

**iMaster NetEco 6000
V600R021C00**

Device Installation and Commissioning Guide

Issue	03
Date	2021-11-23



Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

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

Trademarks and Permissions



HUAWEI 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: <https://e.huawei.com>

About This Document

Purpose

This document describes the iMaster NetEco 6000 V600R021C00 in terms of its hardware installation, cable connection, commissioning, and maintenance to help readers better understand the NetEco product.

For details about NetEco product software commissioning, see *iManager NetEco 6000 Product Documentation (V600R021C00)*.

The figures provided in this document are for reference only.

The software version of the NetEco is V600R021C00.

Intended Audience

This document is intended for:

- Sales engineers
- Technical support engineers
- System engineers

Symbol Conventions

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

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

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

Change History

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

Issue 03 (2021-11-23)

Optimized [Configuring Camera Parameters on the NetEco](#).

Issue 02 (2021-05-12)

- Added descriptions about the infrared sensor.
- Added descriptions about the UIM20A expansion module.
- Optimized the content related to the video management system.
- Optimized and added the content related to the UPS.

Issue 01 (2020-09-03)

This issue is the first official release.

Contents

About This Document.....	ii
1 Safety Information.....	1
1.1 General Safety.....	1
1.2 Personnel Requirements.....	4
1.3 Electrical Safety.....	4
1.4 Installation Environment Requirements.....	6
1.5 Mechanical Safety.....	8
1.6 Others.....	10
2 Installation Preparations.....	11
2.1 Unpacking and Acceptance.....	11
2.2 Tools and Instruments.....	11
2.3 Personnel Requirements.....	14
2.4 Device Networking Solution Overview.....	15
2.5 Installation Process.....	15
3 Installing Devices.....	17
3.1 Layout in the Network Cabinet.....	17
3.2 Installing a Server.....	18
3.2.1 Installing a TaiShan 200 Server.....	18
3.2.2 Installing a 2288X V5 Server.....	20
3.3 Installing a LAN Switch.....	22
3.4 Installing an ECC800-Pro Collector.....	23
3.5 Installing a Smart U Space Manager (BOM Number: 52273314).....	24
3.6 Installing a UIM20A Expansion Module.....	26
3.7 Installing Sensors.....	28
3.7.1 Installing Cabinet Temperature Sensors.....	28
3.7.2 Installing a Hydrogen Sensor.....	29
3.7.3 Installing the Hydrogen Detection System.....	30
3.7.4 Installing a Smoke Detector.....	33
3.7.5 Installing a Temperature and Humidity Sensor (BOM Number: 33010346).....	34
3.7.6 Installing a Temperature and Humidity Sensor (BOM Number: 02312PBL).....	35
3.7.7 Installing a Region-type Water Sensor.....	37
3.7.8 Installing a Location-type Water Sensor.....	40

3.7.9 Installing an Infrared Sensor.....	43
3.8 Installing the Video Management System.....	45
3.8.1 Installing the VCN510.....	45
3.8.2 Installing the VCN520.....	51
3.8.3 Installing the VCN540.....	54
3.8.4 Installing an IVS1800.....	57
3.8.5 Installing a C3220 Camera.....	62
3.8.6 Installing the M2121 Camera.....	65
3.9 Installing the Access Management System.....	68
3.9.1 Installing an A8802RS Access Controller.....	68
3.9.2 Installing an In-Room Double-Door Magnetic Lock.....	70
3.9.3 Installing an In-Room Single-Door Magnetic Lock.....	72
3.9.4 Installing a Fingerprint and Card Reader with a Keypad.....	76
3.9.5 Installing a Fingerprint and Card Reader.....	77
3.9.6 Installing a Card Reader with a Keypad.....	78
3.9.7 Installing an Exit Button.....	80
3.9.8 Installing an In-room Emergency Door Release Button.....	80
4 Connecting Monitoring Cables to Devices.....	82
4.1 Scenarios for Connecting a Server.....	82
4.1.1 Server Ports (TaiShan 200 Server).....	82
4.1.2 Server Ports (2288X V5 Server).....	83
4.1.3 Installing the SMS Modem.....	85
4.1.4 Connecting Cables to the 4G SMS Modem.....	86
4.2 Scenarios for Connecting a LAN Switch.....	88
4.2.1 LAN Switch Introduction (S5320-28X-PWR-SI).....	88
4.2.2 LAN Switch Introduction (S5720-28X-PWR-SI).....	92
4.2.3 LAN Switch Introduction (S5331-H24P4XC).....	95
4.2.4 LAN Switch Introduction (S5731-H24P4XC).....	98
4.2.5 Introduction to Switches (S5335-S24P4X).....	101
4.2.6 Introduction to Switches (S5735-S24P4X).....	105
4.2.7 Connecting a Monitoring Cable to the NetEco.....	108
4.2.8 Connecting the Video Management System Cable.....	109
4.2.8.1 Connecting a Monitoring Cable to a VCN510.....	109
4.2.8.2 Connecting a Monitoring Cable to a VCN520.....	109
4.2.8.3 Connecting a Monitoring Cable to a VCN540.....	110
4.2.8.4 Connecting a Monitoring Cable to the IVS1800.....	111
4.2.8.5 Connecting a Monitoring Cable to a Camera.....	111
4.2.9 Connecting the Smart Cooling Product Monitoring Cable.....	112
4.2.10 Connecting the UPS Monitoring Cable.....	114
4.2.10.1 Connecting the UPS2000-G Monitoring Cable (SNMP).....	114
4.2.10.2 Connecting the UPS5000-A Monitoring Cable.....	115
4.2.10.3 Connecting a Monitoring Cable to the UPS5000-E/UPS5000-H/UPS5000-S.....	116

4.2.11 Connecting the SmartLi Monitoring Cable.....	116
4.2.12 Connecting the PDU8000 Monitoring Cable.....	117
4.2.13 Connecting the MTS9604B-N20B1 Power Monitoring Cable.....	117
4.2.14 Connecting a Monitoring Cable to TP483000D.....	118
4.2.15 Connecting a Monitoring Cable to an iBOX.....	118
4.3 Scenarios for Connecting the ECC800-Pro Outside the Smart Module.....	118
4.3.1 Preparing a Monitoring Cable.....	119
4.3.2 ECC800-Pro.....	120
4.3.2.1 Product Configuration.....	120
4.3.2.2 Main Control Module.....	123
4.3.2.3 Power Module.....	131
4.3.3 UIM20A Expansion Module.....	133
4.3.4 Connecting a Monitoring Cable to the UIM20A Expansion Module.....	136
4.3.5 Connecting the Access Management System Cable.....	136
4.3.5.1 Connecting a Monitoring Cable to the A8802RS Access Controller.....	137
4.3.5.2 Connecting a Monitoring Cable to the Door Status Sensor.....	144
4.3.6 Connecting Cables to Sensors.....	145
4.3.6.1 Connecting Cables to Sensors.....	145
4.3.6.2 Connecting the Temperature Sensor Monitoring Cable.....	147
4.3.6.3 Connecting a Monitoring Cable to the Hydrogen Detection System.....	147
4.3.6.4 Connecting a Monitoring Cable to the Smoke Sensor.....	148
4.3.6.5 Connecting a Monitoring Cable to a T/H Sensor.....	148
4.3.6.6 Connecting a Monitoring Cable to the Region-type Water Sensor.....	149
4.3.6.7 Connecting a Monitoring Cable to the Location-type Water Sensor.....	149
4.3.6.8 Connecting a Monitoring Cable to the Infrared Sensor.....	150
4.3.7 Connecting the Smart Cooling Product Monitoring Cable.....	150
4.3.7.1 Connecting the NetCol5000 Monitoring Cable.....	151
4.3.7.2 Connecting the NetCol8000 Monitoring Cable.....	155
4.3.8 Connecting a Monitoring Cable to a Chiller.....	158
4.3.9 Connecting the UPS Monitoring Cable.....	158
4.3.9.1 Connecting a Monitoring Cable to the UPS2000-G (Modbus).....	159
4.3.9.2 Connecting a Monitoring Cable to the UPS5000-A.....	159
4.3.10 Connecting the PDC Monitoring Cable.....	160
4.3.10.1 Connecting the PDU8000 Monitoring Cable.....	161
4.3.10.2 Connecting a Monitoring Cable to the Monitoring Type-PDU2000-32-1PH-20/4-M1.....	161
4.3.10.3 Connecting a Monitoring Cable to an HPXPDU2000-16-3PH-24-6-M1.....	162
4.3.11 Connecting the Fresh Air Unit Monitoring Cable.....	162
4.3.11.1 Connecting a Monitoring Cable to the Fresh Air Unit.....	163
4.4 Scenarios for Connecting the ECC800-Pro in the Smart Module.....	163
4.4.1 Connecting a Monitoring Cable to the ECC800-Pro Collector.....	163
5 Checking the Installation.....	165
5.1 Checking the Installation of the Cabinet.....	165

5.2 Checking the Installation of Components in the Cabinet.....	166
5.3 Checking the Installation of Power Cables and Ground Cables.....	166
5.4 Checking the Connection of Signal Cables.....	167
6 Adding Devices.....	169
6.1 Performing Basic Operations Before Adding Devices.....	169
6.1.1 IP Address Preinstallation Planning.....	170
6.1.2 Obtaining the NetEco Software License.....	170
6.1.3 Powering On a Server.....	171
6.1.4 Logging In to the NetEco Client.....	172
6.1.5 Loading the NetEco Software License.....	172
6.1.6 Installing NE Adapters.....	173
6.1.7 Creating a Management Domain.....	174
6.1.8 Adding a Module.....	175
6.1.9 Process of adding a device.....	178
6.2 Scenarios for Connecting the ECC800-Pro in the Smart Module.....	179
6.2.1 Commissioning Southbound Devices of the ECC800-Pro.....	180
6.2.2 Adding a Smart U Space Manager.....	180
6.2.2.1 Commissioning the Smart U Space Manager on the ECC800-Pro WebUI.....	180
6.2.2.2 Determining the Position of the Smart U Space Manager (Connected to a UIM20A Expansion Module).....	181
6.2.2.3 Registering Assets.....	182
6.2.3 iCooling Energy Management.....	184
6.2.3.1 Setting Cooling Management Parameters.....	185
6.2.3.2 Configuring iCooling Parameters.....	186
6.2.3.3 Viewing iCooling Energy Efficiency.....	188
6.2.4 (Optional) Viewing a Temperature Map on the NetEco.....	189
6.3 Scenarios for Connecting the Server.....	189
6.3.1 Setting SMS.....	190
6.4 Scenarios for Connecting the LAN Switch.....	192
6.4.1 Adding an iBOX Collector.....	192
6.4.1.1 Setting Parameters on the iBOX WebUI.....	192
6.4.1.2 Creating an iBOX Collector on the NetEco.....	197
6.4.1.3 iBOX and iBAT Networking.....	200
6.4.2 Adding a Video Management System.....	202
6.4.2.1 Obtaining Video Management System Documents.....	202
6.4.2.2 Commissioning a C3220/M2121 Camera.....	202
6.4.2.3 Commissioning the VCN.....	210
6.4.2.3.1 Initializing VCN510 Disks.....	210
6.4.2.3.2 Initializing VCN520 or VCN540 Disks.....	212
6.4.2.3.3 Setting Parameters on the VCN WebUI.....	215
6.4.2.3.4 Setting Parameters on the VCN IVS Client.....	218
6.4.2.4 Commissioning the IVS1800.....	221

6.4.2.4.1 Setting Parameters on the IVS1800 WebUI.....	221
6.4.2.4.2 Setting Parameters on the IVS1800 WebUI.....	226
6.4.2.5 Configuring Camera Parameters on the NetEco.....	232
6.4.2.6 Registering with the OCX Plug-in.....	234
6.4.2.7 Adding the Video Management System.....	237
6.4.2.8 Setting Video Playback.....	238
6.4.3 Adding a Smart Cooling Product.....	238
6.4.3.1 Setting Monitoring Parameters for the Smart Cooling Product (over Modbus-TCP).....	239
6.4.3.2 Creating a Smart Cooling Product on the NetEco.....	241
6.4.4 Adding a Refrigeration Station.....	243
6.4.4.1 Creating a Chiller Subsystem on the NetEco (Modbus-TCP Protocol).....	243
6.4.4.2 Creating a Chiller on the NetEco.....	245
6.4.5 Adding a UPS.....	246
6.4.5.1 Setting Monitoring Parameters for a UPS2000-G (over SNMP).....	246
6.4.5.2 Setting UPS5000 Monitoring Parameters (over SNMP).....	250
6.4.5.3 Setting UPS5000 Monitoring Parameters (Modbus TCP).....	254
6.4.5.4 Creating a UPS on the NetEco.....	256
6.4.6 Adding a PDU.....	259
6.4.6.1 Setting PDU8000 Monitoring Parameters (SNMP).....	259
6.4.6.2 Setting PDU8000 Monitoring Parameters (Modbus TCP).....	260
6.4.6.3 Creating a PDU on the NetEco.....	261
6.4.7 Adding an MTS9604B-N20B1 Power Supply.....	262
6.4.7.1 Creating a MTS9604B-N20B1 Power Supply on the NetEco.....	262
6.4.8 Adding a SmartLi.....	264
6.4.8.1 Setting SmartLi Monitoring Parameters (Modbus TCP).....	264
6.4.8.2 Creating a SmartLi on the NetEco.....	265
6.4.9 Adding a CO Power Module.....	266
6.4.9.1 Setting Monitoring Parameters for the TP483000D and TP482000B.....	266
6.4.9.2 Creating a Power Module on the NetEco.....	267
6.4.10 Adding an rPDU.....	268
6.4.10.1 Setting RPDU_HUAWEI_PDU2000-32-1PH-20-4-M2 Monitoring Parameters.....	269
6.4.10.2 Creating an rPDU on the NetEco.....	269
6.5 Scenarios for Connecting the ECC800-Pro Outside the Smart Module.....	271
6.5.1 Setting and Adding the ECC800-Pro Collector.....	271
6.5.1.1 Preparations and Login.....	271
6.5.1.2 Setting the ECC800-Pro IP Address.....	275
6.5.1.3 Setting the ECC800-Pro System Type.....	276
6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector.....	277
6.5.1.5 Setting NetEco Parameters.....	279
6.5.1.6 Creating an ECC800-Pro Collector on the NetEco.....	280
6.5.1.7 Setting the Transparent Transmission Function for the ECC800-Pro Collector.....	283
6.5.1.8 Setting Transparent Transmission for the UIM20A Expansion Module.....	284

6.5.2 Adding Sensors.....	287
6.5.2.1 Adding Dry Contact Interface Devices.....	287
6.5.2.1.1 Setting Door Status Sensor Monitoring Parameters on the ECC800-Pro Web.....	287
6.5.2.1.2 Setting Smoke Sensor and Water Leakage Sensor Parameters on the ECC800-Pro Web.....	288
6.5.2.1.3 Setting Infrared Sensor Monitoring Parameters on the ECC800-Pro Web.....	289
6.5.2.1.4 Setting Device Monitoring Parameters of an NO/NC Dry Contact on the ECC800-Pro Web.....	290
6.5.2.1.5 Creating an Icon for a Door Status Sensor on the NetEco.....	291
6.5.2.1.6 Creating the Water Sensor on the NetEco.....	294
6.5.2.1.7 Modifying Alarm Names for Devices on the NetEco.....	296
6.5.2.1.8 Modifying Performance Counter Names for Devices on the NetEco.....	297
6.5.2.2 Adding a Temperature and Humidity Sensor.....	297
6.5.2.2.1 Setting Monitoring Parameters for a T/H Sensor (BOM Number: 33010346).....	298
6.5.2.2.2 Creating a Temperature and Humidity Sensor on the NetEco.....	298
6.5.2.3 Adding a Water Leakage Sensor.....	299
6.5.2.3.1 Creating a Water Leakage Sensor on the NetEco.....	300
6.5.2.4 Adding a Hydrogen Sensor.....	301
6.5.2.4.1 Setting Monitoring Parameters for a Hydrogen Sensor.....	301
6.5.2.4.2 Creating a Hydrogen Sensor on the NetEco.....	302
6.5.3 Adding the Access Management System.....	303
6.5.3.1 Setting Monitoring Parameters for the A8802RS Access Controller.....	303
6.5.3.2 Creating an Access Controller on the NetEco.....	303
6.5.3.3 Formatting an Access Controller.....	305
6.5.3.4 Setting Monitoring Parameters for the NEWABEL CHD200G Fingerprint Controller.....	306
6.5.3.5 Creating a NEWABEL CHD200G Fingerprint Controller on the NetEco.....	306
6.5.4 Adding a Smart Cooling Product.....	308
6.5.4.1 Setting Monitoring Parameters for Smart Cooling Products (over Modbus-RTU).....	308
6.5.4.2 Creating a Smart Cooling Product on the NetEco.....	309
6.5.5 Adding a Chiller.....	311
6.5.5.1 Creating a Chiller on the NetEco.....	311
6.5.6 Adding a UPS.....	312
6.5.6.1 Setting Monitoring Parameters for a UPS2000.....	312
6.5.6.2 Creating a UPS on the NetEco.....	313
6.5.7 Adding a PDU.....	314
6.5.7.1 Setting Monitoring Parameters for a PDU8000.....	314
6.5.7.2 Creating a PDU on the NetEco.....	315
6.5.8 Adding a Fresh Air Unit.....	316
6.5.8.1 Creating a Fresh Air Unit on the NetEco.....	316
6.5.9 Adding an rPDU.....	317
6.5.9.1 Setting Monitoring Parameters for HPXPDU2000-16-3PH-24-6-M1.....	317
6.5.9.2 Creating an rPDU on the NetEco.....	318
7 Device Maintenance.....	320
7.1 Routine Maintenance.....	320

7.1.1 Monthly maintenance.....	320
7.1.1.1 Routine Maintenance for the Collector.....	320
7.1.1.2 Routine Maintenance for the UIM20A Expansion Module.....	321
7.1.1.3 Routine Maintenance for VCN.....	321
7.1.1.4 Routine Maintenance for the Smoke Detector.....	322
7.1.1.5 Routine Maintenance for the Hydrogen Detection System.....	323
7.1.1.6 Routine maintenance for the region-type water sensor and water detection cable.....	324
7.1.1.7 Routine maintenance for the location-type water sensor and water detection cable.....	324
7.1.1.8 Routine Maintenance for Infrared Sensors.....	325
7.1.2 Semi-Annual Maintenance.....	325
7.1.2.1 Routine maintenance for the switch.....	326
7.1.2.2 Routine Maintenance for the Smart U space manager.....	327
7.1.2.3 Routine Maintenance for Temperature Sensors.....	327
7.1.2.4 Routine maintenance for the temperature and humidity sensor.....	327
7.1.2.5 Routine maintenance for the camera.....	328
7.1.2.6 Routine maintenance for the access control system.....	329
7.1.2.7 Routine Maintenance for the Access Controller.....	329
7.1.2.8 Routine maintenance for the single-door/double-door magnetic lock.....	330
7.1.2.9 Routine maintenance for the emergency door release button.....	330
7.2 Parts Replacement.....	330
7.2.1 Parts Replacement for the ECC800-Pro.....	330
7.2.1.1 Replacing an ECC800-Pro Main Control Module.....	330
7.2.1.2 Replacing an ECC800-Pro PSU.....	332
7.2.1.3 Replacing ECC800-Pro Antennas.....	333
7.2.1.4 Replacing a SIM Card.....	333
7.2.2 Replacing a UIM20A expansion module.....	335
7.2.3 Replacing a Smart U Space Manager (Connected to a UIM20A Expansion Module) (BOM Number: 52273314).....	336
7.2.4 Replacing Sensors.....	339
7.2.4.1 Replacing a Temperature Sensor.....	339
7.2.4.2 Replacing the Hydrogen Detection System.....	339
7.2.4.3 Replacing a Smoke Detector.....	342
7.2.4.4 Replacing a T/H Sensor.....	343
7.2.4.5 Replacing a Region-type Water Sensor and Water Detection Cable.....	343
7.2.4.6 Replacing a Location-type Water Sensor and Water Detection Cable.....	345
7.2.4.7 Replacing an Infrared Sensor.....	346
7.2.5 Replacing the Management System.....	347
7.2.5.1 Replacing the VCN510 Hard Disk.....	347
7.2.5.2 Replacing the VCN520/VCN540 Hard Disk.....	352
7.2.5.3 Replacing a VCN510.....	354
7.2.5.4 Replacing a VCN520.....	355
7.2.5.5 Replacing a VCN540.....	356
7.2.5.6 Replacing an IVS1800.....	358

7.2.5.7 Replacing a Hard Disk for the IVS1800.....	359
7.2.5.8 Replacing an IPC6325 Camera.....	362
7.2.5.9 Replacing an IPC6225 camera.....	363
7.2.5.10 Replacing an M2121 Camera.....	364
7.2.6 Replacing the Access Management System.....	364
7.2.6.1 Replacing an Access Controller.....	364
7.2.6.2 Replacing a Double-Door Magnetic Lock.....	366
7.2.6.3 Replacing a Single-Door Magnetic Lock.....	370
7.2.6.4 Replacing a Card Reader.....	370
7.2.6.5 Replacing a Fingerprint and Card Reader.....	373
7.2.6.6 Replacing a Card Reader with a Keypad.....	375
7.2.6.7 Replacing a Fingerprint and Card Reader with a Keypad.....	376
7.2.6.8 Replacing an Emergency Door Release Button.....	377
8 FAQ.....	380
8.1 How Do I Handle Abnormal Door Control Status?.....	380
8.2 How Do I Change the NetEco IP Address?.....	380
9 Acronyms and Abbreviations.....	383

1 Safety Information

1.1 General Safety

Statement

Before installing, operating, and maintaining the equipment, carefully read this document and observe all safety instructions provided herein and written on the equipment itself.

The "NOTICE", "CAUTION", "WARNING", and "DANGER" statements in this document do not cover all the safety instructions. They are only supplements to the safety instructions. The Company will not be liable for any consequence caused by the violation of general safety requirements or design, production, and usage safety standards.

Ensure that the equipment is used in environments that meet its design specifications. Otherwise, the equipment may become faulty, and the resulting equipment malfunction, component damage, personal injuries, or property damage will not be covered under the warranty.

Follow local laws and regulations when installing, operating, or maintaining the equipment. The safety instructions in this document are only supplements to local laws and regulations.

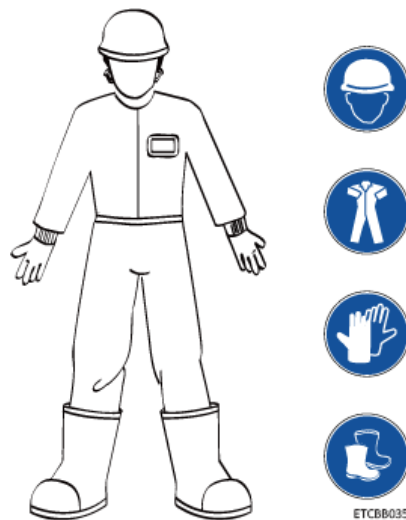
The Company will not be liable for any consequences of the following circumstances:

- Operation beyond the conditions specified in this document
- Installation or use in environments which are not specified in relevant international or national standards
- Unauthorized modifications to the product or software code or removal of the product
- Failure to follow the operation instructions and safety precautions on the product and in this document
- Equipment damage due to force majeure, such as earthquakes, fire, and storms

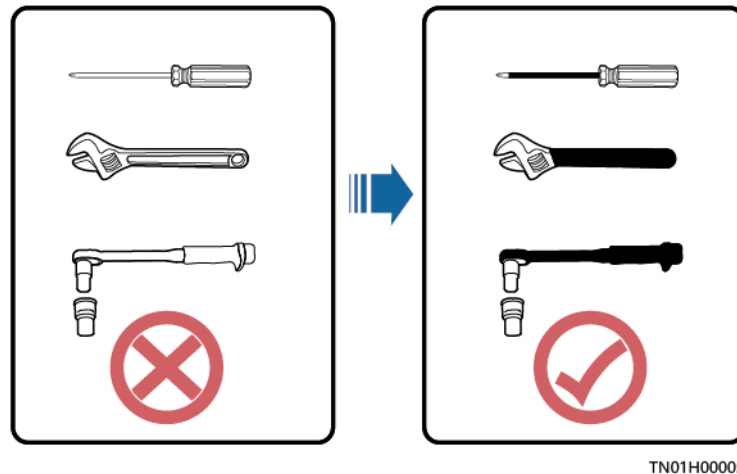
- Damage caused during transportation by the customer
- Storage conditions that do not meet the requirements specified in this document

General Requirements

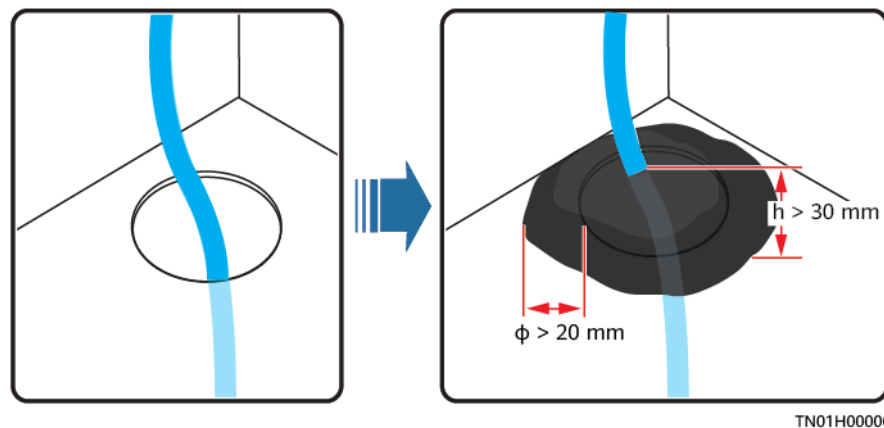
- Do not install, use, or operate outdoor equipment and cables (including but not limited to moving equipment, operating equipment and cables, inserting connectors to or removing connectors from signal ports connected to outdoor facilities, working at heights, and performing outdoor installation) in harsh weather conditions such as lightning, rain, snow, and level 6 or stronger wind.
- Before installing, operating, or maintaining the equipment, remove any conductive objects such as watches or metal jewelry like bracelets, bangles, and rings to avoid electric shock.
- When installing, operating, or maintaining the equipment, wear dedicated protective gears such as insulation gloves, goggles, and safety clothing, helmet, and shoes, as shown in the following figure.



- Follow the specified procedures for installation, operation, and maintenance.
- Before handling a conductor surface or terminal, measure the contact point voltage and ensure that there is no risk of electric shock.
- After installing the equipment, remove idle packing materials such as cartons, foam, plastics, and cable ties from the equipment area.
- In the case of a fire, immediately leave the building or the equipment area and activate the fire alarm or call emergency services. Do not re-enter the building or affected area until it has been deemed safe by qualified professionals.
- Do not stop using protective devices. Pay attention to the warnings, cautions, and related precautionary measures in this document and on the equipment. Promptly replace warning labels that have worn out.
- Keep irrelevant people away from the equipment. Only operators are allowed to access the equipment.
- Use insulated tools or tools with insulated handles, as shown in the following figure.



- All cable holes should be sealed. Seal the used cable holes with firestop putty. Seal the unused cable holes with the caps delivered with the cabinet. The following figure shows the criteria for correct sealing with firestop putty.



- Do not scrawl, damage, or block any warning label on the equipment.
- When installing the equipment, use a torque wrench with a proper range to tighten the screws. When using a wrench to tighten the screws, ensure that the wrench does not tilt and the torque error does not exceed 10% of the specified value.
- Do not work with power on during installation.
- Repaint any paint scratches caused during equipment transportation or installation in a timely manner. Equipment with scratches cannot be exposed to an outdoor environment for an extended period of time.
- Before operations, ensure that the equipment is firmly secured to the floor or other solid objects, such as a wall or an installation rack.
- Do not use water to clean electrical components inside or outside of a cabinet.
- Do not change the structure or installation sequence of equipment without permission.
- Do not touch a running fan with your fingers, components, screws, tools, or boards before the fan is powered off or stops running.

Personal Safety

- If there is a likelihood of personal injury or equipment damage during operations, immediately stop, report the case to the supervisor, and take feasible protective measures.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telecommunication network voltage (TNV) circuits.
- Do not power on the equipment before it is installed or confirmed by professionals.

1.2 Personnel Requirements

- Personnel who plan to install or maintain the equipment must receive thorough training, understand all necessary safety precautions, and be able to correctly perform all operations.
- Only qualified professionals or trained personnel are allowed to install, operate, and maintain the equipment.
- Only qualified professionals are allowed to remove safety facilities and inspect the equipment.
- Personnel who will operate the equipment, including operators, trained personnel, and professionals, should possess the local national required qualifications in special operations such as high-voltage operations, working at heights, and operations of special equipment.
- Professionals: personnel who are trained or experienced in equipment operations and are clear of the sources and degree of various potential hazards in equipment installation, operation, maintenance
- Trained personnel: personnel who are technically trained, have required experience, are aware of possible hazards on themselves in certain operations, and are able to take protective measures to minimize the hazards on themselves and other people
- Operators: operation personnel who may come in contact with the equipment, except trained personnel and professionals
- Only professionals or authorized personnel are allowed to replace the equipment or components (including software).

1.3 Electrical Safety

Grounding

- For the equipment that needs to be grounded, install the ground cable first when installing the equipment and remove the ground cable last when removing the equipment.
- Do not damage the ground conductor.
- Do not operate the equipment in the absence of a properly installed ground conductor.
- Ensure that the equipment is connected permanently to the protective ground. Before operating the equipment, check its electrical connection to ensure that it is securely grounded.

General Requirements

Use dedicated insulated tools when performing high-voltage operations.

AC and DC Power

DANGER

Do not connect or disconnect power cables with power on. Transient contact between the core of the power cable and the conductor will generate electric arcs or sparks, which may cause fire or personal injury.

- If a "high electricity leakage" tag is attached on the equipment, ground the protective ground terminal on the equipment enclosure before connecting the AC power supply; otherwise, electric shock as a result of electricity leakage may occur.
- Before installing or removing a power cable, turn off the power switch.
- Before connecting a power cable, check that the label on the power cable is correct.
- If the equipment has multiple inputs, disconnect all the inputs before operating the equipment.
- A circuit breaker equipped with a residual current device (RCD) is not recommended.
- A damaged power cable must be replaced by the manufacturer, service agent, or professionals to avoid risks.
- High voltage operations and installation of AC-powered facilities must be performed by qualified personnel.

Cabling

- When routing cables, ensure that a distance of at least 30 mm exists between the cables and heat-generating components or areas. This prevents damage to the insulation layer of the cables.
- Do not route cables behind the air intake and exhaust vents of the equipment.
- Ensure that cables meet the VW-1 or ZB flame spread rating requirements or higher.
- Bind cables of the same type together. When routing cables of different types, ensure that they are at least 30 mm away from each other.
- If an AC input power cable is connected to the cabinet from the top, bend the cable in a U shape outside the cabinet and then route it into the cabinet.
- When the temperature is low, violent impact or vibration may damage the plastic cable sheathing. To ensure safety, comply with the following requirements:
 - Cables can be laid or installed only when the temperature is higher than 0°C. Handle cables with caution, especially at a low temperature.
 - Cables stored at subzero temperatures must be stored at room temperature for at least 24 hours before they are laid out.

- Do not perform any improper operations, for example, dropping cables directly from a vehicle.
- When selecting, connecting, and routing cables, follow local safety regulations and rules.

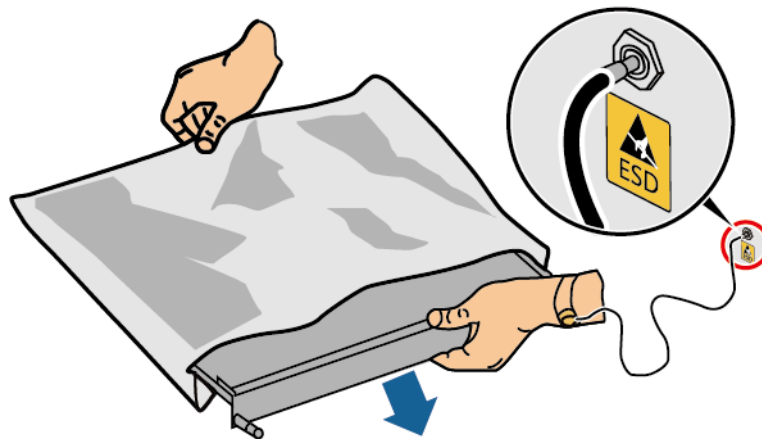
ESD

NOTICE

The static electricity generated by human bodies may damage the electrostatic-sensitive components on boards, for example, the large-scale integrated (LSI) circuits.

- Wear ESD gloves or a well-grounded ESD wrist strap when touching the device or handling boards or application-specific integrated circuits (ASICs).
- When holding a board, hold its edge without touching any components. Do not touch the components with your bare hands.
- Package boards with ESD packaging materials before storing or transporting them.

Figure 1-1 Wearing an ESD wrist strap



DC15000001

Neutral-Ground Voltage

It is recommended that the three-phase loads be equalized and the neutral-ground voltage be kept at less than 2 V to meet power distribution requirements.

1.4 Installation Environment Requirements

- To prevent fire due to high temperature, ensure that the ventilation vents or heat dissipation system are not blocked when the equipment is running.
- Install the equipment in an area far away from liquids. Do not install it under areas prone to condensation, such as under water pipes and air exhaust vents, or areas prone to water leakage, such as air conditioner vents, ventilation

vents, or feeder windows of the equipment room. Ensure that no liquid enters the equipment to prevent faults or short circuits.

- If any liquid is detected inside the equipment, immediately disconnect the power supply and contact the administrator.
- Do not expose the equipment to flammable or explosive gas or smoke. Do not perform any operation on the equipment in such environments.
- Ensure that the equipment room provides good heat insulation, and the walls and floor are dampproof.
- Install a rat guard at the door of the equipment room.

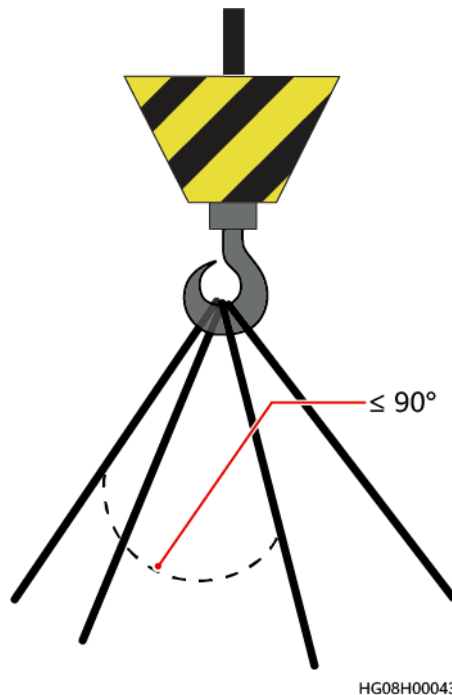
Installation at Heights

- Working at heights refers to operations that are performed at least 2 meters above the ground.
- Do not work at heights if the steel pipes are wet or other potential danger exists. After the preceding conditions no longer exist, the safety director and relevant technical personnel need to check the involved equipment. Operators can begin working only after obtaining consent.
- When working at heights, comply with local relevant laws and regulations.
- Only trained and qualified personnel are allowed to work at heights.
- Before working at heights, check the climbing tools and safety gears such as safety helmets, safety belts, ladders, springboards, scaffolding, and lifting equipment. If they do not meet the requirements, take corrective measures or disallow working at heights.
- Wear personal protective equipment such as the safety helmet and safety belt or waist rope and fasten it to a solid structure. Do not mount it on an insecure moveable object or metal object with sharp edges. Make sure that the hooks will not slide off.
- Set a restricted area and eye-catching signs for working at heights to warn away irrelevant personnel.
- Carry the operation machinery and tools properly to prevent them from falling off and causing injuries.
- Personnel involving working at heights are not allowed to throw objects from the height to the ground, or vice versa. Objects should be transported by tough slings, hanging baskets, highline trolleys, or cranes.
- Ensure that guard rails and warning signs are set at the edges and openings of the area involving working at heights to prevent falls.
- Do not pile up scaffolding, springboards, or other sundries on the ground under the area involving working at heights. Do not allow people to stay or pass under the area involving working at heights.
- Inspect the scaffolding, springboards, and workbenches used for working at heights in advance to ensure that their structures are solid and not overloaded.
- Any violations must be promptly pointed out by the site manager or safety supervisor and the involved personnel should be prompted for correction. Personnel who fail to stop violations will be forbidden from working.

1.5 Mechanical Safety

Hoisting

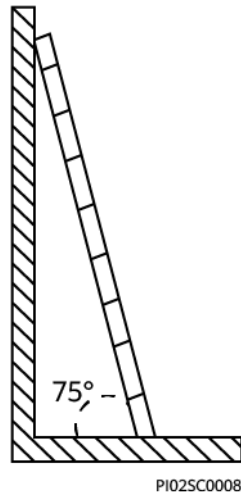
- Do not walk under hoisted objects.
- Only trained and qualified personnel should perform hoisting operations.
- Check that hoisting tools are available and in good condition.
- Before hoisting objects, ensure that hoisting tools are firmly secured onto a load-bearing object or wall.
- Ensure that the angle formed by two hoisting cables is no more than 90 degrees, as shown in the following figure.



- Do not drag steel ropes and hoisting tools or bump hoisted objects against hard objects during hoisting.

Using Ladders

- Use wooden or fiberglass ladders when you need to perform live working at heights.
- When a step ladder is used, ensure that the pull ropes are secured and the ladder is held firm.
- Before using a ladder, check that it is intact and confirm its load bearing capacity. Do not overload it.
- Ensure that the ladder is securely positioned. The recommended angle for a ladder against the floor is 75 degrees, as shown in the following figure. An angle rule can be used to measure the angle. Ensure that the wider end of the ladder is at the bottom, or protective measures have been taken at the bottom to prevent the ladder from sliding.



- When climbing a ladder, take the following precautions to reduce risks and ensure safety:
 - Keep your body steady.
 - Do not climb higher than the fourth rung of the ladder from the top.
 - Ensure that your body's center of gravity does not shift outside the legs of the ladder.

Drilling Holes

When drilling holes into a wall or floor, observe the following safety precautions:

NOTICE

Do not drill holes into the equipment. Doing so may affect the electromagnetic shielding of the equipment and damage components or cables inside. Metal shavings from drilling may short-circuit boards inside the equipment.

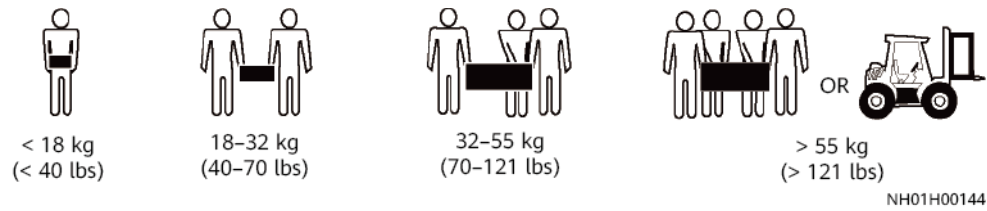
- Obtain consent from the customer and contractor before drilling holes.
- Wear goggles and protective gloves when drilling holes.
- When drilling holes, protect the equipment from shavings. After drilling, clean up any shavings that have accumulated inside or outside the equipment.

Moving Heavy Objects

DANGER

When pulling the equipment out of a cabinet, be aware of unstable or heavy objects on the cabinet to prevent injury.

- Be cautious to avoid injury when moving heavy objects.



- When moving the equipment by hand, wear protective gloves to prevent injuries.
- Move or lift the equipment by holding its handles or lower edges. Do not hold the handles of modules (such as power supply units, fans, and boards) that are installed in the equipment because they cannot support the weight of the equipment.
- Avoid scratching the cabinet surface or damaging cabinet components and cables during equipment transportation.
- When transporting the equipment using a forklift truck, ensure that the forks are properly positioned so that the equipment does not topple. Before moving the equipment, secure it to the forklift truck using ropes. When moving the equipment, assign dedicated personnel to take care of it.
- Choose a road with good conditions or sea for transportation to ensure equipment safety. Avoid tilt or jolt during transportation.
- Move the cabinet with caution. Any bumping or falling may damage the equipment.

1.6 Others

- Exercise caution when shutting down the smart cooling product. Doing so may cause equipment and room overheating, which will damage the equipment.
- Exercise caution when powering off the rPDU or PDU2000. Doing so may affect the power supply to equipment, which will interrupt services.
- Exercise caution when manually shutting down the UPS inverter for transferring to bypass mode, or when adjusting the UPS output voltage level or frequency. Doing so may affect the power supply to equipment.
- Exercise caution when setting battery parameters. Incorrect settings will affect the power supply and battery lifespan.
- To protect loads during UPS upgrade, set the output to maintenance bypass mode. To avoid load power failure or damage, ensure that the bypass input is within the specified power supply range.

2 Installation Preparations

2.1 Unpacking and Acceptance

Unpack and inspect all cabinets, mechanical parts, and components. Check that all the items are intact and comply with the packing list on the presence of both the project supervisor and customer.

Procedure

- Step 1** Unpack the carton labeled **Contain Packing List** and take out the *Packing List*.
- Step 2** Check all items against the *Packing List*.
- Step 3** If shortage or miscarriage occurs, fill in the *Cargo Shortage and Miscarriage Report*.
- Step 4** If cargo damage occurs, fill in the *Cargo Replacement Application Form*.
- Step 5** Sign on the *Packing List* with the customer after verifying that all required items are delivered.
- Step 6** Store the items properly.

----End

Follow-up Procedure

Put the items to be installed immediately onto an ESD surface, such as a polyethylene (PE) bag or an expandable polyethylene (EPE) foam. Pack the items not to be installed immediately with their original packing materials. Put them in a dry and cool environment without exposure to sunlight or electromagnetic radiation.

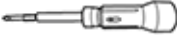
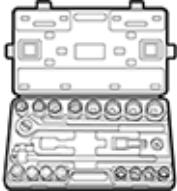
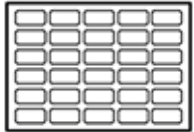
2.2 Tools and Instruments

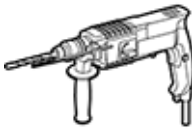
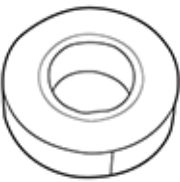
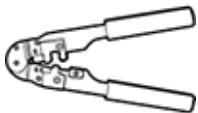
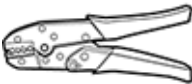
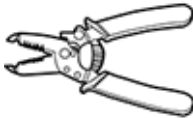
Before the installation, prepare the following common tools and transportation tools. Tools required vary with the actual installation scenarios.

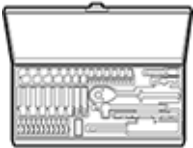
Common tools

Tools that are commonly used for onsite installation, such as tools for measuring dimensions, preparing cables, and fastening

Table 2-1 Common tools

Protective gloves 	Marker 	Measuring tape (5 m) 	Level 
Step ladder (2 m) 	Phillips screwdriver 	Phase sequence meter 	Flat-head screwdriver (2–5 mm) 
Adjustable wrench (6") 	Socket wrench M4/M6/M8/M12 	Hex key 	Box-end wrench M6/M8/M12 
Torque wrench (28 mm) 	Solid wrench (12#/13#/18#) 	Cotton cloth 	Label 

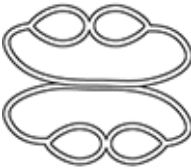
Electric screwdriver 	Hand drill (Φ3/Φ3.7/Φ4/Φ4.5/Φ5/Φ6/Φ10/Φ12 bit) 	Hammer drill (Φ16 bit) 	Heat gun 
Laser locator 	Utility knife 	Electrician's knife 	Impact tool 
Polyvinyl chloride (PVC) insulation tape 	Needle-nose pliers 	Diagonal pliers 	RJ11 crimping tool 
Crimping tool 	Wire stripper 	Hydraulic pliers 	Wire clippers 
Cable tie 	Multimeter 	Electroprobe 	Brush 
Claw hammer 	Vacuum cleaner 	Hacksaw 	Handsaw 

Right angle 	Heat shrink tubing 	Network cable tester 	Rubber mallet 
Adjustable socket screwdriver 	Flashlight 	Clamp meter 	-
NOTE This table may not list some tools required at specific sites. Onsite installation personnel and technical support personnel should prepare tools based on site requirements.			

Transportation Tools

Auxiliary tools used for transporting equipment

Table 2-2 Transportation and unpacking tools

Pallet truck 	Diesel forklift 	Lifting rope (bearing capacity ≥ 400 kg) 	Lever (bearing capacity ≥ 400 kg) 

2.3 Personnel Requirements

Only trained and qualified personnel who fully understand basic safety precautions are allowed to install and operate a Smart Module.

 **CAUTION**

Huawei will not be liable for any consequence caused by the violation of this document.

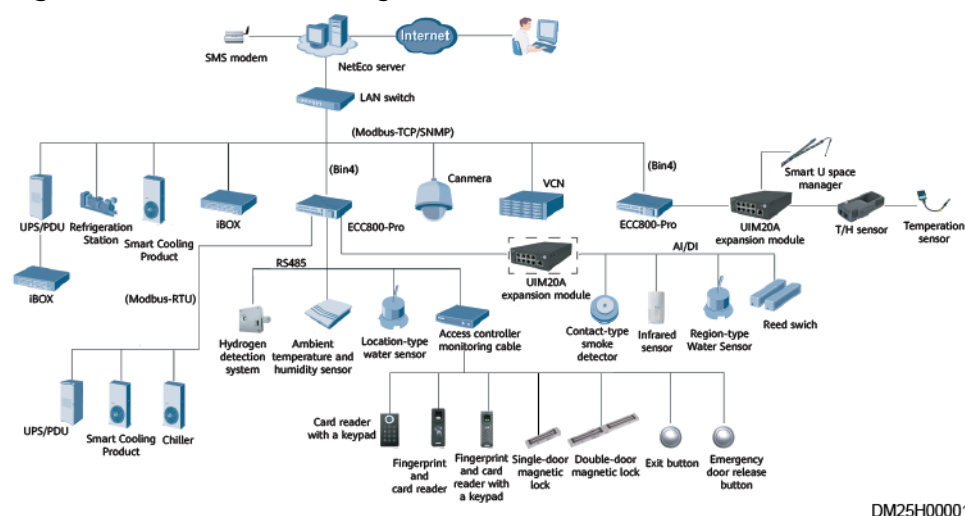
The requirements are as follows:

- Customers' installation personnel must be trained by Huawei and understand how to install and operate a Smart Module.
- The number of installation personnel varies depending on the project progress and the installation environment. Typically, three to five persons are required.

2.4 Device Networking Solution Overview

Figure 2-1 shows the iMaster NetEco device networking solution in the data center scenario.

Figure 2-1 Device networking solution



NOTE

When the number of AI/DI ports on the ECC800-Pro collector is insufficient, collect the device to the UIM20A expansion module.

2.5 Installation Process

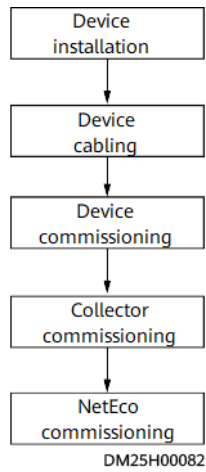
Figure 2-2 shows the process for installing and commissioning the iMaster NetEco devices.

Recommended installation sequence: **devices inside the cabinet** > **devices outside the cabinet** > **in-room devices**. You can adjust the installation sequence based on the site requirements.

NOTE

- The collector is ECC800-Pro.
- Ensure that the collector and the NetEco are installed in the same network segment.

Figure 2-2 Flowchart for the installation and commissioning of NetEco devices

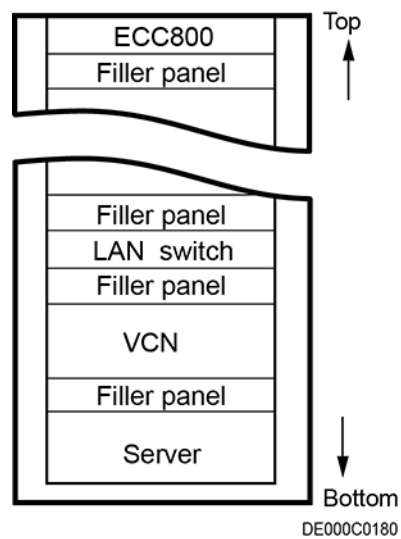


3 Installing Devices

3.1 Layout in the Network Cabinet

There are multiple types of monitoring components. Make installation plans based on the configurations. [Figure 3-1](#) shows the installation positions for some monitoring components for your reference.

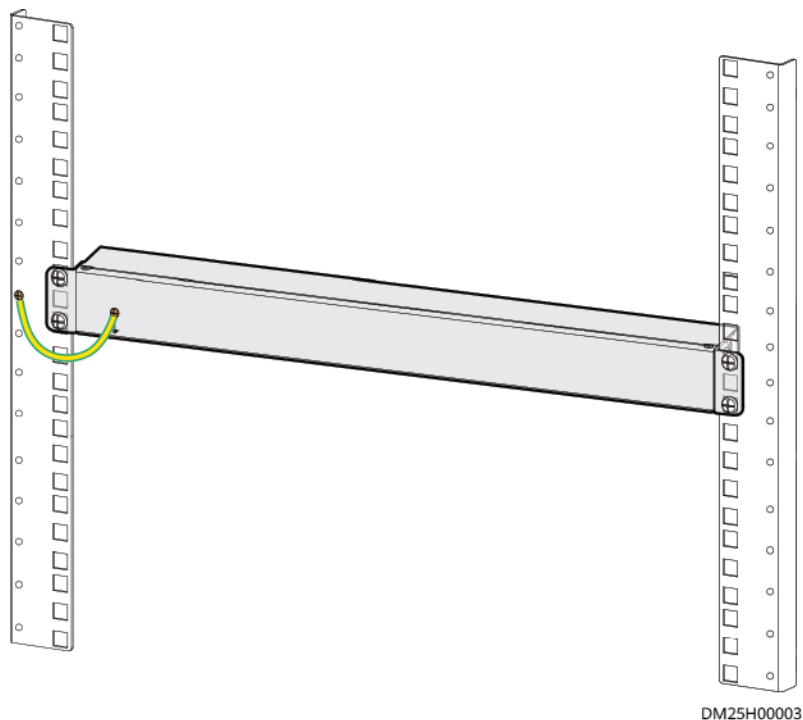
Figure 3-1 Device layout in the network cabinet



 NOTE

- Relocate the cable manager in the rear door position as high as the device to be installed.
- Use a flat-head screwdriver to insert floating nuts into the device mounting holes in the rack rails of the network cabinet. Ensure that the floating nuts on both sides are on the same horizontal line.
- Before connecting power cables for the device, use the ground cable delivered with the device to connect from the device ground point to the cabinet ground point close to the device mounting holes, as shown in [Figure 3-2](#). When there is a special grounding requirement and a cabinet ground bar can be deployed, use the ground cable prepared by the customer to connect from the device ground point to the cabinet ground bar.
- If no ground cable is delivered with the device, the customer needs to prepare the ground cable.

Figure 3-2 Connecting a device ground cable



3.2 Installing a Server

3.2.1 Installing a TaiShan 200 Server

Context

Tools: Phillips screwdriver, ESD wrist strap

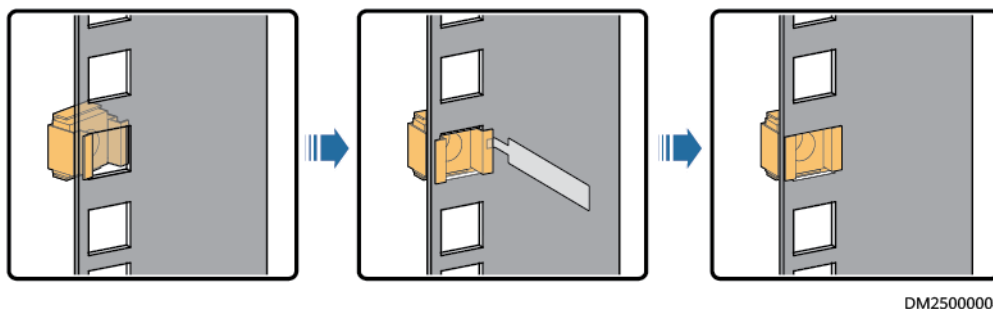
Materials: TaiShan 200 server, guide rail, rubber plug

Space required: 2 U

Procedure

- Step 1** Determine the installation position of the server and check whether floating nuts are installed. If not, install floating nuts.

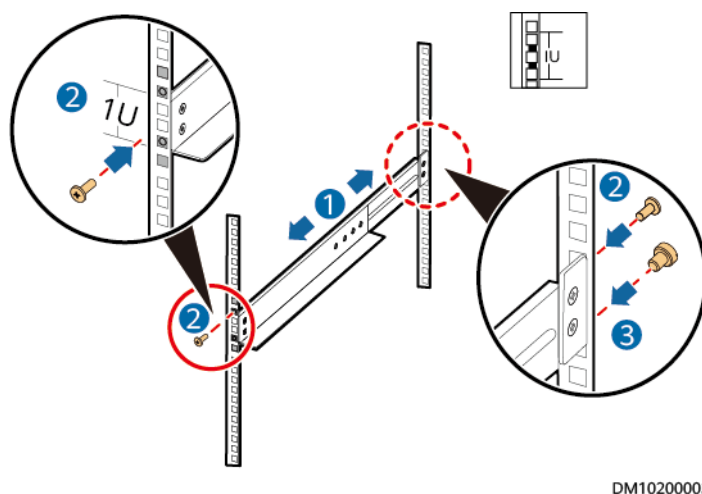
Figure 3-3 Installing floating nuts



- Step 2** Install L-shaped guide rails.

1. Place a guide rail horizontally in the planned position, and keep the guide rail in close contact with mounting bars.
2. Tighten the screws of the guide rail clockwise.

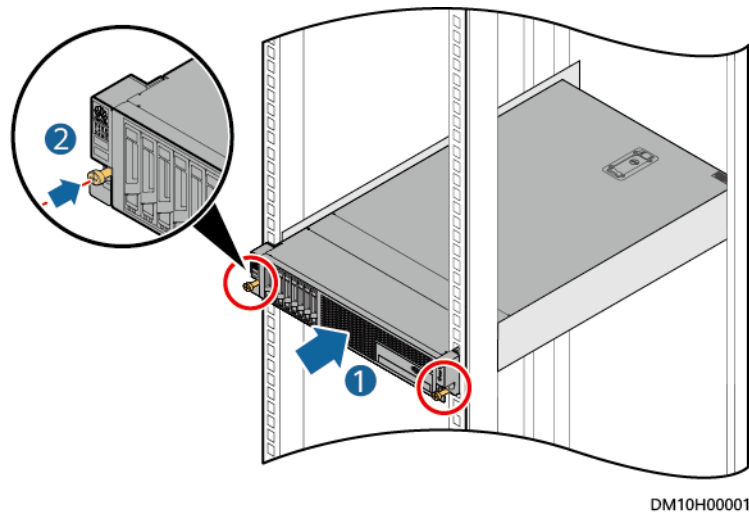
Figure 3-4 Installing a guide rail



- Step 3** Install the server.

1. Lift the server. This task requires at least two people.
2. Place the server on the guide rails and slide it into the cabinet. See (1) in [Figure 3-5](#).
3. When the two mounting ears of the server come into contact with the mounting bars on the cabinet, tighten their captive screws to secure the server. See (2) in [Figure 3-5](#).

Figure 3-5 Installing a server



Step 4 Connect the server power cables to the PDU.



WARNING

Wear an ESD wrist strap when connecting power cables.



NOTE

The server uses dual power supplies. Connect the two power cables to different PDUs.

----End

3.2.2 Installing a 2288X V5 Server

Context

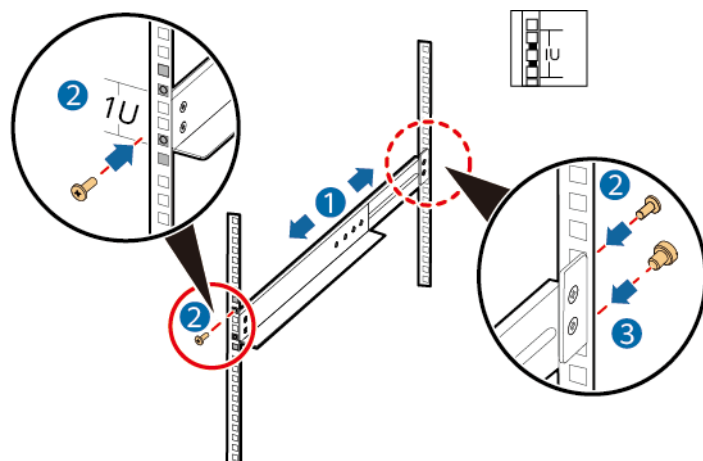
Tool: Phillips screwdriver

Materials: 2288X V5 server, guide rail, rubber plug, screw

Procedure

Step 1 Install guide rails.

Figure 3-6 Installing a guide rail



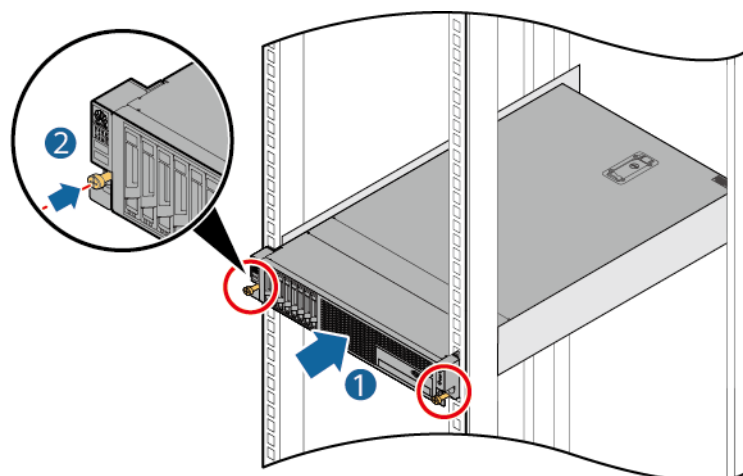
DM10200003

1. Place a guide rail horizontally at the installation position in the cabinet.
2. Fix the guide rail using rubber plugs.
 - a. In front of the guide rails: If a server is installed using the upper mounting holes, insert rubber plugs tightly into the holes at the middle. If a server is installed using mounting holes at the middle, insert rubber plugs tightly into the upper holes.
 - b. Behind the guide rails: Insert rubber plugs tightly into the upper mounting holes.
3. (Optional) To enhance the rigidity and seismic-proof performance of a server, you can install bolts at the rear of flexible guide rails.

Step 2 Place the server on the guide rails and slide it along the guide rails into the cabinet.

Step 3 Align the two mounting ears of the server with the mounting bars of the cabinet and tighten the screws on the mounting ears.

Figure 3-7 Installing a server



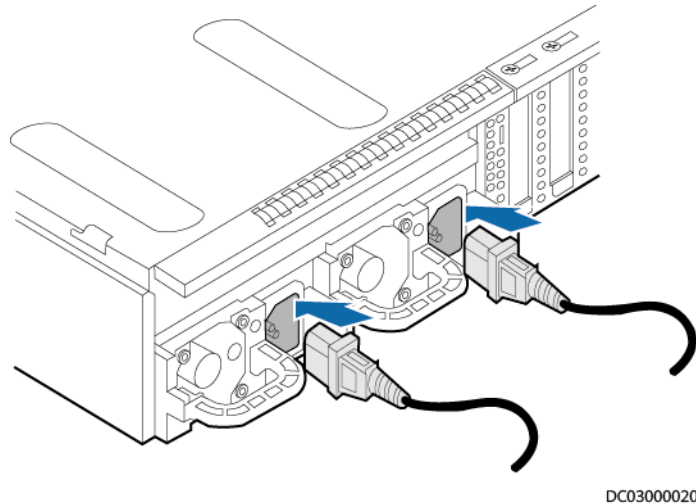
DM10H00001

Step 4 Connect the server power cables to the PDU2000.

 NOTE

The server uses dual power supplies. Connect the two power cables to different PDU2000s.

Figure 3-8 Connecting server power cables



----End

3.3 Installing a LAN Switch

Procedure

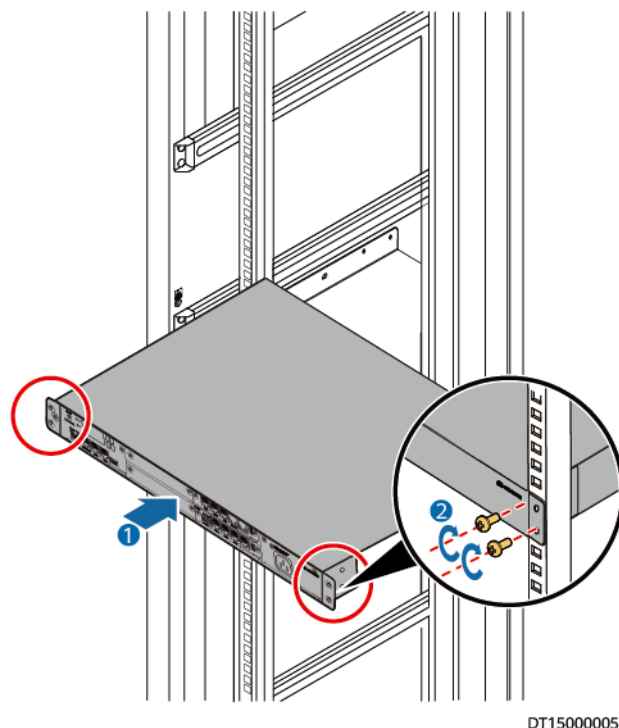
Step 1 Determine the mounting holes for the LAN switch based on the network cabinet device layout, adjust the guide rails or trays, and install floating nuts.

Step 2 Install the mounting ears delivered with the LAN switch and secure the LAN switch to the mounting bars in the front of the cabinet.

 NOTE

This section describes only the installation method. The actual product appearance prevails.

Figure 3-9 Installing a LAN switch



Step 3 Connect the LAN switch power cable to the PDU2000.

NOTE

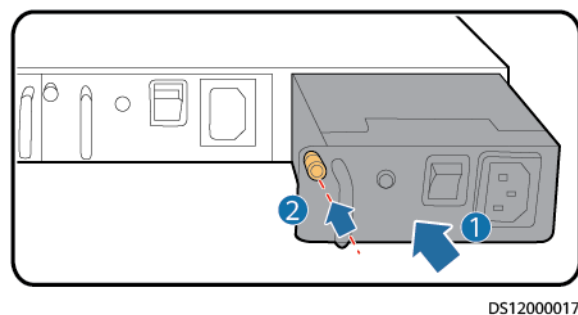
The positions of power cable ports vary depending on the LAN switch models. Connect the power cable based on the actual power port of the LAN switch.

----End

Follow-up Procedure

If a 24-port LAN switch is configured, one or two power modules need to be installed for the LAN switch onsite. Insert the power module into the power slot of the 24-port LAN switch and tighten the captive screws on the power module panel.

Figure 3-10 Installing a power module for a 24-port LAN switch

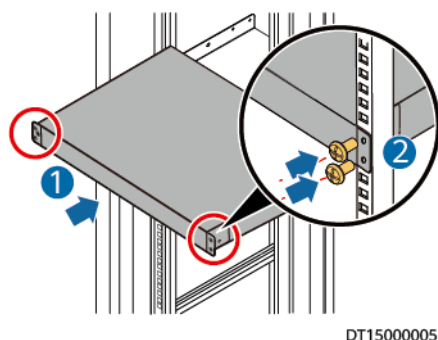


3.4 Installing an ECC800-Pro Collector

Procedure

- Step 1** Determine the mounting holes for the ECC800-Pro collector in the network cabinet based on the engineering layout diagram, adjust the guide rails or trays, and install floating nuts.
- Step 2** Gently put the ECC800-Pro collector into the network cabinet.
- Step 3** Secure the ECC800-Pro collector in the network cabinet by clockwise tightening the M6 screws on the left and right mounting ears.

Figure 3-11 Installing an ECC800-Pro collector



- Step 4** Connect the ECC800-Pro collector power cable to the PDU2000.

----End

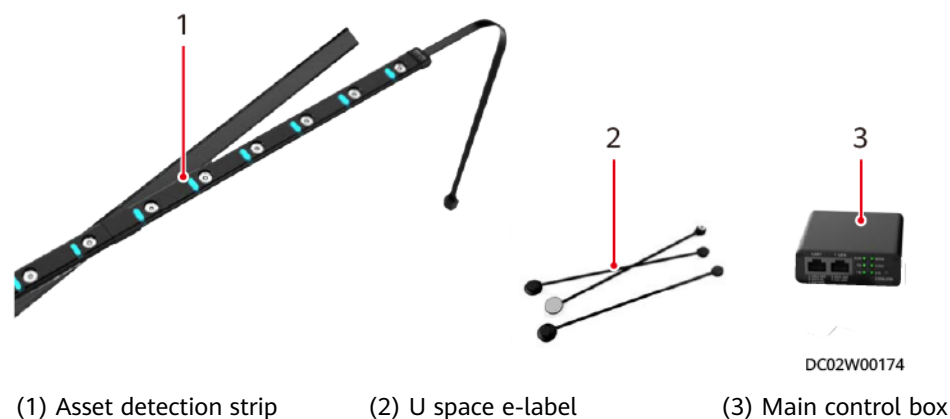
3.5 Installing a Smart U Space Manager (BOM Number: 52273314)

Context

The BOM number of the U space e-label for the smart U space manager is 52273315.

The smart U space manager consists of the following components.

Figure 3-12 Smart U space manager appearance



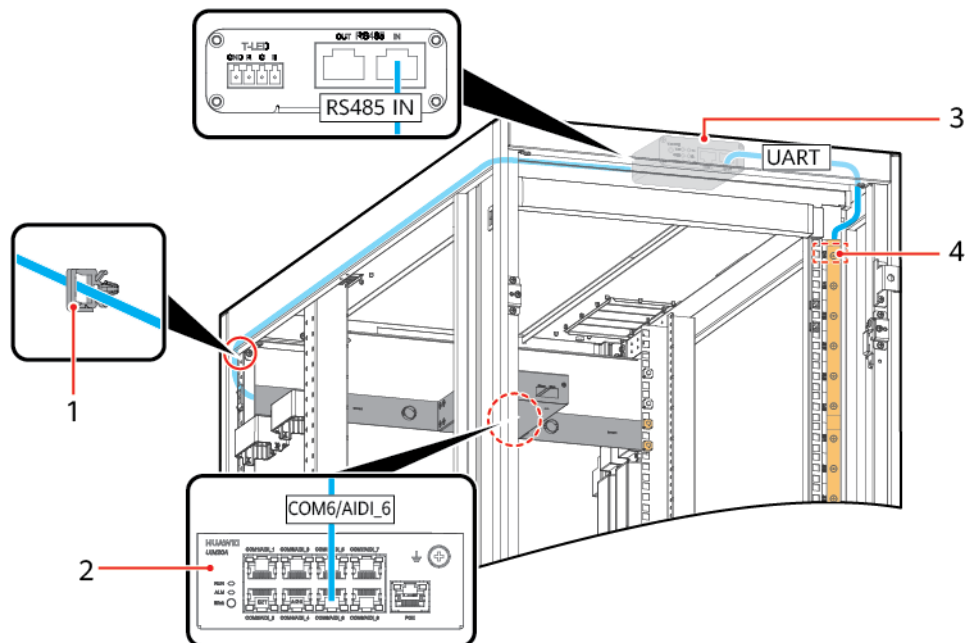
Procedure

- Step 1** Align the first detection point of the asset detection strip with the cabinet 42 U position and attach it to the rack.
- Step 2** Attach the main control box to the top of the cabinet front door interior (if there is space at the top of the cabinet interior) or exterior (if there is no space at the top of the cabinet interior).
- Step 3** Connect cables between devices and secure the cables using fasteners.

NOTE

- The securing positions of fasteners are for reference only. The actual mounting holes on the cabinets are used.
- The cable between the main control box and the UIM20A expansion module unit is delivered with the smart U space manager.
- Attach the U space e-label to the detection point on the asset detection strip, facilitating asset management.
- In a standard scenario of one-to-one connection through an expansion module, connect a smart U space manager to the COM6/AIDI_6 port on the UIM20A expansion module.
- In a scenario where one UIM20A expansion module maps to four cabinets, connect smart U space managers to the COM1/AIDI_1, COM3/AIDI_3, COM5/AIDI_5, and COM7/AIDI_7 ports on the UIM20A expansion module. If the number of IT cabinets is not an integer multiple of 4, according to the cable connection rules, redundant COM ports exist on the UIM20A expansion module.

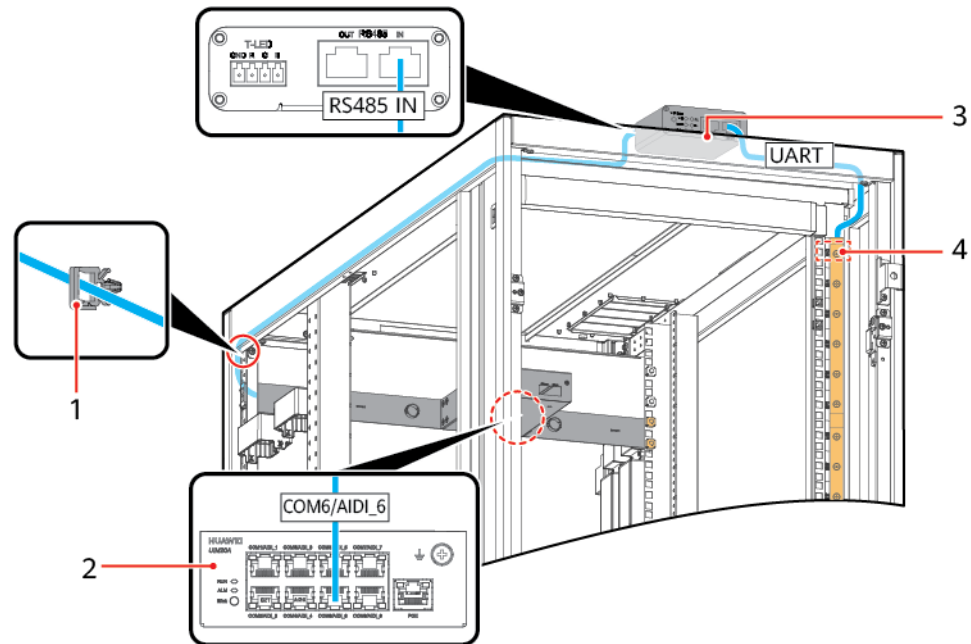
Figure 3-13 Installing a smart U space manager (main control box attached to the top of the cabinet interior)



DF17110003

- (1) Fastener (2) UIM20A expansion module (3) Main control box
(4) Asset detection strip (42 U - detection point) -

Figure 3-14 Installing a smart U space manager (main control box attached to the top of the cabinet exterior)



DF17110004

- (1) Fastener (2) UIM20A expansion module (3) Main control box
(4) Asset detection strip (42 U - detection point) -

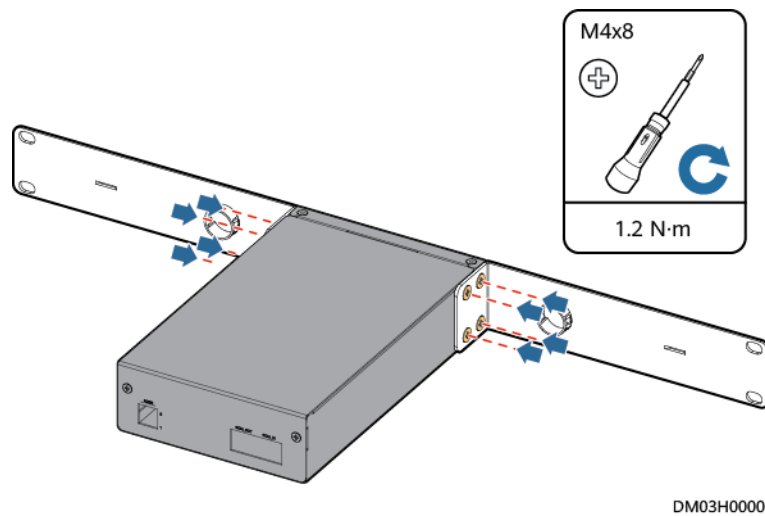
-----End

3.6 Installing a UIM20A Expansion Module

Procedure

- Step 1** Secure a mounting ear to each of the two sides of the UIM20A expansion module using four M4 screws.

Figure 3-15 Installing mounting ears

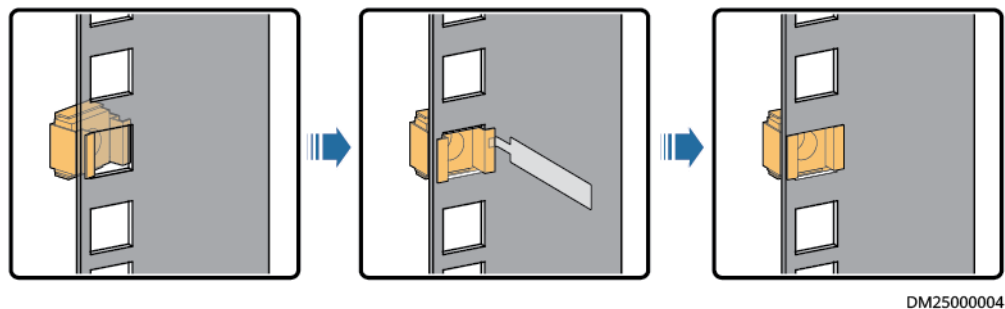


Step 2 Determine the mounting holes for the UIM20A expansion module in a cabinet based on the engineering layout diagram, and install floating nuts.

NOTE

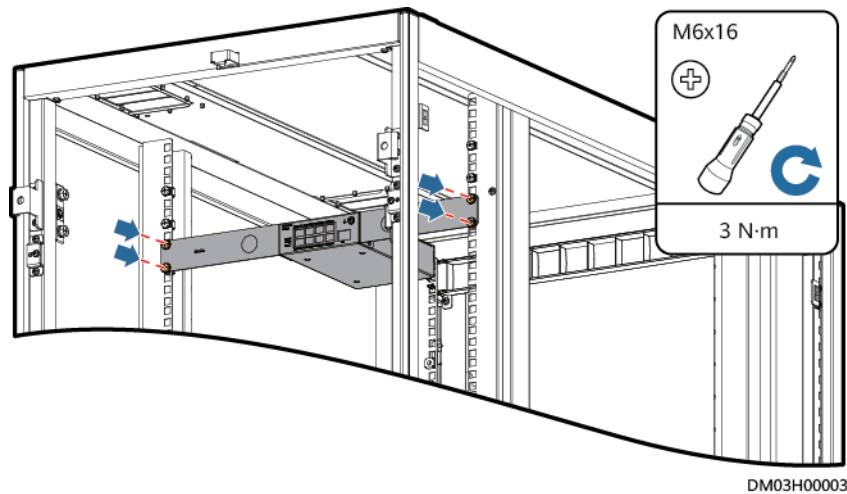
Recommended installation position: The third U space from the top to the bottom at the rear of the cabinet.

Figure 3-16 Installing floating nuts



Step 3 Secure the UIM20A expansion module to the cabinet by tightening the M6 screws on the left and right mounting ears clockwise.

Figure 3-17 Installing a UIM20A expansion module



----End

3.7 Installing Sensors

3.7.1 Installing Cabinet Temperature Sensors

Context

- The BOM number of the temperature sensor is 33010557, including two temperature sensor cables and one extension cable. Each temperature sensor cable contains three NTCs.
- Install temperature sensors in the IT cabinet and network cabinet.

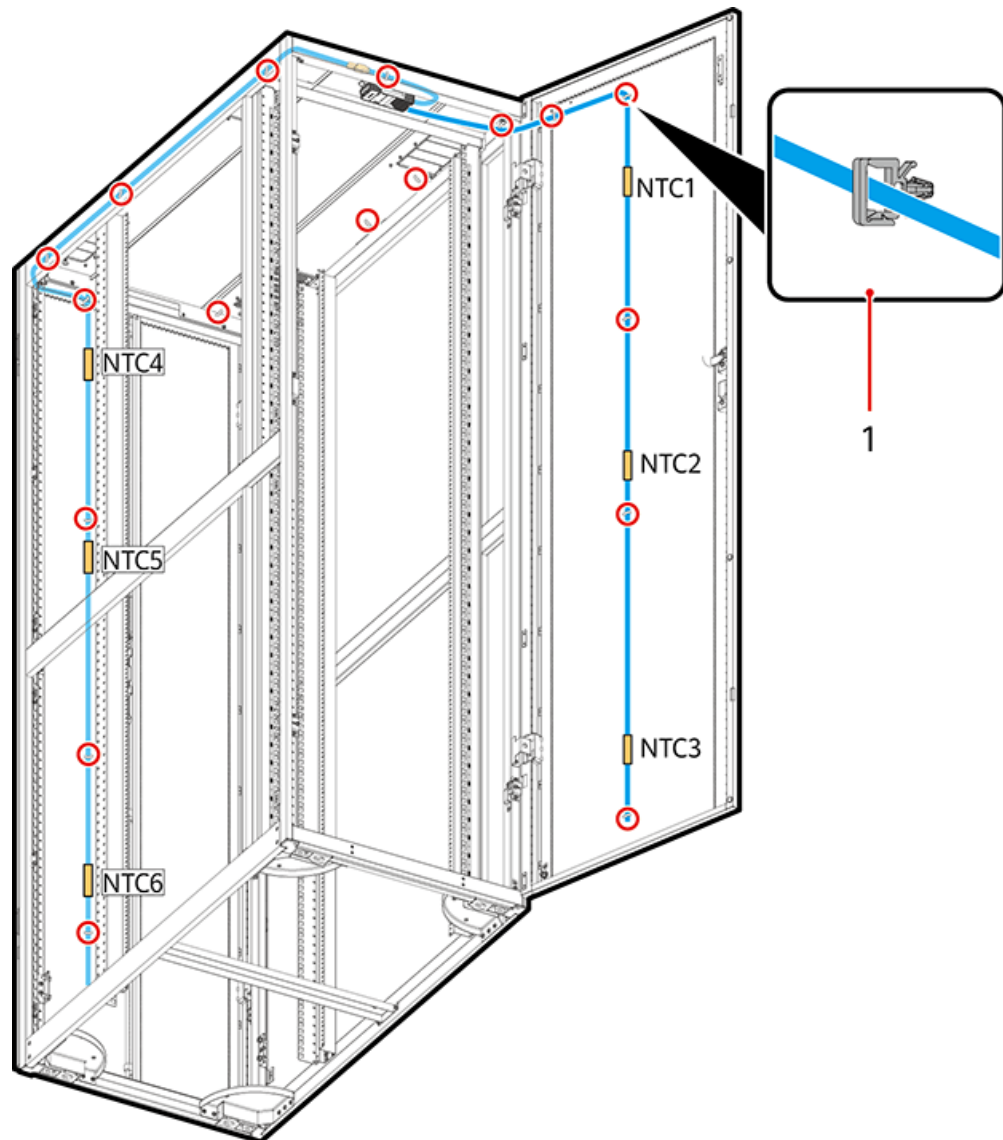
Procedure

- Step 1** Secure temperature sensors to the corresponding cabinet.
- Step 2** Route the extension cable through the sponge strips between the rack rail and side panel, and secure the cable.
- Step 3** Connect one end of the extension cable to the temperature sensor on the front door.
- Step 4** Connect the other end of the extension cable and the temperature sensor on the rear door to the T/H sensor.
- Step 5** Bind the cables with fasteners.

NOTE

- The securing positions of fasteners are for reference only. The actual mounting holes on the cabinets prevail.
- The temperature sensor is installed in the middle of the cabinet door and is vertical from top to bottom after installation.
- NTC1–NTC3 of the T/H sensor must be placed in the cold air area, and NTC4–NTC46 must be placed in the hot air area.

Figure 3-18 Installing temperature sensors



DF03110002

(1) Fastener

----End

3.7.2 Installing a Hydrogen Sensor

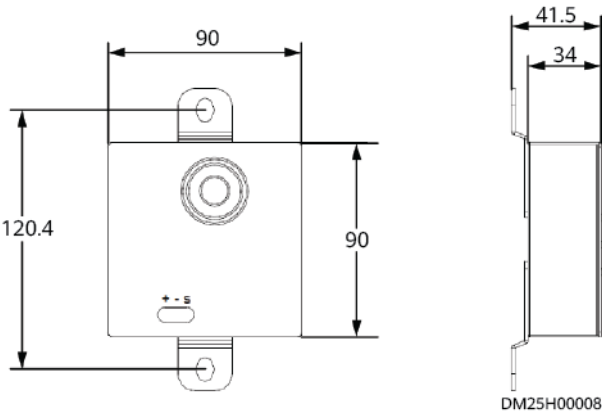
Context

- A hydrogen sensor is used to detect the hydrogen density indoors. It works with the hydrogen detection system.
- The hydrogen detection system is installed on the ceiling of the area to be detected.

Procedure

- Step 1** Install two expansion bolts (M6x60) at the specified positions, align the two mounting ears of the hydrogen sensor with the expansion bolts, and tighten the M6 nuts.

Figure 3-19 Installing a hydrogen sensor (unit: mm)

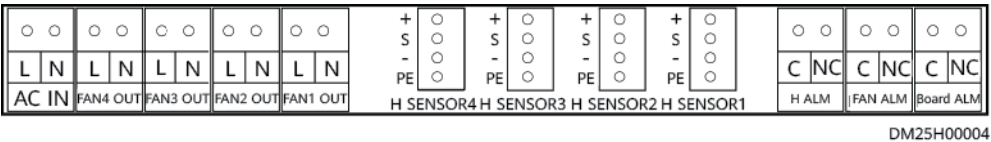


- Step 2** Connect the power cable of the hydrogen sensor to + and - of the hydrogen detection system, connect the signal cable to **S**, and connect the shell to the **PE** cable.

NOTE

Pay attention to the negative and positive polarities of the power supply. If the polarities are connected incorrectly, the device may be burned.

Figure 3-20 Connecting cables



----End

3.7.3 Installing the Hydrogen Detection System

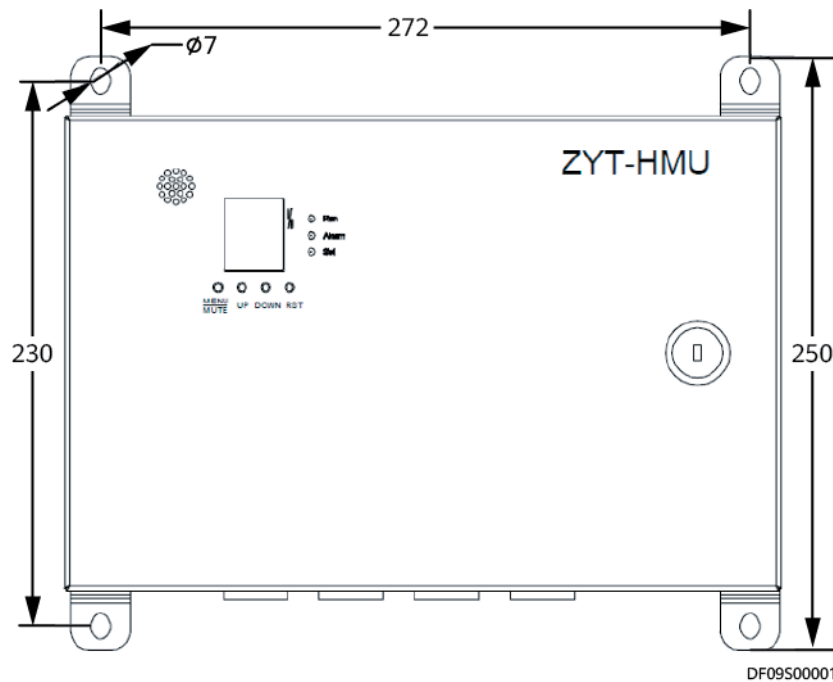
Context

- The hydrogen detection system is used to detect the hydrogen density indoors. When the hydrogen density exceeds the alarm threshold, the system generates alarms.
- The hydrogen detection system is installed on the interior wall of the area to be detected.

Procedure

- Step 1** Install four expansion bolts (M6x60) to the specified positions, align the four mounting ears of the hydrogen detection system with the expansion bolts, and tighten the M6 nuts.

Figure 3-21 Installing a hydrogen detection system (unit: mm)

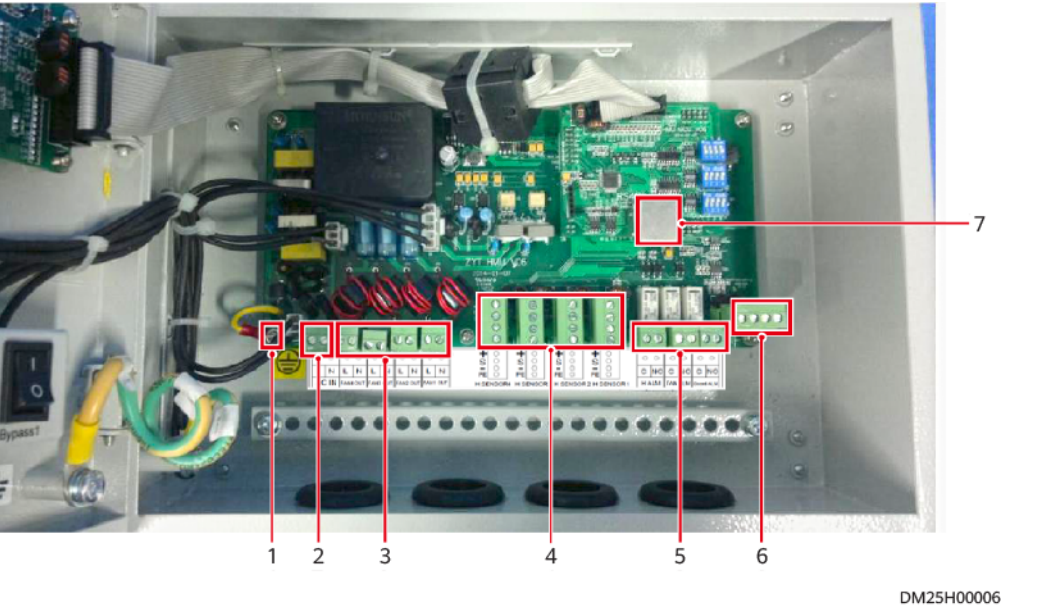


- Step 2** According to the silk screen and [Figure 3-22](#), connect the ground cable to (1), input power cable to (2), fan cables to (3), and hydrogen sensor cables to (4).
- Step 3** Prepare one end of a network cable according to [Table 3-1](#), and connect the cable to (7).

⚠ DANGER

Pay attention to the negative and positive polarities of the power supply. If the polarities are connected incorrectly, the device may be burned.

Figure 3-22 Connecting cables



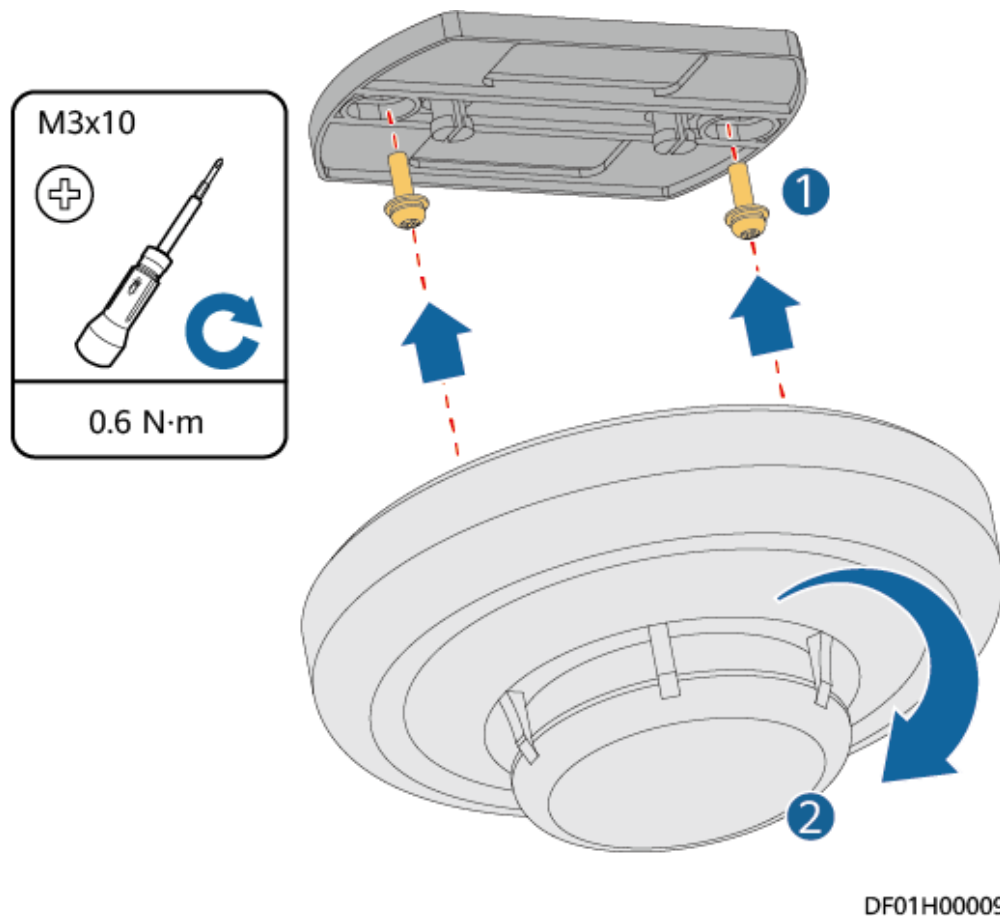
- (1) PE
- (2) AC IN
- (3) Output ports for fan 1 to fan 4
- (4) Output ports for hydrogen sensor 1 to hydrogen sensor 4
- (5) Hydrogen concentration and alarm port, fan alarm port, and idle ports (reserved ports)
- (6) RS485+, RS485-, GND, and idle ports (reserved ports)
- (7) RS485 port
-
-

Table 3-1 Pin mapping for the RS485 port

Pin	Signal	Function
Pin 1 (orange-white)	D+	RS485+
Pin 2 (orange)	D-	RS485-
Pin 3 (green-white)	12V+	12+ input
Pin 4 (blue)	NC	-
Pin 5 (blue-white)	NC	-
Pin 6 (green)	NC	-
Pin 7 (brown-white)	NC	-
Pin 8 (brown)	12V-	12- input

----End

Figure 3-24 Installing a smoke detector



Step 3 Align the mounting holes in the smoke detector with its base, and then rotate the smoke detector until it is secured.

----End

3.7.5 Installing a Temperature and Humidity Sensor (BOM Number: 33010346)

Prerequisites

A temperature and humidity sensor (BOM number: 33010346) and tools for installing it have been prepared.

Context

- For details about how to install an ambient temperature and humidity sensor and connect its cables, see shipped documents.
- Connect cables to an ambient temperature and humidity sensor before installation.

Preparations

Tool: Phillips screwdriver

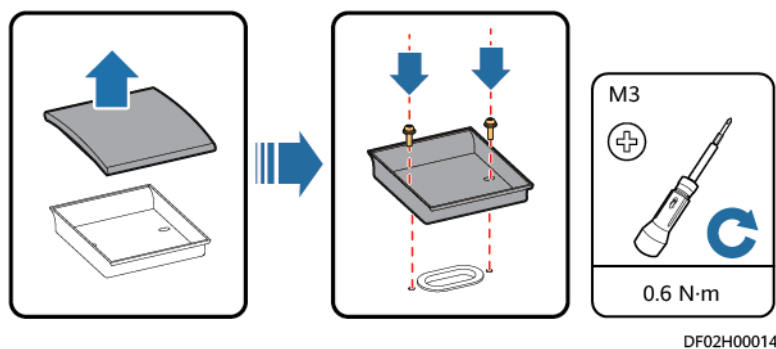
Materials: temperature and humidity sensor, temperature and humidity sensor base

Document: temperature and humidity sensor installation position diagram

Procedure

- Step 1** Remove the front cover from the temperature and humidity sensor.
- Step 2** Install the ambient temperature and humidity sensor to the position specified on the wall, and secure it using bolts.
- Step 3** Reinstall the front cover for the temperature and humidity sensor.

Figure 3-25 Installing the temperature and humidity sensor



----End

3.7.6 Installing a Temperature and Humidity Sensor (BOM Number: 02312PBL)

Prerequisites

A temperature and humidity sensor (BOM number: 02312PBL) and tools for installing it have been prepared.

Context

- For details about how to install an ambient temperature and humidity sensor and connect its cables, see shipped documents.
- Connect cables to an ambient temperature and humidity sensor before installation.

Preparations

Tool: Phillips screwdriver

Materials: temperature and humidity sensor, temperature and humidity sensor base

Document: temperature and humidity sensor installation position diagram

Procedure

Step 1 Install the T/H sensor base at the right column position of the IT cabinet about 1.6 m high above the floor in the aisle, and then clamp the T/H sensor onto the base.

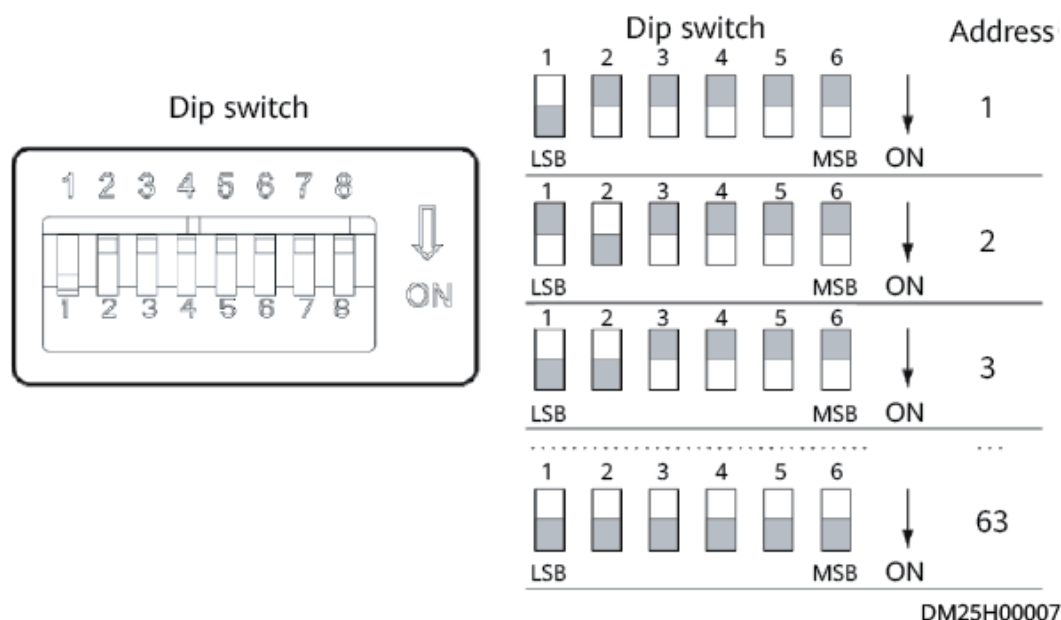
Step 2 Set device addresses for the T/H sensors.

Set the device address for a T/H sensor by operating the DIP switch on the sensor. Toggle switches 1–6 are used to set the device address, toggle switch 7 is reserved, and toggle switch 8 is used to switch the temperature display mode. The device address is set in binary coding format in the range of 1–63. The first bit is the least significant, and the sixth bit is the most significant. ON indicates 1 and OFF indicates 0. The address range is 1–63.

NOTE

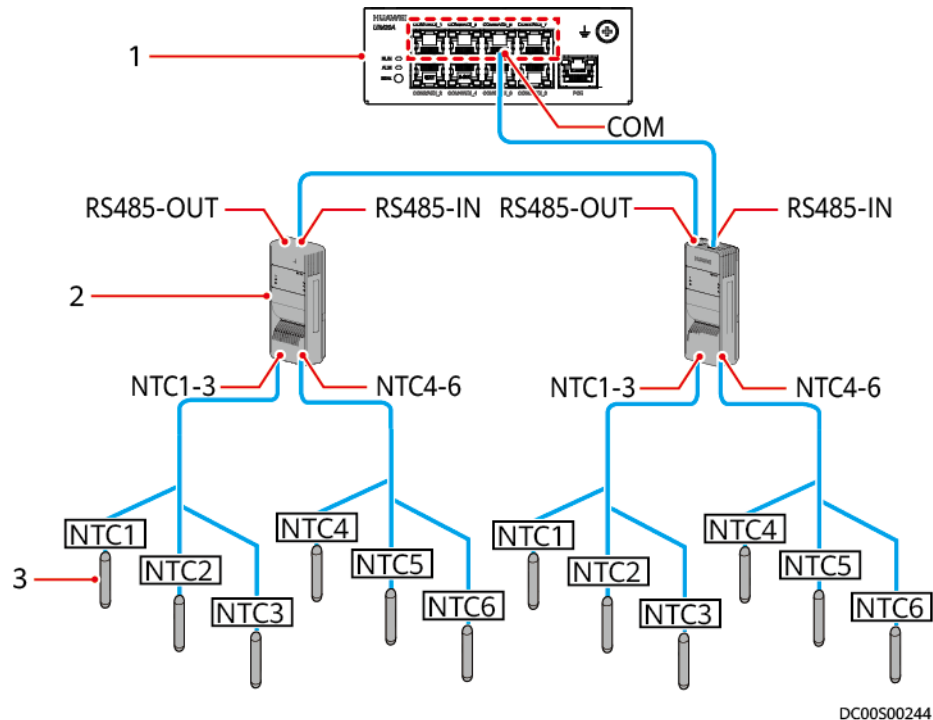
The numbers indicate the DIP switch settings of the T/H sensors.

Figure 3-26 DIP switch settings for T/H sensors



Step 3 Connect the communications cables to the T/H sensors.

Figure 3-27 Cable connections to T/H sensors



(1) UIM20A expansion module (2) T/H sensor

(3) NTC sensor

DC00S00244

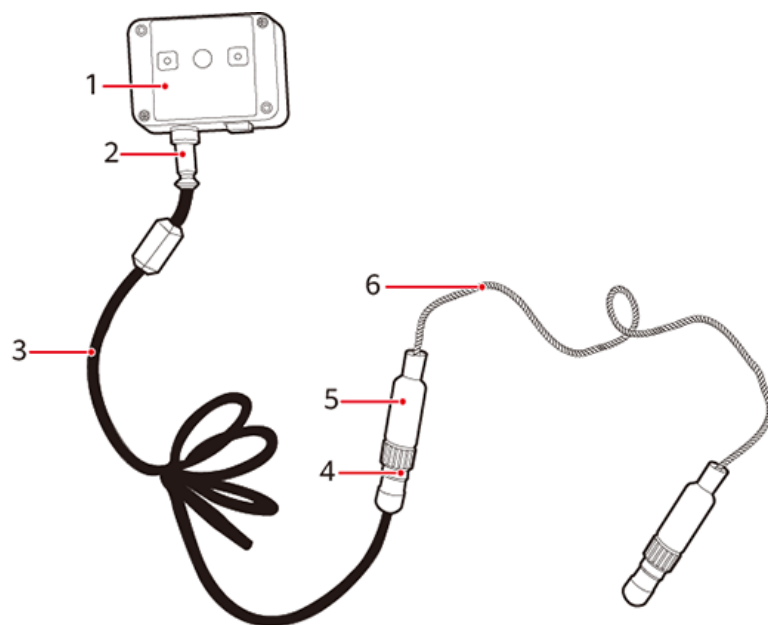
-----End

3.7.7 Installing a Region-type Water Sensor

Context

A water sensor consists of a water detection cable, water detector, and conversion cable. The water detection cable is laid out on the floor, connecting to the water detector placed near the collector by the conversion cable.

Figure 3-28 Water sensor components

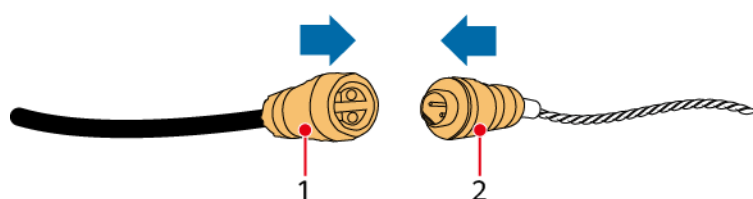


(1) Water detector	(2) Conversion cable end A, connecting to the water detector	(3) Conversion cable
(4) Conversion cable end B, connecting to the water detection cable	(5) Water detection cable end A, connecting to the conversion cable	(6) Water detection cable

Procedure

- Step 1** Install the water detector near the collector and secure it using screws or other methods.
- Step 2** Connect the water detection cable to the conversion cable.

Figure 3-29 Connecting the water detection cable to the conversion cable



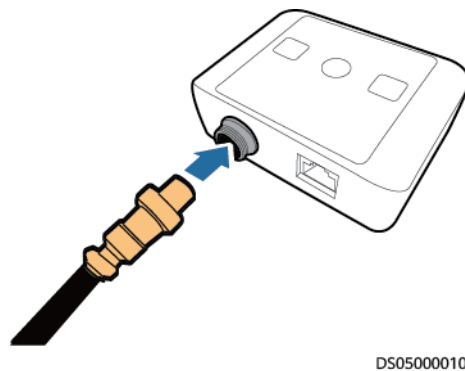
(1) Conversion cable end B, connecting to the water detection cable	(2) Water detection cable end A, connecting to the conversion cable

NOTE

The water detection cable and conversion cable are interconnected through the male and female connectors.

- Step 3** Connect the other end of the conversion cable to the water detector.

Figure 3-30 Connecting the water detector



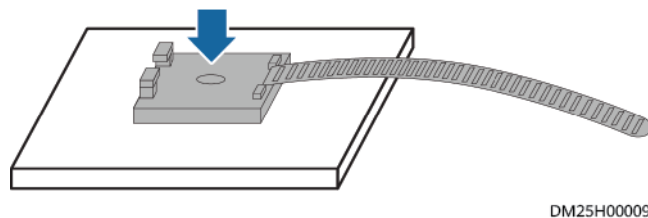
- Step 4** Plan the installation position for the fastener of the water detection cable. Ensure that the water detection cable placed on the fastener is in good contact with the floor.

NOTICE

Do not contact the water detection cable to metal, for this action will cause a false alarm. Take protective measures when routing a water detection cable.

- Step 5** Tear off the protection paper on the rear of the fastener, then securely attach the fastener to the floor.

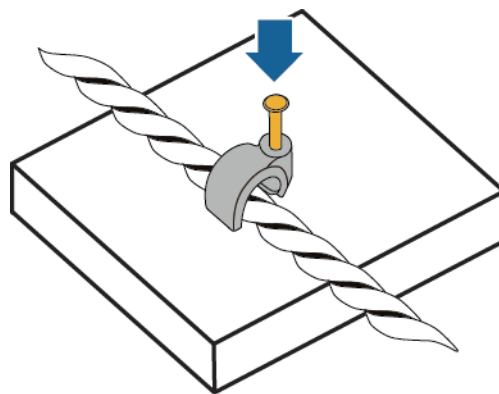
Figure 3-31 Installing a fastener



NOTE

- One fastener is provided for a 1 m long water detection cable.
- When securing the water detection cable to the concrete floor, use the cable nail clips delivered with the cable to secure the cable.

Figure 3-32 Installing a cable nail clip



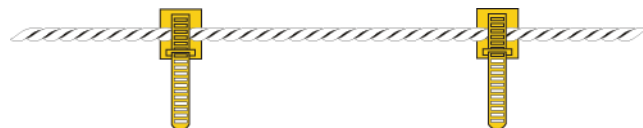
DF05H00001

NOTICE

- When laying out the water detection cable, ensure that the water detector is close to the planned position for the network cabinet to facilitate further cable connections.
- The water detection cable should not be laid out near air exhaust vents of smart cooling products. If unavoidable, take measures to prevent condensation.

Step 6 Place the water detection cable onto the fastener, secure the fastener, and keep the water detection cable in close contact with the floor.

Figure 3-33 Securing a water detection cable



DS05000009

NOTE

If multiple water detection cables need to be connected in series, connect the male connector of one cable to the female connector of another cable.

----End

3.7.8 Installing a Location-type Water Sensor

Context

- The location-type water sensor is installed on a 35 mm DIN guide rail and can be installed on the wall around the detected area.
- Install water detection cables surrounding the water leakage area.
- To avoid damaging the water sensor, do not unpack it until right before installation.

Procedure

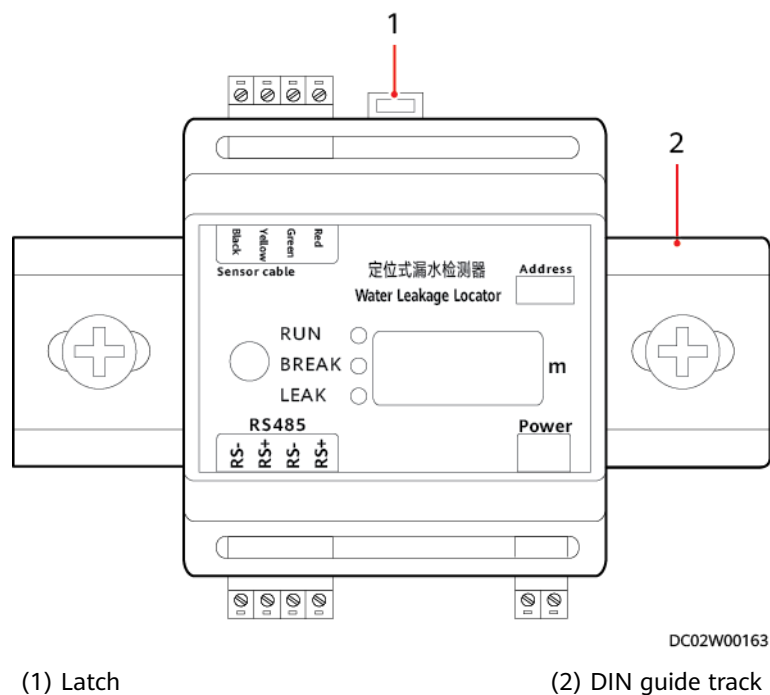
Step 1 Fix a proper length of DIN guide rail to the wall around the detected area.

Step 2 Unpack the location-type water sensor, buckle the module to the DIN guide rail, and ensure that the latch faces upwards during installation.

NOTE

- The water leakage locator should be installed within 1200 meters of the control host.
- The installation height must not exceed 1.5 m. Ensure that the water detection rope is no higher than the ground.
- Hand-write the address in the address blank area.

Figure 3-34 Installation diagram

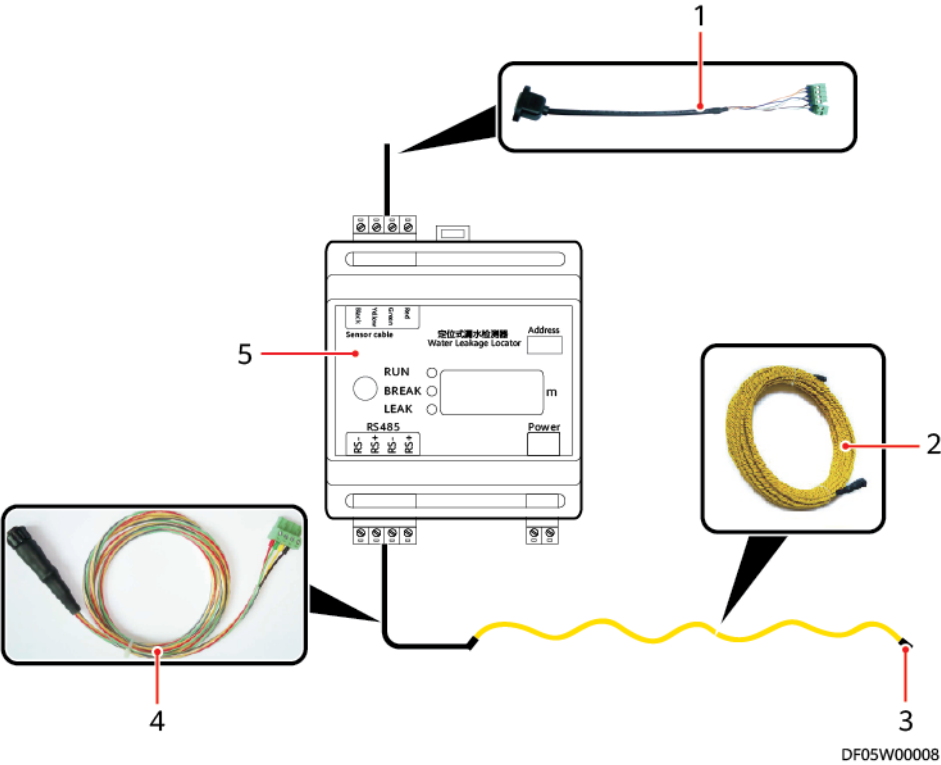


NOTE

- Touch grounded devices or pipes to eliminate ESD before taking the location-type water sensor module.
- Place it gently. Protect it against mechanical impact and collision. Keep it dry.
- Prevent it against metal filings, grease, pipe paint, and other contaminants.

Step 3 The location-type water sensor consists of a water leakage locator, tieline, and water leakage location cable, the connection diagram is as follows.

Figure 3-35 Connection diagram for location-type water sensor components



- (1) Tie line
- (2) Water leakage location cable
- (3) Terminal
- (4) Extension line
- (5) Water leakage locator
-

NOTE

- Two types (A and B) of end caps are delivered in early stage. The site may support only one type. In the later delivery, there is only one type supported, that is, type A and type B are not distinguished any more.
- If there are two types (A and B) delivered with the product, select either of the types to complete cable connection. After the cable is connected and the water leakage locator is powered on and initialized, if the buzzer keeps buzzing and the alarm location is a stable value that is greater than the total length of the water leakage location cable, replace the end cap with the other end cap.

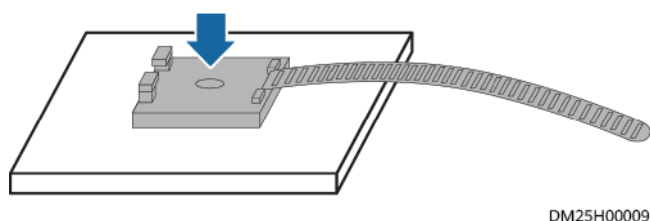
Table 3-2 RJ45 cable wire sequence of the Tie line

Pin	Definition
Pin 1 (orange-and-white)	RS485+
Pin 2 (orange)	RS485-
Pin 3 (green-and-white)	12VDC
Pin 4 (blue)	RS485+
Pin 5 (blue-and-white)	RS485-
Pin 6 (green)	-

Pin	Definition
Pin 7 (brown-and-white)	-
Pin 8 (brown)	GND

- Step 4** Tear off the protection paper on the rear of the fastener, then securely attach the fastener to the floor.

Figure 3-36 Installing a fastener

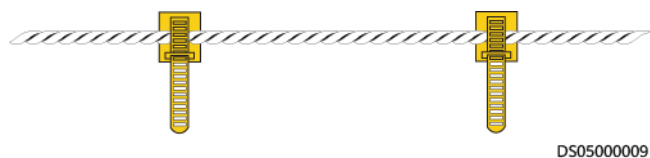


NOTE

15 fasteners are furnished with the device.

- Step 5** Place the water detection cable onto the fastener, secure the fastener, and keep the water detection cable in close contact with the floor.

Figure 3-37 Securing a water detection cable



----End

3.7.9 Installing an Infrared Sensor

Prerequisites

An infrared sensor and installation tools are available.

Context

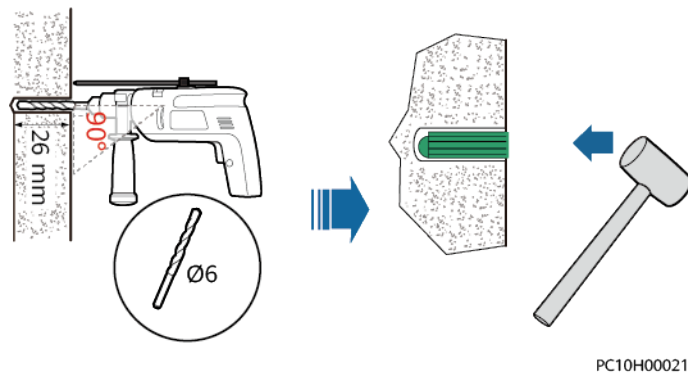
- The infrared sensor is used to monitor the entry status of people in the equipment room.
- The infrared sensor is installed on the wall in the detection area.

Procedure

- Step 1** Take out the infrared sensor base and mark the mounting hole for the base in an appropriate area.

Step 2 Drill a hole and install an expansion sleeve, as shown in [Figure 3-38](#).

Figure 3-38 Drilling a hole and installing an expansion sleeve



Step 3 Install the infrared sensor base on the wall.

Step 4 Secure the infrared sensor to the base, as shown in [Figure 3-39](#) or [Figure 3-40](#).

NOTE

Install the infrared sensor in an appropriate way based on the shape of the base.

Figure 3-39 Installing an infrared sensor (method 1)

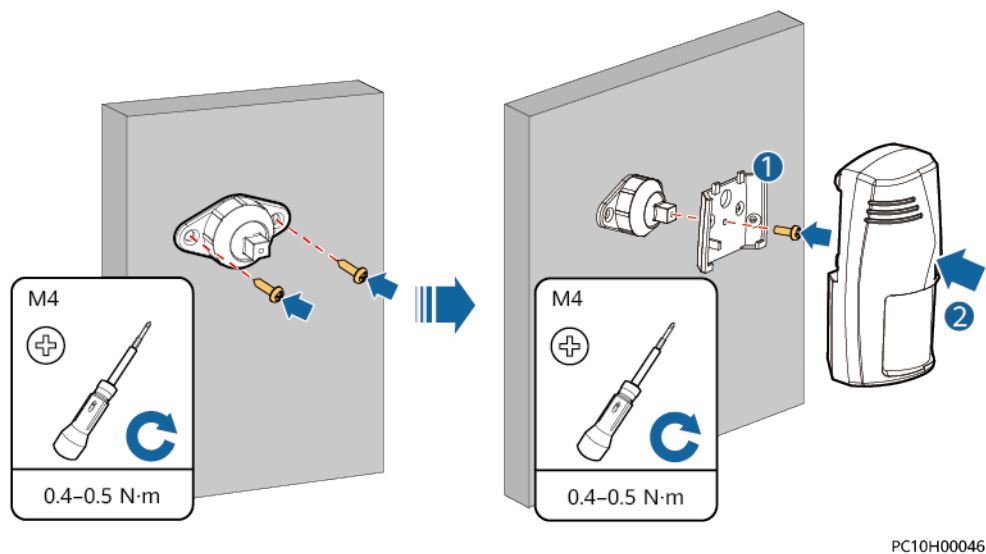
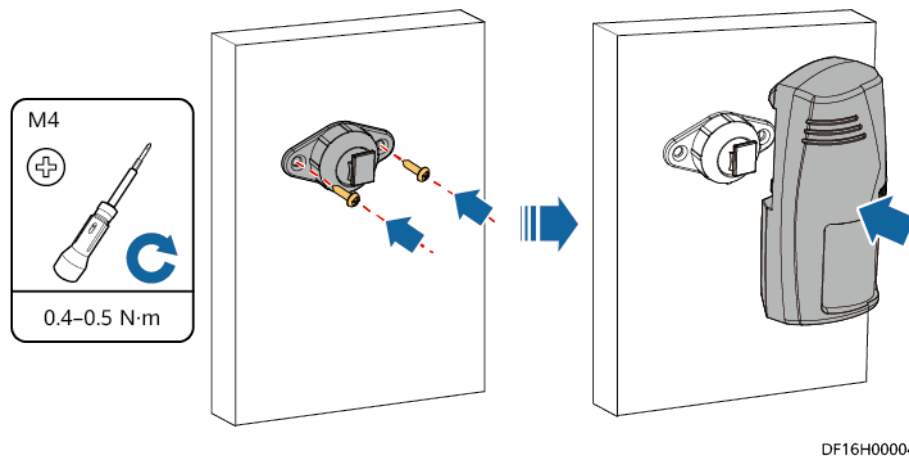


Figure 3-40 Installing an infrared sensor (method 2)



Step 5 Loosen the support on the base, adjust the sensor angle so that the sensor can cover the target area, and then tighten the support.

----End

3.8 Installing the Video Management System

3.8.1 Installing the VCN510

Context

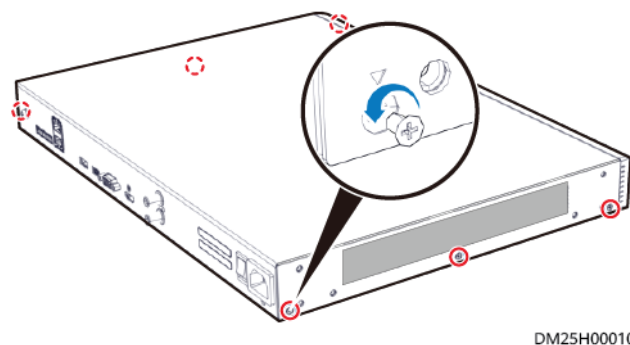
The VCN510 does not carry disks when being delivered. First install disks and then install the device in a network cabinet.

Procedure

Step 1 Install a hard disk.

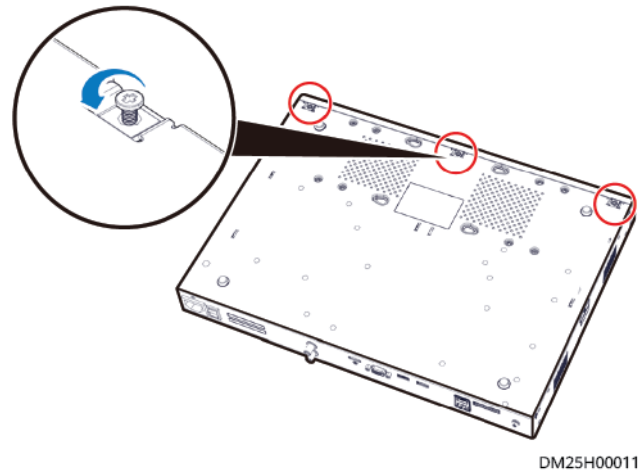
1. Use a Phillips screwdriver to loosen three fastening screws (M3 x 6 countersunk screw, black) on the left and right of the subrack covers shown in the lower-left figure.

Figure 3-41 Removing screws



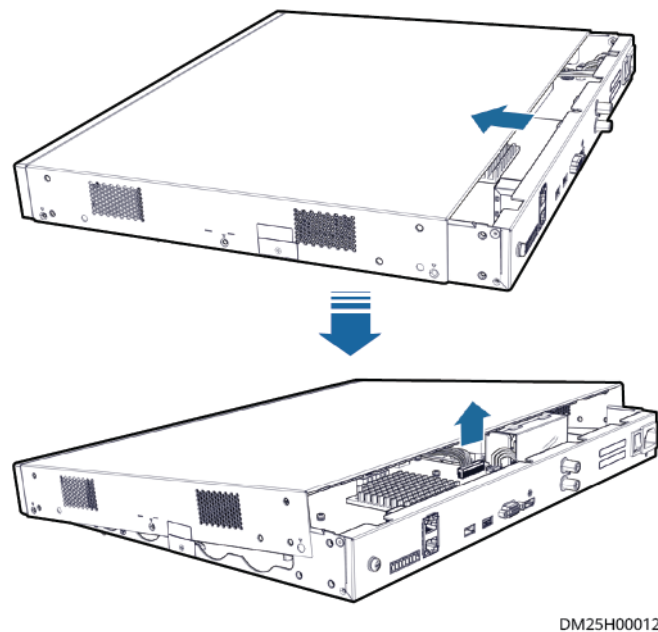
2. Then loosen the three fastening screws (M3 x 5 grub screw, white) that are used to connect the subrack bottom to the front panel.

Figure 3-42 Removing screws



3. Remove the upper cover of the chassis as follows: Hold the lower cover of the chassis with one hand, and push the upper cover of the chassis toward the front panel with the other hand. Then remove the upper cover with both hands.

Figure 3-43 Removing the upper cover of the chassis



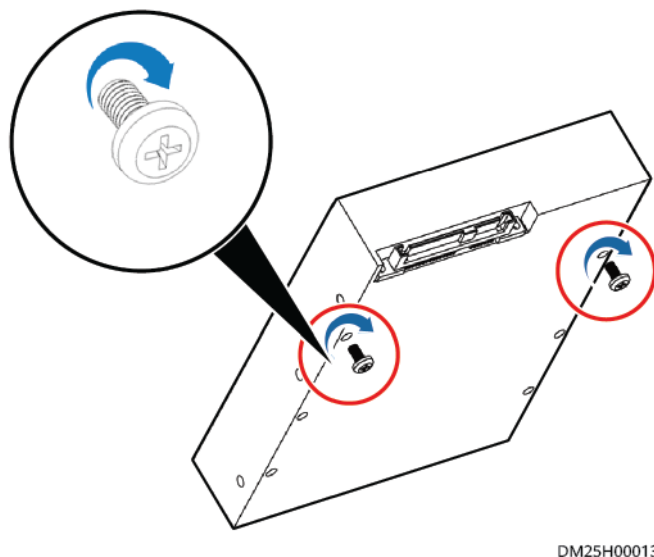
NOTE

When removing the upper cover from the chassis, do not use one hand to perform this operation. Otherwise, the upper cover may collide with the components inside the device, bringing risks of component damage.

4. Take two #6-32UNC screws from the screw package (there are eight screws in the package) and preinstall the two screws in the holes near the cable outlet

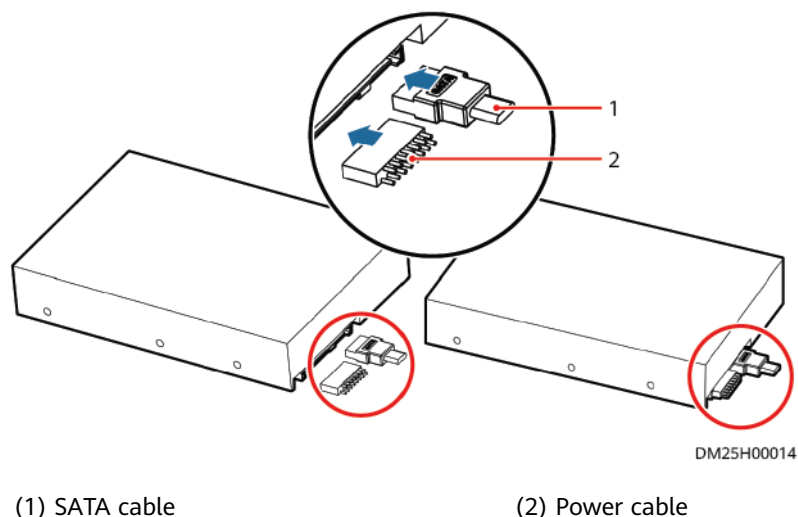
on the hard disk backplane. Tighten the screw threads for three circles (ensure that the screws do not fall naturally).

Figure 3-44 Installing hard disk screws



5. Insert the SATA and power cables into the corresponding interfaces on the disk. During cable connection, ensure that the metallic plate of the SATA cable faces upward.

Figure 3-45 Installing the SATA cable and power cable

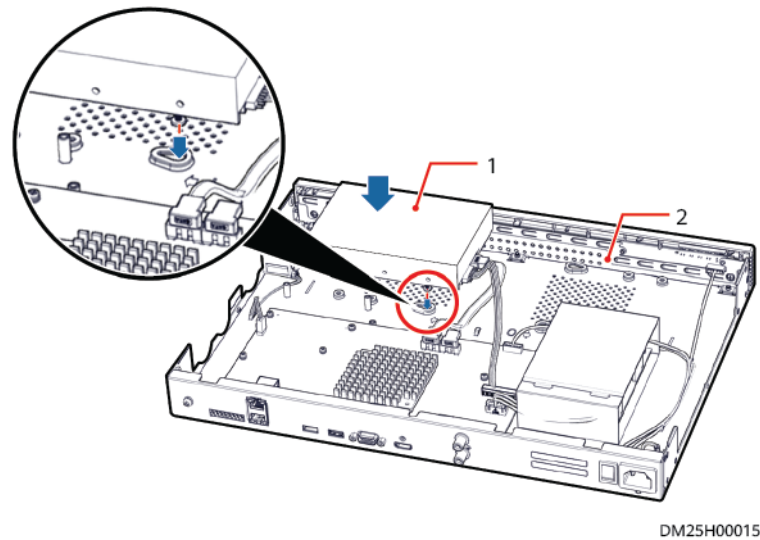


NOTE

When the VCN510 is delivered, the SATA cable connecting to the hard disk is fixed using blue tapes. Before installing the hard disk, remove the tapes.

6. Install a disk in No. 1 position. Place the disk above the No.1 disk installation position. Align the preinstalled screws with the cucurbit holes on the bottom cover of the chassis. Then, horizontally place the disk. Ensure that the screws are in the holes.

Figure 3-46 Disk installation positions

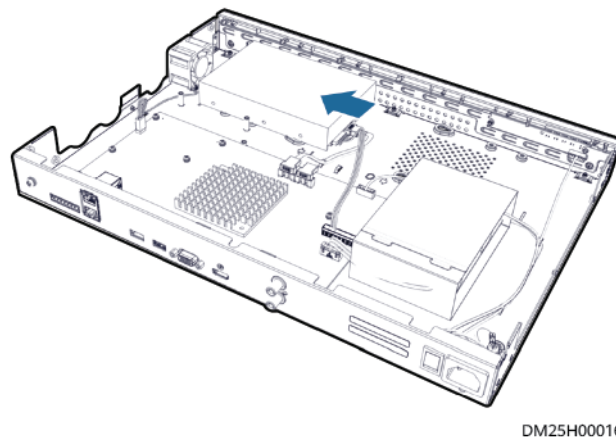


(1) No. 1 disk installation position

(2) No. 0 disk installation position

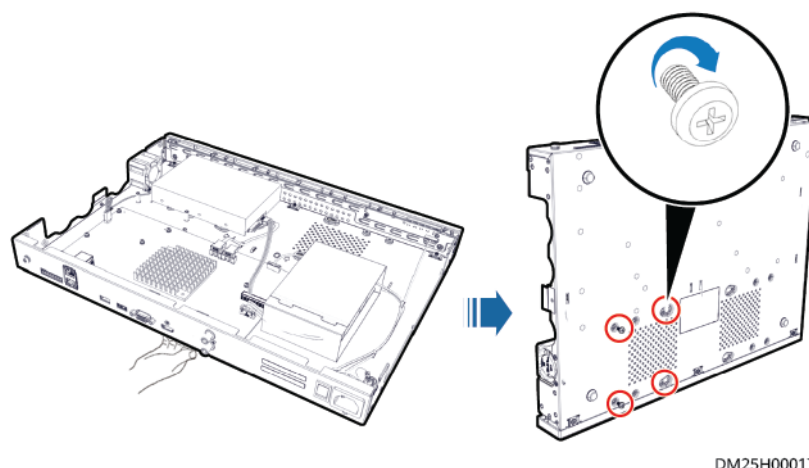
7. Push the disk following the direction shown in the lower-right figure to enable the two preinstalled screw heads to slide into the cucurbit holes.

Figure 3-47 Installing a hard disk



8. Hold the disk with one hand. Use the other hand to turn over the device at a 90-degree angle. Fasten the preinstalled screws from the rear panel of the device. Take another two #6-32UNC screws. Insert them into another two holes on the disk (for a disk with six holes, you are advised to install the screws into the two holes that are far away from the cable outlet) and tighten them.

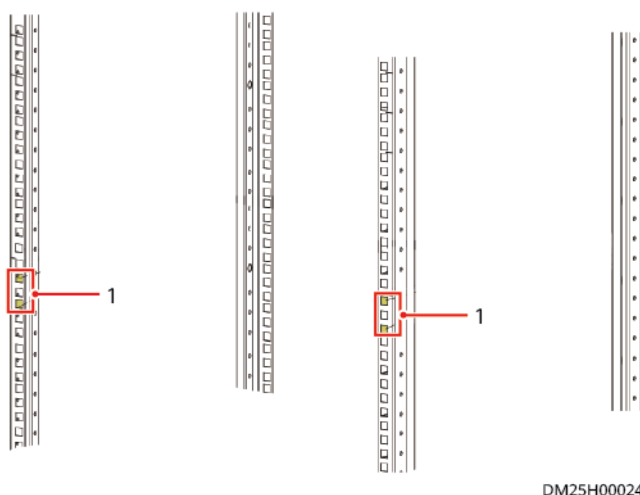
Figure 3-48 Installing a hard disk



9. Install a disk in No. 0 position. Install the disk in No.0 position in the same way for installing a disk in No.1 position. During disk installation, ensure that the direction for pushing the disk in No.0 position is opposite to that for pushing the disk in No.1 position.
10. Install the upper cover of the chassis. Place the upper cover of the chassis. Fasten the three screws on the bottom cover of the chassis and the six screws on the left and right sides of the chassis to fix the upper cover of the chassis.

Step 2 Install the floating nuts. Determine the mounting holes for the VCN510 in the network cabinet based on the engineering layout diagram, adjust the guide rails and install floating nuts.

Figure 3-49 Installing the floating nuts



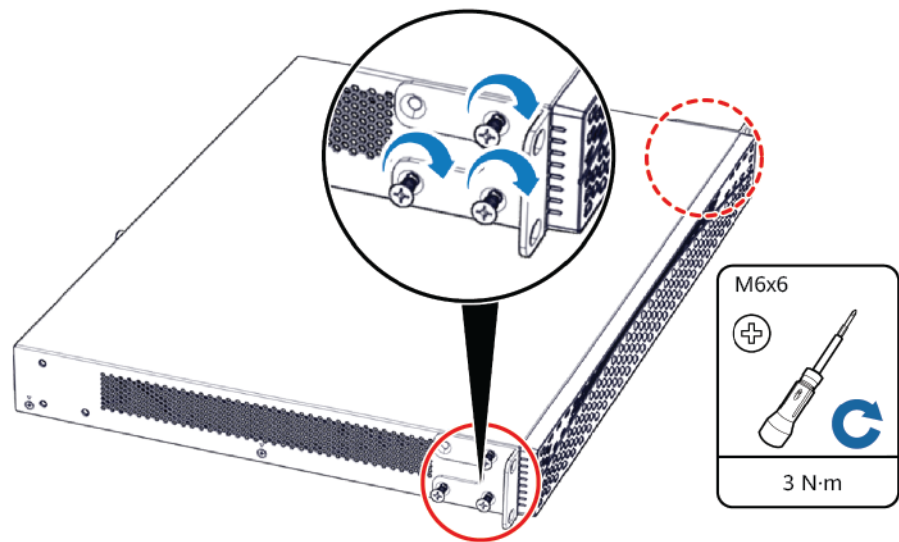
(1) Floating nuts

NOTE

The VCN510 is compact and lightweight. It can be directly fixed on the cabinet with M6 screws and mounting ears without using a guide rail. If a guide rail has been installed in the cabinet, you are advised to remove the guide rail first and then install the device in the cabinet. The VCN510 is equipped with right-to-left airflow, so installing a guide rail may affect the heat dissipation and lower the device performance accordingly.

- Step 3** Install mounting ears. Take six mounting ear screw (M4 x 6 countersunk screws, white). Use three screws to configure one mounting ear on the left of the front panel and the same way to configure the other ones on the right side. Then use a Phillips screwdriver to fasten the screws to fix the mounting ears.

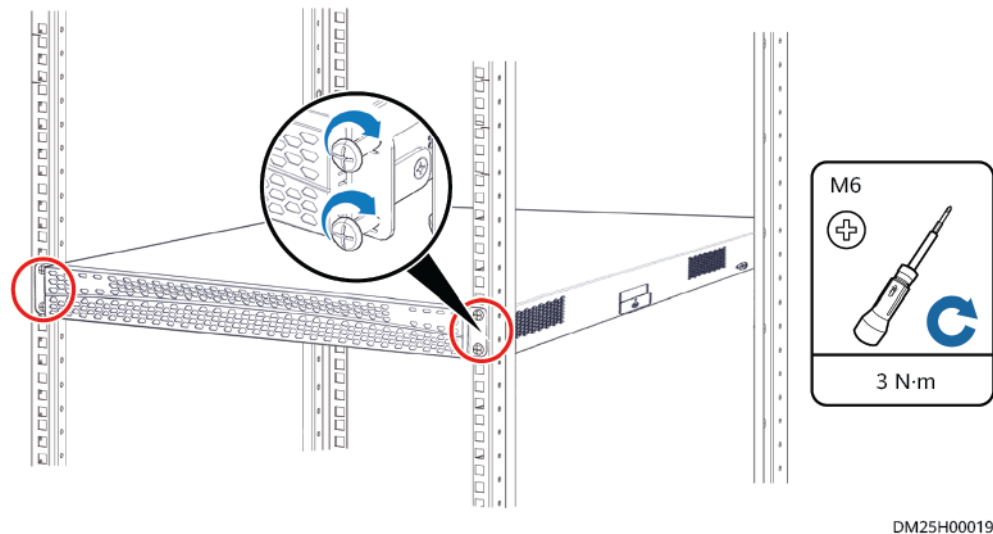
Figure 3-50 Installing mounting ears



DM25H00018

- Step 4** Install the device. Carry the device to the cabinet. Ensure that the mounting ears at both sides of the device are tightly attached to the mounting bars in front of the cabinet. Use one hand to hold the device. Use the other hand to thread M6 screws through the slotted hole on the mounting ear. Use a Phillips screwdriver to tighten the M6 screws on the mounting ears. Each mounting ear uses two M6 screws.

Figure 3-51 Installing the VCN510



----End

3.8.2 Installing the VCN520

Context

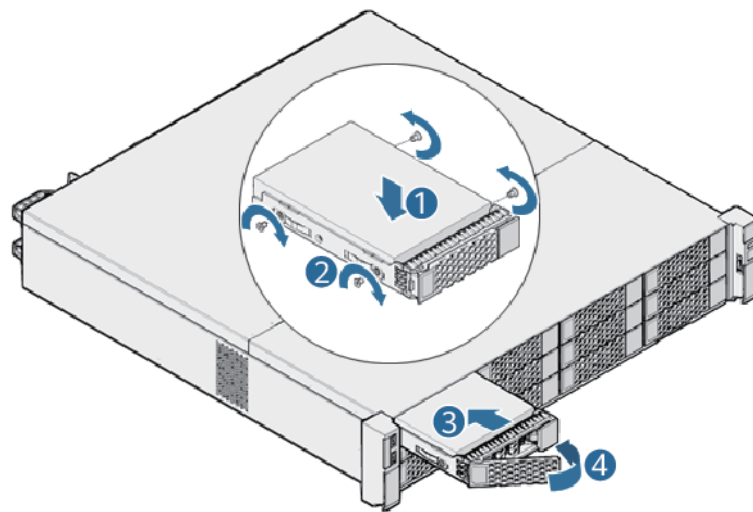
- The VCN520 does not carry disks when being delivered. First install disks and then install the device in a network cabinet.
- After the VCN520 is delivered to the site, disk filler panels are installed in slots where disks are not installed, by default. You are not advised to remove the filler panels from the slots where disks are not installed, because removing the filler panels will affect the heat dissipation of fans and generate some noises.

Procedure

Step 1 Install a hard disk.

1. Install a hard disk.
2. Secure the hard disk to the front panel using a screwdriver.
3. Push the hard disk into the subrack along the guide rails until it cannot move forwards.
4. Close the ejector lever and push the hard disk in position.

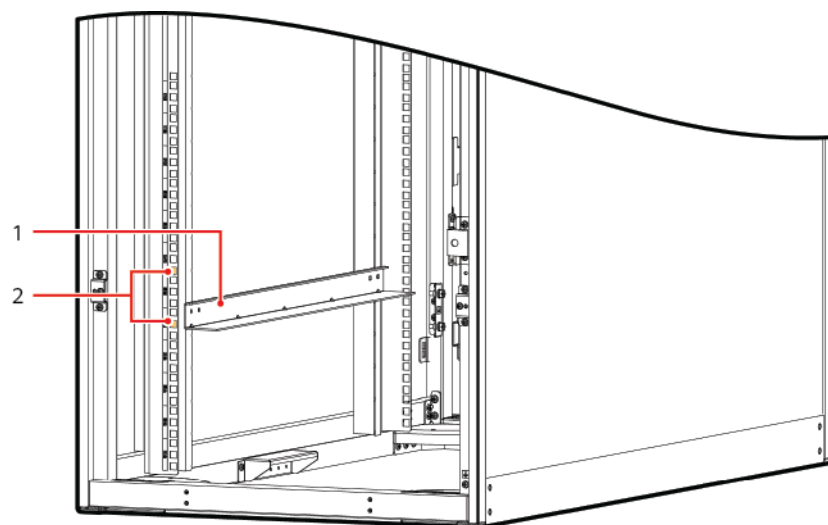
Figure 3-52 Installing a hard disk



DS31000012

Step 2 Determine the mounting holes for the VCN520 in the network cabinet based on the network cabinet device layout, adjust the guide rails, and install floating nuts.

Figure 3-53 Installing floating nuts



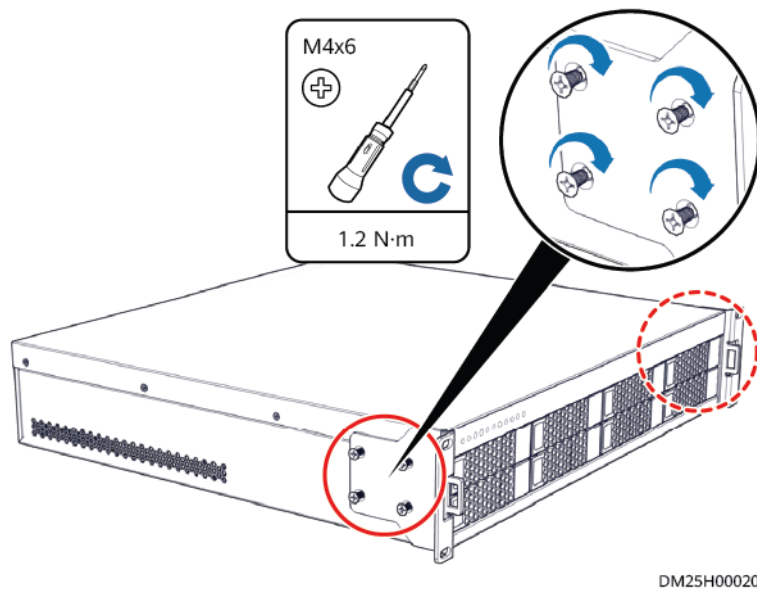
DM25H00023

(1) Guide rail

(2) Floating nut installation position

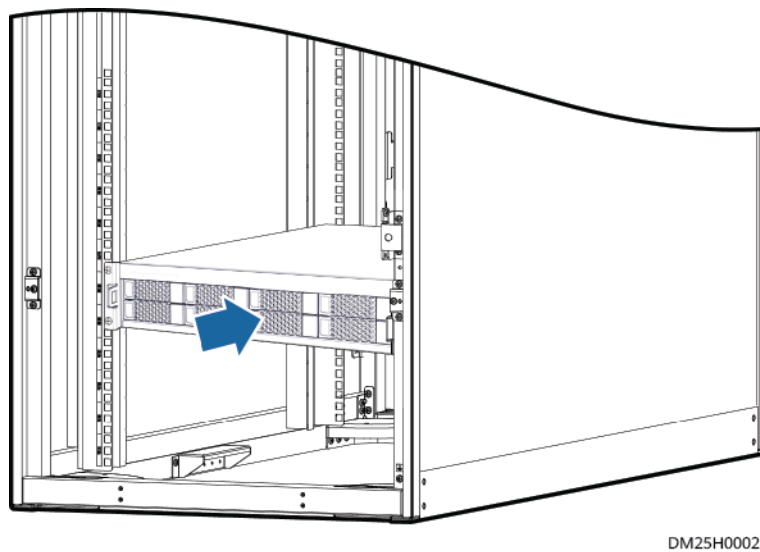
Step 3 Use four screws to configure one mounting ear on the left of the front panel and the same way to configure the other ones on the right side. Then use a Phillips screwdriver to fasten the screws to fix the mounting ears.

Figure 3-54 Installing mounting ears



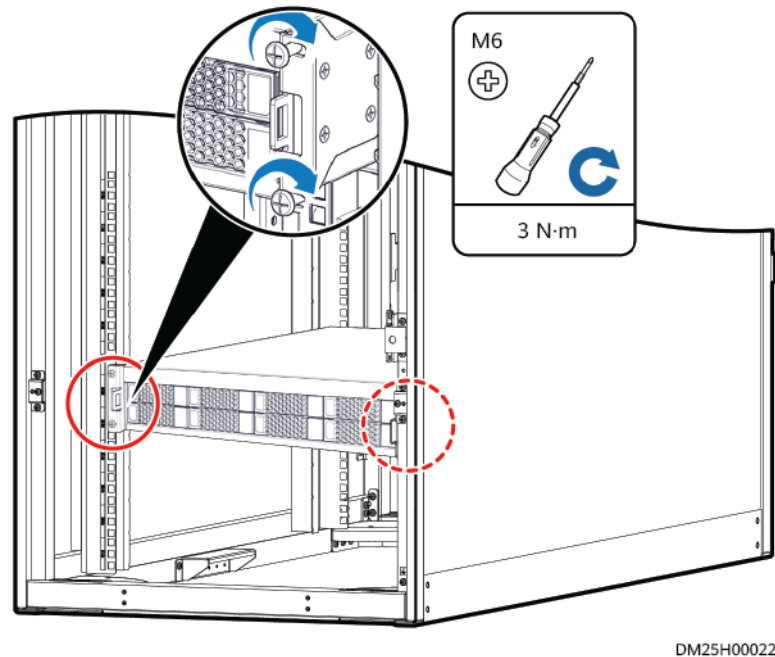
- Step 4** Slide the VCN520 into the network cabinet until the mounting ears on both sides of the network cabinet are in close contact with the mounting bars in front of the network cabinet.

Figure 3-55 Placing the VCN520



- Step 5** Secure each mounting ear with two M6 screws. Put the M6 screws through the mounting holes on the mounting ears, and tighten the screws using a Phillips screwdriver to secure the device to the mounting bars in front of the network cabinet.

Figure 3-56 Securing the VCN520



----End

3.8.3 Installing the VCN540

Context

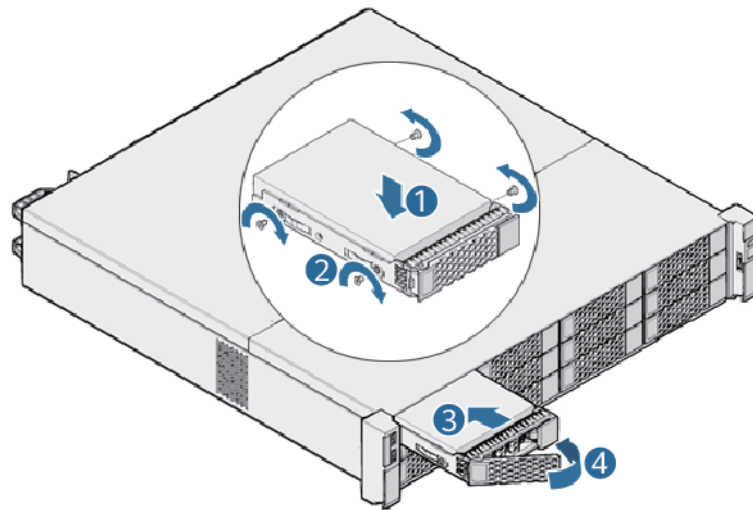
- The VCN540 does not carry disks when being delivered. First install disks and then install the device in a network cabinet.
- After the VCN540 is delivered to the site, disk filler panels are installed in slots where disks are not installed, by default. You are not advised to remove the filler panels from the slots where disks are not installed, because removing the filler panels will affect the heat dissipation of fans and generate some noises.

Procedure

Step 1 Install a hard disk.

1. Install a hard disk.
2. Secure the hard disk to the front panel using a screwdriver.
3. Push the hard disk into the subrack along the guide rails until it cannot move forwards.
4. Close the ejector lever and push the hard disk in position.

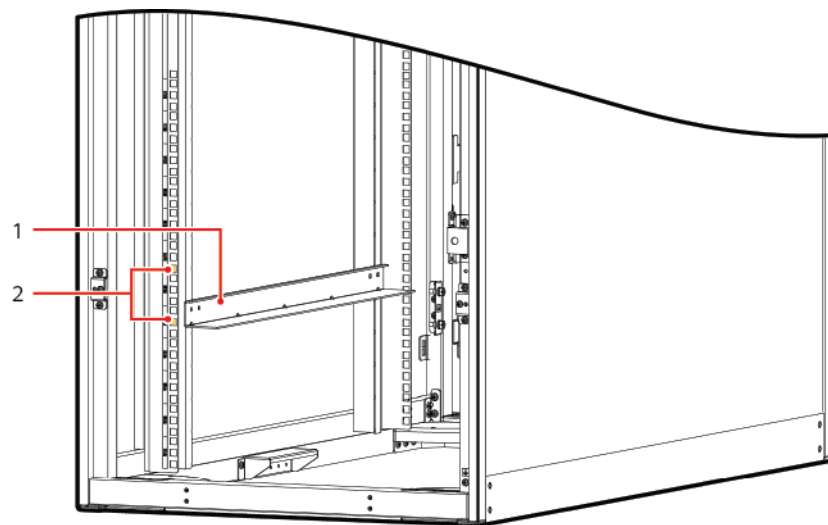
Figure 3-57 Installing a hard disk



DS31000012

Step 2 Determine the mounting holes for the VCN540 in the network cabinet based on the network cabinet device layout, adjust the guide rails, and install floating nuts.

Figure 3-58 Installing floating nuts



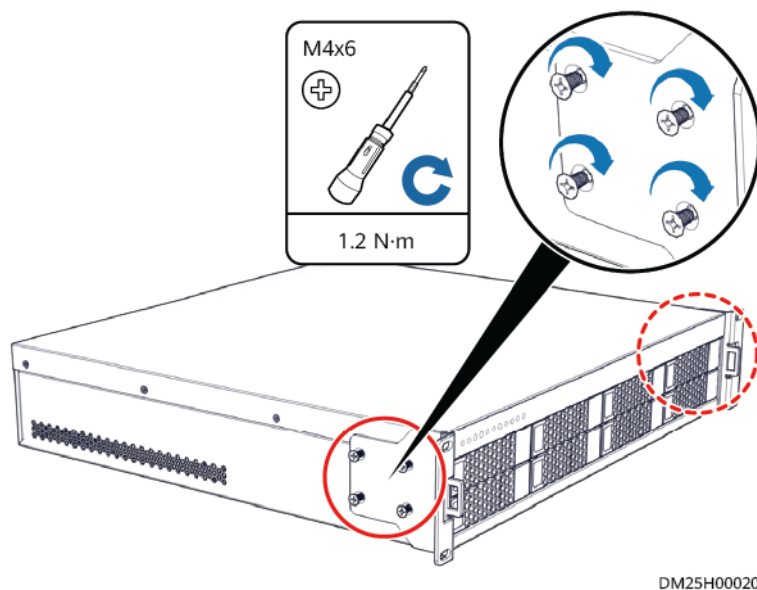
DM25H00023

(1) Guide rail

(2) Floating nut installation position

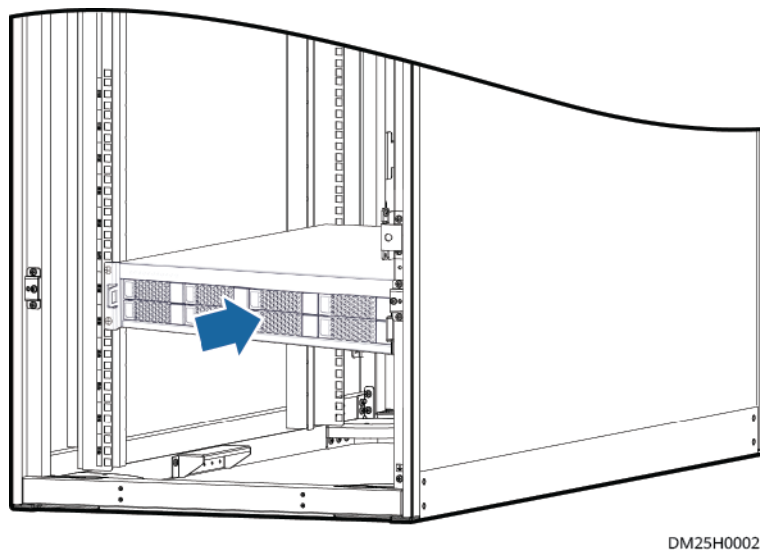
Step 3 Use four screws to configure one mounting ear on the left of the front panel and the same way to configure the other ones on the right side. Then use a Phillips screwdriver to fasten the screws to fix the mounting ears.

Figure 3-59 Installing mounting ears



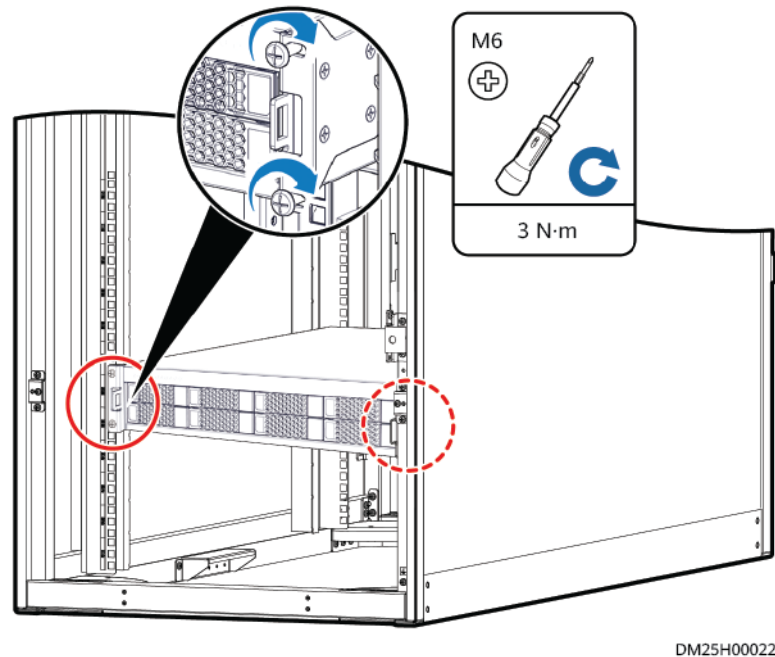
- Step 4** Slide the VCN540 into the network cabinet until the mounting ears on both sides of the network cabinet are in close contact with the mounting bars in front of the network cabinet.

Figure 3-60 Placing the VCN540



- Step 5** Secure each mounting ear with two M6 screws. Put the M6 screws through the mounting holes on the mounting ears, and tighten the screws using a Phillips screwdriver to secure the device to the mounting bars in front of the network cabinet.

Figure 3-61 Securing the VCN540



----End

3.8.4 Installing an IVS1800

Context

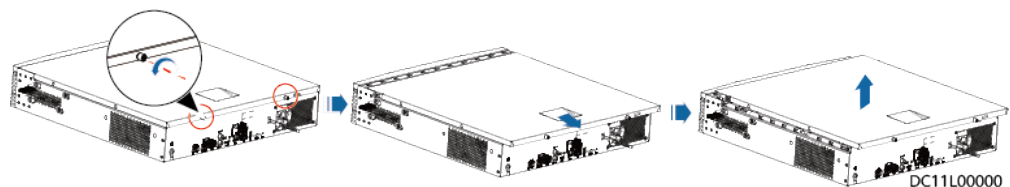
By default, the IVS1800 is delivered without disks. After the IVS1800 is delivered to the site, install hard disks as required and then install the IVS1800 in the cabinet.

Procedure

Step 1 Install hard disks.

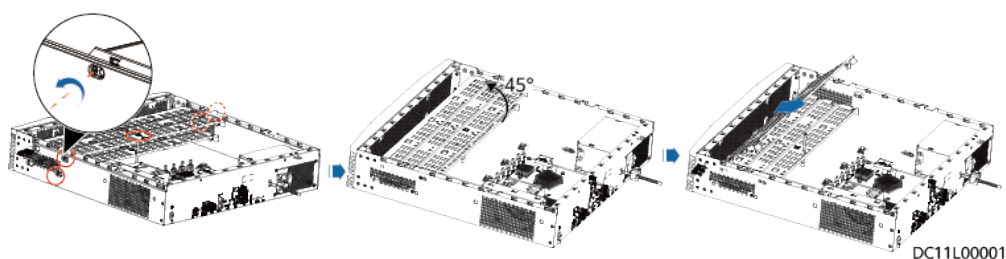
1. Use a PH2 screwdriver to remove the two black screws on the rear of the chassis cover, and take off the chassis cover.

Figure 3-62 Removing the chassis cover



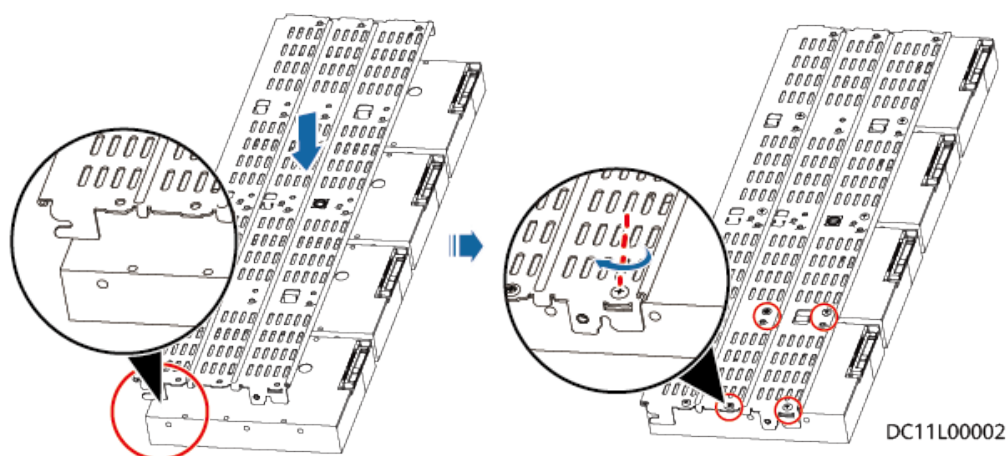
2. Remove two black screws on each side of the chassis and the silvery white one on top of the hard disk tray, raise the hard disk tray by 45 degrees, and take out the upper and then lower layers of hard disk tray.

Figure 3-63 Removing the hard disk tray



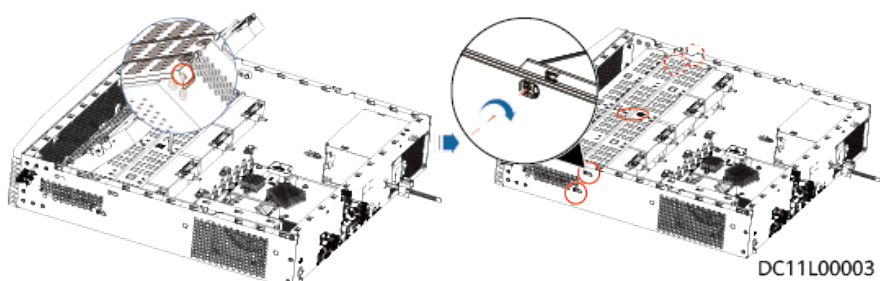
3. Place the hard disks with ports facing upwards and align the screw holes on the hard disk tray with the hard disks and fasten the screws. Before the installation, ensure that the fastener of the hard disk tray is on a different side from the hard disk port, as shown in the lower left figure.

Figure 3-64 Installing hard disks



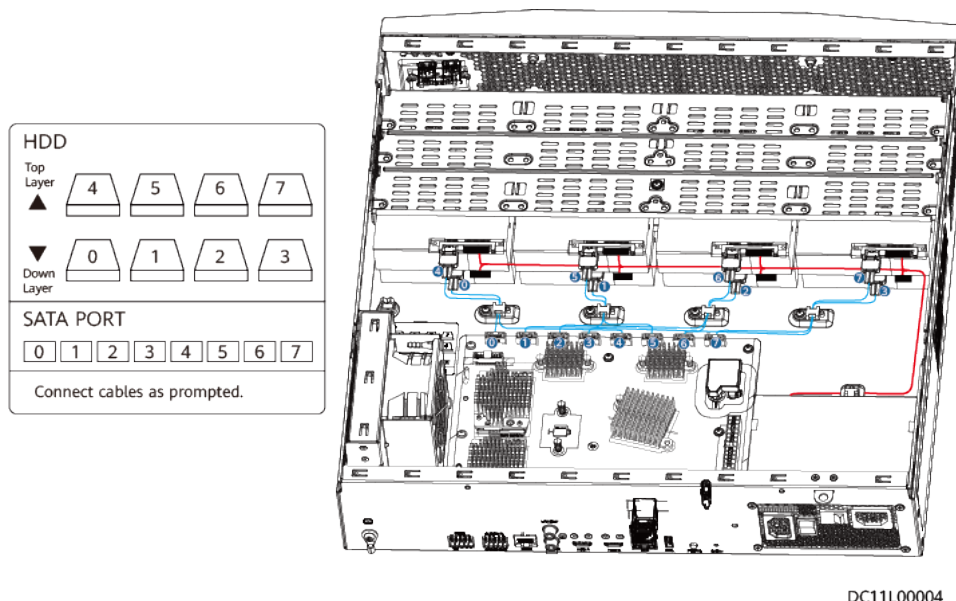
4. Insert the hard disk tray back at 45 degrees with the opening of its locking buckle facing downwards, hold the screw in the red-framed part to lower the hard disk tray until it is level, and fasten the black screws on the left and right sides and the white screw on the top.

Figure 3-65 Fastening the screw on the panel and the screws on the hard disk tray



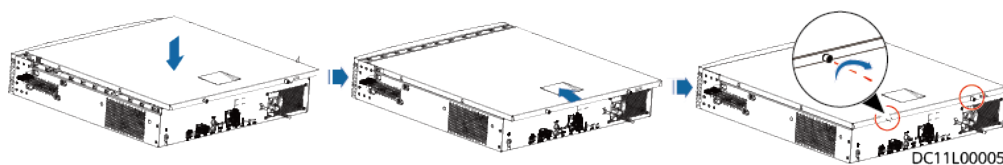
5. Connect data and power cables to hard disks. Connect hard disk cable ports P0-P3 to hard disks on the lower-layer hard disk tray and ports P4-P7 to hard disks on the upper-layer, as shown in the lower left figure.

Figure 3-66 Connecting data and power cables to hard disks



6. Close the chassis cover, and use a PH2 screwdriver to fasten the rear screws.

Figure 3-67 Closing the chassis cover

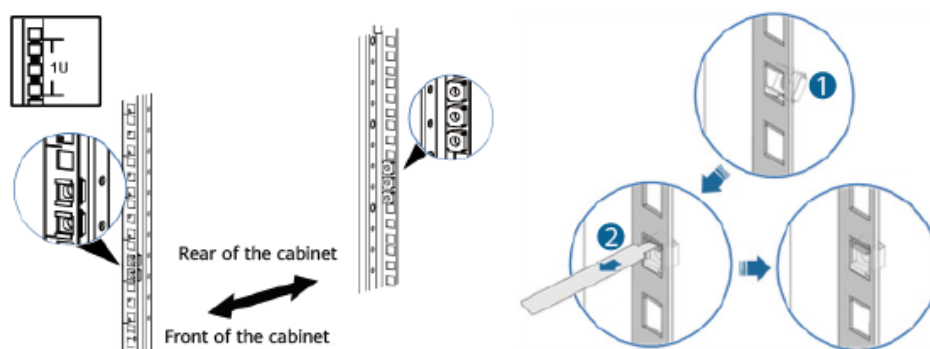


Step 2 Install the device.

NOTE

- Before installing the IVS1800 in a cabinet, install guide rails to hold the device. If guide rails have been installed in the cabinet, check whether they match the device and whether they block the air intake or exhaust vents of the chassis as the fan is located on the side. If the vents are blocked, change the guide rails.
 - Huawei provides guide rails that can be adjusted from 500 mm to 800 mm for additional purchase if required for IVS1800 installation.
 - Do not attach rubber feet on the IVS1800 to save space during cabinet installation.
1. Confirm the installation location of guide rails in the cabinet. Install cage nuts (two at the front and three at the back on each side) to secure the guide rails at the proper position in the cabinet, as shown in the lower left figure. The lower right figure shows how to install cage nuts.
 1. Insert a cage nut into the square hole from the inside of the cabinet and clamp it to the lower frame of the square hole.
 2. Use a mounting bar to pull the cage nut until it clamps the upper frame of the square hole.

Figure 3-68 Installing a cage nut



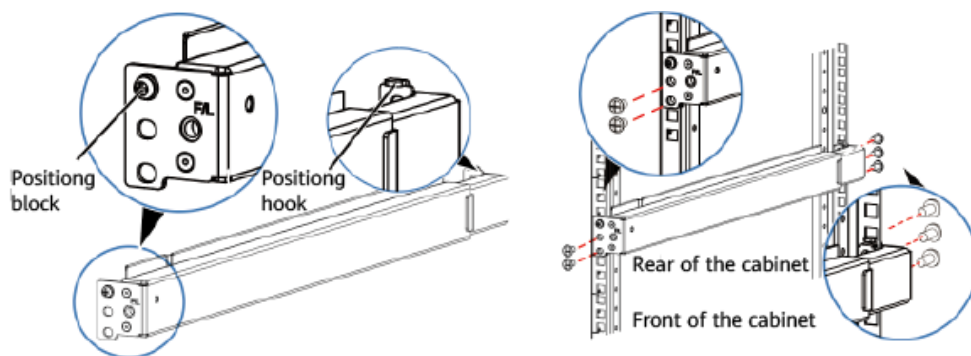
DC11L00018

2. Install guide rails. Horizontally place a guide rail to the installation location through the positioning block at the front of the guide rail and the positioning hook at the rear of the guide rail. Fasten four M6 screws (two on each side) to fix the front end and six M6 screws (three on each side) to fix the rear end, as shown in the lower right figure.

CAUTION

Before installing a guide rail, check the (F/L, F/R) labels on the guide rail to identify whether it is for the left or right and which part is the front or rear. F/L indicates the front end of the left guide rail, and F/R indicates the front end of the right guide rail.

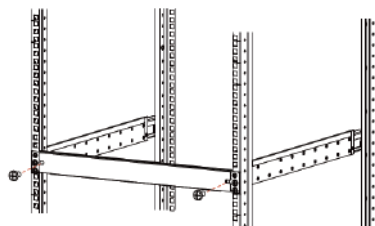
Figure 3-69 Installing a guide rail



DC11L00019

3. Install a filler panel for guide rails. Fasten the M6 screws to install the filler panel for the guide rails.

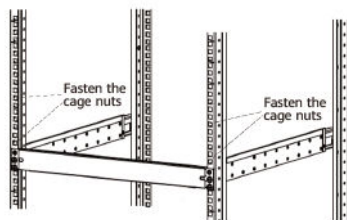
Figure 3-70 Installing a filler panel for guide rails



DC11L00013

4. Install the cage nuts that secure the IVS1800. The cage nut installation locations are the first and sixth holes along the guide rails, as shown in the following figure.

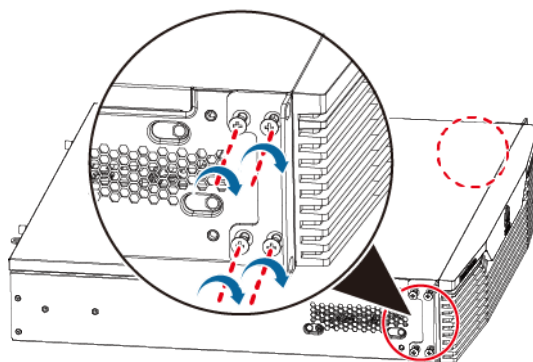
Figure 3-71 Installing cage nuts



DC11L00020

5. Install mounting ears. Use a PH2 screwdriver to secure the mounting ears to both sides of the front panel of the device with four screws on each side. When the device is near the front door of the cabinet, fasten screws in hole groups 1 and 2; when the device is near the rear door, fasten screws in hole groups 2 and 3.

Figure 3-72 Installing mounting ears

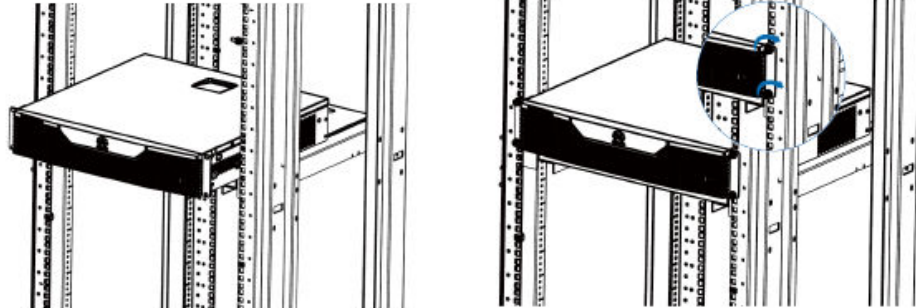


DC11L00015

6. Install the IVS1800 in the cabinet.
 1. Lift the device from both sides and carefully position it at the front of the cabinet.
 2. Lift the device slightly above the guide rails, gently place it on the guide rails, and then slide it into the cabinet until the mounting ears of the subrack contact the mounting bars at the front of the cabinet.
7. Thread M6 screws (prepared by the customer) through two slotted holes on each mounting ear. Fasten the M6 screws using a Phillips screwdriver to fix

the mounting ears on the front mounting bars of the cabinet, as shown in the lower right figure.

Figure 3-73 Securing the device



DC11L00016

Step 3 Power on the device.

1. Turn on the power switch.
2. Check the indicators on the front panel of the device for its running status.

----End

3.8.5 Installing a C3220 Camera

Prerequisites

- Control skylights have been installed.
- A camera and tools for installing it have been prepared.
- A network cable for connecting the camera to the LAN switch has been prepared.
- The LAN switch has been normally powered on.

Context

The camera needs to be installed on a control skylight.

Preparations

Tool: Phillips screwdriver

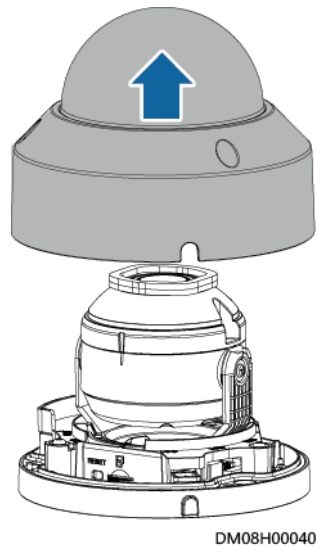
Materials: SD card, camera

Procedure

Step 1 Install an SD card.

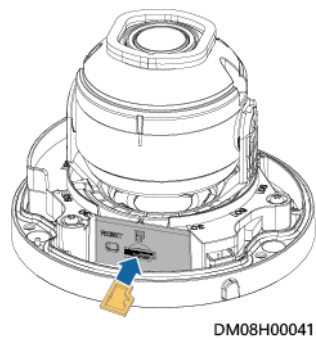
1. Remove the transparent cover using a Phillips screwdriver.

Figure 3-74 Removing the transparent cover



2. Gently insert the SD card into the SD card slot.

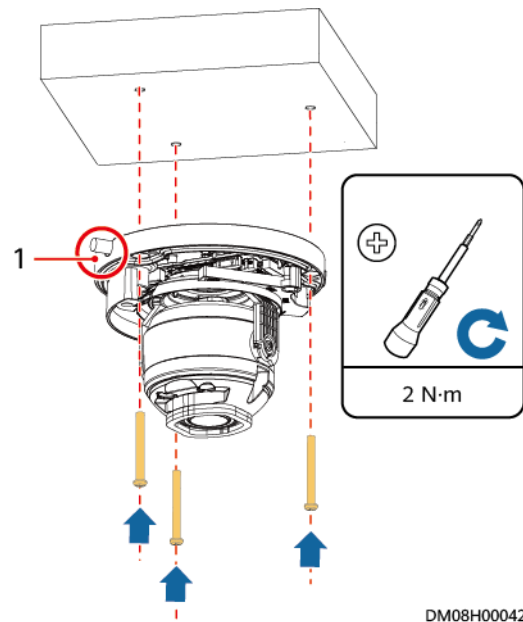
Figure 3-75 Installing an SD card



Step 2 Route the camera cable through the control skylight.

Step 3 Align the holes in the camera base with the holes on the control skylight, and secure the camera to the control skylight.

Figure 3-76 Installing a camera base



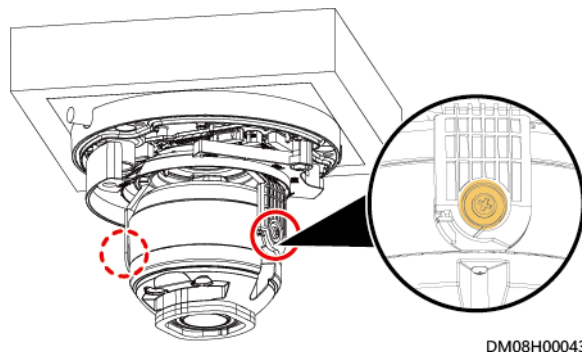
(1) Cable outlet

- Step 4** Use a Phillips screwdriver to loosen the screws on both sides of the lens, adjust the surveillance angle, and tighten the screws to 0.6 N·m.

NOTICE

- By default, the camera is horizontally installed, and the surveillance video is displayed horizontally. During the installation, adjust the surveillance angle to avoid video image rotation after the installation.
- When adjusting the surveillance angle, pay attention to the position of the illuminator to prevent the illuminator from being blocked.

Figure 3-77 Adjusting the camera

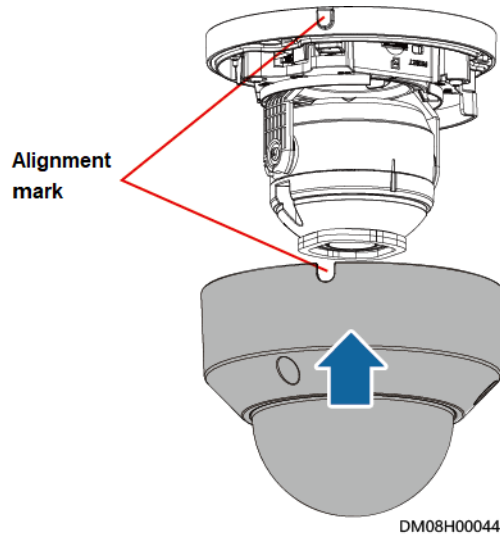


NOTE

The camera features a three-axis design. The camera can be adjusted by -175° to $+180^{\circ}$ horizontally, and the lens can rotate -175° to $+180^{\circ}$ and be adjusted by 0° to 65° vertically.

- Step 5** Align the transparent cover with the screw holes on the base, close the transparent cover, and use a Phillips screwdriver to tighten the screws to 0.8 N·m.

Figure 3-78 Installing the transparent cover



----End

3.8.6 Installing the M2121 Camera

Cameras can be installed on different objects based on scenarios. This section describes how to install a M2121 camera on the wall.

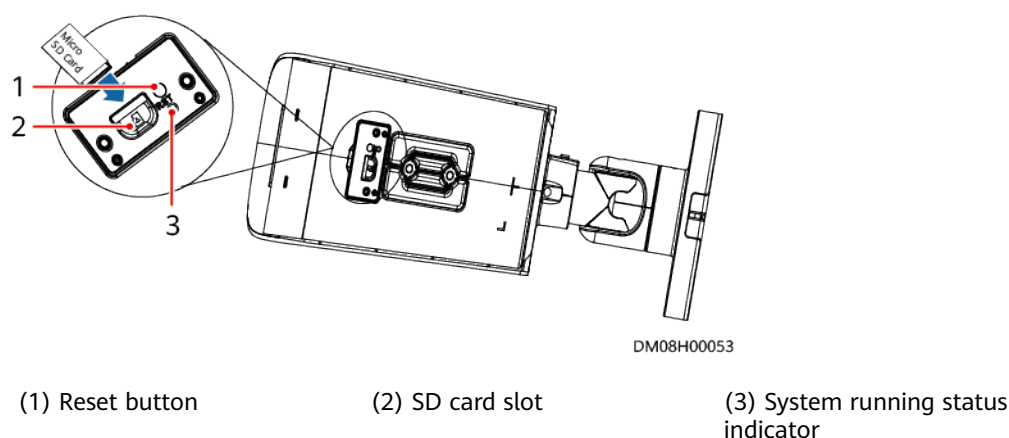
Prerequisites

- A camera and tools for installing it have been prepared.
- A network cable for connecting the camera to the LAN switch has been prepared.
- The LAN switch has been normally powered on.

Procedure

- Step 1** Use a Phillips screwdriver to remove the bottom cover of the camera and insert the SD card. For details about the SD card insertion direction, see the marks on the maintenance window. After the installation is complete, tighten the bottom cover to a torque of 0.49 N·m.

Figure 3-79 Installing an SD card

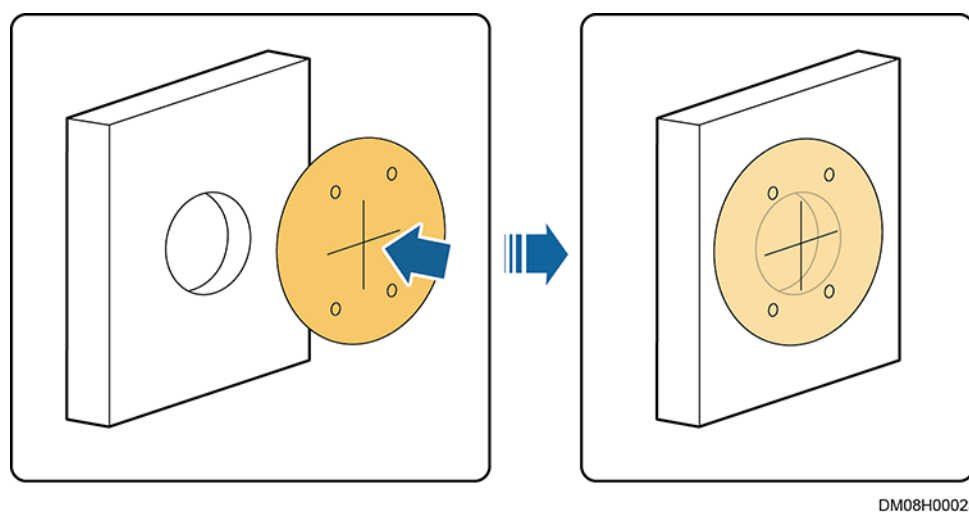


CAUTION

- If the camera cannot connect to the platform for a long time or is not connected to the platform, you are advised to disable the video buffering function of the camera to increase the service life of the SD card.
- Do not remove the window protective film before the installation is complete.

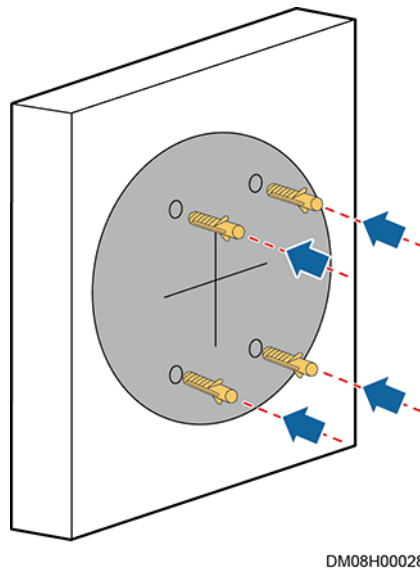
Step 2 Check the diameter of the cable outlet on the wall to ensure that the tails can be routed through the cable outlet. Paste the drilling sticker in the camera installation position. Ensure that the center of the sticker overlaps the center of the cable outlet on the wall.

Figure 3-80 Determining the camera installation position



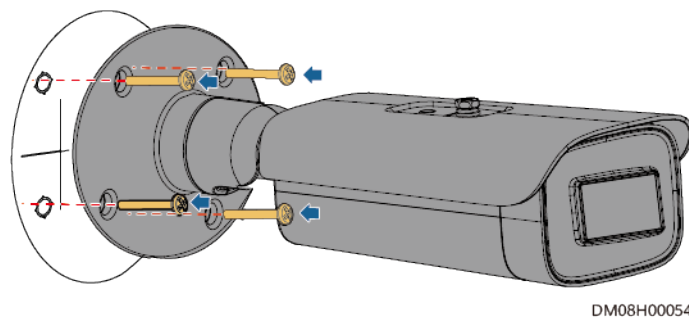
Step 3 Obtain a drill bit with a diameter of 8 mm and drill 55 mm holes in the specified positions marked by the stickers. Use a claw hammer to install expansion bolts into the holes.

Figure 3-81 Inserting the expansion tube



Step 4 Connect the cables to the tails of the camera, perform insulation operations on the cables, and put the cables through the cable entry on the wall. Tighten the tapping screws. Ensure that the cable outlet in the camera base points down, and seal the outlet with waterproof sealant.

Figure 3-82 Installing the M2121 camera

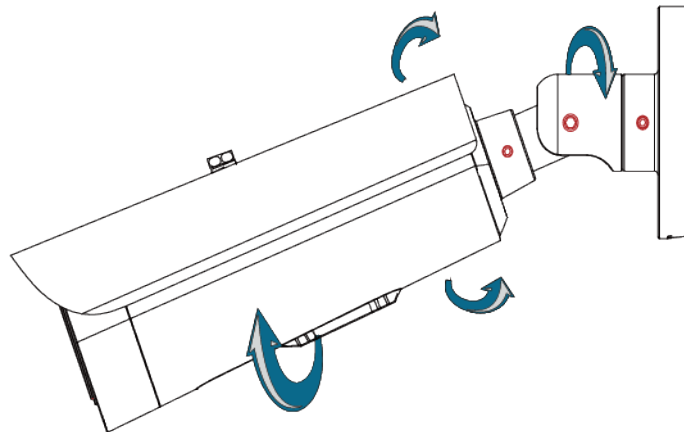


NOTE

- The preceding installation method is to route the pigtail through the wall. If the pigtail does not need to be routed through the wall, route the pigtail out of the cable outlet on the base and cover it with a corrugated pipe.
- Face the cable outlet with BOTTOM on the camera base downwards to prevent water from flowing into the camera and cause damage to the camera.

Step 5 Loosen the three hexagon socket head cap screws on the bracket, adjust the camera angle, and tighten the screws.

Figure 3-83 Adjusting the M2121 camera



DM08H00055

----End

3.9 Installing the Access Management System

3.9.1 Installing an A8802RS Access Controller

Context

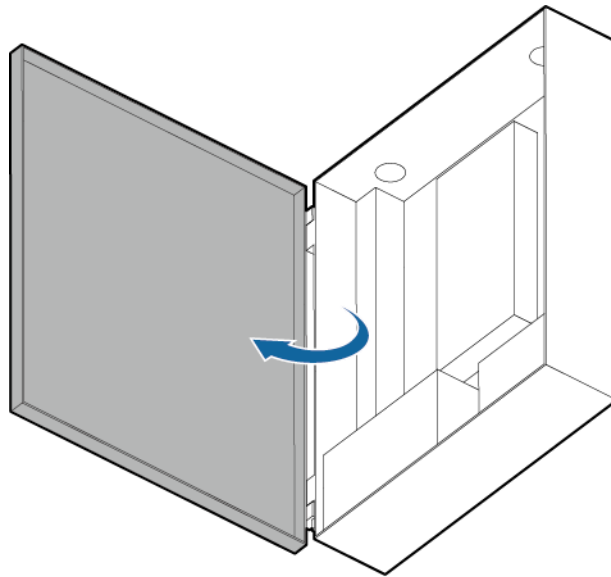
- The access controller can be wall-mounted. You are advised to install it in a weak-current well.
- If a twisted pair is connected between the access controller and the card reader, it is recommended that the distance between them do not exceed 30 m.
- Install double-door and quadruple-door access controllers by referring to this section.

Procedure

Step 1 Mark the mounting holes using the access controller and marker, and drill holes using a hammer drill.

Step 2 Unlock the access controller with the delivered key.

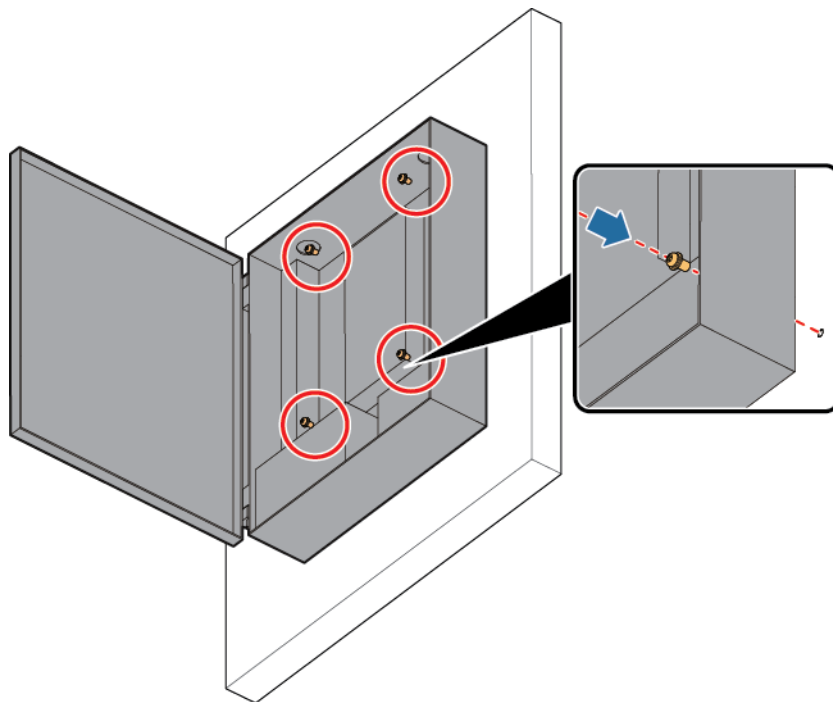
Figure 3-84 Unlocking an access controller



DM04H00011

Step 3 Use four screws to install the access controller on the wall.

Figure 3-85 Installing an access controller



DM04H00010

----End

3.9.2 Installing an In-Room Double-Door Magnetic Lock

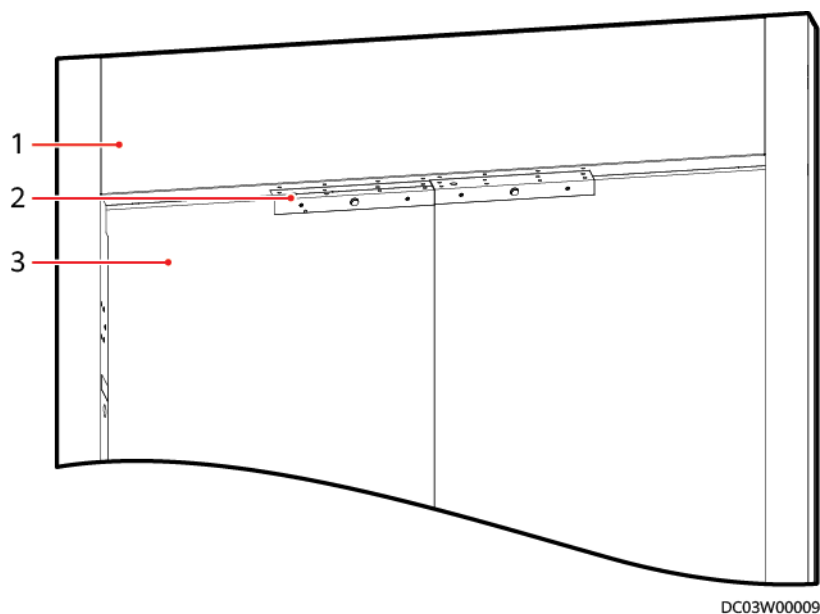
Context

- The magnetic lock supports a double-door that can be rotated open outwards. The door frame should be over 42 mm thick. A glass door is not supported.
- The cable routes are planned.

Procedure

- Step 1** Fold the delivered cutout template along the dotted line by 90 degrees, as shown by (2) in [Figure 3-86](#).
- Step 2** Close the door, place the cutout template at the midline of the door frame in the door opening direction, mark the mounting holes, and drill holes, as shown in [Figure 3-86](#).

Figure 3-86 Mark the installation position



(1) Door frame

(2) Cutout template

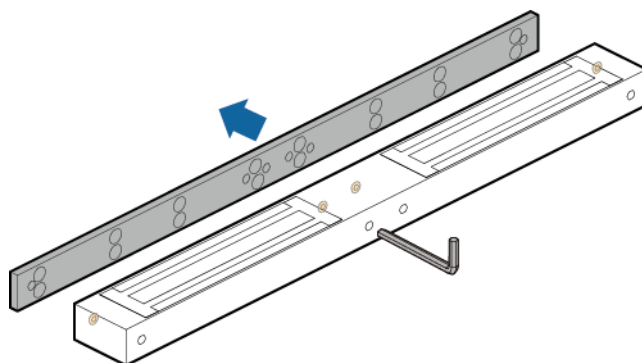
(3) Door panel

- Step 3** Remove the hoisting strip using the delivered hex key.

NOTE

Four hex socket screws need to be removed in this step.

Figure 3-87 Removing a hoisting strip



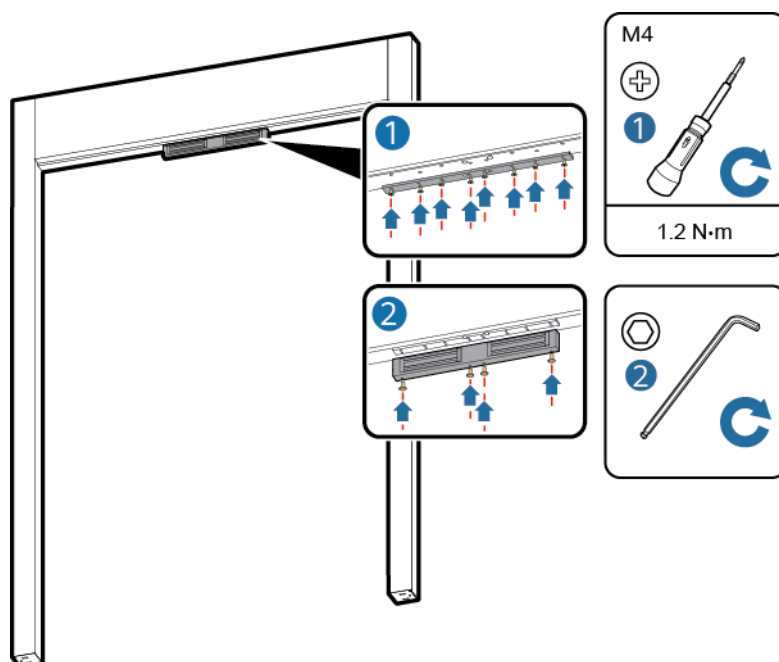
DM22000022

Step 4 Secure the hosting strip using the delivered screws, as shown by (1) in [Figure 3-88](#).

NOTICE

Pay attention to the direction of the hoisting strip, and ensure that the bulging surface of the magnetic lock faces the magnet.

Figure 3-88 Installing a magnetic lock



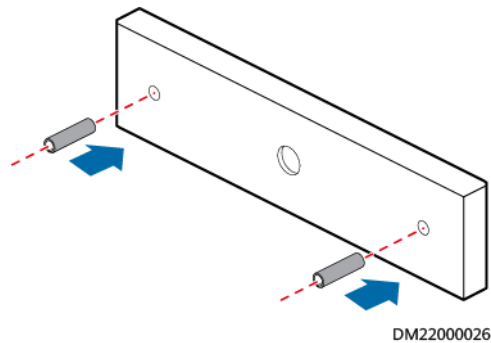
DC03H00106

Step 5 Route the electronic lock cable through the cable hole, and secure the electronic lock using a hex key, as shown by (2) in [Figure 3-88](#).

Step 6 Install the magnet.

1. Take out the magnet, and knock the positing pins of the magnet into the magnet using a rubber mallet.

Figure 3-89 Installing positioning pins of a magnet

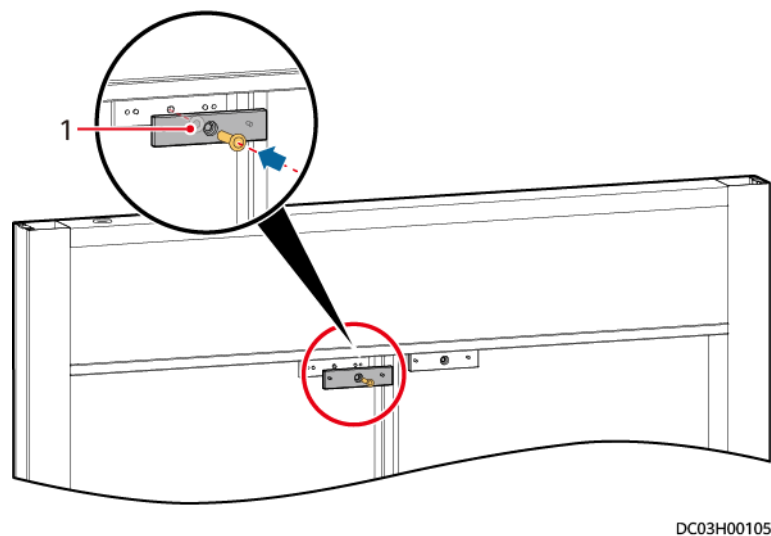


2. Insert the assembled magnet into the positioning holes in the door, and secure the magnet to the door using the screws and rubber pad delivered with the electronic lock, as shown in [Figure 3-90](#).

NOTE

When securing the magnet to the door panel, do not over-tighten the screws so that the rubber pad is elastic. The rubber pad will adjust the magnet to a correct position because of its elasticity.

Figure 3-90 Installing a magnet



(1) Rubber pad

Step 7 (Optional) Adjust the magnet.

1. If the magnet cannot attract the door properly after power-on, place a magnetized metal part near the magnet to check whether the magnet provides a proper magnetic force.
2. If the magnetic lock and the magnet do not work properly, check and troubleshoot the circuit.

----End

3.9.3 Installing an In-Room Single-Door Magnetic Lock

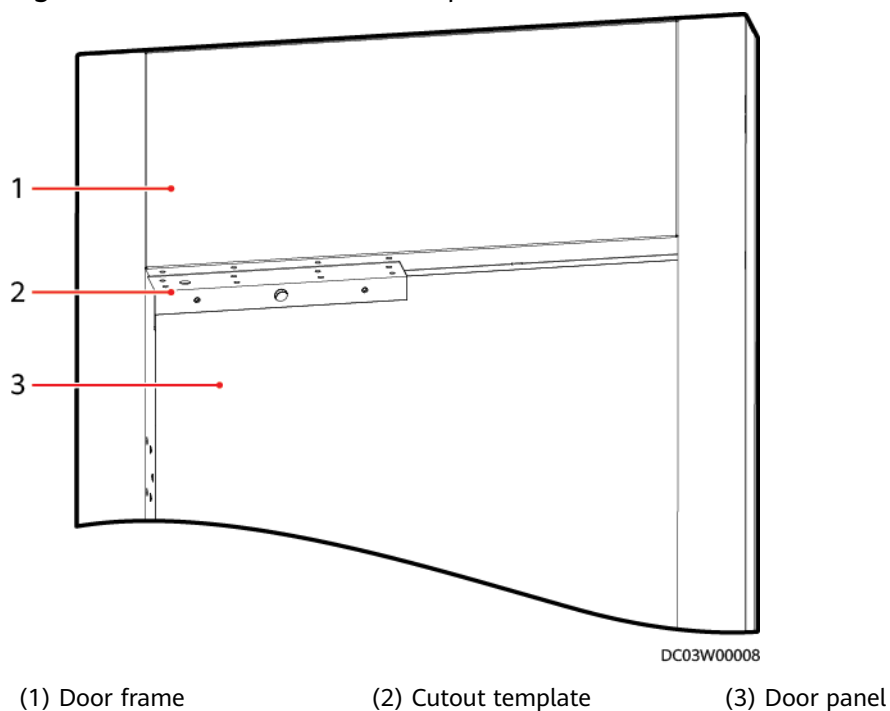
Context

- Check that the room door is a single-door that can be rotated open outwards. The door frame should be over 42 mm thick. A glass door is not supported.
- The cable routes are planned.

Procedure

- Step 1** Fold the delivered cutout template along the dotted line by 90 degrees, as shown by (2) in [Figure 3-91](#).
- Step 2** Close the door, place the cutout template near the top of the door frame in the door opening direction, mark the mounting holes, and drill holes, as shown in [Figure 3-91](#).

Figure 3-91 Mark the installation position

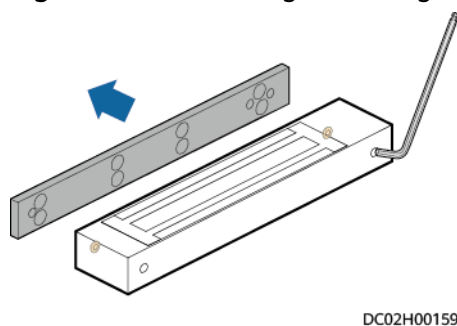


- Step 3** Remove the hoisting strip using the delivered hex key.

NOTE

Two hex socket screws need to be removed in this step.

Figure 3-92 Removing a hoisting strip

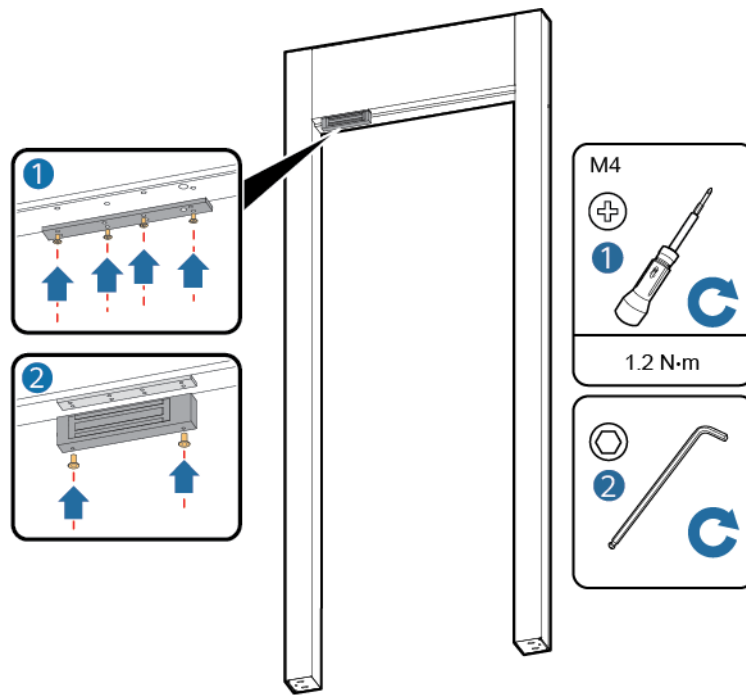


- Step 4** Secure the hosting strip using the delivered screws, as shown by (1) in [Figure 3-93](#).

NOTICE

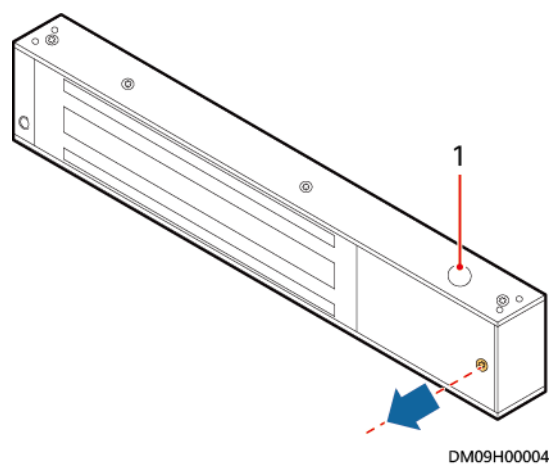
Pay attention to the direction of the hoisting strip, and ensure that the bulging surface of the magnetic lock faces the magnet.

Figure 3-93 Installing a magnetic lock



- Step 5** Remove the small cover from the magnetic lock, and route the cable out of the cable hole, as shown in [Figure 3-94](#).

Figure 3-94 Connecting cables



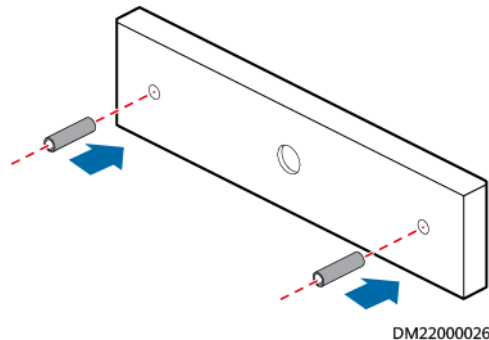
(1) Cable outlet

Step 6 Secure the magnetic lock, as shown by (2) in [Figure 3-93](#).

Step 7 Install the magnet.

1. Take out the magnet, and knock the positing pins of the magnet into the magnet using a rubber mallet.

Figure 3-95 Installing positioning pins of a magnet

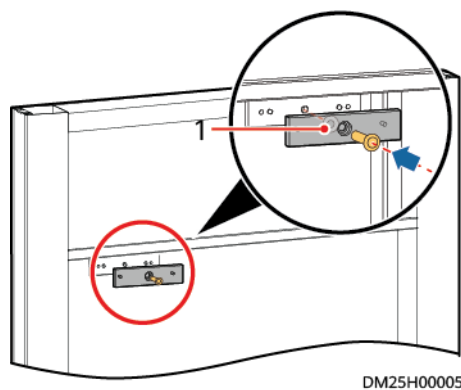


2. Insert the assembled magnet into the positioning holes in the door, and secure the magnet to the door using the screws and rubber pad delivered with the electronic lock, as shown in [Figure 3-96](#).

NOTE

When securing the magnet to the door panel, do not over-tighten the screws so that the rubber pad is elastic. The rubber pad will adjust the magnet to a correct position because of its elasticity.

Figure 3-96 Installing a magnet



(1) Rubber pad

Step 8 (Optional) Adjust the magnet.

1. If the magnet cannot attract the door properly after power-on, place a magnetized metal part near the magnet to check whether the magnet provides a proper magnetic force.
2. If the magnetic lock and the magnet do not work properly, check and troubleshoot the circuit.

----End

3.9.4 Installing a Fingerprint and Card Reader with a Keypad

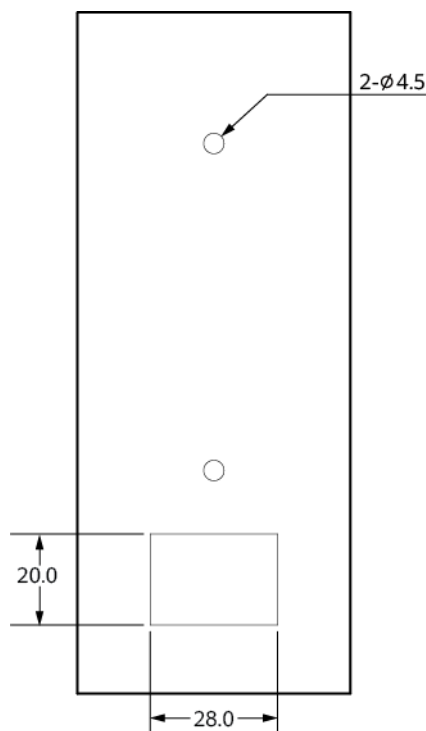
Context

- It is recommended that the product be installed 30–300 mm close to the equipment room door and 1.4–1.6 m above the floor.
- Do not install the product in a place with heavy dust or exposed to sunlight.

Procedure

- Step 1** Remove the screws (set aside) from the fingerprint and card reader with a keypad and remove the baseplate, as shown by (1) in [Figure 3-98](#).
- Step 2** Mark the mounting holes using a marker, and drill holes using a hammer drill.

Figure 3-97 Marking mounting holes (unit: mm)



DC02500029

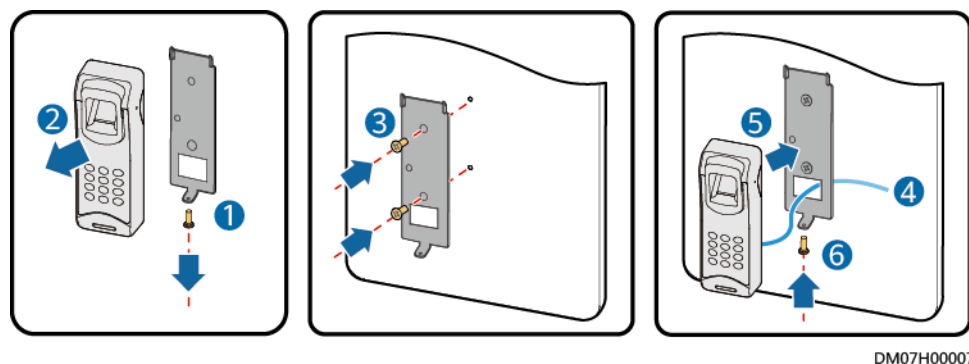
- Step 3** Install the baseplate, as shown by (3) in [Figure 3-98](#).
- Step 4** Route the cable of the fingerprint and card reader with a keypad through the cable hole in the baseplate, as shown by (4) in [Figure 3-98](#).

NOTE

The fingerprint and card reader with a key pad is connected to the access actuator by a network cable.

- Step 5** Check that cables are correctly connected.
- Step 6** Secure the fingerprint and card reader with a keypad to the baseplate, as shown by (5) and (6) in [Figure 3-98](#).

Figure 3-98 Installing a fingerprint and card reader with a keypad



----End

3.9.5 Installing a Fingerprint and Card Reader

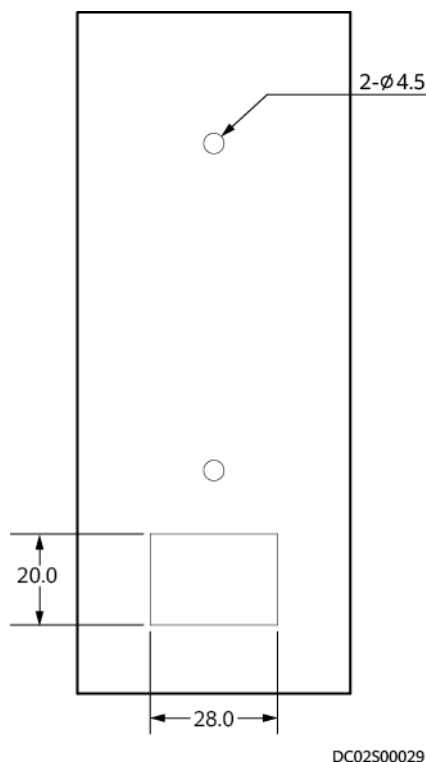
Context

- It is recommended that the product be installed 30–300 mm close to the equipment room door and 1.4–1.6 m above the floor.
- Do not install the product in a place with heavy dust or exposed to sunlight.

Procedure

- Step 1** Remove the screws (set aside) from the fingerprint and card reader and remove the baseplate, as shown by (1) in [Figure 3-100](#).
- Step 2** Mark the mounting holes using a marker, and drill holes using a hammer drill.

Figure 3-99 Marking mounting holes (unit: mm)



Step 3 Install the baseplate, as shown by (3) in [Figure 3-100](#).

Step 4 Route the fingerprint and card reader cable through the cable hole in the baseplate, as shown by (4) in [Figure 3-100](#).

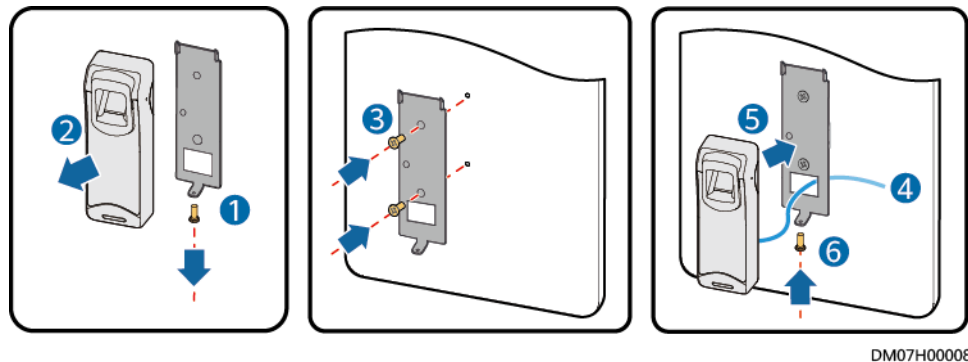
 NOTE

The fingerprint and card reader is connected to the access actuator by a network cable.

Step 5 Check that cables are correctly connected.

Step 6 Secure the fingerprint and card reader to the baseplate, as shown by (5) and (6) in [Figure 3-100](#).

Figure 3-100 Installing a fingerprint and card reader



----End

3.9.6 Installing a Card Reader with a Keypad

Context

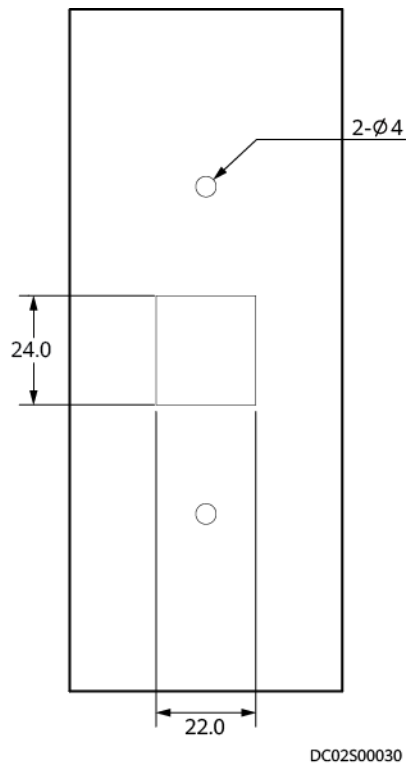
- It is recommended that the product be installed 30–300 mm close to the equipment room door and 1.4–1.6 m above the floor.
- Do not install the product in a place with heavy dust or exposed to sunlight.

Procedure

Step 1 Remove the screws (set aside) from the card reader with a keypad and remove the baseplate, as shown by (1) in [Figure 3-102](#).

Step 2 Mark the mounting holes using a marker, and drill holes using a hammer drill.

Figure 3-101 Marking mounting holes (unit: mm)



Step 3 Install the baseplate, as shown by (3) in [Figure 3-102](#).

Step 4 Route the cable of the card reader with a keypad through the cable hole in the baseplate, as shown by (4) in [Figure 3-102](#).

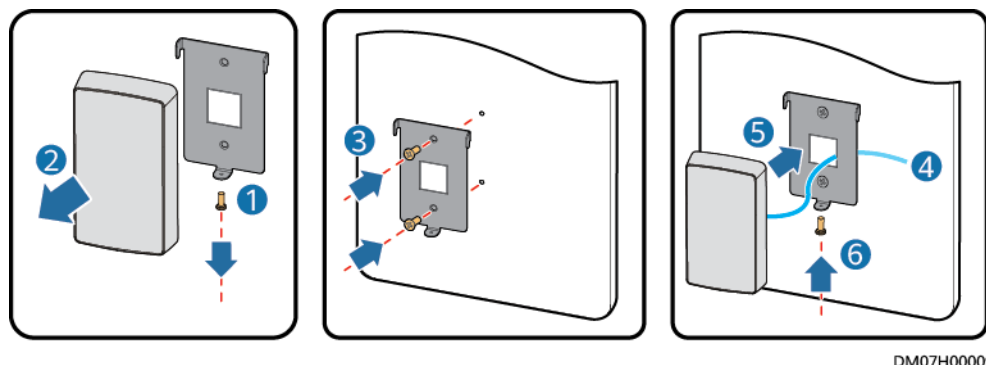
NOTE

The card reader with a keypad is connected to the access actuator by a network cable.

Step 5 Check that cables are correctly connected.

Step 6 Secure the card reader with a keypad to the baseplate, as shown by (5) and (6) in [Figure 3-102](#).

Figure 3-102 Installing a card reader with a keypad



----End

3.9.7 Installing an Exit Button

Procedure

- Step 1** Remove the exit button cover using a flat-head screwdriver.
- Step 2** Remove screws from the exit button, remove the base, and mark mounting holes using the base and a marker.
- Step 3** Drill holes and install the exit button base.
- Step 4** Take out any two of the four core wires and connect them to the NO and COM ports on the exit button.
- Step 5** Route the cable through the cable hole.
- Step 6** Reinstall the exit button and the cover.

----End

3.9.8 Installing an In-room Emergency Door Release Button

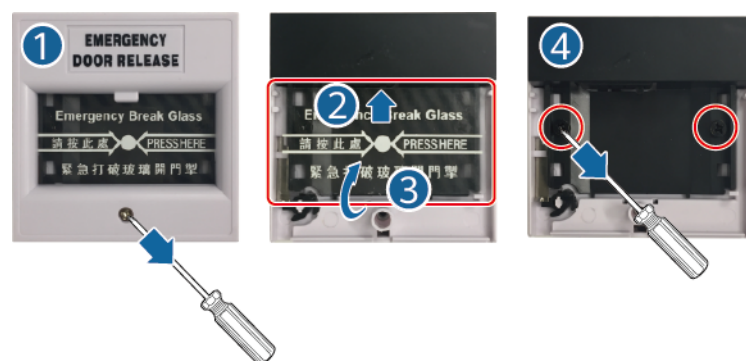
Context

- It is recommended that the button be installed 1.4–1.6 m away from the inner door of the protected area and 1.6 m above the floor.
- The appearance of the emergency door release button is for reference only. The actual appearance may vary.

Procedure

- Step 1** Remove the emergency door release button.

Figure 3-103 Removing an emergency door release button



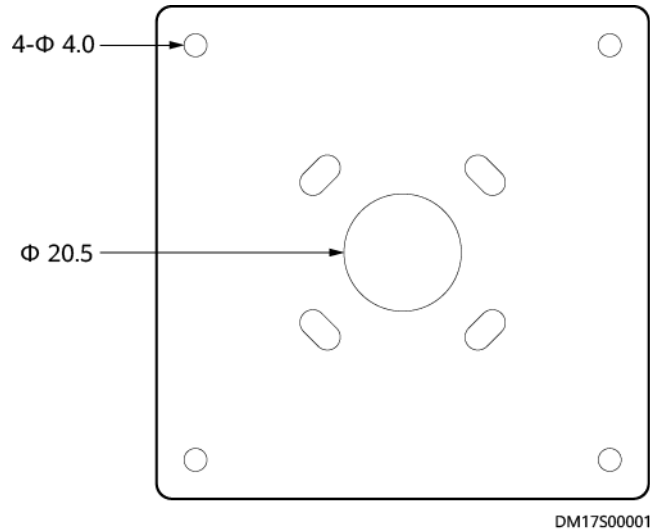
DS27000009

1. Remove screws from the emergency door release button using a Phillips screwdriver, as shown by (1) in [Figure 3-103](#).
2. Remove the glass panel of the emergency door release button, as shown by (2) and (3) in [Figure 3-103](#).

3. Remove screws from the base, and remove the base, as shown by (4) in [Figure 3-103](#).

Step 2 Mark the mounting holes using a marker and the base.

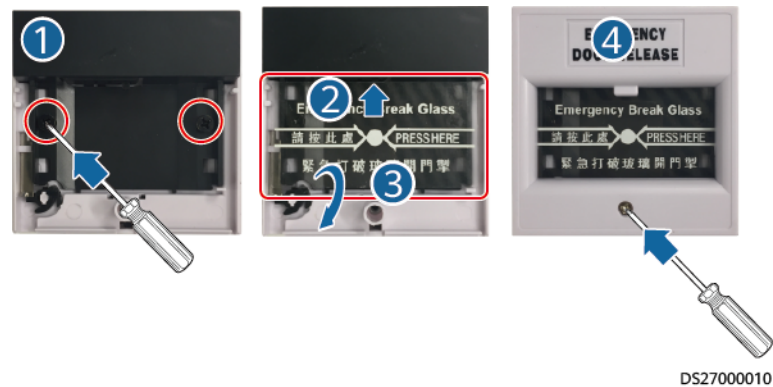
Figure 3-104 Marking mounting holes (unit: mm)



Step 3 Drill holes using a hammer drill, and route cables out of the cable hole.

Step 4 Install the emergency door release button.

Figure 3-105 Installing an emergency door release button



1. Install the base of the emergency door release button, as shown by (1) in [Figure 3-105](#).
2. Install the glass panel of the emergency door release button, as shown by (2) and (3) in [Figure 3-105](#).
3. Tighten screws of the emergency door release button using a Phillips screwdriver, as shown by (4) in [Figure 3-105](#).

----End

4 Connecting Monitoring Cables to Devices

NOTICE

Cable connections specified in this document are based on the cable connection sequences specified in **Preparing a Monitoring Cable**. Connect cables in required sequences by referring to **Preparing a Monitoring Cable** to prevent device connection failures.

Unless otherwise specified, all network cables in this document are crossover cables.

4.1 Scenarios for Connecting a Server

4.1.1 Server Ports (TaiShan 200 Server)

The TaiShan 200 server (Model 2280) is a next-generation data center server developed by Huawei. Based on Huawei Kunpeng processors, the server features efficient computing, high security and reliability, and an open ecosystem. As the monitoring host of the NetEco management system, the server processes and analyzes data.

Figure 4-1 Ports on the TaiShan 200 server (Model 2280)

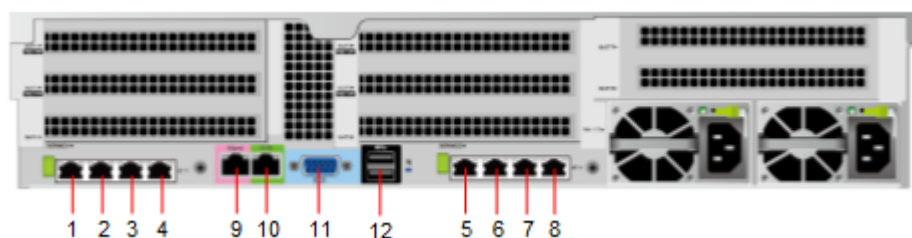


Table 4-1 Description of ports on the TaiShan 200 server (Model 2280)

No.	Port Type	Description
1	eth0 GE port	Used for connecting to the LAN switch. - Scenario where the southbound and northbound networks are not isolated: Connect eth0 and eth1, which are configured as bond0 by default, to provide southbound and northbound services. Connect eth2 and eth3, which are configured as bond1 by default, to provide southbound 2 services. - Scenario where the southbound and northbound networks are isolated: Connect eth0 and eth1, which are configured as bond0 by default, to provide northbound services. Connect eth2 and eth3, which are configured as bond1 by default, to provide southbound services. Connect eth4 and eth5, which are configured as bond2 by default, to provide southbound 2 services.
2	eth1 GE port	
3	eth2 GE port	
4	eth3 GE port	
5	eth4 GE port	
6	eth5 GE port	
7	eth6 GE port	Reserved.
8	eth7 GE port	
9	iBMC remote management port	Used for connecting to a PC to manage the TaiShan 200 server (Model 2280).
10	Server serial port	Used for connecting to an SMS modem or for commissioning.
11	VGA port	Used for connecting to a monitor.
12	USB port	Used for connecting to an external device.

4.1.2 Server Ports (2288X V5 Server)

The 2288X V5 server is a next-generation Huawei data center server that integrates patented technologies such as Dynamic Energy Management Technology (DEMT) and fault diagnosis & management (FDM). It features efficient computing, high security and reliability, and an open ecosystem. Suitable for efficient acceleration of applications such as big data, distributed storage, native applications, high-performance computing, and databases, the server aims to meet the requirements of diversified computing and green computing in data centers.

Figure 4-2 Ports on the 2288X V5 server

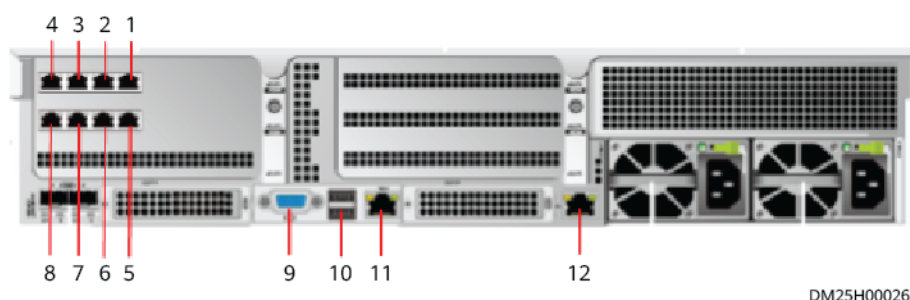


Table 4-2 2288X V5 server port description

No.	Port Type	Description
1	eth0 GE port	Used for connecting to the LAN switch. - Scenario where the southbound and northbound networks are not isolated: Connect eth0 and eth1, which are configured as bond0 by default, to provide southbound and northbound services. Connect eth2 and eth3, which are configured as bond1 by default, to provide southbound 2 services. - Scenario where the southbound and northbound networks are isolated: Connect eth0 and eth1, which are configured as bond0 by default, to provide northbound services. Connect eth2 and eth3, which are configured as bond1 by default, to provide southbound services. Connect eth4 and eth5, which are configured as bond2 by default, to provide southbound 2 services.
2	eth1 GE port	
3	eth2 GE port	
4	eth3 GE port	
5	eth4 GE port	
6	eth5 GE port	
7	eth6 GE port	Reserved.
8	eth7 GE port	
9	VGA port	Used for connecting to a monitor.
10	USB port	Used for connecting to an external device.
11	iBMC remote management port	Used for connecting to a PC to manage the 2288X V5 server.
12	Server serial port	Used for connecting to an SMS modem or for commissioning.

4.1.3 Installing the SMS Modem

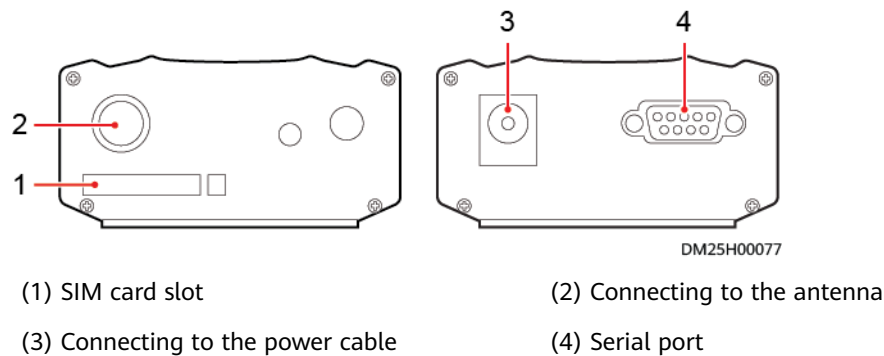
Prerequisites

An idle serial port is available on the server.

Context

Figure 4-3 shows the ports on the SMS modem.

Figure 4-3 Ports on the SMS modem



Procedure

Step 1 Use cable ties to bind the GSM modem to the mounting bar near the server installation position on the rear door of the network cabinet.

Step 2 Insert a SIM card into the SMS modem.

Use a tool such as the small screwdriver to press the yellow key. Put the SIM card on the ejected tray, and insert the tray into the SMS modem.

Step 3 Connect the antenna to the antenna connector.

Step 4 Connect the serial cable.

Connect one end of the serial cable to the modem, and the other end to the transfer cable. Connect the other end of the transfer cable to an idle serial port on the server. For details about the serial ports on the server, see **Server Ports**.

NOTE

For details, see the user manual delivered with the SMS modem.

Use the connector convertor delivered with the SMS modem if the connector of the serial cable does not match the serial port on the server.

Step 5 Connect the power cable.

1. Connect one end of the power adapter to the SMS modem. For details, see the specifications delivered with the SMS modem.
2. Connect the other end of the power adapter to the universal conversion C1 socket.
3. Connect the other end of the universal conversion C1 socket to the rPDU through a transfer cable (C13/C14 cable or China standard C13 cable).

After the power cable is connected, switch on the power. Normally, the indicator of the SMS modem blinks regularly. [Table 4-3](#) describes the relationships between the indicator status and the modem status.

Table 4-3 Relationships between the indicator status and the modem status

Indicator Status	Modem Status
On	The SMS modem is activated and is not registered with the network.
Blinks slowly	The SMS modem is connected to the network and is in idle mode.
Blinks quickly	The SMS modem is in transmission mode.
Off	The SMS modem is deactivated.

Step 6 Install the SMS modem driver.

To install the SMS modem driver, see the specifications delivered with the SMS modem.

 NOTE

You need to install the driver only when the installation of the driver is required in the specifications delivered with the SMS modem.

----End

4.1.4 Connecting Cables to the 4G SMS Modem

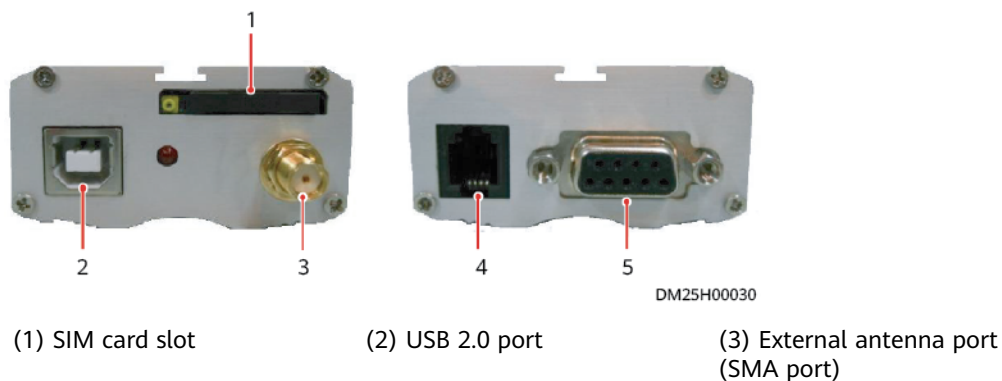
Prerequisites

An idle USB port is available on the server.

Context

The following figure shows the ports on the 4G SMS modem.

Figure 4-4 Ports on the 4G SMS modem



- (4) RJ11 analog audio port (5) RS232 standard serial port -

Procedure

Step 1 Use cable ties to bind the GSM modem to the mounting bar near the server installation position on the rear door of the network cabinet.

Step 2 Insert a SIM card into the 4G SMS modem.

Use a tool such as the small screwdriver to press the yellow key. Put the SIM card on the ejected tray, and insert the tray into the SMS modem.

Step 3 Connect the antenna to the antenna connector.

Step 4 Connect the serial cable.

Connect one end of the serial cable to the modem, and the other end to the transfer cable. Connect the other end of the transfer cable to an idle serial port on the server. For details about the serial ports on the server, see **Server Ports**.

NOTE

Use the connector convertor delivered with the SMS modem if the connector of the serial cable does not match the serial port on the server.

Step 5 Connect the power cable.

1. Connect one end of the USB cable to the USB 2.0 port on the modem.
2. Connect the other end of the power adapter to the universal conversion C1 socket.
3. Connect the other end of the universal conversion C1 socket to the rPDU through a transfer cable (C13/C14 cable or China standard C13 cable).

After the power cable is connected, turn on the power supply. The modem indicator should blink regularly. [Table 4-4](#) describes the relationships between the indicator status and the modem status.

Table 4-4 Relationships between the indicator status and the modem status

Indicator Status	Modem Status
On	The modem is searching for a network or a call is set up.
Blinks at intervals of 800 ms	The modem is connected to the network.
Blinks at intervals of 200 ms	The modem is transmitting data.
Off	The modem is powered off.

NOTE

For details about how to connect the modem, see the product manual delivered with the modem.

- Step 6** Install the SMS modem driver.
- To install the SMS modem driver, see the specifications delivered with the SMS modem.
- End

4.2 Scenarios for Connecting a LAN Switch

4.2.1 LAN Switch Introduction (S5320-28X-PWR-SI)

Figure 4-5 Ports on the LAN switch

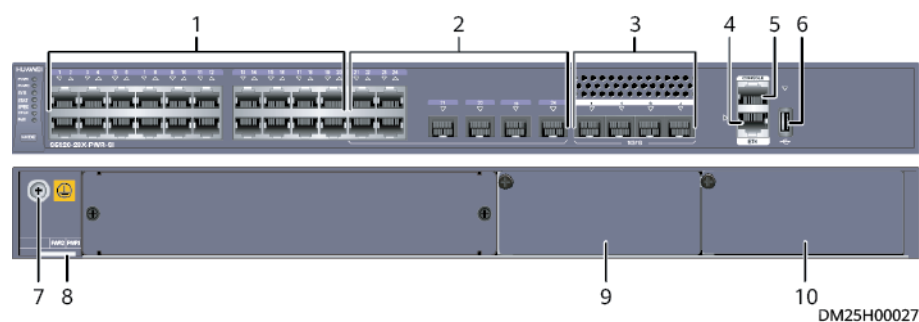


Table 4-5 LAN switch port description

No.	Description
1	Twenty PoE+ 10/100/1000BASE-T Ethernet electrical ports
2	Four combo ports (10/100/1000BASE-T (PoE+) + 100/1000BASE-X) Combo optical ports support the following modules: - FE optical module - GE optical module - GE-CWDM optical module - GE-DWDM optical module

No.	Description
3	Four 10GE SFP+ Ethernet optical ports Modules and cables supported: • GE optical module • GE-CWDM optical module • GE-DWDM optical module • GE optical/electrical module (supporting only the rate of 1000 Mbit/s) • 10GE SFP+ optical module (OSXD22N00 not supported) • 10GE-CWDM optical module • 10GE-DWDM optical module • 1 m, 3 m, 5 m, and 10 m SFP+ high-speed cables • 3 m and 10 m AOC cables • 0.5 m and 1.5 m SFP+ dedicated stack cables (used for zero-configuration stacking, supported in V200R011C10 and later versions)
4	One ETH management port
5	One console port NOTE The port needs to be used with a console cable. A console cable is not delivered with the device and needs to be purchased separately if required.
6	One USB port
7	Ground screw NOTE The screw needs to be used with a ground cable.
8	Serial number label NOTE The LAN switch can be pulled out to check its serial number and MAC address.
9	Power module slot 2 NOTE Supported power modules: • 500 W AC PoE power module • 650 W DC PoE power module
10	Power module slot 1 NOTE Supported power modules: • 500 W AC PoE power module • 650 W DC PoE power module

Table 4-6 Technical specifications

Item	Specifications
Dimensions (H x W x D)	44.4 mm x 442.0 mm x 420.0 mm
Memory (RAM)	512 MB
Flash	240 MB
Mean time between failures (MTBF)	66.78 years
Mean time to repair (MTTR)	2 hours
Availability	> 0.99999
Service port surge protection	Common mode: ± 6 kV
Power port surge protection	500 W AC power module: ± 6 kV in differential mode, ± 6 kV in common mode 650 W DC power module: ± 2 kV in differential mode, ± 4 kV in common mode
Weight (including packing materials)	9.3 kg
Stack port	GE electrical ports and 10GE SFP+ optical ports on the front panel (excluding combo ports)
RTC	Supported
RPS	Not supported
PoE	Supported
Rated voltage range	AC input: 100–240 V AC; 50/60 Hz DC input: –48 V DC to –60 V DC
Maximum voltage range	AC input: 90–264 V AC; 47–63 Hz DC input: –38.4 V DC to –72 V DC
Maximum power consumption (100% traffic, full fan speed)	- Without PoE: 56.1 W - Full PoE load: 913 W (device power consumption: 173 W; PoE: 740 W)

Item	Specifications
Typical power consumption (30% traffic) • Tested according to the ATIS standard • EEE function enabled • No PoE power consumption	31.8 W
Operating temperature range	0–45°C (altitude: 0–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m.
Short-term operating temperature range	–5°C to +50°C (altitude: 0–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m. The device can work for a short period of time when the operating temperature is outside the normal range, but the following conditions must be met: • The consecutive hours during which the operating temperature exceeds 45°C does not exceed 96 in a year. • The total time when the operating temperature exceeds 45°C in a year is less than or equal to 360 hours. • The number of times that the operating temperature exceeds 45°C is less than or equal to 15 in a year. If any of the preceding conditions is not met, the device may be damaged or an unknown error may occur. The device cannot be started when the ambient temperature is lower than 0°C. During short-term operation, the maximum distance of optical modules cannot exceed 10 km.
Storage temperature range	–40°C to +70°C
Noise at room temperature (27°C, sound power)	< 56.5 dB(A)
Relative humidity	5%–95% RH (non-condensing)
Operating altitude	0–5000 m
Product certification	• EMC certification • Safety certification • Production certification

4.2.2 LAN Switch Introduction (S5720-28X-PWR-SI)

Figure 4-6 Ports on the LAN switch

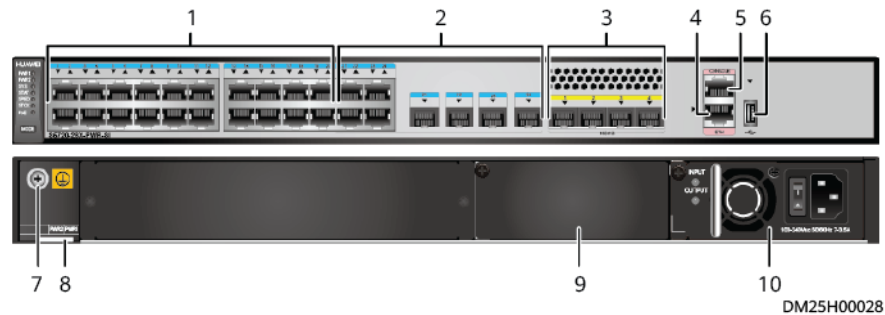


Table 4-7 LAN switch port description

No.	Description
1	Twenty PoE+ 10/100/1000BASE-T Ethernet electrical ports
2	Four combo ports (10/100/1000BASE-T (PoE+) + 100/1000BASE-X) Combo optical ports support the following modules: • FE optical module • GE optical module • GE-CWDM optical module • GE-DWDM optical module
3	Four 10GE SFP+ Ethernet optical ports Modules and cables supported: • GE optical module • GE-CWDM optical module • GE-DWDM optical module • GE optical/electrical module (supporting only the rate of 1000 Mbit/s) • 10GE SFP+ optical module (OSXD22N00 not supported) • 10GE-CWDM optical module • 10GE-DWDM optical module (supported in V200R009C00 and later versions) • 1 m, 3 m, and 10 m SFP+ high-speed cables • 5 m SFP+ high-speed cables (supported in V200R009C00 and later versions) • 3 m and 10 m AOC cables
4	One ETH management port

No.	Description
5	One console port NOTE The port needs to be used with a console cable. A console cable is not delivered with the device and needs to be purchased separately if required.
6	One USB port
7	Ground screw NOTE The screw needs to be used with a ground cable.
8	Serial number label NOTE The LAN switch can be pulled out to check its serial number and MAC address.
9	Power module slot 2 NOTE Supported power modules: • 500 W AC PoE power module • 650 W DC PoE power module
10	Power module slot 1 NOTE Supported power modules: • 500 W AC PoE power module • 650 W DC PoE power module

Table 4-8 Technical specifications

Item	Specifications
Dimensions (H x W x D)	44.4 mm x 442.0 mm x 420.0 mm
Memory (RAM)	512 MB
Flash	240 MB
MTBF	66.78 years
MTTR	2 hours
Availability	> 0.99999
Service port surge protection	Common mode: ± 6 kV

Item	Specifications
Power port surge protection	500 W AC power module: ± 6 kV in differential mode, ± 6 kV in common mode 650 W DC power module: ± 2 kV in differential mode, ± 4 kV in common mode
Weight (including packing materials)	9.3 kg
Stack port	GE electrical ports and 10GE SFP+ optical ports on the front panel (excluding combo ports)
RTC	Supported
RPS	Not supported
PoE	Supported
Rated voltage range	AC input: 100–240 V AC; 50/60 Hz DC input: –48 V DC to –60 V DC
Maximum voltage range	AC input: 90–264 V AC; 47–63 Hz DC input: –38.4 V DC to –72 V DC
Maximum power consumption (100% traffic, full fan speed)	- Without PoE: 56.1 W - Full PoE load: 913 W (device power consumption: 173 W; PoE: 740 W)
Typical power consumption (30% traffic) - Tested according to the ATIS standard - EEE function enabled - No PoE power consumption	31.8 W
Operating temperature range	0–45°C (altitude: 0–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m.

Item	Specifications
Short-term operating temperature range	–5°C to +50°C (altitude: 0–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m. The device can work for a short period of time when the operating temperature is outside the normal range, but the following conditions must be met: • The consecutive hours during which the operating temperature exceeds 45°C does not exceed 96 in a year. • The total time when the operating temperature exceeds 45°C in a year is less than or equal to 360 hours. • The number of times that the operating temperature exceeds 45°C is less than or equal to 15 in a year. If any of the preceding conditions is not met, the device may be damaged or an unknown error may occur. The device cannot be started when the ambient temperature is lower than 0°C. During short-term operation, the maximum distance of optical modules cannot exceed 10 km.
Storage temperature range	–40°C to +70°C
Noise at room temperature (27°C, sound power)	< 56.5 dB(A)
Relative humidity	5%–95% RH (non-condensing)
Operating altitude	0–5000 m
Product certification	• EMC certification • Safety certification • Production certification

4.2.3 LAN Switch Introduction (S5331-H24P4XC)

Figure 4-7 Ports on the LAN switch

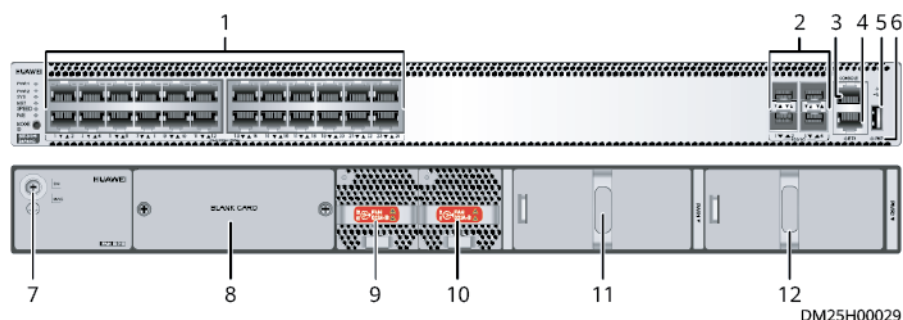


Table 4-9 LAN switch port description

No.	Description
1	Twenty-four 10/100/1000BASE-T PoE+ Ethernet electrical ports
2	Four 10GE SFP+ Ethernet optical ports Modules and cables supported: • GE optical module • GE-CWDM optical module • GE-DWDM optical module • GE optical/electrical module (supporting 100M/1000M auto-negotiation) • 10GE SFP+ optical module (OSXD22N00 not supported) • 10GE-CWDM optical module • 10GE-DWDM optical module • 1 m, 3 m, 5 m, and 10 m SFP+ high-speed cables • 3 m and 10 m SFP+ AOC cables • 0.5 m and 1.5 m SFP+ dedicated stack cables (used for zero-configuration stacking)
3	One console port
4	One ETH management port
5	One USB port
6	One PNP button NOTE • Holding down the button for more than 6s restores the factory settings and resets the device. • Pressing the button resets the device. • Resetting the device will interrupt services. Exercise caution when using this button.
7	Ground screw
8	Rear card slot
9	Fan module slot 1
10	Fan module slot 2
11	Power module slot 1
12	Power module slot 2

Table 4-10 Technical specifications

Item	Specifications
Memory (RAM)	4 GB
Flash	Physical space: 1 GB. To view the actual available space, run display version .
MTBF	57.21 years
MTTR	2 hours
Availability	> 0.99999
Service port surge protection	Common mode: ± 6 kV
Power port surge protection	Differential mode: ± 6 kV; common mode: ± 6 kV
Dimensions (H x W x D)	- Basic dimensions (the depth excludes the protruding parts of the front and rear panels): 43.6 mm x 442.0 mm x 420.0 mm - Maximum dimensions (the depth is the maximum distance from the protruding port on the front panel to the module handle on the rear panel): 43.6 mm x 442.0 mm x 448.0 mm
Weight (including packing materials)	8.6 kg
Stack port	10GE SFP+ ports on the front panel and ports on the rear card
RTC	Supported
RPS	Not supported
PoE	Supported
Rated voltage range	- AC input: 100–130 V AC, 200–240 V AC; 50/60 Hz - High-voltage DC input: 240 V DC
Maximum voltage range	- AC input: 90–290 V AC; 45–65 Hz - High-voltage DC input: 190–290 V DC
Maximum power consumption (100% traffic, full fan speed)	- Without PoE: 121 W (without cards) - Full PoE load: 977 W (PoE: 720 W, without cards)
Typical power consumption (30% traffic, tested according to the ATIS standard)	95 W (without cards)

Item	Specifications
Operating temperature range	-5°C to +45°C (altitude: 0 m–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m. The device cannot be started when the ambient temperature is lower than 0°C.
Storage temperature range	-40°C to +70°C
Noise at room temperature (27°C, sound power)	< 62.3 dB(A)
Relative humidity	5%–95% RH (non-condensing)
Operating altitude	0–5000 m
Product certification	• EMC certification • Safety certification • Production certification

4.2.4 LAN Switch Introduction (S5731-H24P4XC)

Figure 4-8 Ports on the LAN switch

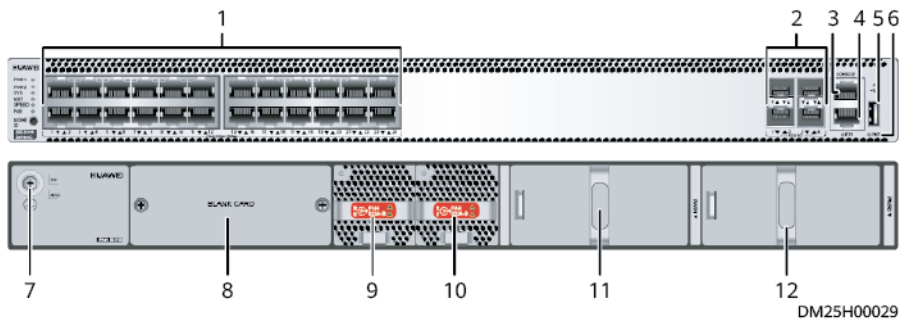


Table 4-11 LAN switch port description

No.	Description
1	Twenty-four 10/100/1000BASE-T PoE+ Ethernet electrical ports

No.	Description
2	Four 10GE SFP+ Ethernet optical ports Modules and cables supported: • GE optical module • GE-CWDM optical module • GE-DWDM optical module • GE optical/electrical module (supporting 100M/1000M auto-negotiation) • 10GE SFP+ optical module (OSXD22N00 not supported) • 10GE-CWDM optical module • 10GE-DWDM optical module • 1 m, 3 m, 5 m, and 10 m SFP+ high-speed cables • 3 m and 10 m SFP+ AOC cables • 0.5 m and 1.5 m SFP+ dedicated stack cables (used for zero-configuration stacking)
3	One console port
4	One ETH management port
5	One USB port
6	One PNP button NOTE • Holding down the button for more than 6s restores the factory settings and resets the device. • Pressing the button resets the device. • Resetting the device will interrupt services. Exercise caution when using this button.
7	Ground screw
8	Rear card slot
9	Fan module slot 1
10	Fan module slot 2
11	Power module slot 1
12	Power module slot 2

Table 4-12 Technical specifications

Item	Specifications
Memory (RAM)	4 GB

Item	Specifications
Flash	Physical space: 1 GB. To view the actual available space, run display version .
MTBF	57.21 years
MTTR	2 hours
Availability	> 0.99999
Service port surge protection	Common mode: ± 6 kV
Power port surge protection	Differential mode: ± 6 kV; common mode: ± 6 kV
Dimensions (H x W x D)	- Basic dimensions (the depth excludes the protruding parts of the front and rear panels): 43.6 mm x 442.0 mm x 420.0 mm - Maximum dimensions (the depth is the maximum distance from the protruding port on the front panel to the module handle on the rear panel): 43.6 mm x 442.0 mm x 448.0 mm
Weight (including packing materials)	8.6 kg
Stack port	10GE SFP+ ports on the front panel and ports on the rear card
RTC	Supported
RPS	Not supported
PoE	Supported
Rated voltage range	- AC input: 100–130 V AC, 200–240 V AC; 50/60 Hz - High-voltage DC input: 240 V DC
Maximum voltage range	- AC input: 90–290 V AC; 45–65 Hz - High-voltage DC input: 190–290 V DC
Maximum power consumption (100% traffic, full fan speed)	- Without PoE: 121 W (without cards) - Full PoE load: 977 W (PoE: 720 W, without cards)
Typical power consumption (30% traffic, tested according to the ATIS standard)	95 W (without cards)

Item	Specifications
Operating temperature range	-5°C to +45°C (altitude: 0–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m. The device cannot be started when the ambient temperature is lower than 0°C.
Storage temperature range	-40°C to +70°C
Noise at room temperature (27°C, sound power)	< 62.3 dB(A)
Relative humidity	5%–95% RH (non-condensing)
Operating altitude	0–5000 m
Product certification	• EMC certification • Safety certification • Production certification

4.2.5 Introduction to Switches (S5335-S24P4X)

Exterior and interior

Figure 4-9 Appearance of the S5335-S24P4X

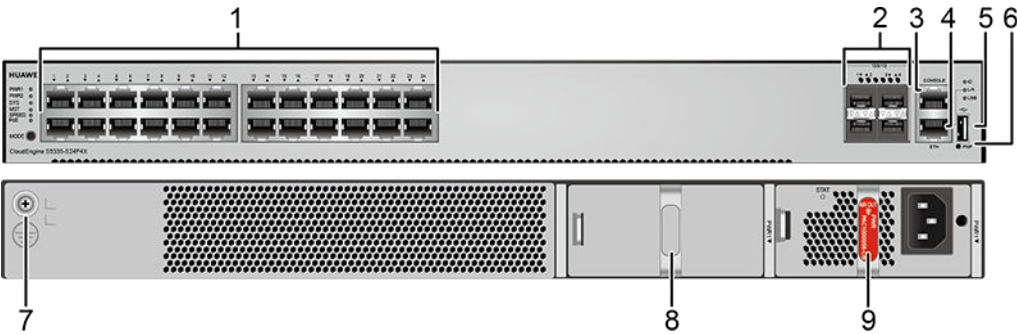


Table 4-13 S5335-S24P4X description

No.	Description
1	Twenty-four 10/100/1000 BASE-T Ethernet electrical ports

No.	Description
2	Four 10GE SFP+ Ethernet optical ports Modules and cables supported: • GE optical module • GE-CWDM optical module • GE-DWDM optical module • GE optical/electrical module (supporting 100M/1000M auto-negotiation) • 10GE SFP+ optical module (OSXD22N00 not supported) • 10GE-CWDM optical module • 10GE-DWDM optical module • 1 m and 3 m SFP+ high-speed cables • 3 m and 10 m SFP+ AOC cables • 0.5 m and 1.5 m SFP+ dedicated stack cables (used for zero-configuration stacking)
3	One console port
4	One ETH management port
5	One USB port
6	One PNP button NOTICE • Holding down the button for more than 6s restores the factory settings and resets the device. • Pressing the button resets the device. • Resetting the device will interrupt services. Exercise caution when using this button.
7	Ground screw NOTE The screw needs to be used with a ground cable.
8	Power module slot 1 NOTE Supported power module: 1000 W AC PoE power module (PAC1000S56-CB)
9	Power module slot 2 NOTE Supported power module: 1000 W AC PoE power module (PAC1000S56-CB)

Item

lists technical specifications of the S5335-S24P4X.

Table 4-14 Technical specifications

Specifications	Specifications
Memory (RAM)	1 GB
Flash	Physical space: 512 MB. To view the actual available space, run display version .
MTBF	59.88
MTTR	2
Availability	> 0.99999
Service port surge protection	Common mode: ± 7 kV (The maximum voltage is ± 10 kV, and the device is not damaged.)
Power port surge protection	Differential mode: ± 6 kV; common mode: ± 6 kV
Dimensions (H x W x D)	- Basic dimensions (the depth excludes the protruding parts of the front and rear panels): 43.6 mm x 442.0 mm x 420.0 mm - Maximum dimensions (the depth is the maximum distance from the protruding port on the front panel to the module handle on the rear panel): 43.6 mm x 442.0 mm x 444.2 mm
Weight (including packing materials)	7.39 kg
Stack port	Any 10/100/1000BASE-T Ethernet electrical port or 10GE SFP + Ethernet optical port
RTC	Supported
RPS	Not supported
PoE	Supported
Rated voltage range	- AC input: 100–240 V AC; 50/60 Hz - High-voltage DC input: 240 V DC
Maximum voltage range	- AC input: 90–290 V AC; 45–65 Hz - High-voltage DC input: 190–290 V DC
Maximum power consumption (100% traffic, full fan speed)	- Without PoE: 65 W - Full PoE load: 847 W (PoE: 720 W)

Specifications	Specifications
Typical power consumption (30% traffic) • Tested according to the ATIS standard • EEE function enabled • No PoE power consumption	51 W
Operating temperature range	-5°C to +50°C (altitude: 0–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m. The device cannot be started when the ambient temperature is lower than 0°C.
Short-term operating temperature range	-5°C to +55°C (altitude: 0–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m. The device can work for a short period of time when the operating temperature is outside the normal range, but the following conditions must be met: • The consecutive hours during which the operating temperature exceeds 45°C does not exceed 96 in a year. • The total time when the operating temperature exceeds 45°C in a year is less than or equal to 360 hours. • The number of times that the operating temperature exceeds 45°C is less than or equal to 15 in a year. If any of the preceding conditions is not met, the device may be damaged or an unknown error may occur. The device cannot be started when the ambient temperature is lower than 0°C. During short-term operation, the maximum distance of optical modules cannot exceed 10 km.
Storage temperature range	-40°C to +70°C
Noise at room temperature (27°C, sound power)	< 58.9 dB (A)
Relative humidity	5%–95% RH (non-condensing)
Operating altitude	0–5000 m

Specifications	Specifications
Product certification	• EMC certification • Safety certification • Production certification
Item Code	98010910

4.2.6 Introduction to Switches (S5735-S24P4X)

Exterior and interior

Figure 4-10 Appearance of the S5735-S24P4X

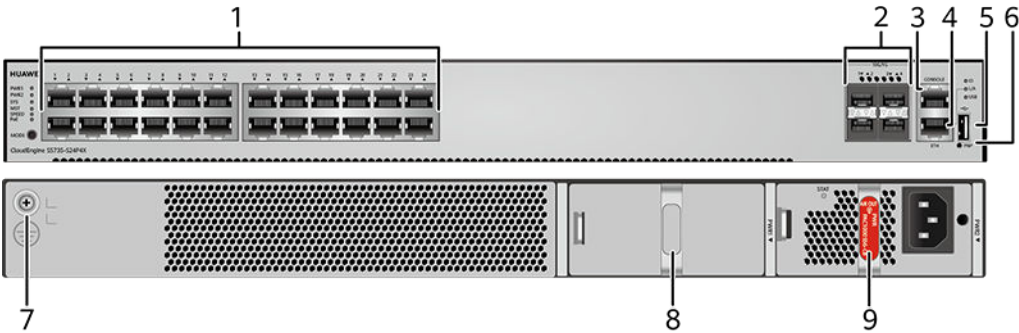


Table 4-15 S5735-S24P4X description

No.	Description
1	Twenty-four 10/100/1000 BASE-T Ethernet electrical ports
2	Four 10GE SFP+ Ethernet optical ports Modules and cables supported: • GE optical module • GE-CWDM optical module • GE-DWDM optical module • GE optical/electrical module (supporting 100M/1000M auto-negotiation) • 10GE SFP+ optical module (OSXD22N00 not supported) • 10GE-CWDM optical module • 10GE-DWDM optical module • 1 m and 3 m SFP+ high-speed cables • 3 m and 10 m SFP+ AOC cables • 0.5 m and 1.5 m SFP+ dedicated stack cables (used for zero-configuration stacking)
3	One console port

No.	Description
4	One ETH management port
5	One USB port
6	One PNP button NOTICE - Holding down the button for more than 6s restores the factory settings and resets the device. - Pressing the button resets the device. - Resetting the device will interrupt services. Exercise caution when using this button.
7	Ground screw NOTE The screw needs to be used with a ground cable.
8	Power module slot 1 NOTE Supported power module: 1000 W AC PoE power module (PAC1000S56-CB)
9	Power module slot 2 NOTE Supported power module: 1000 W AC PoE power module (PAC1000S56-CB)

Item

lists technical specifications of the S5735-S24P4X.

Table 4-16 Technical specifications

Specifications	Specifications
Memory (RAM)	1 GB
Flash	Physical space: 512 MB. To view the actual available space, run display version .
MTBF	59.88
MTTR	2
Availability	> 0.99999
Service port surge protection	Common mode: ± 7 kV (The maximum voltage is ± 10 kV, and the device is not damaged.)
Power port surge protection	Differential mode: ± 6 kV; common mode: ± 6 kV

Specifications	Specifications
Dimensions (H x W x D)	- Basic dimensions (the depth excludes the protruding parts of the front and rear panels): 43.6 mm x 442.0 mm x 420.0 mm - Maximum dimensions (the depth is the maximum distance from the protruding port on the front panel to the module handle on the rear panel): 43.6 mm x 442.0 mm x 444.2 mm
Weight (including packing materials)	7.39 kg
Stack port	Any 10/100/1000BASE-T Ethernet electrical port or 10GE SFP + Ethernet optical port
RTC	Supported
RPS	Not supported
PoE	Supported
Rated voltage range	- AC input: 100–240 V AC; 50/60 Hz - High-voltage DC input: 240 V DC
Maximum voltage range	- AC input: 90–290 V AC; 45–65 Hz - High-voltage DC input: 190–290 V DC
Maximum power consumption within the maximum voltage range (100% traffic, full speed of fans)	- Without PoE: 65 W - Full PoE load: 847 W (PoE: 720 W)
Typical power consumption (30% traffic) - Tested according to the ATIS standard - EEE function enabled - No PoE power consumption	51 W

Specifications	Specifications
Operating temperature range	-5°C to +50°C (altitude: 0–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m. The device cannot be started when the ambient temperature is lower than 0°C.
Short-term operating temperature range	-5°C to +55°C (altitude: 0–1800 m) NOTE When the altitude ranges from 1800 m to 5000 m, the highest temperature decreases by 1°C for each additional 220 m. The device can work for a short period of time when the operating temperature is outside the normal range, but the following conditions must be met: • The consecutive hours during which the operating temperature exceeds 45°C does not exceed 96 in a year. • The total time when the operating temperature exceeds 45°C in a year is less than or equal to 360 hours. • The number of times that the operating temperature exceeds 45°C is less than or equal to 15 in a year. If any of the preceding conditions is not met, the device may be damaged or an unknown error may occur. The device cannot be started when the ambient temperature is lower than 0°C. During short-term operation, the maximum distance of optical modules cannot exceed 10 km.
Storage temperature range	-40°C to +70°C
Noise at room temperature (27°C, sound power)	< 58.9 dB (A)
Relative humidity	5%–95% RH (non-condensing)
Operating altitude	0–5000 m
Product certification	• EMC certification • Safety certification • Production certification
Item Code	98010940

4.2.7 Connecting a Monitoring Cable to the NetEco

For details, see *iMaster NetEco 6000 V600R021C00 Management System Wiring Diagram*.

4.2.8 Connecting the Video Management System Cable

4.2.8.1 Connecting a Monitoring Cable to a VCN510

Prerequisites

A network cable used for monitoring is prepared.

Procedure

- Step 1** Use a Phillips screwdriver to connect one end of the PGND cable to the ground terminal of the device, and connect the other end to the ground point of the cabinet or work station. The ground screw uses M4 screws. The PGND cable is prepared by the customer. The PGND cable is green and yellow, and its diameter must range from 16 AWG to 18 AWG.

 NOTE

The customer needs to prepare the ground cable.

- Step 2** Connect one end of the network cable to any GE network port on the VCN510.

Figure 4-11 VCN510 ports



(1) Ground terminal	(2) GE1 port	(3) GE2 port
(4) Power button	(5) Power port	

- Step 3** Connect the other end to the Ethernet port on the LAN switch.

----End

4.2.8.2 Connecting a Monitoring Cable to a VCN520

Prerequisites

A network cable used for monitoring is prepared.

Procedure

- Step 1** Use a Phillips screwdriver to connect one end of the PGND cable to the ground terminal of the device, and connect the other end to the ground point of the cabinet or work station. The ground screw uses M4 screws. The PGND cable is

prepared by the customer. The PGND cable is green and yellow, and its diameter must range from 16 AWG to 18 AWG.

NOTE

The customer needs to prepare the ground cable.

Step 2 Connect one end of the network cable to any GE network port on the VCN520.

Figure 4-12 VCN520 ports



(1) Ground terminal

(2) GE1 port

(3) GE2 port

(4) Power button

(5) Power port

Step 3 Connect the other end to the Ethernet port on the LAN switch.

----End

4.2.8.3 Connecting a Monitoring Cable to a VCN540

Prerequisites

A network cable used for monitoring is prepared.

Procedure

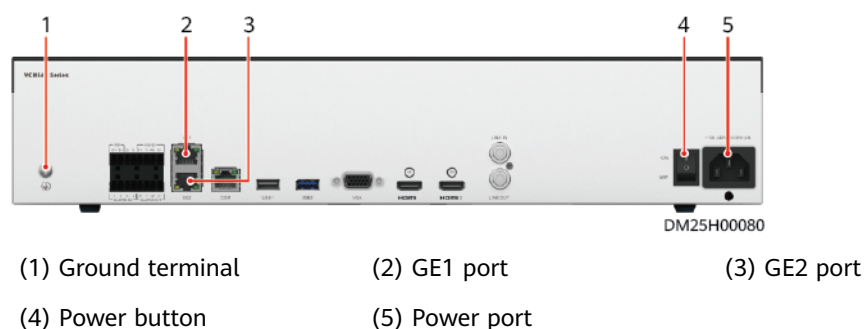
Step 1 Use a Phillips screwdriver to connect one end of the PGND cable to the ground terminal of the device, and connect the other end to the ground point of the cabinet or work station. The ground screw uses M4 screws. The PGND cable is prepared by the customer. The PGND cable is green and yellow, and its diameter must range from 16 AWG to 18 AWG.

NOTE

The customer needs to prepare the ground cable.

Step 2 Connect one end of the network cable to any GE network port on the VCN540.

Figure 4-13 VCN540 ports



Step 3 Connect the other end to the Ethernet port on the LAN switch.

----End

4.2.8.4 Connecting a Monitoring Cable to the IVS1800

Prerequisites

A network cable used for monitoring is prepared.

Procedure

Step 1 Connect one end of the network cable to any GE network port on the IVS1800.

Step 2 Connect the other end of the network cable to the Ethernet port on the LAN switch.

----End

4.2.8.5 Connecting a Monitoring Cable to a Camera

Prerequisites

- A network cable used for monitoring is prepared.
- An idle network port supporting the PoE function is available on the LAN switch.
- The camera has the PoE function.

Procedure

Step 1 Connect the monitoring port on the camera to any network port on the switch by using the network cable. The switch is powered by using the PoE technology.

NOTICE

Device cables not mentioned in the document do not need to be connected onsite and should be insulated only.

----End

4.2.9 Connecting the Smart Cooling Product Monitoring Cable

Prerequisites

A network cable used for monitoring is prepared.

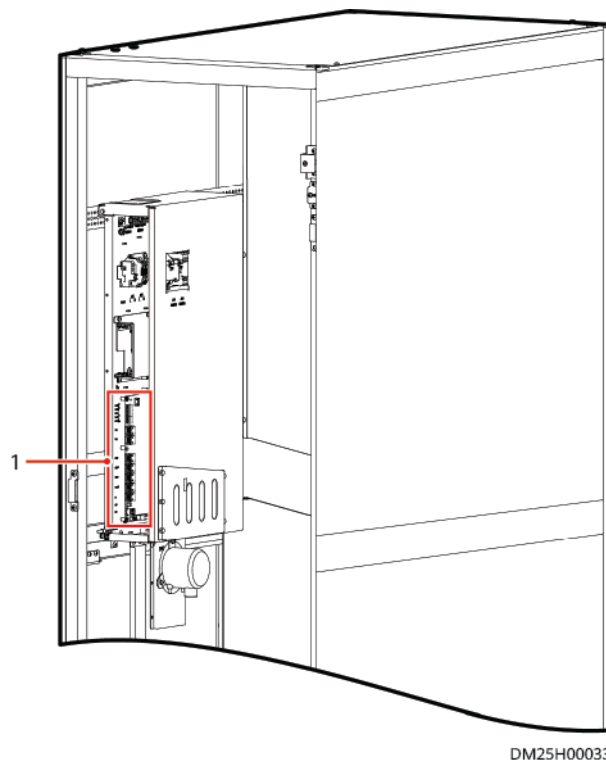
Context

When NetCol5000-C(065, 080), NetCol5000-A050/A042/A035/A020/C030/C070/C150, NetCol8000-A060/A120, or FusionCol8000-E220/E400/C080/C210 connects to the NetEco over Modbus TCP, connect cables by referring to this section.

Procedure

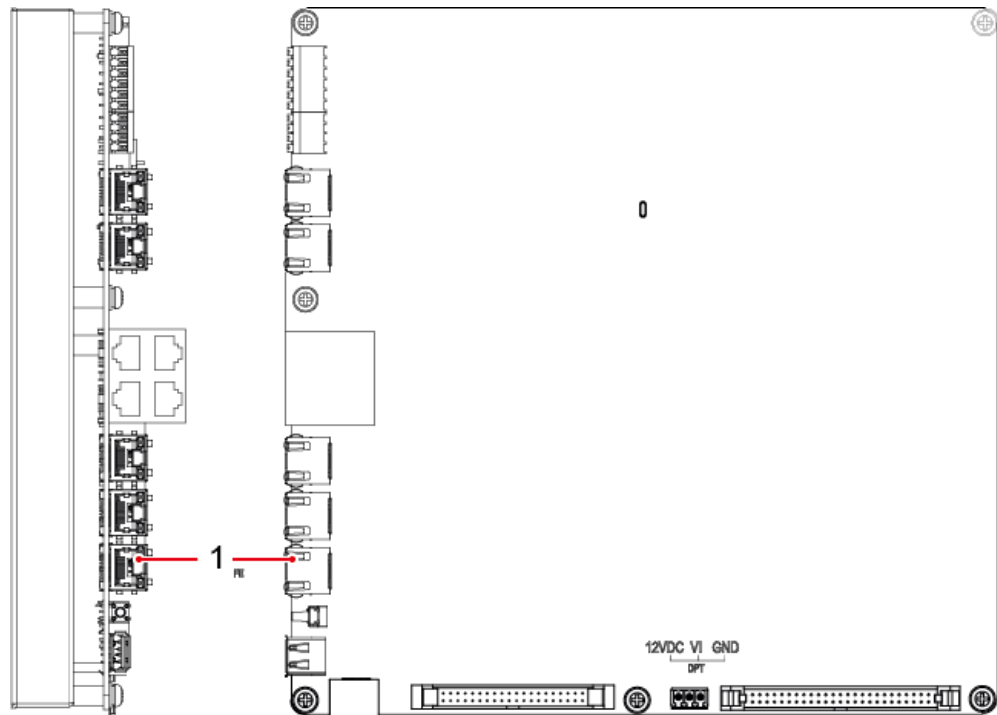
- Step 1** Connect one end of the network cable to the monitoring port on the smart cooling product.
- For NetCol5000-C(065, 080), open the rear door, and connect one end of the network cable to the FE port on the main control board of the smart cooling product.

Figure 4-14 NetCol5000-C(065, 080) main control board



(1) Main control board

Figure 4-15 Main control board

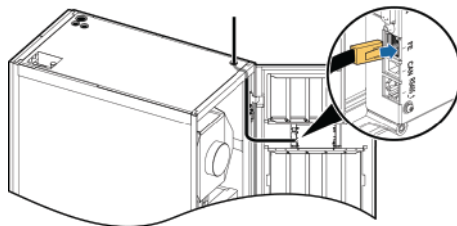


DM25H00047

(1) FE port

- For NetCol5000-A020, open the front door, and connect one end of the network cable to the FE port on the side of the smart cooling product LCD.

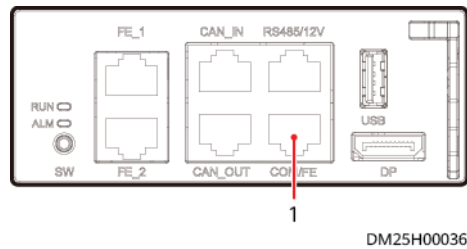
Figure 4-16 FE ports on the NetCol5000-A020



DM25H00035

- For NetCol5000-A050, NetCol5000-A042, NetCol5000-A035, NetCol8000-C070, NetCol8000-C150, NetCol8000-A060/A120, and FusionCol8000-E220/E400/C080/C210, open the rear door, and connect one end of the network cable to the COM/FE port on the main control module of the smart cooling product.

Figure 4-17 Main control module



(1) COM/FE port

Step 2 Connect the other end of the network cable to the Ethernet port on the LAN switch.

----End

4.2.10 Connecting the UPS Monitoring Cable

4.2.10.1 Connecting the UPS2000-G Monitoring Cable (SNMP)

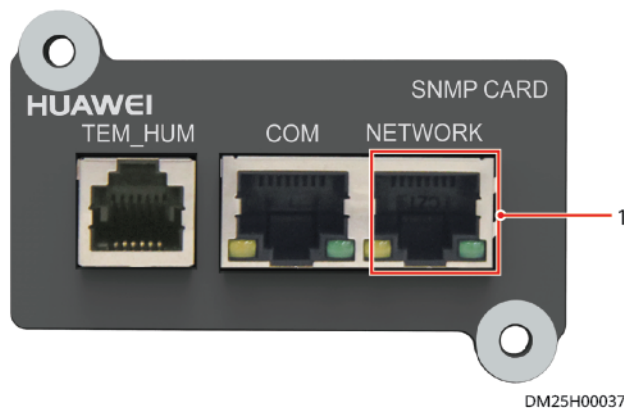
Prerequisites

A network cable used for monitoring is prepared.

Procedure

Step 1 Connect one end of a network cable to the Ethernet port on the SNMP card of the UPS2000-G.

Figure 4-18 Ethernet port



(1) Ethernet port

Step 2 Connect the other end of the network cable to the Ethernet port on the LAN switch.

----End

4.2.10.2 Connecting the UPS5000-A Monitoring Cable

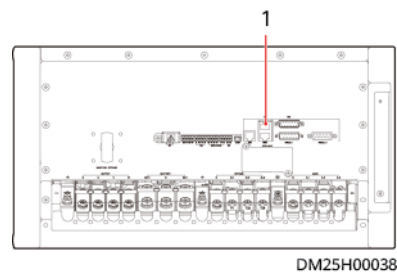
Prerequisites

A network cable used for monitoring is prepared.

Procedure

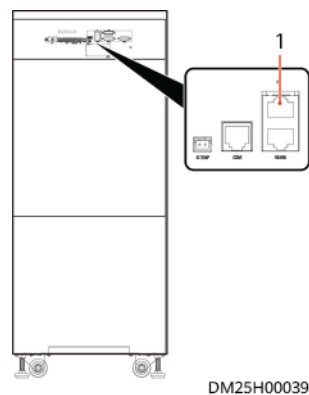
Step 1 Connect one end of a network cable to the FE port of the UPS5000-A.

Figure 4-19 UPS5000-A-30 kVA/40 kVA functional components and control signal ports



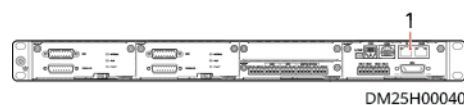
(1) FE port

Figure 4-20 UPS5000-A-60 kVA/80 kVA/120 kVA functional components and control signal ports



(1) FE port

Figure 4-21 FE port on the UPS monitoring module of the 300 kVA UPS and models with higher capacities



(1) FE port

Step 2 Connect the other end of the network cable to the Ethernet port on the LAN switch.

----End

4.2.10.3 Connecting a Monitoring Cable to the UPS5000-E/UPS5000-H/UPS5000-S

Prerequisites

A network cable used for monitoring is prepared.

Procedure

- Step 1** Connect one end of a network cable to the FE port on the UPS5000-E/UPS5000-H/UPS5000-S monitoring card.
 - Step 2** Connect the other end of the network cable to the Ethernet port on the LAN switch.
- End

4.2.11 Connecting the SmartLi Monitoring Cable

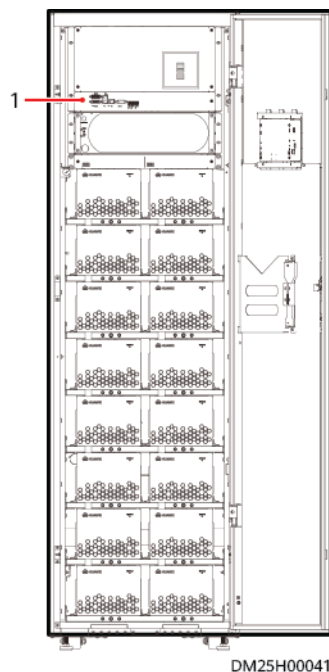
Prerequisites

A network cable used for monitoring is prepared.

Procedure

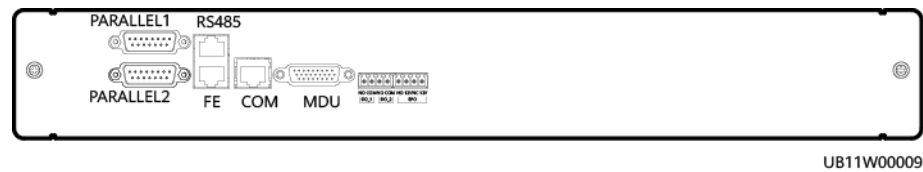
- Step 1** Connect one end of the network cable to the FE port on the monitoring interface unit.

Figure 4-22 Monitoring interface unit of the SmartLi



(1) Monitoring interface unit

Figure 4-23 FE port on the monitoring interface unit



Step 2 Connect the other end of the network cable to the Ethernet port on the LAN switch.

----End

4.2.12 Connecting the PDU8000 Monitoring Cable

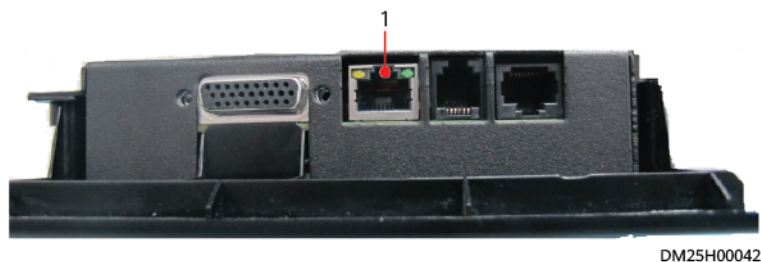
Prerequisites

A network cable used for monitoring is prepared.

Procedure

Step 1 Connect one end of the network cable to the FE port on the display panel of PDU8000, as shown in [Figure 4-24](#).

Figure 4-24 Connecting a monitoring cable to the PDU8000 (FE port)



(1) FE port

Step 2 Connect the other end of the network cable to the Ethernet port on the LAN switch.

----End

4.2.13 Connecting the MTS9604B-N20B1 Power Monitoring Cable

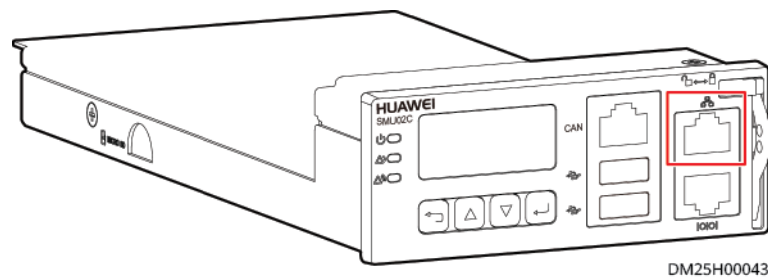
Prerequisites

A network cable used for monitoring is prepared.

Procedure

Step 1 Connect one end of the network cable to the FE port on the SMU02C in the MTS9604B-N20B1 cabinet.

Figure 4-25 FE communications port



Step 2 Connect the other end to the Ethernet port on the LAN switch.

----End

4.2.14 Connecting a Monitoring Cable to TP483000D

Prerequisites

A network cable used for monitoring is prepared.

Procedure

Step 1 Connect one end of the network cable to the fast Ethernet (FE) port on TP483000D.

Step 2 Connect the other end of the network cable to the Ethernet port on the LAN switch.

----End

4.2.15 Connecting a Monitoring Cable to an iBOX

Prerequisites

A network cable used for monitoring is prepared.

Procedure

Step 1 Connect one end of the network cable to the PoE port on the iBOX.

Step 2 Connect the other end of the network cable to the Ethernet port on the LAN switch.

----End

4.3 Scenarios for Connecting the ECC800-Pro Outside the Smart Module

4.3.1 Preparing a Monitoring Cable

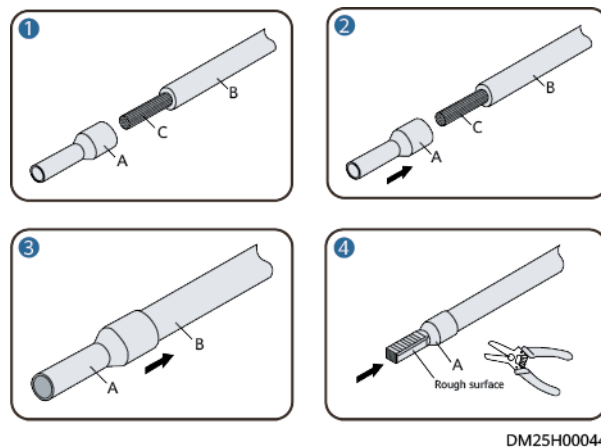
Prerequisites

- A twisted pair, cord end terminal, and RJ45 connector are prepared.
- The following tools are prepared:
 - Wire stripper
 - Crimping tool
 - RJ11 crimping tool
 - Electrician's knife
 - Polyvinyl chloride (PVC) insulation tape

Preparing a Cord End Terminal

Figure 4-26 shows how to prepare a cord end terminal.

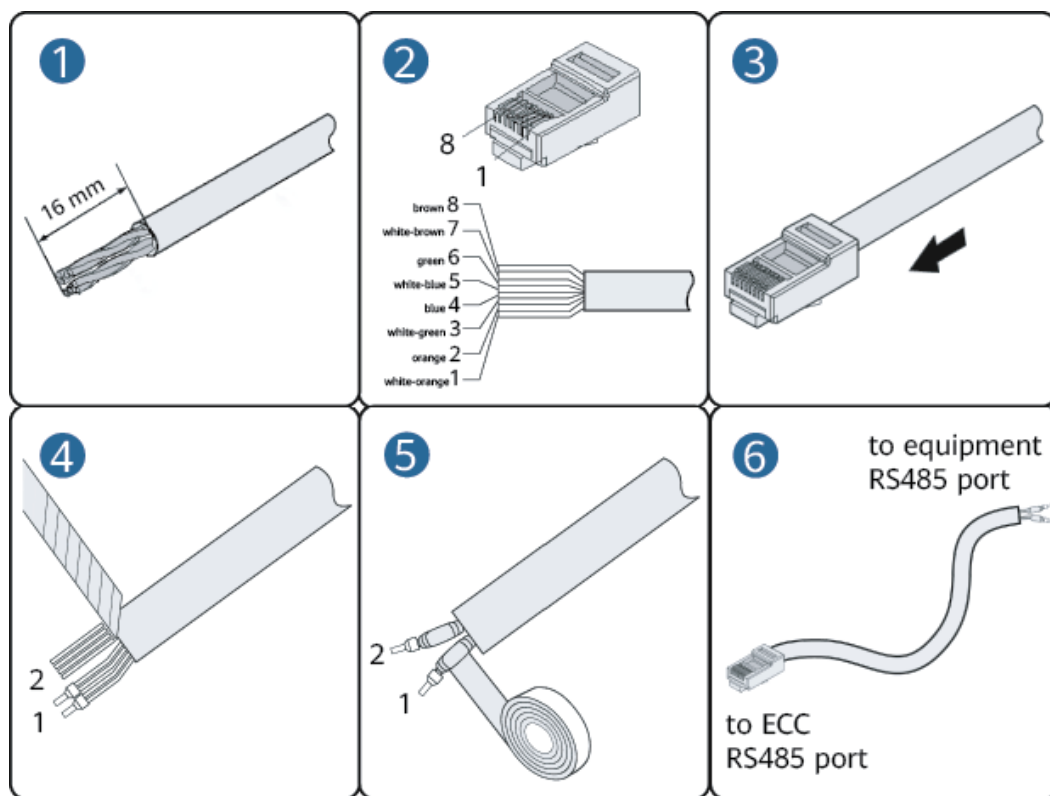
Figure 4-26 Preparing a cord end terminal



Preparing the RS485 Monitoring Cable

Figure 4-27 shows how to prepare a cord end terminal for the ECC800-Pro collector.

Figure 4-27 Preparing the RS485 monitoring cable for ECC800-Pro collector



DM25H00045

Preparing a Dry Contact Monitoring Cable

The method of preparing a dry contact monitoring cable is similar to the method of preparing the RS485 monitoring cable. Prepare cord end terminals on both ends of each required core wire based on the number of dry contacts.

4.3.2 ECC800-Pro

4.3.2.1 Product Configuration

The ECC800-Pro data center controller is mainly used to monitor the devices and environment in a data center. It consists of the power module and main control module, which are pluggable.

You can configure the ECC800-Pro collector in the following two manners:

Configuration 1 (typical configuration): one power module and one main control module

Configuration 2: two power modules and one main control module.

NOTE

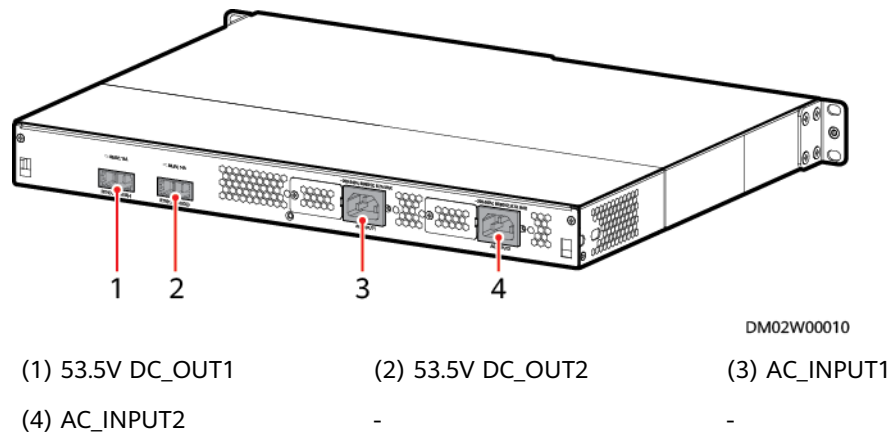
- In configuration 1, install a filler panel in slot 2.
- In configuration 2, install power modules in slots 1 and 2.

(1) Slot 1: power modules (2) Slot 2: power modules (3) Slot 3: main control module

Item	Specifications
Operating temperature	-20°C to +50°C
Storage temperature	-40°C to +70°C
Relative humidity	5%–95% RH (non-condensing)
Altitude	0–4000 m (When the altitude is between 3000 m and 4000 m, the temperature decreases by 1°C for each additional 200 m.)

Item	Specifications
Dimensions (L x W x H)	442 mm x 330 mm x 43.6 mm
Weight	7.5 kg (dual power supplies + main control module)
Color	Black
Installation requirements	Can be installed in a 1 U space in a standard 19-inch cabinet
Environmental protection	RoHS5, REACH, WEEE

Figure 4-29 ECC800-Pro (rear view)



Power Port

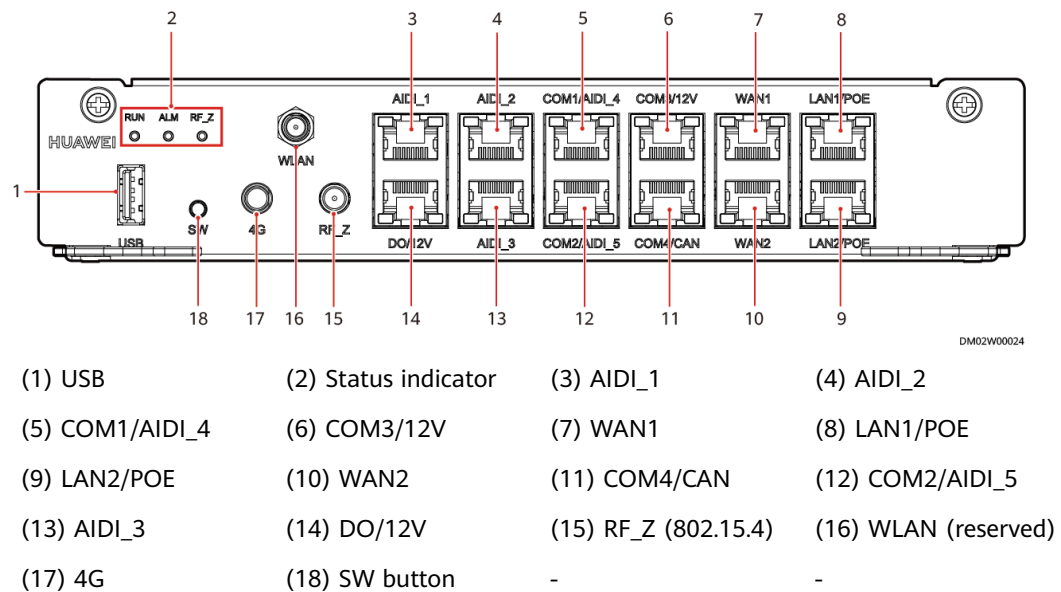
The ECC800-Pro provides four power ports, including two AC input ports (AC_INPUT1 and AC_INPUT2) and two DC output ports (DC_OUT1 and DC_OUT2). [Table 4-19](#) provides the power port pin definitions.

Table 4-19 Power port pin definitions

Port Type	Pin sequence	Description
AC	Pin1	L
	Pin2	PE
	Pin3	N
DC	Pin1	48V+
	Pin2	48VGND

4.3.2.2 Main Control Module

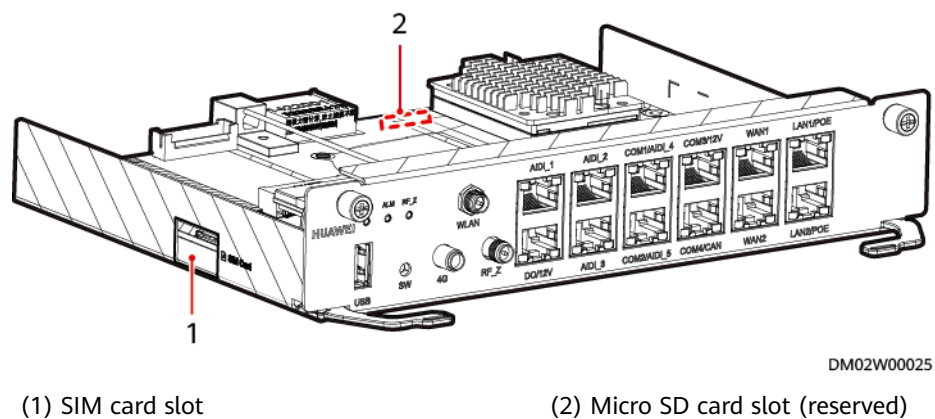
Figure 4-30 ECC800-Pro collector main control module



NOTE

The WLAN port is reserved and cannot be connected to a WLAN antenna for WLAN communication.

Figure 4-31 ECC800-Pro main control module (side view)



Technical Specifications

Table 4-20 Technical specifications of the ECC800-Pro main control module

Item	Specifications
Power input	- Supports one AC input or two AC inputs - Rated voltage: 200–240 V AC - Rated frequency: 50/60 Hz
Maximum power consumption of the main control module	70 W
Power output	- Output voltage: 42–58 V DC (rated voltage: 53.5 V DC) - Output power of two power module supplies: 2000 W (200–240 V AC); 940 W (linear derating at 85–175 V AC) - Output power of a single power module supply: 1000 W (200–240 V AC); 470 W (linear derating at 85–175 V AC)
WAN port	- Supports two WAN ports. WAN1 is used to connect to the management system, and WAN2 is used for maintenance. The ports support autonegotiation of 10/100/1000 Mbit/s communication rates. - Connect shielded network cables to the WAN ports.
LAN port	- Supports two LAN ports, which can be connected to the LAN. The ports support autonegotiation of 10/100/1000 Mbit/s communication rates. - Connect shielded network cables to the LAN ports.
RS485 serial port expansion	- Output voltage: 13–15 V DC (rated voltage: 14.5 V DC) - Four RS485 ports with the default communications rate of 9600 bit/s - COM1–COM3 ports provide 12 V DC power. - The power supply can be switched on or off and is on by default.
PoE expansion	Supports two PoE (GE) ports for expansion of the PoE bus, and supports network isolation and ring network.
AIDI expansion (RJ45)	- Output voltage: 13–15 V DC (rated voltage: 14.5 V DC) - Provides five universal AIDI ports for connecting to sensors such as smoke sensors, water sensors, and NTC sensors. AIDI_1 to AIDI_3 are full-function AIDI ports, and AIDI_4 to AIDI_5 are simplified AIDI ports without type identification. - The power supply can be switched on or off and is on by default.

Item	Specifications
DO expansion (RJ45)	- Output voltage: 13–15 V DC (rated voltage: 14.5 V DC) - Supports one active DO port. - The power supply can be switched on or off and is on by default.
Fault isolation	There are three groups of 12 V ports. A group has a maximum current of 660 mA, a route has a maximum current of 800 mA, and the maximum total current is 2 A. Group 1: AIDI_1 and DO/12V ports Group 2: AIDI_2, COM1/AIDI_4, and COM3/12V ports Group 3: AIDI_3 and COM2/AIDI_5 ports
Wireless communication	Supports wireless communication that complies with IEEE802.15.4.
4G	Supports the 4G module, SMS sending, and 3G communication, and provides a standard SIM card slot. - China: 2G and 4G networks support China Unicom or China Mobile SIM cards, and 3G networks support only China Unicom SIM cards. - Outside China: Select SIM cards according to the following wireless modes and frequency bands: 4G: LTE-FDD, covering frequency bands B1, B3, B5, B7, B8 and B20; LTE-TDD, covering frequency bands B38, B40, and B41 3G: WCDMA, covering frequency bands B1, B5, and B8 2G: GSM, covering frequency bands 900 MHz/1800 MHz NOTE - The prerequisite for using a SIM card is that the site has signal coverage. - Due to the performance limitation of the wireless module, China Telecom SIM cards are not supported.
USB	- Supports USB 2.0 and 5 V/1 A power supply. - After installing the WiFi module, connect the WiFi module to the ECC800-Pro using the app on the mobile phone or pad to view the basic information about the smart module, such as layout, resources, energy efficiency, environment, and alarms. - You can insert a USB flash drive to export historical data and configuration files and import configuration files.
SW button	- Restores the default IP address, factory settings, and user information. - Supports RF_Z (802.15.4) networking.

Table 4-21 ECC800-Pro RF_Z parameters

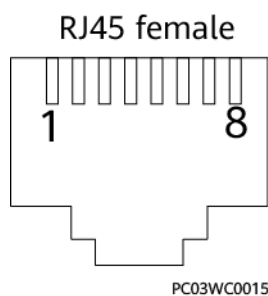
Item	Specifications
RF_Z operating frequency	2405–2480 MHz
RF_Z EIRP (max.)	8 dBm

Table 4-22 ECC800-Pro 4G parameters

Item	Specifications
Operating frequency	• 4G: LTE-FDD, covering frequency bands B1, B3, B5, B7, B8 and B20; LTE-TDD, covering frequency bands B38, B40, and B41 • 3G: WCDMA, covering frequency bands B1, B5, and B8 • 2G: GSM, covering frequency bands 900 MHz/1800 MHz
EIRP (max.)	23 dBm

Communications Port

The ECC800-Pro provides the following communications ports. [Figure 4-32](#) shows the pins of the RJ45 port.

Figure 4-32 RJ45 port pins

There are four GE ports, that is, two WAN ports (WAN1 and WAN2) and two LAN ports (LAN1/POE and LAN2/POE).

Table 4-23 GE port pin definitions

Item		Description
Pin sequence	Pin1	GE1+
	Pin2	GE1-

Item		Description
	Pin3	GE2+
	Pin4	GE3+
	Pin5	GE3-
	Pin6	GE2-
	Pin7	GE4+
	Pin8	GE4-
Indicator	Green indicator	Linked, steady on
	Yellow indicator	ACT data communication, blinking

Table 4-24 COM1/AIDI_4, COM2/AIDI_5 port pin definitions

Item		Description
Pin sequence	Pin1	RS485+
	Pin2	RS485-
	Pin3	12V DC_OUT
	Pin4	RS485+
	Pin5	RS485-
	Pin6	DI-
	Pin7	DI+
	Pin8	GND
Indicator	Green indicator	Power output indicator - Steady on: The 12 V DC output is normal. - Off: No 12 V DC output is provided.

Table 4-25 COM3/12V port pin definitions

Item		Description
Pin sequence	Pin1	RS485+
	Pin2	RS485-
	Pin3	12V DC_OUT

Item		Description
	Pin4	RS485+
	Pin5	RS485-
	Pin6	-
	Pin7	-
	Pin8	GND
Indicator	Green indicator	Power output indicator - Steady on: The 12 V DC output is normal. - Off: No 12 V DC output is provided.

Table 4-26 COM4/CAN port pin definitions

Item		Description
Pin sequence	Pin1	RS485+
	Pin2	RS485-
	Pin3	-
	Pin4	RS485+
	Pin5	RS485-
	Pin6	-
	Pin7	CAN_H
	Pin8	CAN_L

The following provides the AIDI_1, AIDI_2, and AIDI_3 ports pin definitions.

 NOTE

- Pins 1, 2, 4, and 5 identify sensor types.
- Pin 3 and Pin 8 are power output ports.
- Pin 6 and Pin 7 collect sensor data. Pin 7 can detect current type sensors (4–20 mA). Pin 6 and Pin 7 can detect the output status of passive dry contact type sensors. Pin 3 and Pin 7 can detect temperature sensors.

Table 4-27 AIDI_1, AIDI_2 and AIDI_3 ports pin definitions

Item		Description
Pin sequence	Pin1	Type_1
	Pin2	Type_2

Item		Description
	Pin3	12V DC
	Pin4	Type_3
	Pin5	Type_4
	Pin6	DI-
	Pin7	DI+
	Pin8	GND
Indicator	Green indicator	Power output indicator - Steady on: The 12 V DC output is normal. - Off: No 12 V DC output is provided.

Table 4-28 DO/12V port pin definitions

Item		Description
Pin sequence	Pin1	-
	Pin2	-
	Pin3	12V DC_OUT
	Pin4	-
	Pin5	-
	Pin6	DO_OUT+
	Pin7	DO_OUT-
	Pin8	GND
Indicator	Green indicator	Power output indicator - Steady on: The 12 V DC output is normal. - Off: No 12 V DC output is provided.

Table 4-29 USB port pin definitions

Item		Description
Pin sequence	Pin1	5V
	Pin2	DM
	Pin3	DP
	Pin4	GND

Indicators

Table 4-30 Indicators on the ECC800-Pro main control module

Indicator	Color	Name	Status	Description
RUN	Green	Running status indicator	Steady on	The power supply is normal, the program is being loaded.
			Off	The power supply is abnormal.
			Blinking at long intervals	The software runs properly (the indicator blinks at 0.5 Hz, on for 1s and then off for 1s) or the ECC800-Pro registers with the NetEco successfully.
			Blinking at short intervals	The ECC800-Pro does not register with the NetEco (the indicator blinks at 5 Hz, on for 0.125s and then off for 0.125s).
ALM	Red	Alarm indicator	Steady on	A system failure alarm is generated.
			Off	The system is normal.
RF_Z	Green	Communication status indicator	Blinking at long intervals	A network is set up, and no node access is allowed (the indicator blinks at 0.5 Hz, on for 1s and then off for 1s).
			Blinking at super short intervals	A network is set up, and node access is allowed (the indicator blinks at 10 Hz, on for 0.05s and then off for 0.05s).

SW Button

Table 4-31 SW button description

Function Description	Operation Description	Indicator Status
Wireless network RF_Z (802.15.4) pairing	In non-wireless network (802.15.4) pairing mode, press and hold the button for 3s to 5s to enter the wireless network pairing mode.	The RF_Z indicator is blinking at super short intervals.

Function Description	Operation Description	Indicator Status
	In wireless network (802.15.4) pairing mode, press and hold the button for 3s to 5s to exit the pairing mode; or the system automatically exits the pairing mode after 30 minutes without pressing the button.	The RF_Z indicator is blinking at long intervals.
	Press and hold the button for more than 8s to erase network parameters. The system automatically enters the wireless network pairing mode.	The RF_Z indicator is blinking at super short intervals.
WLAN enabling	Press the button for less than 3s to enable WLAN.	None
Restoring the default IP address, factory settings, and user information	Press and hold down the button for 1 minute.	None

4.3.2.3 Power Module

Indicators

Table 4-32 Power module indicator description

Indicator	Color	Name	Status	Description
	Green	Power indicator	Steady on	The module has input power.
			Off	The module has no input power or is faulty.
			Blinking at long intervals	The module is being queried (the indicator blinks at 0.5 Hz, on for 1s and then off for 1s).
			Blinking at short intervals	The module application program is being loaded (the indicator blinks at 4 Hz, on for 0.125s and then off for 0.125s).

Indicator	Color	Name	Status	Description
	Yellow	Alarm indicator	Steady on	Power limiting warning due to ambient overtemperature; protection shutdown alarm due to ambient overtemperature or undertemperature
				Power input overvoltage or undervoltage protection
				Reverse DC input connection
				Slight current imbalance
				Output overvoltage
				Hibernation
			Off	The module generates no protection alarms.
			Blinking at long intervals	The communication between the module and the outside is interrupted (the indicator blinks at 0.5 Hz, on for 1s and then off for 1s).
	Red	Fault indicator	Steady on	The module locks out due to output overvoltage.
				The module has no output due to internal faults.
			Off	The module is normal.

4.3.3 UIM20A Expansion Module

Figure 4-33 UIM20A expansion module front panel

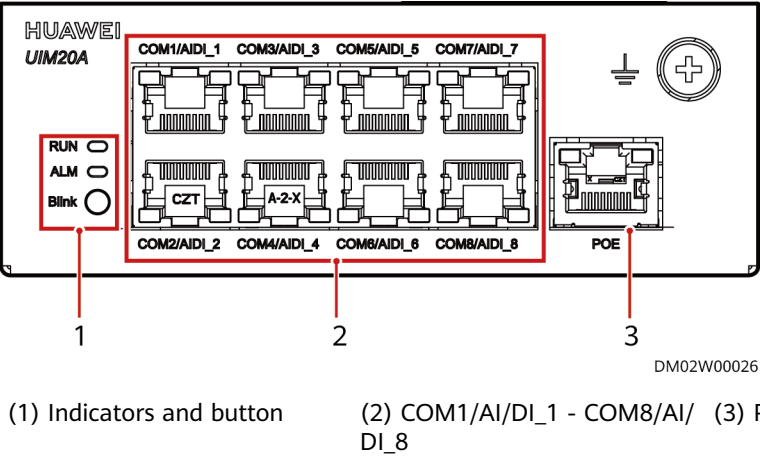


Figure 4-34 UIM20A expansion module rear panel

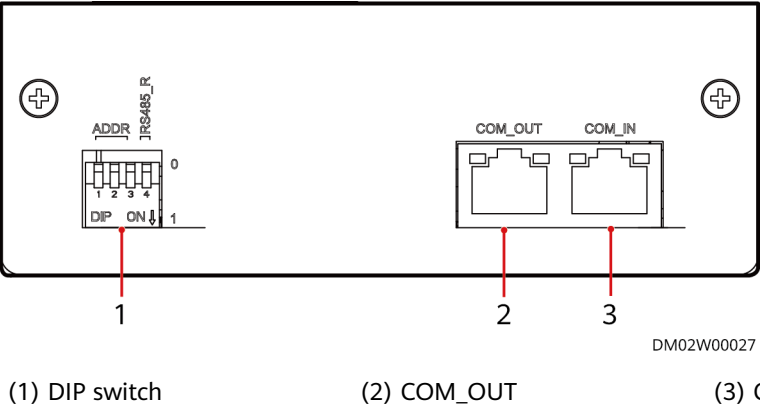


Table 4-33 UIM20A expansion module specifications

Item	Specifications
Width	120 mm
Depth	200 mm
Height	43 mm
Operating temperature	-30°C to +65°C
Installation requirements	Installed in a 19-inch rack
Environmental protection	RoHS5

Specifications

Table 4-34 UIM20A technical specifications

Item	Specifications
Power input	Supports the RS485 or PoE power supply.
COM/AIDI (RJ45)	- Supports eight RS485 or AI/DI signal inputs. - Can connect to sensors such as the smoke sensor, water sensor, door status sensor, and infrared sensor. - Each port can supply power. Two RJ45 ports share one 12 V DC power supply that is controlled independently. The maximum output current is 900 mA when the voltage is 12 V. (COM1/AIDI_1 and COM2/AIDI_2 form a group, COM3/AIDI_3 and COM4/AIDI_4 form a group, COM5/AIDI_5 and COM6/AIDI_6 form a group, and COM7/AIDI_7 and COM8/AIDI_8 form a group). - The 12 V DC power supply can be switched on or off and is on by default.
POE	Connects to the ECC800-Pro through the PoE port.
DIP switch	- One 4-bit DIP switch is used to set the RS485 address. - OFF indicates 0 and ON indicates 1. - Bit 1 is the least significant bit, and bit 4 is the most significant bit. For example, if the board address is 5, the corresponding bits are ON, OFF, ON, and OFF, and the corresponding binary number is 1010 (ON is 1 and OFF is 0).
E-label 4.0	Supported

Communications Port

The following table describes the pin assignment for ports COM1/AIDI_1 to COM8/AIDI_8.

Table 4-35 Pin assignment for ports COM1/AIDI_1 to COM8/AIDI_8

Item	Description
Pin sequence	Pin1 RS485+
	Pin2 RS485-
	Pin3 12V
	Pin4 RS485+

Item		Description
	Pin5	RS485-
	Pin6	D-
	Pin7	D+
	Pin8	GND

The following table describes the pin assignments for the COM_IN and COM_OUT ports.

Table 4-36 Pin assignment for the COM_IN and COM_OUT ports

Item		Description
Pin sequence	Pin1	RS485+
	Pin2	RS485-
	Pin3	12 V (input power, supplying power to the module)
	Pin4	RS485+
	Pin5	RS485-
	Pin6	-
	Pin7	-
	Pin8	GND

Indicators and Buttons

Table 4-37 UIM20A indicators

Indicator	Status	Description
RUN	Steady on	A board application is being loaded.
	Off	The board is not running.
	Blinking at long intervals	The ECC800-Pro is successfully registered, and the software runs properly (blinking at long intervals (0.5 Hz), on for 1s and then off for 1s).
	Blinking at short intervals	The communication is interrupted or the ECC800-Pro is unsuccessfully registered (blinking at 2.5 Hz, on for 0.2s and then off for 0.2s).

Indicator	Status	Description
	Blinking	Blinking at super short intervals for 0.5s and then off for 0.5s; last 10s (blinking at super short intervals: 10 Hz, on for 0.05s and then off for 0.05s)
ALM	Steady on	A system fault alarm is raised.
	Off	The system is normal.

Table 4-38 BLINK button description

Function Description	Operation Description	Indicator Status
Blinking	Press the button for less than 2s.	The RUN indicator blinks at super short intervals for 0.5s and then off for 0.5s; last 10s (blinking at super short intervals for 10 Hz, on for 0.05s and then off for 0.05s).

4.3.4 Connecting a Monitoring Cable to the UIM20A Expansion Module

Prerequisites

A network cable used for monitoring is prepared.

Procedure

- Step 1** Connect one end of the network cable to the PoE port on the UIM20A expansion module.
- Step 2** Connect the other end of the network cable to the LAN port on the ECC800-Pro.

NOTE

If the COM or AI/DI ports on the ECC800-Pro are insufficient, you can connect devices to the UIM20A expansion module.

----End

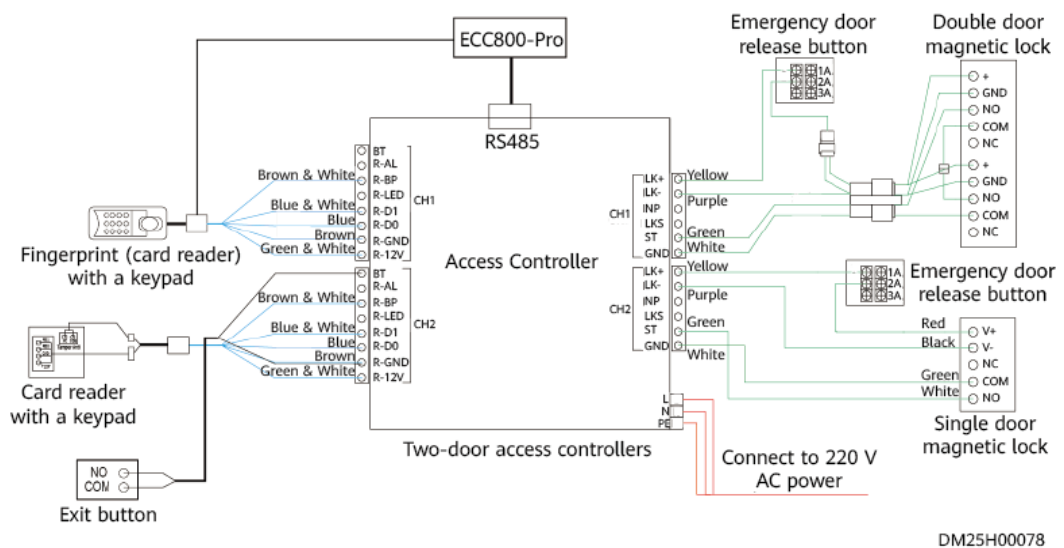
4.3.5 Connecting the Access Management System Cable

4.3.5.1 Connecting a Monitoring Cable to the A8802RS Access Controller

General Cable Connections to an Access Controller

- When connecting the door access system, you need to connect a door access controller, an ECC800-Pro collector (or a UIM20A expansion module), a door exit button, the fingerprint and card reader (with a keypad), card reader with a keypad, single-door/double-door magnetic lock, and emergency door release button.
- You can connect the fingerprint and card reader (with a keypad), card reader with a keypad, and exit button to the CH1 or CH2 terminal on the left of the access controller in the following figure, and connect the double-door and single-door magnetic locks to the CH1 or CH2 terminal on the right of the access controller in the following figure.
- The following figure uses the double-door access controller as an example to illustrate the wiring method for the access control system. In this example, the fingerprint and card reader (with a keypad) connects to the CH1 terminal on the left of the access controller, the card reader with a keypad connects to the CH2 terminal on the left of the access controller, the double-door magnetic lock connects to the CH1 terminal on the right of the access controller, and the single-door magnetic lock connects to the CH2 terminal on the right of the access controller.

Figure 4-35 General cable connections for the access control system



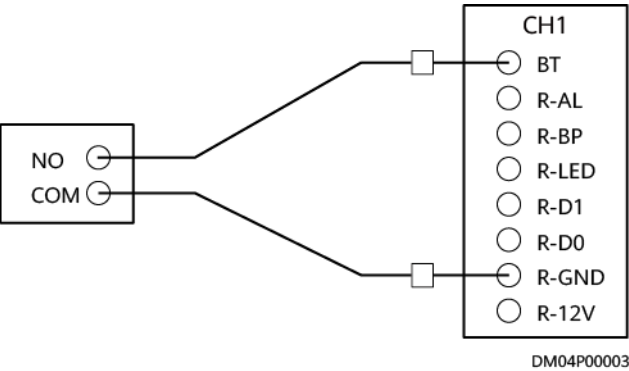
NOTE

- Connect the RS485 ports on the access controller and the fingerprint and card reader (with a keypad) respectively to any two of COM1 to COM4 ports on the ECC800-Pro collector.
- Fingerprint and card reader (with a keypad) refers to the fingerprint and card reader with a keypad or the fingerprint and card reader.

Connecting Cables to the Exit Button

Figure 4-36 shows the cable connections to the access controller and exit button, using the cord end terminal to crimp the cable.

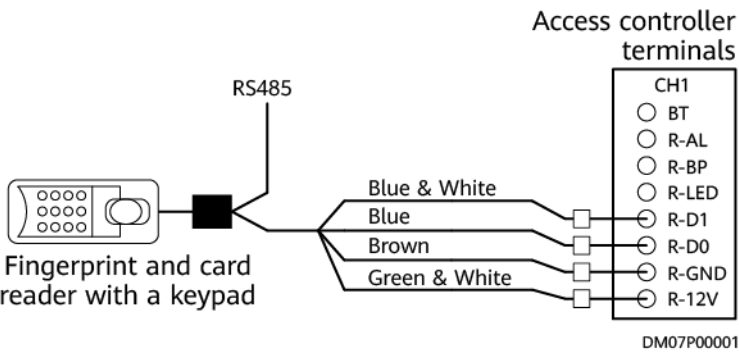
Figure 4-36 Connecting cables to the exit button



Connecting Cables to the Fingerprint and Card Reader with a Keypad

The following figure shows the cable connections to the access controller and fingerprint and card reader with a keypad, using the cord end terminal to crimp the cable.

Figure 4-37 Connecting cables to the fingerprint and card reader with a keypad



- Connect one end of the network cable to the female connector of the fingerprint and card reader with a keypad. Strip the other end of the network cable and connect it to the access controller terminal, as shown in the preceding figure.

NOTE

If the network is non-standard, connect it by referring to the cable sequence in the following table.

Table 4-39 Cable connections for the fingerprint and card reader with a keypad

Conversion Cable	Wire of the Network Cable	Access Controller Terminal
Red wire	Pin3	R-12V
Green wire	Pin4	R-D0
White wire	Pin5	R-D1

Conversion Cable	Wire of the Network Cable	Access Controller Terminal
Black wire	Pin8	R-GND

- Connect one end of another network cable to the RS485 port on the fingerprint and card reader with a keypad, and connect the other end of the network cable to the non-energized COM port on the ECC800-Pro collector. The following table shows the pin mapping for the RS485 port and the COM port.

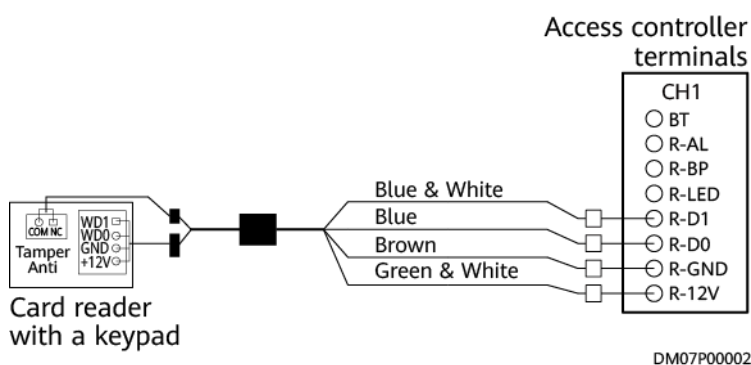
Table 4-40 Pin mapping for the RS485 port and the COM port

RS485 Port on Fingerprint and Card Reader with a Keypad		COM Port on ECC800-Pro Collector
Pin	Definition	Pin
Pin1	485A (brown)	Pin1
Pin2	485B (gray)	Pin2

Connecting Cables to the Card Reader with a Keypad

The following figure shows the cable connections to the access controller and card reader with a keypad, using the cord end terminal to crimp the cable.

Figure 4-38 Connecting cables to the card reader with a keypad



Connecting Cables to the Single-Door Magnetic Lock, Double-Door Magnetic Lock, and Emergency Door Release Button

- The double-door magnetic lock is delivered with eight cables. Connect the cables to the double-door magnetic lock, as shown in [Figure 4-39](#). Crimp the cable on the access controller side using a cord end terminal.
- [Figure 4-40](#) shows the cable connections to the access controller, single-door magnetic lock, and emergency door release button. Crimp the cables using cord end terminals.

NOTE

- The magnetic lock is delivered with a small white terminal. Cut off the white terminal and then use a cord end terminal for crimping.
- The cable installation sequences shown in the following figure are for reference only. If any differences exist between the wiring diagram and this figure, the wiring diagram prevails.

Figure 4-39 Connecting cables to the double-door magnetic lock and emergency door release button

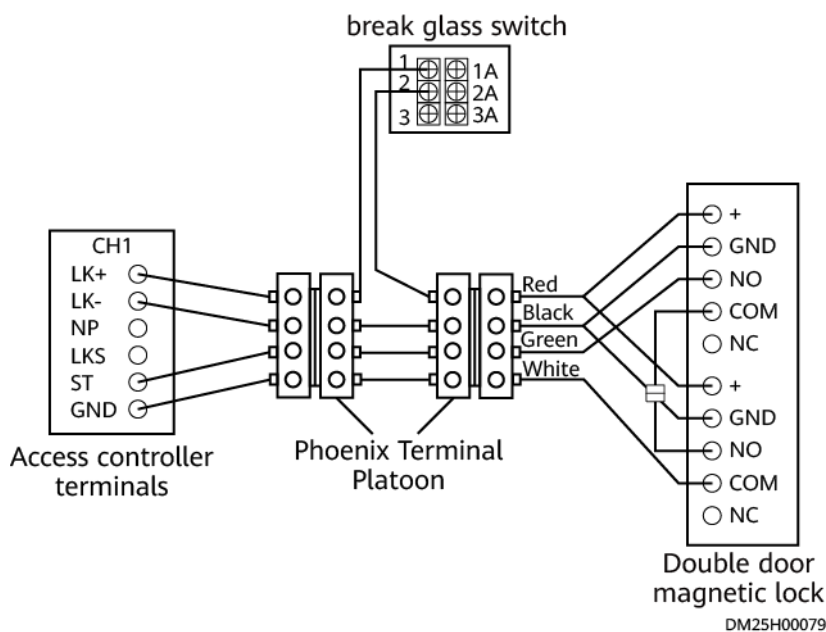
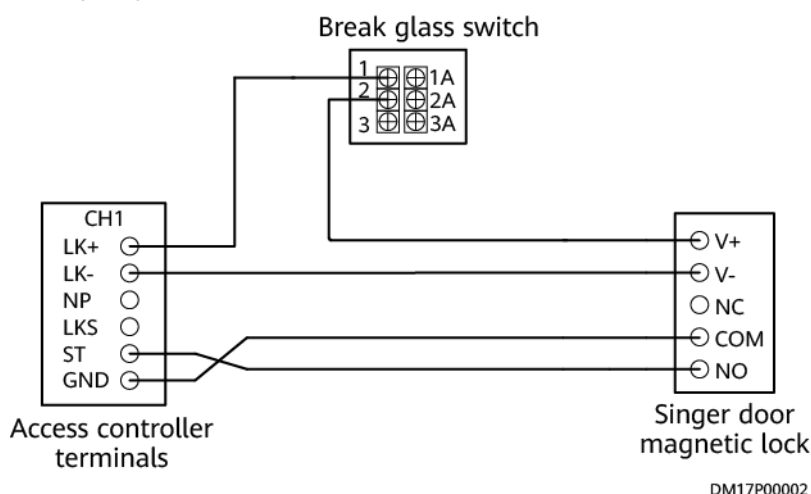


Figure 4-40 Connecting cables to the single-door magnetic lock and emergency door release button



Connecting the Power Cable to the Access Controller

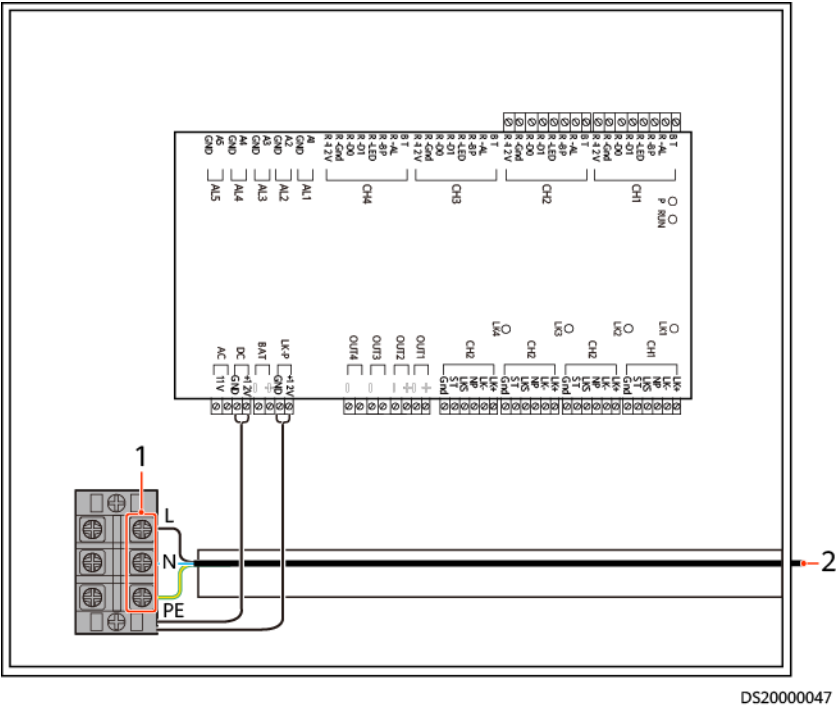
The access controller is powered by 220 V power supply. The power module is installed inside the access controller. The access controller can obtain power from a power supply outside the equipment room.

Strip the cable, install the connector (BOM number: 14170096), and connect the wires respectively to the L, N, and PE wiring terminals on the terminal block in the access controller power module, as shown by (1) in [Figure 4-41](#). Route the other end of the cable along the cable trough inside the access controller and then out of the cable outlet, and connect it to the power supply to receive power.

 NOTE

Pay attention to the polarity when connecting cables.

Figure 4-41 Connecting cables to the access controller



(1) Connecting the power cable for the access controller (2) Connecting to the power supply, as described in [Table 4-41](#)

Table 4-41 Power cable connection for the access controller

Power Supply	Cable Connection
Power supply outside the equipment room	Install the connector (BOM number: 14170096) to the other end of the power cable and connect the power cable to a circuit breaker in the power supply outside the equipment room.

Related Information

Table 4-42 Card reader and key terminal definition

Terminal Identity	Definition
BT	Key input
R-AL	Card reader pry signal input
R-BP	Control card reader buzzer
R-LED	Control card reader LED lights
R-D1	Card reader data 1
R-D0	Card reader data 0
R-Gnd	Card reader public ground
R-12V	Reader power + 12 V

Table 4-43 Lock and door magnetic terminal definition

Terminal Identity	Definition
LK+	Lock output power +
LK-	Lock output power -/Passive output -
NP	Passive output +
LKS	Lock signal input +
ST	Door magnetic signal input +
Gnd	Common ground

Table 4-44 Alarm input terminal definition

Terminal Identity	Definition
AL(1-2)	Two-door controller, no power supply output signal
Gnd	Common ground

Table 4-45 Power terminal definition

Terminal Identity	Definition	
LK-P	+12V	Lock the power input + 12 V
	GND	Lock the power input -
BAT	+	Battery +
	-	Battery -
DC	+12V	Controller + 12 V DC power input
	GND	Controller DC power input-
AC	11V	Controller AC power input

Table 4-46 Indicator light definition

Terminal Identity	Definition
P	The controller power light, red
RUN	Controller working indicator light, white blue, flashing
LK(1-4)	Lock status indicator light

Table 4-47 RS485 interface

Terminal Identity	Definition
AL3(A8802RS)	RS485-A
Gnd	RS485-B

Table 4-48 Access control system cable list

BOM Number	BOM Description	Cable Position
25030384	Electric Cable, 300V/500V, 60227 IEC 53(RVV), 3x1mm ² , Black(3Cores: Brown, Blue, Yellow/Green), 10A, Outdoor Cable, CCC, CE	Access controller power cable

BOM Number	BOM Description	Cable Position
25030641	Electric Cable, 300V, UL2464, 4x20AWG, Black(4Cores: Yellow, Green, Violet, White), 9A, Non-shielding Outdoor Cable, UL	Cable from the magnetic lock to the access controller
25030393	Electric Cable, 300V/500V, 60227 IEC 53(RVV), 2x0.75mm ² , Black(2Cores: Brown, Blue), 6A, Flat Outdoor Cable, CCC, CE	Cable from the emergency door release button to the access controller
14180327	Terminal Block, 4-Pin, Screw Fixed, 24–12 AWG, Pitch 5.08 mm, Male and Female Using Together, Only for Power Supply	
25031053	Electric Cable, 300V, UL2464, 7x20AWG, Black(7Cores: Red, Black, Yellow, Green, Orange, White, Blue), 9A, Non-shielding Cable, UL	Cable from the card reader to the access controller
14180327	Terminal Block, 4-Pin, Screw Fixed, 24–12 AWG, Pitch 5.08 mm, Male and Female Using Together, Only for Power Supply	
25030393	Electric Cable, 300V/500V, 60227 IEC 53(RVV), 2x0.75mm ² , Black(2Cores: Brown, Blue), 6A, Flat Outdoor Cable, CCC, CE	Cable from the door exit button to the access controller

4.3.5.2 Connecting a Monitoring Cable to the Door Status Sensor

Prerequisites

A monitoring cable required is prepared.

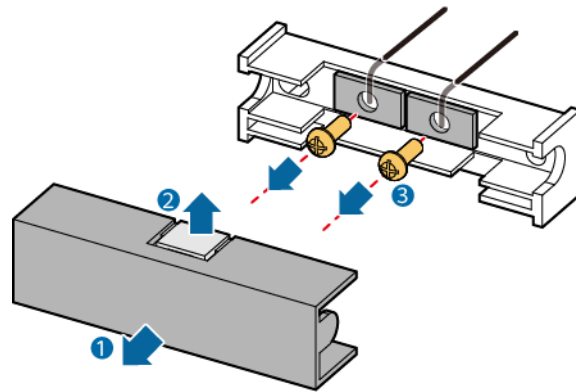
Context

When connecting the door status sensor to an ECC800-Pro collector or a UIM20A expansion module, you need to perform the following steps to prepare a special monitoring cable.

Procedure

Step 1 Open the door status sensor, connect two cables, as shown in [Figure 4-42](#).

Figure 4-42 Connecting a monitoring cable to the door status sensor



DM82000007

- Step 2** Prepare an RJ45 connector on one end of the network cable by following to the instruction in [4.3.1 Preparing a Monitoring Cable](#).
- Step 3** Connect the green core wire 6 and the brown-white core wire 7 to the cables routed out from the door status sensor.
- Step 4** Connect one end of the RJ45 network cable to the AI/DI port on the ECC800-Pro collector.

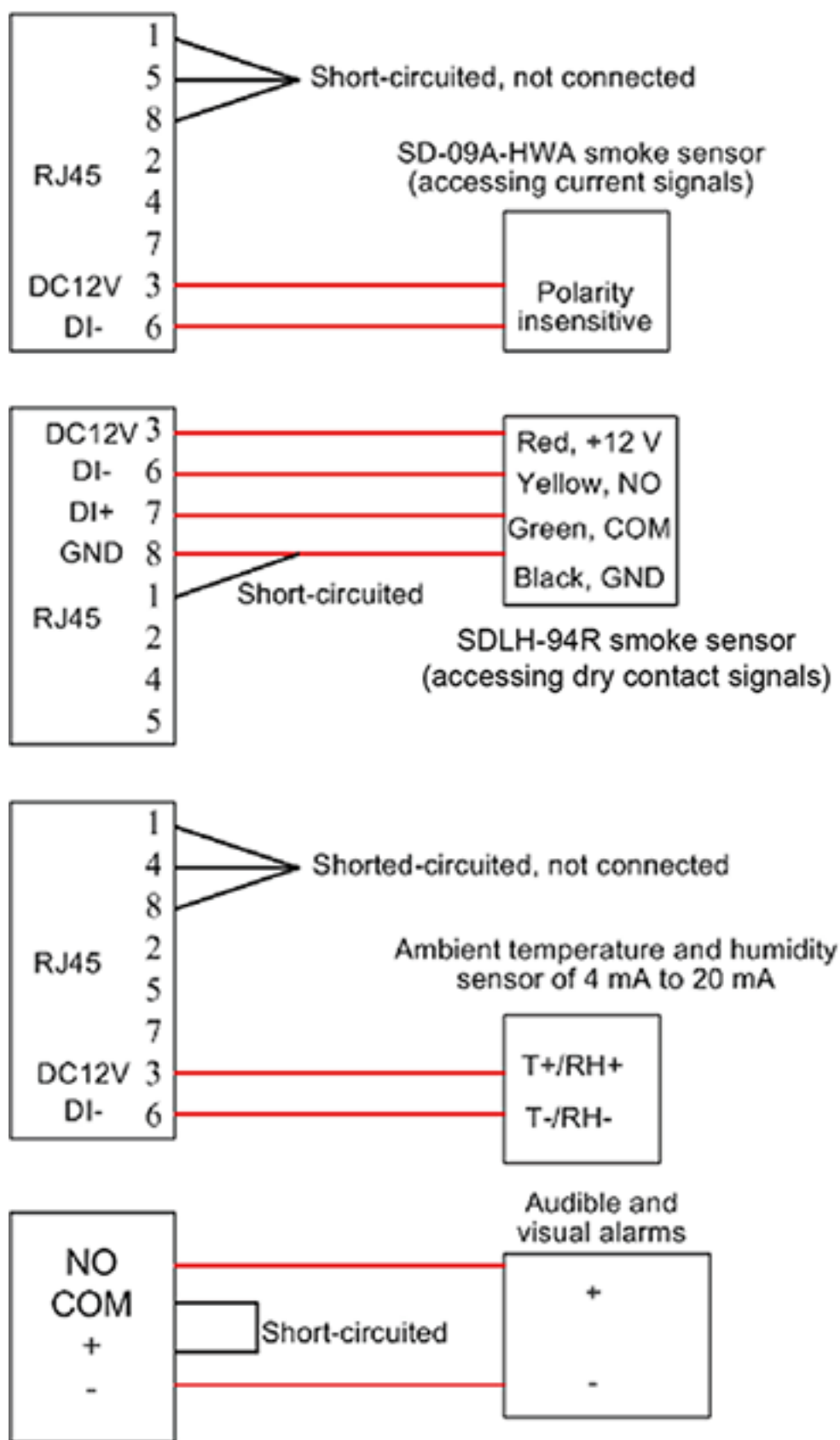
-----End

4.3.6 Connecting Cables to Sensors

4.3.6.1 Connecting Cables to Sensors

If the ECC800-Pro collector is connected to the following types of sensors, connect cables to the devices by referring to [Figure 4-43](#).

Figure 4-43 Wiring diagram for sensors



DS100E0056

4.3.6.2 Connecting the Temperature Sensor Monitoring Cable

Prerequisites

The RS485 monitoring cable is prepared.

Procedure

Step 1 Connect the temperature sensor to the temperature and humidity sensor.

1. Connect one end of the network cable to the wiring port on the temperature sensor.
2. Connect the other end of the network cable to the NTC1~3 or NTC4~6 port on the temperature and humidity sensor.

Step 2 Connect the temperature and humidity sensor to the UIM20A expansion module.

1. Connect one end of the network cable to the RS485-OUT port on the temperature and humidity sensor.
2. Connect the other end of the network cable to the COM1/AIDI_1, COM3/AIDI_3, COM5/AIDI_5, or COM7/AIDI_7 port on the UIM20A expansion module.

NOTE

- Temperature and humidity sensors can be cascaded through the RS485-IN and RS485-OUT ports. A maximum of eight temperature and humidity sensors can be cascaded.
- A maximum of four temperature and humidity sensors can be connected to the UIM20A expansion module. Temperature and humidity sensors need to be connected to the COM1/AIDI_1, COM3/AIDI_3, COM5/AIDI_5, and COM7/AIDI_7 ports on the UIM20A expansion module in sequence.

----End

4.3.6.3 Connecting a Monitoring Cable to the Hydrogen Detection System

Prerequisites

The RS485 monitoring cable is prepared.

Procedure

Step 1 Connect one end of a common network cable to the hydrogen detection system RJ45 RS485 port.

Step 2 Connect the other end to the COM port on an ECC800-Pro collector or a UIM20A expansion module.

----End

4.3.6.4 Connecting a Monitoring Cable to the Smoke Sensor

Prerequisites

A monitoring cable required is prepared.

Context

When connecting the smoke sensor and the ECC800-Pro collector or the UIM20A expansion module, you need to perform the following steps to prepare a special monitoring cable.

Procedure

- Step 1** Prepare an RJ45 connector on one end of the network cable by following to the instruction in Preparing a Monitoring Cable.
- Step 2** Short-circuit core wires 1 and 8 on the other end of the network cable.
- Step 3** Connect the core wires of the network cable to the cables for the smoke sensor, based on the mappings in [Table 4-49](#).

Table 4-49 Connecting cables to the smoke sensor

Core Wires of the Network Cable	Cables for the Smoke Sensor
Core wire 1 (orange-white), core wire 8 (brown)	GND (black)
Core wire 3 (green-white)	+12 V (red)
Core wire 6 (green)	Normally closed end (yellow)
Core wire 7 (brown-white)	Common end (green)
None (reserved, cable connection not required, only insulation required)	Normally opened end (blue)

- Step 4** Connect one end of the RJ45 network cable to the AI/DI port on the ECC800-Pro collector or a UIM20A expansion module.

----End

4.3.6.5 Connecting a Monitoring Cable to a T/H Sensor

Procedure

- Step 1** Connect one end of the network cable to the pins of the T/H sensor.
 - Connect the T/H sensor (BOM number: 33010346) to the RS485 port.
 - Connect the T/H sensor (BOM number: 02312PBL) to the RJ45 port.

Figure 4-44 Interface for the T/H sensor network cable

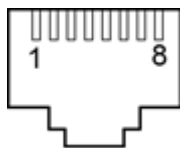


Table 4-50 Network cable wire sequence

PIN	Definition
pin1	RS485 (A)
pin2	RS485 (B)
pin3	V+12V input
pin4	-
pin5	-
pin6	-
pin7	-
pin8	V-12V input

Step 2 Connect the other end of the network cable to the COM1/AIDI_1, COM3/AIDI_3, COM5/AIDI_5, or COM7/AIDI_7 port on the UIM20A expansion module.

----End

4.3.6.6 Connecting a Monitoring Cable to the Region-type Water Sensor

Prerequisites

A monitoring cable is prepared.

Procedure

Step 1 Connect one end of the network cable to the Ethernet port on the water detector.

Step 2 Connect the other end of the network cable to the AI/DI port on the ECC800-Pro collector or the UIM20A expansion module.

----End

4.3.6.7 Connecting a Monitoring Cable to the Location-type Water Sensor

Prerequisites

A network cable used for monitoring is prepared.

Procedure

- Step 1** Connect one end of the network cable to the RJ45 port on the tie line.
- Step 2** Connect the other end of the network cable to the live COM port on the ECC800-Pro or the UIM20A expansion module.

----End

4.3.6.8 Connecting a Monitoring Cable to the Infrared Sensor

Prerequisites

A network cable used for monitoring is prepared.

Context

When connecting an infrared sensor to the ECC800-Pro collector, you need to perform the following steps to prepare a special monitoring cable.

Procedure

- Step 1** Prepare an RJ45 connector on one end of the network cable by following to the instruction in [4.3.1 Preparing a Monitoring Cable](#).
- Step 2** Connect the network cable to the infrared sensor terminals, as shown in [Table 4-51](#).

Table 4-51 Connecting the cable to the infrared sensor

Network Cable Core	Infrared Sensor Terminal
Core wire 3 (green-white)	+12V
Core wire 8 (brown)	GND
Core wire 6 (green)	ALARM
Core wire 7 (brown-white)	ALARM
None (reserved, cable connection not required, only insulation required)	TAMPER

- Step 3** Connect one end of the RJ45 network cable to the AI/DI port on the ECC800-Pro collector.

----End

4.3.7 Connecting the Smart Cooling Product Monitoring Cable

4.3.7.1 Connecting the NetCol5000 Monitoring Cable

Prerequisites

A network cable used for monitoring is prepared.

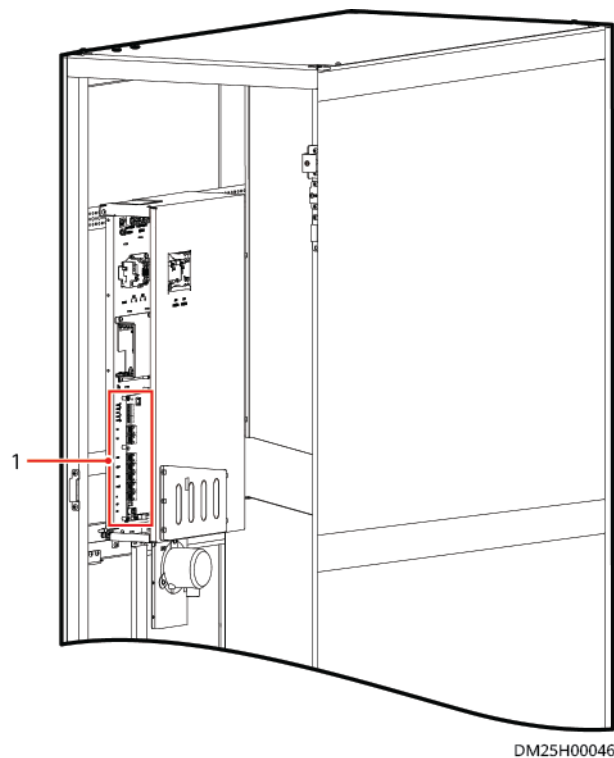
Context

When NetCol5000-C(065, 080) or NetCol5000-A050/A042/A035/A025/A020/C030 connects to the NetEco over Modbus RTU, connect cables by referring to this section.

Procedure

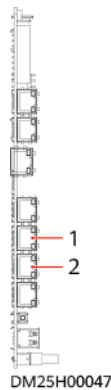
- Step 1** Connect one end of the network cable to the communications port on the NetCol5000 side panel.
- The COM port of NetCol5000-C(065, 080) is on the main control board at the smart cooling product rear doors.

Figure 4-45 NetCol5000-C(065, 080) main control board



(1) Main control board

Figure 4-46 COM ports



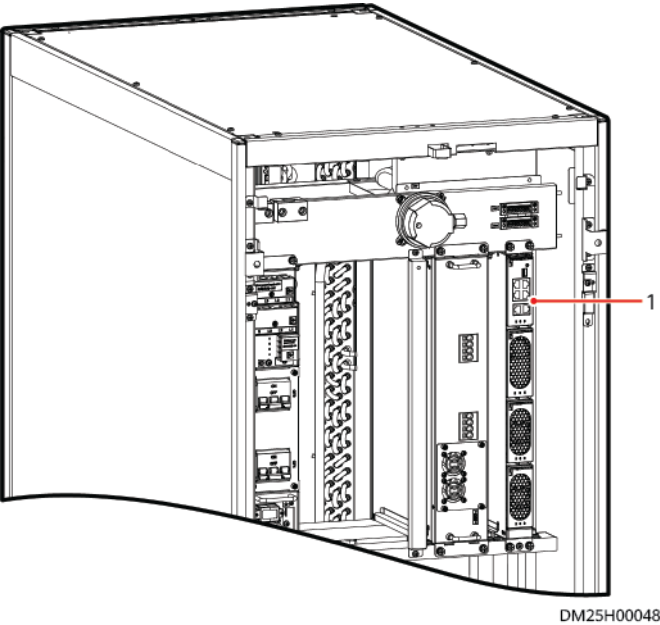
(1) COM1 port

(2) COM2 port

NOTE

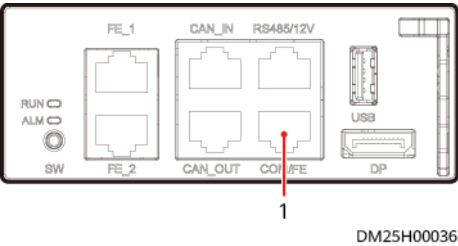
- When there is only one smart cooling product, it communicates with the ECC collector over the COM1 port.
- If multiple smart cooling products are networked, connect the COM1 port on the first smart cooling product to the COM port on the ECC collector, connect the COM2 port on the first smart cooling product to the COM1 port on the second smart cooling product, and connect the other smart cooling products in the same way. A maximum of four smart cooling products can be networked.
- Both the COM ports of NetCol5000-A050, NetCol5000-A042, NetCol5000-A035 and NetCol5000-A025 are on the main control modules at the smart cooling product rear doors. The NetCol5000-A042 is used as an example to show the position of the main control module.

Figure 4-47 NetCol5000-A042 main control module



(1) Main control module

Figure 4-48 COM port on the main control module



(1) COM port

- Open the smart cooling product rear door, remove the filter, and connect the network cable to the communications port J73 on the main control module in NetCol5000-A020/NetCol5000-C030.

NOTE

The following figure shows the pin sequence of the network cable that connects to the J73 communications port.

Figure 4-49 Pin sequence of a network cable

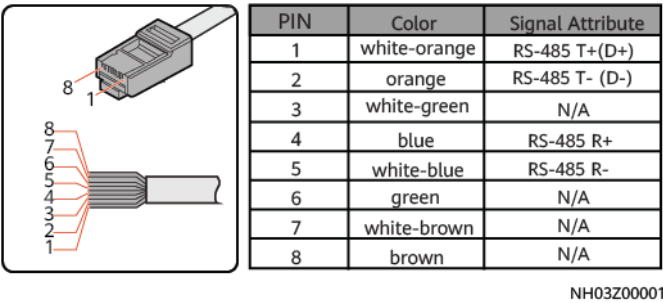
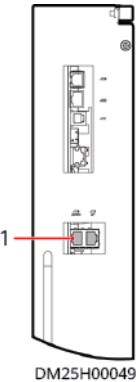


Figure 4-50 NetCol5000-A020/NetCol5000-C030 communications port J73

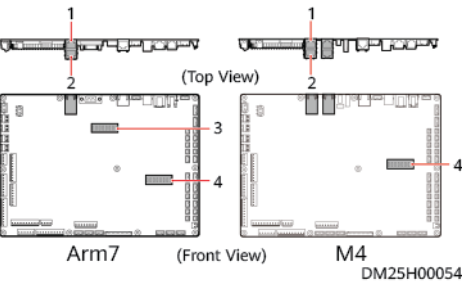


(1) J73 (teamwork bus port and host monitoring port)

NOTICE

- The main control board can be Arm7 or M4. The appearance varies with the model delivered.
- The Arm7 main control board has S1 and S2 DIP switches, and the M4 main control board has only the S2 DIP switch. The S1 DIP switch needs to be set for the Arm7 main control board and does not need to be set for the M4 main control board.
- The Arm7 main control board uses the software of V100R001, and the M4 main control board uses the software of V100R002.
- You need to set only the seventh toggle switch based on teamwork requirements and leave other toggle switches in their default status.

Figure 4-51 NetCol5000 main control board



- (1) Teamwork communications port 1
- (2) Teamwork communications port 2
- (3) S1 DIP switch of the main control board
- (4) S2 DIP switch of the main control board

Table 4-52 Operations of the DIP switch

Toggle Switch	Default Value	Operations
1	OFF	Remaining in OFF

Toggle Switch	Default Value	Operations
2	OFF	Remaining in OFF
3	ON	Remaining in ON
4	ON	Remaining in ON
5	OFF	Remaining in OFF
6	ON	Remaining in ON
7	OFF	- Not in teamwork mode: Remaining in OFF - In teamwork mode: Set toggle switch 7 on the main control boards of the first and last smart cooling products to ON, and toggle switch 7 on the main control boards of the other smart cooling products to OFF.
8	ON	Remaining in ON

Step 2 Connect the other end of the network cable to the COM port on the ECC800-Pro collector or the UIM20A expansion module.

----End

4.3.7.2 Connecting the NetCol8000 Monitoring Cable

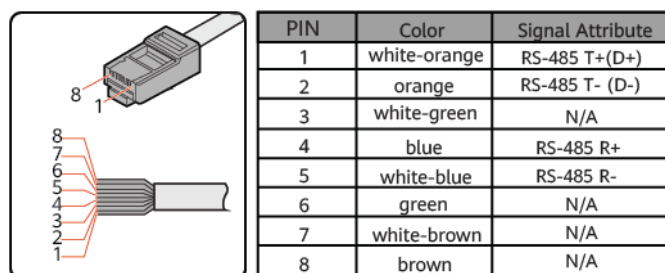
Prerequisites

A network cable used for monitoring is prepared.

Context

- When NetCol8000-C070/C150, NetCol8000-A050/A060/A100/A120, or FusionCol8000-E220/E400/C080/C210 connects to the NetEco over Modbus RTU, connect cables by referring to this section.
- The following figure shows the pin sequence of the network cable.

Figure 4-52 Pin sequence of a network cable

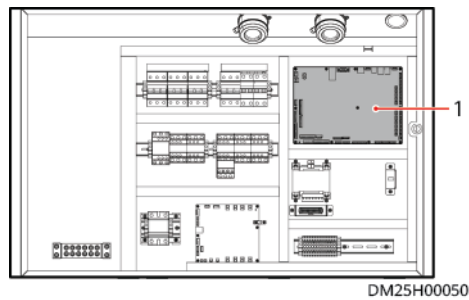


NH03Z00001

Procedure

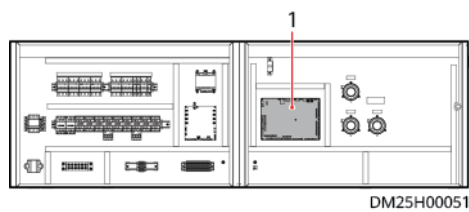
- Step 1** Connect one end of the network cable to the monitoring port on the smart cooling product.
- For NetCol8000-A050/A100/C070/C150, open the front door of the cabinet and connect one end of the network cable to teamwork communications port 1 or 2 on the main control board of the cabinet.

Figure 4-53 Main control board of the NetCol8000-A050



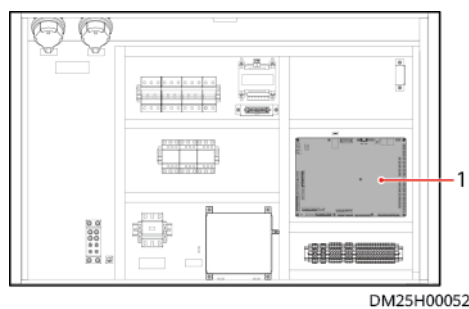
(1) Main control board

Figure 4-54 Main control board of the NetCol8000-A100



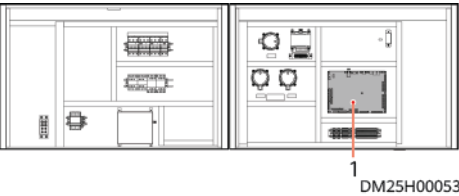
(1) Main control board

Figure 4-55 Main control board of the NetCol8000-C070



(1) Main control board

Figure 4-56 Main control board of the NetCol8000-C150

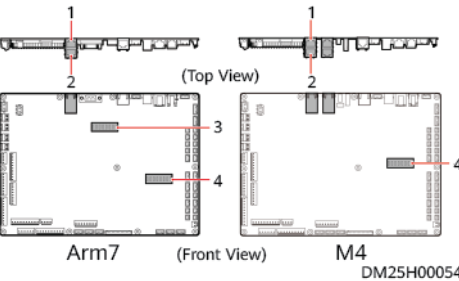


(1) Main control board

NOTICE

- The main control board can be Arm7 or M4. The appearance varies with the model delivered.
- The Arm7 main control board has S1 and S2 DIP switches, and the M4 main control board has only the S2 DIP switch. The S1 DIP switch needs to be set for the Arm7 main control board and does not need to be set for the M4 main control board.
- The Arm7 main control board uses the software of V100R001, and the M4 main control board uses the software of V100R002.
- You need to set only the seventh toggle switch based on teamwork requirements and leave other toggle switches in their default status.

Figure 4-57 NetCol8000 main control board



- (1) Teamwork communications port 1
- (2) Teamwork communications port 2
- (3) S1 DIP switch of the main control board
- (4) S2 DIP switch of the main control board

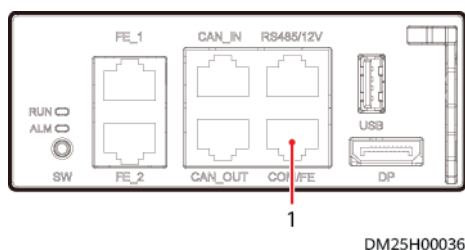
Table 4-53 Operations of the DIP switch

Toggle Switch	Default Value	Operations
1	OFF	Remaining in OFF
2	OFF	Remaining in OFF
3	ON	Remaining in ON
4	ON	Remaining in ON
5	OFF	Remaining in OFF

Toggle Switch	Default Value	Operations
6	ON	Remaining in ON
7	OFF	- Not in teamwork mode: Remaining in OFF - In teamwork mode: Set toggle switch 7 on the main control boards of the first and last smart cooling products to ON, and toggle switch 7 on the main control boards of the other smart cooling products to OFF.
8	ON	Remaining in ON

- For NetCol8000-A060/A120 or FusionCol8000-E220/E400/C080/C210, open the rear door and connect one end of the network cable to the COM/FE port on the main control module of the smart cooling product.

Figure 4-58 Main control module



(1) COM/FE port

- Step 2** Connect the other end of the network cable to the COM port on the ECC800-Pro collector or the UIM20A expansion module.

----End

4.3.8 Connecting a Monitoring Cable to a Chiller

Prerequisites

A network cable used for monitoring is prepared.

Procedure

- Step 1** Connect one end of the network cable to the COM port on the chiller.
- Step 2** Connect the other end of the network cable to the COM port on the ECC800-Pro collector or the UIM20A expansion module.

----End

4.3.9 Connecting the UPS Monitoring Cable

4.3.9.1 Connecting a Monitoring Cable to the UPS2000-G (Modbus)

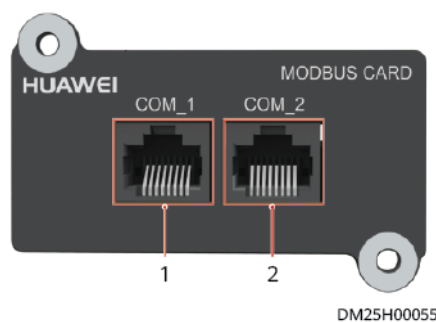
Prerequisites

A network cable used for monitoring is prepared.

Procedure

- Step 1** Connect one end of the network cable to the COM_1 or COM_2 port on the Modbus expansion card of the UPS2000-G.

Figure 4-59 RS485 port



(1) COM1 port (RS485 supported)

(2) COM2 port (RS485 supported)

- Step 2** Connect the other end of the network cable to the COM port on the ECC800-Pro collector or the UIM20A expansion module.

----End

4.3.9.2 Connecting a Monitoring Cable to the UPS5000-A

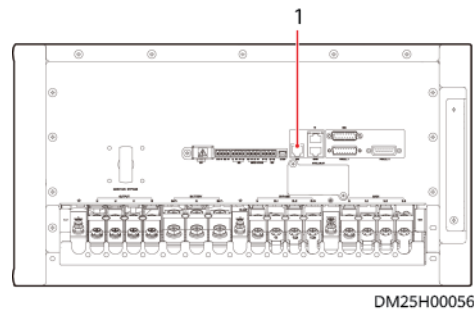
Prerequisites

A network cable used for monitoring is prepared.

Procedure

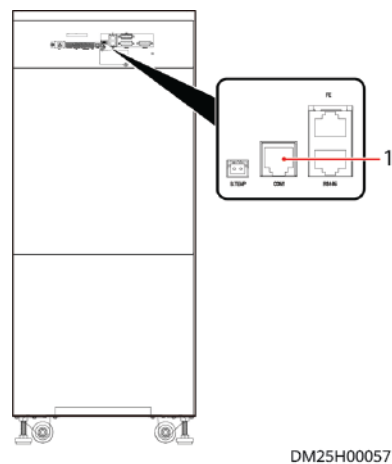
- Step 1** Connect one end of a network cable to the COM port of the UPS5000-A.

Figure 4-60 UPS5000-A-30 kVA/40 kVA functional components and control signal ports



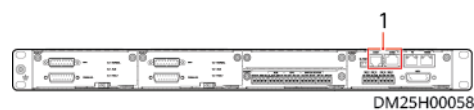
(1) COM port

Figure 4-61 UPS5000-A-60 kVA/80 kVA/120 kVA functional components and control signal ports



(1) COM port

Figure 4-62 COM port on the UPS monitoring module of the 300 kVA UPS and models with higher capacities



(1) COM port

Step 2 Connect one end of the network cable to the COM port on the ECC800-Pro collector or the UIM20A expansion module.

----End

4.3.10 Connecting the PDC Monitoring Cable

4.3.10.1 Connecting the PDU8000 Monitoring Cable

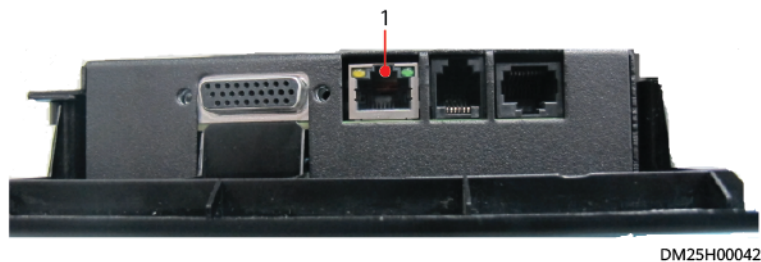
Prerequisites

A network cable used for monitoring is prepared.

Procedure

- Step 1** Connect one end of the network cable to the COM port in the display panel of PDU8000.

Figure 4-63 Connecting the PDU8000 monitoring cable (COM port)



(1) COM port

- Step 2** Connect the other end of the network cable to the COM port on the ECC800-Pro collector or the UIM20A expansion module.

----End

4.3.10.2 Connecting a Monitoring Cable to the Monitoring Type-PDU2000-32-1PH-20/4-M1

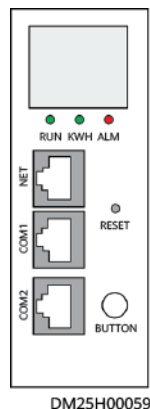
Prerequisites

A network cable used for monitoring is prepared.

Procedure

- Step 1** Connect one end of the network cable to the COM1 port or the COM2 port on the PDU2000.

Figure 4-64 PDU2000 ports



Step 2 Connect the other end of the network cable to the COM port on the ECC800-Pro collector or the UIM20A expansion module.

Step 3 (Optional) If multiple PDU2000s need to be cascaded, connect the COM1 or COM2 port of one PDU2000 to the COM1 or COM2 port on the next PDU2000.

 NOTE

A maximum of four PDU2000s can be cascaded.

----End

4.3.10.3 Connecting a Monitoring Cable to an HPXPDU2000-16-3PH-24-6-M1

Prerequisites

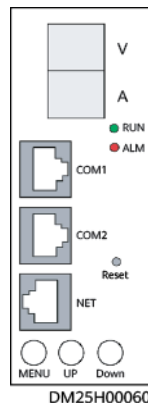
A network cable used for monitoring is prepared.

Procedure

Step 1 Connect the monitoring cable.

1. Connect one end of the network cable to port COM1 or COM2 on the PDU2000. [Figure 4-65](#) shows the ports on the PDU2000.

Figure 4-65 PDU2000 ports



2. Connect the other end of the network cable to the COM port on the ECC800-Pro collector or the UIM20A expansion module.

Step 2 (Optional) Connect PDU2000 cascading cables. Use a common network cable to connect port COM1 or COM2 on the PDU2000 to port COM1 or COM2 on another PDU2000.

 NOTE

- A maximum of four PDU2000s can be cascaded.
- If PDU2000s are cascaded, you need to connect only one PDU2000 to the ECC800-Pro collector.

----End

4.3.11 Connecting the Fresh Air Unit Monitoring Cable

4.3.11.1 Connecting a Monitoring Cable to the Fresh Air Unit

Prerequisites

A network cable used for monitoring is prepared.

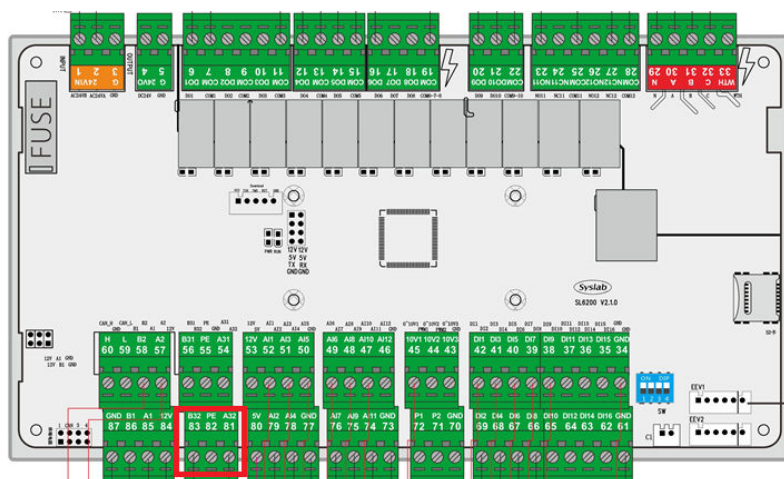
Procedure

- Step 1** Connect core wires 1 (orange-white) and 2 (orange) at one end of the network cable to pins 81 and 83 of the fresh air unit controller respectively.

NOTE

Pin 81 is defined as RS485+, and pin 83 is defined as RS485-.

Figure 4-66 Positions of pins 81 and 83



- Step 2** Connect the other end of the network cable to the COM port on the ECC800-Pro collector or the UIM20A expansion module.

----End

4.4 Scenarios for Connecting the ECC800-Pro in the Smart Module

4.4.1 Connecting a Monitoring Cable to the ECC800-Pro Collector

Procedure

- Step 1** For details about how to connect monitoring cables to the ECC800-Pro, see the *Smart Modular Data Center Management System Wiring Diagram*.

 NOTE

The onsite wiring diagram of the management system prevails. The method described in this section is for reference only.

----End

5 Checking the Installation

5.1 Checking the Installation of the Cabinet

SN	Check Item
1	The cabinet is placed as designed.
2	The rack is secure and reliable and meets the anti-seismic requirements. The horizontal and vertical differences do not exceed 3 mm. You can use a horizontal ruler and a lead ruler to measure the differences.
3	If the cabinet is placed on an ESD floor, all the expansion bolts of the supports are secure with the floor; the installation sequence of the insulation washers, flat washers, spring washers, and nuts (bolts) are correct; the installation holes of the supports are secure with the expansion bolts. The supports are insulated from the floor and guide rails. The resistance of all the insulated points between the supports and cabinets measured by the MΩ level of the multimeter is greater than 5 MΩ.
4	All the screws are secure; a flat washer and a spring washer are installed for each screw; the washers are properly placed.
5	The cabinets are arranged in order. The cabinet queue at both sides of the passage is straight, and the difference does not exceed 5 mm.
6	The connecting plates are installed properly when two cabinets are deployed on one site.
7	The front, side, and rear doors of the cabinets are installed. The front and rear doors can be opened and closed. The door locks function normally.
8	The exteriors and interiors of the cabinets (including the front door, rear door, and sides of each cabinet) are clean. No dirt, damage, or fingerprint is allowed.

SN	Check Item
9	All the outlets or inlets of the cabinets are sealed. The gap around a cover plate does not exceed the width of the cover plate. If a bag is used, the opening of the bag is tied up. The sizes of the outlets that use plastics are appropriate. You can use other appropriate, insulated, or flame-resistant materials to seal the outlets.
10	There are excessive hair bands, lines, and other wastes.
11	All the configured filler panels are installed.
12	The ESD wrist strap is inserted into the ESD installation hole.
13	The cabinet labels are smooth and tidy.

5.2 Checking the Installation of Components in the Cabinet

SN	Check Item
1	The devices are installed in the correct positions as designed.
2	All the panel screws of the devices are installed and secure.
3	The panel and exterior of each device are not dirty, and the paint is not scraped off.
4	The labels (coating of the subrack, plate nameplate, transport label, and product nameplate) of each device are not peeled off.
5	The bar code of each device is not peeled off.
6	The ejector lever of each board is placed in position.
7	The captive screws of each board are secure.
8	There is no vacant slot in the subrack, and filler panels are installed in vacant slots.
9	A protective cover is installed for the power module if the power module is configured with a protective cover.

5.3 Checking the Installation of Power Cables and Ground Cables

SN	Check Item
1	All the power cables and ground cables are copper-core cables.
2	There are no solder joints or connectors in power cables and ground cables.
3	The extra length of power cables or ground cables is truncated and the cables are not coiled.
4	There is no breaking equipment such as switches and fuses in the electrical connection of the grounding system.
5	The ground bars and PGND bars are connected to one grounding conductor.
6	The OT terminals at both ends of the power cables or ground cables are crimped securely.
7	The bare wires and OT terminals at the wiring terminals are tightly wrapped up with PVC insulation tapes or heat shrink tubing.
8	The power cables and ground cables connecting the PDB with each device, and the ground cables connecting each device with the PGND busbar of the cabinet are all correctly installed and have good contact.
9	The power cables and ground cables are bound separately from other cables.
10	Labels are attached at both ends of the power cables and ground cables.
11	The plastic cover plate on the top of wiring terminals of the PDB is properly installed.

5.4 Checking the Connection of Signal Cables

SN	Check Item
1	There are no solder joints or connectors in signal cables. The signal cables are not scratched or broken.
2	The connectors of signal cables are tight and secure.
3	Proper length of the cable is reserved at the connectors.
4	Proper length is reserved for signal cables at turning points. The turning radius meets the requirement.
5	The optical fibers must be sheathed using corrugated pipes at outsides of cabinets. Both ends of the pipes must be fastened. The edges are smooth or be processed for cutting prevention.
6	No other cables are laid on optical fibers.

SN	Check Item
7	The extra optical cables are coiled on the cable coiler at the rear of the cabinet.
8	The signal cables connected to the left part of the subrack are led out of the subrack from the left. Similarly, the signal cables connected to the right part of the subrack are led out of the subrack from the right.
9	The signal cables are bound separately from the power cables. The signal cables are bound and arranged neatly and closely. The cable ties are spaced evenly. The tips of the cable ties point to the same direction.
10	The extra length of the cable ties must be cut and the cut surface must be smooth.
11	The cables whose connectors are far away from the cable entrance are arranged at the external side of the cable bundle, while those near the entrance are arranged at the internal side of the cable bundle. The trunk cables are laid out smoothly without any tangling.

6 Adding Devices

6.1 Performing Basic Operations Before Adding Devices

Software installation and commissioning are required before the device commissioning, collector commissioning, and NetEco commissioning. For details, see **NetEco Product Documentation**. Commission the software by referring to relevant sections in **NetEco Software Installation and Commissioning Guide**.

Table 6-1 Encryption algorithms

Insecure Encryption Algorithm	Secure Encryption Algorithm
• DES/3DES (except the scenario where $K1 \neq K2 \neq K3$) • SKIPJACK • RC2 • RSA (1024-bit or shorter) • MD2/MD4 • MD5 is used in scenarios where digital signatures are generated or passwords are encrypted for storage. • SHA1 is used in scenarios where digital signatures are generated.	• Symmetric encryption algorithm: AES (128-bit or longer) • Asymmetric encryption algorithm: RSA (2048-bit or longer) • Hash algorithm: SHA2 (256-bit or longer) • Hash-based message authentication code (HMAC) algorithm: HMAC-SHA2

Table 6-2 Communication protocols

Insecure Communication Protocol	Secure Communication Protocol
SNMPv1/v2	SNMPv3
IPMI 1.5	IPMI 2.0

Insecure Communication Protocol	Secure Communication Protocol
Non-SSL protocol, SSL 2.0, and SSL 3.0	TLS 1.2
TLS 1.0 and TLS 1.1	N/A

NOTICE

- The device may use insecure algorithms and protocols, which may pose security risks. You are advised to replace the device with a device that supports secure algorithms and protocols or upgrade the device to a version that supports secure algorithms and protocols.
- In transparent transmission channel management settings, the compatibility mode has security risks. You are advised to select the security protocol mode.

6.1.1 IP Address Preinstallation Planning

The IP address must be in compliance with the following requirements:

- The static IP address must be used.
- The IP address must be unique on the live network.
- You can plan only one IP address for one network interface. It is not allowed to plan or set multiple IP addresses for the same network interface.
- The NetEco server can communicate with managed devices.
- The NetEco server can communicate with Web clients.

NOTE

The subnet mask of all IP addresses is **255.255.255.0**.

Table 6-3 IP address list

Item	Preinstallation Setting	Description
Server IP address	192.168.8.11	Used for logging in to the NetEco and PowerEcho.

6.1.2 Obtaining the NetEco Software License

The NetEco software license is not provided together with software to the customer. Therefore, obtain the NetEco software license in advance.

Obtain the license from the Huawei's enterprise support website.

- For enterprise users:
 - a. Log in to Huawei's enterprise support website <https://support.huawei.com/enterprise>.

- b. Browse or search for **iManager NetEco 6000 License Application Guide**, and apply for the license of the NetEco software by referring to the guide.
- For carriers:
 - a. Log in to Huawei's carrier support website <https://support.huawei.com>.
 - b. Browse or search for **iManager NetEco 6000 License Application Guide**, and apply for the license of the NetEco software by referring to the guide.

6.1.3 Powering On a Server

This topic describes how to power on a server.

Procedure

- Step 1** Check that the power cables and ground cables of the upstream components of the server are securely connected with correct polarity and in good contact.
- Step 2** Ensure that the upstream input power supply is not connected. Use a multimeter to measure the resistance between the upstream output power supplies and between the working ground and the protection ground. It is required that short circuits not occur between power outputs or between the working ground and protective ground.
- Step 3** Turn on the switch for the upstream power supply of the server.
- Step 4** Press the power button on the chassis of the server to power on the server.

NOTE

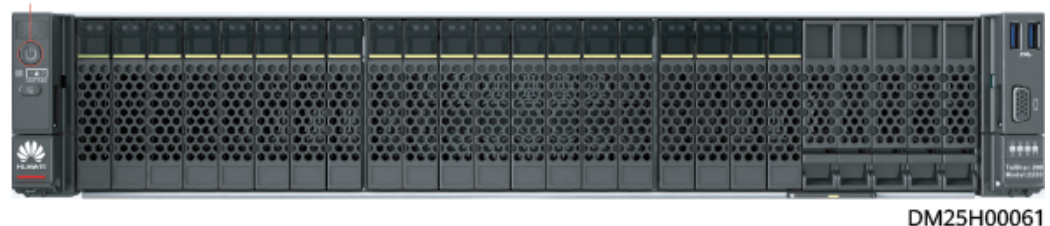
After the server is started properly, the button/indicator of its power switch is displayed green.

Figure 6-1 Power button on the 2288X V5 server



Figure 6-2 TaiShan 200 server power button

Power



----End

6.1.4 Logging In to the NetEco Client

This section describes how to log in to the NetEco client using a web browser.

Prerequisites

Valid user name and password are available.

Procedure

- Step 1** In the browser address box, enter `https://IP address of the NetEco server:31943`, and then press **Enter**.

 NOTE

- 192.168.8.11 is the default IP address of the NetEco.
- Latest Chrome (Stable Channel) and Firefox (ESR Release) are recommended.
- You are advised to set the display resolution as 1920*1080 or higher.
- Make sure that the IP address of the NetEco server is not contained in the compatibility view website.

- Step 2** Enter the **User Name**, **Password**, and click **Login**.

 NOTE

- The preset user of NetEco is **admin**, the preset password is **Changeme_123**. This user has all the operation rights on the managed objects. 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.
- If the number of online users reaches the maximum number supported by the system, a message is displayed, indicating that you cannot log in. In this case, contact the system administrator.
- After you enter the incorrect password for three consecutive times, you must enter the verification code upon the fourth login. After you enter the incorrect password for five consecutive times, the user account or the IP address is locked for 10 minutes.

----End

6.1.5 Loading the NetEco Software License

The NetEco license file is used to control the functions and management capabilities of the NetEco. Before using NetEco, you need to load a commercial license.

Prerequisites

- You have obtained a license.
- You have logged in to the NetEco client using a web browser.

Procedure

- Step 1** Click **Import License file** when you log in to the NetEco at the first time.

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

Step 3 Click **Upload**.

The information about the imported license file is displayed.

Step 4 Click **Apply**.

----End

6.1.6 Installing NE Adapters

Prerequisites

You have logged in to the NetEco client using a browser.

Procedure

Step 1 Obtain the adapter software installation packages.

- For enterprise users:
 - a. Log in to Huawei's enterprise support website <https://support.huawei.com/enterprise>.
 - b. Obtain **iManager NetEco 6000 V600R021C00SPCXXX ReleaseDoc_ENG.zip**, **NetEco6000_V600R021C00SPCXXX_Adapters.zip**, and **NetEco6000_V600R021C00SPCXXX_DomainAdapters.zip** from **Support > Digital Power > Fusion Modular Data Center > iManager NetEco 6000**. Decompress the files and locate the mediation software installation packages in the **NetEco6000_V600R021C00SPCXXX_Adapters** and **NetEco6000_V600R021C00SPCXXX_DomainAdapters** folders based on the NE types and versions in *iManager NetEco 6000 V600R021 Version Mapping Table*.
- For carriers:
 - a. Log in to Huawei's carrier support website <https://support.huawei.com>.
 - b. Obtain **iManager NetEco 6000 V600R021C00SPCXXX ReleaseDoc_ENG.zip**, **NetEco6000_V600R021C00SPCXXX_Adapters.zip**, and **NetEco6000_V600R021C00SPCXXX_DomainAdapters.zip** from **Support > Product Support > Digital Power > Data Center Facility > Fusion Modular Data Center > iManager NetEco 6000**. Decompress the files and locate the adapter software installation packages in the **NetEco6000_V600R021C00SPCXXX_Adapters** and **NetEco6000_V600R021C00SPCXXX_DomainAdapters** folders based on the NE types and versions in *Manager NetEco 6000 V600R021 Version Mapping Table*.

Step 2 Choose **System > Service Settings > Adapter Management** from the main menu.

Step 3 Click **Upload**. On the displayed **Upload Adapter Package** page, click + and select the files to be uploaded.

Step 4 Click **Upload** to upload the files.

Step 5 Select the NE adapter packages to be installed on the **Adapter Management** page, and click **Install**. Then, click **Yes** in the displayed dialog box. The time

required for the installation is related to the number of adapters. Wait for the installation to complete.

----End

6.1.7 Creating a Management Domain

This section describes how to create a management domain.

Prerequisites

- You have logged in to the NetEco client using a web browser.
- The management domain adapter has been preconfigured or installed.

Context

The management domains include **Park**, **Building**, **Room**, **ContainerDC**, **Subnet**, **NetecoSite**, **FusionModule500**, **Modular**, **Room-ShapeNode**, and **Building-ShapeNode**. You are advised to plan the subordinate relationship between domains and devices before performing operations.

The NetEco is preconfigured with management domains such as cabinets, battery cabinets, buildings, containers, floors, FusionModule500, smart modules, NetEco sites, parks, PDCs, equipment rooms, and subnets. To use more management domains, you need to install the corresponding adapter software package on the NetEco.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Add a management domain.

1. In the navigation tree, choose the upper-level node where you want to add a management domain.
2. In the **Domain** area which is below the navigation tree, drag a management domain icon to the required position in the view.

NOTE

You can adjust the shape of **Room**, **Room-ShapeNode**, **Building-ShapeNode**, **Floor-ShapeNode**, **Container-ShapeNode**, and **NetecoSite** by: Holding down the **Shift** key and the left mouse button and then clicking on the corresponding frame lines can increase the small yellow dot. You can drag the small yellow dot to adjust the shape of the managed domain icon.

To delete a domain, click the domain icon and select **Delete** under .

3. In the right side of the view area, set **Management Info**. Set parameters as required. The parameter marked with an asterisk (*) is mandatory.

NOTE

You can configure **Management Info**, **Electricity Info**, and **Refrigeration Info** for the equipment room management domain.

4. Click  on the toolbar.

Repeat steps [Step 2.1](#) to [Step 2.4](#) until the configuration is complete.

Step 3 Click  on the toolbar.

----End

6.1.8 Adding a Module

This section describes how to create a module in the root node, subnet, equipment room, Container, or site management domain.

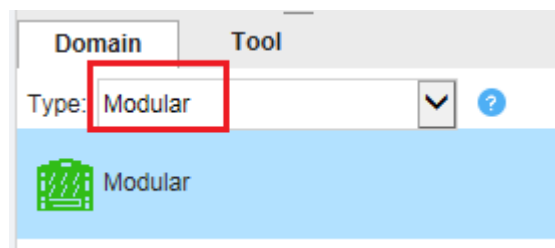
Prerequisites

- You have logged in to the NetEco client using a web browser.
- You have created management domains in **Data Center Planning**. For detailed operations, see *Creating a Domain*.

Procedure

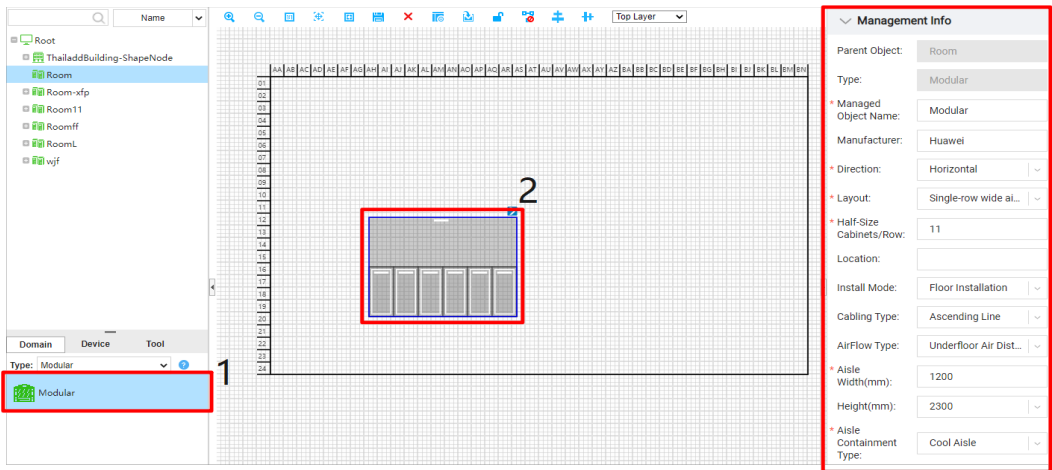
- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** window is displayed.
- Step 2** Choose the management domain where you want to add a modular from the navigation tree on the left.
- Step 3** Click **Domain**. The infrastructure area is displayed.
- Step 4** Select **Modular** from the **Type** drop-down list.

Figure 6-3 Selecting the modular



- Step 5** Select the **Modular** to be added and drag the modular icon to the **Room** area.

Figure 6-4 Adding the modular in the room area



Step 6 Modify **Management Info** of the module or retain the default values, and then click .

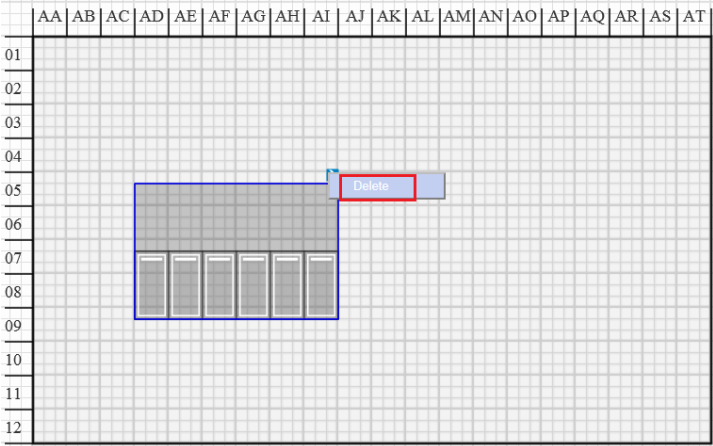
NOTICE

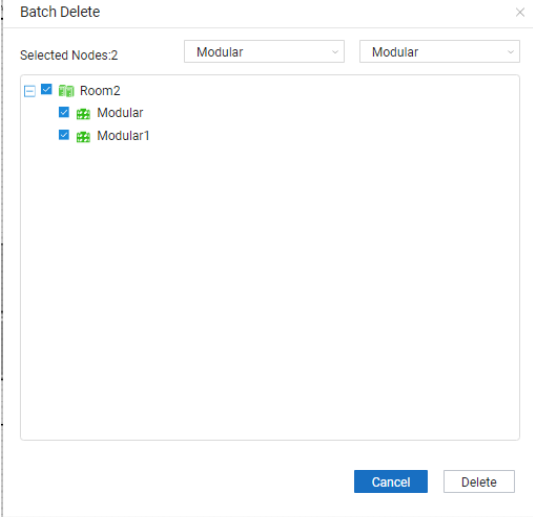
The parameters with * are mandatory.

----End

Follow-up Procedure

Perform the following operations in the **Data Center Planning** page as required.

If You Need To...	Then...
Delete modules	You can delete one module or multiple modules in batches on the current page. NOTE If a module contains subdevices, you cannot delete it. You can delete the module only after you delete subdevices in the module. • Delete one module. 1. Select Modular and click Delete under , as shown in Figure 6-5. Figure 6-5 Deleting one module  2. In the displayed Confirm dialog box, click Yes. • Delete multiple modules in batches. 1. Click  on the toolbar to display the Figure 6-6 page.

If You Need To...	Then...
	Figure 6-6 Deleting multiple modules in batches  2. Add filter conditions, select multiple modules and click Delete. 3. In the displayed Confirm dialog box, click Yes.
Add tools	1. Select the module for which you want to add a pillar. 2. In the lower left corner of the current page, click Tool. 3. Select the Pillar component to be added. NOTE After the component is added, you can set attributes for the component in the Component Info list in the right pane. The system automatically displays values for Parent Name and Control Type, and you do not need to manually set them, you only need to set Name. 4. In the upper area of the current page, click .

6.1.9 Process of adding a device

Prerequisites

- You have logged in to the NetEco client using a web browser.
- You have the operation rights for **Data Center Planning**.

Interface Introduction

Figure 6-7 Adding a device

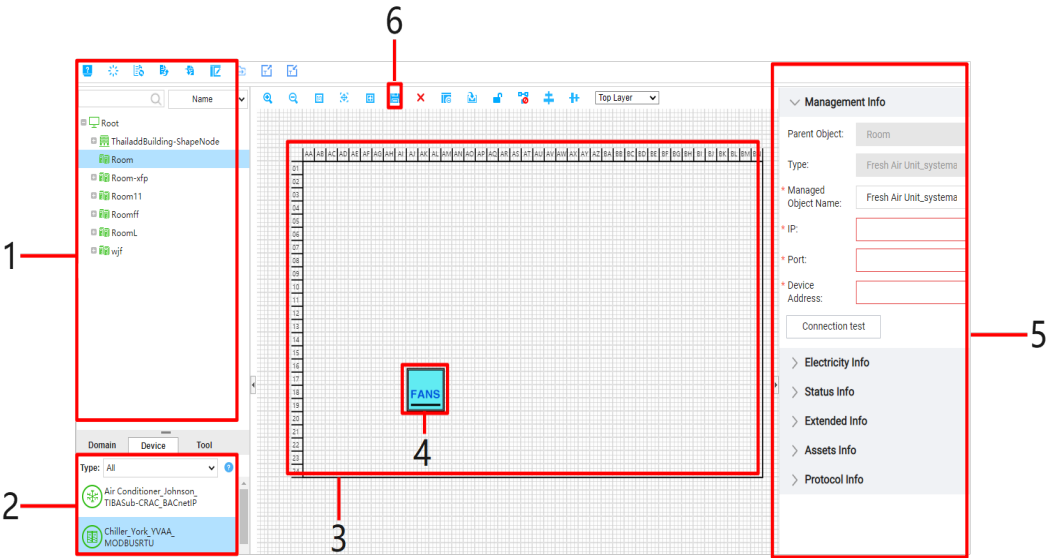


Table 6-4 Description of the page for adding a device

Area	Operation
(1) Management domain navigation tree	In the management domain navigation tree, select the management domain to which the device to be added belongs.
(2) Device selection area	Click the Device tab, select a device type from the drop-down list box, and click the device to be added.
(3) Management domain	Drag the selected device to the management domain.
(4) Device	Click the device. The parameter setting area is displayed in the right pane.
(5) Parameter setting area	Set device parameters in the parameter setting area.
(6) Save	Click Save. The device is added.

6.2 Scenarios for Connecting the ECC800-Pro in the Smart Module

6.2.1 Commissioning Southbound Devices of the ECC800-Pro

For details, see the commissioning documents of solutions such as FusionModule500/FusionModule800/FusionModule1000/FusionModule2000.

6.2.2 Adding a Smart U Space Manager

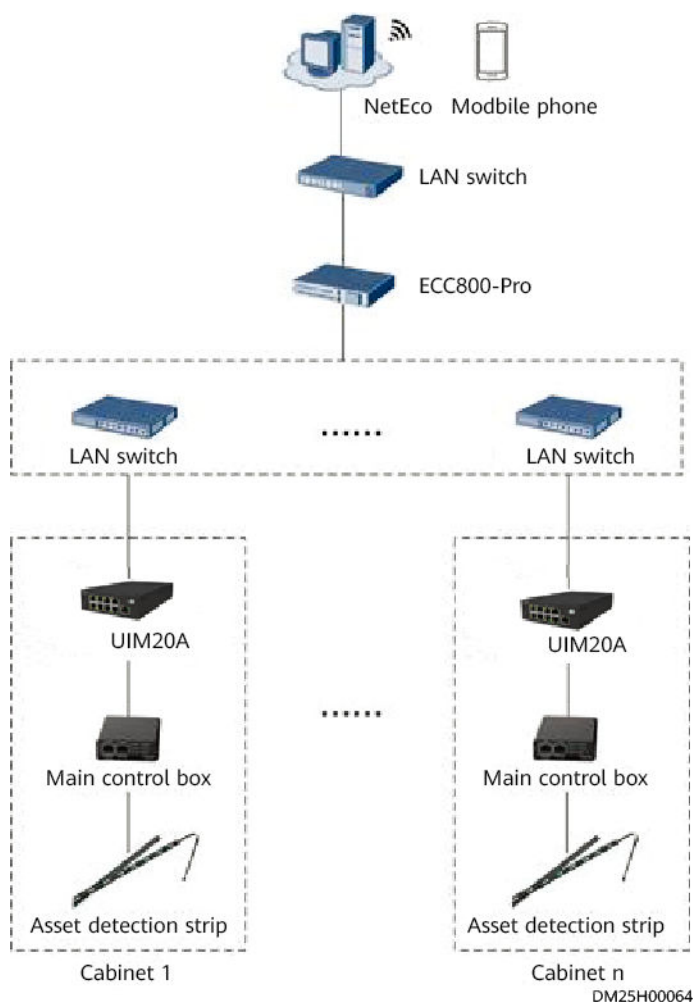
Prerequisites

The ECC800-Pro has been added on the NetEco.

Context

This topic describes how to connect a smart U space manager to the ECC800-Pro. After the ECC800-Pro is connected to the NetEco, the NetEco can manage the smart U space manager.

Smart U Space Manager Networking



6.2.2.1 Commissioning the Smart U Space Manager on the ECC800-Pro WebUI

Prerequisites

- Connect the smart U space manager to the COM port on the UIM20A expansion module.

NOTE

- In a standard scenario, connect a smart U space manager to the COM6/AIDI_6 port on the UIM20A expansion module.
- In a scenario where one UIM20A expansion module maps to four cabinets, connect smart U space managers to the COM1/AIDI_1, COM3/AIDI_3, COM5/AIDI_5, and COM7/AIDI_7 ports on the UIM20A expansion module. If the number of IT cabinets is not an integer multiple of 4, according to the cable connection rules, leave the unconnected COM ports on the UIM20A expansion module idle.
- The smart U space manager has been connected to the ECC800-Pro through automatic discovery.

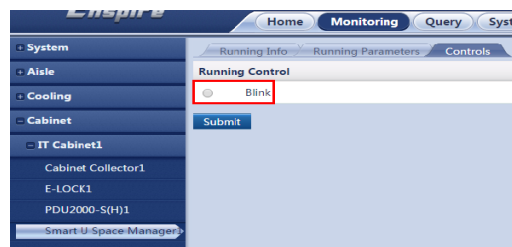
Procedure

Step 1 Log in to the ECC800-Pro WebUI as an administrator.

Step 2 View the position of the smart U space manager.

- Choose **Monitoring > Cabinet > IT Cabinet n > Smart U Space Manager**.
- Select **Running Control** and click **Blink**. In the actual environment, you will see that the smart U space manager blinks to ensure that the device location in the view is consistent with that in the smart module.

Figure 6-8 Viewing the position of the smart U space manager



----End

6.2.2.2 Determining the Position of the Smart U Space Manager (Connected to a UIM20A Expansion Module)

If a smart U space manager is installed, perform the following steps to configure it.

Prerequisites

- The smart U space manager has been connected to a COM port on the UIM20A expansion module.

 NOTE

- In a standard scenario, connect a smart U space manager to the COM6/AIDI_6 port on the UIM20A expansion module.
- In a scenario where one UIM20A expansion module maps to four cabinets, connect smart U space managers to the COM1/AIDI_1, COM3/AIDI_3, COM5/AIDI_5, and COM7/AIDI_7 ports on the UIM20A expansion module. If the number of IT cabinets is not an integer multiple of 4, according to the cable connection rules, leave the unconnected COM ports on the UIM20A expansion module idle.
- The smart U space manager has been connected to the ECC800-Pro through automatic discovery. To enable automatic device identification, choose **System Settings > Device Management > Device Addition > Auto Discover Device**.

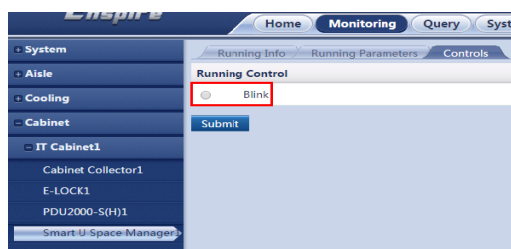
Procedure

Step 1 Log in to the ECC800-Pro WebUI as an administrator.

Step 2 View the position of the smart U space manager.

1. Choose **Monitoring > Cabinet > IT Cabinet n > Smart U Space Manager**.
2. Select **Running Control** and click **Blink**. In the actual environment, you will see that the smart U space manager blinks to ensure that the device location in the view is consistent with that in the smart module.

Figure 6-9 Viewing the position of the smart U space manager



----End

6.2.2.3 Registering Assets

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Asset Account**.
- You have the operation rights for **Model Library** and **Manufacturer**.
- You have the operation rights for **Data Center Planning**.
- On the **Data Center Planning** page, you have created a management domain for the assets to be registered.

Procedure

Step 1 Import a device template.

1. Choose **Operation > Asset Management > Asset Configuration** from the main menu, and click **Model Management > Model Library** on the left.
2. Click **Activate Template**. In the displayed **Import** dialog box, select the device template for the assets to be imported, and click **OK**.

Step 2 Register assets.

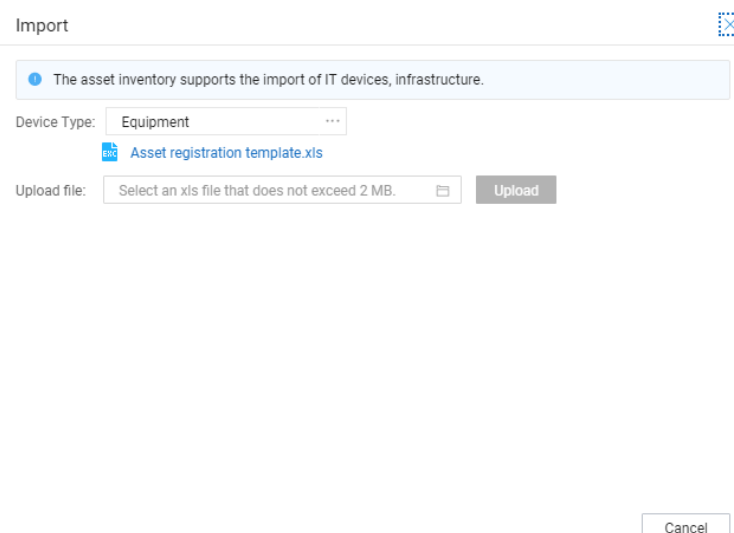
1. Choose **Operation > Asset Management > Asset Inventory** from the main menu, and click **Import**.

 NOTE

On the **Asset Inventory** page, you can click **New Device** and specify the asset information to register a single asset.

2. In the **Import** dialog box, click  [Asset registration template.xls](#) to download the template.

Figure 6-10 Batch import



3. Open the template and specify asset information.
 - If an asset is located in a cabinet, you must specify the name, manufacturer, model, asset location, and start U.
 - If an asset is located in a management domain that is not a cabinet, you must specify the name, manufacturer, model, and asset location. Asset Label, serial numbers, and asset numbers are optional.
4. In the **Import** dialog box, click , select the edited template, and click **Upload**.
5. When the message indicating that the uploading is successful is displayed, click **Close**.

Step 3 View the registered assets.

1. After assets are registered, you can view the assets on the **Asset Inventory** page.
2. Enter any information about registered assets and click **Search** to search for assets.

Figure 6-11 Viewing registered assets

----End

6.2.3 iCooling Energy Management

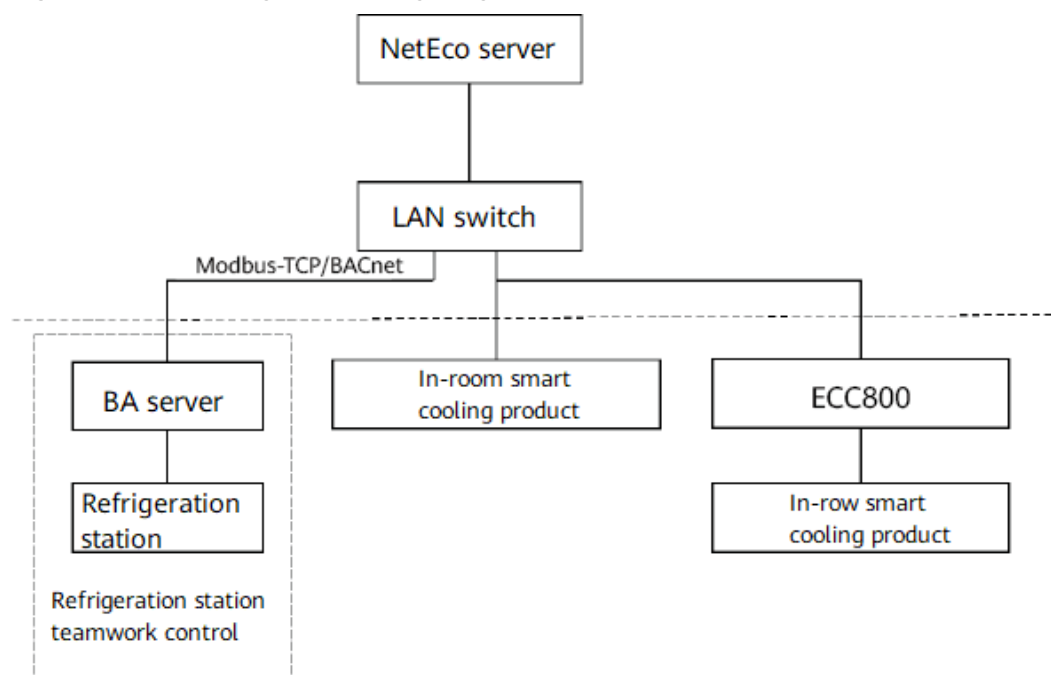
The instantaneous power usage effectiveness (PUE) and Coefficient of Performance (COP) of the cooling system are obtained in real time. The iCooling energy saving algorithm is introduced to reduce the energy consumption of the heating, ventilation, and air conditioning (HVAC) system for optimal energy efficiency of the HVAC system.

Prerequisites

- You have logged in to the NetEco client.
- You have created a management domain on the **Data Center Planning** page.
- You have added the **ChillerPlantControl** device to the management domain.
- The **Cooling Optimization for Water Cooled System** license has been imported to the NetEco.
- The communication between the NetEco and the **ChillerPlantControl** device connected to the LAN switch is normal.
- The NetEco communicates properly with the ECC800-Pro and the smart cooling product connected to the ECC800-Pro.
- Power management has been configured for the smart cooling product connected to the ECC800-Pro, and the IT cabinet power statistics are correct.
- The number of smart cooling products (number of started smart cooling products) with the valid maximum cooling capacity received by the ECC800-Pro is greater than or equal to the **Number of running smart cooling products in this group** in **Teamwork settings** of smart cooling products.

Networking Diagram

Figure 6-12 iCooling networking diagram



DM25H00065

6.2.3.1 Setting Cooling Management Parameters

The cooling capacity of the chilled water smart cooling products in the smart module can be managed by collecting the running parameters of the chilled water smart cooling products and using the smart module electricity management function.

Prerequisites

- The communication between the NetEco and the **ChillerPlantControl** device connected to the LAN switch is normal.
- The NetEco communicates properly with the ECC800-Pro and the smart cooling product connected to the ECC800-Pro.
- Power management has been configured for the smart cooling product connected to the ECC800-Pro, and the IT cabinet power statistics are correct.
- The number of smart cooling products (number of started smart cooling products) with the valid maximum cooling capacity received by the ECC800-Pro is greater than or equal to the **Number of running smart cooling products in this group** in **Teamwork settings** of smart cooling products.

----End

Context

After the smart cooling product is successfully connected to the ECC800-Pro, the **cooling capacity management function** is **enabled** by default.

Procedure

- Step 1** Log in to the ECC800-Pro WebUI as an administrator.
- Step 2** Choose **Monitoring > Cooling > Running Parameters** to access the **Temperature and Humidity Parameters** page. Set **Local yearly highest temperature** as required and click **Submit**.
- Step 3** Choose **Monitoring > Cooling > Running Parameters** to access the **Running Parameters** page. Set **Number of redundant smart cooling products** and **Local yearly highest temperature** as required and tap **Submit**.

Figure 6-13 Setting running parameters

iCooling Parameters			
Running Parameters			
☐ All	Signal Name	Signal Value	Remarks
☐	Number of redundant air conditioners	0 - +	(0~8)
☐	Local yearly highest temperature	35.0 - +	°C (-50.0~150.0)

Submit Restore

- Step 4** Choose **Monitoring > Cooling > Running Parameters**. In the **Cooling Capacity Management** area, set the parameters related to cooling capacity management for the water cooled smart cooling product, such as the target cooling load factor and recommended supply water temperature statistics cycle.

----End

6.2.3.2 Configuring iCooling Parameters

Context

- The following devices support the iCooling system: chiller, chilled water pump, smart cooling product, and cooling tower.
- Cooling pPUE = Cooling energy consumption/IT energy consumption
- The terminal smart cooling product configuration function works as follows: The system calculates the water temperatures of the smart cooling products in the data center where the refrigeration station is located and the water temperatures of the in-room smart cooling products. Then, it uses algorithms to calculate the optimal water temperature with the actual load considered, and delivers the optimal water temperature to each refrigeration station.

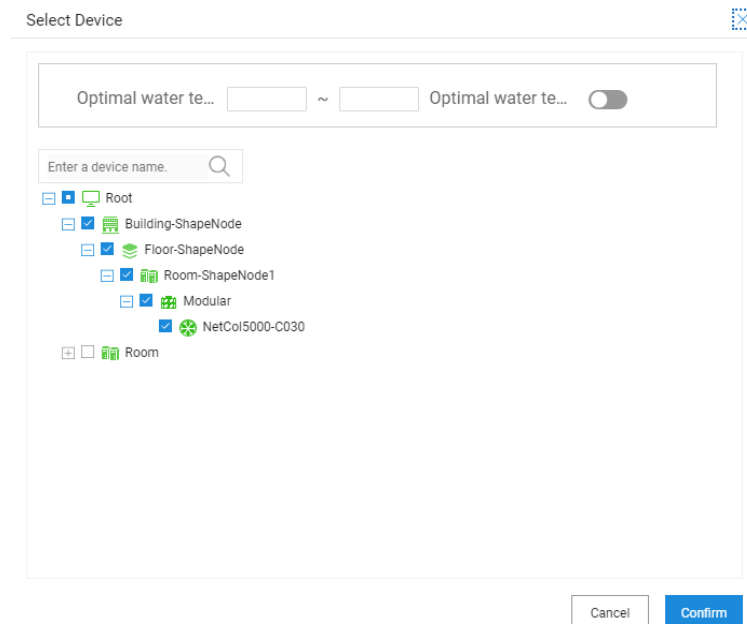
Procedure

- Step 1** Log in to the NetEco client.
- Step 2** Choose **Energy > Energy Efficiency Management > iCooling Energy** from the main menu and click **Monitor** to go to the **Monitor** tab page.
- Step 3** Click **HVAC System Configuration** to go to the page for configuring iCooling energy efficiency parameters.
- Step 4** Configure the terminal smart cooling product as follows: Click **Terminal Smart Cooling Product configuration**. In the displayed **Select Device** dialog box, select the smart cooling products to function as the data sources, and click **Confirm**.

 NOTE

You can enter a smart cooling product name in the search box for search.

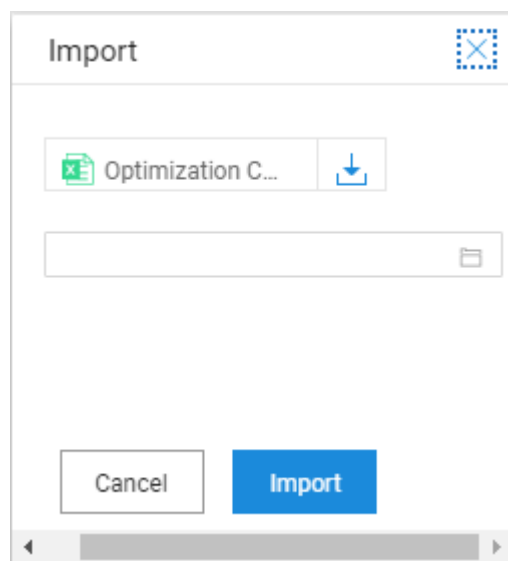
Figure 6-14 Searching for a smart cooling product



Step 5 Import configuration parameters. Click **Import** > **Configuration Parameters**. In

the displayed **Import** dialog box, click  to obtain the configuration parameter template. Fill in parameters in the template. Click , select the specified configuration parameter file, and click **Import**.

Figure 6-15 Importing configuration parameters



- Step 6** (Optional) Export configuration parameters. Click **Export > Configuration Parameters**, export the configuration parameter form, and modify configuration parameters.

Figure 6-16 Exporting configuration parameters



- Step 7** Import algorithm parameters. Click **Import > Algorithm Parameters**, and import the algorithm parameter form.

- Step 8** (Optional) Export algorithm parameters. Click **Export > Algorithm Parameters**, and export the algorithm parameter form.

- Step 9** Click  in the upper-left corner. On the **Monitor** tab page, click the iCooling energy saving mode switch  **OFF** to enable the iCooling function.

 NOTE

- **OFF** indicates that the iCooling energy saving mode is not enabled, and **ON** indicates that the mode is enabled.
- When the iCooling energy saving mode is enabled, you cannot configure the terminal smart cooling product, import configuration parameters, or import algorithm parameters.

----End

6.2.3.3 Viewing iCooling Energy Efficiency

Prerequisites

- You have logged in to the NetEco client.
- You have created a management domain on the **Data Center Planning** page.
- You have added the **ChillerPlantControl** device to the management domain.
- You have installed the iCooling energy efficiency management license and obtained the iCooling energy efficiency management permission.
- You have configured power and cooling capacity counters on the **PUE Configuration** page.

 NOTE

- Path: Choose **Energy > Energy Efficiency Management > Energy Configuration**, and choose **Electric Energy Configuration > PUE Electric Energy Configuration** on the left.
- For details, see "Configuring PUE Counters" in *iManager NetEco 6000 Product Documentation (V600R021C00)*.

Context

On the overview page, you can view the PUE, accumulated energy consumption, and running overview of the data center. After the iCooling function is enabled, the system displays the running information in energy saving mode.

Procedure

Step 1 Choose **Energy > Energy Efficiency Management > iCooling** from the main menu to go to the **iCooling Energy** page.

Step 2 Select a management domain in the upper-right corner of the page to view **Overall Running Status, PUE(Hours), Energy Saving and Total Consumed Energy**, and **Running Overview**.

NOTE

- **Overall Running Status** covers **PUE in Common Mode, PUE in Energy Saving Mode, Dry-bulb Temperature, Wet-bulb Temperature**, and **IT Load Rate**. In the upper right corner of the curve chart, you can click the color block before a parameter to hide or display the curve about this parameter.
- You can click **Hour, Day**, or **Month** to view the overall running status by day, month, or year respectively.
- You can click the **Custom** icon to customize the query time.

----End

6.2.4 (Optional) Viewing a Temperature Map on the NetEco

After obtaining the temperature map license, set the temperature map by following the instructions provided in this section.

Prerequisites

- A temperature sensor has been successfully connected.
- You have logged in to the NetEco client.
- You have created a management domain for the device to be added on the Data Center Planning page.

Procedure

Step 1 Choose **Monitor > Device Management > Data Center View** from the main menu, and click the management domain for which a temperature sensor has been deployed in the navigation tree on the left.

Step 2 Click  to view the temperature map.

Step 3 Click . In the displayed **Room temperature setting** dialog box, set the room temperature.

NOTE

If a temperature sensor has been added to a management domain but the temperature is not set, the average value of the temperatures collected by the sensor is displayed.

----End

6.3 Scenarios for Connecting the Server

6.3.1 Setting SMS

When short messages need to be sent, you need to set parameters for notifications sent in SMS messages and commission the settings to ensure that SMS messages can be properly sent.

Prerequisites

- An SMS modem has been installed and commissioned.
- You have obtained the interconnection parameters of the SMS modem from the user, such as mobile number for receiving notifications.
- You have the operation rights for **SMS Settings**.

Context

- To send notifications to related personnel, you need to enter their personal information, such as mobile numbers and email addresses. Therefore, you are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the personal data of users is fully protected.
- For security purposes, personal information, such as mobile number and email address, is anonymized on the GUI and encrypted during transmission.

Procedure

- Step 1** Log in to the NetEco client.
- Step 2** Choose **System > System Settings > Notifications** from the main menu.
- Step 3** In the navigation tree on the left, choose **SMS Modem Settings** and set interworking parameters of the SMS modem.

Table 6-5 SMS modem parameters

Parameter	Description	Example
Network system of SMS modem	The options are GSM, CDMA, LTE and FDDLTE. The default value is CDMA. • The following GSM SMS modems are supported: E-TEK GSM modem TD-8011, E-TEK GSM modem TD-8013, and wavecom WMOD2B GSM/GPRS modem. • The following CDMA SMS modems are supported: E-TEK CDMA modem TD-8022R and E-TEK CDMA modem TD-8022. • The following LTE and FDDLTE SMS modems are supported: E-TEK TD-8412 modem.	CDMA
Serial port for connecting SMS modem	Serial port connections are secure hardware-level connections. The options are COM1 and COM2 . By default, this parameter is left blank.	COM1
SMS modem bound rate	Baud rate of the SMS modem serial port. The default value is 9600 .	115200
Mobile number for receiving notification	A country code must be added before a mobile number. For example, the country code of China is 86, and the format of the mobile number is as follows: 86+mobile number . The recipient mobile number is used only for testing. When this parameter is left blank, the test button is unavailable.	8613111111111

Parameter	Description	Example
Allow long SMS messages	It is recommended that long SMS messages be supported.	Yes
Enabled	If you select No , the settings are unavailable and short messages cannot be sent.	Yes

Step 4 Click **Test** to check whether the system is properly interconnected with the SMS modem.

- If "Test succeeded." is displayed, they are properly connected. The received SMS messages are in English.
- If no, "Connectivity failed." is displayed. Check that all parameter settings are correct.

Step 5 Click **Apply**. In the **Warning** dialog box, click **OK**.

 NOTE

If you click only **Test**, the interconnection status between the system and the mail server can be tested and the entered parameter values cannot be stored in the database. Only after you click **Apply**, all entered parameter values can be stored in the database.

----End

6.4 Scenarios for Connecting the LAN Switch

6.4.1 Adding an iBOX Collector

6.4.1.1 Setting Parameters on the iBOX WebUI

The parallel iBOX communication is used to synchronize the analog parameters and configuration parameters of each iBOX system. It can also be used to coordinate the measurement of internal resistance so that only one iBAT is measuring the internal resistance at one time.

Prerequisites

- Operating system: Support Windows XP or later
- Browser: Internet Explorer 9 or later, FireFox 43 or later, and Chrome 41 or later
- The IP addresses, subnet masks, and gateways for the PC and iBOX are in the same network segment.

 NOTE

The default settings of the IP address, subnet mask, and gateway are as follows:

- IP address: 192.168.0.10
- Subnet mask: 255.255.255.0
- Gateway: 192.168.0.1

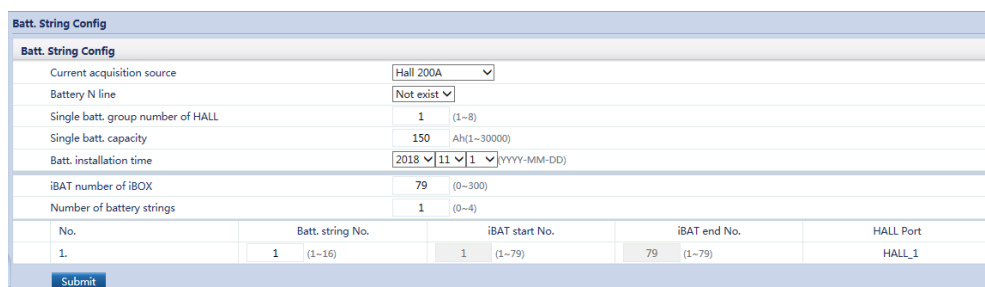
Procedure

1. Connect a straight-through cable from the PC network port to the Ethernet port on the switch.
2. Open Internet Explorer and choose **Tools > Internet Options**.
3. Select the **Advanced** tab, check that **Use TLS 1.1** and **Use TLS 1.2** are selected, and then click **OK**.
4. Enter **https://iBOX IP address** in the address box of a browser. The login page is displayed. After you log in successfully, the home page is displayed.

 NOTE

- In this document, the iBOX WebUI snapshots are obtained from iBOX V296B019. The WebUI snapshots may vary with the iBOX version.
 - The preset iBOX IP address is 192.168.0.10. You can set the iBOX IP address on the WebUI.
 - Enter the user name and password. The preset user name is **admin**, and the preset password is **Changeme**. To protect the access security, change the password after the first login.
 - If you enter wrong passwords for five consecutive times, the system will be locked for one hour. Then, you can operate normally.
 - If you forget the IP address, hold down the Default button on the iBOX for more than 10 seconds. Then the ALM indicator blinks at short intervals, and the iBOX IP address is restored to the factory default value (192.168.0.10).
 - If the user certificate is invalid, the browser prompts **There is a problem with this website's security certificate**. Click **Continue to this website (not recommended)** to go to the normal login page. The operation does not affect WebUI functions but has potential risks. Therefore you are advised to update the security certificate as soon as possible.
5. On the iBOX WebUI, choose **System Settings > Batt. String Config**, and set **Batt. String Config**.

Figure 6-17 Batt. String Config



No.	Batt. string No.	iBAT start No.	iBAT end No.	HALL Port
1	1 (1~16)	1 (1~79)	79 (1~79)	HALL_1

Batt. String Config	Description
Current acquisition source	The actual specifications of the Hall effect sensor prevail.
Battery N line	Set whether there is a battery N wire according to the actual situation.
Single batt. group number of HALL	Indicates the number of Hall effect sensors connected to a single battery string.
Single batt. capacity	Specifies the capacity of each battery that is connected in the battery string in series.
Batt. installation time	Time when the battery is installed for the first time. Does not need to be reset when part of batteries are replaced.
iBAT number of iBOX	Indicates the total number of iBATs managed by the iBOX.
Number of battery strings	Indicates the total number of battery strings managed by the iBOX.
Batt. string No.	Sets the battery string numbers of the iBOXs connected in parallel to unique ones when multiple iBOXs are connected in parallel.

- On the iBOX WebUI, choose **System Settings > Running Parameter**, and set **Running Parameter**.

Figure 6-18 Running Parameter

Running Parameter	Description
Parallel Communication Configuration	There is no need to set this parameter for a single iBOX. If multiple iBOXs are connected in parallel, set iBOX parallel communication switch to Yes , set Number of iBOX configured under each UPS , and set the IP address for each iBOX.

Running Parameter	Description
Modbus Config	Set ModbusTCP encryption and ModbusTCP authentication parameters, which should be consistent with the setting of Connection Mode on the NetEco.
Alarm Threshold Settings	Set the battery internal resistance, charge overcurrent, charge overvoltage, and bias alarm thresholds.
iBAT Parameters Config	Set the iBAT intelligent hibernation and battery undervoltage protection threshold.
Basic Information	If a BCB is configured, set BCB configuration to Done and Batt. abnormal BCB trip to Enable .
Hall Reverse Config	If the Hall effect sensor is reversely installed, you can set reverse connection to correct it.
IScan Register Config	Enable or disable iScan registration.
Parallel Comm TLS Config	Enable or disable the TLSv1.1 protocol for parallel communication

- On the **System Settings** page, set **Alarm Parameters**, **Time**, **IP Address**, **Certificate Management**, **Battery Curve**, **NetEco**, and **Parallel Net Join Configuration Information**.

Figure 6-19 Alarm Parameters

Alarm Parameters					
Select a Device type: iBOX System Confirm					
☐ All	No.	Alarm Name	Alarm Enable	Severity	Setting Result
☐	1	iBAT comm. failure	Enable	Minor	
☐	2	Inconsistent iBAT versions	Disable	Minor	
☐	3	Web security cert. about to expire	Enable	Warning	
☐	4	Web security cert. not take effect	Enable	Warning	
☐	5	Web security cert. has expired	Enable	Warning	
☐	6	DI Alarm	Enable	Warning	
☐	7	iBOX1 comm. Failure	Enable	Minor	

Figure 6-20 Time

Time

Time Zone

Local Time Zone: (UTC +08:00)Beijing Submit

Time Synchronization

☐ NTP Server Synchronization

Date Format: YYYY-MM-DD

Local Date: 2018-12-13

Local Time: 15:30:12 (HH:MM:SS) Obtain Local Time

Submit

Figure 6-21 IP Address

IP Address

IP Address	192, 168, 0, 10
Subnet Mask	255, 255, 255, 0
Default Gateway	192, 168, 0, 1

Submit

Figure 6-22 Certificate Management

Certificate Management

Web Security Certificate

Select certificate format: crt format

Please select a web security certificate: **browse...** **Upload**

Please select upload web security certificate key: **browse...** **Upload**

☐ Enable key cryptography

Submit

Modbus TCP Certificate Management

Please select upload Modbus TCP certificate: **browse...** **Upload**

☐ Enable key cryptography

Submit

Modbus TCP CA Certificate Management

Please select upload Modbus TCP CA certificate: **browse...** **Upload**

Submit

Parallel Communication Certificate Management

Select client or server: Client

Please select upload Parallel Communication certificate: **browse...** **Upload**

Please select upload Parallel Communication certificate key: **browse...** **Upload**

☐ Enable key cryptography

Submit

Figure 6-23 Battery Curve

Battery Curve

BatteryCurve File Management

Please select upload BatteryCurveFile: **View...** Please upload file less than 1MB **Upload**

Please select the BatteryCurveFile to be deleted: SHOTO@6-GFM-100 **Delete**

Please set the brand and format for file filtering

Select	Batt. string No.	Battery Brand	Format	Battery curve	Filter
☐	Batt. string1			SHOTO@GFM-500	Filter
☐	Batt. string2			SHOTO@6-GFM-xxx	Filter
☐	Batt. string3			SHOTO@6-GFM-xxx	Filter
☐	Batt. string4			SHOTO@6-GFM-xxx	Filter
☐	Batt. string5			SHOTO@6-GFM-xxx	Filter
☐	Batt. string6			SHOTO@6-GFM-xxx	Filter
☐	Batt. string7			SHOTO@6-GFM-xxx	Filter
☐	Batt. string8			SHOTO@6-GFM-xxx	Filter
☐	Batt. string9			SHOTO@6-GFM-xxx	Filter
☐	Batt. string10			SHOTO@6-GFM-xxx	Filter
☐	Batt. string11			SHOTO@6-GFM-xxx	Filter
☐	Batt. string12			SHOTO@6-GFM-xxx	Filter
☐	Batt. string13			SHOTO@6-GFM-xxx	Filter
☐	Batt. string14			SHOTO@6-GFM-xxx	Filter
☐	Batt. string15			SHOTO@6-GFM-xxx	Filter
☐	Batt. string16			SHOTO@6-GFM-xxx	Filter

Submit

Figure 6-24 NetEco

Figure 6-25 Parallel Net Join Config

System Settings	Description
Alarm Parameters	Select a device type, and check the alarm name, alarm enabling, severity, and setting result.
Time	Set the local time zone, date, and time.
IP Address	Set the IP address, subnet mask, and default gateway for the iBOX based on the IP address assigned by the administrator.
Certificate Management	Set the web security certificate, Modbus TCP certificate management, Modbus TCP CA certificate management, parallel communication certificate management, and parallel communication CA certificate management parameters.
Battery Curve	Set the battery curve based on the battery brand and model.
NetEco	Select the NMS type and restore the default Modbus TCP authentication password.
Parallel Net Join Configuration Information	Set this parameter when you connect iBOXs in parallel.

6.4.1.2 Creating an iBOX Collector on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.

Context

You can create an iBOX collector by manually creating the iBOX on the NetEco or by adding a UPS for synchronizing the iBOX to the NetEco.

The following operations describe how to manually create an iBOX.

- UPS_Huawei_UPS5000E_V1R3C00C01_MODBUSTCP
- UPS_Huawei_UPS2000G_V1R1C38_MODBUSTCP
- UPS_Huawei_UPS5000E_V1R1C39_MODBUSTCP
- UPS_Huawei_UPS5000_MODBUSTCP
- UPS_Huawei_UPS5000E_V3R1C00_MODBUSTCP
- UPS_Huawei_UPS5000S-V3R2C30_MODBUSTCP
- UPS_Huawei_UPS5000S-1.2MW_V3R2C10_MODBUSTCP

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **Battery Detector**.

NOTE

If the UPS is created in "Context", after **UPS** is added, the BMU will be automatically synchronized.

Step 5 Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-6 Modbus-TCP device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the device IP address.
Port	Set this parameter to the port number of the device. NOTE The port number is 502 by default. You can modify the port number based on requirements.

Parameter	Description
Device Address	Fixed value: 2. NOTE This parameter does not need to be configured.
Timeout period	Timeout duration for a connection test. The default value is 3s.
Connection Mode	Connection mode of a device. You can set this parameter to Non-SSL Connection or SSL Connection. If you modify the connection mode on the NetEco, you must modify the connection mode on the device WebUI accordingly. NOTE • Connection Mode for the NetEco and device must be the same. • By default, Connection Mode is set to SSL Connection for the NetEco and device. • A non-SSL connection has security risks. You are advised to select the secure SSL connection. NOTE Battery detectors accessed through the UPS do not support device software management.
Authentication Password	Re-authentication password for the NetEco and device. 1. Click Modify. NOTE After the device is saved, the Modify button is displayed. 2. In the displayed dialog box, enter the New Password and Confirm Password. NOTE – The default re-authentication password for the NetEco and device is Modifyme_123. – The device password should be consistent with the NetEco password. – If the password does not meet requirements, modify it on the device. 3. Select a value for Send To Device. NOTE If you select YES, the re-authentication password for the NetEco and device is changed at the same time. If you select NO, only the re-authentication password of NetEco is changed on the server. 4. Click OK.

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.4.1.3 iBOX and iBAT Networking

Prerequisites

Before networking, ensure that all the iBOXs and iBATs have no network parameters, that is, the RF_Z indicator on the iBOX is steady green and the RUN/ALM indicator on the iBAT is steady red.

NOTICE

- If the RF_Z indicator on the iBOX is not steady green, hold down the networking switch on the iBOX for 10–20 seconds to clear the original network.
 - If the RUN/ALM indicator on the iBAT is not steady red, hold down the networking switch on the iBAT for at least 5 seconds to clear the original network.
 - Do not operate the networking switch during networking. Otherwise, the networking fails.
-

Context

To prevent the iBAT in a different group from connecting to another iBOX, ensure that only one iBOX is under networking at a time. That is, only the RF_Z indicator of this iBOX is blinking at super short intervals.

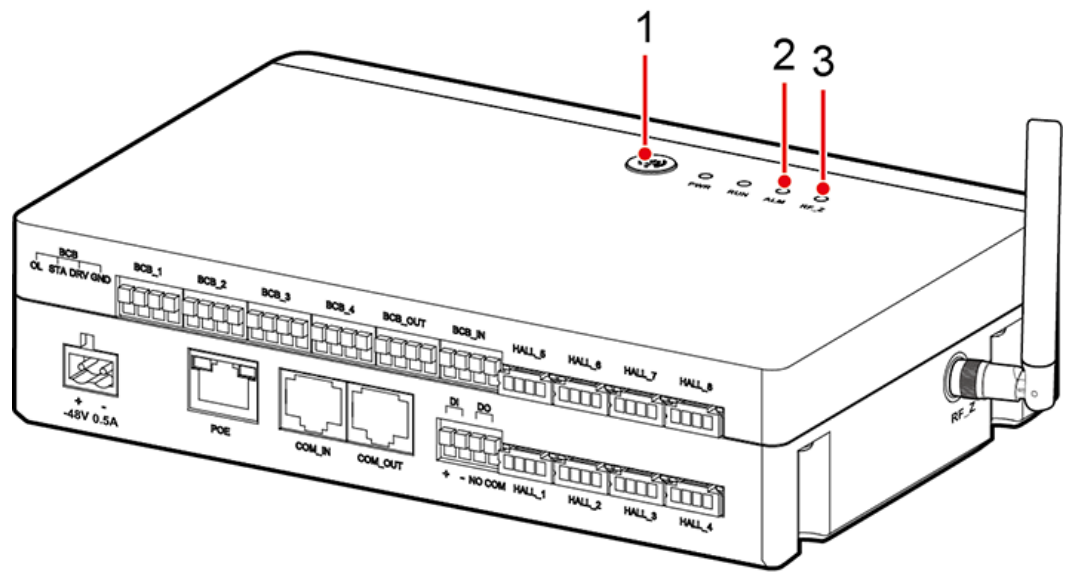
Procedure

- Step 1** Hold down the networking switch on the iBOX for 2 seconds. The ALM indicator blinks red once, and the RF_Z indicator turns from steady green to blinking green at super short intervals, which indicates that the iBOX is being networked.

NOTE

- Blinking at long intervals: The indicator is on for 1s and then off for 1s alternately.
- Blinking at super short intervals: The indicator is on for 0.05s and then off for 0.05s alternately.

Figure 6-26 iBOX



UB07000029

- (1) Networking switch (2) ALM indicator (3) RF_Z indicator

Step 2 Hold down the iBAT networking switch for 2 seconds. When the RUN/ALM indicator turns from steady red to blinking green at short intervals, and finally to blinking green at long intervals, the iBAT connects to the iBOX network.

NOTE

- It is recommended that iBATs be networked from the positive battery string terminal according to the battery cable connection sequence.
- The sequence of connecting the iBAT to the iBOX determines the battery number.

Step 3 Perform networking operations on the next iBAT only after networking for the previous iBAT is successful. Repeat [Step 2](#) to add other iBATs to the iBOX network.

Step 4 Hold down the networking switch on the iBOX for 2 seconds. When the RF_Z indicator on the iBOX turns from blinking green at super short intervals to blinking green at long intervals, the networking is complete.

NOTE

After the networking is complete, if the ALM indicator on the iBOX is steady on, the number of devices online is smaller than the value of **iBAT number of iBOX**. Check that **iBAT number of iBOX** is set to a correct value and that the iBATs are successfully networked (The RUN/ALM indicator is blinking green at long intervals).

Step 5 (Optional) If multiple iBOXs are cascaded, repeat [Step 1](#) to [Step 4](#) to perform networking for other iBOXs and iBATs.

----End

6.4.2 Adding a Video Management System

NOTE

- Because cameras and the VCN do not support northbound and southbound isolation, the VCN service IP address must be set to a northbound IP address.
- The camera IP address and the VCN service IP address must be in the same network segment.
- For details about the northbound IP address, see the section about the overview of southbound and northbound network isolation in *iMaster NetEco 6000 Product Documentation*.

6.4.2.1 Obtaining Video Management System Documents

Before commissioning a camera, prepare the following documents in addition to this document.

Table 6-7 Documentation for commissioning

Component	Document
C3220/M2121	Huawei C Series SDC 8.0.1 Product Documentation
VCN500/VCN510/ VCN520/VCN540	VCN500: VCN500 Product Documentation VCN510/VCN520/VCN540: VCN510&VCN520&VCN540 Product Documentation
IVS1800	IVS1800 8.1.0 Product Documentation

6.4.2.2 Commissioning a C3220/M2121 Camera

Prerequisites

If multiple cameras are accessed, retain the connection of one camera and disconnect connections from other cameras. After commissioning the connected camera, commission other cameras in the same way.

Procedure

Step 1 Log in to the camera WebUI.

1. Configure the PC IP address and the camera IP address in the same network segment. Enter the camera IP address (192.168.0.120 by default) in the address bar of the Internet Explorer and press **Enter**.

 NOTE

The following lists the requirements for the operating system and browser of the camera WebUI:

- Supports Windows 7: Internet Explorer 10/11, Chrome 38+, FireFox 35-51
- Supports Windows 8: Internet Explorer 10/11, Chrome 38+, FireFox 35-51
- Supports Windows 10: Internet Explorer 11, Chrome 38+, FireFox 35-51
- The Internet Explorer tab plugin needs to be installed for Google Chrome 45 and later versions.
- Only 32-bit browsers are supported.

2. Set the password as prompted upon the first login. Then use the new password to log in.

 NOTE

- To prevent security risks, the system prompts you to set the password of the **admin** user when you log in to the system for the first time.
- If you enter incorrect passwords for five consecutive times, the account will be locked for 5 minutes by default.
- To prevent security risks, periodically log in to the system as the **admin** user, click the drop-down list in the upper right corner, and click **Change Password** to change the administrator password.
- You need to set Internet Explorer before accessing the camera WebUI for the first time.

Table 6-8 Internet Explorer settings

Settings	Procedure
Disable the proxy server.	1. Choose Tools > Internet Options. The Internet Options dialog box is displayed. 2. Click the Connections tab. 3. Click LAN Settings. 4. Deselect Use a proxy for your LAN. 5. Click OK.

Settings	Procedure
Enable the ActiveX controls and plug-ins or set them to the prompt mode.	1. Choose Tools > Internet Options. The Internet Options dialog box is displayed. 2. Click the Security tab. 3. Select Internet. 4. Click Custom level. The Security Settings-Internet Zone dialog box is displayed. 5. Set Automatic prompting for ActiveX controls to Enable, and set Download unsigned ActiveX controls and Initialize and script ActiveX controls not marked as safe for scripting to Prompt. 6. Click OK.
Enable TLS 1.1 or TLS 1.2.	NOTE You must enable TLS 1.1 or TLS 1.2 when the HTTPS protocol is used to access the camera. Otherwise, the camera WebUI cannot be opened. 1. Choose Tools > Internet Options. The Internet Options dialog box is displayed. 2. Click the Advanced tab. 3. Select Use TLS 1.1 or Use TLS 1.2. 4. Click OK.
Set Use Pop-up Blocker to Disable .	1. Choose Tools > Internet Options. The Internet Options dialog box is displayed. 2. Click the Security tab. 3. Select Internet. 4. Click Custom level. The Security Settings-Internet Zone dialog box is displayed. 5. Set Use Pop-up Blocker to Disable. 6. Click OK.

- Step 2** Commission cameras and set parameters for them. For details, see the delivered documents.
1. Preview the site situation in real time and check the camera coverage through videos. Adjust the lens if necessary.
 2. On the **View** tab page, click the **Network/Time** tab to access the **Network/Time** tab page.

Figure 6-27 Setting the IP address

IPv4 address assignment: Use the following IP address▼

IPv4 address: [. . .] Q

IPv4 subnet mask: [. . .]

IPv4 gateway: [. . .]

Primary DNS: [. . .]

Secondary DNS: [. . .]

Save

Table 6-9 IP address parameters

Parameter	Description
IPv4 address assignment	Method for obtaining the IP address. The options are Obtain IP address automatically and Use the following IP address . The default value is Obtain IP address automatically .
IPv4 address	Camera IP address. This parameter is available only when IPv4 address assignment is set to Use the following IP address . Enter the planned IP address, for example, 192.168.1.161 . IP addresses starting with 127 are invalid. You must enter an IP address starting with a value that ranges from 1 to 223.
IPv4 gateway	Gateway IP address of the network where the camera is located. The default value is 192.168.0.1 .
IPv4 subnet mask	Subnet mask of the network where the camera is located. The default value is 255.255.255.0 .
Primary DNS	Primary DNS IP address. The default value is 0.0.0.0 .
Secondary DNS	Secondary DNS IP address. The default value is 0.0.0.0 .

3. On the **View** tab page, click the **General** tab to access the **General** tab page. Select **Video** and set the parameters, as shown in the following figures.

Figure 6-28 Setting primary stream parameters

The screenshot displays the 'Primary stream' configuration tab, with 'Secondary stream 1' also visible. The 'Intelligent encoding' checkbox is unchecked. Below it, a note states: '(Note: ROI and stream smoothing cannot take effect after intelligent encoding is enabled.)'. The configuration parameters are as follows:

Parameter	Value
Intelligent encoding	☐
Encoding protocol	H.265
Encoding complexity	Main profile
Resolution	1280 * 720
Bit rate type	Variable bit rate
Max. bit rate (kbit/s)	2048
Frame rate	25
Image quality	Supreme
I-frame interval	50
Layered encoding	☐

Figure 6-29 Setting secondary stream 1 parameters

Primary stream
Secondary stream 1

Intelligent encoding
☐

1

5

3

(Note: ROI and stream smoothing cannot take effect after intelligent encoding is enabled.)

Encoding protocol

H.265

Encoding complexity

Main profile

Resolution

720 * 576

Bit rate type

Variable bit rate

Max. bit rate (kbit/s)

256

4096

1024

Frame rate

25

Image quality

Supreme

I-frame interval

1

500

50

Layered encoding
☐

Enable area cropping
☐

(Note: This function supports zooming through ePTZ operation.)

(Note: It is recommended that the area cropping function be enabled for the primary stream.)

Table 6-10 Video stream parameters

Parameter	Description
Primary stream/ Secondary stream	Set the stream type based on the site requirements. Primary stream: The primary streams feature high bit rate, definition, and bandwidth usage. They are applicable to local storage. Secondary stream: The secondary streams provide smooth video, occupy small bandwidth, and are applicable to data transmission over low-bandwidth networks. NOTE SD card recording supports only primary streams.
Intelligent encoding	After intelligent encoding is enabled, a camera can automatically adapt to scenarios to reduce the bit rate and save the storage space. A higher intelligent encoding level indicates more significant reduction of the bit rate, which however may lead to image quality deterioration.

Parameter	Description
Slice	This parameter is available only when you set Encoding protocol to H.264. Multi-slice encoding indicates that video streams are divided into multiple segments. Each segment forms a slice. The encoding process of each slice is independent of each other. Therefore, the camera can encode and decode multiple slices in parallel, improving encoding and decoding performance. This parameter is selected by default.
Encoding protocol	Set the coding protocol based on the site requirements. The options are as follows: – H.264: The H.264 protocol requires relatively small bandwidth to ensure video quality. – MJPEG: The MJPEG protocol decodes and displays each frame independently without referring to the previous and next frames. This protocol has a small compression ratio and requires large bandwidth to ensure video quality. This protocol is suitable for video editing. – H.265: The H.265 protocol is bandwidth-conserving compared with the H.264 protocol.
Encoding complexity	The options of H.264 profiles include Base profile, Main profile, and High profile. Among these profiles, the baseline profile has the lowest encoding compression performance and lowest requirements on hardware decoding performance, while the high profile has the highest.
Resolution	A higher resolution indicates clearer images and higher bandwidth consumption.
Bit rate type	This parameter is available only when you set Encoding protocol to H.264 or H.265. The bit rate is measured by data bits transmitted in a unit of time. – Variable bit rate: The bit rate varies depending on the image complexity to ensure the clarity of images with great dynamic changes. The bit rate is low if the image is simple or static. The variable bit rate is recommended. – Constant bit rate: The constant bit rate remains the same. The upper limit of the instantaneous bit rate is set to 110%. If the bit rate is incorrectly configured for images with great dynamic changes, the images will be unclear.

Parameter	Description
Max. bit rate	This parameter is available only when you set Bit rate type to Variable bit rate . The bit rate range depends on the selected resolution.
Bit rate value	Average bit rate when Bit rate type is set to Constant bit rate . The bit rate range depends on the selected resolution.
Bit rate control mode	This parameter is available only when you set Bit rate type to Constant bit rate . The options are as follows: – Frame rate priority: Ensure the smoothness of the video image. – Image quality priority: Ensure the quality of the video image.
Frame rate	The frame rate is measured by the number of frames displayed in a second. A higher frame rate indicates clearer and smoother images and higher bandwidth consumption.
Image quality	This parameter is available only when you set Encoding protocol to H.264 or H.265 and Bit rate type to Variable bit rate . Better image quality requires higher bandwidth. Therefore, select proper image quality based on the site requirements.
I-frame interval	This parameter is available only when you set Encoding protocol to H.264 or H.265 . An I frame is an intra-coded frame that represents a fixed image independent of other picture types. Each group of pictures (GOP) begins with this type of frame. A smaller I-frame interval indicates better video quality and higher bandwidth consumption.
Layered encoding	This parameter is available only when you set Encoding protocol to H.264 or H.265 . To enable layered encoding, select Layered encoding .
JPEG quality	This parameter is available only when you set Encoding protocol to MJPEG . A larger value indicates higher image quality.

----End

Follow-up Procedure

Commission other cameras by referring to this section.

6.4.2.3 Commissioning the VCN

6.4.2.3.1 Initializing VCN510 Disks

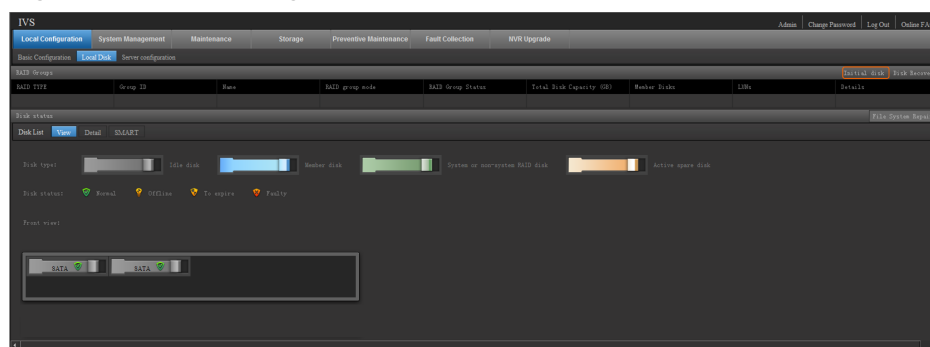
Context

When the VCN510 is delivered to the site, recording data can be stored only after you install and initialize the disks.

Procedure

- Step 1** Log in to the OMU portal of the VCN.
- Step 2** Choose **Local Configuration > Local Disk**.
- Step 3** In the upper-right corner of the **RAID Groups** area, click **Initial disk**.

Figure 6-30 Initializing disks



- Step 4** Choose whether to create a RAID group. To set disks as a RAID group, select **RAID1**. To set disks to work independently, select **NON-RAID**.

NOTE

The VCN510 supports only **RAID1** or **NON-RAID**. If only one disk is configured, the VCN510 supports only **NON-RAID**. This section assumes that two disks are configured for the VCN510.

Table 6-11 Disk modes

RAID Mode	Description
RAID1	Two disks are required in RAID 1 mode. If RAID 1 is used, disks back up each other. After recording data is stored in a disk, the data will be simultaneously backed up to another disk, ensuring high data storage reliability. However, the disk usage of RAID 1 is lower than that of disks that work independently.
NON-RAID	If disks work independently, recording data is stored into two disks in sequence, ensuring high disk usage. However, the data storage reliability of disks that work independently is lower than that of RAID 1.

Step 5 Click **Start**. A risk warning is displayed.

Step 6 Click **OK**. The system starts to initialize the disks.

NOTE

The server will be restarted during the initialization of disks. The process takes about 5 to 10 minutes.

----End

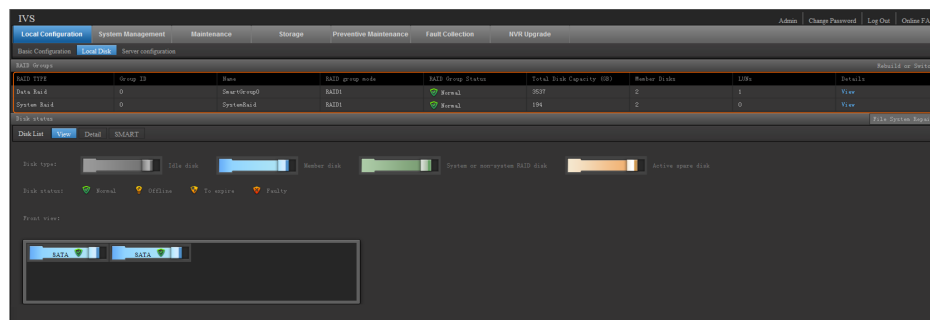
Verification

Step 1 Choose **Local Configuration > Local Disk**.

Step 2 View the RAID group status in the **RAID Groups** area.

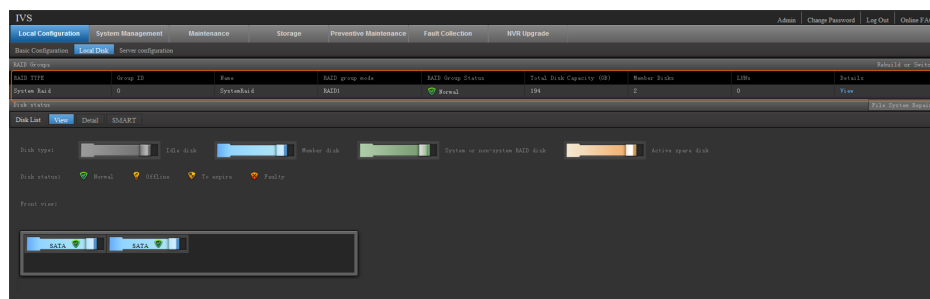
If **RAID1** is selected for the disks, RAID 1 is created for both the system partition (used to store system data) and data partition (used to store recordings).

Figure 6-31 RAID group status of RAID 1



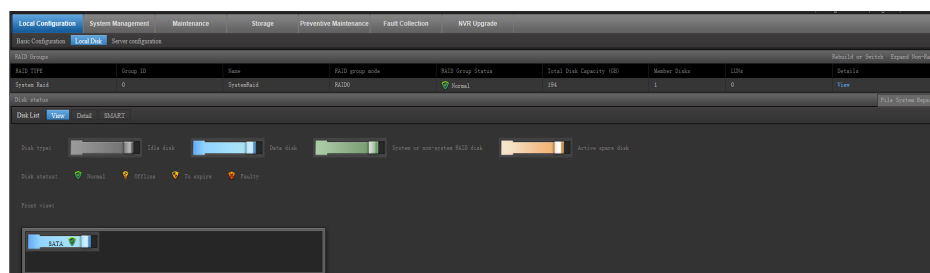
When two disks are configured, if **NON-RAID** is selected for the disks, RAID 1 is created for the system partition.

Figure 6-32 RAID group status of disks that work independently (two disks)



If only one disk is configured, RAID 0 is created for the system partition after disks are initialized.

Figure 6-33 RAID group status of disks that work independently (one disk)



NOTE

- After a RAID 1 is created for the system partition, the system partition's RAID group is in data restoration state. At this time, one disk is synchronizing data in the system partition to the system partition of another disk. The synchronization process takes about 20 hours, which does not impact services. During this process, do not remove and insert disks.
- If the OMU portal stays at the **Local Disk** tab page, even if users do not perform any operation for a long period of time, the OMU portal will not automatically return to the login page. For service security reasons, if users do not perform any operation for a long period of time, the OMU portal will return to the login page or does not stay at the **Local Disk** tab page.

----End

6.4.2.3.2 Initializing VCN520 or VCN540 Disks

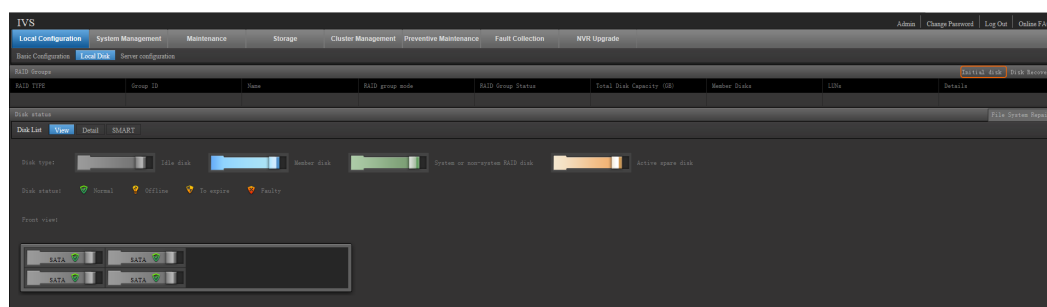
Context

When the VCN520 or VCN540 is delivered to the site, recording data can be stored only after you install and initialize the disks. The function and configuration procedure of the VCN520 are the same as those of the VCN540. This section describes how to initialize VCN540 disks.

Procedure

- Step 1** Log in to the OMU portal of the VCN.
- Step 2** Choose **Local Configuration > Local Disk**.
- Step 3** In the upper-right corner of the **RAID Groups** area, click **Initial disk**.

Figure 6-34 Initializing disks



- Step 4** Choose whether to create a RAID group. To set disks as a RAID group, select **RAID5**. To set disks to work independently, select **NON-RAID**.

Table 6-12 Disk modes

Disk Mode	Description
RAID5	In RAID 5 mode, all disks form a RAID 5 group. At least three disks need to be configured for the VCN. The data storage reliability is high, but the disk space usage is lower than that in non-RAID mode. RAID 5 has the following two configuration modes: • Recommended configuration: More than three disks are required. One of the disks is used as a hot spare disk. In normal cases, the hot spare disk does not store data. When a disk in the RAID group is faulty, the hot spare disk replaces the faulty hard disk to join the RAID group. Therefore, the recommended configuration mode has lower disk space usage but higher data storage reliability than the economical configuration mode. • Economical configuration: Three or more disks are required, and no hot spare disk is configured. The economical configuration mode has higher disk space usage but lower data storage reliability than the recommended configuration mode.
NON-RAID	If disks work independently, recording data is stored into two disks in sequence, ensuring high disk usage. However, the data storage reliability of disks that work independently is lower than that of RAID 5.

- Step 5** (Perform this step only when the RAID mode is set to **RAID5**.) Select **RAID configuration**. This step uses **Recommended configuration** as an example.

- Step 6** Click **Start**. A risk warning is displayed.

- Step 7** Click **OK**. The system starts to initialize the disks.

 NOTE

The server will be restarted during the initialization of disks. The process takes about 5 to 10 minutes.

----End

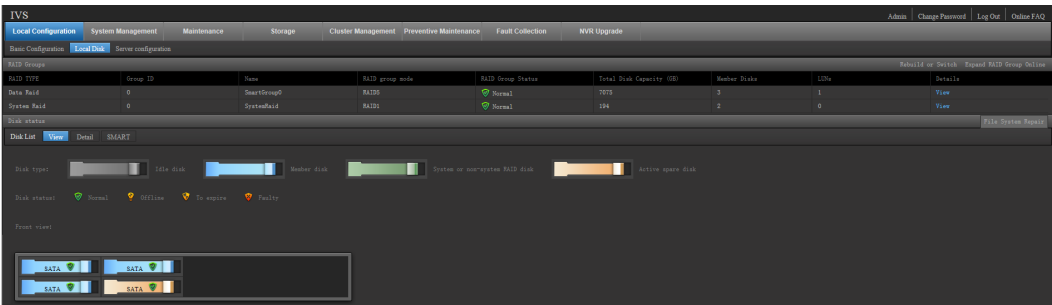
Verification

- Step 1** Choose **Local Configuration > Local Disk**.

- Step 2** View the RAID group status in the **RAID Groups** area.

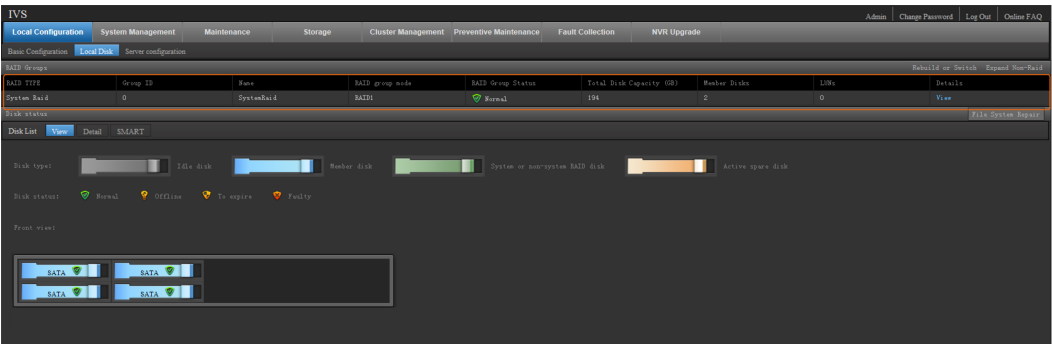
If you select the RAID 5 mode, RAID 1 is created for the system partition (for storing system data) and RAID 5 is created for the data partition (for storing recordings). The disk in yellow in the following figure is a hot spare disk.

Figure 6-35 RAID group status of RAID 5



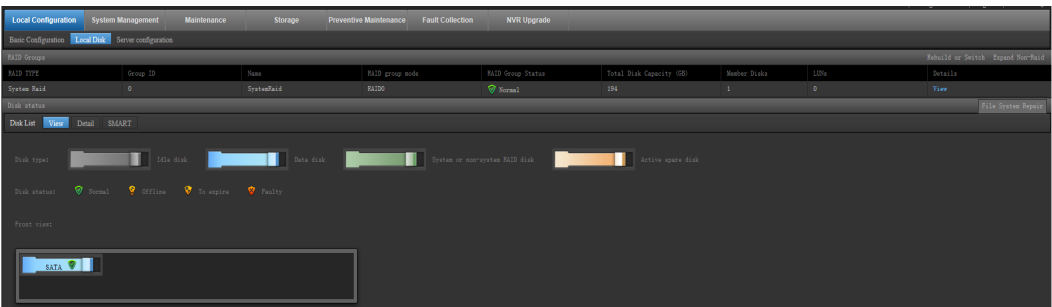
When multiple disks are configured, if **NON-RAID** is selected for the disks, RAID 1 is created for the system partition.

Figure 6-36 RAID group status of disks that work independently (multiple disks)



If only one disk is configured, RAID 0 is created for the system partition after disks are initialized.

Figure 6-37 RAID group status of disks that work independently (one disk)



 NOTE

- After a RAID 1 is created for the system partition, the system partition's RAID group is in data restoration state. At this time, one disk is synchronizing data in the system partition to the system partition of another disk. The synchronization process takes about 20 hours, which does not impact services. During this process, do not remove and insert disks.
- If the OMU portal stays at the **Local Disk** tab page, even if users do not perform any operation for a long period of time, the OMU portal will not automatically return to the login page. For service security reasons, if users do not perform any operation for a long period of time, the OMU portal will return to the login page or does not stay at the **Local Disk** tab page.

----End

6.4.2.3.3 Setting Parameters on the VCN WebUI

Prerequisites

For details about the VCN hardware description and installation, see the "Hardware Guide" in the corresponding VCN product documentation. For details about the VCN configuration, see *Configuration Guide*.

 NOTE

The version number is subject to the *Quick Start* delivered with the VCN. The description and link in this document are for reference only.

Context

A default IP address has been configured for the VCN before delivery. Modify the IP address based on the actual network plan.

Procedure

Step 1 Modify the IP address for the VCN.

1. Configure the PC IP address and the VCN IP address in the same network segment. Enter the OMU Portal address (the default address for VCN500 is <https://192.168.1.100:8443>; the default address for VCN510&VCN520&VCN540 is <https://192.168.2.101:8443>) in the address bar of the Internet Explorer and press the **Enter** button.

 NOTE

The OMU Portal supports Internet Explorer 8.0 and later versions.

2. On the login page, enter the user name **admin** and preset password **Change_Me**, and click **Log In** to enter the OMU Portal page. A message is displayed upon the first login indicating that you should modify the password. After modifying the password, keep it properly.

 NOTE

- If the VCN software version is V100R003 or later, the default user name is **admin**.
 - If the VCN software version is V100R002 or earlier, the default user name is **Admin**.
 - The following uses V100R003 as an example.
3. Choose **Local Configuration > Server configuration**. Set the service IP address (internal IP address of the VCN), time zone, and time according to the site requirements.

Figure 6-38 Configuring the server

Retired adapter name: `h0m0`

Business IPs: `10.43.163.50`

Subnet mask: `255.255.255.0`

Outgoing IP: `10.43.163.1`

R2 Code: `16d7f182af0b9430a3ef31e0a`

The R2 clock source name: `Yes`

R2 server IP: `10.43.163.50`

Timezone Config: `UTC+08.00`

Time Config: `Automatic (NTP)`

DST Status: `OUT`

Weekly view

☒ Enabled DST

Start time: `April` `1` `Second` `Sunday` `22 Hour` `00 Minute`

End time: `September` `1` `Second` `Sunday` `22 Hour` `00 Minute`

Offset time: `00 Minutes`

Warning:
 It is recommended that you set the R2 clock source during initial configuration. If you set the R2 clock source to other phases, server management may occur. For example, the video recording may be interrupted when performing this operation; it cannot be properly placed, or cannot be placed by itself. Changing the R2 clock source may affect the I/O between the time synchronization with the R2 clock source server. Therefore, setting when performing this operation that you set up the R2, you're not allowed to modify the time.
 It is recommended that you set the time zone and time during initial configuration. If you set the time zone and time to other phases, server management may occur. For example, the video recording may be interrupted when performing this operation; it cannot be properly placed, or cannot be placed by itself. Changing the time zone and the time setting of the R2 server that time-synchronization with the R2 clock source server. Therefore, setting when performing this operation.

Save

Not Applicable (Superior)()

 NOTE

Set **Business IP** to XXX.XXX.XXX.XXX, **Subnet mask** to 255.255.255.0, and **Gateway IP** to XXX.XXX.XXX.XXX. The values here are examples. The actual value prevails.

- (Optional) Configure the NTP synchronization. After setting **The NTP clock source server** to **Yes**, set the IP address of the NTP server.

 NOTE

Currently, the VCN and NTP source server must be in the same LAN for NTP synchronization. For details, see [Step 2](#).

If the VCN and the NTP source server are not in the same LAN, you need to manually set the time as follows: Choose **Local Configuration > Server configuration** and change **Timezone config** and **Time config** based on the time of the source server to be synchronized.

5. Choose **Maintenance > Unified Configuration**, set **Module name** to **MU**, and click **Search**.
6. In the search result, click **Edit** in the row where the value of **Parameter Name** is **NatIP** and set **Value** to the external IP address of the VCN. Click **Save**.

Figure 6-39 Setting the external IP address of the MU

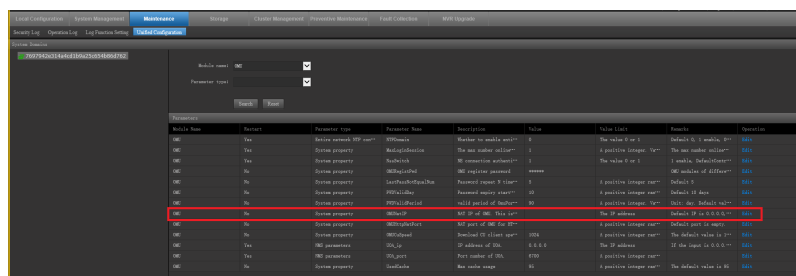
[illegible]

NOTE

Set NatIP to the external IP address of the VCN, which is the same as the external IP address mapped by the VCN on the ECC800-Pro.

- Set **Module name** to **OMU** and click **Search**.
- In the search result, click **Edit** in the row where the value of **Parameter Name** is **OMUNatIP** and set **Value** to the NATIP address of the MU. Click **Save**.

Figure 6-40 Setting the external IP address of the OMU

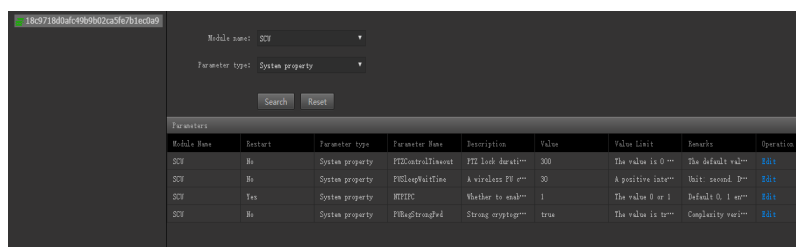


Step 2 Enable camera NTP synchronization.

The camera NTP synchronization function for the server is disabled by default. The camera NTP synchronization function needs to be enabled for the server that connects to the camera. After the camera NTP synchronization function is enabled, cameras will automatically time-synchronize from their access servers.

- Log in to the OMU portal of the VCN as user **admin**.
- Choose **Maintenance > Unified Configuration**.
- Select the server that the camera needs to access, set **Module name** to **SCU** and **Parameter type** to **System property**, and click **Search**.

Figure 6-41 Configuring camera NTP synchronization



- In the search results, click **Edit** in the row where **Parameter Name** is **NTPIP** and set **Value** to **1**.
- Click **Save**. After the camera NTP synchronization function is enabled, the camera, after being connected to the server, will automatically time-synchronize with the server.

----End

Follow-up Procedure

- The VCN automatically restarts after the IP address is modified. The restart takes about 5 minutes. After the restart, use the new IP address to access the VCN.

- Change the PC IP address to an address in the network of the new VCN IP address, enter the VCN IP address in the address box of the Internet browser, and log in to the OMU Portal system.
- (Optional) Deploy VCN in stack mode. For details, log in to the <https://e.huawei.com/>, search for the VCN product documentation, open the documentation, and see the section **(Optional) Deploying IVS in Stack Mode**.
- (Optional) Create a VCN cluster. For details, log in to the <https://e.huawei.com/>, search for the VCN product documentation, open the documentation, and see the section **(Optional) Deploying MPUs in Cluster Mode**.

NOTE

For the VCN500, search for **VCN500 Product Documentation**. For the VCN510&VCN520&VCN540, search for **VCN510&VCN520&VCN540 Product Documentation**.

6.4.2.3.4 Setting Parameters on the VCN IVS Client

Prerequisites

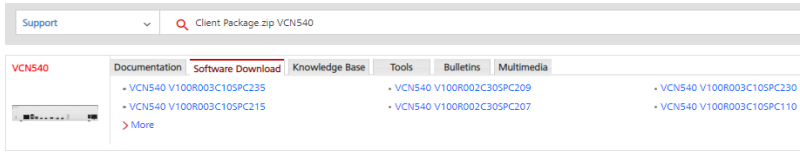
The network communication between the VCN and the camera is normal.

Procedure

Step 1 Install the VCN IVS client.

1. Download the VCN IVS client.

You can obtain the VCN IVS in either of the following ways:

Method 1	Obtain the HW_IVS_Client.exe file from the software CD-ROM delivered with the VCN.
Method 2	1. Log in to the VCN OMU Portal, choose Local Configuration > Basic Configuration, and view Current version. 2. Log in to https://support.huawei.com/enterprise/, and search for Client Package.zip followed by the VCN model (Client Package.zip VCN540 for example). In the search result, click the Software Download tab, click the version and patch number corresponding to the current version, and download the Client Package.zip software package. Figure 6-42 Client Package search result 

2. Right-click **HW_IVS_Client.exe** and choose **Run as administrator** from the shortcut menu. Use the default installation mode until the installation is complete.

3. Right-click the client program and choose **Run as administrator** from the shortcut menu. The login page is displayed, enter the user name **admin** and preset password **Change_Me**, and set **Server address** to the actual service IP address (VCN IP address) and **Port** to 9900 in the lower-right corner.

 NOTE

If the VCN IVS and VCN are deployed in the same LAN, set **Server IP address** to the VCN internal IP address (192.168.248.55, for example). If the VCN IVS is on an extranet and the VCN is on a LAN, set **Server IP address** to the VCN external IP address.

4. Click **Log In** to access the client home page. A message is displayed upon the first login indicating that you should modify the password. After modifying the password, keep it properly.

Step 2 Add a camera. For details, see the documentation delivered with the equipment or obtain the documentation by referring to the "Preparing Documentation" section. View the corresponding section.

 NOTE

The driver protocol of IPC6325 and C3220 cameras is HWSDK.

1. In the **Quick Setup** area on the VCN IVS home page, double-click **Add Camera** in the **Other** tree.
2. Click **+** in the lower left corner on the **Search criteria** page, setting the parameters according to the following table, and click **Next**.

Table 6-13 Setting search criteria

Item	Value
Start IP Address and End IP Address	IP address range
Drive	HWSDK
Access domain	Select the domain that cameras need to access
Mount server	Select the server that cameras need to access

 NOTE

If there are multiple VCNs for multiple smart modules, you are advised to evenly distribute the cameras to each VCN.

3. Click **Search**, in each camera record, enter the user name and password in the text boxes and click **Verify**. If the camera is verified successfully, select cameras to add and click **Next**.
4. Preview live video images, click the camera in the camera list on the left, and adjust camera parameters to optimize the image effect. Then click **Next**.
5. (Optional) Group the cameras and click **Next** after grouping.
6. Click **Finish** to finish adding a camera.

Step 3 Configure a server recording plan.

1. In the **Quick Setup** area on the VCN IVS home page, double-click **Server Recording Plan** in the **Other** tree.
2. Select the camera on the **Cameras** list and click **Next**.
3. (Optional) Set recording parameters, and click **Next**.
4. Set recording plan parameters in the **Time settings**. Drag the timeline to select the time segment for implementing video recording.

 NOTE

If you set the recording plan policy is to **All**, you do not need to set the recording plan time.

5. Click **Next** to complete the recording plan setting. When  is displayed in the status bar, the recording plan has been set successfully.
6. Click **Finish**.

Step 4 Create a user.

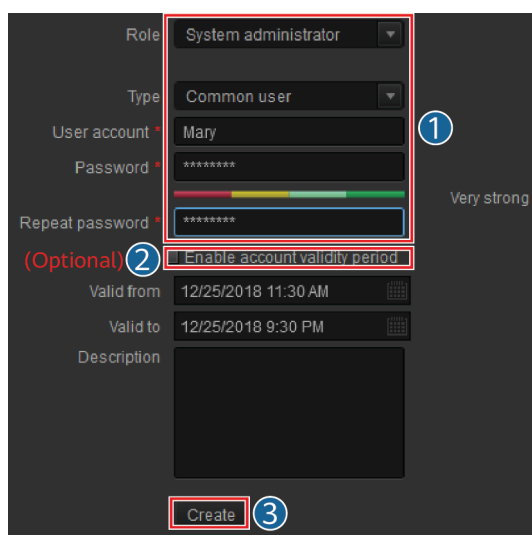
When connecting to the VCN on the NetEco, you need to log in to the VCN as a non-admin user.

1. Log in to the VCN IVS as user **admin**.
2. On the VCN IVS home page, double-click **Add User**, create a user, and click **Next**. The **Assign Rights** page is displayed.

 NOTE

When creating a user, you can select **Enable account validity period** and set **Valid from** and **Valid to** to set the account validity period for the created user.

Figure 6-43 Creating a user



DM25H00137

3. Set **Multi-point logins** to a value greater than 2.
4. In the **Assign Device View Rights** area, select the cameras to be browsed and queried by the user. Set other parameters based on the documentation

delivered with the equipment or the documentation obtained by referring to the **Preparing Documentation** section, and click **Finish**.

----End

6.4.2.4 Commissioning the IVS1800

6.4.2.4.1 Setting Parameters on the IVS1800 WebUI

Context

A default IP address has been configured for the IVS1800 before delivery. Modify the IP address based on the actual network plan.

Procedure

Step 1 Check whether the network connection between the PC for logging in to the OMU portal and the IVS1800 is normal.

If the device is just delivered or has just been restored to factory settings, ensure that the PC for logging in to the OMU portal is directly connected to the IVS1800 and is in the same network segment as the IVS1800.

For the device that is just delivered or has just been restored to factory settings, its network information is as follows:

- IP address: 192.168.3.111
- Subnet mask: 255.255.255.0
- Gateway address: 192.168.3.1

Step 2 Enter **https://IP address:8443** in the address box, and press **Enter**.

In the URL, **IP address** indicates the IP address of the IVS1800.

NOTE

The OMU portal supports Internet Explorer 10.0 and later versions.

Step 3 Log in to the OMU portal. Set the service system and operating system passwords at the first login.

1. Set the password for user **admin** of the service system.
2. Set the password for user **admin** of the operating system.
3. Set the password for user **root** of the operating system.
4. Use the configured service system password to log in to the OMU portal again.

Step 4 Configure disk initialization.

NOTE

Recording data can be stored only after you install and initialize the disks.

1. Choose **Local Configuration > Local Disk**.
2. In the upper right corner of the **RAID Groups** area, click **Initial Disk**

3. Configure disk initialization.

Figure 6-44 Disk initialization (RAID 5 economical configuration by default)

1. RAID mode: ☒ RAID5 ☐ NON-RAID

2. RAID configuration mode: ☐ Recommended ☒ Economic

Kindly Reminder: Recommended: This configuration only create a Raid group with 1 active spare disk, and safe; Economic: This Configuration only create a Raid group, large capacity, but no active spare disk, reliability and safety is low

3. HdAlgSize(GB): 30

Kindly Reminder: range(20-1024). When it is empty, the maximum available capacity is 20GB, which can be adjusted by the customer

4. Start Back

Table 6-14 RAID mode description

Parameter Name	Description
RAID High Reliability	– RAID5 Recommended Four or more hard disks are required, and one hard disk is used as the hot spare disk. – RAID5 Economical Three or more hard disks are required, and one hard disk is used as the hot spare disk.
NON-RAID	– Each recording file is stored on only one hard disk. The disk usage is high, but the data storage reliability is lower than that in RAID 5 mode. – When the number of hard disks is greater than or equal to 7, the system automatically uses the three hard disks with the smallest slot numbers to form a RAID 1 group, in which one hard disk functions as the hot spare disk. Every four of the remaining hard disks form a RAID 10 group. If the number of remaining hard disks is less than 4, the disks do not form a RAID 10 group.

Step 5 Modify the IP address for the IVS1800.

1. Choose **Local Configuration > Server configuration**. Set the service IP address (internal IP address of the IVS1800), time zone, and time according to the site requirements.

Figure 6-45 Configuring the server (Single Mode by default)

NetworkConfig

*NIC Mode	☒ Single Mode ☐ Double Mode
Network adapter name	bond0
*Business IP	192.168.3.11
*Subnet mask	255.255.255.0
*Gateway IP	192.168.3.1

NOTE

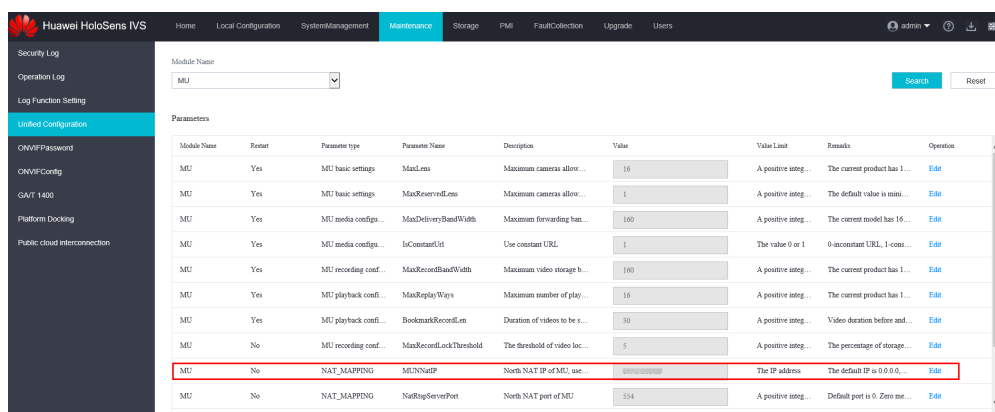
Set **Business IP** to XXX.XXX.XXX.XXX, **Subnet mask** to 255.255.255.0, and **Gateway IP** to XXX.XXX.XXX.XXX. The values here are examples. The actual values may vary.

2. Change the PC IP address to an address in the network segment of the new IVS1800 IP address, enter the IVS1800 IP address in the address box of the Internet browser, and log in to the OMU portal system.

Step 6 Configure NAT on the IVS1800.

(1) Configure the MU:

1. Choose **Maintenance > Unified Configuration**, set **Module Name** to **MU**, and click **Search**.
2. Click **Edit** in the record where the value of **Parameter Name** is **MUNatIP**, set the external IP address of the IVS1800, and click **Save**.

Figure 6-46 Setting the external IP address of the MU

Module Name	Runat	Parameter type	Parameter Name	Description	Value	Value Limit	Remarks	Operation
MU	Yes	MU basic settings	MaxLens	Maximum camera allow...	16	A positive integ...	The current product has 1...	Edit
MU	Yes	MU basic settings	MaxReservedLens	Maximum camera allow...	1	A positive integ...	The default value is maxi...	Edit
MU	Yes	MU media config...	MaxDeliveryBandWidth	Maximum forwarding han...	160	A positive integ...	The current model has 16...	Edit
MU	Yes	MU media config...	IsConstantUrl	Use constant URL	1	The value 0 or 1	0-constant URL, 1-cons...	Edit
MU	Yes	MU recording conf...	MaxRecordBandWidth	Maximum video storage b...	160	A positive integ...	The current product has 1...	Edit
MU	Yes	MU playback confi...	MaxReplyWays	Maximum number of play...	16	A positive integ...	The current product has 1...	Edit
MU	Yes	MU playback confi...	BookmarkRecordLen	Duration of videos to be s...	30	A positive integ...	Video duration before and...	Edit
MU	No	MU recording conf...	MaxRecordLockThreshold	The threshold of video loc...	5	A positive integ...	The percentage of storage...	Edit
MU	No	NAT_MAPPING	MUNatIP	North NAT IP of MU, use...	192.168.3.11	The IP address	The default IP is 0.0.0.0...	Edit
MU	No	NAT_MAPPING	NatRtpServerPort	North NAT port of MU	554	A positive integ...	Default port is 0. Zero me...	Edit

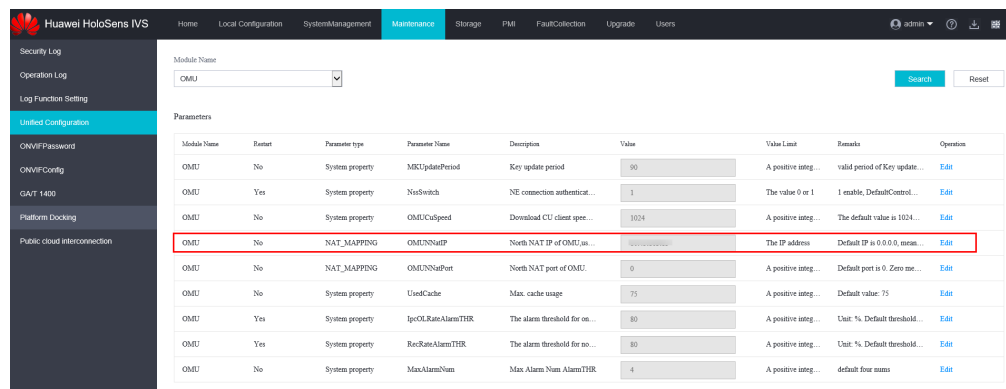
3. Click **Edit** in the row where the value of **Parameter Name** is **NatRtpServerPort**, and set the NAT port number of the MU. Ensure that the setting is the same as the NAT mapped port number configured on the firewall. Click **Save**.

NOTE

If no external IP address is mapped, retain the default value of **NatRtspServerPort**.

(2) Configure the OMU:

1. Set **Module Name** to **OMU** and click **Search**.
2. Click **Edit** in the row where the value of **Parameter Name** is **OMUNNatIP** and set **Value** to the **MUNNatIP** address of the MU. Click **Save**.

Figure 6-47 Setting the external IP address of the OMU

(3) Configure the SMU:

1. Set **Module Name** to **SMU** and click **Search**.
2. Click **Edit** in the row where the value of **Parameter Name** is **SDKNatIP** and set **Value** to the NAT-mapped IP address configured on the firewall. Click **Save**.
3. Click **Edit** in the row where the value of **Parameter Name** is **SDKNatPort** and set **Value** to the NAT mapped port number configured on the firewall. Click **Save**.

(4) Set other parameters based on the site requirements by referring to the preceding steps.

Table 6-15 Parameter description

Module Name	Parameter Name	Setting
IMGU	IMGUNNatIP	Northbound IP address of the IVS1800, which must be the same as the NAT-mapped IP address configured on the firewall.
	IMGUNNatPort	NAT port number of the IVS1800 IMGU, which must be the same as the NAT-mapped port number configured on the firewall. The default port number of the IMGU before mapping is 9554.

Module Name	Parameter Name	Setting
MU	MUNatIP	Northbound IP address of the IVS1800, which must be the same as the NAT-mapped IP address configured on the firewall.
	NatRtspServerPort	NAT port number of the IVS1800 MU, which must be the same as the NAT mapped port number configured on the firewall. The default port number of the MU before mapping is 554.
	NatRtspTlsServerPort	TLS NAT port number of the IVS1800 MU, which must be the same as the NAT mapped port number configured on the firewall. The default TLS port number of the MU before mapping is 322.

Step 7 (Optional) Configure the IVS1800 to synchronize time with the NTP server. Choose **Local Configuration > Server configuration** and configure the server time information.

Table 6-16 Parameter description

Parameter	Setting
The NTP clock source server	Indicates whether the NTP clock source server is specified for time synchronization. • Select Yes if an NTP server is configured onsite. • Select No If no NTP server is configured onsite.
NTP server IP	Indicates the IP address of the NTP clock source server. After this parameter is specified, the server synchronizes the time to this clock source.

- If an NTP server is configured onsite, synchronize the time with the NTP server.
- If no NTP server is configured onsite, manually configure the server time: Change **Timezone config** and **Time config** based on the time of the source server to be synchronized.

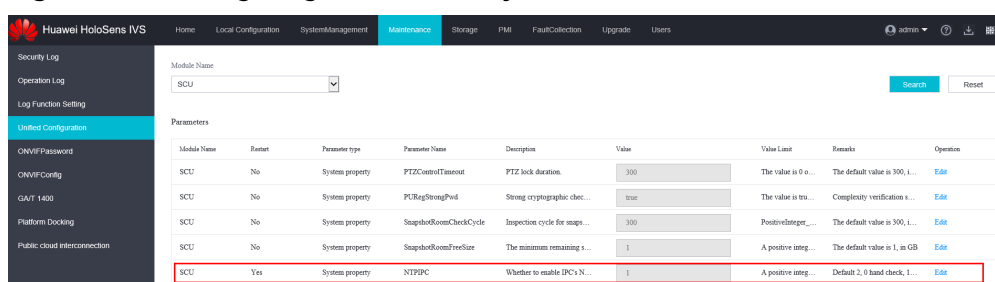
Step 8 Configure cameras to synchronize time with the IVS1800.

The camera NTP synchronization function for the server is disabled by default. The camera NTP synchronization function needs to be enabled for the server that

connects to the camera. After the camera NTP synchronization function is enabled on the server, cameras will automatically synchronize time with the server.

1. Log in to the OMU portal as user **admin**.
2. Choose **Maintenance > Unified Configuration**.
3. Set **Module Name** to **SCU** and click **Search**.
4. In the search results, click **Edit** in the row where **Parameter Name** is **NTPIPC** and set **Value** to **1**.
5. Click **Save**. After the camera NTP synchronization function is enabled, the camera, after being connected to the server, will automatically time-synchronize with the server.

Figure 6-48 Configuring camera NTP synchronization



Step 9 Create a user.

When connecting to the IVS1800 on the NetEco, you need to log in as a non-admin user.

1. Log in to the OMU portal as user **admin**.
2. Choose **User Management > Add User**.

NOTE

When creating a user, you can select **Enable account validity period** and set **Valid from** and **Valid to** to set the account validity period for the created user.

3. Set **Multi-point logins** to a value greater than 2.
4. On the **User List** page, click **Permission Settings** next to the new user, select the cameras to be browsed and queried, set other parameters, and click **Save**.

----End

6.4.2.4.2 Setting Parameters on the IVS1800 WebUI

Context

A default IP address has been configured for the IVS1800 before delivery. Modify the IP address based on the actual network plan.

Procedure

- Step 1** Check whether the network connection between the PC for logging in to the OMU portal and the IVS1800 is normal.

If the device is just delivered or has just been restored to factory settings, ensure that the PC for logging in to the OMU portal is directly connected to the IVS1800 and is in the same network segment as the IVS1800.

For the device that is just delivered or has just been restored to factory settings, its network information is as follows:

- IP address: 192.168.3.111
- Subnet mask: 255.255.255.0
- Gateway address: 192.168.3.1

Step 2 Enter **https://IP address:8443** in the address box, and press **Enter**.

In the URL, **IP address** indicates the IP address of the IVS1800.

 NOTE

The OMU portal supports Internet Explorer 10.0 and later versions.

Step 3 Log in to the OMU portal. Set the service system and operating system passwords at the first login.

1. Set the password for user **admin** of the service system.
2. Set the password for user **admin** of the operating system.
3. Set the password for user **root** of the operating system.
4. Use the configured service system password to log in to the OMU portal again.

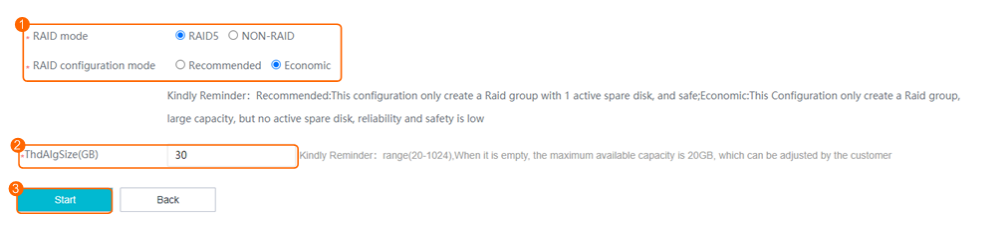
Step 4 Configure disk initialization.

 NOTE

Recording data can be stored only after you install and initialize the disks.

1. Choose **Local Configuration > Local Disk**.
2. In the upper right corner of the **RAID Groups** area, click **Initial Disk**
3. Configure disk initialization.

Figure 6-49 Disk initialization (RAID 5 economical configuration by default)



1. RAID mode: ☒ RAID5 ☐ NON-RAID

2. RAID configuration mode: ☐ Recommended ☒ Economic

Kindly Reminder: Recommended: This configuration only create a Raid group with 1 active spare disk, and safe; Economic: This Configuration only create a Raid group, large capacity, but no active spare disk, reliability and safety is low

3. ThdAlgSize(GB): Kindly Reminder: range(20-1024). When it is empty, the maximum available capacity is 20GB, which can be adjusted by the customer

Start Back

Table 6-17 RAID mode description

Parameter Name	Description
RAID High Reliability	– RAID5 Recommended Four or more hard disks are required, and one hard disk is used as the hot spare disk. – RAID5 Economical Three or more hard disks are required, and one hard disk is used as the hot spare disk.
NON-RAID	– Each recording file is stored on only one hard disk. The disk usage is high, but the data storage reliability is lower than that in RAID 5 mode. – When the number of hard disks is greater than or equal to 7, the system automatically uses the three hard disks with the smallest slot numbers to form a RAID 1 group, in which one hard disk functions as the hot spare disk. Every four of the remaining hard disks form a RAID 10 group. If the number of remaining hard disks is less than 4, the disks do not form a RAID 10 group.

Step 5 Modify the IP address for the IVS1800.

1. Choose **Local Configuration > Server configuration**. Set the service IP address (internal IP address of the IVS1800), time zone, and time according to the site requirements.

Figure 6-50 Configuring the server (Single Mode by default)

NetworkConfig

*NIC Mode

☒ Single Mode ☐ Double Mode

Network adapter name

bond0

*Business IP

192.168.3.11

*Subnet mask

255.255.255.0

*Gateway IP

192.168.3.1

NOTE

Set **Business IP** to XXX.XXX.XXX.XXX, **Subnet mask** to 255.255.255.0, and **Gateway IP** to XXX.XXX.XXX.XXX. The values here are examples. The actual values may vary.

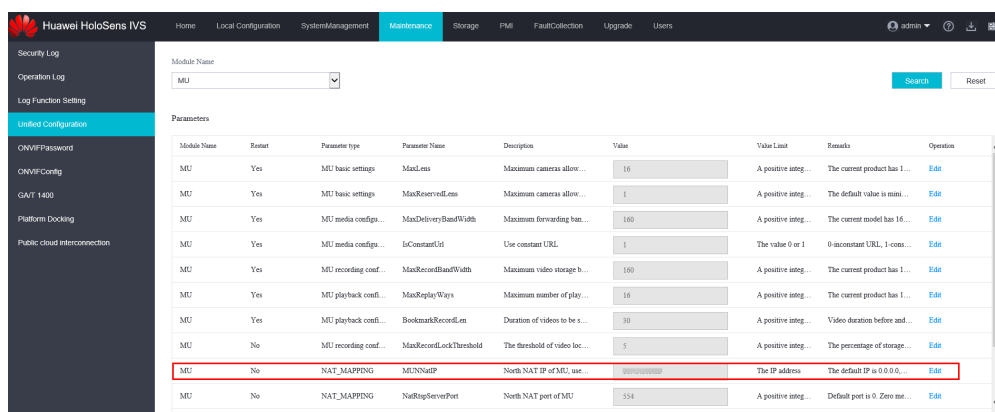
2. Change the PC IP address to an address in the network segment of the new IVS1800 IP address, enter the IVS1800 IP address in the address box of the Internet browser, and log in to the OMU portal system.

Step 6

 Configure NAT on the IVS1800.

- (1) Configure the MU:

1. Choose **Maintenance > Unified Configuration**, set **Module Name** to **MU**, and click **Search**.
2. Click **Edit** in the record where the value of **Parameter Name** is **MUNatIP**, set the external IP address of the IVS1800, and click **Save**.

Figure 6-51 Setting the external IP address of the MU

Module Name	Runat	Parameter type	Parameter Name	Description	Value	Value Limit	Remarks	Operation
MU	Yes	MU basic settings	MaxLens	Maximum camera allow...	16	A positive integ...	The current product has 1...	Edit
MU	Yes	MU basic settings	MaxReservedLens	Maximum camera allow...	1	A positive integ...	The default value is maxi...	Edit
MU	Yes	MU media config...	MaxDeliveryBandWidth	Maximum forwarding han...	160	A positive integ...	The current model has 16...	Edit
MU	Yes	MU media config...	IsConstantUrl	Use constant URL	1	The value 0 or 1	0-constant URL, 1-cons...	Edit
MU	Yes	MU recording conf...	MaxRecordBandWidth	Maximum video storage b...	160	A positive integ...	The current product has 1...	Edit
MU	Yes	MU playback confi...	MaxReplyWays	Maximum number of play...	16	A positive integ...	The current product has 1...	Edit
MU	Yes	MU playback confi...	BookmarkRecordLen	Duration of videos to be s...	30	A positive integ...	Video duration before and...	Edit
MU	No	MU recording conf...	MaxRecordLockThreshold	The threshold of video loc...	5	A positive integ...	The percentage of storage...	Edit
MU	No	NAT_MAPPING	MUNatIP	North NAT IP of MU, use...	192.168.3.11	The IP address	The default IP is 0.0.0.0...	Edit
MU	No	NAT_MAPPING	NatRtpServerPort	North NAT port of MU	554	A positive integ...	Default port is 0. Zero me...	Edit

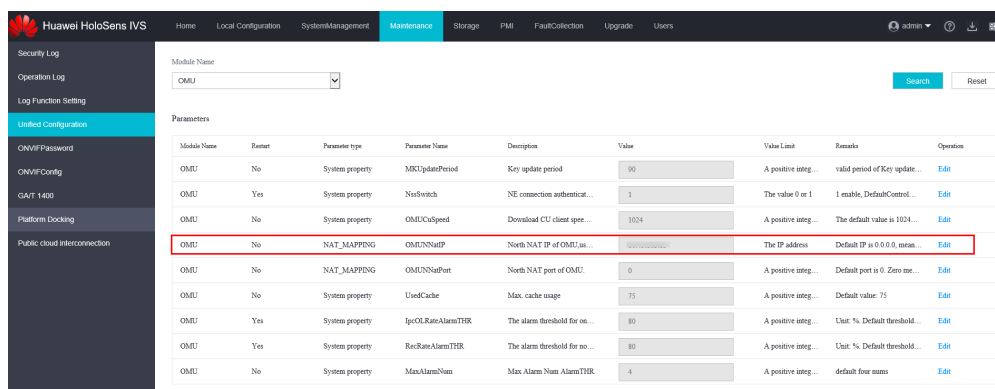
3. Click **Edit** in the row where the value of **Parameter Name** is **NatRtpServerPort**, and set the NAT port number of the MU. Ensure that the setting is the same as the NAT mapped port number configured on the firewall. Click **Save**.

NOTE

If no external IP address is mapped, retain the default value of **NatRtspServerPort**.

(2) Configure the OMU:

1. Set **Module Name** to **OMU** and click **Search**.
2. Click **Edit** in the row where the value of **Parameter Name** is **OMUNNatIP** and set **Value** to the **MUNNatIP** address of the MU. Click **Save**.

Figure 6-52 Setting the external IP address of the OMU

(3) Configure the SMU:

1. Set **Module Name** to **SMU** and click **Search**.
2. Click **Edit** in the row where the value of **Parameter Name** is **SDKNatIP** and set **Value** to the NAT-mapped IP address configured on the firewall. Click **Save**.
3. Click **Edit** in the row where the value of **Parameter Name** is **SDKNatPort** and set **Value** to the NAT mapped port number configured on the firewall. Click **Save**.

(4) Set other parameters based on the site requirements by referring to the preceding steps.

Table 6-18 Parameter description

Module Name	Parameter Name	Setting
IMGU	IMGUNNatIP	Northbound IP address of the IVS1800, which must be the same as the NAT-mapped IP address configured on the firewall.
	IMGUNNatPort	NAT port number of the IVS1800 IMGU, which must be the same as the NAT-mapped port number configured on the firewall. The default port number of the IMGU before mapping is 9554.

Module Name	Parameter Name	Setting
MU	MUNatIP	Northbound IP address of the IVS1800, which must be the same as the NAT-mapped IP address configured on the firewall.
	NatRtspServerPort	NAT port number of the IVS1800 MU, which must be the same as the NAT mapped port number configured on the firewall. The default port number of the MU before mapping is 554.
	NatRtspTlsServerPort	TLS NAT port number of the IVS1800 MU, which must be the same as the NAT mapped port number configured on the firewall. The default TLS port number of the MU before mapping is 322.

Step 7 (Optional) Configure the IVS1800 to synchronize time with the NTP server. Choose **Local Configuration > Server configuration** and configure the server time information.

Table 6-19 Parameter description

Parameter	Setting
The NTP clock source server	Indicates whether the NTP clock source server is specified for time synchronization. • Select Yes if an NTP server is configured onsite. • Select No If no NTP server is configured onsite.
NTP server IP	Indicates the IP address of the NTP clock source server. After this parameter is specified, the server synchronizes the time to this clock source.

- If an NTP server is configured onsite, synchronize the time with the NTP server.
- If no NTP server is configured onsite, manually configure the server time: Change **Timezone config** and **Time config** based on the time of the source server to be synchronized.

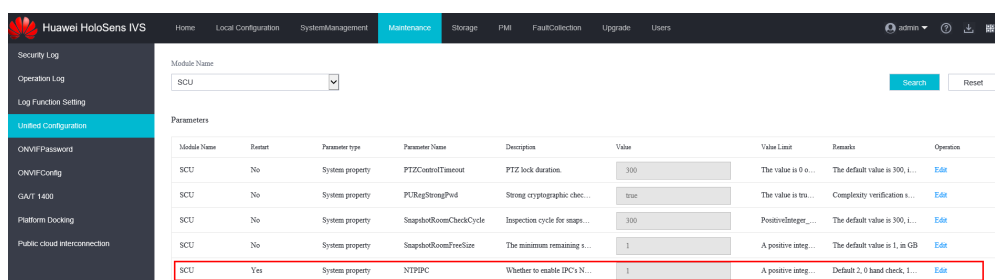
Step 8 Configure cameras to synchronize time with the IVS1800.

The camera NTP synchronization function for the server is disabled by default. The camera NTP synchronization function needs to be enabled for the server that

connects to the camera. After the camera NTP synchronization function is enabled on the server, cameras will automatically synchronize time with the server.

1. Log in to the OMU portal as user **admin**.
2. Choose **Maintenance > Unified Configuration**.
3. Set **Module Name** to **SCU** and click **Search**.
4. In the search results, click **Edit** in the row where **Parameter Name** is **NTPICP** and set **Value** to **1**.
5. Click **Save**. After the camera NTP synchronization function is enabled, the camera, after being connected to the server, will automatically time-synchronize with the server.

Figure 6-53 Configuring camera NTP synchronization



Step 9 Create a user.

When connecting to the IVS1800 on the NetEco, you need to log in as a non-admin user.

1. Log in to the OMU portal as user **admin**.
2. Choose **User Management > Add User**.

NOTE

When creating a user, you can select **Enable account validity period** and set **Valid from** and **Valid to** to set the account validity period for the created user.

3. Set **Multi-point logins** to a value greater than 2.
4. On the **User List** page, click **Permission Settings** next to the new user, select the cameras to be browsed and queried, set other parameters, and click **Save**.

----End

6.4.2.5 Configuring Camera Parameters on the NetEco

This section describes how to configure video parameters on the **Parameter Configuration** page.

Prerequisites

- You have the video management permission.
- Use Google Chrome or Mozilla Firefox of the latest version to play videos.
- The video-related adapter software installation package has been installed.

Procedure

- Step 1** Choose **Monitor > Security > Camera Management** from the main menu. The **Camera Management** window is displayed.
- Step 2** Choose **VCN/IVS** on the left of the page. The **VCN/IVS** page is displayed.
- Step 3** Specify parameters in the right pane based on [Table 6-20](#).

NOTICE

- If not all ActiveX controls are enabled, the test connection fails after filling in the correct parameter information and clicking **Test**.
- Enable **ActiveX** controls. For details, see [6.4.2.6 Registering with the OCX Plug-in](#).

Table 6-20 Parameter description

Parameter	Description	Example
Server IP Address	Indicates the IP address of the VCN or IVS server. It is a correct IPv4 address. The IP address consists of four digits separated with dots. Each digit ranges from 0 to 255. The IP address cannot be 0.0.0.0.	XXX.XXX.XXX.XXX
Server Port Number	Indicates the port number of the VCN or IVS server. NOTE The default port number is 9900 .	9900

Parameter	Description	Example
Login User	User name for logging in to the VCN or IVS client. NOTE • The NetEco needs to have browse and query permissions. Configure the video system users with browse and query permissions. • It is recommended that the new user name created using the IVS be used to access the camera. Before accessing the camera, ensure that the initial password of the user has been changed and the user has successfully logged in to the IVS. • It is recommended that the number of IVS clients to which the user can log in to a value greater than 5. Otherwise, when the user has logged in to the IVS client, the user cannot log in to it through the NetEco. • The Admin user cannot log in to the NetEco to connect to the VCN.	Huawei123
Login Password	Password for logging in to the VCN or IVS client. Click Set Password and configure the password on the displayed page. If the password does not comply with the rules, please change the password on device.	Change_Me

Step 4 Click **Test** after configuring parameters.

 NOTE

- During the first test, the page turns blank. Wait 30s.
- If the test fails, a message indicating a connection failure is displayed.

Step 5 Click **Apply**.

----End

6.4.2.6 Registering with the OCX Plug-in

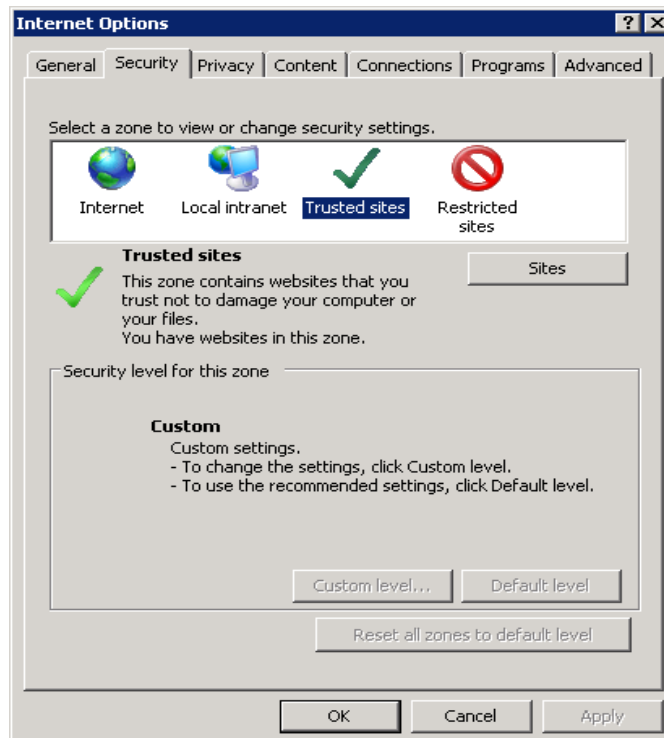
Only after you register with the OCX plug-in, you can play videos recorded by the camera on the NetEco in real time.

Procedure

Step 1 Open Internet Explorer and choose **Tools > Internet Options**.

Step 2 Click **Security**, as shown in [Figure 6-54](#).

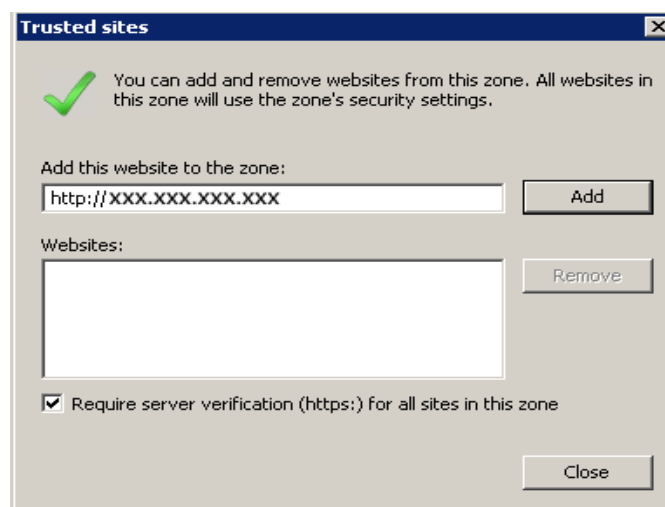
Figure 6-54 Security tab page



Step 3 Add the IP address of the client to the trusted site list.

1. Select **Trusted sites** and click **Sites**. Add the IP address of the client to the trusted site list, as shown in [Figure 6-55](#).

Figure 6-55 Trusted site list



2. Click **Add** and then click **Close**.

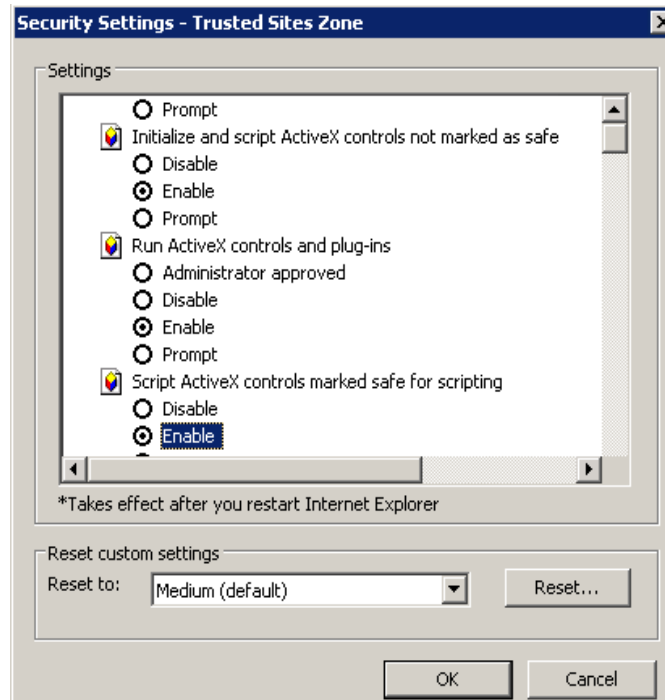
Step 4 Enable ActiveX-related options for trusted sites.

 NOTE

After ActiveX-related options are enabled, a message is displayed, indicating that the computer is prone to risks due to security settings. Ignore the message.

1. Choose **Trusted sites > From definition rank**. The **Security setting – trusted stand region** dialog box is displayed, as shown in [Figure 6-56](#).

Figure 6-56 Security setting – trusted stand region



2. Enable the following options and then click **Ok**.
 - **Initialize and script ActiveX controls not marked as safe**
 - **Script ActiveX controls marked safe for scripting**
 - **Download signed ActiveX controls**
 - **Download unsigned ActiveX controls**
3. A dialog box is displayed, indicating **Does the determination need to change the establishment of this region?** Click **Yes**.

Step 5 Register with the OCX plug-in.

Restart Internet Explorer and enter the IP address to be accessed by the client. The page for watching videos is displayed. Click **Install** according to the prompt message. After the OCX plug-in is installed, you can watch the videos. If videos are not displayed, contact Huawei technical support.

 NOTE

If it is the first time to install the plug, you need to wait about 10 to 20 seconds.

Step 6 If the OCX plug-in needs to be registered on the client again, perform the following operations to uninstall the OCX plug-in and then re-install it:

1. Close Internet Explorer.
2. Find **C** disk directory folder exists **eSDK_IVS** folder, right-click to select **Delete**.
3. Restart Internet Explorer, enter the IP address for accessing the NetEco client, and open the page for video modules. The NetEco automatically installs the OCX plug-in.

----End

6.4.2.7 Adding the Video Management System

This topic describes how to quickly add an online camera that is not in any management domain to a management domain using the automatic discovery function provided by the system.

Prerequisites

- You have logged in to the NetEco client using a web browser.
- You have the operation rights for **Camera Management**.
- You have set parameters on the **Parameter Configuration** page, and the connection between the NetEco and VCN500 server is successful.
- A camera has connected to the VCN server.

Procedure

Step 1 Choose **Monitor > Security > Camera Management** from the main menu.

Step 2 In the left navigation tree, choose **Discovery Camera**.

Step 3 Select one or more cameras and click **Create**.

Step 4 In the **Add camera** dialog box, set related parameters, select the required management domain, and click **Confirm**.

NOTE

- Add a camera to management domains excluding the root node, subnets and cabinet using the automatic discovery function.
- After a camera is added, it will be displayed under the corresponding management domain on the **Data Center Planning** page. On the **Data Center Planning** page, you can set parameters such as the **Name** for the camera.

----End

Follow-up Procedure

Table 6-21 describes the operations that can be performed on the **Camera Management** page.

Table 6-21 Follow-up procedure

If You Want To...	Then...
Query the information about a camera	On the Camera Management page, specify one or multiple of the keywords Name and IP Address .

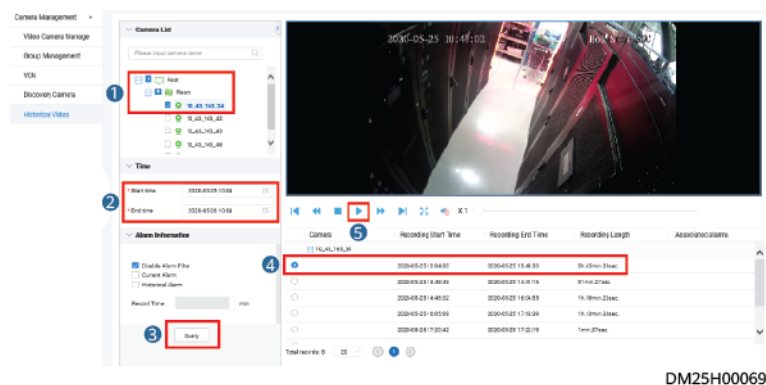
6.4.2.8 Setting Video Playback

Prerequisites

- A server recording plan has been configured on the VCN IVS client.
- Video parameters have been set on the NetEco and cameras have been connected to the NetEco.
- The VCN/IVS server has been connected properly and cameras have been connected.
- The camera adapter has been installed on the NetEco.

Procedure

- Step 1** Choose **Monitor > Security > Camera Management** from the main menu.
- Step 2** In the navigation pane, choose **Historical Video**.
- Step 3** In the **Camera List** area, select a camera for video playback.
- Step 4** In the **Time** area, select a time range for video playback and click **Query**.
- Step 5** Select the recording file to be viewed and click the play button.

Figure 6-57 Setting video playback

----End

6.4.3 Adding a Smart Cooling Product

6.4.3.1 Setting Monitoring Parameters for the Smart Cooling Product (over Modbus-TCP)

The monitoring parameter settings are similar for smart cooling products that connect to the NMS over Modbus-TCP. This section uses FusionCol8000-E400 as an example.

Prerequisites

- You have obtained the IP address, subnet mask, and default gateway information planned for the smart cooling product.
- The smart cooling product is powered on.

Procedure

Step 1 Tap **Settings** on the FusionCol8000-E400 home screen.

Step 2 Enter the user name and password of an administrator.

 NOTE

The preset user name and password are respectively **admin** and **000001**. To ensure access security, change the password upon the first login.

Step 3 Choose **Comm Settings** > **Modbus Settings** and set Modbus-TCP parameters by referring to [Table 6-22](#).

 NOTE

The encryption mode must be the same as it on the NMS.

 WARNING

After the **Encryption operation CBC** parameter is set, the system automatically restarts. Exercise caution when performing this operation.

Figure 6-58 Warning dialog box

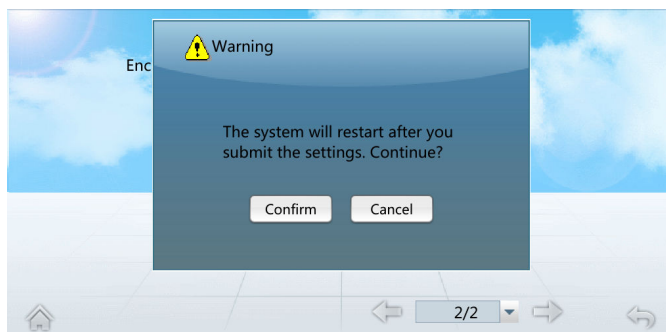


Table 6-22 Modbus TCP parameter settings

Parameter	Setting	Setting Method
Link mode	Server, Client, Server and client	- If you set Link mode to Server, the smart cooling product, as a server, supports two client connection and establishes communication. - If you set Link mode to Client, the smart cooling product, as a client, can connect to a remote server and establish communication. - If you set Link mode to Server and client, the smart cooling product, as a server, supports two client connection and establishes communication. In addition, the smart cooling product, as a client, can connect to a remote server and establish communication.
Client encryption	Enable, Disable	This parameter is configurable when Link mode is set to Client .
Server encryption	Enable, Disable	This parameter is configurable when Link mode is set to Server .
Encryption operation CBC	Enable, Disable	Encryption operation CBC is enabled by default. Determine whether to use the encryption operation CBC when connecting to other devices based on the site requirements.
NMS IP address	-	Enter the actual IP address of the NMS. IP addresses of the display panel, NMS client, and NMS server must be unique. This parameter is configurable when Link mode is set to Client .
NMS port number	-	This parameter is configurable when Link mode involves Client. - Connecting to the NetEco: Set this parameter to 32907 if Client encryption is enabled, or set it to 32906 if Client encryption is disabled. - Connecting to other NMSs: You are advised not to change the value. In special cases, set this parameter based on the site requirements.
Pre-shared password	-	Secondary authentication password used for Modbus-TCP connection.

Step 4 Return to the home screen, and choose **Settings > Comm Settings > WAN IP Settings** or **Settings > Comm Settings > IP Settings**.

Table 6-23 Parameters for WAN IP settings

Parameter	Setting
IP address	Set according to the actual plan.

Parameter	Setting
Subnet mask	Set according to the actual plan.
Gateway	Set according to the actual plan.

----End

6.4.3.2 Creating a Smart Cooling Product on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **Air Conditioner**.

Step 5 Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-24 Modbus-TCP device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set the IP address of the device.
Port	Set this parameter to the port number of the device. NOTE When you need to create a Modbus TCP smart cooling product, specify the port number based on scenarios. If the smart cooling product works as the server, specify the port number as 502. If the smart cooling product works as the client, specify the port number as 1.

Parameter	Description
Device Address	Set this parameter to the address set on the device.
Timeout period	Timeout duration for a connection test. The default value is 3s .
Connection Mode	Indicates the connection mode of a device. You can set this parameter to Non-SSL Connection or SSL Connection. If you modify Connection Mode on the NetEco, you must modify Connection Mode on the WebUI of the device at the same time. NOTE • Connection Mode for the NetEco and device must be the same. • By default, Connection Mode is set to SSL Connection for the NetEco and device. • A non-SSL connection has security risks. You are advised to select the secure SSL connection.
Authentication Password	Indicates the re-authentication password for the NetEco and device. 1. Click Modify. NOTE After the device is saved, the Modify button is displayed. 2. In the displayed dialog box, enter the New Password and Confirm Password. NOTE - The default re-authentication password for the NetEco and device is Modifyme_123. - The device password should be consistent with the NetEco password. - If the password does not meet requirements, modify it on the device. 3. Select Send To Device. NOTE If you select YES, the re-authentication password for the NetEco and device is changed at the same time. If you select NO, only the re-authentication password of NetEco is changed on the server. 4. Click OK.
Receive Timeout(ms)	Specifies the timeout period for waiting for the response packet from the NE after a packet is sent.
Max Register Num	During data collection, the number of requested registers is too large. As a result, the NE response times out or does not respond. This parameter is added to specify the number of requested registers. When a collection task is delivered, the task is split into multiple requests based on this parameter and then delivered to the NE.

Parameter	Description
Heartbeat Period(s)	Specifies the instance-level heartbeat interval.

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.4.4 Adding a Refrigeration Station

A refrigeration station is a management domain that includes plate heat exchangers, chilled water pumps, cooling pumps, water chillers, cooling towers, and chiller group control.

6.4.4.1 Creating a Chiller Subsystem on the NetEco (Modbus-TCP Protocol)

When the chiller subsystem is configured, bind all devices in the refrigeration station to the chiller subsystem in sequence by referring to this section.

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **ChillerPlantControl**.

Step 5 Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-25 Modbus-TCP subsystem parameter description

Parameter	Description
Managed Object Name	Name of the subsystem and device to be created
IP	IP address of the chiller subsystem
Port	Port number of the chiller subsystem The default port number is 502 . You can change the port number as required.
Device Address	Set this parameter to the address set on the device.
Connection Mode	Connection mode of a device. You can set this parameter to Non-SSL Connection or SSL Connection. If you modify the connection mode on the NetEco, you must modify the connection mode on the device WebUI accordingly. NOTE - The connection mode settings for the NetEco and device must be the same. - By default, Connection Mode is set to SSL Connection for the NetEco and device. - A non-SSL connection has security risks. You are advised to select the secure SSL connection.
Authentication password	Indicates the re-authentication password for the NetEco and device. - Click Modify. In the displayed dialog box, enter the New Password and Confirm Password. NOTE - After the device is saved, the Modify button is displayed. - For details about the device password, see the user manual of the device. - The device password should be consistent with the NetEco password. - If the password does not meet requirements, modify it on the device. - Select a value for Send To Device. NOTE If you select YES, the re-authentication password for the NetEco and device is changed at the same time. If you select NO, only the re-authentication password of NetEco is changed on the server. - Click OK.
Timeout Period	Timeout duration for a connection test. The default value is 3s .

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.4.4.2 Creating a Chiller on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.

Context

This section describes how to add refrigeration station devices (chiller group control, for example) on the NetEco.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **Chiller**.

Step 5 Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-26 Subsystem device parameter description

Parameter	Description
Managed Object Name	Name of the subsystem and device to be created
Subsystem	Subsystem corresponding to the chiller created in 6.4.4.1 Creating a Chiller Subsystem on the NetEco (Modbus-TCP Protocol)

Step 7 After the binding the subsystem, select the subsystem to add the mapping file on the current page, click  on the top of the navigation tree, and import the corresponding mapping file based on the subsystem type.

 NOTE

- The mapping file must contain information about all devices to be monitored.
- The mapping file imported last time is used. The mapping file imported earlier will be overwritten.

Step 8 Click  on the toolbar to save the device information.

----End

6.4.5 Adding a UPS

6.4.5.1 Setting Monitoring Parameters for a UPS2000-G (over SNMP)

Before connecting UPS2000-G to NetEco, you should set the IP address on the UPS2000-G, add user and set permissions on the WebUI of UPS2000-G.

Prerequisites

- You have obtained the IP address, subnet mask, and default gateway planned for the UPS2000-G. UPS stands for uninterruptible power system.
- The UPS2000-G is powered on.

Context

- UPSs have various versions, for which UPS WebUIs may differ. Perform operations based on the actual WebUI.
- Connecting the UPS2000-G to the NetEco in DES and MD5 protocols poses potential risks. Therefore, exercise caution when deciding to do so.

Procedure

Step 1 Set the IP address on the UPS2000-G.

1. Press  next to the UPS2000-G LCD.
2. Press  and select **Settings**.
3. Press  and enter the password.

 NOTE

The preset password is **000001**. For access security, change the password after the first login.

4. Press , select **Communication card**.
5. Press  to enter the IP address setting.
6. Press , set the value size by  and .
7. Press  and move the cursor to **Sub mask** and **Default GW**, set **Sub mask** and **Default GW** by using the same as the preceding steps.
8. Press **ESC** to exit.

Step 2 Log in to the UPS2000-G WebUI.

1. On the PC with an IP address in the same network segment as the UPS2000-G, type **https://IP address** of the UPS2000-G in the address box of a browser and press **Enter**.
2. Enter the user name and password for logging in to the UPS2000-G and click **Login**.

 NOTE

The preset user name and password for the UPS2000-G are **admin** and **Changeme**, respectively. To ensure access security, change the password after first login.

3. Set user permissions by referring to [Step 3](#) or [Step 4](#) based on the site requirements.

Step 3 Add a user and set user permissions on the WebUI (WebUI 1).

1. Choose **System Settings > SNMP Settings**.
2. In the **SNMP** area, set **SNMP Version** to **SNMPv3** and **SNMP Port** to **161**, and click **Submit**.
3. In the **SNMPv3** area, click **Add**.
4. In the displayed **SNMPv3** dialog box, set SNMPv3 parameters, and click **Confirm**.
 - You are advised to set **MD5/SHA password** and **DES/AES password** to different values.
 - MD5 is an insecure protocol. SHA is recommended. DES is an insecure protocol. AES is recommended.
 - Record the **User Name**, **MD5/SHA password**, and **DES/AES password** for using when creating a UPS on the NetEco.

Figure 6-59 Setting SNMPv3 parameters

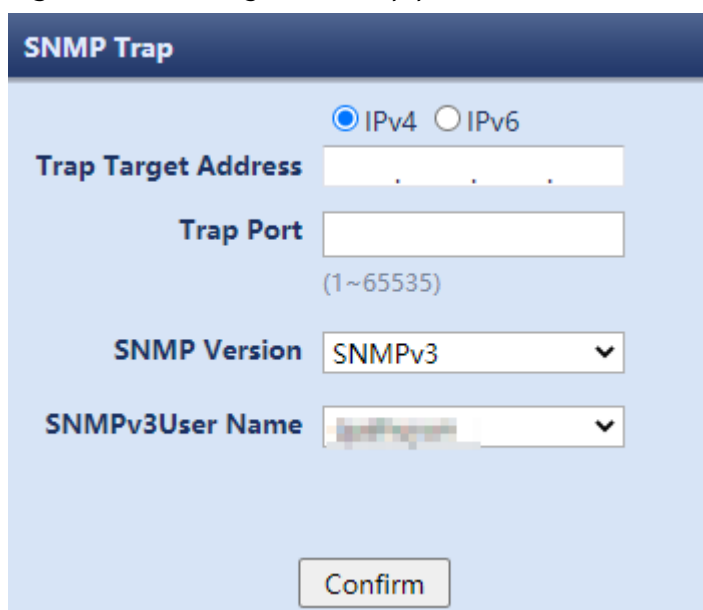


The image shows a web-based configuration dialog box titled "SNMPv3". It contains the following fields and options:

- User Name**: A text input field with a placeholder showing allowed characters: 'a~z', 'A~Z', '0~9', '_', '(1-15characters)
- Authentication Protocol**: A dropdown menu currently set to "SHA2-512".
- MD5/SHA password**: A text input field.
- Confirm MD5/SHA password**: A text input field with a placeholder showing allowed characters: 'a-z', 'A-Z', '0-9', '.', '_' (8-15 characters. A combination of at least two types of characters. Different from the user name or
- Confirm**: A button at the bottom right.

5. In the **SNMP Trap** area, click **Add**.
6. In the displayed **SNMP Trap** dialog box, set SNMP trap parameters, and click **Confirm**.
 - Enter the IP address of the NetEco server in the **Trap Target Address** text box.
 - Set **Trap Port** to **162**.

Figure 6-60 Setting SNMP trap parameters



The image shows a dialog box titled "SNMP Trap". At the top, there are two radio buttons: "IPv4" (selected) and "IPv6". Below this, there are four input fields: "Trap Target Address" (with a dotted line placeholder), "Trap Port" (with a range of 1~65535), "SNMP Version" (a dropdown menu showing "SNMPv3"), and "SNMPv3User Name" (a dropdown menu with a blurred selection). At the bottom right, there is a "Confirm" button.

Step 4 Add a user and set user permissions on the WebUI (WebUI 2).

1. Choose **Configure > SNMP**.
2. Select **SNMPv3** for **SNMP version**, enter **161** for **SNMP port**, and click **Confirm**.

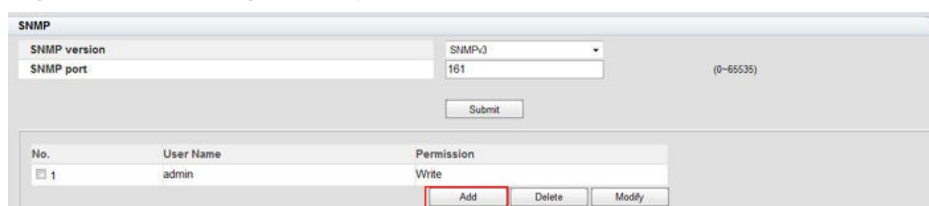
Figure 6-61 Setting SNMP parameters



The image shows a web page titled "SNMP". It has two input fields: "SNMP version" (a dropdown menu showing "SNMPv3") and "SNMP port" (a text box containing "161"). To the right of the "SNMP port" field, there is a range indicator "(0~65535)". Below these fields is a "Submit" button.

3. Click **Add** in **SNMP**.

Figure 6-62 Setting SNMP parameters_02



The image shows the same "SNMP" configuration page as in Figure 6-61, but with an additional table below the "Submit" button. The table has three columns: "No.", "User Name", and "Permission". It contains one row with "1" in the "No." column, "admin" in the "User Name" column, and "Write" in the "Permission" column. Below the table, there are three buttons: "Add", "Delete", and "Modify". The "Add" button is highlighted with a red box.

4. In the displayed **Add SNMPv3 User** dialog box, set related parameters and click **Add**.
 - You are advised to set **MD5/SHA Password** and **DES/AES Password** to different values.
 - MD5 is an insecure protocol. SHA is recommended. DES is an insecure protocol. AES is recommended.
 - For security purposes, you are advised to set **Permission** to **Read**.
 - Record the **User Name**, **MD5/SHA Password**, and **DES/AES Password** for using when creating a UPS2000-G on the NetEco.

Figure 6-63 Setting SNMP parameters_03

Add SNMPv3 User

User Name
Max. 15 characters: a-z, A-Z, 0-9, _

Authentication protocol

MD5/SHA Password

Confirm MD5/SHA Password

Special characters (8–15 characters of at least two types. Different from the user name or its reverse).

Privacy protocol

DES/AES Password

Confirm DES/AES password

Special characters (8–15 characters of at least two types. Different from the user name or its reverse).

Permission

5. Click **Add** in **NMS Address and Permission Settings**.
6. In the displayed **Add NMS Address Info** dialog box, set related parameters and click **Add**.
 - Enter the IP address of the NetEco server in the **NMS addr.** text box.
 - For security purposes, you are advised to set **Permission** to **Read**.

Figure 6-64 Adding the NMS IP address

Add NMS Address Info

NMS addr.

Permission

7. Click **Add** under **SNMP TRAP**.
8. In the displayed **Add SNMP Trap** dialog box, set related parameters and click **Add**.
 - Enter the IP address of the NetEco server in the **Trap Address** text box.
 - Set **Trap port** to **162**.

----End

6.4.5.2 Setting UPS5000 Monitoring Parameters (over SNMP)

Before connecting the UPS5000 to the NetEco, set the IP address on the UPS5000, and add a user and set permissions on the UPS5000 WebUI.

Prerequisites

- You have obtained the IP address, subnet mask, and default gateway planned for the UPS5000.
- The UPS5000 is powered on.

Context

- UPS WebUIs may vary slightly depending on the UPS software version. Perform operations based on the actual WebUI.
- The non-encryption algorithm used in UPS5000 poses potential risks. Therefore, exercise caution when deciding to use the non-encryption algorithm.

Procedure

Step 1 Set the IP address for the UPS5000 on the LUI.

1. Choose **System Info > Settings > Comm Settings > IP Settings**.

NOTE

The preset password is **000001**.

2. Set **IP address assign** to **Manual**, and set **IP address**, **Subnet mask**, **Gateway**, **IPv6 Address**, and so on.

Step 2 Access the UPS5000 WebUI.

1. On the PC with an IP address in the same network segment as the UPS5000, type the UPS5000 IP address in the address box of a browser and press **Enter**. The UPS5000 IP address is set in [Step 1](#).
2. Enter the user name and password for logging in to the UPS5000 and click **Login**.

NOTE

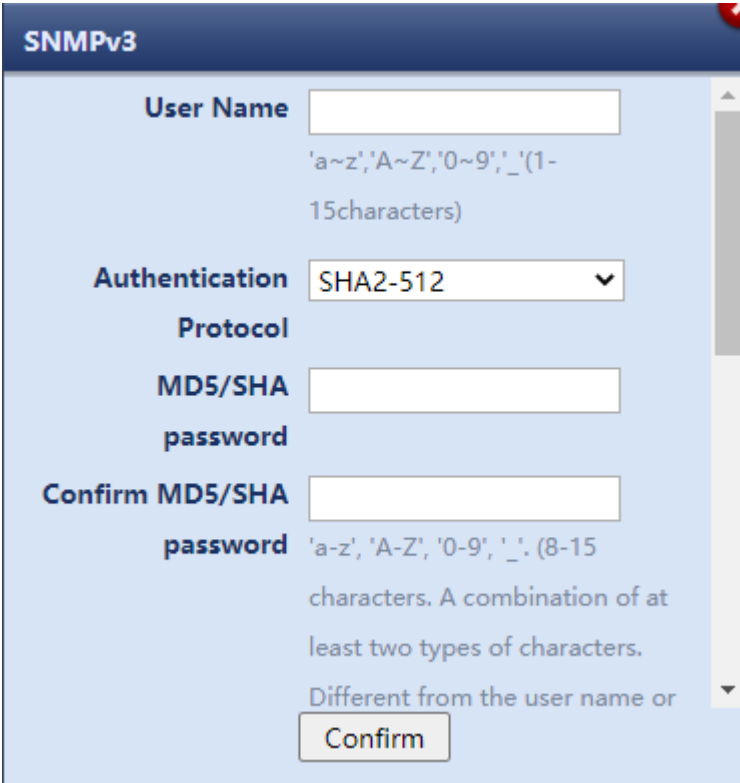
The preset user name and password are **admin** and **Changeme** respectively for the UPS5000.

3. Set user permissions by referring to [Step 3](#) or [Step 4](#) based on the site requirements.

Step 3 Add a user and set user permissions on the WebUI (WebUI 1).

1. Choose **System Settings > SNMP Settings**.
2. In the **SNMP** area, set **SNMP Version** to **SNMPv3** and **SNMP Port** to **161**, and click **Submit**.
3. In the **SNMPv3** area, click **Add**.
4. In the displayed **SNMPv3** dialog box, set SNMPv3 parameters, and click **Confirm**.
 - You are advised to set **MD5/SHA password** and **DES/AES password** to different values.
 - MD5 is an insecure protocol. SHA is recommended. DES is an insecure protocol. AES is recommended.
 - Record the **User Name**, **MD5/SHA password**, and **DES/AES password** for using when creating a UPS on the NetEco.

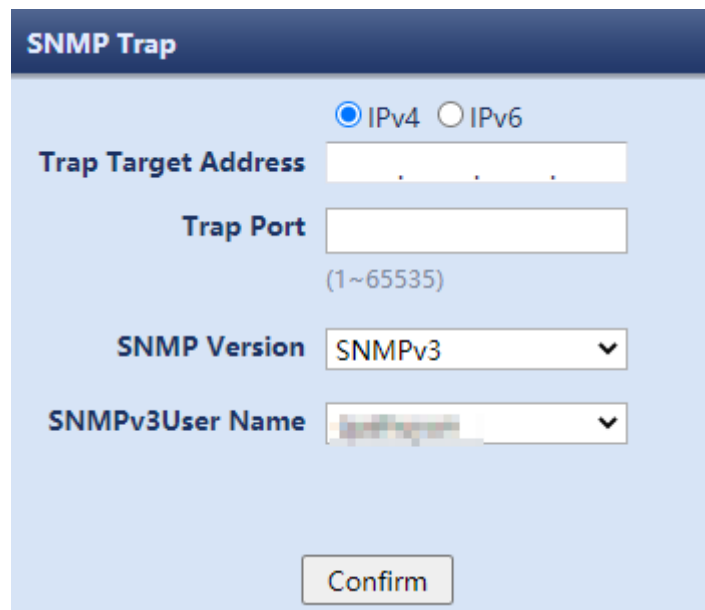
Figure 6-65 Setting SNMPv3 parameters



The image shows a web-based configuration dialog box titled "SNMPv3". It contains several input fields and a dropdown menu. The "User Name" field has a hint: "'a~z','A~Z','0~9','_' (1-15 characters)". The "Authentication Protocol" dropdown is set to "SHA2-512". Below it are two empty text boxes for "MD5/SHA password" and "Confirm MD5/SHA password". The "Confirm MD5/SHA password" field has a hint: "'a-z', 'A-Z', '0-9', '._' (8-15 characters. A combination of at least two types of characters. Different from the user name or)". At the bottom right is a "Confirm" button.

5. In the **SNMP Trap** area, click **Add**.
6. In the displayed **SNMP Trap** dialog box, set SNMP trap parameters, and click **Confirm**.
 - Enter the IP address of the NetEco server in the **Trap Target Address** text box.
 - Set **Trap Port** to **162**.

Figure 6-66 Setting SNMP trap parameters



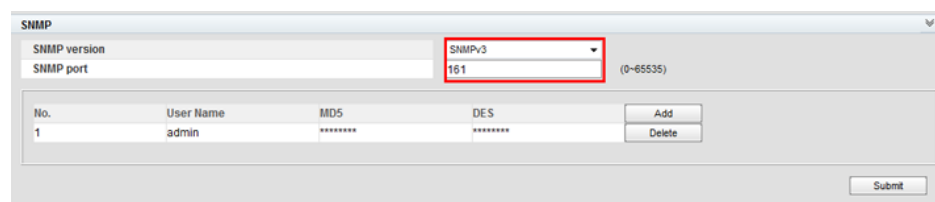
The figure shows a web interface titled "SNMP Trap". It contains the following fields and controls:

- Protocol selection: ☒ IPv4 and ☐ IPv6.
- Trap Target Address: A text input field with a dotted pattern.
- Trap Port: A text input field with a range indicator "(1~65535)".
- SNMP Version: A dropdown menu currently showing "SNMPv3".
- SNMPv3User Name: A dropdown menu showing a masked name.
- A "Confirm" button at the bottom.

Step 4 Add a user and set user permissions on the WebUI (WebUI 2).

1. Choose **Config. > Site Config.**.
2. In the **SNMP** area, set **SNMP version** to **SNMPv3**, and set **SNMP port** to **161**.

Figure 6-67 Setting SNMP parameters

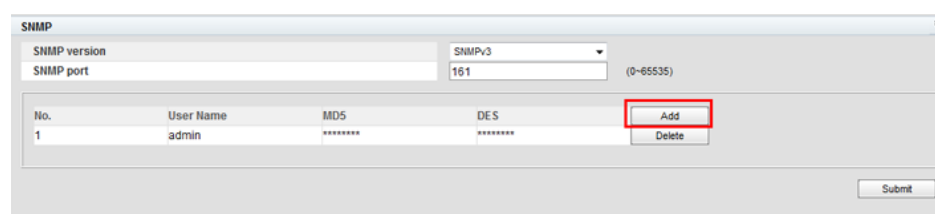


The figure shows a web interface titled "SNMP". It contains the following fields and controls:

- SNMP version: A dropdown menu currently showing "SNMPv3".
- SNMP port: A text input field with the value "161" and a range indicator "(0-65535)".
- A table with columns: No., User Name, MD5, and DES. The first row shows "1", "admin", and two masked password fields.
- Buttons: "Add", "Delete", and "Submit".

3. Click **Add** in **SNMP**.

Figure 6-68 Setting SNMP parameters_02



The figure shows the same "SNMP" configuration interface as Figure 6-67, but with the "Add" button highlighted by a red rectangle.

4. Set **User name**, **MD5/SHA Password**, and **DES/AES Password** for the user to be added.
 - You are advised to set **MD5/SHA password** and **DES/AES password** to different values.

- MD5 is an insecure protocol. SHA is recommended. DES is an insecure protocol. AES is recommended.
 - Record the **User Name**, **MD5/SHA password**, and **DES/AES password** for using when creating a UPS5000 on the NetEco.
5. After setting the SNMP information, click **Submit**.
 6. Click **Add** in **SNMP Trap**.

Figure 6-69 Setting SNMP parameters_03

The screenshot displays the 'UPS Power Manager' web interface. The top navigation bar includes 'Monitoring', 'Query', 'Config.', and 'Maint.'. The 'Config.' tab is active, showing 'User Mgmt.' and 'Site Config.' sub-tabs. The 'Site Config.' section is expanded, revealing several configuration areas:

- System Date and Time:** Includes fields for Date (Local), Time (Local), and Time zone. A 'Synchronize with NTP servers' checkbox is present.
- System Information:** Includes fields for Name, Location, and Contact information.
- SNMP:** Includes a dropdown for 'SNMP version' (set to SNMPv3) and a text field for 'SNMP port' (set to 161).
- SNMP Trap:** Contains a table with columns 'No.', 'Trap addr.', and 'Trap port'. The first row shows '1', 'XXX.XXX.XXX.XXX', and '162'. An 'Add' button is highlighted with a red box next to the 'Trap port' field.
- Certificate Management:** Includes an 'Upload' button and a 'Send' button.

7. Set **Trap Address** to the IP address of the NetEco server, and set **Trap Port** to **162**.

Step 5 (Optional) If an iBOX is configured for the UPS5000, verify that the UPS5000 and iBOX communications addresses are unique.

1. Log in to the UPS5000 WebUI.
2. Choose **System Settings > Comm. Settings > RS485 Settings** or choose **Monitoring > Comm. Config. > RS485 Settings** and verify that **Address** is set to **1** for the UPS5000.
3. Choose **System Settings > iBOX Settings > Basic Parameters** or choose **Monitoring > iBOX Param. > Basic Param.** and verify that **iBOX logical start addr** is set to **2** for the UPS5000.

----End

6.4.5.3 Setting UPS5000 Monitoring Parameters (Modbus TCP)

Before connecting the UPS5000 to the NetEco, set monitoring parameters such as the IP address on the UPS5000.

Prerequisites

- You have obtained the IP address, subnet mask, and default gateway planned for the UPS5000.
- UPS WebUIs may vary slightly depending on the UPS software version. Perform operations based on the actual WebUI.
- The UPS5000 is powered on.

Context

Before connecting the UPS5000 to the NetEco, set monitoring parameters such as the IP address on the UPS5000.

Procedure

Step 1 Set the IP address for the UPS5000 on the LUI.

1. Choose **System Info > Settings > Comm Settings > IP Settings**.

 NOTE

The preset password is **000001**.

2. Set **IP address assign** to **Manual**, and set **IP address**, **Subnet mask**, **Gateway**, **IPv6 Address**, and so on.

Step 2 Connect a network management system over SSL or non-SSL as follows:

1. On the PC with an IP address in the same network segment as the UPS5000, type the UPS5000 IP address in the address box of a browser and press **Enter**. The UPS5000 IP address is set in [Step 1](#). Log in to the UPS5000 WebUI.
2. Enter the user name and password for logging in to the UPS5000 and click **Login**.

 NOTE

The preset user name and password are **admin** and **Changeme** respectively for the UPS5000.

3. Set UPS5000 parameters.

 NOTE

- Set parameters on the WebUI based on the actual situation. For details, see "Operation (UPS5000 WebUI 1)" or "Operation (UPS5000 WebUI 2)" in the following table.
- A non-SSL connection has security risks. You are advised to select the secure SSL connection.

Table 6-27 UPS5000 settings

Connec tion Mode (NetEco UI)	Operation (UPS5000 WebUI 1)	Operation (UPS5000 WebUI 2)
SSL connection	1. Choose System Settings > Comm Settings. The Comm Settings page is displayed. 2. In the ModbusTCP Settings area, set ModbusTCP Encryption to Enable. 3. Click Submit. 4. Choose System Settings > ModbusTCP. 5. In the Set Authentication Password area, set Pre-shared Password and Confirm Pre-shared Password. 6. Click Submit. Record the value of Pre-shared Password in Authentication Password of the added device on the NetEco.	1. Choose Monitoring > Comm Settings. The Comm Settings page is displayed. 2. In the ModbusTCP Settings area, set ModbusTCP Encryption to Enable. 3. Click Submit. 4. Choose Config. > Site Config. > ModbusTCP Authentication. 5. Set Authentication to Enable, and set New password and Confirm password. 6. Click Submit. Record the value of Confirm Password in Authentication Password of the added device on the NetEco.
Non-SSL connection	1. Choose System Settings > Comm Settings. The Comm Settings page is displayed. 2. In the ModbusTCP Settings area, set ModbusTCP Encryption to Disable. 3. Click Submit.	1. Choose Monitoring > Comm Settings. The Comm Settings page is displayed. 2. Set ModbusTCP Encryption to Disable. 3. Click Submit.

Step 3 (Optional) If an iBOX is configured for the UPS5000, verify that the UPS5000 and iBOX communications addresses are unique.

1. Log in to the UPS5000 WebUI.
2. Choose **System Settings > Comm. Settings > RS485 Settings** or choose **Monitoring > Comm. Config. > RS485 Settings** and verify that **Address** is set to **1** for the UPS5000.
3. Choose **System Settings > iBOX Settings > Basic Parameters** or choose **Monitoring > iBOX Param. > Basic Param.** and verify that **iBOX logical start addr** is set to **2** for the UPS5000.

----End

6.4.5.4 Creating a UPS on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 2** Select the management domain to add a device.
- Step 3** In the lower-left corner of the page, click the **Device** tab.
- Step 4** Click the drop-down list box in **Type** and select **UPS**.
- Step 5** Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

- Step 6** Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-28 Modbus-TCP device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set the IP address of the device.
Port	Set this parameter to the port through which the device connects to the collector. The port number is 502 by default. You can modify the port number based on requirements.
Device Address	Set this parameter to the address set on the device.
Timeout period	Timeout duration for a connection test. The default value is 3s .

Parameter	Description
Connection Mode	Indicates the connection mode of a device. You can set this parameter to Non-SSL Connection or SSL Connection. If you modify the connection mode on the NetEco, you must modify the connection mode on the device WebUI accordingly. NOTE • Connection Mode for the NetEco and device must be the same. • By default, Connection Mode is set to SSL Connection for the NetEco and device. • A non-SSL connection has security risks. You are advised to select the secure SSL connection.
Authentication password	Indicates the re-authentication password for the NetEco and device. 1. Click Modify. NOTE After the device is saved, the Modify button is displayed. 2. In the displayed dialog box, enter the New Password and Confirm Password. NOTE – The default re-authentication password for the NetEco and device is Modifyme_123. – The device password should be consistent with the NetEco password. – If the password does not meet requirements, modify it on the device. 3. Select a value for Send To Device. NOTE If you select YES, the re-authentication password for the NetEco and device is changed at the same time. If you select NO, only the re-authentication password of NetEco is changed on the server. 4. Click OK.

Table 6-29 SNMPv1/v2 device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the device IP address.
Port	Set this parameter to the port number of the device. (set to 161 by default)

Parameter	Description
Read Community	Set this parameter to the read community set on the device. It is recommended that the community be modified every three months.
Write Community	Set this parameter to the write community set on the device. Modifying community per three months is advised.
Timeout period	Timeout duration for a connection test. The default value is 3s .

Table 6-30 SNMP v3 device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the device IP address.
Port	Set this parameter to the port number of the device. (set to 161 by default)
Security Name	Set this parameter to the user name added in SNMPv3 on the WebUI of the device.
Authentication Protocol	Set this parameter to the authentication protocol set on the device. The default selection is SHA . Support SHA and MD5 agreement. NOTE MD5 is an insecure protocol. SHA is recommended.
Authentication Password	Set this parameter to the SHA or MD5 password set on the device.
Privacy Protocol	Set this parameter to the privacy protocol set on the device. The default selection is AES128 . Support CBC_DES , AES128 , AES192 , and AES256 agreement.
Privacy Password	Set this parameter to the AES or DES password set on the device. NOTE - You are advised to set Authentication Password and Privacy Password to different values. - DES is an insecure protocol. AES is recommended.
Timeout period	Timeout duration for a connection test. The default value is 3s .

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

 NOTE

For UPS, if a battery monitor unit (BMU) is connected, the BMU will be automatically created.

----End

6.4.6 Adding a PDU

6.4.6.1 Setting PDU8000 Monitoring Parameters (SNMP)

Prerequisites

- You have obtained the IP address, subnet mask, and default gateway planned for the PDU8000.
- The PDU8000 is powered on.

Context

- Before connecting the PDU8000 to the NetEco over SNMP, set monitoring parameters, such as the IP address, subnet mask, and gateway, on the PDU8000.
- The menus on the LCD vary with the PDU8000 version.

Procedure

Step 1 Tap **Settings** on the PDU8000 home screen.

Step 2 Enter the PDU8000 user name and password and tap .

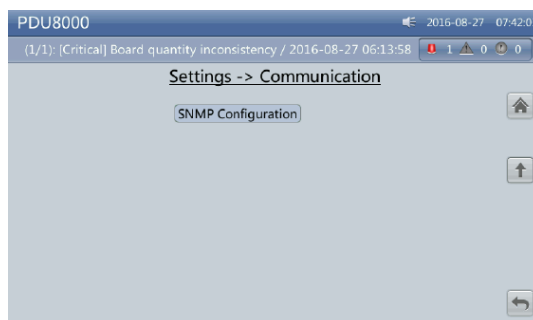
 NOTE

The preset user name and password for the PDU8000 are **admin** and **000001** respectively. To ensure access security, change the password upon the first login.

Step 3 Tap **Communication**.

1. Check that **IP address assign** is set to **Manual**.
2. Set **IP address**, **Subnet mask**, and **Gateway** as planned.
3. Tap **SNMP Configuration** to enter the setting screen.

Figure 6-70 SNMP Configuration



4. On the **SNMP Configuration** screen, set **SNMP Version** to **SNMPv3**, retain the default value **161** for **SNMP Port**, and tap **Submit**.
 5. Tap **Add** under **SNMPv3 User**. Set **User Name**. Set **Auth. protocol** to **SHA**, and specify **MD5/SHA** and **Confirm Password**. Set **Private protocol** to **AES**, and specify **DES/AES** and **Confirm Password**. After setting the parameters, tap .
 6. Select **Privacy protocol** to **AES**, specify **DES/AES** and **Confirm Password**, and tap .
 7. On the **Trap Config.** screen, tap **Add**, set **Trap Des. Address** to the IP address of the NetEco server and set **Trap Port** to **162**. Select **SNMP Version** to **SNMPv3**. After setting the parameters, tap .
- End

6.4.6.2 Setting PDU8000 Monitoring Parameters (Modbus TCP)

Prerequisites

- You have obtained the IP address, subnet mask, and default gateway planned for the PDU8000.
- The PDU8000 is powered on.

Context

Before connecting the PDU8000 to the NetEco, set monitoring parameters such as the IP address on the PDU8000.

Procedure

Step 1 Tap **Settings** on the PDU8000 home screen.

Step 2 Enter the PDU8000 user name and password and tap .

NOTE

The preset user name and password for the PDU8000 are **admin** and **000001** respectively. To ensure access security, change the password upon the first login.

Step 3 Choose **Communication**.

1. Set **IP address assign** to **Manual**, and set **IP address**, **Subnet mask**, and **Gateway**.
2. Set **SSL** to **Enable** and **ModbusTCPcertification** to **Enable**.

----End

6.4.6.3 Creating a PDU on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 2** Select the management domain to add a device.
- Step 3** In the lower-left corner of the page, click the **Device** tab.
- Step 4** Click the drop-down list box in **Type** and select **PDU**.
- Step 5** Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

- Step 6** Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-31 Modbus TCP device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Device IP address
Port	Device port number The default port number is 502 . You can change the port number as required.
Device Address	Address set on the device
Timeout period	Timeout duration for a connection test. The default value is 3s .
Connection Mode	Connection mode of the device. Select SSL connection .

Table 6-32 SNMPv3 device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Device IP address
Port	Set this parameter to the port number of the device. (set to 161 by default)
Security Name	Set this parameter to the user name added in SNMPv3 on the device.
Authentication Protocol	Set this parameter to the authentication protocol set on the device. The default selection is SHA . Support SHA and MD5 agreement. NOTE MD5 is an insecure protocol. SHA is recommended.
Authentication Password	Set this parameter to the SHA or MD5 password set on the device.
Privacy Protocol	Set this parameter to the proprietary algorithm set on the device. The default selection is AES128 . CBC_DES , AES128 , AES192 , and AES256 are supported.
Privacy Password	Set this parameter to the password set for AES or DES on the device. NOTE - You are advised to set Authentication Password and Privacy Password to different values. - DES is an insecure protocol. AES is recommended.
Timeout period	Timeout duration for a connection test. The default value is 3s .

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.4.7 Adding an MTS9604B-N20B1 Power Supply

6.4.7.1 Creating a MTS9604B-N20B1 Power Supply on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.

- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The mediation of the MTS9604B-N20B1 power supply has been installed.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 2** Select the management domain to add a device.
- Step 3** In the lower-left corner of the page, click the **Device** tab.
- Step 4** Click the drop-down list box in **Type** and select **PDU**.
- Step 5** Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

- Step 6** Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-33 SNMPv3 device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Device IP address
Port	Set this parameter to the port number of the device. (set to 161 by default)
Security Name	Set this parameter to the user name added in SNMPv3 on the WebUI of the device.
Authentication Protocol	Set this parameter to the authentication protocol configured on the device. The default value is SHA . The SHA and MD5 protocols are supported. NOTE MD5 is an insecure protocol. SHA is recommended.
Authentication Password	Set this parameter to the password set for SHA or MD5 on the device.
Privacy Protocol	Set this parameter to the proprietary algorithm set on the device. The default selection is AES128 . CBC_DES , AES128 , AES192 , and AES256 are supported.

Parameter	Description
Privacy Password	Set this parameter to the password set for AES or DES on the device. NOTE - You are advised to set Authentication Password and Privacy Password to different values. - DES is an insecure protocol. AES is recommended.

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.4.8 Adding a SmartLi

6.4.8.1 Setting SmartLi Monitoring Parameters (Modbus TCP)

Before connecting the SmartLi to the NetEco, set monitoring parameters such as the IP address on the SmartLi.

Prerequisites

- You have obtained the IP address, subnet mask, and default gateway planned for the SmartLi.
- The SmartLi is powered on.

Context

SmartLi model: SmartLi-512V-80AH-F-01

Procedure

Step 1 On the SmartLi LCD home screen, tap **Settings**.

Step 2 Enter the SmartLi password.

 **NOTE**

The preset password is **000001**.

Step 3 Choose **Communication**.

- Set **IP address assign** to **Manual**, and set **IP address**, **Subnet mask**, and **Gateway**.
- Set **ModbusTCP encryption** to **Enable**.

 **NOTE**

If Modbus TCP encryption is disabled on the device, SSL connection must be disabled on the NetEco.

----End

6.4.8.2 Creating a SmartLi on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The SmartLi adapter has been installed on the NetEco.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 2** Select the management domain to add a device.
- Step 3** In the lower-left corner of the page, click the **Device** tab.
- Step 4** Click the drop-down list box in **Type** and select **Battery**.
- Step 5** Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

- Step 6** Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-34 SmartLi parameter description

Parameter	Description
Managed Object Name	Device name
IP	Device IP address
Port	Set this parameter to the port number of the device. (set to 502 by default)
Device Address	Set this parameter to the address set on the device.
Timeout period	Timeout duration for a connection test. The default value is 3s .

Parameter	Description
Connection Mode	Connection mode of the device. You can set this parameter to Non-SSL Connection or SSL Connection. If you modify the connection mode on the NetEco, you must modify the connection mode on the device WebUI accordingly. NOTE • The connection mode settings for the NetEco and device must be the same. • By default, Connection Mode is set to SSL Connection for the NetEco and device. • A non-SSL connection has security risks. You are advised to select the secure SSL connection.
Authentication password	Re-authentication password for the NetEco and device. The default value is Modifyme_123 .

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.4.9 Adding a CO Power Module

6.4.9.1 Setting Monitoring Parameters for the TP483000D and TP482000B

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

Step 2 Set the IP type, IP address, subnet mask, and gateway on the SMU's LCD.

Table 6-35 IP parameters

Main Menu	Second-Level Menu	Third-Level Menu	Default Value	Settings
Setting Wizard	Network Parameters	IP Type	IPv4	Set as required.
		IP Address	192.168.0.10	Set this parameter according to the IP address assigned by the network administrator.
		Subnet Mask	255.255.255.0	Set this parameter according to the subnet mask provided by the network administrator.

Main Menu	Second-Level Menu	Third-Level Menu	Default Value	Settings
		Default Gateway	192.168.0.1	Set this parameter according to the gateway address provided by the network administrator.

Step 3 Set the **IP Addresses** and **Ports** for the active servers of the NetEco on the SMU's LCD.

Table 6-36 NetEco parameters

Main Menu	Second-Level Menu	Third-Level Menu	Fourth-Level Menu	Default Value	Settings
Parameters Settings	Comm. Parameters	Network Parameters	NetEco Primary IP	192.168.0.10	Set an IP address for the active NetEco server.
			NetEco Backup IP	192.168.0.10	Set an IP address for the standby NetEco server.
			NetEco Port Number	31220	Set a port for the NetEco.

----End

6.4.9.2 Creating a Power Module on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 2** Select the management domain to add a device.
- Step 3** In the lower-left corner of the page, click the **Device** tab.
- Step 4** Click the drop-down list box in **Type** and select **PDU**.
- Step 5** Select the device to be added and drag its icon to the management domain.

 NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-37 SNMPv3 device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the device IP address.
Port	Set this parameter to the port number of the device. (set to 161 by default)
Security Name	Set this parameter to the user name added in SNMPv3 on the WebUI of the device.
Authentication Protocol	Set this parameter to the authentication protocol set on the device. The default selection is SHA . Support SHA and MD5 agreement. NOTE MD5 is an insecure protocol. SHA is recommended.
Authentication Password	Set this parameter to the SHA or MD5 password set on the device.
Privacy Protocol	Set this parameter to the privacy protocol set on the device. The default selection is AES128 . Support CBC_DES , AES128 , AES192 , and AES256 agreement.
Privacy Password	Set this parameter to the AES or DES password set on the device. NOTE - You are advised to set Authentication Password and Privacy Password to different values. - DES is an insecure protocol. AES is recommended.

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.4.10 Adding an rPDU

6.4.10.1 Setting RPDU_HUAWEI_PDU2000-32-1PH-20-4-M2 Monitoring Parameters

Prerequisites

- You have obtained the IP address (factory default: 192.168.1.45) of the PDU2000.
- You have installed the hardware and powered on the PDU2000.
- A PC with an IP address in the same network segment as that of the PDU2000 is prepared, and the PC has connected to the PDU2000 over a switch.
- You have obtained the planned IP address and subnet mask of the PDU2000.

Context

Set the PDU2000 IP address before you connect the PDU2000 to the NetEco.

Procedure

- Step 1** Use a PC with an IP address in the same network segment as that of the PDU2000. Enter `https://192.168.1.45` in the address bar, and press **Enter** on the keyboard.
- Step 2** Enter monitoring parameters of the PDU2000. For the input method, see [Table 6-38](#). For parameters not mentioned in the table, retain the default value.

Table 6-38 Remarks

Parameter	Setting Method
IP address	Enter the planned PDU2000 IP address.
Subnet mask	Enter the planned PDU2000 subnet mask.
Gateway	Enter the planned PDU2000 gateway.
Address reporting the SNMP	Enter the IP address of the NetEco the PDU2000 connects to.

----End

6.4.10.2 Creating an rPDU on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **PDU**.

Step 5 Select the device to be added and drag its icon to the management domain.

NOTE

- If the management domain is a rack or DDF, click the management domain and choose **Design** under . The page for adding a device is displayed.
- To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-39 SNMPv1/v2 device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the device IP address.
Port	Set this parameter to the port number of the device. (set to 161 by default)
Read Community	Set this parameter to the read community set on the device. Modifying community per three months is advised.
Write Community	Set this parameter to the write community set on the device. Modifying community per three months is advised.
Timeout period	Timeout duration for a connection test. The default value is 3s .

NOTE

SNMPv1 and SNMPv2 are insecure. SNMPv3 is recommended because it is more secure.

Table 6-40 SNMPv3 device parameter description

Parameter	Description
Managed Object Name	Device name

Parameter	Description
IP	Set this parameter to the device IP address.
Port	Set this parameter to the port number of the device. (set to 161 by default)
Security Name	Set this parameter to the user name added in SNMPv3 on the WebUI of the device.
Authentication Protocol	Set this parameter to the authentication protocol set on the device. The default selection is SHA . Support SHA and MD5 agreement. NOTE MD5 is an insecure protocol. SHA is recommended.
Authentication Password	Set this parameter to the SHA or MD5 password set on the device.
Privacy Protocol	Set this parameter to the privacy protocol set on the device. The default selection is AES128 . CBC_DES , AES128 , AES192 , and AES256 are supported.
Privacy Password	Set this parameter to the AES or DES password set on the device. NOTE - You are advised to set Authentication Password and Privacy Password to different values. - DES is an insecure protocol. AES is recommended.
Timeout period	Timeout duration for a connection test. The default value is 3s .

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.5 Scenarios for Connecting the ECC800-Pro Outside the Smart Module

6.5.1 Setting and Adding the ECC800-Pro Collector

6.5.1.1 Preparations and Login

Prerequisites

- Supported operating system: Windows 7 and later versions
- It is recommended that the screen resolution be 1366 x 768 or higher.
- Browser: Chrome, Firefox 32, Internet Explorer 11 or later

Procedure

- Step 1** Connect a network cable between the PC network port and the WAN1 port (protected by a security mechanism) on the ECC800-Pro.

Table 6-41 Default IP addresses for the WAN and LAN ports on the ECC800-Pro

Port	Default IP Address
WAN1	192.168.8.10
WAN2	192.168.0.10 192.168.248.10 (FusionModule500/800)
LAN1 and LAN2	192.168.248.10

NOTICE

- In ECC800 V100R002C10 and earlier versions, the default IP address of port WAN_1 is 192.168.1.10.
- The WAN1 port IP address cannot be set to an IP address in any of the following network segments: 192.168.0.x, 192.168.245.x, 192.168.246.x and 192.168.248.x.
- IP addresses for the WAN1 and WAN2 ports should not be set in the same network segment.
- In some customized scenarios, the default IP address for the WAN2 port is 192.168.248.10. The default value may vary.
- WAN ports support the Internet access and LAN ports support the intranet access. Connect the PC network port to the WAN1 port or LAN port on the ECC800-Pro based on the access network.

- Step 2** Configure the PC IP address and the WAN1 IP address in the same network segment.

If the WAN1 port IP address is 192.168.8.10, subnet mask is 255.255.255.0, and default gateway is 192.168.8.1, set the PC IP address to 192.168.8.12, subnet mask to 255.255.255.0, and default gateway to 192.168.8.1.

- Step 3** Set LAN parameters.

 NOTE

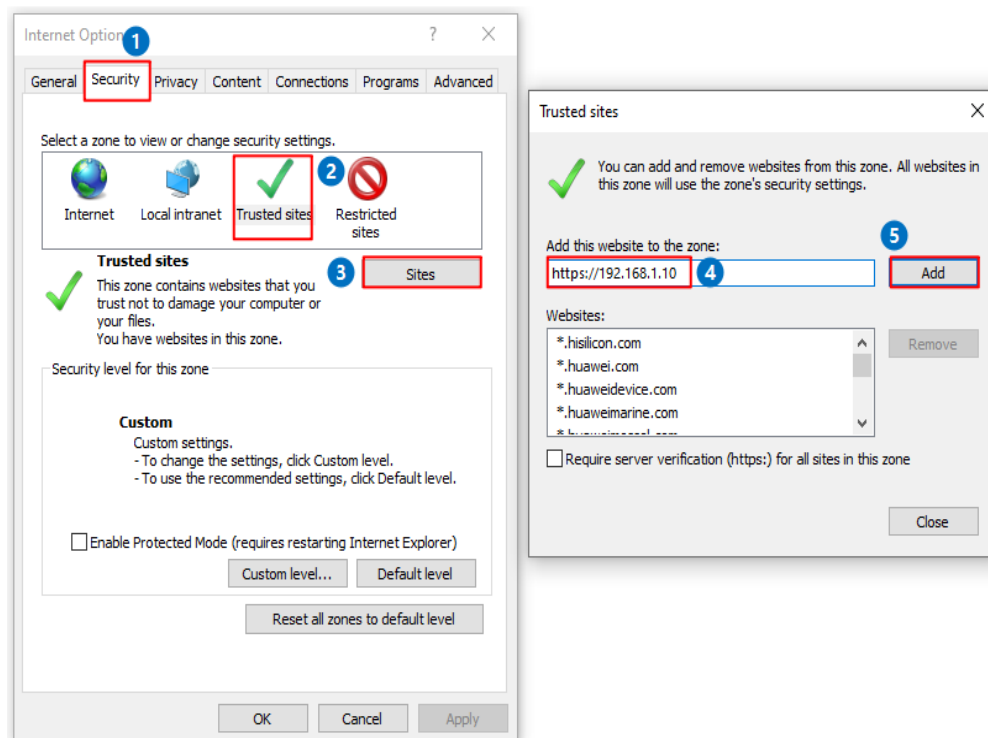
- If the ECC800-Pro connects to a LAN and a proxy server has been selected, perform [Step 3.3](#) and [Step 3.4](#).
- If the ECC800-Pro connects to the Internet, and the PC in a LAN accesses the Internet over a proxy server, do not perform [Step 3.3](#) and [Step 3.4](#). Otherwise, you will fail to access the ECC800-Pro.

1. Open the Internet Explorer and choose **Tools > Internet Options**.
2. Click the **Advanced** tab and select **Use TLS1.1** and **Use TLS1.2**.
3. (Optional) Click the **Connections** tab and select **LAN settings**.
4. (Optional) On **Proxy server**, clear **Use a proxy server for your LAN**.
5. Click **OK**.

Step 4 Set Internet Explorer parameters.

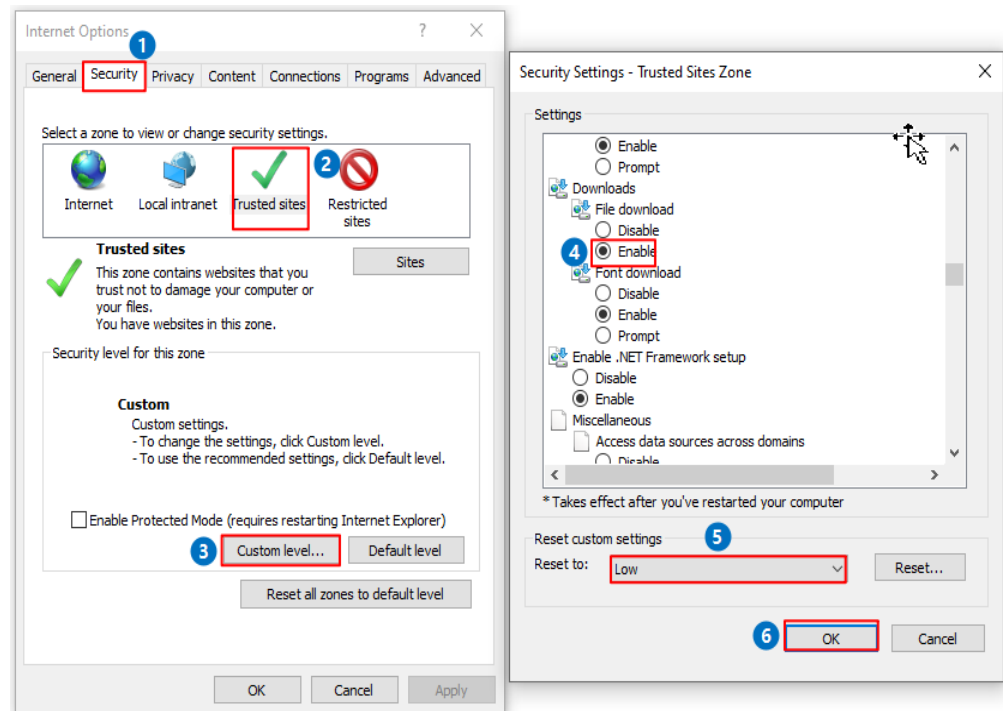
1. When you use Internet Explorer for access, set Internet Explorer to ensure the normal display of and operations on the WebUI. Choose **Tools > Compatibility View**, and add the web access address to the compatibility view.
2. Choose **Tools > Internet options > Security**, choose **Add the ECC800-Pro IP address** to the list of trusted sites.

Figure 6-71 Adding an address



3. Enable file download and set the security level of the trusted site to low.

Figure 6-72 Setting parameters



NOTE

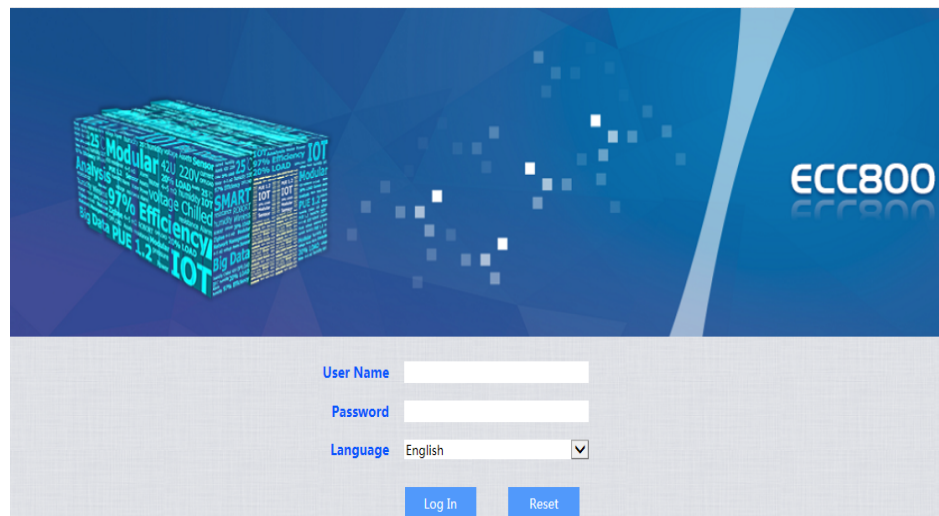
When switching between different versions of the ECC800-Pro on your PC, you are advised to clear the historical Internet Explorer cache. Failing to do so may cause some information missed or exception after login. The following provides the details:

1. Open Internet Explorer and choose **Tools > Internet Options > General**.
2. Select **Delete browsing history on exit** and click **Delete**.
3. In the **Delete Browsing History** dialog box, select all options except **Password**, and click **Delete**.

Step 5 Log in to the ECC800-Pro WebUI.

1. Enter **https://monitoring IP address** (such as monitoring IP address **https://192.168.8.10**) in the address box of the browser, and then press **Enter** to enter the WebUI login page.

Figure 6-73 WebUI login page



2. On the login page, enter the preset user name **admin** and preset password **Changeme**, set the language, and click **Log In**.

 NOTE

- After the first login, change the password in time to ensure account security and prevent unauthorized network attacks, such as data tampering. The Company will not be liable for any security issues caused by your failure to change the preset password in time or password loss after changing.
- Change the password of the user account periodically.
- Record and keep the password properly. If you forgot the password, you will be unable to log in to the WebUI.
- When the event notification is configured and the password retrieval mode is configured under user management, the password can be retrieved.
- An account is logged out due to timeout if no operation is performed within 10 minutes after system login.
- A maximum of three users can log in to the ECC800-Pro WebUI at the same time.

----End

6.5.1.2 Setting the ECC800-Pro IP Address

Before connecting the ECC800-Pro to the NetEco, configure the IP address, subnet mask, and default gateway for the ECC800-Pro.

Prerequisites

- You have obtained the IP address (192.168.8.10 by default) of the ECC800-Pro.
- The browser (Internet Explorer 11 or later, Firefox, or Chrome) for logging in to the ECC800-Pro WebUI is available.
- You have installed hardware for the ECC800-Pro and powered it on.
- A PC with an IP address in the same network segment as that of the ECC800-Pro is connected to the ECC800-Pro over a LAN switch.
- You have obtained the IP address, subnet mask, and default gateway planned for the ECC800-Pro.

Context

A unified IP address (192.168.8.10) is configured for all ECC800-Pros before delivery. Reconfigure an IP address for the ECC800-Pro as required to ensure normal communication with a server.

Procedure

- Step 1** Log in to the ECC800-Pro WebUI as an administrator.
- Step 2** Choose **System Settings** > **System Parameters** > **Monitor IP**, and change the IP address, subnet mask, and default gateway of the ECC800-Pro based on the parameters planned for the ECC800-Pro collector, as shown in [Figure 6-74](#).

Figure 6-74 Changing the ECC800-Pro IP address

The screenshot shows the 'Monitor IP' configuration page in the ECC800-Pro WebUI. The left sidebar contains a menu with 'System Parameters' selected. The main content area has tabs for 'Site Configuration', 'Monitor IP', and 'Time'. Under 'Monitor IP', there are two sections: 'WAN_1' and 'WAN_2'. Each section contains fields for IP, Subnet mask, and Default gateway. Below these fields is a note and a 'Submit' button.

WAN_1	
IP	192.168.8.10
Subnet mask	255.255.254.0
Default gateway	192.168.8.10
Note: The WAN_1 port IP address cannot be set to an IP address in any of the following	
DNS Server Address	
Primary DNS server	192.168.8.10
Secondary DNS server	192.168.8.10
Submit	

WAN_2	
IP	192.168.0.10
Subnet mask	255.255.255.0
Default gateway	192.168.0.1
Note: The WAN_2 port IP address cannot be set to an IP address in any of the following	
Submit	

- Step 3** Click **Submit**.

----End

6.5.1.3 Setting the ECC800-Pro System Type

Prerequisites

- You have obtained the IP address (192.168.8.10 by default) of the ECC800-Pro.
- The browser (Internet Explorer 11 or later, Firefox, or Chrome) for logging in to the ECC800-Pro WebUI is available.
- You have installed hardware for the ECC800-Pro and powered it on.
- A PC with an IP address in the same network segment as that of the ECC800-Pro is connected to the ECC800-Pro over a LAN switch.
- You have obtained the IP address, subnet mask, and default gateway planned for the ECC800-Pro.

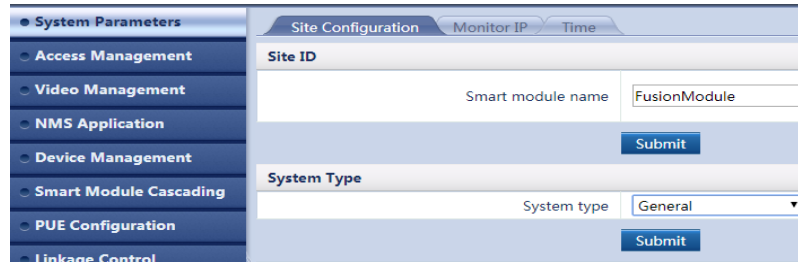
Context

When connecting the ECC800-Pro outside the smart module to the NetEco, you need to set the system type to **General**.

Procedure

- Step 1** Log in to the ECC800-Pro WebUI as an administrator.
- Step 2** Choose **System > System Parameters > Site Configuration**, set **System type** to **General**, and click **Submit**.

Figure 6-75 Setting the system type



----End

6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector

Prerequisites

- You have obtained the IP address and login user name and password for the ECC800-Pro collector.
- A PC with an IP address in the same network segment as the ECC800-Pro collector is prepared, and the PC has been connected to the ECC800-Pro collector over a switch.

Context

To ensure the normal connection between the ECC800-Pro collector and devices, properly set the RS485 parameters for the ECC800-Pro collector, such as **BaudRate**, **DataBit**, **StopBit** and **Parity**. Ensure these parameters stay consistent with those of the devices.

This section describes how to set RS485 port parameters for the COM1 port on the ECC800-Pro.

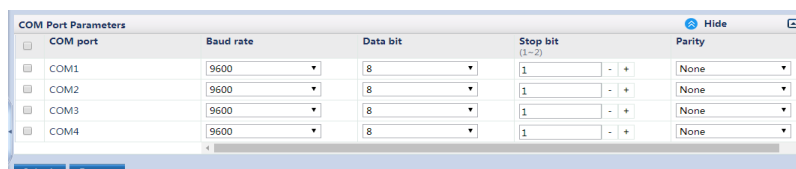
Procedure

- Step 1** Set RS485 port parameters on the WebUI of the ECC800-Pro collector.
- Use a PC, enter `https://XX.XX.XX.XX` in the address bar to log in to the WebUI of the ECC800-Pro collector.

NOTE

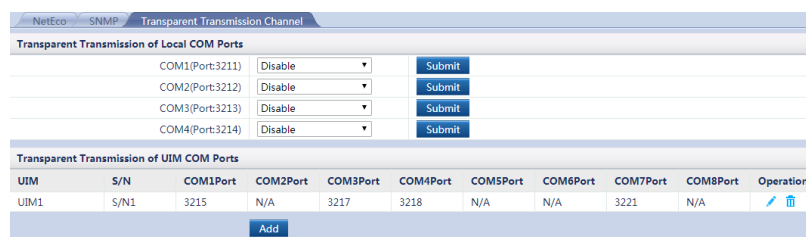
- `XX.XX.XX.XX` indicates the IP address of the collector.
 - To ensure the security of data transmission, the NetEco transmits data after encrypting it over the Secure Sockets Layer (SSL).
- Choose **Monitoring > System > ECC800 > Running Parameters**.
 - Click **Unhide All Advanced Signals**.

- Click **COM Port Parameters**.
- Select a value from the **Baud rate**, **Data bit**, **Stop bit**, and **Parity** drop-down list boxes, and click **Submit**, as shown in [Figure 6-76](#).

Figure 6-76 Setting RS485 port parameters

Step 2 Choose **System > NMS Application > Transparent Transmission Channel** and confirm the corresponding port of the ECC800-Pro collector.

When creating an RS485 device on the NetEco, you need to specify the port number corresponding to the ECC800-Pro RS485 port to which the device is connected.

Figure 6-77 Transparent Transmission Channel**Table 6-42** Mapping between ECC800-Pro ports and port numbers

COM Port	COM1	COM2	COM3	COM4
Port Number	3211	3212	3213	3214

If a device is connected to a COM port on the UIM20A expansion module, the port number is displayed on the WebUI after transparent transmission is enabled for the COM port and the configuration is saved. For example, the port number of COM1 on UIM1 is 3215 in [Figure 6-77](#).

NOTE

- An ECC800-Pro can connect to a maximum of four UIM20A expansion modules with the transparent transmission function.
- A UIM20A expansion module provides a maximum of eight COM ports with the transparent transmission function.
- If the port is set for the first time, you are prompted to set an authentication password. On the **Set Authentication Password** tab page, set **Authentication password** and **Confirm authentication password** and click **Submit**.

 NOTE

Enable Security Authentication is set to **Enable** by default. If so, an authentication password must be set. If **Enable Security Authentication** is set to **Disable**, there is no need to set an authentication password but this is risky.

- If the port has been used, you will be prompted that the transparent transmission function cannot be enabled and you need to select an idle port.

----End

6.5.1.5 Setting NetEco Parameters

Procedure

Step 1 Apply for a fixed IP address to the equipment room network administrator.

Step 2 Set the IP address, subnet mask, and default gateway on the ECC800-Pro WebUI.

Table 6-43 IP parameters

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

Step 3 Click **Submit**.

Step 4 Set NetEco communications parameters and authentication password on the ECC800-Pro WebUI.

Table 6-44 NetEco parameters

Path	Parameter	Default Value	Setting
System Settings > NMS Application > NetEco > Communication Parameters	Server IP	192.168.8.11	IP address of the primary NetEco server NOTE The NetEco IP address and the ECC800-Pro IP address must be configured in the same network to ensure normal connection between the NetEco and the ECC800-Pro.

Path	Parameter	Default Value	Setting
	Port number	31220	31220
	Network port for link setup	WAN_1	WAN_1

Table 6-45 Setting an authentication password

Path	Parameter	Default Value	Setting
System Settings > NMS Application > NetEco > Set Authentication Password	Authentication password	Modify me _123	Set this parameter based on customer requirements. NOTE Requirements for setting passwords: 'a~z','A~Z','0~9','~!@#^*_={}.~/?~` \$(8-32 characters that include at least three of the following types: lowercase letters, uppercase letters, digits, and special characters)
	Confirm authentication password	-	-

Step 5 Click **Submit**.

----End

6.5.1.6 Creating an ECC800-Pro Collector on the NetEco

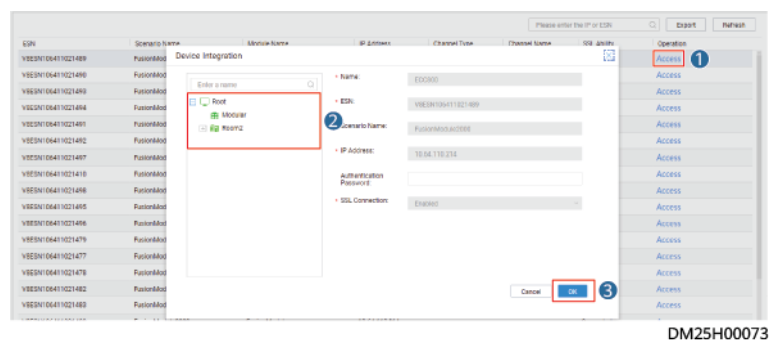
Prerequisites

- You have logged in to the NetEco client using a web browser.
- You have created a modular or container in **Data Center Planning**. For detailed operations, see Creating a Domain.
- The IP address of the NetEco connected has been configured on the ECC800-Pro WebUI.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 2** On the **Data Center Planning** page, create a management domain as required.
- Step 3** Click  in the upper left area of the **Data Center Planning** page.
- Step 4** Click **Access** to switch to the **Add Device** page. You can add an ECC800-Pro device to the specified modular in the **Add Device** page.

Figure 6-78 Adding an ECC800-Pro device to the modular



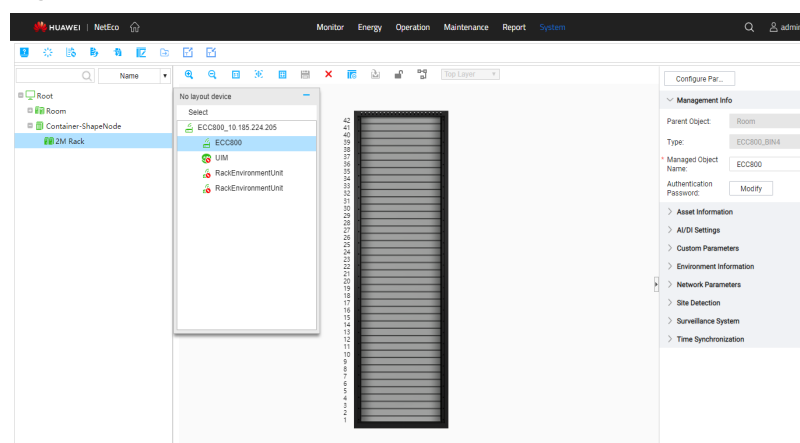
DM25H00073

NOTE

- There is no requirement on the type of management domain for connecting the ECC800-Pro whose system type is **General**.
- The ECC800-Pros whose system type is **General** can be deployed in different management domains. In equipment room scenario, such ECC800-Pros can be deployed on the same floor. In a container scenario, such ECC800-Pros can be deployed in the same container.
- Multiple ECC800-Pros whose system type is **General** can be connected to the same management domain.
- Click **OK**, and you can view the task information, including **Type**, **Device Name**, **Region**, **Progress**, **Status**, **Start Time**, **End Time**, and **Information** in the displayed **Progress** window.
- After the ECC800-Pro is bound to a modular, you can view the ECC800-Pro in the corresponding modular on the **Data Center Planning** page, or configure **Management Info** and **Asset Information** for the device as required.

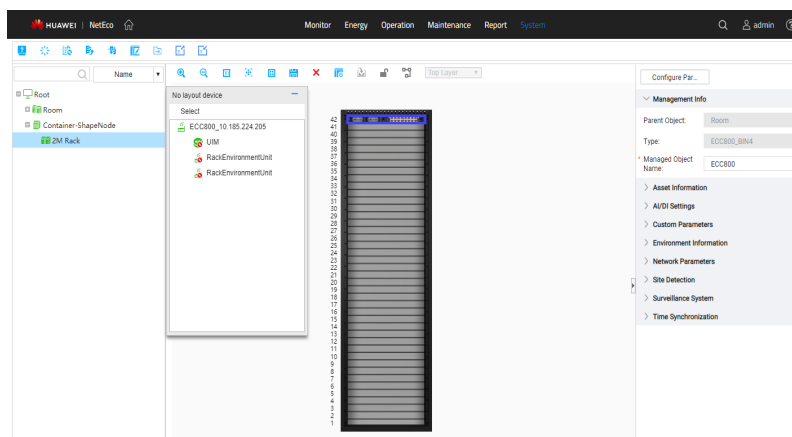
Step 5 Access the management domain and ECC800-Pro devices based on the site requirements.

Figure 6-79 ECC800-Pro device



Step 6 Drag a device to the corresponding U position in the cabinet.

Figure 6-80 Dragging a device



Step 7 Select the device icon, and configure parameters for the device in the right pane based on actual conditions.

NOTE

Names of devices connected through ECC800-Pro:

- For devices that are synchronized to the NetEco through the ECC800-Pro for the first time, their names are different on the NetEco and web-based ECC800-Pro client and are all the default names.
- The modification of the device name on the ECC800-Pro web client will be synchronized to the NetEco.

Step 8 Click  in the upper area of the page to save device information.

NOTE

After the ECC800-Pro device is bound, select the ECC800-Pro device in the left navigation tree. Then, change the authentication password in the **Management Info** area so that the password on the ECC800-Pro WebUI is the same as that on the NetEco for the ECC800-Pro to connect to the NetEco properly. The preset authentication password for the ECC800-Pro device is Modifyyme_123.

Perform the following operations on the **Modify** page:

1. Enter the new password in the **New password** and **Confirm password** text boxes.
2. Perform the following operations as required in the **Send To Device** column.

If **YES** is selected, change and synchronize the authentication passwords for the ECC800-Pro and ECC800-Pro WebUI synchronized on the server so that the authentication passwords on both sides are the same.

If **NO** is selected, change the authentication password for the ECC800-Pro synchronized on the server.
3. Click **OK**.

You are advised to change the password once every three months.

Step 9 You can perform the following operations after clicking the device icon:

Select **Manage** under  to view **Overview**.

----End

6.5.1.7 Setting the Transparent Transmission Function for the ECC800-Pro Collector

Context

- Using the transparent transmission function, the NMS can directly manage southbound components that are not monitored by the ECC800-Pro.
- A device connected to the COM port on the ECC800-Pro or UIM20A expansion module can be connected to the NetEco using the transparent transmission function.
- In this example, the COM2 port of the ECC800-Pro is used for transparent transmission.

Procedure

Step 1 Log in to the ECC800-Pro WebUI as an administrator.

Step 2 Choose **System Settings > NMS Application > Transparent Transmission Channel**.

Step 3 Set **COM2(Port:3212)** to **Enable** and click **Submit**.

 NOTE

Mapping relationship: COM1 corresponds to port 3211, COM2 port 3212, COM3 port 3213, and COM4 port 3214.

- If the port is set for the first time, you are prompted to set an authentication password. On the **Set Authentication Password** tab page, set **Authentication password** and **Confirm authentication password** and click **Submit**.

 NOTE

Enable Security Authentication is set to **Enable** by default. If so, an authentication password must be set. If **Enable Security Authentication** is set to **Disable**, there is no need to set an authentication password but this is risky.

- If the port has been used, you will be prompted that the transparent transmission function cannot be enabled and you need to select an idle port.

Step 4 Log in to the NetEco WebUI as an administrator.

Step 5 Choose **System > Service Settings > Data Center Planning**. The **Data Center Planning** page is displayed.

Step 6 Select the management domain to add a device.

 NOTE

- Ensure that the ECC800-Pro connected to the device has been synchronized to the NetEco.
- Ensure that the management domain to add the device is the management domain or sub-management domain of the ECC800-Pro.

Step 7 (Optional) If the management domain is a rack, click the management domain and choose **Design** under . The page for adding a device is displayed. Otherwise, skip this step.

- Step 8** In the lower-left corner of the page, click the **Device** tab.
- Step 9** Click the drop-down list box in **Type** and select **Sensor**.
- Step 10** In this example, a Polymer temperature and humidity (T/H) sensor is added in the equipment room of the root node. Select the device to be added and drag its icon to the management domain.
- Step 11** Click the device. In the device parameter area on the right, set device parameters.

 NOTE

IP Address indicates the ECC800-Pro login IP address. **Port** indicates the ECC800-Pro COM2 port (3212). **Device Address** indicates the Polymer T/H sensor address.

- Step 12** Click  to save the created device view.

- Step 13** Choose **System > Service Settings > Management > Transmission Channel Management**.

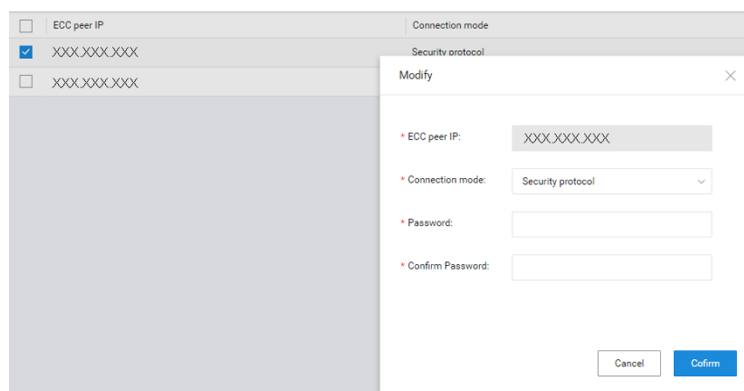
- Step 14** Click **Modify** after selecting the IP address of the ECC800-Pro connected to the NMS.

- If **Connection mode** is set to **Compatible**, click **Confirm**.

 NOTE

- On the ECC800-Pro WebUI, set **Enable Security Authentication** to **Disable**.
- In transparent transmission channel management settings, the compatibility mode has security risks. You are advised to select the security protocol mode.
- If **Connection mode** is set to **Security protocol**, enter the value of **Confirm password** that has been set on the ECC800-Pro WebUI, and click **Confirm**.

Figure 6-81 Page for managing transparent transmission channels



----End

6.5.1.8 Setting Transparent Transmission for the UIM20A Expansion Module

Context

- Using the transparent transmission function, the NMS can directly manage southbound components that are not monitored by the ECC800-Pro.

- A device connected to the COM port on the UIM20A expansion module can be connected to the NetEco using the transparent transmission function.
- In this example, the COM1 port on UIM20A expansion module 1 is used for transparent transmission.
- The UIM20A expansion module has been connected to the ECC800-Pro.

Procedure

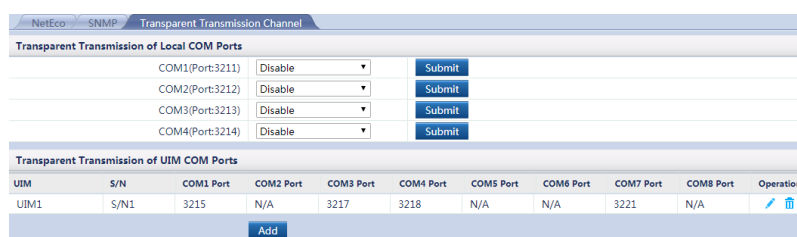
Step 1 Log in to the ECC800-Pro WebUI as an administrator.

Step 2 Choose **System Settings > NMS Application > Transparent Transmission Channel**.

Step 3 In the **Transparent Transmission of UIM COM Ports** area, click **Add**.

Step 4 Select **UIM1** from the **UIM** drop-down list box, select **Enable** from the **COM1Port** drop-down list box, and click  to **Submit**.

Figure 6-82 Enabling transparent transmission for a UIM COM port



Transparent Transmission of Local COM Ports										
COM1(Port:3211)	Disable	Submit								
COM2(Port:3212)	Disable	Submit								
COM3(Port:3213)	Disable	Submit								
COM4(Port:3214)	Disable	Submit								

Transparent Transmission of UIM COM Ports										
UIM	S/N	COM1 Port	COM2 Port	COM3 Port	COM4 Port	COM5 Port	COM6 Port	COM7 Port	COM8 Port	Operation
UIM1	S/N1	3215	N/A	3217	3218	N/A	N/A	3221	N/A	 

Add

NOTE

After transparent transmission is enabled for the COM1 port, the port number 3215 is displayed on the ECC800-Pro WebUI. Record the value.

- If the port is set for the first time, you are prompted to set an authentication password. On the **Set Authentication Password** tab page, set **Authentication password** and **Confirm authentication password** and click **Submit**.

NOTE

Enable Security Authentication is set to **Enable** by default. If so, an authentication password must be set. If **Enable Security Authentication** is set to **Disable**, there is no need to set an authentication password but this is risky.

- If the port has been used, you will be prompted that the transparent transmission function cannot be enabled and you need to select an idle port.

Step 5 Log in to the NetEco WebUI as an administrator.

Step 6 Choose **System > Service Settings > Data Center Planning**. The **Data Center Planning** page is displayed.

Step 7 Select the management domain to add a device.

 NOTE

- Ensure that the ECC800-Pro connected to the device has been synchronized to the NetEco.
- Ensure that the management domain to add the device is the management domain or sub-management domain of the ECC800-Pro.

Step 8 (Optional) If the management domain is a rack, click the management domain and choose **Design** under . The page for adding a device is displayed. Otherwise, skip this step.

Step 9 In the lower-left corner of the page, click the **Device** tab.

Step 10 Click the drop-down list box in **Type** and select **Sensor**.

Step 11 In this example, a Polymer temperature and humidity (T/H) sensor is added in the equipment room of the root node. Select the device to be added and drag its icon to the management domain.

Step 12 Click the device. In the device parameter area on the right, set device parameters.

 NOTE

IP Address indicates the ECC800-Pro login IP address. **Port** indicates the UIM1 COM1 port. **Device Address** indicates the Polymer T/H sensor address.

Step 13 Click  to save the created device view.

Step 14 Choose **System > Service Settings > Management > Transmission Channel Management**.

Step 15 Click **Modify** after selecting the IP address of the ECC800-Pro connected to the NMS.

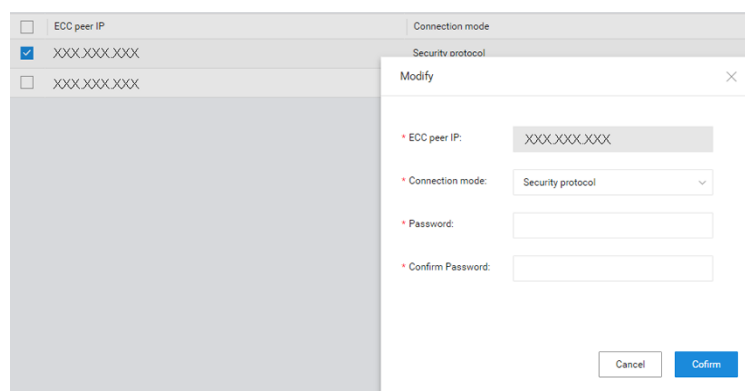
- If **Connection mode** is set to **Compatible**, click **Confirm**.

 NOTE

On the ECC800-Pro WebUI, **Enable Security Authentication** is set to **Disable**.

- If **Connection mode** is set to **Security protocol**, enter the value of **Confirm password** that has been set on the ECC800-Pro WebUI, and click **Confirm**.

Figure 6-83 Page for managing transparent transmission channels



----End

6.5.2 Adding Sensors

6.5.2.1 Adding Dry Contact Interface Devices

6.5.2.1.1 Setting Door Status Sensor Monitoring Parameters on the ECC800-Pro Web

After connecting a door status sensor (DSS) to the AI/DI port of an ECC800-Pro collector, you need to set DSS parameters on the web user interface (WebUI) of the collector.

Prerequisites

- You have obtained the IP address, and login user name and password for the ECC800-Pro collector.
- A PC with an IP address in the same network segment as the ECC800-Pro collector is prepared, and the PC has been connected to the ECC800-Pro collector over a switch.

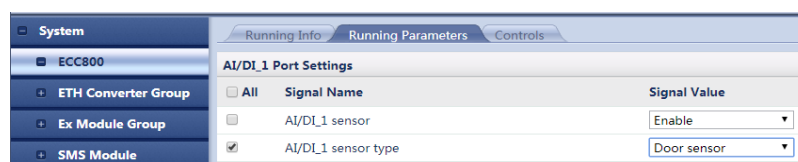
Context

This section describes how to set DSS monitoring parameters when a DSS is connected to the AI/DI_1 port of the ECC800-Pro collector. Set the parameters based on the actual port connected to the DSS onsite.

Procedure

- Step 1** Log in to the WebUI of the ECC800-Pro collector.
- Step 2** Choose **Monitoring > System > ECC800 > Running Parameters > AI/DI_1 Port Settings**.
- Step 3** Set **AI/DI_1** to **Enable**.
- Step 4** Click **Submit**.
- Step 5** Select **Door sensor** from the **AI/DI_1 sensor type** drop-down list box.

Figure 6-84 Setting a sensor type for a dry contact



- Step 6** Click **Unhide All Advanced Signals**, then click **Power Supply Parameters**. Ensure that **III power supply enable(AIDI_1/DO)** is **Yes**.

- Step 7** Click **Submit**.

----End

6.5.2.1.2 Setting Smoke Sensor and Water Leakage Sensor Parameters on the ECC800-Pro Web

After connecting a smoke sensor or water leakage sensor to the AI/DI port of an ECC800-Pro collector, you need to set smoke sensor or water leakage sensor parameters on the web user interface (WebUI) of the collector.

Prerequisites

- You have obtained the IP address, and login user name and password for the ECC800-Pro collector.
- A PC with an IP address in the same network segment as the ECC800-Pro collector is prepared, and the PC has been connected to the ECC800-Pro collector over a switch.

Context

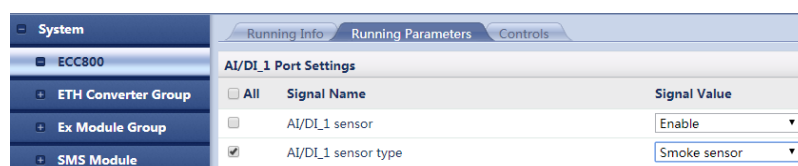
- This section describes how to set smoke sensor or water leakage sensor monitoring parameters when a smoke sensor or water leakage sensor is connected to the AI/DI_1 port of the ECC800-Pro collector. Set the parameters based on the actual port connected to the smoke sensor or water leakage sensor onsite.
- A smoke sensor or water leakage sensor is a self-identification device. After a smoke sensor or water leakage sensor is connected to the AI/DI port of an ECC800-Pro collector, the sensor type is automatically identified and you do not need to manually set **AI/DI_1 Sensor Type** on the WebUI.

To enable automatic device identification, choose **System Settings > Device Management > Device Addition > Auto Discover Device**.

Procedure

- Step 1** Log in to the WebUI of the ECC800-Pro collector.
- Step 2** Choose **Monitoring > System > ECC800 > Running Parameters > AI/DI_1 Port Settings**.
- Step 3** Set **AI/DI_1** to **Enable**.
- Step 4** Click **Submit**.
- Step 5** Check whether **AI/DI_1 sensor type** is automatically identified. The following uses **Smoke sensor** as an example.

Figure 6-85 Setting a sensor type for a dry contact



- Step 6** Click **Unhide All Advanced Signals**, then click **Power Supply Parameters**. Ensure that **III power supply enable(AIDI_1/DO)** is **Yes**.

Step 7 Click **Submit**.

----End

6.5.2.1.3 Setting Infrared Sensor Monitoring Parameters on the ECC800-Pro Web

After a normally open (NO) or normally closed (NC) dry contact is connected to the AI/DI port of an ECC800-Pro collector, you need to set device parameters of the NO or NC dry contact on the WebUI.

Prerequisites

- You have obtained the IP address, and login user name and password for the ECC800-Pro collector.
- A PC with an IP address in the same network segment as the ECC800-Pro collector is prepared, and the PC has been connected to the ECC800-Pro collector over a switch.

Context

- An NO or NC dry contact is a device whose normal status signal is open (or closed) and whose alarm signal is closed (or open), such as an infrared sensor.
- This section describes how to set monitoring parameters for the infrared sensor when the infrared sensor is connected to the AI/DI_1 port on the ECC800-Pro. Set the parameters based on the actually connected port.

Procedure

Step 1 Log in to the WebUI of the ECC800-Pro collector.

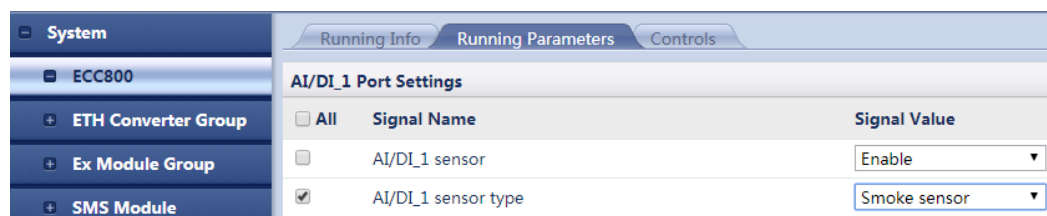
Step 2 Choose **Monitoring > System > ECC800 > Running Parameters > AI/DI_1 Port Settings**.

Step 3 Set **AI/DI_1** to **Enable**.

Step 4 Click **Submit**.

Step 5 Select **NC** for **AI/DI_1 Sensor Type** from the drop-down list.

Figure 6-86 Setting the infrared sensor type



Step 6 Click **Unhide All Advanced Signals**, then click **Power Supply Parameters**. Ensure that **III power supply enable(AIDI_1/DO)** is **Yes**.

Step 7 Click **Submit**.

----End

6.5.2.1.4 Setting Device Monitoring Parameters of an NO/NC Dry Contact on the ECC800-Pro Web

After a normally open (NO) or normally closed (NC) dry contact is connected to the AI/DI port of an ECC800-Pro collector, you need to set device parameters of the NO or NC dry contact on the WebUI.

Prerequisites

- You have obtained the IP address, and login user name and password for the ECC800-Pro collector.
- A PC with an IP address in the same network segment as the ECC800-Pro collector is prepared, and the PC has been connected to the ECC800-Pro collector over a switch.

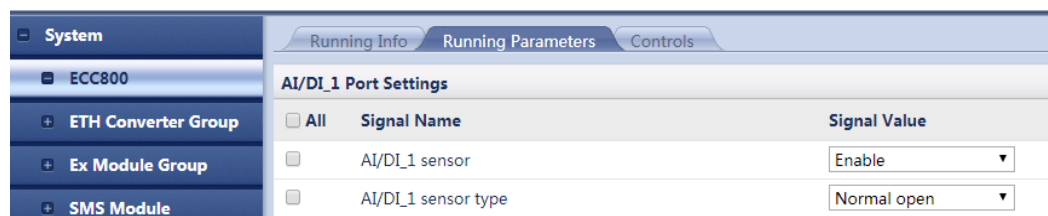
Context

- An NO or NC dry contact is a device whose normal status signal is open (or closed) and whose alarm signal is closed (or open), such as a skylight controller.
- This section describes how to set skylight controller monitoring parameters when a skylight controller is connected to the AI/DI_1 port of the ECC800-Pro collector. Set the parameters based on the actual port connected to the skylight controller onsite.

Procedure

- Step 1** Log in to the WebUI of the ECC800-Pro collector.
- Step 2** Choose **Monitoring > System > ECC800 > Running Parameters > AI/DI_1 Port Settings**.
- Step 3** Set **AI/DI_1** to **Enable**.
- Step 4** Click **Submit**.
- Step 5** Select **NO** or **NC** for **AI/DI_1 Sensor Type** from the drop-down list.

Figure 6-87 Setting the sensor type of a dry contact



NOTE

- NO: indicates a normally open dry contact. The dry contact will report an alarm in the normally closed state.
- NC: indicates a normally closed dry contact. The dry contact will report an alarm in the normally open state.

- Step 6** Click **Unhide All Advanced Signals**, then click **Power Supply Parameters**. Ensure that **III power supply enable(AIDI_1/DO)** is **Yes**.

Step 7 Click **Submit**.

----End

6.5.2.1.5 Creating an Icon for a Door Status Sensor on the NetEco

This section describes how to create and configure an icon for a door status sensor in an equipment room or container.

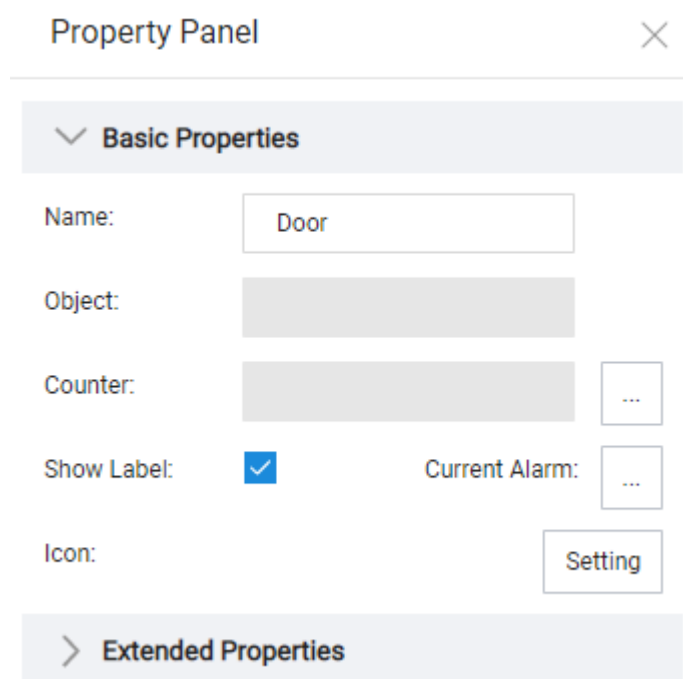
Prerequisites

- You have logged in to the NetEco client using a web browser.
- You have the operation rights for configuring **Data Center View**.

Procedure

- Step 1** Choose **Monitor > Device Management > Data Center View** from the main menu. The **Data Center View** window is displayed.
- Step 2** On the view page, double-click the equipment room or container where the door status sensor is installed.
- Step 3** In the editing window, click . The **Toolbox** dialog box is displayed.
- Step 4** Drag  to the required position in the view. The **Property Panel** dialog box is displayed.

Figure 6-88 Property Panel



Property Panel

Basic Properties

Name: Door

Object:

Counter:

Show Label: ☒ Current Alarm:

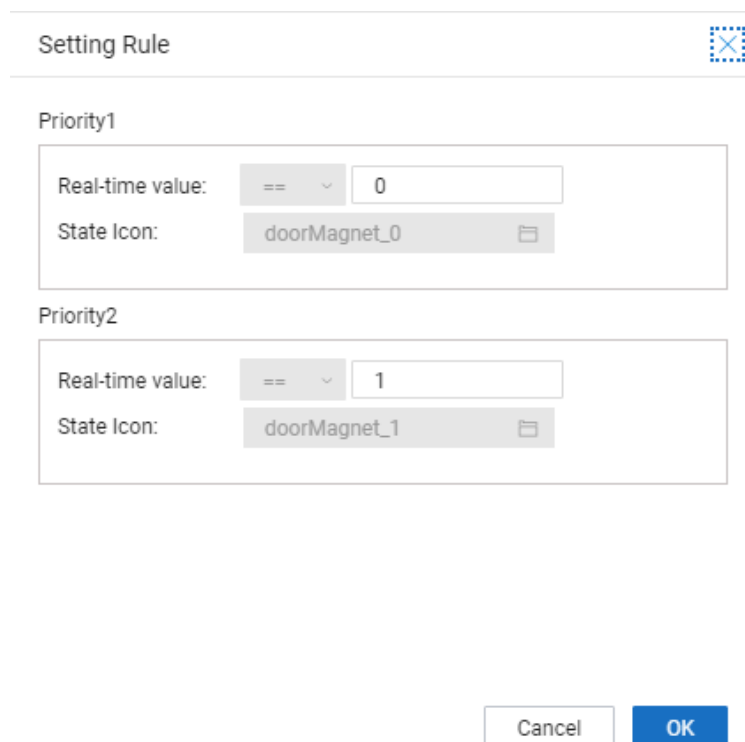
Icon: Setting

Extended Properties

- Step 5** Type the name for the icon and click **Setting**. The **Setting Rule** dialog box is displayed.

1. In the **Setting Rule** dialog box, configure the real-time value. The value consistent with real-time signal value.
2. Click **OK**.

Figure 6-89 Setting Rule



The image shows a 'Setting Rule' dialog box with a close button in the top right corner. It contains two sections: 'Priority1' and 'Priority2'. Each section has a 'Real-time value' field with a dropdown menu set to '==' and a text box containing '0' for Priority1 and '1' for Priority2. Below each 'Real-time value' field is a 'State Icon' field with a dropdown menu showing 'doorMagnet_0' for Priority1 and 'doorMagnet_1' for Priority2, each with a folder icon to its right. At the bottom of the dialog are 'Cancel' and 'OK' buttons.

Step 6 In the **Basic Properties** pane in the **Property Panel** dialog box, click ... following the **Attribute** to configure data for the door status sensor icon.

Step 7 On the displayed **Select Data** page, select **Managed Object** and **Attribute**. Then, click **OK**.

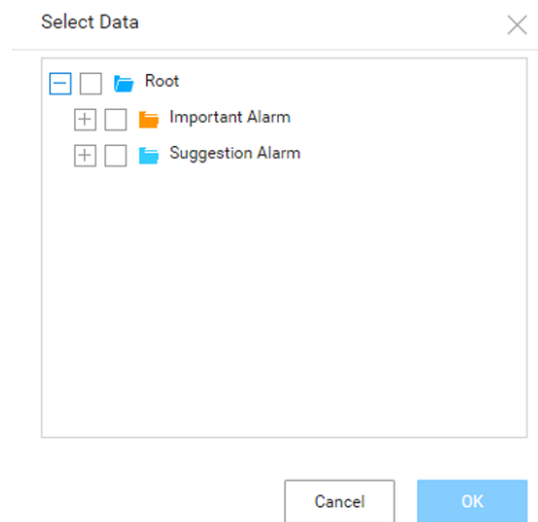
 NOTE

After the managed object and counter are bound, you can remotely open and close a door using the door status sensor icon.

1. Click the door status sensor icon and choose **Close** or **Open** under .
2. In the displayed dialog box, click **Yes**.

Step 8 Click ... following the **Current Alarm**. Select alarms to be bound to the icon.

Figure 6-90 Binding alarms



Step 9 Click **Yes**.

NOTE

You can bind a maximum of 20 alarms to a measurement object. After an alarm is bound with a device icon, the color of the device icon will be changed to that of the color indicating that the bound alarm is generated.

Step 10 In the **Property Panel**, click **Extend Properties** then configure basic properties for the icon.

Figure 6-91 Extend properties of the icon

The screenshot shows a 'Property Panel' dialog box with a close button (X) in the top right corner. It has two tabs: 'Basic Properties' and 'Extended Properties', with 'Extended Properties' currently selected. The 'Extended Properties' section contains the following controls:

- Transparency:** A slider bar and a numeric input field showing '1'.
- Background:** A checkbox.
- Font Bold:** A checkbox, a 'B' icon, and a numeric input field showing '12'.
- Border:** A checkbox.
- Background:** A button labeled 'Apply to Others'.
- Position and Size:** A grid of six numeric input fields with up/down arrows:
 - Place X: 471
 - Y: 114
 - Offset X: 0
 - Y: 0
 - Icon W: 30
 - H: 30

----End

6.5.2.1.6 Creating the Water Sensor on the NetEco

This section describes how to create **Water Sensor** icons to bind the managed objects, indicators, and alarms.

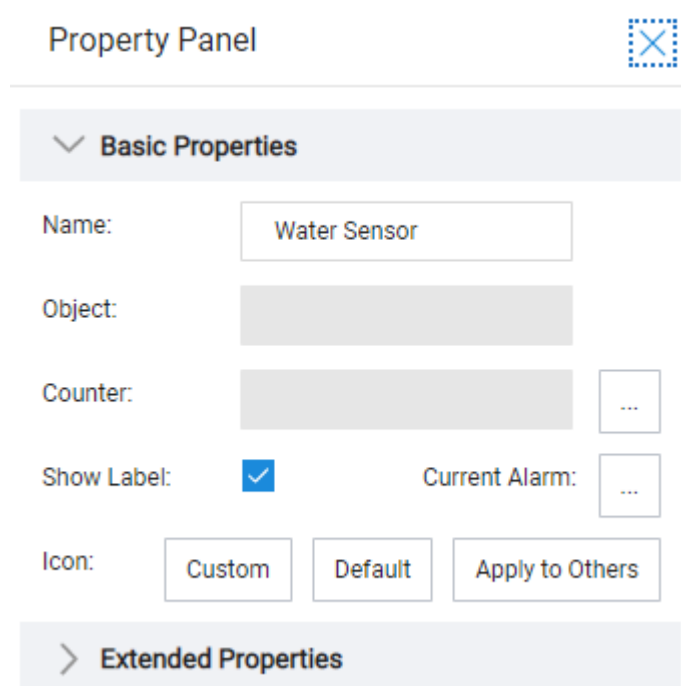
Prerequisites

- You have logged in to the NetEco client using a web browser.
- You have the operation rights for configuring **Data Center View**.

Procedure

- Step 1** Choose **Monitor > Device Management > Data Center View** from the main menu. The **Data Center View** window is displayed.
- Step 2** On the view page, double-click the equipment room or container where the door status sensor is installed.
- Step 3** In the editing area, click  on the toolbar. The **Toolbox** dialog box is displayed.
- Step 4** Drag  to the required position in the view. The **Property Panel** dialog box is displayed.

Figure 6-92 Property Panel



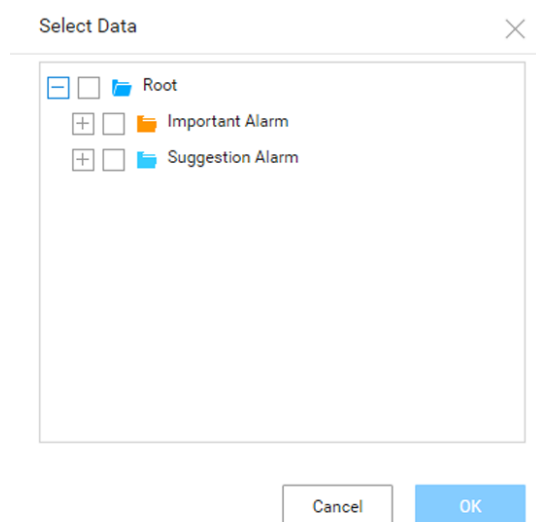
The Property Panel is titled 'Property Panel' with a close button (X) in the top right corner. It features a 'Basic Properties' section with a dropdown arrow. Below this section, there are several fields: 'Name' with the value 'Water Sensor', 'Object' with a greyed-out field, 'Counter' with a greyed-out field and a selection button (...), 'Show Label' with a checked checkbox, 'Current Alarm' with a selection button (...), and 'Icon' with three buttons: 'Custom', 'Default', and 'Apply to Others'. At the bottom, there is an 'Extended Properties' section with a right-pointing arrow.

Step 5 Click ... following the **Attribute**. In the **Select Data** dialog box, select managed objects and indicators.

Step 6 Click **OK**.

Step 7 Click ... following the **Current Alarm**. Select alarms to be bound to the icon.

Figure 6-93 Binding alarms



The 'Select Data' dialog box has a title bar with a close button (X). It contains a tree view with the following structure: 'Root' (expanded), 'Important Alarm' (indicated by an orange folder icon), and 'Suggestion Alarm' (indicated by a blue folder icon). Each item has a checkbox to its left. At the bottom of the dialog, there are 'Cancel' and 'OK' buttons.

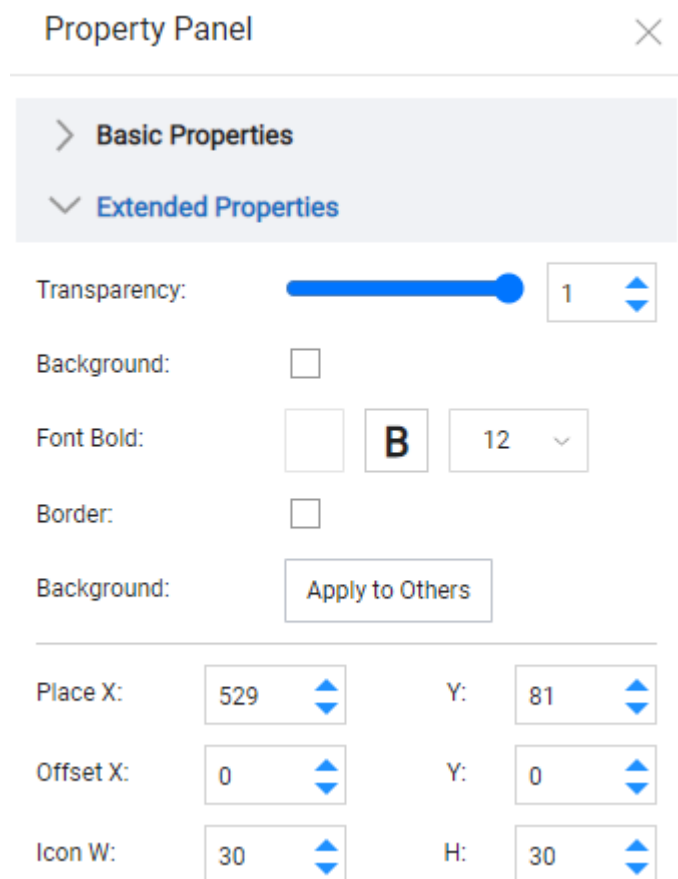
Step 8 Click **Yes**.

NOTE

You can bind a maximum of 20 alarms to a measurement object. After an alarm is bound with a device icon, the color of the device icon will be changed to that of the color indicating that the bound alarm is generated.

- Step 9** In the **Property Panel**, click **Extend Properties** then configure basic properties for the icon.

Figure 6-94 Extend properties of the icon



----End

6.5.2.1.7 Modifying Alarm Names for Devices on the NetEco

Prerequisites

You have logged in to the NetEco client.

Procedure

1. On the main menu, choose **Monitor > Alarm Management > Alarm Settings** to go to the **Alarm Settings** page.
2. In the navigation pane on the left, click **Redefine Alarm**.
3. In the management domain tree, select the device whose alarms need to be redefined. All the alarms of the device are displayed.
4. Click  in the **Operation** column for the entry that contains the alarm to be redefined, set **New Name**, **New Severity**, **New Type** and so on, and click .

5. Click **Batch Apply to Devices**, below the current alarm list. In the **Batch Apply to Devices** dialog box, you can apply the selected alarm rule to other devices in batches.

 NOTE

For **Selected items**, you can select either of the following values for batch application:

- **Selected:** Selects the selected data.
- **Select All:** Selects all data in the table.

For **Application items**, you can select the alarm, severity, alarm type, cause, suggestion and so on for batch application to other devices of the same type.

You can select either of the following options for batch application:

- **All objects:** The rules are applied to all existing and future devices of the same type.
- **Custom:** The rules are applied to devices of the same type under the current root node.

Rules for applying an empty rule:

- For two devices of the same type, if the redefinition alarm rule is not set for one device and you want to apply the rule to another device that has been configured with an alarm rule, the redefinition alarm rule that has been set on the other device is cleared.

6.5.2.1.8 Modifying Performance Counter Names for Devices on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created an ECC800-Pro collector in the **Date Center Planning** page.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Click  on the toolbar to access **Signal Management**.

Step 3 In the navigation pane on the left, select a device whose counter name needs to be modified.

Step 4 Click the **Sampling, Configuration, or Statistic** tab and modify performance counter names.

Step 5 Click **Apply**.

----End

6.5.2.2 Adding a Temperature and Humidity Sensor

6.5.2.2.1 Setting Monitoring Parameters for a T/H Sensor (BOM Number: 33010346)

Prerequisites

- The device address planned for the ambient temperature and humidity sensor is obtained.
- The ambient temperature and humidity sensor connects to the collector and displays values on the display panel.
- The IP address, user name, and password for logging in to the collector are obtained.
- A PC with an IP address in the same network segment as the collector is prepared, and the PC connects to the collector over a switch.

Context

Before connecting the ambient temperature and humidity sensor to the NetEco, set monitoring parameters, such as the device address and baud rate, on the sensor, and then modify the port parameters for the collector connecting to the sensor to ensure that the values of **BaudRate**, **DataBit**, **StopBit**, and **Parity** on the sensor are consistent with those for the collector port.

Procedure

- Step 1** Hold down **Set** on the display panel of the ambient temperature and humidity sensor for 2 seconds.
- Step 2** When **Add** is displayed, set the device address by pressing + and -. When creating an ambient temperature and humidity sensor on the NetEco, set **Device Address** to the same value.
- Step 3** Press **Set**.
- Step 4** When **bAu** is displayed, retain the default value or change the baud rate by pressing + and -. Set **BaudRate** for the collector port to the same value.

NOTE

DataBit, **StopBit**, and **Parity** for the ambient temperature and humidity sensor cannot be set on the WebUI. Their values are **8**, **1**, and **None** respectively.

- Step 5** Set RS485 port parameters for the collector based on the value of **BaudRate**, **DataBit**, **StopBit**, and **Parity** of the device. For ECC800-Pro collector settings, see [6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector](#).

----End

6.5.2.2.2 Creating a Temperature and Humidity Sensor on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.

- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **Sensor**.

Step 5 Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-46 MODBUS-RTU device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the IP address of the collector to which the device is connected.
Port	Set this parameter to the port through which the device connects to the collector. For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Set this parameter to the address set on the device.

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.5.2.3 Adding a Water Leakage Sensor

6.5.2.3.1 Creating a Water Leakage Sensor on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **Sensor**.

Step 5 Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-47 MODBUS-RTU device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set the IP address of the data collector to which the device connects.
Port	Set this parameter to the port through which the device connects to the collector. For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Set this parameter to the address set on the device (set to 1 by default).

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.5.2.4 Adding a Hydrogen Sensor

6.5.2.4.1 Setting Monitoring Parameters for a Hydrogen Sensor

Prerequisites

- The device address planned for the hydrogen sensor is obtained.
- The hydrogen sensor is powered on.
- The IP address, user name, and password for logging in to the collector are obtained.
- A PC with an IP address in the same network segment as the collector is prepared, and the PC connects to the collector over a switch.

Context

Before connecting the hydrogen sensor to the NetEco, modify the port parameters for the collector connecting to the hydrogen sensor to ensure that the values of **BaudRate**, **DataBit**, **StopBit**, and **Parity** on the hydrogen sensor are consistent with those for the collector port.

Procedure

Step 1 Set the hydrogen sensor device address by setting the **ADD** dual in-line package (DIP) on the hydrogen detector RS485 monitoring card.

- If a toggle switch is flipped to **OFF**, the value of this toggle switch is **0**.
- If a toggle switch is flipped to **ON**, the value of this toggle switch is **1**.

Table 6-48 Mapping between Hydrogen Sensor communications address and DIP switch

Communications Address	SW1	SW2	SW3	SW4
1	1	1	1	0
5	1	0	1	0
10	0	1	0	1
15	0	0	0	0

BaudRate, **DataBit**, **StopBit** and **Parity** on hydrogen sensor cannot be set, the default setting is **9600**, **8**, **1** and **None**.

- Step 2** Set RS485 port parameters for the collector based on the value of **BaudRate**, **DataBit**, **StopBit**, and **Parity** of the device. For ECC800-Pro collector settings, see [6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector](#).

----End

6.5.2.4.2 Creating a Hydrogen Sensor on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 2** Select the management domain to add a device.
- Step 3** In the lower-left corner of the page, click the **Device** tab.
- Step 4** Click the drop-down list box in **Type** and select **Sensor**.
- Step 5** Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

- Step 6** Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-49 MODBUS-RTU device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set the IP address of the data collector to which the device connects.
Port	Set this parameter to the port through which the device connects to the collector. For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Set this parameter to the address set on the device.

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.5.3 Adding the Access Management System

6.5.3.1 Setting Monitoring Parameters for the A8802RS Access Controller

Procedure

Step 1 Set the address of the access controller using the DIP toggle switches, set the device address to 0 by default, as shown in [Table 6-50](#).

Table 6-50 Setting the address of the access controller

Device Address	Toggle Switch 1	Toggle Switch 2
0	OFF	OFF
1	ON	OFF
2	OFF	ON
3	ON	ON

Step 2 Set the baud rate of the access controller to **19200**. The preset data bit, stop bit, and check bit are **8**, **1**, and **none respectively**. For ECC800-Pro collector settings, see [6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector](#).

----End

6.5.3.2 Creating an Access Controller on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Access Control Management** and **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

Step 1 Choose **Monitor > Security > Access Control Management** from the main menu. The **Access Control Management** window is displayed.

Step 2 On the **Device Management** page, click **Create**. The **Data Center Planning** page is displayed.

Step 3 Add an access controller to the **Data Center Planning** page.

1. Select the management domain to add a device.
2. In the lower-left corner of the page, click the **Device** tab.
3. Click the drop-down list box in **Type** and select **Access Controller**.
4. Select an access controller and drag its icon to the management domain.

 NOTE

To delete a device, click the device and choose **Delete** under .

5. Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-51 Parameter description

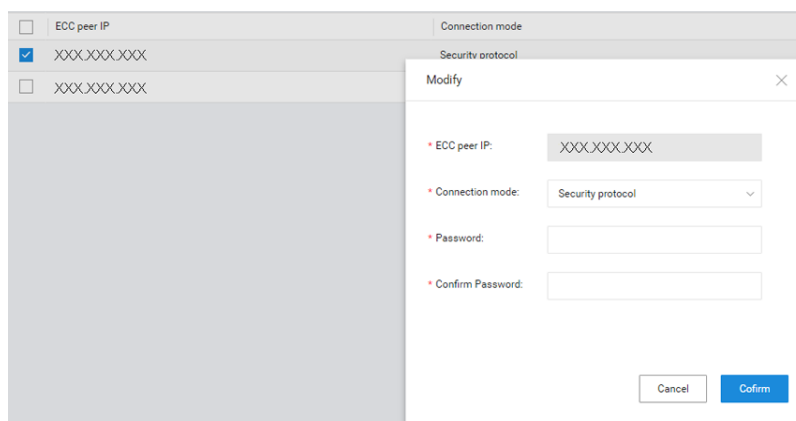
Parameter	Description
Managed Object Name	Device name
IP	IP address of the collector to which the device is connected
Port	Port through which the device connects to the collector For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Address set on the device (set to 0 by default)
Timeout period	Timeout duration for a connection test. The default value is 3s .

Step 4 Click  on the toolbar to save the device information.

Step 5 On the **Transmission Channel Management** page, set the connection mode to secure mode and set the security password.

- Choose **System > Service Settings > Transmission Channel Management** from the main menu. Select the IP address of the ECC800-Pro connected to the access controller.
- Click **Modify**. In the dialog box that is displayed, set **Connection Mode** to **Security protocol**. Set **Password** to the authentication password that you have set on the ECC800-Pro, enter the confirm password, and click **OK**.

Figure 6-95 Transmission Channel Management



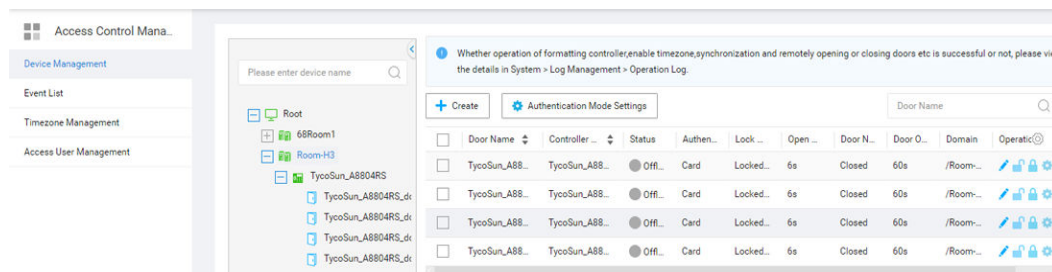
Step 6 Go back to the data center planning page of the access controller. Click **Connection test**. If the connection is successful, the A8802RS access controller is connected to the NetEco.

----End

Follow-up Procedure

After an **Access Controller** is created, its information is displayed on the **Device Management** page, as shown in [Figure 6-96](#).

Figure 6-96 Checking the access controller information



NOTICE

After the access controller is added, format it manually in the access controller list to avoid failure in initializing the access controller.

6.5.3.3 Formatting an Access Controller

This topic describes how to format access control cards, historical records, timezones, and holidays.

Prerequisites

- You have logged in to the NetEco client using a web browser.
- You have the operation rights for **Access Control Management**.

Context

The door access controller synchronized by the ECC800-Pro to the NetEco does not support formatting.

Procedure

Step 1 Choose **Monitor > Security > Access Control Management** from the main menu. The **Access Control Management** window is displayed.

Step 2 In the **Device Management** tab page, click  in the **Operation** column. The confirm dialog box is displayed.

Step 3 Click **Yes**. The access controller is successfully formatted.

NOTE

- After formatting the access controller, click  to initialize parameters. In this manner, the timezones are enabled. The access controller is not disabled even if the parameters are not initialized or the timezones are not enabled.
- Synchronize the timezones and then the user groups or holidays after an access controller is formatted and parameters are initialized.

----End

6.5.3.4 Setting Monitoring Parameters for the NEWABEL CHD200G Fingerprint Controller

Context

This section applies to the settings of the card reader with a keypad, fingerprint and card reader, and fingerprint and card reader with a keypad.

Procedure

Step 1 Set the baud rate of the NEWABEL CHD200G fingerprint controller to **9600** on the ECC800-Pro collector. The preset address is 1. The address does not need to be set. When creating the device on the NetEco, set **Device Address** to 1.

----End

6.5.3.5 Creating a NEWABEL CHD200G Fingerprint Controller on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The access controller has been connected to the NetEco.
- The Newabel CHD200G fingerprint controller and the access controller are connected to the same ECC800-Pro collector.

- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Context

This section applies to the settings of the card reader with a keypad, fingerprint and card reader, and fingerprint and card reader with a keypad.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **Fingerprint Controller**.

Step 5 Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Specify parameters in the right pane based on the following table.

Table 6-52 Device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the IP address of the collector to which the device is connected.
Port	Set this parameter to the port through which the device connects to the collector. For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Set this parameter to the address set on the device (set to 0 by default).
Timeout period	Timeout duration for a connection test. The default value is 3s.

Step 7 Click **Connection test** to start the connection test. After the connection test is successful, click  on the toolbar to save the device information.

- Step 8** Click **Bind AccessController** and select an access controller to bind the fingerprint controller and select a door passage for the access controller from respective drop-down menus.

----End

6.5.4 Adding a Smart Cooling Product

6.5.4.1 Setting Monitoring Parameters for Smart Cooling Products (over Modbus-RTU)

The monitoring parameter settings are similar for smart cooling products that connect to the NMS over Modbus-RTU. This section uses NetCol5000-A050 as an example.

Prerequisites

- The device address planned for the NetCol5000-A050 is obtained.
- The NetCol5000-A050 is powered on.
- The IP address, user name, and password for logging in to the collector are obtained.
- A PC with an IP address in the same network segment as the collector is prepared, and the PC connects to the collector over a switch.

NOTE

The Modbus TCP protocol is recommended for connecting FusionCol8000-E/FusionCol8000-C series smart cooling products to the NetEco.

Context

Before connecting the NetCol5000-A050 to the NetEco, set monitoring parameters, such as the device address and baud rate, on the NetCol5000-A050, and then modify the port parameters for the collector connecting to the NetCol5000-A050 to ensure that the values of **BaudRate**, **DataBit**, **StopBit**, and **Parity** on the NetCol5000-A050 are consistent with those for the collector port.

Procedure

- Step 1** Tap **Settings** on the NetCol5000-A050 home screen.

- Step 2** Enter the user name and password of an administrator.

NOTE

The preset user name and password for the NetCol5000-A050 are **Admin** and **000001**, respectively. To ensure access security, change the password after first login.

- Step 3** Choose **Comm Settings** > **Modbus Settings**.

- Step 4** Set **Baud Rate** and **Com address**.

Table 6-53 Parameter description

Parameter	Setting
Communication address	1-255 Indicates the actual address for the NetCol5000-A050. The devices with the same address cannot connect to the same port. When creating a NetCol5000-A050 on the NetEco, set Device Address to the same value.
Baud Rate	9600, 19200 Indicates the baud rate. The default baud rate is 9600. Set BaudRate for the collector port to the same value.
RS485 monitoring grouping	Enable, Disable - For scenarios without grouping, set this parameter to Enable for the last device. - For scenarios with grouping, set this parameter to Enable for the last device in each teamwork control group.

The **DataBit**, **StopBit**, and **Parity** of the NetCol5000-A050 cannot be set on the WebUI. Their default values are **8**, **1**, and **None** respectively.

- Step 5** Set RS485 port parameters for the collector based on the value of **BaudRate**, **DataBit**, **StopBit**, and **Parity** of the device. For ECC800-Pro collector settings, see [6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector](#).

----End

6.5.4.2 Creating a Smart Cooling Product on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **Air Conditioner**.

Step 5 Select the device to be added and drag its icon to the management domain.

 NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-54 MODBUS-RTU device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the IP address of the collector to which the device is connected.
Port	Set this parameter to the port through which the device connects to the collector. For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Set this parameter to the address set on the device.
Timeout period	Timeout duration for a connection test. The default value is 3s .
Receive Timeout(ms)	Specifies the timeout period for waiting for the response packet from the NE after a packet is sent.
Max Register Num	During collection, the number of requested registers is too large. As a result, the NE response times out or does not respond. This parameter is added to specify the number of requested registers. When a collection task is delivered, the task is split into multiple requests based on this parameter and then delivered to the NE.
Heartbeat Period(s)	Specifies the instance-level heartbeat interval.

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.5.5 Adding a Chiller

6.5.5.1 Creating a Chiller on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **Chiller**.

Step 5 Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-55 MODBUS-RTU device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the IP address of the collector to which the device is connected.
Port	Set this parameter to the port through which the device connects to the collector. For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Set this parameter to the address set on the device.

Parameter	Description
Timeout period	Timeout duration for a connection test. The default value is 3s.

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.5.6 Adding a UPS

6.5.6.1 Setting Monitoring Parameters for a UPS2000

Prerequisites

- You have obtained the IP address and user name and password for logging in to the collector.
- A PC with an IP address in the same network segment as the collector has been prepared and connected to the collector over a switch.

Context

Before connecting the UPS2000 to the NetEco, set monitoring parameters on the UPS2000. Then, modify the port parameters for the collector connecting to the UPS2000 to ensure that the values of **BaudRate**, **DataBit**, **StopBit**, and **Parity** on the UPS2000 are consistent with those for the collector port.

Procedure

Step 1 Set the UPS2000 device address using the DIP switch S2 on the optional Modbus card.

Toggle switches 1 to 8 of DIP switch S2 specify the device address in binary mode. ON indicates 0 and OFF indicates 1. [Table 6-56](#) shows an example of the address settings.

Table 6-56 Mapping between device addresses and Modbus card DIP switch settings

Device Address	Toggle Switch 1	Toggle Switch 2	Toggle Switch 3	Toggle Switch 4	Toggle Switch 5	Toggle Switch 6	Toggle Switch 7	Toggle Switch 8
1	OFF	ON	ON	ON	ON	ON	ON	ON
2	ON	OFF	ON	ON	ON	ON	ON	ON
3	OFF	OFF	ON	ON	ON	ON	ON	ON

Device Address	Toggle Switch 1	Toggle Switch 2	Toggle Switch 3	Toggle Switch 4	Toggle Switch 5	Toggle Switch 6	Toggle Switch 7	Toggle Switch 8
4	ON	ON	OFF	ON	ON	ON	ON	ON

Step 2 Set RS485 port parameters for the collector based on the value of **BaudRate**, **DataBit**, **StopBit**, and **Parity** of the device. For ECC800-Pro collector settings, see [6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector](#).

 NOTE

For the UPS2000, the default values of **BaudRate**, **DataBit**, **StopBit**, and **Parity** are **9600**, **8**, **1**, and **None**, respectively. If the parameters are changed, the actual parameter values prevail.

----End

6.5.6.2 Creating a UPS on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **UPS**.

Step 5 Select the device to be added and drag its icon to the management domain.

 NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-57 MODBUS-RTU device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set the IP address of the data collector to which the device connects.
Port	Set this parameter to the port through which the device connects to the collector. For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Set this parameter to the address set on the device.
Timeout period	Timeout duration for a connection test. The default value is 3s .

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.5.7 Adding a PDU

6.5.7.1 Setting Monitoring Parameters for a PDU8000

Prerequisites

- The IP address planned for the PDU8000 is obtained.
- The PDU8000 is powered on.

NOTE

The Modbus TCP protocol is recommended for connecting the PDU8000 to the NetEco.

Context

Before connecting the PDU8000 to the NetEco over Modbus-RTU, set monitoring parameters, such as **Serial port baud rate** and **Serial port address**.

Procedure

Step 1 Tap **Settings** on the PDU8000 home screen.

Step 2 Enter the PDU8000 user name and password and tap .

 NOTE

The preset user name and password for the PDU8000 are **admin** and **000001** respectively. To ensure access security, change the password upon the first login.

Step 3 Click **Communication**.

Set **Serial port baud rate** and **Serial port address**.

Table 6-58 Parameter description

Parameter	Description
Serial port baud rate	Indicates the baud rate. The default baud rate is 9600. Set BaudRate for the collector port to the same value. DataBit , StopBit , and Parity for the PDU8000 cannot be set on the WebUI. Their values are 8 , 1 , and None respectively.
Serial port address	Indicates the device address planned for the PDU8000. The devices with the same address cannot connect to the same port. When creating a PDU8000 on the NetEco, set Device Address to the same value.

Step 4 Set RS485 port parameters for the collector based on the value of **BaudRate**, **DataBit**, **StopBit**, and **Parity** of the device. For ECC800-Pro collector settings, see [6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector](#).

----End

6.5.7.2 Creating a PDU on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

Step 1 Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 2 Select the management domain to add a device.

Step 3 In the lower-left corner of the page, click the **Device** tab.

Step 4 Click the drop-down list box in **Type** and select **PDU**.

Step 5 Select the device to be added and drag its icon to the management domain.

 NOTE

To delete a device, click the device and choose **Delete** under .

Step 6 Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-59 MODBUS-RTU device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set the IP address of the data collector to which the device connects.
Port	Set this parameter to the port through which the device connects to the collector. For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Set this parameter to the address set on the device.
Timeout period	Timeout duration for a connection test. The default value is 3s .

Step 7 Click  on the toolbar to save the device information.

Step 8 Click **Connection test** to start the connection test.

----End

6.5.8 Adding a Fresh Air Unit

6.5.8.1 Creating a Fresh Air Unit on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The ECC800-Pro connected to the device has been connected to the NetEco.
- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 2** Select the management domain to add a device.
- Step 3** In the lower-left corner of the page, click the **Device** tab.
- Step 4** Click the drop-down list box in **Type** and select **Air Conditioner**.
- Step 5** Select the device to be added and drag its icon to the management domain.

NOTE

To delete a device, click the device and choose **Delete** under .

- Step 6** Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-60 Modbus RTU device parameter description

Parameter	Description
Managed Object Name	Device name
IP	IP address of the collector to which the device is connected
Port	Port through which the device connects to the collector For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Address set on the device
Timeout period	Timeout duration for a connection test. The default value is 3s .

- Step 7** Click  on the toolbar to save the device information.

- Step 8** Click **Connection test** to start the connection test.

----End

6.5.9 Adding an rPDU

6.5.9.1 Setting Monitoring Parameters for HPXPDU2000-16-3PH-24-6-M1

Prerequisites

- You have obtained the device address planned for the PDU2000.
- The PDU2000 is connected to the collector, and digits are displayed on the LCD.

- You have obtained the collector IP address and login user name and password.
- A PC with an IP address in the same network segment as the collector has been prepared and connected to the collector over a switch.

Context

Before connecting the PDU2000 to the NetEco, set its device address and then modify the port parameters for the collector connecting to the PDU2000 to ensure that the values of **BaudRate**, **DataBit**, **StopBit**, and **Parity** on it are consistent with those for the collector port.

Procedure

Step 1 Press **MENU** on the PDU2000 display panel.

Step 2 Press **UP** until  is displayed and **ADD** blinks.

Step 3 Press **MENU**,  is displayed, and **01** blinks. The current device address is 01.

Step 4 Press **UP** or **DOWN** to select the device address value.

Step 5 Press **MENU** to confirm the setting.

- If  is displayed, the setting succeeds.
- If  is displayed, the setting fails. Reset the parameter.

NOTE

The PDU2000 **BaudRate**, **DataBit**, **StopBit**, and **Parity** cannot be set on the WebUI. Their values are **9600**, **8**, **1**, and **None** respectively.

Step 6 Press **Button**.  is displayed. Then press **MENU** to exit.

Step 7 Set RS485 port parameters for the collector based on the value of **BaudRate**, **DataBit**, **StopBit**, and **Parity** of the device. For ECC800-Pro collector settings, see [6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector](#).

----End

6.5.9.2 Creating an rPDU on the NetEco

Prerequisites

- You have logged in to the NetEco client.
- You have the operation rights for **Data Center Planning**.
- You have created a management domain for the device to be added on the **Data Center Planning** page.
- The ECC800-Pro connected to the device has been connected to the NetEco.

- Transparent transmission has been enabled for the COM port on the ECC800-Pro or UIM20A expansion module to which the device is connected.

Procedure

- Step 1** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 2** Select the management domain to add a device.
- Step 3** In the lower-left corner of the page, click the **Device** tab.
- Step 4** Click the drop-down list box in **Type** and select **PDU**.
- Step 5** Select the device to be added and drag its icon to the management domain.

NOTE

- If the management domain is a rack or DDF, click the management domain and choose **Design** under . The page for adding a device is displayed.
 - To delete a device, click the device and choose **Delete** under .
- Step 6** Click the device. In the device parameter area on the right, set device parameters according to the following table.

Table 6-61 MODBUS-RTU device parameter description

Parameter	Description
Managed Object Name	Device name
IP	Set this parameter to the IP address of the collector to which the device is connected.
Port	Set this parameter to the port through which the device connects to the collector. For details about the ports on the ECC800-Pro collector, see 6.5.1.4 Setting RS485 Parameters for the ECC800-Pro Collector .
Device Address	Set this parameter to the address set on the device.
Timeout period	Timeout duration for a connection test. The default value is 3s .

- Step 7** Click  on the toolbar to save the device information.
- Step 8** Click **Connection test** to start the connection test.

----End

7 Device Maintenance

7.1 Routine Maintenance

7.1.1 Monthly maintenance

7.1.1.1 Routine Maintenance for the Collector

Table 7-1 Routine maintenance for the PSU in the ECC800-Pro

Check Item	Expected Result	Troubleshooting
AC input	Input voltage: 200–240 V AC Frequency: 45-66 Hz	If the input voltage is abnormal, check the power grid and input cable connection.
Output voltage	Output voltage: 53.5 V DC (tolerance $\pm 5\%$)	If the output voltage is abnormal, check the load power and cable connection.
Indicator	The green indicator is steady on, and the red indicator is faulty.	Check the output voltage and determine whether the PSU is faulty. If the PSU is faulty, replace it.
Fan	No abnormal noise is generated.	If abnormal noise is generated, clean the fan.
Cable connection	The cable connection is secure.	Secure loose cables.
	Cables are not damaged.	Replace damaged cables.

Table 7-2 Routine maintenance for the main control module in the ECC800-Pro

Check Item	Expected Result	Troubleshooting
Indicator	The green indicator is steady on or blinking.	If the indicator is off or any abnormal condition occurs, see common faults and troubleshooting to rectify the fault.
Network port indicator	The green indicator is steady on, and the yellow indicator is blinking.	If the indicator status is abnormal, check the network cable connection.
Cable connection	The cable connection is secure.	Secure loose cables.
	Cables are not damaged.	Replace damaged cables.

7.1.1.2 Routine Maintenance for the UIM20A Expansion Module

Table 7-3 Routine Maintenance for the UIM20A Expansion Module

Item	Maintenance Interval	Method	Expected Result	Exception Handling
UIM20A expansion module ALM indicator	Monthly	Observe and check whether the ALM indicator on the UIM20A expansion module is normal.	The ALM indicator steady on.	If the indicator steady on, the UIM20A expansion module is faulty or the cables are not properly connected. Check the cables or replace the UIM20A expansion module.

7.1.1.3 Routine Maintenance for VCN

Table 7-4 Routine Maintenance for VCN

Item	Mainten ance Interval	Method	Expected Result	Exception Handling
Check the VCN indicator.	Monthly	Observe the VCN indicator.	The VCN indicator is steady green.	See the delivered documents.

7.1.1.4 Routine Maintenance for the Smoke Detector

Table 7-5 Routine Maintenance for the Smoke Detector

Item	Mainten ance Interval	Method	Expected Result	Exception Handling
Smoke detector indicator	Monthly	Observe and check whether the indicator on the smoke detector is normal.	The indicator blinks once every 6 seconds. (The interval varies with sensors. See the product instructions.)	If the indicator blinks twice every 6 seconds or does not blink, the smoke detector is faulty or the cables are not properly connected. Check the cables or replace the smoke detector.
Smoke detector availability	Monthly	Use a dedicated test instrument or a smoke generator to test the smoke detector. Blow smoke to the smoke detector probe and observe the indicator status.	- If the smoke density is below the alarm threshold, the alarm indicator blinks once every 6 seconds. - If the smoke density exceeds the alarm threshold, the alarm indicator is steady on.	- If the smoke density is below the alarm threshold but the alarm indicator blinks twice every 6 seconds, the smoke detector is faulty. Replace the smoke detector. - If the smoke density exceeds the alarm threshold but the alarm indicator is not steady on, replace the smoke detector.

 NOTE

You are advised to clean the smoke detectors every two years.

7.1.1.5 Routine Maintenance for the Hydrogen Detection System

Table 7-6 Routine Maintenance for the Hydrogen Detection System

Item	Maintenance Interval	Expected Result	Exception Handling
Check whether the hydrogen collector has generated alarms.	Monthly	The hydrogen collector is working properly, and no alarm is generated.	Troubleshoot by following instructions in documents delivered with the hydrogen collector.
Check the LCD of the hydrogen collector.	Monthly	The LCD displays the hydrogen density.	1. Check that the AC input power cable is normal. 2. Check whether the circuit breaker of the hydrogen collector can be switched on and off normally.
Check the indicator of the hydrogen collector.	Monthly	The RUN indicator is blinking.	1. If the indicator does not light up, check the AC input or replace the power module by following instructions in the delivered documents. 2. If the fault persists, contact Huawei technical support.

7.1.1.6 Routine maintenance for the region-type water sensor and water detection cable

Table 7-7 Routine maintenance for the region-type water sensor and water detection cable

Item	Maintenance Interval	Method	Expected Result	Exception Handling
Functions of the water sensor and water detection cable	Monthly	Place the water detection cable into water and check whether a water leakage alarm is generated by the water sensor.	A water leakage alarm is generated.	If no water leakage alarm is generated, replace the water detection cable.

7.1.1.7 Routine maintenance for the location-type water sensor and water detection cable

Table 7-8 Routine maintenance for the location-type water sensor and water detection cable

Item	Maintenance Interval	Method	Expected Result	Exception Handling
Functions of the water sensor and water detection cable	Monthly	Place the water detection cable into water and check whether a water leakage alarm is generated by the water sensor.	A water leakage alarm is generated.	When there is no water leakage alarm generated, replace the water sensor if the sensor sends an alarm, and replace the water detection cable if the detection cable sends an alarm.

7.1.1.8 Routine Maintenance for Infrared Sensors

Table 7-9 Routine maintenance for infrared sensors

Maintenance Item	Maintenance Interval	Method	Check Standard	Troubleshooting
Infrared sensor	Monthly	The monitoring personnel walk past the monitoring range of the infrared sensor at a speed of 1 m/s. If the red indicator turns on, the sensor enters the alarm state. If the indicator turns off, the sensor enters the monitoring state again.	The infrared sensor indicator works normally and reports alarms.	If the infrared sensor cannot work normally, replace it.

7.1.2 Semi-Annual Maintenance

7.1.2.1 Routine maintenance for the switch

Table 7-10 Routine maintenance for the switch

Item	Maintenance Interval	Method	Expected Result	Exception Handling
LAN switch availability	Semi-annually	Check the power indicator (marked PWR) of the switch. Check the running indicator (marked SYS) of the switch.	The PWR indicator is steady green. The SYS indicator is blinking green.	Take corrective measures based on the PWR indicator status: - Off: The power supply unit (PSU) is not detected, or the board power supply is abnormal when the switch is configured with one PSU. - Steady red, The possible causes are as follows: Two PSUs configured on the switch are detected, but the circuit breaker is off. The power supply is disconnected. Both the board and power over Ethernet (PoE) power supplies are faulty. - Steady orange: When the switch is configured with one PSU, the PoE power supply is abnormal. When the switch is configured with two PSUs, the board or PoE power supply is abnormal. Take corrective measures based on the SYS indicator status: - Off: The switch is not running. - Steady green: The switch is not running properly or is starting. - Steady orange: The indicator takes a self-test during startup. - Steady red: The switch does not run properly after being registered, or alarms indicating that the power supply, fan, or temperature is abnormal are generated.

7.1.2.2 Routine Maintenance for the Smart U space manager

Table 7-11 Routine Maintenance for the Smart U space manager

Item	Mainten ance Interval	Method	Expected Result	Exception Handling
Check the availability of the smart U space manager.	Semi-annually	If there is a U Asset Label on the asset detection strip, check the corresponding indicator on the asset detection strip.	The indicator on the asset detection strip that has U Asset Label is on.	If the indicator is off, check whether the cable of the asset detection strip is loose. Otherwise, replace the asset detection strip.

7.1.2.3 Routine Maintenance for Temperature Sensors

Table 7-12 Routine Maintenance for Temperature Sensors

Item	Maintena nce Interval	Method	Expected Result	Exception Handling
Check the availability of the temperature sensor.	Semi-annually	Hold the temperature sensor probe in your palm, and check the temperature displayed for the corresponding rack environment unit on the WebUI.	Hold the temperature sensor probe in your palm, and check the temperature displayed for the corresponding rack environment unit on the WebUI.	If the temperature does not go up, check whether the temperature sensor cable is loose or disconnected. If so, reconnect the cable. If not, replace the temperature sensor.

7.1.2.4 Routine maintenance for the temperature and humidity sensor

Table 7-13 Routine maintenance for the temperature and humidity sensor

Item	Mainten ance Interval	Method	Expected Result	Exception Handling
Check the availability of the temperature and humidity sensor.	Semi-annually	Check the reading on the temperature and humidity sensor.	The reading is normal and accurate.	If the reading is inaccurate, check and calibrate the temperature and humidity sensor using a temperature and humidity measuring instrument with higher precision.

7.1.2.5 Routine maintenance for the camera

Table 7-14 Routine maintenance for the camera

Item	Mainten ance Interval	Method	Expected Result	Exception Handling
Camera availability	Semi-annually	On the NetEco, click Configuration > Camera Management > Video Camera Management , to enter the camera management page. Type the camera name or IP address to find the camera, and click the camera name or icon  on the left to view the real-time monitoring page.	A monitoring page is displayed.	If the monitoring page is not displayed, check whether the IP address is correctly set and the PoE function is enabled on the LAN switch. Then check the cables or replace the camera. For details about how to replace a camera.

7.1.2.6 Routine maintenance for the access control system

Table 7-15 Routine maintenance for the access control system

Item	Mainten ance Interval	Method	Expected Result	Exception Handling
Card reader	Semi- annually	Use a spare card reader to check whether the access control system works properly.	The card reader functions properly.	If the access controller fails to operate properly, replace the card reader.
Door status sensor	Semi- annually	Power on the door status sensor and check whether the door has strong attracting capability.	The door status sensor functions properly.	If the door status sensor fails to attract properly, replace the sensor.

7.1.2.7 Routine Maintenance for the Access Controller

Table 7-16 Routine maintenance for the access controller

Item	Maintenance Interval	Method	Expected Result	Exception Handling
Access controller function	Semi-annually	Check whether the access controller works properly by referring to the installatio n guide.	The access controller works properly.	If the access controller fails to operate properly, replace the controller.

7.1.2.8 Routine maintenance for the single-door/double-door magnetic lock

Table 7-17 Routine maintenance for the single-door/double-door magnetic lock

Item	Maintenance Interval	Method	Expected Result	Exception Handling
Functions of the single-door/double-door magnetic lock	Semi-annually	Check whether the magnetic lock attracts and separates properly when being powered on and off respectively.	The magnetic lock attracts and separates properly.	If the magnetic lock fails to attract or separate properly, replace the lock.

7.1.2.9 Routine maintenance for the emergency door release button

Table 7-18 Routine maintenance for the emergency door release button

Item	Maintenance Interval	Method	Expected Result	Troubleshooting
Emergency door release button function	Semi-annually	Check whether the glass plate for the emergency door release button is intact.	The glass plate for the emergency door release button is intact.	If the emergency door release button is broken, replace the button.

7.2 Parts Replacement

7.2.1 Parts Replacement for the ECC800-Pro

7.2.1.1 Replacing an ECC800-Pro Main Control Module

Prerequisites

NOTICE

- The ECC800-Pro main control module is hot-swappable.
- Before disconnecting cables from the ECC800-Pro main control module, label the cables based on the corresponding ports.

- Tools: ESD wrist strap, ESD gloves, Phillips screwdriver, labels, marker
- Materials: a new undamaged and undeformed ECC800-Pro main control module of the appropriate model

Procedure

Step 1 Log in to the ECC800-Pro WebUI as an administrator.

Step 2 Use the **Back Up Current Settings** function to record the ECC800-Pro configuration information or manually record the information.

Path: **Maintenance > Configuration File > Back Up Current Settings**

NOTE

If the main control module is damaged, you may fail to log in to the ECC800-Pro. In this case, you cannot back up the settings.

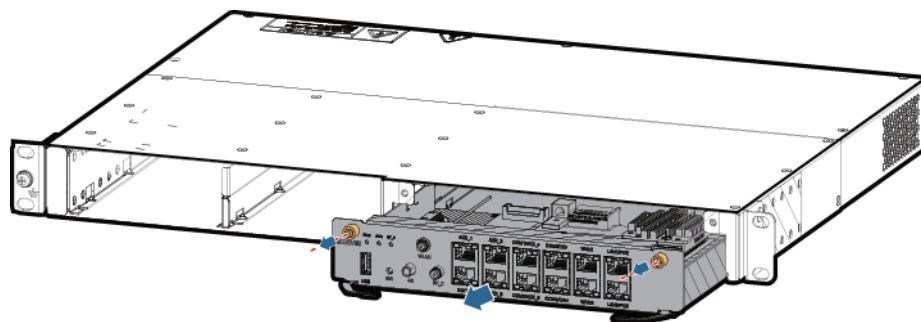
The following information cannot be backed up: monitoring module IP address parameters, smart module certificate, NetEco certificate, NetEco second-challenge password, time configuration parameters, access user management, access permission management, device access certificate, log, and user configuration information.

Step 3 Label each cable and antenna based on the corresponding ports on the ECC800-Pro main control module.

Step 4 Remove cables, USB flash drive, USB-to-WiFi module, and antennas from the ECC800-Pro main control module.

Step 5 Loosen the screws on both sides of the ECC800-Pro main control module and pull the handles on both sides of the ECC800-Pro main control module to remove the main control module.

Figure 7-1 Removing the ECC800-Pro main control module

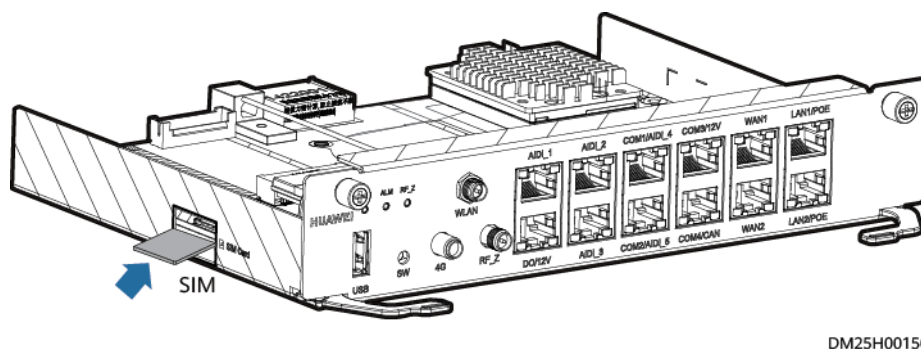


DM02H00026

Step 6 (Optional) Remove the SIM card from the corresponding slots of the ECC800-Pro main control module.

Step 7 (Optional) Install the removed SIM card in the corresponding slot of the new ECC800-Pro main control module.

Figure 7-2 Installing a SIM card



- Step 8** Install the spare ECC800-Pro main control module in the ECC800-Pro subrack and tighten the screws on both sides of the ECC800-Pro main control module.
- Step 9** Connect the communications cables and antennas to the ECC800-Pro main control module.
- Step 10** Choose **Maintenance > Configuration File** and import the backup configuration file, or set parameters for the devices that connect to the ECC800-Pro to ensure normal communication.

----End

7.2.1.2 Replacing an ECC800-Pro PSU

Prerequisites



DANGER

Do not touch the terminals in the rear of a removed PSU to avoid electric shocks.

- Tool: insulation gloves
- Materials: a reserved undamaged and undeformed PSU of the appropriate model.

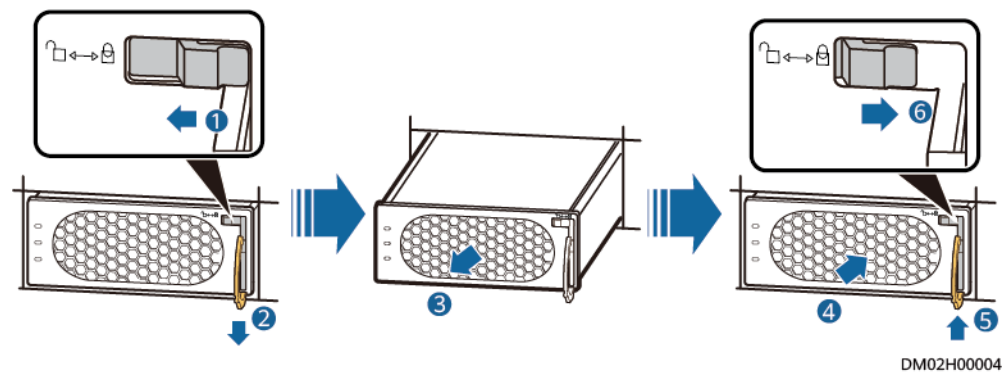
Context

The PSU is hot-swappable.

Procedure

- Step 1** Push the locking latch in the upper right corner of the PSU panel leftwards.
- Step 2** Pull out the handle of the PSU to remove the PSU from the subrack.
- Step 3** Gently push the reserved PSU into the subrack along guide rails, and push the locking latch rightwards to secure the handle.

Figure 7-3 Replacing a PSU



----End

7.2.1.3 Replacing ECC800-Pro Antennas

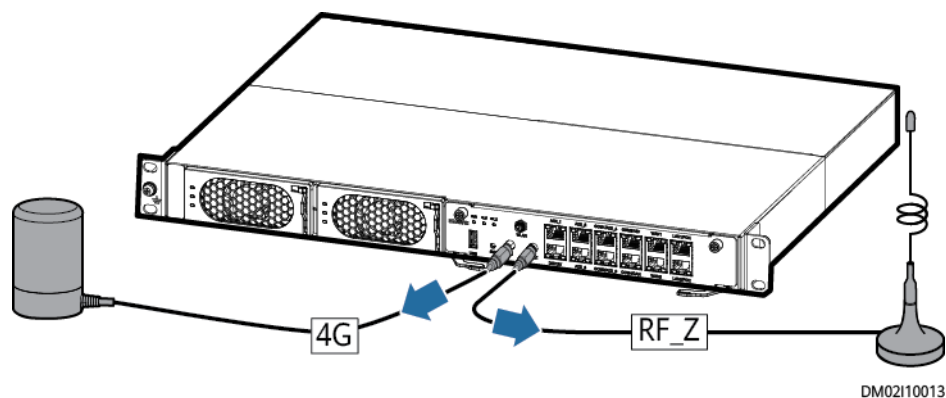
Prerequisites

- Tools: ESD wrist strap, ESD gloves
- Materials: Spare ECC800-Pro antennas of the same model are available and functional.

Procedure

- Step 1** Remove the 4G antenna cables and RF_Z antenna cables connected to the ports on the ECC800-Pro, as shown in [Figure 7-4](#).

Figure 7-4 Removing antennas



- Step 2** Install the spare 4G antenna cables and RF_Z antenna cables in the original positions and connect them to the ECC800-Pro.

----End

7.2.1.4 Replacing a SIM Card

Prerequisites

- Tools: ESD wrist strap, ESD gloves
- Materials: A spare SIM card of the same model is available and functional.

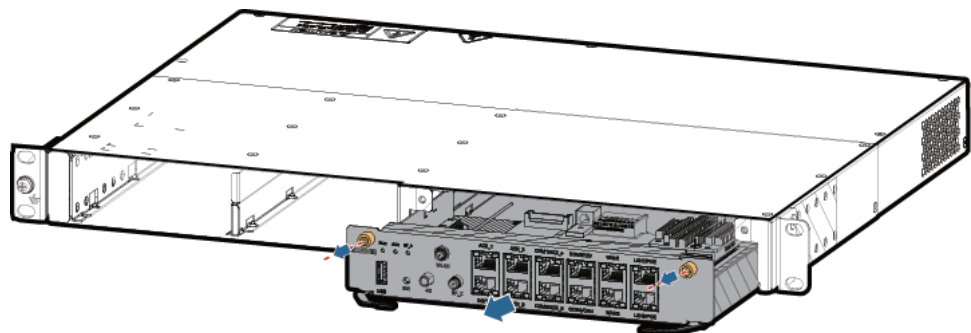
Procedure

Step 1 Record the position of the signal cable connected to the ECC800-Pro main control module panel, and then disconnect the signal cable.

Step 2 Loosen the screws on both sides of the ECC800-Pro main control module.

Step 3 Pull the handles on both sides of the ECC800-Pro main control module, and to remove the main control module.

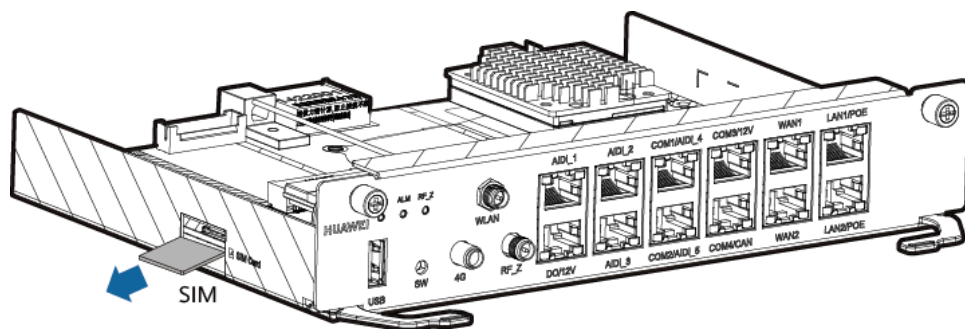
Figure 7-5 Removing the ECC800-Pro main control module



DM02H00026

Step 4 Remove the SIM card from the card slot.

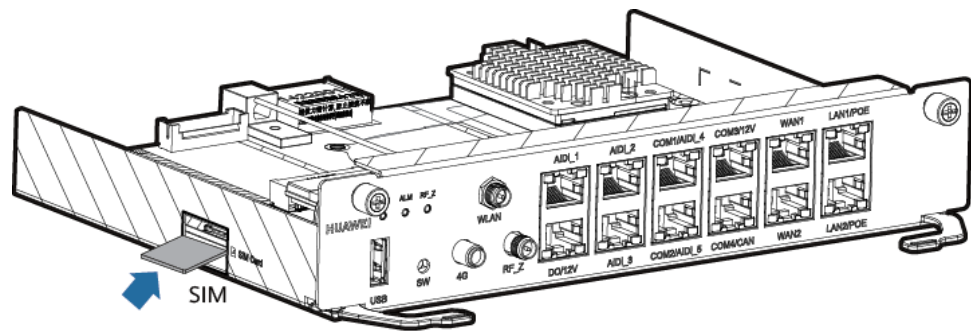
Figure 7-6 Removing a SIM card



DM25H00151

Step 5 Insert the spare SIM card into the card slot.

Figure 7-7 Installing a SIM card



DM25H00150

Step 6 Install the ECC800-Pro main control module in the card slot.

Step 7 Tighten the screws on both sides of the ECC800-Pro main control module.

Step 8 Reconnect signal cables to the ECC800-Pro main control module panel based on the recorded information.

----End

7.2.2 Replacing a UIM20A expansion module

Prerequisites

- Tools: Phillips screwdriver, label, marker
- Material: UIM20A expansion module

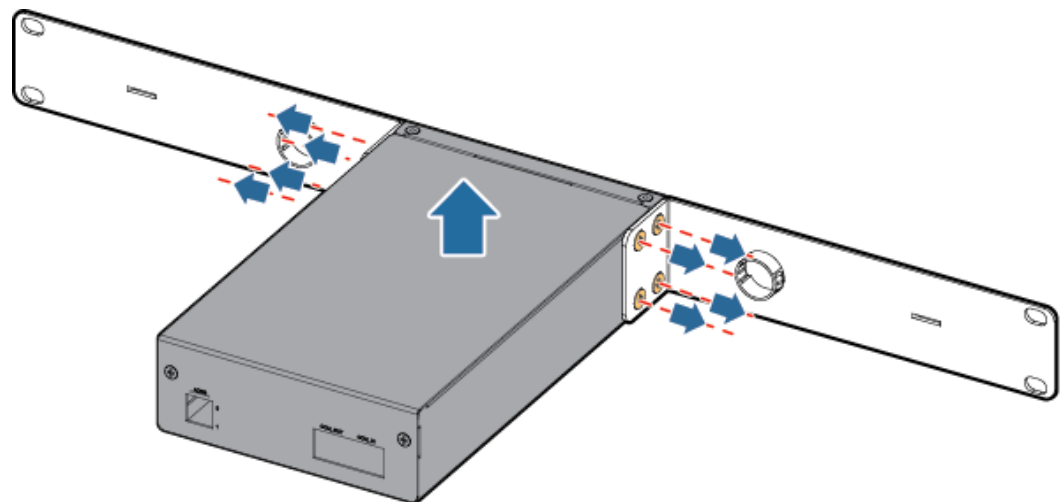
Procedure

Step 1 Label each cable based on the corresponding ports on the UIM20A expansion module.

Step 2 Disconnect cables from the UIM20A expansion module.

Step 3 Unscrew the mounting ears from the two sides of the UIM20A expansion module, and remove the UIM20A expansion module.

Figure 7-8 Removing a UIM20A



DM05H00037

- Step 4** Secure a mounting ear to each of the two sides of the spare UIM20A expansion module using four M4 screws, and then secure the spare UIM20A expansion module to the original installation position.
- Step 5** Connect cables to the UIM20A expansion module based on the cable labels.
- Step 6** Synchronize parameters of the UIM20A expansion module on the ECC800-Pro WebUI.
- Step 7** On the ECC800-Pro WebUI, choose **Monitoring > System > ECC800 > Controls > Delete device with communication failure**, and click **Submit**.
- Step 8** Log in to the ECC800-Pro WebUI, and check the parameters and communication status of the UIM20A expansion module to ensure that the communication is normal.

----End

7.2.3 Replacing a Smart U Space Manager (Connected to a UIM20A Expansion Module) (BOM Number: 52273314)

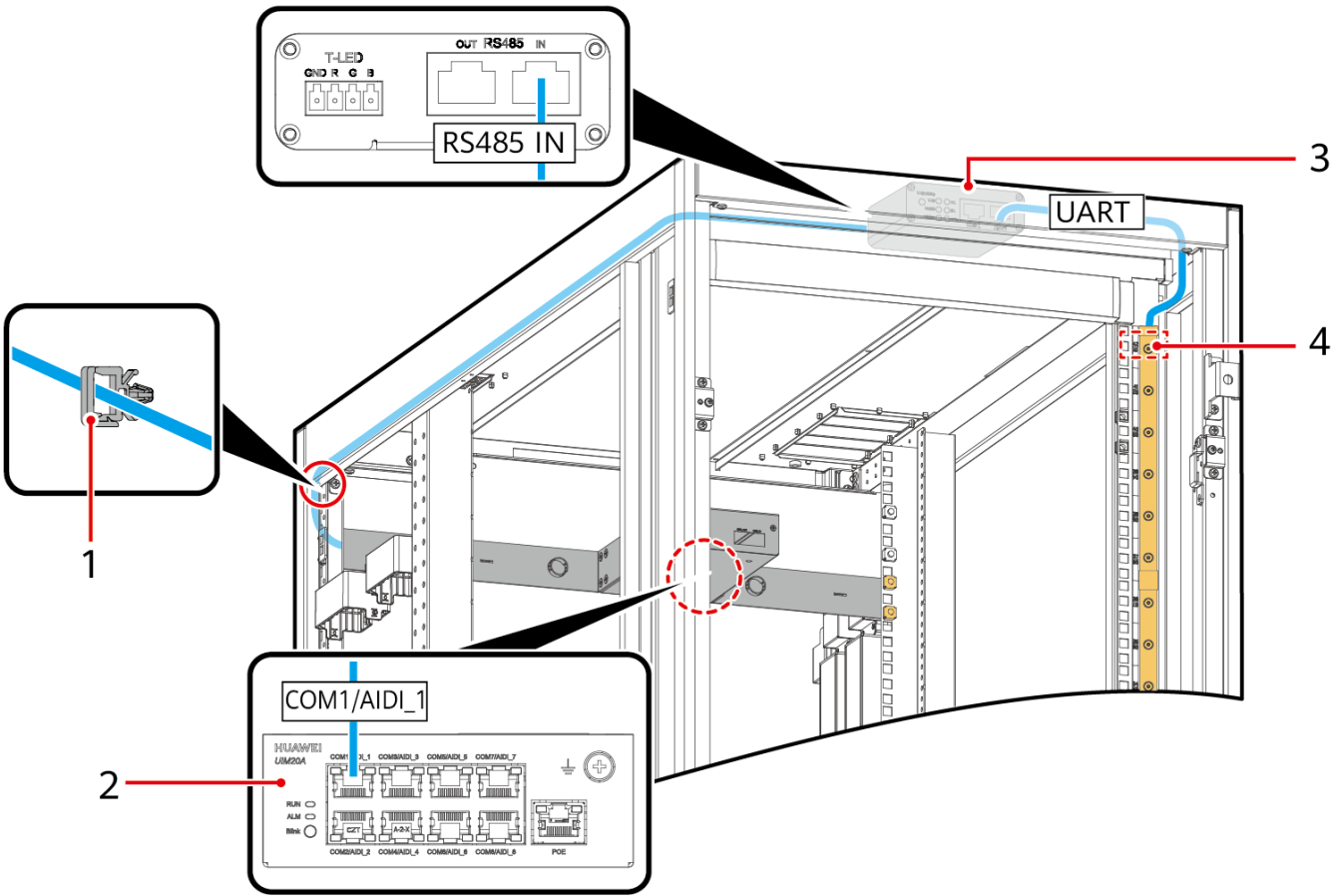
Impact on the System

The U space status of the equipment cannot be displayed during replacement.

Preparations

- Tools: ESD gloves, label, marker
- Material: smart U space manager

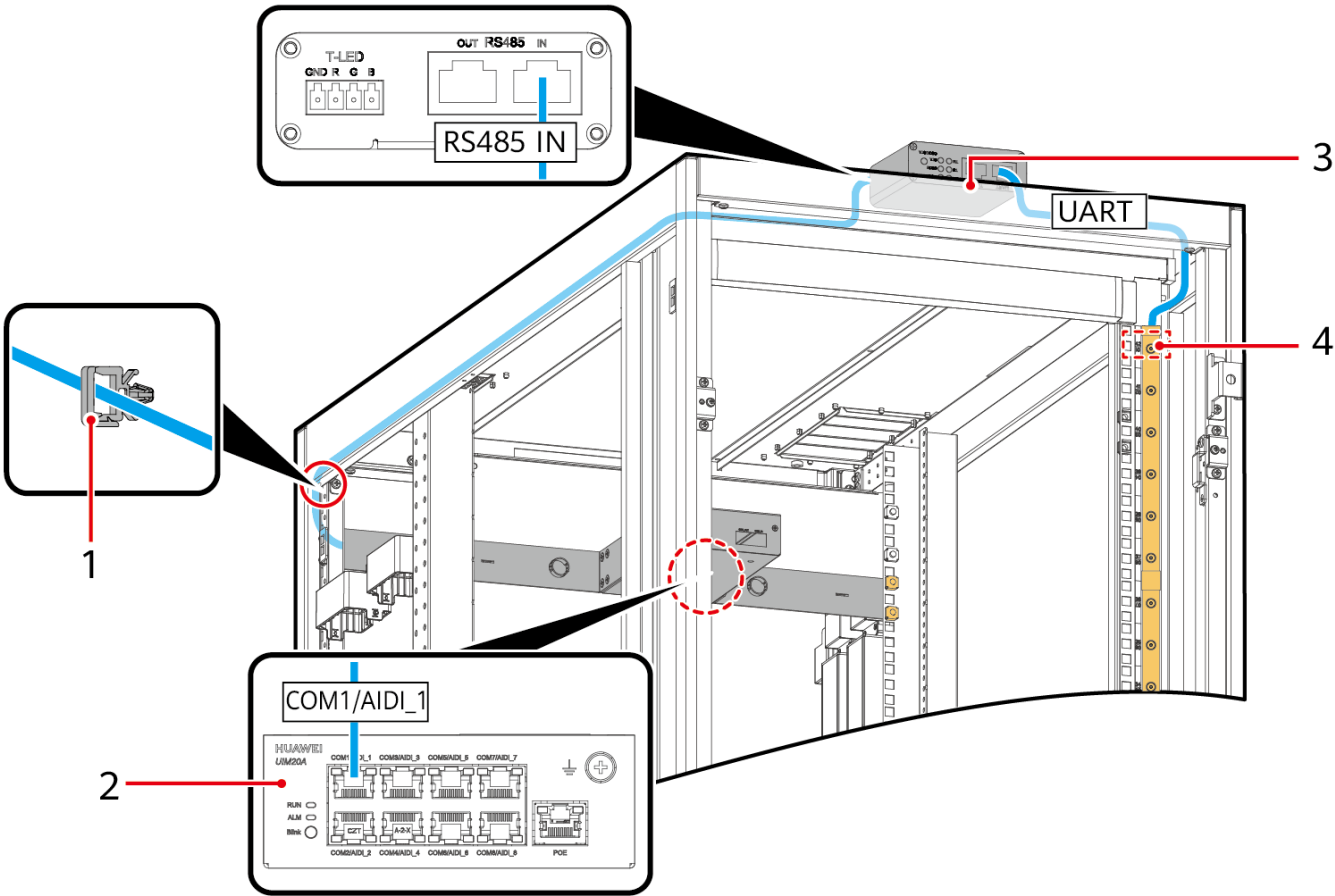
Figure 7-9 Installing a smart U space manager (main control box attached to the top of the cabinet interior)



DF17110003

(1) Fastener	(2) UIM20A expansion module	(3) Main control box
(4) Asset detection strip (42 U detection point)	-	-

Figure 7-10 Installing a smart U space manager (main control box attached to the top of the cabinet exterior)



DF17110004

(1) Fastener	(2) UIM20A expansion module	(3) Main control box
(4) Asset detection strip (42 U detection point)	-	-

Procedure

Step 1 (Optional) If U space e-labels are faulty, perform the following steps to replace them.

1. Remove faulty U Asset Label from the customer equipment and the asset detection strip.
2. Record the asset according to the commissioning guide.

Step 2 (Optional) If the asset detection strip is faulty, perform the following steps to replace it.

1. Label the position of each U space e-label on the asset detection strip.
2. Remove all U space e-labels from the asset detection strip.

3. Remove the faulty asset detection strip.
4. Install a new asset detection strip in the original position.
5. Install the U space e-labels in the original positions based on the position labels.

Step 3 (Optional) If the main control box is faulty, perform the following steps to replace it.

1. Label each cable based on the corresponding ports on the main control box.
2. Remove the faulty main control box.
3. Install a new main control box in the original position.
4. Connect the cables to the new main control box based on the cable labels.

----End

7.2.4 Replacing Sensors

7.2.4.1 Replacing a Temperature Sensor

Prerequisites

- Recommended tools and materials: diagonal pliers, insulation tape, cable tie, step ladder (2 m).
- A temperature sensor needs to be replaced.
- Spare temperature sensors of the same model are available and functional.

Procedure

Step 1 Cut the cable ties on the temperature sensor using diagonal pliers, and remove the network cable from the temperature sensor.

Step 2 Install the spare temperature sensor, bind it to the original position using cable ties, and connect cables to it.

NOTICE

- When installing temperature sensors, bind the cables behind the sensors to the cable bridge, keeping them 20 mm away from the sensor probes.
 - Temperature sensors must not be in touch with metal parts or cabinets.
 - Keep the temperature sensors facing the inside of the cabinets to ensure accurate measurement of cabinet interior temperatures.
-

----End

7.2.4.2 Replacing the Hydrogen Detection System

Prerequisites

- The hydrogen detection system needs to be replaced.
- A spare hydrogen detection system of the same model is available and functional.

Preparations



Do not operate with power on. Take appropriate insulation measures.

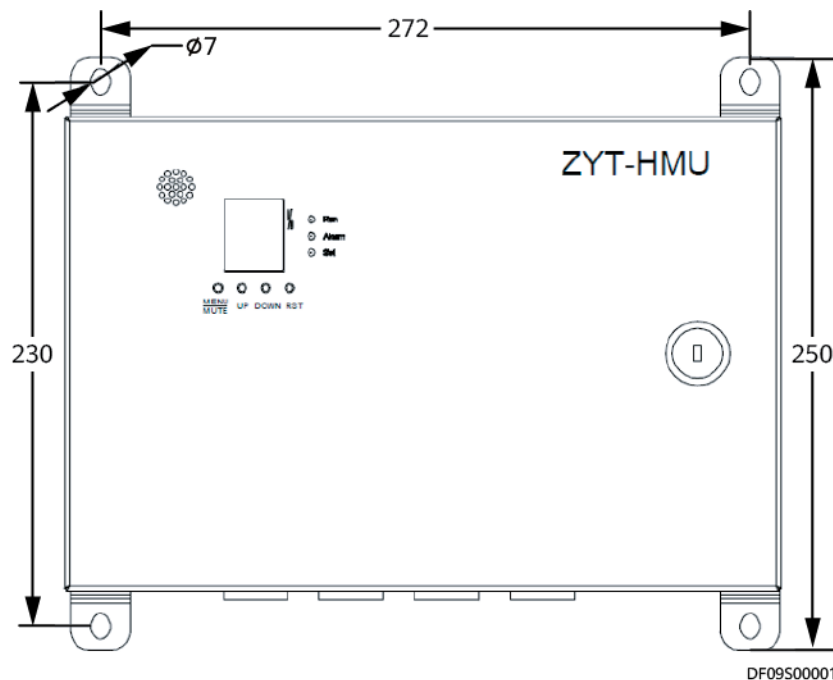
Tools: Phillips screwdriver, adjustable wrench, protective gloves

Materials: spare hydrogen detection system

Procedure

- Step 1** Switch off the upstream circuit breaker of the hydrogen detection system to power off the hydrogen detection system.
- Step 2** Remove cables from the hydrogen detection system.
- Step 3** Use a Phillips screwdriver to loose nuts on the mounting ears and remove the faulty hydrogen detection system.
- Step 4** Align the four mounting ears of the new hydrogen detection system with the expansion bolts, and tighten the M6 nuts.

Figure 7-11 Installing a hydrogen detection system



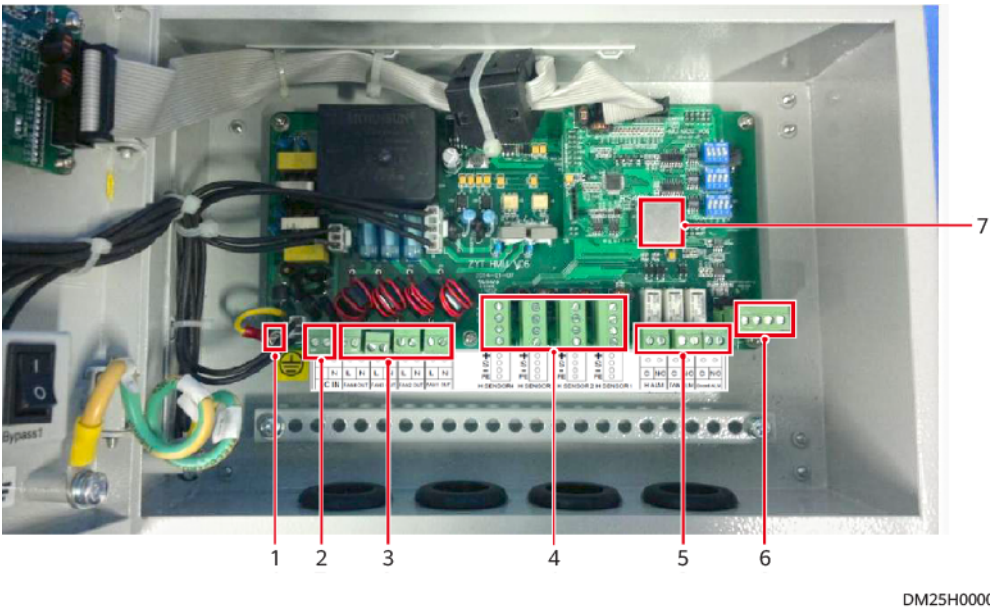
- Step 5** According to the silk screen and [Figure 7-12](#), connect the ground cable to (1), input power cable to (2), fan cables to (3), and hydrogen sensor cables to (4).

Step 6 Prepare one end of a network cable according to [Table 7-19](#), and connect the cable to (7).

DANGER

Pay attention to the negative and positive polarities of the power supply. If the polarities are connected incorrectly, the device may be burned.

Figure 7-12 Connecting cables



(1) PE	(2) AC IN	(3) Output ports for fan 1 to fan 4
(4) Output ports for hydrogen sensor 1 to hydrogen sensor 4	(5) Hydrogen concentration alarm port, fan alarm port, and hardware fault port (reserved ports)	(6) RS485+, RS485-, GND, and idle ports (reserved ports)
(7) RS485	-	-

Table 7-19 Pin mapping for the RS485 port

Pin	Signal	Function
Pin 1 (orange-white)	D+	RS485+
Pin 2 (orange)	D-	RS485-
Pin 3 (green-white)	12V+	12+ input

Pin	Signal	Function
Pin 4 (blue)	NC	-
Pin 5 (blue-white)	NC	-
Pin 6 (green)	NC	-
Pin 7 (brown-white)	NC	-
Pin 8 (brown)	12V-	12- input

Step 7 Switch on the circuit breaker of the hydrogen detection system, and check whether it is working properly.

NOTE

If the hydrogen density displayed on the hydrogen detection system, the hydrogen detection system is working properly.

----End

Follow-up Procedure

Dispose of the removed hydrogen detection system that is confirmed faulty.

7.2.4.3 Replacing a Smoke Detector

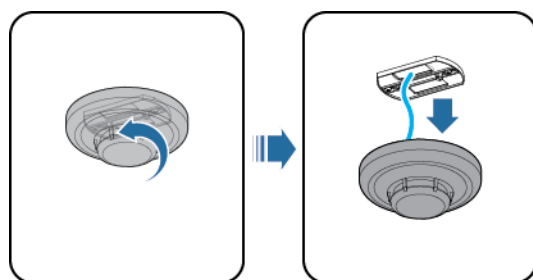
Prerequisites

- Recommended tools and materials: Phillips screwdriver, insulation tape, step ladder (2 m).
- A smoke detector needs to be replaced.
- A spare smoke detector of the same model is available and functional.

Procedure

Step 1 Rotate the smoke detector to remove it from the base.

Figure 7-13 Removing a smoke detector



DF02H00018

Step 2 Remove the cables from the smoke detector and apply insulation measures such as wrapping the cables with insulation tape to avoid hazards.

- Step 3** Install a new smoke detector and reconnect the cables.
- Step 4** Install the new smoke detector to the base by rotating it in a direction opposite to [Step 1](#).
- Step 5** Blow smoke towards the smoke detector using a smoke pistol until the smoke detector indicator changes from blinking once every 6s to steady on. If a smoke detector fire alarm is triggered, the smoke detector is functional.
- End

7.2.4.4 Replacing a T/H Sensor

Prerequisites

- Recommended tools: Phillips screwdriver, flat-head screwdriver
- A T/H sensor needs to be replaced.
- A spare T/H sensor of the same model is available and functional.

Procedure

- Step 1** Remove cables from the T/H sensor.
- Step 2** Remove the T/H sensor from its base.

NOTICE

After removing cables, wrap exposed terminals with insulation tape and do not block cable labels. If cable labels are blocked, cables may be connected incorrectly.

- Step 3** Install a new T/H sensor onto the base.

NOTICE

Before removing a T/H sensor, remember the DIP switch setting on it. When you install a new T/H sensor, you need to set the same DIP switch setting for the new one.

- Step 4** Reconnect cables to the new T/H sensor.

----End

7.2.4.5 Replacing a Region-type Water Sensor and Water Detection Cable

Prerequisites

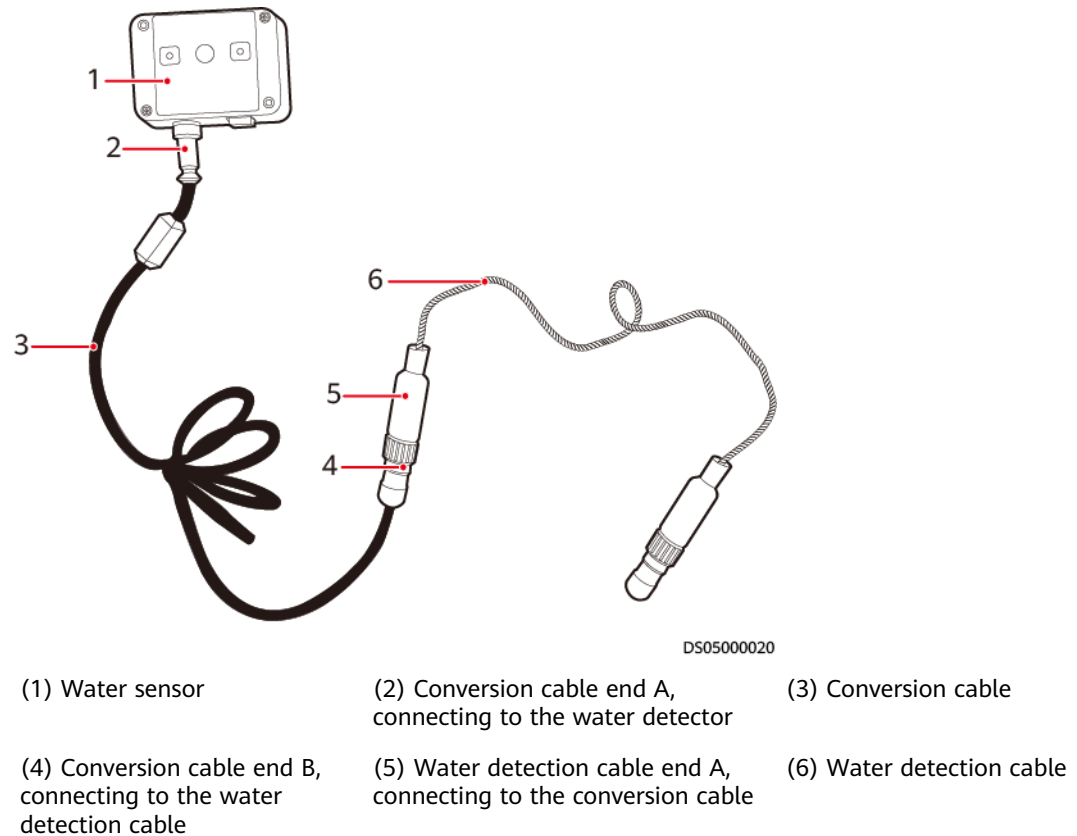
- The water sensor needs to be replaced.
- A spare water sensor of the same model is available and functional.

Context

Prepare a water sensor or water detection cable of the same model.

A water sensor consists of a water detection cable, water detector, and conversion cable. The water detection cable is laid out on the floor, connecting to the water detector placed near the collector by the conversion cable. **Figure 7-14** shows the components.

Figure 7-14 Water sensor components



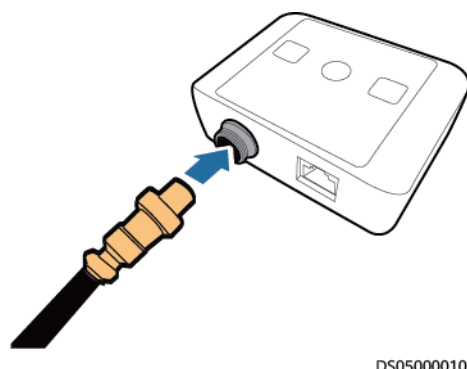
Recommended tool and material: crimping tool

Procedure

Step 1 Replace the water sensor.

1. Remove the conversion cable at the conversion port for the water sensor and conversion cable.
2. Connect a new water sensor to the conversion cable, as shown in **Figure 7-15**.
3. Secure the new water sensor.

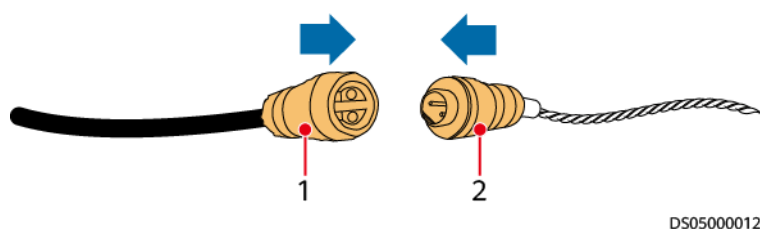
Figure 7-15 Connecting a conversion cable to a water sensor



Step 2 Replace a water detection cable.

1. Remove the faulty water detection cable from the port.
2. Install a new water detection cable, as shown in [Figure 7-16](#).

Figure 7-16 Connecting a new water detection cable



(1) Conversion cable end B, connecting to the water detection cable

(2) Water detection cable end A, connecting to the conversion cable

NOTE

The water detection cable and conversion cable are interconnected through the male and female connectors.

----End

Follow-up Procedure

Check whether the new water sensor works properly. Connect the network cable between the water detector and the ECC800-Pro, immerse the water detection cable in water, and check whether an alarm is generated. If an alarm is generated, the replacement is complete.

7.2.4.6 Replacing a Location-type Water Sensor and Water Detection Cable

Prerequisites

- The water sensor needs to be replaced.
- A spare water sensor of the same model is available and functional.

Context

- Prepare a location-type water sensor or water detection cable of the same model.
- The location-type water sensor consists of a water leakage locator, tieline, and water leakage location cable. The water detection cable is laid out on the floor. The liquid level sensor is deployed around the collector. The water detection cable and the liquid level sensor are connected using the lead wire.
- Recommended tool and material: crimping tool

Procedure

Step 1 Replace the water sensor.

1. Pull out the water detection cable from the lead wire port on the water leakage locator.
2. Remove the water leakage locator from the DIN guide rail.
3. Install the new water leakage locator on the DIN guide rail with the latch facing upwards.

NOTE

- Touch grounded devices or pipes to eliminate ESD before taking the water sensor module.
 - Place it gently. Prevent it against mechanical impact and collision. Keep it dry.
 - Prevent it against metal filings, grease, pipe paint, and other contaminants.
4. Connect one end of the black quick-connect terminal of the lead wire from the liquid level sensor to the location-type water detection cable, and connect the other end of the quick-connect terminal to the sensor.

Step 2 Replace a water detection cable.

1. Remove the faulty water detection cable from the port.
2. Install a new water detection cable.

----End

Follow-up Procedure

Check whether the new location-type water sensor works properly. Connect the network cable between the water sensor and the ECC800-Pro, immerse the water detection cable in water, and check whether an alarm is raised. If an alarm is raised, the replacement is complete.

7.2.4.7 Replacing an Infrared Sensor

Prerequisites

- The ESD wrist strap, protective gloves, ESD box or bag, cabinet door key, and required tools are available.
- The new infrared sensor is intact.

Procedure

- Step 1** Connect the ground cable of the ESD wrist strap, and wear the ESD wrist strap and ESD gloves.
 - Step 2** Disconnect the signal and power cables from the infrared sensor and record the cable connection positions.
 - Step 3** Remove the infrared sensor from the support buckle.
 - Step 4** Connect the signal and power cables for the new infrared sensor according to the information you recorded.
 - Step 5** Mount the new infrared sensor on the support buckle and adjust the sensor angle.
- End

7.2.5 Replacing the Management System

7.2.5.1 Replacing the VCN510 Hard Disk

Prerequisites

- The hard disk needs to be replaced.
- Data in the hard disk has been backed up.
- A spare hard disk of the same model is available and functional.
- Before replacing a faulty disk, ensure that the power switch on the rear panel is off and disconnect the power cable to power off the device.

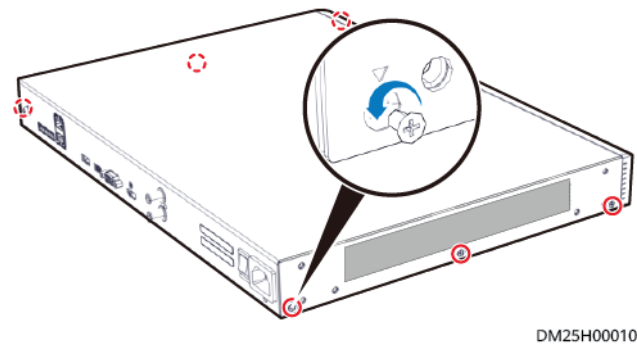
Context

Recommended tools and materials: Phillips screwdriver, ESD wrist strap (or ESD gloves).

Procedure

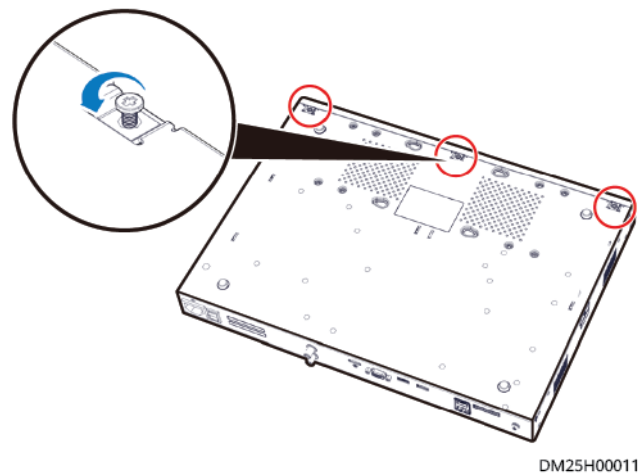
- Step 1** Put on an ESD wrist strap (or ESD gloves) and insert the ground terminal into the ESD jack in the cabinet.
- Step 2** Remove the faulty hard disk.
 1. Use a Phillips screwdriver to loosen three fastening screws on the left and right of the subrack cover.

Figure 7-17 Removing screws



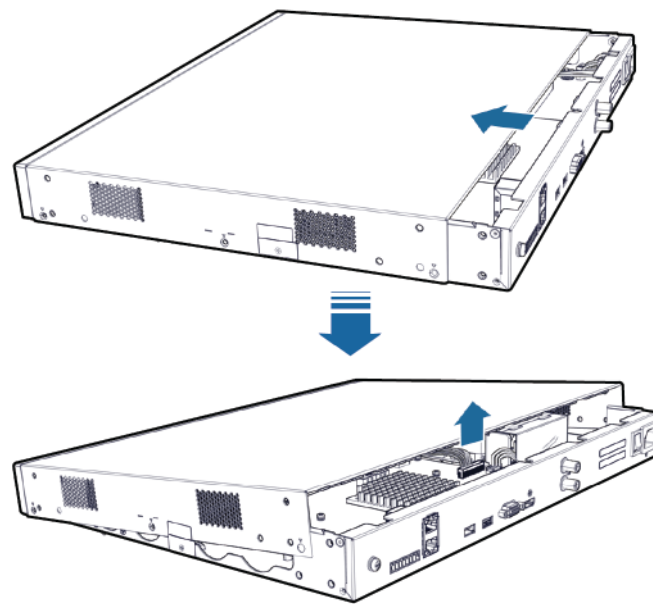
2. Use a Phillips screwdriver to loosen the three screws that secure the lower cover of the chassis to the front panel.

Figure 7-18 Removing screws



3. Remove the upper cover of the chassis as follows: Hold the lower cover of the chassis with one hand, and push the upper cover of the chassis toward the rear panel with the other hand. Then remove the upper cover with both hands.

Figure 7-19 Removing the upper cover of the chassis



DM25H00012

NOTE

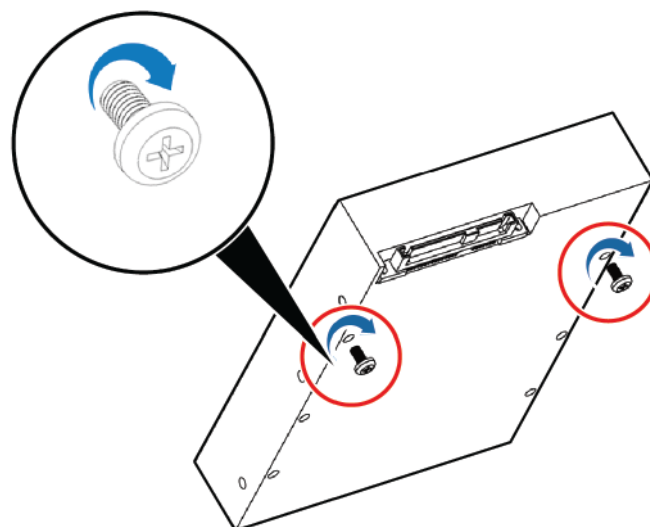
When removing the upper cover from the chassis, do not use one hand to perform this operation. Otherwise, the upper cover may collide with the components inside the device, bringing risks of component damage.

4. Loosen the screws that are used to fix the disk at the back of the device, remove the power and SATA cables from the disk, and remove the disk.

Step 3 Install a new hard disk.

1. Take two removed screws, and preinstall the two screws in the holes near the cable outlet on the hard disk backplane. Tighten the screw threads for three circles (ensure that the screws do not fall naturally).

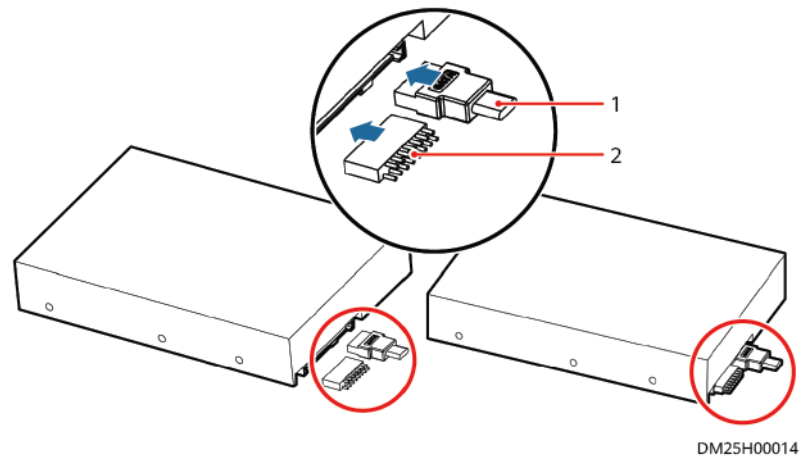
Figure 7-20 Installing hard disk screws



DM25H00013

2. Insert the SATA and power cables into the corresponding ports on the hard disk. During cable connection, ensure that the metallic plate of the SATA cable faces upward.

Figure 7-21 Installing SATA and power cables



(1) SATA cable

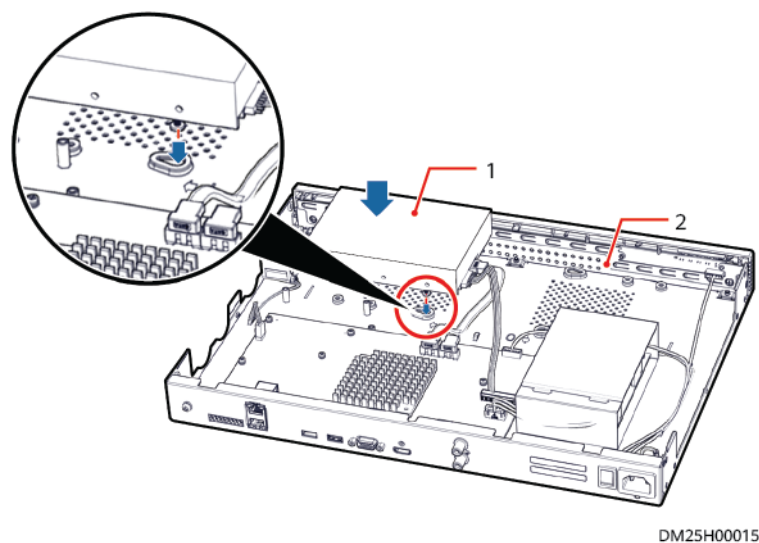
(2) Power cable

NOTE

When the VCN510 is delivered, the SATA cable connecting to the hard disk is fixed using blue tapes. Before installing the hard disk, remove the tapes.

3. Install a disk in No. 1 position. Place the disk above the No. 1 disk installation position. Align the preinstalled screws with the cucurbit holes on the bottom cover of the chassis. Then, horizontally place the disk. Ensure that the screws are in the holes.

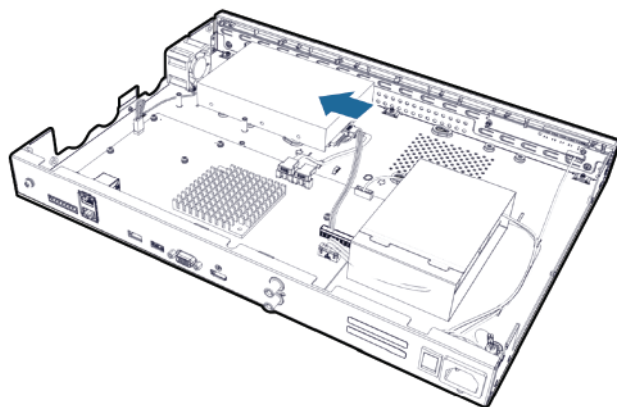
Figure 7-22 Hard disk installation positions



(1) No. 1 disk installation position (2) No. 0 disk installation position

4. Push the disk to slide the two preinstalled screws into the small holes of the cucurbit holes.

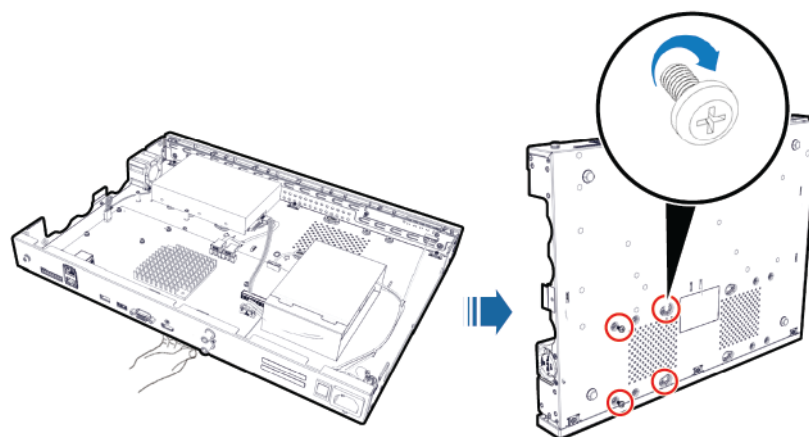
Figure 7-23 Installing a hard disk



DM25H00016

5. Hold the disk with one hand, turn the device 90 degrees with the other hand, and tighten the preinstalled screws from the rear panel of the device. Take another two screws removed from the disk. Insert them into another two holes on the disk (for a disk with six holes, you are advised to install the screws into the two holes that are far away from the cable outlet) and tighten them.

Figure 7-24 Installing a hard disk



DM25H00017

6. Hold the disk with one hand, turn the device 90 degrees with the other hand, and tighten the preinstalled screws from the rear panel of the device. Take another two screws removed from the disk. Insert them into another two holes on the disk (for a disk with six holes, you are advised to install the screws into the two holes that are far away from the cable outlet) and tighten them.
7. Install the upper cover of the chassis. Place the upper cover of the chassis. Fasten the three screws on the bottom cover of the chassis and the six screws on the left and right sides of the chassis to fix the upper cover of the chassis.

- Step 4** Check the hard disk indicators to determine whether the new hard disk works properly.

----End

Follow-up Procedure

If the new hard disk is abnormal, immediately contact Huawei technical support engineers.

7.2.5.2 Replacing the VCN520/VCN540 Hard Disk

Prerequisites

- The hard disk needs to be replaced.
- Data in the hard disk has been backed up.
- A spare hard disk of the same model is available and functional.
- Before replacing a faulty disk, ensure that the power switch on the rear panel is off and disconnect the power cable to power off the device.

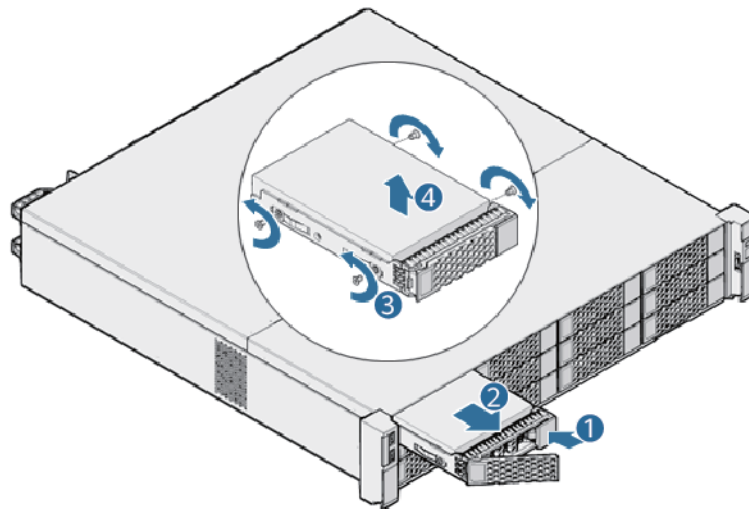
Context

Recommended tools and materials: Phillips screwdriver, ESD wrist strap (or ESD gloves).

Procedure

- Step 1** Put on an ESD wrist strap (or ESD gloves) and insert the ground terminal into the ESD jack in the cabinet.
- Step 2** Remove the faulty hard disk.
1. Press the button on the hard disk panel to open the ejector lever.
 2. Pull out the hard disk for about 3 cm, wait for 30 seconds at least until the hard disk stops rotating, and pull it out.
 3. Use a screwdriver to loosen the screws from the hard disk and remove the hard disk.

Figure 7-25 Removing a hard disk

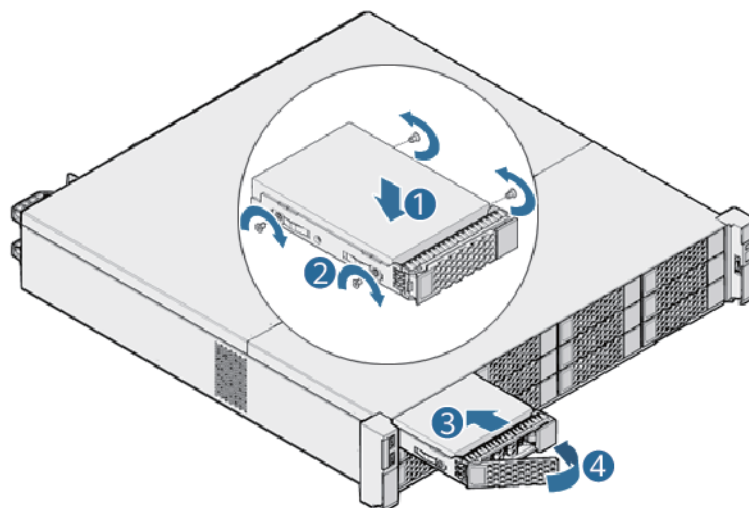


DS31000011

Step 3 Install a new hard disk.

1. Install the new hard disk.
2. Secure the hard disk to the front panel using a screwdriver.
3. Push the hard disk into the subrack along the guide rails until it cannot move forwards.
4. Close the ejector lever and push the hard disk in position.

Figure 7-26 Installing a new hard disk



DS31000012

Step 4 Observe the hard disk indicator to check whether the hard disk works properly.

----End

Follow-up Procedure

If the hard disk works abnormally, contact Huawei technical support.

7.2.5.3 Replacing a VCN510

Prerequisites

- Recommended tool: Phillips screwdriver
- A VCN510 needs to be replaced.
- A spare VCN510 of the same model is available and functional.

Context

NOTICE

Videos cannot be recorded during the replacement of the VCN510.

 DANGER

Do not operate with power on. Take appropriate insulation measures.

Procedure

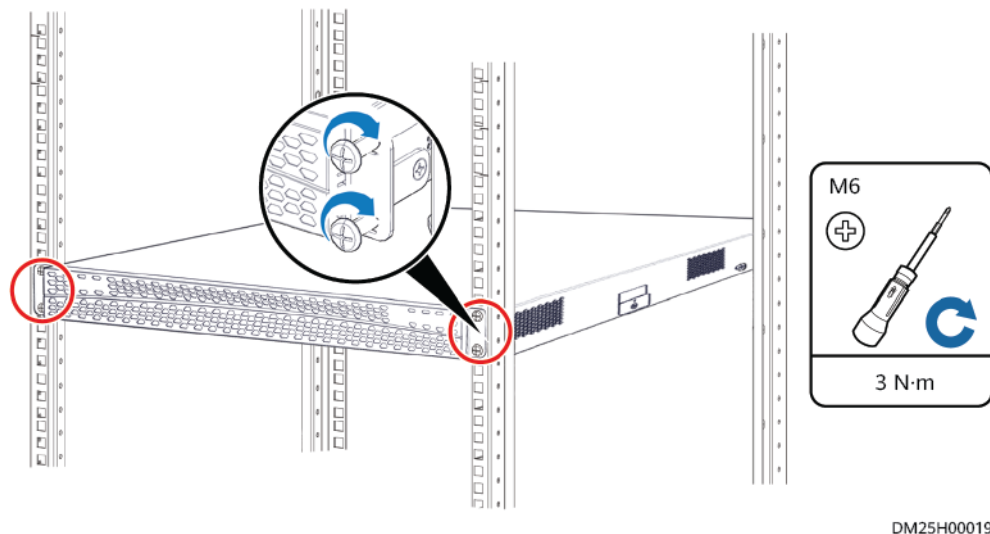
- Step 1** Turn off the power switch of the VCN510, disconnect the power supply of the VCN510, remove the cables from the VCN510, label the cables, and record the original connection positions of the cables.

NOTICE

After removing cables, wrap exposed terminals with insulation tape and do not block cable labels. If cable labels are blocked, cables may be connected incorrectly.

- Step 2** Remove the faulty VCN510 from the cabinet.
- Step 3** Carry the device to the cabinet. Ensure that the mounting ears at both sides of the device are tightly attached to the mounting bars in front of the cabinet. Use one hand to hold the device. Use the other hand to thread M6 screws through the slotted holes on the mounting ears. Use a Phillips screwdriver to tighten the M6 screws on the mounting ears. Each mounting ear uses two M6 screws.

Figure 7-27 Installing the device



Step 4 Reconnect the cables to the new VCN510.

Step 5 Turn on the power switch of the VCN510.

Step 6 Commissioning the VCN510. If the video recording function works properly after commissioning, the VCN510 is functional.

----End

7.2.5.4 Replacing a VCN520

Prerequisites

- Recommended tool: Phillips screwdriver
- A VCN520 needs to be replaced.
- A spare VCN520 of the same model is available and functional.

Context

NOTICE

Videos cannot be recorded during the replacement of the VCN520.

⚠ DANGER

Do not operate with power on. Take appropriate insulation measures.

Procedure

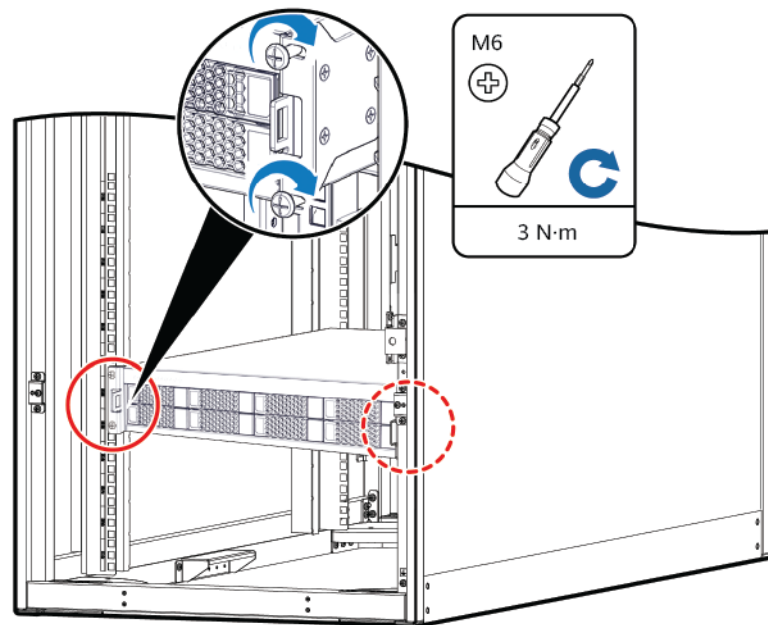
- Step 1** Turn off the power switch of the VCN520, disconnect the power supply of the VCN520, remove the cables from the VCN520, label the cables, and record the original connection positions of the cables.

NOTICE

After removing cables, wrap exposed terminals with insulation tape and do not block cable labels. If cable labels are blocked, cables may be connected incorrectly.

- Step 2** Remove the faulty VCN520 from the cabinet.
- Step 3** Put two M6 screws through the slotted holes of one mounting ear and use a Phillips screwdriver to fasten the screws to secure the device to the rack rail at front of the network cabinet.

Figure 7-28 Securing the VCN520



DM25H00022

- Step 4** Reconnect the cables to the new VCN520.
- Step 5** Turn on the power switch of the VCN520.
- Step 6** Commissioning the VCN520. If the video recording function works properly after commissioning, the VCN520 is functional.

----End

7.2.5.5 Replacing a VCN540

Prerequisites

- Recommended tool: Phillips screwdriver

- A VCN540 needs to be replaced.
- A spare VCN540 of the same model is available and functional.

Context

NOTICE

Videos cannot be recorded during the replacement of the VCN540.

DANGER

Do not operate with power on. Take appropriate insulation measures.

Procedure

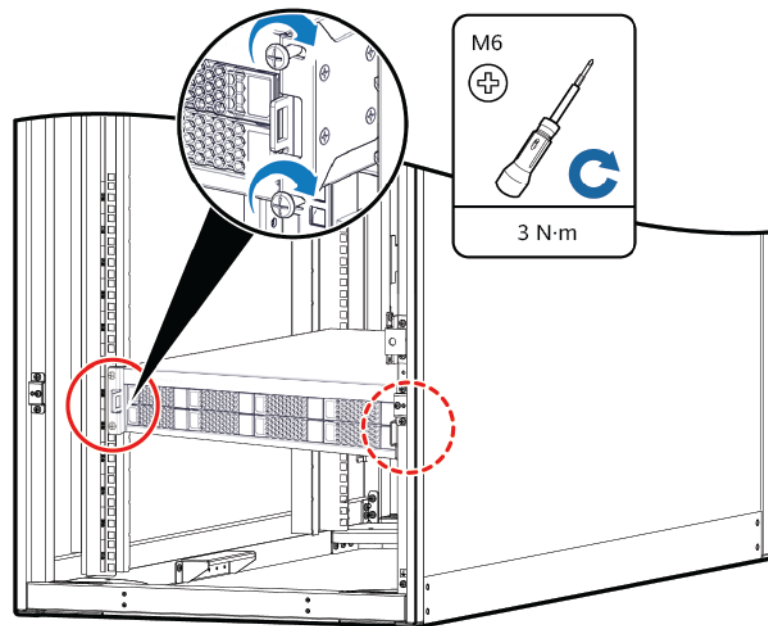
- Step 1** Turn off the power switch of the VCN540, disconnect the power supply of the VCN540, remove the cables from the VCN540, label the cables, and record the original connection positions of the cables.

NOTICE

After removing cables, wrap exposed terminals with insulation tape and do not block cable labels. If cable labels are blocked, cables may be connected incorrectly.

- Step 2** Remove the faulty VCN540 from the cabinet.
- Step 3** Put two M6 screws through the slotted holes of one mounting ear and use a Phillips screwdriver to fasten the screws to secure the device to the rack rail at front of the network cabinet.

Figure 7-29 Securing the VCN540



DM25H00022

Step 4 Reconnect the cables to the new VCN540.

Step 5 Turn on the power switch of the VCN540.

Step 6 Commissioning the VCN540. If the video recording function works properly after commissioning, the VCN540 is functional.

----End

7.2.5.6 Replacing an IVS1800

Prerequisites

- Recommended tool: Phillips screwdriver
- An IVS1800 needs to be replaced.
- A spare IVS1800 of the same model is available and functional.

Context

NOTICE

Videos cannot be recorded during the replacement of the IVS1800.

⚠ DANGER

Do not operate with power on. Take appropriate insulation measures.

Procedure

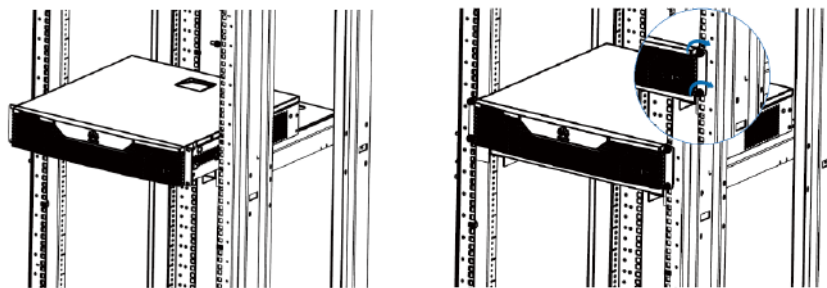
- Step 1** Turn off the power switch of the IVS1800, disconnect the power supply of the IVS1800, remove the cables from the IVS1800, label the cables, and record the original connection positions of the cables.

NOTICE

After removing cables, wrap exposed terminals with insulation tape and do not block cable labels. If cable labels are blocked, cables may be connected incorrectly.

- Step 2** Remove the faulty IVS1800 from the cabinet.
- Step 3** Carry the device to the cabinet. Ensure that the mounting ears at both sides of the device are tightly attached to the mounting bars in front of the cabinet. Use one hand to hold the device. Use the other hand to thread M6 screws through the slotted holes on the mounting ears. Use a Phillips screwdriver to tighten the M6 screws on the mounting ears. Each mounting ear uses two M6 screws.

Figure 7-30 Installing a device



DC11L00016

- Step 4** Reconnect the cables to the new IVS1800.
- Step 5** Turn on the power switch of the IVS1800.
- Step 6** Commissioning the IVS1800. If the video recording function works properly after commissioning, the IVS1800 is functional.

----End

7.2.5.7 Replacing a Hard Disk for the IVS1800

Prerequisites

- A hard disk needs to be replaced.
- Data in the hard disk has been backed up.
- A spare hard disk of the same model is available and functional.
- Before replacing a faulty disk, ensure that the power switch on the rear panel is off and disconnect the power cable to power off the device.

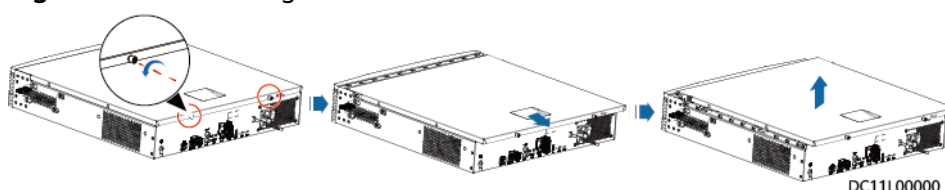
Context

Recommended tools and materials: Phillips screwdriver, ESD wrist strap (or ESD gloves).

Procedure

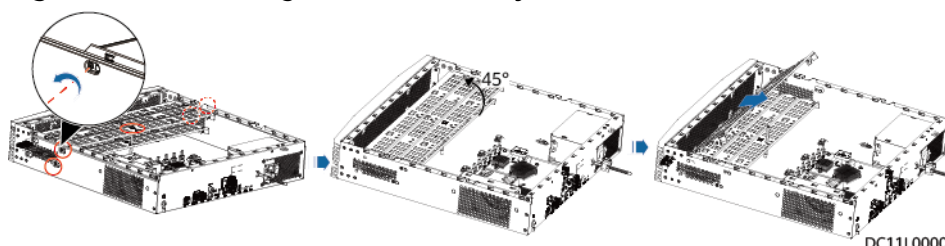
- Step 1** Put on an ESD wrist strap (or ESD gloves) and insert the ground terminal into the ESD jack in the cabinet.
- Step 2** Remove the faulty hard disk.
1. Use a PH2 screwdriver to remove the two black screws on the rear of the chassis cover, and take off the chassis cover.

Figure 7-31 Removing the chassis cover



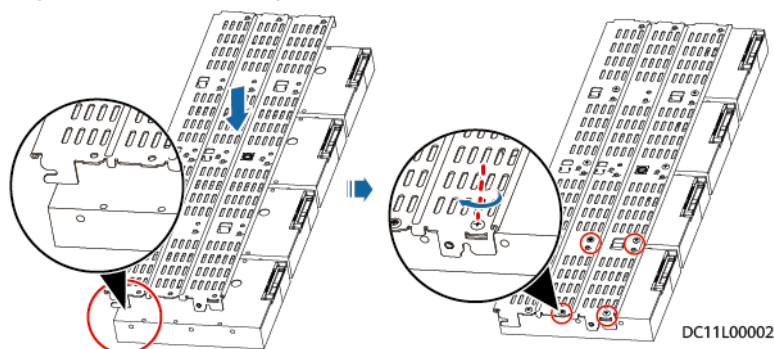
2. Remove two black screws on each side of the chassis and the silvery white one on top of the hard disk tray, raise the hard disk tray by 45 degrees, and take out the upper and then lower layers of hard disk tray.

Figure 7-32 Removing the hard disk tray



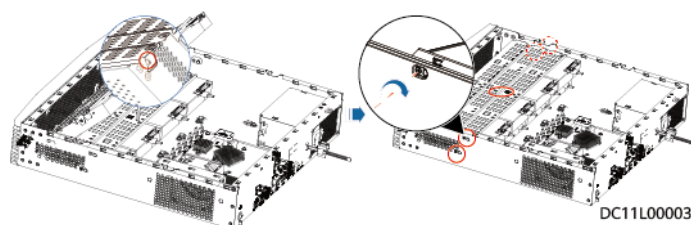
- Step 3** Install a new hard disk.
1. Place the hard disk with ports facing upwards and align the screw holes on the hard disk tray with the hard disk and fasten the screws. Before the installation, ensure that the fastener of the hard disk tray is on a different side from the hard disk port, as shown in the lower left figure.

Figure 7-33 Installing hard disks



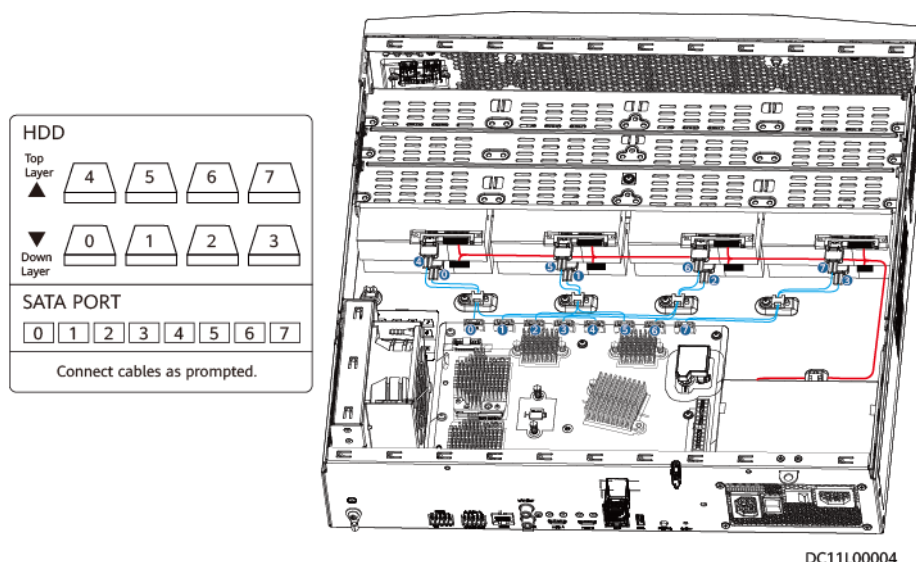
2. Insert the hard disk tray back at 45 degrees with the opening of its locking buckle facing downwards, hold the screw in the red-framed part to lower the hard disk tray until it is level, and fasten the black screws on the left and right sides and the white screw on the top.

Figure 7-34 Fastening the screw on the panel and the screws on the hard disk tray



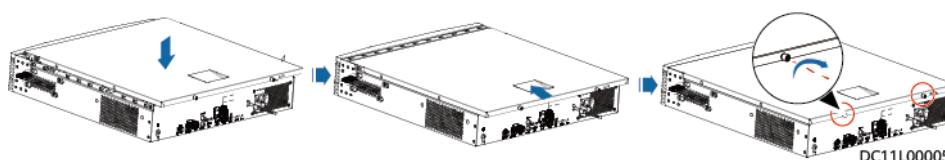
3. Connect data and power cables to hard disks. Connect hard disk cable ports P0–P3 to hard disks on the lower-layer hard disk tray and ports P4–P7 to hard disks on the upper-layer.

Figure 7-35 Connecting data and power cables to hard disks



4. Close the chassis cover, and use a PH2 screwdriver to fasten the rear screws.

Figure 7-36 Closing the chassis cover



Step 4 Observe the hard disk indicator to check whether the hard disk works properly.

----End

Follow-up Procedure

If the hard disk works abnormally, contact Huawei technical support.

7.2.5.8 Replacing an IPC6325 Camera

Prerequisites

- A camera needs to be replaced.
- A spare camera of the same model is available and functional.

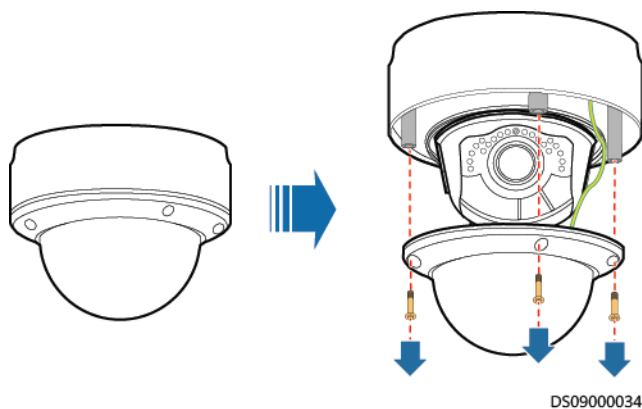
Context

Recommended tools and materials: inner hexagon screwdriver (delivered with the product package), step ladder (2 m)

Procedure

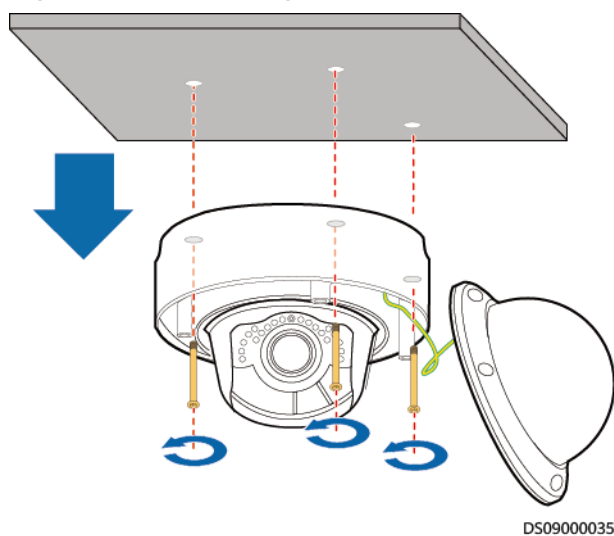
Step 1 Unscrew and remove the front cover from the camera, as shown in [Figure 7-37](#).

Figure 7-37 Removing the front cover



Step 2 Remove the screws from the camera, as shown in [Figure 7-38](#).

Figure 7-38 Removing a camera



Step 3 Disconnect the monitoring network cable and remove the camera from the control ceiling.

Step 4 Install a new camera, reconnect the network cable, and secure the camera to the base using screws.

Step 5 Adjust the camera coverage based on video images.

Step 6 Tighten the screws on the front cover of the camera.

----End

Follow-up Procedure

Check whether the new camera works properly and adjust the camera angle. If video images are properly displayed on the video screen of the management system client, the new camera works properly.

7.2.5.9 Replacing an IPC6225 camera

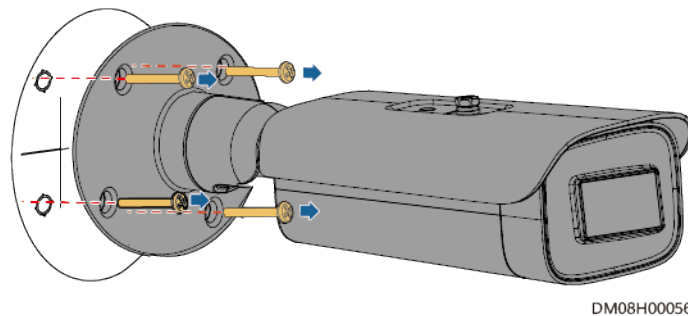
Prerequisites

- A camera needs to be replaced.
- A spare camera of the same model is available and functional.

Procedure

Step 1 Loosen the four ST39 tapping screws on the camera.

Figure 7-39 Removing an IPC6211 camera



Step 2 Disconnect the monitoring network cable and remove the camera from the wall.

Step 3 Install a new camera, reconnect the network cable, and secure the camera to the base using screws.

Step 4 Adjust the camera coverage based on video images.

----End

Follow-up Procedure

Check whether the new camera works properly. If video images are properly displayed on the video screen of the management system client, the new camera works properly.

7.2.5.10 Replacing an M2121 Camera

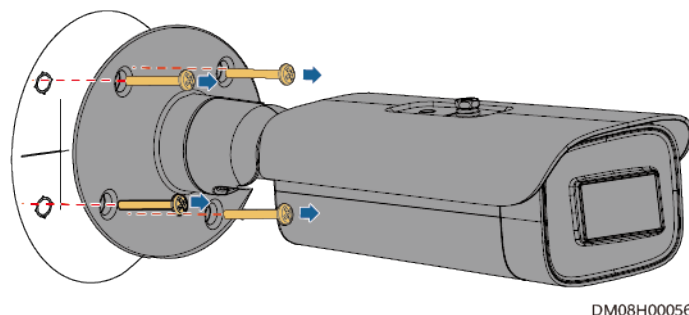
Prerequisites

- A camera needs to be replaced.
- A spare camera of the same model is available and functional.

Procedure

Step 1 Loosen the four ST39 tapping screws on the camera.

Figure 7-40 Removing the M2121 camera



Step 2 Disconnect the monitoring network cable and remove the camera from the wall.

Step 3 Install a new camera, reconnect the network cable, and secure the camera to the base using screws.

Step 4 Adjust the camera coverage based on video images.

-----End

Follow-up Procedure

Check whether the new camera works properly. If video images are properly displayed on the video screen of the management system client, the new camera works properly.

7.2.6 Replacing the Access Management System

7.2.6.1 Replacing an Access Controller

Prerequisites

- An access controller needs to be replaced.
- A spare access controller of the same model is available and functional.

Context



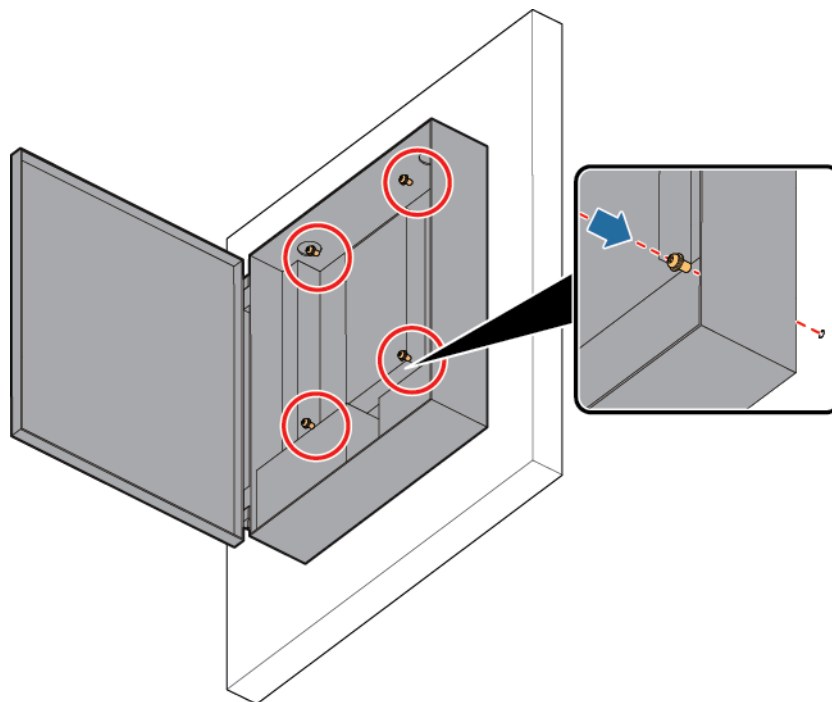
Do not operate with power on. Take appropriate insulation measures.

Recommended tools and materials: diagonal pliers, crimping tool, insulation tape, Phillips screwdriver, cord end terminal

Procedure

- Step 1** Disconnect power supply from the access controller. Then, remove cables that connect to the access controller, label the cables, and record where the labeled cables were connected.
- Step 2** Remove the access controller from the wall, as shown in [Figure 7-41](#).

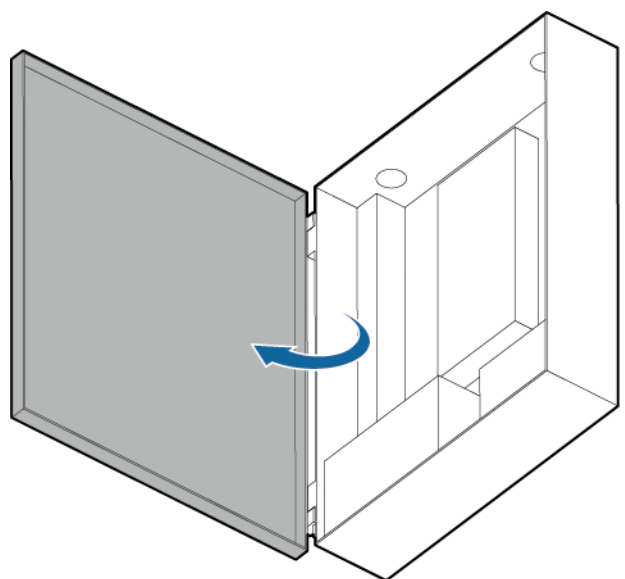
Figure 7-41 Removing an access controller



DM04H00010

- Step 3** Unpack and take out the new access controller.
- Step 4** Unlock the access controller with the delivered key.

Figure 7-42 Unlocking an access controller



DM04H00011

- Step 5** Install the new access controller by performing the operations prior to [Step 3](#) in reverse order.
- Step 6** Reinstall the removed cables for the access controller according to the labels and start the access controller.
- Step 7** Set the address of the access controller using the DIP switch, as shown in [Table 7-20](#).

Table 7-20 Setting the address of the access controller

Address Value	Toggle Switch 1	Toggle Switch 2
0	OFF	OFF
1	ON	OFF
2	OFF	ON
3	ON	ON

- Step 8** Set the baud rate of the access controller to **19200**. The preset data bit, stop bit, and check bit are **8**, **1**, and **none respectively**.

----End

7.2.6.2 Replacing a Double-Door Magnetic Lock

Prerequisites

- A double-door magnetic lock needs to be replaced.
- Spare magnetic locks of the same model are available and functional.

Context

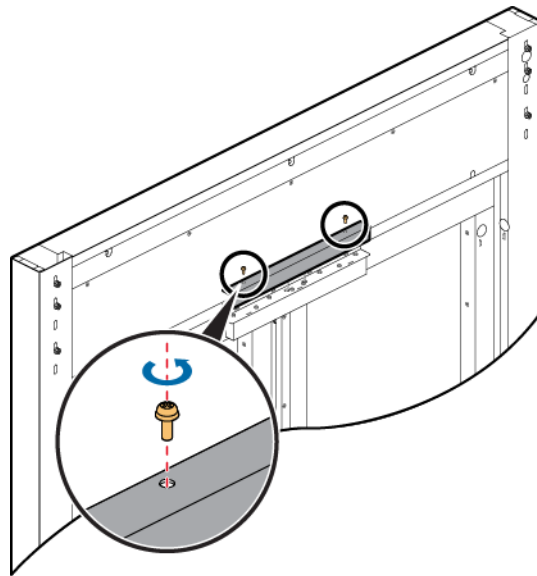
Prepare magnetic locks of the same model.

Recommended tools and materials: crimping tool, Phillips screwdriver, hex key (delivered with the product package), step ladder (2 m).

Procedure

Step 1 Remove the cover of the magnetic lock, as shown in [Figure 7-43](#).

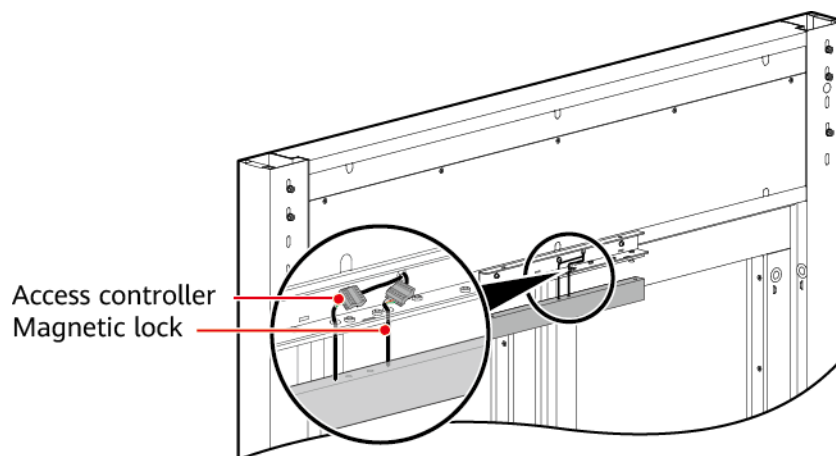
Figure 7-43 Removing a cover



DM22000057

Step 2 Remove magnetic lock cables from the terminals and route the cables out of the cable holes, as shown in [Figure 7-44](#).

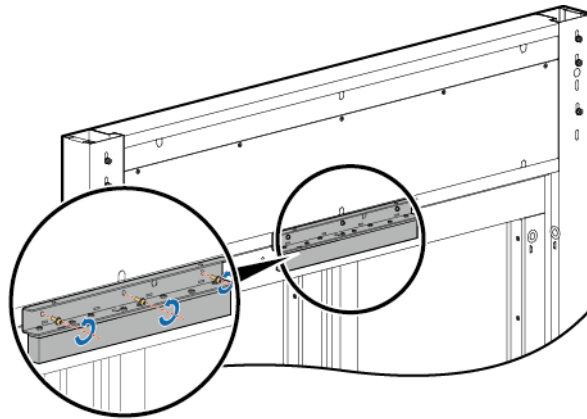
Figure 7-44 Removing cables



DM220E0024

Step 3 Remove the base and the magnetic lock, as shown in [Figure 7-45](#).

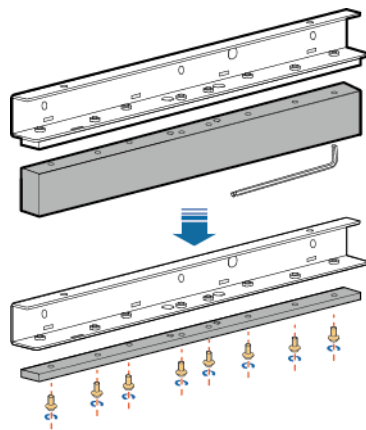
Figure 7-45 Removing the base



DM22000061

Step 4 Separate the base from the magnetic lock using a hex key, as shown in [Figure 7-46](#). Unpack and take out a new magnetic lock.

Figure 7-46 Separating a magnetic lock



DM22000062

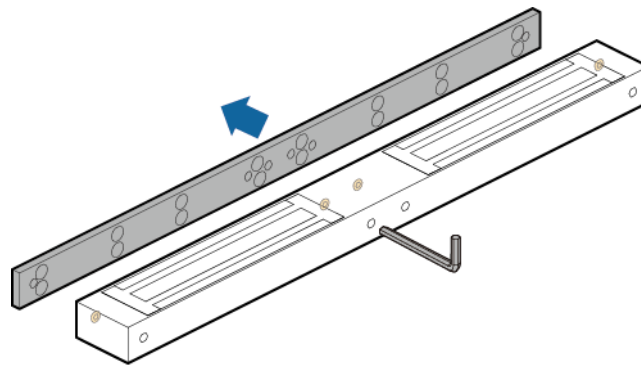
Step 5 Install the new magnetic lock.

1. Remove the fixing plate from the magnetic lock using the delivered hex key as shown in [Figure 7-47](#).

NOTE

The four hex socket screws should be removed in this step.

Figure 7-47 Remove the fixing plate of the magnetic lock



DM22000022

2. After the base and the fixing plate are secured, route the magnetic lock cables into the base and secure all the components.
3. Install a double-door magnetic lock by performing the operations prior to [Step 3](#) in a reverse order.

----End

Follow-up Procedure

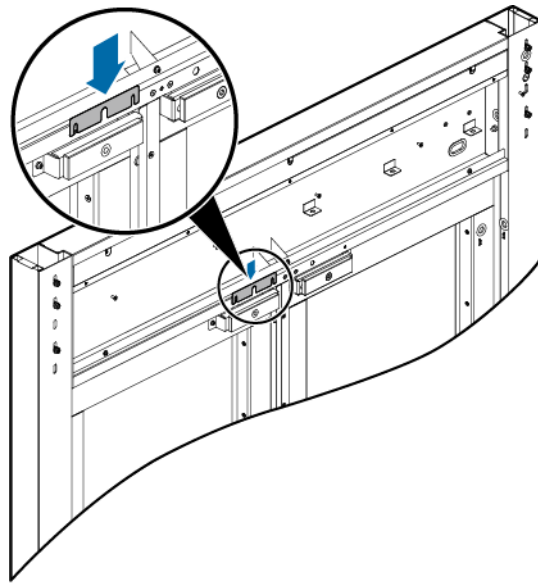
If the electromagnet does not work properly after power-on, check the following items:

1. Check whether the electromagnets provide magnetic force by attaching magnetizable iron parts to them.
2. Check whether the magnetic iron plates align with the electromagnets.
3. Check whether gaps exist between the magnetic iron plates and the electromagnets.

If any of the preceding conditions occur, troubleshoot the magnetic lock as follows:

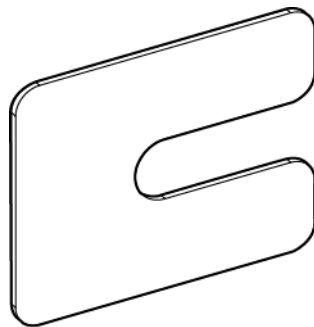
1. Check the circuit and rectify any circuit fault.
2. Adjust the magnetic iron plate base and door panels to ensure that the magnetic iron plates align with the electromagnets. Ensure that the position deviation is no too large.
3. If gaps exist between the electromagnets and the magnetic iron plates, rectify the fault by referring to [Figure 7-48](#).
4. If the magnetic iron plates are not level with each other, adjust them by using the spacer shown in [Figure 7-49](#).

Figure 7-48 Adjusting the gap



DM22000033

Figure 7-49 Spacer



DM22000032

7.2.6.3 Replacing a Single-Door Magnetic Lock

The method of replacing a single-door magnetic lock is similar to that of replacing a double-door magnetic lock. For details, see the section about replacing a double-door magnetic lock.

7.2.6.4 Replacing a Card Reader

Prerequisites

- A card reader needs to be replaced.
- Spare card readers of the same model are available and functional.

Context

Prepare a spare access card reader of the same model.

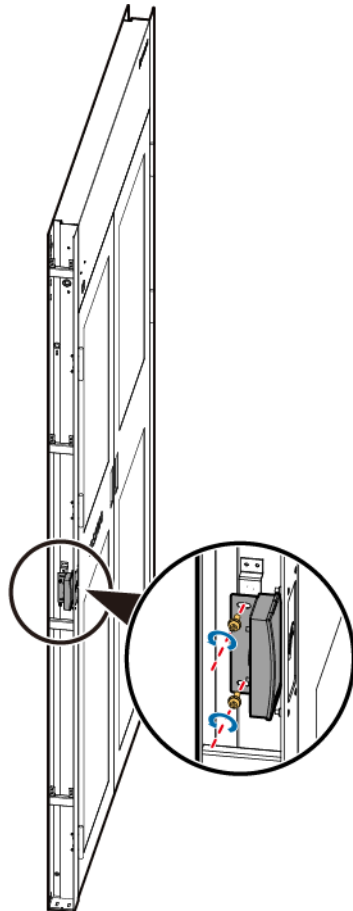
Recommended tools and materials: crimping tool and Phillips screwdriver

Procedure

Step 1 Remove the post side panel.

Step 2 Remove the mounting plate of the card reader, as shown in [Figure 7-50](#).

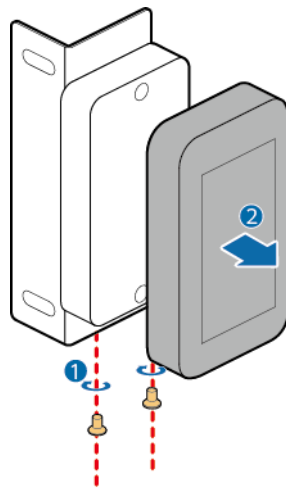
Figure 7-50 Removing the mounting plate



DS07000010

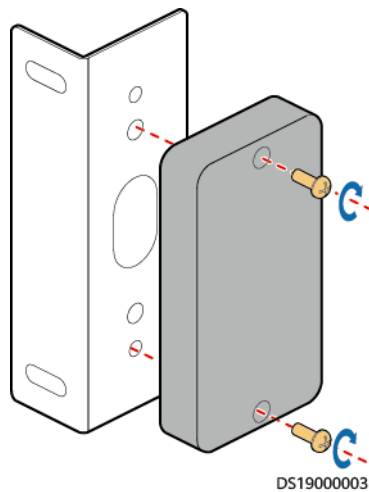
Step 3 Remove the screws on the card reader cover and remove the cover, as shown in [Figure 7-51](#).

Figure 7-51 Removing the cover



Step 4 Remove the card reader, as shown in [Figure 7-52](#).

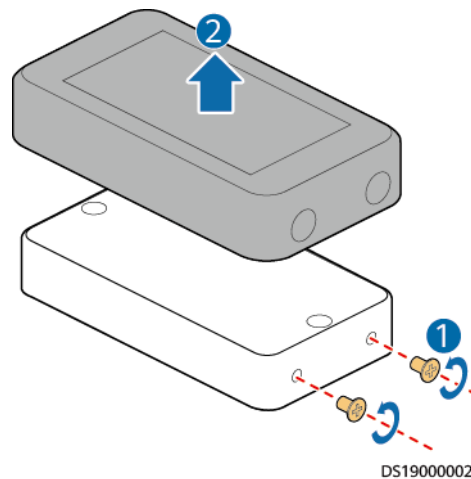
Figure 7-52 Removing the card reader



Step 5 Take out a new card reader.

Step 6 Remove the screws that secure the card reader and take out the card reader cover, as shown in [Figure 7-53](#).

Figure 7-53 Removing the card reader cover



Step 7 Install the new card reader by performing the operations prior to **Step 5** in reverse order.

Step 8 Reinstall the post side panel.

----End

Follow-up Procedure

Power on the access controller and check whether the card reader works properly.

7.2.6.5 Replacing a Fingerprint and Card Reader

Prerequisites

- Recommended tool: Phillips screwdriver
- A fingerprint and card reader needs to be replaced.
- A spare fingerprint and card reader of the same model is available and functional.

Context

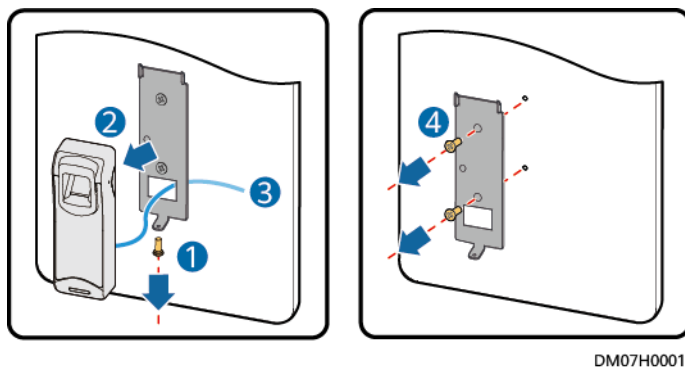
Figure 7-54 Fingerprint and card reader



Procedure

- Step 1** Remove the screw that secures the fingerprint and card reader, and remove the cable, as shown by (1), (2), and (3) in [Figure 7-55](#).

Figure 7-55 Removing a bottom plate



- Step 2** Remove the original bottom plate, as shown by (4) in [Figure 7-55](#).
- Step 3** Take out the bottom plate of the new fingerprint and card reader and secure it.
- Step 4** Connect the cable.
- Step 5** Secure the fingerprint and card reader to the bottom plate.
- Step 6** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.

Step 7 Select the new fingerprint and card reader, and click **Connection test**. When **Connection success** is displayed, the replacement is complete.

----End

7.2.6.6 Replacing a Card Reader with a Keypad

Prerequisites

- Recommended tool: Phillips screwdriver
- A card reader with a keypad needs to be replaced.
- A spare card reader with a keypad of the same model is available and functional.

Context

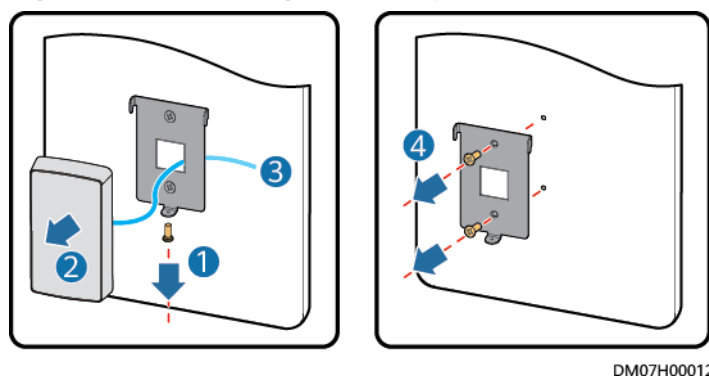
Figure 7-56 Card reader with a keypad



Procedure

Step 1 Remove the screw that secures the card reader with a keypad, and remove the cable, as shown by (1), (2), and (3) in [Figure 7-57](#).

Figure 7-57 Removing a bottom plate



- Step 2** Remove the original bottom plate, as shown by (4) in [Figure 7-57](#).
- Step 3** Take out the bottom plate of the new card reader with a keypad and secure it.
- Step 4** Connect the cable.
- Step 5** Secure the card reader with a keypad to the bottom plate.
- Step 6** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 7** Select the new card reader with a keypad, and click **Connection test**. When **Connection success** is displayed, the replacement is complete.

----End

7.2.6.7 Replacing a Fingerprint and Card Reader with a Keypad

Prerequisites

- Recommended tool: Phillips screwdriver
- A fingerprint and card reader with a keypad needs to be replaced.
- A spare fingerprint and card reader with a keypad of the same model is available and functional.

Context

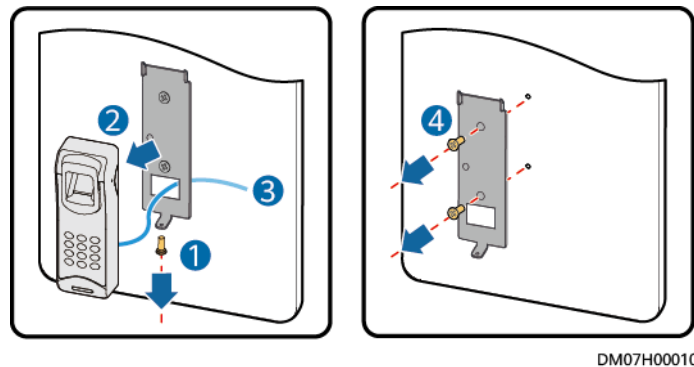
Figure 7-58 Fingerprint and card reader with a keypad



Procedure

- Step 1** Remove the screw that secures the fingerprint and card reader with a keypad, and remove the cable, as shown by (1), (2), and (3) in [Figure 7-59](#).

Figure 7-59 Replacing a fingerprint and card reader with a keypad



- Step 2** Remove the original bottom plate, as shown by (4) in [Figure 7-59](#).
- Step 3** Take out the bottom plate of the new fingerprint and card reader with a keypad and secure it.
- Step 4** Connect the cable.
- Step 5** Secure the fingerprint and card reader with a keypad to the bottom plate.
- Step 6** Choose **System > Service Settings > Data Center Planning** from the main menu. The **Data Center Planning** page is displayed.
- Step 7** Select the new fingerprint and card reader with a keypad, and click **Connection test**. When **Connection success** is displayed, the replacement is complete.

----End

7.2.6.8 Replacing an Emergency Door Release Button

Prerequisites

- Recommended tool: Phillips screwdriver
- An emergency door release button needs to be replaced.
- A spare emergency door release button of the same model is available and functional.

Context

Figure 7-60 Emergency door release button

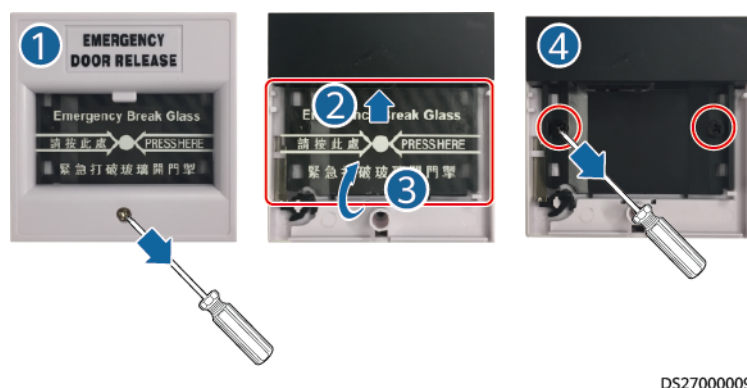


Procedure

Step 1 Remove the emergency door release button.

1. Remove the screw that secures the emergency door release button, as shown by (1) in [Figure 7-61](#).
2. Remove the glass panel of the emergency door release button, as shown by (2) and (3) in [Figure 7-61](#).
3. Remove the screws that secure the base, as shown by (4) in [Figure 7-61](#).
4. Disconnect cables and remove the emergency door release button.

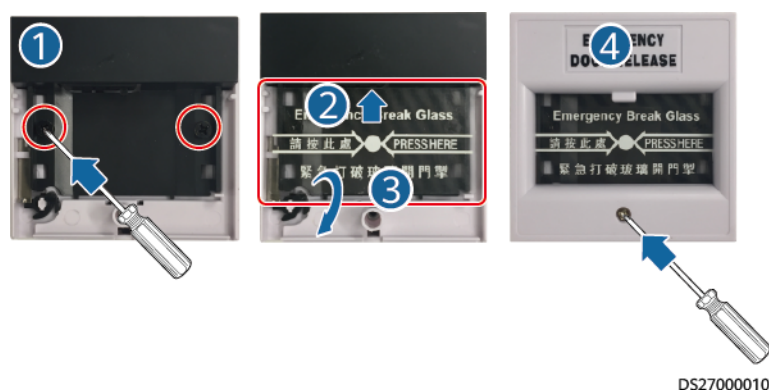
Figure 7-61 Removing an emergency door release button



Step 2 Install a new emergency door release button.

1. Connect cables.
2. Tighten screws on the base, as shown by (1) in [Figure 7-62](#).
3. Install the glass panel, as shown by (2) and (3) in [Figure 7-62](#).
4. Tighten the screw, as shown by (4) in [Figure 7-62](#).

Figure 7-62 Installing an emergency door release button



Step 3 Close the room door, and open the protection box of the emergency door release button.

Step 4 Remove the cover of the emergency door release button using a Phillips screwdriver and remove the glass. If the room door can be opened normally, the emergency door release button is functional.

Step 5 Install the emergency door release button.

----End

8 FAQ

8.1 How Do I Handle Abnormal Door Control Status?

Context

If the door control status collected by the NetEco is always open, resolve the issue by following the procedure in this section.

Procedure

- Step 1** Check whether the door in the door control system is open.
- If the door is open, close the door.
 - If the door is closed, go to [Step 2](#).
- Step 2** Check whether cables are connected to the door access controller and door lock properly.
- If cables are not connected properly, reconnect cables.
 - If cables are connected properly, go to [Step 3](#).
- Step 3** Check whether the angle and tightness of the door magnet are appropriate.
- If the angle and tightness are inappropriate, adjust them.
 - If the angle and tightness are appropriate, contact Huawei technical support.
- End

8.2 How Do I Change the NetEco IP Address?

Prerequisites

You have the operation rights of the ECC800-Pro WebUI and UPS2000-G.

Procedure

Step 1 Change the NetEco IP address.

1. In the browser address bar, enter https://client IP address of PowerEcho:31945, enter the **User Name** and **Password**, and press **Enter** to access the PowerEcho client.

NOTE

The default user name for PowerEcho is **admin** and the preset password is **Changeme_123**.

2. On PowerEcho, choose **Maintenance > Network Configuration > Configure IP Address** from the main menu.
3. Choose **Modify IP Address**, select the NetEco to be configured, and click **Edit**, set **IP Address**, **Subnet Mask/Prefix Length** and **NIC Usage**, and click **Apply**.

NOTE

After you change IP address of a database node, the product services and the databases will be automatically restarted.

Step 2 Update the NetEco IP address on the ECC800-Pro WebUI.

1. Log in to the ECC800-Pro WebUI.
2. Set NetEco communications parameters.

Table 8-1 NetEco communications parameters

Path	Parameter	Default Value	Setting
System Settings > NMS Application > NetEco > Communication Parameters	Server IP	192.168.8.11	IP address of the primary NetEco server NOTE The NetEco IP address and the ECC800-Pro IP address must be configured in the same network to ensure normal connection between the NetEco and the ECC800-Pro.
	Port number	31220	31220
	Network port for link setup	WAN_1	WAN_1 or WAN_2

3. Click **Submit**.

Step 3 Modify the UPS2000-G SNMP trap parameters (WebUI 1)

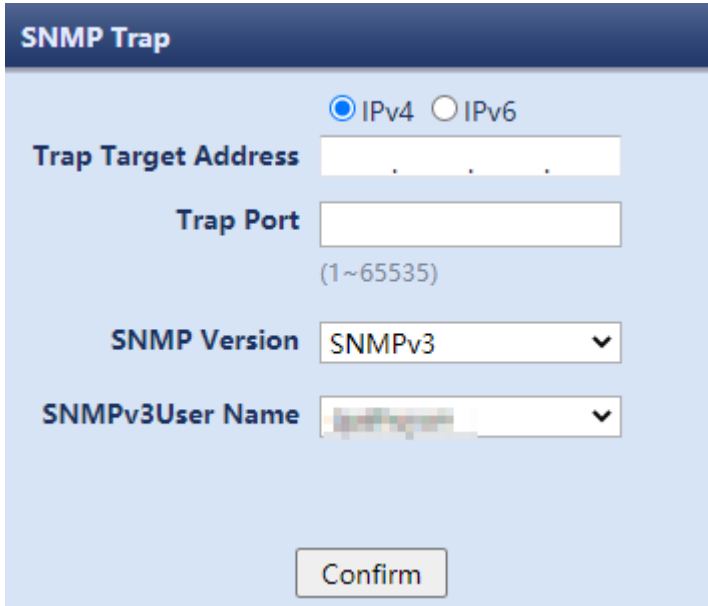
1. Log in to the UPS2000-G WebUI.
2. Choose **Configure > SNMP**.
3. In the **NMS Address and Permissions Settings** area, select the line where the value of **NMS addr.** is the same as the NetEco IP address before change in the **No.** column, and click **Delete**.

4. Click **Add**, enter the IP address of the NetEco server in the **NMS addr.** text box, and click **Add**.
5. In the **SNMP TRAP** area, select the line where the value of **Trap addr.** is the same as the NetEco IP address before change in the **No.** column, and click **Delete**.
6. Click **Add**, enter the IP address of the NetEco server in the **Trap addr.** text box, enter **162** in the **Trap port** text box, and click **Add**.

Step 4 Modify the UPS2000-G SNMP trap parameters (WebUI 2)

1. Log in to the UPS2000-G WebUI.
2. Choose **System Settings > SNMP Settings**.
3. In the **SNMP Trap** area, if **Trap Target Address** is the same as the NetEco IP address before the modification, select this row and click **Delete**.
4. In the **SNMP Trap** area, click **Add**.
5. In the displayed **SNMP Trap** dialog box, set SNMP trap parameters, and click **Confirm**.
 - Enter the IP address of the NetEco server in the **Trap Target Address** text box.
 - Set **Trap Port** to **162**.

Figure 8-1 Setting SNMP trap parameters

The image shows a web-based configuration dialog titled "SNMP Trap". At the top, there are two radio buttons: "IPv4" (which is selected) and "IPv6". Below this, there are four main input fields: "Trap Target Address" with a text box containing three dots, "Trap Port" with a text box and a range "(1~65535)" below it, "SNMP Version" with a dropdown menu showing "SNMPv3", and "SNMPv3User Name" with a dropdown menu showing a blurred name. At the bottom center is a "Confirm" button.

6. Click **Confirm**.

----End

9 Acronyms and Abbreviations

A	
AC	alternating current
AES	Advanced encryption standard
AI	analog input
APP	application
B	
BCB	battery control I/O board
C	
COM	component object model
D	
DC	direct current
DES	Data Encryption Standard
DI	digital input
DO	digital output
E	
ECC	Energy Control Center
ESN	equipment serial number
ETH	Ethernet
F	
FE	Fast Ethernet

G	Gigabit Ethernet
GE	
I	
iBAT	iBattery
IC	integrated circuit
iCooling	iCooling
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IT	Internet technology
L	
LED	light emitting diode
M	
MTBF	mean time between failures
MTTR	mean time to repair
MAC	Media Access Control
MD5	message digest algorithm
Mib	Mib
N	
NAT	network address translation
NetEco	iManager NetEco data center infrastructure management system
NTC	negative temperature coefficient
P	
PDU	power distribution unit
POE	power over Ethernet
PSU	power supply unit
PUE	power usage effectiveness
R	
RF	radio frequency
RH	relative humidity

RJ	Registered Jack
RoHS	restriction of the use of certain hazardous substances
S	
SD	secure digital
SHA	SecureHashAlgorithm
SIM	subscriber identity module
SMS	short message service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SSID	service set identifier
T	
TLS	Transport Layer Security
U	
UPS	uninterruptible power system
USB	universal serial bus
V	
VCN	video cloud node
W	
WiFi	wireless fidelity
WPS	WiFi protected setup