Contents

Chapter 1 Product Description

The 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 of network communication. The 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 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 RDU-SIC G2 card can meet the requirements of TCP/IP, RS232/485 networking modes and can be flexibly configured according to various application conditions.

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

1.1 Components Description

The appearance and ports of the RDU-SIC G2 card are shown in Figure 1-1.

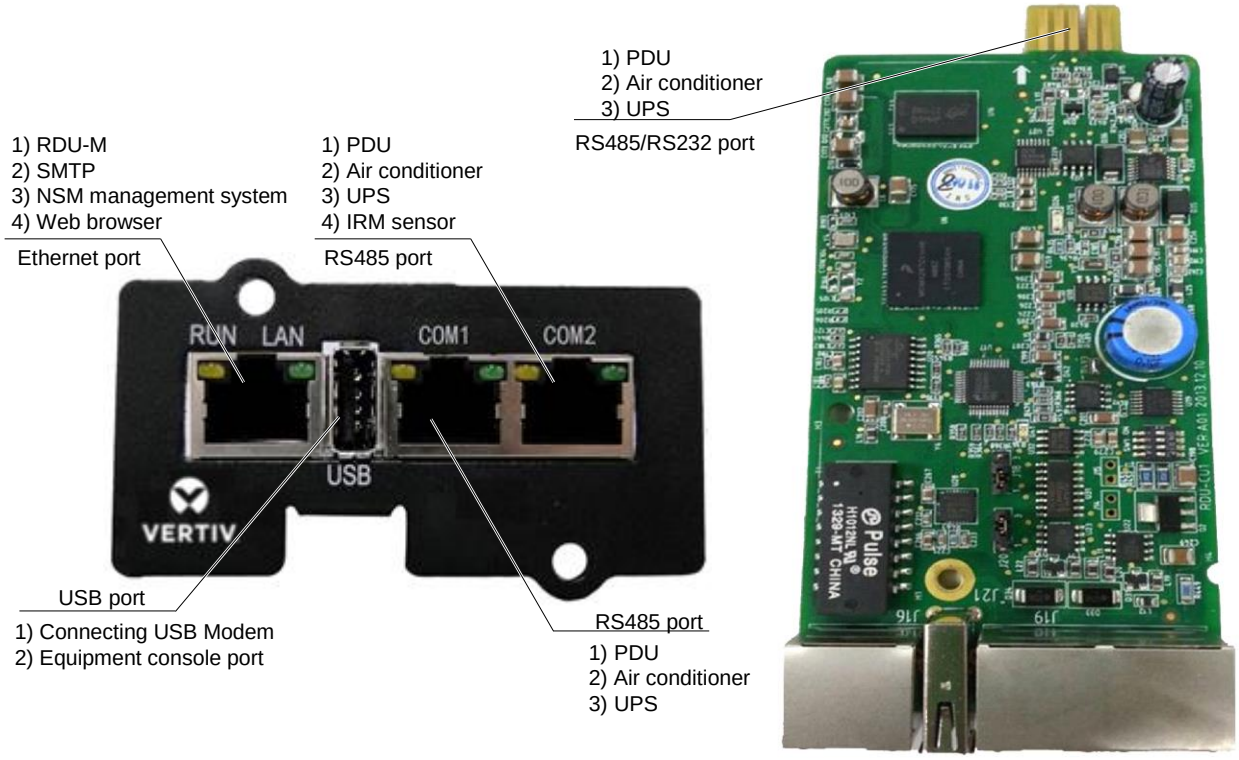


Figure 1-1 Appearance and ports of RDU-SIC G2 card

Console port

The RDU-SIC G2 card supplies a console port (USB port, see Figure 1-1 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.

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 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. Its position is shown in Figure 1-1.

Network port

The RDU-SIC G2 card provides one network port which adopts 10/100M Base-T self-adaptable Ethernet port. Its position is shown in Figure 1-1. See Table 1-2 for default configuration of the network port.

Table 1-2 Default configuration parameters of the network port

Parameter / Network card	IP address	Subnet mask	Default gateway
Default parameter	192.168.0.252	255.255.255.0	192.168.0.1

COM port

The RDU-SIC G2 card supplies three independent COM ports. Their positions are shown in Figure 1-1.

The port adopts RS-485 communication mode; the gold finger adopts RS-485/232C (adaptive) communication mode. See Table 1-3 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.

Table 1-4 Main functions of RDU-SIC G2

Main function	Description	
Device monitoring	Realizing camera viewing in 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 NetworkShutdown 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 customized according to user requirements, that is, alarm notification content can be customized; 2. You can choose the communication mode to receive alarm information of different level 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 & History	Device information	Querying 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; 2. Can install and uninstall equipment type and support connecting 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

Main function	Description	
System Options	Monitoring unit	Collecting the system information of RDU-SIC G2
	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; 3. Remote service setting
	User management	Adding, modifying and deleting user information
	Date/time setting	Calibrating the real time clock of RDU-SIC G2
	Restore system	Rebooting the RDU-SIC G2 and restoring default configuration
	Site setting	Modifying site information online
	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	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 for the environment specifications of RDU-SIC G2.

Table 1-5 Environment conditions

Item	Requirement
Application location	Usually in data center or computer room, with air conditioner
Working temperature	-10ºC ~ +60ºC
Relative humidity	5%RH ~ 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 ~ 106kpa
Storage temperature	-40ºC ~ +70ºC
Cooling	Natural cooling
Power distribution network	TT/TN
Protection level	IP20

1.3.2 Performance Specifications

See Table 1-6 for the performance specifications of RDU-SIC G2.

Table 1-6 Performance specifications

Connected component	Cable standard	Connected distance (unit: m)	Connected number / connection point
Connecting nodes of COM ports	Standard category 4 twisted-pair cable	≤ 100	Three Intelligent devices 8 test points[1] of Sensor
Note: [1]: The RDU-SIC G2 can connect intelligent devices through COM1 or COM2. The connected devices of single COM cascade cannot exceed two			

Chapter 2 Hardware Installation

This chapter expounds the hardware installation of the RDU-SIC G2.

2.1 Installation Preparation

2.1.1 Notes

When installing RDU-SIC G2, 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
- Ensure that the external devices are connected to the correct ports of the RDU-SIC G2
- 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.

Figure 2-1 Jumper locations of the RDU-SIC G2 card

Make sure that the jumpers of RDU-SIC G2 card are set to correct position. See Table 2-1 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’, password of Web system administrator ‘admin’ and IP address, set the jumpers according to this mode, reboot the RDU-SIC G2 card, and wait 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 normal mode by default.

2.1.2 Ambient Requirements

Operation environment

The RDU-SIC G2 must be installed indoor. Refer to Table 1-5 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).
- 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 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.
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.

Chapter 3 Web Page Of RDU-SIC G2

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

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 its connectivity. Refer to Q5 in *4.2 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 IE General setting

Double-click the icon of IE 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.

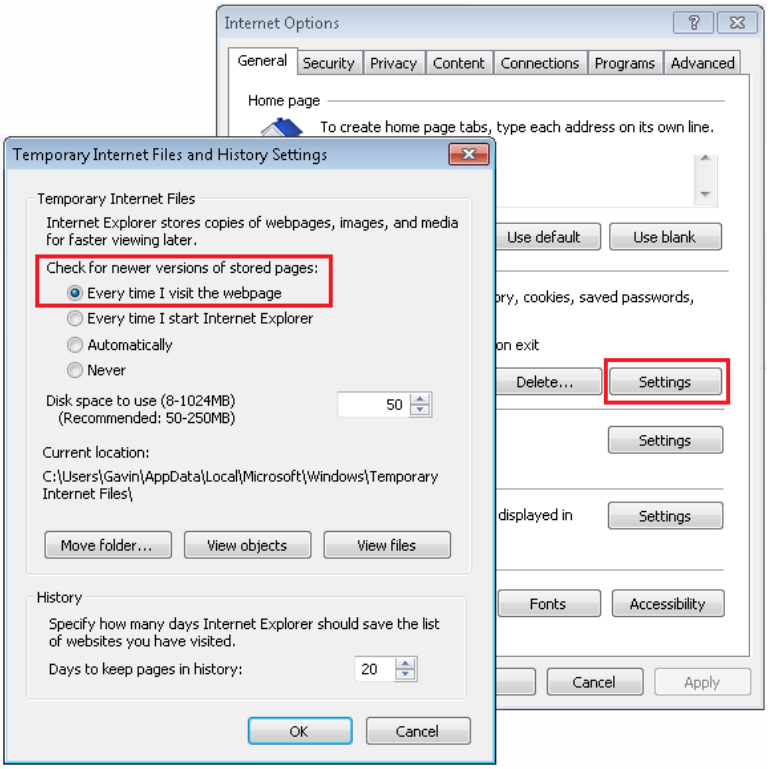


Figure 3-1 General setting

Checking IE proxy setting

1. Double-click the icon of IE 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.

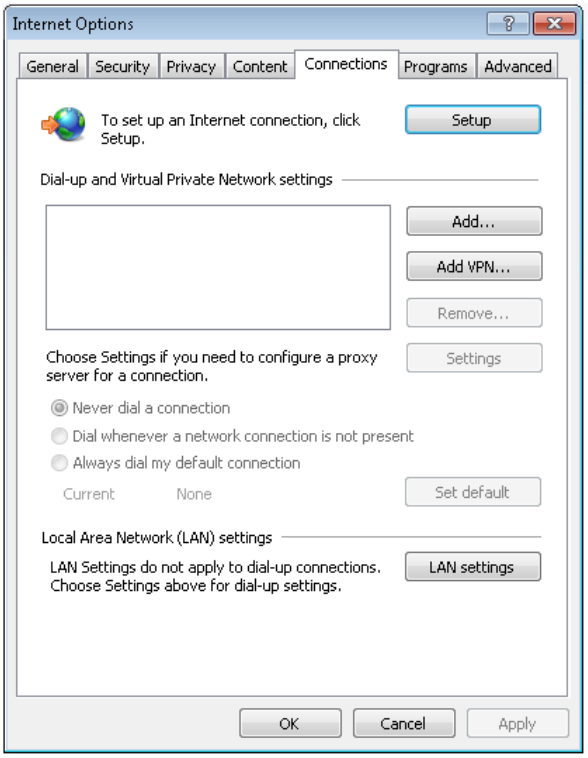


*Figure 3-2 Choosing the **Connections** tab*

2. In the window shown in Figure 3-2, click the button **LAN Settings** to pop up the window shown in Figure 3-3.

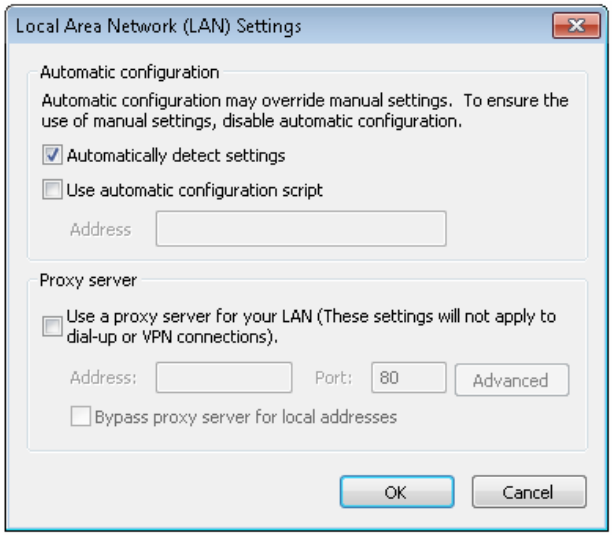


Figure 3-3 LAN setting

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 IE security setting

1. Double-click the icon of IE 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.

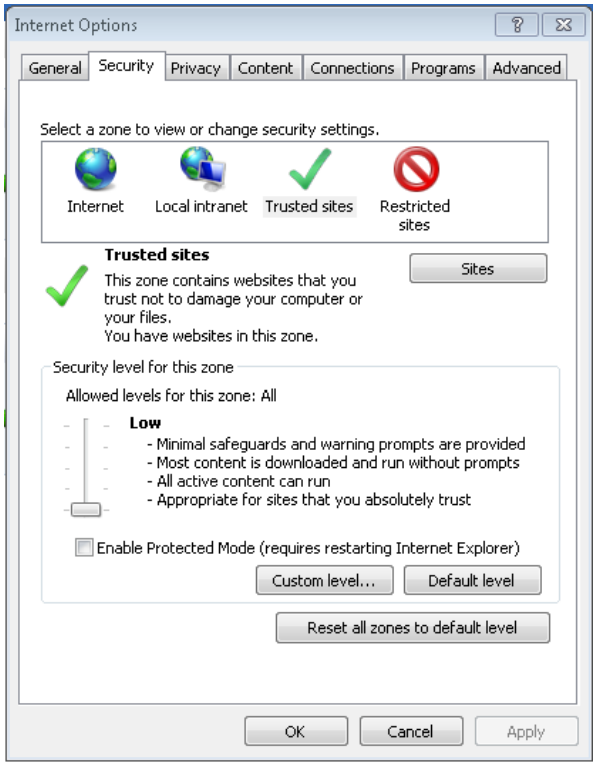


Figure 3-4 Security setting 1

2. In the window shown in Figure 3-4, choose **Local intranet** and click the **Custom level** button to pop up the window shown in Figure 3-5.

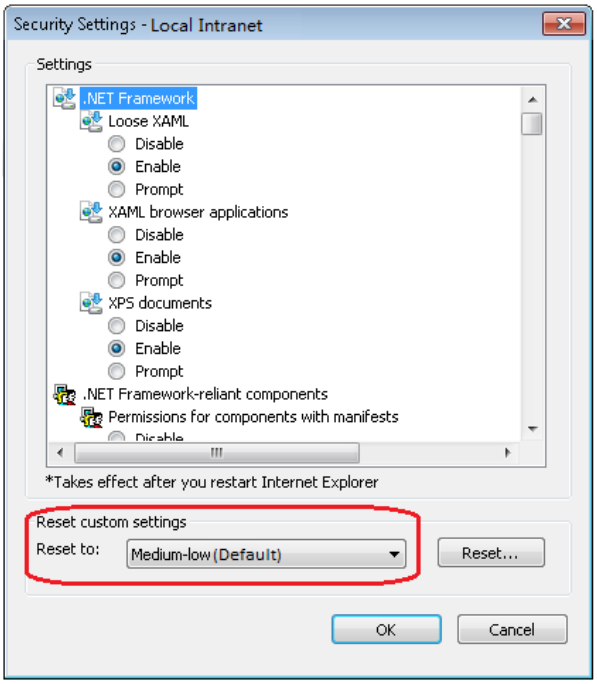


Figure 3-5 Security setting 2

3. In the window shown in Figure 3-5, set 'Medium-low' for the security level. Click the **Reset** button to finish Reset custom settings, at last, click **OK**.

4. In the window shown in Figure 3-6, set **Enable** for **File download**.

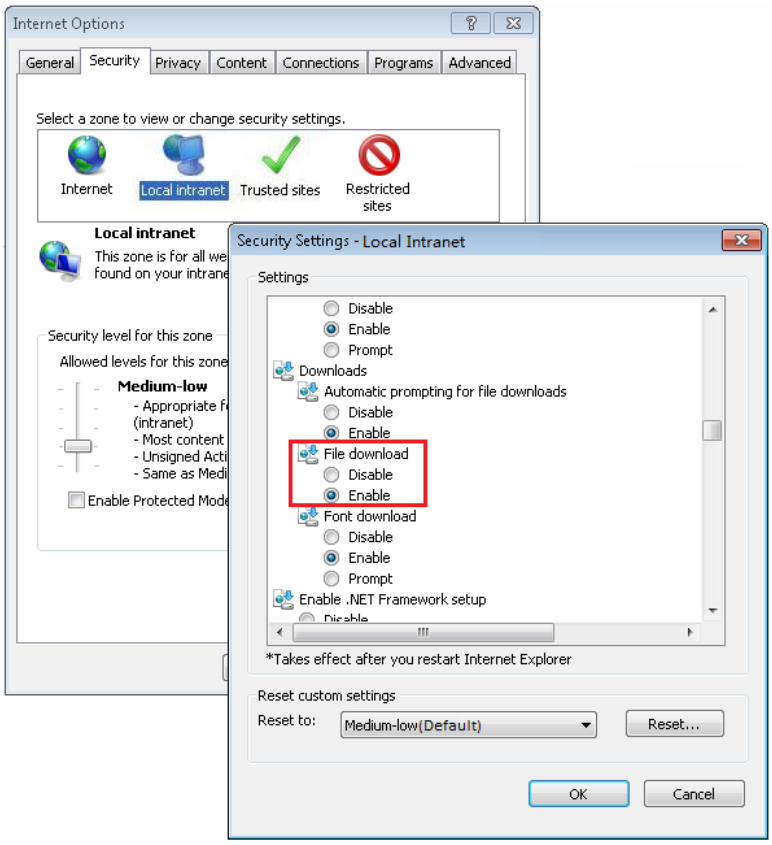


Figure 3-6 Enabling file download

5. In the window shown in Figure 3-7, set **Enable** for **Initialize and script ActiveX controls not marked as safe for scripting**.

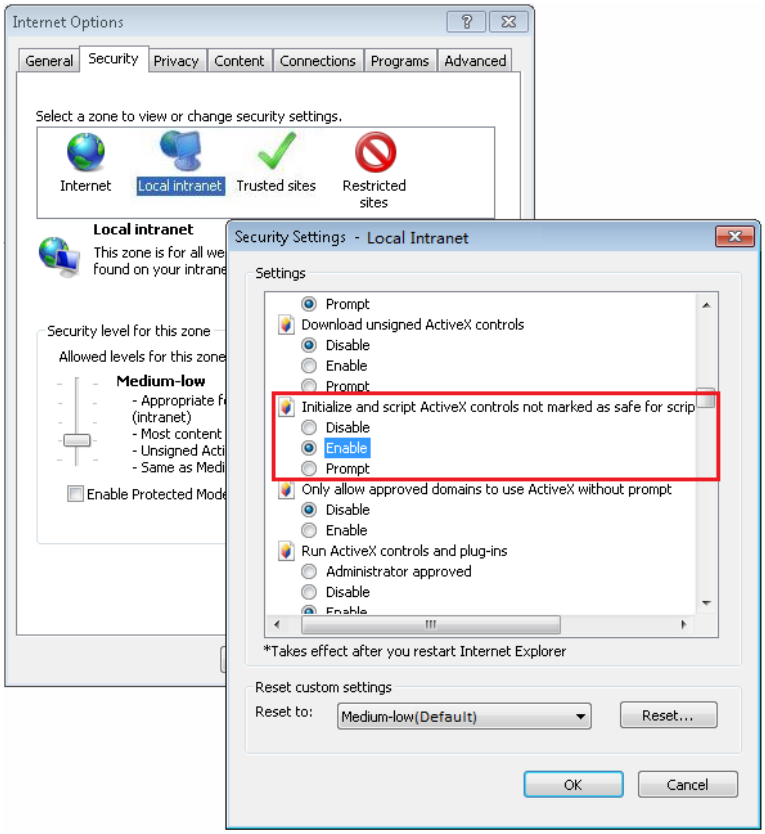


Figure 3-7 Enabling ActiveX controls

6. In the window shown in Figure 3-8, add the IP address of the RDU-SIC G2 into the trusted site list.

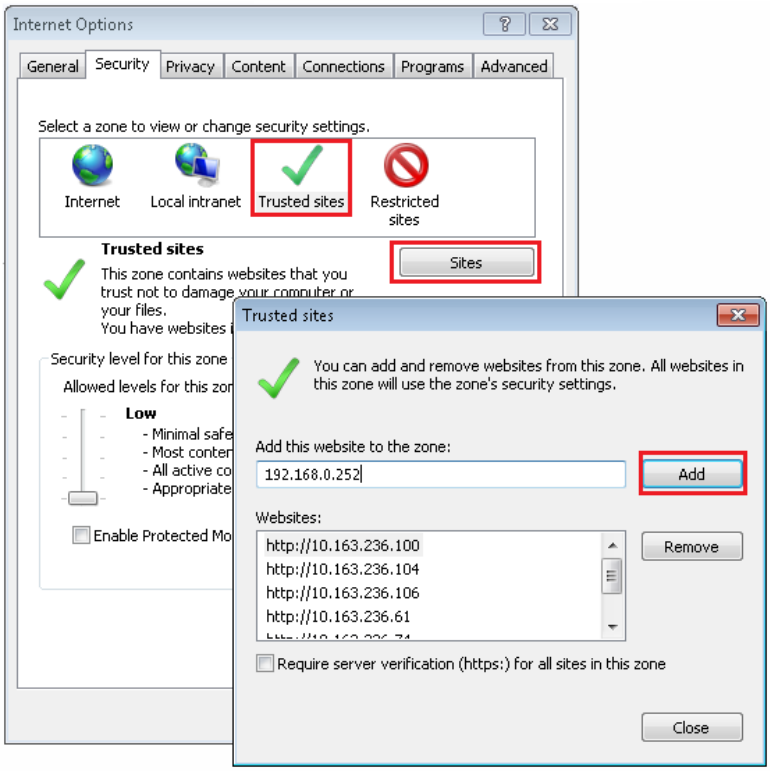


Figure 3-8 Adding trusted sites

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. If the login page does not appear, refer to *Q5* in *4.2 FAQ*.

Crystal blue *Ocean blue*

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.

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.

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.

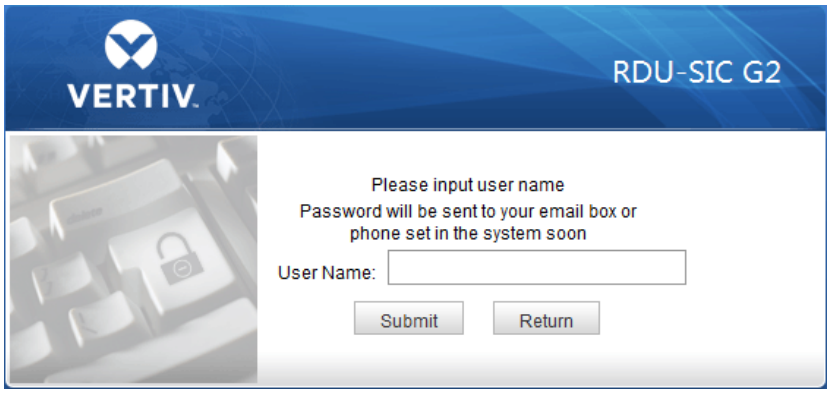


Figure 3-10 Page of getting password

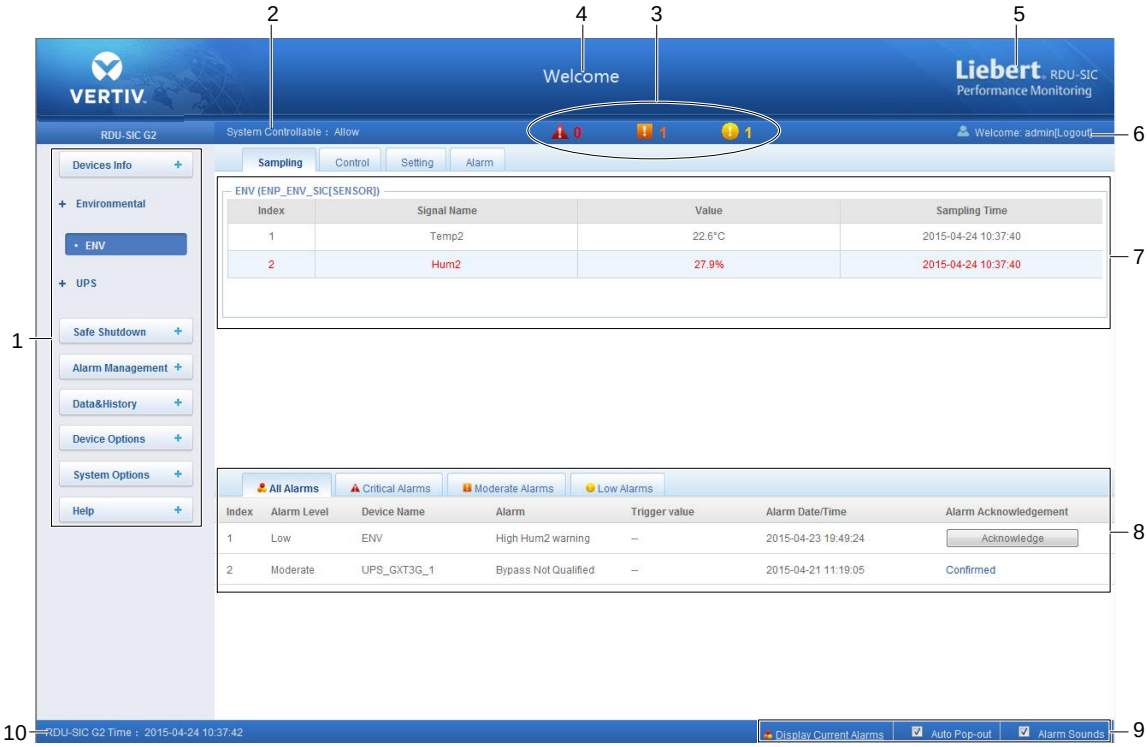
Type your username, and click the **Submit** button, your password will be sent to the email box or phone which you have configured before. Clicking the **Return** button cancels the operation.

Note

1. 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 Notification* in *3.4.3 Alarm Management* for detailed setting method.
2. 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.



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

Figure 3-11 Homepage of RDU-SIC G2

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 *3.4.6 System Options*.

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.

Figure 3-12 Controllable status

Click **[Clear] Time-out**, the input box shown in Figure 3-13 will appear. After typing the password, the controllable status will become normal after about 5s.

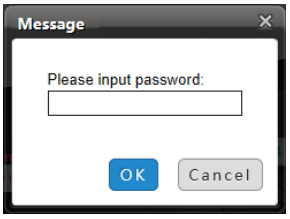


Figure 3-13 Password verification

3.3.3 Logout

Click the **Logout** at the upper right corner of the homepage, the prompt box shown in Figure 3-14 will appear, clicking **OK** will log out safely.

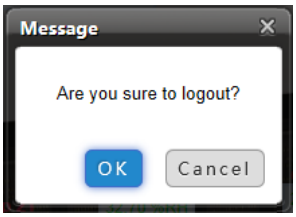


Figure 3-14 Logout

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:

1. Click **Display Current Alarms** 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.

3.4 Menu Items

On the homepage of RDU-SIC G2, the menu items include **Device Info**, **Safe Shutdown**, **Alarm Management**, **Data&History**, **Device Options**, **System Options** and **Help**.

3.4.1 Device Information

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 & humidity sensors connected to RDU-SIC G2.

Sampling

Clicking the **Sampling** tab can enter the sampling page, which displays sampling signals of selected device, as shown in Figure 3-15.

Figure 3-15 Sampling signals

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

Control

Clicking the **Control** tab can enter the control page, which displays control signals of selected device, as shown in Figure 3-16.

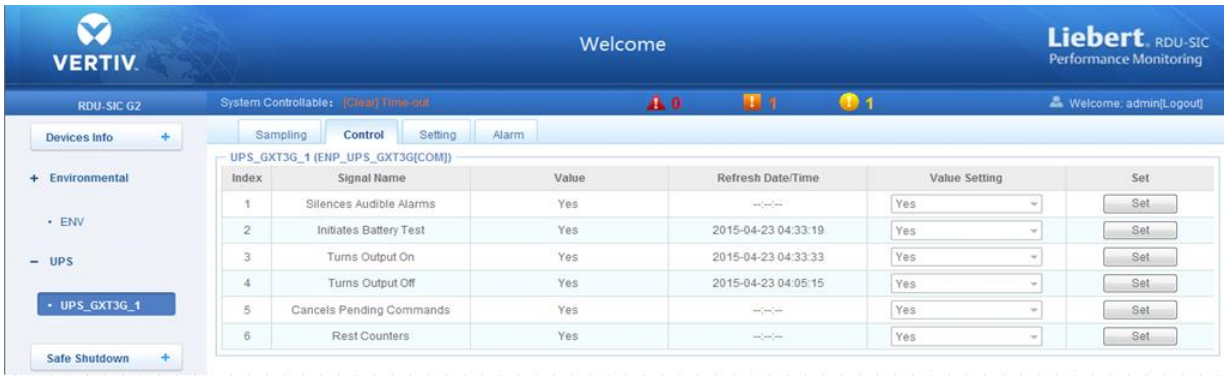


Figure 3-16 Control signals

Click the **Set** button to control the device.

Setting

Clicking the **Setting** tab can enter the setting page, which displays setting signals of selected device, as shown in Figure 3-17.

Figure 3-17 Setting signals

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 selected device, as shown in Figure 3-18.

Figure 3-18 Alarm signals

You can set alarm level of several alarm signals at the same time, and at most 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 pops up.

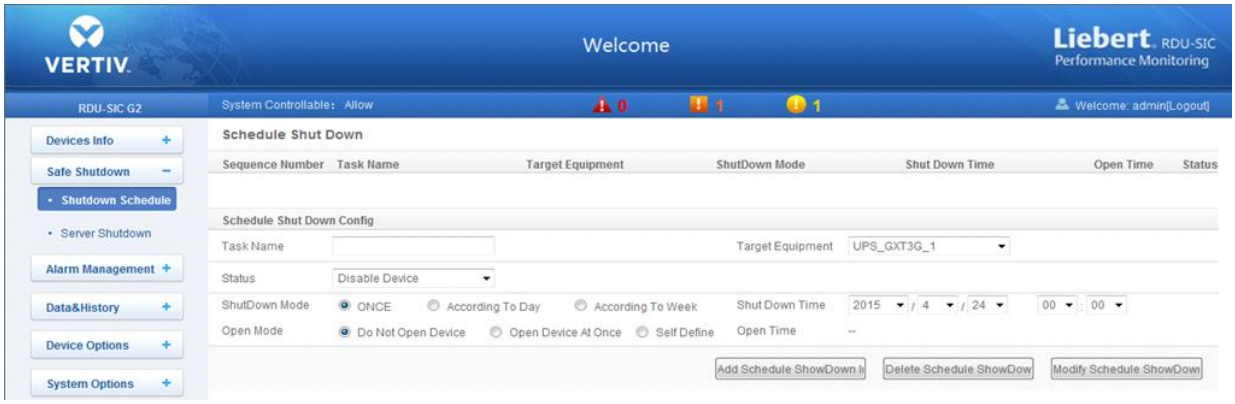


Figure 3-19 Shutdown Schedule page

The Shutdown Schedule page is used to add, delete and modify schedule shutdown task of UPS devices.

As shown in Figure 3-19, 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.

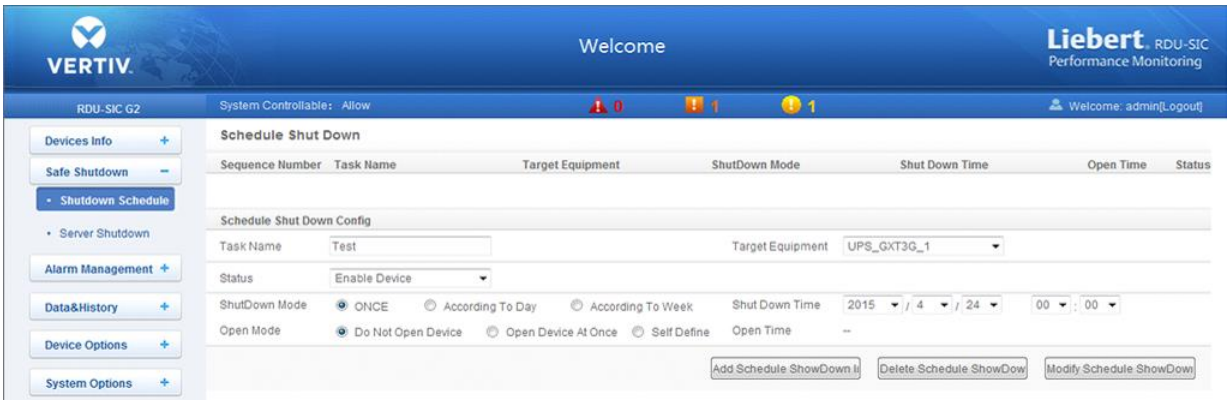


Figure 3-20 Schedule shutdown task list

Click the **Add Schedule Shutdown** button, the task will be successfully added. As shown in Figure 3-21, a new task has been added in the schedule shutdown task list. The tasks in the task list will be executed automatically according to their Enable/Disable status.

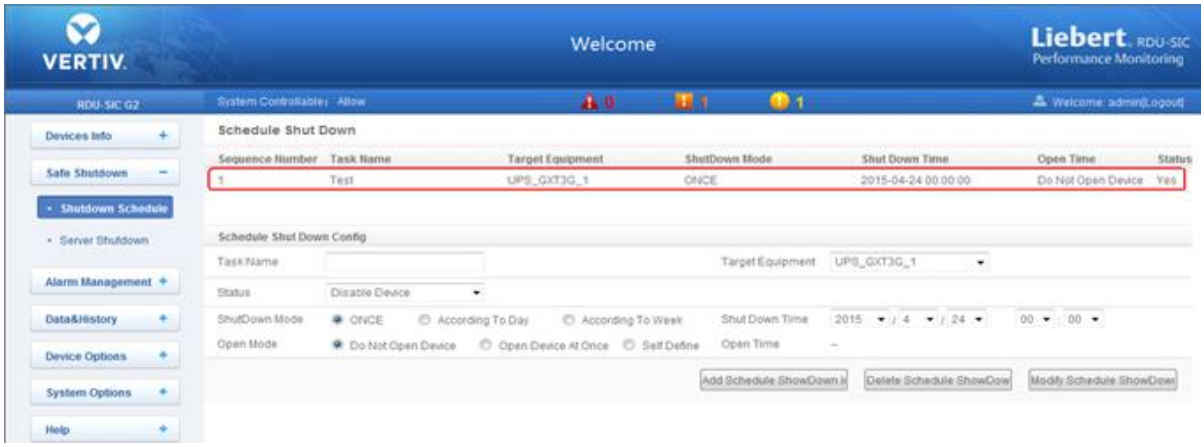


Figure 3-21 Schedule shutdown task list

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 **ShutDown Time** changes with different options of **ShutDown Mode** automatically, as shown in Figure 3-22.

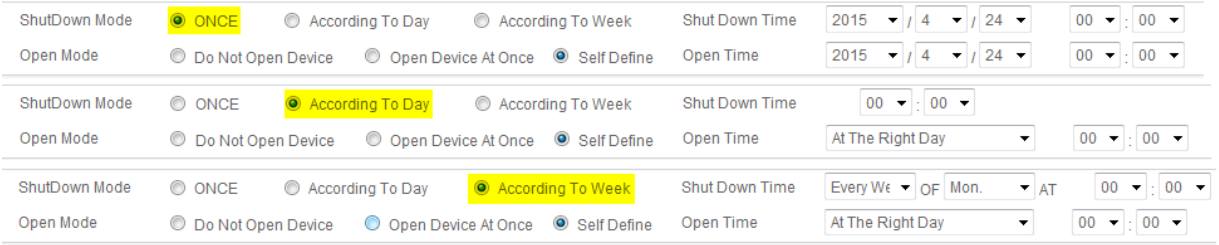


Figure 3-22 Format of shutdown time

Note

1. The RDU-SIC G2 can support up to ten shutdown tasks.
2. 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, the Server Shutdown page will pop up, as shown in Figure 3-23.

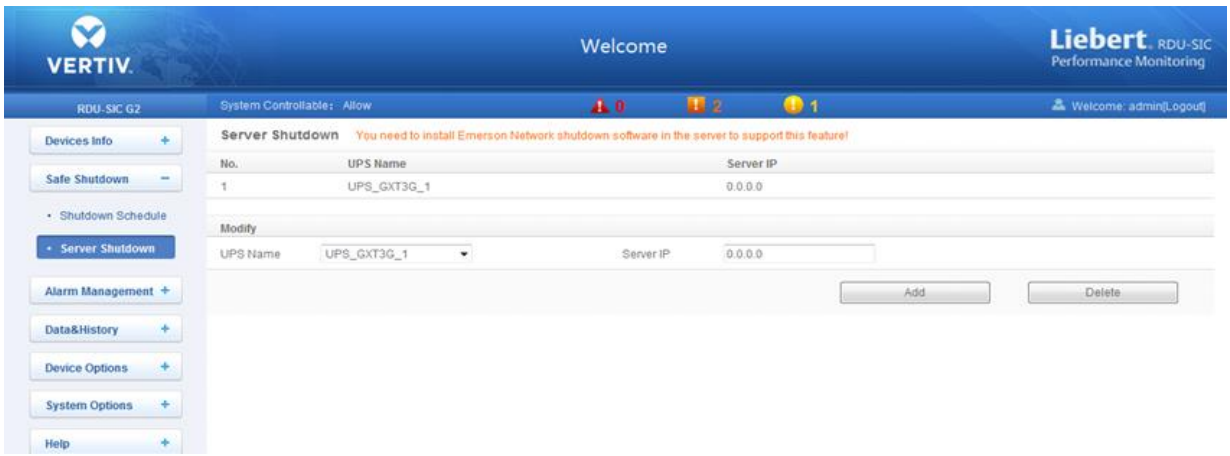


Figure 3-23 Server Shutdown page

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 of 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, three submenus appear, including **Current Alarm**, **History Alarm** and **Alarm Notification**.

Current Alarms

Click **Current Alarms** under the **Alarm Management** menu, or refer to *3.3.5 Real-Time Alarm Pop-Up Setting*, the current alarm list will pop up, as shown in Figure 3-24.

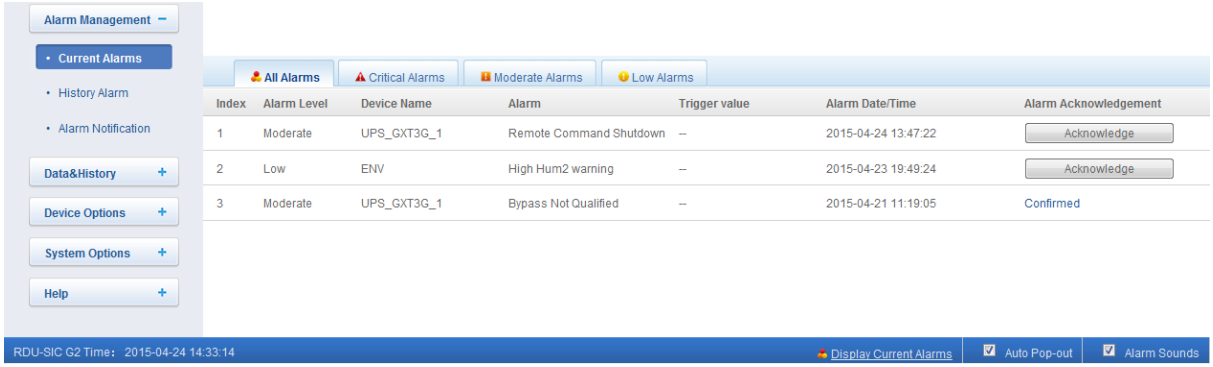


Figure 3-24 Current alarms

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 conformation, no alarm notification about the conformed 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.

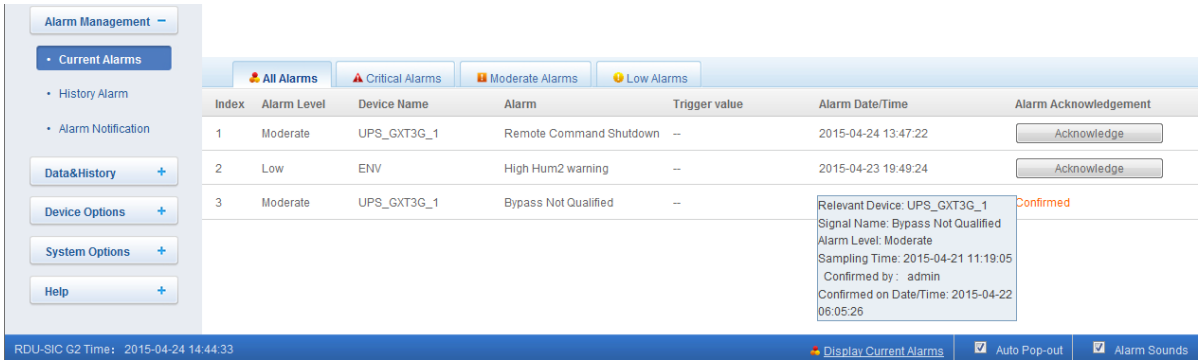


Figure 3-25 Confirming information

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.

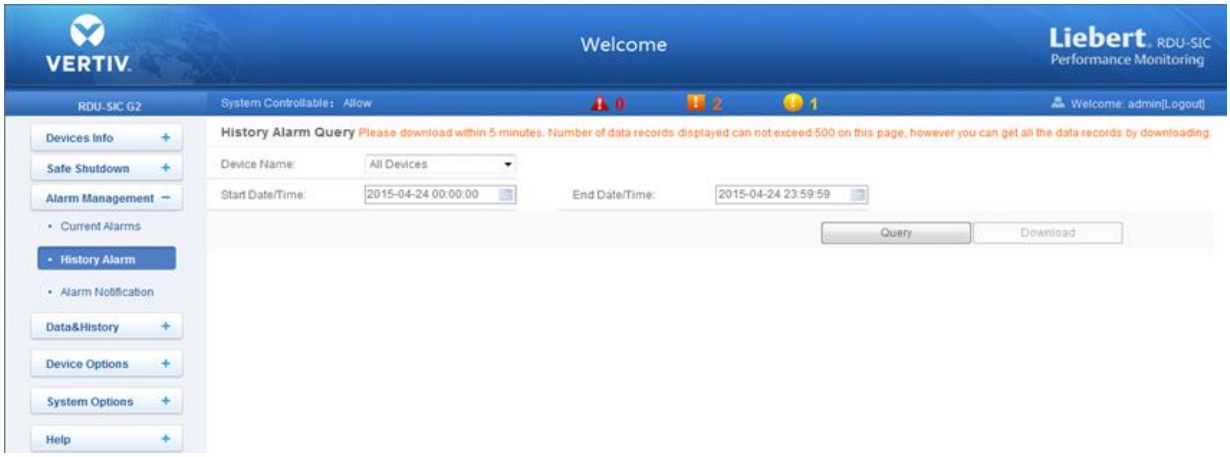


Figure 3-26 History alarm query

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

Alarm Notification

1. User Alarm Notification Configuration

Click the **Alarm Notification** under the **Alarm Management** menu, the page shown in Figure 3-27 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

1. Users must tick the notification method first in the **Notification by** check boxes, and then the alarm table below can be edited;
2. When all devices are chosen, all devices will be configured with the same alarm level;
3. When low level alarm is chosen, the alarm level above this level will also be chosen;
4. When some device is chosen, the highest level **Critical Alarm** will be chosen by default.

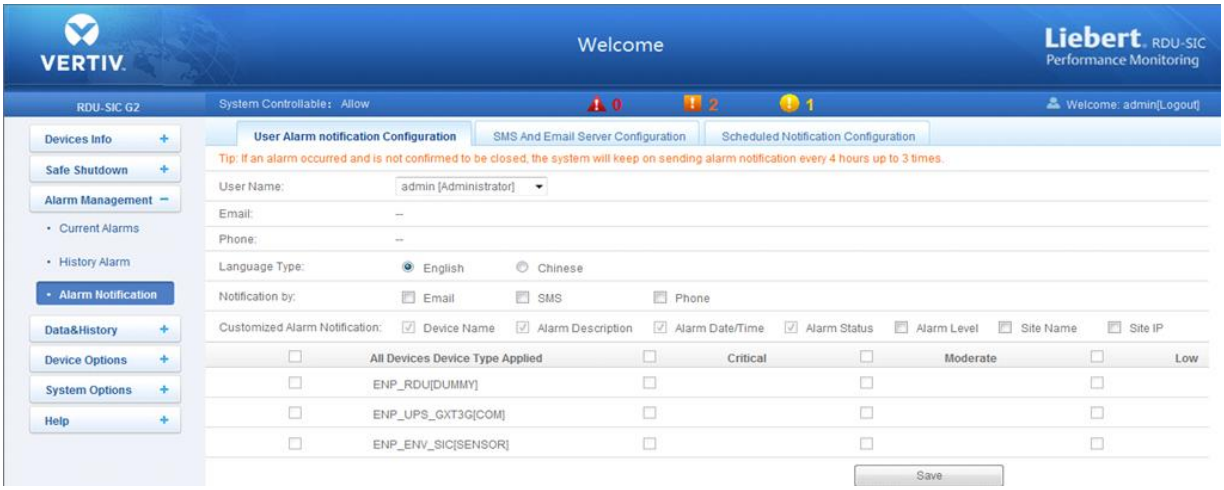


Figure 3-27 User alarm notification configuration

2. 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 pops up.

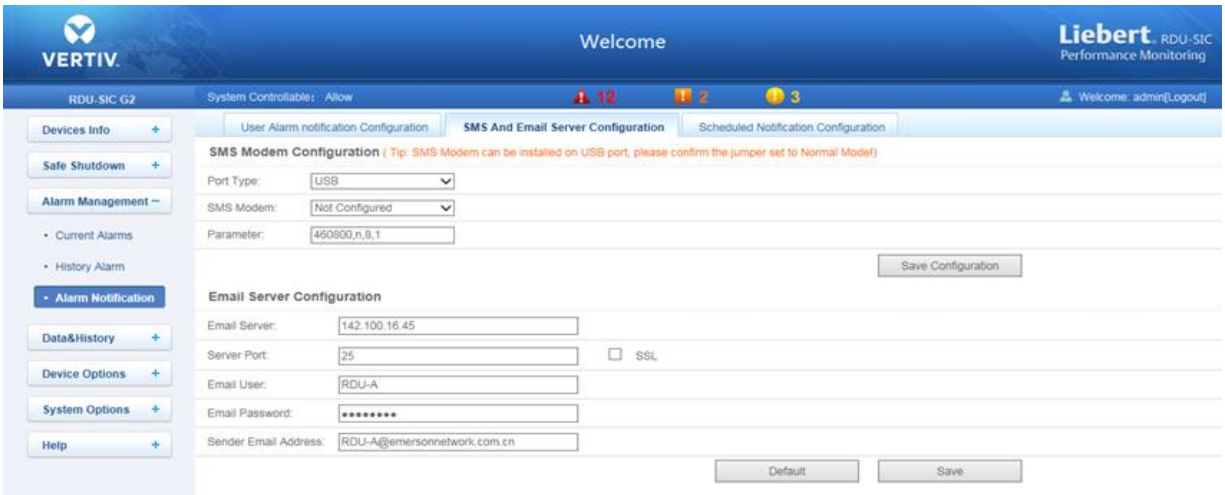


Figure 3-28 SMS/Email server configuration

On the page shown in Figure 3-28, you can perform **SMS Modem Configuration** for alarm notification reminding through SMS or phone, you can also perform **Email Server Configuration** for alarm notification reminding through email, the procedures are as follows:

●SMS Modem Configuration

1) Connect an SMS Modem through USB port according to need, and choose **Port Type**, the page will display **Parameter** automatically;

2) Choose **SMS Modem** (GPRS/CDMA) according to the SMS Modem type;

3) Set the communication parameter of the SMS Modem;

4) Click the **Save Configuration** button to save the configuration of 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.

●Email Server Configuration

1) Type the server IP address or domain name in the **Email Server** field;

2) Type the **Server Port**, **Email User**, **Email Password** and **Sender Email Address** in the corresponding fields;

3) Click the **Save** button to save the configuration of current user's Email server.

Note

1. The **Server Port** is '25' by default. When **SSL** is chosen, the **Server Port** will become '465' automatically;
2. The **Email User** is 'RDU-A' by default;
3. When using SSL, you need to ensure that the Email server supports SSL function.

3. 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 pops up.

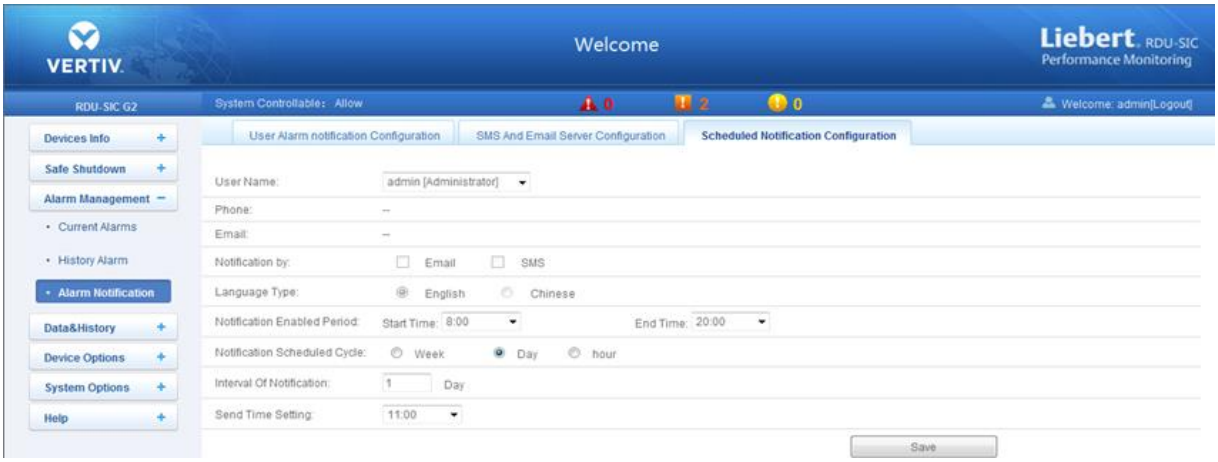


Figure 3-29 Scheduled notification configuration

Note

1. Scheduled notification configuration must be used together with user alarm notification configuration; otherwise, you cannot select **User Name**, **Notification by** and **Language Type**;
2. For scheduled notification configuration, the notification method 'Phone' is not supported;
3. 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 **Notification Enabled Period** (setting range: 8:00 ~ 20:00), **Notification Scheduled Cycle** (default: Hour), **Interval of Notification** (default: 1) and **Send Time Setting** (default: start time).

3) Click the **Save** button to save the system notification configuration.

3.4.4 Data & History

The **Data & 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, four submenus appear, including: **Device Information**, **History Data**, **History Log** and **Clear History**.

Device Information

Click the **Device Information** under the **Data & History** menu, the page shown in Figure 3-30 pops up. The page includes two tabs: **Device Information List** and **Export SNMP MIB**.

1. Device Information List

As shown in Figure 3-30, the page lists the main information of all equipment. Click the **Download** button to download the query result.

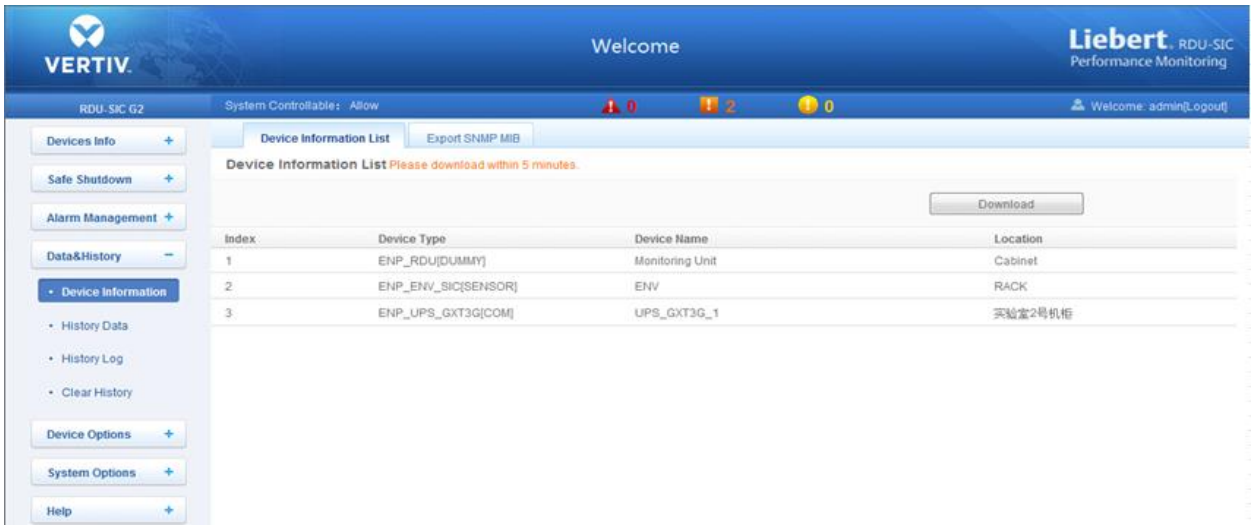


Figure 3-30 Device information list

2. Export SNMP MIB

As shown in Figure 3-31, you can export MIB information according to device type. After selection, click the **Download** button to export MIB information.

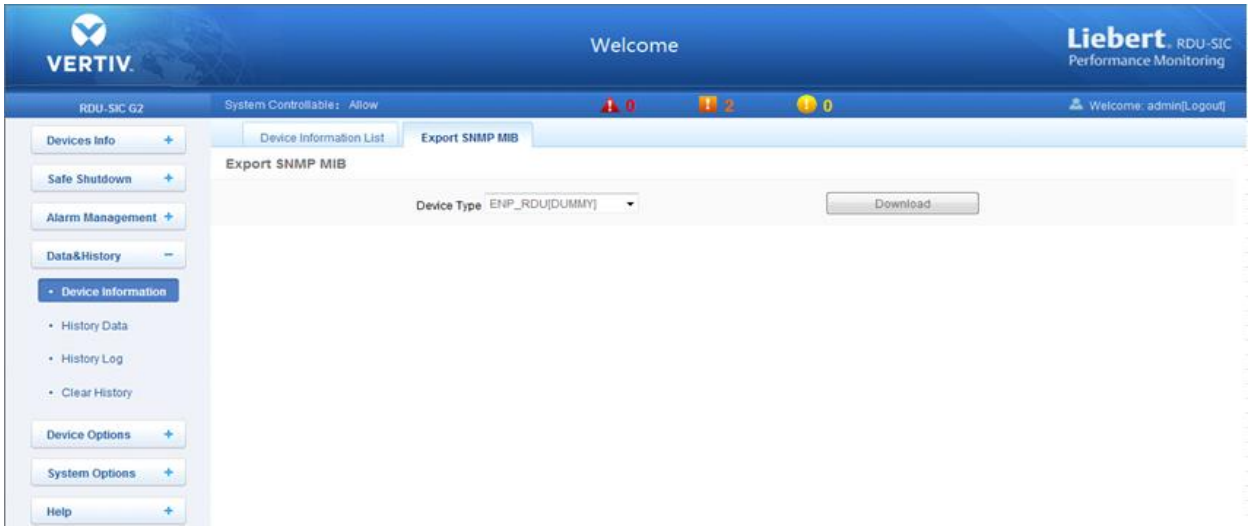


Figure 3-31 Export SNMP MIB

History Data

Click the **History Data** under the **Data & History** menu, the page shown in Figure 3-32 pops up. The page has two tabs: **History Data** and **Historical Curve**.

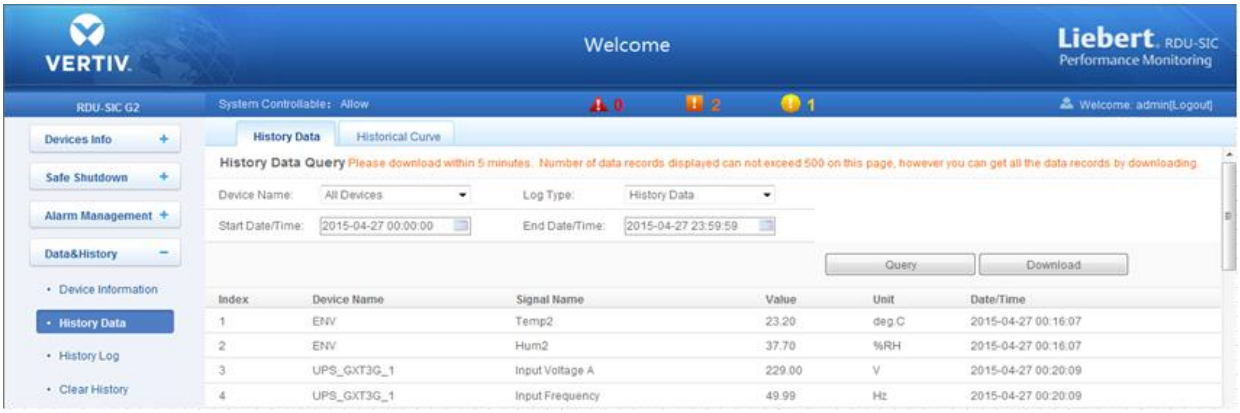


Figure 3-32 History data

1. History Data

As shown in Figure 3-32, 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.

2. Historical Curve

As shown in Figure 3-33, 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.

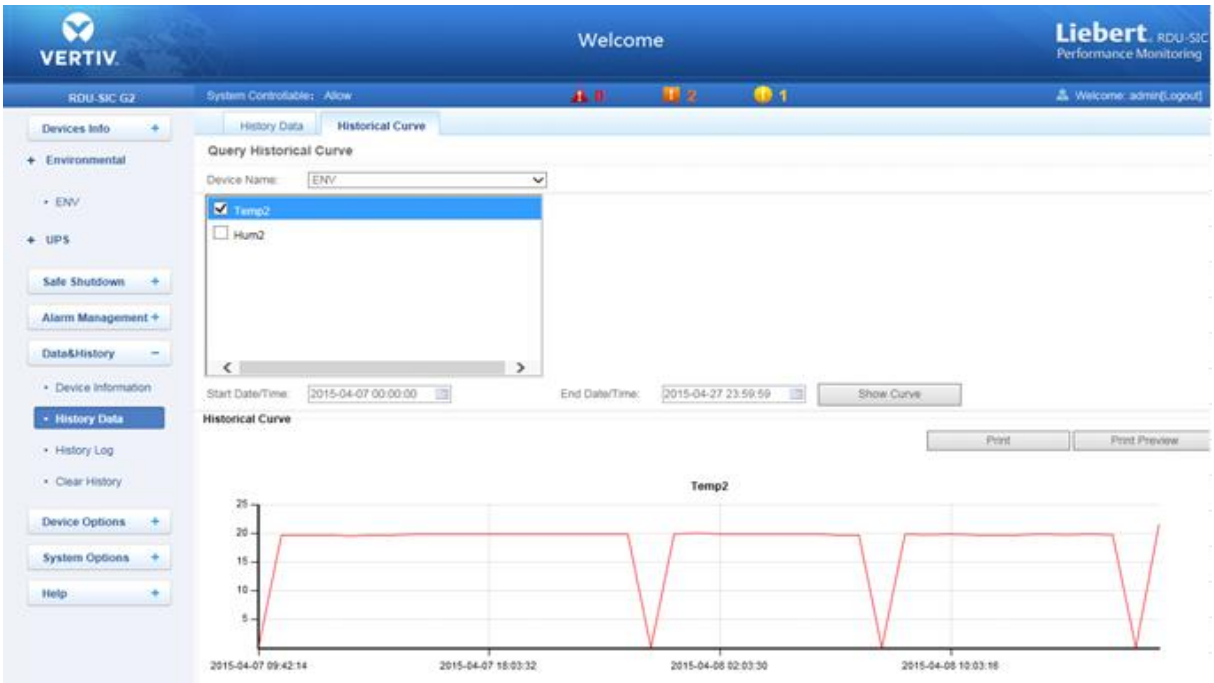


Figure 3-33 Historical curve

History Log

Click the **History Log** under the **Data & History** menu, the page shown in Figure 3-34 pops up.

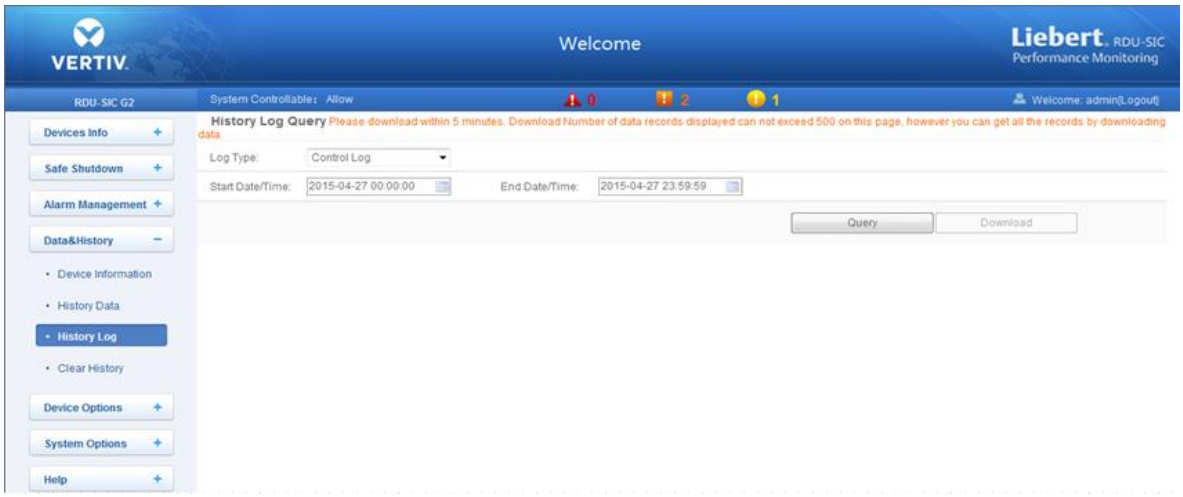


Figure 3-34 History log

On the page shown in Figure 3-34, 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

1. Add/Modify/Delete Device

Click the **Device Management** under the **Device Options** menu, the page shown in Figure 3-35 pops up.

Figure 3-35 Add/modify/delete equipment

As shown in Figure 3-35, you can add/modify/delete a new device, the procedures are as follows:

●Adding a new device

1) Choose the device type in the **Device Type** textbox;

2) Type 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;

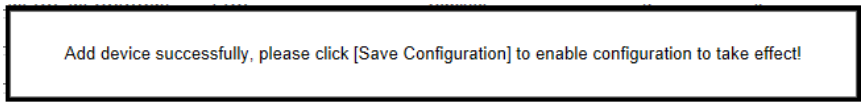
4) Type the device address, which must be numbers from 1 to xx, in the **Device Address** textbox. The device addresses under the same port number must be different; for some device types, you need not type the device address, at this point, the **Device Address** textbox turn gray and cannot be edited. 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;

5) Choose or type the device location;

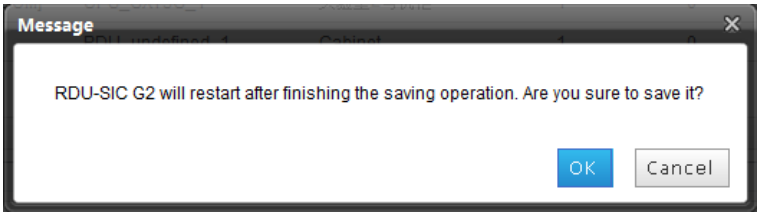
6) Type the communication parameter in the **Parameter** textbox. In the event that the device type is certain, the communication parameter prompt information will appear in the **Parameter** textbox, including the communication parameter format and default communication parameter of the equip type;

7) Click the **Add** button, the page shown in *Prompt information 1* in Figure 3-36 pops up, at the same time, a piece of new device information will be added in the device list;

8) Click the **Save Configuration** button, the page shown in *Prompt information 2* in Figure 3-36 pops up;



Prompt information 1



Prompt information 2

Figure 3-36 Prompt information

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.

9) Type the login password of current user, and click **OK**. The reboot page pops up, as shown in Figure 3-37;

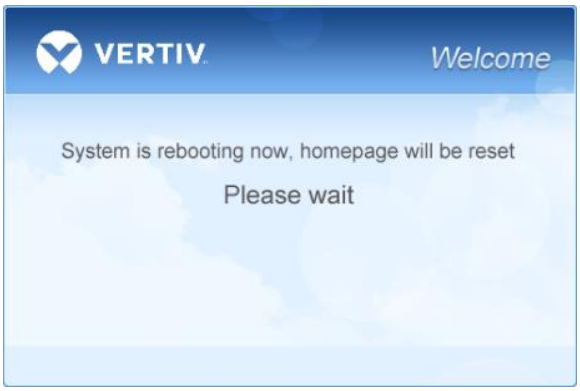


Figure 3-37 Reboot page

After the system reboots, adding a device becomes effective.

10) 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.

●Deleting a device

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.

●Modifying a device

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 of saving the configuration, as shown in Figure 3-38.

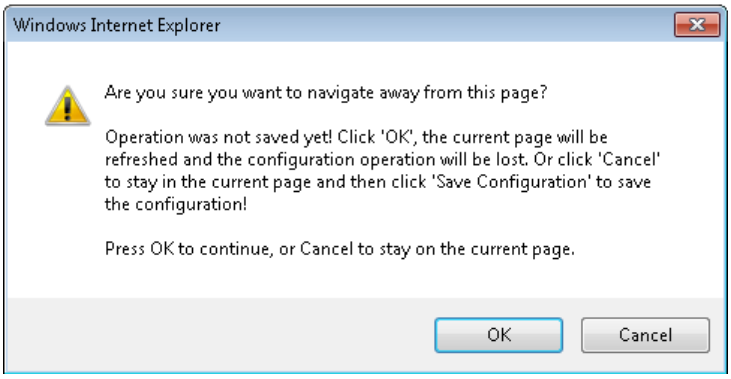


Figure 3-38 Prompt information 3

Note

Clicking the **Save Configuration** button can save all the operations at one time.

2. 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 3-39 pops up.

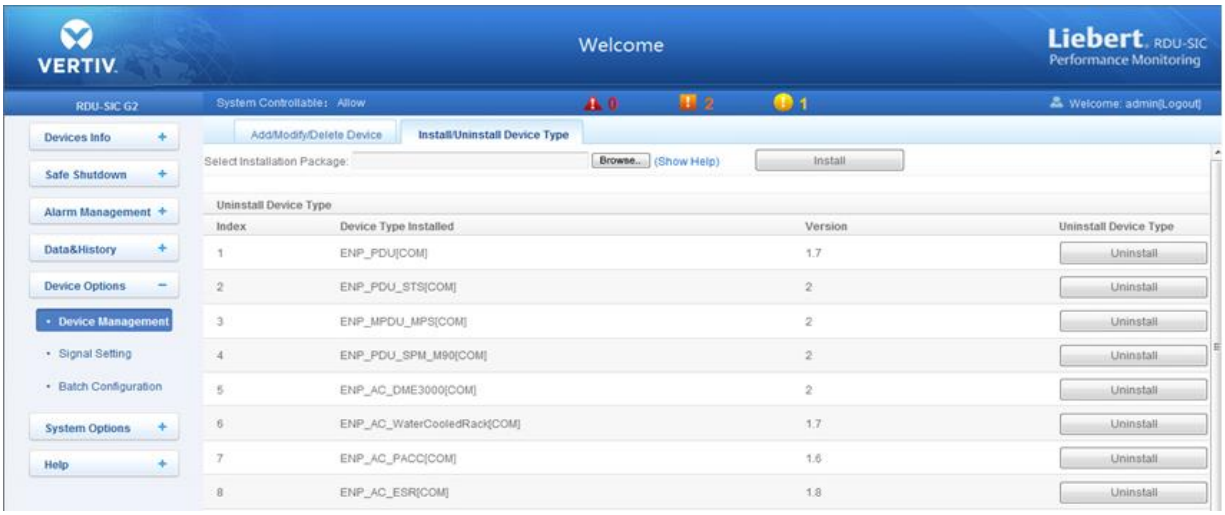


Figure 3-39 Install/Uninstall Device Type

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.

Note

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.

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 3-40.

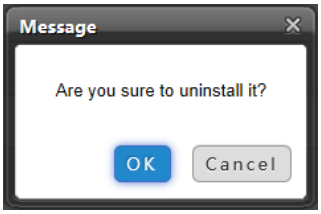


Figure 3-40 Confirming dialog box

Click **OK**, the dialog box of Security authentication pops up, as shown in Figure 3-13, type the login password of current user, and click **OK** to uninstall the corresponding equipment type.

Note

1. 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;
2. If the installation pack has no version information, or the version information does not match the software version, the device type cannot be installed.
2. 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 3-41 pops up.

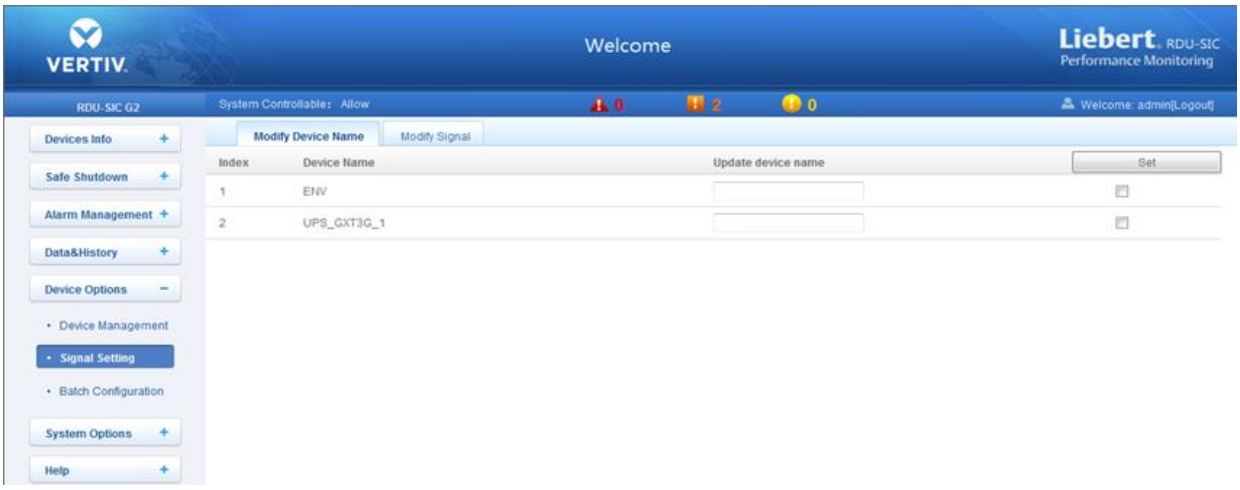


Figure 3-41 Modify device name

On the page shown in Figure 3-41, 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 3-42 will pop up.

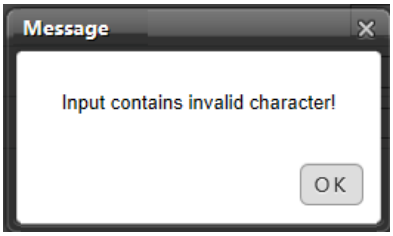


Figure 3-42 Prompt box of invalid characters

Batch Configuration

Click the **Batch Configuration** under the **Device Options** menu, the page shown in Figure 3-43 pops up.

Figure 3-43 Batch configuration

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

Note

1. Only 'admin' has the authority of batch configuration. If you fail in performing batch configuration, please click **Show Help** to view the help information.
2. The batch configuration file is encrypted after downloaded to local.

3.4.6 System Options

On the RDU-SIC G2 homepage, click the **System Options** menu in the left part, 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 3-44.

Figure 3-44 Monitoring unit (Sampling)

As for the operation method of the three tabs of **Sampling**, **Setting** and **Alarm** on the Monitoring unit page, refer to *3.4.1 Device Information*.

Note

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

1. For current alarms, the page only displays the alarm signals, but not send alarm notifications; after the alarm disappears, it will not be saved in history alarm;
2. The 'Blocked' setting for **Outgoing Alarm Blocked** will be automatically cleared in 24h.

Network Setting

1. IP Setting

Click the **Network Setting** under the **System Options** menu, the page shown in Figure 3-45 pops up.

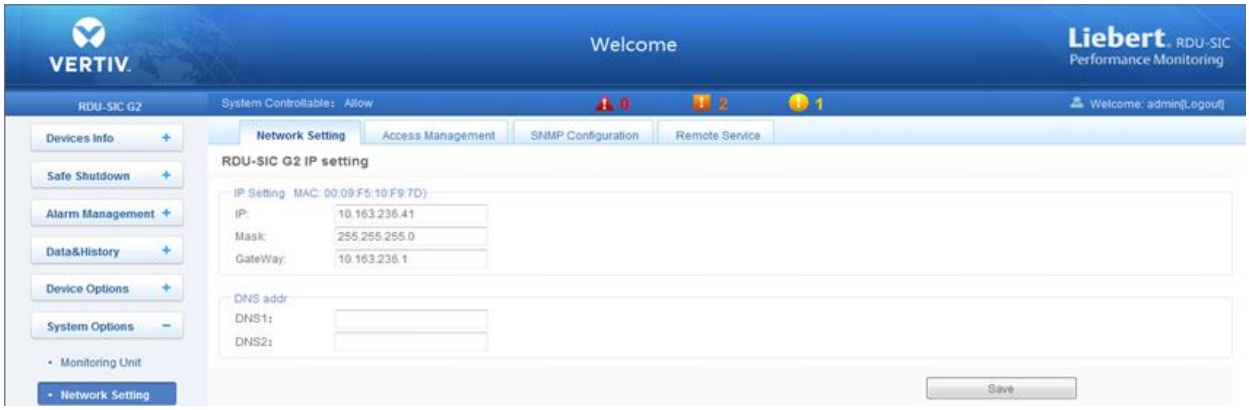


Figure 3-45 IP setting

On the page shown in Figure 3-45, you can configure the network parameters, such as IP addressing mode, **IP**, **Mask**, **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

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 RDU-SIC G2.

2. Access Management

Click the **Network Setting** under the **System Options** menu, and then click the **Access Management** tab, the page shown in Figure 3-46 pops up.

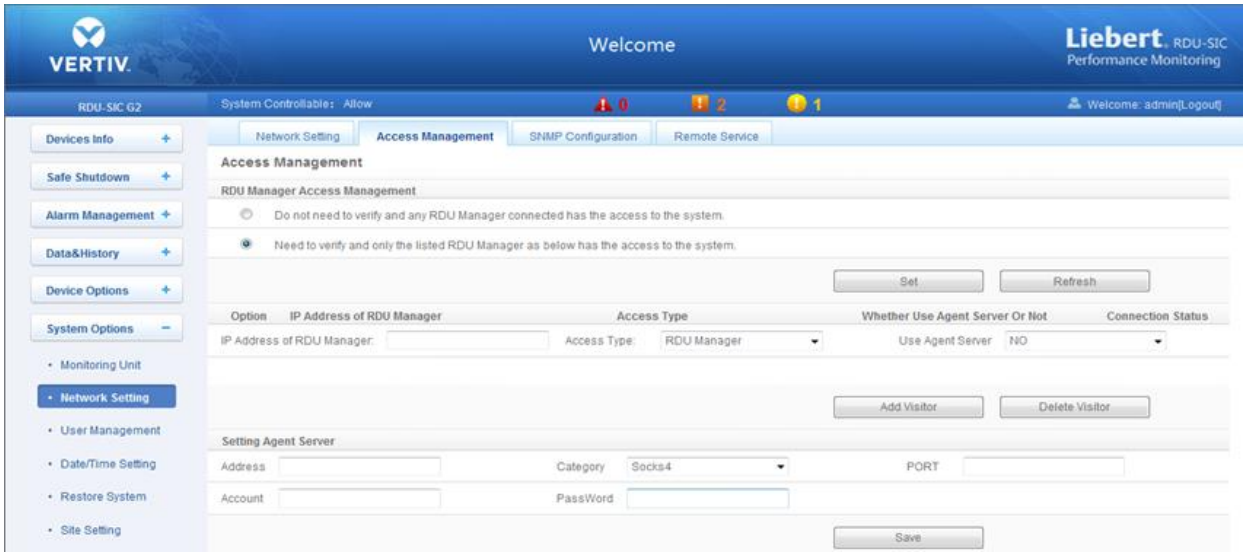


Figure 3-46 Access management

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

1. Up to three RDU manager IP addresses can be added in the system.
2. In the event of adding visitor, if you select to use an agent, you also need to configure the agent server.

3. 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 3-47, 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**: ‘Enable’ or ‘disable’;

3) Keep defaults for other items.

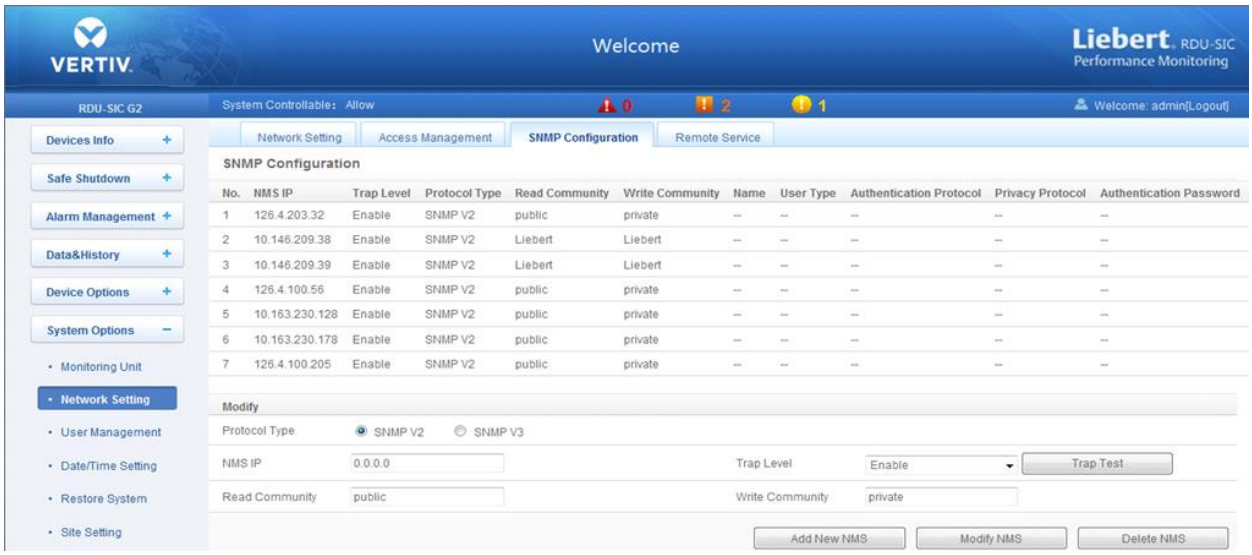


Figure 3-47 SNMP V2 setting

As shown in Figure 3-47, 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**: ‘Enable’ or ‘disable’;

3) Set the **Name**;

4) Set the **User Type**: ‘Authenticated & Encrypted’, ‘Authenticated & Not Encrypted’, ‘Not Authenticated & Not Encrypted’;

5) Select **Authentication Protocol**: ‘MD5’, ‘SHA’;

6) Select **Privacy Protocol**: ‘DES’;

7) Self-define **Authentication Password** and **Privacy Password**.

Note

1. On the base of SNMP V2, SNMP V3 adds user authentication and privacy strategies.
2. If you select ‘Not Authenticated & Not Encrypted’ for **User Type**, the drop-down boxes of **Authentication Protocol** and **Privacy Protocol** will become gray, so you cannot set them;
3. Currently, only ‘DES’ is supported for **Privacy Protocol**.
4. 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.

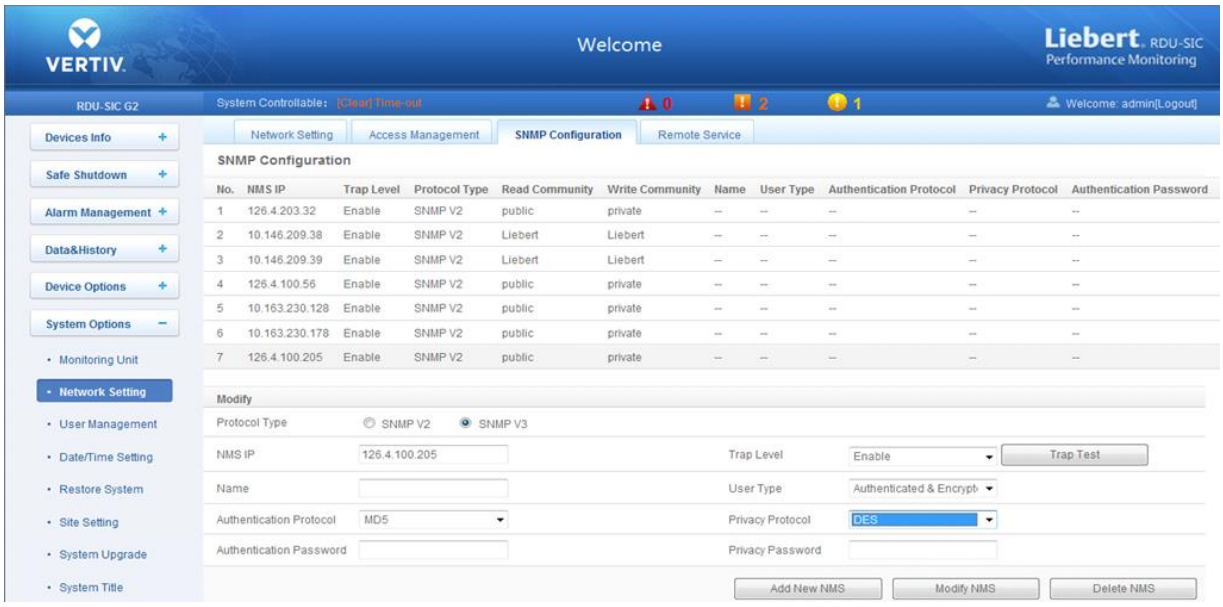


Figure 3-48 SNMP V3 setting

4. Remote Service

Click the **Network Setting** under the **System Options** menu, and then click the **Remote Service** tab, the page shown in Figure 3-49 pops up.

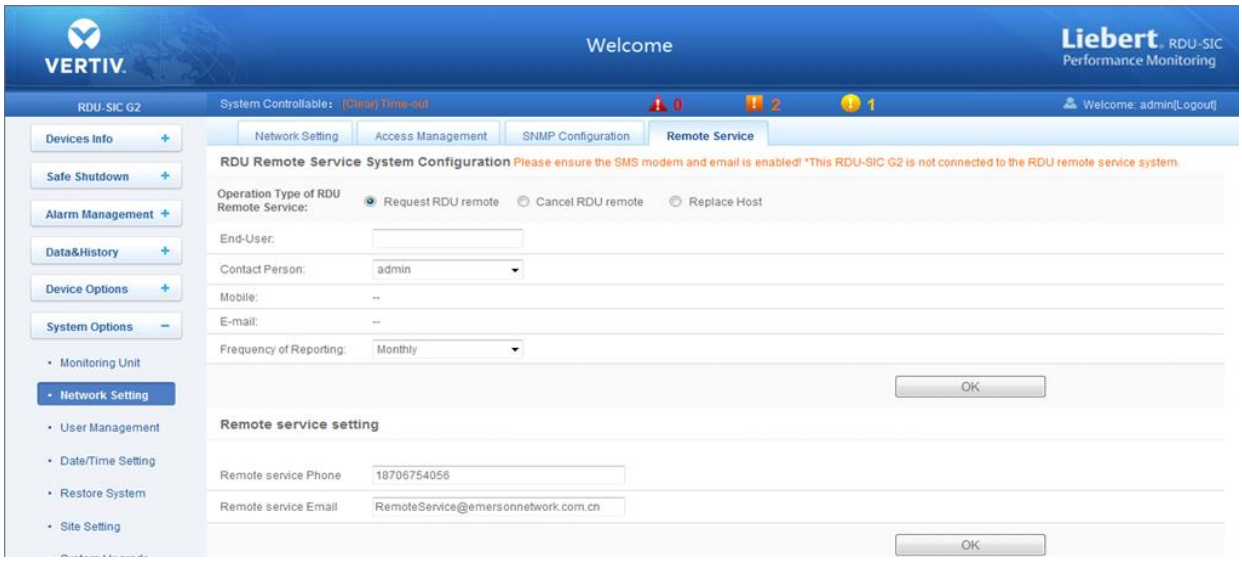


Figure 3-49 Remote service setting

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.

●Request RDU remote: used to establish remote service relationship

1) Type the self-defined customer name in the **End-User** textbox;

2) 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* in this section for detailed setting method.

3) Choose **Frequency of Reporting**: 'Monthly', 'Seasonal';

4) 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.

User Management

Click the **User Management** submenu under the **System Options** menu, the page shown in Figure 3-50 pops up.

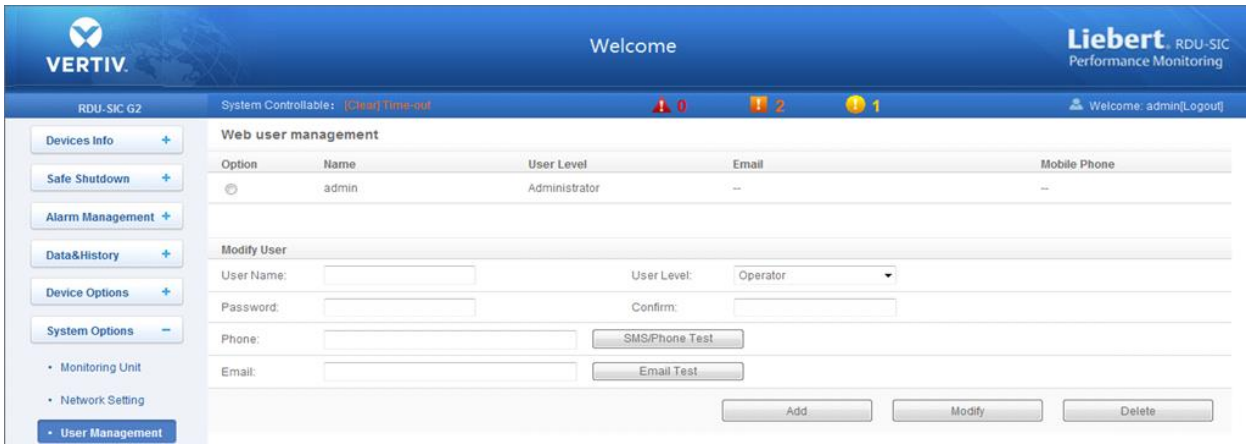


Figure 3-50 User management

On the page shown in Figure 3-50, you can add user, modify user and delete user.

●Add user

1. Type username in the **User Name** textbox;
2. Choose the user authority;
3. Configure the user password, which cannot be vacant and should contain at least six letters or digits.
4. Re-type the password in the **Confirm** textbox;
5. (Optional) Type the user telephone number, which can use the following digits and characters: 0123456789, +;
6. (Optional) Type the email address;
7. Click the **Add** button, the dialog box of Security authentication pops up, as shown in Figure 3-13. 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.

●Delete user

1. Choose the user which needs to be deleted in the username list;
2. Click the **Delete** button to pop up the confirming dialog box, as shown in Figure 3-51.

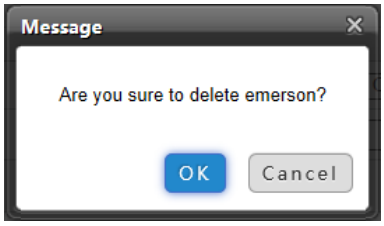


Figure 3-51 Confirming dialog box

3. Click **OK**, the dialog box of Security authentication pops up, as shown in Figure 3-13. Type the login password of current user, and click **OK** to delete the chosen user.

Note

The user of 'admin' cannot be deleted.

●Modify user

1. Choose the user which needs to be modified in the username list;
2. Modify the user information;
3. Click the **Modify** button, the dialog box of Security authentication pops up, as shown in Figure 3-13. 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 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 3-50, 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 *3.4.3 Alarm Management* for details.

- 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 properly connected.

- 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 3-52, 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.

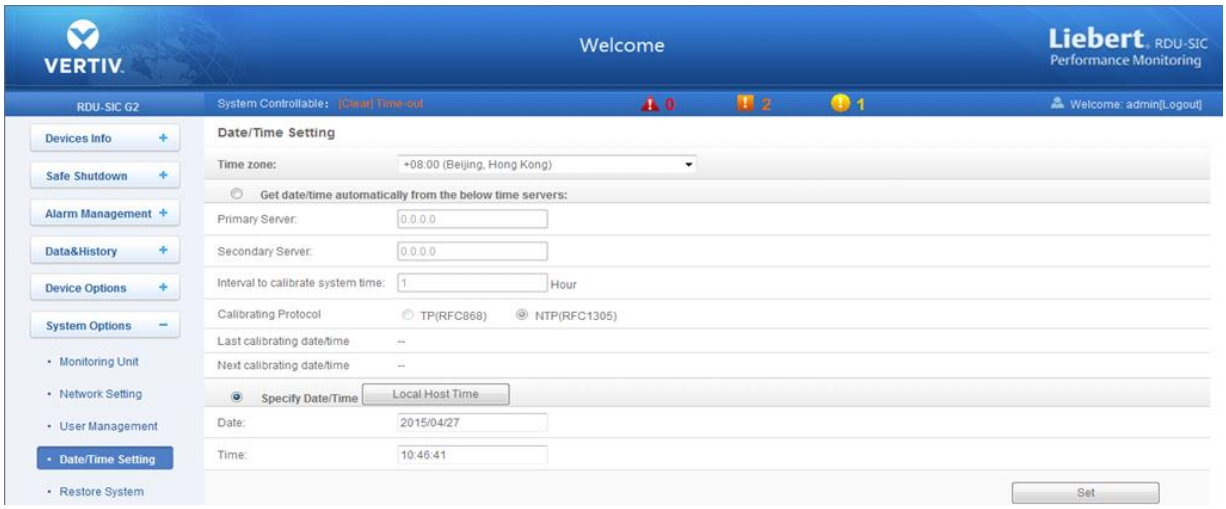


Figure 3-52 Date/time setting

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 3-53 pops up.

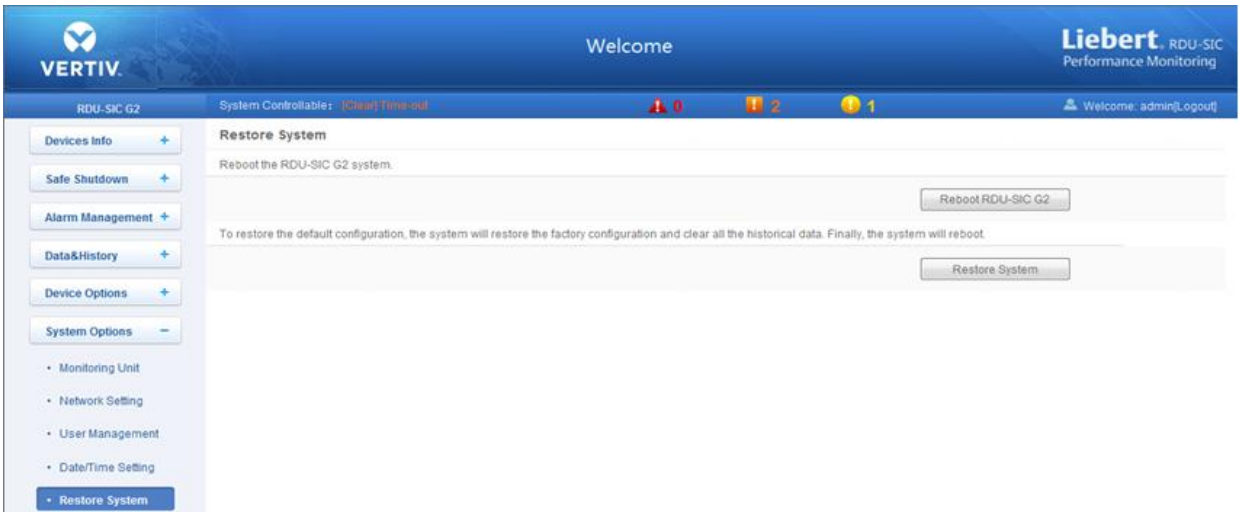


Figure 3-53 Restore System

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 RDU-SIC G2 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 3-54 pops up.

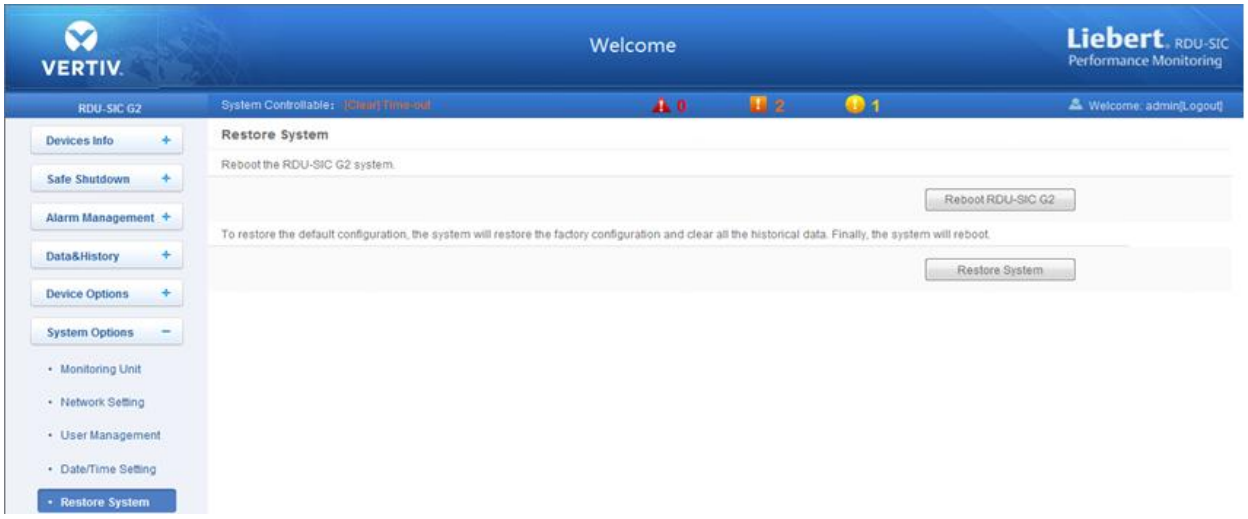


Figure 3-54 Site information setting

On the page shown in Figure 3-54, you can modify the site information of RDU-SIC G2, including **Site Name**, **Site Location** and **Site Description**.

System Upgrade

Click the **System Upgrade** under the **System Options** menu, the page shown in Figure 3-55 pops up.

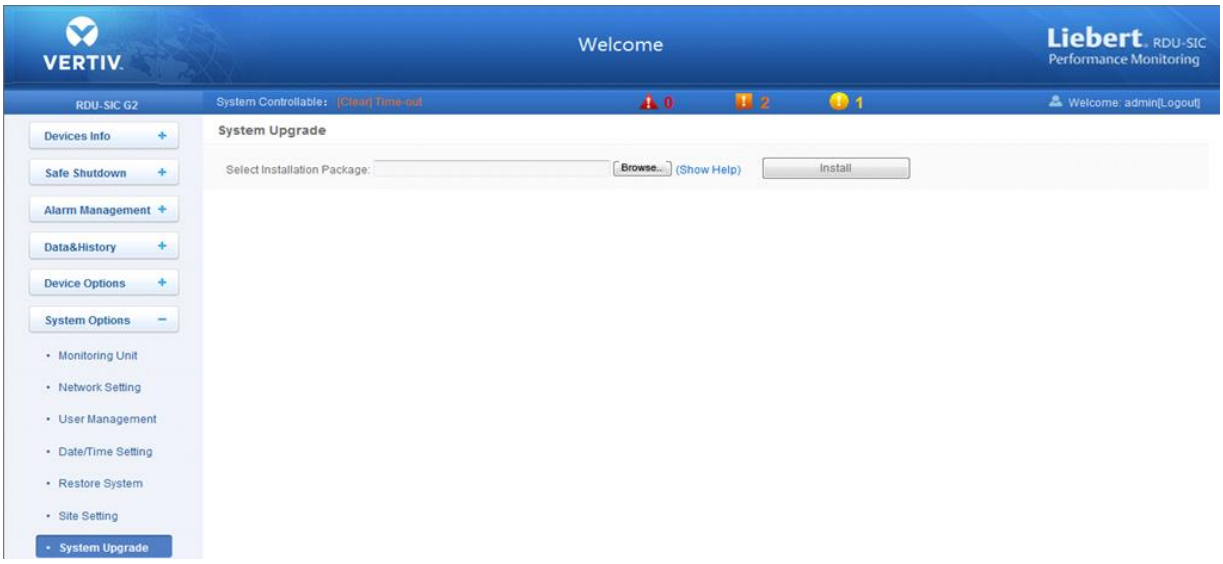


Figure 3-55 System upgrade

On the page shown in Figure 3-55, 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-SIC G2 supports incremental upgrading function.

System Title

Click the **System Title** under the **System Options** menu, the page shown in Figure 3-56 pops up.

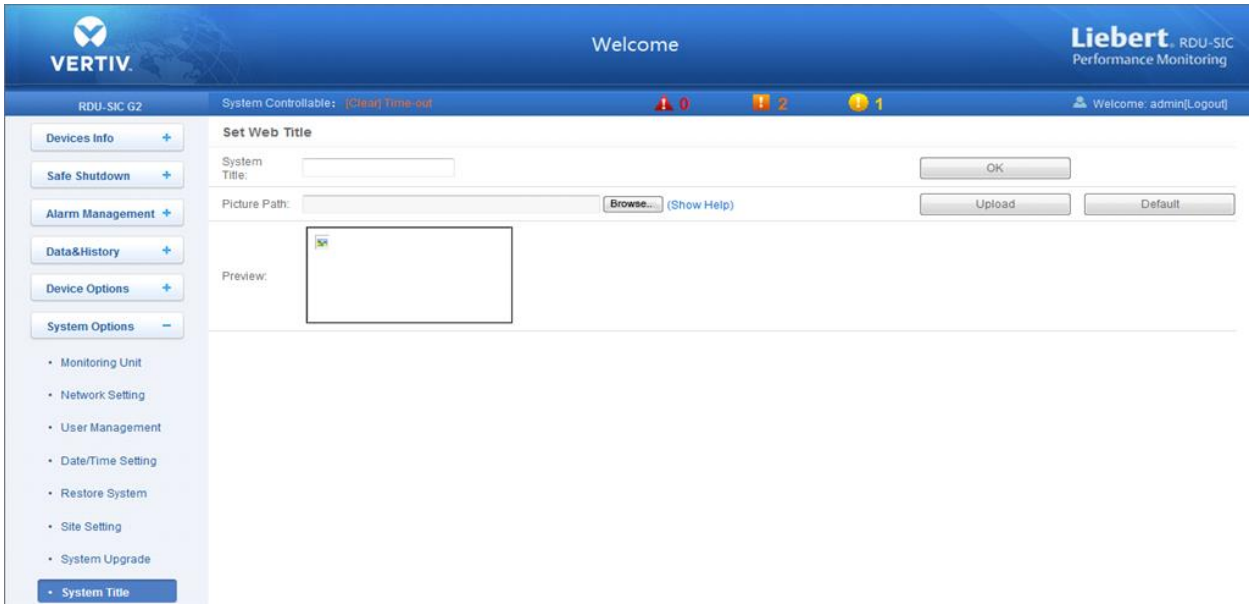


Figure 3-56 Title setting

As shown in Figure 3-56, 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-SIC 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 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 part, one submenu appears: **About RDU-SIC G2**.

The **About RDU-SIC G2** page displays **Software Version**, **Serial Number** and **Identify Code** of RDU-SIC G2, as shown in Figure3-57.

Figure 3-57 About RDU-SIC G2

Chapter 4 Maintenance

This chapter expounds the maintenance of RDU-SIC G2, including 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* in *3.4.6 System Options*.

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.

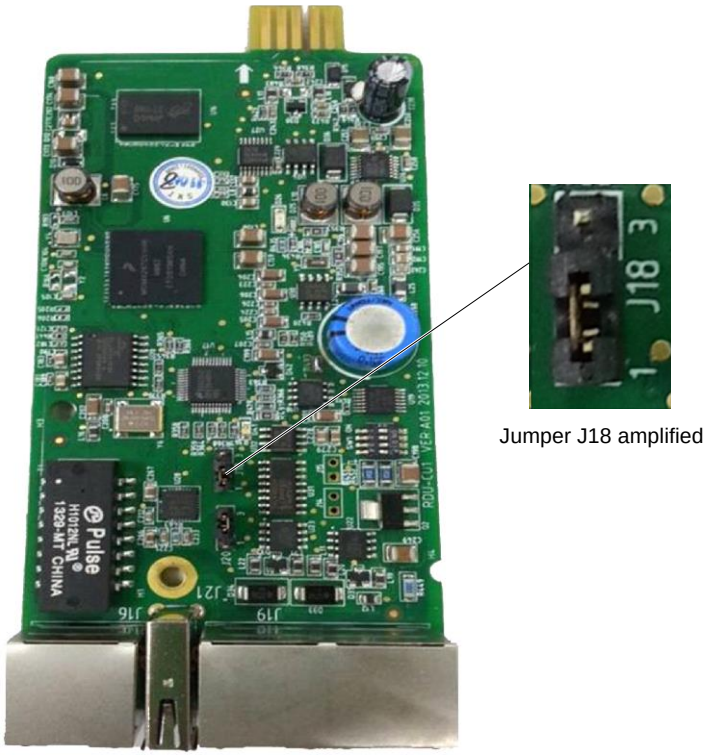


Figure 4-1 Position of jumper J18

4.2 FAQ

Q1: After RDU-SIC 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 with that the communication of COM port is abnormal?

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:

Step 1: Ensure that the IP address is correct;

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

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:

1) Click the icon at the lower left corner, and type 'cmd' in the textbox, as shown in Figure 4-2.

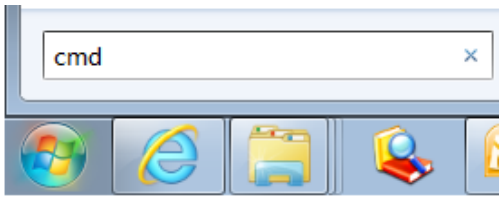


Figure 4-2 Typing 'cmd'

2) Press the Enter key, the page shown in Figure 4-3 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.

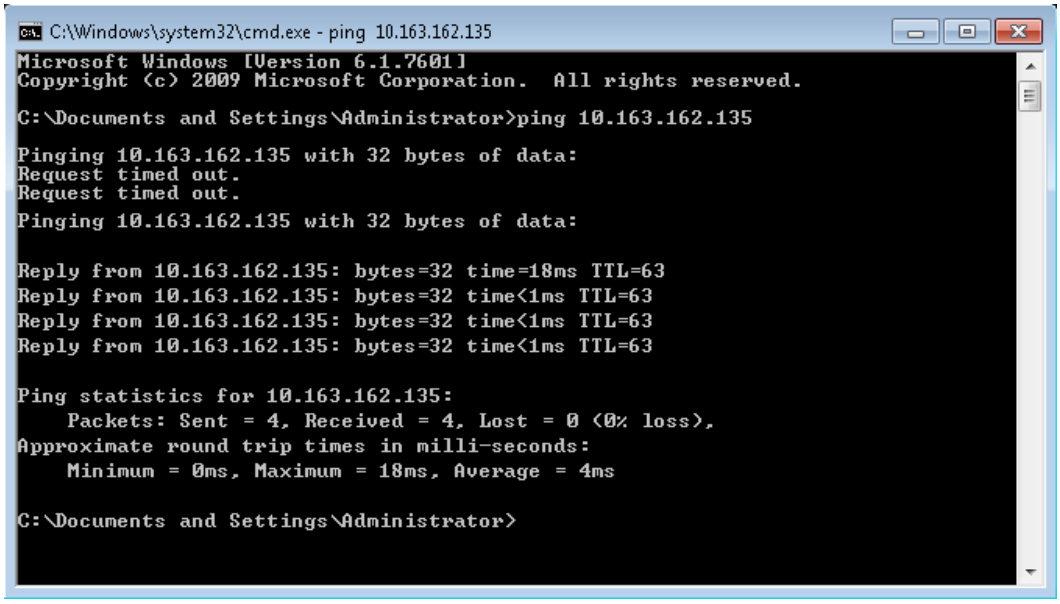


Figure 4-3 Communication test

Step 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 for the use of jumper cap.

Step 4: Refer to *3.1 Login Preparation* 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* in *3.4.3 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.

Appendix 1 Glossary

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

Appendix 2 Standard Configuration List

No.	Description	Number	Unit
1	RDU-SIC G2 intelligent port monitoring card	1	EA
2	User manual- 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

Appendix 3 Hazardous Substance or Elements Announcement

Parts	Hazardous Substances					
	Plumbum	Hydrargyrum	Cadmium	Chrome	PBB	PBDE
	Pb	Hg	Cd	Cr^{6+}	PBB	PBDE
PCBA	×	○	○	○	○	○
Cables	×	○	○	○	○	○
○: 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; ×: 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: RDU-SIC G2						