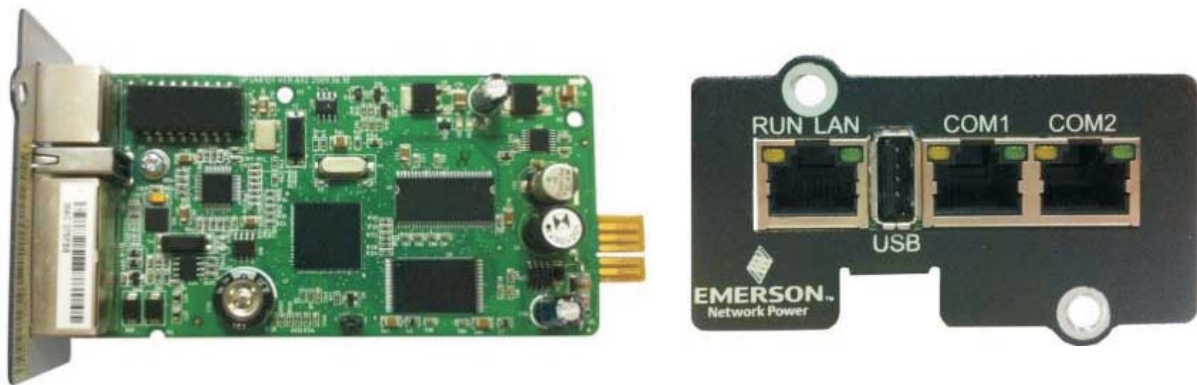


## SIC Card UF-SNMP810

User Manual – For APM, ITA, EPM, LTS, NX, NXC 30 - 40kVA, NXr And GXE Series UPS





## Application Scope

This manual is the user directions of the Site Interface Web/SNMP agent card (SIC card for short) V1.00. It will guide you through the installation, configuration, operation and troubleshooting of the SIC card.

The operation of the SIC card involves the monitored equipment, Web browser and network management system (NMS). This manual only deals with the SIC card-related operations. As for the use of other operation systems, please refer to relevant manuals.

## Reading Guide

This manual briefly introduces the SIC card and provides use directions, including installation, configuration and operation, ending with an appendix.

The manual contains eight independent chapters and an appendix. Except for the first chapter, you may choose to read all chapters according to you needs. However, if it is the first time you use the SIC card, we suggest you read through the manual to get an overall understanding. The following is the reading guide of each chapter.

| Chapter  | Reading guide   |
|--|---|
| Chapter 1 SIC Card Description                     | Provides a brief introduction to the SIC card, including its functions, technical specifications, models and appearance. This chapter will greatly help you to understand the following chapters  |
| Chapter 2 SIC Card Installation                    | Introduces the system requirement (including software environment and hardware environment) and installation of the SIC card. If you need to install the SIC card in your intelligent equipment, please read this chapter and Chapter 3 carefully. If you have already installed the SIC card and just want to use Web browser or NMS to monitor your intelligent equipment through the SIC card, you may skip this chapter and Chapter 3 |
| Chapter 3 Configuring SIC Card Basic Parameters    | Tells you how to configure the basic parameters (such as IP address) of the SIC card through Hyper Terminal and telnet. After installing the SIC card for the first time, you must configure its basic parameters before you can use it to monitor your intelligent equipment and the environment   |
| Chapter 4 Monitoring Method 1: Through Web Browser | Tells you how to use Web browser to monitor your intelligent equipment and the environment through the SIC card. If you need to use Web browser to monitor your intelligent equipment and the environment through the SIC card, please read this chapter carefully  |
| Chapter 5 Monitoring Method 2: Through NMS         | Tells you how to use the NMS to monitor your intelligent equipment and the environment through the SIC card. If you need to use the NMS to monitor your intelligent equipment and the environment through the SIC card, please read this chapter carefully  |
| Chapter 6 Monitoring Method 3: Through SiteMonitor | Tells you how to use the SiteMonitor software to monitor your intelligent equipment and the environment through the SIC card. If you need to use the SiteMonitor software to monitor your intelligent equipment and the environment through the SIC card, please read this chapter carefully  |
| Chapter 7 Guarding Computer With Network Shutdown  | Tells you how to use the SIC card and Network Shutdown computer safe shutdown program to protect your computer system in the case of a mains or UPS failure   |
| Chapter 8 Q's & A's                                | Lists fast Q's & A's in SIC card operation. If you encounter any questions during operation, to save your precious time, we suggest you quickly look through this chapter for solutions before seeking technical assistance from the local customer service center of Emerson Network Power Co., Ltd.   |

## Target

- User
- Technical support personnel, operation and maintenance personnel

## Glossary

UPS: uninterruptible power supply

NMS: network management system. For example, HP OpenView, IBM NetView or Novell Network NMS

SNMP: simple network management protocol

MIB: management information base

HTTP: hypertext transfer protocol

Web browser: such as Internet Explorer, FireFox

SiteMonitor: a network management software for equipment room power and environment developed by Emerson Network Power Co., Ltd.

Network Shutdown: a computer safe shutdown program developed by Emerson Network Power Co., Ltd.

Trap: SNMP trap, non-request information sent by SIC card to NMS

NTP: network time protocol

TFTP: trivial file transfer protocol

# Contents

|   |    |
|---|----|
| Chapter 1 SIC Card Description.....   | 1  |
| 1.1 Function .....  | 1  |
| 1.2 Technical Specifications .....  | 1  |
| 1.3 Models & Appearance.....  | 2  |
| Chapter 2 SIC Card Installation.....  | 3  |
| 2.1 System Requirement .....  | 3  |
| 2.2 Unpacking Inspection.....   | 3  |
| 2.3 Installation Preparation .....  | 3  |
| 2.4 Installing SIC Card .....   | 4  |
| Chapter 3 Configuring SIC Card Basic Parameters .....                                   | 5  |
| 3.1 Login & Logout.....   | 5  |
| 3.1.1 Using TTY Or Telnet To Login SIC Card .....                                       | 5  |
| 3.1.2 Logout.....   | 6  |
| 3.2 Using Super User To Configure Basic SIC Card Parameters Through TTY Or Telnet ..... | 7  |
| 3.2.1 Basic Commands .....  | 7  |
| 3.2.2 Configuring Basic Parameters .....  | 7  |
| 3.3 Using Reset User To Configure Basic SIC Card Parameters Through TTY .....           | 10 |
| 3.3.1 Basic Commands .....  | 10 |
| 3.3.2 Configuring Basic Parameters .....  | 10 |
| Chapter 4 Monitoring Method 1: Through Web Browser .....                                | 12 |
| 4.1 Checking Web Browser Settings.....  | 12 |
| 4.2 Using Web Browser To Login SIC Card.....  | 13 |
| 4.3 Monitoring Homepage.....  | 14 |
| 4.4 Adding Equipment.....   | 15 |
| 4.5 Viewing Equipment Status .....  | 15 |
| 4.6 Controlling And Configuring Equipment Remotely .....                                | 17 |
| 4.6.1 Controlling Equipment Remotely .....  | 17 |
| 4.6.2 Configuring Equipment Remotely .....  | 18 |
| 4.7 Viewing Sensor Status And Parameters .....  | 19 |
| 4.8 Viewing Alarms .....  | 19 |
| 4.8.1 Viewing Active Alarms .....   | 19 |
| 4.8.2 Viewing Historical Alarms .....   | 20 |
| 4.9 Viewing And Configuring Data Record.....  | 20 |
| 4.9.1 Viewing Data Record.....  | 20 |
| 4.9.2 Configuring Data Record .....   | 21 |
| 4.10 Configuring SIC Card System .....  | 21 |
| 4.10.1 Configuring User Password .....  | 21 |

|   |    |
|---|----|
| 4.10.2 Configuring Authentication Mode.....                             | 22 |
| 4.10.3 Configuring Terminal Access Mode.....                            | 23 |
| 4.10.4 Configuring SNMP Agent Parameters And Conducting Trap Test ..... | 24 |
| 4.10.5 Configuring E-Mail Parameters And Conducting E-Mail Test .....   | 27 |
| 4.10.6 Configuring Network Parameters.....                              | 29 |
| 4.10.7 Configuring System Time .....                                    | 30 |
| 4.10.8 Configuring Identification Information .....                     | 31 |
| 4.10.9 System Reboot.....   | 31 |
| 4.11 Viewing SIC Card Version Information.....                          | 32 |
| Chapter 5 Monitoring Method 2: Through NMS.....                         | 33 |
| 5.1 Protocol And NMS Supported By SIC Card .....                        | 33 |
| 5.2 Installing Equipment MIB .....                                      | 33 |
| 5.3 Applying For Management Authority.....                              | 33 |
| Chapter 6 Monitoring Method 3: Through SiteMonitor .....                | 36 |
| Chapter 7 Guarding Computer With Network Shutdown.....                  | 37 |
| Chapter 8 Q's & A's.....  | 38 |
| 8.1 Q's & A's In Installation .....                                     | 38 |
| 8.2 Q's & A's In Running.....   | 38 |
| 8.3 Q's & A's In Web Monitoring .....                                   | 39 |
| 8.4 Q's & A's In NMS Monitoring .....                                   | 40 |
| 8.5 Q's & A's In SiteMonitor Monitoring .....                           | 44 |
| 8.6 Q's & A's In Using Network Shutdown .....                           | 44 |

# Chapter 1 SIC Card Description

This chapter gives a brief introduction to the SIC card, including its functions, technical specifications, models and appearance.

## 1.1 Function

The SIC card is a network management card. It can make your Emerson intelligent equipment real network equipment, such as UPS, air conditioner, static transfer system (STS), server power management system (SPM), and so on. The SIC card can also connect to IRM series sensors to provide environment monitoring function. In the case of equipment alarm, it notifies the user by recording, sending Trap message, or sending E-Mail.

The SIC card provides three approaches for you to monitor your intelligent equipment and equipment room environment:

- Web browser. You can use Web browser to monitor your intelligent equipment and equipment room environment through the Web server function provided by the SIC card
- NMS. You can use NMS to monitor your intelligent equipment and equipment room environment through the SNMP agent function provided by the SIC card
- SiteMonitor. SiteMonitor is a piece of network management software for equipment room power and environment. You can use SiteMonitor to monitor your intelligent equipment and equipment room environment through the TCP/IP interface provided by the SIC card

The SIC card can also work with the Network Shutdown computer safe shutdown program developed by Emerson Network Power Co., Ltd. to provide automatic safe shutdown function for your computer installed with Network Shutdown, so as to prevent data loss.

## 1.2 Technical Specifications

- Network type: automatically adapt to 10/100MB/s Ethernet
- Concurrent Web browsers' number: 10
- Concurrent NMS number: 10
- Protocol : SNMP v2c and SNMP v1
- Concurrent SiteMonitor and Network Shutdown number: 200
- E-Mail recipient number: 10
- Total alarm records: 2048 pieces
- Total data records: 2048 pieces

### 1.3 Models & Appearance

The SIC card is a built-in card, available in two models: UF-SNMP710 and UF-SNMP810. Its appearance is shown in Figure 1-1. Its hardware functions are described in Table 1-1.

**Note**

The SIC card should be inserted in the SNMP interface or intellislot intelligent slot of the Emerson intelligent equipment. The two models of the card look completely the same except that they differ slightly in size to suit the SNMP interface or intellislot intelligent slot of different specifications.

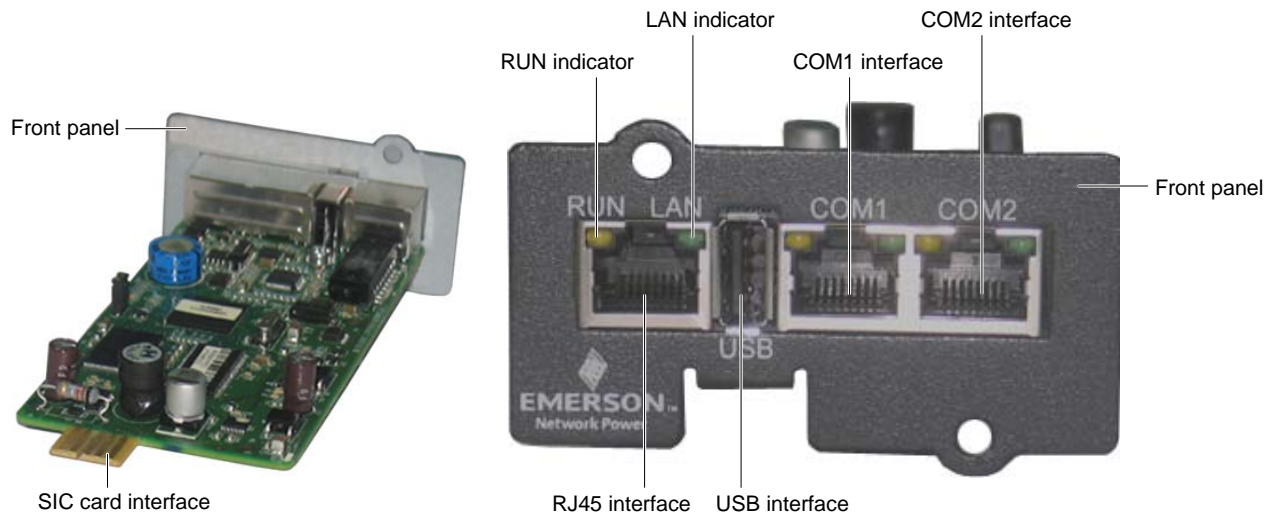


Figure 1-1 SIC card appearance

Table 1-1 SIC card hardware description

| Component              | Function  |
|------------------------|---|
| LAN indicator (green)  | Off: The network cable is not connected<br>On: The network cable is connected   |
| RUN indicator (yellow) | On: The SIC card is on<br>Blink once every second: The communication between the SIC card and the main equipment (the intelligent equipment that accommodates the SIC card) is normal.<br>Blink once every five seconds: The communication between the SIC card and the main equipment is interrupted |
| RJ45 interface         | Connect to the network  |
| SIC card interface     | To be inserted into SNMP interface or intellislot intelligent slot of intelligent equipment   |
| USB interface          | Connect to computer by means of the accessory USB communication cable. Used for parameter configuration   |
| COM1 interface         | Connect to intelligent equipment or sensor  |
| COM2 interface         |   |



## Chapter 2 SIC Card Installation

This chapter deals with the SIC card installation, including the system requirement, unpacking inspection, installation preparation and procedures of the SIC card.

---

### Warning

Some electronic components on the SNMP card are sensitive to static electricity. Do not touch the circuit or components with hands or through electrified articles, otherwise the card might be damaged. Hold the side edges when moving or installing the card.

---

## 2.1 System Requirement

### Hardware requirement

- Emerson intelligent equipment with SNMP interface or intellislot intelligent slot matching your SIC card size
- IRM series sensors

### Software requirement

1. Local area network (LAN), metropolitan area network (MAN), or wide area network (WAN), 10 MB/s or 100MB/s Ethernet, using TCP/IP protocol and HTTP protocol.
2. Computer with one of the following installed:
  - Web browser: Internet Explorer 5.0 or above, FireFox 1.0 or above
  - NMS compatible with SNMPv1 and SNMP v2c protocols: HP OpenView, IBM NetView, Novell ManageWise or SunNet Manager, and so on
  - Emerson-developed SiteMonitor, a network management software for equipment room power and environment

## 2.2 Unpacking Inspection

Open the package of the SIC card, take out the delivery list, and check the goods against the delivery list. Report any discrepancy to your dealer.

## 2.3 Installation Preparation

Before installation,

1. Use the delivery accessory USB communication cable to connect the USB interface of the computer to that (see Figure 1-1) of the SIC card.

For the first time the SIC card is installed, please install the USB driver from the CD delivered with the SIC card, and note down the used serial port number of the computer according to the answer to question 2 in *8.1 Q's & A's In Installation*.

2. Start Hyper Terminal, and correctly configure the serial port property of the Hyper Terminal according to the instructions provided in the part *Using TTY to login SIC card* in *3.1.1 Using TTY Or Telnet To Login SIC Card*. Note that the serial port for Hyper Terminal must be the one connected to the SIC card.
3. Prepare a category 5 twisted pair cable for connecting the card to the Ethernet, and connect one end to the network.

---

### Note

For 100MB/s Ethernet, please use super category 5 twisted pair cable meeting EIA/TIA 568 standard. Otherwise the network cable length must be limited within 100m, and the conducted emission will increase slightly.

---

## 2.4 Installing SIC Card

---

**Note**

The SIC card is hot-pluggable, you can install it without turning off the intelligent equipment.

---

Use the following procedures to install the SIC card:

1. Remove the cover of the SNMP interface or intellislot intelligent slot of the intelligent equipment.

Retain the screws and the cover for use in the future. Refer to the user manual of the intelligent equipment for the location of the SNMP interface or intellislot intelligent slot.

2. Insert the SIC card into position along the guide grooves on both sides of the SNMP interface or intellislot intelligent slot, and tighten the screws.

3. Connect the network cable to the RJ45 interface (see Figure 1-1) of the SIC card.

At this point, you will see the green indicator (LAN indicator) turn on. When the card is connected to the network and there is ongoing data exchange, the yellow indicator (RUN indicator) will blink, indicating the card is working. Observe the Hyper Terminal screen on the computer, and you will see the SIC card login information, as shown in Figure 2-1.

```
Insmod Device Driver
Emerson SNMP WDT driver version: 1.00
Found AT91 i2c
PCF8563 Real-Time Clock Driver, $Revision: 1.16 $
Emerson SNMP FLASH driver version: 1.00
Emerson SNMP SPI driver version: 1.00
sic login: _
```

Figure 2-1 SIC card login information

If the yellow indicator is off, please check whether the SIC card is connected to the network and whether there is something wrong with the network cable.

4. If you need to monitor more pieces of intelligent equipment or connect the SIC card to sensors, please connect the RJ45 interface of the RS485 optional card of the intelligent equipment or the RJ45 interface of the sensor to the COM1 or COM2 interface (see Figure 1-1) of the SIC card. The SIC card can cascade-connect up to three pieces of intelligent equipment and six sensors.

## Chapter 3 Configuring SIC Card Basic Parameters

You may configure the basic parameters of the SIC card through Hyper Terminal (TTY) or Remote Login (Telnet or SSH), including the card IP address and super user password. If the card is installed for the first time or you do not know the card IP address, you must use Hyper Terminal to configure the basic parameters of the card. If you know the card IP address, you can configure the card basic parameters through Telnet.

This chapter tells how to configure the basic parameters of the SIC card through TTY and Telnet.

### Note

1. The configuration modes (TTY, Telnet, SSH) of the SIC card basic parameters have the same interface.
2. The default remote login access mode of SIC card is Talent. If you want to change it, set it through Web browser, refer to *4.10.3 Configuring Terminal Access Mode*.
3. The SSH version supported by SIC card is SSH2, and only user name + password is identified.

## 3.1 Login & Logout

### 3.1.1 Using TTY Or Telnet To Login SIC Card

#### Using TTY to login SIC card

TTY is a system tool of Windows. For the creation and start of TTY, please refer to relevant computer OS manual.

When creating TTY, note that the serial port No. is the one that connects to the SIC card. Refer to Question 2 in *8.1 Q's & A's In Installation* to obtain the serial port No.. Refer to Table 3-1 for serial port configuration.

Table 3-1 TTY serial port configuration

| Parameter    | Setting   |
|--------------|-----------|
| Baud rate    | 115200bps |
| Data bit     | 8         |
| Parity check | None      |
| Stop bit     | 1         |
| Flow control | None      |

After the SIC card starts up, press the Enter key, and the system will prompt login information.

#### Using Telnet to login SIC card

To log in SIC card, you can use the Telnet client from the operation system. Type the 'telnet SIC card IP address' in the command line, for example, 'telnet 10.76.12.228', and the system will prompt login information.

#### Using SSH to login SIC card

The client for supporting SSH2 is required. To successfully log in SIC card, you should configure the correct host IP address (IP address of SIC card) and access port in client, then enter the user name and password.

#### Login information

Figure 2-1 shows the login information. Enter the user name and password. The password will not be displayed, as shown in Figure 3-1.

```
Insmod Device Driver
Emerson SNMP WDT driver version: 1.00
Found AT91 i2c
PCF8563 Real-Time Clock Driver, $Revision: 1.16 $
Emerson SNMP FLASH driver version: 1.00
Emerson SNMP SPI driver version: 1.00

sic login: admin
Password: _
```

Figure 3-1 Enter user name and password

If you login successfully, the system will display the login interface and the command prompt, super user is **sic\_admin#**, as shown in Figure 3-2, and reset user is **sic\_reset#**, as shown in Figure 3-3.

```

Site Interface Card
MontaVista(R) Linux(R) Professional Edition 3.1

*****
*
*   Service Terminal for Site Interface Card
*
*   Copyright(c) 2008-2010, Emerson Network Power Co., Ltd.
*   ALL RIGHTS RESERVED
*
*   Version 1,0   Date 2008-4-16
*
*****

sic_admin#

```

Figure 3-2 Successful login of super user

```

Site Interface Card
MontaVista(R) Linux(R) Professional Edition 3.1

*****
*
*   Service Terminal for Site Interface Card
*
*   Copyright(c) 2008-2010, Emerson Network Power Co., Ltd.
*   ALL RIGHTS RESERVED
*
*   Version 1.0   Date 2008-4-16
*
*****

sic_reset#

```

Figure 3-3 Successful login of reset user

If your user name or password is incorrect, the system will not allow you in and will prompt you to enter them again.

#### Note

1. Only the super user admin can log in the SIC card through Hyper Terminal or Telnet. The default password of admin is admin. The password is case sensitive.
2. Reset user (reset is the user name) can access the SIC card through Hyper Terminal. The password is reset, which can not be changed. The password is case sensitive.
3. For Telnet mode, only two users can login at the same time.

## 3.1.2 Logout

### Manual Logout

After configuring the basic parameters of the SIC card, you may type the **exit** or **logout** command to logout.

### Automatic Logout

If you have not done any key operation within five minutes, the system will log you out automatically to ensure system safety.

### Re-login after logout

If you adopt TTY mode, you may simply re-enter your user name and password to re-login; but in Telnet mode, you have to rebuild Telnet connection.

## 3.2 Using Super User To Configure Basic SIC Card Parameters Through TTY Or Telnet

### 3.2.1 Basic Commands

TTY and Telnet in super user support the commands shown in Table 3-2.

Table 3-2 Command supported by TTY and Telnet

| Command  | Description   |
|----------|---|
| help     | View the commands supported by SIC card   |
| logout   | Manually logout   |
| password | Modify the password of super user admin   |
| ping     | Check whether the destination address is reachable                              |
| reboot   | Your are required to reboot the SIC card after modifying some system parameters |
| setmode  | Set the SIC card as a normal operating mode                                     |
| setip    | Set the card IP address, subnet mask, gateway address                           |
| setaddr  | Reserved  |
| version  | View SIC card application version and operation system version                  |

After you log in the SIC card, type the command 'help' or '?' after **sic\_admin#**, and press the **Enter** key, the system will prompt all the commands and their descriptions, as shown in Figure 3-4.

```
sic_admin#?
Following commands are supported:
?           - alias for help
help        - print online help
logout      - logout from the current console
password    - change password
ping        - detect network status
reboot      - reboot system
setmode     - set normal mode
setip       - set ip address
setaddr     - set modbus address
version     - view version info

sic_admin#
```

Figure 3-4 Command supported by TTY and Telnet in super user

### 3.2.2 Configuring Basic Parameters

Type a command behind **sic\_admin#**. If the command is incorrect, the system will prompt **command not found**. If you have typed a command corresponding to a parameter, the system will prompt you to configure the parameter. At first the system will display the current setting, and prompt you to select the command ID to confirm or modify the current setting, as shown in Figure 3-5.

```
1. confirm current setting
2. modify current setting
```

Figure 3-5 Command ID selection prompt

#### Note

When typing a command, you may just type the first several letters of it, the SIC card can identify them, for example, pi for ping.

1. Password: change the password of the super user admin

#### Warning

Keep in mind the password of admin. If you forget it, you can use the USB (accessory) to connect the SIC card. Then use the reset user to log in, the password of admin will be resumed to the default password admin.

Because admin has the highest authority, to ensure the safety of the connected equipment and sensors, we suggest you change the password of admin immediately after installing the SIC card.

Configuration method: type **password** after **sic\_admin#**

Configuration steps: see Figure 3-6.

```
sic_admin#password
Changing password for admin
Please use a combination of upper and lower case letters and numbers.
Enter new password(maximum of 31 characters):

Warning: weak password--too short(continuing...)
Warning: weak password--too simple(continuing...)
Re-enter new password:

Password changed.
sic_admin#
```

Figure 3-6 Modify login password

Interface description:

Input the new password(31 at most) ——the password will not be displayed.

Confirm the new password.

If the password is not strong enough, the following warning will be displayed:

**Warning: weak password—too short(continuing...)**

**Warning: weak password—too simple(continuing...)**

2. ping: check if the destination address is reachable

The ping command is used to test whether data from the SIC card can be sent to certain computer through network.

Configuration method: type **ping** after **sic\_admin#**

Configuration steps: see Figure 3-7.

```
sic_admin#ping
Please enter an IP address:127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes
84 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.4 ms
84 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.3 ms
84 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.3 ms
84 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.3 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.4 ms
sic_admin#_
```

Figure 3-7 Ping command

3. Setmode: The SIC card should be in normal operating state

Setmode command is used for resuming the SIC card to normal operating mode if the SIC card has incorrect operating mode. Generally, the customer service will diagnose and handle it.

4. Setip: set the SIC card IP address, subnet mask, and gateway address

If the SIC card is installed for the first time or moved from one LAN to another, you must set the card network parameters including the IP address through TTY.

Configuration method: type **setip** after **sic\_admin#**

Configuration steps: see Figures 3-8 through 3-10.

```
sic_admin#setip
Mode:          static
IP Address:    192.168.1.1
Subnet Mask:   255.255.255.0
Default Gateway: 0.0.0.0

1. confirm current setting
2. modify current setting

please select the command id:
```

Figure 3-8 Select the command ID

```

sic_admin#setip
Mode:          static
IP Address:    192.168.1.1
Subnet Mask:   255.255.255.0
Default Gateway: 0.0.0.0

1. confirm current setting
2. modify current setting

please select the command id:2
Obtain an IP address automatically? Y/N:y
The system is going down NOW !!

```

Figure 3-9 Obtain an IP address automatically

```

sic_admin#setip
Mode:          static
IP Address:    192.168.1.1
Subnet Mask:   255.255.255.0
Default Gateway: 0.0.0.0

1. confirm current setting
2. modify current setting

please select the command id:2
Obtain an IP address automatically? Y/N:n
input IP Address:142.100.8.36
input NetMask:255.255.254.0
input Default GateWay:142.100.8.1
The system is going down NOW !!

```

Figure 3-10 Set SIC card IP address

**Interface description:**

After you enter the command **setip**, the system will display the current SIC card network mode, IP address, subnet mask and gateway address. Command ID 1 means to confirm the current settings, that is not to change them. Command ID 2 means to change them.

**Obtain an IP address automatically?** The system prompts you to select whether to obtain the IP address automatically or manually set it. Entering **Y** or **y** means to obtain the IP address automatically; entering **N** or **n** means to manually set it.

If you select to manually set it, you need to set the IP address, subnet mask and gateway.

If the network address you entered is illegal, the system will prompt **input wrong IP Address! please input again**, or **input wrong NetMask! please input again**, or **input wrong GateWay! please input again**.

If your setting is wrong for three times, the system will prompt **input wrong more than 3 times**, and exit the setip command.

If the command ID you enter is invalid, the system will prompt **command is wrong. please input again**. In this case, please enter a valid command ID.

After you obtain the IP address automatically or manually set it, the system will be rebooted automatically.

**Note**

If you need to use the Dynamic Host Configure Protocol (DHCP) function, you should contact your network administrator to make sure the system has a DHCP server.

It is suggested that you contact your network administrator to bind the MAC address of the SIC card with the obtained IP address, so that the current IP address will be allocated to the SIC card in future IP address allocation. For obtaining the MAC address, refer to 4.10.6 *Configuring Network Parameters*.

5. version: view the SIC card application version and operation system version

Viewing method: type **version** after **sic\_admin#**, as shown in Figure 3-11.

```

sic_admin#version

Application Module
  Version: V100B000D000
  Date: 2008-04-09
  Time: 19:10:00

Linux OS
  Version: 2.4.20_mvl31-integrator
  Date: 2007-10-22
  Time: 18:21:13

sic_admin#

```

Figure 3-11 View SIC card version

Interface description:

**Application Module:** the application of the SIC card.**Linux OS:** the operating system adopted by SIC card.

### 3.3 Using Reset User To Configure Basic SIC Card Parameters Through TTY

#### 3.3.1 Basic Commands

TTY in reset user supports the commands shown in Table 3-3.

Table 3-3 Command supported by TTY

| Command        | Description   |
|----------------|---|
| help           | View the commands supported by SIC card   |
| logout         | Manually logout   |
| all            | Resume user password, network parameter, authentication mode, terminal access mode to default |
| password       | Resume the password of super user to admin, and general user to user                          |
| network        | Resume the IP of SIC card to 192.168.1.1, and subnet mask to 255.255.255.0                    |
| authentication | Resume the authentication mode to local authentication  |
| console        | Resume the terminal access mode to Telnet access  |

After you log in the SIC card, type the command 'help' or '?' after **sic\_reset#**, and press the **Enter** key, the system will prompt all the commands and their descriptions, as shown in Figure 3-12.

```

sic_reset#?

Following commands are supported:

?           - alias for help
help        - print online help
logout      - logout from the current console
all         - reset all (password, network, authentication, console)
password    - reset password (admin/admin)
network     - reset network (192.168.1.1/255.255.255.0)
authentication - reset authentication (local authentication)
console     - reset console (telnet access)

sic_reset#

```

Figure 3-12 Command supported by TTY and Telnet in reset user

#### 3.3.2 Configuring Basic Parameters

Type a command behind **sic\_reset#**. If the command is incorrect, the system will prompt **command not found**. If you have typed a command corresponding to a parameter, the system will resume the default setting of corresponding parameters. After every command is executed, the SIC card will restart, as shown in Figure 3-13.



```
sic_reset#all
The system is going down NOW !!
Sending SIGTERM to all processes.
Sending SIGKILL to all processes.
device_release(c1408d00,c1494a20)
Please stand by while rebooting the system.
Restarting system.

Testing Watchdog...
```

Figure 3-13 Command executed in reset user

---

 **Note**

1. When inputting command, the SIC card can support fast identification, that is, use the front several characters used to distinguish this command to represent the whole command input, and without inputting the whole command. For example, pass means password.
  2. Reset user (reset is the user name) can access the SIC card only through Hyper Terminal. The password id reset, which can not be changed. The password is case sensitive.
-

## Chapter 4 Monitoring Method 1: Through Web Browser

This chapter tells how to use Web browser to monitor the intelligent equipment and environment in real time, control and configure the intelligent equipment remotely, view alarm information, configure SIC card system parameters, and view SIC card version information.

### 4.1 Checking Web Browser Settings

Before using Web browser to monitor the intelligent equipment and environment, please verify that your Web browser meets the requirement listed in this section.

#### Browser type and version

The SIC card supports the following browsers:

- Internet Explorer 5.0 or above
- FireFox 1.0 or above

The SIC card might support other browser types compatible with HTTP1.1, HTML4.0 and JavaScript1.0, but this is not for sure.

The SIC card supports Chinese and English. If you select Chinese, the browser must support simplified Chinese (GB2312) character set but not necessarily be Chinese version. If your browser cannot display Chinese, please upload or install corresponding software components. Future version SIC card will support more languages.

#### Enabling graphic and animation display

Your browser must be able to display graphic and animation

#### Enabling JavaScript

Your browser must allow JavaScript. The setting method is as follows:

- Internet Explorer: **Tools->Internet Options->Security->Custom Level**, scroll down to **Scripting->Active Scripting**, select **Enable** and click **OK**
- FireFox: **Tools->Options**, choose **Web Features** from the left navigation bar, select the checkbox next to **Enable JavaScript** and click **OK**

#### Web page Cache setting

Browsers use Cache (called temporary file in IE) to increase web page display speed. When you visit web pages in the Cache, the browser will check whether there is any new version of them in Web server according to the configuration below:

- Check every time visiting pages
- Check every time starting the browser
- Automatic
- No check

When visiting the SIC card, the configuration must be **Automatic**. Otherwise, the monitoring web pages cannot be displayed normally. For example, the newly opened web page is still the web page before you exit the browser last time. The configuration steps for common Web browsers are as follows:

- Internet Explorer: **View->Internet Options->General->Internet Temporary Internet files->Settings->Check for newer version of stored pages->Every visit to the page**
- FireFox: **Tools->Options->cache**, select the editbox next to **check\_doc\_frequency**, and input '1'

#### Definition and browser font setting

We recommend you to set the monitor definition to 1024×768 or above. Otherwise, the monitoring page might not be displayed fully.

If your monitor definition is 1024x768, but you still cannot view the full page, please decrease the browser font and close less useful tool bars to increase the valid display area.

## 4.2 Using Web Browser To Login SIC Card

### Login

Start the Web browser, type the IP address of the SIC card, and the login interface will appear, as shown in Figure 4-1.

Figure 4-1 Login SIC card

Enter your user name and password, and click the **OK** button.

### Note

For the first time you access the new SIC card through Web browser, you must login with super user's name "admin" and password ("admin" by default).

### Language selection

After your user name and password pass the verification, the monitoring homepage of the SIC card will appear, as shown in Figure 4-2.


Main menu area

Display area

Figure 4-2 Monitoring homepage

The monitoring homepage provides a language selection drop-down box at the upper right corner. During interface operation, whenever you wish to change the display language, you may click this drop-down box to select the language.

---

 **Note**

The default display language is the language of the current browser.

---

---

 **Warning**

If you are super user or have control authority, do remember to close the browser before you leave. Otherwise, if somebody else uses your account to issue equipment control command, the consequence might be serious!

---

## 4.3 Monitoring Homepage

### Main menu area and display area

As shown in Figure 4-2, the monitoring homepage consists of the main menu area and display area.






#### 1. Main menu area

The main menu area displays the main Web monitoring function options of the SIC card: **Equipment Monitor, Alarm Manage, Data Analysis, System Configure, About**. Click a function option button, and the monitoring page of the corresponding main menu will appear.

#### 2. Display area

The display area displays the page information of the selected main menu.

### Status icons

As shown in Figure 4-2, the monitoring pages present the equipment status and sensor status with three icons:  for normal status,  for general alarm,  for serious alarm. The figure following the icons  and  represents the alarm number.

## 4.4 Adding Equipment

The SIC card can automatically search the connected intelligent equipment and sensors. The intelligent equipment and sensors the SIC card searched out are displayed respectively under **Device** and **Sensor** in the display area, as shown in Figure 4-3. For those not searched out, you need to click the **Add Device** button at the lower left corner of the monitoring homepage to enter the equipment adding page shown in Figure 4-3 and add them under **Device** and **Sensor** as appropriate.

Figure 4-3 Equipment adding page

Procedures are as follows:

1. Select the intelligent equipment type or sensor type from the **Device Type** drop-down box.
2. Select the port of the SIC card connected to the intelligent equipment and sensor from the **Port** drop-down box.
3. Type the address of the intelligent equipment or sensor in the **Address** box. The address should be exclusive.
4. Select the communication baud rate from the **Communication Rate** drop-down box.
5. Click the **Confirm** button, and the intelligent equipment or sensor will be added under **Device** and **Sensor** as appropriate.



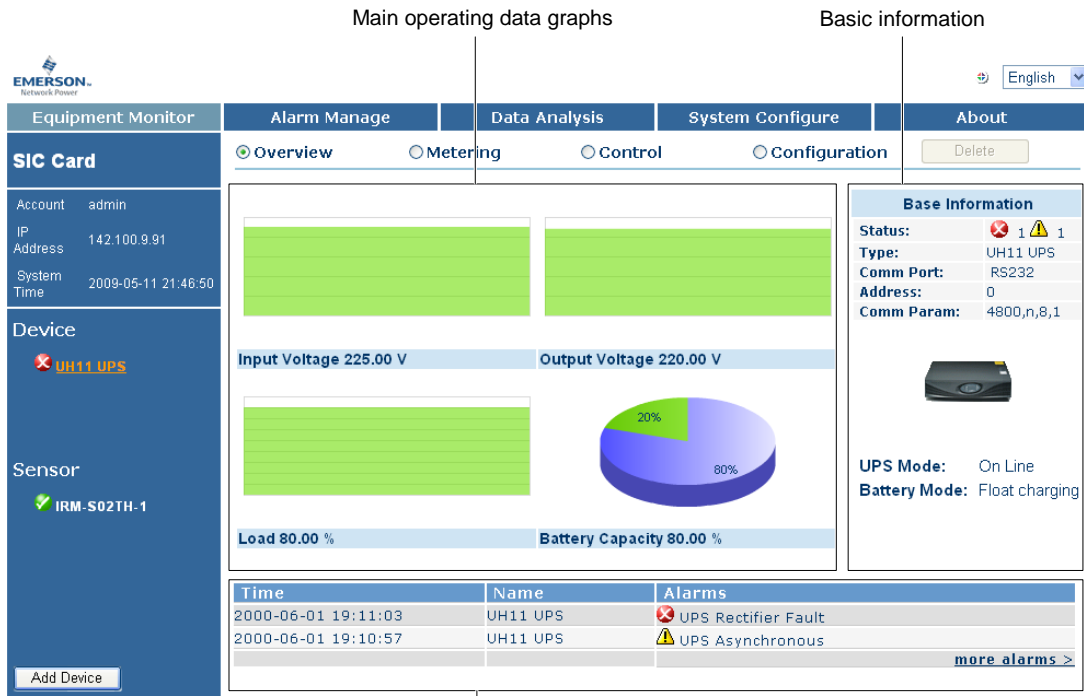
### Note

1. There are two naming rules for the intelligent equipment and sensors under **Device** and **Sensor**:
  - 1) The name of the main equipment, which accommodates the SIC card, is the equipment type itself. For example, **UH11 UPS** in Figure 4-3.
  - 2) The names of the intelligent equipment and sensors connected to the COM1 and COM2 interfaces of the SIC card are composed of the corresponding equipment type and address. For example, **IRM-S02TH-1** in Figure 4-3 consists of the equipment type 'IRM-S02TH' and address '1'.
2. The monitoring pages in this manual take UH11 UPS and IRM-S02TH-1 as examples. As different types of intelligent equipment and sensors have different monitoring parameters, the data in the monitoring pages you actually see may not be exactly the same as those in this manual.

## 4.5 Viewing Equipment Status

### Method 1

Select the main menu **Equipment Monitor**, click **UH11 UPS** under **Device**, and the overview page will appear, as shown in Figure 4-4. The overview page displays the main operating data graphs, basic information and active alarms of the equipment.



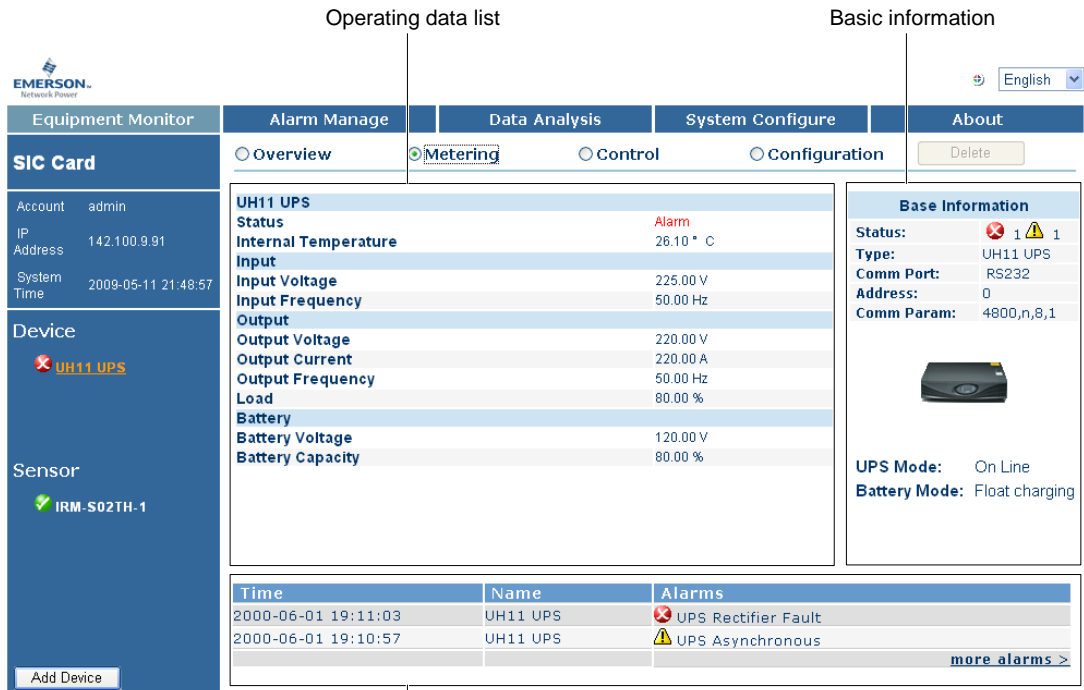
Active alarms

Figure 4-4 Overview page

This page can display up to six active alarms. To view more active alarms and historical alarms, click the **more alarms >** button at the lower right corner to enter the **Alarm Manage** main menu. Refer to 4.8 *Viewing Alarms*.

**Method 2**

Select the main menu **Equipment Monitor**, click **UH11 UPS** under **Device**, and select 'Metering', and the metering page will appear, as shown in Figure 4-5. The metering page displays the operating data list, basic information and active alarms of the equipment.



Active alarms

Figure 4-5 Metering page

In the operating data list, green status value means the corresponding equipment signal is normal, red status value means the corresponding equipment signal is in alarm.

## 4.6 Controlling And Configuring Equipment Remotely

### 4.6.1 Controlling Equipment Remotely

Select the main menu **Equipment Monitor**, click **UH11 UPS** under **Device**, and select 'Control', and the remote control page will appear, as shown in Figure 4-6. This page displays the remote control parameter list, basic information and active alarms.

Remote control parameter list

Basic information

EMERSON Network Power

Equipment Monitor

Alarm Management

Data Analysis

System Configure

About

SIC Card

Overview

Metering

Control

Configuration

Delete

Account admin

IP Address 142.100.9.91

System Time 2009-05-11 21:49:12

Device

UH11 UPS

Sensor

IRM-S02TH-1

Add Device

Base Information

Status: 1 1

Type: UH11 UPS

Comm Port: RS232

Address: 0

Comm Param: 4800,n,8,1

UPS Mode: On Line

Battery Mode: Float charging

| Time                | Name     | Alarms              |
|---------------------|----------|---------------------|
| 2000-06-01 19:11:03 | UH11 UPS | UPS Rectifier Fault |
| 2000-06-01 19:10:57 | UH11 UPS | UPS Asynchronous    |

more alarms >

Active alarms

Figure 4-6 Remote control page

In the remote control parameter list, you can select a command, and click the **Confirm** button to submit the command to the SIC card. If the SIC card successfully sends the command, the prompt **Success** will appear, otherwise the prompt **Communication Interrupt, Remote Control Failed** will appear.

### 4.6.2 Configuring Equipment Remotely

Select the main menu **Equipment Monitor**, click **UH11 UPS** under **Device**, and select 'Configuration', and the remote configuration page will appear, as shown in Figure 4-7. This page displays the remote configuration parameter list, basic information and active alarms.

Remote configuration parameter list
Basic information

**SIC Card**

Account: admin

IP Address: 142.100.9.91

System Time: 2009-05-11 21:49:22

**Device**

UH11 UPS

**Sensor**

IRM-S02TH-1

Add Device

**Configuration**

UPS turn off delay(sec): 120 [120 - 600]

UPS automatic restart delay(sec): 0 [0 - 43200]

Automatic restart enable: enable

Battery self test duration(sec): 5 [1 - 600]

Master,Slave,Single: Master

Master,Slave alternate work time(day): 7

Confirm

**Base Information**

Status: ✖ 1 ⚠ 1

Type: UH11 UPS

Comm Port: RS232

Address: 0

Comm Param: 4800,n,8,1

UPS Mode: On Line

Battery Mode: Float charging

| Time                | Name     | Alarms   |
|---------------------|----------|--|
| 2000-06-01 19:11:03 | UH11 UPS | <span style="color: red;">✖</span> UPS Rectifier Fault |
| 2000-06-01 19:10:57 | UH11 UPS | <span style="color: orange;">⚠</span> UPS Asynchronous |

[more alarms >](#)

Active alarms

Figure 4-7 Remote configuration page

In the remote configuration parameter list, the parameter values are the current remote configuration parameter values. If you need to change the value of a parameter, type or select the new value in the corresponding box, and click the **Confirm** button to submit the configuration command to the SIC card. If the parameter value is saved successfully, the prompt **Success** will appear, otherwise the prompt **Communication Interrupt, Remote Control Failed** will appear.



## 4.7 Viewing Sensor Status And Parameters

Select the main menu **Equipment Monitor**, click **IRM-S02TH-1** under **Sensor**, and the status data graphs, basic information and active alarms of the sensor will be displayed, as shown in Figure 4-8. The basic information of the sensor mainly provides the basic parameters of the sensor besides the sensor name, status icon, and so on.

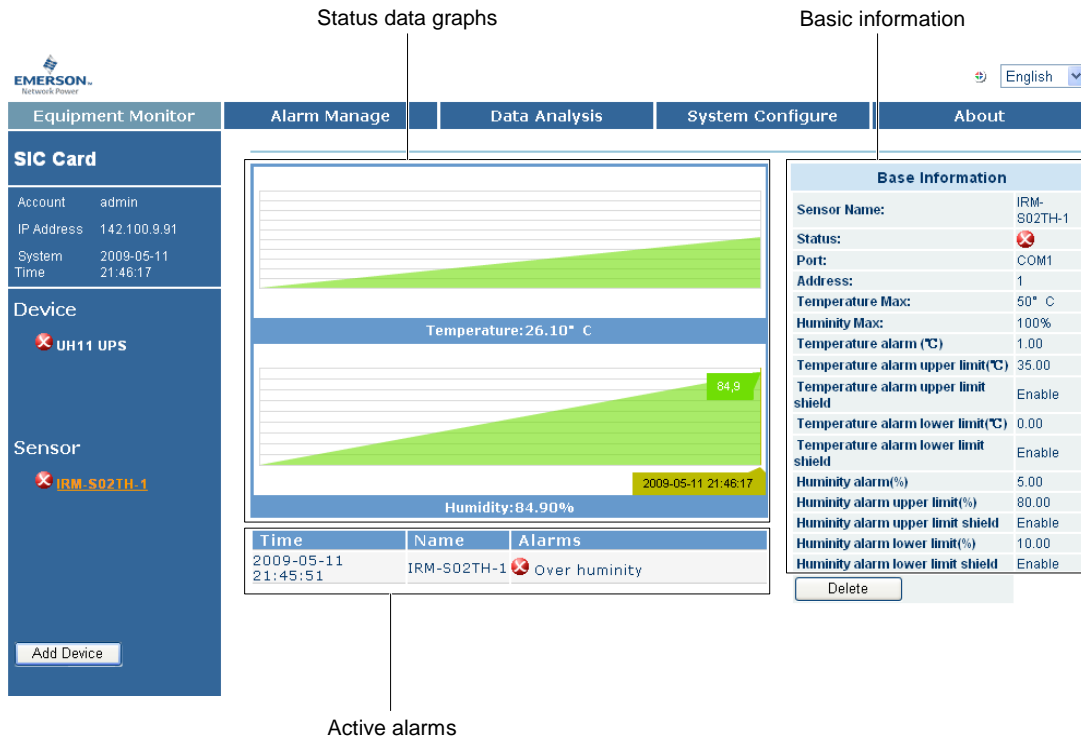


Figure 4-8 Sensor status and parameter page

## 4.8 Viewing Alarms

### 4.8.1 Viewing Active Alarms

Select the main menu **Alarm Manage**, click **Active Alarms**, and the active alarm page will appear, as shown in Figure 4-9. In this page, you can view all active alarms of the monitored intelligent equipment and sensors.

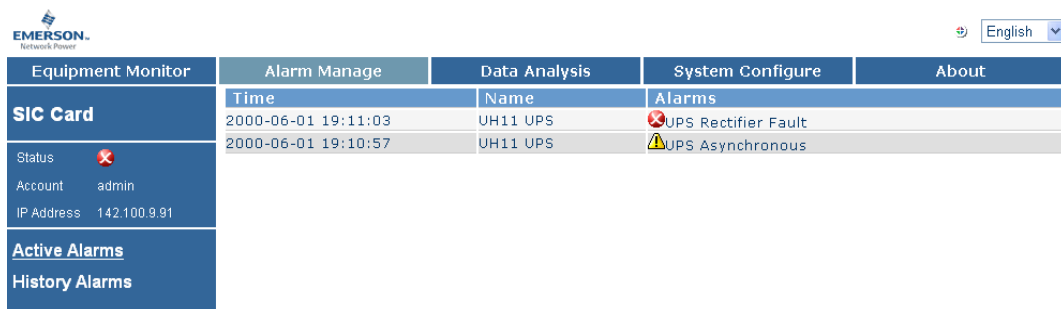


Figure 4-9 Active alarm page

### 4.8.2 Viewing Historical Alarms

Select the main menu **Alarm Manage**, click **History Alarms**, and the historical alarm page will appear, as shown in Figure 4-10. In this page, you can view all historical alarms of the monitored intelligent equipment and sensors.

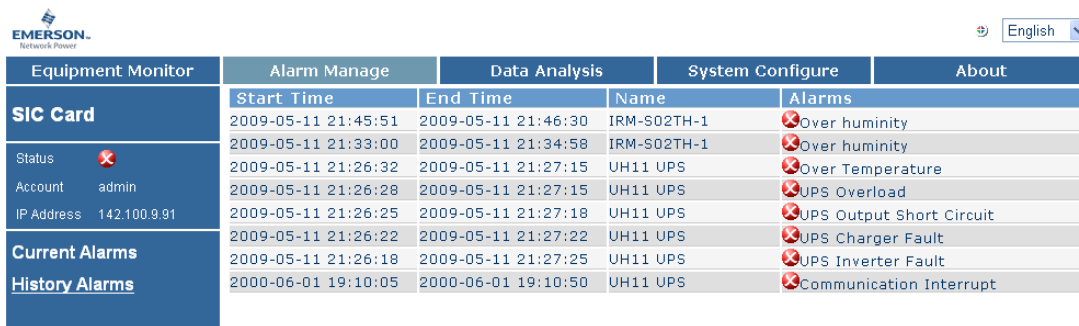


Figure 4-10 Historical alarm page

## 4.9 Viewing And Configuring Data Record

### 4.9.1 Viewing Data Record

Select the main menu **Data Analysis**, click **Data Record**, and the data record page will appear, as shown in Figure 4-11.

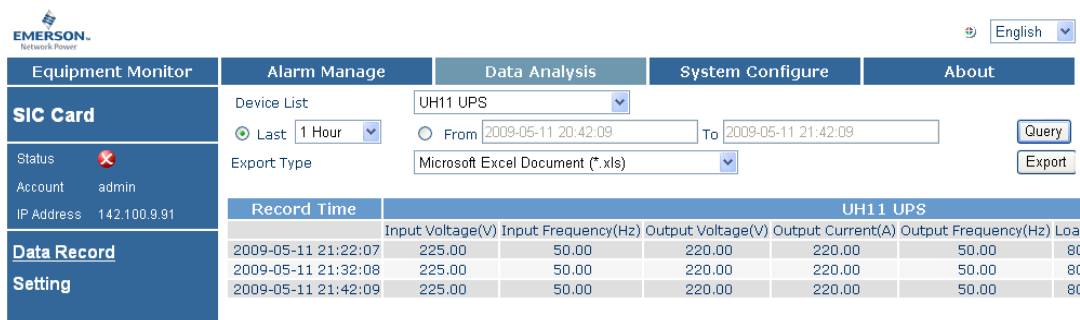


Figure 4-11 Data record page

You can select your desired intelligent equipment or sensor from the **Device List** drop-down box, and define the data record query period (the latest 1 hour by default). The data record page can display up to 2048 pieces of data records of the selected intelligent equipment or sensor. You can also export the displayed data record in Excel, XML, or Text format.

## 4.9.2 Configuring Data Record

Select the main menu **Data Analysis**, click **Setting**, and the data record setting page will appear, as shown in Figure 4-12. In this page, you can change the data record time interval.

Figure 4-12 Data record setting page

In the display area, the upper part displays **Current Setting**, including **Max Record Time** and **Time Interval**; the lower part displays **Configuration**, where you can change the current settings.

If you need to change the time interval of the data record, select 'Time Interval', type the new time interval, and click the **Submit** button to save the change. The setting range is from one minute to 24 hours. The default setting is 10 minutes.

## 4.10 Configuring SIC Card System

### 4.10.1 Configuring User Password

User password is used to verify the authority of the user who attempts to use Web browser to access the SIC card, so as to prevent illegal access and control, and ensure the safety of the equipment operation.

#### User authorization

The system has two users only: Administrator (user name "admin") and User (user name "user"). Neither of their user names can be changed. You can only change their passwords. The user authorization is shown in Table 4-1.

Table 4-1 User authorization

| User          | Authority   |
|---------------|---|
| Administrator | <input checked="" type="checkbox"/> Configuration <input checked="" type="checkbox"/> Control <input checked="" type="checkbox"/> Viewing |
| User          | <input type="checkbox"/> Configuration <input type="checkbox"/> Control <input checked="" type="checkbox"/> Viewing                       |

#### Changing user password

##### Note

- Administrator can change the passwords of both Administrator and User. User has no such authority.
- The default passwords of Administrator and User are respectively admin and user. To ensure system security, after installing the SIC card, please use the authority of Administrator to login the SIC card and change the passwords. Meanwhile, it is suggested that you change the passwords regularly.

Select the main menu **System Configure**, click **Account Management**, select 'Administrator' or 'User', and the page shown in Figure 4-13 will appear. Type the current password and new password, and re-type the new password, then click the **Submit** button. The password may contain any characters (including Chinese characters), in length limited within 20 characters.

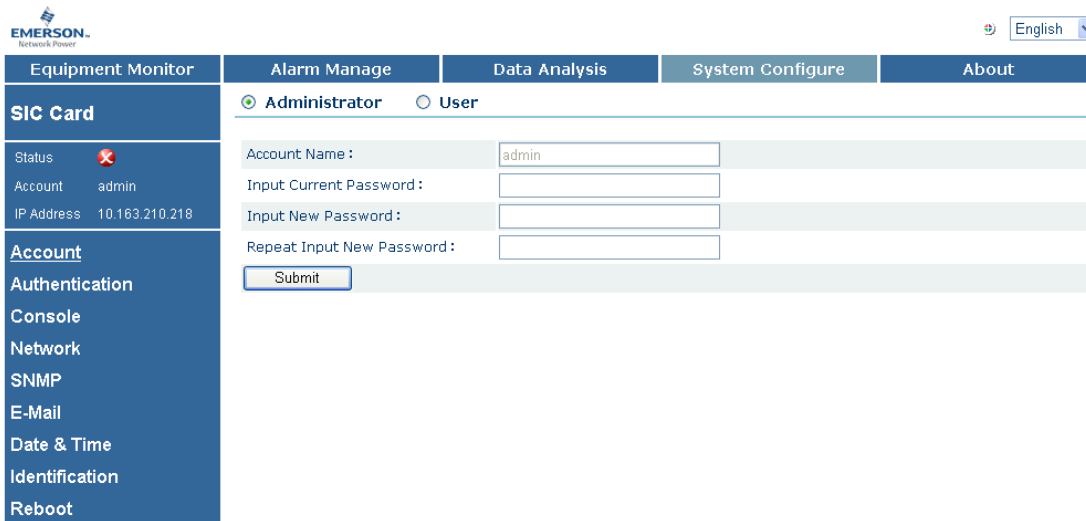


Figure 4-13 Password change page

#### 4.10.2 Configuring Authentication Mode

Select the main menu **System Configure**, click **Authentication**, the page shown in Figure 4-14 will appear. Through Figure 4-14, you can change the authentication mode of the SIC card into local authentication, RADIUS authentication or RADIUS+ local authentication. Through these authentication modes, you can control the account whether has the authority to access SIC page. In local authentication mode, you can log in the SIC card through the built-in admin and user account. In RADIUS authentication mode, you can log in the SIC card through the account admitted by RADIUS server. In RADIUS+ local authentication mode, you can log in the SIC card through all valid accounts from the two authentication modes.

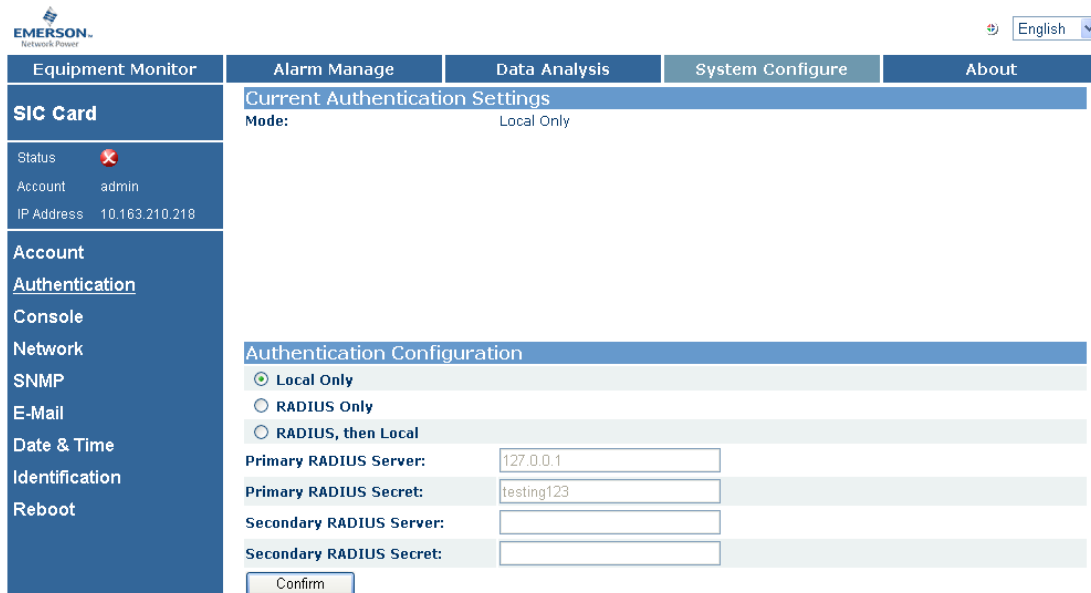


Figure 4-14 Authentication settings page

The upper part of the page displays **Current Authentication Settings**, through **Mode**, you can view the authentication mode of the current configuration; the lower part of the page displays **Authentication Configuration**, you can select 'Local Only', 'RADIUS Only', 'RADIUS, then Local' (that is RADIUS + Local).

If you select 'RADIUS Only' or 'RADIUS, then Local', you need to input the IP address and shared cipher code of the RADIUS server. To ensure the stability of the RADIUS authentication, the SIC card provides two RADIUS servers,

which are master and slave. The SIC card first get the information whether the login account is valid from the master RADIUS server. When the master RADIUS server is unavailable (network failure), or the return information shows that the login account is invalid, the SIC card will turn to get information whether the login account is valid from the slave RADIUS server. If any RADIUS server admits the login account is valid, then this account can access the SIC page, otherwise, not allowed. You can determine whether configure the slave RADIUS server according to your need. After selecting the authentication mode and inputting the required information, click the **Confirm** button to save it.

After changing the authentication mode, the SIC card does not need to restart, and the authentication mode will be valid in time, then input the corresponding account to log in according to the prompt authentication mode. As shown in Figure 4-15, the SIC card uses the authentication mode of RADIUS + Local.



Figure 4-15 Login window of authentication mode prompt



#### Note

1. When selecting 'RADIUS Only' or 'RADIUS, then Local', you need a server to realize the RADIUS protocol, and must ensure that the shared cipher code is the same as that of the RADIUS server, otherwise the RADIUS authentication will be invalid. When the shared cipher code of the master RADIUS server is incorrect, for safety reason, the SIC will not continue to get information from the slave server, considering there is a third-party attack.
2. To ensure the safety of the RADIUS authentication, you should modify the shared cipher code of the RADIUS server and SIC card regularly.

### 4.10.3 Configuring Terminal Access Mode

Select the main menu **System Configure**, click **Console**, the page shown in Figure 4-16 will appear. Through this page, you can change the debugging terminal remote login mode of the SIC card into Telnet or SSH.

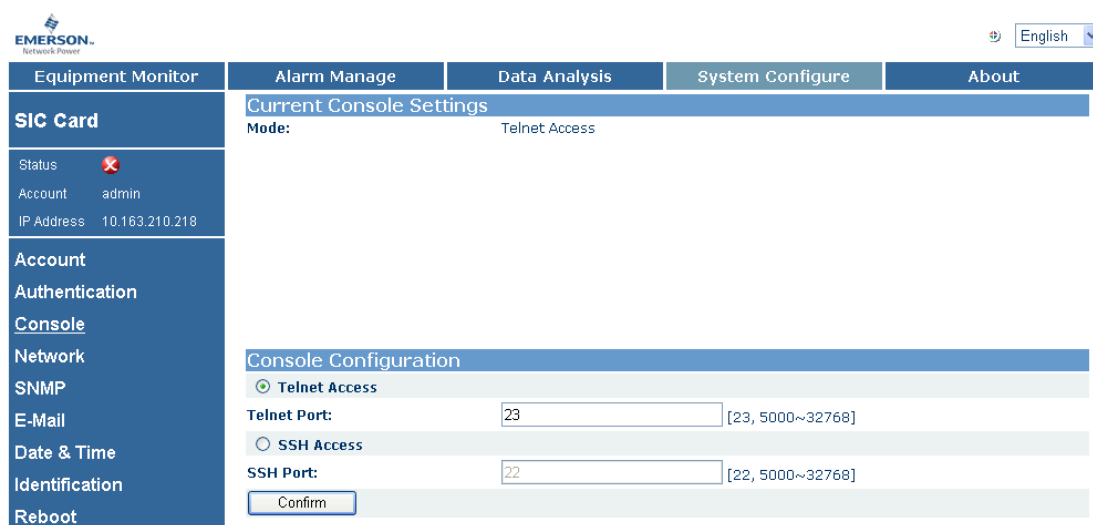


Figure 4-16 Network parameter setting page

The upper part of the page displays **Current Console Settings**, through **Mode**, you can view the terminal access mode of the current configuration; the lower part of the page displays **Console Configuration**, you can select 'Telnet Access', or 'SSH Access'.

If you need to change the terminal access mode, select 'Telnet Access' or 'SSH Access', and change the access port. Telnet access has the port number: 23 (default) or 5000 ~ 32768; SSH access has the port number: 22 (default) or 5000 ~ 32768.

After changing the terminal setting, the SIC card does not need to restart, and the terminal access mode will be valid in time, then the link built through the original access mode will automatically disconnect.

**Note**

1. SSH2 is the SSH version supported by SIC card, which only supports the authentication mode of user name + password.
2. When selecting the terminal access mode SSH, you need the client supporting SSH2, then configure the correct host IP address (IP address of SIC card) and access port in the client.
3. Only the super user (user name is admin) is allowed to log in Telnet (through Telnet) or access SIC card in SSH mode. The default password of super user is admin, case sensitive.

#### 4.10.4 Configuring SNMP Agent Parameters And Conducting Trap Test

##### Configuring SNMP Agent Parameters

Select the main menu **System Configure**, click **SNMP Configuration**, and the access control parameter configuration page will appear, as shown in Figure 4-17. In this page, you can add, configure and delete an NMS.

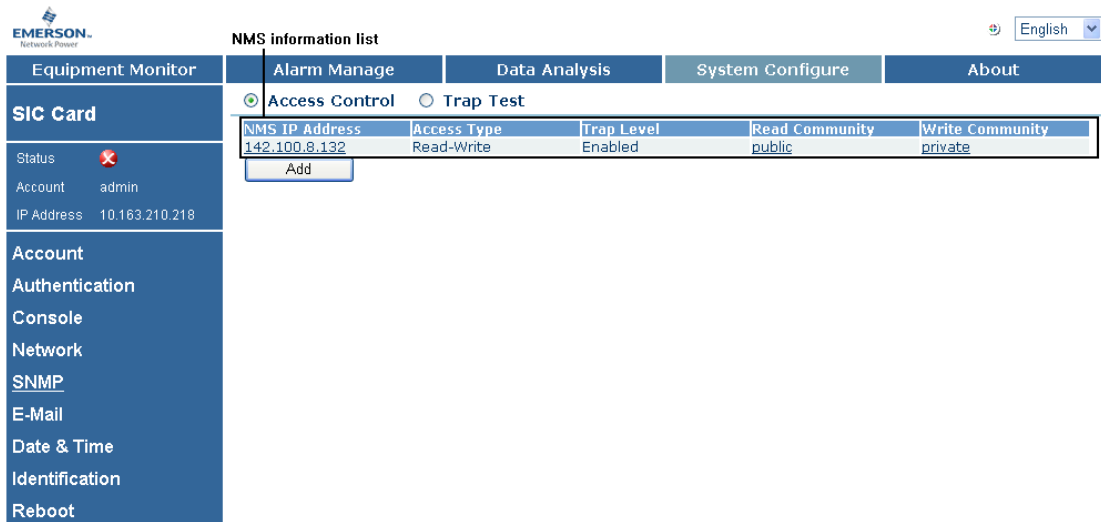


Figure 4-17 Access control parameter configuration page

## 1. Adding NMS

If you need to allow an NMS to access the SIC card, you must add this NMS to the NMS information list shown in Figure 4-17. In the page shown in Figure 4-16, click the **Add** button, and the display area will display in the lower part the **Access Control Configuration** pane, as shown in Figure 4-18.

The screenshot shows the Emerson Network Power web interface. The top navigation bar includes 'Equipment Monitor', 'Alarm Manage', 'Data Analysis', 'System Configure', and 'About'. The left sidebar contains 'SIC Card', 'Account', 'Authentication', 'Console', 'Network', 'SNMP', 'E-Mail', 'Date & Time', 'Identification', and 'Reboot'. The main content area is titled 'Access Control' and 'Trap Test'. A table lists NMS information with columns: NMS IP Address (142.100.8.132), Access Type (Read-Write), Trap Level (Enabled), Read Community (public), and Write Community (private). Below the table is the 'Access Control Configuration' form with fields for NMS IP, Access Type (Read-Write), Trap Level (Enabled), Read Community (public), and Write Community (private). Buttons for 'Confirm' and 'Delete' are at the bottom.

Figure 4-18 Adding NMS

The access control parameters include: **NMS IP**, **Access Type**, **Trap Level**, **Read Community** and **Write Community**.

### 1) NMS IP

The IP address of the NMS computer which you wish to allow to access the SIC card, for example, '71.19.8.29'.

### 2) Access Type

The authority for the NMS to access the SIC card. There are three options:

- Read-write: The NMS can read and write the SIC card
- Read-only: The NMS can only read the SIC card
- Disable: The NMS cannot access the SIC card

Generally, give read-write authority to the NMS which you want to use to control the equipment, and give read-only authority to others.

### 3) Trap Level

Whether the SIC card will send trap message (that is, alarm) to the NMS in the case of an intelligent equipment or sensor alarm.

- Enabled: The SIC card will send all alarm information to the NMS
- Disabled: The SIC card will not send any alarm information to the NMS

### 4) Read Community

Community string for getting SIC card variables, the default is 'public'.

### 5) Write Community

Community string for getting and setting SIC card variables, the default is 'private'.

## Note

The community strings are the passwords for the NMS to access the SIC card. The passwords are case sensitive.

After configuring the preceding access control parameters, click the **Confirm** button, and the NMS is added to the NMS information list.

### 2. Configuring NMS

To configure the access control parameters of an NMS, click the NMS IP address in the NMS information list in the page shown in Figure 4-17, and the page shown in Figure 4-19 will appear. After configuring the NMS access control parameters, click the **Confirm** button to save the configuration.

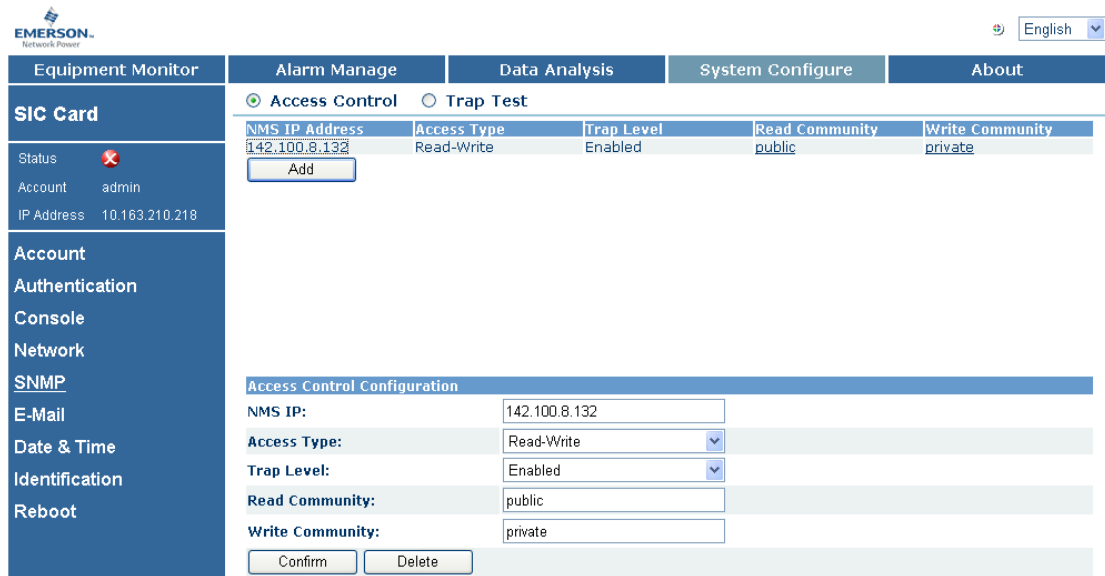


Figure 4-19 Configuring and deleting NMS

### 3. Deleting NMS

To delete an NMS, click the NMS IP address in the NMS information list in the page shown in Figure 4-17, and the page shown in Figure 4-19 will appear. Click the **Delete** button, and the NMS is deleted from the NMS information list.

**Note**

After you delete an NMS, it cannot access the SIC card.

### Conducting trap test

Select the main menu **System Configure**, click **SNMP Configuration** and select 'Trap Test', and the trap test page will appear, as shown in Figure 4-20.

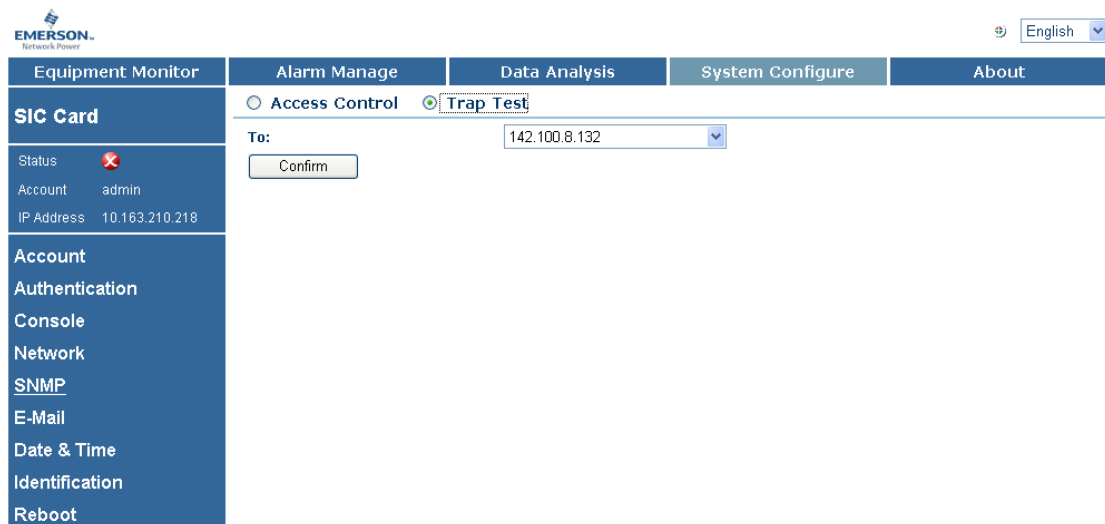


Figure 4-20 Trap test page

Select the NMS IP address from the **To:** drop-down box, and click the **Confirm** button to conduct the trap test. If the test is successful, the prompt **Success** will appear.



## 4.10.5 Configuring E-Mail Parameters And Conducting E-Mail Test

### Configuring E-Mail Server

Select the main menu **System Configure**, click **E-Mail Configuration**, and the E-Mail server configuration page will appear, as shown in Figure 4-21. In this page, you can set the SMTP server address, addresser address, E-Mail account and E-Mail password.

The screenshot shows the 'E-Mail Server' configuration page. The left sidebar contains the following menu items: Equipment Monitor, Alarm Manage, Data Analysis, System Configure, About, SIC Card, Status, Account (admin), IP Address (10.163.210.218), Account, Authentication, Console, Network, SNMP, E-Mail, Date & Time, Identification, and Reboot. The main content area has three radio buttons: E-Mail Server (selected), E-Mail Recipient, and E-Mail Test. Below these are input fields for SMTP Server, From Address, E-mail Account, and E-mail Password. There is an 'Identity Confirm' checkbox and a 'Confirm' button.

Figure 4-21 E-Mail server configuration page

The SMTP server address must be an IP address. If the SMTP server requires identity confirmation, you must set the E-Mail account and E-Mail password.

### Configuring E-Mail Recipient

Select the main menu **System Configure**, click **E-Mail Configuration** and select 'E-Mail Recipient', and the E-Mail recipient configuration page will appear, as shown in Figure 4-122. In this page, you can add, delete and modify recipient.

The screenshot shows the 'E-Mail Recipient' configuration page. The left sidebar is the same as in Figure 4-21. The main content area has three radio buttons: E-Mail Server, E-Mail Recipient (selected), and E-Mail Test. Below these is a table with the following data:

| To Address                   | E-Mail Generation | Alarm Severity |
|------------------------------|-------------------|----------------|
| fanliu@emersonnetwork.com.cn | Enabled           | Warning        |

Below the table is an 'Add' button.

Figure 4-22 E-Mail recipient configuration page

#### 1. Adding recipient

If you need to allow the SIC card to send E-Mail to a person, you must add this person to the recipient list in Figure 4-22. Click the **Add** button in the page shown in Figure 4-22, and the **Recipient Setting** pane will appear in the lower part of the display area, as shown in Figure 4-23, where you can configure the recipient parameters.

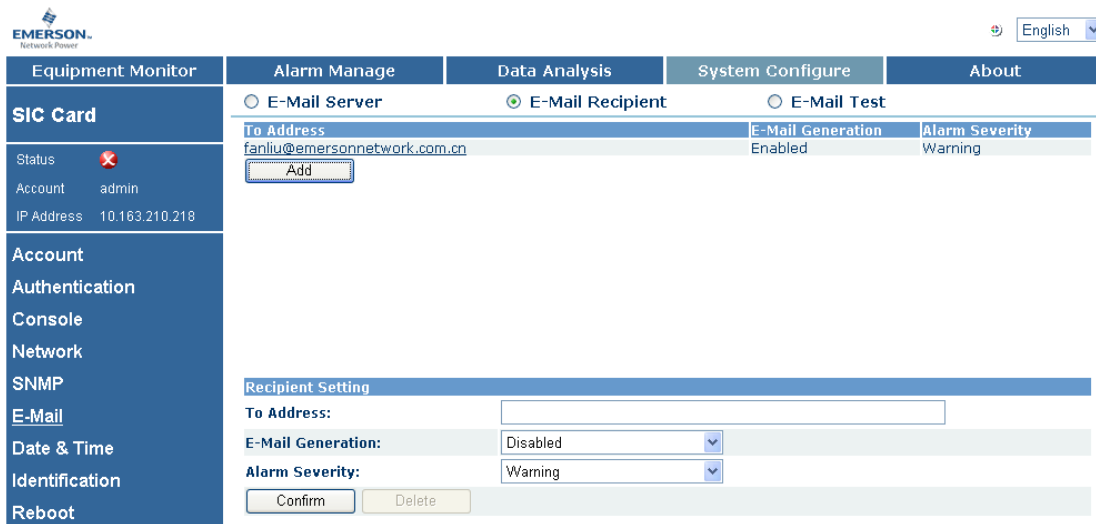


Figure 4-23 Adding recipient

The recipient parameters include **To Address**, **E-Mail Generation**, **Alarm Severity**.

**1) To Address**

The E-Mail address allowed to receive E-Mails from the SIC card. For example, 'martin.su@emersonnetwork.com.cn'.

**2) E-Mail Generation**

Whether to enable the SIC card to send E-Mail (that is, alarm) to the recipient in the case of intelligent equipment or sensor alarm.

- Enabled: The SIC card will send alarm to the recipient
- Disabled: The SIC card will not send any alarm to the recipient

**3) Alarm Severity**

The severity of the alarms that will be sent to the recipient.

- Warning: The SIC card will send warning alarms and critical alarms to the recipient
- Critical: The SIC card will send only critical alarms to the recipient

After configuring the preceding recipient parameters, click the **Confirm** button, and this recipient is added to the recipient list.

**2. Modifying recipient**

If you need to modify the parameters of a recipient, click the recipient address in the recipient list in the page shown in Figure 4-22, and the page shown in Figure 4-24 will appear. After modifying the recipient parameters, click the **Confirm** button to save the change.

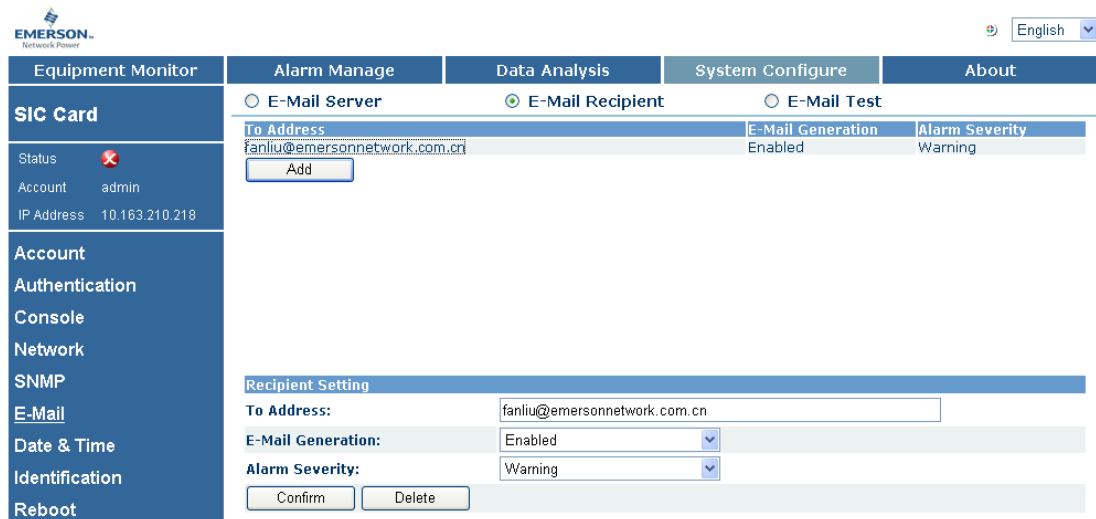


Figure 4-24 Modifying and deleting recipient

### 3. Deleting recipient

If you need to delete a recipient, click the recipient address in the recipient list in the page shown in Figure 4-22, and the page shown in Figure 4-24 will appear. Click the **Delete** button, and the recipient is deleted from the recipient list.

### Conducting E-Mail test

Select the main menu **System Configure**, click **E-Mail Configuration** and select 'E-Mail Test', and the E-Mail test page will appear, as shown in Figure 4-25.

| Equipment Monitor   | Alarm Manage | Data Analysis | System Configure | About |
|---|--------------|---------------|------------------|-------|
| <div style="text-align: right;">English</div>   |              |               |                  |       |
| <input type="radio"/> E-Mail Server <input type="radio"/> E-Mail Recipient <input checked="" type="radio"/> E-Mail Test |              |               |                  |       |
| To: fanliu@emersonnetwork.com.cn  |              |               |                  |       |
| <input type="button" value="Confirm"/>  |              |               |                  |       |
| <b>SIC Card</b>   |              |               |                  |       |
| Status <span style="color: red;">✘</span><br>Account admin<br>IP Address 10.163.210.218                                 |              |               |                  |       |
| Account<br>Authentication<br>Console<br>Network<br>SNMP<br>E-Mail<br>Date & Time<br>Identification<br>Reboot            |              |               |                  |       |

Figure 4-25 E-Mail test page

Select the recipient address from the **To:** drop-down box, and click the **Confirm** button to conduct the E-Mail test. If the test is successful, the prompt **Success** will appear.

### 4.10.6 Configuring Network Parameters

Select the main menu **System Configure**, click **Network Configuration**, and the network parameter configuration page will appear, as shown in Figure 4-26. In this page, you can change the IP address, subnet mask and default gateway of the SIC card.

| Equipment Monitor   | Alarm Manage | Data Analysis | System Configure | About |
|---|--------------|---------------|------------------|-------|
| <div style="text-align: right;">English</div>   |              |               |                  |       |
| <b>SIC Card</b>   |              |               |                  |       |
| Status <span style="color: red;">✘</span><br>Account admin<br>IP Address 10.163.210.218   |              |               |                  |       |
| Account<br>Authentication<br>Console<br>Network<br>SNMP<br>E-Mail<br>Date & Time<br>Identification<br>Reboot                                |              |               |                  |       |
| <b>Current Network Settings</b>   |              |               |                  |       |
| Mode: Static<br>IP Address: 10.163.210.218<br>Subnet Mask: 255.255.254.0<br>Default Gateway: 10.163.210.1<br>MAC Address: 00:09:f5:03:f3:3a |              |               |                  |       |
| <b>Network Configuration</b>  |              |               |                  |       |
| <input type="radio"/> Obtain an IP address automatically<br><input checked="" type="radio"/> Use the following IP address                   |              |               |                  |       |
| IP Address: 10.163.210.218<br>Subnet Mask: 255.255.254.0<br>Default Gateway: 10.163.210.1   |              |               |                  |       |
| <input type="button" value="Confirm"/>  |              |               |                  |       |

Figure 4-26 Network parameter configuration page

The display area displays in the upper part **Current Network Settings**, including **Mode**, **IP Address**, **Subnet Mask**, **Default Gateway**, **MAC Address**; in the lower part **Network Configuration**, where you can select 'Obtain an IP address automatically' or 'Use the following IP address' (that is, to set the IP address manually).

To change the network parameters, select 'Use the following IP address', and type the new network parameters, including **IP Address**, **Subnet Mask** and **Default Gateway**, and click the **Confirm** button to save the change.

After you change the network parameters, the SIC card will be rebooted automatically. Please wait one minute and use the new address to login the SIC card again.

#### Note

1. Before you select 'Use the following IP address', please confirm with you IT system administrator that DHCP server system is available in the network. Meanwhile, it is suggested that you contact your network administrator to bind the MAC address of the SIC card with the obtained IP address, so that the current IP address will be allocated to the SIC card in future IP address allocation.
2. Do not change the network parameters at will. If the IP address you configured conflicts with that of other network equipment (like computer), they cannot be accessed. So please consult your network administrator to obtain the network parameters.
3. The connection between the SIC card and SiteMonitor, Network Shutdown and NMS will be interrupted due to the change of the network parameters. Therefore, after changing the network parameters, please re-configure the relevant SiteMonitor, Network Shutdown and NMS.

### 4.10.7 Configuring System Time

Select the main menu **System Configure**, click **Time Configuration**, and the system time configuration page will appear, as shown in Figure 4-27.



Figure 4-27 System time configuration page

The display area displays in the upper part **Current Data & Time Settings**, in the lower part **Data & Time Configuration** pane, where you can set the current date, time and time zone of the SIC card, with two options of configuration mode available: 'Manual' and 'Automatic'.

#### 1. 'Manual'

select 'Apply local computer time' to obtain the date and time of the computer, or type the date and time respectively in the **Date** and **Time** boxes. In either way, the system will automatically obtain the time zone of the computer.

#### 2. 'Automatic'

That is, to choose the time server for timing. Please type the IP addresses of the primary NTP server and secondary NTP server, and select the time zone. The time servers comply with NTP or SNTP time protocol.

After configuring the preceding parameters, click the **Confirm** button.

#### Note

1. If no time server is available or the time server has not been configured, you must reconfigure the system time after you install the SIC card for the first time or the card is rebooted for reasons like changing IP address, so as to ensure that the card time is consistent with the real time.
2. If the time server is available and accessible, the SIC card time will be automatically calibrated by the time server after you install the card for the first time or the card is rebooted for reasons like changing IP address.

### 4.10.8 Configuring Identification Information

Select the main menu **System Configure**, click **Identify Configuration**, and the identification information configuration page will appear, as shown in Figure 4-28. In this page, you can configure the host name, contact information and location of the SIC card.

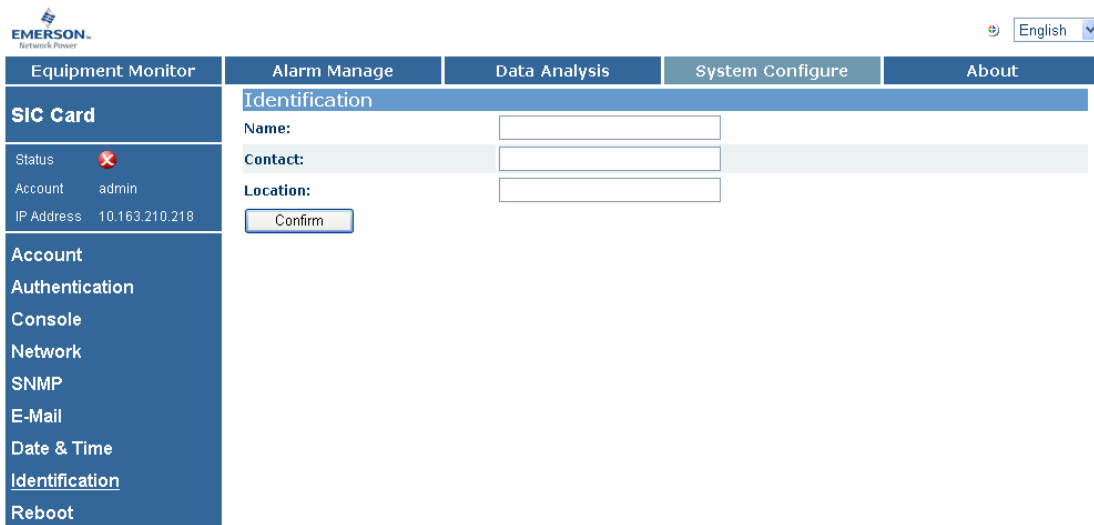


Figure 4-28 Identification information configuration page

### 4.10.9 System Reboot

Select the main menu **System Configure**, click **Reboot**, the page shown in Figure 4-29 will appear. You can click the **Confirm** button to restart the SIC card. As shown in Figure 4-30 and Figure 4-31, the pages displays the prompt 'SIC will reboot now! Please wait' and reboot progress bar, and you should wait till the reboot is finished.

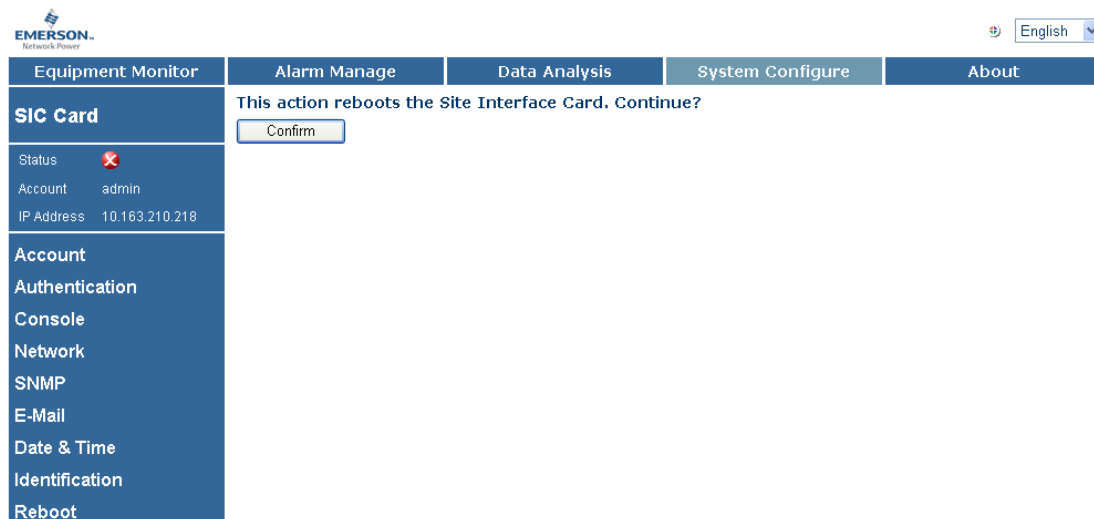


Figure 4-29 SIC reboot page



Figure 4-30 Reboot prompt page

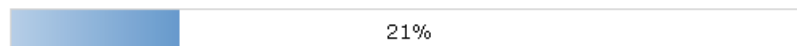
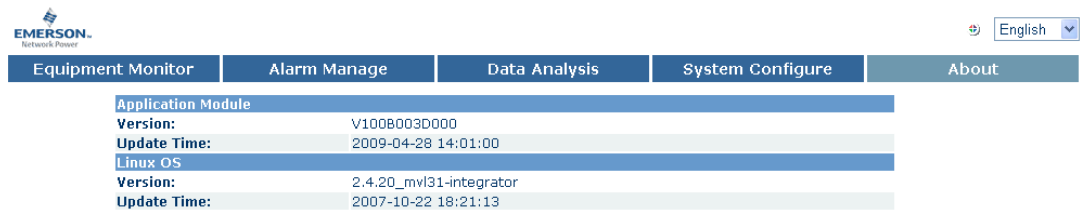


Figure 4-31 Reboot progress bar

## 4.11 Viewing SIC Card Version Information

Select the main menu **About**, and the SIC card version information page will appear, as shown in Figure 4-32. This page displays the version and update time of the application module and Linux operating system.

The screenshot shows the top navigation bar of the web interface with the "About" menu item selected. Below the navigation bar, the "Application Module" and "Linux OS" sections are displayed, each with "Version:" and "Update Time:" fields.

| Application Module |                     |
|--------------------|---------------------|
| Version:           | V100B003D000        |
| Update Time:       | 2009-04-28 14:01:00 |

| Linux OS     |                         |
|--------------|-------------------------|
| Version:     | 2.4.20_mv131-integrator |
| Update Time: | 2007-10-22 18:21:13     |

Figure 4-32 SIC card version information page

## Chapter 5 Monitoring Method 2: Through NMS

Through the SNMP agent function of the SIC card, you may use an NMS to view the parameters and alarm information of the intelligent equipment and environment in real time, configure the operating parameters and control the equipment. In case of equipment or environment alarm, the SIC card will send trap information to the NMS.

This chapter tells how to use an NMS to monitor your intelligent equipment and environment.

### 5.1 Protocol And NMS Supported By SIC Card

The SIC card currently supports SNMP v2c and SNMP v1. NMSs supporting SNMP v1 and SNMP v2c can access the SIC card, like HP OpenView, IBM NetView, Novell ManageWise, SunNet Manager.

### 5.2 Installing Equipment MIB

If you wish to use an NMS to access the SIC card to monitor the intelligent equipment and environment, you need to use the MIB import function of the NMS to load the MIB of the intelligent equipment. For the loading method, refer to the user directions of the NMS.

You may get the equipment MIB from:

- the CD delivered with the SIC card
- the local customer service center of Emerson
- our website: [www.emersonnetworkpower.com.cn](http://www.emersonnetworkpower.com.cn)

### 5.3 Applying For Management Authority

To enable the NMS to manage the intelligent equipment and environment through the SNMP agent function provided by the SIC card, first of all, you must apply to the system administrator of the SIC card for management authority, ask the system administrator to add the NMS into the NMS access control list of the SIC card. For procedures refer to the *1. Adding NMS* part in *4.10.2 Configuring Authentication Mode*

Select the main menu **System Configure**, click **Authentication**, the page shown in Figure 4-14 will appear. Through Figure 4-14, you can change the authentication mode of the SIC card into local authentication, RADIUS authentication or RADIUS+ local authentication. Through these authentication modes, you can control the account whether has the authority to access SIC page. In local authentication mode, you can log in the SIC card through the built-in admin and user account. In RADIUS authentication mode, you can log in the SIC card through the account admitted by RADIUS server. In RADIUS+ local authentication mode, you can log in the SIC card through all valid accounts from the two authentication modes.

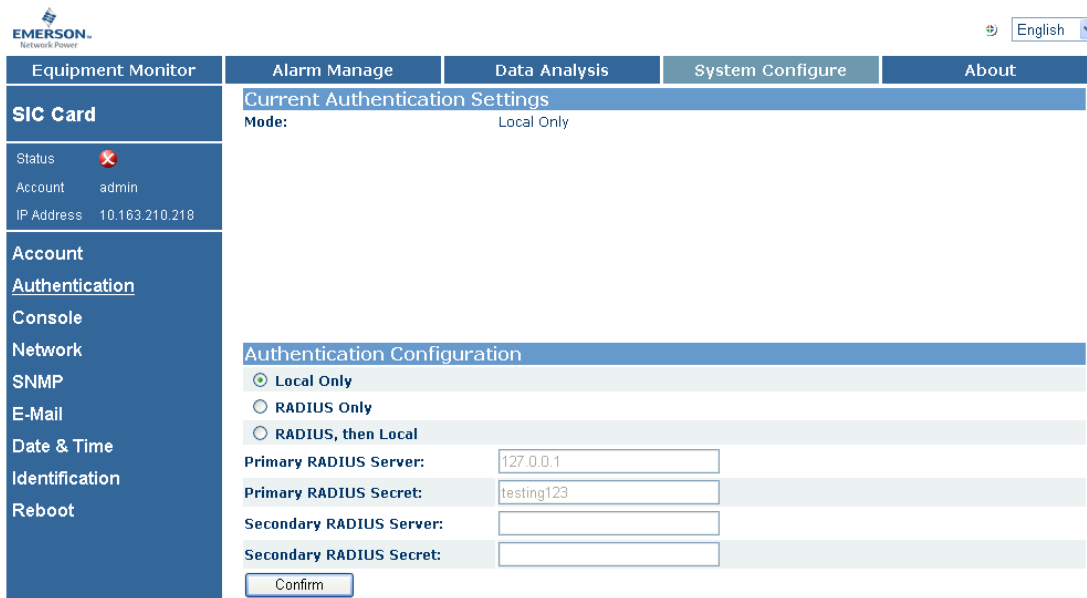


Figure 5-1 Authentication settings page

The upper part of the page displays **Current Authentication Settings**, through **Mode**, you can view the authentication mode of the current configuration; the lower part of the page displays **Authentication Configuration**, you can select 'Local Only', 'RADIUS Only', 'RADIUS, then Local' (that is RADIUS + Local).

If you select 'RADIUS Only' or 'RADIUS, then Local', you need to input the IP address and shared cipher code of the RADIUS server. To ensure the stability of the RADIUS authentication, the SIC card provides two RADIUS servers, which are master and slave. The SIC card first get the information whether the login account is valid from the master RADIUS server. When the master RADIUS server is unavailable (network failure), or the return information shows that the login account is invalid, the SIC card will turn to get information whether the login account is valid from the slave RADIUS server. If any RADIUS server admits the login account is valid, then this account can access the SIC page, otherwise, not allowed. You can determine whether configure the slave RADIUS server according to your need. After selecting the authentication mode and inputting the required information, click the **Confirm** button to save it.

After changing the authentication mode, the SIC card does not need to restart, and the authentication mode will be valid in time, then input the corresponding account to log in according to the prompt authentication mode. As shown in Figure 4-15, the SIC card uses the authentication mode of RADIUS + Local.



Figure 5-2 Login window of authentication mode prompt

**Note**

3. When selecting 'RADIUS Only' or 'RADIUS, then Local', you need a server to realize the RADIUS protocol, and must ensure that the shared cipher code is the same as that of the RADIUS server, otherwise the RADIUS authentication will be invalid. When the shared cipher code of the master RADIUS server is incorrect, for safety reason, the SIC will not continue to get information from the slave server, considering there is a third-party attack.
4. To ensure the safety of the RADIUS authentication, you should modify the shared cipher code of the RADIUS server and SIC card regularly.



### 5.3.2 Configuring Terminal Access Mode

Select the main menu **System Configure**, click **Console**, the page shown in Figure 4-16 will appear. Through this page, you can change the debugging terminal remote login mode of the SIC card into Telnet or SSH.

The screenshot shows the 'Current Console Settings' page. At the top, there is a navigation bar with 'Equipment Monitor', 'Alarm Manage', 'Data Analysis', 'System Configure', and 'About'. Below this is a 'SIC Card' section with a status indicator (red X) and details: Account: admin, IP Address: 10.163.210.218. A sidebar menu on the left includes 'Account', 'Authentication', 'Console', 'Network', 'SNMP', 'E-Mail', 'Date & Time', 'Identification', and 'Reboot'. The main content area is titled 'Current Console Settings' and shows 'Mode: Telnet Access'. Below this is the 'Console Configuration' section, which has two radio buttons: 'Telnet Access' (selected) and 'SSH Access'. Under 'Telnet Access', there is a 'Telnet Port' field with the value '23' and a range '[23, 5000~32768]'. Under 'SSH Access', there is an 'SSH Port' field with the value '22' and a range '[22, 5000~32768]'. A 'Confirm' button is located at the bottom of the configuration section.

Figure 5-3 Network parameter setting page

The upper part of the page displays **Current Console Settings**, through **Mode**, you can view the terminal access mode of the current configuration; the lower part of the page displays **Console Configuration**, you can select 'Telnet Access', or 'SSH Access'.

If you need to change the terminal access mode, select 'Telnet Access' or 'SSH Access', and change the access port. Telnet access has the port number: 23 (default) or 5000 ~ 32768; SSH access has the port number: 22 (default) or 5000 ~ 32768.

After changing the terminal setting, the SIC card does not need to restart, and the terminal access mode will be valid in time, then the link built through the original access mode will automatically disconnect.

#### Note

4. SSH2 is the SSH version supported by SIC card, which only supports the authentication mode of user name + password.
5. When selecting the terminal access mode SSH, you need the client supporting SSH2, then configure the correct host IP address (IP address of SIC card) and access port in the client.
6. Only the super user (user name is admin) is allowed to log in Telnet (through Telnet) or access SIC card in SSH mode. The default password of super user is admin, case sensitive.

#### Configuring SNMP Agent Parameters And Conducting Trap Test.

For the details on how to use the NMS to monitor your intelligent equipment and environment, refer to the NMS user directions. In operation, please note the following points:

1. The community string used in getting UPS data must be the same as the read community string set in the SIC card.
2. The community string used in configuring parameters and controlling equipment must be the same as the write community string set in the SIC card.
3. If you are granted the read-only authority, you will not be able to use the NMS to perform control or configuration operations, but can only view the operating parameters and alarm data, PS state and input/output signals.
4. If you want to modify a table, you must configure all the writable properties of it and submit them to the SIC card. Only in this way can your modifications be accepted.
5. In the case of control failure due to lack of authorization or community string error, the NMS will receive an AUTH\_FAILURE trap.

## Chapter 6 Monitoring Method 3: Through SiteMonitor

SiteMonitor is an SIC card centralized management software developed by Emerson Network Power Co., Ltd.. Through TCP/IP protocol, you can use SiteMonitor to obtain the real-time data and alarm data of the intelligent equipment and environment from the SIC card, control the equipment and configure operating parameters. SiteMonitor can manage up to ten thousand pieces of intelligent equipment.

To use SiteMonitor to manage intelligent equipment and environment through the SIC card, you need to open the IE browser on the computer installed with SiteMonitor, and configure the IP address of the SIC card into SiteMonitor.

For details on how to use SiteMonitor to monitor the intelligent equipment and environment, refer to *SiteMonitor UPS Monitoring Software User Manual*.

---

## Chapter 7 Guarding Computer With Network Shutdown

The computer safe shutdown program Network Shutdown is developed by Emerson Network Power Co., Ltd.. In case of UPS alarm, the SIC card will send alarm information to the preset computer installed with Network Shutdown. Network Shutdown receives and processes the alarm information and take the following protective measures to protect the computer according to the user configurations:

- Notify the administrator
- Execute the command file
- Save the application files automatically and shutdown the computer

For the installation and operation of Network Shutdown, refer to *Network Shutdown Software (UNIX & Netware Version) User Manual* and *Network Shutdown Software (Windows Version) User Manual*.

## Chapter 8 Q's & A's

This chapter introduces the Q's & A's in the daily use of the SIC card. In case you encounter any problems, you are recommended to seek solution in this chapter before seeking technical assistance from the local customer service center of Emerson.

### 8.1 Q's & A's In Installation

**Question 1: The indicators remain off after installation.**

Answer: The UPS is shut down or has not been connected to the utility. Turn on the UPS. If the UPS cannot be turned on, check the connection of UPS with the utility and connect the network cable, then observe if the indicators turn on.

**Question 2: When using the USB interface of the SIC card for the first time, how to use TTY to make connection?**

Answer: Before inserting the SIC, you must start the TTY and use the accessory USB cable to connect the intelligent equipment with the computer. Because it takes only about five seconds to start the card, you cannot see the start process if you do not run TTY before inserting the card. If you do have started TTY before inserting the card but cannot see the process, refer to the answer to Question 2 in 8.2 Q's & A's *In Running*.

Besides, please install the USB driver in the CD delivered with the SIC card, and find the serial port of **CP2101 USB to UART** on the menu **COM & PT** in **Device Manager**, and remember it. You need to use this serial port to make connection.

**Question 3. Can I finish the installation without computer at hand to run Hyper Terminal?**

Answer: No, if you don't know the IP address. If you know the IP address, or if it is a new card (default address: 192.168.1.1), you may use the following steps to configure your card through Telnet mode.

1. Connect the card to the network.
2. Modify the network parameters of a computer located in the same LAN (better in the same HUB or switch) with the card to get them in the same network section. Suppose the card IP address is: 192.168.1.1, subnet mask: 255.255.255.0, gateway: 0.0.0.0, then the computer IP address can be: 192.168.1.2, subnet mask: 255.255.255.0, gateway: 0.0.0.0.
3. Reboot the computer, connect to the card in Telnet mode, login with user name admin and admin's password. For a new SIC card, the default password is admin.
4. After login, set the card's IP address and other network parameters. The card will be rebooted automatically, and later on you may access the card using the new IP address.
5. Restore the network parameters of the computer.

### 8.2 Q's & A's In Running

**Question 1: Why the yellow indicator of the SIC card does not illuminate?**

Answer: The card is not connected to the network. Please connect it to the network. After building up network connection, when the card is receiving data from the network, the yellow indicator will blink; when it is not receiving data, the yellow indicator will keep illuminating.

**Question 2: The SIC card is running, but when I start TTY and intend to configure the SIC parameters, why no login information appears on the screen?**

Answer: Press the Enter key, and the login information should appear. If not, please verify that the card is running (green indicator is on) and check that:

1. the intelligent equipment is connected to the computer with USB cable.

2. the USB driver has been properly installed, and the serial port **CP2101 USB to UART** is on the menu **COM&PT** in **Device Manager**.
3. the serial port set in TTY is the same as the one connected to the intelligent equipment.
4. the serial port set in TTY is correct. Refer to the part *Using TTY to login SIC card* in 3.1.1 *Using TTY Or Telnet To Login SIC Card*.
5. TTY and serial port can communicate well.

**Question 3: What shall I do if I lose my password?**

Answer: Use the USB communication cable (accessory) to connect the computer USB interface and the SIC card USB interface, then use the reset function to resume default password setting. See 3.3 *Using Reset User To Configure Basic SIC Card Parameters Through TTY*.

**Question 4: Why can some computers visit the card while some others cannot, but these computers can visit one another?**

Answer: Incorrect SIC card gateway setting. If the card default gateway is 0.0.0.0, the card can be accessed only by the computers in the same network segment. Please reset the card gateway according to gateway of the computer. Even though the gateway is set correctly, if firewall is installed in your network, you will also meet with this problem. If so, contact your network administrator.

## 8.3 Q's & A's In Web Monitoring

**Question 1: When I type in Web browser the IP address of the computer connected to the equipment installed with the SIC card, the prompt cannot find server appears, why?**

Answer: Suppose the IP address is correct, maybe:

1. The SIC card is not running.

If this is because the intelligent equipment is off, please turn on the equipment and try again.

2. Network connection has not been built.

Use the ping command to check whether your computer can connect to the card. Refer to your OS manual for the usage of the ping command. If you cannot ping successfully, check whether the card IP address is wrong.

**Question 2: Why does the system prompt connection timeout while the browser is visiting the SIC card?**

Answer: Too many network users (including Web users and NMSs). The card can respond only 10 Web users and 5 inquiring NMS concurrently. Please close or stop some Web browsers or NMSs and try again.

**Question 3: Why are the intelligent equipment status and SIC card configuration displayed on Web browser inconsistent with the actual situation.**

Answer: It might be caused by:

1. incorrect computer time.
2. incorrect card time.
3. incorrect cache setting of the Web browser.
4. web page time error.

Please set the card time, computer time and browser cache correctly, and delete all temporary web pages on your computer.

**Question 4: The browser sometimes prompts web page error and cannot continue while sometimes not, why?**

Answer: This problem usually occurs when you have just started to browse the SIC card and the browser is downloading the monitoring homepage from the SIC card, while at this point, you click other link on the homepage, and the download process is thus interrupted. Please wait till correct status data appear on the homepage before you carry out other operations.

**Question 5: I have typed correct user name and password and there is no error message, but the homepage does not come next, why?**

Answer: Because the SIC card homepage is programmed by JavaScript, this problem may be caused by the following two reasons:

1. You have installed anti-virus firewall, the software cannot identify normal web pages or web pages that contain virus, so the homepage cannot be displayed. Please configure or close the firewall software.
2. JavaScript is disabled in your Web browser. To visit the SIC card web page, you must enable JavaScript. Refer to the part *Enabling JavaScript* in 4.1 *Checking Web Browser Settings*.

## 8.4 Q's & A's In NMS Monitoring

**Question 1: Why timeout error often occurs when NMS is visiting the SIC card?**

Answer: This may be caused by the following three reasons:

1. The NMS is not in the **Access Control** list of the SIC card. Ask the system administrator to add it in the **Access Control** list. Refer to the *Configuring SNMP Agent Parameters* part in 4.10.2 *Configuring Authentication Mode*. Select the main menu **System Configure**, click **Authentication**, the page shown in Figure 4-14 will appear. Through Figure 4-14, you can change the authentication mode of the SIC card into local authentication, RADIUS authentication or RADIUS+ local authentication. Through these authentication modes, you can control the account whether has the authority to access SIC page. In local authentication mode, you can log in the SIC card through the built-in admin and user account. In RADIUS authentication mode, you can log in the SIC card through the account admitted by RADIUS server. In RADIUS+ local authentication mode, you can log in the SIC card through all valid accounts from the two authentication modes.

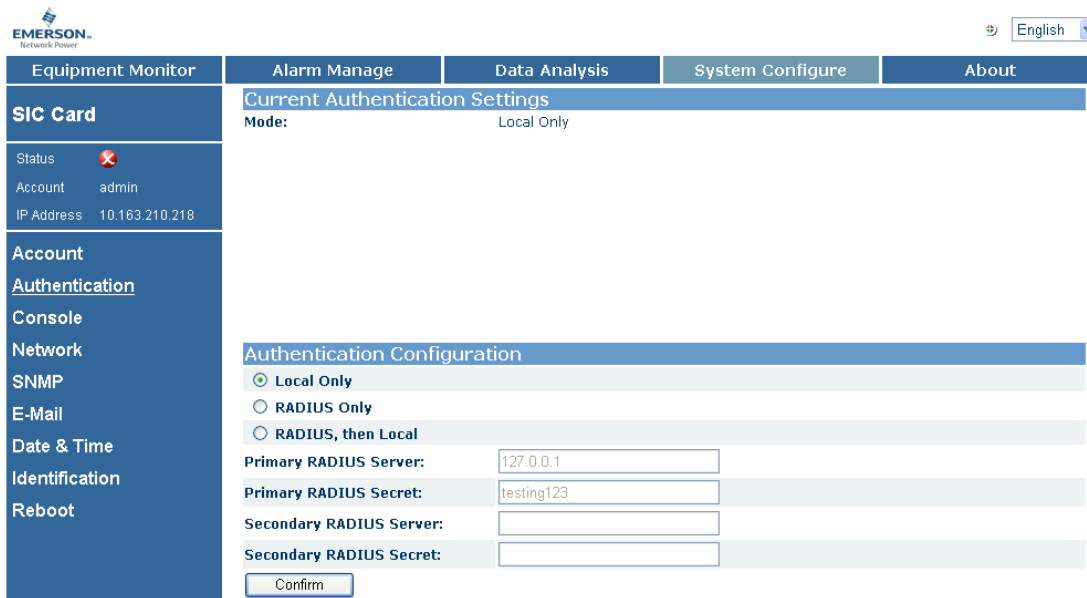


Figure 8-1 Authentication settings page

The upper part of the page displays **Current Authentication Settings**, through **Mode**, you can view the authentication mode of the current configuration; the lower part of the page displays **Authentication Configuration**, you can select 'Local Only', 'RADIUS Only', 'RADIUS, then Local' (that is RADIUS + Local).

If you select 'RADIUS Only' or 'RADIUS, then Local', you need to input the IP address and shared cipher code of the RADIUS server. To ensure the stability of the RADIUS authentication, the SIC card provides two RADIUS servers, which are master and slave. The SIC card first get the information whether the login account is valid from the master RADIUS server. When the master RADIUS server is unavailable (network failure), or the return information shows that the login account is invalid, the SIC card will turn to get information whether the login account is valid from the slave RADIUS server. If any RADIUS server admits the login account is valid, then this account can access the SIC page, otherwise, not allowed. You can determine whether configure the slave RADIUS server according to your need. After selecting the authentication mode and inputting the required information, click the **Confirm** button to save it.

After changing the authentication mode, the SIC card does not need to restart, and the authentication mode will be valid in time, then input the corresponding account to log in according to the prompt authentication mode. As shown in Figure 4-15, the SIC card uses the authentication mode of RADIUS + Local.



Figure 8-2 Login window of authentication mode prompt

#### Note

- When selecting 'RADIUS Only' or 'RADIUS, then Local', you need a server to realize the RADIUS protocol, and must ensure that the shared cipher code is the same as that of the RADIUS server, otherwise the RADIUS authentication will be invalid. When the shared cipher code of the master RADIUS server is incorrect, for safety reason, the SIC will not continue to get information from the slave server, considering there is a third-party attack.
- To ensure the safety of the RADIUS authentication, you should modify the shared cipher code of the RADIUS server and SIC card regularly.

## 8.4.2 Configuring Terminal Access Mode

Select the main menu **System Configure**, click **Console**, the page shown in Figure 4-16 will appear. Through this page, you can change the debugging terminal remote login mode of the SIC card into Telnet or SSH.

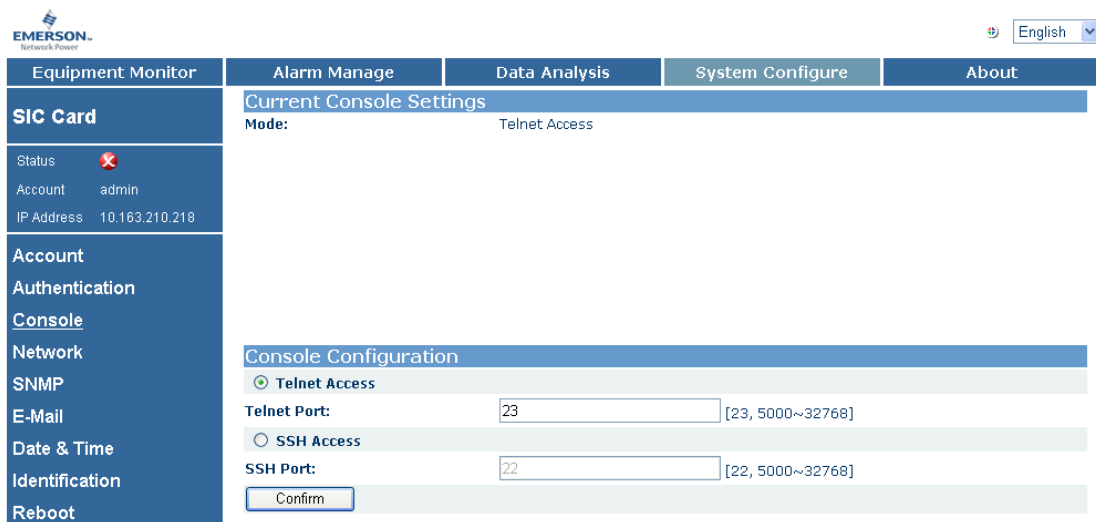


Figure 8-3 Network parameter setting page

The upper part of the page displays **Current Console Settings**, through **Mode**, you can view the terminal access mode of the current configuration; the lower part of the page displays **Console Configuration**, you can select 'Telnet Access', or 'SSH Access'.

If you need to change the terminal access mode, select 'Telnet Access' or 'SSH Access', and change the access port. Telnet access has the port number: 23 (default) or 5000 ~ 32768; SSH access has the port number: 22 (default) or 5000 ~ 32768.

After changing the terminal setting, the SIC card does not need to restart, and the terminal access mode will be valid in time, then the link built through the original access mode will automatically disconnect.

**Note**

7. SSH2 is the SSH version supported by SIC card, which only supports the authentication mode of user name + password.
8. When selecting the terminal access mode SSH, you need the client supporting SSH2, then configure the correct host IP address (IP address of SIC card) and access port in the client.
9. Only the super user (user name is admin) is allowed to log in Telnet (through Telnet) or access SIC card in SSH mode. The default password of super user is admin, case sensitive.

Configuring SNMP Agent Parameters And Conducting Trap Test.

2. Community string error. In this case, the NMS will receive an **AUTH-FAILURE** trap. The community string used in sending request must be the same as that set in the access control parameters of the SIC card. Refer to the *Configuring SNMP Agent Parameters* part in 4.10.2 *Configuring Authentication Mode*

Select the main menu **System Configure**, click **Authentication**, the page shown in Figure 4-14 will appear. Through Figure 4-14, you can change the authentication mode of the SIC card into local authentication, RADIUS authentication or RADIUS+ local authentication. Through these authentication modes, you can control the account whether has the authority to access SIC page. In local authentication mode, you can log in the SIC card through the built-in admin and user account. In RADIUS authentication mode, you can log in the SIC card through the account admitted by RADIUS server. In RADIUS+ local authentication mode, you can log in the SIC card through all valid accounts from the two authentication modes.

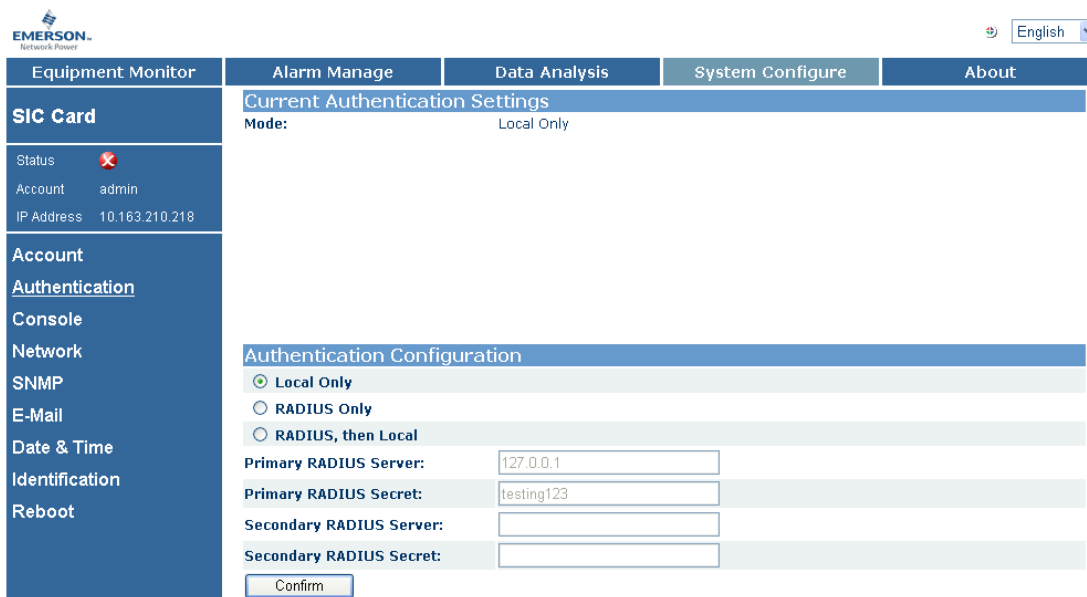


Figure 8-4 Authentication settings page

The upper part of the page displays **Current Authentication Settings**, through **Mode**, you can view the authentication mode of the current configuration; the lower part of the page displays **Authentication Configuration**, you can select 'Local Only', 'RADIUS Only', 'RADIUS, then Local' (that is RADIUS + Local).

If you select 'RADIUS Only' or 'RADIUS, then Local', you need to input the IP address and shared cipher code of the RADIUS server. To ensure the stability of the RADIUS authentication, the SIC card provides two RADIUS servers, which are master and slave. The SIC card first get the information whether the login account is valid from the master RADIUS server. When the master RADIUS server is unavailable (network failure), or the return information shows that the login account is invalid, the SIC card will turn to get information whether the login account is valid from the slave RADIUS server. If any RADIUS server admits the login account is valid, then this account can access the SIC page, otherwise, not allowed. You can determine whether configure the slave RADIUS server according to your need. After selecting the authentication mode and inputting the required information, click the **Confirm** button to save it.

After changing the authentication mode, the SIC card does not need to restart, and the authentication mode will be valid in time, then input the corresponding account to log in according to the prompt authentication mode. As shown in Figure 4-15, the SIC card uses the authentication mode of RADIUS + Local.





Figure 8-5 Login window of authentication mode prompt

#### Note

7. When selecting 'RADIUS Only' or 'RADIUS, then Local', you need a server to realize the RADIUS protocol, and must ensure that the shared cipher code is the same as that of the RADIUS server, otherwise the RADIUS authentication will be invalid. When the shared cipher code of the master RADIUS server is incorrect, for safety reason, the SIC will not continue to get information from the slave server, considering there is a third-party attack.
8. To ensure the safety of the RADIUS authentication, you should modify the shared cipher code of the RADIUS server and SIC card regularly.

### 8.4.3 Configuring Terminal Access Mode

Select the main menu **System Configure**, click **Console**, the page shown in Figure 4-16 will appear. Through this page, you can change the debugging terminal remote login mode of the SIC card into Telnet or SSH.

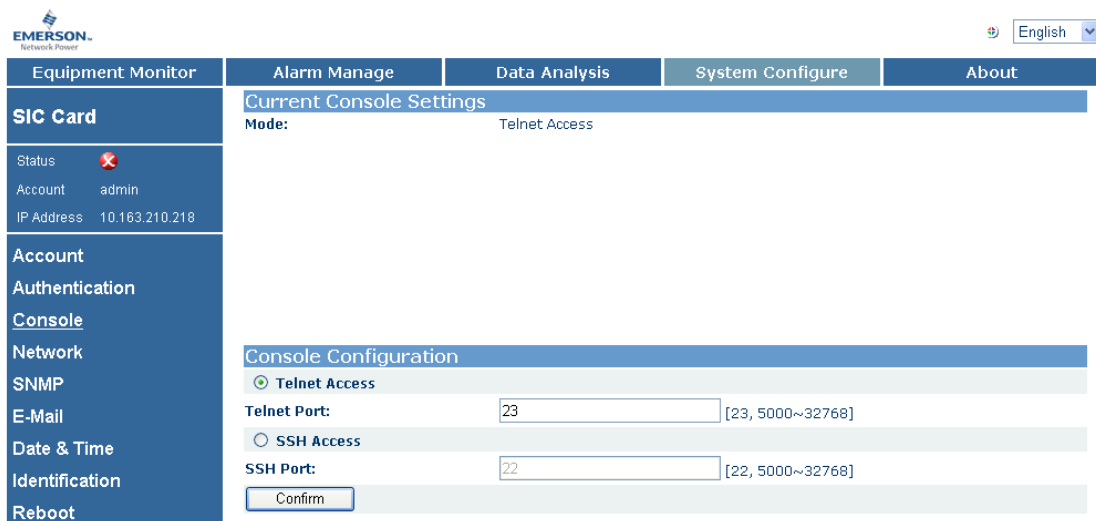


Figure 8-6 Network parameter setting page

The upper part of the page displays **Current Console Settings**, through **Mode**, you can view the terminal access mode of the current configuration; the lower part of the page displays **Console Configuration**, you can select 'Telnet Access', or 'SSH Access'.

If you need to change the terminal access mode, select 'Telnet Access' or 'SSH Access', and change the access port. Telnet access has the port number: 23 (default) or 5000 ~ 32768; SSH access has the port number: 22 (default) or 5000 ~ 32768.

After changing the terminal setting, the SIC card does not need to restart, and the terminal access mode will be valid in time, then the link built through the original access mode will automatically disconnect.

#### Note

10. SSH2 is the SSH version supported by SIC card, which only supports the authentication mode of user name + password.
11. When selecting the terminal access mode SSH, you need the client supporting SSH2, then configure the correct host IP address (IP address of SIC card) and access port in the client.

12. Only the super user (user name is admin) is allowed to log in Telnet (through Telnet) or access SIC card in SSH mode. The default password of super user is admin, case sensitive.
- 

Configuring SNMP Agent Parameters And Conducting Trap Test.

3. Network error. Check the network connection.

**Question 2: When NMS attempts to configure SIC card parameters, genErr is replied, why?**

Answer: **genErr** occurs when:

1. The NMS is lack of control authority.
2. The SIC card fails in sending the configuration request of the NMS to the intelligent equipment. Please check whether the parameters sent by the NMS are correct, and whether a communication failure trap is received.

**Question 3: I just cannot use an NMS to add another one in Access Control list of the SIC card, why?**

Answer: Only the system administrator can add, delete, or modify NMS. Besides, you must submit all writable properties of the NMS when you do this.

## 8.5 Q's & A's In SiteMonitor Monitoring

**Question: How can SiteMonitor manage intelligent equipment through the SIC card?**

Answer: Use the configuration function of SiteMonitor to add the SIC card IP address to the configuration file of SiteMonitor, and start SiteMonitor, then you can use it to manage intelligent equipment.

## 8.6 Q's & A's In Using Network Shutdown

**Question: How can Network Shutdown get information from the SIC card in the case of UPS alarm?**

Answer: Run Network Shutdown and enter the SIC card IP address to build up connection between the card and the computer.

### **Emerson Network Power, a business of Emerson**

(NYSE:EMR), a global company that leads by applying a unique combination of industry expertise, technology, and resources to make the future of our customers' enterprises and networks possible.

Emerson Network Power provides innovative solutions and expertise in areas including AC and DC power and precision cooling systems, embedded computing and power, integrated racks and enclosures, power switching and controls, infrastructure management and connectivity. All solutions are supported globally by local Emerson Network Power service technicians.

While every precaution has been taken to ensure the accuracy and completeness of this literature, Emerson Network Power assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions.

All rights reserved throughout the world.

Specifications subject to change without notice.

All names referred to are trademarks or registered trademarks of their respective owners