Prerequisites

You have logged in to the SmartPVMS as a security administrator.

Procedure

Step 1 Choose **System** > **System** > **Security Policies** from the main menu.

Step 2 In the navigation pane, choose **Login Time Policies**.

Step 3 On the **Login Time Policies** page, click **Create**.

Step 4 Set the parameters of the login time policy and click **OK**.

NOTE

- The system administrator user is not restricted by the login time policy.
- If the start time is later than the end time for **Effective hours**, the system will automatically set the end time to the next day. For example, if **Effective hours** is set to 16:00–15:00, login is allowed within 16:00–24:00 today and 0:00–15:00 the next day.

----End

1.6.3 Log Management

Log management enables the system to automatically record security logs, system logs, and operation logs at runtime. These logs can be queried, exported, and dumped.

1.6.3.1 Querying and Exporting Logs

To learn user operations, system operations, and system tasks, you can view logs online or view exported logs offline. Based on logs, you can identify security risks, diagnose issues, and rectify faults in a timely manner.

Prerequisites

You have permission to query and export different types of logs. For details, see **Table 1-26**.

Table 1-26 Permissions required for different types of logs

Log Type	Permission
Security logs	**Query Security Log**
System logs	**Query System Log**
Operation logs generated by all users	**Query Operation Log**

Procedure

Step 1 Open the desired log pages as follows:

- Security logs: Choose **System** > **Log Management** > **Security Logs** from the main menu.
- System logs: Choose **System** > **Log Management** > **System Logs** from the main menu.
- Operation logs: Choose **System** > **Log Management** > **Operation Logs** from the main menu.

Step 2 **Optional:** Select a time range and click **Filter**.

NOTE

By default, the system displays the logs generated within past 48 hours. If time is left blank, a maximum of 100,000 logs are displayed.

Step 3 Query logs.

- Online query: Click next to **Filter Criteria**, set filter criteria, and click **Filter**.

  NOTE

  - On the **System Logs** page, **Source** indicates the modules that automatically triggered operations.
  - On the **Security Logs** and **Operation Logs** pages, **Operation Object** indicates the objects involved with user operations. For example, **Operation Object** is an NE for alarm masking.
  - On the **Operation Logs** page, **Source** indicates the modules involved with user operations. For example, **Source** is **Alarm Management** for alarm masking.
- Offline query: To query all logs offline, click **Export All** above the log list. To query specific logs, select these logs and click **Export Selected** above the log list.

----End

Follow-up Procedure

If **Level** is **Risk** or **Result** is **Failed**, **Partially successful**, or **Unknown**, view **Details** to diagnose and rectify faults.

1.6.3.2 Log Forwarding Settings

The log forwarding settings feature can forward security logs, operation logs, system logs, and other types of logs to Syslog servers — servers that can receive logs through the Syslog protocol. The forwarded logs will be permanently saved on Syslog servers so that users can query, trace, and analyze them to identify security risks, diagnose issues, and rectify faults.

1.6.3.2.1 Configuring Log Forwarding Servers

The system will delete logs if there are more than 1000 log files or the log files consume more than 1024 MB disk space or have been stored for more than 45 days. To trace and manage the deleted logs for timely risk identification, issue diagnosis, and fault rectification, you can configure log forwarding servers to forward logs.

Prerequisites

- The trust certificates of Syslog servers have been imported. For details, see "Importing the Trust Certificate of the Syslog Server (the SmartPVMS)" in *Administrator Guide*.
- You have the **Log Transfer Management** permission.
- You have obtained the IP addresses, port numbers, protocol types, and Syslog levels of the active and standby Syslog servers to be interconnected.

Procedure

Step 1 Choose **System** > **Log Management** > **Log Forwarding Settings** from the main menu.

Step 2 In the navigation pane, choose **Forwarding Server**.

Step 3 On the **Forwarding Server** page, click **Create**.

Step 4 Set Syslog server parameters. For details about some of the parameters, see **Table 1-27**.

Table 1-27 Syslog server parameters

Parameter	Description
Active server port/Standby server port	The port numbers of the active and standby servers must be in the range of 1 to 65535.
Protocol	The system supports the TLS, UDP, and TCP protocols. • The UDP protocol cannot ensure transmission reliability. **Connection Status** in the forwarding server list determines whether logs can be successfully sent out as Syslog packets. It does not mean that packets can successfully arrive at Syslog servers. • TLS is recommended, because it is more secure than UDP and TCP. If TLS is used, the system encrypts logs before forwarding them to a Syslog server. • When **Protocol** is set to **TCP** or **TLS**, the log forwarding service sends Syslog packets to the active server first. If the sending fails, the log forwarding service sends Syslog packets to the standby server. After the active server is restored, the log forwarding service sends logs to the active server again. If **Protocol** is set to **UDP**, Syslog packets are sent only to the active server. If **Protocol** is set to **TLS**, the trust certificate for the log forwarding server is required. **NOTE** For security purposes, the system uses TLSv1.2 or later by default.

Parameter	Description
Syslog level	When setting **Syslog level**, consider the levels of all logs to be forwarded.
Required string	If **Required string** is set, only the logs that contain the specified strings will be forwarded. Regular expressions and wildcard characters are not allowed in **Required string**.
Syslog server time zone	You can set **Syslog server time zone** based on the time zone where the Syslog server is located. After the setting, the time in the forwarded Syslog packets is automatically converted to the time of the time zone where the Syslog server is located.
Enable DST	When DST is used in the region where the Syslog server is located, you can enable the DST. After the setting, when the time zone where the Syslog server is located is in the DST period, the forwarded Syslog packets contain DST identifiers.

Step 5 Click **OK**.

The new Syslog server is displayed on the **Forwarding Server** page.

NOTE

- If **Connection Status** is **Normal**, the system is successfully interconnected with the Syslog server.
- If **Connection Status** is **Unknown**, it is uncertain whether the Syslog server has been successfully interconnected. In this situation, click **Refresh** later to check the latest status.
- If **Connection Status** is **Disconnected**, the system fails to interconnect with the Syslog server. In this situation, check the parameter settings or contact technical support.

----End

Related Tasks

- Viewing Syslog server information
  - On the **Forwarding Server** page, view **Active Server IP Address**, **Active Server Port**, **Protocol**, **Connection Status**, **Enable Status**, and **Operation**.
  - Click > on the left of an active server IP address to view **Standby server IP address**, **Standby server port**, **Syslog level**, **Required string**, and **Remarks**.
- Modifying a Syslog server

  On the **Forwarding Server** page, click the IP address of an active server. On the page that is displayed, modify the server information.
- Deleting Syslog servers
  - To delete a single Syslog server, click **Delete** in the **Operation** column.

– To delete multiple Syslog servers, select the servers and click **Delete** above the list.

1.6.3.2.2 Configuring a Log Forwarding Rule

The log forwarding rule defines the levels of different types of logs to be forwarded.

Prerequisites

You have the **Log Transfer Management** permission.

Procedure

Step 1 Choose **System** > **Log Management** > **Log Forwarding Settings** from the main menu.

Step 2 In the navigation pane, choose **Forwarding Rule**.

Step 3 On the **Forwarding Rule** page, click the desired levels for different types of logs.

Step 4 Click **Apply**.

Then the system forwards logs based on the log forwarding rule and **Syslog level** on the **Forwarding Server** page.

----End

1.6.4 Message Management

1.6.4.1 Public Notice

This topic describes how to view received public notices to learn messages.

Procedure

Step 1 Choose **System** > **Message Management** > **Announcements**.

Step 2 Click the **Message Subject** of an unread message. In the displayed **Message** dialog box, view the details about the message.

----End

1.6.4.2 Sending a Public Notice

This topic describes how to create, send, and delete public notices.

Prerequisites

You have the permission for **Send Public Notice**.

Procedure

Step 1 Choose **System** > **Message Management** > **Send Announcement**.

The messages created by the current user are displayed. You can click a message subject to view the message details.

Step 2 Click **Add**. The **Create message** dialog box is displayed.

Step 3 Set **Recipient** or select **All**, and set **Subject** and **Content**.

Step 4 Perform either of the following operations as required:

- Click **Sending** to send the message. The message status is **Sent**.
- Click **Save** to save but not send the message. The message status is **Draft**.

NOTE

For a message in **Draft** state, you can click the message subject to edit, save, or send the message.

----End

1.6.5 Business settings

1.6.5.1 System Parameter Settings

On the **System Parameter Settings** page, you can query and modify parameters required by services such as energy saving and emission reduction, data subscription, diagnosis and warning, and report. If the default parameter values do not comply with the parameter standards in the area where the PV plant is located, you can modify the parameter values.

Prerequisites

You have the operation permission for **Business Configuration**.

Procedure

Step 1 Choose **System** > **Business Configuration** > **System Parameter Settings** from the main menu.

Step 2 Select a company or plant under the root node on the left.

Step 3 Select a parameter to be modified and click **Modify**.

Step 4 In the displayed dialog box, change the parameter value.

Step 5 Click **OK**.

----End

1.6.5.2 Data Amendment

1.6.5.2.1 Data Recovery

After the communication between the device and the system recovers, you can create a data synchronization task to synchronize data to ensure the integrity of the plant data.

Prerequisites

You have the permission for **Business Configuration**.

Procedure

Step 1 Choose **System** > **Business Configuration** > **Data Amendment**. The **Data Recovery** page is displayed.

Step 2 Under the root node in the left pane, select device.

Step 3 Select the device type.

Step 4 Select the time range for supplementary collection.

Step 5 Click **Create Tasks**.

Step 6 In the displayed dialog box, click **Yes**.

The synchronization progress of the device is updated in the right pane.

----End

Follow-up Procedure

You can perform the following operations on the **Synchronize Data** page.

Operation	Procedure
Querying supplementary collection tasks	You can view the status of supplementary collection tasks and retry or cancel a task. 1. Select the device under the root node on the left. 2. Specify the time range for supplementary collection. 3. Click **Query Tasks**.
Retrying data collection	You can re-collect the data that is in the **Canceled** or **Failed** state. In the supplementary collection task list, select the **Canceled** or **Failed** state and click **Retry**.
Canceling the supplementary collection of data	Cancel the supplementary collection operation in the data collection process. In the supplementary collection task list, select the task whose progress does not reach 100% and click **Cancel**.

1.6.5.2.2 Data Repair

If the collected device running data is incorrect, you can use the data repair function to correct the data.

Prerequisites

You have the **Business Configuration** permission.

Procedure

Step 1 Choose **System** > **Business Configuration** > **Data Amendment**.

Step 2 In the right pane, click the **Data Repair** tab.

Step 3 Export repair data.

1. Click **Export Repair Data**.
2. In the dialog box that is displayed, select devices and the time period, and then click **Next**.

   NOTE

   The data of a maximum of 10 devices can be exported at a time, and the time span cannot exceed three months.
3. Select the signal points to be repaired and click **OK**.

   NOTE

   A maximum of 10 signal points can be exported at a time.

Step 4 Open the data exported in **Step 3** and correct the signal data.

Step 5 Create a repair task.

1. Click **Create Repair Task**.
2. In the dialog box that is displayed, click **Upload** and select the file whose data has been corrected in **Step 4**.
3. Select the checkbox of the statement (This operation will directly modify equipment data and may affect the accuracy of plant statistics and report data. Ensure that you have obtained authorization from the owner.) and click **OK**.

----End

1.6.5.2.3 Manual Aggregation

If the report data of a device in a specified period is missing, you can aggregate the report data manually.

Prerequisites

You have the **Business Configuration** permission.

Procedure

Step 1 Choose **System** > **Business Configuration** > **Data Amendment**.

Step 2 In the right pane, click the **Manual Aggregation** tab.

Step 3 Specify the devices and time period.

Step 4 Click **Create Task**.

Step 5 In the dialog box that is displayed, click **Yes**.

The page displays the data aggregation progress and whether the aggregation succeeded or not.

----End

1.6.5.3 Northbound Management

You can manage northbound systems to provide plant and device data to them for displaying or using the data in a customized manner.

Prerequisites

You have the permission for **Business Configuration**.

Context

- The access permissions of northbound interfaces (NBIs) are independent of third-party user accounts and are created by the administrator when adding a northbound system.
- For details about NBI parameters, see *SmartPVMS V500R007C00 NBI Reference*.

Procedure

Step 1 Choose **System** > **Business Configuration** > **Northbound Management**.

Step 2 Manage northbound users based on the application scenario. For details, see **Table 1-28**.

Table 1-28 Northbound management operations

Operation	Procedure
Adding a northbound system	1. Click **Add**. The **Add** dialog box is displayed. 2. Enter **System name** and **System introduction**, and select **Deadline**. 3. Enter the user name and password. **NOTE** The user name and password are used by the northbound user to log in to the third-party system. Keep the user name and password secure. 4. Select the northbound interfaces to be enabled and click . 5. Click on the left of **Interface Name** and select the plant, device, and indicator to be enabled. 6. click **OK**.
Deleting northbound systems	● Select one or multiple northbound data records and click **Delete**. ● In the Operation column, click .
Viewing the details about a northbound system	Click .
Modifying information	1. Click in the Operation column. 2. Complete the modification as prompted and click **OK**.
Search northbound system	Enter a system name and click **Search**.

----End

1.6.5.4 Server Management

You can set a third-party web system in the SmartPVMS to integrate system status information to the SmartPVMS server for management. You can quickly access the system status information on the login page.

Prerequisites

You have the permission for **Business Configuration**.

Procedure

Step 1 Choose **System** > **Business Configuration** > **Server Management**.

Step 2 Manage servers based on the application scenario. For details, see **Table 1-29**.

Table 1-29 Operations allowed on the Server Management page

Operation	Description	Procedure
Querying a server	Used to search for concerned server.	Set **Domain name** and click **Search**.
Creating a server	Create server information for quick access on the login page.	1. Click **Add**. In the displayed dialog box, set **Server name**, **Structure name**, and **Description**. 2. Click **OK**. **NOTE** After the server is created, its status automatically changes to **Enable**.
Deleting one or multiple servers	Used to delete useless servers information.	• Select one or more server records and click **Delete**. In the displayed dialog box, click **OK**. • Click 🗑 for a server. In the displayed dialog box, click **OK**.
Enabling a server	Enable the servers that are disabled for quick access on the login page.	Select a disabled server and click **Enable**.
Disabling a server	Used to disable an invalid server. After this command is executed, the sserver becomes unavailable.	Select an enabled server and click **Disable**. After a server is disabled, it is unavailable.
Modifying server information	Used to update server information.	Click ✎ for a server record. In the displayed dialog box, modify the site information and click **OK**.

----End

1.6.5.5 Document Management

You can view the space usage and file information of each module in the system and download files through document management.

Prerequisites

You have the permission for **Business Configuration**.

Procedure

Step 1 Choose **System** > **Business Configuration** > **Document Management**.

- Module space management: On this page, you can view the space usage of each module.
- File management: On this page, you can view the information about a file.
  a. Set **Business module**, **File name**, and **File type**, and click **Search** to search for the required file information.
  b. Click **Download** for the required file to save the file to the client.

----End

1.6.5.6 Alarm Configuration

1.6.5.6.1 Configuring Notification Rules

Notification rules enable O&M personnel to email notifications about concerned alarms so that they can handle alarms in real time.

Prerequisites

- You have the permission for **Business Configuration**.
- The email server of the company has been configured. For details, see **1.6.1.4 Configuring an Email Server**.

Context

- The alarm push rule takes effect only for newly reported alarms. If an alarm has been reported to the SmartPVMS before the push rule takes effect, no notification email will be sent.
- When a new alarm that meets the push rule is reported to the SmartPVMS, the push rule is triggered immediately to send an email to the specified users.
- If the time zone of the recipient is different from that of the server, the alarm generation time in the email is displayed based on the time zone of the server.
- By default, the rules are sorted by the enabled and disabled states, and the rules in the same state are sorted by update time in descending order.
- A maximum of 1000 notification rules can be created.

Procedure

1. Choose **System** > **Business Configuration** > **Alarm Configuration**.
2. In the navigation pane, choose **Push Configuration**.
3. On the **Push Settings** page, click **Add**.
4. In the **Create Rule** dialog box, set the rule as prompted.

NOTE

To send notifications to relevant personnel, you need to enter their personal information, such as email addresses. You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the user's personal information is fully protected.

5. Click **Save**.

Related Tasks

- Deleting a rule: You can select a redundant rule from the rule list and click **Delete** to reduce the rule maintenance workload.
- Enabling/disabling a rule: You can select a rule that is not used temporarily from the rule list and click **Disable**. To use a disabled rule, select the rule and click **Enable**.
- Backing up, collecting statistics on, and reviewing rules, and modifying rules in batches: You can click **Export** on the rule page to export rules and back up, review, and collect statistics on the rules. If you need to modify rules in batches, you can modify the rules in batches in the exported rule file. Then, click **Import** on the rule page to import the modified rule file.

  NOTE

  When the notification rules are exported, the email addresses of the recipient users are exported. You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the user's personal information is fully protected.

1.6.5.6.2 Redefine Alarm

To quickly search for and handle key device alarms to which you pay special attention, you can redefine these alarms. The SmartPVMS provides three types of alarm redefinition rules: redefine alarm name, redefine alarm type and redefine alarm severity.

Table 1-30 description of the function of redefining alarms.

Table 1-30 Function of Redefining Alarms

Task Description	Operation entry	Procedure
Configuring Redefinition Alarms	1. Choose **System** > **Business Configuration** > **Alarm Configuration**. 2. In the navigation tree on the left, choose **Redefine Alarm**.	1. In the device tree and select a target device. 2. Click the operation column . 3. Enter the **New Alarm Name** and **New Alarm Severity** based on the site requirements. 4. Click the operation column , saving customized alarm information. **NOTE** After saving redefinition alarms, the redefined alarm status is changed to enabled after the synchronization is complete.
Clearing Redefining Alarm Rules **NOTE** After saving redefinition alarms, the alarm redefinition rule can be cleared.		Use either of the following methods to clear redefinition alarms: • On the **Redefine Alarm** page, Click in the row where the indicator to be cleared is located. • On the **Redefine Alarm** page, Select the target data to be cleared and click **Clear** above the page.

Task Description	Operation entry	Procedure
enabling Redefining Alarm Rules **NOTE** After saving redefinition alarms, the alarm redefinition rule can be enabled redefining alarm rules.		Use either of the following methods to enable redefinition alarms: • On the **Redefine Alarm** page, click  the row of the target data row to be enabled. • On the **Redefine Alarm** page, select the target data for which redefinition alarm rules need to be enabled, click **Enable** in the upper part of the page.
Disabling Redefining Alarm Rules **NOTE** After saving redefinition alarms, the alarm redefinition rule can be disabled Redefining alarm rules.		Use either of the following methods to disable redefinition alarms: • On the **Redefine Alarm** page,Click  the row of the target data row to be disabled. • On the **Redefine Alarm** page, select the target data for which redefinition alarm rules need to be disabled, click **Disable** in the upper part of the page.
Refresh the redefined alarm		On the **Redefine Alarm** page, click **Refresh** in the upper part of the page to refresh the redefined alarm page.

Task Description	Operation entry	Procedure
Batch Redefinition Rule Application		On the **Redefine Alarm** page, click in the operation column for the target alarm in the active alarm list to apply **Alarm Severity** and **Alarm Type** specified in the alarm rule to other rules in batches.
Batch Apply to Devices		1. In the device tree and choose a target device. 2. You can click Batch Apply below the active alarm list to apply the selected alarm rules to other devices in batches. **NOTE** Rules for applying an empty rule: For two devices of the same type, if the redefinition alarm rule is not set for one device and you want to apply the rule to another device that has been configured with an alarm rule, the redefinition alarm rule that has been set on the other device is cleared.

1.6.5.7 Hyperlink Trustlist Management

The hyperlink trustlist is used to verify the hyperlink address of an enterprise website and the address in the rich text involved in the message sending module.

Prerequisites

You have the permission for **Business Configuration**.

Procedure

Step 1 Choose **System** > **Business Configuration** > **Hyperlink Trustlist**.

Step 2 Manage the hyperlink trustlist based on the application scenario. For details, see **Table 1-31**.

Table 1-31 Operations allowed on the Hyperlink Trustlist Management page

Operation	Procedure
Searching for a hyperlink	Set **Hyperlink information** and click **Search**.
Adding a hyperlink	Click **Add**. In the displayed **Add** dialog box, set **Hyperlink information** and click **OK**.
Deleting one or multiple hyperlinks	• Select one or more hyperlinks and click **Delete**. • Click for a hyperlink.
Modifying hyperlink information	1. Click for a hyperlink. 2. In the displayed **Modify** dialog box, modify the hyperlink information and click **OK**.

----End

1.6.6 System Settings

1.6.6.1 License Management

License management allows you to initially load, revoke, update and export a license file and query and export license information. These functions help manage licenses in an effective way and ensure that you can use the system properly.

1.6.6.1.1 Initially Loading a License

After the system is deployed, you need to load valid license files on the GUI to ensure that you can use the system properly.

Prerequisites

- You have the operation rights for **Update License**.
- You have obtained the license files to be loaded.

Procedure

Step 1 Log in to the SmartPVMS at **https://intl.fusionsolar.huawei.com**.

Step 2 Click **Import License**.

Step 3 Click next to **License File**.

Step 4 Select the license file to be imported and click **Open**.

Step 5 Click **Upload** to view the current license information.

Step 6 Click **Apply**.

You can log in to the SmartPVMS only after the license is initially loaded successfully.

NOTE

During the initial loading, the default value of **Update mode** is **Full**, which cannot be changed.

----End

Follow-up Procedure

- After the license is initially loaded, log in to the system again to make the license take effect.
- After the license fails to be initially loaded, locate the causes based on the error information and import the license file again.

1.6.6.1.2 Viewing the License Overview

On the **License Overview** page, you can view the license file status and consumption of resource items or sales items. If a license file is about to expire or the resource items or sales items do not meet service requirements, you can update the license in a timely manner to ensure that you can properly use the system.

Procedure

Step 1 Choose **System** > **System Settings** > **License Management** from the main menu.

Step 2 On the **License Overview** page, view the license file status and consumption of resource items or sales items.

If a license file is about to expire or the resource items or sales items do not meet service requirements, you can apply for and update the license in a timely manner.

NOTE

- The bar chart displays the license file status, and the ring chart displays the overall status of resource items or sales items. You can click modules in different colors in the bar chart and ring chart to view details in the list in the lower part.
- License 3.00 has sales items.

----End

1.6.6.1.3 Viewing License Information

During routine maintenance, you can query current license information to detect problems (for example, a license is about to expire or capacity is insufficient) and update the license file in a timely manner, ensuring proper running of the system.

Procedure

Step 1 Choose **System** > **System Settings** > **License Management** from the main menu.

Step 2 In the navigation pane, choose **License Information**.

Step 3 On the **License Information** page, select a product from the product drop-down list.

Step 4 Click the **Resource Control Items**, **Function Control Items**, or **Sales Information Items** tab to view related license information of this product.

NOTE

License 3.00 has sales information items.

- Table 1-32 describes the basic license information.
- Table 1-33 describes the license information on the **Resource Control Items** tab page.
- Table 1-34 describes the license information on the **Function Control Items** tab page.
- Table 1-35 describes the license information on the **Sales Information Items** tab page.

Table 1-32 Basic license information

Parameter	Description	Example
Software ID	Software ID. The software ID is used to measure the inventory software scale on the live network, and is composed of 12 characters. It is the unit for measuring the capacity of the users' live network and functions as a software service credential. **NOTE** • This item is displayed on the GUI only when the license file contains the software ID. • Users need to provide this ID when contacting technical support to query their maintenance information. • If the license of a product contains multiple software IDs, separate the IDs with commas (,).	1902345T8FL6
Software Upgrade Expired On	Expiration date of free upgrade and maintenance for software. **NOTE** • This item is displayed on the GUI only when the license file contains the expiration date. • An "Annual software service fee is due soon" alarm is reported when the number of remaining days to the software upgrade expiration date is equal to or less than the number of expiration warning days (15 days by default). • An "Annual software service fee has expired" alarm is reported after the software upgrade expiration date.	2019-06-29

Table 1-33 License information on the **Resource Control Items** tab page

Item	Parameter	Description	Example
List fields	Used/ Total Capacity	Capacity consumption and capacity of a resource control item specified in the license file.	**30/2000**: The capacity of a resource control item in the license file is 2000 and the capacity consumption is 30.
	Alarm Threshold	The "The license resource exceeds the threshold" alarm is reported when the consumption of a resource control item reaches or exceeds the specified the consumption percentage (alarm threshold). This alarm is automatically cleared when the consumption falls below the percentage. **NOTE** The default threshold is 90% and can be changed. For details, see **1.6.6.1.6 Setting Alarm Thresholds**.	90%
	Max. Capacity Exceeded On	Time when the consumption exceeds 100% of the capacity.	2019-09-25 10:25:35
Consumption details	Used/ Total Capacity	Capacity consumption and capacity of a resource control item specified in the license file.	**30/2000**: The capacity of a resource control item in the license file is 2000 and the capacity consumption is 30.
	End of Grace Period	Date when a resource control item expires. Generally, it is the day when the grace period expires.	2019-06-29

Item	Parameter	Description	Example
	End of Validity Period	Date when a resource control item becomes invalid.	2019-04-29
Sub-item details **NOTE** • Only license 2.00 has this item, but license 3.00 does not. • Sub-item details can be displayed only when the license files are license 2.00, sub-items have been set for **hasSubItem** in the **license_config.json** file, and the sub-items are consumed.	Sub-item Name	Sub-item name of a resource control item.	ESR8850
	Consumption	Consumption of a sub-item.	5

Table 1-34 License information on the **Function Control Items** tab page

Parameter	Description	Example
End of Grace Period	Date when a function control item expires.	2019-06-29
End of Validity Period	Date when a function control item becomes invalid.	2019-04-29

Table 1-35 License information on the **Sales Information Items** tab page (for license 3.00)

Item	Parameter	Description	Example
List fields	Used/ Total Capacity	Capacity consumption value of a sales information item and capacity value allowed in the license file.	0/100: The capacity of a sales information item in the license file is 100 and the capacity consumption is 0.

Item	Parameter	Description	Example
	Alarm Threshold	The "The license sales item exceeds the threshold" alarm is reported when the capacity consumption of a sales information item reaches or exceeds the specified the consumption percentage (alarm threshold). This alarm is automatically cleared when the capacity consumption falls below the threshold. **NOTE** The default threshold is 90% and can be changed. For details, see **1.6.6.1.6 Setting Alarm Thresholds**.	90%
	Max. Capacity Exceeded On	Time when the consumption exceeds 100% of the capacity.	-
Consumption details	Used/Total Capacity	Capacity consumption value of a sales information item and capacity value allowed in the license file.	0/100: The capacity of a sales information item in the license file is 100 and the capacity consumption is 0.
	End of Grace Period	Date when a sales information item expires. Generally, it is the day when the grace period expires.	2019-06-29
	End of Validity Period	Date when a sales information item becomes invalid.	2019-04-29

Step 5 **Optional:** Click **Export**. In the dialog box that is displayed, select a format for saving the license information file.

NOTE

License information files can be exported in CSV or XLSX format. The file name is in the format of *Product name*_**License**_*Timestamp*.**csv** or *Product name*_**License**_*Timestamp*.**xlsx**.

In an exported license information file, information about each resource control item or sales information item varies by license file type. For details, see **Table 1-36**.

Table 1-36 Description of exported license information files

License File Type	Description
Permanent commercial	Each resource control item or sales information item has one record, recording information about the permanent commercial item, for example, the consumption and capacity of the permanent commercial item.
Fixed-term	Each resource control item or sales information item has one record, recording information about the fixed-term item, for example, the consumption and capacity of the fixed-term item.
Permanent commercial +fixed-term	Each resource control item or sales information item has three records. The first records the comprehensive information about the permanent commercial item and fixed-term item, for example, the total consumption and capacity of the permanent commercial item and fixed-term item. The second records information about the fixed-term item, for example, the consumption and capacity of the fixed-term item. The third records information about the permanent commercial item, for example, the consumption and capacity of the permanent commercial item.

----End

1.6.6.1.4 Viewing a License File

During routine maintenance, you can view the license file to obtain the license revocation code and ESN so that you can check the license file status.

Procedure

Step 1 Choose **System** > **System Settings** > **License Management** from the main menu.

Step 2 In the navigation pane, choose **License File**.

Table 1-37 describes information contained in a license file.

Table 1-37 License file information

Parameter	Description
LSN	License serial number which uniquely identifies a license file.

Parameter	Description
File Status	• **Valid and available**: The license file is in the validity period. In this case, users can properly use the resources and functions specified in the license file. • **Invalid but available**: The license file is in the grace period. In this case, users can use the resources and functions specified in the license file until the grace period expires. • **Invalid and unavailable**: The license file is invalid. In this case, the resources and functions specified in the license file cannot be used and the license file needs to be updated.

Step 3 Click > on the left to view details of the license file.

----End

1.6.6.1.5 Backing Up License Files

Before updating a license file, export the license file. You can use the backup to restore the license file if the update failed.

Prerequisites

You have the operation rights for **Update License**.

Procedure

Step 1 Choose **System** > **System Settings** > **License Management** from the main menu.

Step 2 In the navigation pane, choose **License File**.

Step 3 In the license file list, select the license file to be backed up and click **Export License**.

NOTE

- A maximum of 10 license files can be exported at a time.
- **LSN** indicates the license serial number which uniquely identifies a license file.
- License 2.00 files are exported in .dat format and license 3.00 files are exported in .xml format.

A package in .zip format is exported. In the package, the license files are named **License**_*product name*_*license file type*.*file format*. The license file types are as follows:

- Permanent commercial: permanent
- Fixed-term: demo
- Permanent commercial+fixed-term: permanent

----End

1.6.6.1.6 Setting Alarm Thresholds

When the consumption of a resource control item or sales information item for the license reaches or exceeds the threshold, an alarm is generated. In this way, users can apply for and update license files in a timely manner to ensure proper running of the system.

Prerequisites

You have the operation rights for **Update License**.

Procedure

Step 1 Choose **System** > **System Settings** > **License Management** from the main menu.

Step 2 In the navigation pane, choose **License Information**.

Step 3 On the **License Information** page, click the **Resource Control Items** or **Sales Information Items** tab.

- To modify the alarm threshold for a single item, click **Modify** of the item in the **Operation** column.
- To modify the alarm thresholds for multiple items, select the items and click **Batch Modify**.
- To modify the alarm thresholds for all items, click **Modify All**.

NOTE

If the license file in the system is license 2.00, you can set alarm thresholds only for resource control items.

Step 4 In the displayed dialog box, set the threshold for each resource control item or sales information item, and specify whether to send an alarm or to enable the scheduled reminder when the consumption of an item reaches the threshold.

- Modify the alarm threshold for a single item in the displayed **Modify Alarm Threshold** dialog box.
- Modify the alarm thresholds for multiple items in the displayed **Batch Modify Alarm Thresholds** dialog box.
- Modify the alarm thresholds for all items in the displayed **Modify All Alarm Thresholds** dialog box.

NOTE

- If **Send alarms** is selected, the alarm "The license resource exceeds the threshold" or "The license sales item exceeds the threshold" is sent when the consumption of a resource control item or sales information item reaches **Alarm threshold**. This alarm is automatically cleared when the consumption falls below **Alarm threshold**.
- If **Send notifications** is selected, the **Information** dialog box is displayed at an interval specified by **Notification interval** in **Step 6** when the capacity consumption of a resource control item or sales information item reaches **Alarm threshold**.

Step 5 Click **OK**.

Step 6 **Optional:** Set the prompting interval.

1. On the **License Information** page, click below **Notification interval**.
2. Set **Notification interval**.
3. Click **OK**.

----End

1.6.6.1.7 Obtaining a License Revocation Code

If the ESN of a commercial license is changed due to NIC replacement, server replacement, VM reinstallation, or incorrect ESN, you can manually revoke the license and obtain the revocation code to apply for a new license file without manual approval, which increases the application efficiency.

Prerequisites

You have permission to perform the operation **Revoke License**.

NOTE

A fixed-term license cannot be revoked. For a fixed-term license file or an invalid license file, the revocation code cannot be used for license application. You need to apply for a new license file.

Procedure

Step 1 Choose **System** > **System Settings** > **License Management** from the main menu.

Step 2 In the navigation pane, choose **License File**.

Step 3 Revoke licenses.

- To revoke a single license: In the license list, click **Revoke License** in the **Operation** column of the row that contains the license file to be revoked.
- To revoke licenses in batches: In the license list, select the license files to be revoked and click **Revoke License** above the list.

  NOTE

  When a license is revoked, it enters the grace period. After the grace period is reached, you cannot log in to the system. Apply for a new license file and update it before the grace period expires.

Step 4 In the dialog box that is displayed, click **OK**.

Step 5 In the license list, click > on the left of a license file to view and obtain **Revocation code**.

----End

1.6.6.1.8 Updating a License File

You need to update the license file in the following scenarios so that you can use the system properly: 1. The current license file in the system is about to expire or has expired. 2. A resource control item or function control item in the license file does not meet service requirements. 3. The software service annual fee in the license is about to expire or has expired.

Prerequisites

- You have the operation rights of **Revoke License** and **Update License**.
- You have obtained the license file.

Context

- You are advised to export the current license file as a backup before updating the license file. If the license file fails to be updated, you can use the backup to update the license file again.
- If a product in the system has license files that contain unmatched ESN, you cannot update such a license file.
- An expired license file cannot be normally updated. You need to apply for a new license file and import it. For details, see **1.6.6.1.1 Initially Loading a License**.

Procedure

Step 1 Choose **System** > **System Settings** > **License Management** from the main menu.

Step 2 In the navigation pane, choose **Update License**.

Step 3 On the **Update License** page, click next to **License File**.

Step 4 Select the license file to be updated and click **Open**.

Step 5 Click **Upload**.

Step 6 Select a license file update mode as required.

License files are classified into three types: permanent commercial, fixed-term, and permanent commercial+fixed-term. The license update mode of a product is determined by the types of its license file and the license file used for the update. **Table 1-38** lists the mapping between update modes and license file types.

Table 1-38 Mapping between update modes and license file types

Current License File Type	New License File Type	Update Mode
Permanent commercial	Permanent commercial	Full update
	Fixed-term	Full update or incremental update
	Permanent commercial +fixed-term	Full update
Fixed-term	Fixed-term	Full update
	Permanent commercial	Full update or incremental update
	Permanent commercial +fixed-term	Full update

Current License File Type	New License File Type	Update Mode
Permanent commercial +fixed-term	Permanent commercial	Full update
	Fixed-term	Full update
	Permanent commercial +fixed-term	Full update
A permanent commercial license file and a fixed-term license file for a product	Permanent commercial	Full update or incremental update
	Fixed-term	Full update or incremental update
	Permanent commercial +fixed-term	Full update

NOTE

- A license file can be incrementally updated using a license file of the same version. For example, a license 2.00 file can be incrementally updated using a license 2.00 file, but not a license 3.00 file.
- A license file can be fully updated using a different license file version.

Step 7 Check the comparison result between the licenses before and after the update.

Risk Level indicates the level of a risk caused by license file update. **Table 1-39** provides the causes for each risk level.

- For resource control items, the risk levels from high to low are **Risk**, **Warning**, **Suggestion**, and **No risk**.
- For function control items, the risk levels are as follows:
  - **Risk**: **Supported by Current License** is set to **Yes** and **Supported by New License** is set to **No**.
  - **Suggestion**: **Supported by Current License** is set to **No** and **Supported by New License** is set to **Yes**.
  - **No risk**: **Update Type** is set to **Unchanged**.
- For sales information items, the risk levels from high to low are **Risk**, **Warning**, **Suggestion**, and **No risk**.

  NOTE

  Sales information items are available only when you update license 3.00 files.

Table 1-39 Risk level description

Risk Level	Description	Caused By
Risk	Updating a license file causes high risks. After the update, certain resources or functions may be unavailable.	For a resource control item or sales information item, the value of **New Capacity** is less than that of **Consumption** or **Update Type** is set to **Deleted**.
Warning	Updating a license file causes high risks. After the update, certain resources may be unavailable.	For a resource control item or sales information item, **Update Type** is set to **Modified**, or the value of **New Capacity** is greater than or equal to that of **Consumption** and less than that of **Current Capacity**.
Suggestion	No risks are caused by a license file update. It is only a suggestion for the update.	For a resource control item or sales information item, **Update Type** is set to **Modified**, the value of **New Capacity** is greater than or equal to that of **Consumption** and greater than that of **Current Capacity**, or **Update Type** is set to **Added**.
No risk	The value of **Risk Level** is empty, indicating that no risks are caused by a license update.	For a resource control item or sales information item, **Update Type** is set to **Unchanged**, or the value of **New Capacity** is equal to that of **Current Capacity** and greater than or equal to that of **Consumption**. For a function control item, **Update type** is set to **Unchanged**.

Step 8 Click **Apply**.

----End

Follow-up Procedure

If the license file fails to be updated, locate the causes based on the error information and update the license file again.

1.6.6.2 Personal Settings

This feature enables users to customize personal settings.

1.6.6.2.1 Changing Personal Password

If passwords are disclosed or remain unchanged for a long time, users can change their personal passwords by setting personal information. To improve user security, it is recommended that passwords be changed periodically (for example, every three months). When a user logs in to the SmartPVMS for the first time or after the administrator resets the user password, the user needs to change the initial password.

Context

If you cannot change your password, contact the administrator.

Procedure

Step 1 Choose **System** > **System Settings** > **Personal Settings** from the main menu.

Step 2 In the navigation pane, choose **Change Password**.

Step 3 On the **Change Password** tab page, enter **Old password** and set **New password** and **Confirm password**.

Step 4 Click **Apply**.

NOTE

User information is more secure if a password is changed more frequently. If a user forgets the password due to frequent password changes, the user needs to contact administrators to reset the password.

----End

Related Tasks

In the following cases, the system prompts a user to change the password after the user logs in to the SmartPVMS:

- The user uses the initial password for login. For example, the password for the user has been reset, or the password is the one used for creating the user account.
- The user account is enabled again, but the user uses the password when the account is disabled for login.

1.6.6.2.2 Modifying Personal Information

When personal information such as mobile numbers and email addresses changes or needs to be supplemented, users can periodically maintain their personal information by setting personal information to ensure its accuracy.

Procedure

Step 1 Choose **System** > **System Settings** > **Personal Settings** from the main menu.

NOTICE

- When you modify your personal information, such as mobile numbers and email addresses, you are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that your personal data is fully protected.
- To ensure the security of personal information, such as mobile numbers and email addresses, these data is anonymized on the page, and HTTPS encryption transmission channels are used.

Step 2 In the navigation pane, choose **Modify Personal Info**.

Step 3 On **Modify Personal Info**, modify personal information as required.

NOTE

If the SMS and email verification codes cannot be obtained, ensure that the remote notification function is configured correctly.

Table 1-40 Parameter description

Parameter	Description	Procedure
Associate Mobile Number	Mobile number associated with a user account.	• Editing the mobile number 1. Click **Edit**. 2. Verify the identity information as prompted and click **Next**. 3. Select a country or region code and enter a new mobile number. 4. Click **Send Code** and enter the obtained verification code to verify that the mobile number is valid. 5. Click **OK**. • Verifying the mobile number 1. Click **Verify**. 2. Click **Send Code** and enter the obtained verification code to verify that the mobile number is valid. 3. Click **OK**.

Parameter	Description	Procedure
Associate Email Address	Email address associated with a user account.	● Editing the email address 1. Click **Edit**. 2. Verify the identity information as prompted and click **Next**. 3. Enter a new email address. 4. Click **Send Code** and enter the obtained verification code to verify that the email address is valid. 5. Click **OK**. ● Verifying the email address 1. Click **Verify**. 2. Click **Send Code** and enter the obtained verification code to verify that the email address is valid. 3. Click **OK**.
Auto-Logout If No Activity Within	If a user does not perform any operation within the period specified by this parameter after login, the user will be logged out. This parameter can be set for local users and remote users. The default value for the third-party user is 30 minutes and cannot be changed.	1. Click the drop-down list and select a value for **Auto-Logout If No Activity Within**. 2. Click **Save**.
Welcome Message	You can set the information to be displayed upon the next login.	1. Click **Edit**. 2. Enter the information to be displayed upon the next login. 3. Click **OK**.
Export personal information	Only the system administrator with the user management permission can modify or export user information. If you need to export personal information, contact and authorize the system administrator to export the information.	-

----End

1.6.6.2.3 Modifying Personal Client IP Address Control Policies

With the **Update ACL Policy** permission, you can configure your personal client IP address control policies. ACL is short for access control list.

Procedure

Step 1 Choose **System** > **System Settings** > **Personal Settings** from the main menu.

Step 2 In the navigation pane, choose **Personal Client IP Address Policies**.

Step 3 On the **Personal Client IP Address Policies** page, create, view, or modify your IP address control policies.

NOTE

The client IP address control policies created or modified by you take effect for you.

----End

1.6.7 Configuration Items Management

1.6.7.1 Configuring the Protocol Switch

By default, the SmartPVMS communicates with devices only through security protocols, arithmetic and certificate. If the SmartPVMS wants to communicate with devices through non-secure protocols, arithmetic or certificate, perform the operations provided in this topic. Exercise caution when performing the operations in this topic because these operations will compromise the security of information transmission between the SmartPVMS and devices.

Prerequisites

- The required adapter software has been installed.
- You have the permission for **Configuration Items**.

Procedure

Step 1 Choose **System** > **Configuration Items** > **Protocols**.

Step 2 Enable or disable protocols as required and click **OK**.

Step 3 In the displayed dialog box, click **OK**.

Step 4 Restart the system service for the settings to take effect. For details, see sections **Starting Product Services** in the *Administrator Guide*.

----End

1.6.7.2 Modifying the FTP Password

This topic describes how to change the FTP password. To improve security, you are advised to change the password periodically.

Prerequisites

You have the permission for **Configuration Items**.

Procedure

Step 1 Choose **System** > **Configuration Items** > **FTP Password**.

Step 2 Select a username, enter the old password, new password, and confirm password, and click **Confirm**.

----End

1.6.7.3 Configuring NAT

When Network Address Translation (NAT) is required between the SmartPVMS client and server, you must configure the NAT IP address to ensure that you can use the server IP address or host name to log in to the server from the client.

Prerequisites

You have the permission for **Configuration Items**.

Procedure

Step 1 Choose **System > Configuration Items > NAT Configuration**.

Step 2 Click modify, In the displayed dialog box, enter the SmartPVMS server IP address after NAT, and click **OK**.

Step 3 In the displayed dialog box, click **Confirm**.

Step 4 Restart the system service for the settings to take effect. For details, see sections **Starting Product Services** in the *Administrator Guide*.

----End

1.6.7.4 Configuring Demo Account

This section describes how to enable or disable the demo account function. When this function is enabled, the demo account can be used to log in to the system to experience the system.

Prerequisites

You have the permission for **Configuration Items**.

Procedure

Step 1 Choose **System** > **Configuration Items** > **Demo Account**.

Step 2 Set the login control function based on the application scenario.

- When **Login control** is 

, the function of experiencing the system is unavailable.

- When **Login control** is On, set **Maximum online demo accounts** and click **OK**.

NOTICE

- When **Login control** is enabled, the **Demo Site** function item is displayed on the system login page.
- When the demo account function is enabled, the demo account **guest_account** is created. The initial password is randomly generated.

Step 3 Click **Reset Password**, enter a new password, confirm the password, and click **OK**.

NOTE

After the password is reset for the demo account, you can use the demo account **guest_account** and the password to log in to the system.

----End

1.6.7.5 Configuring the Weather Service

This section describes how to set global weather services to forecast the local weather conditions of a plant.

Prerequisites

You have the permission for **Configuration Items**.

Procedure

Step 1 Choose **System** > **Configuration Items** > **Weather**.

Step 2 Set **API Key** and click **Submit**.

Table 1-41 IP addresses involved in obtaining the API key

IP Address	Description
https://api.worldweatheronline.com	URL used to obtain the global weather service.

NOTE

Obtain the value of **API Key** from a third-party system. The weather forecast information is displayed in the plant overview only after the **API Key** is set.

----End

1.6.7.6 Other

This section describes the system configuration items, including whether to allow remote startup/shutdown.

Prerequisites

You have logged in to SmartPVMS as a administrator.

Procedure

Step 1 Choose **System** > **Configuration Items** > **Other**.

Step 2 Click  .

Step 3 In the dialog box that is displayed, enter the password of the system administrator and click **OK**.

----End

1.7 FAQs

This section describes the common faults of the SmartPVMS client, possible causes of the faults, and troubleshooting methods.

1.7.1 What Do I Do to Avoid the Logout When No Operation Is Prformed on the SmartPVMS Page for a Long Time

When users use browser to visit the SmartPVMS, avoid the Logout When No Operation Is Performed on the SmartPVMS Page for a Long Time.

Problem Description

To prevent other users from performing unauthorized operations, the SmartPVMS allows you to set related idle parameters. If you do not perform operations on the SmartPVMS page for a long time, you will automatically log out of the client and the current page is switched back to the login page. In this case, you need to log in to the client again. This is not friendly for some special application scenarios, such as presentation or large-screen display.

Procedure

1. Choose **System** > **System Settings >Personal Settings** from the main menu.
2. In the navigation tree on the left, choose **Personal Settings** > **Modify Personal Info**.
3. On the **Modify Personal Info** page, modify the property of **Auto-logout if no activity within** .
4. Click **Apply**.

NOTE

To prevent other users from performing unauthorized operations during the absence of a login user, you are advised to enable the **Auto-logout if no activity within** function after the special application scenarios are finished.

1.7.2 How Do I Handle the Problem of Certificate Error or Security Alarm Displayed in the Web Browser

Symptom

- When the Google Chrome is used to log in to SmartPVMS, the system displays a connection error message as shown in **Figure 1-2**.
- When the Mozilla Firefox is used to log in to SmartPVMS, the system displays a connection error message as shown in **Figure 1-3**.

Figure 1-2 A connection error prompted by the Chrome

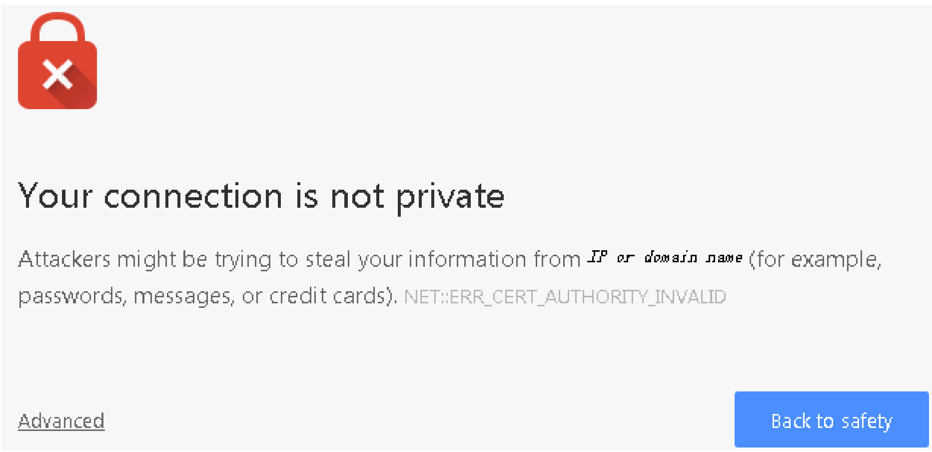
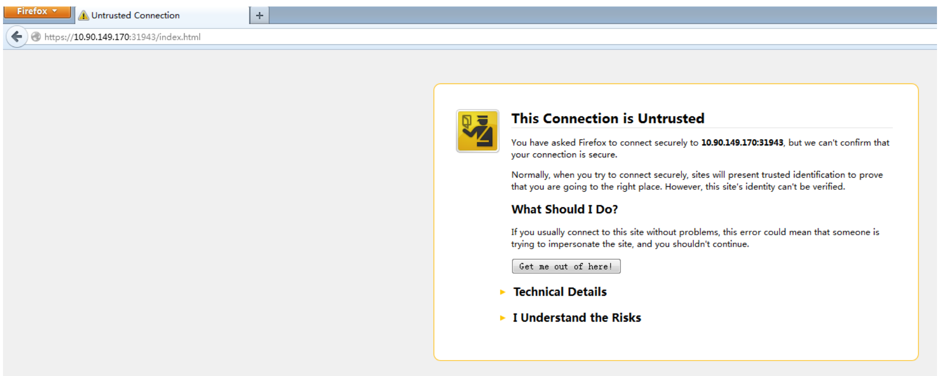


Figure 1-3 A connection error prompted by the Firefox



Procedure

NOTE

Operations on the browser may vary depending on browser versions but are similar to the examples in the following steps. You are advised to perform the operations based on actual situations.

- Install the security certificate in Google Chrome.

  Please select whether to execute the subsequent operations according to the following scenarios.

  a. Obtaining the Trust Certificate from the SmartPVMS Server.

     Use FileZilla to download the **trust.cer** certificate file from the **/opt/oss/NetEco/etc/ssl/er** directory on the SmartPVMS server as user **ossuser** to the local PC.

  b. Installing the Trust Certificate on the Browser:

     i. Open Google Chrome and click in the upper right corner of the browser  Icon Go to **Customise and control Google Chrome** Interface.

     ii. Click **Settings**.

     iii. Click **Show advanced settings**,Click again **Manage certificates**.

     iv. Importing Steps in a Trusted Root Certification Authorities a Certificates that have been saved to the local computer,Click **Import**.

     v. Click **Next step** Browse **Selecting a certificate**.

     vi. Click **Next step**.

     vii. Click **Next step**.

     viii. Click **Completed**.

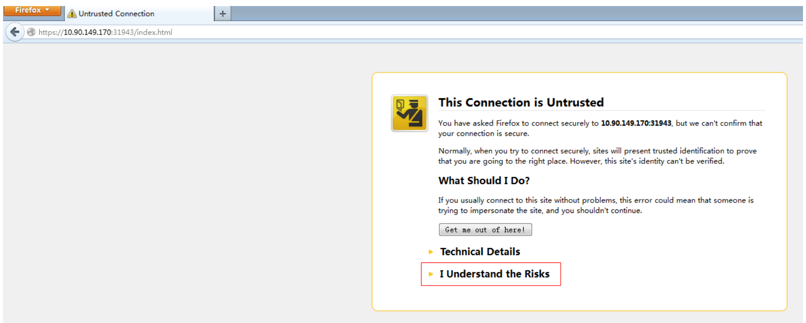
     ix. The **Security Warning** dialog box is displayed. Select **Yes(Y)**.

     x. Click **Yes** Restart the browser.

- Add the exception in Mozilla Firefox.

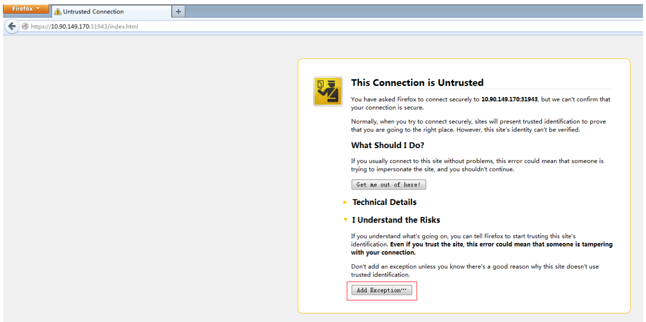
  a. Click **I Understand the Risks** as shown in **Figure 1-4**.

  Figure 1-4 Clicking I Understand the Risks

  b. In the expanded area, click **Add Exception** as shown in **Figure 1-5**.

Figure 1-5 Adding exception.



c. Click **Confirm Security Exception** as shown in **Figure 1-6**.

Figure 1-6 Confirming security exception

1.7.3 How Do I Resolve the Failure to Upload or Download a File?

Symptom

When a user attempts to upload or download a file on the SmartPVMS, the system displays a message indicating that the operation fails or the page does not respond after the user clicks the upload or download button.

Possible Causes

The file exceeds the upload and download traffic limit of the network firewall when the client accesses the SmartPVMS. As a result, the operation fails.

Solution

- Contact the network administrator to remove the traffic limit. After the operation is complete, reconfigure the firewall.
- Access the SmartPVMS from a public network that is not restricted by networks.

1.7.4 How Do I Obtain a Mail Server Certificate on Google Chrome?

Question

How do I obtain a mail server certificate on Google Chrome?

Answer

NOTE

Operations on the browser may vary depending on browser versions but are similar to the examples in the following steps. You are advised to perform the operations based on actual situations.

Step 1 In the address box on Google Chrome, enter the IP address for logging in to the mail server and press **Enter**.

Step 2 Press **F12**. On the displayed console, click the **Security** tab and click **View Certificate**.

NOTE

If the console is not displayed after you press **F12**, allow the console to be displayed in the pop-up blocker and press **F12** again.

Step 3 In the **Certificate** window, click the **Certificate Path** tab, and then select the certificate root path.

Step 4 Click the **Details** tab and click **Copy to File**.

Step 5 In the displayed **Certificate Export Wizard** window, click **Next**.

Step 6 Select **Base64 code X.509 (.CER)** for **Export Format** and click **Next**.

Step 7 Click **Browse**. In the displayed **Save As** dialog box, select the certificate storage path, enter a name for the certificate, and click **Save**.

Step 8 Click **Next**.

Step 9 In the displayed dialog box, click **Finish**."The export was successful." is displayed.

----End

1.7.5 How Do I Obtain an Email Server Certificate on Firefox?

Question

How do I obtain an email server certificate on Firefox?

Answer

NOTE

Operations on the browser may vary depending on browser versions but are similar to the examples in the following steps. You are advised to perform the operations based on actual situations.

Step 1 In the address box on Firefox, enter the IP address for logging in to the email server and press **Enter**.

Step 2 Click on the left of the address box.

Step 3 Click **More Information**.

Step 4 On the **Security** tab page, click **View Certificate**.

Step 5 On the **Details** tab page, click **Export**.

Step 6 Select the certificate storage path, enter a name for the certificate, and click **Save**.

----End

1.8 Environment Parameters

Parameter	Unit	Definition	Formula	Remarks
Global irradiation	kWh/m²	Total solar radiation energy measured by an environmental monitoring instrument (EMI).	/	An EMI is required.
Average temperature	°C	Average ambient temperature measured by the EMI in the plant.	/	

Parameter	Unit	Definition	Formula	Remarks
CO_2 avoided	kg	Amount of CO_2 emitted by burning fossil fuel to produce the same amount of power generated by the plant. 1 kWh of power is equivalent to about 475 g of CO_2 emission (global average value).	Energy yield (kWh) of the plant x per kWh CO_2 emission (0.475)	If the value changes, contact the company administrator to modify the value. For details, see **1.6.5.1 System Parameter Settings**.
Equivalent trees planted	N/A	Number of trees that can absorb the amount of CO_2 avoided by the plant. A tree absorbs 18.3 kg of CO_2 in one year and has a lifespan of 40 years.	CO_2 avoided/CO_2 absorbed by a tree in one year (18.3)/40	
Standard coal saved	kg	Amount of standard coal needed to produce the amount of PV power generated by the plant. 0.4 kg of standard coal is needed to produce 1 kWh of power.	Energy yield (kWh) of the plant x Standard coal needed per kWh (0.4)	

1.9 Power Parameters

Parameter	Unit	Definition	Formula	Remarks
Total string capacity	kWp	Total capacity of PV arrays installed in the PV plant.	Total capacity of the strings connected to all inverters	This parameter is configured during plant creation.
Power per MWp	kW/MWp	Power generated per MWp.	Active power/Total string capacity x 1000	-

Parameter	Unit	Definition	Formula	Remarks
Theoretical yield (daily/ monthly/ yearly)	kWh	Theoretical amount of power that can be generated by the PV arrays installed in a plant.	Hourly: Hourly global irradiation x String capacity Daily: Daily irradiation x String capacity Monthly: Total theoretical yield of each day in a month Yearly: Total theoretical yield of each month in a year	An EMI is required.
PV output power	kW	Total output power of PV arrays.	PV output power	-
PV yield	kWh	Total yield of PV arrays in a given reporting period.	Hourly: PV yield each hour Daily: PV yield each day Monthly: Total yield of each day in a month Yearly: Total yield of each month in a year	-
Inverter yield	kWh	Yield of a plant.	Hourly: Inverter output energy each hour Daily: Inverter output energy each day Monthly: Total inverter output energy of each day in a month Yearly: Total inverter output energy of each month in a year	-
Total yield	kWh	Total output energy of the PV plant throughout the lifetime.	Total PV energy yield	-

Parameter	Unit	Definition	Formula	Remarks
Performance ratio	%	Ratio of measured output energy to total irradiation received by the plant.	PV energy yield/ Theoretical energy yield	-
Specific yield	kWh/kWp	Ratio of the energy yield to the total string capacity.	PV energy yield/ Total PV string capacity	-
Consumption (daily/ monthly/ yearly)	kWh	Power consumed by the loads during a given reporting period.	Daily: Amount of power consumed by the loads each day Monthly: Total amount of power consumed by the loads each day in a month Yearly: Total amount of power consumed by the loads each month in a year	-
Feed-in to grid (daily/ monthly/ yearly)	kWh	Amount of power fed to the power grid from the plant in a give reporting period.	Daily: Amount of power fed to the grid from the plant each day Monthly: Total amount of power fed to the grid from the plant each day in a month Yearly: Total amount of power fed to the grid from the plant each month in a year	A power meter is required. Otherwise, the amount of power purchased from or fed to the grid cannot be displayed.

Parameter	Unit	Definition	Formula	Remarks
Supply from grid (daily/ monthly/ yearly)	kWh	Amount of power purchased from the grid in a given reporting period.	Daily: Amount of power purchased from the grid each day Monthly: Total amount of power purchased from the grid each day in a month Yearly: Total amount of power purchased from the grid each month in a year	
Self-consumption (daily/ monthly/ yearly)	kWh	Amount of power consumed locally. It includes the amount of PV power consumed directly by loads and the amount of PV power stored in batteries.	Daily: Daily PV yield – Daily feed-in to grid Monthly: Total amount of self-consumed power of each day in a month Yearly: Total amount of self-consumed power of each month in a year	-
Self-supplied power (daily/ monthly/ yearly)	kWh	Amount of energy consumption supplied by the PV plant. It includes the amount of PV power consumed directly by loads and the amount of PV power discharged from batteries.	Daily: Daily power consumption – Daily supply from grid Monthly: Total amount of self-supplied power of each day in a month Yearly: Total amount of self-supplied power of each day month in a year	-
Load power	kW	Load consumption power.	Load consumption power	-

Parameter	Unit	Definition	Formula	Remarks
Self-consumption power	kW	Power of PV energy consumed locally.	When feeding to the grid: PV output power – Feed-in power When purchasing power from the grid: PV output power	When the active power of the bi-directional meter is a positive value, the power is the feed-in power. When the active power of the bi-directional meter is a negative value, the power is the power of supply from the grid.

Parameter	Unit	Definition	Formula	Remarks
Battery charge/ discharge power	kW	Battery charge/ discharge power.	Battery charge/ discharge power	If the symbol before the power value is +, the battery is charging. If the symbol before the power value is –, the battery is discharging.
Yield loss due to curtailment	kWh	Energy yield loss caused by power limitation at the grid-connection point.	Theoretical yield x Performance ratio – Actual PV yield	An EMI is required.
Revenue loss due to curtailment	-	Loss of revenue due to power limitation.	Yield loss due to curtailment x Feed-in tariff	If the price unit is inconsistent with the local type, contact the company administrator to change the currency. For details, see **1.6.1.3 Company Information Configuration**.
PV revenue	-	Revenues from photovoltaic power generation. It consists of two parts, which are revenue of power fed in to the grid and the saved electricity bills. Electricity prices need to be configured.	Revenue of power fed in to the grid (power fed to the grid x feed-in tariff) + Saved electricity bills (self-supplied power x electricity price)	

Parameter	Unit	Definition	Formula	Remarks
On-grid duration	h	The time period during which the inverter is connected to the power grid.	Daily: daily on-grid duration Monthly: total daily on-grid durations in a month Year: total monthly on-grid durations in a year	The string capacity needs to be configured. If the string capacity is not configured, the calculated on-grid duration will be inaccurate.

NOTE

Unless otherwise specified, the energy yield in this document refers to AC power yield.