Liebert® IntelliSlot™ RDU-SIC G2 Card

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 Product Description

The Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card is a network management card. It can make the intelligent equipment (such as UPS, PDU, air conditioner, and so on) developed by Vertiv have the capacity for network communication. The Liebert® IntelliSlot™ RDU-SIC G2 Card can also connect to the environment monitoring equipment, including IRM series temperature & humidity sensor or dry contact signal input & detecting sensors. In the case of an equipment alarm, it notifies the user by multiple ways: recording, sending a trap message, sending an E-Mail or sending an SMS.

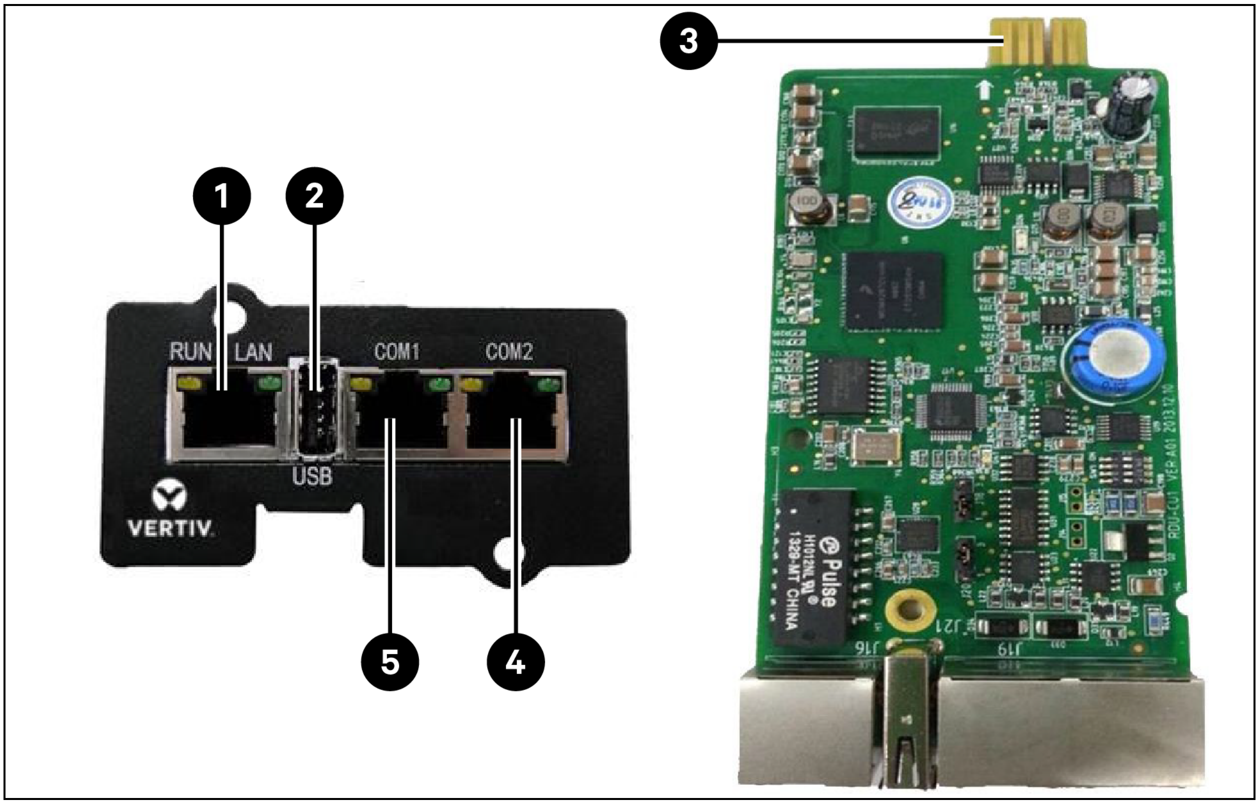
The Liebert® IntelliSlot™ RDU-SIC G2 Card can meet the requirements of TCP/IP and RS232/485 networking modes and can be flexibly configured according to various application conditions.

This chapter expounds the components description, main functions, and technical specifications.

1.1 Components Description

The appearance and ports of the Liebert® IntelliSlot™ RDU-SIC G2 Card are shown in Figure 1.1 below .

Figure 1.1 Appearance and Ports of RDU-SIC G2 Card



Item	Description
1	Ethernet port: • RDU-M • SMTP • NSM management system • Web browser
2	USB port: • Connecting USB modem • Equipment console port
3	RS485/RS232 port: • PDU • Air conditioner • UPS
4	RS485 port: • PDU • Air conditioner • UPS • IRM sensor
5	RS485 port: • PDU • Air conditioner • UPS

Console Port

The Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card supplies a console port (USB port, see **Figure 1.1** on the previous page for its position), which adopts USB communication mode. Short pin 2 and pin 3 of jumper J20. The communication parameters are given in **Table 1.1** below .

Table 1.1 Communication Parameters of Console Port

Parameter	Baud Rate	Bit	Parity	Stop Bit
Value	115200bps	8 bits	None	1 bit

USB Port

The Liebert® IntelliSlot™ RDU-SIC G2 Card supplies one USB A type socket port for connecting USB Modem of designated model. Short pin 1 and pin 2 of jumper J20. It's position is shown in **Figure 1.1** on the previous page .

Network Port

The Liebert® IntelliSlot™ RDU-SIC G2 Card provides one network port which adopts 10/100M Base T self-adaptable ethernet port. It's position is shown in **Figure 1.1** on the previous page . See **Table 1.2** below for default configuration of the network port.

Table 1.2 Default Configuration Parameters of the Network Port

Network Card / Parameter	IP Address	Subnet Mask	Default Gateway
Default parameter	192.168.0.252	255.255.255.0	192.168.0.1

COM Port

The Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card supplies three independent COM ports. Their positions are shown in **Figure 1.1** on page 1 .

The port adopts RS-485 communication mode and the gold finger adopts RS-485/232C (adaptive) communication mode.See **Table 1.3** below for the communication parameters.

Table 1.3 Communication Parameters of COM Port

Parameter	Baud Rate	Bit	Parity	Stop Bit
Value	1200bps, 2400bps, 4800bps, 9600bps, 19200bps (optional)	5 ~ 8 bits	Even/Odd/None/Mark/Space	1 ~ 2 bits
NOTE: The combination mode of 5-bit word size and 2-bit stop bit is not supported.				

1.2 Main Functions

The main functions of RDU-SIC G2 Card are listed in **Table 1.4** below .

Table 1.4 Main Functions

Main function	Descriptions	
Device monitoring	Realizing camera viewing in the data center; getting and handling the data of different intelligent devices and controlling them through Web interface.	
Safe shutdown	Shutdown schedule	Configure the maintenance policy of the UPS and can periodically reboot or close the supervised UPS.
	Sever shutdown	Used together with the network shutdown software. When the UPS has certain critical alarm, the system will notify the server shutdown to avoid the sever going down.
Alarm Management	Current alarm	Displaying alarm in real time and confirming the current alarm.
	History alarm	Querying the history alarm.
	Alarm notification	1. Can be customizable according to user requirements. It means that the alarm notification content can be customized. 2. Can choose the communication mode to receive alarm information of different levels from different equipment. 3. The communication mode includes Email, SMS, and phone. 4. Email supports SSL function. 5. Supplying alarm test function to test whether or not users have received the alarm notification information. 6. Sending the system running status periodically according to user configuration.
Data and History	Device information	Providing the main data of equipment.
	History data	Querying the history data.
	History log	Querying the log data.
	Clear history	Clearing the history data and log data.
Device Options	Device management	1. Can add, modify and delete equipment actively, and support adding four pieces of intelligent equipment at most.

Table 1.4 Main Functions (continued)

Main function	Descriptions	
		2. Can install and uninstall equipment type and support connecting the third party equipment. **NOTE: The default installed equipment cannot be deleted and modified.**
	Signal setting	Modifying equipment name and alarm level online.
	Batch configuration	Updating and downloading configuration files and system files.
System Options	Monitoring unit	Collecting the system information of Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card.
	Network setting	1. Setting the network information such as IP, subnet mask, gateway, and DNS. 2. Controlling whether the upper monitoring system (RDU-M manager) can visit the RDU-SIC G2 Card. 3. Remote service setting.
	User management	Adding, modifying, and deleting user information.
	Date/time setting	Calibrating the real time clock of RDU-SIC G2 Card.
	Restore system	Rebooting the RDU-SIC G2 Card and restoring default configuration.
	Site setting	Modifying site information online.
System Options	System upgrade	Upgrading the application program online.
	System title	Setting title and logo picture at the top of the web page.
Help	About RDU-SIC G2 Card	Displaying serial number, identify code and software version, and supplying links for downloading user manual and tool software.

1.3 Technical Specifications

1.3.1 Environment specifications

See Table 1.5 below for the environment specifications of RDU-SIC G2 Card.

Table 1.5 Environment Conditions

Item	Requirement
Application location	Usually in the data center or computer room, with air conditioner
Working temperature	-10°C (14°F) to +60°C (140°F)
Relative humidity	5%RH to 95%RH, no condensing
Working environment	Dust: compliant with the indoor requirements of GR-63. No corrosive gas, flammable gas, oily mist, steam, water drops, or salt
Air pressure	70kpa to 106kpa
Storage temperature	40°C (104°F) to +70°C (158°F)
Cooling	Natural cooling
Power distribution network	TT/TN
Protection level	IP20

1.3.2 Performance specifications

See Table 1.6 below for the performance specifications of Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card.

Table 1.6 Performance Specifications

Connected Component	Cable Standard	Connected Distance (meter)	Connected Number / Connection Point
Connecting nodes of COM ports	Standard category 4 twisted-pair cable	≤ 100	Three Intelligent devices 8 test points of sensor
NOTE: The RDU-SIC G2 Card can connect intelligent devices through COM1 or COM2. The connected devices of single COM cascade cannot exceed two.			

This page intentionally left blank

2 Hardware Installation

This chapter expounds the hardware installation of the Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card.

2.1 Installation Preparation

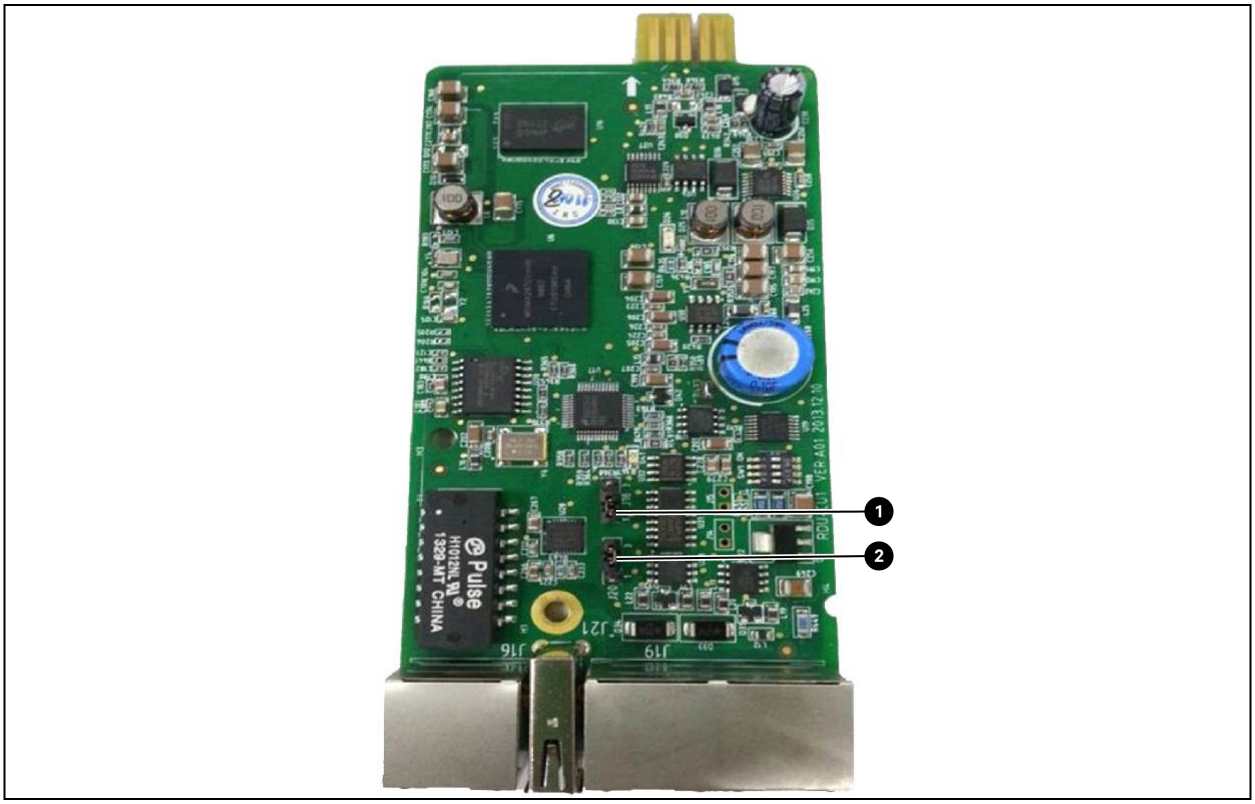
2.1.1 Notes

When installing RDU-SIC G2 Card, take the following precautions to avoid personnel injury and device damage by accident.

- Always cut off the power before performing any installation operation on the RDU-SIC G2 Card.
- Ensure that the external devices are connected to the correct ports of the RDU-SIC G2 Card.
- Wear an ESD-proof glove during installation.
- Arrange the wires properly, and do not put any heavy objects on the wires or stamp the wires.

The jumper locations of the RDU-SIC G2 Card are shown in **Figure 2.1** below .

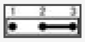
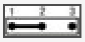
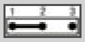
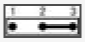
Figure 2.1 Jumper Locations of the Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card



Item	Description
1	Jumper J18
2	Jumper J20

Make sure that the jumpers of Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card are set to the correct position. See **Table 2.1** below for the jumper setting of the RDU-SIC G2 Card.

Table 2.1 Jumper Setting of the RDU-SIC G2 Card

Working Mode	Jumper Setting	Description
Maintenance mode	J20  J18 	The USB port is used to login the RDU-SIC G2 Card through Hyper Terminal (TTY).
Normal mode	J20  J18	The USB port is used to connect to the SMS Modem.
Reset mode	J18 	When you forget the password of 'rduadmin', the password of Web system administrator 'admin' and IP address, set the jumpers according to this mode, reboot the RDU-SIC G2 Card, and wait for more than 20s to recover the above three parameters to be default values. After successful resetting, you must set the jumpers according to the normal mode to avoid resetting the user setting again after rebooting the RDU-SIC G2 Card.

The jumper setting of the RDU-SIC G2 Card is the normal mode by default.

2.1.2 Ambient requirements

Operation Environment

The RDU-SIC G2 Card must be installed indoor. Refer to **Table 1.5** on page 4 for specific requirement.

ESD Proof

To make the static electricity reduce to zero, you must take measures as follows:

- Keep proper temperature and humidity in the data center (see **Table 1.5** on page 4)
- Wear the ESD proof gloves and work clothes before contacting with the PCB. If there are not ESD proof gloves and work clothes, wash hands with water and dry them

Immunity

Take the following measures for immunity:

- Keep the working ground of RDU-SIC G2 Card away from earthing device of electricity device or SPD earthing device
- Keep away from the radio transmitting station, radar transmitter and high frequency large current device
- Use the electromagnetic shielding method, if necessary

2.2 Installing RDU-SIC G2 Card

1. Set the jumpers of the RDU-SIC G2 Card according to **Table 2.1** above .
2. Insert the RDU-SIC G2 Card into position along the guide grooves on both sides of the intellislot intelligent slot and tighten the screws.
3. Open the power device. At this point, if the RUN indicator (yellow) of the RDU-SIC G2 Card turns on, it indicates that the RDU-SIC G2 Card is starting up.

3 Web Page Of Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card

This chapter introduces how to log to the RDU-SIC G2 Card through a Web browser and relevant functions of the RDU-SIC G2 Card.

3.1 Login Preparation

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

3.1.1 Checking IP address connectivity

Before logging in RDU-SIC G2 through web, please first confirm the IP address of RDU-SIC G2, and test it's connectivity. Refer to Q5 in FAQ for the test method.

3.1.2 Checking browser version

For the best user experience, the recommended browser is internet explorer, its version includes: IE8, IE9, IE10 or

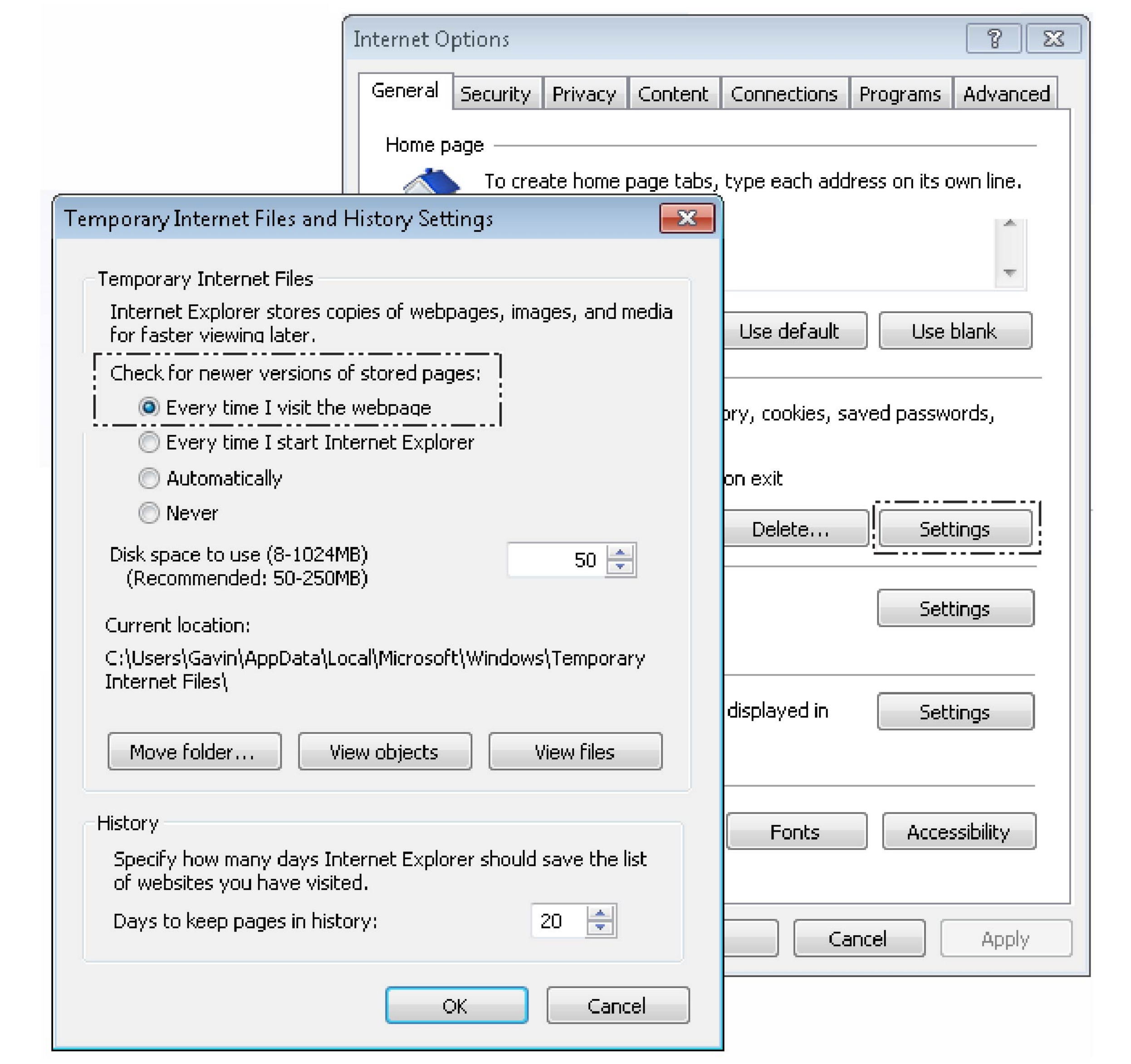
IE11; you can also use other pop web browsers such as chrome, firefox.

3.1.3 Checking browser setting

Checking Internet Explorer General Setting

Double click the icon of Internet Explorer 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 webpage* for Check for newer versions of stored pages, as shown in Figure 3.1 on the next page .

Figure 3.1 General Setting



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Home page

To create home page tabs, type each address on its own line.

Use default | Use blank

ory, cookies, saved passwords,

on exit

Delete... | Settings

Settings

displayed in | Settings

Fonts | Accessibility

Cancel | Apply

Temporary Internet Files and History Settings

Temporary Internet Files

Internet Explorer stores copies of webpages, images, and media for faster viewing later.

Check for newer versions of stored pages:

● Every time I visit the webpage

○ Every time I start Internet Explorer

○ Automatically

○ Never

Disk space to use (8-1024MB) (Recommended: 50-250MB): 50

Current location:

C:\Users\Gavin\AppData\Local\Microsoft\Windows\Temporary Internet Files\

Move folder... | View objects | View files

History

Specify how many days Internet Explorer should save the list of websites you have visited.

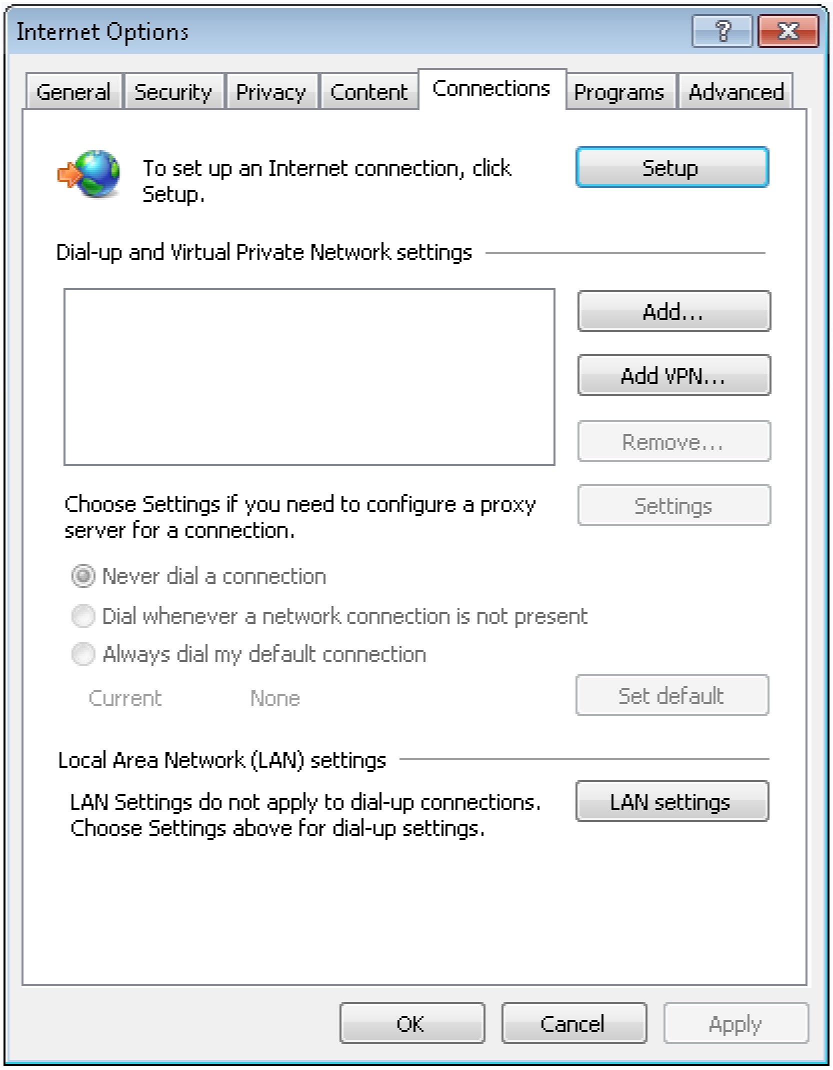
Days to keep pages in history: 20

OK | Cancel

Checking Internet Explorer Proxy Setting

1. Double click the icon of Internet Explorer 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 3.2 on the facing page .

Figure 3.2 Choosing the Connections Tab



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

○ Always dial my default connection

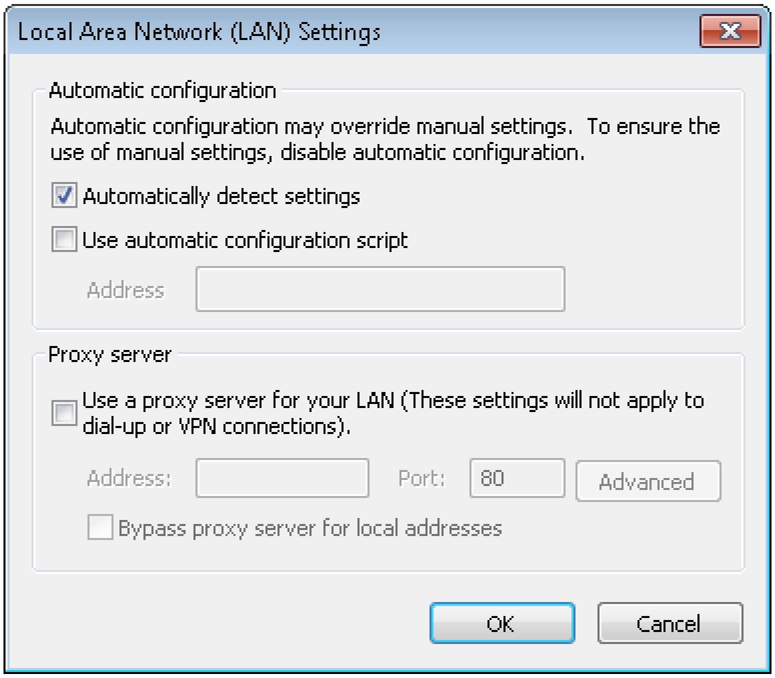
Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

2. In the window shown in **Figure 3.2** above , click the button *LAN Settings* to pop up the window shown in **Figure 3.3** on the next page .

Figure 3.3 LAN Setting



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80 Advanced

□ Bypass proxy server for local addresses

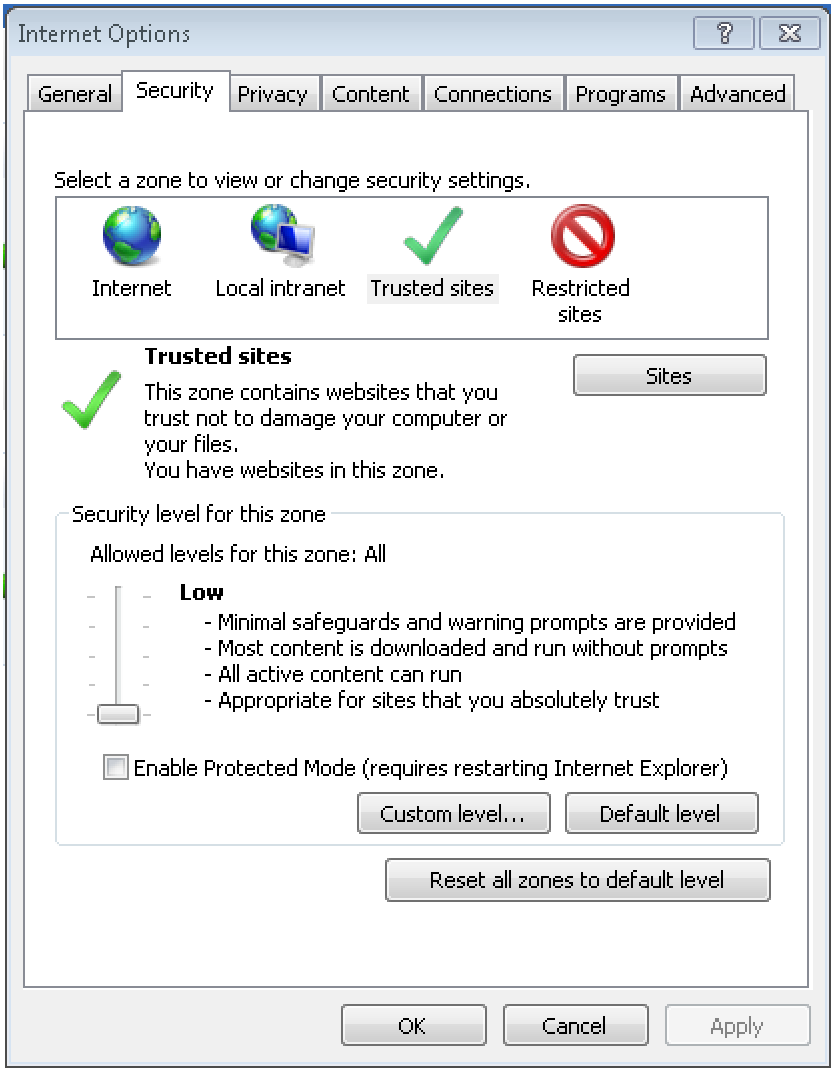
OK Cancel

3. Consult the network manager of your area, ask if you need to set a proxy server and get the configuration method. If there is no need to set a proxy server, do not tick any option.

Checking Internet Explorer Security Setting

1. Double-click the icon of Internet Explorer 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 3.4** on the facing page .

Figure 3.4 Security Setting 1



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

Allowed levels for this zone: All

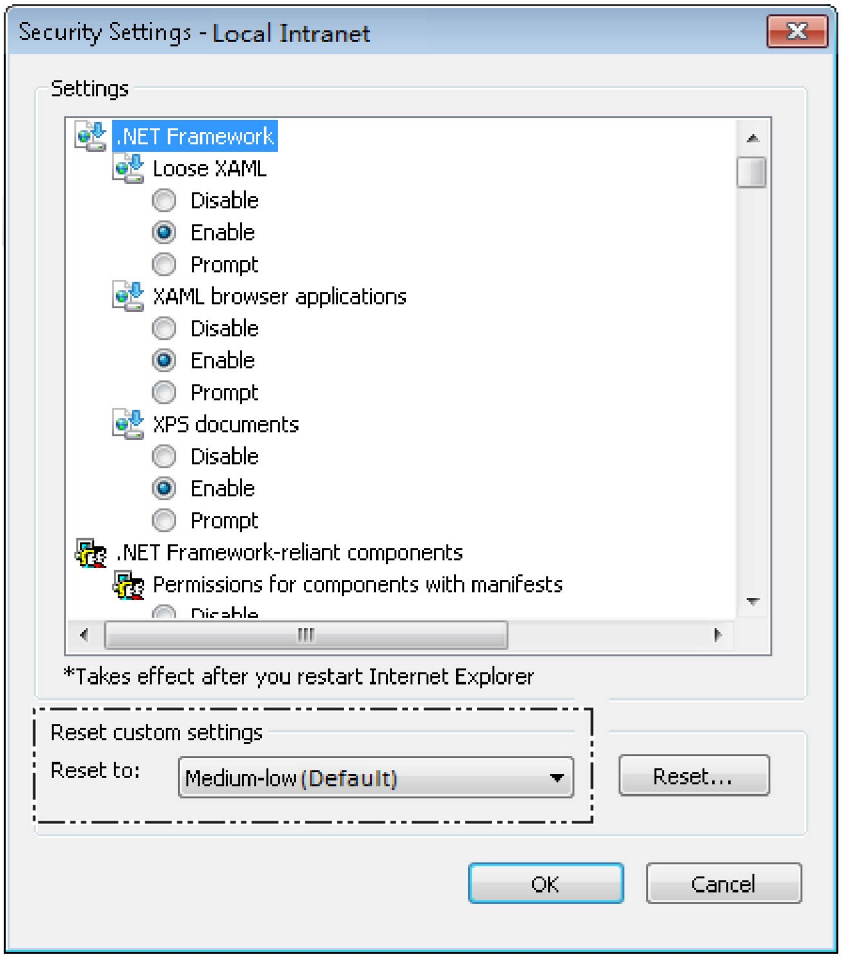
Low

- Minimal safeguards and warning prompts are provided
- Most content is downloaded and run without prompts
- All active content can run
- Appropriate for sites that you absolutely trust

□ Enable Protected Mode (requires restarting Internet Explorer)

2. In the window shown in Figure 3.4 above , choose *Local intranet* and click the *Custom level* button to pop up the window shown in Figure 3.5 on the next page .

Figure 3.5 Security Setting 2



Security Settings - Local Intranet

Settings

.NET Framework
- Loose XAML
  - ○ Disable
  - ● Enable
  - ○ Prompt
- XAML browser applications
  - ○ Disable
  - ● Enable
  - ○ Prompt
- XPS documents
  - ○ Disable
  - ● Enable
  - ○ Prompt

.NET Framework-reliant components
- Permissions for components with manifests
  - ○ Disable

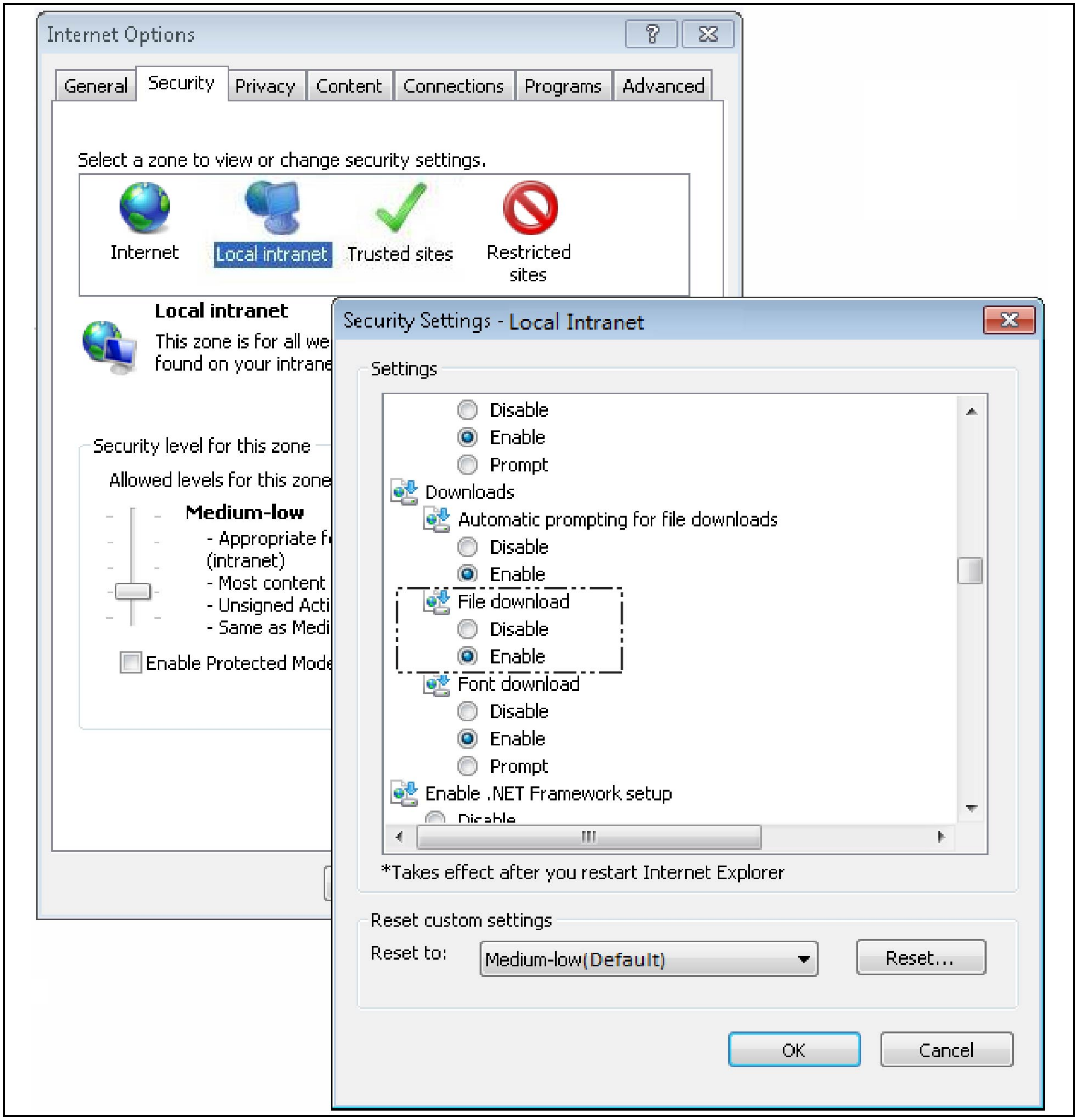
*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-low (Default)

3. In the window shown in Figure 3.5 above , set *'Medium-low'* for the security level. Click the *Reset* button to the finish reset custom settings, at last, click *OK*.
4. In the window shown in Figure 3.6 on the facing page , set *Enable* for File download.

Figure 3.6 Enabling File Download



Internet Options

Select a zone to view or change security settings.

Local intranet

This zone is for all we
found on your intrane

Security level for this zone

Allowed levels for this zone

Medium-low

- Appropriate f
(intranet)
- Most content
- Unsigned Acti
- Same as Medi

□ Enable Protected Mode

Security Settings - Local Intranet

Settings

○ Disable
● Enable
○ Prompt

Downloads

Automatic prompting for file downloads

○ Disable
● Enable

File download

○ Disable
● Enable

Font download

○ Disable
● Enable
○ Prompt

Enable .NET Framework setup

○ Disable

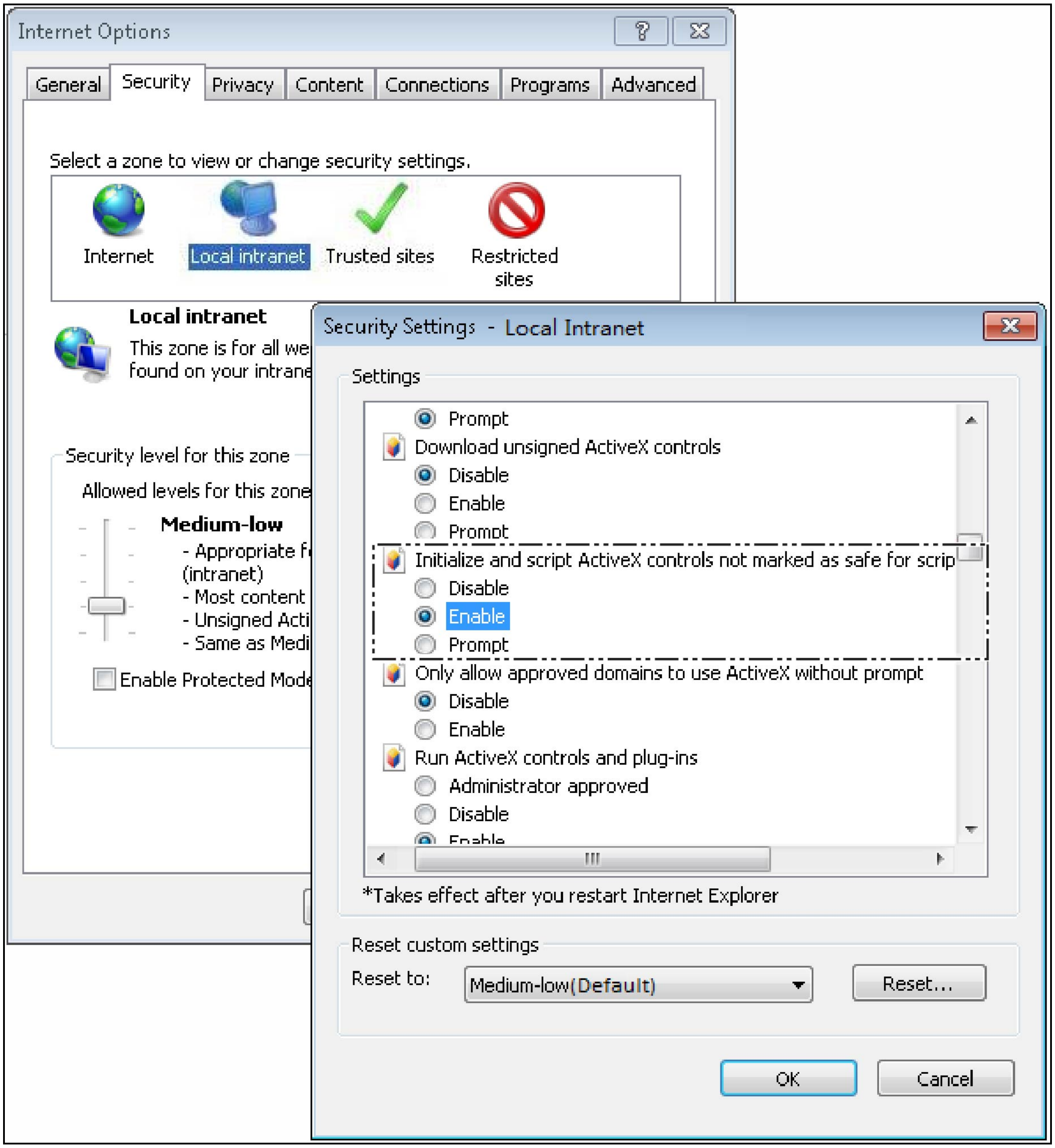
*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-low(Default)

5. In the window shown in **Figure 3.7** on the next page , set *Enable* for Initialize and script ActiveX controls not marked as safe for scripting.

Figure 3.7 Enabling ActiveX Controls



Internet Options

Select a zone to view or change security settings.

Local intranet

This zone is for all we
found on your intrane

Security level for this zone

Allowed levels for this zone

Medium-low

- Appropriate f
(intranet)
- Most content
- Unsigned Acti
- Same as Medi

□ Enable Protected Mode

Security Settings - Local Intranet

Settings

● Prompt

Download unsigned ActiveX controls

● Disable

○ Enable

○ Prompt

Initialize and script ActiveX controls not marked as safe for scrip

○ Disable

● Enable

○ Prompt

Only allow approved domains to use ActiveX without prompt

● Disable

○ Enable

Run ActiveX controls and plug-ins

○ Administrator approved

○ Disable

● Enable

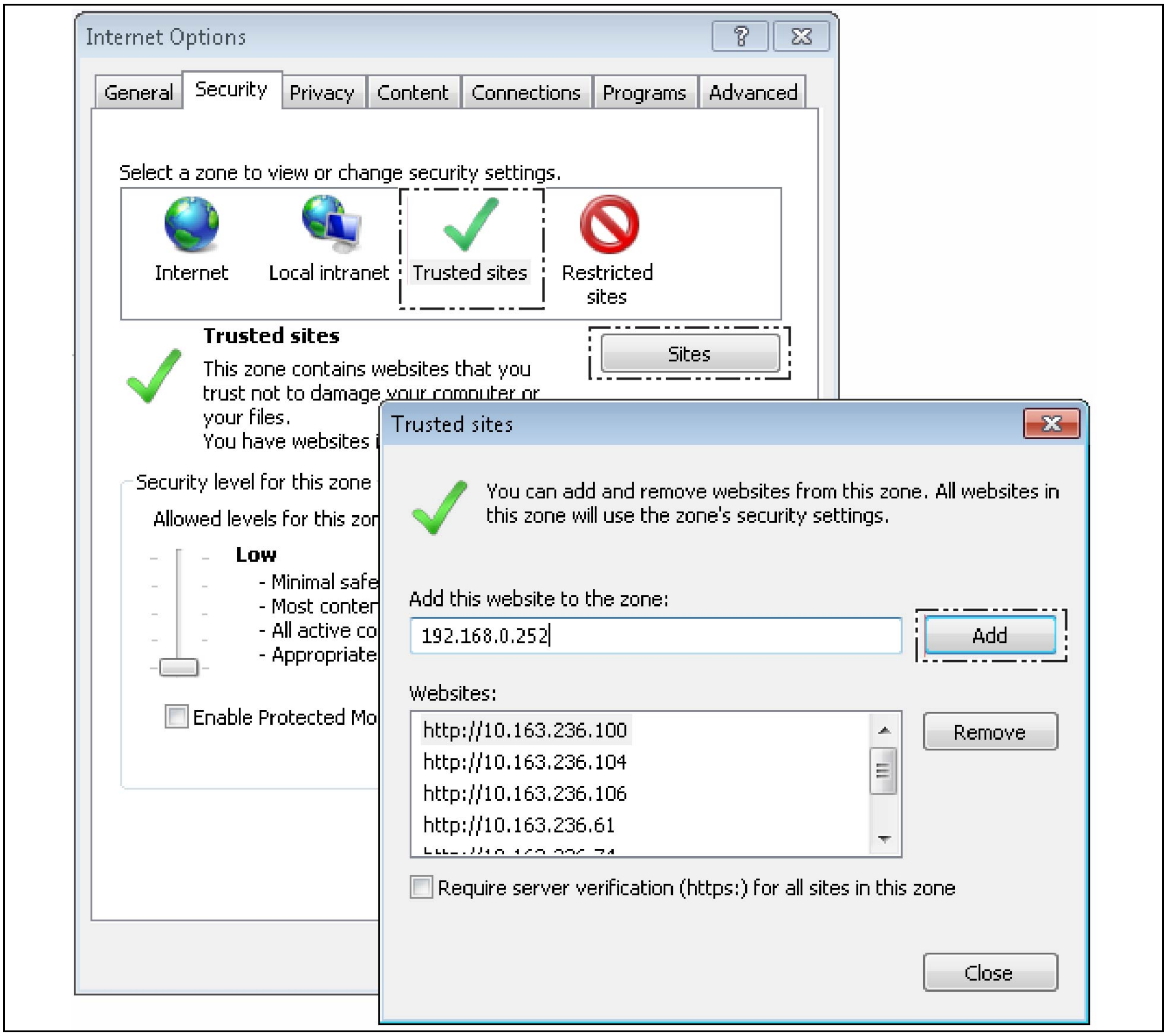
*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-low(Default)

6. In the window shown in **Figure 3.8** on the facing page , add the IP address of the RDU-SIC G2 into the trusted site list.

Figure 3.8 Adding Trusted Sites



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites i

Security level for this zone

Allowed levels for this zor

- Minimal safe
- Most conter
- All active co
- Appropriate

□ Enable Protected Mo

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:
192.168.0.252

Websites:

http://10.163.236.100
http://10.163.236.104
http://10.163.236.106
http://10.163.236.61

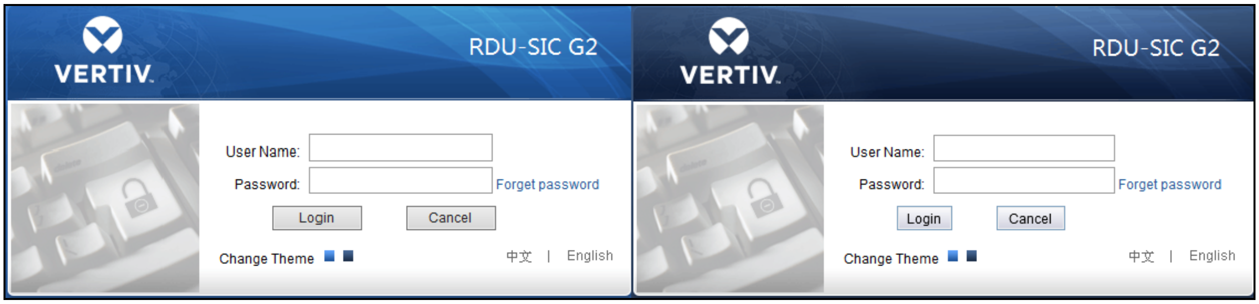
□ Require server verification (https:) for all sites in this zone

3.2 Log In RDU-SIC G2

3.2.1 Login page

1. Open the *IE browser*, and enter the IP address of the RDU-SIC G2 in the address box, the login page will appear, as shown in **Figure 3.9** below . If the login page does not appear, refer to Q5 in FAQ .

Figure 3.9 Login Page of RDU-SIC G2

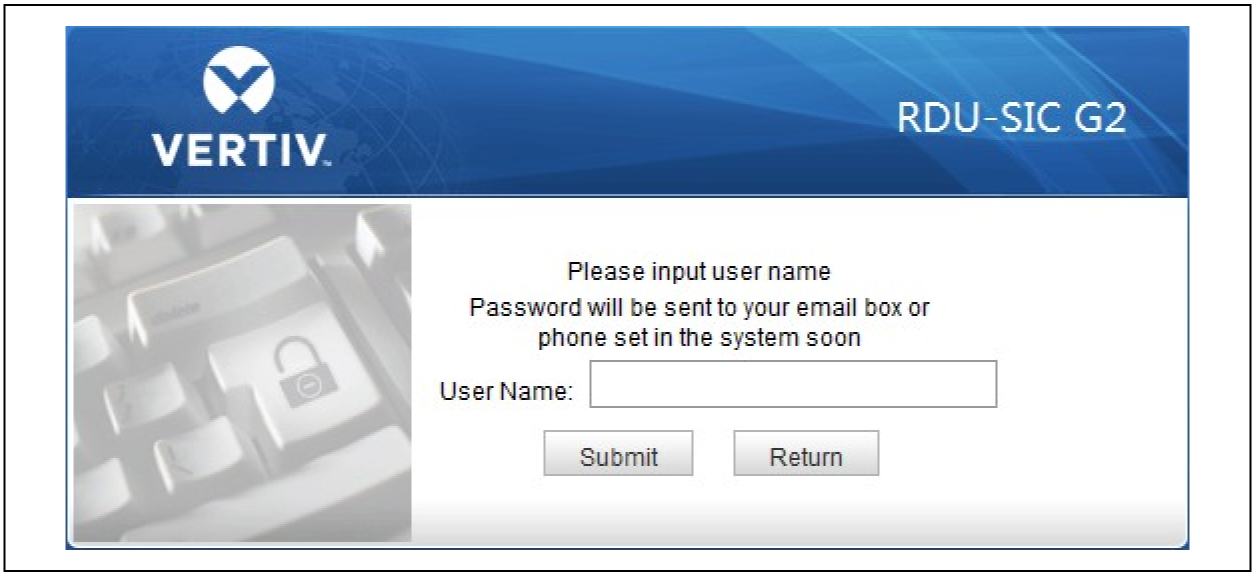


2. On the login page, select a preferable theme by clicking 🟦 or ■ : 🟦 means crystal blue; ■ means ocean blue, as shown in **Figure 3.9** above .
3. Type the username and password (default username: 'admin', default password: 'Vertiv'), and click the *Login* button, the homepage will appear, as shown in **Figure 3.11** on the facing page .

3.2.2 Forgetting 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 3.10** below .

Figure 3.10 Page of Getting Password


Please input user name
Password will be sent to your email box or phone set in the system soon

Type your username, and click the *Submit* button, your password will be sent to the email box or phone which you have configured before. Clicking the Return button cancels the operation.

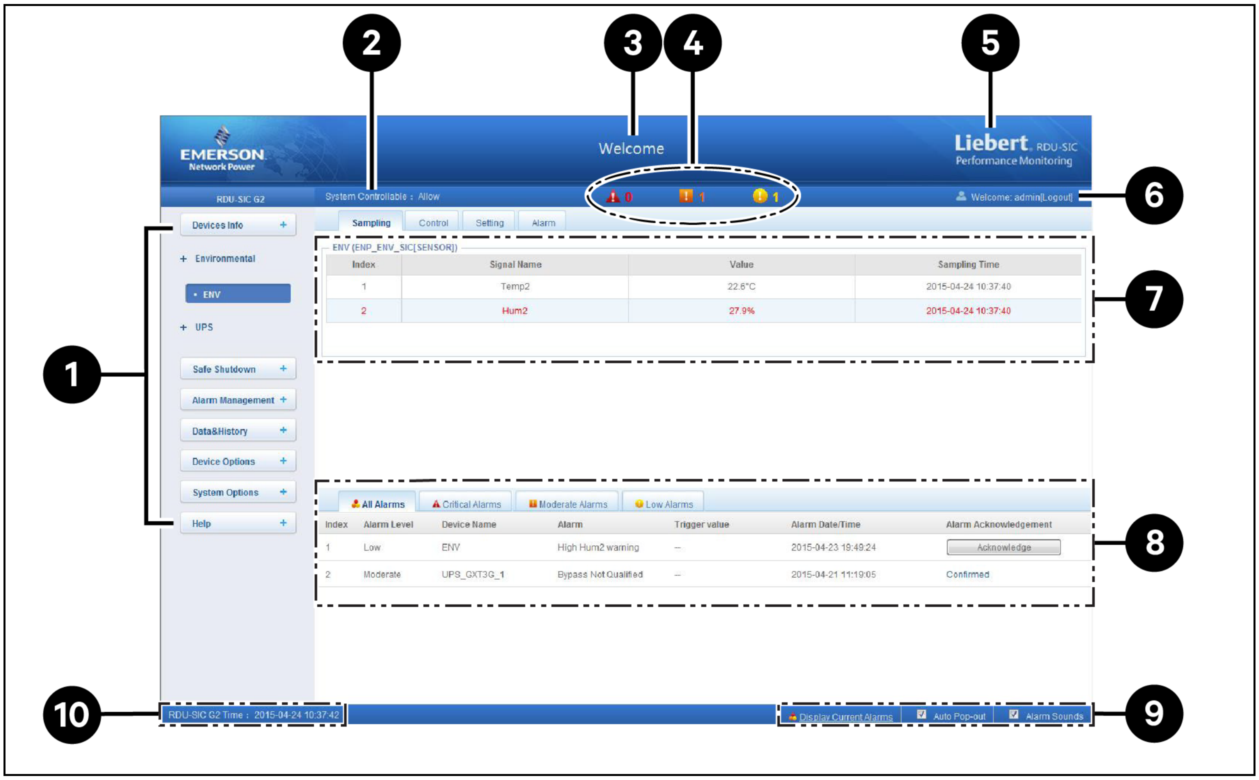
NOTE: Only when you have correctly configured the email and SMS parameters on the SMS and Email Server Configuration page can you receive the password sent by the system. Refer to Alarm management on page 25 for detailed setting method.

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

3.3 Homepage Of RDU-SIC G2

After successful login, the homepage of RDU-SIC G2 is displayed by default, as shown in Figure 3.11 below .

Figure 3.11 Homepage of RDU-SIC G2



ENV (ENP_ENV_SIC[SENSOR])

Index	Signal Name	Value	Sampling Time
1	Temp2	22.6°C	2015-04-24 10:37:40
2	Hum2	27.9%	2015-04-24 10:37:40

Index	Alarm Level	Device Name	Alarm	Trigger value	Alarm Date/Time	Alarm Acknowledgement
1	Low	ENV	High Hum2 warning	--	2015-04-23 19:49:24	Acknowledge
2	Moderate	UPS_GXT3G_1	Bypass Not Qualified	--	2015-04-21 11:19:05	Confirmed

RDU-SIC G2 Time : 2015-04-24 10:37:42

Item	Description
1	Menu item
2	Controllable status
3	Current number of every level alarm
4	System title
5	Logo
6	[User] Logout
7	Function display area

Item	Description
8	Real-time alarm displaying list
9	Alarm pop-out setting
10	Time calibrating link

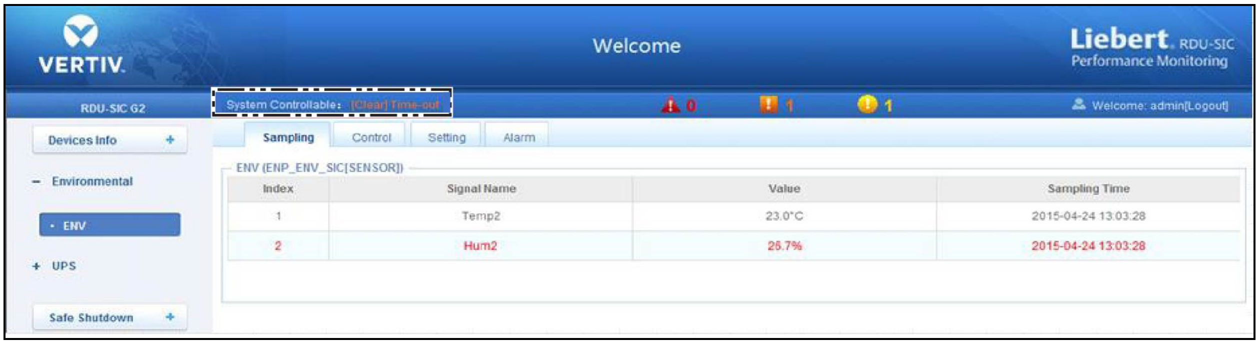
3.3.1 Time calibrating link

The lower left part displays the system time of RDU-SIC G2. Clicking the RDU-SIC G2 time will jump to the time calibrating page. For detailed operation, refer to Date/Time Setting in System Options on page 38 .

3.3.2 Clearing time out

When there is no operation on the page within 15min, the page will become uncontrollable, as shown in **Figure 3.12** below .

Figure 3.12 Controllable Status



System Controllable: [Clear] Time-out

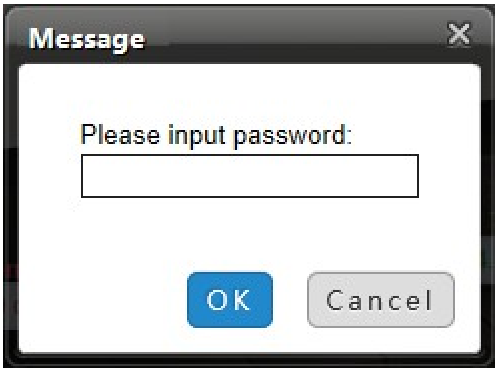
Welcome: admin[Logout]

ENV (ENP_ENV_SIC[SENSOR])

Index	Signal Name	Value	Sampling Time
1	Temp2	23.0°C	2015-04-24 13:03:28
2	Hum2	25.7%	2015-04-24 13:03:28

Click *[Clear] Time-out*, the input box shown in **Figure 3.13** below will appear. After typing the password, the controllable status will become normal after about 5s.

Figure 3.13 Password Verification



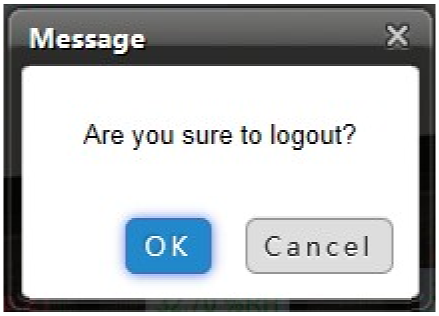
Message

Please input password:

3.3.3 Logout

Click the *Logout* at the upper right corner of the homepage, the prompt box shown in **Figure 3.14** on the facing page will appear, clicking *OK* will log out safely.

Figure 3.14 Logout



Message

Are you sure to logout?

3.3.4 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 3.11 on page 19 :

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

3.4 Menu Items

On the homepage of RDU-SIC G2, the menu items include:

- Device Info
- Safe Shutdown
- Alarm Management
- Data and History
- Device Options
- System Options
- Help

3.4.1 Device Info

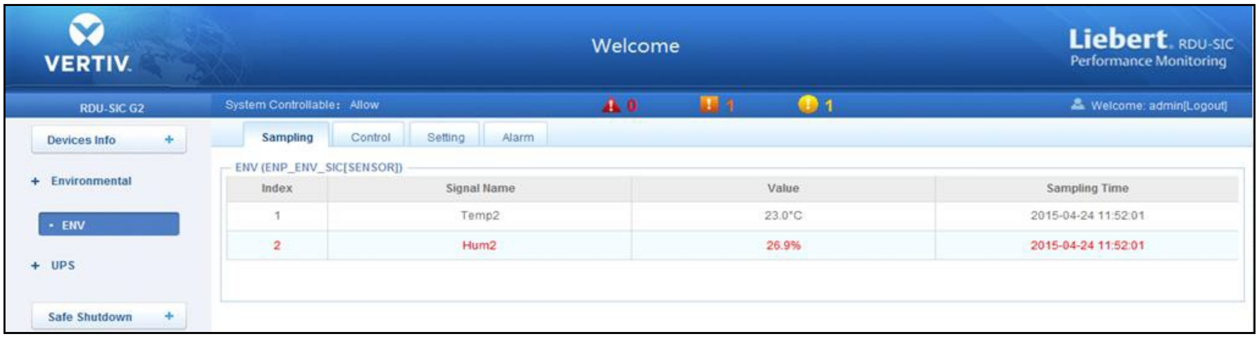
Click the *Device Info* menu in the left, the submenus will appear. When you click the specific device, the right part will display the relative information of the device including Sampling, Control, Setting, and Alarm.

NOTE: ENV in Device Info is a dummy device, which indicates all temperature sensors and temperature and humidity sensors connected to Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card.

Sampling

Clicking the *Sampling* tab can enter the sampling page, which displays sampling signals of the selected device, as shown in Figure 3.15 on the next page .

Figure 3.15 Sampling Tab



System Controllable: Allow

ENV (ENP_ENV_SIC[SENSOR])

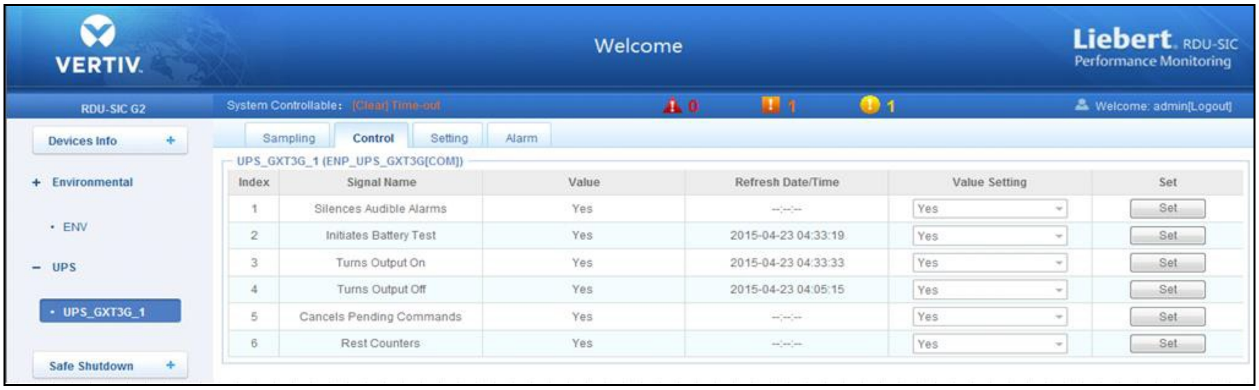
Index	Signal Name	Value	Sampling Time
1	Temp2	23.0°C	2015-04-24 11:52:01
2	Hum2	26.9%	2015-04-24 11:52:01

If some signals are found in sampling tab, which is the alarm status, it will be displayed in red.

Control

Clicking the *Control* tab can enter the control page, which displays control signals of the selected device as shown in **Figure 3.16** below .

Figure 3.16 Control Tab



System Controllable: [Clear] Time-out

UPS_GXT3G_1 (ENP_UPS_GXT3G[COM])

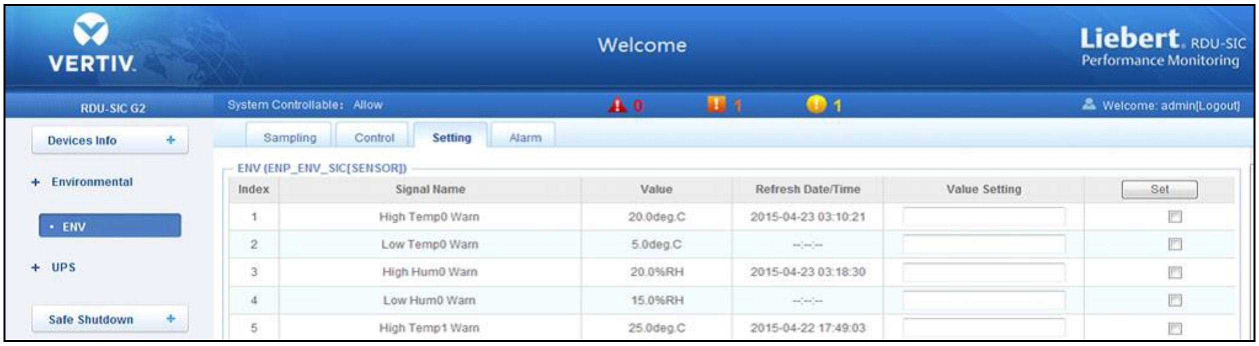
Index	Signal Name	Value	Refresh Date/Time	Value Setting	Set
1	Silences Audible Alarms	Yes	--:--:--	Yes	Set
2	Initiates Battery Test	Yes	2015-04-23 04:33:19	Yes	Set
3	Turns Output On	Yes	2015-04-23 04:33:33	Yes	Set
4	Turns Output Off	Yes	2015-04-23 04:05:15	Yes	Set
5	Cancels Pending Commands	Yes	--:--:--	Yes	Set
6	Rest Counters	Yes	--:--:--	Yes	Set

Click the *Set* button to control the device.

Setting

Clicking the *Setting* tab can enter the setting page, which displays setting signals of the selected device as shown in **Figure 3.17** below .

Figure 3.17 Setting Tab



System Controllable: Allow

ENV (ENP_ENV_SIC[SENSOR])

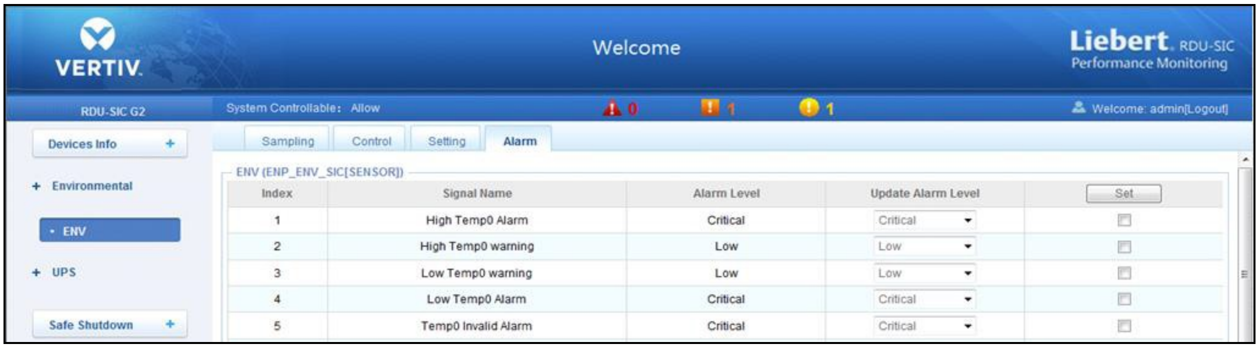
Index	Signal Name	Value	Refresh Date/Time	Value Setting	Set
1	High Temp0 Warn	20.0deg.C	2015-04-23 03:10:21		□
2	Low Temp0 Warn	5.0deg.C	--:--:--		□
3	High Hum0 Warn	20.0%RH	2015-04-23 03:18:30		□
4	Low Hum0 Warn	15.0%RH	--:--:--		□
5	High Temp1 Warn	25.0deg.C	2015-04-22 17:49:03		□

You can set several signals at the same time and at most 16 signals can be set at the same time for each time.

Alarm

Clicking the *Alarm* tab can enter the alarm page, which displays alarm signals of the selected device, as shown in **Figure 3.18** below .

Figure 3.18 Alarm Tab



ENV (ENP_ENV_SIC[SENSOR])

Index	Signal Name	Alarm Level	Update Alarm Level	Set
1	High Temp0 Alarm	Critical	Critical	□
2	High Temp0 warning	Low	Low	□
3	Low Temp0 warning	Low	Low	□
4	Low Temp0 Alarm	Critical	Critical	□
5	Temp0 Invalid Alarm	Critical	Critical	□

You can set the alarm level of several alarm signals at the same time and maximum 16 signals can be set at the same time for each time.

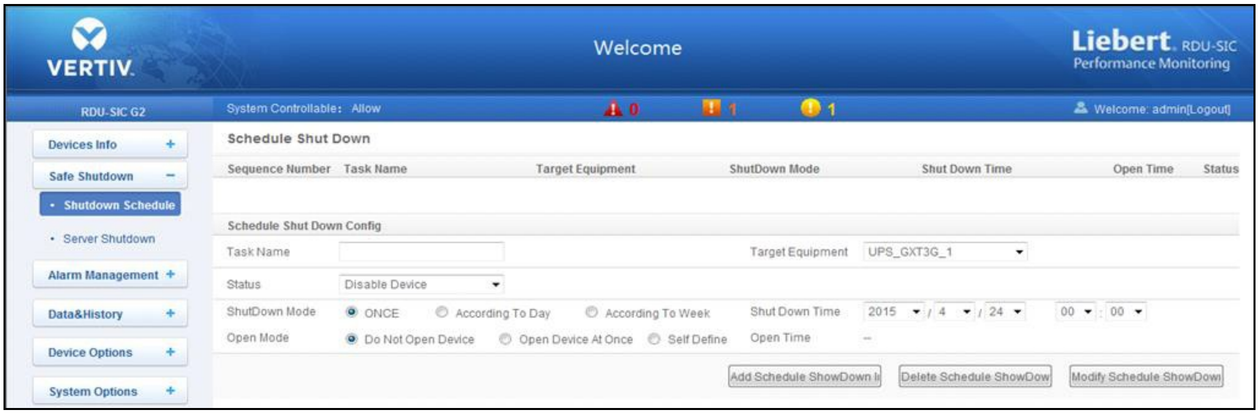
3.4.2 Safe Shutdown

On the RDU-SIC G2 homepage, click the *Safe Shutdown* menu on the left, two submenus appear including Shutdown Schedule and Server Shutdown.

Shutdown Schedule

Click *Shutdown Schedule* under the Safe Shutdown menu, the page shown in **Figure 3.19** below pops up.

Figure 3.19 Shutdown Schedule Page



Schedule Shut Down

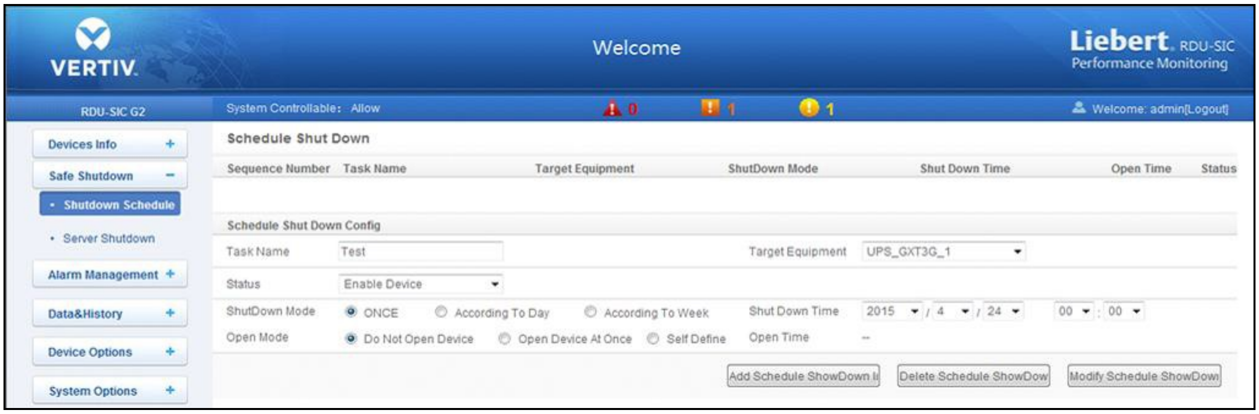
Sequence Number	Task Name	Target Equipment	ShutDown Mode	Shut Down Time	Open Time	Status

Schedule Shut Down Config

Task Name:
Target Equipment: UPS_GXT3G_1
Status: Disable Device
ShutDown Mode: ● ONCE ○ According To Day ○ According To Week
Shut Down Time: 2015 / 4 / 24 00 : 00
Open Mode: ● Do Not Open Device ○ Open Device At Once ○ Self Define
Open Time: --

The shutdown schedule page is used to add, delete, and the modify the schedule shutdown tasks of UPS devices. As shown in **Figure 3.19** above , type a *Task Name* of schedule shutdown in the field of Task Name, select a *Target Equipment*, select whether to enable the task in the Status field, select *Shutdown Mode* and *Open Mode* and then add *Open Time* according to the corresponding prompt, the page is shown in **Figure 3.20** on the next page .

Figure 3.20 Schedule Shutdown Task List



Schedule Shut Down

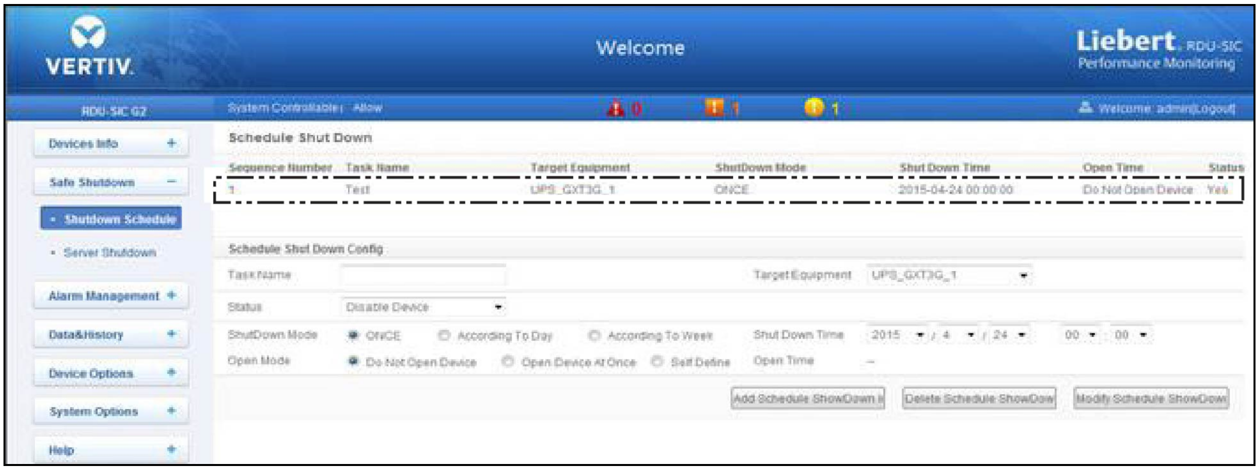
Sequence Number	Task Name	Target Equipment	ShutDown Mode	Shut Down Time	Open Time	Status

Schedule Shut Down Config

Task Name: Test
Target Equipment: UPS_GXT3G_1
Status: Enable Device
ShutDown Mode: ● ONCE ○ According To Day ○ According To Week
Shut Down Time: 2015 / 4 / 24 00 : 00
Open Mode: ● Do Not Open Device ○ Open Device At Once ○ Self Define
Open Time: --

Click the *Add Schedule Shutdown* button, the task will be successfully added. As shown in **Figure 3.21** below , a new task has been added to the schedule shutdown task list. The tasks in the task list will be executed automatically according to their Enable/Disable status.

Figure 3.21 Schedule Shutdown Task List



Schedule Shut Down

Sequence Number	Task Name	Target Equipment	ShutDown Mode	Shut Down Time	Open Time	Status
1	Test	UPS_GXT3G_1	ONCE	2015-04-24 00:00:00	Do Not Open Device	Yes

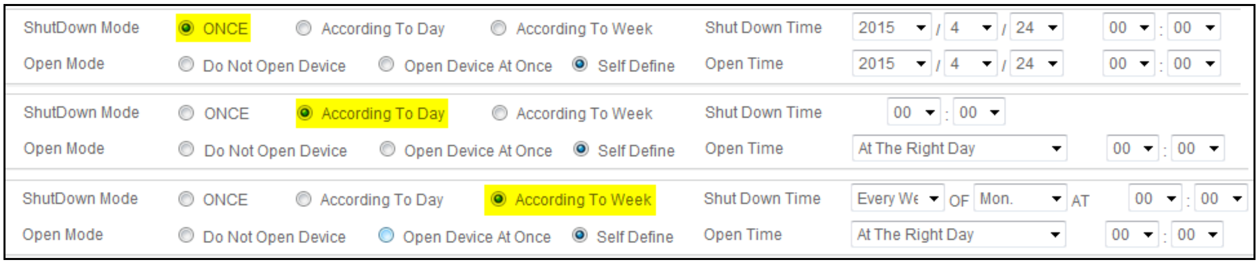
Schedule Shut Down Config

Task Name:
Target Equipment: UPS_GXT3G_1
Status: Disable Device
ShutDown Mode: ● ONCE ○ According To Day ○ According To Week
Shut Down Time: 2015 / 4 / 24 00 : 00
Open Mode: ● Do Not Open Device ○ Open Device At Once ○ Self Define
Open Time: --

The descriptions about the RDU-SIC G2 schedule shutdown function are as follows:

1. When the Open Mode is set to 'Do Not Open Device' or 'Open Device At Once', the Open Time cannot be set, and it is displayed as '--';
2. The format of Shut Down Time changes with different options of Shut Down Mode automatically as shown in **Figure 3.22** below .

Figure 3.22 Format of Shut Down Time



ShutDown Mode: ● ONCE ○ According To Day ○ According To Week
Shut Down Time: 2015 / 4 / 24 00 : 00
Open Mode: ○ Do Not Open Device ○ Open Device At Once ● Self Define
Open Time: 2015 / 4 / 24 00 : 00

ShutDown Mode: ○ ONCE ● According To Day ○ According To Week
Shut Down Time: 00 : 00
Open Mode: ○ Do Not Open Device ○ Open Device At Once ● Self Define
Open Time: At The Right Day 00 : 00

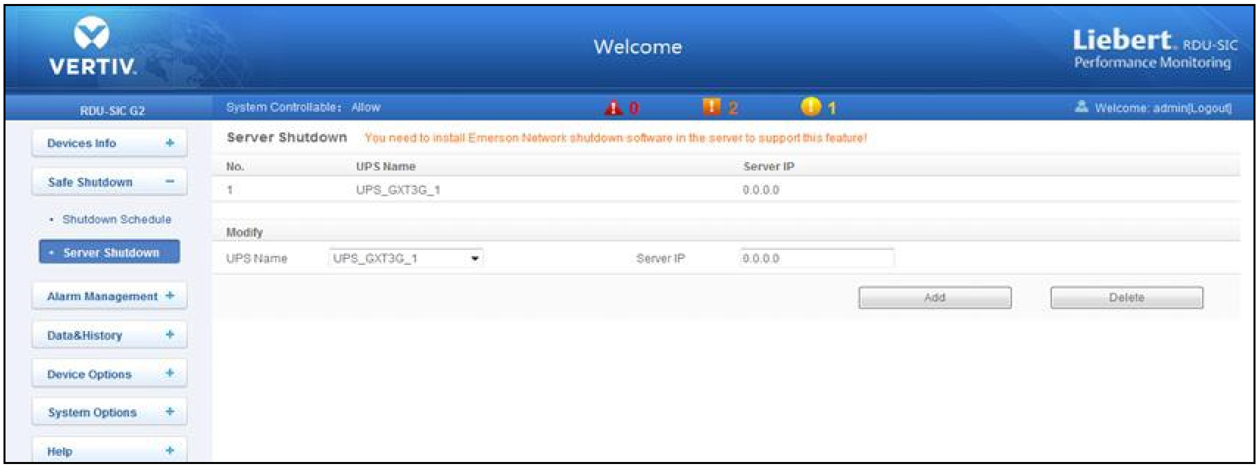
ShutDown Mode: ○ ONCE ○ According To Day ● According To Week
Shut Down Time: Every We OF Mon. AT 00 : 00
Open Mode: ○ Do Not Open Device ○ Open Device At Once ● Self Define
Open Time: At The Right Day 00 : 00

NOTE: The RDU-SIC G2 can support up to ten shutdown tasks. Only when 'Enable Device' is set for status can the schedule shutdown task be enabled.

Server Shutdown

Click *Server Shutdown* under the Safe Shutdown menu and the Server Shutdown page will pop up, as shown in Figure 3.23 below .

Figure 3.23 Server Shutdown Page



Server Shutdown You need to install Emerson Network shutdown software in the server to support this feature!

No.	UPS Name	Server IP
1	UPS_GXT3G_1	0.0.0.0

Modify

UPS Name UPS_GXT3G_1 Server IP 0.0.0.0

On the Server Shutdown page, you can add and delete server shutdown task.

The procedures for adding a server shutdown task are as follows:

1. Select a UPS from the drop-down box of UPS Name;
2. In the Server IP field, type the IP address of the server to be closed;
3. Click the *Add* button, the server shutdown task is added, and the basic information of the UPS will be displayed in the upper list of the page.

NOTE: If you want to use the server shutdown function, please install 'Vertiv network shutdown' software in the server.

The procedures for deleting a server shutdown task are as follows:

- Select the task to be deleted in the server shutdown task list and click the *Delete* button to finish the operation.

3.4.3 Alarm management

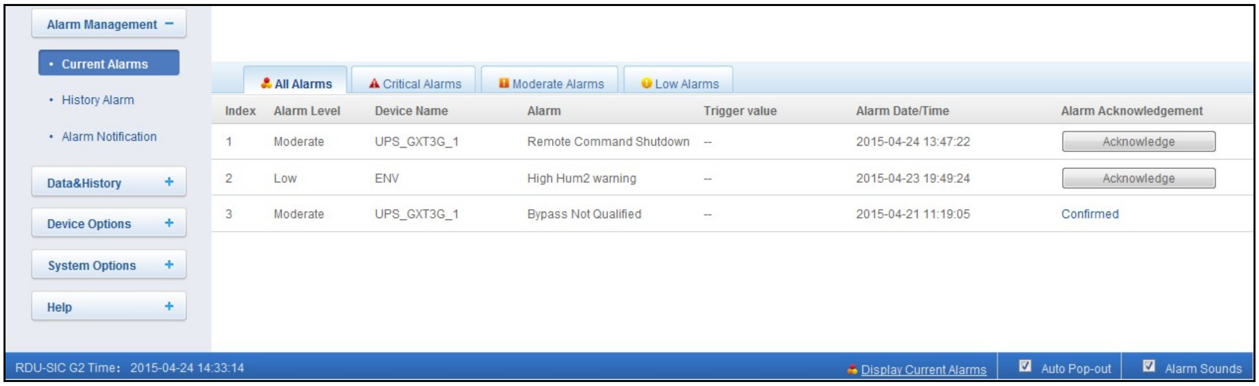
The Alarm Management menu supplies alarm centralized management function, enabling you to self-defining alarm notification and alarm linkage rules, and viewing historic alarm.

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

Current Alarms

Click *Current Alarms* under the Alarm Management menu, or refer to Real time alarm pop-up setting on page 21 , the current alarm list will pop up, as shown in Figure 3.24 on the next page .

Figure 3.24 Current Alarms

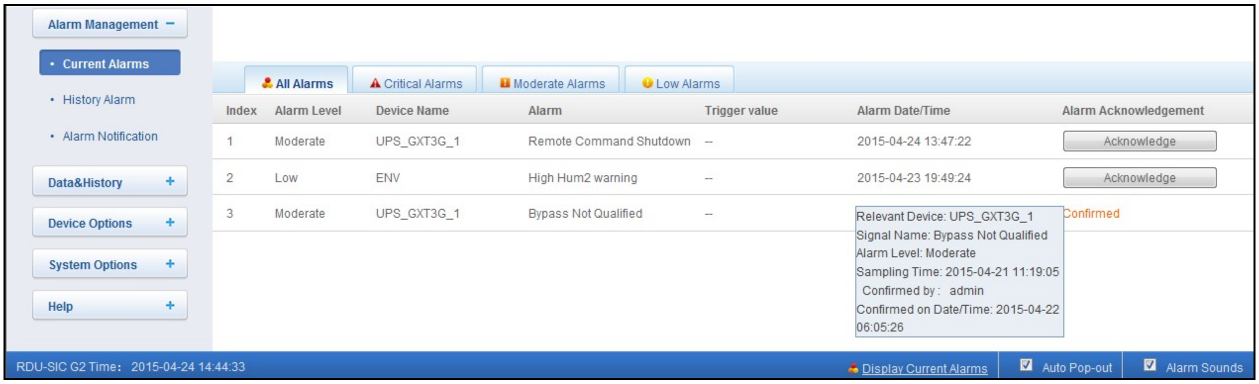


Index	Alarm Level	Device Name	Alarm	Trigger value	Alarm Date/Time	Alarm Acknowledgement
1	Moderate	UPS_GXT3G_1	Remote Command Shutdown	--	2015-04-24 13:47:22	Acknowledge
2	Low	ENV	High Hum2 warning	--	2015-04-23 19:49:24	Acknowledge
3	Moderate	UPS_GXT3G_1	Bypass Not Qualified	--	2015-04-21 11:19:05	Confirmed

RDU-SIC G2 Time： 2015-04-24 14:33:14

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. After confirmation, no alarm notification about the confirmed alarm will be sent.
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 3.25** below .

Figure 3.25 Confirming Information



Index	Alarm Level	Device Name	Alarm	Trigger value	Alarm Date/Time	Alarm Acknowledgement
1	Moderate	UPS_GXT3G_1	Remote Command Shutdown	--	2015-04-24 13:47:22	Acknowledge
2	Low	ENV	High Hum2 warning	--	2015-04-23 19:49:24	Acknowledge
3	Moderate	UPS_GXT3G_1	Bypass Not Qualified	--		Confirmed

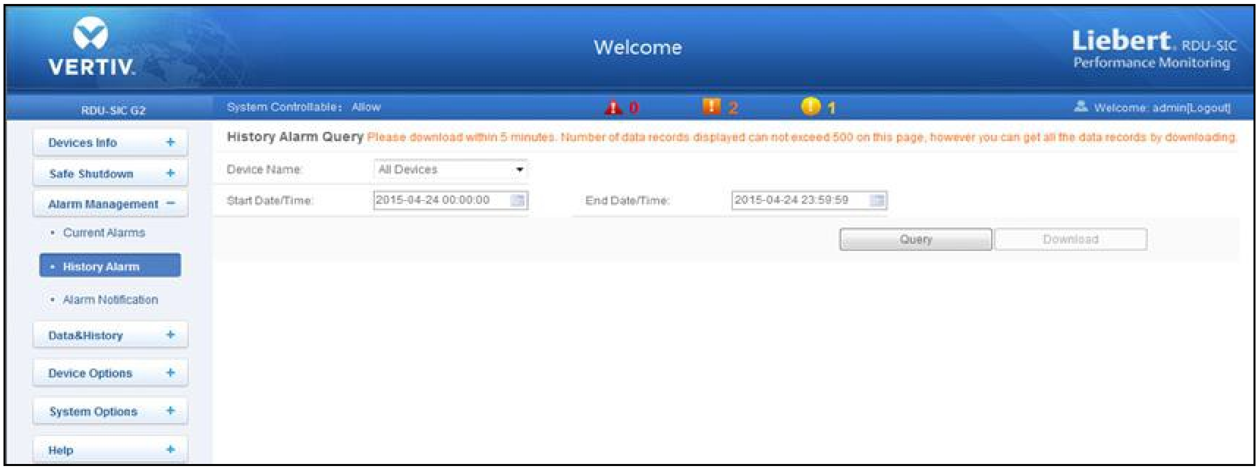
Relevant Device: UPS_GXT3G_1
Signal Name: Bypass Not Qualified
Alarm Level: Moderate
Sampling Time: 2015-04-21 11:19:05
Confirmed by : admin
Confirmed on Date/Time: 2015-04-22 06:05:26

RDU-SIC G2 Time： 2015-04-24 14:44:33

History Alarm

Click *History Alarm* under the Alarm Management menu to look over historical alarm records. Select a device (for instance, 'All Devices') and set the start time and end time (for instance, from 2015-04-24 00:00:00 to 2015-04-24 23:59:59). Then 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 3.26** on the facing page .

Figure 3.26 History Alarm Query



History Alarm Query Please download within 5 minutes. Number of data records displayed can not exceed 500 on this page, however you can get all the data records by downloading.

Device Name: All Devices

Start Date/Time: 2015-04-24 00:00:00

End Date/Time: 2015-04-24 23:59:59

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

Alarm Notification

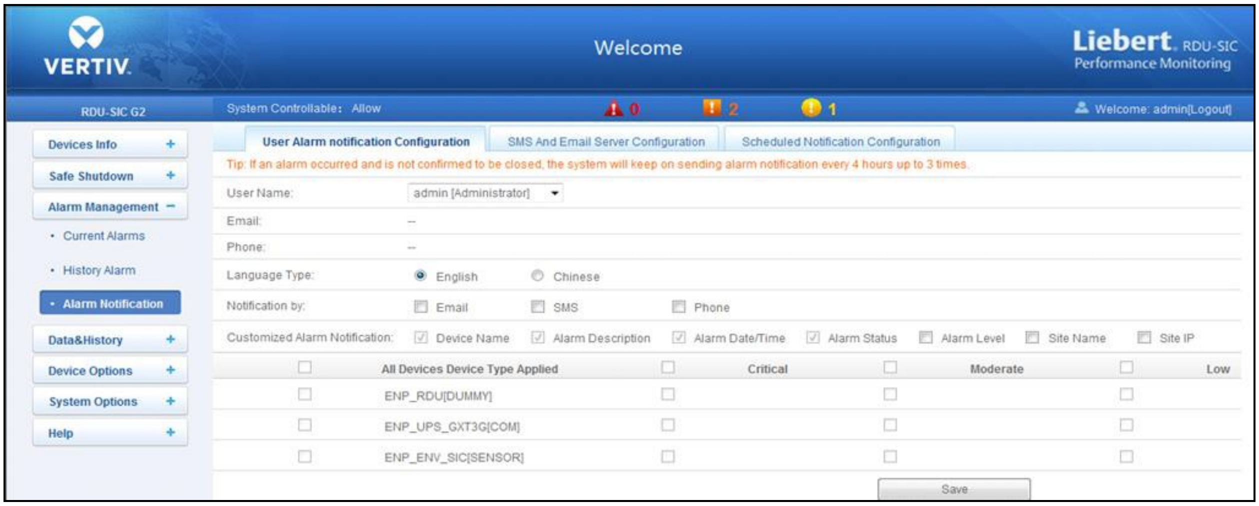
User Alarm Notification Configuration

Click the *Alarm Notification* under the alarm management menu, the page shown in Figure 3.27 below pops up. 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 (including equip name, alarm description, alarm time, and alarm state by default).

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 can be edited. There are three settings for the alarm table like when all devices are chosen, all devices will be configured with the same alarm level, when the low level alarm is chosen, the alarm level above this level will also be chosen and when some device is chosen, the highest level critical alarm will be chosen by default.

Figure 3.27 User Alarm Notification Configuration



Tip: If an alarm occurred and is not confirmed to be closed, the system will keep on sending alarm notification every 4 hours up to 3 times.

User Name: admin [Administrator]

Email: --

Phone: --

Language Type: ● English ○ Chinese

Notification by: □ Email □ SMS □ Phone

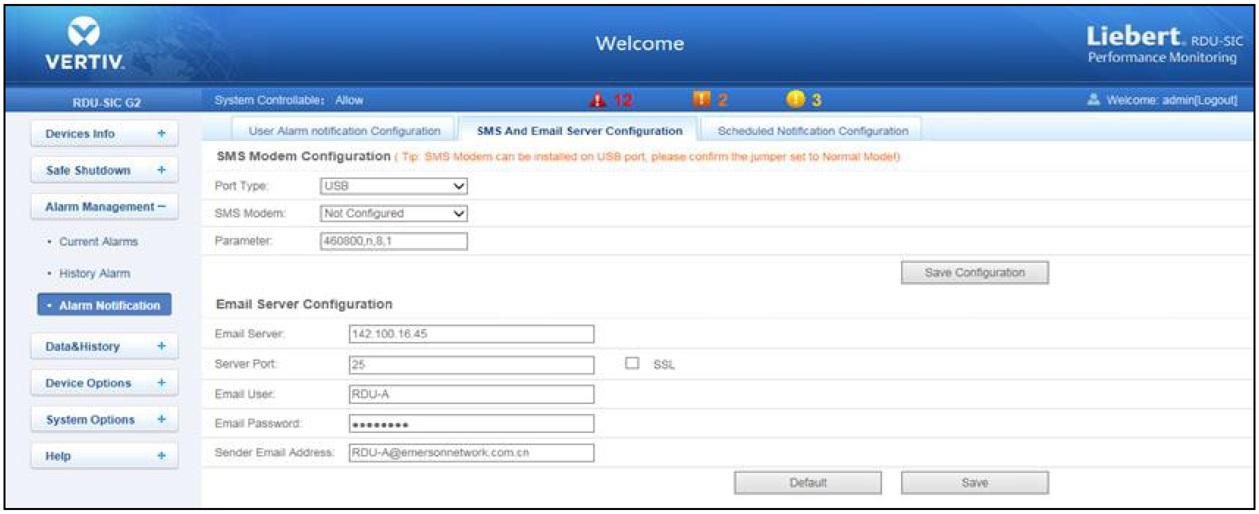
Customized Alarm Notification: ☑ Device Name ☑ Alarm Description ☑ Alarm Date/Time ☑ Alarm Status □ Alarm Level □ Site Name □ Site IP

□	All Devices Device Type Applied	□	Critical	□	Moderate	□	Low
□	ENP_RDU[DUMMY]	□		□		□	
□	ENP_UPS_GXT3G[COM]	□		□		□	
□	ENP_ENV_SIC[SENSOR]	□		□		□	

SMS and Email Server Configuration

Click the *Alarm Notification* under the Alarm Management menu, and then click the *SMS and Email Server Configuration* tab, the page shown in **Figure 3.28** below pops up.

Figure 3.28 SMS/Email Server Configuration



SMS Modem Configuration (Tip: SMS Modem can be installed on USB port, please confirm the jumper set to Normal Mode!)

Port Type: USB

SMS Modem: Not Configured

Parameter: 460800,n,8,1

Email Server Configuration

Email Server: 142.100.16.45

Server Port: 25 □ SSL

Email User: RDU-A

Email Password: ●●●●●●●●

Sender Email Address: RDU-A@emersonnetwork.com.cn

On the page shown in **Figure 3.28** above , you can perform SMS Modem Configuration for alarm notification reminding through SMS or phone, you can also perform Email Server Configuration for alarm notifications reminding through email, the procedures are as follows:

1. SMS Modem Configuration
   a. Connect an SMS modem through a USB port according to need, and choose Port Type, the page will automatically display parameter.
   b. Choose SMS modem (GPRS/CDMA) according to the SMS modem type.
   c. Set the communication parameter of the SMS modem.
   d. Click the *Save Configuration* button to save the configuration of the current user's SMS modem.

NOTE: If the SMS modem is connected through USB port, you need to set the jumper by referring to Table 2.1 on page 8 .

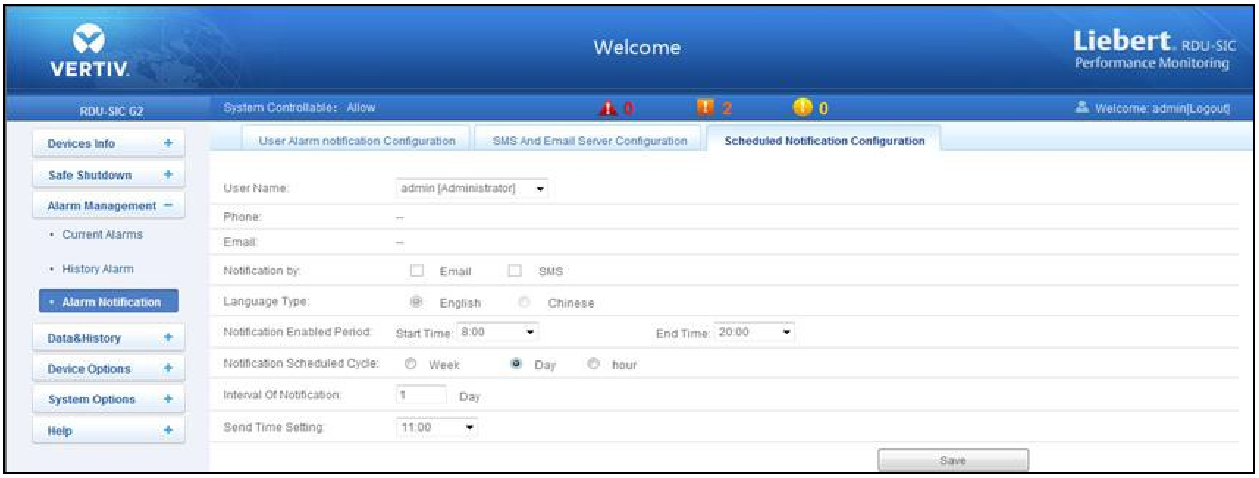
2. Email Server Configuration
   a. Type the server IP address or domain name in the Email Server field;
   b. Type the Server Port, Email User, Email Password, and Sender Email Address in the corresponding fields;
   c. Click the *Save* button to save the configuration of current user's email server.

NOTE: The server port is '25' by default. When SSL is chosen, the server port will become '465' automatically. The email user is 'RDU-A' by default. When using SSL, you need to ensure that the email server supports SSL function.

Scheduled Notification Configuration

Click the *Alarm Notification* under the alarm management menu, and then click the *Scheduled Notification Configuration* tab, the page shown in **Figure 3.29** on the facing page pops up.

Figure 3.29 Scheduled Notification Configuration



User Name: admin [Administrator]

Phone: --

Email: --

Notification by: □ Email □ SMS

Language Type: ● English ○ Chinese

Notification Enabled Period: Start Time: 8:00 End Time: 20:00

Notification Scheduled Cycle: ○ Week ● Day ○ hour

Interval Of Notification: 1 Day

Send Time Setting: 11:00

NOTE: Scheduled notification configuration must be used together with user alarm notification configuration; otherwise, you cannot select User Name, Notification by and Language Type. For scheduled notification configuration, the notification method 'Phone' is not supported. The scheduled notification means sending the running state of the RDU-SIC G2 system (normal or alarm) to the user.

1. First of all, on the User Alarm Notification Configuration page, complete and save the setting of User, Notification by and Language Type.
2. On the Scheduled Notification Configuration page, set the parameter as per mentioned below:
   - Notification Enabled Period (setting range: 8:00 ~ 20:00)
   - Notification Scheduled Cycle (default: Hour)
   - Interval of Notification (default: 1)
   - Send Time Setting (default: start time).
3. Click the *Save* button to save the system notification configuration.

3.4.4 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-SIC G2 homepage, click *Data & History* in the left part, and four submenus appear, including: Device Information, History Data, History Log, and Clear History.

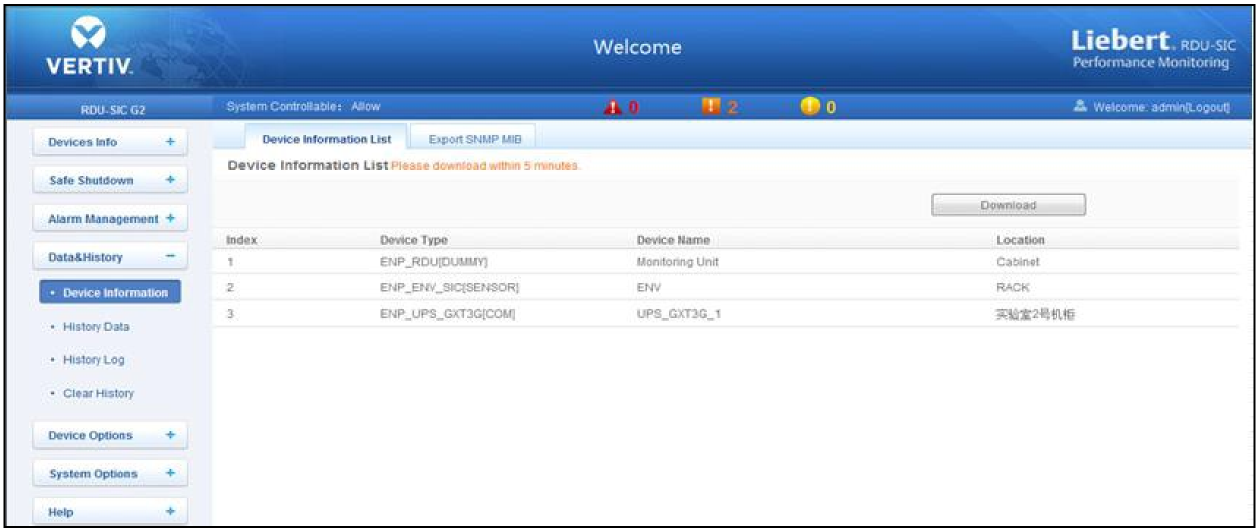
Device Information

Click the *Device Information* under the data and history menu, the page shown in Figure 3.30 on the next page pops up. The page includes two tabs: Device Information List and Export SNMP MIB.

Device Information List

As shown in Figure 3.30 on the next page , the page lists the main information of all equipment. Click the *Download* button to download the query result.

Figure 3.30 Device Information List



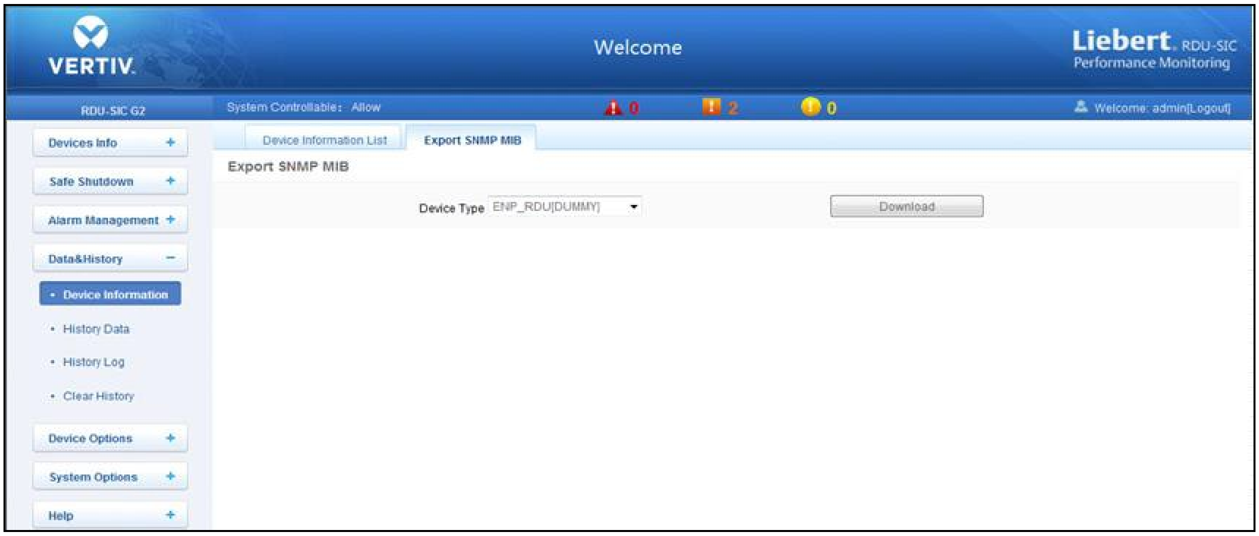
Device Information List Please download within 5 minutes.

Index	Device Type	Device Name	Location
1	ENP_RDU[DUMMY]	Monitoring Unit	Cabinet
2	ENP_ENV_SIC[SENSOR]	ENV	RACK
3	ENP_UPS_GXT3G[COM]	UPS_GXT3G_1	实验室2号机柜

Export SNMP MIB

As shown in **Figure 3.31** below , you can export MIB information according to device type. After selection, click the *Download* button to export MIB information.

Figure 3.31 Export SNMP MIB



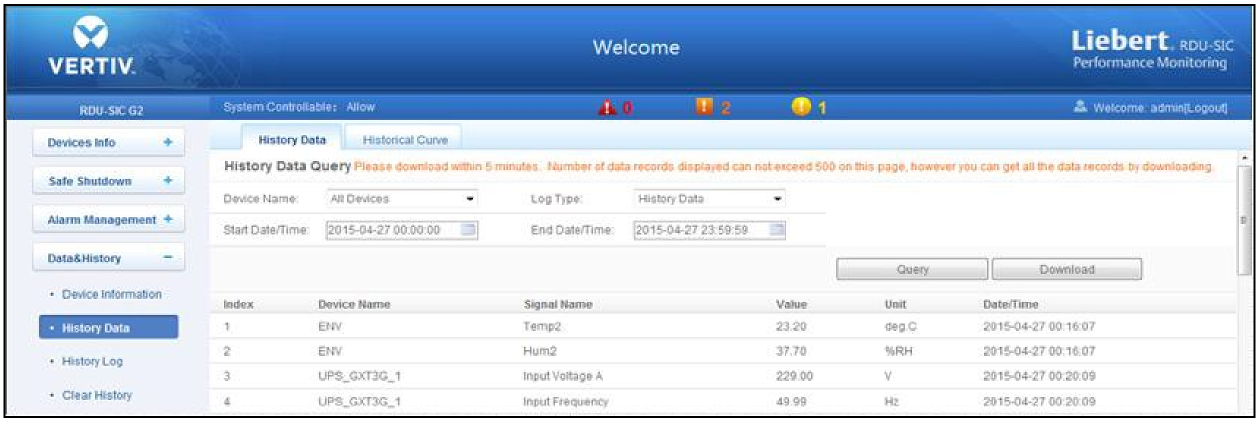
Export SNMP MIB

Device Type ENP_RDU[DUMMY]

History Data

Click the *History Data* under the Data and History menu, the page shown in **Figure 3.32** on the facing page appears. The page has two tabs: History Data and Historical Curve.

Figure 3.32 History Data



System Controllable: Allow

History Data Query Please download within 5 minutes. Number of data records displayed can not exceed 500 on this page, however you can get all the data records by downloading.

Device Name: All Devices

Log Type: History Data

Start Date/Time: 2015-04-27 00:00:00

End Date/Time: 2015-04-27 23:59:59

Index	Device Name	Signal Name	Value	Unit	Date/Time
1	ENV	Temp2	23.20	deg.C	2015-04-27 00:16:07
2	ENV	Hum2	37.70	%RH	2015-04-27 00:16:07
3	UPS_GXT3G_1	Input Voltage A	229.00	V	2015-04-27 00:20:09
4	UPS_GXT3G_1	Input Frequency	49.99	Hz	2015-04-27 00:20:09

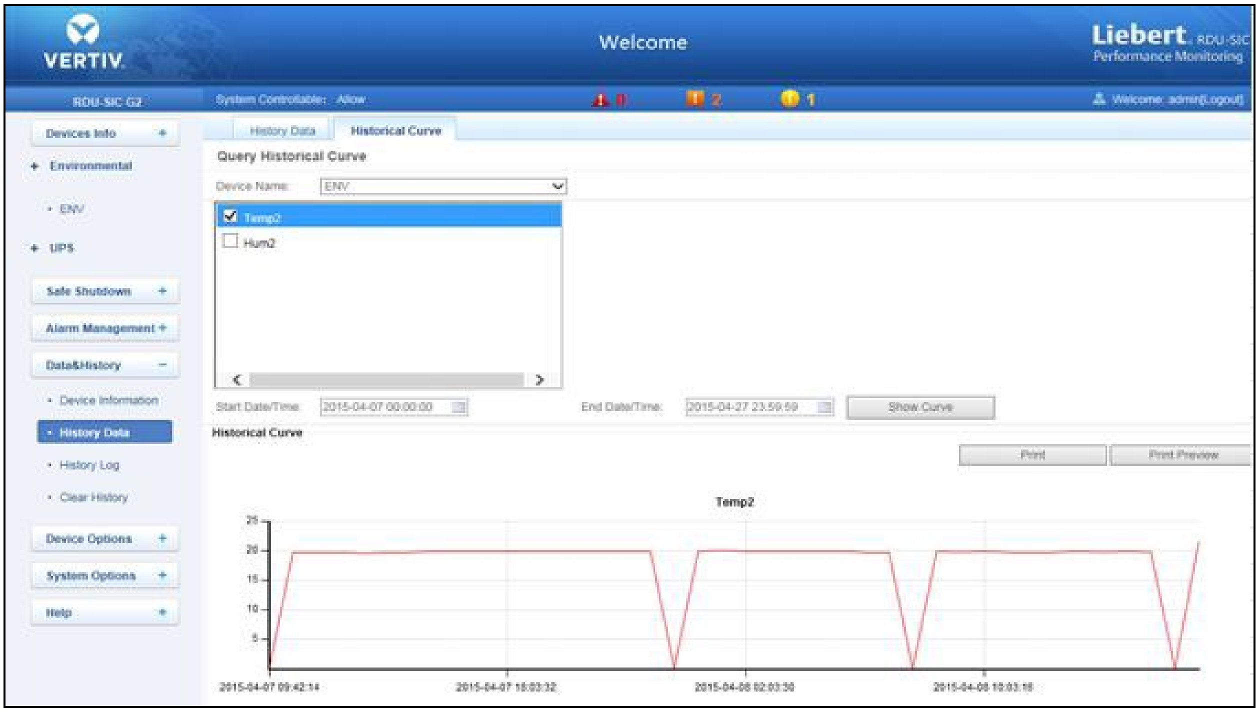
History Data

As shown in Figure 3.32 above , 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 2014-07-30 00:00:00 to 2014-07-30 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 3.33 below , choose a device (for instance, 'ENV') and the query type (for instance, 'Temp2'), and set the start time and the end time (for instance, from 2014-07-30 00:00:00 to 2014-07-30 23:59:59). Then click the *Show Curve* button, if history data are queried, a historical curve of the signal will be shown.

Figure 3.33 Historical Curve



System Controllable: Allow

Query Historical Curve

Device Name: ENV

☑ Temp2

□ Hum2

Start Date/Time: 2015-04-07 00:00:00

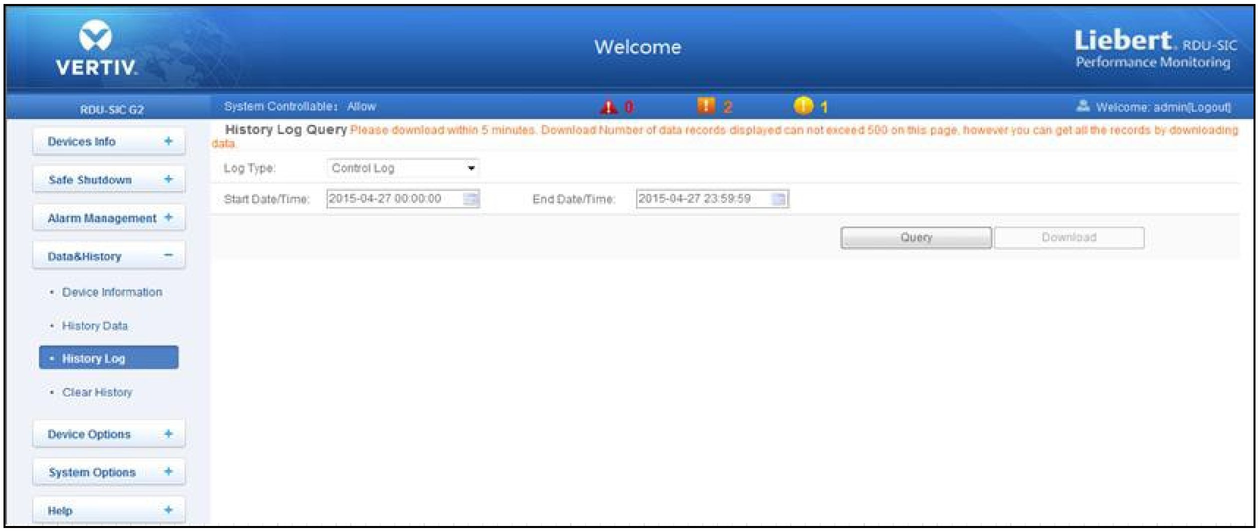
End Date/Time: 2015-04-27 23:59:59

Historical Curve

History Log

Click the *History Log* under the Data and History menu, the page shown in Figure 3.34 below pops up.

Figure 3.34 History Log



History Log Query Please download within 5 minutes. Download Number of data records displayed can not exceed 500 on this page, however you can get all the records by downloading data.

Log Type: Control Log

Start Date/Time: 2015-04-27 00:00:00

End Date/Time: 2015-04-27 23:59:59

On the page shown in History Log above , choose the log type (for instance, 'Control Log') and set the start time and the end time (for instance, from 2014-07-30 00:00:00 to 2014-07-30 23:59:59). Then click the *Query* button, all control 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.

3.4.5 Device Options

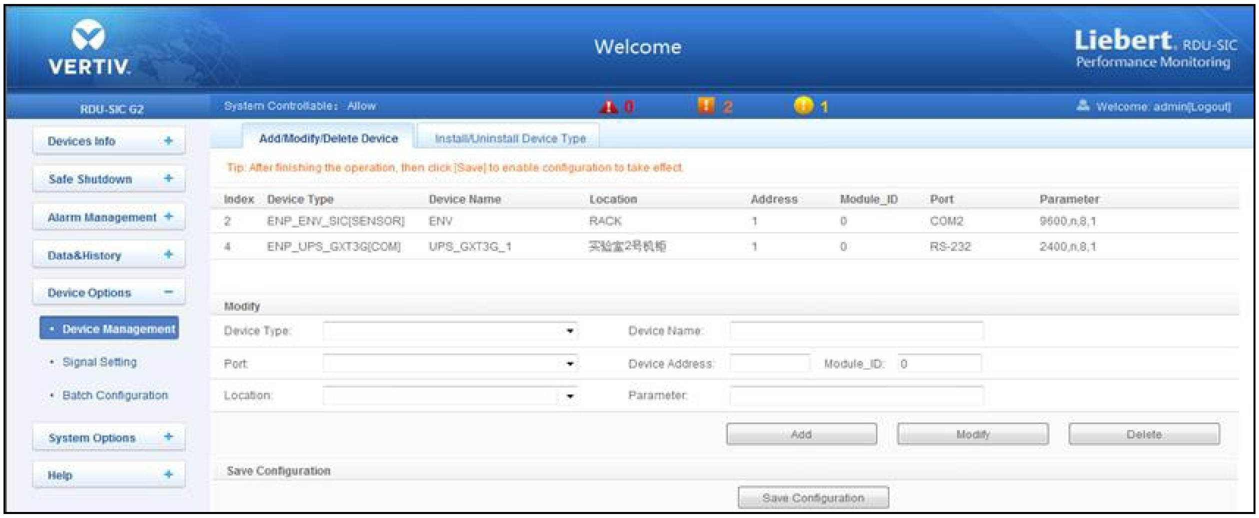
On the RDU-SIC G2 homepage, click *Device Options* in the left part, three submenus will appear, including Device Management, Signal Setting, and Batch Configuration.

Device Management

Add/Modify/Delete Device

Click the *Device Management* under the Device Options menu, the page shown in Figure 3.35 on the facing page pops up.

Figure 3.35 Add/Modify/Delete Equipment



Tip: After finishing the operation, then click [Save] to enable configuration to take effect.

Index	Device Type	Device Name	Location	Address	Module_ID	Port	Parameter
2	ENP_ENV_SIC[SENSOR]	ENV	RACK	1	0	COM2	9600,n,8,1
4	ENP_UPS_GXT3G[COM]	UPS_GXT3G_1	实验室2号机柜	1	0	RS-232	2400,n,8,1

Modify

Device Type:

Device Name:

Port:

Device Address:

Module_ID: 0

Location:

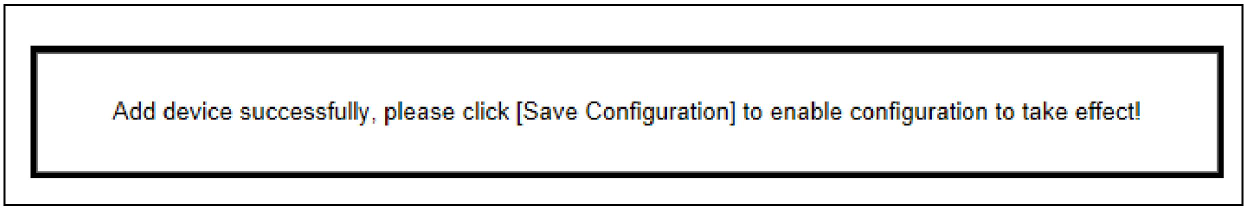
Parameter:

Save Configuration

As shown in **Figure 3.35** above , you can add/modify/delete a new device, the procedures are as follows:

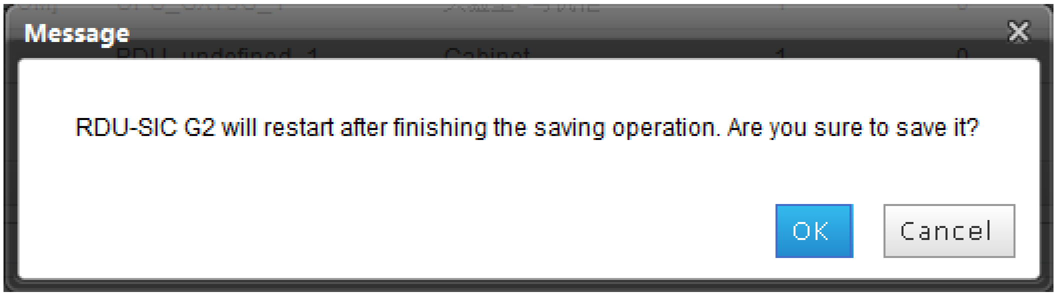
1. Adding a New Device:
   a. Choose the device type in the Device Type textbox.
   b. Type the device name in the Device Name textbox, or use the default device name.
   c. After the device type is chosen, the drop-down box of port will list the default port number(s) of the device type automatically; if the device type is not chosen, the port number cannot be chosen.
   d. Type 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.
   e. Choose or type the device location.
   f. Type 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.
   g. Click the *Add* button, the page shown in Prompt information 1 in **Figure 3.36** below appears, at the same time, a piece of new device information will be added in the device list.
   h. Click the *Save Configuration* button, the page shown in Prompt information 2 in **Figure 3.37** on the next page appears.
   If clicking the *Cancel* button, the added equipment fails; if clicking *OK*, the dialog box of Security authentication pops up, as shown in **Figure 3.13** on page 20 .

Figure 3.36 Prompt Information 1



Add device successfully, please click [Save Configuration] to enable configuration to take effect!

Figure 3.37 Prompt Information 2

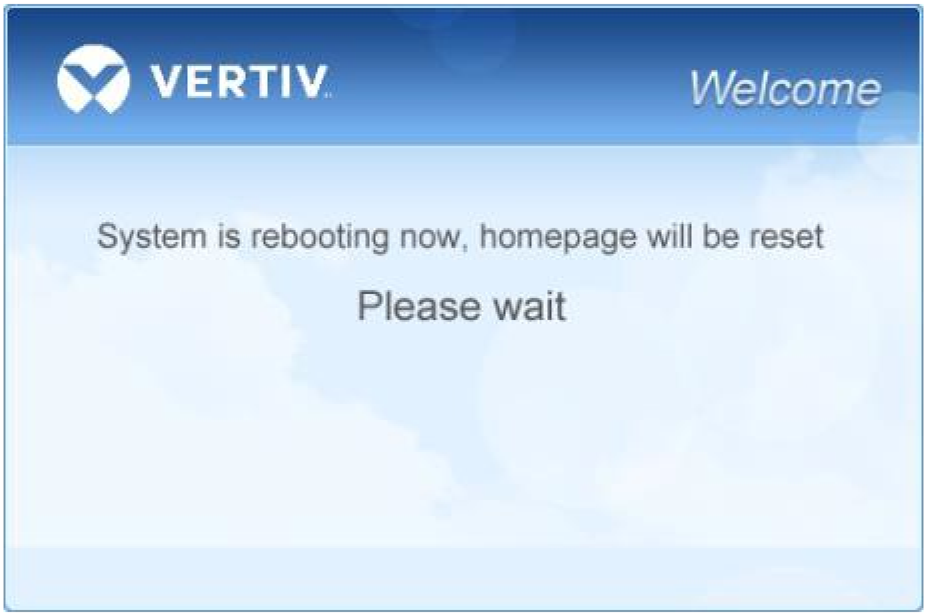


Message

RDU-SIC G2 will restart after finishing the saving operation. Are you sure to save it?

i. Type the login password of current user, and click *OK*. The reboot page will be appearing as shown in Figure 3.38 below .
Once the system reboots is completed, adding a device becomes effective.

Figure 3.38 Reboot Page



System is rebooting now, homepage will be reset

Please wait

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

NOTE: Up to four intelligent devices (excluding RDU-SIC G2 itself) can be added in the system by default.

2. Deleting a Device:
   a. Choose the device which needs to be deleted from the device list.
   b. Click the *Delete* button to delete the device.
   c. 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: If the device information has been modified before clicking the Delete button, it cannot be deleted.

3. Modifying a Device:

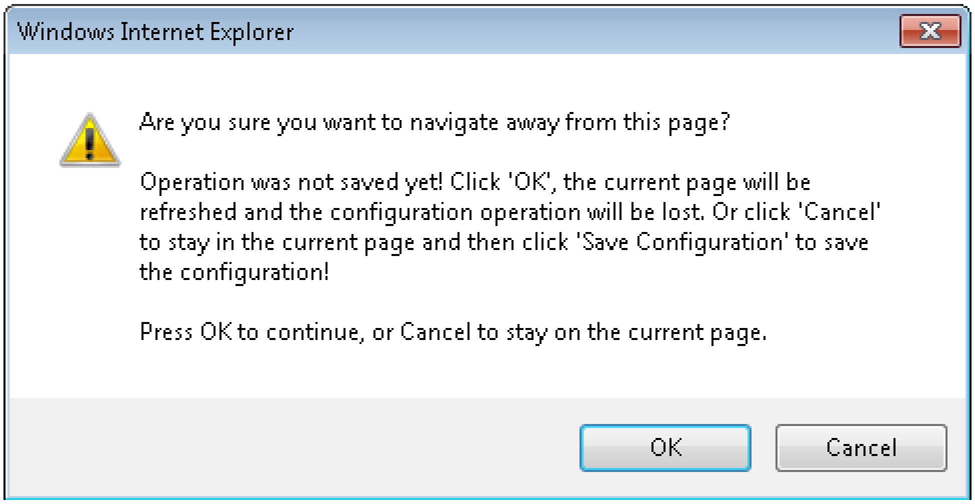
a. Choose the device which needs to be modified to the device list.

b. Modify the device information.

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

d. 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 of saving the configuration as shown in Figure 3.39 below .

Figure 3.39 Prompt information 3



Windows Internet Explorer

Are you sure you want to navigate away from this page?

Operation was not saved yet! Click 'OK', the current page will be refreshed and the configuration operation will be lost. Or click 'Cancel' to stay in the current page and then click 'Save Configuration' to save the configuration!

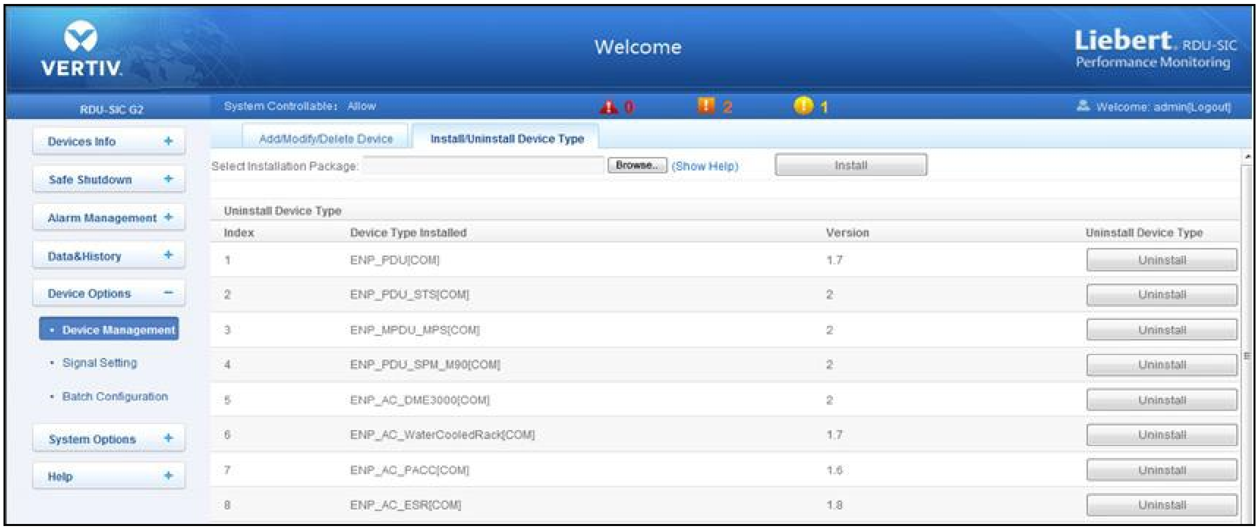
Press OK to continue, or Cancel to stay on the current page.

NOTE: All the operations can save at one time, when clicking the save configuration button.

Install/Uninstall Device Type

Click the *Device Management* under the Device Options menu, and then click the *Install/Uninstall Device Type* tab, the page shown in Figure 3.40 on the next page pops up.

Figure 3.40 Install/Uninstall Device Type



System Controllable: Allow

Select Installation Package:

Uninstall Device Type

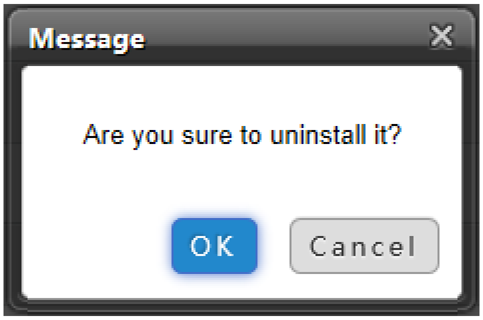
Index	Device Type Installed	Version	Uninstall Device Type
1	ENP_PDU[COM]	1.7	Uninstall
2	ENP_PDU_STS[COM]	2	Uninstall
3	ENP_MPDU_MPS[COM]	2	Uninstall
4	ENP_PDU_SPM_M90[COM]	2	Uninstall
5	ENP_AC_DME3000[COM]	2	Uninstall
6	ENP_AC_WaterCooledRack[COM]	1.7	Uninstall
7	ENP_AC_PACC[COM]	1.6	Uninstall
8	ENP_AC_ESR[COM]	1.8	Uninstall

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.

NOTE: More than 64 devices doest not supported by the system as it depends on the available system memory and the size of driver configuration packages.

The page displays the installed device type information in the lower right part. The confirming dialog box appears when clicking the Uninstall button as shown in Figure 3.41 below .

Figure 3.41 Confirming Dialog Box



Are you sure to uninstall it?

Click *OK*. The dialog box of Security authentication appears as shown in Figure 3.13 on page 20 . Then type the login password of current user, and click *OK* to uninstall the corresponding equipment type.

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

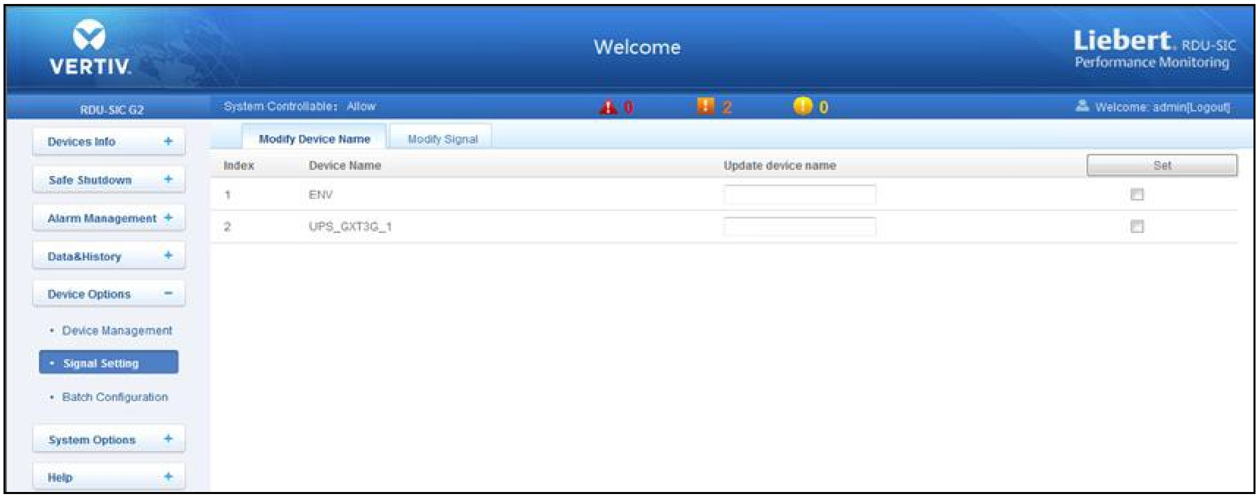
If the installation pack has no version information, or the version information does not match the software version, the device type cannot be installed.

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* under the Device Options menu, the page shown in **Figure 3.42** below below appears.

Figure 3.42 Modify Device Name

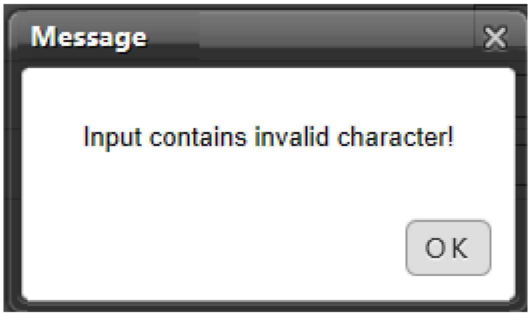


Index	Device Name	Update device name	Set
1	ENV		□
2	UPS_GXT3G_1		□

On the page shown in **Figure 3.42** above , you can modify the device name. Type 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. If other characters are typed, the prompt box shown in Figure 3.43 below will appear.

Figure 3.43 Prompt Box of Invalid Characters

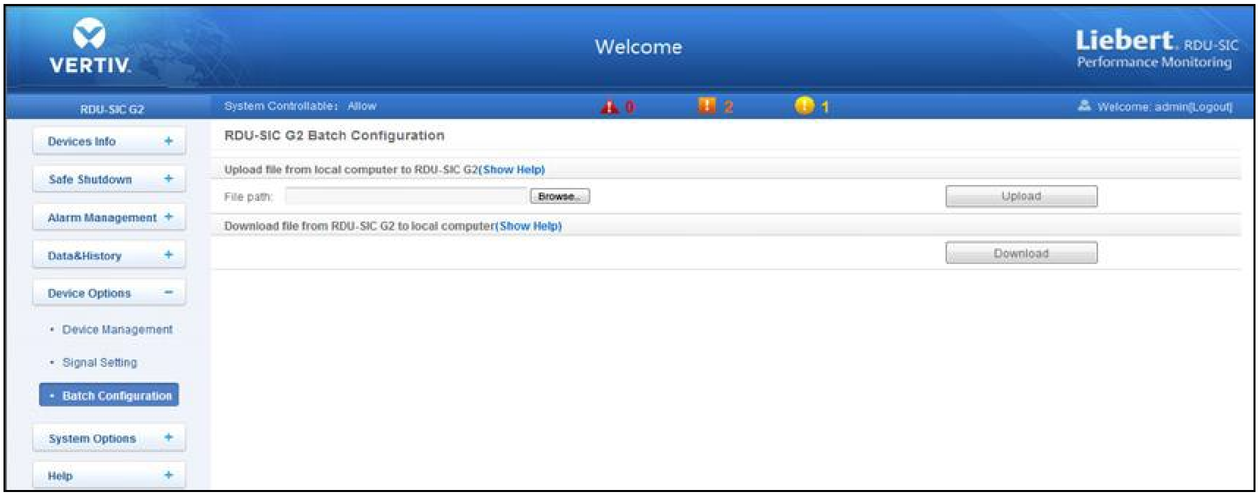


Input contains invalid character!

Batch Configuration

Click the *Batch Configuration* under the Device Options menu, the page shown in **Figure 3.44** on the next page appears.

Figure 3.44 Batch Configuration



System Controllable： Allow

RDU-SIC G2 Batch Configuration

Upload file from local computer to RDU-SIC G2(Show Help)

File path:

Download file from RDU-SIC G2 to local computer(Show Help)

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

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

The batch configuration file is encrypted after being downloaded to local.

3.4.6 System Options

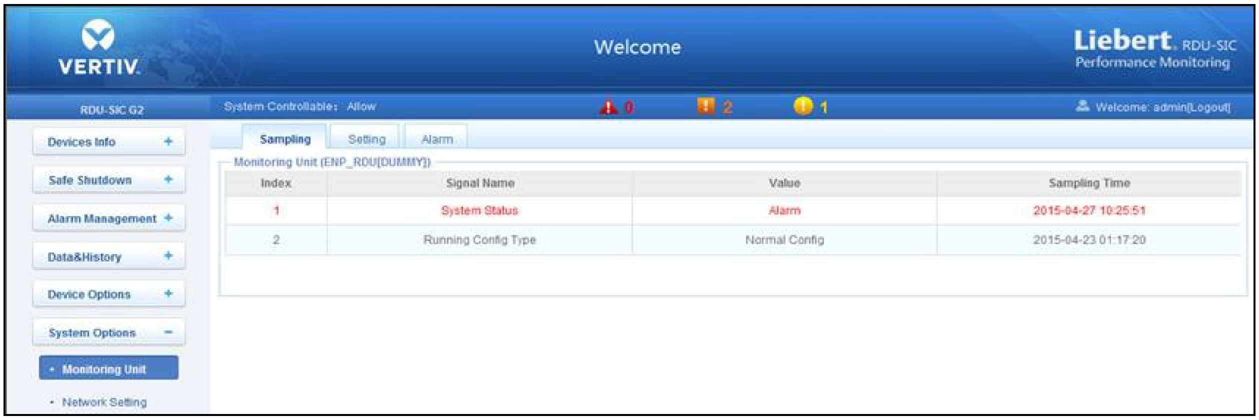
On the RDU-SIC G2 homepage, click the *System Options* menu in the left pane, eight submenus appear, including:

- Monitoring Unit
- Network Setting
- User Management
- Date/Time Setting
- Restore System
- Site Setting
- System Upgrade and System Title.

Monitoring Unit

The Monitoring Unit is used to set the signals of RDU-SIC G2 system, including Sampling, Setting and Alarm signals, the page is shown in Figure 3.45 on the facing page .

Figure 3.45 Sampling Tab



System Controllable: Allow

Monitoring Unit (ENP_RDU[DUMMY])

Index	Signal Name	Value	Sampling Time
1	System Status	Alarm	2015-04-27 10:25:51
2	Running Config Type	Normal Config	2015-04-23 01:17:20

As for the operation method of the three tabs of Sampling, Setting and Alarm on the Monitoring unit page, refer to Device Info on page 21 .

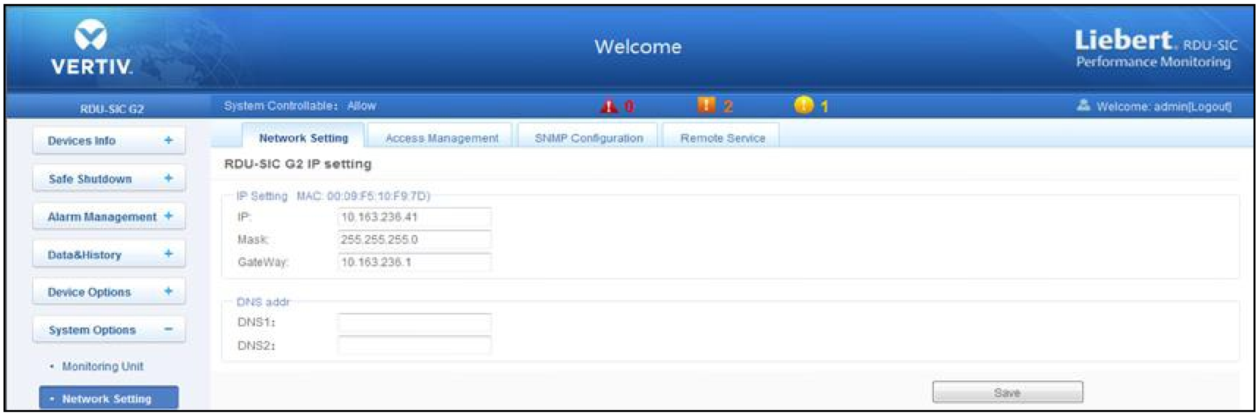
NOTE: On the Setting tab, when an alarm occurs and if you set 'Blocked' for Outgoing Alarm Blocked, then it will be blocked. In this case, the page only displays the alarm signals for current alarms but does not send alarm notifications and after the alarm disappears, it will not be saved in the history alarm. The 'Blocked' setting for Outgoing Alarm Blocked will be automatically cleared in 24h.

Network Setting

Network Setting

Click the *Network Setting* under the System Options menu, the page shown in **Figure 3.46** below appears..

Figure 3.46 IP Setting



System Controllable: Allow

RDU-SIC G2 IP setting

IP Setting MAC: 00:09:F5:10:F9:7D)

IP: 10.163.236.41

Mask: 255.255.255.0

GateWay: 10.163.236.1

DNS addr

DNS1:

DNS2:

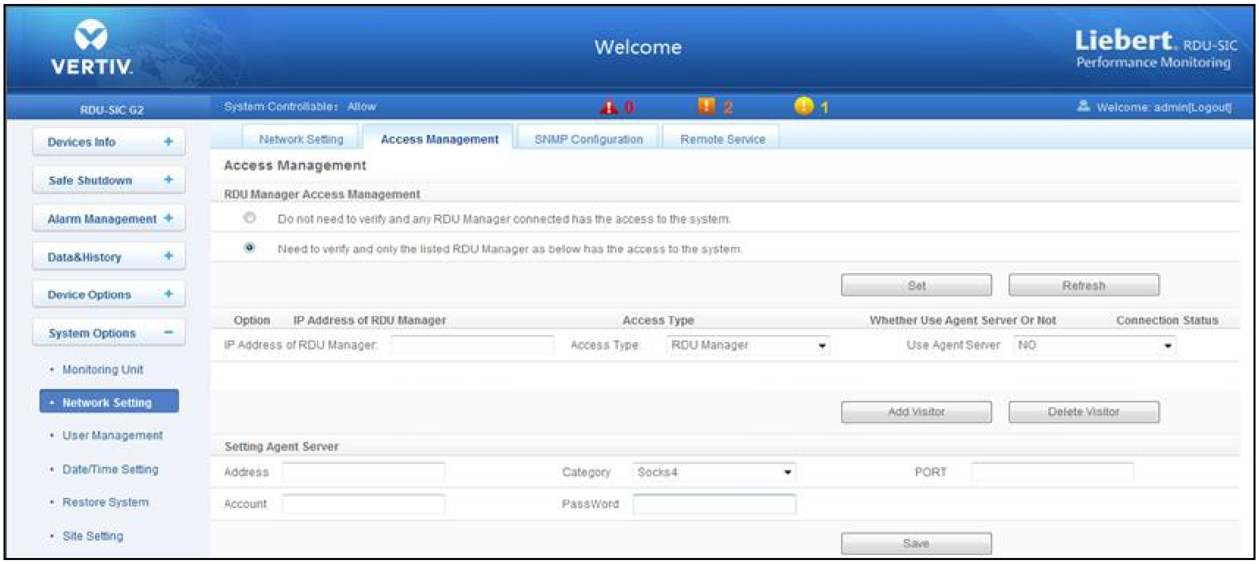
Configure the network parameters, such as IP addressing mode, IP, Mask, GateWay, DNS1 (Preferred DNS server) and DNS2 (Alternate DNS server). Click the *Save* button to save the setting.

NOTE: After modifying the IP address, the system will jump to the new IP address by default. You must use the new IP address to re-login the Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card.

Access Management

Click the *Network Setting* under the System Options menu, and then click the *Access Management* tab, the page shown in Figure 3.47 below will appear.

Figure 3.47 Access Management



System Controllable: Allow

Access Management

RDU Manager Access Management

○ Do not need to verify and any RDU Manager connected has the access to the system.

● Need to verify and only the listed RDU Manager as below has the access to the system.

Option	IP Address of RDU Manager	Access Type	Whether Use Agent Server Or Not	Connection Status

IP Address of RDU Manager: Access Type: RDU Manager Use Agent Server: NO

Setting Agent Server

Address: Category: Socks4 PORT:

Account: PassWord:

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.

If you select to use an agent, you also need to configure the agent server in the event of adding a visitor.

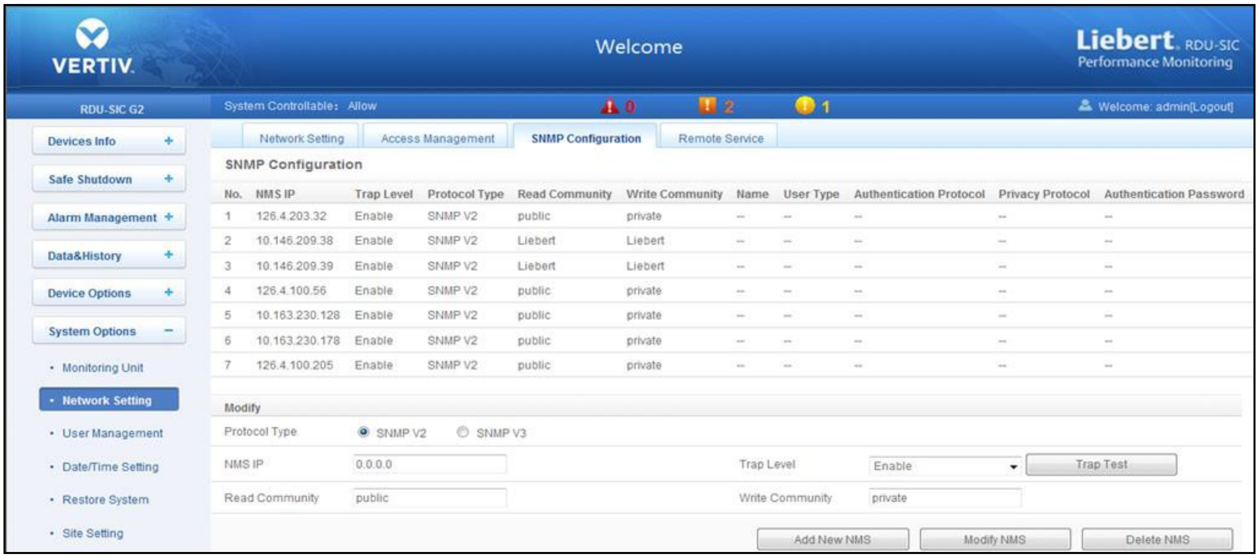
SNMP Configuration

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

As shown in Figure 3.48 on the facing page , the specific setting method of SNMP V2 is as follows:

1. Set NMS IP (host IP address of SNMP agent data receiving end).
2. Set Trap Level as 'Enable' or 'Disable'.
3. Keep other parameters as it is.

Figure 3.48 SNMP V2 Setting



SNMP Configuration

No.	NMS IP	Trap Level	Protocol Type	Read Community	Write Community	Name	User Type	Authentication Protocol	Privacy Protocol	Authentication Password
1	126.4.203.32	Enable	SNMP V2	public	private	--	--	--	--	--
2	10.146.209.38	Enable	SNMP V2	Liebert	Liebert	--	--	--	--	--
3	10.146.209.39	Enable	SNMP V2	Liebert	Liebert	--	--	--	--	--
4	126.4.100.56	Enable	SNMP V2	public	private	--	--	--	--	--
5	10.163.230.128	Enable	SNMP V2	public	private	--	--	--	--	--
6	10.163.230.178	Enable	SNMP V2	public	private	--	--	--	--	--
7	126.4.100.205	Enable	SNMP V2	public	private	--	--	--	--	--

Modify

Protocol Type ● SNMP V2 ○ SNMP V3

NMS IP 0.0.0.0 Trap Level Enable

Read Community public Write Community private

As shown in Figure 3.49 on the next page , the specific setting method of SNMP V3 is as follows:

1. Set NMS IP (host IP address of SNMP agent data receiving end).
2. Set the Trap Level as 'Enable' or 'Disable'.
3. Set the Name.
4. Set the User Type as ‘Authenticated and Encrypted’, ‘Authenticated and Not Encrypted’, ‘Not Authenticated and Not Encrypted’.
5. Select Authentication Protocol as ‘MD5’, ‘SHA’.
6. Select Privacy Protocol as ‘DES’;
7. Set Self-define Authentication Password and Privacy Password.
8. After parameter setting, click the *Add* button to add NMS.

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

If you select ‘Not Authenticated & Not Encrypted’ for User Type, the drop-down boxes of Authentication Protocol and Privacy Protocol will become gray and then you cannot set them;

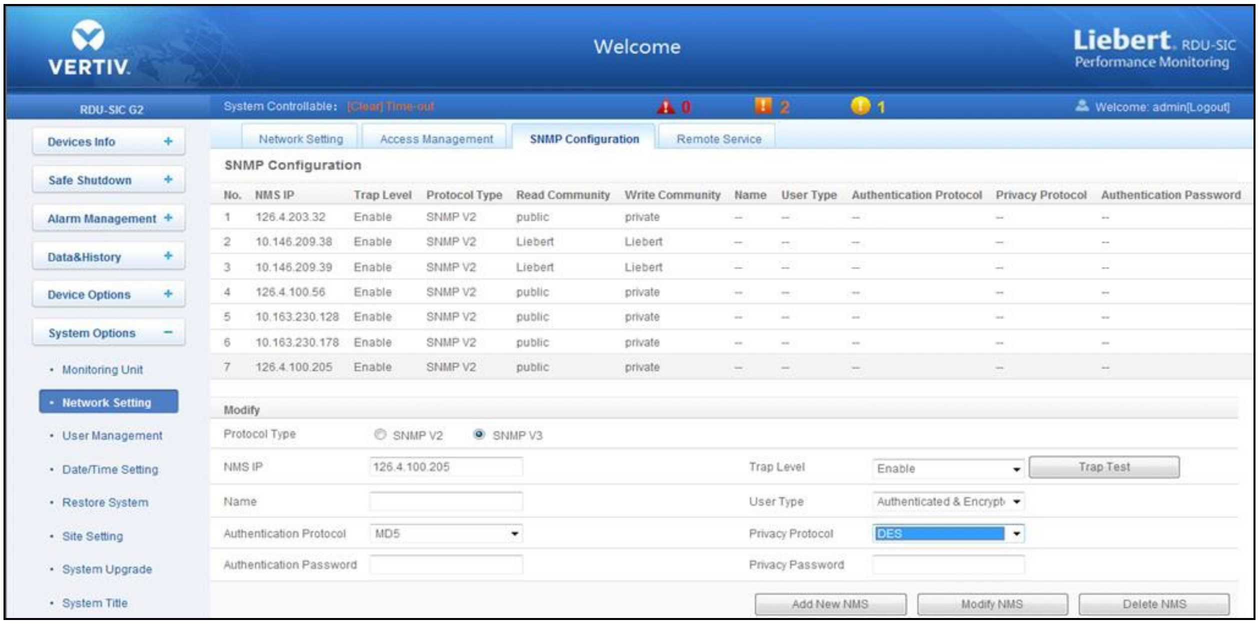
Currently, only ‘DES’ is supported for Privacy Protocol.

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.

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 3.49 SNMP V3 Setting



SNMP Configuration

No.	NMS IP	Trap Level	Protocol Type	Read Community	Write Community	Name	User Type	Authentication Protocol	Privacy Protocol	Authentication Password
1	126.4.203.32	Enable	SNMP V2	public	private	--	--	--	--	--
2	10.146.209.38	Enable	SNMP V2	Liebert	Liebert	--	--	--	--	--
3	10.146.209.39	Enable	SNMP V2	Liebert	Liebert	--	--	--	--	--
4	126.4.100.56	Enable	SNMP V2	public	private	--	--	--	--	--
5	10.163.230.128	Enable	SNMP V2	public	private	--	--	--	--	--
6	10.163.230.178	Enable	SNMP V2	public	private	--	--	--	--	--
7	126.4.100.205	Enable	SNMP V2	public	private	--	--	--	--	--

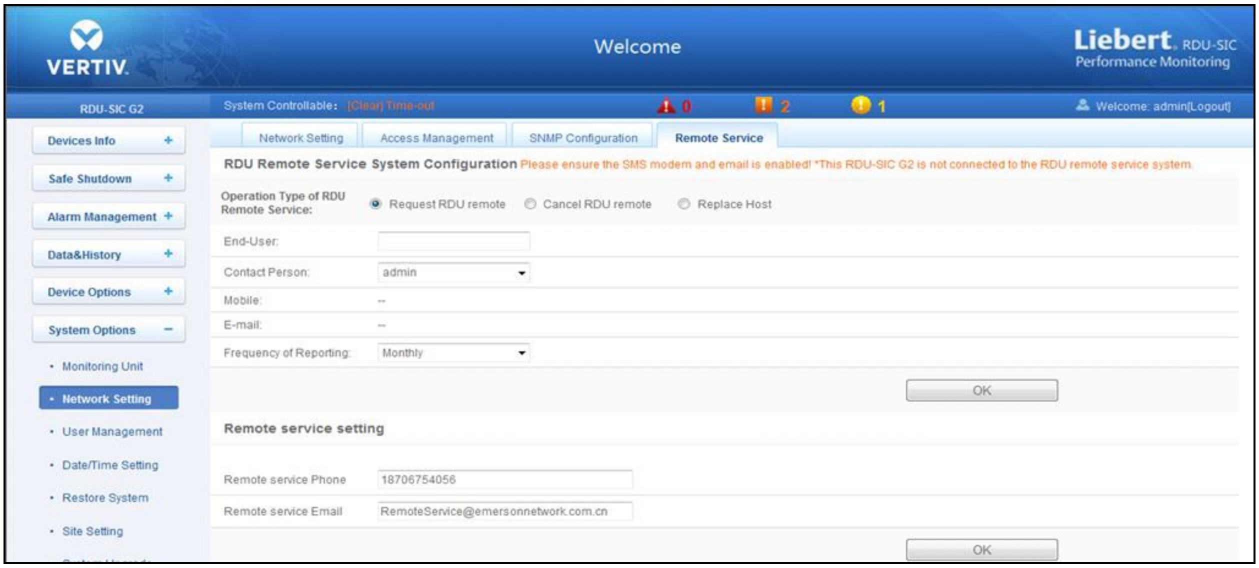
Modify

Protocol Type	○ SNMP V2 ● SNMP V3		
NMS IP	126.4.100.205	Trap Level	Enable
Name		User Type	Authenticated & Encrypt
Authentication Protocol	MD5	Privacy Protocol	DES
Authentication Password		Privacy Password	

Remote Service

Click the *Network Setting* under the System Options menu, and then click the *Remote Service* tab, the page shown in **Figure 3.50** below appears.

Figure 3.50 Remote Service Setting



RDU Remote Service System Configuration Please ensure the SMS modem and email is enabled! *This RDU-SIC G2 is not connected to the RDU remote service system.

Operation Type of RDU Remote Service:	● Request RDU remote ○ Cancel RDU remote ○ Replace Host
End-User:	
Contact Person:	admin
Mobile:	--
E-mail:	--
Frequency of Reporting:	Monthly

Remote service setting

Remote service Phone	18706754056
Remote service Email	RemoteService@emersonnetwork.com.cn

The remote service setting includes three parts: Request RDU remote, Cancel RDU remote, and Replace Host. Meanwhile, you can set the communication parameters of remote service system.

1. Request RDU remote: used to establish remote service relationship
   a. Type 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 below in this section for detailed setting method.

   c. Choose Frequency of Reporting: 'Monthly', 'Seasonal';
   d. Click *OK* to send the remote service request.

2. 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.

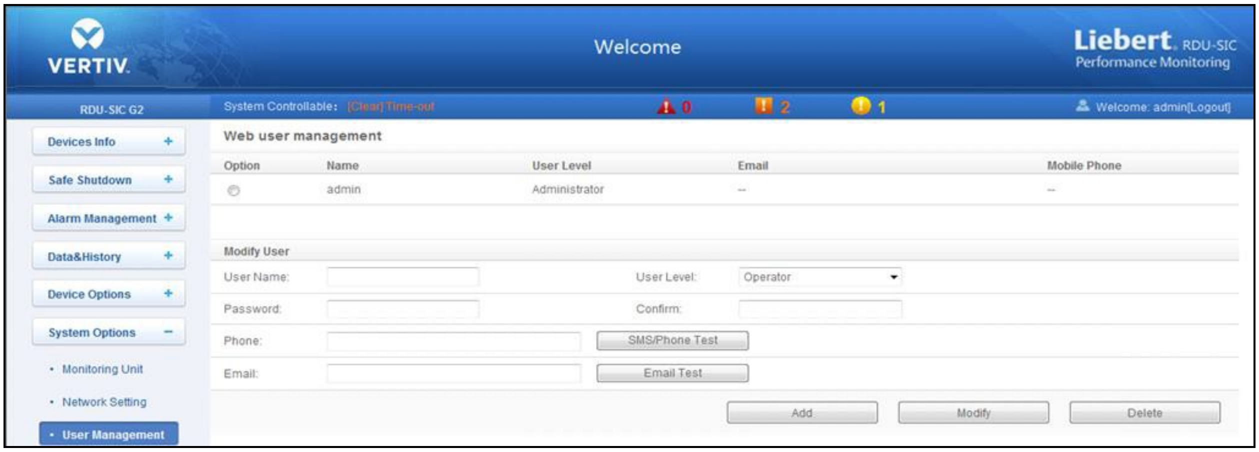
3. Replace Host: used to replace the local host during remote service

   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.

User Management

Click the *User Management* submenu under the System Options menu, the page shown in **Figure 3.51** below appears.

Figure 3.51 User Management



Web user management

Option	Name	User Level	Email	Mobile Phone
○	admin	Administrator	--	--

Modify User

User Name:
User Level: Operator
Password:
Confirm:
Phone:
Email:

On the page shown in **Figure 3.51** above , you can add user, modify user, and delete user.

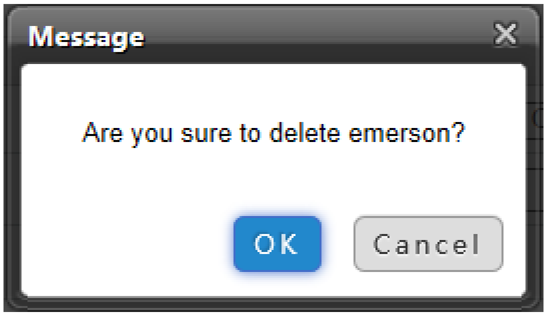
1. Add User
   a. Type username in the User Name textbox;
   b. In the User Level select the user type from the available list;
   c. Configure the user password, which cannot be vacant and should contain at least six letters or digits;
   d. Re-type the password in the Confirm textbox;
   e. (Optional) Type the user telephone number, which can use the following digits and characters: 0123456789, +;
   f. (Optional) Type the email address;

g. Click the *Add* button, the dialog box of Security authentication pops up, as shown in Figure 3.13 on page 20 . Type the login password of current user, and click *OK* to add a new user.

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

2. Delete User
   a. Choose the user which needs to be deleted in the username list;
   b. Click the *Delete* button to pop up the confirming dialog box, as shown in Figure 3.52 below ;

Figure 3.52 Confirming Dialog Box



Message

Are you sure to delete emerson?

   c. Click *OK*, the dialog box of Security authentication pops up, as shown in Figure 3.13 on page 20 . Type the login password of current user, and click *OK* to delete the chosen user.

NOTE: The admin level user cannot be deleted.

3. Modify User
   a. Choose the user which needs to be modified in the username list;
   b. Modify the user information;
   c. Click the *Modify* button, the dialog box of Security authentication pops up, as shown in Figure 3.13 on page 20 . Type the login password of current user, and click *OK* to make the modified user information effective.

Users who access RDU-SIC G2 can be divided into four user groups, and they have different security level and user authority, see Table 3.1 below for detailed information.

Table 3.1 User Security Level

Security Level	User Group	User Authority
Level A	Browser	All users can browse equipment information
Level B	Operator	The operators can send control command to intelligent equipment
Level C	Engineer	The engineers can get the following access: send control command to intelligent equipment; Browse, control and modify parameters; Download files; Modify user information of their own.
Level D	Administrator	• The administrator can get full access: Send control command to intelligent equipment; Brows, control and modify parameters; Upload and download files; Modify, add and delete user information; AC teamwork parameter setting; • System upgrade

On the page shown in **Figure 3.51** on page 43 , 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 in Alarm management on page 25 for details.

4. SMS/Phone Test

   Type 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, please check that the telephone number is correct and the SMS Modem is properl connected.

5. Email Alarm Notify Test

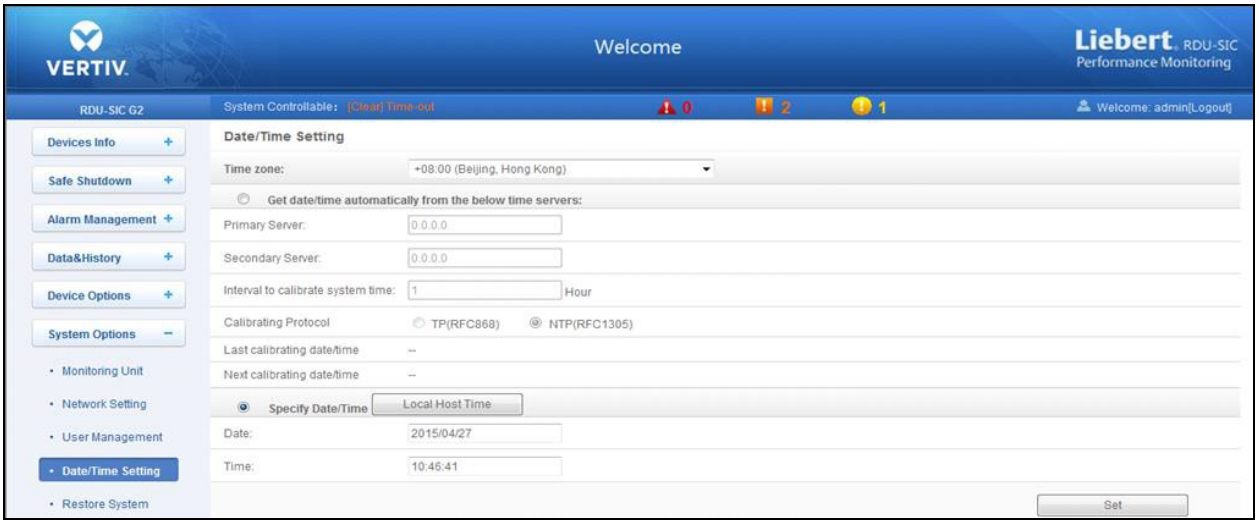
   Type the email address in the Email field, and click the Email Test button to test that the email address of current user is correct. If users receive the test email, the test is successful; if not, the test fails, please check that the information above is correctly typed.

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

Date/Time Setting

Clicking the *Date/Time Setting* under the System Options menu can synchronize the time. On the page shown in **Figure 3.53** below , RDU-SIC 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 3.53 Date/Time Setting



Date/Time Setting

Time zone: +08:00 (Beijing, Hong Kong)

○ Get date/time automatically from the below time servers:

Primary Server: 0.0.0.0

Secondary Server: 0.0.0.0

Interval to calibrate system time: 1 Hour

Calibrating Protocol ○ TP(RFC868) ● NTP(RFC1305)

Last calibrating date/time --

Next calibrating date/time --

● Specify Date/Time

Date: 2015/04/27

Time: 10:46:41

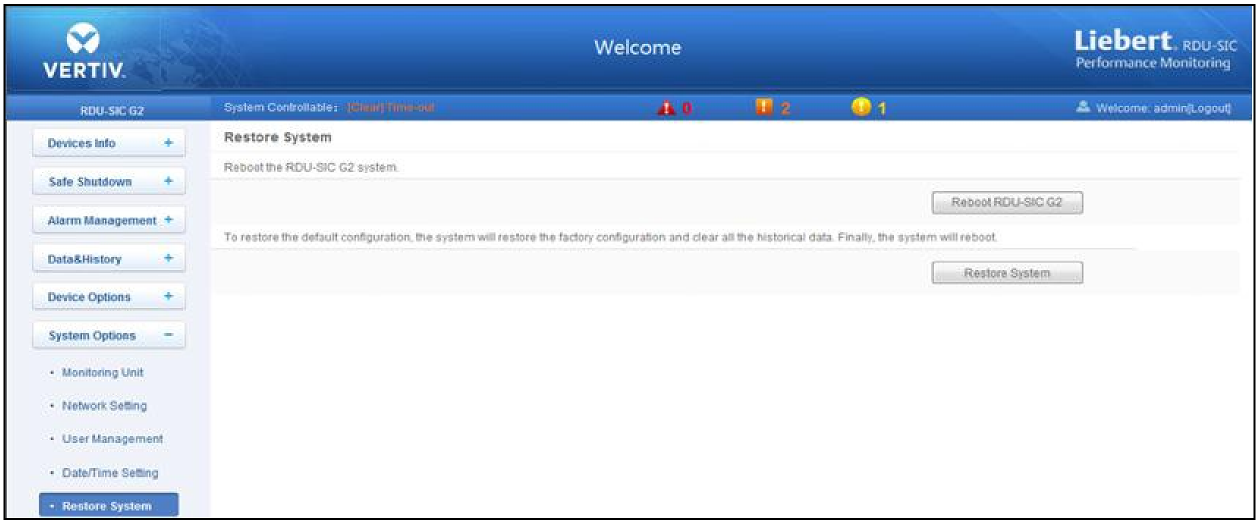
The RDU-SIC G2 can also get the local time. Choose Specify Date/Time, click the *Local Host Time* button to get the local time, and then click the *Set* button to make the new time effective.

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

Restore System

Click the *Restore System* under the System Options menu, the page shown in **Figure 3.54** on the next page .

Figure 3.54 Restore System



Reboot the RDU-SIC G2 system.

To restore the default configuration, the system will restore the factory configuration and clear all the historical data. Finally, the system will reboot.

Click the *Reboot RDU-SIC G2* button to reboot the system.

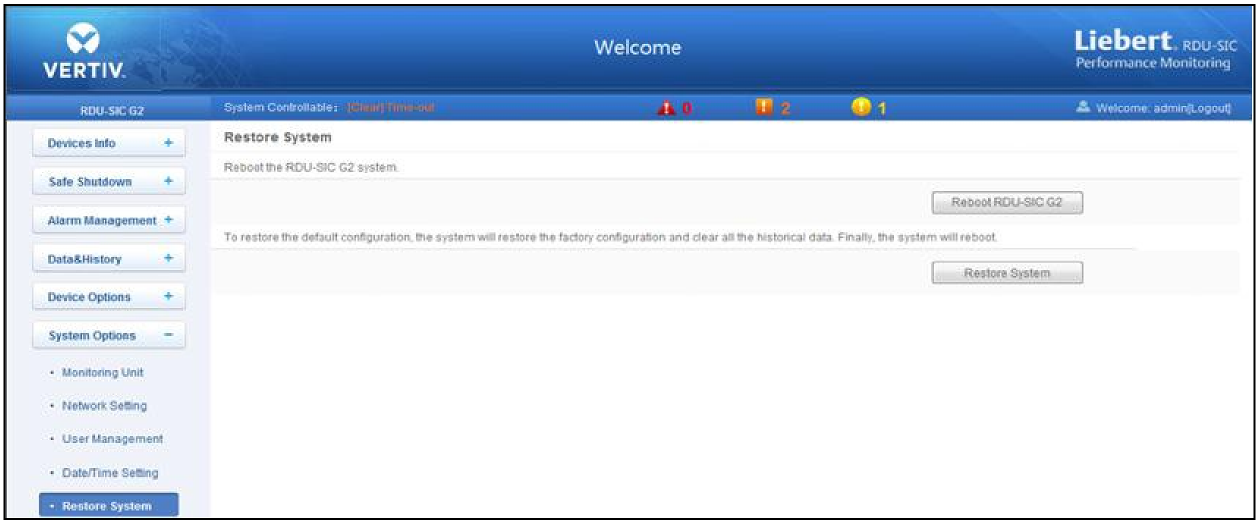
Click the *Restore System* button to restore all the default settings.

NOTE: If you use the restore function, the Liebert® IntelliSlot™ RDU-SIC G2 Card may lose the original configuration solution. After the restore operation, make sure to wait two minute for the RDU-SIC G2 conducting complete initializing work before re-accessing it through Web.

Site Setting

Click the *Site Setting* under the System Options menu, the page shown in Figure 3.55 below appears.

Figure 3.55 Site Information Setting



Reboot the RDU-SIC G2 system.

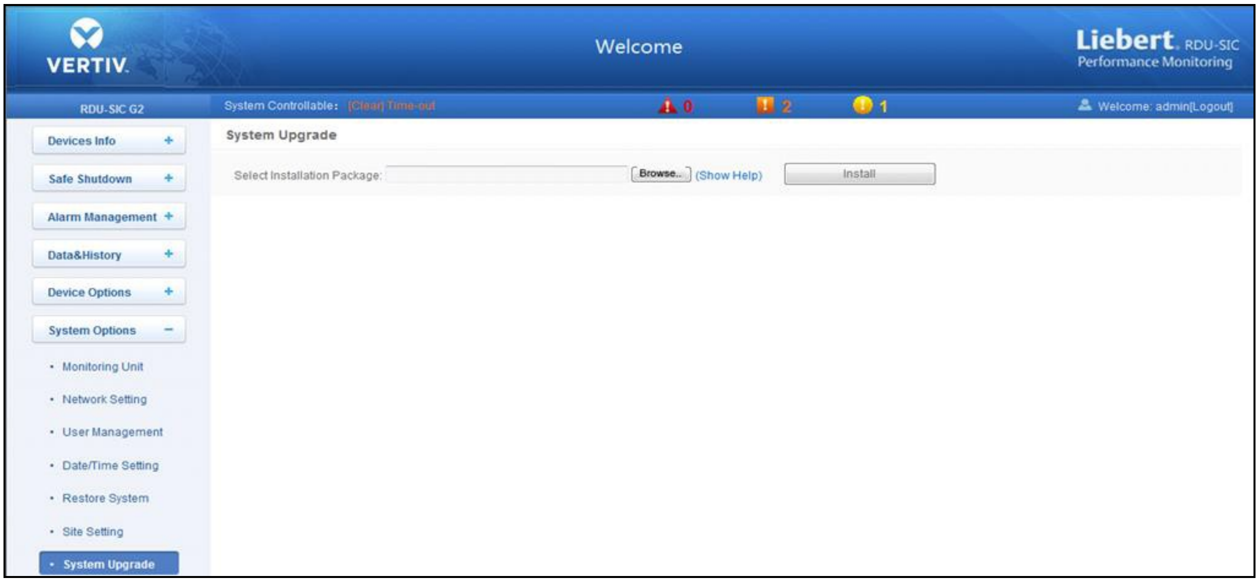
To restore the default configuration, the system will restore the factory configuration and clear all the historical data. Finally, the system will reboot.

On the page shown in Figure 3.55 above , you can modify the site information of Liebert® IntelliSlot™ RDU-SIC G2 Card, including Site Name, Site Location and Site Description.

System Upgrade

Click the *System Upgrade* under the System Options menu, the page shown in Figure 3.56 below appears.

Figure 3.56 System Upgrade



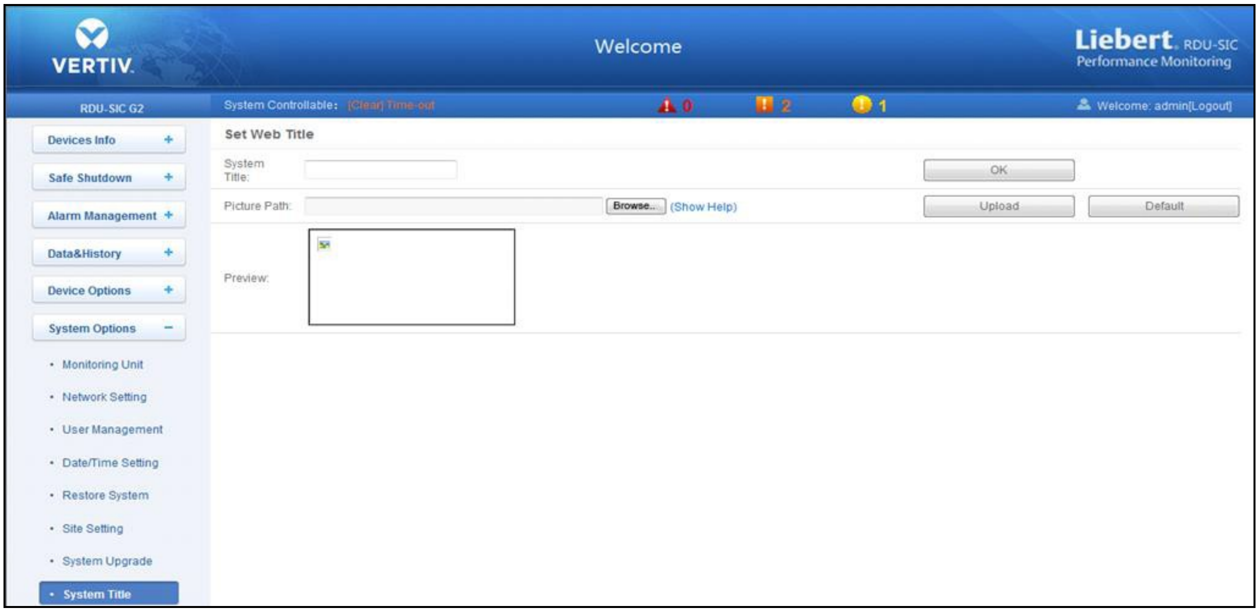
On the page shown in Figure 3.56 above , click the *Browse* button to download configure pack (.rdu file format) from the local catalogue, and then click the *Install* button to upgrade the system.

NOTE: The Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card supports incremental upgrading function.

System Title

Click the *System Title* under the System Options menu, the page shown in Figure 3.57 below appears.

Figure 3.57 System Title



As shown in Figure 3.57 on the previous page , you can replace the Logo picture in the upper right part by the uploading system Logo picture. Click the *Browse* button, choose the needed Logo picture, and click the *Upload* button to upload the file to RDU-SIC G2. Only [.gif], [.bmp], [.jpg] and [.png] format pictures are allowed, and the picture size should be less than 500Kb. Clicking the *Default* button can restore the default Logo picture.

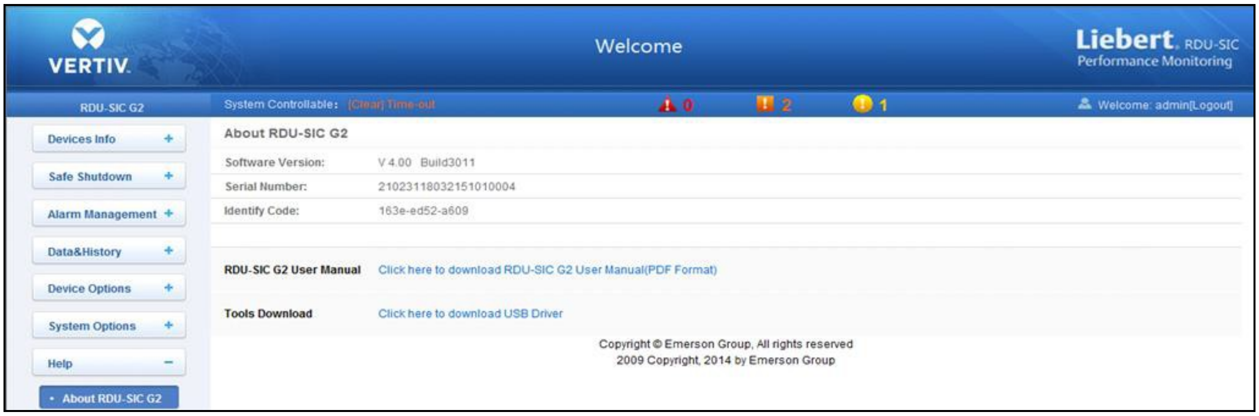
You can also modify the system title Welcome at the top of the page. Type the customized title in the System Title textbox and click *OK* to make it effective.

3.4.7 Help

On the RDU-SIC G2 homepage, click the *Help* menu in the left pane, one submenu appears as About RDU-SIC G2.

The page displays Software Version, Serial Number and Identify Code of RDU-SIC G2, as shown in Figure 3.58 below .

Figure 3.58 About RDU-SIC G2 Tab



System Controllable: [Clear] Time-out   0   2   1   Welcome: admin[Logout]

About RDU-SIC G2

Software Version:	V 4.00 Build3011
Serial Number:	21023118032151010004
Identify Code:	163e-ed52-a609
RDU-SIC G2 User Manual	Click here to download RDU-SIC G2 User Manual(PDF Format)
Tools Download	Click here to download USB Driver

Copyright © Emerson Group, All rights reserved
2009 Copyright, 2014 by Emerson Group

4 Maintenance

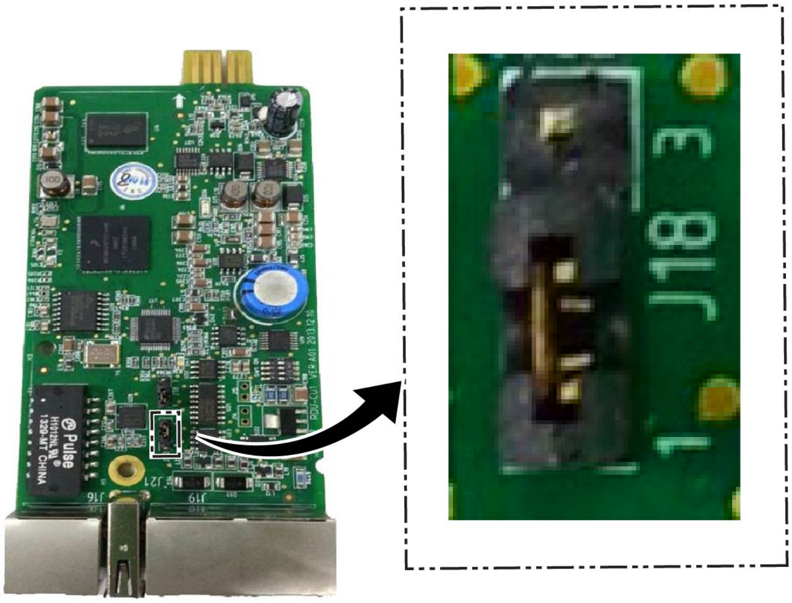
The maintenance of Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card includes restoring default setting and FAQ.

4.1 Restoring Default Setting

Restoring default setting can be finished through two modes: software or hardware. For software restoring, refer to Restore System on page 45 .

Hardware restoring includes restoring admin password (default username: ‘admin’, password: ‘Vertiv) and IP address of RDU-SIC G2 (the default IP address is 192.168.0.252). You can short pin2 and pin3 of jumper J18 on the RDU-SIC G2 card to complete hardware restoring. The jumper position is shown in **Figure 4.1** below .

Figure 4.1 Position of Jumper J18



4.2 FAQ

Q1: After RDU-SIC G2 is powered on, why the power indicator is not blinks/activates?

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

Q2: How to deal with that the abnormal communication of COM port ?

A: Check that the COM ports on the RDU-SIC G2 and the expansion card are RS-232/RS-485 adaptive ports; please ensure that the communication parameters are correctly configured.

Q3: How to deal with that there is no access to RDU-SIC G2 login page when the RDU-SIC G2 communication is normal?

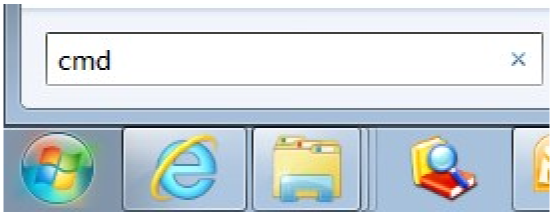
A: There are three measures to solve the problem:

1. Ensure that the IP address is correct;
   a. Please ensure that the network cable is connected to the correct port.
   b. Ensure that the IP address of RDU-SIC G2 is 192.168.0.252.
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:

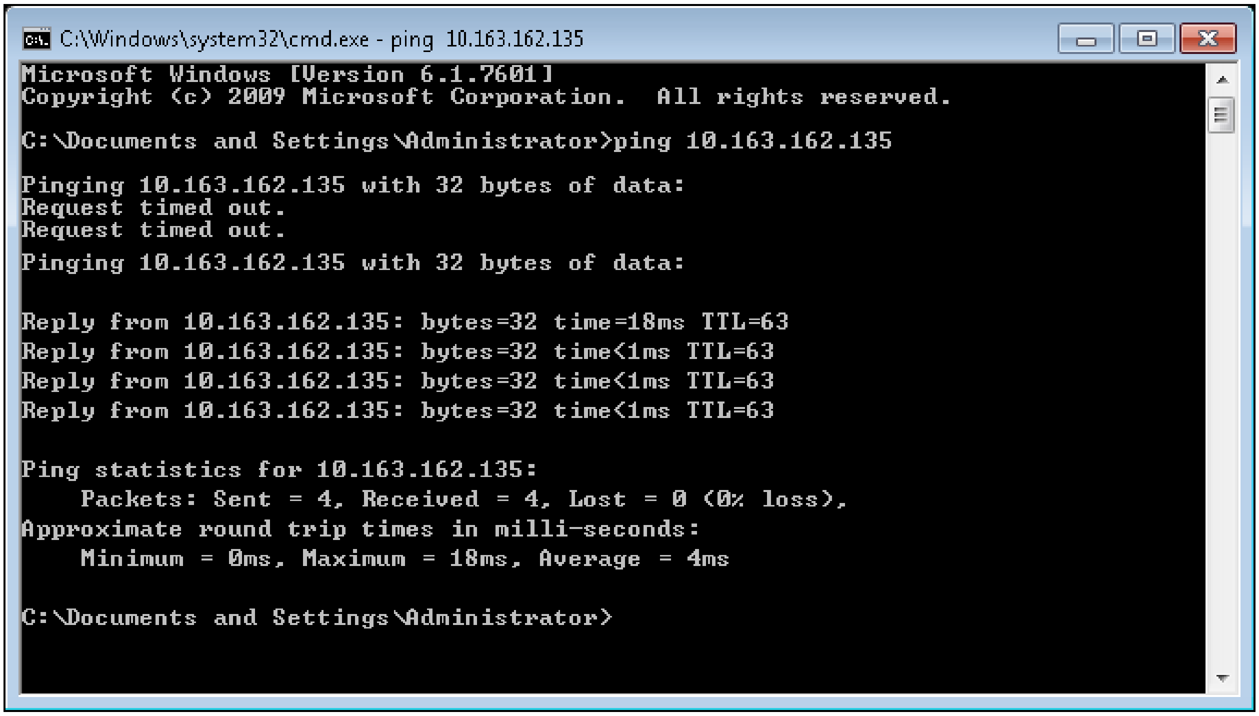
   a. Click the icon at the lower left corner, and type 'cmd' in the textbox, as shown in **Figure 4.2** below .

Figure 4.2 Typing 'cmd'



   b. Press the *Enter key*, the page shown in **Figure 4.3** 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 4.3 Communication Test



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Documents and Settings\Administrator>ping 10.163.162.135

Pinging 10.163.162.135 with 32 bytes of data:
Request timed out.
Request timed out.
Pinging 10.163.162.135 with 32 bytes of data:

Reply from 10.163.162.135: bytes=32 time=18ms TTL=63
Reply from 10.163.162.135: bytes=32 time<1ms TTL=63
Reply from 10.163.162.135: bytes=32 time<1ms TTL=63
Reply from 10.163.162.135: bytes=32 time<1ms TTL=63

Ping statistics for 10.163.162.135:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 4ms

C:\Documents and Settings\Administrator>
```

3. If the above-mentioned steps cannot handle the problem, please use the jumper cap on the card to restore default IP. Refer to **Table 2.1** on page 8 for the use of jumper cap.

4. Refer to Login Preparation on page 9 to complete relevant operations.

Q4: You have chosen the ocean blue theme, but the page still adopts crystal blue theme while you are viewing the webpage of the RDU-SIC 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.

Q5: 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 27 in Alarm Management.
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.

This page intentionally left blank

5 Appendices

Appendix A: Glossary

Abbreviation	Description
AC	Alternating Current
CA	Critical Alarm
DC	Direct Current
DI	Digital Input
IE	Internet Explorer, a Web browser developed by Microsoft@
FAQ	Frequently Asked Questions
FTP	File Transfer Protocol, used to transfer large chunks of data
HTML	Hypertext Mark-Up Language, used to create Web pages
HTTP	Hypertext Transfer Protocol, used to convey HTML
LED	Light Emitting Diode
Linux	A UNIX-like operating system with open source, developed under Free Software Foundation (FSF)
LLP	Local Language Package
LUI	Local User Interface
MA	Moderate Alarm
NA	No Alarm
LA	Low Alarm

This page intentionally left blank

Appendix B: Standard Configuration List

Sr. No.	Description	Number	Unit
1	RDU-SIC G2 intelligent port monitoring card	1	EA
2	User manual - Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card User Manual (V1.1, Chinese & English Version) - 16mo-Glue Binding	1	EA
3	Whole set cable - UH52SA1SL2-UH52SA1Z UPS USB cable - ROHS	1	EA
4	Whole set or other labels – certificate label	1	EA

This page intentionally left blank

Appendix C: Hazardous Substance or Elements

Part	Hazardous Substances					
	Plumbum	Hydrargyrum	Cadmium	Chrome	PBB	PBDE
	Pb	Hg	Cd	Cr6+	PBB	PBDE
PCBA	x	o	o	o	o	o
Cables	x	o	o	o	o	o
0: Means the content of the hazardous substances in all the average quality materials of the part is within the limits specified in SJ/T-11363-2006; x: Means the content of the hazardous substances in at least one of the average quality materials of the part is outside the limits specified in SJ/T11363-2006						
Vertiv Tech Co., Ltd. has been committed to the design and manufacturing of environment-friendly products. It will reduce and eventually eliminate the harzardous substances in the products through unremitting efforts in research.						
About Environment Protection Period: The Environment Protection Period of the product is marked on the product. Under normal working conditions and normal use of the products observing relevant safety precautions, the hazardous substances in the product will not seriously affect the environment, personnel safety or property in the Environment Protection Period starting from the manufacturing date.						
Applicable product: Vertiv™ Liebert® IntelliSlot™ RDU-SIC G2 Card						

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™

Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA