Huawei DCF Certification Training

HCIP-DCF-Deployment

Huawei UPS5000 Lab Guide

ISSUE:2.0

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

 and other Huawei trademarks are trademarks 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 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 Technologies Co., Ltd.

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

Website: http://e.huawei.com

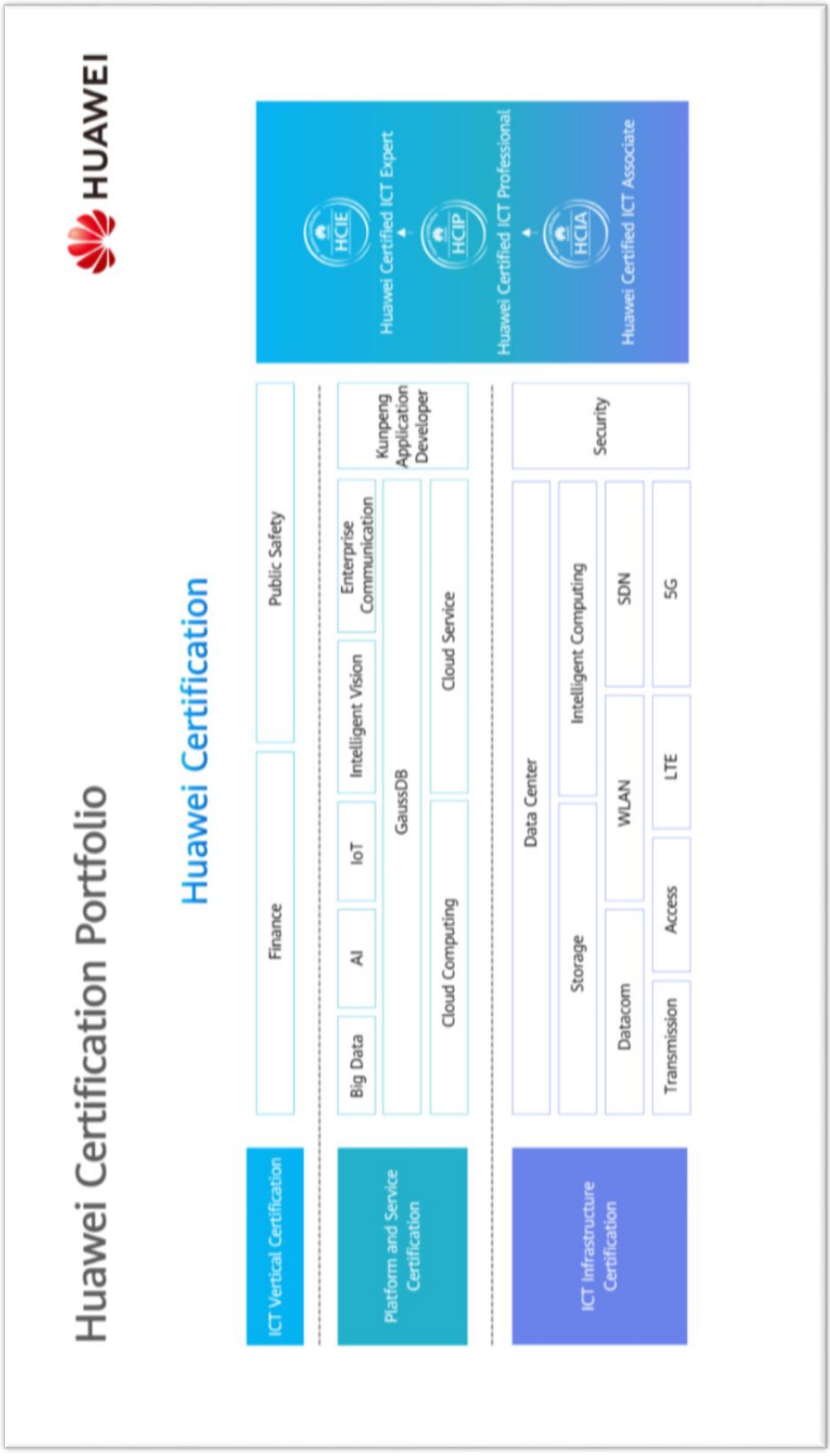
Huawei Certificate System

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, Platform and Service certification and ICT vertical certification, and grants Huawei certification the only all-range technical certification in the industry.

Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE).

HCIP-Data Center Facility Deployment V2.0 is aim to train and certify senior engineers who need to perform deployment and system commissioning for Huawei data center infrastructure products.

After passing the HCIP-Data Center Facility Deployment V2.0 certification, you will be familiar with Huawei data center infrastructure products and have the deployment and commissioning capabilities of Huawei data center infrastructure products. The full series of products include Huawei modular data center Fusion Module series products, Huawei UPS and precision PDC series products, Huawei data center energy storage products, Huawei data center smart cooling products, and Huawei data center DCIM system products.


HUAWEI
Huawei Certification Portfolio
Huawei Certification
ICT Vertical Certification
Finance
Public Safety
Platform and Service Certification
Big Data
AI
IoT
Intelligent Vision
Enterprise Communication
Kunpeng Application Developer
GaussDB
Cloud Computing
Cloud Service
ICT Infrastructure Certification
Data Center
Storage
Intelligent Computing
Security
Datacom
WLAN
SDN
Transmission
Access
LTE
5G
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Introduction

This document is intended for trainees who are preparing to take the HCIP-DCF-Deployment exam or readers who want to understand the features, parameter settings, and operations of Huawei UPS5000 series products.

Description

This document consists of three experiments. It describes the parameter settings and configurations and operations of a single UPS and parallel UPSs.

- Exercise 1: Understand the UPS5000 hardware architecture. This exercise helps you familiarize yourself with the UPS5000 hardware components and functions of each module.
- Experiment 2 describes how to set parameters for a single UPS5000, including setting output parameters, battery parameters, power-on/shutdown, and operating mode switching.
- Experiment 3 describes how to set parallel system parameters, start and shut down the parallel system, isolate a UPS5000 from the parallel system, and add a UPS5000 to the parallel system. This exercise helps readers learn how to set parallel system parameters.

Reader's Knowledge Background

This course is an intermediate course for Huawei certification. To better master the contents of this course, the readers of this course must meet the following requirements:

- Have basic knowledge about power distribution, UPS, and batteries.

Content

1 Experiment Tasks

1.1 Task List

Table 1-1 Task List

Task Name		Dration	Completed
UPS5000 Hardware Architecture	UPS5000-E product structure	30min	☐Yes ☐No
Operations on a UPS5000	Powering On and Starting the UPS	70min	☐Yes ☐No
	Shutting Down and Powering Off the UPS		☐Yes ☐No
	Starting the UPS in Battery Mode		☐Yes ☐No
	Transferring to Bypass Mode		☐Yes ☐No
	Transfer to maintenance bypass		☐Yes ☐No
	Transferring to Maintenance Bypass Mode		☐Yes ☐No
	Transferring from Maintenance Bypass Mode to Normal Mode		☐Yes ☐No
	Performing EPO		☐Yes ☐No
	Clearing the EPO State		☐Yes ☐No
	Setting ECO Mode		☐Yes ☐No
	Setting the BSC Mode (Bus Synchronization Controller)		☐Yes ☐No
	Web client connection		☐Yes ☐No
UPS5000 Parallel Operations	Starting the parallel system.	80min	☐Yes ☐No
	Powering off and shutting down the parallel system		☐Yes ☐No
	Emergency shutdown (EPO)		☐Yes ☐No

	Isolating Single UPS Operations in the Parallel System		☐Yes ☐No
	Restoring the Isolated UPS in the Parallel System		☐Yes ☐No

2 UPS5000 Hardware Architecture

2.1 Introduction to the Experiment

2.1.1 About this Lab

This exercise describes the UPS5000 architecture and the functions of each module.

2.1.2 Objectives

After completing this lab, you will be able to:

- Understand the structure of the UPS5000-E.
- Master the functions of each component.

2.2 Experiment Tasks

2.2.1 Task 1: Understand the UPS5000-E product structure.

Step 1 The following figure shows the UPS5000-E structure.

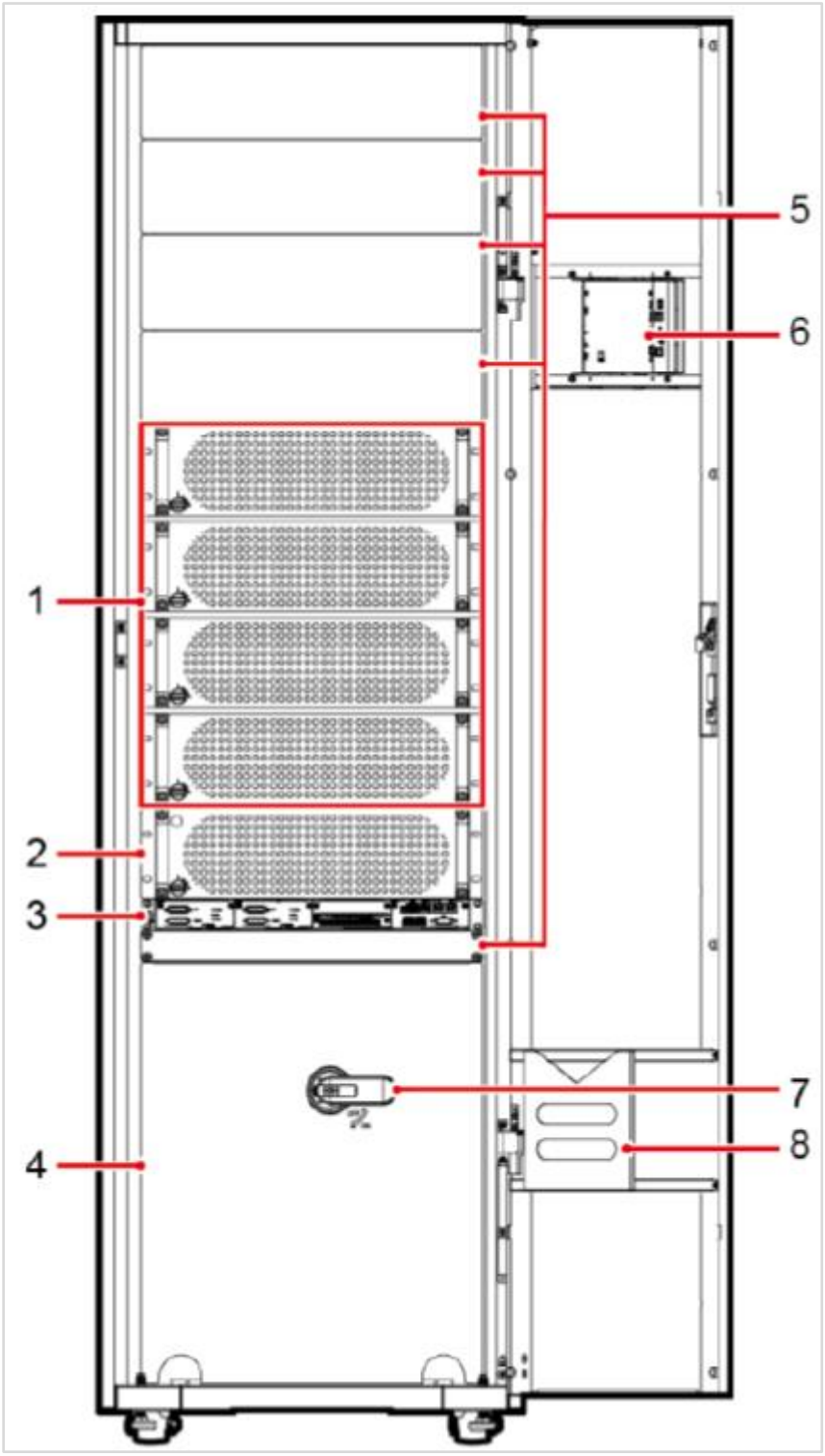


Figure 2-1 Product Structure

(1) Power modules (2) Bypass module (3) Control module

(4) Power distribution subrack cover (5) Filler panel (6) MDU

(7) Maintenance bypass switch (8)Folder

Step 2 The following figure shows the structure of the power module.

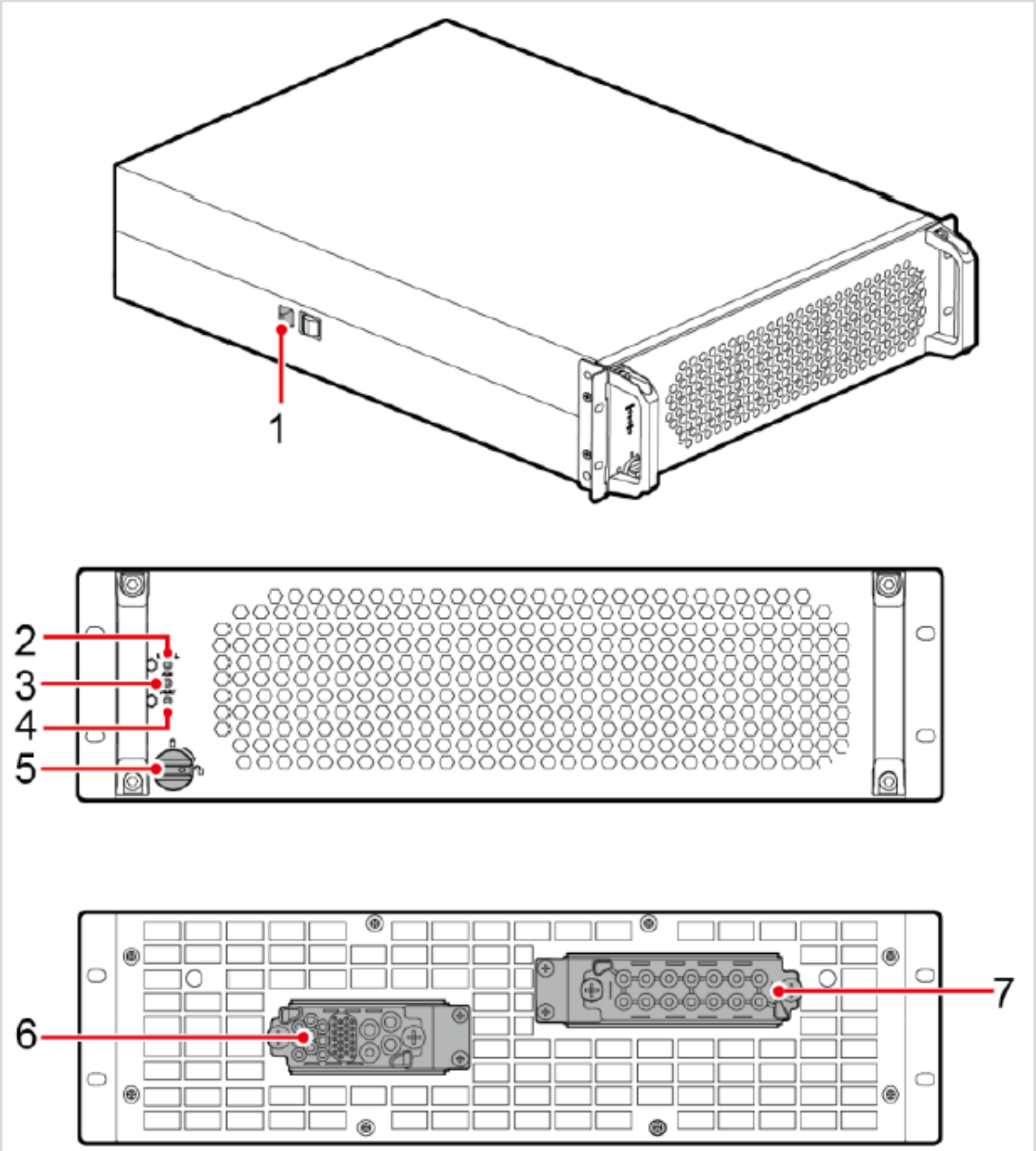


Figure 2-2 Power module

1. Limit lock	2. Running indicator	3. Alarm indicator	4. Fault indicator
5. Ready switch	6. Output port	7. Input port	

Power Module Functions

The main power module consists of a PFC rectifier and an inverter. It transmits mains and battery inputs to AC/DC.

After DC/DC conversion, the bus voltage is stabilized and then converted to sine wave output through the inverter (DC/AC).

Table 2-1 Power module specifications

Item	Parameter
Dimensions:	130 mm (H) x 442 mm (W) x 620 mm (D)
weighted	32 kg
Rated output capacity	50kVA/50kW
power density	23W/inch3

Step 3 The following figure shows the structure of the bypass module.

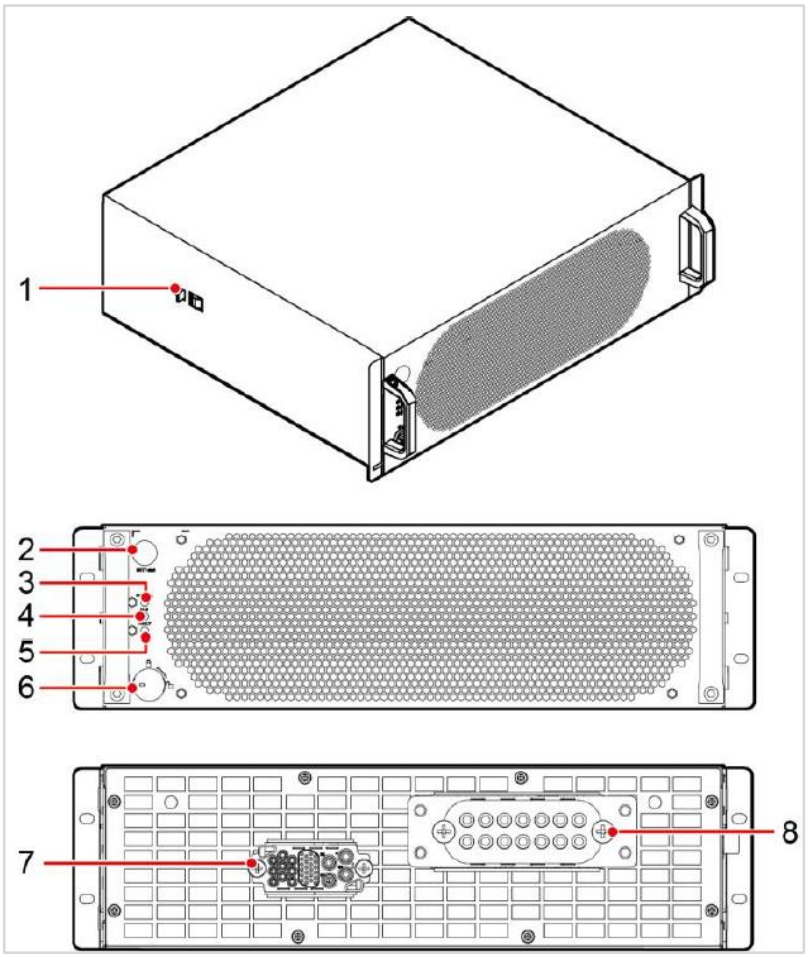


Figure 2-3 Bypass module

(1) Limit lock (2) Cold start button (3) Working indicator (4) Alarm indicator

(5) Fault indicator (6) Ready switch (7) Signal port (8) Input and output ports

Functions of the bypass module

Bypass power supply is used in the following scenarios:

- The UPS works in ECO mode and the bypass voltage is within the specified range.
- The power module is overloaded and the bypass mode is used.
- If both the active and standby ECMs are abnormal, the bypass takes over power supply.
- The UPS transfers to bypass mode if the UPS is abnormal.
- The UPS transfers to bypass mode manually.

Table 2-2 Bypass Module Specifications

Item	Parameter
Dimensions:	130 mm (H) x 420 mm (W) x 500 mm (D)
weighted	200kVA:19kg

Step 4 Refer to the following figure to understand the product structure of the control module.

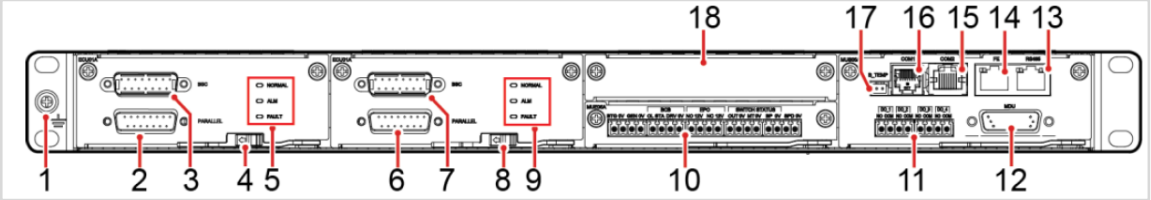


Figure 2-4 Control module

1. Ground terminal	2. Parallel port 1	3. BSC port 1	4. EMC1 in position switch
5. ECM1 indicator	6. Parallel port 2	7. BSC port 2	8. EMC2 position switch
9. ECM2 indicator	10. Dry contact	11. Dry contact port	12. MDU port
13. RS485 port	14. FE port	15. COM2 port	16. COM1 port
17. Battery temperature sensor port		18. Optional card subrack cover	

In a standard configuration, the control module consists of two ECMs, one dry contact card, and one monitoring interface card (from left to right). The four cards are hot swappable. One subrack is reserved above the dry contact card. A backfeed protection card or dry contact extended card can be inserted into this subrack.

Step 5 See the following figure to understand the product structure of the ECM.

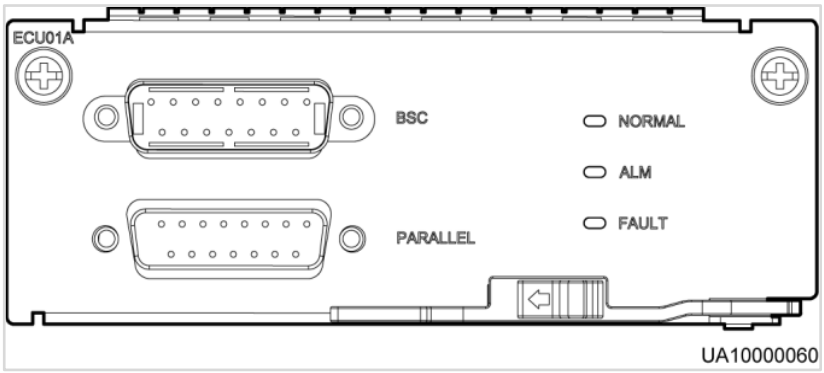


Figure 2-5 ECM

The control module consists of two ECMs in active/standby mode. Each ECM has two external ports. The lower part is the parallel port and the upper part is the BSC port. In a parallel system, connect the parallel ports on the ECMs in each cabinet in a ring topology using parallel cables. The BSC is used in a dual-bus system to process communication information between two UPS systems. It is hot-swappable.

Table 2-3 ECM Function

Panel Silkscreen	Description
PARALLEL	Inter-cabinet parallel signal port. When multiple UPSs are connected in parallel, connect the parallel ports on each UPS by using parallel control cables. N parallel control cables are required to connect N UPSs to ensure that each UPS has at least two parallel control cables, improving parallel reliability.
BSC	The BSC is used in a dual-bus system. It synchronizes the output frequency and phase of each system in the dual-bus system to ensure that the two buses can switch between each other.

Table 2-4 Indicator Description

Panel Silkscreen	color	Status	Explanation
NORMAL	green	Steady on	This ECM is the active ECM.
		Blinking at 0.5 Hz	The ECM is the standby ECM and is in the ready state.
		Off	The ECM is not ready or the CPLD of the ECM is being upgraded.
		Blinking at 4 Hz	The DSP of the ECM is being upgraded or not configured.
ALM	yellow	Steady on	A minor alarm is generated on the ECM, but the ECM does not need to be replaced.

		Off	No minor alarm is generated on the ECM or the DSP of the ECM is being upgraded.

Step 6 The following figure shows the structure of the dry contact card.

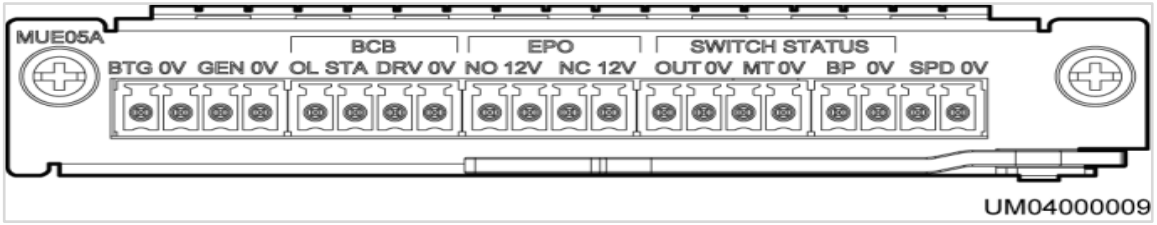


Figure 2-6 Dry contact card

Functions of the dry contact card

The dry contact card allows the UPS to detect and manage the switch status of the battery system (including the external battery switch) and implement remote emergency power-off (EPO).

Table 2-5 Ports on the dry contact card

Port Silkscreen	Signal Description	Status Description	Initial state
BTG	Battery grounding fault detection port	Closed: The battery is grounded incorrectly. Open: No battery grounding fault	Disconnected
0V	Signal ground		
GEN	D.G. mode detection port	Closed: D.G. mode Open: non-DG mode	Disconnected
0V	Signal ground		
BCB_OL	Whether the BCB is connected to the detection signal port	Grounding: connected to the BCB Floated: The BCB is not connected.	earthing
BCB_STA	Port for monitoring the battery circuit breaker status	Closed: The battery circuit breaker is closed. Off: battery circuit breaker	Disconnected
BCB_DRV	The battery circuit breaker tripped. When the voltage is +12 V, the drive tripped.	0 V: The BCB is not tripped. 12 V: The BCB is not driven to trip.	0V

BCB_0V	Signal ground		
EPO_NO	EPO port, NO and EPO_12V normally open signals EPO triggered when closed	Close the EPO to trigger an EPO.	Disconnected
EPO_12V	+12V		
EPO_NC	EPO signal port. NC and EPO_12V are normally closed. EPO is triggered when the EPO_12V signal pair is disconnected.	Disconnect the EPO to trigger an EPO.	closed
EPO_12V	+12V		
SWITCH STATUS_OUT	UPS output switch status monitoring port	Closed: The UPS output switch is ON. Off: The UPS output circuit breaker is OFF.	closed
SWITCH STATUS_0V	Signal ground		
SWITCH STATUS_MT	Maintenance switch status monitoring interface	Open: The maintenance switch is ON. On: The maintenance switch is off.	Disconnected
SWITCH STATUS_0V	Signal ground		
SWITCH STATUS_BP	Bypass input switch status monitoring port	Closed: The bypass input switch is ON. Open: The bypass input switch is off.	closed
SWITCH STATUS_0V	Signal ground		
SPD	Input AC SPD status monitoring port	Closed: The input AC SPD is working properly. Open: The input AC SPD fails.	closed
0V	Signal ground		

- The dry contact interface card takes effect only after it is set on the monitoring system. Set the unused dry contact signal to the unused status.

- Set the EPO port to NO or NC as required.
- When multiple UPSs are paralleled, all dry contact signals to be used need to connect to each UPS.
- Single cables require dual-insulated twisted cables. If the length of a power cable is within 25–50 m, its cross-sectional area must be 0.5 mm2 to 1.5 mm2

Step 7 The following figure shows the structure of the monitoring interface card.

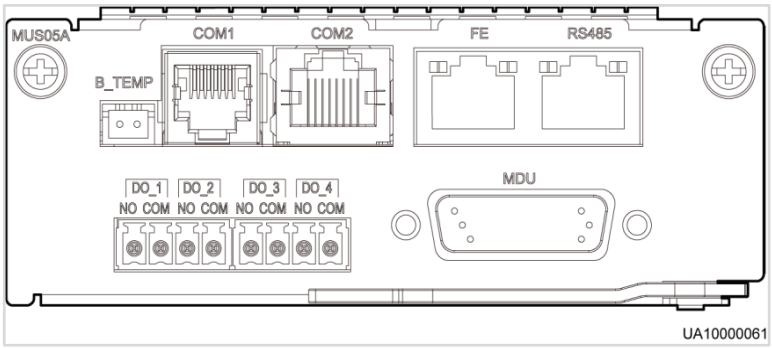


Figure 2-7 Monitoring interface card

The monitoring interface card provides external ports as well as monitoring and control functions for the MDU. The ports include the ambient temperature and humidity sensor port, iBattery port, FE port, battery temperature monitoring port, and network management port.

The MDU monitors the UPS, allows users to set parameters, delivers commands, reports information, and displays the UPS key information and parameters on the LCD.

Table 2-6 Monitoring interface card interface

Port	Panel Silkscreen	Signal Description
DO_1	NO	DO_1 indicates the alarm output. The default value is critical. You can set this parameter to Minor, Bypass, Battery, or Battery Low Voltage.
	COM	
DO_2	NO	DO_2 indicates the alarm output. It is a minor alarm by default and can be set to Critical, Bypass, Battery, or Battery Low Voltage.
	COM	
DO_3	NO	DO_3 indicates the alarm output. By default, the bypass mode is used. The options are Critical, Minor, Battery, and Battery Low Voltage.
	COM	
DO_4	NO	DO_4 indicates the alarm output. The default value is battery power supply. The value can be Critical, Minor, Bypass, or Battery Low Voltage.
	COM	
DB26	MDU	Provides FE, RS485, I2C, and CAN signals.
Battery	B_TEMP	Connects to the indoor battery temperature sensor.

temperature		
Southbound communication port 1	COM1	Connects to the ambient temperature and humidity sensor, 2-wire system.
Southbound communication port 2	COM2	Connects to southbound devices, such as iBAT 2.0.
Network port	FE	Network port, which is connected to the network port of the PC.
Northbound communication port	RS485	Connects to the northbound NMS device or third-party NMS device, two-wire.

- The signal cable must be a double-insulated twisted cable. If the cable length ranges from 25 m to 50 m, the cross-sectional area must range from 0.5 mm2 to 1.5 mm2.
- RS485 cables and FE cables must be shielded cables.

Step 8 The following figure shows the LCD panel structure.

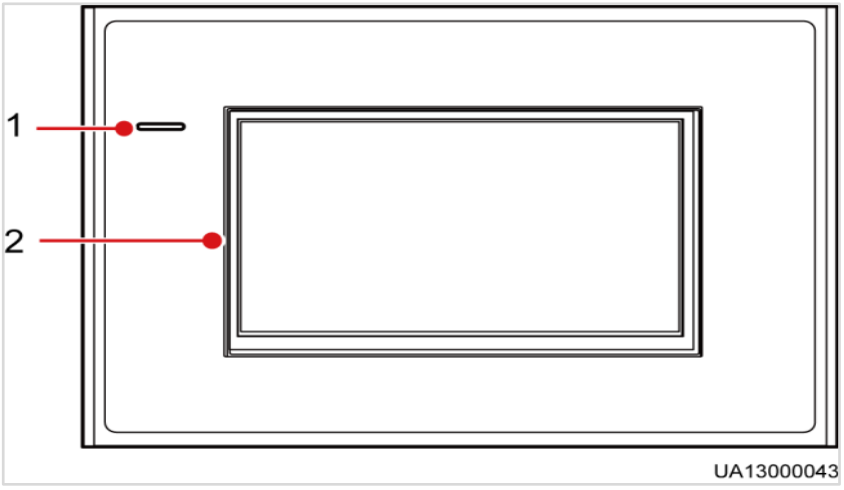


Figure 2-8 LCD

(1) Status indicator (2) LCD touchscreen

The monitoring screen uses an industrial resistive screen and needs to be pressed slightly. Touch with your fingernails. It is recommended that you touch it with a small force area, high pressure, high accuracy, and quick response.

Table 2-7 Indicator Description

Status	Indicator color	Meaning
On	red	A critical alarm is generated on the UPS panel and the buzzer buzzes.

	yellow	A minor alarm is generated on the UPS panel, and the buzzer buzzes intermittently (2 Hz).
	green	The UPS is running properly.
off	/	The UPS panel is powered off.

Step 9 See the following figure to identify wiring terminals.

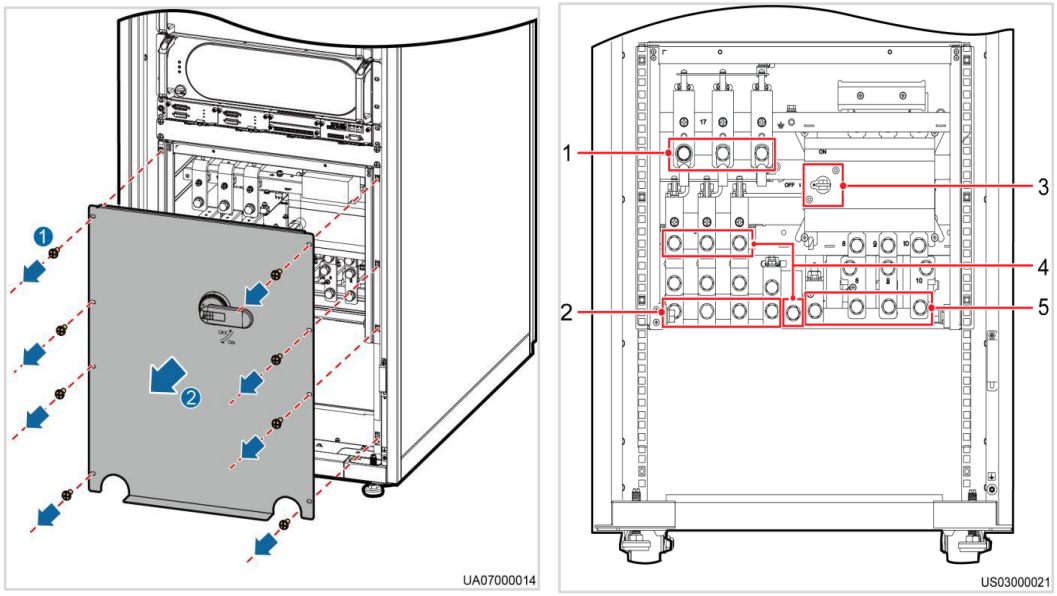


Figure 2-9 Wiring terminal

(1) Battery input terminals (+, N, and –)

(2) Mains input (1L1, 1L3, and N)

(3) Maintenance bypass switch

(4) Bypass input (2L1, 2L3, and N)

(5) Output terminals (U, V, W, and N)

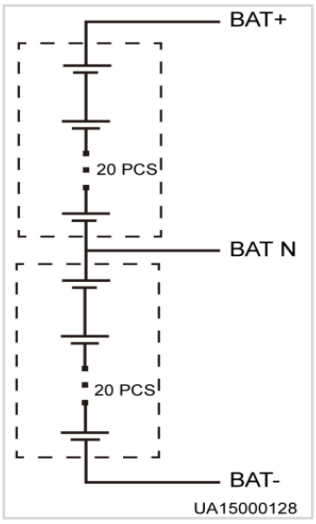


Figure 2-10 Battery cable connection

- **Single mains input**: You do not need to remove the copper bar between the mains input and bypass input wiring terminals, and do not need to connect bypass input cables. If the mains and bypass input power sources are different, remove the copper bars between the mains and bypass input terminals, and connect the mains and bypass input power cables respectively.
- The battery N cable is led out from the connection point between the positive and negative battery strings. Assume that there are 40 battery strings. The positive and negative battery strings are evenly distributed. Each battery string contains 20 batteries. The battery N cable is led out from the connection point between the positive and negative batteries.

3 Operations on a single UPS5000

3.1 Introduction to the Experiment

3.1.1 About this Lab

This experiment uses a single UPS5000 to master the operation procedure and parameter settings.

3.1.2 Objective

- Have a good command of UPS5000 parameter settings.
- Master the operations such as powering on and powering off the UPS5000.

3.2 Experiment Tasks

3.2.1 Task 1: Powering On and Starting the UPS

Before each power-on, perform post-installation check items.

Before powering on the UPS, ensure that all ready switches on the UPS bypass module and power module are turned on. Before powering on the UPS, ensure that all input and output switches are OFF.

Step 1 Before powering on the UPS, measure the voltage and frequency of the input switches (mains and bypass input switches) on the UPS input PDC or the external input power distribution switch. Voltage range: 138–485 V Frequency range: 40–70 Hz.

Step 2 Power on the UPS in full configuration and simple configuration.

For a full configuration UPS: Built-in mains input switch, built-in bypass input switch, built-in output switch, and built-in maintenance bypass switch. Perform the following operations in sequence:

- Switch on the external bypass input power distribution switch and external mains input power distribution switch.
- Switch on the bypass input switch inside the UPS.
- Switch on the UPS internal output switch.
- Switch on the mains input switch inside the UPS.

- Switch on the input SPD circuit breaker (if any).

For a simple configuration UPS: Only a built-in maintenance bypass switch, perform the following operations in sequence:

- Switch on the external bypass input power distribution switch and external mains input power distribution switch.
- Switch on the input SPD circuit breaker (if any).

Step 3 After the SMU is started, you can set parameters such as the language, time, date, network, and system on the quick setting wizard after the SMU is powered on for the first time. When the SMU is powered on for the second time, the system automatically sets the language, time, date, network, and system parameters. If these parameters have been set, the default settings are used.

- Language setting: You can set multiple languages such as Chinese and English on the GUI.
- Click **Next**. The Time and Date Settings page is displayed. You can set the date format, for example, Year/Month/Day.
- Network parameter settings, including the IP address allocation mode, IP address, subnet mask, and gateway.
- After network parameters are set, connect the UPS to the network using a network cable for remote management and control. If remote management is not required, you are advised to use the default value.
- Set system parameters, including single UPS and parallel UPS (default), voltage level, output frequency, battery capacity, and number of batteries.
- System parameter settings affect the normal running of the UPS. Exercise caution when setting system parameters.
- Ensure that the UPS is running in single-node system or multiple-node system mode. Otherwise, the UPS cannot run properly.
- Output Voltage Level indicates the line voltage. Set this parameter based on the site requirements.
- The output frequency must be correct. Otherwise, the load may be affected and cannot work properly.
- Battery type: lead-acid battery and lithium battery. If lithium battery is selected, battery parameters do not need to be set on the UPS. The lithium battery parameters are set by default. If lead-acid batteries are used, set the following parameters:
- Check the battery capacity repeatedly and set it correctly. Otherwise, the charging power will be affected. When multiple UPSs share a battery string, the battery capacity of each UPS is the total capacity of all connected battery strings. If battery strings are not shared, the UPS battery capacity is the battery capacity of a single UPS.
- If the charging power is too high or too low, the battery life may be shortened. In serious cases, the battery may be damaged for a short time.

- The number of cells refers to the number of cells in a single battery string connected to the UPS by using 2 V batteries as a single cell. For example, if 150 Ah/12 V batteries are connected in series, and two battery strings are connected in parallel to the UPS, the number of batteries is 216 (36 x 6), and the battery capacity is 300 Ah (150 Ah + 150 Ah). 300 Ah/2 V batteries are connected in series. Two battery strings are connected in parallel to the UPS. The number of batteries is 192 x 1 = 192, and the battery capacity is 300 Ah + 300 Ah = 600 Ah. This parameter affects the charging voltage and discharging time. If this parameter is set incorrectly, the battery charging voltage will be high or low, greatly shortening the battery lifespan. In addition, the UPS may be shut down in advance during discharging, which may cause data backup failures.

Step 4 After the quick setting is complete, if no alarm is generated on the monitoring page, go to the next step. If an alarm is generated on the monitoring page, clear all the alarms.

- After the quick settings are complete, choose **System Info > Settings > Advanced Parameters**. Check whether the settings of **Capacity, Power Module Capacity**, **Basic Modules** in Rack, and **Redundant Modules** in Rack are consistent with the actual situation.
- If dry contact signals are connected to the system, choose Sys**tem Info > Settings > Dry Contacts** and ensure that the dry contact settings corresponding to the dry contact signals are enabled. For dry contacts that are not connected to the system, set this parameter to **Disable**.

Step 5 Check that the bypass input is normal and the system works in bypass mode. View the system running diagram on the LCD to check whether the system works in bypass mode.

Step 6 Start the inverter.

- Method 1

On the main menu of the LCD, choose **Common Functions > Inv .ON**. In the displayed login window, enter the user name and password, and click . In the displayed dialog box, click **Yes**.

- Method 2

On the main menu of the LCD, choose **System Info**. On the **Maintenance** screen, click . If the current user has not logged in, the login screen is displayed. Enter the user name and password, and click to log in. Click **Inv .ON**.. In the displayed dialog box, click **Yes**.

Step 7 After the inverter starts, the UPS transfers to normal mode. The Bypass alarm on the MDU disappears. Check whether the UPS transfers to normal mode by viewing the system running diagram.

During commissioning, you can check the UPS three-phase output voltage and frequency based on real-time data on the monitoring screen. Use a multimeter to check whether the three-phase output voltage and frequency of the output switch on the output PDC or external output power distribution switch are normal. (Output voltage: Three-phase

output voltage = Output voltage fine-tuning ±1 V) Three-phase output frequency = ±0.125 Hz)

If the tested voltage is incorrect, choose Maintenance > Calibration, expand Module, enter the measured voltage in the Actual Measured Value column of Phase A Output Voltage, Phase B Output Voltage, and Phase C Output Voltage, and click Submit. Press the button to adjust the voltage.

Step 8 Use a multimeter to measure the voltage at the battery switch. If there are multiple battery strings, use a multimeter to measure the voltage at the battery switch and then the voltage at the general battery switch. Switch on the battery string input switch. If there are multiple battery strings, Switch on the switch for each battery string, Switch on the general switch between the battery string and the UPS.

- After the battery string input switch is turned on, the No Battery alarm is cleared on the MDU.
- Use a multimeter to measure the voltage of each battery string. Measure the positive and N poles of the positive battery string, and measure the negative and N poles of the negative battery string. If the voltage of the positive battery string is greater than a certain value (1.9 x 6 x Number of batteries) and the voltage of the negative battery string is less than a certain value (–1.9 x 6 x Number of batteries), the battery string is properly connected.

Step 9 Switch on the external output power distribution switch or external output power distribution switch to supply power to loads.

----End

3.2.2 Task 2: Powering Off and Shutting Down the UPS

If the bypass is normal, the UPS transfers to bypass mode after the inverter shuts down. If the bypass is abnormal, the inverter shuts down and the system enters no output mode, and the system output is disconnected. Before shutting down the load, ensure that the load is shut down and can withstand power-off at any time.

Step 1 Shut down the inverter.

- Method 1

On the main menu of the LCD, choose Common **Functions > Inv. Off**. In the displayed login window, enter the user name and password, and click .In the displayed dialog box, click **Yes**.

- Method 2

On the main menu of the LCD, choose **System Info**. On the **Maintenance** screen, click . If the current user has not logged in, the login screen is displayed. Enter the user name and password, and click to log in. Click **Inv. Off** In the displayed dialog box, click **Yes**.

Step 2 The inverter shuts down. If the bypass is normal, the UPS enters bypass mode after the inverter shuts down. If the bypass is abnormal, the UPS enters no output mode after the inverter shuts down, causing loads to be disconnected.

- After the inverter is shut down, a bypass alarm is displayed on the MDU.

Step 3 After the inverter shuts down, switch off the output switch of the UPS output PDC or the external output power distribution switch.

Step 4 Switch off the battery string switch. If there are multiple battery strings, switch off the general switch between the battery string and the UPS, and then switch off the switch for each battery string.

Step 5 Switch off the external input power distribution switch and the UPS internal switch. Two models are available: full configuration and simple configuration.

For a full configuration UPS: Built-in mains input switch, built-in bypass input switch, built-in output switch, and built-in maintenance bypass switch, perform the following operations in sequence:

- Switch off the mains input switch and bypass input switch inside the UPS.
- Switch off the built-in output switch of the UPS.
- Switch off the external mains input power distribution switch and external bypass input power distribution switch.
- Switch off the input SPD switch on the UPS input PDC (if any).

For a simple configuration UPS: Only built-in maintenance bypass switch), perform the following operations in sequence:

- Switch off the external mains input power distribution switch and external bypass input power distribution switch.
- Switch off the input SPD switch on the UPS input PDC (if any).

----End

3.2.3 Task 3: Starting the UPS in Battery Mode

Step 1 Check that batteries are properly connected. Use a multimeter to test that the voltage of the positive battery string is greater than a certain value (+1.9 x 6 x Number of batteries), and the voltage of the negative battery string is less than a certain value (–1.9 x 6 x Number of batteries).

Step 2 Switch off the mains and bypass input switches. If there is no mains or bypass input, Switch on the battery switch. If there are multiple battery strings, Switch on the switch for each battery string and then the general switch between the battery string and the UPS.

Step 3 Use a multimeter to measure the voltage of the positive and negative battery strings connected to the UPS battery input terminal. If the voltage of the positive battery string is greater than a certain value (+1.9 x 6 x Number of batteries) and the voltage of the negative battery string is less than a certain value (–1.9 x 6 x Number of batteries), batteries are connected properly.

Step 4 Press the battery cold start button on the device. The system automatically enters the battery cold start state. The LCD displays the Huawei logo and initialization progress bar.

Step 5 After the LCD is initialized, start the inverter.

----End

3.2.4 Task 4: Transferring to Bypass Mode

Before shutting down the inverter, ensure that the bypass is normal. If the bypass is abnormal, the system has no output after you manually shut down the inverter, causing loads to be disconnected.

Step 1 You can shut down the inverter on the LCD or WebUI. The UPS transfers to bypass mode.

----End

3.2.5 Task 5: Transferring to the Maintenance Bypass Mode

You are advised to lock the maintenance bypass switch with a diameter of 5–10 mm.

Strictly follow the following steps to transfer the UPS to maintenance bypass mode. Otherwise, loads may be disconnected.

In maintenance bypass mode, loads are powered by the mains through the maintenance bypass. If the mains is abnormal, loads may be disconnected.

Step 1 Manually transfer the UPS to bypass mode.

Step 2 Switch on the maintenance bypass switch.

If the maintenance bypass circuit breaker is locked, unlock it first. Switch on the UPS maintenance bypass switch in the specified direction. The UPS transfers to maintenance bypass mode. The maintenance bypass switch is turned off by default. The handle of the 200 kVA system is horizontally rightward. Hold the handle and rotate it 90 degrees clockwise until it is vertical to the ground. The maintenance bypass switch is turned on. In addition, the maintenance circuit breaker closed alarm is displayed in the alarm list.

----End

3.2.6 Task 6: Transferring from Maintenance Bypass Mode to Normal Mode

Before restoring the maintenance bypass mode to normal mode, ensure that the bypass input is normal.

Step 1 Switch off the maintenance bypass switch.

When the UPS5000-E-200 kVA is powered on, the handle of the maintenance bypass switch is vertically downwards, and the operation faces the cabinet. Hold the handle and rotate it 90 degrees counterclockwise until the handle is horizontally rightward. Switch off the maintenance bypass switch. In addition, the maintenance circuit breaker closed alarm is cleared on the LCD. You can check whether the UPS works in bypass mode by viewing the system running diagram on the LCD or WebUI.

Step 2 Start the inverter.

----End

3.2.7 Task 7: Performing EPO

After you press the EPO button, the UPS has no output and loads are disconnected.

When the system is in maintenance bypass mode, the UPS still has output after you press the EPO button.

Step 1 Press the external EPO switch on the control module or remove the 4-pin terminal from the EPO port on the dry contact card. The UPS enters the EPO state. The alarm is displayed on the LCD and WebUI.

----End

Operation Result

3.2.8 Task 8: Clearing the EPO State

Step 1 Clears the EPO state of the system. Ensure that the external EPO switch connected to the dry contact card is not in the EPO state or connect the 4-pin terminal to the EPO port on the dry contact card.

Step 2 Clears the emergency shutdown alarm.

On the main menu of the LCD, choose System Info. On the **System Info** page, click . The **Alarms** page is displayed. If the current user has not logged in, the login window is displayed. Enter the user name and password, and click to log in. Click **Clear Faults.** In the displayed dialog box, click Yes to clear the EPO alarm.

Step 3 Check whether the EPO alarm is cleared. If the bypass input is normal, the UPS transfers to bypass mode.

On the main menu of the LCD, choose **System Info.** On the System Info page, click . The Alarms page is displayed. Click **Current Alarms** and check whether the critical alarm is cleared.

Step 4 Step 4: Start the inverter.

----End

3.2.9 Task 9: Setting ECO Mode

By default, the system works in non-ECO mode. To enable the system to work in economical mode, set the working mode to ECO mode.

In ECO mode, the bypass takes precedence over the inverter. When the bypass fails, the system switches to the inverter. The interruption duration in typical working conditions is less than 2 ms and that in bad working conditions is less than 10 ms.

Both the single and parallel systems support the ECO mode, which achieves higher efficiency.

The bypass input is unstable or sensitive to load changes, which may cause frequent switching between the ECO mode and the mains inverter mode. Therefore, the ECO mode is not appropriate.

When the load is less than 10%, the ECO mode is not recommended.

Before setting the ECO mode, ensure that the bypass is normal and the power supply is available.

Step 1 Manually shut down the inverter to transfer the system to bypass mode.

Step 2 Set the ECO voltage range (±5%, ±6%, ±7%, ±8%, ±9%, ±10%).

Step 3 Set Working Mode to ECO. The LCD displays the single-node ECO mode.

Step 4 Manually start the inverter. (After the inverter is started, the UPS is still in bypass mode. The inverter is in standby mode. If the bypass is abnormal, the UPS transfers to normal mode immediately.) If the inverter is not started, the bypass cannot transfer to normal mode immediately when the bypass is abnormal, and the system may be powered off.

----End

3.2.10 Task 10: Setting the BSC Mode (Bus Synchronization Controller)

By default, the system works in non-BSC mode. When the system consists of a dual-bus system, set the mode to BSC.

The two UPS systems in the dual-bus system are the BSC master system and BSC slave system, which are randomly defined by users. (The two UPS systems cannot be the BSC master system or BSC slave system at the same time. The setting is complete when the UPS is started. If the UPS system is changed later, set this parameter to BSC master mode and BSC slave mode under the guidance of maintenance engineers.

Ensure that the BSC signal cables between the two BSC systems and the BSC hardware are correctly installed.

Step 1 Set the BSC main system.

On the main menu of the LCD of all UPSs, choose **System Info > Settings.** If the current user has not logged in, the login window is displayed. Enter the user name and password, and click  to log in. On the Settings tab page, click Advanced Parameters and set BSC Mode to BSC Main Mode.

Step 2 Set the secondary system of the BSC.

On the main menu of the LCD of all UPSs, choose **System Info > Settings**. If the current user has not logged in, the login window is displayed. Enter the user name and password, and click  to log in. On the Settings tab page, click Advanced Parameters and set BSC Mode to BSC Slave Mode.

Step 3 If no alarm is generated, the system runs properly.

----End

3.2.11 Task 11: Connecting to the Web Client

Step 1 Open a browser (Internet Explorer 8 is used as an example), choose Tools > Internet Options, click the Advanced tab, confirm that Use TLS 1.0 and Use TLS 1.1 are selected, and click OK, as shown in the following figure.

- If the monitoring version and power version are earlier than V100R003C00B006 (software package version: V100R003C00SPC700), use the default settings of Internet Explorer. Ensure that Use SSL3.0 and Use TLS1.0 are selected.
- For the monitoring and power versions of V100R003C00SPC008 (software package version: V100R001C00SPC700) or later, select Use TLS1.1 based on the default settings of the IE. Ensure that Use TLS1.0 and Use TLS1.1 are selected.

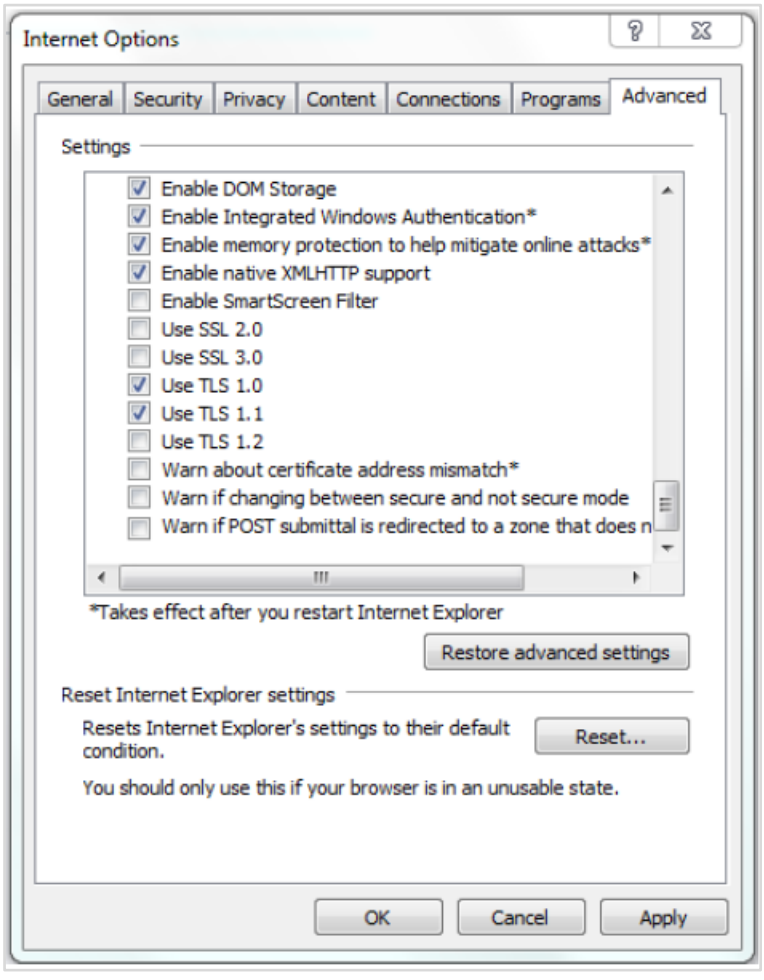


Figure 3-1 Setting Internet Options

Step 2 Enter https://UPS IP address in the address box of the browser and select a common language. The text is displayed in this language. Enter the correct user name and password, and click Login. The system supports Internet Explorer 6, Internet Explorer 8, and Firefox 31.0.

Figure 3-2 Web login

- The following table describes the default users, preset passwords, and rights.
- If a user enters incorrect passwords for three consecutive times, the system locks the user and cannot log in again within 5 minutes.

Table 3-1 Permission Description

Default user	Preset Password		Permission
admin (admin user)	LCD	000001	Has the permission to use all functions provided by the LCD and WebUI, allows users to browse system running information, export system information (historical alarms, logs, electronic labels, and fault point data), set parameters (system and battery), control (startup/shutdown, fault clearance, runtime clearing, and battery management), and configure system parameters (network parameters, user management, time, date, and site information). and system maintenance (upgrade, calibration, and debugging variables).
	WEB	Changeme	
operator (common user)	LCD	000001	Allows users to view system running information, export system information (historical alarms, logs, electronic labels, and fault point data), start and shut down the system, clear faults, and control the buzzer. Other parameter setting, control, and maintenance functions that may affect system running are unavailable.
	WEB	Changeme	

browser (browsing user)	WEB	-	You can view the current system running information but cannot modify the system.

4 Operations on a Parallel UPS5000

4.1 Introduction to the Experiment

4.1.1 About this Lab

In this lab, you can master the operation procedure and parameter settings by connecting a UPS5000 in parallel.

4.1.2 Objective

- Have a good command of UPS5000 parallel system parameters.
- Understand how to operate the UPS5000 parallel system.

4.2 Experiment Tasks

4.2.1 Task 1: Start the parallel system.

All the parameters have default values, but some parameters must match the actual power consumption environment and networking configuration. You must reset the parameters before running the system. Otherwise, the system may fail to work properly. The mandatory parameters are as follows:

Table 4-1 Parallel system parameters

Setting Item	Parameter description
Single/parallel system	Set to Parallel
Networking Mode	Set this parameter to one-to-many for the master server and one-to-one for the slave server.
Basic number of parallel racks	Set this parameter based on the actual number of servers.
Number of redundant racks connected in parallel	Set this parameter based on the actual number of servers.
Parallel No.	Number by UPS sequence (1, 2, 3, 4)
Shared battery string	If the parallel system shares one battery string, set this parameter to Shared. If each UPS uses an independent

	battery, set this parameter to Not Shared.

- Before starting the parallel system, commission each UPS.
- Before commissioning and powering on the parallel system, ensure that all input and output power cables are correctly connected and the phase sequence is correct. The parallel cable is routed and disconnected.
- Before starting the parallel system, ensure that all loads are OFF.
- If you Switch on the UPS output switch by mistake before connecting parallel cables, a bypass SCR short-circuit may be reported. In this case, power off the UPS to rectify the fault.

Step 1 Power on all UPS mains and bypasses. Switch on the mains and bypass input switches of all UPSs (maintain all UPS output circuit breakers to be OFF). If the input power is normal, the rectifier automatically starts, the MDU starts, and the Huawei logo and progress bar are displayed. After the SMU is started, you can set parameters such as the language, time, date, network, and system by following the instructions provided in Quick Settings.

Step 2 Check whether the software versions of all UPSs are the same. Check the software versions of all UPSs. Choose **System Info > About** and click **Detailed Version**. If the software versions are the same, go to step 3. If not, update all software versions to be the same.

Step 3 Start the inverters on each UPS. Ensure that all UPSs work in bypass mode and no alarm is generated. Manually start the inverters on each UPS. All UPSs transfer to normal mode.

Step 4 Test the output voltage and frequency of each UPS. After each UPS transfers to normal mode (you can check whether the UPS is in normal mode based on the system running diagram), check whether the UPS three-phase output voltage and frequency are normal based on the real-time data on the LCD. Use a multimeter to measure the three-phase output voltage of the output circuit breaker on the output PDC or the external output power distribution switch. Ensure that the inverter output voltage is normal. (The three-phase output voltage measured by the multimeter is equal to the output voltage fine-tuning ±1.0 V.) The three-phase output voltage displayed on the LCD is equal to the output voltage fine-tuning ±1.0 V, and the inverter output frequency is normal (three-phase output frequency = output frequency set on the LCD ±0.125 Hz). Record the valid three-phase output voltage of each UPS measured using a multimeter.

Step 5 Compare the output voltages of each UPS. After the output voltage and frequency of each UPS are tested, compare the output voltages of the UPSs. Ensure that the difference between the valid voltages of any two UPSs is less than 2 V. If the conditions are not met, the UPS with a large voltage deviation cannot be connected to the system. In this case, commission the UPS again.

Step 6 Shut down the inverters of each UPS. After confirming that no alarm is generated on each UPS, manually shut down the inverter on each UPS. All UPSs transfer to bypass mode.

Step 7 Check the bypass phase sequence. Switch on the UPS 1 output circuit breaker (ensure that the general switch for loads is turned off. Otherwise, the UPS 1 output circuit breaker will supply power to loads after it is turned on). Keep the output circuit breakers of other UPSs off. Set the multimeter to the AC voltage range. Connect a pen to the front-end phase A of the UPS 2. Connect the other probe to phase A at the rear of UPS 2 output switch. Measure the voltage difference between the UPS 2 output switch and phase B and phase C in the same way. If the phase sequence is correct, the voltage difference of each phase is less than 5 V. If the phase sequence is incorrect, the voltage difference of at least one phase is greater than 5 V. Use the same method to check whether the bypass phase sequence of all UPSs to be combined is correct. (When testing the phase sequence of other UPSs, keep the output switch of UPS 1 ON and the output switch of other UPSs OFF.) If the bypass phase sequence of all UPSs is correct, go to the next step. If the phase sequence of any UPS is incorrect, power off the system and check whether the bypass input and output cables are correctly connected to each UPS.

Step 8 Switch off the output switch of UPS 1. The output switches of all UPSs are OFF.

Step 9 Activate the EPO of each UPS. Press the external EPO switches connected to the dry contact cards of all UPSs one by one or the EPO switches in the general system. On the monitoring page, check that the EPO is activated successfully.

Step 10 Connect inter-rack parallel cables for all UPSs.

Step 11 Set the DIP switches on each UPS. Ensure that the first DIP switch of the UPS with the largest parallel number is set to ON, the other DIP switches are set to OFF, and the DIP switches of other UPSs are set to OFF.

Step 12 Set parallel parameters. On the LCD, choose System Info. On the Settings screen, if you have not logged in, enter the user name and password in the displayed login screen, and press. Then click the Basic Parameters icon. Set System Settings to Single by default and set it to Parallel. Four basic parallel parameters are displayed on the page.

- Parallel number: Set this parameter to 1, which is called UPS 1 or UPS 1.
- Networking mode: Set this parameter to one-to-many. By default, the first UPS is set to one-to-many, indicating that the UPS is the master UPS, and the remaining UPSs are set to one-to-one, indicating that the UPS is the slave UPS.
- Basic number of parallel racks: Set this parameter based on customer requirements.
- Number of redundant racks connected in parallel: Set this parameter based on customer requirements.
- Set Basic Parallel Racks and Redundant Parallel Racks for each UPS based on the actual system requirements. The two parameters must be the same for all UPSs in the same parallel system.
- Number of parallel racks + Number of redundant racks = Actual number of parallel racks.

- In a parallel UPS system, only one UPS can be connected in one-to-many networking mode.
- In this case, the UPS may generate alarms, such as the number of racks mismatch, insufficient rack redundancy, and inter-rack parallel cable alarm. The alarms will be automatically cleared one minute after all parallel cables are connected. The alarm "Parameter Asynchronization" may also be reported.

Step 13 Synchronize parallel system parameters. Synchronize the UPS parameters on the LCD of UPS 1. On the LCD, choose System Info. On the Settings screen, if you have not logged in, enter the user name and password and press Enter. Then click the Synchronize Parameter icon. Synchronize the UPS parameters in the parallel system. Ensure that no alarm is generated for each UPS and proceed with subsequent operations. Otherwise, clear the alarm first.

Step 14 Switch on all UPS output switches. Ensure that no alarm is generated on each UPS, and then Switch on the output switches of all UPSs one by one. The output switches of all UPSs are turned on.

Step 15 Remove the EPO of each UPS. Switch off the EPO switch on each UPS and tap Clear Fault on the LCD to clear the alarm. Each UPS transfers to bypass mode and the load switch remains OFF.

Step 16 Start the inverters on each UPS. After confirming that no alarm is generated, manually start the inverter on UPS1. UPS1 starts to work in normal mode.

Step 17 Check whether the inverter output of the parallel system is normal. After all UPSs in the parallel system transfer to normal mode, no alarm is generated on the SMU.

Step 18 Connect batteries to the parallel system. If no alarm is generated on the monitoring screen of each UPS, Switch on the battery input switch of each UPS (if there are multiple battery strings, Switch on the switch of each battery string and then the general switch between battery strings and the UPS). Ensure that batteries are properly connected. (The No battery alarm on the monitoring screen disappears within two minutes.) and no other abnormal alarms are reported.

Step 19 Shut down the inverters of each UPS. Ensure that no alarm is generated on each UPS and shut down the inverters of all UPSs.

Step 20 Switch on the load output switch. After the parallel system transfers to bypass mode, Switch on the general load output switch. The bypass supplies power to loads.

Step 21 Start each UPS one by one on the LCD. The UPS transfers to normal mode.

----End

4.2.2 Task 2: Powering Off and Shutting Down a Parallel System

Step 1 Shut down all loads in the parallel UPS.

Step 2 Shut down all UPS inverters or select Parallel Inverter Shutdown to shut down all UPSs. The system transfers to bypass mode.

Step 3 Switch off the general load switch, external output power distribution switch, battery switch, external input power distribution switch (or mains and bypass input switches in the external PDC), internal mains input switch (if any), internal bypass input switch (if any), and internal output switch (if any).

If you only need to shut down the UPS inverter, the system transfers to bypass mode without powering on loads, perform step 2. To power off the entire UPS, perform the preceding steps.

----End

4.2.3 Task 3: EPO

Step 1 Press the external EPO switches connected to the dry contact cards of all UPSs one by one or the EPO switches of the system.

----End

4.2.4 Task 4: Isolating Operations on a Single UPS in the Parallel System

Step 1 Shut down the inverter for the faulty UPS. The UPS has no output and the other UPSs continue to work in normal mode.

Step 2 Switch off the output switch or external output power distribution switch on the output PDC of the faulty UPS.

Step 3 Switch off the battery switch or upstream power distribution switch of the faulty UPS.

Step 4 Switch off the mains and bypass input switches or the upstream power distribution switch on the input PDC of the faulty UPS.

Step 5 The faulty UPS is isolated from the system and other maintenance operations can be performed.

----End

4.2.5 Task 5: Restoring the Isolated Single UPS in the Parallel System

Step 1 Switch on the input switch or upstream power distribution switch of the isolated UPS mains and bypass input PDCs.

Step 2 After the system is powered on, initialized, and configured, the monitoring screen of the UPS displays no output and no other alarm is generated.

Step 3 If no other alarm is generated on the LCD, Switch on the output PDC switch or external output power distribution switch of the UPS.

Step 4 Start the inverter on the UPS. All UPSs in the system work in inverter mode to restore the isolated UPS in the parallel system.

Step 5 Switch on the battery input switch of the UPS. The No Battery alarm disappears on the LCD.

----End

Huawei DCF Certification Training

HCIP-DCF-Deployment Huawei NetCol5000-A042 Lab Guide

ISSUE:2.0

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Technologies Co., Ltd.

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

Website: http://e.huawei.com

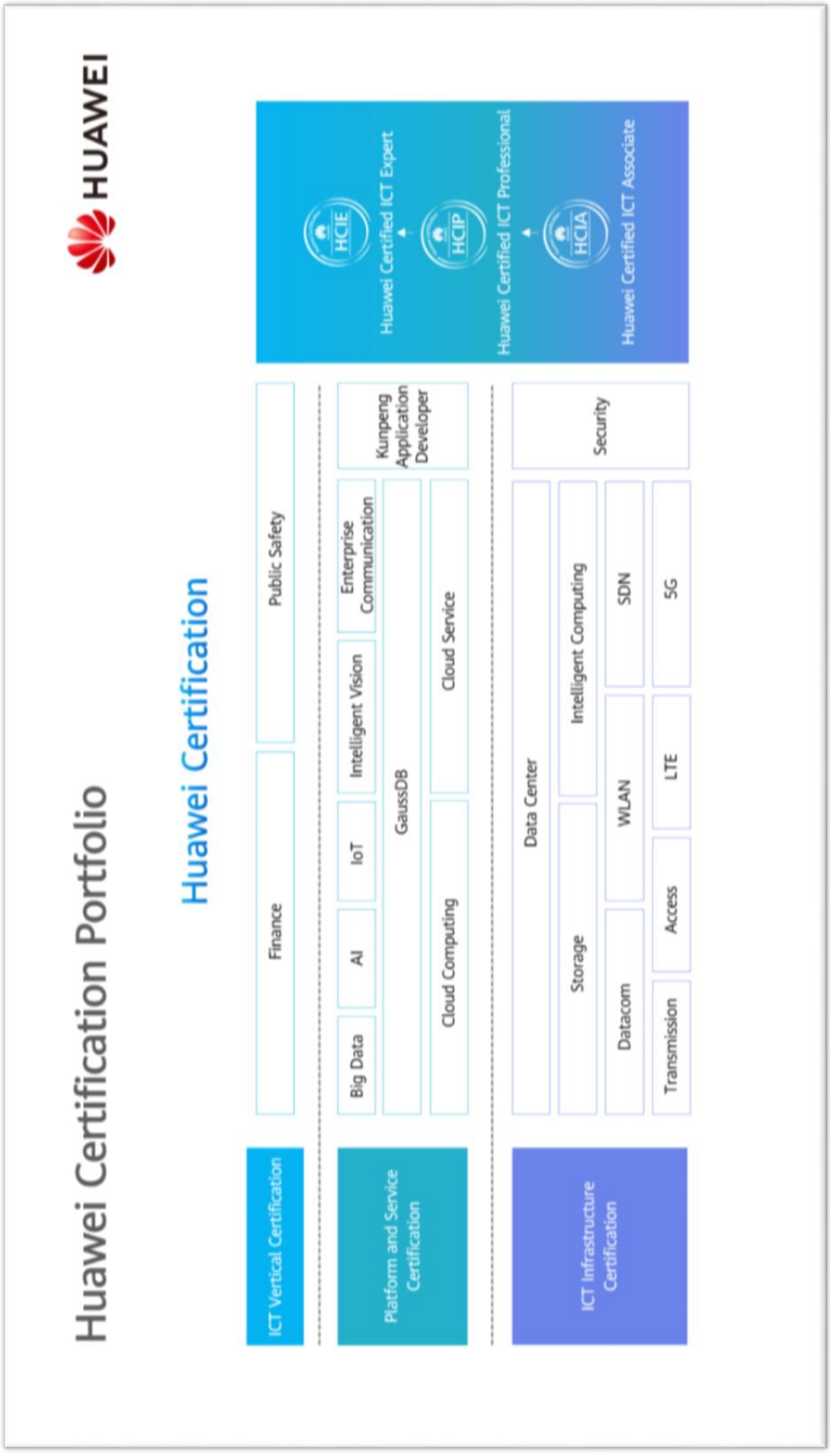
Huawei Certificate System

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, Platform and Service certification and ICT vertical certification, and grants Huawei certification the only all-range technical certification in the industry.

Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE).

HCIP-Data Center Facility Deployment V2.0 is aim to train and certify senior engineers who need to perform deployment and system commissioning for Huawei data center infrastructure products.

After passing the HCIP-Data Center Facility Deployment V2.0 certification, you will be familiar with Huawei data center infrastructure products and have the deployment and commissioning capabilities of Huawei data center infrastructure products. The full series of products include Huawei modular data center Fusion Module series products, Huawei UPS and precision PDC series products, Huawei data center energy storage products, Huawei data center smart cooling products, and Huawei data center DCIM system products.


HUAWEI
Huawei Certification Portfolio
Huawei Certification
ICT Vertical Certification
Finance
Public Safety
Platform and Service Certification
Big Data
AI
IoT
Intelligent Vision
Enterprise Communication
Kunpeng Application Developer
GaussDB
Cloud Computing
Cloud Service
ICT Infrastructure Certification
Data Center
Storage
Intelligent Computing
Security
Datacom
WLAN
SDN
Transmission
Access
LTE
5G
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Description

This document consists of three experiments. It describes the parameter settings and configurations and operations of NetCol5000.

- Exercise 1: Understand the NetCol5000 hardware architecture. This exercise helps you familiarize yourself with the NetCol5000 hardware components and functions of each module.
- Experiment 2 describes how to set parameters for a single NetCol5000, including setting output parameters, battery parameters, power-on/shutdown, and operating mode switching.
- Experiment 3 describes how to set parallel system parameters, start and shut down the parallel system, isolate a NetCol5000 from the parallel system, and add a NetCol5000 to the parallel system. This exercise helps readers learn how to set parallel system parameters.

Reader's Knowledge Background

This course is an intermediate course for Huawei certification. To better master the contents of this course, the readers of this course must meet the following requirements:

- Have basic knowledge about NetCol5000.

Content

1 Experiment Tasks

1.1 Task List

Table 1-1 Task List

Task Name			Recommendation task duration	Completed
Understanding Controllers	Appearance of the controller		30min	☐YES ☐NO
	Controller interface			☐YES ☐NO
	Main Page and Menu			☐YES ☐NO
Powering On Devices	Device management	Power-on Preparations	20min	☐YES ☐NO
		Powering On		☐YES ☐NO
	Subsequent Processing	Compressor check		☐YES ☐NO
		Compressor preheating		☐YES ☐NO
		Complete warm-up		☐YES ☐NO
Initial Configuration	Common Settings	Quick Setup	20min	☐YES ☐NO
		Setting parameters		☐YES ☐NO
		Parameter description		☐YES ☐NO
	Communication parameter setting			☐YES ☐NO
	Teamwork Settings			☐YES ☐NO
Startup and Wizard-based Commissioning	Wizard-based startup	Wizard-based startup preparation	30min	☐YES ☐NO
		Wizard-based		☐YES ☐NO

		commissioning components		
		Parameter Measurement Description		☐YES ☐NO
		Complete wizard-based commissioning.		☐YES ☐NO
	Normal power-on	Normal startup process		☐YES ☐NO
		Introduction to the Service Expert App		☐YES ☐NO
		Shutdown		☐YES ☐NO
Routine Operations	Querying Temperature and Humidity		60min	☐YES ☐NO
	Handling Current Alarms			☐YES ☐NO
	Querying Logs			☐YES ☐NO
	Querying System Parameters			☐YES ☐NO
	Querying Version Information			☐YES ☐NO
	Delete historical alarms.			☐YES ☐NO
	Deleting Logs			☐YES ☐NO
	Exporting Data			☐YES ☐NO
	Clear the device running time.			☐YES ☐NO
	Calibration sensor			☐YES ☐NO
	Adjusting the touchscreen			☐YES ☐NO
FQA	Change Password		15min	☐YES ☐NO
	Restore factory settings			☐YES ☐NO
	Enabling the T/H sensor			☐YES ☐NO

2 Controllers

2.1 Appearance and Ports

- The controller provides a 7-inch true color touchscreen and man-machine interfaces for query, setting, monitoring, and maintenance.
- The indicator on the panel displays operating status of the smart cooling product. Figure 2-1 shows the position of the indicator. Table 2-1 describes the mapping between indicators, buzzers, and alarms. If alarms of different severities (critical, major, minor, or warning) are raised simultaneously, the indicator status corresponds to the alarm with the highest severitylevel and the buzzer status corresponds to the unacknowledged alarm with the highest severitylevel.

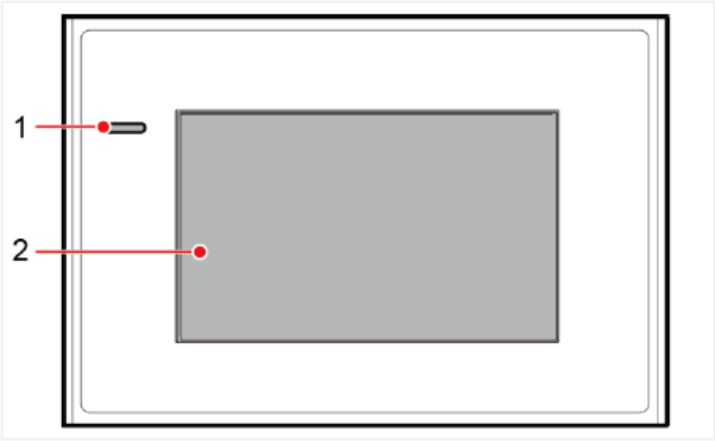


Figure 2-1 Indicators and buzzer status

Table 2-1 Indicator and buzzer status description

Indicates the alarm status.	Indicator	buzzer
The device is running properly or a warning alarm is generated.	Green light	No buzzing
A major alarm is generated.	Yellow light	intermittent chirp
A critical alarm is generated.	Red light	Constant buzzing

2.2 Controller interface

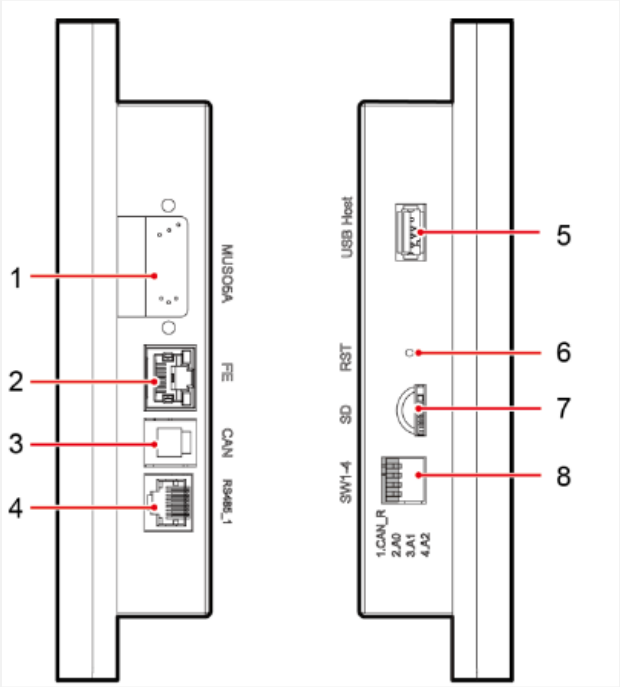


Figure 2-2 Ports on the controller side

(1) MUS05A (reserved) (2) Fast Ethernet (FE) port

(3) CAN (communication port between the main control board and the LCD)

(4) RS485_1 port (reserved)

(5) USB host (for software upgrade, data import, and export)

(6) RST (display restart switch)

(7) SD (reserved) (8) DIP switch on the LCD

2.3 Home Screen

The home screen displays the current system status. You can also quickly access other function menus, such as Run, Alarm, and Settings. Figure 2-3 shows the home screen of the controller.The value must be unique on the network.

Figure 2-3 Home screen

Table 2-2 Note for the page

No.	Option	Commented
1	Permission Status	Indicates that the user is not logged in. Indicates that you have logged in to the system as an operator. Indicates that you have logged in as the admin user.
2	Communication status between the display panel and the main control board	in the status bar indicates that the display panel communicates properly with the main control board. If is displayed in this position in the status bar, the communication fails.
3	USB status	in the status bar indicates that the USB flash drive is successfully connected to the display panel
4	Diagnostic Mode Status	in the status bar indicates that the smart cooling product is in diagnostic mode. Tap the icon to exit from the diagnostic mode
5	Buzzer status	The buzzer status can be set to On or Off. The icon indicates that the buzzer is on. When the buzzeris on, it buzzes when an alarm is generated. When the buzzer is buzzing, you can tap anywhere on the screen to mute the buzzer. After the buzzer is muted, it still buzzes when a new alarm is generated. The icon indicates that the buzzer is off (silenced).

		After the buzzer is silenced, it does not buzz when an alarm is generated.
6	The current critical alarm and their quantity	 refers to the current critical alarm and their quantity.
7	Critical alarm signals and their number	 Indicates the current critical alarm signals and the number of critical alarms.
8	Major alarm signals and their number	 Indicates the current major alarm signals and the number of major alarms.
9	Warning alarm signals and their number	 Indicates the number of current warning alarms.
10	Status bar	-
11	Login/Logout button	 Indicates that you have not logged in. You can click this icon to log in.  Indicates that you have logged in as the admin or operator user. You can click this icon to log out of the system.
12	Teamwork button	 No teamwork control is available.  The teamwork is in progress and no teamwork alarm is generated.  Teamwork control is performed and a teamwork alarm is generated.

2.4 Menu structure

The functions of each menu are as follows:

- Common Functions

View the component status, system parameters, and historical alarms of the precision air conditioner.

- Temperature and humidity curve

View the temperature and humidity curves of the precision air conditioner in the recent period (optional).

- Teamwork control

Set teamwork parameters and view teamwork information based on the teamwork networking requirements of the precision air conditioner.

running

View the component status, system parameters, names, control/running status, and related information of components in the precision air conditioner system.

- Alarm

View current and historical alarms of the precision air conditioner and delete historical alarms.

- Setting

Set the parameters involved in the operation of the precision air conditioner.

- Maintenance

View or clear the logs or component runtime/points of the precision air conditioner, manually diagnose components, calibrate sensors or touchscreens, export data, and upgrade the system.

- About

View the model, manufacturer, monitoring version, detailed version, and electronic label of the controller.

2.5 Preparing for Power-On

- Procedure

Step 1 Verify that the smart cooling product switch in the upstream power distribution cabinet (PDC) is OFF.

Step 2 Verify that the input voltage meets the requirement.

Step 3 Verify that the L1, L2, L3, N, and PE wires are connected to the indoor and outdoor units incorrect phase sequence.

Step 4 Verify that the signal cable between the indoor and outdoor units is properly connected.

Step 5 Verify that the water sensor is properly installed.

Step 6 If teamwork networking is **required, verify that the teamwork cable is correctly connected.**

DANGER

Ensure that there is no reverse or open phase for the input power cable of the smart cooling product. Otherwise, the smart cooling product may be damaged beyond repair.

2.6 Power-On

- Context

All switches are set to OFF before delivery. If the preset status is changed, restore the preset status before any operation.

Step 1 Turn on the upstream power input switch of the air conditioner. The LCD lights up.

Step 2 Step 2 Turn on the switch QF3 that controls the outdoor unit and compressor, and switch QF4 that controls the electric heater. (If electric heater is not configured, it is not need to turn on the QF4.)

Step 3 After the system is powered on for the first time, the Quick Settings screen is displayed. Log in as the admin user, as shown in Figure 2-4.

Figure 2-4 Initial power-on

NOTICE

- The operator user can access customer and delivery parameters. Parameters in the advanced menu are the delivery parameters. The admin user can access customer, delivery, maintenance, and R&D parameters. Parameters in the advanced menu are the R&Dparameters.
- To prevent the effect of misoperation on the system during the O&M, log in as the operator user first before modifying parameters. Confirm with Huawei before modifying parameters that cannot be modified by operator users; otherwise, Huawei will not be liablefor any consequences of the unauthorized modification.
- Only certified pros are allowed to modify the advanced parameters. Unauthorized modifications may lead to device malfunction or damage.
- After the first login, change the password in time to ensure account security and prevent unauthorized network attacks, such as data tampering. Huawei will not be liable for any security issues caused by your failure to change the preset password in time or password loss after changing.

- After login, you are allowed to perform operations until being logged out if no operation is performed within 3 minutes (user set). For security purposes, tap at Logout the lower-right corner of the screen to manually log out after you have completed all operations.

Step 4 Figure 2-5 shows how to configure relevant parameters. Click **Next** until the LCD home screen is displayed after the configuration.

Figure 2-5 Quick Settings

- Follow-up Procedure

After powering on, the compressor starts preheating, and the system generates an alarm indicating that the compressor is preheating (for 12 hours). Do not start the air conditioner before the preheating ends. Figure 2-6 is shown if you tap Start.

Figure 2-6 Compressor preheating warning

- If you need to query the remaining preheating time, choose Running > Device Details >Compressor on the home screen.

2.7 Initial Configuration

2.7.1 Setting Temperature and Humidity Values and EnablingT/H Sensors

- Prerequisites

The T/H sensors outside the cabinet need to be enabled when they are installed, otherwise, skip Step 2.

If you need to enable a humidity and temperature sensor, log in as the admin user.

This section describes how to enable Cold aisle sensor 1.

- Procedure

Step 1 On the home screen, choose Settings > System Settings > T/H sensor.

Step 2 Set Cold aisle sensor 1 to Enable.

Step 3 Set the temperature and humidity values by referring to Table 2-3.

Table 2-3 Parameter description

Parameter	Description	Configuration Principle
T/H control type	Sets **Cold-aisle**, **Hot-aisle**, **Return-air**, or **Supply-air** as required. The temperature and humidity set points correspond to the	• **Return-air**: For a hot aisle, select **Return-air** to control the temperature and humidity around the air return vent of the precision air conditioner. • **Supply-air**: For a cold aisle, select **Supply-air** to control the temperature and humidity around the air supply vent of

Parameter	Description	Configuration Principle
	selected control type can be set.	the precision air conditioner. • **Cold-aisle**: For a cold aisle, select **Cold-aisle** to control the temperature and humidity of the aisle. The temperature and humidity values come from the humidity and temperature sensor in the aisle. • **Hot-aisle**: For a hot aisle, choose **Hot-aisle** to control the temperature and humidity of the aisle. The temperature and humidity values come from the humidity and temperature sensor in the aisle.
Temp control mode	Controls the temperature inside the room or aisles based on the **Average**, **Maximum**, or **Minimum** of the temperatures collected by each sensor.	• **Average**: Select **Average** if the temperature is to be controlled based on the averaged data value collected by the collector. • **Maximum**: Select **Maximum** if the temperature is to be controlled based on the maximum data value collected by the collector. • **Minimum**: Select **Minimum** if the temperature is to be controlled based on the minimum data value collected by the collector.
Supply-air temp set point, Supply-air humid set point	Sets the required humidity and temperature in a room or aisle.	The ACC controls the temperature and humidity based on the set value. For example, if **Temp control type** is set to **Return-air**, **Return-air temp set point** is set to **30.0**, and **Return-air humid set point** is set to **25.0**, the ACC will control the temperature and humidity around the return-air vent of the precision air conditioner to a temperature of 30°C and humidity of 25% RH.
Return-air temp set point, Return-air humid set point		
Cold-aisle temp set point, Cold-aisle humid set point		
Hot-aisle temp set point, Hot-aisle humid set point		
Cold aisle	Sets the sensors in	Enable the corresponding humidity and

Parameter	Description	Configuration Principle
sensor 1, 2, 3	cold aisles to **Enable**.	temperature sensor installed in the cold aisle.
Hot aisle sensor 1, 2, 3	Sets the sensors in hot aisles to **Enable**.	Enable the corresponding humidity and temperature sensor installed in the hot aisle.

2.7.2 (Optional) Setting the Pressure Difference Control

- Prerequisites

If the differential pressure sensors are installed, perform the following operations accordingly.

If the differential pressure sensors are not installed, skip this part.

Step 1 On the home screen, choose Settings > System Settings > Indoor fan, set Air-side difference pressure sensor type to 0~50 Pa.

Step 2 Set Indoor fan control type to Pressure diff ctrl.

Step 3 Change the other parameters based on the following instructions.

Table 2-4 Parameter description

Parameter	Description	Configuration Principle
Indoor fan control type	Sets the control type for the indoor fan.	Normally, retain R/S air temp diff rate ctrl. If the differential pressure sensors are configured, change to Pressure diff ctrl.
Indoor fan pressure difference setpoint	Sets the value for the pressure difference control.	When there are partial hot spots indoors, you are advised to raise the value to ensure that the air volume of the indoor fans is between 60%–70%.
Air-side difference pressure sensor type	Sets the measuring range for the air side differential pressure sensor.	There is no default value. Set it to 0~50 Pa..
Min indoor fan speed	Sets the minimum speed for the indoor fan.	The default value is 30%.You are advised not to change the value.
Max indoor fan speed	Sets the maximum speed for the indoor fan.	The default value is NA.

-End

2.7.3 Setting Teamwork Control Parameters

- Prerequisites

Assign teamwork control numbers and addresses for the teamwork controlled precision air conditioners as follows:

Teamwork group no: Group the precision air conditioners in adjacent areas as one, that is, assign one teamwork control number for them. At most four teamwork control groups can be assigned (1–4).

Teamwork unit address: The address for the precision air conditioner in the same group cannot be the same (address range: 1–32). The precision air conditioner addressed 1 is the master one that collects, processes, and delivers data. Set the unit address numbers from one to the number of units in this group. If the address of a device exceeds the range, the device cannot enter the teamwork control. If the address of any unit amid the range is unavailable, the teamwork topology shows that this device is offline.

- Context

The figures and parameters in this section are for reference only. Set actually parameter values as required.

To change alarm settings, log in as the Admin or Engineer user.

Step 1 On the home screen, tap  > Teamwork Settings, to enter Teamwork Settings page.

Step 2 Set teamwork control parameters.

All teamwork control parameters can be set on the master smart cooling product. Only Teamwork group No., Smart cooling product address, Enable teamwork CAN resistor, Teamwork function and Networking mode can be set on slave smart cooling products. Other parameters of the slave units will be modified by the master unit synchronously.

Table 2-5 Teamwork settings

Parameter	Description	Configuration Principle	Default Value
Teamwork group No.	The number of the teamwork controlled group, which is the same for all the devices in the group	Set the assigned teamwork control number.	1
Teamwork unit address	Only one device in each group can be set to **1**. Other device addresses should be different from each other.	Set the assigned unit address..	NA
Teamwork function	Disable or enable the teamwork function. If the teamwork function is	Set this parameter based on the onsite device heat distribution.	Disable

Parameter	Description	Configuration Principle	Default Value
	disabled, this device is operating according to its own control If the teamwork function is enabled, this device works in harmony with others that in the same group.		
Teamwork mode	Set the teamwork mode. The options include Smart and iCooling.	Determine whether to enable the iCooling mode based on onsite heat load variations. If the heat load varies greatly, it is recommended that you enable the iCooling mode. The parameter can only be modified on the ECC WebUI and cannot be modified on the airconditioner screen.	Smart
Enable L1/L2 linkage	Enable or disable L1/L2 linkage.	Set this parameter based on site requirements. The parameter can only be modified on the ECC WebUI and cannot be modified on the air conditioner screen.	Disable
Network	Networking mode for the teamwork.	Networked over CAN.	Over CAN
Total number of units	Number of the precision air conditioners in this group (1 to 32 can be set).	Total number of the precision air conditioners in this group.	3
Number of running units	Number of running units in a group. The value ranges from 1 to **Total number of units**.	The master unit assigns the devices to be active units by the device number, beginning with the address 1 until to **Number of running units**. The rest will become the standby ones..	2
Rotation	Disable or enable the active and standby precision air conditioners to change identity after a certain time, maximizing their service life.	This function is recommended when the heat is even.	Disable

Parameter	Description	Configuration Principle	Default Value
Rotation period	Rotation days (1-30).	7 by default.	7 days
Rotation time	24 hours in a day (0-23)	0 by default.	0
Forced rotation	**Forced rotation** specifies whether to enable a forcible rotation on the group before the specified rotation time. After a forced rotation, the accumulated time is recalculated.	This item is set to **No** by default. If forced rotation is required, the function is set to **Yes**.	No
Requirement control	Enable or disable the requirement control for the master device. When the requirement control is **Enable**, the master device synchronizes data (the temperature and humidity control type and set points of the master device) to the slave device, and all the precision air conditioners in the group refer to the mode delivered by the master device. When the requirement control is **Disable**, the master device does not synchronize data to the slave device, and all the air conditioners operate based on their own requirements, not referring to the mode delivered by the master device.	The requirement control function is recommended for the following scenario: In one teamwork, the temperature and humidity control type and temperature and humidity set point of units are the same, and device heat loads are distributed evenly.	Disable
Cascade	After the requirement control is enabled, you can configure Cascade. The cascade function starts standby precision air conditioners if the active one cannot meet the refrigerating requirements.	If the heat load to the device increases, the cascade function is recommended.	Disable

Parameter	Description	Configuration Principle	Default Value
Large ring cooling capacity P	Proportion coefficient in L1/L2 linkage PID control.	You are not recommended to change the value.	350s
Large ring cooling capacity D	Differential coefficient in L1/L2 linkage PID control.	You are not recommended to change the value.	10s
Cooling capacity adjustment period	Adjustment period in L1/L2 linkage PID control.	You are not recommended to change the value.	5s
L1/L2 linkage cooling stop ref.temp	Reference temperature at which the air conditioner stops cooling in the cooling mode in L1/L2 linkage.	Set this parameter based on the lowest temperature allowed onsite. Normally you are not recommended to change the value.	18.0°C
L1/L2 linkage dehumid stop ref.temp	Reference temperature at which the air conditioner stops dehumidification in the dehumidification mode in L1/L2 linkage.	Set this parameter based on the lowest temperature allowed onsite. Normally you are not recommended to change the value.	18.0°C
L1/L2 linkage cooling stop delay	Duration within which the device is still cooling when the cooling stop condition is met in L1/L2 linkage.	Set this parameter based on the lowest temperature allowed onsite. Normally you are not recommended to change the value.	180s
L1/L2 linkage fastest temp rise	Maximum temperature rise rate when the temperature rises rapidly caused by sudden load power increase.	Set this parameter based on the micro-module size and maximum load power. The smaller the module and the higher the load power, the greater the temperature rise rate is.	4.0°C/min
L1/L2 linkage temperature	Temperature setpoint in L1/L2 linkage.	Target temperature controlled in the micro-module. The parameter can only be modified on the ECC WebUI and cannot be modified on the air conditioner screen.	24.0°C
L1/L2	Humidity setpoint in L1/L2	Target humidity	45.0%RH

Parameter	Description	Configuration Principle	Default Value
linkage humdity	linkage.	controlled in the micro-module. The parameter can only be modified on the ECC WebUI and cannot be modified on the air conditioner screen.	
Note: In the **ACC V100R002C00** software versions, DIP switch is replaced by the **Teamwork CAN resistor enable** parameter. If teamwork is not set onsite, remain the parameter in **OFF**. If teamwork is set, change the parameters of the first and last units to **ON**, and remain the others in **OFF**.			

Step 3 Complete the teamwork settings for all the smart cooling products by performing Step 1 and Step 2.

Step 4 On the home screen of any teamwork controlled smart cooling product, If the teamwork control succeeds, the teamwork topology of the smart cooling product in the group is displayed, as shown in Figure 2-8. Table 2-6 describes the note for the screen.

Figure 2-7 Teamwork topology

Table 2-6 Teamwork topology

No.	Parameters	Note
1	On/Off/NA	**On** indicates the precision air conditioner is started and **Off** indicates the opposite. **NA** indicates the precision air conditioner is offline.
2	01, 02, 03	Indicates the device address. **01** is the

No.	Parameters	Note
		master one and the rest are all slave ones. NOTE If the master one offline, the teamwork networking failed.
3	Active/Standby	Active: properly responds to the requirement control. Standby: responds to the requirement control when **Active** is faulty (critical alarms, shutdown, and offline) or **Active** cannot meet cooling requirements.
4	M/S	M indicates the master unit, and S indicates a slave unit. Blue indicates that the device is operating, and gray indicates that the device is idle.
5	Frame: green/non-green	A device with green frame indicates the device itself, as shown in 
		A non-green frame indicates the other device in the group, as shown in 
6	Ground color: red, bright gray, dark gray	Red indicates that a critical alarm is generated, as shown in 
		Bright gray indicates that the device is operating without any critical alarms, as shown in 

NOTE

If teamwork succeeds, the teamwork icon is green. If teamwork fails, the teamwork icon is red. If teamwork mode is disabled, the teamwork icon is gray.

- Follow-up Procedure

After you have completed the settings, perform the following checks to confirm whether the teamwork control is available:

1. Check whether the device number on the topology is the same as the actual device number.

– If yes, go to 2.

– If no, check the cable connection and the settings of teamwork control parameters.

2. Check whether the number of active devices on the topology is the same as the actual device number.

– If yes, go to 3.

– If no, check the cable connection and the settings of teamwork control parameters.

3. Check whether the number of standby devices on the topology is the same as the actual device number.

– If yes, go to 4.

– If no, check the cable connection and the settings of teamwork control parameters.

4. Check whether the number of online devices on the topology is the same as the actual device number.

– If yes, the check is complete.

– If no, check the cable connection and the settings of teamwork control parameters.

2.8 Setting Communications Parameters

2.8.1 Setting Communications Parameters (Modbus RTU Protocol)

- Procedure

Step 1 On the home screen, choose Settings > Comm Settings > Modbus Settings.

Figure 2-8 Modbus Settings

Step 2 Set baud rate and communication address

Table 2-7 Figure Teamwork Communications Parameters

Parameter	Specification	Setting Method
Baud rate	9600, 19200	Set the baud rate as required. The value should be consistent with that at the EMS side. This parameter is configurable when **Protocol** is set to **Modbus RTU**.
Comm address	1–255	Set the address of the precision air conditioner. The EMS communicates with the precision air conditioner through this address, and the addresses of two precision air conditioners connected to the same EMS must be unique. This parameter is configurable when **Protocol** is set to **Modbus RTU**.

2.8.2 Setting Communications Parameters (Modbus TCP Protocol)

- Context

  To set communications parameters, log in as the admin user.

  If Link mode is Server, a smart cooling product can be accessed by element management system (EMS) client. If Link mode is Client, a smart cooling product can be connected only to the EMS with the corresponding IP address. If Link mode is Server and client, a smart cooling product can be accessed by EMS client and connect to the EMS with the corresponding IP address at the same time.

- Procedure

Step 1 On the home screen, choose Settings > Comm Settings > IP Settings.

Figure 2-9 IP Settings

Step 2 Set the parameters according to the actual plan.

Step 3 Tap Submit.

Step 4 On the home screen, choose Settings > Comm Settings > Modbus Settings.

Figure 2-10 Modbus Settings

Step 5 Set parameters for Modbus TCP by following instructions.

2.8.3 Setting Communications Parameters (SNMP Protocol)

- Context

To set communications parameters, log in as the admin user.

This section is suitable only for SNMP. Skip this section if you use Modbus.

Record the values entered in this section. They will be used when you access a smart cooling product to an EMS (element management system).

One smart cooling product supports concurrent access of up to 6 EMSs through SNMP.

- Procedure

Step 1 On the home screen, choose Settings > Comm Settings > SNMP Settings. Figure 2-11 is displayed.

Figure 2-11 Setting SNMP communications parameters

Step 2 Set SNMP Version based on site requirements, and then tap Submit.

If you set SNMP Version to ALL or SNMPv1&v2c, you can set Read Community and Write Community by performing Step 3.

If you set **SNMP Version** to **ALL** or **SNMPv3**, you can add SNMPv3 users by performing **Step 4**.

Step 3 Set Read Community and Write Community

1. Tap the text box after Read Community, as shown in Figure 2-12. Set Read Community as planned, tap  and then tap Submit.

Figure 2-12 Setting read community

2. Tap the text box after Write Community, as shown in Figure2-13. Set Write Community as planned, tap  and then tap Submit.

Figure 2-13 Setting write community

Step 4 Add an SNMPv3 user.

1. Tap Add under SNMP V3.
2. Enter a planned value for User Name, select values for Auth Protocol and Prop Protocol from drop-down list boxes, and tap  , as shown in Figure 2-14.
MD5 and DES protocols are not secure. It is recommended that you set Auth Protocol to SHA, and set Prop Protocol to AES. The following operations use the recommended settings as an example.
3. Set SHA Password and Confirm Password as planned, and tap  ,as shown in Figure 2-16.

Figure 2-14 Setting the protocol type

NOTICE

Passwords of an authentication protocol and proprietary protocol must comply with the following policies:

The password must consist of 8–15 characters and contain at least two types of characters among uppercase letters (A–Z), lowercase letters (a–z), and digits (0–9).

A password must be different from the corresponding user name or inverted user name.

A password must not be a string containing duplicate sections, such as 12a12a12a.

Figure 2-15 Setting an SHA password

4. Set AES Password and Confirm Password as planned, and tap , as shown in Figure 2-15.

5. Tap Submit.

Step 5 Tap the text box after SNMP Port, as shown in Figure 2-16. Set SNMP Port to the actual port number, tap , and then tap Submit.

Figure 2-16 Setting an AES password

Figure 2-17 Setting SNMP port

Step 6 Tap Next Page.

Step 7 Set SNMP trap parameters.

1. Tap Add under **SNMP** Trap.
2. Set Trap Address as planned and **Trap Port** to the actual port number.
3. Select the **SNMP Version.** If an **SNMPv3** user is configured, it is recommended that SNMP Version be set to SNMPv3.
4. If SNMP Version is set to SNMPv3, select an SNMPv3 user name, and then tap as shown in Figure 2-18.

Figure 2-18 Setting SNMP trap parameters

5. Tap Submit under SNMP Trap.

----End

2.8.4 (Optional) Setting WIFI Parameters

- Prerequisites

After connecting the WIFI module of the USB interface to the USB port of the smart cooling product display, WIFI Settings is enable to be set.

- Procedure

Step 1 On the home screen, choose Settings > Comm Settings > WIFI Settings. Figure 2-19 is displayed.

Figure 2-19 Setting WiFi parameters

Step 2 Set the parameters.

WiFi SSID: Set WiFi SSID based on the actual configuration; WiFi SSID is the name used for the WiFi hotspot over which a mobile phone can connect to the smart cooling product.

WiFi Password: Enter the WiFi password when you use a mobile phone to connect to the WiFi. When you enable the WiFi function for the first time, you need to set a password (the WiFi has no preset password).

Enable WiFi: Enable the WiFi function. The default status is Disable.

Step 3 Tap Submit.

2.8.5 Startup

- Context

Tap the **Start** or **Shutdown** buttons on the home screen to start or shut down the smart cooling product.

If a power failure occurs and the smart cooling product is powered on again, the smart cooling product automatically restores to the original state (start or shutdown) before the power failure.

The hardware port for controlling the status of the remote dry contact or On/Off status on remote is reserved on the ACC. The status of the remote dry contact and On/Off status on remote is on by default.

The operations that start the smart cooling product successfully by the display button or by element management system (EMS) is effective only when the remote dry contact or On/Off status on remote is on the status of on.

- Procedure

Step 1 Tap Start on the home screen of the ACC

If the screen shown in Figure 2-20 is displayed, tap **Yes**. Indicating initial startup, perform Step 2 for initial startup verification

Figure 2-20 Initial startup

Figure 2-21 Password screen

If the screen shown in Figure 2-22 is displayed, indicating not initial startup, tap **Yes** to start the smart cooling product.

Figure 2-22 Startup

Step 2 Open the Service Expert app.

Step 3 Tap StartUp on the home screen of the app and the screen shown in Figure 2-23 is displayed.

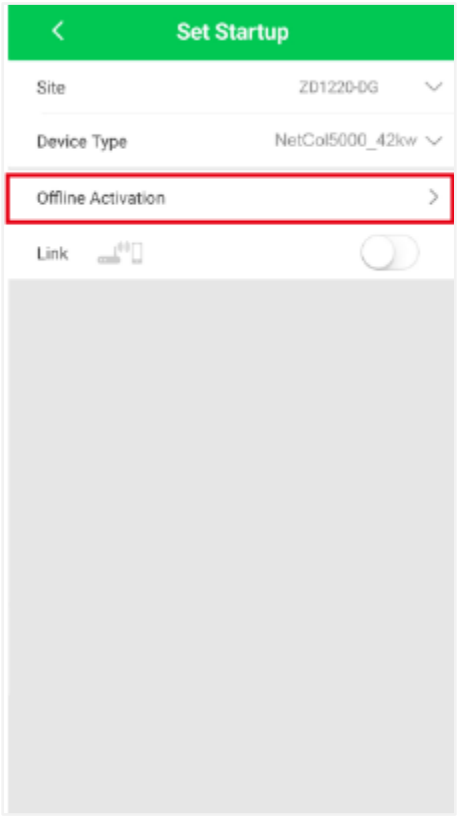


Figure 2-23 Offline activation

Step 4 Tap Offline Activation and the screen shown in Figure 2-24 is displayed

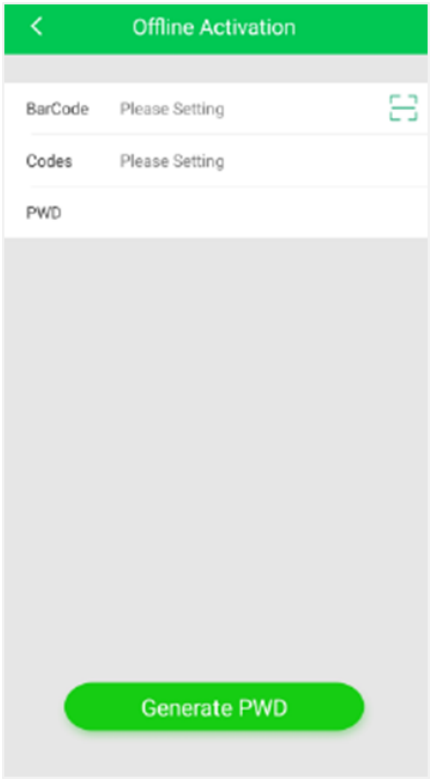


Figure 2-24 Generating a startup password

Step 5 On the Offline Activation screen, enter Bar code and Verification code, which are available on the home screen of the ACC shown. Tap Generate PWD to generate a startup password.

Step 6 Tap Password on the home screen of the ACC and enter the generated startup password in the displayed dialog box.

Step 7 After you power on the smart cooling product, the screen displays the **Wizard Startup** screen.

If the refrigerant is charged exactly as required, complete the wizard commissioning.

If the remaining refrigerant is not charged, tap **No**.

Complete refrigerant charging, and then perform the wizard commissioning by choosing **Maint > Wizard** Startup to enter the wizard startup screen.

2.8.6 Charging the Remaining Refrigerant

- Check that the outdoor unit switch is turned on before you start the compressor.
- Remove the refrigerant steel vessel after checking that no more refrigerant is required.
- Charge refrigerant in an amount exactly as standard charge required. Otherwise, the devices may be damaged.

  Procedure

Step 1 Tap Start on the home screen.

Step 2 Choose Maint > Diagnostic Mode > Enter to enter the diagnostic mode.

Step 3 Set the compressor to 3000 rpm.

Step 4 Charge refrigerant on the basis of the precharging.

Step 5 If there are no low-temperature components, open the low-pressure valve of the pressure gauge, and charge the remaining refrigerant from the low-pressure needle valve in small flow or intermittently.

3 Startup wizard

3.1 Startup wizard

3.1.1 Prerequisites

Check that refrigerant is fully charged before performing the wizard startup.

3.1.2 Context

The startup wizard allows for commissioning of components such as the indoor fan, electric heater, humidifier, condensate pump, and cooling system. It also supports component automatic operation and automatic device checking, and can output commissioning report. After you power on the smart cooling product for the first time, the screen displays the **Wizard Startup** screen. If the smart cooling product is not started for the first time, choose **Maint > Wizard Startup** to enter the **Wizard Startup** screen.

NOTICE

Tapping **No** or **Exit,** submission timeout, and system exception all result in commissioning failures. Choose **Maint > Wizard Startup** to enter the **Wizard Startup** screen for new commissioning.

3.1.3 Procedure

Step 1 On the home screen, choose **Maint > Wizard Startup**

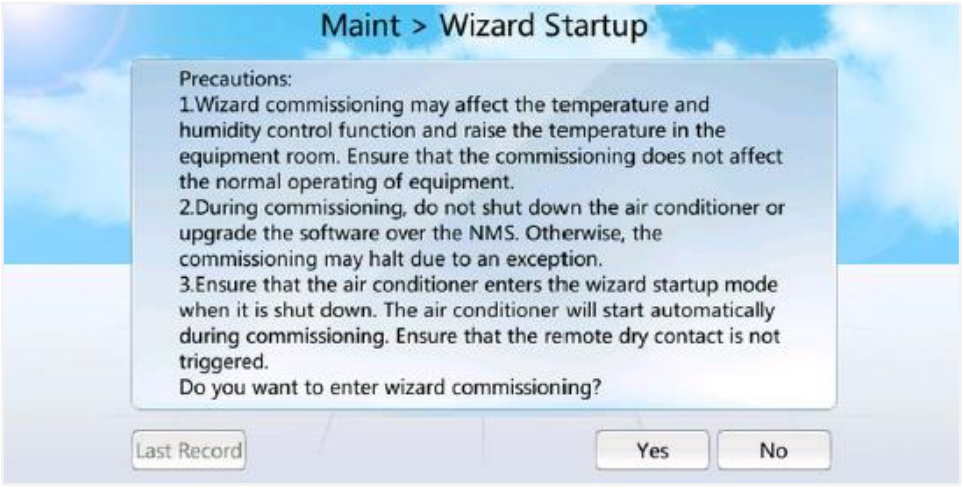


Figure 3-1 Startup wizard

Step 2 Tap Yes. The checking before startup screen is displayed, as shown in Figure 3-2.

Figure 3-2 Checking before startup

NOTICE

If the remaining refrigerant is not charged, tap No. Complete refrigerant charging, and then perform the wizard commissioning.

Step 3 Tap **Yes** for check items one by one according to the prompt messages on the screen.

Step 4 Tap **Yes** and enter the screen where you select commissioning items, as shown in Figure 3-3.

Figure 3-3 Selecting commissioning items

NOTE

If the system is not configured with the electric heater and humidifier components, the electric heaterand humidifier commissioning items will not appear on the screen.

If the heating function and humidification function are disabled, you cannot select the electric heaterand humidifier items.

All the items are selected by default if you first enter the screen where you select commissioning items. Except that the indoor fan item is mandatory, you can clear other commissioning items that are not required.

Step 5 Tap **Yes**, a dialog box is displayed as follows. Choose whether to select Humidifier commissioning or not onsite.

Figure 3-4 Dialog box

Step 6 Tap **Confirm**. The fan commissioning screen is displayed, as shown in Figure 3-5.

Figure 3-5 Fan commissioning

Step 7 After the fan commissioning, the electric heater commissioning screen is displayed.

If the software version is V200R001, use a clamp meter to measure the currents of cables L1, L2, and L3. (Measure the currents of main power for dual power supply.) Enter the measured values on the screen, and tap Submit within the time limit displayed on the screen. The controller automatically determines whether the current of the smart cooling product is within the normal range.

Figure 3-6 Electric heater commissioning (L1/L2/L3)

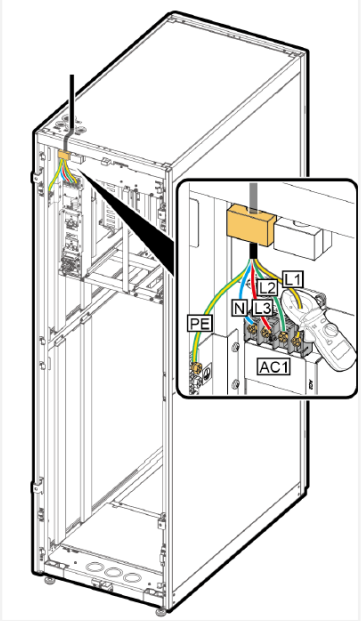


Figure 3-7 L1/L2/L3 current detection

If the software version is V200R002, use a clamp meter to measure the currents of X102.1, X102.2, and X102.3 cables of X102 terminal. Enter the measured values on the screen, and tap **Submit** within the time limit displayed on the screen. The controller automatically determines whether the current of the smart cooling product is within the normal range.

Figure 3-8 Electric heater commissioning (X102)

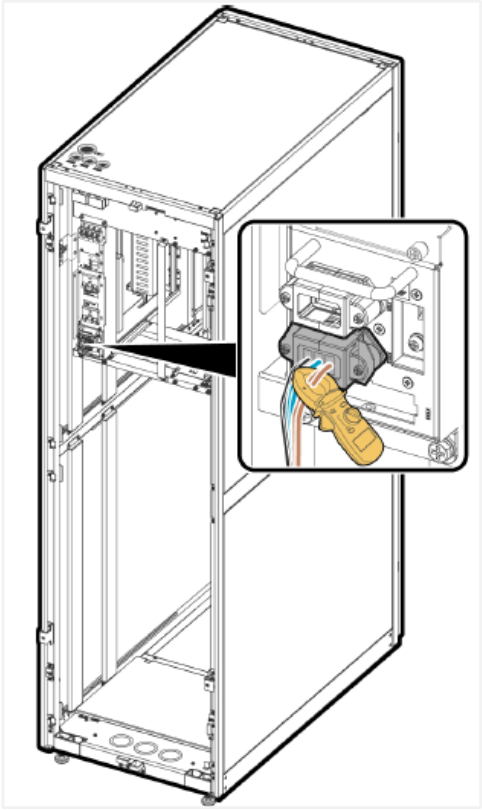


Figure 3-9 X102 current detection

Step 8 After the electric heater commissioning, the humidifier commissioning screen is displayed.Verify that the main water inlet valve is open. Check whether the humidifier pipes and the solenoid valve leak.

If yes, select Leak, and tap Submit. The commissioning has failed. Locate and repair the leak points.

If no, select No leak, and tap Submit within the time limit displayed on the screen.

Figure 3-10 Humidifier commissioning

Step 9 After the humidifier commissioning, the condensate pump commissioning screen is displayed.Check whether the condensate pump vibrates and generates operating sound.

If yes, select **Yes**, and tap Submit within the time limit displayed on the screen.

If no, select **No**, and tap Submit. The commissioning has failed. Locate and rectify the faults of the condensate pump.

Figure 3-11 Condensate pump commissioning

After the condensate pump commissioning, the cooling system commissioning screen is displayed. Check whether the electric heating belt is firmly attached to the compressor outer wall and whether there is noticeable temperature rise by touching the belt surface.

Figure 3-12 Cooling system commissioning

Step 10 View the commissioning result.

Figure 3-13 is displayed if component commissioning succeeds.

Figure 3-13 Commissioning successfully

Figure 3-14 is displayed if component commissioning fails, which ends startup wizard commissioning.

Figure 3-14 Commissioning unsuccessfully

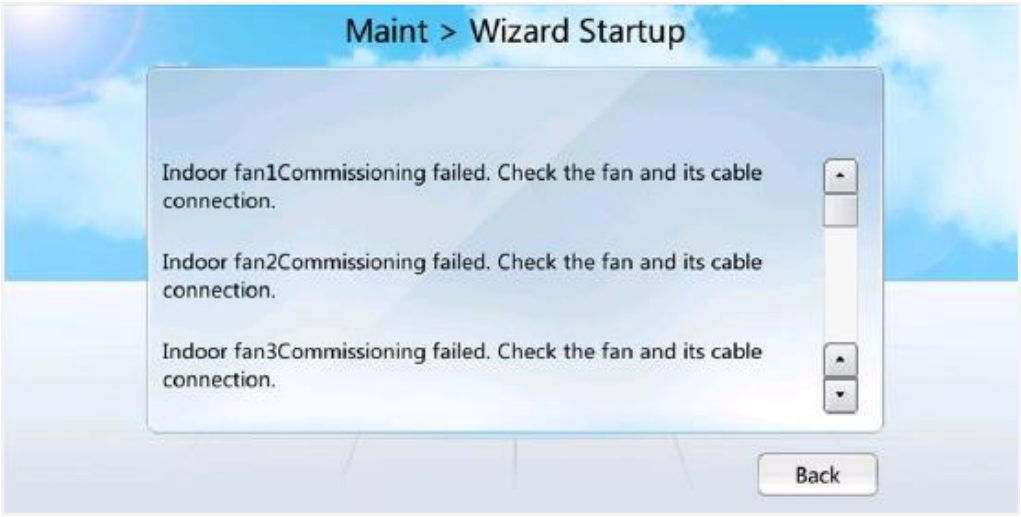


Figure 3-15 Details of failure

---End

3.2 (Optional) Adjusting the Air Deflecting Assembly

- Prerequisites

Adjust the air deflecting assembly on the inner side of the front door to a proper angle based on actual needs. The air deflecting assembly can be adjusted to 30° , 60° , 90° , 120° , and 150° (90° by default).

- Procedure

Step 1 Raise the button on the top of the air deflecting assembly, and the air deflector is loosened.

Step 2 Rotate the air deflector assembly along the chute to the leftmost (30°).

NOTE

From the leftmost to the rightmost of the chute, the angle is 30°, 60°, 90°, 120°, and 150° respectively.Determine the adjustment angle of the air deflector assembly based on the airflow.

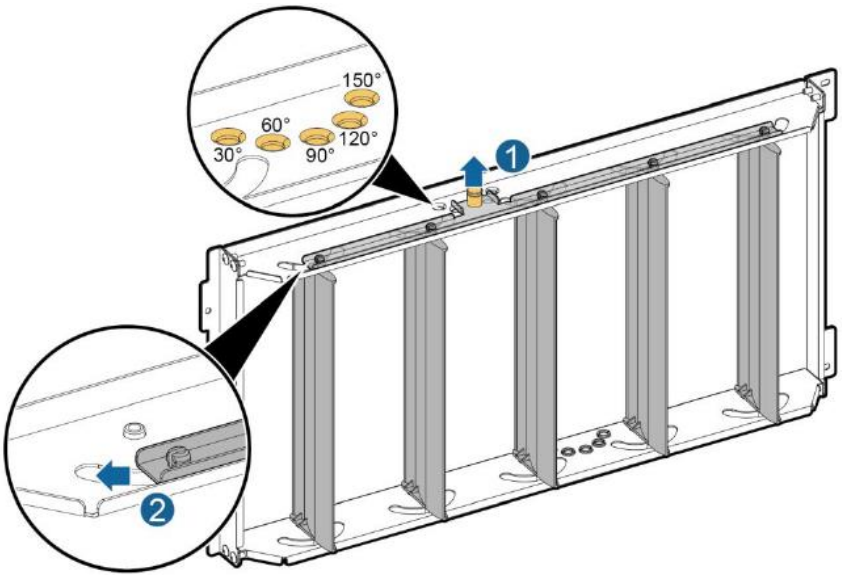


Figure 3-16 Adjusting the air deflecting assembly

3.3 (Optional) Power-off

- Context

In shutdown mode, the Shutdown button is green (unavailable) and the Start button is gray(available).

- Procedure

Step 1 Tap Shutdown on the home screen. A warning is displayed, indicating whether to shut down the smart cooling product, as shown in Figure 3-17.

Figure 3-17 Shutdown

Step 2 Tap Confirm. If the device is successfully shut, the system displays a message, indicating that the command is successfully triggered.

Step 3 Turn off the primary power switch QF1 and standby power switch QF2. (You do not need to turn off the standby switch QF2 when there is only one power supply.)

Step 4 (Optional) If the smart cooling product needs to be maintained in power-off mode or long-term power-off, switch off the smart cooling product circuit breaker on PDC.

----End

3.4 Checking After Commissioning

Step 1 lists the commissioning checklist.

Check Item	Actual Result
No oil stain exists on the copper pipe thermal insulation foam or bottom plate, or it has been cleaned.	☐Passed ☐ Failed
The needle valve plug is secured (torque of 0.45 ± 0.05 N · m), and valve bonnet is tightened.	☐Passed ☐ Failed
The foreign matter inside the water pan and bottom plate is cleaned up.	☐Passed ☐ Failed
The air filter is correctly installed according to the air flow direction on the frame.	☐Passed ☐ Failed

4 Operations on the LCD

4.1 Querying Temperature and Humidity Curves

- Context

The **T/H Curve** screen displays temperature and humidity curves showing the recent temperature and humidity changes. You can choose to display the curves showing data changes of recent one hour, one day, seven days, or 30 days.

- Procedure

Step 1 On the home screen, tap **T/H Curve**. Figure 4-1 is displayed.

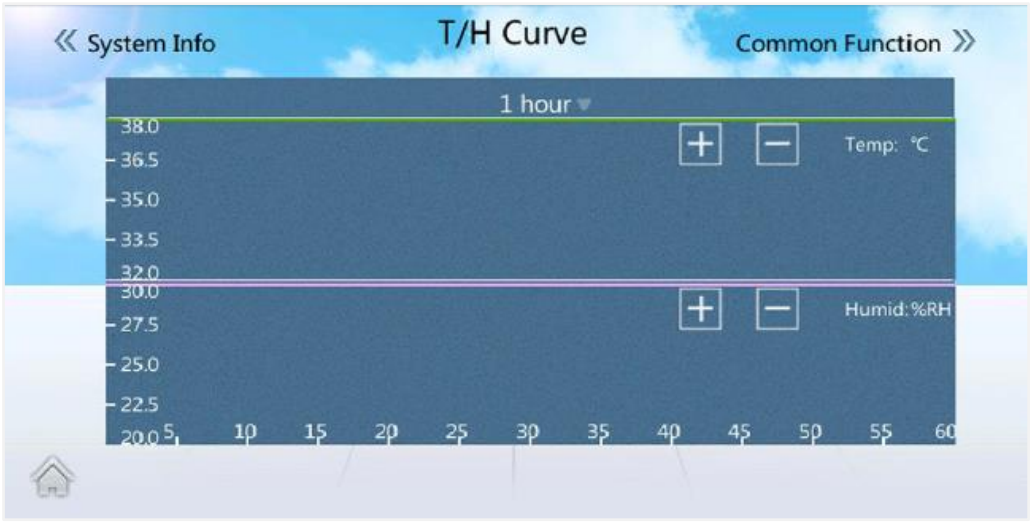


Figure 4-1 T/H curve screen

NOTE

The temperature curve (upper) and the humidity curve (lower) are displayed on the same screen. The abscissa shows time. The temperature set point is the midpoint temperature on the upper ordinate while the humidity set point is the midpoint humidity on the lower ordinate.

The temperature and humidity curves show the current average temperature and humidity of the control type.

You can view the temperatures from (temp set point – 3° C) to (temp set point + 3° C) at least and from (temp set point – 30° C) to (temp set point + 30° C) at most.

You can view the humidity from (humidity set point – 5%) to (humidity set point + 5%) at least, and from (humidity set point – 50%) to (humidity set point + 50%) at most. Specific humidity fluctuation range displayed varies according to different models of smart cooling products.

----End

4.2 Querying Logs

- Procedure

Step 1 On the home screen, choose Maint > Query Logs. Figure 4-2 is displayed.

Maint > Log Maintenance > Query Logs

No.	User Name	Time	Source	Parameter
1	admin	09/23/2017 12:07:04	LCD	A/C System-Teamwork function: Enable->Disable
2	admin	09/23/2017 11:58:00	LCD	A/C System-Requirement control: Disable->Anti-competitive running
3	admin	09/23/2017 11:57:48	LCD	A/C System-Rotation function: Disable->Enable
4	admin	09/23/2017 11:57:03	LCD	A/C System-Teamwork function: Disable->Enable
5	admin	09/23/2017 11:12:28	LCD	Indoor fan-Indoor fan control type: R/S air temp diff rate ctrl->Pressure diff ctrl
6	admin	09/23/2017 11:12:21	LCD	Indoor fan-Air-side difference pressure sensor type: No->0~50Pa

Total: 24 1/4

Figure 4-2 Query logs screen

----End

4.3 Querying Component Status

- Context

You can query component status in the following two ways.

Enter the Status Summary screen. The control or running status of major components such as the compressor, EEV, indoor fan are displayed.

Enter the Device Details screen and then enter the menu of a specific component. All parameters for the component are displayed.

- Procedure

Step 1 When viewing the component status through Status Summary, choose Common

Function > Status Summary or Running > Status Summary on the home screen. The general component status screen is displayed.

When querying component status through Device Details (using the T/H sensor as an example), choose Running > Device Details > T/H Sensor on the home screen to query the status of the T/H Sensor.

4.4 Querying System Parameters

- Procedure

Step 1 Choose Common Function > Operating Info on the home screen, the related screen is displayed.

Step 2 Choose Running > System Overview on the home screen, the related screen is displayed.

4.5 Querying Version Details

- Procedure

Step 1 On the home screen, select **About.**

Step 2 On the About screen, tap Version Info or E-label. Figure4-3 and Figure 4-4 are displayed.

Figure 4-3 Version Info

Figure 4-4 E-label

NOTE

The Version Info screen displays version details of the display board, control board, and temperature and humidity collection board. The E-label screen displays electronic labels of the entire system, control board, display board, and temperature and humidity collection board.

When some T/H boards of the cold or hot aisles are enabled, T/H Board on the About > Version Info screen, or T/H Board on the About > E-label screen shows the information of these T/H boards.

When some T/H boards of the cold or hot aisles are disabled, T/H Board on the About > Version Info screen, or T/H Board on the About > E-label screen does not show the information of these T/H boards.

4.6 How to View Teamwork Control Information

- Procedure

Step 1 On the home screen, choose  >  . The teamwork control information is displayed, as shown in Figure4-5.

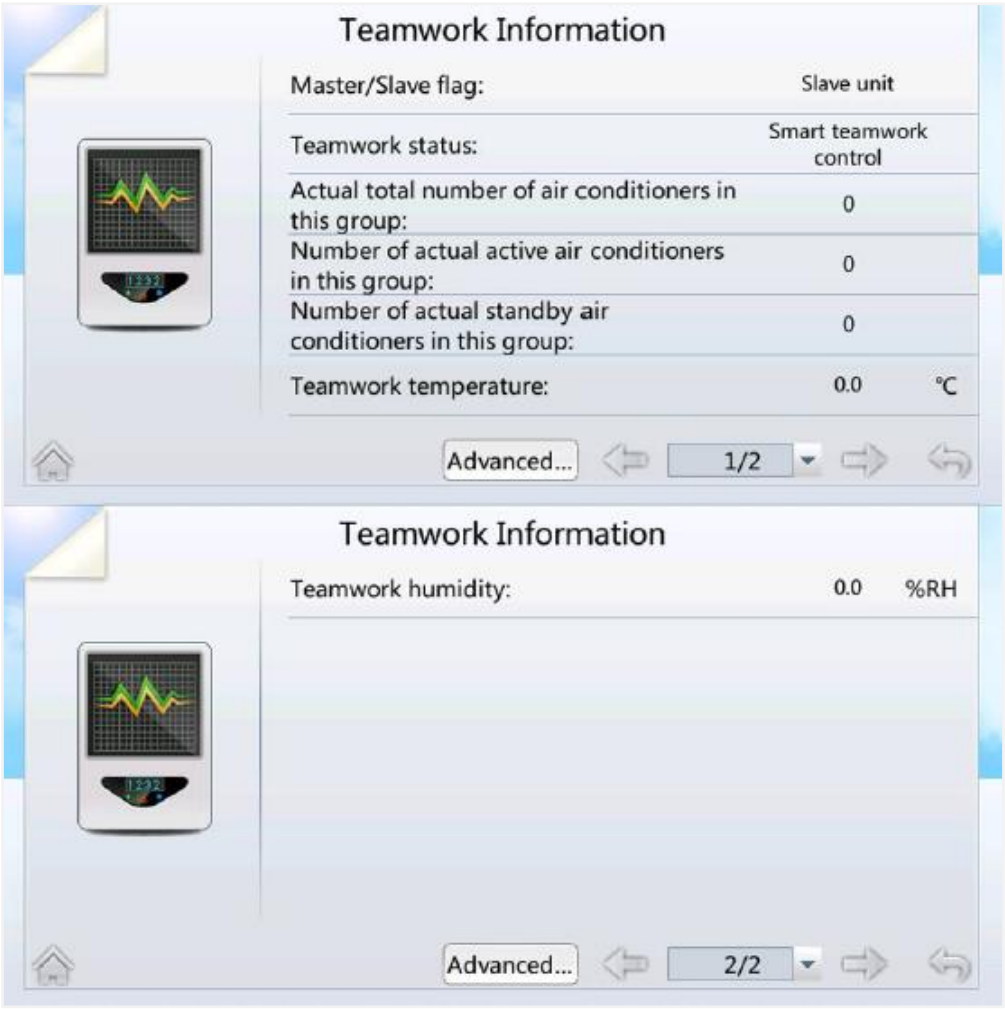


Figure 4-5 Teamwork control information screen

NOTE

Master/Slave flag indicates the information of this single unit. Other information is about the teamwork control information of the group.

4.7 How to Silence the Buzzer

- Procedure

Step 1 Tap the icon in the status bar and tap Off to silence the buzzer. After the buzzer is silenced, the icon changes to .

End

4.8 How Can I Handle Active Alarms?

- Procedure

Step 1 Tap 

(or choose Alarms > Query Act Alarms) on the home screen to enter the active alarms screen.

Figure 4-6 Act Alarms

Step 2 Click each alarm to open the Details page, which contains Name, Generated, Severity, Location, Cause ID, Code, Possible Causes and Procedure for the alarm.

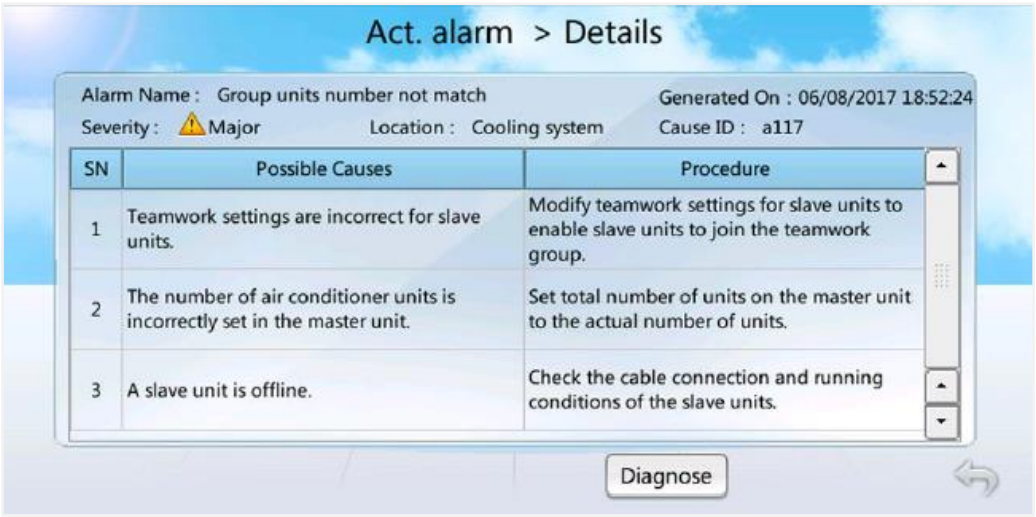


Figure 4-7 Details

Step 3 Tap Diagnostic Mode to view the diagnosis report. Rectify the faults following instructions in the diagnosis report.

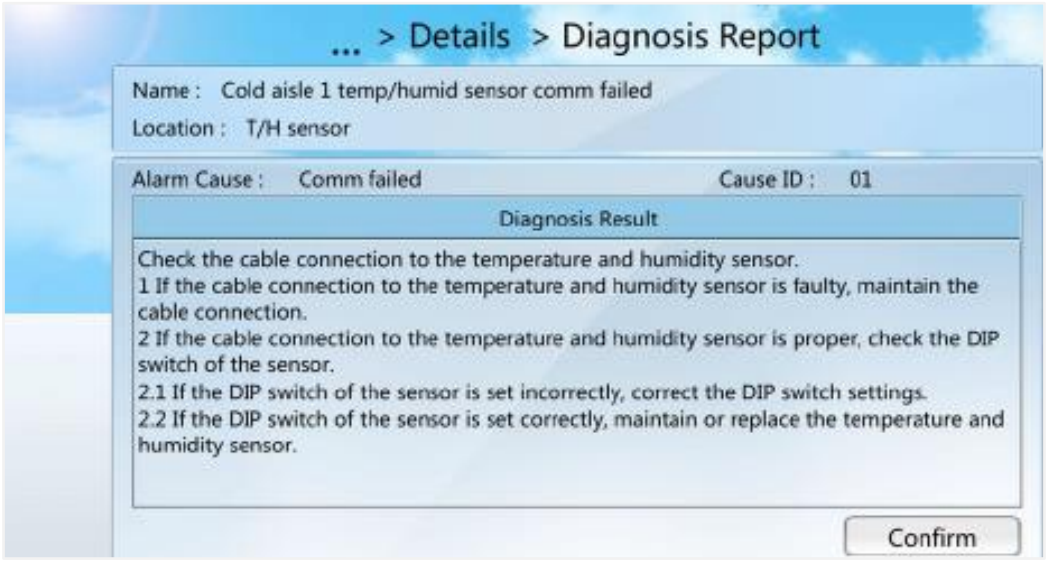


Figure 4-8 Diagnosis report

4.9 Deleting Historical Alarms

- Procedure

Step 1 On the home screen, choose Alarms > Delete Hist Alarms. Figure 4-9is displayed.

Figure 4-9 Delete historical alarms screen

4.10 Deleting Logs

- Procedure

Step 1 On the home screen, choose **Maint > Log Maintenance > Delete Logs > Yes** to delete all thelogs.

NOTE

After logs are deleted, the log deletion operation is recorded in the first log that is displayed.

4.11 Calibrating a Sensor

- Context

Calibrate a sensor if the displayed temperature or humidity on the sensor deviates from the actual value. For example, if the return air temperature measured by other temperature detection devices at the return air detection point is 20° C while the value measured by the sensor is 22° C, the sensor has an error of 2° C, and the calibration value should be set to –2° C.

- Procedure

Step 1 On the home screen, choose Maint > Sensor Calibration.

Step 2 Fill the calibration value based on the measured error.

5 FQA

5.1 How to Modify a Password

- Procedure

Step 1 On the home screen, choose Settings > User Settings to enter the User Settings screen, shown in Figure 5-1.

Figure 5-1 User Settings

Step 2 Tap Password to enter the password changing screen, as shown in Figure 5-2.

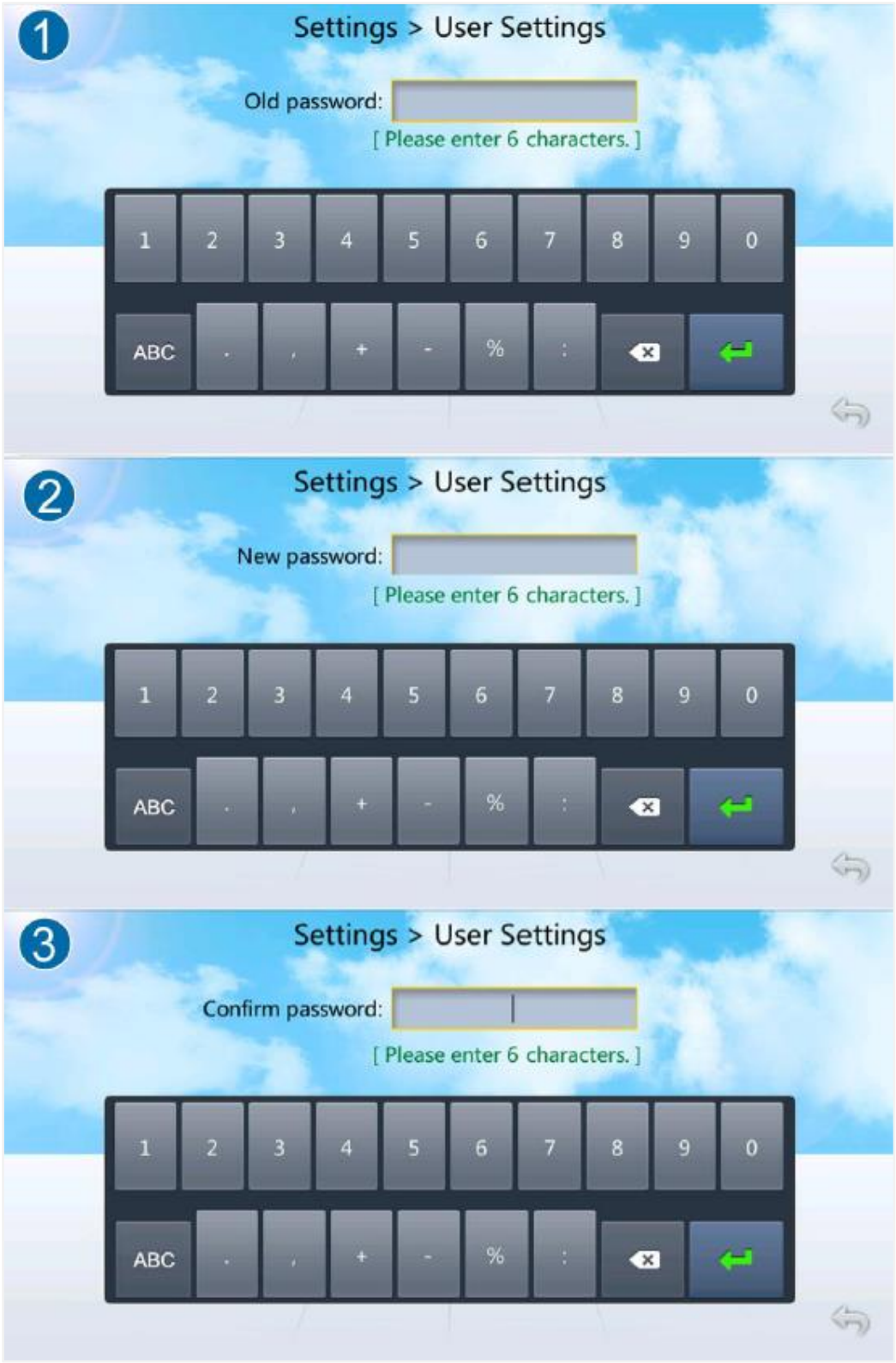


Figure 5-2 Modifying the password

5.2 Restoring Factory Settings

- Procedure

Step 1 Tap Shutdown on the screen and wait for the system to shut down.

Step 2 Press the SW button on the main control module for at least 10s.

Figure 5-3 shows the SW button on the main control module.

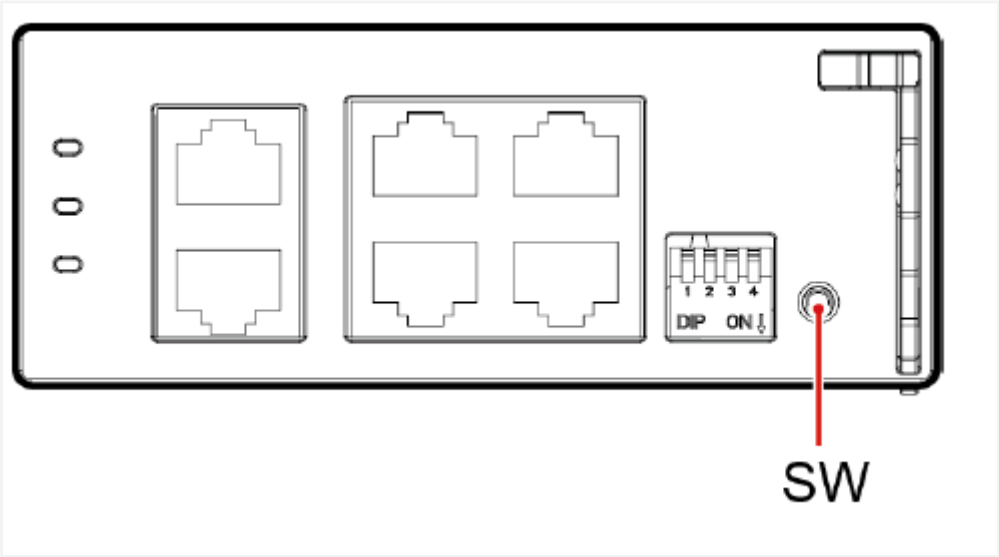


Figure 5-3 SW button on the main control module

Step 3 The LCD displays a dialog box asking you to confirm the operation of restoring factory setting.

Step 4 After the restart completes, the LCD displays the setup wizard screen for setting parameters.

-End

Huawei DCF Certification Training

HCIP-DCF-Deployment

Huawei DCIM Software Installation and Deployment Lab Guide

ISSUE:2.0

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Technologies Co., Ltd.

Address:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China
Website:	http://e.huawei.com

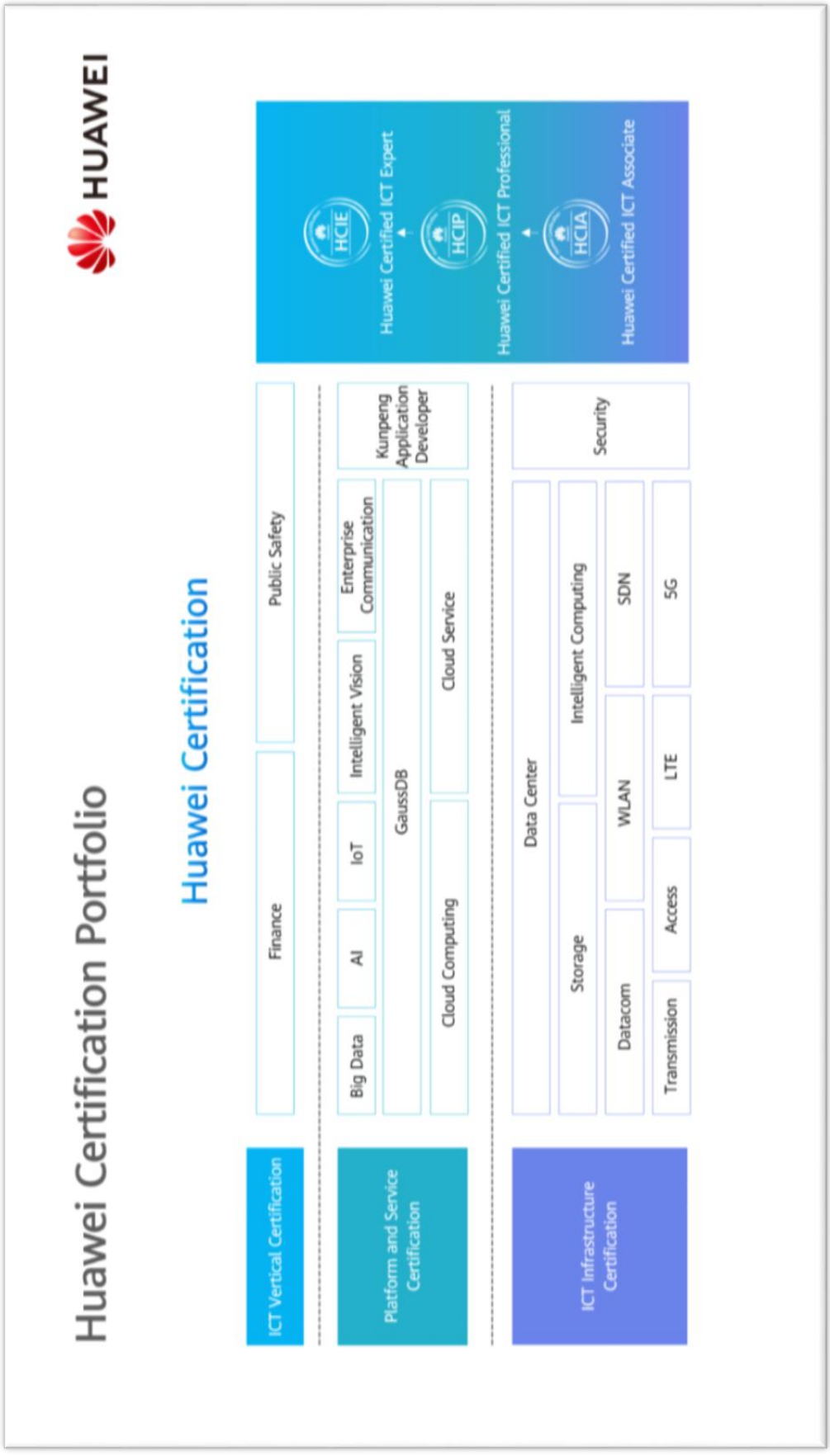
Huawei Certificate System

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, Platform and Service certification and ICT vertical certification, and grants Huawei certification the only all-range technical certification in the industry.

Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE).

HCIP-Data Center Facility Deployment V2.0 is aim to train and certify senior engineers who need to perform deployment and system commissioning for Huawei data center infrastructure products.

After passing the HCIP-Data Center Facility Deployment V2.0 certification, you will be familiar with Huawei data center infrastructure products and have the deployment and commissioning capabilities of Huawei data center infrastructure products. The full series of products include Huawei modular data center Fusion Module series products, Huawei UPS and precision PDC series products, Huawei data center energy storage products, Huawei data center smart cooling products, and Huawei data center DCIM system products.


HUAWEI
Huawei Certification Portfolio
Huawei Certification
ICT Vertical Certification
Finance
Public Safety
Platform and Service Certification
Big Data
AI
IoT
Intelligent Vision
Enterprise Communication
Kunpeng Application Developer
GaussDB
Cloud Computing
Cloud Service
ICT Infrastructure Certification
Data Center
Storage
Intelligent Computing
Security
Datacom
WLAN
SDN
Transmission
Access
LTE
5G
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Overview

This document is a training course for HCIP-DCF-Deployment certification. It is intended for trainees who are preparing to take the HCIP-DCF-Deployment exam or readers who want to understand the Huawei DCIM software installation and deployment process.

Description

This document describes how to install and commission Huawei DCIM - NetEco in three

Content

1 Precautions for Installing the NetEco

Background Knowledge Required

1.1 Term Description

Server: hardware or software in different scenarios.

- In the description of the Browser/Server structure, the server refers to the server application of the software.
- The server refers to the TaiShan 200 server.

Host: refers to a computer running EulerOS (EulerOS).

Network management software: refers to the NetEco management software in this document.

Virtual: Virtualizes a computer into multiple logical computers by using the virtual technology. Multiple logical computers can run on one computer at the same time. Each logical computer can run a different operating system, and applications can run in an independent space without affecting each other. This greatly improves the work efficiency of the computer. Each logical computer is a virtual machine. When the NetEco is deployed on a virtual machine, install the NetEco operating system and database on the virtual machine.

FusionSphere is a Huawei proprietary cloud operating system that integrates the virtual platform and cloud management features to simplify the construction and use of the cloud computing platform and meet the cloud computing requirements of enterprises and carriers.

FusionManager: FusionSphere management software deployed on VMs. Manages FusionSphere virtual and hardware resources and provides system monitoring management, O&M management, and service catalog management.

FusionCompute: FusionSphere software components, including VRM and host components. Virtualizes physical resources and provides VM services for FusionSphere.

Virtual Resource Management (VRM): virtual resource management. Huawei virtual management software, which works with the UVP to form a virtual infrastructure product.

1.2 Restrictions

In all installation scenarios, observe the following restrictions:

- To avoid program conflicts, you are advised not to install unnecessary software on the NetEco server.
- Only one NetEco system can be installed on one server.
- The NetEco software can be installed only on the operating system of the simplified Chinese or English version.
- During the installation or startup of the NetEco, do not operate the server by multiple users. Otherwise, the installation or startup may fail.
- Do not modify system configurations (such as environment variables) without permission. Otherwise, U2000 functions may be abnormal.
- Check whether the NE version meets the mapping requirements. If the requirements are not met, upgrade NEs. You can download it from Huawei technical support website.

1.3 NetEco system software package and tool software

The NetEco software system consists of five parts, as shown in Table 1-1.The installation package can be obtained from Huawei technical support website.

Table 1-1 NetEco software components

Application software	Software Package Name	Description	Detials
Operating system	OS_EulerOS2.0SPXX_arm64_X.X.X.iso	Used to install EulerOS on the server.	In the preinstallation scenario, preinstallation has been performed. In the new installation scenario and virtual scenario, download and install it onsite.
Deployment tool	iManagerNetEco_DeployTool_V600R020C00XXX_Euler_arm64.zip	Used to install the NetEco software in one-click mode.	In the preinstallation scenario, preinstallation has been performed. In the new installation scenario and virtual scenario, download and install it onsite.
Platform software package	iManagerNetEco_Platform_V600R020C00XXX_Euler_arm64.zip iManagerNetEco_Platform_V600R020C00XXX_Euler_arm64.z	Used to install the platform software.	In the preinstallation scenario, preinstallation has been performed. In the new installation scenario and virtual

	ip.cms iManagerNetEco_Platform_V600R020C00XXX_Euler_arm64.zip.crl		scenario, download and install it onsite.
Product service package	iManagerNetEco6000_V600R009C00XXX_Euler_arm64.zip iManagerNetEco6000_V600R009C00XXX_Euler_arm64.zip.cms iManagerNetEco6000_V600R009C00XXX_Euler_arm64.zip.crl	Used to install the NetEco.	In the preinstallation scenario, preinstallation has been performed. In the new installation scenario and virtual scenario, download and install it onsite.
NetEco NE mediation software	iManagerNetEco6000_Mediation_pkgs_x.x.x	Used to install the NetEco NE mediation software to shield NE differences.	You need to download and install it onsite.

During the installation and deployment, some operations need to be performed with other tools. The involved tools and software are as follows:

Table 1-2 Tool and software list

Tool software	Purpose	Description
PuTTY	Log in to the server in SSH mode through the CLI.	Visit https://www.putty.org.
FileZilla tool	Use FileZilla to transfer files using SFTP.	Address: https://filezilla-project.org
Decompression software	Used to decompress files.	/

2 Experiment Tasks

2.1 Task List

Table 2-1 Task List

Task Name		Duration	Completed
Preinstallation Scenario	Preparing for the Installation	60 min	☐YES ☐NO
	Setting System Parameters - Deployment Commissioning		☐YES ☐NO
	Logging In to the NetEco		☐YES ☐NO
	Loading a License File		☐YES ☐NO
	(Optional) Installing the NE Mediation		☐YES ☐NO
New installation scenario	Preparing for the Installation	60 min	☐YES ☐NO
	Installing and Configuring the Operating System		☐YES ☐NO
	Installing the NetEco Software		☐YES ☐NO
	Setting System Parameters - Deployment Commissioning		☐YES ☐NO
	Logging In to the NetEco		☐YES ☐NO
	Loading a License File		☐YES ☐NO
	(Optional) Installing the NE Mediation		☐YES ☐NO
Virtual Deployment Scenario (Optional)	Preparing for the Installation	60 min	☐YES ☐NO
	Creating a VM (FusionSphere)		☐YES ☐NO
	Creating a VM (FusionCompute Scenario)		☐YES ☐NO
	Configuring IP Addresses		☐YES ☐NO
	Installing the NetEco Software		☐YES ☐NO

3 Preinstallation Scenario

In the preinstallation scenario, the NetEco software has been installed on the onsite server. You need to set the NetEco parameters based on the actual networking and commission the NetEco software.

3.1 Installation Process

The following figure shows the NetEco software installation and deployment process in the EulerOS-based preinstallation scenario.

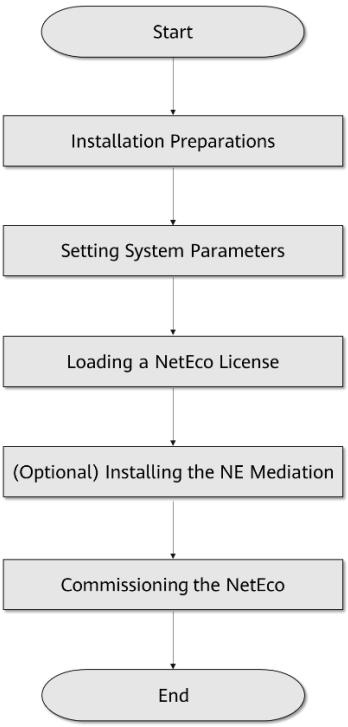


Figure 3-1 Installation process in the preinstallation scenario

3.2 Preparing for the Installation

3.2.1 Server Planning

In the NetEco system software preinstallation scenario, delivery engineers need to learn about the preinstallation information and related operations before the configuration.

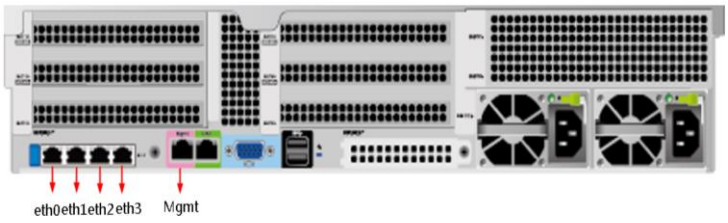
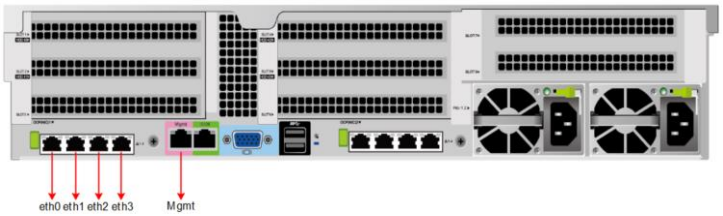
3.2.1.1 Host name preinstallation plan

The default host name is **osssvr**. You can plan the host name based on the site requirements or retain the default value. To ensure that the NetEco works properly, the host name must meet the following rules and restrictions if you need to change the host name:

- The value must be unique on the network.
- The host name consists of letters (A to Z or a to z), digits (0 to 9), and hyphens (-). The first character of the host name must be a letter.
- The host name can contain uppercase letters and lowercase letters.
- The host name cannot contain a single character. That is, the host name must contain at least two characters.
- The host name contains a maximum of 24 characters.

3.2.1.2 Network port preinstallation plan

Table 3-1 Server Network Port Planning

Server Type	Planning Example	Planning Description
TaiShan 200 server (model: 2180)		eth0 and eth1 form a bond group, and eth2 and eth3 form a bond group to provide services externally. (usually eth0 and eth1) Mgmt: iBMC maintenance network port of a Huawei server.
TaiShan 200 server (model 2280)		

3.2.1.3 IP address preinstallation plan

The IP address must meet the following requirements:

- The IP address must be a static IP address.
- The IP address must be unique on the network.
- Only one IP address can be planned for a network port. Do not plan and configure multiple IP addresses for the same network port.
- The server can communicate with the device properly.
- The server communicates with the web client properly.

Table 3-2 IP address preinstallation parameters

Item	Default IP Address	Explanation
Server IP Address	192.168.8.11	Used to log in to the NetEco.
IP address of the iBMC maintenance network port	192.168.8.10	Used to maintain the TaiShan 200 server.

3.2.1.4 Disk Partition Preinstallation Plan

Table 3-3 Disk partition plan (basic configuration: 2 x 1200 GB hard disks)

Server	Disk Sequence	RAID	Space (GB)	subdivision	Partition Name	Size (GB)	File system
TaiShan 200 server (model: 2180) basic configurations	1-2	1	1200	sda1	/boot/efi	1	ext4
				sda2	/boot	1	
				sda3(lvm)vg_root	/	20	
					swap	32	
					/home	1	
					/tmp	10	
					/var	5	
					/var/log	10	
					/var/log/audit	2	
					/usr	5	
					/var/tmp	5	
				sda4(lvm)vg_root	/opt	Remaining	

						space	

Table 3-4 Disk partition plan (standard configuration: 2 x 1200 GB + 8 x 1800 GB)

Server	Disk Sequence	RAID	Space (GB)	subdivision	Partition Name	Size (GB)	File system
TaiShan 200 server (model: 2180) basic configurations	1-2	1	1200	sda1	/boot/efi	1	ext4
				sda2	/boot	1	
				sda3(lvm)vg_root	/	20	
					swap	32	
					/home	Remaining space	
					/tmp	10	
					/var	5	
					/var/log	10	
					/var/log/audit	2	
					/usr	5	
					/var/tmp	5	
	3-10	10	7200	sdb(lvm)ossvg	/opt	Remaining space	

3.2.1.5 Installation path preinstallation plan

Table 3-5 Installation path preinstallation parameters

Item	Preinstallation Path	Explanation
NetEco	/opt/oss	The NetEco software cannot be installed in the root directory. The NetEco installation directory and its path cannot contain letters, digits, and underscores (_). The path must start with a letter or underscore (_). The length of the absolute path cannot exceed 50 characters.

3.2.1.6 User name and password preinstallation plan

Remember the password of the NetEco user. Otherwise, you may need to reinstall the NetEco.

Table 3-6 iBMC user name and password

User name	Initial password	Explanation
Administrator	Admin@90000	iBMC administrator who remotely maintains servers.

Table 3-7 Operating system user name and password

User name	Initial password	Explanation
root	Changeme_123	Operating system administrator. This user is used to log in to the OS and run all commands.
ossadm	Changeme_123	Operating system user. This user is created when the operating system is installed. It is used to install, start, stop, and manage product software.
ossuser	Changeme_123	Operating system user. This user is created when the operating system is installed. It is used to install, upgrade, and routinely maintain product software.
backupuser	Changeme_123	Backup account.

Table 3-8 NetEco GaussDB 100 V3 database users and passwords

User name	Initial password	Explanation
sys	Admin@123	Administrator user, which is used to modify database configurations, add, delete, modify, and query users and databases, and change user passwords. Only local login is allowed.
{ossdbuser} and ossdbuser	Changeme_123	Application read/write user. This user is used to read, write, create, and delete database tables using database services. {ossdbuser} indicates the application database name. Each application database name corresponds to a user.
switchdbuser	321_emegnahC	Switchover management user, which is used to switch over the database and set the database to read-only.
readdbuser	Changeme@123	Read-only O&M user, which is used to read database status and configure data.

public	N/A	Preset database user. A preset public user (incapable of logging in to the database). It is a set of all database users. If a permission is granted to public, all database users can have the permission. To ensure database data security, do not grant object permissions to user public.

Table 3-9 PowerEcho Web User and Password

User name	Initial password	Explanation
admin	Changeme_123	When you log in to the newly installed PowerEcho system for the first time, the system prompts you to change the initial password of the user.

Table 3-10 NetEco user name and password

User name	Initial password	Explanation
admin	Changeme_123	When you log in to the newly installed NetEco for the first time, the system prompts you to change the initial password of the user.

3.2.2 Obtaining the NetEco Software License

The license of the NetEco software is not provided with the software. Therefore, you need to prepare the license of the NetEco software before commissioning. Engineers can apply for the NetEco software license by referring to iManager NetEco 6000 License Application Guide.

3.2.3 Obtaining the Mediation Software Installation Package

Obtain the mediation software installation package in advance to prepare for the installation of the mediation software. Engineers can find the mediation software installation package in the iManagerNetEco6000_Mediation_pkgs_x.x.x file based on the NE type and version in the iManager NetEco 6000 V600R009 Version Mapping and Access Table. After the software package is downloaded, use the digital certificate and verification tool provided at support.huawei.com to verify the digital signature of the software package. (You need to apply for the iManagerNetEco6000_Mediation_pkgs_x.x.x file based on the project information.)

- On the NetEco software download page, download the .asc digital signature file with the same name as the installation package.
- Use the digital certificate and verification tool provided at support.huawei.com to verify the digital signature of the software package.

3.2.4 Powering On Devices

Perform the following steps to check and power on the NetEco server:

Step 1 Check that the power cables and ground cables of each component are securely connected, the polarities are correct, and the contact is good.

Step 2 Ensure that the input power of the PDB is turned off. Use a multimeter to measure the resistance between each output power supply and between the working ground and the protection ground. There is no short circuit between each output power supply or between the working ground and the protection ground.

Step 3 Turn on the power switch of the cabinet.

Step 4 Turn on the circuit breaker on the power distribution box. The hardware devices in the cabinet are powered on.

Step 5 Press the power button on the server chassis panel to power on the server.

After the server is started, the power button/indicator of the server is green.

3.3 Setting System Parameters - Deployment Commissioning

3.3.1 Logging In to PowerEcho

The network connection between the PC and the PowerEcho client is normal. The PowerEcho provides only one admin user. This user has all operation rights on the PowerEcho Web page.

Step 1 Open a web browser, enter https://PowerEcho client login IP address:31945 in the address box, and press Enter.

Step 2 On the login page, enter the user name and password, and click Log In. After logging in to the PowerEcho for the first time, change the password as prompted. If the admin user enters incorrect passwords for five consecutive times within 10 minutes, the login IP address will be locked for 10 minutes.

3.3.2 Deployment commissioning

Step 1 On the PowerEcho main menu, choose Commissioning > Deployment Commissioning.

Step 2 Select NetEco and click Deployment Commissioning.

Step 3 Commission the following system parameters in sequence:

- Commissioning preview: Export and archive the current system configuration information.

- (Optional) Change the password of the operating system user. To ensure system security, change the initial password and keep the new password secure.
- (Optional) Change the password of the database user. To ensure system security, change the initial password and keep the new password secure.
- Configure the time zone and time: Ensure that the node time is the same as the NTP server time to ensure that each node can properly synchronize time with the NTP server. If the time zone of the node is different from that of the NTP server, change the time zone to be the same.
- Configure NTP: Add an NTP server to ensure time consistency between nodes.
- Change the host name: (Optional) Set it to the planned host name.
- (Optional) Set IP Address to the planned IP address.
- Configure Route: (Optional) Set this parameter to the planned route.
- (Optional) Updating the ER certificate: (Optional) To ensure communication security, apply for a certificate from the CA and update the preconfigured ER certificate.
- (Optional) Set backup parameters. After setting backup server parameters and backup file storage policies, you can save backup files to the corresponding backup server. By default, the master server is configured as the backup server. In the single-node system scenario, data is backed up to the local host by default. If you want to back up data to the local host, you are advised to use the backupuser user. The backup path is root directory of the backup server user/Path specified in backup parameters, for example, /opt/neteco_backup/. If data is backed up to another host, the customer needs to provide the IP address, user name, password, and backup path.
- Configuring a scheduled backup task: No commissioning is required. After the product planning data package is imported, the system automatically creates a scheduled backup task for the product.
- Commissioning summary: Check whether commissioning operations are complete and whether the current system configuration is correct.

If the system displays a message indicating that **The product service and product database are running or partially running**, you are advised not to select **Automatically start product database and product service after modification** and click **OK**, after all commissioning tasks are complete, start the product database and product services.

Step 4 (Optional) Start the service and database on the product node.

- Choose **Product > System Monitoring** from the main menu of PowerEcho.
- In the upper left corner of the System Monitoring page, move the cursor to and select the NetEco product.
- In the upper left corner of the page, click **Start** and select **Start All** from the drop-down list.

Step 5 Check the commissioning result.

- Check whether the tasks generated for each commissioning item are successfully executed.
  - On the PowerEcho main menu, choose **System > Task List**.
  - On the **Task** List page, check whether the status of each task is Execution Succeeded. If the status is **Execution Succeeded**, the commissioning is successful.
- Check whether the product service is running properly.
  - Choose **Product > System Monitoring** from the main menu of PowerEcho.
  - On the **System Monitoring** page, check whether the status of each service on the **Nodes** tab page is **Running**. If the status is **Running**, the system has been commissioned successfully.

3.4 Logging In to the NetEco

The NetEco works in browser/server (B/S) mode. Users need to use a browser to log in to the NetEco.

Step 1 In the address box of the browser, enter ***https://IP address of the NMS:31943*** and press Enter.

- The Chrome or Firefox browser is recommended.
- The optimal resolution is 1920 x 1080.

Step 2 Enter the user name and password, and click Log In.

- When you log in as the admin user for the first time, the system prompts you to change the password. Change the password as required and remember it.
- If you enter incorrect passwords for three consecutive times, you need to enter the verification code for the fourth time. If you enter incorrect passwords for five consecutive times, the user or IP address will be locked for 10 minutes.

3.5 Loading a License

The NetEco license file controls the functions and management capabilities of the NetEco. Before using the NetEco, load a commercial license. For details, see.3.2.2 Obtaining the NetEco Software License.

Step 1 Log in to the NetEco client and click **Import License**.

Step 2 Click  next to the **License** file text box, select a license file, and click **Upload**.

Step 3 After the upload is complete, click **Apply**.

3.6 (Optional) Installing the NE Mediation

Obtain the NE mediation installation package by referring to section 3.2.3 Obtaining the Mediation Software Installation Package.

Step 1 Choose System > Service Settings > Adapter Management.

Step 2 Click **Upload**. On the displayed **Upload adapter package** page, click **+** and select the files to be uploaded.

Step 3 Click **Upload** to upload the files.

Step 4 Select the NE mediation packages to be installed on the **Adapter Management** page and click **Install**. Then click **Yes** in the displayed dialog box. In the displayed Confirm dialog box, click **OK**.

3.7 Configuring NetEco System Security

Configure the NetEco system security based on the site requirements, including:

- Configuring Reauthentication.
- Replacing a Security Certificate for Connection between NetEco and NE.
- Replacing a Northbond Certificate.
- Replacing the influxdb client Certificate.
- Replacing the influxdb server Certificate
- Replacing the FTPS Certificate.

For details, see iManager NetEco6000 Product Documentation.

3.8 Commissioning the NetEco

This section describes how to install and deploy the NetEco software. For details about how to install the NetEco software, see Huawei NetEco Operation Lab Guide.

4 New installation scenario

4.1 Installation Process

The following figure shows the NetEco software installation and deployment process in the EulerOS installation scenario.

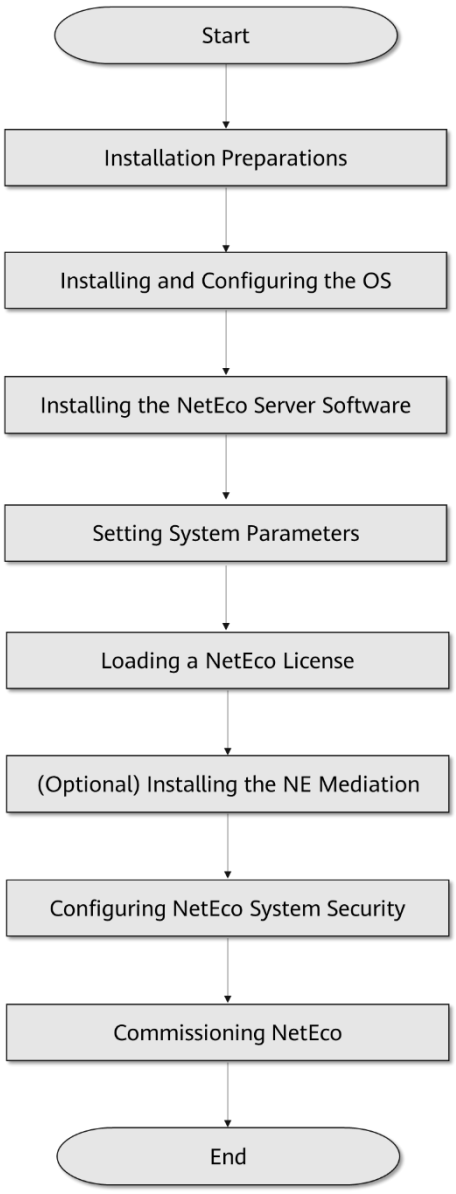


Figure 4-1 New installation process

4.2 Preparing for the Installation

4.2.1 Server Planning

Before installing the NetEco server, plan the installation information, such as the user name, IP address, and password of the NetEco server, to quickly and correctly install the NetEco server.

4.2.1.1 Host name planning

The default host name is osssvr. You can plan the host name based on the site requirements or retain the default value. To ensure that the NetEco works properly, the host name must meet the following rules and restrictions if you need to change the host name:

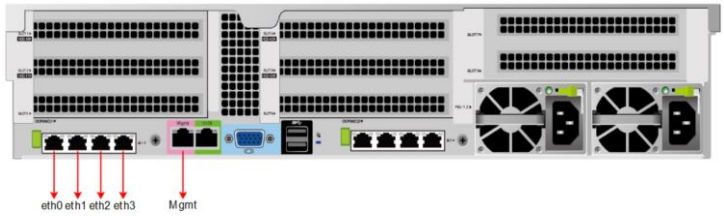
- The value must be unique on the network.
- The host name consists of letters (A to Z or a to z), digits (0 to 9), and hyphens (-). The first character of the host name must be a letter.
- The host name can contain uppercase letters and lowercase letters.
- The host name cannot contain a single character. That is, the host name must contain at least two characters.
- The host name contains a maximum of 24 characters.

Table 4-1 Host name planning

Server	Item	Planning Example
NetEco server 1	Host name	neteco-1
NetEco server 2	Host name	neteco-2
NetEco server 3	Host name	neteco-3

4.2.1.2 Network port planning

Table 4-2 Server Network Port Planning

Server Type	Planning Example	Planning Description
TaiShan 200 server (model 2280)		eth0 and eth1 form a bond group, and eth2 and eth3 form a bond group to provide services externally. (usually eth0 and

		eth1) Mgmt: iBMC maintenance network port of a Huawei server.

4.2.1.3 IP Address Planning

The IP addresses of the NetEco system devices must be planned based on the actual network conditions.

The IP address must meet the following requirements:

- The IP address must be a static IP address.
- The IP address must be unique on the network.
- Only one IP address can be planned for a network port. Do not plan and configure multiple IP addresses for the same network port.
- The server can communicate with the device properly.
- The server communicates with the web client properly.

Table 4-3 IP address preinstallation parameters

Device	Item	Default IP Address	Explanation
NetEco server 1/2/3	Server IP Address	192.168.8.11	This parameter must be modified. Used to log in to the NetEco.
	IP address of the iBMC maintenance network port	192.168.2.100	This parameter is optional. Used to maintain the TaiShan 200 server. The default iBMC IP address is 192.168.2.100. If preinstallation has been performed onsite, change the value to 192.168.8.10. Replace it with the actual address.

4.2.1.4 Disk Partition Planning

Table 4-4 Disk partition plan (standard configuration: 2 x 1200 GB + 8 x 1800 GB)

Server	Disk Sequence	RAID	Space (GB)	subdivision	Partition Name	Size (GB)	File system
TaiShan 200	1-2	1	1200	sda1	/boot/efi	1	ext4
				sda2	/boot	1	

server (model: 2180) basic configurations				sda3(lvm)vg_root	/	20	
					swap	32	
					/home	Remaining space	
					/tmp	10	
					/var	5	
					/var/log	10	
					/var/log/audit	2	
					/usr	5	
					/var/tmp	5	
	3-10	10	7200	sdb(lvm)ossvg	/opt	Remaining space	

4.2.1.5 User name and password planning

Remember the password of the NetEco user. Otherwise, you may need to reinstall the NetEco.

Table 4-5 iBMC user name and password

User name	Initial password	Explanation
Administrator	Admin@90000	iBMC administrator who remotely maintains servers.

Table 4-6 Operating system user name and password

User name	Initial password	Explanation
root	Changeme_123	Operating system administrator. This user is used to log in to the OS and run all commands.
ossadm	Changeme_123	Operating system user. This user is created when the operating system is installed. It is used to install, start, stop, and manage product software.
ossuser	Changeme_123	Operating system user. This user is created when the operating system is

		installed. It is used to install, upgrade, and routinely maintain product software.
backupuser	Changeme_123	Backup account.

Table 4-7 NetEco Redis database users and their passwords

User name	Initial password	Explanation
dbuser	Admin@123	Database administrator. Used to log in to the database of the node and run all commands.
ossdbuser	Changeme_123	Common user. Reads and edits database data, and creates and deletes database tables.
readdbuser	Changeme@123	Read-only user. Reads the database status, database configuration, and database data.

Table 4-8 NetEco GaussDB 100 V3 database users and passwords

User name	Initial password	Explanation
sys	Admin@123	Administrator user, which is used to modify database configurations, add, delete, modify, and query users and databases, and change user passwords. Only local login is allowed.
{ossdbuser} and ossdbuser	Changeme_123	Application read/write user. This user is used to read, write, create, and delete database tables using database services. {ossdbuser} indicates the application database name. Each application database name corresponds to a user.
switchdbuser	321_emegnahC	Switchover management user, which is used to switch over the database and set the database to read-only.
readdbuser	Changeme@123	Read-only O&M user, which is used to read database status and configure data.
public	N/A	Preset database user. A preset public user (incapable of logging in to the database). It is a set of all database users. If a permission is granted to public, all database users can have the permission. To ensure database data security, do not grant object

		permissions to user public.

Table 4-9 PowerEcho Web User and Password

User name	Initial password	Explanation
admin	Changeme_123	When you log in to the newly installed PowerEcho system for the first time, the system prompts you to change the initial password of the user.

Table 4-10 NetEco user name and password

User name	Initial password	Explanation
admin	Changeme_123	When you log in to the newly installed NetEco for the first time, the system prompts you to change the initial password of the user.

4.2.2 Obtaining Installation Software

Download the NetEco installation software package from support.huawei.com. You need to apply for some software based on project information.

4.2.3 Obtaining the Mediation Software Installation Package

For details, see 3.2.3 Obtaining the Mediation Software Installation Package.

4.2.4 Powering On Devices

For details, see 3.2.4 Powering On Devices.

4.3 Installing and Configuring the Operating System

The EulerOS is installed and configured using the automatic installation and configuration scripts in the quick installation CD-ROM.

If a 4G SMS modem is used, ensure that the 4G SMS modem is disconnected from the NetEco server (that is, disconnect the cable from the NetEco server) before performing operations in this section. After performing operations in this section, reconnect the 4G SMS modem to the NetEco server.

4.3.1 Configuring and Using the Remote Management Port

This port is used by engineers to remotely start and manage the server. Before using the remote management port, you need to configure the IP address of the remote management port.

4.3.1.1 Configuring iBMC Parameters

The iBMC remote management system of the server provides the function of remotely managing and monitoring the server. To securely access the iBMC remote management system of the server, you need to set parameters for the iBMC remote management system of the server. If the cluster solution is used onsite, perform this operation on each server.

Step 1 Log in to the iBMC remote management system of the server.

- Set the IP address of the PC to be in the same network segment as the IP address of the remote management port on the NetEco server.
- In the address box of the browser, enter the default IP address https://192.168.2.100 and press Enter. The login page of the iBMC remote management system is displayed.
- The default IP address is 192.168.2.100. If preinstallation has been performed onsite, change the value to 192.168.8.10. If the IP address is changed to the planned IP address, use the actual IP address.
- Enter the initial user name (**Administrator**) and password (**Admin@9000**), and click **Log In**. The homepage of the iBMC remote management system is displayed.

Step 2 Configure the iBMC remote management port (iBMC 3.XX is used as an example).

- On the menu bar, choose **Configuration**. In the navigation pane, choose **Network** Configuration.
- In the Select IP Version and Configure IP area, set IP Protocol to **IPV4** or **IPV4/IPV6**.
- In the **IPv4** area, select **Manually set IP Address**.
- Specify **IP Address, Subnet Mask,** and **Default Gateway** to the planned iBMC remote management port. Click **Save**.

Step 3 Configure System Startup Items.

- On the menu bar, choose **Configuration**. In the navigation pane, choose **Boot Device**.
- Set the **Effective of the boot medium** to one-time, and the boot medium to **DVD-ROM drive**. Click **Save**.

Step 4 Change the user password of the iBMC remote management system.

- In the navigation pane on the left, choose **Local Users**.
- Locate the row that contains **Administrator**, and click  in the **Operation** column.
- Enter the old password in **Current User Password**.
- Select **Change Password**.
- Enter the new password in **Password and Confirm**. Click **Save**.

Step 5 Change the iBMC time zone.

- On the menu bar, choose **Configuration**. In the navigation pane, choose **Network Configuration**.
- In the **Set Time Zone** area, set the iBMC time zone based on the site requirements and click **Save**.

4.3.1.2 Configuring Server Disks

You need to configure the physical disks that are connected to the RAID card of the server as logical disks when the operating system is installed for the first time before the delivery of the server or before the operating system is reinstalled because the hard disks are replaced. In this case, you need to perform operations described in this section.

TaiShan 200 server (model 2280) is used as an example.

Step 1 Disable the JBOD. On the iBMC home page, choose **Information** from the main menu. In the navigation pane, choose **System Info**. On the **System Info** page, choose **Storage > Configure**. In the **RAID Controller** area, select **Disable** from the **JBOD State** drop-down list box and click **Save**.

- JBOD: Just a Bundle of Disks. Multiple disks are stacked to provide storage resources. No RAID policies are supported.

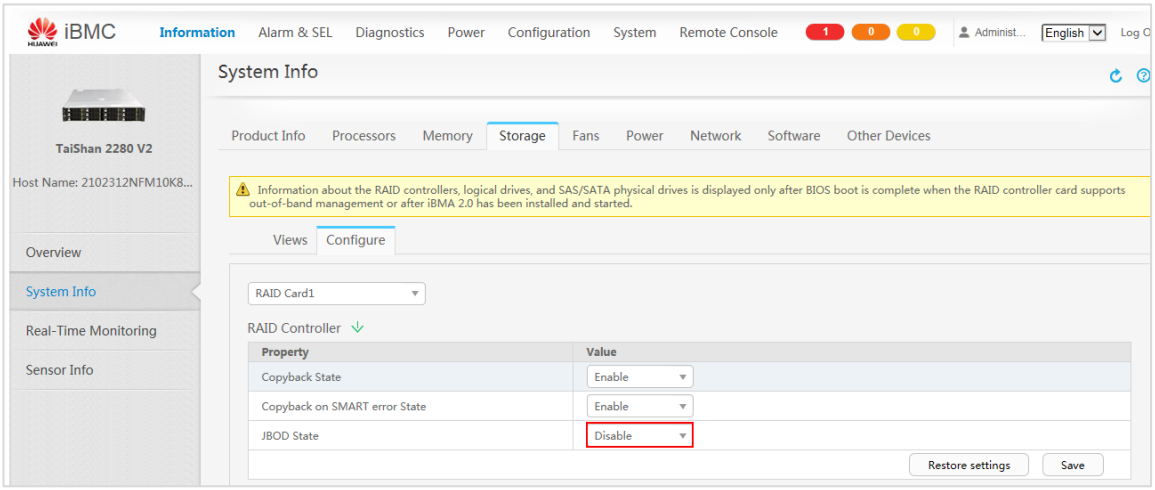


Figure 4-2 Disabling JBOD

Step 2 On the System Info page, choose Storage > View.

- The number of disks is sorted by Disk0. The number of disks is displayed as the number of disks.
- The TaiShan 200 server (model 2280) (standard configuration) has two 1200 GB hard disks and eight 1800 GB hard disks.
- If the information shown in Figure 4-3 is displayed, the disk of the server is initialized. Go to step 4 to partition the disk space.

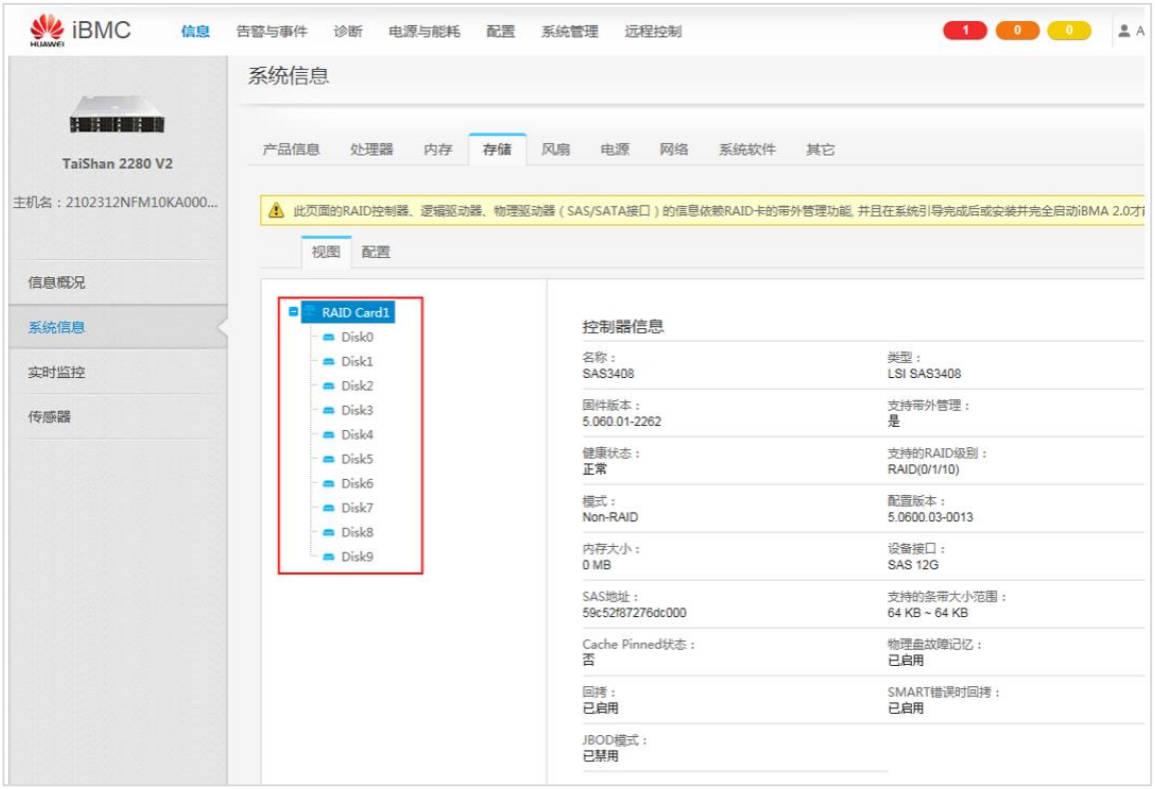


Figure 4-3 System Information

- If the information shown in Figure 4-4 is displayed, disk space has been allocated to the server disk. Go to step 3 to initialize the server disk to prepare for disk space reconfiguration.

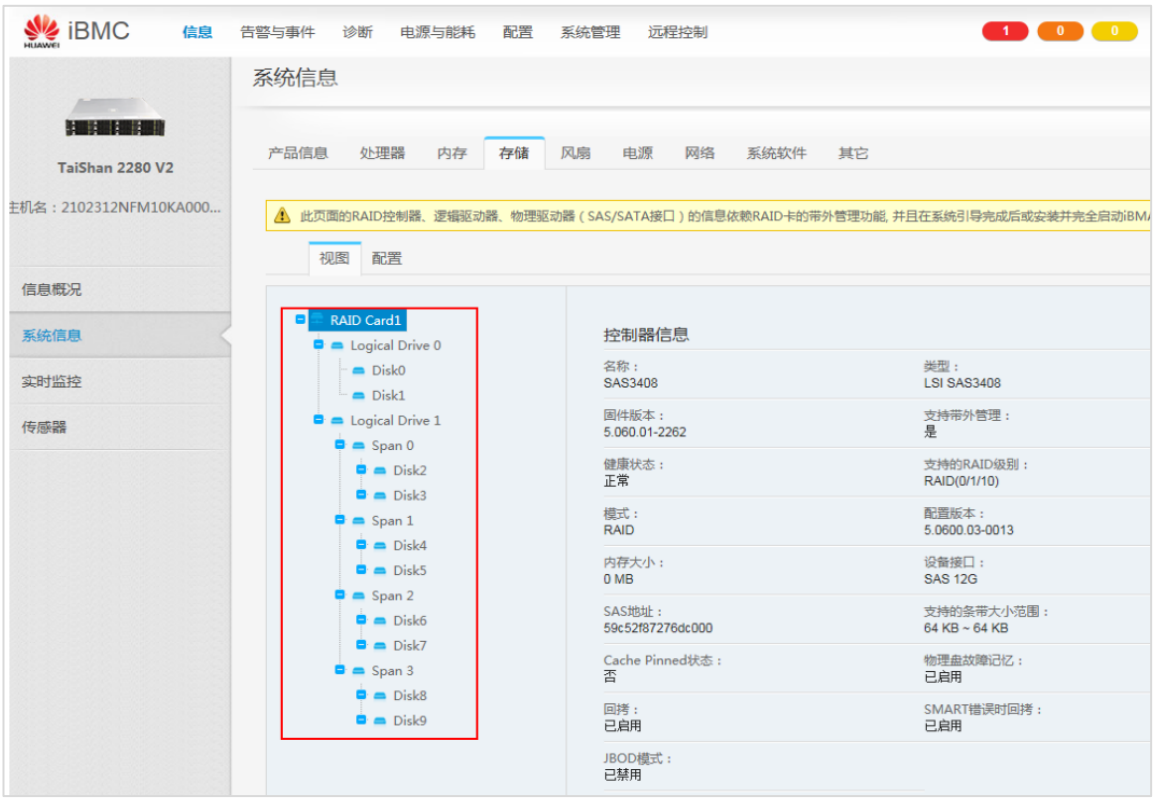


Figure 4-4 System Information

Step 3 Initialize the server disks to prepare for disk reconfiguration.

- Click the Configure tab.
- Click → next to **Logical Drive.**
- Click Delete, select all entries where a RAID is configured, and click **Save**.

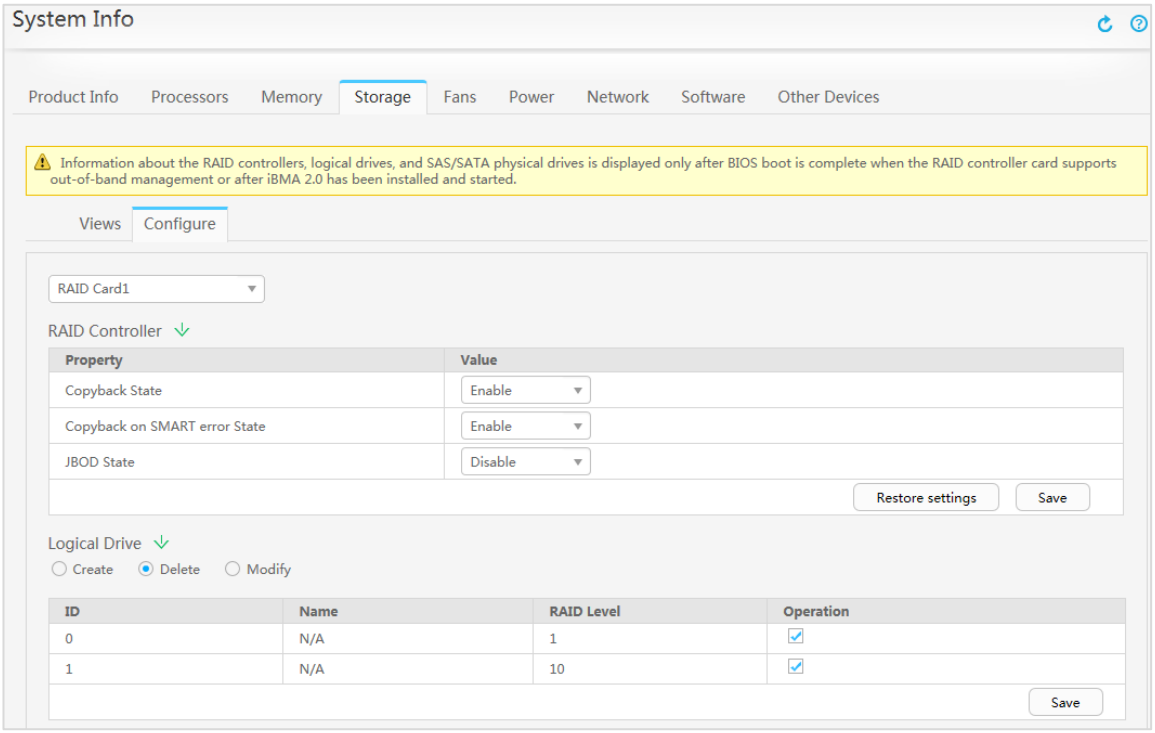


Figure 4-5 Delete the configured logical disk data.

- In the displayed dialog box, click **Yes**. If Operation **Successful** is displayed at the top, the operation is complete.

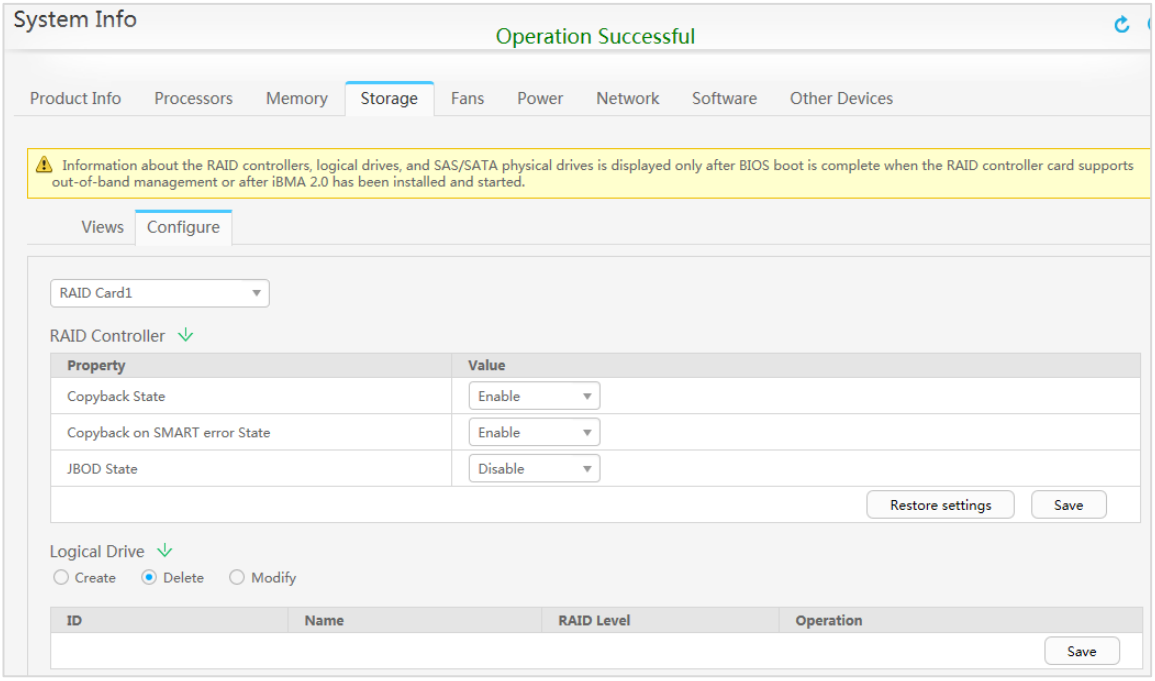


Figure 4-6 Disk initialization completed

Step 4 Partition RAID 1 and RAID 10 logical drives, and set RAID 1 logical drive as the boot disk.

- Choose the Configure tab.
- Click → next to **Logical Drive.**
- Partitioning RAID 1 logical drive and setting it as the boot disk.
  - Click **Create**, set **Initialization State** to **Quick Init**, Level to **1**, select **Disk0** and **Disk1** for **Disk**, and click **Save**.

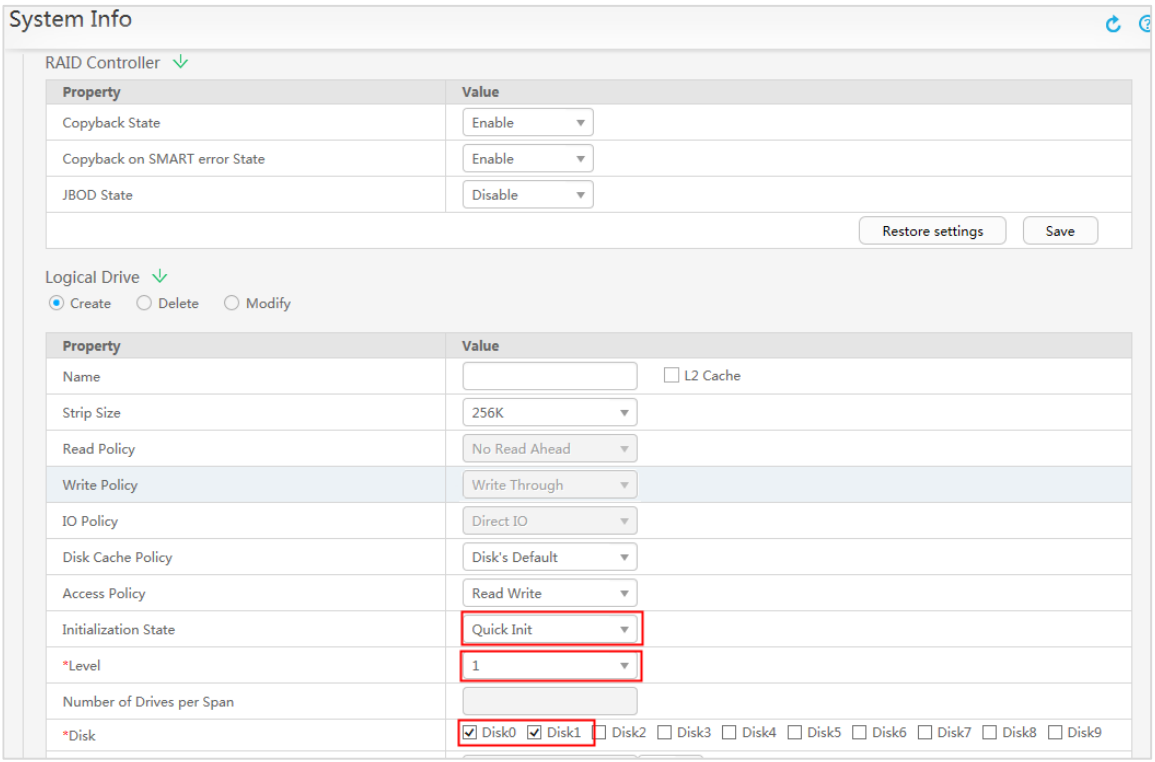


Figure 4-7 Creating RAID1 Logical Disks

- In the dialog box that is displayed, click **YES**. If the message "**Operation successful**" is displayed, the operation is complete.
- Click **Modify**, set **Boot Disk** to **Yes**, and click **Save**.

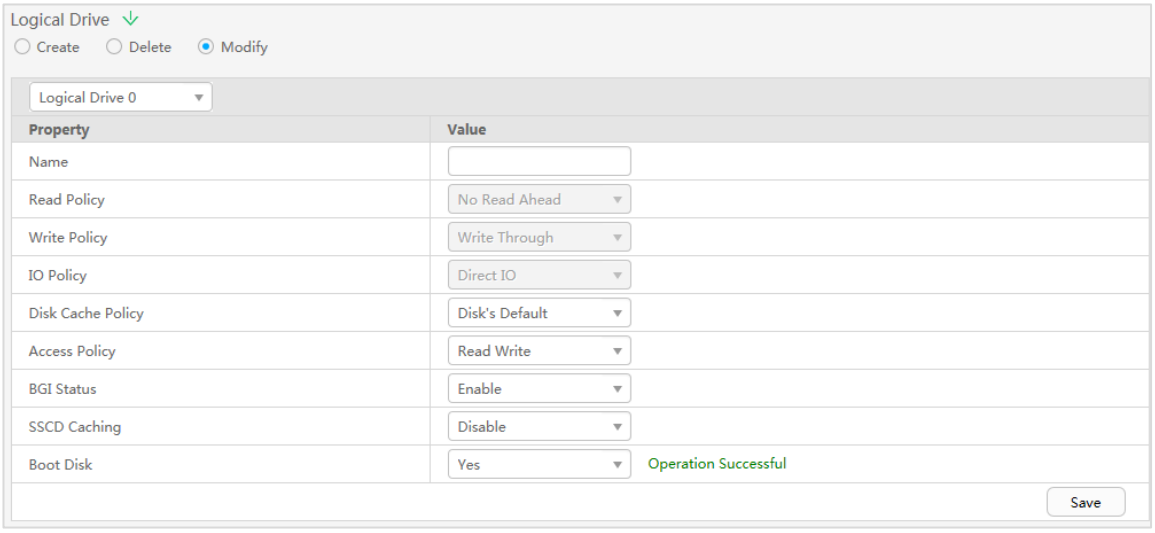


Figure 4-8 Set as the boot disk.

- In the displayed dialog box, click **YES**. If the message "**Operation successful**" is displayed, the operation is complete.

- Partitioning RAID 10 logical drive.
  - Click **Create**, set **Initialization State** to **Quick Init** and Level to **10**, select **Disk2** to **Disk9** for Disk, and click **Save**.

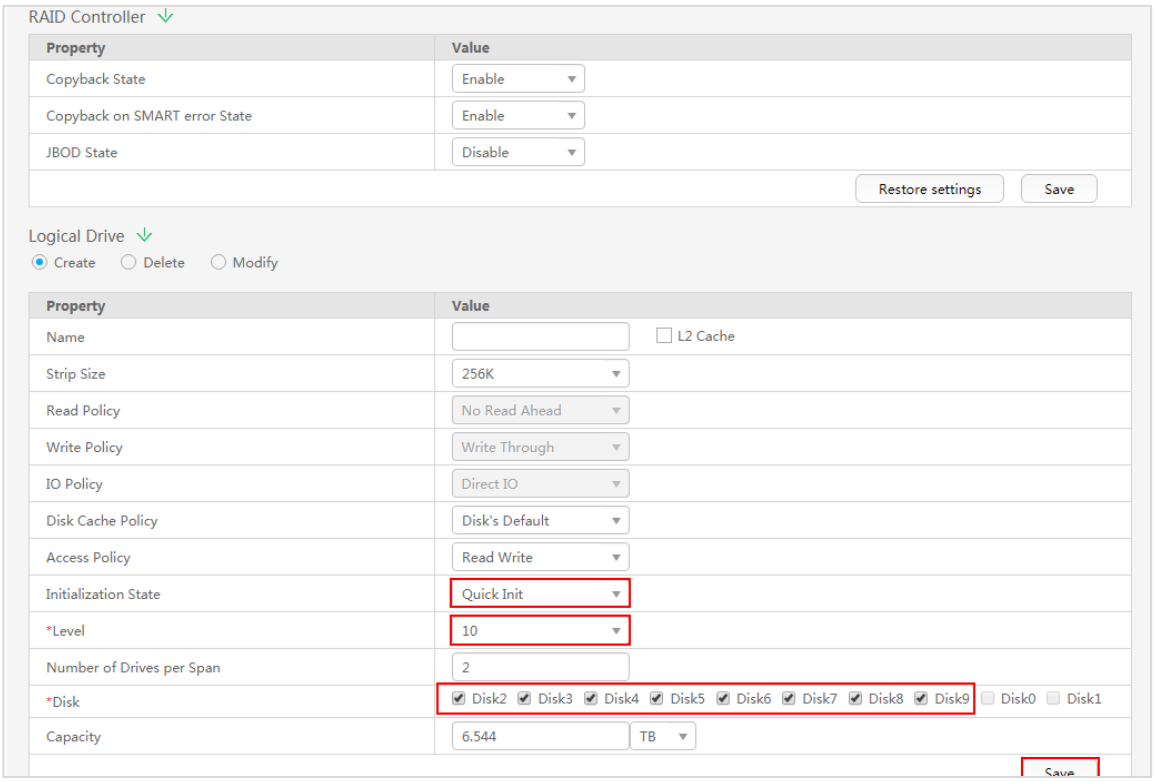


Figure 4-9 Creating RAID 10 Logical Disks

- In the dialog box that is displayed, click **YES**. If the message "**Operation successful**" is displayed, the operation is complete.

Step 5 On the Views tab page, expand the logical drive tree, and confirm the configured disk information.

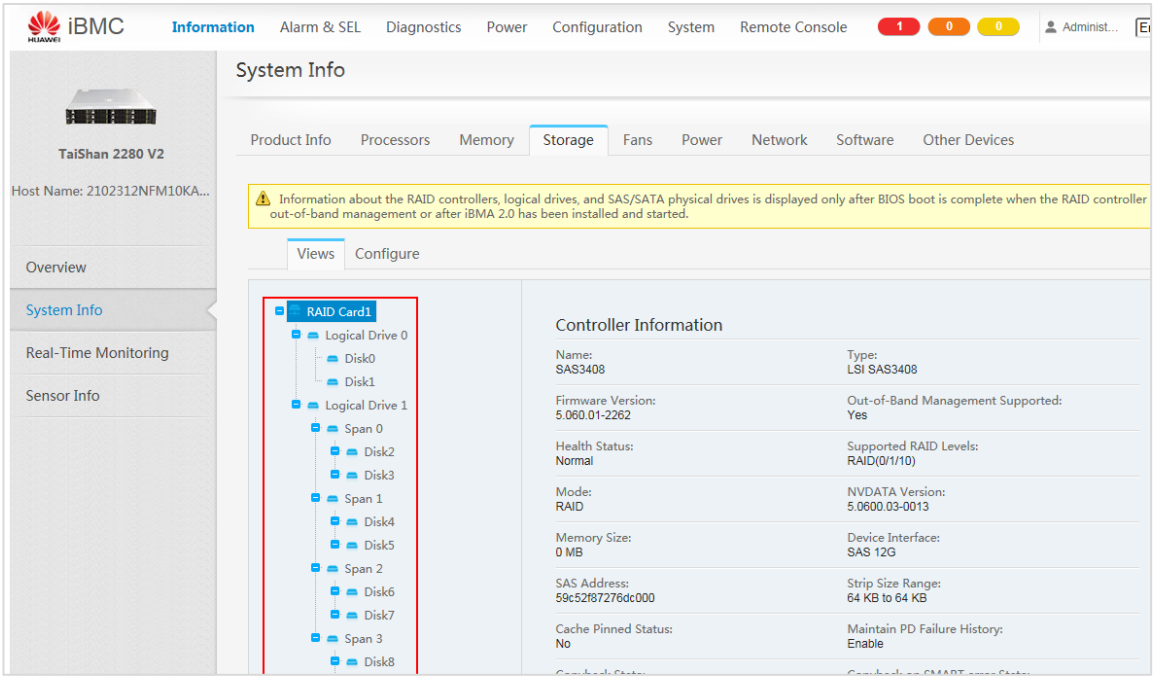


Figure 4-10 Viewing and Confirming the Configured Disk Information

4.3.1.3 Accessing the remote management page of the server

Log in to the remote management page of the server through a browser to manage the server.

Step 1 Run the ping command to check whether the PC is properly connected to the remote management port of the server.

Step 2 Open a web browser on the PC, enter *https://IP address of the remote management port* in the address box, and press Enter. The remote management login page is displayed.

Step 3 Enter the user name **Administrator** and its password, and click **Login**.

Step 4 Choose Remote Control from the main menu. On the Remote Control page, choose HTML5 Integrated Remote Console (Private).

4.3.1.4 Mounting the ISO file

Mount the ISO file on the PC to the server through the remote management port. If the cluster solution is used onsite, perform this operation on each server.

Copy the image file OS_EulerOS2.0SPXX_arm64_X.X.X.iso of the installation CD-ROM to the PC in advance.

Step 1 Click  in the upper part of the screen. The dialog box shown in Figure 4-11 is displayed.

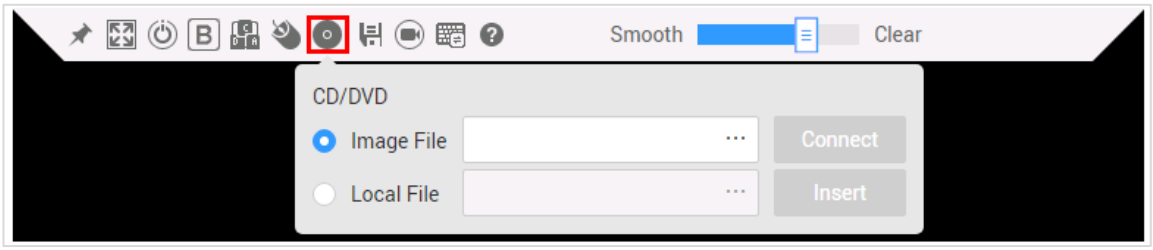


Figure 4-11 CD Options

Step 2 Select Image File.

Step 3 Click Select LocalPCImage file of the VM.isoFor details about how to obtain the image package, see.1.3 NetEco System software package and tool software.

Step 4 Click **Connect**.

- When the Connect button changes to Disconnect, the DVD-ROM is loaded to the server.
- Do not click Eject while loading the CD-ROM.
- If you need to select an image file again after the loading is complete, click Eject to upload the new image package.

4.3.2 Installing the OS

Use the quick installation DVD-ROM to install EulerOS. If the cluster solution is used onsite, perform this operation on each server.

Step 1 Click  on the top of the iBMC management page and select CD/DVD-ROM Drive.

Step 2 Click  in the upper part of the iBMC management page and select Forcibly Restart.

Step 3 After the server is restarted, the Boot Options screen is displayed, as shown in Figure 4-12. Select Install EulerOS V2.0SPXX and press Enter.

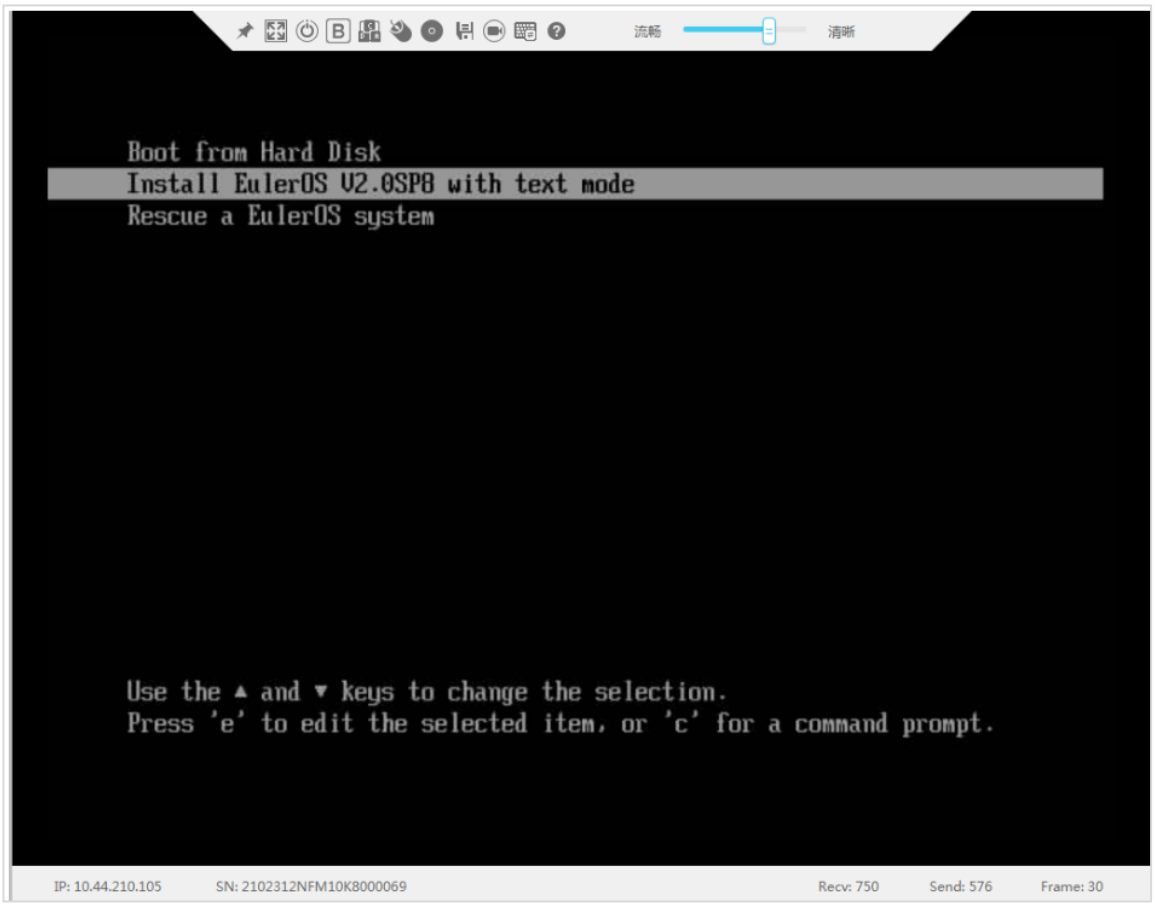


Figure 4-12 Boot Options

- During the installation, the server automatically restarts. No manual intervention is required.
- The EulerOS installation takes about 40 minutes.
- The IP address of the server is 192.168.8.11 by default according to the system plan.

Step 4 If the information shown in Figure 4-13 is displayed during the installation, the OS is successfully installed.

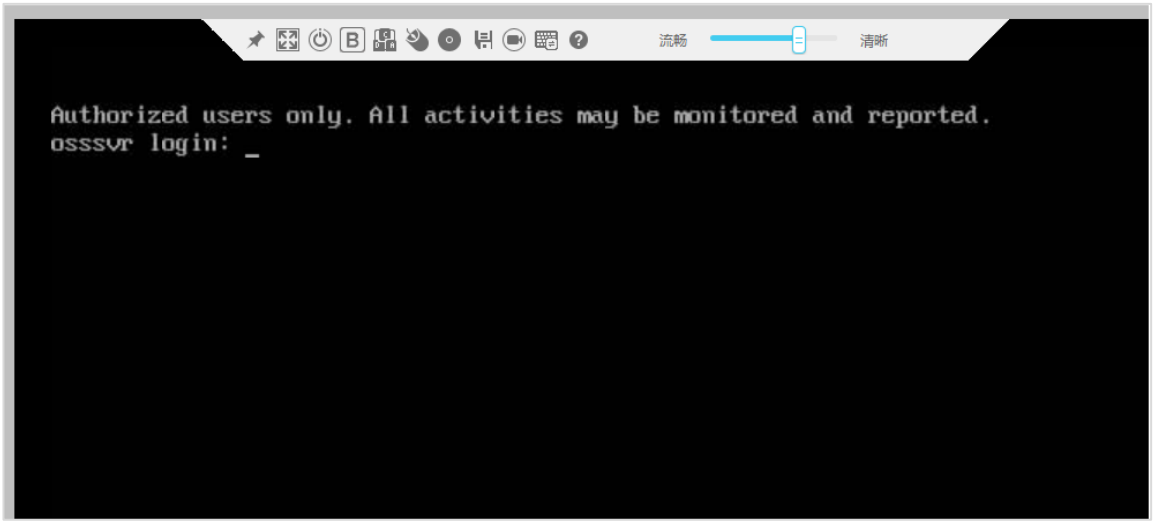


Figure 4-13 Installing the OS

Step 5 After the OS is installed, use the root user name and password of the EulerOS to log in to the server, as shown in Figure 4-14.

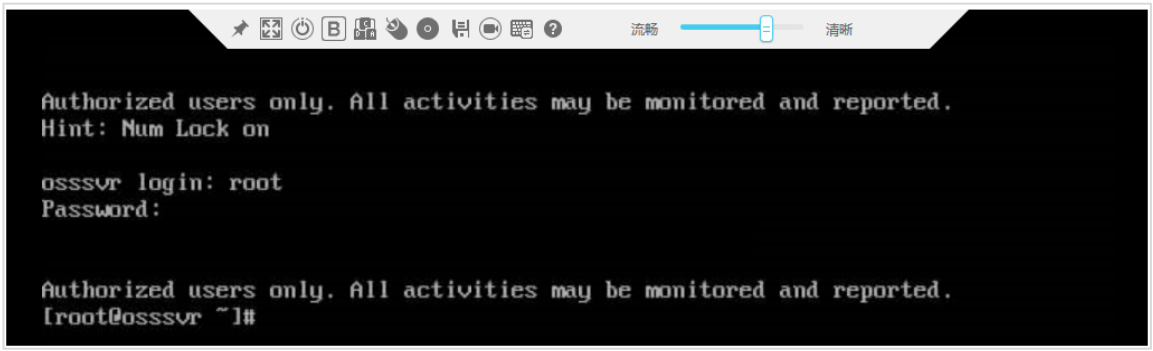


Figure 4-14 Login page

4.3.3 Configuring the Server IP Address

Change the IP address according to the actual plan.

You must log in to the server as the root user before performing this operation.

Step 1 Change the IP address according to the actual plan.

```
# cd /usr/local/PlatformTools
# ./modifyip.sh
```

- The ./modifyip.sh script can be used only when the NMS software is not installed. If the NMS software is installed, change the server IP address on the PowerEcho.

Please input IP address [Current IP:192.168.8.11]:

- When the preceding information is displayed, enter the IP address and press Enter.

Please input net masks [Current Netmask:255.255.255.0]:

- When the preceding information is displayed, enter the subnet mask and press Enter.

Please input default route [Current RouteIP:192.168.8.1]:

- When the preceding information is displayed, enter the gateway and press Enter.
- If the following information is displayed, the IP address is changed successfully:

Modify IP success.

4.4 Installing the NetEco Software

Obtain the following software packages and tools before the installation:,Obtaining Method,For details, see.1.3 NetEco System software package and tool software:

- iManagerNetEco_DeployTool_V600R020C00XXX_Euler_arm64.zip
- iManagerNetEco_Platform_V600R020C00XXX_Euler_arm64.zip
- iManagerNetEco_Platform_V600R020C00XXX_Euler_arm64.zip.cms
- iManagerNetEco_Platform_V600R020C00XXX_Euler_arm64.zip.crl
- iManagerNetEco6000_V600R009C00XXX_Euler_arm64.zip
- iManagerNetEco6000_V600R009C00XXX_Euler_arm64.zip.cms
- iManagerNetEco6000_V600R009C00XXX_Euler_arm64.zip.crl
- PuTTY
- FileZilla tool

Step 1 Log in to the NetEco server as user ossadm using PuTTY.

Step 2 Run the following commands to switch to user root and create the /opt/install directory:

```
# su - root
Password: root password
```

- After you switch to the root user, "root@host name:~ #" is displayed.
- The default password of user root is Changeme_123.

```
# mkdir /opt/install
# chown -h ossadm:ossgroup /opt/install
```

Step 3 Use FileZilla to upload the software packages obtained in the prerequisites to the /opt/install directory on the NetEco server.

- User name and password: ossadm and its password.
- Port: Port 22 is used by default for SFTP.
- IP address: fixed physical IP address of the host.

Step 4 Run the following commands to decompress the deployment tool:

```
# chown -Rh root:root /opt/install
# chmod 700 /opt/install
# cd /opt/install
# unzip iManagerNetEco_DeployTool_V600R020C00XXX_Euler_arm64.zip
```

- iManagerNetEco_DeployTool_V600R020C00XXX_Euler_arm64.zip is only an example. Replace it with the actual software package name.

Step 5 Run the following commands to install the NetEco software:

```
# screen -S "install_ha.sh" bash /opt/install/install_ha.sh
============================================================
Please select a Installation language:
1--zh
2--en
Q--Exit
============================================================
Please make a choice:
```

- Enter a number to select the installation language as prompted and press Enter.

```
Please input the first node IP address:
```

- Enter the IP address of NetEco server 1 as prompted and press Enter.

```
Please input the second node IP address:
```

- Enter the IP address of NetEco server 2 as prompted and press Enter.

```
Please input the third node IP address:
```

- Enter the IP address of NetEco server 3 as prompted and press Enter.

```
Please input the floating IP address:
```

- Enter the floating IP address of the NetEco server as prompted and press Enter.

```
Make sure the root passwords of all nodes are the same.
Please input the password for root:
```

- Enter the password of user root as prompted and press Enter to start the installation.
- The installation takes about 60 minutes. If the following information is displayed, the installation is successful:

```
Install neteco successfully.
```

- During the installation, the system automatically deploys the PowerEcho and NetEco. Ensure that the server is powered on properly and no manual intervention is required during the installation.

- During the initial installation, you can install the NetEco only in the background. After the PowerEcho is installed, you can install and upgrade the NetEco on the PowerEcho.
- Installing the NetEco in one-click mode takes a long time, including configuring the OS, installing the PowerEcho, installing the database, installing the NetEco, hardening the OS, and installing the cluster monitoring software.
- To return to the original command line, press Ctrl+A and then D.
- If PuTTY is interrupted during the installation, log in to the NetEco server again and switch back to the task session window when PuTTY is interrupted.
- The NetEco installation takes a long time. If you have logged out after the installation, log in to the NetEco server as user ossadm and then run the following command to switch to user root:

```
# su - root
```

Step 6 Run the following command to delete the install directory:

```
# cd /opt
# rm -rf install
```

- Restart NetEco-1, NetEco-2, and NetEco-3 in sequence to prevent switchovers and make security hardening operations during the installation take effect. Run the following command:

```
# sync
# reboot
```

- Do not perform other operations during the restart.
- Log in to the system at least 5 to 10 minutes after the restart.

4.5 Setting System Parameters - Deployment Commissioning

4.5.1 Logging In to PowerEcho

The network connection between the PC and the PowerEcho client is normal. The PowerEcho provides only one admin user. This user has all operation rights on the PowerEcho Web page.

Step 1 Open a web browser, enter https://PowerEcho client login IP address:31945 in the address box, and press Enter.

Step 2 On the login page, enter the user name and password, and click Log In. After logging in to the PowerEcho for the first time, change the password as prompted. If the admin user enters incorrect passwords for five consecutive times within 10 minutes, the login IP address will be locked for 10 minutes.

4.5.2 Deployment commissioning

Step 1 On the PowerEcho main menu, choose Commissioning > Deployment Commissioning.

Step 2 Select NetEco and click Deployment Commissioning.

Step 3 Commission the following system parameters in sequence:

- Commissioning preview: Export and archive the current system configuration information.
- (Optional) Change the password of the operating system user. To ensure system security, change the initial password and keep the new password secure.
- (Optional) Change the password of the database user. To ensure system security, change the initial password and keep the new password secure.
- Configure the time zone and time: Ensure that the node time is the same as the NTP server time to ensure that each node can properly synchronize time with the NTP server. If the time zone of the node is different from that of the NTP server, change the time zone to be the same.
- Configure NTP: Add an NTP server to ensure time consistency between nodes.
- Change the host name: (Optional) Set it to the planned host name.
- (Optional) Set IP Address to the planned IP address.
- Configure Route: (Optional) Set this parameter to the planned route.
- (Optional) Updating the ER certificate: (Optional) To ensure communication security, apply for a certificate from the CA and update the preconfigured ER certificate.
- (Optional) Set backup parameters. After setting backup server parameters and backup file storage policies, you can save backup files to the corresponding backup server. By default, the master server is configured as the backup server. In the single-node system scenario, data is backed up to the local host by default. If you want to back up data to the local host, you are advised to use the backupuser user. The backup path is root directory of the backup server user/Path specified in backup parameters, for example, /opt/neteco_backup/. If data is backed up to another host, the customer needs to provide the IP address, user name, password, and backup path.
- Configuring a scheduled backup task: No commissioning is required. After the product planning data package is imported, the system automatically creates a scheduled backup task for the product.
- Commissioning summary: Check whether commissioning operations are complete and whether the current system configuration is correct.

If the system displays a message indicating that The product service and product database are running or partially running, you are advised not to select Automatically start product database and product service after modification and click OK, after all commissioning tasks are complete, start the product database and product services.

Step 4 (Optional) Start the service and database on the product node.

- Choose **Product > System Monitoring** from the main menu of PowerEcho.
- In the upper left corner of the System Monitoring page, move the cursor to and select the NetEco product.
- In the upper left corner of the page, click **Start** and select **Start All** from the drop-down list.

Step 5 Check the commissioning result.

- Check whether the tasks generated for each commissioning item are successfully executed.
  - On the PowerEcho main menu, choose **System > Task List**.
  - On the **Task** List page, check whether the status of each task is Execution Succeeded. If the status is **Execution Succeeded**, the commissioning is successful.
- Check whether the product service is running properly.
  - Choose **Product > System Monitoring** from the main menu of PowerEcho.
  - On the **System Monitoring** page, check whether the status of each service on the **Nodes** tab page is **Running**. If the status is **Running**, the system has been commissioned successfully.

4.6 Logging In to the NetEco

The NetEco works in browser/server (B/S) mode. Users need to use a browser to log in to the NetEco.

Step 1 In the address box of the browser, enter ***https://IP address of the NMS:31943*** and press Enter.

- The Chrome or Firefox browser is recommended.
- The optimal resolution is 1920 x 1080.

Step 2 Enter the user name and password, and click Log In.

- When you log in as the admin user for the first time, the system prompts you to change the password. Change the password as required and remember it.
- If you enter incorrect passwords for three consecutive times, you need to enter the verification code for the fourth time. If you enter incorrect passwords for five consecutive times, the user or IP address will be locked for 10 minutes.

4.7 Loading a License

The NetEco license file controls the functions and management capabilities of the NetEco. Before using the NetEco, load a commercial license. For details, see.3.2.2 Obtaining the NetEco Software License.

Step 1 Log in to the NetEco client and click **Import License**.

Step 2 Click  next to the **License** file text box, select a license file, and click **Upload**.

Step 3 After the upload is complete, click **Apply**.

4.8 (Optional) Installing the NE Mediation

Obtain the NE mediation installation package by referring to section 3.2.3 Obtaining the Mediation Software Installation Package.

Step 1 Choose System > Service Settings > Adapter Management.

Step 2 Click **Upload**. On the displayed **Upload adapter package** page, click **+** and select the files to be uploaded.

Step 3 Click **Upload** to upload the files.

Step 4 Select the NE mediation packages to be installed on the **Adapter Management** page and click **Install**. Then click **Yes** in the displayed dialog box. In the displayed Confirm dialog box, click **OK**.

4.9 Configuring NetEco System Security

Configure the NetEco system security based on the site requirements, including:

- Configuring Reauthentication.
- Replacing a Security Certificate for Connection between NetEco and NE.
- Replacing a Northbond Certificate.
- Replacing the influxdb client Certificate.
- Replacing the influxdb server Certificate
- Replacing the FTPS Certificate.

For details, see iManager NetEco6000 Product Documentation.

4.10 Commissioning the NetEco

This section describes how to install and deploy the NetEco software. For details about how to install the NetEco software, see Huawei NetEco Operation Lab Guide.

5 Virtual Deployment Scenario

This section is optional.

NetEco V600R009C00 supports virtual deployment. In virtual deployment, the OS and database are installed on VMs, which reduces hardware server deployment and maintenance workload. In the FusionSphere scenario, you need to provide the FusionSphere OpenStack environment. In the FusionCompute scenario, you need to provide the FusionCompute environment.

5.1 Installation Process

The following figure shows the process of installing and deploying the NetEco software in the virtual deployment scenario.

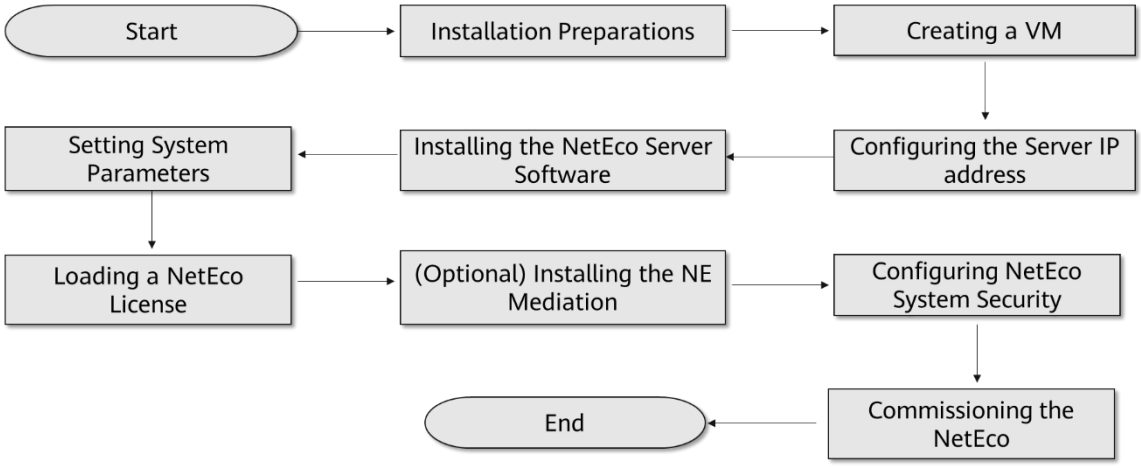


Figure 5-1 Installation process for virtual deployment

5.2 Preparing for the Installation

5.2.1 Server Planning

Before installing the NetEco server, plan the installation information, such as the user name, IP address, and password of the NetEco server, to quickly and correctly install the NetEco server.

5.2.1.1 Host name planning

The default host name is osssvr. You can plan the host name based on the site requirements or retain the default value. To ensure that the NetEco works properly, the host name must meet the following rules and restrictions if you need to change the host name:

- The value must be unique on the network.
- The host name consists of letters (A to Z or a to z), digits (0 to 9), and hyphens (-). The first character of the host name must be a letter.
- The host name can contain uppercase letters and lowercase letters.
- The host name cannot contain a single character. That is, the host name must contain at least two characters.
- The host name contains a maximum of 24 characters.

Table 5-1 Host name planning

Item	Planning Example
NetEco server host name	osssvr

5.2.1.2 VM configuration

Table 5-2 Basic VM Configuration

Item	Configuration
vCPU	32
Memory	32 GB
System hard disk	92 GB
Data disk	1024 GB

Table 5-3 Standard VM configuration

Item	Configuration
vCPU	64
Memory	128 GB
System hard disk	92 GB
Data disk	4096 GB

5.2.1.3 User name and password planning

Remember the password of the NetEco user. Otherwise, you may need to reinstall the NetEco.

Table 5-4 Operating system user name and password

User name	Initial password	Explanation
root	Changeme_123	Operating system administrator. This user is used to log in to the OS and run all commands.
ossadm	Changeme_123	Operating system user. This user is created when the operating system is installed. It is used to install, start, stop, and manage product software.
ossuser	Changeme_123	Operating system user. This user is created when the operating system is installed. It is used to install, upgrade, and routinely maintain product software.
backupuser	Changeme_123	Backup account.

Table 5-5 NetEco Redis database users and their passwords

User name	Initial password	Explanation
dbuser	Admin@123	Database administrator. Used to log in to the database of the node and run all commands.
ossdbuser	Changeme_123	Common user. Reads and edits database data, and creates and deletes database tables.
readdbuser	Changeme@123	Read-only user. Reads the database status, database configuration, and database data.

Table 5-6 NetEco GaussDB 100 V3 database users and passwords

User name	Initial password	Explanation
sys	Admin@123	Administrator user, which is used to modify database configurations, add, delete, modify, and query users and databases, and change user passwords. Only local login is allowed.
{ossdbuser} and	Changeme_123	Application read/write user. This user is used to read, write, create, and delete database tables using

ossdbuser		database services. {ossdbuser} indicates the application database name. Each application database name corresponds to a user.
switchdbuser	321_emegnahC	Switchover management user, which is used to switch over the database and set the database to read-only.
readdbuser	Changeme@123	Read-only O&M user, which is used to read database status and configure data.
public	N/A	Preset database user. A preset public user (incapable of logging in to the database). It is a set of all database users. If a permission is granted to public, all database users can have the permission. To ensure database data security, do not grant object permissions to user public.

Table 5-7 PowerEcho Web User and Password

User name	Initial password	Explanation
admin	Changeme_123	When you log in to the newly installed PowerEcho system for the first time, the system prompts you to change the initial password of the user.

Table 5-8 NetEco user name and password

User name	Initial password	Explanation
admin	Changeme_123	When you log in to the newly installed NetEco for the first time, the system prompts you to change the initial password of the user.

5.2.2 Obtaining Installation Software

Download the NetEco installation software package from support.huawei.com. You need to apply for some software based on project information.

5.2.3 Obtaining the Mediation Software Installation Package

For details, see 3.2.3 Obtaining the Mediation Software Installation Package.

5.3 Creating a VM (FusionSphere Openstack)

This section uses FusionSphere OpenStack OM 6.5.1RC1 basic edition as an example to describe how to create a VM.

In this scenario, obtain the following information in advance:

- You have obtained the VM template compressed package VM_EulerOS2.0SP8_X.X.X_aarch64_qcow2.zip.
- You have obtained the address as well as the user names and passwords for logging in to the FusionSphere OpenStack administrator view and tenant view.

Step 1 Register an image.

- Decompress the obtained VM template package VM_EulerOS2.0SP8_X.X.X_aarch64_qcow2.zip to obtain the VM template file VM_EulerOS2.0SP8_X.X.X_aarch64_qcow2.qcow2.
- Log in to the FusionSphere OpenStack Management Console in the administrator view, choose Resources > Computing > Images, and click Register.
- On the **Register image** page, set the parameters according to Table 5-9 and click **Register**. After the registration is complete, view the registered image in the image list.

Table 5-9 Parameters for registering an image

Parameter	Dscription	Example Value for NetEco Image
Provioded As Service	Select **Not Supported**.	Not supported
CPU Architecture	Select **x86** or **ARM**.	ARM
Type	Select an image type, which can be **FusionCompute, KVM,** or **Ironic**.	KVM
Name	Enter an image name, which can contain a maximum of 255 characters.	NetEco_FusionSphere_ image
Applicable OS	Select the OS used in the image file.	Linux
OS version	Select the OS version used in the image file.	EulerOS 2.8 64bit
Min Disk (GB)	Enter the minimum system disk size required by the VM that is to be created using the image. The value must be greater than or equal to the system disk size of the VM used for creating the image.	92

Min Memory (MB)	Enter the minimum memory size required by the VM that is to be created using the image.	65536
Disk Device Type	Select the type of bus used for communication between the system disk and the host. Set this parameter to virtio when registering a EulerOS image.	virtio
Upload Mode	If you set **Upload Mode** to **HTTPS**, the image file will be uploaded locally. If you set **Upload Mode** to **NFS**, the image file will be uploaded through the NFS server.	HTTPS
Image file	Select a **VM** image file stored on the local PC.	VM_EulerOS2.0SP8_X.X.X_aarch64_qcow2.qcow2
Disk format	Select the disk format specified in the image file.	qcow2

Step 2 Create a flavor.

- On the FusionSphere OpenStack management console, choose **Resources > Computing > Flavors** and click **Create**.
- In the displayed dialog box, set the parameters according to Table 5-10, and click **OK**.

Table 5-10 Parameters for creating a flavor

Parameter Name	Parameter description	Example
Type	Select the type of the compute instance to be created using the flavor.	Virtual Machine
CPU Architecture	Select **x86** or **ARM**.	ARM
Boot Source	**Local Disk**: The local disk of the host is used. Compared with the cloud disks, the local disk provides stable I/O performance and high throughput, but is not limited by VDC quotas and cannot collect statistics on usage. The performance is related to the host load and has risks of a single point of failure. It applies to short-term running systems that do not require high stability and	Local disk

	reliability. You are advised to synchronize important data to other instances or back up important data to the cloud disk. **Cloud Disk**: Shared storage is used. The cloud disk provides high data reliability and storage performance and supports hot migration and disk size expansion and reduction. It applies to long-term running systems that require high stability and reliability.	
Name	Set this parameter to a maximum of 255 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed in the value.	NetEco_Flavor
vCPUs	Set this parameter to an integer ranging from 1 to 256.	Basic configuration 32 Standard configuration: 64
Memory (MB)	Set this parameter to an integer ranging from 1 to 6291456.	Basic configuration: 32768 Standard configuration: 131072
Root Disk (GB)	Set this parameter to the system disk size of the VM to be created using the flavor. The value must be greater than or equal to the system disk size of the image. Otherwise, the VM fails to be created.	92
vCPU Bound to Physical Thread	**Enabled**: vCPUs of the VM are bound to the physical thread to reduce CPU competition and improve performance. **Disabled**: vCPUs of the VM are not bound to the physical thread.	Disabled
NUMA Affinity	Set this parameter to specify whether physical resources occupied by the VM vCPU and memory are allocated from the same NUMA node. The default value is Enabled in the following conditions: Huge page memory is set, vCPU Bound to Physical Thread is enabled, or real-time VMs are used. If you set this parameter to Disabled in the preceding conditions, the setting will not take effect.	Disabled

Tag	Both the host group tag and user-defined tag can be added to flavors. For flavors whose tag is the same as that of a host group, when creating a compute instance using the flavors, the system selects a host in the host group with the tag. For flavors with user-defined tags, they cannot be filtered by tag.	Customize Tag or select existing tag.

Step 3 Create a VM.

- On the FusionSphere OpenStack management console, log in to the tenant view, choose **Resources > Computing > VMs**, and click **Create**.
- Select the value planned for **Availability Zones** and click **Next**.
- Select the VM template created in step 1, set the system disk storage type to **Local Disk**, and click **Next**.
- Set **Flavor** to **NetEco_Flavor and** click **Next**, as shown in Figure 5-2.

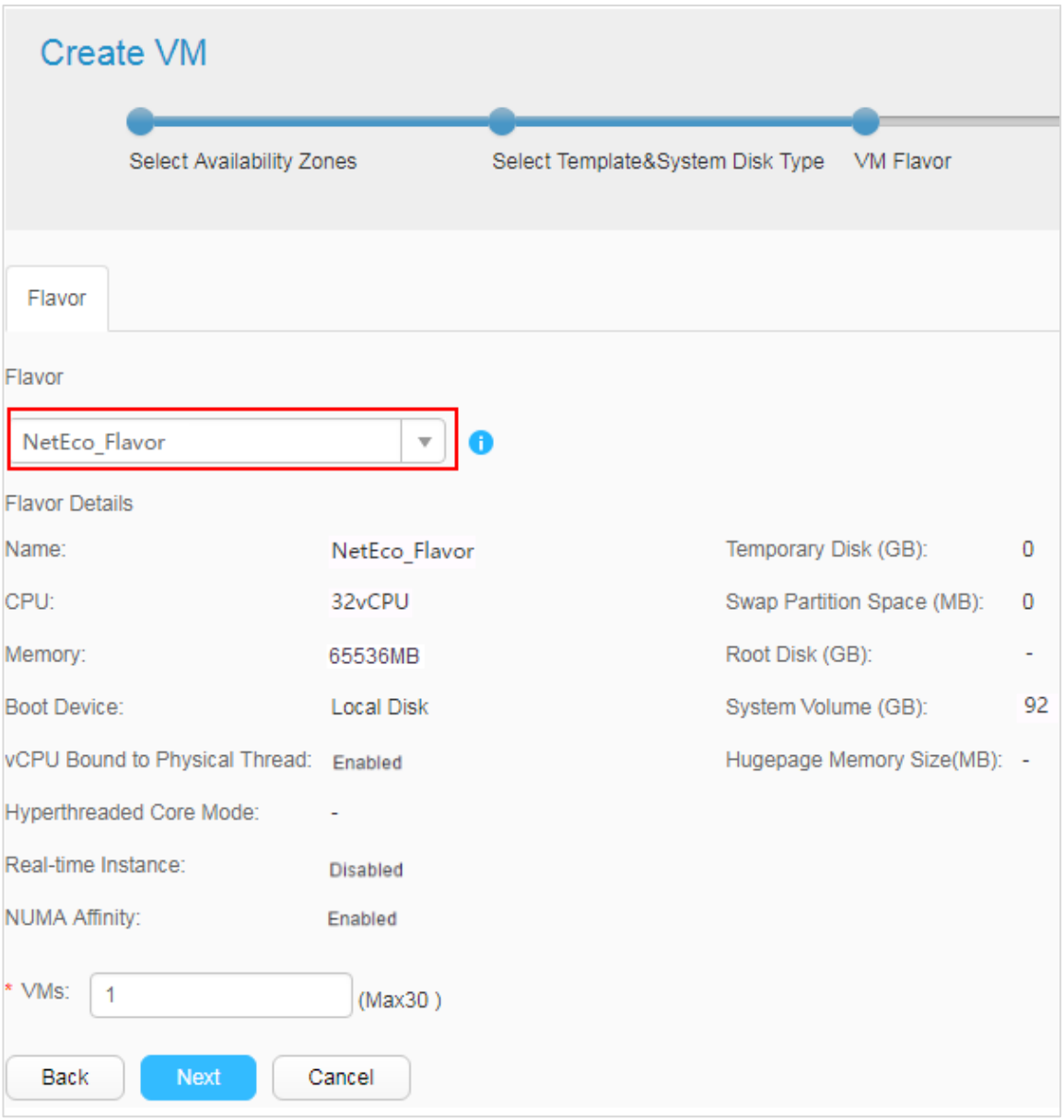


Figure 5-2 Selecting a flavor

- Add a network interface card (NIC) for the VM, and click Next, as shown in Figure 5-3. The actual network may not be a direct network.

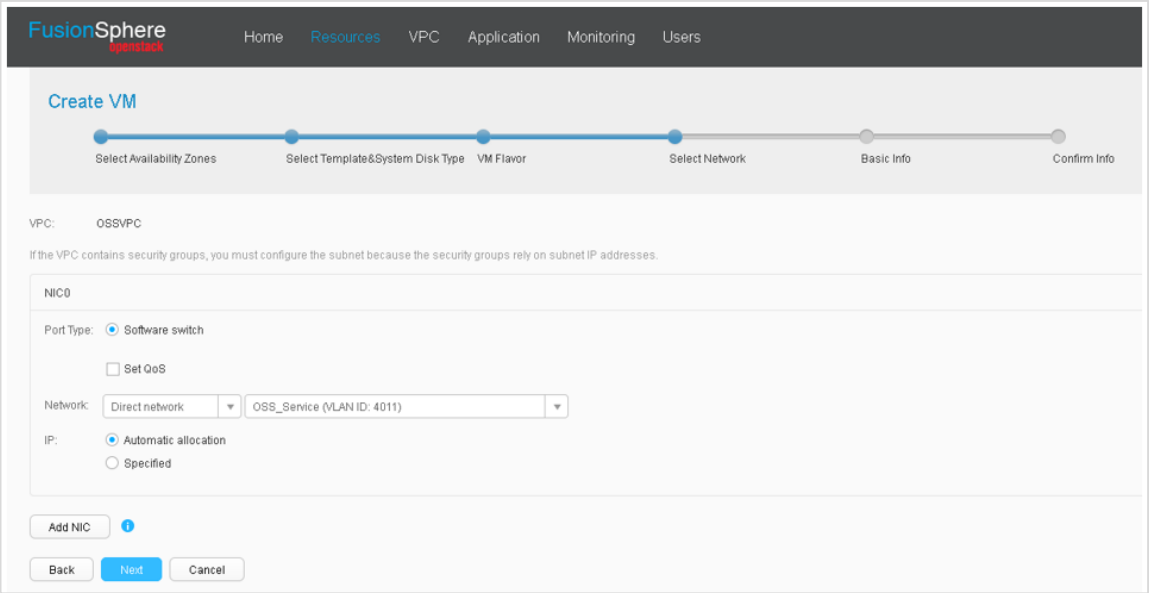


Figure 5-3 Adding a NIC

- Set the **VM** name and click **Next**.
- Confirm the VM information and click **Complete**. In the displayed dialog box, click **OK**.
- The creation takes about 5 minutes. After the VM is created, you can view the created VM in the Task Center.

Step 4 Add a Data Disk

- In the VM list, click  to view the VM information, as shown in Figure 5-4.

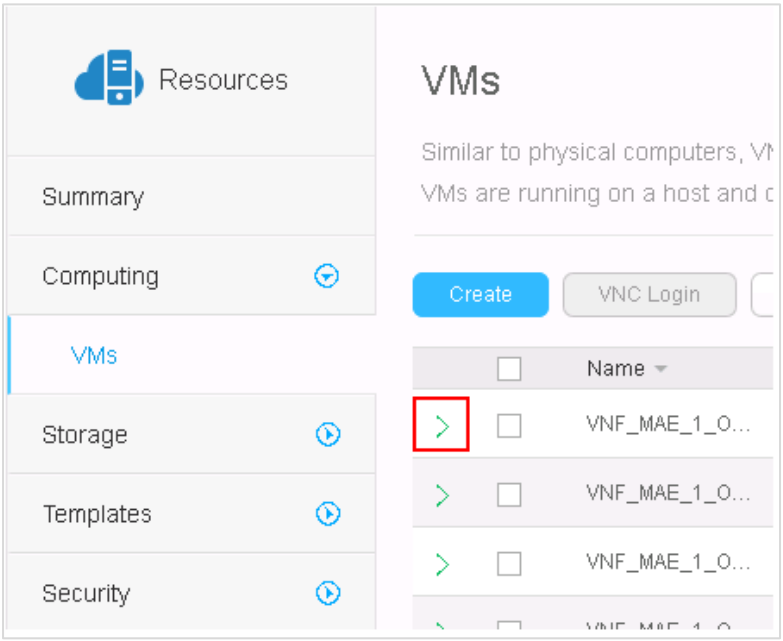


Figure 5-4 Viewing VM Information

- In the **hardware info** list, click  next to Disk.

- On the displayed Disk Configuration page, click **Add Data Disk**.
- In the **Add Data Disk** dialog box, enter the planned VM capacity, select **Storage SLA** and click **OK**. In the displayed dialog box, click **OK**.
- Set the data disk capacity to 1024 GB for basic configuration and to 4096 GB for standard configuration.
- You are advised to select Cloud Disk.
- Check the task status in the task center, as shown in Figure 4. If the status is **Succeeded**, the data disk has been added successfully.

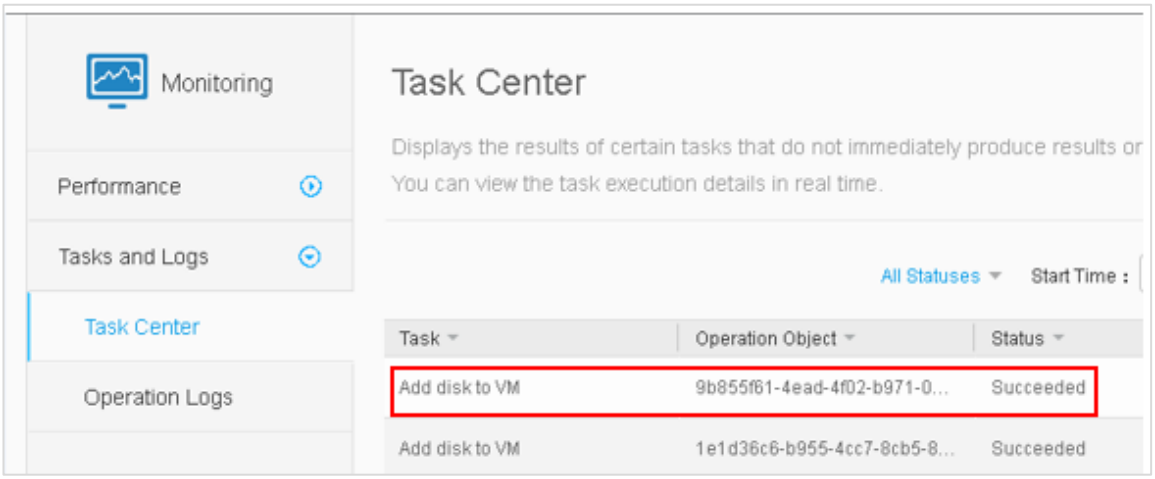


Figure 5-5 Data disk added successfully.

5.4 Creating a VM (FusionCompute Scenario)

This section uses FusionCompute 8.0.RC2 (basic version) as an example to describe how to create a VM.

In this scenario, obtain the following information in advance:

- You have obtained the VM template compressed package VM_EulerOS2.0SP8_X.X.X_aarch64_qcow2.zip.
- You have obtained the address, user name, and password for logging in to FusionCompute.

Step 1 Import the template.

- Decompress the obtained VM template package **VM_EulerOS2.0SP8_X.X.X_aarch64_qcow2.zip** to obtain the VM template file **VM_EulerOS2.0SP8_X.X.X_aarch64_qcow2.qcow2**.
- Log in to FusionCompute as local user admin and click **Import Template** in the navigation bar. If the system prompts you to install the plug-in, click **OK**, as shown in Figure 5-6.

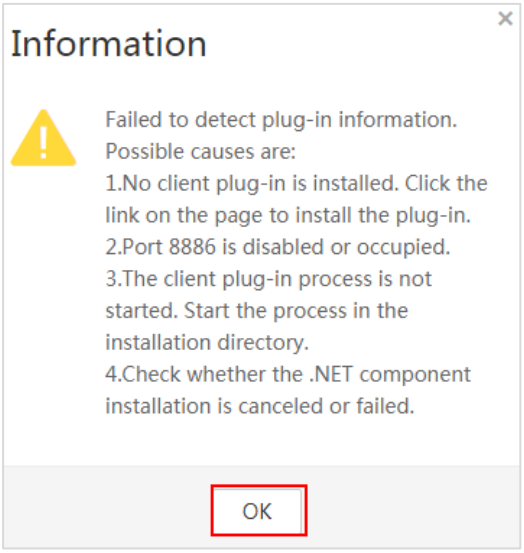


Figure 5-6 Message prompting for plug-in installation

- In the dialog box for creating a template, click Link to download the plug-in and install it as prompted, as shown in Figure 5-7.

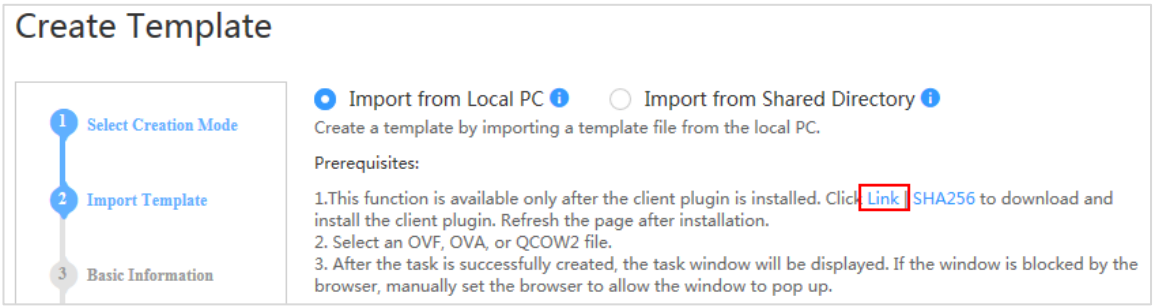


Figure 5-7 Installing the plug-in

- In the dialog box for creating a template, click **Select**. If the dialog box shown in Figure 5-8 is displayed, click **Open FCPortalClientPluginKvm.exe**. If no dialog box is displayed, go to the next step.

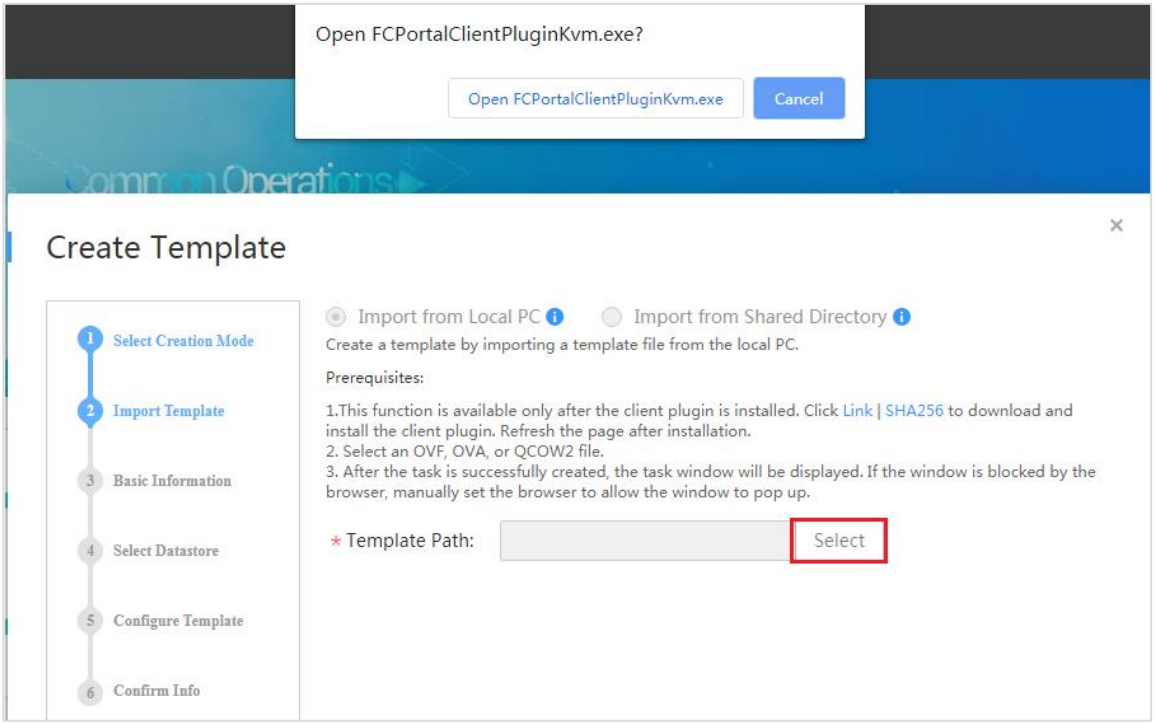


Figure 5-8 Running the plug-in

- Select the obtained **VM_EulerOS2.0SP8_X.X.X_aarch64_qcow2.qcow2** file on the local PC and click **Next.**
- In the Basic Information step, enter basic information as required or according to Table 5-11, and click **Next**.

Table 5-11 Parameters for configuring basic parameters

Parameter Name	Parameter description	NetEco parameters
Name	Set this parameter to a maximum of 255 characters.	New Virtual Machine
Description	Enter remarks.	/
Select Template Location	Select a value based on the node planned on the FusionCompute platform. You can customize the value.	site
Select Computer Resource	Select the resource corresponding to a node. Select **ManagementCluster** for a single-node system. In a cluster scenario, multiple resources are available for you to select one.	ManagementCluster
OS	Select the OS used in the image file.	Linux
OS Version	Select the OS version used in the image file.	EulerOS2.8 64bit

- In the **Select Datastore** step, select a storage location that meets the capacity

requirement based on the available capacity, and click **Next**.

- In the **Configure Template** step, set **CPU** to **8** and **Memory** to **16** and click **Next**.
- In the **Confirm Info** step, confirm the template information and click **OK**.
- When the system displays a message indicating successful import, the template has been imported successfully.

Step 2 Deploy the VM.

- In the navigation bar on the home page, click **Deploy VM Using Template**.
- In the **Basic Information** step, enter basic information as required or according to Table 5-12, and click **Next.**

Table 5-12 Parameters for configuring basic parameters

Parameter Name	Parameter description	NetEco parameters
Name	Set this parameter to a maximum of 255 characters.	NetEco_FC
Description	Enter remarks.	/
Select template	Select the imported template.	NetEco_Flavor
Select VM location	In single-node and multi-node scenarios, select a value based on the FusionCompute platform.	site
Set Computer Resource	Select the resource corresponding to a node. Select **ManagementCluster** for a single-node system. In a cluster scenario, multiple resources are available for you to select one.	ManagementCluster

- In the **Configure VM** step, configure the CPU and memory according to Table 5-13, retain the default values for other parameters, and click **Next**.

Figure 5-9 Parameter description

Parameter Name	Parameter description	Example
CPU	The number of vCPUs ranges from 1 to 86.	Basic Configuration:32
		Standard configuration:64
Memory	Specifies the memory size.	Basic Configuration:32
		Standard configuration:128

- In the **Customize OS** step, retain the default settings and click **Next**.
- In the **Confirm Info** step, confirm the basic information about the VM, select **Start VM immediately after creation**, and click **OK**.

- In the **Basic Information** area on the **Summary** tab page, check the VM creation result. If the VM status is **Running** and you can log in using VNC, the VM has been created successfully.

Step 3 Add a data disk.

- On the VM information page, click the Configuration tab. In the navigation tree on the left, click **Disk**. Then, click **Attach Disk**. In the displayed **Attach Disk** dialog box, click **Create and Attach Disk**.
- In the **Create and Attach Disk** dialog box, set **Capacity** and **Name** as required, retain the default values for other parameters, and click **OK**.
- The capacity of the data disk in basic configuration is 1024 GB, and that in standard configuration is 4096 GB. On the Configuration tab page, choose **Hardware > Disk** to view the status of the added disk.

5.5 Configuring IP Addresses

By default, the IP address of the created VM is empty. Change the IP address based on the site requirements.

5.5.1 Log in to the VM (Using VNC)

You have obtained the password of user root in advance.

Step 1 Log in to FusionSphere OpenStack Management Console, log in to the tenant view, and choose **Resources > Computing > VMs**.

Step 2 On the **VMs** page, select the created VM, and click **VNC Login.**

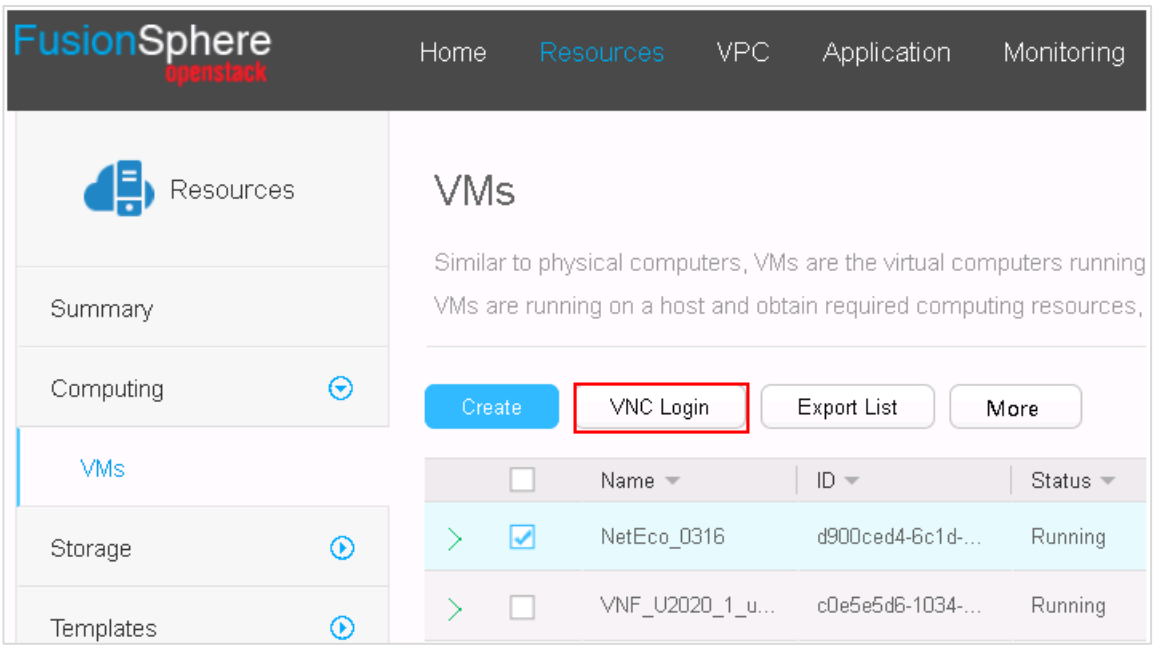


Figure 5-10 VNC Login

Step 3 Replace the domain name in the address box with the obtained reverse proxy front-end IP address and press **Enter**. The command line interface is displayed.

- For example, if the domain name is https://nova-novncproxy.az1.dc1.huawei.com:8002/vnc_auto.html, replace nova-novncproxy.az1.dc1.huawei.com with https://172.28.96.201:8002/vnc_auto.html. Then, the domain name is https://172.28.96.201:8002/vnc_auto.html.

5.5.2 Configuring IP Addresses

Step 1 Run the following command to change the server IP address based on the actual plan:

```
# cd /usr/local/PlatformTools
# ./modifyip.sh
```

- The ./modifyip.sh script can be used only when the NMS software is not installed. If the NMS software is installed, change the server IP address on the PowerEcho.
- Enter the server IP address and route information as prompted.

Please input IP address [Current IP:null]:

- When the preceding information is displayed, enter the IP address and press Enter.

Please input net masks [Current Netmask:null]:

- When the preceding information is displayed, enter the subnet mask and press Enter.

Please input default route [Current RouteIP:null]:

- When the preceding information is displayed, enter the gateway and press Enter.
- If the following information is displayed, the IP address is changed successfully:

Modify IP success.

5.6 Installing the NetEco Software

Obtain the following software packages and tools before the installation:,Obtaining Method,For details, see.1.3 NetEco System software package and tool software:

- iManagerNetEco_DeployTool_V600R020C00XXX_Euler_arm64.zip
- iManagerNetEco_Platform_V600R020C00XXX_Euler_arm64.zip
- iManagerNetEco_Platform_V600R020C00XXX_Euler_arm64.zip.cms
- iManagerNetEco_Platform_V600R020C00XXX_Euler_arm64.zip.crl
- iManagerNetEco6000_V600R009C00XXX_Euler_arm64.zip

- iManagerNetEco6000_V600R009C00XXX_Euler_arm64.zip.cms
- iManagerNetEco6000_V600R009C00XXX_Euler_arm64.zip.crl
- PuTTY
- FileZilla tool

Step 1 Log in to the NetEco server as user ossadm using PuTTY.

Step 2 Run the following commands to switch to user root and create the /opt/install directory:

```
# su - root
Password: root password
```

- After you switch to the root user, "root@host name:~ #" is displayed.
- The default password of user root is Changeme_123.

```
# mkdir /opt/install
# chown -h ossadm:ossgroup /opt/install
```

Step 3 Use FileZilla to upload the software packages obtained in the prerequisites to the /opt/install directory on the NetEco server.

- User name and password: ossadm and its password.
- Port: Port 22 is used by default for SFTP.
- IP address: fixed physical IP address of the host.

Step 4 Run the following commands to decompress the deployment tool:

```
# chown -Rh root:root /opt/install
# chmod 700 /opt/install
# cd /opt/install
# unzip iManagerNetEco_DeployTool_V600R020C00XXX_Euler_arm64.zip
```

- iManagerNetEco_DeployTool_V600R020C00XXX_Euler_arm64.zip is only an example. Replace it with the actual software package name.

Step 5 Run the following commands to install the NetEco software:

```
# screen -S "install_ha.sh" bash /opt/install/install_ha.sh
============================================================
Please select a Installation language:
1--zh
2--en
Q--Exit
============================================================
Please make a choice:
```

- Enter a number to select the installation language as prompted and press Enter.

```
Please input the first node IP address:
```

- Enter the IP address of NetEco server 1 as prompted and press Enter.

Please input the second node IP address:

- Enter the IP address of NetEco server 2 as prompted and press Enter.

Please input the third node IP address:

- Enter the IP address of NetEco server 3 as prompted and press Enter.

Please input the floating IP address:

- Enter the floating IP address of the NetEco server as prompted and press Enter.

Make sure the root passwords of all nodes are the same.
Please input the password for root:

- Enter the password of user root as prompted and press Enter to start the installation.
- The installation takes about 60 minutes. If the following information is displayed, the installation is successful:

Install neteco successfully.

- During the installation, the system automatically deploys the PowerEcho and NetEco. Ensure that the server is powered on properly and no manual intervention is required during the installation.
- During the initial installation, you can install the NetEco only in the background. After the PowerEcho is installed, you can install and upgrade the NetEco on the PowerEcho.
- Installing the NetEco in one-click mode takes a long time, including configuring the OS, installing the PowerEcho, installing the database, installing the NetEco, hardening the OS, and installing the cluster monitoring software.
- To return to the original command line, press Ctrl+A and then D.
- If PuTTY is interrupted during the installation, log in to the NetEco server again and switch back to the task session window when PuTTY is interrupted.
- The NetEco installation takes a long time. If you have logged out after the installation, log in to the NetEco server as user ossadm and then run the following command to switch to user root:

```
# su - root
```

Step 6 Run the following command to delete the install directory:

```
# cd /opt
# rm -rf install
```

- Restart NetEco-1, NetEco-2, and NetEco-3 in sequence to prevent switchovers and make security hardening operations during the installation take effect. Run the following command:

```
# sync
# reboot
```

- Do not perform other operations during the restart.
- Log in to the system at least 5 to 10 minutes after the restart.

5.7 Setting System Parameters - Deployment Commissioning

5.7.1 Logging In to PowerEcho

The network connection between the PC and the PowerEcho client is normal. The PowerEcho provides only one admin user. This user has all operation rights on the PowerEcho Web page.

Step 1 Open a web browser, enter https://PowerEcho client login IP address:31945 in the address box, and press Enter.

Step 2 On the login page, enter the user name and password, and click Log In. After logging in to the PowerEcho for the first time, change the password as prompted. If the admin user enters incorrect passwords for five consecutive times within 10 minutes, the login IP address will be locked for 10 minutes.

5.7.2 Deployment commissioning

Step 1 On the PowerEcho main menu, choose Commissioning > Deployment Commissioning.

Step 2 Select NetEco and click Deployment Commissioning.

Step 3 Commission the following system parameters in sequence:

- Commissioning preview: Export and archive the current system configuration information.
- (Optional) Change the password of the operating system user. To ensure system security, change the initial password and keep the new password secure.
- (Optional) Change the password of the database user. To ensure system security, change the initial password and keep the new password secure.
- Configure the time zone and time: Ensure that the node time is the same as the NTP server time to ensure that each node can properly synchronize time with the NTP server. If the time zone of the node is different from that of the NTP server, change the time zone to be the same.
- Configure NTP: Add an NTP server to ensure time consistency between nodes.

- Change the host name: (Optional) Set it to the planned host name.
- (Optional) Set IP Address to the planned IP address.
- Configure Route: (Optional) Set this parameter to the planned route.
- (Optional) Updating the ER certificate: (Optional) To ensure communication security, apply for a certificate from the CA and update the preconfigured ER certificate.
- (Optional) Set backup parameters. After setting backup server parameters and backup file storage policies, you can save backup files to the corresponding backup server. By default, the master server is configured as the backup server. In the single-node system scenario, data is backed up to the local host by default. If you want to back up data to the local host, you are advised to use the backupuser user. The backup path is root directory of the backup server user/Path specified in backup parameters, for example, /opt/neteco_backup/. If data is backed up to another host, the customer needs to provide the IP address, user name, password, and backup path.
- Configuring a scheduled backup task: No commissioning is required. After the product planning data package is imported, the system automatically creates a scheduled backup task for the product.
- Commissioning summary: Check whether commissioning operations are complete and whether the current system configuration is correct.

If the system displays a message indicating that **The product service and product database are running or partially running**, you are advised not to select **Automatically start product database and product service after modification** and click **OK**, after all commissioning tasks are complete, start the product database and product services.

Step 4 (Optional) Start the service and database on the product node.

- Choose **Product > System Monitoring** from the main menu of PowerEcho.
- In the upper left corner of the System Monitoring page, move the cursor to and select the NetEco product.
- In the upper left corner of the page, click **Start** and select **Start All** from the drop-down list.

Step 5 Check the commissioning result.

- Check whether the tasks generated for each commissioning item are successfully executed.
  - On the PowerEcho main menu, choose **System > Task List**.
  - On the **Task** List page, check whether the status of each task is Execution Succeeded. If the status is **Execution Succeeded**, the commissioning is successful.
- Check whether the product service is running properly.
  - Choose **Product > System Monitoring** from the main menu of PowerEcho.

- On the **System Monitoring** page, check whether the status of each service on the **Nodes** tab page is **Running**. If the status is **Running**, the system has been commissioned successfully.

5.8 Logging In to the NetEco

The NetEco works in browser/server (B/S) mode. Users need to use a browser to log in to the NetEco.

Step 1 In the address box of the browser, enter ***https://IP address of the NMS:31943*** and press Enter.

- The Chrome or Firefox browser is recommended.
- The optimal resolution is 1920 x 1080.

Step 2 Enter the user name and password, and click Log In.

- When you log in as the admin user for the first time, the system prompts you to change the password. Change the password as required and remember it.
- If you enter incorrect passwords for three consecutive times, you need to enter the verification code for the fourth time. If you enter incorrect passwords for five consecutive times, the user or IP address will be locked for 10 minutes.

5.9 Loading a License

The NetEco license file controls the functions and management capabilities of the NetEco. Before using the NetEco, load a commercial license. For details, see.3.2.2 Obtaining the NetEco Software License.

Step 1 Log in to the NetEco client and click **Import License**.

Step 2 Click  next to the **License** file text box, select a license file, and click **Upload**.

Step 3 After the upload is complete, click **Apply**.

5.10 (Optional) Installing the NE Mediation

Obtain the NE mediation installation package by referring to section 3.2.3 Obtaining the Mediation Software Installation Package.

Step 1 Choose System > Service Settings > Adapter Management.

Step 2 Click **Upload**. On the displayed **Upload adapter package** page, click **+** and select the files to be uploaded.

Step 3 Click **Upload** to upload the files.

Step 4 Select the NE mediation packages to be installed on the **Adapter Management** page and click **Install**. Then click **Yes** in the displayed dialog box. In the displayed Confirm dialog box, click **OK**.

5.11 Configuring NetEco System Security

Configure the NetEco system security based on the site requirements, including:

- Configuring Reauthentication.
- Replacing a Security Certificate for Connection between NetEco and NE.
- Replacing a Northbond Certificate.
- Replacing the influxdb client Certificate.
- Replacing the influxdb server Certificate
- Replacing the FTPS Certificate.

For details, see iManager NetEco6000 Product Documentation.

5.12 Commissioning the NetEco

This section describes how to install and deploy the NetEco software. For details about how to install the NetEco software, see Huawei NetEco Operation Lab Guide.

6 FAQs

6.1 How Do I Log In to the Server in SSH Mode?

Step 1 Decompress **PuTTY.zip** on the PC and double-click PuTTY.exe in the decompressed folder to start PuTTY.

Step 2 (Optional) To record operation logs, choose **Session > Logging** in the navigation tree on the left. In the Session logging area, select Printtable output. In the Log file name area, set the directory for storing operation logs, as shown in Figure 6-1.

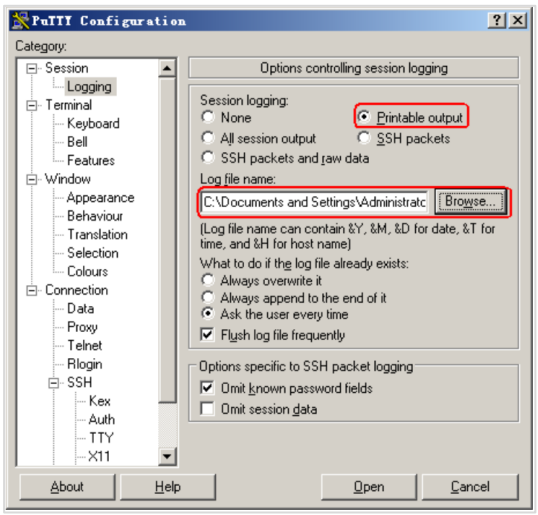


Figure 6-1 PuTTY Configuration

Step 3 In the navigation tree on the left, choose **Session**. In the right pane, enter the IP address of the service network port on the server in Host Name (or IP address). In the Connection type area, select **SSH**. In the Close window on exit window, select **Only on clean exit** in the area and click Open, as shown in Figure 6-2.

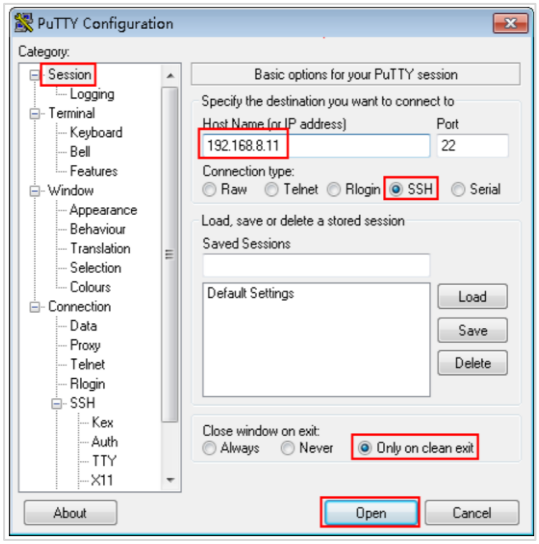


Figure 6-2 PuTTY Configuration

Step 4 If the alarm page shown in Figure 6-3 is displayed, check whether the serial number of the server is the same as that displayed in the PuTTY Security Alert dialog box. If yes, click Yes. Otherwise, click Cancel.

- Log in to the NetEco server through the remote management port and run the following command as user root to obtain the serial number of the server:

```
#cd /etc/ssh
#ssh-keygen -l -f ssh_host_rsa_key
```

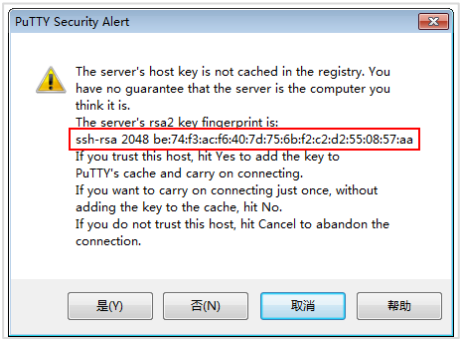


Figure 6-3 PuTTY Security Alarm

Step 5 When the following information is displayed, enter the user name and press Enter:

```
login as: User
```

Step 6 When the following information is displayed, enter the password and press Enter:

```
password:
```

If information similar to Last login: Mon Aug 11 14:47:55 2014 from 10.66.101.113 is displayed, the login is successful.

6.2 How Do I Uninstall the NE Mediation Software?

Step 1 Log in to the NetEco web client.

Step 2 Choose **System > Configuration Management > Device Access** from the main menu. In the navigation pane, choose Adaptation Package Management.

Step 3 Select the mediation package to be uninstalled and click **Uninstall**.

Step 4 In the displayed dialog box, click **Yes** and **Comfirm**.

- The original installation package is not retained during mediation uninstallation. The mediation in use cannot be uninstalled.

6.3 How Do I Use FileZilla to Transfer Files?

FileZilla is a dedicated file transfer tool that supports both FTP transfer and resumable transfer.

Step 1 Double-click filezilla.exe to run filezilla.exe.

Step 2 In the FileZilla window, set parameters according to Table 6-1.

Table 6-1 Parameter description

Parameter	Explanation
Host	Enter the IP address of the destination server.
User	Enter the user name and password of the target server. The user must have the permission to access the target directory.
cipher	
Port	22. Port 22 is used by the SFTP protocol by default.

Step 3 Click Quick Connect.

- Ignore the dialog box displayed during the connection and click OK.
- After the connection is successful, the directory information of the remote server is displayed in the Remote site area.

Step 4 In the Remote site area, set the destination directory on the destination server, for example, /opt. After the path is set, all files in the path are displayed in the Remote site area.

Step 5 In the Local site area, set the path of the file to be uploaded on the PC, for example, D:\FILE. After the path is set, all files in the path are displayed in the Local site area.

Step 6 Perform operations as required. For details, see Table 5-2.

Table 6-2 Operation Description

If...	Then...
Uploading a file	In the Local site area, right-click the file to be uploaded on the PC and choose Upload.
Downloading a file	In the Remote site area, right-click the file to be downloaded to the PC and choose Download.

- If the upload or download fails, click the Failed Transfer tab in the lower left corner of the FileZilla window, right-click the file that fails to be transferred, and choose Reset and requeue selected files from the shortcut menu to resume the file transfer.

6.4 How Do I Rectify the Fault that FileZilla Cannot Connect to the NetEco Server?

Table 6-3 FileZilla Fault Causes

Fault Symptom	Possible Causes
When the FileZilla tool is used to connect to the NetEco server, an error message similar to "Failed to connect to the server" is displayed.	The IP address of the NetEco server is incorrect.
	The password is incorrect.
	The port number is incorrect.
	The firewall is enabled on the local PC.
	iAccess is enabled to connect to the Huawei office network.

Perform the following operations:

Step 1 Type the correct IP address in the Host text box.

- The NetEco has two IP addresses: one is the iBMC IP address and the other is the service IP address of the NetEco (that is, the IP address for logging in to the NetEco WebUI). Ensure that the IP address is the service IP address of the NetEco. If the PC is directly connected to the server using a network cable, ensure that the network cable between the PC and the server is connected to service network port 1.

Step 2 The user name or password is incorrect. Generally, the user name is ossuser or ossadm.

- If the NetEco software has been installed, the default SFTP user name is ossuser or ossadm.
- If the NetEco software is not installed, the default SFTP user name is ossadm.

Step 3 Enter port 22 in the Port text box to check whether the connection is successful.

Step 4 Choose Start > Control Panel > System and Security > Windows Firewall, click Turn Windows Firewall on or off, and select Disable.

Step 5 Close the iAccess connection and try to connect to the server.

6.5 How Do I Switch Back to the Task Window After PuTTY Is Interrupted?

If PuTTY is interrupted during the commissioning and the task is not complete, perform the following steps to switch back to the task window:

Step 1 Run the following command to switch to user root:

```
$ su - root
Password: Password of user root
```

Step 2 Run the following command to check whether the task is complete:

```
# screen -ls
```

- Information similar to the following is displayed:

```
There is a screen on:
313550.install_ha.sh (Detached)
```

- In the command output, 31350.install_ha.sh indicates the process ID of the task, and install_ha.sh indicates the task name.
- If the command output contains the task script name, the task is being executed. Go to Step 3.
- If the command output contains No Sockets found in /var/run/screens/S -root, the task is complete. View the script log information to check whether the task is successfully executed.

```
# cd /opt/install/log
# tail -n 5 install_ha.log
```

- When the system displays the following information, the installation is successful:

```
Install neteco successfully
```

Step 3 Run the following command to switch back to the task session window when PuTTY is interrupted:

```
# screen -r "Task name"
```

- If information similar to the following is displayed, the task session window has been opened by another PuTTY or the task is complete:

```
There is no screen to be resumed matching install.sh.
```

Huawei DCF Certification Training

HCIP-DCF-Deployment

Huawei DCIM Operation Lab Guide

ISSUE:2.0

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Technologies Co., Ltd.

Address:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China
Website:	http://e.huawei.com

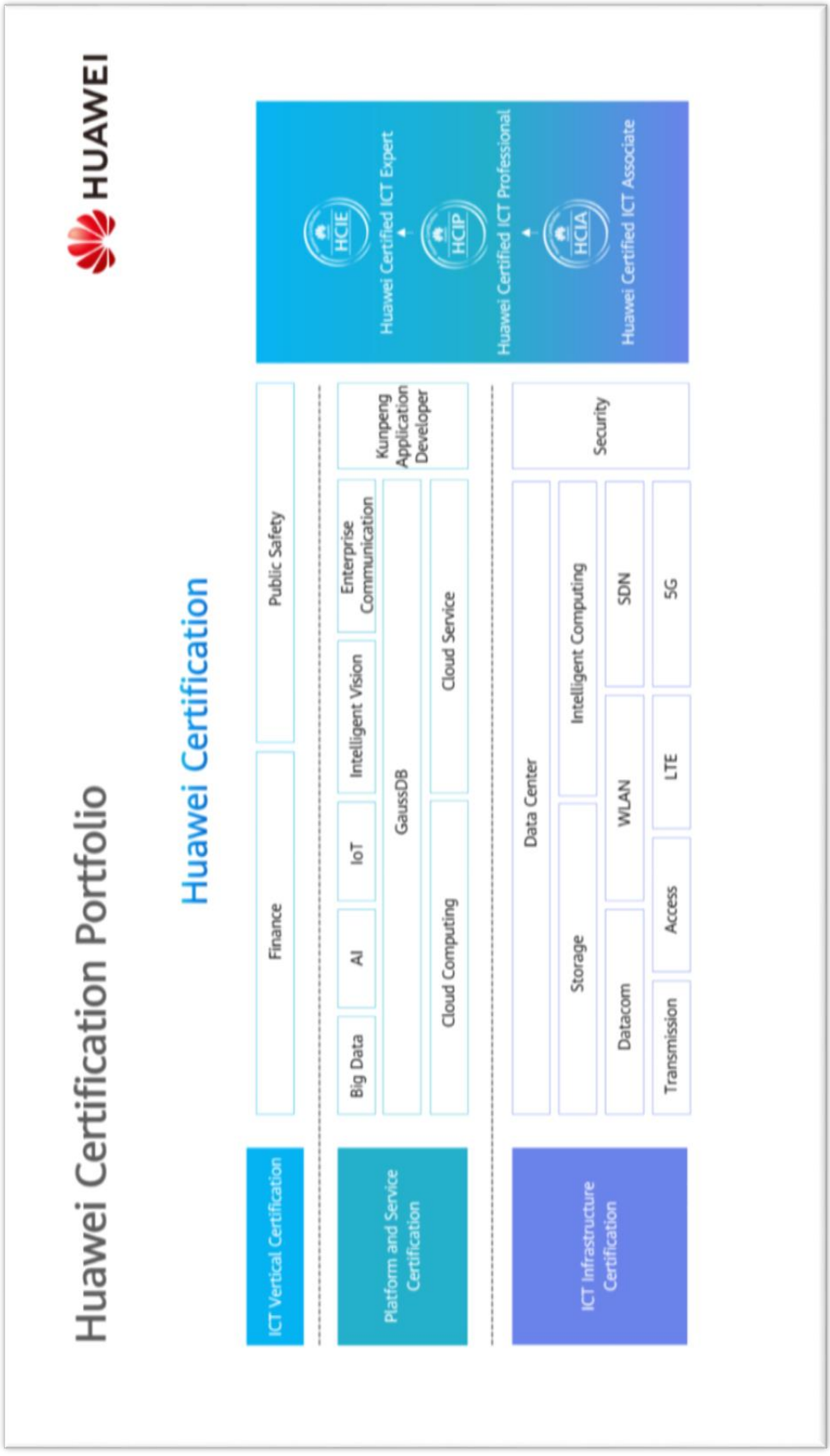
Huawei Certificate System

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, Platform and Service certification and ICT vertical certification, and grants Huawei certification the only all-range technical certification in the industry.

Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE).

HCIP-Data Center Facility Deployment V2.0 is aim to train and certify senior engineers who need to perform deployment and system commissioning for Huawei data center infrastructure products.

After passing the HCIP-Data Center Facility Deployment V2.0 certification, you will be familiar with Huawei data center infrastructure products and have the deployment and commissioning capabilities of Huawei data center infrastructure products. The full series of products include Huawei modular data center Fusion Module series products, Huawei UPS and precision PDC series products, Huawei data center energy storage products, Huawei data center smart cooling products, and Huawei data center DCIM system products.


HUAWEI
Huawei Certification Portfolio
Huawei Certification
ICT Vertical Certification
Finance
Public Safety
Platform and Service Certification
Big Data
AI
IoT
Intelligent Vision
Enterprise Communication
Kunpeng Application Developer
GaussDB
Cloud Computing
Cloud Service
ICT Infrastructure Certification
Data Center
Storage
Intelligent Computing
Security
Datacom
WLAN
SDN
Transmission
Access
LTE
5G
HCIE
Huawei Certified ICT Expert
HCIP
Huawei Certified ICT Professional
HCIA
Huawei Certified ICT Associate

About This Document

Overview

This document is a training course for HCIP-DCF-Deployment certification. It is intended for trainees who are preparing to take the HCIP-DCF-Deployment exam or readers who want to understand the Huawei DCIM software installation and deployment process.

Description

This document describes how to install and commission Huawei DCIM - NetEco in three

Content

1 Precautions for Operations on NetEco

1.1 Hardware Requirements for Logging In to the NetEco

The NetEco works in browser/server (B/S) mode. Users need to log in to the NetEco using a browser. To better browse and operate the NetEco on the client, the PC must meet certain requirements.

Verify that the NetEco is running properly. The requirements for the PC used for login are as follows:

Table 1-1 NetEco operating environment requirements

Configuration Item	Basic Configuration Requirements
PC Hardware Configuration	Inter(R) Pentium(R) Dual CPU E2180 @ 2.00 GHz, 2 GB memory
Operating system	Windows 7, Windows 2008, Windows 10
Resolution	1920*1080

1.2 Browser Requirements

You are advised to use the latest Chrome browser (Stable Channel version) or Firefox browser (ESR version).

1.3 Logging In to the NetEco

You have obtained an available NetEco user name and password in advance. For the first login, use the **admin** account. The default password is **Changeme_123**.

Step 1 In the address box of the browser, enter ***https://IP address of the NMS:31943*** and press **Enter**.

Step 2 Enter the **user** and **password**, and click **Log In**.

- When the number of online users reaches the maximum supported by the current version, the system displays a message indicating that the login fails. In this case, contact the system administrator.

- If you enter incorrect passwords for three consecutive times, you need to enter the verification code for the fourth time. If you enter incorrect passwords for five consecutive times, the user or IP address will be locked for 10 minutes.

1.4 Understanding the Workbench

The main menu of the data center is displayed.

- Operation entry
- Platform bulletins are provided, and key public information is clearly displayed.
- Collects statistics on to-do information to improve O&M efficiency.

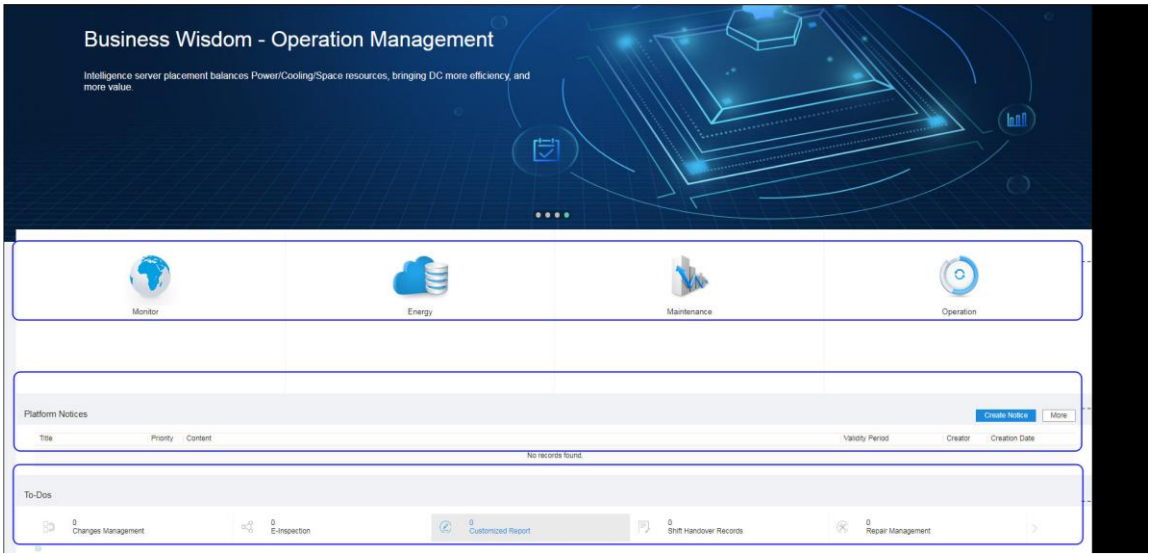


Figure 1-1 Workbench

2 Experiment Tasks

2.1 Task List

Table 2-1 Task List

Task Name			Recommendation task duration	Completed
NetEco Commissioning	Creating a Management Domain		40 min	☐Yes ☐No
	Adding a smart module			☐Yes ☐No
	Adding a device			☐Yes ☐No
Monitoring Operations	Device management	View management	20 min	☐Yes ☐No
		Customizing Large-Screen Monitoring		☐Yes ☐No
	Performance data	Querying Historical Data		☐Yes ☐No
		Re-collect historical data		☐Yes ☐No
		Setting a Monitoring Template		☐Yes ☐No
Alarm management	Current alarms	Monitoring alarms	20 min	☐Yes ☐No
		Querying Alarms		☐Yes ☐No
		Handling Alarms		☐Yes ☐No
	Historical alarms			☐Yes ☐No
	Alarm Settings			☐Yes ☐No
Security management	Access control management	Creating an Access Control Device	40 min	☐Yes ☐No

		Event List Record		☐Yes ☐No
		Time Group Management		☐Yes ☐No
		Access control user management		☐Yes ☐No
	Video management	Adding Huawei Cameras to the VCN		☐Yes ☐No
		Setting Video Server Parameters		☐Yes ☐No
		Adding Cameras in Automatic Discovery Mode		☐Yes ☐No
		Group Management		☐Yes ☐No
		Camera management		☐Yes ☐No
		View Video Playback		☐Yes ☐No
Energy efficiency management	Energy efficiency configuration	Electricity price configuration	15 min	☐Yes ☐No
		PUE Parameter Configuration		☐Yes ☐No
		Power configuration		☐Yes ☐No
		iCooling energy efficiency		☐Yes ☐No
		Power supply and distribution		☐Yes ☐No
O&M management	On-duty scheduling management		15 min	☐Yes ☐No
	Availability management			☐Yes ☐No
	Supplier management			☐Yes ☐No
Report management	Report Task		15 min	☐Yes ☐No
	Report system configuration			☐Yes ☐No

System management	Service Settings		15 min	☐Yes ☐No
	System management			☐Yes ☐No
	Remote notification	Commissioning the Remote Notification Function		☐Yes ☐No
		Setting Remote Notification Parameters		☐Yes ☐No

3 NetEco Commissioning

3.1 Creating a Management Domain

Management domains include: Park, Building, Room, ContainerDC, Subnet, NetecoSite, Site, FusionModule500, Modular, Room-ShapeNode, Building-ShapeNode.

You are advised to plan the subordinate relationships between management domains and devices before performing this operation.

The procedure is as follows:

Step 1 Choose System > Service Settings > Data Center Planning.

Step 2 Add a management domain.

- In the navigation tree, select the upper-level node to which you want to add a domain.
- In the **Management Domain** area in the lower part of the navigation tree, drag the domain to be added to the configuration design area.
- You can adjust the shape of Room, Room-ShapeNode, Building-ShapeNode, Floor-ShapeNode, Container-ShapeNode, background planning NetEco site, and management domains created at the background planning NetEco site: To design an irregular polygon equipment room, hold down the **Shift** button, click the frame to add more yellow dots, and drag the yellow dots to adjust the angles of lines.
- If you want to delete a management domain, click the management domain icon and click **Delete** under.
- In the right pane of the configuration design area, configure the management attributes of the domain based on the site requirements. The parameters marked with an asterisk (*) are mandatory.
- You can configure management attributes, power supply attributes, and cooling attributes for the equipment room management domain.
- Click on the toolbar.
- Repeat to add a management domain until the configuration is complete.

----End

3.2 Adding a Module

The root node, subnet, equipment room, container, or branch management domain can be used to create a smart module.

The procedure is as follows:

Step 1 Choose System > Service Settings > Data Center Planning.

Step 2 In the navigation tree on the left, select the management domain for which you want to create a smart module.

Step 3 In the lower left corner of the page, click Managed Domains to expand the Managed Domains area.

Step 4 Select Module from the Type drop-down list box.

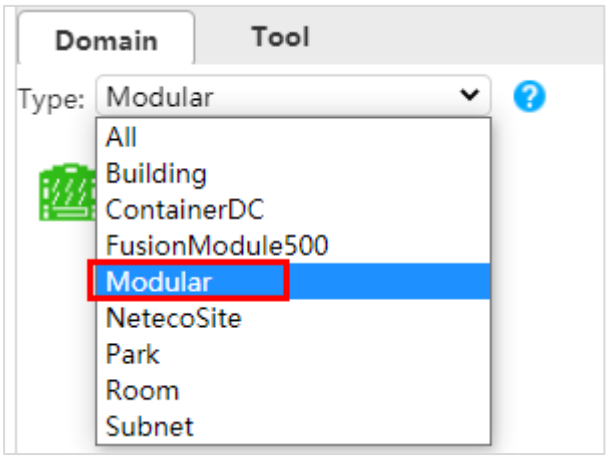


Figure 3-1 Selecting a smart module

Step 5 Select the smart module to be added and drag the icon to the management domain.

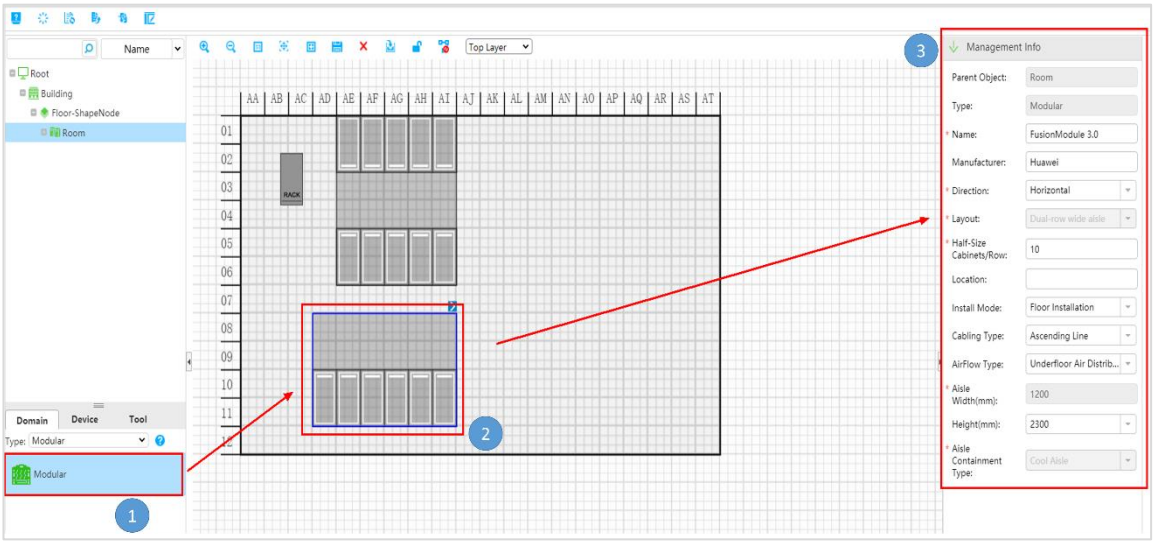


Figure 3-2 Adding a smart module in the equipment room

Step 6 Set Management Attributes for the smart module based on the site requirements or use the default parameters, and click.

----End

3.3 Adding a Device

3.3.1 Setting ECC800-Pro Communication Parameters

You have obtained the fixed IP address of the ECC800-Pro.

The procedure is as follows:

Step 1 Set the **IP address, subnet mask**, and **default gateway** on the ECC800-Pro WebUI.

Table 3-1 ECC800-Pro IP parameters

Operation Path	Parameter Name	Default Address	Set Address
System Settings > System Parameters > Monitor IP > WAN_1	IP address	192.168.8.10	Set this parameter based on the IP address assigned by the network administrator.
	Subnet mask	255.255.255.0	
	Default gateway	192.168.8.1	

Step 2 Click **Submit**.

Step 3 Set the NetEco communication parameters and authentication password on the ECC800-Pro WebUI.

Table 3-2 Setting NetEco Communication Parameters

Operation Path	Parameter Name	Default value	Set Value
System Settings > Network Management Application > NetEco > Communication Parameters	NetEco Deployment Position	Local	Set this parameter based on the type of the connected NetEco management system. Local: NetEco Cloud: CloudOpera NetEco
	Server IP Address	192.168.8.11	Set this parameter to the IP address of the active NetEco server.
	Port No.	31220	31220
	Link setup monitoring IP address	WAN_1	WAN_1 or WAN_2

Table 3-3 Setting the Authentication Password

Operation Path	Parameter	Default value	Set Value

	Name		
System Settings > Network Management Application > NetEco > Set Authentication Password	Authentication password	Modifyme_123	Set this parameter based on user requirements.
	Confirm Authentication Password	/	/

Step 4 Click **Submit**.

----End

3.3.2 Creating an ECC800-Pro on the NetEco

You have created a Mdule management domain.

The procedure is as follows:

Step 1 Choose System > Service Settings > Data Center Planning.

Step 2 On the Planning gpage, click **Uncreated Device** in the upper left corner.

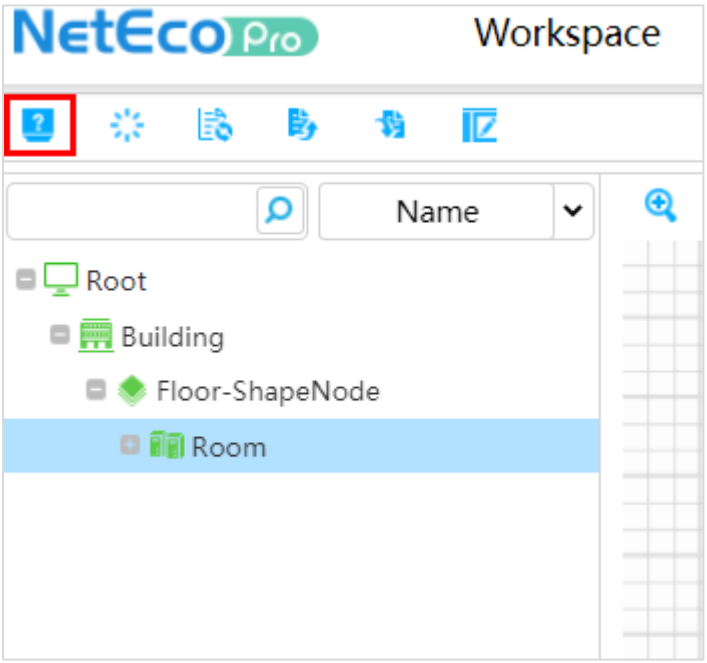


Figure 3-3 Uncreated Device Infomation

Step 3 Click **Access**. On the displayed Device Access page, you can add the ECC800-Pro to the specified smart module.

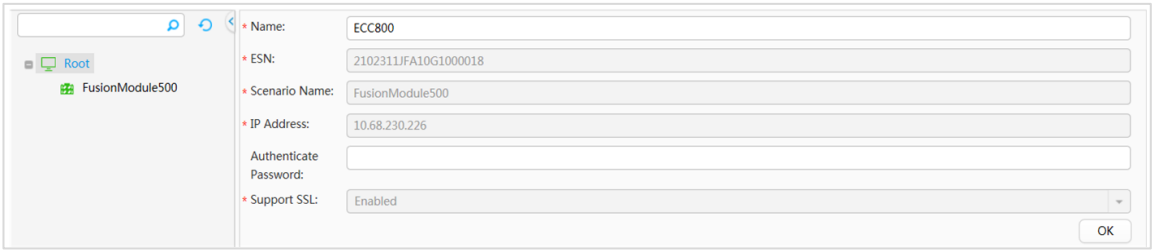


Figure 3-4 Adding the ECC800-Pro

Step 4 Perform subsequent operations as prompted.

----End

4 Monitoring Operations

4.1 Device Management

The centralized management and real-time monitoring of data center devices helps users learn about device running status and handle exceptions, ensuring device security.

4.1.1 View Management

View management displays the layout and running status of devices in the equipment room and monitors the running status of devices on the entire network in real time.

4.1.1.1 Toolbar Overview

After a management domain is created, you can use the tool in the toolbar to operate and manage objects in the management domain view.

The procedure is as follows:

Step 1 Choose Monitor > Device Management > Data Center View.

Step 2 Click the right arrow on the left of the page to expand the navigation tree. Select an equipment room and use the toolbar in Table 4-1 to view and edit the equipment room view.

Table 4-1 Toolbar

tooling	Explanation
	Select 2D, 2.5D, or 3D to display the equipment room view. The 2.5D view is displayed by default.
	View the basic information about sub-administrator domains or devices in the management domain and the statistics of faulty devices, license consumption, and disconnected devices in the management domain.
	View the real-time monitoring indicator signals of IT cabinet devices in the management domain.
	After adding a control to the management domain, save the modification. Controls in the toolbox must be unlocked  to be added to administrative domains.

	When the toolbox is locked, the current view cannot be edited.
	Control elements can be created in 2D and 2.5D equipment rooms.
	After a temperature sensor is configured in the management domain, you can view the temperature map in the equipment room, container, smart module, or floor layout outlet in the 2D view and in the floor, equipment room, smart module, or floor layout outlet in the 3D view.
	If a camera has been added to the management domain, click this button to view the camera information. Click the name of an online camera in the Name column. The playback page is displayed.
	Aligns the selected control vertically.
	Aligns the selected control horizontally.
	You can select a management domain or device type from the drop-down list box to display the management domain or device.
	View the power supply link diagram of the equipment room. This button is displayed in the equipment room after the equipment room electrical single line diagram has been configured on the Single Line Diagram page or the NetEco automatically generates a power supply link diagram based on data obtained from the ECC800-Pro. After you create an integrated PDC, integrated UPS, precision PDC, or smart busway in the smart module 3.0 of the ECC800-Pro, configure the power distribution parameters and synchronize the parameters to the NetEco, the power supply link diagram can be automatically generated on the NetEco but cannot be edited.
	View the cooling link diagram of the smart module. This button is displayed when the smart module contains at least one of air conditioner_NetCol5000-A025_BIN4 and air conditioner_NetCol5000-A042_BIN4. When the air conditioner is properly connected: ➢ When the air conditioner fan is started, the air inlet and outlet flow charts of the air conditioner in the smart module are displayed. ➢ When the compressor is started, the refrigerant can be dynamically circulated. ➢ When the outdoor unit is started, the fan status of the outdoor unit is displayed as rotating, and the outdoor temperature is displayed next to the outdoor unit.

	➢ The color of the cold aisle varies with the temperature. ➢ When the air conditioner is disconnected, the flow effect is still.
	Rotate the view.
	The system displays the device view based on the size of the screen, so that all the elements of the view are displayed in the window.
	Zoom in the view.
	Zooms out the view.
	Click this icon in the lower right corner of the 2D or 2.5D page. The panorama is displayed. Click  to close the panorama.

----End

4.1.1.2 Viewing the Management Domain View

The NetEco can display the management domain view in 2D, 2.5D, or 3D mode to meet the view requirements in different scenarios.

The procedure is as follows:

Step 1 Choose Monitor > Device Management > Data Center View.

Step 2 Click the right arrow on the left of the page to expand the navigation tree and select an equipment room.

- In the view, you can view details about equipment rooms and all devices or management domains in the equipment room and handle alarms.
- 2D/2.5D view
  - Move the cursor to the management domain or device to view the tips that are displayed. Double-click a device to view the view page of the device in the current equipment room.
  - Click  to view the temperature map of the upper, middle, and lower layers of the equipment room. The color of the temperature map varies with the temperature in the room.
- 3D view
  - Click Power, Cooling, Space, and Load Bearing to determine the cabinet usage based on the color and height of the color projection in the cabinet. The color and height of the color projection in the cabinet vary with the cabinet usage.

- Click  to view the temperature map of the upper, middle, and lower layers of the equipment room. The color of the temperature map varies with the temperature in the room.
- Click  or drag the mouse to rotate the 3D view.
- Click Transparent Wall. The wall color changes to transparent.

- In the right pane of the current page, view the resources, energy efficiency, environment, and alarm information of the management domain.
- Resources.
  - Displays the capacity and real-real-time device details of the equipment room. Click Resource. In the displayed Resource dialog box, the power, cooling, and space usage of the smart module and other cabinets (excluding the smart module in the equipment room) are displayed.
- Energy efficiency.
  - By default, the PUE, total power consumption, IT power, and cooling power of the equipment room are displayed.
  - Click Energy Efficiency. In the displayed dialog box, the PUE, IT power consumption, air conditioner power consumption, and other power consumption in the equipment room are displayed by hour, day, month, or year. You can click PUE, IT Power Consumption, or Air Conditioner and Other Power Consumption to display or hide the trend chart. When the trend chart is highlighted, it is displayed.
- Environment
  - If 25 kW or 42 kW air conditioners are installed in the equipment room, measure the average temperature, maximum temperature, average humidity, and maximum humidity of the cold aisle. If no, measure the average temperature, maximum temperature, average humidity, and maximum humidity of the equipment room.
  - Click Environment of a non-cabinet. In the displayed Average Temperature and Humidity Change Curve dialog box, view the 24-hour average temperature and humidity of the management domain.
  - Click Environment of the cabinet. In the displayed Average Temperature Change Curve dialog box, view the average temperature of the cabinet before and after 24 hours. You can click Average Temperature (Front) or Average Temperature (Bear) to display or hide the trend chart. When the trend chart is highlighted, the temperature is displayed.
- Alarm
  - By default, the number of uncleared alarms in the equipment room is displayed by alarm severity and device type. For details about the device types, see Table 4-2.
  - Click Alarms. In the displayed dialog box, the list of uncleared alarms is displayed. You can sort, export, and clear alarms.

Table 4-2 Device Type

Device Type	Device Name
Power supply	PDU, UPS, ATS, D.G., transformer, battery string category, and RPDU.
refrigeration	Chillers, pumps, cooling towers, and air conditioners.
environment	Water sensor, smoke sensor, and temperature and humidity sensor in the equipment room or smart module.
Security protection	Access control, camera, cabinet electronic lock, and fingerprint controller.
Others	Alarms reported through the collector.

----End

4.1.1.3 Viewing the Device

Displays device information, such as overview, alarms, and signals. Users can learn device status in real time and handle abnormal data to better understand device running status.

The procedure is as follows:

Step 1 Choose Monitor > Device Management > Data Center View.

Step 2 Click the right arrow on the left of the page. In the navigation tree, select a device in the equipment room. Details about the device are displayed. You can perform related operations as required. For details, see Table 4-3.

Table 4-3 Operation Task

Operation Type	Explanation	Operation Method
Modifying Device Configurations	Users can quickly modify device configurations.	Click the device name to go to the Configuration Design page.
Setting Monitoring Indicators for Devices	You can set device monitoring indicators to monitor devices more effectively and handle abnormal data in a timely manner.	1. Click  . 2. In the dialog box that is displayed, select indicators to be displayed. 3. Click OK. After the setting is complete, the configured indicator information is displayed.
Managing Device Alarms	Users can view and handle device alarms in a timely manner.	Click the alarm name to view the alarm details.
Setting a	This feature enables users to	Click the metric name to go to the

Monitoring Template	quickly set device monitoring templates.	Monitoring Template Configuration page.
Managing Monitoring Views	You can view and modify the monitoring view to learn the detailed running status of the device.	Click in the Operation column of a device signal value indicator. In the Monitoring View dialog box, view and modify the monitoring view.
Viewing Device Signals	View the real-time signals of the device to learn the device running status.	In the navigation tree on the left, select a device and click the Signal tab to view the monitoring signal information of the device.

----End

4.1.1.4 Viewing the Temperature Nephogram

You can view the temperature map in the 2D view of the equipment room, container, smart module, or floor layout, and in the 3D view of the floor, equipment room, smart module, or floor layout, helping you learn about the indoor temperature and better monitor the device running status.

The color of the temperature map changes with the indoor temperature and is refreshed in real time. The color of the temperature map is displayed as the color of the corresponding temperature.

The procedure is as follows:

Step 1 Choose Monitor > Device Management > Data Center View.

Step 2 Click the right arrow on the left of the page to expand the navigation tree and select an equipment room.

Step 3 View the Temperature Nephogram.

- In the 2D or 2.5D view, click on the toolbar. The temperature map of the equipment room is displayed, as shown in Figure 4-1. You can move the pointer to a device or sensor to view the current temperature and location information. Click the up arrow in the lower part of the page to view the top 5 temperature data of the temperature cloud sensor.

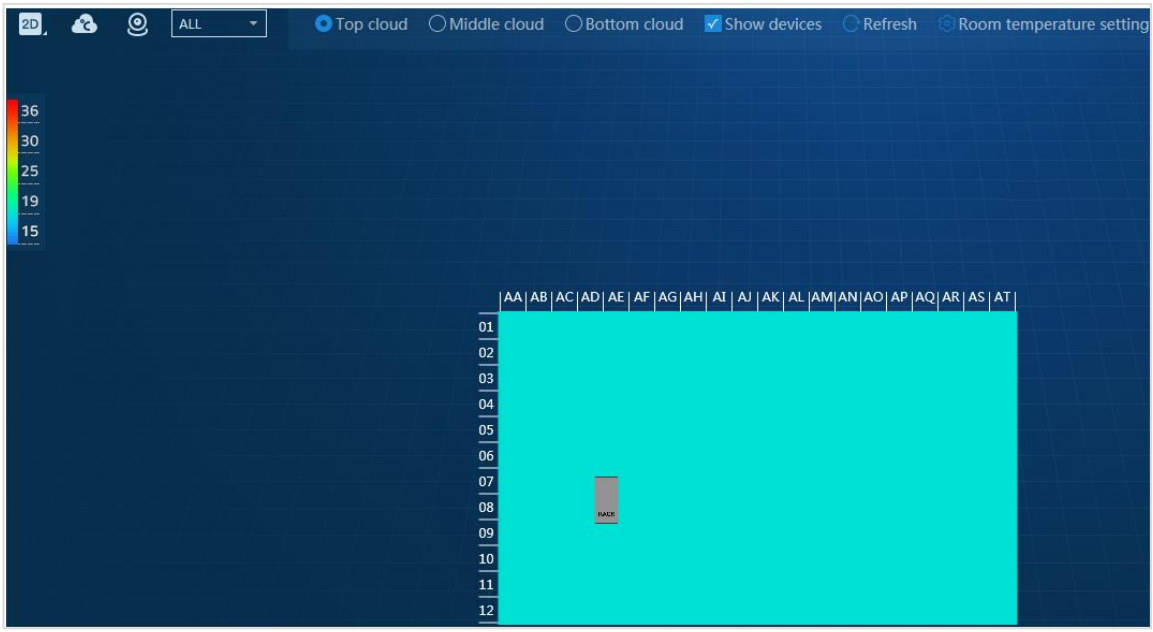


Figure 4-1 Temperature Nephogram of 2D view

- In the 3D view, click Temperature Map. The temperature map of the equipment room is displayed, as shown in Figure 4-2. Click Top5 at Air Inlet or Top5 at Air Outlet to view the top5 temperatures of air inlet sensors or air outlet sensors in the cabinet.

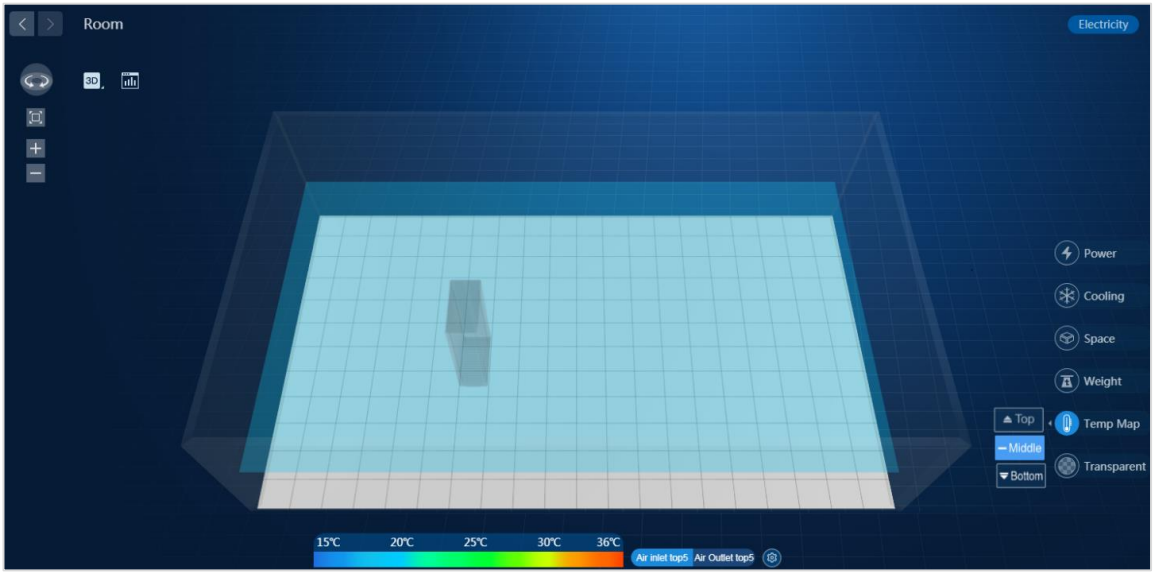


Figure 4-2 temperature nebula

----End

4.1.2 Customizing a Monitoring View for a Large Screen

The large-screen monitoring function allows users to display monitoring services such as topology on a large-resolution screen, helping users monitor important information and display IT O&M effects.

The procedure is as follows:

Step 1 Choose Monitor > Device Management > Big Screen Monitor.

Step 2 To customize a monitoring view on a large screen, perform the following steps:

- Click  in the row of view.
- In the **Create View** window, set the name of the view.
- Click **OK**.
- Click **Add Widget**.
- Click the selected widget to add it to the view. Table 4-4 describes the services that can be added to the big-screen monitoring view.

Table 4-4 Monitoring Service Description

Type	Portlet	Description
Monitor	Title Bar	Helps customers customize titles.
	Topo	Displays the view of the management domain.
	Cooling	Displays the cooling teamwork topology.
	Electricity	Displays the topology of the power transformation and distribution system.
	Chiller Group	Displays the Chiller Group topology.
Capacity	SPC change	Displays the monthly change curve of used and available SPC (Space, Power, and Cooling Capacity) under a management domain within the latest year.
	SPC Usage	Displays the SPC (Space, Power, and Cooling Capacity) usage of a management domain.
Alarm	Alarms on Top N Devices	Displays alarm statistics collected on the **Current Alarms** devices. You can click the number in the corresponding alarm severity column to switch to the **Current Alarms** page.
	Alarms by Device Type	Collects alarm statistics by device type. Refresh interval: 1s (default value)
	Alarms by Severity	Collects alarm statistics by severity.
	Alarm radar	Displays the current alarm sources.
	Device Operating Status	Displays the Operating Status of IT devices.
	Latest Alarms	Displays the latest alarms.

battery	Battery Group SOC	Displays the SOC of a battery group.
	Battery Group SOH	Displays the state of health (SOH) of a battery group.
	SOC of Multiple Battery Groups	Displays the SOC of multiple battery groups.
	SOH of Multiple Battery Groups	Displays the state of health (SOH) of multiple battery groups.
	Battery Info	Displays the battery string information about a UPS device.
	Single Battery Info	Displays the information of a single battery. Refresh interval: 1s (default value)
Energy efficiency analysis (PUE parameters must be configured in advance.)	PUE	Displays the energy efficiency data in real time, namely, the real-time PUE of the management domain selected.
	PUE change	Displays the PUE trends in the past month.of the management domain selected.
	Today Energy Consumption Statistics	Displays the total energy consumption and the energy consumption of IT devices on the current day of the management domain selected.
	Monthly Energy Consumption Change	Displays the energy consumption change trends by IT device, cooling and Other type collected in the past month of the management domain selected.
	Yesterday Carbon Emission	Display yesterday's carbon emission of domains. Carbon emissions = Power consumption x Carbon emission coefficient.
	Energy Consumption Proportion	Displays the energy consumption proportion of IT, cooling devices and other devices (except IT and cooling devices) in the past month.
	Today IT Energy Consumption Proportion	Displays the proportion of IT device energy consumption in the total energy consumption on the current day.
	Today PUE Change	Displays the hourly PUE change within the latest 25 hours.
	Safe Operation Status	Displays the power consumption and fees of the selected management domain.

	Energy Consumption Trend	Displays the IT energy consumption of each management of the room, modular, and container in the past and current months.
	Monthly Energy Consumption Curve	Displays the past month energy consumption change of the IT device, cooling device, and other devices.
	PUE Rankin	Displays the real-time PUE rankings of the room, modular, and container.
KPI	KPI	Displays the changes of multiple KPIs of a device.

Step 3 Click **Save**.

Step 4 To display the current view in full screen, click **Big-screen mode**.

Step 5 You can set the screen matrix and resolution as follows:

- Click  on the current page. In the displayed Settings dialog box, click Screen Settings and perform the settings. You can also click **Slide Settings** and set the polling interval for each split screen and select the portlets for polling.Set the screen resolution to the resolution of the large screen used for projection. The resolution is not affected by the number of split screens.
- If the content needs to be projected onto one large screen, set the number of split screens to 1*1. If the content needs to be projected onto four split screens (the content on each split screen is different), set the number of split screens to 2*2. Set the number of split screens by following the preceding principles.

----End

4.2 Performance Management

Performance management provides a monitoring method for network management and maintenance personnel to check and monitor the running status of devices in the past period, learn about the running trend of devices, and take measures based on the running status.

4.2.1 Querying Historical Data

Historical data refers to the measurement values of performance indicators during device running or statistics in a period. By querying historical data, you can learn about the running status of the device in a specified period. Users can query historical data by device type. The query result can be displayed in a report or line chart.

The procedure is as follows:

Step 1 Choose Monitor > Performance Management > Historical Data.

Step 2 In the left pane, select a device to be queried.

Step 3 Select **Device Type**, and click **Query** in the lower part.

Step 4 Select devieces and counters by device type, at the top of the query results screen.

Step 5 Click on the chart location and select the query time at the top left of the interface.

Step 6 Check the historical data result.

----End

4.2.2 Sync History Data

This feature enables users to learn about the loss of power consumption data in a timely manner and take measures to rectify the loss. If the data is incomplete or lost in a certain period of time, you can recollect historical data.

The historical data supplementary collection function supports all devices connected to the BIIN4.0 protocol.

The procedure is as follows:

Step 1 Choose Monitor > Performance Management > Historical Data Sync.

Step 2 Under the root node in the left pane, select ECC800-Pro device.

Step 3 Select the time range for supplementary collection.

Step 4 Click **Create Task** to recollect historical data.

Step 5 In the displayed dialog box, click **OK**. The synchronization progress of the device is updated in the right pane. Check whether the supplementary collection is successful.

----End

4.2.3 Monitoring Template Configuration

The device monitoring template enables the system to automatically collect key device data. After a device is created, the NetEco automatically generates a collection task based on the preset template to collect device indicator data.

The procedure is as follows:

Step 1 Choose Monitor > Performance > Monitoring Template Settings.

Step 2 Select a device type from the navigation tree on the left and click the Sampling, Configuration, or Statistics tab in the right pane. After the setting is complete, the collection task of the corresponding indicator is delivered to the connected device along with the template.

Table 4-5 Monitoring Template Function

Function Type	Scenario	Purpose
Sampling	You need to collect the running data of each indicator connected to the monitoring device.	Used to display data of the AI and DI access types on the Device Signal page.
Configration	Collect the running data of each indicator output by the monitoring device.	Used to display the AO and DO output data on the Device Signal page.
Statistics	Collect statistics on historical device data.	Used to query historical data.

Table 4-6 Monitoring Template Comfigration

Operation Type	Scenario	Operation Method
Apply	Modify the attribute values related to device component information collection.	In the device part list, set the corresponding attribute values. Click **Apply** in the upper left corner.
Revoked	The collection periods of some device indicators have been modified but have not been applied. The configured parameters are canceled.	Click **Revoke** in the upper left corner.
Batch apply	Set parameters for certain counters in batches.	Click **Batch Apply** in the upper left corner. In the displayed **Batch Apply** dialog box, set Indicator Name and Attribute Name and set the corresponding attribute values. Click **OK**.

----End

5 Alarm Management

The NetEco provides management functions, such as monitoring network alarms, querying alarms, and setting remote alarm notification, to quickly detect, locate, and rectify network faults.

5.1 Current Alarms

On the **Current Alarms** page, engineers can view the current alarms that are updated in real time to learn the latest alarm status. Engineers can handle alarms to facilitate troubleshooting. For example, you can specify an alarm handler, acknowledge an alarm, and clear an alarm.

5.1.1 Monitoring Alarms

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Current Alarms.

Step 2 Table 5-1 describes the alarm monitoring methods.

Table 5-1 Alarm monitoring methods

Task	Task Description
Monitor alarms in the alarm list of the Current Alarms window.	On the Current Alarms page, you can monitor alarms reported by all network elements and the system in real time. This page displays a maximum of 100,000 alarms.
Monitor alarms in the alarm panel of the Current Alarms window.	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.

----End

5.1.2 Querying Alarms

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Current Alarms.

Step 2 You can click **Template Management** in the upper left corner of the page to view all filter templates, and select a filter template on the **Quick Filter** panel. Users with the Administrators role can manage templates saved by all users.

The system provides the following types of templates:

- **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. A user with the Administrators role and the current template is not shared can set a custom template as the key template. The alarms that are filtered using the key template are displayed both on the Emergency Maintenance Notification panel and in the alarm list. However, only the users who manage all objects can view these alarms.
- **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.

Step 3 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.

Step 4 Click **Save** or **Save As** to save the current filter criteria as a filter template.

Step 5 Export current alarms. Alarms can be exported to an .xlsx or .csv file. When the number of alarms to be exported exceeds 100,000, the file is compressed to a .zip package and then exported.

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

----End

5.1.3 Handling Alarms

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Current Alarms.

Step 2 Alarm management provides the operations of acknowledging and clearing alarms, as shown in Table 4-2. Figure 4-1 shows the alarm status transition relationship.

Table 5-2 Alarm Handling Operations

Name	Function	Explanation
Acknowledge	Identifies the user who handles an alarm to avoid one alarm being handled by multiple users.	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 engineer B wants to handle an alarm acknowledged by engineer A, engineer B can unacknowledge the alarm. When the alarm is unacknowledged, the alarm status is changed from acknowledged to unacknowledged.
Clear	Identifies whether the fault that causes an alarm is rectified.	When a fault occurs on the interconnected NE or in the system, an alarm is generated. When the fault is rectified, a clear alarm is generated and the alarm is cleared. If the system fails to receive the clear alarm or the alarm cannot be automatically cleared due to a network fault, you need to manually clear the alarm. When you manually clear the alarm, an alarm clearance command is sent from Alarm Management, and then the corresponding NE or system clears the corresponding alarm.

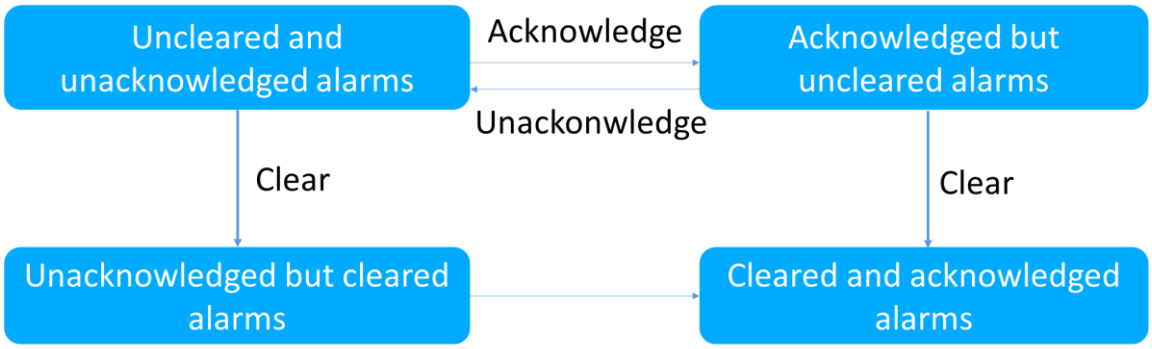


Figure 5-1 Alarm status transition

Step 3 On the Current Alarms page, perform the following operations. For details, see Table 5-3.

Table 5-3 Operation Description

Operation Name	Scenario	Operation Method
Viewing alarm details	Obtains key alarm information, including alarm names, repair recommendations, and location	In the alarm list, click the arrow on the left of the row

	information, to facilitate fault diagnosis and troubleshooting.	that contains a desired alarm to view the alarm details.
Manually acknowledging alarms	An acknowledged alarm indicates that the alarm is being handled by the user whose name is displayed in the Acknowledged By column. When the alarm is acknowledged, the alarm status is changed from unacknowledged to acknowledged.	You can select one or more alarms and click Acknowledge above the alarm list. You can also click ✓ in the Operation column of the row that contains the desired alarm. After you have acknowledged an alarm, the username is displayed in the Acknowledged By column.
Specify a handler	Assigns the O&M personnel to handle an alarm.	In the alarm list, select an alarm and click ••• in the Operation column to select a user to handle the alarm. After the alarm is acknowledged, the username is displayed in the Handler column.
Manually clearing alarms	Some alarms cannot be automatically cleared. Therefore, you need to clear the alarms manually after the faults are rectified.	You can select one or more alarms and click Clear above the alarm list. You can also click  in the Operation column of the row that contains the desired alarm.
Recording experience	After handling an alarm, the O&M personnel can record the handling experience for future reference in a timely manner. Choose **Alarm > Alarms > Alarm Settings** from the main menu. In the navigation pane, choose Experience to manage the experience.	In the alarm list, click the arrow on the left of the row that contains a desired alarm to view the alarm details. On the Experience tag page, click Modify to enter comments.

----End

5.2 Historical Alarms

By analyzing historical alarms, you can learn about the running status of the device and check whether the rule configuration is proper.

By default, 20,000 historical alarms are displayed. When the number of alarms exceeds the upper limit, the top 20,000 alarms are displayed based on the filter criteria and sorting. To query other alarms, you can modify the filter criteria and sort the alarms.

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Historical Alarms.

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 system provides the following types of templates:

- **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.

Step 4 Export historical alarms or masked alarms. The system supports the export of .xlsx or .csv files. If the number of exported alarms exceeds 100,000, the files are exported in .zip format.

- Export some alarms: Select the alarms to be exported, click **Export**, and **Selected**.
- To export all alarms, click Export and select **All**.

5.3 Alarm Settings

You can set alarm rules to customize alarm monitoring policies to improve fault rectification efficiency.

5.3.1 Setting Alarm Colors

You can set colors for alarms of different severities so that you can easily browse concerned alarms.

By default, the system provides four alarm severities: red, orange, yellow, and blue.

Critical:

Major:

Minor:

Warning:

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Alarm Settings.

Step 2 In the navigation pane on the left, choose **Personalization > Color Settings**.

Step 3 On the **Color Setting** page, set colors for different alarm severities.

Step 4 Click **OK**.

----End

5.3.2 Setting Alarm Sounds

You can set alarm sounds at different severities or specify alarm sounds for alarm names to facilitate alarm monitoring. When an alarm is generated, the sound box on the user's computer plays the corresponding sound.

The system provides four alarm sounds by default. Critical or sounding by alarm name: Critical.mp3; Major.mp3; Minor.mp3; Warning.mp3.

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Alarm Settings.

Step 2 In the navigation pane on the left, choose **Personalization > Alarm Sound**.

Step 3 On the Alarm Sound page, set the sound for different severities.

- Click  to preview the selected sound file.
- Click  in the displayed **Custom Alarm** Sound dialog box, you can upload, view, and delete custom sound files.
- Click  and select the alarms that are sounded by alarm name. A maximum of 20 alarms can be selected.

Step 4 Set Alarm Status for alarms at different severities for which the system will play sounds.

- When an alarm of a specific severity is reported or the alarm status changes to the specified monitoring status, an alarm sound is generated.
- The system can sound based on the alarm monitoring status only when the number of current alarms exceeds 50,000.

Step 5 Set the duration for playing the alarm sound. When an alarm is reported, the alarm sound is automatically stopped after the specified duration. When all the alarms at a severity with an alarm sound being played are cleared, the alarm sound is automatically stopped.

Step 6 Select whether to enable the sound setting. If the sound setting is disabled, the sound is not played when an alarm at the corresponding severity is reported.

Step 7 Click **OK**.

----End

5.3.3 Highlighting Alarms

If an alarm is not handled within the specified period (that is, the alarm status remains unchanged), the alarm is highlighted in the alarm list, prompting you to pay attention to the alarm. By default, this function is disabled.

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Alarm Settings.

Step 2 In the navigation pane on the left, choose **Personalization > Highlight**.

Step 3 On the Highlight page, set **Effective Time** (min) and **Alarm Status.** After an alarm at the severity is generated, the alarm is highlighted if the duration of the alarm in the specified status is greater than or equal to the specified effective time.

Step 4 Specifies whether to highlight alarms of the corresponding severity.

Step 5 Click **OK**.

----End

5.3.4 Configuring a Masking Rule

You can create masking rules for alarms that are reported but do not need to be concerned. Then, the alarms that meet the masking rules are not displayed in the current alarm list. A maximum of 1000 masking rules can be created.

Device alarms are critical to O&M. Before configuring masking rules, obtain approval from the O&M director or manager. If necessary, contact Huawei technical support.

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Alarm Settings.

Step 2 In the navigation pane on the left, choose **Masking Rules**.

Step 3 On the Masking Rules page, click Create and select **Alarm Masking Rules**.

Step 4 In the **Basic Information** area, set the rule name, description, and whether to enable the rule.

Step 5 In the **Condition** area, set the alarm severity, alarm, and alarm source for the rule to take effect. You can set advanced conditions to filter the alarms for which the rule takes effect based on alarm parameters.

- By default, Specified alarm is deselected, indicating that the rule takes effect for all alarms.
- You can select All alarm sources only when the managed objects are all resources.
- When setting Alarm Source, select All alarm sources to mask the alarms generated by the system and all managed objects. Exercise caution when setting Alarm Source.

Step 6 In the **Time Filter** area, set the time when the rule takes effect. You can select the effective time and period as required.

- By default, all conditions in Time Condition are deselected, indicating that the rule takes effect at all times.

Step 7 Masked alarms can be discarded or displayed in the **Masked Alarms** list.

- When you create an event masking rule, masked events can only be discarded.
- If you select Discard, the alarm cannot be viewed. Exercise caution when performing this operation.

Step 8 Set the priority of the rule. When two masking rules mask the same alarm, the rule with the highest priority takes effect.

Step 9 Click **OK**.

----End

5.3.5 Configuring an Auto Acknowledgment Rule

When the number of current alarms reaches the threshold, the system processes the current alarms and changes the current alarms to historical alarms. To prevent the number of major alarms from being fully processed, you can set automatic acknowledgment rules to automatically acknowledge cleared current alarms as historical alarms.

Automatic acknowledgment rules take effect only for unacknowledged and cleared alarms. Alarms cleared before immediate acknowledgment is enabled are not affected.

A maximum of 1000 automatic acknowledgment rules can be configured. The system has four preset rules, and a maximum of 996 rules can be created.

If an alarm meets the automatic acknowledgment rules of both immediate acknowledgment and delayed acknowledgment, the alarm is acknowledged in immediate acknowledgment mode.

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Alarm Settings.

Step 2 In the navigation pane on the left, choose **Auto Acknowledgement Rules**.

Step 3 In the automatic acknowledgment rule list, check whether the first four preset automatic acknowledgment rules of each alarm severity meet the requirements.

- If yes, go to Step 4.
- If no, go to Step 5.

Step 4 Enable the automatic acknowledgment rule by alarm severity. For example, after the automatic acknowledgment rule for major alarms is enabled, cleared but unacknowledged major alarms are automatically acknowledged. In the automatic acknowledgment rule list, the first four rules are preconfigured in the system. Only users whose managed objects are all resources can enable or disable automatic

acknowledgment rules. (Before performing these operations, obtain the approval of the O&M director or manager.)

- Select the required automatic acknowledgment rule and click Enable.
- In the Confirmation Mode column, view the confirmation mode of the rule.
  - Immediate acknowledgment: The alarm is automatically acknowledged immediately after being cleared.
  - Delayed acknowledgment: After an alarm is cleared, the alarm is automatically acknowledged based on the parameters set in Delay Settings.

Step 5 Create a custom automatic acknowledgment rule.

- On the Auto Acknowledgment Rule page, click Create.
- In the Basic Information area, set the rule name, description, and whether to enable the rule.
- In the Condition area, set the alarm severity, alarm, and alarm source for the rule to take effect. You can set advanced conditions to filter the alarms for which the rule takes effect based on alarm parameters.
  - By default, **Specified Alarm** is deselected, indicating that the rule takes effect for all alarms.
  - You can select All alarm sources only when the managed objects are all resources.
- In the **Others** area, set the rule confirmation mode.
- Click **OK**.

Step 6 On the **Auto Acknowledgement Rules** page, click **Change Delay** and set the parameters. If the acknowledgement mode is set to **Delay**, the system automatically acknowledges alarms based on the configuration in the **Change Delay** area.

- Click Delay Settings and set Execution Time and Duration.

Table 5-4 Parameters on the Delay Settings tab page

Parameter	Explanation
Execution Time	Time when an automatic alarm acknowledgement rule is executed on a daily basis.
Duration (Days)	A cleared alarm can be automatically acknowledged only when it has not been acknowledged for a period longer than the duration you set.

- Click **OK**.

----End

5.3.6 Configuring Remote Alarm Notification Rules

If O&M personnel cannot view alarms or events on the alarm management page due to non-working hours or business trips, they can configure remote notification rules to send concerned alarms or events to O&M personnel by email or short message, this helps users learn about alarms and events in time and take corresponding measures.

A maximum of 1000 remote notification rules can be created.

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Alarm Settings.

Step 2 In the navigation pane on the left, choose **Notification Rules**.

Step 3 On the Notification Rules page, click Create and select Alarm Notification Rules.

Step 4 In the **Basic Information** area, set the rule name, description, and whether to enable the rule.

Step 5 In the **Conditions** area, set the alarm severity, status, alarm, and alarm source for the rule to take effect. Set advanced conditions to filter the alarms for which the rule takes effect based on alarm parameters.

- By default, **Specified Alarm** is deselected, indicating that the rule takes effect for all alarms.
- You can select **All** alarm sources only when the managed objects are all resources.

Step 6 In the **Time Filter** area, set the time when the rule takes effect. You can select the effective time and period as required.

Step 7 Set the notification sending mode, content, recipient time zone, and recipient. When an alarm is reported, the system sends an email or SMS notification to users in the specified user group. Table 5-5 describes the parameters for creating a remote notification rule.

Table 5-5 Parameters for creating a remote notification rule

Parameter	Parameter Name	Explanation
Conditions	Alarms	If you select Designated alarms, the rule takes effect only for the alarms you added. Alarm ID and Group Name: Unique identifiers of an alarm. If you do not select Designated alarms, the rule takes effect for all alarms by default.
	Alarm sources	All alarm sources: indicates that this rule takes effect for the alarms generated by all alarm sources. Custom alarm sources: indicates that this rule takes effect only for the alarms of specified alarm

		sources.
	Advanced Conditions	Restrictions on items such as location information and alarm source type. For example, if you want to filter alarms by location information, select Location Info and contains and enter the alarm location information in the text box.
Time Filter	By period	Time range within which the rule will take effect. By default, Server time is selected.
	By month	Month for the rule to take effect in a year.
	By day	Days on which the rule takes effect in a week.
	By time	Period for the rule to take effect in a day.
Notification Method	E-mail	Indicates that notifications will be sent by email. You need to select a notification template.
	SMS message	Indicates that notifications will be sent by SMS message. You need to select a notification template.
	Delay (min)	Indicates that you can set the delay time for sending a notification. The system records the time when the alarm arrives at the alarm management system. If the alarm is cleared within the delay time after the alarm arrives at the system, no notification is sent. Otherwise, the notification is sent.
Recipient Time Zone	Recipient time zone	Indicates the time zone of the user who receives the notification. When the time zone of the recipient is different from that of the server, the alarm generation time in the notification is converted based on the time zone of the recipient.
Recipient Groups	Recipient groups	Sets the user groups for receiving the notification.

----End

5.3.7 Configuring a notification content template

If the default notification template does not meet user requirements, you can create a notification template and use it when configuring remote notification rules. The system fills the alarm information in an email or SMS message based on the notification template and sends the email or SMS message to the user.

The procedure is as follows:

Step 1 Choose Monitor > Alarm Management > Alarm Settings.

Step 2 In the navigation pane on the left, choose **Notification Content Template**.

Step 3 On the Notification Content Template page, click Create.

Step 4 In the **Basic Information** area, enter the template name and description.

Step 5 In the **Notification Method and Content** area, select an **Email** or **SMS** notification mode, and set the title and important information, such as the severity, name, and occurrence time.

Step 6 Click **OK**.

----End

6 Security Management

By managing access control devices and controlling access rights, the VCN integrates with the video management system to detect and handle exceptions in the equipment room in a timely manner, improving the security capability of the equipment room.

6.1 Access Control Management

Access control management includes access control device management, event list management, time group management, and access control user management.

6.1.1 Device Management

Device management allows users to browse, modify, add, and delete doors, and display the switch status in real time.

6.1.2 Creating an Access Control Device

You can add access control devices to the campus, building, floor, equipment room, container, cabinet, cabling cabinet, or some PDCs for security management.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 In the navigation pane on the left, choose **Device Management** and click **Create**. The System Design page is displayed.

Step 3 Add an access controller in the **Configuration Design** area. After the access control device is created, the created access controller is displayed in the device management list.

----End

6.1.2.2 Formatting an Access Controller.

Formatting can clear card permission, history, time group, and holiday information.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 In the navigation pane, choose **Device Management.**

Step 3 Click  in the Operation column. The Confirm dialog box is displayed.

Step 4 Click **OK**.

----End

6.1.2.3 Enabling a Time Group

After formatting, you need to enable the time group so that the time group and holiday can be used. Currently, only the Tycosun access controller supports time groups.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 In the navigation pane, choose **Device Management.**

Step 3 Click  in the **Operation** column. The Confirm dialog box is displayed.

Step 4 Click **Yes** to complete parameter initialization.

----End

6.1.2.4 Delivering Permissions

Delivers all access control user information related to the controller in the database to the controller.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 In the navigation pane, choose D**evice Management.**

Step 3 Click  in the **Operation** column. The Confirm dialog box is displayed.

Step 4 Click **OK**.

----End

6.1.2.5 Modifying door information

You can modify the door name and permission group of the access controller.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 Click **Device Management** and click  in the **Operation** column.

Step 3 On the page that is displayed, modify the door information and click **OK**.

----End

6.1.2.6 Setting door parameters

Set the door opening delay, lock status, bidirectional door, and linkage output of the access controller.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 In the navigation pane, choose **Device Management**.

Step 3 On the Device Management tab page, click  in the **Operation** column of a door. The Set Door Parameters dialog box is displayed.

Step 4 Set door parameters according to Table 6-1 and select the access controller to be set.

Table 6-1 Parameter description

Parameter	Explanation
Lock Status	The power supply status while doors are locked. Locked in power-on state: indicates that power is on while the door is locked. While the authentication is successful, power is off and the door opens. Locked in power-off state: indicates that power is off while the door is locked. While the authentication is successful, power is on and the door opens.
Output Linkage	After this parameter is set, if the smoke sensor and water sensor on the device side are properly connected, the corresponding door is automatically opened when a smoke sensor or water sensor alarm is generated.
Open Delay	Delay time for automatic lock after a door is opened by swiping the card.
Door Open Duration	This parameter specifies the period after which an event log is reported and an alarm is generated because the door stays open for this period.
Bidirectional Door	You can enable or disable the bidirectional door to determine whether two doors share the same lock.
Two Door Interlock	Only the door access controllers of Access Controller_TycoSun_A8804RS_ACESCTRL support the two door interlock function.

Step 5 Click **Finish**.

Step 6 In the displayed Confirm dialog box, click **OK**.

----End

6.1.2.7 Remote door opening and closing

You can remotely close or close the door.

The door of the access controller synchronized from the ECC800-Pro to the NetEco does not support remote door closing. After the door is opened remotely, the door automatically closes 6 seconds later.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 In the navigation pane on the left, choose **Device Management.**

Step 3 In the **Operation** column, perform the following operations:

- Click  to remotely open the door.
- After the door is opened remotely, the Tycosun access control system automatically closes 6 seconds by default. If you want to close the door in advance, you can close the door remotely.
- Click  to remotely close the door.

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

----End

6.1.2.8 Setting the authentication mode.

You can set the authentication mode of the access controller to select the door opening mode.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 In the navigation pane, choose **Device Management.**

Step 3 Click Authentication Mode Settings. The Authentication Mode Settings page is displayed.

Step 4 Set the parameters listed in Table 6-2. Select the access control device whose parameters need to be set.

Table 6-2 Parameter description

Parameter Value	Explanation
card	Swipe one card to open the door.
Fingerprint	Verify the fingerprint to open the door.
Card + password	Swipe one card and then type the four digits password in 6 seconds.
Dual cards	Swipe the primary card and then the secondary card within 6 seconds.
Card or	Open the door using a card, password, or fingerprint.

password or fingerprint	
Fingerprint + password	Record your fingerprint, enter a four-digit password within 6 seconds, and press the #.
Card + fingerprint sensor	Swipe your card and record your fingerprint within 6 seconds.
Card + password + fingerprint	Swipe your card, enter the password within 6 seconds, press #, and record your fingerprint within 6 seconds.

Step 5 Click Finish.

Step 6 In the displayed Confirm dialog box, click **OK**.

----End

6.1.3 Managing Event Lists

Records information about events such as card swiping on the access controller.

6.1.3.1 Querying Access Records

This interface is used to query the operation records of accessing the access controller in authentication mode.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 Choose Event List > Access Record.

Step 3 In the navigation tree, select the access controller whose door information you want to view, and set the search time range in **Time Period**.

Step 4 By default, access records of all access control devices in the 24 hours of the current day are displayed.

Step 5 Click Search.

----End

6.1.3.2 Querying Event Records

This interface is used to query the records of events such as opening and closing the door of the access controller.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 Choose Event List > Event Record.

Step 3 In the navigation tree, select the access controller to be viewed and set the search time range in the **Time Range** area.

Step 4 By default, all access control device event records within the 24 hours of the current day are displayed.

Step 5 Click **Search**.

Step 6 On the **Event Record** page, click  and select **Export Selected** or **Export All** to export event records.

----End

6.1.4 Time Group Management

6.1.4.1 Creating a Time Group

Create a time segment in which a user can use the access control function. (The time group is disabled by default.)

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 Choose Time Group Management > Time Group. The Time Group page is displayed.

Step 3 Click Create.

Step 4 Enter the time group name and set the time range as required.

Step 5 Click **OK**.

----End

6.1.4.2 Creating a holiday

Create a holiday period and a holiday time segment.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 Choose Time Group Management > Holidays. The Holidays page is displayed.

Step 3 Click **Create**.

Step 4 Enter a holiday name, select a time group, set a time period, and set a holiday period.

Step 5 Click OK.

----End

6.1.5 Access Control User Management

Allows users to browse, modify, add, and delete access users. Access control user information can be imported in batches.

The role permission group to which the user belongs and the members in the role permission group can be viewed.

6.1.5.1 Creating an Access Group

Create an access group based on the authorization plan and assign operation rights to the access controller.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 Choose Access User Management > Access Group. The Access Group page is displayed.

Step 3 Click **Create** to create a group.

Step 4 On the **Access Group** page, enter the name of the access permission group and click **Add**.

- In the **Select Permission** dialog box, select the door to be added.
- Click b.

Step 5 Click **OK**.

Access control users created on the ECC800-Pro can be automatically synchronized to the NetEco. After the synchronization, access control rights groups can be automatically created.

- After an access user created on the ECC800-Pro is synchronized to the NetEco, an access permission group named in the format of Access controller location/Collector name/User name_User ID is automatically created. The access rights group cannot be modified and cannot be selected when an access user is created.
- Access users who have unauthorized access rights created on the ECC800-Pro are automatically added to the Unprocessed Rights Group after being synchronized to the NetEco.

----End

6.1.5.2 Dual card Authentication group management

You can view information about a dual-card authentication group and change the name of the dual-card authentication group based on the site requirements.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 In the navigation pane, choose **Access User Management** and click  in the **Operation** column.

Step 3 Modify Authentication Group Name and Description.

Step 4 Click **OK.**

----End

6.1.5.3 Creating an Access Control User

Create an access user and add the user to an access permission group. Then, the user has the rights of the access permission group.

User authorization.

The procedure is as follows:

Step 1 Choose Monitor > Security > Access Control Management.

Step 2 In the navigation tree on the left, choose **Access User Management.**

Step 3 On the Access Control User page, click Create.

Step 4 Enter the basic information about the user, including the card number, card issuer settings, registration fingerprint, dual-card home group, dual-card pairing group, and expiration date.

- Card number: automatically displayed after you enter a card number or connect a card dispenser.
- Card Dispenser Settings: Set this parameter when the access control system is accessed by swiping a card. After the configuration is complete, swipe the card on the corresponding USB card reader to record the card number information.
- Register fingerprint: Set this parameter when the access control system is accessed using a fingerprint. You can enable fingerprint recording only when a USB fingerprint reader is properly connected.
- Password: Set this parameter when the access control system is accessed using a password.
- Dual cards Group & Dual cards match group: Set these parameters when the authentication mode of the TycoSun access controller is Dual cards.
- Expiry Date: User-defined expiration date must be earlier than or equal to the latest expiration date allowed by the system: 2037-12-31.

Step 5 Select a group.

Step 6 Click **OK**. The user is created and the access control information is delivered to the access controller in the permission group.

----End

6.2 Video management

Video management provides camera management, video grouping, and parameter setting functions.

6.2.1 Adding Huawei Cameras to the VCN

The following conditions must be met:

- The VCN has been connected to the camera through a switch, and the VCN and camera have been powered on.
- The IP addresses of the VCN and camera must be in the same network segment.
- The VCN IVS client has been installed.
- You have obtained the user name and password of the camera.

The procedure is as follows:

Step 1 Log in to the VCN IVS client as the Admin user.

- The default user name is **Admin** and the default password is **Change_me**. When you log in to the system as the Admin user for the first time, the system prompts you to change the password. Remember the new password.
- Set Server Address to the IP address of the VCN.
- The default value of Port is 9900. You are advised to retain the default value.

Step 2 In the **Quick Configuration** area on the IVS client home page, double-click **Add Camera**.

Step 3 Set search criteria.

- Select Driver. The default value is **ONVIF**. If an IPC6325 camera is added, set Driver to HWSDK.
- Click ➕ in the lower left corner and enter the start IP address and end IP address of the camera, as shown in Figure 6-1.

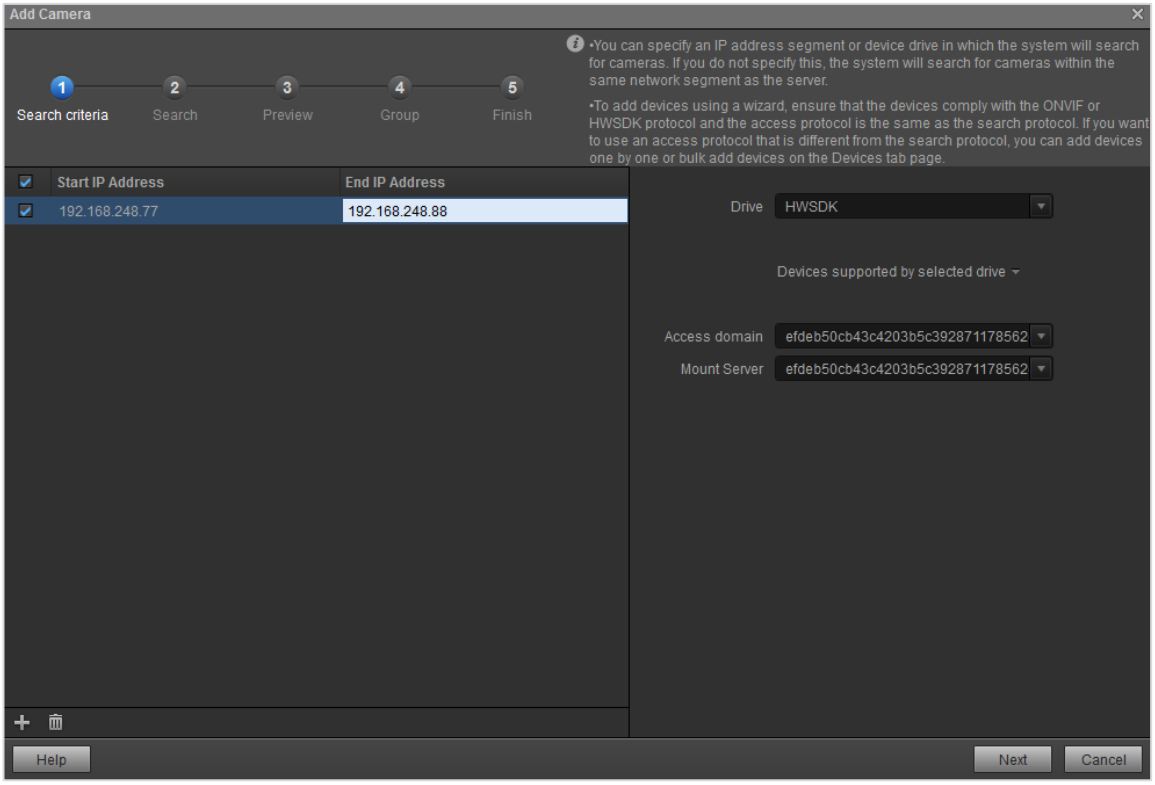


Figure 6-1 Set the start and end IP addresses.

Step 4 Search for and verify cameras.

- Click **Search**. The camera IP address is displayed.
- In the **Verification** area, enter the user name and password of the camera and click Verify. After the verification is successful, the icon turns green.

Step 5 Select the camera to be added and click **Next**. The camera preview page is displayed.

Step 6 Preview live video images and adjust camera name, installation position, and brightness.

Step 7 Click **Next**. The camera group page is displayed.

Step 8 After you click **Next**, the camera is added successfully.

Step 9 Click **Finish**.

----End

6.2.2 Setting Video Server Parameters

Set video server parameters. After the video server is connected, the camera information of the video server is automatically synchronized to the NetEco.

The procedure is as follows:

Step 1 Choose Monitor > Security > Camera Management.

Step 2 On the left of the page, choose **VCN.** The **Video Server Parameter Settings** page is displayed.

Step 3 Set video server parameters according to Table 6-3.

Table 6-3 Video server parameters

Parameter	Explanation	Example
Server IP Address	Server IP address: IP address of the VCN server. The value must be a number ranging from 0 to 255. The IP address cannot be 0.0.0.0.	10.144.197.253
Server port number	Port number of the VCN server.	9900
Login User	User name for logging in to the IVS client.	Admin
Login password	Password for logging in to the IVS client. Click Set Password. In the Set Password dialog box, enter the password of the login user.	Change_me

Step 4 Set the parameters and click **Test**. If the test fails, check whether the parameters are set correctly.

Step 5 Click **Apply**.

----End

6.2.3 Adding Cameras Using Automatic Discovery

You can quickly add online or offline Huawei cameras that have not been added to the management domain by using the NetEco automatic discovery function.

The procedure is as follows:

Step 1 Choose Monitor > Security > Camera Management.

Step 2 In the navigation pane on the left, choose **Camera Auto Discovery**.

Step 3 On the **Discovery Camera** page, select one or more cameras and click **Create**.

Step 4 In the **Create Camera** dialog box, set parameters.

Step 5 Click **OK**.

----End

6.2.4 Group Management

Create multiple cameras as a group. Videos in the same group are played in split-screen mode.

You can delete, modify, or query camera group information.

The procedure is as follows:

Step 1 Choose Monitor > Security > Camera Management.

Step 2 In the navigation pane on the left, choose **Group Management.**

Step 3 On the **Group Management** page, perform operations as required. For details, see Table 6-4.

Table 6-4 Operation Task

Operation Task	Operation Method
Creating a group	➢ Click **Create**. The **Create Group** page is displayed. ➢ Enter the group name and description as prompted. ➢ Select a camera from the camera list and select the number of split screens in the right area. ➢ Click **OK.**
Deleting a group	You can delete one or more groups as required.
Modifying a group	➢ Click  next to a group. The page for modifying a group is displayed. ➢ Change the group name and description as prompted. In the camera list, change the number of split screens in the right area. ➢ Click **OK**.
Playing Videos	➢ Click  next to the group to view the surveillance videos of the group.

----End

6.2.5 Camera Management

View camera details, create cameras, and play videos.

The procedure is as follows:

Step 1 Choose Monitor > Security > Camera Management.

Step 2 In the navigation tree on the left, choose **Camera Management.**

Step 3 On the Camera Management page, perform operations as required.

- View camera information.
- Create a camera.
- Play a video.

----End

6.2.6 Viewing Historical Videos

Users can view manually recorded videos and videos automatically recorded by the VCN IVS client when an associated alarm is generated.

The procedure is as follows:

Step 1 Choose Monitor > Security > Camera Management.

Step 2 On the Video Management page, choose Historical Video.

- If the system prompts you to install the OCX control, click Yes.

Step 3 On the **Video Playback** page, set search criteria on the left and view the Historical Video on the right.

----End

7 Energy Efficiency Management

Energy efficiency management provides energy efficiency analysis, energy efficiency configuration, iCooling energy efficiency, and cooling capacity management functions. Users can customize energy efficiency parameters and optimal iCooling algorithms, and collect and analyze energy efficiency and cooling capacity data.

7.1 Energy Efficiency Configuration

You can create, modify, delete, and view electricity price policies, configure electricity price units, view current configurations and PUE alarm thresholds, and configure and query power usage effectiveness (PUE) indicators and cabinet electricity.

7.1.1 Tariff Configuration

Users can create, delete, modify, and view electricity price policies.

7.1.1.1 Tariff Policies

You can create, modify, and delete electricity price policies based on the local electricity price.

The procedure is as follows:

Step 1 Choose Energy > Energy Efficiency Management > Energy Configuration.

Step 2 In the navigation tree, choose Tariff Configuration > Tariff Policy.

Step 3 In the **Tariff Policy** page, you can create, modify, or delete tariff policies.

Table 7-1 Task Description

Task	Explanation
Creating a tariff policy	➢ Click **Create**. The page for creating a tariff policy is displayed, enter the tariff policy information. ➢ Click **Energy Policy**, **Month Policy** or **Hour Policy** to create tariff policies ➢ Click **Next**. The page for selecting management domains is displayed, select management domains. ➢ Click **Next**. The information confirming page is displayed, Click **Finish**. The tariff policy is successfully created.

Modifying a tariff policy	➢ Click in the **Operation** column corresponding to the target policy to modify the policy information. ➢ Click **OK**.
Deleting a tariff policy	Click in the **Operation** column corresponding to the target policy to delete it.

----End

7.1.1.2 Tariff unit

You can select a built-in electricity price unit or manually enter an international currency unit as the electricity price unit based on the local currency usage.

The procedure is as follows:

Step 1 Choose Energy > Energy Efficiency Management > Energy Configuration.

Step 2 In the navigation tree, choose Tariff Configuration > Tariff Unit.

Step 3 Select the default tariff unit from the drop-down list box on the **Tariff Unit** page, or manually enter an international currency unit as the tariff unit.

Step 4 Click **Apply** to finish the setting of tariff unit.

----End

7.1.1.3 Current Configuration

You can view the created electricity price policy and its management domain.

The procedure is as follows:

Step 1 Choose Energy > Energy Efficiency Management > Energy Configuration.

Step 2 In the navigation tree, choose Tariff Configuration > Current Configuration.

Step 3 On the **Current Configuration** page, enter the name of the management domain or the tariff policy. Click **Search.** The management domain or tariff policy that matches the searching criterion is displayed in a list

----End

7.1.2 PUE Parameter Setting

Users can set the PUE threshold and PUE baseline.

7.1.2.1 Setting the PUE Threshold

You can set the upper and lower thresholds of alarms of different severities and the upper and lower thresholds of alarm clearance conditions to monitor the power usage of devices and report alarms if the power usage is beyond the specified range.

The procedure is as follows:

Step 1 Choose Energy > Energy Efficiency Management > Energy Configuration.

Step 2 In the navigation tree, choose Parameters Setting > PUE Threshold Configuration.

Step 3 Select the alarm thresholds to be configured and configure the alarm thresholds.

Step 4 Click Apply.

Step 5 Click **OK** in the dialog box. The PUE thresholds are successfully configured.

----End

7.1.2.2 Set the PUE Reference Value.

You can set the PUE reference value for the NetEco based on the time period. You can view the change of the PUE reference value in the energy efficiency analysis. The PUE reference value is the energy efficiency expected by users in the entire management domain. The PUE reference value can be set to different values in different time segments of a day or can be set in batches.

The procedure is as follows:

Step 1 Choose Energy > Energy Efficiency Management > Energy Configuration.

Step 2 In the navigation tree on the left, choose Parameters Setting > PUE Reference Value Configuration.

- Setting a PUE reference value.
  - On the **PUE Reference Value Configuration** page, set PUE reference value.
  - Click **Apply**.
  - In the dialog box that is displayed, click **OK**.
- Setting multiple PUE reference values.
  - Click **Batch Setup**.
  - Enter the PUE reference value.
  - Click **OK**.

----End

7.1.3 Electric Energy Configuration

Users can configure and query the PUE and cabinet power.

7.1.3.1 Configuring PUE Counters

You can configure the power or cooling capacity indicator value to calculate the PUE. PUE indicators cannot be configured for subnets and root nodes.

The ECC800-Pro does not support the PUE function. You need to configure PUE indicator data on the NetEco and use the data to calculate the PUE algorithm.

The procedure is as follows:

Step 1 Choose Energy > Energy Efficiency Management > Energy Configuration.

Step 2 Choose Electric Energy Configuration > PUE Electric Energy Configuration from the navigation tree on the left.

Step 3 Click **Create**. The **Select Managed Domains** dialog boxis displayed.

Step 4 Select the management domain for which you want to configure PUE counters and click Confirm.

Step 5 On the **Bind Device** tab page, click the device name in the navigation tree on the left.

Step 6 Bind the device to Total Energy Consumption, IT Energy Consumption, or Cooling Energy Consumption, and set the indicator multiplier.

Step 7 Click **Save**.

----End

7.1.3.2 Configuring Cooling Capacity Counters

Users can configure the cooling capacity indicator value to calculate the PUE.

The procedure is as follows:

Step 1 Choose Energy > Energy Efficiency Management > Energy Configuration.

Step 2 Choose Electric Energy Configuration > Cooling Capacity Configuration from the navigation tree on the left.

Step 3 On the Cooling Capacity Configuration page, click Select Management Domain.

Step 4 Select a management domain and click **Confirm**.

Step 5 On the current page, click Cooling Capacity Consumption, Output Cooling Capacity, or Total Electric Energy of Cooling Devices. The Select Cooling Capacity Counters dialog box is displayed.

Step 6 Select the devices and counters to be configured in the **Select Devices and Select Counters columns.**

Step 7 Select **Backflow** or **Input** from the **Load Type** drop-down list.

Step 8 Click **Save**.

- If cooling capacity counters and power counters are both configured, PUE = (Total Energy Consumption + Cooling Device Power Consumption)/IT Energy Consumption, Cooling Device Power Consumption = Total Electric Energy of Cooling Devices x Cooling Capacity Coefficient, Cooling Capacity Coefficient = (Input output cooling capacity – Backflow output cooling capacity)/(Input cooling capacity consumption – Backflow cooling capacity consumption).
- Load Type for Cooling Capacity Consumption, Output Cooling Capacity are configured and Output Cooling Capacity must contain Input. Otherwise, the operation fails.
- You can select the counters to be deleted in the Cooling Capacity Consumption, Output Cooling Capacity, or Total Electric Energy of Cooling Devices area and click Delete. In the displayed confirmation dialog box, click Yes to delete the selected counters.

----End

7.1.4 (Optional) iCooling energy efficiency

The iCooling energy efficiency uses the iCooling energy-saving algorithm. When the iCooling energy-saving mode is enabled, the energy consumption of the HVAC system in the management domain is effectively reduced and the energy efficiency of the HVAC system is optimal.

7.1.4.1 Viewing iCooling Energy Efficiency Information

You can view the overall and real-time energy efficiency monitoring information of a management domain in iCooling mode.

The procedure is as follows:

Step 1 Choose Energy > Energy Efficiency Management > iCooling Energy.

Step 2 View iCooling energy efficiency information, as described in Table 7-2.

Table 7-2 iCooling energy efficiency information

Operation	Description
Viewing the energy efficiency overview of the iCooling	➢ You can click  in the upper right corner of the page to switch the management domain to view the iCooling energy efficiency overview information. ➢ If the iCooling energy saving mode is not enabled, only the PUE of the common mode is displayed in a curve chart. If the iCooling energy saving mode is enabled, only the PUE of the energy saving mode is displayed in a curve chart. ➢ The dry-bulb temperature is the real temperature of the air. It can be measured directly with a normal thermometer. The wet-bulb temperature refers to the temperature of the wet air. ■ IT load rate = IT power/Total data center power ■ The calculation formula for PUE is as follows: ◆ If the cooling capacity is not configured: PUE = Total energy consumption/IT energy consumption ◆ If the cooling capacity is configured: PUE = (Total energy consumption + Chiller power consumption)/IT energy consumption
Viewing the real-time monitoring information of the iCooling energy efficiency	➢ The cooling power usage effectiveness (cPUE) is an extension of the data center PUE concept. It is used to evaluate and analyze the energy efficiency of cooling devices in the data center. cPUE= Total energy consumption of cooling devices/Energy consumption of IT devices ➢ Coefficient of Performance (COP) refers to the cooling

	capacity that can be obtained by the unit power consumption, also known as the cooling performance coefficient. It is an important technical and economic index of the cooling system (refrigerator). A large cooling performance coefficient indicates that the cooling system (refrigerating machine) has high energy utilization efficiency. This is a coefficient related to the refrigerant type and operating conditions. COP = Cooling capacity/Cooling energy consumption

7.1.4.2 Configuring iCooling Energy Efficiency

Configure parameters for the refrigeration station in the management domain to enable the iCooling energy-saving mode.

The procedure is as follows:

Step 1 Choose Energy > Energy Efficiency Management > iCooling Energy

Step 2 Perform operations based on the scenario described in Table 7-3.

Table 7-3 Operation Scenario

Task	Explanation
Enabling the iCooling Energy Saving Mode	➢ On the **Monitoring** page, click **HVAC System Configuration**. ➢ Import configuration parameters as follows: ■ Click next to **Import** and **select Configuration Parameters**. ■ In the displayed dialog box, click . Download the template to the local PC, open it, and edit it. ■ Click to import the edited template file from the local PC. ■ Click Import. ➢ Import algorithm parameters as follows: ■ Click next to Import and select **Algorithm Parameters**. ■ In the displayed dialog box, click . Download the template to the local PC, open it, and edit it. ■ Click to import the edited template file from the local PC. ■ Click **Import.** ■ Algorithm parameters can be imported only when the iCooling energy saving mode is not enabled and iCooling energy efficiency configuration is enabled. To enable iCooling energy efficiency configuration, choose System > System Settings > System

	Configuration. click iCooling Energy Configuration. In the right pane, click ON, and click Apply. ➢ On the **Monitoring** page, click  on the right of **iCooling Energy Saving Mode**. ➢ In the displayed dialog box, click **OK**.
Disabling the iCooling Energy Saving Mode	➢ On the **Monitoring** page, click  on the right of iCooling Energy Saving Mode. ➢ In the displayed dialog box, click **OK**.
Enable iCooling energy saving mode dialog box function	➢ On the **Monitoring** page, click  . ➢ In the displayed dialog box, click **Yes**. ➢ In the displayed dialog box, click **OK**.
Disabling the iCooling energy saving mode dialog box function	➢ On the Monitoring page, click  . ➢ In the displayed dialog box, click **Yes**. ➢ In the displayed dialog box, click **OK**.
Setting the scheduled task for executing the iCooling energy saving mode	➢ In the upper right corner of the **Monitoring** tab page, click  . ➢ In the displayed dialog box, set **Cycle, Start Time, Cycle interval, End time, and Execution order.** ➢ Click **Comfirm.** ➢ In the displayed dialog box, click **OK**.
Enabling the water temperature optimization function	➢ On the **Monitoring** page, click **HVAC System Configuration.** ➢ On the **HVAC Configuration** page, click **Terminal Air-conditioning configuration.** ➢ In the dialog box that is displayed, set **Optimal Water Temperature Range** and click  on the right of **Optimal Water Temperature Enable Switch.** ➢ In the displayed dialog box, click **OK**.
Disabling the water temperature optimization function	➢ On the **Monitoring** page, click **HVAC System Configuration.** ➢ On the **HVAC Configuration** page, click **Terminal Air-conditioning configuration.** ➢ In the displayed dialog box, click  on the right of **Optimal Water Temperature Enable Switch.** ➢ In the displayed dialog box, click **OK**.
Configuring air conditioners	➢ On the **Monitoring** page, click **HVAC System Configuration.** ➢ On the **HVAC Configuration page**, click **Terminal Air-**

	conditioning configuration. ➢ In the dialog box that is displayed, select the air conditioners ➢ Click **OK**.

----End

7.1.5 Power Supply and Dstribution

Design all electrical link diagrams and single-line diagrams based on logical topologies to implement visualized management and operations on devices in the management domain, helping users optimize management.

7.1.5.1 Logical Link Management

Logical link management implements visualized management and operations through logical topology design, enabling measurement, evaluation, and optimization of logical links in management domains.

7.1.5.1.1 Logical Link Configuration and Design

Configure and design a full-power link for the management domain to facilitate the visual management of all components in the management domain.

The procedure is as follows:

Step 1 Choose Energy > Power Supply and Distribution > Logical Link.

Step 2 Click  on the right of the logical link diagram name in the navigation tree, and choose **Modify** or **Delete** to modify or delete the link.

Step 3 Click  in the upper-right corner of the page.

Step 4 Click  on the toolbar.

- Based on the requirements for designing the logical link, drag the controls in the Logical Component or Switch and Transducer area in the lower left corner of the view to the design area.
- Unfold the conducting wire and connector, and click the conducting wire. Select two nodes in sequence in the design area to connect the nodes. Then, connect the controls
- Method for adjusting the position of a conducting wire: Select the wire and click  on the wire.
- The method of vertically placing the busbar is as follows:
  - Place the pointer over the bus end, and the pointer turns into a cross.
  - Drag the end to the other end until the bus turns into a point.
  - Keep dragging the end downwards or upwards.
- Modify the line width, dotted line, and color of the conducting wire. You can set only the line width and color for the bus.

- The width of the conducting wire ranges from 1 to 5 and that of the bus ranges from 1 to 10.
- After the logical link diagram is drawn, you can bind the controls to the corresponding control instances in the configuration pane on the right of the design area.
- Select the control to be bound with a control instance, and click on the right of Control Instance. In the displayed Select Control Instance dialog box, select the control instance to be bound.

Table 7-4 Properties of a switch or transducer

Parameter	Explanation
Control Name	Indicates the name of the device.
Control Instance	Component Instance: Select devices in the management domain for the logical component. Electric energy configuration: Configure electric energy input and output groups for devices.
Display Name	Select Display Name to display the component name below the component. After you select this option, you can set Border Color, Font Color, Text Background, Transparency, Horizontal Move, and Vertical Move for Component Name.
Rotation Angle	The component can be rotated by '0', '90', '180', or '270' degrees.

Step 5 Click on the toolbar to save the operation.

Step 6 Click on the toolbar to lock the view.

----End

7.1.5.1.2 Logical Link Data Analysis

View All-electric chain, energy efficiency, and UPS energy saving data in the management domain to help users make decision analysis.

The procedure is as follows:

Step 1 Choose Energy > Power Supply and Distribution > Logical Link.

Step 2 Click the right arrow on the left of the page and select a constructed logical link diagram to view the detailed information.

- You can view the chain comparison data change trend of each component in the electrical link diagram in the upper part of the page. The arrow indicates that the chain comparison data increases, the arrow indicates that the chain comparison data decreases, and the arrow indicates that the chain comparison data remains unchanged.

- The pPUE of the UPS group, HVDC group, transformer group, chiller group, equipment room group, and smart module group can be displayed in the full-electrical link diagram.

Step 3 View the energy efficiency analysis of the management domain corresponding to the logical link.

- View the power consumption KPIs of key nodes in the logical link.
- View the details about site energy efficiency analysis: top 5 PUE changes, top 5 power consumption changes, PUE trend chart, and energy consumption distribution and trend chart.

Step 4 View the UPS energy saving details of the management domain corresponding to the logical link diagram.

- View the table listing the running details of the UPS group: UPS name, group, number of basic modules, number of redundant modules, rated module capacity, load capacity, and real-time load rate.
- View UPS optimization suggestions.

----End

7.1.5.2 Creating a Single-Line Diagram System

You can create a single-line electrical diagram system for a park, building, floor, room, ContainerDC, container, modular, or NetEco to achieve visualized operation and management and even function- and domain-specific management of the single-line electrical diagram.

The procedure is as follows:

Step 1 Choose Energy > Power Supply and Distribution > Single Line.

Step 2 Choose a room, for which you want to create a single-line electrical diagram system, under Root

Step 3 Click  on the toolbar. The design area becomes editable.

Step 4 Select a method for creating a single-line electrical diagram system as required.

Table 7-5 Creating a Single Line Diagram System

Method	Application Scenario	Operation Method
By importing a file	You can import an existing single-line diagram file as required.	➢ Click  on the toolbar. ➢ Select the system file (in XML format) of the electrical single line diagram to be imported and click **OK**. ➢ Modify the attributes of each component. ➢ Click  on the toolbar.

By using a template	You can create a single-line electrical diagram view using a preset template.	➢ Click  on the toolbar. ➢ In the **Select Template** dialog box, select a template and click **OK**. ➢ On the **Design View** page, adjust the electrical single-line view. ➢ Click  on the toolbar. ➢ Click  on the toolbar to lock the editing page.
By manual creation	You can design a new single-line electrical diagram view according to a single-line electrical diagram.	➢ In the component pane on the left, drag the required components from **Switch** and **Transducer**, **High-Voltage Switch Cabinet**, **Detector**, **Wire and Connector**, **Base Shape, Tool or Custom Control** to the view design area. ➢ Select wires and connectors in the **Wire and Connector** area to connect components. ➢ On the **Design View** page, select a component as required and perform the following operations: ■ Set its properties in Properties. ◆ **Switch and Transducer and High Voltage Switch Cabinet**: Select the corresponding component instance and alarm. ◆ **Wire and Connector**: Modify the line width, dashed line, and color of the wire. Only the width and color of the bus can be set. ■ Binding KPIs and alarms in batches: On the **Design View** page, select the corresponding component and click **KPI** Customization under  to bind the KPIs. ■ Bind indicators in batches: Click  on the toolbar, select controls, indicators, and alarms, and bind them in batches. ➢ On the **Design View** page, click a component, select **Display Name** in **Shape Options**, and set its attributes. ➢ Optional: Expand Tool, drag components

		to the design area, and mark the single-line electrical diagram. ➢ Optional: You can set and bind counter thresholds so that you can view the changes of the bound counters on the single-line chart page. ➢ Bind **Detector** in the component bar to the corresponding components. ➢ Click  on the toolbar. ➢ Click  on the toolbar to lock the editing page.

----End

8 O&M Management

8.1 Shift Scheduling Management

By managing personnel and on-duty schedules, users can manage personnel in a unified manner, detect problems in a timely manner, and adjust the on-duty schedules to ensure normal work.

8.1.1 Personnel Scheduling

Users can manage all O&M personnel in a unified manner.

Navigation path: Choose **Maintenance > Shift Scheduling Management > Personnel Shift**.

The procedure is as follows:

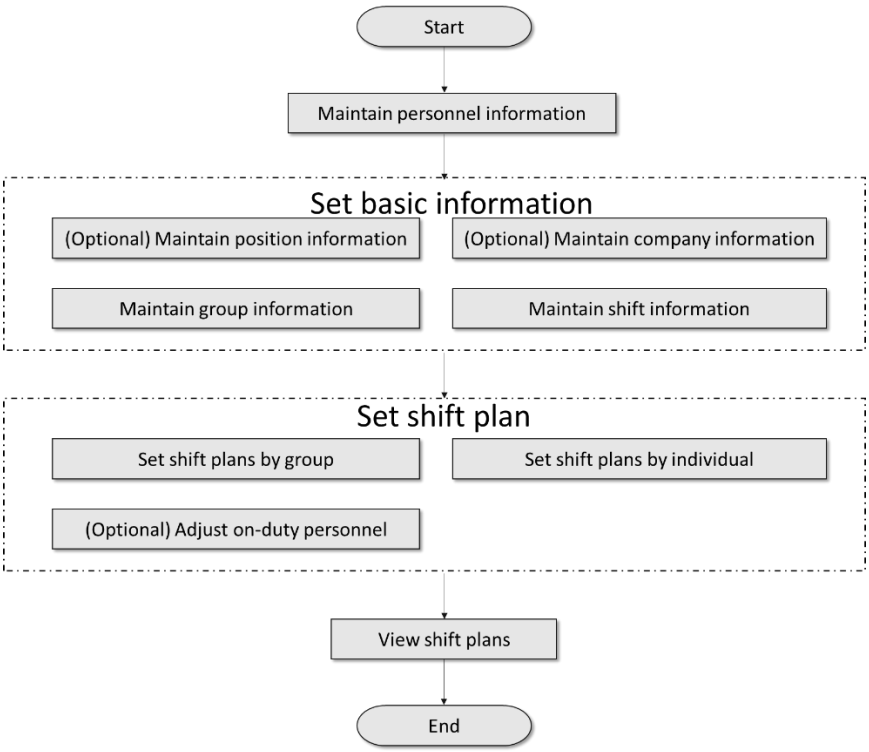


Figure 8-1 Service process of agent scheduling

8.1.2 Shift Handover Record

Users can manage shift handover records to ensure that the handover tasks are performed in an orderly manner.

Navigation path: Choose **Maintenance > Shift Scheduling Management > Shift Handover Records.**

For details, see Table 8-1.

Table 8-1 Task Content

O&M Scenario	Major Tasks
Shift handover record management	➢ Create shift handover records: You can create shift handover records for tracing. ➢ Handle a shift handover record: You can coordinate and handle the handover records to be processed, including transferring the handover records, specifying the handling mode, and next handler. ➢ View records: View the information about the handled and created shift handover records. ➢ Send a reminder for shift handover record processing: Remind the handler of shift handover records by email or short message and notify the creator of the handling progress.
Notification task management	➢ Create a notification task: Pushes handover records that meet the conditions to related personnel periodically or manually. ➢ Manually send notifications: When creating a notification task, you need to manually push notifications.
Shift handover record statistics and analysis	➢ Customize a statistical template: You can create a custom template and view the trend analysis of shift handover records. ➢ Collect statistics on all shift handover records: collects statistics on the trend analysis of shift handover records in the query period.
View management	➢ Query all views: Users can view all shift handover records and learn about the handling status of shift handover records. You can also create, import, export, transfer, and remind shift handover records. ➢ Customize a view: You can customize a view based on the fields you concern.

8.1.3 Customized Report

By creating and delivering customized reports, you can periodically track the basic information and existing problems of the work to ensure the normal operation of the work.

Navigation path: Choose **Maintenance > Shift Scheduling Management > Customized Report.**

For details, see Table 8-2.

Table 8-2 Task Content

O&M Scenario	Major Tasks
My customized reports	➢ Create a customized report: Create a new custom report and track the process. ➢ Handle a customized report: Process custom reports that have been submitted to the current user. ➢ View processed customized reports: You can view and edit the custom reports that have been processed by the current user. ➢ View created customized reports: View and edit customized reports created by the current user.
Notification Task Management	➢ Create a notification task: You can create a notification task to periodically or manually push the filtered user-defined reports to specified personnel to view the reports. ➢ Manually send notification: Manually push the filtered customized reports to specified personnel to remind them to view and process the customized reports in a timely manner.
Statistics and analysis	➢ Customize a statistical template: Select filter criteria and save the template as a custom statistical template for next query. ➢ Collect statistics on customized reports: Set the statistical period and select the query counter to collect the report trend analysis information in the query period.
View management	➢ Query all views: View the status of all user-defined reports and learn about the closure status of user-defined reports so that the owner can handle the reports in a timely manner. ➢ Customize a view: View the status of custom reports of all users in the custom view to learn about the closure status of custom reports so that the owner can handle the reports in a timely manner.

8.2 Availability management

You can perform routine maintenance on devices through availability management to ensure that the NetEco runs properly and efficiently.

8.2.1 E-inspection

Electronic inspection implements tool-based O&M, electronic O&M data, and paperless inspection records. In this way, equipment room inspection data can be collected and analyzed, and the operating status of the equipment room can be clearly understood. The modules involved include template configuration. Electronic inspection can also be implemented on the mobile app to improve O&M efficiency.

Navigation path: **Maintiance > Availability Management > E-inspection.**

For details, see Figure 8-2.

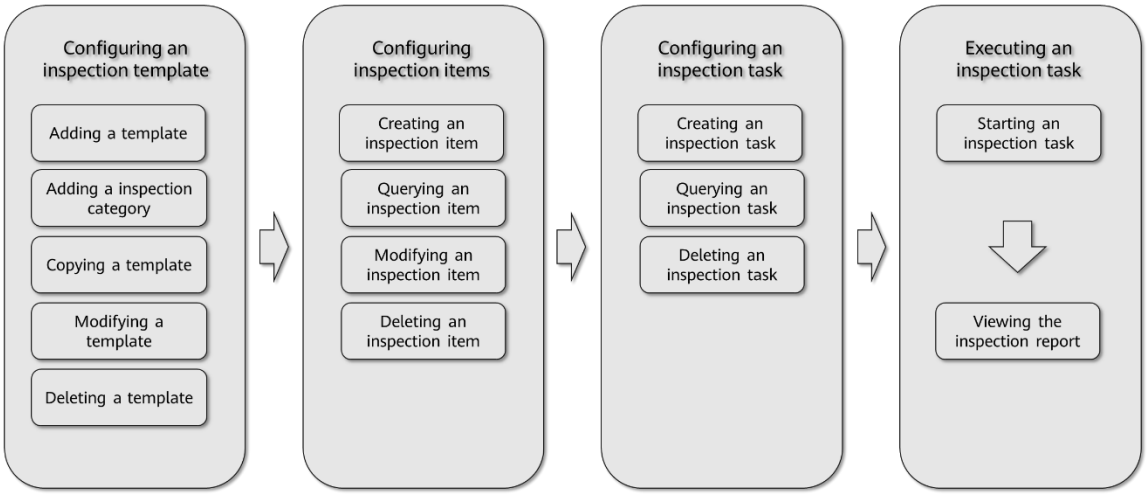


Figure 8-2 Inspection Operation Panorama

8.2.1.1 Task delivery

After configuring templates and role permissions, you can deliver inspection tasks. You can select the template, task period, time, and equipment room to be inspected based on inspection requirements to deliver inspection tasks. After a task is delivered, the owner can view the corresponding inspection task in the My To-Dos area when the task execution time arrives.

The procedure is as follows:

Step 1 Choose E-inspection > To-Dos and click Create.

Step 2 On the **Create** Task page, set task parameters and click **Save**.

----End

8.2.1.2 Perform inspection.

The inspection can be performed on the mobile APP or WebUI.

On the App: Choose **NetEcoAPP > E-inspection**, find the delivered inspection task, and enter the inspection result.

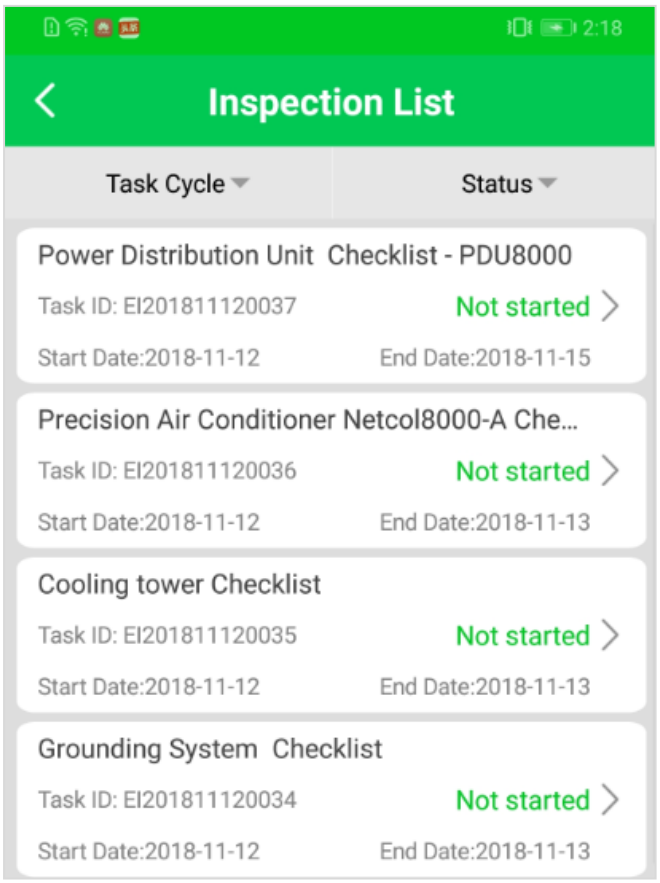


Figure 8-3 App inspection list

On the WebUI, choose **E-inspection > To-Dos**, select a task, click Execute, and enter the inspection result, as shown in Figure 6-4.

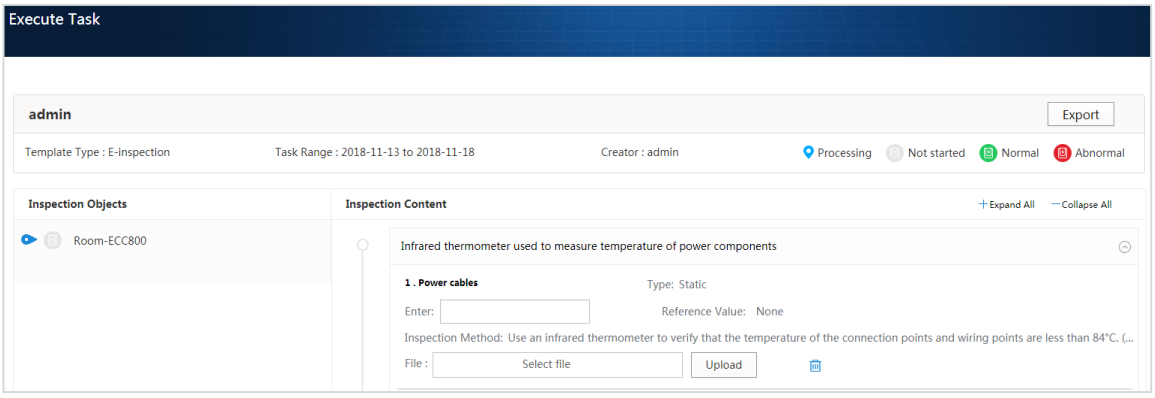


Figure 8-4 Executing an Inspection Task on the Web

8.2.2 Routine Drill

Routine drills are used for data center maintenance personnel to get familiar with emergency measures. If emergencies occur, they can implement emergency measures in an orderly manner to minimize losses and facilitate stable O M of the data center.

Navigation path: Choose **Maintenance > Availability Management > Routine Drill.**

For details, see Table 8-3.

Table 8-3 Task Content

O&M Scenario	Major Tasks
Routine drill	➢ Create a drill: When creating a drill task, you can select any of the following options: Custom template Select template Upload file. ➢ Handle a drill: Handle a drill task that has been sent to you. ➢ View records: View processed drill tasks.
Notification Task Management	➢ Create a notification task: Create a notification task and push the filtered drill tasks to specified personnel periodically or manually. ➢ Manually send notification: Manually send filtered drill orders to specified personnel.
Statistics and analysis	➢ Customize a statistical template: Select filter criteria and query the template. ➢ Collect statistics on all drill tasks: Set the statistical period, select the query indicator, and collect statistics on all drill tasks.
View management	➢ Query all views: You can view the drill task status of all users and learn about the drill task processing status. You can also create, delete, export, and remind drill tasks at a scheduled time. ➢ Customize a view: displays the drill task status of all users in the custom view.

8.2.3 Conserve Inspection

By creating and delivering maintenance tasks, you can periodically remind the owner to track maintenance tasks and maintain devices in a timely manner to ensure the normal running of devices.

Navigation path: Choose **Maintenance > Availability Management > Conserve.**

For details, see Table 8-4.

Table 8-4 Task Content

O&M Scenario	Major Tasks
Conserve	➢ Create a maintenance task: When creating a maintenance task, you can select any of the following items: Custom template Select template Upload file. ➢ Handle a maintenance task: Process maintenance tasks that have been transferred to the current user. ➢ View processed tasks: In the list of processed maintenance tasks, you can view and edit the tasks. ➢ View created tasks: You can view and edit maintenance tasks in

	the list of maintenance tasks created by the current user.
Notification Task Management	➢ Create a notification task: You can create a notification task to periodically or manually push the filtered maintenance tasks to specified personnel to view the tasks, reminding the owner to track and handle the maintenance tasks in a timely manner. ➢ Manually send notification: Manually send the filtered maintenance tasks to specified personnel to remind the owner to track and handle the maintenance tasks in a timely manner.
Statistics and analysis	➢ Customize a statistical template: Select filter criteria and query the template. ➢ Collect statistics on all maintenance tasks: Set the statistical period and select the query indicator to collect statistics on all maintenance tasks. ➢ View the maintenance calendar: View the distribution status of maintenance tasks on the calendar and track the tasks in a timely manner.
View management	➢ Query all views: You can view the maintenance task status of all users and learn about the processing of drill, and maintenance tasks. You can also create, delete, export, transfer, and remind maintenance tasks. ➢ Customize a view: View the maintenance task status of all users in the custom view.

8.2.4 Repair management

Maintenance management is used to track the overall maintenance process of equipment to ensure that maintenance tasks are completed in time.

Navigation path: Choose **Maintenance > Availability Management > Repair Management.**

For details, see Table 8-5.

Table 8-5 Task Content

O&M Scenario	Major Tasks
Repair Management	➢ Create a repair order: Create a new repair process order. ➢ Handle a repair order: Handle the repair order that has been moved to the current user. ➢ View records: View processed repair process orders. ➢ Send a reminder: Remind the handler of the repair order by email or SMS and notify the creator of the handling progress.
Notification Task Management	➢ Create a notification task: You can create a notification task to periodically or manually push the filtered repair order status to specified personnel.

	➢ Manually send notifications: Manually send the filtered repair order process to specified personnel.
Statistics and analysis	➢ Customize a statistical template: Select filter criteria and query the template. ➢ Collect statistics on all repair orders: Set the statistical period and select the query index to collect statistics on all repair tasks.
View management	➢ Query All Views: You can view the repair order status of all users to learn about the repair order processing status. You can also create, import, export, transfer, and urge repair orders. ➢ Customize a view: View the repair order status of all users in the custom view.

8.3 Supplier Management

Maintain the basic data of suppliers and assign tasks to comprehensively evaluate the implementation.

8.3.1 Supplier Maintenance

Maintenance management is used to track the overall maintenance process of equipment to ensure that maintenance tasks are completed in time.

Navigation path: Choose **Maintenance > Supplier Management > Supplier Evaluation.**

For details, see Table 8-6.

Table 8-6 Task Content

Service	Explanation	Operation Method
Supplier information	Allows you to configure basic supplier information.	➢ In the navigation tree on the left, choose **Supplier Information**. ➢ Click **Creat**, set related parameters, and click **Save**. ➢ Click **Edit** in the row where the task is located to modify related parameters.
Supplier categories	Allows you to configure basic supplier category information.	➢ In the navigation tree on the left, choose **Supplier Categories**. ➢ Click **Creat,** set related parameters, and click Save. ➢ Click **Edit** in the row where the task is located to modify related parameters.
Evaluation Items	Allows you to configure the	➢ In the navigation pane on the left, choose **Evaluate Items**.

	basic information about the evaluation items corresponding to supplier categories.	➢ Click **Creat**, set related parameters, and click Save. ➢ Click **Edit** in the row where the task is located to modify related parameters.

8.3.2 Supplier Evaluation

Navigation path: Choose **Maintenance > Supplier Management > Supplier Evaluation.**

For details, see Table 8-7.

Table 8-7 Task Content

Service	Explanation	Operation Method
Supplier Evaluation List	Displays the created supplier evaluation tasks and approve the tasks.	➢ In the navigation tree on the left, choose **Supplier Evaluation List**. You can search for the created evaluation tasks based on the filter criteria. ➢ Click for a task whose approval status is **Pending** or **Rejected**. ➢ Set the parameters and click **Submit**.
Supplier Evaluation Tasks	Allows you to generate supplier evaluation tasks.	➢ In the navigation tree on the left, choose **Supplier Evaluation Task** and click **New Task**. ➢ Set parameters for creating a task and click **Submit** to generate task data. ➢ Click in the column corresponding to the task to view the approval status details of the task.

8.4 Knowledge Management

The knowledge base allows you to collect, classify, save, and share cases, facilitating knowledge sharing and experience exchange.

Navigation path: Choose **Maintenance > Knowledge Management > Knowledge.**

For details, see Table 8-8.

Table 8-8 Task Content

Task	Explanation
Knowledge Base	➢ View a case: Search for the required case.

Overview	➢ Create a case: Create a case. ➢ View category details: View the category details set in the category management module.
My Knowledge Base Management	➢ Approve a case: Approve a case that have been submitted. ➢ Modify a created case: You can edit a created case. ➢ Modify a Handled Case: Modify a handled case.
My Settings	➢ Create a category: You can create a category to classify cases for easy case search. A maximum of five levels can be created for each category. When creating a level-2 category, you need to set the security level and access permission. ➢ Modify a category: You can edit a category.
My Views	➢ View favorruted cases: View all cases in favorites. ➢ View shared cases: View all shared cases. ➢ View commented cases: View all commented cases.

9 Report Management

The NetEco provides a comprehensive performance report management solution. With powerful report analysis and display methods and a customized report customization system, the NetEco can flexibly customize indicator data and service performance reports, and the network performance changes are under control. The NetEco presets reports such as power consumption reports, resource reports, and alarm reports.

9.1 Report Task

The NetEco provides the functions of creating and viewing report tasks to facilitate report management.

9.1.1 Creating a Report Task

You can create a report task and set the execution frequency of the report task to automatically generate a report and send the report by email.

The procedure is as follows:

Step 1 Choose Report > Report Management > Report Task.

Step 2 On the **Report Task** page, click **Create**.

- The default predefined template and user-defined template are available for the selected report parameters. Determine whether to create a template in advance based on the site requirements.

Step 3 Select a report format.

Step 4 (Optional) Select Forward by Email. If a recipient has been defined, click Recipient. In the displayed Select User Group dialog box, select a recipient. Otherwise, click Edit User Group to create a recipient.

- PDF and Excel files, supporting charts.
- Personal data, such as phone numbers and email addresses, is anonymized on the NetEco and encrypted during batch transmission in the NetEco to ensure personal data security.

Step 5 Click **OK**.

----End

9.1.2 Viewing Report Tasks

You can delete, export, or send reports by email on the task report page.

The procedure is as follows:

Step 1 Choose Report > Report Management > Report Task.

Step 2 Click in the row where the report task to be viewed is located.

- Deleting a report: Select the report to be deleted and click **OK**.
- Exporting a report: Select the report to be exported and click **Export.** Select **CSV, Excel**, or **PDF** from the drop-down list.
- To forward a report by email, select the report to be sent and click Forward by **Email.** In the displayed dialog box, set the recipient and file format, and click **OK**.

----End

9.2 Report system configuration

You can configure the threshold of the report storage area through the report system configuration. This prevents the report storage area from being insufficient and provides the alarm function of disk space insufficient. Configure the customer logo so that the customer logo can be displayed in reports.

The procedure is as follows:

Step 1 Choose Report > Report Management > Report System Config.

- In the navigation tree on the left, choose **Reports Disk Usage**. In the pane on the right, set the maximum value of the storage area and click **Save**. You can view the usage of the storage area on the lower part of the window.
- In the navigation tree on the left, choose **Customer Information**. On the right, click , select the customer logo image, and click **Upload**.

----End

10 System Management

10.1 Service Settings

10.1.1 Signal Management

Users can change the name of a counter to identify the counter more easily.

The procedure is as follows:

Step 1 Choose System > Service Settings > Signal Management.

Step 2 In the navigation tree on the left, select the device to be modified.

The system supports search by device type and device name.

- Search by device type: Select a device type from the drop-down list box.
- Search by device name: Enter a device name in the search box.

Step 3 Support customized name, including modifying Sampling, Configuration, Statistic, and Alarm. Figure 10-1 and Figure 10-2 show the details.

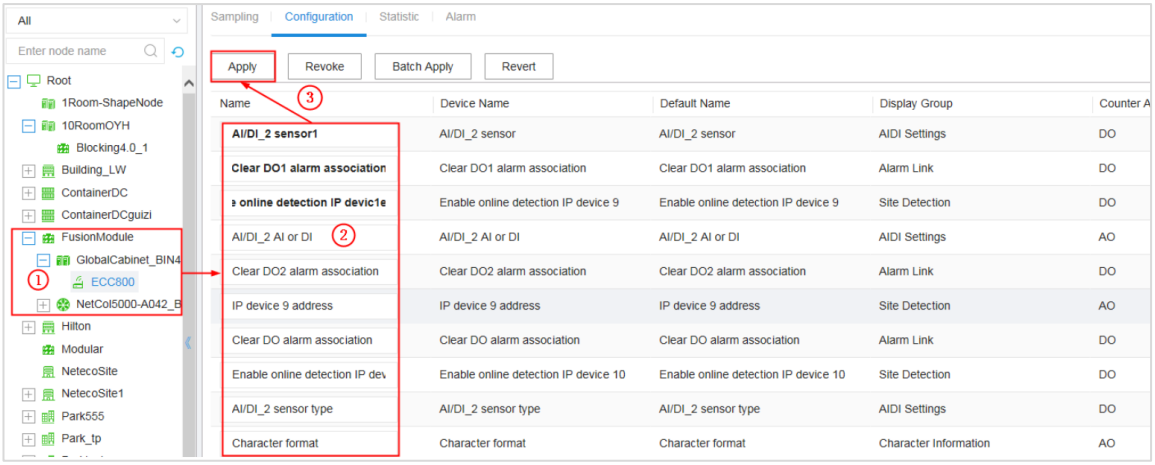


Figure 10-1 Changing the customized name

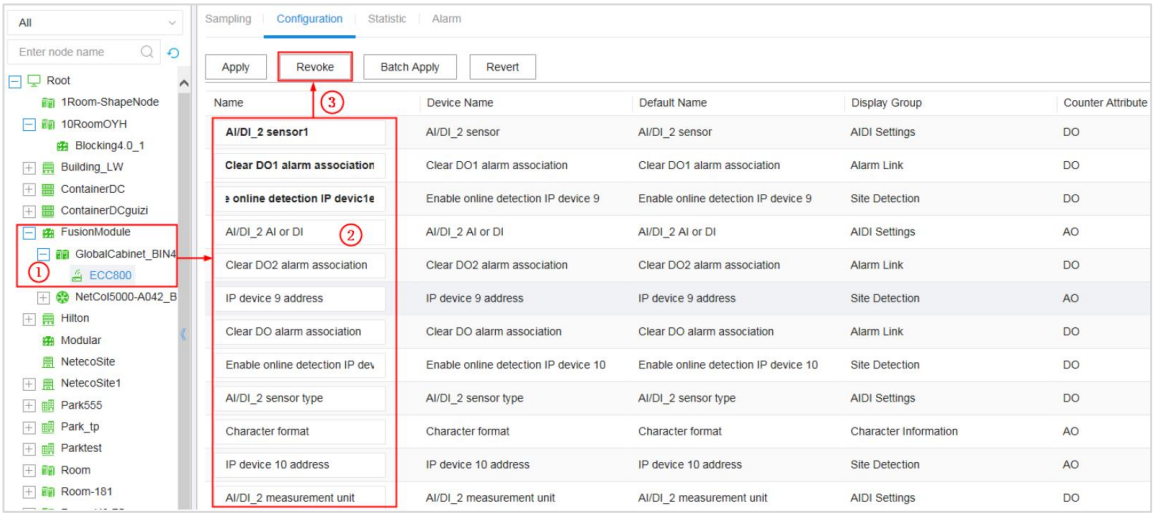


Figure 10-2 Changing the customized name in batches

Step 4 You can set **Display** or **Not** to change whether the corresponding counter is displayed on the related page.

Step 5 After the modification is successful, the new names of other modules are displayed.

----End

10.1.2 Autocontrol Strategy Management

The autocontrol strategyl management involves the management of the policies, event list, action list, and logs.

The procedure is as follows:

Step 1 Choose System > Service Settings > Autocontrol Strategy.

Step 2 In the navigation pane on the left, choose Policy. For details, see Table 10-1.

Table 10-1 Strategy management

Operation Name	Operation Method
Create the strategy	➢ Click **Create**. The page for **Strategy Information** is displayed. ➢ Enter the name for the strategy as prompted, select period, and enter the strategy description. ➢ Click **Next**. The page for **selecting events** is displayed. ➢ Click **Create Event**. The dialog box for Select Event is displayed. ➢ (Optional)Enter the name of the event, select the management objects, and click **Confirm**. ➢ Select events and click **Confirm**.

	➢ Click **Next**. The **Customize Strategy** age is displayed. ■ When only one event is selected, the strategy is **Single event** by default. ■ When two or more events are selected, you can select **AND**, **OR**, or **CUSTOM** from the **Select Strategy** drop-down list. ➢ Click **Next**. The page for selecting actions is displayed. ➢ Click **Create Action**. The dialog box for **Select Action** is displayed. ➢ (Optional)Enter the name of the action, select the management objects, and click **Confirm**. ➢ Select actions and click **Confirm**. ➢ Click **Next**. The **Result Confirm** page is displayed.
Modify the strategy	➢ Click of an autocontrol strategy. The page for modifying the autocontrol strategy is displayed. The page varies with the strategy. The following operate uses the **AND** strategy as an example. ➢ You can modify another period or strategy description, or add or delete events and actions. ➢ Click **Confirm**. The autocontrol strategy is modified.
Delete the strategy	➢ Select the policy to be deleted and click **Delete**. A confirmation dialog box is displayed. ➢ Click **Yes** to delete the policy.
Disable the strategy	➢ Click in the row where the target policy is located to disable the policy.
Enable the strategy	➢ Click in the row where the target policy is located to enable the policy.

----End

10.1.3 Adpter Management

Perform operations on the mediation through the NetEco.

The procedure is as follows:

Step 1 Choose System > Service Settings > Adpter Management.

Step 2 On the Adpter Management page, click Upload.

Step 3 In the displayed **Upload adpter package** dialog box, click **Select File**.

Step 4 Select the adpter file to be uploaded and click **Upload**.

- The NE mediation verification becomes stricter with the NetEco upgrade. If the NE mediations that can be connected to earlier versions are reconnected to the NetEco in later versions, the verification may fail. For the NE mediation of this

type (the verification of the earlier version is successful, but the verification of the later version fails), contact the system administrator to disable the verification function. Exercise caution when performing this operation.

Step 5 The information about the uploaded mediation is displayed in the list. In the mediation list, select the uploaded mediation and click **Install**.

Step 6 In the displayed **Information** dialog box, click **YES**. Information about the installed mediation is displayed in the list.

----End

10.1.4 Transmission Channel Management

Access the NetEco through the ECC, you need to add the password of ECC challenge handshake authentication for the NetEco to ensure the validity of identity authentication between devices and the NetEco.

The procedure is as follows:

Step 1 Choose System > Service Settings > Transmission Channel Management.

Step 2 The **Transmission Channel Management** page is displayed. Click **Refresh**. All peer IP addresses of ECCs connected to the NetEco are listed.

Step 3 Set **Connection Mode** to **Compatible** by default. Determine whether to set Connection Mode based on the following scenarios:

- If the ECC does not support the second challenge authentication, no further action is required.
- If the ECC supports the second challenge authentication,
  - If the re-authentication password of the ECC800-Pro is the default password, do not set **Connection Mode**.
  - If the re-authentication password of the ECC800-Pro is not the default password, select the ECC800-Pro you need to modify and click **Modify**. In the displayed dialog box, set **Connection Mode** to **Security Protocol**, specify **Password** and **Confirm Password**, and click **Confirm**.
- If required, change **Connection Mode** from **Security Protocol** to **Compatible** or from **Compatible** to **Security Protocol**.
- Select the ECC800-Pro you need to modify and click **Modify**. In the displayed dialog box, change the value of **Connection Mode**, specify **Password and Confirm Password**, and click **Confirm**.

Step 4 Restart the NetEco service.

----End

10.2 System Management

10.2.1 User Management

10.2.1.1 User Authorization

10.2.1.1.1 Authorization Process

After the system is installed and commissioned, security administrators need to grant different permissions to users of different roles based on the service plan. Figure 8-3 shows the user authorization process.

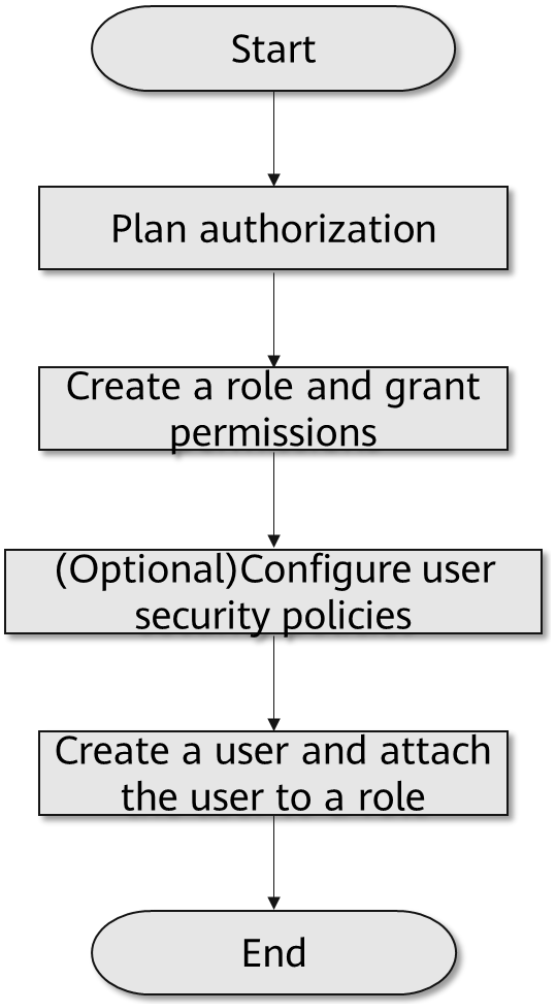


Figure 10-3 User authorization process

Authorization planning is to classify users by responsibilities. Before performing user authorization, plan authorization first to reduce the workload of authorization and permission maintenance. Proper authorization planning improves system security and ease of use. Authorization planning principles:

- Assign users with the same responsibilities to the same role, and assign users with different responsibilities to different roles.

- If the application operations required by multiple roles are the same, you can plan a common application operation set for these roles. Otherwise, plan an application operation set or grant application operation rights to each role.
- If the device operations required by multiple roles are the same, you can plan the same device operation set for these roles. Otherwise, plan a device operation set or grant device operation rights to each role separately.

10.2.1.1.2 Creating a Role and Granting Permissions

If the default settings provided by the system cannot meet user authorization requirements in the authorization plan, security administrators can create roles separately or in batches based on the authorization plan and assign operation rights to roles.

The procedure is as follows:

Creating a single role

Step 1 Choose System > System Management > User Management.

Step 2 In the navigation pane on the left, choose **Roles**.

Step 3 On the **Roles** page, click **Create.**

Step 4 On the **Create Role** page, enter basic information about the role.

Step 5 Select the users to be included in the role. After the role is authorized, the selected user has the permissions of the role.

Step 6 Click **Next** and select managed objects for the role based on the managed objects planned for the role in authorization planning.

Step 7 Click **Next** and select operation rights as required. When granting device-level operation rights, select the object to be authorized. The device operations that can be bound to the managed object are automatically displayed in the Operation column. Then, select the device operations to be authorized.

Step 8 Click **OK**.

Creating Roles in Batches

Step 1 Choose System > System Management > User Management.

Step 2 In the navigation pane on the left, choose **Roles**.

Step 3 On the **Roles** page, click ••• and choose **Batch Create Roles.**

Step 4 On the **Batch Create Roles** page, click the template name to download the template. The system provides two types of templates: Role Template.xls and Role Template.xlsx. Select a template as required.

Step 5 Enter role information based on the template.

Step 6 Click . In the displayed window, select the edited template.

Step 7 Click Import.

Step 8 Click **OK**.

----End

10.2.1.1.3 Creating a User and Adding the User to a Role

After the administrator creates a user and adds the user to a role, the user can have the rights of the role.

The procedure is as follows:

Creating a Single User

Step 1 Choose System > System Management > User Management.

Step 2 In the navigation pane on the left, choose **Users**.

Step 3 On the User page, click **Create**.

- You can create a user based on the existing user by clicking Copy in the Operation column of the target user. The information about the selected user is copied to the new user. Set Username and Password and modify other information as required.

Step 4 On the page that is displayed, set basic user information.

Step 5 There are three types of users: **Local, Third-party** and **Remote**. The parameters of different types of users are different.

Step 6 Select the role to which the user belongs and click **Next**. Click the role name to view the permissions of the role. You can create a role for the user. For details, see. After the role is created, click Refresh in the role list and select the new role.

Step 7 Select the login time control policy and login IP address control policy. You can also click **Create** to create a login time control policy and login IP address control policy as required.

Step 8 Click **Finish**.

Creating Users in Batches

Step 1 Choose System > System Management > User Management.

Step 2 In the navigation pane on the left, choose **Users**.

Step 3 On the Users page, click ••• and choose **Import Users in Batches**.

Step 4 In the displayed Import Users dialog box, click the template name to download the template and enter user information based on the template.

- The system provides two templates: User Template.xls and User Template.xlsx. You can edit the template in CSV format. Select a template as required.

Step 5 Select **Create User** as the user import mode.

Step 6 Click . In the displayed window, select the edited template.

Step 7 Click **Import**.

Step 8 Click **OK**.

----End

10.3 Remote notification

Remote notification is a function that can send messages remotely. After remote notification settings are configured, the system can communicate with the SMS gateway, Simple Message Notification (SMN), SMS modem, or email server. In this way, users can obtain important service notifications such as alarms and events by SMS or email in a timely manner.

10.3.1 Process of Using the Remote Notification Service

Before using remote notification, O&M personnel need to make preparations, such as commissioning the communication function of remote notification and setting notification parameters so that notifications can be automatically or manually sent to related personnel based on notification rules and templates.

Table 10-2 Process of using the remote notification service

Stage	Task
Commissioning the Remote Notification Function	➢ Commission the SMS notification function. ➢ Verify the email notification function.
Setting Notification Parameters	➢ Create a notification user. ➢ Create a notification user group. ➢ Set traffic control. ➢ Set a notification template. ➢ Set notification rules.
Send Notification	➢ Automatically send notifications. ➢ Manually send notifications.

10.3.2 Commissioning the Remote Notification Function

10.3.2.1 (Optional) Commissioning the SMS Notification Function

Remote Notification provides the SMS notification function. When O&M personnel need to send SMS messages, set SMS notification parameters and verify the settings to ensure that SMS messages can be sent properly.

The procedure is as follows:

Step 1 Setting **SMS Gateway** Interconnection Parameters

- Choose **System > System Settings > Notifications**.
- Set the SMS gateway.
  - In the navigation tree on the left, choose **SMS Settings > SMS Server Settings**.
  - Set the information such as the port number and number for sending SMs. For the parameter description, see Table 10-3.

Table 10-3 Parameters for configuring the SMS gateway

Parameter	Explanation	Example
Domain name/IP address of the SMS server	Domain name or IP address of the SMS server.	10.1.1.1
SMS Protocol	Encoding protocol used for sending SMs.	SMGP
SMS server Port	Port number of the SMS server.	8900
SMS server user name	User created on the SMS server. This user is used for remote notification to connect to the SMS server.	Test123
Password	Password corresponding to the user name of the SMS server.	/
Sender mobile number	Specifies the sender number displayed when a remote notification is sent in short messages. The sender number is specified by the SMS gateway or SMS provider.	13XXXXXXXXX
Recipient mobile number	If you want to test whether the SMS gateway is set successfully, enter this number to receive verification SMS messages.	13XXXXXXXXX
Failed retry times	The default value is 3. The value is an integer ranging from 0 to 10.	3
Enabled	By default, this parameter is set to Yes. If this parameter is set to No, the setting is unavailable and SMS messages cannot be sent.	Yes.

- Click **Test** to check whether the system is connected to the SMS gateway.
  - If the test is successful, a message is displayed, indicating that the test is successful.
  - If the test fails, the message "Connection failed." is displayed. Check whether the parameter settings are correct.

- Click **Apply**.

Step 2 Set SMN interconnection parameters.

- Choose **System > System Settings > Notifications.**
- In the navigation pane on the left, choose **SMN Settings**. On the **SMN Settings page**, set SMN parameters.
  - Peer IP address: IP address provided by SMN for interconnection.
  - Peer port: indicates the port provided by SMN for interconnection. Example: 65534
  - User name: management tenant account corresponding to remote notification.
  - Password: password of the management tenant account for remote notification.
  - Recipient mobile number: If you want to test whether SMN settings are successful, enter this number to receive SMS verification messages.
  - Enabled: The default value is Yes. If you select No, the setting is unavailable and SMS messages cannot be sent.
- Click **Test** to check whether the system can communicate with SMN.
  - If the test is successful, a message is displayed, indicating that the test is successful.
  - If the test fails, a message is displayed indicating that the connection fails. Check whether the parameters are correctly set.
- Click **Apply.**

Step 3 Setting Interconnection Parameters for the SMS Modem

Choose **System > System Settings > Notifications.**

In the navigation tree on the left, choose SMS modem settings. On the SMS modem settings page, set the network standard, serial port for connecting to the SMS modem, baud rate, mobile number for receiving notifications, and whether to support long SMS messages. For details about the parameters, see Table 10-4.

Table 10-4 SMS modem parameters

Parameter Name	Explanation	Example
Network system of SMS modem	The value can be GSM, CDMA, or LTE. The default value is CDMA.	CDMA
SMS modem serial port	The serial port is a local hardware connection, including COM1 and COM2. The default value is null.	COM1
SMS modem baud rate	Indicates the baud rate of the serial port of the SMS modem. Default value: 9600.	115200

Recipient mobile number	The mobile number must be prefixed with a country code. For example, if the country code of China is 86, the mobile number format is 86 + mobile number.	8613XXXXXXXXX
Allow long SMS messages	It is recommended that long SMS messages be supported.	Yes
Enabled	By default, this parameter is set to Yes. If this parameter is set to No, the setting is unavailable and SMS messages cannot be sent.	Yes

- Click **Test** to check whether the system is connected to the SMS modem.
  - If the test is successful, a message is displayed, indicating that the test is successful.
  - If the test fails, a message is displayed indicating that the connection fails. Check whether the parameters are correctly set.
- Click **Apply**.

----End

10.3.2.2 Commissioning Email-based Notifications

Remote Notification provides the email notification function. When O&M personnel need to send emails, set email notification parameters and verify the settings to ensure that emails can be sent properly.

The procedure is as follows:

Step 1 Choose **System > System Settings > Notifications.**

Step 2 In the navigation pane on the left, choose **Email Server Settings** and set the domain name and IP address of the SMTP server, email address for sending notifications, code, and port number. For details about the parameters, see Table 10-5.

Table 10-5 Parameters for setting email addresses

Parameter Name	Explanation	Example
SMTP server domain name/IP address	Domain name or IP address of the SMTP server.	10.1.1.1
Sender email address	Specifies the sender's email address displayed when remote notifications are sent by email. This email address must be registered on the interconnected SMTP server and must be filled in completely. Otherwise, the email will fail to be sent. Recipients can see the address when they	s@example.com

	receive the mail. You are not advised to use a private email address to send notifications.	
Charset	Encoding format of the sending email server. The default value is UTF-8.	UTF-8
Enable secure connection over SMTP (Applies when an email server certificate for SMTP server is already installed. TLS is recommended.)	If SSL/TLS connections are required, the default port number for TLS is 587 and the default port number for SSL is 465. By default, the secure connection is enabled. The default value is TLS. To ensure that emails can be sent successfully, ensure that the port on the email server is available and the configuration certificate is valid. If SSL/TLS connections are not required, the default SMTP port is **25**. To ensure successful email sending, ensure that the port on the email server is available.	TLS
Server Port	Port number of the SMTP server.	25
Require identity authentication for the SMTP server	Indicates whether to authenticate emails sent by the SMTP server. Obtain the value from the SMTP server administrator. If the SMTP server requires identity authentication, obtain the user name and password from the administrator.	/
User Name	User name for logging in to the SMTP server. The user name must be the same as the user name for sending notifications.	Test123
Password	Password for logging in to the SMTP server. The password must be the same as that of the email address for sending notifications.	/
Enabled	The default value is Yes. If you select No, the settings are unavailable and SMS messages cannot be sent.	Yes

Step 3 Click **Test** to check whether the system is connected to the email server.

- If the test is successful, a message is displayed, indicating that the test is successful.
- If the test fails, a message is displayed indicating that the connection fails. Check whether the parameters are correctly set.

Step 4 Click **Apply**.

----End

10.3.3 Setting Notification Parameters

Before sending notifications to users, O&M personnel need to create users and user groups, and set notification templates and notification rules.

10.3.3.1 Creating a Notified User

O&M personnel can set message recipients to meet message sending requirements.

The procedure is as follows:

Step 1 Choose **System > System Settings > Notifications**.

Step 2 In the navigation pane on the left, choose **Notified Users Management > Users.**

Step 3 On the **Users** page, click **Create**.

Step 4 Enter the user information. At least one of the mobile number and email address must be set.

- The user name is case sensitive.

Step 5 Click **OK.**

----End

10.3.3.2 Creating a Notified User Group

Notification provides the function of creating notification user groups. O&M personnel can create user groups to send notifications to users.

The procedure is as follows:

Step 1 Choose **System > System Settings > Notifications.**

Step 2 In the navigation pane on the left, choose **Notified User Management > Notified Groups.**

Step 3 On the **Notified Groups** page, click **Create**.

Step 4 Enter the user group information and add the user to the user group.

- On the Notified Users tab page, you can click Create to add a notification user. The newly created user is added to the user group by default.
- A maximum of 200 users can be added to a notification user group.
- When adding a user to a user group, you can search by user name, mobile number, or email address on the Notified User and O&M User tab pages.
- If both the mobile number and email address of a user are empty, the user cannot be added to the user group.
- The user group name is case sensitive.

Step 5 Click **OK.**

----End

10.3.3.3 Creating a notification template

When O&M personnel need to send notifications to users, O&M personnel can set common notification content as templates and use the templates to improve the content standardization and efficiency.

The procedure is as follows:

Step 1 Choose **System > System Settings > Notifications**.

Step 2 In the navigation pane on the left, choose **Notification Templates**.

Step 3 On the **Notification Template** page, click **Create**.

Step 4 Enter the template information.

Step 5 Click **OK**.

----End

10.3.3.4 Setting Remote Notification Rules

If O&M personnel cannot view alarms and events on the alarm management page due to non-working hours or business trips, they can configure remote notification rules to send concerned alarms and events to O&M personnel through SMS messages or emails, this helps users learn about alarms and events in time and take corresponding measures.

The procedure is as follows:

Step 1 Choose **Monitor > Alarm Management > Alarm Settings.**

Step 2 In the navigation pane on the left, choose **Notification Rules**. Click **Create** and choose **Alarm Notification Rules**.

- Set Severity to Critical and Major.
- Set Alarm Source to Custom Alarm Source and add system A to the alarm source list.
- In the Advanced Condition area, set certain conditions for some fields in the alarm content as required.
- Set Notification Mode to SMS and Email, and select Message_A and Email_A for Template.
- In the Notified User Group area, select the recipient of the alarm, that is, the notification user group of O&M personnel A.

Step 3 Click **OK**.

----End