

**SMU11B_X Site Monitoring Unit
V100R023C10**

User Manual

Issue 03
Date 2024-05-24



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

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

Huawei Digital Power Technologies Co., Ltd.

Address: Huawei Digital Power Antuoshan Headquarters
Futian, Shenzhen 518043
People's Republic of China

Website: <https://digitalpower.huawei.com>

About This Document

Purpose

This document describes the product, user interface, network management, and common operations.

This document describes all the functions of the SMU, including the product introduction and system maintenance.

The figures provided in this document are for reference only.

Intended Audience

The document is intended for:


- Technical support engineers
- Hardware installation engineers
- Commissioning engineers
- Maintenance engineers





References

Document
Site App Fact Sheet

Symbol Conventions

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

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

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

Change History

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

Issue 03 (2024-05-24)

Updated [Table 2-2](#) and [Table 2-5](#). Added Safety Information.

Issue 02 (2023-12-15)

Updated [2 Overview](#).

Issue 01 (2023-09-01)

The issue is the first official release.

Software version: eMIMO Embedded Power_V100R023C10

Contents

About This Document.....	ii
1 Safety Information.....	1
1.1 Personal Safety.....	2
1.2 Environment Requirements.....	4
2 Overview.....	7
3 User Interface.....	13
3.1 WebUI.....	13
3.1.1 Permission Description.....	13
3.1.2 Logging In to the WebUI.....	14
3.1.3 UI Introduction.....	15
3.2 Site App.....	15
3.2.1 Permission Description.....	16
3.2.2 Installing the Site App.....	16
3.2.3 Logging In to the Site App.....	17
3.2.4 UI Introduction.....	18
4 Network Management.....	19
4.1 Management Through the NetEco.....	19
4.1.1 IP Networking.....	19
4.1.2 Logging In to the NetEco.....	20
4.2 Network Management (over SNMP).....	21
4.2.1 Connecting a Communications Cable.....	21
4.2.2 Setting Parameters.....	22
4.2.3 Setting SNMP Parameters.....	23
4.2.4 Commissioning on the NMS.....	26
5 Common Operations.....	27
5.1 WebUI Common Operations.....	27
5.1.1 Backing Up Current Settings.....	27
5.1.2 Importing a Configuration File.....	27
5.1.3 Restoring Factory Settings.....	28
5.1.4 Upgrading Software.....	28
5.1.5 Importing an Individual File.....	28

5.1.6 Changing Password.....	29
5.1.7 Viewing Active Alarms.....	30
5.1.8 Viewing Historical Alarms.....	30
5.1.9 Viewing Version Information.....	30
5.1.10 Collecting Fault Information.....	31
5.1.11 Exporting Maintenance Information.....	31
5.2 App Common Operations.....	31
A FAQ.....	34
A.1 How Do I Prepare the WebUI Operating Environment.....	34
B Acronyms and Abbreviations.....	39

1 Safety Information

Statement

Before transporting, storing, installing, operating, using, and/or maintaining the equipment, read this document, strictly follow the instructions provided herein, and follow all the safety instructions on the equipment and in this document. In this document, "equipment" refers to the products, software, components, spare parts, and/or services related to this document; "the Company" refers to the manufacturer (producer), seller, and/or service provider of the equipment; "you" refers to the entity that transports, stores, installs, operates, uses, and/or maintains the equipment.

The **Danger, Warning, Caution, and Notice** statements described in this document do not cover all the safety precautions. You also need to comply with relevant international, national, or regional standards and industry practices. **The Company shall not be liable for any consequences that may arise due to violations of safety requirements or safety standards concerning the design, production, and usage of the equipment.**

The equipment should be used in an environment that meets the design specifications. Otherwise, the equipment may be faulty, malfunctioning, or damaged, which is not covered under the warranty. The Company shall not be liable for any property loss, personal injury, or even death caused thereby.

Comply with applicable laws, regulations, standards, and specifications during transportation, storage, installation, operation, use, and maintenance.

Do not perform reverse engineering, decompilation, disassembly, adaptation, implantation, or other derivative operations on the equipment software. Do not study the internal implementation logic of the equipment, obtain the source code of the equipment software, violate intellectual property rights, or disclose any of the performance test results of the equipment software.

The Company shall not be liable for any of the following circumstances or their consequences:

- Equipment damage due to force majeure such as earthquakes, floods, volcanic eruptions, debris flows, lightning strikes, fires, wars, armed conflicts, typhoons, hurricanes, tornadoes, and extreme weather conditions
- Operation beyond the conditions specified in this document

- Installation or use in environments that do not comply with international, national, or regional standards
- Installation or use by unqualified personnel
- Failure to follow the operation instructions and safety precautions on the product and in the document
- Unauthorized modifications to the product or software code or removal of the product
- Damage caused during transportation by you or a third party authorized by you
- Storage conditions that do not meet the requirements specified in the product document
- Failure to comply with local laws, regulations, or related standards due to the materials and tools prepared by you
- Damage caused by your or a third party's negligence, intentional breach, gross negligence, or improper operations or damage not caused by the Company

1.1 Personal Safety

 **DANGER**

Do not work with power on during installation. Do not install or remove a cable with power on. Transient contact between the core of the cable and a conductor will generate electric arcs or sparks, which may cause a fire or personal injury.

 **DANGER**

Non-standard and improper operations on the energized equipment may cause fire or electric shocks, resulting in property damage, personal injury, or even death.

 **DANGER**

Before operations, remove conductive objects such as watches, bracelets, bangles, rings, and necklaces to prevent electric shocks.

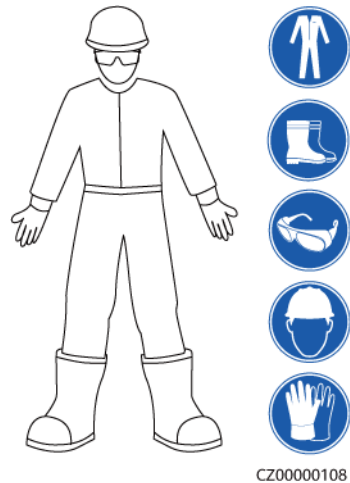
 **DANGER**

During operations, use dedicated insulated tools to prevent electric shocks or short circuits. The insulation and voltage resistance must comply with local laws, regulations, standards, and specifications.

WARNING

During operations, wear personal protective equipment such as protective clothing, insulated shoes, goggles, safety helmets, and insulated gloves.

Figure 1-1 Personal protective equipment



General Requirements

- Do not stop protective devices. Pay attention to the warnings, cautions, and related precautionary measures in this document and on the equipment.
- If there is a likelihood of personal injury or equipment damage during operations, immediately stop, report the case to the supervisor, and take feasible protective measures.
- Do not power on the equipment before it is installed or confirmed by professionals.
- Do not touch the power supply equipment directly or with conductors such as damp objects. Before touching any conductor surface or terminal, measure the voltage at the contact point to ensure that there is no risk of electric shock.
- Do not touch a running fan with your hands, components, screws, tools, or boards. Otherwise, personal injury or equipment damage may occur.
- In the case of a fire, immediately leave the building or the equipment area and activate the fire alarm or call emergency services. Do not enter the affected building or equipment area under any circumstances.

Personnel Requirements

- Only professionals and trained personnel are allowed to operate the equipment.
 - Professionals: personnel who are familiar with the working principles and structure of the equipment, trained or experienced in equipment operations and are clear of the sources and degree of various potential hazards in equipment installation, operation, maintenance
 - Trained personnel: personnel who are trained in technology and safety, have required experience, are aware of possible hazards on themselves in

certain operations, and are able to take protective measures to minimize the hazards on themselves and other people

- Personnel who plan to install or maintain the equipment must receive adequate training, be able to correctly perform all operations, and understand all necessary safety precautions and local relevant standards.
- Only qualified professionals or trained personnel are allowed to install, operate, and maintain the equipment.
- Only qualified professionals are allowed to remove safety facilities and inspect the equipment.
- Personnel who will perform special tasks such as electrical operations, working at heights, and operations of special equipment must possess the required local qualifications.
- Only authorized professionals are allowed to replace the equipment or components (including software).
- Only personnel who need to work on the equipment are allowed to access the equipment.

1.2 Environment Requirements

 **DANGER**

Do not expose the equipment to flammable or explosive gas or smoke. Do not perform any operation on the equipment in such environments.

 **DANGER**

Do not store any flammable or explosive materials in the equipment area.

 **DANGER**

Do not place the equipment near heat sources or fire sources, such as smoke, candles, heaters, or other heating devices. Overheat may damage the equipment or cause a fire.

 **WARNING**

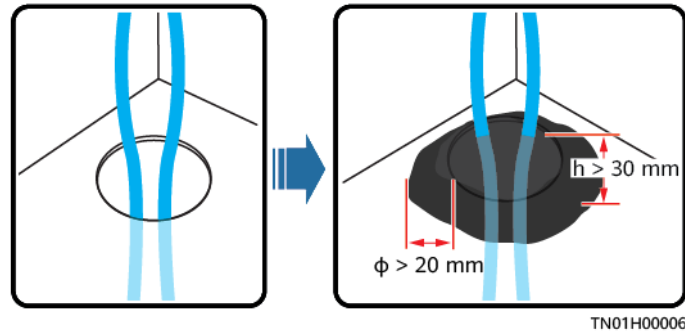
Install the equipment in an area far away from liquids. Do not install it under areas prone to condensation, such as under water pipes and air exhaust vents, areas prone to water leakage, such as air conditioner vents, ventilation vents, or feeder windows of the equipment room, or low-lying areas with poor drainage. Ensure that no liquid enters the equipment to prevent faults or short circuits.

 **WARNING**

To prevent damage or fire due to high temperature, ensure that the ventilation vents or heat dissipation systems are not obstructed or covered by other objects while the equipment is running.

General Requirements

- Ensure that the equipment is stored in a clean, dry, and well ventilated area with proper temperature and humidity and is protected from dust and condensation.
- Keep the installation and operating environments of the equipment within the allowed ranges. Otherwise, its performance and safety will be compromised.
- Do not install, use, or operate outdoor equipment and cables (including but not limited to moving equipment, operating equipment and cables, inserting connectors to or removing connectors from signal ports connected to outdoor facilities, working at heights, performing outdoor installation, and opening doors) in harsh weather conditions such as lightning, rain, snow, and level 6 or stronger wind.
- Do not install the equipment in an environment with dust, smoke, volatile or corrosive gases, infrared and other radiations, organic solvents, or salty air.
- Do not install the equipment in an environment with conductive metal or magnetic dust.
- Do not install the equipment in an area conducive to the growth of microorganisms such as fungus or mildew.
- Do not install the equipment in an area with strong vibration, noise, or electromagnetic interference.
- Ensure that the site complies with local laws, regulations, and related standards.
- Ensure that the ground in the installation environment is solid, free from spongy or soft soil, and not prone to subsidence. The site must not be located in a low-lying land prone to water or snow accumulation, and the horizontal level of the site must be above the highest water level of that area in history.
- If the equipment is installed in a place with abundant vegetation, in addition to routine weeding, harden the ground underneath the equipment using cement or gravel.
- Before opening doors during the installation, operation, and maintenance of the equipment, clean up any water, ice, snow, or other foreign objects on the top of the equipment to prevent foreign objects from falling into the equipment.
- When installing the equipment, ensure that the installation surface is solid enough to bear the weight of the equipment.
- All cable holes must be sealed. Seal the used cable holes with sealing putty. Seal the unused cable holes with the caps delivered with the equipment. The following figure shows the criteria for correct sealing with sealing putty.

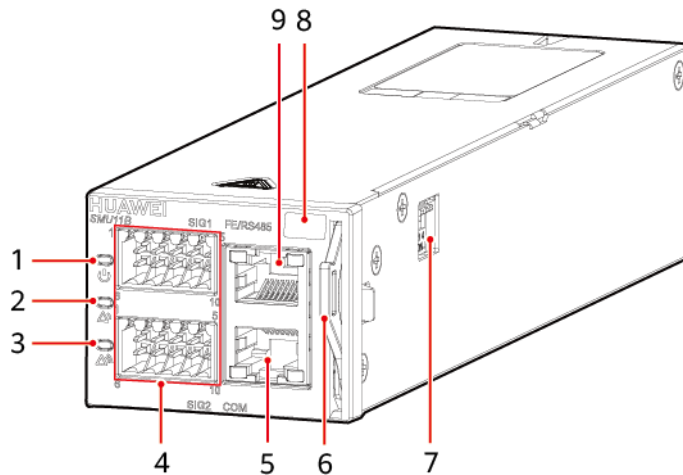


- After installing the equipment, remove the packing materials such as cartons, foam, plastics, and cable ties from the equipment area.

2 Overview

Appearance

Figure 2-1 SMU11B appearance



ZX00000040

- (1) Running indicator
- (2) Minor alarm indicator
- (3) Major alarm indicator
- (4) Wiring terminals
- (5) Communications port COM
- (6) Handle
- (7) DIP switch
- (8) Position of the SN code
- (9) Northbound FE/RS485 port

Indicators

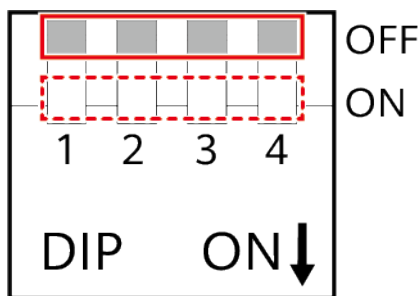
Table 2-1 Indicator description

Name	Color	Status	Description
Running indicator	Green	Off	The SMU is faulty or has no power input.
		Blinking slowly (0.5 Hz)	The SMU is running and communicating with the host properly.

Name	Color	Status	Description
		Blinking fast (4 Hz)	The SMU is running properly but fails to communicate with the host.
Minor alarm indicator	Yellow	Off	No minor alarm or warning is generated.
		Steady on	A minor alarm or warning is generated.
Major alarm indicator	Red	Off	No critical or major alarm is generated.
		Steady on	A critical or major alarm is generated.

DIP Switch

Figure 2-2 DIP switch



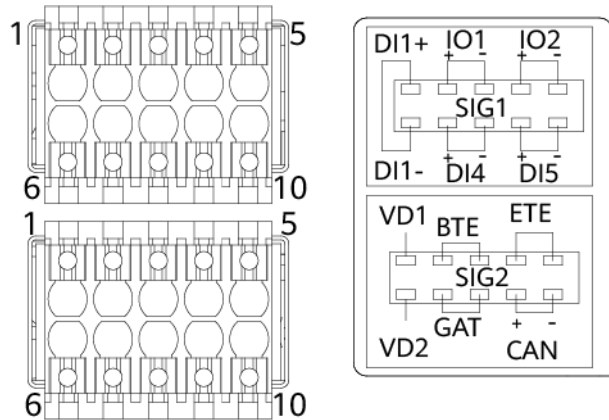
TO11W00136

Table 2-2 DIP switch description

Pin	Description
1	When the DIP switch is turned off, the input level is high, and the FE/RS485 port is used for northbound FE communication. When the DIP switch is turned on, the input level is low, and the FE/RS485 port is used for northbound RS485 communication.
2	When the DIP switch is turned on or turned off, the IP address is reset.
3	When the DIP switch is turned off, the input level is high, and the WiFi function is disabled. When the DIP switch is turned on, the input level is low, and the WiFi function is enabled.
4	Reserved I/O input

Wiring Terminals

Figure 2-3 Wiring terminals



WYR0000597

Table 2-3 Pin definitions for SIG1 wiring terminals

Pin	Signal	Dry Contact	Description
1	DI1+	DIN1	Dry contact inputs
6	DI1-		
7	DI4+	DIN4	
8	DI4-		
9	DI5+	DIN5	
10	DI5-		
2	IO1+	ALM1/DIN2 (ALM1 by default)	Dry contact inputs/Dry contact outputs (When used as dry contact inputs, the alarm condition is as follows: normal when open, alarm when closed. When used as dry contact outputs, the alarm action is as follows: open when normal, closed when alarm.)
3	IO1-		
4	IO2+	ALM2/DIN3 (ALM2 by default)	
5	IO2-		

Table 2-4 Pin definitions for SIG2 wiring terminals

Pin	Signal	Description
1	VD1	Battery midpoint voltage detection port 1
6	VD2	Battery midpoint voltage detection port 2
2	BTE	Battery temperature sensor port
3		
4	ETE	Ambient temperature sensor port
5		
7	GAT	Door status sensor port
8		
9	CAN+	CAN communications port
10	CAN-	

Communications Ports

Table 2-5 Communications port description

Communications Port	Communications Parameter	Communications Protocol		Function
COM	Baud rate: 9600 bit/s, 19200 bit/s, 115200 bit/s, auto-negotiation Communications address: 33	Modbus		Connects to a third-party network management system (NMS).
		Modbus		Manages site or third-party devices.
		-		Provides 12 V power supply for external devices.
FE/RS485	10M/100M autonegotiation	FE	SNMP	Connects to a third-party NMS (pin 1 of the DIP switch: OFF).

Communications Port	Communications Parameter	Communications Protocol		Function
			BIN	Connects to a Huawei NMS (pin 1 of the DIP switch: OFF).
			HTTPS	Connects to a PC and manages the SMU on the WebUI (pin 1 of the DIP switch: OFF).
	Baud rate: 9600 bit/s, 19200 bit/s, 115200 bit/s, auto-negotiation Communications address: 3	RS485	Master/Slave	Connects to a Huawei NMS (pin 1 of the DIP switch: ON).
<p>Notes:</p> <ul style="list-style-type: none"> • All these ports are protected by a security mechanism. • The COM port is a multiplexing port. To connect the port to a third-party NMS, you need to set the parameter. On the WebUI, choose System Settings > Basic Settings > Setup Parameter > Basic Parameter. Set Front Panel Serial Port Apply to North Access. 				

Figure 2-4 Pins in the COM port
RJ45 female

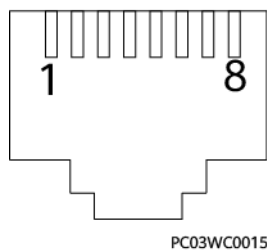


Table 2-6 Pin definitions for the COM port

Pin	Signal	Description
1	RS485+	RS485 data, positive
2	RS485-	RS485 data, negative

Pin	Signal	Description
3	12V	Power supply
4	RS485+	RS485 data, positive
5	RS485-	RS485 data, negative
6	SCL	I ² C clock
7	SDA	I ² C data
8	GND	Ground

Figure 2-5 Pins in the FE/RS485 port
RJ45 female

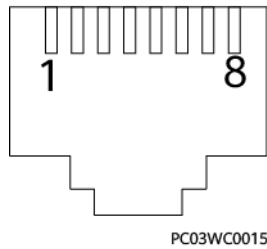


Table 2-7 Pin definitions for the FE/RS485 port

Pin	Signal	Description
1	TX+	Transmit data over northbound FE/RS485.
2	TX-	
3	RX+	Receives data over northbound FE.
6	RX-	
4	RX+	Receive data over northbound RS485.
5	RX-	
7, 8	Reserved	-

3 User Interface

3.1 WebUI

3.1.1 Permission Description

NOTICE

- The administrator password can only be used by the administrator. It must not be provided for third-party maintenance personnel.
- Change the password upon the first login. To ensure system security, you are advised to change the password periodically. You can change the password under **User Management** on the **Maintenance** tab page.
- The Company will not be liable for any security issues caused by your failure to change the password in time or password loss after changing. (Forgotten passwords cannot be recovered.)

On the WebUI, the SMU supports three permission levels, as described in the following table.

Table 3-1 Three-level password management

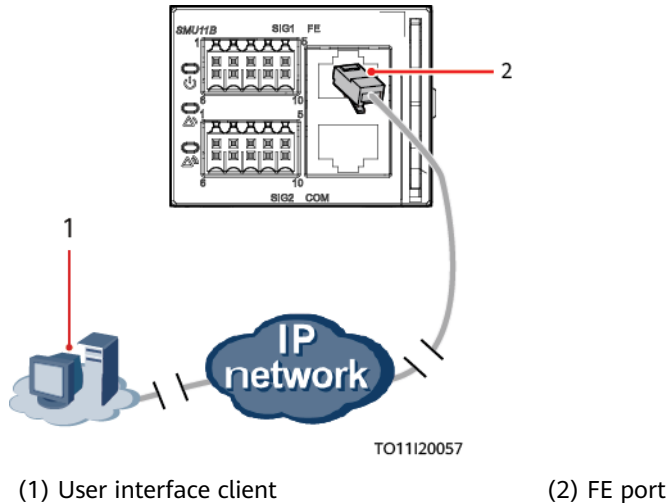
Level	Username	Operation Permission	Preset Password
Administrator	admin	Has all operation permissions.	Changeme
Engineer	engineer	Has all permissions except for changing the administrator password.	Changeme
Operator	operator	Has the permission to view parameters only.	Changeme

3.1.2 Logging In to the WebUI

Procedure

- Step 1** Prepare the WebUI operating environment by referring to [A.1 How Do I Prepare the WebUI Operating Environment](#).
- Step 2** Connect a network cable to the FE port on the SMU.

Figure 3-1 Connecting a communications cable



- Step 3** Set the PC IP address to be in the same network segment as the SMU IP address.

For example, if the SMU has an IP address of 192.168.0.10, a subnet mask of 255.255.255.0, and a default gateway of 192.168.0.1, set the IP address to 192.168.0.11, subnet mask to 255.255.255.0, and default gateway to 192.168.0.1 on the PC.

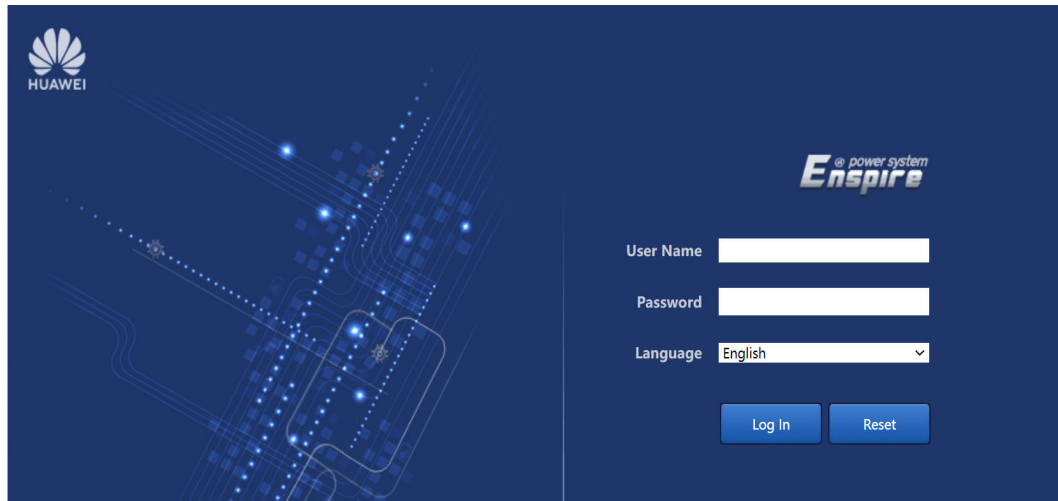
NOTE

If IPv6 networking is used, you need to set the **Value data** of **DisabledComponents** to 0 in Registry Editor, restart the PC for the change to take effect, and then set the IP address of the PC.

- Step 4** If IPv4 networking is used, enter **https://*SMU local IP address*** (such as https://192.168.0.10) in the address box of the browser, and then press Enter to enter the login page.

If IPv6 networking is used, enter **https://[*SMU local IP address*]** (such as https://[2001::2002]) in the address box of the browser, and then press Enter to enter the login page.

Figure 3-2 WebUI login page



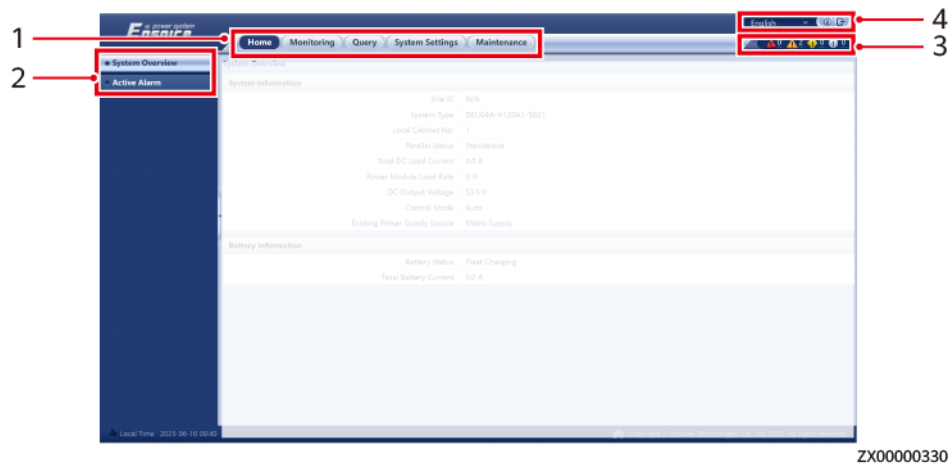
NOTE

The preset username is **admin**, and the preset password is **Changeme**.

----End

3.1.3 UI Introduction

Figure 3-3 WebUI homepage



(1) Main menu

(2) Navigation pane

(3) Active alarm bar

(4) Language bar

3.2 Site App

3.2.1 Permission Description

NOTICE

- The permissions of the app user are the same as those of the web user.
- The administrator password can only be used by the administrator. It must not be provided for third-party maintenance personnel.
- Change the password upon the first login. To ensure system security, you are advised to change the password periodically. If the app does not provide the password change function, change the password on the WebUI.
- The Company will not be liable for any security issues caused by your failure to change the password in time or password loss after changing. (Forgotten passwords cannot be recovered.)

On the app, the SMU supports three permission levels, as described in the following table.

Table 3-2 Three-level password management

Level	Username	Operation Permission	Preset Password
Administrator	admin	Has all operation permissions.	Changeme
Engineer	engineer	Has all permissions except for changing the administrator password.	Changeme
Operator	operator	Has the permission to view parameters only.	Changeme

3.2.2 Installing the Site App

Prerequisites

- You have a mobile phone running Android 8.0 or later.
- The mobile phone can properly connect to the Internet.

Procedure

Step 1 Contact technical support engineers to obtain the latest Site app installation package.

1. Log in to the Huawei support website.

NOTE

Login address: <https://support.huawei.com/enterprise/en/index.html>

2. Search for **DP*Site.apk**.
3. Select **Software & Tools**, and then select **Product Software** from the **Filter by Document Type** drop-down list.
4. Download the **DP_XXXXX_Site.apk** installation package.

Step 2 Install the Site app on the mobile phone.

Figure 3-4 Site app icon



----End

3.2.3 Logging In to the Site App

Prerequisites

- Enable the GPS positioning function on the mobile phone and grant the GPS permission to the app.
- You have obtained the Site app username and password.
- The mobile phone is within 10 m (without obstacles) away from the power supply device.
- The app may be occasionally disconnected due to poor WiFi signal. In this case, connect again later.

Procedure

- Step 1** Set pin 3 of the DIP switch to ON to enable the WiFi function of the SMU11B.
- Step 2** Log in to the WebUI, choose **System Settings > Network Config**, set **Enable WIFI** to **Yes** on the WiFi page, and record the values of **SSID** and **Password**.
- Step 3** On the WLAN settings screen on your mobile phone, enable the WLAN function, find the device based on the recorded SSID on the WebUI, and enter the recorded password to connect to the device.
- Step 4** Tap the Site app icon to open the app.
- Step 5** Tap **WIFI connection** and enter the username and password. (The preset username is **admin**. The preset password is **Changeme**.)

NOTICE

The login password of the Site app is the same as that of the WebUI. Once the WebUI login password is changed, the Site app login password is changed simultaneously.

Step 6 Tap **Log In** to enter the home screen.

----End

3.2.4 UI Introduction

For details about the UI, see [Site App Fact Sheet](#).

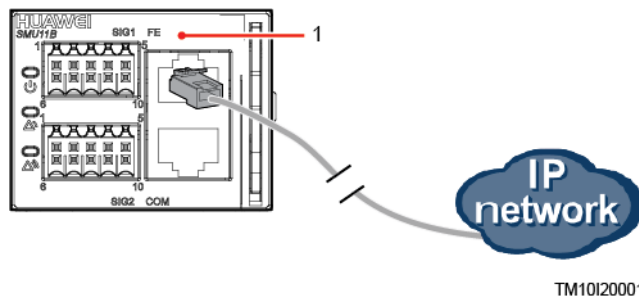
4 Network Management

4.1 Management Through the NetEco

4.1.1 IP Networking

Step 1 Connect a network cable to the FE port on the SMU.

Figure 4-1 Connecting a communications cable



(1) FE port

Step 2 Apply for a fixed IP address from the network administrator of the site or equipment room.

Step 3 Set the IP protocol version, IP address, subnet mask, and gateway address on the WebUI.

NOTICE

If the IP address of the SMU11B is changed on the WebUI, record the IP address for future login.

Table 4-1 IPv4 parameters

Path	Parameter	Default Value	Setting
System Settings > Network Config	IP Address	192.168.0.10	Set this parameter based on the address assigned by the network administrator.
	Subnet Mask	255.255.255.0	Set this parameter based on the address assigned by the network administrator.
	Default Gateway	192.168.0.1	Set this parameter based on the address assigned by the network administrator.

Step 4 Set the IP addresses and port numbers for the primary and backup NetEco servers on the WebUI.

Table 4-2 NetEco parameters

Path	Parameter	Default Value	Setting
System Settings > NetEco	NetEco Primary IP	192.168.0.10	Set this parameter to the IP address of the primary NetEco server.
	NetEco Backup IP	192.168.0.10	Set this parameter to the IP address of the backup NetEco server.
	NetEco Port Number	31220	31220 Contact Huawei technical support if you need to change the port number.

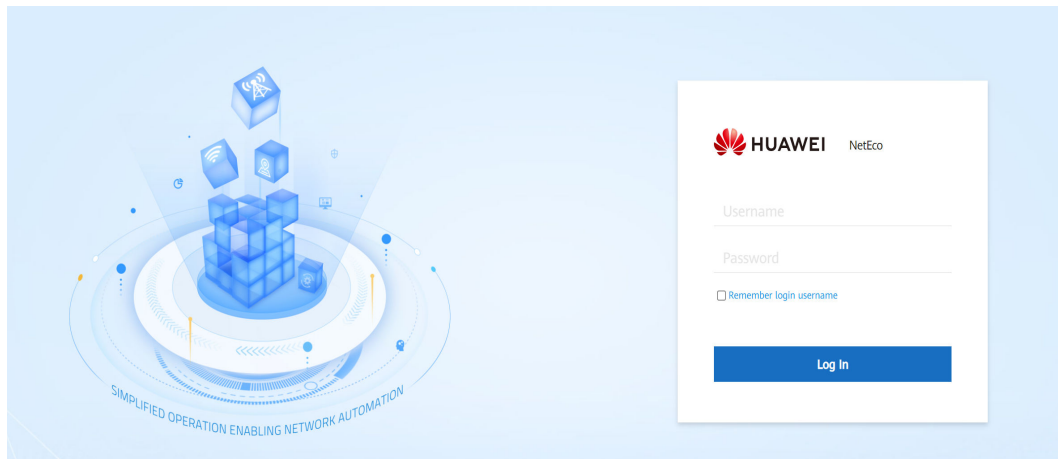
----End

4.1.2 Logging In to the NetEco

Procedure

Step 1 Enter ***https://NetEco IP address:port number for NetEco login*** (for example, ***https://10.10.10.1:31943***) in the address box of the browser and press Enter to go to the NetEco login page.

Figure 4-2 NetEco login page



Step 2 Enter the correct username and password and click **Log In**.

NOTICE

To obtain the NetEco username and password, contact the network administrator of the site or equipment room.

----End

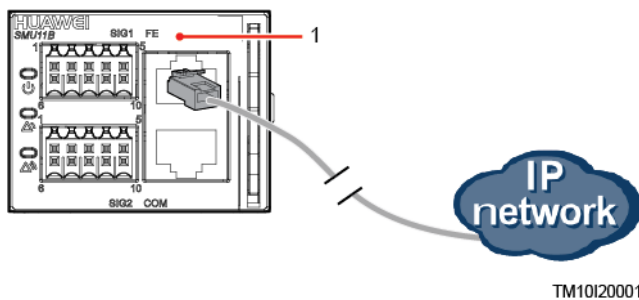
4.2 Network Management (over SNMP)

4.2.1 Connecting a Communications Cable

Procedure

Step 1 Connect a network cable to the FE port on the SMU.

Figure 4-3 Connecting a communications cable



(1) FE port

----End

4.2.2 Setting Parameters

Procedure

Step 1 Apply for a fixed IP address from the network administrator of the site or equipment room.

Step 2 On the WebUI, select an IP protocol version and set IP parameters.

Table 4-3 IPv4 parameters

Path	Parameter	Default Value	Setting
System Settings > Network Parameters	IP Address	192.168.0.10	Set this parameter according to the address provided by the network administrator.
	Subnet Mask	255.255.255.0	Set this parameter according to the subnet mask provided by the network administrator.
	Default Gateway	192.168.0.1	Set this parameter according to the gateway address provided by the network administrator.

Table 4-4 IPv6 parameters

Path	Parameter	Default Value	Setting
System Settings > Network Parameters	IP Address	2001::2002	Set this parameter according to the address provided by the network administrator. a to f, A to F, 0 to 9, and .; (a maximum of 45 characters)
	Subnet Prefix Length	64	1-128
	Default Gateway	2001::2001	Set this parameter according to the gateway address provided by the network administrator. a to f, A to F, 0 to 9, and .; (a maximum of 45 characters)

----End

4.2.3 Setting SNMP Parameters

Prerequisites

 **NOTE**

You can set SNMP parameters remotely or locally on the WebUI.

Before setting SNMP parameters, obtain the information listed in [Table 4-5](#) from the SNMP-based NMS.

Table 4-5 Information obtained from the NMS

Information	Description
SNMP Version	SNMP version and port number used for communication between the SMU and the NMS. The SNMP version can be SNMPv1, SNMPv2c, or SNMPv3.
SNMP Port Number	
Read Community Name	If you use SNMPv1 or SNMPv2c, enter the read and write community names that comply with the NMS. Otherwise, the SMU will not connect to the NMS. The read community name must be different from the write community name.
Write Community Name	
User Name	To enhance the security, you need a username and password for authentication if you use SNMPv3. After the authentication succeeds, the SMU can communicate with the NMS.
MD5/SHA Password	
DES/AES Password	
Trap Target Address	IP address and port number used for reporting alarm trap packets
Trap Port	
Trap Community	If you use SNMPv1 or SNMPv2c, this parameter is the community name used for reporting alarm trap packets.

 **NOTE**

- The standard protocols SNMPv1 and SNMPv2c have security risks. You are advised to use SNMPv3.
- The standard encryption algorithms MD5 and DES have security risks. You are advised to use the secure encryption algorithms SHA and AES.

Procedure

Step 1 Log in to the WebUI.

 **NOTE**

The preset username is **admin**, and the preset password is **Changeme**.

Step 2 Choose **System Settings > SNMP**. The SNMP page is displayed.

Step 3 In the **SNMP** area, set SNMP parameters.

Table 4-6 Setting SNMP parameters

Parameter	Description
SNMP Version	Specifies the SNMP version used by the SMU and NMS. Set this parameter to ALL , SNMPv1&SNMPv2c , or SNMPv3 based on site requirements. If there are more than two NMSs and the SNMP versions are SNMPv1/SNMPv2c and SNMPv3, set this parameter to ALL .
SNMP Port Number	Specifies the SNMP port number used by the SMU and NMS. Set this parameter based on site requirements. Value range: 1 to 65535.
Read Community Name	Set this parameter based on site requirements. This parameter is not displayed when the SNMP version is set to SNMPv3 .
Write Community Name	Set this parameter based on site requirements. This parameter is not displayed when the SNMP version is set to SNMPv3 .

Step 4 In the **SNMPv3** area, click **Add**. The **SNMPv3** dialog box is displayed. Add a user.

Table 4-7 Adding an SNMPv3 user

Parameter	Description
User Name	Set this parameter based on site requirements. a to z, A to Z, 0 to 9, and _ (1 to 15 characters)
Authentication Protocol	Select MD5, SHA1, SHA2-256, SHA2-384, or SHA2-512 as required.
MD5/SHA Password	Set this parameter based on site requirements. a to z, A to Z, 0 to 9, and _ (8 to 15 characters; a combination of at least two types of characters; different from the username or its reverse)
Confirm MD5/SHA Password	The value must be the same as the MD5/SHA password.
Proprietary Protocol	Select DES, AES-128, AES-192, or AES-256 as required.

Parameter	Description
DES/AES Password	Set this parameter based on site requirements. a to z, A to Z, 0 to 9, and _ (8 to 15 characters; a combination of at least two types of characters; different from the username or its reverse)
Confirm DES/AES Password	The value must be the same as the DES/AES password.
Password Validity Period	Set this parameter based on site requirements. Value range: 1 to 11000 (days).
Advance Warning Before Password Expires (days)	Set this parameter based on site requirements. Value range: 1 to 90 (days).

Step 5 In the **SNMP Trap** area, click **Add**. The **SNMP Trap** dialog box is displayed. Set the trap address.

Table 4-8 Setting the trap address

Parameter	Description
IPv4/IPv6	Select an IP protocol version based on site requirements.
Trap Target Address	Specifies the IP address used for reporting alarm trap packets. Set this parameter based on site requirements.
Trap Port	Specifies the port number used for reporting alarm trap packets. Set this parameter based on site requirements. Value range: 1 to 65535.
SNMP Version	Set this parameter to SNMPv1 , SNMPv2c , or SNMPv3 based on site requirements.
SNMPv3 User Name	This parameter is displayed when the SNMP version is set to SNMPv3 . Set this parameter based on site requirements.
Trap Community	This parameter is displayed when the SNMP version is set to SNMPv1 or SNMPv2c . Set this parameter based on site requirements. a to z, A to Z, 0 to 9, and _ (8–20 characters, a combination of at least two types of characters)

 **NOTE**

The SNMP version here can be different from the version in [Step 3](#).

Step 6 In **Mib File**, click **Export** to export the MIB file and then import it into the NMS.

 NOTE

If there is only one NMS, perform [4.2.3 Setting SNMP Parameters](#) once only.

----End

4.2.4 Commissioning on the NMS

You can manage the power system on the NMS that is connected over SNMP. For details, see the related documents of the NMS.

5 Common Operations

 **WARNING**

On the WebUI, when you set parameters about air conditioner startup/shutdown, LLVD/BLVD voltage, load connection/disconnection, battery connection/disconnection, rectifier startup/shutdown, and rectifier power limit, the site power supply may be affected.

5.1 WebUI Common Operations

5.1.1 Backing Up Current Settings

The configuration file contains all user configuration information (such as parameter values and alarm configurations) about the current system.

You can back up the configuration file for the current site, and use the configuration file to rapidly configure parameters for other sites.

- Step 1** Choose **Maintenance > Configuration File**, enter the encryption password for exporting the configuration file in the **Back Up Current Settings** area, and click **Back Up Current Settings**.

----End

5.1.2 Importing a Configuration File

You can quickly configure site parameters by importing a configuration file.

- Step 1** Choose **Maintenance > Configuration File**, enter the decryption password for importing the configuration file in the **Import a new configuration file** area, select the new configuration file, and click **Upload**.

----End

 NOTE

- When importing the backup configuration file, ensure that the system types of the exported and imported configuration files are consistent.
- If an encryption password is set when the configuration file is exported, the decryption password for importing the configuration file must be the same as the encryption password.

5.1.3 Restoring Factory Settings

Step 1 Choose **Maintenance > Configuration File**. In the **Restore Factory Settings** area, click **Restore Factory Settings**.

----End

 CAUTION

- After factory settings are restored, the SMU restarts.
- After factory settings are restored, all parameter values change to their factory defaults. You are advised to back up the current settings before restoring factory settings.

5.1.4 Upgrading Software

You can use the WebUI to upgrade software for the SMU BSP, SMU, intelligent device SO library package, and southbound devices.

Step 1 Choose **Maintenance > Software Upgrade**, select the upgrade file in **Software Upgrade**, and click **Upload**.

----End

 CAUTION

- To retain pre-upgrade parameter settings, back up the data before upgrading software.
- The SMU will restart automatically after the software for the SMU BSP, SMU, and intelligent device SO library package is upgraded.
- Exercise caution to choose the version rollback function during software upgrade. After version rollback, the user accounts created are deleted, and the preset username and password are required for login.

5.1.5 Importing an Individual File

The SMU restarts after an individual file is imported.

Step 1 Choose **System Settings > Basic Settings > Site Config**. In the **System Individual File** area, select a system individual file to be uploaded based on the file storage path and click **Upload**.

----End

5.1.6 Changing Password

Context

For security purposes, change your password periodically.

Changing a User Password

- Step 1** Choose **Maintenance > User Management**. The user management page is displayed.
- Step 2** Select the user whose password needs to be changed and click **Modify**. The dialog box for modifying user information is displayed.
- Step 3** Change the user password.

Table 5-1 Changing a user password

Parameter	Description
Old Password	Specifies the current password of the selected user. This parameter is required only when administrator users change their own passwords.
New Password	Set this parameter based on site requirements. a to z, A to Z, 0 to 9, and !@*_?{}= (8 to 20 characters; a combination of at least two types of characters; different from the username or its reverse)
Confirm password	The confirm password must be the same as the new password.
Permission	Modify the management rights of the selected user, including administrator, engineer, and operator users. An administrator user can change the passwords of all users. Engineer and operator users can change their own passwords.
Password Validity Period	Set this parameter based on site requirements. Value range: 1 to 11000 (days).
Advance Warning Before Password Expires (days)	Set this parameter based on site requirements. Value range: 1 to 90 (days).

----End

Changing the WiFi Password

NOTICE

- You are advised to periodically change the WiFi password to improve account security and prevent network attacks, such as data tampering.
- The Company will not be liable for any security issues caused by your failure to change the password in time or password loss after changing. (Forgotten passwords cannot be recovered.)
- The WiFi function is disabled by default. Enable the WiFi function before using it and disable it after using it to ensure cybersecurity.

Table 5-2 Setting the WiFi parameters

Path	Parameter	Default Value	Setting
System Settings > Basic Settings > Network Config > WIFI	WIFI Enable	Enable	Enable, Disable
	SSID	POWER_SIT E	a to z, A to Z, 0 to 9, and _#@.- (a maximum of 31 characters)
	Password	Changeme	a to z, A to Z, 0 to 9, and _#@.- (a maximum of 31 characters; recommendation: more than eight characters and at least two types of characters)

5.1.7 Viewing Active Alarms

Active alarms are alarms that are not cleared.

- Step 1** Choose **Home > Active Alarm** to view active alarms. You can filter active alarms by **Equipment** or **Severity**.

----End

5.1.8 Viewing Historical Alarms

Historical alarms are alarms that have been cleared.

- Step 1** Choose **Query > Historical Alarm**. You can filter historical alarms by **Equipment**, **Start Time**, and **End Time**, and click **Query** to view historical alarms.

----End

5.1.9 Viewing Version Information

You can query the SMU version information to facilitate fault diagnosis and check whether the upgrade is successful.

- Step 1** Choose **Maintenance > Version Information** and view the version information.
----End

5.1.10 Collecting Fault Information

The SMU11B collects fault information about rectifiers. The fault information records the running information about the rectifier for a specified period of time. The information can be used to locate faults. You can choose **Maintenance > Fault Information** to export the fault information file of the corresponding device only after fault information is collected.

- Step 1** Collect rectifier fault information. Choose **Monitoring > Digital Power > Rectifier Group > Running Control**, select **Collect Fault Information** under **Fault Information Collection Control**, and click **Submit**.
----End

5.1.11 Exporting Maintenance Information

You can export historical alarms, active alarms, performance data, operation logs, and battery test records on the WebUI.

You can view and export e-label information about the power subrack, SMU, and rectifiers on the WebUI.

You can export version and system operation information in one-click mode on the WebUI to quickly collect information and identify system faults.

- Step 1** Export historical data. Choose **Query > Export Data**, select a data type, and click **Export**.
- Step 2** Export e-labels. Choose **Maintenance > E-label** and click **Export All**.
- Step 3** Export fault information. Choose **Maintenance > Fault Information**, set **Encryption Password for Export** in the **Export Fault Information** area, and click **Export Fault Information**.

If you want to export lithium battery logs, select **Lithium battery n log** in the **Export Concurrently** area. The lithium battery logs and fault information are exported together.

----End

NOTE

If information export fails due to a browser error, wait for a certain period (30 minutes at most), log in, and try again.

5.2 App Common Operations

Upgrading Software

- The SMU restarts after the software is upgraded.
- Obtain the latest upgrade package from Huawei technical support.

Step 1 Access the **Upgrade management** menu.

On the Site app: Choose **Maintenance > Upgrade management**, and select the upgrade file.

Step 2 Upgrade the file.

----End

Resetting the SMU

Resetting the SMU takes several minutes. During the resetting, the SMU cannot monitor or manage rectifiers, batteries, and other connected devices. Resetting the SMU has no impact on parameter settings so there is no need to set parameters again.

On the Site app: Choose **Home > Controller > Control > Basic Control > Reset SMU**.

Deleting the Rectifiers Failing in Communication

After you remove one or more rectifiers, the SMU generates a communication failure alarm. If you confirm that the rectifiers will not be reinstalled, manually delete the information about the removed rectifiers.

On the Site app: Choose **Home > Digital Power > Device > Rectifier Group > Control > Basic Control > Delete Rectifier Failed in Communication**.

Collecting Rectifier Fault Information

If you cannot rectify the faults based on the alarm handling suggestions, you can collect the fault information and provide the information to Huawei technical support for fault diagnosis.

On the Site app: Choose **Home > Digital Power > Device > Rectifier Group > Control > Fault Information Collection Control > Collect Fault Info**.

Switching Between Boost and Float Charge for Lead-Acid Batteries

- You can manually switch between boost charge and float charge when the system works in manual control mode.
- Batteries keep in boost charge state after boost charge is manually started. When the float charge conditions are met (for example, time for boost charge expires), the batteries automatically switch to the float charge state.

On the Site app:

To set the control mode, choose **Home > Digital Power > Control > Basic Control**.

To set the charge control, choose **Home > Digital Power > Device > Battery Group > Control > Basic Control > Charge Control**

Exporting Historical Alarms and Battery Test Records

You can export historical alarms and battery test records on the app to quickly collect information and locate system faults.

On the Site app: **Maintenance > Log Export**

Exporting Fault Logs

You can export fault logs to quickly collect information and locate system faults.

On the Site app: **Maintenance > Log Export**

Exporting E-label Information

You can view and export e-label information about the power subrack, monitoring board, and rectifier on the app.

On the Site app: **Maintenance > E-Label**

A FAQ

A.1 How Do I Prepare the WebUI Operating Environment

Before logging in to the WebUI, you need to prepare the WebUI operating environment to connect to the monitoring unit.

Operating Environment

Supported operating system: Windows 10 or later

Browser: Internet Explorer 8.0 or later, FireFox 13 or later, and Chrome 20 or later

NOTE

Internet Explorer is used as an example to illustrate all WebUI operations mentioned in this document.

Setting a LAN

NOTICE

If the monitoring unit is connected to a LAN and a proxy server has been selected, cancel the proxy server settings.

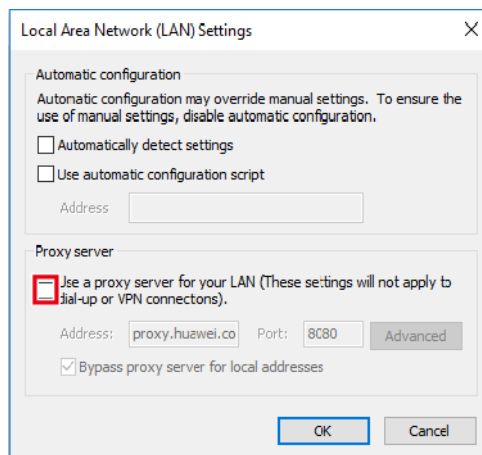
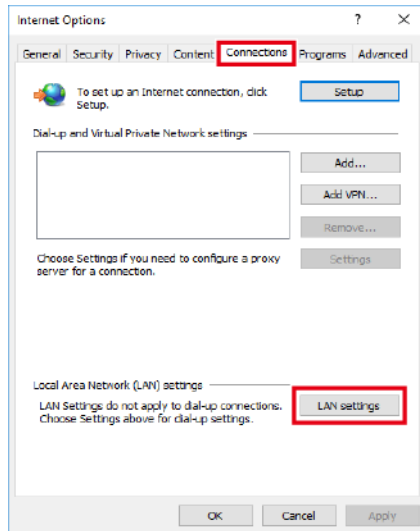
If the monitoring unit is connected to the Internet but your computer is connected to a LAN, do not cancel the proxy server settings. Otherwise, you cannot access the SMU.

To cancel proxy server settings, perform the following steps:

1. Open Internet Explorer.
2. Choose **Tools > Internet Options**.
3. Choose **Connections** tab, click **LAN Settings**.

4. Clear **Use a proxy server for your LAN**.

Figure A-1 Canceling proxy server settings



5. Click **OK**.

Setting Internet Explorer Security

NOTICE

Set Internet Explorer security before you perform the following operations:

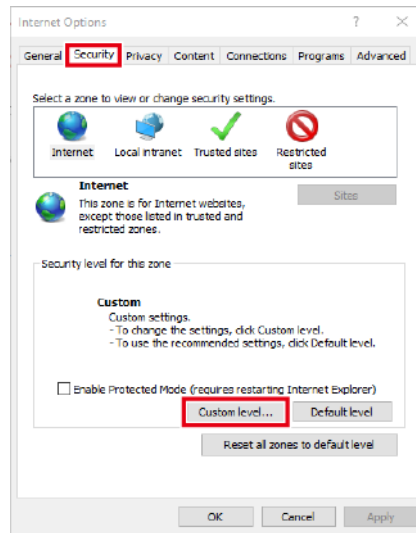
- Export historical logs, historical data, statistics, and battery test records.
- Upload system configuration files.
- Download system configuration files.
- Upgrade software.

To set Internet Explorer security, perform the following steps:

1. Open Internet Explorer.

2. Choose **Tools > Internet Options**.
3. Choose **Security** Tab.
4. Click **Internet** and click **Custom level**. After you specify Internet security settings, click **Local intranet** and click **Custom level**.

Figure A-2 Internet Explorer security



5. Specify the security settings.
Enable the following:
 - Initialize and script ActiveX controls not marked as safe for scripting
 - Allow previously unused ActiveX controls to run without prompt
 - Include local directory path when uploading files to a server

Figure A-3 Internet Explorer security setting 1

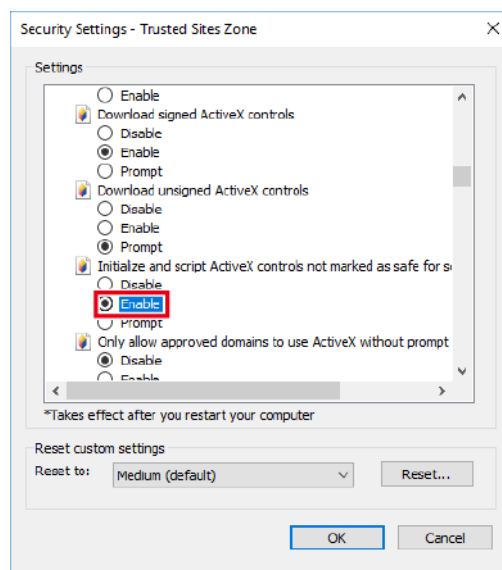


Figure A-4 Internet Explorer security setting 2

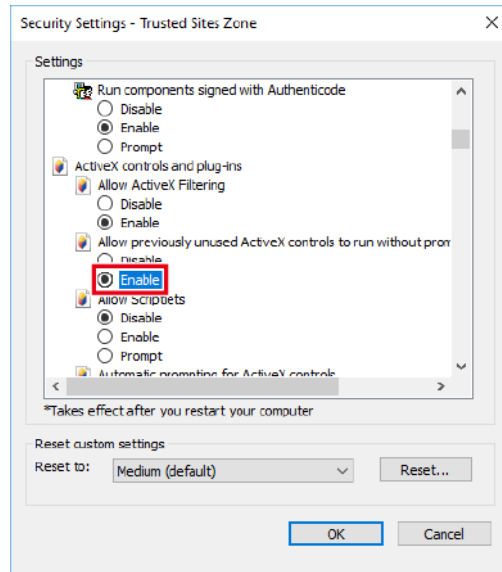
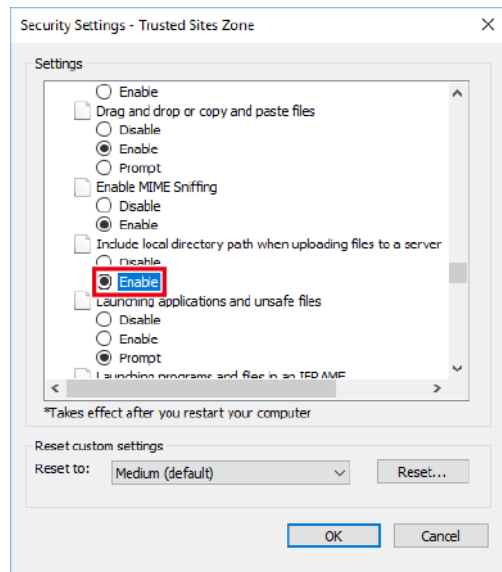
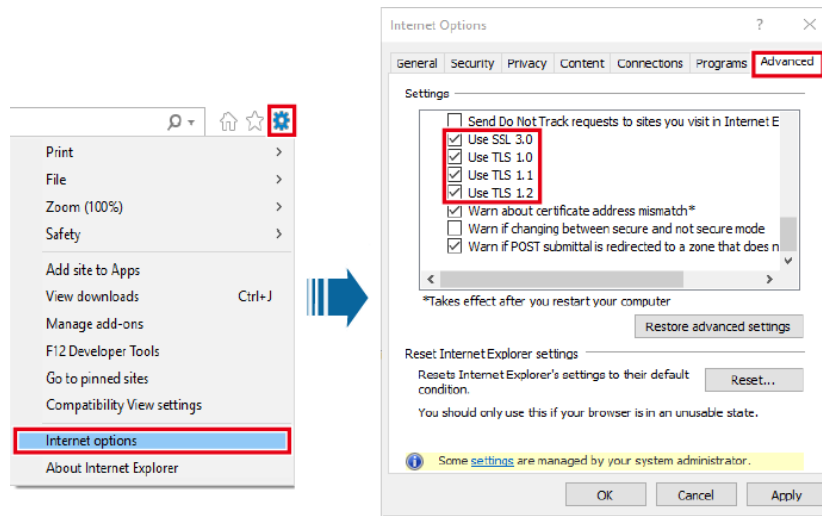


Figure A-5 Internet Explorer security setting 3



6. Click **OK**.
7. Click the **Advanced** tab, and select **Use SSL 3.0, Use TLS 1.0, Use TLS 1.1,** and **Use TLS 1.2**.

Figure A-6 Internet Explorer security setting 5



8. Click **OK**.

B Acronyms and Abbreviations

C	
CAN	Control area network
I	
IP	Internet Protocol
S	
SNMP	Simple Network Management Protocol
SMU	Site monitoring unit
U	
UI	User interface