VERTIV.

SmartCabinet™

User Manual

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages result from use of this information or for any errors or omissions.

Refer to local regulations and building codes relating to the application, installation, and operation of this product. The consulting engineer, installer, and/or end user is responsible for compliance with all applicable laws and regulations relation to the application, installation, and operation of this product.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use, or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit https://www.vertiv.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

1 Important Safety Instructions

Save these instructions

This manual contains important safety instructions that should be followed during the installation and maintenance of the Vertiv™ SmartCabinet™. Read this manual thoroughly before installing or operating this unit. Only qualified personnel should move, install or service this equipment. Any operation that requires opening doors or equipment panels must be carried out only by the qualified person. Adhere to all warnings, cautions, notices, and installation, operating and safety instructions on the unit and in this manual. Follow all installation, operation, and maintenance instructions and all applicable national and local building, electrical and plumbing codes. To identify the unit model and serial number for assistance or spare parts, locate the identification label on the cabinet.

Electrical Safety

High Pressure

⚠️ **WARNING! Risk of improper handling. Some parts of the unit have high voltage. Direct or indirect contact with these parts through damp objects can cause injury, or death.**

The installation of AC power supply equipment must comply with the safety regulations of the relevant industry, and the personnel who carry out the installation of AC equipment must have high voltage, ALTER, and other operational qualifications.

It is strictly forbidden to wear watches, bracelets, rings, and other conductive objects on your wrist.

Turn off the power immediately if you find water or moisture in the cabinet. When operating in humid conditions, water should be strictly prevented from entering the equipment.

A prohibition sign must be mounted on switches and buttons that cannot be operated during installation.

⚠️ **WARNING! Risk of high voltage lines construction. Can cause fire or electric shock hazards. The installation and routing of AC cables must comply with local and national codes and regulations. The cables with large leakage currents must be grounded before the power supply is switched on.**

⚠️ **WARNING! The installation and routing of cables must comply with local and national codes and regulations. The cables with large leakage currents must be grounded before the power supply is switched on.**

NOTE: According to EN 61000-3-11, the system is conditionally connected to the power grid, and the maximum allowable system impedance Z max at the user's power interface point is mentioned below:
Z -phase A = 0.114 Ohm + j 0.071 Ohm (0.114 Ohm + 227 uH).
Z -neutral A = 0.076 Ohm + j 0.048 Ohm (0.076 Ohm + 151 uH).

⚠️ **CAUTION: Risk of improper handling. Can cause equipment damage. Some parts of the unit have high voltage. Special tools must be used when operating the unit.**

⚠ CAUTION: Risk of thunderstorms lightning damage. Can cause equipment damage. It is recommended to ground the unit in time as strong electromagnetic fields are produced in atmosphere in thunderstorms.

⚠ CAUTION: Static electricity generated by the human body can damage electrostatic sensitive components on board, such as large scale integrated circuits (ICs). In order to prevent the human body static damage sensitive components when in contact with equipment, hand-held boards, circuit boards, IC chips, etc. one must wear anti-static wrist band.

⚠ WARNING! Risk of improper wiring. Can cause system equipment damage, injury or death. It is strictly forbidden to reverse the fire wire (L) and zero wire (N) entered by the C.

⚠ WARNING! Risk of electric shock. Can cause injury or death. It is not permitted to wear watches, bracelets, rings, and other conductive objects on your wrist when operating with an electricity. An insulating tool must be used by th operator. Ensure to keep your hands, wrists and arms firmly to avoid accidents in the event that the tool slips and the tool or human body moves too much.

⚠ CAUTION: Risk of contact with sharp edges, splinters, and exposed fasteners. Can cause injury. Only properly trained and qualified personnel wearing appropriate, OSHA approved PPE should attempt to move, lift, remove packaging from the unit or prepare the unit for installation.

Power Cable

⚠ WARNING! Risk of improper wiring. Can cause equipment damage. Before connecting cables, confirm whether the cable and cable labels match site requirements.

⚠ WARNING! Risk of electric shock. Can cause injury or death. It is not permitted to wear watches, bracelets, rings, and other conductive objects on your wrist when operating with an electricity. An insulating tool must be used by th operator. Ensure to keep your hands, wrists and arms firmly to avoid accidents in the event that the tool slips and the tool or human body moves too much.

⚠ WARNING! Battery has high pressure.

⚠ WARNING! Physical maintenance and maintenance of all batteries must be carried out by trained personnel.

⚠ CAUTION: A battery can present a risk of electrical shock and high short circuit current. The following precautions should be followed when working on batteries:

- Remove watches, rings, and other metal objects.
- Use tools with insulated handles.
- Wear rubber gloves and shoes.
- Do not lay tools or metal parts on the battery surface.
- Disconnect the charging power source prior to connecting or disconnecting battery terminals.
- Check if the battery is accidentally grounded. If it is accidentally grounded, remove the source of the ground. Contact with any part of a grounded battery can result in electrical shock. Make sure that the battery is not grounded during installation and maintenance work.

Strapping of the Signal Line

⚠ CAUTION: The signal line should be secured separately from the high current or high voltage line, at least at the spacing of 150 mm.

This page intentionally left blank

2 Product Overview

The Vertiv™ SmartCabinet™ enables enterprise class IT infrastructure through the provision of the integrated enclosure, power, cooling, and service. Critically it also enables the most vital element of 360 degrees visibility of all the IT system components. This enables review and real-time monitoring as well as insight into IT system performance. SmartCabinet™ customers can effectively manage and plan their IT infrastructure. Continuous availability in turn depends on the power and cooling infrastructure that supports these systems, which is comprised of the following:

- Power quality
- Cooling
- Enclosure and physical infrastructure
- Monitoring and management

2.1 Product Features

SmartCabinet™ has the following features:

- **Dust proof and noise reduction, high efficiency, and energy saving**: Enclosed operation and internal cycle system ensure optimized temperature and humidity inside the cabinet, to prolong the lifetime of IT devices. A highly efficient UPS dedicated for server room is deployed, and a precision Air Conditioner AC (RCU unit) operates with closed cold/hot aisle technology to improve efficiency in server room. The fan is embedded with reduced noise level device, which make it suitable for office area.

- **RDU (Intelligent monitoring)**: Intelligent control functions such as integrated environment monitoring, device monitoring, alarm linkage provides centralized monitoring platform for server room management.

- **Highly integrated and space saving**: One standard cabinet provides stable operating conditions for all IT devices, only cabinet connection and air conditioning are needed on-site. The system only occupies area of around $1\,m^2$, which is compact.

- **User-friendly HMI and operation**: Large 7 in. LCD wide screen displays the device operation/alarm/safety information. The all-in-one solution enables all-day remote monitoring at the cabinet-level data center to perform different applications.

- **Quick delivery**: Easy transportation, built within a day, and smooth installation.

- **Access control management**: Cabinet level intelligent lock can be selected to ensure the safety of IT devices in the cabinet.

- **Video management**: Enables the video monitoring function of the network camera.

2.2 Product Views and Components

The appearance and components of the Vertiv™ SmartCabinet™ India product is shown in **Figure 2.1** below.

Figure 2.1 SmartCabinet™ (800 mm Wide Standard Unit 42U)

Item	Description
1	Flat surface

Table 2.1 Component Specifications

Sr No.	Specifications	Make	Model	Qty
1	RCU with fix scroll	Vertiv	RCU 2TR	1
2	800 W × 1100 D rack	Vertiv	743003800028	1
3	Vertiv™ Liebert® ITA2 10 kVA UPS	Vertiv	536600103001	2
4	Internal battery backup	Vertiv approved	325722000015	1
5	POD	Vertiv approved	325702000001	1
6	Sub-assembly, RDU kit	Vertiv	402003000246	1
7	Internal/External fire suppression kit	Vertiv approved	325705000219/325705000242	1
8	Geist monitored PDU	Vertiv	CP8853	1
9	Biometric access control	Vertiv approved	325705000244	1
10	Sub-assembly for 16 A LTS	Vertiv	325721000028	1
11	LCD KVM	Vertiv	402001000473	1
12	Rodent repellent	Vertiv approved	325705000033	1
13	Camera with local surveillance	Vertiv approved	325715000034	1

Figure 2.2 Vertiv™ SmartCabinet™ (800 mm Wide Standard Unit 47U)

Item	Description
1	Flat surface

2.3 Model Number and Nomenclature

The **Table 2.2** below and **Table 2.3** below describe the 8 digit model number.

Table 2.2 Vertiv™ SmartCabinet™ Model Number Nomenclature

1	2	3	4	5	6	7	8
SC	-	4	21	RC4	-	U20	2N

Table 2.3 SmartCabinet™ Model Number Digit Definitions

Digit	Feature	Description
1	Enterprise Code	SmartCabinet™
2	Default	-
3	No. of rack	4 racks
4	Cooling capacity/heat load	21 kW capacity
5	Redundancy	RC4 redundant cooling
6	Default	-
7	UPS load	U20 kVA load
8	Redundancy for UPS	2N

2.4 Product Specifications

Table 2.4 SmartCabinet™ Specifications

Specifications	SC-1-3-U3 2N	SC-2-3 CW-RCU3 2N	SC-2-7-U6 2N	SC-2-7 RC DSU10 2N	SC-3-14 RC3-U10 2N	SC-4-21 RC4 DSU20 2N
IT capacity	3 kVA	3 kVA	6 kVA	7 kVA	10 kVA	20 kVA
Number of rack	1	2	2	2	3	4
Cooling capacity	3.5 kW	2 × 3.5 kW CW	7 kW FS	2 × 7 kW DS	3 × 7 kW FS	3 × 7 kW FS
Cooling redundancy	No	Yes	No	Yes	Yes	Yes
UPS capacity	2 × 3 kVA	2 × 3 kVA	2 × 6 kVA	2 × 10 kVA	2 × 10 kVA	2 × 20 kVA
UPS redundancy	Yes					
Backup time	Minimum 5 min to maximum 60 min					
Monitoring	Yes					
Fire suppression and access control	Optional					
Display panel	7 in. HMI display					
Usable U space*	25	61	64	50	86	109
Rack PDU type	All types (basic, metered, and monitored)					
Accessories	KVM, LCD console, camera with local surveillance, LTS, and DCIM					

Table 2.4 SmartCabinet™ Specifications (continued)

Specifications	SC-1-3-U3 2N	SC-2-3 CW-RCU3 2N	SC-2-7-U6 2N	SC-2-7 RC DSU10 2N	SC-3-14 RC3-U10 2N	SC-4-21 RC4 DSU20 2N
CE certification	Yes					
Dimension						
Width	800	1600	1600	1600	2400	3200
Height	2100 (42U)					
	2300 (47U)					
Depth	1100 to 1200					

NOTE: Battery backup and cooling unit capacity can be modified as per requirement.

NOTE: * indicates U space available is subjected to change as per configuration.

NOTE: Additional Vertiv™ SmartCabinet™ Models being offered are SC-1-2, SC-1-2-U3 2N, SC-1-3, SC-1-3-U3 2N, SC-1-3-U6 2N, SC-1-3-U10 2N, SC-1-7, SC-1-7-U6 2N, SC-1-7-U10 2N, SC-1-7 DS, SC-1-7 DS-U6 2N, SC-1-7 DS-U10 2N, SC-1-3 CW, SC-1-3 CW-U3 2N, SC-1-3 CW-U6 2N, SC-2-3, SC-2-3-U3 2N, SC-2-3-U6 2N, SC-2-3-U10 2N, SC-2-3 RC, SC-2-3 RC-U3 2N, SC-2-3 RC-U6 2N, SC-2-3 RC-U10 2N, SC-2-7, SC-2-7 RC, SC-2-7-U6 2N, SC-2-7 RC-U6 2N, SC-2-7-U10 2N, SC-2-7 RC-U10 2N, SC-2-7 DS, SC-2-7 RC DS, SC-2-7 DS-U6 2N, SC-2-7 RC DS-U6 2N, SC-2-7 DS-U10 2N, SC-2-7 RC DS-U10 2N, SC-2-3 CW RC, SC-2-3 CW, SC-2-3 CW-U3 2N, SC-2-3 CW RC-U3 2N, SC-2-3 CW-U6 2N, SC-2-3 CW RC-U6 2N, SC-3-7 RC3, SC-3-7 RC3-U6 2N, SC-3-7 RC3-U10 2N, SC-3-7 RC3-U20 2N, SC-3-14 RC3, SC-3-14 RC3, SC-3-14 RC3-U6 2N, SC-3-14 RC3-U10 2N, SC-3-14 RC3-U20 2N, SC-3-14 RC3 DS, SC-3-14 RC3 DS-U6 2N, SC-3-14 RC3 DS-U10 2N, SC-3-14 RC3 DS U20 2N, SC-3-7 CW RC3, SC-3-7 CW RC3-U6 2N, SC-3-7 CW RC3-U10 2N, SC-3-7 CW RC3-U20 2N, SC-4-10 RC4, SC-4-10 RC4-U10 2N, SC-4-10 RC4-U20 2N, SC-4-21 RC4, SC-4-21 RC4-U10 2N, SC-4-21 RC4-U10 2N, SC-4-21 RC4-U20 2N, SC-4-21 RC4 DS, SC-4-21 RC4 DS-U10 2N, SC-4-21 RC4 DS-U20 2N, SC-4-10 CW RC4, SC-4-10 CW RC4 U10 2N, SC-4-10 CW RC4 U20 2N.

2.5 Functional Components

SmartCabinet™ product mainly includes the functional parts as IT rack, air conditioner (RCU), UPS with battery backup, power output distribution (POD), power distribution unit, ventilation system, monitoring system, access control with additional feature such as fire suppression and local LCD screen.

Table 2.5 Functional Components

System Type	Component	Main Function	Feature
Rack supporting system	19 in. floor Mount 42U/47U IT rack	Used to store the 19 in. rack mount hardware equipment, such as server, voice, data, internet network equipment, and UPS	The whole cabinet system is totally enclosed when operating, to keep the system clean without dust, which can save energy and reduce noise.
Power supply and distribution system	POD	Power distribution, surge suppression	Safe and energy saving.
	UPS and battery	Uninterrupted power supply with battery backup	
	Basic PDU	Power distribution	
	Intelligent PDU	Power distribution	
	LED lamp	System auxiliary lighting	

Table 2.5 Functional Components (continued)

System Type	Component	Main Function	Feature
Air conditioning system (RCU)	Air conditioner	Cooling the devices inside the cabinet actively	Small sized precision environmental control system, using advanced frequency conversion technology, specially designed for the cooling of electronic devices, with high energy efficiency ratio and automatic adjustment, keeping the environment in the cabinet to be stable so that the IT devices can operate safely and reliably.
	Emergency ventilation system	Prevent high temperature partially inside the cabinet	An emergency device that can startup automatically when over temperature occurs inside the cabinet or in case the air conditioner shuts down or fails, to prevent the devices from operating at high temperatures. When the system is operating normally, the emergency ventilation kit is off, to ensure airtight environment in the system and high efficiency cooling of the air conditioner.
Monitoring and management system	RDU	Local display and monitoring functions	An intelligent management system that provides power inside the cabinet and environmental monitoring, support plug-and-play of Vertiv intelligent sensors, providing alarm notification of various types of devices and environmental status, providing integrated web page visit function, local display and control function for the user.
	Sensors	Environmental and door status collecting	
Selection of safety system	Biometric access control	Intelligent lock with finger/card/pin access	A lock that supports the local ID card and can be opened by a key and can intelligently record access control history events, produce an alarm for unclosed door timeout and support remote door opening.
	Fire suppression system	Safety alarm suppress the fire during emergency conditions and provide notification	The fire fighting enclosure installed inside the system has a wealth of alarms and action indication notifications and can be connected to the monitoring platform, for more details refer to **Fire and Suppression Manual**.
	Video management	Real time monitoring	Support single route IPC (IP Camera) can obtain real time monitoring and photographing triggered by alarms.

2.6 Accessories

Table 2.6 IT Cabinet Accessories

BOM for Vertiv™ SmartCabinet™ Rack Frame (800 W)			
Item	**Description**	**Quantity**	**Remark**
1	Rack main structure includes 800 W x 1100 D x 2000 H (mm) in 2 mm thick with front glass door and rear plain split	1	Assembly one part
2	Integral panel base 800 W x 1100 D x 100 H mm	1	
3	Top panel with cable brush arrangement	1	Rack top side
4	Fixed shelf 500 W x 740 D	1	
5	Insulation tool kit comprising of insulation for top tray, insulation for bottom tray, and insulation for front side	1	
6	Gas Spring for auto door opening	2	
7	Electromagnetic lock on front and back door (2 No. on each door)	4	
8	LED lamp with bracket	2	
9	Cable tie 100 mm L (pkt of 100 No.)	1	

Table 2.6 IT Cabinet Accessories (continued)

Item	Description	Quantity	Remark
	BOM for Vertiv™ SmartCabinet™ Rack Frame (800 W)		
10	Cable tie 150 mm L (pkt of 100 No.)	1	
11	Gasket roll 30 mm x 1 mm for filling gaps	1	
12	Earthing rail 25 mm x 500 L copper strip	1	
13	1U cable manager with cable lups	1	
14	2U PVC dummy plate	14	
15	Industrial brush 150 - L (8x) + 200 - L (5x) + 100 - L (8X) in 1 set	5	
16	Vertical cable tray	2	
17	PDU channel	2	
18	Red blue tube light with 3 m 3 core wires with bracket	1	
19	Smoke detector bracket	2	

Table 2.7 Air Conditioning Cabinet Accessories

Name	Use	Quantity
Cable tie	Bundled cables	10
Cross recessed countersunk head screw M5 x 10	Cabinet screws (frame and cabinet pieces)	5
Plug M13.5	Unused through holes on the sealed cabinet (side plate screw mounting holes 2 x 2 = 4 Pcs)	4
Hexagon head bolt M12 x 30	Seal the upper lifting hole of the cabinet	12
Discharge pipe right angle elbow OD16	For air-conditioning air pipe connection	1
Liquid pipe right angle elbow OD12.7	Used for air-conditioning liquid pipe connection	1
Discharge pipe adapter tube OD16	For air-conditioning air pipe connection	1
Liquid pipe adapter tube OD12.7	Used for air-conditioning liquid pipe connection	1
Seal 6800 mm	Seal the gap between the connected cabinets	1
Sponge strip 20 x 20 mm/1702 mm	Used for sealing between PMC cabinet and air conditioning cabinet	2
Cross recessed hexagon head combination screws M6 x 25	Used in conjunction with M6 flange nut, used for cabinet fastening	8
Flange nut M6	Used in conjunction with cross-recessed hexagonal head combination screws, used to fasten cabinets	8

2.7 Environmental and Storage Requirements

2.7.1 Operational Environment

The Vertiv™ SmartCabinet™ should be installed away from the heat source or sparks. Avoid exposure to the direct sunlight and the contact with corrosive gases and organic solvent in the room. The operating conditions are shown in Table 2.8 below.

Table 2.8 Environmental Requirements (Operational Conditions)

Item	Requirements
Model dimension	42U 800 mm wide standard unit
Installation site	Indoor, Floor mount
Temperature	Indoor and outdoor unit of air conditioner for a standard model, 0 °C to +45 °C
Ambient humidity [1]	30% RH to 95% RH
Altitude [2]	Derating is required when the altitude is above 1000 m
Operation voltage range	3P + N, 380 VAC/400 VAC/415 VAC

NOTE: When the whole unit is operating at a high temperature and high humidity, condensate may appear on the external surface of front glass door and the display panel, but it does not affect the usage.

NOTE: For the air conditioner, derating is required for an altitude above 1000 m for the UPS. Refer to Vertiv™ Liebert® ITA2 (3 kVA to 20 kVA) UPS User Manual .

2.7.2 Storage Environment

Table 2.9 Storage Environment

Item	Requirements
Storage site	Indoor and free from dust
Ambient humidity	5% RH to 95% RH (Non-condensing)
Ambient temperature	-30 °C to 70 °C

2.7.3 Clearance Requirements

The clearance for the Vertiv™ SmartCabinet™ is shown in **Figure 2.3** below and **Figure 2.4** on the next page.

Figure 2.3 SmartCabinet™ 1100 mm Depth Rack
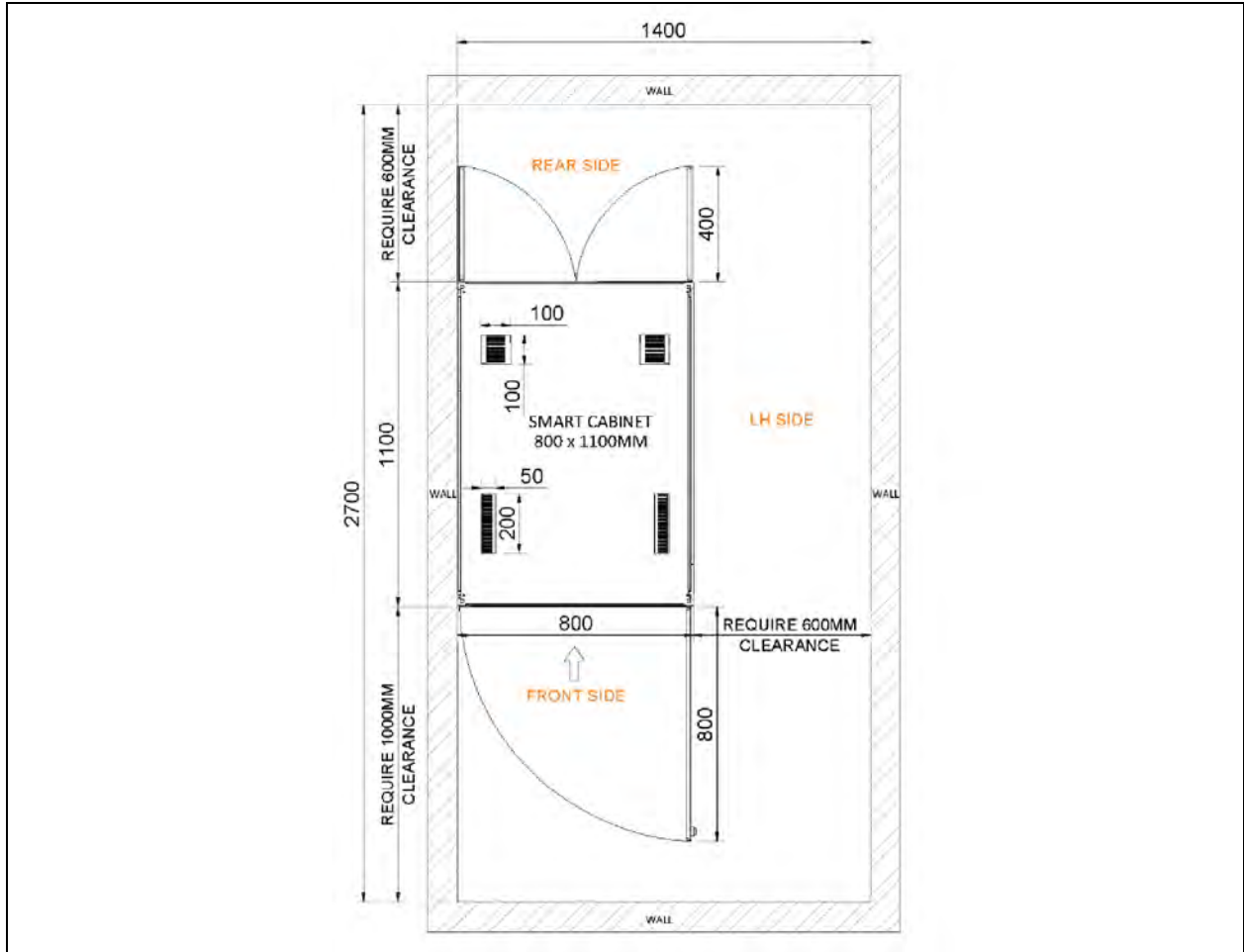
Figure 2.4 SmartCabinet™ 1200 mm Depth Rack
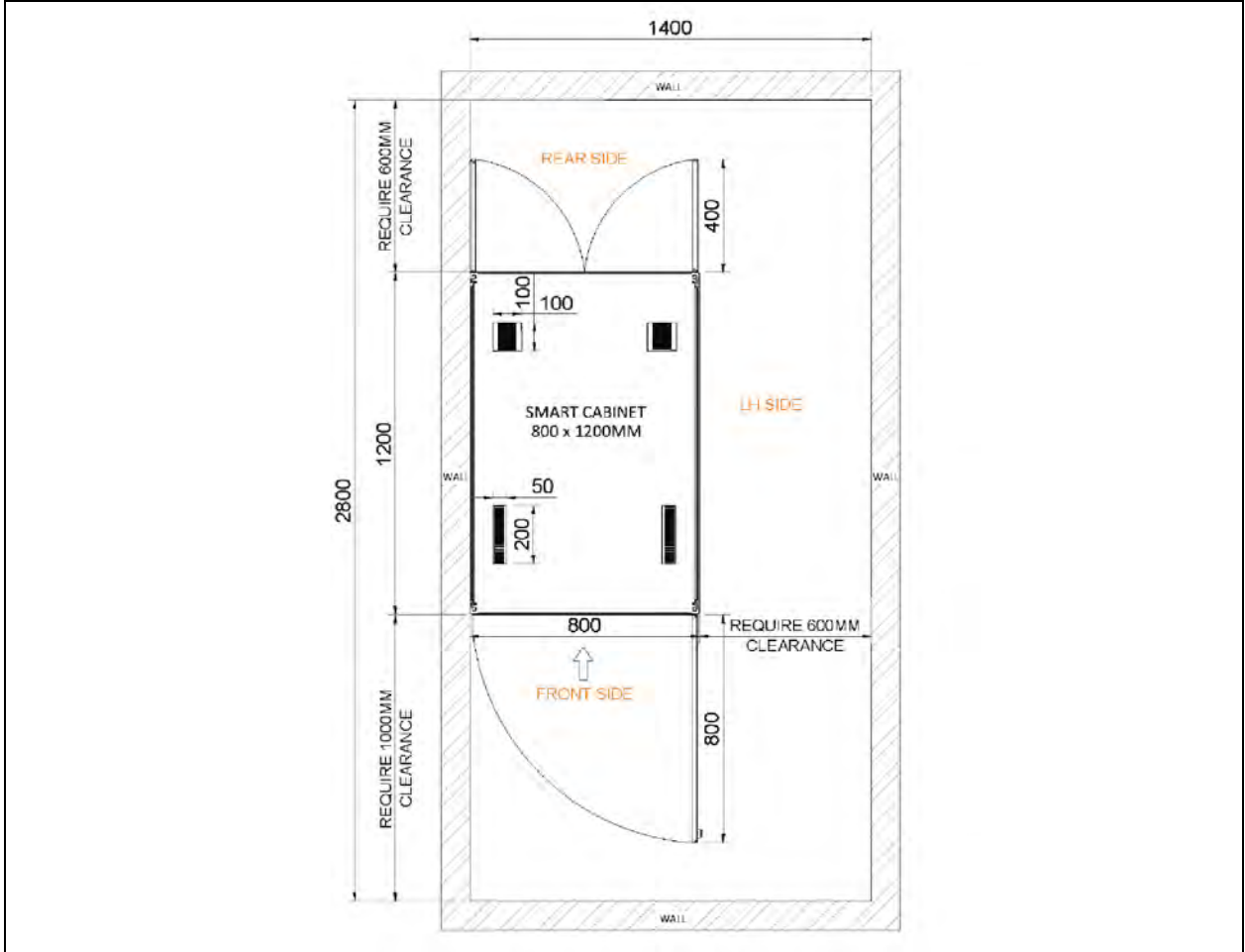
3 Pre-installation Requirements

This chapter describes the installation preparations for modular Vertiv™ SmartCabinet™ products, including installation tools, handling, unpacking, inspection, installation precautions, and room requirements.

Follow the below steps for pre-installation preparations:

1. Verification of pre-requisite readiness like floor leveling and maintaining clean room.
2. Marking of the racks on the flooring as per layout.
3. Unpacking and positioning of the smart cabinet racks.
4. Baying of racks for multirack smart cabinet.
5. Installation of UPS, batteries, and RCU indoor unit.
6. Installation of POD, connecting customer input cable and distribution of cables to UPS, and RCU inputs.
7. Installation of RDU sensors and network cabling.
8. Positioning of RCU ODU, installation of cable trays and copper piping from RCU indoor to outdoor.
9. Pressure testing and vacuuming of RCU units.
10. Installation and testing of fire suppression system and access control system.
11. Powering and commission of UPS, RCU, ACS, and fire suppression system.
12. Configuration of IP addresses in devices.
13. Configuration of RDU as per customer requirement.
14. Operational training to customer and the product final handover.

3.1 Installation Tools

SmartCabinet™ is a site assembled product. Refer to **Table 3.1** below and **Table 3.2** on the next page for tools required for SmartCabinet™ assembly and **Table 2.6** on page 10 and **Table 2.7** on page 11 for list of accessories.

Table 3.1 Tools Required for SmartCabinet™ Assembly

Item	Description	Quantity
1	Spanner set for M10 and M12 bolt	1
2	Bit set for M6, M5, and M4 hex head bolt	1
3	Bit for minus slot	1
4	Bit for plus slot	1
5	Mallet (plastic hammer)	1
6	Plyer	2
7	Nose plyer	1
8	Stripper cutter	1
9	Blade cutter	1
10	Screwdriver set plus, minus (M6, M5, M4, M3)	2
11	Connector	1

Table 3.1 Tools Required for SmartCabinet™ Assembly (continued)

Item	Description	Quantity
12	Poker	1
13	Allen key set	1
14	Nut runner Set	1
15	Chisel	1
16	Leveling gauge	1
17	Hex wrench set	1
18	File	1

NOTE: All hardware of Vertiv™ SmartCabinet™ to be supplied with racks.

3.1.1 Required Material

Table 3.2 Required Material

Name	Specification				
	Project	System Maximum Current (A)	Minimum Cable Cross-sectional Area (mm^2) (Ambient Temperature: 25 °C)	Minimum Specification of Circuit Breaker	Yellow-Green Ground Wire Cross-sectional Area (mm^2) (Ambient Temperature: 25 °C)
Distribution cables and circuit breakers from the server room to the product	10 kVA	40	16	3P 125 A	16
	20 kVA	75	16	3P 125 A	16
Air conditioner condenser power cord	Minimum cable cross-sectional area (mm^2) (ambient temperature: 25 °C)				
	1.5				
Connecting copper pipes for indoor and outdoor air conditioners	Discharge line: 16 mm, liquid pipe: 12.7 mm				
	Project	Equivalent length	Discharge line	Liquid line	
The air-conditioned indoor and outdoor machines are connected to copper pipes	MSR2-F12	10 m	16	12.7	
		20 m	16	12.7	
		30 m	19	12.7	
		40 m	19	16	
		50 m	19	16	
	MSR2-F25	10 m	19	12.7	
		20 m	19	16	
		30 m	22	16	
		40 m	22	16	
		50 m	22	19	

Proprietary and Confidential ©2024 Vertiv Group Corp. 3 Pre-installation Requirements

NOTE: The maximum current of the system is calculated based on the full load of the system and the heating and humidification of the air conditioning configuration.

NOTE: * Indicates the need to add long line pipe kit.

NOTE: If the pipe length is more than 50 m, consult Vertiv representative.

NOTE: If the ambient temperature of the outdoor unit of the air conditioner is lower than -20 °C, low temperature components are required.

3.2 Equipment Handling, Unpacking, and Inspection

3.2.1 Equipment Component Size

Table 3.3 Dimensions and Weight

Item No.	Item Description	Weight Details (kg)
5060S0130000	Automatic, regulatory apparatus, for IT systems, SC-1-3	390
5060S0133200	Automatic, regulatory apparatus, for IT systems, SC-1-3 U3 2N	450
5060S0170000	Automatic, regulatory apparatus, for IT systems, SC-1-7	440
5060S0270201	Automatic, regulatory apparatus, for IT systems, SC-2-7 RC	800
5060S0136200	Automatic, regulatory apparatus, for IT systems, SC-1-3 U6 2N	550
5060S0233200	Automatic, regulatory apparatus, for IT systems, SC-2-3-RC U3 2N	950
5060S2710201	Automatic, regulatory apparatus, for IT systems, SC-27 RC U10 2N	1150
5060S0230200	Automatic, regulatory apparatus, for IT systems, SC-2-3-RC	670
5060S0170001	Automatic regulatory apparatus for IT systems, SC-1-7 DS	480
5060S0276201	Automatic, regulatory apparatus, for IT systems, SC-2-7-RC-U6 2N	980
5060S0230201	Automatic regulatory apparatus for IT systems, rack accessories for SC-2-3 RC	670
5060S0434000	Automatic regulatory apparatus for IT systems, for SC4-3 RC4	1360
5060S0236200	Automatic, regulatory apparatus, for IT systems, SC-2-3-RC U6 2N	885
5060S2710202	Automatic, regulatory apparatus, for IT systems, SC-27 RC DS-U10 2N	1250
5060S2710200	Automatic, regulatory apparatus, for IT systems, SC-2-7 U10 2N	1150
5060S0230000	Automatic, regulatory apparatus, for IT systems, SC-2-3	590
5060S0176201	Automatic regulatory apparatus for IT systems, SC-1-7 DS U6 2N	680

3.2.2 Equipment Inspection

Check the list is complete according to the packing list and inspect whether the parts are damaged.

⚠️ **WARNING! Risk of top heavy unit falling over. Improper handling can cause equipment damage, injury, or death. Read all the following instructions and verify that all lifting and moving equipment is rated for the weight of the unit before attempting to move, lift, remove packaging from or prepare the unit for installation.**

⚠️ **CAUTION: Risk of overhead interference! Can cause unit and/or structure damage. The unit may be too tall to fit through a doorway while on the pallet. Measure the unit and doorway heights and refer to the installation plans prior to moving the unit to verify clearances.**

⚠️ **CAUTION: Risk of unit damage if improperly stored! Keep the unit vertically upright, indoors, and protected from dampness, freezing temperatures, and contact damage.**

⚠️ **CAUTION: Risk of sharp edges, splinters, and exposed fasteners. Can cause personnel injury. Only authorized and trained personnel wearing appropriate safety headgear, gloves, shoes, and glasses should attempt to move, lift, remove packaging from the unit, or preparing unit for installation.**

Before unpacking the unit, it is the customer's responsibility to:

- Verify that the labeled equipment matches the bill of material.
- Carefully inspect all items for visible or concealed damage.
- Report damage immediately to the carrier and file a damage claim with a copy sent to Vertiv or to the local Vertiv representative.

Packing Material

All materials used to package this unit are recyclable. Save for future use or dispose of the material appropriately.

NOTE: Packing list comes along with the invoice.

Figure 3.1 Recyclable Packaging Materials
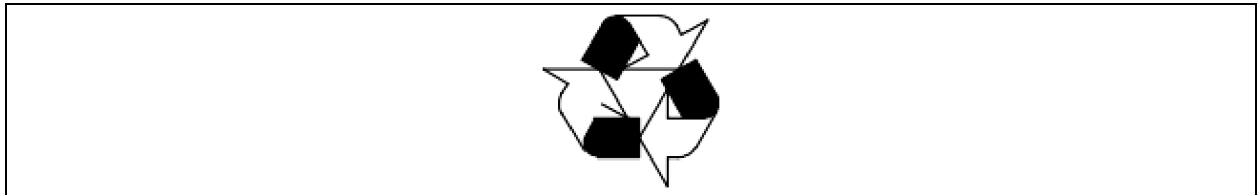
3.2.3 Equipment Handling

⚠️ **WARNING! Risk of improper lifting and handling of the unit. Can cause equipment damage, injury, or death. The unit is supplied in two modules placed side by side. Do not use the eyebolts that are fixed on top of the unit to lift the two modules together. These eyebolts can only be used to lift the single module, after it has been removed from the packaging.**

⚠️ **CAUTION: Risk of lifting or moving unit with high speed. Can cause equipment damage. Lift the unit with a speed suitable for the load to be moved.**

Recommended unit handling equipment

Figure 3.2 Handling Equipment
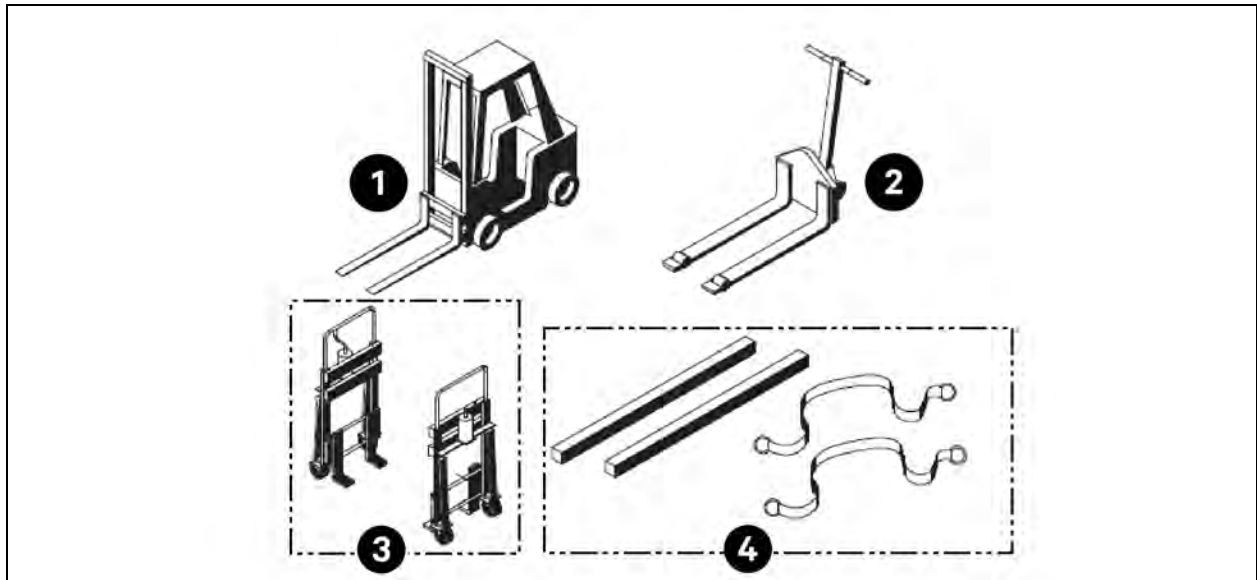
Item	Description
1	Fork lift
2	Piano jack lift
3	Pallet jack
4	Spreader bars and slings

Handling the unit while packaged

NOTE: Transport the packaged unit using a forklift or pallet jack, otherwise use a crane with slings and spreader bars.

When using a forklift or pallet jack:

- Ensure that the fork length is suitable for the unit length and, if adjustable, spread to the widest allowable distance that will fit under the pallet.
- When moving the packaged unit, lift the unit from either end of the pallet, and do not lift the unit higher than 2 in. (51 mm) to 4 in. (102 mm) from the ground.

NOTE: Any personnel are not allowed to operate closer than 3.7 m from the handled packaged unit.

- If the unit requires to lift higher than 4 in. (102 mm), necessary precautions must be taken and ensure that all personnel not directly involved in moving the unit must be away 12.1 ft (3.7 m) from the lift point of the unit.
- Always refer to the location of the center-of-gravity indicators when lifting the unit.

3.2.4 Unpacking the Unit

To unpack the unit, follow the below procedure:

1. Remove the exterior stretch wrap packaging material from around the unit, exposing the protective corner and side packaging planks as shown in **Figure 3.3** below.

Figure 3.3 Removing the Exterior Stretch Wrap
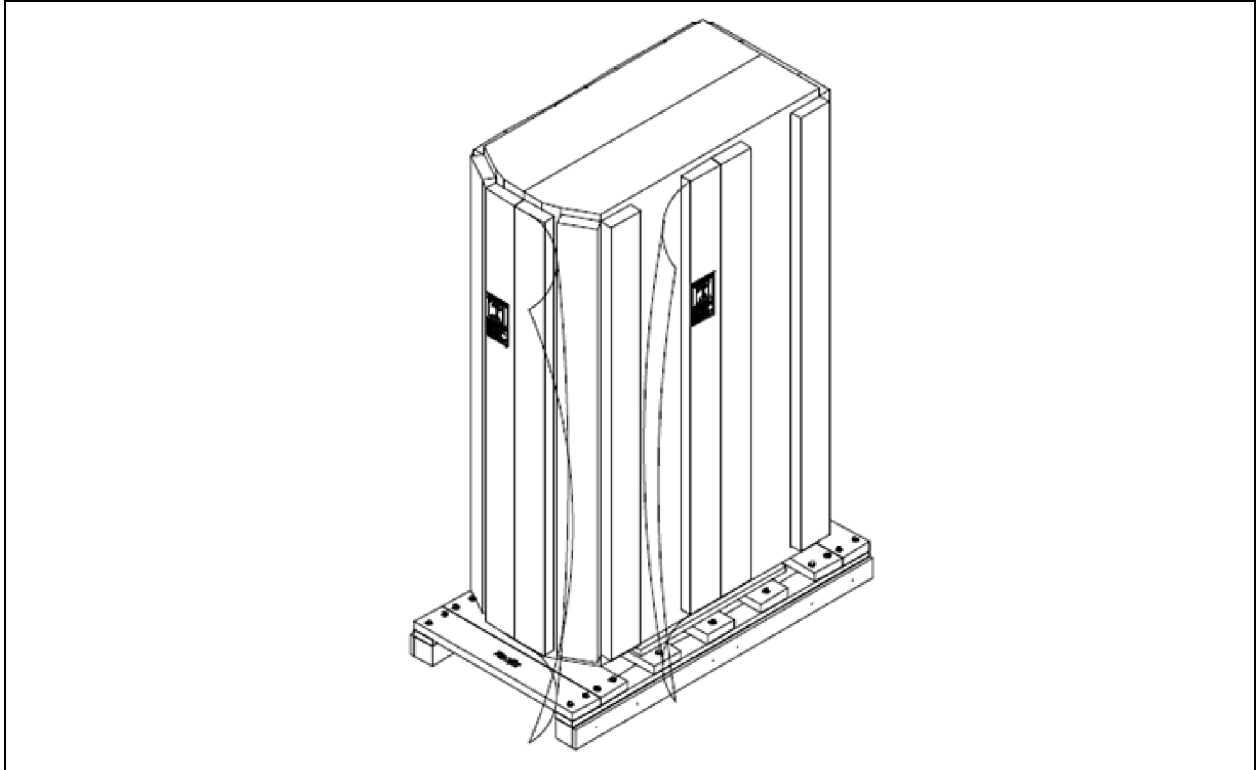
2. Remove the corner and side packaging planks from the unit, exposing the packaging bag over the unit as shown in **Figure 3.4** on the facing page.

NOTE: The bag may remain in place to protect unit panels and from dust, or it may be removed for immediate unit installation.

Figure 3.4 Removing the Corner and Side Packaging Planks
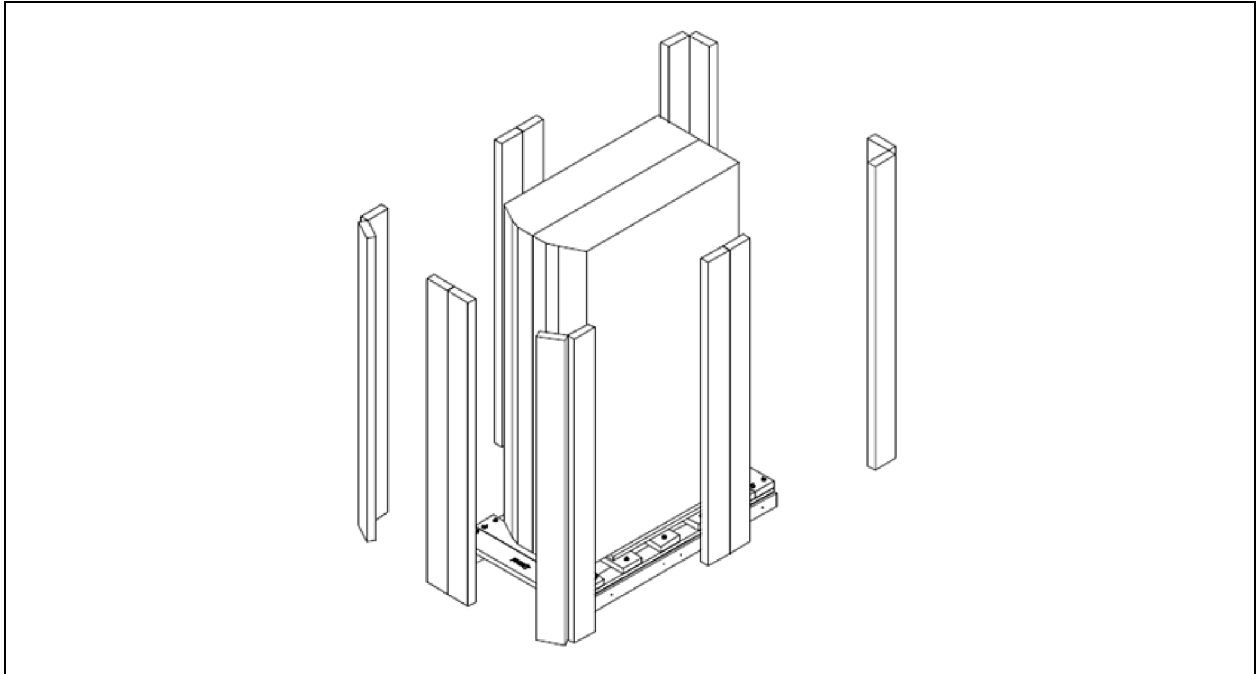
3. Remove the packaging bag from the unit when ready to remove the pallet and install the unit.

Figure 3.5 Remove the Packaging Bag
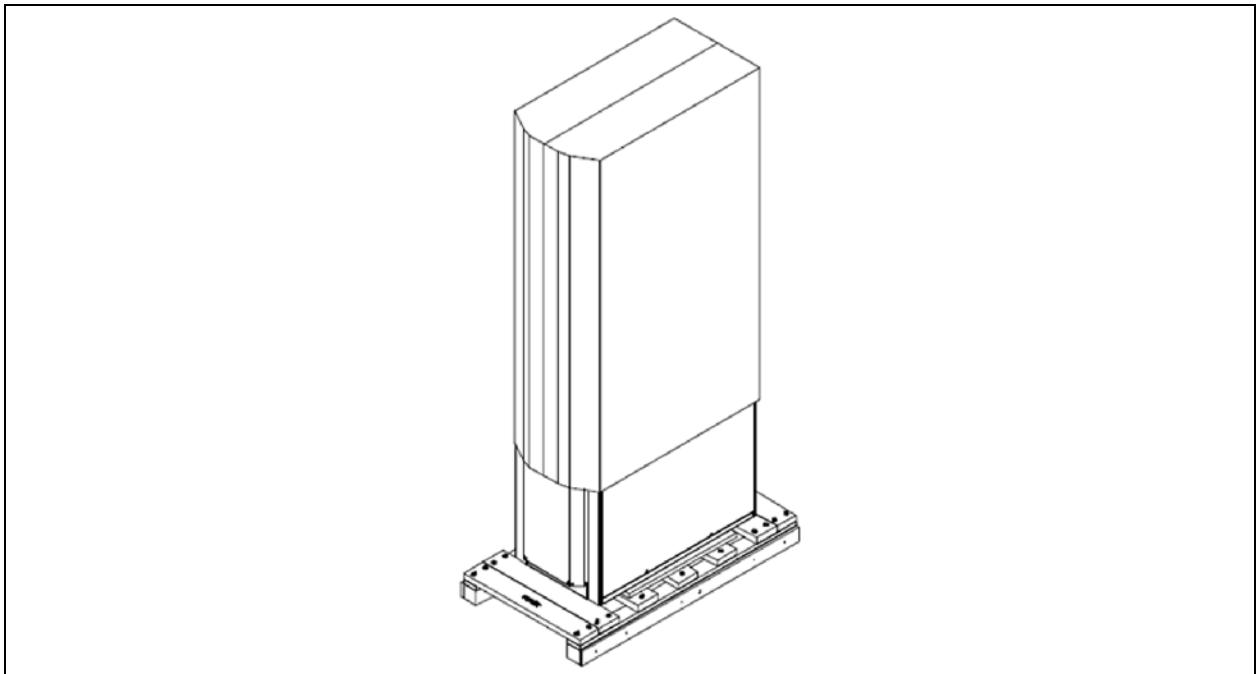
3.2.5 Removing the Unit from the Pallet

Using Forklift

1. Align a forklift with either the front or rear side of the unit.

NOTE: Ensure that the fork length and distance is suitable for the unit length and ensure the unit stability.

2. Use the center of gravity indicators on the unit to determine the entry points for the tines. Center of gravity varies per unit size and selected options.

NOTE: The tines shall be equally spaced on either side of the center of gravity indicator.

3. Insert the tines of the forklift completely under the base of the unit.

NOTE: Ensure that the tines are level and not angled in an upward direction.

NOTE: The height of the tines must provide the suitable clearance under the unit.

NOTE: Spread the forks to the widest allowable distance that will fit under the unit and ensure that the tines of the forklift are locked to the widest location.

4. Remove the bolts that secures the unit to the pallet from the base of the unit.
5. Slightly lift the unit off the pallet to an elevation point where the pallet is not supporting the weight of the unit and remove the pallet under the unit.

Figure 3.6 Remove the Pallet with a Forklift
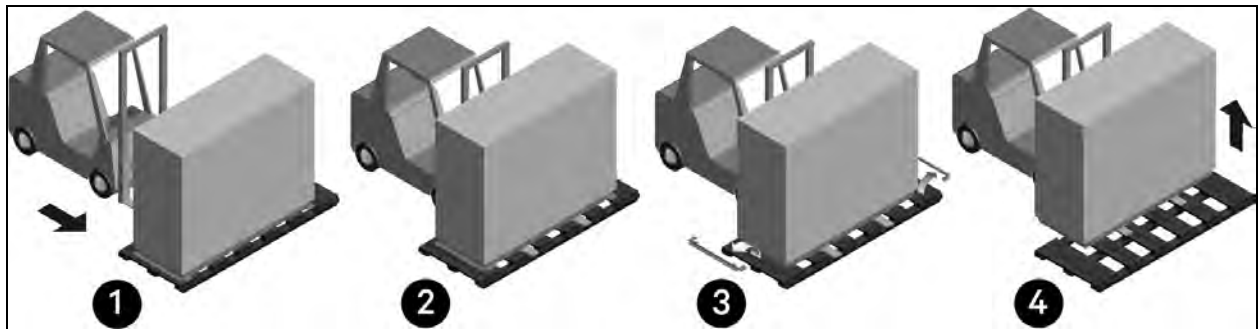
Item	Description
1	Align forklift with front or rear of unit.
2	Insert tines completely under base of unit.
3	Remove bolts which secures unit to the pallet.
4	Lift unit and remove the pallet.

Removing the Unit from the pallet using Crane

1. Use the center of gravity indicators on the unit to determine the position of the slings.

NOTE: The slings shall be equally spaced on either side of the center of gravity indicator.

NOTE: Ensure that the distance between slings maintains the unit stability.

2. Place the slings between the bottom rails of the unit and the pallet at the widest allowable distance as shown in **Figure 3.7** below.

NOTE: Unit is shown without packaging. These instructions may be followed with or without the outer packaging in place.

Figure 3.7 Removing the Unit from Pallet with a Crane
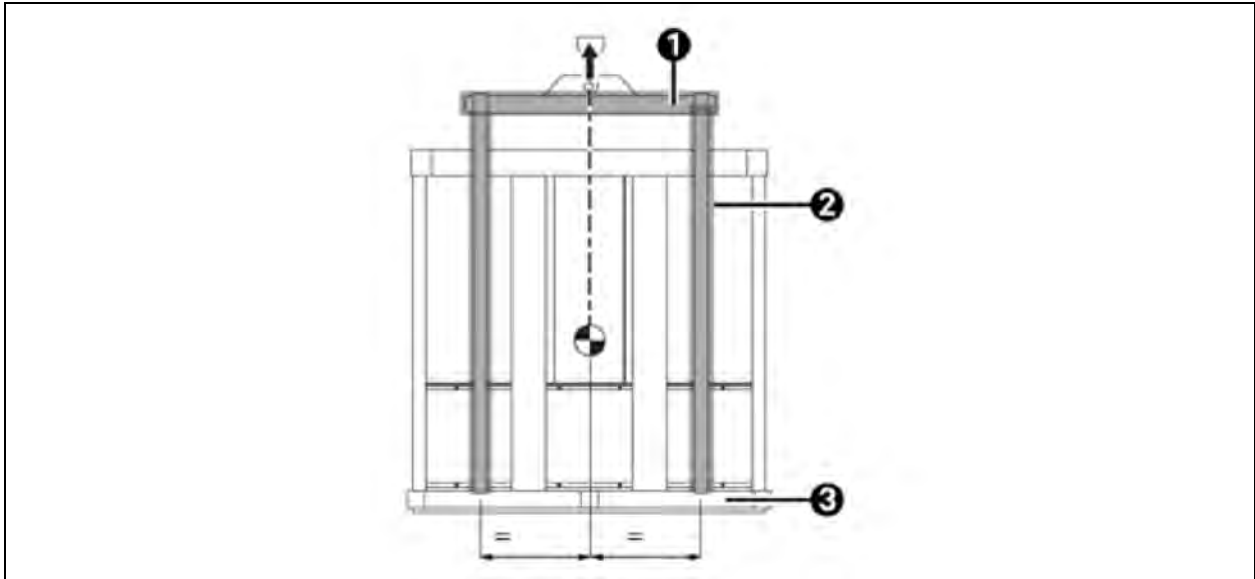
Item	Description
1	Spreader bar
2	Slings
3	Pallet

3. Align the slings as described previously. Use spreader bars or equivalent device to ensure proper protection of the unit, see **Figure 3.7** above.

4. Secure the slings to a spreader bar.

5. Remove the bolts that secures the unit to the pallet from the base of the unit, see **Figure 3.7** above.

NOTE: Depending on final installation location, the pallet may need to remain under the unit. Therefore, the bolts would not yet be removed.

6. Slightly lift the unit off the pallet to an elevation point where the pallet is not supporting the weight of the unit and remove the pallet under the unit, see **Figure 3.7** above.

Figure 3.8 Removing the Unit from the pallet Using Crane
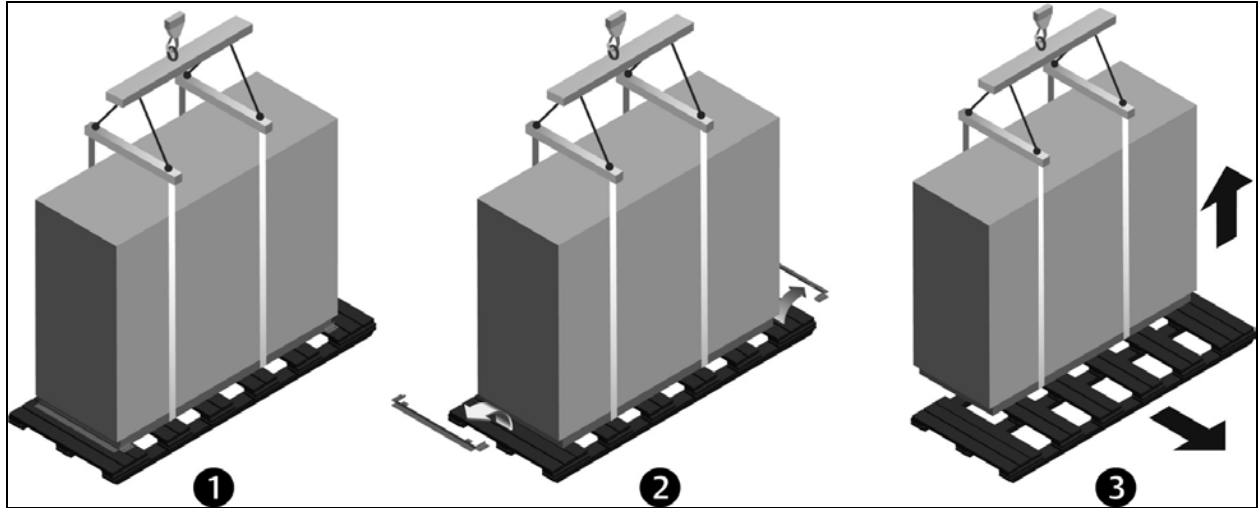
Item	Description
1	Spreader bars and rigging on unit.
2	Remove lag bolts and brackets.
3	Lift the unit and remove the skid.

NOTE: All cabinet packaging materials are recyclable. Keep the packaging materials for future use or dispose properly.

3.2.6 Moving the Unit to the Installation Location Using Piano Jacks

1. With the unit elevated, position piano jacks at each end of the unit.
2. Lower the unit to a height suitable for the piano jacks, place protective material between the unit and the piano jacks and straps.
3. With the unit secured to the piano jacks, move the forklift away from the unit.
4. Using the piano jacks, at least two trained personnel can move the unit to the site for installation.

 3 Pre-installation Requirements

Figure 3.9 Moving the Unit with Piano Jacks
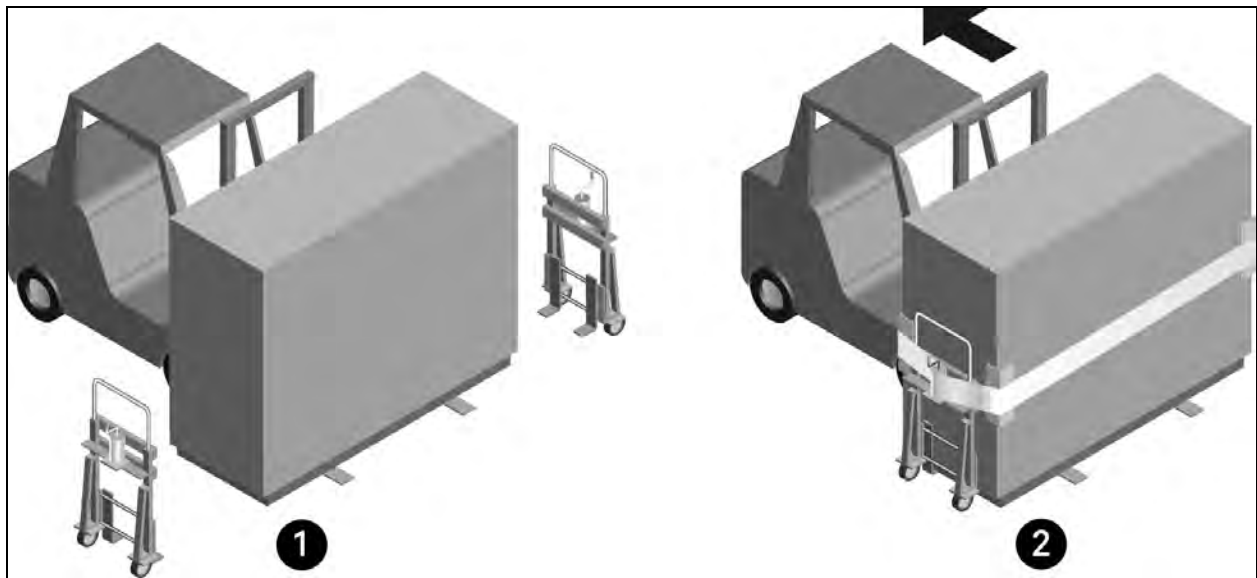
Item	Description
1	Place piano jacks on each end of the unit.
2	Use padding between unit and straps and, with the unit secured to the piano jacks, move the forklift away from the unit.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp. 3 Pre-installation Requirements

4 Mechanical Installation

This chapter describes the installation of the Vertiv™ SmartCabinet™.

NOTE: Keep all the installation tools and components handy before installation and operation according to the content in this chapter.

There are two types of installation of two kinds of units: The installation flow chart for 800 mm wide and 1100 mm and 1200 mm deep unit is shown in **Figure 2.3** on page 13.

4.1 Rack Placement

The steps for placement of rack are as mentioned below:

1. Ensure to maintain sufficient clearance to facilitate the installation and maintenance of the Cabinet. See **Figure 2.3** on page 13 and **2.7.3** on page 13 for clearance requirement.

2. Mount the rack having dimensions 2100 mm(H) x 800 mm (W) x 1100 mm (D) on flat surface as shown in **Figure 4.1** below.

Figure 4.1 800 mm Wide Standard Unit 42U

Item	Description
1	Flat surface

4.2 Horizontal Cable Manager

Hardware Required:

- M6 x 20 Bolt (04 numbers)

- M6 Cage Nut (04 numbers)
1. Install the cage nut in the top square cut-outs of the U space on front rack flange.
2. Mount a 19 in. horizontal cable manager on front top side U space and bolt it by M6 x 20 bolts and M6 cage nut. See **Figure 4.2** below.

Figure 4.2 Horizontal Cable Manager
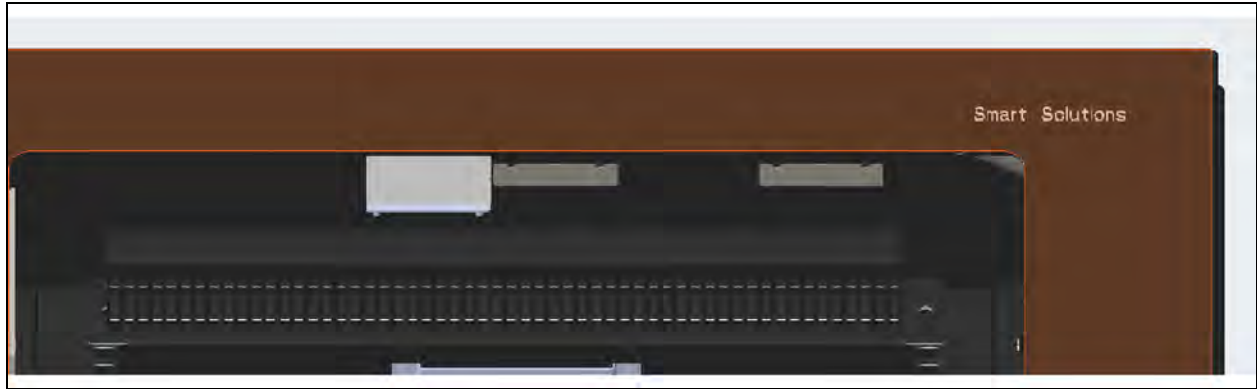
4.3 Power Output Distribution (POD) Device 3 kVA/6 kVA

1. Mount the 19 in. rack mount POD device on the front top side U space and below the cable manager.
2. Secure it by M6 x 20 bolts. See **Figure 4.3** below.

Figure 4.3 POD Device 3 kVA/6 kVA (1)

Proprietary and Confidential ©2024 Vertiv Group Corp. 4 Mechanical Installation

Figure 4.4 POD Device 3 kVA/6 kVA (2)
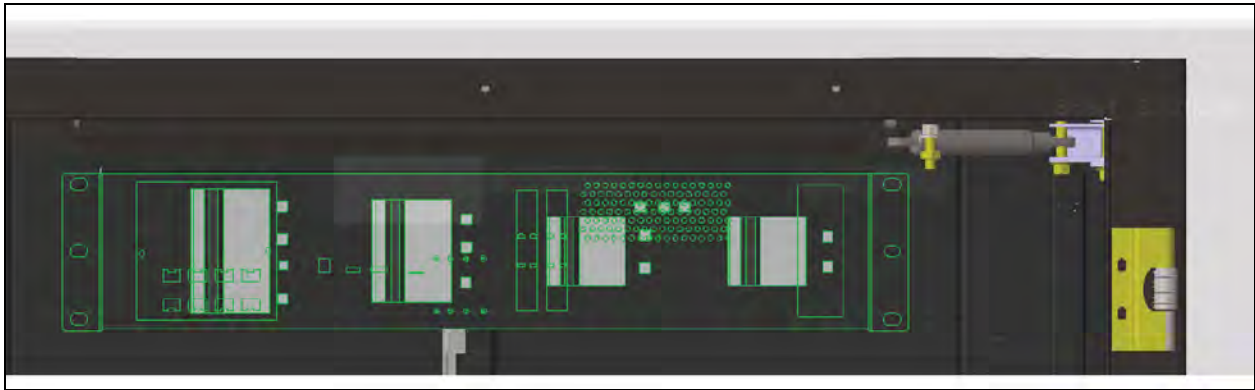
4.3.1 Cabling Details

Figure 4.5 6 kVA UPS
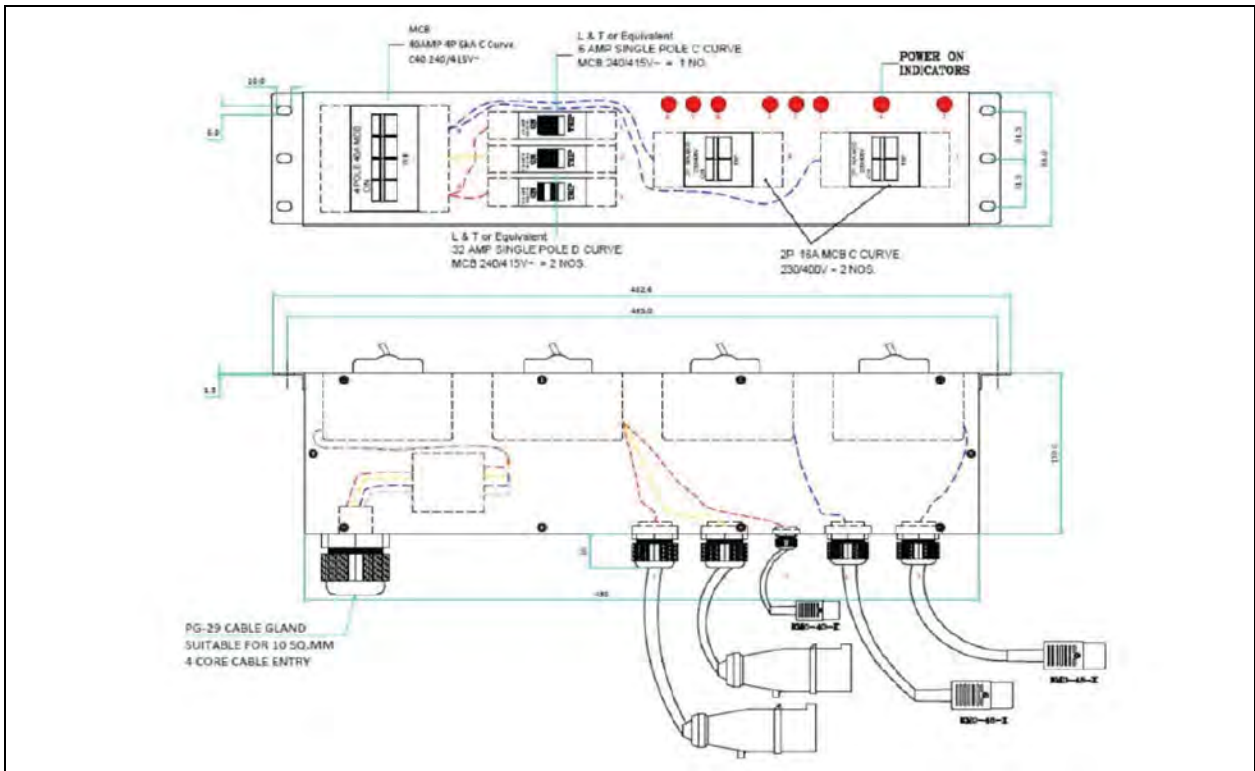
Figure 4.6 10 kVA UPS
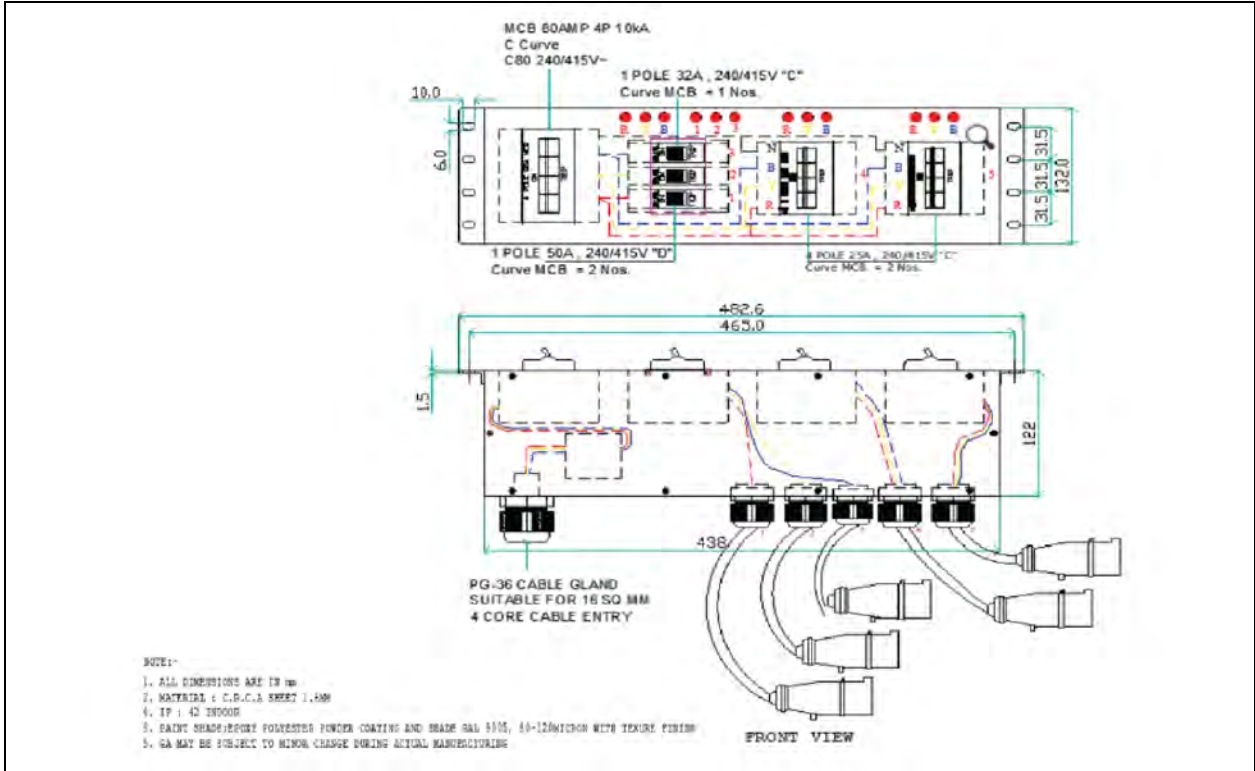
4.4 RDU-A (Rack Mount)

Hardware Required:

1. M6 × 20 Bolt Hex (quantity: 04).

2. M6 Cage Nut (quantity: 04).

3. Before mounting the RDU-A, place the 4-Com card from rear side, See **Figure 4.7** on the facing page for the mounting location of the card.

4. Mount RDU-A on the front side U space of the rack and below POD device, secure it with bolts (M6 × 20).

Figure 4.7 Mounting RDU-A Inside Rack
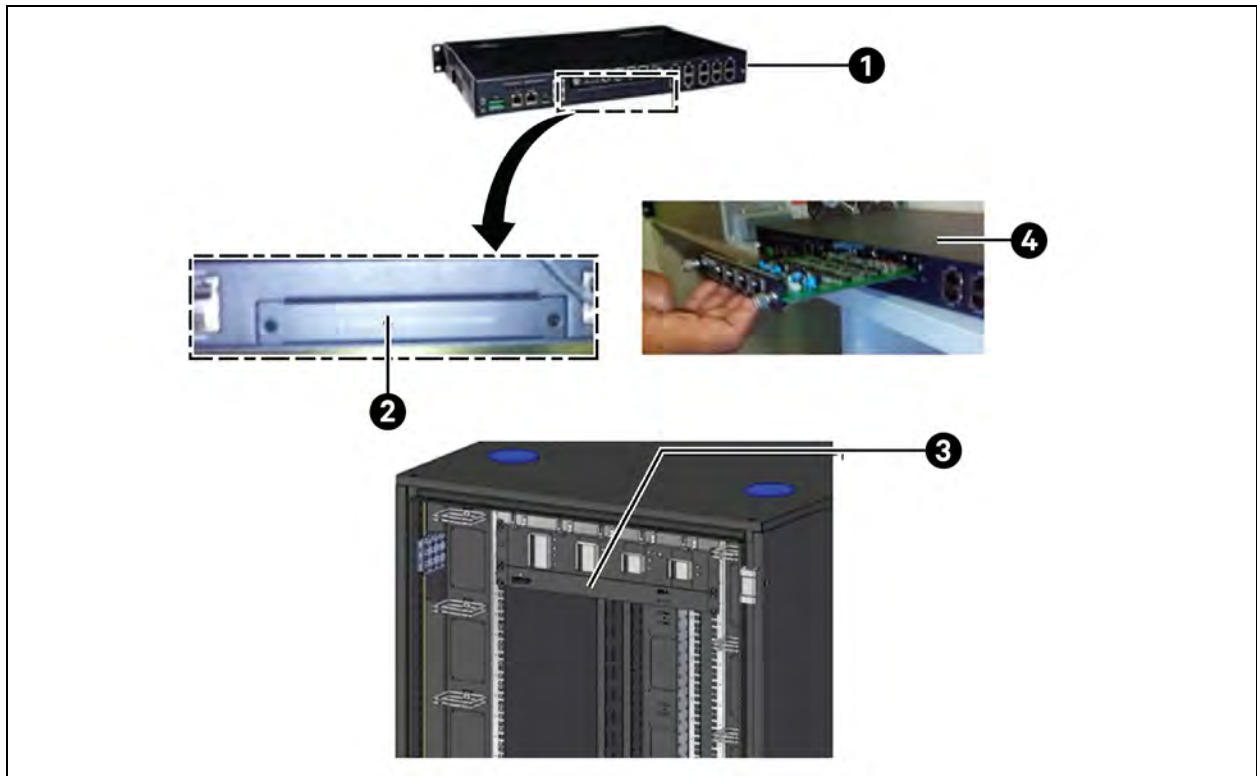
Item	Description
1	RDU-A (19 in. rack mount)
2	Location for 4-com card
3	RDU-A (19 in. rack mount 1U)
4	Place the 4-com card

Figure 4.8 RDU-A (19 in. rack mount)

4.5 UPS Installation

Vertiv™ Liebert® GXT RT + 3 kVA, ITA2 6 kVA/10 kVA long backup, quantity: 02.

The system can choose to configure with the products Liebert® GXT RT 3 kVA UPS, ITA2 6 kVA UPS, ITA2 10 kVA UPS, ITA2 20 kVA UPS, and batteries. The UPS is installed in the lower U space of the cabinet through the power distribution unit (referred to as PDU) installed in the same cabinet to achieve the introduction of municipal power and power distribution Unit functions. The UPS in the system configuration needs to be installed on-site with the customer, and the battery and UPS installation methods are described below.

NOTE: Liebert® ITA2 3 kVA UPS comes both with its own battery or external battery, so there is a need to install an independent battery module if the battery is external.

Figure 4.9 UPS Brackets Installation
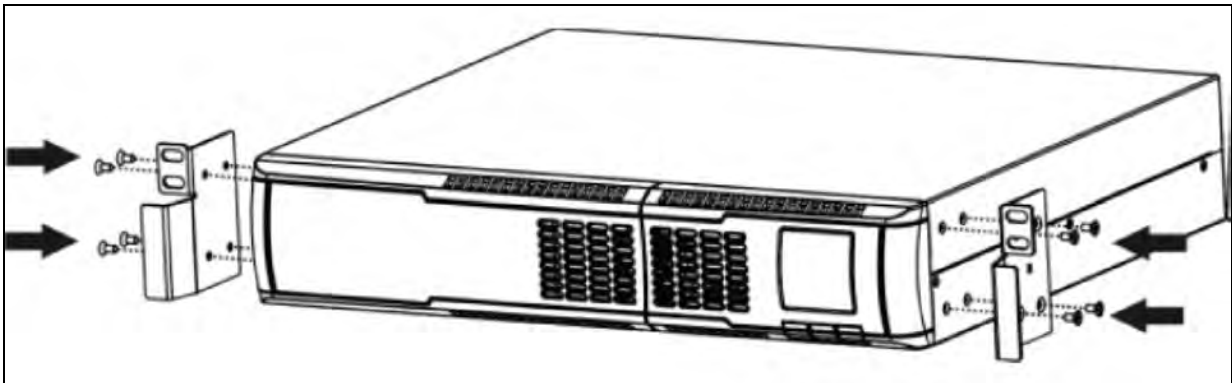
To mount UPS mount first mount the L brackets on LH and RH side of U space of vertical rail and below the RDU-A. Keep 2U distance between the RDU-A and L bracket, mount cage nuts in square cutouts and fix brackets by M6 x 20 Bolt, then Lift the UPS onto the L brackets and slide the UPS to the rear of the rack cabinet until the front face of the UPS gets closer to front vertical rail. Mount the two UPS sets using same procedure.

Hardware Required:

1. M6 x 20 bolt hex (quantity: 12)/set.
2. M6 nut (quantity: 12)/set.

Cabling Details:

1. Input supply - POD.
2. Output supply - PDU.

Input cable - Join the IEC connector of input cable POU to input of UPS. Input cable will provide with UPS for details refer **UPS User Manual**.

Figure 4.10 Installation of UPS
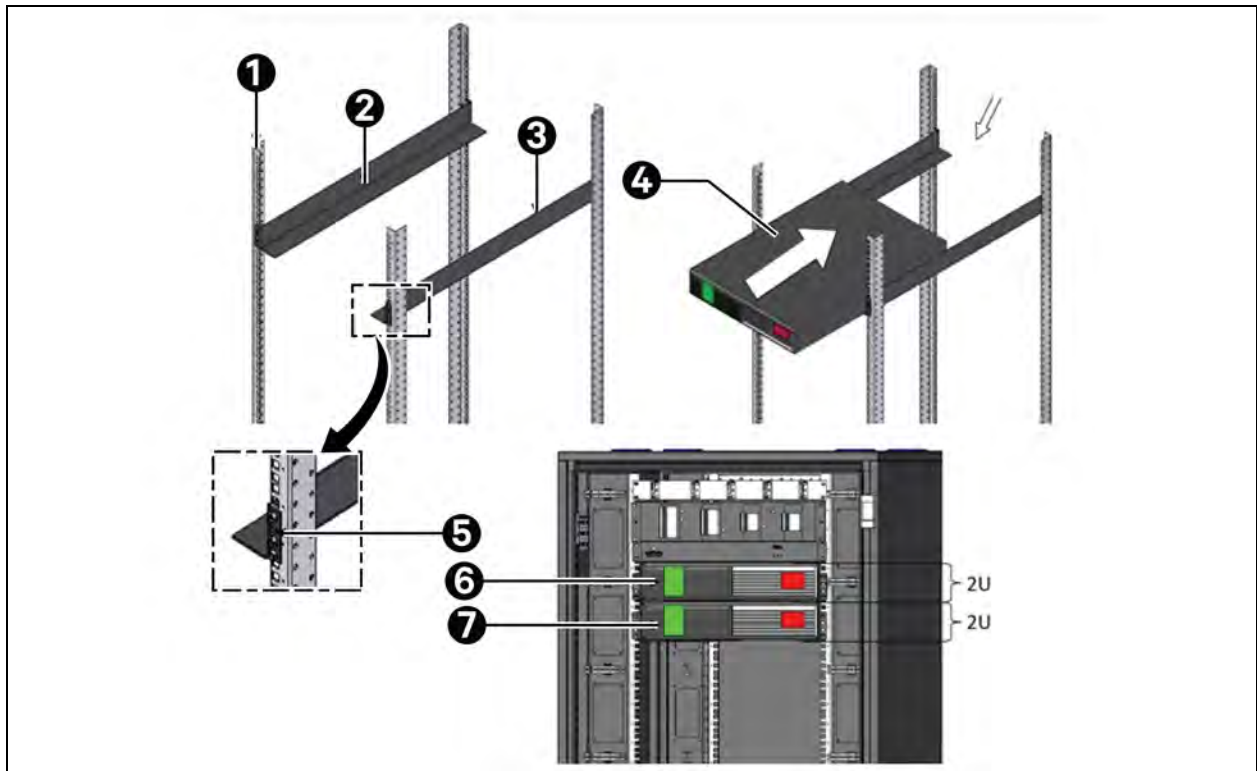
Item	Description
1	Vertical rail
2	LH bracket
3	LH bracket
4	3 kVA UPS
5	M6 x 20 bolt
6	3 kVA UPS-1
7	3 kVA UPS-2

NOTE: For PCA modbus card setting refer to Communication Card Manual.

Figure 4.11 UPS installed Position
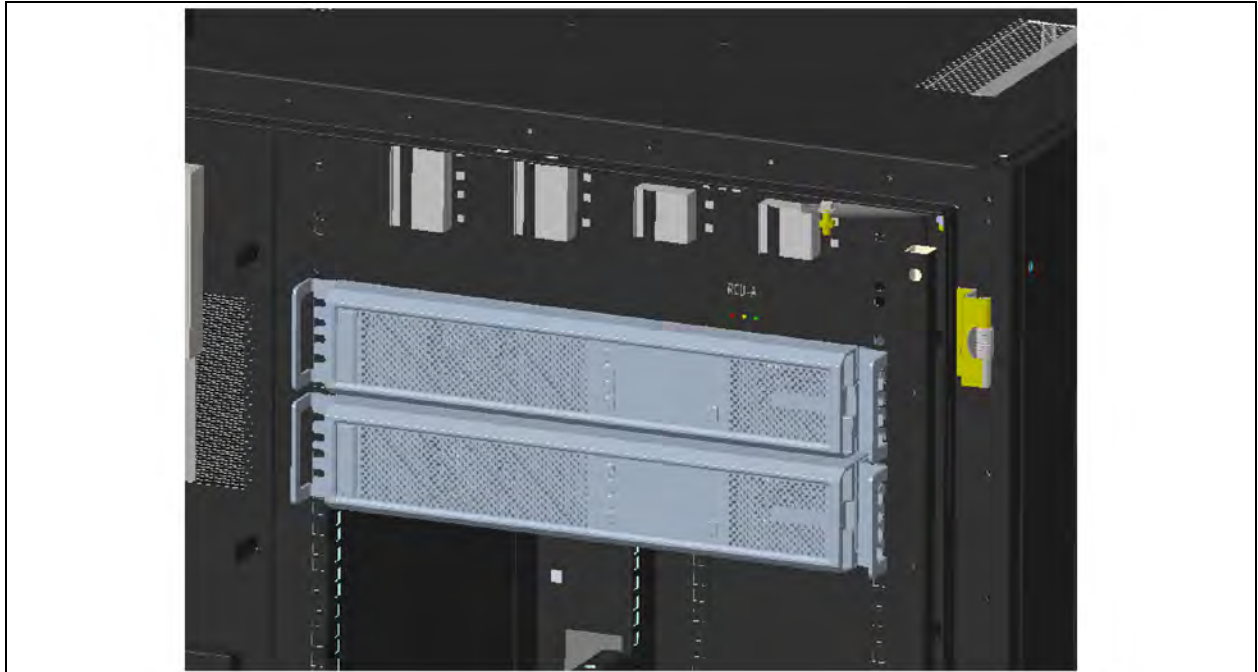
4.5.1 Battery Module

To place battery, we have to first mount L brackets on LH and RH side on rail exactly under UPS and then lift the battery module onto the L brackets and slide it to the rear of the rack cabinet until front face of battery closer to front vertical rail. Keep 2U distance between component shelf and lower end of L bracket, mount two batteries set using same procedure.

Hardware required:

1. M6 x 20 bolt hex (quantity: 08)/set.
2. M6 Cage Nut (quantity: 08)/set.

Figure 4.12 Installation of Battery Module
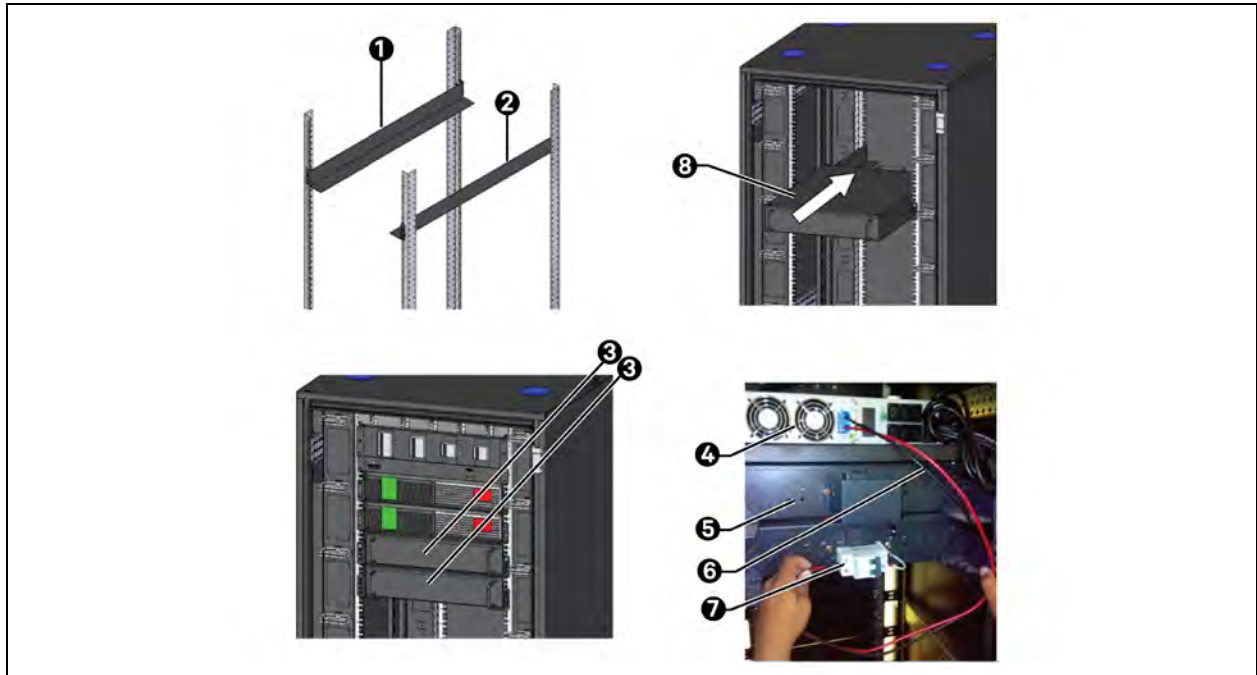
Item	Description
1	LH bracket
2	RH bracket
3	Battery module 7 Ah, block (2U) - 02 numbers
4	UPS 3 kVA
5	Battery module
6	Cables
7	MCB on rear side of battery module
8	Battery module

Figure 4.13 Installed Position of Battery Module

Cable detail:

Take battery connection cable from UPS kit; connect one end on UPS and other end with battery. Ensures that red cable is connected to the phase (red) terminal and black to neutral (black) terminal. See **Figure 4.12** on the previous page. Make connections for UPS-2 and battery-2.

NOTE: Vertiv™ Liebert® ITA2 3 kVA UPS comes both with its own battery or external battery, so there is a need to install an independent battery module if the battery is external.

4.6 Installation of Vertical Socket Strip (PDU)

The standard vertical PDU needs to be mounted on the key slots available on the PDU channel. In case of mounting any non-standard vertical PDU on rear right side of rack, first we must mount sheet metal bracket on rear right vertical channel of rack to fix position of bracket make marking by putting PDU on rack vertical channel and then mount sheet metal bracket as shown in **Figure 4.14** on the facing page use M5 self. Take PDU first mount it on depth manager M5 self-tapping screw after that mount on sheet metal bracket. Follow the same procedure to mount second PDU on rear left side of rack as shown below:

Hardware Required:

1. M5 x 10 self-tapping screw (quantity: 04).

Figure 4.14 Installation of Vertical Socket Strip (PDU)
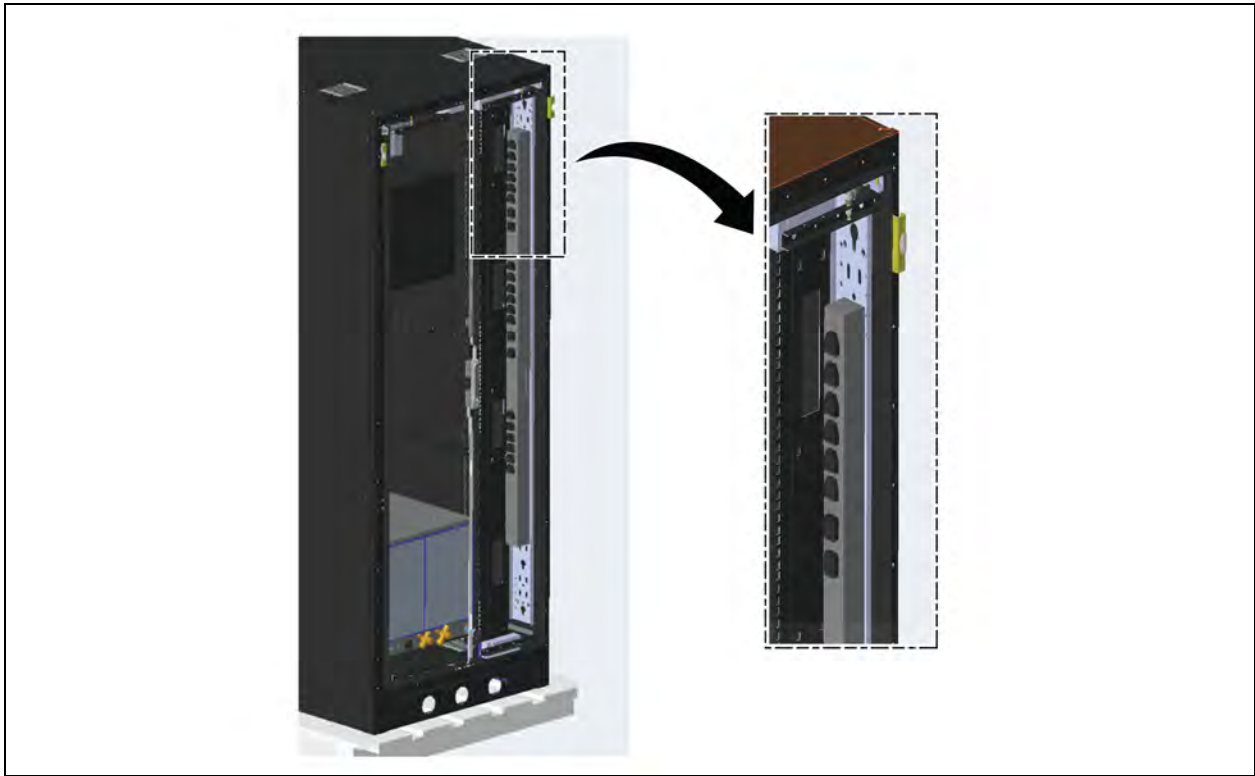
4.7 RCU Cooling Unit

Steps to mount RCU unit at the bottom of vertical rail are as mentioned below:

1. At first Keep three cutouts empty (as shown in **Figure 4.15** on the next page).
2. Then mount given L bracket LH and RH on vertical rail.
3. Install 8 cage nuts as needed into the square holes on the vertical rail at front and rear.
4. Fastened with M6 bolt and then lift the RCU unit onto the L brackets.
5. Slide it to the rear of the rack cabinet until front side of RCU closer to front vertical rail.

NOTE: For cabling and piping details refer to RCU manual.

Hardware required:

1. M6 x 20 bolt hex washers slotted (quantity: 08).
2. M6 cage nut (quantity: 08).

Figure 4.15 Installation of RCU Cooling Unit
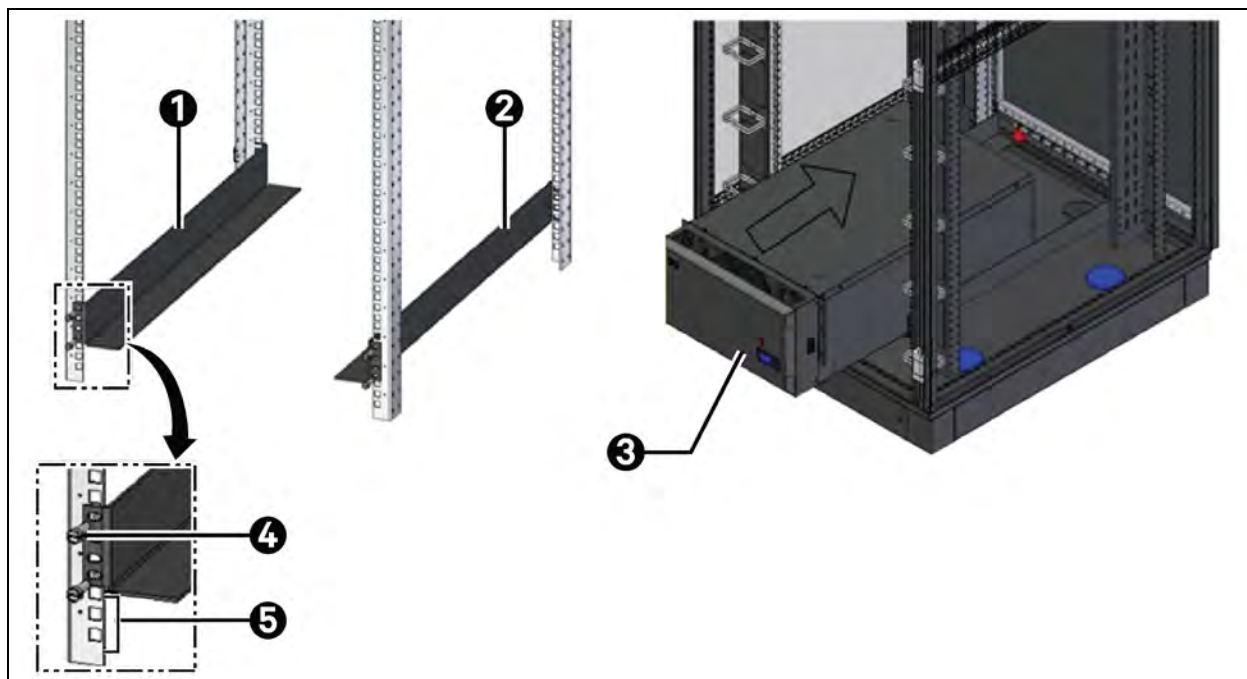
Item	Description
1	LH bracket
2	RH bracket
3	RCU cooling unit (3.5 kW)
4	M6 x 20 bolts
5	Keep three cutouts empty then mount L-bracket

Proprietary and Confidential ©2024 Vertiv Group Corp.   4 Mechanical Installation

Figure 4.16 Installed Position of RCU Cooling Unit
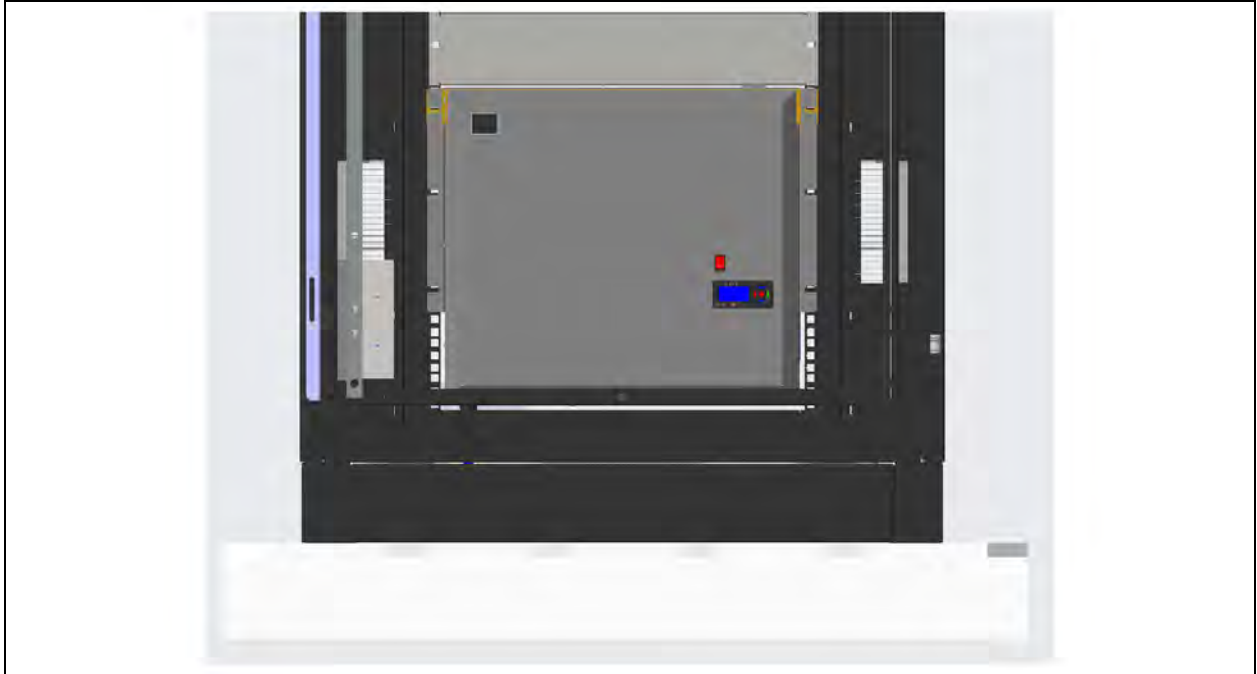
4.7.1 RCU Piping Assembly

To connect the piping of RCU cooling unit first remove rear plate of SO Plinth using allen key and then make piping assembly, use available circular cut outs given on the bottom cover for piping as shown in **Figure 4.17** on the next page.

Figure 4.17 Rear Side View
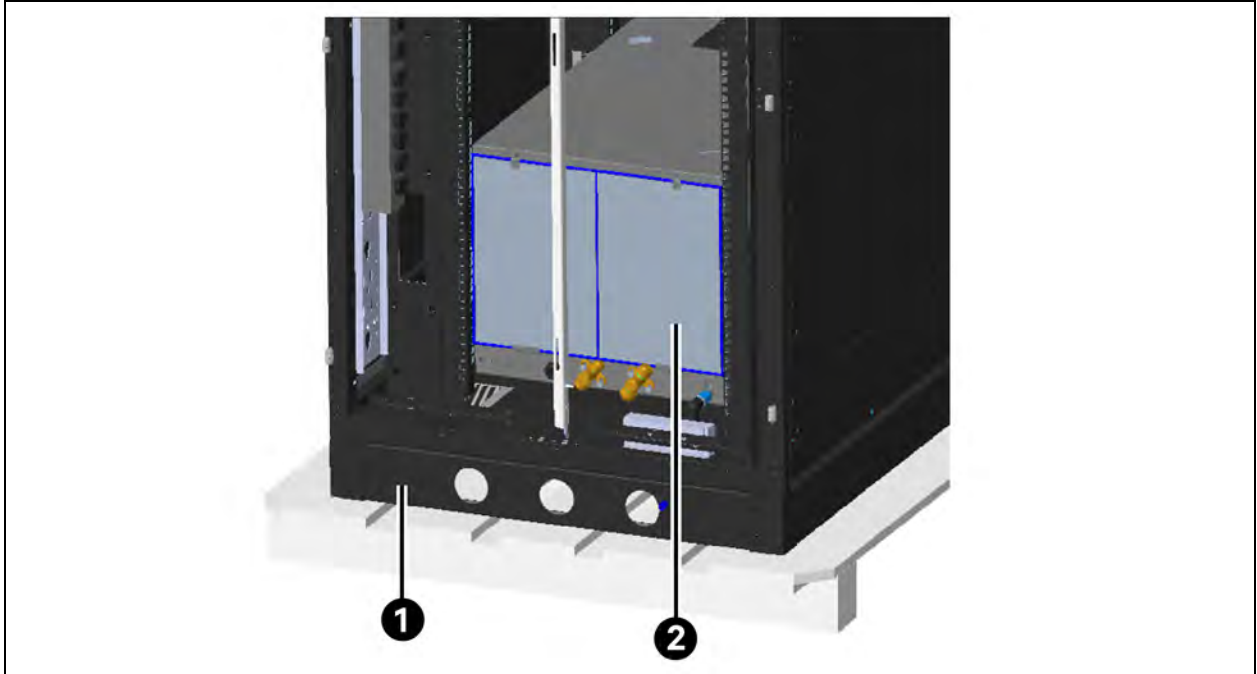
Item	Description
1	Rear plates
2	RCU cooling unit

Figure 4.18 RCU Pipping Assembly (1)
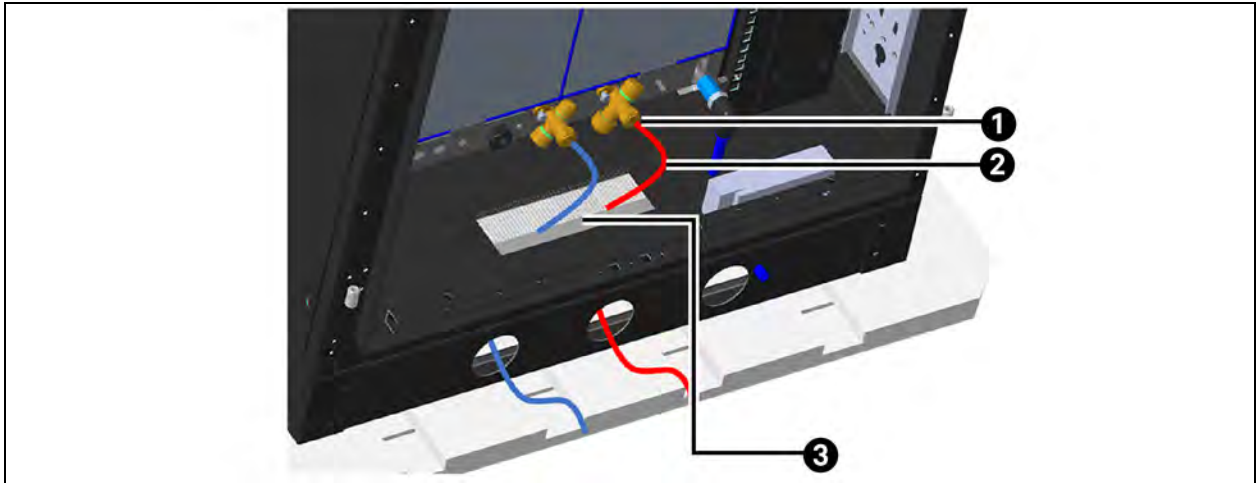
Item	Description
1	Nozzle
2	Piping
3	Square cut-out for piping

 4 Mechanical Installation

Figure 4.19 RCU Pipping Assembly (2)
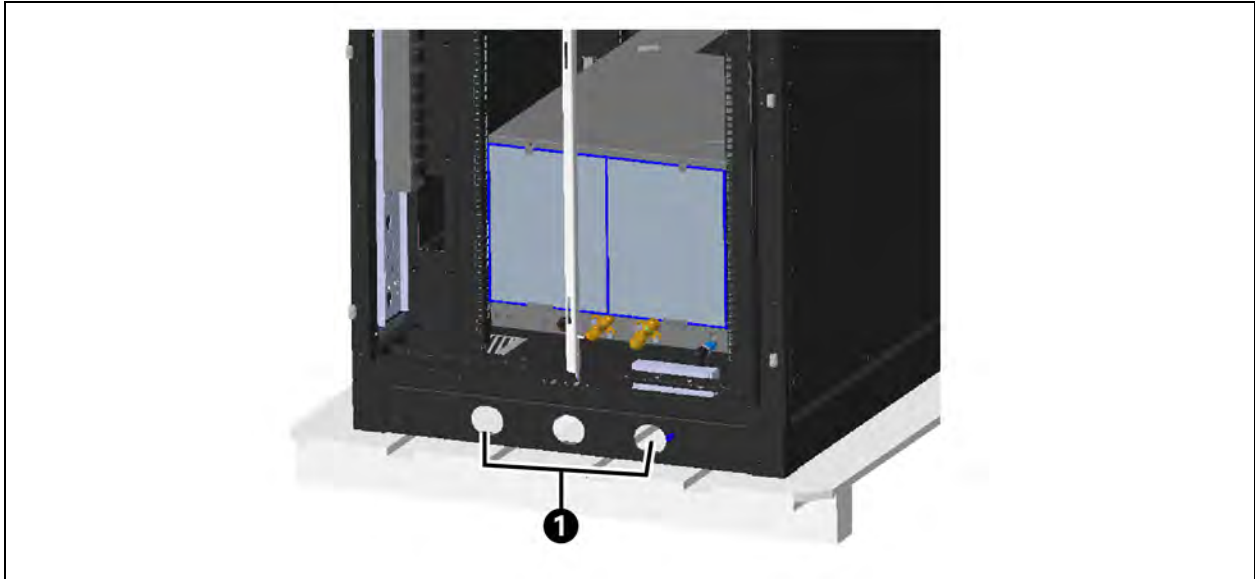
Item	Description
1	Circles cut-out for piping

NOTE: For detail piping connections refer to RCU manual.

4.7.2 Blanking Panel

As the portion between battery set and RCU unit remains empty, customer will use this space to mount their servers/equipment as per their requirements. For the empty space we use blanking panels to cover the blank portion of rack and to have a no leakage cooling inside the rack.

Hardware Required:

1. M6 x 20 bolt hex (quantity: 32)
2. M6 cage nut (quantity: 32)

Figure 4.20 Blanking Panel
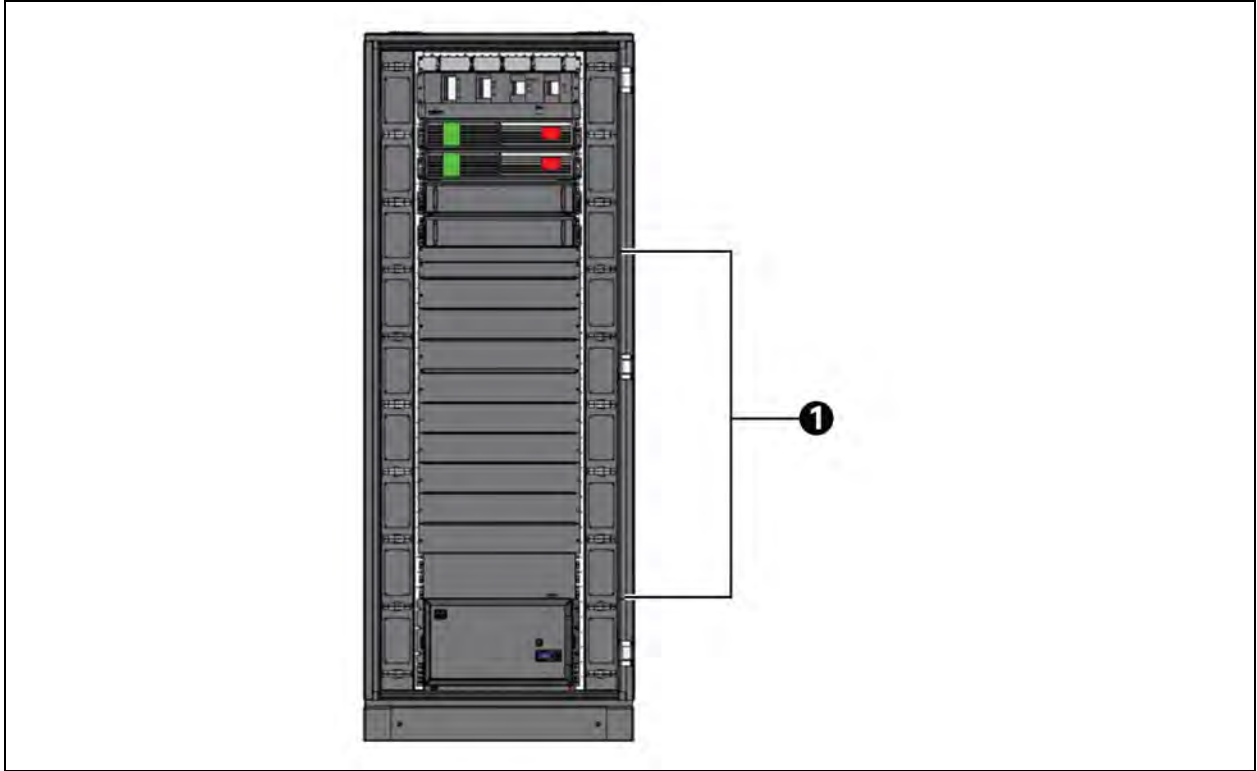
Item	Description
1	Area covered by blanking panels

4.8 Installation of Sensors and Camera

4.8.1 Door Sensor

Assembly of Door Status Sensor (Door Mounted)

To mount door status sensor, we must use sheet metal bracket, door status sensor having two parts, one is mounted on door and one on rack. Before fixing door status sensor (Door Mounted) on front glass door remove existing plastic bracket mounted on aluminum bar and then mount it at 5 to 6 hole below on same bar as shown in **Figure 4.21** on the facing page. Mount door sensor on sheet metal bracket using M3 × 10 bolt and mount this assembly on glass door's aluminum bar on below shown position in **Figure 4.21** on the facing page, use M5 × 10 Self tapping to fix sheet metal bracket.

Hardware Required:

1. M5 × 10 self-taping screw (quantity: 02)
2. M3 × 10 bolt (quantity: 02)

Figure 4.21 Installation of Door Sensor (Door mounted-1)
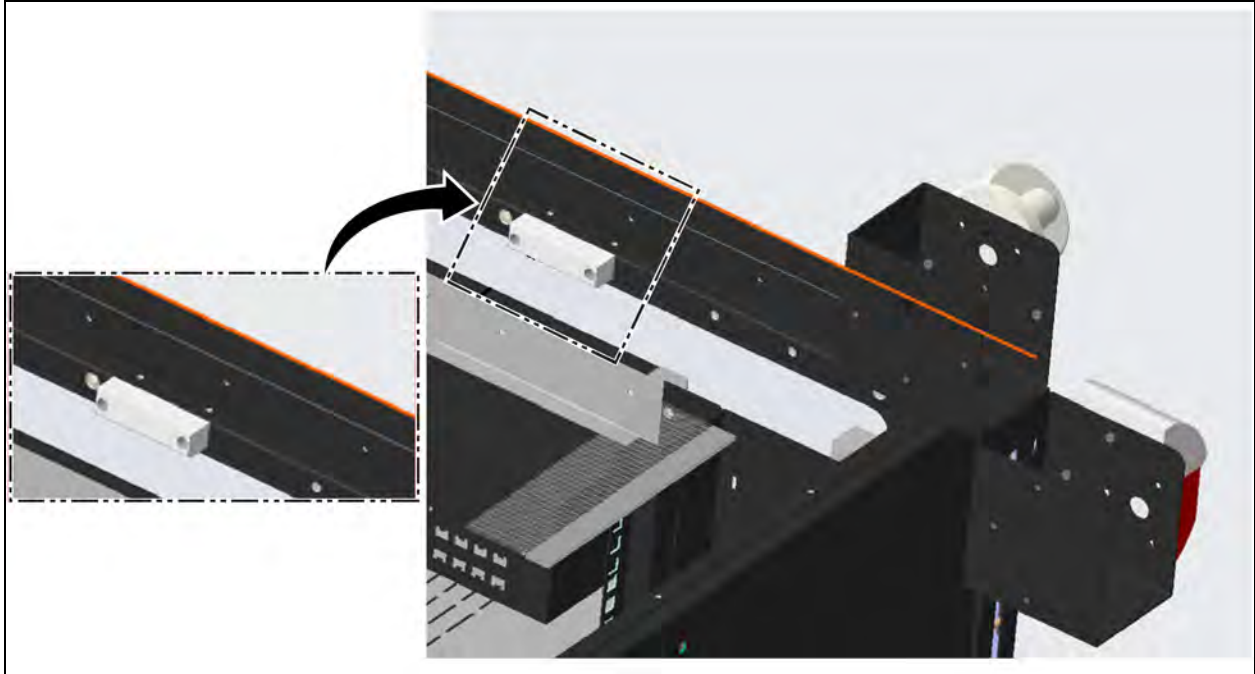
Figure 4.22 Installation of Door Sensor (Door mounted-2)
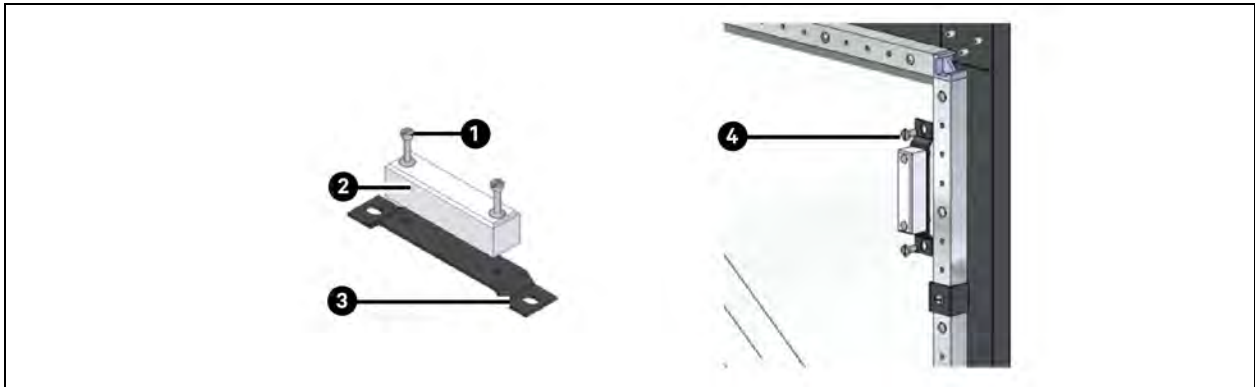
Item	Description
1	M3 × 10 Bolt
2	Door Sensor Door
3	Sheet metal Bracket
4	M5 × 10 self-taping crew

Assembly of Door Status Sensor (Body Mounted)

To mount door status sensor (body) on rack. Mount door status sensor (body) on sheet metal bracket using M3 × 10 bolt and M3 Nut mount this assembly on left top corner of rack use existing M8 cage nuts and M8 × 10 Bolt to fix Door sensor assembly as shown in **Figure 4.23** on the next page:

Hardware Required:

1. M3 × 10 bolt (quantity: 02)
2. M8 × 10 bolt hex washer slotted (quantity: 01)

Figure 4.23 Positions of Both Door Sensors in closed door Condition
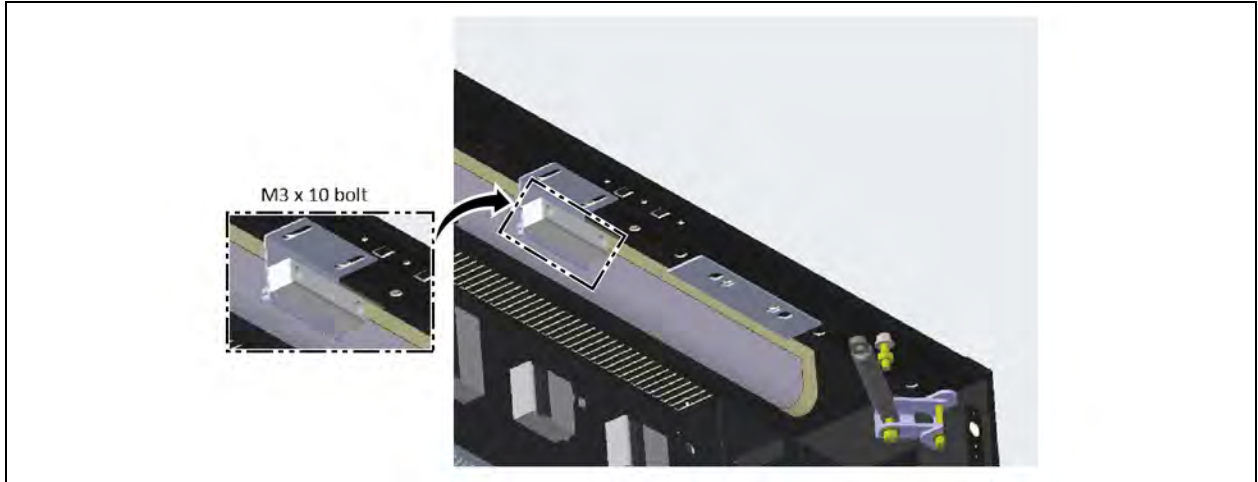
NOTE: After closing the door, ensure that both sensors are in place.

4.8.2 Smoke Detector Sensor

Mount the smoke detector on horizontal channel given at rear top side bolt it by M4 self-taping screw as shown in **Figure 4.24** below.

Hardware Required:

1. M5 x 30 self-taping Screw (quantity: 02)

Figure 4.24 Smoke Detector Sensor
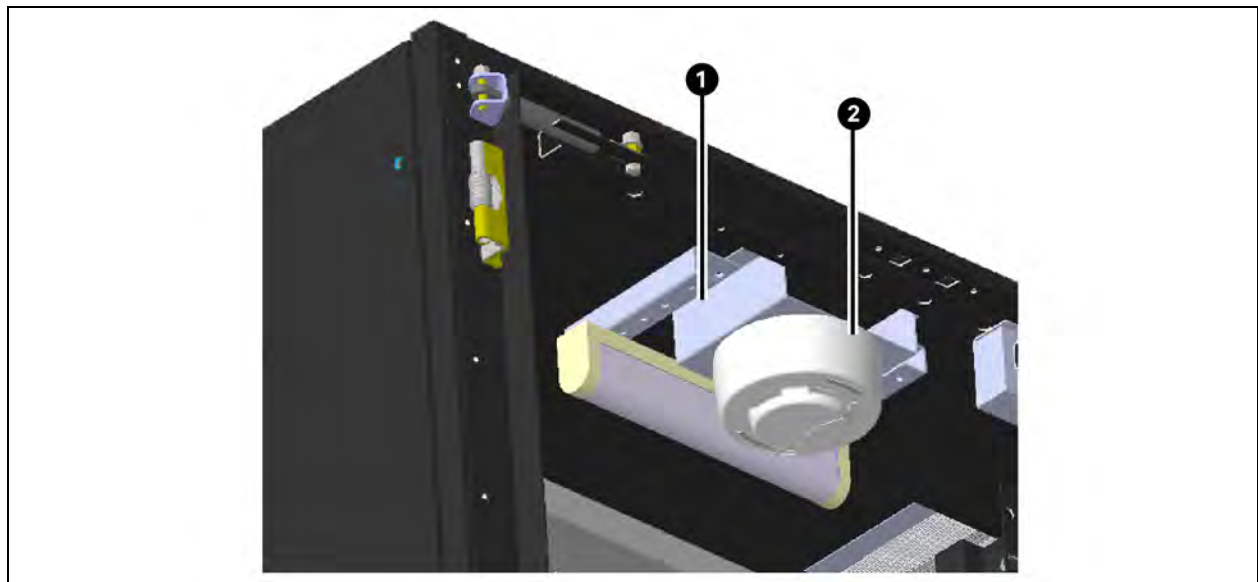
Item	Description
1	Smoke mounting bracket
2	Smoke detector

4.8.3 Temperature and Humidity Sensor

Mount the temperature and humidity sensor on vertical channel and on similar position mount it on rear side.

Mounting: Magnetic contact with additional cable tie as shown in **Figure 4.25** below.

Figure 4.25 Temperature Sensor
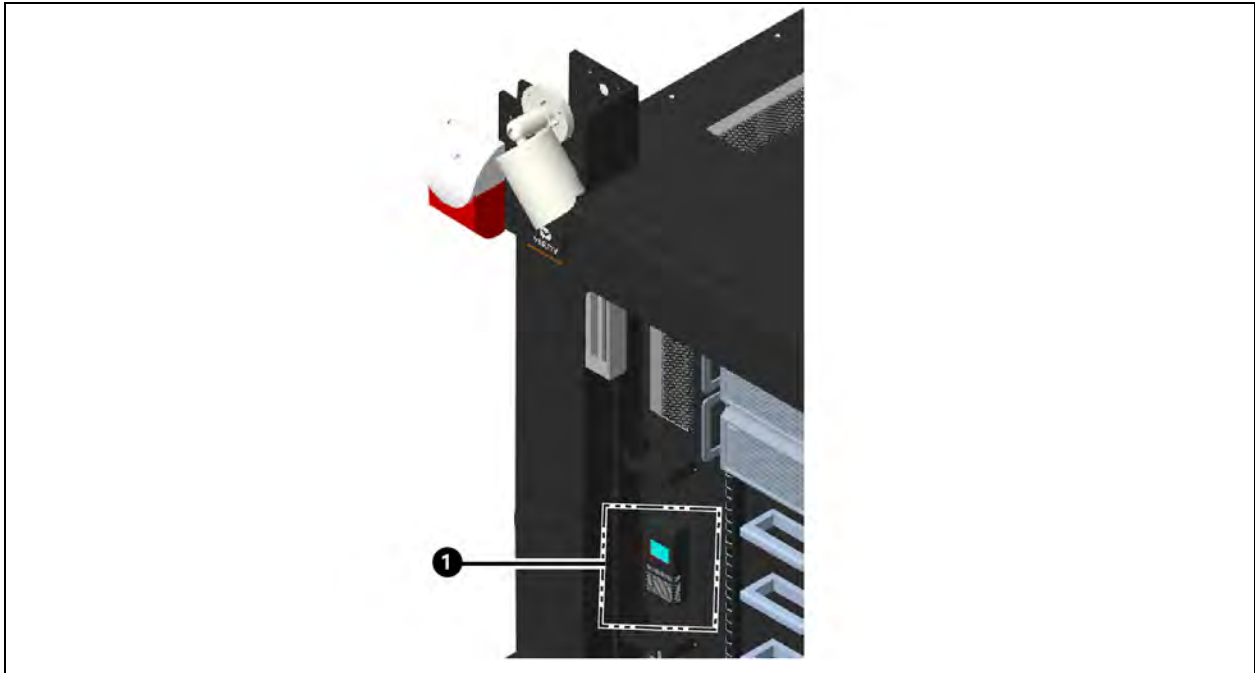
Item	Description
1	Temperature Sensor

DIP Switch Setting

For working temperature sensor, we must do below switch settings

1. For front side sensor (Temperature Sensor-01) switch on 6 no. switch remaining all must be in off condition as shown in **Figure 4.26** below.

Figure 4.26 Temperature Sensor for Front Side (Temperature Sensor-01)

2. For rear side sensor (Temp. Sensor-02) switch on 5 no. switch remaining all must be in off condition as shown in **Figure 4.27** below.

Figure 4.27 Temperature Sensor for Rear Side (Temperature Sensor-02)

NOTE: RDU-A will show Temperature Sensor names as Temperature Sensor 01 and Temperature Sensor 02.

NOTE: For the installation procedures of the intelligent sensors, refer to the corresponding Intelligent Sensor User Manual - IRM-S01T Intelligent Temperature Sensor User Manual for IRM-S01T.

4.8.4 Water Leak Detector Sensor

Water leak detector is a rope type sensor to be routed on bottom and wherever required. Use cable tie to fix the position then connect wires this rope with Water Leak Detector module (IRM-S01W) as shown in **Figure 4.28** on the facing page.

Figure 4.28 Installation of Water Leak Detector (Rope type)

Item	Description
1	Water leak detector rope

Figure 4.29 Connection of Water Leak Detector (Rope type)
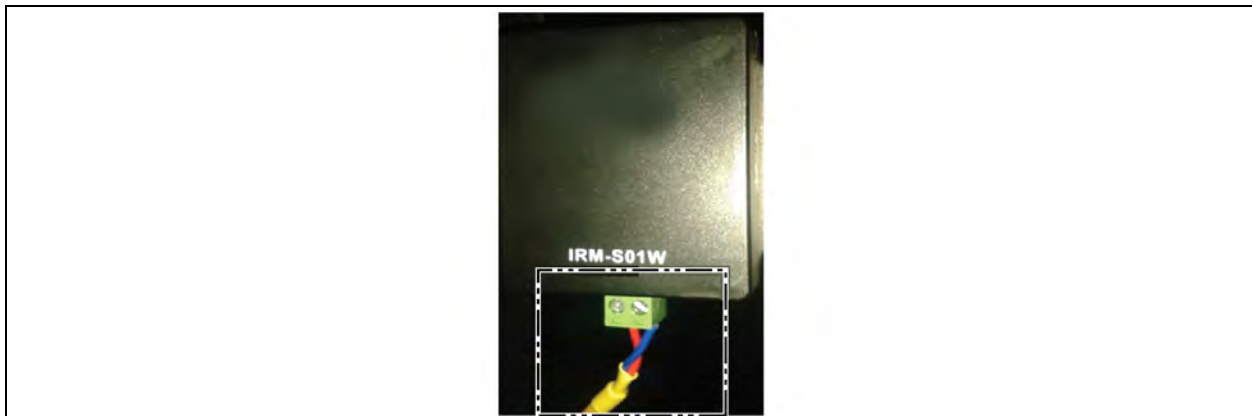
Item	Description
1	Water Leak Detector

4.8.5 Assembly of Beacon and Camera

To mount sheet metal bracket on Left Top of Rack remove existing M12 bolt of rack and use same bolt to fix bracket at below shown position and then mount Beacon on side flange of sheet metal bracket use M3 x 15 bolts, now mount Camera on top flange of bracket as shown in **Figure 4.30** on the next page.

Hardware Required:

1. M12 x 10 Bolt Hex Washer Slotted (quantity: 01)
2. M3 x 10 Bolt (quantity: 03)

Figure 4.30 Installation of Beacon and Camera
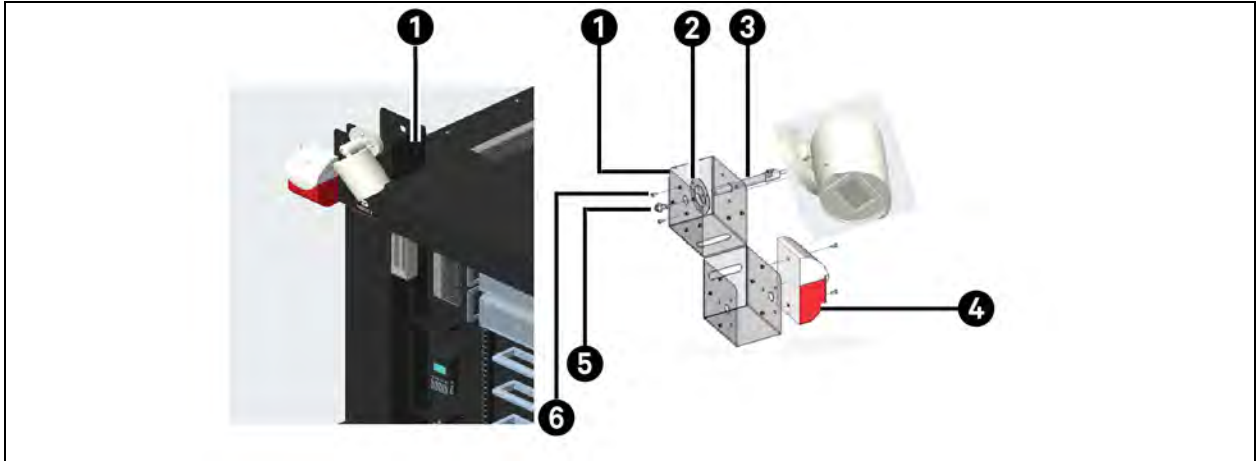
Item	Description
1	Sheet metal bracket
2	M3 x 10 bolt
3	M5 x 10 bolt
4	Sheet metal bracket
5	Circular bracket
6	Guide rod of camera
7	M3 x 15 bolt
8	Camera

4.9 RDU-A Installation Guideline

Follow the steps as below for RDU-A installation and implementation.

When RDU-A boots for first time it will ask for one time password connect RDU-A LAN port to your laptop via a RJ45 LAN cable:

1. Change IP address of your laptop as 192.168.0.100 subnet mask as 255.255.255.0.
2. Power on RDU-A.
3. Open internet browser from your laptop and type the URL- http://192.168.0.254 a webpage will load.

Cabling of Door Status Sensor

Connect one end of CAT 5 cable to Door Status Sensor then connect other end of Cat 5 cable to Port no.10 (Door status port) Of RDU-A.

Figure 4.31 CAT 6 Cable having RJ 45 Connector on Both Ends
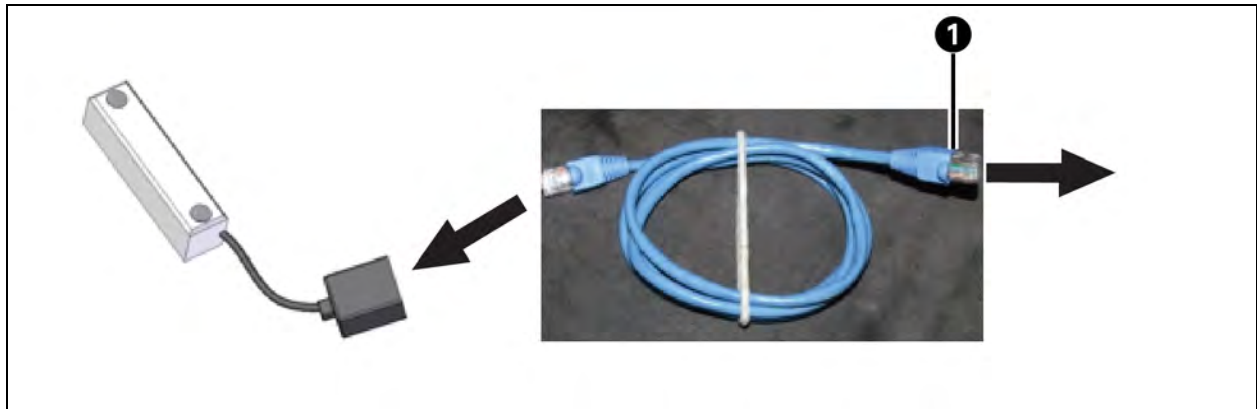
Item	Description
1	Port No. 10

Cabling of Beacon

Connect one end of CAT 6 Cable to Beacon then connect other end of Cat 6 cable to Port No. 8 (Relay output port 1) of RDU-A.

Figure 4.32 Beacon
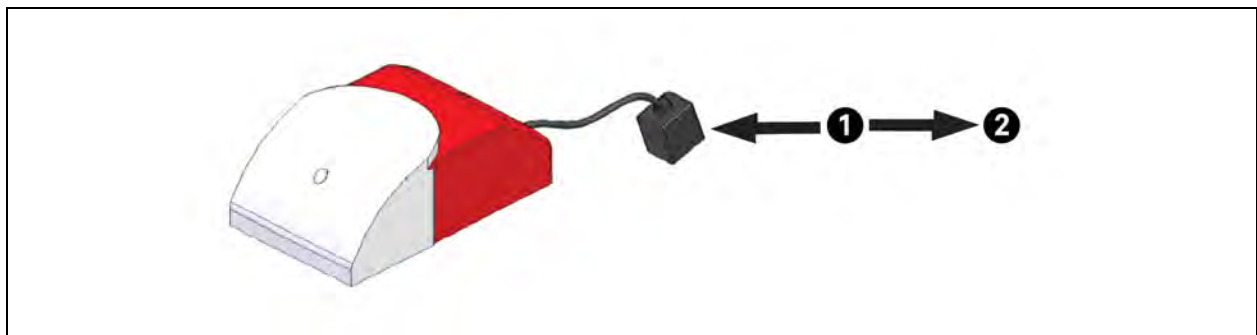
Item	Description
1	CAT 5 Cable having RJ 45 Connector on both ends
2	Port No. 8 (Relay output port 1) of RDU-A

Cabling of Camera

Figure 4.33 Cabling of Camera
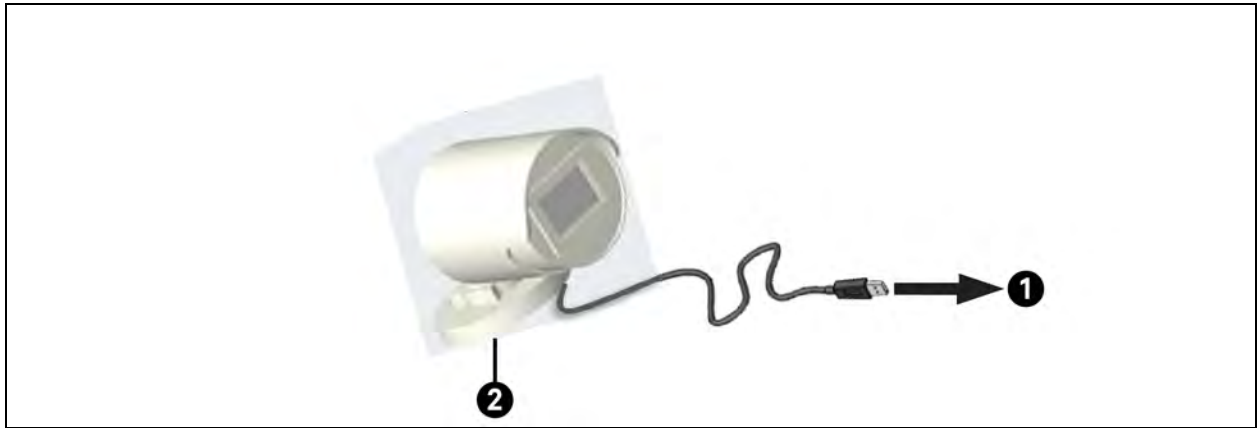
Item	Description
1	Camera
2	Port no. 6 (USB Port) of RDU-A

Cabling of Smoke Detector

Connect one end of CAT 6 Cable to Smoke Detector then connect other end of Cat 6 cable to Port no. 12 (Smoke port) of RDU- A.

Figure 4.34 Smoke Detector
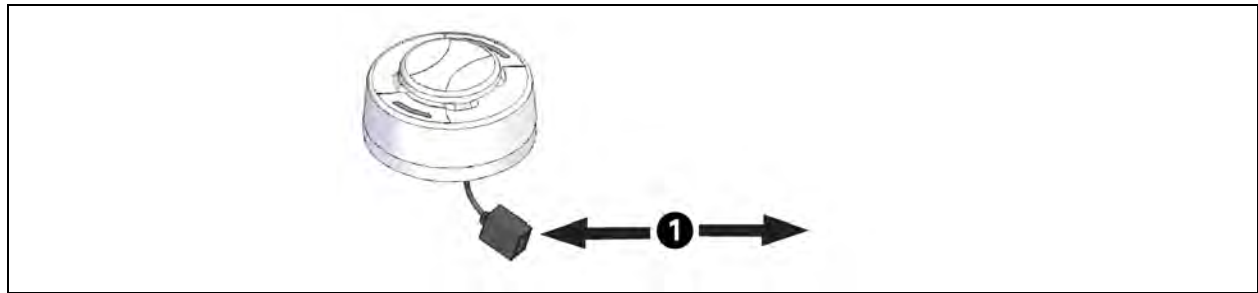
Cabling of Water Leak Detector

First connect water leak sensor rope to detector and then connect one end of CAT 5 cable to water leak detector and second end to RDU-A Port No.17 (Water Port).

 4 Mechanical Installation

Figure 4.35 Cabling of Water Leak Detector
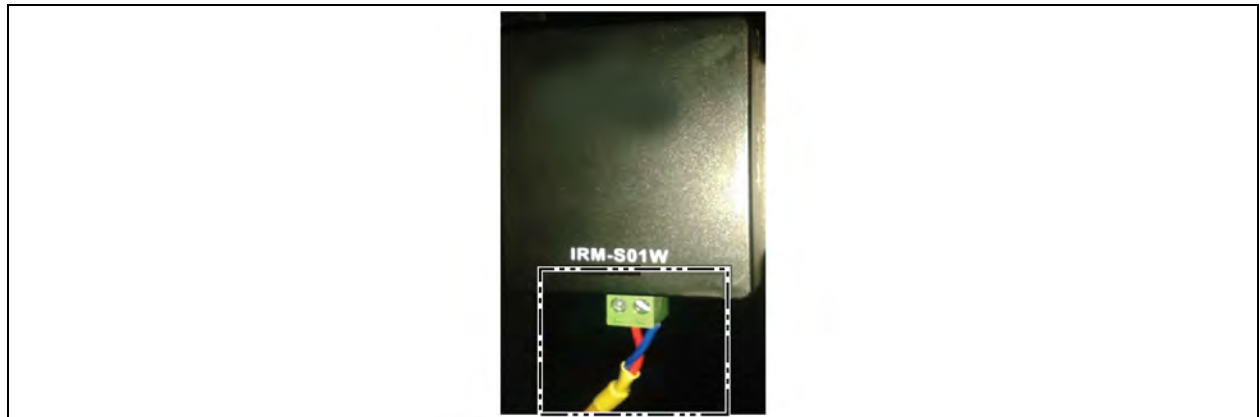
Cabling of Temperature and Humidity Sensor

Connect all two temperature sensors by CAT 5 Cable and then connect to RDU-A Port No.16 (Com1) as shown in **4.9** on page 48.

Figure 4.36 Cabling of Temperature and Humidity Sensor
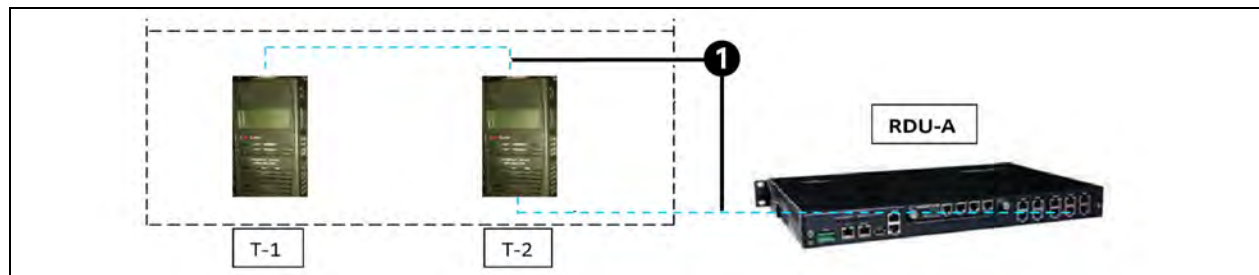
Item	Description
1	Cable having RJ 45 connector on both ends

Assigning Modbus ID to RCU unit and connecting multiple RCU to RDU-A for monitoring

Sites with more than one RCU unit and we want to monitor them in RDU.

Pre-requisite:

1. They should be wired properly for communication with RDU.
2. Modbus slave address needs to be assigned to them.

Following information is for how to give Modbus slave address to RCU:

This must be done only in machine number 2 of RCU as by default RCU will have ID =1.

RCU has a local LED display where you can configure this (also it has 5 keys similar to mobile phone key pad).

1. Press **down** button for 5 seconds success it will display 0.
2. Type 66 with help of up key success it will display 66.
3. Press **right** button **set** button success it will show some parameters running (anything running at that time).
4. Press **up** button go to id 2 (this is where the slave address is set).

5. Press **set** button, by default it will be 1 by factory settings.

6. Press **up** button and make it 2 (example: if more than 2 are there then ID could be 1,2,3 and 4 for 4 units).

7. Press **set**.

8. Press **up** button and go to EP screen will show EP (EP stands for end programming).

9. Press **set**.

NOTE: Modbus ID is given to each unit and the information is convey to RDU configuration engineer.

Wiring Steps:

1. Prepare a cable.

2. Connect the cable to RCU and RDU.

3. Load drivers (extract and install. password is **123**).

4. Configure RDU for monitoring.

Figure 4.37 RS 485 Connector
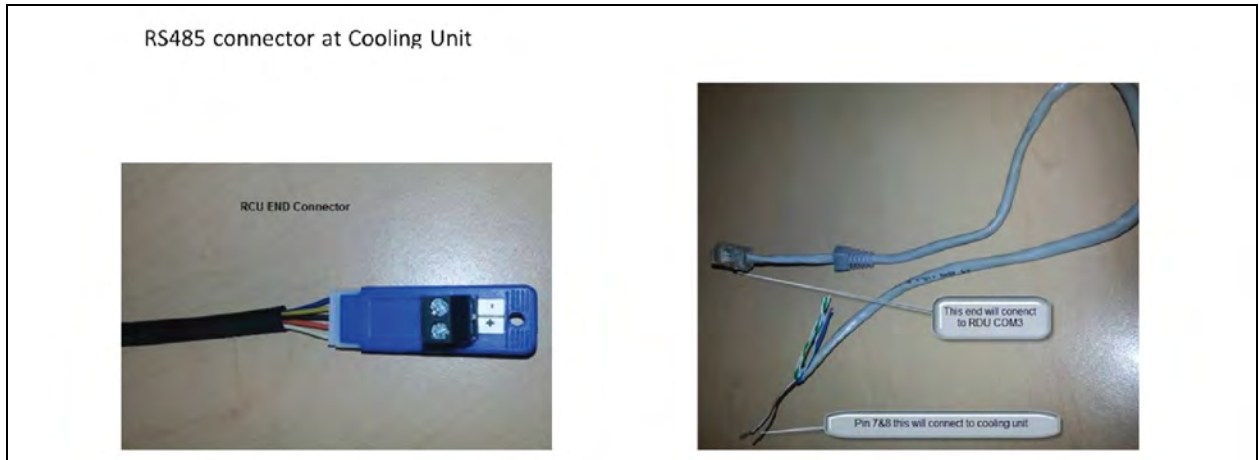
Figure 4.38 RCU1, RCU2, and RDU-A Connection

Proprietary and Confidential ©2024 Vertiv Group Corp. 4 Mechanical Installation
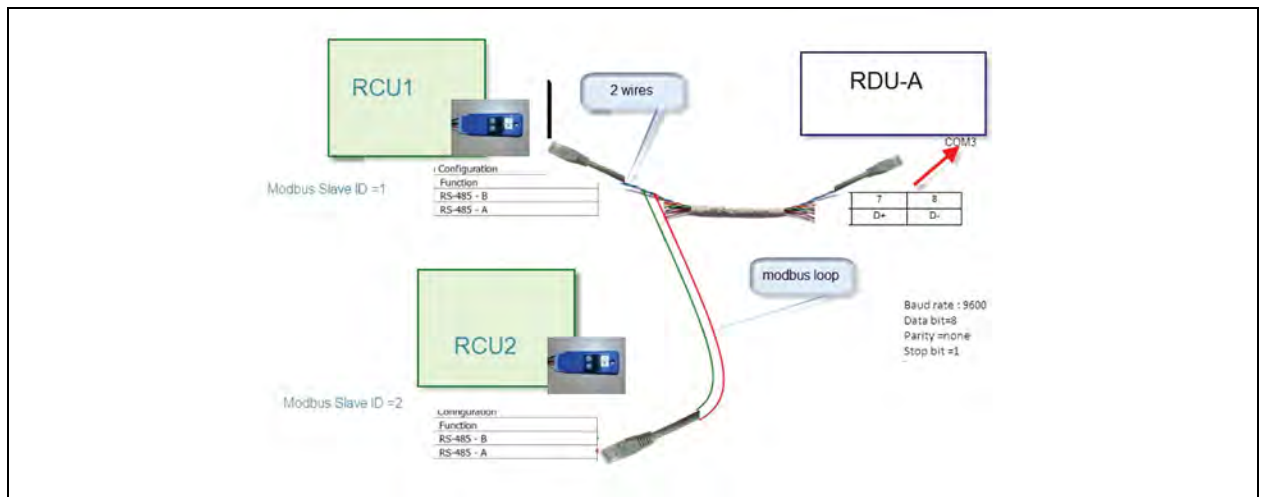
4.10 Access Control

Access control is a fingerprint and card access control system.

Figure 4.39 Access Controller

Figure 4.40 Placement of Access Controller
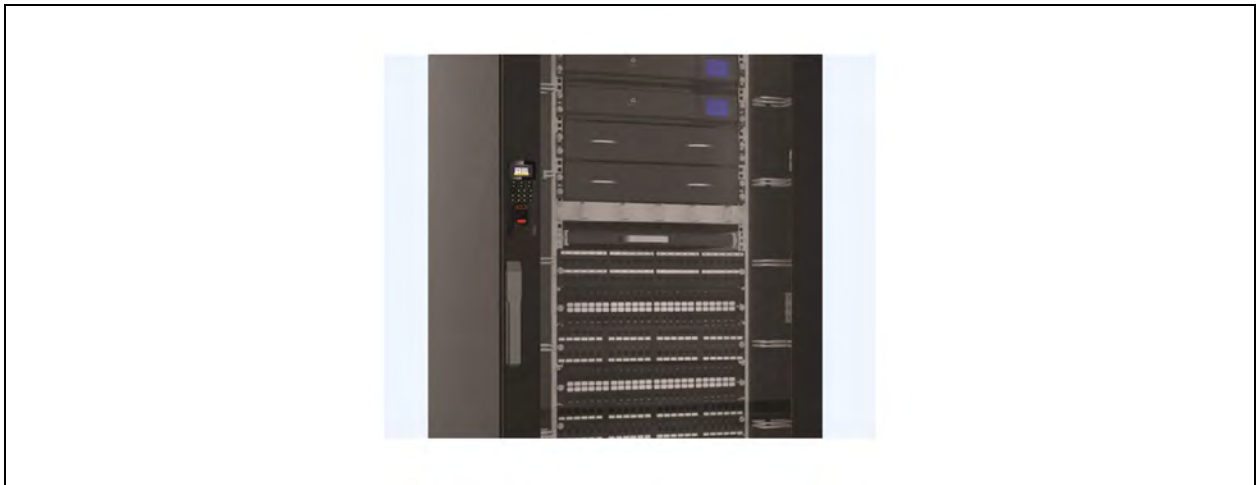
Now Vertiv™ SmartCabinet™ is ready, and client can place the server or network equipment inside the rack. After completing the assembly of all parts, fully assembled system looks as shown in **Figure 4.41** on the next page.

Figure 4.41 Vertiv™ SmartCabinet™

             4 Mechanical Installation

5 Commissioning

This chapter introduces the operation instructions of Vertiv™ SmartCabinet™, including a check before startup, and procedures of power on and system commissioning.

5.1 Commissioning Procedures

The commissioning procedures of SmartCabinet™ are as shown in **Figure 5.1** below.

Figure 5.1 Commissioning Flow Chart
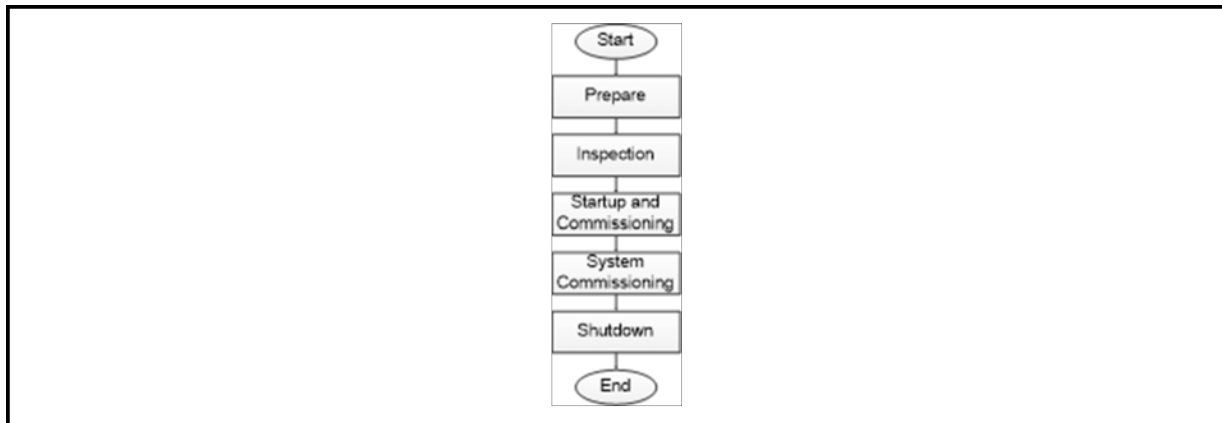
5.2 Preparation

The product commissioning is used to support the product deployment. Before commissioning, the hardware installation and inspection work, as well as cabling and inspections, should be completed.

5.3 Inspection

Prior to starting up the SmartCabinet™, perform the inspections as per the checklist below:

Table 5.1 Checklist

Inspection Items	Inspection Criteria	Remark
Thermal management system	Check if the air conditioner is charged with refrigerants	
	Check if the air conditioner pipes are normally connected without leakage	
	Check if the emergent fan power supply port is correct	
Power distribution	Check, measure and confirm if the AC mains voltage and frequency are normal and confirm if the AC mains connection is correct without a short circuit	
	Check and confirm if the distribution cables of UPS and PMU are correct without a short circuit	
	Check if the battery (if configured) installation and wiring are correct and check if the battery positive and negative polarities are correct	
Monitoring unit	Check if the all the communication network cables are connected in correct sequence according to the wiring diagram and cable number	

Table 5.1 Checklist (continued)

Inspection Items	Inspection Criteria	Remark
Access control	Check access and check if the distribution and signal cables of the access control are correct according to the wiring diagram and cable number control	
Fire and suppression	Against the wiring diagram, according to the cable label, check the firebox power distribution, signal cable connection is normal	Optional
System	Check if the vacant space has been sealed by dummy plates	
	Check the isolated sheet metal parts in the sealed frame of the air conditioner to ensure the refrigerant pipe and the power supply communication cables are led out from the top of the isolated sheet metal part	

5.4 Startup

5.4.1 RCU Commissioning

At the time of RCU commissioning check all the points as per the commissioning checklist as shown in **Table 5.2** below.

Table 5.2 Commissioning Checklist

Check	Inspection Criteria	Remark
Physical check	Installation of machines	
	Sealing of gaps around the units	
	Controller fitment	
	Grilles fitment	
	Cleanliness of air filter	
	Cleanliness of evaporator coil	
	Cleanliness of condenser coil	
	Insulation fitment	
	Fan rotation	Optional
	Condenser fan rotation	
	Compressor rotation	
	Blower fan free rotation	
	Unit vibration if any	
	Refrigerant pipes rubbing	
	Oil trace/refrigerant leak if any	
	Drain pipe clear for water movement	
	Unit changeover	

Table 5.2 Commissioning Checklist (continued)

Check	Inspection Criteria	Remark
Electrical	Incoming voltage (volts)	
	Loose connection	
	Earthing of units	
	Earthing of controller	
	Total unit current (amp)	
	Blower fan current (amp)	
	Condenser fan current (amp)	
	Compressor current (amp)	
Mechanical readings	Compressor suction pressure	
	Compressor discharge pressure	
	Room temperature	
	Controller settings	
	Mode of operation	
	Unit selection	
	Cycling hours	
	Temperature set points	

5.4.2 UPS Commissioning

Single UPS commissioning

ITA 2 10 kVA/ 20 kVA start up Checks

1. Check and confirm if the power distribution mode of the UPS and the POD (if configured) is correct, for the connection of the power cables and signal cables is correct and there is no short circuit.
2. Check that the battery installation for correct polarity and the cable connection are correct.
3. Measure and confirm that the mains voltage and frequency are normal.
4. The output terminals of the UPS and the POD (if configured) are energized upon the start-up. If the load is connected with the output terminals, make sure that the power to the load is safe.

Start-up interface

If the system is first start-up, only mains input mode can be used, and the LCD screen will display the start-up interface as shown in **Figure 5.2** on the next page.

When the UPS is started for the first time use the mains input mode only and the LCD screen will display the start-up interface. See **Figure 5.2** on the next page.

Figure 5.2 Start-up Interface
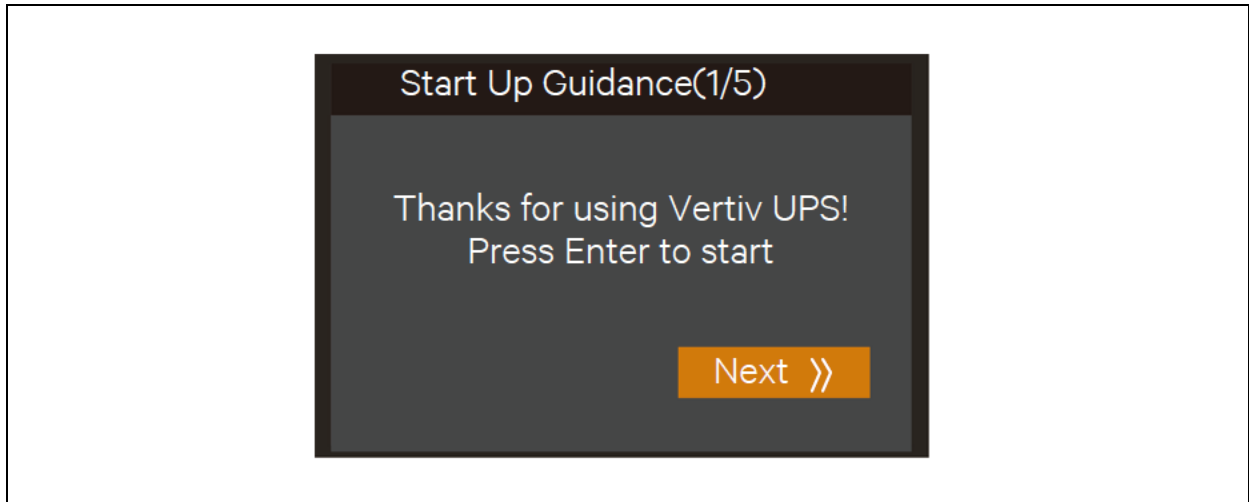
Normal Mode Start-up

1. Close the external output MCB and input MCB of the UPS one by one.

NOTE: If the single POD is selected to connect with the UPS, close the input MCB, bypass MCB and output MCB of the POD.

⚠️ **WARNING! After closing the external output MCB or the POD output MCB of the UPS, the output terminal block of the UPS, output terminal block of the POD and power distribution end of the load will be live, pay attention to personal safety to avoid electric shock. Check whether it is safe to feed power to the load.**

2. The rectifier runs in normal state for about 30 seconds, the start-up of the rectifier is finished.
3. Finish and check the parameter settings of the single UPS.

    a. At main menu screen, press the ⋀ or ⋁ icon to select 'Settings', and press the key to enter the interface shown in **Figure 5.3** below.

Figure 5.3 Main Menu Screen
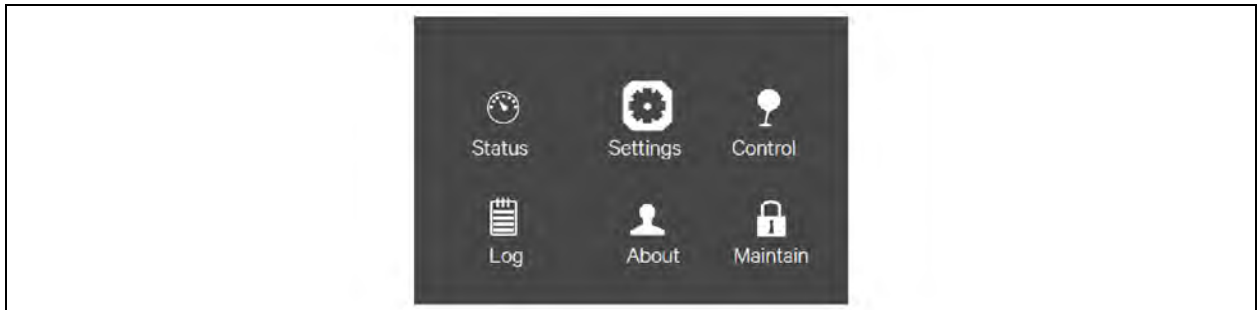
    b. Press the ⋀ or ⋁ icon to select and set corresponding parameters . See **Figure 5.4** on the facing page below for example of Output settings.

Figure 5.4 Output Interface

4. After setting corresponding parameters, press the **power** button for two seconds, and the pop up to confirm will appear. **Figure 5.5** below.

Figure 5.5 Turning On UPS

5. After selecting 'YES', the run indicator changes to green, the inverter starts, and the run indicator turns ON.

6. Measure whether the inverter output voltage is normal.

NOTE: If the battery is not connected to the UPS, the alarm indicator is yellow. If the battery is connected, the alarm indicator turns off.

Battery mode start-up

1. Close the battery MCB and press the **power** button on the UPS front panel for two seconds, the LCD displays the startup screen. The alarm indicator will turn yellow and the alarm will continuously beep after the rectifier completes the startup.

2. Press the **power** button for two seconds, the LCD prompts a dialogue box shown in **Figure 5.6** on the next page.

Figure 5.6 Turning on UPS
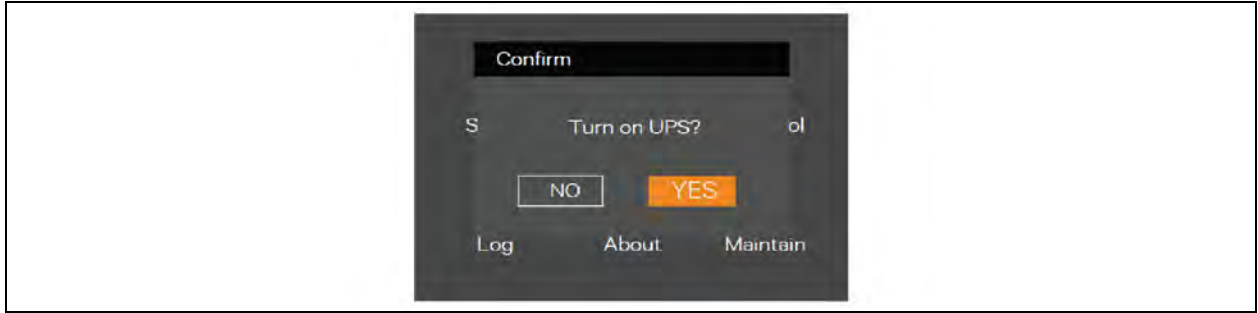
After selecting 'YES', the inverter starts, and the run indicator turns green.

5.4.3 RDU Commissioning

For RDU Commissioning, refer to

5.5 Access Control Commissioning

Default activation password: **Tipl@9910**

Add Administrator

After the device activation and system language selection, you are required to add an administrator. You can set the administrator's user name, the card No. You can also add the user fingerprint, set the password, the department, and the authentication mode.

1. To enter new page, hover the cursor and select the User, click *new*.

2. Select admin ID Number.

NOTE: Default ID No. will be increased in sequence. You can edit the ID according to your preference.

3. Create a new User Name.

NOTE: Upto 32 characters are allowed in the User Name.

4. Select mode of authorization. Card, FP (fingerprint) or PWD (password).

5. Press **ESC** button and select *Yes* to save the settings and exit the page.

6. Log in the device as an administrator to manage the device parameters, including the user, the department, the shift, the holiday, the shift schedule, the report, the communication, the system, the time, etc.

7. Press and hold **OK** button for 3 seconds to open the login page.

8. Select FP, Device PWD, or Card, and authenticate to open the home page.

Adding User

You can add users by setting the ID No., the User Name, and the card No. You can also record the user fingerprint, set the password, the department, the role and the authentication mode.

1. Move the cursor and select User → New to enter the new page.

2. Select *admin* ID Number.

NOTE: Default ID No. will be increased in sequence. You can edit the ID according to your preference.

3. Create a new User Name.

NOTE: Upto 32 characters are allowed in the User Name.

4. Select mode of authorization that is Access Card, FP (fingerprint) or PWD (password).

5. Authentication by Default is Controller, leave it at default setting.

6. Select the user role as administrator or normal. user.

NOTE: Admin: The admin has all permissions to operate the device.
User: The normal user can check attendance on the initial page.

7. Press **ESC** button and select *Yes* to save the settings and exit the settings.

User Management

NOTE: You can add, edit and delete the usersuser access credentials (password, fingerprints, access cards).

1. Select User to access the user list.

2. Enter the user name or employee ID in the search box and press **OK** to start search.

Deleting User

To delete a user, password, fingerprint credentials, access card credentials:

1. **User:** Delete the selected user.

2. **Password:** Delete the selected user's password.

3. **Fingerprint credentials:** Clear the fingerprint credentials of the selected user.

4. **Card credentials:** Delete the cards credentials of the selected user.

5.6 Fire and Suppression

Refer to **Fire and Suppression Manual** for more information.

6 RDU-A G2

This chapter explains how to access RDU-A G2 through Web, and relative functions, including login preparation, log in RDU-A G2, RDU-A G2 homepage and menus.

The web UI is compatible with the latest 32-bit and 64-bit versions of the following web browsers:

- Google Chrome
- Microsoft Edge
- Apple Safari
- Mozilla Firefox

6.1 Login Preparation

To ensure that the RDU-A G2 page function can be normally used, refer to this section for selecting and setting browser options.

1. **Checking IP address connectivity:**

   Before logging in RDU-A G2 through Web, first confirm the IP address of RDU-A G2 and test its connectivity. Refer to Q5: How to deal if there is no access to RDU-A G2 login page when the RDU-A G2 communication is normal? on page 141 in FAQ in RDU maintenance for the test method.

2. **Checking browser version:**

   Support mainstream browsers such as Google Chrome, Firefox, Safari, and Edge.

3. **Checking browser setting:**

   Checking browser general setting

   Double-click the icon of browser to run the software, click *the menus of Tools -> Internet Options*, then click the *Settings* button on the General tab, and select Every time I visit the web page for checking newer versions of stored pages, as shown in **Figure 6.1** below.

Figure 6.1 General Setting
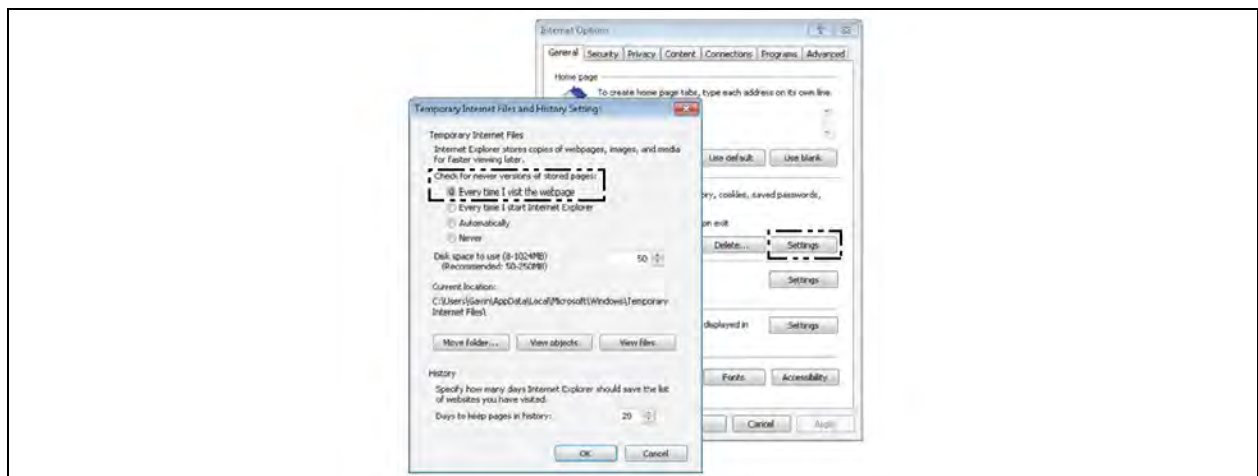
Checking browser proxy setting

a. Double-click the icon of browser to run the software, click the *menus of Tools -> Internet Options* and then choose the Connections tab to pop up the window shown in **Figure 6.2** below.

Figure 6.2 Choosing the Connections Tab
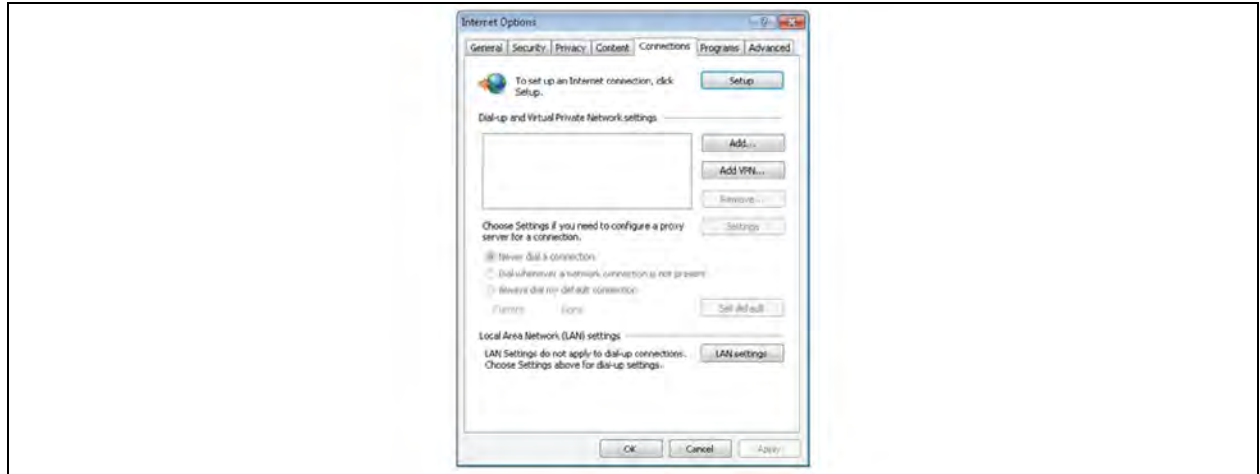
b. In the window shown in **Figure 6.2** above, click the button *LAN Settings* to pop up the window shown in **Figure 6.3** below.

Figure 6.3 LAN Setting
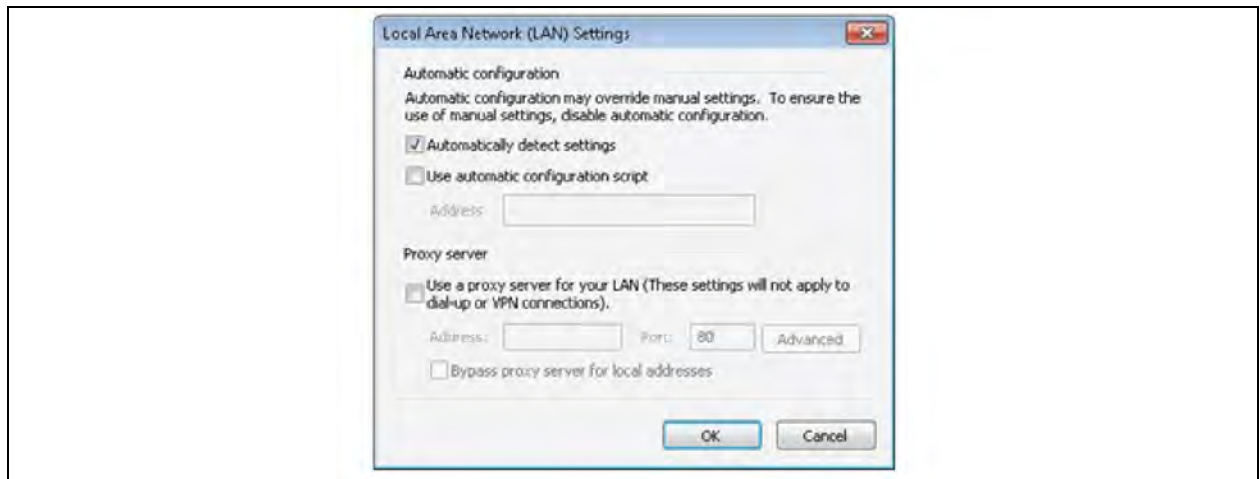
c. Consult the network manager of your area, ask if you need to set a proxy server and get the configuration method.

NOTE: If there is no need to set a proxy server, do not tick any option.

Checking browser security setting

    a.   Double-click the icon of browser to run the software, click the *menus of Tools -> Internet Options* and then choose the Security tab to pop up the window shown in **Figure 6.4** below.

Figure 6.4 Security Setting 1
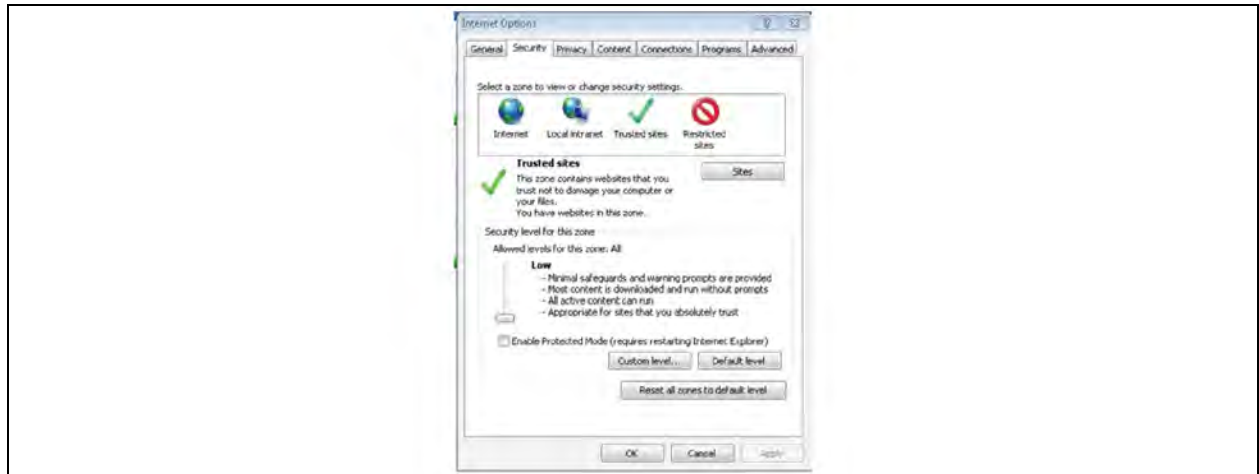
    b.   In the window shown in **Figure 6.4** above, choose trusted sites and click the *Custom level* button to pop up the window shown in **Figure 6.5** below.

Figure 6.5 Security Setting 2
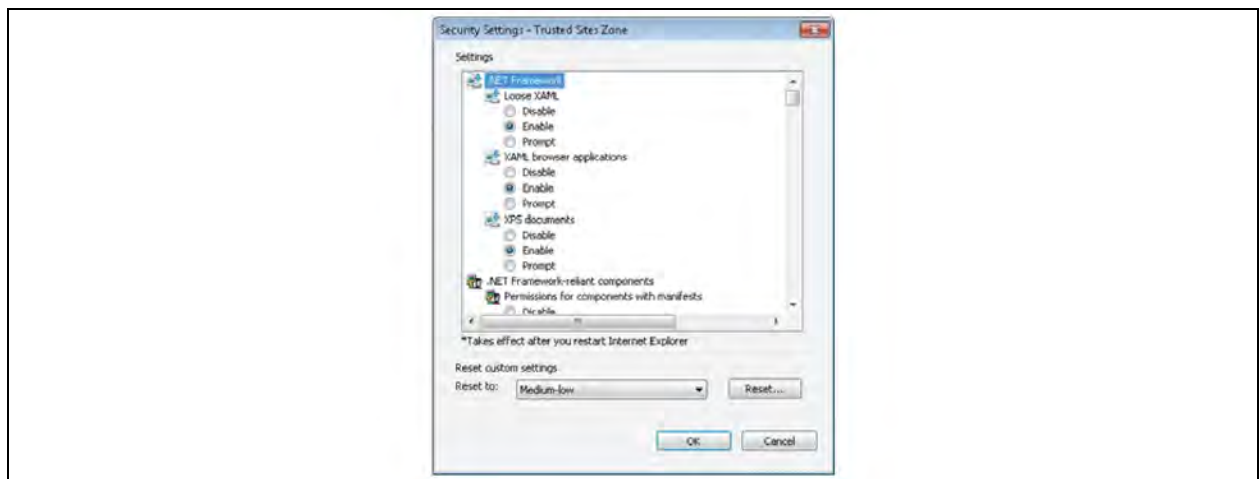
    c.   In the window shown in **Figure 6.5** above, set Medium-low for the security level. Click the *Reset* button to finish Reset custom settings, at last, click *OK*.

    d.   In the window shown in **Figure 6.6** on the next page, set Enable for File download.

Figure 6.6 Enabling File Download
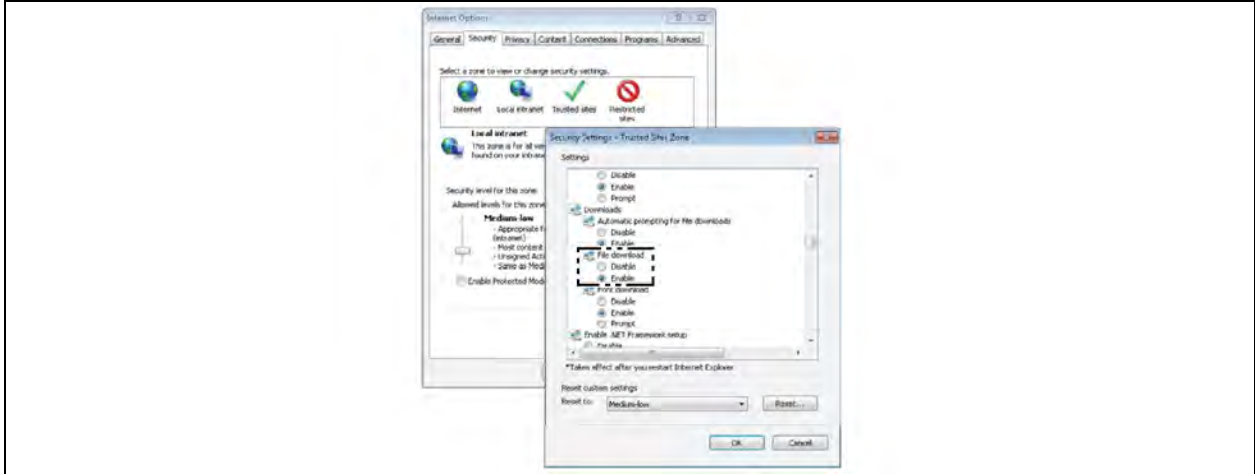
e. In the window shown in **Figure 6.7** below, set Enable for Initialize and script ActiveX controls not marked as safe for scripting.

Figure 6.7 Enabling ActiveX Controls
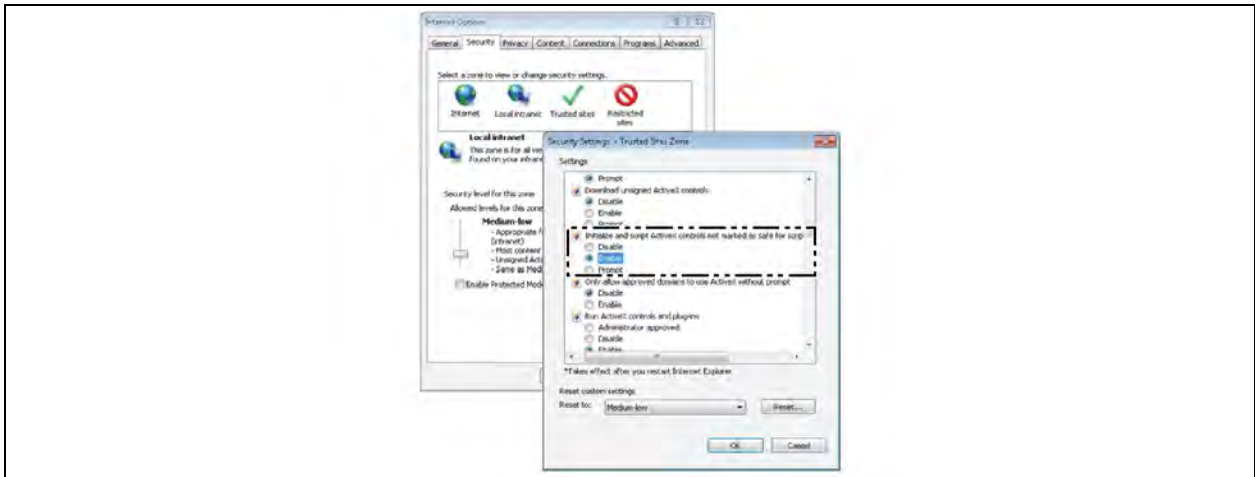
f. In the window shown in **Figure 6.8** on the facing page, add the IP address of the RDU-A G2 into the trusted site list.

Figure 6.8 Adding Trusted Sites

6.2 Login RDU-A G2

Authorizing Boot-strap

1. When logging in RDU-A G2 for the first time, open the browser, and enter the IP address of the RDU-A G2 (the default IP of LAN1 is 192.168.0.254; the default IP of LAN2 is 192.168.1.254) in the address box, the authorizing boot-strap page will appear, as shown in **Figure 6.9** below. If the authorizing boot-strap page does not appear, Refer to Q5: How to deal if there is no access to RDU-A G2 login page when the RDU-A G2 communication is normal? on page 141 in FAQ in RDU Maintenance for the test method.

Figure 6.9 Authorizing Boot-Strap Page
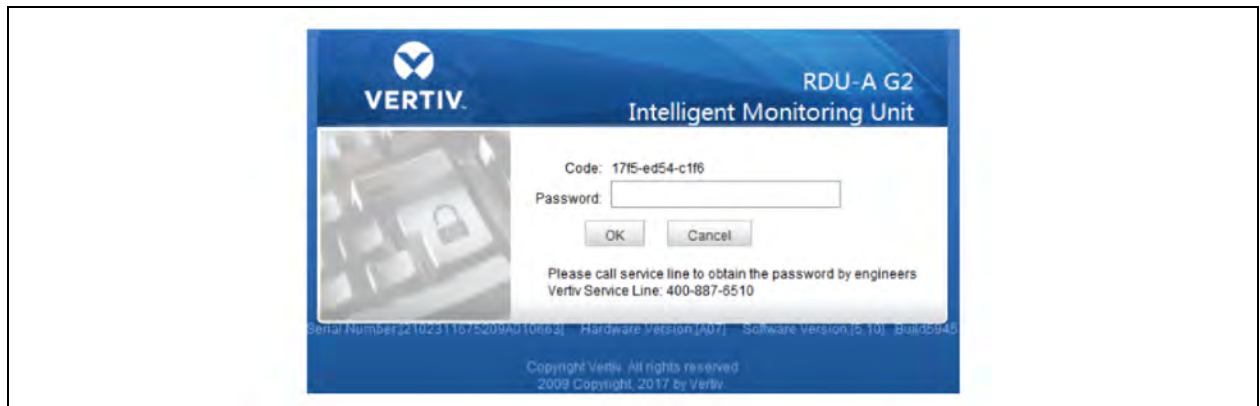
2. Call the Vertiv customer service. Tell the code, serial number, and necessary customer information to the customer service personnel, and you will get the password.

3. Enter the password in the textbox of Password, and then click *OK*. If the password is correct, the system will jump to the login page automatically, see **Figure 6.10** on the next page and **Figure 6.11** on the next page.

Login

1. Open the browser and enter the IP address of the RDU-A G2 in the address box, the login page will appear, as shown in **Figure 6.10** below. If the login page does not appear, Refer to Q5: How to deal if there is no access to RDU-A G2 login page when the RDU-A G2 communication is normal? on page 141 in FAQ in RDU Maintenance for the test method.

Figure 6.10 Login Page of RDU-A G2 (Crystal Blue)
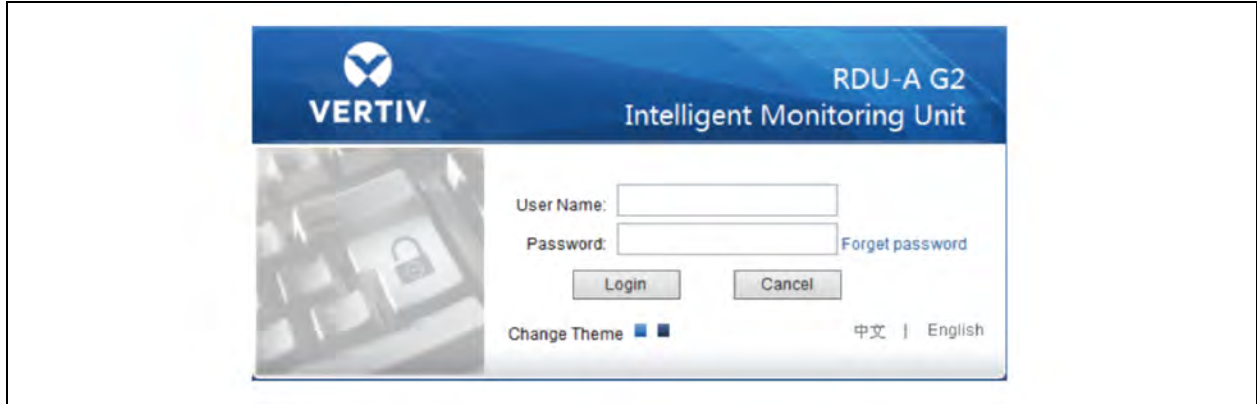
Figure 6.11 Login Page of RDU-A G2 (Ocean Blue)

2. On the login page, select a preferable theme by clicking ▣ or ▪ .

   ▣ means crystal blue, ▪ means ocean blue, as shown in **Figure 6.10** above and **Figure 6.11** above.

3. Enter the User Name and password (default User Name:**admin** and password: **Vertiv**), and click the *Login* button, the homepage will appear. If you cannot visit the homepage after entering correct User Name and password, refer to Checking browser setting: on page 63 and set the browser again.

Getting password

If you forget the password, click the *Forget Password* button on the login page, and the screen will display the page of getting password, as shown in **Figure 6.12** on the facing page.

Figure 6.12 Page of Getting Password

Enter your User Name, and click the *Get Password* button, your password will be sent to the email box or phone which you have configured before. Clicking the *Return Login* button cancels the operation.

NOTE: Only when you have correctly configured the email and SMS parameters on the SMS, and Email Server Configuration page can you receive the password sent by the system.

NOTE: The gotten password is a random new password generated by the system; modify the password after logging in the system successfully.

6.3 Homepage of RDU-A G2

The homepage of RDU-A G2 can be viewed by device or by location. After successful login, the homepage is displayed by location by default, as shown in **Figure 6.13** on the next page.

Viewing by Location

As shown in **Figure 6.13** on the next page, click *By Location* in the upper part of menu items, the display area at right side will display the page viewed by location. You can self-define a plane layout for centralized display according to physical locations of devices in the machine room. After simple configuration, the effect is shown in **Figure 6.13** on the next page.

Figure 6.13 Homepage of RDU-A G2 (by Location)
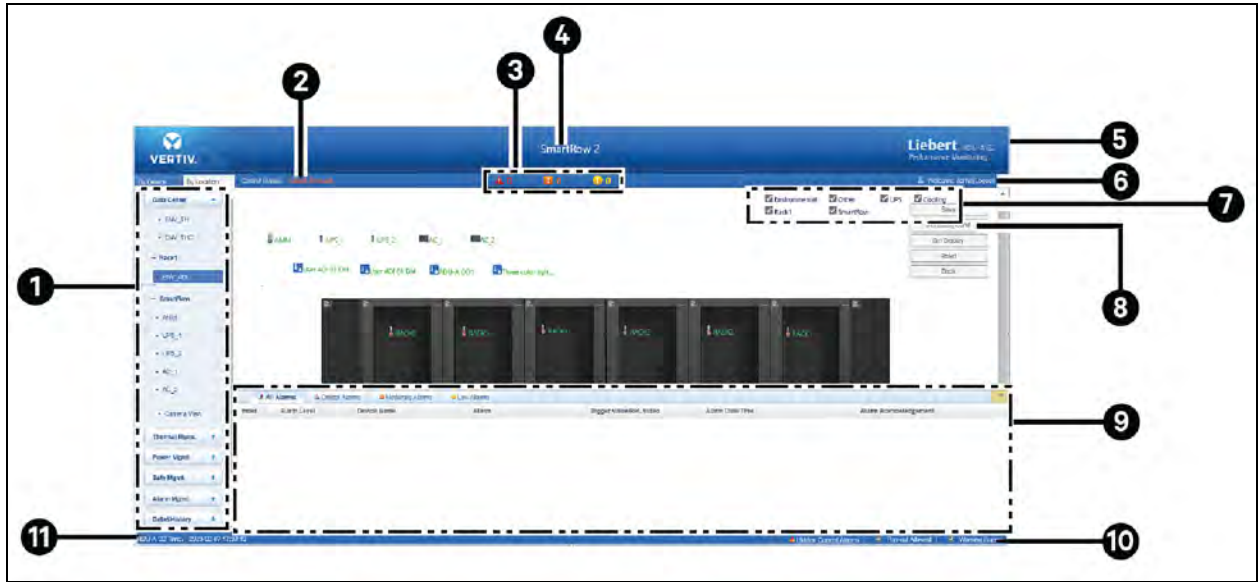
Item	Description	Item	Description
1	Menu item	7	Set background
2	Controllable status	8	Device filter options
3	Current number of every level alarm	9	Real-time alarm displaying list
4	System title	10	Alarm pop-out setting
5	Logo	11	Time calibrating link
6	[User] Logout		

Clicking the ⚙ button shown in directs to the setting status of the homepage, as shown in **Figure 6.14** on the facing page.

Figure 6.14 Setting Page

After the homepage enters setting status, the setting method is as follows:

Background setting

1. Click the *Set Background* button, the window shown in **Figure 6.15** below pops up.

2. Click the *Upload New* button to select the background picture, the Preview area will display the preview effect.

3. Click the *Select Picture* button, the page will display the background picture.

Figure 6.15 Setting Background

NOTE: Only .gif, .ipg, and .bmp format pictures are allowed to be uploaded, and the picture size cannot exceed 500K.

Display setting

1. Click the *Set Display* button, the window shown in **Figure 6.16** on the next page pops up.

2. Select the Signal Display mode: Mouse hover or always.

3. Select whether to display Device icon.

4. After selecting the device name, the device signals will be displayed in the lower box. You can select the device signals to be displayed according to your needs, however, the selected signals cannot exceed 4.

Figure 6.16 Display Setting
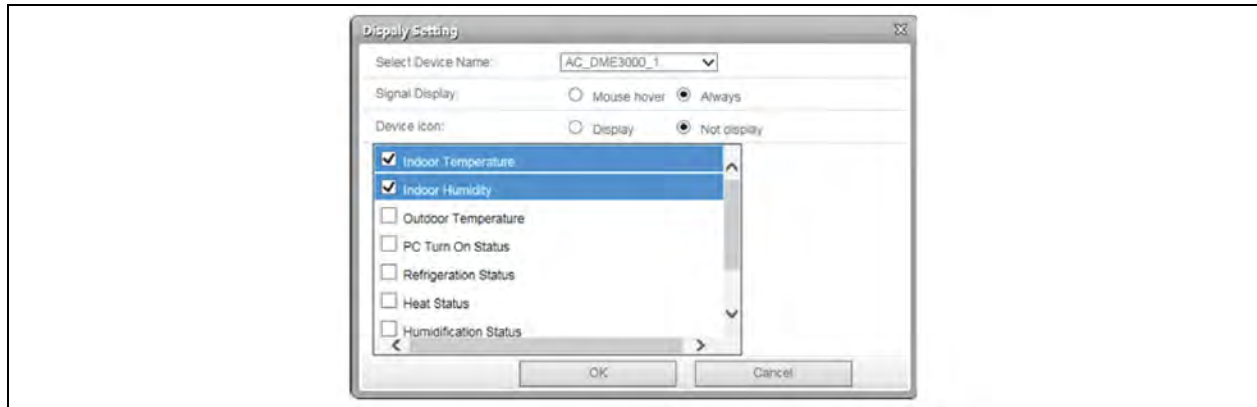
NOTE: Signal Display mode and Device icon options are applicable to the currently selected device. For different devices, their display mode can be set to be different independently.

NOTE: For the display mode of temperature, humidity, and 4DI signals select 'other Devices or Sensors' and perform settings.

Self-define the device location

1. After the homepage enters setting status mode, move the device (signal) icon on the homepage to change its location as needed.

Reset

1. Using the *Reset* button, user can restored the homepage viewed by location to initial status.

Save

1. Using the Back button user can return to view status page from setting status.

Back

1. Click the *Back* button, the homepage will return to view status from setting status.

NOTE: Except for uploading background, only after you click the *Save* button, the configuration can take effect and be displayed.

NOTE: Except for uploading background, if you click the *Back* button directly after configuration, all configuring information will be lost.

Viewing By Device

As shown in **Figure 6.17** on the facing page, click *By Device* in the upper part of menu items, the display area at right side will display the page viewed by device. After simple configuration, the homepage will display corresponding information according to device type, as shown in **Figure 6.17** on the facing page.

For the detailed configuration method, refer to relative descriptions about the Set Display button in Viewing by Location on page 69.

Figure 6.17 Homepage of RDU-A G2 (By Device)

Item	Description
1	Device type and device number
2	Device name
3	Device signal valve

NOTE: For temperature, humidity, and 4DI sensors, the page viewed by device only displays the whole status.

NOTE: For other devices, the page viewed by device displays four signals at most.

Time Calibrating Link

The lower left part displays the system time of RDU-A G2. Clicking the system time of RDU-A G2 will jump to the time calibrating page. For detailed operation, refer to Date/Time Setting on page 133.

Clearing Time-Out

1. When there is no operation on the page within 15 min, the page will become uncontrollable, as shown in **Figure 6.18** on the next page.

Figure 6.18 Controllable Status
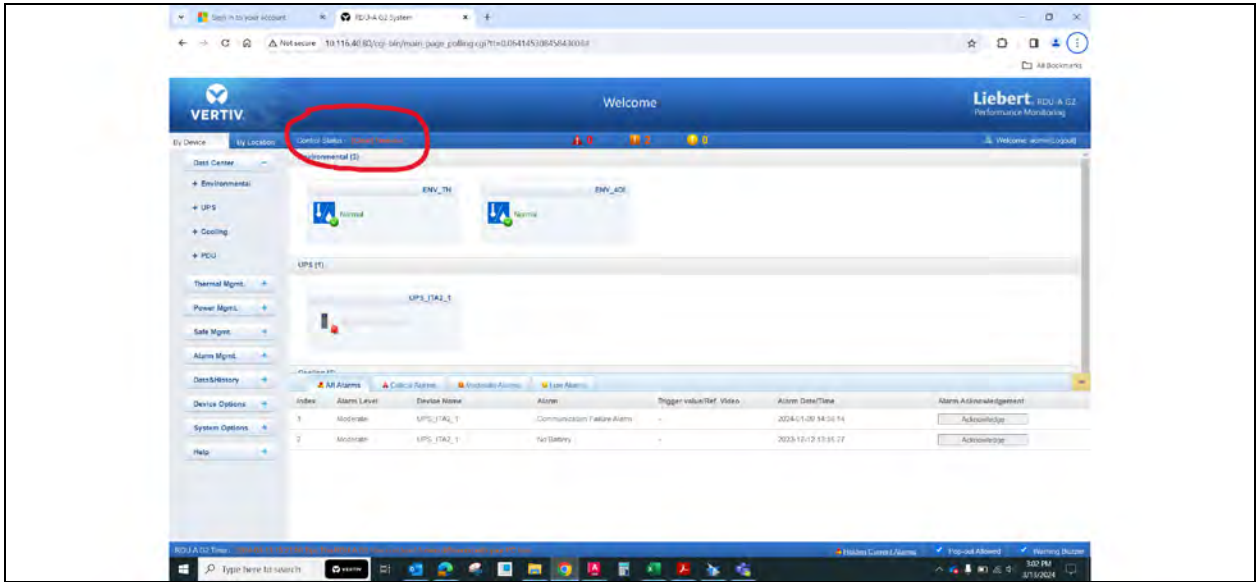
2.   Click *Clear Time-out,* the input box shown in **Figure 6.19** below will appear. After typing the password, click *OK* the controllable status will become normal.

Figure 6.19 Dialog Box of Security Authentication

Logout

1. Click the *Logout* link at the upper right corner of the homepage, the prompt box shown in **Figure 6.20** below will appear, clicking *OK* will log out safely.

Figure 6.20 Logout

Real-Time Alarm Pop-Up Setting

The real-time alarm displaying list is contracted on the bottom of the page by default. You can perform the following operation by referring to **Figure 6.17** on page 73.

1. Click *Display/Hide Current Alarm* manually, and the real-time alarm displaying list will pop up.
2. Tick Auto Pop-out, and the real-time alarm displaying list will pop up when an alarm is generated.
3. Tick Alarm Sounds, and the system will play alarm sound through the browser when an alarm is generated.

After the real-time alarms have been confirmed, the turned-on alarm sound will stop and be on when a new alarm occurs.

6.4 Menu Items

On the homepage of RDU-A G2, the menu items include Data Center, Thermal Management, Power Management, Safe Management, Alarm Management, Data and History, Device Options, System Options, and Help.

6.4.1 Data Center

Click the *Data Center menu* in the left, the submenus will appear. According to the two selections of By Device and By Location, the submenus will be classified and displayed according to device type and device location respectively. Clicking the specific device, the right part will display the relative information of the device, including Overview, Sampling, Control, Setting, and Alarm.

NOTE: ENV-TH in Data Center is a dummy device, which indicates all temperature sensors, and temperature and humidity sensors connected to RDU-A G2, and the name cannot be changed.

Overview

Click the *Overview* tab, and then click the *Edit* button, you can define the overview page, as shown in **Figure 6.21** on the next page.

Figure 6.21 Overview Tab
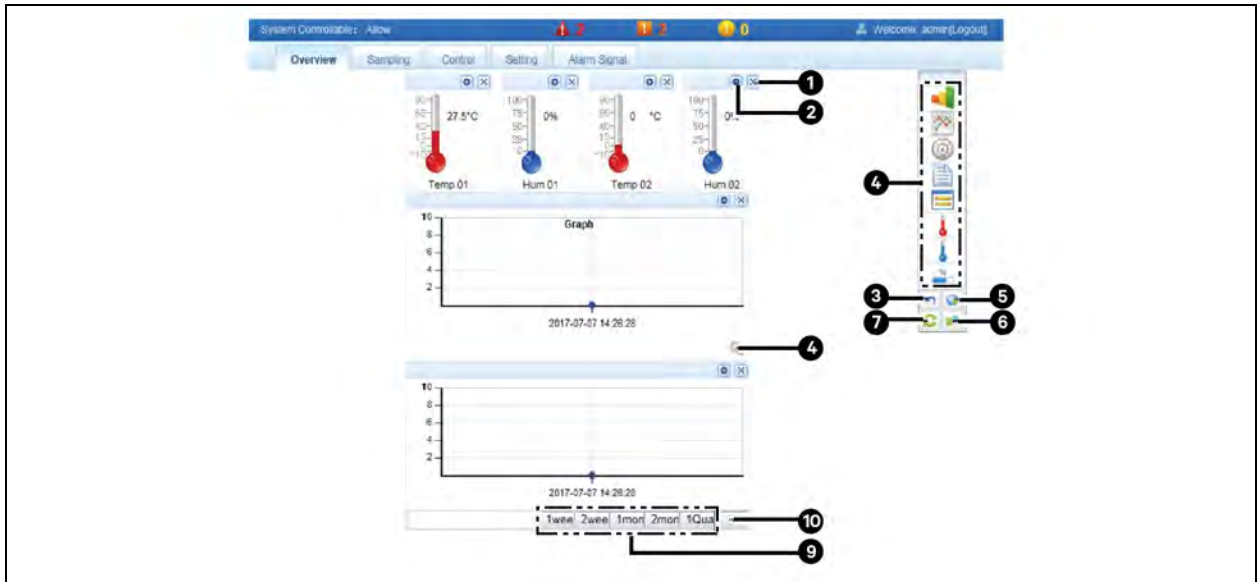
Item	Description	Item	Description
1	Signal configuration icon	6	Effective to same type of equipment icon
2	Remove component icon	7	Restore icon
3	Back to browse icon	8	View history chart icon
4	Component list	9	History data selection icon
5	Save icon	10	View real chart icon

In editing status, clicking the [icon] icon can restore default; clicking the [icon] icon can configure the same type of other devices: click the [icon] icon can save the configuration; click the [icon] icon can return to view status.

NOTE: The Overview page has different default display mode of components for different device type, and clicking the *restore* icon will restore to this state.

NOTE: Certain types of devices (such as air conditioner and UPS) have special status charts, which cannot be deleted or configured. However, the locations of these status charts can be changed.

Sampling

Clicking the *Sampling* tab can enter the sampling page, which displays sampling signals of selected device, as shown in **Figure 6.22** on the facing page.

Figure 6.22 Sampling Signals

1. If some signal is in alarm status, it will be displayed in red.

2. You can click the corresponding signal name for modifying or restoring, as shown in **Figure 6.23** below.

Figure 6.23 Modifying Signal Name
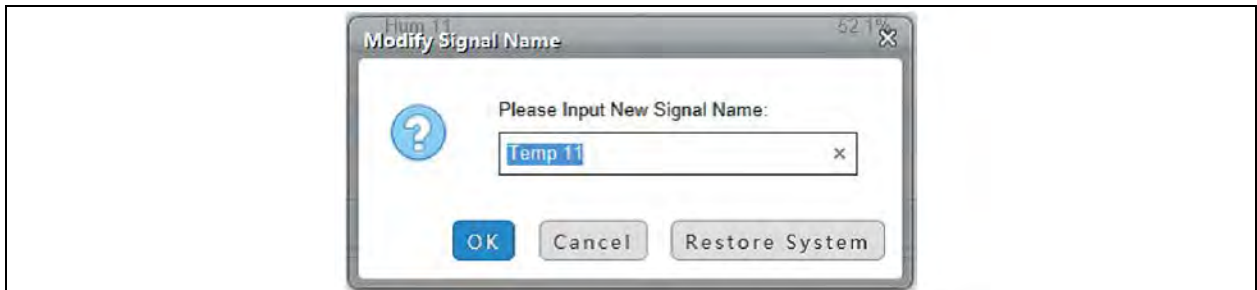
NOTE: For ENV-TH and ENV-4DI devices, see the following descriptions:

After modifying the name of Sampling signals, the names of Control, Setting and Alarm will be modified at the same time.

On the Control, Setting, and Alarm pages, it is prohibited from modifying the signal name.

Control

Clicking the *Control* tab can enter the control page, which displays control signals of selected device, as shown in **Figure 6.24** below.

Figure 6.24 Control Signals

1. Clicking the *Set* button can control the device.

2. For the name of Control signals (except ENV-TH and ENV-4DI), you can click the corresponding signal name for modifying or restoring, as shown in **Figure 6.21** on the previous page.

Setting

Clicking the *Setting* tab can enter the setting page, which displays setting signals of selected device, as shown in **Figure 6.25** below.

Figure 6.25 Setting Signals

1. You can tick multiple check boxes at the most right side to set the signals in batches and you can set up to 16 signals one time.
2. For the name of Setting signals (except ENV-TH and ENV-4DI), you can click the corresponding signal name for modifying or restoring, as shown in **Figure 6.21** on page 76.

NOTE: The ENV-TH device only displays effective setting signals, however, other devices display all setting signals.

Alarm

Clicking the Alarm tab can enter the alarm page, which displays alarm signals of selected device, as shown in **Figure 6.26** on the facing page.

Figure 6.26 Alarm Signals

1. You can tick multiple check boxes at the most you can set up to 16 signals one time, right side to set the signals in batches.

2. For the name of Alarm signals (except ENV-TH and ENV-4DI), you can click the corresponding signal name for modifying or restoring, as shown in **Figure 6.21** on page 76.

6.4.2 Thermal Management

AC TeamWork

The AC teamwork function is used to monitor and control each AC which participates in the AC teamwork according to a certain rule, to achieve the goals of reducing AC power consumption, prolonging AC lifespan and avoiding competition among various ACs in the team.

On the RDU-A G2-A homepage, click the *AC TeamWork* menu in the left, two submenus will appear, including TeamWork Status and TeamWork Setting.

1. TeamWork Status

Click the *TeamWork Status* submenu under the AC TeamWork menu, the page shown in **Figure 6.27** on the next page pops up.

Figure 6.27 TeamWork Status Page
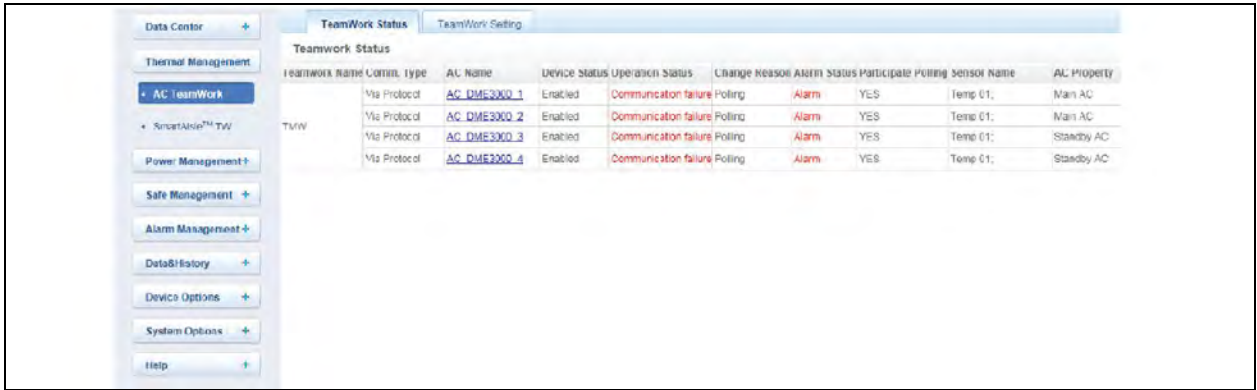
The TeamWork status page displays the main AC running parameters in all AC teams.
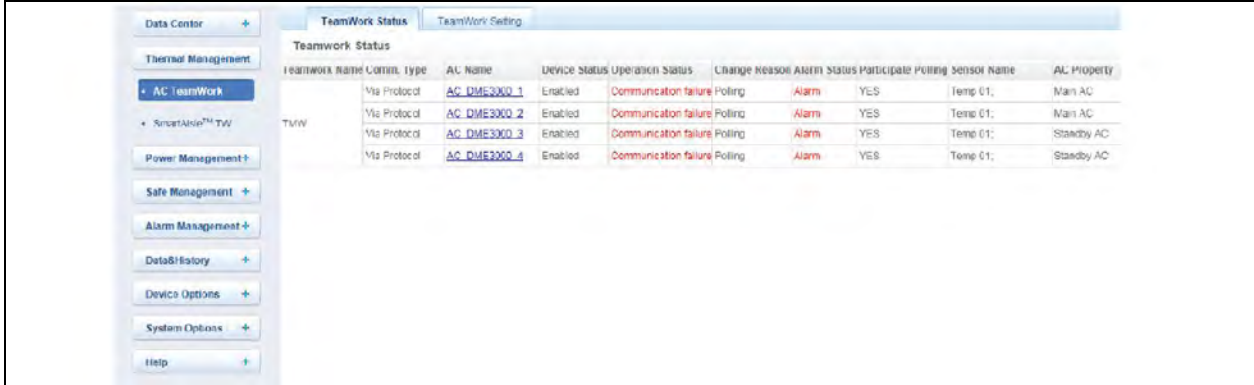
2. TeamWork Setting

NOTE: The AC Teamwork function of RDU-A G2 is available in two versions: standard version and authorized version. The standard version has the AC Teamwork function configured with the RDU-A G2 standard software; the authorized version is a software version which needs to be purchased separately.

    a. Teamwork parameters
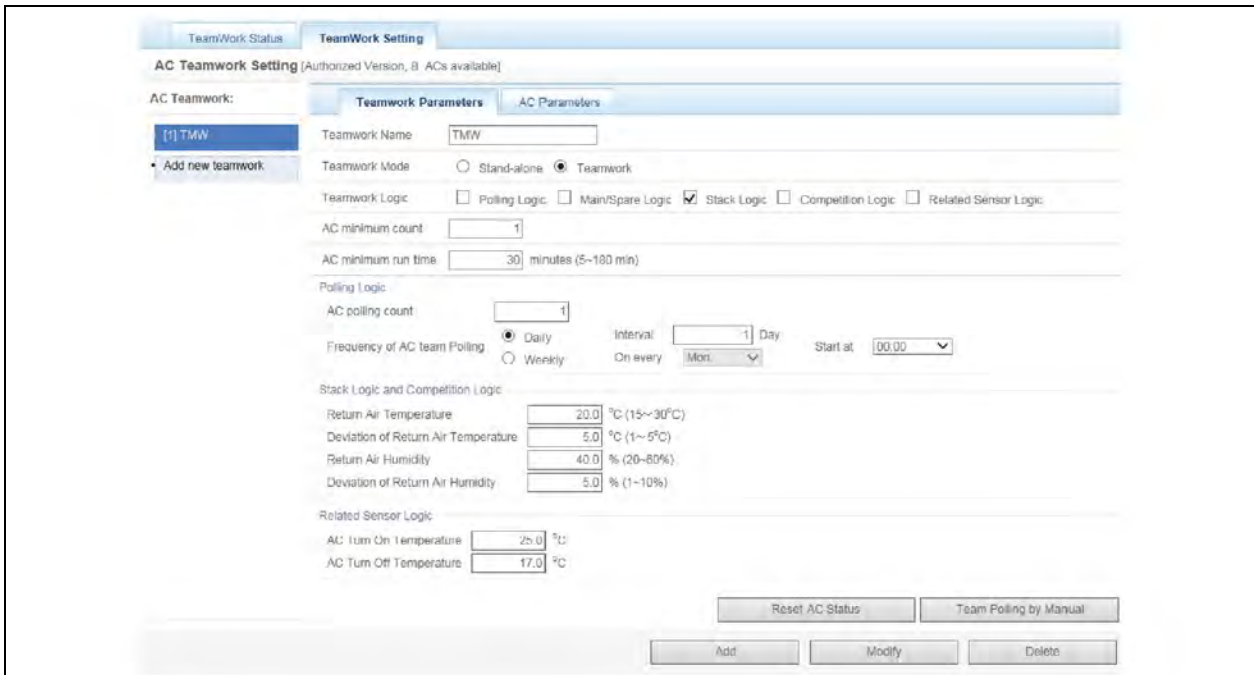
    Click the *TeamWork Setting* submenu under the AC TeamWork menu, the teamwork parameters setting page pops up, the standard version is shown in **Figure 6.28** on the facing page, and the authorized version is shown in **Figure 6.29** on the facing page.

Figure 6.28 Teamwork Parameters Setting Page (Standard Version)

Figure 6.29 Teamwork Parameters Setting Page (Authorized Version)

As for the AC Teamwork function of RDU-A G2 standard version, the descriptions are as follows:

The AC Teamwork function only supports one AC team, [1] TMW by default, without adding and deleting functions; meanwhile, the TeamWork Name cannot be changed. However, the authorized version does not have such limit.

Click the *Click here* to add teamwork link in the AC Teamwork list, you can add a new AC team. After the team parameters are configured, click the *Add* button to save the setting, at this time, the new-added team will be displayed in the left AC Teamwork list.

For detailed parameter descriptions of the teamwork parameters setting page, see **Table 6.1** on the next page.

Add, edit, or delete AC in the team on the AC parameters setting page, see **Figure 6.30** on page 83. Select the AC team which needs to be edited in the AC Teamwork list. Similar to the adding team procedures, edit the team parameters on the teamwork parameters setting page, and set the AC parameters in the team on the AC parameters setting page. After editing, click the *Modify* button to save the setting.

Select the AC team which needs to be deleted in the AC Teamwork list and click the *Delete* button to save the Setting.

Table 6.1 Parameters on the Teamwork Parameters Setting Page

Team Parameter	Default	Low	Upper	Description	Standard Version	Authorized Version
Teamwork mode	Single-alone	Single-alone (0)	Teamwork (1)	Single-alone (0): Each AC in the team operates separately; Teamwork (1): Each AC in the team participated in team Boolean calculation.	✓	✓
AC minimum count	1	1	AC number in the team	/		✓
AC minimum run time	30	5	180	Unit: min		✓
Return air temerature	20	15	30	Unit: °C	✓	✓
Deviation of return air temperature	5	1	5	Unit: °C	✓	✓
Return air humidity	40%	20%	60%	/		✓
Deviation of return air humidity	5%	1%	10%	/		✓
AC polling count	1	1	AC number in the team	Lower value between the running AC number and the backup AC number		✓
Frequency of AC team polling	Daily	Daily, Weekly		/	✓	✓
Interval	1	1	99	Daily mode	✓	✓
On every	1	1	7	Weekly mode Mon, Tue, Wed, Thur, Fri, Sat, Sun	✓	✓
Start at	00:00	00:00	23:00	/	✓	✓
Team polling by manual	No	No	Yes	Used for test	✓	✓
Reset AC status	No	No	Yes	Initializing AC status	✓	✓
AC turn on temperature	25	15	30		✓	✓
AC turn off temperature	17	15	30		✓	✓
NOTE: ✓ means the corresponding version can be configured.						

NOTE: If you need the RDU-A G2 authorized version, contact the Vertiv service center and purchase it.

NOTE: Only four Vertiv DME series ACs with standard configuration are supported by default.

NOTE: RDU-A G2 supports at most eight teams.

b. AC parameters

Click the *TeamWork Setting* submenu under the AC TeamWork menu, and then click the *AC Parameters* button, the AC parameters setting page pops up, as shown in **Figure 6.30** on the facing page.

Figure 6.30 AC Parameters Setting Page

On the AC parameters setting page, you can add, edit and delete AC in the team.

- The procedures for adding an AC are as follows:

    - Select the AC which needs to participate in teamwork from the drop-down box of AC Device.

    - In the AC Index field, type the index of the AC in the team (the AC index will be automatically added from 1).

    - Set the temperature sensors and temperature and humidity sensors related to the AC. Each AC can be related to relevant signals of at most five temperature sensors and temperature and humidity sensors (including at most ten signals of temperature and humidity). When the highest temperature of the related sensors is higher than the AC Turn on temperature, if the air conditioner is off at the time, the air conditioner will start; when the highest temperature of the related sensors is lower than the AC Turn off temperature, if the air conditioner is on at the time, the air conditioner will stop.

    - Set Alarm Signals, that is, when the selected alarm signals are generated, it means that the AC is faulty or cannot be used. At most 15 fault or alarm signals can be set for each AC, and the default fault or alarm signals include: High Temperature Alarm, High Pressure Lock, Low Pressure Lock, and Exhaust Lock.

    - Click the *Add AC* button to add an AC, and the AC basic information will be displayed in the upper list of the page.

NOTE: The AC index cannot be set larger than the AC number of the team.

- The procedures for editing an AC are as follows:

    - Select the AC which needs to be edited in the AC list, and edit the AC rotate index, related temperature and humidity sensors, and AC fault or alarm signals.

- After editing, click the *Modify AC* button to complete modifying, and the AC basic information will be displayed in the upper list of the page.

- The procedures for deleting an AC are as follows:

  - Select the AC which needs to be deleted, and click the *Delete AC* button to complete deleting, and the AC basic information will be deleted from the upper list of the page.

NOTE: After modifying the AC parameters, click the *Modify* button (click the *Add* button after adding a new teamwork) to make it take effect, or the data will be lost after you leave the page.

6.4.3 Power Management

The power management page displays real time and historical energy consumption data according to user-defined rule, to achieve the goal of helping user analyze whole energy consumption of the machine room.

On the RDU-A G2 homepage, click the *Power Management* menu in the left, three submenus will appear, including Current PUE, History PUE, and Calculation Setting.

Current PUE

Click *Power Management -> Current PUE* submenu, the page will display real time PUE and the real time load percent according to user-defined energy consumption setting, for more information see Calculation Setting on the facing page, as shown in **Figure 6.31** below.

Figure 6.31 Current PUE
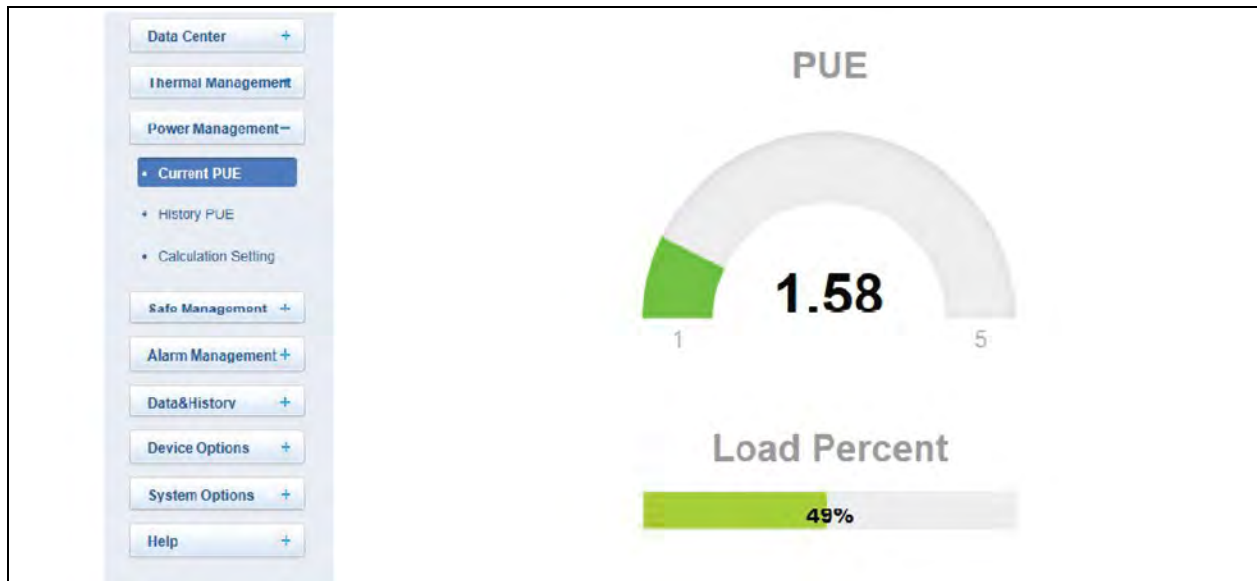
History PUE

Click *Power Management -> History PUE* submenu, the page will display the historical data recorded in the system, as shown in **Figure 6.32** below.

Figure 6.32 History PUE

NOTE: The RDU-A G2 can record and display up to 1000 pieces of PUE historical records.

NOTE: After you perform calculation setting, the system will save a piece of record every 24 hours according to your configuration.
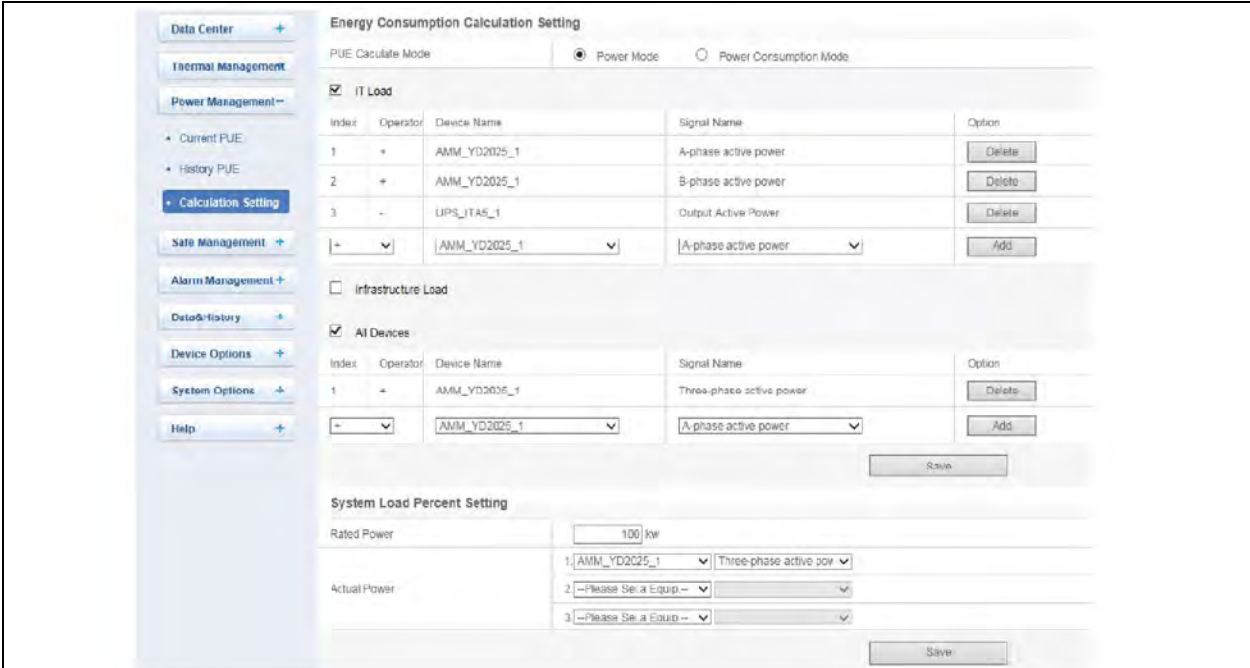
NOTE: If you do not perform calculation setting, the system will not save the PUE records.

NOTE: If you perform calculation setting but do not perform system load percentage setting, the system will still save the PUE records, but the load percent will always be 0.

Calculation Setting

Click *Power Management -> Calculation Setting* submenu, the page shown in above will appear.

Figure 6.33 Calculation Setting

1. Energy consumption calculation setting.

   a. You need to select two types of devices for Energy Consumption Calculation. To facilitate illustration, we define that: A = Energy Consumption of IT load, B = Energy Consumption of Infrastructure load, C = Energy Consumption of all devices. The rules are as follows:

   If you configure calculating A and B, PUE = (A + B)/A.

   If you configure calculating A and C, PUE = C/A.

   If you configure calculating B and C, PUE = C/(C - B).

   Up to 10 signals can be configured for each energy consumption type, and addition and subtraction operations can be selected for each signal. The values of A, B, and C are arithmetic sums of the respective signal values.

   b. Power Mode or Power Consumption Mode.

   - Power mode:

   In the power mode, it is the real time PUE and the system will measure the instantaneous value of device power in real time to calculate the PUE value.

   For example;

   If the IT device power is 8 kW, and the total power of all the devices is 10 kW, then the PUE is 10/8 = 1.25.

   - Power Consumption Mode:

   In Power Consumption Mode, the system will count the device power consumption valve within 8h every 8h from 00:00:00 to 00:00:00 on next day and calculate the PUE value for that period.

   For example;

   The power value at 00:00: The electric energy of IT device is 28kWh, and the total electric energy of all the devices is 62kWh.

   The power value at 08:00 The electric energy of IT device is 36kWh, and the total electric energy of all the devices is 72kWh.

   The PUE from 00:00 to 08:00 is (72 62) / (36 28) = 10 / 8 = 1.25.

NOTE: On the day you perform Calculation Setting, the system will calculate the counting times and valves from the setting time to 00:00:00 on next day and use them to calculate an average valve as the PUE of that day.

NOTE: If Power Mode is selected, you need to select power signals; if Power Consumption Mode is selected, you need to select power consumption signals.

2. System load percent setting.

   You can configure the actual power and rated power to calculate the system load percent, and the rules are as follows:

   - System load percent = actual power/rated power.
   - Among the above, the actual power is summary of the three power signals on the right of actual power.

6.4.4 Safe Management

The safe management monitors the safety of the cabinet through video monitoring, door access management function and fire fighting management.

In the main page of RDU-A G2, left click *Safe Management* menu to show 3 submenus including Door Access, Fire Fighting Management, and Video Surveillance.

Door Access

Click the *Door Access* submenu in the Safe Management menu and the page shown in **Figure 6.34** below appears.

Figure 6.34 Card Management
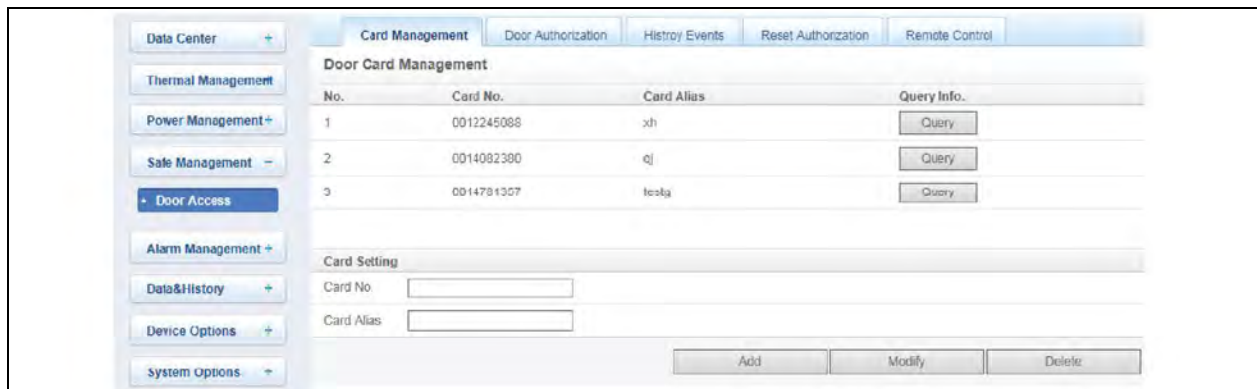
Card management

1. Enter the Door Card No., Card Alias, and Card Password. Click *Add* button to add Door Access Card.
2. Select a *Door Access Card*, and you can Modify and Delete the card information. Click *Query* button, and you can check the authorization information of the card.

NOTE: User can display or hide the access control module in System Setting ->Monitoring Unit->Signal Setting, as shown in **Figure 6.35** on the next page.

NOTE: After connecting RDU-A to RDU-M, the access control management function can be fulfilled through RDU-M.

NOTE: Max number of access controller: 2 access controllers for cold aisle doors + 2 × 24 cabinet door lock controllers.

NOTE: When adding the access control card, you can enter the card number manually, and you can also click *card number* from the access control history log to add the card.

Figure 6.35 Show or Hide the Access Control Management Module
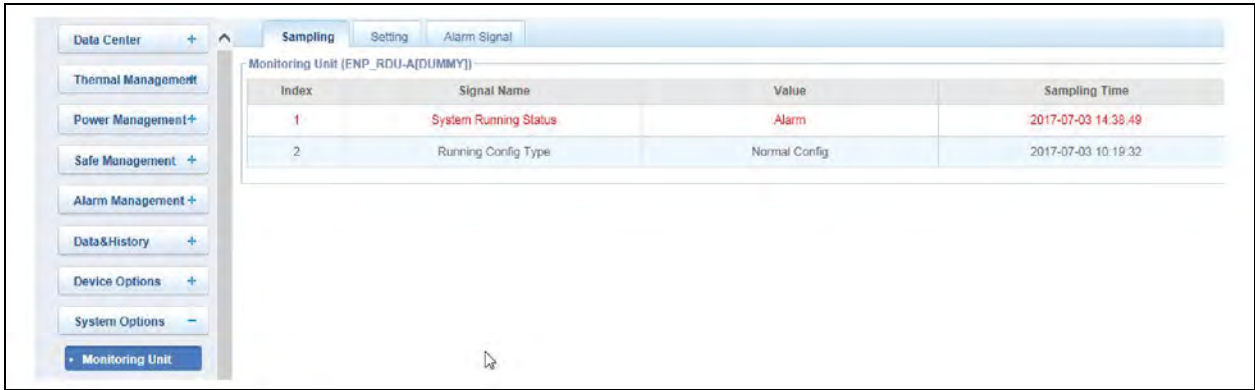
Door authorization

1. Click the *Door Authorization* tab in the Door Access Menu, the page as shown in **Figure 6.36** below will be displayed.

Figure 6.36 Authorization Management
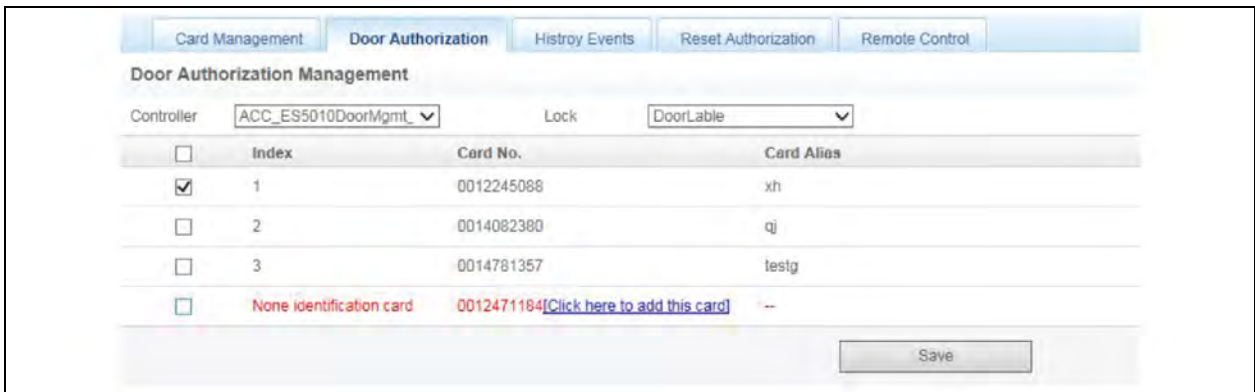
2. After the user selects Controller and Lock, tick the access control card or cancel the ticking, and click the *Save* button to authorize or disable the access control card.

History events

1. Click the *History Events in Door Access* menu, the page as shown in **Figure 6.37** on the facing page will be displayed.

Figure 6.37 History Events

2. User can select the Door Access Controller Name and click *Query* button to query the history events and click *Download* to download the query results.

3. Click the Card Number Link of the invalid card reading event in the history events, and you can go to the Door Access page to add the access control card.

Reset authorization

1. Click the *Reset Authorization* in Door Access menu to show the page as shown in **Figure 6.38** below.
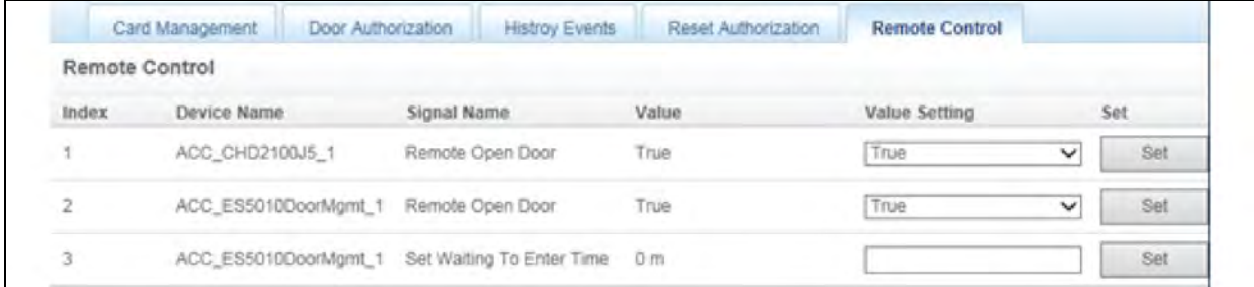
Figure 6.38 Reset Authorization

2. User can select the Access Control Device and click *Clear Authorization* to clear the authorization information of all the access control cards.

Remote control

1. Click the *Remote Control* in Door Access menu, the page as shown in **Figure 6.39** below will be displayed.

Figure 6.39 Remote Control
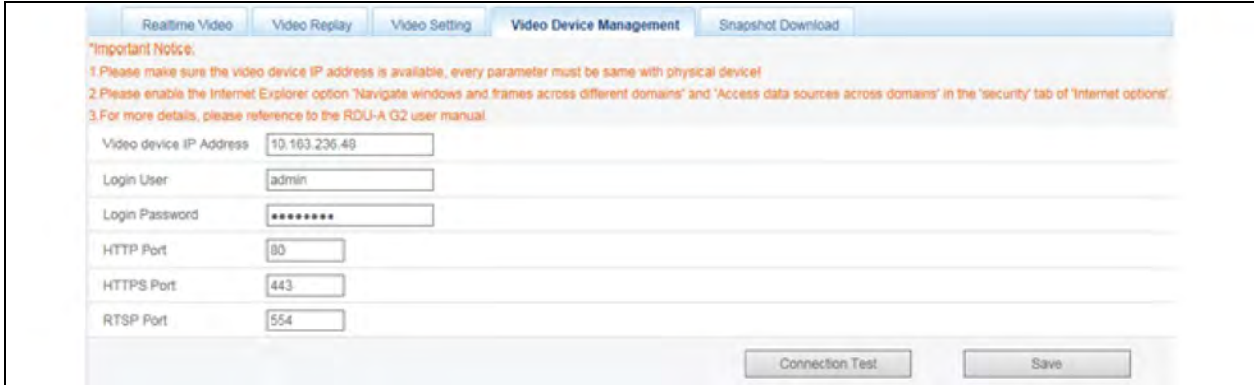
2. User can perform the operation of remotely opening the access control device.

Video Device Management

Click the *Video Device Management* in the Safe Management, and the page as shown in **Figure 6.40** below will be displayed.

Figure 6.40 Video Device Management

Video Device Management

1. Enter the Video device IP Address, Login User and Login Password, HTTP Port, HTTPS Port, and RTSP Port.

2. Click *Connection Test Video* button to test if the video device connection is successful.

3. If the prompt information is "Video Device Connection Test Success" this means the connection is successful, otherwise the connection fails.

4. Check if the entered information of the video device is correct and if the video device connection is correct.

5. Click *Save* button to save the entered information of the video device.

NOTE: Ensure that the IP Address of the video device can be used, and each parameter must be consistent with actual device.

NOTE: Enable the "Cross Field Browse Window and Frame" and "Access Data Source via Field" in the "Safety" of "Internet Option" in browser, as shown in **Figure 6.41** on the facing page.

NOTE: Support single IPC(IP Camera) or one NVR (Network Video Recorder).

NOTE: Under the connection of NVR, support up to 4 channels of video signals.

NOTE: Video management only supports browser.

Figure 6.41 Internet Settings
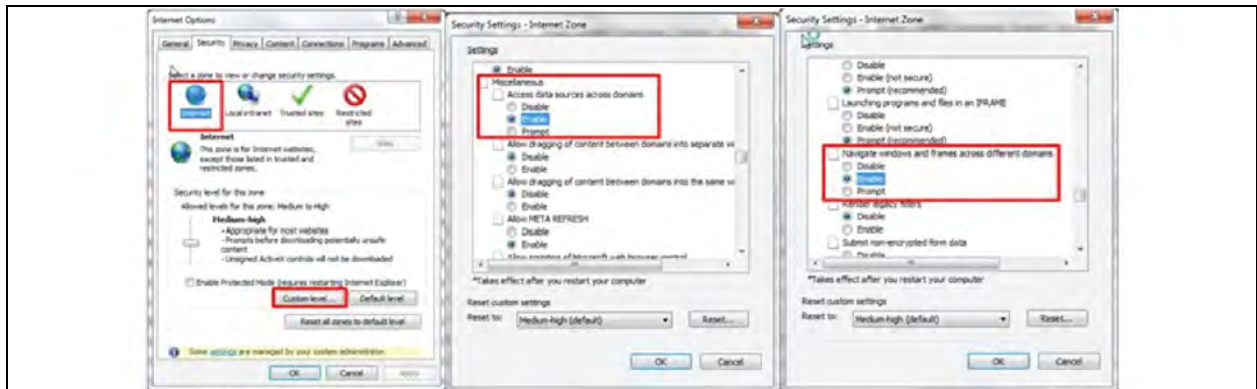
Realtime Video

Click *Realtime Video* in Video Management menu and the page as shown in **Figure 6.42** below is displayed.
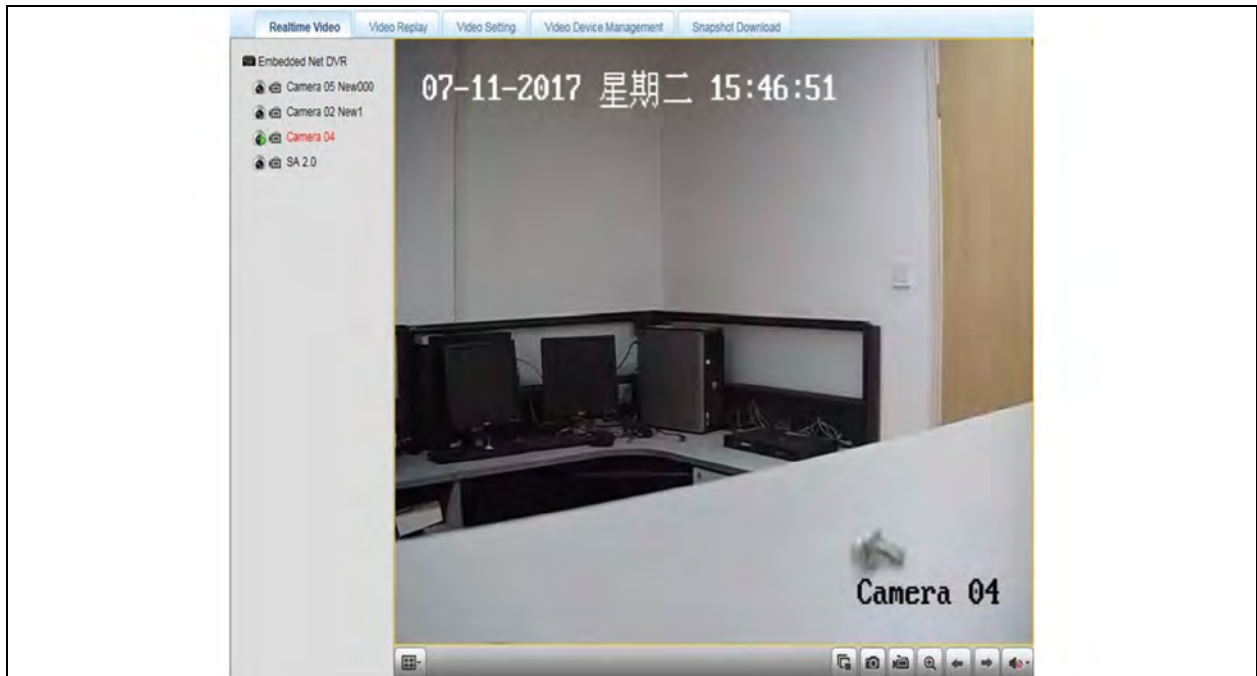
Figure 6.42 Real Time Video

Table 6.2 Description of Icons of Realtime Video

Icons	Description
	Single device start/stops real time browsing
	Set the current page to perform browsing in the 1*1 or 2*2 mode
	All the devices start/stop real time browsing
	Capture image
	Video recording
	Enlarge the video image selected area
	When the current page performs browsing in 1*1 mode, switch to the video monitoring of different devices
	Set the volume of sound

NOTE: After the operations of image capturing and video recording, the files are saved in the corresponding Save Path of Parameter Setting\Local Setting.

Video Replay

Click the *Video Replay* button in the Video Management menu, the page as shown in **Figure 6.43** on the facing page is displayed.

Figure 6.43 Video Replay

Table 6.3 Description of Icons of Video Replay

Icons	Description
	Select the device to the replayed
	Select the replay date and search
	Locate the replay time point
	Play
	Stop
	Play at a slow speed
	Play at a high speed
	Play single frame

Table 6.3 Description of Icons of Video Replay (continued)

Icons	Description
	Capturing image
	Download replayed video file
	Set the volume of sound

Video Setting

Click the *Video Setting* button in the Video Management menu, and the page as shown in **Figure 6.44** below is displayed.

Figure 6.44 Video Setting
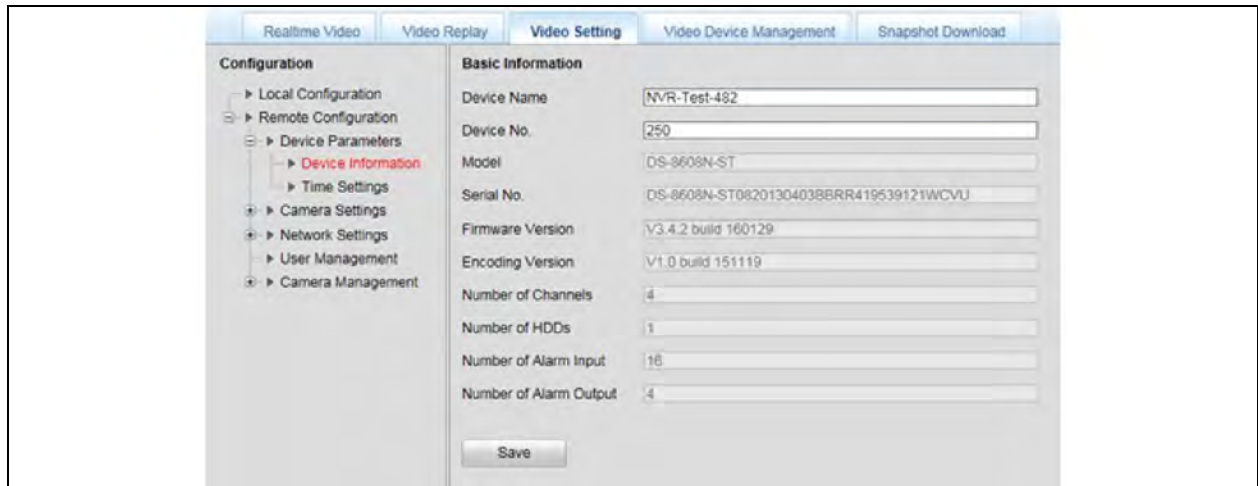
The parameter setting page provides various kinds of parameter settings for the camera and refer to Network Video Camera Operating Instructions provided by NVR for detailed descriptions of the parameters.

Alarm Linkage Snapshot Download

Click *Snapshot Download* submenu in Alarm Management menu, and then the page as shown in **Figure 6.45** on the facing page is displayed.

Figure 6.45 Alarm Linkage Configuration

After the configured alarm conditions are triggered, the video device will capture images or record videos, and the captured images can only be downloaded by clicking *Alarm Linkage Snapshot* Download in Video Management menu in Web page, and you can view and delete the pictures, as shown in **Figure 6.46** below. Up to 50 latest photos can be saved, and you can check the captured videos by clicking *Replay* in Video Management menu.

Figure 6.46 Alarm Linkage Snapshot Download
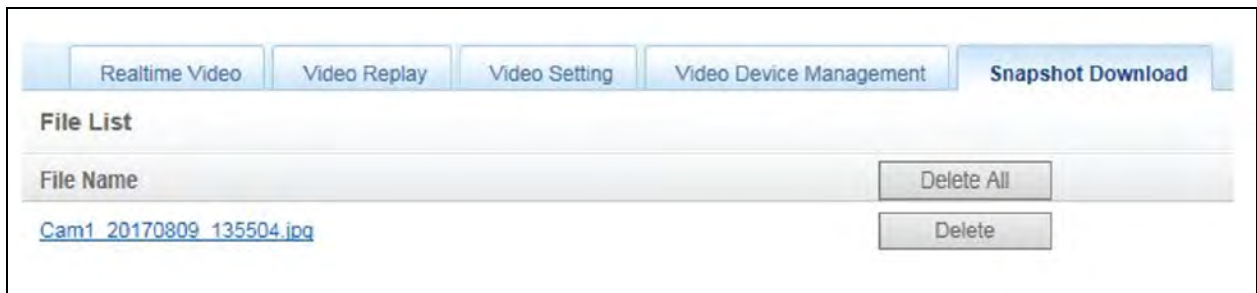
NOTE: For the video recording triggered by alarm, it should be displayed as yellow manual recording during replay.

Fire Fighting Management

Under the condition of equipping fire fighting device (ENP_ENV_FIREFIGHTING[SENSOR]), click the *Fire Fighting* submenu in Safe Management menu, the page as shown in **Figure 6.47** on the next page is displayed.

Figure 6.47 Fire Fighting
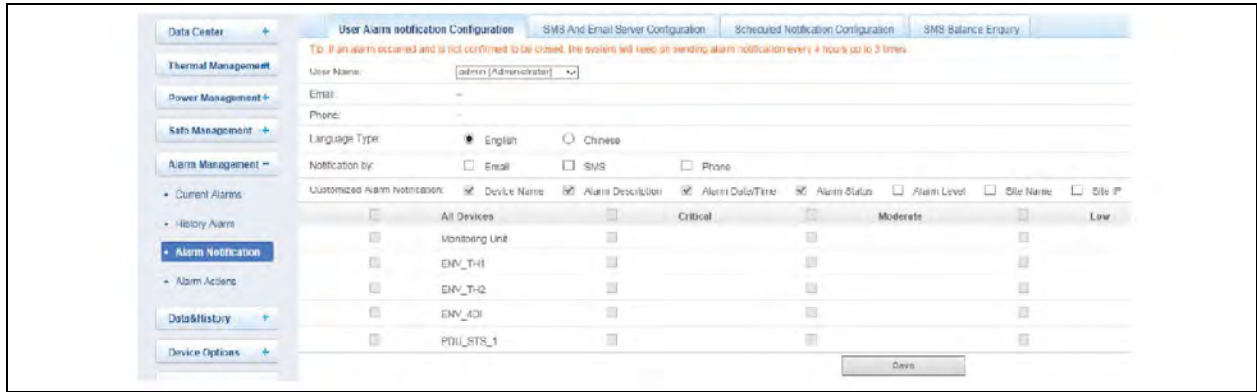
Each firefighting device has up to 4 DI signals that are respectively power supply fault signal, internal fault signal, fire alarm signal and gas spraying signal. They are connected via one IRM-4DI sensor and the address of these 4DI sensors is defined as F1(User Mode). You can realize firefighting signal connection by adding Fire Fighting Device (ENP_ENV_FIREFIGHTING [SENSOR]) in Add/Modify/Delete Device page.

6.4.5 Alarm Management

The Alarm Management menu supplies alarm centralized management function, enabling you of self-defining alarm notification and alarm linkage rules, and viewing historic alarm.

On the RDU-A G2 homepage, click the *Alarm Management* menu on the left, four submenus appear, including Current Alarm, History Alarm, Alarm Notification, and Alarm Actions.

Current Alarms

Click *Current Alarms* submenu under the Alarm Management menu, or refer to 3.3.6 Real-Time Alarm Prompt Setting, the current alarm list will pop up, as shown in **Figure 6.48** below.

Figure 6.48 Current Alarm

1. You can click the tabs above the alarm list to view current alarms according to alarm levels.

2. Click the *Acknowledge* button to confirm the alarm. The confirmed alarm will not participate in alarm linkage, and the alarm notification is sent once only.

3. When the mouse is located on the Confirmed link, the alarm confirming information will be hovered; when you move the mouse, the information will disappear, as shown in **Figure 6.49** below.

Figure 6.49 Confirming Information

History Alarm

Click the *History Alarm* submenu in Alarm Management menu and the following page as shown in **Figure 6.50** below is popped up and has two options of History Alarm Query and Alarm Reports.

Figure 6.50 History Alarm Query

History alarm query

1. Click *History Alarm* submenu under the Alarm Management menu to look over historical alarm records.

2. Select a device (for instance, All Device) and set the start time and end time (for instance, from 2017-036-26 00:00:00 to 2017-06-27 23:59:59).

3. Click the *Query* button, all alarm records generated between the start time and end time will be listed, including: Index, Device Name, Signal Name, Alarm Level, Trigger valve, Start Date/Time, Confirmed by, Confirmed on Date/Time and End Date/Time, as shown in **Figure 6.50** above.

4. Click the *Download* button to download the query results.

Alarm reports

Figure 6.51 Alarm Reports
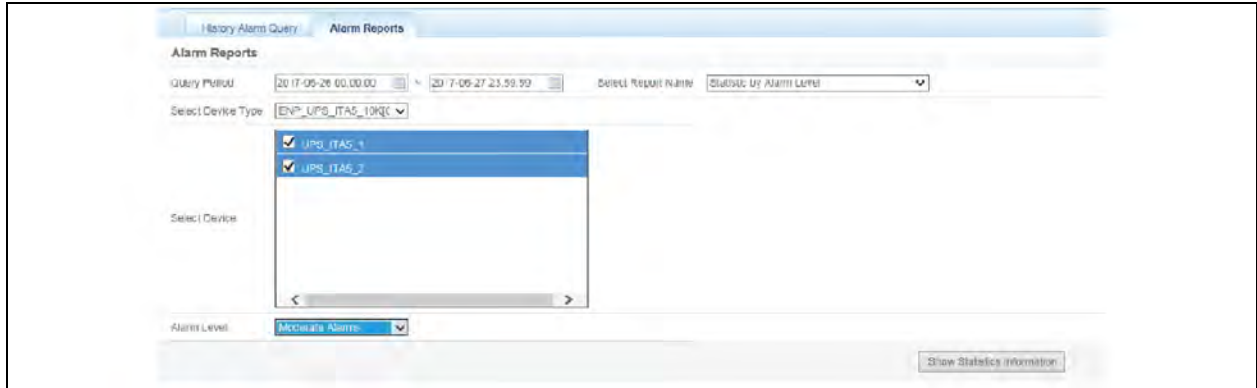
1. Click *Alarm Report* submenu to check the statistic alarm information. Set the query time duration (for example: 2017-06-26 00:00:00" and "2017--06-27 23:59:59).

2. Select report name (for example: "Marking Statistic but Alarm Level") and then select the device type (for example: "ENV_UPS_ITA5_10K[COM]", and select one or more device "Major Alarm"), as shown in **Figure 6.51** above.

3. Click *Generating Statistic Information* button. The statistic report will be generated in graphic mode, as shown in **Figure 6.52** below.

4. Move the mouse cursor to , a dropdown list with options of "PNG", "PDF", and "JPG" will be displayed, and the statistic information will be generated in the file of corresponding format, and you download the file and save it.

Figure 6.52 Making Statistic by Alarm Level
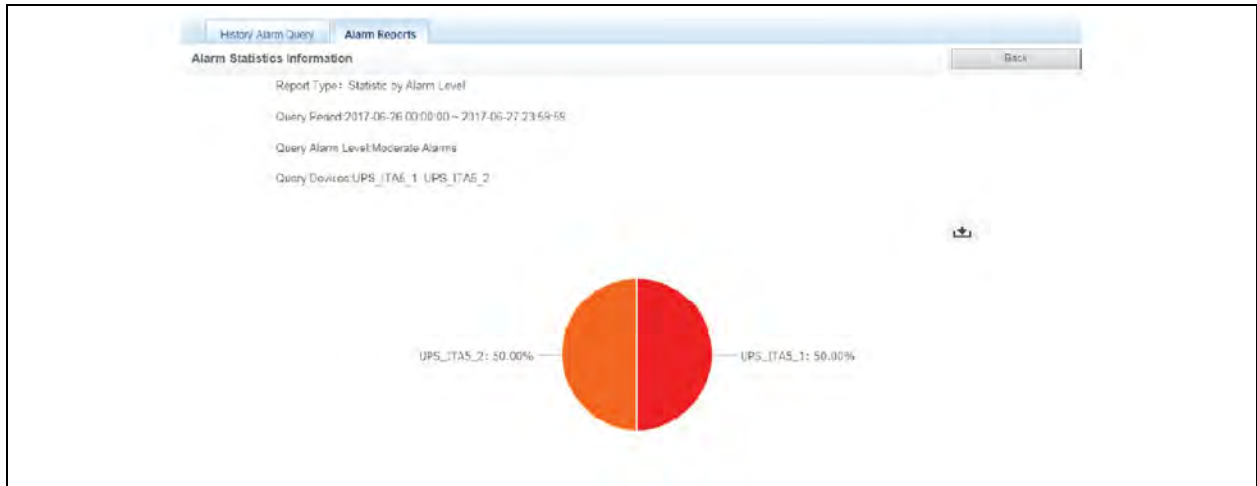
5. Click *Back* button to go back to the alarm report configuration page as shown in **Figure 6.51** above to query other types of alarm reports.

The alarm report provides the following 3 aspects for checking alarm information:

1. Statistic by alarm levels: Use pie-chart to show the percentage of a certain alarm level out of all alarms of multiple devices that belong to one device type in a specific time period.

2. Statistic by alarm signals: Use pie-chart to show the percentage of a certain alarm signals out of all alarms of multiple devices that belong to one device type in a specific time period.

3. Statistic by all sites: Generate the pie-chart that shows the percentages of each alarm level in the selected time period, and use bar-chart to show the number of alarms recorded by months, or the 5 alarms that occur most frequently, as shown in **Figure 6.53** below.
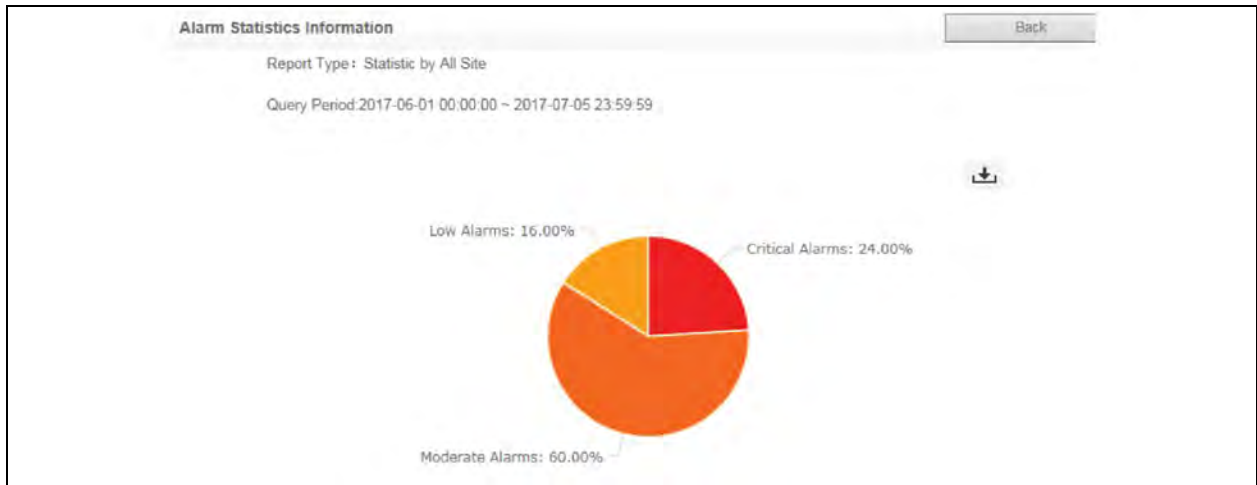
Figure 6.53 Statistic by All Sites (1)

Figure 6.54 Statistic by All Sites (2)
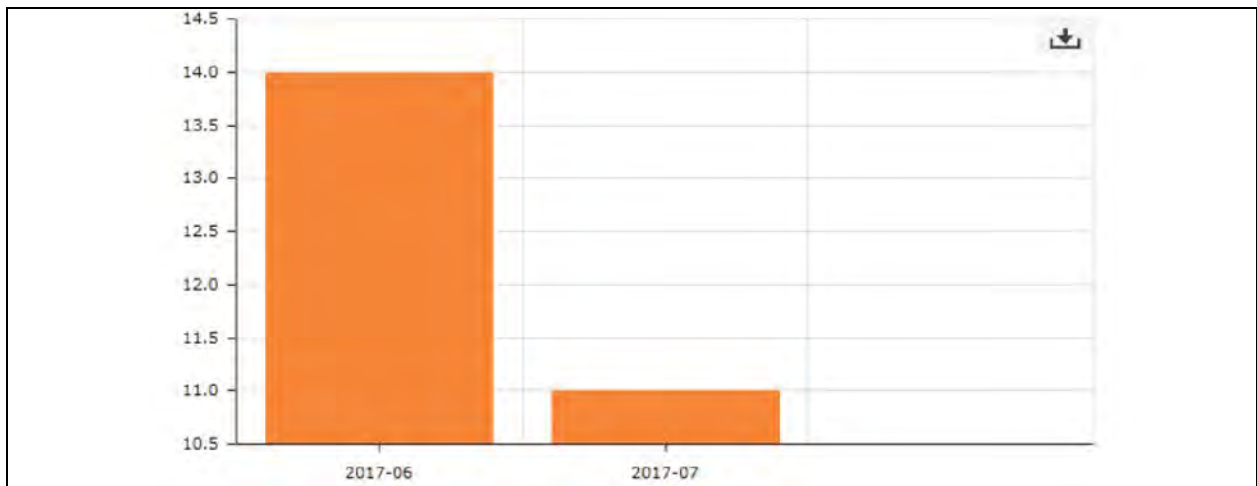
Figure 6.55 Statistic by All Sites (3)

Index	Device Name	Signal Name	Alarm Level	Totally Occur Times
1	ENV_TH1	High Temp 01 Alarm	Critical Alarms	4
2	Monitoring Unit	Outgoing Alarms Blocked	Low Alarms	3
3	ENV_TH1	High Temp 01 Alarm	Moderate Alarms	2
4	UPS_ITA5_1	Communication Failure Alarm	Moderate Alarms	2
5	AC_DME3000_1	Communication Failure Alarm	Moderate Alarms	2

Alarm Notification

Alarm notification configuration

1. Click the *Alarm Notification* submenu under the Alarm Management menu, the page shown in **Figure 6.56** below pops up.

2. You can choose the notification method to receive notification of chosen level alarm from chosen equipment, meanwhile, you can also choose the language of alarm notification information and customize the alarm content (includingDevice name, Alarm Description, Alarm Date/Time, Alarm Status, Alarm Level, Site Name and Site IP by default).

3. Click the *Save* button to finish the alarm configuration. When an alarm is generated, the system will notify users through the chosen notification method.

NOTE: Users must tick the notification method first in the Notification by check boxes, and then the alarm table below can be edited.

NOTE: When all devices are chosen, all devices will be configured with the same alarm level.

NOTE: When low level alarm is chosen, the alarm level above this level will also be chosen.

NOTE: When some device is chosen, the highest level Critical Alarm will be chosen by default.

NOTE: When the alarm is not acknowledged or ended, the system will generate an alarm notification every 4 hours for up to 3 times.

Figure 6.56 Alarm Notification Configuration
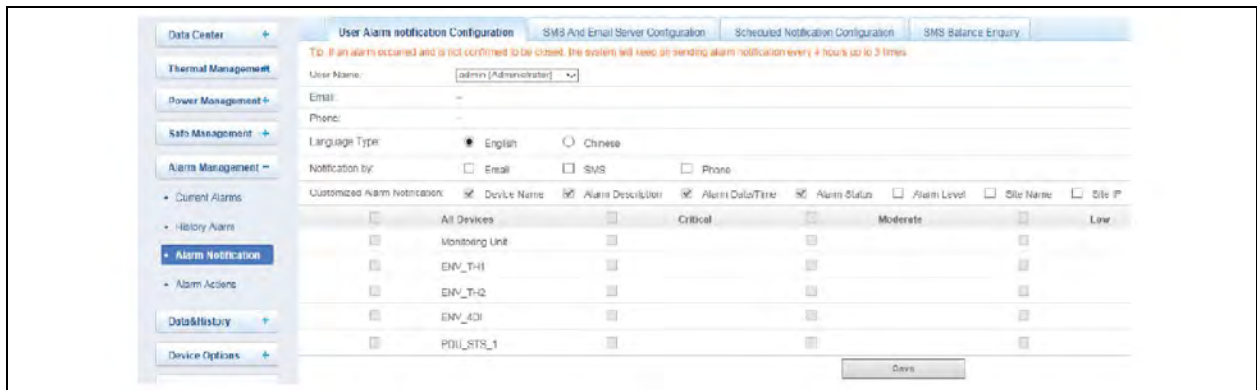
SMS/Email server configuration

1. Click the *Alarm Notification* submenu under the Alarm Management menu, and then click the *SMS/Email Server Configuration* tab, the page shown in **Figure 6.57** below pops up.

Figure 6.57 SMS/Email Server Configuration

2. On the page shown in **Figure 6.57** above, you can perform SMS Modem Configuration and RDU Voice Notification System Setting for alarm notification reminding through SMS or phone, you can also perform Email Server Configuration for alarm notification reminding through email, at the same time, you can modify the product service information through the Email Content Configuration the procedures are as follows:

3. SMS Modem Configuration

   a. Connect an SMS Modem through COM port or USB port according to need, and choose Port Type, the page will display Parameter automatically.

   b. Choose SMS Modem (GSM) according to the SMS Modem type.

   c. Set the communication parameter of the SMS Modem.

   d. Click the *Save* button to save the configuration of current user SMS Modem.

NOTE: If the SMS Modem is connected through COM port, set the communication parameter of the SMS Modem as 9600, n, 8, 1 before using it.

NOTE: If the SMS Modem is connected through USB port, use the default value of the communication parameter of the SMS Modem.

- RDU voice notification system setting.
  a. Enter the server IP address in the Server IP field.
  b. Enter the port number in the Port field, and the default is 13393.
  c. Click the *Save* button to save the voice notification system setting.
- Email server configuration.
  a. Enter the server IP address or domain name in the Email Server field.

b.   Enter the Server Port, Email User, Email Password, and Sender Email Address in the corresponding fields.

c.   Click the *Save* button to save the configuration of current user Email server.

NOTE: The Server Port is 25 by default. When SSL is chosen, the Server Port will become 465 automatically.

NOTE: When using SSL, you need to ensure that the Email server supports SSL function.

NOTE: The format of email is HTML format by default and you can also select text format.

- The email content configuration.

  a.   Enter the email address of the service center in the Contact field.

  b.   Enter the phone number of the service center in the Service Phone field.

  c.   Click the *Save* button to save the email content configuration.

Scheduled Notification Configuration

Click the *Alarm Notification* submenu under the Alarm Management menu, and then click the *Scheduled Notification Configuration* tab, the page shown in **Figure 6.58** below pops up.

Figure 6.58 Scheduled Notification Configuration

NOTE: Scheduled notification configuration must be used together with alarm notification configuration; otherwise, you cannot select User Name, Notification by, and Language type.

NOTE: For scheduled notification configuration, the notification method Phone is not supported.

NOTE: The scheduled notification means sending the running state of the RDU-A G2 system (normal or alarm) to the user.

1.   First, on the Alarm Notification Configuration page, complete and save the setting of User, Notification by, and Language type.

2.   On the Scheduled Notification Configuration page, user can choose whether to enable the notify.

3.   When the Enable the notify is Enabled on the Scheduled Notification Configuration page, set the Notification Scheduled Cycle (default: Day), Interval of Notification (default: Day) and Send Time Setting (default: 11:00).

4.   Click the *Save* button to save the system notification configuration.

SMS Balance Enquiry

Click *Alarm Notification Configuration* submenu in Alarm Management menu, and then click *SMS Balance Enquiry*, the page shown in **Figure 6.59** on the facing page pops up.

     6 RDU-A G2

Figure 6.59 SMS Balance Enquiry

The SMS Balance Enquiry provides periodical query and manual query, as shown in **Figure 6.59** above, fill in the operator number, business number and query period, and click *Save and Enquiry* to save the configurations and send out the enquiry short message. After the system receives the Balance Message returned by the operator, it will save it in the database and forward the information to admin user cell phone. Manually click *Refresh Enquiry Record* to check the balance information in Web page, as shown in **Figure 6.59** above.

NOTE: The SMS balance information will be sent to the admin user cell phone and the user should be configured with a cell phone number.

NOTE: Since there is a delay for the SMS balance information sent by the operator, pay attention to the receive time of the SMS to determine if the SMS has been updated.

Alarm Actions

Click the *Alarm Actions* submenu under the Alarm Management menu to obtain the alarm linkage function, the page shown in **Figure 6.60** below pops up.

**Figure 6.60 Alarm Linkage Configuration 1**

- Alarm output in DO1

If Alarm output in DO1 is ticked, the relay will control the output of DO1 port separately. If the system has an alarm and the alarm has not been confirmed, the relay will be closed; if the system has no alarm or all alarms have been confirmed, the relay will be open, at this time, DO1 will not participate in alarm linkage any more.

- Linkage function

  As shown in **Figure 6.60** on the previous page, the Key to Operator/Symbol list shows all the commands and their usages. Click the *Add* button to add new alarm linkage expression, as shown in **Figure 6.61** below.

Figure 6.61 Alarm Linkage Configuration 2
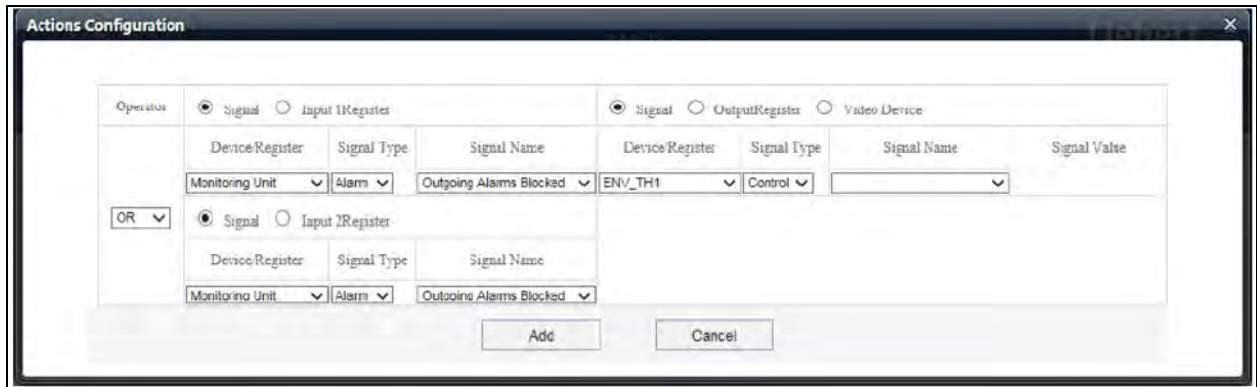
Firstly, select a command, for instance, OR. In this case, the expression is signal 1 [Input1 Register] OR signal 2 [Input2 Register] = signal 3 [Output Register].

Secondly, when Signal is chosen for the input and output parameters, first choose the equip name from the drop-down lists of Equip/Register; then choose the signal type from the drop-down lists of Signal Type; at last choose the signal name from the drop-down lists of Signal Name; signal 1, 2, 3 can be any available signals of the RDU-A G2-A.

Thirdly, when Register is chosen for the parameters, users need to type the register name in the textbox of the register, for instance, R(0), R(1) and so on, as shown in **Figure 6.62** below.

Figure 6.62 Alarm Linkage Configuration 3
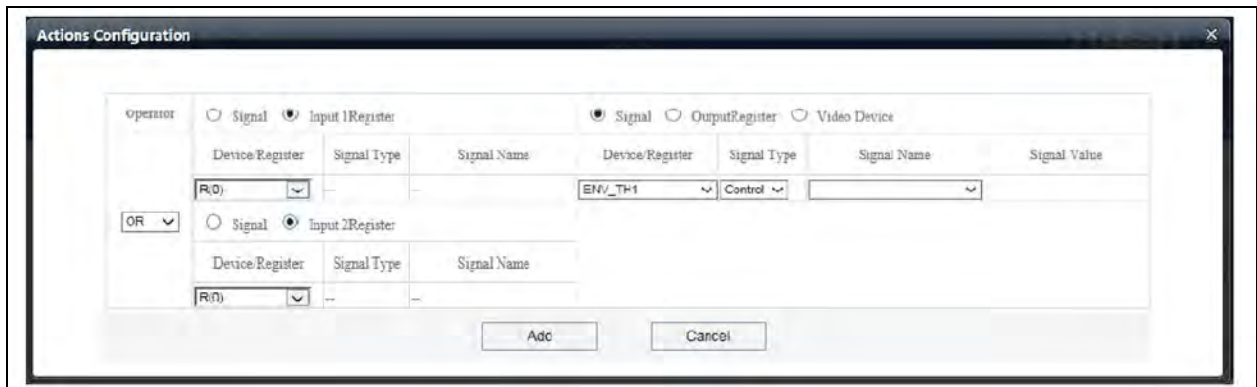
Click the *Add* button to add the new alarm linkage expression, otherwise click the *Cancel* button.

If you click the *Add* button, as shown in **Figure 6.63** on the facing page, an alarm linkage expression is added. Click the *Save and Apply* button to make it effective. Click the *Delete NMS* button to delete the PLC expression and click the *Save and Apply* button to make the setting effective.

Figure 6.63 Alarm Linkage Configuration 4

The operator usages in the alarm linkage are listed below:

Table 6.4 Operator Usage in the Alarm Linkage

Operator	Input 1	Input 2	Param 1	Param 2	Output	Expression
SET	/	/	P1	/	Sout/Rout	SET__P1_Output
AND	Sin/Rin 1	Sin 2/Rin 2	/	/	Sout/Rout	Sin 1 [Rin1} AND Sin2 [Rin2] = Sout [Rout]
OR	Sin/Rin 1	Sin 2/Rin 2	/	/	Sout/Rout	Sin 1 [Rin1} OR Sin2 [Rin2] = Sout [Rout]
NOT	Sin/Rin 1	/	/	/	Sout/Rout	Sin 1 [Rin1}NOT = Sout [Rout]
XOR	Sin/Rin 1	Sin 2/Rin 2	/	/	Sout/Rout	Sin 1 [Rin1}XOR Sin2[Rin2] = Sout [Rout]
GT	Sin/Rin 1	/	P1	P2	Sout/Rout	When Sin1 [Rin1] > P1, Sout [Rout]=1 When Sin1 [Rin1] < P1 - P2, Sout [Rout]=0;
LT	Sin/Rin 1	/	P1	P2	Sout/Rout	When Sin1 [Rin1] < P1, Sout [Rout]=1; When Sin1 [Rin1] > P1 + P2, Sout [Rout]=0;
DS	Sin/Rin 1	/	P1	P2	Sout/Rout	Sin [Rin 1] DS P1 output to Sout [Rout]

NOTE: 1. Sin1, Rin1, Sin2, Rin2, P1, P2, Sout, Rout respectively refer to Signal 1, Input1 Register, Signal 2, Input2 Register, Parameter 1, Parameter 2, Signal 3, Output Register.
2. The input signal of logic operator AND/OR/NOT/XOR/DS can only be alarm signal.
3. The input signal value of arithmetic operator GT/LT can only be float, int or long int.
4. The output signal can be a control signal or a signal setting.

The following illustrates the alarm linkage with examples:

Example 1:

If it is required that when the temperature and humidity sensor of RDU-A G2 system generates a high temperature alarm, the alarm lamp turns on. Suppose that the alarm lamp is mounted on the DO1 port, you can achieve the alarm linkage function through the following configuration:

Expression: [High Temp 11 Alarm] DS P(3) [RDU-A DO1] [Close].

The configuration method is shown in **Figure 6.64** on the facing page. When the High Temp 11 Alarm is generated, RDU-A DO1 will close after a delay of 3s, thus the alarm lamp turns on.

Figure 6.64 Example 1 for Alarm Linkage

Example 2:

If it is required that when the front door or back door of the rack is open, the alarm lamp turns on. Suppose that the DI1 and DI2 ports of the RDU-A G2 are respectively connected with the door status sensors on the front and back door, and the alarm lamp is mounted on the DO1 port. You can achieve the alarm linkage function through the following configuration:

Expression: [RDU-A DI1 Alarm] OR [RDU-A DI2 Alarm] = [RDU-A DO1] [Close].

The configuration method is shown in **Figure 6.65** below. When the alarm signal of RDU-A G2 DI1 Open or RDU-A G2 DI2 Open generates an alarm, RDU-A G2 DO1 will close, thus the alarm lamp turns on.

Figure 6.65 Example 2 for Alarm Linkage

6.4.6 Data and History

The Data and History menu supplies query service of all types of historical data and logs for the user.

On the RDU-A G2 homepage, click *Data and History* in the left part, four submenus appear, including: Device Information, History Data, History Log, and Clear History.

Device Information

Click the *Device Information* submenu under the Data and History menu, the page shown in **Figure 6.66** on the next page pops up.

The page includes four tabs: Device Information List, Export SNMP MIB, Asset Inventory, and Asset Batch Configuration.

Device information list

As shown in **Figure 6.66** below, the page lists the main information of all equipment. Click the *Download* button to download the query result.

Figure 6.66 Device Information List
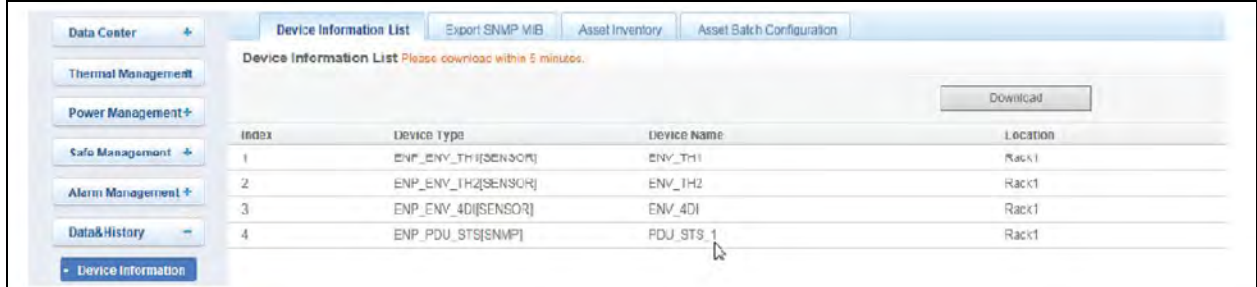
Export SNMP MIB

As shown in **Figure 6.67** below, you can select Export All Device MIB or Export MIB By Device. After selection, click the *Download* button to export MIB information.

Figure 6.67 Export SNMP MIB

NOTE: If you do not get the SNMP service authorization, the Export SNMP MIB page will not appear. If you need to get the SNMP service license, contact Vertiv service representative for purchase.

Asset Inventory

Click the *Device Information* submenu under the Data and History menu, and then click the *Asset Inventory* tab, the page shown in **Figure 6.68** on the facing page pops up.

You can check all the asset information of RDU-A G2. Select the query type, enter query conditions to check all the information of the assets that meet the conditions.

Figure 6.68 Asset Inventory

Asset Inventory Query

The asset information provides 4 query methods:

> **Query by name:** Enter a character string that is not void, return the asset information of the asset name that contains the character string.

Figure 6.69 Query by Name

> **Query by Number:** Enter a character string that is not void, return the asset information of the asset number that contains the character string.

Figure 6.70 Query by Number

> **Query by ID Range:** Enter two integers M and N, wherein M < N, return the information of the asset with its ID number not less than M but is not more than N.

Figure 6.71 Query by ID Range

Query by Expired Date: Select one date, return the information of the asset that is 3-month earlier than or after the expired date.

Figure 6.72 Query by Expired Date

The queried information will be displayed in the format of table, as shown in **Figure 6.73** below.

Figure 6.73 List of Asset Information

Modify asset information

You can add, modify, and delete the asset information in the page as shown in **Figure 6.74** below.

Figure 6.74 Edit Asset Information

NOTE: When starting up RDU-A for the first time, the asset information page has no asset data, you need to add asset through the "Save Configuration" Button in the Configuration Management->Device Management ->Add /Modify/Delete page, or add common asset manually in asset information page.

NOTE: We added the asset type property to meet the needs of the RDU-M asset information to differentiate the device asset and common asset, and the differentiation is made when importing the asset. RDU-A does not care about the asset type, so the asset type is not differentiated in web page.

NOTE: Device asset: Correspond to the devices in the RDU-A Add /Modify /Delete page, and automatically import the asset information by clicking the *Save Configuration* button in the ADD/Modify/Delete page.

NOTE: Common asset: The asset is not in the monitoring range of RDU-A and can be manually added in asset information page.

Enable asset maintenance reminder

RDU-A G2 provides the function of reminding asset maintenance and user can enable the asset maintenance reminder function, as shown in **Figure 6.75** below.

Figure 6.75 Enable Asset Maintenance Reminder

Figure 6.76 Highlight the Expired Date

If an asset will be expired within 3 months, it will be counted into the expired device list, and the expired date will be highlighted in red color in asset information list, as shown in **Figure 6.76** above. When user refreshes or logs in RDU-A G2 WEB page, the system will prompt the expired devices in pop-up window and user can close the window manually, and the window can be closed automatically after 5 min.

The system will detect at 9 o'clock on the first day of every month. If there is an expired device in the asset list and if the admin user of RDU-A G2 is configured with a cell phone or email, the expiry reminder information will be sent to the user's cell phone or email box. If the user purchases and renews the warranty and updates the expired date, the notification will not be sent out again.

Asset Batch Configuration

Click the *Asset Batch Configuration* in Data & History submenu in Device Information menu, the page as shown in **Figure 6.77** on the next page is popped up.

Click *Download* button to export the current asset information to the local computer, and the information is saved in the format of.xlsx file. Use this file as the template, after editing and adding asset information, click *Upload* button to import the asset information in local computer into RDU-A G2 in batches.

Figure 6.77 Asset Batch Configuration
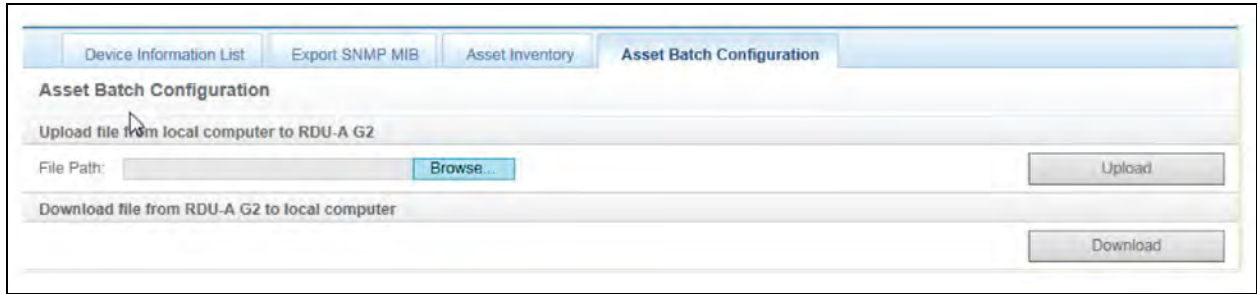
NOTE: If the asset code in the file is not the same with that in the RDU-A G2, then add new asset and this asset is considered as common asset.

NOTE: If the asset code in the file is the same with that in the RDU-A G2, then use the asset information in the file to overwrite the information in RDU-A G2. If the original asset is the device asset, it is still the device asset, otherwise it is the common asset.

NOTE: When importing the asset information, the system will check if the information field is valid and if the field has invalid information, the system will pop up a prompt window to tell the user the information in which cell has errors.

History data

Click the *History Data* submenu under the Data & History menu, the page shown in **Figure 6.78** below pops up. The page has three tabs: History Report, Historical Curve, and Curve Setting.

Figure 6.78 History Report

- History Report

  As shown in **Figure 6.78** on the previous page, choose a device for instance, All Devices and the Log Type (for instance, History Data), and set the start time and the end time (for instance, from 2014-04-01 00:00:00 to 2014-04-01 23:59:59). Then click the *Query* button, all the history data during the time will be listed, click the *Download* button to download the query result.

- Historical Curve

  As shown in **Figure 6.79** below, Select a report name (for example: "THH"), and set the query time duration (for example: from 2017-06-23 00:00:00 to 2017-06-27 23:59:59), and then click *Show Curve* button, if history data is queried, then history curve will be generated by signals.

Figure 6.79 Historical Curve

NOTE: Report name: The name added in the "Curve Report Setting" page, refer to Curve Setting on the next page.

- Curve Setting

  As shown in **Figure 6.80** on the next page, enter device (for example: "ENV_TH"), select signal (for example: "temperature 11", "temperature 41"), enter the reference report name (for example: "THH"), select device type (for example: "ENV_TH"), select curve values (for example: "Note need"), click *Add* button, and a curve report can be added, as shown in **Figure 6.80** on the next page. Up to 16 reports can be added.

NOTE: In the same coordinates, up to 8 curves can be displayed, that is 1 <=m*n <=8. If more than 8 curves are needed, export the history data by yourself.

Figure 6.80 Curve Setting
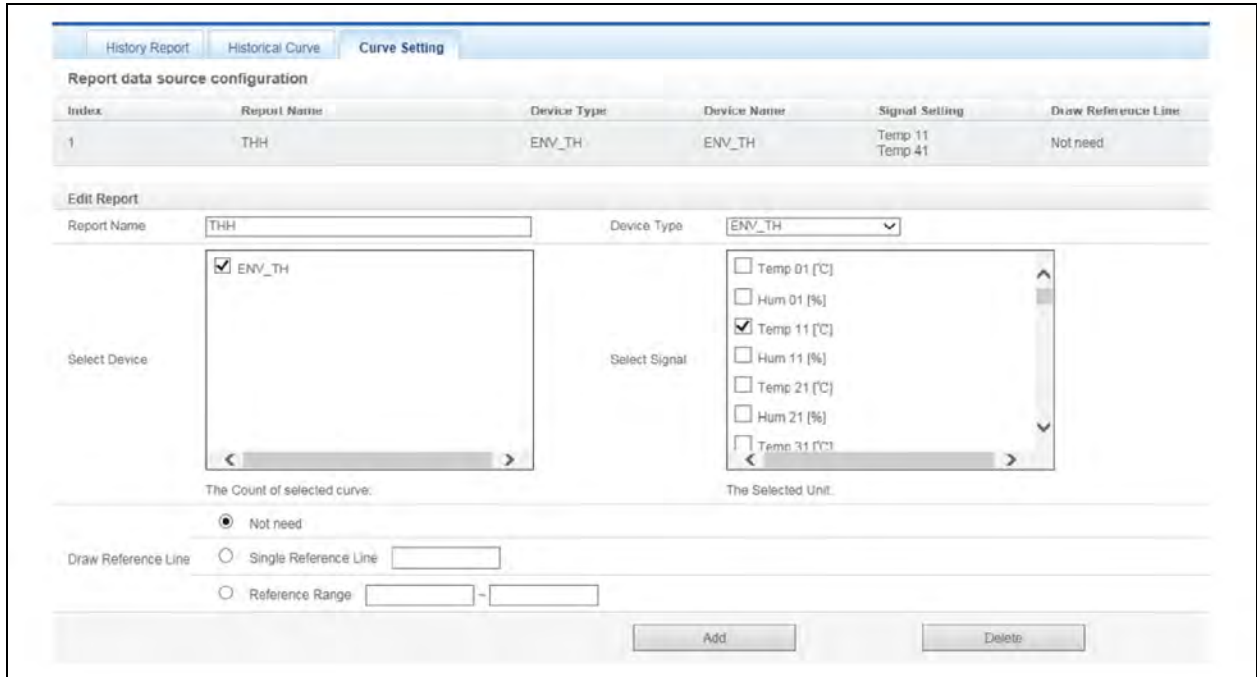
- Smart Reports

  Click the *Smart Reports* submenu in Data & History menu to pop up the page as shown in **Figure 6.81** below, and the page has two options of Smart Reports View and Smart Reports Setting.

Figure 6.81 Smart Reports View 1
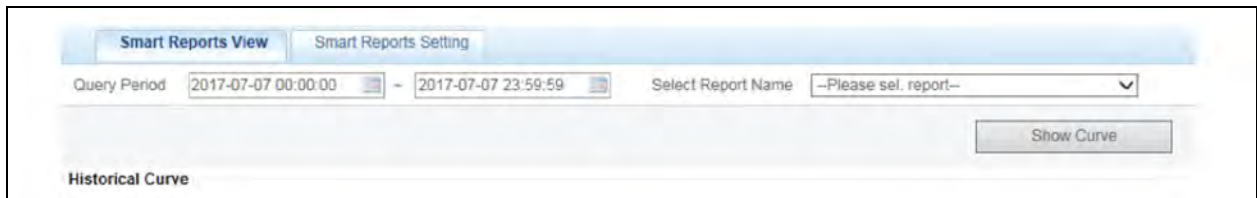
In the page as shown in **Figure 6.81** above select the report name (for example: "Cold aisle Temperature Curve Report"), and set the query time duration (for example: from 2017-06-23 00:00:00 to 2017-06-27 23:59:59), and then click *Generate Curve* button, if history data is queried, then history curve will be generated by signals, as shown in **Figure 6.82** on the facing page.

Figure 6.82 Smart Reports View 2

- Smart Report Setting

    As shown in **Figure 6.83** on the next page, Smart report only provides "Cold Aisle Temperature Curve Report", "Hot Aisle Temperature Curve Report" and "UPS Output Power Curves".

    Select report type (for example: "Cold Aisle Temperature Curve Report"), select device type (for example: "ENV_TH"), select device (for example: "ENV_TH"), select signal (for example: "temperature 11", "temperature 41"), and enter the reference standard range (for example: "26" and "32", and click *save* button to save the curve report setting).

Figure 6.83 Smart Reports Setting
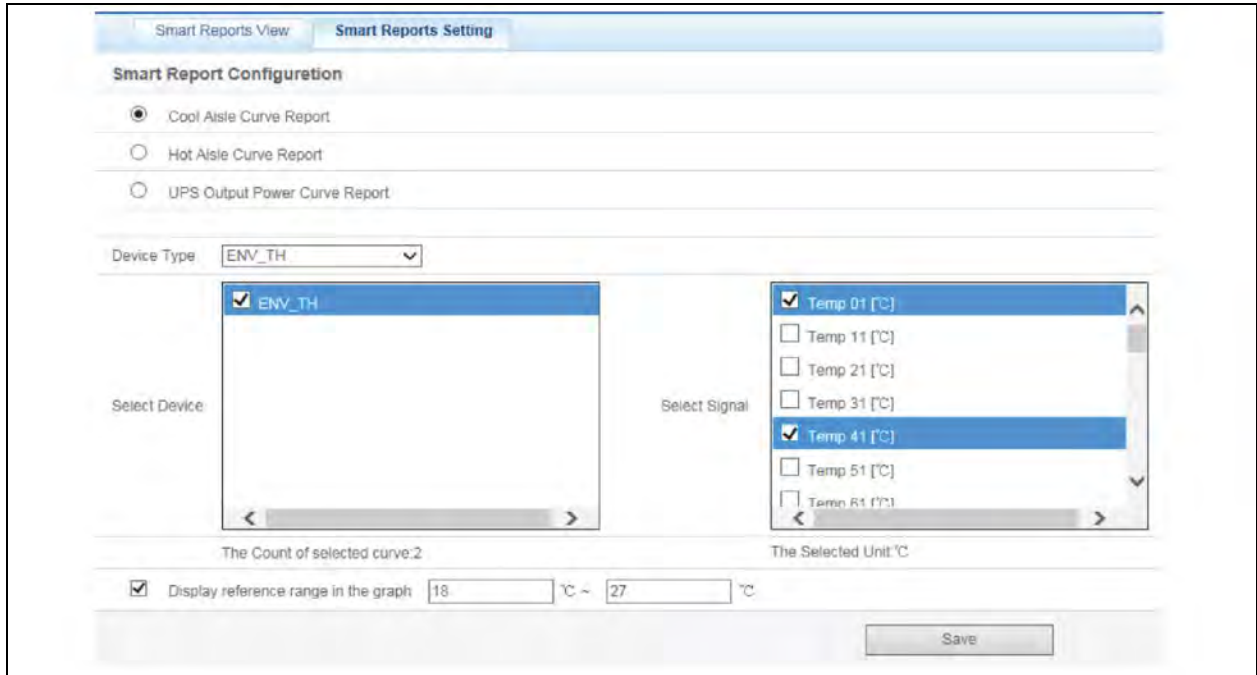
NOTE: In the same coordinates, up to 24 curves can be displayed, that is 1 <= m*n <= 24. If more than 24 curves are needed, Export the history data by yourself.

- History Log

Click the *History Log* submenu under the Data & History menu, the page shown in **Figure 6.84** below pops up.

Figure 6.84 History Log
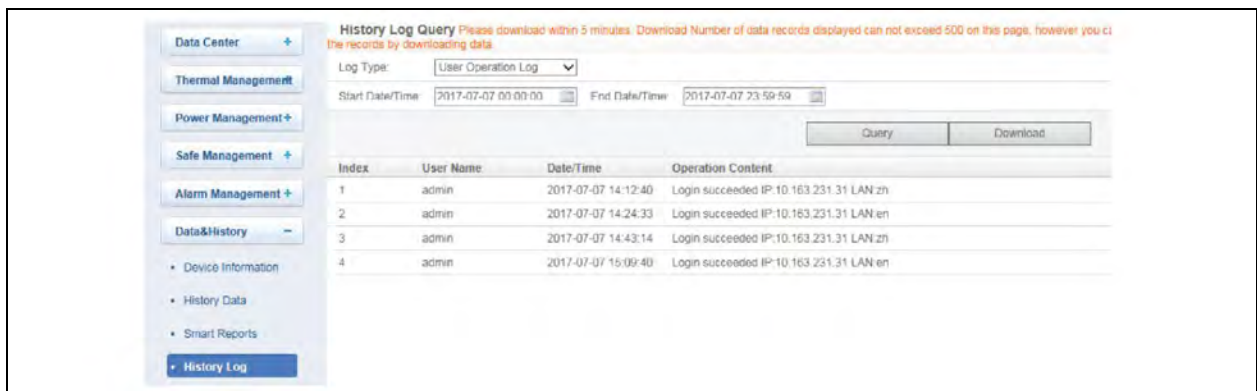
On the page shown in **Figure 6.84** above, choose the log type (for instance, User Operation Log) and set the start time and the end time (for instance, from 2017-07-07 00:00:00 to 2017-07-07 23:59:59). Then click the *Query* button, all user operation logs during the time will be listed, click the *Download* button to download the query result.

NOTE: When the log type is selected as System Log or Driver Log , after clicking the *Query* button, the query result will not be displayed on the page, instead, it will be directly downloaded as a zip file.

- Clear History

  Click the *Clear History* submenu under the Data & History menu, the page shown in **Figure 6.85** below pops up.

Figure 6.85 Clear History
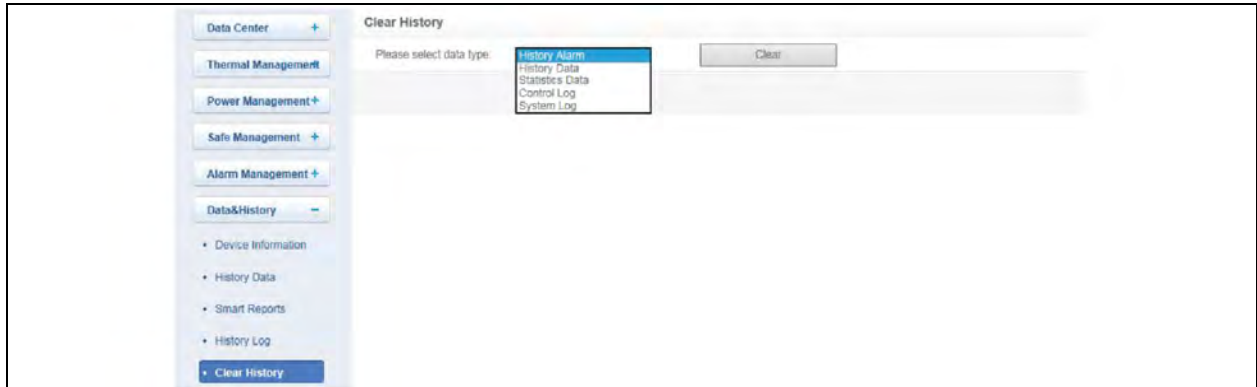
As shown in **Figure 6.85** above, you can choose History Alarm and click the *Clear* button to clear all the history alarm. In the same way, you can clear any other getable data in the drop-down box.

6.4.7 Device Options

On the RDU-A G2 homepage, click *Device Options* in the left part, three submenus will appear, including Device Management, Signal Setting, and Batch Configuration.

Device Management

Add/Modify/Delete Device

Click the *Device Management* submenu under the Device Options menu, the page shown in **Figure 6.86** on the next page pops up.

Figure 6.86 Add/Modify/Delete Equipment

As shown in **Figure 6.86** above, you can add/modify/delete a new device, the procedures are as follows:

To add new device, follow the below procedure:

1. Choose the device type in the Device Type textbox.
2. Enter the device name in the Device Name textbox, or use the default device name.
3. After the device type is chosen, the drop-down box of Port will list the default port number(s) of the device type automatically; if the device type is not chosen, the port number cannot be chosen.
4. Enter the device address, which must be numbers from 1 to xx, in the Device Address textbox. The device addresses under the same port number must be different; for some device types, you need not type the device address, at this point, the Device Address textbox turn gray and cannot be edited. When one kind of device has many models, you need to type the model ID, which must be numbers from 1 to xx. The model IDs under one kind of device must be different.
5. Choose or type the device location.
6. Enter the communication parameter in the Parameter textbox. In the event that the device type is certain, the communication parameter prompt information will appear in the Parameter textbox, including the communication parameter format and default communication parameter of the equip type.
7. Click the *Add* button, the page shown in **Figure 6.87** below pops up, at the same time, a piece of new device information will be added in the device list.

Figure 6.87 Prompt Information 1
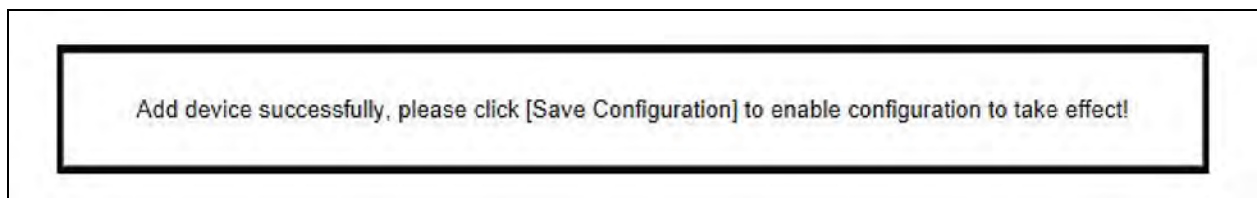
8. Click the *Save Configuration* button, the page shown in **Figure 6.88** on the facing page pops up.

Figure 6.88 Prompt Information 2
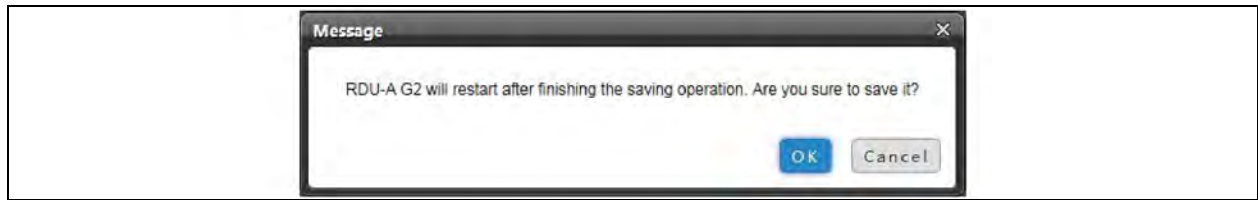
9. If clicking the *Cancel* button, the added equipment fails; if clicking *OK*, the dialog box of Security authentication pops up.

10. Enter the login password of current user and click *OK*. The reboot page pops up, as shown in **Figure 6.89** below.

Figure 6.89 Reboot Page
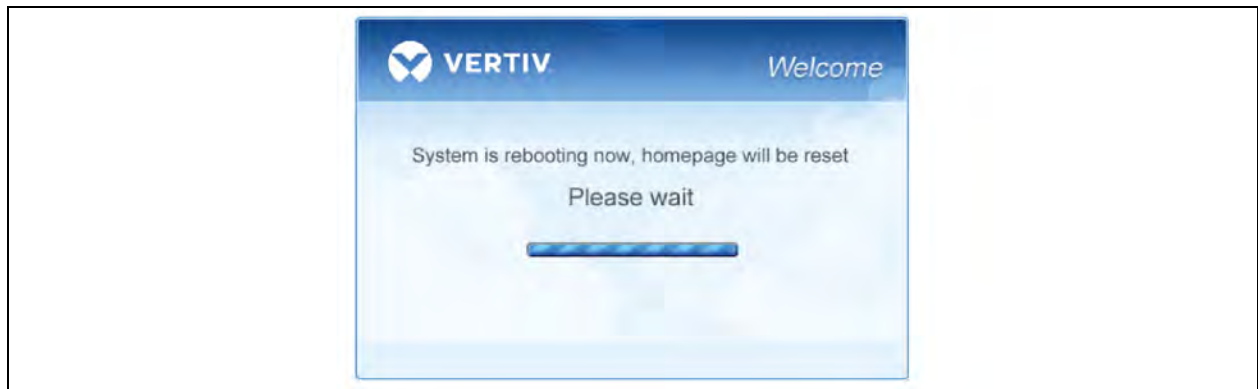
After the system reboots, adding a device becomes effective.

11. Log in the RDU-A G2 webpage again and the added device will appear in the list on device management page.

NOTE: Up to 16 intelligent devices (excluding RDU-A G2 itself, ENV-TH, ENV-4DI, 8DIAI card, 8DOAO card and Cabinet Level Access Control Device) can be added in the system by default. Through authorization, the connecting capacity can be expanded. If you need to expand the connecting capacity, contact Vertiv customer service center for purchase, and the contact number is *4008876510*.

NOTE: If the 4COM extension card has been configured with a device, remove 4COM card at this time, then the device configuration status will be changed to disabled status, and a che -83, after re-enable the device.

To Delete a device, follow the below procedure:

1. Choose the device which needs to be deleted in the device list.

2. Click the *Delete* button to delete the device.

3. Click the *Save Configuration* button to make the settings become effective, and the detailed procedures are the same as those of adding a new device.

NOTE: Before clicking the *Delete* button, if the device information has been modified, it cannot be deleted.

To Modify a device, follow the below procedure:

1. Choose the device which needs to be modified in the device list.

2. Modify the device information.

3. Click the *Modify* button to make the setting effective.

4. Click the *Save Configuration* button to make the settings become effective, and the detailed procedures are the same as those of adding a new device.

    After adding, modifying or deleting procedures, if you leave the Add/Modify/Delete Device page without clicking the *Save Configuration* button to make the settings effective, the prompt information will pop up to remind you, as shown in **Figure 6.90** below.

Figure 6.90 Prompt Information 3
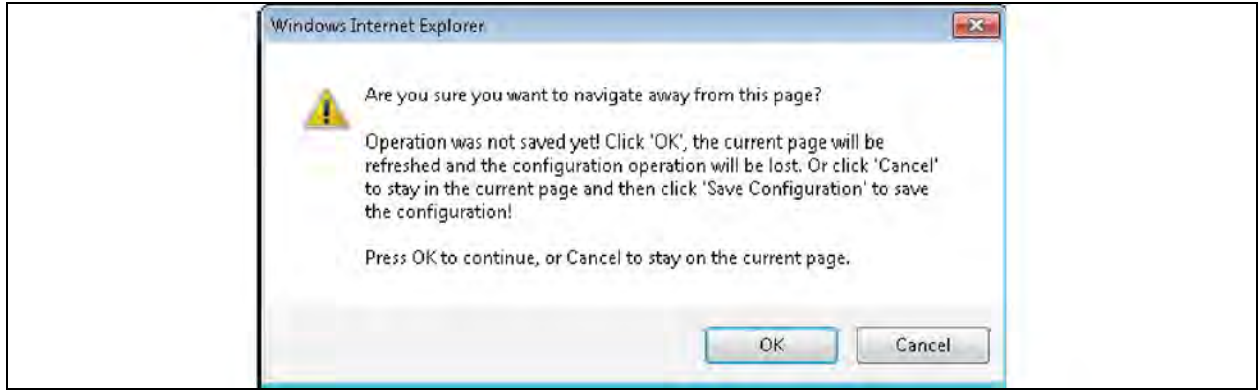
NOTE: Clicking the *Save Configuration* button can save all the operations at one time.

Install/Uninstall Device Type

Click the *Device Management* submenu under the Device Options menu, and then click the *Install/Uninstall Device Type* tab, the page shown in **Figure 6.91** on the facing page pops up.

Figure 6.91 Install/Uninstall Device Type
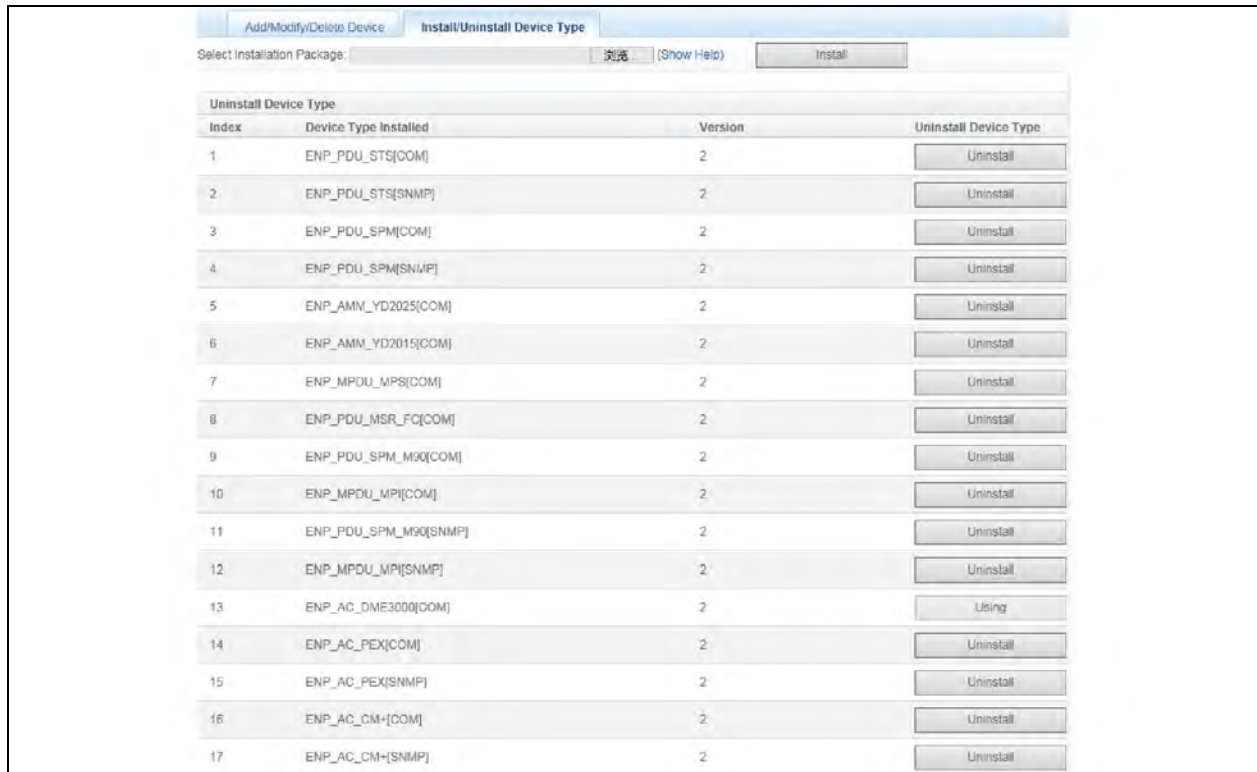
Click the *Browse* button to download configure package (file format of .iru) from local content, and click the *Install* button to install the new device type.

The device type number supported by the system is related to the system remaining memory and the size of driver configuration package, but the number cannot exceed 64.

NOTE: The page displays the installed device type information in the lower right part. Click the *Uninstall* button, the confirming dialog box pops up, as shown in Figure 6.91 above.

Figure 6.92 Confirming Dialog Box
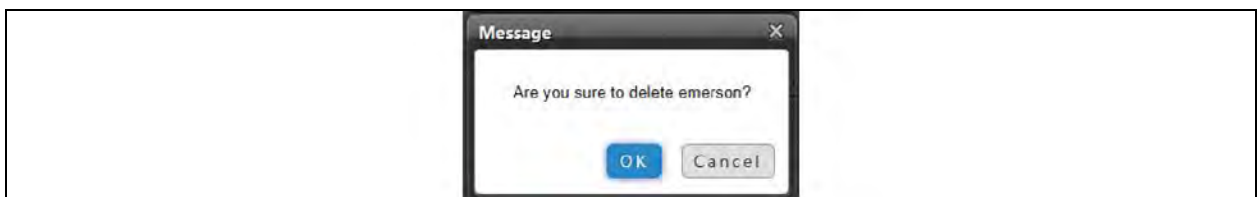
Click *OK*, the dialog box of Security authentication pops up, type the login password of current user, and click *OK* to uninstall the corresponding equipment type.

NOTE: While installing device type, if the device type exists and the device driver has a higher version than the driver to be added, it cannot be installed repeatedly.

NOTE: If the installation pack has no version information, or the version information does not match the software version, the device type cannot be installed.

NOTE: If some device uses the device type, the Uninstall button becomes gray, displaying Using, and the device type cannot be uninstalled.

Signal setting

Click the *Signal Setting* submenu under the Device Options menu, the page shown in **Figure 6.93** below pops up.

Figure 6.93 Modify Device Name
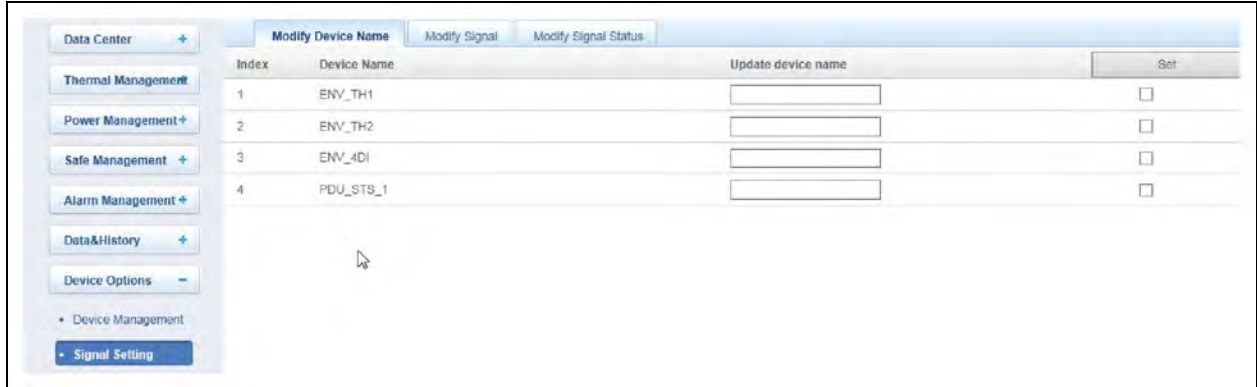
On the page shown in **Figure 6.93** above, you can modify the device name. Enter the new device name and click the *Set* button to make all setting effective.

NOTE: The characters of device name and signal name can be English letters, digits, space, and underline, other characters are invalid.

Click *Modify Signal*, the page shown in **Figure 6.94** below pops up.

Figure 6.94 Modify Signal
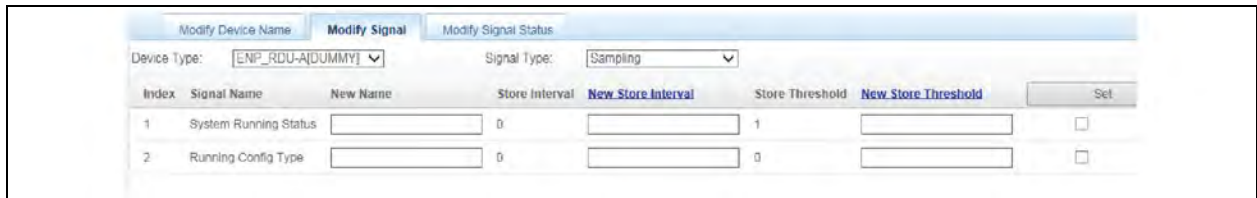
In the page as shown in **Figure 6.94** above, user can change the signal name, storage cycle of acquired signals, storage threshold of acquired signal and alarm level of alarm signals according to the device type. Select device type and Signal type, enter new signal information and click *Set* button to set in batches.

Click *New Store Interval* or *New Store Threshold* to modify all the store intervals of this device type or modify the store interval or store threshold of the acquired signal with non-zero store threshold.

NOTE: For Env TH and Env 4DI, the system has the linkage modifying function for the signal name, that is, when the sampling signal name is modified, the names of corresponding control signal, setting signal, and alarm signal will be modified as well. Therefore, the page only supplies the function of modifying sampling signal name.

NOTE: The signal name modified here will be used as default signal name of the device.

Click *Modify Signal Status*, the page shown in **Figure 6.95** on the facing page pops up.

   6 RDU-A G2

Figure 6.95 Modify Signal Status

In the page as shown in **Figure 6.95** above, user can change the signal status name according to the device type. Select device type, and all the status signals in this device type will be displayed on web page in list mode, select any signal and an edit frame will be displayed below the list, enter new status name, click *Modify* button to change the status name.

Click *New Store Interval* or *New Store Threshold* to modify the store intervals or store thresholds of all the acquired signals of this device type.

Batch configuration

Click the *Batch Configuration* submenu under the Device Options menu, the page shown in **Figure 6.96** below pops up.

Figure 6.96 Batch Configuration

On the page, you can perform Upload and Download operations to complete batch configuration.

NOTE: Only admin has the authority of batch configuration. If you fail in performing batch configuration, click *Show Help* to view the help information.

NOTE: The batch configuration file is encrypted after downloaded to local.

6.4.8 System Options

On the RDU-A G2 homepage, click the *System Options* menu in the left part, seven submenus appear, including: Monitoring Unit, Network Setting, User Management, Date/Time Setting, Restore System, Site Setting, License Management, System Upgrade and System Title.

Monitoring Unit

The Monitoring Unit submenu is used to set the signals of RDU-A G2 system, including Sampling, Setting and Alarm signals, the page is shown in **Figure 6.97** on the next page.

Figure 6.97 Monitoring Unit (Sampling)
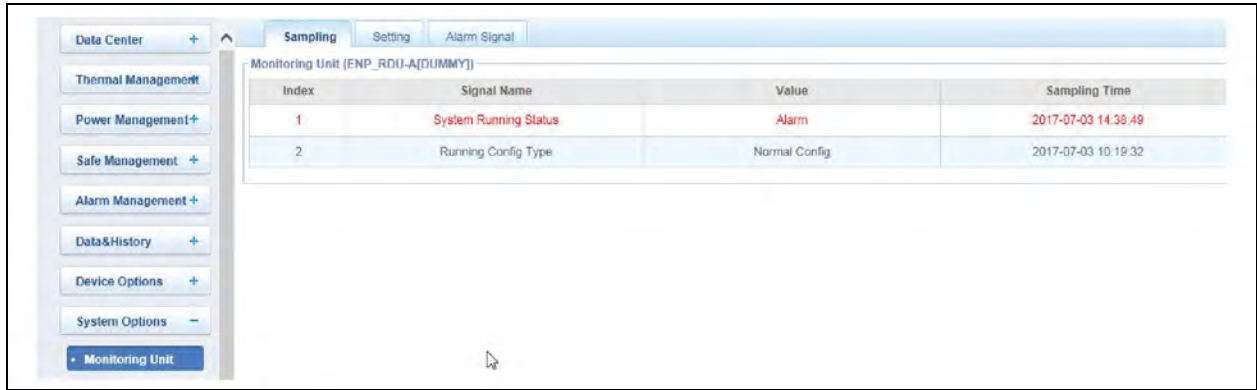
As for the operation method of the three tabs of Sampling, Setting, and Alarm on the Monitoring unit page, refer to Data Center on page 75.

NOTE: On the Setting tab, if you set Blocked for Outgoing Alarm Blocked, when an alarm occurs, it will be blocked, in this case:

NOTE: Among the current alarms, except Outgoing Alarms Blocked , other alarms will all end.

NOTE: The Blocked setting for Outgoing Alarm Blocked will be automatically cleared in 24 hours.

Network Setting

IP setting

Click the *Network Setting* submenu under the System Options menu, the page shown in **Figure 6.98** below pops up.

Figure 6.98 IP Setting
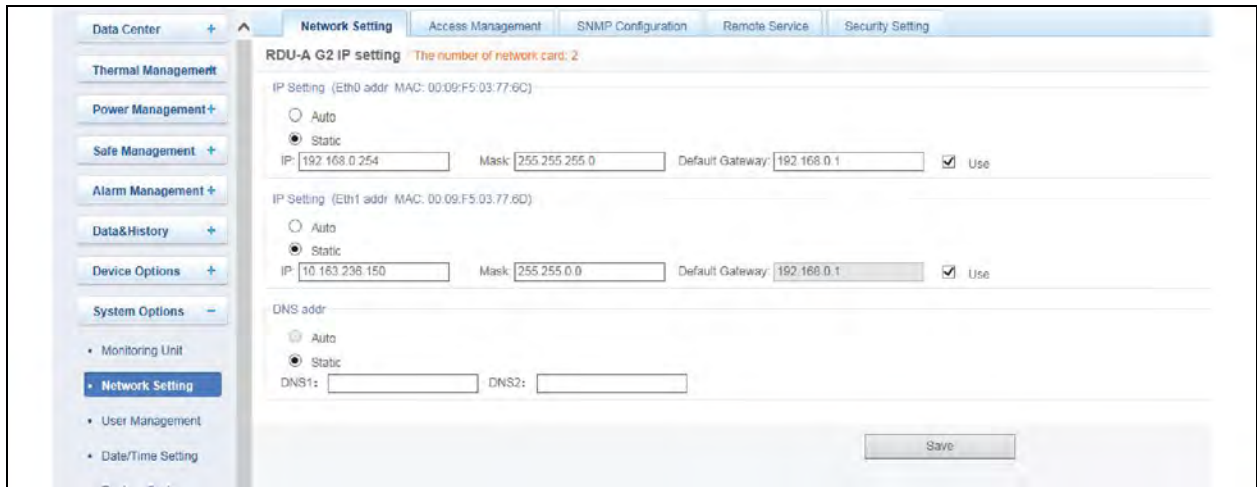
The RDU-A G2 supplies two IP setting methods: DHCP auto addressing and manual static addressing, meanwhile, it supports DNS.

On the page shown in **Figure 6.98** above, you can configure the network parameters, such as IP addressing mode, IP, Mask, Default Gateway, DNS1 (Preferred DNS server) and DNS2 (Alternate DNS server). After modifying the network parameters, click the *Save* button to make the setting effective.

NOTE: If network card 1 and network card 2 both use Static IP, the DNS address cannot be automatically obtained.

NOTE: After modifying the IP address, you must use the new IP address to re-login the RDU-A G2. The system will jump to the IP address of network card 1 by default.

Access management

Click the *Network Setting* submenu under the System Options menu, and then click the *Access Management* tab, the page shown in **Figure 6.99** below pops up.

Figure 6.99 Access Management

In the event of adding visitor, in the textbox of IP Address of RDU Manager, type the new IP address of the RDU manager, and click the *Add Visitor* button to finish the configuration.

NOTE: Up to three RDU manager IP addresses can be added in the system.

NOTE: In the event of adding visitor, if you select to use an agent, you also need to configure the agent server.

SNMP configuration

Click the *Network Setting* submenu under the System Options menu, and then click the *SNMP Configuration* tab, you can configure SNMP agent. The RDU-A G2 system supports V2 and V3 versions of SNMP agent.

As shown in **Figure 6.100** on the next page, the specific setting method of SNMP V2 is as follows:

     a.   Set NMS IP (host IP address of SNMP agent data receiving end).

     b.   Set Trap Level: Enable or disable .

     c.   Keep defaults for other items.

Figure 6.100 SNMP V2 Setting

As shown in **Figure 6.101** on the facing page, the specific setting method of SNMP V3 is as follows:

a. Set NMS IP (host IP address of SNMP agent data receiving end).

b. Set the Trap Level: Enable or disable.

c. Set the Name.

d. Set the User Type: Authenticated and Encrypted, Authenticated & Not Encrypted , Not Authenticated and Not Encrypted.

e. Select Authentication Protocol: MD5, SHA .

f. Select Privacy Protocol: DES .

g. Self-define Authentication Password and Privacy Password.

NOTE: On the base of SNMP V2, SNMP V3 adds user authentication and privacy strategies.

NOTE: If you select Not Authenticated and Not Encrypted for User Type, the drop-down boxes of Authentication Protocol and Privacy Protocol will become gray, so you cannot set them.

NOTE: Currently, only DES is supported for Privacy Protocol.

NOTE: You need to self-define Authentication Password and Privacy Password, which contain at least 8 characters, and be the same as the password set by the host of SNMP agent data receiving end, or it cannot be decrypted and received.

After parameter setting, click the *Add* button to add NMS.

If you need to modify NMS setting, select the NMS which needs to be modified, modify the setting and then click the *Modify* button to save the setting.

If you need to delete NMS, select the NMS which needs to be deleted, and then click the *Delete* button to delete the NMS.

Figure 6.101 SNMP V3 Setting

NOTE: The RDU-A G2 does not supply SNMP agent service by default. If you need SNMP service license, contact Vertiv customer service center for purchase, and the contact number is 4008876510.

Remote Service

Click the *Network Setting* submenu under the System Options menu, and then click the *Remote Service* tab, the page shown in **Figure 6.102** below pops up.

Figure 6.102 Remote Service Setting

The remote service setting includes three parts: Request RDU remote, Cancel RDU remote and Replace Host.

Request RDU remote: Used to establish remote service relationship

    a. Enter the self-defined customer name in the End-User textbox.

    b. Choose the contactor for remote service in the Contact Person textbox, when the contactor is chosen, the corresponding mobile and email will be displayed.

NOTE: The contactor for remote service must be set through System Options -> User Management in advance, and you must provide the mobile or email, or the service request cannot be conducted. Refer to User Management on page 130 for detailed setting method.

      c.   Choose Frequency of Reporting: Monthly, Seasonal.

      d.   Click *OK* to send the remote service request.

Cancel RDU remote: Used to cancel the established remote service.

Choose Cancel RDU remote and click *OK* to send a command to cancel the current remote service.

NOTE: Canceling the remote service is effective only under the precondition that the remote service has been established, otherwise, a prompt of failure will pop up after you click *OK*.

Replace Host: Used to replace the local host during remote service.

When the host that has established remote service need to quit, but you want to remain the established remote service relationship, you need to replace the local host to participate in the remote service. The detailed setting method is the save as Request RDU remote, besides, type the hardware serial number of the replaced host.

Security Setting

Only the administrator has rights to browse and configure the security setting.

In System Setting, choose Network Setting > Security Setting. A page is displayed, as shown in **Figure 6.103** below.

Figure 6.103 Security Setting
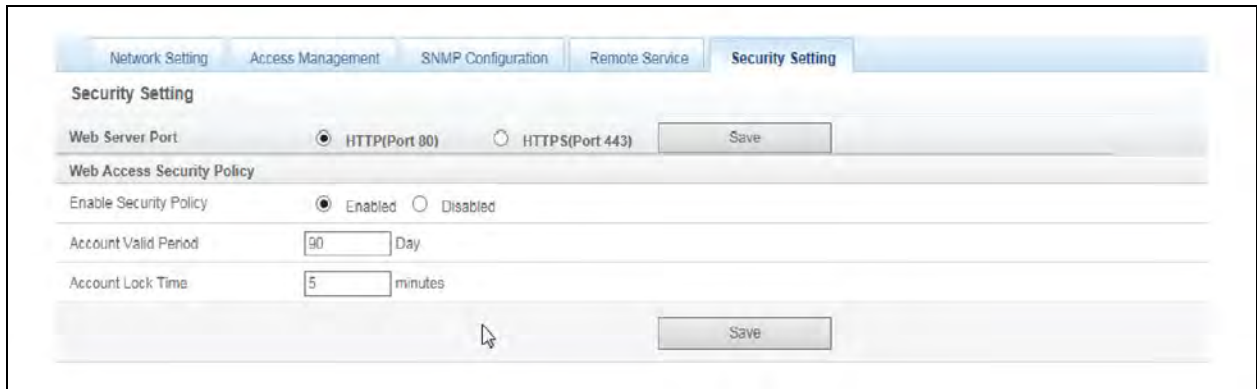
The security setting include Web Access Mode and Web Access Security Policy.

- Web Access Mode: Specifies whether the HTTP or HTTPS protocol is used to access the web pages. By default, the HTTP is used.

  After setting, click *Save*. The browser prompts you to wait for a while, as shown in **Figure 6.104** on the facing page.

Figure 6.104 Restarting the Web Server
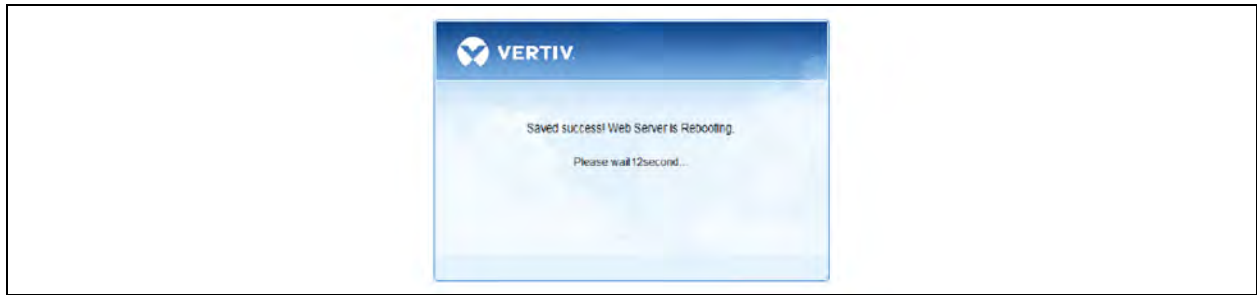
After the waiting period ends, the browser displays a new access hyperlink, as shown in **Figure 6.105** below. Click the hyperlink to access the user login page in web access mode.

Figure 6.105 Displaying a New Web Access Connection
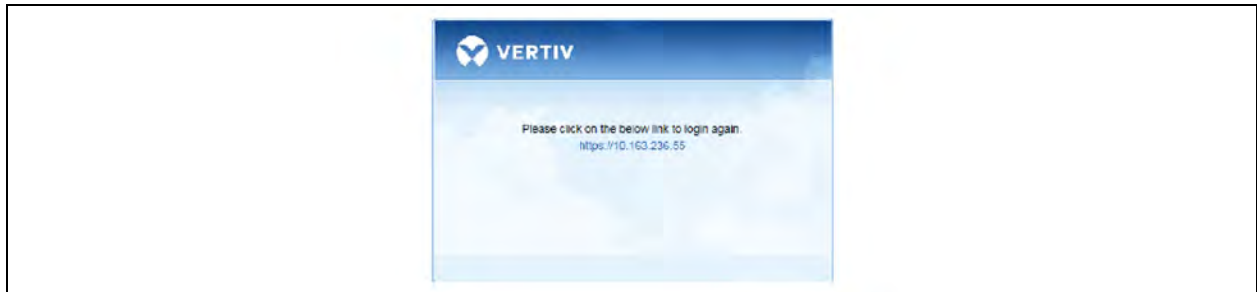
NOTE: You can connect the mobile APP to the RDU-A G2 only when the Web access mode is based on the HTTPS protocol.

- Web access security policy: Specifies whether the Web access security policy is enabled. By default, the Web access security policy is enabled.

    The Web access security policy includes account locking policy, login verification code, password complexity policy, and password expiration policy.

    a. Account locking policy:

    If a valid user continuously fails the login for five times, the user cannot enter the password to log in to the system. After the specified locking period ends, the user can try to log in again. The admin account will not be locked.

    The admin can reset the locked user account to unlock the user. For details, see Unlocking on page 133.

    The locking period can be configured in the Account Lock Time edit box. By default, the locking period is 5 min.

    b. Login verification code:

    If a user enters an incorrect user name or password, the system immediately displays a verification code and requests the user to enter it upon the next login, as shown in **Figure 6.106** on the next page.
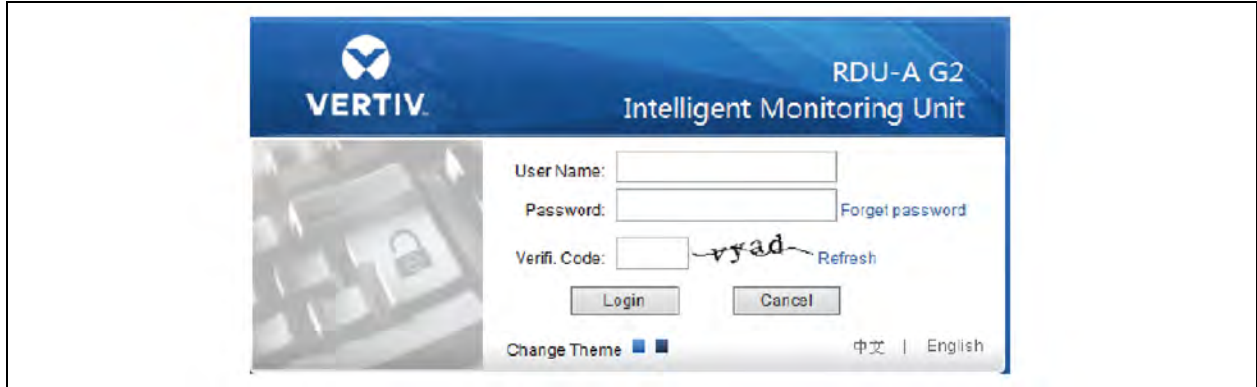
c. Password complexity:

The user password must contain at least 6 characters, including at least any two of the following types: upper-case letters (A-Z), lower-case letters (a-z), digits (0-9), and special characters (!, $, #, or %).

When the Web access security policy is enabled, the passwords of the existing user accounts are not affected. However, for new account creation or password modification, the new passwords must meet the complexity requirements.

d. Password expiration policy:

The password expiration policy indicates that a user password is valid within a specified period after the password is created or modified. The period of validity can be configured in the User Password Validity edit box. The period of validity ranges from 0 to 999. By default, the validity is 90 days. Value 0 indicates that the password is never expired.

This policy is valid to all accounts except for the admin. The password of the admin account is permanently valid.

The admin has the rights to update the period of validity of a user password. The updated password is valid from the moment of update and expires after the period of validity is reached. For details, see Update validity on page 133.

User Management

Click the *User Management* submenu under the System Options menu, the page shown in above pops up.

Figure 6.107 User Management
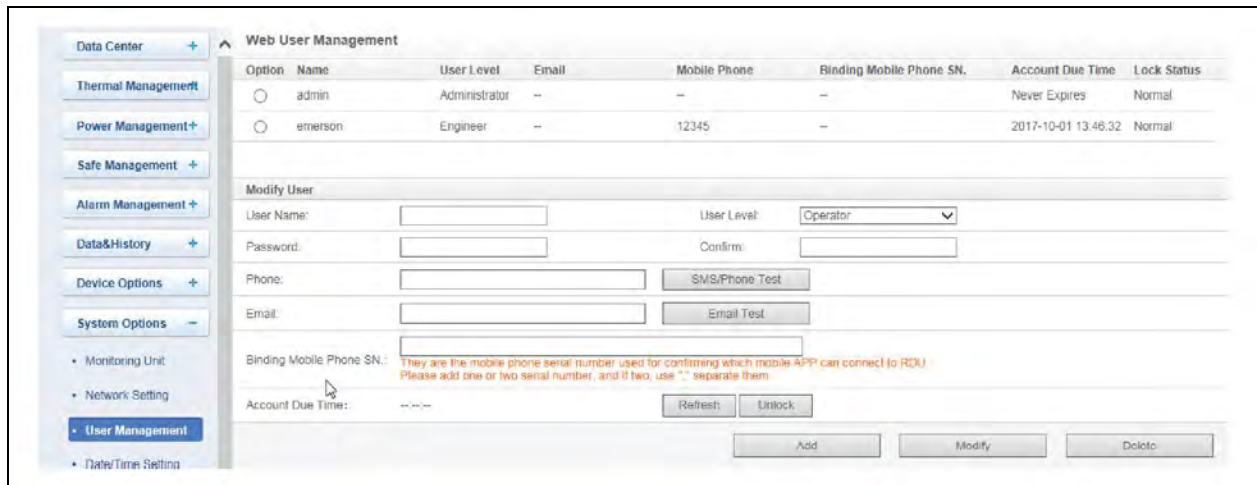
On the page shown in on the previous page, you can add user, modify user and delete user.

- Add user
    a. Enter User Name in the User Name textbox.
    b. Choose the user authority.
    c. Configure the user password, which cannot be vacant and should contain at least six letters or digits.
    d. Retype the password in the Confirm textbox.
    e. (Optional) Enter the user telephone number, which can use the following digits and characters: 0123456789, +.
    f. (Optional) Enter the email address.
    g. (Optional) Entering the SNs of mobile terminals that allow mobile apps to access the RDU-A G2.
    h. Click the *Add* button, the dialog box of Security authentication pops up. Enter the login password of current user, and click *OK* to add a new user.

NOTE: The characters of User Name can only be English letters, digits, -, and _. In addition, the initial characters must be letters.

NOTE: If the Web access security policy is enabled, more requirements are applied on passwords. For details, see Security Setting on page 128.

NOTE: Up to two SNs of bound mobile terminals can be entered, separated by ",".

NOTE: If no bound SN is entered, the system bounds the SNs of two mobile terminals over which the apps connect to the system first.

NOTE: After binding, the system allows only the bound mobile terminals to access the RDU-A G2 through the apps. To re-bind the SNs, you can modify or delete the bound SNs.

NOTE: The telephone number and email address cannot be void at the same time, and you can enter "--" if you do not need the telephone number and email address.

- Delete user
    a. Choose the user which needs to be deleted in the User Name list.
    b. Click the *Delete* button to pop up the confirming dialog box, as shown in **Figure 6.108** on the next page.

Figure 6.108 Confirming Dialog Box

c. Click *OK*, the dialog box of Security authentication pops up as shown **Figure 6.19** on page 74. Enter the login password of current user, and click *OK* to delete the chosen user.

NOTE: The user of admin cannot be deleted.

- Modify user

  a. Choose the user which needs to be modified in the User Name list.

  b. Modify the user information.

  c. Click the *Modify* button, the dialog box of Security authentication pops up, as shown in on page 130. Enter the login password of current user, and click *OK* to make the modified user information effective.

Users who access RDU-A G2 can be divided into four user groups, and they have different security level and user authority, see **Table 6.5** below for detailed information.

Table 6.5 User Security Level

Security level	User group	User authority
Level A	Administrator	The administrator can get full access: Send control command to intelligent equipment; Browsing, controlling and modifying parameters; Upload and download files; Modifying, adding and deleting user information; AC teamwork parameter setting; System upgrade; Modifying the account validity: releasing the locked user account.
Level B	Engineer	The engineers can get the following access: Send control command to intelligent equipment; Browsing, controlling and modifying parameters; Download files; Modifying user information of their own (Excluding the account validity and locked state).
Level C	Operator	The operators can send control command to intelligent equipment.
Level D	Browser	All users can browse equipment information.

On the page shown in on page 130, choose the current user, you can perform SMS/Phone Test and Email Test.

Before using the test function, users need to configure the SMS/Email server of current user, refer to Alarm Notification on page 100.

SMS/Phone test

Enter the phone number in the Phone field, and click the *SMS/Phone Test* button to test that the telephone number of current user can be gotten through. If users receive the test SMS and telephone, the test is successful, if not, the test fails, check that the telephone number is correct and the SMS Modem is properly connected.

Email alarm notify test

Enter the email address in the Email field, and click the *Email Test* button to test that the email address of current user is correct. If users receive the test email, the test is successful, if not, the test fails, check that the information above is correctly entered.

Update validity

If the Web access security policy is enabled, the page displays the password expiration time of the selected user account. The admin can click the *Update Validity* button to update the password validity. For details about the effective date of the updated validity, see Password expiration policy: on page 130 in Web Access Security Policy in section "Network Settings".

Unlocking

If the Web access security policy is enabled, the admin can click the *Unlock* button to unlock a user account. For details, see Account locking policy: on page 129 in Web Access Security Policy in section "Network Settings."

NOTE: When adding, modifying user, you must Enter the phone number or the email address, or the setting cannot be completed.

Date/Time Setting

Clicking the *Date/Time Setting* submenu under the System Options menu can synchronize the time. On the page shown in **Figure 6.109** below, RDU-A G2 can get time from the time servers automatically. Type IP address in the Primary server textbox and Secondary server textbox in sequence, type a figure in Interval to calibrate system time textbox, select the Time zone and Calibrating Protocol, and then click the *Set* button to make the setting effective.

Figure 6.109 Date/Time Setting

The RDU-A G2 can also get the local time. Choose Specify Date/Time, click the *Local Host Time* button to get the local time, and then click the *Set* button to make the new time effective.

NOTE: Time calibration adopts Specify Date/Time by default.

Restore System

Click the *Restore System* Submenu under the System Options menu, the page shown in **Figure 6.110** on the next page pops up.

Figure 6.110 Restore System
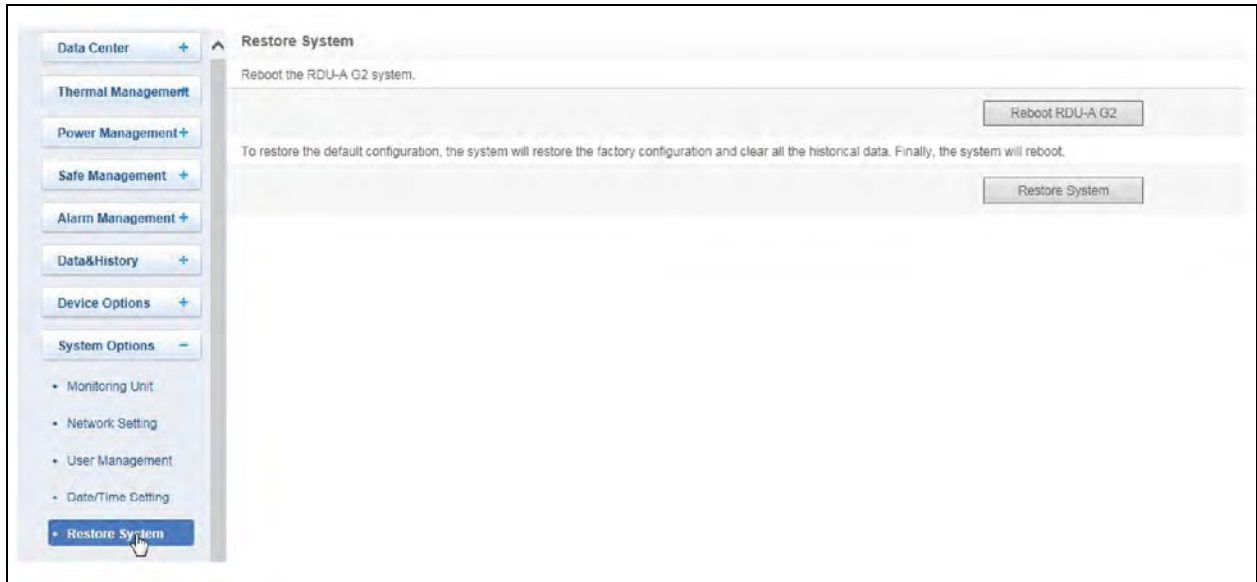
Click the *Reboot RDU-A G2* button to reboot the system.

Click the *Restore System* button to restore all the default settings.

NOTE: If you use the restore function, the RDU-A G2 may lose the original configuration solution. After the restore operation, make sure to wait 1 min for the RDU-A G2 conducting complete initializing work before re-accessing it through Web.

Site Setting

Click the *Site Setting* submenu under the System Options menu, the page shown in **Figure 6.111** below pops up.

Figure 6.111 Site Information Setting
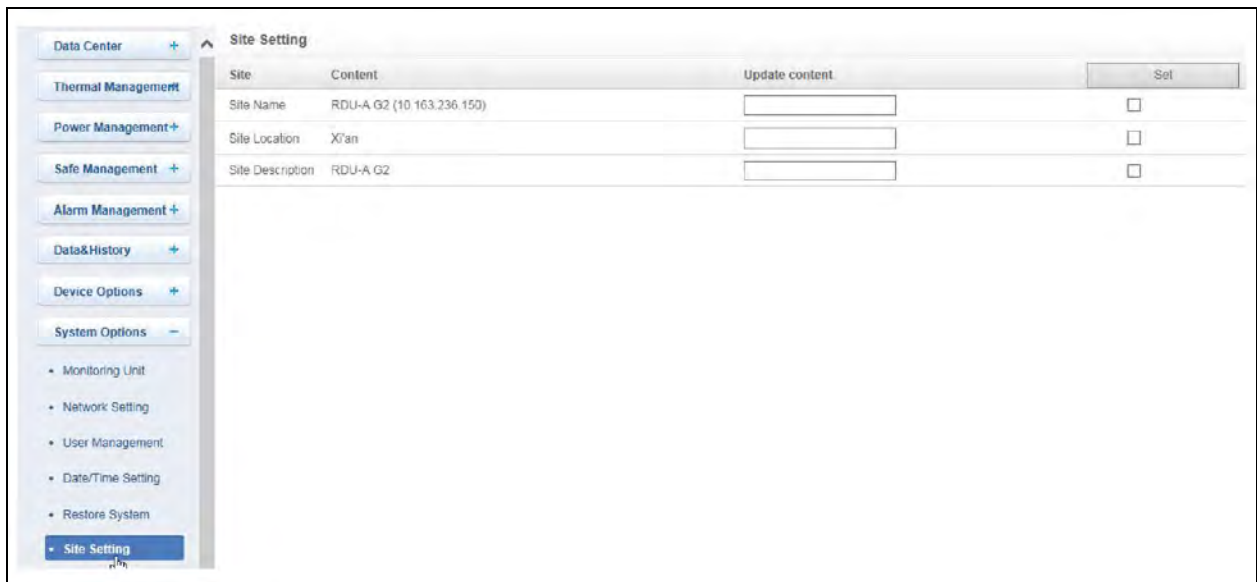
On the page shown in **Figure 6.111** on the previous page, you can modify the site information of RDU-A G2, including Site Name, Site Location, and Site Description.

License Management

Click the *License Management* submenu under the System Options menu, the page shown in above pops up.

Figure 6.112 License Management
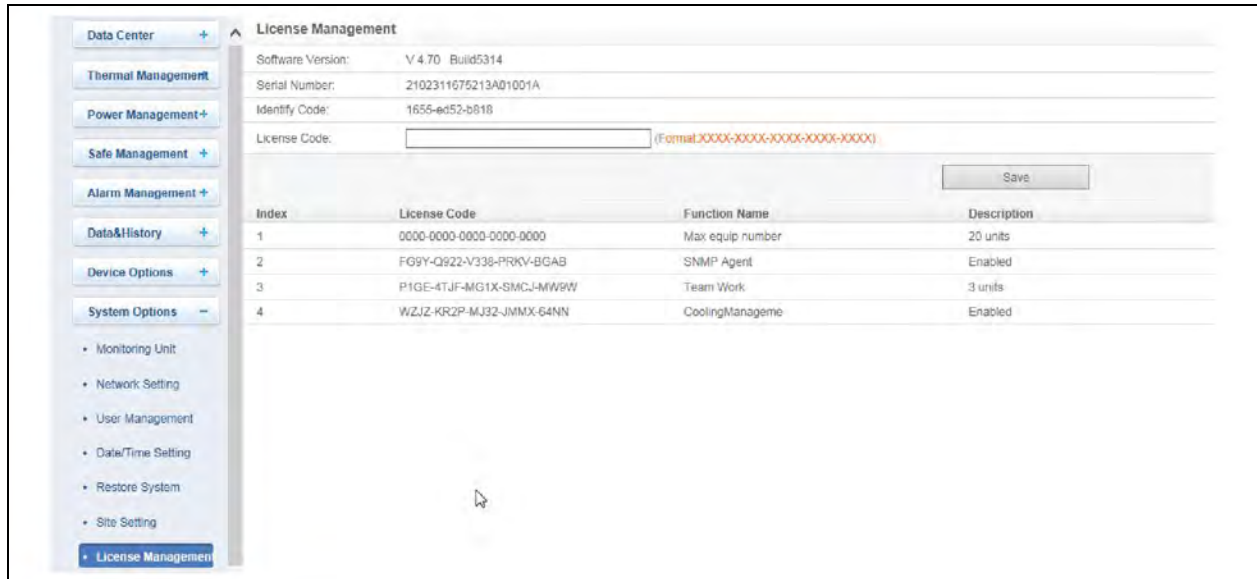
On the License Management page, you can conduct authorization of limited service (such as SNMP service) and view authorized functions. After you get the license code, input legal license code in the textbox, and click the *Save* button to finish installing. See **Table 6.6** below for the functions which can be authorized by the RDU-A G2.

Table 6.6 Overview of RDU-A G2 Authorized Functions

Authorized Functions	Descriptions
AC TeamWork	AC TeamWork authorized version and AC number participating in AC TeamWork, at most 32 ACs can be authorized to participating in AC TeamWork
SNMP service	SNMP agent service is open to user through authorization
Maximum connecting number	Maximum connecting number is expanded to 32 devices through authorization
SmartAisle Air Conditioner Teamwork Control	Authorize to enable SmartAisle Air Conditioner Teamwork Control, and disable the standard Air Conditioner Teamwork Control
Video Function	Authorize to support max 4 channels of IPC

NOTE: After installing license code of some function successfully, you must reboot the system for taking effect.

NOTE: After connecting the IRM4-COM expansion card, 4 will be added to the maximum connecting number.

System upgrade

Click the *System Upgrade* submenu under the System Options menu, the page shown in **Figure 6.113** on the next page pops up.

Figure 6.113 System Upgrade

On the page shown in **Figure 6.113** above, click the *Browse* button to download configure pack (.rdu file format) from the local catalogue, and then click the *Install* button to upgrade the system.

NOTE: The RDU-A G2 supports incremental upgrading function.

System title

Click the *System Title* submenu under the System Options menu, the page shown in **Figure 6.114** below pops up.

Figure 6.114 Title Setting
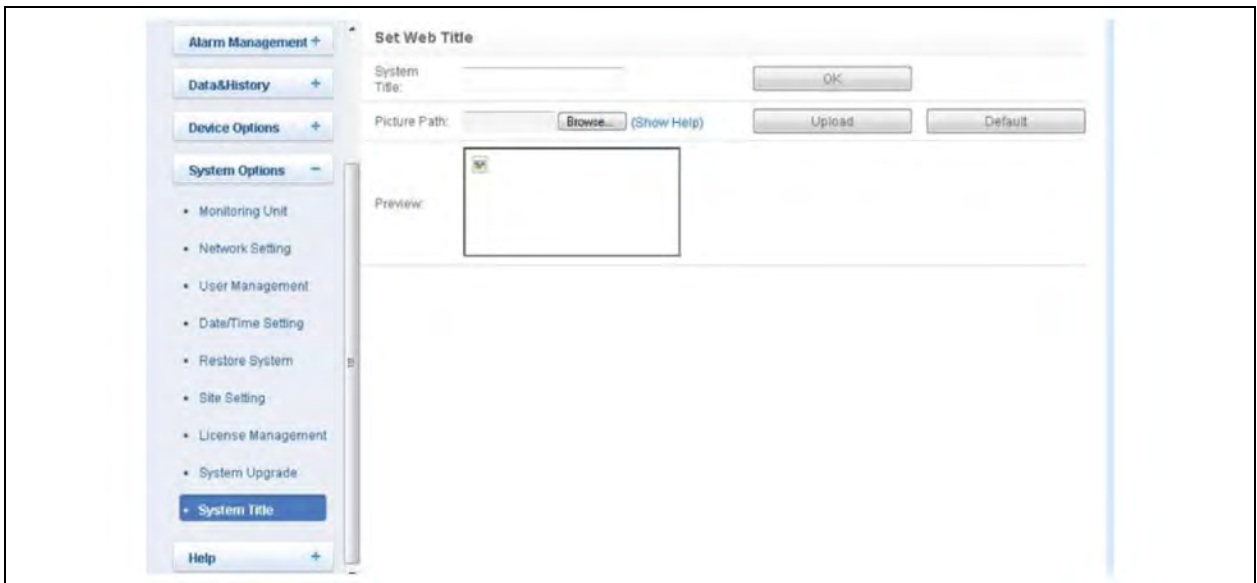
As shown in **Figure 6.114** on the previous page, you can replace the Logo picture in the upper right part by uploading system Logo picture. Click the *Browse* button, choose the needed Logo picture and click the *Upload* button to upload the file to RDU-A G2. Only [.gif], [.bmp], [.jpg] and [.png] format pictures are allowed, and the picture size should be less than 500K. Clicking the *Default* button can restore the default Logo picture.

You can also change the system title Welcome at the top of the page. Type the customized title in the System Title textbox and click *OK* to make it effective.

Help

On the RDU-A G2 homepage, click the *Help* menu in the left part, one submenu appears: About RDU-A G2.

The About RDU-A G2 page displays Software Version, Serial Number and Identify Code of RDU-A G2, and supplies download links for user manual and tools, as shown in **Figure 6.115** below.

Figure 6.115 About RDU-A G2

This page intentionally left blank

 6 RDU-A G2

7 Maintenance

This chapter explains the maintenance of Vertiv™ SmartCabinet™ including safety instructions, maintenance of the main components, disassembly, and troubleshooting.

7.1 Safety Instructions

⚠ **WARNING! Switch off the power input during the equipment maintenance. Switch off the equipment power unless the testing device needs power.**

⚠ **WARNING! Only authorized professional technicians are allowed to maintain the system.**

1. Follow the local laws especially about electric power, refrigeration and production for maintenance and operation. Follow the manufacturer's instructions during maintenance. If any Failure to observe this could result in invalidation of warranty. Pay close attention to the safety requirements to prevent any threats to the environment and personnel safety.
2. Use the components made by Vertiv to avoid performance decrease or equipment shutdown.

7.2 Maintenance of the Main Components

NOTE: Regular maintenance and inspection are necessary to ensure proper operation of the equipment.

7.2.1 RDU Monitoring Maintenance

Restoring Default Setting

Restoring default setting can be finished through two modes: software or hardware. For software restoring, refer to Restore System on page 134.

Hardware restoring includes restoring RDU-A G2 admin password (default User Name: **admin**, password: **vertiv**) and RDU-A G2 IP address (for default IP address, refer to Login RDU-A G2 on page 67 RDU-A G2 Host).

Follow the below steps for the hardware restoring:

    a. Press and hold the **reset** button, see **Figure 7.1** on the next page for four seconds, release your hand until the run/alarm indicator turns off.

    b. The IP address and password of the RDU-A G2 will be restored to factory defaults after the system restart.

Figure 7.1 Reset Button

Item	Description
1	Reset Button

FAQ

Q1: After RDU-A G2 is powered on, why the power indicator is not on?

A: Please check that the power cable is connected correctly.

Q2: How to deal if the POWER indicator is not on or the COM port does not work after the IRM-4COM\IRM-8DIAI\IRM-8DOAO expansion card is inserted?

A: If the POWER indicator is not on, please check that the expansion card is inserted correctly and completely; if it is inserted normally, the RDU-A G2 will restarts automatically, if the RDU-A G2 does not restart, please try to insert the expansion card again.

Q3: How to deal if the communication of COM port is abnormal?

A: Firstly, ensure that the device communication mode is matched. The COM ports on the RDU-A G2 and the expansion card are RS-232/RS-485 adaptive ports; secondly, please ensure that the communication parameters are correctly configured.

Q4: How to deal if the relay output port cannot control user equipment normally?

A: Check that the line sequences of user equipment terminals are correct, see Table 7.1 below.

Table 7.1 Line Sequence Definition of RDU-A G2 and Expansion Cards

RJ45	DO	DI/Smoke	Sensor	COM	DOAO Card	DIAI Card
1	12 V	12 V	12 V	RTS	0 to 10 V	12 V
2				NC		
3	Normally-closed	NC	12 V	TXD	normally-closed	AI_I
4	Disengaging detection	Disengaging detection	GND	GND	Disengaging detection	Disengaging detection
5	GND	GND			GND	GND

Table 7.1 Line Sequence Definition of RDU-A G2 and Expansion Cards (continued)

RJ45	DO	DI/Smoke	Sensor	COM	DOAO Card	DIAI Card
6	Normally-open	DI	NC	RXD	Normally-open	DI
7	COM		D+	D+	COM	
8	NC	NC	D-	D-	NC	AI_V
NOTE: The line sequence of RJ45 interface is 1 to 8 from left to right, with the gap downwards. The D+, D- are two kinds of levels of the RS485 differential signal. NC: Not Connected.						

Q5: How to deal if there is no access to RDU-A G2 login page when the RDU-A G2 communication is normal?

A: There are three measures to solve the problem:

Step 1: Ensure that the IP address is correct: the RDU-A G2 has two network cards, ensure that the network cable is connected to the correct port. If it is static addressing, refer to Network Port below of RDU-A G2 Host for default IP of RDU-A G2; if it is set to get IP in DHCP mode, view the current IP by referring to

Network Port

The RDU-A G2 host supplies two network ports which adopt 10/100M self-adaptable Ethernet ports. Its position is shown in **Figure 7.2** on the next page. See **Table 7.2** below for default configuration of the network ports.

Table 7.2 Default Configuration Parameters of the Network Ports

Network Card	IP Address	Subnet Mask	Default Gateway
Network Card 1 (eth0)	192.168.0.254	255.255.255.0	192.168.0.1
Network Card 1 (eth1)	192.168.1.254	255.255.255.0	192.168.0.1
NOTE: The login password of the Web browser will be restored to Vertiv.			

Figure 7.2 Appearance and Interfaces of RDU -AG2
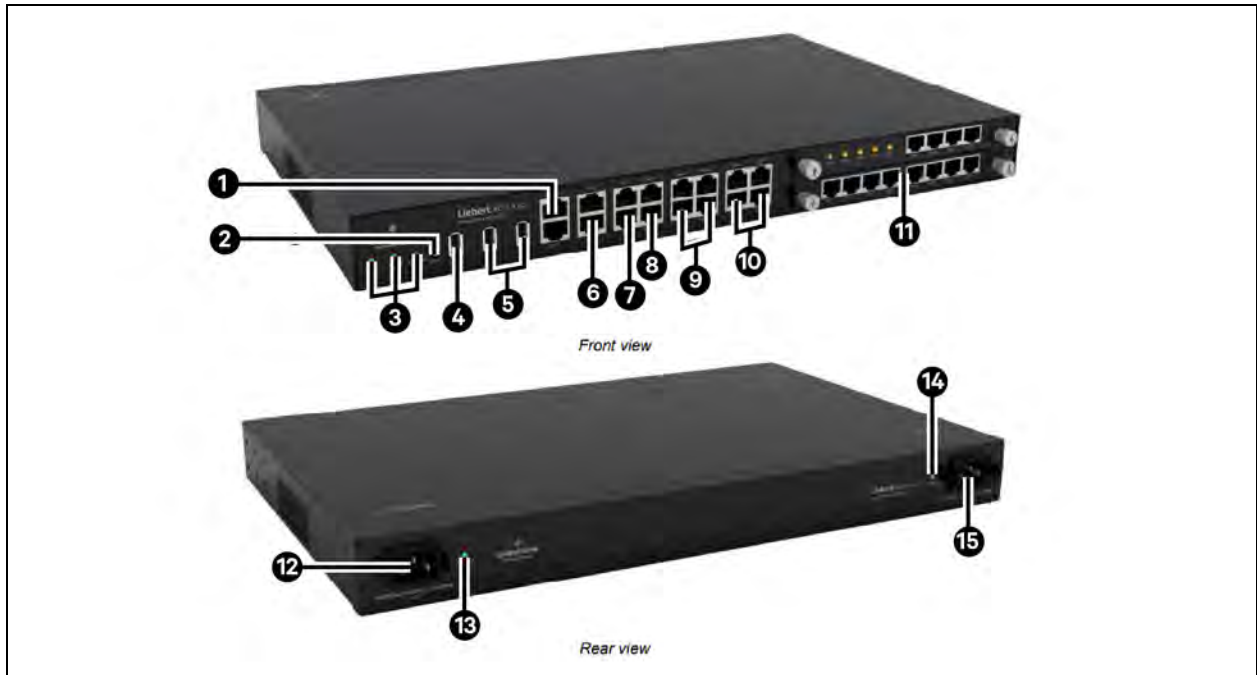
Item	Description	Item	Description
1	Network ports	9	Sensor ports
2	Reset button	10	COM ports
3	Indicators	11	Extension slots
4	Console port	12	Power input 1
5	USB Ports	13	Indicator
6	Relay output ports	14	Indicator
7	Digital input ports	15	Power input 2
8	Smoke		

Step 2: Ensure the connectivity of IP address: To ensure the connectivity of IP address, you can use PING/ping command, and the method is as follows.

To ensure the connectivity of IP address, you can use PING/ping command, and the method is as follows:

1. Click the ![icon] icon at the lower left corner, and type cmd in the ![textbox] textbox, as shown in **Figure 7.3** on the facing page.

Figure 7.3 Typing 'cmd'
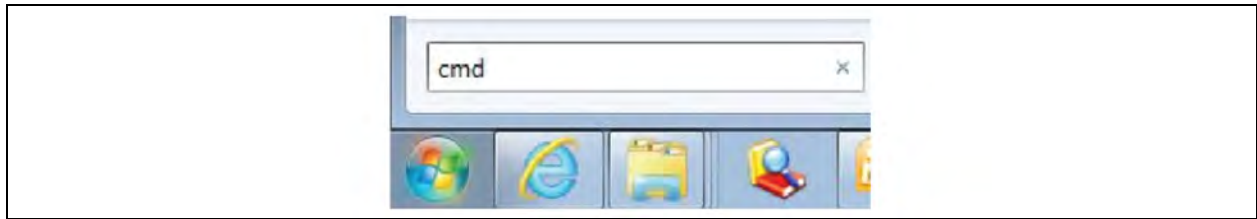
2. Press the **Enter** button key, the page shown in **Figure 7.4** below pops up. Type ping and IP address in the command line (for instance, ping 10.163.162.135) and check whether the communication is successful.

Figure 7.4 Communication Test
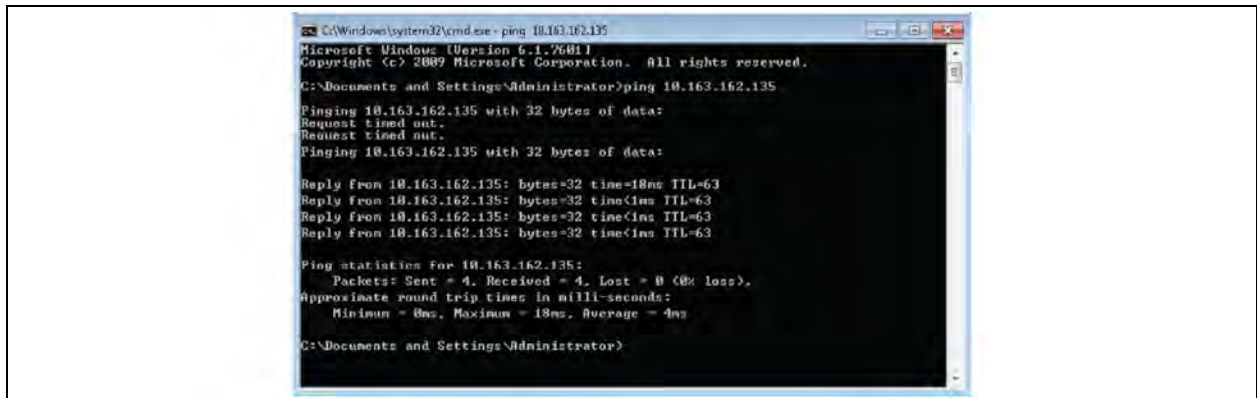
Step 3: If the above-mentioned steps cannot handle the problem, use the Reset button on the host to restore default IP.

Step 4: Refer to Login Preparation on page 63 to complete relevant operations.

Q6: After setting DHCP, how to view the current IP address?

A: After setting DHCP, you need to visit the RDU-A G2 through COM port to get the current IP address. The method is as follows:

Step1: Refer to Help below, download USB driver of console port and install it in the user computer.

Help

On the RDU-A G2 homepage, click the *Help* menu in the left part, one submenu appears: About RDU-A G2. The About RDU-A G2 page displays Software Version, Serial Number and Identify Code of RDU-A G2, and supplies download links for user manual and tools, as shown in **Figure 7.5** on the next page.

Figure 7.5 About RDU-A G2

Step2: Use the USB cable in the RDU-A G2 host package to connect the Console port on the RDU-A G2 to the computer USB port and use a COM port tool (such as Secure CRT) to connect the RDU-A G2.

Step3: Type username rduadmin and password vertiv to log in the RDU-A G2 system, type command setip1 and press the **Enter** key, to view the IP address, subnet mask, and gateway. The method of viewing network parameters of network card 2 is the same as that of network card 1, type command setip2, as shown in Figure 7.6 below.

Figure 7.6 Viewing Network Parameters

Q7: How to perform troubleshooting of sensor?

Fault 1: The intelligent sensor has no display, and it cannot be displayed on the RDU-A G2 webpage.

A: Please perform troubleshooting according to the following procedures:

1. Ensure that the intelligent sensor is connected to the SENSOR port of the RDU-A G2; meanwhile, the sensor whose address within the group is 1 can only be connected to SENSOR1; the sensor whose address within the group is 2 can only be connected to SENSOR2.
2. Check that the connected cable is intact and it is straight network cable, and the connector is intact.
3. Check that the intelligent sensor is normal.
4. Ensure that the sensor address is not 00.
5. If multiple intelligent sensors are connected, ensure that the sensor addresses are not the same, and perform troubleshooting according to procedures 2 and 3 one by one.

Fault 2: The alarm indicator of the intelligent sensor is on.

A: Send the intelligent sensor back to the service center of Vertiv local office for repair.

Fault 3: There are frequent communication failure alarms of intelligent sensors in the History Alarm of RDU-A G2.

A: Check that the network cable connector is intact, and that the network cable connection is not loosened.

Q8: You have chosen the ocean blue theme, but the page still adopts crystal blue theme while you are viewing the webpage of the RDU-A G2, how to deal with it?

A: Click the *[User] Logout* button to return the login page, click ▣ the icon to choose the ocean blue theme, and log in the system again.

Q9: After an alarm is generated, you do not receive any email or SMS notification; or when the alarm does not finish, the email or SMS notification is less than three times, how to deal with it?

A: Please perform troubleshooting according to the following procedures:

1. Please check that the SMS/Email server configuration is correct, refer to Alarm Notification on page 100.
2. If you do not receive the SMS notification, please check that the phone is out of service because of overdue payment.
3. If you do not receive the email notification, please click the menu *Data & History -> History Log* to query the system log and check whether there is a record of failure in sending email. If so, it indicates that the network is busy, or the email server communication is busy.

7.2.2 RDU Maintenance

1. Checks return air temperature on daily basis.
2. Avoid unauthorized entry in data center.
3. Always keep RCU unit air intake and outlet area without obstacles.
4. Check the physical verification of outdoor units on weekly basis.
5. Keep smart cabinet neat and clean with dust free environment.
6. Don't touch the setting parts of RCU display.
7. Don't switch off RCU unit until and unless required.
8. Don't touch IDU and ODU Cu piping.
9. Always keep front and back doors close of Racks.

7.2.3 UPS Power Distribution System Maintenance

Fan Maintenance

NOTE: Before the fan is completely stopped, do not insert your fingers or some tools into the fan so as to avoid device damage or personal injury.

The UPS fans are expected to run for 20000 hours to 40000 hours continuously. The higher the ambient temperature, the shorter the fan life is.

During the UPS operation, verify the fan status once every half year by confirming that air blows out from the ventilation holes on the rear panel.

Battery Maintenance

NOTE: Never reverse connect the battery, otherwise the fire will occur.

NOTE: Never open the battery to prevent physical injury because of the electrolyte. If you accidentally touch the electrolyte, wash the area immediately with plenty of clean water and go to hospital.

The internal battery module of the UPS is sealed, lead-acid and require less maintenance. The battery life depends on the ambient temperature, charge and discharge times. High ambient temperature and deep discharge shortens the battery life.

To ensure the battery life, it is required to:

1. Keep the ambient temperature ranging from 15 °C to 25 °C.
2. Prevent small current discharge. Continuous battery operation time exceeding 24 hours is strictly prohibited.
3. Charge the battery for at least 12 hours, if the battery does not been charged for three months at specified ambient temperature, or two months at high ambient temperature.

NOTE: Check regularly the screws at the battery connection parts, fasten it immediately if not tight.

NOTE: Make sure that the safety equipment are complete and that the function is normal, especially that the settings of the battery management parameters are normal.

NOTE: Measure and record the internal temperature of the battery room.

NOTE: Check whether the battery ports are damaged or hot, and whether the chassis and the covers are damaged.

If liquid leakage and damage to the battery are found, place the battery in the anti-vitriol tank, and deal with it according to the local regulations.

The waste lead acid battery is dangerous waste material. Controlling the pollution from used batteries is one of the national priorities. Its storage, transportation, usage, and disposal must follow the national and local law and other criteria about the dangerous waste material and the waste battery pollution prevention.

According to the related regulations, recycle the waste lead-acid battery, and other disposal methods are prohibited. Throwing away randomly the waste lead-acid battery and other improper disposal methods can result in serious environment pollution, which will be investigated the legal responsibility.

As the provider of the lead-acid battery, Vertiv has built perfect service network and recycle system for the waste battery to assist users to deal with the waste battery by law. Contact Vertiv or the nearest service center for the detailed information of the recycle system about the waste battery.

Vertiv is not liable for the environment results caused by failure to comply with the notices in this section or to use the waste battery recycle system provided by Vertiv.

Cleaning UPS

Clean the UPS periodically, especially the ventilation holes, to ensure free airflow inside the UPS. If necessary, clean the UPS with a vacuum cleaner. Verify that the ventilation openings are unblocked.

Checking UPS State

It is recommended to check the UPS operation status once every half year. Check the following items:

1. Check if the UPS is faulty, Check whether the alarm indicator on working properly
2. Check if the UPS is operating in Bypass mode. Normally, the UPS operates in Normal mode. If it is operating in Bypass mode, you should find out the reason, such as operator intervention, overload, internal fault, and so on.
3. Check if the battery is discharging, when AC mains is normal, the battery should not discharge; if the UPS operates in Battery mode, you should find out the reason, such as mains failure, battery test, operator intervention, and so on.

Checking UPS Functions

NOTE: UPS functions check procedures may cause power interruption to load.

It is recommended to check the UPS functions once every half year.

Backup the load data before conducting the UPS functions check. Procedures are as follows:

1. Press the **power** button to check if the buzzer beeps, indicators are on and the LCD display is normal.
2. Press the **ESC** key to check again if the indicators are on, the LCD display is normal, and the UPS has been transferred to the inverter mode.

RCU Maintenance

1. **Filter**- In RCU a replaceable and washable evaporator air filter is supplied with the unit. The filter is easily serviceable from the backside. Filters are usually the most neglected item in an environmental control system. To maintain efficient operation, they should be checked monthly and changed as required.
2. **Blower package**- Periodic checks of the blower package include blower wheels, motor and motor mounting bracket. With the power off, inspect and remove any debris removed from the wheels and housings. Also check to see that they are tightly mounted and rotate freely without rubbing against the housing.
3. **Refrigeration system**- Each month the components of the refrigeration system should be inspected for proper function and signs of wear. Since in most cases evidence of malfunction is present prior to component failure, periodic inspections can be a major factor in the prevention of most system failures.
4. **Refrigerant Lines**- Check all refrigerant lines and capillaries for vibration isolation, and support as necessary. Visually inspect all refrigerant lines for leaks.
5. **Thermostatic Expansion Valve**- The thermostatic expansion valve (TEV) keeps the evaporator supplied with enough refrigerants to satisfy load conditions. It does not turn the compressor on or off, but correct valve adjustment is necessary for proper system operation. Determine TEV operation by measuring superheat (see Superheat below). The superheat will be high if the evaporator is receiving too little refrigerant and low if it is receiving too much refrigerant.

Superheat

To determine superheat:

1. Measure the temperature of the suction line at the point where the TEV bulb is clamped.
2. Obtain the gauge pressure at the compressor suction valve.
3. Add the estimated pressure drop between bulb location and the suction valve.
4. Convert the sum of the two pressures to the saturated temperature.
5. Subtract this temperature from the actual suction line temperature, the difference is superheat.

Air-cooled Condenser

Restricted airflow through the condenser coil will reduce the operating efficiency of the unit and can result in high compressor head pressure and loss of cooling.

To avoid this follow the below steps:

1. Clean the condenser coil each time the evaporator filters are replaced.
2. Check for bent or damaged coil fins and repair as needed.
3. Check all refrigerant lines for leaks.

4. Clean the condenser coil of all debris that will inhibit airflow. This can be done with compressed air or commercial coil cleaner.

5. For access to the coil, first remove the top panel by rotating fasteners.

6. Remove the condenser grille by pulling it up and forward.

7. Remove the side panels by removing screws, and then pull panel down and forward.

8. Removing all these components it can possible to inspection and cleaning of the coil. Replace all panels in reverse order.

Compressor Replacement

In the properly installed system burnouts rearly occurs but a frequently fault in the motor insulation may result in a motor burn. Of those that do,most are the effects of mechanical or lubrication failures, resulting in the burnout as a secondary consequence.

If problems that can cause compressor failures are detected and corrected early, a large percentage can be prevented. Periodic maintenance inspections by alert service personnel on the lookout for abnormal operation can be a major factor in, reducing maintenance costs. It is easier and far less costly to take the steps necessary to ensure proper system operation than it is to allow a compressor to fail and require replacement.

When troubleshooting a compressor, check all electrical components for proper operation as below:

1. Check all fuses and circuit breakers.

2. Check hi-low pressure switch operation.

3. If a compressor failure has occurred, determine whether it is an electrical or mechanical failure.

Mechanical Failure

A mechanical compressor failure will be indicated by no burned odour. The motor will attempt to run. If you have determined that a mechanical failure has occurred, the compressor must be replaced.

Electrical Failure

An electrical failure will be indicated by a distinct pungent odor. If a severe burnout has occurred, the oil will be black and acidic. In the event that there is an electrical failure and a complete burnout of the refrigeration compressor motors the proper procedures must be performed in order to clean the system to remove any acids that would cause a future failure.

⚠️ **CAUTION: Damage to a replacement compressor caused by improper system cleaning constitutes abuse under the terms of the warranty, and the warranty will be voided.**

⚠️ **CAUTION: Avoid skin contact with the gas and oils. Severe burns will result. Use long rubber gloves when handling contaminated parts.**

Compressor Replacement

Replacement compressors are available from your nearest Vertiv Energy (India) Private Limited office. They will be shipped in a crate to the job site by franchisee.

1. Disconnect power.

2. Attach suction and discharge gauges to access fittings.

3. Recover refrigerant, using standard recovery procedures and equipment. Use a filter drier when charging the system with recovered refrigerant.

4. Remove pressure switch capillaries and disconnect all electrical connections.

5. Remove failed compressor.

6. Install replacement compressor and make all connections.

7. Pressurize and leak test the system at approximately 350 PSIG pressure.

8. Follow manufacturer's instructions for cleanout kits.

9. Connect a vacuum pump to both the high and low sides of the system through properly sized connections. Evacuate the system twice. Break the vacuum each time with R-22 Refrigerant gas.

10. Charge the system with refrigerant.

Fire Fighting

1. Identify the fire/fault exact location from the panel display.

2. In case of the false alarm press the **reset** button to reset the panel.

3. In case of emergency/genuine fire press **manual call point** switch.

4. Evacuate the room immediately.

5. In case of power failure check the power socket.

6. Allow only trained person to operate the panel.

7. Do not keep the rack door open in case of fire.

8. Do not enter the room in case of fire.

9. Do not press the **manual abort** switch in case of fire.

10. Do not open the rack door until 30 min after gas released.

7.3 Disassembly

Vertiv™ SmartCabinet™ has substances and components (electronic elements) harmful to the environment. Only professional technicians are allowed to disassemble SmartCabinet™ after the product life is ended. SmartCabinet™ must be sent to a special harmful substance handling center.

This page intentionally left blank

8 Troubleshooting

Below are the details of some common issues faced at sites. For corrective action it is recommended to contact Vertiv service representative.

Table 8.1 Troubleshooting for Vertiv™ SmartCabinet™

Fault Condition	Possible Cause	Check or Remedy
Unit not cooling properly	1. Clogged Filter 2. Condenser coil gets clogged 3. High condenser pressure 4. Low fan speed 5. Lower compressor performance 6. Gas leak/gas undercharged. LP get tripped	1. Clean filter. 2. Clean condenser coil. 3. Purge, evacuate, and recharge the refrigerant system as per specified refrigerant qty. 4. Fan connection/performance check. If required replace it. 5. Compressor connection/performance check. If required replace it. 6. Find the leak, correct it and charge refrigerant as per specific quantity.
Noisy unit	1. Loose parts of mountings 2. Refrigerant tubing rattling 3. Fan blades deform 4. Noisy compressor 5. Noisy fan	1. Locate the defect and tighten it. 2. Harness the tubing to avoid the contacts. 3. Replace the fan. 4. Find the cause and if required replace it. 5. Find the cause and if required replace it.
Compressor not starting/tripping	1. Electrical connection wrong 2. Control contacts open 3. Compressor motor defective 4. High pressure trip/low pressure trip	1. Correct the wiring as per wiring diagram. 2. Check the contacts and correct the connection. 3. Check and replace the compressor. 4. Find the possible cause to connect the situation. In case of HP, clogged condenser, air flow low of condenser fan. In case of LP, lower refrigerant charge.
Compressor sweating	1. High refrigerant 2. Lower expansion	1. Purge the refrigerant to correct weight or till you get specified head pressures. 2. Check for correct use of expansion device. If required replace.

Table 8.2 Troubleshooting for RDU-A G2

Fault Condition		Check or Remedy
After RDU-A G2 is powered on, the power indicator is not turning on.		Check that the power cable is connected correctly.
The POWER indicator is not on or the COM port does not work after the IRM-4COM\IRM-8DIAI\IRM-8DOAO expansion card is inserted.		If the POWER indicator is not on, check that the expansion card is inserted correctly and completely; if it is inserted normally, the RDU-A G2 will restarts automatically, if the RDU-A G2 does not restart, try to insert the expansion card again.
The communication of COM port is abnormal.		Firstly, ensure that the device communication mode is matched. The COM ports on the RDU-A G2 and the expansion card are RS-232/RS-485 adaptive ports; secondly, ensure that the communication parameters are correctly configured.
Troubleshooting of sensor	The intelligent sensor has n display, and it cannot be displayed on the RDU-A G2 webpage.	1. Ensure that the intelligent sensor is connected to the SENSOR port of the RDU-A G2; meanwhile, the sensor whose address within the group is 1 an only be connected to SENSOR1; the sensor whose address within the group is 2 can only be connected to SENSOR2. 2. Check that the connected cable is intact and it is straight network cable, and the connector is intact. 3. Check that the intelligent sensor is normal. 4. Ensure that the sensor address is not 00. 5. If multiple intelligent sensors are connected, ensure that the sensor addresses are not the same, and perform troubleshooting according to procedures 2 and 3 one by one.
	The alarm indicator of the intelligent sensor is on.	Send the intelligent sensor back to the service center of Vertiv local office for repair.
	There are frequent communication failure alarms of intelligent sensors in the History Alarm of RDU-A G2.	Check that the network cable connector is intact, and that the network cable connection is not loosened.
While accessing the RDU-A G2's website, you have selected the ocean blue theme, yet the page still uses the crystal blue theme.		Click the *[User] Logout* button to return the login page, click the icon to choose the ocean blue theme, and log in the system again.
After an alarm is generated, you do not receive any email or SMS notification; or when the alarm does not finish, the email or SMS notification is less than three times		1. Check that the SMS/Email server configuration is correct, refer to Alarm Notification on page 1. 2. If you do not receive the SMS notification, check that the phone is out of service because of overdue payment. 3. If you do not receive the email notification, click the *menu Data & History -> History Log* to query the system log and check whether there is a record of failure in sending email. If so, it indicates that the network is busy, or the email server communication is busy.

Appendices

Appendix A: Technical Support and Contacts

A.1 Technical Support/Service in the United States

Vertiv Group Corporation

24x7 dispatch of technicians for all products.

1-800-543-2378

Liebert® Thermal Management Products

1-800-543-2378

Liebert® Channel Products

1-800-222-5877

Liebert® AC and DC Power Products

1-800-543-2378

A.2 Locations

United States

Vertiv Headquarters

505 N Cleveland Ave

Westerville, OH 43082

Europe

Via Leonardo Da Vinci 8 Zona Industriale Tognana

35028 Piove Di Sacco (PD) Italy

Asia

7/F, Dah Sing Financial Centre

3108 Gloucester Road, Wanchai

Hong Kong

This page intentionally left blank

Connect with Vertiv on Social Media

https://www.facebook.com/vertiv/

https://www.instagram.com/vertiv/

https://www.linkedin.com/company/vertiv/

https://www.twitter.com/Vertiv/

VERTIV