



Liebert» D6GZ7J

User Manual

RDU-EX

用户手册

资料版本 V1.0
归档时间 2016-03-07
BOM 编码 31013487

RDU-EX

User Manual

Version V1.0
Revision date May 27, 2015
BOM 31013487

艾默生网络能源有限公司为客户提供全方位的技术支持，用户可与就近的艾默生网络能源有限公司办事处或客户服务中心联系，也可直接与公司总部联系。

艾默生网络能源有限公司
版权所有，保留一切权利。内容如有改动，恕不另行通知。

艾默生网络能源有限公司
地址：深圳市南山区学苑大道 1001 号南山智园 B2 栋
邮编：518055
公司网址：
www.emersonnetworkpower.com.cn
客户服务热线：4008876510
E-mail: enpc.service@emerson.com

Emerson Network Power provides customers with technical support. Users may contact the nearest Emerson local sales office or service center.

Copyright © 2015 by Emerson Network Power Co., Ltd.
All rights reserved. The contents in this document are subject to change without notice.

Emerson Network Power Co., Ltd.
Address: Block B2, Nanshan I Park, No.1001 Xueyuan Road, Nanshan District, Shenzhen, 518055, P. R. China
Homepage: www.emersonnetworkpower.com
E-mail: overseas.support@emerson.com

目 录

第一章 产品简介	1
1.1 部件说明.....	1
1.1.1 RDU-EX.....	1
1.1.2 封堵挡板（选配）	3
1.2 主要功能.....	3
1.3 技术指标.....	4
1.3.1 环境指标	4
1.3.2 机械指标	4
1.3.3 性能指标	4
1.3.4 产品认证	5
第二章 硬件安装	6
2.1 安装准备.....	6
2.1.1 注意事项	6
2.1.2 环境要求	6
2.2 安装 RDU-EX	6
2.2.1 挂式安装	6
2.2.2 机架安装	7
2.2.3 磁吸安装	7
2.3 电气连接.....	8
第三章 RDU-EX 的 Web 界面	9
3.1 登录准备.....	9
3.1.1 检查 IP 地址连通性	9
3.1.2 检查浏览器版本.....	9
3.1.3 检查浏览器设置.....	9
3.2 登录 RDU-EX	13
3.2.1 登录页面	13
3.2.2 忘记密码	13
3.3 RDU-EX 主页	13
3.3.1 校时链接	14
3.3.2 解除超时	14
3.3.3 注销登录	14
3.3.4 实时告警提醒设置.....	15
3.4 菜单项	15
3.4.1 设备信息	15
3.4.2 安全关机	17
3.4.3 告警管理	19
3.4.4 数据管理	22

3.4.5 配置管理	24
3.4.6 系统设置	28
3.4.7 帮助信息	38
第四章 维护	39
4.1 恢复默认设置	39
4.2 常见故障处理	39
附录一 缩略词	41
附录二 标准配置清单	42
附录三 有毒有害物质或元素标识表	43

第一章 产品简介

RDU-EX 是一种网络管理设备，它可以对智能设备如不间断电源系统（UPS）、配电单元（PDU）、精密空调等智能设备进行集中监控，还可以接入环境监测设备，包括 IRM 系列温湿度传感器或干接点信号输入检测传感器。当智能设备发生告警时，可通过记录日志、发送 Trap 消息、发送电子邮件、发送短消息等多种方式通知用户。

RDU-EX 可满足 TCP/IP、RS232/485 组网方式的要求，能根据各种应用场合的具体要求进行灵活配置。

本章主要介绍 RDU-EX 部件说明、主要功能和技术指标。

1.1 部件说明

RDU-EX 包含 RDU-EX 主机以及选配件封堵挡板。

1.1.1 RDU-EX

RDU-EX 外观和接口如图 1-1 所示。

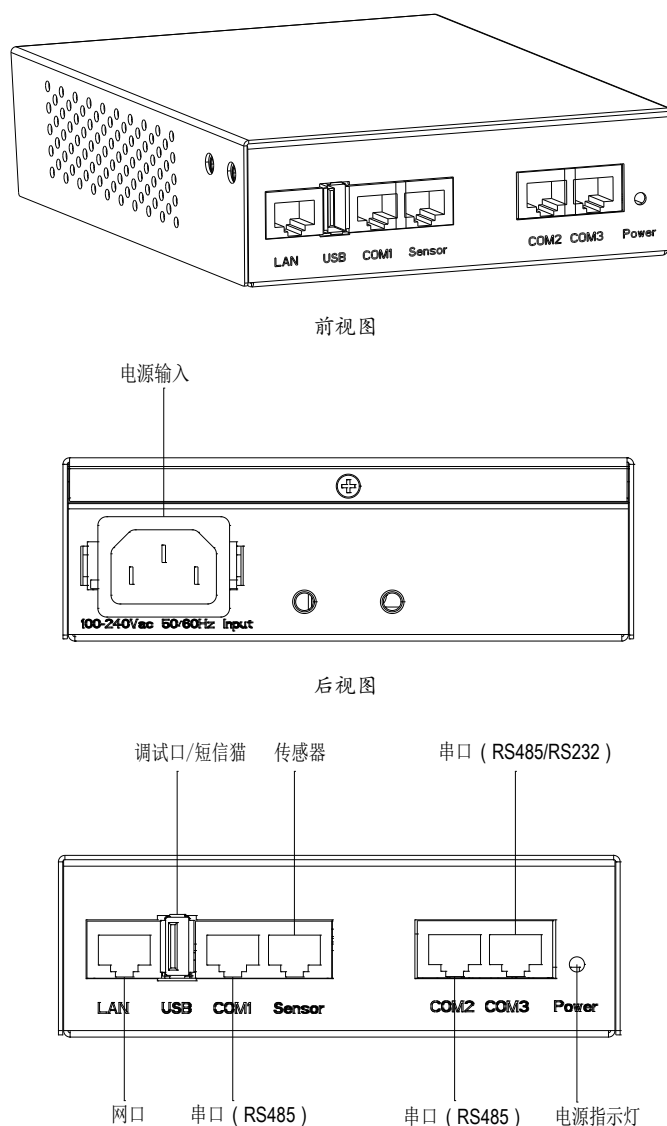


图1-1 RDU-EX 外观和接口图

网口

RDU-EX 提供 1 路网络接口，采用 10/100M Base-T 自适应的以太网口，位置如图 1-1 所示，网口默认配置见表 1-1。

表1-1 网口默认配置参数

参数 网卡号	IP 地址	子网掩码	默认网关
默认参数	192.168.0.252	255.255.255.0	192.168.0.1

USB 接口（出厂默认）

RDU-EX 提供 1 路 USB-A 型插座接口，可接入指定型号的 USB 短信 Modem。

串口

RDU-EX 提供 4 个独立串口（其中 1 路支持智能传感器），位置如图 1-1 所示，接口线序定义见表 1-2。

表1-2 接口线序定义

-	COM1	Sensor	COM2	COM3
Port type	RS485	RS485	RS485	RS232/RS485
1	NC	12V	NC	NC
2				
3	NC	NC	NC	TXD
4	GND	GND	GND	GND
5				
6	NC	NC	NC	RXD
7	D+	D+	D+	D+
8	D-	D-	D-	D-

注：
 1. RJ45 端口的线序排列为缺口向下，从左到右依次为 1~8；
 2. 检查用于连接的网线为直连网线；
 3. D+、D- 为 RS485 差分信号的两种电平；
 4. NC: Not Connected

通信参数见表 1-3。

表1-3 串口通信参数

参数	波特率	数据位	奇偶校验位	停止位
数值	1200bps, 2400bps, 4800bps, 9600bps, 19200bps (可选)	5 至 8 位	Even/Odd/None/Mark/Space	1~2 位

注：不支持字长 5 位、停止位 2 位的组合方式

传感器接口

RDU-EX 提供 1 路传感器接口，位置如图 1-1 所示，其参数见表 1-4。

表1-4 传感器接口电气参数

丝印	定义	额定输出电压	输出电流（总）	最大输出功率（总）	端口保护
Sensor	传感器接口	+12Vdc	≤0.25A	3W	支持短路保护

该接口采用 RS-485 通信方式，用于接入 Emerson 智能温湿度传感器、智能温度传感器、智能数字量扩展传感器或支持 RS-485 通信的智能设备，通信参数见表 1-5。

注意

Sensor 口接入传感器时，不可接入智能设备。
接入智能设备时信号线只接 D+、D-。

表1-5 Sensor口通信参数

接入设备	波特率	数据位	奇偶校验位	停止位
智能传感器	9600bps	8 位	无	1 位
智能设备	1200bps, 2400bps, 4800bps, 9600bps, 19200bps (可选)	5 至 8 位	Even/Odd/None/Mark/Space	1~2 位
注：不支持字长 5 位、停止位 2 位的组合方式				

1.1.2 封堵挡板（选配）

封堵挡板可对机架空余部分进行遮挡（挡板左右两侧皆可安装），外观及安装示意图如图 1-2 所示：

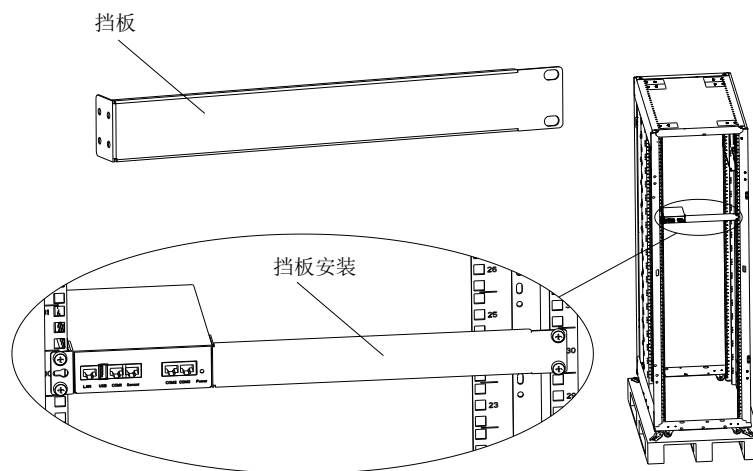


图1-2 外观及安装示意图

1.2 主要功能

RDU-EX 的主要功能见表 1-6。

表1-6 RDU-EX 主要功能

主要功能	说明	
设备监控	实现对机房环境的监视和对不同智能设备的数据采集和处理，并且通过 Web 界面控制智能设备	
安全关机	计划关机	配置 UPS 的维护策略，可定时重启或关闭监控的 UPS
	服务器关机	配合 NetworkShutdown 软件，当 UPS 有严重告警事件，可通知服务器关机，以免服务器突然断电宕机
告警管理	当前告警	实时告警显示、进行当前告警确认
	历史告警	历史告警查询
	告警通知配置	<ol style="list-style-type: none"> 可根据用户要求进行定制，自定义告警通知内容； 用户可以选择通知方式接收不同设备的不同级别的告警信息； 通知方式包括电子邮件、短消息、电话等； Email 支持 SSL 功能； 提供告警测试功能，测试用户是否接收到告警提醒信息； 根据用户配置定时发送系统运行状态
数据管理	设备数据	设备主要数据查询
	历史数据	历史数据查询
	日志数据	日志数据查询
	清除数据	清除历史数据和日志数据
配置管理	设备管理	<ol style="list-style-type: none"> 可动态添加、修改和删除设备，最多支持 4 个智能设备的添加； 可安装卸载设备类型，支持第三方设备接入 注：默认安装的设备不允许删除和修改
	设备信号配置	在线修改设备名称和告警级别
	批量配置	上传、下载配置文件及系统文件

主要功能	说明	
系统设置	监控单元	采集 RDU-EX 系统信息
	网络设置	1. IP、子网掩码、网关、DNS 等相关网络信息设置； 2. 上层监控系统 RDU-M 机房管理器访问 RDU-EX 的权限设置； 3. 远程服务设置
	用户管理	增加、修改和删除用户信息
	时间校准	校准 RDU-EX 实时时钟
	系统重置	重启 RDU-EX 和恢复默认配置
	站点信息设置	在线修改站点信息
	系统升级	在线升级应用程序
	标题栏设置	设置 Web 页面上方的标题和 Logo 图片
帮助信息	关于 RDU-EX	显示 RDU-EX 的产品序列号、特征码及版本信息，并提供用户手册及工具软件的下载

1.3 技术指标

1.3.1 环境指标

RDU-EX 的环境指标见表 1-7。

表1-7 环境条件

项目	要求
使用场所	通常为数据中心或者计算机房，一般有空调环境
工作温度	-10℃~+55℃
相对湿度	5%RH~95%RH，无冷凝
使用环境	尘埃满足 GR-63 的室内标准。无腐蚀性气体、可燃性气体、油雾、水蒸气、滴水或盐分等
大气压力	70kPa~106kPa
存储温度	-40℃~+70℃
冷却方式	自然冷
配电网络	TT/TN
防护等级	IP20

1.3.2 机械指标

RDU-EX 的机械指标见表 1-8。

表1-8 机械指标

对外型号	度量	数值	误差
RDU-SICP	高度	42mm	< ±0.5 mm
	宽度	130mm	< ±1 mm
	深度	170mm	< ±1 mm
	重量	<1kg	
封堵挡板	高度	42mm	< ±0.5 mm
	宽度	31mm	< ±1 mm
	深度	331mm	< ±1 mm
	重量	<0.5kg	

1.3.3 性能指标

RDU-EX 的北向接口见表 1-9。

表1-9 北向接口

设备类型	接入方式	说明
RDU-M	网络	私有协议
RDU-A G2	网络	SNMP 协议
第三方监控	网络	SNMP 协议

RDU-EX 的南向接口见表 1-10。

表1-10 南向接口

设备类型	最大数量	说明
智能设备	4	COM1、Sensor、COM2、COM3 可接入智能设备，每个端口最大接入数量 2 个、总数量最大接入 4 个。（Sensor 口接入传感器时，不可接入智能设备，其它接口正常接入）
传感器	4+2	Sensor 可接入传感器，最大接入 4 个温湿度传感器和 2 个 4DI 扩展（最大 19 个测点）；温湿度地址：20、21、22、23；4DI 传感器地址：F0、F1。

注：端口线缆总长不超过 100 米。

1.3.4 产品认证

RDU-EX 满足 CE 宣称。

第二章 硬件安装

本章介绍 RDU-EX 的硬件安装。

2.1 安装准备

2.1.1 注意事项

安装 RDU-EX 时，应注意以下事项，以避免出现意外事故对人身及设备造成伤害。

- RDU-EX 底面带有强磁铁，放置或安装时请注意安全
- 对 RDU-EX 的所有安装操作都必须在断电情况下进行
- 确保外部设备接入到正确的 RDU-EX 端口
- 在安装过程中，安装人员需佩戴防静电手套
- 妥善布线，确保没有重物压在电源线上，不要踩踏线缆

2.1.2 环境要求

运行环境

RDU-EX 必须安装在室内。具体要求参见表 1-6。

防静电

为了将静电影响降到最低点，需要采取下列措施：

- 机房内保持适当的温度和湿度（参见表 1-6）
- 当人体接触电路板前，应佩戴防静电手套，穿防静电工作服。如果在现场无防静电手套和防静电工作服，则需用水将手部冲洗干净，并擦干

抗干扰

为了抗干扰，需要采取下列措施：

- 避免将 RDU-EX 工作地和电力设备的接地装置或防雷接地装置合用，两者尽可能远离
- 远离强功率无线电发射台、雷达发射台、高频大电流设备
- 必要时采取电磁屏蔽的方法

2.2 安装 RDU-EX

2.2.1 挂式安装

RDU-EX 可挂装在机柜理线板、墙面等平面上。挂耳安装方式和理线板安装效果如图 2-1 所示。

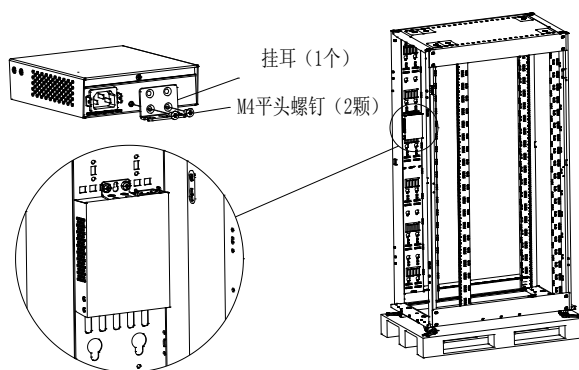


图2-1 安装挂耳和挂式安装效果图

2.2.2 机架安装

1. 确认安装机架已被固定好，机架内外没有影响安装的障碍物。
2. 用所附 M4 螺钉将挂耳（挂耳为多用途零部件，即用于挂式安装也用于机架安装）固定在 RDU-EX 卡盒侧面（左右两侧皆可），如图 2-2 所示。
3. 用 M6 浮动螺母将 RDU-EX 通过侧面的挂耳固定在机架上。

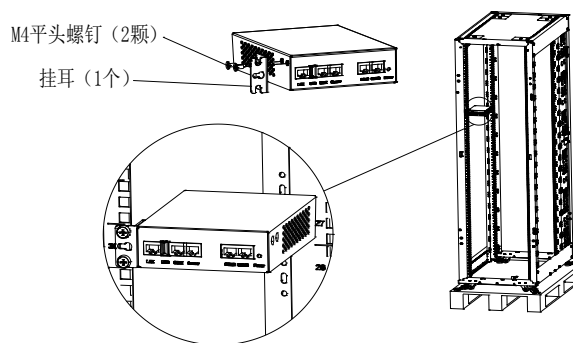


图2-2 安装挂耳和机架安装效果图

注意

1. 用户可采用挡板（选配件）遮挡机架空余部分，挡板左右两侧亦皆可安装；
2. 按照图 2-3 先连接挡板与 RDU-EX，然后再进行机架安装。

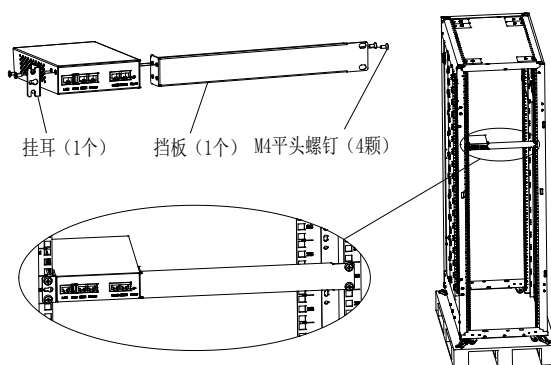


图2-3 安装挂耳、挡板和安装示意图

2.2.3 磁吸安装

RDU-EX 的底面安装有三个强磁铁，如图 2-4 所示。可吸附在平整的机柜表面。

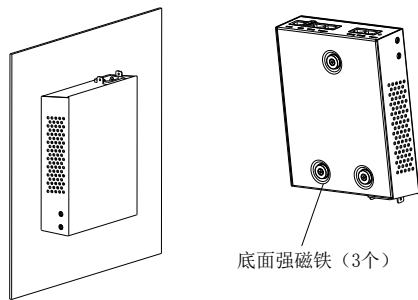




图2-4 RDU-EX 底面强磁铁和安装效果图

 注意

磁铁吸力强，安装时请小心夹手！

2.3 电气连接

 注意

RDU-EX 输入电压：100Vac~240Vac，频率：50/60Hz。

按图 2-5 中的方式插接电源线缆，并搭接防脱卡扣。完成后将线缆另一端接入供电电源。

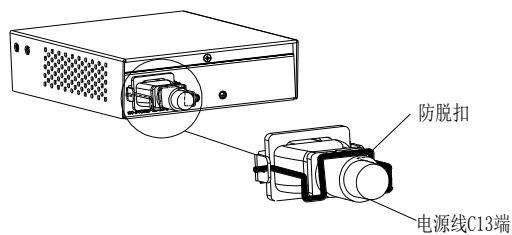


图2-5 电源防脱扣示意图

第三章 RDU-EX 的 Web 界面

本章详细介绍如何通过 Web 浏览器登录 RDU-EX 及 RDU-EX 的相关功能。

3.1 登录准备

为保证 RDU-EX 页面功能的正常使用，请参照本章所述内容选择并设置浏览器选项。

3.1.1 检查 IP 地址连通性

通过 Web 登录 RDU-EX 前请首先确认 RDU-EX 的 IP 地址，并测试其网络连通性，测试方法参见 4.2 常见问题处理中的问题 5。

3.1.2 检查浏览器版本

为获得最佳用户体验，推荐使用 Internet Explorer 浏览器，版本包括：**IE8、IE9、IE10 或 IE11**。

3.1.3 检查浏览器设置

检查 IE 常规设置

双击 IE 图标运行该软件，点击菜单**工具->Internet 选项**，点击**常规**页签中的**设置 (S)**，将**检查所存网页的较新版本**选择为**每次访问网页时 (E)**，如图 3-1 所示。

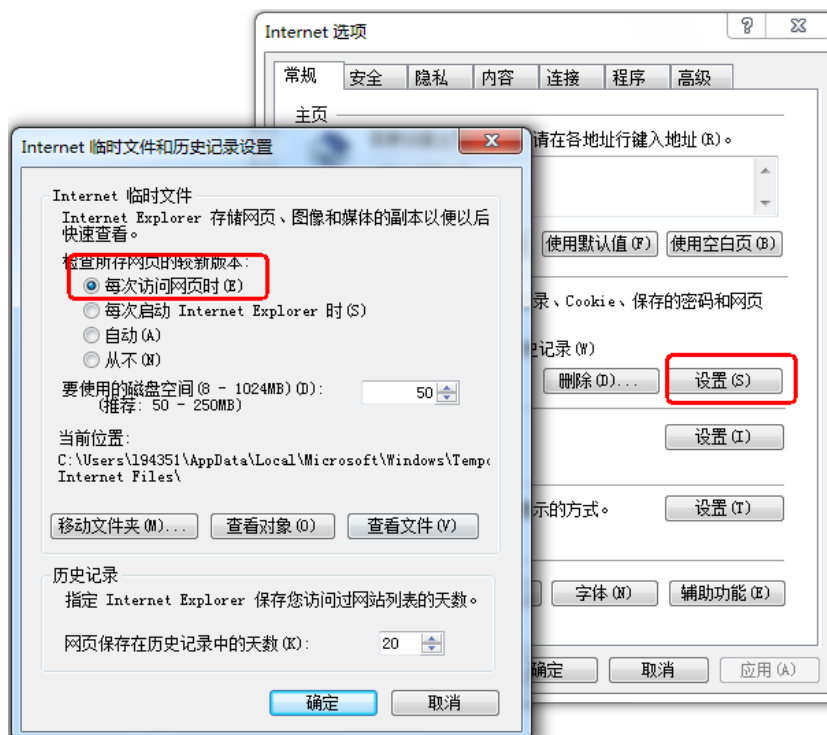


图3-1 选择常规页签

检查 IE 代理设置

1. 双击 IE 图标运行该软件，点击菜单**工具->Internet 选项**，然后选择**连接**页签，弹出如图 3-2 所示页面。

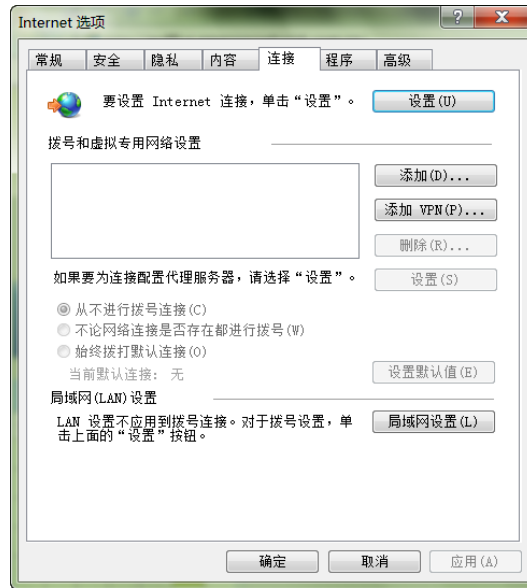


图3-2 选择连接页签

2. 如图 3-2 所示的页面中，点击**局域网设置 (L)**，弹出如图 3-3 所示页面。

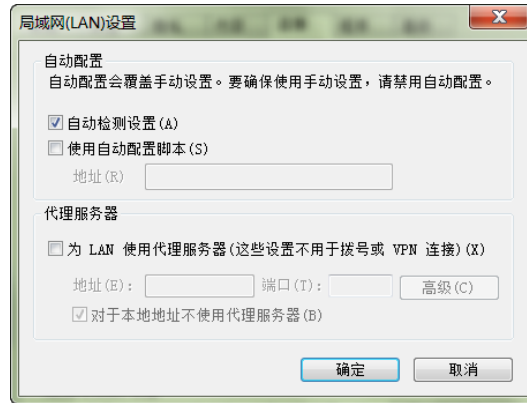


图3-3 局域网设置

3. 请咨询您所在网络的网络管理员，询问其是否需要代理配置及配置方法，如果无需代理请不要勾选任何选项。

检查 IE 安全设置

1. 双击 IE 图标运行该软件，点击菜单**工具**→**Internet 选项**，然后选择**安全**页签，弹出如图 3-4 所示页面。

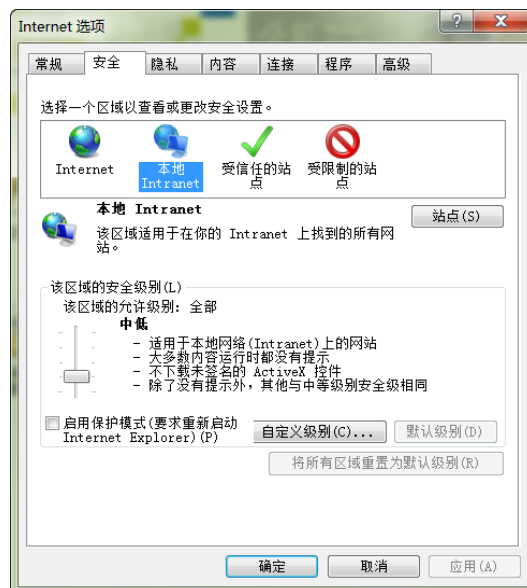


图3-4 安全设置 1

2. 如图 3-4 所示，选择本地 Intranet，点击自定义级别 (C)，弹出如图 3-5 所示对话框。

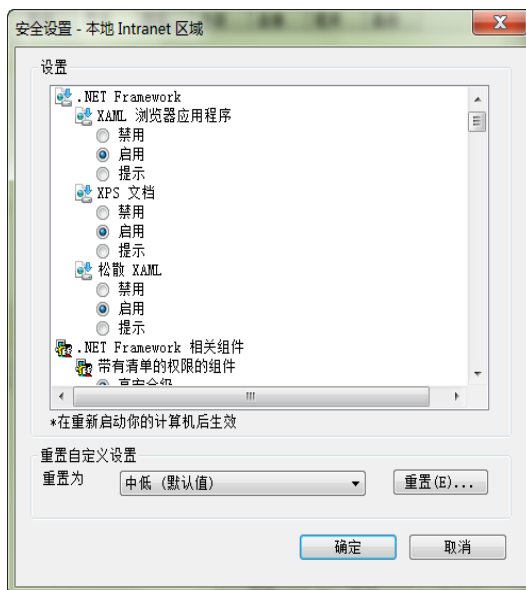


图3-5 安全设置 2

3. 如图 3-5 所示，将自定义设置选为安全性-中低，并点击**重置 (E)** 按钮结束重置自定义设置。
4. 如图 3-6 所示，设置启用文件下载。

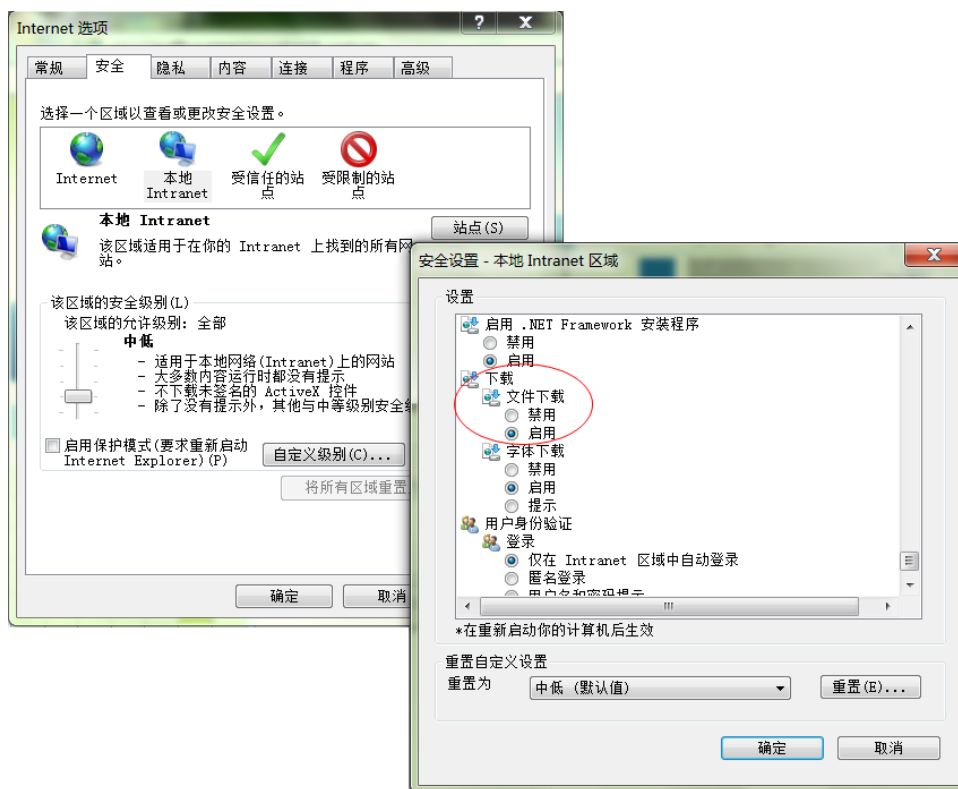


图3-6 启用文件下载

5. 如图 3-7 所示，设置启用对没有标记为安全的 ActiveX 控件进行初始化和脚本运行。

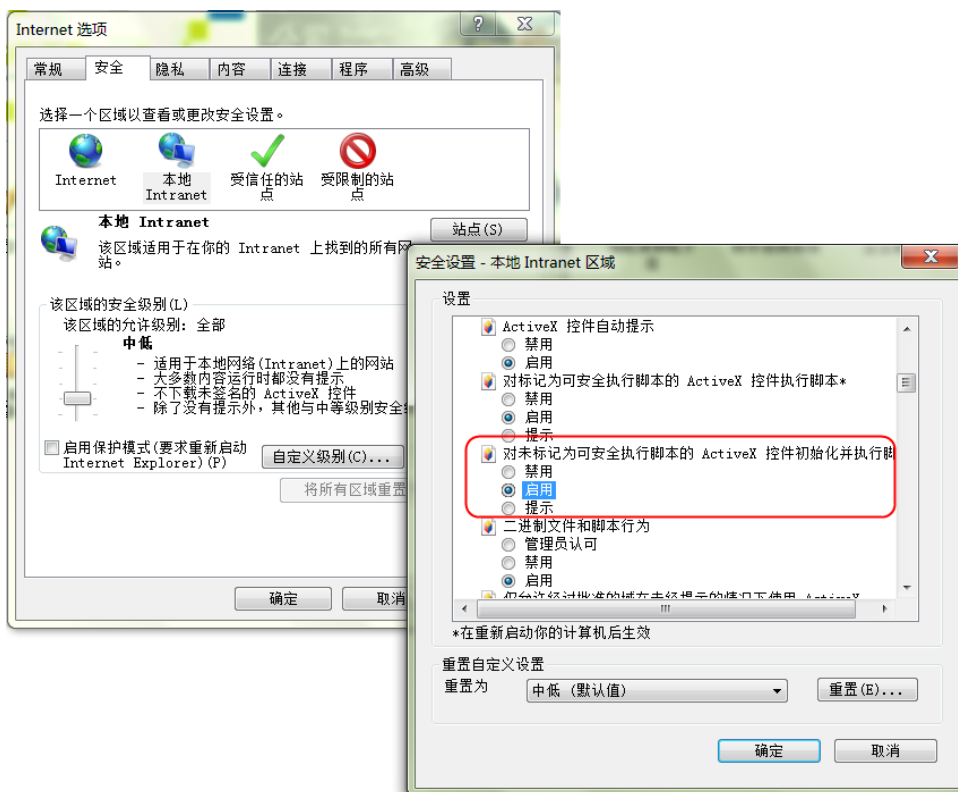


图3-7 启用 ActiveX 控件

6. 如图 3-8 所示，将 RDU-EX 的 IP 地址添加到受信任的站点的列表中。

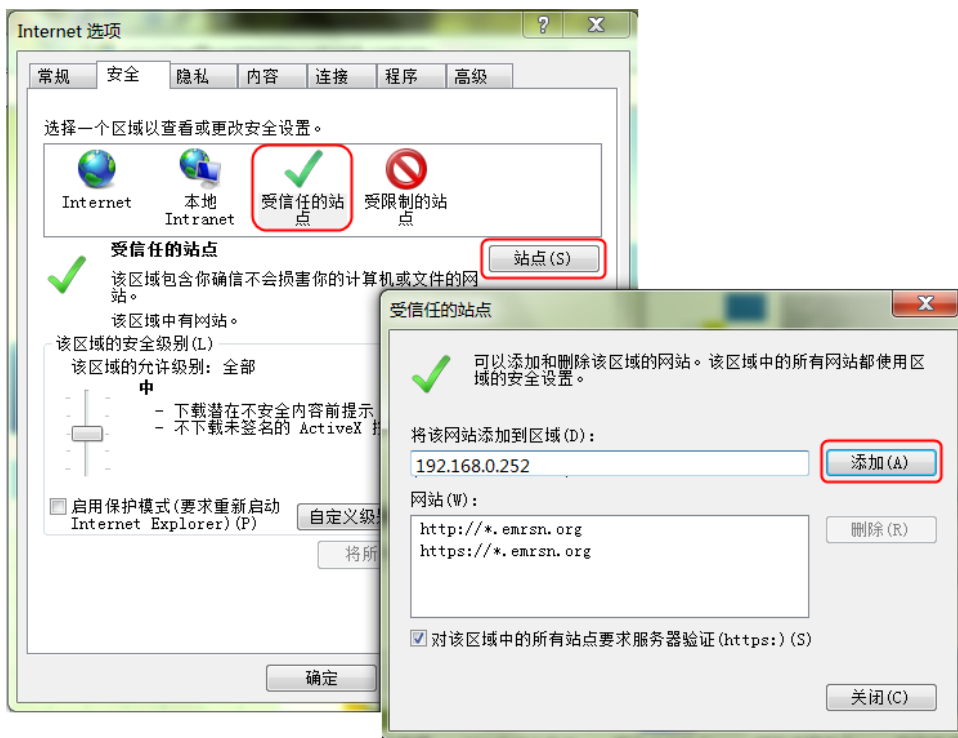


图3-8 添加到可信站点





3.2 登录 RDU-EX

3.2.1 登录页面

1. 启动 IE，在地址栏中输入 RDU-EX 的 IP 地址，出现登录页面，如图 3-9 所示，若未出现登录页面，参见 4.2 常见问题处理中的问题 5 进行处理。



图3-9 RDU-EX 登录页面

2. 在登录页面中，点击  或  选择喜欢的主题风格， 代表清澈蓝； 代表深海蓝，效果如图 3-9 所示。
3. 输入用户名和密码（默认用户名：`admin`，默认密码：`emerson`）登录 RDU-EX，弹出主页如图 3-11 所示。

3.2.2 忘记密码

若忘记用户密码，可在登录页面，单击 **忘记密码** 按钮，屏幕显示取回密码页面，如图 3-10 所示。



图3-10 取回密码页面

输入您的用户名，单击**取回密码**按钮，您的密码会发送到您之前设置的邮箱或手机；单击**返回登录**按钮取消操作。

注意

1. 您只有事先在**短信模块**和**邮件服务器配置**页面正确设置了邮件或短信参数，才能收到系统发出的密码，具体的设置方法见 3.4.3 告警管理中的**告警通知配置**。
2. 取回的密码是系统随机生成的新密码，请成功登录后自行修改。

3.3 RDU-EX 主页

登录成功后，默认显示 RDU-EX 主页，如图 3-11 所示。



- 1. 菜单项
- 2. 可控状态
- 3. 各级别告警数目
- 4. 系统标题
- 5. Logo
- 6. 注销[当前用户]
- 7. 功能显示区
- 8. 告警显示列表
- 9. 告警提醒设置
- 10. 校时链接

图3-11 RDU-EX 主页

3.3.1 校时链接

页面左下方显示 RDU-EX 系统时间，单击 **RDU-EX 系统时间**，会跳转至**时间校准**页面，具体操作详见 3.4.6 *系统设置* 中的**时间校准**功能的描述。

3.3.2 解除超时

当页面超过 15 分钟没有操作时，页面将变成不可控状态，如图 3-12 所示。

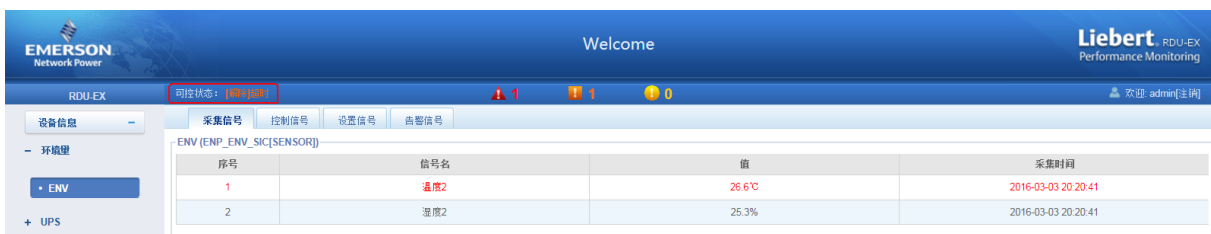


图3-12 可控状态

点击【**解除**】超时后，出现如图 3-13 所示的输入框，校验通过后，大约 5 秒后可控状态恢复正常。



图3-13 密码校验

3.3.3 注销登录

点击主页右上角**注销**链接，出现如图 3-14 所示提示框，点击**确认**后可安全退出。



图3-14 注销登录

3.3.4 实时告警提醒设置

实时告警显示列表默认收缩于页面底部，可参照图 3-11 进行如下操作：

1. 点击**查看当前告警**手动弹出实时告警显示列表；
2. 勾选**自动弹出**复选框使实时告警列表在告警产生时自动弹出；
3. 勾选**告警声音**复选框使系统在有告警的时候通过浏览器播放告警声音。

3.4 菜单项

在 RDU-EX 主页中，菜单项包括**设备信息**、**安全关机**、**告警管理**、**数据管理**、**配置管理**、**系统设置**和**帮助信息**。

3.4.1 设备信息

点击左边的**设备信息**菜单，将出现设备信息树，点击具体的设备会在右侧显示该设备的相关信息，包括**采集信号**、**控制信号**、**设置信号**、**告警信号**等四个标签页。

注意

设备信息中 ENV 设备为虚拟设备，表示 RDU-EX 机身上接入的所有温度及温湿度传感器。

采集信号

点击**采集信号**选项卡，可进入采集信号页面显示选定设备的采集信号，如图 3-15 所示。

序号	信号名	值	采集时间
1	温度2	27.2°C	2016-03-03 20:02:59
2	湿度2	24.4%	2016-03-03 20:02:59

图3-15 采集信号

如果某个信号处于告警状态则该信号所在行显示为红色。

控制信号

点击**控制信号**选项卡，进入控制信号页面显示选定设备的控制信号，如图 3-16 所示。



图3-16 控制信号

可点击**设置**按钮对该设备进行控制。

设置信号

点击**设置信号**选项卡，进入设置信号页面显示选定设备的设置信号，如图 3-17 所示。



图3-17 设置信号

可针对信号进行批量设置，且每次最大批量设置 16 个信号。

告警信号

点击**告警信号**选项卡，可进入告警信号页面显示选定设备的告警信号，如图 3-18 所示。



图3-18 告警信号

可针对告警信号的级别进行批量设置，每次最大批量设置 16 个信号。

3.4.2 安全关机

在 RDU-EX 主页中，点击左边**安全关机**菜单，可见 2 个子菜单，包括：**计划关机设置**和**服务器关机**。

计划关机设置

点击**安全关机**菜单下的**计划关机设置**，弹出如图 3-19 所示页面。



图3-19 计划关机设置页面

计划关机设置页面用于添加、删除和修改 UPS 设备的计划关机任务。

如图 3-19 所示，在**任务名称**栏输入计划关机任务名称，选择目标设备，选择状态标识该任务信息是否启用，选择关机模式和开机模式，并按照相应提示信息，添加关机时间，完成后如图 3-20 所示。



图3-20 计划关机任务

点击**增加**按钮，该任务信息既添加成功，如图 3-21，计划关机任务列表中已经增加了一条计划关机任务，任务列表中的计划关机任务，根据状态栏的启用状态，自动执行。



图3-21 计划关机任务列表

关于 RDU-EX 计划关机功能说明如下：

1. 开机模式为“不开机”“立即开机”方式的，开机时间不可设置，显示为“--”；
2. 关机时间可根据关机模式，自动适应时间设置格式，如图 3-22 所示。



图3-22 关机时间格式

注意

1. RDU-EX 最大支持 10 个关机任务。
2. 计划关机任务状态必须选择“启用”才能使用该任务。

服务器关机

点击**安全关机**菜单下的**服务器关机**，弹出服务器关机设置页面，如图 3-23 所示。



图3-23 服务器关机设置页面

在服务器关机设置页面中，用户可增加和删除服务器关机任务。

- 增加服务器关机操作步骤如下：

- 1) 从 **UPS** 下拉框中选择 UPS 设备；

- 2) 在**关联服务器 IP** 栏中，输入需要关闭的服务器 IP 地址；
- 3) 点击**增加**按钮即可完成增加服务器关机任务，UPS 基本信息也会显示在页面上方列表中。

注意

使用服务器关机功能请在服务器中安装“Emerson network shutdown”软件。

- 删除 UPS 操作步骤如下：

在服务器关机任务列表中选择需要删除的任务，点击**删除**按钮即可完成删除操作。

3.4.3 告警管理

告警管理提供针对告警集中管理功能，使用户可以自定义告警通知，并可在此完成历史告警的查询功能。在 RDU-EX 主页中，点击左边**告警管理**菜单，可见 3 个子菜单，包括：**当前告警**、**历史告警**和**告警通知配置**。

当前告警

点击**告警管理**菜单下的**当前告警**或按 3.3.4 *实时告警提醒设置*操作，可弹出当前告警显示列表，如图 3-24 所示。



图3-24 当前告警

1. 当前告警可通过点击告警列表上方的 Tab 页按告警等级显示系统当前的告警。
2. 点击**未确认**按钮，进行告警确认，已确认的告警将不再发送告警通知。
3. 当鼠标光标位于**已确认**链接上时，会悬浮显示该告警确认信息，鼠标光标移走后自动消失，如图 3-25 所示。



图3-25 确认信息

历史告警

点击**告警管理**菜单下的**历史告警**，查看历史告警记录。选择一个设备（例如“所有设备”），并设置开始时间（例如“2016-03-04 00:00:00”）和截至时间（例如“2016-03-04 23:59:59”）。然后点击**查询**按钮，将列出开始时间到截至时间里的所有告警记录，包括的信息有：序数、设备名称、信号名名称、告警级别、触发值、开始时间、确认人、确认时间和结束时间，如图 3-26 所示。

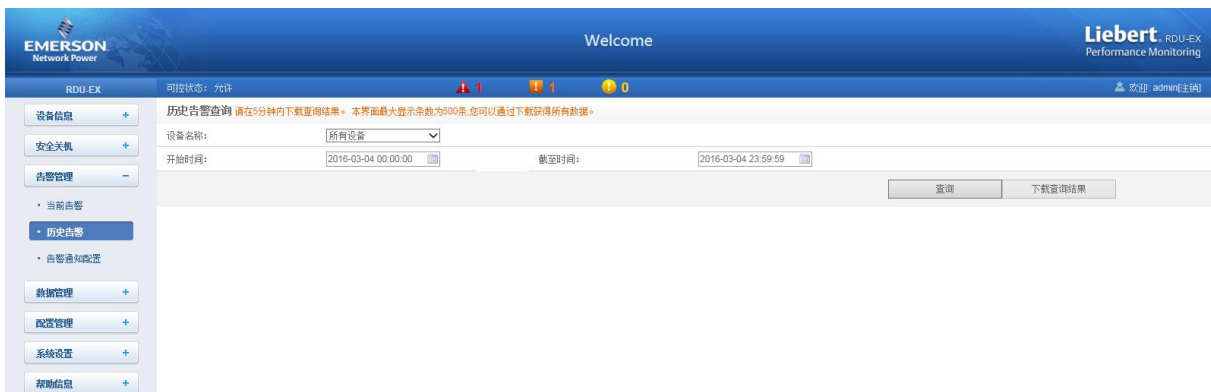


图3-26 历史告警查询

点击**下载查询结果**按钮还可下载查询结果。

告警通知配置

1. 用户告警通知配置

点击**告警管理**菜单下的**告警通知配置**，弹出如图 3-27 所示页面。用户可以选择采用哪些通知方式接收哪些设备的哪一级别告警通知，同时用户可以选择告警通知信息的语言类型，并自定义告警内容（默认包括设备名称、告警描述、告警时间和告警状态）。

点击**保存配置**按钮完成告警配置。当告警产生时会通过配置的通知方式通知用户。

注意

1. 用户首先必须选择**通知方式**，页面下方的**告警通知配置**表方可编辑；
2. 选择**选择全部**时，所有设备同时被配置相同的告警级别；
3. 选择低级别告警时，此级别以上级别告警将全部选中；
4. 选择某个设备的同时，最高级别告警**紧急告警**默认被选中。



图3-27 用户告警通知配置

2. 短信模块和邮件服务器配置

点击**告警管理**菜单下的**告警通知配置**，然后点击**短信模块和邮件服务器配置**按钮，弹出如图 3-28 所示页面。



图3-28 短信模块和邮件服务器配置

在图 3-28 所示页面中，用户可配置短信模块使系统通过短信进行告警通知，也可配置邮件服务器使系统通过邮件进行告警通知，其配置步骤如下：

- 短信模块配置

- 1) 根据需要通过 USB 端口接入短信 MODEM，然后选择**端口类型**，页面会自动显示**通信参数**；
- 2) 根据接入短信 MODEM 的型号选择**短信模块**的类型（GSM）；
- 3) 设置短信 MODEM 的通信参数；
- 4) 点击**保存配置**按钮，保存当前用户的短信模块配置。

- 邮件服务器配置

- 1) 在**邮件服务器**处输入服务器 IP 地址或域名；
- 2) 在对应栏输入**端口号**、**邮件用户名**、**邮件密码**和**发件箱地址**；
- 3) 点击**保存配置**按钮，保存当前用户的邮件服务器配置。

注意

1. 端口号默认为“25”，当选择启用 SSL 时，端口号自动变为“465”；
2. 用户名默认为“RDU-A”；
3. 使用 SSL 时，需确保邮件服务器支持 SSL 功能。

3. 系统状态定时通知配置

点击**告警管理**菜单下的**告警通知配置**，然后点击**系统状态定时通知配置**按钮，弹出如图 3-29 所示页面。



图3-29 系统状态定时通知配置

注意

1. 系统状态定时通知配置须与用户告警通知配置配合使用，否则无法选择用户名、通知方式以及发送语言；
2. 对于系统状态定时通知，不支持电话通知方式；
3. 系统状态定时通知是指给用户发送当前 RDU-EX 整个系统的运行状态，即正常或告警状态。

- 1) 在用户告警通知配置页面完成并保存发送用户、通知方式以及发送语言的设置；
- 2) 在系统状态定时通知配置页面依次设置发送时段设置（设置范围：8:00~20:00）、发送周期模式（默认：小时）、发送间隔设置（默认：1）和发送时间设置（默认：开始时间）。
- 3) 点击保存按钮，保存系统状态定时通知配置。

3.4.4 数据管理

数据管理为用户提供各种类型的历史数据和日志的查询服务。

在 RDU-EX 主页中，点击左边的数据管理菜单，可见 4 个子菜单，包括：设备数据、历史数据、日志数据和清除数据。

设备数据

点击数据管理菜单下的设备数据，弹出如图 3-30 所示页面，其包含设备信息列表和 SNMP MIB 导出两个子页面。

1. 设备信息列表

如图 3-30 所示的页面中列出了所有设备的主要信息，点击下载设备信息按钮可下载查询结果。



图3-30 设备数据

2. SNMP MIB 导出

如图 3-31 所示，可按设备类型导出 MIB 信息，选择好后点击下载设备信息即可完成 MIB 信息的导出。

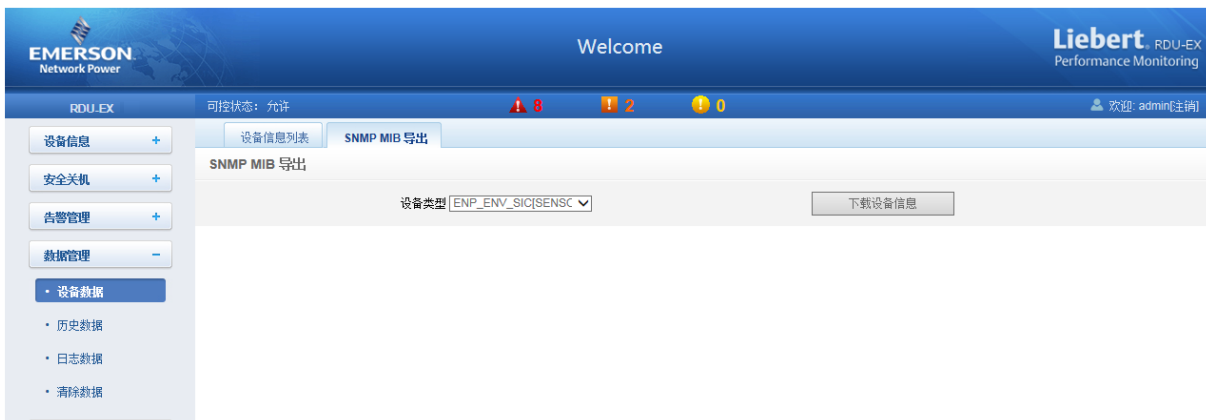


图3-31 SNMP MIB 信息导出

历史数据

点击**数据管理**菜单下的**历史数据**，弹出如图 3-32 所示页面，内有**历史数据**和**历史曲线**两个子选项卡。

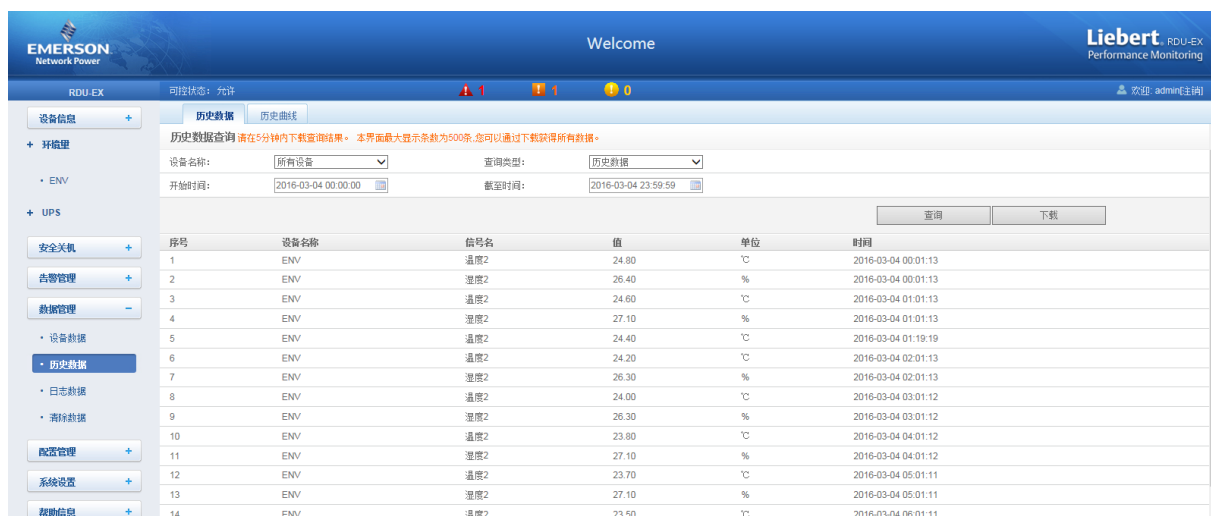


图3-32 历史数据

1. 历史数据

如图 3-32 所示，选择一个设备名（例如，“所有设备”），选择查询类型（例如，“历史数据”）并设置开始时间和截至时间（例如，从 2016-03-04 00:00:00 到 2016-03-04 23:59:59），然后点击**查询**按钮，将列出开始时间到截至时间里的所有历史数据。点击**下载**按钮下载所有查询结果。

2. 历史曲线

如图 3-33 所示，选择一个设备名（例如，“ENV”），选择查询类型（例如，“温度”）并设置开始时间和截至时间（例如，从 2016-03-04 00:00:00 到 2016-03-04 23:59:59），然后点击**生成曲线**按钮，如果查询到历史数据，则会按信号生成历史曲线。

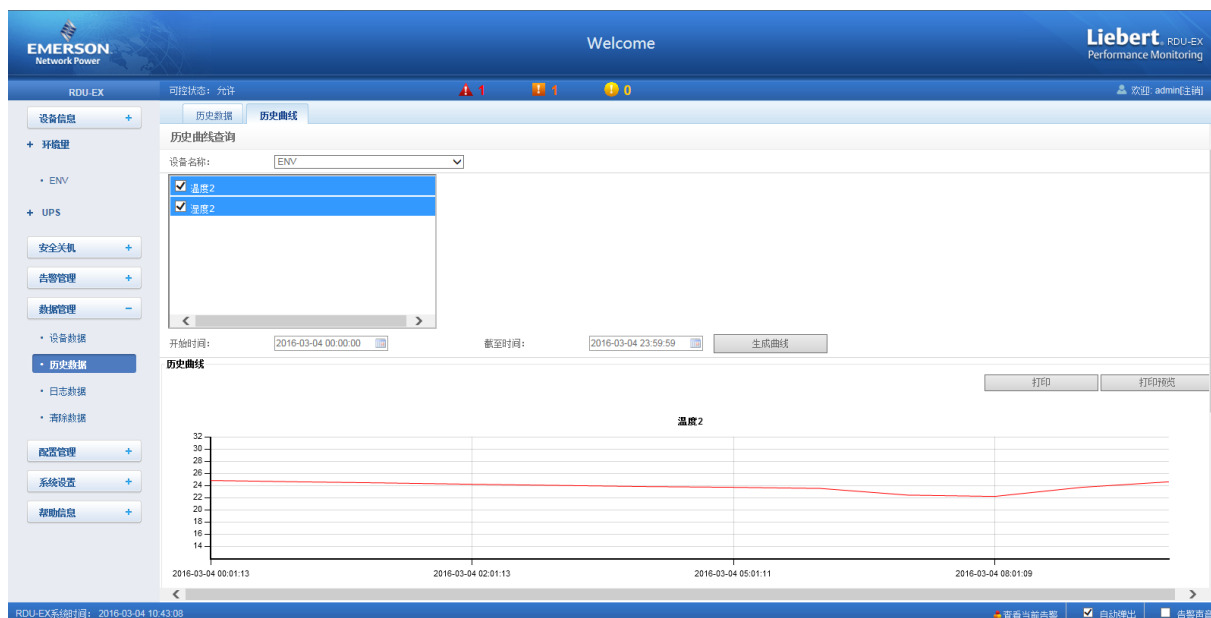


图3-33 历史曲线

日志数据

点击**数据管理**菜单下的**日志数据**，弹出如图 3-34 所示页面。

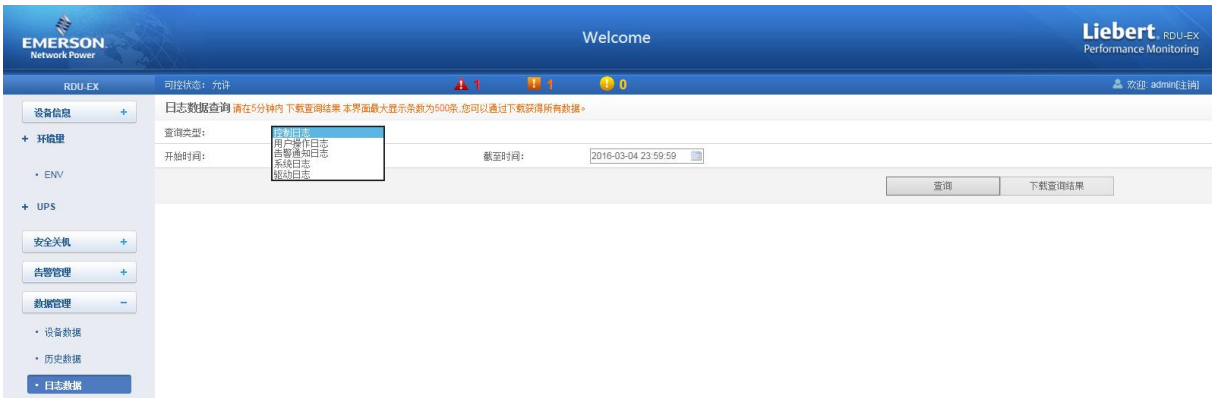


图3-34 日志数据

在图 3-34 所示页面中，选择查询类型（例如，“控制日志”）并设置开始时间和截至时间（例如，从 2016-03-04 00:00:00 到 2016-03-04 23:59:59），然后点击**查询**按钮，将列出开始时间到截至时间里的所有控制日志。点击**下载查询结果**按钮下载所有查询结果。

注意

查询类型为“系统日志”或“驱动日志”时，点击**查询**按钮后查询结果不会显示在页面上，其会直接以压缩包的形式下载。

清除数据

点击**数据管理**菜单下的**清除数据**子菜单，弹出如图 3-35 所示页面。

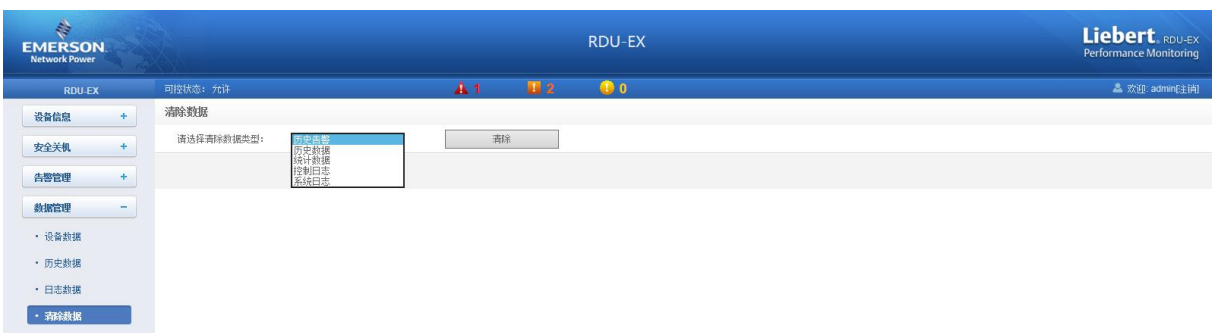


图3-35 清除数据

图 3-35 所示的页面中，用户可以选择“历史告警”，然后点击**清除**按钮清除所有历史告警。同样地，用户可以清除下拉框中的其他任何可获得的数据。

3.4.5 配置管理

在 RDU-EX 主页中，点击左边的**配置管理**菜单，可见 3 个子菜单，包括：**设备管理**、**设备信号配置**和**批量配置**。

设备管理

1. 添加/修改/删除设备

点击**配置管理**菜单下的**设备管理**，弹出如图 3-36 所示页面。



图3-36 添加/修改/删除设备

图 3-36 所示的页面中，用户可以添加/修改/删除设备信息，方法如下：

- 添加设备

- 1) 选择设备类型；
- 2) 在**设备名称**的文本框里输入设备名称，或使用默认的设备名称；
- 3) 选择设备类型后，**端口号**的下拉框中将自动列出此设备类型的默认端口号；如未选择设备类型，端口号不可选择；
- 4) 在**设备地址**的文本框里输入设备地址，设备地址必须是从 1 到 XX 的阿拉伯数字，并且同一端口号下的设备地址不允许重复。有些设备类型不需要输入设备地址，此时，设备地址的文本框将变为灰色，并且不可编辑。当一种设备有多个模块时，需要添加模块地址，模块地址必须是从 1 到 XX 的阿拉伯数字，并且一种设备下的模块地址不允许重复；
- 5) 选择或输入设备位置；
- 6) 在**通信参数**的文本框里输入通信参数，在设备类型确定的情况下，通信参数的文本框上会显示通信参数的提示语，其中包括该设备类型通信参数格式和默认通信参数；
- 7) 点击**添加设备**按钮，弹出如图 3-37 所示提示信息 1，同时在设备列表中增加一条设备信息；
- 8) 点击**保存配置**按钮，弹出如图 3-37 所示提示信息 2；

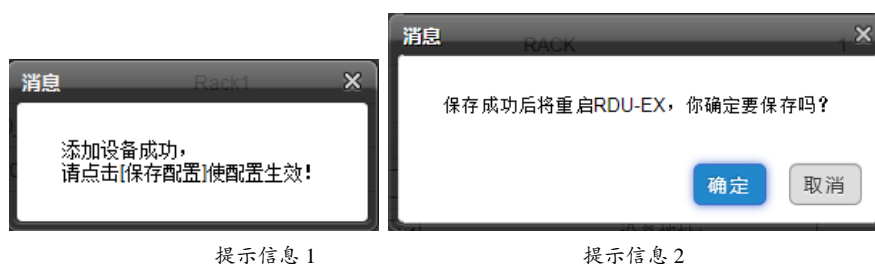


图3-37 提示信息

若点击**取消**按钮，新添设备无效；若点击**确定**按钮，弹出用户安全验证对话框，如图 3-13 所示。

- 9) 输入当前用户的登录密码，点击**确定**按钮，校验通过后将跳转到系统重启界面，如图 3-38 所示；



图3-38 系统重启页面

系统重启后，新添加的设备生效。

10) 系统重启完毕后，新添加的设备将显示在设备管理页面的列表中。

注意

系统默认可以添加 4 个智能设备，不包含 RDU-EX 自身。

● 删除设备：

- 1) 在设备列表中选择需要删除的设备；
- 2) 点击**删除设备**按钮将设备删除；
- 3) 点击**保存配置**按钮使删除设备生效，具体操作与增加新设备相同。

注意

点击**删除设备**按钮前，如果更改了此设备的相关信息，则该设备不能删除。

● 修改设备：

- 1) 在设备列表中选择需要修改的设备；
- 2) 修改设备信息；
- 3) 点击**修改设备**按钮修改设备信息；
- 4) 点击**保存配置**按钮使设备添加生效，具体操作与增加新设备相同。

在**添加/修改/删除设备**页面进行了添加、修改或删除操作后，未点击**保存配置**按钮使配置生效，在离开该页面时会弹出提示信息如图 3-39 所示，提示用户保存配置。

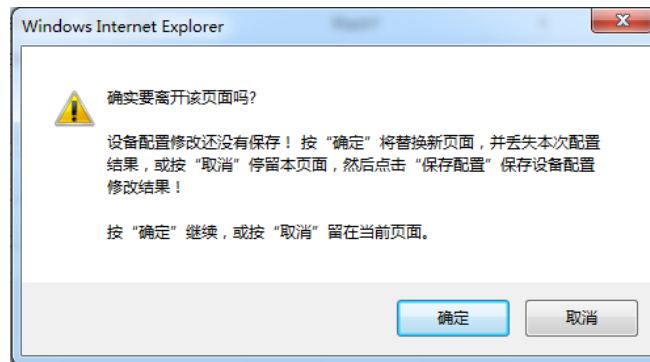


图3-39 提示信息 3

注意

保存配置按钮可以一次性保存所有操作结果。

2. 安装/卸载设备类型

点击**配置管理**菜单下的**设备管理**，然后点击**安装/卸载设备类型**选项卡，弹出如图 3-40 所示页面。



图3-40 安装/卸载设备类型

点击**浏览...**按钮，可以从本地目录上传驱动配置包（.iru 文件格式），点击**安装**按钮，安装新的设备类型。

注意

系统支持的设备类型数量与系统剩余空间和驱动配置包本身大小有关，但最多不超过 64 个。

页面右边显示已安装设备的设备类型信息，点击**卸载**按钮，弹出确认对话框，如图 3-41 所示。



图3-41 确认对话框

点击**确定**按钮，弹出用户安全验证对话框，如图 3-13 所示。输入当前用户的登录密码，点击**确定**按钮，即可卸载相应的设备类型。

注意

1. 安装时，如果设备类型存在，且设备驱动版本高于待安装的驱动时，将无法重复安装该设备类型；
2. 如果安装包没有版本信息或者版本信息与软件版本不匹配，也无法安装该设备类型；
3. 如果有设备使用此设备类型，**卸载**按钮将变为灰色，显示**使用中**，无法卸载该设备类型。

设备信号配置

点击**配置管理**菜单下的**设备信号配置**，弹出如图 3-42 所示页面。



图3-42 修改设备名

图 3-42 所示的页面中，用户可以修改设备名称。输入新的设备名称后，点击**设置**按钮进行批量设置。

注意

设备名称字符可以是英文字母、数字、空格和下划线，输入其它字符将弹出如图 3-43 所示提示框。



图3-43 无效字符提示信息

批量配置

点击**配置管理**菜单下的**批量配置**，弹出如图 3-44 所示页面。



图3-44 批量配置

用户可执行**上传**和**下载**操作，完成系统批量配置。

注意

1. 只有 admin 用户才有执行批量配置的权限，如果无法执行批量配置，请点击**查看帮助**获取帮助信息。
2. 批量配置的文件下载到本地后是加密的。

3.4.6 系统设置

在 RDU-EX 主页中，点击左边的**系统设置**菜单，可见 8 个子菜单，包括：**监控单元**、**网络设置**、**用户管理**、**时间校准**、**恢复默认**、**站点信息设置**、**系统升级**和**标题栏设置**。

监控单元

监控单元是针对 RDU-EX 系统自身的信号进行设置，包括采集信号、设置信号和告警信号，如图 3-45 所示。



图3-45 监控单元（采集信号）

关于监控单元中**采集信号**、**设置信号**、**告警信号**三个子页面的操作方法请参考 3.4.1 设备信息。

注意

在设置信号中如果设置**当前告警阻塞**为**阻塞**，则出现当前告警时阻塞告警，这种情况下：

1. 当前告警中除当前告警阻塞告警外，其余全部结束；
2. **当前告警阻塞**的**阻塞**设置在 24 小时后自动解除。

网络设置

1. IP 设置

点击**系统设置**菜单下的**网络设置**，弹出如图 3-46 所示页面。



图3-46 IP 设置

图 3-46 所示的页面中，用户可以配置的网络参数如下：**IP 地址**、**子网掩码**、**默认网关**、**DNS1**（首选服务器）和 **DNS2**（备用服务器）。修改网络参数之后，点击**保存参数**按钮使参数生效。

注意

修改 IP 地址之后，默认跳转至新网络地址重新登录 RDU-EX。

2. 访问控制

点击**系统设置**菜单下的**网络设置**，然后点击**访问控制**按钮，弹出如图 3-47 所示页面。



图3-47 访问控制

添加访问者时，在**易睿管理器 IP** 文本框中输入新的易睿管理器 IP 地址，点击**添加访问者**按钮完成配置。

注意

1. 系统最多可以添加 3 个易睿管理器 IP 地址。
2. 如果在添加访问者时选择使用代理，则还需对代理服务器进行配置。

3. SNMP 设置

点击**系统设置**菜单下的**网络设置**，然后点击**SNMP 设置**按钮，可对 SNMP 代理进行配置，RDU-EX 系统的 SNMP 代理支持 V2 和 V3 两种版本：

如图 3-48 所示，SNMP V2 的具体设置方法如下：

- 1) 设置 NMS IP（SNMP 代理数据接收端的主机 IP 地址）；
- 2) 设置是否发送 Trap：“允许”、“禁止”；
- 3) 其它参数保持默认值。



图3-48 SNMP (v2) 设置

如图 3-49 所示，SNMP V3 的具体设置方法如下：

- 1) 设置 NMS IP（SNMP 代理数据接收端的主机 IP 地址）；
- 2) 选择是否 Trap 发送：“允许”、“禁止”；
- 3) 设置用户名；
- 4) 选择用户类型：“认证并加密”、“认证不加密”、“不认证不加密”；
- 5) 选择认证类型：“MD5”、“SHA”；
- 6) 选择加密类型：“DES”；
- 7) 自定义设置认证算法和加密算法的密码。

注意

1. 在 SNMP V2 的基础上，SNMP V3 加入了用户认证和加密策略；
2. 如果用户类型选择了“不认证不加密”策略，则**认证类型**和**加密类型**下拉框变灰，无法进行设置；
3. 现阶段加密类型只支持 DES 加密类型；
4. 用户需自定义 8 个字符以上的认证和加密密码，并且该密码必须与 SNMP 代理数据接收端的主机设置的密码相同，否则无法解密接收。

完成参数设置后，点击**增加**按钮，即可增加 NMS；

如需修改 NMS 设置，选中需要修改的 NMS，修改设置，然后点击**修改**按钮保存设置；

如需删除 NMS，选中需要删除的 NMS，然后点击**删除**按钮删除 NMS。



图3-49 SNMP (v3) 设置

4. 远程服务器设置

点击**系统设置**菜单下的**网络设置**，然后点击**远程服务设置**选项卡，弹出如图 3-50 所示页面。



图3-50 远程服务设置

远程服务设置包括**远程服务请求**、**取消远程服务**及**本地主机更换**三个部分，同时用户可对远程服务系统的通信参数进行设置。

- 远程服务请求：用于建立远程托管关系

- 1) 在**客户名称**文本框中输入自定义的客户名称；
- 2) 选择**远程服务客户联系人**，当联系人选定时，会显示相应的电话及 Email；

注意

远程服务客户联系人需事先在**系统设置->用户管理**中进行设置，且必须提供电话或者 Email，否则无法进行托管请求。具体设置方法参见本节中的用户管理。

- 3) 选择**报表生成周期**：“月”、“季度”；
- 4) 点击**确定**按钮发送远程托管请求。

- 取消远程服务：用于取消已经建立的托管服务

选择**取消远程服务**，点击**确定**按钮发送命令取消当前的远程服务。

📖 注意

取消远程服务只在已建立远程托管服务的前提下有效，否则点击**确定**按钮会提示失败。

- 本地主机更换：用于远程服务中本地主机的更换

当建立远程服务的主机要退出，但又想保留已经建立的远程服务关系时，用户需更换本地主机加入远程服务，具体的设置方法同**远程服务请求**，此外加入被替换主机的硬件序列号即可。

5. 安全设置

只有管理员才能浏览和配置**安全设置**。

点击**系统设置**菜单下的**网络设置**子菜单，然后点击**安全设置**页签，弹出如图 3-51 所示页面。



图3-51 安全设置

安全设置的内容包括 **Web 访问方式**和 **Web 访问安全策略**两个部分。

1. **Web 访问方式**：选择访问 Web 页面可采用的协议是 HTTP 还是 HTTPS。默认为 HTTP 协议。

选择后，点击**保存**按钮，浏览器提示用户等待，如图 3-52 所示。



图3-52 系统重启 Web 服务器

等待的时间到达后，浏览器显示新的访问超链接，如图 3-53 所示。点击其中的超链接，即可出现以新的 Web 访问方式启动的用户登录界面。



图3-53 显示新的 Web 访问连接

注意

只有在 Web 访问方式采用 HTTPS 的情况下，才允许移动终端 APP 连接 RDU-EX。

2. Web 访问安全策略：选择是否启用 Web 访问安全策略。默认为启用。

Web 访问安全策略包括 4 个部分：账户锁定策略、登录验证码、密码复杂度策略、密码过期策略。

1) 账户锁定策略：

同一个有效用户连续登录失败 5 次后，不可再输入密码进行登录操作，只有等到指定的时间过后，才可以继续登录。admin 账户不会被锁定。

管理员可将目前处于锁定状态的账户进行重置解锁。具体操作步骤参见下一节**用户管理**中的**解锁**。

锁定时间的长短可以在图 3-51 中**账户锁定时间**编辑框中配置，默认为 5 分钟。

2) 登录验证码：

用户登录时，一旦输入了错误的用户名或密码，系统立即显示一个验证码，要求下一次登录时必须输入此验证码，如图 3-54 所示。



图3-54 登录要求输入验证码

3) 密码复杂度策略：

用户密码长度至少为 6 个字符；密码中至少包含以下字符中的两种：大写英文字符(A~Z)，小写英文字符(a~z)，数字(0~9)和非字母字符(!,\$,#,%等)。

启用 Web 访问安全策略时，不影响已有用户帐户的密码，但新建用户账户或修改已有用户密码时，新密码必须符合此复杂度要求。

4) 密码过期策略：

用户账户密码从被创建或修改时刻开始，在指定时间之内有效。有效时间长度可以在图 3-51 中**用户密码有效期**编辑框中配置，范围为 0~999 天，默认 90 天。0 天表示密码永不过期。

密码有效时间长度对除 admin 之外的所有其他账户适用，admin 账户密码永不过期。

管理员可以刷新某个帐户的有效期，新的有效期从设置的时刻开始，至有效时间长度到达为止。具体操作步骤参见下一节**用户管理**中的**刷新有效期**。

用户管理

点击**系统设置**菜单下的**用户管理**，弹出如图 3-55 所示页面。



图3-55 用户管理

图 3-55 所示的页面中，用户可以增加用户、修改用户和删除用户。

● 增加用户

- 1) 在**用户名**的文本框里输入用户名；
- 2) 选择用户的权限；
- 3) 配置用户密码，密码不能为空，且至少 6 位字母或数字；
- 4) 在**确认密码**文本框中重复输入密码；
- 5) (可选) 输入用户电话号码，电话号码可以使用以下数字和字符：0123456789、+；
- 6) (可选) 输入邮件地址；
- 7) 点击**增加用户**按钮，将弹出用户安全验证对话框，如图 3-13 所示。输入当前用户的登录密码，点击**确定**按钮，增加新用户。

📖 注意

1. 用户名只能使用英文字母、数字以及-和_，并且首字符必须为字母或数字。
2. 如果启用了 Web 访问安全策略，对密码有更多的要求，参见“网络设置”下的“安全设置”一节。
3. 允许最多输入两个绑定手机序列号，以逗号分隔。
4. 如果未输入绑定序列号，则系统会绑定最先两个从 APP 登录的移动设备的序列号。
5. 绑定后，系统只允许所绑定的移动终端从 APP 访问 RDU-EX。如果要重新绑定，只需修改或删除绑定序列号即可。

● 删除用户

- 1) 在用户名单中选择需要删除的用户；
- 2) 点击**删除用户**按钮，将弹出确认对话框，如图 3-56 所示。



图3-56 确认对话框

- 3) 点击**确定**按钮，将弹出用户安全验证对话框，如图 3-13 所示。输入当前用户的登录密码，点击**确定**按钮，将所选用用户删除。

📖 注意

admin 用户不可删除。

● 修改用户

- 1) 在用户名单中选择需要修改的用户；
- 2) 修改用户信息；
- 3) 点击**修改用户**按钮，将弹出用户安全验证对话框，如图 3-13 所示。输入当前用户的登录密码，点击**确定**按钮，使修改后的用户信息生效。

登录 RDU-EX 的用户可分为 4 个用户组，他们分别具有不同的安全级别和用户权限，具体信息参见表 3-1。

表3-1 用户安全级别

安全级别	用户组	用户权限
A 级	浏览者	所有用户均能浏览设备信息
B 级	操作员	操作者可发送控制命令到智能设备
C 级	工程师	工程师拥有以下权限：发送控制命令到智能设备；浏览、控制、修改参数；下载文件；修改自身用户信息
D 级	管理员	管理员拥有全部权限：发送控制命令到智能设备；浏览、控制、修改参数；上传和下载文件；修改、增加、删除用户信息；空调群控参数设置；系统固件升级

在图 3-55 所示页面中，选择当前用户，可以进行**短信/电话告警通知测试**和**电子邮件告警通知测试**。

使用该测试功能前，需先对当前用户进行短信模块和邮件服务器配置，具体信息参见 3.4.3 告警管理中的**告警通知配置**。

- 短信/电话告警通知测试

输入**电话号码**，点击**短信/电话告警通知测试**按钮，测试当前用户的电话号码是否接通。若用户收到测试短信和电话，表示测试成功。否则测试失败，请检查当前用户的电话号码是否正确，短信 MODEM 连接是否正确。

- 电子邮件告警通知测试

输入**邮件地址**，点击**电子邮件告警通知测试**按钮，测试当前用户的邮箱地址是否正确。若收到测试邮件，表示测试成功，否则测试失败，请检查以上信息是否输入正确。

- 刷新有效期

如果启用了 Web 访问安全策略，界面上会显示所选用户的账户到期时间。管理员点击**刷新有效期**按钮，即可为所选用户刷新新的密码有效期，新的有效期起止时间参见**网络设置**一节 **Web 访问安全策略**中的**密码过期策略**。

- 解锁

如果启用了 Web 访问安全策略，对于已锁定的账户，管理员点击**解锁**按钮，即可为其解锁。参见**网络设置**一节 **Web 访问安全策略**中的**账户锁定策略**。

注意

增加、修改用户时，必须输入电话号码或邮件地址，否则无法完成设置。

时间校准

点击**系统设置**菜单下的**时间校准**可以校准时钟。图 3-57 所示页面中，RDU-EX 可以从时间服务器上自动获取时间。依次输入**主服务器**和**从服务器**的 IP 地址，输入**校时间隔**、选择**设置时区**和**校时协议类型**，然后点击**设置**按钮使得设置生效。



图3-57 时间校准

RDU-EX 也可以获取本机时间，选择**使用当前时间校时**并点击**获取本机时间**按钮来获得本机时间，然后点击**设置**按钮使新时间生效。

注意

时间校准默认选择**使用当前时间校时**。

恢复默认

点击**系统设置**菜单下的**恢复默认**，弹出如图 3-58 所示页面。



图3-58 恢复默认

点击**重启 RDU-EX** 按钮，实现系统重启。

点击**恢复默认**按钮，恢复 RDU-EX 至默认设置。

注意

如果用户使用恢复功能，RDU-EX 会恢复原始配置方案。在恢复操作之后，请确认等待 2 分钟再通过网络重新进入 RDU-EX 以使其进行完整的初始化工作。

站点信息设置

点击**系统设置**菜单下的**站点信息设置**，弹出如图 3-59 所示页面。

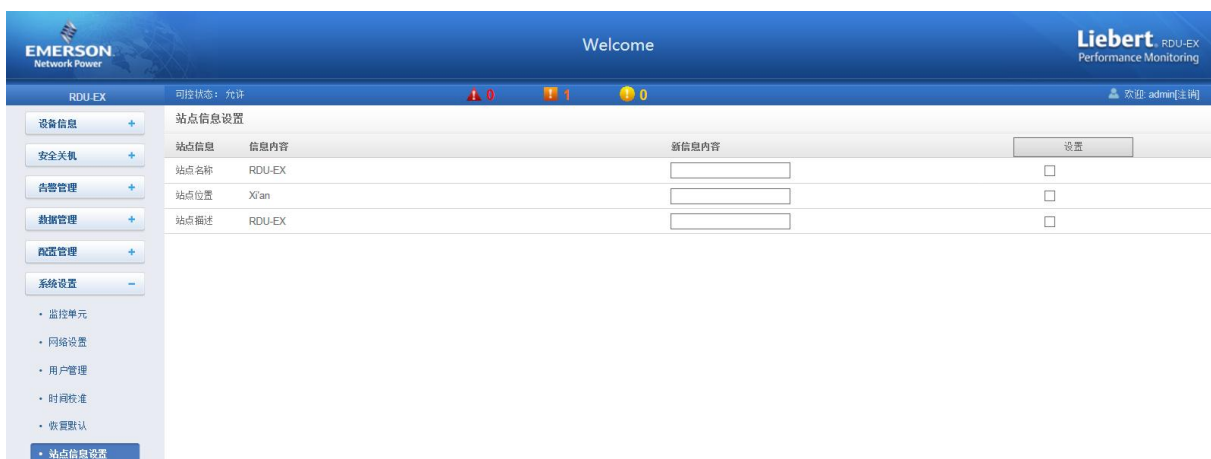


图3-59 站点信息设置

如图 3-59 所示，用户可以修改 RDU-EX 的站点信息，包括**站点名称**、**站点位置**和**站点描述**。

系统升级

点击**系统设置**菜单下的**系统升级**，弹出如图 3-60 所示页面。

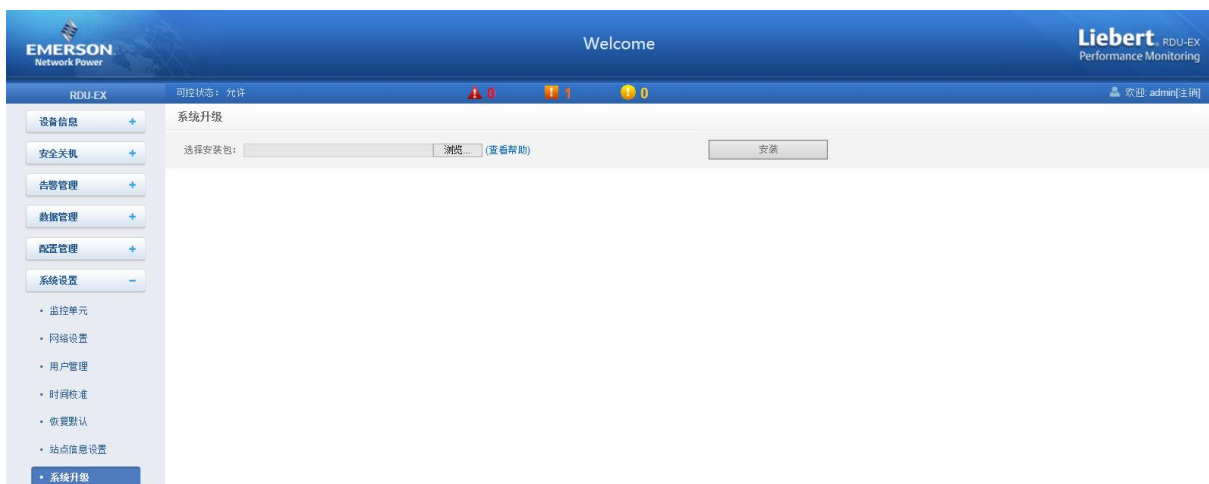


图3-60 系统升级

图 3-60 所示的页面中，点击**浏览...**按钮从本地目录下载升级包（.rdu 文件格式），然后点击**安装**按钮，进行固件升级。

注意

RDU-EX 支持增量升级功能。

标题栏设置

点击**系统设置**菜单下的**标题栏设置**，弹出如图 3-61 所示页面。

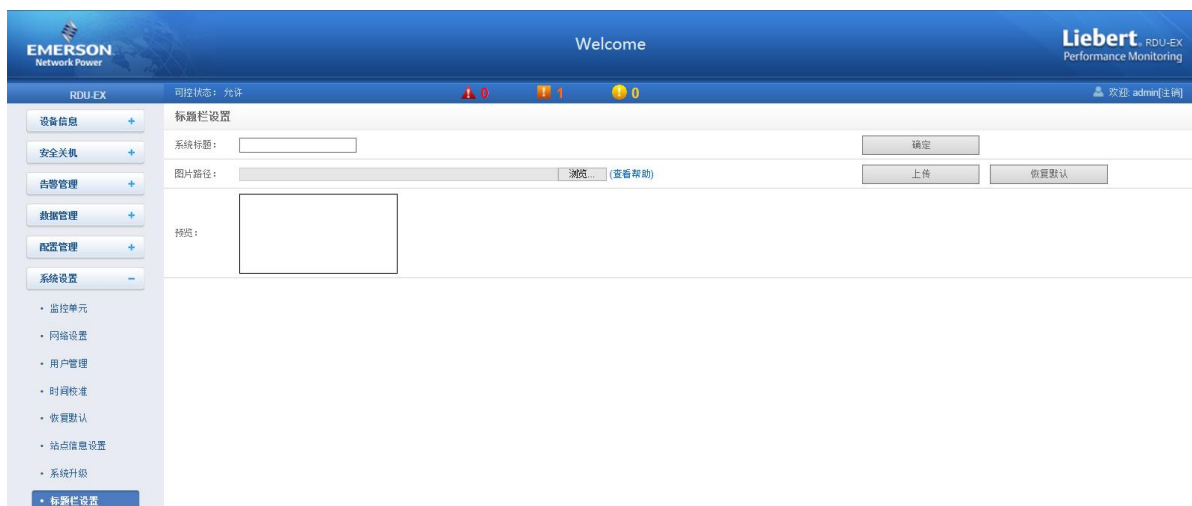


图3-61 标题设置

图 3-61 所示的页面中，用户可上传系统 Logo 图片替换页面右上方的 Logo 图片，点击**浏览...**按钮，选择需要上传的 Logo 图片，然后点击**上传**按钮将文件上传到 RDU-EX。只允许上传 [.gif]或 [.bmp]或 [.jpg]格式的图片到 RDU-EX 里，且图片大小不超过 500K。点击**恢复默认**按钮可以恢复默认 Logo 图片。

用户也可修改页面正上方的系统标题 Welcome。在**系统标题**文本框里输入自定义系统标题，点击**确定**按钮使之生效。

3.4.7 帮助信息

在 RDU-EX 主页中，点击左边的**帮助信息**菜单，可见 1 个子菜单，即：**关于 RDU-EX**。

关于 RDU-EX 页面显示 RDU-EX **软件版本**、**序列号**、**特征码**等信息，可下载 RDU-EX 用户手册和 USB 调试驱动程序，如图 3-62 所示。



图3-62 关于 RDU-EX

第四章 维护

本章介绍 RDU-EX 的维护，包括恢复默认设置和常见故障处理。

4.1 恢复默认设置

恢复默认设置可通过软件和硬件两种方式完成。

软件恢复请参见 3.4.6 系统设置中的恢复默认说明。

硬件恢复包括恢复 RDU-EX 管理员密码（默认用户名：admin，密码：emerson）和 RDU-EX 的 IP 地址（默认 IP 地址：192.168.0.252）。用户可以打开机壳参考上盖内部丝印短接 RDU-EX 板卡上 J18 跳线的 2、3 脚完成硬件恢复，跳线位置如图 4-1 所示。

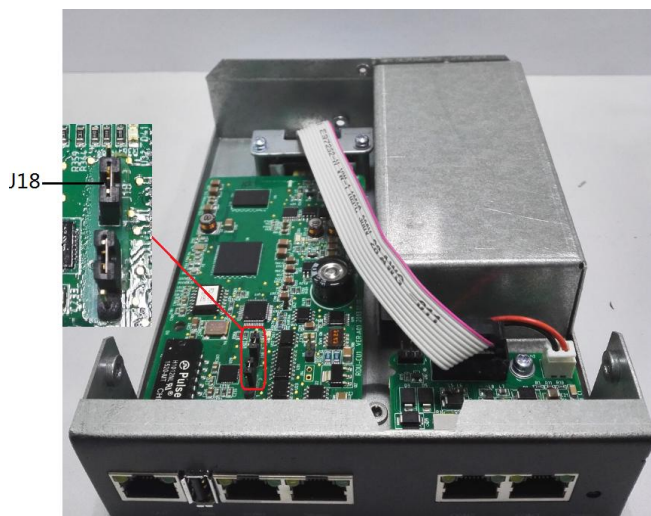


图4-1 跳线 J18 位置

4.2 常见故障处理


问题 1: RDU-EX 上电后，电源指示灯怎么不亮？

答：请检查电源线缆连接是否正确。

问题 2: 如何处理串口通信不正常？

答：请检查 RDU-EX 串口为 RS-232/RS-485 自适应串口，请确认通信参数的配置是否正确。

问题 3: 用户已选择深海蓝主题，但浏览 RDU-EX 的 Web 界面时，页面仍然为清澈蓝主题，如何处理？

答：点击[当前用户]注销按钮，返回登录界面，点击图标选择深海蓝主题，重新登录系统即可。

问题 4: 告警产生后，没有收到邮件或短信通知，或在告警没有结束情况下，邮件或短信通知次数少于 3，怎么处理？

答：按以下步骤进行排查：

- 1) 请检查短信模块和邮件服务器配置是否正确，参见 3.4.3 告警管理中的告警通知配置；
- 2) 如果没有收到短信通知，请确认电话卡是否已欠费停机；
- 3) 如果没有收到邮件通知，请点击菜单数据管理->日志数据，查询告警通知发送日志是否有发送邮件失败的记录。如果有，则表示网络忙或邮件服务器通信忙。

问题 5: 在 RDU-EX 通信正常情况下，为什么没有出现 RDU-EX 的登录页面？

答：出现以上问题有三种解决措施：

第一步：请确认 IP 地址的正确性。

请确认网线连接是否正确。

确认 RDU-EX 的 IP 地址是 192.168.0.252。

第二步：请确认 IP 地址的连通性。

确认 IP 地址连通性可使用 PING/ping 命令，方法如下：

1) 点击左下角  图标，在  框中输入“cmd”，如图 4-2 所示。

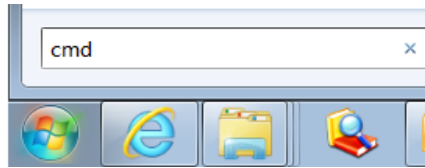


图4-2 输入“cmd”

2) 按下回车键，将弹出图 4-3 所示页面。在命令行输入“ping”和 IP 地址，（例如 ping 10.163.162.135）查看是否通信成功。

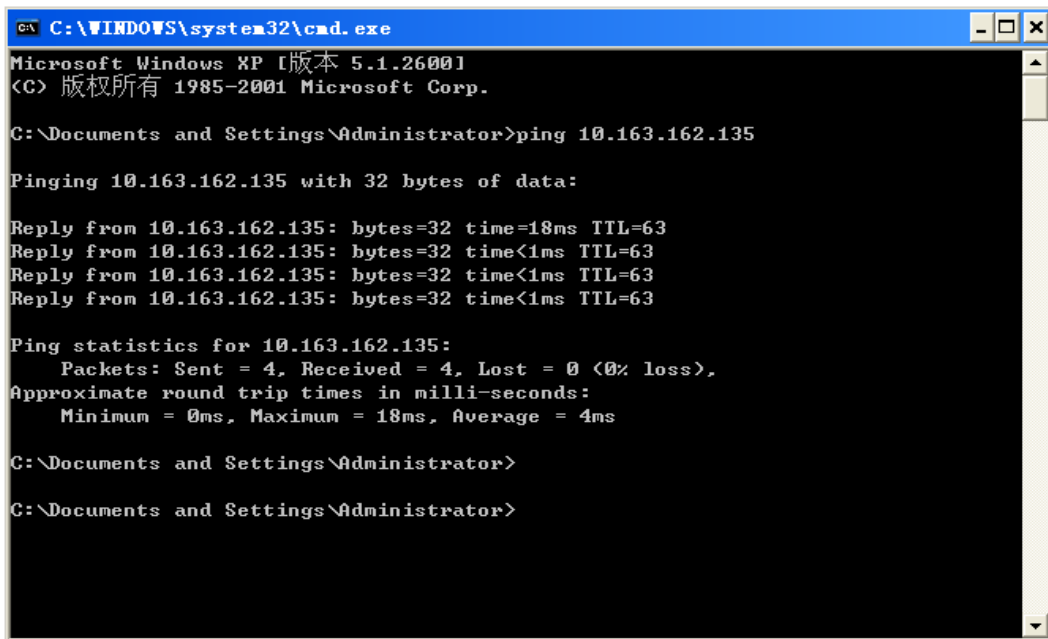


图4-3 通信测试

第三步：如果经过上述两步还是未能使网络连通，请使用机身上跳线帽恢复默认 IP，跳线帽参考上盖内部丝印所述内容。

第四步：请参照 3.1 登录准备所述内容完成登录准备。

附录一 缩略词

AC	Alternating Current	交流
CA	Critical Alarm	紧急告警
DC	Direct Current	直流
DI	Digital Input	数字输入
IE	Internet Explorer, a Web browser developed by Microsoft@	微软开发的网页浏览器
FAQ	Frequently Asked Questions	常见问题处理
FTP	File Transfer Protocol, used to transfer large chunks of data	文件传输协议, 用于传输大量数据
HTTP	Hypertext Transfer Protocol, used to convey HTML	超文本传输协议, 用于链接 HTML
LED	Light Emitting Diode	发光二极管
MA	Moderate Alarm	重要告警
NA	No Alarm	无告警
LA	Low Alarm	一般告警

附录二 标准配置清单

序号	项目描述	数量	单位
1	RDU-EX 监控单元	1	EA
2	用户手册-《RDU-EX 快速安装手册》	1	EA
3	采购成套电缆-UH52SA1SL2-UH52SA1Z UPS 电源 USB 电缆-ROHS	1	EA
3	电线电缆-IEC60320 C13 Plug-IEC60320 C14 Plug-H05VV-F-3C-1mm ² -Black-2000mm-EU	1	EA
4	小五金件--挂耳	1	EA
5	标准件-GB819.1-2000-十字槽沉头螺钉 M4×10	2	EA

附录三 有毒有害物质或元素标识表

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴联苯醚
	Pb	Hg	Cd	Cr6+	PBB	PBDE
制成板	○	○	○	○	○	○
线缆	○	○	○	○	○	○
○：表示该有毒有害物质在该部件所有均质材料中的含量在 SJ/T-11363-2006 规定的限量要求以下；						
×：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T11363-2006 规定的限量要求						
艾默生网络能源有限公司一直致力于设计和制造环保的产品，我们会通过持续的研究来减少和消除产品中的有毒有害物质						
关于环保使用期限的说明：本产品的环保使用期限（已标识在产品本体），是指在正常使用条件和遵守本产品的安全注意事项的情况下，从生产日起本产品含有的有毒有害物质或元素不会对环境、人身和财产造成严重影响的期限						
适用范围：RDU-EX						

Contents

Chapter 1 Product Description	1
1.1 Components Description.....	1
1.1.1 RDU-EX.....	1
1.1.2 Sealing Baffle Panel (Optional).....	3
1.2 Main Functions.....	3
1.3 Technical Specifications	4
1.3.1 Environment Specifications	4
1.3.2 Mechanical Specifications	4
1.3.3 Performance Specifications	4
1.3.4 Product Certification	5
Chapter 2 Hardware Installation	6
2.1 Installation Preparation	6
2.1.1 Notes	6
2.1.2 Ambient Requirements	6
2.2 Installing RDU-EX	6
2.2.1 Hanging Mode Installation	6
2.2.2 Installation in Rack	7
2.2.3 Installation Through Magnetic Iron	7
2.3 Electrical Connections	8
Chapter 3 Web Page Of RDU-EX	9
3.1 Login Preparation.....	9
3.1.1 Checking IP Address Connectivity.....	9
3.1.2 Checking Browser Version	9
3.1.3 Checking Browser Setting	9
3.2 Log In RDU-EX	13
3.2.1 Login Page	13
3.2.2 Forgetting Password.....	13
3.3 Homepage Of RDU-EX.....	14
3.3.1 Time Calibrating Link	14
3.3.2 Clearing Time-Out	14
3.3.3 Logout.....	15
3.3.4 Real-Time Alarm Pop-Up Setting	15
3.4 Menu Items	15
3.4.1 Device Information.....	15
3.4.2 Safe Shutdown	17
3.4.3 Alarm Management	19
3.4.4 Data & History	22
3.4.5 Device Options	24
3.4.6 System Options	28
3.4.7 Help	37

Chapter 4 Maintenance 38

 4.1 Restoring Default Setting 38

 4.2 FAQ 38

Appendix 1 Glossary 40

Appendix 2 Standard Configuration List 41

Chapter 1 Product Description

The RDU-EX is a network management. It can make the intelligent equipment (such as UPS, PDU, air conditioner and so on) are centralized monitoring. The RDU-EX can also connect to the environment monitoring equipment, including IRM series temperature & humidity sensor or dry contact signal input & detecting sensors. In case of an equipment alarm, it notifies the user by multiple ways: recording, sending a Trap message, sending an E-Mail or sending an SMS. The RDU-EX can meet the requirements of TCP/IP, RS232/485 networking modes and can be flexibly configured according to various application conditions.

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

1.1 Components Description

RDU-EX includes the RDU-EX host and an optional part of sealing baffle plate.

1.1.1 RDU-EX

The appearance and ports of the RDU-EX are shown in Figure 1-1.

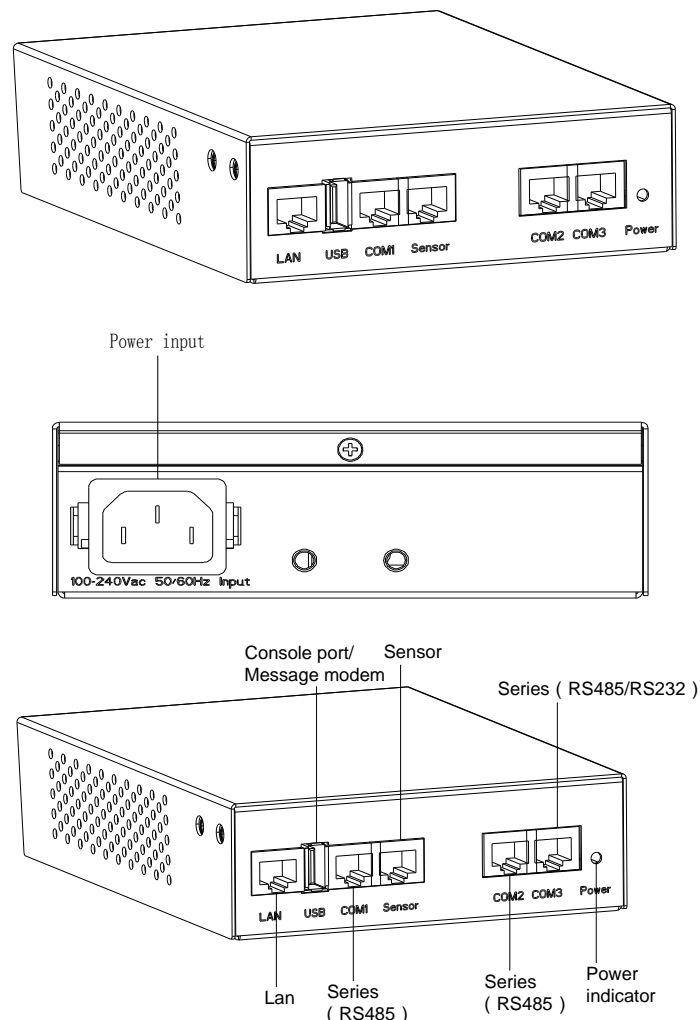


Figure 1-1 Appearance and ports of RDU-EX

Network port

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

Table 1-1 Default configuration parameters of the network port

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

USB port (Factory default)

The RDU-EX supplies one USB-A type socket port for connecting USB Modem of designated model.

COM port

The RDU-EX supplies four independent COM ports (one way to support smart sensors). Their positions are shown in Figure 1-1. See Table 1-2 for the Interface definition.

Table 1-2 Interface definition

-	COM1	Sensor	COM2	COM3
Port type	RS485	RS485	RS485	RS232/RS485
1	NC	12V	NC	NC
2				
3	NC	NC	NC	TXD
4	GND	GND	GND	GND
5				
6	NC	NC	NC	RXD
7	D+	D+	D+	D+
8	D-	D-	D-	D-

Note:

1. The cabling sequence of RJ45 port is 1 to 8 from left to right with the notch facing downward;
2. Check if the connecting network cable is the directly connected network cable;
3. D+ and D- are two kinds of voltage levels of RS485 differential signals;
4. NC: Not Connected

See Table 1-3 for the communication parameters.

Table 1-3 Communication parameters of COM port

Parameter	Baud rate	Bit	Parity	Stop bit
Value	1200bps, 2400bps, 4800bps, 9600bps, 19200bps (optional)	5 ~ 8 bits	Even/Odd/None/Mark/Space	1 ~ 2 bits

Note: The combination mode of 5-bit word size and 2-bit stop bit is not supported

Sensor port

The RDU-EX supplies one sensor port. Their positions are shown in Figure 1-1. See Table 1-4 for parameters of the sensor port.

Table 1-4 Electrical parameters of sensor interface

Silk printing	Definition	Rated output voltage	Rated output current (total)	Max output power (total)	Protection against port
Sensor	Sensor port	+12Vdc	≤0.25A	3W	Support protection against short circuit

This interface uses RS-485 communication mode to connect the Emerson intelligent temperature and humidity sensor, intelligent temperature sensor, intelligent digital extension sensor or the intelligent devices that support RS-485 communication and the communication parameters are given in Table 1-5.

Note

When the sensor interface is connected to a sensor, it cannot connect an intelligent device.
When connecting the intelligent device, the signal cables can only connect D+ and D-.

Table 1-5 Communication parameters of sensor interface

Connected device	Baud rate	Data bit	Even / odd parity bit	Stop bit
Intelligent sensor	9600bps	8 bits	None	1 bit
Intelligent device	1200bps, 2400bps, 4800bps, 9600bps, 19200bps (optional)	5 to 8 bits	Even/Odd/None/Mark/Space	1~2 bits

Note: The combination mode of "5-bit length and 2 stop bits" is not supported

1.1.2 Sealing Baffle Panel (Optional)

The sealing baffle panel can seal the vacant part of the rack (both left and right sides of the plate can be installed). The appearance and installation are illustrated in Figure 1-2.

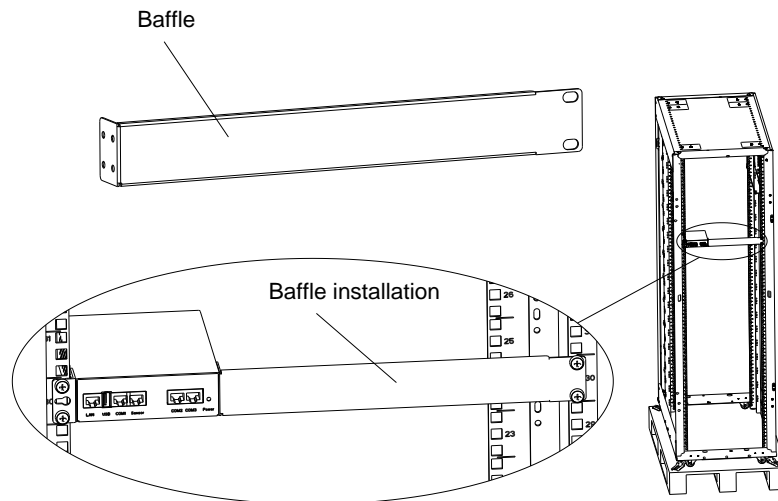


Figure 1-2 Illustration of appearance and installation

1.2 Main Functions

The main functions of RDU-EX are listed in Table 1-6.

Table 1-6 Main functions of RDU-EX

Main function	Description	
Device monitoring	getting and handling the data of different intelligent devices and controlling them through Web interface	
Safe shutdown	Shutdown schedule	Configure the maintenance policy of the UPS, and can periodically reboot or close the supervised UPS
	Sever shutdown	Used together with the NetworkShutdown software. When the UPS has certain critical alarm, the system will notify the sever shutdown to avoid the sever going down
Alarm Management	Current alarm	Displaying alarm in real time, and confirming the current alarm
	History alarm	Querying the history alarm
	Alarm notification	<ol style="list-style-type: none"> 1. Can be customized according to user requirements, that is, alarm notification content can be customized; 2. You can choose the communication mode to receive alarm information of different level from different equipment; 3. The communication mode includes Email, SMS and phone; 4. Email supports SSL function; 5. Supplying alarm test function to test whether or not users have received the alarm notification information; 6. Sending the system running status periodically according to user configuration
Data & History	Device information	Querying the main data of equipment
	History data	Querying the history data
	History log	Querying the log data
	Clear history	Clearing the history data and log data
Device Options	Device management	<ol style="list-style-type: none"> 1. Can add, modify and delete equipment actively, and support adding four pieces of intelligent equipment at most; 2. Can install and uninstall equipment type and support connecting third party

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

1.3 Technical Specifications

1.3.1 Environment Specifications

See Table 1-7 for the environment specifications of RDU-EX.

Table 1-7 Environment conditions

Item	Requirement
Application location	Usually in data center or computer room, with air conditioner
Working temperature	-10°C ~ +55°C
Relative humidity	5%RH ~ 95%RH, no condensing
Working environment	Dust: compliant with the indoor requirements of GR-63. No corrosive gas, flammable gas, oily mist, steam, water drops or salt
Air pressure	70kpa ~ 106kpa
Storage temperature	-40°C ~ +70°C
Cooling	Natural cooling
Power distribution network	TT/TN
Protection level	IP20

1.3.2 Mechanical Specifications

See Table 1-8 for the mechanical specifications of RDU-EX.

Table 1-8 Mechanical specifications

External model	Measures	Values	Tolerance
RDU-SICP	Height	42mm	< ±0.5 mm
	Width	130mm	< ±1 mm
	Depth	170mm	< ±1 mm
	Weight	< 1kg	
Sealing baffle panel	Height	42mm	< ±0.5 mm
	Width	31mm	< ±1 mm
	Depth	331mm	< ±1 mm
	Weight	< 0.5kg	

1.3.3 Performance Specifications

The Northern interface of RDU-EX is shown in Table 1-9.

Table 1-9 Northern Interface

Device type	Connection mode	Description
RDU-M	Network	Private protocol
RDU-A G2	Network	SNMP protocol
Third party monitoring	Network	SNMP protocol

The Southern interface of RDU-EX is shown in Table 1-10.

Table 1-10 Southern Interface

Device type	Max number	Description
Intelligent device	4	COM1, Sensor, COM2 and COM3 can connect intelligent device, and up to 2 devices can be connected to each interface and totally 4 devices can be connected. (When the sensor interface is connected to a sensor, it cannot connect an intelligent device. The other interfaces can connect the intelligent device normally)
Sensor	4+2	The Sensor interface can connect sensors and can connect up to 4 temperature and humidity sensors and 2 extended 4DI (maximally 19 measure points); The addresses of temperature and humidity sensors: 20, 21, 22 and 23; The addresses of 4DI sensors: F0, F1.
Note: The total length of the cable connected to the interface is less than 100m.		

1.3.4 Product Certification

RDU-EX complies with CE directives through self-claim mode.

Chapter 2 Hardware Installation

This chapter expounds the hardware installation of the RDU-EX.

2.1 Installation Preparation

2.1.1 Notes

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

- RDU-EX has a strong magnetic iron on its bottom surface, take care when placing or installing it.
- Always cut off the power before performing any installation operation on the RDU-EX
- Ensure that the external devices are connected to the correct ports of the RDU-EX
- Wear an ESD-proof glove during installation
- Arrange the wires properly, and do not put any heavy objects on the wires or stamp the wires

2.1.2 Ambient Requirements

Operation environment

The RDU-EX must be installed indoor. Refer to Table 1-7 for specific requirement.

ESD-proof

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

- Keep proper temperature and humidity in the data center (see Table 1-7).
- Wear the ESD-proof gloves and work clothes before contacting with the PCB. If there are not ESD-proof gloves and work clothes, wash hands with water and dry them.

Immunity

Take the following measures for immunity:

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

2.2 Installing RDU-EX

2.2.1 Hanging Mode Installation

RDU-EX can be hanged on the flat surfaces such as cable management plate of the cabinet or wall. The bracket installation mode and the installation effect of cable management plate are shown in Figure 2-1.

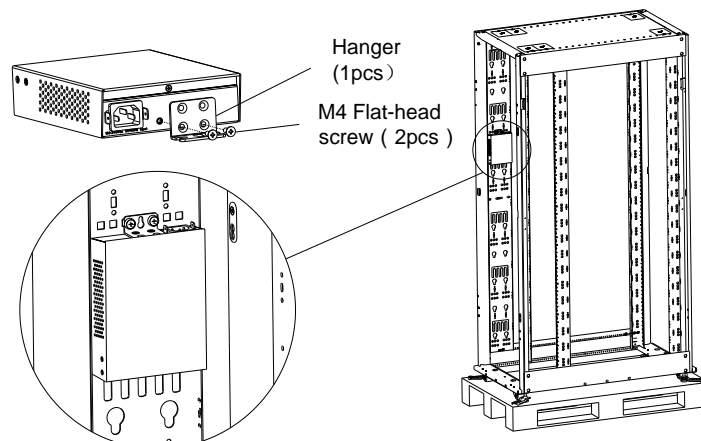


Figure 2-1 Installation bracket and hanging mode installation effect

2.2.2 Installation in Rack

1. Confirm that the cabinet well fixed to floor, and no obstacle is inside or outside the cabinet.
2. Use M4 screws (from accessories) to fix the brackets (usually the multi-purpose parts, can be used both for hanging mode installation and installation in rack) on the sides of the RDU-EX box (on either left or right sides), as shown in Figure 2-2.
3. Use M6 floating nuts to fasten the RDU-EX to the cabinet through the brackets on two sides.

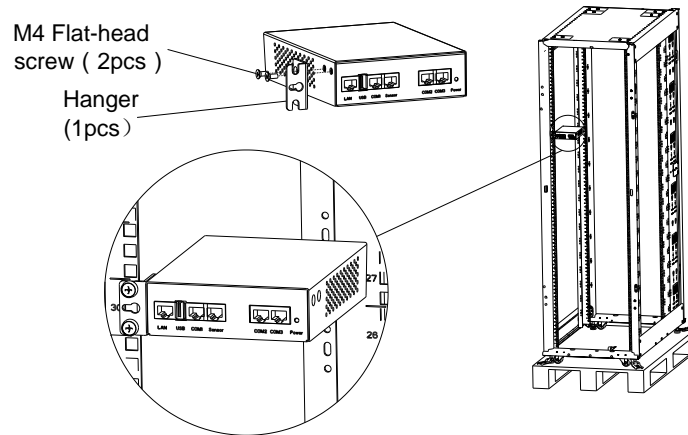


Figure 2-2 Installation bracket and rack-installation effect

Note

1. Use can use baffle panels (optional parts) to cover the vacant part in the rack, both left and right sides of the plate can be installed;
2. Connect the baffle panel and RDU-EX according to Figure 2-3, and then install the unit in a rack.

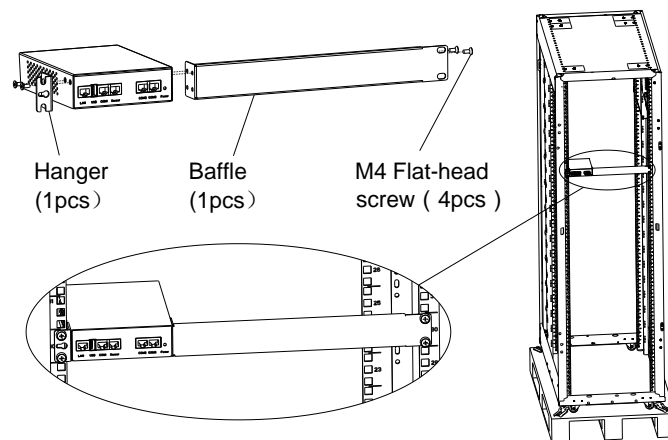


Figure 2-3 Illustrations for installation bracket and baffle plate and installation effect

2.2.3 Installation Through Magnetic Iron

The bottom surface of RDU-EX has three strong magnetic irons, as shown in Figure 2-4. The unit can be attached to the flat surface of the cabinet by magnetic forces.

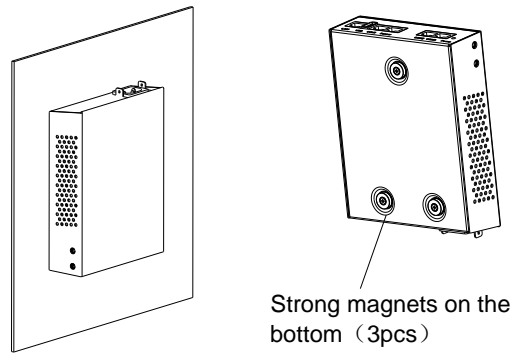


Figure 2-4 Magnetic irons on the bottom surface of RDU-EX and installation effect

 **Note**

The magnetic iron has strong magnetic forces, so be sure to take care to avoid hurting your hand during installation process!

2.3 Electrical Connections

 **Note**

Input voltage of RDU-EX: 100Vac~240Vac, frequency: 50/60Hz.

Connect the power cables according to Figure 2-5, and connect the breakaway-prevention clip. After completing the connection, connect the other end of the cable to the power supply.

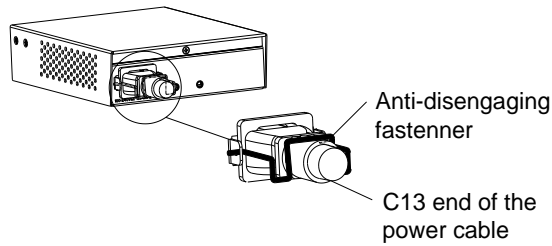


Figure 2-5 Illustration for breakaway-prevention clip

Chapter 3 Web Page Of RDU-EX

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

3.1 Login Preparation

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

3.1.1 Checking IP Address Connectivity

Before logging in RDU-EX through Web, please first confirm the IP address of RDU-EX, and test its connectivity. Refer to Q5 in 4.2 FAQ for the test method.

3.1.2 Checking Browser Version

For the best user experience, the recommended browser is Internet Explorer, its version includes: **IE8, IE9, IE10 or IE11**.

3.1.3 Checking Browser Setting

Checking IE General setting

Double-click the icon of IE to run the software, click the menus of **Tools -> Internet Options**, then click the **Settings** button on the **General** tab, and select **Every time I visit the webpage** for **Check for newer versions of stored pages**, as shown in Figure 3-1.

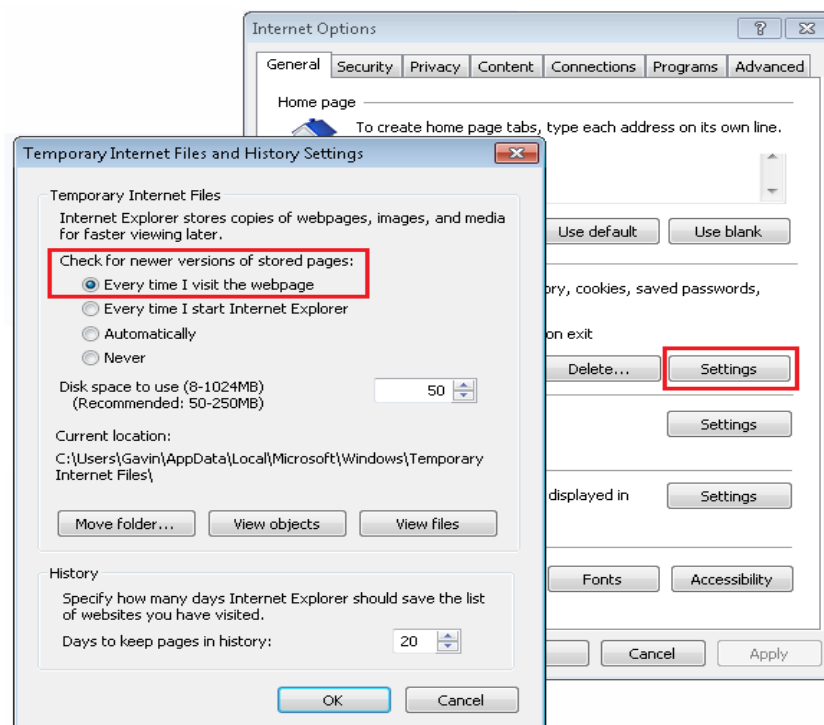


Figure 3-1 General setting

Checking IE proxy setting

1. Double-click the icon of IE to run the software, click the menus of **Tools -> Internet Options** and then choose the **Connections** tab to pop up the window shown in Figure 3-2.

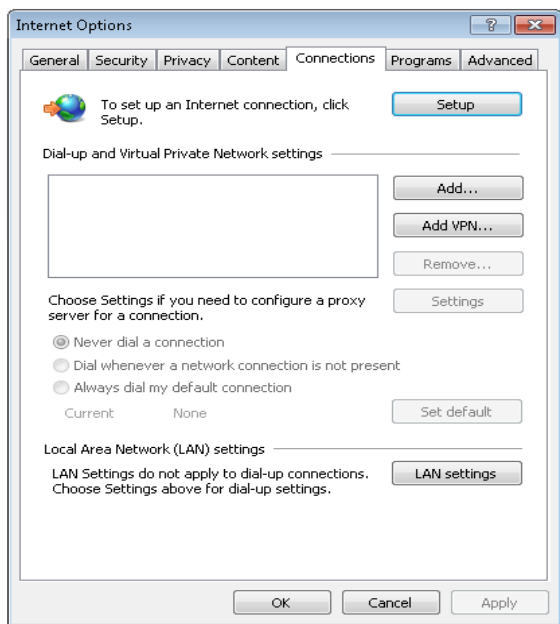


Figure 3-2 Choosing the Connections tab

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

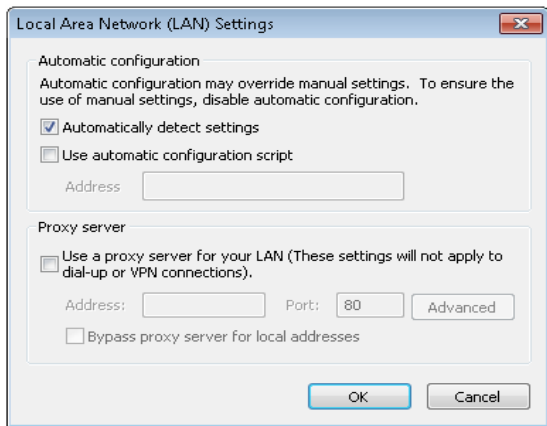


Figure 3-3 LAN setting

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

Checking IE security setting

1. Double-click the icon of IE to run the software, click the menus of **Tools -> Internet Options** and then choose the **Security** tab to pop up the window shown in Figure 3-4.

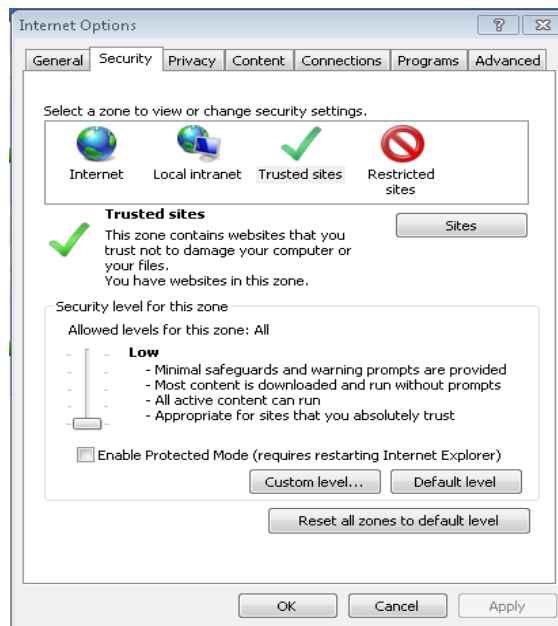


Figure 3-4 Security setting 1

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

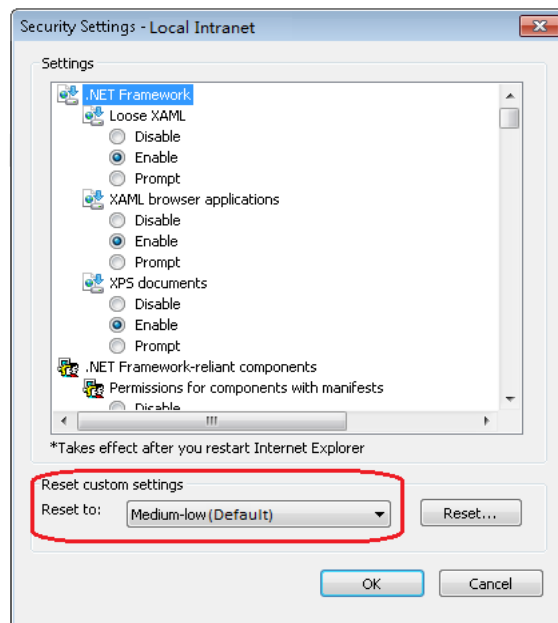


Figure 3-5 Security setting 2

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

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

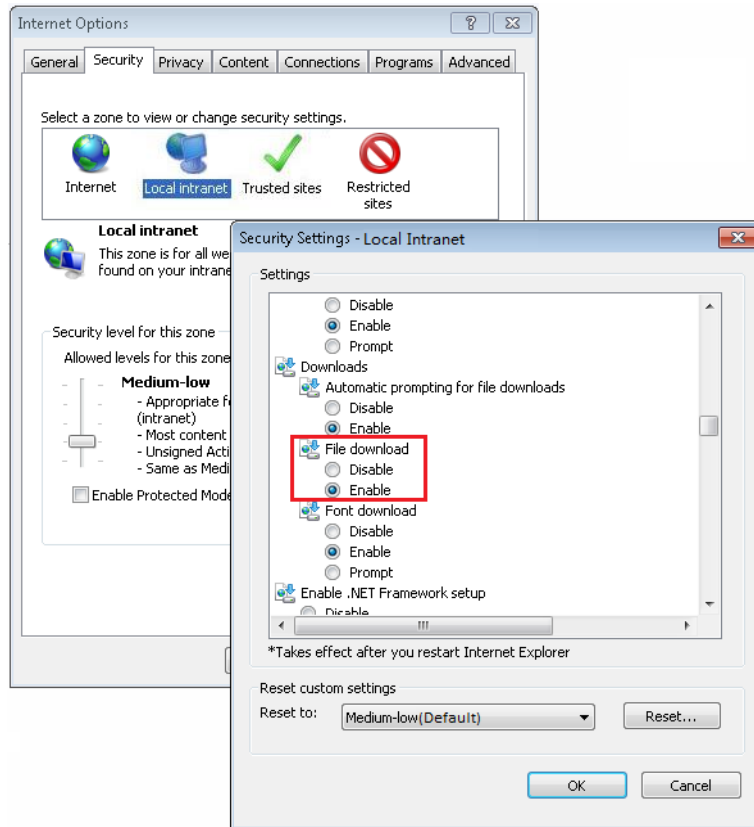


Figure 3-6 Enabling file download

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

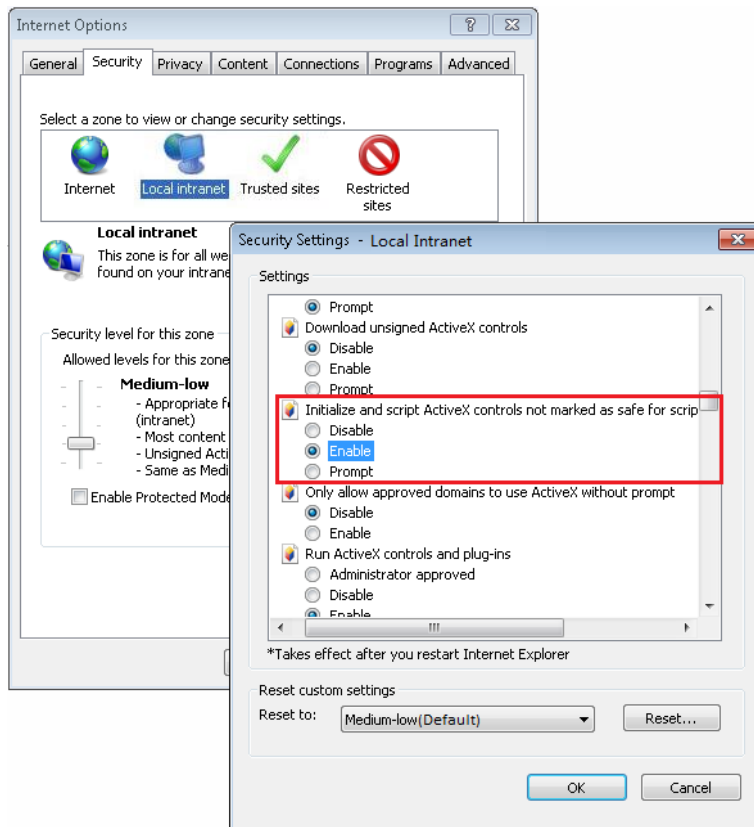


Figure 3-7 Enabling ActiveX controls

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

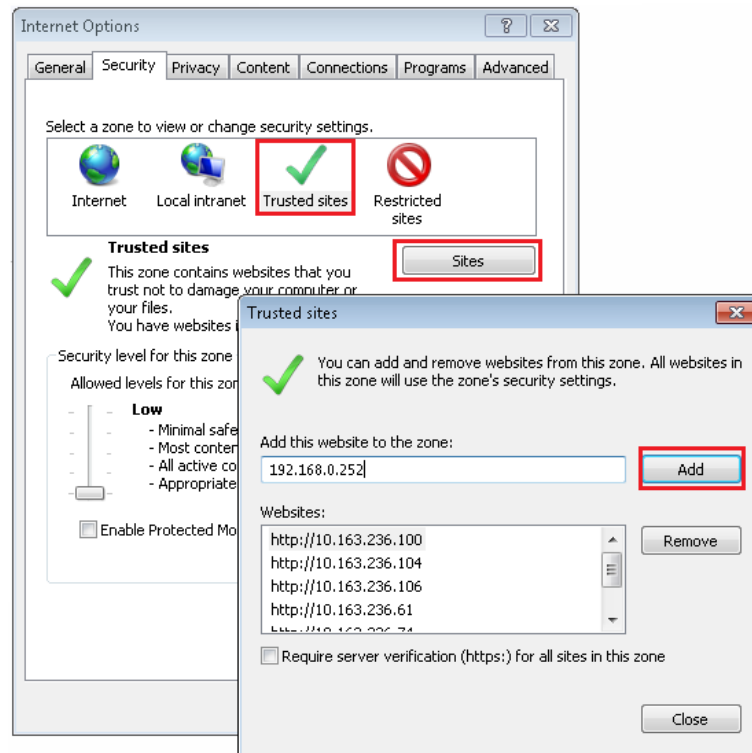


Figure 3-8 Adding trusted sites

3.2 Log In RDU-EX

3.2.1 Login Page





1. Open the IE browser, and enter the IP address of the RDU-EX in the address box, the login page will appear, as shown in Figure 3-9. If the login page does not appear, refer to Q5 in 4.2 FAQ.



Crystal blue

Ocean blue

Figure 3-9 Login page of RDU-EX

2. On the login page, select a preferable theme by clicking  or :  means crystal blue;  means ocean blue, as shown in Figure 3-9.
3. Type the username and password (default username: 'admin', default password: 'emerson'), and click the **Login** button, the homepage will appear, as shown in Figure 3-11.

3.2.2 Forgetting Password

If you forget the password, click the **Forget Password** button on the login page, and the screen will display the page of getting password, as shown in Figure 3-10.

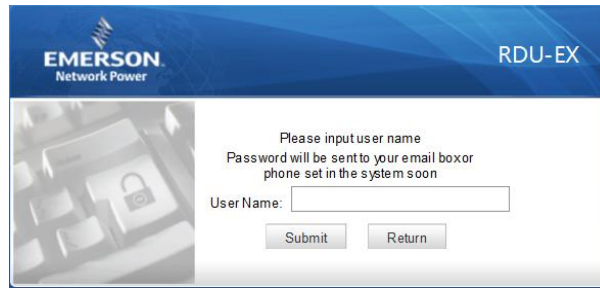


Figure 3-10 Page of getting password

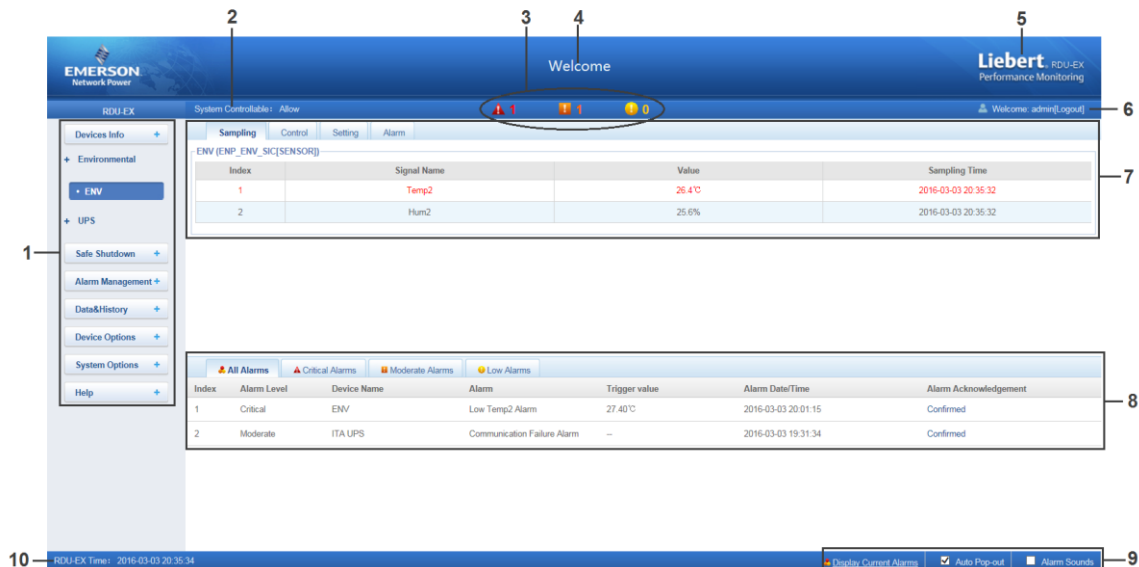
Type your username, and click the **Submit** button, your password will be sent to the email box or phone which you have configured before. Clicking the **Return** button cancels the operation.

Note

1. Only when you have correctly configured the email and SMS parameters on the **SMS and Email Server Configuration page** can you receive the password sent by the system. Refer to Alarm Notification in 3.4.3 *Alarm Management* for detailed setting method.
2. The gotten password is a random new password generated by the system; please modify the password after logging in the system successfully.

3.3 Homepage Of RDU-EX

After successful login, the homepage of RDU-EX is displayed by default, as shown in Figure 3-11.



- | | | |
|---------------------------|------------------------------------|--|
| 1. Menu item | 2. Controllable status | 3. Current number of every level alarm |
| 4. System title | 5. Logo | 6. [User] Logout |
| 7. Function display area | 8. Real-time alarm displaying list | 9. Alarm pop-out setting |
| 10. Time calibrating link | | |

Figure 3-11 Homepage of RDU-EX

3.3.1 Time Calibrating Link

The lower left part displays the system time of RDU-EX. Clicking the **RDU-EX time** will jump to the time calibrating page. For detailed operation, refer to *Date/Time Setting* in 3.4.6 *System Options*.

3.3.2 Clearing Time-Out

When there is no operation on the page within 15min, the page will become uncontrollable, as shown in Figure 3-12.



Figure 3-12 Controllable status

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

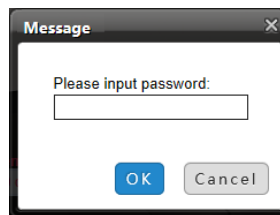


Figure 3-13 Password verification

3.3.3 Logout

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

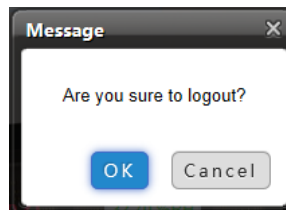


Figure 3-14 Logout

3.3.4 Real-Time Alarm Pop-Up Setting

The real-time alarm displaying list is contracted on the bottom of the page by default. You can perform the following operation by referring to Figure 3-11:

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

3.4 Menu Items

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

3.4.1 Device Information

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

Note

ENV in **Device Info** is a dummy device, which indicates all temperature sensors and temperature & humidity sensors connected to RDU-EX.

Sampling

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

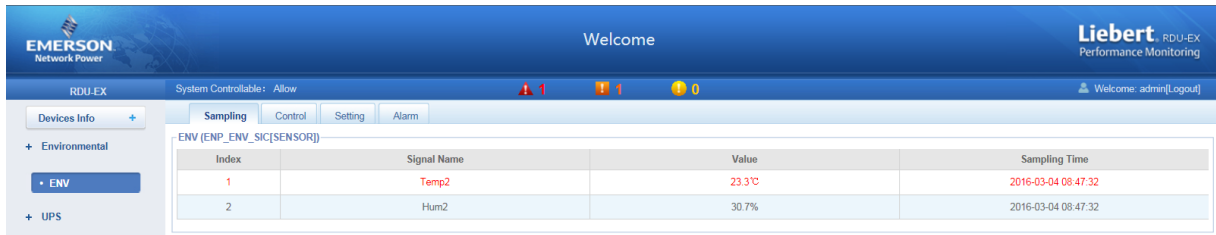


Figure 3-15 Sampling signals

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

Control

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

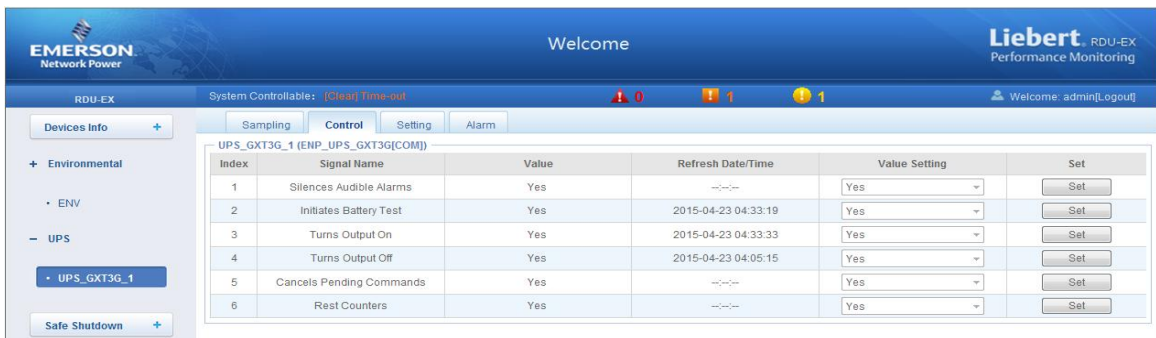


Figure 3-16 Control signals

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

Setting

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

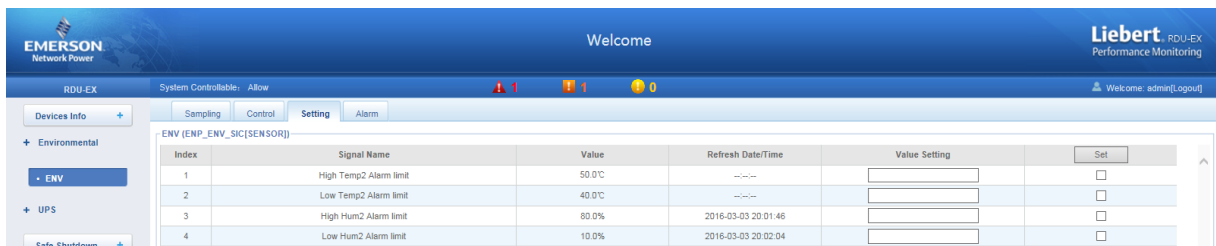


Figure 3-17 Setting signals

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

Alarm

Clicking the **Alarm** tab can enter the alarm page, which displays alarm signals of selected device, as shown in Figure 3-18.

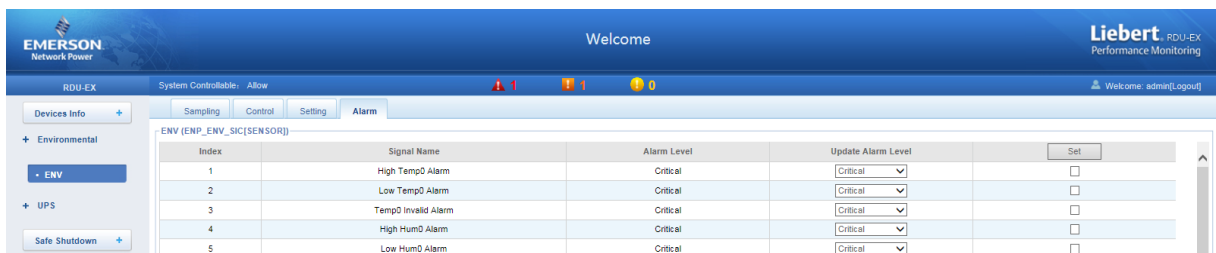


Figure 3-18 Alarm signals

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

3.4.2 Safe Shutdown

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

Shutdown Schedule

Click **Shutdown Schedule** under the **Safe Shutdown** menu, the page shown in Figure 3-19 pops up.

Figure 3-19 Shutdown Schedule page

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

As shown in Figure 3-19, type a task name of schedule shutdown in the field of **Task Name**, select a **Target Equipment**, select whether to enable the task in the **Status** field, select **ShutDown Mode** and **Open Mode**, and then add **ShutDown Time** according to the corresponding prompt, the page is shown in Figure 3-20.

Figure 3-20 Schedule shutdown task list

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

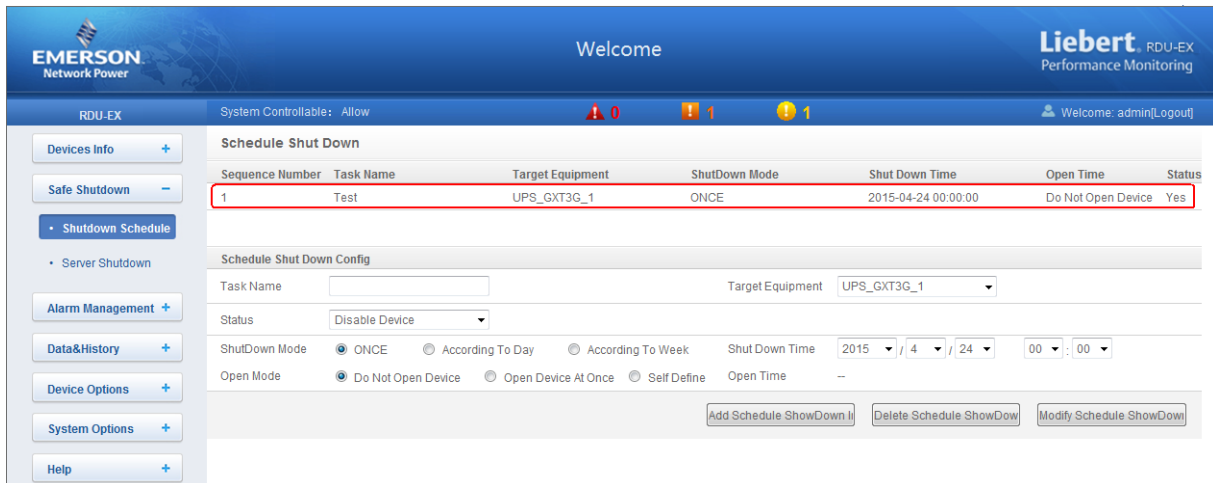


Figure 3-21 Schedule shutdown task list

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

1. When the **Open Mode** is set to 'Do Not Open Device' or 'Open Device At Once', the **Open Time** cannot be set, and it is displayed as '--';
2. The format of **ShutDown Time** changes with different options of **ShutDown Mode** automatically, as shown in Figure 3-22.

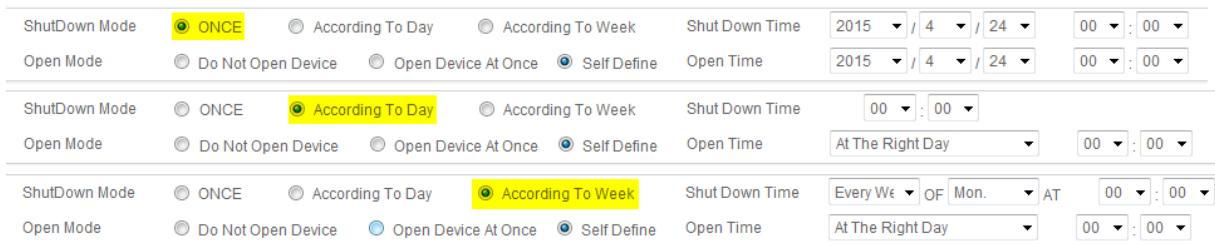


Figure 3-22 Format of shutdown time

Note

1. The RDU-EX can support up to ten shutdown tasks.
2. Only when 'Enable Device' is set for Status can the schedule shutdown task be enabled.

Server Shutdown

Click **Server Shutdown** under the **Safe Shutdown** menu, the Server Shutdown page will pop up, as shown in Figure 3-23.

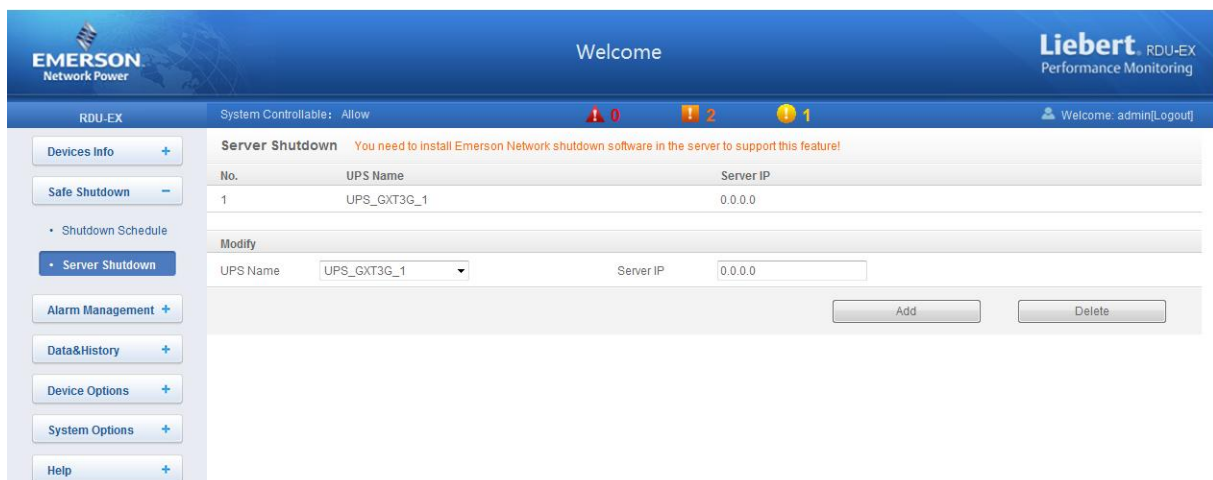


Figure 3-23 Server Shutdown page

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

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

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

Note

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

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

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

3.4.3 Alarm Management

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

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

Current Alarms

Click **Current Alarms** under the **Alarm Management** menu, or refer to 3.3.4 *Real-Time Alarm Pop-Up Setting*, the current alarm list will pop up, as shown in Figure 3-24.

Index	Alarm Level	Device Name	Alarm	Trigger value	Alarm Date/Time	Alarm Acknowledgement
1	Critical	ENV	Low Temp2 Alarm	27.40°C	2016-03-03 20:01:15	Confirmed
2	Moderate	ITA UPS	Communication Failure Alarm	--	2016-03-03 19:31:34	Confirmed

Figure 3-24 Current alarms

1. You can click the tabs above the alarm list to view current alarms according to alarm levels.
2. Click the **Acknowledge** button to confirm the alarm. After conformation, no alarm notification about the conformed alarm will be sent.
3. When the mouse is located on the **Confirmed** link, the alarm confirming information will be hovered; when you move the mouse, the information will disappear, as shown in Figure 3-25.

Index	Alarm Level	Device Name	Alarm	Trigger value	Alarm Date/Time	Alarm Acknowledgement
1	Critical	ENV	Low Temp2 Alarm	27.40°C	2016-03-03 20:01:15	Confirmed
2	Moderate	ITA UPS	Communication Failure Alarm	--	2016-03-03 19:31:34	Confirmed

Relevant Device: ITA UPS
 Signal Name: Communication Failure Alarm
 Alarm Level: Moderate
 Sampling Time: 2016-03-03 19:31:34
 Confirmed by: admin
 Confirmed on Date/Time: 2016-03-03 20:02:24

Figure 3-25 Confirming information

History Alarm

Click **History Alarm** under the **Alarm Management** menu to look over historical alarm records. Select a device (for instance, 'All Devices') and set the start time and end time (for instance, from 2016-03-04 00:00:00 to 2016-03-04 23:59:59). Then click the **Query** button, all alarm records generated between the start time and end time will be listed, including: Index, Device Name, Signal Name, Alarm Level, Trigger valve, Start Date/Time, Confirmed by, Confirmed on Date/Time and End Date/Time, as shown in Figure 3-26.

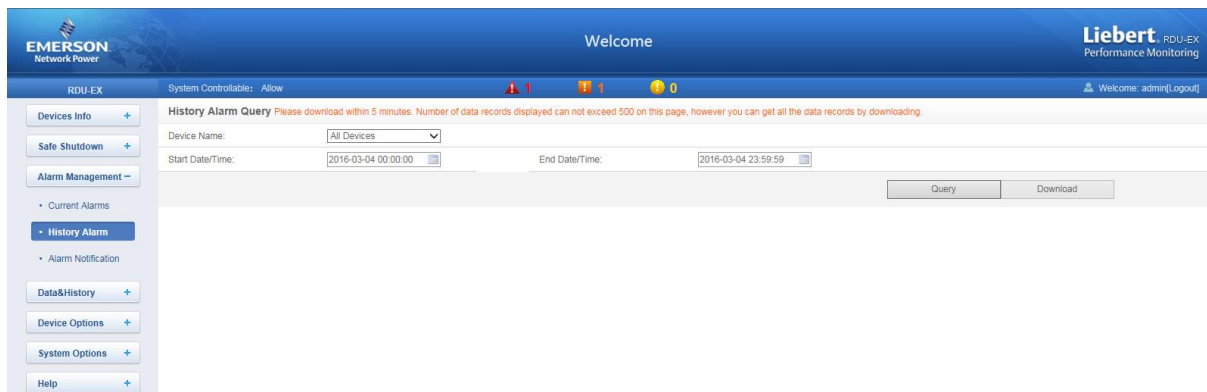


Figure 3-26 History alarm query

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

Alarm Notification

1. User Alarm Notification Configuration

Click the **Alarm Notification** under the **Alarm Management** menu, the page shown in Figure 3-27 pops up. You can choose the notification method to receive notification of chosen level alarm from chosen equipment, meanwhile, you can also choose the language of alarm notification information and customize the alarm content (including Equip name, Alarm description, Alarm TIME and Alarm state by default).

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

Note

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

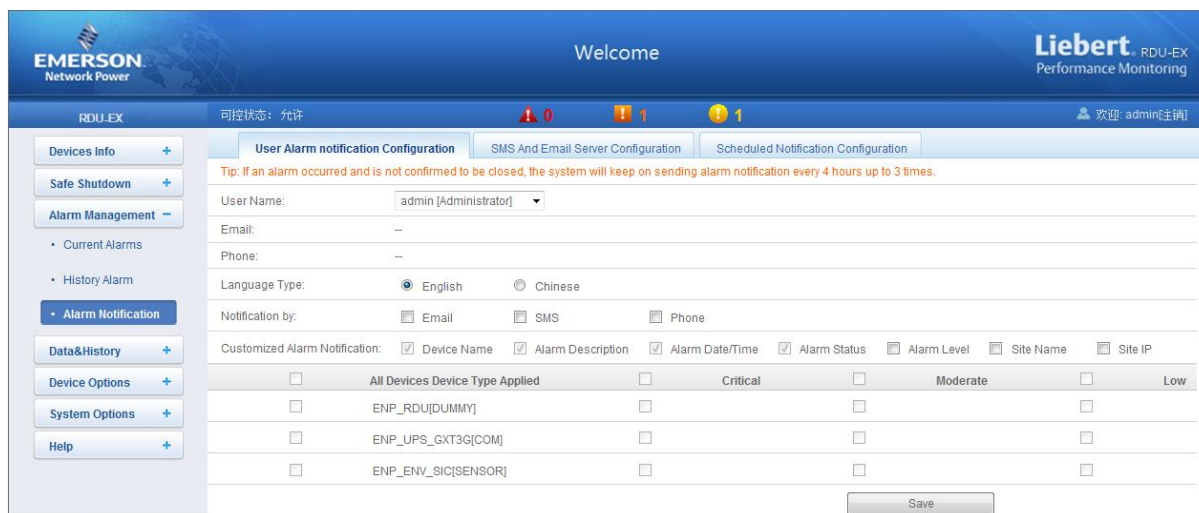


Figure 3-27 User alarm notification configuration

2. SMS And Email Server Configuration

Click the **Alarm Notification** under the **Alarm Management** menu, and then click the **SMS And Email Server Configuration** tab, the page shown in Figure 3-28 pops up.

The screenshot displays the 'SMS And Email Server Configuration' page in the RDU-EX web interface. The page is divided into two main sections: 'SMS Modem Configuration' and 'Email Server Configuration'. The 'SMS Modem Configuration' section includes fields for 'Port Type' (set to USB), 'SMS Modem' (set to Not Configured), and 'Parameter' (set to 460800,n,8,1). The 'Email Server Configuration' section includes fields for 'Email Server' (142.100.16.45), 'Server Port' (25), 'Email User' (RDU-A), 'Email Password' (masked with asterisks), and 'Sender Email Address' (RDU-A@emersonnetwork.com.cn). There are 'Save Configuration', 'Default', and 'Save' buttons at the bottom of the form.

Figure 3-28 SMS/Email server configuration

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

●SMS Modem Configuration

- 1) Connect an SMS Modem through USB port according to need, and choose **Port Type**, the page will display **Parameter** automatically;
- 2) Choose **SMS Modem** (GSM) according to the SMS Modem type;
- 3) Set the communication parameter of the SMS Modem;
- 4) Click the **Save Configuration** button to save the configuration of current user's SMS Modem.

●Email Server Configuration

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

Note

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

3. Scheduled Notification Configuration

Click the **Alarm Notification** under the **Alarm Management** menu, and then click the **Scheduled Notification Configuration** tab, the page shown in Figure 3-29 pops up.

The screenshot displays the 'Scheduled Notification Configuration' page in the RDU-EX web interface. The page includes fields for 'User Name' (admin [Administrator]), 'Phone', 'Email', 'Notification by' (Email and SMS), 'Language Type' (English and Chinese), 'Notification Enabled Period' (Start Time: 8:00, End Time: 20:00), 'Notification Scheduled Cycle' (Week, Day, hour), 'Interval Of Notification' (1 Day), and 'Send Time Setting' (11:00). There is a 'Save' button at the bottom right of the form.

Figure 3-29 Scheduled notification configuration

Note

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

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

3.4.4 Data & History

The **Data & History** menu supplies query service of all types of historical data and logs for the user. On the RDU-EX homepage, click **Data & History** in the left part, four submenus appear, including: **Device Information**, **History Data**, **History Log** and **Clear History**.

Device Information

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

1. Device Information List

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



Figure 3-30 Device information list

2. Export SNMP MIB

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

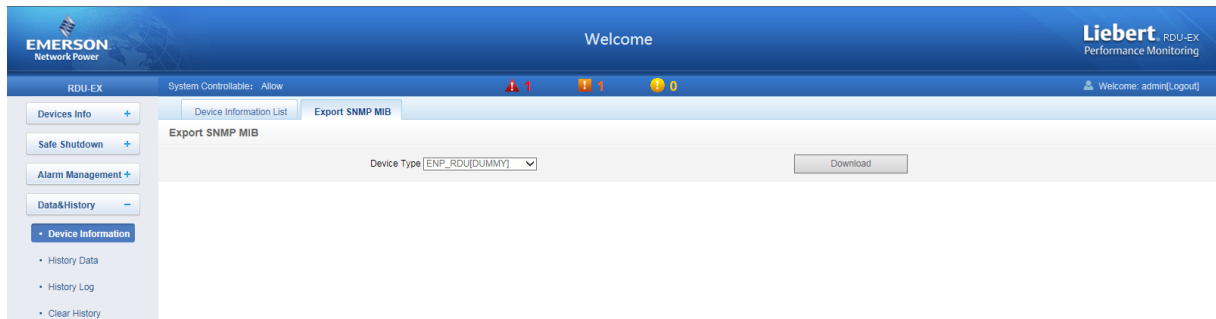


Figure 3-31 Export SNMP MIB

History Data

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

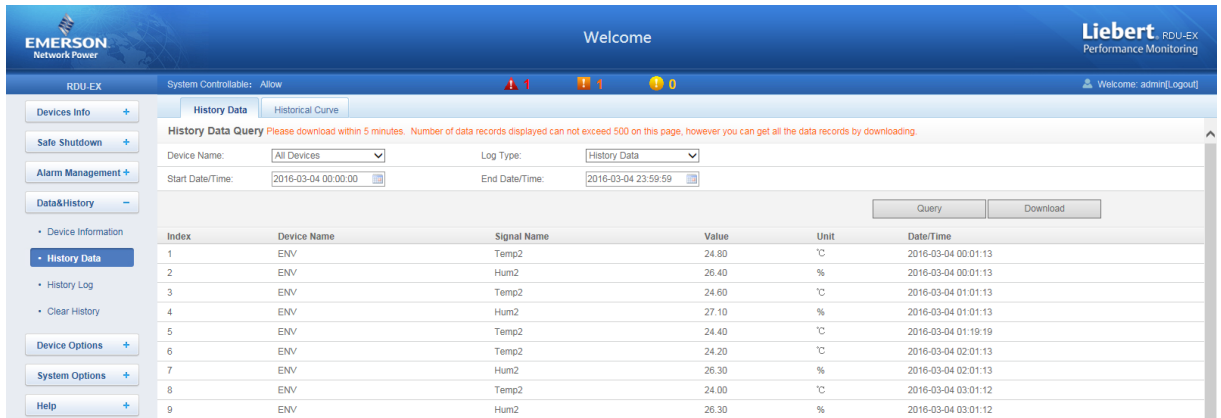


Figure 3-32 History data

1. History Data

As shown in Figure 3-32, choose a device (for instance, 'All Devices') and the log type (for instance, 'History Data'), and set the start time and the end time (for instance, from 2016-03-04 00:00:00 to 2016-03-04 23:59:59). Then click the **Query** button, all the history data during the time will be listed, click the **Download** button to download the query result.

2. Historical Curve

As shown in Figure 3-33, choose a device (for instance, 'ENV') and the query type (for instance, 'Temp2'), and set the start time and the end time (for instance, from 2016-03-04 00:00:00 to 2016-03-04 23:59:59). Then click the **Show Curve** button, if history data are queried, a historical curve of the signal will be shown.

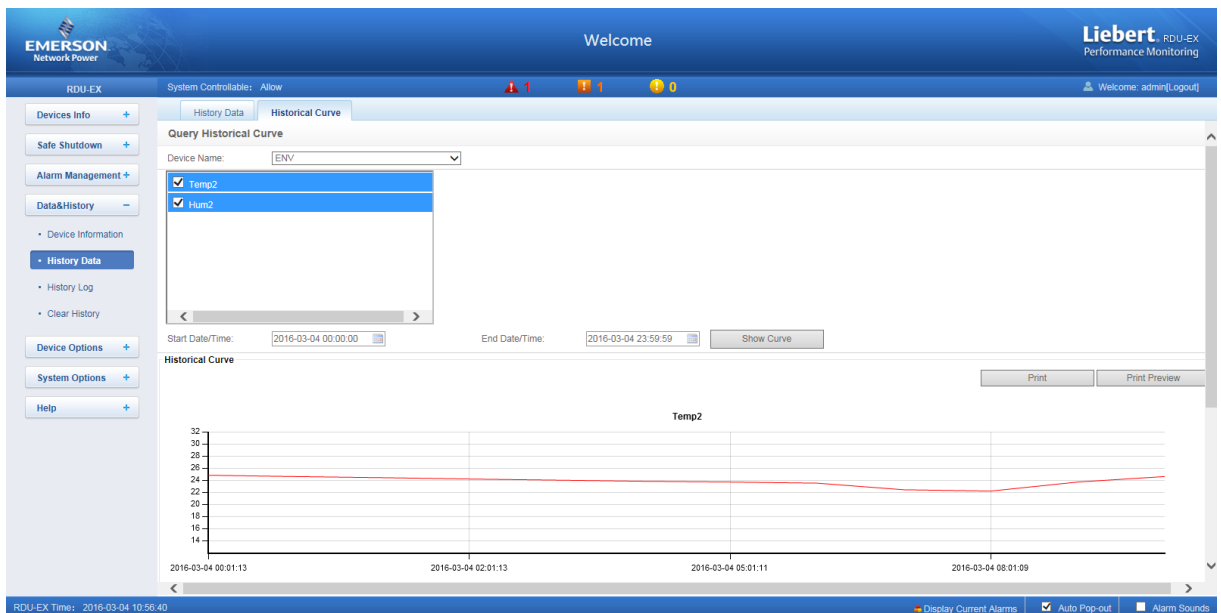


Figure 3-33 Historical curve

History Log

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

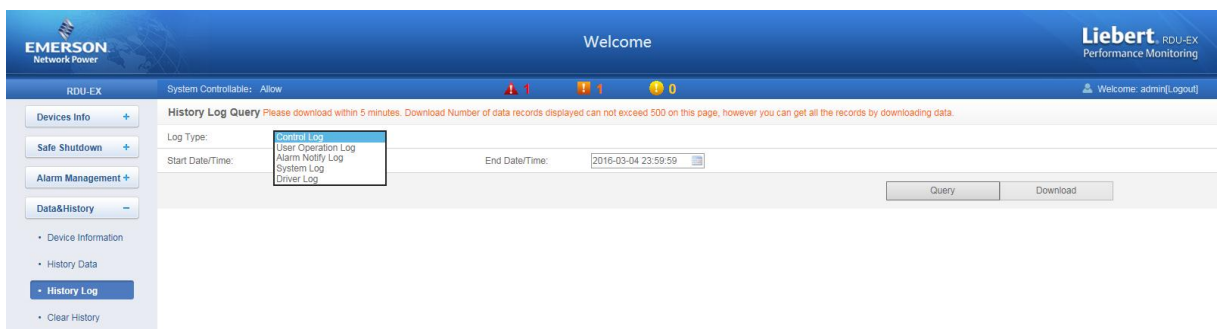


Figure 3-34 History log

On the page shown in Figure 3-34, choose the log type (for instance, 'Control Log') and set the start time and the end time (for instance, from 2016-03-04 00:00:00 to 2016-03-04 23:59:59). Then click the **Query** button, all control logs during the time will be listed, click the **Download** button to download the query result.

Note

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

Clear History

Click the **Clear History** submenu under the **Data & History** menu, the page shown in Figure 3-35 pops up.

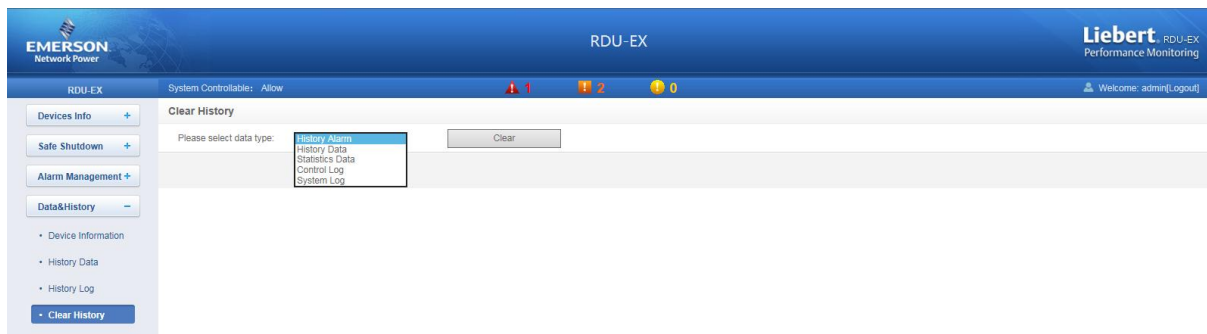


Figure 3-35 Clear history

As shown in Figure 3-35, you can choose 'History Alarm' and click the **Clear** button to clear all the history alarm. In the same way, you can clear any other gettable data in the drop-down box.

3.4.5 Device Options

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

Device Management

1. Add/Modify/Delete Device

Click the **Device Management** under the **Device Options** menu, the page shown in Figure 3-36 pops up.

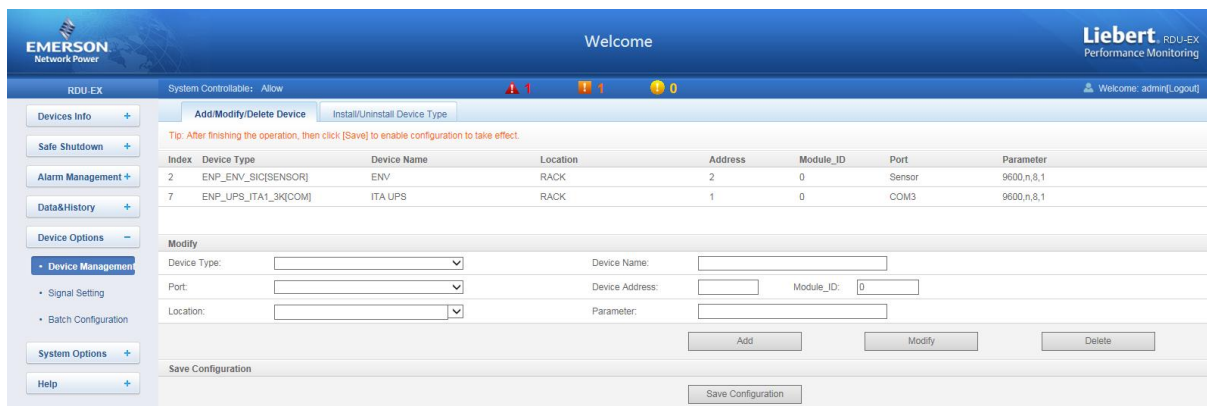


Figure 3-36 Add/modify/delete device

As shown in Figure 3-36, you can add/modify/delete a new device, the procedures are as follows:

● Adding a new device

- 1) Choose the device type in the **Device Type** textbox;
- 2) Type the device name in the **Device Name** textbox, or use the default device name;
- 3) After the device type is chosen, the drop-down box of **Port** will list the default port number(s) of the device type automatically; if the device type is not chosen, the port number cannot be chosen;
- 4) Type the device address, which must be numbers from 1 to xx, in the **Device Address** textbox. The device addresses under the same port number must be different; for some device types, you need not type the device address, at this point, the **Device Address** textbox turn gray and cannot be edited. When one kind of device has many

models, you need to type the model ID, which must be numbers from 1 to xx. The model IDs under one kind of device must be different;

5) Choose or type the device location;

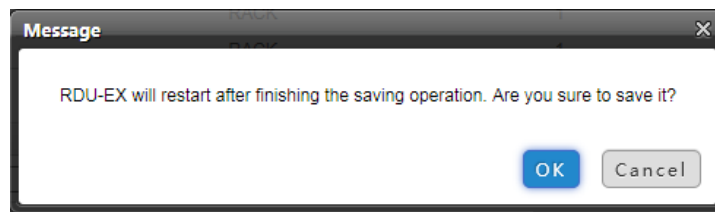
6) Type the communication parameter in the **Parameter** textbox. In the event that the device type is certain, the communication parameter prompt information will appear in the **Parameter** textbox, including the communication parameter format and default communication parameter of the equip type;

7) Click the **Add** button, the page shown in *Prompt information 1* in Figure 3-37 pops up, at the same time, a piece of new device information will be added in the device list;

8) Click the **Save Configuration** button, the page shown in *Prompt information 2* in Figure 3-37 pops up;

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

Prompt information 1



Prompt information 2

Figure 3-37 Prompt information

If clicking the **Cancel** button, the added equipment fails; if clicking **OK**, the dialog box of Security authentication pops up, as shown in Figure 3-13.

9) Type the login password of current user, and click **OK**. The reboot page pops up, as shown in Figure 3-38;

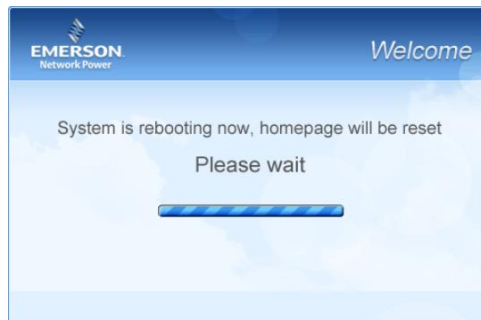



Figure 3-38 Reboot page

After the system reboots, adding a device becomes effective.

10) Log in the RDU-EX webpage again and the added device will appear in the list on device management page.

 **Note**


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

●Deleting a device

1) Choose the device which needs to be deleted in the device list;

2) Click the **Delete** button to delete the device;

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

 **Note**

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

●Modifying a device

1) Choose the device which needs to be modified in the device list;

2) Modify the device information;

3) Click the **Modify** button to make the setting effective;

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

After adding, modifying or deleting procedures, if you leave the **Add/Modify/Delete Device** page without clicking the **Save Configuration** button to make the settings effective, the prompt information will pop up to remind you of saving the configuration, as shown in Figure 3-39.

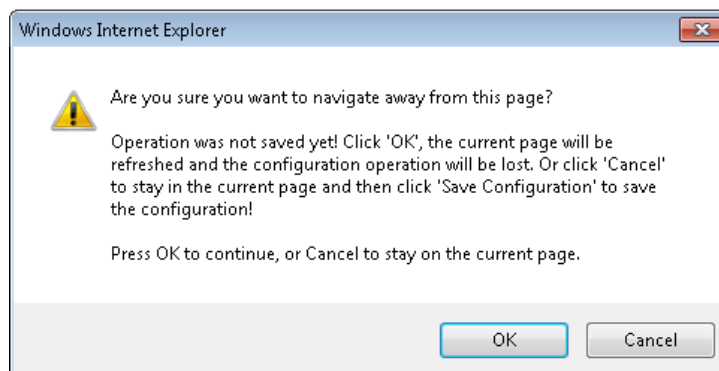


Figure 3-39 Prompt information 3

Note

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

2. Install/Uninstall Device Type

Click the **Device Management** under the **Device Options** menu, and then click the **Install/Uninstall Device Type** tab, the page shown in Figure 3-40 pops up.

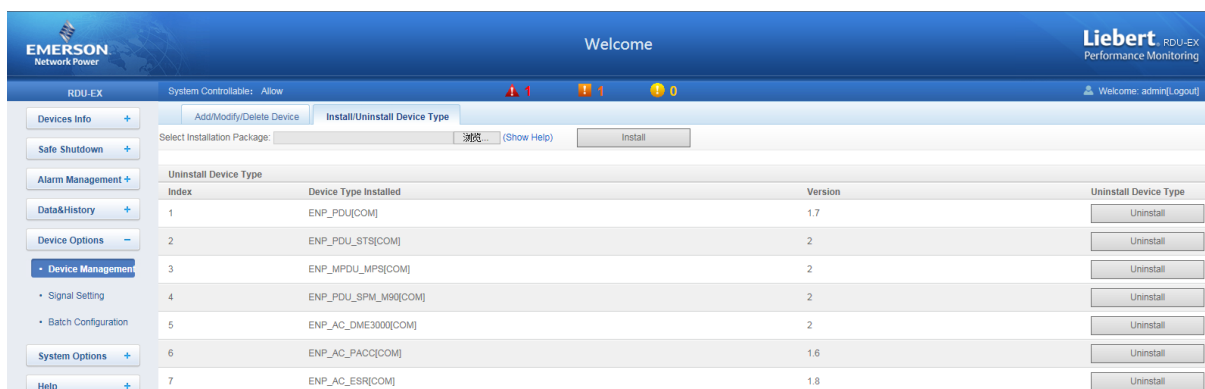


Figure 3-40 Install/Uninstall Device Type

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

Note

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

The page displays the installed device type information in the lower right part. Click the **Uninstall** button, the confirming dialog box pops up, as shown in Figure 3-41.

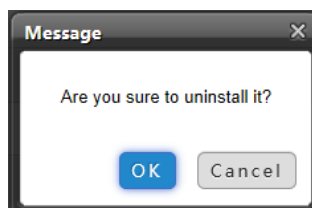


Figure 3-41 Confirming dialog box

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

Note

1. While installing device type, if the device type exists and the device driver has a higher version than the driver to be added, it cannot be installed repeatedly;
2. If the installation pack has no version information, or the version information does not match the software version, the device type cannot be installed.
3. If some device uses the device type, the **Uninstall** button becomes gray, displaying **Using**, and the device type cannot be uninstalled.

Signal Setting

Click the **Signal Setting** under the **Device Options** menu, the page shown in Figure 3-42 pops up.

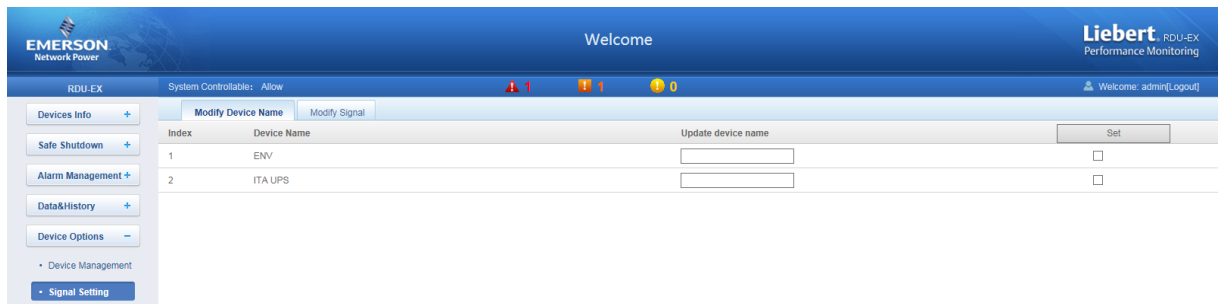


Figure 3-42 Modify device name

On the page shown in Figure 3-42, you can modify the device name. Type the new device name and click the **Set** button to make all setting effective.

Note

The characters of device name and signal name can be English letters, digits, space and underline. If other characters are typed, the prompt box shown in Figure 3-43 will pop up.

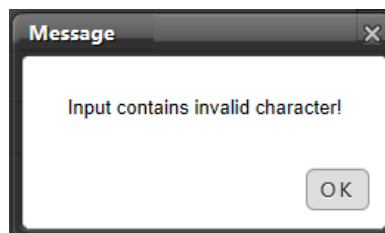


Figure 3-43 Prompt box of invalid characters

Batch Configuration

Click the **Batch Configuration** under the **Device Options** menu, the page shown in Figure 3-44 pops up.

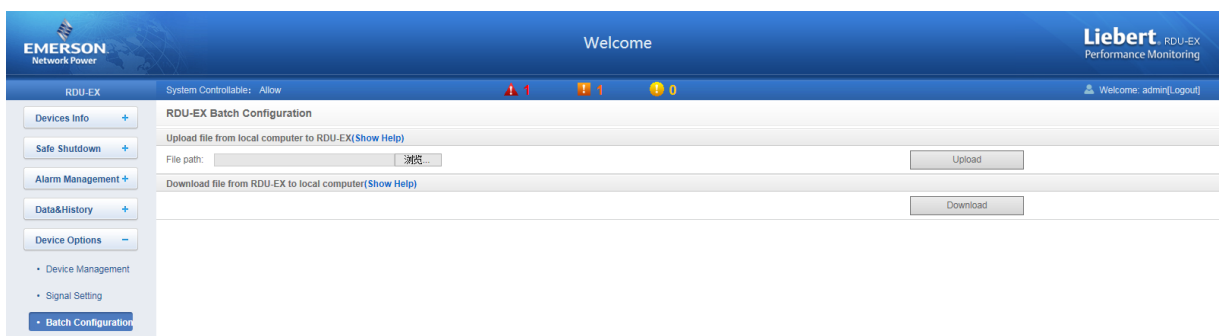


Figure 3-44 Batch configuration

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

Note

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

3.4.6 System Options

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

Monitoring Unit

The **Monitoring Unit** is used to set the signals of RDU-EX system, including **Sampling, Setting** and **Alarm** signals, the page is shown in Figure 3-45.

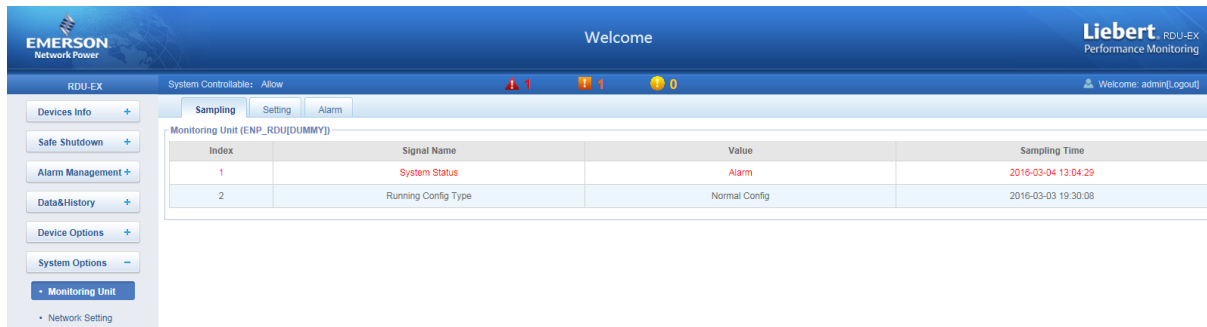


Figure 3-45 Monitoring unit (Sampling)

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

Note

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

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

Network Setting

1. IP Setting

Click the **Network Setting** under the **System Options** menu, the page shown in Figure 3-46 pops up.

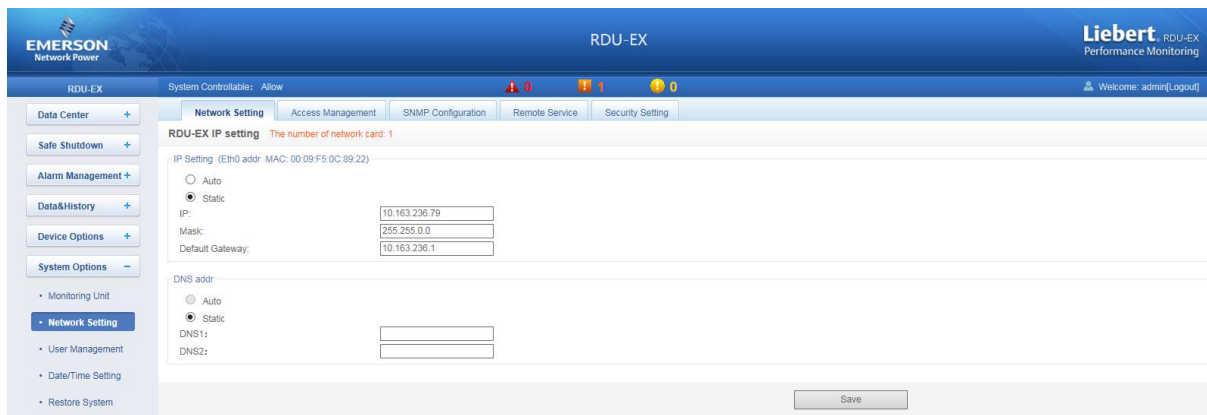


Figure 3-46 IP setting

On the page shown in Figure 3-46, you can configure the network parameters, such as IP addressing mode, **IP, Mask, GateWay, DNS1** (Preferred DNS server) and **DNS2** (Alternate DNS server). After modifying the network parameters, click the **Save** button to make the setting effective.

Note

After modifying the IP address, the system will jump to the new IP address by default. You must use the new IP address to re-login the RDU-EX.

2. Access Management

Click the **Network Setting** under the **System Options** menu, and then click the **Access Management** tab, the page shown in Figure 3-47 pops up.

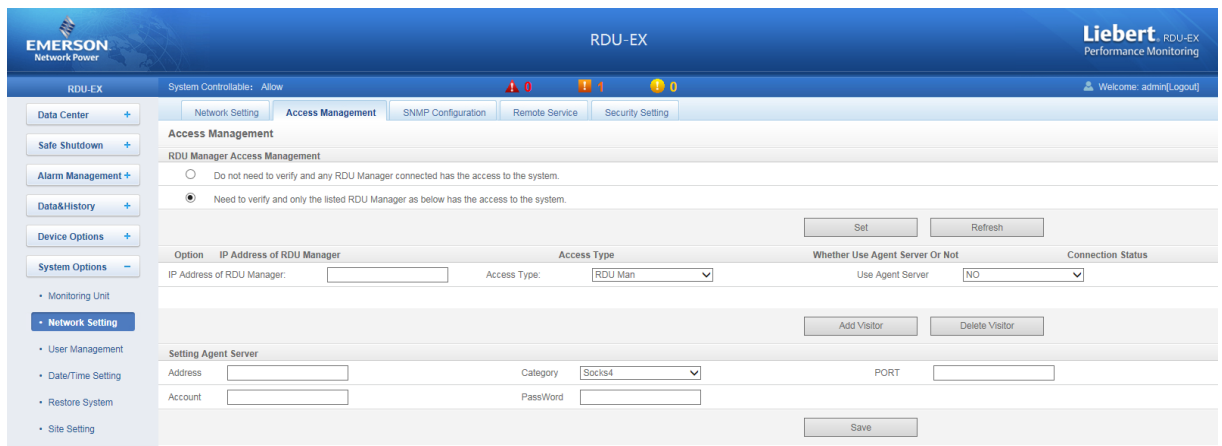


Figure 3-47 Access management

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

Note

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

3. SNMP Configuration

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

As shown in Figure 3-48, the specific setting method of SNMP V2 is as follows:

- 1) Set **NMS IP** (host IP address of SNMP agent data receiving end);
- 2) Set **Trap Level**: 'Enable' or 'disable';
- 3) Keep defaults for other items.

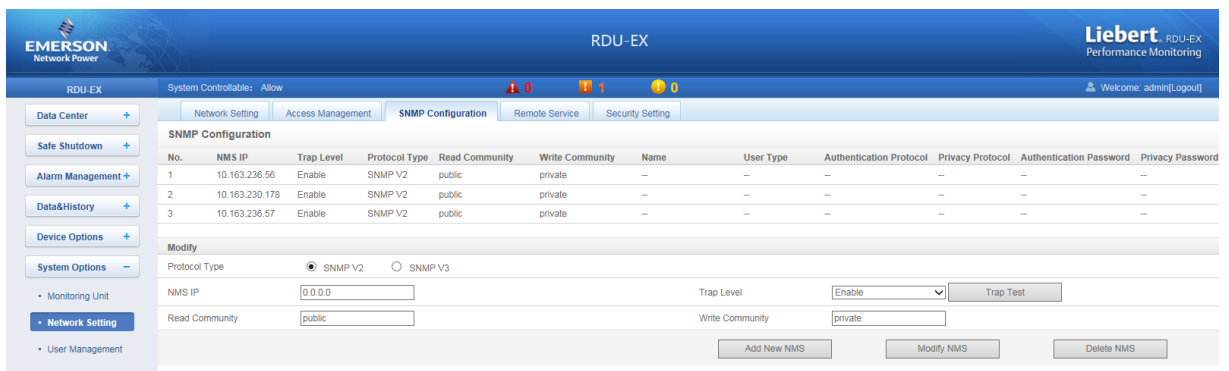


Figure 3-48 SNMP V2 setting

As shown in Figure 3-49, the specific setting method of SNMP V3 is as follows:

- 1) Set **NMS IP** (host IP address of SNMP agent data receiving end);
- 2) Set the **Trap Level**: 'Enable' or 'disable';
- 3) Set the **Name**;
- 4) Set the **User Type**: 'Authenticated & Encrypted', 'Authenticated & Not Encrypted', 'Not Authenticated & Not Encrypted';
- 5) Select **Authentication Protocol**: 'MD5', 'SHA';
- 6) Select **Privacy Protocol**: 'DES';
- 7) Self-define **Authentication Password** and **Privacy Password**.

Note

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

3. Currently, only 'DES' is supported for **Privacy Protocol**.
4. You need to self-define **Authentication Password** and **Privacy Password**, which contain at least 8 characters, and be the same as the password set by the host of SNMP agent data receiving end, or it cannot be decrypted and received.

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

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

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

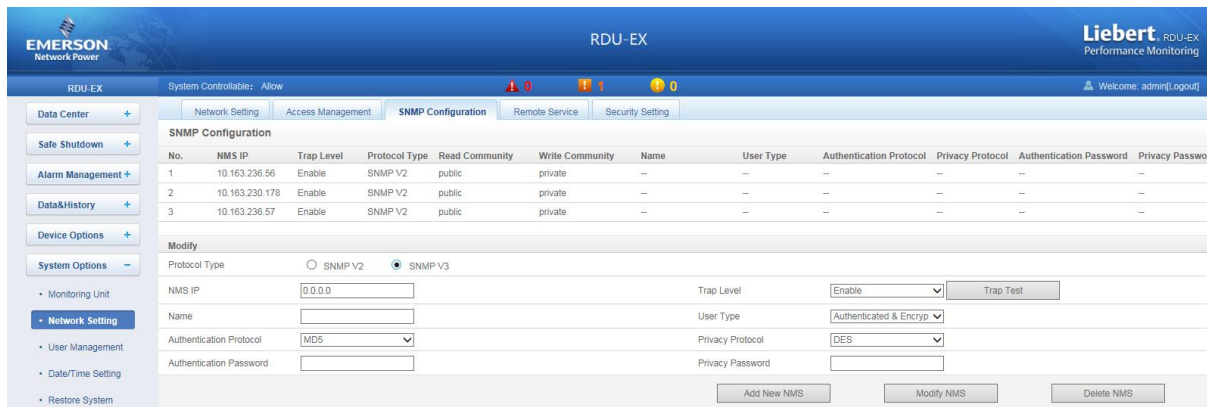


Figure 3-49 SNMP V3 setting

4. Remote Service

Click the **Network Setting** under the **System Options** menu, and then click the **Remote Service** tab, the page shown in Figure 3-50 pops up.

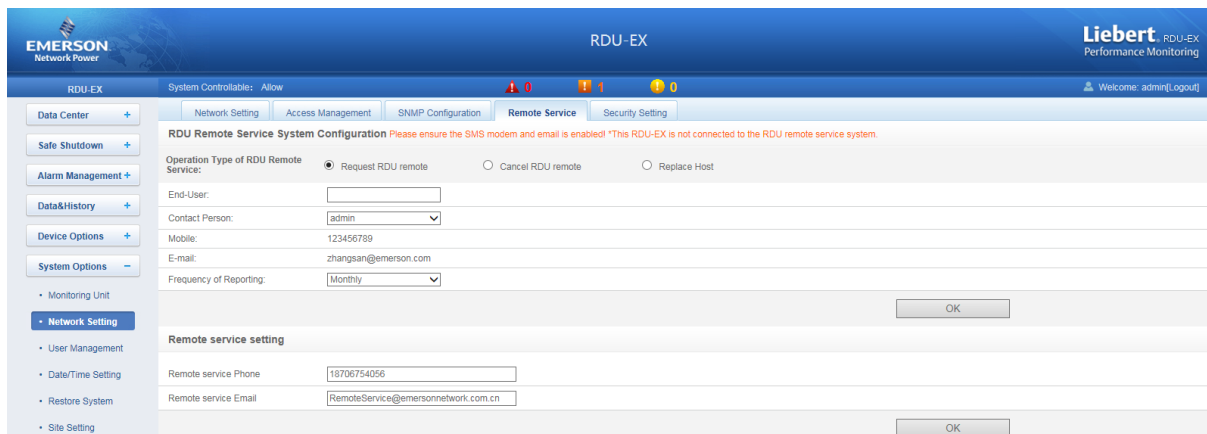


Figure 3-50 Remote service setting

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

- Request RDU remote: used to establish remote service relationship

- 1) Type the self-defined customer name in the **End-User** textbox;
- 2) Choose the contactor for remote service in the **Contact Person** textbox, when the contactor is chosen, the corresponding mobile and email will be displayed;

Note

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

- 3) Choose **Frequency of Reporting**: 'Monthly', 'Seasonal';
- 4) Click **OK** to send the remote service request.

- Cancel RDU remote: used to cancel the established remote service

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

Note

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

- **Replace Host:** used to replace the local host during remote service

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

5. Security setting

Only the administrator can browse and configure the **Security Setting**.

Click the **Network Setting** submenu in **System Options**, and then click **Security Setting**, the page as shown in Figure 3-51 is popped up.

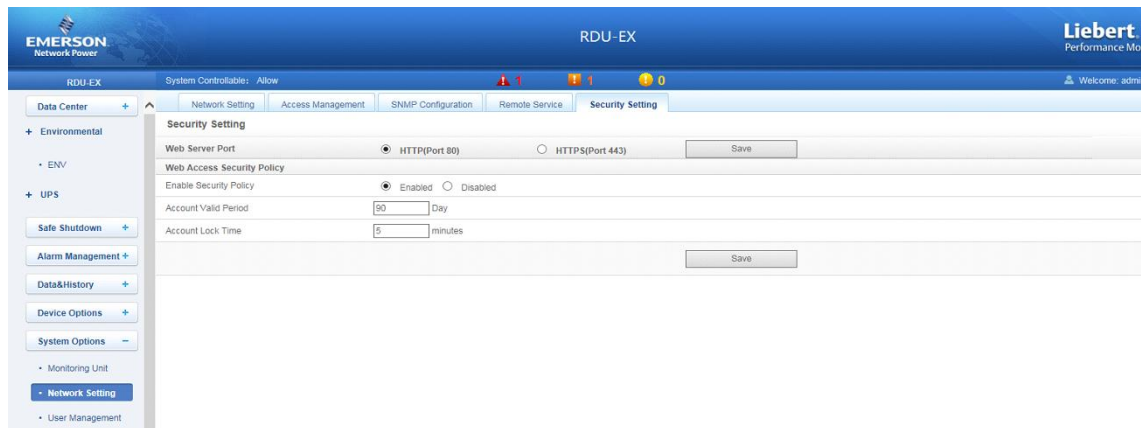


Figure 3-51 Security setting

The contents of **Security Settings** include **Web Access Mode** and **Web Access Security Strategy**.

1. **Web Access Mode:** Select whether the HTTP or HTTPS protocol is used for Web access and HTTP protocol is the default one.

After selecting the protocol, click Save button, the browser will prompt user to wait as shown in Figure 3-52.

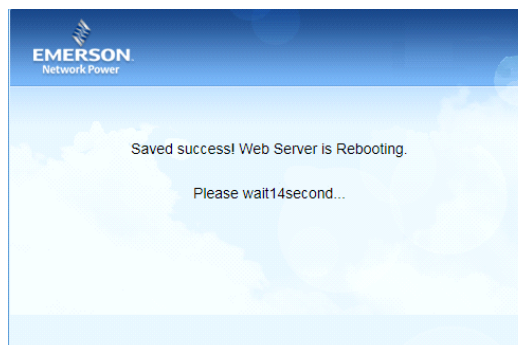


Figure 3-52 Restarting Web server

After the waiting time is exceeded, the browser will display the new access hyperlink, as shown in Figure 3-53. Click the hyperlink, the user login interface started according to a new Web access mode is popped up.

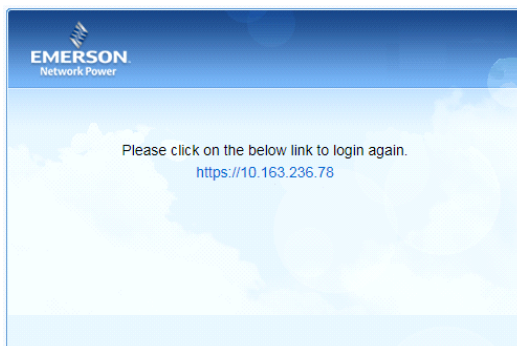



Figure 3-53 Displaying new Web access

 **Note**

Only when the HTTPS is selected in Web access mode, can the mobile terminal APP connect to the RDU-EX.

2. Web Access Security Strategy: Select whether to enable the Web Access Security Strategy, and the default is "Enable".

The Web Access Security Strategy has 4 parts: Account Locking Strategy, Password Verification for Login, Password Complexity Strategy and Password Expiration Strategy.

1) Account Locking Strategy:

When the same account has failed to log in for consecutive 5 times, you cannot enter the password to operate again until a specified time has passed. The admin account will not be locked.

The administrator can reset and unlock the locked account, and see **Unlock** in **User Management** for the operating procedures.

The locking time length can be set in the field of "**Account Locking Time**" in Figure 3-51, and the default time is 5min.

2) Password Verification for Login:

When user logs in, if the user enters the wrong user name or password, the system will immediately display a verification code to require the user to enter the verification code in the next login, as shown in Figure 3-54.

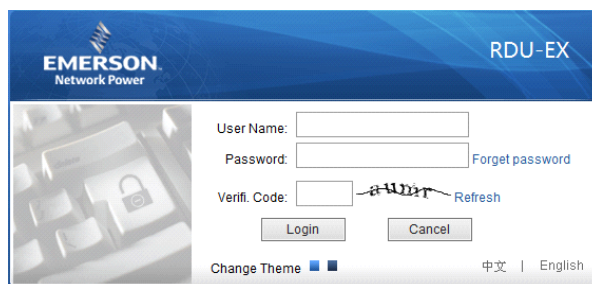


Figure 3-54 Verification code required for login

3) Password Complexity Strategy:

The user password length should have at least 6 characters which must contain two kinds of following characters: Upper case English letters (A~Z), lower case English letters (a~z), numbers (0~9), and special characters (!, \$, #, %, etc).

When the Web Access Security Strategy is enabled, the password of the existing account will not be affected, but when you create a new account or modify the existing user password, the new password must meet the requirement of complexity.

4) Password Expiration Strategy:

The user account and password are only valid in specified time when it is created or modified. The length of valid time can be edited in the field of "**User Password Effective Time**" in Figure 3-51, and the range is 0~999 days and the default time is 90 days. "0" day means the password will be valid forever.

The length of valid time of password is applicable to all the other accounts except admin, and the password of admin account will never be expired.

The administrator can refresh the valid time of some account and the new valid time will start from the set time and will end when the valid time length is expired. See "**Refresh Valid Time**" in **User Management** for detailed operating procedures.

User Management

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

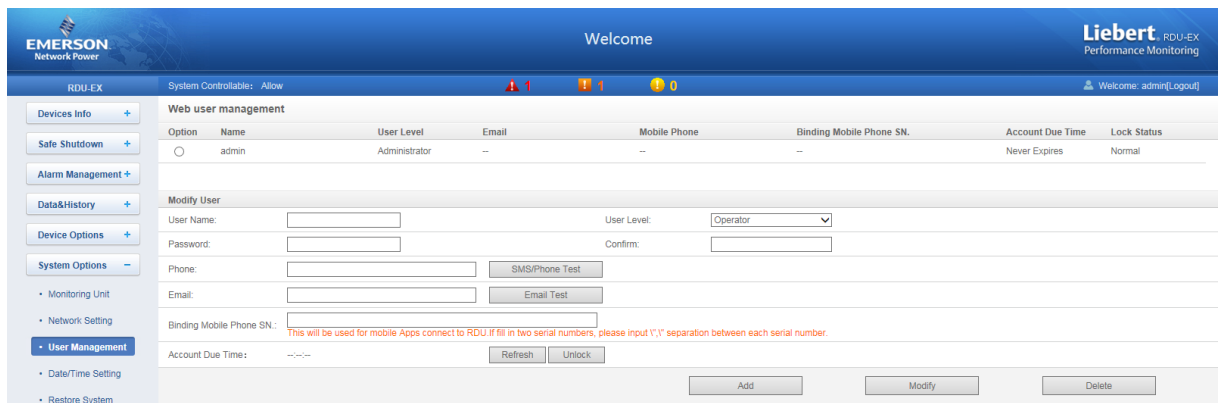


Figure 3-55 User management

On the page shown in Figure 3-55, you can add user, modify user and delete user.

●Add user

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

📖 Note

1. The characters of username can only be English letters, digits, -, and _. In addition, the initial characters must be letters or digits.
2. If the Web Access Security Strategy is enabled, there are more requirements for the password, see “Security Setting” in Network Setting”.
3. Only up to two serial numbers of bundled cell phones can be entered, and the numbers should be separated by a comma.
4. If the serial number of bundled cell phone is not entered, the system will bundle the serial numbers of the first two mobile devices that logged in through APP.
5. After bundling, the system only allows the mobile device to access the RDU-EX via APP. If you want to bundle again, you only need to delete or modify the bundled serial number.

●Delete user

1. Choose the user which needs to be deleted in the username list;
2. Click the **Delete** button to pop up the confirming dialog box, as shown in Figure 3-56.

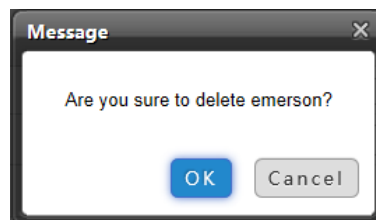


Figure 3-56 Confirming dialog box

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

📖 Note

The user of 'admin' cannot be deleted.

●Modify user

1. Choose the user which needs to be modified in the username list;
2. Modify the user information;
3. Click the **Modify** button, the dialog box of Security authentication pops up, as shown in Figure 3-13. Type the login password of current user, and click **OK** to make the modified user information effective.

Users who access RDU-EX can be divided into four user groups, and they have different security level and user authority, see Table 3-1 for detailed information.

Table 3-1 User security level

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

On the page shown in Figure 3-55, choose the current user, you can perform **SMS/Phone Test** and **Email Test**.

Before using the test function, users need to configure the SMS/Email server of current user, refer to *Alarm Notification* in 3.4.3 *Alarm Management* for details.

●SMS/Phone Test

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

●Email Alarm Notify Test


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

●Refresh expiration date

If the Web Access Security Strategy is enabled, the account expiration date will be displayed on the screen. User can click “Refresh Expiration Date” to set the expiration date, and refer to the “Password Expiration Strategy” of “Web Access Security Strategy” for the start/end time of new expiration time.

●Unlock

If the Web Access Security Strategy is enabled, for the account that has been locked, the administrator clicks “**Unlock**” to unlock the account. Refer to the “Account Locking Strategy” of “Web Access Security Strategy” in “Network Settings” for details.

 **Note**

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

Date/Time Setting

Clicking the **Date/Time Setting** under the **System Options** menu can synchronize the time. On the page shown in Figure 3-57, RDU-EX can get time from the time servers automatically. Type IP address in the **Primary Server** textbox and **Secondary Server** textbox in sequence, type a figure in **Interval to calibrate system time** textbox, select the **Time zone** and **Calibrating Protocol**, and then click the **Set** button to make the setting effective.

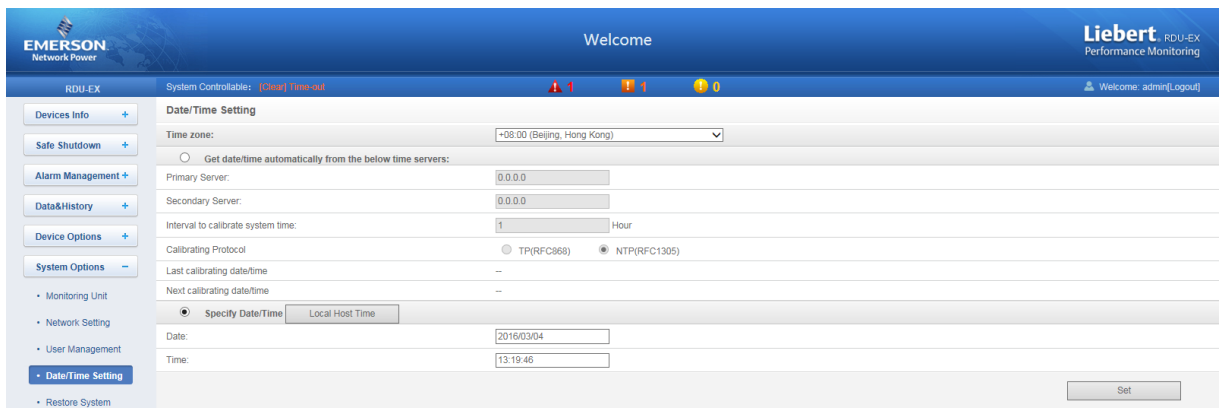


Figure 3-57 Date/time setting

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

Note

Time calibration adopts **Specify Date/Time** by default.

Restore System

Click the **Restore System** under the **System Options** menu, the page shown in Figure 3-58 pops up.

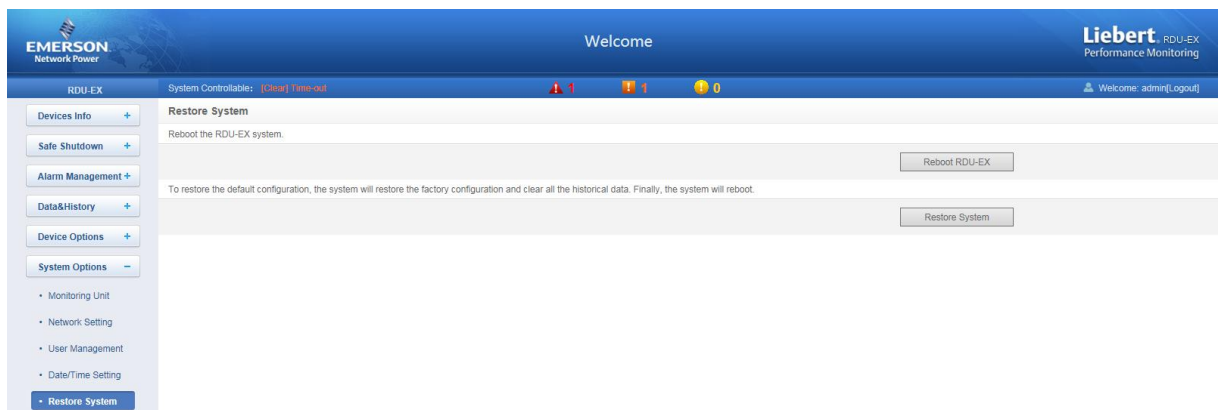


Figure 3-58 Restore System

Click the **Reboot RDU-EX** button to reboot the system.

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

Note

If you use the restore function, the RDU-EX may lose the original configuration solution. After the restore operation, make sure to wait two minute for the RDU-EX conducting complete initializing work before re-accessing it through Web.

Site Setting

Click the **Site Setting** under the **System Options** menu, the page shown in Figure 3-59 pops up.

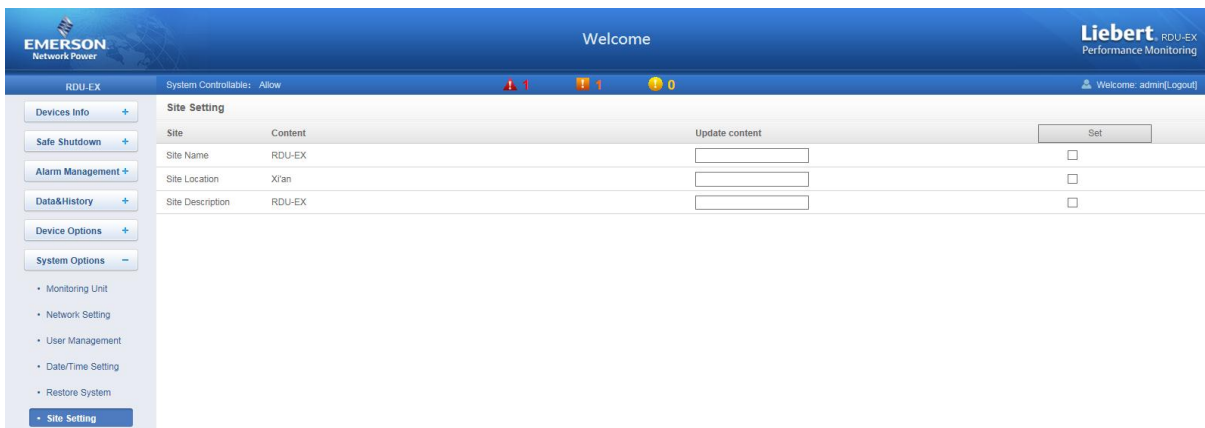


Figure 3-59 Site information setting

On the page shown in Figure 3-59, you can modify the site information of RDU-EX, including **Site Name**, **Site Location** and **Site Description**.

System Upgrade

Click the **System Upgrade** under the **System Options** menu, the page shown in Figure 3-60 pops up.

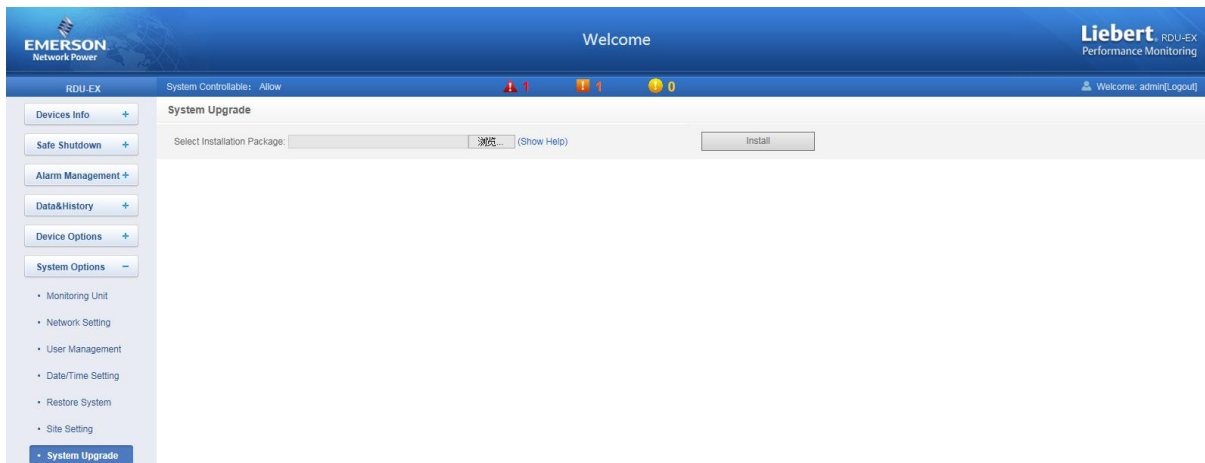



Figure 3-60 System upgrade

On the page shown in Figure 3-60, click the **Browse...** button to download configure pack (.rdp file format) from the local catalogue, and then click the **Install** button to upgrade the system.

 **Note**

The RDU-EX supports incremental upgrading function.

System Title

Click the **System Title** under the **System Options** menu, the page shown in Figure 3-61 pops up.

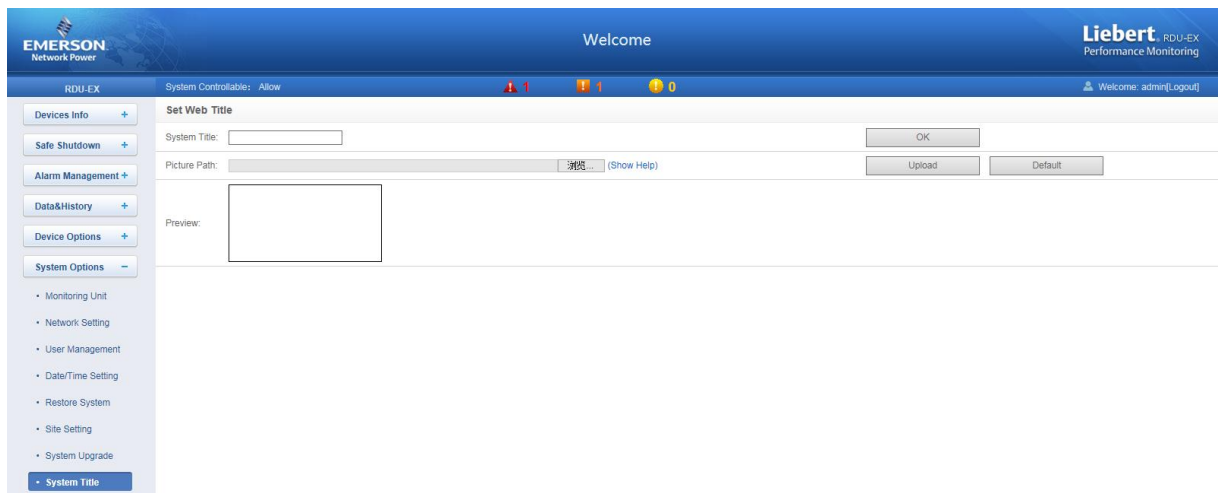


Figure 3-61 Title setting

As shown in Figure 3-61, you can replace the Logo picture in the upper right part by uploading system Logo picture. Click the **Browse...** button, choose the needed Logo picture and click the **Upload** button to upload the file to RDU-EX. Only [.gif], [.bmp], [.jpg] and [.png] format pictures are allowed, and the picture size should be less than 500K. Clicking the **Default** button can restore the default Logo picture.

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

3.4.7 Help

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

The **About RDU-EX** page displays **Software Version**, **Serial Number** and **Identify Code** of RDU-EX, You can download RDU-EX User Manual and USB debugging drive program, as shown in Figure3-62.

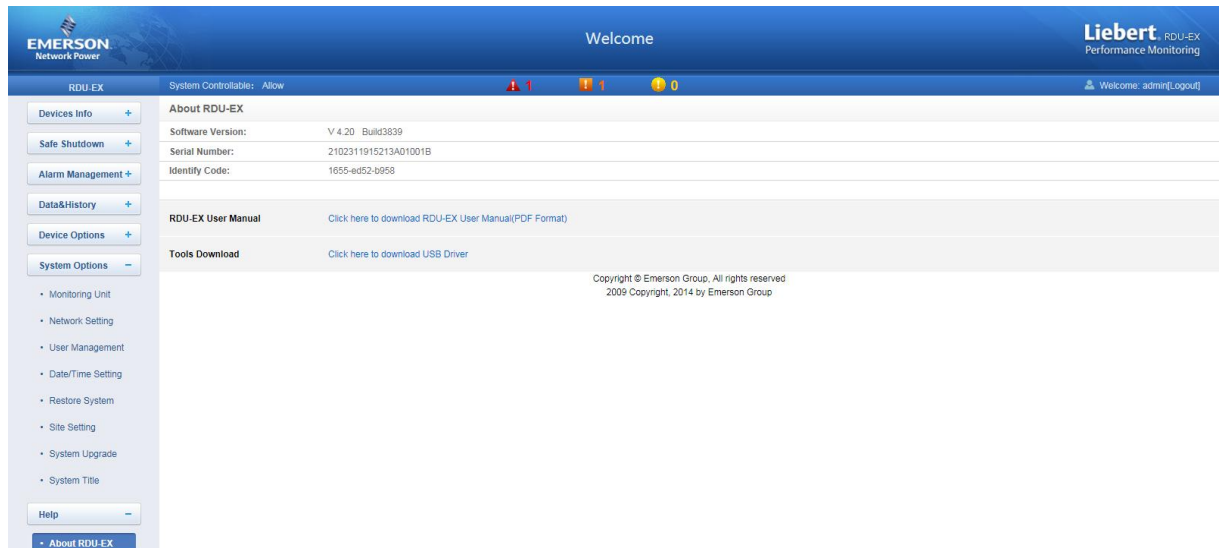


Figure 3-62 About RDU-EX

Chapter 4 Maintenance

This chapter expounds the maintenance of RDU-EX, including restoring default setting and FAQ.

4.1 Restoring Default Setting

Restoring default setting can be finished through two modes: software or hardware.

For software restoring, refer to *Restore System* in 3.4.6 *System Options*.

Hardware restoring includes restoring admin password (default username: 'admin', password: 'emerson') and IP address of RDU-EX (the default IP address is 192.168.0.252). User can recovery the hardware settings by shorting circuit pin 2 and pin 3 of jumper J18 on RDU-EX board with reference to the drawings printed on the top cover of the box. The jumper position is shown in Figure 4-1.

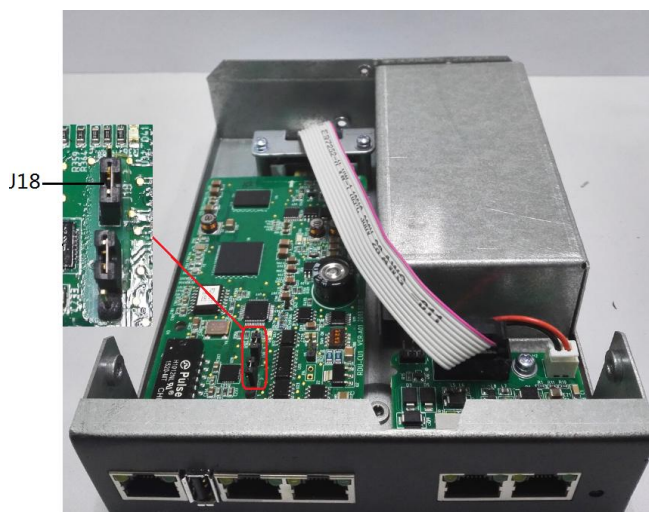


Figure 4-1 Position of jumper J18

4.2 FAQ


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

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

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

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

Q3: You have chosen the ocean blue theme, but the page still adopts crystal blue theme while you are viewing the webpage of the RDU-EX, how to deal with it?

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

Q4: After an alarm is generated, you do not receive any email or SMS notification; or when the alarm does not finish, the email or SMS notification is less than three times, how to deal with it?

A: Please perform troubleshooting according to the following procedures:

1) Please check that the SMS/Email server configuration is correct, refer to *Alarm Notification* in 3.4.3 *Alarm Management*.

2) If you do not receive the SMS notification, please check that the phone is out of service because of overdue payment;

3) If you do not receive the email notification, please click the menu **Data & History** -> **History Log** to query the system log and check whether there is a record of failure in sending email. If so, it indicates that the network is busy or the email server communication is busy.

Q5: How to deal with that there is no access to RDU-EX login page when the RDU-EX communication is normal?



A: There are three measures to solve the problem:

Step 1: Ensure that the IP address is correct;

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

Step 2: Ensure the connectivity of IP address.

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

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

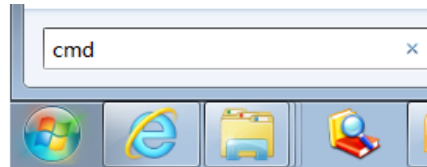
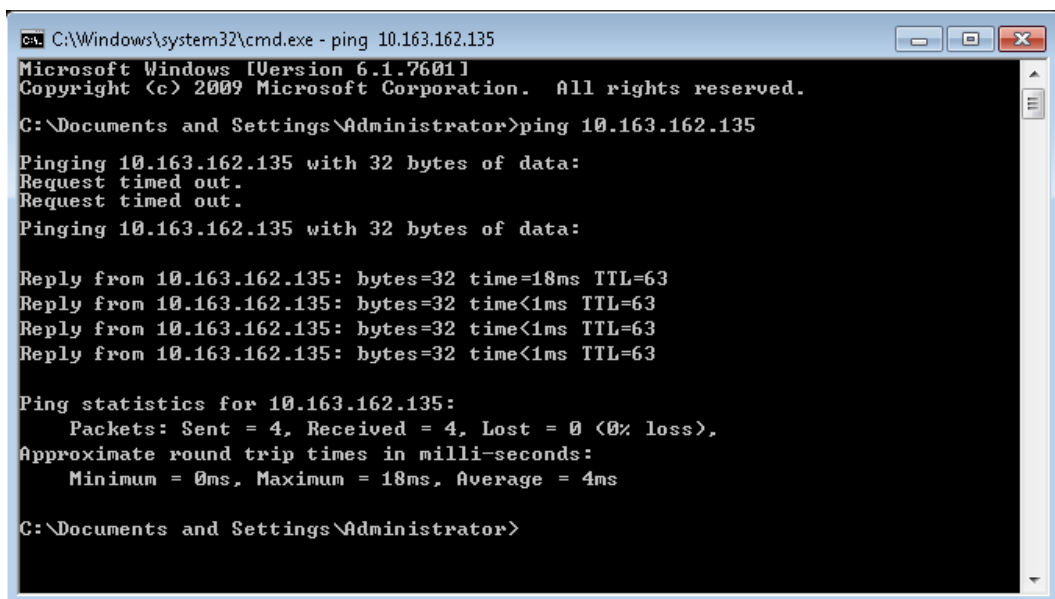


Figure 4-2 Typing 'cmd'

- 2) Press the Enter key, the page shown in Figure 4-3 pops up. Type 'ping' and IP address in the command line (for instance, 'ping 10.163.162.135') and check whether the communication is successful.

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\Windows\system32\cmd.exe - ping 10.163.162.135'. The window content shows the following text:

```
C:\Windows\system32\cmd.exe - ping 10.163.162.135
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Documents and Settings\Administrator>ping 10.163.162.135

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

Pinging 10.163.162.135 with 32 bytes of data:

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

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

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

Figure 4-3 Communication test

Step 3: If the above-mentioned steps cannot handle the problem, please use the jumper cap on the card to restore default IP. Jumper cap cover internal reference screen printing the content.

Step 4: Refer to 3.1 *Login* Preparation to complete relevant operations.

Appendix 1 Glossary


AC	Alternating Current
CA	Critical Alarm
DC	Direct Current
DI	Digital Input
IE	Internet Explorer, a Web browser developed by Microsoft®
FAQ	Frequently Asked Questions
FTP	File Transfer Protocol, used to transfer large chunks of data
HTTP	Hypertext Transfer Protocol, used to convey HTML
LED	Light Emitting Diode
MA	Moderate Alarm
NA	No Alarm
LA	Low Alarm

Appendix 2 Standard Configuration List

No.	Description	Number	Unit
1	RDU-EX monitoring unit	1	EA
2	RDU-EX Monitoring Unit Installation & Commissioning Manual	1	EA
3	Outsourced Cable Set,UH52SA1SL2,USB Cable for UH52SA1Z UPS power ,ROHS	1	EA
4	Cable and wire,IEC60320 C13 Plug,IEC60320 C14 Plug,H05VV-F,3C,1mm ² ,Black,2000mm,EU	1	EA
5	Metal Fittings/Ironware--hanger	1	EA
6	Standard Component,GB819.1-2000, Cross-head countersunk head screws M4 x 10	2	EA



VertivCo.com

© 2017 Vertiv Co. All rights reserved. Vertiv  the Vertiv logo are trademarks or registered trademarks of Vertiv Co. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness herein, Vertiv Co. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications are subject to change without notice.